Citrix Endpoint Management™

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

シトリックス エンドポイント マネジメント 49

Citrix® と顧客の責任 49

マイクロソフト エンドポイント マネージャー との統合 50

Cloud Connector とリソースの場所 50

Citrix Endpoint Management の使用を開始する 51

次のステップ 52

非推奨のお知らせ 52

シトリックス エンドポイント マネジメント サポート 52

サービスレベル契約 53

新機能 54

シトリックス エンドポイント管理 26.8.0 54

CEM 26.8.0で修正された問題 55

シトリックス エンドポイント マネジメント 26.5.0 55

CEM 26.5.0で修正された問題 56

シトリックス エンドポイント マネジメント 26.2.0 56

CEM 26.2.0で修正された問題 57

シトリックス エンドポイント マネジメント 25.11.0 57

CEM 25.11.0 で修正された問題 57

シトリックス エンドポイント マネジメント 25.9.0 58

CEM 25.9.0で修正された問題 60

シトリックス エンドポイント マネジメント 25.7.0 60

シトリックス エンドポイント マネジメント 25.5.0 60

CEM 25.5.0 で修正された問題 61

シトリックス エンドポイント マネジメント 25.3.0 61

CEM 25.3.0で修正された問題 62

シトリックス エンドポイント管理 25.1.0 62

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CEM 25.1.0で修正された問題 63
シトリックス エンドポイント管理 24.10.0 63
CEM 24.10.0で修正された問題 64
シトリックス エンドポイント マネジメント 24.8.0 65
CEM 24.8.0で修正された問題 65
シトリックス エンドポイント マネジメント 24.6.0 65
CEM 24.6.0で修正された問題 66
シトリックス エンドポイント マネジメント 24.4.0 66
CEM 24.4.0で修正された問題 67
シトリックス エンドポイント マネジメント 24.1.0 67
シトリックス エンドポイント マネジメント 23.12.0 67
現在の既知の問題 67
Citrix Endpoint Management 25.9.0 の既知の問題 67
Citrix Endpoint Management 22.6.0 の既知の問題 67
Citrix Endpoint Management 22.4.0 の既知の問題 68
Citrix Endpoint Management 21.12.0 の既知の問題 68
Citrix Endpoint Management 21.11.0 の既知の問題 68
Citrix Endpoint Management 21.10.0 の既知の問題 69
Citrix Endpoint Management 21.9.1 の既知の問題 69
Citrix Endpoint Management 21.5.0 の既知の問題 69
Citrix Endpoint Management 21.4.0 の既知の問題 69
Citrix Endpoint Management 21.2.0 の既知の問題 69
Citrix Endpoint Management 20.10.1の既知の問題 70
Citrix Endpoint Management 20.2.1の既知の問題 70
Citrix Endpoint Management 20.1.0の既知の問題 70
Citrix Endpoint Management 19.11.0の既知の問題 70
Citrix Endpoint Management 19.5.0 の既知の問題 71
Citrix Endpoint Management 19.4.1 の既知の問題 71

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 19.2.1 の既知の問題 71
Citrix Endpoint Management 19.2.0 の既知の問題 71
Citrix Endpoint Management 10.19.1 の既知の問題 71
Citrix Endpoint Management 10.18.5 の既知の問題 71
Citrix Endpoint Management 10.18.3 の既知の問題 72
Citrix Endpoint Management 10.7.4 の既知の問題 72
新機能の履歴 72
シトリックス エンドポイント マネジメント 23.9.0 72
シトリックス エンドポイント マネジメント 23.7.0 72
シトリックス エンドポイント管理 23.6.0 73
シトリックス エンドポイント管理 23.4.0 73
シトリックス エンドポイント マネジメント 23.2.0 73
シトリックス エンドポイント マネジメント 23.1.0 73
シトリックス エンドポイント マネジメント 22.12.0 73
シトリックス エンドポイント マネジメント 22.10.0 73
シトリックス エンドポイント マネジメント 22.9.0 74
シトリックス エンドポイント マネジメント 22.7.0 74
修正 74
シトリックス エンドポイントマネージメント 22.6.0 74
シトリックス エンドポイントマネージメント 22.5.0 75
シトリックス エンドポイント マネジメント 22.4.0 75
シトリックス エンドポイント マネジメント 22.3.0 76
シトリックス エンドポイント マネジメント 22.2.0 76
シトリックス エンドポイント マネジメント 22.1.0 77
シトリックス エンドポイント管理 21.12.0 77
Citrix Endpoint Management 21.12.0で修正された問題 77
シトリックス エンドポイント管理 21.11.0 77
Citrix Endpoint Management 21.11.0で修正された問題 78

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント マネジメント 21.10.1 78
Citrix Endpoint Management 21.10.1で修正された問題 78
シトリックス エンドポイント マネジメント 21.10.0 78
Citrix Endpoint Management 21.10.0で修正された問題 79
シトリックス エンドポイント マネジメント 21.9.1 79
Citrix Endpoint Management 21.9.1で修正された問題 80
シトリックス エンドポイント マネジメント 21.9.0 81
Citrix Endpoint Management 21.9.0で修正された問題 81
シトリックス エンドポイント マネジメント 21.8.0 81
Citrix Endpoint Management 21.8.0 で修正された問題 82
シトリックス エンドポイント マネジメント 21.7.1 82
Citrix Endpoint Management 21.7.1 で修正された問題 82
シトリックス エンドポイント マネジメント 21.7.0 82
シトリックス エンドポイント マネジメント 21.6.0 83
シトリックス エンドポイント マネジメント 21.5.1 85
シトリックス エンドポイント マネジメント 21.5.0 85
Citrix Endpoint Management 21.5.0で修正された問題 85
シトリックス エンドポイント マネジメント 21.4.0 85
Citrix Endpoint Management 21.4.0で修正された問題 87
シトリックス エンドポイント マネジメント 21.3.0 87
シトリックス エンドポイント マネジメント 21.2.0 88
Citrix Endpoint Management 21.2.0で修正された問題 89
シトリックス エンドポイント マネジメント 21.1.1 89
シトリックス エンドポイント マネジメント 21.1.0 90
シトリックス エンドポイント マネジメント 20.12.0 90
Citrix Endpoint Management 20.12.0で修正された問題 91
シトリックス エンドポイント マネジメント 20.11.0 91
シトリックス エンドポイント マネジメント 20.10.1 91

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 20.10.1で修正された問題 91
シトリックス エンドポイント マネジメント 20.10.0 92
Citrix Endpoint Management 20.10.0で修正された問題 92
Citrix エンドポイント管理 20.9.1 92
Citrix Endpoint Management 20.9.1で修正された問題 93
Citrix エンドポイント管理 20.9.0 93
Citrix Endpoint Management 20.9.0で修正された問題 93
シトリックス エンドポイント管理 20.8.0 93
Citrix Endpoint Management 20.8.0で修正された問題 94
シトリックス エンドポイント管理 20.7.1 94
Citrix Endpoint Management 20.7.1 で修正された問題 94
シトリックス エンドポイント マネジメント 20.7.0 95
Citrix Endpoint Management 20.7.0 で修正された問題 95
シトリックス エンドポイント マネジメント 20.6.0 95
Citrix Endpoint Management 20.6.0で修正された問題 96
シトリックス エンドポイント マネジメント 20.5.0 96
Citrix Endpoint Management 20.5.0で修正された問題 97
シトリックス エンドポイント マネジメント 20.4.1 97
Citrix Endpoint Management 20.4.1で修正された問題 98
シトリックス エンドポイント マネジメント 20.4.0 98
Citrix Endpoint Management 20.4.0で修正された問題 99
シトリックス エンドポイント マネジメント 20.3.0 99
すべての顧客向けに強化された登録プロファイルが有効化されました 99
AndroidデバイスはデフォルトでAndroid Enterpriseに登録されます 100
Citrix Endpoint Management 20.3.0で修正された問題 100
シトリックス エンドポイント マネジメント 20.2.1 101
単一環境で複数のデバイスおよびアプリ管理モードを構成する 101
Citrix Endpoint Management 20.2.1のその他の更新 107

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 20.2.1で修正された問題 107
シトリックス エンドポイント マネジメント 20.1.0 107
Citrix Endpoint Management 20.1.0の修正された問題 108
シトリックス エンドポイント マネジメント 19.12.0 108
Citrix Endpoint Management 19.12.0の修正された問題 109
シトリックス エンドポイント マネジメント 19.11.0 109
Apple ボリューム購入プログラムからApple Business Manager (ABM) およびApple School Manager (ASM) への移行 109
登録プロファイルでAndroidデバイスの登録オプションを制御 110
Citrix Endpoint Management 19.11.0で修正された問題 111
シトリックス エンドポイント マネジメント 19.10.0 112
Citrix Endpoint Management 19.10.0で修正された問題 112
シトリックス エンドポイント マネジメント 19.9.1 112
Citrix Endpoint Management 19.9.1の修正された問題 114
シトリックス エンドポイント マネジメント 19.9.0 114
Citrix Endpoint Management 19.9.0で修正された問題 115
シトリックス エンドポイント マネジメント 19.8.0 115
Citrix Endpoint Management 19.8.0 で修正された問題 116
シトリックス エンドポイント マネジメント 19.7.1 116
Citrix Endpoint Management 19.7.1で修正された問題 117
シトリックス エンドポイント マネジメント 19.6.1 117
Citrix Endpoint Management 19.6.1で修正された問題 117
シトリックス エンドポイントマネジメント 19.6.0 118
Citrix Endpoint Management 19.6.0で修正された問題 118
シトリックス エンドポイントマネジメント 19.5.0 118
Citrix Endpoint Management 19.5.0で修正された問題 120
シトリックス エンドポイント管理 19.4.1 120
Citrix Endpoint Management 19.4.1 で修正された問題 121

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント管理 19.3.1 122
Citrix Endpoint Management 19.3.1で修正された問題 122
シトリックス エンドポイント マネジメント 19.3.0 122
Citrix Endpoint Management 19.3.0で修正された問題 123
TLSバージョンの非推奨化 123
この変更がお客様に与える影響 124
実施事項 124
シトリックス エンドポイント マネジメント 19.2.1 124
Citrix Endpoint Management 19.2.1 で修正された問題 125
シトリックス エンドポイント マネジメント 19.2.0 125
Citrix Endpoint Management 19.2.0で修正された問題 126
シトリックス エンドポイント マネジメント 19.1.2 126
Citrix Endpoint Management 19.1.2 の修正された問題 127
サードパーティ通知 127
非推奨 127
非推奨および削除 127
システム要件 143
Cloud Connector の要件 143
サポートされている Active Directory 機能レベル 143
NetScaler Gateway の要件 144
Citrix Filesの要件 145
ポート要件 146
NetScaler Gateway のポート要件 146
ネットワークとファイアウォール要件 149
AutoDiscoveryサービス接続のポート要件 155
Android Enterpriseのネットワーク要件 156
アプリの要件 156
シトリックス エンドポイント マネジメントの互換性 156

© 1997–2026 Citrix Systems, Inc. All rights reserved.

モバイル生産性向上アプリ 157
MAM SDK 157
MDXツールキット 157
ブラウザのサポート 157
サポートされているデバイスオペレーティングシステム 157
オペレーティングシステムのサポートリスト 158
Androidに関する考慮事項 159
言語サポート 159
Citrix Endpoint Managementコンソールとセルフヘルプポータル 160
Citrixモバイル生産性向上アプリ 160
iOSおよびAndroid 160
右から左への言語サポート 161
FIPS 140-2 準拠 162
シトリックス エンドポイント マネジメント について 163
アーキテクチャ 169
コアリファレンスアーキテクチャ 170
Citrix Virtual Apps and Desktops™ を使用したリファレンスアーキテクチャ 171
Exchange ActiveSync 用 Citrix Endpoint Management コネクタを使用したリファレンスアーキテクチャ 172
Exchange ActiveSync 用 NetScaler Gateway コネクタを使用したリファレンスアーキテクチャ 173
Citrix Endpoint Management MDM+MAM および Intune MAM を使用したリファレンスアーキテクチャ 173
リソースの場所 174
クラウドコネクタ 174
Citrix Endpoint Managementコンポーネント 175
Citrix Endpoint Managementの技術的なセキュリティ概要 177
データフロー 177

© 1997–2026 Citrix Systems, Inc. All rights reserved.

データ分離 178
資格情報の処理 178
展開に関する考慮事項 178
その他のリソース 178
モバイル脅威防御ソフトウェアとの統合 179
シトリックス エンドポイント マネジメント と マイクロソフト エンドポイント マネージャー の統合 180
システム要件 181
MDX対応 181
マイクロソフト 181
ファイアウォールルール 181
前提条件 182
NetScaler Gatewayの構成 182
委任されたアクセス許可プロンプトへの同意 183
Citrix Endpoint ManagementとMEMの統合を構成するには 184
マイクロ VPN 用に NetScaler Gateway を構成するには 186
デバイス管理を構成するには 187
Intuneで管理されているアプリをデバイスに配信するように構成する 191
Microsoft IntuneアプリをCitrix Cloudライブラリに追加する 191
Android EnterpriseアプリをCitrix Cloudライブラリに追加する 195
管理対象アプリ間で転送されるデータの種類を制御する 202
アプリとデバイスポリシーのデリバリーグループを構成する 203
Citrix Secure Mailを構成する 205
トラブルシューティング 208
一般的な問題 208
NetScaler Gatewayに関する問題 208
OAuth エラーの条件とステータス 209
制限事項 210

© 1997–2026 Citrix Systems, Inc. All rights reserved.

既知の問題 210
サードパーティの既知の問題 210
オンボーディングとリソースのセットアップ 211
新規Citrix®のお客様向け 211
Manageボタンが利用可能になったら 212
リソースセンター 213
プロビジョニング中 214
リソースの場所を構成する 214
認証の構成 214
IdPを構成するには 214
LDAPを構成するには 215
NetScaler Gateway の構成 215
オンプレミスNetScaler Gatewayのユースケース 217
通知サーバーの構成 217
Appleデバイス用のApple Push Notification service（APNs）証明書の構成 217
Android Enterprise を構成する 218
Firebase Cloud Messaging を構成する 219
Microsoft Endpoint Manager と統合する 220
既存のShareFileアカウントをCitrix Cloudにリンクする 221
Cloud Connectors の規模とサイズに関する考慮事項 223
テスト構成 223
テスト結果 224
デバイスの登録とリソースの配信の準備 225
iOSデバイス用のApple Push Notificationサービス（APNs）証明書をセットアップする 226
Android デバイス向けに Firebase Cloud Messaging (FCM) を設定する 227
Citrix Endpoint Management AutoDiscovery サービスを設定する 227
前提条件 228
ドメインの要求 228

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WindowsデバイスのAutoDiscoveryを要求する 232

Azure AD条件付きアクセスとの統合 233

前提条件 233

Azure AD 条件付きアクセスポリシーによるデバイスコンプライアンスの構成 234

Azure AD コンプライアンス管理のために Citrix Endpoint Management を構成する 234

Azure AD で条件付きアクセス ポリシーを構成する 236

Citrix Endpoint Managementでのアプリの構成 237

ユーザー認証ワークフロー 237

デフォルトのデバイスポリシーとモバイル生産性向上アプリ 237

Citrix Endpoint Managementの構成を続行する 238

証明書と認証 242

証明書 244

LDAP認証 245

IDプロバイダー認証 246

証明書のアップロード、更新、および再発行 247

証明書のアップロード 248

キーストアをインポートするには 249

証明書をインポートするには 250

証明書の更新 255

証明書を更新するには 256

PKIサービス証明機関（CA）を更新するには 257

デバイス証明書を更新する 257

コンソールを使用してデバイス証明書を更新するには 257

REST APIを使用してデバイス証明書を更新するには 258

Citrix Secure Mail 用 APNs 証明書 258

iOS デバイス管理用 APNs 証明書 259

MDX Toolkit (iOS 配布証明書) 259

Android キーストア 260

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネットスケーラー ゲートウェイ 260
ネットスケーラー ゲートウェイ と シトリックス エンドポイント マネジメント 261
内部ネットワークへのリモートデバイスアクセスの認証を構成する 261
Citrix Gatewayサービスインスタンス（プレビュー）を追加する 262
Citrix Endpoint Managementで使用するためのオンプレミスNetScaler Gatewayの構成 263
NetScaler Gateway 構成スクリプトを使用するための前提条件 264
Citrix Endpoint Management からスクリプトバンドルをエクスポートする 264
環境にスクリプトをインストールする 266
構成をテストする 269
複数のドメインの認証を構成する 270
NetScaler Gatewayの構成 270
シトリックス エンドポイント マネジメント の構成 271
特定のURLへのインバウンド接続要求を破棄する 272
ドメインまたはドメインとセキュリティトークン認証 272
LDAPについて 273
Citrix Endpoint ManagementでLDAP接続を追加または編集するには 273
LDAP準拠ディレクトリを削除するには 276
ドメインとセキュリティトークン認証を構成する 276
LDAP設定の構成 276
NetScaler Gateway設定の構成 277
Citrix PINとユーザーパスワードキャッシュを有効にする 278
ドメインおよびセキュリティトークン認証用にNetScaler Gatewayを構成する 278
クライアント証明書または証明書とドメイン認証 278
前提条件 279
Microsoft Management Consoleに証明書スナップインを追加する 280
テンプレートを証明機関に追加する 283
CAサーバーからPFX証明書を作成する 284
Citrix Endpoint Managementへの証明書のアップロード 289

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書ベースの認証用のPKIエンティティの作成 290
資格情報プロバイダーの構成 291
証明書ベースの認証を使用するようにCitrix Secure Mailを構成する 293
Citrix Endpoint ManagementでのNetScaler Gateway証明書配信の構成 293
Citrix PINとユーザーパスワードのキャッシュを有効にする 294
クライアント証明書構成のトラブルシューティング 294
クライアント証明書がモバイルデバイスに配信されたかどうかを確認するには 296
クライアント証明書ネゴシエーションが有効になっているかどうかを検証するには 296
PKIエンティティ 297
一般的なPKIの概念 298
CA証明書について 298
Microsoft 証明書サービス 299
Microsoft Certificate Servicesエンティティを追加する 299
NetScaler Gateway証明書失効リスト（CRL） 302
裁量CA 302
CAの証明書を生成してインポートする 303
裁量CAを追加する 306
資格情報プロバイダーを構成する 308
資格情報プロバイダー 312
証明書の発行方法 313
証明書の配信 314
証明書の失効 315
証明書の更新 316
資格情報プロバイダーの作成 316
APNs証明書 321
証明書署名要求を作成する 322
macOS のキーチェーンアクセスを使用して CSR を作成する 322
Microsoft IISを使用してCSRを作成する 323

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OpenSSL を使用して CSR を作成する 323
CSR に署名する 324
署名済みのCSRをAppleに提出してAPNs証明書を取得する 326
CSRを完了し、PKCS #12ファイルをエクスポートする 326
macOS のキーチェーンアクセスを使用して PKCS #12 ファイルを作成する 327
Microsoft IIS を使用して PKCS #12 ファイルを作成する 328
OpenSSLを使用してPKCS #12ファイルを作成する 328
APNs 証明書を Citrix Endpoint Management にインポートする 329
APNs 証明書を更新する 329
Citrix FilesとのシングルサインオンのためのSAML 330
前提条件 331
ShareFileアクセスを構成する 332
ラップされた Citrix Files MDX アプリの SAML を設定する 332
Citrix Filesモバイルアプリを検証する 333
Citrix Secure Mailで検証する 333
その他のCitrix Filesクライアント向けにNetScaler Gatewayを構成する 333
ホームページのリダイレクトを無効にする 334
Citrix Filesセッションポリシーとリクエストプロファイルの作成 334
NetScaler Gateway仮想サーバーでポリシーを構成する 336
Citrix Files.com SSO設定を変更する 337
構成を検証する 339
Citrix Cloud を介した Azure Active Directory による認証 339
前提条件 340
IDプロバイダーとしてAzure Active Directoryを使用するようにCitrix Cloudを構成する 341
Citrix Endpoint Management の IdP タイプとして Citrix ID を構成する 342
Citrix Secure Hubの認証フロー 342
Azure Active Directory グループベースの管理による認証 343
主な機能強化 343

© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能フラグ 343
前提条件 343
構成手順 344
MAM登録のためのNetScaler Gateway経由のAzure Active Directory認証 344
前提条件 344
MAMのIdPとしてAzure ADを構成する 345
予期される動作 346
Citrix Cloud を介した Okta との認証 348
前提条件 348
OktaをIDプロバイダーとして使用するようにCitrix Cloudを構成する 349
Citrix Endpoint ManagementのIdPタイプとしてCitrix IDを構成する 349
Citrix Secure Hubの認証フロー 350
MAM登録のためのNetScaler Gatewayを介したOktaによる認証 351
前提条件 351
シトリックス エンドポイント マネジメントでネットスケーラー ゲートウェイを構成する 351
オンプレミスNetScaler Gatewayを準備する 352
Oktaを構成する 353
予期される動作 356
Citrix Cloudを介したオンプレミスのNetScaler Gatewayでの認証 357
前提条件 357
NetScaler GatewayをIDプロバイダーとして使用するようにCitrix Cloudを構成する 358
Citrix IDプロバイダーをCitrix Endpoint ManagementのIdPタイプとして構成する 358
Citrix Secure Hub認証フロー 359
nFactor認証 359
前提条件 360
nFactor認証を構成する 361
既存のNetScaler Gatewayで従来のポリシーをAdvanced認証ポリシーに更新する 361
Advancedポリシーを使用してNetScaler Gatewayのセットアップを構成する 361

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーアカウント、役割、および登録 363
ユーザーアカウントについて 364
登録セキュリティモードを構成する 364
登録セキュリティモードを編集するには 366
登録セキュリティモードをデフォルトとして設定するには 368
登録セキュリティモードを無効にするには 368
ローカルユーザーアカウントの追加、編集、ロック解除、または削除 368
ローカルユーザーアカウントを追加するには 369
ローカルユーザーアカウントを編集するには 370
ローカルユーザーアカウントのロックを解除するには 371
ローカルユーザーアカウントを削除するには 372
Active Directoryユーザーを削除するには 372
ユーザーアカウントのインポート 372
プロビジョニングファイルの形式 374
ユーザープロビジョニングコンテンツの例 374
ユーザー属性プロビジョニングコンテンツの例 375
グループの追加または削除 375
ローカルグループを追加するには 375
グループを削除するには 377
ワークフローの作成と管理 379
ワークフローの詳細を表示および削除するには 381
登録プロファイル 381
グローバル登録プロファイル 382
登録プロファイル、デリバリーグループ、および登録 383
登録プロファイルを作成するには 384
通知 385
前提条件 386
SMTP サーバーを構成する 386

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SMTPサーバーの追加 387
通知テンプレートの作成と更新 389
通知テンプレートの追加 389
通知テンプレートを編集する 392
通知テンプレートを削除する 392
RBACでロールを構成する 392
RBAC機能を使用する 393
役割の作成または編集 393
Citrix Cloud管理者への役割の追加 396
事前定義されたロール 396
管理者ロール 397
ユーザーロール 410
ライセンス 413
デバイス管理 414
デバイス管理ワークフロー 415
登録招待 417
前提条件 418
登録招待を作成する 418
ユーザーに登録招待を送信するには 419
グループに登録招待を送信するには 421
インストールリンクを送信するには 423
プラットフォーム別の登録セキュリティモード 425
セキュリティアクション 430
Citrix Endpoint Managementコンソールからデバイスを削除する 435
デバイスを選択的にワイプする 435
デバイスを削除する 436
アプリのロック、ロック解除、ワイプ、またはワイプ解除 436
アプリのワイプとワイプ解除 436

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスに関する情報の取得 437
プロビジョニングファイルからのデバイスのインポート 438
デバイスに展開する 439
デバイスに通知を送信する 439
デバイステーブルをエクスポートする 440
ユーザーデバイスを手動でタグ付けする 440
Active Directoryユーザー属性をカスタマイズする 441
デバイスの検索 442
デバイスプロビジョニングファイル形式 442
アレクサ フォー ビジネス 444
Citrix Endpoint Management への AWS アカウントの認証 444
Citrix Endpoint Management でアレクサ フォー ビジネスを構成する 445
ルームプロファイルの構成 446
会議室の構成 447
スキルグループを構成する 448
スキルグループでスキルを利用可能にする 450
会議設定を構成する 451
Android 453
デバイス管理からAndroid Enterpriseへの移行 453
デバイス管理の非推奨化の影響 453
分析 454
要件のマッピング 455
概念実証 457
展開 458
アンドロイド エンタープライズ 458
Android Enterprise の利用開始 459
Citrix Endpoint Managementで管理対象Google Playを使用する 462
デバイス展開シナリオとプロファイル 464

© 1997–2026 Citrix Systems, Inc. All rights reserved.

登録セキュリティ 466
要件 467
Citrix Endpoint ManagementをGoogle Playに接続する 467
Android EnterpriseユーザーにCitrixモバイル生産性アプリを提供する 469
登録プロファイルの作成 477
Android Enterpriseワークプロファイルデバイスのプロビジョニング 483
Android Enterprise完全管理デバイスのプロビジョニング 483
専用のAndroid Enterpriseデバイスのプロビジョニング 501
ワークプロファイルまたは会社所有デバイス上のワークプロファイルを持つAndroid Enterpriseの完全管理対象デバイスのプロビジョニング 502
Citrix Endpoint ManagementコンソールでのAndroid Enterpriseデバイスの表示 503
Android Enterpriseのデバイスおよびアプリポリシーを構成する 504
セキュリティアクション 507
Android Enterpriseエンタープライズの登録解除 508
Android Enterpriseアプリの配布 509
マネージドアプリストアアプリ 510
MDXアプリ 512
エンタープライズアプリ 515
MDX対応のプライベートアプリ 518
Google Workspace (旧 G Suite) のお客様向けレガシー Android Enterprise 530
Android Enterprise アカウントを作成する 531
Android Enterpriseサービスアカウントを設定し、Android Enterprise証明書をダウンロードする 532
EMMへのバインド 541
P12証明書をインポートする 542
Android Enterpriseサーバー設定をセットアップする 543
SAMLベースのシングルサインオンを有効にする 543
Android Enterpriseデバイスポリシーを設定する 544

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android Enterpriseアカウント設定を構成する 545
Citrix Endpoint Management向けGoogle Workspaceパートナーアクセスを設定する 546
Android Enterprise デバイスの登録 548
Android Enterpriseエンタープライズの登録解除 548
Android Enterprise での完全管理対象デバイスのプロビジョニング 550
Android Enterprise でのワークプロファイルデバイスのプロビジョニング 558
アンドロイドOS 558
サポートされている登録方法 559
Androidデバイスポリシーを構成する 562
Androidデバイスを登録する 563
セキュリティアクション 564
Firebase クラウド メッセージング 565
前提条件 566
アーキテクチャ 566
FCM用にGoogleアカウントを設定するには 566
FCM用にCitrix Endpoint Managementを構成するには 568
構成をテストするには 570
管理対象構成フィードバックのサポート（テクニカルプレビュー） 571
前提条件 571
構成フィードバックを管理および利用する手順 572
トラブルシューティング 574
Android セーフティネット 574
必要なSafetyNet Attestation APIリクエストの数を推定する 574
SafetyNet APIキーを取得する 575
Android SafetyNetを有効にする 575
Android SafetyNetの結果を表示する 576
プレイ インテグリティ API 577
Play Integrity API を有効にする 577

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Play Integrity API アッテステーションの結果を表示および分析する 578
制限事項 579
サムスン 580
サポートされている登録方法 581
Samsungライセンスキーの展開 581
Samsungデバイスポリシーの構成 581
セキュリティアクション 581
ネットワークアクセスコントロール 582
サポートされているNAC準拠フィルター 583
構成の概要 584
Citrix Endpoint ManagementでNACフィルターを有効にする 585
NACをサポートするようにNetScaler Gatewayポリシーを更新する 585
Apple 589
iOS 589
iOS 14の互換性 590
開放しておく必要があるAppleホスト名 591
サポートされている登録方法 591
iOSデバイスポリシーを構成する 595
iOSデバイスを登録する 596
セキュリティアクション 598
macOS 604
開放しておく必要があるAppleホスト名 605
サポートされている登録方法 605
macOSデバイスポリシーを構成する 606
macOSデバイスの登録 606
セキュリティアクション 608
ブートストラップトークン 610
Apple Deployment Programs を介したデバイスの展開 610

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件 611
ABMまたはASMに登録する 611
ABMまたはASMアカウントをCitrix Endpoint Managementに接続する 612
デバイスを注文する 626
デバイスをCitrix Endpoint Managementに割り当てる 626
コンテンツを一括購入し、Citrix Endpoint Managementに同期する 627
デバイスポリシーとアプリの展開ルールを構成する 627
Appleデバイスを一括登録する 628
一括登録について 628
ユーザーがADP対応デバイスを登録する方法 629
ADP対応デバイスを再登録する 630
Apple Configurator 2 を使用してデバイスを展開する 631
Apple Configurator 2 を使用してデバイスを ABM または ASM に追加する 633
ADP トークンを更新する 633
Apple Education機能との統合 634
アップルスクールマネージャー 634
前提条件 634
iPad用Classroomアプリ 635
Apple School Managerユーザーのパスワードを追加する 635
Citrix Endpoint Management にリソースとデリバリーグループを計画して追加する 637
教員および学生デバイスの登録をテストする 642
デバイスの配布 643
教師、生徒、クラスのデータを管理する 644
紛失または盗難にあったデバイスの管理 645
共有iPad 647
共有iPadの前提条件 647
共有iPadを構成する 647
Appleアプリの配布 657

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ配布の一般的な手順 658
公開App Storeアプリ 660
Apple Volume Purchase で配信されるパブリックアプリストアアプリ 662
エンタープライズアプリ 664
MDXアプリ 667
Apple Volume Purchaseを使用して配布されるMDXアプリ 669
カスタムアプリ 673
MDX対応カスタムアプリ 675
オプションアプリ（iOS/iPadOSのみ） 679
ネットワークアクセスコントロール 679
サポートされているNAC準拠フィルター 680
構成の概要 681
Citrix Endpoint ManagementでNACフィルターを有効にする 682
NACをサポートするようにNetScaler Gatewayポリシーを更新する 682
Windows 686
Windowsデスクトップおよびタブレット 686
サポートされている登録方法 687
Windowsデスクトップおよびタブレットデバイスポリシーの構成 689
Azure Active Directory を介した Windows 10 および Windows 11 デバイスの登録 689
AutoDiscoveryサービスを使用してWindowsデバイスを登録する 691
Windowsの一括登録 692
セキュリティアクション 692
Citrix Endpoint ManagementをAzure ADに接続する 692
Workspace Environment Management™と統合した場合のデバイス管理 694
BitLocker回復キー 694
Windowsデバイスを一括登録する 696
デバイスごとにデバイスを割り当てる 696
デバイスの一括追加 698

© 1997–2026 Citrix Systems, Inc. All rights reserved.

一括登録の構成 699
プロビジョニングパッケージの作成と適用 700
デバイスをすぐに一括登録する 701
デバイスポリシー 703
前提条件 704
デバイスポリシーを追加する 704
展開ルール、割り当て、およびスケジュールを構成するには 706
デバイスからデバイスポリシーを削除する 709
デバイスポリシーを編集する 709
ポリシー展開ステータスを確認する 710
追加されたデバイスポリシーのリストをフィルターする 711
デバイスポリシーの概要 711
プラットフォーム別のデバイスポリシー 722
AirPlayミラーリングデバイスポリシー 733
iOS設定 733
macOS設定 734
AirPrintデバイスポリシー 735
iOS設定 736
アプリの権限デバイスポリシー 736
Android Enterpriseの設定 737
APNデバイスポリシー 738
iOS設定 739
Android設定 740
アプリケーションアクセスデバイスポリシー 741
iOSおよびAndroid（レガシーDA）設定 742
アプリのアクセスコンプライアンスに基づいた自動アクションを構成する 742
アプリ属性デバイスポリシー 743
関連ドメインについて 743

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定 744
App StoreでアプリのバンドルIDを見つける 744
アプリ構成デバイスポリシー 745
iOS設定 745
Windowsデスクトップ/タブレット設定 746
アプリインベントリデバイスポリシー 747
iOS、macOS、Android（レガシーDA）、Android Enterprise、およびWindowsデスクトップ/タブレット 748
`Win32`アプリのインベントリと削除 748
誤ったプロダクトコードによって引き起こされるアプリのインストールとアンインストールの問題 749
Application Guard デバイスポリシー 749
要件 750
Windows デスクトップおよびタブレットの設定 750
アプリロックデバイスポリシー 751
iOS設定 752
iPadをキオスクとして構成する 753
Android (レガシーDA) 設定 754
Windowsデスクトップおよびタブレットの設定 755
App Lockの前提条件 755
WindowsからポリシーXMLファイルを構成およびエクスポートするには 756
ポリシーXMLファイルをCitrix Endpoint Managementにインポートするには 756
アプリロックポリシーの適用を停止するには 756
アプリ通知デバイスポリシー 757
iOS設定 757
アプリのアンインストールデバイスポリシー 758
iOSおよびmacOSの設定 759

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android (レガシーDA)、Android Enterprise、およびWindowsデスクトップ/タブレットの設定 759

対応するパブリックアプリストアアプリのインストール後にエンタープライズアプリを自動的にアンインストールする 760

アプリのアンインストール制限デバイスポリシー 760

Amazonの設定 760

管理対象アプリの自動更新デバイスポリシー 761

BitLockerデバイスポリシー 762

要件 763

Windowsデスクトップおよびタブレットの設定 764

Bluetoothデバイスポリシー 769

iOS設定 769

カレンダー (CalDav) デバイスポリシー 770

iOS 設定 770

macOS設定 770

携帯電話デバイスポリシー 771

iOS設定 771

接続スケジューリングデバイスポリシー 772

AndroidおよびAndroid Enterpriseの設定 772

接続時間枠の定義 773

連絡先 (CardDAV) デバイスポリシー 774

iOS 設定 774

macOS設定 775

資格情報デバイスポリシー 776

iOS設定 776

macOS設定 778

Android設定 779

Android エンタープライズ設定 780

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windowsデスクトップ/タブレット設定 782
カスタムXMLデバイスポリシー 783
Windowsデスクトップ/タブレットの設定 784
Windows AutoPilot を使用してデバイスをセットアップおよび構成する 784
前提条件 784
Windows 11デバイスにシングルアプリキオスクを展開する 786
宣言型デバイス管理ポリシー 788
アプリ設定デバイスポリシー 789
前提条件 789
iOS設定 789
外部インテリジェンス設定デバイスポリシー 790
前提条件 790
iOS設定 791
Googleアカウントデバイスポリシー 791
前提条件 791
iOS設定 792
インテリジェンス設定デバイスポリシー 792
前提条件 792
iOS設定 792
パスコードデバイスポリシー 793
前提条件 794
iOS設定 794
ソフトウェアアップデート強制デバイスポリシー 795
前提条件 795
iOS設定 796
ソフトウェアアップデート設定デバイスポリシー 797
前提条件 797
iOS設定 798

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステータスサブスクリプションデバイスポリシー 800
前提条件 800
iOS設定 800
ユーザーIDデバイスポリシー 800
前提条件 801
iOS設定 801
Defenderデバイスポリシー 801
Windowsデスクトップおよびタブレットの設定 802
Device Guard デバイスポリシー 803
前提条件 803
Windows デスクトップおよびタブレットの設定 803
デバイス正常性構成証明デバイスポリシー 804
Windowsデスクトップ/タブレット設定 805
Microsoft Cloudを使用してDHAを構成する場合 805
オンプレミスのWindows DHAサーバーを使用してDHAを構成する場合 806
デバイス名デバイスポリシー 806
iOSおよびmacOSの設定 806
教育構成デバイスポリシー 807
iOS設定 807
ポリシー内のクラス情報を編集するには 809
Endpoint Managementオプションデバイスポリシー 809
Android設定 810
アンドロイド エンタープライズ 設定 811
Citrix Endpoint Management アンインストールデバイスポリシー 811
Android設定 811
Exchangeデバイスポリシー 812
iOS設定 812
同期されたExchangeサービス 814

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS設定 815
Windowsデスクトップ/タブレット設定 817
ファイルデバイスポリシー 818
アンドロイド エンタープライズ 設定 818
Android設定 819
FileVaultデバイスポリシー 820
macOS設定 820
ファイアウォールデバイスポリシー 823
macOS設定 823
Windowsデスクトップおよびタブレットの設定 824
フォントデバイスポリシー 824
iOS設定 825
macOS設定 825
ホーム画面レイアウトデバイスポリシー 825
iOS設定 826
iOSおよびmacOSプロファイルデバイスポリシーのインポート 827
ユースケース 827
Apple Configurator 2を使用して構成プロファイルを作成する 829
Profile Creator を使用して構成プロファイルを作成する 829
iOS および macOS の設定 830
Androidデバイスのコンプライアンス強制 (テクニカルプレビュー) 830
Androidデバイスのコンプライアンス管理手順 831
トラブルシューティング 834
キーガード管理デバイスポリシー 836
Android Enterpriseの設定 837
キオスクデバイスポリシー 839
Windowsデスクトップおよびタブレットの設定 840
Android Enterpriseの設定 842

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Knox Platform for Enterprise Key デバイスポリシー 843
アンドロイド エンタープライズ 設定 843
ランチャー構成デバイスポリシー 844
Android Enterprise および Android の設定 844
LDAPデバイスポリシー 845
iOS設定 845
macOS設定 846
ロケーションデバイスポリシー 847
iOS設定 848
Android (レガシーDA) 設定 849
Android Enterpriseの設定 851
ワークプロファイルを持つ完全に管理されたデバイスに適用 851
管理対象デバイス 852
ワークプロファイル 854
ロック画面メッセージデバイスポリシー 854
iOS設定 854
メールデバイスポリシー 855
iOSおよびmacOSの設定 855
マネージド構成ポリシー 857
前提条件 858
アプリごとのVPNの要件 858
制限事項 859
Android Enterprise の設定 859
Android Enterprise 用の VPN プロファイルを構成する 859
Citrix SSO 用の Android Enterprise 管理対象構成を作成する 860
デバイスからのVPNプロファイルへのアクセス 866
Zebra OEMConfig を使用したZebra Androidデバイスの管理 867
Zebra OEMConfigアプリのAndroid Enterprise管理対象構成を作成する 867

© 1997–2026 Citrix Systems, Inc. All rights reserved.

事前定義されたブックマークでChromeブラウザを管理する 868
管理対象構成フィードバックのサポート (テクニカルプレビュー) 870
マネージド ドメイン デバイス ポリシー 870
iOS設定 870
最大常駐ユーザーデバイスポリシー 872
iOS設定 873
MDMオプションデバイスポリシー 873
iOS設定 874
ネットワークデバイスポリシー 875
前提条件 875
iOS設定 876
iOSにおけるWPA、WPA Personal、Any (Personal) の構成設定 879
iOS向けWEP Enterprise、WPA Enterprise、WPA2 Enterprise、WPA3 Enterprise、任意の (エンタープライズ) の設定 879
macOS設定 881
macOSのWPA、WPAパーソナル、WPA 2パーソナル、任意（パーソナル）設定 884
macOSのWEPエンタープライズ、WPAエンタープライズ、WPA2エンタープライズ、任意（エンタープライズ）設定 884
アンドロイド エンタープライズ 設定 886
Android EnterpriseのOpen、共有設定 886
Android Enterprise の WPA、WPA-PSK、WPA2、WPA2-PSK 設定 886
Android Enterprise 向け 802.1x 設定 887
Android (レガシー DA) 設定 888
Android のオープン、共有設定 888
Android の WPA、WPA-PSK、WPA2、WPA2-PSK 設定 888
Android の 802.1x 設定 889
Windowsデスクトップ/タブレットの設定 889
Windows 10およびWindows 11のオープン設定 890

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows 10およびWindows 11のWPA Personal、WPA-2 Personal設定 890
Windows 10およびWindows 11のWPA-2 Enterprise設定 890
ネットワーク使用状況デバイスポリシー 891
iOS設定 891
Officeデバイスポリシー 892
Windowsデスクトップ/タブレット設定 892
組織情報デバイスポリシー 893
iOS設定 893
OS更新デバイスポリシー 893
iOS設定 895
macOSの設定 896
iOSおよびmacOSのアップデートアクションのステータスを取得 897
Windowsデスクトップおよびタブレットの設定 899
Citrix Endpoint ManagementがWindowsデスクトップおよびタブレットデバイスへの承認済みアップデートを処理する方法 903
Android Enterpriseの設定 906
パスコードデバイスポリシー 906
iOS設定 907
macOS設定 909
Android (レガシーDA) 設定 911
Android Enterpriseの設定 913
Windowsデスクトップ/タブレットの設定 918
パスコードロック猶予期間デバイスポリシー 919
iOS設定 919
パーソナルホットスポットデバイスポリシー 919
iOS設定 919
プロファイル削除デバイスポリシー 920
macOS設定 920

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プロビジョニングプロファイルデバイスポリシー 920
iOS設定 921
プロビジョニングプロファイル削除デバイスポリシー 921
iOS設定 922
プロキシデバイスポリシー 922
前提条件 922
iOS設定 922
制限デバイスポリシー 923
iOS設定 924
macOS設定 951
Android設定 959
アンドロイド エンタープライズ 設定 960
Windowsデスクトップ/タブレット設定 979
Amazon の設定 981
ローミングデバイスポリシー 982
iOS設定 982
SCEP デバイスポリシー 983
iOS 設定 983
macOS の設定 985
Siriと音声入力のポリシー 986
SSOアカウントデバイスポリシー 988
iOS設定 989
ストアデバイスポリシー 990
iOS、Android、およびWindowsデスクトップ/タブレットの設定 990
購読済みカレンダーデバイスポリシー 990
前提条件 990
iOS設定 990
利用規約デバイスポリシー 991

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS および Android の設定 991

Windows タブレットの設定 991

トンネルデバイスポリシー 992

Android設定 992

VPNデバイスポリシー 993

アプリごとのVPNの要件 993

iOS設定 995

iOS用L2TPプロトコルの構成 996

iOS用PPTPプロトコルの構成 996

iOS用IPsecプロトコルの構成 997

iOS 用 Cisco レガシー AnyConnect プロトコルの構成 998

iOS 用の Juniper SSL プロトコルを構成する 999

iOS向けF5 SSLプロトコルの構成 1000

iOS向けSonicWALLプロトコルの構成 1001

iOS向けAriba VIAプロトコルを構成する 1002

iOS向けIKEv2プロトコルの構成 1003

iOS向けCitrix SSOプロトコルの構成 1006

iOS用のカスタムSSLプロトコルを構成する 1007

NACをサポートするようにVPNデバイスポリシーを構成する 1009

iOSのVPNオンデマンドオプションを有効にするように構成する 1009

アプリごとのVPNを構成する 1013

macOS設定 1013

macOS用L2TPプロトコルの構成 1014

macOS用PPTPプロトコルの構成 1014

macOS 用 IPsec プロトコルを構成する 1015

macOS 用の Cisco AnyConnect プロトコルを構成する 1015

macOS 用 Juniper SSL プロトコルの構成 1016

macOS 用 F5 SSLプロトコルの構成 1017

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS 用 SonicWALL Mobile Connect プロトコルの構成 1018
macOS 用のAriba VIAプロトコルを構成する 1019
macOS用のカスタムSSLプロトコルを構成する 1020
VPNオンデマンドオプションの有効化を構成する 1021
Android (レガシーDA) 設定 1025
Android 用 Cisco AnyConnect VPN プロトコルの構成 1025
Android 用 Citrix SSO プロトコルを構成する 1026
NAC をサポートするように VPN を構成する 1027
Android Enterprise向けVPNの構成 1028
Android Enterpriseの設定 1028
Windowsデスクトップ/タブレットの設定 1029
Amazon の設定 1031
Amazon の L2TP PSK 設定を構成する 1032
AmazonのL2TP RSA設定を構成する 1032
AmazonのIPSEC XAUTH PSK設定を構成する 1033
Amazon の IPSEC AUTH RSA 設定を構成する 1033
Amazon の IPSEC HYBRID RSA 設定を構成する 1034
AmazonのPPTP設定を構成する 1034
壁紙デバイスポリシー 1035
iPhone 1035
iPad 1036
iOS設定 1036
Webコンテンツフィルターデバイスポリシー 1036
iOS設定 1037
組み込みフィルターの種類 1037
プラグインフィルターの種類 1038
Webクリップデバイスポリシー 1039
iOS設定 1039

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS設定 1040
Android設定 1040
ウィンドウズ デスクトップ/タブレットの設定 1041
Windows Agentデバイスポリシー 1041
Windowsデスクトップおよびタブレットの設定 1042
自動アクションをトリガーするPowerShellスクリプトを展開する 1043
Windows GPO構成デバイスポリシー 1044
Windows 10およびWindows 11デバイスに展開するためのGPOをインポートする 1045
Citrix Workspace Environment Managementに展開するためのGPOを構成する 1045
Windowsデスクトップおよびタブレットの設定 1046
Windows Hello for Business デバイスポリシー 1048
Windowsデスクトップ/タブレットの設定 1048
アプリの追加 1050
アプリの種類と機能 1051
サイレントインストールについて 1053
必須アプリとオプションアプリについて 1053
必須アプリの強制展開の要件 1053
例 1054
エンタープライズアプリおよびパブリックストアアプリ向けのiOS必須アプリのワークフロー 1054
エンタープライズアプリ向けのAndroid必須アプリのワークフロー 1055
パブリックストアアプリのAndroid必須アプリワークフロー 1055
必須として構成されているアプリをアンインストールする 1055
アプリを整理する（Android Enterprise） 1056
アプリカテゴリについて（iOSおよびMDX） 1057
MDXアプリを追加する 1060
パブリックアプリストアアプリを追加する 1064
Google Playアプリのアプリ設定を構成する 1066

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOSアプリのアプリ設定を構成する 1067

WebアプリまたはSaaSアプリを追加する 1071

既存のアプリコネクタを構成するには 1071

新しいアプリコネクタを構成するには 1073

エンタープライズアプリを追加する 1077

Win32アプリをエンタープライズアプリとして追加する 1081

要件 1081

メタデータの検索 1081

Citrix Endpoint Management に Win32 アプリを追加する 1081

Win32アプリのアップグレード 1084

Citrix CDNからエンタープライズアプリとMDXアプリを配信する 1084

CDNの仕組み 1085

Citrix CDNからエンタープライズアプリを配信する 1085

Citrix CDNからMDXアプリを配信する 1086

Webリンクを追加する 1088

Microsoft 365アプリを有効にする 1092

ワークフローを適用する 1092

アプリストアとCitrix Secure Hubのブランディング 1093

アプリストアを介したCitrix Virtual Apps and Desktops 1095

アプリコネクタの種類 1096

Citrix ランチャー 1097

Android Enterpriseデバイス向けCitrix Launcherのセットアップ 1098

レガシーAndroidデバイス向けCitrix Launcherのセットアップ 1099

デリバリーグループを追加してリソースを展開する 1099

Citrix Launcherなしでデバイスを管理する 1100

Apple Volume Purchase を使用してアプリを追加する 1101

Apple Volume Purchase について 1101

Volume Purchase アカウントを追加する 1102

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ボリューム購入アプリの構成 1104
アプリライセンスの使用状況を追跡および管理する 1105
ボリューム購入アカウントからユーザーを廃止する 1106
アプリ情報の同期 1107
デフォルトの同期間隔を変更する 1107
アプリ情報を手動で同期する 1107
アプリの更新を確認する 1108
Volume Purchaseアカウントのコンテンツトークンを更新する 1109
Citrix Endpoint Management で ShareFile を使用する 1109
シトリックス ファイル 1109
ストレージゾーンコネクタ 1110
要件 1111
インストールタスク 1111
ストレージゾーンコントローラーをインストールする 1112
ストレージゾーンコネクタのみで使用するためのストレージゾーンコントローラーの準備 1113
セカンダリストレージゾーンコントローラーをストレージゾーンに参加させる 1116
Citrix Endpoint Management でストレージゾーンコントローラー接続を定義する 1116
Citrix Endpoint Managementでストレージゾーンコネクタを追加する 1119
ストレージゾーンコネクタリストをフィルターする 1120
Enterpriseアカウントに切り替える 1120
HDX™アプリ向けSmartAccess 1121
エンドポイント向けHDXアプリのSmartAccess 1121
Citrix Endpoint Managementサーバー証明書をエクスポートして構成し、StoreFrontストアにアップロードする 1122
Citrix Endpoint ManagementからSAML証明書をエクスポートする 1123
証明書をPEMからCERに変換する 1123
証明書をStoreFrontサーバーにコピーする 1125

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFrontストアで証明書を構成する 1125
Citrix Virtual Apps and Desktops のSmartAccessポリシーを構成する 1126
Citrix Endpoint Managementで自動アクションを設定する 1127
デバイスが非準拠としてマークされたときにユーザーに表示される通知を作成する 1129
デバイスが非準拠とマークされたときに通知を送信するアクションを作成します 1130
ユーザーが HDX アプリへのアクセスを回復する方法 1131
MDXまたはエンタープライズアプリをアップグレードする 1132
メディアを追加 1135
前提条件 1135
書籍の構成 1135
Apple Bookを展開用に構成するには 1136
リソースを展開する 1138
デリバリーグループについて 1138
リソースの展開について 1139
展開順序 1139
計算手順 1140
管理者定義の順序による計算の例 1141
展開ルールの構成 1141
デリバリーグループの操作 1143
デリバリーグループを追加する 1143
デリバリーグループにポリシーを追加する 1147
デリバリーグループにアプリを追加する 1147
デリバリーグループにメディアを追加する 1148
デリバリーグループにアクションを追加する 1148
ShareFile構成を適用する 1148
構成されたオプションを確認し、展開順序を変更する 1149
Android Enterpriseにリソースをデプロイするルールを作成する 1150
デリバリーグループを編集する 1151

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AllUsersデリバリーグループを有効/無効にする 1151
デリバリーグループへの展開 1151
デリバリーグループのクローンを作成する 1152
デリバリーグループを削除する 1153
デリバリーグループテーブルをエクスポートする 1153
マクロ 1153
マクロの構文 1154
デフォルト通知テンプレート用のマクロ 1156
特定のポリシーのマクロ 1159
組み込みデバイスプロパティを取得するためのマクロ 1160
すべてのデバイスプロパティのマクロ 1160
組み込みユーザープロパティを取得するためのマクロ 1188
すべてのユーザープロパティのマクロ 1188
自動アクション 1192
アクションの例 1193
アクションの追加と管理 1194
MAM専用モードのアプリロックおよびアプリワイプアクション 1198
自動アプリワイプまたはアプリロックを構成するには 1198
アプリロックまたはアプリワイプのステータスを確認するには 1200
Azure ADでWindows 10およびWindows 11デバイスを非準拠としてマークする 1201
Windowsエージェントデバイスポリシーの結果に基づいて自動アクションを作成する 1202
監視とサポート 1205
ヘルプデスク管理者向けのモニターページ 1207
コンソールからのCitrix Endpoint Managementツールへのアクセス 1209
Citrix Endpoint Managementでのログファイルの表示と分析 1210
接続性チェック 1211
Citrix Endpoint Managementの接続性チェックを実行する 1211
NetScaler Gatewayの接続性チェックの実行 1213

© 1997–2026 Citrix Systems, Inc. All rights reserved.

接続チェックの詳細 1213

モバイルサービスプロバイダー 1217

レポート 1218

レポートを生成するには 1223

レポートの詳細を表示するには 1223

テーブルの列を並べ替え、フィルター、または検索するには、列見出しをクリックしま 1223

日付でレポートをフィルターするには 1223

グラフまたはテーブルをエクスポートするには 1224

REST API 1225

REST API にアクセスするために必要な権限 1225

REST APIサービスを呼び出すには 1226

ログイン 1226

関連情報 1227

メールアクセス制限 1228

ActiveSync ゲートウェイ 1228

ActiveSync Gateway設定を構成するには 1229

エクスチェンジ アクティブシンク 用 シトリックス エンドポイント マネジメント コネクタ 1230

バージョン 10.1.10 の新機能 1231

バージョン10.1.9の新機能 1232

以前のバージョンの新機能 1234

バージョン10.1.8の新機能 1234

バージョン10.1.7の新機能 1235

バージョン10.1.6.20での更新 1236

バージョン10.1.6の新機能 1236

バージョン 10.1.5 の新機能 1238

バージョン 10.1.4 の新機能 1239

バージョン 10.1.3 の新機能 1240

バージョン 10.1.2 の新機能 1241

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アーキテクチャ 1242
システム要件と前提条件 1243
前提条件 1243
Office 365 Exchangeの要件 1245
インストールと構成 1246
ActiveSync IDでメールポリシーを適用する 1251
アクセス制御ルール 1252
ルール評価について 1254
ルールの用語 1254
ルール分析ダイアログボックスでのルールの種類の表示方法 1255
複雑な式の例 1259
オーバーライドを分析する方法 1260
補足と競合を分析する方法 1263
ルールの詳細な分析方法 1264
通常の式ローカルルールを構成するには 1264
正規表現を追加するには 1265
既存のフィールド値から正規表現を作成するには 1265
アクセスルールを作成するには 1266
デバイスを検索するには 1267
個々のユーザー、デバイス、またはデバイスタイプを静的ルールに追加するには 1268
デバイスの監視 1268
トラブルシューティングと診断 1269
ログレベルを変更するには 1269
一般的なエラー 1269
トラブルシューティングツール 1270
Exchange ActiveSync 用 NetScaler Gateway コネクタ 1270
バージョン 8.5.3 の新機能 1271
以前のバージョンの新機能 1271

© 1997–2026 Citrix Systems, Inc. All rights reserved.

バージョン 8.5.2 の新機能 1271

バージョン 8.5.1.11 の新機能 1272

Exchange ActiveSync 用 NetScaler Gateway コネクタの監視 1272

Exchange ActiveSync 用コネクタで ActiveSync トラフィックをシミュレートするには 1272

Exchange ActiveSync 用コネクタのフィルターを選択する 1272

Exchange ActiveSync 用 NetScaler Gateway コネクタへの接続を構成するには 1274

Citrix Endpoint Management からポリシーをインポートするには 1275

NetScaler Gateway connector for Exchange ActiveSync のポリシーモードの構成 1276

静的ルールを構成するには 1277

GroupRefノード 1279

グループノード 1280

Exchange ActiveSync 用 NetScaler Gateway コネクタの構成 1280

Exchange ActiveSync 用 NetScaler Gateway コネクタのセキュリティモデルの選択 1281

許可モデル (許可モード) 1281

制限モデル (ブロックモード) 1282

Exchange ActiveSync用NetScaler Gatewayコネクタの管理 1282

XNCをアンインストールするには 1282

Exchange ActiveSync用コネクタをインストール、アップグレード、またはアンインストールするには 1282

Exchange ActiveSync 用 NetScaler Gateway コネクタのインストール 1283

Exchange ActiveSync 用 NetScaler Gateway コネクタのシステム要件 1283

デバイスのメールクライアント 1284

ネットスケーラー ゲートウェイ コネクタ Exchange ActiveSync 用の展開 1285

Exchange ActiveSync用コネクタのコンポーネント 1285

NetScaler Gateway connector for Exchange ActiveSyncのリスニングアドレスを設定するには 1285

NetScaler Gateway connector for Exchange ActiveSyncでデバイスアクセスコントロールポリシーを構成するには 1286

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementとの通信を構成するには 1286
冗長性とスケーラビリティのためのExchange ActiveSync用NetScaler Gatewayコネクタの展開 1287
高度な概念 1289
Citrix Endpoint Management のデプロイメント 1289
評価 1290
設計と構成 1290
運用と監視 1291
管理モード 1291
モバイルデバイス管理 (MDM) 1291
モバイルアプリ管理 (MAM) 1292
MDM+MAM 1293
デバイス管理とMDM登録 1293
MDM登録がオプションの場合 1293
MDM登録が必要な場合 1294
デバイス要件 1294
セキュリティとユーザーエクスペリエンス 1295
アプリとデバイス 1296
認証 1296
ユーザーエントロピー 1297
ポリシー 1297
アプリ 1297
ユーザーコミュニティ 1306
セキュリティ要件 1312
アプリ 1315
ユースケース 1319
ユーザーコミュニティ 1324
ユースケース 1325

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メール戦略 1331
メールクライアントの選択 1331
メールトラフィックフローとフィルタリングに関する考慮事項 1333
メールトラフィックフィルタリングの考慮事項 1335
エクスチェンジ アクティブシンク用ネットスケーラー ゲートウェイ コネクタ 1335
シトリックス エンドポイント マネジメントのExchange ActiveSync用コネクタ 1336
メールプラットフォームの意思決定ツリー 1337
シトリックス エンドポイント マネジメントの統合 1339
ネットスケーラー ゲートウェイ 1339
StoreFront 1341
シェアファイルとシトリックスファイル 1342
アクセス制御 1346
NetScaler Gateway と Citrix ADC との統合 1347
設計上の決定事項 1347
展開の概要 1353
MDXアプリのSSOとプロキシに関する考慮事項 1354
NetScaler Gatewayの認証方法 1355
セキュアトンネル化 - Web SSO 1358
NetScaler Gateway のスプリットトンネリング 1359
認証 1359
認証モード 1360
認証に関する重要なポリシー、設定、およびクライアントプロパティ 1361
推奨される構成 1367
サーバープロパティ 1375
サーバープロパティの追加、編集、または削除 1375
サーバープロパティの定義 1376
デバイスとアプリのポリシー 1388
セキュリティリスクに対処するポリシー 1389

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementが保存データを保護する方法 1389
Citrix Endpoint Management が転送中のデータを保護する方法 1390
アプリポリシーとユースケースシナリオ 1392
デバイスポリシーとユースケースの動作 1396
クライアントプロパティ 1400
クライアントプロパティを追加するには 1401
クライアントプロパティを編集するには 1402
クライアントプロパティを削除するには 1403
クライアントプロパティのリファレンス 1403
ユーザー登録オプション 1414
登録招待 1414
セルフヘルプポータル 1415
手動登録 1415
ユーザーオンボーディング 1416
ユーザーとの最初の連絡 1416
アプリのプロビジョニングとプロビジョニング解除 1417
ダッシュボードベースの操作 1420
ユースケース 1421
レポート 1422
ロールベースのアクセス制御とCitrix Endpoint Managementのサポート 1422
組み込みロール 1422
管理者ロール 1422
ユーザー 1423
Citrix Endpoint Managementサポートモデルに関する考慮事項 1423
Citrixサポートプロセス 1424
Citrix Endpoint Management でグループ登録招待を送信する 1425
一般的な手順 1425
ネストされたグループのサポート 1427

© 1997–2026 Citrix Systems, Inc. All rights reserved.

トラブルシューティングと既知の制限事項 1427
Citrix Secure Mailプッシュ通知用のEWSによる証明書ベース認証の構成 1427
関連情報 1430
オンプレミスのデバイス正常性構成証明サーバーの構成 1430
DHAサーバーの前提条件 1430
WindowsサーバーにDHAサーバーの役割を追加する 1431
サーバーの証明書ストアにSSL証明書を追加します 1432
証明書のサムプリントを取得して保存する 1433
署名証明書と暗号化証明書をインストールする 1434
TPMルート証明書を抽出し、信頼された証明書パッケージをインストールする 1435
DHAサービスを構成する 1435
構成を確認する 1438
index 1440
エンタープライズハブデバイスポリシー 1440
Windows Phoneの設定 1440
マップデバイスポリシー 1441
Windows Phoneの設定 1441
Citrix Endpoint Managementドキュメント履歴 1442

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント マネジメント

Citrix Endpoint Management は、エンドポイントを管理するためのソリューションであり、モバイルデバイス管理 (MDM) およびモバイルアプリケーション管理 (MAM) の機能を提供します。Citrix Endpoint Management を使用すると、デバイスとアプリのポリシーを管理し、ユーザーにアプリを配信できます。ID、デバイス、アプリ、データ、ネットワークに対する厳格なセキュリティにより、ビジネス情報が保護されます。

Citrix® と顧客の責任

Citrix Cloud Operations は、さまざまなインフラストラクチャおよび監視タスクを処理します。その結果、ユーザーエクスペリエンスと、デバイス、アプリ、ポリシーの管理に集中できます。

Citrix の責任:

- シトリックス エンドポイント マネジメント サーバーノード
- NetScaler Gateway (サービスまたはオンプレミス) の初期統合と構成
- NetScaler Gateway ロードバランサー
- データベース
- Cloud Connector ソフトウェア構成
- ShareFile との SAML 認証統合
- Citrix Endpoint Management サイト監視: インスタンス、データベース、エンタープライズ接続 (LDAP)、VPN トンネル (該当する場合)、パブリック SSL 証明書、Citrix Endpoint Management ライセンス

顧客の責任:

- NetScaler Gateway (オンプレミス) の管理と更新
- Cloud Connector および Gateway Connector (Citrix Gateway サービス用) がインストールされているマシン
- LDAP/アクティブディレクトリ
- DNS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ShareFile: 初期ShareFile構成、オンプレミスストレージゾーンコントローラーのインストール、Citrix Filesの更新
- Citrix Endpoint Managementの構成: デバイス、ポリシー、アプリ、デリバリーグループ、アクション、クライアント証明書

マイクロソフト エンドポイント マネージャー との統合

Citrix Endpoint ManagementはMicrosoft Endpoint Manager (MEM) と統合します。この統合により、Microsoft EdgeブラウザなどのMicrosoft Intune対応アプリにCitrix Endpoint Managementのマイクロ VPNの価値が加わります。この統合により、次のことが可能になります。

- Azure ADによる条件付きアクセスでOffice 365アプリケーションを保護します。詳細については、「Azure AD条件付きアクセスとの統合」を参照してください。
- IntuneとCitrixを使用して独自の基幹業務アプリをラップし、Intuneモバイルアプリ管理 (MAM) コンテナ内でマイクロVPN機能を提供します。
- Office 365アプリ、基幹業務アプリ、Citrix Secure Mailを1つのコンテナで管理および配信します。この管理方法は、究極のセキュリティと生産性を提供します。たとえば、次のことが可能です。
  - 個々のデバイスまたはオペレーティングシステムをブロックする
  - デバイス、ユーザー、またはユーザーグループに基づいてActiveSyncポリシーをカスタマイズする
  - デバイスレベルで隔離する
  - 個々の接続またはデバイスを監視する
  - 資格情報とデータキャッシュのセキュリティリスクを回避する

デバイスの管理には、Citrix Endpoint Management MDM+MAMまたはIntune MDMを使用します。詳細については、「Citrix Endpoint ManagementとMicrosoft Endpoint Managerの統合」を参照してください。

Cloud Connector とリソースの場所

Citrix Endpoint Management には Cloud Connector を介して接続します。Cloud Connector は、Citrix Cloud とリソースの場所との間の通信チャネルとして機能します。Cloud Connector を使用すると、VPN や IPsec トンネルなどの複雑なネットワークやインフラストラクチャの構成を必要とせずに、クラウド管理が可能になります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リソースの場所には、サブスクライバーにサービスを提供するために必要なリソースがあります。Citrix Endpoint Management の場合、リソースの場所は NetScaler Gateway、LDAP、DNS、および PKI サーバーです。

リソースの場所 (/en-us/citrix-endpoint-management/media/cloud-connector-diagram.png)

Cloud Connector とリソースの場所の詳細については、「Citrix Endpoint Management について」を参照してください。

Citrix Endpoint Management の使用を開始する

ヒント:

XenMobile® 移行サービス

オンプレミスで XenMobile Server を使用している場合、当社の XenMobile 移行サービスを利用して Citrix Endpoint Management の使用を開始できます。XenMobile Server から Citrix Endpoint Management への移行では、デバイスを再登録する必要はありません。
詳細については、お近くの Citrix 営業担当者、システムエンジニア、または Citrix パートナーにお問い合わせください。
移行サービスの詳細は、「Citrix Endpoint Management サービスに移行する 3 つの理由」を参照してください。
移行する理由、移行方法、および Citrix Endpoint Management への移行の利点については、CEM Migration Service Course Catalog を参照するか、Citrix Endpoint Management (CEM) Migration Service ガイドを参照してください。
Citrix Endpoint Management を評価または購入する際、Citrix Endpoint Management オペレーションチームが継続的なオンボーディングサポートを提供します。オペレーションチームはまた、Citrix Endpoint Management のコアサービスが正しく稼働し、構成されていることを確認するために、お客様と連絡を取ります。この図はオンボーディングの手順を示しています。

オンボーディングワークフロー (/en-us/citrix-endpoint-management/media/cloud-onboarding-flow.png)

Citrix アカウントにサインアップして Citrix Endpoint Management の試用版をリクエストするには、Citrix 営業担当者にお問い合わせください。準備ができたら、https://onboarding.cloud.com にアクセスしてください。

Citrix Endpoint Managementのオンボーディングと構成の概要を素早く知るには、このビデオをご覧ください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

<iframe src="https://www.youtube.com/embed/ycFLYxn7aII" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
開始する前にもっと詳しく知りたいですか？以下のリソースをお試しください。

Citrix Endpoint Managementドキュメント: オンボーディングから初期構成、高度な構成まで、Citrix Endpoint Managementの完全なドキュメントを提供します。「新機能」の記事では、新機能と修正について説明しています。Citrixは、新しいバージョンでその記事が利用可能になったときに通知します。

Citrix Endpoint Managementオンボーディングハンドブック**:** Citrix Endpoint Managementに関する利用可能なすべての情報を統合し、Citrix Endpoint Managementのスムーズな有効化とオンボーディングを継続できるようにします。このドキュメントを使用して、内部プロセスの変更を記録したり、高レベルおよび機能設計を文書化したりできます。

Citrix Endpoint Management展開ハンドブック**:** Citrix Endpoint Managementの展開を計画するには、多くの考慮事項があります。このハンドブックには、Citrix Endpoint Management環境に関する推奨事項、よくある質問、およびユースケースが含まれています。

SalesIQ**:** Citrixパートナー向けのその他のリソース。

次のステップ

Citrix Endpoint Managementのオンボーディングプロセスについては、「オンボーディングとリソースのセットアップ」を参照してください。

オンボーディングが完了したら、「デバイスの登録とリソースの配信の準備」を参照してください。

非推奨のお知らせ

段階的に廃止されるCitrix Endpoint Management機能の事前通知については、「非推奨」を参照してください。

シトリックス エンドポイント マネジメント サポート

Citrix Endpoint Managementコンソールでサポートされている関連情報とツールにアクセスする方法の詳細については、「監視とサポート」を参照してください。

Citrix Endpoint Managementリリースのローリングアップデートは、約2週間ごとに実施されます。お客様にとって、このプロセスは透過的です。最初のアップデートはCitrixの内部サイトにの

© 1997–2026 Citrix Systems, Inc. All rights reserved.

み適用され、その後、顧客環境に段階的に適用されます。製品の品質を確保し、可用性を最大化するために、アップデートは段階的に波状に提供されます。

Citrix Endpoint Managementのお客様は、Citrix Endpoint Management Cloud Operationsチームから直接、更新情報や連絡を受け取ります。これらの更新により、新機能、既知の問題、修正された問題などが常に最新の状態に保たれます。

Citrix Cloud Operationsチームは、最新のCitrix Endpoint Managementローリングパッチを使用してCitrix Endpoint Management環境を維持します。ローリングパッチの前に必要な特定のパッチや修正を入手するには、Citrixテクニカルサポートにお問い合わせください。

環境に問題がある場合は、CitrixテクニカルサポートまたはCitrixアカウントチームにお問い合わせください。このような問題には、モバイルデバイスの登録、Citrix Endpoint Managementコンソールへのアクセス、Citrix Secure Mailの問題などが含まれる場合があります。

クラウドまたはCitrix Endpoint ManagementのNetScaler Gatewayで統合または変更が必要な場合は、Citrixテクニカルサポートを通じてリクエストを送信してください。

リクエストできる変更の例は次のとおりです。

- クラウドでのNetScaler GatewayとCitrix Filesの統合
- NetScaler Gateway認証タイプの変更
- 顧客データセンターリソースへの接続の検証
- マイクロVPNの分割トンネル構成の変更
- サーバー構成の変更によるCitrix Endpoint Managementコンポーネントの再起動

サービスレベル契約

Citrix Endpoint Managementは、業界のベストプラクティスを活用して、クラウド規模と高いサービス可用性を実現しています。

Citrix Cloudサービスの可用性に関するCitrixのコミットメントの詳細については、サービスレベル契約を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

新機能

Citrixは、Citrix Endpoint Managementのお客様が利用可能になった時点で、新機能と製品アップデートを提供することを目指しています。新しいリリースはより多くの価値を提供するので、アップデートを遅らせる理由はありません。

- Citrix Endpoint Managementへのローリングアップデートは、約3か月ごとにリリースされます。
- これらのアップデートによって、インスタンスやデバイスユーザーのダウンタイムが発生することはありません。
- すべてのリリースに新機能があるわけではなく、一部のアップデートには修正とパフォーマンスの強化が含まれています。

お客様にとって、このプロセスは透過的です。Citrix®は、最初のアップデートをCitrix®の内部サイトにのみ適用し、その後、段階的にお客様の環境に適用します。アップデートを段階的に提供することで、製品の品質を確保し、可用性を最大化するのに役立ちます。

また、Citrix Endpoint Managementのアップデートと通信は、Citrix Endpoint Management Cloud Operationsチームから直接受け取ります。これらのアップデートにより、新機能、既知の問題、修正された問題などについて常に最新の状態を保つことができます。

クラウド規模やサービス可用性などの詳細については、Citrix Endpoint Managementのサービスレベル契約を参照してください。サービスの中断や予定されているメンテナンスを監視するには、サービス稼働状況ダッシュボードを参照してください。

シトリックス エンドポイント管理 26.8.0

- **ソフトウェアアップデート設定デバイスポリシーでの「セキュリティアップデートのインストール」のサポート:** iOSデバイスのソフトウェアアップデート設定デバイスポリシーに、新しい設定**セキュリティアップデートのインストール**が追加されました。この設定は、利用可能なセキュリティアップデートの自動インストールをユーザーが制御できるかどうかを指定します。この機能はiOS 18以降で利用可能です。デフォルトは**許可**です。詳細については、ソフトウェアアップデート設定デバイスポリシーを参照してください。
- **アプリ設定デバイスポリシーのサポート: 構成 (宣言型)** の下に新しいデバイスポリシー**アプリ設定**が追加されました。このポリシーを使用すると、Appleの宣言型デバイス管理を使用して

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリの許可リストと拒否リストを構成できます。このポリシーは、監視対象のiOS 27以降のデバイスのみをサポートします。詳細については、アプリ設定デバイスポリシーを参照してください。

- **外部インテリジェンス設定デバイスポリシーのサポート: 構成 (宣言型)** の下に新しいデバイスポリシー**外部インテリジェンス設定**が追加されました。このポリシーを使用すると、監視対象のiOS 26.4以降のデバイスで外部AI統合を管理できます。詳細については、外部インテリジェンス設定デバイスポリシーを参照してください。
- **インテリジェンス設定デバイスポリシーのサポート: 構成 (宣言型)** の下に新しいデバイスポリシー**インテリジェンス設定**が追加されました。このポリシーを使用すると、監視対象のiOS 26.4以降のデバイスでApple Intelligence機能を管理できます。詳細については、インテリジェンス設定デバイスポリシーを参照してください。
- **iOS 27のサポート:** Citrix Endpoint ManagementおよびCitrix Mobile生産性向上アプリは、iOS 27と互換性があります。
- **Secure Hub APNs証明書の更新:** Citrix Endpoint Management 26.5用のSecure Hub Apple Push Notificationサービス (APNs) 証明書は、November 9, 2026に期限切れになります。このアップデートにより、Secure Hub APNs証明書は、September 18, 2027まで有効な新しい証明書に自動的に更新されます。
- **Androidレガシーデバイス管理者モードの非推奨化:** AndroidレガシーDAモードは、CEM 26.8.0以降のCitrix Endpoint Managementで非推奨になりました。MDXアプリの**Android (legacy DA)**プラットフォームは、Citrix MAMのみのモードで登録されたAndroidデバイスで使用するために、**Android (Citrix MAM Only)**に名称変更されました。

CEM 26.8.0で修正された問題

- 2,100を超えるライセンスが割り当てられている場合、ユーザーはSecure Hubを介してオプションのVolume Purchase Program (VPP) アプリをインストールできず、インストールはApp Storeにリダイレクトされます。

シトリックス エンドポイント マネジメント 26.5.0

- **Android Enterpriseデバイスでの資格情報マネージャーアプリケーションのサポート:** Android Enterpriseデバイスの制限ポリシーに、新しい設定**Credential manager applications**が追加されました。この設定は、アプリケーションが資格情報プロバイダーとして機能できるかどうかを制御し、デフォルトで**Off**に設定されています。この機能はAndroid 14以降で利用可能で、Secure Hubバージョン26.5.0以降が必要です。詳細については、「」を参照してください。(/ja-jp/citrix-endpoint-management/policies/restrictions-policy.html#android-enterprise-settings).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Android 17のサポート:** Citrix Endpoint ManagementおよびCitrix Mobile生産性向上アプリは、Android 17を実行するAndroid Enterpriseデバイスをサポートするようになりました。セキュリティとプライバシーの詳細については、を参照してください。(https://developer.android.com/about/versions/17).

CEM 26.5.0で修正された問題

- CEMコンソールでデバイスの**コンプライアンス違反**ステータスを手動で編集しても、Azure ADへのコンプライアンスステータスの同期はトリガーされません。
- `/api/v1/application/store/{id}/platform/iphone` REST APIを介したiOSアプリの更新がエラー1493で失敗します。
- Citrix Cloud Secure Clientからサービスプリンシパル認証に移行した後、デバイスクエリなどのパブリックREST API呼び出しがエラー1001で失敗します。

シトリックス エンドポイント マネジメント 26.2.0

- **アプリインベントリの強化によるiOS 26.xアプリサイズの取得サポート:** Citrix Endpoint Managementは、iOS 26.xを実行するデバイスのアプリサイズ情報の取得をサポートします。この情報は、**Device details > Apps**で確認できます。
- **デバイス証明書のトラブルシューティングの強化:** Citrix Endpoint Managementには、**Citrix Secure Hub**で導入されたデバイス証明書のトラブルシューティング強化をサポートするためのサーバー側アップデートが含まれるようになりました。この機能を有効にすると、エンドユーザーはデバイス証明書の健全性ステータスを表示し、**Secure Hub**アプリから直接証明書の問題を自動的に修正できます。

  既存のユーザーに対してこの機能を有効にするには、顧客管理者はクライアントプロパティ `aeDeviceCertRenewSupport` を追加する必要があります。詳細については、「」を参照してください。(/ja-jp/citrix-endpoint-management/advanced-concepts/deployment/client-properties.html).

  クライアント側のこの機能の詳細については、「」を参照してください。(/ja-jp/citrix-secure-hub/whats-new.html#device-certificate-troubleshooting-enhancement).
- **iOSデバイスのキャリアネットワーク関連デバイス情報取得のサポート:** Citrix Endpoint Managementは、iOSデバイスの各SIMに関する追加のキャリアネットワーク関連デバイス情報の取得をサポートするようになりました。これらの詳細は、 **> >** で確認できます。新しくサポートされるフィールドは次のとおりです。
  - スロットx — キャリア設定バージョン

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- スロットx — 現在のキャリアネットワーク
- スロットx — 現在のモバイル国コード（以前はネットワーク情報に記載）
- スロットx — 現在のモバイルネットワークコード（以前はネットワーク情報に記載）
- スロットx — データ優先
- スロットx — ローミング中
- スロットx — 音声優先
- スロットx — ラベルID

- **Microsoft Exchange OnlineのOAuth認証のサポート:** Microsoftは、Exchange Onlineが2026年3月にクライアント送信（SMTP AUTH）での基本認証のサポートを完全に終了し、April 30, 2026には100%拒否されるようになると発表しました。 詳細については、「Exchange Online to retire Basic auth for Client Submission (SMTP AUTH)」を参照してください。

  Citrix Endpoint Managementは、SMTPサーバーのOAuth認証をサポートしています。この機能を有効にするには、 を選択し、必要な 、、および を指定します。Microsoft Exchange Onlineを使用している場合は、OAuth認証への切り替えをCitrixが推奨します。構成の詳細については、「通知」を参照してください。

CEM 26.2.0で修正された問題

- Citrix Endpoint Managementコンソールでのデバイス、アプリ、デリバリーグループの管理などの操作が著しく遅くなり、場合によっては失敗します。

シトリックス エンドポイント マネジメント 25.11.0

- **Secure Hub APNs証明書の更新:** Citrix Endpoint Management 25.9のSecure Hub Apple Push Notification service (APNs) 証明書は、January 4, 2026に期限切れになります。この更新により、Secure Hub APNs証明書は、November 9, 2026まで有効な新しい証明書に自動的に更新されます。

CEM 25.11.0 で修正された問題

- iOS デバイスにアンインストールされたアプリケーションのアプリロックポリシーが設定されている場合、デバイスは「ガイド付きアクセスアプリは利用できません。管理者にお問い合わせください」というエラーでロックされ、強制再起動後もタッチスクリーンが応答しなくなります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 管理者が既存のエンタープライズアプリを更新するためにアプリケーションファイルをアップロードすると、モバイルプラットフォームに関わらず更新が失敗します。新しいエンタープライズアプリの作成は影響を受けず、既存のアプリの編集のみが影響を受けます。

シトリックス エンドポイント マネジメント 25.9.0

- **Android 16 のサポート:** Citrix Endpoint Management および Citrix Mobile 生産性向上アプリは、Android 16 を実行する Android Enterprise デバイスをサポートするようになりました。セキュリティとプライバシーの詳細については、Android 開発者向けドキュメントを参照してください。
- **iOS 26 のサポート:** Citrix Endpoint Management および Citrix Mobile 生産性向上アプリは、iOS 26 と互換性があります。
- **レガシー MDX ポリシーアップグレード通知のサポート:** Citrix Endpoint Management は、レガシーポリシーを使用している既存の Secure Mail および Secure Web MDX アプリがバージョン 25.9.0 に更新されたときに、アップグレードアラートを表示するようになりました。
- **証明書ベースの認証における新しい強力な証明書マッピングのサポート:** 強力なマッピング要件を満たす証明書の発行において、より高い柔軟性を可能にする新しいマッピング方法が導入されました。Citrix Endpoint Management (CEM) は、証明書のサブジェクト代替名 (SAN) に `URL=tag:microsoft.com`、`2022-09-14:sid:<user's SID>` を追加するようになりました。
  - 既存のユーザーに対してこの機能を有効にするには、顧客管理者がクライアントプロパティ `MICROSOFT_CERTIFICATE_STRONG_MAPPING` を追加する必要があります。詳細については、「クライアントプロパティ」を参照してください。
  - 強力な証明書マッピングは、**Windows Server 2019 以降**でのみサポートされています。詳細については、「Microsoft Strong Mapping」を参照してください。
- **Apple Deployment Programs ページでの新しい iOS セットアップアシスタントオプションのサポート:** Apple Business Management 登録のために、Apple はいくつかの新しい iOS セットアップアシスタントオプション画面を追加しました。以下の新しいオプションが、**> >** ページに追加されました。Citrix Endpoint Management (CEM) を設定して、これらの画面をスキップできます。詳細については、「iOS セットアップアシスタントオプション」を参照してください。
  - アクションボタン
  - ロックダウンモード
  - インテリジェンス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - カメラボタン

- **iOS 18.xバージョン向けの新しいiOS制限のサポート:** iOSの制限ポリシーに、Apple Intelligence (AI) へのアクセスをブロックしたり、一部の新機能を制限したりするための以下の新しい設定が追加されました。これらの設定は、iOSバージョン18以降に適用されます。デフォルトは**オン**です。詳細については、「制限ポリシー」を参照してください。

  - 外部インテリジェンス統合を許可
  - 外部インテリジェンス統合へのサインインを許可
  - メールのスマートリプライを許可
  - メモの文字起こしを許可
  - Safariの要約を許可
  - ビジュアルインテリジェンスの要約を許可
  - メモの文字起こし要約を許可
  - Apple Intelligenceレポートを許可
  - デフォルトの通話アプリの変更を許可
  - デフォルトのメッセージングアプリの変更を許可
  - 外部インテリジェンスワークスペースIDを許可
  - デフォルトブラウザの変更
  - FaceTimeリモートコントロールを許可

- **iOS 17.xバージョン向けの新しいiOS制限のサポート:** iOSの制限ポリシーに、iOSバージョン17.2以降向けの以下の新しい設定が追加されました。デフォルトは**オン**です。詳細については、「制限ポリシー」を参照してください。

  - ライブ留守番電話を許可

- **構成管理ポリシーのテキストボックス:** お客様が**Knox Service Plugin**を**管理対象構成ポリシー**と併用する場合、**分離されたアプリポリシー**のすべてのテキストボックスの最大文字長が8,192文字に増加します。
- **Android Enterpriseデバイス向けデュアルSIMおよびeSIMサポートの強化:** Citrix Endpoint Management (CEM) は、Android Enterpriseデバイス向けに包括的なデュアルSIMサポートを提供するようになり、iOSとの機能パリティを確保します。この機能強化により、管理者は、2つの物理SIMカード、1つのSIMカードと1つのeSIM、または2つのeSIMの構成を含む、デバイスプロパティ内のすべてのインストール済みSIMカードとeSIMを表示できます。このアップデートは、デュアルSIM Android Enterpriseデバイスの採用拡大に対応し、以前iOSデバイス向

© 1997–2026 Citrix Systems, Inc. All rights reserved.

けに提供されたeSIM機能と一致する、モバイルデバイスの接続オプションに関する完全な可視性をお客様に提供します。この機能は、以下でのみサポートされています。

- Secure Hubバージョン25.7.0以降、および
- Android 13以降

CEM 25.9.0で修正された問題

- Legacy MDXアプリケーションがアップロードされていない場合でも、Legacy MDXアラートがCEMコンソールに表示され続けます。
- デバイス登録プログラム (DEP) デバイスは、登録プロファイルが**MDMのみ**として構成されている場合でも、**MDM+MAM**登録を実行し続けます。
- 「**新しいビューの表示**」機能が有効になっている場合、デバイスリストにフィルターが適用されていても、デバイス数が正しく表示されません。
- Android Enterpriseデバイスは、Citrix Endpoint Management™ (CEM) を介して管理者が送信した**登録アプリ**通知を受信できません。
- iOSユーザーは、Secure Mail/Secure Webアプリケーションを起動できず、Secure Mail/Secure WebからSecure Hubにリダイレクトする際に「開けません」というエラーが発生します。

シトリックス エンドポイント マネジメント 25.7.0

- **ユーザー認証ワークフローの強化:** オンプレミスActive Directory (AD) でデバイスを登録し、その後Microsoft Azure Active Directory (AAD) を使用してCitrix IDプロバイダーと統合したユーザーは、再登録する必要がありません。オンプレミスActive DirectoryからMicrosoft Azure Active Directoryにアカウントを同期できます。詳細については、「ユーザー認証ワークフロー」を参照してください。

シトリックス エンドポイント マネジメント 25.5.0

- **Apple Business Managementとの同期によるデバイス割り当ての管理:** Citrix Endpoint Management (CEM) は、Apple Business Management (ABM) と同期することで、正確なデバイス割り当てを保証するようになりました。このアップデートにより、正しく割り当てられたデバイスのみがCEMに表示されることが確認され、CEMから削除され、別のベンダー管理ソリューションに割り当てられたデバイスの記録が残ることを防ぎます。たとえば、デバイスが別のソリューションに移動された場合、同期後にはCEMに表示されなくなります。この機能は、お客様が管理するテナントサーバープロパティ `remove.unassigned.abm.devices` に

© 1997–2026 Citrix Systems, Inc. All rights reserved.

よって制御されます。デフォルトでは、このプロパティは**False**に設定されています。詳細については、「サーバープロパティ」を参照してください。

注記:

管理者が移動しようとしても、すでに登録されているApple Business Management (ABM) デバイスはCEMから削除されません。

- **宣言型デバイス管理 (DDM) のサポート:** iOS 15以降のAppleの宣言型デバイス管理 (DDM) との互換性を有効にするため、「宣言型デバイス管理のサポート」という新機能が導入されました。この機能は、宣言型データモデルを使用することでパフォーマンスとスケーラビリティを向上させ、シリアル化されたコマンドやデバイスポーリングへの依存を軽減します。詳細については、宣言型管理データモデルを活用してデバイスを拡張するを参照してください。必要に応じて、管理者に連絡してこの機能を有効にしてください。

  DDM機能を有効にすると、以下の宣言型デバイスポリシーがサポートされます。

  - Googleアカウント
  - パスコード
  - ソフトウェアアップデートの適用
  - ソフトウェアアップデート設定
  - ステータスサブスクリプション
  - ユーザーID

CEM 25.5.0 で修正された問題

- ロールベースのアクセス制御 (RBAC) 管理者が**サーバープロパティ**権限を持っていない場合、デバイスページで**新しいビューを表示**を切り替えると予期せずログアウトされます。
- 新しいビューの表示機能が有効になっている場合、ロールベースのアクセス制御 (RBAC) 管理者に予期せず検索入力ボックスが表示されます。
- **展開スケジュール**で**展開条件**が「以前の展開が失敗した場合のみ」に設定されている場合、一部のポリシーが再登録中にAEデバイスに展開されません。

シトリックス エンドポイント マネジメント 25.3.0

- **デバイスページでの永続フィルターのサポート:** 新しいデバイスページでは、すべての**フィルター可能な**オプションでフィルターがサポートされるようになりました。これらのフィルターは、ログインしているユーザーのセッション間で保存されるため、管理者がデバイスページに

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アクセスするたびに同じフィルターを再適用する必要がなくなります。対応する列が選択解除されると、フィルターは自動的に削除されます。

- **システムがデバイスを消去する際のeSIM保持のサポート:** 制限ポリシーに新しい設定「**消去時にeSIMを保持**」が追加されました。この設定により、パスワードの入力に複数回失敗した場合や、「**設定 > 一般 > リセット**」で「**すべてのコンテンツと設定を消去**」オプションが選択された場合に、システムがデバイスを消去してもeSIMが保持されます。この機能はiOSバージョン17.2以降で利用可能で、デフォルト設定は「**オフ**」です。詳細については、「制限ポリシー」を参照してください。

CEM 25.3.0で修正された問題

- MDM証明書の更新に失敗すると、古い証明書はCitrix Endpoint Management (CEM)によって失効済みとしてマークされ、Secure Hub (SH)がサーバーに再接続できなくなります。その結果、SHは古い証明書がまだ期限切れになっていないにもかかわらず、それを使用してサーバーと通信できなくなります。
- アプリケーションが新しいバージョンにアップグレードされても、Volume Purchase Program (VPP)アプリのアイコンが更新されません。

シトリックス エンドポイント管理 25.1.0

- **Secure Hub APNs証明書の更新:** Citrix Endpoint Management 24.10のSecure Hub Apple Push Notification service (APNs)証明書は、February 9, 2025に期限切れになります。この更新により、Secure Hub APNs証明書は、January 4, 2026まで有効な新しい証明書に自動的に更新されます。
- **iOS向けApple Intelligenceのブロックまたは制限のサポート:** iOSの制限ポリシーに、Apple Intelligence (AI)へのアクセスをブロックしたり、一部の新機能を制限したりするための新しい設定が追加されました。これらの設定はiOSバージョン18以降に適用され、デフォルトは「**オン**」です。詳細については、「制限ポリシー」を参照してください。新しい設定には以下が含まれます。
  - ジェン文字
  - イメージプレイグラウンド
  - イメージワンド
  - iPhoneミラーリング
  - パーソナライズされた手書き入力結果
  - ライティングツール

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 通話録音
- 非表示にするアプリ
- ロックするアプリ
- メール概要
- RCSメッセージング

- **macOS向けApple Intelligenceのブロックまたは制限のサポート:** macOSの制限ポリシーに、Apple Intelligence (AI) へのアクセスをブロックしたり、一部の新機能を制限したりするための新しい設定が追加されました。これらの設定はmacOSバージョン15以降に適用され、デフォルトは**オン**に設定されています。詳細については、制限ポリシーを参照してください。新しい設定には以下が含まれます。
  - イメージプレイグラウンド
  - iPhoneミラーリング
  - ライティングツール
  - メディア共有の変更を許可

CEM 25.1.0で修正された問題

- 多数のペイロード証明書がAEデバイス用に生成されていました。
- **展開スケジュール**で**展開条件**が「前回の展開が失敗した場合のみ」に設定されている場合、再登録時に一部のポリシーがAEデバイスに展開されません。
- GEO固有のVolume Purchase Program (VPP) アプリケーションをCitrix Endpoint Management (CEM) サーバーに同期しようとすると、エラーメッセージなしで同期が失敗します。手動でのボリューム購入同期中であっても、VPPアプリケーションはCitrix Endpoint Managementアプリリストに反映されません。

シトリックス エンドポイント管理 24.10.0

- **Azure Active Directoryグループベース管理による認証:** Citrix Endpoint Managementは、Azure Active Directory (AAD) を介したグループベースのID認証をサポートしており、管理者はAADグループメンバーシップを使用してグループレベルでアクセスを管理できます。このアップデートにより、一元化されたグループ制御を通じて、柔軟性とセキュリティが向上します。この新しい機能によりアクセス管理が効率化されますが、下位互換性を確保するために従来のCitrix Identityログインメカニズムも引き続き利用できます。詳細については、Azure Active Directoryグループベース管理による認証を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web配布のサードパーティ製アプリのブロックをサポート:** 制限ポリシーに、iOSデバイス上のWeb配布のサードパーティ製アプリをブロックするための新しい設定「**Web配布アプリ**」が追加されました。この設定は、iOSバージョン17.5以降に適用されます。詳細については、「制限ポリシー」を参照してください。必要に応じて、管理者に連絡してこの機能を有効にしてください。
- **統合プラットフォームエクスペリエンス:** Citrix Endpoint Managementは、Citrix製品全体で統一されたナビゲーションを提供することで、統合されたプラットフォームエクスペリエンスを実現します。この機能により、ユーザーインターフェイス全体のナビゲーションバーの位置が変更され、新しい左ナビゲーションバーが追加されます。
- **Windows 2022 CAサーバーをサポートするためのCitrix Endpoint Managementの機能強化:** Citrix Endpoint Managementは、以下のCAサーバーをサポートしています。
  - ウィンドウズ サーバー 2016
  - ウィンドウズ サーバー 2019
  - ウィンドウズ サーバー 2022
- **監視タブは非推奨になりました:** Citrix Endpoint Managementの監視タブは、2024年10月をもって非推奨となります。詳細については、「非推奨と削除」を参照してください。
- **デバイスの紛失モードAPIを含めるように公開REST APIドキュメントを更新:** 公開REST APIドキュメントに紛失モードAPIを追加しました。
- **API呼び出しをURLではなくPOSTボディにするように変更:** 公開REST APIドキュメントで、API呼び出しをURLではなくリクエストボディにデータを含めるように更新しました。
- **Android 15のサポート:** Citrix Endpoint ManagementおよびCitrix Mobile生産性向上アプリは、Android EnterpriseデバイスのAndroid 15へのアップデートをサポートするようになりました。セキュリティとプライバシーの利点の詳細については、Android開発者向けドキュメントを参照してください。
- **iOS 18のサポート:** Citrix Endpoint ManagementおよびCitrix Mobile生産性向上アプリはiOS 18と互換性がありますが、現時点ではiOS 18のすべての新機能はサポートしていません。
- **macOS 15のサポート:** Citrix Endpoint ManagementおよびCitrix Mobile生産性向上アプリはmacOS 15と互換性がありますが、現時点ではmacOS 15のすべての新機能はサポートしていません。

CEM 24.10.0で修正された問題

- 一部のアプリでVPP接続テストとVPP同期が失敗しました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント マネジメント 24.8.0

- **管理対象構成フィードバックのサポート (テクニカルプレビュー):** 管理対象構成フィードバック機能を使用すると、管理者は管理対象構成ポリシーで構成されたAndroidデバイスからアプリの状態に関するフィードバックを取得できます。詳細については、「管理対象構成フィードバックのサポート (テクニカルプレビュー)」を参照してください。
- **Androidデバイスのコンプライアンス強制 (テクニカルプレビュー):** デバイス所有者モードで登録されたAndroidデバイスの場合、顧客管理者はデバイスのコンプライアンスを管理できます。詳細については、「Androidデバイスのコンプライアンス強制 (テクニカルプレビュー)」を参照してください。

CEM 24.8.0で修正された問題

- 共有iPadでセキュアアクション「すべてのユーザーを削除」が失敗しました。
- Citrix Endpoint Management上の一部のiOS公開アプリがApple Storeで見つかりません。
- Citrix Endpoint Management 24.4.0では、CEMをSAML SSO IDプロバイダー (IDP) として使用している場合、SAML証明書の更新後にSAML SSOが失敗します。
- 証明書ベースの認証シナリオでは、証明書の更新の失敗によりSecure Hubで機能上の問題が発生しています。システム管理者は、特にAndroidプラットフォームで、PKI証明書の生成が停止しないことに気づくかもしれません。
- 新しいバージョンのMAM SDK対応アプリの場合、Secure Hubストアで更新オプションが利用できません。

シトリックス エンドポイント マネジメント 24.6.0

- **iOS 17.4以降でのサードパーティ製アプリのブロックをサポート:** 制限ポリシーに新しい設定「**代替アプリマーケットプレイス**」が追加され、Webからの代替マーケットプレイスアプリのインストールを防止し、インストール済みの代替マーケットプレイスアプリがアプリをインストールするのを防止します。詳細については、「制限デバイスポリシー」を参照してください。
- **新しいHTTP v1 APIを使用するFirebase Cloud Messagingのサポート:** HTTP用のFCMレガシーAPIは、GoogleによってJune 21, 2024に非推奨になります。FCMが新しいAPIで適切に機能するように、サービスアカウントキーJSONファイルをアップロードするための新しいフィールド「**サービスアカウントキーファイル**」がFirebase Cloud Messagingページに追加されました。詳細については、Firebase Cloud Messagingを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CEM 24.6.0で修正された問題

- 管理者がADグループを更新した後、デリバリーグループに割り当てられたモバイルアプリがエンドユーザーからアクセスできなくなり、ユーザーが匿名になる可能性があります。
- 顧客が**クライアントサポート**設定で「**デバイスログをITヘルプデスクに直接送信**」を選択した場合、Secure HubログをITヘルプデスクに送信できません。

シトリックス エンドポイント マネジメント 24.4.0

- **新しいKnox Platform for Enterprise Keyデバイスポリシーを追加:** 新しいデバイスポリシー**Knox Platform for Enterprise Key**が追加されました。このポリシーを使用すると、必要なSamsung Knox Platform for Enterprise (KPE)ライセンス情報を提供し、KPEライセンスを使用してSamsungデバイスのセキュリティを強化できます。詳細については、Knox Platform for Enterprise Keyデバイスポリシーを参照してください。
- **自動登録でセットアップを完了するために最小OSバージョンを適用:** iOS 17では、MDMは自動デバイス登録を使用する際に、登録デバイスに最小オペレーティングシステムバージョンを適用できるようになりました。詳細については、Citrix Endpoint Managementにアカウントを追加するのステップ3を参照してください。
- **iOS 17のReturn to Serviceをサポート:** Return to Service機能により、MDMサーバーはWi-Fiの詳細とデフォルトのMDM登録プロファイルを含む消去コマンドをユーザーデバイスに送信できます。その後、デバイスはすべてのユーザーデータを自動的に消去し、指定されたWi-Fiネットワークに接続し、提供された登録プロファイルを使用してMDMサーバーに再登録します。
- **Samsung Enhanced Attestation v3をサポート:** Samsung Enhanced Attestation v3は、Samsung KnoxデバイスにおけるCEMのセキュリティ機能を向上させます。詳細については、Samsung Knox Enhanced Attestationを参照してください。
- **デバイス登録における並べ替えとフィルタリングの最新化:** CEMのリストビューは現在、ナビゲートが難しく、ユーザーフレンドリーではありません。フィルタリングと並べ替えのオプションを列ヘッダーに移動することで、顧客はこれらの機能を簡単に組み合わせることができ、必要なデータを見つけるのがはるかに簡単で直感的になります。
- **iOSデバイスのOSアップデートを即座にインストールするサポート:** OSアップデートデバイスポリシーに、iOSのOSアップデートオプションとして**Install ASAP**という新しいラジオボタンが追加されました。この機能により、以前にダウンロードしたOSアップデートをiOSデバイスに即座にインストールできます。詳細については、iOS用OSアップデートデバイスポリシーを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **自動Always-On VPN接続の再起動を強化:** Citrix Secure Accessアプリに新しい管理構成設定**Always On VPN (optional)**が追加されました。この強化がAlways On VPNプロファイルで確実に機能するためには、これを「true」に設定する必要があります。詳細については、Android用Citrix SSOプロトコルを構成するおよびCitrix SSO用のAndroid Enterprise管理構成を作成するを参照してください。

CEM 24.4.0で修正された問題

- iOSデバイスでアップグレード後にエンタープライズアプリが誤ったバージョン番号を報告する場合があります。
- 登録済みのiOSデバイスでSecure HubにUPNの入力を求められます。

シトリックス エンドポイント マネジメント 24.1.0

このバージョンでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題が修正されています。新機能の追加はありません。

シトリックス エンドポイント マネジメント 23.12.0

Androidの802.1x設定に新しい必須フィールド「ドメイン」を追加: Android Enterpriseプラットフォームネットワークポリシー設定ページに、**802.1x EAP**認証タイプ用の新しいフィールド**ドメイン**が追加されました。詳細については、Androidの802.1x設定を参照してください。

現在の既知の問題

Citrix Endpoint Management 25.9.0 の既知の問題

管理者がiOS、macOS、またはAndroid（レガシーデバイス管理者）用の既存のエンタープライズアプリを更新するためにアプリケーションファイルをアップロードすると、更新が失敗します。新しいエンタープライズアプリの作成は影響を受けず、既存のアプリの編集のみが影響を受けます。

Citrix Endpoint Management 22.6.0 の既知の問題

トラブルシューティングとサポート > ログで、3つのログタイプ（**デバッグ**、**管理者監査**、**ユーザー監査**）すべてを選択してダウンロードしようとすると、断続的に機能しません。デバッグログのみがダウンロードされます。回避策として、各ログを個別にダウンロードするか、ブラウザをシークレットモードで開き、3つのチェックボックスすべてをオンにしてすべてのログをダウンロードできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android EnterpriseでWebリンクを作成する際、アイコン付きでアプリを保存しようとするとエラーが発生します。このエラーはGoogleサービスの問題です。回避策として、アイコンをアップロードせずにアプリを保存してください。

Samsung Knox/SAFEポリシーは、非推奨となった後も登録済みデバイスで引き続き有効であり、無効にしたり構成したりすることはできません。回避策として、デバイスの登録を解除し、再登録してください。

Citrix Endpoint Management 22.4.0 の既知の問題

監視タブで登録済みActive Directoryユーザーを検索しても、そのユーザーに登録されているデバイスは表示されません。ユーザーに割り当てられているポリシーやアプリは引き続き表示され、**管理 > デバイス**からすべてのセキュリティアクションを使用できます。iOSおよびAndroidの両方の登録済みデバイスが影響を受けます。

Googleサービスの問題により、Android Enterpriseを使用したプライベートアプリの公開に失敗します。この問題が解決され次第、ドキュメントを更新します。

Citrix Endpoint Management 21.12.0 の既知の問題

Citrix CloudベースのRBACに移行した後、Citrix Cloudでフルアクセス権限を持つ管理者ユーザーは、移行前にカスタム権限を持っていた場合でも、CEMでフルアクセス権限を取得します。回避策として、Citrix CloudのIDおよびアクセス管理ページで、必要なアクセス権限を持つ管理者権限を更新できます。

2018年以前にオンボーディングしたお客様は、コンソールへのローカル管理者アクセス権を持っています。ローカルユーザーの追加または編集権限を持つCEM管理者ユーザーは、Citrix Cloudでもローカルユーザーを追加または編集できます。これらの権限には、ローカルユーザーのパスワード変更が含まれます。この問題を解決するには、サポートに連絡して、コンソールへの直接ローカル管理者アクセスをブロックし、Citrix Cloud管理者アクセスのみを許可するように依頼できます。

Citrix Endpoint Management 21.11.0 の既知の問題

MAMのみに登録されているiOSデバイスでは、エンタープライズアプリのインストールに失敗します。

CEMサーバーが21.11.0にアップグレードされると、Android Enterpriseの**管理対象アプリを自動的に更新**ポリシーがデバイスに適用されません。このポリシーの失敗は、デバイス上のアプリの更新に影響を与えます。回避策として、管理者はポリシーを編集して保存し、デフォルト値を更新できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 21.10.0 の既知の問題

VPNデバイスポリシーが、管理対象のWindows 11デバイスで正常に動作しません。この問題はMicrosoftに報告済みであり、解決に向けて協力しています。進捗があり次第、更新情報を提供します。

Citrix Endpoint Management 21.9.1 の既知の問題

会社所有デバイスモードの仕事用プロファイルに登録されているAndroidデバイスの場合：ユーザーは、個人用プロファイルでアプリをインストールまたは検索できないというエラーが表示されることがあります。これらのエラーが表示された場合は、Google Playストアアプリを更新して、もう一度試してください。

Citrix Endpoint Management 21.5.0 の既知の問題

ユーザーが次の条件を満たす場合、Azure Active Directory (AAD) に対して認証できません。

1. AAD資格情報を使用してデバイスをCitrix Endpoint Managementに登録する。
2. Office 365アプリを起動し、AAD登録を完了する。
3. Microsoft Authenticatorアプリからアカウントを削除する。
4. Office 365アプリを起動し、サインアウトする。

回避策として、デバイスをCitrix Endpoint Managementから登録解除し、再登録します。

Citrix Endpoint Management 21.4.0 の既知の問題

再登録しようとしているユーザーが、デバイスに最初に登録されたユーザーとは異なるAzure Active Directoryユーザーである場合、iOSデバイスでの再登録は失敗します。回避策として、再登録する前に、デバイスのMicrosoft Authenticatorアプリから元のユーザーの登録を解除してください。

Citrix Endpoint Management 21.2.0 の既知の問題

Citrix Secure WebをAndroid Enterprise用のMDXアプリとして追加する場合、Managed Google Playはアプリ識別子を使用してアプリを見つけることができません。アプリ識別子の代わりに「Citrix Secure Web」で検索すると、Managed Google Playはアプリを見つけることができます。この問題はGoogleのバグです。

SSLリスナー証明書のインポートに失敗する場合があります。CTX-297153の手順に従って、証明書キーストアを再パッケージ化してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 20.10.1の既知の問題

オンプレミスのCitrix ADCを13.0-64.35以降にアップグレードし、Citrix Endpoint ManagementがWorkspace対応でない場合：Citrix FilesまたはShareFileドメインURLへのシングルサインオンでエラーが発生します。ユーザーはサインインできません。このエラーは、**会社従業員サインイン**オプションのあるブラウザでのみ発生します。

この問題を回避するには：NetScaler GatewayのADC CLIから以下のコマンドをまだ実行していない場合は、グローバルSSOを有効にするために実行してください。

```
set vpn parameter SSO ON
```

```
bind vpn vs <vsName> -portalTheme X1
```

詳細については、以下を参照してください。

- Citrix ADCリリース
- 影響を受けるSSO構成

回避策を完了すると、ユーザーは**会社従業員サインイン**オプションのあるブラウザでSSOを使用してCitrix FilesまたはShareFileドメインURLに認証できるようになります。

Citrix Endpoint Management 20.2.1の既知の問題

Citrix Endpoint ManagementコンソールでShareFile URLを使用してShareFileを設定した後、**接続テスト**ボタンをクリックするとエラーが発生します。この問題を解決するには、ShareFileの多要素認証を無効にします。この問題と回避策の詳細については、2段階認証のユーザー電話番号をリセットを参照してください。

Citrix Endpoint Management 20.1.0の既知の問題

Citrix Cloudのライブラリにユーザーを追加する際、Citrix Endpoint Managementは成功を報告しますが、ユーザーは追加されません。

Citrix Endpoint Management 19.11.0の既知の問題

MDX およびパブリックアプリはコンソールから削除できません。回避策として、削除したいアプリを選択し、**編集**をクリックします。**Android Enterprise**の選択を解除し、プラットフォームリストから他のプラットフォームを選択します。アプリを保存します。その後、アプリを削除できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 19.5.0 の既知の問題

Citrix Ready® workspace hub デバイスを登録する際、登録失敗を避けるために、許可リストにイーサネット (eth0) MAC アドレスを定義してください。

Citrix Endpoint Management 19.4.1 の既知の問題

Windows GPO デバイスポリシーのオプションをタブで移動すると、ラジオボタンとチェックボックスがスキップされます。

Citrix Endpoint Management 19.2.1 の既知の問題

Google 管理コンソールから削除することで Android Enterprise エンタープライズの登録を解除した場合、そのエンタープライズを再登録しようとすると失敗する可能性があります。Android Enterprise エンタープライズの登録解除で説明されているように、Android Enterprise エンタープライズの登録解除には常に Citrix Endpoint Management コンソールを使用してください。Google Workspace のお客様は、Android Enterprise エンタープライズの登録解除の手順に従ってください。

Citrix Endpoint Management 19.2.0 の既知の問題

Citrix Endpoint Management 10.18.3 でパブリックストアアプリを作成する際、iPad アプリ設定ページでアプリを検索せずに**戻る**をクリックし、その後**次へ**をクリックすると、以下の問題が発生します。ナビゲーションボタンが応答しなくなり、アプリを検索できなくなります。この問題は、iOS または Android の両方でパブリックストアアプリを作成する際に発生します。

Citrix Endpoint Management 10.19.1 の既知の問題

設定 > Android Enterprise ページで登録プロセスを完了すると、次のエラーメッセージが表示されます: `A configuration error occurred. Please try again`。エラーメッセージを閉じると、Android Enterprise の構成は保存されますが、**Android Enterprise を有効にする**は**オフ**になります。この問題を回避するには、アプリカテゴリの数を 30 以下に減らしてください。

Citrix Endpoint Management 10.18.5 の既知の問題

Chrome アプリが Chrome OS デバイスの必須アプリとして構成されている場合、ユーザーはアプリをインストールするためにログオフして再度ログインする必要がある場合があります。このサードパーティの問題は、Google のバグ ID #76022819 です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 10.18.3 の既知の問題

デバイスが登録されている Citrix Cloud 管理者を削除した後、管理者が Citrix Secure Hub アプリまたはセルフヘルプポータルから再度ログインするまで、Citrix Endpoint Management コンソールでユーザーロールが更新されません。

Citrix Endpoint Management 10.7.4 の既知の問題

Citrix Endpoint Management を Citrix ID プロバイダーと Azure Active Directory を使用してシングルサインオン (SSO) 用に構成した場合: Citrix Endpoint Management の管理者またはユーザーが **Azure Active Directory サインイン**画面にリダイレクトされると、その画面には「Citrix Secure Hub のサインインページ」というメッセージが表示されます。正しいメッセージは「Citrix Endpoint Management コンソールのサインインページ」です。

新機能の履歴

以前のCitrix Endpoint Managementリリースに関するセクションを、新機能からこの記事に移動しました。

シトリックス エンドポイント マネジメント 23.9.0

注:

製品リリースのロールバックにより、Citrix Endpoint Management 23.9.0のドキュメント更新はロールバックされました。

シトリックス エンドポイント マネジメント 23.7.0

- **Play Integrity API:** Play Integrity APIは、Googleによる非推奨のタイムラインに従い、間もなく非推奨となるSafetyNet Attestation APIに代わるものです。このAPIを有効にするための詳細と手順については、Play Integrity APIを有効にするを参照してください。
- **iOSデバイスでのeSIMおよびデュアルSIM機能のサポート:** Citrix Endpoint Managementは、iOSデバイスでのeSIMおよびデュアルSIM機能をサポートするようになりました。eSIMサポートにより、iOSデバイスから電話番号、IMEI、ICCIDなどの情報を取得し、Citrix Endpoint Management UIに表示できます。デバイスのプロパティの詳細については、デバイスプロパティ名と値を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント管理 23.6.0

macOS 14デバイスのサポート: Citrix Endpoint Managementは、macOS 14を使用しているAppleデバイスをサポートするようになりました。詳細については、オペレーティングシステムのサポートリストを参照してください。

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題が解決されています。

シトリックス エンドポイント管理 23.4.0

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題が解決されています。新機能は追加されていません。

シトリックス エンドポイント マネジメント 23.2.0

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題が解決されています。新機能は追加されていません。

シトリックス エンドポイント マネジメント 23.1.0

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題が解決されています。新機能は追加されていません。

シトリックス エンドポイント マネジメント 22.12.0

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題が解決されています。新機能は追加されていません。

シトリックス エンドポイント マネジメント 22.10.0

以下の機能は現在、商用顧客向けに展開されています。米国政府機関の顧客へのリリースは3か月以内に開始されます。商用版と米国政府機関向け版の機能の違いについては、「Citrix Endpoint Management service for US Government」を参照してください。

Windows Information Protectionポリシーは削除されました。詳細については、「Deprecation」を参照してください。

Windows 11 22H2のサポート。Citrix Endpoint Managementでは、IT管理者が既存のMDM機能を使用してWindows 11 22H2デバイスをCEMに登録できるようになりました。Windowsデバイスの登録の詳細については、「Windows Desktop and Tablet」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS 13がサポートされるようになりました。Citrix Endpoint Managementは、macOSバージョン13を使用するAppleデバイスをサポートするようになりました。

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つさまざまな問題も解決されています。

シトリックス エンドポイント マネジメント 22.9.0

Android 13およびiOS 16のサポート。Citrix Endpoint Managementは、Android 13およびiOS 16をサポートするようになりました。

プロセッサの種類とプロセッサアーキテクチャ。CEMコンソールのWindowsデバイスには、各デバイスのプロセッサの種類とプロセッサアーキテクチャも表示されるようになりました。

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つさまざまな問題も解決されています。

シトリックス エンドポイント マネジメント 22.7.0

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つさまざまな問題が解決されています。新機能は追加されていません。

修正

断続的に、**トラブルシューティングとサポート > ログ**でダウンロードする3種類のログ（**デバッグ**、**管理者監査**、**ユーザー監査**）をすべて選択しても、機能しません。デバッグログのみがダウンロードされます。回避策として、各ログを個別にダウンロードするか、ブラウザをシークレットモードで開き、3つのチェックボックスすべてをオンにしてすべてのログをダウンロードできます。

Android EnterpriseでWebリンクを作成する際、アイコン付きでアプリを保存しようとするとエラーが発生します。これはGoogleサービスの問題です。回避策として、アイコンをアップロードせずにアプリを保存してください。

Samsung Knox/SAFE ポリシーは、非推奨になった後も登録済みデバイス上で有効なままであり、無効にしたり構成したりすることはできません。回避策として、デバイスの登録を解除し、再登録してください。

シトリックス エンドポイントマネージメント 22.6.0

デバイス上のすべてのプロファイルでGoogle Play以外のアプリを許可する新しい制限ポリシーを追加しました。詳細については、「制限デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

モバイルサービスプロバイダー（MSP）インターフェイスのサポートを非推奨にしました。コンソールからMSPインターフェイスを削除する新しいサーバープロパティを追加しました。詳細については、「サーバープロパティ」を参照してください。

Nexmo SMSゲートウェイのサポートを非推奨にしました。Nexmo SMSのサポートは、デフォルトでTrueに設定されているdeprecate.carrier.sms.gatewayというサーバープロパティを追加することで非推奨になりました。Nexmo SMSはセルフヘルプポータルでも非推奨になりました。詳細については、「通知」を参照してください。

Android Enterpriseの仕事用プロファイルと個人用プロファイル間で、選択したアプリが通信できるようになりました。Android Enterpriseの制限ポリシーに「接続済みアプリを有効にする」という新しいトグルが追加され、選択したアプリが仕事用データと個人用データの両方を使用できるようになりました。詳細については、「制限ポリシー」を参照してください。

Googleは、Citrix Endpoint Managementでアプリのカテゴリとライセンスに使用されるいくつかのAPIを非推奨にしています。

- アプリを承認するのではなく、追加するアプリを選択するようになりました。詳細については、「管理対象アプリストアアプリ」を参照してください。
- Android Enterpriseでは、アプリをカテゴリではなくコレクションに整理するようになりました。詳細については、「アプリの整理（Android Enterprise）」を参照してください。
- MDXアプリを承認する必要がなくなりました。詳細については、「MDXアプリの追加」を参照してください。
- アプリライセンスをユーザーから関連付け解除できなくなりました。詳細については、「アプリの追加」を参照してください。

シトリックス エンドポイントマネージメント 22.5.0

Windows 10デバイス向けの「WiFi Senseホットスポットへの自動接続を許可する」制限ポリシーのサポートが削除されました。詳細については、Windowsデスクトップ/タブレット設定を参照してください。

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つ多くの問題も解決されています。

シトリックス エンドポイント マネジメント 22.4.0

OSアップデートデバイスポリシーに、OSアップデートをインストールできないフリーズ期間を設定する新しいオプションが追加されました。詳細については、OSアップデートデバイスポリシーを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つ多くの問題も解決されています。

シトリックス エンドポイント マネジメント 22.3.0

一定期間非アクティブだったデバイスを自動的に削除できるようになりました。(プレビュー) プレビューとして、**指定された期間非アクティブとしてマークされたデバイスの削除を許可する**という新しいサーバープロパティが追加されました。これは、指定された期間（日数）非アクティブだったデバイスを削除するバックグラウンドジョブを実行します。詳細については、サーバープロパティを参照してください。

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つ多くの問題も解決されています。

シトリックス エンドポイント マネジメント 22.2.0

Windows 11デバイスを使用する場合、インベントリ結果が表示されるまでに24時間待つ必要があるという注意書きが、アプリインベントリデバイスポリシーに追加されました。詳細については、アプリインベントリデバイスポリシーを参照してください。

Android Enterpriseの「システムアップデートポリシー」に「デフォルト」オプションが追加され、管理者がシステムアップデートポリシーをデフォルト値に復元できるようになりました。詳細については、OSアップデートデバイスポリシーを参照してください。

デバイス上のすべてのプロファイルでGoogle Play以外のアプリを許可する新しい制限ポリシーが追加されました。詳細については、制限デバイスポリシーを参照してください。

以下の機能のサポートは削除されました。

- **RBACロール - 共有デバイスおよびCOSUデバイス登録者**
- **Android - Sony および HTC**
- **高セキュリティ登録モード**
- **派生資格情報**
- **SEAMS**
- **Windows Phoneデバイス** 詳細については、廃止を参照してください。

個人プロファイルから仕事用プロファイルへのファイルのコピー、貼り付け、インポートを制限する新しい制限ポリシーを追加しました。詳細については、「制限デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント マネジメント 22.1.0

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つ多数の問題が解決されています。新機能は追加されていません。

シトリックス エンドポイント管理 21.12.0

Citrix Identity Providerを使用したApple Deployment Program対応iOSデバイスの登録のサポート。Apple Deployment Programを通じてiOSデバイスを展開する場合、Apple Business Managerユーザーが Citrix Identity ProviderをIDプロバイダーとして使用してデバイスを登録できるようになりました。この機能は、Citrix Cloudを介したAzure Active DirectoryおよびOktaとの認証をサポートします。詳細については、「Apple Deployment Programによるデバイスの展開」を参照してください。

iOSでユーザーがデフォルトでプロキシを構成および使用できるようにする。iOSデバイスのユーザーは、デバイスで構成したプロキシをデフォルトで使用できるようになりました。クライアント側プロキシの使用を防止するには、この機能のクライアントプロパティをfalseに変更します。この設定の詳細については、「クライアントプロパティ」を参照してください。

iOSデバイスにBluetoothデバイスポリシーを追加。監視対象のiOSデバイスでBluetoothを有効または無効にするBluetoothデバイスポリシーを構成できるようになりました。この設定の詳細については、「Bluetoothデバイスポリシー」を参照してください。

Citrix Endpoint Management 21.12.0で修正された問題

Android Enterpriseの**管理対象アプリを自動的に更新**ポリシーは、CEMサーバーが21.11.0にアップグレードされると、デバイスに適用されません。ポリシーの失敗は、デバイス上のアプリの更新に影響します。回避策として、管理者はポリシーを編集して保存し、デフォルト値を更新できます。

シトリックス エンドポイント管理 21.11.0

Android Enterprise管理対象アプリの自動更新の優先度を構成します。 Android Enterprise管理対象アプリを低優先度または高優先度で自動更新するかどうかを指定できるようになりました。自動更新を延期することもできます。詳細については、「管理対象アプリの自動更新デバイスポリシー」を参照してください。

グループ化タイプとプレビュータイプの設定に対するアプリ通知デバイスポリシーのサポート。これらの2つの設定により、監視対象のiOSデバイスでアプリ通知がどのようにグループ化され、プレビューされるかを制御できます。詳細については、「アプリ通知デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ属性デバイスポリシーがより多くのiOSアプリ属性をサポート。 iOSデバイスにインストールされているアプリに対して、次の属性を指定できるようになりました。

- **削除可能なアプリ:** 管理対象アプリである場合に、ユーザーがアプリを削除できるかどうかを指定します。iOS 14以降に適用されます。

関連ドメイン機能の属性:

- **関連ドメイン:** アプリに追加する関連ドメインを指定します。iOS 13以降に適用されます。
- **関連ドメインの直接ダウンロードを有効にする:** 要求されたサイト関連付けの検証をドメインで直接有効にするかどうかを指定します。iOS 14以降に適用されます。

詳細については、「アプリ属性デバイスポリシー」を参照してください。

Citrix Endpoint Management 21.11.0で修正された問題

断続的に、**［設定］>［NetScaler Gateway］ページから［構成スクリプトのエクスポート］**をクリックすると、破損したCSVファイルが受信されます。回避策として、NetScaler Gateway構成を追加または編集する際に構成スクリプトをダウンロードします。

シトリックス エンドポイント マネジメント 21.10.1

非アクティブ後のデバイスロックの延長。 デバイスがロックされるまでの最大非アクティブ時間が15分に延長されました。詳細については、「パスコードデバイスポリシー」を参照してください。

iOSアプリからのコンテンツの貼り付けに関する制限設定を追加。 制限デバイスポリシーがiOSの**［管理対象ペーストボードを要求］**をサポートするようになりました。この制限設定により、管理対象アプリから非管理対象アプリへのコンテンツの貼り付け、およびその逆をブロックまたは許可できます。

この設定はiOS 15以降に適用されます。詳細については、「iOS用制限デバイスポリシー」を参照してください。

Citrix Endpoint Management 21.10.1で修正された問題

WPA2およびWPA3ネットワークセキュリティタイプを使用しているiOSおよびmacOSデバイスにネットワークポリシーを展開できません。

シトリックス エンドポイント マネジメント 21.10.0

Citrix Cloudでクラウド管理者用のカスタムロールを割り当てる。 October 4, 2021以降にオンボーディングされた新規のCitrix Endpoint Managementのお客様は、Citrix Cloudでクラウド管理者

© 1997–2026 Citrix Systems, Inc. All rights reserved.

にカスタムロールを割り当てることができるようになりました。以前は、Citrix Endpoint Managementでカスタムロールを割り当てる必要がありました。この機能により、Citrix CloudとCitrix Endpoint Managementを切り替えることなく、管理者関連のカスタマイズを実行できます。さらに、**COSUデバイス登録者**および**共有デバイス登録者**テンプレートはCitrix Endpoint Managementから削除されました。**COSUデバイス登録者**は登録プロファイルを通じて処理されるようになり、**共有デバイス登録者**はキオスクモードまたはCitrix Launcherを使用してプラットフォームレベルで処理されます。

Windows 11デバイスのサポート。 Citrix Endpoint Managementを使用してWindows 11デバイスを管理できるようになりました。詳しくは、オペレーティングシステムサポートリストを参照してください。

iOSユーザー登録モードがパブリックプレビューとして利用可能になりました。 iOSおよびiPadOSデバイスでAppleユーザー登録機能を利用できるようになりました。ユーザー登録は、管理対象Apple IDを統合してデバイス上にユーザーIDを作成します。ユーザー登録の詳細については、管理対象Apple IDを参照してください。

iOSデバイスの位置追跡の最大値が更新されました。 位置情報ポリシーを構成して、iOSデバイスの位置を最大10時間追跡できるようになりました。位置情報デバイスポリシーを参照してください。

Citrix Endpoint Management 21.10.0で修正された問題

Citrix Cloudコンソールで管理者ロールを更新しても、その変更がCitrix Endpoint Managementコンソールに反映されません。この問題は厳密にはユーザーインターフェイスの問題であり、機能には影響しません。バージョン21.10.0以降でオンボーディングされたお客様のみが影響を受けます。

Androidデバイスの登録プロファイルを作成して、企業所有デバイスモードで仕事用プロファイルに登録する場合、**BYOD仕事用プロファイル**設定を有効にする必要があります。この設定を有効にしないと、デバイスの登録に失敗します。

シトリックス エンドポイント マネジメント 21.9.1

Cloud Connectorなしでユーザーデバイスを登録および管理するためのIDプロバイダーとしてAzure ADまたはOktaを構成する（プレビュー）。 Citrix Cloudを通じてIDプロバイダーを構成する場合、Citrix Endpoint ManagementとCitrix Cloud間の通信を確立するためにCloud Connectorは必要ありません。Citrix Endpoint Managementでは、以下の目的でCloud Connectorが引き続き必要です。

- LDAP
- PKIサーバー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 内部DNSクエリ
- シトリックス バーチャル アプリ™

この機能の詳細については、「IDプロバイダー認証」を参照してください。

iOS 15およびmacOS 12デバイスのサポート。 Citrix Endpoint Managementを使用して、iOS 15およびmacOS 12デバイスを管理できるようになりました。詳細については、「オペレーティングシステムのサポートリスト」を参照してください。

Android Enterprise向け常時接続VPN。 Android Enterpriseデバイスで常時接続VPNを有効にできるようになりました。ロックダウン機能を有効にすることもできます。ロックダウンから除外しない限り、アプリがネットワークにアクセスするにはVPN接続が必要です。詳細については、「VPNデバイスポリシー」を参照してください。

完全に管理されたAndroid 11以降のデバイスが、企業所有デバイスモードで仕事用プロファイルに登録されるようになりました。 この新しいモードでは、デバイス上の個人用プロファイルと仕事用プロファイルがさらに分離されます。この変更により、組織は管理対象プロファイルをより詳細に制御できるようになり、ユーザーは個人用プロファイルのプライバシーをより保護できるようになります。詳細については、「Android Enterprise」を参照してください。

クライアントアプリのグローバル同意を設定する機能。 グローバル同意を設定できるようになり、ユーザーは各デバイスで同意を提供する必要がなくなりました。詳細については、「Azure ADコンプライアンス管理のためにCitrix Endpoint Managementを構成する」を参照してください。

Azure ADの権限変更が検出されるようになりました。 Azure ADの権限に変更が発生すると、Citrix Endpoint Managementは自動的にその変更について警告し、**Azure ADコンプライアンス管理**設定を使用して承認できるようになりました。同意リンクに従って**承認**をクリックし、変更を受け入れます。以前は、この承認を手動で開始する必要がありました。詳細については、「Azure ADコンプライアンス管理のためにCitrix Endpoint Managementを構成する」を参照してください。

Citrix Endpoint Management 21.9.1で修正された問題

展開ルールをデリバリーグループに追加すると、リソースレベル（ポリシー、アプリ、アクション）の新規または既存の展開ルールは適用されなくなります。

Citrix Endpoint Managementのデータエクスポート機能では、完全なデータセットがエクスポートされません。管理対象デバイスに関するデータを取得するには、以下の回避策を使用してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- コンソールから**Analyze > Reporting > Device Enrollment**に移動してデータをエクスポートします。
- レポートAPIを使用してデータをエクスポートします。レポートAPIの詳細については、「開発者向けドキュメント」を参照してください。

Citrix Cloud経由でCitrix Endpoint Managementにアクセスしている場合、macOS用のエンタープライズアプリを追加すると、認証エラーが発生します。回避策として、サポートに連絡してCitrix Endpoint Managementコンソールへの直接アクセスを要求してください。その後、macOSデバイス用のエンタープライズアプリを追加できます。

シトリックス エンドポイント マネジメント 21.9.0

Chrome OS資格情報ポリシー設定（プレビュー）。 Chrome OSで資格情報ポリシー設定が利用可能になりました。Chromebookデバイスは、資格情報ポリシーを使用して、Chromeオペレーティングシステムの組み込み証明書管理を活用できます。管理者は、クライアント証明書の署名と発行のために、証明機関の秘密証明書をアップロードできます。この証明書により、Citrix Endpoint ManagementはChromebookデバイスに証明書を作成してプッシュできます。詳細については、「資格情報デバイスポリシー」を参照してください。

Citrix Endpoint Management 21.9.0で修正された問題

iOS 15 または macOS 12 デバイスを登録した後、MDM 構成プロファイルが「未確認」と表示されます。

シトリックス エンドポイント マネジメント 21.8.0

Android 12 のサポート。 Citrix Endpoint Management は、Android Enterprise デバイスの Android 12 への更新をサポートするようになりました。セキュリティとプライバシーの利点の概要については、Android ドキュメント を参照してください。

Android Enterprise 登録用の QR コードを生成する際の JSON 出力編集のサポート。 Android Enterprise 登録用の QR コードを生成する際に、JSON 出力を直接編集することで、登録情報を QR コードに追加できるようになりました。詳細については、Android Enterprise を参照してください。

管理対象のオプションアプリを自動的に更新。 管理対象のオプションアプリは自動的に更新されるようになりました。この機能には、オプションのエンタープライズアプリ、オプションのボリューム購入アプリ、およびオプションのパブリックアプリが含まれます。ボリューム購入アプリの詳細については、Apple ボリューム購入アカウントの追加 を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS デバイスを Wi-Fi ネットワークに接続する際に Active Directory を使用してユーザーを認証。 Citrix Endpoint Management は、macOS デバイスが構成された Wi-Fi ネットワークに接続するたびに Active Directory を使用した認証をサポートするようになりました。この機能は、以下のセキュリティタイプにのみ適用されます。

- **WEP エンタープライズ**
- **WPA エンタープライズ**
- **WPA2 エンタープライズ**
- **任意 (エンタープライズ)**

詳細については、ネットワークデバイスポリシー を参照してください。

新しいデリバリーグループのベースとしてデリバリーグループを複製。 この機能を使用すると、複数のポリシー、アプリ、およびアクションを含む複雑なデリバリーグループをコピーできます。その後、登録プロファイルや新しい Active Directory ユーザーセットの追加など、コピーを編集できます。詳細については、デリバリーグループの複製 を参照してください。

Azure AD デバイスコンプライアンスの一般提供。 Citrix Endpoint Management は、Azure AD 条件付きアクセスポリシーを介した Azure AD デバイスコンプライアンスをサポートするようになりました。この機能の詳細については、Azure AD 条件付きアクセスとの統合 を参照してください。

Citrix Endpoint Management 21.8.0 で修正された問題

ユーザー名またはパスワードに特定の特殊文字が含まれているユーザーは登録できません。

シトリックス エンドポイント マネジメント 21.7.1

このリリースには、全体的なパフォーマンスと安定性の改善に役立つ機能強化が含まれています。

Citrix Endpoint Management 21.7.1 で修正された問題

Citrix Endpoint Management のIDプロバイダーを構成する際、オプションフィールドを構成しない場合、エンドユーザーは認証できません。

シトリックス エンドポイント マネジメント 21.7.0

Citrix Cloud を介して Azure Active Directory または Okta で認証する場合、iOS および Android デバイス用に異なる登録プロファイルを作成できるようになりました。 Citrix Cloud を介して Azure Active Directory または Okta を認証方法として構成すると、Citrix Endpoint Management は、さまざまな登録タイプの複数の登録プロファイルをサポートします。詳細については、登録プロファイルを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスの種類と登録モードに基づいてデバイスを自動的にタグ付けします。 サーバープロパティ `enable.device.tagging` を有効にすると、Citrix Endpoint Management は、新しく登録されたすべてのデバイスにタグを付けます。デバイスタグを使用して、ポリシーとアプリを展開したり、デリバリーグループを構成したりできます。Citrix Endpoint Management は、以下のデバイスにタグを適用します。

- BYOD タグ
  - iOS ユーザー登録
  - Android Enterprise ワークプロファイル
- 企業タグ
  - Android Enterprise の完全に管理された企業デバイス
  - 一括登録
    - Apple Business Manager デバイス
    - Apple School Manager デバイス
    - Windows AutoPilot デバイス
    - Android Enterprise 一括登録

詳細については、「サーバープロパティ」を参照してください。

ワークスペースエクスペリエンスが有効なCitrix Endpoint Managementのお客様向け: Citrix Endpoint Managementは、Citrix Workspaceアプリを介してMDMに登録するユーザー向けに、Azure Active Directory、Okta、およびオンプレミスのNetScaler Gatewayによる認証をサポートしています。詳細については、「Citrix Cloudを介したAzure Active Directoryによる認証」、「Citrix Cloudを介したOktaによる認証」、および「Citrix Cloudを介したオンプレミスのNetScaler Gatewayによる認証」を参照してください。

シトリックス エンドポイント マネジメント 21.6.0

Wi-Fiデバイスポリシーをネットワークデバイスポリシーに名称変更しました。macOSのイーサネットサポートに対応するため、Wi-Fiデバイスポリシーを「ネットワークデバイスポリシー」に名称変更しました。 macOSでは、Wi-Fiオプションに加えて、以下のイーサネットオプションが利用できるようになりました。

- グローバルイーサネット
- 最初の有効なイーサネット
- 2番目の有効なイーサネット

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 3番目の有効なイーサネット
- 最初のイーサネット
- 2番目のイーサネット
- 3番目のイーサネット

詳細については、「ネットワークデバイスポリシー」を参照してください。

Shared iPadでのApple Business Manager (ABM) およびすべてのユーザーの削除のサポート。 ユーザーはABMアカウントを使用してShared iPadにサインインできるようになりました。「すべてのユーザーの削除」セキュリティアクションもShared iPadで利用できます。詳細については、「Shared iPad」を参照してください。

Citrix Endpoint Management REST APIを使用して、iOSデバイスに証明書を一括アップロードします。 証明書を1つずつアップロードするのが実用的でない場合は、Citrix Endpoint Management Server REST APIを使用して、iOSデバイスに証明書を一括アップロードします。

1. 接続タイプを**Always on IKEv2**としてiOS VPNデバイスポリシーを構成します。
2. デバイス認証方法として**デバイスIDに基づくデバイス証明書**を選択します。
3. 使用する**デバイスIDタイプ**を選択します。
4. REST APIを使用してデバイス証明書を一括インポートします。

VPNデバイスポリシーの構成については、「VPNデバイスポリシー」を参照してください。証明書の一括インポートについては、「REST APIを使用してiOSデバイスに証明書を一括アップロードする」を参照してください。

iOSアプリのフルトンネルモードの廃止。 このリリース以降、MDXはiOS向けCitrixモバイル生産性向上アプリのフルトンネルモードをサポートしなくなりました。ネットワークアクセスアプリポリシーから以下のオプションが削除されました。

- 以前の設定を使用
- トンネル化 - フルVPN
- トンネル化 - フルVPNおよびWeb SSO

トンネル化 - フルVPNまたは**トンネル化 - フルVPNおよびWeb SSO**ポリシーを使用している場合は、**トンネル化 - Web SSO**ポリシーに切り替える必要があります。廃止されたポリシーを使い続けると、メールは同期されません。詳細については、「MDXアプリのSSOとプロキシに関する考慮事項」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

より詳細な証明書選択。 Microsoft PKI、汎用PKI、資格情報ポリシー、または資格情報プロバイダーを構成する場合、証明書メニューは証明書を区別するためのより役立つ情報を提供します。この情報には以下が含まれます:

- 証明書名
- 証明書が有効になる日付
- 証明書が有効な期限日
- 証明書のシリアル番号

シトリックス エンドポイント マネジメント 21.5.1

このリリースには、全体的なパフォーマンスと安定性の向上に役立つ機能強化が含まれています。

シトリックス エンドポイント マネジメント 21.5.0

Citrix Secure Hub APNs証明書の更新。 Citrix Endpoint Management 用のCitrix Secure Hub Apple Push Notification Service (APNs) 証明書は、June 17, 2021に期限切れになります。このアップデートにより、May 7, 2022に期限切れとなるCitrix Secure Hub APNs証明書が更新されます。

FIPS 140-2準拠。 Citrix Endpoint Managementのサーバー側コンポーネントは、FIPS 140-2に準拠するようになりました。詳細については、「FIPS 140-2準拠」を参照してください。

Citrix Endpoint Management 21.5.0で修正された問題

以前の「Get Devices by Filters」APIの問題を解決し、一度に最大100台のデバイスに対してページ分割された結果を返す新しい「Get Devices by Filters」APIが追加されました。詳細については、Public API for REST Services PDFの「3.16.3 Get Devices by Filters」セクションを参照してください。

パッケージIDを使用してCitrix Endpoint Managementコンソールに追加するGoogle Playアプリを検索すると、必須の**名前**フィールドが空で表示されます。アプリ名は手動で入力できます。

シトリックス エンドポイント マネジメント 21.4.0

Citrixは、Google Android Enterprise Advanced Management Solution Setの検証を受けました。詳細については、「Citrix Endpoint Management earns new Android Enterprise verification」を参照してください。

Azure AD条件付きアクセスとの統合 (プレビュー)。 Citrix Endpoint Managementを構成して、Office 365アプリケーションにAzure AD条件付きアクセスサポートを適用できるようになりまし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

た。この機能は現在プレビュー版であり、Office 365アプリケーションを展開する際に、デバイスユーザーにゼロトラスト手法を展開できます。管理対象のAndroid EnterpriseおよびiOSデバイス上のOffice 365アプリケーションへのアクセスを定義するために、デバイスの状態、リスクスコア、場所、およびデバイス保護を使用できます。詳細については、「Integrate with Azure AD Conditional Access」を参照してください。

Androidデバイスプロパティルールを使用して、デリバリーグループのAndroid Enterpriseデバイスへの展開を管理する。 複数のAndroid Enterpriseデバイスを同じユーザーに登録する場合、デバイス登録プロファイルまたはアプリケーションパッケージIDに基づいてデリバリーグループリソースを展開できるようになりました。デリバリーグループ内で、Androidプラットフォームのデバイスプロパティを使用して、新規または既存のAndroid Enterpriseデバイスの高度なルールを作成します。詳細については、「Add a delivery group」を参照してください。

Apple Deployment Programを通じて登録されたmacOSデバイスの管理者パスワードのローテーションのサポート。 Apple Business ManagerアカウントをCitrix Endpoint Managementに追加する際に、macOSデバイスに管理者アカウントを作成するための設定を指定できます。Citrix Endpoint Managementは、セットアップアシスタントのワークフロー中にデバイス上に管理者アカウントを自動的に作成します。ユーザーは、指定された情報を使用してmacOSデバイスにサインインします。Citrix Endpoint Managementは、セキュリティ強化のために、その管理者アカウントのパスワードのローテーションをサポートするようになりました。詳細については、「Deploy devices through the Apple Deployment Program」を参照してください。

Citrix Cloudを介した新しいAutoDiscoveryサービス構成。 AutoDiscoveryサービスは現在Citrix Cloudでホストされています。Citrixは、既存のすべてのAutoDiscoveryサービス構成をサービス中断なしで移行しました。新しいAutoDiscoveryサービスにアクセスするか、構成を変更するには、`https://adsui.cloud.com` (商用) または `https://adsui.cem.cloud.us/` (政府機関向け) にアクセスしてください。詳細については、「Set up the AutoDiscovery service for Citrix Endpoint Management」を参照してください。

新しいAutoDiscoveryサービス構成では、MAMトラフィックをデータセンターに誘導するために、**NetScaler Gateway FQDN**の代わりに**MAM Port**設定を使用します。NetScaler Gatewayのポートとともに完全修飾ドメイン名を入力すると、クライアントデバイスは**MAM Port**設定の構成を使用します。

新しいAutoDiscoveryサービスユーザーインターフェイスにアクセスするために`https://adsui.cloud.com` (商用) または`https://adsui.cem.cloud.us/` (政府機関向け) に移動すると、広告ブロッカーによってサイトが開かない場合があります。AutoDiscoveryサービスにアクセスするには、ウェブサイト全体で広告ブロッカーを無効にしてください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android Enterpriseの制限に設定を追加しました。 Googleの設定との整合性を高め、構成を簡素化するために、すべての登録モードに2つの設定を追加しました。

- **Bluetooth共有を許可:** 選択されていない場合、ユーザーはデバイスでBluetoothによる発信共有を確立できません。
- **アプリのアンインストールを許可:** ユーザーがManaged Google Playストア内からアプリをアンインストールできるようにします。

また、**無線でのアップグレードを許可**設定を制限ポリシーからOSアップデートポリシーに移動しました。

これらの変更の詳細については、「制限デバイスポリシー」および「OSアップデートデバイスポリシー」を参照してください。

コンテンツ配信ネットワーク (CDN) からのMDXアプリ配信のサポート。 MDXアプリでCDNサポートが利用可能になりました。アプリのダウンロードを高速化するために、CDNはCitrix Endpoint Managementサーバーの近くにあるユーザーデバイスにMDXアプリを送信します。CDNを使用することで、アプリのダウンロード時間が短縮されます。開始するには、「Citrix CDNからMDXアプリを配信する」を参照してください。

Citrix Endpoint Management 21.4.0で修正された問題

macOS 11.0以降を実行しているデバイスにエンタープライズアプリをインストールできませんが、Citrix Endpoint Managementコンソールには正常にインストールされたと表示されます。

シトリックス エンドポイント マネジメント 21.3.0

Intune管理環境にAndroid Enterpriseアプリを追加するフローを合理化しました。 Android EnterpriseアプリをCitrix Endpoint ManagementコンソールとIntuneコンソールに同時に追加できるようになりました。このワークフローの詳細については、「Citrix Cloud LibraryにAndroid Enterpriseアプリを追加する」を参照してください。

Android Enterprise登録用のQRコードを生成します。 Citrix Endpoint Managementは、Android Enterprise登録用のQRコードを生成できるようになりました。Citrix Endpoint Managementコンソールを使用して登録用のQRコードを生成することで、悪意のある外部サイトを回避できます。QRコードの生成の詳細については、「QRコードを作成する」を参照してください。

macOSデバイスのブートストラップトークンサポート。 Citrix Endpoint Managementは、macOSデバイスのブートストラップトークンのエスクローをサポートするようになりました。ブートストラップトークンは、セットアップアシスタントワークフロー中に生成されます。Citrix Endpoint Managementでブートストラップトークンをエスクローする利点の1つは、リモートアカウントで

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FileVaultを有効にし、FileVaultボリュームのロックを解除できることです。詳細については、「ブートストラップトークン」を参照してください。

シトリックス エンドポイント マネジメント 21.2.0

更新されたCitrix Launcherアプリでは、Android Enterpriseデバイスでユーザーアクセスを1つのアプリまたは少数のアプリに制限できます。 また、オプションで**Citrix Launcher**アイコンのカスタムロゴ画像をアップロードし、ユーザーがアプリを終了するために必要なパスワードを指定することもできます。詳細については、Citrix Launcherを参照してください。

iOSおよびmacOS用の新しい設定アシスタントオプション。 ユーザーがiOSまたはmacOSデバイスを設定する際にスキップする設定画面をさらに指定できるようになりました。

- iOS
  - **復元完了:** セットアップ中に復元が完了したかどうかをユーザーが見るのを防ぎます。iOS 14.0以降の場合。
  - **アップデート完了:** セットアップ中にソフトウェアアップデートが完了したかどうかをユーザーが見るのを防ぎます。iOS 14.0以降の場合。
- macOS
  - **アクセシビリティ:** ユーザーがVoice Overを自動的に聞くのを防ぎます。デバイスがイーサネットに接続されている場合にのみ利用可能です。macOS 11以降の場合。
  - **生体認証:** ユーザーがTouch IDとFace IDを設定するのを防ぎます。macOS 10.12.4以降の場合。
  - **True Tone:** ユーザーがディスプレイのホワイトバランスを動的に調整するための4チャンネルセンサーを設定するのを防ぎます。macOS 10.13.6以降の場合。
  - **Apple Pay:** ユーザーがApple Payを設定するのを防ぎます。この設定がクリアされている場合、ユーザーはTouch IDとApple IDを設定する必要があります。**Apple ID**と**生体認証**の設定がクリアされていることを確認してください。
  - **スクリーンタイム:** ユーザーがスクリーンタイムを有効にするのを防ぎます。macOS 10.15以降の場合。

セットアップオプションの構成の詳細については、Apple Deployment Programを介したデバイスの展開を参照してください。

macOS PKGファイルのアップロードが、ファイルサイズではなくアップロード時間によって制限されるようになりました。 これにより、macOSデバイス用のMicrosoft Officeなどのより大きなPKGファイルをアップロードできるようになります。Citrix Endpoint Managementは、以前のファ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イルサイズ制限0.5 GBを撤廃し、代わりにファイルアップロード時間を制限します。デフォルトでは、アップロードは100秒以内に完了する必要があります。詳細については、エンタープライズアプリの追加を参照してください。

Citrix Endpoint Managementは、証明書ベースの認証における脆弱な暗号化アルゴリズムをサポートしなくなりました。 Citrix Endpoint Managementコンソールで資格情報プロバイダーの証明書署名要求を作成する際は、より強力な暗号を選択してください。削除された署名アルゴリズムのリストについては、非推奨を参照してください。

Citrix Endpoint Management 21.2.0で修正された問題

ユーザーを作成すると、同じユーザーに対して2つのPKI証明書が作成されます。ユーザーはCitrix Secure Webを介して内部Webサイトにアクセスしたり、Citrix Secure Mailを介して電子メールを受信したりできない場合があります。

RBACロールを追加すると、Citrix Endpoint Managementは次の操作後に応答しなくなります。

- 特定のユーザーグループに権限を適用し、Active Directoryドメインのチェックボックスをオフにします。
- 承認されたアクセス項目またはコンソール機能項目を繰り返し選択します。

シトリックス エンドポイント マネジメント 21.1.1

注:

障害の結果、デリバリーグループの履歴が削除された可能性があります。デリバリーグループの履歴収集は再開されました。

新しいルックアンドフィール。 Citrixは、Citrix Endpoint Managementコンソールを新しい色、フォント、トグル、その他の書式設定の変更で更新しました。ブラウザのキャッシュをクリアして更新するまで、一部の新しいUI要素が正しく読み込まれない場合があります。

macOSでアプリのアンインストールポリシーが利用可能になりました。 アプリのアンインストールポリシーを使用して、macOSデバイスから管理対象アプリを削除できるようになりました。詳細については、アプリのアンインストールデバイスポリシーを参照してください。

デリバリーグループの機能強化。 既存のユーザープロパティルールに加えて、デバイスプロパティルールを使用してデリバリーグループの展開を管理できるようになりました。同じユーザーに複数のデバイスを登録する場合、デバイスの所有権、モデル、OSバージョン、コンプライアンス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

などの固有のデバイスプロパティに基づいて、デリバリーグループ内に高度なフィルターを作成できるようになりました。詳細については、デリバリーグループの追加を参照してください。

レポート作成用のAPIが利用可能になりました。 レポートAPIは、クエリ言語としてJSONを使用する読み取り専用APIです。APIを使用すると、次のことができます。

- アプリケーションのバージョン管理、デバイスOSのパッチ適用、Android DA (レガシー) からAndroid Enterpriseへの移行の進捗状況などに関する堅牢なコンプライアンスレポートを作成します。
- クラウドデータベースに対してカスタムクエリを安全に発行します。
- アプリケーション、デバイス、ユーザー、登録、ソフトウェアのリストなど、クラウドサービスに関するデータをエクスポートします。
- 情報をJSONまたはCSV形式で保存します。

これらのAPIは、オンプレミスデータベースにアクセスしてカスタムSQLクエリを実行することに相当するクラウド機能です。レポートAPIの詳細については、Citrix Developer portalのドキュメントを参照してください。

シトリックス エンドポイント マネジメント 21.1.0

Citrix Cloud APIキーを使用してREST APIに認証します。 Citrix Cloudアカウントを使用して、REST APIにアクセスするための固有のクライアントIDとクライアントシークレットを生成できるようになりました。詳細については、REST APIを参照してください。

Android Enterpriseの制限の再編成。 Android Enterpriseの制限設定が、わかりやすさのために再編成されました。設定名に軽微な変更が加えられている場合があります。再編成の詳細については、Android Enterprise設定を参照してください。

シトリックス エンドポイント マネジメント 20.12.0

このリリースには、全体的なパフォーマンスと安定性の向上に役立つ機能強化が含まれています。

Android Enterpriseデバイスの登録時にAzure Active Directory (AAD) またはOktaを使用して認証します (プレビュー)。 Android Enterpriseデバイスの登録時にAADまたはOktaを認証方法として使用する機能が、プレビューとして利用可能になりました。この機能は、拡張された登録プロファイルに加えて、BYODおよび完全に管理されたモードをサポートします。Oktaを使用したシングルサインオンの詳細については、Citrix Cloudを介したOktaによる認証を参照してください。AADを使用したシングルサインオンの詳細については、Citrix Cloudを介したAzure Active Directoryによる認証を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

エンタープライズアプリとボリューム購入アプリをmacOSデバイスに管理対象アプリとしてインストールする。 アプリを管理対象にする設定がmacOSで利用可能になりました。インストール済みだがまだ管理されていないアプリを管理したい場合は、そのアプリの設定をオンにしてデバイスに展開します。アプリは自動的に管理対象アプリとしてインストールされます。ユーザーにはプロンプトが表示されません。アプリが存在しないデバイスにアプリを展開した場合、設定の状態に関係なく、アプリは管理対象アプリとしてインストールされます。詳細については、エンタープライズアプリの追加とボリューム購入アプリの構成を参照してください。

Citrix Endpoint Management 20.12.0で修正された問題

デフォルトの通知テンプレートでは、Citrix Endpoint ManagementではなくXenMobileという名前が使用されています。

Android Enterpriseユーザーは、登録後に新たに追加されたアプリを受信できない場合があります。

WindowsデバイスのBitLocker暗号化回復キーは、セルフヘルプポータル (SHP) で利用できません。BitLockerデバイスポリシーで**OSドライブの回復**設定を有効にし、BitLockerを使用して登録済みのWindowsデバイスを暗号化しても、回復キーはSHPに表示されません。回避策として、CEMHELPチケットを開き、製品管理とのSREディスカッションを要求してください。

シトリックス エンドポイント マネジメント 20.11.0

Android TouchDownサポートの削除。 DigiCertはJuly 2, 2018をもってAndroid TouchDownのサポートを終了しました。Citrix Endpoint Managementコンソールからすべてのオプションが削除されました。

シトリックス エンドポイント マネジメント 20.10.1

REST APIへのアクセス方法を制限します。 Citrixサポートに連絡することで、Citrix CloudアカウントのみがREST APIにアクセスできるようにすることができます。この機能が有効になっている場合、ローカル管理者アカウントはAPIにアクセスできません。詳細については、REST APIを参照してください。

Citrix Endpoint Management 20.10.1で修正された問題

ユーザーが登録招待メールを受信しません。

Citrix Endpoint Managementを裁量的な証明機関として構成した場合、VPN、ネットワーク、およびその他の資格情報デバイスポリシーは展開されません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント マネジメント 20.10.0

静的または動的MACアドレスを許可します。 ネットワークポリシーの一部として、iOSおよびiPadOSデバイスは、設定されたWi-Fiネットワークに接続するたびに異なるMACアドレスを使用できるようになりました。MACアドレスを静的に保つことも選択できます。ただし、動的MACアドレスを使用すると、デバイスを一貫して識別することがより困難になり、プライバシーが強化されます。詳細については、ネットワークポリシーを参照してください。

Azure Active Directory (AAD) またはOktaをIDプラットフォームとして使用します。 AADまたはOktaをIDプラットフォームとして使用する機能が、パブリックプレビューとして利用可能になりました。Citrix Secure Hubを介して登録するユーザーは、AADまたはOktaの資格情報を使用できます。これらの方法のいずれかをシングルサインオンに使用するには、NetScaler Gatewayを証明書ベースの認証用に構成します。Oktaを使用したシングルサインオンの詳細については、Citrix Cloudを介したOktaによる認証を参照してください。AADを使用したシングルサインオンの詳細については、Citrix Cloudを介したAzure Active Directoryによる認証を参照してください。

Okta認証にUPNまたはメールを使用します。 OktaをIDプラットフォームとして設定すると、ユーザーはUPNまたはメールアドレスでログインできるようになります。詳細については、Oktaによるシングルサインオンを参照してください。

Citrix Endpoint Management 20.10.0で修正された問題

ユーザーが登録招待メールを受信しません。

Citrix エンドポイント管理 20.9.1

割り当てられたポリシーをiOSおよびAndroidデバイスに再展開します。 ユーザーがポリシーを削除した場合、そのポリシーをiOSおよびAndroidデバイスに再展開できるようになりました。**管理 > デバイス > 割り当てられたポリシー**に移動し、ポリシーを選択して、**ステータスのリセット**をクリックして展開ステータスを保留中に変更します。詳細については、iOSでサポートされている登録方法およびAndroidデバイスでサポートされている登録方法を参照してください。

FileVaultデバイスポリシーでキーの保存とローテーションが可能になりました。 FileVaultデバイスポリシーを使用すると、Citrix Endpoint Management内に個人用回復キーを保存できるようになりました。エンドユーザーはセルフヘルプポータルを使用して回復キーを要求でき、管理者はセキュリティアクションを使用して個人用回復キーをローテーションできます。新機能の詳細については、FileVaultデバイスポリシーを参照してください。

macOSアップデートオプションのより詳細な制御。 OSアップデートデバイスポリシーにより、macOSデバイスがアップデートをチェック、ダウンロード、インストールする方法を制御できる

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ようになりました。許可されるソフトウェアアップデートの種類も構成できます。新しい設定の詳細については、OSアップデートデバイスポリシーを参照してください。

Citrix Endpoint Management 20.9.1で修正された問題

一部のiOSデバイスのMDM証明書が更新されません。その場合、**管理 > デバイス > デバイスの詳細 > 証明書**ページには、有効期限が近いApple MDM証明書が表示されます。Citrix Endpoint Managementサーバーログには、**新しいMDMペイロードが古いペイロードと一致しません**というメッセージが含まれます。この問題を解決するには、影響を受けるデバイスを再登録することをお勧めします。Citrixテクニカルサポートは、再登録が必要なデバイスを特定し、必要に応じて一時的な軽減策を実装できます。

Citrix エンドポイント管理 20.9.0

このリリースには、全体的なパフォーマンスと安定性の向上に役立つ機能強化が含まれています。

Citrix Endpoint Management 20.9.0で修正された問題

Azure ADユーザーがキオスクとして構成された一部のAzure AD参加済みWindows 10デバイスにログインしても、キオスクモードがアクティブになりません。

macOS 10.14以降を実行しているデバイスを登録した直後、Citrix Endpoint Managementコンソールにデバイスプロパティが常に表示されるとは限りません。プロパティを表示するには、デバイスを再起動してください。

展開されたリソースが、デバイスを再起動するまでmacOS 10.14以降のデバイスで有効にならないことがあります。

シトリックス エンドポイント管理 20.8.0

管理対象構成での証明書エイリアスの使用がより簡単に。 資格情報デバイスポリシーの新しい**証明書エイリアス**設定を、**Android Enterprise管理対象構成**デバイスポリシーと組み合わせて使用します。これにより、ユーザーの操作なしでアプリがVPNで認証できるようになります。アプリログで資格情報エイリアスを見つける代わりに、資格情報エイリアスを作成します。**Android Enterprise管理対象構成**デバイスポリシーの**証明書エイリアス**フィールドに入力してエイリアスを作成します。次に、**資格情報**デバイスポリシーの**証明書エイリアス**設定に同じ証明書エイリアスを入力します。管理対象構成ポリシーおよび資格情報デバイスポリシーを参照してください。

パスコードデバイスポリシーにより、コンプライアンスに準拠していないAndroid Enterpriseデバイスでアプリとショートカットを表示できます。 Android Enterpriseのパスコードデバイスポリシーに、新しい設定**パスコードがコンプライアンスに準拠していないときにアプリとショートカットを表示する**が追加されました。この設定を有効にすると、デバイスのパスコードが準拠し

© 1997–2026 Citrix Systems, Inc. All rights reserved.

なくなった場合でも、アプリとショートカットが表示されたままになります。Citrixは、パスコードが準拠していない場合にデバイスを非準拠としてマークする自動アクションを作成することをお勧めします。パスコードデバイスポリシーを参照してください。

Android Enterpriseデバイスでの「1つのロックを使用」設定の制御。 パスコードデバイスポリシーの新しい**統合パスコードを有効にする**設定により、デバイスとワークプロファイルに個別のパスコードが必要かどうかを制御できます。この設定が導入される前は、ユーザーはデバイスの**1つのロックを使用**設定でこの動作を制御していました。**統合パスコードを有効にする**が**オン**の場合、ユーザーはデバイスとワークプロファイルに同じパスコードを使用できます。**統合パスコードを有効にする**が**オフ**の場合、ユーザーはデバイスとワークプロファイルに同じパスコードを使用できません。デフォルトは**オフ**です。**統合ロックを有効にする**設定は、Android 9.0以降を実行しているAndroid Enterpriseデバイスで利用できます。パスコードデバイスポリシーを参照してください。

Citrix Endpoint Management 20.8.0で修正された問題

Citrix Endpoint Managementを19.12.0以降でオンボーディングした場合、Android Enterpriseサブスクリプションを削除するには、コンソールからAndroid Enterpriseの登録を解除します。次に、Google Playから構成を削除します。最初にGoogle Playストアで**Enterpriseを削除**をクリックすると、Android Enterpriseサブスクリプションは Citrix Endpoint Managementコンソールでアクティブなままになります。

シトリックス エンドポイント管理 20.7.1

登録画面のプロファイル名をCitrix Workspaceに変更しました。 ユーザーがデバイスをCitrix Endpoint Managementに登録すると、表示されるプロファイル名がCitrix Workspaceになりました。この名前をカスタマイズして、代わりに組織名を表示できます。名前をカスタマイズするには、新しいサーバープロパティ `apple.mdm.enrollment.profile.organization.name` の値を変更します。サーバープロパティを参照してください。

Citrix Endpoint Management 20.7.1 で修正された問題

一部のクラウドサイトでは、Citrix Endpoint Management コンソールの ページが読み込まれません。

`optional.user.identity.attributes` サーバープロパティの値を編集して変更を保存すると、エラーメッセージが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント マネジメント 20.7.0

Citrix Endpoint Management は、プレビュー機能としてオンプレミスの NetScaler Gateway を使用した認証をサポートします。 Citrix Secure Hub を介して登録するユーザーの ID プロバイダーとして、オンプレミスの NetScaler Gateway を構成できるようになりました。詳しくは、「Citrix Cloud を介したオンプレミスの NetScaler Gateway を使用した認証 (プレビュー)」を参照してください。

オプションの Active Directory ユーザー属性のリストをカスタマイズします。 新しいサーバープロパティ `optional.user.identity.attributes` を使用すると、Citrix Endpoint Management が Active Directory でユーザーアカウントを識別するために使用するオプションの属性を削除および復元できます。詳しくは、「Active Directory ユーザー属性のカスタマイズ」を参照してください。

Citrix Endpoint Management 20.7.0 で修正された問題

Apple iTunes Volume Purchase アプリは Citrix Endpoint Management と同期できません。

Citrix Cloud Connector を使用して複数の LDAP Active Directory (AD) を Citrix Endpoint Management にインストールすると、最初にインストールされた AD のみが Citrix Endpoint Management 設定に表示されます。回避策として、Citrix Cloud を確認できます。これらのドメインが未使用としてマークされている場合は、手動で としてマークします。ドメインを使用済みとしてマークすると、Citrix Endpoint Management で利用できるようになります。

Citrix Endpoint Management を 19.12.0 (2019 年 12 月) 以降にオンボーディングした場合: 複数の LDAP 認証ドメインを追加すると、デフォルトドメインを変更できません。

シトリックス エンドポイント マネジメント 20.6.0

19.8.0 リリース (August 1, 2019) 以降に Citrix Endpoint Management をオンボーディングした場合は、Citrix Cloud にサインインし、Citrix Endpoint Management サービスタイルをクリックしてコンソールにアクセスしてください。19.8.0 以前にオンボーディングしたすべてのお客様は、まもなく Citrix Cloud サインインに移行します。セキュリティを強化するために、Citrix はシングルサインオンを構成することをお勧めします。サポートが必要な場合は、Citrix テクニカルサポートにお問い合わせください。

Citrix Endpoint Management 用の Citrix Secure Hub Apple Push Notification Service (APNs) 証明書は July 12, 2020 に期限切れになります。その結果、エージェント通知が失敗し、iOS デバイスでのアプリケーションプッシュが遅延する可能性があります。この更新プログラムは、June 18, 2021 に期限切れになる Citrix Secure Hub APNs 証明書を更新します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android Enterprise のワークプロファイルまたは完全に管理されたデバイスでの印刷機能を無効にします。 制限デバイスポリシーの 設定を使用すると、ユーザーが Android Enterprise デバイスからアクセスできるプリンターに印刷できるかどうかを指定できます。詳しくは、「Android Enterprise の設定」を参照してください。

macOS の接続モードとネットワーク優先度を構成します。 ネットワークデバイスポリシーで、macOS デバイスの 設定を有効にして、ユーザーがネットワークに参加する方法を選択します。デバイスは、システム資格情報またはログインウィンドウで入力された資格情報を使用してユーザーを認証できます。複数のネットワークがある場合は、 フィールドに数値を入力して、ネットワーク接続の優先度を設定します。デバイスは、最も小さい番号のネットワークを選択します。詳しくは、「ネットワークデバイスポリシー」の macOS 設定を参照してください。

iOSデバイスで構成されたプロキシを有効にする。 Citrix Endpoint Managementでは、iOSユーザーが**設定 > ネットワーク**で構成したプロキシサーバーを使用できるようにする場合、新しいクライアントプロパティ `ALLOW_CLIENTSIDE_PROXY` を有効にする必要があります。詳細については、クライアントプロパティリファレンスの `ALLOW_CLIENTSIDE_PROXY` を参照してください。

管理対象Google Playアプリの管理対象アプリポリシーを自動的に更新する。 この新しいポリシーにより、Android Enterpriseデバイス上の管理対象Google Playアプリについて、ユーザーがアプリの自動更新を構成する機能を制限できます。ユーザーがポリシーを構成できるようにすることも、自動更新を常に適用するか、決して適用しないか、またはデバイスがWi-Fiに接続されている場合にのみ適用するかを指定することもできます。

Citrix Endpoint Management 20.6.0で修正された問題

Citrix Endpoint Managementコンソールでは、MDXでラップされたiOSおよびAndroidアプリのパッケージIDを確認できません。

Citrix Endpoint ManagementがActive Directoryグループメンバーのクエリを送信すると、IDサービスはクエリを再帰的に実行します。これらのクエリはより多くのリソースを消費します。そのため、多数のActive Directoryユーザーがいるサイトでは、日常業務に支障をきたす可能性があります。

Citrix Endpoint Managementコンソールでは、一部のアプリのステータスが「保留中」と表示されますが、すでにインストールされています。この制限はmacOSによるもので、pkgとアプリの識別子が異なるPKGファイルに固有のものです。

シトリックス エンドポイント マネジメント 20.5.0

Citrix Endpoint ManagementとMicrosoft Endpoint Managerの統合を使用する際のIntune管理対象アプリの構成を簡素化。 Intune管理対象アプリを構成する際、Citrix Endpoint Managementコ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ンソールで**アプリの管理を強制する**オプションを設定する必要がなくなりました。このオプションはEMSコンソールで設定するようになりました。

Citrix Endpoint ManagementとMicrosoft Endpoint Managerの統合を使用してMicrosoft Edge経由で公開されたIntune管理対象アプリのWebコンテンツ転送制限をサポート。 Citrix Endpoint ManagementとMicrosoft Endpoint Managerの統合は、EMSコンソールでMicrosoft Edgeの新しい管理対象ブラウザポリシー**他のアプリとのWebコンテンツ転送を制限する**をサポートします。

ローカルユーザーアカウントのロック解除。 ユーザーが連続して無効なログイン試行の最大数に達すると、ローカルユーザーアカウントは30分間ロックされます。ロックアウト期間が終了するまで、それ以降のすべての認証試行は拒否されます。Citrix Endpoint Managementコンソールでアカウントのロックを解除するには、**管理 > ユーザー**に移動し、ユーザーアカウントを選択して、**ローカルユーザーのロック解除**をクリックします。詳細については、ローカルユーザーアカウントのロックを解除するにはを参照してください。失敗したログイン試行回数とロックアウト時間を変更するには、**local.user.account.lockout.time**および**local.user.account.lockout.limit**サーバープロパティを更新します。詳細については、サーバープロパティを参照してください。

Citrix Content Delivery Network (CDN) がmacOS向けエンタープライズアプリ (MDM登録) を配信するようになりました。 アプリのダウンロード速度を向上させるため、CDNは世界中のCitrix Endpoint Managementサーバーの近くにあるユーザーデバイスにmacOSアプリを送信します。詳細については、Citrix CDNからエンタープライズアプリを配信するを参照してください。

Citrix Endpoint Management 20.5.0で修正された問題

登録招待をエクスポートするRBAC権限を持つ管理者は、制限に関係なく、すべての登録招待をエクスポートできます。

Windowsデバイスで自動アクションをトリガーするためにPowerShellスクリプトを展開しようとすると、500内部サーバーエラーで失敗する場合があります。この問題は、**アクション情報**ページの**説明**フィールドを空白のままにし、トリガーとして**ポリシーの戻り値**を選択した場合に発生します。この問題を回避するには、**ポリシーの戻り値**をトリガーとして使用する場合、**説明**フィールドを空白のままにしないでください。

既存のiOS制限ポリシーを編集すると、エラーが発生します。

シトリックス エンドポイント マネジメント 20.4.1

最新のHTTP/2ベースのAPNsプロバイダーAPIのサポート。 Apple Push Notificationサービスレガシーバイナリプロトコルに対するAppleのサポートは、March 31, 2021をもって終了します。Appleは、代わりにHTTP/2ベースのAPNsプロバイダーAPIを使用することを推奨しています。Citrix Endpoint Managementは、HTTP/2ベースのAPIをサポートするようになりました。詳細につ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

いては、`<https://developer.apple.com/>`のニュース更新「Apple Push Notification Service Update」を参照してください。APNsへの接続確認については、Connectivity checksを参照してください。

ローカルユーザーアカウントのパスワード要件。 Citrix Endpoint Managementコンソールでローカルユーザーアカウントを追加または編集する際は、最新のパスワード要件に従っていることを確認してください。詳細については、To add a local user accountを参照してください。

アプリバンドルID番号を使用して、アプリをアプリ通知デバイスポリシーに追加します。 **Add new**をクリックし、表示されるフィールドにアプリバンドルIDを入力します。詳細については、Apps notifications device policyを参照してください。

iOS 13向けデバイスポリシーの更新。 iOS 13向けデバイスポリシーには、以下の機能が追加されました。

- **ネットワーク使用状況ポリシー:** アプリネットワーク使用状況ポリシーに機能を追加し、ネットワーク使用状況ポリシーに名称変更しました。iOS 13デバイスでは、SIM ICCIDに基づいてネットワーク使用状況ルールを設定することもできるようになりました。Network usage device policyを参照してください。
- **制限ポリシー:** 共有デバイスの一時セッション、eSIMの変更、iPhoneを探すなどを制限できるようになりました。詳細については、Restrictions device policyのiOS設定セクションを参照してください。

Citrix Endpoint Management 20.4.1で修正された問題

Azure Active Directoryベースの認証とデバイス登録を使用している場合、Androidデバイスのユーザーは登録に失敗します。エラーには、ユーザー認証にデバイスアクセスがないと表示されます。

シトリックス エンドポイント マネジメント 20.4.0

Citrix Endpoint ManagementコンソールでAndroid Enterprise向けWebアプリを公開。 Citrix Endpoint Management向けAndroid Enterprise Webアプリを公開するために、管理対象Google PlayまたはGoogle Developerポータルにアクセスする必要がなくなりました。**Configure > Apps > Web link**で**Upload**をクリックすると、管理対象Google Playストアの UIが開き、ファイルをアップロードして保存できます。アプリの承認と公開には約10分かかります。詳細については、Add a Web linkを参照してください。

iOS 13向けデバイスポリシーの更新。 iOS 13向けデバイスポリシーには、以下の機能が追加されました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アプリロックポリシー:** 音声コントロールを有効にし、ユーザーに音声コントロール調整へのアクセスを許可できます。App lock device policyを参照してください。
- **Exchangeポリシー:** カレンダー、連絡先、メール、メモ、リマインダーの同期を有効または無効にできます。Exchange device policyを参照してください。
- **プロファイル削除ポリシー:** iOSデバイスでのポリシー削除を許可する設定は、iOSがその機能をサポートしなくなったため削除されました。Profile Removal device policyを参照してください。
- **VPNポリシー:** 以下の接続プロトコルについて、すべてのネットワークトラフィックを含めるか、ローカルネットワークをVPNから除外できるようになりました。
  - iOS用CiscoレガシーAnyConnectプロトコル
  - iOS用カスタムSSLプロトコル

  Wi-FiアシストがWi-Fiから切り替わったときに、以下の接続プロトコルについて、セルラーVPNトンネルを介したトラフィックのフローを許可できるようになりました。
  - iOS用IKEv2プロトコル
- **ネットワークポリシー: セキュリティの種類**のオプションとして、WPA3 PersonalおよびWPA3 Enterpriseを使用できるようになりました。ネットワークデバイスポリシーを参照してください。

Citrix Endpoint Management 20.4.0で修正された問題

分析ダッシュボードのデータ視覚化チャートは、ブラウザのズームを使用すると正しくスケーリングされません。

MAMのみの登録を使用している場合でも、ユーザーはMDM用のApple Over-the-Air登録ポータルにアクセスできます。

デバイスがスタンバイ状態の場合、選択的ワイプアクションが失敗します。

シトリックス エンドポイント マネジメント 20.3.0

すべての顧客向けに強化された登録プロファイルが有効化されました

このリリースでは、Citrix Endpoint Management 20.2.1で一部の顧客にリリースされた強化された登録プロファイル機能が、すべての顧客向けに有効になります。この機能の詳細については、「単一環境で複数のデバイスおよびアプリ管理モードを構成する」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Androidデバイスはデフォルトで Android Enterpriseに登録されます

このリリースから、Android EnterpriseはAndroidデバイスのデフォルトの登録オプションとなります。Citrix Endpoint Management展開でAndroid Enterpriseが有効になっている場合、新しく登録または再登録されたすべてのAndroidデバイスは、デフォルトでAndroid Enterpriseデバイスとして登録されます。

この変更は、GoogleがAndroidに対して行っている変更をサポートします。Googleはデバイス管理のデバイス管理者モードを非推奨とし、すべてのAndroidデバイスをAndroid Enterpriseを使用して管理するよう顧客に推奨しています。（Google Android Enterprise開発者ガイドのデバイス管理者モードの非推奨化を参照してください。）

Citrix Endpoint Management 19.11.0以降、CitrixはすべてのAndroidデバイスをAndroid Enterpriseに移行するために必要なアクションを通知しました。Android Enterpriseへの移行に関するCitrix Endpoint Managementのサポートの詳細については、ブログ「Citrix Endpoint Managementサービスのデフォルトとしての Android Enterprise」を参照してください。

Citrix Endpoint Managementの展開に、デバイス管理者モードで管理を継続する必要があるデバイスが含まれている場合は、これらのレガシーデバイス用の登録プロファイルを作成します。

レガシーデバイス用の登録プロファイルを作成するには：

1. Citrix Endpoint Managementコンソールで、 > の順に移動します。
2. 登録プロファイルを追加するには、 をクリックします。ページで、登録プロファイルの名前を入力します。
3. をクリックするか、 の下にある を選択します。ページが表示されます。
4. を に設定します。 をクリックします。
5. を選択します。画面が表示されます。
6. 専用デバイスを登録する管理者が所属するデリバリーグループを選択します。次に、 をクリックします。

レガシーデバイスをデバイス管理者モードで管理し続けるには、このプロファイルを使用してデバイスを登録または再登録します。ユーザーにCitrix Secure Hubをダウンロードさせ、登録サーバーURLを提供することで、ワークプロファイルデバイスと同様にデバイス管理者デバイスを登録します。

Citrix Endpoint Management 20.3.0で修正された問題

または でデバイスを並べ替えようとすると、500内部サーバーエラーが発生します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Amazon Web Servicesと新しいCitrix拡張登録プロファイルを使用しているお客様の場合：iOSデバイスが登録されません。回避策として、すべてのデリバリーグループを含むデフォルトの登録プロファイルを作成します。登録プロファイルを作成するにはを参照してください。

macOSデバイスにパスコードデバイスポリシーを展開すると、ポリシーはユーザーレベルではなくシステムレベルに適用されます。その結果、ユーザーは数時間、あるいは数日間パスコードの変更を求められません。

シトリックス エンドポイント マネジメント 20.2.1

単一環境で複数のデバイスおよびアプリ管理モードを構成する

この機能について:

強化された登録プロファイルのサポートは、2つのリリースにわたって展開されます。Citrix®は、今後のリリースに関する通知を送信します。

強化された登録プロファイル機能が有効になるまでは、登録プロファイルはユーザーが登録できるデバイスの数を制限するだけです。
単一のCitrix Endpoint Managementサイトで、複数の登録構成をサポートするように設定できるようになりました。登録プロファイルの役割は、デバイスおよびアプリ管理の登録設定を含むように拡張されました。

登録プロファイルは、単一のCitrix Endpoint Managementコンソール内で複数のユースケースとデバイス移行パスをサポートします。ユースケースには以下が含まれます。

- モバイルデバイス管理 (MDMのみ)
- MDM+モバイルアプリケーション管理 (MAM)
- MAMのみ
- 企業所有の登録
- BYOD登録 (MDM登録をオプトアウトする機能)
- Androidデバイス管理者登録からAndroid Enterprise登録への移行 (完全管理、仕事用プロファイル、専用デバイス)

登録プロファイルは、現在非推奨となっているサーバープロパティ `xms.server.mode` に置き換わります。この変更は、既存のデリバリーグループおよび登録済みデバイスには影響しません。

次の表は、既存のサーバープロパティモードから新しい登録プロファイル機能への自動移行パスを示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

既存のサーバープロパティ	新しい管理モード
ENTモード (iOS)	Citrix MAMによるAppleデバイス登録
ENTモード (Android)	Citrix MAMによるレガシーデバイス管理者
ENTモード (アンドロイド エンタープライズ)	Citrix MAMによる完全管理型でのワークプロファイル
MAMモード (iOSおよびAndroid)	シトリックス MAM
MDMモード (iOS)	Appleデバイス登録
MDMモード (Android)	レガシーデバイス管理者
MDMモード (アンドロイド エンタープライズ)	フルマネージドデバイス上の仕事用プロファイル

デリバリーグループを作成する際、そのグループに登録プロファイルをアタッチできます。登録プロファイルをアタッチしない場合、Citrix Endpoint Management はグローバル登録プロファイルをアタッチします。

登録プロファイルは、以下のデバイス管理機能を提供します。

- **Android デバイス管理者 (DA) モードから Android Enterprise への移行がより簡単に。**
  Android Enterprise デバイスの場合、設定には、フルマネージド、フルマネージドデバイス上の仕事用プロファイル、または専用などのデバイス所有者モードが含まれます。詳細については、「Android Enterprise」を参照してください。

  Android の登録プロファイルページ(/en-us/citrix-endpoint-management/media/enrollment-profile-android.png)

  このアップグレードでは、サーバーモードおよび > の現在の Citrix Endpoint Management 構成は、新しい登録プロファイル設定に次のようにマッピングされます。

現在の構成	管理設定	デバイス所有者モード設定	CITRIX MAM 設定
MDM; マネージド Google Play (アンドロイド エンタープライズ)	アンドロイド エンタープライズ	フルマネージドデバイス上の仕事用プロファイル	オフ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

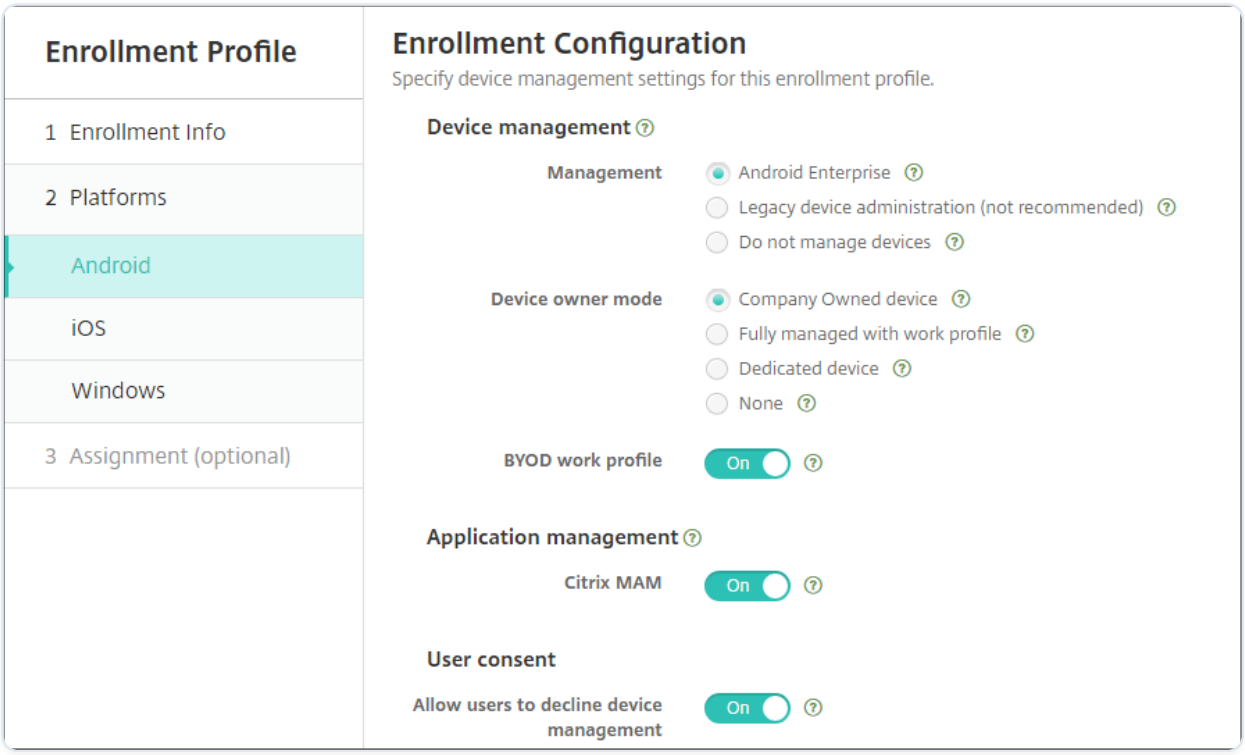
現在の構成	管理設定	デバイス所有者モード設定	CITRIX MAM 設定
MDM; Google Workspace (レガシー DA)	レガシーDA	該当なし	オフ
MAM	デバイスを管理しない	該当なし	オン
MDMとMAMの組み合わせ; マネージド Google Play (Android Enterprise)	アンドロイド エンタープライズ*	完全管理対象のワークプロファイル	オン
MDM+MAM; Google Workspace (レガシーDA)	レガシーDA*	該当なし	オン

* 登録が必要な場合、**ユーザーによるデバイス管理の拒否を許可**は**オフ**です。

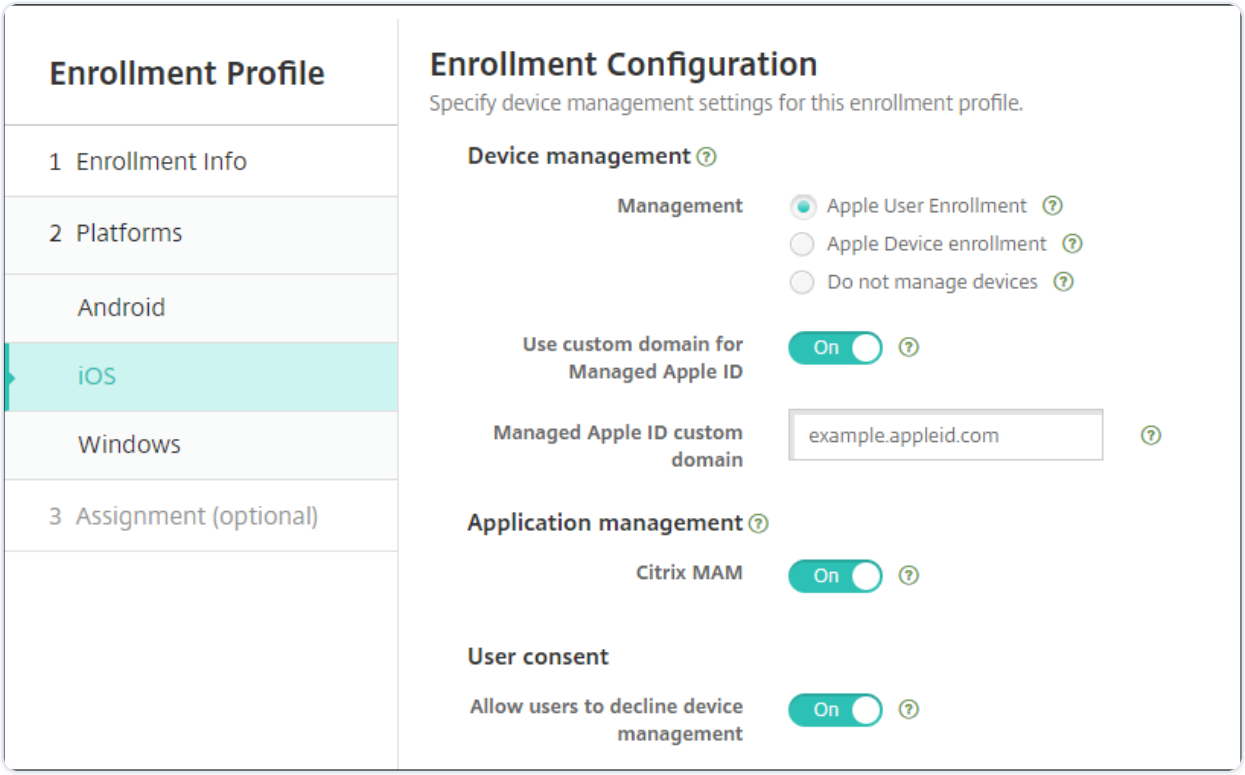
アップグレード後、現在の登録プロファイルにこれらのマッピングが反映されます。レガシーDAから移行する際に、新しいユースケースに対応するために他の登録プロファイルを作成するかどうかを検討してください。

Citrix Endpoint Management 19.12.0以降にオンボードする場合、グローバル登録プロファイルにはこれらの事前定義された設定があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **iOS管理の簡素化。** iOSデバイスの場合、設定にはデバイスを管理対象として登録するか、管理対象外として登録するかの選択肢が含まれます。



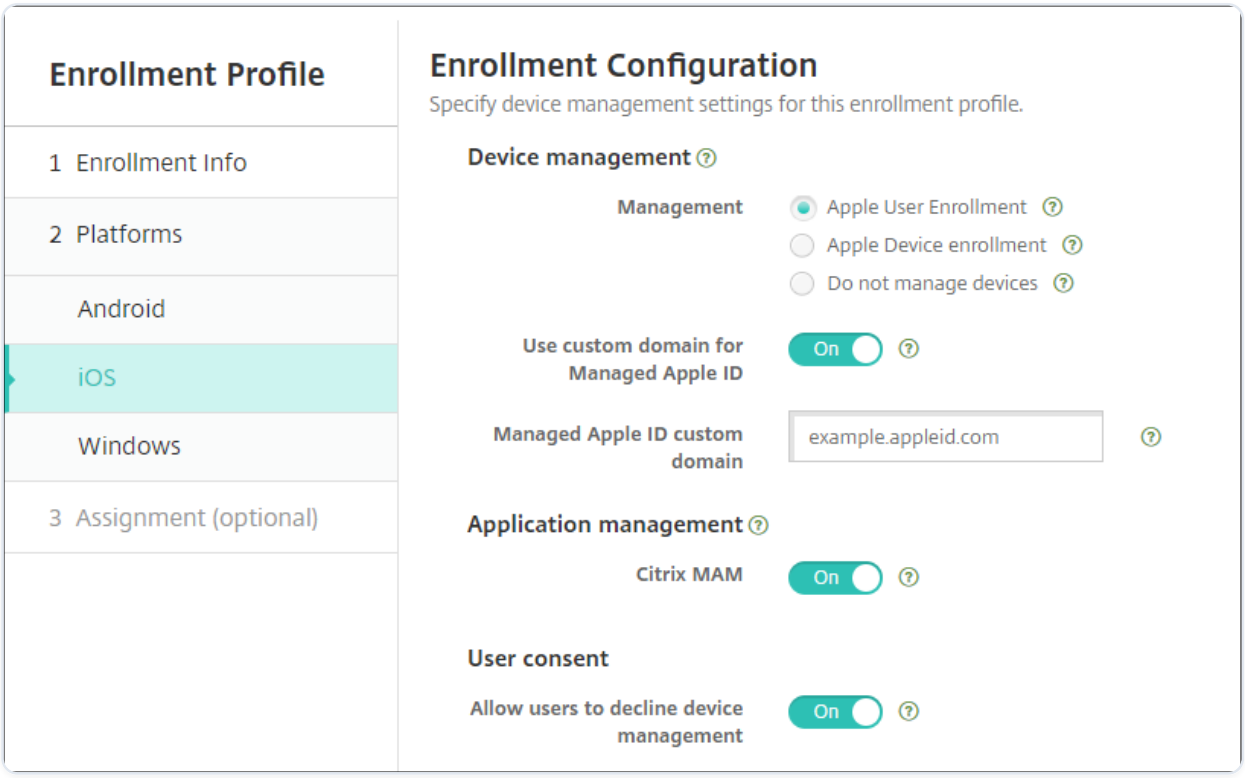
このアップグレードでは、以前の設定は新しい登録プロファイル設定に次のようにマッピングされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サーバーモード	管理設定	CITRIX MAM設定
MDM	デバイス登録	オフ
MAM	デバイスを管理しない	オン
MDM+MAM	デバイス登録	オン

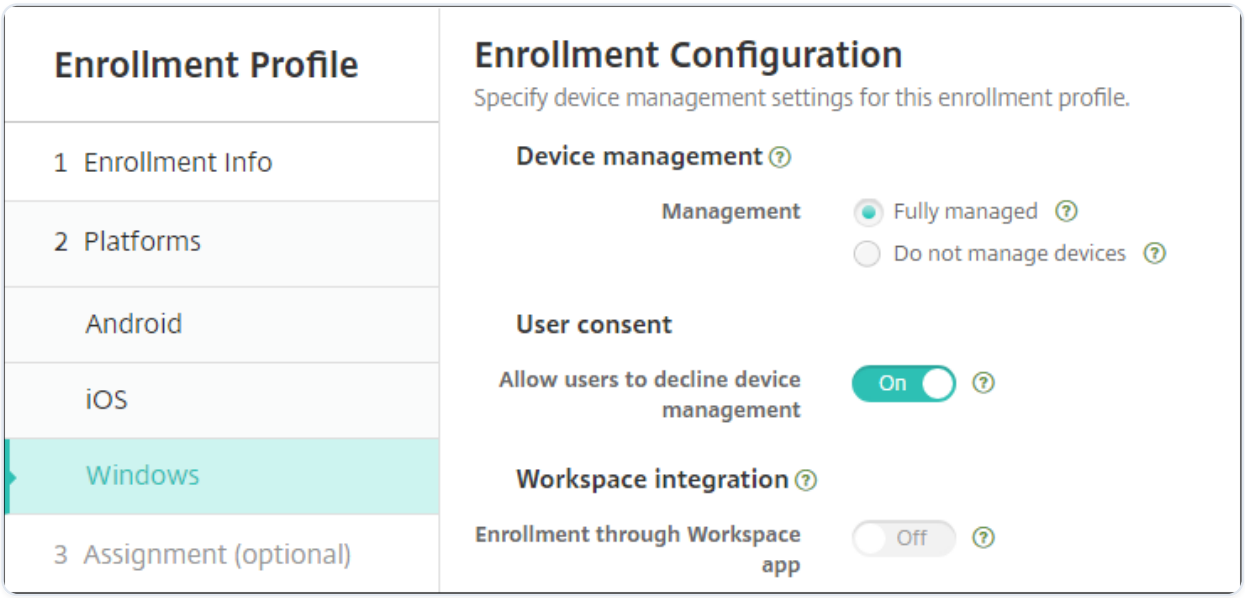
登録が必要な場合、**ユーザーがデバイス管理を拒否することを許可**は**オフ**になります。

Citrix Endpoint Management 19.12.0以降を導入する場合、グローバル登録プロファイルにはこれらの事前定義された設定があります。



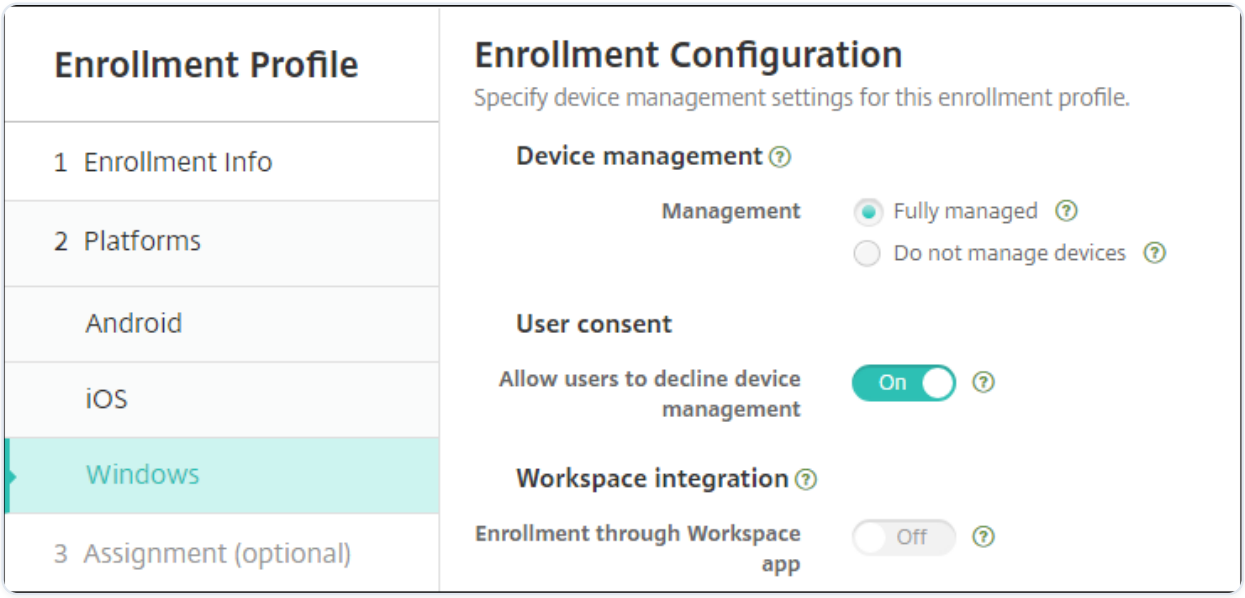
- **Windows 10デバイスがCitrix Workspaceアプリに自動的に登録されることを許可します。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



このアップグレードでは、以前のMDM構成は新しい登録プロファイル設定**完全管理**にマッピングされます。

Citrix Endpoint Management 19.12.0以降を導入する場合、グローバル登録プロファイルにはこれらの事前定義された設定があります。



拡張登録プロファイルには、次の制限があります。

- Citrix Endpoint ManagementがCitrix Workspaceと統合されている場合、拡張登録プロファイル機能はiOSおよびAndroidデバイスでは機能しません。
- 拡張登録プロファイル機能は、ワンタイムPINまたは2要素認証の登録招待では利用できません。

詳細については、登録プロファイルを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 20.2.1のその他の更新

- **専用のAndroid Enterprise (COSU) デバイスの登録を簡素化。** Citrix Endpoint Managementでは、登録プロファイルを作成することで、専用のAndroid Enterpriseデバイス（COSUデバイスとも呼ばれる）を登録できるようになりました。専用デバイスを登録するために、ロールベースのアクセス制御（RBAC）ロールを作成する必要はなくなりました。専用のAndroid Enterpriseデバイスのプロビジョニングを参照してください。
- **Keyguard管理ポリシーを使用してAndroidデバイスの生体認証を無効にする。** Keyguard管理デバイスポリシーにより、Android 9.0以降を実行しているデバイスで、指紋認証ロック解除、顔認証、虹彩認証、またはすべての生体認証を無効にできるようになりました。
- **リソースセンターでガイダンスを入手する。** リソースセンターを使用して、製品内のデータにアクセスします。ダッシュボードからガイダンスを得るには、右下隅のアイコンをクリックします。



Citrix Endpoint Management 20.2.1で修正された問題

以前は、Citrix Endpoint Management APIを使用してデバイスに通知を送信する前に、デバイスを編集する権限が必要でした。通知を送信するには、通知送信権限が必要になりました。

WEMが有効なWindowsデスクトップ/タブレットデバイスを登録し、その後同じデバイスをMDMに登録すると、Citrix Endpoint Managementコンソールにそのデバイスの2つのエントリが別々に表示されます。

シトリックス エンドポイント マネジメント 20.1.0

- **Android Enterprise COPEデバイスのサポート。** Citrix Endpoint Managementは、ワークプロファイルを持つAndroid Enterpriseの完全管理デバイスをサポートします。Googleは以前、これらのデバイスをCOPE（corporate-owned personally enabled）デバイスと呼んでいました。

  Android Enterpriseの完全管理デバイスには、デバイスプロファイルとワークプロファイルがあります。デバイスとワークプロファイルに個別のポリシー設定を適用できます。このリリースでは、次のようになります。

  - 次のデバイスポリシーを使用して、デバイスとワークプロファイルに個別の設定を適用できます: 資格情報、Keyguard管理、パスコード、および制限。
  - 位置情報デバイスポリシーの位置情報モード設定は、COPEデバイス自体に適用できますが、COPEデバイスのワークプロファイルには適用できません。位置情報デバイスポリ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シーのその他の設定は、COPEデバイスでは利用できません。位置情報デバイスポリシーを参照してください。

- ロックセキュリティアクションは、デバイスまたはワークプロファイルに個別に適用できます。

- **Citrix Workspaceアプリを介したWindows 10デバイスの自動登録。** Citrix Endpoint Managementは、Citrix Workspaceアプリを使用してWindows 10デスクトップおよびタブレットを自動登録できるようになりました。

Citrix Endpoint Management 20.1.0の修正された問題

Settings > Apple Deployment Programページには、新しいiOS 13セットアップアシスタント画面のスキップオプションが含まれていません。登録中に、ユーザーは「開始」と「外観」の画面をクリックする必要があります。

Manage > Devicesでは、**Filters**タブがデフォルトで開いています。

同じ仮想マシンセット上のマルチテナント顧客の場合、ShareFileシングルサインオン（SSO）が失敗します。

シトリックス エンドポイント マネジメント 19.12.0

デバイスプロパティに基づいてWindowsデバイスのデリバリーグループを構成できるようになりました。（プレビュー） デリバリーグループを構成する際、デバイスプロパティに基づいてグループを構成できるようになりました。この機能はWindowsデスクトップおよびタブレットでのみ利用可能です。このプレビュー機能へのアクセスをリクエストするには、Citrixの営業担当者またはサポート担当者にお問い合わせください。この機能の詳細については、「デリバリーグループの追加（プレビュー）」を参照してください。

グループポリシーオブジェクト（GPO）をCitrix Endpoint Managementにインポートし、Windows 10デバイスに直接展開します。 AD管理者がグループポリシー管理コンソールからGPOを展開するのではなく、Citrix Endpoint Managementコンソールを通じてGPOをインポートおよび展開できます。「Windows GPO構成デバイスポリシー」を参照してください。

WindowsデスクトップおよびタブレットのEXEアプリをインストールします。 WindowsデスクトップおよびタブレットのエンタープライズアプリとしてEXEアプリケーションをアップロードできるようになりました。詳細については、「エンタープライズアプリとしてWin32アプリを追加する」を参照してください。

ユーザーはiOSデバイスからポリシーを削除できなくなりました。 一部のデバイスポリシーでは、ユーザーがiOSデバイスからポリシーを削除することができなくなりました。以下のポリシー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

から、iOSの**Allow user to remove policy**設定が削除されました：APNポリシー、メールポリシー、パスコードポリシー、プロビジョニングプロファイルポリシー、プロキシポリシー、およびVPNポリシー。

Citrix Endpoint Management 19.12.0の修正された問題

Citrix Endpoint Management Public REST APIを使用してアプリのバージョン番号を更新し、その後コンソールを使用した場合、アプリのバージョンは更新されません。

ファイルハッシュが正しくないため、Citrix Endpoint ManagementがWindowsデバイスにEXEアプリをインストールできない場合があります。

シトリックス エンドポイント マネジメント 19.11.0

Apple ボリューム購入プログラムからApple Business Manager (ABM) およびApple School Manager (ASM) への移行

Apple Volume Purchase Program (VPP) を使用している企業や教育機関は、December 1, 2019 までに Apple Business Manager または Apple School Manager の「App とブック」に移行する必要があります。

Citrix Endpoint Management で VPP アカウントを移行する前に、このAppleサポート記事を参照してください。

組織または学校が Volume Purchase Program (VPP) のみを使用している場合は、ABM/ASM に登録し、既存の VPP 購入者を新しい ABM/ASM アカウントに招待できます。ASM の場合は `<https://school.apple.com>` に移動します。ABM の場合は `<https://business.apple.com>` に移動します。

Citrix Endpoint Management で Volume Purchase (旧 VPP) アカウントを更新するには：

1. Citrix Endpoint Management コンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **Volume Purchase** をクリックします。**Volume Purchase** 設定ページが表示されます。
3. ABM または ASM アカウントが、以前の VPP アカウントと同じアプリ構成になっていることを確認してください。
4. ABM または ASM ポータルで、更新されたトークンをダウンロードします。
5. Citrix Endpoint Management コンソールで、次の操作を行います。
    a. その場所の更新されたトークン情報で、既存の Volume Purchase アカウントを編集します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. ABM または ASM の資格情報を編集します。サフィックスは変更しないでください。

c. **保存**を2回クリックします。

詳細については、以下を参照してください。

- Apple ボリューム購入
- Apple Deployment Program を介したデバイスの展開
- Appleデバイスの一括登録(/ja-jp/citrix-endpoint-management/device-management/apple/ios-bulk-enrollment.html)

登録プロファイルでAndroidデバイスの登録オプションを制御

登録プロファイルは、Citrix Endpoint Management展開でAndroid Enterpriseが有効になっている場合に、Androidデバイスがどのように登録されるかを制御するようになりました。登録プロファイルは、AndroidデバイスがデフォルトのAndroid Enterpriseモード（完全管理または仕事用プロファイル）で登録されるか、レガシー（デバイス管理者）モードで登録されるかを決定します。

デフォルトでは、グローバル登録プロファイルは、新規および工場出荷時設定にリセットされたAndroid Enterpriseデバイスを完全管理デバイスとして登録し、BYOD Android Enterpriseデバイスを仕事用プロファイルデバイスとして登録します。詳しくは、「Android Enterprise」(/ja-jp/citrix-endpoint-management/device-management/android/android-enterprise.html)を参照してください。

デフォルト登録としてのAndroid Enterprise向けレガシーAndroidデバイスの準備

Googleは、デバイス管理のデバイス管理者モードを非推奨とし、すべてのAndroidデバイスをデバイス所有者モードまたはプロファイル所有者モードで管理するよう顧客に推奨しています。（Google Android Enterprise開発者ガイドのデバイス管理者の非推奨を参照してください。）この変更をサポートするため、CitrixはAndroid EnterpriseをAndroidデバイスのデフォルトの登録オプションとします。

この変更は、Citrix Endpoint Management展開でAndroid Enterpriseが有効になっている場合、新しく登録された、または再登録されたすべてのAndroidデバイスがAndroid Enterpriseデバイスとして登録されることを意味します。

この変更に備えるため、Citrix Endpoint Managementでは、Androidデバイスの登録方法を制御する登録プロファイルを作成できるようになりました。

組織によっては、レガシーAndroidデバイスをデバイス所有者モードまたはプロファイル所有者モードで管理する準備ができていない場合があります。その場合、デバイス管理者モードで管理を継続できます。レガシーデバイス用の登録プロファイルを作成し、登録済みのすべてのレガシーデバイスを再登録します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レガシーデバイス用の登録プロファイルを作成するには：

1. Citrix Endpoint Managementコンソールで、**［構成］>［登録プロファイル］** の順に選択します。
2. 登録プロファイルを追加するには、**［追加］** をクリックします。［登録情報］ページで、登録プロファイルの名前を入力します。
3. **［次へ］** をクリックするか、**［プラットフォーム］** で **［Android］** を選択します。［登録構成］ページが表示されます。
4. **［管理］** を **［レガシーデバイス管理（非推奨）］** に設定します。**［次へ］** をクリックします。
5. **［割り当て（オプション）］** を選択します。［デリバリーグループの割り当て］画面が表示されます。
6. 専用デバイスを登録する管理者が属するデリバリーグループを選択します。次に、**保存**をクリックします。

デバイス管理者モードでレガシーデバイスの管理を続行するには、このプロファイルを使用してデバイスを登録または再登録します。デバイス管理者デバイスは、ユーザーにCitrix Secure Hubをダウンロードさせ、登録サーバーURLを提供させることで、ワークプロファイルデバイスと同様に登録します。

Android Enterpriseへの移行に関するCitrix Endpoint Managementのサポートの詳細については、ブログ「Android Enterprise as the default for Citrix Endpoint Management service」を参照してください。

Citrix Endpoint Management 19.11.0で修正された問題

Citrix Endpoint ManagementコンソールでGoogle Playストアアプリを検索すると、アプリ名が空になります。アプリを保存するには、名前を手動で入力できます。

Android Enterprise用のMDXアプリをアップロードした後、Citrix Endpoint Managementコンソールで管理対象Google PlayストアのUIが開かない場合があります。この問題が修正されるまで、管理対象Google Playストアにアクセスして、アプリを手動で承認および保存してください。

iOSの場合、以下の操作を行うと位置情報追跡が機能しません：位置情報ポリシーを構成して展開し、デバイスセキュリティアクションから追跡を有効にし、その後、展開済みの位置情報ポリシーを削除して新しいものを作成する。

ユーザー名にアポストロフィが含まれるユーザーは、LDAPからユーザー名がインポートされた場合、デバイスを登録できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント マネジメント 19.10.0

Zebra OEMConfigのサポートを拡張。 Citrix Endpoint Managementは、Zebra Technologiesの管理ツールであるZebra OEMConfigを使用してZebraデバイスを管理できるようになりました。（詳細については、Zebra TechnologiesのWebサイトを参照してください。）Zebra OEMConfigアプリを使用してデバイスを管理するには、アプリを公開し、管理対象構成デバイスポリシーを構成します。

Windowsアプリでコンテンツデリバリーネットワーク（CDN）が利用可能に。 コンテンツデリバリーネットワークを使用してWindowsアプリを展開できるようになりました。Citrix CDNからエンタープライズアプリを配信するを参照してください。

名前に特殊文字を含むユーザーに対するグループ招待のサポート。 登録招待を受け取るグループを選択すると、Citrix Endpoint ManagementはActive Directoryからユーザーリストを取得するようになりました。このリストには、名前に特殊文字が含まれるユーザーも含まれます。登録招待を参照してください。

Citrix Endpoint Management 19.10.0で修正された問題

新しいデバイスを登録するか、古いデバイスを再登録した後、**管理 > デバイス**にエラーメッセージが断続的に表示されます。

管理 > デバイス > 登録済みデバイスでChromeまたはWorkspaceハブデバイスを選択し、**編集**をクリックすると、次のメッセージが表示されます。`A configuration error occurred. Please try again.` このメッセージは、デバイスリストでこれらのデバイスにマウスオーバーして**詳細を表示**をクリックしたときにも表示されます。どちらの場合も、**OK**をクリックして続行します。

シトリックス エンドポイント マネジメント 19.9.1

- **iOSおよびAndroidの暗号化管理のサポート。** 注：この機能は2021年3月以降非推奨です。代わりに、Citrix Endpoint ManagementはiOSおよびAndroidプラットフォームが提供するデバイス暗号化を使用します。Citrix Endpoint Managementは、Citrix MAM SDKを通じて利用可能なコンプライアンスチェックなどの機能で、プラットフォームベースの暗号化を補完します。
- **iPadOSのサポート。** Citrix Endpoint ManagementはiPadOS 13.xをサポートしています。iOSのデバイスポリシーは、iPadOSを実行しているデバイスに適用されます。
    - **Android Enterprise向けアプリ管理の簡素化。** Citrix Endpoint Managementのアプリを承認または公開するために、Managed Google PlayまたはGoogle Developerポータルにアクセスする必要がなくなりました。これにより、アプリの承認と公開に数時間ではなく約10分しかかかりません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **Citrix Endpoint Managementコンソールで、パブリックアプリストア向けAndroid Enterpriseアプリを承認する。** Citrix Endpoint Managementコンソールを離れることなく、Managed Google Playストアアプリを承認できるようになりました。検索フィールドにアプリ名を入力すると、Managed Google PlayストアのUIが開き、アプリを承認して保存するための手順が表示されます。その後、アプリが結果に表示され、詳細を設定できるようになります。パブリックアプリストアアプリの追加を参照してください。
  - **Citrix Endpoint Managementコンソールで、Android Enterprise向けMDXアプリを承認する。** Citrix Endpoint Managementコンソールを離れることなく、Android Enterprise向けManaged Google Playストアアプリを承認できるようになりました。MDXファイルをアップロードすると、Managed Google PlayストアのUIが開き、アプリを承認して保存するための手順が表示されます。MDXアプリの追加を参照してください。
  - **Citrix Endpoint Managementコンソールで、Android Enterprise向けエンタープライズアプリを公開する。** Android Enterpriseプライベートアプリを追加する際に、Google Play開発者アカウントに登録する必要がなくなりました。Citrix Endpoint ManagementコンソールからManaged Google PlayストアのUIが開き、APKファイルをアップロードして公開できます。エンタープライズアプリの追加を参照してください。

- **ワークプロファイルモードまたは完全管理モードのAndroid Enterpriseデバイス向け証明書管理機能の追加。** 管理対象キーストアに証明機関をインストールするだけでなく、以下の機能を管理できるようになりました。

  - **特定の管理対象アプリで使用される証明書を構成する。** Android Enterpriseの資格情報デバイスポリシーに、**証明書を使用するアプリ**設定が追加されました。このポリシーで選択された資格情報プロバイダーによって発行されたユーザー証明書を使用するアプリを指定できます。アプリには、実行時にサイレントで証明書へのアクセスが許可されます。すべてのアプリで証明書を使用するには、アプリリストを空白のままにします。資格情報デバイスポリシーを参照してください。
  - **管理対象キーストアから証明書をサイレントに削除するか、すべての非システム証明機関証明書をアンインストールする。** 資格情報デバイスポリシーを参照してください。
  - **ユーザーが管理対象キーストアに保存されている資格情報を変更できないようにする。** Android Enterpriseの制限デバイスポリシーに、**ユーザーがユーザー資格情報を構成することを許可する**設定が追加されました。デフォルトでは、この設定は**オン**になっています。制限デバイスポリシーを参照してください。

- **Android Enterpriseで位置情報デバイスポリシーが利用可能に。** 管理対象または管理対象プロファイルモードで実行されているAndroid Enterpriseデバイスの位置情報設定を定義できます。Androidの位置情報追跡にはAndroid 8.5以降が必要です。位置情報デバイスポリシーを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **BitLocker回復キーへの簡単なアクセス。** ユーザーがBitLocker回復キーを紛失した場合、デバイスのロック解除が困難になることがあります。Citrix Endpoint Managementは、Windowsデスクトップおよびタブレットの BitLocker回復キーをデバイスの詳細の下に表示するようになりました。BitLocker回復キーを参照してください。

Citrix Endpoint Management 19.9.1の修正された問題

特殊文字を含むカスタムプロパティを追加した後、管理者はXenMobile®コンソールのデバイスページにアクセスできません。

macOSでは、Citrix Endpoint Managementからプッシュされたエンタープライズアプリが保留状態のままになります。このサードパーティの問題はAppleのバグ#50311461であり、macOS 10.14.4で修正されています。

RBACロール `Tier 2 techs` は、2000人を超えるユーザーを含むユーザーグループへの登録招待を作成できません。招待を作成できるのは、完全な管理者ユーザーのみです。

iOSデバイスでは、デバイスがiOS 13.1.xにアップグレードされた後、管理者がパスコードで保護されたデバイスに「デバイスのロック解除」コマンドを送信する機能を失う可能性があります。この問題を解決するには、`https://support.citrix.com/article/CTX262076` を参照してください。

シトリックス エンドポイント マネジメント 19.9.0

- **Android Enterpriseのワークプロファイルデバイスと完全に管理されたデバイスのキーガード機能を管理します。** Androidキーガードは、デバイスとワークチャレンジのロック画面を管理します。キーガード管理デバイスポリシーを使用して、以下を制御します。

  - ワークプロファイルデバイスでのキーガード管理。ユーザーがデバイスのキーガードとワークチャレンジのキーガードを解除する前に利用できる機能を指定できます。たとえば、デフォルトでは、ユーザーは指紋認証によるロック解除を使用したり、ロック画面で編集されていない通知を表示したりできます。
  - 完全に管理されたデバイスおよび専用デバイスでのキーガード管理。キーガード画面を解除する前に、信頼エージェントやセキュアカメラなどの利用可能な機能を指定できます。または、すべてのキーガード機能を無効にすることもできます。

  キーガード管理デバイスポリシーを参照してください。

- **Samsung Knoxコンテナのパスワードリセット。** **コンテナパスワードのリセット**セキュリティアクションは、Android EnterpriseのSamsung Knoxデバイスでは利用できなくなりました。Samsung Knoxコンテナのパスワードをリセットするには、**コンテナロック**セキュリティ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アクションを使用します。**コンテナパスワードのリセット**セキュリティアクションは、デバイス管理者モードのSamsungデバイスでは引き続き利用できます。

- **Android Enterpriseアプリのプロダクトトラックを構成します。** Android Enterprise用のパブリックストアアプリまたはMDXアプリを追加するときに、ユーザーデバイスにプッシュするプロダクトトラックを構成します。たとえば、テスト用に設計されたトラックがある場合、それを選択して特定のデリバリーグループに割り当てることができます。リリースの展開の詳細については、Google Playヘルプセンターを参照してください。プロダクトトラックの構成については、MDXアプリの追加またはパブリックアプリストアアプリの追加を参照してください。
- **Windows GPO構成ポリシーが自動的に有効になります。** Citrix CloudでCitrix Workspace Environment Managementサイトをプロビジョニングすると、Windows GPO構成ポリシーが自動的に有効になります。詳細については、Windows GPO構成デバイスポリシーを参照してください。
- **コンソールでモバイルデバイス管理（MDM）とWorkspace Environment Management（WEM）が管理するデバイスが統合されました。** デバイスがMDMとWEMの両方で管理されている場合、Citrix Endpoint Managementコンソールでは1つのデバイスとして表示されるようになりました。コンソールでのデバイスラベルは**MDM, WEM**です。以前は、デバイスは2つの異なるデバイスとして表示されていました。MDMとWEMの両方で管理されているデバイスも削除できるようになりました。

Citrix Endpoint Management 19.9.0で修正された問題

アプリケーションアクセスデバイスポリシーを展開した後、非準拠デバイスは構成されたアクションをトリガーしません。

Chrome OSデバイスのGoogle Workspace管理者資格情報を構成できません。

Citrix Endpoint Management と Apple School Manager 間の接続に失敗します。

MAMデバイスは、ユーザーのドメイン詳細の取得に失敗したため、アプリとアプリデータを消去します。その結果、デバイスはユーザーを削除済みと見なします。

新しいデバイスを登録した後、または古いデバイスを再登録した後、**Manage** タブにエラーメッセージが断続的に表示されます。

シトリックス エンドポイント マネジメント 19.8.0

- **既存のお客様向け: Citrix Endpoint Management コンソールおよびセルフヘルプポータルへのポートアクセス制限:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 19.8.0 (August 1, 2019) より前にオンボーディングしたお客様向け:

- 管理者がCitrix Endpoint ManagementコンソールへのSSOアクセスにCitrix Cloudコンソールにサインオンすることを要求できます。Citrixは、すべてのコンソールアクセスをCitrix Cloud経由で行うことを強く推奨します。

  新しいサーバープロパティ `enable.cloud.console.sso` を **True** に設定します。これは、Citrix Endpoint Management コンソールに直接アクセスできないことを意味します。ポート 4443 で Citrix Endpoint Management コンソールに直接アクセスしようとすると、500 エラーが発生します。
- セルフヘルプポータルへのアクセスはポート 443 経由でのみ可能です。ポート 4443 経由でのアクセス試行は、「アクセス拒否」メッセージになります。

- **Citrix Endpoint Management 19.8.0 (August 1, 2019) 以降にオンボーディングしたお客様向け:**
  - 新規のお客様は、Citrix Endpoint Management コンソールへのSSOアクセスにCitrix Cloud コンソールにサインオンします。
  - セルフヘルプポータルへのアクセスには、サーバープロパティの変更が必要です。デフォルトでは、新規のお客様はセルフヘルプポータルにアクセスできません。

    ユーザーにセルフヘルプポータルへのアクセスを許可するには、`shp.console.enable` を **True** に更新します。

Citrix Endpoint Management 19.8.0 で修正された問題

CA証明書をインポートしても、コンソールは**PKI entities**の下に更新された証明書や新しい証明書を表示しません。

iOS 用 VPN デバイスポリシーを Citrix SSO プロトコルで使用するように構成する場合: **接続時にPINを要求**設定を有効にしてポリシーを保存すると、その設定が**オフ**に戻ります。

以前のバージョンから移行したお客様の場合、デバイスの登録プロファイルが削除されていると、コンソールで**管理**タブを開いたときにエラーが表示されます。

シトリックス エンドポイント マネジメント 19.7.1

- **管理対象のGoogle Playストア内のすべてのGoogle Playアプリにアクセスする。 管理対象のGoogle Playストア内のすべてのアプリにアクセスする**サーバープロパティにより、公開Google Playストアのすべてのアプリが管理対象のGoogle Playストアからアクセス可能になります。このプロパティを**true**に設定すると、すべてのAndroid Enterpriseユーザーが公開Google

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Playストアアプリを使用できるようになります。管理者は、制限デバイスポリシーを使用して、これらのアプリへのアクセスを制御できます。

- **Android Enterpriseデバイスでシステムアプリを有効にする。** ユーザーがAndroid Enterpriseの仕事用プロファイルモードまたは完全管理モードでプリインストールされたシステムアプリを実行できるようにするには、制限デバイスポリシーを構成します。この構成により、ユーザーはカメラ、ギャラリーなどのデフォルトのデバイスアプリにアクセスできるようになります。特定のアプリへのアクセスを制限するには、アプリの権限ポリシーを使用してアプリの権限を設定します。

Citrix Endpoint Management 19.7.1で修正された問題

SMTP/SMSを使用して登録リンクを送信すると、送信されたリンクが機能しません。

Citrix Endpoint Managementコンソールを使用して公開iOSアプリを更新しようとすると、構成エラーが表示されます。

一部のサードパーティ製Volume Purchaseアプリが自動更新に失敗します。この問題は、ブロックされたホスト名が原因で発生しました。詳細については、`<https://support.apple.com/ja-jp/HT201999>`を参照してください。

Microsoft WordまたはPowerPoint for iOSをクラウドアプリライブラリに追加すると、アプリをユーザーグループに割り当てることができません。この問題が発生しているIntuneアプリは、削除して再追加する必要があります。

シトリックス エンドポイント マネジメント 19.6.1

- **位置情報デバイスポリシーでAndroidのデバイス追跡が可能になりました。** 定義した頻度で特定のデバイスをポーリングするデバイス追跡を有効にできるようになりました。このポリシーを使用して、配達員の追跡によるより正確な配達見積もり、紛失または盗難されたデバイスの追跡、または地理的境界の強制を行うことができます。詳細については、位置情報デバイスポリシーを参照してください。

Citrix Endpoint Management 19.6.1で修正された問題

自動的にアップロードされたアプリのアイコンが、Citrix Endpoint Managementコンソールに表示されません。

サーバープロパティ`bulk.enrollment.fetchRosterInfoDelay`の期間が終了し、Apple School Managerデバイスがサーバーと同期した後: Apple School Managerユーザーアカウントがサーバーから削除され、デバイスは匿名状態になります。

表示名にウムラウトなどの特殊なドイツ語文字を含むユーザーは登録できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apple Storeの新しいアプリURLを使用してパブリックアプリを構成しようとすると、次のエラーメッセージが表示されます。「入力したアプリが見つかりませんでした。URLを確認して、もう一度お試しください。」

シトリックス エンドポイントマネジメント 19.6.0

- **Appleボリューム購入アプリの自動更新。** ボリューム購入アカウント（**設定 > iOS設定**）を追加すると、すべてのiOSアプリの自動更新を有効にできるようになりました。Appleボリューム購入の**アプリの自動更新**設定を参照してください。

Citrix Endpoint Management 19.6.0で修正された問題

レジストリ値の長さが2048文字を超えると、Windows Embedded Compactポリシーにレジストリキーを追加する際に次のエラーが表示されます。 `Console error: could not execute statement; SQL [n/a]; nested exception is org.hibernate.exception.DataException: could not execute statement` 。

iOSデバイスでのプロファイルインストール中に、プロファイル情報に「未確認」と表示されます。

Azure ADユーザーがキオスクとして構成された一部のWindows 10 Azure AD参加済みデバイスにサインインすると、キオスクモードがアクティブになりません。この問題は、Azure ADユーザー名を `azuread\user` の形式で入力した場合には発生しません。詳細については、キオスクデバイスポリシーを参照してください。

自動的にアップロードされたアプリのアプリアイコンが、Citrix Endpoint Managementコンソールに表示されません。

ボリューム購入アカウント（**設定 > iOS設定**）を追加する際に、トークンが350文字を超えると、次のメッセージが表示されます。 `The entered company token is not valid, please enter a new one.`

シトリックス エンドポイントマネジメント 19.5.0

- **iOS MDM登録ワークフローの変更。** 誤解を招くプロファイルのインストールを減らすことでプラットフォームのセキュリティを向上させるため、AppleはMDMにデバイスを手動で登録するための新しいワークフローをリリースしました。この新しいワークフローは、Citrix Endpoint Managementを含むすべてのMDMソリューションに影響します。

  Apple Business ManagerまたはApple School Managerで割り当てられたサーバーへのMDM登録に変更はありません。ワークフローの変更は、MDMへの手動登録のみに適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrixは登録も簡素化しました。以前は、iOSデバイスユーザーは登録中に2つのプロンプトを受け取っていました。ルートCAのプロンプトとMDMデバイス証明書のプロンプトです。Citrixは、署名なし証明書と署名済み証明書を柔軟に使用できるようにルートCAをインストールしていました。すべてのCitrix Cloud展開で信頼された証明書が使用されるため、ルートCAは不要になりました。

iOSデバイスユーザーは、登録中にMDMデバイス証明書のプロンプトのみを受け取ります。このプロンプトには「XenMobile Profile Service」というラベルが付いています。

この変更をサポートするため、Citrix はサーバープロパティ `ios.mdm.enrollment.installRootCaIfRequired` の値を `false` に変更しました。MDM登録中にSafariウィンドウが開き、ユーザーのプロファイルインストールを簡素化します。詳細については、iOSデバイスの登録 および以下のYouTubeビデオを参照してください。



- **新規Citrix Endpoint Managementのお客様向けの変更点:**
  - **Workspaceエクスペリエンスの展開。** 新しいデバイスにWorkspaceエクスペリエンスを展開し始めるために、Workspaceという名前の個別のデリバリーグループを作成できます。Workspaceデリバリーグループを使用することで、すべてのユーザーに影響を与えることなく、少数のグループにWorkspaceエクスペリエンスを提供できます。
  - **Citrix Endpoint Management 19.5.0以降の新規顧客向けの事前構成済みポリシーとアプリ。** Citrix Endpoint Management 19.5.0以降でオンボーディングする場合、いくつかのデバイスポリシーとモバイル生産性アプリが事前構成されています。この構成により、デバ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イスユーザーに基本的な機能をすぐに展開できます。デフォルトのデバイスポリシーとモバイル生産性アプリを参照してください。

- **Android Enterprise向けKnox Platform for Enterpriseデバイスポリシー（非推奨）。** Knoxバージョン3.0以降を実行しているAndroid EnterpriseデバイスのKPE PremiumおよびStandardライセンスキーを入力できるようになりました。
- **Chrome OS向けパブリックセッションデバイスポリシー。** Chrome OSデバイスをゲストセッションをサポートするように構成できるようになりました。このポリシーの構成については、「パブリックセッションデバイスポリシー」を参照してください。
- **RBAC権限の変更。** RBAC権限「ローカルユーザーの追加/削除」は、「ローカルユーザーの追加」と「ローカルユーザーの削除」の2つの権限に分割されました。

Citrix Endpoint Management 19.5.0で修正された問題

iOS 11.4以降を実行している監視対象デバイスでは、エンタープライズアプリはサイレントアップグレードされません。

デバイスポリシーを編集すると、次のエラーメッセージが表示されます: `A configuration error occurred. Please try again`。

シトリックス エンドポイント管理 19.4.1

- **Workspace Environment Management (WEM)とCitrix Endpoint Managementの統合により、サポートされているすべてのドメイン参加済みWindowsデバイスを管理できます。** この統合は、以下の利点と機能を提供します:
  - WEM単独では、MDM展開は不可能です。Citrix Endpoint Management単独では、Windows 10デバイスの管理に限定されます。2つの製品を統合することで:
    - WEMはMDM機能にアクセスできます
    - Citrix Endpoint Management を通じて、より広範な Windows オペレーティングシステムを管理できます。
  - その管理は、Windows GPO の構成という形で行われます。現在、管理者は ADMX ファイルを Citrix Endpoint Management にインポートし、それを Windows 10 デスクトップおよびタブレットにプッシュして、特定のアプリケーションを構成しています。Windows GPO 構成デバイスポリシーを使用すると、GPO を構成し、WEM サービスに変更をプッシュできます。その後、WEM エージェントが GPO をデバイスとそのアプリに適用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- WEM 統合に MDM 管理は必須ではありません。Citrix Endpoint Management がそのデバイスをネイティブにサポートしていない場合でも、WEM がサポートするすべてのデバイスに GPO 構成をプッシュできます。
- サポートされているデバイスのリストについては、「オペレーティングシステムの要件」を参照してください。
- Windows GPO 構成デバイスポリシーを受信するデバイスは、WEM と呼ばれる新しい Citrix Endpoint Management モードで実行されます。登録済みデバイスの **>** リストでは、WEM 管理デバイスの 列に **WEM** と表示されます。

詳細については、「Windows GPO 構成デバイスポリシー」を参照してください。

- **Citrix Endpoint Management 19.4.1 以降の新規マルチテナンシーのお客様の場合、エンタープライズアプリの CDN 配信がデフォルトになりました。** アジア太平洋地域の新規のお客様は、CDN 配信を有効にするには Citrix サポート担当者にお問い合わせください。すべての地域で、CDN を使用してエンタープライズアプリを配信したい既存のお客様は、機能を有効にした後、既存のアプリを再アップロードする必要があります。「Citrix CDN からエンタープライズアプリを配信する」を参照してください。
- **Android Enterprise 向け Web および SaaS アプリと Web リンクのサポート。** Citrix Endpoint Management は、Web または SaaS アプリのリンクと Web リンクを Android Enterprise デバイスに配信できるようになりました。Web および SaaS アプリと Web リンクは、他のプラットフォームに追加するのと同じ方法で Android Enterprise に追加されます。「Web または SaaS アプリを追加する」および「Web リンクを追加する」を参照してください。
- **Chrome OS デバイスの制限事項の追加:**
  - **無効なデバイスに指示を表示。** 無効な Chrome OS デバイスに表示するカスタムメッセージを追加できるようになりました。
  - **ユーザーが特定の拡張機能、アプリ、テーマをインストールできるようにする。** これらのソースからのダウンロードを許可する URL のリストを入力します。

  詳細については、「Chrome OS の設定」を参照してください。

Citrix Endpoint Management 19.4.1 で修正された問題

Android Enterprise デバイスでは、Citrix Secure Hub に次のアプリの種類が表示されない場合があります: Google Play プラットフォームで構成された公開アプリストアアプリと、Android プラットフォームで構成されたエンタープライズアプリ。

Android Enterprise アプリは、デバイスが登録解除されてから再度登録されるまで表示されません。配信グループでアプリを更新した場合も表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

自動アクションがAndroid Enterpriseデバイスに展開されない場合があります。

Google Playストアの管理者コンソールで、Android Enterpriseエンタープライズの名前と所有者が正しく表示されない場合があります。

シトリックス エンドポイント管理 19.3.1

Citrix Endpoint Management 19.3.1で修正された問題

リリース19.3.1より前にWindows 10デスクトップおよびタブレットデバイス用のストアデバイスポリシーを展開した場合、ユーザーがスタートメニューのWindowsストアリンクをクリックすると、「500 Internal Server Error」または「HTTP Status 404 - Either you've reached an old URL or this device isn't registered」というメッセージが表示されます。この問題を解決するには、ストアデバイスポリシーを再作成して展開する必要があります。

Active Directoryユーザーグループが RBACロールの権限に割り当てられている場合、そのユーザーグループを持つLDAP構成を削除することはできません。回避策として、対応するActive Directoryグループを RBACから割り当て解除すると、ドメインを削除できます。

シトリックス エンドポイント マネジメント 19.3.0

- **Android Enterpriseポリシー統合におけるSamsung Knoxのサポート。** Samsung Knox 3.0以降およびAndroid 8.0以降を実行しているAndroid Enterpriseデバイスの場合、KnoxとAndroid Enterpriseは統合されたデバイスおよびプロファイル管理ソリューションに結合されます。以下のデバイスポリシーのAndroid Enterpriseページで Knox設定を構成します。
  - **OS更新デバイスポリシー。** Samsung Enterprise FOTAの更新を制御します。OS更新デバイスポリシーを参照してください。
  - **パスコードデバイスポリシー。** パスコードデバイスポリシーを参照してください。
  - **制限デバイスポリシー。** 制限デバイスポリシーを参照してください。
  - **Samsung MDMライセンスキーデバイスポリシー（非推奨）。** Knoxライセンスキーを構成します。
- **Android Enterprise用アプリインベントリデバイスポリシー。** 管理対象デバイス上のAndroid Enterpriseアプリのインベントリを収集できるようになりました。詳細については、アプリインベントリデバイスポリシーを参照してください。
- **Android Enterprise用ファイルデバイスポリシー。** Citrix Endpoint Managementにスクリプトファイルを追加して、Android Enterpriseデバイスで機能を実行できるようになりました。ファイルデバイスポリシーを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Android Enterpriseのパスワードのロックとリセット。** Citrix Endpoint Managementは、Android 8.0以降を実行しているワークプロファイルモードで登録されたAndroid Enterpriseデバイスのパスワードのロックとリセットのセキュリティアクションをサポートするようになりました。セキュリティアクションを参照してください。
- **Windows 10デスクトップおよびタブレットデバイスのキオスクでのAzure Active Directoryサポート。** キオスクモードでドメイン参加済みのAzure ADデバイスを追加できるようになりました。「キオスクデバイスポリシー」を参照してください。
- **ワークスペースエクスペリエンスが有効になっているCitrix Endpoint Managementのお客様向け: Citrix Endpoint Managementは、iOSおよびAndroid上のCitrix Workspaceアプリを介したフェデレーション認証をサポートします。** この機能はAzure Active Directoryをサポートしていません。詳細については、「認証方法の選択または変更」を参照してください。
- **パブリックREST APIの変更。** Citrix Endpoint ManagementのRESTサービス用パブリックAPIに、MDXアプリのコンテナ内のプラットフォーム詳細を編集するAPIが追加されました。PDFの「Section 3.15.2.4 Update platform details inside the container for MDX apps」にある「RESTサービス用パブリックAPI」を参照してください。

Citrix Endpoint Management 19.3.0で修正された問題

パスコードでロックセキュリティアクションを使用して完全に管理されたAndroid Enterpriseデバイスをリモートでロックすると、失敗を通知することなく失敗する場合があります。デバイスがロックされていることを確認するには、**パスコードでロック**を2回設定します。デバイスは、設定した2番目のパスコードでロックされます。

Managed Google Playからエンタープライズが削除され、Citrix Endpoint Managementサーバーで更新された場合、Android Enterpriseデバイスが登録できないことがあります。

Microsoft Endpoint ManagerとのCitrix Endpoint Management統合の場合: Intuneストアアプリの名前または説明に加えられた変更が保存されません。

iOS Intuneアプリを編集した後、そのアプリはMicrosoft Company Portalアプリからインストールされません。

フル管理者ではなくCitrix Cloudカスタム管理者として権限が割り当てられている場合、リソースをナビゲートするために**管理**ボタンをクリックできません。

TLSバージョンの非推奨化

Citrix Endpoint Managementサービスのセキュリティを向上させるため、Citrixは現在、Transport Layer Security (TLS) 1.0および1.1を介したすべての通信をブロックしています。セキュリティの脆弱化のため、PCI CouncilはTLS 1.0を非推奨にしています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

この変更がお客様に与える影響

オンプレミスのNetScaler Gateway (NetScaler Gateway) を介してモバイルアプリケーション管理を使用している場合、ロードバランサーサービスを更新してTLS 1.2を有効にする必要があります。

以下のコネクタの古いバージョンはTLS 1.0のみをサポートしています:

- エクスチェンジ アクティブシンク 用 シトリックス エンドポイント マネジメント コネクタ
- Exchange ActiveSync 用 NetScaler Gateway コネクタ

コネクタを次のようにアップグレードしてください。

- Exchange ActiveSync 用 Citrix Endpoint Management コネクタのビルド 10.1.3 以前を使用している場合は、ビルド 10.1.4 以降にアップグレードしてください。
- Exchange ActiveSync 用 NetScaler Gateway コネクタのビルド 8.5.0 以前を使用している場合は、ビルド 8.5.1.11 以降にアップグレードしてください。

実施事項

オンプレミスの NetScaler Gateway (NetScaler Gateway) を使用している場合は、ロードバランサーサービスで TLS 1.2 を有効にしてください。詳細については、`<https://support.citrix.com/article/CTX247095>` を参照してください。

Exchange ActiveSync 用のいずれかのコネクタをダウンロードするには：

```
1.  Go to `<https://www.citrix.com/downloads>`.

1.  Navigate to **Citrix Endpoint Management (and Citrix XenMobile Server)
> XenMobile Server (on-premises) > Product Software > XenMobile Server 10
> Server Components**.

1.  Locate the connector tile and then click **Download File**.
```

シトリックス エンドポイント マネジメント 19.2.1

- **Chrome デバイスのキオスクで複数のアプリを実行する。** Chrome OS のキオスクポリシーに複数のアプリを追加できるようになりました。ユーザーがデバイスを起動したときに、オプションでアプリを自動的に起動できます。キオスクデバイスポリシー を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management 19.2.1 で修正された問題

Android Enterprise の登録を解除してから再登録すると、承認されたアプリがワークプロファイルモードで登録されたデバイスに表示されない場合があります。

ユーザーが Intune MDM+MAM で Citrix Secure Mail を初めて実行すると、セットアップにより Intune MAM/XenMobile を選択するワークフローが案内されます。

シトリックス エンドポイント マネジメント 19.2.0

- **コンテンツデリバリーネットワーク (CDN) からエンタープライズアプリを配信する。** ユーザーが Citrix Endpoint Management サーバーの近くにいない場合、エンタープライズアプリの配信には時間がかかることがあります。アプリのダウンロードを高速化するために、代わりに世界中のコンテンツデリバリーネットワーク (CDN) の場所からエンタープライズアプリを配信できます。エンタープライズアプリの CDN サポートは、iOS アプリ (MDM または MAM 登録) および Android アプリ (MDM または MAM 登録) で利用できます。エンタープライズアプリの CDN サポートは、Windows アプリでは利用できません。開始するには、Citrix CDN からエンタープライズアプリを配信する を参照してください。
- **Citrix Workspace の DEP デバイス登録の変更。** Citrix Endpoint Management が Citrix Workspace と統合されている場合、Citrix Workspace アプリは必須アプリとして DEP 展開パッケージに含まれます。この機能では、iOS 用の DEP アカウント設定を、必要な資格情報がオフに設定されている状態で構成する必要があります。Citrix Secure Hub は、Citrix Endpoint Management に登録する前に、Citrix Workspace にデバイスを登録するようユーザーに促します。
- **サーバープロパティ ios.mdm.enrollment.installRootCalfRequired が false に設定されました。** Citrix Endpoint Management は公開されている信頼された証明書チェーンを使用するため、ルートCAをデバイスにプッシュする必要はありません。その結果、iOSデバイスユーザーは登録中にルートCAのインストールを促されることがなくなりました。
- **ネットワークおよび資格情報ポリシーがApple TV OSをサポートするようになりました。** さらに、AirPlayセキュリティデバイスポリシーを構成して、どのデバイスがApple TVデバイスに接続できるかを制御できるようになりました。詳細については、ネットワーク、資格情報、およびAirPlayセキュリティデバイスポリシーの記事を参照してください。
- **Android Enterpriseで位置情報デバイスポリシーが利用可能になりました。** 管理対象または管理対象プロファイルモードで実行されているAndroid Enterpriseデバイスの位置情報設定を定義できます。位置情報デバイスポリシーを参照してください。
- **Alexa for Businessのサポートが強化されました。** Citrix Endpoint Managementは、Alexa for Business会議、組織へのAlexaスキルの追加、スキルグループの編集をサポートするようになりました。Alexa for Businessを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Windowsエージェントポリシーの自動アクション。** Windowsエージェントポリシーを使用すると、レジストリ値に基づいてWindowsデスクトップおよびタブレットで実行するアクションを自動化できます。詳細については、Windowsエージェントデバイスポリシーおよび自動アクションの記事を参照してください。
- **Android Enterpriseでは、パスコードの必須文字に対する「制限なし」オプションは非推奨になりました。** Android 7以降を実行しているAndroid Enterpriseデバイスは、文字制限なしで作成されたパスコードをサポートしなくなりました。以前に**必須文字**を**制限なし**に設定していた場合、この更新によりその値が**数字のみ**に変更されます。この変更は、現在のユーザーサインインエクスペリエンスには影響しません。詳細については、Android Enterprise設定を参照してください。

Citrix Endpoint Management 19.2.0で修正された問題

Intuneライブラリからアプリが削除され、ユーザーがCitrix Cloudライブラリから削除しようとすると、削除できません。

Endpoint Managerコンソールでアプリのアイコン画像を追加せずにGoogle Playアプリをアップロードした後、後でそのアプリの画像をアップロードしても、その画像はアプリリストに表示されません。

シトリックス エンドポイント マネジメント 19.1.2

- **Android Enterpriseでファイルデバイスポリシーが利用可能になりました。** Citrix Endpoint Managementにスクリプトファイルを追加して、Android Enterpriseデバイスで機能を実行できます。ファイルデバイスポリシーを参照してください。
- **Chrome OSデバイスのタイムゾーン設定を構成します。** Chromeデバイスのタイムゾーンを選択し、タイムゾーンを検出する方法を指定できるようになりました。詳細については、制限デバイスポリシーを参照してください。
- **RBAC管理者のグループ権限により、ユーザーおよび登録招待ページに表示されるユーザー情報が制限されるようになりました。** 以前は、Citrix Endpoint Managementコンソールには、**管理 > ユーザー**および**管理 > 登録招待**ページにすべてのローカルユーザーとドメインユーザーの情報が含まれていました。

  RBAC管理者が表示および管理する権限を持つユーザーグループを指定するには、管理者ロールを編集してユーザーグループを指定します。詳細については、RBACでロールを構成するを参照してください。
- **Citrix Workspaceアプリからサードパーティ製アプリを起動します。** Citrix Workspaceが有効になっているお客様の場合: 新しいアプリをユーザーに展開する前に、Citrix Workspaceアプリ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

からアプリを起動するためのURLのコンマ区切りリストを追加できます。詳細については、アプリの追加を参照してください。

Citrix Endpoint Management 19.1.2 の修正された問題

Citrix Endpoint Management コンソールでは、Google Play 開発者サービス APK のバージョン 11.5.09 以降をアップロードできません。

Configure > Apps > Public App Store で Windows デスクトップおよびタブレットアプリを編集すると、「Application search failed」というメッセージが表示されます。これらのアプリを検索すると、「Error connecting to the windows desktop store url: Failed to retrieve public app details」というメッセージが表示されます。

サードパーティ通知

Citrix Endpoint Management には、以下のドキュメントに定められた条件に基づいてライセンスされたサードパーティソフトウェアが含まれている場合があります。

Citrix Endpoint Management サードパーティ通知

非推奨

この記事の発表は、段階的に廃止されるCitrix Endpoint Management機能の事前通知であり、お客様が適切なビジネス上の意思決定を行えるようにするためのものです。Citrixは、お客様の使用状況とフィードバックを監視し、いつ廃止されるかを決定します。発表は以降のリリースで変更される可能性があり、すべての非推奨機能や機能が含まれていない場合があります。製品ライフサイクルサポートの詳細については、製品ライフサイクルサポートポリシーの記事を参照してください。

重要:

Citrix Endpoint Management Analyzer Toolをご利用いただきありがとうございます。頻繁で安定したリリースサイクルにより、このツールは不要になりました。Citrixは、March 31, 2023をもってこのサービスを停止することを決定しました。Citrix Endpoint ManagementコンソールまたはCitrix NetScaler Gateway内で利用可能な接続性チェックを使用することをお勧めします。詳細については、接続性チェックを参照してください。

非推奨および削除

以下の一覧は、非推奨または削除されたCitrix Endpoint Management機能を示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

*非推奨*の項目はすぐに削除されません。Citrix®は、将来のリリースで削除されるまで、非推奨の項目を引き続きサポートします。

*削除済み*の項目は、Citrix Endpoint Managementで削除されるか、サポートされなくなります。

サポート終了（EOL）に達したモバイル生産性アプリに関する情報については、EOLおよび非推奨アプリを参照してください。

項目	説明	非推奨の発表	削除済み	代替
Citrix Cloud™ (CC) ライブラリを介して Microsoft Intune アプリを管理する。	CCライブラリを介した Microsoft Intune アプリ管理のサポートを廃止しました。Intune アプリを既に使用している場合は影響を受けません。	2025年3月	2025年4月	代替手段はありません。
Android Enterprise向けのSamsung完全管理対象デバイスのみの2つの制限。	制限ポリシーから次の設定を廃止しました: ODE Trusted Boot検証を有効にする、および失効チェックを有効にする。	2025年2月	2025年3月	代替手段はありません
Android Enterprise向けのSamsung Knoxコンテナのみの制限。	制限ポリシーから次の設定を廃止しました: アプリをコンテナに移動する、多要素認証を強制する、コンテナの認証を強制する、およびセキュアキーパッドを有効にする。	2025年2月	目標: 2025年6月	代替手段はありません

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
ShareFileとの統合	ShareFile (現在はProgress) がサポートを終了した場合、ShareFile との統合は非推奨になります。	2025年1月		代替なし
モニタータブ	Citrix Endpoint Management のモニタータブは非推奨になりました。	2024年9月	2024年10月	代替なし
Citrix Endpoint Management Government オファリング	Citrix Endpoint Management Government オファリングのサポートは非推奨になりました。	2022年1月	2022年7月	Citrix Endpoint Management Standard エディション
SafetyNet アッテステーション API	Google からの発表 ((https://developer.android.com/training/safetynet/deprecation-timeline)こちら) に基づき、Android SafetyNet Attestation のサポートは非推奨になりました。	2023年7月	2023年11月	プレイ インテグリティ API
クローム OS	Chrome OS のサポートは非推奨になりました。	2022年7月	2023年5月	代替なし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
tvOS	tvOS のサポートは非推奨になりました。	2022年7月	2023年5月	代替なし
Windows 情報保護 (WIP)	Microsoft からの発表 ((https://techcommunity.microsoft.com/t5/windows-it-pro-blog/announcing-the-sunset-of-windows-information-protection-wip/ba-p/3579282)) に基づき、Windows Information Protection のサポートは非推奨になりました。	2022年8月	2022年10月	代替なし
シトリックス エンドポイントマネジメントアナライザー	Citrix Endpoint Management Analyzerツールのサポートを非推奨にしました。	2022年7月	目標: March 31, 2023	代替なし
Workspace hub デバイス管理	Citrix Ready® workspace hub デバイスのサポートを非推奨にしました。	2022年1月	2022年6月	代替なし
マイクロソフトストア for ビジネス	Microsoft Store for Businessのサポートを非推奨にしました。Microsoftはこの	2021年7月	目標: 2023年3月	代替なし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
	プラットフォームのサポートを終了しました。詳細については、Microsoftのドキュメントを参照してください。			
サムスン SAFE	Samsung SAFEのサポートを非推奨にしました。	2022年1月	2022年6月	Android Enterpriseを使用してください。
Zebra用カスタムXML	ZebraデバイスでのカスタムXMLのサポートを非推奨にしました。	2022年1月	2022年6月	Android Enterpriseの管理対象構成を使用してください。
PKI ID: 汎用、Symantec PKI、DigiCert、および Entrust	Generic、DigiCert Managed、EntrustアダプターPKIエンティティのサポートを非推奨にしました。	2021年6月	2022年1月	代替手段なし
ワークスペース向け Android	Android for Workspace のサポートを廃止	2022年1月	2022年4月	代替手段なし
キャリアSMSゲートウェイ	Nexmo SMSゲートウェイ通知のサポートを廃止	2022年1月	2022年4月	SMTPサーバー通知を使用
モバイルサービスプロバイダー (MSP)	Blackberryおよびその他のExchange ActiveSyncデバ	2022年1月	2022年4月	代替なし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
	イスを照会し、操作を発行するためのMSPインターフェースのサポートを廃止			
MDX ツールキット	Mobile App Management (MAM) SDKを優先して、MDX Toolkitのサポートを非推奨にします。移行期間中は、MDXでラップされたアプリとMAM SDKで開発されたアプリの両方を使用できます。	2020年3月	2023年7月	エンタープライズアプリケーションの管理を継続するには、MAM SDKを使用してください。
RBACロール - 共有デバイス登録者およびCOSUデバイス登録者	共有デバイス登録者とCOSUデバイス登録者の両方について、事前定義されたロールベースアクセス制御設定のサポートを非推奨にします。	2021年7月	2021年12月	iOSデバイスは(/ja-jp/citrix-endpoint-management/device-management/apple/shared-ipads.html#prerequisites-for-shared-ipads)経由で構成します。Android COSU (専用) デバイスは(/ja-jp/citrix-endpoint-management/users/enrollment-profiles.html)経

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
				由で構成します。
Windowsデバイス向けのWi-Fi Senseホットスポットへの自動接続を許可する制限。	Windows 10デバイス向けのWi-Fi Senseホットスポットへの自動接続を許可する制限のサポートを削除します。Windows 10はこの機能をサポートしなくなりました。詳細については、(https://docs.microsoft.com/ja-jp/windows/configuration/manage-wifi-sense-in-enterprise)を参照してください。	2021年10月	2022年2月	代替なし
MDX: 代替ゲートウェイサーバー	iOSおよびAndroidデバイスのステップアップ認証を非推奨化。	2020年3月	2021年9月	代替なし
MDX: マイクロVPN (フルトンネルモード)	iOSおよびAndroidデバイス向けのフル仮想プライベートネットワーク (VPN) トンネルを非推奨化。	2020年3月	2021年9月	MAM SDK Web SSOモードを使用するか、Citrix SSO接続タイプでアプリごとのVPNポリシーを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
MDX: PACファイルサポート	iOSおよびAndroidデバイス向けのフルVPNトンネル展開におけるプロキシ自動構成 (PAC) ファイルのサポートを非推奨化。	2020年3月	2021年9月	内部ネットワークにアクセスするために、プロキシサーバー経由で接続するにはNetScaler Gatewayを使用します。
MDX共有デバイスのサポート	MDXアプリの共有デバイスサポートは非推奨になりました。	2020年3月	2021年9月	Android Enterpriseの場合、専用デバイスとして登録された共有デバイスを使用します。iOSの場合、Apple School ManagerまたはGroundControlを使用します。
Android - ソニー	Android Sonyデバイスおよび Sony固有のポリシーのサポートは非推奨になりました。	2021年1月	2022年2月	Android Enterpriseを使用します
アンドロイド - HTC	Android HTCデバイスおよび HTC固有のポリシーのサポートは非推奨になりました。	2021年1月	2022年2月	Android Enterpriseを使用
アンドロイド - アマゾン	Android Amazonデバイスおよび Amazon固有の	2021年1月	2022年2月	Android Enterpriseを使用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
	ポリシーのサポートを廃止しました。			
ノックス モバイル エンロールメント (レガシーDA)	すべてのAndroidバージョンにおけるレガシーのデバイス管理者モードでのKnox Mobile Enrollment (KME) のサポートを廃止しました。	May 4, 2021	2021年9月	KMEを使用してAndroid Enterpriseモードに登録します。Android 8、9、10、11はAndroid Enterpriseをサポートしています。
高セキュリティ登録モード	**高セキュリティ**登録セキュリティモードでの登録招待の生成のサポートを廃止しました。	2021年7月	2022年2月	サポートされている登録セキュリティモードのリストについては、登録招待を参照してください。
派生資格情報	派生資格情報とCitrix Derived Credential Managerアプリのサポートは非推奨になりました。	2021年3月	2021年12月	iOSでサポートされている認証タイプのリストについては、iOSを参照してください。
APNs送信ポート	AppleによるAPNsレガシーバイナリプロトコルのサポートは、March 31, 2021をもって終了します。Appleは、代わりにHTTP/2	2020年10月	2021年3月	代わりにポート443を使用してください。ネットワークとファイアウォールの要件を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
	ベースのAPNsプロバイダーAPIを使用することを推奨しています。この変更の一環として、`*.push.apple.com`にAPNs通知を送信するために使用されるポート2195および2196のサポートを非推奨とします。			
MDXサービス	MDXサービスは、Mobile App Management (MAM) SDKを優先してサポートが非推奨になりました。移行期間中は、MDX Toolkitを使用したMDXラップアプリとMAM SDKで開発されたアプリの両方を使用できます。	2020年3月	2021年9月	エンタープライズアプリケーションのラッピングを継続するには、MDX Toolkitを使用してください。
セルフヘルプポータルでの登録招待のセットアップ	ユーザーがセルフヘルプポータルから登録招待を生成する機能のサポートを廃止しました。	2021年7月	2021年7月	Citrix Endpoint Managementコンソールで登録招待を生成するには、管理者にお問い合わせください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
登録招待のセットアップ	デバイスのIMEI、シリアル番号、UDIDを使用して登録招待を作成する機能のサポートを廃止しました。	2021年4月	2021年7月	登録招待を作成する際は、Citrix Endpoint Managementコンソールの**[管理] > [登録招待]**で利用可能な設定を構成してください。
証明書ベースの認証署名アルゴリズム（非FIPSおよび脆弱な暗号）	以下の署名アルゴリズムのサポートを廃止しました: SHA1withRSA、SHA224withRSA、SHA1withECDSA、SHA224withECDSA、SHA1withDSA、RIPEMD160withRSA、RIPEMD128withRSA、RIPEMD256withRSA。	2020年5月	2021年6月	Citrix Endpoint Managementコンソールで資格情報プロバイダーのCSRを作成する際 (**設定 > 資格情報プロバイダー > 証明書署名要求**)、より強力な暗号を選択してください。
Android 7.xおよびiOS 12.x向けCitrixモビリティアプリとWorkspaceアプリ	Citrix Secure Hub、Citrix Secure Mail、Citrix Secure Web、およびCitrix WorkspaceアプリのAndroid 7.xおよびiOS 12.xバージョンのサ	2021年4月	2021年6月	各主要オペレーティングシステムプラットフォームの、少なくとも現在および以前のバージョンを使用してください。古いデバイスは登録されたままで

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
	ポートを廃止しました。			す。ただし、Citrixはレガシーデバイスのテストやサポートを行いません。
Android向けRSAソフトトークンのサポート	Android版Citrix Secure HubへのRSAソフトトークンの直接インポートのサポートを廃止しました。	2021年1月	2021年2月	Google Playで入手可能なRSA Secure IDアプリ内でRSAソフトトークンをインポートできます。その後、そのトークンをNetScaler Gateway認証に使用できます。
インターネットエクスプローラー 11	Citrix Endpoint ManagementコンソールでのInternet Explorerの使用のサポートを廃止しました。	2021年1月	2021年1月	これらのWebブラウザの最新バージョンを使用してください: Google Chrome、Mozilla Firefox、Microsoft Edge、Apple Safari
Citrix Endpoint Management AnalyzerでのゲートウェイI構成チェック	ゲートウェイ構成チェックオプションのサポートを廃止しました。	2020年11月	2020年11月	AnalyzerのCitrix Insight Servicesチェックを使用して、Citrix Endpoint Managementの展開準備状況についてCitrix ADC構成を確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
Android Enterpriseデバイス上のレガシーなデバイス管理者モード向けに公開されたアプリ	レガシーDAプラットフォーム向けに公開されたアプリは、Android Enterpriseに登録されているデバイスには配信しなくなりました。	2020年10月	2020年11月	Android Enterpriseデバイスの場合、Android Enterpriseプラットフォーム向けにアプリを公開します。DAモードのデバイスにレガシーDAアプリを公開し続けるには、それらのアプリ用に個別のデリバリーグループを作成します。
Android 10デバイス向けのレガシーなデバイス管理者モード	Googleは一部のデバイス管理者APIを廃止しました。Citrixは、Android APIレベル29をターゲットとするCitrix Secure Hubへのアップグレード以降、デバイス管理者モードに登録されたAndroid 10デバイスをサポートしていません。	2020年2月	2020年11月	Android 10デバイスをAndroid Enterpriseに移行します。
アンドロイドタッチダウン	DigiCertはAndroid TouchDownのサポートを終了しました。Citrixは、	2018年7月	2020年11月	推奨事項: Citrix Secure Mailを使用してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
	Exchangeデバイスポリシーから Android TouchDownプラットフォームページを削除しました。			
Android 10の新しいデバイス管理者登録	Android 10デバイスでのレガシーなデバイス管理者モードへの新規登録または再登録のサポートは非推奨になりました。すでに登録されているデバイスは引き続き機能します。	2020年2月	2020年9月	新しいAndroid 10以降のデバイスをAndroid Enterpriseに登録します。
MDX暗号化	MDX暗号化と、Citrix Endpoint Managementコンソール内のMDX暗号化機能は非推奨になりました。	2019年10月	2020年9月	コンプライアンスチェック機能が追加された当社の暗号化管理機能を使用して、iOSまたはAndroidプラットフォームの暗号化を有効にします。2020年7月までにMDX暗号化からの移行をテストし、計画していることを確認してください。
ウィンドウズモバイル/CE	ウィンドウズモバイル/CEデバイスのサポー	2018年4月	2020年9月	Windows 10デスクトップおよびラップトップ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
	トは非推奨になりました。			を使用してください。
Samsung SEAMSコンテナ	Samsung SEAMSコンテナのサポートは非推奨になりました。	2020年6月	2020年8月	Android Enterpriseを使用してください。
リモートサポート	リモートサポートクライアントは非推奨になりました。	2019年1月	2020年8月	代替なし
Android 6.xおよびiOS 11.x向けCitrixモビリティアプリおよびWorkspaceアプリ	Citrix Secure Hub、Citrix Secure Mail、Citrix Secure Web、およびCitrix WorkspaceアプリのAndroid 6.xおよびiOS 11.xバージョンに対するサポートを非推奨にしました。	2020年4月	2020年6月	少なくとも、各主要オペレーティングシステムプラットフォームの現在および以前のバージョンを使用してください。古いデバイスは登録されたままですが、Citrixはレガシーデバイスのテストやサポートを行いません。
iOS向けCitrix Secure Hub ネットワーク拡張機能	iOSデバイスのネットワーク機能をカスタマイズできるネットワーク拡張フレームワークを非推奨にしました。Citrix Secure Hubリリース20.3.0。	2018年10月	2020年3月	代替なし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

項目	説明	非推奨の発表	削除済み	代替
ローカルアカウントを使用したAPIサインイン	管理者はローカルアカウントを使用してREST APIにサインインできなくなりました。	2020年10月		管理者はCitrix Cloudアカウントを使用してログインできます。(/ja-jp/citrix-endpoint-management/rest-apis.html)を参照してください。
自己署名型Secure Sockets Layer (SSL) 証明書	すべてのデバイスプラットフォームにおける自己署名型SSL証明書のサポートは非推奨になりました。	2020年5月		既存の自己署名型証明書を、信頼できる認証局 (CA) から発行された信頼済みSSL証明書に置き換えてください。
フルVPNトンネル - Android	AndroidフルVPNトンネルのサポートは非推奨になりました。	2020年3月	2021年9月	MAM SDK Web SSOモード。
VPNモード切り替えの許可 - Android	AndroidのVPNモード切り替え許可のサポートは非推奨になりました。	2020年3月	2021年9月	代替手段なし
インバウンドドキュメント交換 - Android	Androidインバウンドドキュメント交換のサポートを非推奨にしました。	2020年3月	2021年9月	代替手段なし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

システム要件

Citrix が Citrix Endpoint Management をプロビジョニングするのを待っている間に、Cloud Connector をインストールして Citrix Endpoint Management の展開に備えてください。Citrix が Citrix Endpoint Management ソリューションをホストおよび提供しますが、一部の通信とポート設定が必要です。この設定により、Citrix Endpoint Management インフラストラクチャが Active Directory などの企業サービスに接続されます。

Cloud Connector の要件

Citrix は Cloud Connector を使用して、Citrix Endpoint Management アーキテクチャを既存のインフラストラクチャに統合します。Cloud Connector は、ポート 443 を介して以下のリソースロケーションを Citrix Endpoint Management に安全に統合します: LDAP、PKI Server、内部 DNS クエリ、および Citrix Workspace 列挙。

- Active Directory ドメインに参加している専用の Windows Server マシンが少なくとも 2 台必要です。これらのマシンは仮想でも物理でも構いません。コネクタをインストールするマシンは、適切なインストールと操作のために UTC 時刻と同期している必要があります。最新の要件の完全なリストについては、Citrix アカウントチームが提供する展開資料を参照してください。

  オンボーディングウィザードは、それらのマシンに Cloud Connector をインストールする手順を案内します。
- その他のプラットフォームシステム要件については、Citrix Cloud Connector を参照してください。

サポートされている Active Directory 機能レベル

Citrix Endpoint Management で使用する場合、Citrix Cloud Connector は Active Directory の以下のフォレストおよびドメイン機能レベルをサポートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

フォレスト機能レベル	ドメイン機能レベル	サポートされているドメインコントローラー
ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2016、ウィンドウズ サーバー 2019
ウィンドウズ サーバー 2016	ウィンドウズ サーバー 2019	ウィンドウズ サーバー 2019
ウィンドウズ サーバー 2019	ウィンドウズ サーバー 2019	ウィンドウズ サーバー 2019

注記:

Windows Server 2012 R2、2012、および 2008 R2 は、ライフサイクルが終了したためサポート対象外となりました。詳細については、Microsoft 製品のライフサイクルに関するドキュメントを参照してください。

NetScaler Gateway の要件

Citrix Endpoint Management では、次のシナリオでリソースの場所に NetScaler Gateway をインストールする必要があります。

- 基幹業務アプリの内部ネットワークリソースにアクセスするには、マイクロVPNが必要です。これらのアプリはCitrix MDXテクノロジーでラップされています。マイクロVPNは、内部バックエンドインフラストラクチャに接続するためにNetScaler Gatewayを必要とします。
- Citrix Secure MailなどのCitrixモバイル生産性向上アプリを使用する予定がある場合。
- Citrix Endpoint ManagementをMicrosoft Endpoint Managerと統合する予定がある場合。

要件:

- ドメイン (LDAP) 認証
- NetScaler Gateway 12.1 以降、Platform/Universal ライセンス付き

詳細については、ライセンスを参照してください。

- パブリックSSL証明書。

詳細については、Citrix ADCアプライアンスでSSL証明書を作成して使用するを参照してください。

- NetScaler Gateway仮想サーバー用の未使用のパブリックIPアドレス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway仮想サーバー用の公開解決可能な完全修飾ドメイン名 (FQDN)
- クラウドホスト型Citrix Endpoint Management中間証明書およびルート証明書 (スクリプトバンドルで提供)
- プロキシロードバランサーIP用の未使用の内部プライベートIPアドレス
- ポート要件については、この記事の後半にあるNetScaler Gatewayのポート要件を参照してください。
- マイクロソフト エンドポイント マネージャーとのシトリックス エンドポイント マネージメント統合
- Microsoft AzureにCitrix ADC VPXインスタンスを展開する

NetScaler Gatewayの要件については、Citrixアカウントチームが提供する展開資料を参照してください。

Android Enterpriseの要件については、Android Enterpriseセクションを参照してください。

Citrix Filesの要件

Citrix Filesのファイル同期および共有サービスは、Citrix Endpoint Management Premium Serviceで利用できます。Storage zones controllerは、Citrix Filesアカウントにプライベートデータストレージを提供することで、Citrix Filesのサービスとしてのソフトウェア (SaaS) クラウドストレージを拡張します。

ストレージゾーンコントローラの要件:

- 専用の物理マシンまたは仮想マシン
- Windows Server 2012 R2 (データセンター、スタンダード、またはエッセンシャルズ)、Windows Server 2016、Windows Server 2019、または Windows Server 2022
- 2 vCPU
- 4 GB RAM
- 50 GB のハードディスク容量
- Web サーバー (IIS) のサーバーの役割:
  - アプリケーション開発: ASP. NET 4.5.2
  - セキュリティ: 基本認証
  - セキュリティ: Windows 認証

Citrix Files のプラットフォーム要件:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Files インストーラーには、Windows Server 上での管理者権限が必要です
- Citrix Files 管理者ユーザー名

ポート要件

デバイスとアプリが Citrix Endpoint Management と通信できるようにするには、ファイアウォールで特定のポートを開きます。次の図は、Citrix Endpoint Management のトラフィックフローを示しています。

Citrix Endpoint Management のトラフィックフロー(/en-us/citrix-endpoint-management/media/traffic-flow.png)

以下のセクションでは、開く必要があるポートを一覧表示します。モバイル生産性向上アプリが使用するURLについては、「機能フラグ管理」を参照してください。

NetScaler Gateway のポート要件

NetScaler Gateway を介してCitrix Secure HubおよびCitrix Workspaceからのユーザー接続を許可するために、以下のポートを開きます。

- シトリックス エンドポイント マネージメント
- StoreFront
- その他の内部ネットワークリソース（イントラネットWebサイトなど）

NetScaler Gateway の詳細については、NetScaler Gateway のドキュメントにある「Citrix Endpoint Management 環境の設定」を参照してください。IPアドレスについては、NetScaler Gateway のドキュメントにある「NetScaler Gateway がIPアドレスを使用する方法」を参照してください。

TCPポート	説明	送信元	宛先
53 (TCP および UDP)	DNS接続に使用されます。	ネットスケーラー ゲートウェイ SNIP	DNSサーバー
80/443	NetScaler Gateway は、2番目のファイアウォールを介して、マイクロVPN接続を内部ネットワークリソースに渡します。	ネットスケーラー ゲートウェイ SNIP	イントラネットWeb サイト

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCPポート	説明	送信元	宛先
123 (TCPおよびUDP)	Network Time Protocol (NTP) サービスに使用されます。	ネットスケーラーゲートウェイ SNIP	NTPサーバー
389	安全でないLDAP接続に使用されます。	NetScaler Gateway NSIP (または、ロードバランサーを使用している場合はSNIP)	LDAP認証サーバーまたはMicrosoft Active Directory
443	Citrix WorkspaceからCitrix Virtual Apps and DesktopsへのStoreFrontへの接続に使用されます。	インターネット	ネットスケーラーゲートウェイ
443	Web、モバイル、SaaSアプリの配信のためにCitrix Endpoint Managementへの接続に使用されます。	インターネット	ネットスケーラーゲートウェイ
443	Cloud Connector通信（LDAP、DNS、PKI、Citrix Workspaceの列挙）に使用されます。	クラウドコネクタサーバー	`https://*.citrixworkspacesapi.net`, `https://*.cloud.com` (commercial), `https://*.blob.core.windows.net/`, `https://*.servicebus.windows.net`
443	有効になっている場合、ブラウザを介してCitrix Endpoint Managementセルフヘルプポータルにア	アクセスポイント (ブラウザ)	シトリックス エンドポイント マネジメント (`https://`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCPポート	説明	送信元	宛先
	クセスするために使用されます。		`<sitename>/zdm/shp`)
636	安全なLDAP接続に使用されます。	NetScaler Gateway NSIP (または、ロードバランサーを使用している場合はSNIP)	LDAP認証サーバーまたはActive Directory
1494	内部ネットワーク内のWindowsベースのアプリケーションへのICA接続に使用されます。Citrixは、このポートを開放しておくことを推奨しています。	ネットスケーラーゲートウェイ SNIP	シトリックス バーチャル アプリ アンド デスクトップ
1812	RADIUS接続に使用されます。	ネットスケーラーゲートウェイ NSIP	RADIUS認証サーバー
2598	セッションの信頼性を使用して、内部ネットワーク内のWindowsベースのアプリケーションへの接続に使用されます。Citrixは、このポートを開放しておくことを推奨しています。	ネットスケーラーゲートウェイ SNIP	シトリックス バーチャル アプリ アンド デスクトップ
3269	Microsoft Global Catalog のセキュアな LDAP 接続に使用されます。	NetScaler Gateway NSIP (またはロードバランサーを使用している場合は SNIP)	LDAP 認証サーバーまたは Active Directory
4443	管理者がブラウザを介して Citrix Endpoint Management コンソールにアクセスす	アクセスポイント (ブラウザ)	シトリックス エンドポイント マネジメント

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCPポート	説明	送信元	宛先
	るために使用されます。		
8443	登録、アプリストア、およびモバイルアプリ管理 (MAM) に使用されます。	ネットスケーラー ゲートウェイ SNIP	シトリックス エンドポイント マネジメント
8443	Citrix Secure Mail 認証トークンに使用される Secure Ticket Authority (STA) ポート	ネットスケーラー ゲートウェイ SNIP	シトリックス エンドポイント マネジメント

ネットワークとファイアウォール要件

デバイスとアプリがCitrix Endpoint Managementと通信できるようにするには、ファイアウォールで特定のポートを開きます。以下の表にそれらのポートを示します。

内部ネットワークからCitrix Cloudへのポートを開く:

TCPポート	送信元IP	説明	宛先	宛先IP	
443		クラウドコネクタ	`https://*.citrixworkspacesapi.net`, `https://*.cloud.com` (commercial), `https://*.sharefile.com`, `https://cwsproduction.blob.core.windows.net/downloads`,		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCPポート	送信元IP	説明	宛先	宛先IP	
			`https://*.servicebus.windows.net`		
443		管理コンソール	`https://*.citrixworkspacesapi.net`, `https://*.cloud.com` (commercial), `https://*.citrix.com`, `https://cwsproduction.blob.core.windows.net/downloads`		
443		Citrix Endpoint Management セルフヘルプポータルへのブラウザ経由でのアクセス (ポータルが有効な場合)	シトリックス エンドポイント マネジメント		
4443		Citrix Endpoint Management コンソールへのブラウ	シトリックス エンドポイント管理		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCPポート	送信元IP	説明	宛先	宛先IP	
		ザ経由でのアクセス			

インターネットからDMZへ開放するポート:

TCPポート	説明	送信元IP	宛先	宛先IP
443	Citrix Endpoint Management クライアントデバイス		NetScaler Gateway IPアドレス	
443	Citrix Endpoint Management クライアントデバイス		ネットスケーラー ゲートウェイ VIP	
443	Citrix Files パブリックIP	CTX208318	ネットスケーラー ゲートウェイ VIP	

DMZから内部ネットワークへのポートを開く:

TCPポート	説明	送信元IP	宛先	宛先IP
389または636	ネットスケーラー ゲートウェイ NSIP		アクティブディレクトリ IP	
53 (UDP)	ネットスケーラー ゲートウェイ NSIP		DNSサーバーIP	
443	ネットスケーラー ゲートウェイ SNIP		Exchange (EAS) サーバーIP	
443	ネットスケーラー ゲートウェイ SNIP		内部Webアプリ/サービス	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCPポート	説明	送信元IP	宛先	宛先IP
443	ネットスケーラー ゲートウェイ SNIP		ストレージゾーンコントローラー IP	

内部ネットワークからDMZへのオープンポート:

TCPポート	説明	送信元IP	宛先	宛先IP
443	管理クライアント		ネットスケーラー ゲートウェイ NSIP	

内部ネットワークからインターネットへのポートを開く:

TCPポート	説明	送信元IP	宛先	宛先IP
443	Exchange (EAS) サーバー IP		Citrix Endpoint Management プッシュ通知リスナー (1)	
443	ストレージゾーンコントローラー IP		Citrix Files コントロールプレーン	CTX208318

`(1) us-east-1.mailboxlistener.xm.citrix.com, eu-west-1.mailboxlistener.xm.citrix.com, ap-southeast-1.mailboxlistener.xm.citrix.com`

社内Wi-Fiからインターネットへのポートを開放します。

TCPポート	説明	送信元IP	宛先	宛先IP
8443 / 443	Citrix Endpoint Management クライアントデバイス		シトリックス エンドポイント マネジメント	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCPポート	説明	送信元IP	宛先	宛先IP
5223	Citrix Endpoint Management クライアントデバイス		Apple APNS サーバー	`17.0.0.0/8`
5228	Citrix Endpoint Management クライアントデバイス		Firebase クラウド メッセージング	`android.apis.google.com`, `fcm.googleapis.com`
5229	Citrix Endpoint Management クライアントデバイス		ファイアベース クラウド メッセージング	`android.apis.google.com`, `fcm.googleapis.com`
5230	Citrix Endpoint Management クライアントデバイス		ファイアベース クラウド メッセージング	`android.apis.google.com`, `fcm.googleapis.com`
443	Citrix Endpoint Management クライアントデバイス		ファイアベース クラウド メッセージング	`fcm.googleapis.com`
443	Citrix Endpoint Management クライアントデバイス		Windows プッシュ通知サービス	`*.notify.windows.com`
443 / 80	Citrix Endpoint Management クライアントデバイス		アップル iTunes App Store	`ax.apps.apple.com`, `*.mzstatic.com`, `vpp.itunes.apple.com`
443 / 80	Citrix Endpoint Management ク		グーグル プレイ	`play.google.com`, `android.clients.google.com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCPポート	説明	送信元IP	宛先	宛先IP
	ライアントデバイス			`, android.l.google.com, android.com, google-analytics.com`
443 / 80	Citrix Endpoint Management クライアントデバイス		マイクロソフト アプリ ストア	`login.live.com, *.notify.windows.com`
443	Citrix Endpoint Management クライアントデバイス		iOSおよびAndroid用Citrix Endpoint Management AutoDiscovery サービス	`discovery.cem.cloud.us`
443	Citrix Endpoint Management クライアントデバイス		Windows 用 シトリックス エンドポイント マネジメント オートディスカバリー サービス	`enterpriseenrollment.mycompany.com`, `discovery.cem.cloud.us`
443	ストレージゾーンコントローラーIP		Citrix Filesコントロールプレーン	CTX208318
443	Citrix Endpoint Managementクライアントデバイス		グーグル モバイル管理、グーグル API、グーグル Play ストア API	`*.googleapis.com`
443	Citrix Endpoint Managementクライアントデバイス		v470より前のCloudDPCバージョンの接続チェック。N	`connectivitycheck.android.com,`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCPポート	説明	送信元IP	宛先	宛先IP
			MR1以降のAndroid接続チェックでは、`https://www.google.com/generate_204`に到達可能であるか、指定されたWi-Fiネットワークが到達可能なPACファイルを指している必要があります)	`www.google.com`

AutoDiscoveryサービス接続のポート要件

このポート構成により、Citrix Secure Hub for Androidから接続するAndroidデバイスが、内部ネットワーク内からCitrix Endpoint Management AutoDiscoveryサービス (ADS) にアクセスできるようになります。ADSを介して利用可能になるセキュリティ更新プログラムをダウンロードする際には、ADSへのアクセス機能が重要です。

注:

ADS接続はプロキシサーバーをサポートしない場合があります。このような場合は、ADS接続がプロキシサーバーをバイパスできるようにします。

証明書ピン留めを有効にする場合は、次の前提条件を完了してください。

- **Citrix Endpoint ManagementサーバーおよびNetScaler Gateway証明書を収集する:** 証明書はPEM形式であり、公開証明書である必要があり、秘密鍵であってはなりません。
- **Citrixサポートに連絡し、証明書ピン留めを有効にするようリクエストする:** このプロセス中に、証明書の提出を求められます。

証明書ピン留めでは、デバイスが登録される前にADSに接続する必要があります。この要件により、最新のセキュリティ情報がCitrix Secure Hubで利用可能になります。Citrix Secure Hubがデバ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イスを登録するには、デバイスがADSに到達できる必要があります。したがって、内部ネットワーク内でADSアクセスを開放することは、デバイスの登録を可能にする上で非常に重要です。

Android/iOS版Citrix Secure HubがADSにアクセスできるようにするには、次のFQDNに対してポート443を開放してください。

FQDN	ポート	IPおよびポートの使用状況
`discovery.cem.cloud.us`	443	Citrix Secure Hub - CloudFront経由のADS通信

サポートされているIPアドレスについては、AWSのクラウドベースストレージセンターを参照してください。

Android Enterpriseのネットワーク要件

Android Enterpriseのネットワーク環境をセットアップする際に考慮すべきアウトバウンド接続については、Googleサポート記事のAndroid Enterprise Network Requirementsを参照してください。

アプリの要件

Citrix Endpoint Management は、最大300個のアプリの追加および維持をサポートしています。この制限を超えると、システムが不安定になります。

シトリックス エンドポイント マネジメントの互換性

新機能、修正、およびポリシーの更新を利用するには、Citrix® は以下の最新バージョンをインストールすることを推奨します。

- Citrix は、MDX 機能性をアプリに適用するために、エンタープライズ向け iOS および Android アプリに Mobile Application Management (MAM) SDK を統合することを推奨します。

  MDX Toolkit は 2023 年 7 月に EOL に達する予定です。エンタープライズアプリの管理を継続するには、MAM SDK を組み込む必要があります。
- モバイル生産性向上アプリ

この記事では、統合できるサポート対象の Citrix Endpoint Management コンポーネントのバージョンを要約しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Hub、MDX Toolkit、およびモバイル生産性向上アプリの最新バージョンは、Citrix Endpoint Management の最新バージョンと、その前の 2 つのバージョンと互換性があります。

モバイル生産性向上アプリ

ユーザーは公開アプリストアからモバイル生産性向上アプリにアクセスします。モバイル生産性向上アプリの最新バージョンには、Citrix Secure Hub の最新バージョンが必要です。アプリの以前の 2 つのバージョンは、最新の Citrix Secure Hub と互換性があります。

モバイル生産性向上アプリの 2 週間ごとの段階的リリースサイクルについては、「リリーススケジュール」を参照してください。サポートの詳細については、「モバイル生産性向上アプリのサポート」を参照してください。

MAM SDK

MAM SDK は、iOS および Android プラットフォームではカバーされていない MDX 機能を提供します。これらのアプリは、社内ストアまたは公開アプリストアで利用可能にできます。「MDX App SDK」を参照してください。

MDXツールキット

MDX Toolkit は 2023 年 7 月に EOL に達する予定です。エンタープライズアプリケーションの管理を継続するには、MAM SDK を組み込む必要があります。

Citrix は、MDX Toolkit の最新の 3 つのリリース (n.n.n) をサポートしています。「MDX Toolkit の新機能」を参照してください。

ブラウザのサポート

Citrix Endpoint Management コンソールには、次のいずれかのサポートされているWebブラウザが必要です。

- Google Chrome の最新バージョン
- Mozilla Firefox の最新バージョン
- Microsoft Edge の最新バージョン
- Apple Safari の最新バージョン

サポートされているデバイスオペレーティングシステム

この記事では、Citrix Endpoint Management を使用したエンタープライズモビリティ管理でサポートされているデバイスについて説明します。プラットフォームの制限とセキュリティ機能のため、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management はすべてのプラットフォームですべての機能をサポートしているわけではありません。

モバイル生産性向上アプリの最新バージョンについては、「モバイル生産性向上アプリのサポート」を参照してください。

注:

- Citrix は、各主要オペレーティングシステムプラットフォームの現在および以前のバージョンをサポートしています。一部の Citrix Endpoint Management 機能は、古いプラットフォームバージョンでは動作しません。廃止のお知らせについては、「廃止」を参照してください。
- Citrix Endpoint Management™ は、Windows x86 および ARM タイプデバイスのデバイス管理をサポートしています。

オペレーティングシステムのサポートリスト

Citrix Endpoint Management は、次のオペレーティングシステムをサポートしています。

- **アンドロイド:** 10.x、11.x、12.x、13.x、14.x、15.x、16.x、17.x

  Citrix® は、Android Enterprise を使用する前に Android 10 以降にアップグレードすることをお勧めします。詳細については、「Android の考慮事項」を参照してください。

- **アイオーエス:** 13.x、14.x、15.x、16.x、17.x、18.x、26.x、27.x

  Citrix Endpoint Management および Citrix モバイルアプリは、現在、iOS 14.x、iOS 15.x、iOS 16.x、iOS 17.x、iOS 18.x、iOS 26.x、および iOS 27.x で利用可能なすべての新機能をサポートしていません。

- **アイパッドオーエス:** 13.x、14.x、15.x、16.x、17.x、18.x、26.x、27.x

  Citrix Endpoint Management および Citrix モバイルアプリは、現在、iPadOS 14.x、iPadOS 15.x、iPadOS 16.x、iPadOS 17.x、iPadOS 18.x、iPadOS 26.x、および iPadOS 27.x のすべての新機能をサポートしていません。

- **マックオーエス:** 11.x、12.x、13.x、14.x、15x

  Citrix Endpoint ManagementおよびCitrixモバイル生産性向上アプリは、現在、macOS 11、macOS 12、macOS 13、macOS 14、およびmacOS 15で利用可能なすべての新機能をサポートしていません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Windows 10およびWindows 11デスクトップおよびタブレット:** (MDMのみ)
  - Windows 10 プロフェッショナル および Windows 11 プロフェッショナル
  - Windows 10 エンタープライズ および Windows 11 エンタープライズ
  - Windows 10 エデュケーション および Windows 11 エデュケーション
  - Windows IoT エンタープライズ

  特定のオペレーティングシステムのサポートレベルについては、Microsoftのドキュメントを参照してください。

Androidに関する考慮事項

Android 10以降にアップグレードする前に: Google Device Administration APIの非推奨化がAndroid 10以降を実行しているデバイスに与える影響については、Migrate from device administration to Android Enterpriseを参照してください。また、このCitrix blogも参照してください。

- GoogleはDevice Administration APIを非推奨化しました。これはAndroid 10以降を実行しているデバイスに影響を与えます。レガシーのデバイス管理モードでのAndroid 10以降のデバイスの登録は失敗します。Citrixは、デバイス管理モードでのAndroidデバイスの登録をサポートしていません。
- CitrixはAndroidデバイスにAndroid Enterpriseを使用することを推奨しています。詳細については、Migrate from device administration to Android Enterpriseを参照してください。
- Google APIの変更は、MAM専用モードで登録されたデバイスには影響しません。
- このCitrix blogも参照してください。

アップグレードする前に:

- サーバーインフラストラクチャが、subjectAltName (SAN) 拡張機能に一致するホスト名を持つセキュリティ証明書に準拠していることを確認してください。
- ホスト名を検証するには、サーバーは、一致するSANを持つ証明書を提示する必要があります。Citrixは、ホスト名と一致するSANを持つ証明書のみを信頼します。

言語サポート

Citrixモバイル生産性向上アプリとCitrix Endpoint Managementコンソールは、英語以外の言語での使用に対応しています。このサポートには、アプリがユーザーの優先言語にローカライズされていない場合でも、英語以外の文字とキーボード入力が含まれます。すべてのCitrix製品のグローバ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ル化サポートの詳細については、`<https://support.citrix.com/article/CTX119253>`を参照してください。

この記事では、Citrix Endpoint Managementの最新バージョンでサポートされている言語を一覧表示します。

Citrix Endpoint Managementコンソールとセルフヘルプポータル

- フランス語
- ドイツ語
- スペイン語
- 日本語
- 韓国語
- ポルトガル語
- 簡体字中国語

Citrixモバイル生産性向上アプリ

Xは、その特定の言語でアプリが利用可能であることを示します。

iOSおよびAndroid

言語	セキュアハブ	セキュアメール	セキュアウェブ	セキュアノート	セキュアタスク	QUICKED IT
日本語	X	X	X	X	X	X
簡体字中国語	X	X	X	X	X	X
繁体字中国語	X	X	X	X	X	X
フランス語	X	X	X	X	X	X
ドイツ語	X	X	X	X	X	X
スペイン語	X	X	X	X	X	X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

言語	セキュアハブ	セキュアメール	セキュアウェブ	セキュアノート	セキュアタスク	QUICKED IT
韓国語	X	X	X	X	X	X
ポルトガル語	X	X	X	X	X	X
オランダ語	X	X	X	X	X	X
イタリア語	X	X	X	X	X	X
デンマーク語	X	X	X	X	X	X
スウェーデン語	X	X	X	X	X	X
ヘブライ語	X	X	X	X	X	iOSのみ
アラビア語	X	X	X	X	X	X
ロシア語	X	X	X	X	X	X
トルコ語	X	X	Androidのみ	-	-	-
ポーランド語	X	X	X	-	-	-

右から左への言語サポート

次の表は、各アプリにおける中東言語のテキストのサポートをまとめたものです。「X」は、そのプラットフォームで機能が利用可能であることを示します。Windowsデバイスでは、右から左への言語サポートは利用できません。

アプリ	IOS	アンドロイド
シトリックス セキュア ハブ	X	X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ	IOS	アンドロイド
シトリックス セキュア メール	X	X
シトリックス セキュア ウェブ	X	X
QuickEdit	X	X

FIPS 140-2 準拠

米国国立標準技術研究所 (NIST) は、連邦情報処理標準 (FIPS) を発行しています。FIPS は、セキュリティシステムで使用される暗号モジュールのセキュリティ要件を規定しています。FIPS 140-2 は、この標準の第2版です。NIST 検証済み FIPS 140 モジュールの詳細については、NIST Computer Security Resource Center を参照してください。

iOS 上のすべての保存データおよび転送データの暗号化操作は、FIPS 検証済み暗号モジュールを使用します。Android では、すべての保存データの暗号化操作は、Citrix® が提供する FIPS 検証済み暗号モジュール、またはデバイスメーカーが提供するプラットフォームの暗号モジュールを使用します。デバイスメーカーのモジュールの詳細については、Citrix 担当者にお問い合わせください。

サポートされている Windows デバイス上のモバイルデバイス管理 (MDM) のすべての保存データおよび転送データの暗号化操作は、FIPS 検証済み暗号モジュールを使用します。

Citrix Endpoint Management MDM のすべての保存データおよび転送データの暗号化操作は、FIPS 検証済み暗号モジュールを使用します。MDM フローのすべての保存データおよび転送データは、エンドツーエンドで FIPS 準拠の暗号モジュールを使用します。このセキュリティには、モバイルデバイスについて前述した暗号化操作に加え、モバイルデバイスと NetScaler Gateway 間の暗号化操作が含まれます。

MDX Vault は、iOS および Android デバイス上の MDX でラップされたアプリと関連する保存データを、FIPS 検証済み暗号モジュールを使用して暗号化します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント マネジメント について

Citrix Endpoint Management は、すべてのアプリとエンドポイントを統合された単一のビューにまとめ、セキュリティを強化し、生産性を向上させる Unified Endpoint Management (UEM) ソリューションです。UEM の概要については、Citrix Tech Zone の技術概要「Citrix Endpoint Management」を参照してください。

Citrix Endpoint Management は、モバイルデバイス管理 (MDM) とモバイルアプリケーション管理 (MAM) を提供します。

Citrix Endpoint Management の MDM 機能を使用すると、次のことができます。

- デバイスポリシーとアプリを展開する。
- 資産インベントリを取得する。
- デバイスのワイプなど、デバイスに対するアクションを実行する。

Citrix Endpoint Management の MAM 機能を使用すると、次のことができます。

- BYO モバイルデバイス上のアプリとデータを保護する。
- エンタープライズモバイルアプリを配信する。
- アプリをロックし、そのデータをワイプする。

MDM と MAM の機能を組み合わせることで、次のことができます。

- MDM を使用して企業支給デバイスを管理する
- デバイスポリシーとアプリを展開する
- 資産インベントリを取得する
- デバイスをワイプする
- エンタープライズモバイルアプリを配信する
- アプリをロックし、デバイス上のデータをワイプする

次の表は、MDM、MAM、またはMDM+MAMでサポートされるCitrix Endpoint Managementの機能の概要を示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能 (プラットフォーム別)	MDM (1)	MAM (2)	MDM+MAM
アンドロイド エンタープライズ:			
デバイス登録のサポート	はい	はい	はい
ドメイン認証のサポート	はい	なし	あり
ドメインとセキュリティトークン認証のサポート	なし	なし	あり
クライアント証明書認証のサポート	なし	あり	あり
クライアント証明書とドメイン認証のサポート	なし	なし	あり
クライアント証明書とセキュリティトークンのサポート	いいえ	いいえ	はい
Azure AD IDプロバイダーのサポート	はい	いいえ	はい
Okta IDプロバイダーのサポート	はい	いいえ	はい
ネイティブSaaSアプリへのシングルサインオン	はい	いいえ	はい
Citrix Content Delivery Networkのエンタープライズアプリ向けサポート	はい	はい	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能 (プラットフォーム別)	MDM (1)	MAM (2)	MDM+MAM
Citrix Content Delivery NetworkのMDXアプリ向けサポート	はい	はい	はい
専用のAndroid Enterprise (COSU) デバイスをプロビジョニングすることによる共有デバイスのサポート	はい	いいえ	はい
Android (レガシー):			
デバイス登録のサポート	はい	はい	はい
ドメインまたはドメインとセキュリティトークン認証のサポート	いいえ	いいえ	はい
クライアント証明書認証のサポート	いいえ	はい	はい
クライアント証明書とドメイン認証のサポート	いいえ	いいえ	はい
クライアント証明書とセキュリティトークンのサポート	いいえ	いいえ	はい
Azure ADおよびCitrix IDプロバイダーのサポート	はい	いいえ	はい
Okta IDプロバイダーのサポート	はい	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能 (プラットフォーム別)	MDM (1)	MAM (2)	MDM+MAM
ネイティブSaaSアプリへのシングルサインオン	はい	いいえ	はい
エンタープライズアプリ向けCitrix Content Delivery Networkサポート	はい	はい	はい
MDXアプリ向けCitrix Content Delivery Networkサポート	はい	はい	はい
クローム:			
デバイス登録サポート	はい	いいえ	はい
ユーザー名とパスワード認証のサポート	はい	不可	可能
iOS:			
デバイス登録のサポート	可能	可能	可能
ドメインまたはドメインとセキュリティトークン認証のサポート	不可	不可	可能
クライアント証明書認証のサポート	不可	可能	可能
クライアント証明書とドメイン認証のサポート	いいえ	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能 (プラットフォーム別)	MDM (1)	MAM (2)	MDM+MAM
Azure ADとCitrix IDプロバイダーのサポート	はい	いいえ	はい
Okta IDプロバイダーのサポート	はい	いいえ	はい
ネイティブSaaSアプリへのシングルサインオン	はい	いいえ	はい
エンタープライズアプリ向けCitrix Content Delivery Networkサポート	はい	はい	はい
MDXアプリ向けCitrix Content Delivery Networkサポート	はい	はい	はい
Apple Educationとの統合	はい	いいえ	はい
macOS:			
デバイス登録のサポート	はい	いいえ	いいえ
ドメインまたはドメインとワンタイムパスワードのサポート	はい	いいえ	いいえ
招待URLとワンタイムパスワードのサポート	はい	いいえ	いいえ
ウィンドウズ:			

© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能 (プラットフォーム別)	MDM (1)	MAM (2)	MDM+MAM
デバイス登録のサポート	はい	いいえ	いいえ
Citrix Workspaceアプリを介したWindows 10およびWindows 11デバイスの自動登録	はい	いいえ	いいえ
ドメインまたはドメインとセキュリティトークン認証のサポート	はい	いいえ	いいえ
クライアント証明書認証のサポート	はい	いいえ	いいえ
クライアント証明書とドメイン認証のサポート	はい	いいえ	いいえ
Azure ADまたはCitrix IDプロバイダーを介したフェデレーション認証	はい	いいえ	いいえ
エンタープライズアプリ向けCitrix Content Delivery Networkサポート	はい	いいえ	いいえ
ワークスペース環境管理™ 統合 (3)	はい	いいえ	いいえ

注記:

(1) 展開順序は、MDM 用に構成された登録プロファイルを持つデリバリーグループ内のデバイスにのみ適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

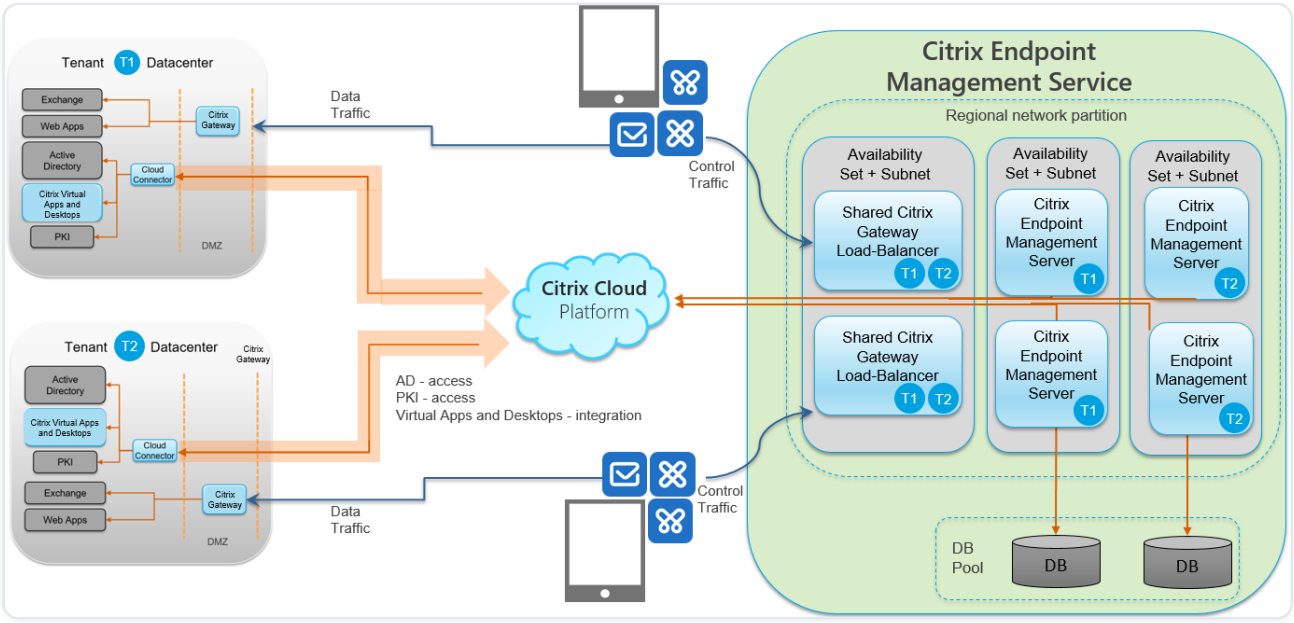
(2) MAM の登録には NetScaler Gateway が必要です。
(3) Workspace Environment Management (WEM) の統合により、幅広い Windows オペレーティングシステムで MDM 機能にアクセスできます。
詳細については、「管理モード」を参照してください。

アーキテクチャ

組織のデバイスおよびアプリ管理要件によって、Citrix Endpoint Management アーキテクチャ内の Citrix Endpoint Management コンポーネントが決まります。Citrix Endpoint Management のコンポーネントはモジュール式であり、相互に連携します。たとえば、展開には NetScaler Gateway が含まれます。

- NetScaler Gateway は、ユーザーにモバイルアプリへのリモートアクセスを提供し、ユーザーデバイスの種類を追跡します。
- Citrix Endpoint Management は、それらのアプリとデバイスを管理する場所です。

次の図は、Citrix Endpoint Management クラウド展開の一般的なアーキテクチャの概要と、データセンターとの統合を示しています。



以下のサブセクションには、次のリファレンスアーキテクチャ図があります。

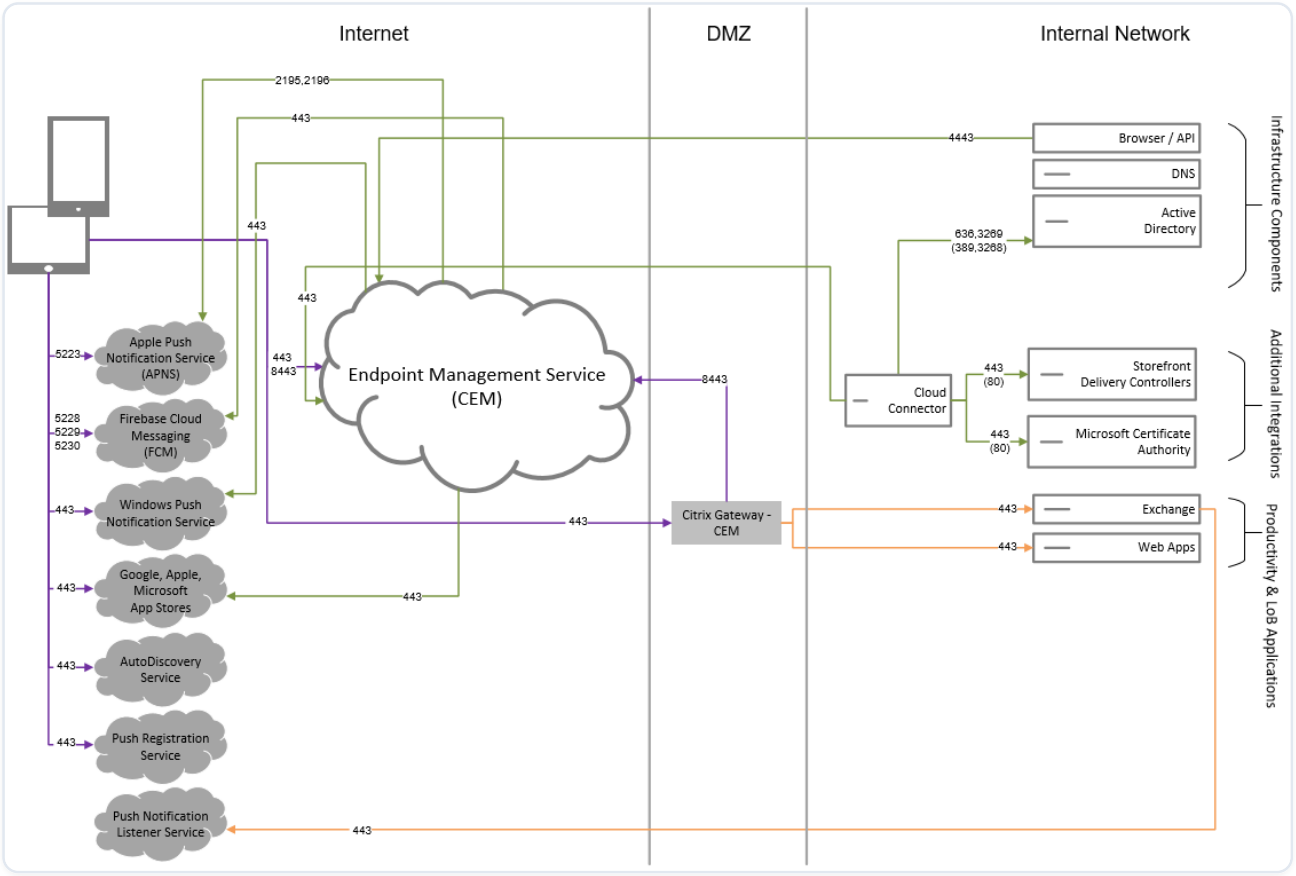
- シトリックス エンドポイント マネジメント
- 外部証明機関、Exchange ActiveSync 用 Citrix Endpoint Management コネクタ、Citrix Endpoint Management MDM+MAM および Intune MAM トラフィックフローなどのオプションコンポーネント。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix ADC および NetScaler Gateway の要件の詳細については、`<https://docs.citrix.com/>` の Citrix 製品ドキュメントを参照してください。

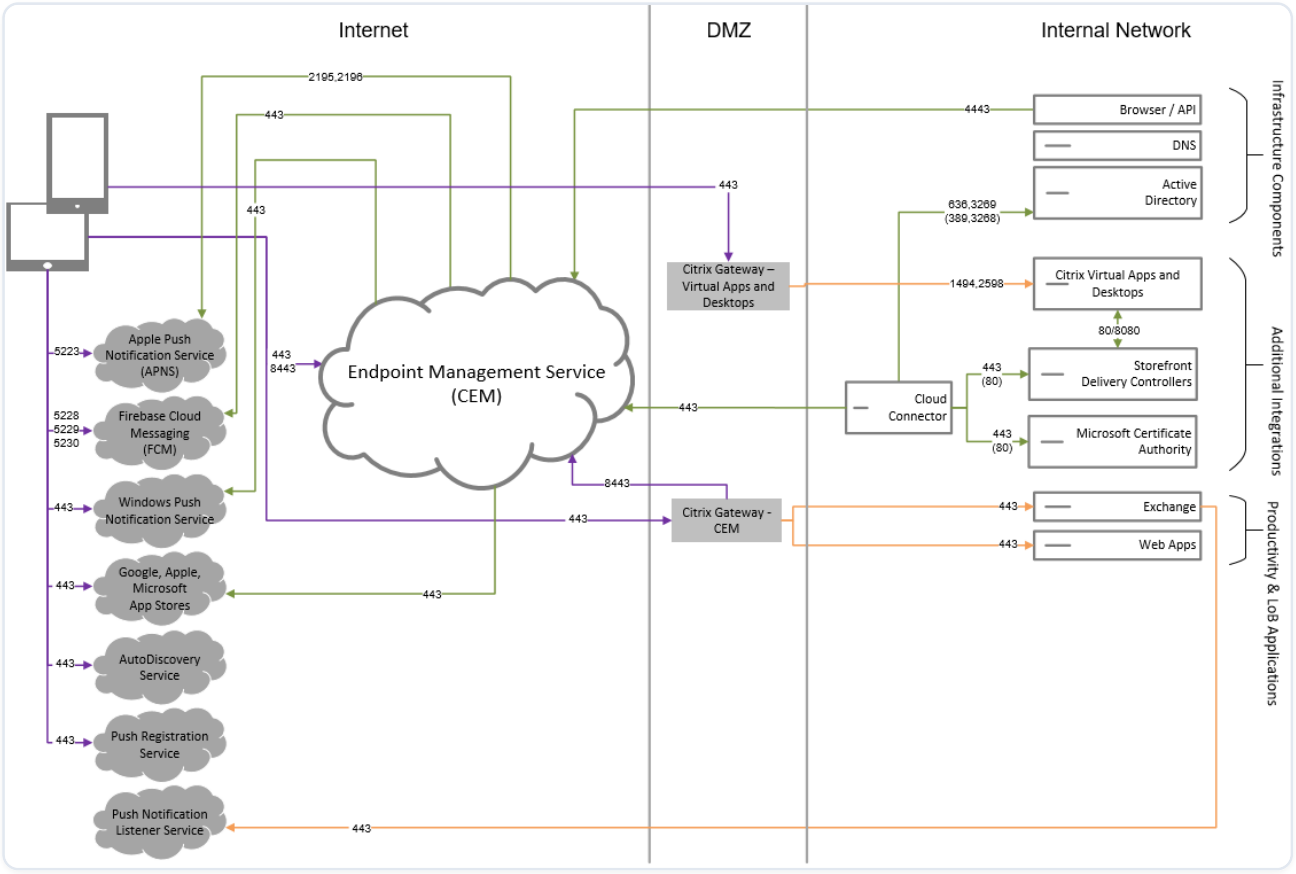
コアリファレンスアーキテクチャ

ポート要件の詳細については、「システム要件」を参照してください。



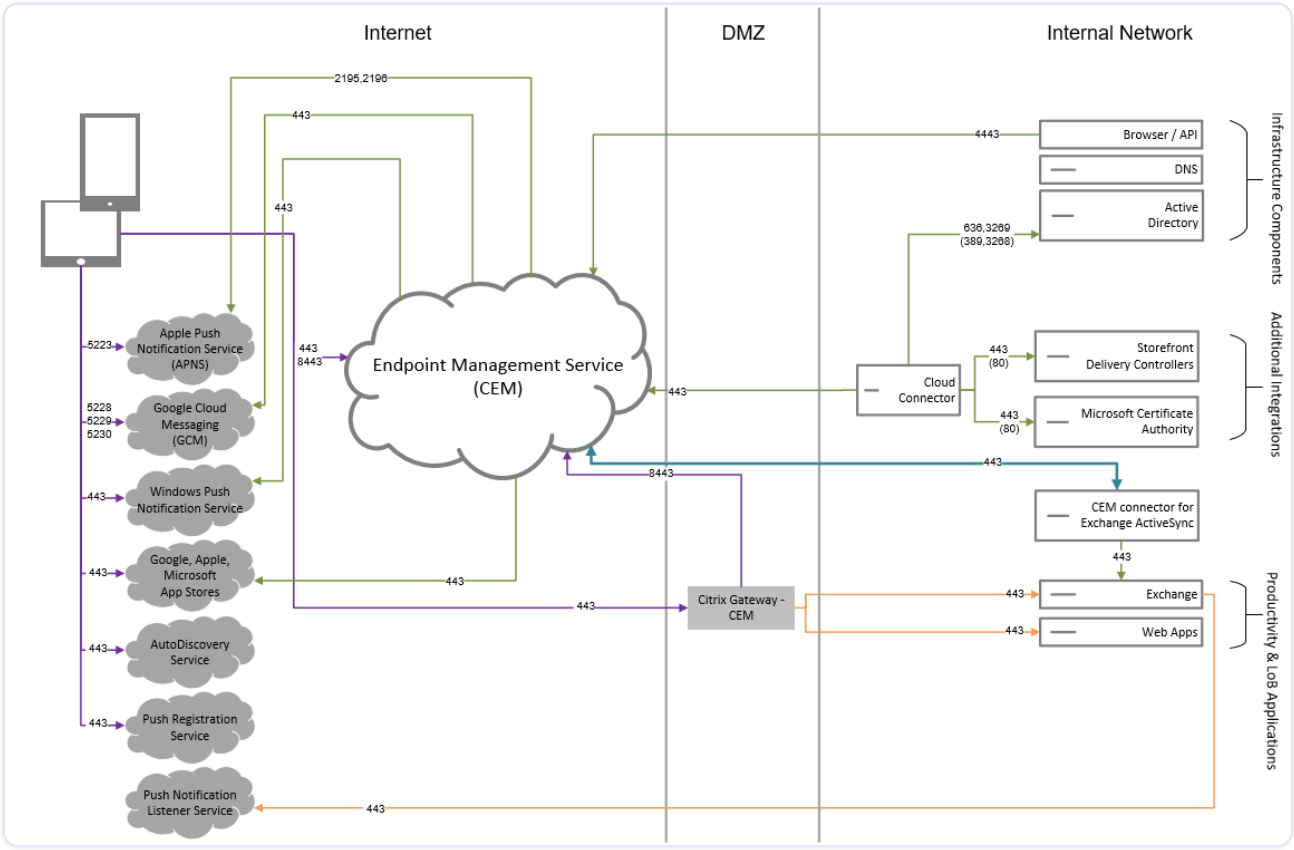
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Virtual Apps and Desktops™ を使用したリファレンスアーキテクチャ



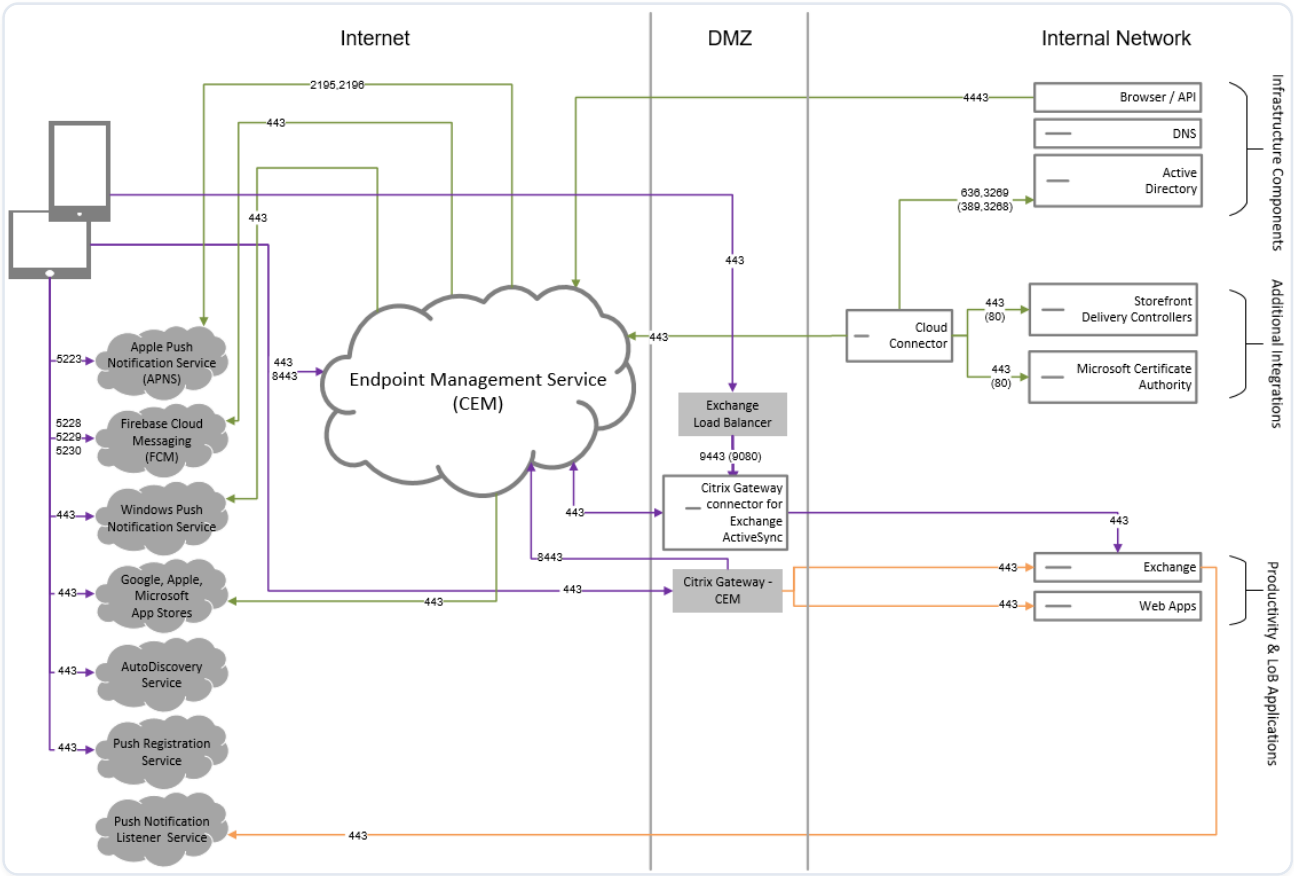
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exchange ActiveSync 用 Citrix Endpoint Management コネクタを使用したリファレンスアーキテクチャ

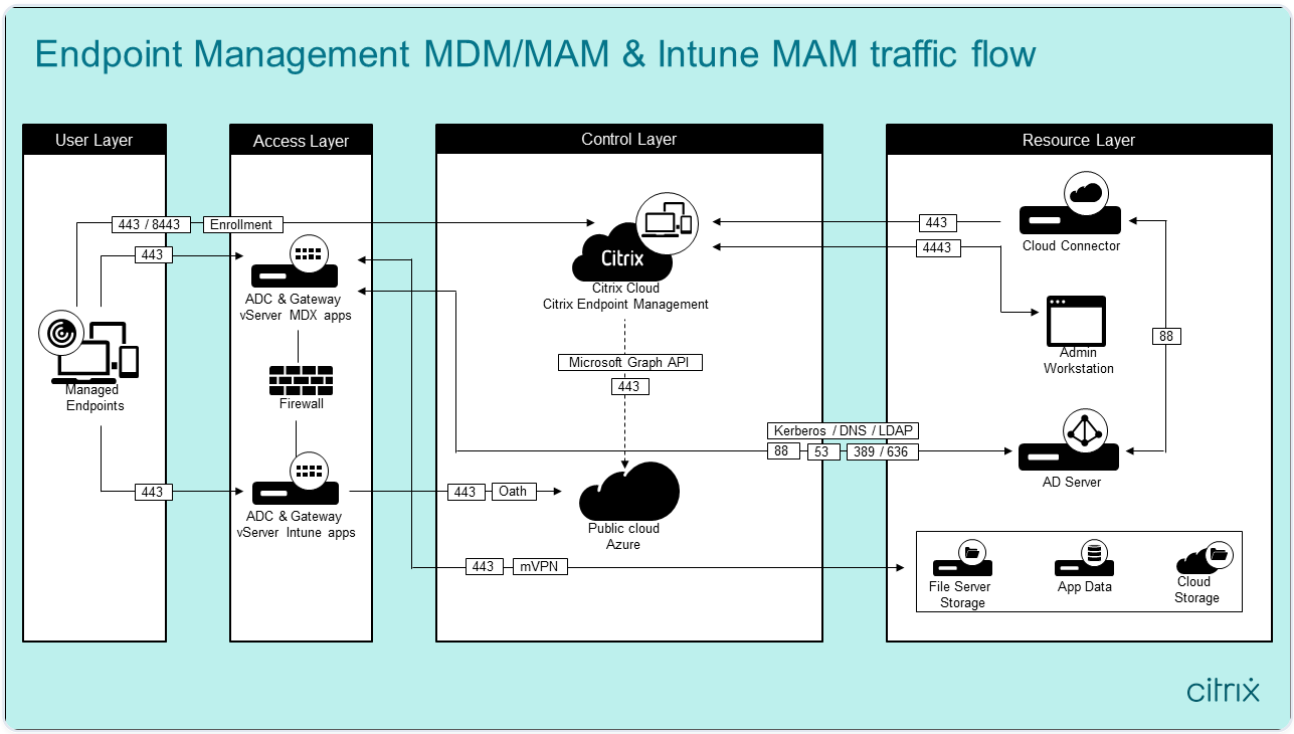


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exchange ActiveSync 用 NetScaler Gateway コネクタを使用したリファレンスアーキテクチャ



Citrix Endpoint Management MDM+MAM および Intune MAM を使用したリファレンスアーキテクチャ



© 1997–2026 Citrix Systems, Inc. All rights reserved.

リソースの場所

リソースの場所は、ビジネスニーズに最も適した場所に配置します。たとえば、パブリッククラウド、支社、プライベートクラウド、データセンターなどです。場所の選択を決定する要因には、次のものがあります。

- サブスクライバーへの近接性
- データへの近接性
- スケール要件
- セキュリティ属性

任意の数のリソースの場所を構築できます。たとえば、次のようにします。

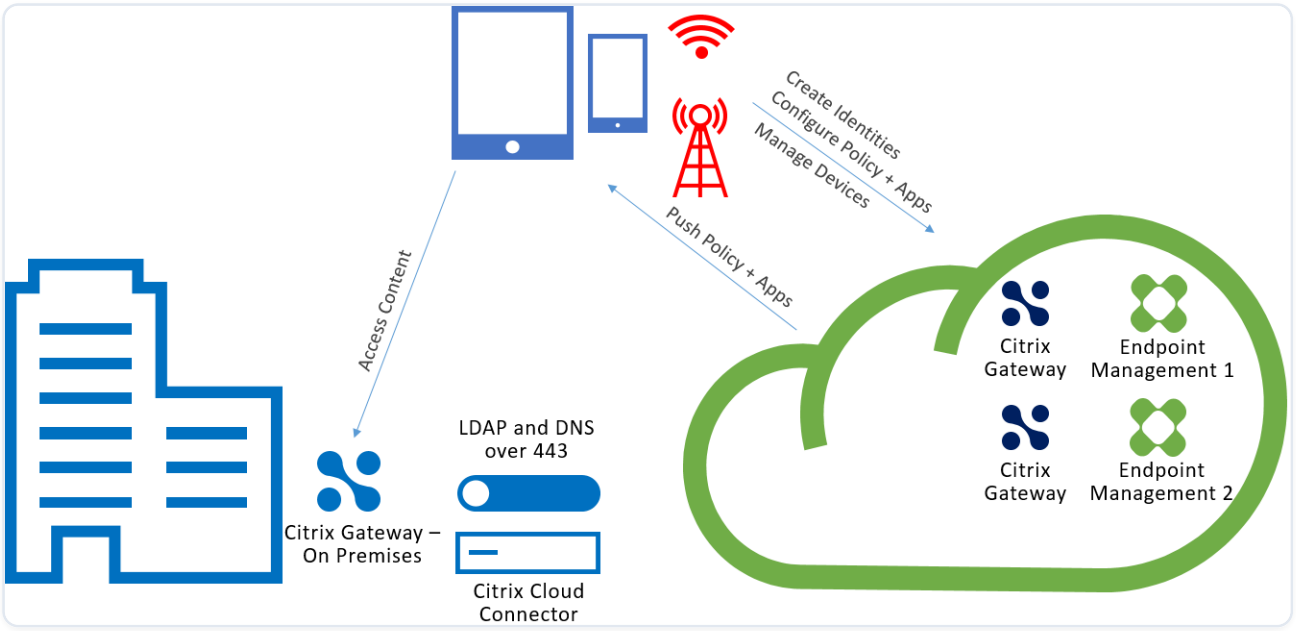
- データへの近接性を必要とするサブスクライバーとアプリケーションに基づいて、本社用のリソースの場所をデータセンターに構築します。
- グローバルユーザー用にパブリッククラウドに個別のリソースの場所を追加します。または、支社の従業員に近い場所で最適に提供されるアプリケーションを提供するために、支社に個別のリソースの場所を構築します。
- 制限付きアプリケーションを提供する別のネットワークに、さらにリソースの場所を追加します。この設定により、他のリソースの場所を調整することなく、他のリソースやサブスクライバーへの可視性を制限できます。

クラウドコネクタ

Cloud Connector は、Citrix Cloud とリソースの場所間のすべての通信を認証および暗号化します。Cloud Connector は、LDAP、IdP、PKI サーバー、内部 DNS クエリ、Citrix Virtual Apps、NetScaler Gateway、Citrix Workspace、Microsoft Endpoint Manager などのサービスにアクセスするために必要です。

次の図は、Cloud Connector のトラフィックフローを示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Cloud Connector は Citrix Cloud への接続を確立します。Cloud Connector は受信接続を受け入れません。

Cloud Connector は、デバイス登録中のみ負荷がかかります。詳細については、「Cloud Connector のスケーリングとサイズ設定に関する考慮事項」を参照してください。

Mobile App Management (MAM) を含むソリューションには、オンプレミスの NetScaler Gateway によって提供されるマイクロ VPN が必要です。このシナリオでは、次のようになります。

- 次のコンポーネントがデータセンターにあります。
  - クラウドコネクタ
  - ネットスケーラー ゲートウェイ
  - Exchange、Webアプリ、Active Directory、PKI用のサーバー
- モバイルデバイスは、Citrix Endpoint ManagementおよびオンプレミスのNetScaler Gatewayと通信します。

Citrix Endpoint Managementコンポーネント

Citrix Endpoint Managementコンソール。 Citrix Endpoint Management管理者コンソールを使用して、Citrix Endpoint Managementを構成します。Citrix Endpoint Managementコンソールの使用方法の詳細については、Citrix Endpoint Managementの各記事を参照してください。Citrix Endpoint Managementの「新機能」記事が新しいリリース向けに更新されると、Citrixから通知されます。

Citrix Endpoint Managementサービスとオンプレミスリリースとの間の以下の違いに注意してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Remote SupportクライアントはCitrix Endpoint Managementでは利用できません。
- Citrixは、オンプレミスのsyslogサーバーとのCitrix Endpoint Managementにおけるsyslog統合をサポートしていません。代わりに、Citrix Endpoint Managementコンソールの**トラブルシューティングとサポート**ページからログをダウンロードできます。その際、**すべてダウンロード**をクリックする必要があります。

MAM SDK。 MDX Toolkitは2023年7月にEOLに達する予定です。エンタープライズアプリケーションの管理を継続するには、MAM SDKを組み込む必要があります。

- Mobile Application Management（MAM）SDKは、iOSおよびAndroidプラットフォームではカバーされていないMDX機能を提供します。iOSまたはAndroidアプリをMDX対応にして保護できます。これらのアプリは、社内ストアまたは公開アプリストアで利用可能にできます。MDX App SDKを参照してください。

モバイル生産性向上アプリ。 Citrixが開発したモバイル生産性向上アプリは、Citrix Endpoint Management環境内で生産性およびコミュニケーションツールのスイートを提供します。これらのアプリは、会社のポリシーによって保護されます。詳しくは、モバイル生産性向上アプリを参照してください。

Exchange ActiveSync用Citrix Endpoint Managementコネクタ。 Exchange ActiveSync用Citrix Endpoint Managementコネクタは、ネイティブのモバイルメールアプリを使用するユーザーに安全なメールアクセスを提供します。Exchange ActiveSync用コネクタは、Exchangeサービスレベルで ActiveSyncフィルタリングを提供します。その結果、フィルタリングは、メールがCitrix Endpoint Management環境に入る前ではなく、Exchangeサービスに到達した後にのみ行われます。このコネクタは、NetScaler Gatewayの使用を必要としません。既存のActiveSyncトラフィックのルーティングを変更することなく、コネクタを展開できます。詳しくは、Exchange ActiveSync用Citrix Endpoint Managementコネクタを参照してください。

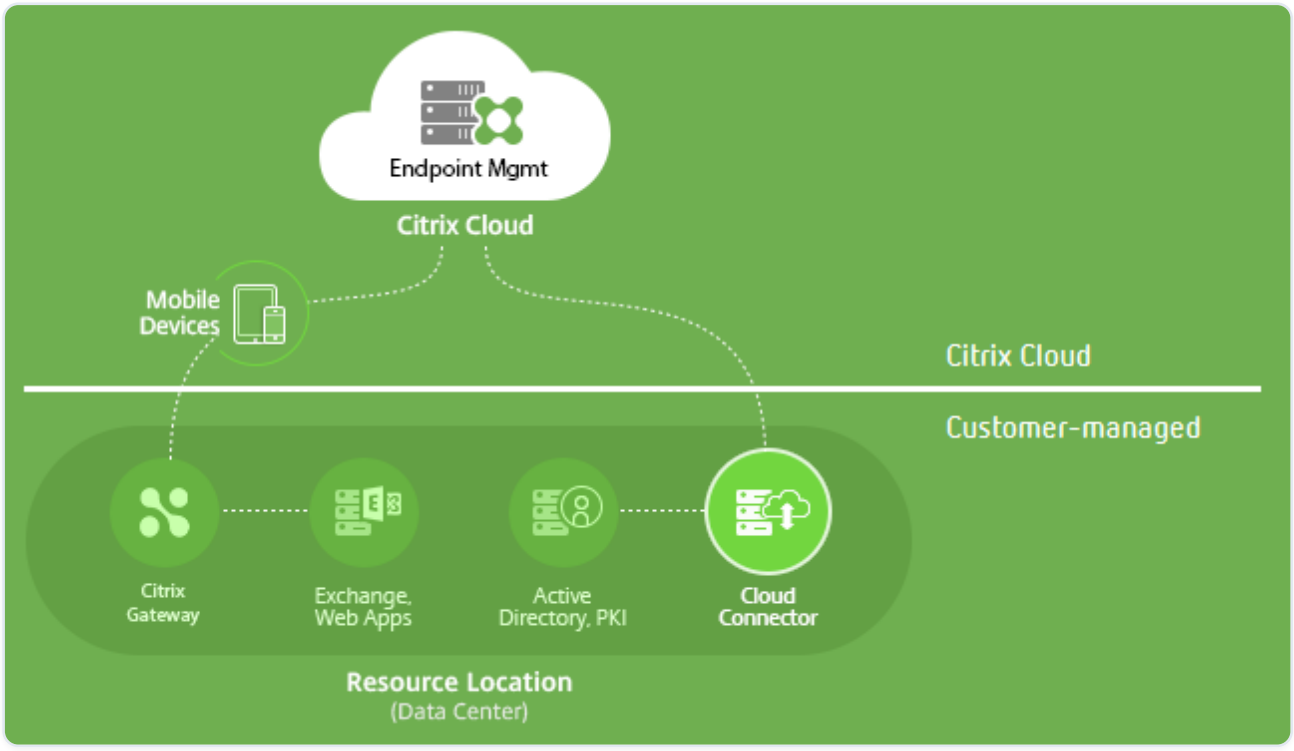
Exchange ActiveSync用NetScaler Gatewayコネクタ。 Exchange ActiveSync用NetScaler Gatewayコネクタは、ネイティブのモバイルメールアプリを使用するユーザーに安全なメールアクセスを提供します。Exchange ActiveSync用コネクタは、境界でActiveSyncフィルタリングを提供します。フィルタリングは、NetScaler GatewayをActiveSyncトラフィックのプロキシとして使用します。その結果、フィルタリングコンポーネントはメールトラフィックフローのパスに位置し、環境に出入りするメールを傍受します。Exchange ActiveSync用コネクタは、NetScaler GatewayとCitrix Endpoint Management間の仲介役として機能します。詳しくは、Exchange ActiveSync用NetScaler Gatewayコネクタを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementの技術的なセキュリティ概要

Citrix Cloudは、Citrix Endpoint Management環境のコントロールプレーンを管理します。コントロールプレーンには、Citrix Endpoint Managementサーバー、Citrix ADCロードバランサー、およびシングルテナントデータベースが含まれます。クラウドサービスは、Citrix Cloud Connectorを使用して顧客データセンターと統合されます。Cloud Connectorを使用するCitrix Endpoint Managementのお客様は、通常、データセンターでNetScaler Gatewayを管理します。

次の図は、サービスとそのセキュリティ境界を示しています。



このセクションの情報は次のとおりです。

- Citrix Cloud のセキュリティ機能の概要を説明します。
- Citrix Cloud の展開を保護するための Citrix とお客様間の責任分担を定義します。
- Citrix Cloud またはそのコンポーネントやサービスの構成または管理ガイダンスではありません。

Citrix Endpoint Management が包括的なエンドツーエンドセキュリティを提供するために使用するテクノロジーについては、「Security and Productivity for the Mobile Enterprise」を参照してください。

データフロー

コントロールプレーンは、ユーザーオブジェクトとグループオブジェクトへの読み取りアクセスが制限されています。これらのオブジェクトは、ディレクトリ、DNS、および同様のサービスにあ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ります。コントロールプレーンは、セキュアな HTTPS 接続を介して Citrix Cloud Connector 経由でこれらのサービスにアクセスします。

メール、イントラネット、Web アプリトラフィックなどの企業データは、NetScaler Gateway を介してデバイスとアプリケーションサーバー間で直接流れます。NetScaler Gateway は、お客様のデータセンターに展開されます。

データ分離

コントロールプレーンは、ユーザーデバイスとそのモバイルアプリケーションを管理するために必要なメタデータを保存します。サービス自体は、マルチテナントコンポーネントとシングルテナントコンポーネントの組み合わせで構成されています。ただし、サービスアーキテクチャに従い、顧客メタデータは常にテナントごとに個別に保存され、一意の資格情報を使用して保護されます。

資格情報の処理

サービスは次の種類の資格情報を処理します。

- **ユーザー資格情報:** ユーザー資格情報は、HTTPS 接続を介してデバイスからコントロールプレーンに送信されます。コントロールプレーンは、セキュアな接続を介して、お客様のディレクトリ内のディレクトリでこれらの資格情報を検証します。
- **管理者資格情報:** 管理者は Citrix Cloud に対して認証を行います。Citrix Cloud は Citrix Online のサインオンシステムを使用します。このプロセスにより、管理者にサービスへのアクセスを許可するワンタイム署名付き JSON Web Token (JWT) が生成されます。
- **Active Directory credentials:** コントロールプレーンは、Active Directoryからユーザーメタデータを読み取るためにバインド資格情報を必要とします。これらの資格情報はAES-256暗号化を使用して暗号化され、テナントごとのデータベースに保存されます。

展開に関する考慮事項

Citrixは、お客様の環境にNetScaler Gatewayを展開するための公開されているベストプラクティスドキュメントを参照することを推奨します。

その他のリソース

お客様は、Citrix製品に関連するセキュリティ速報を確認することをお勧めします。新規および更新されたセキュリティ速報については、Citrix Security Bulletinsを参照してください。また、Alert Settingsでアラートを受信するように登録することも検討してください。

その他のセキュリティ情報については、以下のリソースを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrixセキュリティサイト: `<https://www.citrix.com/security>`
- Citrix Cloud ドキュメント: Citrix Cloud Platform セキュア展開ガイド
- Citrix ADC セキュア展開ガイド

モバイル脅威防御ソフトウェアとの統合

モバイル脅威防御 (MTD) ソフトウェアは、企業モバイルデバイスに対する高度なサイバー攻撃を検出し、分析し、防止を支援します。MTDとUnified Citrix Endpoint Management (UEM) の組み合わせにより、組織のセキュリティと可視性が向上します。

MTDソフトウェアは、Citrix Endpoint Managementが以下の目的で使用する脅威データを提供します。

- マルウェア、フィッシング、ネットワーク攻撃、中間者攻撃から保護する
- デバイスのコンプライアンスステータスを判断する
- リスクレベルを判断する
- ポリシーベースのアクションを実行して、アプリ、データ、デバイス、モバイルネットワークを保護します

Citrix Endpoint Managementは、以下のMTDベンダーと統合されています。

- チェック・ポイント
- ルックアウト
- ワンデラ
- ジンペリウム

詳細情報やデモのリクエストについては、MTDパートナーまたはCitrixの営業担当者にお問い合わせください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント マネジメント と マイクロソフト エンドポイント マネージャー の統合

Citrix Endpoint Management と Microsoft Endpoint Manager (MEM) の統合により、Microsoft Edge ブラウザなどの Microsoft Intune 対応アプリに Citrix Endpoint Management のマイクロ VPN の価値が追加されます。

統合を有効にするには、Citrix Cloud Operations チームにお問い合わせください。

このリリースでは、以下のユースケースをサポートしています。

- インチューン MAM と シトリックス エンドポイント マネジメント MDM+MAM。

  この記事では、Intune MAM + Citrix Endpoint Management MDM+MAM のユースケースに焦点を当てています。Citrix を MDM プロバイダーとして追加した後、Intune で管理されているアプリをデバイスに配信するように構成します。

  重要:

  - このユースケースでは、Citrix Secure Mail は Intune との統合をサポートしていません。
  - Intune との Citrix Secure Mail 統合は非推奨となり、今後のリリースで削除されます。詳細については、Secure Mail の新機能 を参照してください。

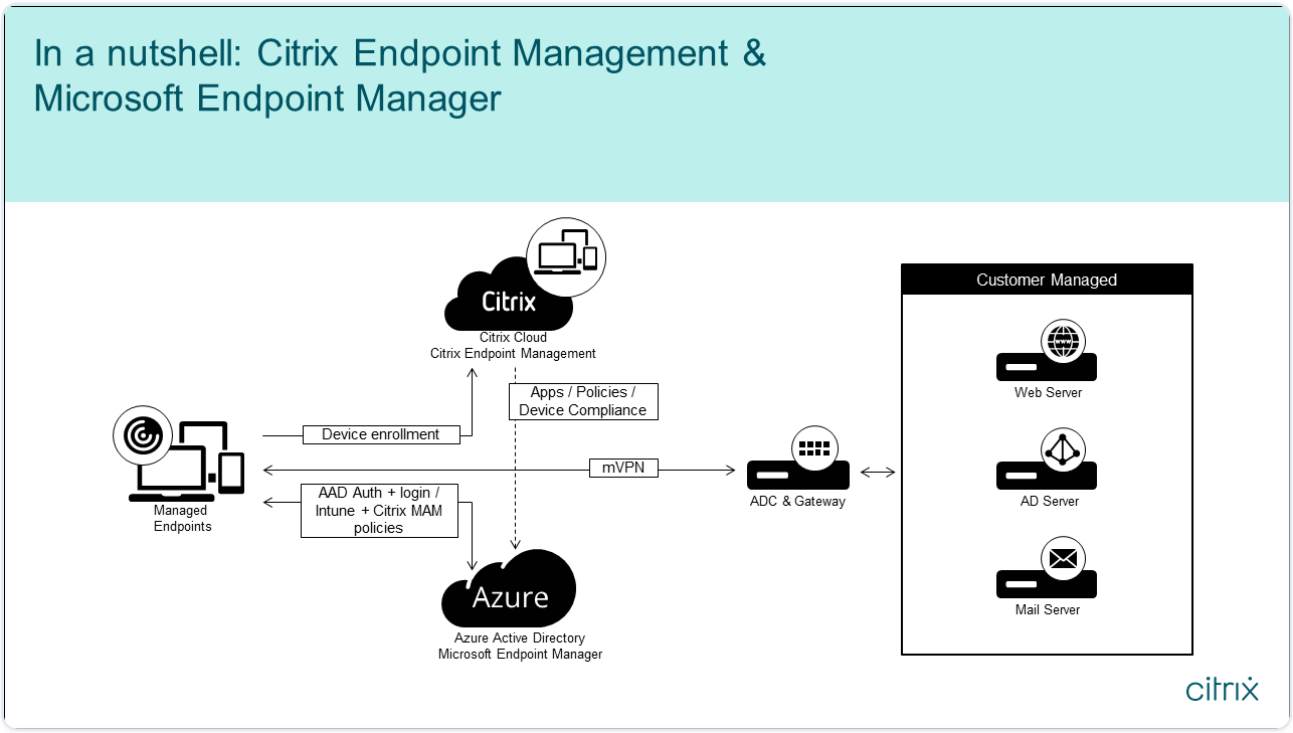
- インチューン エムエーエム と シトリックス エンドポイント マネジメント エムディーエム。
- インチューン エムエーエム。
- Intune MAM と Intune MDM。iOS 用 Citrix Secure Mail は、このユースケースでシングルサインオンをサポートしています。

MEM との Citrix Endpoint Management 統合をセットアップするための、わかりやすいグラフィカルなガイドについては、入門ガイド を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure AD 条件付きアクセスとの統合については、Azure AD 条件付きアクセスとの統合 を参照してください。

次の図は、Citrix Endpoint Management と Microsoft Endpoint Manager の統合の概要を示しています。



システム要件

MDX対応

- MAM SDK

  または

- MDX ツールキット

マイクロソフト

- Azure Active Directory (AD) アクセス（テナント管理者権限を持つ）
- Intuneが有効なテナント

ファイアウォールルール

- NetScaler GatewayサブネットIPから`*.manage.microsoft.com`、`https://login.microsoftonline.com`、および`https://graph.windows.net`へのDNSおよびSSLトラフィックを許可するファイアウォールルールを有効にします（ポート53および443）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

- **Microsoft Edgeブラウザ:** Mobile Apps SDKは、iOSおよびAndroid用のMicrosoft Edgeブラウザアプリに統合されています。Microsoft Edgeの詳細については、Microsoft Edgeドキュメントを参照してください。
- **Citrix Cloudアカウント:** Citrixアカウントにサインアップし、Citrix Endpoint Managementの試用版をリクエストするには、Citrix営業担当者にお問い合わせください。続行する準備ができたら、https://onboarding.cloud.comにアクセスしてください。Citrix Cloudアカウントのリクエストの詳細については、Citrix Cloudへのサインアップを参照してください。

  注:

  提供するメールアドレスは、Azure ADに関連付けられていないアドレスである必要があります。任意の無料メールサービスを使用できます。

- **iOS用APNs証明書:** iOS用APNs証明書を構成していることを確認してください。これらの証明書の設定の詳細については、Citrixブログ記事「Creating and Importing APNs Certificates」を参照してください。
- **Azure AD同期:** Azure ADとオンプレミスのActive Directory間の同期を設定します。AD同期ツールをドメインコントローラーマシンにインストールしないでください。この同期の設定の詳細については、Microsoftのドキュメント「Azure Active Directory」を参照してください。

NetScaler Gatewayの構成

新しいCitrix Endpoint Management展開をセットアップする場合は、次のいずれかのNetScaler Gatewayアプライアンスをインストールします。

- NetScaler® Gateway VPX 3000シリーズ以降
- NetScaler Gateway MPXまたは専用SDXインスタンス

MEMとのCitrix Endpoint Management統合でNetScaler Gatewayを使用するには：

- NetScaler Gatewayを管理インターフェイスとサブネットIPで構成します。
- すべてのクライアントとサーバー間の通信にTLS 1.2を使用します。NetScaler GatewayのTLS 1.2の構成については、CTX247095を参照してください。

MEMとのCitrix Endpoint Management統合をCitrix Endpoint Management MDM+MAM展開で使用している場合は、2つのCitrix Gatewayを構成します。MDXアプリのトラフィックは一方の

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gatewayを経由し、Intuneアプリのトラフィックはもう一方のNetScaler Gatewayを経由します。以下を構成します。

- 2つのパブリックIP。
- オプションで、1つのネットワークアドレス変換されたIP。
- 2つのDNS名。例: `https://mam.company.com`。
- 2つのパブリックSSL証明書。予約済みのパブリックDNS名に一致する証明書を構成するか、ワイルドカード証明書を使用します。
- 内部のルーティング不可能なRFC 1918 IPアドレスを持つMAMロードバランサー。
- LDAP Active Directoryサービスアカウント。

委任されたアクセス許可プロンプトへの同意

ユーザー認証を必要とする管理対象アプリの場合、アプリはMicrosoft Graphによって公開されているアプリケーションのアクセス許可を要求します。これらのアクセス許可プロンプトに同意することで、アプリは必要なリソースとAPIにアクセスできます。一部のアプリでは、Microsoft Azure ADのグローバル管理者の同意が必要です。これらの委任されたアクセス許可の場合、グローバル管理者はCitrix Cloudにトークンを要求する権限を付与する必要があります。その後、トークンによって次のアクセス許可が有効になります。詳細については、「Microsoft Graph permissions reference」を参照してください。

- **サインインしてユーザープロファイルを読み取る:** このアクセス許可により、ユーザーはAzure ADにサインインして接続できます。Citrix®はユーザー資格情報を表示できません。
- **すべてのユーザーの基本プロファイルを読み取る:** アプリは組織内のユーザーのプロパティを読み取ります。プロパティには、組織内のユーザーの表示名、名と姓、メールアドレス、写真が含まれます。
- **すべてのグループを読み取る:** このアクセス許可により、アプリとポリシーの割り当てにAzure ADグループを指定できます。
- **サインインしているユーザーとしてディレクトリにアクセスする:** このアクセス許可は、Intuneサブスクリプションを検証し、NetScaler GatewayおよびVPN構成を有効にします。
- **Microsoft Intuneアプリの読み取りと書き込み:** アプリは以下を読み書きできます。
  - Microsoft管理プロパティ
  - グループの割り当てとアプリのステータス
  - アプリの構成
  - アプリ保護ポリシー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

また、NetScaler Gatewayの構成中に、Azure ADグローバル管理者は次のことを行う必要があります。

- マイクロVPN用に選択されたActive Directoryを承認します。グローバル管理者は、NetScaler GatewayがAzure ADおよびIntuneと通信するために使用するクライアントシークレットも生成する必要があります。
- Citrix管理者としての役割を持たない。代わりに、Citrix管理者は適切なIntuneアプリケーション管理者権限を持つユーザーにAzure ADアカウントを割り当てます。その後、Intune管理者はCitrix Cloud内からIntuneを管理するためにCitrix Cloud管理者としての役割を果たします。

注:

Citrixはセットアップ中にのみIntuneグローバル管理者パスワードを使用し、認証をMicrosoftにリダイレクトします。Citrixはパスワードにアクセスできません。

Citrix Endpoint ManagementとMEMの統合を構成するには

1. Citrix Cloudサイトにログオンし、Citrix Endpoint Managementの試用版をリクエストします。
2. セールスエンジニアがお客様とのオンボーディングミーティングをスケジュールします。Citrix Endpoint ManagementとMEMの統合を希望していることを伝えてください。リクエストが承認されたら、**Manage**をクリックします。

   (/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems1.png)
3. ここから、サイトの右上にある歯車アイコンをクリックするか、**Configure Site**をクリックできます。

   (/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-configure-site.png)
4. 最初のステップのリンクをたどって、**Identity and Access Management**ページに移動します。

   (/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems2.png)
5. **Connect**をクリックして、Azure ADのインストールを接続します。

   (/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems3.png)
6. Azure AD管理者がログオンに使用する一意のログオンURLを入力し、**Confirm**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems4.png)

7. Azure AD グローバル管理者アカウントを追加し、アクセス許可要求を承認します。

   「別のアカウントを使用」ボタン(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems5.png)

   「承認」ボタン](/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems6.png)

8. Azure AD インスタンスが正常に接続されていることを確認します。接続が成功すると、「**未接続**」のテキストが「**有効**」に変わります。

   「切断」ボタン(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems7.png)

9. 「**管理者**」タブをクリックし、Azure AD Intune 管理者を Citrix Cloud 管理者として追加します。ドロップダウンメニューから Azure AD または Citrix Identity を選択し、追加するユーザー名を検索します。「**招待**」をクリックし、「**招待を送信**」をクリックする前に、ユーザーに「**フルアクセス**」または「**カスタムアクセス**」を付与します。

   > **注：**
   >
   > Citrix Endpoint Management では、「**カスタムアクセス**」に次のルールが必要です：ライブラリと Citrix Endpoint Management。

   その結果、Azure AD Intune 管理者は、パスワードを作成して Citrix Cloud にサインインするためのメール招待を受け取ります。管理者がサインインする前に、他のすべてのアカウントからサインアウトしていることを確認してください。

   Azure AD Intune 管理者は、この手順の残りのステップに従う必要があります。

   Azure AD Intune 管理者の招待オプション(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems8.png)

   確認画面(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems9.png)

10. 新しいアカウントでサインインした後、「**Citrix Endpoint Management**」の下にある「**管理**」をクリックします。すべてが正しく構成されている場合、ページには Azure AD 管理者がサインインしており、Intune サブスクリプションが有効であることが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management の管理オプション(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems10.png)

マイクロ VPN 用に NetScaler Gateway を構成するには

IntuneでマイクロVPNを使用するには、NetScaler GatewayをAzure ADに対して認証するように構成する必要があります。既存のNetScaler Gateway仮想サーバーは、このユースケースでは機能しません。

まず、Azure ADをオンプレミスのActive Directoryと同期するように構成します。この手順は、IntuneとNetScaler Gateway間の認証が適切に行われるようにするために必要です。

アクティブディレクトリ同期(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems11.png)

1. Citrix Cloudコンソールで、**Citrix Endpoint Management**の下にある**管理**をクリックします。
2. **Micro VPN**の横にある**Micro VPNの構成**をクリックします。

   Micro VPNの構成ボタン(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems12.png)
3. マイクロVPNサービスの名称とNetScaler Gatewayの外部URLを入力し、**次へ**をクリックします。

   このスクリプトは、NetScaler GatewayがAzure ADとIntuneアプリをサポートするように構成します。

   NetScaler Gatewayの詳細ページ(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems13.png)
4. **スクリプトのダウンロード**をクリックします。zipファイルには、スクリプトを実装するための手順が記載されたreadmeが含まれています。ここから保存して終了することはできますが、NetScaler Gatewayのインストールでスクリプトを実行するまで、Micro VPNはセットアップされません。

   スクリプトのダウンロードボタン(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems14.png)

   注：

   NetScaler Gatewayの構成プロセスが完了したときに、OAuthステータスがCOMPLETE以外の場合は、「トラブルシューティング」セクションを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

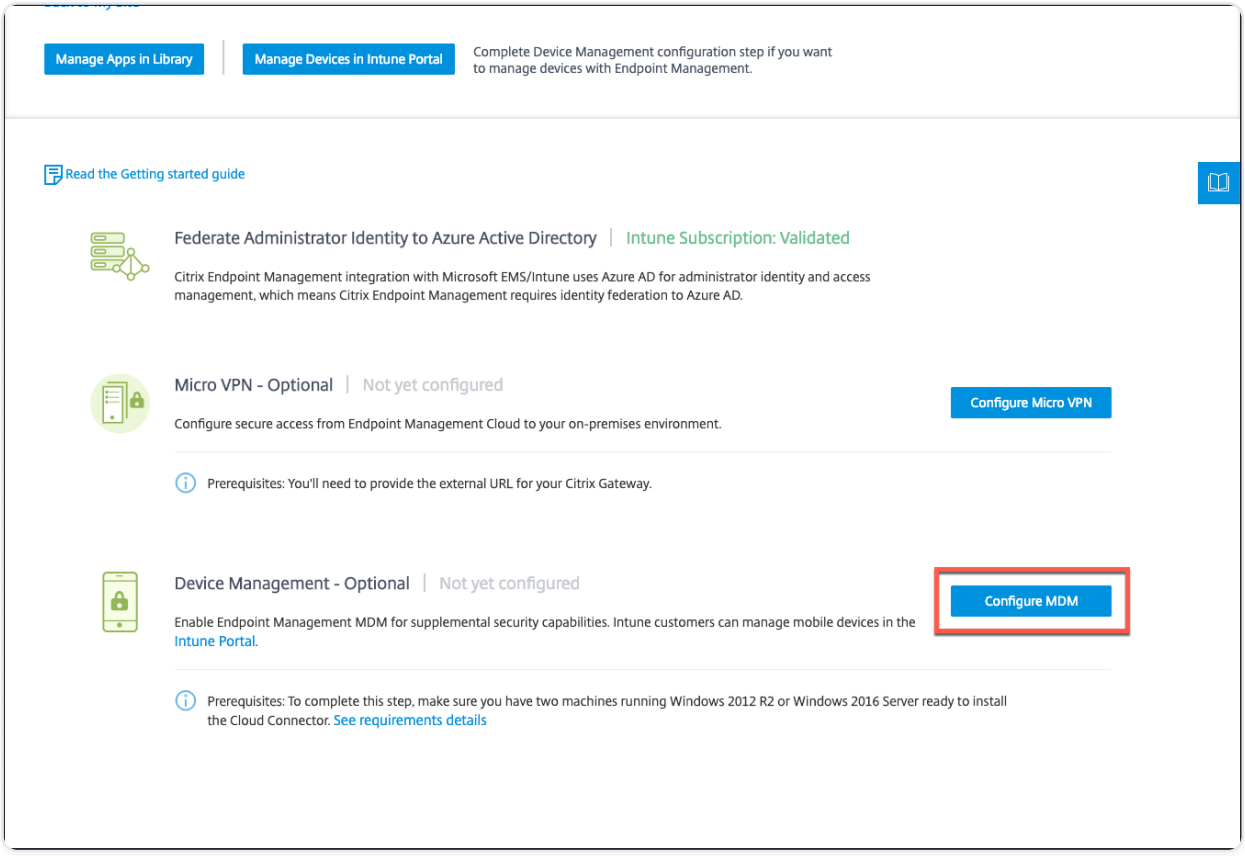
デバイス管理を構成するには

アプリケーションに加えてデバイスを管理したい場合は、デバイス管理の方法を選択します。Citrix Endpoint Management MDM+MAMまたはIntune MDMを使用できます。

注記:

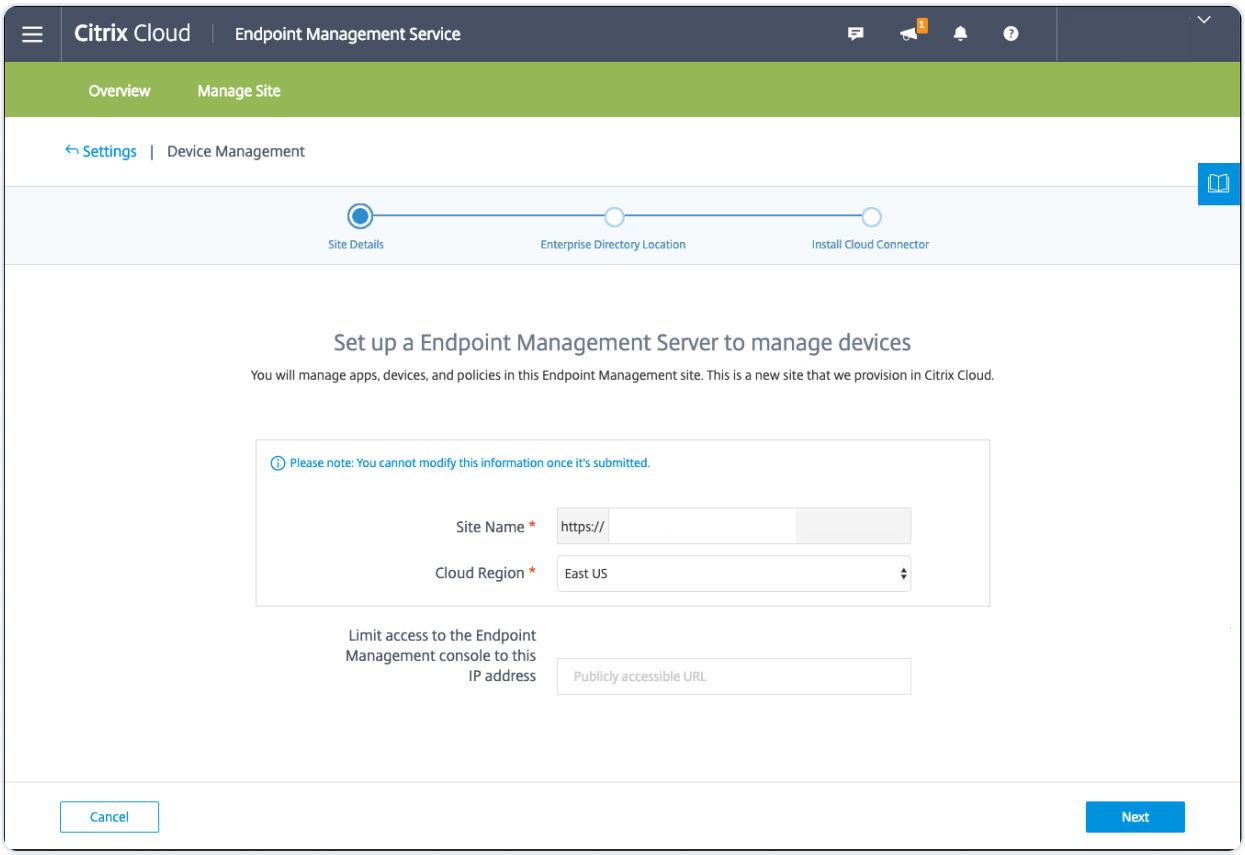
コンソールは既定でIntune MDMを使用します。IntuneをMDMプロバイダーとして使用するには、Microsoft Intuneのドキュメントを参照してください。

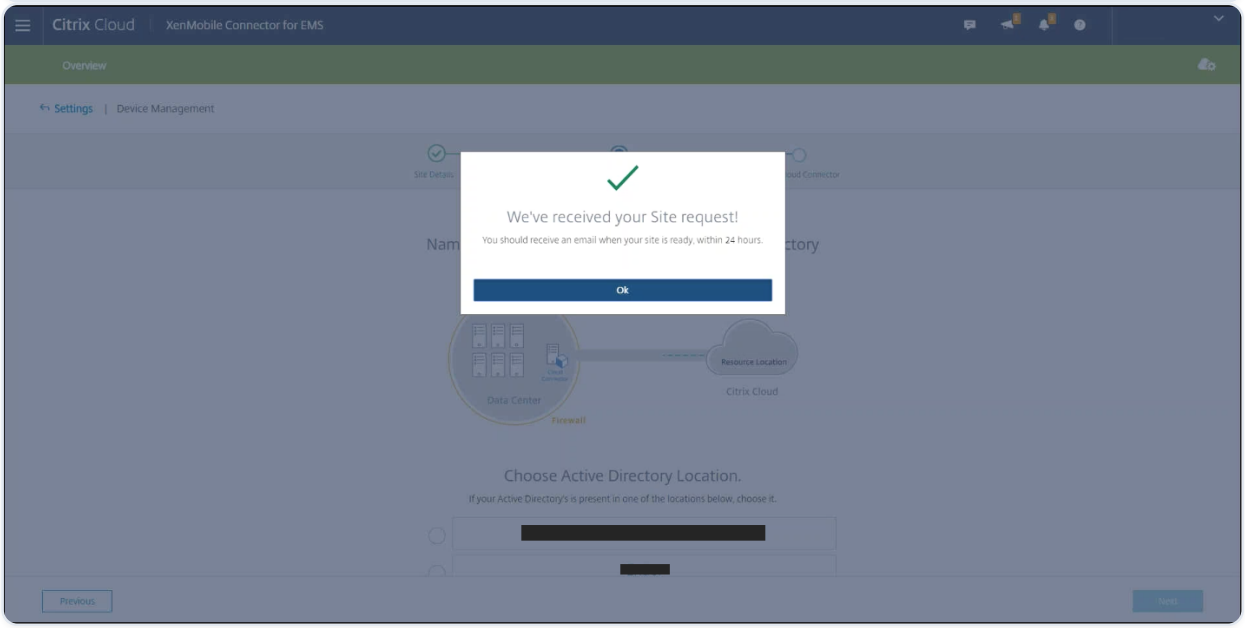
1. Citrix Cloudコンソールで、の下にある**をクリックします。の横にある**をクリックします。



2. 一意のサイト名を入力し、最も近いクラウドリージョンを選択し、****をクリックします。サイトの準備が完了すると、メールが届きます。

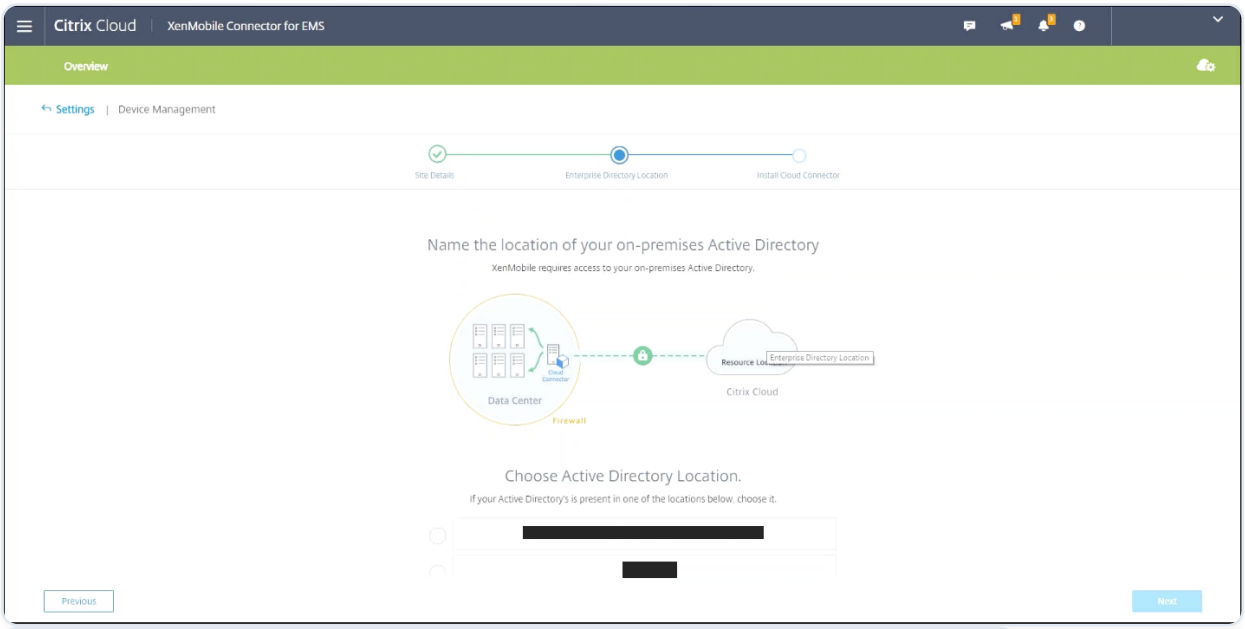
© 1997–2026 Citrix Systems, Inc. All rights reserved.

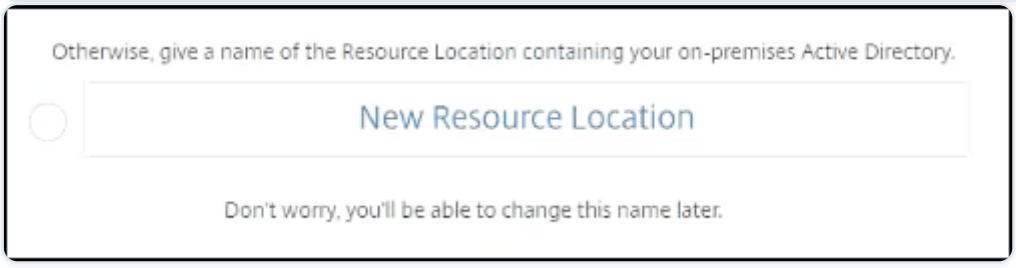




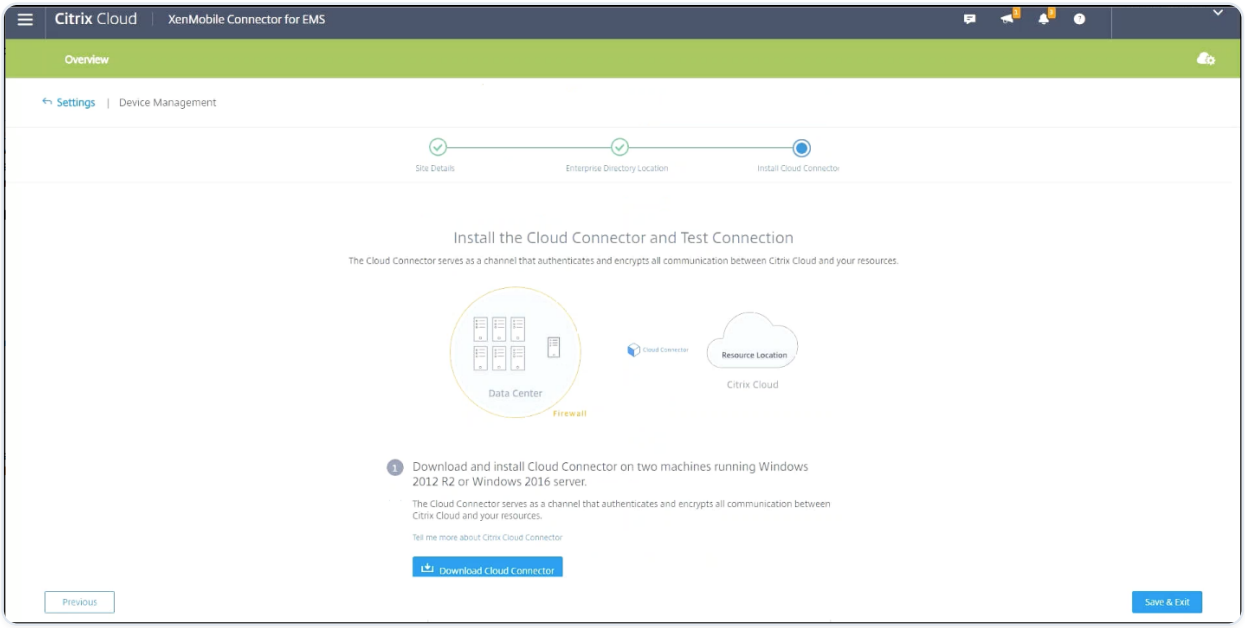
3. プロンプトを閉じるには、**をクリックします。**サイトに関連付けるActive Directoryの場所を選択するか、リソースの場所を作成し、**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

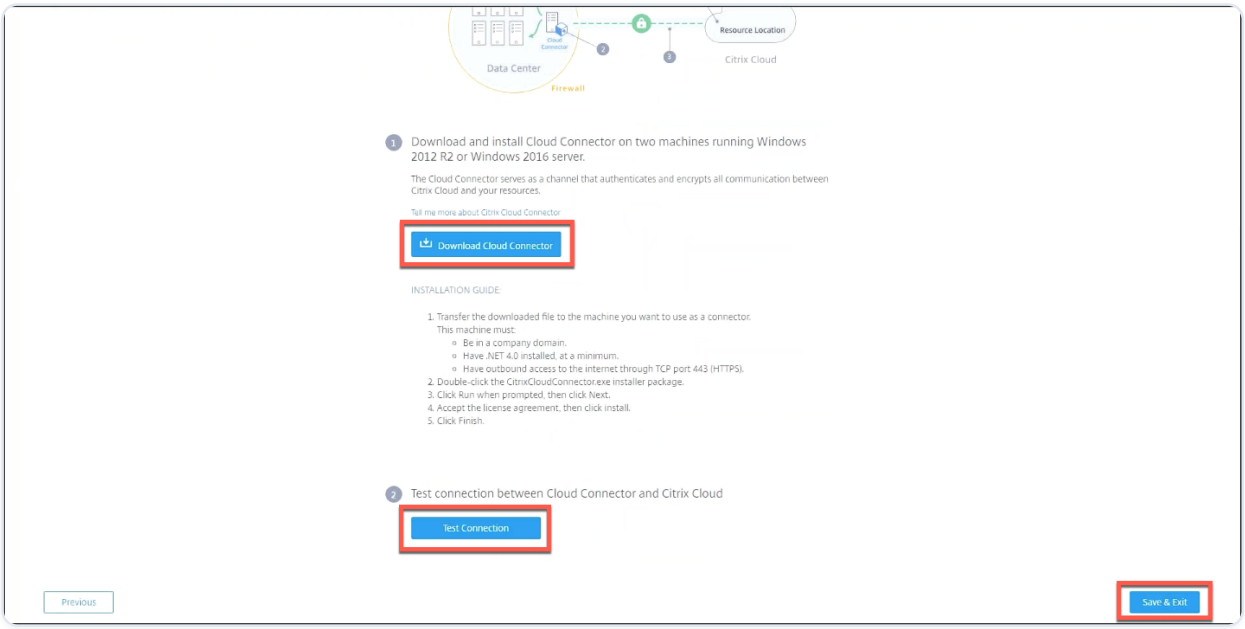




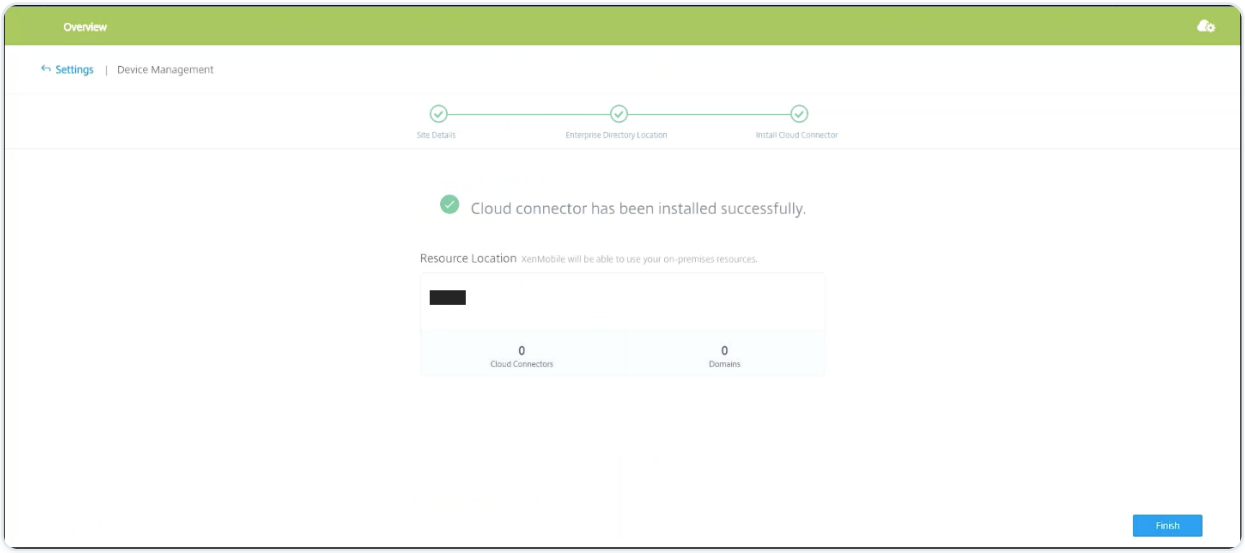
4. **をクリックし、画面の指示に従ってCloud Connectorをインストールします。インストール後、**をクリックして、Citrix CloudとCloud Connector間の接続を確認します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

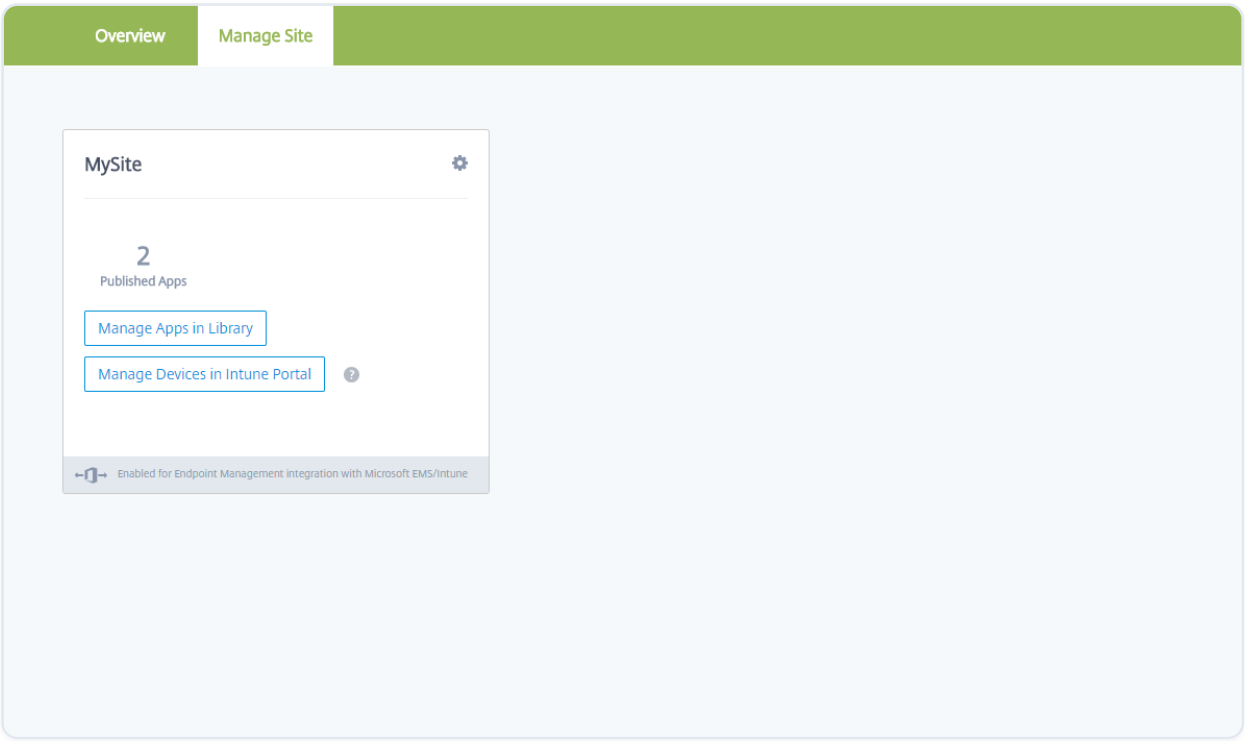


5. 完了するには、**をクリックします。リソースの場所が表示されます。**をクリックすると、設定画面に戻ります。



6. サイトタイルからCitrix Endpoint Managementコンソールにアクセスできるようになりました。ここから、MDM管理タスクを実行し、デバイスポリシーを割り当てることができます。デバイスポリシーの詳細については、「デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Intuneで管理されているアプリをデバイスに配信するように構成する

注：

April 1, 2025 以降、ライブラリを介したMicrosoft Intuneアプリの管理は利用できなくなります。関連サービスについてサポートが必要な場合は、Citrix Supportに連絡してこの機能を有効にしてください。

Intuneで管理されているアプリを配信するように構成するには：

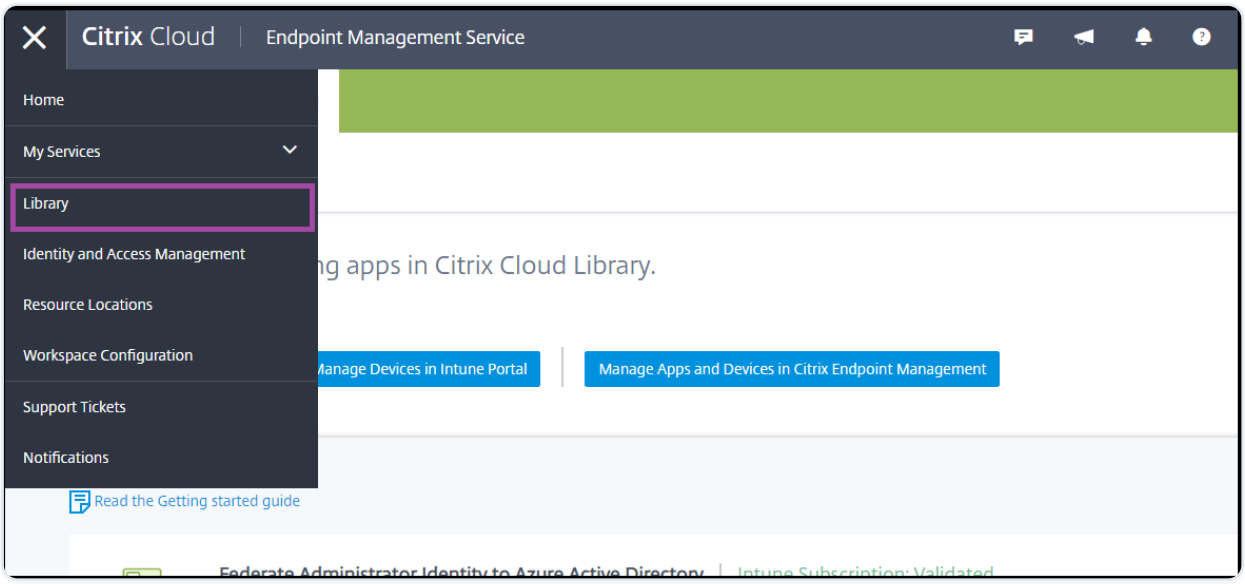
- アプリをCitrix Cloudライブラリに追加する
- データフローを制御するためのCitrix Endpoint Managementデバイスポリシーを作成する
- アプリとポリシーのデリバリーグループを作成する

Microsoft IntuneアプリをCitrix Cloudライブラリに追加する

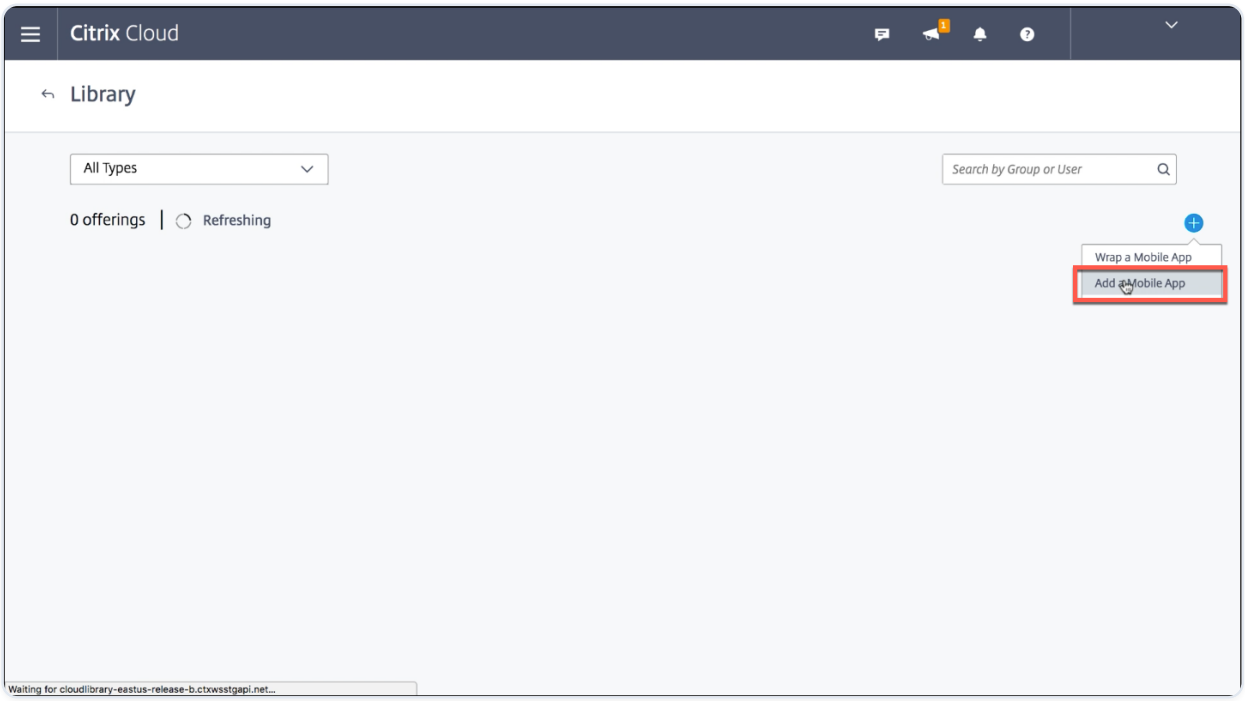
追加する各アプリについて：

1. Citrix Cloudコンソールから、メニューアイコンをクリックし、**［ライブラリ］**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 右上隅にあるプラス記号のアイコンをクリックし、**［モバイルアプリの追加］**をクリックします。



3. Citrix Endpoint Management コンソールで Android Enterprise を構成している場合は、 で を選択します。カスタマイズするアプリテンプレートを選択するか、 をクリックします。

   構成するポリシー(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-integration-with-ems25.png)

   Citrix は既存のアプリテンプレートを提供しており、それぞれに事前構成されたデフォルトポリシーのセットが付属しています。お客様がアップロードするアプリには、次のポリシーが適用されます。

   - **MDXファイル:** MAM SDK対応アプリまたはMDXでラップされたアプリが含まれます。例:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Intuneアプリ保護ポリシーとパッケージ内のデフォルトのMDXポリシー
- バンドルIDまたはパッケージIDに一致するIntuneアプリ保護ポリシーやデフォルトのMDXポリシーなどのパブリックストアアプリ

- **IPAファイル:** Intuneアプリ保護ポリシー。
- **APKファイル:** Intuneアプリ保護ポリシー。

注:

アプリがIntuneでラップされていない場合、Intuneアプリ保護ポリシーは適用されません。

4. をクリックし、.mdxファイルまたはIntuneでラップされたファイルをアップロードします。

   独自のラップ済みファイルのアップロード画面(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-integration-with-ems37.png)

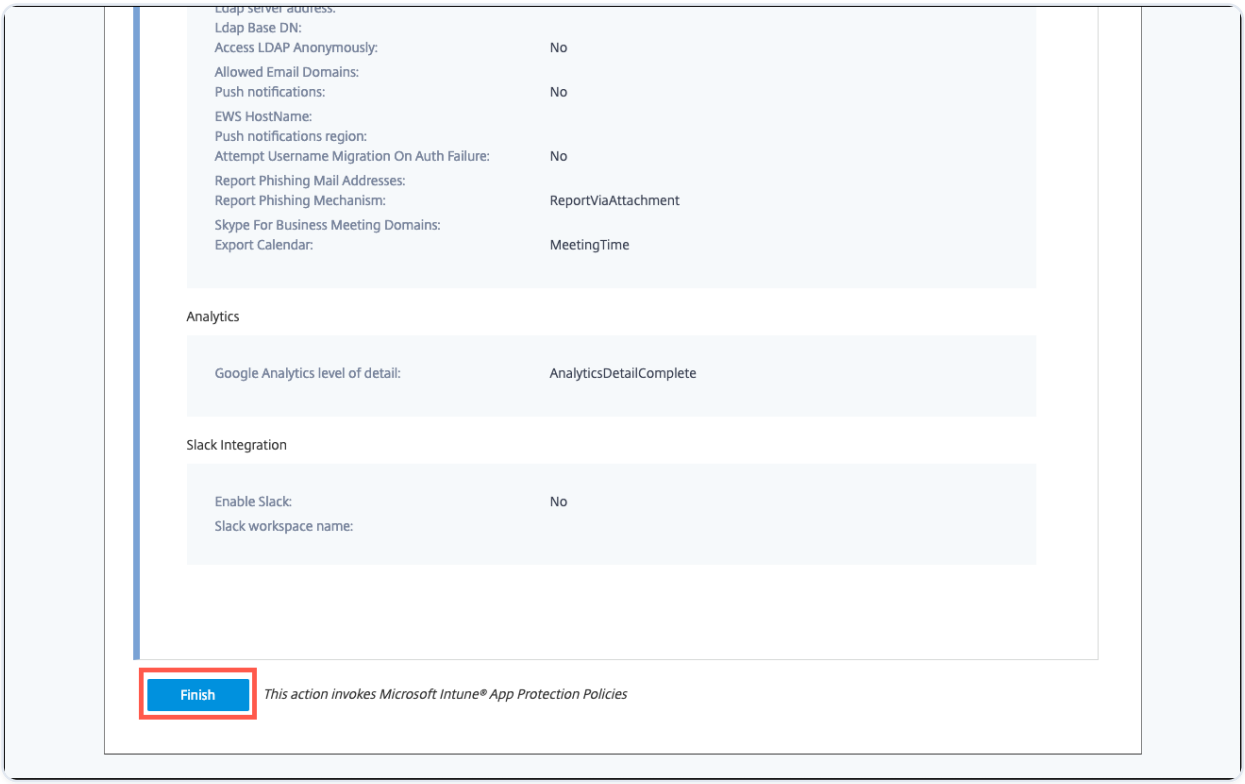
5. アプリの名前と説明を入力し、アプリがオプションか必須かを選択してから、 をクリックします。
6. アプリケーション設定を構成します。以下の構成により、Citrix Endpoint ManagementとIntuneコンテナが相互にデータを転送できるようになります。

   - : を選択します。
   - **アプリが他のアプリにデータを転送することを許可する:** 「**すべてのアプリ**」を選択します。
   - **他のアプリとの切り取り、コピー、貼り付けを制限する:** 「**ポリシー管理対象アプリ**」を選択します。

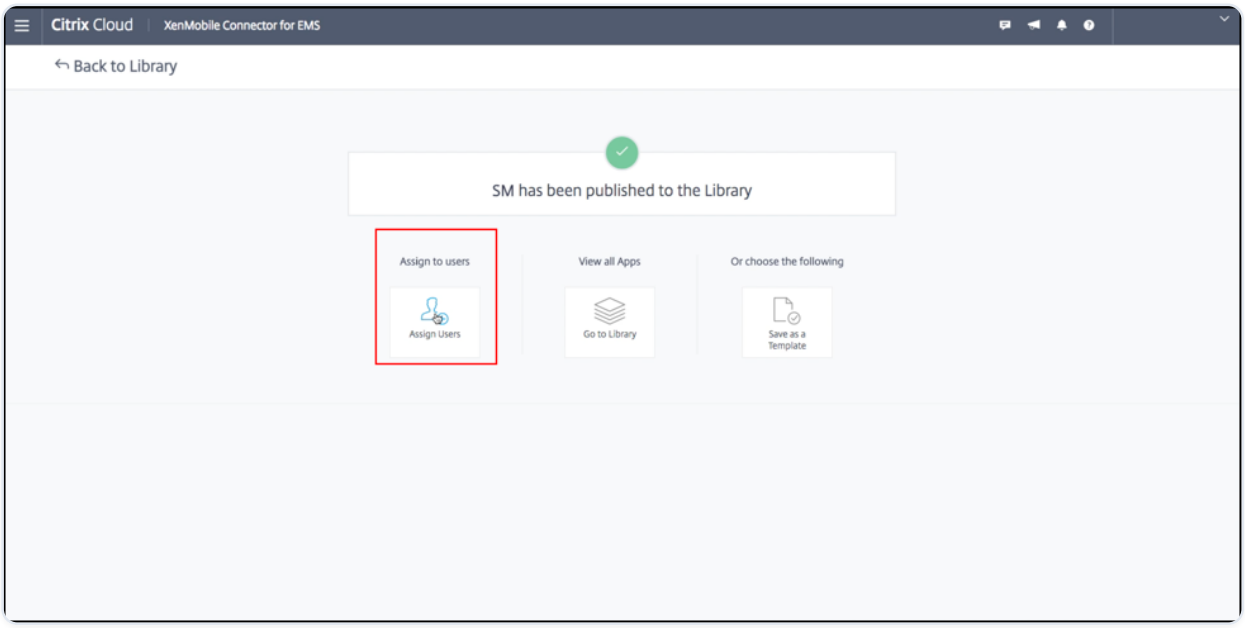
7. 保存されたデータのストレージリポジトリを構成します。「**企業データを保存できるストレージサービスを選択してください**」については、「**LocalStorage**」を選択します。
8. オプション: アプリのデータ再配置、アクセス、PINポリシーを設定します。「**次へ**」をクリックします。
9. アプリの概要を確認し、「**完了**」をクリックします。

   アプリの構成プロセスには数分かかる場合があります。プロセスが完了すると、アプリがライブラリに公開されたことを示すメッセージが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

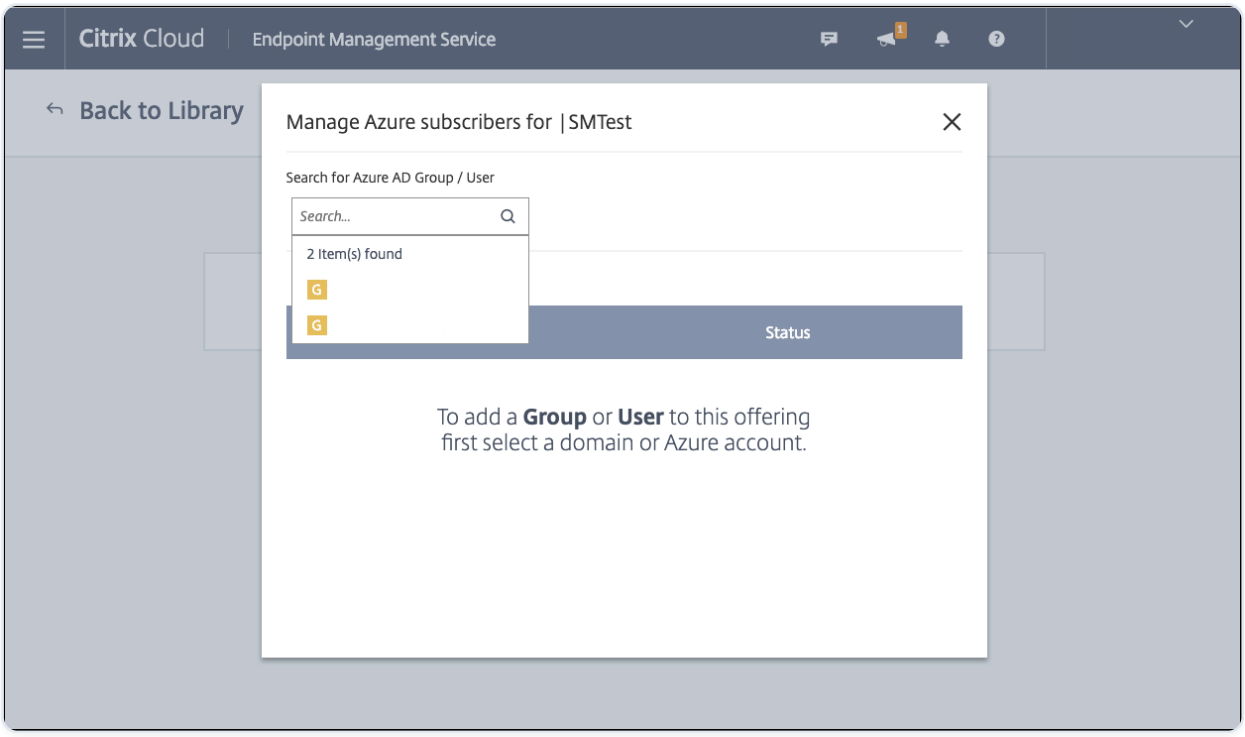


10. アプリにユーザーグループを割り当てるには、「**ユーザーの割り当て**」をクリックします。

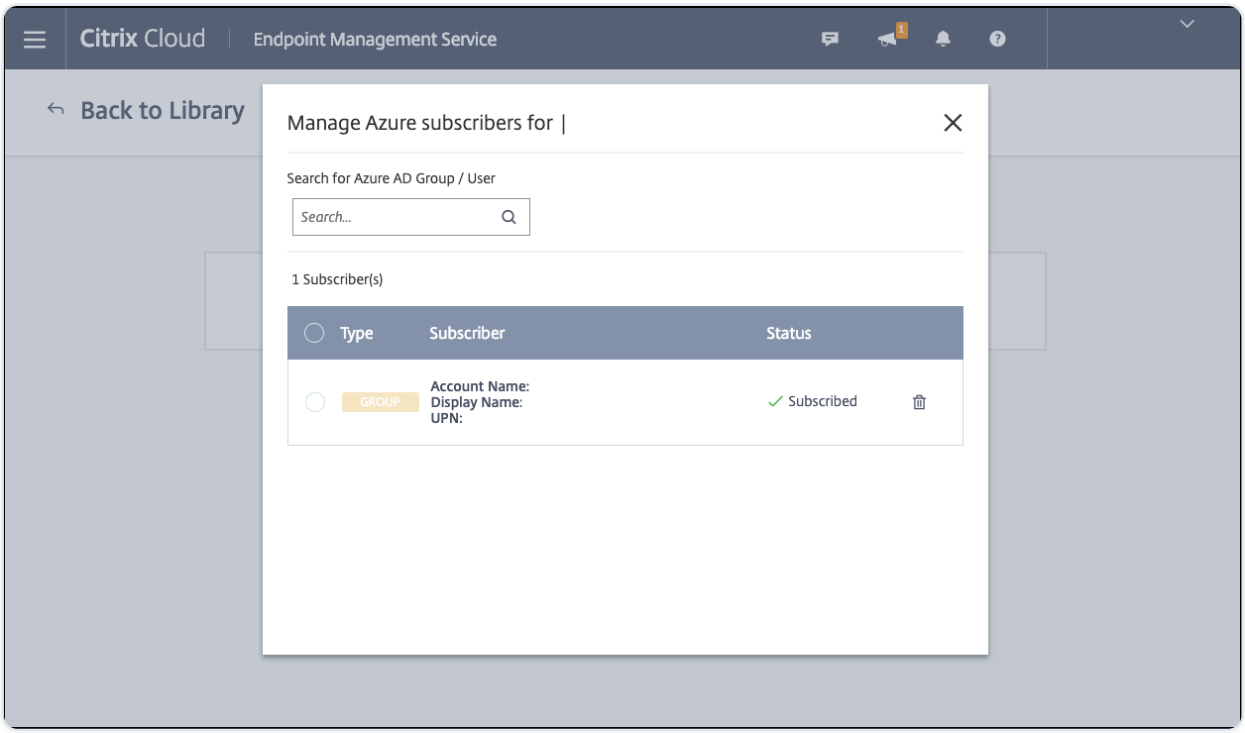


11. 検索ボックスでユーザーグループを検索し、クリックして追加します。個々のユーザーを追加することはできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



12. 必要なグループをすべて追加したら、Xをクリックしてウィンドウを閉じます。



ユーザーグループを追加する際にエラーが表示される場合があります。このエラーは、ユーザーグループがローカルのActive Directoryに同期されていない場合に発生します。

Android EnterpriseアプリをCitrix Cloudライブラリに追加する

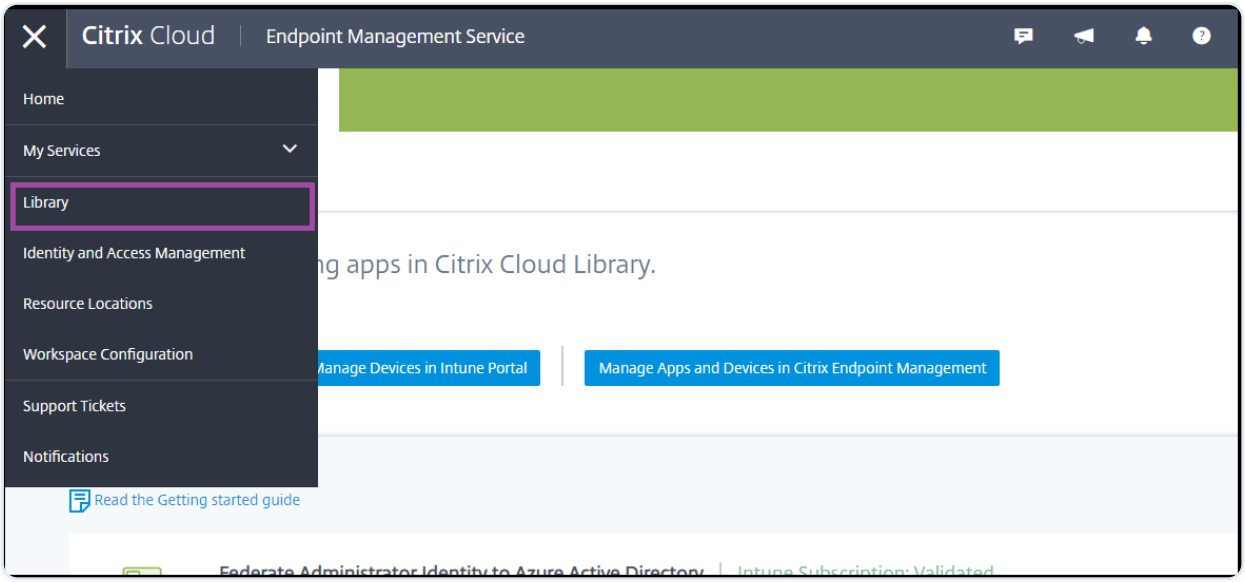
Android EnterpriseアプリをCitrix Cloudライブラリに追加し、Intuneアプリ保護ポリシーを設定するには、クラウド環境を次のように構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix CloudをAzure Active Directory (AAD) アカウントとフェデレーションします。「Azure Active DirectoryをCitrix Cloudに接続する」を参照してください。
- Citrix Endpoint ManagementでLDAPとCloud Connectorを構成します。
- Citrix Endpoint ManagementでAndroid Enterpriseを設定します。Android Enterpriseデバイスが MDM+MAMに登録されていることを確認してください。Android Enterpriseの設定については、「Android Enterprise」を参照してください。

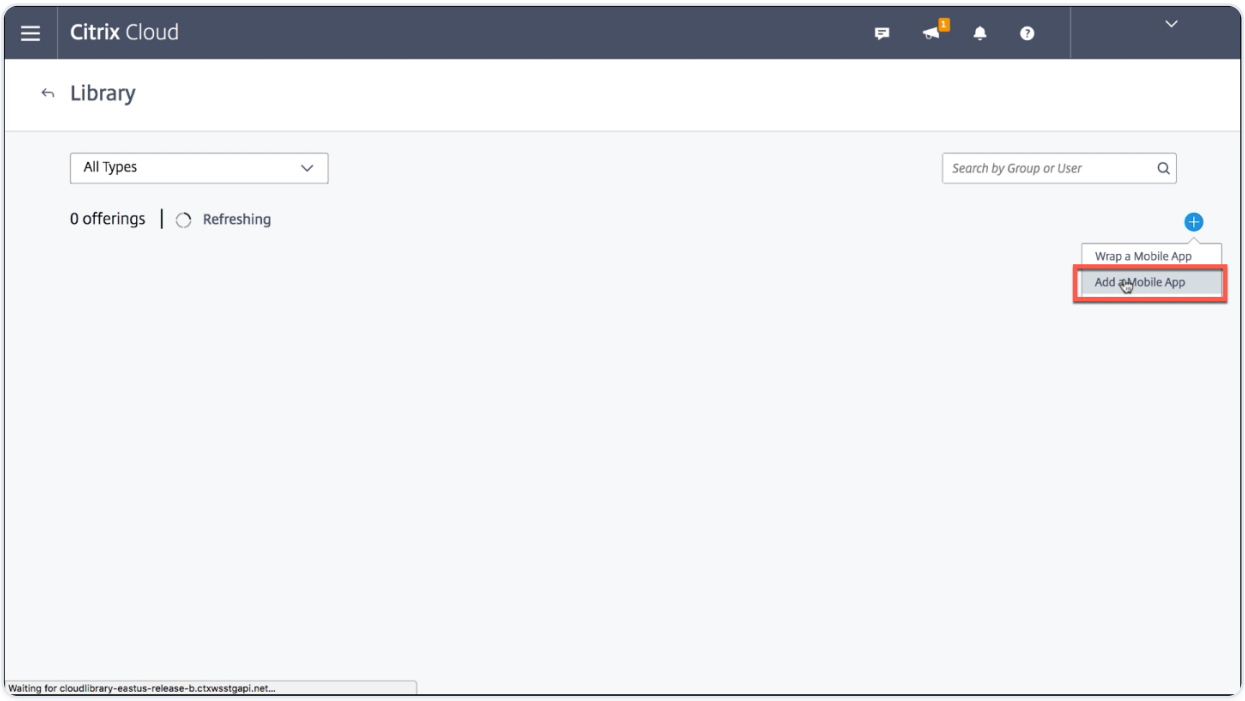
この手順を実行すると、Android EnterpriseアプリがCitrix Endpoint Managementコンソールと Intuneコンソールに同時に追加されます。追加するAndroid Enterpriseアプリごとに、次の手順を実行します。

1. Citrix Cloudコンソールから、メニューアイコンをクリックし、**「ライブラリ」**をクリックします。

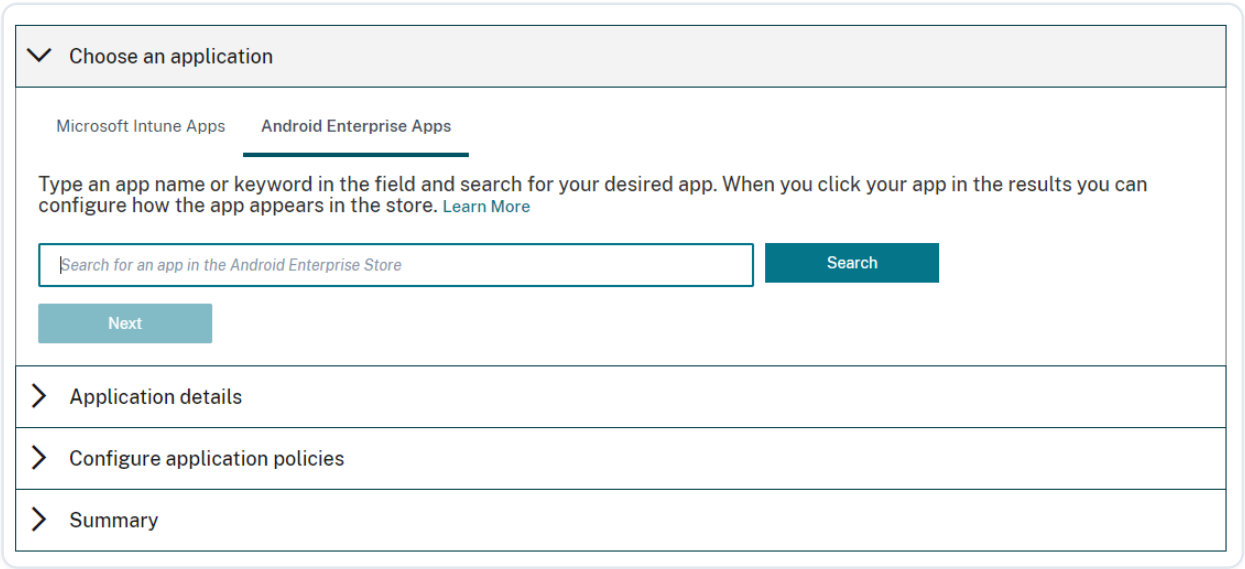


2. 右上隅にあるプラス記号アイコンをクリックし、**「モバイルアプリを追加」**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

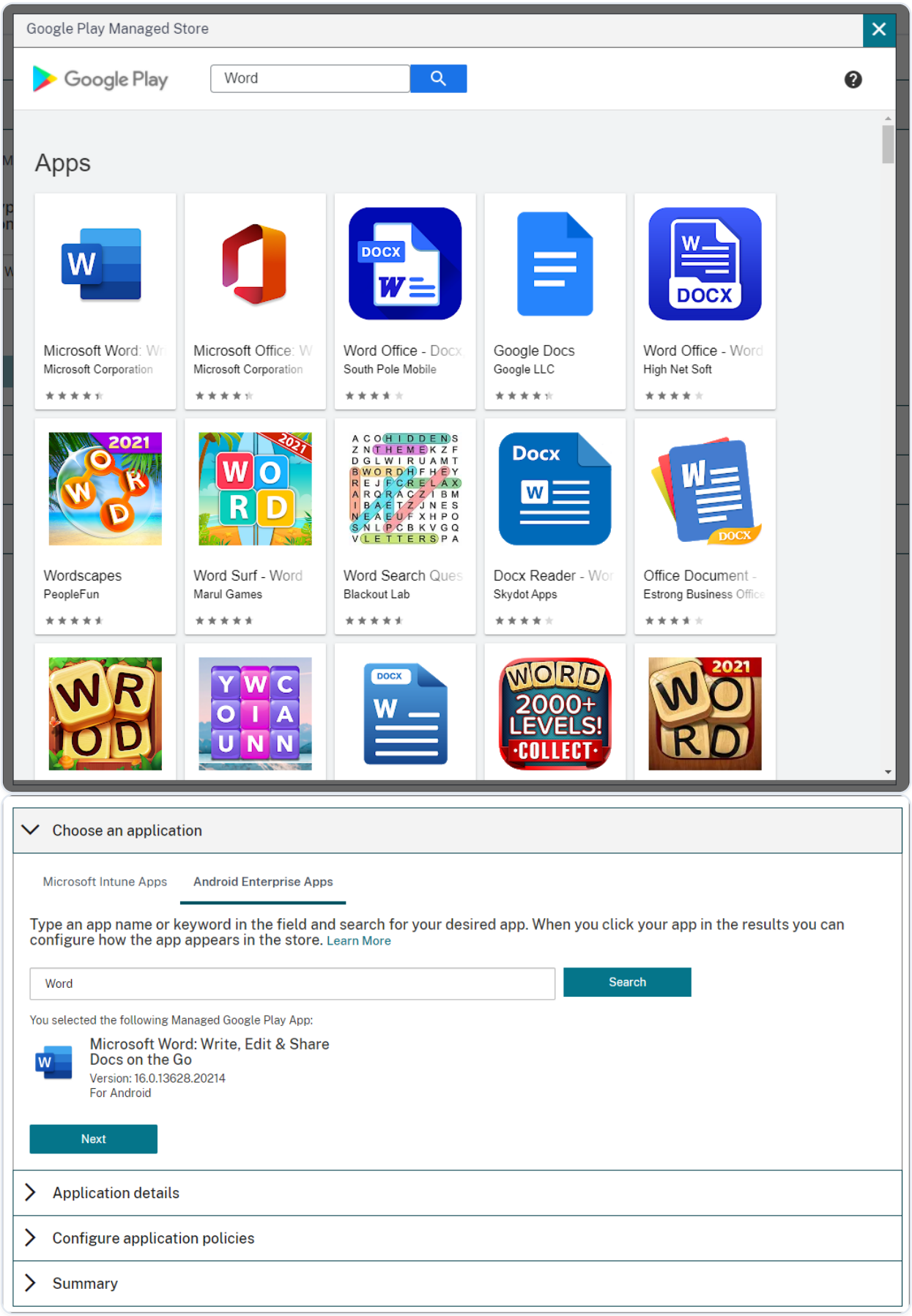


3. **「アプリケーションの選択」で、「Android Enterpriseアプリ」**を選択します。



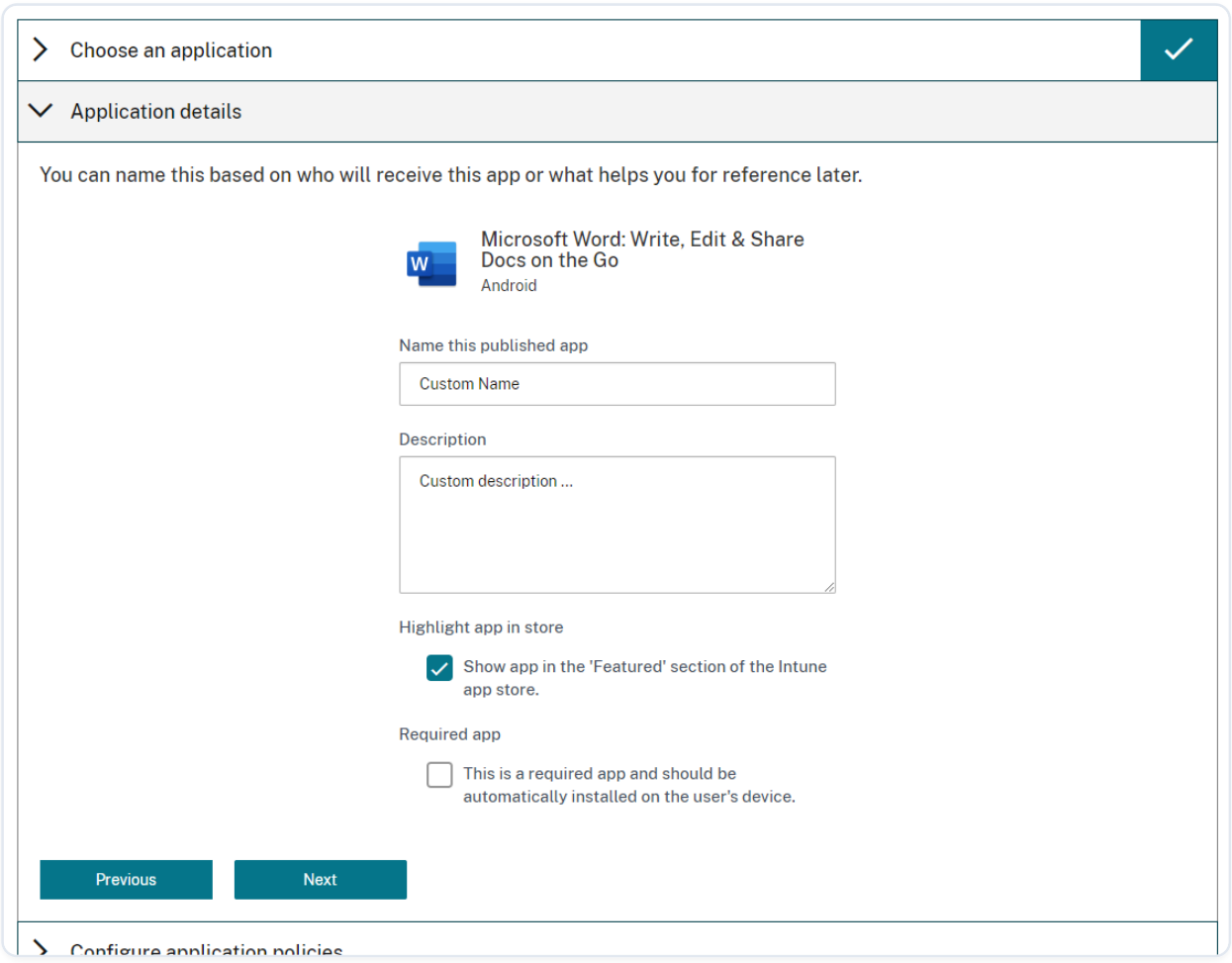
4. アプリを検索し、Managed Google Playストアウィンドウで承認します。Googleウィンドウが閉じたら、**「次へ」**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



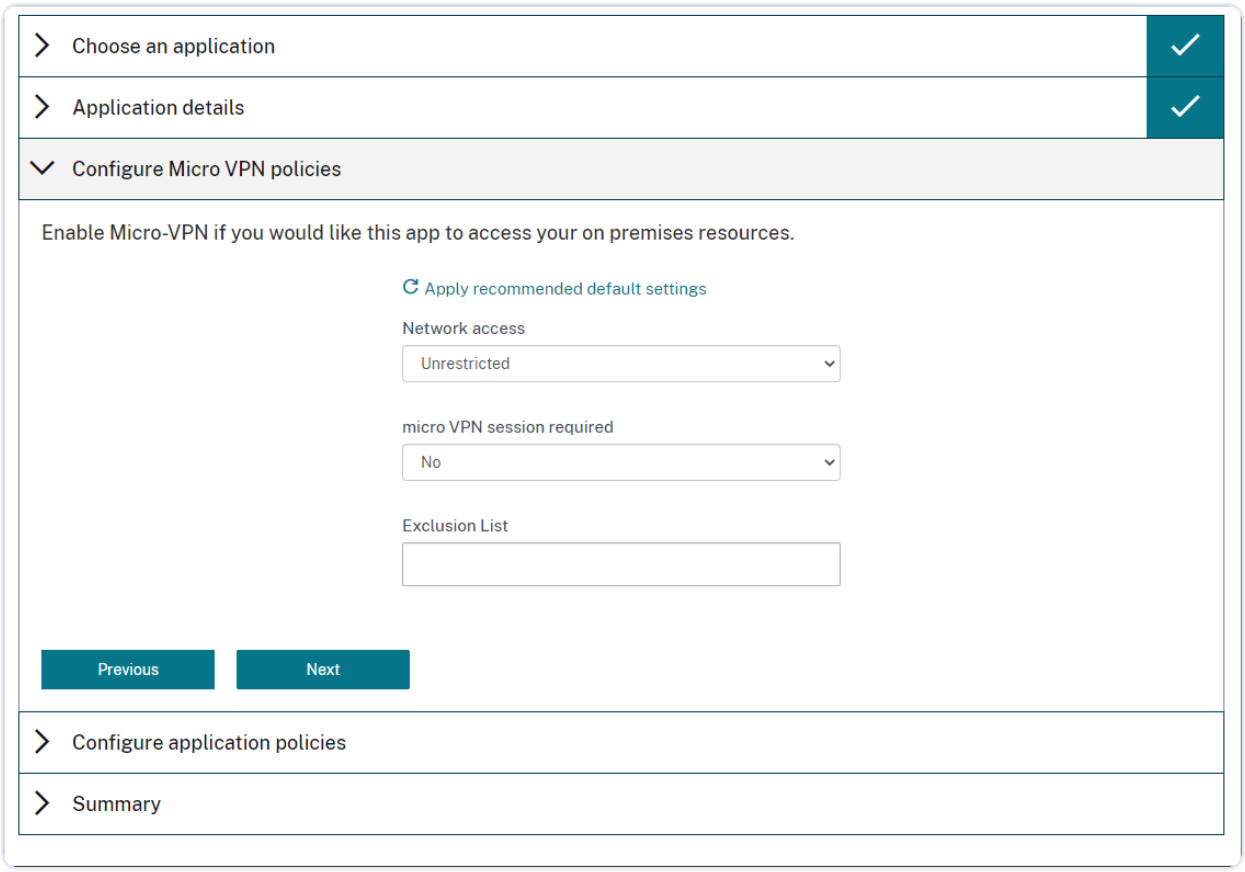
5. アプリケーションの詳細を追加し、**「次へ」**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

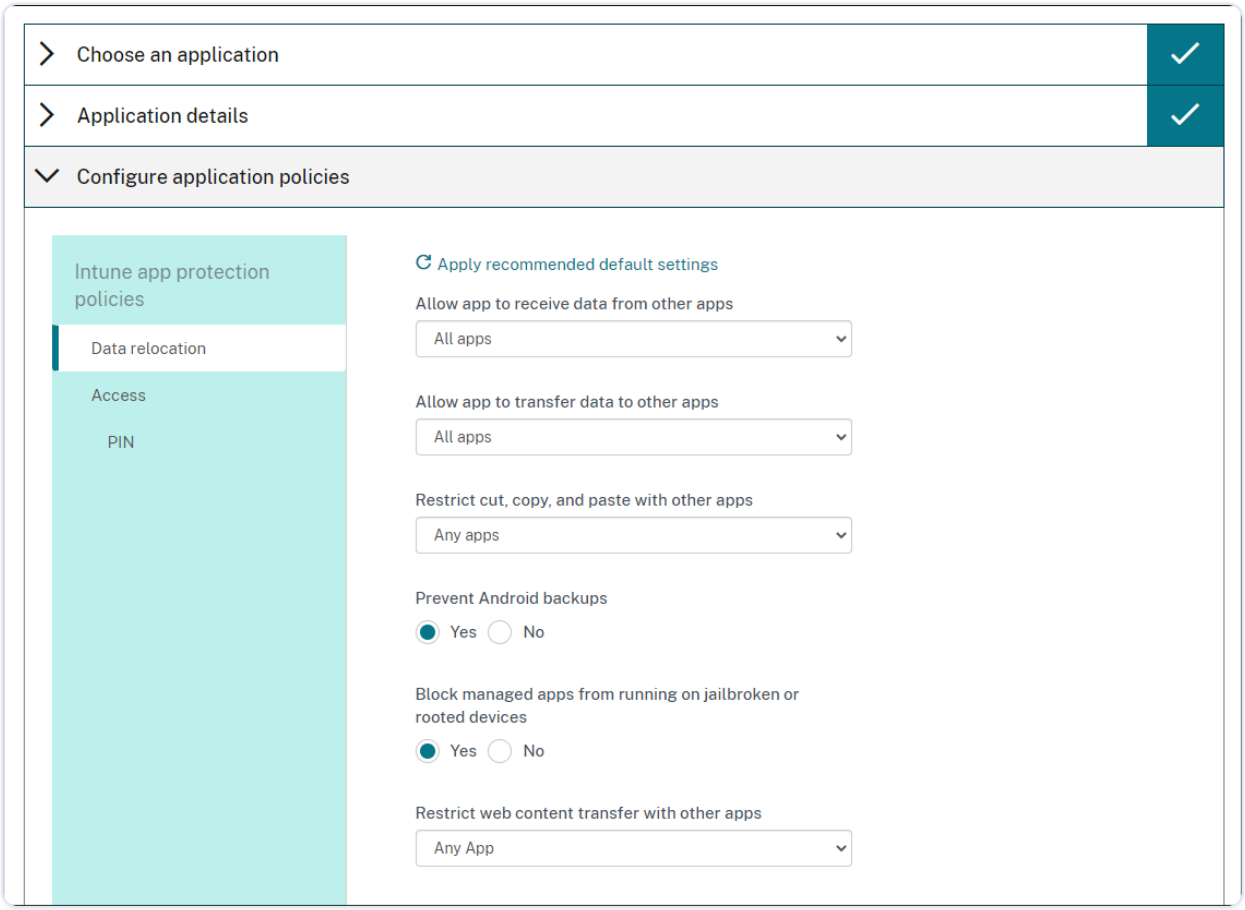


6. Citrixモバイル生産性向上アプリを検索して選択した場合、Micro VPNポリシーを構成できます。これらのポリシーを構成したら、**次へ**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. Intuneアプリ保護ポリシーを構成します。**次へ**をクリックします。



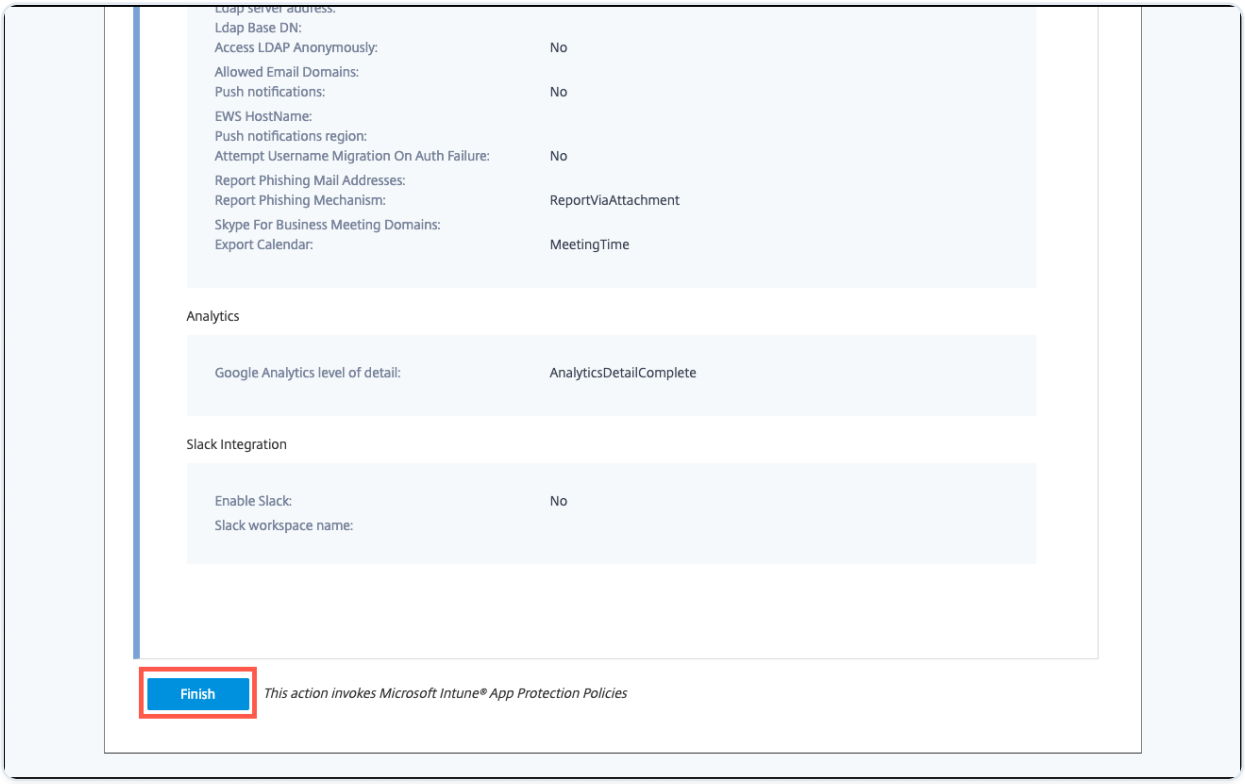
© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. アプリケーション設定を構成します。次の構成により、Citrix Endpoint Managementコンテナとintuneコンテナが相互にデータを転送できるようになります。

   - **アプリが他のアプリからデータを受信することを許可する: ポリシー管理対象アプリ**を選択します。
   - **アプリが他のアプリにデータを転送することを許可する: すべてのアプリ**を選択します。
   - **他のアプリとの切り取り、コピー、貼り付けを制限する: ポリシー管理対象アプリ**を選択します。

9. 保存されたデータのストレージリポジトリを構成します。**企業データを保存できるストレージサービスを選択**で、**LocalStorage**を選択します。
10. オプション: アプリのデータ再配置、アクセス、およびPINポリシーを設定します。**次へ**をクリックします。
11. アプリの概要を確認し、**完了**をクリックします。

    アプリの構成プロセスには数分かかる場合があります。プロセスが完了すると、アプリがライブラリに公開されたことを示すメッセージが表示されます。アプリはCitrix Endpoint ManagementおよびIntuneコンソールで利用できます。Citrix Endpoint Managementコンソールでは、アプリは新しいデリバリーグループの一部であり、パブリックアプリストアアプリとして識別されます。



12. アプリにユーザーグループを割り当てるには、**ユーザーの割り当て**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「ユーザーの割り当て」オプション(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems24.png)

13. 検索ボックスでユーザーグループを検索し、クリックして追加します。個々のユーザーを追加することはできません。

    「サブスクライバーの追加」オプション(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems27.png)

14. 必要なグループをすべて追加したら、Xをクリックしてウィンドウを閉じます。

    準備完了ステータス(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems29.png)

    ユーザーグループを追加する際にエラーが表示されることがあります。このエラーは、ユーザーグループがローカルのActive Directoryに同期されていない場合に発生します。

管理対象アプリ間で転送されるデータの種類を制御する

Citrix Endpoint Managementデバイスポリシーを使用して、Citrix Endpoint ManagementまたはIntuneコンテナ内の管理対象アプリ間で転送できるデータの種類を制御します。「企業」としてタグ付けされたデータのみを許可するように制限ポリシーを構成できます。データをタグ付けするには、アプリ構成ポリシーを構成します。

制限デバイスポリシーを構成するには：

1. Citrix Endpoint Managementコンソールで、**構成 > デバイスポリシー**をクリックします。
2. **デバイスポリシー**ページで、**追加**をクリックします。**新しいポリシーの追加**ページが表示されます。

   デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/configure-device-policies-add.png)

3. ポリシーのリストから**制限**をクリックします。
4. **ポリシー情報**ページで、ポリシーの名前と（オプションで）説明を入力します。**次へ**をクリックします。
5. iOSアプリのデバイスポリシーを作成するには、**プラットフォーム**ペインで**iOS**を選択します。
6. 「**セキュリティ - 許可**」で、「**管理対象外アプリの管理対象アプリからのドキュメント**」を「**オフ**」に設定します。この設定を「**オフ**」にすると、「**管理対象外アプリが管理対象連絡先を読み取る**」と「**管理対象アプリが管理対象外連絡先に書き込む**」も「**オフ**」に設定されます。「**次へ**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. 「**保存**」ボタンが表示されるまで「**次へ**」をクリックします。「**保存**」をクリックします。

各アプリのアプリ構成デバイスポリシーを構成します。

1. Citrix Endpoint Managementコンソールで、「**構成 > デバイスポリシー**」をクリックします。
2. 「**追加**」をクリックします。「**新しいポリシーの追加**」ページが表示されます。
3. ポリシーの一覧から「**アプリ構成**」をクリックします。
4. 「**ポリシー情報**」ページで、ポリシーの名前と（オプションで）説明を入力します。「**次へ**」をクリックします。
5. iOSアプリのデバイスポリシーを作成するには、「**プラットフォーム**」ペインで「**iOS**」を選択します。
6. 構成するアプリの識別子を選択します。
7. iOSアプリの場合、「**辞書コンテンツ**」に次のテキストを追加します。

```
<dict>

    <key>IntuneMAMUPN</key>

    <string>${user.userprincipalname}</string>

</dict>
```

8. 「**辞書を確認**」をクリックします。
9. 「**次へ**」をクリックします。
10. 「**保存**」をクリックします。

アプリとデバイスポリシーのデリバリーグループを構成する

1. Citrix Endpoint Managementコンソールで、「**構成 > デリバリーグループ**」をクリックします。
2. 「**Delivery Groups**」ページで、「**Add**」をクリックします。「**Delivery Group Information**」ページが表示されます。
3. 「**Delivery Group Information**」ページで、デリバリーグループの名前と(オプションで)説明を入力します。「**Next**」をクリックします。
4. 「**Assignments**」ページで、デリバリーグループの展開方法を指定します。「**In Citrix Endpoint Management**」または「**In Citrix Cloud**」を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デリバリーグループ構成画面(/en-us/citrix-endpoint-management/media/configure-delivery-groups-assignments.png)

5. 「**In Citrix Endpoint Management**」を選択した場合:

   - **ドメインの選択:** リストから、ユーザーを選択するドメインを選択します。
   - **ユーザーグループを含める:** 次のいずれかを実行します。

     - ユーザーグループのリストで、追加するグループをクリックします。選択したグループは「**Selected user groups**」リストに表示されます。
     - 選択したドメイン内のすべてのユーザーグループのリストを表示するには、「**Search**」をクリックします。
     - 検索ボックスにグループ名の全部または一部を入力し、「**Search**」をクリックしてユーザーグループのリストを絞り込みます。

   「**Selected user groups**」リストからユーザーグループを削除するには、次のいずれかを実行します。

     - 「**Selected user groups**」リストで、削除する各グループの横にある「**X**」をクリックします。
     - 選択したドメイン内のすべてのユーザーグループのリストを表示するには、「**Search**」をクリックします。リストをスクロールし、削除する各グループのチェックボックスをオフにします。
     - 検索ボックスにグループ名の全部または一部を入力し、「**Search**」をクリックしてユーザーグループのリストを絞り込みます。リストをスクロールし、削除する各グループのチェックボックスをオフにします。

6. 「**Next**」をクリックします。
7. 「**ポリシー**」ページで、作成した制限ポリシーとアプリ構成ポリシーを左から右へドラッグします。「**次へ**」をクリックします。
8. 「**アプリ**」ページで、配信したいアプリをページの左側から「**必須アプリ**」または「**オプションアプリ**」にドラッグします。「**次へ**」をクリックします。
9. オプションで、「**メディア**」ページ、「**アクション**」ページ、および「**登録**」ページで設定を構成します。または、各ページのデフォルトを受け入れて「**次へ**」をクリックします。
10. 「**概要**」ページで、デリバリーグループの設定を確認し、「**保存**」をクリックしてデリバリーグループを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Intuneコンソールでアプリを公開する際、「**アプリの管理を強制する**」を選択します。監視対象外のデバイスのユーザーには、アプリの管理を許可するよう求められます。ユーザーがプロンプトを受け入れると、アプリはデバイスで管理されます。ユーザーがプロンプトを拒否すると、アプリはデバイスで利用できなくなります。

Citrix Secure Mailを構成する

「

注：

」:

IntuneとのCitrix Secure Mail統合は非推奨となり、今後のリリースで削除されます。詳細については、Secure Mailの新機能を参照してください。

Citrix Secure Mailは、さまざまな構成をサポートするようになりました。オンプレミスのExchange Serverに接続するIntune MAMコンテナにCitrix Secure Mailをラップできます。Citrix Secure Mailをホスト型ExchangeまたはOffice 365アカウントに接続できます。ただし、このリリースでは証明書ベースの認証はサポートされていないため、代わりにLDAPを使用してください。

「

重要：

」:

MDXモードでCitrix Secure Mailを使用するには、Citrix Endpoint Management MDM+MAMを使用する必要があります。

Citrix Secure Mailは、ユーザー名も自動的に入力します。この機能を有効にするには、まず以下のカスタムポリシーを構成する必要があります。

1. Citrix Endpoint Managementコンソールから、「**設定 > サーバープロパティ**」に移動し、「**追加**」をクリックします。
2. リストで「**カスタムキー**」をクリックし、「**キー**」フィールドに `xms.store.idpuser_attrs` と入力します。
3. 値を「**true**」に設定し、「**表示名**」に `xms.store.idpuser_attrs` と入力します。「**保存**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「**クライアントプロパティ**」をクリックし、次に「**追加**」をクリックします。
5. 「**カスタムキー**」を選択し、次に「**キー**」フィールドに「**SEND_LDAP_ATTRIBUTES**」と入力します。
6. 「**値**」フィールドに`userPrincipalName=${user.userprincipalname},email=${user.mail},displayname=${user.displayname},sAMAccountName=${user.samaccountname},aadupn=${user.id_token.upn},aadtid=${user.id_token.tid}`と入力します。説明を入力し、次に「**保存**」をクリックします。

   以下の手順は、iOSデバイスにのみ適用されます。

7. 「**構成 > デバイスポリシー**」に移動し、「追加」をクリックし、次に「**アプリ構成**」ポリシーを選択します。
8. ポリシー名を入力し、次に「**次へ**」をクリックします。

   識別子リストで「**新規追加**」をクリックします。表示されるテキストボックスに、Citrix Secure Mailアプリのバンドルを入力します。

9. 「**辞書**」コンテンツボックスに、以下のテキストを入力します。

```
&lt;dict>



&lt;key>XenMobileUserAttributes&lt;/key>



&lt;dict>



&lt;key>userPrincipalName&lt;/key>



&lt;string>${user.userprincipalname}&lt;/string>



&lt;key>email&lt;/key>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
&lt;string>${user.mail}&lt;/string>

&lt;key>displayname&lt;/key>

&lt;string>${user.displayname}&lt;/string>

&lt;key>sAMAccountName&lt;/key>

&lt;string>${user.samaccountname}&lt;/string>

&lt;key>aadupn&lt;/key>

&lt;string>${user.id_token.upn}&lt;/string>

&lt;key>aadtid&lt;/key>

&lt;string>${user.id_token.tid}&lt;/string>

&lt;/dict>

&lt;key>IntuneMAMUPN&lt;/key>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
&lt;string>${user.id_token.upn}&lt;/string>



&lt;/dict>
```

10. 「**Windowsデスクトップ/タブレット**」チェックボックスをオフにし、次に「**次へ**」をクリックします。
11. ポリシーを展開するユーザーグループを選択し、次に「**保存**」をクリックします。

トラブルシューティング

一般的な問題

問題: アプリを開くと、以下のエラーメッセージが表示されます: アプリポリシーが必要です。

解決策: Microsoft Graph APIでポリシーを追加します。

問題: ポリシーの競合が発生しています。

解決策: アプリごとに許可されるポリシーは1つだけです。

問題: アプリが内部リソースに接続できません。

解決策: 正しいファイアウォールポートが開いていること、正しいテナントIDを使用していることなどを確認してください。

NetScaler Gatewayに関する問題

次の表に、NetScaler Gatewayの構成に関する一般的な問題とその解決策を示します。トラブルシューティングのために、以下の手順でログを有効にして確認してください。

1. コマンドラインインターフェイスで、次のコマンドを実行します: `set audit syslogParams -logLevel ALL`
2. シェルから `tail -f /var/log/ns.log` を使用してログを確認します

問題	解決策
Azure上のGatewayアプリに構成する必要がある権限が利用できません。	適切なIntuneライセンスが利用可能か確認してください。manage.windowsazure.comポータルを使用して、権限を追加できるか試してくだ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

問題	解決策
	さい。問題が解決しない場合は、Microsoftサポートに連絡してください。
NetScaler Gatewayが `login.microsoftonline.com` および `graph.windows.net` に到達できません。	NSシェルから、次のMicrosoftウェブサイトに到達できるか確認してください: `curl -v -k https://login.microsoftonline.com`。次に、NetScaler GatewayでDNSが構成されていること、およびファイアウォール設定が正しいこと（DNS要求がファイアウォールでブロックされている場合）を確認してください。
OAuthActionを構成した後、ns.logにエラーが表示されます。	Intuneライセンスが有効になっていること、およびAzure Gatewayアプリに適切な権限が設定されていることを確認してください。
Sh OAuthAction コマンドで OAuth ステータスが完了と表示されない。	Azure Gateway App の DNS 設定と構成された権限を確認してください。
Android または iOS デバイスに二要素認証のプロンプトが表示されない。	Dual Factor Device ID logonSchema が認証仮想サーバーにバインドされているか確認してください。

OAuth エラーの条件とステータス

ステータス	エラー条件
完了	成功
AADFORGRAPH	無効なシークレット、URL が解決されない、接続タイムアウト
MDMINFO	*manage.microsoft.com がダウンしているか、到達不能です
GRAPH	Graph エンドポイントがダウンしているか、到達不能です
CERTFETCH	DNSエラーのため、「トークンエンドポイント: `https://login.microsoftonline.com`」と通信できません。この構成を検証するに

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステータス	エラー条件
	は、シェルに移動して「`curl https://login.microsoftonline.com`」と入力してください。このコマンドは検証される必要があります。

制限事項

以下の項目は、Citrix Endpoint ManagementでMEMを使用する際のいくつかの制限事項について説明しています。

- CitrixとIntuneを使用してマイクロVPNをサポートするアプリを展開する場合：ユーザーがダイジェストサイトにアクセスするためにユーザー名とパスワードを入力すると、資格情報が有効であってもエラーが表示されます。
- **スプリットトンネル**を**オン**から**オフ**に変更し、現在のゲートウェイセッションが期限切れになるのを待った後：ユーザーがフルVPNモードで内部サイトを起動するまで、外部トラフィックはNetScaler Gatewayを経由せずに直接通過します。
- Open-inポリシーを**管理対象アプリ**のみから**すべてのアプリ**に変更した後、ユーザーはCitrix Secure Mailを閉じて再起動するまで、管理対象外のアプリでドキュメントを開くことができません。
- フルVPNモードでスプリットトンネリングが**オン**の場合、スプリットDNSがローカルからリモートに変更されると、内部サイトの読み込みに失敗します。

既知の問題

mVPNポリシーの**HTTP/HTTPSリダイレクトを有効にする（SSOあり）**が無効になっている場合、Citrix Secure Mailは機能しません。

サードパーティの既知の問題

Android版Citrix Secure Mailで、ユーザーが**新しいイベントを作成**をタップすると、新しいイベント作成ページが表示されません。

CitrixとIntuneを使用してマイクロVPNをサポートするiOS版Citrix Secure Mailを展開する場合：ユーザーがアプリをバックグラウンドに移動したときにCitrix Secure Mailの画面を隠すアプリポリシーが適用されません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

オンボーディングとリソースのセットアップ

Citrix、Citrix Cloud、またはCitrix Endpoint Managementを初めてご利用になる場合は、この記事がオンボーディングのガイドとなります。ワークフローと、開始するために必要な詳細について説明します。

- **どこから始めればよいですか？**
  - Citrix Endpoint Managementサブスクリプションを購入していない場合は、「新規Citrixのお客様向け」を参照してください。
  - Citrix Endpoint Managementサブスクリプションをお持ちの場合は、「管理ボタンが利用可能な場合」にスキップしてください。
  - Citrix Endpoint Managementサイトがプロビジョニングされている場合は、「認証の構成」にスキップしてください。
- **構成の順序は重要ですか？** この記事では、推奨される構成シーケンスに従っています。異なる順序で作業することもできます。Citrix Endpoint Managementコンソールは、「プロビジョニング後にセットアップ」などのメッセージを通じて、前提条件が不足しているかどうかを通知します。
- **オンボーディング後に何をすればよいですか？** この記事で説明されているオンボーディングとリソースの構成を完了したら、Citrix Endpoint Managementコンソールで構成を続行してください。次のステップについては、「デバイスの登録とリソースの配信の準備」を参照してください。

新規Citrix®のお客様向け

Citrix Endpoint Managementを初めて利用するCitrix Cloudのお客様向け：

Citrix Endpoint Managementサブスクリプションをすでに購入している場合は、「管理ボタンが利用可能な場合」にスキップしてください。

Citrix Cloudアカウントをまだセットアップしていない場合は、「Citrix Cloudへのサインアップ」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Cloudアカウントをすでにセットアップしているが、Citrix Endpoint Managementを購入していない場合は、サービスデモをリクエストしてください。

1. Citrix Cloud管理者資格情報を使用してCitrix Cloudアカウントにサインインします。Citrix Cloudのホームページが表示されます。

   すべてのCitrix Cloud管理者アカウントは次のように作成されます。

   - Citrix Cloud管理者は、デフォルトでCitrix Endpoint Management管理者です。
   - 顧客アクセス権限で作成されたCitrix Cloud管理者は、Citrix Endpoint Managementを管理するために、Citrix Endpoint Managementが選択されている必要があります。

2. Citrix Cloudのホームページで、Citrix Endpoint Managementサービスタイルを見つけて、**Request Demo**をクリックします。
3. デモリクエストフォームに記入して送信します。Citrix Endpoint Managementサービスタイルのボタンが**Demo Requested**に変わります。

リクエストが処理される前にCitrix Endpoint Managementサービスタイルをクリックすると、担当者またはパートナーに連絡するよう促す画面が表示されます。Citrixの営業担当者が、サービスに関する詳細情報を提供できます。

トライアルを待っている間に、システム要件を確認して、Citrix Endpoint Managementの展開に備えてください。CitrixがCitrix Endpoint Managementソリューションをホストおよび提供しますが、一部の通信およびポート要件はユーザーが処理する必要があります。

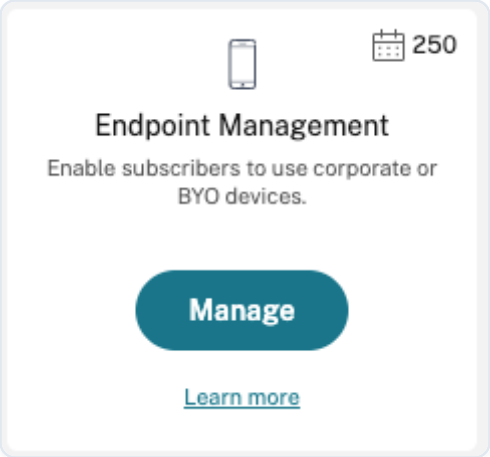
次のセクションに進みます。

Manageボタンが利用可能になったら

このビデオは、オンボーディングについて説明します。

<iframe src="https://www.youtube.com/embed/ycFLYxn7aII" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Citrix Endpoint Managementサービスが利用可能になると、Citrix Endpoint Managementサービスタイルのボタンが**Manage**に変わります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



セットアップを開始するには：

1. Citrix Cloud管理者資格情報を使用して、Citrix Cloudアカウントにサインインします。
2. Citrix Endpoint Managementタイルで**Manage**をクリックし、Citrix Endpoint Managementコンソールにアクセスします。
3. サイト名を入力し、リージョンを選択します。その後、**保存して続行**を選択します。

サイト名とリージョン(/en-us/citrix-endpoint-management/media/onboard-site-region.png)

注:

許可するIPを要求するには、Citrixサポート担当者にお問い合わせください。

Citrix Endpoint Managementコンソールが開き、スイートをプロビジョニング中であること、およびプロビジョニング中は一部のCitrix Endpoint Management機能がロックされることを示すメッセージが表示されます。

1. **ようこそ**画面で、**セットアップの開始**をクリックします。
2. 管理するエンドポイントを選択し、**保存**をクリックします。コンソールでエンドポイントを表示または非表示にするには、いつでもエンドポイントを追加またはクリアできます。エンドポイントの表示/非表示は、構成には影響しません。

管理するエンドポイント(/en-us/citrix-endpoint-management/media/onboard-select-endpoints.png)

プロビジョニングが完了したら、メールを送信します。

リソースセンター

リソースセンターアイコン(/en-us/citrix-endpoint-management/media/resource-center-icon.png) **リソースセンター**アイコンをクリックして、コンソールを離れることなくハウツービデオを視聴できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プロビジョニング中

Citrix Endpoint Managementのプロビジョニング中に、構成を開始できます。

リソースの場所を構成する

Citrix Endpoint ManagementのLightweight Directory Access Protocol (LDAP)接続を構成する前に、リソースの場所が必要です。リソースの場所には、サブスクライバーにクラウドサービスを提供するために必要なリソースが含まれています。ドメインごとに1つのリソースの場所が必要です。詳細については、Citrix Cloudの記事「リソースの場所」を参照してください。

試用版を待っている間に、システム要件を確認して、Citrix Endpoint Managementの展開に備えてください。CitrixがCitrix Endpoint Managementソリューションをホストおよび提供しますが、一部の通信およびポート要件が必要です。このセットアップは、Citrix Endpoint Managementインフラストラクチャを Active Directoryなどの企業サービスに接続します。提供する必要がある情報は、オンボーディングハンドブックの「Citrix Endpoint Management Trial Sales Engineer engagement」に記載されています。

試用版へのアクセスが承認されると、**Citrix Endpoint Management**のボタンが**管理**に変わります。**管理**をクリックして、Citrix Endpoint Managementコンソールを開きます。

認証の構成

サイトがプロビジョニングされたら、引き続き構成を進めることができます。グループ、ユーザーアカウント、および関連プロパティをインポートするために、クラウドホスト型IDプロバイダー（IdP）またはLightweight Directory Access Protocol（LDAP）を設定することをお勧めします。

IdPを構成するには

Citrix Endpoint Managementは、Azure Active Directory、Okta、オンプレミスNetScaler Gatewayなどの IDプロバイダーとの認証をサポートしています。

Citrix CloudでIdPを構成し、Citrix Endpoint Management用に設定するには：

- Citrix Cloudを介したAzure Active Directoryによる認証
- Citrix Cloudを介したOktaによる認証
- Citrix Cloudを介したオンプレミスNetScaler Gatewayによる認証

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LDAPを構成するには

Citrix Endpoint Managementで、ドメインベースの認証のために1つ以上のLDAP準拠ディレクトリへの接続を構成できます。Citrix Endpoint Managementは、LDAPにネストされたグループをサポートしています。ネストされたグループは、現地時間の午前12時に毎日同期されます。

LDAPの構成の一部として、少なくとも1つのCloud Connectorをインストールする必要があります。

概要については、このビデオをご覧ください。

<iframe src="https://www.youtube.com/embed/LJ6IDZyfO8s" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
LDAP をセットアップするには:

1. **設定**ページで、**LDAP**タイルまでスクロールし、**セットアップ**をクリックします。
2. 画面の指示に従って、Cloud Connector をダウンロードしてインストールします。Cloud Connector は、Citrix Cloud とリソース間の通信を有効にするために必要です。詳しくは、「Citrix Cloud Connector」を参照してください。

LDAP 構成があり、Azure AD または Okta を ID プロバイダーとして追加した場合、Citrix Endpoint Management は、Citrix Endpoint Management データベース内の Active Directory グループの IdP 固有の情報を同期します。この構成は、既存のデリバリーグループとユーザー登録には影響しません。ただし、後で Citrix Endpoint Management に LDAP 設定を追加することはできません。詳しくは、「ID プロバイダー認証」を参照してください。

登録後に**ドメインエイリアス**または**ユーザー検索条件**の設定を変更した場合、ユーザーは再登録する必要があります。LDAP 構成について詳しくは、「ドメインまたはドメインとセキュリティトークン認証」を参照してください。

LDAP のセットアップ後、認証構成を続行するか、特定のプラットフォームをセットアップできます。

NetScaler Gateway の構成

Citrix Endpoint Management と統合すると、NetScaler Gateway は内部ネットワークとリソースへのリモートデバイスアクセスを提供します。

Citrix Endpoint Management は、次のシナリオで NetScaler Gateway を必要とします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 基幹業務アプリの内部ネットワークリソースへのアクセスにマイクロ VPN が必要です。これらのアプリは Citrix MDX テクノロジーでラップされています。マイクロ VPN は、内部バックエンドインフラストラクチャに接続するために NetScaler Gateway を必要とします。
- Citrix Endpoint Management を使用してアプリを管理する予定です (MAM または MDM+MAM)。デバイスのみを管理する場合 (MDM) は、NetScaler Gateway は必要ありません。
- Citrix Endpoint Management を Microsoft Endpoint Manager と統合する予定です。(オンプレミスの NetScaler Gateway が必要です。)

概要については、このビデオをご覧ください。

<iframe src="https://www.youtube.com/embed/r79jdnVznE0" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
次の表は、オンプレミスの NetScaler Gateway ソリューションでサポートされる機能の概要です。

サポートされる機能	オンプレミス版NETSCALER GATEWAY
シトリックス セキュアメール (STA)*	はい
トンネル化 - Web SSO (Webシングルサインオン)	はい
フルVPN (iOS向けCitrixモバイル生産性向上アプリでは利用不可)	はい
アプリごとのVPN	はい
モバイルシングルサインオン (アクセス制御)	いいえ
高可用性	はい**
マルチPOP展開	はい***
プロキシサポート	はい
スプリットトンネリング	はい
スプリットDNS	はい

Citrix Cloud セキュアチケット機関 (STA) サービス構成

© 1997–2026 Citrix Systems, Inc. All rights reserved.

** オンプレミス構成

*** グローバルサーバー負荷分散構成

オンプレミスNetScaler Gatewayのユースケース

以下の場合は、Citrix Endpoint Managementで1つ以上のオンプレミスNetScaler Gatewayアプライアンスを使用します。

- アプリごとのVPN機能が必要な場合。
- フルトンネリング、スプリットトンネリング、リバーススプリットトンネリング、またはスプリットDNSが必要な場合。内部ネットワーク内のリソースへのクライアント証明書またはエンドツーエンドSSLを使用する接続には、フルVPNトンネルをお勧めします。
- Microsoft Endpoint ManagerとのCitrix Endpoint Management統合を使用する場合。

オンプレミスのNetScaler Gatewayの使用には、かなりの構成とメンテナンスが必要です。LDAPとNetScaler GatewayをCitrix Endpoint Managementコンソールで構成した後、そのコンソールからスクリプトをエクスポートします。その後、NetScaler Gatewayでスクリプトを実行します。

1. **設定**ページで、**NetScaler Gateway**タイルまでスクロールし、**セットアップを開始**をクリックします。
2. 種類として**NetScaler Gateway（オンプレミス）**を選択します。
3. 画面の指示に従ってください。詳細については、「Citrix Endpoint Managementで使用するためのオンプレミスNetScaler Gatewayの構成」を参照してください。

通知サーバーの構成

通知を送信するには、ゲートウェイと通知サーバーを構成する必要があります。通知サーバーは、エンドユーザーと管理者間の接続性と通信の可能性を確保します。Citrix Endpoint Managementで通知サーバーをセットアップするには、「通知」を参照してください。

Appleデバイス用のApple Push Notification service（APNs）証明書の構成

Citrix Endpoint Managementでは、Appleデバイスを登録および管理するために、AppleからのApple Push Notification service（APNs）証明書が必要です。Citrix Secure Mail for Appleのプッシュ通知を使用する予定がある場合も、Citrix Endpoint ManagementにはAPNs証明書が必要です。Citrix Endpoint ManagementとAPNsの詳細については、「iOS用Citrix Secure Mailのプッシュ通知」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Appleから証明書を取得するには、Apple IDと開発者アカウントが必要です。詳細については、Apple Developer ProgramのWebサイトを参照してください。

概要については、このビデオをご覧ください。

<iframe src="https://www.youtube.com/embed/pVj37DNBxMM" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Citrix証明書署名要求を使用してAPNsを構成するには:

1. **設定**ページで、**Apple**タイルを展開します。
2. **APNs証明書**タイルで、**セットアップ**をクリックし、画面の指示に従ってください。

詳細については、「証明書と認証」を参照してください。

Android Enterprise を構成する

デリバリーグループを作成し、Cloud Library を介してユーザーをデリバリーグループに割り当てると、Citrix Endpoint Management は完全に構成されます。これ以降、Citrix Endpoint Management の管理は Citrix Cloud 内で行われます。統合されたインターフェイスにより、Citrix Cloud と Citrix Endpoint Management の切り替えが簡素化されます。

Citrix Endpoint Management の Android Enterprise は、Google Play または Google Workspace のいずれかを使用してセットアップできます。

1. **組織で Google Workspace を使用していない場合:** マネージド Google Play を使用して、Citrix を EMM プロバイダーとして登録できます。マネージド Google Play を使用する場合、デバイスとエンドユーザー向けにマネージド Google Play アカウントをプロビジョニングします。マネージド Google Play アカウントはマネージド Google Play へのアクセスを提供し、ユーザーが利用可能にした仕事用アプリをインストールして使用できるようにします。組織がサードパーティの ID サービスを使用している場合、マネージド Google Play アカウントを既存の ID アカウントとリンクできます。

   このタイプのエンタープライズはドメインに紐付けられていないため、単一の組織に対して複数のエンタープライズを作成できます。たとえば、組織内の各部門または地域は、異なるエンタープライズとして登録できます。このセットアップにより、異なるエンタープライズを使用して、個別のデバイスとアプリのセットを管理できます。
2. **組織がすでに Google Workspace を使用してユーザーに Google アプリへのアクセスを提供している場合:** Google Workspace を使用して、Citrix を EMM として登録できます。組織が Google Workspace を使用している場合、既存のエンタープライズ ID とユーザー向けの既存の Google アカウントを持っています。Google Workspace で Citrix Endpoint Management を使

© 1997–2026 Citrix Systems, Inc. All rights reserved.

用するには、LDAP ディレクトリと同期し、Google Directory API を使用して Google から Google アカウント情報を取得します。

このタイプのエンタープライズは既存のドメインに紐付けられています。そのため、各ドメインは1つのエンタープライズしか作成できません。Citrix Endpoint Management にデバイスを登録するには、各ユーザーが既存の Google アカウントで手動でサインインする必要があります。このアカウントにより、ユーザーはマネージド Google Play および Google Workspace プランを通じて他の Google サービスにアクセスできます。

概要については、このビデオをご覧ください。

<iframe src="https://www.youtube.com/embed/O_SpR-Eds9k" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
開始するには：

1. 「**設定**」ページで、「**Android**」タイルを展開します。
2. 「**Android Enterprise**」タイルで、「**セットアップ**」をクリックします。
3. ユーザーに Google アプリケーションへのアクセスを提供する方法に応じて、**Google Play**または**G Suite**を選択します。 以前に Android Enterprise プラットフォームを Google Play で構成した場合、UI は再登録のために Google Play ストアに移動します。**再登録**をクリックし、CEM コンソールに戻ってページを更新します。
4. 画面の指示に従います。

参照：

- 「Android Enterpriseアカウントを作成する」(/ja-jp/citrix-endpoint-management/device-management/android/legacy-android-enterprise-for-g-suite-customers.html)

Firebase Cloud Messaging を構成する

Citrixでは、AndroidデバイスがCitrix Endpoint Managementに接続する方法とタイミングを制御するために、Firebase Cloud Messaging (FCM)を使用することをお勧めします。Citrix Endpoint Managementは、FCMが有効になっているAndroidデバイスに接続通知を送信します。セキュリティアクションまたは展開コマンドは、プッシュ通知をトリガーして、ユーザーにCitrix Endpoint Managementサーバーへの再接続を促します。詳細については、「Firebase Cloud Messaging」(/ja-jp/citrix-endpoint-management/device-management/android/firebase-cloud-messaging.html)を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Endpoint Manager と統合する

Citrix Endpoint ManagementとMicrosoft Endpoint Managerの統合により、Microsoft Edgeブラウザーなどの Microsoft Intune対応アプリにCitrix Endpoint ManagementのマイクロVPNの価値が追加されます。

Citrix Endpoint ManagementとMEMの統合により、企業は独自の基幹業務アプリをIntuneおよびCitrixでラップすることもできます。アプリのラッピングは、Intuneモバイルアプリ管理 (MAM) コンテナ内でマイクロVPN機能を提供します。Citrix Endpoint ManagementのマイクロVPNにより、アプリはオンプレミスリソースにアクセスできます。Office 365アプリ、基幹業務アプリ、およびCitrix Secure Mailを1つのコンテナで管理および配信できます。単一のコンテナは、究極のセキュリティと生産性を提供します。

- Citrix Cloud管理者は、デフォルトでCitrix Endpoint Management管理者です。
- 顧客アクセスで作成されたCitrix Cloud管理者は、Citrix Endpoint Managementを管理するためにCitrix Endpoint Managementが選択されている必要があります。

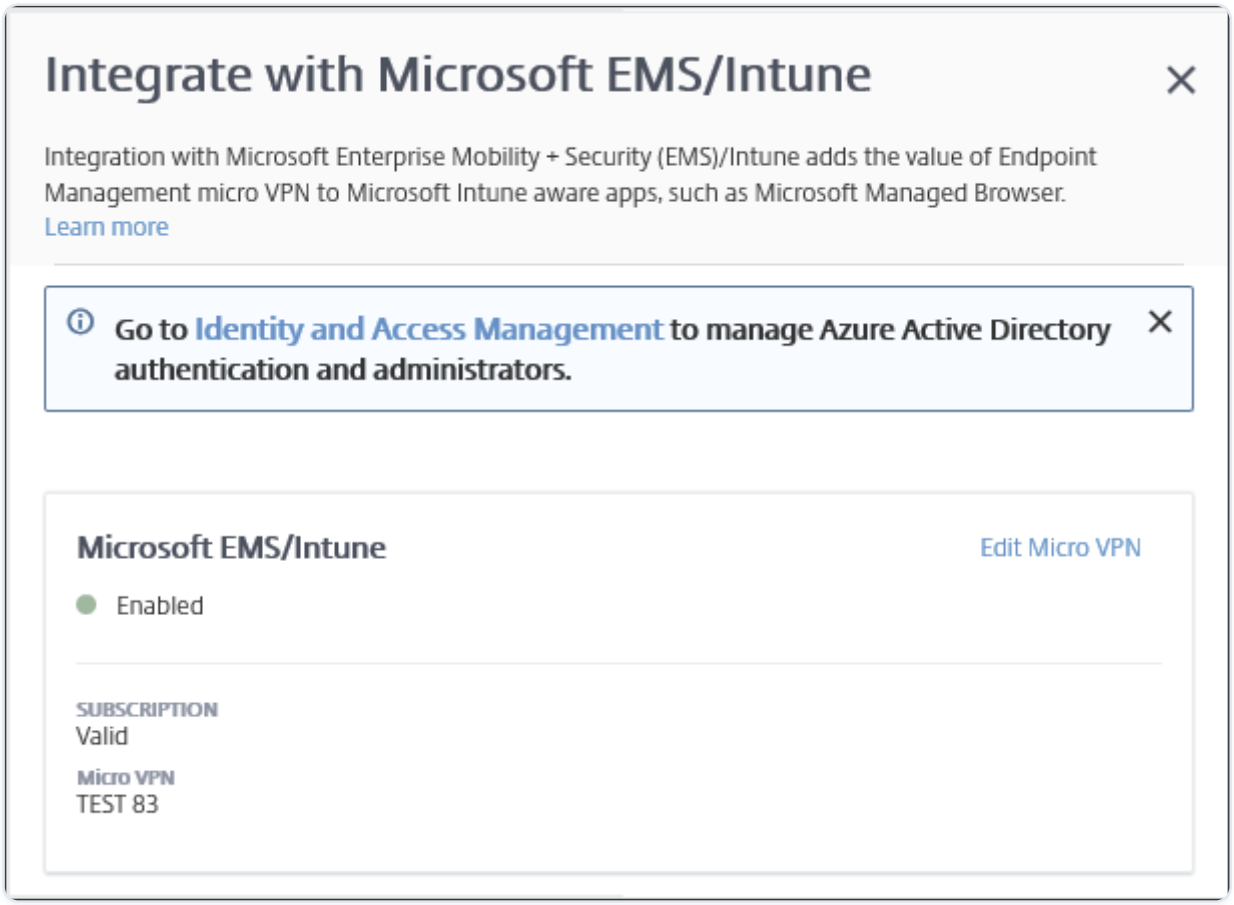
Citrix Endpoint Managementコンソールでは、ユーザーの役割とメンバーシップのみを変更できます。役割をいつでも変更するには、Citrix CloudダッシュボードからCitrix Endpoint Managementコンソールにアクセスします。**Manage**タブに移動し、**Users**をクリックします。特定のユーザーを選択し、**Edit**をクリックして役割を変更します。詳細については、「RBACで役割を構成する」(/ja-jp/citrix-endpoint-management/users/rbac-roles-and-permissions.html)を参照してください。

MEMと統合するには、「Citrix Endpoint ManagementとMicrosoft Endpoint Managerの統合」(/ja-jp/citrix-endpoint-management/integration-with-mem.html)を参照してください。

Citrix Cloudでの構成が完了したら、次のようにCitrix Endpoint Managementコンソールに戻ります。Citrix Cloudの**Home**ページに移動し、**Citrix Endpoint Management**タイルで**Manage**をクリックします。その後、Azure Active DirectoryアカウントでCitrix Endpoint Managementにサインインしたかどうかを確認できます。

1. **Settings**ページで、**Integrate with Microsoft EMS/Intune**タイルまでスクロールします。
2. **See more**をクリックします。UIは、接続が正常に有効になったかどうかを示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



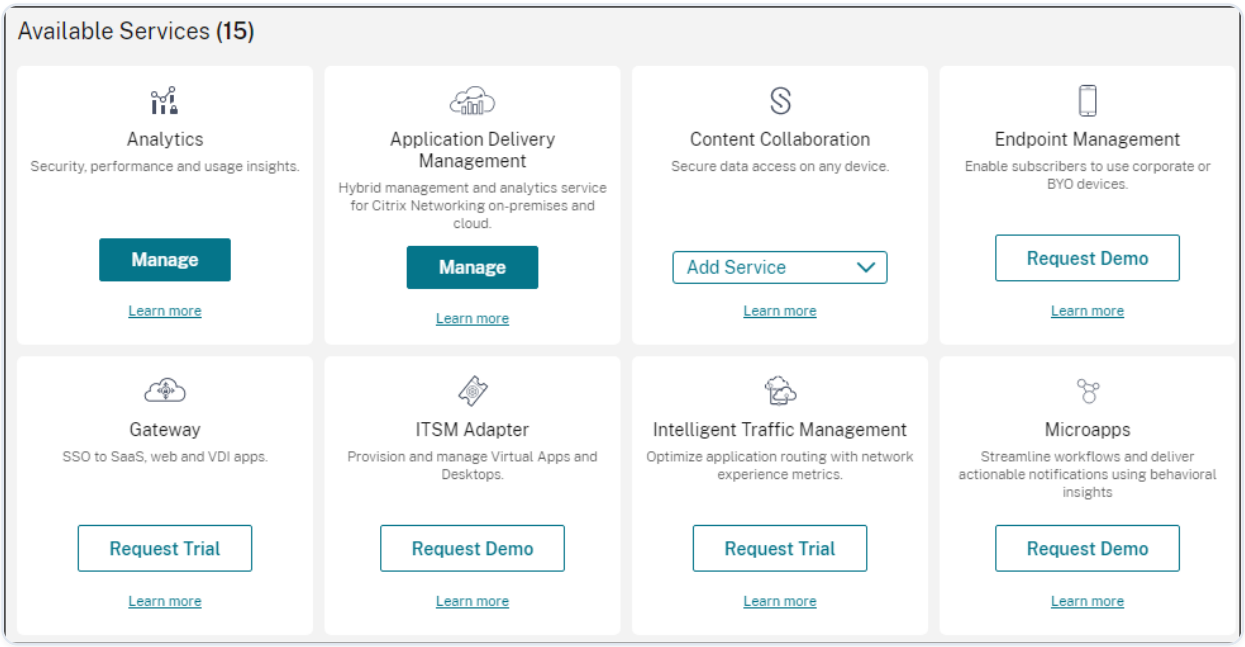
Citrix Cloudコンソールでは、ユーザー名やパスワードの変更、ローカルユーザーの削除や編集もできます。詳細については、「IDおよびアクセス管理」(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management.html)を参照してください。

既存のShareFileアカウントをCitrix Cloudにリンクする

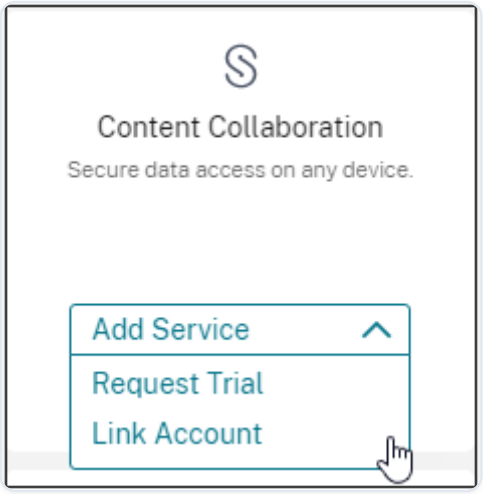
Citrix Cloudにサインアップする前にShareFileアカウントをお持ちだった場合、そのアカウントをCitrix Cloudにリンクする必要があります。アカウントをリンクするには、メールアドレスがShareFileアカウントの管理者である必要があります。続行する準備ができたら、`<https://onboarding.cloud.com>`に移動します。

1. ログイン後、次のような画面が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

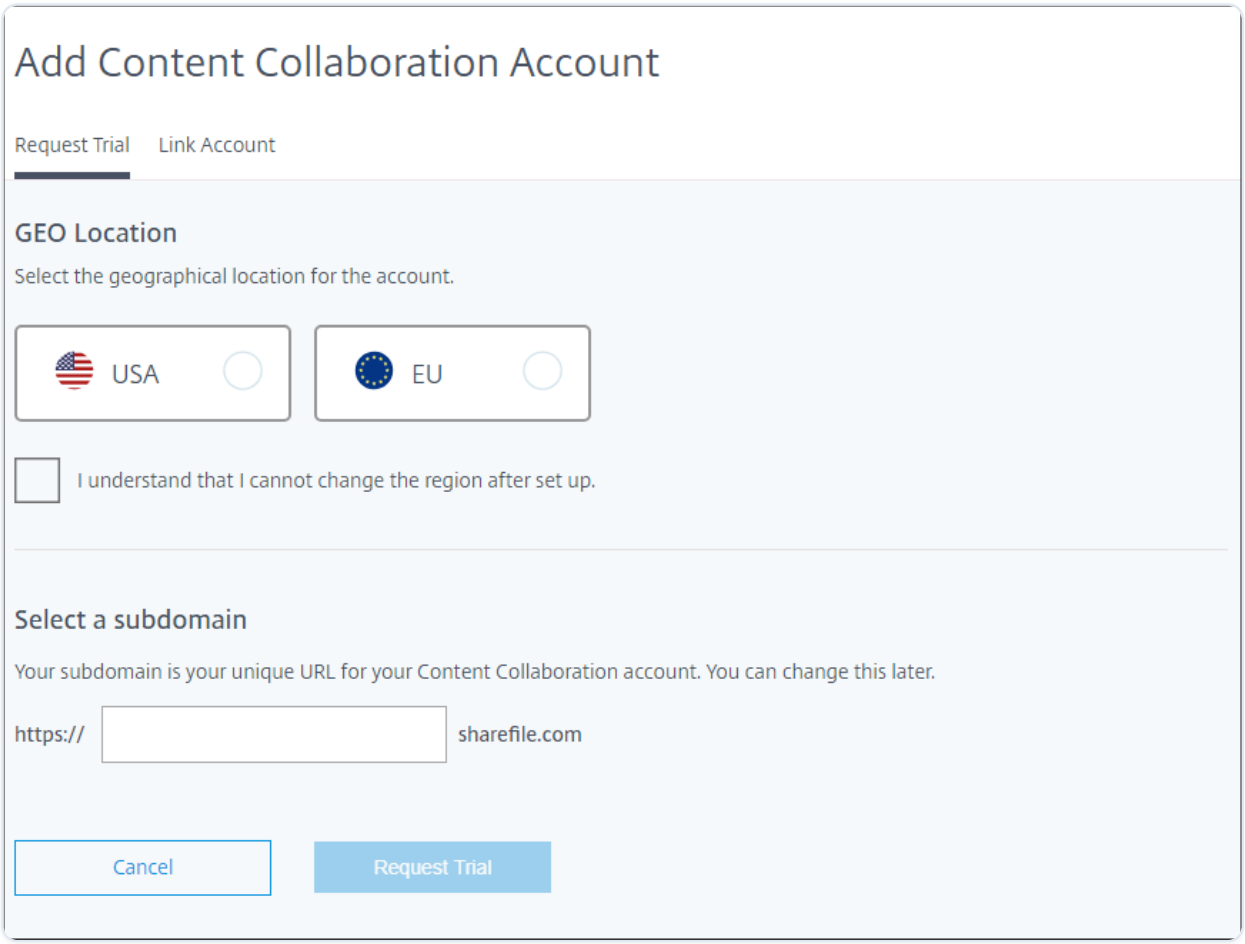


2. **ShareFile**タイルで、**アカウントのリンク**を選択します。



3. ShareFileアカウントを確認すると、次のページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. **アカウントのリンク**タブをクリックしてプロセスを完了します。Citrix CloudからShareFileアカウントをすぐに管理できます。

Cloud Connectors の規模とサイズに関する考慮事項

Citrix Endpoint Management サービスをサイジングとスケーラビリティの観点から評価する際は、特定の要件に合わせて Cloud Connectors の構成を調査し、テストしてください。Cloud Connector はデバイス登録時のみ負荷がかかります。マシンのサイズが不足していると、システムパフォーマンスに悪影響を及ぼす可能性があります。

Citrix® では、リソースロケーションごとに2つの Cloud Connector が必要です。Cloud Connector は、他のコンポーネントや製品と責任を共有しない専用サーバーにインストールしてください。当社のテストでは、Cloud Connector はHAセットで展開されました（**ロードバランスされていません**）。

テスト構成

- 専用の Windows Server 2019、2 vCPU、4 GB メモリを2台
- Android および iOS デバイスの MDM+MAM への登録。8時間で均等に分割。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Management は、1,000台のデバイスあたり1時間あたり125台のデバイスを登録するように構成されています。
  - 1,000台のデバイス（1時間あたり125台のデバイス登録）
  - 5,000台のデバイス（1時間あたり625台のデバイス登録）
  - 10,000台のデバイス（1時間あたり1250台のデバイス登録）
  - 20,000台のデバイス（1時間あたり2500台のデバイス登録）

テスト結果

クラウドコネクタ	1,000台のデバイス	5,000台のデバイス	10,000台のデバイス	20,000台のデバイス
CPU平均	2%	2%	4%	4%
CPU最大	8%	8%	10%	11%
メモリ平均	73%	73%	75%	75%
最大メモリ	76%	76%	76%	79%

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスの登録とリソースの配信の準備

重要:

続行する前に、オンボーディングとリソースのセットアップに記載されているすべてのタスクを完了していることを確認してください。

今後の変更についてユーザーに情報を提供してください。Citrixユーザー導入キットへようこそを参照してください。

Citrix Endpoint Managementは、さまざまな登録オプションをサポートしています。この記事では、サポートされているすべてのデバイスを登録できるようにするために必要な基本的なセットアップについて説明します。次の図は、基本的なセットアップをまとめたものです。



サポートされているデバイスのリストについては、サポートされているデバイスのオペレーティングシステムを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

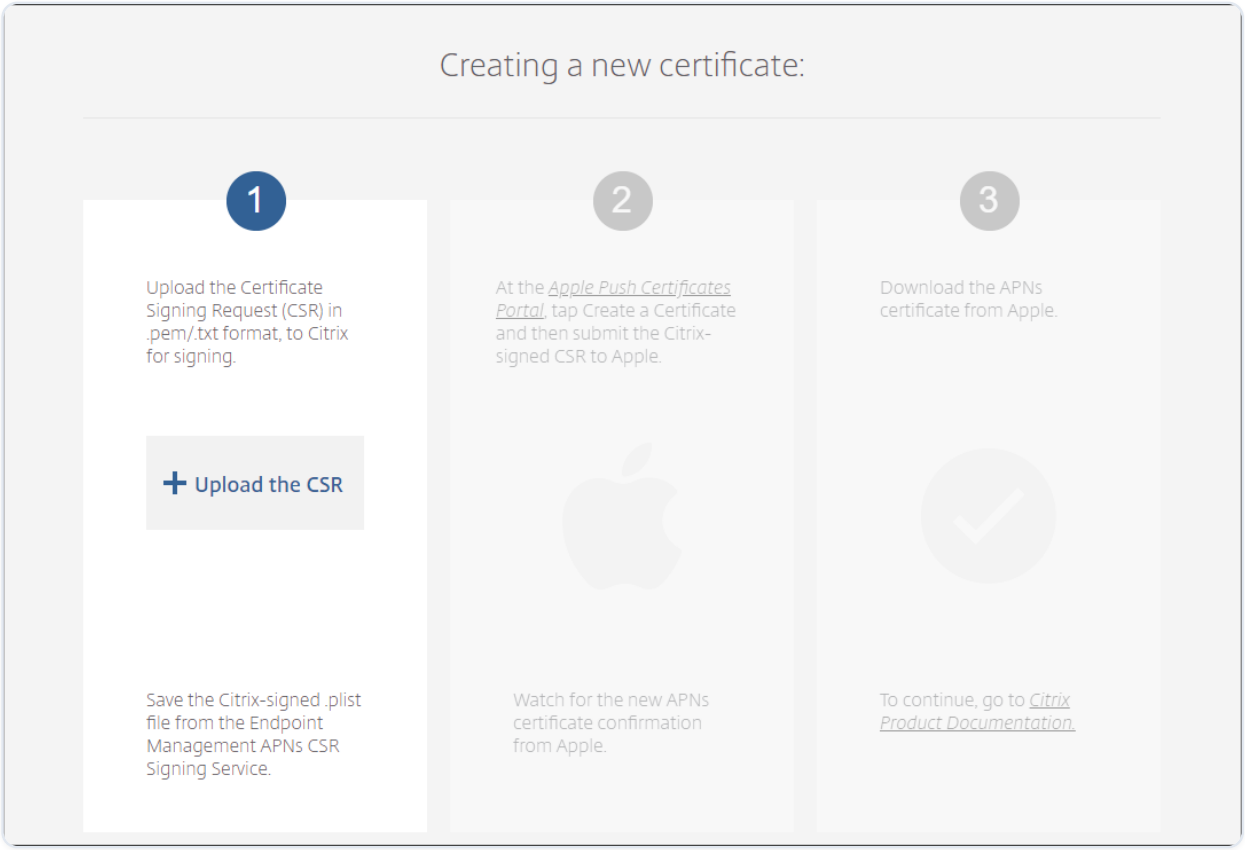
iOSデバイス用のApple Push Notificationサービス（APNs）証明書をセットアップする

重要:

APNsレガシーバイナリプロトコルに対するAppleのサポートは、March 31, 2021に終了します。Appleは、代わりにHTTP/2ベースのAPNsプロバイダーAPIを使用することを推奨しています。バージョン20.1.0以降、Citrix Endpoint ManagementはHTTP/2ベースのAPIをサポートしています。詳細については、`<https://developer.apple.com/>`のニュース更新「Apple Push Notification Service Update」を参照してください。APNsへの接続を確認する方法については、Connectivity checksを参照してください。

Citrix Endpoint Managementは、iOSデバイスを登録および管理するために、AppleからApple Push Notificationサービス（APNs）証明書を必要とします。Citrix Endpoint Managementは、iOSプッシュ通知用のCitrix Secure MailにもAPNs証明書を必要とします。

- Appleから証明書を取得するには、Apple IDと開発者アカウントが必要です。詳細については、Apple Developer ProgramのWebサイトを参照してください。
- APNs証明書を取得してCitrix Endpoint Managementにインポートするには、APNs証明書を参照してください。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint ManagementとAPNsの詳細については、iOS用Citrix Secure Mailのプッシュ通知を参照してください。

Android デバイス向けに Firebase Cloud Messaging (FCM) を設定する

Firebase Cloud Messaging (FCM) は、Android デバイスが Citrix Endpoint Management サービスに接続する方法とタイミングを制御します。セキュリティアクションまたは展開コマンドは、プッシュ通知をトリガーします。この通知は、ユーザーに Citrix Endpoint Management への再接続を促します。

- FCM のセットアップには、Google アカウントの設定が必要です。Google Play の資格情報を作成するには、「開発者アカウント情報の管理」を参照してください。また、Google Play を使用して、デバイス上の Android Enterprise ワークスペースに展開するアプリを追加、購入、承認します。Google Play を使用して、プライベート Android アプリ、公開アプリ、サードパーティ製アプリを展開できます。
- FCM を設定するには、「Firebase Cloud Messaging」を参照してください。

Citrix Endpoint Management AutoDiscovery サービスを設定する

AutoDiscovery サービスは、メールベースの URL 検出を通じて、ユーザーの登録プロセスを簡素化します。AutoDiscovery サービスは、登録検証、証明書ピン留めなどの機能や、Citrix Workspace のお客様向けのその他の利点も提供します。Citrix Cloud でホストされているこのサービスは、多くの Citrix Endpoint Management 展開において重要な部分です。

AutoDiscovery サービスを使用すると、ユーザーは次のことができます。

- 会社のネットワーク資格情報を使用してデバイスを登録できます。
- Citrix Endpoint Management サーバーアドレスに関する詳細を入力する必要がありません。
- ユーザー名をユーザープリンシパル名 (UPN) 形式で入力します。例: `user@mycompany.com`。

セキュリティの高い環境では、AutoDiscovery サービスを使用することをお勧めします。AutoDiscovery サービスは、中間者攻撃を防ぐ公開鍵証明書ピン留めをサポートしています。証明書ピン留めにより、Citrix クライアントが Citrix Endpoint Management と通信する際に、企業によって署名された証明書が使用されることが保証されます。Citrix Endpoint Management サイトの

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書ピン留めを構成するには、Citrix サポートにお問い合わせください。証明書ピン留めの詳細については、「証明書ピン留め」を参照してください。

AutoDiscovery サービスにアクセスするには、`<https://adsui.cloud.com>` (商用) に移動します。

前提条件

- Citrix Cloud の新しい AutoDiscovery サービスには、最新バージョンの Citrix Secure Hub が必要です。
  - iOS の場合、Citrix Secure Hub バージョン 21.6.0 以降
  - Androidの場合、Citrix Secure Hubバージョン21.8.5以降

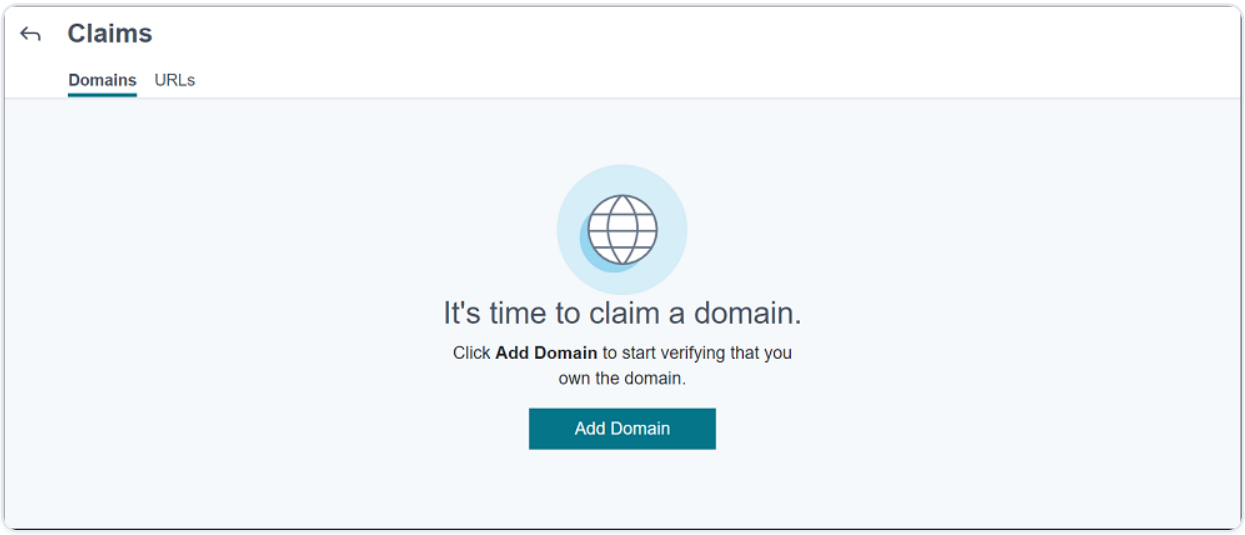
    以前のバージョンのCitrix Secure Hubを実行しているデバイスでは、サービスが中断される可能性があります。
- 新しいAutoDiscoveryサービスにアクセスするには、フルアクセス権を持つCitrix Cloud管理者アカウントが必要です。AutoDiscoveryサービスは、カスタムアクセス権を持つ管理者アカウントをサポートしていません。アカウントをお持ちでない場合は、「Citrix Cloudへのサインアップ」を参照してください。

  Citrixは、既存のすべてのAutoDiscoveryレコードをサービス中断なしにCitrix Cloudに移行しました。移行されたレコードは、新しいコンソールに自動的に表示されません。所有権を証明するには、新しいAutoDiscoveryサービスでドメインを再要求する必要があります。詳細については、「CTX312339」を参照してください。
- Citrix Endpoint Management展開でAutoDiscoveryサービスの使用を開始する前に、ドメインを確認して要求してください。最大10個のドメインを要求できます。要求により、検証済みドメインがAutoDiscoveryサービスに関連付けられます。10個を超えるドメインを要求するには、SREチケットを開くか、Citrixテクニカルサポートにお問い合わせください。
- MAMトラフィックをデータセンターに誘導するには、NetScaler Gateway FQDNの代わりにMAMポート設定を使用します。NetScaler Gatewayのポートとともに完全修飾ドメイン名を入力すると、クライアントデバイスは**MAMポート**設定の構成を使用します。
- 広告ブロッカーによってサイトが開かない場合は、ウェブサイト全体で広告ブロッカーを無効にしてください。

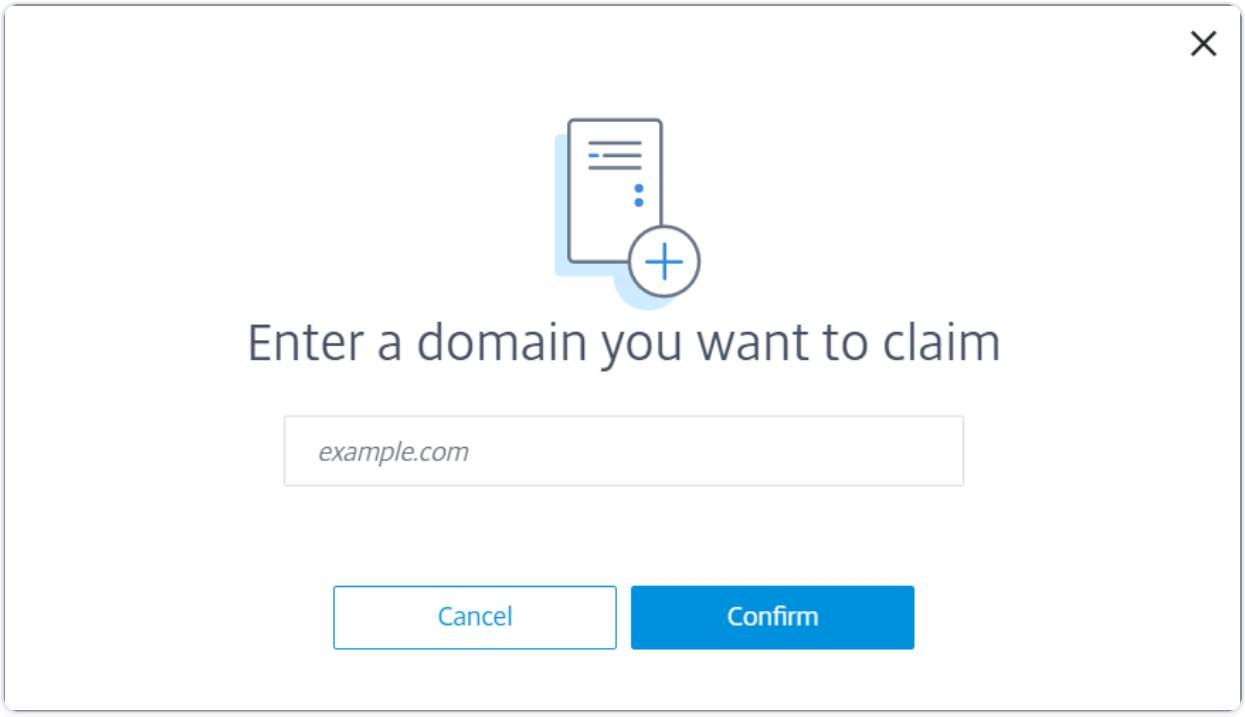
ドメインの要求

1. **>** タブで、 をクリックします。

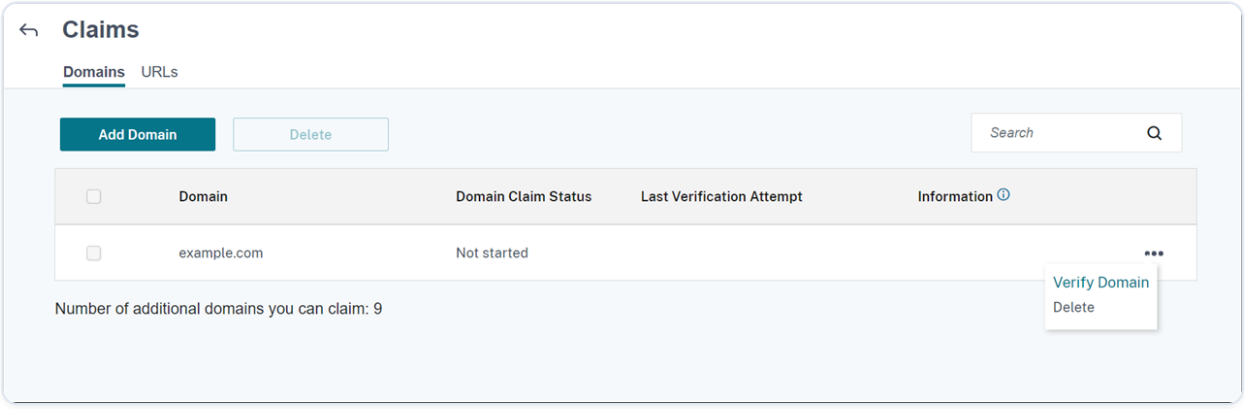
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 表示されるダイアログボックスで、Citrix Endpoint Management環境のドメイン名を入力し、をクリックします。ドメインは** > ** に表示されます。

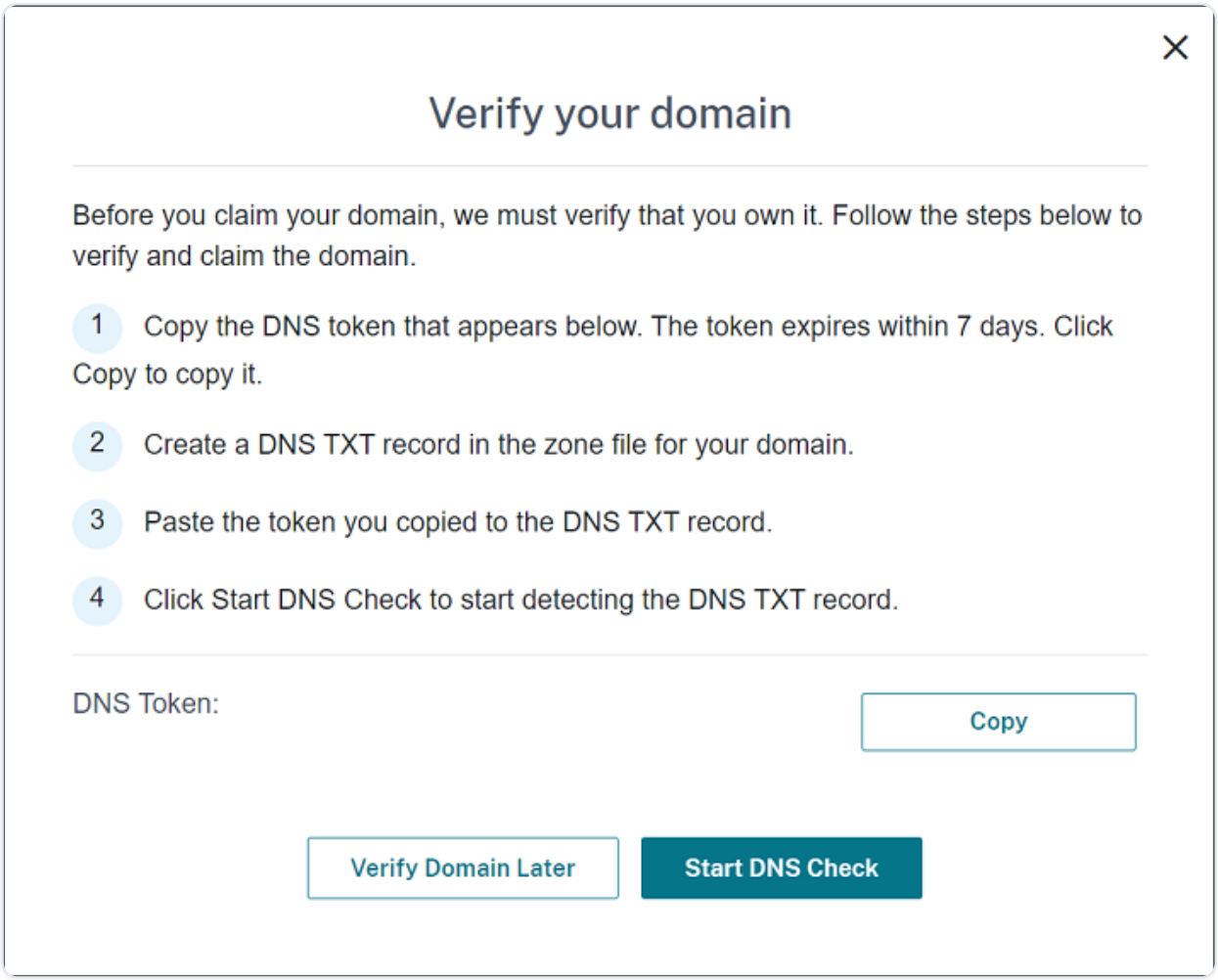


3. 追加したドメインで、省略記号メニューをクリックし、 を選択して検証プロセスを開始します。 ページが表示されます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. ページで、指示に従ってドメインの所有権を確認します。

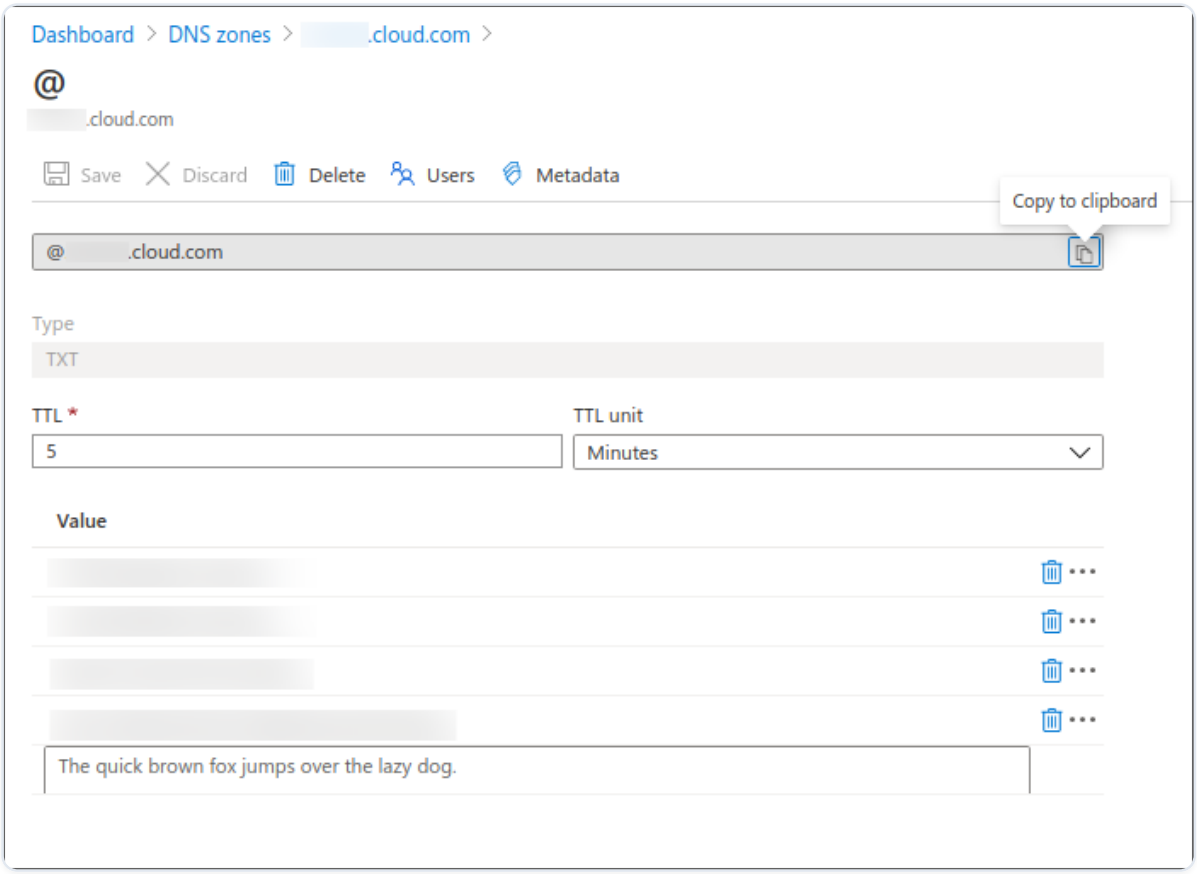


a. 「**コピー**」をクリックして、DNSトークンをクリップボードにコピーします。

b. ドメインのゾーンファイルにDNS TXTレコードを作成します。これを行うには、ドメインホスティングプロバイダーのポータルにアクセスし、コピーしたDNSトークンを追加します。

   次のスクリーンショットは、ドメインホスティングプロバイダーのポータルを示しています。お使いのポータルは異なる場合があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



c. Citrix Cloudの「**ドメインを確認**」ページで、「**DNSチェックを開始**」をクリックしてDNS TXTレコードの検出を開始します。後でドメインを確認する場合は、「**後でドメインを確認**」をクリックします。

検証プロセスには通常約1時間かかります。ただし、応答が返されるまでに最大2日かかる場合があります。ステータスチェック中にログアウトして再度ログインしても問題ありません。

構成が完了すると、ドメインのステータスが「**保留中**」から「**確認済み**」に変わります。

5. ドメインを要求したら、AutoDiscoveryサービスに関する情報を提供します。追加したドメインの省略記号メニューをクリックし、「**Citrix Endpoint Management情報を追加**」をクリックします。「**AutoDiscoveryサービス情報**」ページが表示されます。
6. 次の情報を入力し、「**保存**」をクリックします。

- **Citrix Endpoint ManagementサーバーFQDN:** Citrix Endpoint Managementサーバーの完全修飾ドメイン名を入力します。例: `example.xm.cloud.com`。この設定は、MDMおよびMAMトラフィック制御に使用されます。
- **NetScaler Gateway FQDN:** NetScaler Gatewayの完全修飾ドメイン名を、FQDNまたはFQDN:ポートの形式で入力します。例: `example.com`。この設定は、MAMトラフィックをデータセンターにルーティングするために使用されます。MDMのみの展開の場合は、このフィールドを空白のままにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注:**
>
> Citrixでは、MAMトラフィックを制御するために**NetScaler Gateway FQDN**ではなく**MAMポート**設定を使用することをお勧めします。NetScaler Gatewayのポートとともに完全修飾ドメイン名を入力した場合、クライアントデバイスは**MAMポート**設定の構成を使用します。

- **インスタンス名:** 以前に構成したCitrix Endpoint Managementサーバーのインスタンス名を入力します。インスタンス名が不明な場合は、デフォルト値の**zdm**のままにします。
- **MDMポート:** MDM制御トラフィックとMDM登録に使用されるポートを入力します。クラウドベースのサービスの場合、デフォルトは443です。
- **MAMポート:** MAM制御トラフィック、MAM登録、iOS登録、およびアプリ列挙に使用されるポートを入力します。クラウドベースのサービスの場合、デフォルトは8443です。

WindowsデバイスのAutoDiscoveryを要求する

Windowsデバイスを登録する予定がある場合は、次の手順を実行します。

1. Citrixサポートに連絡し、Windows AutoDiscoveryを有効にするためのサポートリクエストを作成します。
2. `enterpriseenrollment.mycompany.com`用の、公開署名されたワイルドカードではないSSL証明書を取得します。`mycompany.com`の部分は、ユーザーが登録に使用するアカウントを持つドメインです。.pfx形式のSSL証明書とそのパスワードを、前の手順で作成したサポートリクエストに添付します。

   複数のドメインを使用してWindowsデバイスを登録するには、次の構造を持つマルチドメイン証明書を使用することもできます。

   - サービスを提供するプライマリドメインを指定するCNを持つSubjectDN（例: enterpriseenrollment.mycompany1.com）。
   - 残りのドメインに適したSAN（例: enterpriseenrollment.mycompany2.com、enterpriseenrollment.mycompany3.comなど）。
3. DNSに正規名 (CNAME) レコードを作成し、SSL証明書のアドレス (enterpriseenrollment.mycompany.com) をautodisc.xm.cloud.comにマッピングします。

   WindowsデバイスユーザーがUPNを使用して登録すると、Citrix登録サーバーは次の処理を行います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Managementサーバーの詳細を提供します。
- デバイスにCitrix Endpoint Managementから有効な証明書を要求するよう指示します。

この時点で、サポートされているすべてのデバイスを登録できます。次のセクションに進み、デバイスにリソースを配信する準備をします。

Azure AD条件付きアクセスとの統合

Citrix Endpoint Management を構成して、Office 365 アプリケーションに Azure AD 条件付きアクセスサポートを適用できます。この機能により、Office 365 アプリケーションを展開する際に、デバイスユーザーにゼロトラスト手法を展開できます。デバイスの状態、リスクスコア、場所、およびデバイス保護を使用して、自動化されたアクションを適用し、管理対象の Android Enterprise および iOS デバイス上の Office 365 アプリケーションへのアクセスを定義できます。

Azure AD デバイスコンプライアンスを適用するには、個々の Office 365 アプリケーションに対して条件付きアクセスポリシーを構成する必要があります。管理されていない、またはコンプライアンスに準拠していないデバイス上の特定の Office 365 アプリケーションへのユーザーアクセスを制限し、管理されている、またはコンプライアンスに準拠しているデバイス上でのみ個々のアプリケーションへのアクセスを許可できます。

前提条件

- この統合には、Intune および Microsoft Office 365 ライセンスを含む有効な Azure AD Premium サブスクリプションが必要です。
- Citrix Secure Hub バージョン 21.4.0 以降
- Citrix Cloud で Azure AD を ID プロバイダー (IdP) として構成し、Citrix ID を Citrix Endpoint Management の IdP タイプとして設定します。詳しくは、「Citrix Cloud を介した Azure Active Directory による認証」を参照してください。
- モバイルアプリケーションが AAD クライアントアプリで認証できるように、Citrix マルチテナント AAD アプリケーションに同意します。これは、Azure グローバル管理者によって の値がに設定されている場合にのみ必要です。この設定は、Azure ポータルの **> >** で構成します。同意を提供するには、「Azure AD コンプライアンス管理のために Citrix Endpoint Management を構成する」を参照してください。
- Azure AD デバイス登録プロセスを開始する前に、Microsoft Authenticator アプリケーションをデバイスにインストールします。
- Android Enterprise プラットフォームの場合、Web ブラウザアプリを必須のパブリックストアアプリとして構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Azure AD コンソールで 設定を無効にします。Azure AD の構成を開始すると、セキュリティの既定値がより詳細な Azure AD 条件付きアクセスポリシーに置き換えられます。セキュリティの既定値の詳細については、Microsoft ドキュメントを参照してください。

Azure AD 条件付きアクセスポリシーによるデバイスコンプライアンスの構成

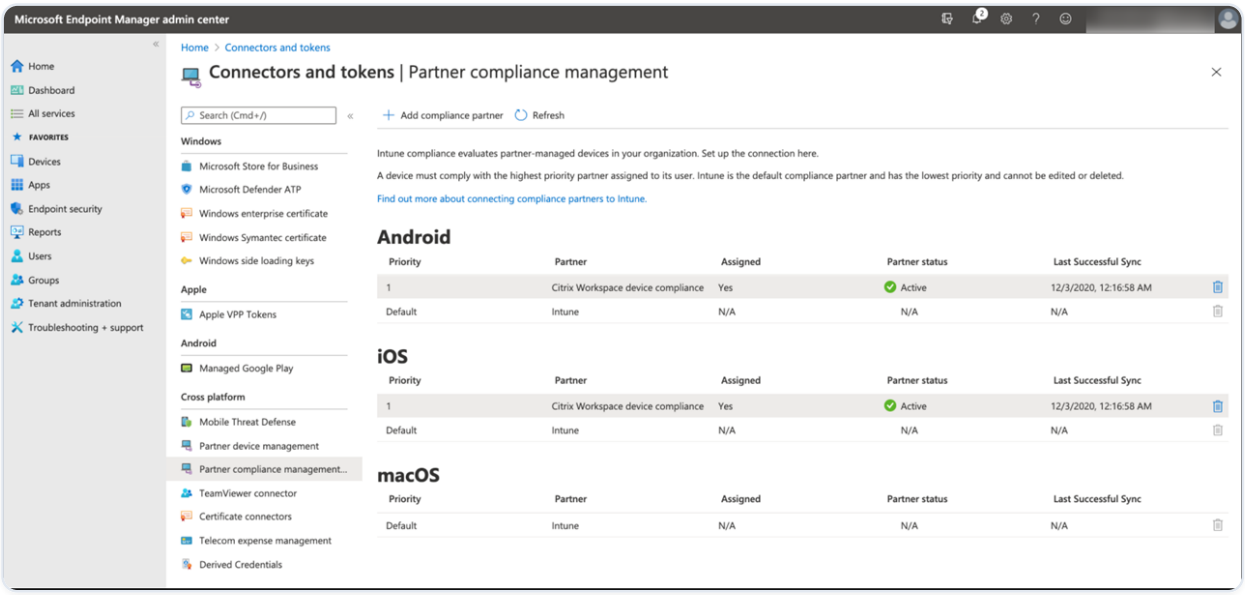
Azure AD 条件付きアクセスポリシーを通じてデバイスコンプライアンスを構成する一般的な手順は次のとおりです。

1. **シトリックス エンドポイント マネジメント の構成:**
    - Microsoft Endpoint Manager 管理センターで、各デバイスプラットフォームのコンプライアンスパートナーとして **Citrix Workspace デバイスコンプライアンス**を追加し、ユーザーグループを割り当てます。
    - Citrix Endpoint Management で、Microsoft Endpoint Manager 管理センターから情報を同期します。
2. **Azure AD の構成:** Azure AD ポータルで、個々の Office 365 アプリケーションの条件付きアクセス ポリシーを設定します。
3. **Citrix Endpoint Management の構成:** Office 365 アプリケーションの条件付きアクセス ポリシーを構成した後、Microsoft Authenticator アプリケーションと Office 365 アプリケーションを Citrix Endpoint Management のパブリックアプリストアアプリケーションとして追加します。これらのパブリックアプリケーションをデリバリーグループに割り当て、必須アプリケーションとして設定します。

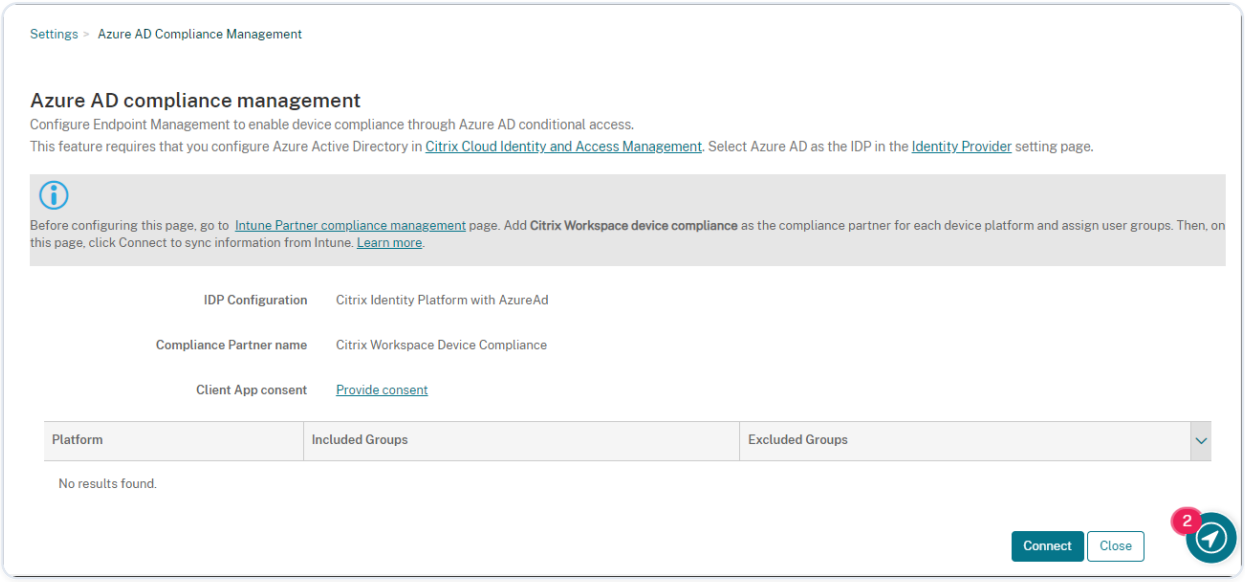
Azure AD コンプライアンス管理のために Citrix Endpoint Management を構成する

1. Microsoft Endpoint Manager 管理センターにサインインし、**テナント管理 > コネクタとトークン > デバイスコンプライアンス管理**に移動します。**コンプライアンスパートナーの追加**をクリックし、各デバイスプラットフォームのコンプライアンスパートナーとして**Citrix Workspace デバイスコンプライアンス**を選択します。次に、ユーザーグループを割り当てます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

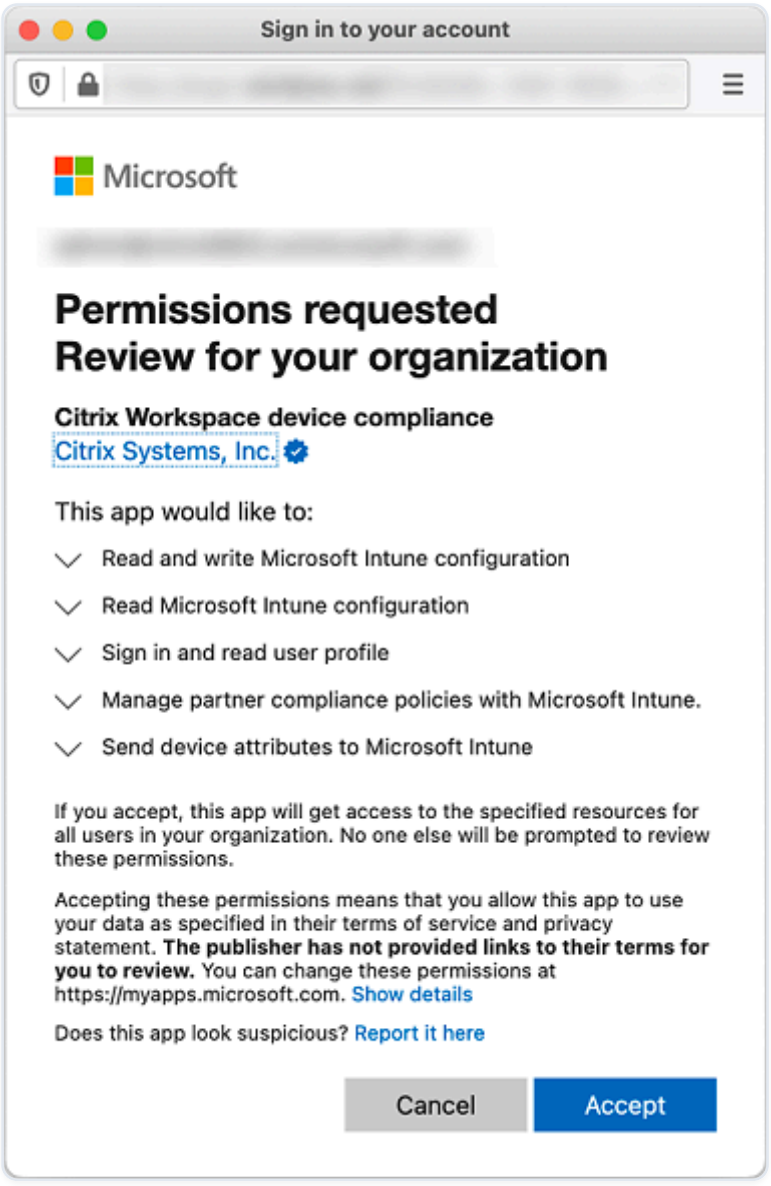


2. Citrix Endpoint Management で、**設定 > Azure AD コンプライアンス管理**に移動します。
3. オプションで、ユーザーが各デバイスで同意を提供する必要がないように、グローバル同意を設定します。**クライアントアプリの同意**の横にある**同意を提供する**をクリックします。グローバル管理者 Azure AD 資格情報を入力し、プロンプトに従ってクライアントアプリのグローバル同意を提供します。
4. **接続**をクリックして、Microsoft Endpoint Manager 管理センターから情報を同期します。



ダイアログボックスが表示され、この構成のアクセス許可を承諾するよう求められます。**承諾**をクリックします。構成が完了すると、同期されたデバイスプラットフォームがリストに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Azure AD で条件付きアクセス ポリシーを構成する

Azure AD ポータルで、デバイスコンプライアンスを適用するために Office 365 アプリケーションの条件付きアクセス ポリシーを構成します。**デバイス > 条件付きアクセス > ポリシー > 新しいポリシー**に移動します。詳細については、Microsoft ドキュメントを参照してください。

Intune で管理されるアプリケーションのデバイスコンプライアンスを構成するには:

- デバイスへの配信のために Intune で管理されるアプリケーションを構成する
- 承認済みクライアントアプリを必須にする
- クラウドアプリへのアクセスにアプリ保護ポリシーと承認済みクライアントアプリを必須にする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementでのアプリの構成

Office 365アプリの条件付きアクセスポリシーを構成したら、Microsoft AuthenticatorアプリとOffice 365アプリをCitrix Endpoint Managementのパブリックアプリストアアプリとして追加します。これらのパブリックアプリをデリバリーグループに割り当て、必須アプリとして設定します。詳しくは、「パブリックアプリストアアプリの追加」を参照してください。

ユーザー認証ワークフロー

1. オンプレミスのActive Directory（AD）でデバイスを登録し、その後Microsoft Azure Active Directory（AAD）を使用してCitrix IDプロバイダーと統合したユーザーは、再登録する必要はありません。オンプレミスのActive DirectoryからMicrosoft Azure Active Directoryにアカウントを同期できます。詳しくは、「Active DirectoryとAzure ADの準備」を参照してください。
2. Citrix Endpoint Managementは、Microsoft Authenticatorと構成済みのOffice 365アプリを必須アプリとしてデバイスにプッシュします。WebブラウザーアプリをAndroidプラットフォームの必須パブリックストアアプリとして構成した場合、Citrix Endpoint Managementはそれもユーザーデバイスにプッシュします。
3. Citrix Secure Hubは、Citrix Endpoint Managementを介して管理されているすべてのアプリを自動的にインストールして表示します。
4. ユーザーが利用可能なOffice 365アプリにサインインしようとすると、デバイスは登録プロセスを開始するために**Azure AD登録**リンクをタップするようユーザーに促します。
5. ユーザーが登録リンクをタップすると、Microsoft Authenticatorアプリが開きます。ユーザーはAzure ADの資格情報を入力し、デバイス登録の条件に同意します。その後、Microsoft Authenticatorアプリが閉じ、Citrix Secure Hubが再度開きます。
6. Citrix Secure Hubは、Azure ADデバイス登録が完了したことを示すメッセージを表示します。これでユーザーはMicrosoftアプリを使用してクラウドのリソースにアクセスできるようになります。

   登録が完了すると、Azure ADはコンソールでデバイスを管理対象および準拠としてマークします。

デフォルトのデバイスポリシーとモバイル生産性向上アプリ

Citrix Endpoint Management 19.5.0以降でオンボーディングを開始する場合、いくつかのデバイスポリシーとモバイル生産性向上アプリが事前構成されています。この構成により、次のことが可能になります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 基本的な機能をデバイスに即座に展開する
- 安全なワークスペースのために推奨されるベースライン構成から始めます。

アンドロイド、アンドロイド エンタープライズ、iOS、macOS、およびWindows デスクトップ/タブレットプラットフォームの場合、お客様のサイトには以下の事前構成済みデバイスポリシーがあります。

- **パスコードデバイスポリシー:** パスコードデバイスポリシーは**オン**になっており、すべてのデフォルトパスコード設定が有効になっています。
- **アプリインベントリデバイスポリシー:** アプリインベントリデバイスポリシーは**オン**になっています。
- **制限デバイスポリシー:** 制限デバイスポリシーは**オン**になっており、すべてのデフォルト制限設定が有効になっています。

これらのポリシーは、すべてのActive Directoryユーザーとローカルユーザーを含む**AllUsers**デリバリーグループにあります。AllUsersデリバリーグループは初期テストのみに使用することをお勧めします。その後、独自のデリバリーグループを作成し、AllUsersデリバリーグループを無効にしてください。事前構成済みのデバイスポリシーとアプリは、独自のデリバリーグループで再利用できます。

すべてのCitrix Endpoint Managementデバイスポリシーは、デバイスポリシーに記載されています。この記事には、コンソールを使用してデバイスポリシーを編集する方法に関する情報が含まれています。一般的に使用されるデバイスポリシーについては、デバイスポリシーとユースケースの動作を参照してください。

iOSおよびAndroidプラットフォームの場合、サイトには以下の事前構成済みモバイル生産性アプリがあります。

- **シトリックス セキュア メール**
- **シトリックス セキュアウェブ**
- **シトリックス ファイル**

これらのアプリは**AllUsers**デリバリーグループにあります。

詳細については、モバイル生産性アプリについてを参照してください。

Citrix Endpoint Managementの構成を続行する

デバイス登録の基本的な設定が完了した後、Citrix Endpoint Managementの構成方法はユースケースによって大きく異なります。例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- セキュリティ要件は何ですか？また、それらの要件とユーザーエクスペリエンスのバランスをどのように取りたいですか？
- どのデバイスプラットフォームをサポートしていますか？
- ユーザーは自分のデバイスを所有していますか、それとも会社所有のデバイスを使用していますか？
- デバイスにプッシュしたいデバイスポリシーは何ですか？
- ユーザーにどのような種類のアプリを提供しますか？

このセクションでは、このドキュメントセット内の記事に誘導することで、多くの構成オプションをナビゲートするのに役立ちます。

サードパーティサイトでの構成を完了する際は、Citrix Endpoint Managementコンソール設定を構成する際の参照用に、情報とその場所をメモしておいてください。

- セキュリティと認証。Citrix Endpoint Managementは、証明書を使用して安全な接続を作成し、ユーザーを認証します。Citrixは、Citrix Endpoint Managementインスタンス用のワイルドカード証明書を提供します。
    - 認証コンポーネントとセキュリティレベルごとの推奨構成については、「高度な概念」の記事、認証を参照してください。また、セキュリティとユーザーエクスペリエンスも参照してください。
    - Citrix Endpoint Managementの操作中に使用される認証コンポーネントの概要については、証明書と認証を参照してください。
    - 以下の認証タイプから選択できます。認証の構成には、Citrix Endpoint ManagementおよびNetScaler Gatewayコンソールでのタスクが含まれます。
        - ドメインまたはドメインとセキュリティトークン認証
        - クライアント証明書または証明書とドメイン認証
    - ユーザーに証明書を配信するには、以下を構成します。
        - PKIエンティティ
        - 資格情報プロバイダー(/ja-jp/citrix-endpoint-management/authentication/credential-providers.html)
    - デバイス登録セキュリティモード。デバイス登録セキュリティモードは、ユーザーがCitrix Endpoint Managementにデバイスを登録するために必要な資格情報の種類と登録手順を指定します。詳細については、「登録セキュリティモードの構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - ユーザーがAzure Active Directory資格情報で認証できるようにするには、「Citrix Cloudを介したAzure Active Directoryでの認証」を参照してください。

- デバイス登録
    - 多数のデバイスを登録するためのプログラムが利用可能です。
        - Apple Deployment Programを介したデバイスの展開(/ja-jp/citrix-endpoint-management/device-management/apple/apple-deployment-program.html)
        - Appleデバイスの一括登録(/ja-jp/citrix-endpoint-management/device-management/apple/ios-bulk-enrollment.html)
        - Windowsデバイスの一括登録(/ja-jp/citrix-endpoint-management/device-management/windows/windows-bulk-enrollment.html)
    - Androidデバイスを登録するには、Android Enterprise管理者アカウントを作成します。「Android Enterprise」を参照してください。または、「Google Workspaceのお客様向けレガシーAndroid Enterprise」を参照してください。
    - 登録招待を使用するか、登録通知を送信できます。
        - 登録招待(/ja-jp/citrix-endpoint-management/device-management.html#enrollment-invitations)。
        - 通知(/ja-jp/citrix-endpoint-management/users/notifications.html)。
    - 登録の詳細については、「デバイス管理」およびそのノード配下の記事を参照してください。

- デバイスポリシーと管理
    - デバイス（MDM）ポリシー。すべてのCitrix Endpoint Managementデバイスポリシーは、「デバイスポリシー」に記載されています。一般的に使用されるデバイスポリシーの詳細については、「デバイスポリシーとユースケースの動作」を参照してください。
    - クライアントプロパティ。クライアントプロパティには、ユーザーデバイス上のCitrix Secure Hubに直接提供される情報が含まれています。詳しくは、クライアントプロパティおよびCitrix Endpoint Managementクライアントプロパティを参照してください。
    - デリバリーグループ。デリバリーグループに関連する使用例については、ユーザーコミュニティおよびデリバリーグループの追加を参照してください。

- アプリを展開する準備をする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Managementでサポートされているアプリについては、アプリの追加を参照してください。
- Apple Volume Purchaseを使用して、iOSアプリのライセンスを管理できます。詳しくは、Apple Volume Purchaseを参照してください。
- Citrix Endpoint Managementを使用して、Apple Volume Purchaseで取得したiBooksを展開できます。メディアの追加を参照してください。
- Citrixは、Citrix Secure MailやCitrix Secure Webなどのモバイル生産性向上アプリを提供しています。モバイル生産性向上アプリについてを参照してください。
- Citrix Secure Mailの代替として、ネイティブメールをデバイスに配信できます。参照：
  - メール戦略
  - エクスチェンジ アクティブシンク 用 シトリックス エンドポイント マネジメント コネクタ
  - Exchange ActiveSync 用 NetScaler Gateway コネクタ
- ユーザーがドキュメントとデータをMicrosoft Office 365アプリに安全に転送できるようにするには、Office 365アプリとの安全な対話の許可およびOfficeデバイスポリシーを参照してください。
- アプリポリシーに関する一般的な情報については、アプリポリシーとユースケースシナリオを参照してください。
- MDX Toolkitは、Citrix Endpoint Managementでエンタープライズアプリを安全に展開するためのアプリラッピングテクノロジーです。MAM SDKはMDX Toolkitに代わるものです。MDX Toolkitは2023年7月にEOLを迎える予定です。

  MAM SDKの詳細については、MAM SDKの概要を参照してください。
- アプリの詳細については、アプリの追加 の他の記事を参照してください。

- Citrix Endpoint Management のロールベースのアクセス制御 (RBAC) 機能を使用すると、事前定義されたロール (アクセス許可のセット) をユーザーおよびグループに割り当てることができます。これらのアクセス許可は、ユーザーがシステム機能にアクセスできるレベルを制御します。詳細については、「RBAC でロールを構成する」を参照してください。
- Citrix Endpoint Management で自動アクションを作成して、イベント、特定の構成、またはユーザーデバイス上のアプリの存在に応じて実行するアクションを指定します。詳細については、「自動アクション」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書と認証

Citrix Endpoint Managementの操作における認証には、いくつかのコンポーネントが関与します。

- **Citrix Endpoint Management:** Citrix Endpoint Managementサーバーは、登録セキュリティと登録エクスペリエンスを定義する場所です。ユーザーをオンボーディングするためのオプションには、以下が含まれます。
  - 登録をすべての人に公開するか、招待者のみにするか。
  - 2要素認証または3要素認証を要求するかどうか。Citrix Endpoint Managementクライアントプロパティを使用すると、Citrix PIN認証を有効にし、PINの複雑さと有効期限を設定できます。
- **NetScaler Gateway:** NetScaler Gatewayは、マイクロVPN SSLセッションの終端を提供します。NetScaler Gatewayは、ネットワークの転送中のセキュリティも提供し、ユーザーがアプリにアクセスするたびに使用される認証エクスペリエンスを定義できます。
- **Citrix Secure Hub:** Citrix Secure HubとCitrix Endpoint Managementは、登録操作で連携します。Citrix Secure Hubは、NetScaler Gatewayと通信するデバイス上のエンティティです。セッションの有効期限が切れると、Citrix Secure HubはNetScaler Gatewayから認証チケットを取得し、そのチケットをMDXアプリに渡します。Citrixは、中間者攻撃を防ぐ証明書ピンニングを推奨しています。詳細については、Citrix Secure Hubの記事のこのセクションを参照してください: 証明書ピンニング。

  Citrix Secure HubはMDXセキュリティコンテナも促進します。Citrix Secure Hubはポリシーをプッシュし、アプリがタイムアウトしたときにNetScaler Gatewayとのセッションを作成し、MDXのタイムアウトと認証エクスペリエンスを定義します。Citrix Secure Hubは、ジェイルブレイク検出、地理位置情報チェック、および適用するすべてのポリシーも担当します。
- **MDXポリシー:** MDXポリシーは、デバイス上にデータボールトを作成します。MDXポリシーは、マイクロVPN接続をNetScaler Gatewayに戻し、オフラインモードの制限を適用し、タイムアウトなどのクライアントポリシーを適用します。

Citrix Endpoint Managementは、以下の認証方法を使用して、ユーザーをリソースに認証します。

- モバイルデバイス管理 (MDM)
  - クラウドホスト型IDプロバイダー (IdP)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 軽量ディレクトリアクセスプロトコル (LDAP)
        - 招待URL + PIN
        - 2要素認証
- モバイルアプリケーション管理 (MAM)
    - LDAP
    - 証明書
    - セキュリティトークン MAM認証にはNetScaler Gatewayが必要です。

その他の構成の詳細については、以下の記事を参照してください。

- 証明書のアップロード、更新、および再発行](/ja-jp/citrix-endpoint-management/authentication/upload-renew-certificates.html)
- ネットスケーラー ゲートウェイ と シトリックス エンドポイント マネジメント
- ドメインまたはドメインとセキュリティトークン認証](/ja-jp/citrix-endpoint-management/authentication/authentication-domain-security-token.html)
- クライアント証明書または証明書とドメイン認証](/ja-jp/citrix-endpoint-management/authentication/client-certificate.html)
- PKIエンティティ](/ja-jp/citrix-endpoint-management/authentication/pki-entities.html)
- 資格情報プロバイダー](/ja-jp/citrix-endpoint-management/authentication/credential-providers.html)
- APNs証明書](/ja-jp/citrix-endpoint-management/authentication/apns.html)
- Citrix FilesでのシングルサインオンのためのSAML](/ja-jp/citrix-endpoint-management/authentication/saml-sso-sharefile.html)
- Citrix Cloudを介したAzure Active Directoryでの認証](/ja-jp/citrix-endpoint-management/authentication/authentication-with-azure-active-directory-through-citrix-cloud.html)
- Citrix Cloudを介したOktaでの認証](/ja-jp/citrix-endpoint-management/authentication/authentication-with-okta-through-citrix-cloud.html)
- Citrix Cloudを介したオンプレミスNetScaler Gatewayでの認証(/ja-jp/citrix-endpoint-management/authentication/authentication-with-citrix-gateway-through-citrix-cloud.html)
- Wi-Fiサーバーに認証するには、証明書をデバイスに送信します: ネットワークデバイスポリシー
- 認証に使用されない一意の証明書（内部ルート証明機関（CA）証明書など）または特定のポリシーをプッシュするには: 資格情報デバイスポリシー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書

Citrix Endpoint Managementは、サーバーへの通信フローを保護するために、インストール中に自己署名Secure Sockets Layer（SSL）証明書を生成します。SSL証明書は、信頼できる証明機関からの信頼できるSSL証明書に置き換えてください。

Citrix Endpoint Managementは、独自の公開鍵基盤（PKI）サービスも使用するか、クライアント証明書のためにCAから証明書を取得します。すべてのCitrix製品は、ワイルドカード証明書とサブジェクト代替名（SAN）証明書をサポートしています。ほとんどの展開では、ワイルドカード証明書またはSAN証明書が2つあれば十分です。

クライアント証明書認証は、モバイルアプリにセキュリティの追加レイヤーを提供し、ユーザーがHDXアプリにシームレスにアクセスできるようにします。クライアント証明書認証が構成されている場合、ユーザーはCitrix PINを入力して、Citrix Endpoint Management対応アプリへのシングルサインオン（SSO）アクセスを行います。Citrix PINは、ユーザー認証エクスペリエンスも簡素化します。Citrix PINは、クライアント証明書を保護したり、Active Directoryの資格情報をデバイスにローカルに保存したりするために使用されます。

Citrix Endpoint ManagementでiOSデバイスを登録および管理するには、AppleからApple Push Notification Service（APNs）証明書を設定および作成します。手順については、APNs証明書を参照してください。

次の表は、各Citrix Endpoint Managementコンポーネントの証明書形式と種類を示しています。

CITRIX ENDPOINT MANAGEMENTコンポーネント	証明書形式	必要な証明書の種類
ネットスケーラー ゲートウェイ	PEM (BASE64), PFX (PKCS #12)	SSL、ルート (NetScaler GatewayはPFXをPEMに自動的に変換します。).
シトリックス エンドポイント マネジメント	.p12 (Windowsベースのコンピューターでは.pfx)	SSL、SAML、APNs (Citrix Endpoint Managementは、インストールプロセス中に完全なPKIも生成します。) **重要:** Citrix Endpoint Managementは、.pem拡張子の証明書をサポートしていません。.pem証明書を使用するには、.pemファイルを証明書とキーに分割し、それぞれをCitrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CITRIX ENDPOINT MANAGEMENTコンポーネント	証明書形式	必要な証明書の種類
		Endpoint Managementにインポートします。
StoreFront	PFX (PKCS #12)	SSL、ルート

Citrix Endpoint Managementは、ビット長が4096および2048のクライアント証明書をサポートしています。

NetScaler GatewayおよびCitrix Endpoint Managementの場合、Verisign、DigiCert、Thawteなどのパブリックcaからサーバー証明書を取得することをお勧めします。NetScaler GatewayまたはCitrix Endpoint Management構成ユーティリティから証明書署名要求 (CSR) を作成できます。CSRを作成したら、署名のためにCAに提出します。CAが署名済み証明書を返したら、NetScaler GatewayまたはCitrix Endpoint Managementに証明書をインストールできます。

重要:

iOS、iPadOS、macOSにおける信頼された証明書の要件

AppleはTLSサーバー証明書に関する新しい要件を設けています。すべての証明書がAppleの要件に従っていることを確認してください。Appleの公開情報 `<https://support.apple.com/ja-jp/HT210176>` を参照してください。
AppleはTLSサーバー証明書の最大許容有効期間を短縮しています。この変更は、2020年9月以降に発行されたサーバー証明書にのみ影響します。Appleの公開情報 `<https://support.apple.com/ja-jp/HT211025>` を参照してください。

LDAP認証

Citrix Endpoint Managementは、Lightweight Directory Access Protocol (LDAP) に準拠した1つ以上のディレクトリに対するドメインベースの認証をサポートしています。LDAPは、グループ、ユーザーアカウント、および関連プロパティに関する情報へのアクセスを提供するソフトウェアプロトコルです。詳細については、ドメインまたはドメインとセキュリティトークン認証 を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IDプロバイダー認証

Citrix Cloud を介して ID プロバイダー (IdP) を構成し、ユーザーデバイスを登録および管理できます。

IdP のサポートされているユースケース:

- シトリックス クラウドを介したアジュール アクティブ ディレクトリ
  - Workspace 統合はオプションです
  - 証明書ベースの認証用に構成された NetScaler Gateway
  - Android Enterprise (プレビュー。BYOD、完全に管理されたデバイス、および拡張された登録プロファイルをサポート)
  - MDM+MAM および MDM 登録用の iOS
  - Apple Business Manager 登録用の iOS および macOS
  - レガシー Android (DA)

  Apple School Manager などの自動登録機能は現在サポートされていません。
- Citrix Cloud を介した Okta
  - Workspace 統合はオプションです
  - 証明書ベースの認証用に構成された NetScaler Gateway
  - Android Enterprise (プレビュー。BYOD、完全に管理されたデバイス、および拡張された登録プロファイルをサポート)
  - MDM+MAM および MDM 登録用の iOS
  - Apple Business Manager登録用のiOSおよびmacOS
  - レガシーAndroid (DA)

  Apple School Managerなどの自動登録機能は現在サポートされていません。
- Citrix Cloudを介したオンプレミスNetScaler Gateway
  - 証明書ベースの認証用に構成されたNetScaler Gateway
  - Android Enterprise (プレビュー。BYOD、完全管理デバイス、拡張登録プロファイルをサポート)
  - MDM+MAMおよびMDM登録用のiOS
  - レガシーAndroid (DA) Apple Deployment Programなどの自動登録機能は現在サポートされていません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書のアップロード、更新、および再発行

Citrix Endpoint Managementの展開に必要な証明書を一覧表示することをお勧めします。このリストを使用して、証明書の有効期限とパスワードを追跡します。この記事は、証明書のライフサイクル全体にわたる管理に役立ちます。

環境には、以下の証明書が含まれる場合があります。

- シトリックス エンドポイント マネジメント サーバー
  - MDM FQDN用SSL証明書（XenMobile ServerからCitrix Endpoint Managementに移行した場合に必要です。それ以外の場合、Citrixがこの証明書を管理します。）
  - SAML証明書（Citrix Files用）
  - 前述の証明書およびその他の内部リソース（StoreFront/Proxyなど）用のルートおよび中間CA証明書
  - iOSデバイス管理用APNs証明書
  - PKIへの接続用PKIユーザー証明書（環境で証明書ベースの認証が必要な場合に必須）
- MDX ツールキット
  - Apple開発者証明書
  - Appleプロビジョニングプロファイル（アプリケーションごと）
  - Apple APNs証明書（Citrix Secure Mailで使用）
  - Androidキーストアファイル

  MAM SDKはアプリをラップしないため、証明書は不要です。
- ネットスケーラー ゲートウェイ
  - MDM FQDN用のSSL証明書
  - Gateway FQDN用のSSL証明書
  - ShareFile SZC FQDN用のSSL証明書
  - Exchangeロードバランシング用のSSL証明書 (オフロード構成)
  - StoreFrontロードバランシング用のSSL証明書
  - 前述の証明書用のルートおよび中間CA証明書

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

クライアントデバイスは、サーバー証明書を発行した認証局との信頼を確立するために、必要なルート/中間証明書を持っている必要があります。そうしないと、SSLエラー61が表示される場合があります。この問題を解決するには:

1. SSL証明書プロバイダーによって発行されたSSLルート/中間証明書ファイル (.crtまたは.cer) をダウンロードまたは取得します。通常、ルート/中間/サーバー証明書は、SSLサービスプロバイダーが提供する証明書バンドルに含まれています。
2. クライアントデバイスにルート/中間証明書をインストールします。
3. クライアントデバイスにウイルス対策ソフトウェアがインストールされている場合、そのウイルス対策ソフトウェアが証明書を信頼していることを確認してください。

証明書のアップロード

アップロードする各証明書には、その内容の概要を含む証明書テーブルのエントリがあります。証明書を必要とするPKI統合コンポーネントを構成する場合、条件を満たすサーバー証明書を選択します。たとえば、Citrix Endpoint ManagementをMicrosoft認証局 (CA) と統合するように構成したい場合があります。Microsoft CAへの接続は、クライアント証明書を使用して認証される必要があります。

Citrix Endpoint Managementは、特定の証明書の秘密キーを持っていない場合があります。同様に、Citrix Endpoint Managementは、アップロードされた証明書に秘密キーを必要としない場合があります。

このセクションでは、証明書をアップロードするための一般的な手順について説明します。クライアント証明書の作成、アップロード、および構成の詳細については、「クライアント証明書または証明書とドメイン認証」を参照してください。

証明書をアップロードするには、次の2つのオプションがあります。

- 証明書を個別にコンソールにアップロードします。
- REST APIを使用して証明書を一括アップロードします。このオプションはiOSデバイスでのみ利用可能です。

証明書をコンソールにアップロードする際、次のことができます。

- キーストアをインポートします。PKCS #12形式をアップロードする場合を除き、インストールするキーストアリポジトリ内のエントリを特定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 証明書をインポートします。

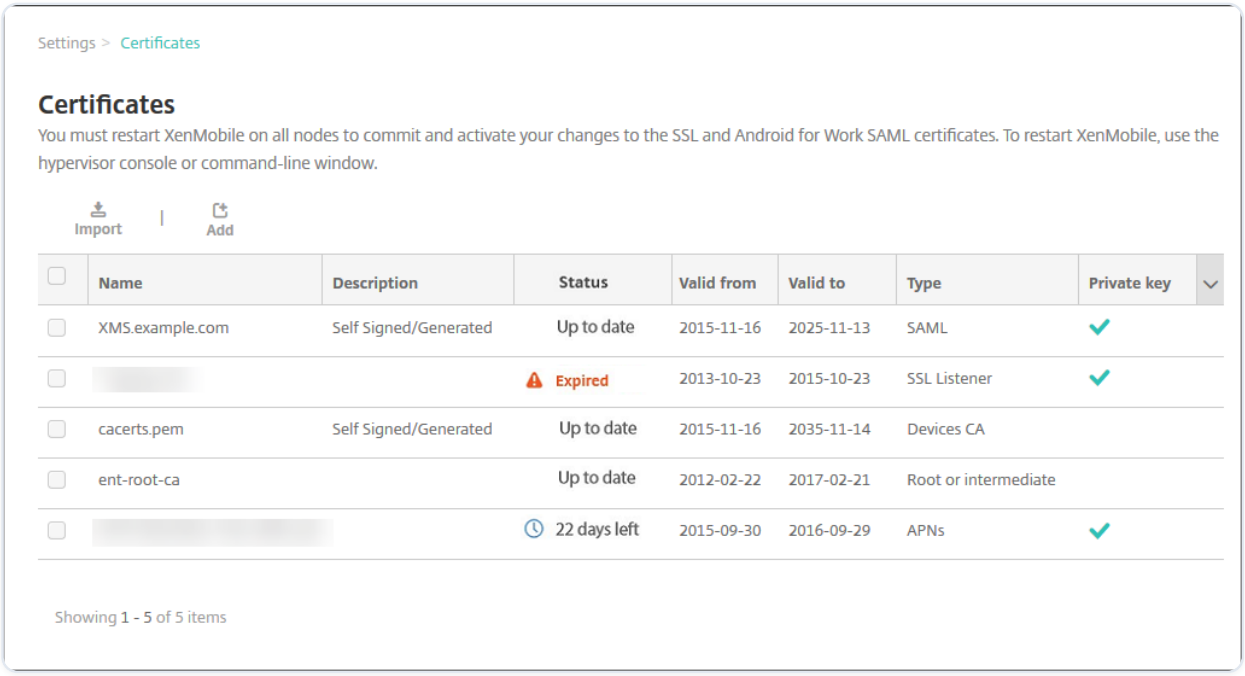
CAが要求の署名に使用するCA証明書（秘密鍵なし）をアップロードできます。また、クライアント認証のためにSSLクライアント証明書（秘密鍵あり）をアップロードすることもできます。

Microsoft CAエンティティを構成する際、CA証明書を指定します。CA証明書であるすべてのサーバー証明書のリストからCA証明書を選択します。同様に、クライアント認証を構成する際、Citrix Endpoint Managementが秘密鍵を持つすべてのサーバー証明書のリストから選択できます。

キーストアをインポートするには

キーストアは、セキュリティ証明書のリポジトリです。設計上、キーストアには多数のエントリを含めることができます。キーストアからロードする場合、ロードしたいエントリを識別するエントリアリアスを指定する必要があります。エイリアスを指定しない場合、ストアの最初のエントリがロードされます。PKCS #12ファイルは通常1つのエントリしか持たないため、キーストアタイプとしてPKCS #12を選択した場合、エイリアスフィールドは表示されません。

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。検索バーを使用して、**証明書**設定を見つけて開きます。



2. **インポート**をクリックします。**インポート**ダイアログボックスが表示されます。
3. 次の設定を構成します。

   - **インポート: キーストア**を選択します。

   証明書構成ページ(/en-us/citrix-endpoint-management/media/settings-certificates-import-keystore.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **キーストアの種類:** ドロップダウンリストで **PKCS #12** をクリックします。
- **用途:** リストで、証明書の使用方法をクリックします。利用可能なオプションは次のとおりです。
  - **サーバー:** サーバー証明書は、Citrix Endpoint Managementによって機能的に使用される証明書です。サーバー証明書はCitrix Endpoint Management Webコンソールにアップロードします。これらの証明書には、CA証明書、RA証明書、およびインフラストラクチャの他のコンポーネントとのクライアント認証用の証明書が含まれます。また、サーバー証明書をデバイスに展開する証明書のストレージとして使用することもできます。この用途は、特にデバイスで信頼を確立するために使用されるCAに適用されます。
  - **SAML:** Security Assertion Markup Language (SAML) 認証により、サーバー、Webサイト、およびアプリへのSSOアクセスを提供できます。
  - **APNs:** AppleからのAPNs証明書は、Apple Push Networkを介したモバイルデバイス管理を可能にします。
  - **SSLリスナー:** Secure Sockets Layer (SSL) リスナーは、SSL暗号化アクティビティをCitrix Endpoint Managementに通知します。
- **キーストアファイル:** インポートするキーストアを参照して見つけます。キーストアは.p12または.pfxファイルです。ファイルを選択し、**開く**をクリックします。
- **パスワード:** 証明書に割り当てられているパスワードを入力します。
- **説明:** オプションで、他のキーストアと区別するために、キーストアの説明を入力します。

4. **インポート**をクリックします。キーストアが証明書テーブルに追加されます。

証明書をインポートするには

証明書をインポートすると、Citrix Endpoint Managementは入力から証明書チェーンを構築しようとします。Citrix Endpoint Managementは、チェーン内のすべての証明書をインポートして、各証明書のサーバー証明書エントリを作成します。この操作は、ファイルまたはキーストアエントリ内の証明書がチェーンを形成している場合にのみ機能します。チェーン内の後続の各証明書は、前の証明書の発行者である必要があります。

インポートされた証明書には、オプションの説明を追加できます。説明はチェーン内の最初の証明書にのみ添付されます。残りの証明書の説明は後で更新できます。

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。検索バーを使用して、**Certificates**設定を見つけて開きます。
2. **Certificates**ページで、**Import**をクリックします。**Import**ダイアログボックスが表示されます。以下を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Import: Certificate**をクリックします。
- **Use as:** 証明書の使用方法を選択します。利用可能なオプションは次のとおりです。
  - **Server:** サーバー証明書は、Citrix Endpoint Managementによって機能的に使用される証明書です。サーバー証明書はCitrix Endpoint Management Webコンソールにアップロードします。これらの証明書には、CA証明書、RA証明書、およびインフラストラクチャの他のコンポーネントとのクライアント認証用の証明書が含まれます。また、サーバー証明書をデバイスに展開する証明書のストレージとして使用することもできます。このオプションは、特にデバイス上で信頼を確立するために使用されるCAに適用されます。
  - **SAML:** Security Assertion Markup Language (SAML) 認証により、サーバー、Webサイト、およびアプリへのシングルサインオン (SSO) アクセスを提供できます。
  - **SSL Listener:** Secure Sockets Layer (SSL) リスナーは、SSL暗号化アクティビティをCitrix Endpoint Managementに通知します。
- **Certificate import:** インポートする証明書を参照して見つけます。ファイルを選択し、**Open**をクリックします。
- **Private key file:** 証明書用のオプションの秘密鍵ファイルを参照して見つけます。秘密鍵は、証明書とともに暗号化と復号化に使用されます。ファイルを選択し、**Open**をクリックします。
- **Description:** オプションで、他の証明書と区別できるように、証明書の説明を入力します。

3. **Import**をクリックします。証明書が証明書テーブルに追加されます。

REST APIを使用して証明書を一括アップロードする

証明書を一度に1つずつアップロードするのは現実的でない場合があります。そのような場合は、REST APIを使用して証明書を一括アップロードします。この方法では、.p12形式の証明書がサポートされます。REST APIの詳細については、「REST API」を参照してください。

1. 各証明書ファイルを`device_identity_value.p12`の形式で名前変更します。`device_identity_value`は、各デバイスのIMEI、シリアル番号、またはMEIDにすることができます。

   例として、識別方法としてシリアル番号を使用することを選択したとします。あるデバイスのシリアル番号が`A12BC3D4EFGH`である場合、そのデバイスにインストールする予定の証明書ファイルの名前を`A12BC3D4EFGH.p12`とします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. .p12証明書のパスワードを保存するためのテキストファイルを作成します。そのファイルに、各デバイスのデバイス識別子とパスワードを新しい行に入力します。
   `device_identity_value=password`の形式を使用します。以下を参照してください。

```
A12BC3D4EFGH.p12=password1!

A12BC3D4EFIJ.p12=password2@

A12BC3D4EFKL.p12=password3#
```

3. 作成したすべての証明書とテキストファイルを.zipファイルにまとめます。
4. REST APIクライアントを起動し、Citrix Endpoint Managementにログインして、認証トークンを取得します。
5. 証明書をインポートし、メッセージ本文に以下を記述していることを確認します。

```
{

    "alias": "",

    "useAs": "device",

    "uploadType": "keystore",

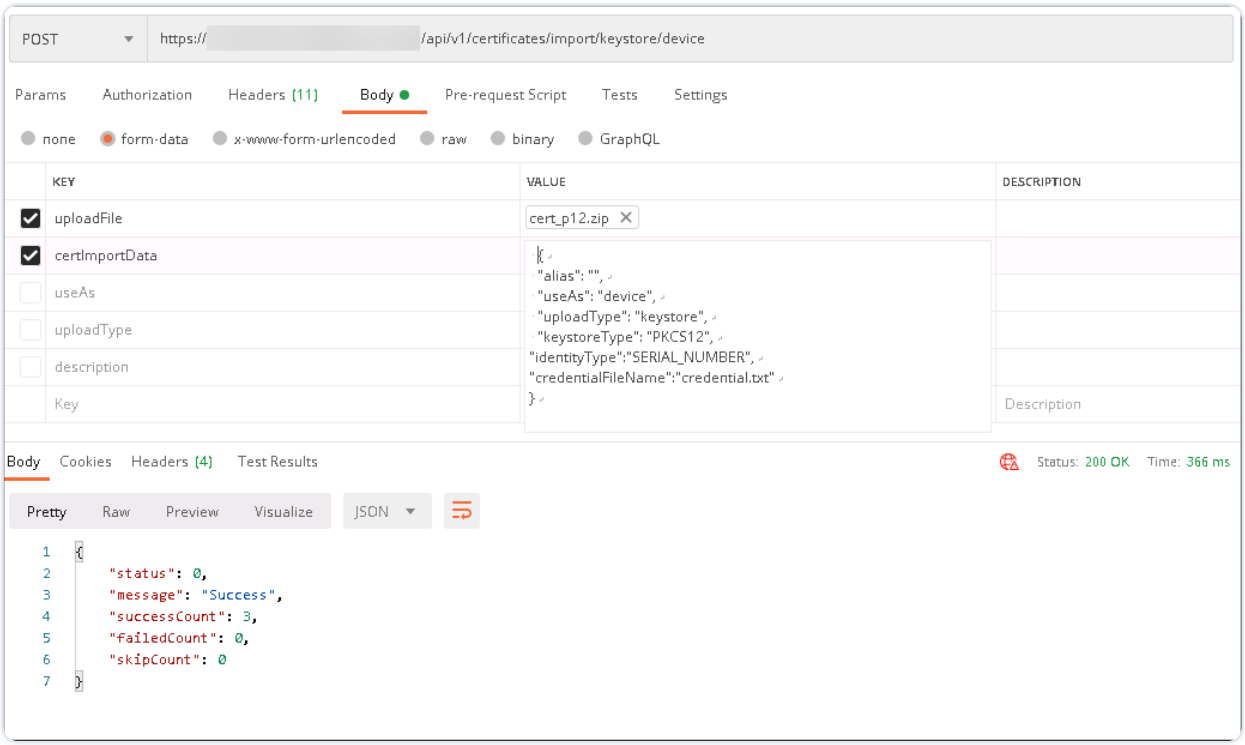
    "keystoreType": "PKCS12",

    "identityType":"SERIAL_NUMBER",        # identity type can be
"SERIAL_NUMBER","IMEI","MEID"

    "credentialFileName":"credential.txt"   # The credential file name
in .zip

}
```

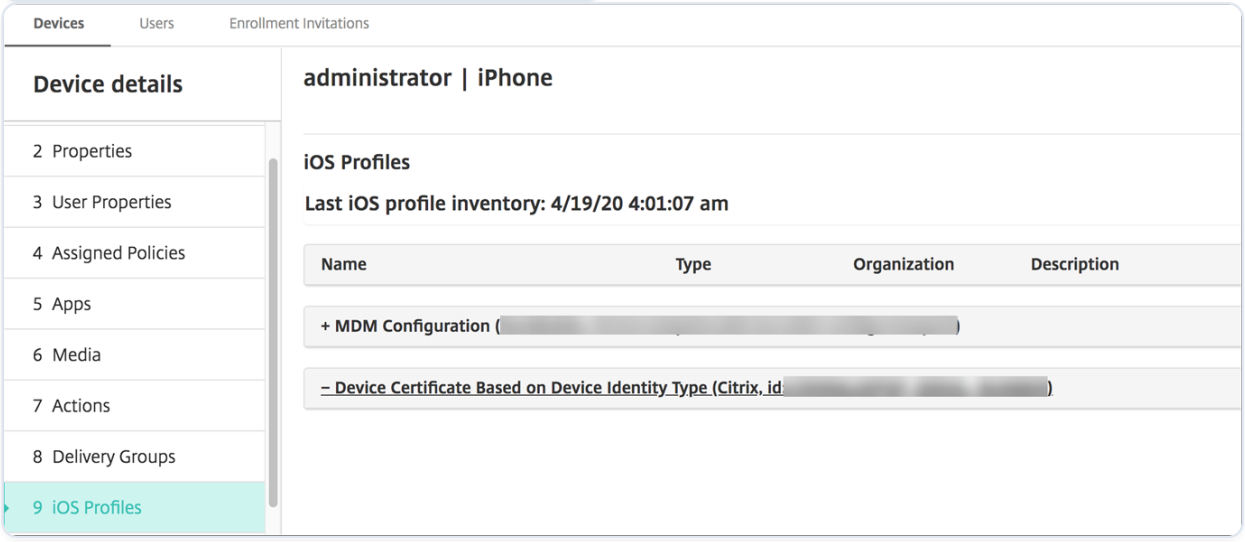
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 資格情報タイプを**Always on IKEv2**に設定し、デバイス認証方法を**Device Certificate Based on Device Identity**に設定して、VPNポリシーを作成します。証明書ファイル名で使用した**デバイスIDタイプ**を選択します。VPNデバイスポリシーを参照してください。
7. iOSデバイスを登録し、VPNポリシーが展開されるのを待ちます。デバイスのMDM構成を確認して、証明書のインストールを確認します。Citrix Endpoint Managementコンソールでデバイスの詳細を確認することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

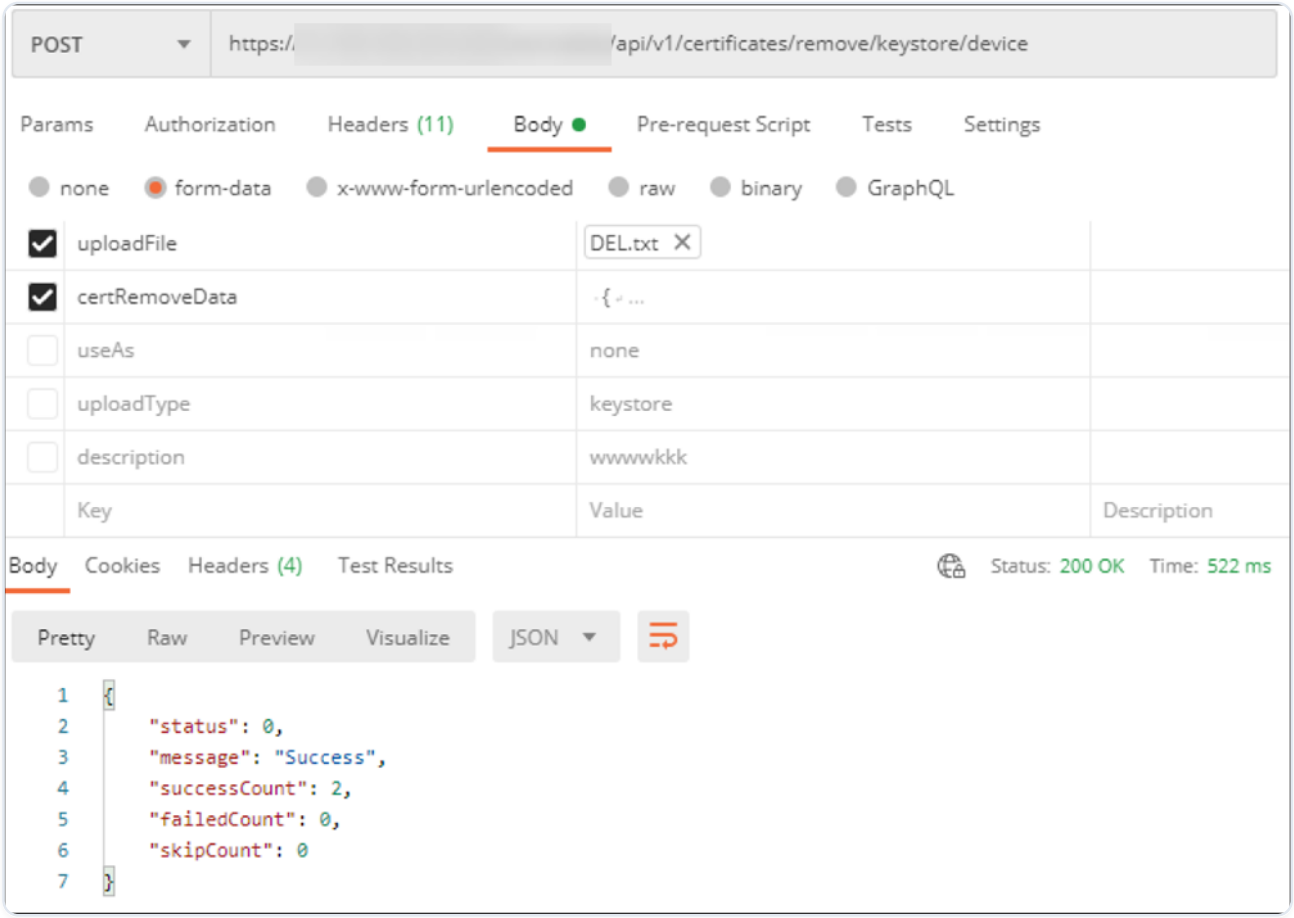




© 1997–2026 Citrix Systems, Inc. All rights reserved.

削除する各証明書について`device_identity_value`をリストしたテキストファイルを作成することで、証明書を一括削除することもできます。REST APIで、削除APIを呼び出し、`device_identity_value`を適切な識別子に置き換えて次のリクエストを使用します。

```
{
    "identityType"="device_identity_value"
}
```



証明書の更新

Citrix Endpoint Managementでは、システム内に同時に存在する公開鍵ごとの証明書は1つのみです。既にインポートされている証明書と同じキーペアの証明書をインポートしようとすると、次のことができます。

- 既存のエントリを置き換えます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- エントリを削除します。

古い証明書を置き換えるために新しい証明書をアップロードした後、古い証明書を削除することはできません。PKIエンティティ設定を構成すると、両方の証明書が**SSLクライアント証明書**メニューに存在します。新しい証明書は、古い証明書よりもリストの下に表示されます。

証明書を更新するには

1. クライアント証明書または証明書とドメイン認証の手順に従って、代替証明書を作成します。

   重要：

   既存の秘密キーで証明書を作成するオプションは使用しないでください。期限切れの証明書を更新するために証明書を作成する場合、秘密キーも新しいものである必要があります。

2. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。検索バーを使用して、**証明書**設定を見つけて開きます。
3. **インポート**ダイアログボックスで、新しい証明書をインポートします。

サーバー証明書を更新すると、以前の証明書を使用していたコンポーネントは自動的に新しい証明書を使用するように切り替わります。同様に、デバイスにサーバー証明書を展開している場合、証明書は次回の展開時に自動的に更新されます。

APNs証明書を更新するには、証明書を作成する手順を実行し、Apple Push Certificates Portalにアクセスします。詳しくは、APNs証明書を更新するを参照してください。

NetScaler GatewayがSSLオフロード用に設定されている場合は、新しいcacert.pemでロードバランサーを更新していることを確認してください。

注：

XenMobileオンプレミスからCitrix Endpoint Managementに移行し、証明書を更新している場合は、上記の手順を完了した後、Citrixサポートに連絡してください。新しい証明書のコピー（PFX形式）と証明書のパスワードを提供する必要があります。Citrixサポートがクラウド NetScalerを更新し、テナントノードを再起動して証明書の更新プロセスを完了します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PKIサービス証明機関（CA）を更新するには

Citrix Cloud Operationsに、Citrix Endpoint Management展開内の内部PKI証明機関（CA）を更新または再生成するよう要求できます。これらの要求については、テクニカルサポートケースを開いてください。

```
When the new CAs are available, Cloud Operations lets you know that you
can proceed with renewing the device certificates for your users.
```

デバイス証明書を更新する

デバイス上の証明書の有効期限が切れると、その証明書は無効になります。環境で安全なトランザクションを実行できなくなり、Citrix Endpoint Managementリソースにアクセスできなくなります。認証局 (CA) は、有効期限が切れる前にSSL証明書を更新するように促します。証明書を更新するには、前述の手順を実行し、登録済みデバイスで証明書の更新を開始します。

サポートされているiOS、macOS、およびAndroidデバイスの場合、セキュリティアクションの「証明書の更新」を通じて証明書の更新を開始できます。Citrix Endpoint Managementコンソールまたはパブリック REST APIからデバイス証明書を更新します。登録済みのWindowsデバイスの場合、ユーザーは新しいデバイス認証局 (CA) を受け取るためにデバイスを再登録する必要があります。

デバイスが次回Citrix Endpoint Managementに接続するときに、Citrix Endpoint Managementサーバーは新しいCAに基づいて新しいデバイス証明書を発行します。

コンソールを使用してデバイス証明書を更新するには

1. **>** に移動し、デバイス証明書を更新するデバイスを選択します。
2. をクリックし、 をクリックします。



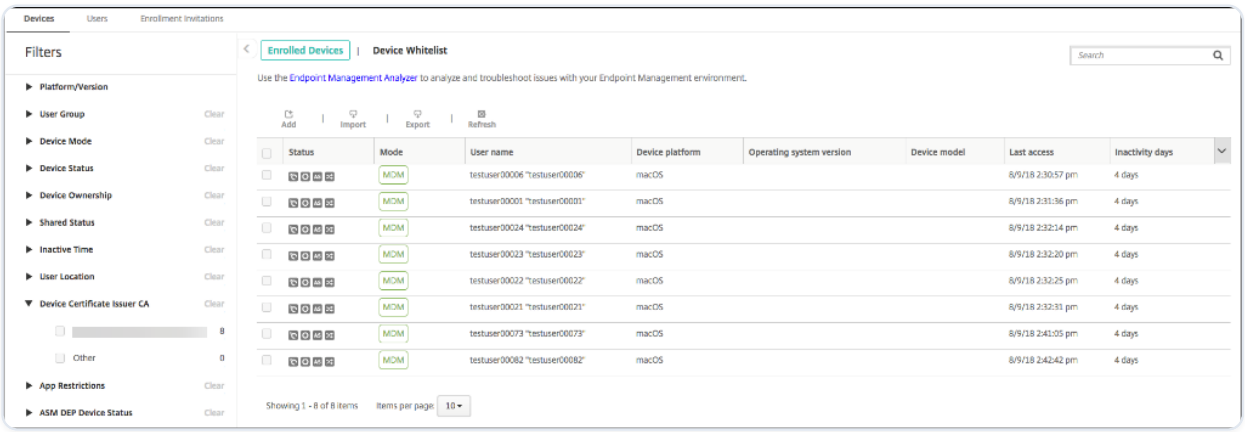
© 1997–2026 Citrix Systems, Inc. All rights reserved.

登録済みのデバイスは中断することなく動作し続けます。Citrix Endpoint Managementは、デバイスがサーバーに再接続したときにデバイス証明書を発行します。

特定のデバイス証明書発行元CAグループに属するデバイスを照会するには：

1. **>** で、 ペインを展開します。
2. ペインで、 を展開し、更新する発行元CAを選択します。

   デバイスのテーブルに、選択した発行元CAのデバイスが表示されます。



REST APIを使用してデバイス証明書を更新するには

Citrix Endpoint Managementは、PKIのために内部的に次の認証局 (CA) を使用します: ルートCA、デバイスCA、およびサーバーCA。これらのCAは論理グループであり、グループ名を持っています。Citrix Endpoint Managementのプロビジョニング中に、サーバーは3つのCAを生成し、それらに「default」というグループ名を付けます。

CA は、デバイス証明書を管理および更新するために次の API を発行します。すでに登録されているデバイスは、中断することなく動作し続けます。Citrix Endpoint Management は、デバイスがサーバーに再接続したときにデバイス証明書を発行します。詳細については、Public API for REST Services PDF をダウンロードしてください。

- 古い CA をまだ使用しているデバイスのリストを返します (Public API for REST Services PDF のセクション 3.16.2 を参照)。
- デバイス証明書の更新 (セクション 3.16.58 を参照)
- すべての CA グループを取得 (セクション 3.23.1 を参照)

Citrix Secure Mail 用 APNs 証明書

Apple Push Notification Service (APNs) 証明書は毎年期限切れになります。証明書の期限が切れる前に、APNs SSL 証明書を作成し、Citrix ポータルで更新してください。証明書の期限が切れる

© 1997–2026 Citrix Systems, Inc. All rights reserved.

と、ユーザーは Citrix Secure Mail のプッシュ通知で不整合に直面します。また、アプリのプッシュ通知を送信できなくなります。

iOS デバイス管理用 APNs 証明書

Citrix Endpoint Management で iOS デバイスを登録および管理するには、Apple から APNs 証明書を設定および作成します。証明書の期限が切れると、ユーザーは Citrix Endpoint Management に登録できなくなり、iOS デバイスを管理できなくなります。詳細については、APNs certificates を参照してください。

Apple Push Certificates Portal にログオンすると、APNs 証明書のステータスと有効期限を表示できます。証明書を作成したのと同じユーザーとしてログオンしてください。

また、有効期限の 30 日前と 10 日前に Apple からメール通知が届きます。通知には次の情報が含まれます。

```
The following Apple Push Notification Service certificate, created for
Apple ID CustomerID will expire on Date. Revoking or allowing this
certificate to expire will require existing devices to be re-enrolled with
a new push certificate.



Please contact your vendor to generate a new request (a signed CSR), then
visit https://identity.apple.com/pushcert to renew your Apple Push
Notification Service certificate.



Thank You,



Apple Push Notification Service
```

MDX Toolkit (iOS 配布証明書)

物理的な iOS デバイスで実行されるアプリ (Apple App Store のアプリを除く) には、次の署名要件があります。

- プロビジョニングプロファイルでアプリに署名します。
- 対応する配布証明書でアプリに署名します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有効な iOS 配布証明書があることを確認するには、次の手順を実行します。

1. Apple Enterprise Developer portal から、MDX でラップする各アプリの明示的な App ID を作成します。許容される App ID の例は次のとおりです: `com.CompanyName.ProductName`。
2. Apple Enterprise Developer portal から、**Provisioning Profiles > Distribution** に移動し、社内プロビジョニングプロファイルを作成します。前の手順で作成した各 App ID について、この手順を繰り返します。
3. すべてのプロビジョニングプロファイルをダウンロードします。詳細については、「Wrapping iOS Mobile Apps」を参照してください。

すべての Citrix Endpoint Management サーバー証明書が有効であることを確認するには、次の手順を実行します。

1. Citrix Endpoint Management コンソールで、**Settings > Certificates** をクリックします。
2. APNs、SSL Listener、Root、および Intermediate 証明書を含むすべての証明書が有効であることを確認します。

Android キーストア

キーストアは、Android アプリの署名に使用される証明書を含むファイルです。キーの有効期間が終了すると、ユーザーはアプリの新しいバージョンにシームレスにアップグレードできなくなります。

ネットスケーラー ゲートウェイ

NetScaler Gateway の証明書の有効期限の処理方法の詳細については、Citrix Support Knowledge Center の「How to handle certificate expiry on NetScaler」を参照してください。

有効期限が切れた NetScaler Gateway 証明書は、ユーザーが登録して Store にアクセスするのを妨げます。また、有効期限が切れた証明書は、Citrix Secure Mail を使用している場合にユーザーが Exchange Server に接続するのを妨げます。さらに、ユーザーは HDX アプリを列挙して開くことができません (どの証明書が有効期限切れになったかによって異なります)。

Expiry Monitor と Command Center は、NetScaler Gateway 証明書を追跡するのに役立ちます。証明書の有効期限が切れると、Center が通知します。これらのツールは、次の NetScaler Gateway 証明書を監視するのに役立ちます。

- MDM FQDN 用 SSL 証明書
- Gateway FQDN 用 SSL 証明書
- ShareFile SZC FQDN 用 SSL 証明書

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Exchangeロードバランシング用SSL証明書 (オフロード構成)
- StoreFrontロードバランシング用SSL証明書
- 上記の証明書用のルートおよび中間CA証明書

ネットスケーラー ゲートウェイ と シトリックス エンドポイント マネジメント

Citrix Endpoint Managementと統合すると、NetScaler Gatewayは内部ネットワークとリソースへのリモートデバイスアクセスを提供します。Citrix Endpoint Managementは、デバイス上のアプリからNetScaler GatewayへのマイクロVPNを作成します。

Citrix Gatewayサービス（プレビュー）またはオンプレミスのNetScaler Gateway（NetScaler Gatewayとも呼ばれます）を使用できます。2つのNetScaler Gatewayソリューションの概要については、「Citrix Endpoint ManagementでのNetScaler Gatewayの使用を構成する」を参照してください。

内部ネットワークへのリモートデバイスアクセスの認証を構成する

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。「**設定**」ページが表示されます。
2. **サーバー**の下にある**NetScaler Gateway**をクリックします。「**NetScaler Gateway**」ページが表示されます。次の例では、NetScaler Gatewayインスタンスが存在します。



3. 次の設定を構成します。
   - **認証:** 認証を有効にするかどうかを選択します。デフォルトは**オン**です。
   - **認証用のユーザー証明書を配信:** Citrix Endpoint Managementが認証証明書をCitrix Secure Hubと共有するかどうかを選択します。証明書を共有すると、NetScaler Gatewayがクライアント証明書認証を処理できるようになります。デフォルトは**オフ**です。
   - **資格情報プロバイダー:** ドロップダウンリストから使用する資格情報プロバイダーをクリックします。詳細については、「資格情報プロバイダー」を参照してください。
4. **保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Gatewayサービスインスタンス（プレビュー）を追加する

認証設定を保存した後、NetScaler GatewayインスタンスをCitrix Endpoint Managementに追加します。

1. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。「**設定**」ページが開きます。
2. 「**設定**」ページで、NetScaler Gatewayタイルまでスクロールし、「**セットアップの開始**」をクリックします。「**NetScaler Gateway**」ページが表示されます。
3. **Citrix Gatewayサービス (クラウド)** を選択し、Gatewayサービスのリソースの場所を指定します。

   NetScaler Gateway構成画面(/en-us/citrix-endpoint-management/media/settings-add-gateway-service.png)

   - **Gatewayサービスのリソースの場所:** は、Citrix Secure Mailを使用する場合に必要です。STAサービスのリソースの場所を指定します。リソースの場所には、構成済みのNetScaler Gatewayが含まれている必要があります。後でGatewayサービス用に構成されているリソースの場所を削除する場合は、この設定を更新します。

   これらの設定を完了したら、**接続** をクリックして接続を確立します。新しいNetScaler Gatewayが追加されます。**Citrix Gatewayサービス (クラウド)** タイルが **設定** ページに表示されます。インスタンスを編集するには、**詳細を表示** をクリックします。選択したリソースの場所でGateway Connectorが利用できない場合は、**Gateway Connectorの追加** をクリックします。画面の指示に従ってGateway Connectorをインストールします。Gateway Connectorは後で追加することもできます。
4. 「**スクリプトの保存とエクスポート**」をクリックします。

   - 「**スクリプトの保存とエクスポート**」をクリックします。このボタンをクリックして設定を保存し、構成バンドルをエクスポートします。バンドルからスクリプトをNetScaler Gatewayにアップロードして、Citrix Endpoint Management設定で構成できます。詳細については、これらの手順の後に「Citrix Endpoint Managementで使用するためのオンプレミスNetScaler Gatewayの構成」を参照してください。

   新しいNetScaler Gatewayが追加されました。「**NetScaler Gateway**」タイルが「**設定**」ページに表示されます。インスタンスを編集するには、「**詳細を表示**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementで使用するためのオンプレミスNetScaler Gatewayの構成

Citrix Endpoint Managementで使用するためにオンプレミスNetScaler Gatewayを構成するには、次のセクションで詳述されている一般的な手順を実行します。

1. 環境が前提条件を満たしていることを確認します。
2. Citrix Endpoint Managementコンソールからスクリプトバンドルをエクスポートします。
3. バンドルからファイルを抽出します。NetScaler Gatewayでクラシックポリシーのみを使用しており、Citrix ADC 13.0以前を実行している場合は、ファイル名に「Classic」を含むスクリプトを使用します。高度なポリシーを使用しているか、Citrix ADC 13.1以降を実行している場合は、ファイル名に「Advanced」を含むスクリプトを使用します。
4. NetScaler Gatewayで適切なスクリプトを実行します。最新の詳細な手順については、スクリプトに付属のreadmeファイルを参照してください。
5. 構成をテストします。

スクリプトは、Citrix Endpoint Management で必要となる以下の NetScaler Gateway 設定を構成します。

- MDM および MAM に必要な NetScaler Gateway 仮想サーバー
- NetScaler Gateway 仮想サーバーのセッションポリシー
- Citrix Endpoint Management サーバーの詳細
- 証明書検証用のプロキシロードバランサー
- NetScaler Gateway 仮想サーバーの認証ポリシーとアクション。スクリプトは LDAP 構成設定について説明します。
- プロキシサーバーのトラフィックアクションとポリシー
- クライアントレスアクセスプロファイル
- NetScaler Gateway 上の静的ローカル DNS レコード
- その他のバインディング: サービスポリシー、CA 証明書

スクリプトは以下の構成を処理しません。

- Exchange ロードバランシング
- Citrix Files ロードバランシング
- ICA® プロキシ構成
- SSL オフロード

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway 構成スクリプトを使用するための前提条件

シトリックス エンドポイント マネジメント の要件:

- スクリプトバンドルをエクスポートする前に、Citrix Endpoint Management で LDAP および NetScaler Gateway の構成を完了します。設定を変更した場合は、スクリプトバンドルを再度エクスポートしてください。

NetScaler Gateway の要件:

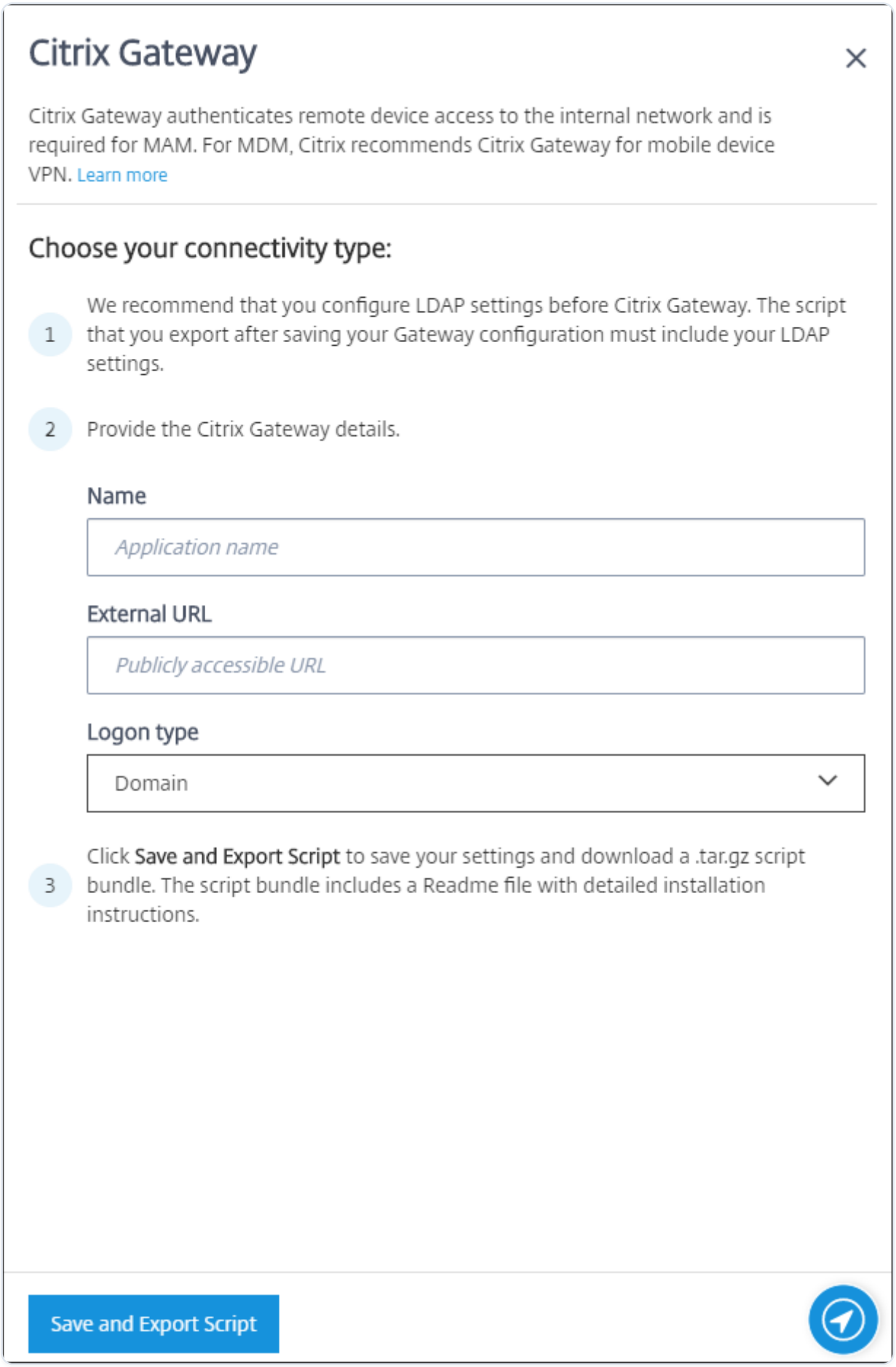
- NetScaler Gateway で証明書ベースの認証を使用する場合は、Citrix ADC Appliance で SSL 証明書を作成する必要があります。Citrix ADC Appliance で SSL 証明書を作成して使用するを参照してください。
- NetScaler Gateway (最小バージョン 11.0、ビルド 70.12)。
- NetScaler Gateway の IP アドレスが構成されており、LDAP がロードバランスされていない限り、LDAP サーバーへの接続が確立されていること。
- NetScaler Gateway サブネット (SNIP) IP アドレスが構成されており、必要なバックエンドサーバーへの接続が確立されており、ポート 8443/TCP を介したパブリックネットワークアクセスがあること。
- DNS がパブリックドメインを解決できること。
- NetScaler Gateway は、Platform/Universal または Trial ライセンスでライセンスされています。詳細については、`<https://support.citrix.com/article/CTX126049>`を参照してください。

Citrix Endpoint Management からスクリプトバンドルをエクスポートする

認証設定を保存した後、NetScaler Gateway インスタンスを Citrix Endpoint Management に追加します。

1. Citrix Endpoint Management コンソールで、右上隅にある歯車アイコンをクリックします。ページが開きます。
2. ページで、NetScaler Gateway タイルまでスクロールし、 をクリックします。 ページが表示されます。
3. を選択し、次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **名前:** NetScaler Gatewayインスタンスの名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **外部URL:** NetScaler Gatewayの公開アクセス可能なURLを入力します。例: `https://receiver.com`.
- **ログオンの種類:** ログオンの種類を選択します。種類には、**ドメイン**、**セキュリティトークンのみ**、**ドメインとセキュリティトークン**、**証明書**、**証明書とドメイン**、**証明書とセキュリティトークン**があります。デフォルトは**ドメイン**です。

複数のドメインがある場合は、**証明書とドメイン**を使用します。詳細については、「複数のドメインの認証を構成する」を参照してください。

NetScaler Gatewayでの証明書ベースの認証には、追加の構成が必要です。たとえば、ルートCA証明書をCitrix ADCアプライアンスにアップロードする必要があります。「Citrix ADCアプライアンスでSSL証明書を作成して使用する」を参照してください。

詳細については、展開ハンドブックの「認証」を参照してください。

4. **スクリプトを保存してエクスポート**をクリックします。

   - **スクリプトを保存してエクスポート**。ボタンをクリックして設定を保存し、構成バンドルをエクスポートします。バンドルからスクリプトをNetScaler Gatewayにアップロードして、Citrix Endpoint Management設定で構成できます。詳細については、これらの手順の後に「オンプレミスNetScaler GatewayをCitrix Endpoint Managementで使用するように構成する」を参照してください。

   新しいNetScaler Gatewayが追加されました。**NetScaler Gateway**タイルが**設定**ページに表示されます。インスタンスを編集するには、**詳細を表示**をクリックします。

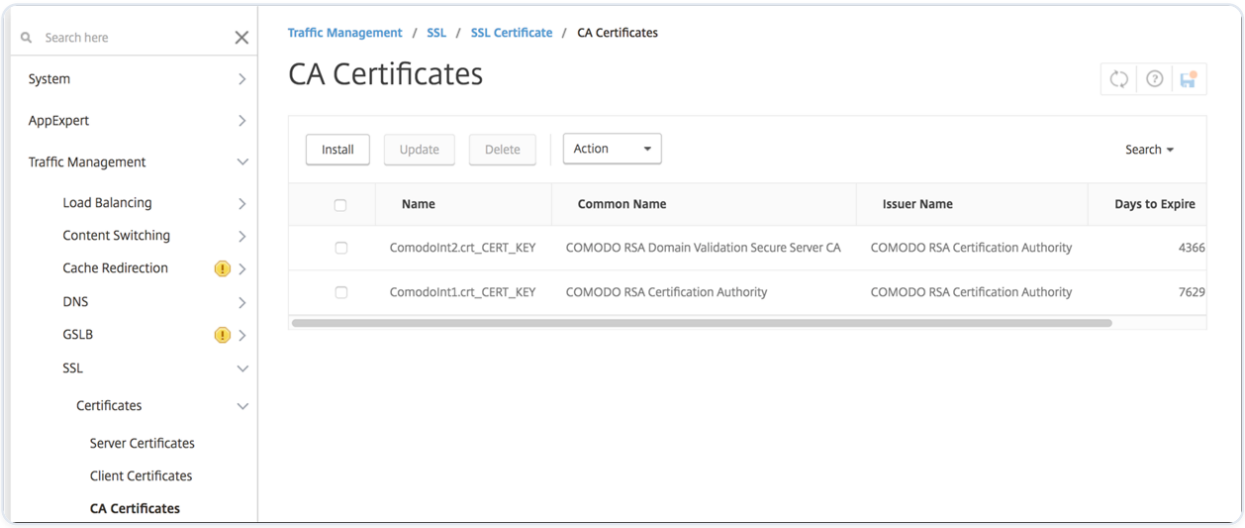
環境にスクリプトをインストールする

スクリプトバンドルには以下が含まれます。

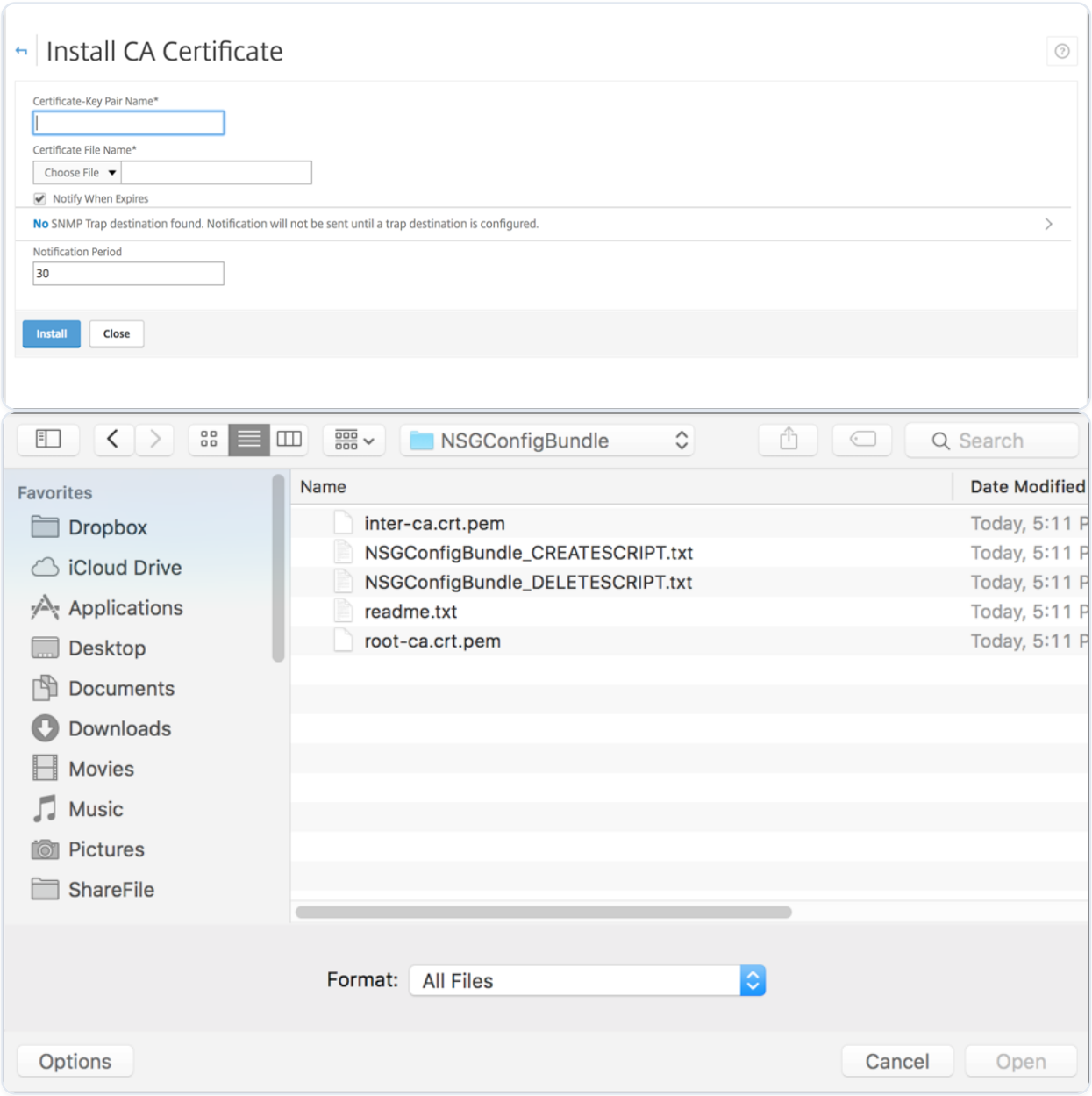
- 詳細な手順が記載されたReadmeファイル
- NetScalerで必要なコンポーネントを構成するために使用されるNetScaler® CLIコマンドを含むスクリプト
- 公開ルートCA証明書と中間CA証明書
- NetScaler構成を削除するために使用されるNetScaler CLIコマンドを含むスクリプト

1. 証明書ファイル（スクリプトバンドルに含まれています）をCitrix ADCアプライアンスの/nsconfig/ssl/ディレクトリにアップロードしてインストールします。「Citrix ADCアプライアンスでSSL証明書を作成して使用する」を参照してください。

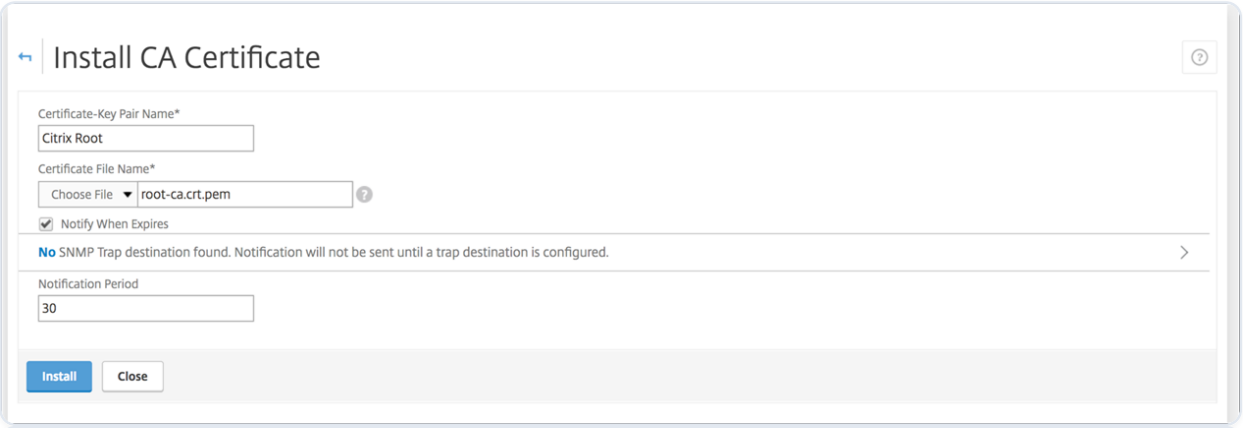
© 1997–2026 Citrix Systems, Inc. All rights reserved.

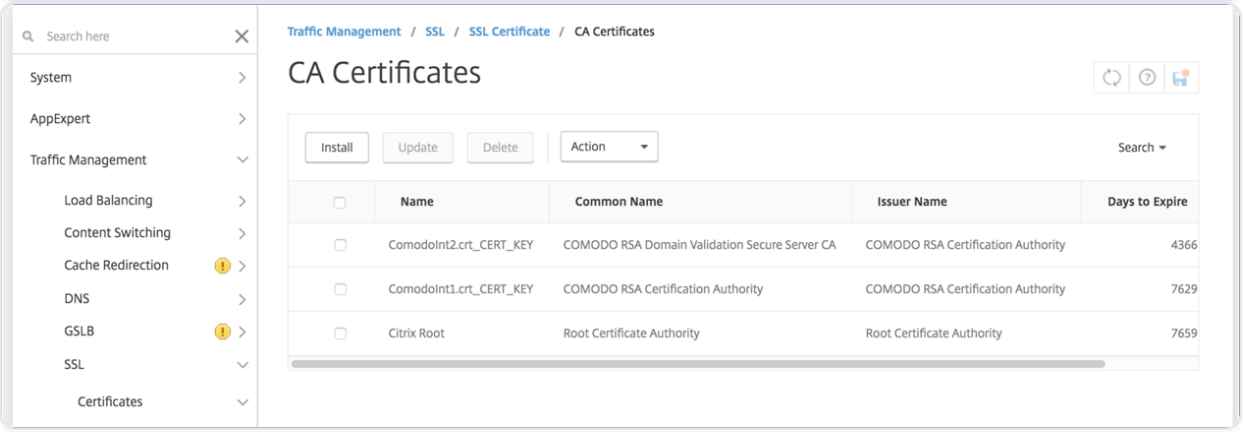


次の例は、ルート証明書をインストールする方法を示しています。



© 1997–2026 Citrix Systems, Inc. All rights reserved.





ルート証明書と中間証明書の両方をインストールしてください。

2. スクリプト（ConfigureCitrixGatewayScript_Classic.txtまたはConfigureCitrixGatewayScript_Advanced.txt）を編集し、すべてのプレースホルダーを環境の詳細に置き換えます。

```
#Important Note: Please update the following placeholders with valid values:
# <NSG_IP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reachable from your devices either directly or via a NAT.
# <PROXY_LB_VIP> -- Virtual IP Address to be assigned to the proxy load-balancer configured on the NetScaler. This IP address must be a private address.
# <LDAP_SVC_USERNAME> -- LDAP Service Account Username.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <SERVER_CERT_NAME> -- Name of the server certificate file on the NetScaler. This certificate is bound to the NetScaler Gateway virtual server.
```

3. スクリプトバンドルに含まれているreadmeファイルに記載されているとおり、編集したスクリプトをNetScaler bashシェルで実行します。例：

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/OfflineNSGConfigtBundle_CREATESCRIPT.txt"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you are not an authorized user!            #
#                                                                              #
################################################################################

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

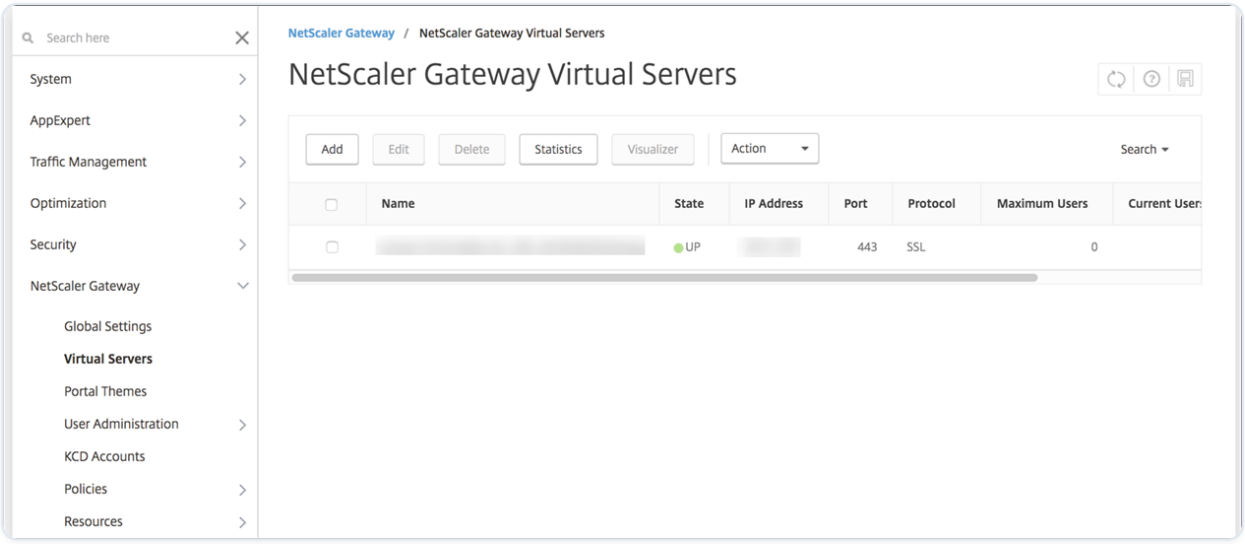
スクリプトが完了すると、次の行が表示されます。

```
exec: save ns config
 Done
 Done
root@ns#
```

構成をテストする

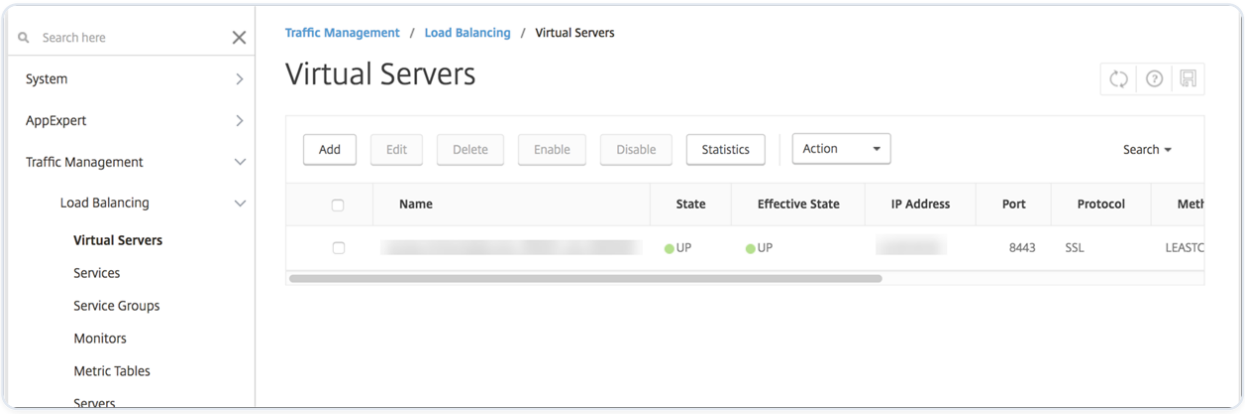
構成を検証するには:

1. NetScaler Gateway仮想サーバーが**UP**状態であることを確認します。



2. プロキシ負荷分散仮想サーバーが**UP**状態であることを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Webブラウザを開き、NetScaler Gateway URLに接続して、認証を試行します。認証が成功すると、「HTTP Status 404 - Not Found」メッセージにリダイレクトされます。
4. デバイスを登録し、MDMとMAMの両方の登録が行われることを確認します。

複数のドメインの認証を構成する

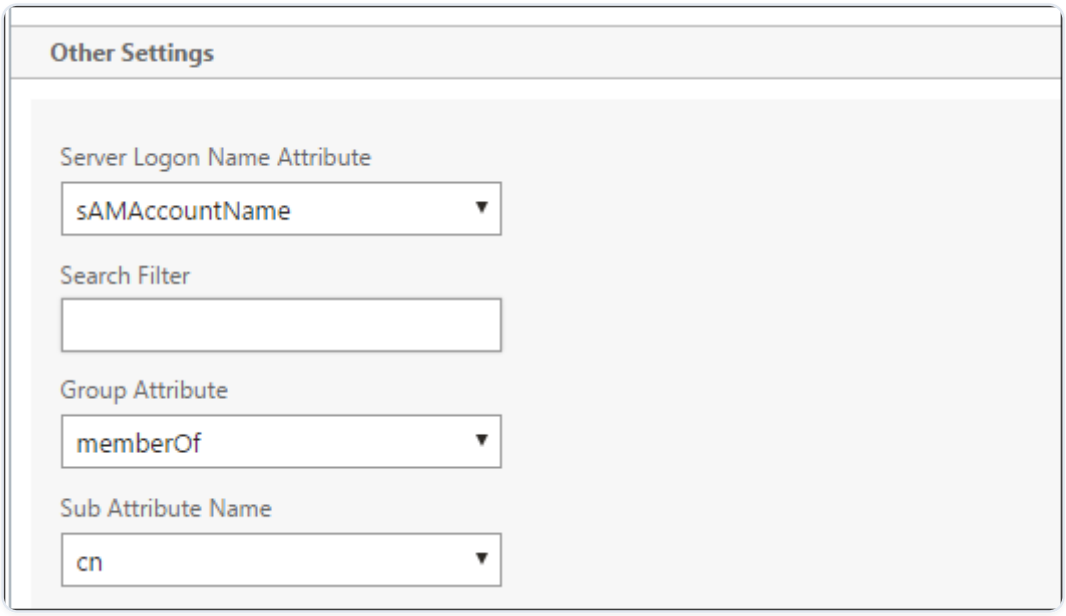
テスト、開発、および本番環境など、複数のCitrix Endpoint Managementインスタンスがある場合は、追加の環境に対してNetScaler Gatewayを手動で構成します。（NetScaler for XenMobileウィザードは1回しか使用できません。）

NetScaler Gatewayの構成

複数ドメイン環境のNetScaler Gateway認証ポリシーとセッションポリシーを構成するには:

1. NetScaler Gateway構成ユーティリティで、**Configuration**タブの**NetScaler Gateway > Policies > Authentication**を展開します。
2. ナビゲーションペインで、**LDAP**をクリックします。
3. LDAPプロファイルを編集するにはクリックします。**サーバーログオン名属性**を**userPrincipalName**または検索に使用する属性に変更します。指定した属性をメモしておきます。これはCitrix Endpoint Managementコンソールで LDAP設定を構成する際に指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

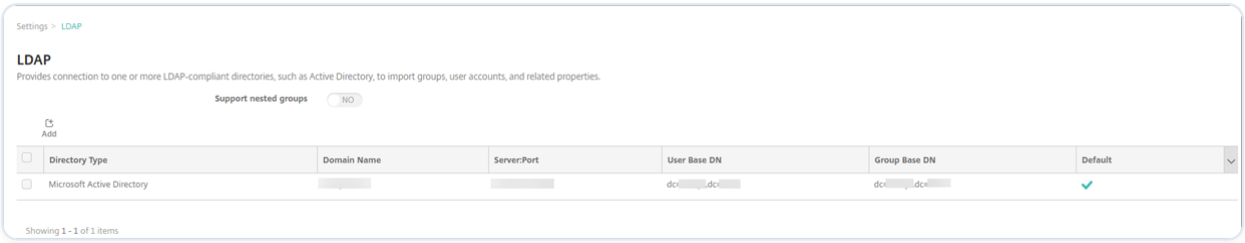


4. 各LDAPポリシーに対してこれらの手順を繰り返します。ドメインごとに個別のLDAPポリシーが必要です。
5. NetScaler Gateway仮想サーバーにバインドされているセッションポリシーで、**セッションプロファイルの編集 > 公開アプリケーション**に移動します。**シングルサインオン ドメイン**が空白であることを確認します。

シトリックス エンドポイント マネジメント の構成

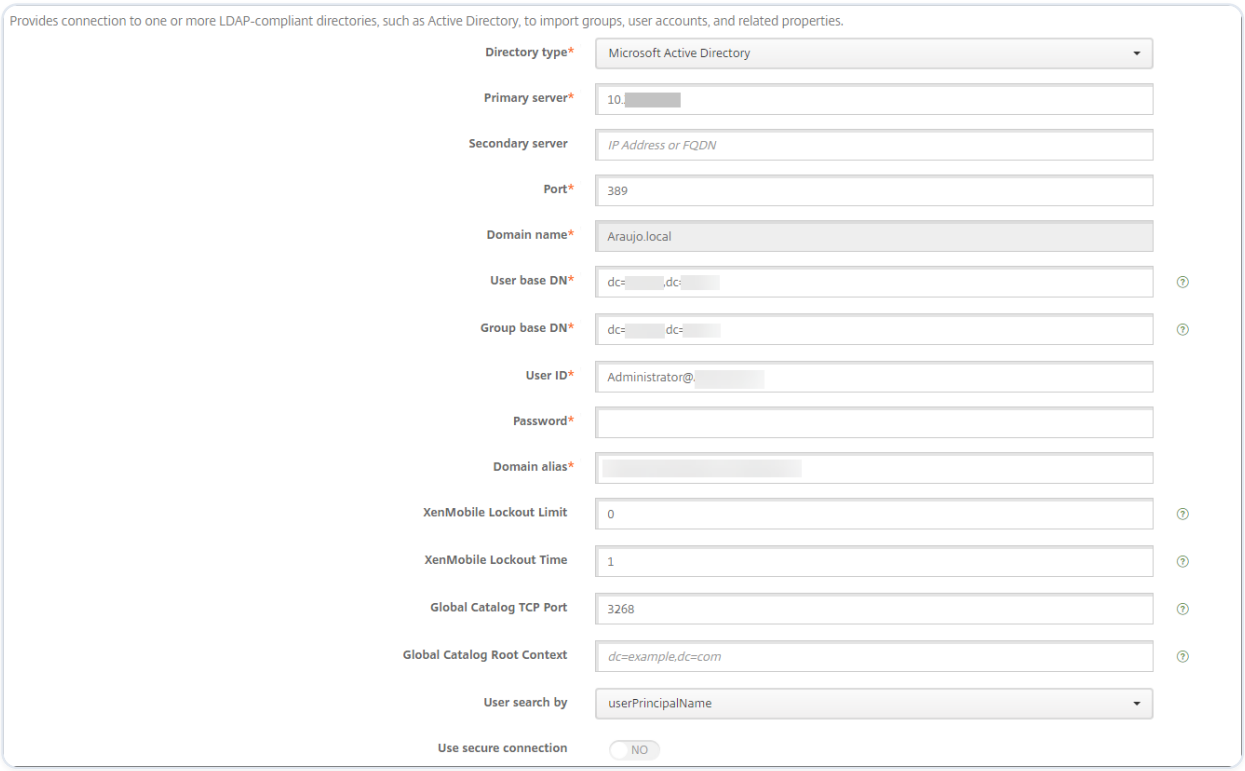
マルチドメイン環境向けにCitrix Endpoint Management LDAPを構成するには：

1. Citrix Endpoint Managementコンソールで、**設定 > LDAP**に移動し、ディレクトリを追加または編集します。



2. 情報を入力します。
   - **ドメインエイリアス**で、ユーザー認証に使用する各ドメインを指定します。ドメインはコンマで区切り、ドメイン間にスペースを使用しないでください。例：domain1.com,domain2.com,domain3.com
   - **ユーザー検索基準**フィールドが、NetScaler Gateway LDAPポリシーで指定された**サーバーログオン名属性**と一致していることを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



特定のURLへのインバウンド接続要求を破棄する

環境内のNetScaler GatewayがSSLオフロード用に構成されている場合、ゲートウェイが特定のURLへのインバウンド接続要求を破棄するように設定することをお勧めします。この追加のセキュリティを希望する場合は、Citrix Cloud Operationsに連絡し、オンプレミスデータセンターへのIPを許可するよう要求してください。

ドメインまたはドメインとセキュリティトークン認証

Citrix Endpoint Managementは、LDAP (Lightweight Directory Access Protocol) に準拠した1つ以上のディレクトリに対するドメインベースの認証をサポートしています。Citrix Endpoint Managementで1つ以上のディレクトリへの接続を構成します。Citrix Endpoint Managementは、LDAP構成を使用してグループ、ユーザーアカウント、および関連プロパティをインポートします。

重要:

Citrix Endpoint Managementは、ユーザーがCitrix Endpoint Managementにデバイスを登録した後で、認証モードをある種類の認証モードから別の認証モードに変更することをサポートしていません。たとえば、ユーザーが登録した後で、認証モードを**ドメイン認証**から**ドメイン + 証明書**に変更することはできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LDAPについて

LDAPは、インターネットプロトコル (IP) ネットワーク上で分散ディレクトリ情報サービスにアクセスし、維持するためのオープンソースのベンダーニュートラルなアプリケーションプロトコルです。ディレクトリ情報サービスは、ネットワーク全体で利用可能なユーザー、システム、ネットワーク、サービス、およびアプリケーションに関する情報を共有するために使用されます。

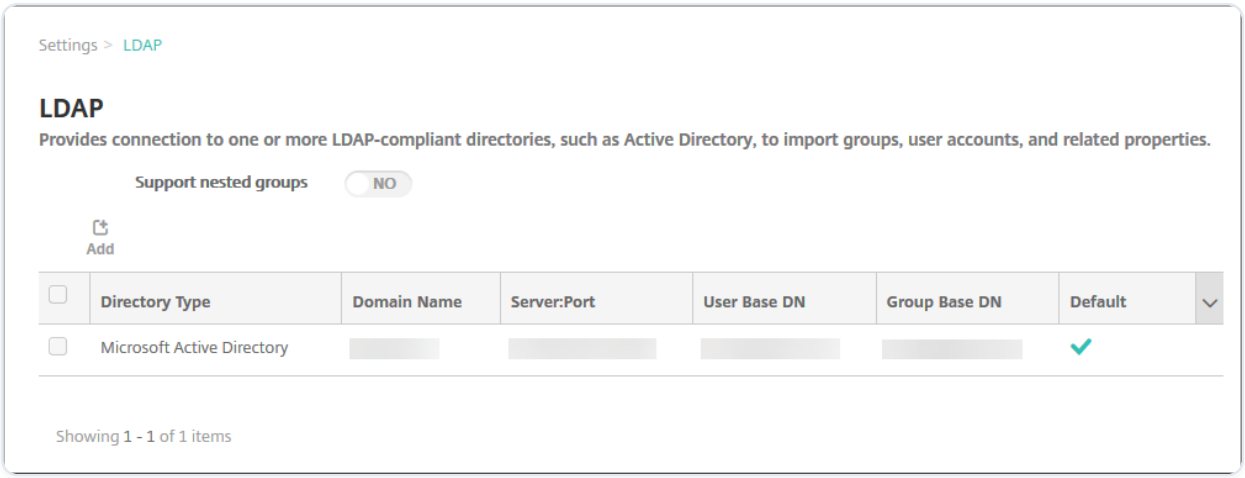
LDAPの一般的な使用法は、ユーザーにシングルサインオン (SSO) を提供することです。これは、1つのパスワード (ユーザーごと) が多くのサービスで共有されるものです。シングルサインオンにより、ユーザーは会社のWebサイトに一度ログオンするだけで、企業イントラネットへの認証済みアクセスが可能になります。

クライアントは、ディレクトリシステムエージェント (DSA) と呼ばれるLDAPサーバーに接続することでLDAPセッションを開始します。その後、クライアントはサーバーに操作要求を送信し、サーバーは適切な認証で応答します。

Citrix Endpoint ManagementでLDAP接続を追加または編集するには

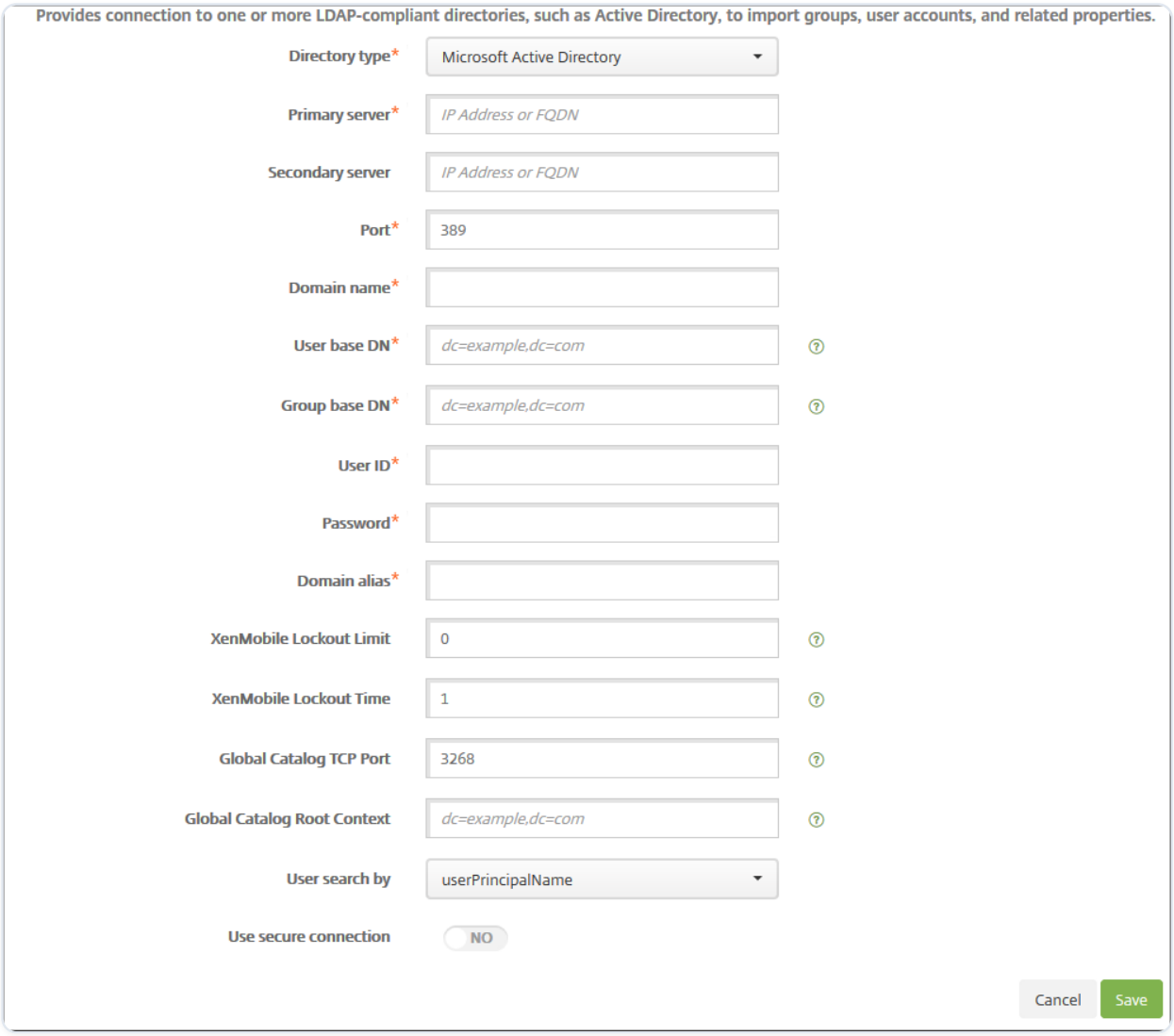
通常、LDAPを構成するにはで説明されているように、Citrix Endpoint Managementにオンボーディングする際にLDAP接続を構成します。そのセクションに示されている画面が利用可能になる前にオンボーディングした場合は、このセクションの情報を使用してLDAP接続を追加してください。

1. Citrix Endpoint Managementコンソールで、**［設定］>［LDAP］**の順に選択します。
2. **［サーバー］の下で、［LDAP］をクリックします。**［LDAP］**ページが表示されます。



3. **［LDAP］ページで、［追加］または［編集］をクリックします。**［LDAPの追加］**または［LDAPの編集］**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 以下の設定を構成します。

- **ディレクトリの種類:** ドロップダウンリストから適切なディレクトリの種類をクリックします。デフォルトは **Microsoft Active Directory** です。
- **プライマリサーバー:** LDAP に使用するプライマリサーバーを入力します。IP アドレスまたは完全修飾ドメイン名 (FQDN) のいずれかを入力できます。
- **セカンダリサーバー:** オプションで、セカンダリサーバーが構成されている場合は、その IP アドレスまたは FQDN を入力します。このサーバーは、プライマリサーバーに到達できない場合に使用されるフェールオーバーサーバーです。
- **ポート:** LDAP サーバーが使用するポート番号を入力します。デフォルトでは、保護されていない LDAP 接続の場合、ポート番号は **389** に設定されています。保護された LDAP 接続にはポート番号 **636** を使用し、Microsoft の保護されていない LDAP 接続には **3268** を、Microsoft の保護された LDAP 接続には **3269** を使用します。
- **ドメイン名:** ドメイン名を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ユーザーベース DN:** 一意の識別子を介して Active Directory 内のユーザーの場所を入力します。構文の例は次のとおりです: `ou=users`、`dc=example`、または `dc=com`。
- **グループベース DN:** Active Directory 内のグループの場所を入力します。たとえば、`cn=users, dc=domain, dc=net` の場合、`cn=users` はグループのコンテナ名を表し、`dc` は Active Directory のドメインコンポーネントを表します。
- **ユーザー ID:** Active Directory アカウントに関連付けられているユーザー ID を入力します。
- **パスワード:** ユーザーに関連付けられているパスワードを入力します。
- **ドメインエイリアス:** ドメイン名のエイリアスを入力します。登録後に **ドメインエイリアス** 設定を変更すると、ユーザーは再登録する必要があります。
- **Citrix Endpoint Management ロックアウト制限:** 失敗したログオン試行回数として、**0** から **999** までの数値を入力します。値が **0** の場合、Citrix Endpoint Management は失敗したログオン試行に基づいてユーザーをロックアウトしません。デフォルトは **0** です。

  このロックアウト制限を、LDAP ロックアウトポリシーよりも低い値に設定することを検討してください。これにより、Citrix Endpoint Management が LDAP サーバーに対して認証できない場合に、ユーザーのロックアウトを防ぐことができます。たとえば、LDAP ロックアウトポリシーが 5 回の試行である場合、このロックアウト制限を **4** 以下に構成します。
- **Citrix Endpoint Management ロックアウト時間:** ロックアウト制限を超過した後、ユーザーが待機する必要がある分数として、**0** から **99999** までの数値を入力します。値が **0** の場合、ユーザーはロックアウト後に待機を強制されません。デフォルトは **1** です。
- **グローバルカタログ TCP ポート:** グローバルカタログサーバーの TCP ポート番号を入力します。デフォルトでは、TCP ポート番号は **3268** に設定されています。SSL 接続の場合はポート番号 **3269** を使用します。
- **グローバルカタログルートコンテキスト:** オプションで、Active Directory でグローバルカタログ検索を有効にするために使用されるグローバルルートコンテキスト値を入力します。この検索は、実際のドメイン名を指定することなく、任意のドメインで標準のLDAP検索に追加して行われます。
- **ユーザー検索基準:** Citrix Endpoint Management がこのディレクトリでユーザーを検索するために使用するユーザー名またはユーザーIDの形式を選択します。ユーザーは登録時にこの形式でユーザー名またはユーザーIDを入力します。登録後に**ユーザー検索基準**の設定を変更した場合、ユーザーは再登録する必要があります。

  userPrincipalName を選択した場合、ユーザーはこの形式でユーザープリンシパル名 (UPN) を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `*username*@*domain*`

sAMAccountName を選択した場合、ユーザーは次のいずれかの形式でセキュアアカウントマネージャー (SAM) 名を入力します。

- `*username*@*domain*`
- `*domain\username*`

- **セキュア接続を使用:** セキュア接続を使用するかどうかを選択します。デフォルトは**いいえ**です。

5. **保存**をクリックします。

LDAP準拠ディレクトリを削除するには

1. **LDAP**テーブルで、削除するディレクトリを選択します。

   各プロパティの横にあるチェックボックスをオンにすることで、複数のプロパティを選択して削除できます。

2. **削除**をクリックします。確認ダイアログボックスが表示されます。もう一度**削除**をクリックします。

ドメインとセキュリティトークン認証を構成する

Citrix Endpoint Management を構成して、RADIUSプロトコルを使用して、ユーザーがLDAP資格情報とワンタイムパスワードで認証することを要求できます。

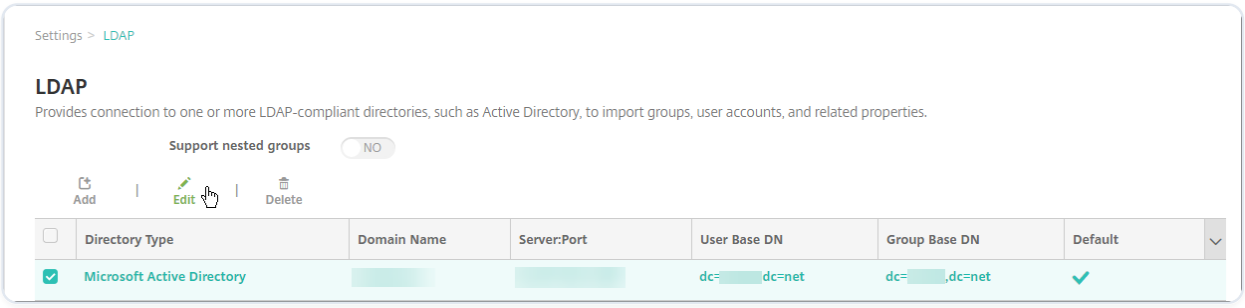
最適な使いやすさのために、この構成をCitrix PINおよびActive Directoryパスワードキャッシュと組み合わせることができます。この構成では、ユーザーはLDAPユーザー名とパスワードを繰り返し入力する必要がありません。ユーザーは、登録、パスワードの有効期限、およびアカウントのロックアウトのためにユーザー名とパスワードを入力します。

LDAP設定の構成

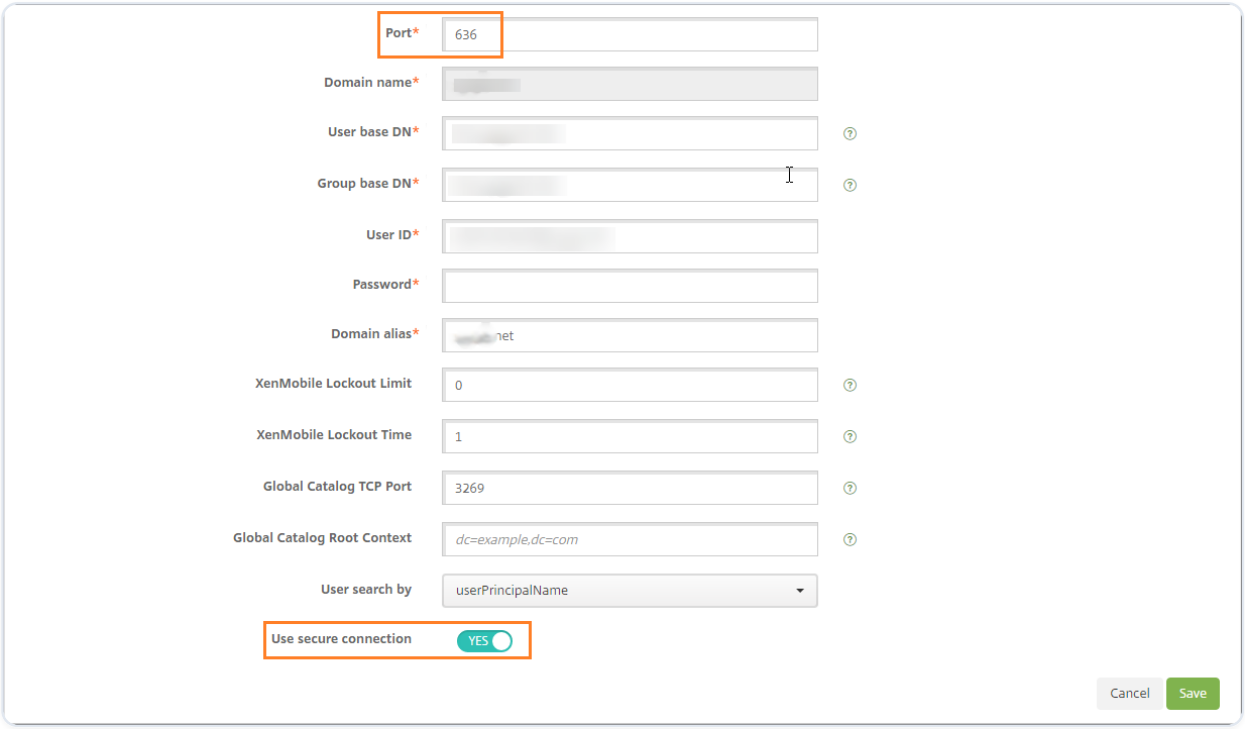
認証にLDAPを使用するには、Citrix Endpoint Managementに認証局からのSSL証明書をインストールする必要があります。詳しくは、「証明書のアップロード」を参照してください。

1. **Settings**で、**LDAP**をクリックします。
2. **Microsoft Active Directory**を選択し、**Edit**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. ポートがセキュアなLDAP接続の場合は**636**、Microsoftのセキュアなセキュアな接続の場合は**3269**であることを確認します。
4. **Use secure connection**を**Yes**に変更します。



NetScaler Gateway設定の構成

以下の手順は、Citrix Endpoint ManagementにNetScaler Gatewayインスタンスをすでに追加していることを前提としています。NetScaler Gatewayインスタンスを追加するには、「NetScaler GatewayとCitrix Endpoint Management」を参照してください。

1. **Settings**で、**NetScaler Gateway**をクリックします。
2. NetScaler Gatewayを選択し、**Edit**をクリックします。
3. **Logon Type**から、**Domain and security token**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix PINとユーザーパスワードキャッシュを有効にする

Citrix PINとユーザーパスワードのキャッシュを有効にするには、 > に移動し、 および のチェックボックスをオンにします。詳しくは、「クライアントプロパティ」(/ja-jp/citrix-endpoint-management/advanced-concepts/deployment/client-properties.html)を参照してください。

ドメインおよびセキュリティトークン認証用にNetScaler Gatewayを構成する

Citrix Endpoint Managementで使用される仮想サーバー向けにNetScaler Gatewayのセッションプロファイルとポリシーを構成します。詳しくは、NetScaler Gatewayのドキュメントを参照してください。

クライアント証明書または証明書とドメイン認証

Citrix Endpoint Management のデフォルト構成は、ユーザー名とパスワード認証です。Citrix Endpoint Management 環境への登録とアクセスに別のセキュリティ層を追加するには、証明書ベースの認証の使用を検討してください。Citrix Endpoint Management 環境では、この構成がセキュリティとユーザーエクスペリエンスの最良の組み合わせです。証明書とドメイン認証は、NetScaler Gateway での二要素認証によって提供されるセキュリティと相まって、最高の SSO の可能性を秘めています。

最適な使いやすさのために、証明書とドメイン認証を Citrix PIN および Active Directory パスワードキャッシュと組み合わせることができます。その結果、ユーザーは LDAP ユーザー名とパスワードを繰り返し入力する必要がなくなります。ユーザーは、登録、パスワードの有効期限切れ、およびアカウントロックアウトのためにユーザー名とパスワードを入力します。

重要:

Citrix Endpoint Management は、ユーザーがデバイスを Citrix Endpoint Management に登録した後で、認証モードをドメイン認証から他の認証モードに変更することをサポートしていません。

LDAP を許可せず、スマートカードまたは類似の方法を使用する場合、証明書を構成することで、スマートカードを Citrix Endpoint Management に提示できます。その後、ユーザーは Citrix Endpoint Management が生成する一意の PIN を使用して登録します。ユーザーがアクセス権を取得すると、Citrix Endpoint Management は、Citrix Endpoint Management 環境への認証に使用される証明書を作成して展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway の証明書のみの認証または証明書とドメイン認証を使用する場合、NetScaler for XenMobile ウィザードを使用して Citrix Endpoint Management に必要な構成を行うことができます。NetScaler for XenMobile ウィザードは一度だけ実行できます。

セキュリティの高い環境では、組織外のパブリックネットワークや安全でないネットワークでの LDAP 資格情報の使用は、組織にとって主要なセキュリティ上の脅威と見なされます。セキュリティの高い環境では、クライアント証明書とセキュリティトークンを使用する二要素認証がオプションです。詳細については、「証明書とセキュリティトークン認証のための Citrix Endpoint Management の構成」を参照してください。

クライアント証明書認証は、MAM および MDM+MAM に登録されているデバイスで利用できます。これらのデバイスでクライアント証明書認証を使用するには、Microsoft サーバー、Citrix Endpoint Management、および NetScaler Gateway を構成する必要があります。この記事で説明されている一般的な手順に従ってください。

Microsoft サーバーで:

1. Microsoft Management Console に証明書スナップインを追加します。
2. テンプレートを証明機関 (CA) に追加します。
3. CA サーバーから PFX 証明書を作成します。

シトリックス エンドポイント マネジメントでは:

1. 証明書を Citrix Endpoint Management にアップロードします。
2. 証明書ベースの認証用のPKIエンティティを作成します。
3. 資格情報プロバイダーを構成します。
4. 認証用のユーザー証明書を配信するようにNetScaler Gatewayを構成します。

NetScaler Gatewayの構成については、Citrix ADCドキュメントの以下の記事を参照してください。

- クライアント認証
- SSLプロファイルインフラストラクチャ
- クライアント証明書認証ポリシーの構成とバインド。

前提条件

- Microsoft Certificate Servicesエンティティテンプレートを作成する際は、特殊文字を除外して、登録済みデバイスでの認証の問題を回避してください。たとえば、テンプレート名に次の文字を使用しないでください: `: ! $ () # % + * ~ ? | {} []`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Exchange ActiveSyncの証明書ベースの認証を構成するには、Exchange Serverに関するMicrosoftドキュメントを参照してください。Exchange ActiveSyncの証明書機関 (CA) サーバーサイトを構成して、クライアント証明書を要求するようにします。
- プライベートサーバー証明書を使用してActiveSyncトラフィックをExchange Serverに保護する場合、モバイルデバイスがすべてのルート/中間証明書を持っていることを確認してください。そうしないと、Citrix Secure Mailでのメールボックス設定中に証明書ベースの認証が失敗します。Exchange IISコンソールでは、次の操作を行う必要があります。
  - Exchangeで使用するCitrix Endpoint Management用のWebサイトを追加し、Webサーバー証明書をバインドします。
  - ポート9443を使用します。
  - そのWebサイトには、「Microsoft-Server-ActiveSync」用と「EWS」用の2つのアプリケーションを追加する必要があります。これらの両方のアプリケーションで、**SSL Settings**の下にある**Require SSL**を選択します。

Microsoft Management Consoleに証明書スナップインを追加する

1. コンソールを開き、次に**スナップインの追加と削除**をクリックします。
2. 次のスナップインを追加します:
   - 証明書テンプレート
   - 証明書 (ローカルコンピューター)
   - 証明書 - 現在のユーザー
   - 証明機関 (ローカル)

   Microsoft 管理コンソール(/en-us/citrix-endpoint-management/media/add-certificate-snap-in-1.png)
3. **証明書テンプレート**を展開します。

   Microsoft 管理コンソール(/en-us/citrix-endpoint-management/media/add-certificate-snap-in-2.png)
4. **ユーザー**テンプレートを選択し、**テンプレートの複製**を選択します。

   Microsoft 管理コンソール(/en-us/citrix-endpoint-management/media/add-certificate-snap-in-3.png)
5. テンプレートの表示名を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

Active Directory に証明書を発行するオプションを選択することはお勧めしません。このオプションを選択すると、Active Directory のすべてのユーザーのクライアント証明書が作成され、Active Directory データベースが煩雑になる可能性があります。

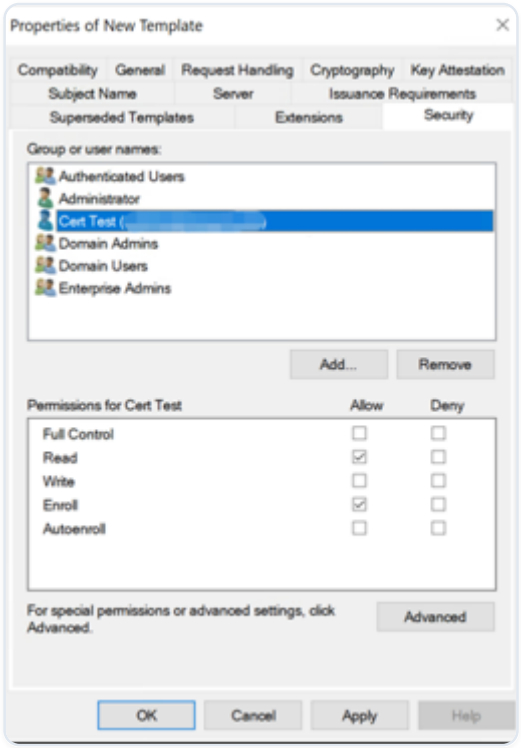
6. テンプレートの種類として**Windows 2003 Server**を選択します。Windows 2012 R2 サーバーでは、**互換性**の下で**証明機関**を選択し、受信者を**Windows 2003**に設定します。
7. 「**セキュリティ**」の下で、以下を構成します。

   a. 「**追加**」をクリックし、Citrix Endpoint Management が証明書の生成に使用する AD ユーザーアカウントを選択します。

   重要:

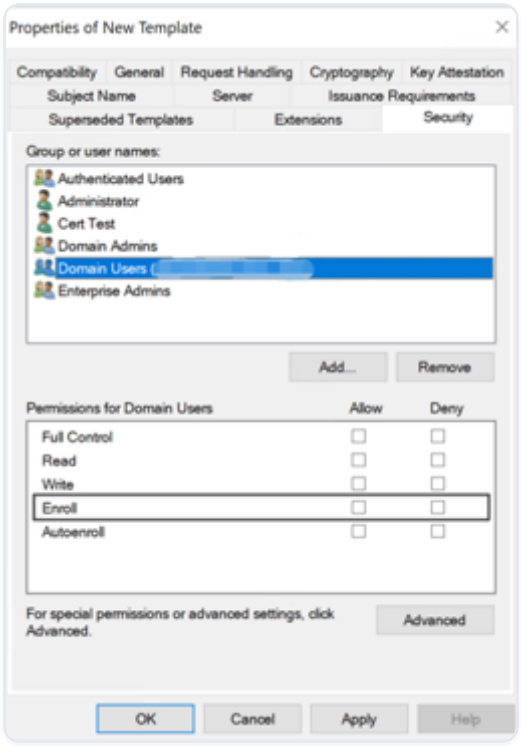
   ここにはサービスアカウントユーザーのみを追加してください。**登録**権限は、この AD ユーザーアカウントにのみ追加してください。

   この記事で後述するように、サービスアカウントを使用してユーザー .pfx 証明書を作成します。詳細については、「CA サーバーから PFX 証明書を作成する」を参照してください。

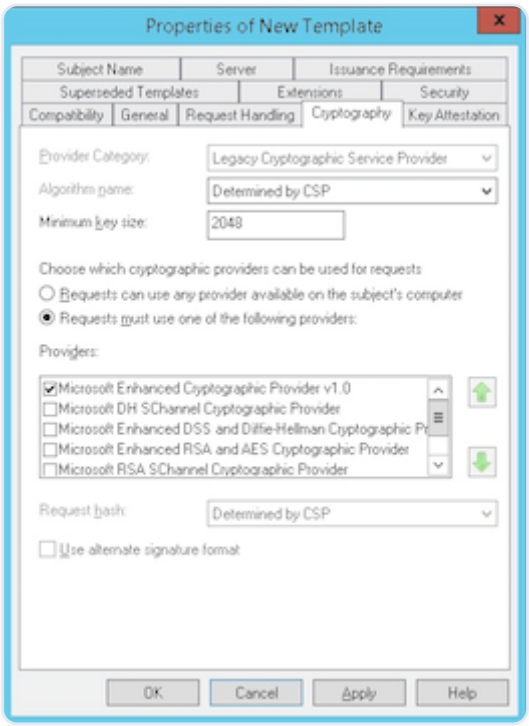


   b. **ドメインユーザー**から**登録**権限を取り消します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

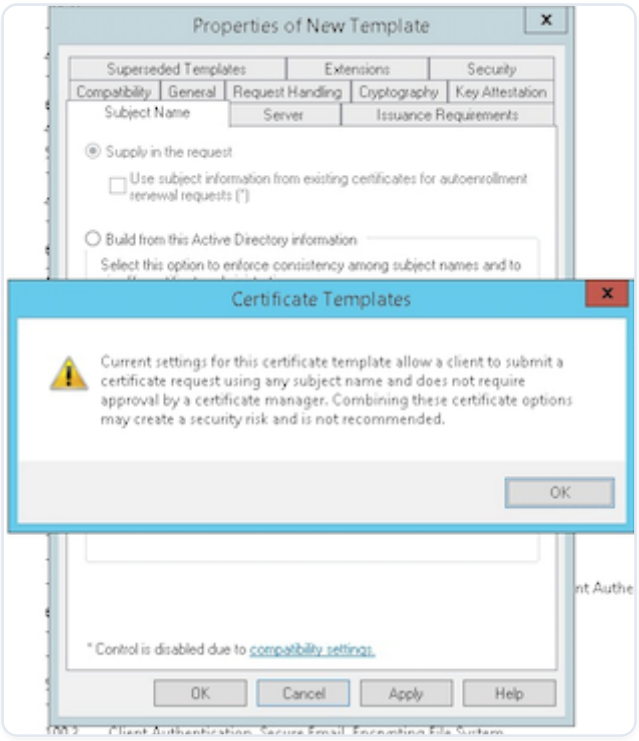


8. 「**暗号化**」の下で、キーサイズが指定されていることを確認してください。キーサイズは、Citrix Endpoint Management の構成時に後で入力します。



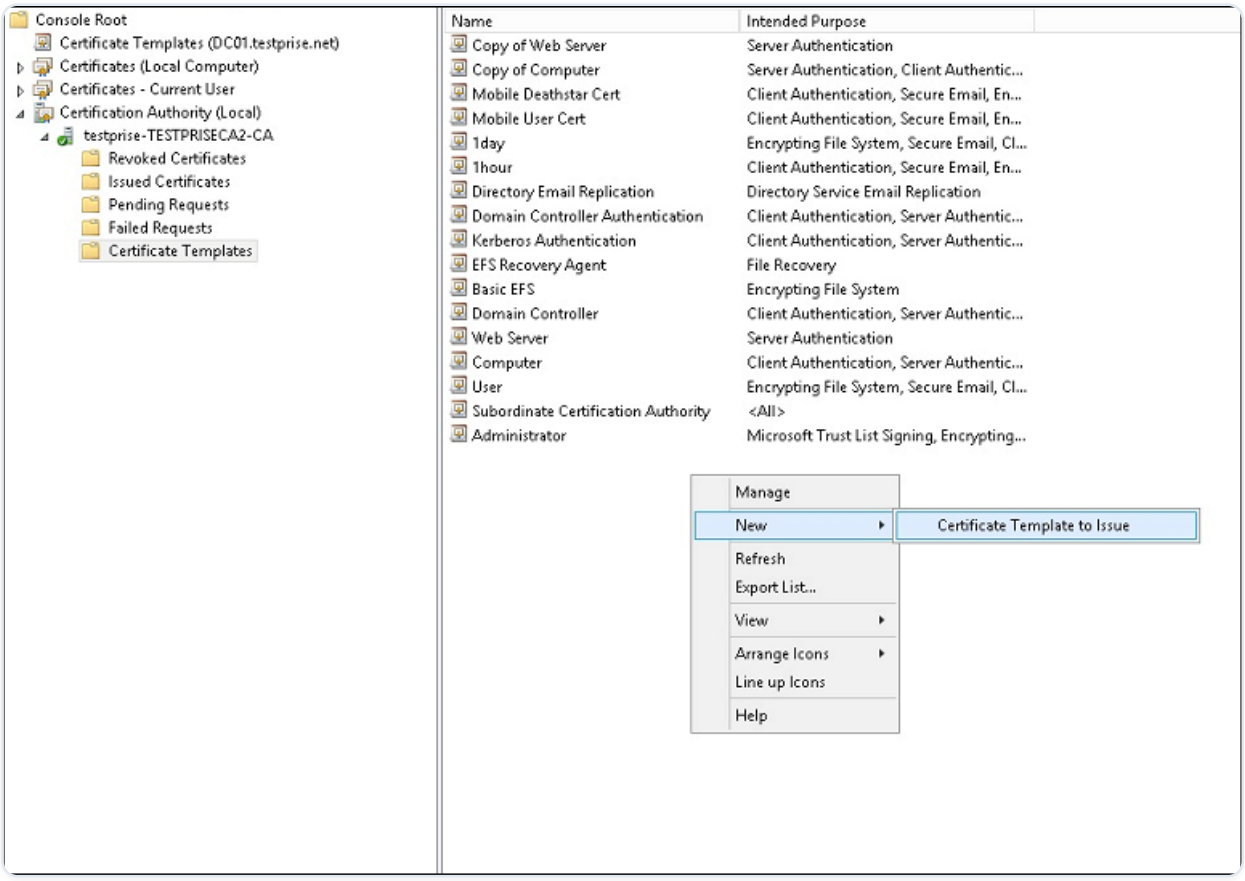
9. 「**サブジェクト名**」の下で、「**要求で指定**」を選択します。変更を適用して保存します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



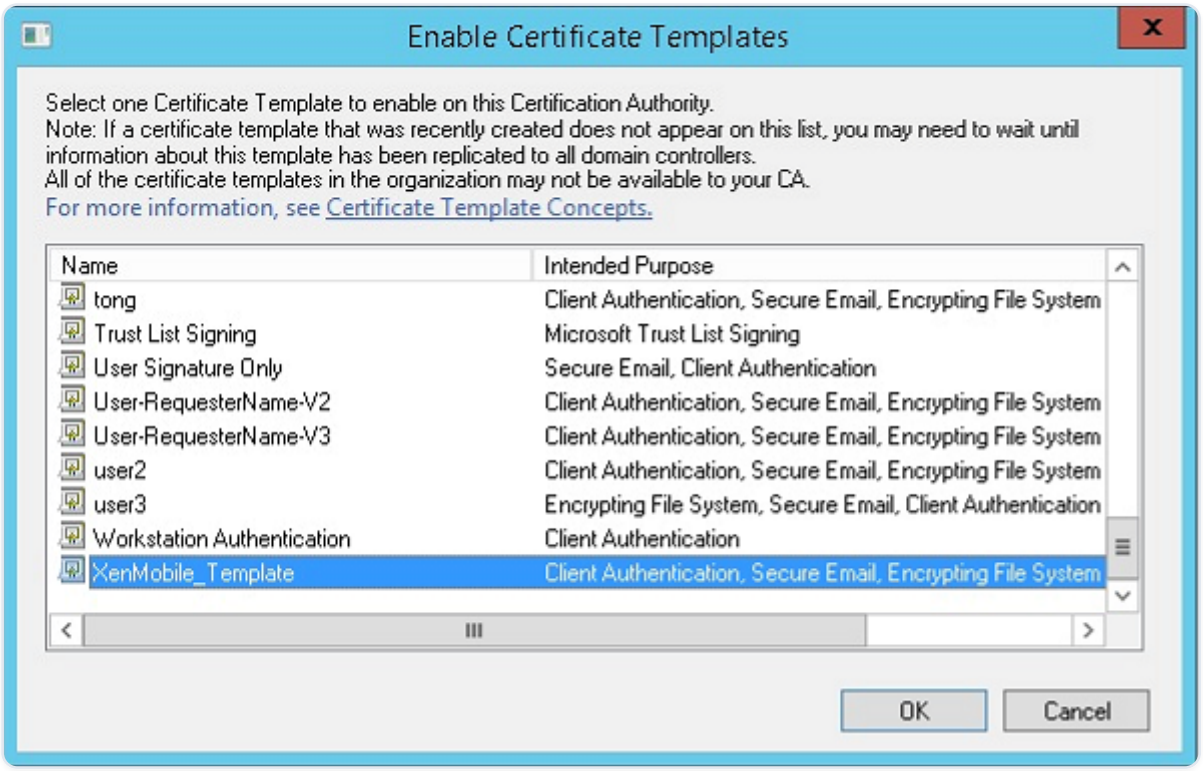
テンプレートを証明機関に追加する

1. 「**証明機関**」に移動し、「**証明書テンプレート**」を選択します。
2. 右ペインを右クリックし、「**新規 > 発行する証明書テンプレート**」を選択します。



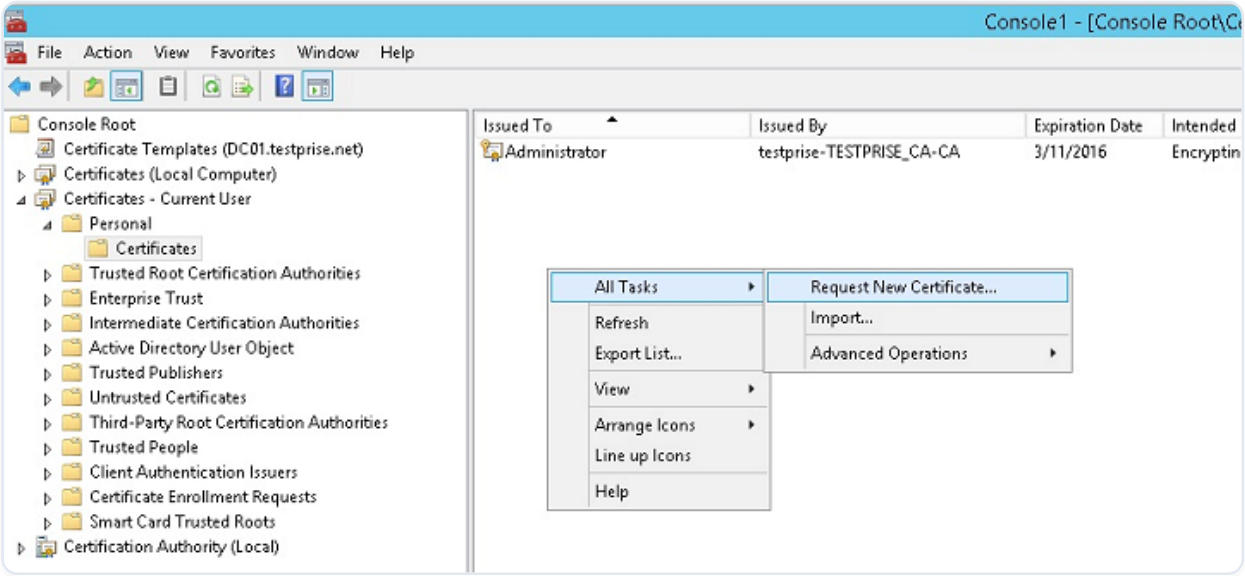
3. 前の手順で作成したテンプレートを選択し、**OK** をクリックして**証明機関**に追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



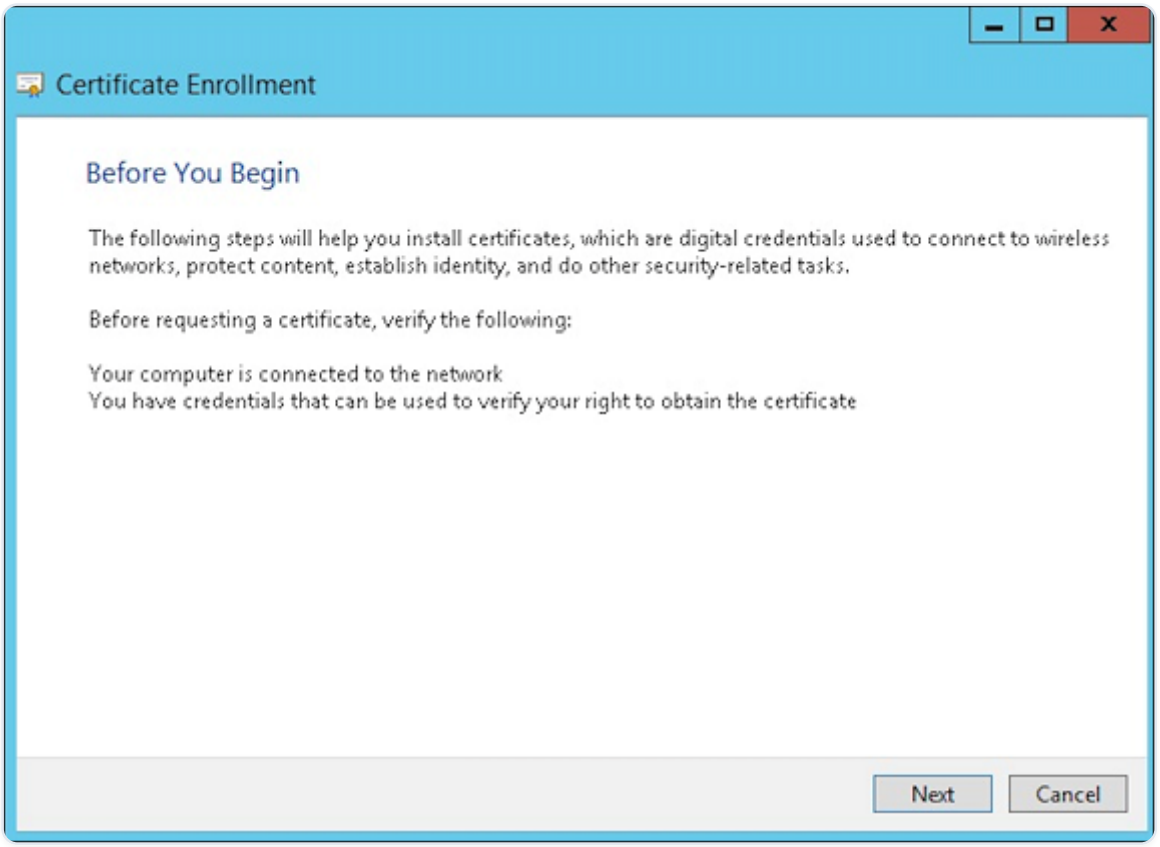
CAサーバーからPFX証明書を作成する

1. ログインしたサービスアカウントを使用して、ユーザーの.pfx証明書を作成します。この.pfxはCitrix Endpoint Managementにアップロードされ、デバイスを登録するユーザーのユーザー証明書を要求します。
2. **現在のユーザー**の下で、**証明書**を展開します。
3. 右側のペインを右クリックし、**新しい証明書を要求**をクリックします。

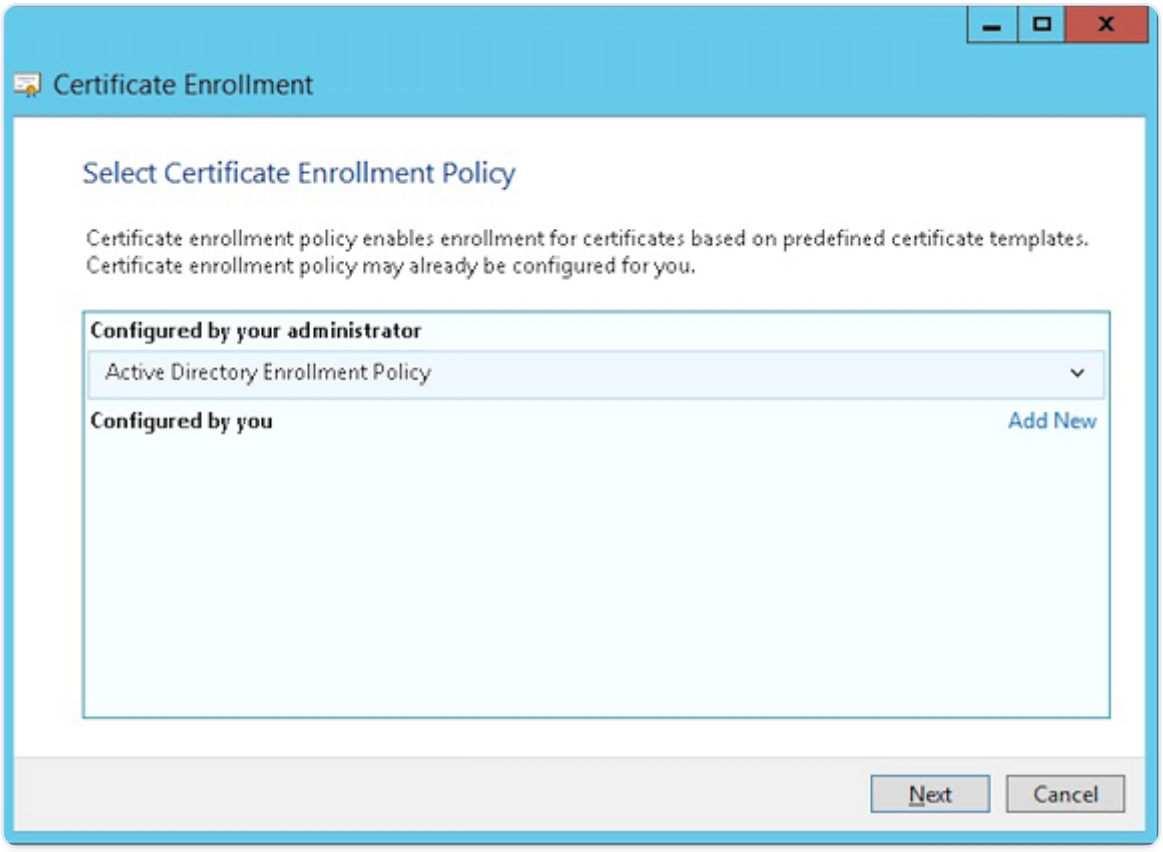


4. **証明書の登録**画面が表示されます。**次へ**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

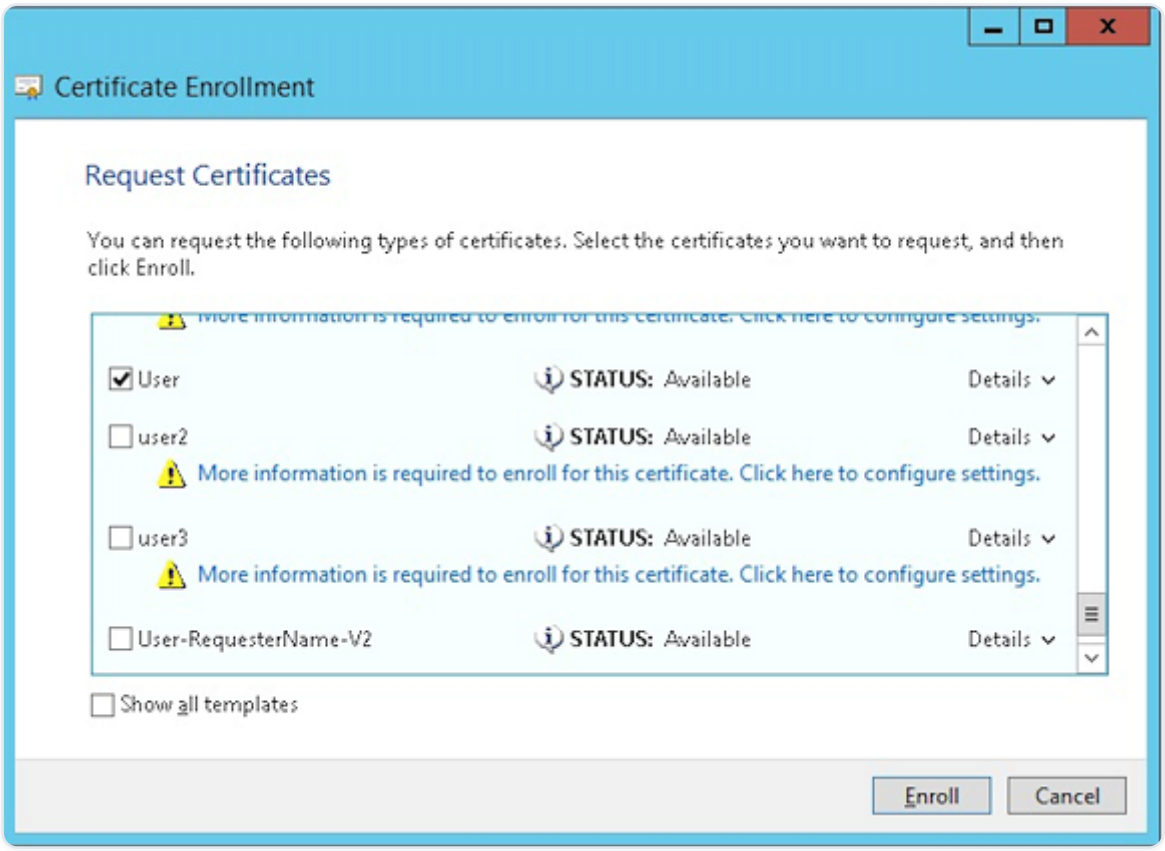


5. **Active Directory登録ポリシー**を選択し、**次へ**をクリックします。

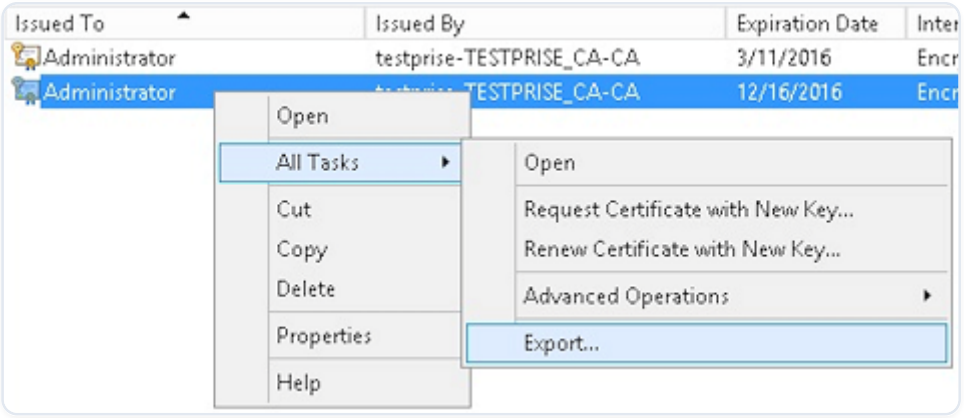


6. **ユーザー**テンプレートを選択し、**登録**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

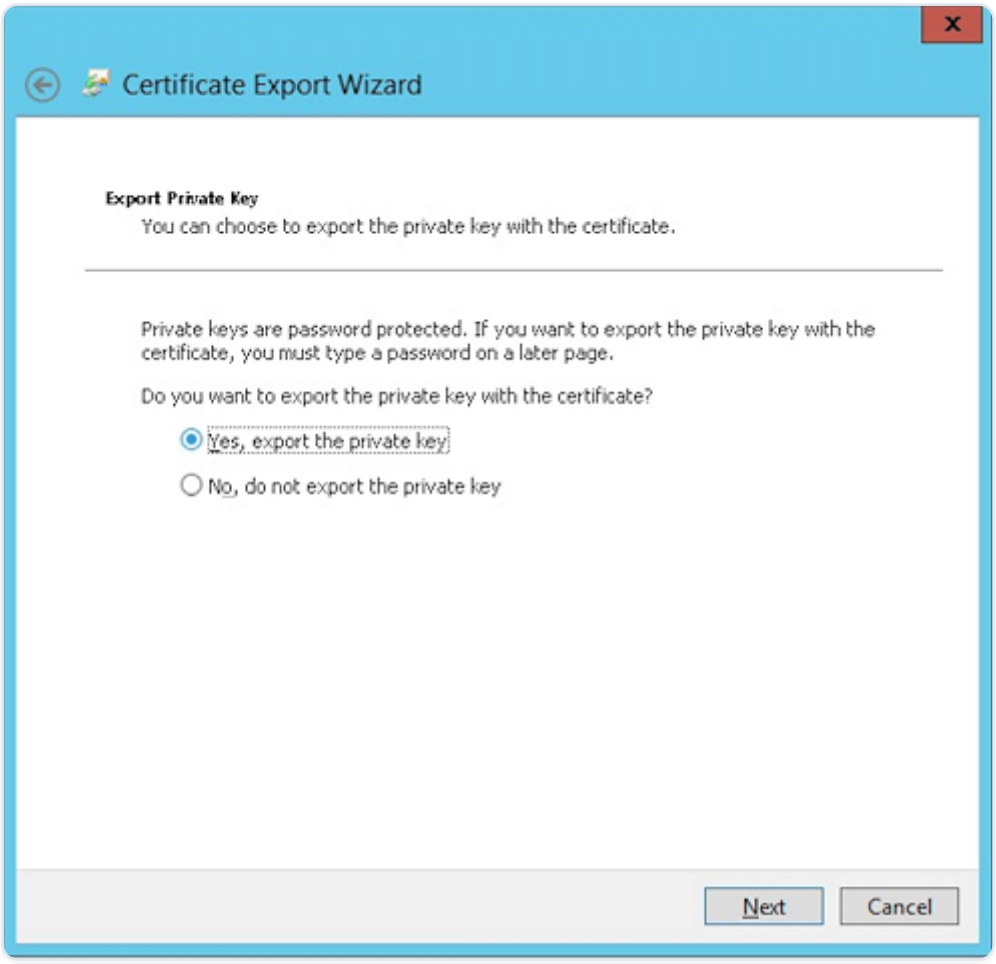


7. 前の手順で作成した.pfxファイルをエクスポートします。



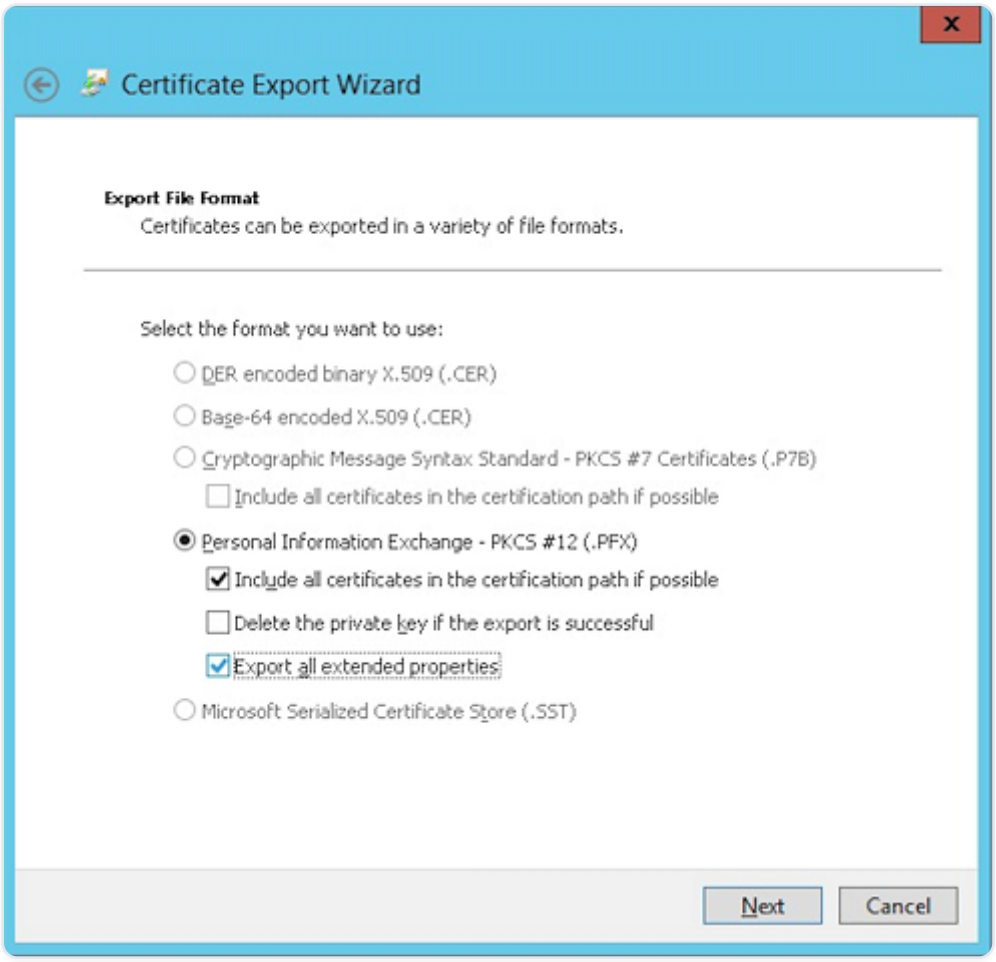
8. 「**はい、秘密キーをエクスポートします**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



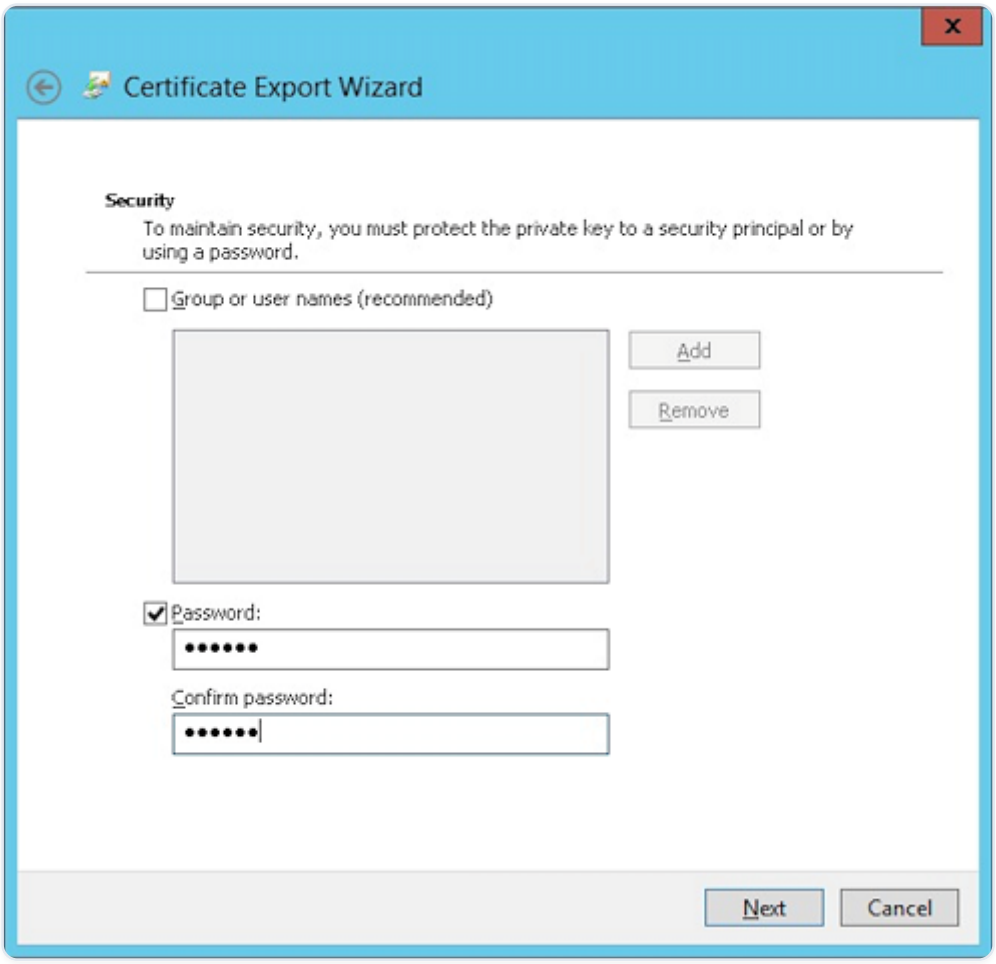
9. 「**可能であれば、証明書パス内のすべての証明書を含める**」を選択し、「**すべての拡張プロパティをエクスポートする**」チェックボックスをオンにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. この証明書をCitrix Endpoint Managementにアップロードするときに使用するパスワードを設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



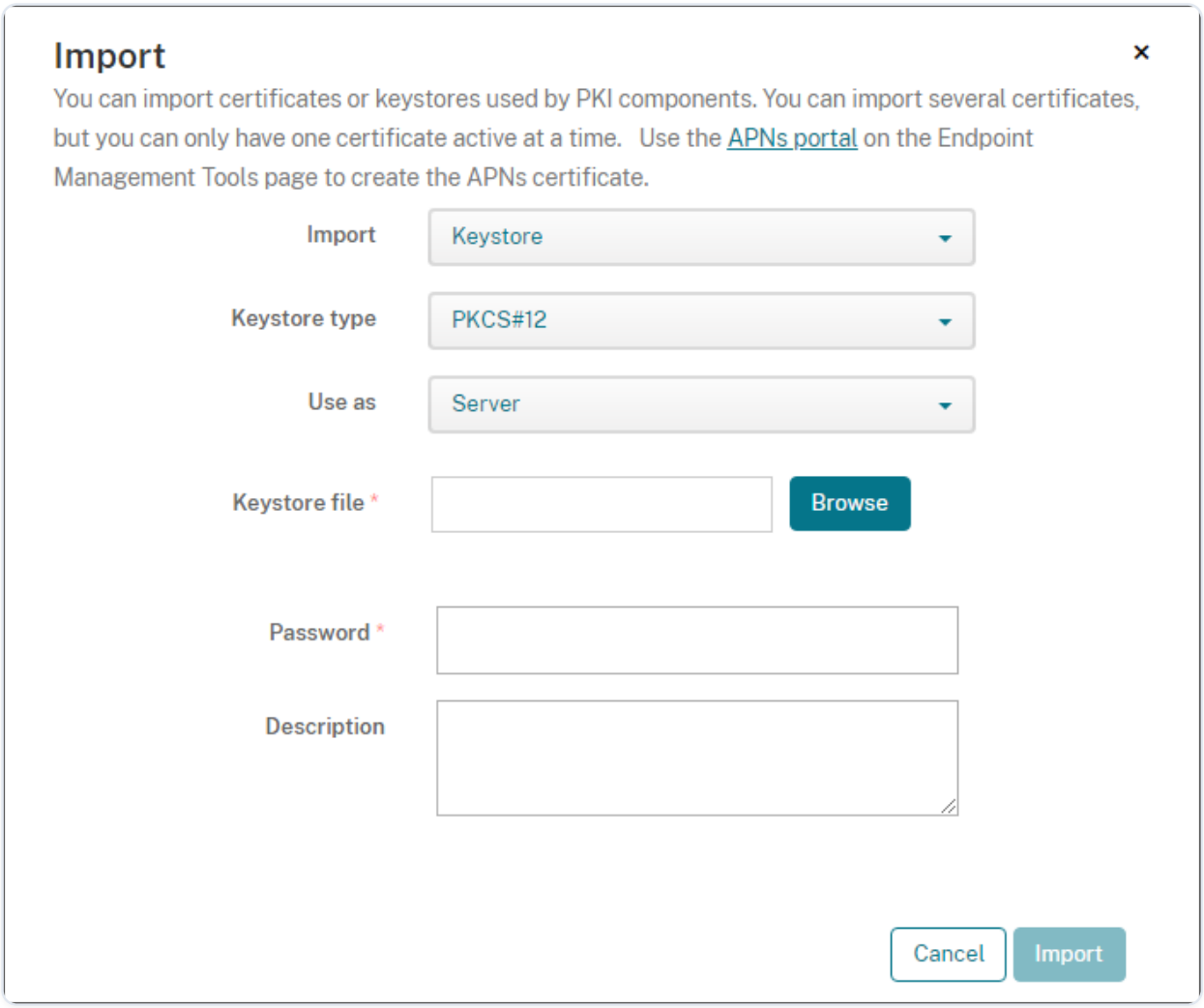
11. 証明書をハードドライブに保存します。

Citrix Endpoint Managementへの証明書のアップロード

1. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。**設定**画面が表示されます。
2. **証明書**をクリックし、次に**インポート**をクリックします。
3. 次のパラメータを入力します。

    - **インポート:** キーストア
    - **キーストアの種類:** PKCS #12
    - **用途:** サーバー
    - **キーストアファイル:** 参照をクリックして、作成した.pfx証明書を選択します。
    - **パスワード:** この証明書用に作成したパスワードを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. **インポート**をクリックします。
5. 証明書が正しくインストールされていることを確認します。正しくインストールされた証明書は、ユーザー証明書として表示されます。

証明書ベースの認証用のPKIエンティティの作成

1. **設定**で、**その他 > 証明書管理 > PKIエンティティ**に移動します。
2. **追加**をクリックし、次に**Microsoft Certificate Servicesエンティティ**をクリックします。**Microsoft Certificate Servicesエンティティ: 一般情報**画面が表示されます。
3. 次のパラメーターを入力します。

   - **名前:** 任意の名前を入力します。
   - **Web登録サービスルートURL:** `https://RootCA-URL/certsrv/` (URLパスの最後のスラッシュ「/」を必ず追加してください。)
   - **certnew.cerページ名:** certnew.cer (デフォルト値)
   - **certfnsh.asp:** certfnsh.asp (デフォルト値)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **認証の種類:** クライアント証明書
- **SSLクライアント証明書:** Citrix Endpoint Managementクライアント証明書の発行に使用するユーザー証明書を選択します。証明書が存在しない場合は、前のセクションの手順に従って証明書をアップロードしてください。

「証明書構成画面」(/en-us/citrix-endpoint-management/media/add-pki-entity-1.png)

4. **テンプレート**で、Microsoft証明書を構成したときに作成したテンプレートを追加します。スペースを追加しないでください。

「証明書構成画面」(/en-us/citrix-endpoint-management/media/add-pki-entity-2.png)

5. HTTPパラメーターをスキップし、**CA証明書**をクリックします。
6. 環境に対応するルートCA名を選択します。このルートCAは、Citrix Endpoint Managementクライアント証明書からインポートされたチェーンの一部です。

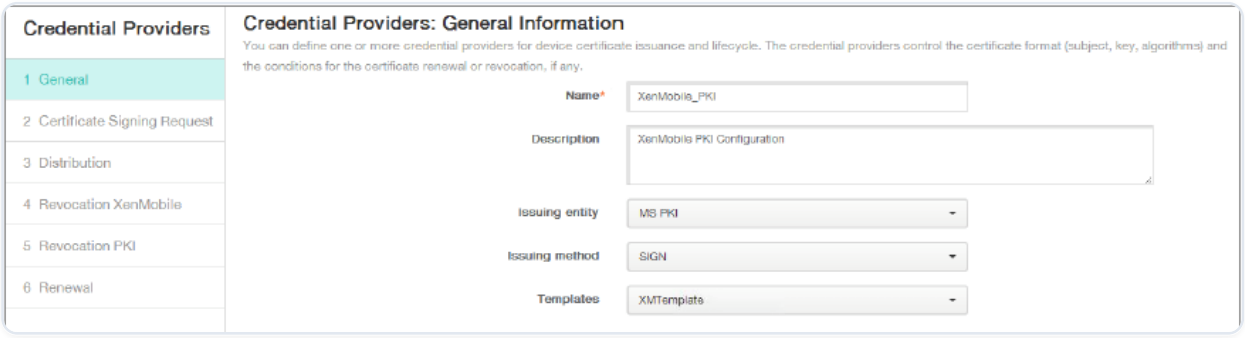
「証明書構成画面」(/en-us/citrix-endpoint-management/media/add-pki-entity-3.png)

7. **保存**をクリックします。

資格情報プロバイダーの構成

1. **設定**で、**その他 > 証明書管理 > 資格情報プロバイダー**に移動します。
2. **追加**をクリックします。
3. **一般**で、次のパラメーターを入力します。

- **名前:** 任意の名前を入力します。
- **説明:** 任意の記述を入力します。
- **発行エンティティ:** 以前に作成したPKIエンティティを選択します。
- **発行方法:** SIGN
- **テンプレート:** PKIエンティティの下に追加されたテンプレートを選択します。



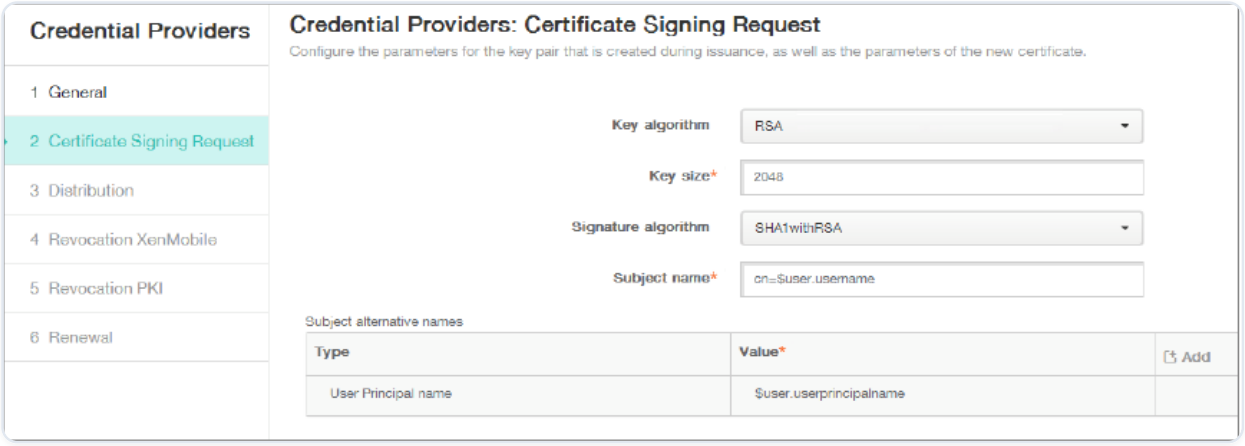
4. **証明書署名要求**をクリックし、次のパラメーターを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **キーアルゴリズム:** RSA
- **キーサイズ:** 2048
- **署名アルゴリズム:** SHA256withRSA
- **サブジェクト名:** `cn=$user.username`

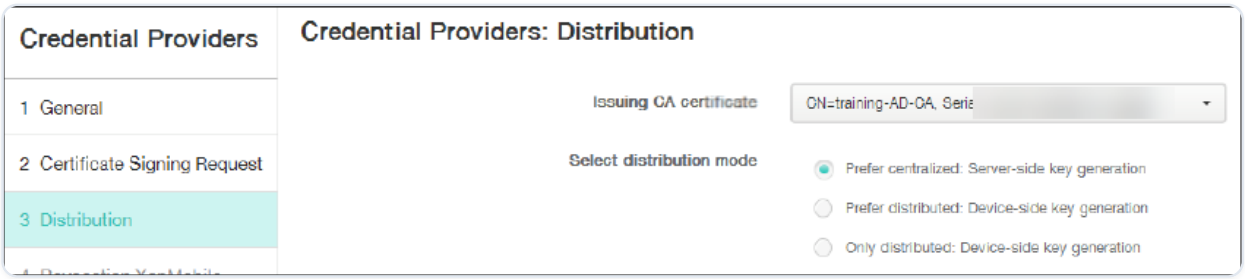
サブジェクトの別名については、**追加**をクリックし、次のパラメーターを入力します。

- **タイプ:** ユーザープリンシパル名
- **値:** `$user.userprincipalname`



5. **配布**をクリックし、次のパラメーターを入力します。

   - **発行CA証明書:** Citrix Endpoint Managementクライアント証明書に署名した発行CAを選択します。
   - **配布モードの選択: 集中型を優先: サーバー側キー生成**を選択します。



6. 次の2つのセクション、「**Revocation Citrix Endpoint Management**」と「**Revocation PKI**」について、必要に応じてパラメーターを設定します。この例では、両方のオプションがスキップされます。
7. 「**Renewal**」をクリックします。
8. 「**Renew certificates when they expire**」を有効にします。
9. 他のすべての設定はデフォルトのままにするか、必要に応じて変更します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

資格情報プロバイダーの構成画面(/en-us/citrix-endpoint-management/media/configure-credential-providers-4.png)

10. 「**Save**」をクリックします。

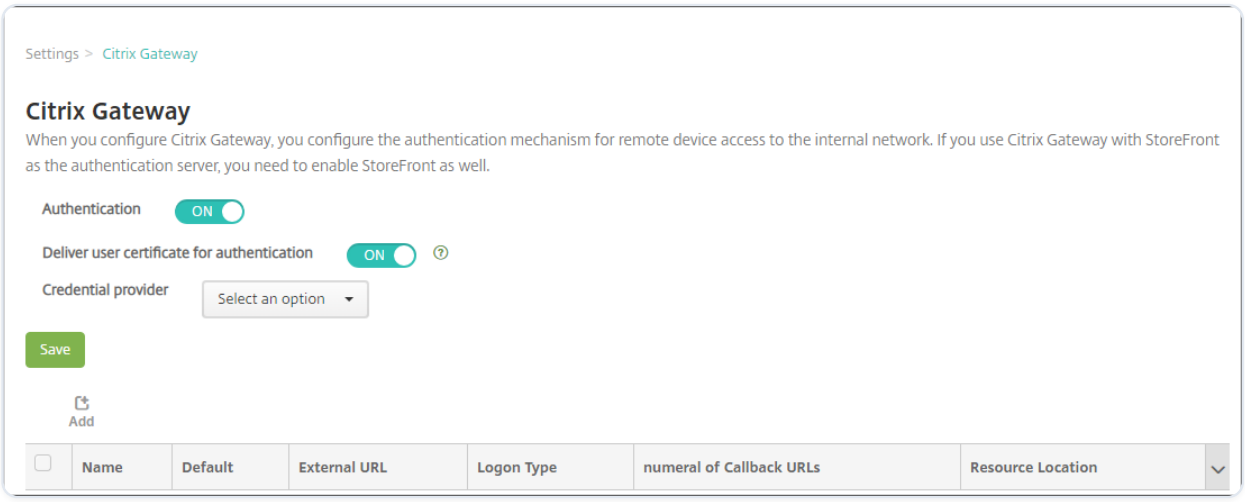
証明書ベースの認証を使用するようにCitrix Secure Mailを構成する

Citrix Secure MailをCitrix Endpoint Managementに追加するときは、「**App Settings**」の下にあるExchange設定を必ず構成してください。

アプリ構成画面(/en-us/citrix-endpoint-management/media/configure-worxmail-certificate-authentication.png)

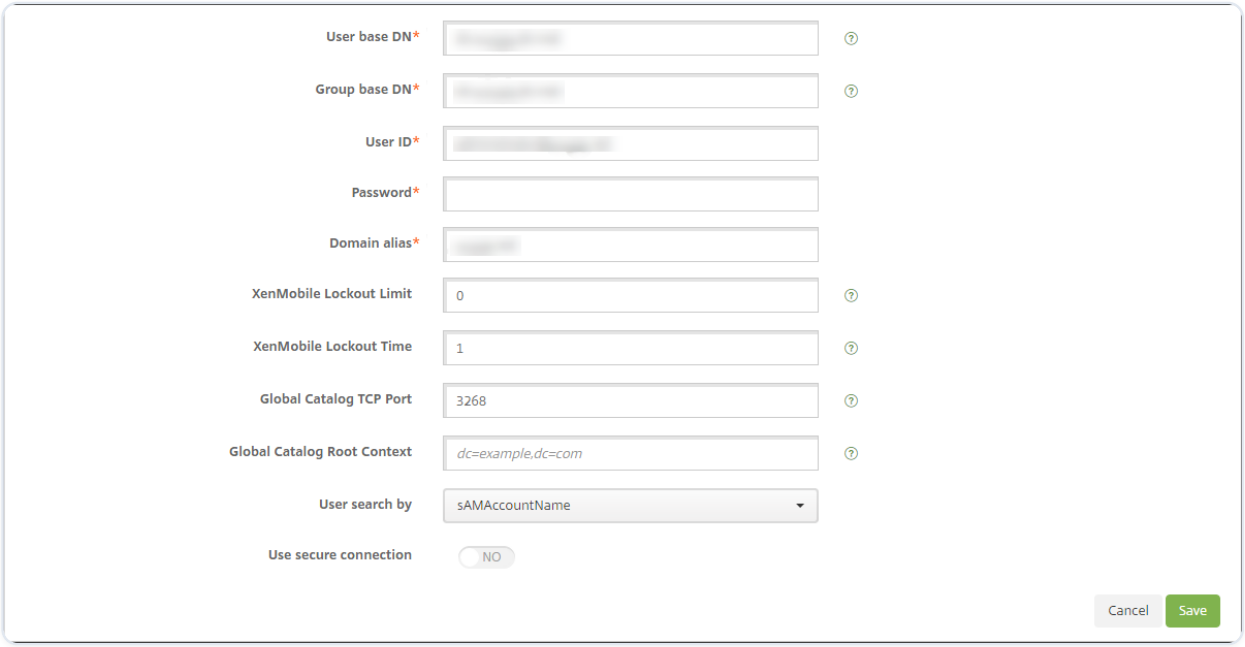
Citrix Endpoint ManagementでのNetScaler Gateway証明書配信の構成

1. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。「**Settings**」画面が表示されます。
2. 「**Server**」の下で、「**NetScaler Gateway**」をクリックします。
3. NetScaler Gatewayがまだ追加されていない場合は、「**Add**」をクリックして設定を指定します。
   - **名前:** アプライアンスのわかりやすい名前。
   - **エイリアス:** アプライアンスのオプションのエイリアス。
   - **外部URL:** `https://YourCitrixGatewayURL`
   - **ログオンの種類: 証明書とドメイン**を選択します
   - **パスワードが必要:** オフ
   - **デフォルトとして設定:** オン
4. **認証**と**認証用のユーザー証明書を配信**については、**オン**を選択します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. **資格情報プロバイダー**については、プロバイダーを選択し、**保存**をクリックします。
6. ユーザー証明書のsAMAccount属性をユーザープリンシパル名 (UPN) の代替として使用するには、Citrix Endpoint ManagementでLDAPコネクタを次のように構成します: **設定 > LDAP**に移動し、ディレクトリを選択して**編集**をクリックし、**ユーザー検索条件**で**sAMAccountName**を選択します。



Citrix PINとユーザーパスワードのキャッシュを有効にする

Citrix PINとユーザーパスワードのキャッシュを有効にするには、**設定 > クライアントプロパティ**に移動し、**Citrix PIN認証を有効にする**と**ユーザーパスワードのキャッシュを有効にする**のチェックボックスをオンにします。詳しくは、「クライアントプロパティ」を参照してください。

クライアント証明書構成のトラブルシューティング

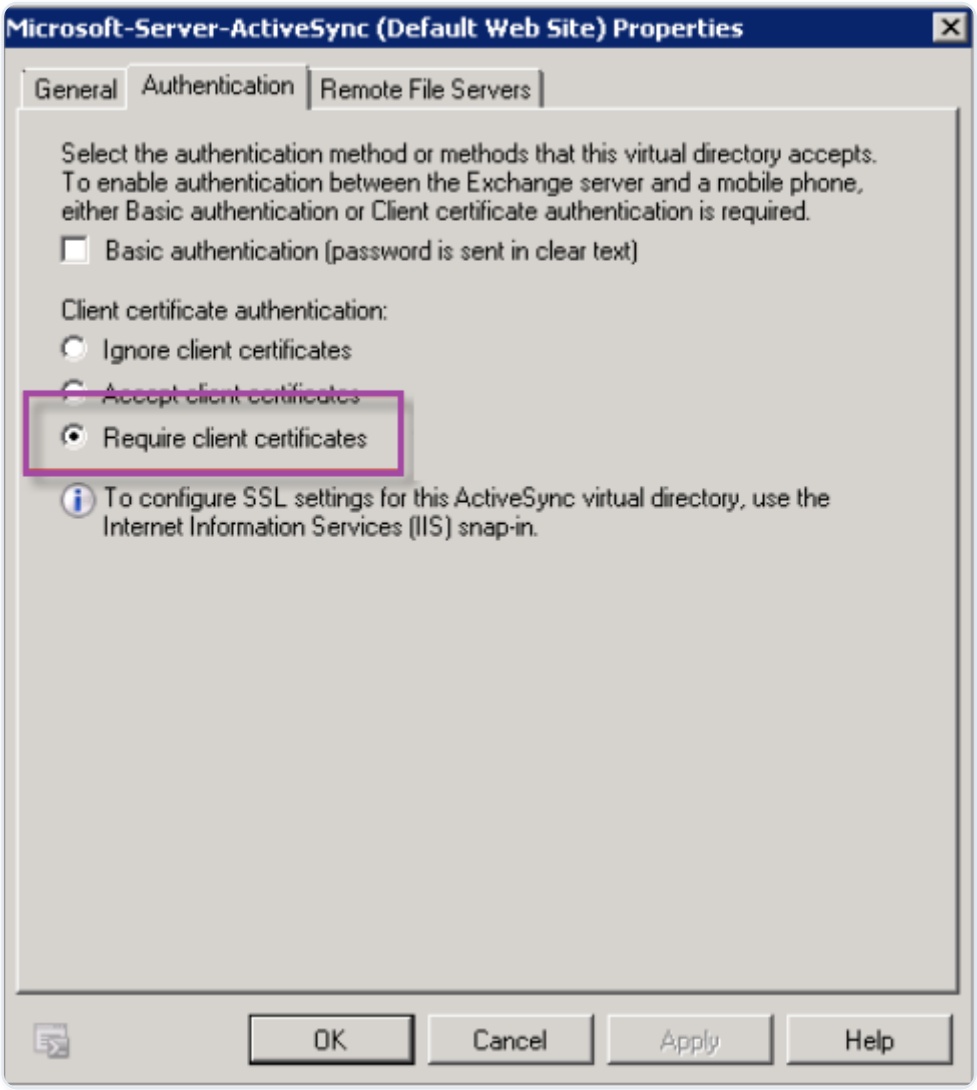
前述の構成とNetScaler Gatewayの構成が正常に完了すると、ユーザーワークフローは次のようになります。

1. ユーザーはモバイルデバイスを登録します。
2. Citrix Endpoint Managementは、Citrix PINを作成するようにユーザーに促します。
3. ユーザーはその後、アプリストアにリダイレクトされます。
4. ユーザーがCitrix Secure Mailを起動すると、Citrix Endpoint Managementはメールボックス構成のためのユーザー資格情報を要求しません。代わりに、Citrix Secure MailはCitrix Secure Hubからクライアント証明書を要求し、認証のためにMicrosoft Exchange Serverに送信します。ユーザーがCitrix Secure Mailを起動したときにCitrix Endpoint Managementが資格情報を要求する場合は、構成を確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

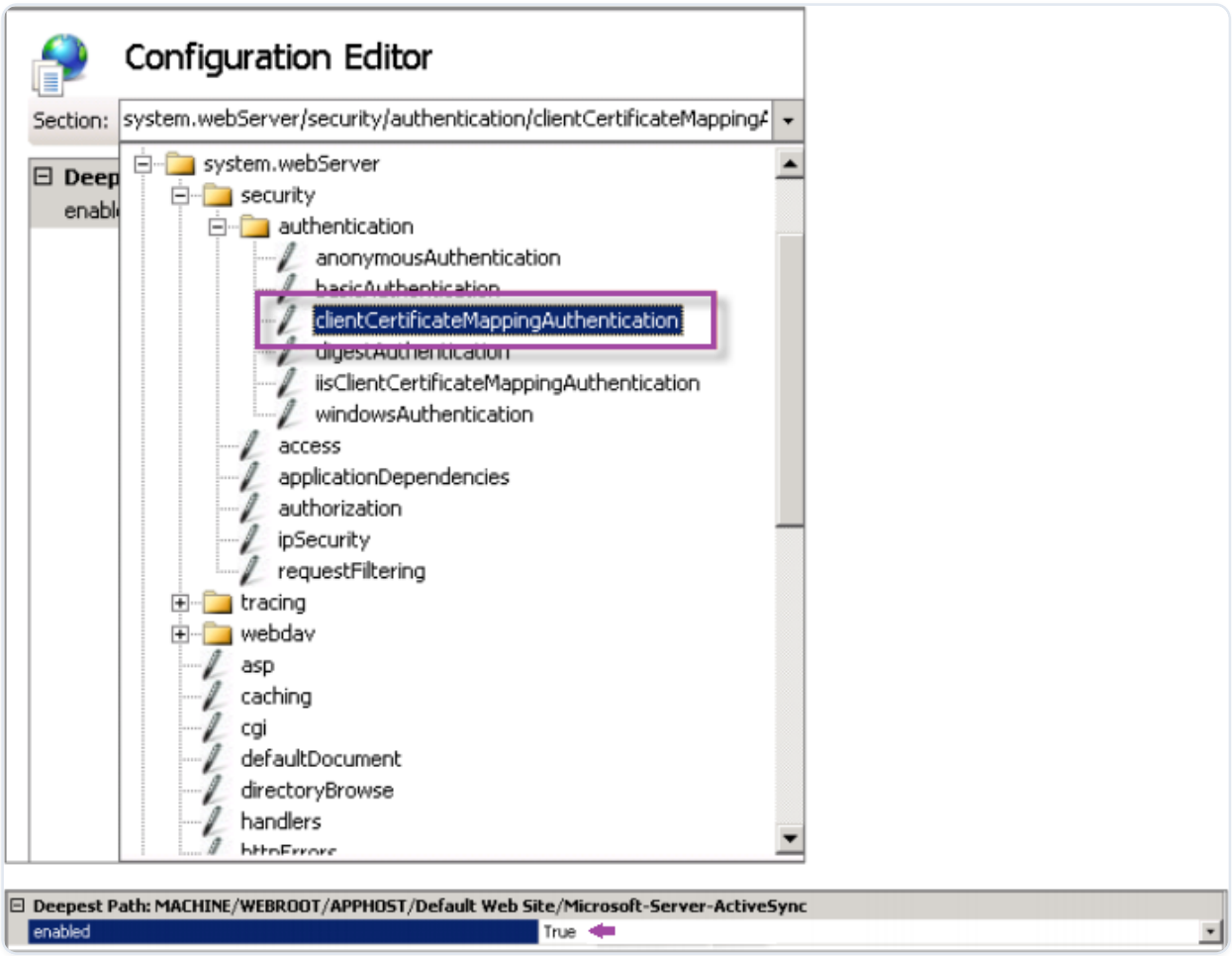
ユーザーがCitrix Secure Mailをダウンロードしてインストールできるが、メールボックス構成中にCitrix Secure Mailが構成を完了できない場合:

1. Microsoft Exchange Server ActiveSync がプライベート SSL サーバー証明書を使用してトラフィックを保護している場合、ルート/中間証明書がモバイルデバイスにインストールされていることを確認してください。
2. ActiveSync用に選択された認証タイプが**クライアント証明書を要求**に設定されていることを確認してください。



3. Microsoft Exchange Serverで、**Microsoft-Server-ActiveSync**サイトを確認し、クライアント証明書マッピング認証が有効になっていることを確認します。デフォルトでは、クライアント証明書マッピング認証は無効になっています。このオプションは、**構成エディター > セキュリティ > 認証**の下にあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Trueを選択した後、変更を適用するために**適用**をクリックしてください。

4. Citrix Endpoint ManagementコンソールでNetScaler Gatewayの設定を確認します。**認証用のユーザー証明書を配信**が**オン**になっており、**資格情報プロバイダー**に正しいプロファイルが選択されていることを確認してください。

クライアント証明書がモバイルデバイスに配信されたかどうかを確認するには

1. Citrix Endpoint Managementコンソールで、**管理 > デバイス**に移動し、デバイスを選択します。
2. **編集**または**詳細を表示**をクリックします。
3. **配信グループ**セクションに移動し、次のエントリを検索します。

   NetScaler Gateway資格情報: 要求された資格情報、CertId=

クライアント証明書ネゴシエーションが有効になっているかどうかを検証するには

1. IIS Webサイトにバインドされ ているSSL証明書構成を表示するには、次の`netsh`コマンドを実行します。

   ```
   netsh http show sslcert
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Negotiate Client Certificate** の値が **Disabled** の場合、次のコマンドを実行して有効にします。

   `netsh http delete sslcert ipport=0.0.0.0:443`

   `netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={app_id} certstorename=store_name verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable`

   例：

   `netsh http add sslcert ipport=0.0.0.0:443 certhash=23498dfsdfhaf98rhkjqf9823rkjhdasf98asfk appid={123asd456jd-a12b-3c45-d678-123456lkjhgf} certstorename=ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable`

Citrix Endpoint Managementを介してルート/中間証明書をWindows Phone 8.1デバイスに配信できない場合：

- ルート/中間証明書（.cer）ファイルを電子メールでWindows Phone 8.1デバイスに送信し、直接インストールします。

Citrix Secure MailがWindows Phone 8.1に正常にインストールされない場合は、以下を確認してください。

- アプリケーション登録トークン（.AETXファイル）は、Enterprise Hubデバイスポリシーを使用してCitrix Endpoint Managementを介して配信されます。
- アプリケーション登録トークンは、Citrix Secure Mailのラップと Citrix Secure Hubアプリの署名に使用された証明書プロバイダーと同じエンタープライズ証明書を使用して作成されました。
- Citrix Secure Hub、Citrix Secure Mail、およびアプリケーション登録トークンの署名とラップには、同じ発行元IDが使用されます。

PKIエンティティ

Citrix Endpoint Managementの公開鍵インフラストラクチャ（PKI）エンティティ構成は、実際のPKI操作（発行、失効、ステータス情報）を行うコンポーネントを表します。これらのコンポーネ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ントは、Citrix Endpoint Managementの内部または外部にあります。内部コンポーネントは裁量的（discretionary）と呼ばれます。外部コンポーネントは、お客様の企業インフラストラクチャの一部です。

Citrix Endpoint Managementは、以下の種類のPKIエンティティをサポートしています。

- マイクロソフト証明書サービス
- 裁量的認証局（CA）

Citrix Endpoint Managementは、以下のCAサーバーをサポートしています。

- Windows サーバー 2016
- Windows サーバー 2019
- ウィンドウズ サーバー 2022

注：

Windows Server 2012 R2、2012、および2008 R2は、サポート終了（EOL）を迎えたため、サポートされなくなりました。詳細については、Microsoft製品のライフサイクルに関するドキュメントを参照してください。

一般的なPKIの概念

種類にかかわらず、すべてのPKIエンティティは以下の機能の一部を備えています。

- **署名（Sign）：** 証明書署名要求（CSR）に基づいて新しい証明書を発行します。
- **取得（Fetch）：** 既存の証明書とキーペアを回復します。
- **失効:** クライアント証明書を失効させること。

CA証明書について

PKIエンティティを構成するときは、そのエンティティによって発行された（または回復された）証明書の署名者であるCA証明書をCitrix Endpoint Managementに示します。そのPKIエンティティは、任意の数の異なるCAによって署名された証明書（取得済みまたは新規署名済み）を返すことができます。

PKIエンティティ構成の一部として、これらの各認証局の証明書を提供します。そのためには、証明書をCitrix Endpoint Managementにアップロードし、PKIエンティティでそれらを参照します。裁量的なCAの場合、証明書は暗黙的に署名CA証明書となります。外部エンティティの場合、証明書を手動で指定する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

Microsoft Certificate Servicesエンティティテンプレートを作成する際は、登録済みデバイスで発生する可能性のある認証の問題を回避してください。テンプレート名に特殊文字を使用しないでください。たとえば、`! : $ ( ) # % + * ~ ? | { } [ ]`は使用しないでください。

Microsoft 証明書サービス

Citrix Endpoint Managementは、Web登録インターフェイスを介してMicrosoft Certificate Servicesと連携します。Citrix Endpoint Managementは、そのインターフェイスを介した新しい証明書の発行のみをサポートしています。Microsoft CAがNetScaler Gatewayユーザー証明書を生成する場合、NetScaler Gatewayはそれらの証明書の更新と失効をサポートします。

Citrix Endpoint ManagementでMicrosoft CA PKIエンティティを作成するには、Certificate Services Webインターフェイスのベースを指定する必要があります。必要に応じて、SSLクライアント認証を使用して、Citrix Endpoint ManagementとCertificate Services Webインターフェイス間の接続を保護します。

Microsoft Certificate Servicesエンティティを追加する

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックし、 をクリックします。
2. ページで、 をクリックします。

   PKIエンティティタイプのメニューが表示されます。
3. をクリックします。

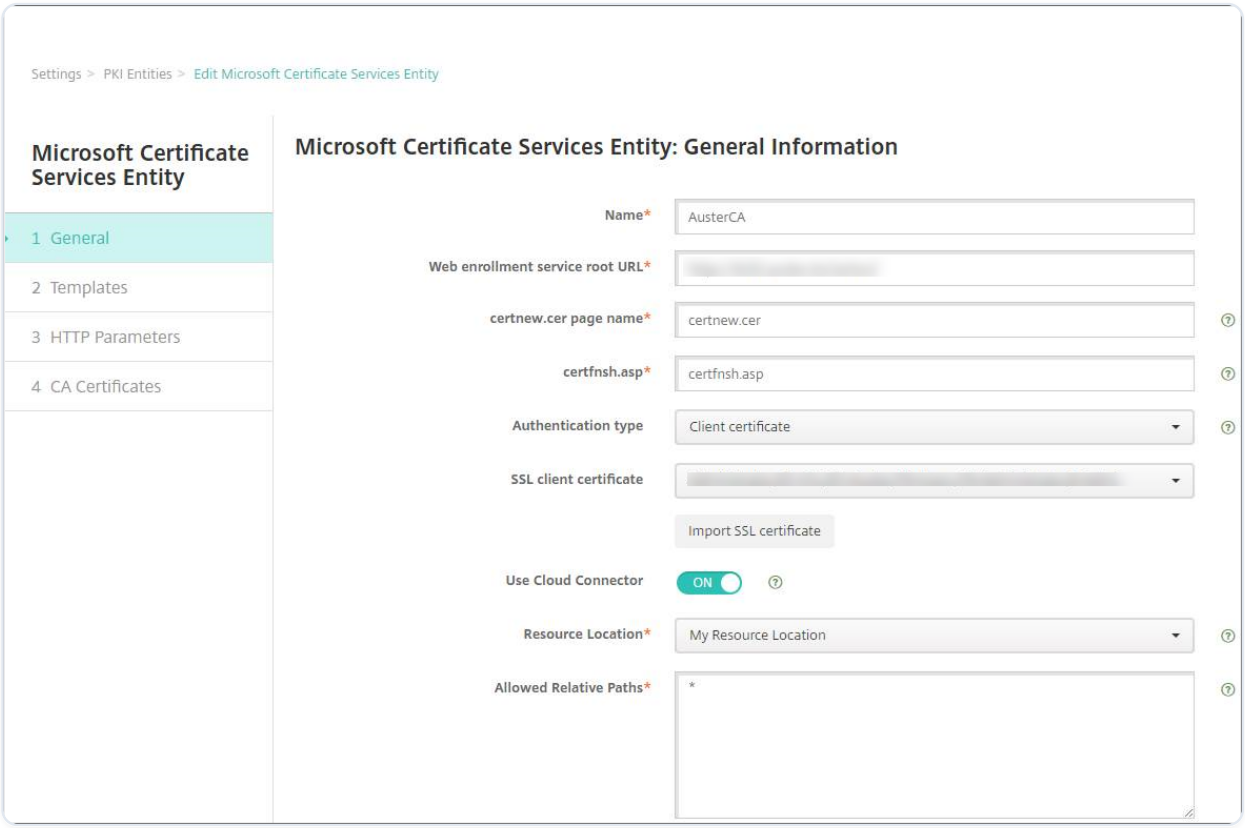
   ページが表示されます。
4. 「**Microsoft Certificate Servicesエンティティ: 一般情報**」ページで、次の設定を構成します。

   - **名前:** 新しいエンティティの名前を入力します。この名前は後でそのエンティティを参照するために使用します。エンティティ名は一意である必要があります。
   - **Web登録サービスルートURL:** Microsoft CA Web登録サービスのベースURLを入力します。例: `https://192.0.0.1/certsrv/`。URLはプレーンHTTPまたはHTTP-over-SSLを使用できます。
   - **certnew.cerページ名:** certnew.cerページの名称。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **certfnsh.asp:** certfnsh.aspページの名称。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
- **認証の種類:** 使用する認証方法を選択します。
  - **なし**
  - **HTTP Basic:** 接続に必要なユーザー名とパスワードを入力します。
  - **クライアント証明書:** 正しいSSLクライアント証明書を選択します。
- **Cloud Connectorを使用:** PKIサーバーへの接続にCloud Connectorを使用するには、**オン**を選択します。次に、接続の**リソースの場所**と**許可される相対パス**を指定します。
  - **リソースの場所:** Citrix Cloud Connectorで定義されているリソースの場所から選択します。
  - **許可される相対パス:** 指定されたリソースの場所で許可される相対パス。1行に1つのパスを指定します。アスタリスク（*）のワイルドカードを使用できます。

    リソースの場所が`https://www.ServiceRoot/certsrv`であるとします。そのパス内のすべてのURLへのアクセスを提供するには、**許可される相対パス**に`/*`を入力します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. **接続のテスト**をクリックして、サーバーにアクセスできることを確認します。アクセスできない場合は、接続に失敗したことを示すメッセージが表示されます。構成設定を確認してください。
6. 「**次へ**」をクリックします。

   「**Microsoft Certificate Servicesエンティティ: テンプレート**」ページが表示されます。このページでは、Microsoft CAがサポートするテンプレートの内部名を指定します。資格情報プロバイダーを作成する際、ここで定義されたリストからテンプレートを選択します。このエンティティを使用するすべての資格情報プロバイダーは、そのようなテンプレートを1つだけ使用します。

   Microsoft Certificate Servicesテンプレートの要件については、お使いのMicrosoft Serverのバージョンに関するMicrosoftドキュメントを参照してください。Citrix Endpoint Managementは、証明書に記載されている証明書形式以外に、配布する証明書に関する要件はありません。
7. 「**Microsoft Certificate Servicesエンティティ: テンプレート**」ページで、「**追加**」をクリックし、テンプレートの名前を入力してから「**保存**」をクリックします。追加するテンプレートごとにこの手順を繰り返します。
8. 「**次へ**」をクリックします。

   「**Microsoft Certificate Servicesエンティティ: HTTPパラメーター**」ページが表示されます。このページでは、Citrix Endpoint ManagementがMicrosoft Web登録インターフェイスへのHTTPリクエストに追加するカスタムパラメーターを指定します。カスタムパラメーターは、CAで実行されているカスタマイズされたスクリプトに対してのみ役立ちます。
9. 「**Microsoft Certificate Servicesエンティティ: HTTPパラメーター**」ページで、「**追加**」をクリックし、追加するHTTPパラメーターの名前と値を入力してから「**次へ**」をクリックします。

   「**Microsoft Certificate Servicesエンティティ: CA証明書**」ページが表示されます。このページでは、このエンティティを通じてシステムが取得する証明書の署名者をCitrix Endpoint Managementに通知する必要があります。CA証明書が更新されたら、Citrix Endpoint Managementで更新します。Citrix Endpoint Managementは、その変更をエンティティに透過的に適用します。
10. 「**Microsoft Certificate Servicesエンティティ: CA証明書**」ページで、このエンティティに使用する証明書を選択します。
11. 「**保存**」をクリックします。

    エンティティがPKIエンティティテーブルに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway証明書失効リスト（CRL）

Citrix Endpoint Managementは、サードパーティの認証局に対してのみ証明書失効リスト（CRL）をサポートします。Microsoft CAが構成されている場合、Citrix Endpoint ManagementはNetScaler Gatewayを使用して失効を管理します。

クライアント証明書ベースの認証を構成する際は、NetScaler Gatewayの証明書失効リスト（CRL）設定「**CRL自動更新を有効にする**」を構成するかどうかを検討してください。この手順により、MAM専用モードのデバイスのユーザーが、デバイス上の既存の証明書を使用して認証できないようにします。

Citrix Endpoint Managementは、証明書が失効した後でもユーザーがユーザー証明書を生成することを制限しないため、新しい証明書を再発行します。この設定は、CRLが期限切れのPKIエンティティをチェックする際に、PKIエンティティのセキュリティを向上させます。

裁量CA

裁量CAは、Citrix Endpoint ManagementにCA証明書と関連する秘密鍵を提供すると作成されます。Citrix Endpoint Managementは、指定されたパラメータに従って、証明書の発行、失効、およびステータス情報を内部的に処理します。

裁量CAを構成する際、そのCAに対してオンライン証明書ステータスプロトコル (OCSP) のサポートを有効にできます。OCSPサポートを有効にすると、CAはCAが発行する証明書に拡張機能 `id-pe-authorityInfoAccess` を追加します。この拡張機能は、以下の場所にあるCitrix Endpoint Management内部OCSPレスポンダーを指します。

`https://<server>/<instance>/ocsp`

OCSPサービスを構成する際、該当する裁量エンティティのOCSP署名証明書を指定します。CA証明書自体を署名者として使用できます。CA秘密鍵の不必要な露出を避けるため（推奨）：CA証明書によって署名された委任OCSP署名証明書を作成し、この拡張機能を含めます: `id-kp-OCSPSigning extendedKeyUsage`。

Citrix Endpoint Management OCSPレスポンダーサービスは、基本的なOCSP応答と、要求における以下のハッシュアルゴリズムをサポートしています。

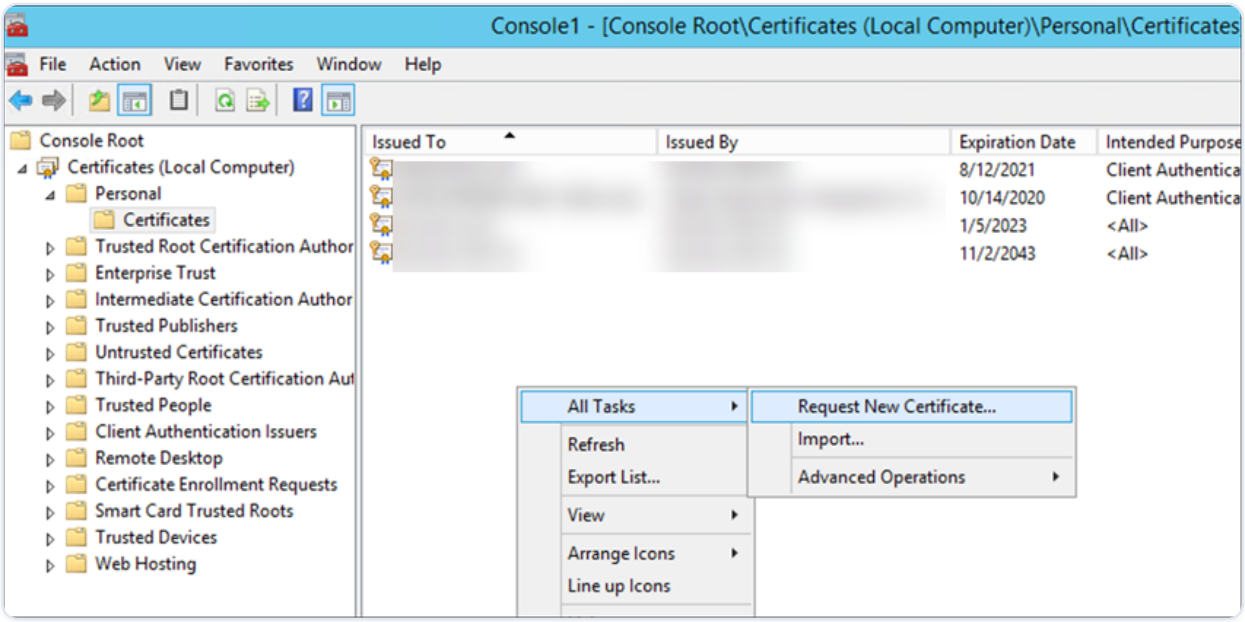
- SHA-256
- SHA-384
- SHA-512

応答はSHA-256と署名証明書鍵アルゴリズム（DSA、RSA、またはECDSA）で署名されます。

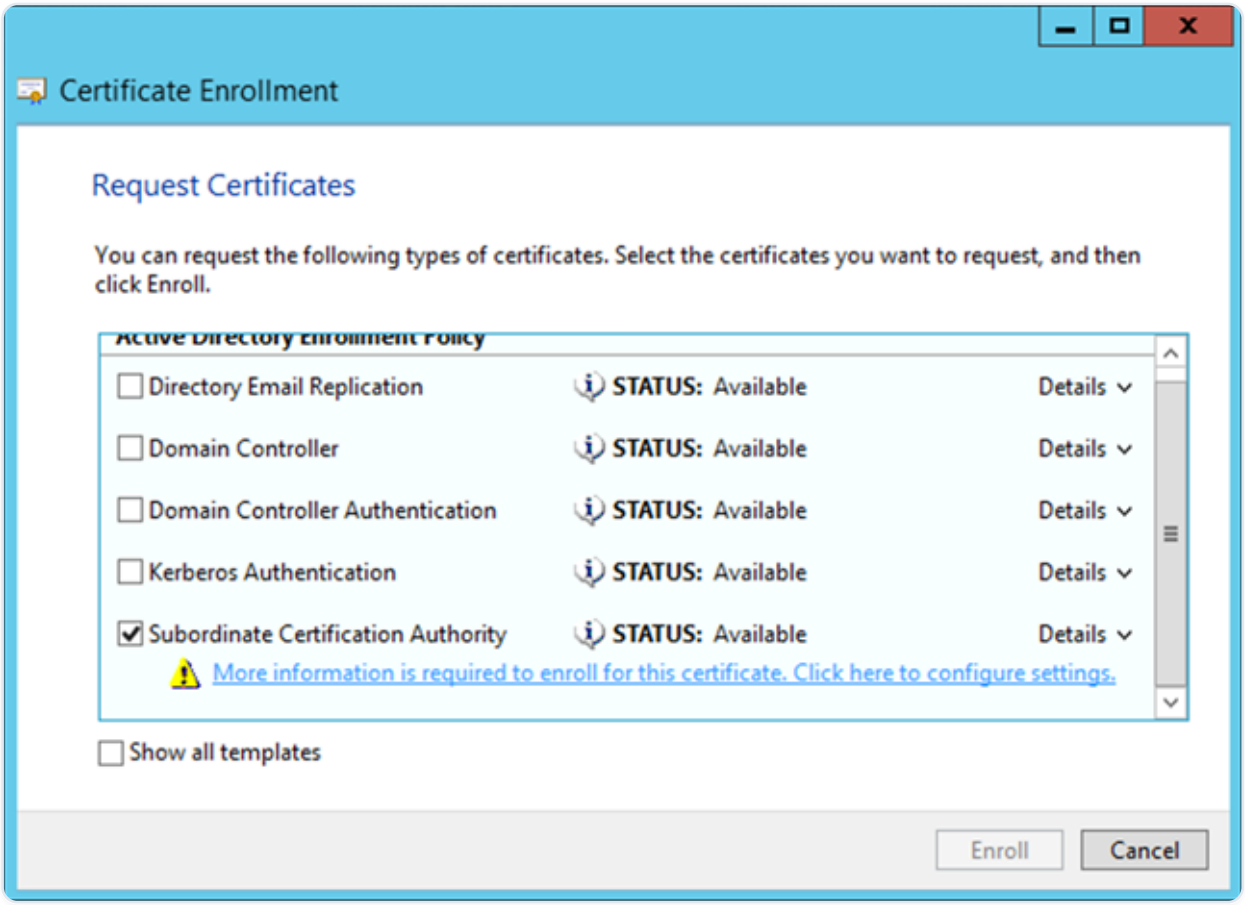
© 1997–2026 Citrix Systems, Inc. All rights reserved.

CAの証明書を生成してインポートする

1. サーバーで、ローカルシステムアカウントを使用してMicrosoft管理コンソール (MMC) を開き、証明書スナップインを開きます。右側のペインで右クリックし、**すべてのタスク > 新しい証明書を要求**をクリックします。

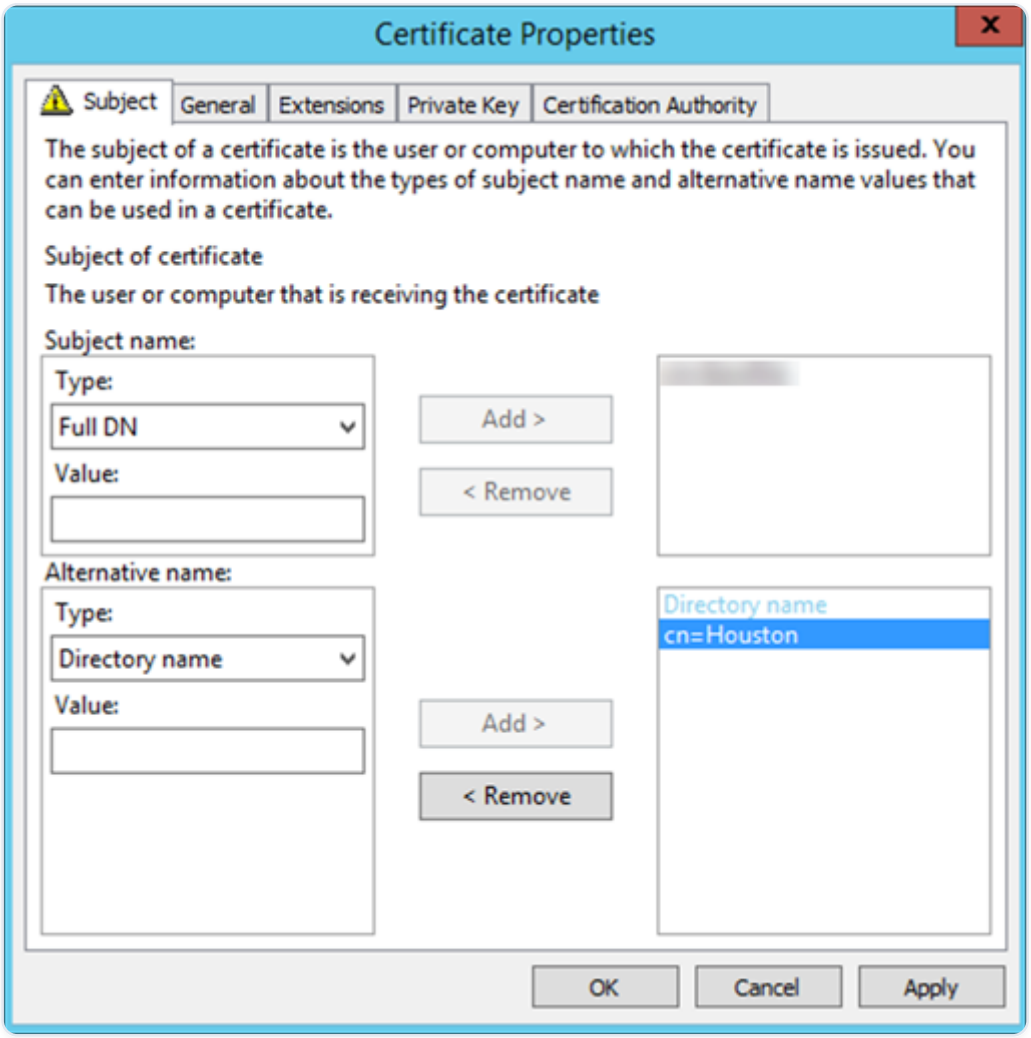


2. 開いたウィザードで、**次へ**を2回クリックします。**証明書の要求**リストで、**下位証明機関**を選択し、**詳細情報**リンクをクリックします。



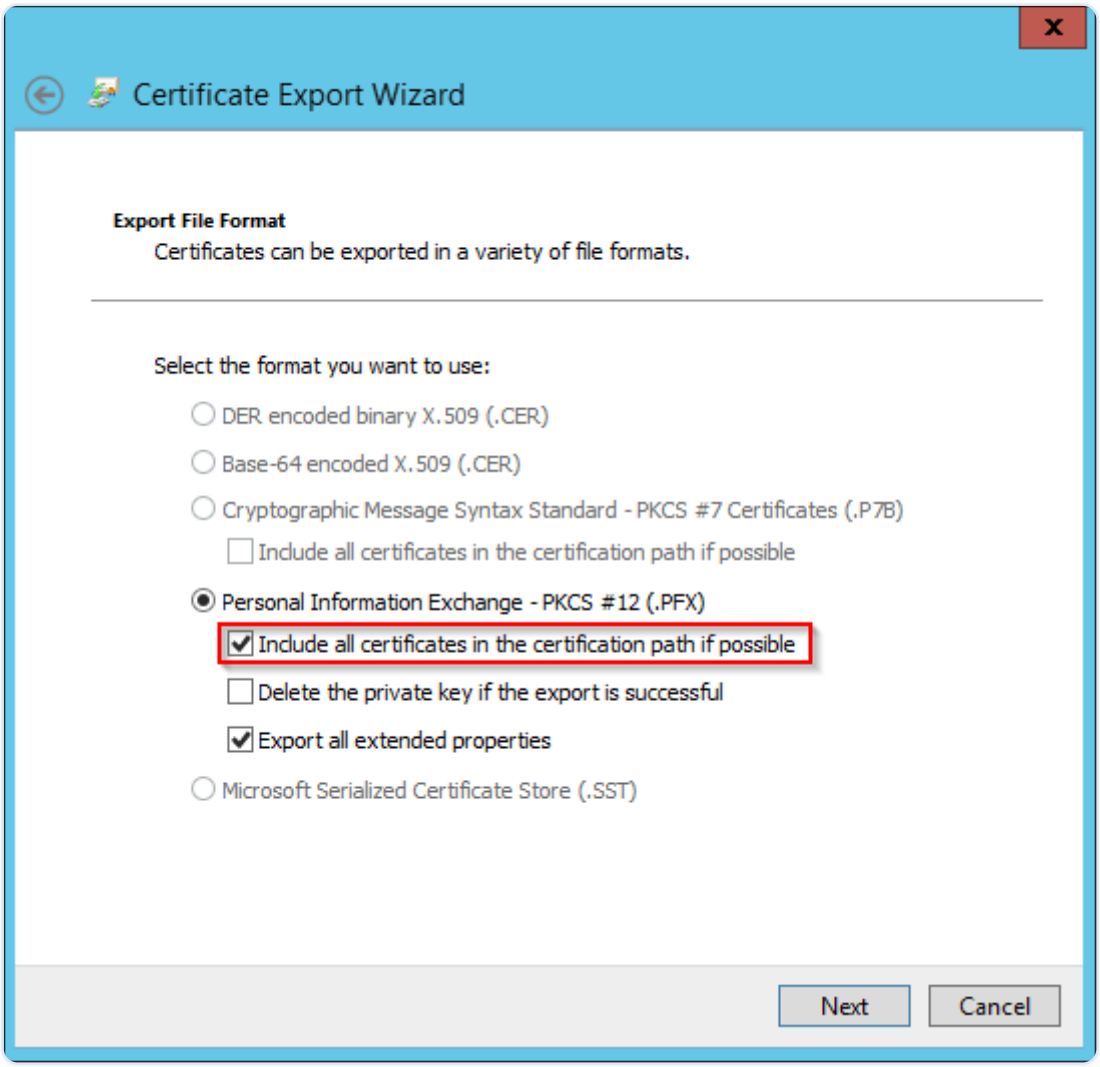
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ウィンドウで、**サブジェクト名**と**代替名**を入力します。「**OK**」をクリックします。

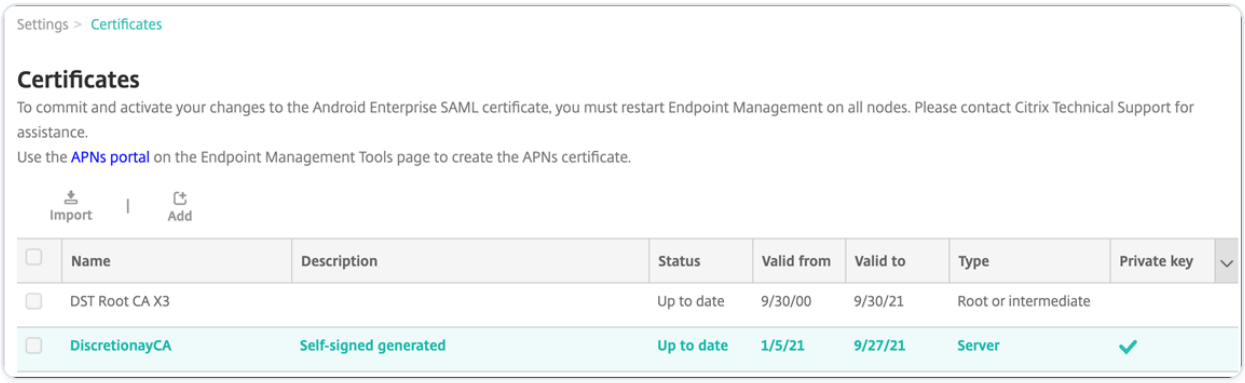


4. 「**登録**」をクリックし、次に「**完了**」をクリックします。
5. MMCで、作成した証明書を右クリックします。「**すべてのタスク > エクスポート**」をクリックします。証明書を秘密キー付きの.pfxファイルとしてエクスポートします。「**可能であれば、証明書パス内のすべての証明書を含める**」オプションを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

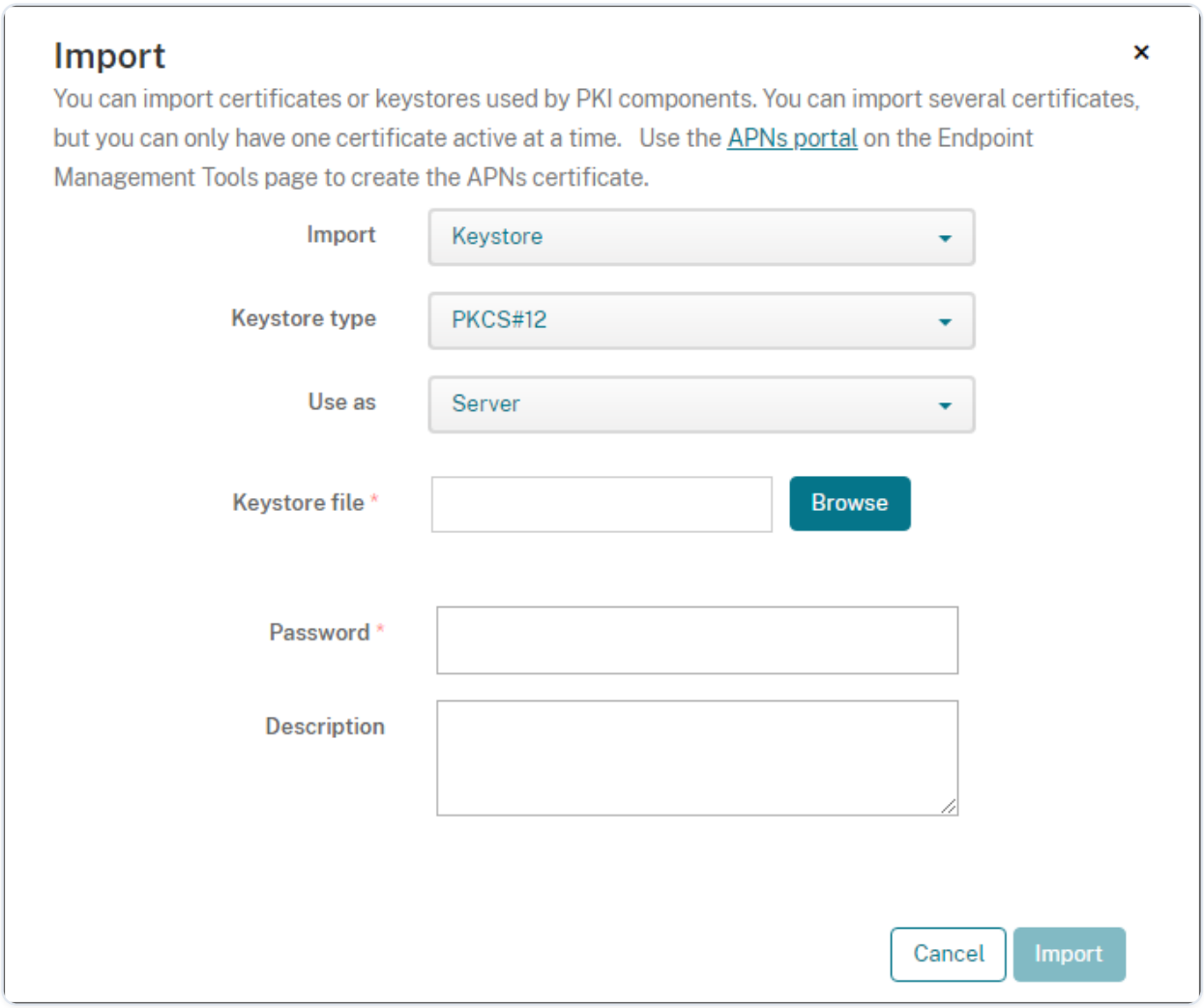


6. Citrix Endpoint Managementコンソールで、「**設定 > 証明書**」に移動します。



7. 「**インポート**」をクリックします。開いたウィンドウで、以前にエクスポートした証明書ファイルと秘密キーファイルを参照します。

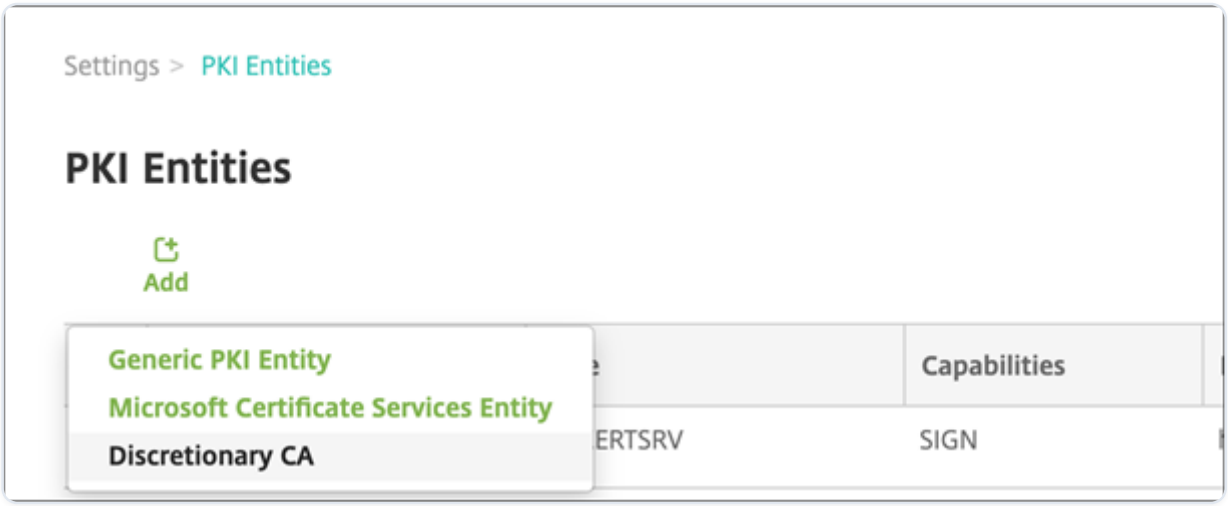
© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. 「**インポート**」をクリックします。証明書がテーブルに追加されます。

裁量CAを追加する

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックし、次に「**その他 > PKIエンティティ**」をクリックします。
2. 「**PKIエンティティ**」ページで、「**追加**」をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 「**裁量CA**」をクリックします。

   PKI全般情報ページ(/en-us/citrix-endpoint-management/media/pki-entities-discretionary-ca-general-info.png)

4. 「**裁量CA: 全般情報**」ページで、以下を構成します。

   - **名前:** 裁量CAのわかりやすい名前を入力します。
   - **証明書要求に署名するCA証明書:** 裁量CAが証明書要求の署名に使用する証明書をクリックします。

     この証明書の一覧は、**構成 > 設定 > 証明書**でCitrix Endpoint Managementにアップロードした秘密キーを持つCA証明書から生成されます。

5. **次へ**をクリックします。

   PKIパラメーターページ(/en-us/citrix-endpoint-management/media/pki-entities-discretionary-ca-parameters.png)

6. 「**裁量CA: パラメーター**」ページで、以下を構成します。

   - **シリアル番号ジェネレーター:** 裁量CAは、発行する証明書のシリアル番号を生成します。この一覧から、番号の生成方法を決定するために、**シーケンシャル**または**非シーケンシャル**をクリックします。
   - **次のシリアル番号:** 次に発行される番号を決定する値を入力します。
   - **証明書の有効期間:** 証明書が有効な日数を入力します。
   - **キー使用法:** 裁量CAが発行する証明書の目的を、適切なキーを**オン**に設定して特定します。一度設定すると、CAはそれらの目的の証明書の発行に限定されます。
   - **拡張キー使用法:** さらにパラメーターを追加するには、**追加**をクリックし、キー名を入力してから**保存**をクリックします。

7. **次へ**をクリックします。

   PKI配布ページ(/en-us/citrix-endpoint-management/media/pki-entities-discretionary-ca-distribution.png)

8. 「**裁量的CA: 配布**」ページで、配布モードを選択します。

   - **集中型: サーバー側でのキー生成**。Citrix®は集中型オプションを推奨します。秘密キーはサーバーで生成および保存され、ユーザーデバイスに配布されます。
   - **分散型: デバイス側でのキー生成**。秘密キーはユーザーデバイスで生成されます。この分散モードではSCEPを使用し、**keyUsage keyEncryption**拡張機能を持つRA暗号化証明書

© 1997–2026 Citrix Systems, Inc. All rights reserved.

と、**keyUsage digitalSignature**拡張機能を持つRA署名証明書が必要です。同じ証明書を暗号化と署名の両方に使用できます。

9. **次へ**をクリックします。

   PKI OCSPページ(/en-us/citrix-endpoint-management/media/pki-entities-discretionary-ca-ocsp.png)

10. 「**裁量的CA: オンライン証明書状態プロトコル (OCSP)**」ページで、以下を構成します。

    - このCAによって署名された証明書に`AuthorityInfoAccess` (RFC2459) 拡張機能を追加する場合は、「**このCAのOCSPサポートを有効にする**」を「**オン**」に設定します。この拡張機能は、`https://<server>/<instance>/ocsp`にあるCA OCSPレスポンダーを指します。
    - OCSPサポートを有効にした場合は、OCSP署名CA証明書を選択します。この証明書リストは、Citrix Endpoint Managementにアップロードした CA証明書から生成されます。

    この機能を有効にすると、Citrix ADCが証明書のステータスを確認できるようになります。Citrixでは、この機能を有効にすることをお勧めします。

11. **保存**をクリックします。

    裁量的CAがPKIエンティティテーブルに表示されます。

資格情報プロバイダーを構成する

1. Citrix Endpoint Managementコンソールで、**設定 > 資格情報プロバイダー**に移動し、**追加**をクリックします。
2. 「**資格情報プロバイダー: 一般情報**」ページで、以下を構成します。

   資格情報プロバイダーの一般ページ(/en-us/citrix-endpoint-management/media/credentials-provider-general-info.png)

   - **名前:** 新しいプロバイダー構成の一意の名前を入力します。この名前は、Citrix Endpoint Managementコンソールの他の部分で構成を識別するために後で使用されます。
   - **説明:** 資格情報プロバイダーについて説明します。このフィールドはオプションですが、説明は資格情報プロバイダーに関する有用な詳細を提供できます。
   - **発行エンティティ: 裁量CA**を選択します。
   - **発行方法: 署名**または**取得**をクリックして、システムが構成されたエンティティから証明書を取得するために使用する方法として機能させます。クライアント証明書認証には、**署名**を使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **次へ**をクリックします。**資格情報プロバイダー: 証明書署名要求**ページで、証明書構成に従って以下を構成します。

   資格情報プロバイダー証明書署名要求ページ(/en-us/citrix-endpoint-management/media/credentials-provider-csr.png)

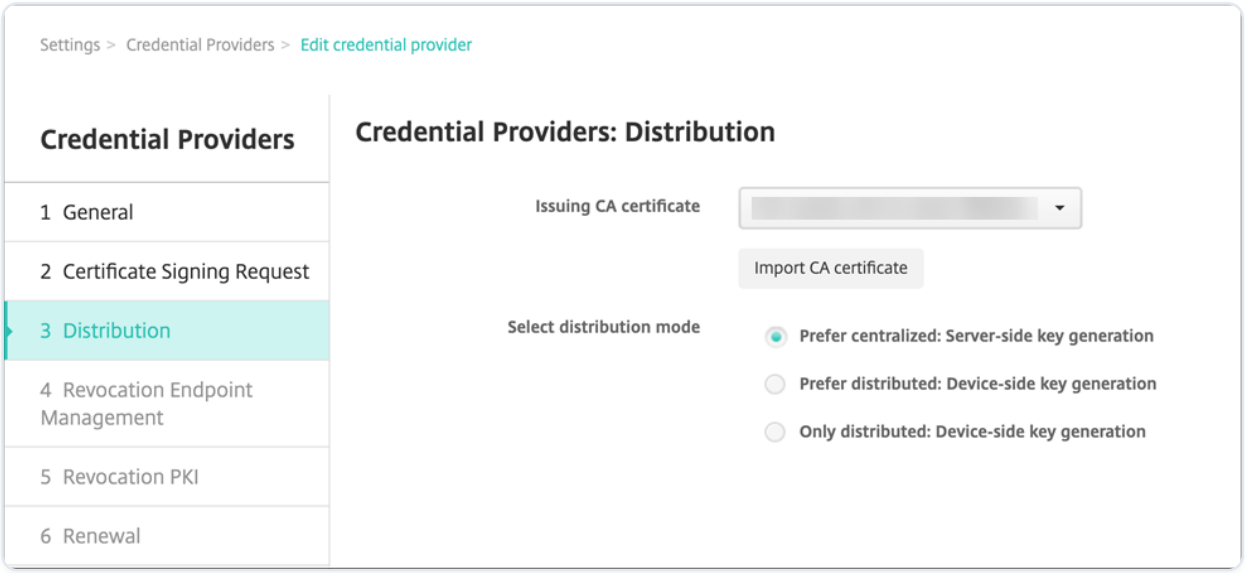
   - **キーアルゴリズム:** 新しいキーペアのキーアルゴリズムを選択します。利用可能な値は、**RSA**、**DSA**、および**ECDSA**です。
   - **キーサイズ:** キーペアのサイズをビット単位で入力します。このフィールドは必須です。Citrixは**2048**ビットの使用を推奨しています。
   - **署名アルゴリズム:** 新しい証明書の値をクリックします。値はキーアルゴリズムによって異なります。Citrixは**SHA256withRSA**を推奨しています。
   - **サブジェクト名:** 必須。新しい証明書サブジェクトの識別名 (DN) を入力します。ユーザー名には`CN=${user.username}`を使用するか、sAMAccountNameを使用するには`CN=${user.samaccountname}`を使用します。
   - **サブジェクトの別名**テーブルにエントリを追加するには、**追加**をクリックします。別名の種類を選択し、2番目の列に値を入力します。

     以下を追加します。

     - **種類:** ユーザープリンシパル名
     - **値:** `$user.userprincipalname`

     サブジェクト名と同様に、値フィールドでCitrix Endpoint Managementマクロを使用できます。

4. 「**次へ**」をクリックします。「**資格情報プロバイダー: 配布**」ページで、以下を構成します。

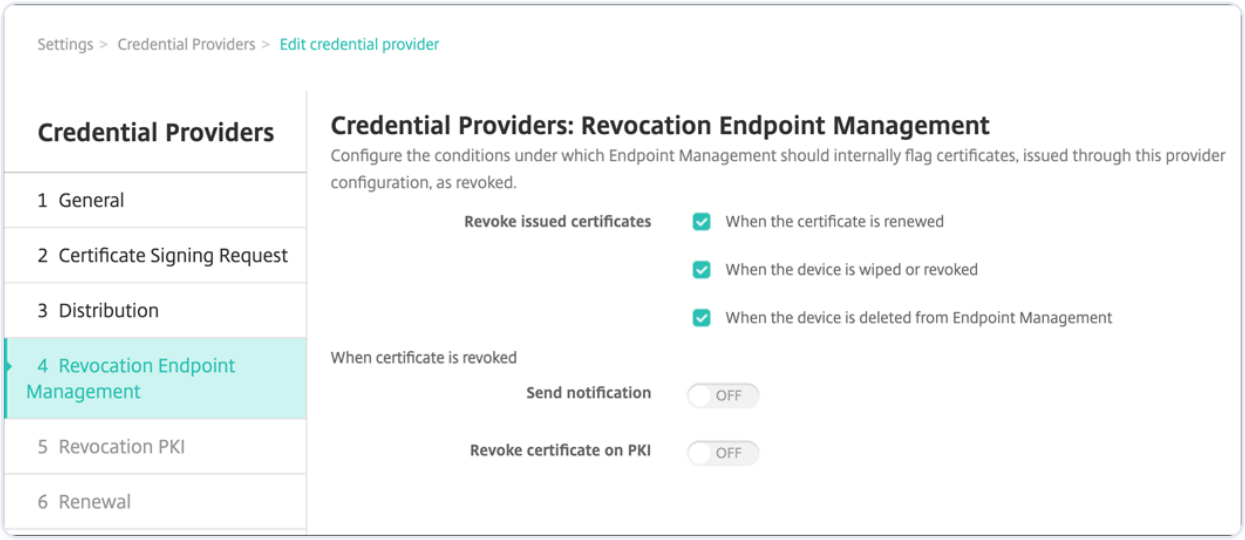


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**発行CA証明書:**」以前追加した裁量CA証明書を選択します。
- 「**配布モードの選択:**」キーを生成および配布する以下のいずれかの方法を選択します。
  - 「**集中型を優先: サーバー側でのキー生成:**」Citrixでは、この集中型オプションを推奨しています。これはCitrix Endpoint Managementでサポートされているすべてのプラットフォームをサポートしており、NetScaler Gateway認証を使用する場合に必要です。秘密キーはサーバーで生成および保存され、ユーザーデバイスに配布されます。
  - 「**分散型を優先: デバイス側でのキー生成:**」秘密キーはユーザーデバイスで生成および保存されます。この分散モードではSCEPを使用し、keyUsage keyEncryptionを持つRA暗号化証明書と、KeyUsage digitalSignatureを持つRA署名証明書が必要です。暗号化と署名の両方に同じ証明書を使用できます。
  - 「**分散型のみ: デバイス側でのキー生成:**」このオプションは「**分散型を優先: デバイス側でのキー生成**」と同じように機能しますが、デバイス側でのキー生成が失敗した場合や利用できない場合は、オプションが利用できません。

「**分散型を優先: デバイス側でのキー生成**」または「**分散型のみ: デバイス側でのキー生成**」を選択した場合、RA署名証明書とRA暗号化証明書をクリックします。両方に同じ証明書を使用できます。これらの証明書に新しいフィールドが表示されます。

5. 「**次へ**」をクリックします。「**資格情報プロバイダー: 失効 Citrix Endpoint Management**」ページで、このプロバイダー構成を通じて発行された証明書を、Citrix Endpoint Managementが内部的に失効済みとしてフラグ付けする条件を構成します。以下を構成します。

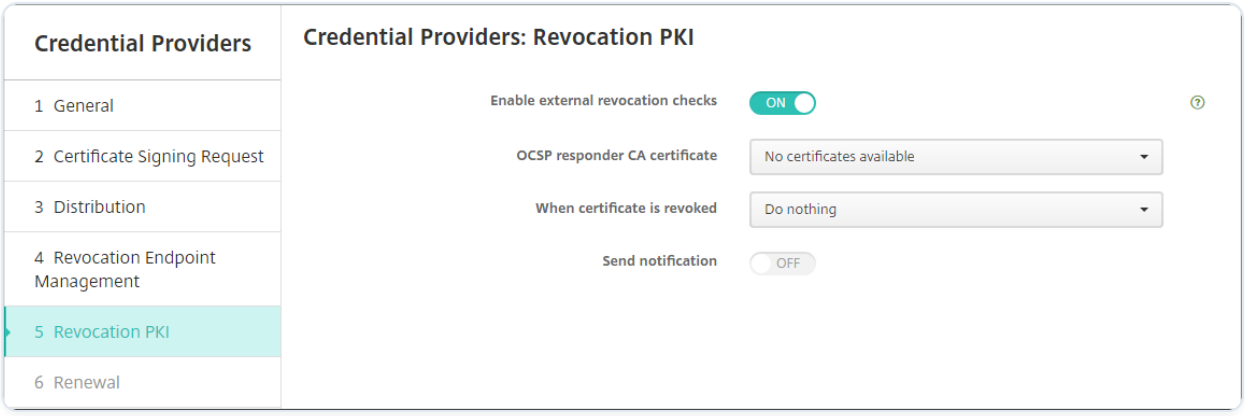


- 「**発行済み証明書の失効**」で、証明書を失効するタイミングを示すオプションのいずれかを選択します。
- 証明書が失効したときにCitrix Endpoint Managementに通知を送信させるには、「**通知の送信**」の値を「**オン**」に設定し、通知テンプレートを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**PKIでの証明書の失効**」は、Citrix Endpoint Managementを裁量PKIとして使用している場合は機能しません。

6. 「**次へ**」をクリックします。「**資格情報プロバイダー: 失効PKI**」ページで、証明書が失効した場合にPKIで実行するアクションを特定します。通知メッセージを作成するオプションもあります。以下を構成します。



- **外部失効チェックを有効にする:** この設定を**オン**にします。失効PKIに関連する追加フィールドが表示されます。
- **OCSPレスポンダーCA証明書**リストで、証明書のサブジェクトの識別名 (DN) を選択します。

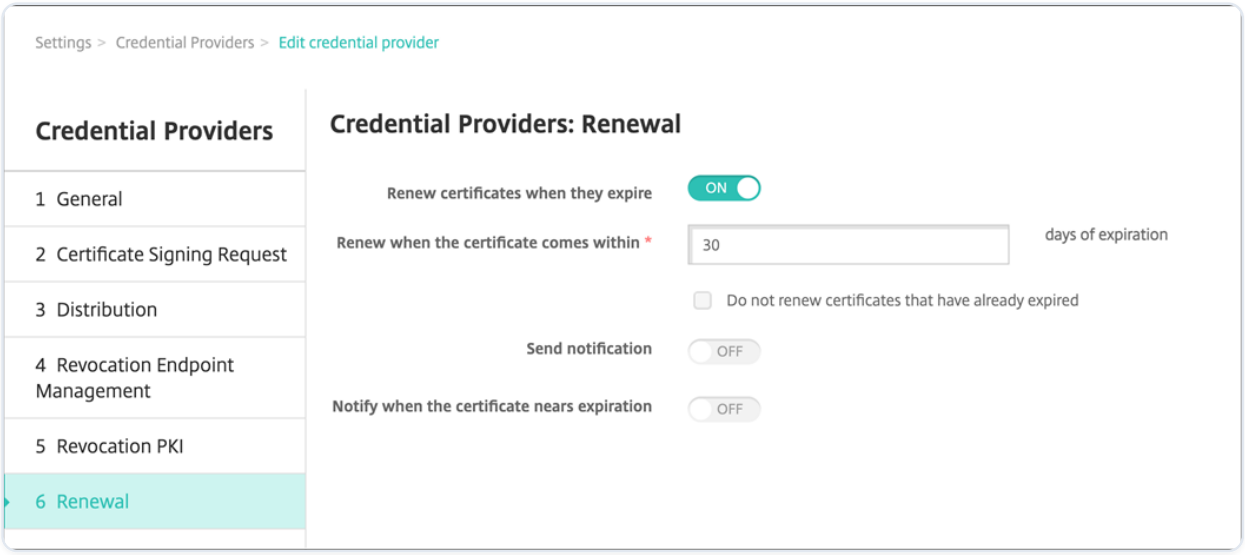
  DNフィールドの値には、Citrix Endpoint Managementのマクロを使用できます。例: `CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`
- **証明書が失効した場合**リストで、証明書が失効したときにPKIエンティティに対して実行する次のいずれかのアクションをクリックします。
  - 何もしない。
  - 証明書を更新する。
  - デバイスを失効させてワイプする。
- 証明書が失効したときにCitrix Endpoint Managementに通知を送信させるには:**通知を送信**の値を**オン**に設定します。

  2つの通知オプションから選択できます。
  - **通知テンプレートを選択**を選択した場合、事前に作成された通知メッセージを選択し、カスタマイズできます。これらのテンプレートは、通知テンプレートリストにあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **通知の詳細を入力**を選択した場合、独自の通知メッセージを作成できます。受信者のメールアドレスとメッセージを提供するだけでなく、通知の送信頻度を設定できます。

7. **次へ**をクリックします。**資格情報プロバイダー: 更新**ページで、以下を構成します。



証明書の有効期限が切れたときに更新を**オン**に設定します。追加フィールドが表示されます。

- **証明書の有効期限が近づいたときに更新**フィールドで、証明書の有効期限が切れる何日前に証明書を更新するかを入力します。
- オプションで、**期限切れの証明書を更新しない**を選択します。この場合、「期限切れ」とは、`NotAfter` の日付が過去のものであり、失効したわけではないことを意味します。Citrix Endpoint Management は、内部的に失効した証明書を更新しません。

証明書が更新されたときに Citrix Endpoint Management に通知を送信させるには、**通知を送信**を**オン**に設定します。証明書の有効期限が近づいたときに Citrix Endpoint Management に通知を送信させるには、**証明書の有効期限が近づいたら通知**を**オン**に設定します。 これらのいずれかの選択肢について、2つの通知オプションから選択できます。

- **通知テンプレートを選択:** 事前に作成された通知メッセージを選択し、カスタマイズできます。これらのテンプレートは、通知テンプレートリストにあります。
- **通知の詳細を入力:** 独自の通知メッセージを作成します。受信者のメールアドレス、メッセージ、および通知を送信する頻度を指定します。

8. **保存**をクリックします。

資格情報プロバイダー

資格情報プロバイダーは、Citrix Endpoint Managementシステムのさまざまな部分で使用する実際の証明書構成です。資格情報プロバイダーは、証明書のソース、パラメーター、およびライフサイ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クルを定義します。これらの操作は、証明書がデバイス構成の一部であるか、スタンドアロンであるか（つまり、そのままデバイスにプッシュされるか）にかかわらず実行されます。

デバイスの登録は、証明書のライフサイクルを制約します。つまり、Citrix Endpoint Managementは登録前に証明書を発行しませんが、登録の一部として一部の証明書を発行する場合があります。また、1つの登録のコンテキスト内で内部PKIから発行された証明書は、登録が取り消されると失効します。管理関係が終了すると、有効な証明書は残りません。

1つの資格情報プロバイダー構成を多くの場所で使用でき、1つの構成で任意の数の証明書を同時に管理できます。その場合の一体性は、展開リソースと展開にあります。たとえば、資格情報プロバイダーPが構成Cの一部としてデバイスDに展開される場合：Pの発行設定によってDに展開される証明書が決定されます。同様に、Cが更新されるとDの更新設定が適用されます。また、Cが削除されるかDが取り消されると、Dの失効設定も適用されます。

これらのルールに従って、Citrix Endpoint Managementの資格情報プロバイダー構成は以下を決定します。

- 証明書のソース。
- 証明書を取得する方法：新しい証明書に署名するか、既存の証明書とキーペアをフェッチ（回復）します。
- 発行または回復のパラメーター：たとえば、キーサイズ、キーアルゴリズム、証明書拡張機能などの証明書署名要求（CSR）パラメーター。
- 証明書がデバイスに配信される方法。
- 失効条件：管理関係が切断されるとCitrix Endpoint Management内のすべての証明書が失効しますが、構成でより早い失効を指定できます。たとえば、関連するデバイス構成が削除されたときに証明書を失効させるように構成で指定できます。また、特定の条件下では、Citrix Endpoint Management内の関連する証明書の失効がバックエンドの公開鍵インフラストラクチャ（PKI）に送信される場合があります。つまり、Citrix Endpoint Managementでの証明書の失効がPKIでの証明書の失効を引き起こす可能性があります。
- 更新設定：特定の資格情報プロバイダーを介して取得された証明書は、有効期限が近づくと自動的に更新できます。または、その状況とは別に、有効期限が近づいたときに通知を発行することもできます。

構成オプションの可用性は、主に資格情報プロバイダーに選択するPKIエンティティのタイプと発行方法によって異なります。

証明書の発行方法

署名によって証明書を取得できます。これは発行方法として知られています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

この方法では、発行には新しい秘密鍵の作成、CSRの作成、および署名のためにCSRを認証局（CA）に提出することが含まれます。Citrix Endpoint Managementは、MS証明書サービスエンティティと裁量CAエンティティの両方で署名方法をサポートしています。

資格情報プロバイダーは、署名発行方法を使用します。

証明書の配信

Citrix Endpoint Managementでは、証明書の配信モードとして、集中型と分散型の2種類が利用可能です。分散モードは、Simple Certificate Enrollment Protocol (SCEP) を使用し、クライアントがプロトコルをサポートしている状況 (iOSのみ) でのみ利用できます。分散モードは、一部の状況で必須です。

資格情報プロバイダーが分散型（SCEP支援）配信をサポートするには、特別な構成手順が必要です。それは、登録機関（RA）証明書の設定です。SCEPプロトコルを使用する場合、Citrix Endpoint Managementは実際の証明機関に対するデリゲート（登録者）として機能するため、RA証明書が必要です。Citrix Endpoint Managementは、そのように機能する権限があることをクライアントに証明する必要があります。その権限は、前述の証明書をCitrix Endpoint Managementにアップロードすることで確立されます。

2つの異なる証明書ロールが必要です（ただし、1つの証明書で両方の要件を満たすことができます）。RA署名とRA暗号化です。これらのロールの制約は次のとおりです。

- RA署名証明書には、X.509キー使用法「デジタル署名」が必要です。
- RA暗号化証明書には、X.509キー使用法「キー暗号化」が必要です。

資格情報プロバイダーのRA証明書を構成するには、証明書をCitrix Endpoint Managementにアップロードし、資格情報プロバイダーでそれらにリンクします。

資格情報プロバイダーが証明書ロール用に構成された証明書を持っている場合にのみ、分散配信をサポートすると見なされます。各資格情報プロバイダーを、集中モードを優先するか、分散モードを優先するか、または分散モードを必須とするように構成できます。実際の結果はコンテキストによって異なります。コンテキストが分散モードをサポートしていないが、資格情報プロバイダーがこのモードを要求する場合、展開は失敗します。同様に、コンテキストが分散モードを要求しているが、資格情報プロバイダーが分散モードをサポートしていない場合、展開は失敗します。その他のすべての場合において、優先設定が尊重されます。

次の表は、Citrix Endpoint Management全体でのSCEPの配布を示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コンテキスト	SCEPサポート	SCEP必須
iOSプロファイルサービス	はい	はい
iOSモバイルデバイス管理登録	はい	いいえ
iOS構成プロファイル	はい	いいえ
SHTP登録	いいえ	いいえ
SHTP構成	いいえ	いいえ
Windowsタブレット登録	いいえ	いいえ
Windowsタブレットの構成	いいえ。ただし、Windows 10およびWindows 11リリースでサポートされているネットワークデバイスポリシーは除きます。	いいえ

証明書の失効

失効には3つの種類があります。

- **内部失効:** 内部失効は、Citrix Endpoint Managementによって維持される証明書の状態に影響します。Citrix Endpoint Managementは、提示された証明書を評価する際、または証明書のOCSPステータス情報を提供する際に、この状態を考慮します。資格情報プロバイダーの構成は、さまざまな条件下でこの状態がどのように影響されるかを決定します。たとえば、資格情報プロバイダーは、証明書がデバイスから削除されたときに、証明書を失効済みとしてフラグ付けするように指定する場合があります。
- **外部伝播失効:** Citrix Endpoint Management失効とも呼ばれるこの種類の失効は、外部PKIから取得した証明書に適用されます。資格情報プロバイダーの構成で定義された条件の下で、Citrix Endpoint Managementが内部的に証明書を失効させると、PKI上で証明書が失効します。
- **外部誘発失効:** PKI失効とも呼ばれるこの種類の失効も、外部PKIから取得した証明書にのみ適用されます。Citrix Endpoint Managementが特定の証明書の状態を評価するたびに、Citrix Endpoint Managementはその状態についてPKIに問い合わせます。証明書が失効している場合、Citrix Endpoint Managementは内部的に証明書を失効させます。このメカニズムはOCSPプロトコルを使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

これら3つの種類は排他的ではなく、むしろ組み合わせて適用されます。外部失効または独立した検出が内部失効を引き起こす可能性があります。内部失効は、外部失効に影響を与える可能性があります。

証明書の更新

証明書の更新とは、既存の証明書の失効と、別の証明書の発行を組み合わせたものです。

Citrix Endpoint Managementは、発行が失敗した場合のサービス中断を避けるため、以前の証明書を失効させる前に新しい証明書を取得しようとします。分散型（SCEP対応）配信の場合、失効は証明書がデバイスに正常にインストールされた後にのみ発生します。それ以外の場合、失効は新しい証明書がデバイスに送信される前に発生します。その失効は、証明書のインストールの成否とは無関係です。

失効構成では、特定の期間（日数）を指定する必要があります。デバイスが接続すると、サーバーは証明書の`NotAfter`日付が現在の日付から指定された期間を引いた日付よりも後であるかどうかを確認します。証明書がその条件を満たしている場合、Citrix Endpoint Managementは証明書の更新を試みます。

資格情報プロバイダーの作成

資格情報プロバイダーの設定は、主に、資格情報プロバイダーに選択する発行エンティティと発行方法によって異なります。内部エンティティまたは外部エンティティを使用する資格情報プロバイダーを区別できます。

- Citrix Endpoint Managementの内部にある裁量エンティティは、内部エンティティです。裁量エンティティの発行方法は常に署名です。署名とは、発行操作ごとに、Citrix Endpoint Managementがエンティティに選択されたCA証明書で新しいキーペアに署名することを意味します。キーペアがデバイスで生成されるかサーバーで生成されるかは、選択した配布方法によって異なります。
- 企業のインフラストラクチャの一部である外部エンティティには、Microsoft CAが含まれます。

1. Citrix Endpoint Managementコンソールで、右上隅の歯車アイコンをクリックし、 **>** をクリックします。
2. ページで、 をクリックします。

   ページが表示されます。
3. ページで、次の操作を行います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **名前:** 新しいプロバイダー構成の一意の名前を入力します。この名前は、後でCitrix Endpoint Managementコンソールの他の部分で構成を識別するために使用されます。
- **説明:** 資格情報プロバイダーについて説明します。このフィールドはオプションですが、説明は資格情報プロバイダーに関する有用な詳細を提供できます。
- **発行エンティティ:** 証明書発行エンティティをクリックします。
- **発行方法:** または をクリックして、システムが構成されたエンティティから証明書を取得するために使用する方法として機能させます。クライアント証明書認証には、 を使用します。
- リストが利用可能な場合は、資格情報プロバイダーのPKIエンティティの下に追加したテンプレートを選択します。

  これらのテンプレートは、 **>** でMicrosoft Certificate Servicesエンティティが追加されると利用可能になります。

4. をクリックします。

   ページが表示されます。

5. 「**Credential Providers: Certificate Signing Request**」ページで、証明書構成に従って以下を設定します。

   - 「**キーアルゴリズム:**」新しいキーペアのキーアルゴリズムを選択します。使用可能な値は、**RSA**、**DSA**、**ECDSA** です。
   - 「**キーサイズ:**」キーペアのサイズをビット単位で入力します。このフィールドは必須です。

     許容される値はキーの種類によって異なります。たとえば、DSA キーの最大サイズは 2048 ビットです。基盤となるハードウェアとソフトウェアに依存する誤検出を避けるため、Citrix Endpoint Management はキーサイズを強制しません。運用環境でアクティブ化する前に、必ずテスト環境で資格情報プロバイダーの構成をテストしてください。
   - 「**署名アルゴリズム:**」新しい証明書の値をクリックします。値はキーアルゴリズムによって異なります。
   - 「**サブジェクト名:**」必須。新しい証明書サブジェクトの識別名 (DN) を入力します。例: `CN=${user.username}, OU=${user.department}, O=${user.companyname},C=${user.c}\endquotation`

     たとえば、クライアント証明書認証の場合は、次の設定を使用します。

     - 「**キーアルゴリズム:**」RSA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**キーサイズ:**」2048
- 「**署名アルゴリズム:**」SHA256withRSA
- 「**サブジェクト名:**」`cn=$user.username`

- 「**サブジェクトの別名**」テーブルにエントリを追加するには、「**追加**」をクリックします。別名の種類を選択し、2番目の列に値を入力します。

  クライアント証明書認証の場合は、以下を指定します。

  - 「**種類:**」ユーザープリンシパル名
  - 「**値:**」`$user.userprincipalname`

    サブジェクト名と同様に、値フィールドでCitrix Endpoint Management マクロを使用できます。

6. **次へ**をクリックします。

   資格情報プロバイダー: 配信ページが表示されます。

7. **資格情報プロバイダー: 配信**ページで、次の操作を行います。

   - **発行CA証明書**リストで、提示されたCA証明書をクリックします。資格情報プロバイダーは裁量的なCAエンティティを使用するため、資格情報プロバイダーのCA証明書は、常にエンティティ自体に構成されているCA証明書です。外部エンティティを使用する構成との整合性を保つために、CA証明書がここに表示されます。
   - **配信モードの選択**で、次のいずれかのキーの生成および配信方法をクリックします。

     - **集中型を優先: サーバー側でのキー生成:** Citrixでは、この集中型オプションを推奨しています。これは、Citrix Endpoint Managementでサポートされているすべてのプラットフォームをサポートし、NetScaler Gateway認証を使用する場合に必要です。秘密キーはサーバーで生成および保存され、ユーザーデバイスに配信されます。
     - **分散型を優先: デバイス側でのキー生成:** 秘密キーはユーザーデバイスで生成および保存されます。この分散モードではSCEPを使用し、keyUsage keyEncryptionを持つRA暗号化証明書と、KeyUsage digitalSignatureを持つRA署名証明書が必要です。同じ証明書を暗号化と署名の両方に使用できます。
     - **分散型のみ: デバイス側でのキー生成:** このオプションは、「分散型を優先: デバイス側でのキー生成」と同じように機能します。ただし、「優先」ではなく「のみ」であるため、デバイス側でのキー生成が失敗した場合や利用できない場合は、オプションは利用できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

分散型を優先: デバイス側でのキー生成または**分散型のみ: デバイス側でのキー生成**を選択した場合は、RA署名証明書とRA暗号化証明書をクリックします。同じ証明書を両方に使用できます。これらの証明書に対して新しいフィールドが表示されます。

8. **次へ**をクリックします。

   資格情報プロバイダー: 失効 Citrix Endpoint Managementページが表示されます。このページでは、Citrix Endpoint Managementがこのプロバイダー構成を通じて発行された証明書を内部的に失効済みとしてフラグ付けする条件を構成します。

9. **資格情報プロバイダー: 失効 Citrix Endpoint Management**ページで、次の操作を行います。

   - **発行済み証明書の失効**で、証明書を失効させるタイミングを示すオプションのいずれかを選択します。
   - 証明書が失効したときにCitrix Endpoint Managementに通知を送信させるには、**通知の送信**の値を**オン**に設定し、通知テンプレートを選択します。
   - Citrix Endpoint Managementから証明書が失効されたときにPKIで証明書を失効させるには、「**PKIで証明書を失効する**」を「**オン**」に設定し、「**エンティティリスト**」でテンプレートをクリックします。エンティティリストには、失効機能を持つすべての利用可能なエンティティが表示されます。Citrix Endpoint Managementから証明書が失効されると、エンティティリストから選択されたPKIに失効呼び出しが送信されます。

10. 「**次へ**」をクリックします。

    「**資格情報プロバイダー: 失効PKI**」ページが表示されます。このページでは、証明書が失効された場合にPKIで実行するアクションを特定します。通知メッセージを作成するオプションもあります。

11. 「**資格情報プロバイダー: 失効PKI**」ページで、PKIから証明書を失効させたい場合は、次の操作を行います。

    - 「**外部失効チェックを有効にする**」の設定を「**オン**」に変更します。失効PKIに関連する追加フィールドが表示されます。
    - 「**OCSPレスポンダーCA証明書**」リストで、証明書のサブジェクトの識別名 (DN) をクリックします。

      DNフィールドの値には、Citrix Endpoint Managementマクロを使用できます。例: `CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`

    - 「**証明書が失効された場合**」リストで、証明書が失効されたときにPKIエンティティに対して実行する次のいずれかのアクションをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 何もしない。
    - 証明書を更新する。
    - デバイスを失効させてワイプする。

- 証明書が失効されたときにCitrix Endpoint Managementに通知を送信させるには、「**通知を送信**」の値を「**オン**」に設定します。

  2つの通知オプションから選択できます。

- 「**通知テンプレートを選択**」を選択すると、事前に作成された通知メッセージを選択し、それをカスタマイズできます。これらのテンプレートは「通知テンプレート」リストにあります。
- 「**通知の詳細を入力**」を選択すると、独自の通知メッセージを作成できます。受信者のメールアドレスとメッセージを提供するだけでなく、通知の送信頻度を設定できます。

12. 「**次へ**」をクリックします。

    「**資格情報プロバイダー: 更新**」ページが表示されます。このページでは、Citrix Endpoint Managementで次の操作を行うように構成できます。

    - 証明書を更新します。オプションで、更新時に通知を送信したり、すでに期限切れの証明書を操作から除外したりできます。
    - 有効期限が近づいている証明書について通知を発行します（更新前の通知）。

13. 証明書の有効期限が切れたときに更新する場合は、「**資格情報プロバイダー: 更新**」ページで次の操作を行います。

    有効期限が切れたときに「**証明書を更新**」を「**オン**」に設定します。追加のフィールドが表示されます。

    - 「**証明書の有効期限が近づいたときに更新**」フィールドに、証明書を更新する有効期限までの日数を入力します。
    - オプションで、「**すでに期限切れの証明書は更新しない**」を選択します。この場合、「すでに期限切れ」とは、`NotAfter`の日付が過去のものであり、失効したわけではないことを意味します。Citrix Endpoint Managementは、内部的に失効した証明書を更新しません。

    証明書が更新されたときにCitrix Endpoint Managementに通知を送信させるには、「**通知を送信**」を「**オン**」に設定します。証明書の有効期限が近づいたときにCitrix Endpoint Managementに通知を送信させるには、「**証明書の有効期限が近づいたときに通知**」を「**オン**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

」に設定します。 これらのいずれかの選択肢について、2つの通知オプションから選択できます。

- 「**通知テンプレートを選択:**」カスタマイズ可能な、事前に作成された通知メッセージを選択します。これらのテンプレートは、通知テンプレートリストにあります。
- 「**通知の詳細を入力:**」独自の通知メッセージを作成します。受信者のメールアドレス、メッセージ、および通知を送信する頻度を指定します。

「**証明書の有効期限が近づいたときに通知**」フィールドに、証明書の有効期限までの何日前に通知を送信するかを入力します。

14. 「**保存**」をクリックします。

資格情報プロバイダーが資格情報プロバイダーテーブルに表示されます。

APNs証明書

Citrix Endpoint ManagementでAppleデバイスを登録および管理するには、AppleからApple Push Notification service (APNs) 証明書を設定します。この証明書により、Apple Push Networkを介したモバイルデバイス管理が可能になります。

ワークフローの概要:

ステップ1: 証明書署名要求 (CSR) をいずれかの方法で作成します:

- macOSのキーチェーンアクセスを使用してCSRを作成する (Citrix®が推奨)
- Microsoft IISを使用してCSRを作成する
- OpenSSLを使用してCSRを作成する

ステップ2: Citrix Endpoint Management ToolsでCSRに署名する

ステップ3: 署名済みCSRをAppleに提出してAPNs証明書を取得する

ステップ4: ステップ1で使用したのと同じコンピューターを使用して、CSRを完了し、PKCS #12ファイルをエクスポートする:

- macOSのキーチェーンアクセスを使用してPKCS #12ファイルを作成する
- Microsoft IISを使用してPKCS #12ファイルを作成する
- OpenSSLを使用してPKCS #12ファイルを作成する

ステップ5: APNs証明書をCitrix Endpoint Managementにインポートする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステップ6: APNs証明書を更新する

証明書署名要求を作成する

macOS のキーチェーンアクセスを使用して CSR を作成することをお勧めします。Microsoft IIS または OpenSSL を使用して CSR を作成することもできます。

重要:

- 証明書の作成に使用する Apple ID について:
  - Apple ID は個人用 ID ではなく、企業用 ID である必要があります。
  - 証明書の作成に使用する Apple ID を記録してください。
  - 証明書を更新するには、同じ組織名と Apple ID を使用してください。異なる Apple ID を使用して証明書を更新すると、デバイスの再登録が必要になります。
- 誤って、または意図的に証明書を失効させた場合、デバイスを管理する機能が失われます。
- iOS Developer Enterprise Program を使用してモバイルデバイスマネージャープッシュ証明書を作成した場合は、Apple Push Certificates Portal で移行された証明書に対するすべてのアクションを必ず処理してください。

macOS のキーチェーンアクセスを使用して CSR を作成する

1. macOS を実行しているコンピューターで、**アプリケーション > ユーティリティ** の下にあるキーチェーンアクセスアプリを起動します。
2. **キーチェーンアクセス** メニューを開き、**証明書アシスタント > 認証局に証明書を要求** をクリックします。
3. 証明書アシスタントは、次の情報の入力を求めます。
   - **メールアドレス:** 証明書を管理する個人またはロールアカウントのメールアドレス。
   - **コモンネーム:** 証明書を管理する個人またはロールアカウントのコモンネーム。
   - **CAメールアドレス:** 認証局のメールアドレス。
4. **ディスクに保存**と**キーペア情報を指定する**オプションを選択し、**続行**をクリックします。
5. CSRファイルの名前を入力し、ファイルをコンピューターに保存してから、**保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. キーペア情報を指定します。**キーサイズ**で2048ビットを、**RSAアルゴリズム**を選択し、**続行**をクリックします。これで、APNs証明書プロセスの一部としてアップロードするCSRファイルの準備ができました。
7. 証明書アシスタントがCSRプロセスを完了したら、**完了**をクリックします。
8. 続行するには、CSRに署名します。

Microsoft IISを使用してCSRを作成する

APNs証明書要求を生成する最初のステップは、証明書署名要求（CSR）を作成することです。Windowsの場合、Microsoft IISを使用してCSRを生成します。

1. Microsoft IISを開きます。
2. IISのサーバー証明書アイコンをダブルクリックします。
3. **サーバー証明書**ウィンドウで、**証明書要求の作成**をクリックします。
4. 適切な識別名（DN）情報を入力します。たとえば、Citrix Endpoint Managementサーバーの完全修飾ドメイン名（FQDN）を`www.domain.com`のように入力できます。次に、**次へ**をクリックします。
5. 暗号化サービスプロバイダーとして**Microsoft RSA SChannel Cryptographic Provider**を、ビット長として**2048**を選択し、**次へ**をクリックします。
6. ファイル名を入力し、CSRを保存する場所を指定してから、**完了**をクリックします。
7. 続行するには、CSRに署名します。

OpenSSL を使用して CSR を作成する

macOS デバイスまたは Microsoft IIS を使用して CSR を生成できない場合は、OpenSSL を使用します。OpenSSL は、OpenSSL の Web サイトからダウンロードしてインストールできます。

1. OpenSSL をインストールしたコンピューターで、コマンドプロンプトまたはシェルから次のコマンドを実行します。

   ```
   openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.csr -newkey rsa:2048
   ```

2. 証明書の命名情報に関する次のメッセージが表示されます。要求された情報を入力します。

   ```
   You are about to be asked to enter information that will be incorporated into your certificate request.

   What you are about to enter is what is called a Distinguished Name or a DN.
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:CA

Locality Name (eg, city) []:RWC

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer

Organizational Unit Name (eg, section) [:Marketing

Common Name (eg, YOUR name) []:John Doe

Email Address []:john.doe@customer.com
```

3. 次のメッセージで、CSR プライベートキーのパスワードを入力します。

```
Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:
```

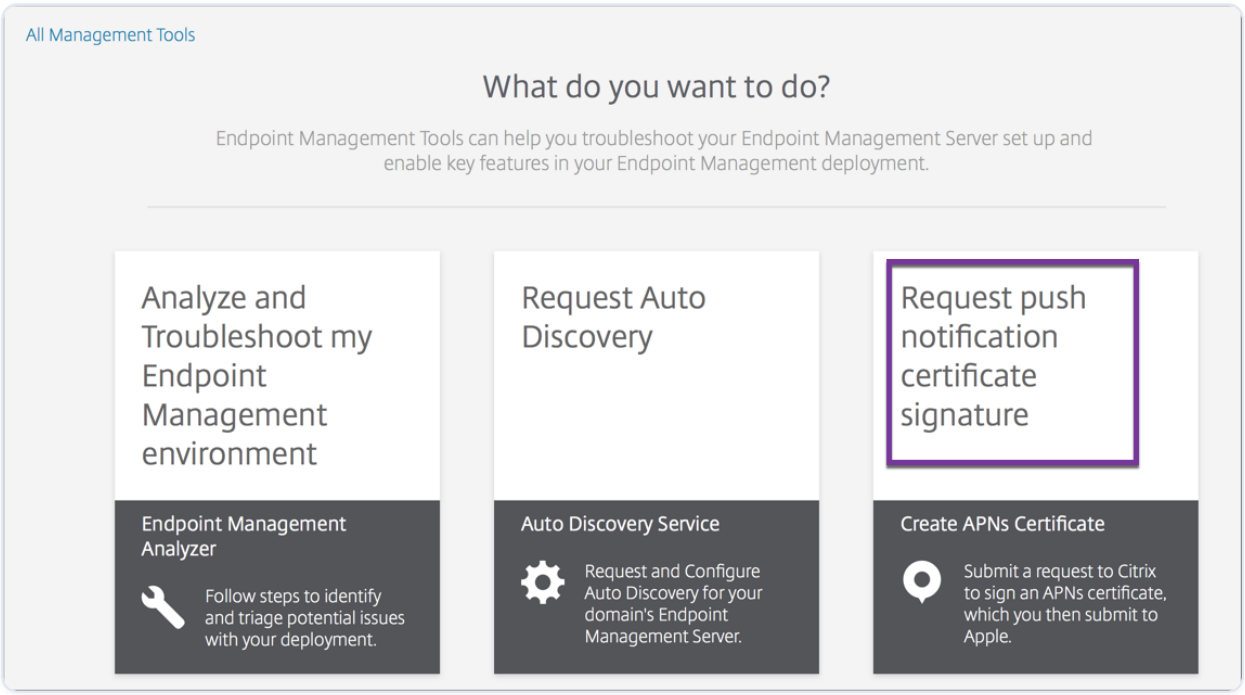
4. 続行するには、次のセクションで説明されているように CSR に署名します。

CSR に署名する

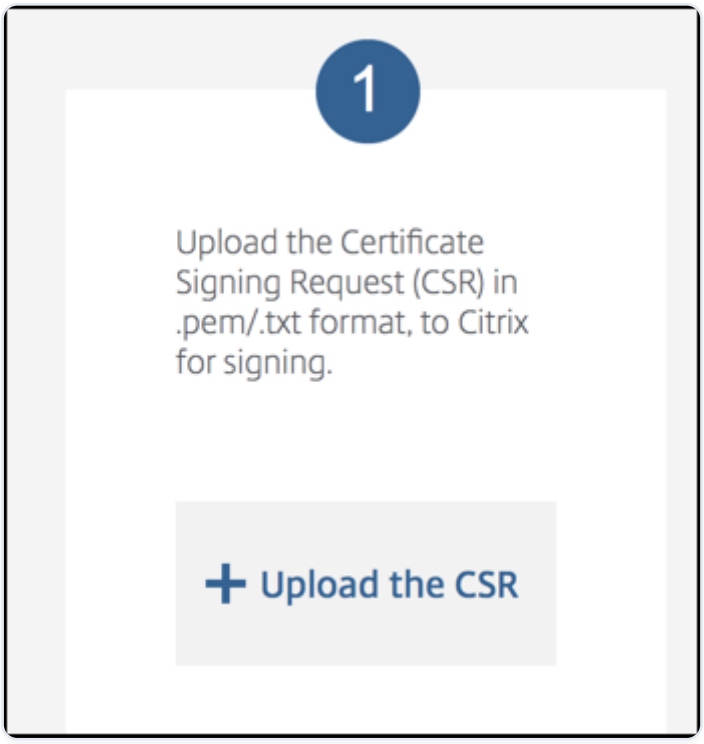
Citrix Endpoint Management で証明書を使用するには、署名のために Citrix に提出する必要があります。Citrix は、Mobile Device Management 署名証明書で CSR に署名し、署名済みファイルを `.plist` 形式で返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. ブラウザーで Citrix Endpoint Management Tools Web サイトにアクセスし、**Request push notification certificate signature** をクリックします。



2. **Creating a new certificate page** で、**Upload the CSR** をクリックします。



3. 証明書を参照して選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

証明書は.pem/.txt形式である必要があります。必要に応じて、ファイルを右クリックして名前を変更し、証明書のファイル名拡張子を.pemまたは.txtに変更してください。

4. **Citrix Endpoint Management APNs CSR署名**ページで、**署名**をクリックします。CSRが署名され、設定済みのダウンロードフォルダーに自動的に保存されます。
5. 続行するには、次のセクションで説明されているように、署名済みのCSRを提出します。

署名済みのCSRをAppleに提出してAPNs証明書を取得する

Citrixから署名済みの証明書署名要求 (CSR) を受け取ったら、そのCSRをAppleに提出して、Citrix Endpoint Managementにインポートするために必要なAPNs証明書を取得します。

注:

一部のユーザーは、Apple Push Portalへのログインで問題を報告しています。代替手段として、Apple Developer Portalにログオンできます。その後、次の手順に従うことができます。

1. ブラウザーで、Apple Push Certificates Portalにアクセスします。
2. **証明書の作成**をクリックします。
3. Appleで証明書を初めて作成する場合: **これらの利用規約を読み、同意します**チェックボックスを選択し、**同意**をクリックします。
4. **ファイルの選択**をクリックし、コンピューター上の署名済みCSRを参照して、**アップロード**をクリックします。確認メッセージが表示され、アップロードが成功したことを示します。
5. **ダウンロード**をクリックして、.pem証明書を取得します。
6. 続行するには、次のセクションで説明されているように、CSRを完了し、PKCS #12ファイルをエクスポートします。

CSRを完了し、PKCS #12ファイルをエクスポートする

AppleからAPNs証明書を受け取ったら、キーチェーンアクセス、Microsoft IIS、またはOpenSSLに戻り、証明書をPCKS #12ファイルにエクスポートします。

PKCS #12 ファイルには、APNS 証明書ファイルと秘密鍵が含まれています。PFX ファイルの拡張子は通常 .pfx または .p12 です。.pfx ファイルと .p12 ファイルは相互に利用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

Citrix では、個人キーと公開キーをローカルシステムから保存またはエクスポートすることをお勧めします。これらのキーは、APNs 証明書を再利用するために必要です。同じキーがない場合、証明書は無効になり、CSR および APNs プロセス全体を繰り返す必要があります。

macOS のキーチェーンアクセスを使用して PKCS #12 ファイルを作成する

重要:

このタスクには、CSR の生成に使用したのと同じ macOS デバイスを使用してください。

1. デバイスで、Apple から受け取った本番 ID (.pem) 証明書を見つけます。
2. キーチェーンアクセスアプリケーションを起動し、**ログイン > 自分の証明書**タブに移動します。製品 ID 証明書を開いているウィンドウにドラッグアンドドロップします。
3. 証明書をクリックし、左矢印を展開して、証明書に関連付けられた秘密鍵が含まれていることを確認します。
4. 証明書を PCKS #12 (.pfx) 証明書としてエクスポートするには、証明書と秘密鍵を選択し、右クリックして**2 項目を書き出す**を選択します。
5. Citrix Endpoint Management で使用する証明書ファイルに一意の名前を付けます。名前にスペースを含めないでください。次に、保存する証明書のフォルダーの場所を選択し、.pfx ファイル形式を選択して、**保存**をクリックします。
6. 証明書をエクスポートするためのパスワードを入力します。Citrix では、一意の強力なパスワードを使用することをお勧めします。また、後で使用および参照できるように、証明書とパスワードを安全に保管してください。
7. キーチェーンアクセスアプリは、ログインパスワードまたは選択したキーチェーンのパスワードを要求します。パスワードを入力し、**OK**をクリックします。保存された証明書は、Citrix Endpoint Management サーバーで使用する準備ができました。
8. 続行するには、「Citrix Endpoint Management への APNs 証明書のインポート」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft IIS を使用して PKCS #12 ファイルを作成する

重要:

このタスクには、CSRの生成に使用したのと同じIISサーバーを使用してください。

1. Microsoft IISを開きます。
2. **サーバー証明書**アイコンをクリックします。
3. **サーバー証明書**ウィンドウで、**証明書要求の完了**をクリックします。
4. Appleから提供されたCertificate.pemファイルを参照します。次に、フレンドリ名または証明書名を入力し、**OK**をクリックします。名前にスペースを含めないでください。
5. 手順4で特定した証明書を選択し、**エクスポート**をクリックします。
6. .pfx証明書の場所とファイル名、およびパスワードを指定し、**OK**をクリックします。

   Citrix Endpoint Managementに証明書をインポートするには、そのパスワードが必要です。
7. .pfx証明書を、Citrix Endpoint Managementをインストールする予定のサーバーにコピーします。
8. 続行するには、Citrix Endpoint ManagementへのAPNs証明書のインポートを参照してください。

OpenSSLを使用してPKCS #12ファイルを作成する

OpenSSLを使用してCSRを作成した場合、OpenSSLを使用して.pfx APNs証明書を作成することもできます。

1. コマンドプロンプトまたはシェルで、次のコマンドを実行します。
   `Customer.privatekey.pem`はCSRからの秘密鍵です。`APNs_Certificate.pem`はAppleから受け取ったばかりの証明書です。

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey
   Customer.privatekey.pem -out apns_identity.pfx
   ```
2. .pfx 証明書ファイルのパスワードを入力します。このパスワードは、Citrix Endpoint Management に証明書をアップロードする際に再度使用するため、覚えておいてください。
3. .pfx 証明書ファイルの場所をメモします。その後、コンソールを使用してファイルをアップロードできるように、Citrix Endpoint Management サーバーにファイルをコピーします。
4. 続行するには、次のセクションで説明されているように、APNs 証明書を Citrix Endpoint Management にインポートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APNs 証明書を Citrix Endpoint Management にインポートする

新しい APNs 証明書を受け取ったら、APNs 証明書を Citrix Endpoint Management にインポートして、初めて証明書を追加するか、既存の証明書を置き換えます。

1. Citrix Endpoint Management コンソールで、**Settings > Certificates** に移動します。
2. **Import > Keystore** をクリックします。
3. **Use as** から **APNs** を選択します。
4. コンピューター上の .pfx または .p12 ファイルを参照します。
5. パスワードを入力し、**Import** をクリックします。

Citrix Endpoint Management の証明書の詳細については、証明書と認証 を参照してください。

APNs 証明書を更新する

重要:

更新プロセスで別の Apple ID を使用する場合、ユーザーデバイスを再登録する必要があります。

APNs 証明書を更新するには、証明書を作成する手順を実行し、Apple Push Certificates Portal にアクセスします。そのポータルを使用して新しい証明書をアップロードします。ログイン後、既存の証明書または以前の Apple Developers アカウントからインポートされた証明書が表示されます。

Certificates Portal で、証明書を更新する際の唯一の違いは、**Renew** をクリックすることです。サイトにアクセスするには、Certificates Portal の開発者アカウントが必要です。証明書を更新するには、同じ組織名と Apple ID を使用してください。

APNs 証明書の有効期限を確認するには、Citrix Endpoint Management コンソールで、**Settings > Certificates** に移動します。証明書の有効期限が切れても、失効させないでください。

1. Microsoft IIS、キーチェーンアクセス (macOS)、または OpenSSL を使用して CSR を生成します。CSR の生成の詳細については、「証明書署名要求の作成」を参照してください。
2. ブラウザで Citrix Endpoint Management Tools にアクセスします。次に、**Request push notification certificate signature** をクリックします。
3. **+ Upload the CSR** をクリックします。
4. ダイアログボックスで CSR に移動し、**Open** をクリックしてから **Sign** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. `.plist` ファイルを受け取ったら、保存します。
6. ステップ 3 のタイトルで、**Apple Push Certificates Portal** をクリックしてサインオンします。
7. 更新する証明書を選択し、**Renew** をクリックします。
8. `.plist` ファイルをアップロードします。出力として .pem ファイルが生成されます。.pem ファイルを保存します。
9. その .pem ファイルを使用して、CSR を完了します (ステップ 1 で CSR を作成した方法に従って)。
10. 証明書を .pfx ファイルとしてエクスポートします。

Citrix Endpoint Management コンソールで、.pfx ファイルをインポートし、次のように構成を完了します。

1. **Settings > Certificates > Import** に移動します。
2. **Import menu** から、**Keystore** を選択します。
3. 「**キーストアタイプ**」メニューから「**PKCS #12**」を選択します。
4. 「**用途**」から「**APNs**」を選択します。

   証明書のインポートダイアログボックス(/en-us/citrix-endpoint-management/media/import-apns-certificate.png)
5. 「**キーストアファイル**」については、「**参照**」をクリックしてファイルに移動します。
6. 「**パスワード**」に証明書のパスワードを入力します。
7. オプションの「**説明**」を入力します。
8. 「**インポート**」をクリックします。

Citrix Endpoint Managementにより、「**証明書**」ページに戻ります。「**名前**」、「**ステータス**」、「**有効期間開始**」、および「**有効期間終了**」の各フィールドが更新されます。

Citrix Filesとのシングルサインオンのための SAML

免責事項:

ShareFile (現 Progress) がサポートを中止した場合、この機能は非推奨になります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint ManagementとShareFileを構成して、Security Assertion Markup Language (SAML) を使用し、Citrix Filesモバイルアプリへのシングルサインオン (SSO) アクセスを提供できます。この機能には以下が含まれます。

- MAM SDKが有効になっている、またはMDX Toolkitを使用してラップされているCitrix Filesアプリ
- ラップされていないCitrix Filesクライアント (Webサイト、Outlookプラグイン、同期クライアントなど)
- **ラップされたCitrix Filesアプリの場合:** Citrix Filesにログオンするユーザーは、ユーザー認証とSAMLトークンの取得のためにCitrix Secure Hubにリダイレクトされます。認証が成功すると、Citrix FilesモバイルアプリはSAMLトークンをShareFileに送信します。初回ログオン後、ユーザーはSSOを介してCitrix Filesモバイルアプリにアクセスできます。また、毎回ログオンすることなく、ShareFileからCitrix Secure Mailメールにドキュメントを添付することもできます。
- **ラップされていないCitrix Filesクライアントの場合:** Webブラウザーまたはその他のCitrix Filesクライアントを使用してCitrix Filesにログオンするユーザーは、Citrix Endpoint Managementにリダイレクトされます。Citrix Endpoint Managementはユーザーを認証し、その後、ShareFileに送信されるSAMLトークンを取得します。初回ログオン後、ユーザーは毎回ログオンすることなく、SSOを介してCitrix Filesクライアントにアクセスできます。

Citrix Endpoint ManagementをShareFileへのSAML IDプロバイダー (IdP) として使用するには、この記事で説明されているように、Citrix Endpoint Managementをエンタープライズアカウントで使用するように構成する必要があります。または、Citrix Endpoint Managementをストレージゾーンコネクタのみで動作するように構成することもできます。詳細については、「ShareFile use with Citrix Endpoint Management」を参照してください。

詳細なリファレンスアーキテクチャ図については、「Architecture」を参照してください。

前提条件

Citrix Endpoint ManagementとCitrix Filesアプリで SSOを構成する前に、次の前提条件を完了してください。

- MAM SDKまたは互換性のあるバージョンのMDX Toolkit (Citrix Filesモバイルアプリ用)。

  詳細については、「Citrix Endpoint Management compatibility」を参照してください。
- 互換性のあるバージョンのCitrix FilesモバイルアプリおよびCitrix Secure Hub。
- ShareFile管理者アカウント。
- Citrix Endpoint ManagementとShareFile間の接続が確認済みであること。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ShareFileアクセスを構成する

ShareFileのSAMLを設定する前に、次のようにShareFileアクセス情報を提供します。

1. Citrix Endpoint Management Webコンソールで、 > の順にクリックします。 構成ページが表示されます。

   ShareFile構成設定(/en-us/citrix-endpoint-management/media/configure-content-collaboration-saml-for-non-mdx-apps.png)

2. 次の設定を構成します。

   - **ドメイン:** ShareFileのサブドメイン名を入力します。例: `example.sharefile.com`。
   - **デリバリーグループに割り当てる:** ShareFileでSSOを使用できるようにするデリバリーグループを選択または検索します。
   - **ShareFile管理者アカウントのログオン**
   - **ユーザー名:** ShareFile管理者ユーザー名を入力します。このユーザーは管理者権限を持っている必要があります。
   - **パスワード:** ShareFile管理者パスワードを入力します。
   - **ユーザーアカウントのプロビジョニング:** この設定は無効のままにします。ユーザープロビジョニングにはShareFileユーザー管理ツールを使用します。「ユーザーアカウントと配布グループのプロビジョニング」を参照してください。

3. をクリックして、ShareFile管理者アカウントのユーザー名とパスワードが指定されたShareFileアカウントに対して認証されることを確認します。
4. をクリックします。

   - Citrix Endpoint Management は ShareFile と同期し、ShareFile の設定である **ShareFile Issuer/Entity ID** および **Login URL** を更新します。
   - **>** ページに が表示されます。その名前は、 で後述する手順を完了するために必要です。

ラップされた Citrix Files MDX アプリの SAML を設定する

MAM SDK で準備された Citrix Files アプリでは、シングルサインオン構成に NetScaler Gateway を使用する必要はありません。Webサイト、Outlookプラグイン、同期クライアントなどのラップされていないCitrix Filesクライアントのアクセスを構成するには、「他のCitrix Filesクライアント向けNetScaler Gatewayの構成」を参照してください。

ラップされた Citrix Files MDX アプリの SAML を構成するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Citrix Endpoint Management クライアント用の ShareFile をダウンロードします。「ShareFile ツール/アプリのダウンロード」を参照してください。
2. MAM SDK を使用して Citrix Files モバイルアプリを準備します。詳細については、「MAM SDKの概要」を参照してください。
3. Citrix Endpoint Management コンソールで、準備した Citrix Files モバイルアプリをアップロードします。MDXアプリのアップロードについては、「Citrix Endpoint ManagementにMDXアプリを追加するには」を参照してください。
4. SAML設定を確認します。以前に構成した管理者ユーザー名とパスワードを使用してShareFileにログオンします。
5. ShareFileとCitrix Endpoint Managementが同じタイムゾーンに構成されていることを確認します。Citrix Endpoint Managementが構成されたタイムゾーンの正しい時刻を表示していることを確認します。そうでない場合、SSOが失敗する可能性があります。

Citrix Filesモバイルアプリを検証する

1. ユーザーデバイスで、Citrix Secure Hubをインストールして構成します。
2. アプリストアから、Citrix Filesモバイルアプリをダウンロードしてインストールします。
3. Citrix Filesモバイルアプリを起動します。Citrix Filesは、ユーザー名やパスワードの入力を求めずに起動します。

Citrix Secure Mailで検証する

1. ユーザーデバイスで、まだ行っていない場合は、Citrix Secure Hubをインストールして構成します。
2. アプリストアからCitrix Secure Mailをダウンロード、インストール、セットアップします。
3. 新しいメールフォームを開き、**ShareFileから添付**をタップします。メールに添付できるファイルが、ユーザー名やパスワードを要求されることなく表示されます。

その他のCitrix Filesクライアント向けにNetScaler Gatewayを構成する

Webサイト、Outlookプラグイン、同期クライアントなど、ラップされていないCitrix Filesクライアントのアクセスを構成するには、Citrix Endpoint ManagementをSAML IDプロバイダーとして使用できるようにNetScaler Gatewayを次のように構成します。

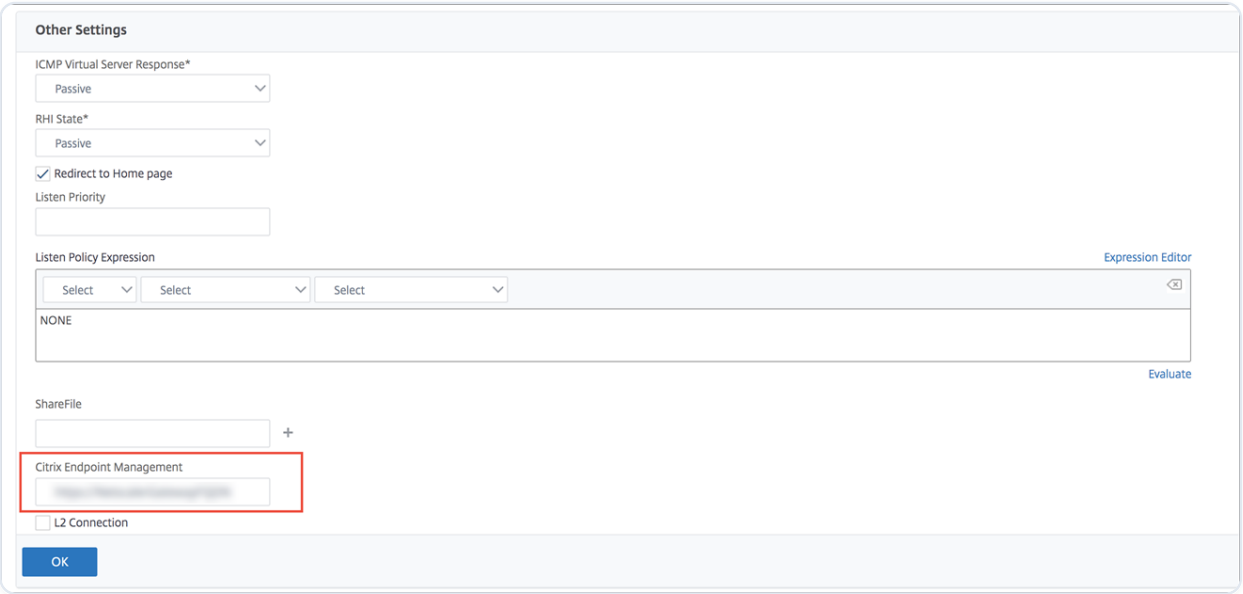
- ホームページのリダイレクトを無効にする。
- Citrix Filesセッションポリシーとプロファイルを作成します。
- NetScaler Gateway仮想サーバーでポリシーを構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ホームページのリダイレクトを無効にする

/cginfraパスを介して行われる要求のデフォルトの動作を無効にします。この操作により、ユーザーは構成されたホームページではなく、最初に要求された内部URLを表示できるようになります。

1. Citrix Endpoint Managementログオンに使用されるNetScaler Gateway仮想サーバーの設定を編集します。NetScaler Gatewayで、**Other Settings**に移動し、**Redirect to Home Page**というラベルのチェックボックスをオフにします。



2. **ShareFile**（現在はShareFileと呼ばれています）の下で、Citrix Endpoint Managementの内部サーバー名とポート番号を入力します。
3. **Citrix Endpoint Management**の下で、Citrix Endpoint ManagementのURLを入力します。

   この構成により、/cginfraパスを介して入力したURLへの要求が承認されます。

Citrix Filesセッションポリシーとリクエストプロファイルの作成

Citrix Filesセッションポリシーとリクエストプロファイルを作成するには、次の設定を構成します。

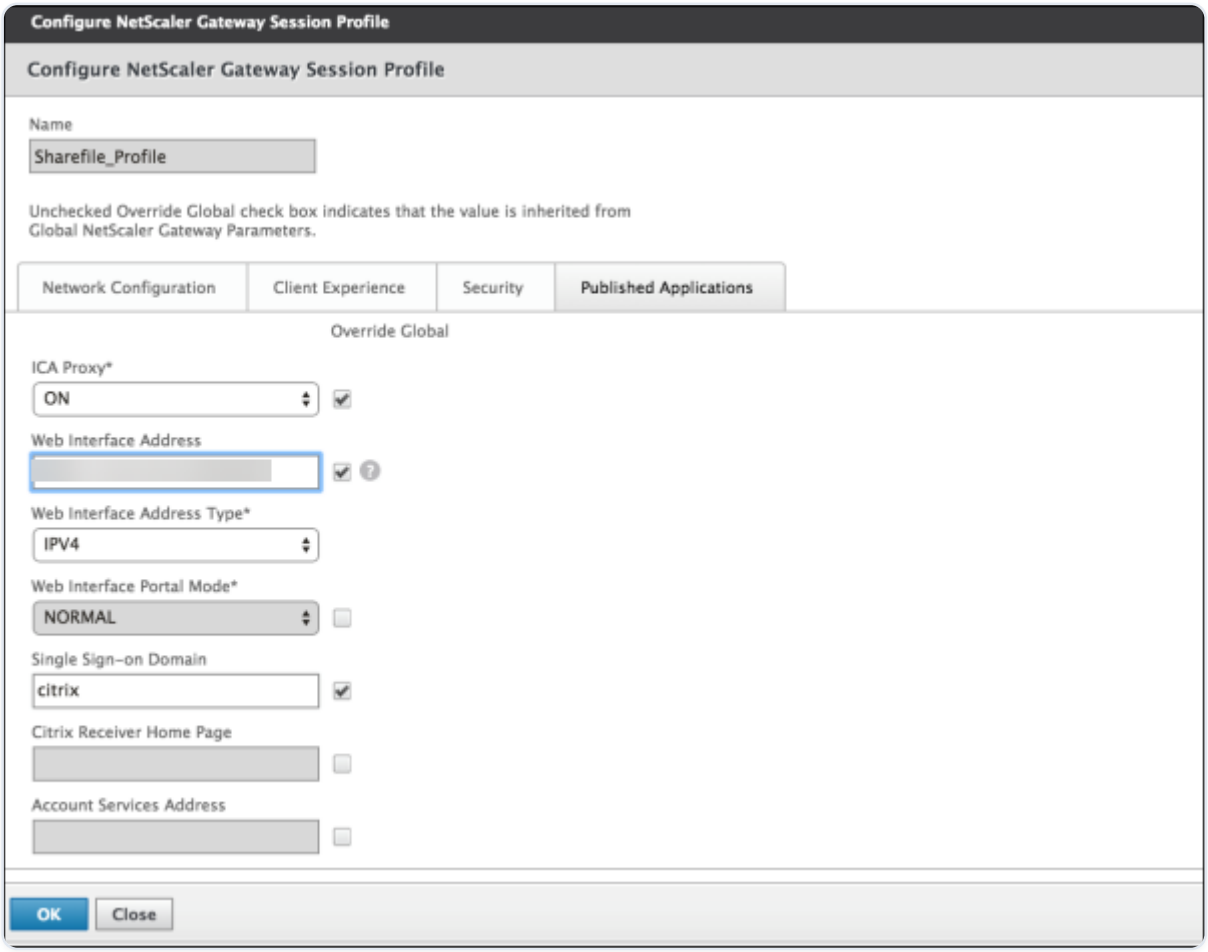
1. NetScaler Gateway構成ユーティリティで、左側のナビゲーションペインにある **NetScaler Gateway > Policies > Session** をクリックします。
2. セッションポリシーを作成します。**Policies** タブで、**Add** をクリックします。
3. 「**名前**」フィールドに「**ShareFile_Policy**」と入力します。
4. **+** ボタンをクリックしてアクションを作成します。**Create NetScaler® Gateway Session Profile** ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gatewayセッションプロファイル画面(/en-us/citrix-endpoint-management/media/configure-sharefile-ns-session-policy.png)

次の設定を構成します。

- **名前:** 「**ShareFile_Profile**」と入力します。
- **Client Experience** タブをクリックし、次の設定を構成します。
  - **ホームページ:** 「**none**」と入力します。
  - **セッションタイムアウト (分):** 「**1**」と入力します。
  - **Webアプリケーションへのシングルサインオン:** この設定を選択します。
  - **資格情報インデックス: PRIMARY** をクリックします。
- **Published Applications** タブをクリックします。



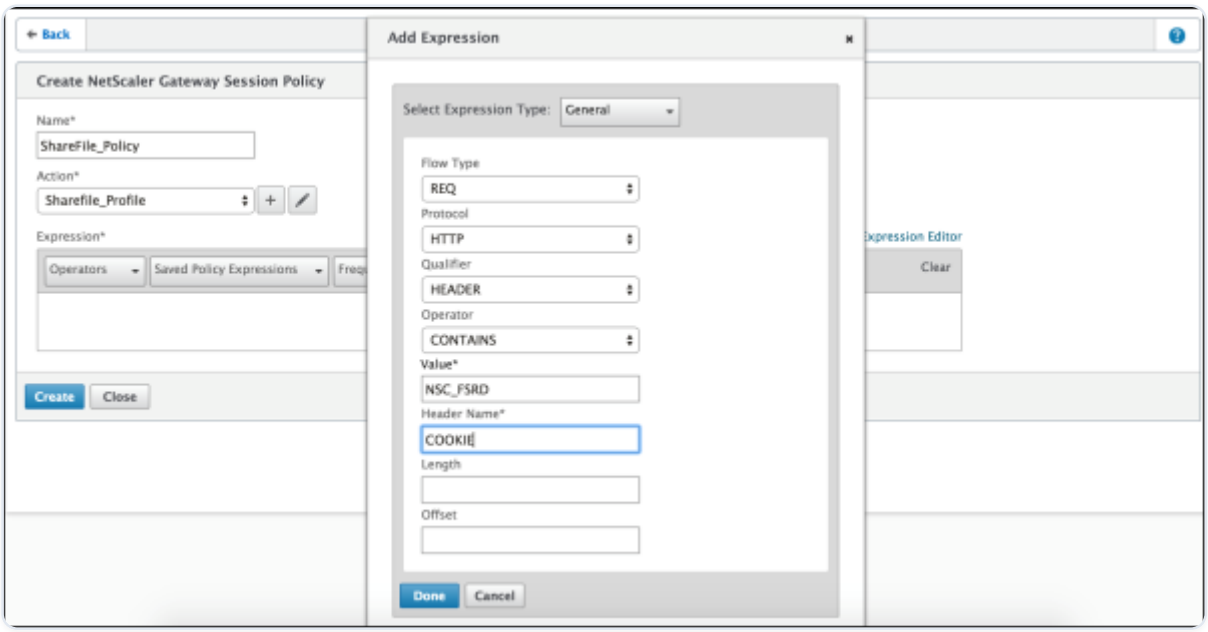
次の設定を構成します。

- **ICA® Proxy: オン**をクリックします。
- **Web Interface Address:** Citrix Endpoint ManagementサーバーのURLを入力します。
- **Single Sign-on Domain:** Active Directoryドメイン名を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gatewayセッションプロファイルを構成する際、**Single Sign-on Domain**のドメインサフィックスは、LDAPで定義されているCitrix Endpoint Managementドメインエイリアスと一致している必要があります。

5. **作成**をクリックして、セッションプロファイルを定義します。
6. **式エディター**をクリックします。



次の設定を構成します。

- **値: NSC_FSRD**と入力します。
- **ヘッダー名: COOKIE**と入力します。

7. **作成**をクリックし、次に**閉じる**をクリックします。

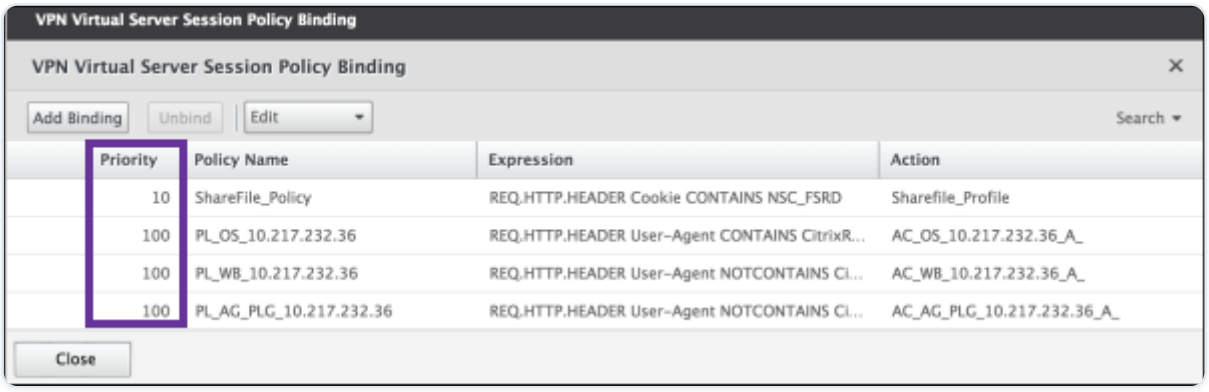


NetScaler Gateway仮想サーバーでポリシーを構成する

NetScaler Gateway仮想サーバーでこれらの設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Gateway構成ユーティリティの左側のナビゲーションペインで、**NetScaler Gateway > Virtual Servers**をクリックします。
2. **詳細**ペインで、NetScaler Gateway仮想サーバーをクリックします。
3. **編集**をクリックします。
4. **構成済みポリシー > セッションポリシー**をクリックし、**バインドの追加**をクリックします。
5. **ShareFile_Policy**を選択します。
6. 選択したポリシーの自動生成された**優先度**番号を編集して、リストされている他のポリシーと比較して最も高い優先度（最小の番号）を持つようにします。例：



7. **完了**をクリックし、実行中のNetScaler Gateway構成を保存します。

Citrix Files.com SSO設定を変更する

MDXおよび非MDXのCitrix Filesアプリの両方について、以下の変更を行います。

重要：

内部アプリケーション名に新しい番号が追加されます。

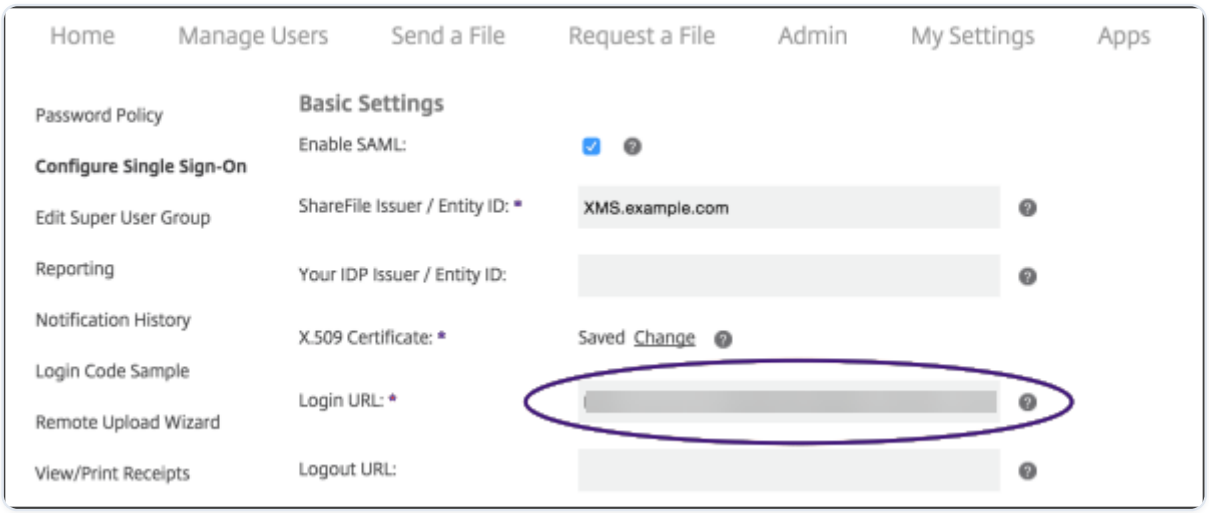
- Citrix Filesアプリを編集または再作成するたびに
- Citrix Endpoint ManagementでShareFile設定を変更するたびに

その結果、更新されたアプリ名を表示するために、Citrix Filesウェブサイトのログイン URLも更新する必要があります。

1. ShareFile管理者としてShareFileアカウント（`https://<subdomain>.sharefile.com`）にログオンします。
2. ShareFile Webインターフェイスで、**Admin** をクリックし、**Configure Single Sign-on** を選択します。
3. **ログインURL** を次のように編集します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

編集前の**ログインURL**の例を次に示します: `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`。



- NetScaler Gateway仮想サーバーの外部FQDNと **/cginfra/https/** をCitrix Endpoint ManagementサーバーのFQDNの前に挿入し、Citrix Endpoint Management FQDNの後に **8443** を追加します。

  編集されたURLの例を次に示します: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

- パラメーター `&app=ShareFile_SAML_SP` を内部のCitrix Filesアプリケーション名に変更します。内部名はデフォルトで `ShareFile_SAML` です。ただし、構成を変更するたびに、内部名に番号が追加されます (`ShareFile_SAML_2`、`ShareFile_SAML_3` など)。**App internal name** は、**Configure > ShareFile** ページで確認できます。

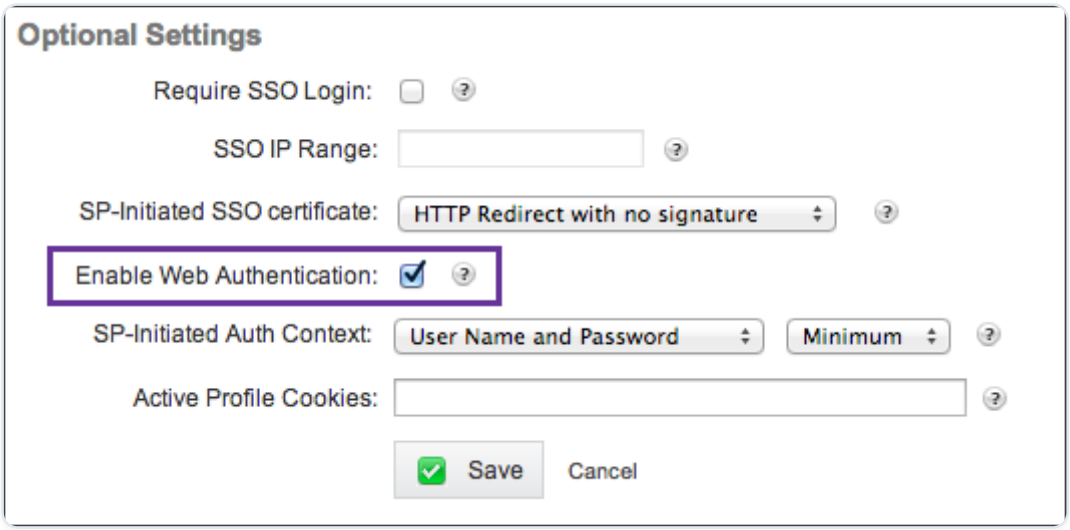
  編集されたURLの例を次に示します: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- URLの末尾に `&nssso=true` を追加します。

  最終的なURLの例を次に示します: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`。

4. **Optional Settings** で、**Enable Web Authentication** チェックボックスをオンにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



構成を検証する

構成を検証するには、次の手順を実行します。

1. ブラウザで `https://<subdomain>sharefile.com/saml/login` にアクセスします。

   NetScaler Gatewayのログオンフォームにリダイレクトされます。リダイレクトされない場合は、前述の構成設定を確認してください。

2. 構成したNetScaler GatewayおよびCitrix Endpoint Management環境のユーザー名とパスワードを入力します。

   `<subdomain>.sharefile.com` にあるCitrix Filesフォルダーが表示されます。Citrix Filesフォルダーが表示されない場合は、適切なログオン資格情報を入力したことを確認してください。

Citrix Cloud を介した Azure Active Directory による認証

Citrix Endpoint Management は、Citrix Cloud を介した Azure Active Directory (Azure AD) 資格情報による認証をサポートしています。この認証方法は、Citrix Secure Hub を介して MDM に登録するユーザーのみが利用できます。

MDM+MAM で Citrix Secure Hub を使用するには、MAM 登録に NetScaler Gateway を使用するように Citrix Endpoint Management を構成します。詳細については、「NetScaler Gateway and Citrix Endpoint Management」を参照してください。

Citrix Endpoint Management は、Citrix Cloud サービスである Citrix Identity を使用して Azure Active Directory とフェデレーションします。Citrix は、Azure Active Directory への直接接続ではなく、Citrix Identity プロバイダーを使用することをお勧めします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management は、以下のプラットフォームで Azure AD による認証をサポートしています。

- Apple Business Manager または Apple School Manager に登録されていない iOS および macOS デバイス
- Apple Business Manager に登録されている iOS および macOS デバイス
- Android Enterprise デバイス (プレビュー) (BYOD および完全管理モードの場合)

Citrix Cloud を介した Azure AD による認証には、以下の制限があります。

- Citrix Endpoint Management のローカルアカウントでは利用できません。
- 登録招待状に対する Azure AD を介した認証はサポートされていません。登録 URL を含む登録招待状をユーザーに送信した場合、ユーザーは Azure AD ではなく LDAP を介して認証されます。

前提条件

注:

Azure Active Directory Standalone はサポートされていません。Citrix Endpoint Management との統合には、オンプレミスの Active Directory が必要です。

- Azure Active Directory ユーザー資格情報。
- Active Directory のユーザーグループは、Azure Active Directory のユーザーグループと一致する必要があります。
- Active Directory のユーザー名とメールアドレスは、Azure Active Directory のユーザー名とメールアドレスと一致する必要があります。
- ディレクトリサービス同期のためにCitrix Cloud Connectorがインストールされているアカウント。
- NetScaler Gateway。Citrixでは、完全なシングルサインオンエクスペリエンスのために、証明書ベースの認証またはAzure ADを有効にすることをお勧めします。MAM登録のために NetScaler GatewayでLDAP認証を使用する場合、エンドユーザーは登録中に二重認証プロンプトを経験します。詳細については、「クライアント証明書または証明書とドメイン認証」を参照してください。
- Android Enterprise の登録プロファイルで、**Allow users to decline device management** を **Off** に設定します。ユーザーがデバイス管理を拒否した場合、IDプロバイダーを使用して認証

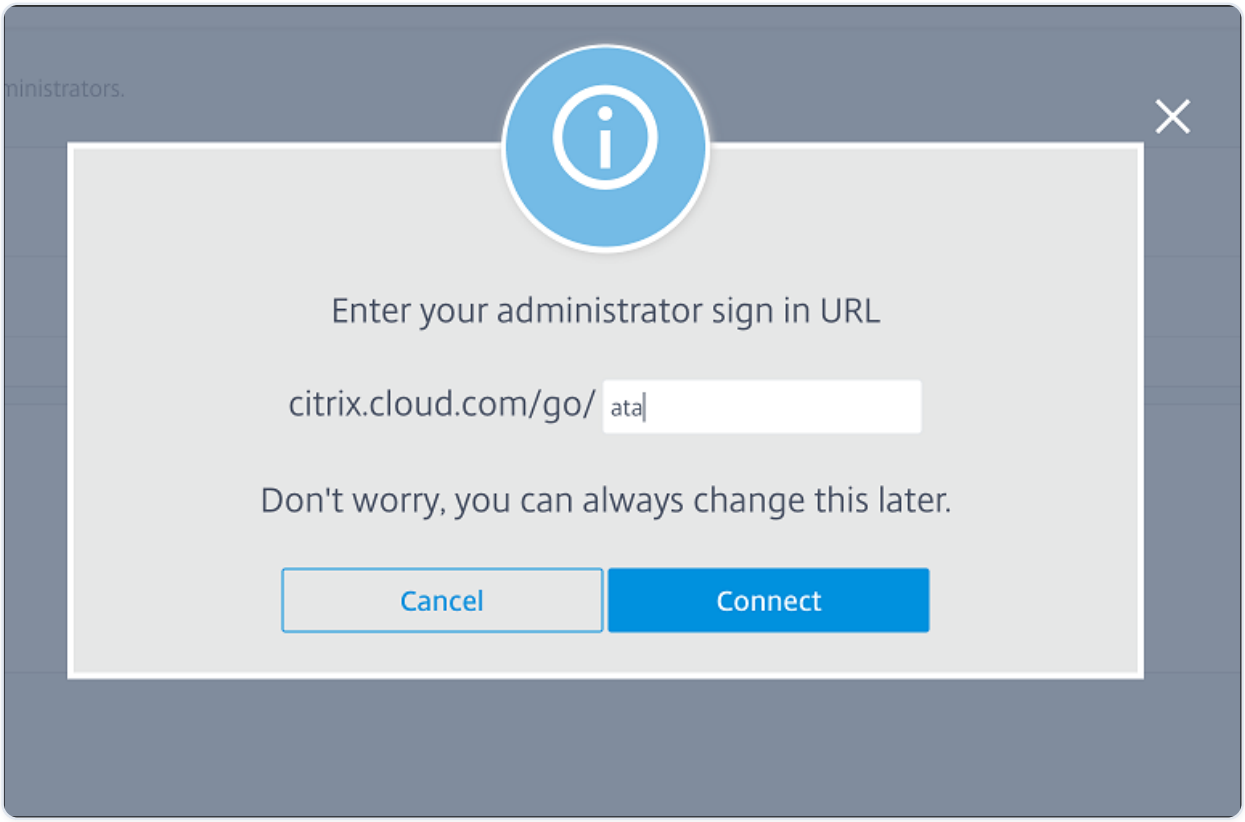
© 1997–2026 Citrix Systems, Inc. All rights reserved.

し、登録することはできません。詳細については、「登録セキュリティ」を参照してください。

IDプロバイダーとしてAzure Active Directoryを使用するようにCitrix Cloudを構成する

Citrix Secure Hub でこのサービスを使用するように設定するには、Citrix Cloud で Azure Active Directory を構成します。

1. https://citrix.cloud.com にアクセスし、Citrix Cloud アカウントにサインインします。
2. Citrix Cloud メニューから、**IDおよびアクセス管理**ページに移動し、Azure Active Directory に接続します。
3. 管理者サインインURLを入力し、**接続**をクリックします。



4. サインイン後、Azure Active Directory アカウントがCitrix Cloudに接続されます。**IDおよびアクセス管理 > 認証**ページには、Citrix CloudアカウントとAzure ADアカウントにサインインするために使用するアカウントが表示されます。
5. Citrix Secure Hub を介して登録するユーザー向けに Azure AD を使用した認証を有効にするには、**ワークスペース構成 > 認証**で、**Azure Active Directory**を選択します。構成が完了すると、Citrix Secure Hub を介してユーザーデバイスを登録できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management の IdP タイプとして Citrix ID を構成する

この構成は、Citrix Secure Hub を介して登録するユーザーにのみ適用されます。Citrix Cloud で Azure Active Directory を構成した後、Citrix Endpoint Management を次のように構成します。

1. Citrix Endpoint Management コンソールで、**Settings > Identity Provider (IDP)** に移動し、**Add** をクリックします。
2. **Identity Provider (IDP)** ページで、以下を構成します。
   - **IDP Name:** 作成するIdP接続を識別するための一意の名前を入力します。
   - **IDP Type: Citrix Identity Platform** を選択します。
   - **Authentication Domain: Azure Active Directory** を選択します。このドメインは、Citrix Cloud の **Workspace Configuration > Authentication** ページにあるIDプロバイダーのドメインに対応します。
3. **Next** をクリックします。**IDP Claims Usage** ページで、以下を構成します。
   - **User Identifier type:** デフォルトでは、このフィールドは **userPrincipalName** に設定されています。オンプレミスのActive DirectoryとAzure Active Directoryの両方で、すべてのユーザーを同じ識別子で構成していることを確認してください。Citrix Endpoint Management は、この識別子を使用して、IDプロバイダー上のユーザーをオンプレミスのActive Directoryユーザーにマッピングします。
   - **User Identifier string:** このフィールドは自動的に入力されます。
4. **Next** をクリックし、**Summary** ページを確認してから、**Save** をクリックします。

   Citrix Secure Hubユーザー、Citrix Endpoint Managementコンソール、およびセルフヘルプポータルユーザーは、Azure Active Directoryの資格情報でサインインできるようになりました。ドメイン参加しているCitrix Secure Hubユーザーは、Citrix Secure Hubを使用してAzure ADの資格情報でサインインできます。Citrix Secure Hubは、MAMデバイスにクライアント証明書認証を使用します。

Citrix Secure Hubの認証フロー

Citrix Endpoint Managementは、Citrix Secure Hubを介して登録されたデバイスで、Azure ADをIdPとしてユーザーを認証するために、以下のフローを使用します。

1. ユーザーがCitrix Secure Hubを起動します。
2. Citrix Secure Hubは認証要求をCitrix Identityに渡し、Citrix Identityはその要求をAzure Active Directoryに渡します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ユーザーはAzure Active Directoryのユーザー名とパスワードを入力します。
4. Azure Active Directory はユーザーを検証し、Citrix Identity にコードを送信します。
5. Citrix Identity はコードを Citrix Secure Hub に送信し、Citrix Secure Hub はそのコードを Citrix Endpoint Management サーバーに送信します。
6. Citrix Endpoint Management は、コードとシークレットを使用して ID トークンを取得し、ID トークン内のユーザー情報を検証します。Citrix Endpoint Management はセッション ID を返します。

Azure Active Directory グループベースの管理による認証

Citrix Endpoint Management は、Azure Active Directory (AAD) を介したサービスへのアクセスに対して、グループベースの ID 認証をサポートするようになりました。この更新により、管理者は AAD グループメンバーシップを使用してグループレベルでアクセスを管理できるようになり、柔軟性とセキュリティが強化されます。従来の Citrix Identity ログインメカニズムは、代替手段として引き続き利用可能です。

主な機能強化

- **Azure AD グループ統合**: 管理者は、Azure AD グループを活用して CEM サービスへのユーザーアクセスを管理できるようになりました。これにより、権限管理が簡素化され、グループベースのアクセス制御が可能になります。
- **Azure AD グループを使用した Citrix Endpoint Management ログイン認証**: ユーザーは Azure AD グループを介して認証できるため、既存の組織の ID インフラストラクチャとシームレスに統合できます。
- **従来の Citrix Identity のサポート**: Citrix Identity ログインは引き続き利用可能であり、ユーザーは自分のペースで移行できます。

機能フラグ

- **Citrix Cloud™ 機能フラグ**: `fullAccessGroups` – この機能は、グループへのフルアクセスを許可するためにデフォルトで有効になっています。
- **Citrix Endpoint Management 機能フラグ**: `cc.group.based.admin` – Citrix Endpoint Management でグループベースの管理機能を有効にします。

前提条件

- Azure AD が Citrix Cloud ポータルで構成されていること。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Cloud の管理者サインイン URL が、Azure AD グループを介して Citrix Endpoint Management にアクセスするために設定されている必要があること。

構成手順

1. Azure Portal にログインし、Azure Active Directory にアクセスします。
2. ユーザーに移動し、新しいユーザーの作成を選択します。
3. 「グループ」に移動し、「新しいグループ」をクリックして、新しく作成したユーザーをこのグループのメンバーとして追加します。
4. 管理者資格情報を使用してCitrix Cloudにサインインします。
5. 「IDとアクセス管理」に移動し、新しいAzure ADグループにフルアクセス権またはカスタム権限を割り当てます。
6. Azure ADグループのユーザーは、管理者サインインURLを使用してCitrix Endpoint Management™にログインできるようになりました。

MAM登録のためのNetScaler Gateway経由のAzure Active Directory認証

Citrix Endpoint Management は、NetScaler Gateway を介した Azure Active Directory (Azure AD) 資格情報による認証をサポートしています。この認証方法は、Citrix Secure Hub を介して MAM に登録するユーザーのみが利用できます。

前提条件

MAM に登録されたデバイスの ID プロバイダー (IdP) として、NetScaler Gateway を介して Azure AD を使用するように Citrix Endpoint Management を構成するには、次の前提条件が満たされていることを確認してください。

- MDM に登録されたデバイスの IdP として、Citrix Cloud を介して Azure AD を使用するように Citrix Endpoint Management を構成します。MDM 用の Azure AD の構成の詳細については、「Citrix Cloud を介した Azure Active Directory 認証」を参照してください。
- Azure AD を Citrix Cloud に接続します。詳細については、「Azure Active Directory を Citrix Cloud に接続する」を参照してください。
- プラットフォームに応じて、次の関連する機能フラグをそれぞれ有効にします。
    - iOS:
        - iOS-V3フォーム-MAM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- iOS-SAML認証-MAM

- アンドロイド:

  - アンドロイド-V3Form-MAM
  - アンドロイド-SAML認証-MAM

> **注:**
>
> この機能を有効にするには、サポートチームにお問い合わせください。

- Androidの場合、**Android Enterprise**を有効にします。

> **注:**
>
> この機能は、従来のAndroidデバイス管理者（DA）モードではテストまたは検証されていません。このモードはサポートされていません。

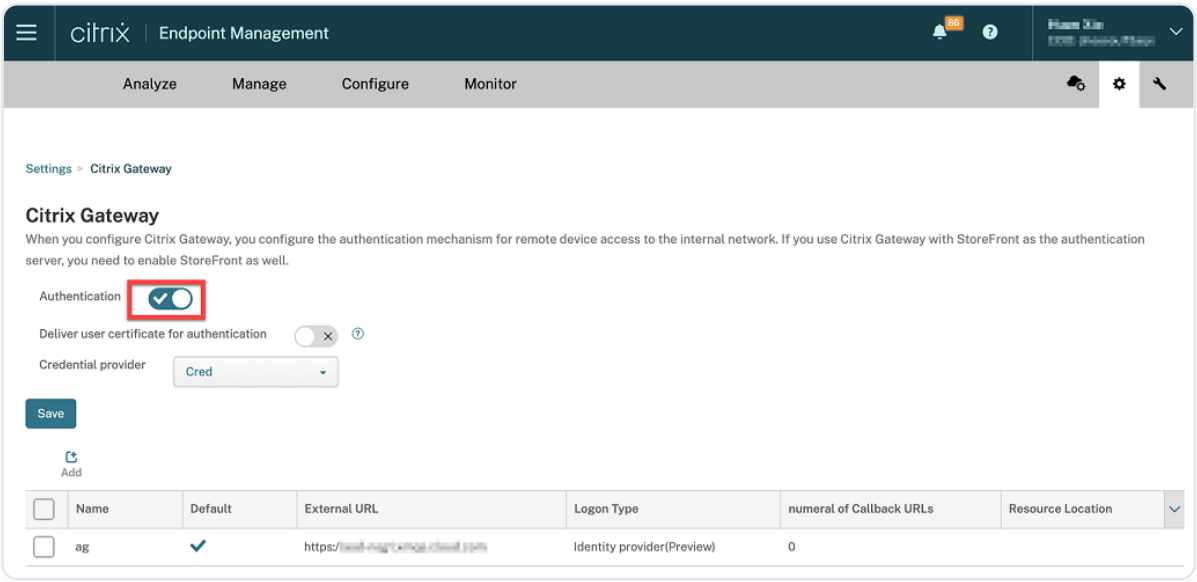
MAMのIdPとしてAzure ADを構成する

1. Citrix Endpoint ManagementでNetScaler Gatewayを次のように構成します。

   a. Citrix Endpoint Managementコンソールにサインインし、**設定**
   
   アイコンをクリックします。

   b. **サーバー**の下にある**NetScaler Gateway**をクリックします。

   c. **認証**トグルボタンを有効にします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. ゲートウェイの**ログオンタイプ**が*IDプロバイダー*であることを確認します。

e. **保存**をクリックします。

2. Configure Azure AD as a SAML IdP を使用して、Azure ADをSAML IdPとして構成します。
3. Configure NetScaler ADC as SAML service provider (SP) を使用して、高度なポリシーを使用してNetScaler ADCをSAML SPとして構成します。
4. To set up an authentication virtual server by using the GUI を使用して、AAA仮想サーバーを作成します。
5. Configure the authentication virtual server を使用して、AAA仮想サーバーを構成します。
6. 認証プロファイルを使用して、認証プロファイルを作成および構成します。
7. 認証プロファイルをGateway仮想サーバーにバインドし、すべての構成を保存します。

これで、MAMに登録されたデバイスのIDプロバイダーとしてAzure ADが追加され、Azure ADを使用してそれらを認証できるようになります。

予期される動作

次の例では、Androidデバイスを使用しています。

1. モバイルデバイスで、Citrix Secure Hubアプリを開きます。

   Citrix Secure Hubアプリのアイコン(/en-us/citrix-endpoint-management/media/secure-hub-app-icon.png)

2. 必要な権限を付与します。
3. サインインページで、組織から提供された資格情報を入力し、**次へ**をタップします。

   Citrix Secure Hubサインインページ(/en-us/citrix-endpoint-management/media/secure-hub-sign-in.png)

   Microsoftサインインページにリダイレクトされます。

4. Microsoftサインインページで、メールIDを入力し、**次へ**をタップします。

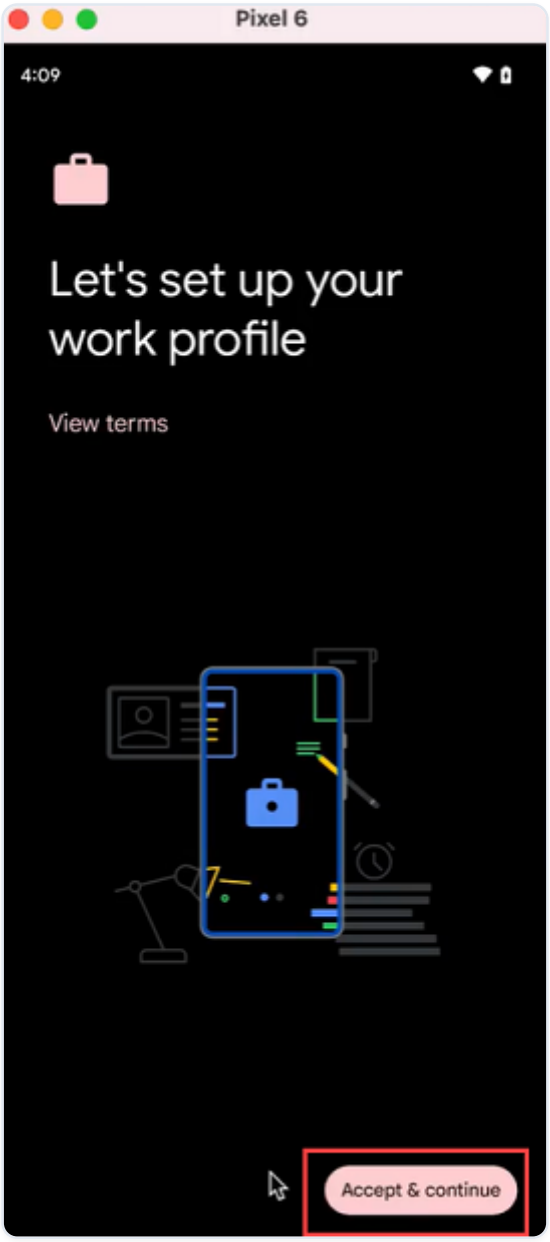
   Microsoftサインインページ - メールID(/en-us/citrix-endpoint-management/media/mam-authentication-microsoft-sign-in-username.png)

5. パスワードを入力し、**サインイン**をタップします。

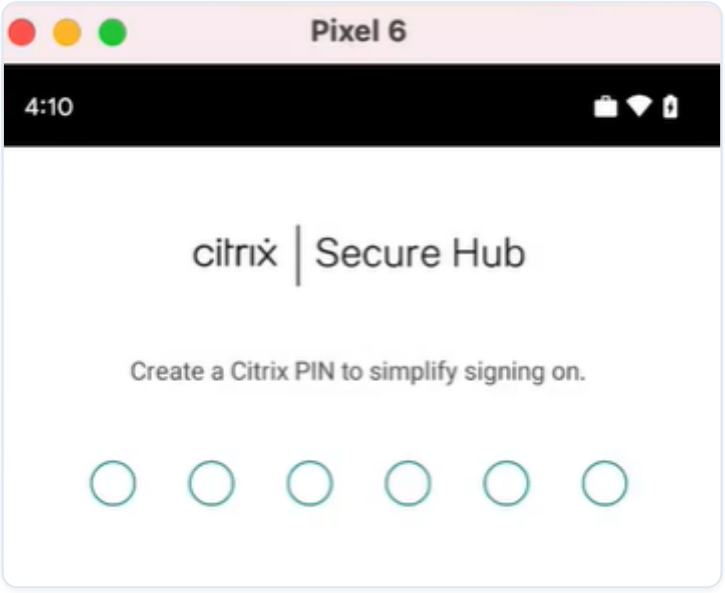
   Microsoftサインインページ - パスワード(/en-us/citrix-endpoint-management/media/mam-authentication-microsoft-sign-in-password.png)

6. **仕事用プロファイルを設定しましょう**ページで、**同意して続行**をタップします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. Citrix Secure HubアプリのPINを作成し、確認します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Hubのホームページに正常にリダイレクトされます。

Citrix Cloud を介した Okta との認証

Citrix Endpoint Management は、Citrix Cloud を介した Okta 資格情報による認証をサポートしています。この認証方法は、Citrix Secure Hub を介して MDM に登録するユーザーのみが利用できます。

MAM に登録するデバイスは、Citrix Cloud を介して Okta 資格情報を使用して認証できません。MDM+MAM で Citrix Secure Hub を使用するには、MAM 登録に NetScaler Gateway を使用するように Citrix Endpoint Management を構成します。詳細については、NetScaler Gateway と Citrix Endpoint Management を参照してください。

Citrix Endpoint Management は、Citrix Cloud サービスである Citrix Identity を使用して Okta とフェデレーションします。Citrix は、Okta への直接接続ではなく、Citrix Identity プロバイダーを使用することをお勧めします。

Citrix Endpoint Management は、以下のプラットフォームでの Okta による認証をサポートしています。

- Apple Business Manager または Apple School Manager に登録されていない iOS および macOS デバイス
- Apple Business Manager に登録されている iOS および macOS デバイス
- Android Enterprise デバイス (プレビュー)、BYOD および完全管理モードの場合

Citrix Cloud を介した Okta による認証には、以下の制限があります。

- Citrix Endpoint Management のローカルアカウントでは利用できません。
- 登録招待状に対する Okta を介した認証はサポートしていません。登録 URL を含む登録招待状をユーザーに送信した場合、ユーザーは Okta ではなく LDAP を介して認証されます。

前提条件

- Okta ユーザー資格情報
- Active Directory のユーザーグループは、Okta のユーザーグループと一致している必要があります。
- Active Directory のユーザー名とメールアドレスは、Okta のユーザー名とメールアドレスと一致している必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ディレクトリサービス同期のためにCitrix Cloud Connectorがインストールされ ているCitrix Cloudアカウント。
- NetScaler Gateway。Citrixでは、完全なシングルサインオンエクスペリエンスのために、証明書ベースの認証を有効にすることをお勧めします。MAM登録にNetScaler GatewayでLDAP認証を使用する場合、エンドユーザーは登録中に二重認証プロンプトを経験します。詳しくは、「クライアント証明書または証明書とドメイン認証」を参照してください。
- Android Enterpriseの登録プロファイルで、**Allow users to decline device management**を**Off**に設定します。ユーザーがデバイス管理を拒否した場合、IDプロバイダーを使用して認証して登録することはできません。詳しくは、「登録セキュリティ」を参照してください。

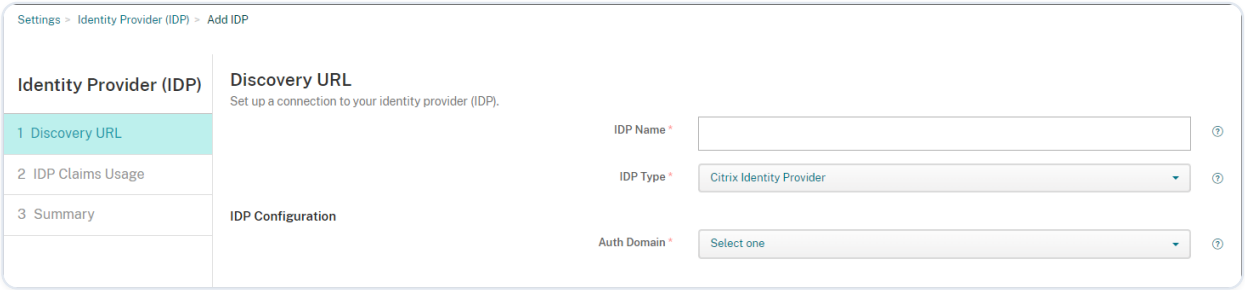
OktaをIDプロバイダーとして使用するようにCitrix Cloudを構成する

Citrix CloudでOktaを構成するには、「OktaをCitrix CloudのIDプロバイダーとして接続する」を参照してください。

Citrix Endpoint ManagementのIdPタイプとしてCitrix IDを構成する

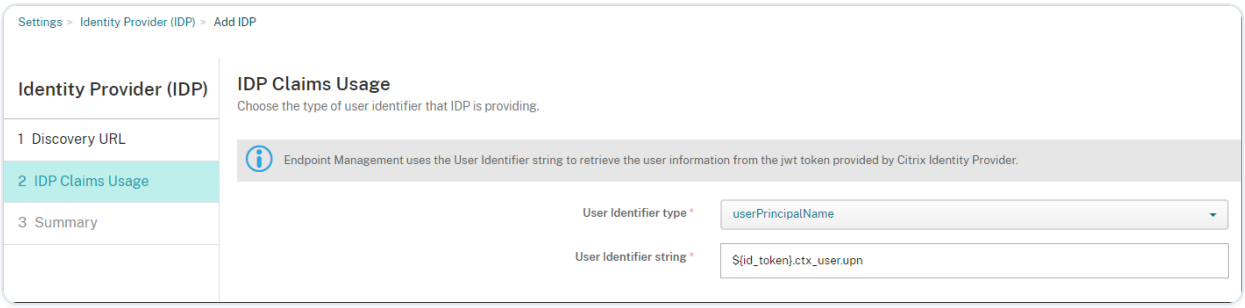
この構成は、Citrix Secure Hubを介して登録するユーザーにのみ適用されます。Citrix CloudでAzure Active Directoryを構成した後、Citrix Endpoint Managementを次のように構成します。

1. Citrix Endpoint Managementコンソールで、**設定 > IDプロバイダー (IDP)** に移動し、**追加** をクリックします。
2. **IDプロバイダー (IDP)** ページで、以下を構成します。



   - **IDP名:** 作成するIdP接続を識別するための一意の名前を入力します。
   - **IDPタイプ: Citrix Identity Provider** を選択します。
   - **認証ドメイン:** Citrix Cloudドメインを選択します。どれを選択すればよいかわからない場合は、Citrix Cloudの**IDおよびアクセス管理 > 認証**ページにドメインが表示されます。
3. **次へ** をクリックします。**IDPクレームの使用** ページで、以下を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **ユーザー識別子の種類:** このフィールドは**userPrincipalName**に設定されています。オンプレミスのActive DirectoryとOktaの両方で、すべてのユーザーが同じ識別子で構成されていることを確認してください。Citrix Endpoint Managementは、この識別子を使用して、IDプロバイダー上のユーザーをオンプレミスのActive Directoryユーザーにマッピングします。
- **ユーザー識別子文字列:** このフィールドは自動的に入力されます。

この構成後、ドメイン参加しているCitrix Secure Hubユーザーは、Citrix Secure Hubを使用してOktaの資格情報でサインインできます。Citrix Secure Hubは、MAMデバイスにクライアント証明書認証を使用します。

Citrix Secure Hubの認証フロー

Citrix Endpoint Managementは、Citrix Secure Hubを介して登録されたデバイスで、OktaをIdPとして使用してユーザーを認証するために、次のフローを使用します。

1. ユーザーがCitrix Secure Hubを起動します。
2. Citrix Secure Hubは認証要求をCitrix Identityに渡し、Citrix Identityはその要求をOktaに渡します。
3. ユーザーはユーザー名とパスワードを入力します。
4. Oktaはユーザーを検証し、コードをCitrix Identityに送信します。
5. Citrix IdentityはコードをCitrix Secure Hubに送信し、Citrix Secure HubはそのコードをCitrix Endpoint Managementサーバーに送信します。
6. Citrix Endpoint Managementは、コードとシークレットを使用してIDトークンを取得し、IDトークン内のユーザー情報を検証します。Citrix Endpoint ManagementはセッションIDを返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAM登録のためのNetScaler Gatewayを介したOktaによる認証

Citrix Endpoint Managementは、NetScaler Gatewayを介したOkta資格情報による認証をサポートしています。この認証方法は、Citrix Secure Hubを介してMAMに登録するユーザーのみが利用できます。

前提条件

MAMに登録されたデバイスのIDプロバイダー (IdP) としてNetScaler Gatewayを介したOktaを使用するようにCitrix Endpoint Managementを構成するには、以下の前提条件が満たされていることを確認してください。

- MDMに登録されたデバイスのIdPとして、Citrix Cloudを介したOktaでCitrix Endpoint Managementを構成します。MDM向けOktaの構成の詳細については、「Citrix Cloudを介したOktaによる認証」を参照してください。
- プラットフォームに応じて、以下の関連する機能フラグをそれぞれ有効にします。
  - iOS:
    - iOS-V3フォーム-MAM
    - iOS-SAML認証-MAM
  - アンドロイド:
    - Android-V3フォーム-MAM
    - Android-SAML認証-MAM

> **注：**
>
> この機能を有効にするには、サポートチームにお問い合わせください。

- Citrix Secure Hubの最新バージョンをダウンロードしてインストールします。
- Oktaサービスが組織で利用可能であり、関連するユーザーとグループがOktaに作成またはインポートされていることを確認してください。

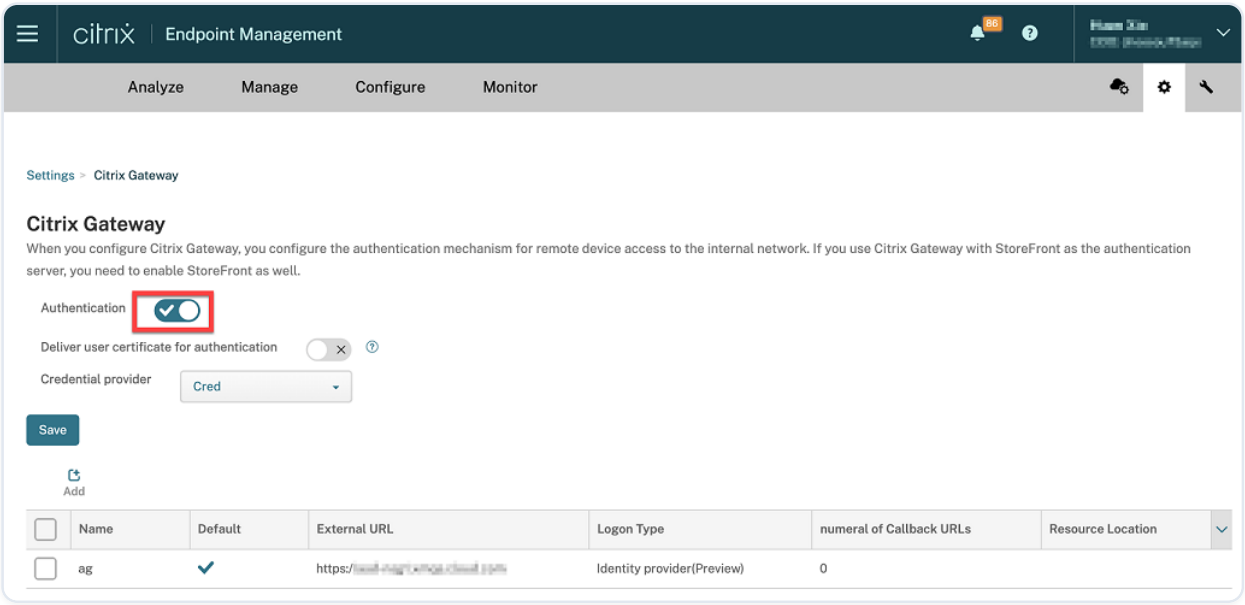
シトリックス エンドポイント マネジメントでネットスケーラー ゲートウェイを構成する

1. Citrix Endpoint Managementコンソールにサインインし、**設定**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アイコンをクリックします。

2. **サーバー**の下にある**NetScaler Gateway**をクリックします。
3. **認証**トグルボタンを有効にします。



4. ゲートウェイの**ログオンの種類**が*IDプロバイダー*であることを確認してください。
5. **保存**をクリックします。

オンプレミスNetScaler Gatewayを準備する

1. Citrix Endpoint Management用にオンプレミスNetScaler Gatewayが構成されていない場合は、次の手順を実行します。

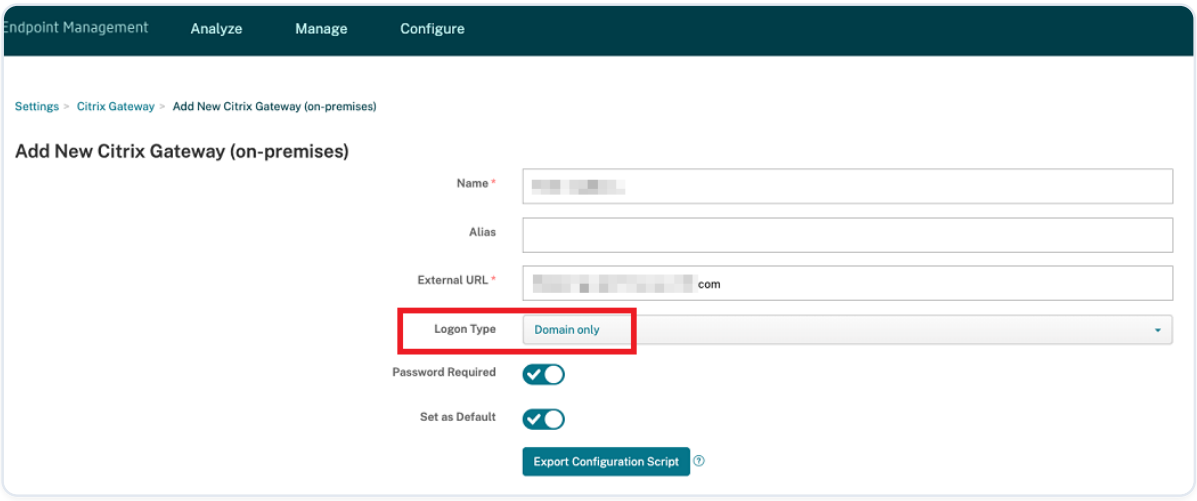
   a. Citrix Endpoint Managementコンソールで、**設定**
   アイコンをクリックします。

   b. **サーバー**の下にある**NetScaler Gateway**をクリックします。

   c. **編集**をクリックします。

   d. **ログオンの種類**ドロップダウンメニューをクリックし、*ドメインのみ*を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



e. 「**構成スクリプトのエクスポート**」をクリックします。

「構成スクリプトのエクスポートをダウンロード」(/en-us/citrix-endpoint-management/media/export-configuration-script.png) **構成スクリプトのエクスポート**がダウンロードされます。

f. 「**ログオンの種類**」ドロップダウンメニューをクリックし、「*IDプロバイダー*」を選択します。

「ログオンの種類をIDプロバイダーとして更新」(/en-us/citrix-endpoint-management/media/logon-type-identity-provider.png)

g. 「**保存**」をクリックします。

h. ダウンロードしたzipファイルを開き、そこからファイルを抽出します。

i. 抽出された.txtファイル内のスクリプトを実行して、オンプレミスのNetScaler Gatewayを準備します。

「zipファイル情報を抽出」(/en-us/citrix-endpoint-management/media/export-configuration-script-zip-file.png)

2. Citrix ADC管理コンソールにサインインし、**NetScaler Gateway** > **仮想サーバー**に移動します。
3. Citrix Endpoint Managementのセットアップに関連するゲートウェイをクリックします。
4. オンプレミスのNetScaler Gatewayで既存の認証ポリシーをすべてバインド解除します。

Oktaを構成する

1. 管理者としてOktaにサインインします。
2. 「**アプリケーション**」>「**アプリケーション**」>「**アプリカタログを参照**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「Oktaでアプリカタログを参照」(/en-us/citrix-endpoint-management/media/browse-app-catalog.png)

3. 「**Browse App Integration Catalog**」の下にある検索バーに「**NetScaler Gateway**」と入力し、「**NetScaler Gateway (SAML, SWA)**」を選択します。

   「アプリ統合カタログの参照」でNetScaler Gatewayを検索(/en-us/citrix-endpoint-management/media/browse-app-citrix-gateway.png)

4. 「**Add Integration**」をクリックします。

   NetScaler Gatewayの統合を追加(/en-us/citrix-endpoint-management/media/citrix-gateway-add-integration.png)

5. 「**Application label**」フィールドに、関連する名前を入力します。
6. 「**Login URL**」フィールドにゲートウェイ仮想サーバーのURLを入力し、「**Next**」をクリックします。

   NetScaler Gatewayの一般設定(/en-us/citrix-endpoint-management/media/add-citrix-gateway-general-settings.png)

   注：

   「**Login URL**」フィールドに入力されたURLは、Citrix Endpoint Management設定のNetScaler Gateway URLと同じである必要があります。

7. 「**Sign-On Options Required**」>「**Sign on methods**」の下で、「**SAML 2.0**」を選択します。

   ネットスケーラー ゲートウェイ - SAML 2.0(/en-us/citrix-endpoint-management/media/citrix-gateway-add-saml.png)

8. 「**View Setup Instructions**」をクリックし、ページに記載されている指示に従って、Citrix®オンプレミスゲートウェイ管理コンソールでSAMLポリシーを作成します。

   NetScaler Gateway SAML - セットアップ手順の表示(/en-us/citrix-endpoint-management/media/saml-view-setup-instructions.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

- NetScaler Gatewayバージョン11.1以降を構成する際にCA証明書をインストールした後、SAMLアクションを作成します。SAMLアクションを作成するには、「**Security**」>「**AAA - Application Traffic**」>「**Policies**」>「**Authentication**」>「**Advanced Policies**」>「**Actions**」>「**SAML Actions**」に移動します。「**Add**」をクリックし、前のページに記載されている情報を入力します。ページに記載されているナビゲーション、つまり「**Netscaler Gateway**」>「**Policies**」>「**Authentication**」>「**SAML**」>「**Servers**」には従わないでください。
- また、SAMLポリシーを作成するために提供されている手順はクラシックポリシーを使用しているため、それに従わないでください。現在、アドバンストポリシーを使用しています。アドバンストポリシーを使用してSAMLポリシーを作成するには、以下のステップ9を実行してください。

9. SAMLアクションに対応するSAMLポリシーを作成し、そのポリシーを認証仮想サーバーに次のようにバインドします。

   a. **Security** > **AAA-Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** に移動し、**Add** をクリックします。

   b. 認証ポリシーの作成ページで、以下の詳細を入力します。

      - **名前** - SAMLポリシーの名前を指定します。
      - **アクションタイプ** - 認証アクションタイプとして *SAML* を選択します。
      - **アクション** - SAMLポリシーをバインドするSAMLサーバープロファイルを選択します。
      - **式** - SAMLポリシーがユーザーをSAMLサーバーで認証する必要があるかどうかを判断するために使用するルールまたは式の名前を表示します。テキストボックスで、SAMLポリシーを有効にし、対応するSAMLアクションを実行するために、**rule** = `true` の値を設定します。

   c. SAMLポリシーをVPN仮想サーバーにバインドし、認証プロファイルを介してVPN仮想サーバーを認証仮想サーバーにリンクします。バインド手順の詳細については、認証ポリシーのバインド を参照してください。

10. GUIを使用して認証仮想サーバーを設定する を使用して、AAA仮想サーバーを作成します。
11. 認証仮想サーバーを構成する を使用して、AAA仮想サーバーを構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. 認証プロファイル を使用して、認証プロファイルを作成および構成します。
13. 認証プロファイルをGateway仮想サーバーにバインドし、すべての構成を保存します。
14. Citrixオンプレミスゲートウェイ管理コンソールでSAMLポリシーを作成した後、をクリックします。

    これで、Citrix Endpoint Management統合用の2つのアプリケーション、つまりCitrix Cloud用のWebアプリケーションと、Citrix Endpoint Management MAM認証用のSAMLアプリケーションが表示されます。
15. 作成したSAMLアプリケーションに関連するユーザーとグループを割り当てます。

これで、OktaはMAMに登録されたデバイスのIDプロバイダーとして追加され、Oktaを使用してそれらを認証できます。

予期される動作

次の例では、Androidデバイスを使用しています。

1. モバイルデバイスで、Citrix Secure Hubアプリを開きます。

   Citrix Secure Hubアプリのアイコン(/en-us/citrix-endpoint-management/media/secure-hub-app-icon.png)
2. 必要な権限を付与します。
3. サインインページで、組織から提供された資格情報を入力し、**次へ**をタップします。

   Citrix Secure Hubサインインページ(/en-us/citrix-endpoint-management/media/mam-authentication-microsoft-sign-in-username.png)

   Oktaサインインページにリダイレクトされます。
4. Oktaサインインページで、資格情報を入力し、**サインイン**をタップします。

   Oktaサインインページ(/en-us/citrix-endpoint-management/media/mam-idp-okta-sign-in.png)
5. **職場プロファイルを設定しましょう**ページで、**同意して続行**をタップします。

   職場プロファイルを設定しましょうページ(/en-us/citrix-endpoint-management/media/lets-setup-your-workprofile.png)
6. Citrix Secure HubアプリのPINを作成し、確認します。

   シトリックス セキュア ハブ の PIN(/en-us/citrix-endpoint-management/media/citrix-secure-hub-create-pin.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Hub のホームページに正常にリダイレクトされます。

Citrix Cloudを介したオンプレミスのNetScaler Gatewayでの認証

Citrix Endpoint Managementは、Citrix Cloudを介したオンプレミスのNetScaler Gatewayでの認証をサポートしています。この認証方法は、Citrix Secure Hubを介してMDMに登録するユーザーのみが利用できます。

MAMに登録するデバイスは、Citrix Cloudを介してオンプレミスのNetScaler Gateway資格情報を使用して認証することはできません。MDM+MAMでCitrix Secure Hubを使用するには、Citrix Endpoint Managementを構成して、MAM登録にNetScaler Gatewayを使用するようにします。詳細については、「NetScaler GatewayとCitrix Endpoint Management」(/ja-jp/citrix-endpoint-management/authentication/gateway-and-endpoint-management.html#configure-on-premises-citrix-gateway-for-use-with-citrix-endpoint-management)を参照してください。

Citrix Endpoint Managementは、以下のプラットフォームでCitrix Cloudを介したオンプレミスのNetScaler Gatewayでの認証をサポートしています。

- iOSデバイス
- BYODおよび完全管理モードのAndroid Enterpriseデバイス

注：

Citrix Endpoint Managementは、登録招待状に対してCitrix Cloudを介したオンプレミスのNetScaler Gatewayでの認証をサポートしていません。登録URLを含む登録招待状をユーザーに送信した場合、ユーザーはIDプロバイダーとしてオンプレミスのNetScaler Gatewayではなく LDAPを介して認証します。

完全なシングルサインオンエクスペリエンスのために、証明書ベースの認証を有効にすることをお勧めします。MAM登録にNetScaler GatewayでLDAP認証を使用する場合、エンドユーザーは登録中に二重認証プロンプトを経験します。詳細については、「クライアント証明書または証明書とドメイン認証」(/ja-jp/citrix-endpoint-management/authentication/client-certificate.html)を参照してください。

前提条件

- NetScaler Gateway。Citrixは、完全なシングルサインオンエクスペリエンスのために、証明書ベースの認証を有効にすることをお勧めします。MAM登録にNetScaler GatewayでLDAP認証

© 1997–2026 Citrix Systems, Inc. All rights reserved.

を使用する場合、エンドユーザーは登録中に二重認証プロンプトを経験します。詳細については、「クライアント証明書または証明書とドメイン認証」(/ja-jp/citrix-endpoint-management/authentication/client-certificate.html)を参照してください。

- ディレクトリサービス同期のためにCitrix Cloud Connectorがインストールされ たCitrix Cloudアカウント。
- シトリックス セキュアハブ 20.5.0 以降。

NetScaler GatewayをIDプロバイダーとして使用するようにCitrix Cloudを構成する

Citrix CloudでNetScaler Gateway認証を設定するには、「オンプレミスのNetScaler GatewayをIDプロバイダーとしてCitrix Cloudに接続する」(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/connect-ad-gateway.html)を参照してください。

Citrix IDプロバイダーをCitrix Endpoint ManagementのIdPタイプとして構成する

この構成は、Citrix Secure Hubを介して登録するユーザーにのみ適用されます。Citrix CloudでNetScaler Gatewayを構成した後、Citrix Endpoint Managementを次のように構成します。

1. Citrix Endpoint Managementコンソールで、 **［設定］> ［IDプロバイダー（IDP）］** の順に移動し、 **［追加］** をクリックします。
2. **［IDプロバイダー（IDP）］** ページで、以下を構成します。
   - **IDP名：** 作成するIdP接続を識別するための一意の名前を入力します。
   - **IDPタイプ：** **［Citrix IDプロバイダー］** を選択します。
   - **認証ドメイン：** **［NetScaler Gateway］** を選択します。このドメインは、Citrix Cloudの **［ワークスペース構成］> ［認証］** ページにあるIDプロバイダードメインに対応します。
3. **［次へ］** をクリックします。 **［IDPクレームの使用状況］** ページで、以下を構成します。
   - **ユーザー識別子の種類：** デフォルトでは、このフィールドは **userPrincipalName** に設定されています。
   - **ユーザー識別子文字列：** このフィールドは自動的に入力されます。
4. **［次へ］** をクリックし、 **［概要］** ページを確認してから、 **［保存］** をクリックします。

これで、オンプレミスのNetScaler GatewayをIDプロバイダーとして使用して、Citrix Secure Hubを介してユーザーデバイスを登録できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Hub認証フロー

Citrix Endpoint Managementは、Citrix Secure Hubを介して登録されたデバイスで、オンプレミスのNetScaler GatewayをIdPとして使用してユーザーを認証するために、次のフローを使用します。

1. ユーザーがCitrix Secure Hubを起動します。
2. Citrix Secure Hubは認証要求をCitrix Identityに渡し、Citrix Identityはその要求をオンプレミスのNetScaler Gatewayに渡します。
3. ユーザーはユーザー名とパスワードを入力します。
4. オンプレミスのNetScaler Gatewayはユーザーを検証し、Citrix Identityにコードを送信します。
5. Citrix IdentityはコードをCitrix Secure Hubに送信し、Citrix Secure HubはそのコードをCitrix Endpoint Managementサーバーに送信します。
6. Citrix Endpoint Managementは、コードとシークレットを使用してIDトークンを取得し、その後、IDトークンに含まれるユーザー情報を検証します。Citrix Endpoint ManagementはセッションIDを返します。

nFactor認証

Citrix Secure Hubを使用している場合、nFactor認証により、NetScalerで現在利用可能なすべての認証モードを使用できます。これにより、ユーザーがアクセスするために複数の身元証明を提供することを要求することで、アプリケーションのセキュリティが強化されます。nFactor認証の詳細については、nFactor認証を参照してください。

また、さまざまな認証および承認方法とその構成方法の詳細については、認証と承認を参照してください。

Citrix Endpoint Managementは、nFactor認証で次の認証タイプをサポートしています。

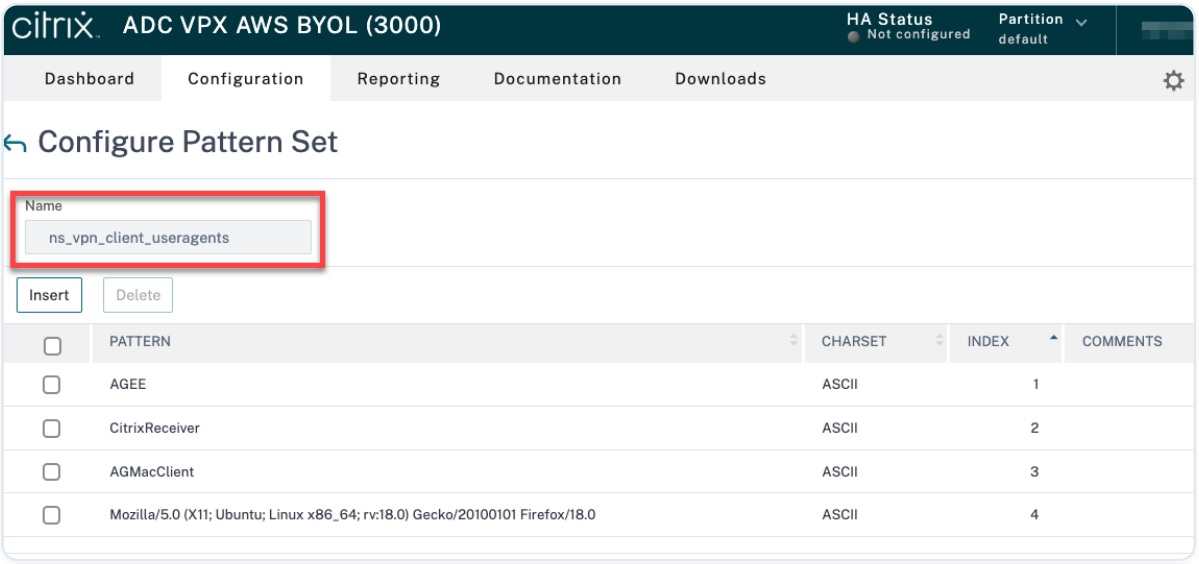
- ローカル
- 軽量ディレクトリアクセスプロトコル (LDAP)
- RADIUS
- SAML
- クライアント証明書認証

© 1997–2026 Citrix Systems, Inc. All rights reserved.

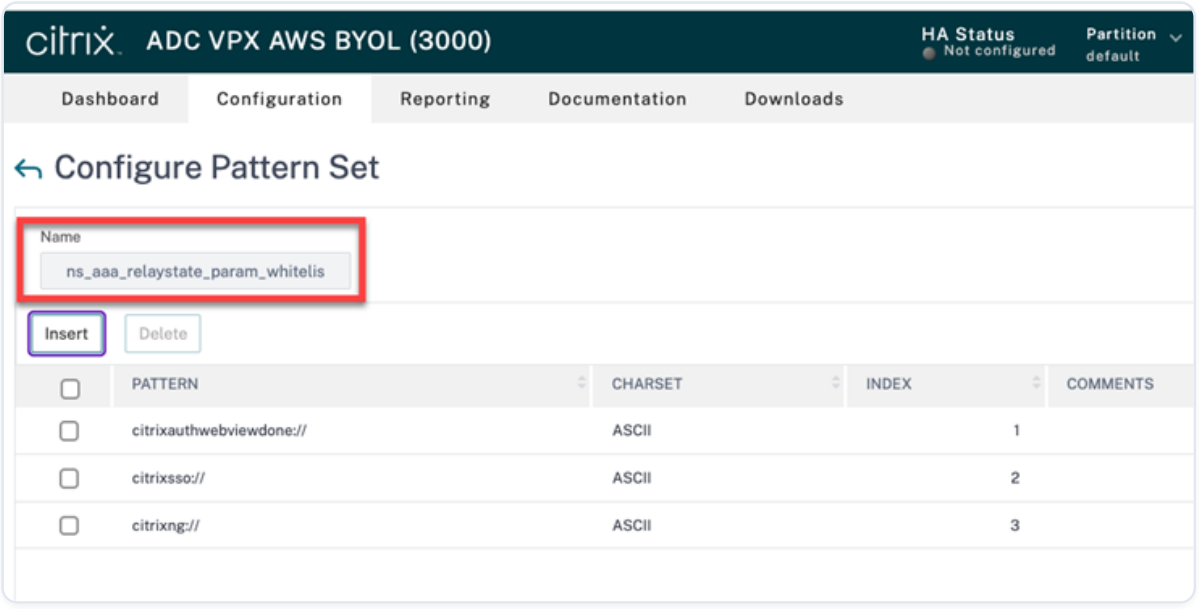
前提条件

Citrix Endpoint ManagementでnFactor認証を使用するように構成するには、次の前提条件が満たされていることを確認してください。

- NetScaler 13.0以降を使用していることを確認してください。
- AndroidおよびiOSデバイス用にNetScaler®で次のパターンセット設定を構成していることを確認してください。
  - Ns_vpn_client_useragents



  - Ns_aaa_relaystate_param_whitelist



- AppleまたはGoogle PlayからCitrix Secure Hubの最新バージョンがインストールされていることを確認してください。
- NetScaler GatewayでAdvanced認証ポリシーを使用していることを確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- オンプレミスとクラウドの両方で、クライアントプロパティ **ENABLE_MAM_NFACTOR_SSO** を **True** に設定していることを確認してください。**ENABLE_MAM_NFACTOR_SSO** プロパティの詳細については、「クライアントプロパティリファレンス」を参照してください。

> **注：**
>
> クライアントプロパティ **Enable nFactor SSO** が **False** に設定されている場合は、従来の認証ポリシーがNetScaler Gatewayにバインドされていることを確認してください。

nFactor認証を構成する

NetScaler Gatewayのセットアップ方法に応じて、Citrix Endpoint ManagementのnFactor認証を次のように構成します。

- Citrix Endpoint Managementは、従来の認証ポリシーを使用してNetScaler Gatewayにすでにセットアップされています。詳細については、「既存のNetScaler Gatewayで従来のポリシーをAdvanced認証ポリシーに更新する」を参照してください。
- Advanced認証ポリシーを使用してNetScaler GatewayをセットアップしたCitrix Endpoint Management。詳細については、「Advancedポリシーを使用してNetScaler Gatewayのセットアップを構成する」を参照してください。

既存のNetScaler Gatewayで従来のポリシーをAdvanced認証ポリシーに更新する

Citrix Endpoint ManagementがNetScaler Gatewayで従来の認証ポリシーを使用してすでにセットアップされている場合は、次のいずれかの方法を使用して、従来の認証ポリシーをAdvanced認証ポリシーに更新する必要があります。

- Advanced認証ポリシーを作成し、ゲートウェイ構成をAdvanced認証ポリシーを使用するように変更します。詳細については、「認証ポリシー」を参照してください。
- 従来の認証ポリシーをAdvanced認証ポリシーに更新します。詳細については、「NSPEPIツールを使用したポリシー式の変換」を参照してください。

Advancedポリシーを使用してNetScaler Gatewayのセットアップを構成する

NetScaler GatewayでCitrix Endpoint ManagementのnFactor認証をAdvanced認証ポリシーを使用して構成するには、「nFactor認証の構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

- サポートされている認証タイプの中から、関連する認証タイプを選択できます。
- SAML認証タイプを使用している場合は、以下のいずれかの方法でMAM IdPを使用してSAMLを構成できます。
  - Azure Active Directoryを使用して構成するには、「MAM登録のためのNetScaler Gatewayを介したAzure Active Directoryによる認証」を参照してください。
  - Oktaを使用して構成するには、「MAM登録のためのNetScaler Gatewayを介したOktaによる認証」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーアカウント、役割、および登録

ユーザー構成タスクは、Citrix Endpoint Managementコンソールの**Manage**タブと**Settings**ページで行います。特に指定がない限り、以下のタスクの手順はこの記事で説明されています。

- 登録セキュリティモードと招待
  - **Settings > Enrollment**から、最大7つの登録セキュリティモードを設定し、登録招待を送信します。各登録セキュリティモードには、独自のセキュリティレベルと、ユーザーがデバイスを登録するために必要な手順の数があります。
- ユーザーアカウントとグループの役割
  - **Settings > Role-Based Access Control**から、事前定義された役割（または一連の権限）をユーザーとグループに割り当てます。これらの権限は、ユーザーがシステム機能にアクセスできるレベルを制御します。詳細については、「RBACで役割を構成する」を参照してください。
  - **Settings > Notification Templates**から、自動アクション、登録、およびユーザーに送信される標準通知メッセージで使用する通知テンプレートを作成または更新します。通知テンプレートは、Citrix Secure HubまたはSMTPの2つの異なるチャネルを介してメッセージを送信するように構成します。詳細については、「通知テンプレートの作成と更新」を参照してください。
- ユーザーアカウントとグループ:
  - **Manage > Users**から、ローカルユーザーアカウントを手動で追加するか、.csvプロビジョニングファイルを使用してアカウントをインポートし、ローカルグループを管理できます。ただし、ほとんどのCitrix Endpoint Management展開では、ユーザーおよびグループ情報のためにLDAPに接続します。次のようなユースケースでは、ローカルでユーザーアカウントを作成することを推奨する場合があります。
    - 小売業などの環境で、デバイスが個々のユーザーに専用ではなく共有されている場合。
    - Novell eDirectoryなど、サポートされていないディレクトリを使用している場合。
  - **Settings > Workflows**から、ワークフローを使用してユーザーアカウントの作成と削除を管理します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーアカウントについて

Citrix Endpoint Managementのユーザーアカウントは、ローカルユーザー、Active Directoryユーザー、またはクラウドユーザーのいずれかです。

- **クラウドユーザー:** クラウドユーザーは、管理者がCitrix Cloudの顧客アカウントに追加されたときにCitrix Cloudが作成する特別なユーザーアカウントです。クラウドユーザーアカウントは、Citrix Cloud上の管理者アカウントと同じユーザー名を使用し、デフォルトで管理者役割になります。クラウドユーザーアカウントはシングルサインオンを提供し、その他の管理機能を実行します。

  Citrix Cloudアカウントに管理者を追加するには、「新しい管理者を招待する」を参照してください。

クラウドユーザーの場合：

- クラウドユーザーの役割とユーザープロパティは、Citrix Cloudコンソールから変更できます。「Citrix Cloud管理者の管理」を参照してください。
- パスワードを変更するには、「管理者」を参照してください。
- クラウドユーザーを削除するには、Citrix Cloudで、**［IDおよびアクセス管理］>［管理者］**の順に移動します。ユーザーの行の末尾にある省略記号をクリックし、［管理者の削除］**を選択します。
- クラウドユーザーをローカルグループに追加することはできません。

登録セキュリティモードを構成する

デバイス登録セキュリティモードを構成して、Citrix Endpoint Managementでのデバイス登録のセキュリティレベルと通知テンプレートを指定します。

Citrix Endpoint Managementには6つの登録セキュリティモードがあり、それぞれに独自のセキュリティレベルと、ユーザーがデバイスを登録するために実行する必要がある手順があります。登録セキュリティモードは、Citrix Endpoint Managementコンソールの**［管理］>［登録招待］**ページで構成します。詳しくは、「登録招待」を参照してください。

注：

カスタム通知テンプレートを使用する予定がある場合は、登録セキュリティモードを構成する前にテンプレートを設定する必要があります。通知テンプレートについて詳しくは、「通知テンプレートの作成または更新」を参照してください。

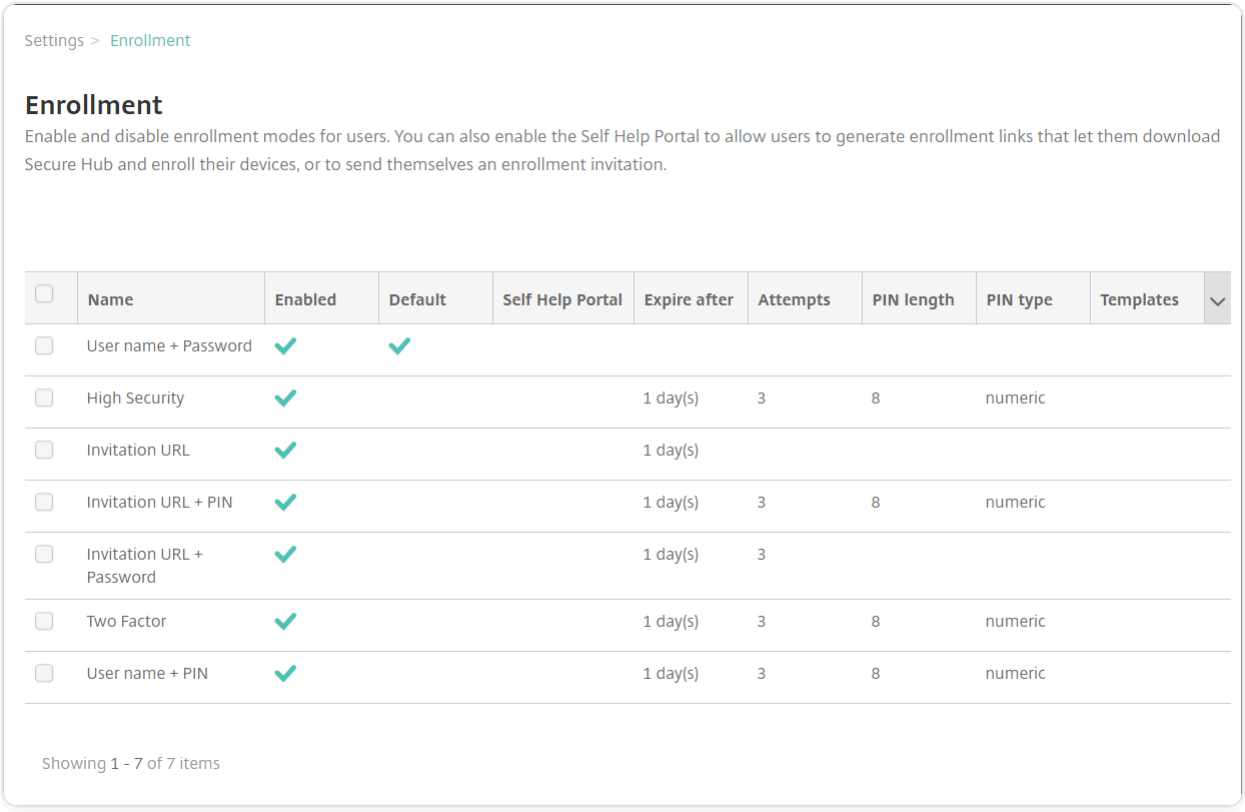
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**［設定］**ページが表示されます。
2. **［登録］をクリックします。**［登録］**ページが表示されます。このページには、利用可能なすべての登録セキュリティモードの表があります。デフォルトでは、すべての登録セキュリティモードが有効になっています。
3. リスト内の任意の登録セキュリティモードを選択して編集します。次に、そのモードをデフォルトとして設定するか、モードを無効にします。

   登録セキュリティモードの横にあるチェックボックスをオンにして、オプションメニューを表示します。または、リスト内の他の場所をクリックして、リストの右側にあるオプションメニューを表示します。

ヒント:

登録セキュリティモードを編集する際、ユーザーがデバイスを登録できなくなる有効期限を指定できます。詳しくは、この記事の「登録セキュリティモードを編集するには」を参照してください。この値は、ユーザーおよびグループの登録招待構成ページに表示されます。



プラットフォームに応じて、次の登録セキュリティモードを選択できます。

- ユーザー名 + パスワード

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 招待URL
- 招待URL + PIN
- 招待URL + パスワード
- 2要素認証
- ユーザー名 + PIN

プラットフォーム固有の登録セキュリティモードについては、「プラットフォーム別の登録セキュリティモード」を参照してください。

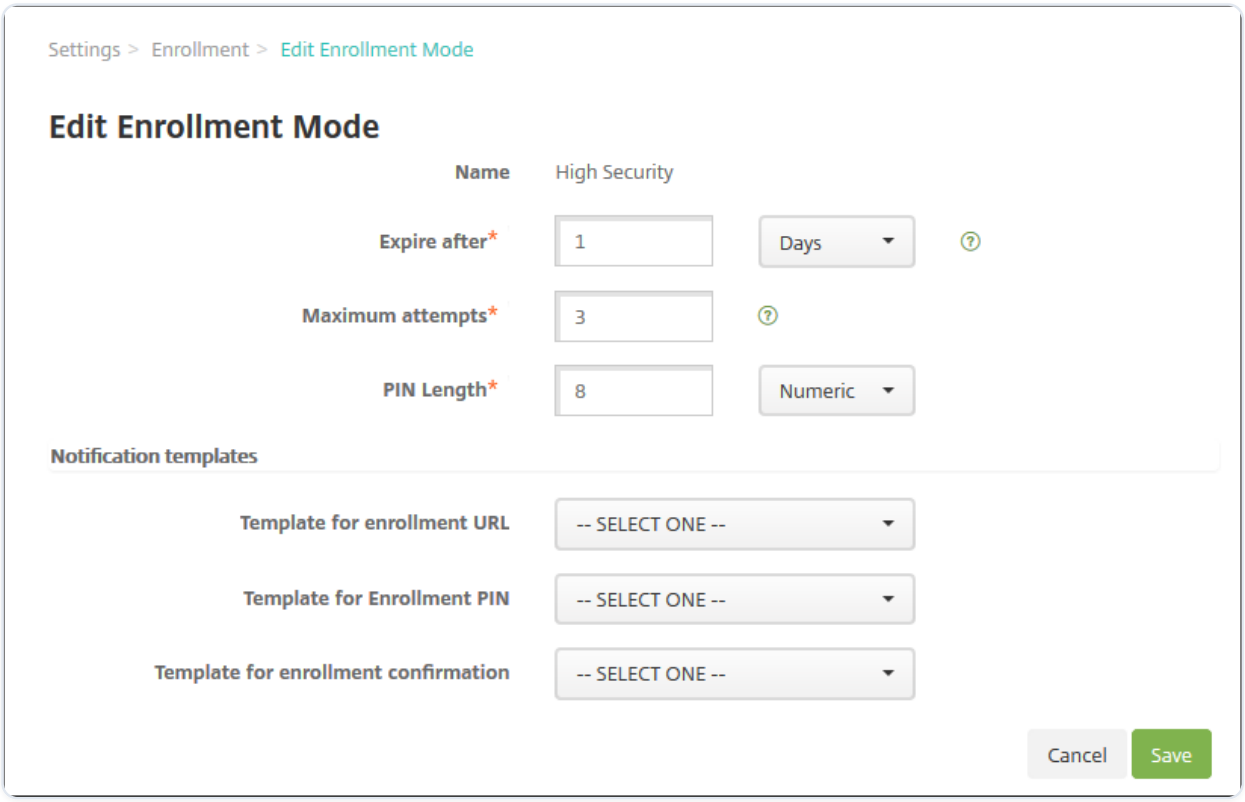
登録招待は、特定のユーザーまたはグループへの登録機能を制限する効果的な方法として使用できます。登録招待を送信するには、**招待URL**、**招待URL + PIN**、または**招待URL + パスワード**の登録セキュリティモードのみを使用できます。**ユーザー名 + パスワード**、**2要素認証**、または**ユーザー名 + PIN**で登録するデバイスの場合、ユーザーはCitrix Secure Hubに資格情報を手動で入力する必要があります。

ワンタイムPIN（OTPとも呼ばれることがあります）登録招待を2要素認証ソリューションとして使用できます。ワンタイムPIN登録招待は、ユーザーが登録できるデバイスの数を制御します。OTP招待はWindowsデバイスでは利用できません。

登録セキュリティモードを編集するには

1. **登録**リストで、登録セキュリティモードを選択し、**編集**をクリックします。**登録モードの編集**ページが表示されます。選択したモードに応じて、異なるオプションが表示される場合があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 必要に応じて、以下の情報を変更します。

- **有効期限：** ユーザーがデバイスを登録できなくなる有効期限を入力します。この値は、ユーザーおよびグループの登録招待構成ページに表示されます。

  招待の有効期限が切れないようにするには、「**0**」と入力します。

- **日数：** ドロップダウンリストで、**有効期限**に入力した有効期限に対応する「**日数**」または「**時間**」をクリックします。
- **最大試行回数：** ユーザーが登録プロセスからロックアウトされるまでに試行できる登録回数を入力します。この値は、ユーザーおよびグループの登録招待構成ページに表示されます。

  試行回数を無制限にするには、「**0**」と入力します。

- **PINの長さ：** 生成されるPINの長さを設定する数値を入力します。
- **数字：** PINの種類として、ドロップダウンリストで「**数字**」または「**英数字**」をクリックします。
- **通知テンプレート：**

  - **登録URLのテンプレート：** 登録URLに使用するテンプレートをドロップダウンリストからクリックします。たとえば、登録招待テンプレートはユーザーにメールを送信します。通知テンプレートについて詳しくは、「通知テンプレートの作成または更新」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **登録PINのテンプレート：** 登録PINに使用するテンプレートをドロップダウンリストからクリックします。
- **登録確認のテンプレート：** ユーザーに登録が成功したことを通知するために使用するテンプレートをドロップダウンリストからクリックします。

3. **保存**をクリックします。

登録セキュリティモードをデフォルトとして設定するには

別の登録セキュリティモードを選択しない限り、すべてのデバイス登録要求に既定の登録セキュリティモードが使用されます。既定の登録セキュリティモードが設定されていない場合は、デバイス登録ごとに登録要求を作成する必要があります。

1. 既定として使用する登録セキュリティモードが有効になっていない場合は、それを選択して をクリックします。既定として使用できる登録セキュリティモードは、、、または のみです。
2. 登録セキュリティモードを選択し、 をクリックします。選択したモードが既定になりました。他の登録セキュリティモードが既定として設定されていた場合、そのモードは既定ではなくなります。

登録セキュリティモードを無効にするには

登録セキュリティモードを無効にすると、グループ登録招待とセルフヘルプポータルの両方で使用できなくなります。1つの登録セキュリティモードを無効にして別のモードを有効にすることで、ユーザーがデバイスを登録する方法を変更できます。

1. 登録セキュリティモードを選択します。

   既定の登録セキュリティモードは無効にできません。既定の登録セキュリティモードを無効にする場合は、まずその既定ステータスを削除する必要があります。
2. をクリックします。登録セキュリティモードは有効ではなくなります。

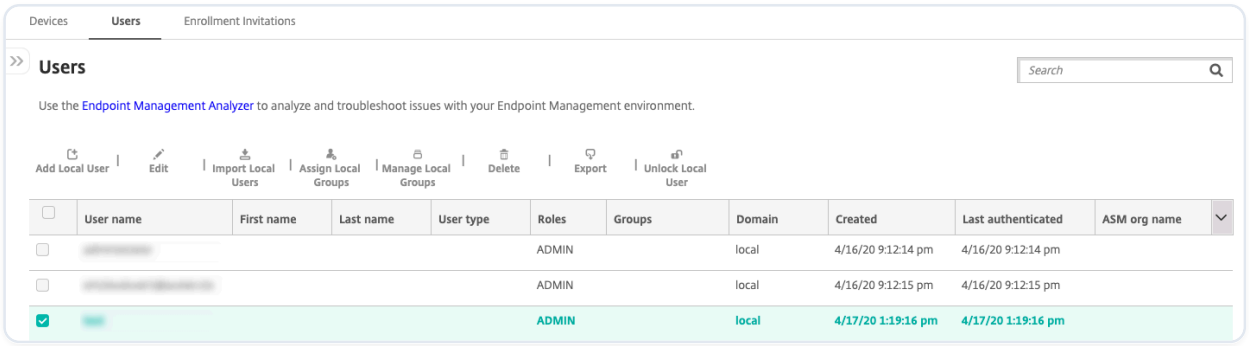
ローカルユーザーアカウントの追加、編集、ロック解除、または削除

Citrix Endpoint Management にローカルユーザーアカウントを手動で追加することも、プロビジョニングファイルを使用してアカウントをインポートすることもできます。プロビジョニングファイルからユーザーアカウントをインポートする手順については、「ユーザーアカウントのインポート」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

すべての Citrix Cloud 管理者は、Citrix Endpoint Management 管理者として作成されます。カスタムアクセス権を持つ Citrix Cloud 管理者を作成する場合は、そのアクセス権に Citrix Endpoint Management が含まれていることを確認してください。Citrix Cloud 管理者の追加については、「管理者の追加」を参照してください。

1. Citrix Endpoint Management コンソールで、 > の順にクリックします。 ページが表示されます。



2. リストをフィルター処理するには、 をクリックします。

ローカルユーザーアカウントを追加するには

1. 「**ユーザー**」ページで、「**ローカルユーザーの追加**」をクリックします。「**ローカルユーザーの追加**」ページが表示されます。

   ユーザー管理(/en-us/citrix-endpoint-management/media/manage-users-add-local.png)

2. これらの設定を構成します:

   - **ユーザー名:** 名前を入力します。これは必須フィールドです。名前に含めることができるのは、スペース、大文字、小文字です。
   - **パスワード:** オプションのユーザーパスワードを入力します。パスワードは14文字以上で、以下のすべての条件を満たす必要があります。
     - 少なくとも2つの数字を含める
     - 少なくとも1つの大文字と1つの小文字を含める
     - 少なくとも1つの特殊文字を含める
     - 辞書に載っている単語や制限された単語（Citrix®ユーザー名やメールアドレスなど）を含めないでください
     - 3つ以上の連続した繰り返し文字やキーボードパターン（例: 1111、1234、asdf）を含めないでください

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **役割:** ドロップダウンリストからユーザーの役割をクリックします。役割の詳細については、「RBACで役割を構成する」を参照してください。選択可能なオプションは次のとおりです。
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- **メンバーシップ:** ドロップダウンリストから、ユーザーを追加するグループをクリックします。
- **ユーザープロパティ:** オプションのユーザープロパティを追加します。追加するユーザープロパティごとに、**追加**をクリックして、次の操作を行います。
  - **ユーザープロパティ:** ドロップダウンリストからプロパティをクリックし、プロパティの横のフィールドにユーザープロパティ属性を入力します。
  - ユーザープロパティを保存するには**完了**をクリックするか、**キャンセル**をクリックします。

既存のユーザープロパティを削除するには、プロパティがある行にカーソルを合わせ、右側の**X**をクリックします。プロパティはすぐに削除されます。

既存のユーザープロパティを編集するには、プロパティをクリックして変更を加えます。変更したリストを保存するには**完了**をクリックするか、リストを変更しないままにするには**キャンセル**をクリックします。

3. **保存**をクリックします。ユーザーを作成した後、ローカルユーザーアカウントの**ユーザーの種類**フィールドは空のままになります。

ローカルユーザーアカウントを編集するには

1. **ユーザー**ページで、ユーザーのリストからユーザーを選択し、**編集**をクリックします。**ローカルユーザーの編集**ページが表示されます。

   ローカルユーザーの編集(/en-us/citrix-endpoint-management/media/manage-users-edit-local.png)

2. 必要に応じて、次の情報を変更します。
   - **ユーザー名:** ユーザー名を変更することはできません。
   - **パスワード:** ユーザーパスワードを変更または追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **役割:** ドロップダウンリストからユーザーの役割をクリックします。
- **メンバーシップ:** ドロップダウンリストから、ユーザーアカウントを追加または編集するグループをクリックします。グループからユーザーアカウントを削除するには、グループ名の横にあるチェックボックスをオフにします。
- **ユーザープロパティ:** 次のいずれかを実行します。
  - 変更するユーザープロパティごとに、そのプロパティをクリックして変更を加えます。変更したリストを保存するには**［完了］をクリックし、リストを変更しないままにするには［キャンセル］**をクリックします。
  - 追加するユーザープロパティごとに、**［追加］**をクリックして次の操作を行います。
    - **ユーザープロパティ:** ドロップダウンリストでプロパティをクリックし、プロパティの横のフィールドにユーザープロパティ属性を入力します。
    - ユーザープロパティを保存するには**［完了］をクリックし、保存しない場合は［キャンセル］**をクリックします。
  - 削除する既存のユーザープロパティごとに、そのプロパティがある行にマウスカーソルを合わせ、右側の**X**をクリックします。プロパティはすぐに削除されます。

3. 変更を保存するには**［保存］をクリックし、ユーザーを変更しないままにするには［キャンセル］**をクリックします。

ローカルユーザーアカウントのロックを解除するには

ローカルユーザーアカウントは、以下のサーバープロパティに従ってロックされます。

- `local.user.account.lockout.time`
- `local.user.account.lockout.limit`

  詳しくは、「サーバープロパティの定義」を参照してください。

ローカルユーザーアカウントがロックされた場合、Citrix Endpoint Managementコンソールからアカウントのロックを解除できます。

1. **［ユーザー］**ページで、ユーザーアカウントのリストからユーザーアカウントをクリックして選択します。
2. **［ユーザーのロック解除］**をクリックします。確認ダイアログボックスが表示されます。
3. ユーザーアカウントのロックを解除するには「**ロック解除**」をクリックするか、ユーザーを変更しないままにするには「**キャンセル**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint ManagementコンソールからActive Directoryユーザーを開くことはできません。ロックされたActive Directoryユーザーは、パスワードのリセットについてActive Directoryヘルプデスクに連絡する必要があります。

ローカルユーザーアカウントを削除するには

1. 「**ユーザー**」ページで、ユーザーアカウントのリストからユーザーアカウントをクリックして選択します。

   各ユーザーアカウントの横にあるチェックボックスをオンにすることで、複数のユーザーアカウントを削除対象として選択できます。
2. 「**削除**」をクリックします。確認ダイアログボックスが表示されます。
3. ユーザーアカウントを削除するには「**削除**」をクリックするか、「**キャンセル**」をクリックします。

Active Directoryユーザーを削除するには

複数のActive Directoryユーザーを一度に削除するには、ユーザーを選択して「**削除**」をクリックします。

削除するユーザーが登録済みデバイスを持っており、それらのデバイスを再登録したい場合は、再登録する前にデバイスを削除してください。デバイスを削除するには、「**管理 > デバイス**」に移動し、デバイスを選択して「**削除**」をクリックします。

ユーザーアカウントのインポート

プロビジョニングファイルと呼ばれる.csvファイルからローカルユーザーアカウントとプロパティをインポートできます。このファイルは手動で作成できます。プロビジョニングファイルの形式の詳細については、「プロビジョニングファイルの形式」を参照してください。

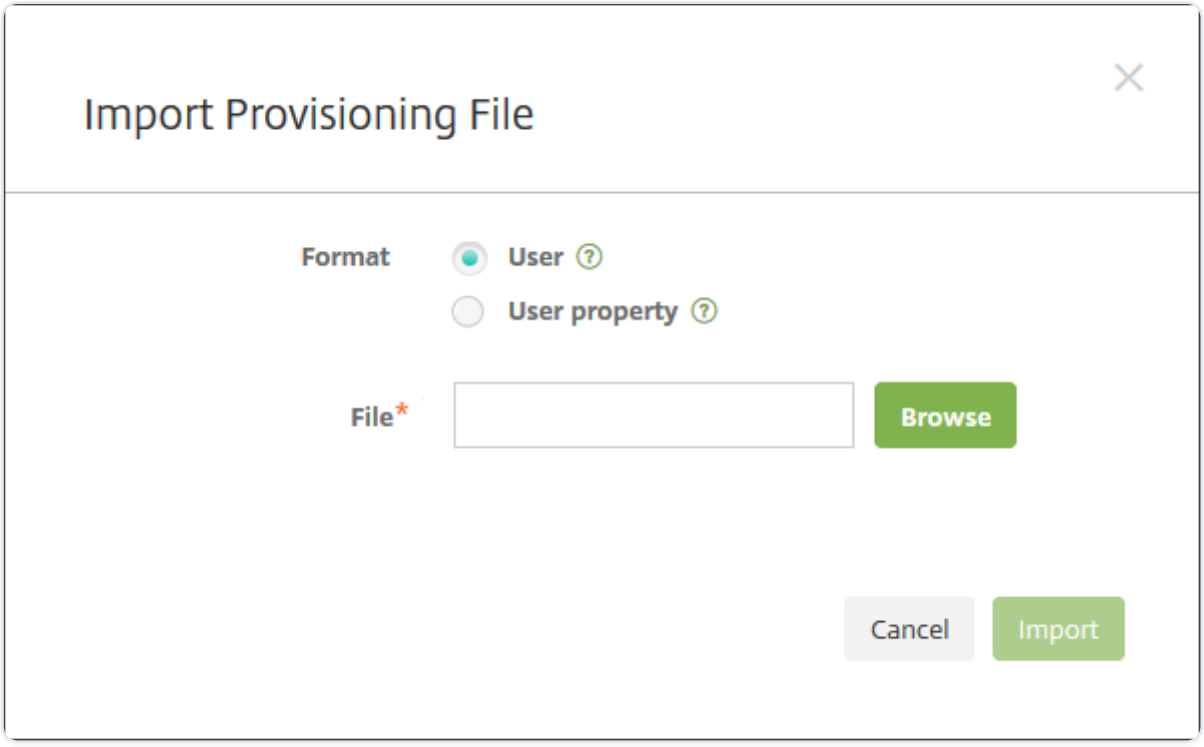
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

- ローカルユーザーの場合、インポートファイルではユーザー名とともにドメイン名を使用します。たとえば、`username@domain`と指定します。作成またはインポートするローカルユーザーがCitrix Endpoint Managementの管理対象ドメインのものである場合、そのユーザーは対応するLDAP資格情報を使用して登録することはできません。
- Citrix Endpoint Managementの内部ユーザーディレクトリにユーザーアカウントをインポートする場合、インポートプロセスを高速化するために、デフォルトドメインを無効にします。ドメインを無効にすると登録に影響することに注意してください。内部ユーザーのインポートが完了したら、デフォルトドメインを再度有効にします。
- ローカルユーザーはUPN（User Principal Name）形式にできます。ただし、Citrixでは管理対象ドメインを使用しないことをお勧めします。たとえば、example.comが管理対象である場合、user@example.comのようなUPN形式でローカルユーザーを作成しないでください。

プロビジョニングファイルの準備ができたら、次の手順に従ってCitrix Endpoint Managementにファイルをインポートします。

1. Citrix Endpoint Managementコンソールで、 > の順にクリックします。 ページが表示されます。
2. をクリックします。 ダイアログボックスが表示されます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. インポートするプロビジョニングファイルの形式として、 または のいずれかを選択します。
4. をクリックしてファイルの場所を参照し、使用するプロビジョニングファイルを選択します。
5. をクリックします。

プロビジョニングファイルの形式

プロビジョニングファイルを作成し、それを使用してユーザーアカウントとプロパティをCitrix Endpoint Managementにインポートできます。プロビジョニングファイルには、次のいずれかの形式を使用します。

- **ユーザープロビジョニングファイルのフィールド：** `user;password;role;group1;group2`
- **ユーザー属性プロビジョニングファイルのフィールド：** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

注：

- プロビジョニングファイル内のフィールドはセミコロン（;）で区切ります。フィールドの一部にセミコロンが含まれる場合は、バックスラッシュ文字 (\) でエスケープします。たとえば、プロパティ **propertyV; test;1;2** は、プロビジョニングファイルでは **propertyV\;test\;1\;2** と入力します。
- **役割** の有効な値は、事前定義された役割であるUSER、ADMIN、SUPPORT、DEVICE_PROVISIONING、および定義したその他の役割です。
- グループ階層を作成するには、区切り文字としてピリオド（.）を使用します。グループ名にはピリオドを使用しないでください。
- 属性プロビジョニングファイルでは、プロパティ属性に小文字を使用してください。データベースでは大文字と小文字が区別されます。

ユーザープロビジョニングコンテンツの例

エントリ `user01;pwd\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` は次のことを意味します。

- **ユーザー:** user01
- **パスワード:** pwd; 01
- **役割:** USER

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **グループ:**
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

別の例として、`AUser0;1.password;USER;ActiveDirectory.test.net` は次のことを意味します。

- **ユーザー:** AUser0
- **パスワード:** 1.password
- **役割:** USER
- **グループ:** ActiveDirectory.test.net

ユーザー属性プロビジョニングコンテンツの例

エントリ `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` は次のことを意味します。

- **ユーザー:** user01
- **プロパティ 1**
  - **名前:** propertyN
  - **値:** propertyV;test;1;2
- **プロパティ 2:**
  - **名前:** prop 2
  - **値:** prop2 の値

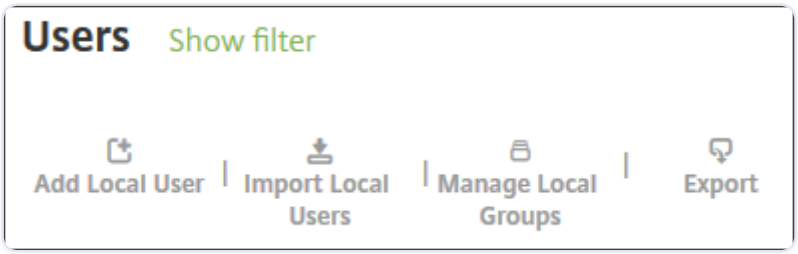
グループの追加または削除

Citrix Endpoint Managementコンソールの**ユーザー**、**ローカルユーザーの追加**、または**ローカルユーザーの編集**ページにある**グループの管理**ダイアログボックスでグループを管理します。グループ編集コマンドはありません。

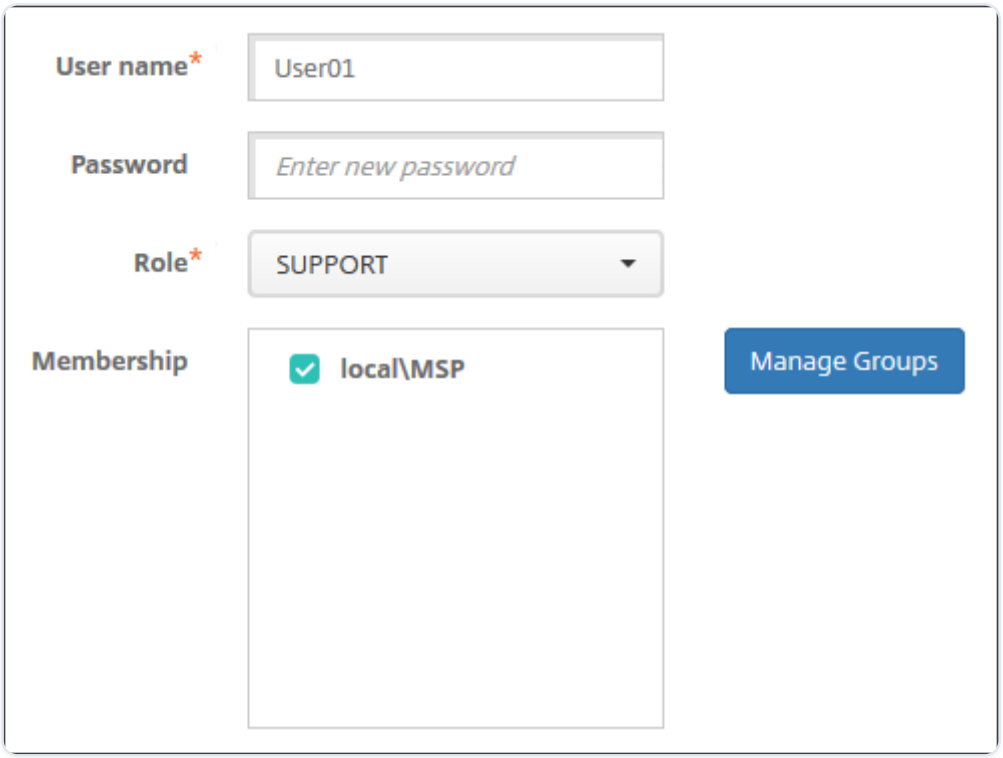
ローカルグループを追加するには

1. 次のいずれかを実行します。
   - **ユーザー**ページで、**ローカルグループの管理**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

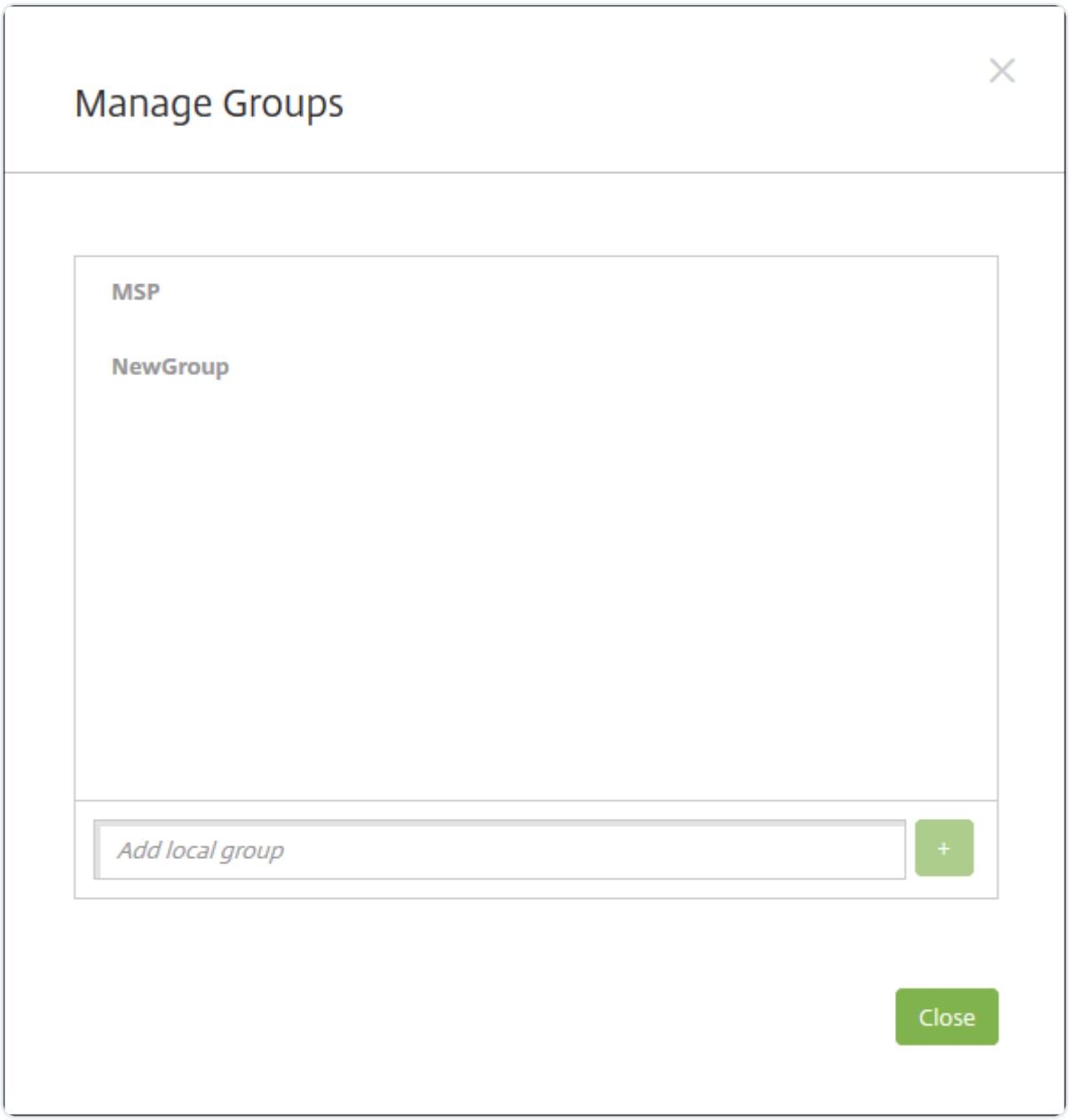


- 「**ローカルユーザーの追加**」ページまたは「**ローカルユーザーの編集**」ページで、「**グループの管理**」をクリックします。



「**グループの管理**」ダイアログボックスが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. グループリストの下に新しいグループ名を入力し、プラス記号（**+**）をクリックします。ユーザーグループがリストに追加されます。
3. 「**閉じる**」をクリックします。

グループを削除するには

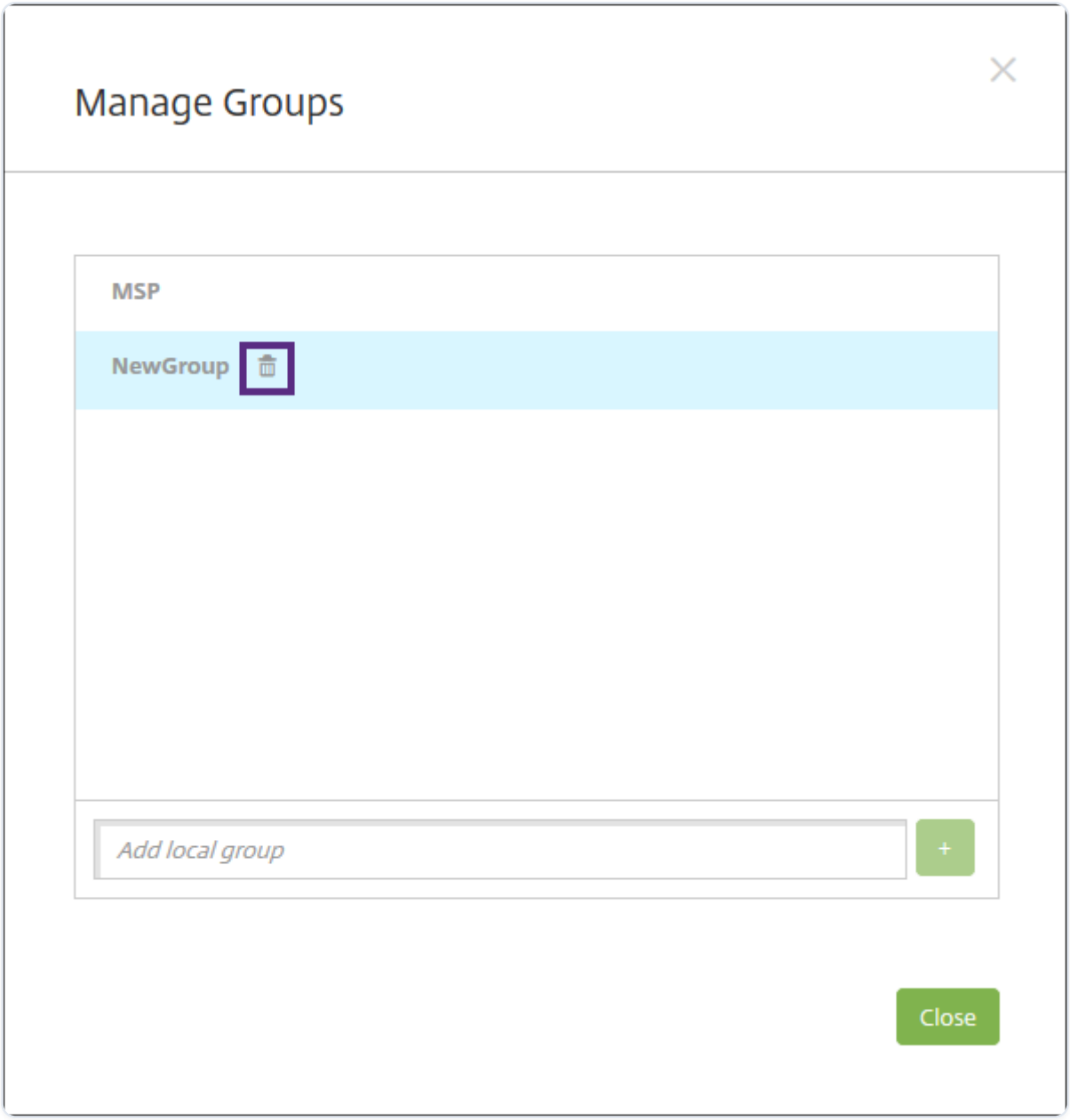
グループを削除しても、ユーザーアカウントには影響しません。代わりに、グループを削除すると、そのグループとのユーザーの関連付けのみが削除されます。ユーザーは、そのグループに関連付けられているデリバリーグループによって提供されるアプリやプロファイルへのアクセスも失います。ただし、他のグループの関連付けはそのまま維持されます。ユーザーが他のローカルグループに関連付けられていない場合、最上位レベルで関連付けられます。

1. 次のいずれかを実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**ユーザー**」ページで、「**ローカルグループの管理**」をクリックします。
- 「**ローカルユーザーの追加**」ページまたは「**ローカルユーザーの編集**」ページで、「**グループの管理**」をクリックします。

「**グループの管理**」ダイアログボックスが表示されます。



2. 「**グループの管理**」ダイアログボックスで、削除するグループをクリックします。
3. グループ名の右側にあるゴミ箱アイコンをクリックします。確認ダイアログボックスが表示されます。
4. 操作を確定してグループを削除するには、**Delete** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

この操作は元に戻せません。

5. **Manage Groups** ダイアログボックスで、**Close** をクリックします。

ワークフローの作成と管理

ワークフローを使用して、ユーザーアカウントの作成と削除を管理できます。ワークフローを作成する前に、ユーザーアカウント要求を承認する権限を持つ組織内の個人を特定します。次に、ワークフローテンプレートを使用してユーザーアカウント要求を作成および承認します。

Citrix Endpoint Management を初めてセットアップするときに、ワークフローのメール設定を構成します。ワークフローを使用するには、この設定を行う必要があります。ワークフローのメール設定はいつでも変更できます。これらの設定には、メールサーバー、ポート、メールアドレス、およびユーザーアカウント作成要求に承認が必要かどうかが含まれます。

Citrix Endpoint Management では、次の2か所でワークフローを構成できます。

- Citrix Endpoint Management コンソールの **Settings > Workflows** ページで。**Workflows** ページでは、アプリ構成で使用する複数のワークフローを構成できます。Workflows ページでワークフローを構成するときに、アプリを構成する際にそのワークフローを選択できます。
- アプリでアプリケーションコネクタを構成するときに、ワークフロー名を入力し、ユーザーアカウント要求を承認する個人を構成します。「アプリの追加」を参照してください。

ユーザーアカウントの管理者承認には、最大3つのレベルを割り当てることができます。他のユーザーにユーザーアカウントの承認を依頼する必要がある場合は、そのユーザーの名前またはメールアドレスを使用して検索し、選択できます。Citrix Endpoint Management がそのユーザーを見つけると、そのユーザーをワークフローに追加します。ワークフロー内のすべての個人は、新しいユーザーアカウントを承認または拒否するためのメールを受信します。

1. Citrix Endpoint Management コンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**Settings** ページが表示されます。
2. **Workflows** をクリックします。**Workflows** ページが表示されます。
3. **Add** をクリックします。**Add Workflow** ページが表示されます。

   ワークフロー管理(/en-us/citrix-endpoint-management/media/settings-workflows-add.png)
4. 次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **名前:** ワークフローの一意の名前を入力します。
- **説明:** 必要に応じて、ワークフローの説明を入力します。
- **メール承認テンプレート:** リストから、割り当てるメール承認テンプレートを選択します。メールテンプレートは、Citrix Endpoint Managementコンソールの**設定**にある**通知テンプレート**セクションで作成します。このフィールドの右側にある目のアイコンをクリックすると、構成しているテンプレートのプレビューが表示されます。
- **マネージャー承認レベル:** リストから、このワークフローに必要なマネージャー承認レベルの数を選択します。デフォルトは**1レベル**です。選択可能なオプションは次のとおりです。
  - 不要
  - 1レベル
  - 2レベル
  - 3レベル
- **Active Directoryドメインの選択:** リストから、ワークフローに使用する適切なActive Directoryドメインを選択します。
- **追加の必須承認者を見つける:** 検索フィールドに名前を入力し、**検索**をクリックします。名前はActive Directoryから取得されます。
- フィールドに名前が表示されたら、名前の横にあるチェックボックスを選択します。名前とメールアドレスは、**選択された追加の必須承認者**リストに表示されます。
  - リストから名前を削除するには、次のいずれかの操作を行います。
    - **検索**をクリックして、選択したドメイン内のすべてのユーザーのリストを表示します。
    - 検索ボックスに氏名または一部を入力し、**検索**をクリックして検索結果を絞り込みます。
    - **選択された追加の必須承認者**リストのユーザーには、検索結果リストの名前の横にチェックマークが付いています。リストをスクロールし、削除したい各名前の横にあるチェックボックスをオフにします。

5. **保存**をクリックします。作成されたワークフローは、**ワークフロー**ページに表示されます。

ワークフローを作成した後、ワークフローの詳細を表示したり、ワークフローに関連付けられているアプリを表示したり、ワークフローを削除したりできます。ワークフローを作成した後は、編集できません。異なる承認レベルまたは承認者を持つワークフローが必要な場合は、別のワークフローを作成してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ワークフローの詳細を表示および削除するには

1. **ワークフロー**ページで、既存のワークフローのリストから特定のワークフローを選択します。そのためには、テーブルの行をクリックするか、ワークフローの横にあるチェックボックスを選択します。
2. ワークフローを削除するには、**削除**をクリックします。確認ダイアログボックスが表示されます。もう一度**削除**をクリックします。

重要:

この操作は元に戻せません。

登録プロファイル

登録プロファイルでは、以下を指定します。

- Android、iOS、Windowsデバイスのデバイス管理登録オプション。
- AndroidおよびiOSデバイスのアプリ管理登録オプション。
- その他の登録オプション:
  - ユーザーが登録できるデバイスの数を制限するかどうか。

    デバイス制限に達した場合、デバイス登録制限を超過したことをユーザーに知らせるエラーメッセージが表示されます。
  - ユーザーがデバイス管理を拒否することを許可するかどうか。

登録プロファイルを使用すると、単一のCitrix Endpoint Managementコンソール内で複数のユースケースとデバイス移行パスを組み合わせることができます。いくつかのユースケースを次に示します。

- モバイルデバイス管理 (MDMのみ)
- MDM+モバイルアプリケーション管理 (MAM)
- MAMのみ
- 企業所有の登録
- BYOD登録 (MDM登録をオプトアウトする機能)
- Androidデバイス管理者登録からAndroid Enterprise登録への移行 (完全管理、ワークプロファイル、専用デバイス)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Windows向けCitrix WorkspaceアプリによるWindows 10およびWindows 11デバイスの自動登録（プレビュー）

現在のサイトがMDMのみで、MAMを追加したい場合は、NetScaler Gatewayを構成する必要があります。詳細については、「NetScaler Gatewayの要件」を参照してください。

デリバリーグループを作成するときは、Globalという名前のデフォルトの登録プロファイルを使用するか、別の登録プロファイルを指定できます。

プラットフォームごとの登録プロファイルの機能は次のとおりです。

- **Androidデバイスの場合:** 管理モードとデバイス所有者モードを指定します。例：会社所有デバイス、ワークプロファイルによる完全管理、BYODワークプロファイル。

  新しいデバイスは、デフォルトでAndroid Enterpriseに登録されます。レガシーのAndroidデバイス管理者（DA）モードを使用してデバイスを管理することもできます。新しいデバイスは、デフォルトでアプリ管理にも登録されます。

  セキュリティレベルと必要な登録手順の指定については、「ユーザーアカウント、役割、および登録」を参照してください。
- **iOSデバイスの場合:** デバイス管理の種類として、**Appleユーザー登録**、**Appleデバイス登録**、または**デバイスを管理しない**を指定します。この**Appleユーザー登録**モードは、パブリックプレビューとして利用可能です。この機能を有効にするには、サポートチームにお問い合わせください。

  Appleユーザー登録を選択した場合、Managed Apple IDにカスタムドメインを使用し、そのドメインを構成することを選択できます。

  新しいデバイスは、デフォルトでAppleデバイス管理に登録されます。新しいデバイスは、デフォルトでアプリ管理にも登録されます。
- **Windows 10およびWindows 11デバイスの場合:** Windows向けCitrix®デバイス管理を使用するかどうかを指定します。新しいデバイスは、デフォルトでデバイス管理に登録されます。

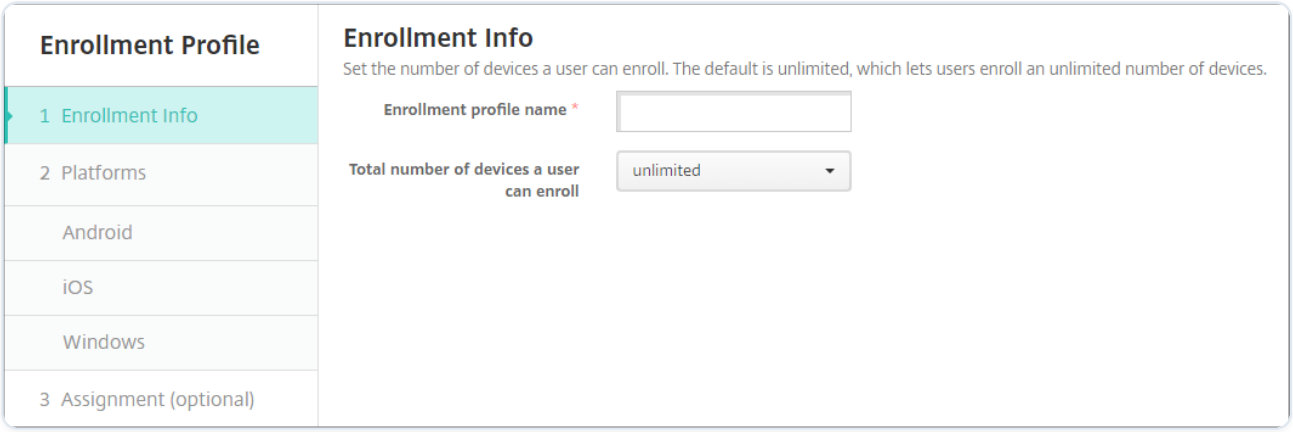
グローバル登録プロファイル

デフォルトの登録プロファイルはGlobalという名前です。Globalプロファイルは、登録プロファイルを作成する機会があるまでのテストに役立ちます。

Citrix Endpoint Management 20.2.1以降にオンボーディングする場合、グローバル登録プロファイルには事前定義された設定があります。以下のスクリーンショットは、グローバル登録プロファ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イルのデフォルト設定を示しています。MAMのみの展開では、これらのオプションの一部が表示されます。



Android用登録プロファイルページ(/en-us/citrix-endpoint-management/media/enrollment-profile-android.png)

iOS用登録プロファイルページ(/en-us/citrix-endpoint-management/media/enrollment-profile-ios.png)

Windows用登録プロファイルページ(/en-us/citrix-endpoint-management/media/enrollment-profile-windows.png)

登録プロファイル、デリバリーグループ、および登録

登録プロファイルとデリバリーグループは次のように連携します。

- 登録プロファイルを1つまたは複数のデリバリーグループに関連付けることができます。
- ユーザーが複数のデリバリーグループに属していて、それぞれ異なる登録プロファイルを持つ場合、デリバリーグループの名前によって使用される登録プロファイルが決まります。Citrix Endpoint Managementは、デリバリーグループのアルファベット順リストで最後に表示されるデリバリーグループを選択します。たとえば、次のような場合を想定します。
    - 「EP1」と「EP2」という名前の2つの登録プロファイル。
    - 「DG1」と「DG2」という名前の2つのデリバリーグループ。
    - 「DG1」は「EP1」に関連付けられています。
    - 「DG2」は「EP2」に関連付けられています。

    登録ユーザーが「DG1」と「DG2」の両方のデリバリーグループに属している場合、Citrix Endpoint Managementは「EP2」登録プロファイルを使用してユーザーの登録の種類を決定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 展開順序は、MDM（デバイス管理）用に登録プロファイルが構成されているデリバリーグループ内のデバイスにのみ適用されます。
- デバイスが登録された後、登録プロファイルに対する一部の変更には再登録が必要です。
  - MDM+MAMからMAMまたはMDM登録へデバイスをダウングレードするための構成の変更。ダウングレードは、登録プロファイルを更新したとき、またはデバイスを別のデリバリーグループに移動したときに発生する可能性があります。
  - MDM用に構成された登録プロファイルにMAMを追加する。
  - MAM用に構成された登録プロファイルにMDMを追加する。
- 別の登録プロファイルに切り替えても、既存の登録済みデバイスには影響しません。ただし、変更を有効にするには、ユーザーはそれらのデバイスの登録を解除してから再登録する必要があります。

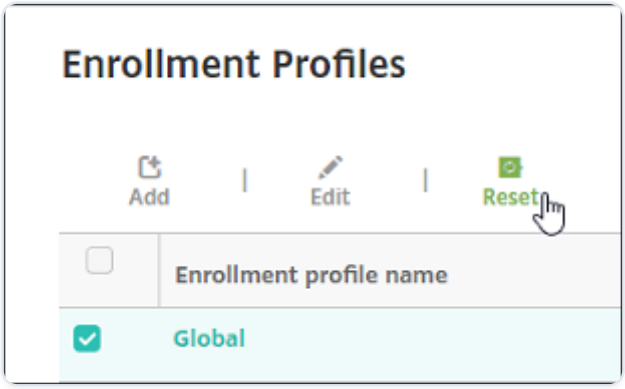
登録プロファイルを作成するには

1. Citrix Endpoint Managementコンソールで、 > の順に選択します。
2. ページで、プロファイルにわかりやすい名前を入力します。デフォルトでは、ユーザーは無制限のデバイスを登録できます。ユーザーあたりのデバイス数を制限する値を設定します。この制限は、ユーザーが登録するMAMまたはMDMで管理されているAndroid、iOS、およびWindowsデバイスの合計に適用されます。
3. プラットフォームページを完了します。プラットフォーム固有の登録設定については、以下を参照してください。
   - Android Enterprise: 登録プロファイルの作成
   - iOS: サポートされている登録方法
   - Windowsデスクトップおよびタブレット: サポートされている登録方法
4. ページで、1つ以上のデリバリーグループを登録プロファイルにアタッチします。

   ユーザーは、異なる登録プロファイルを持つ複数のデリバリーグループに属している場合があります。その場合、デリバリーグループの名前によって使用される登録プロファイルが決まります。Citrix Endpoint Managementは、デリバリーグループのアルファベット順リストで最後に表示されるデリバリーグループを選択します。デリバリーグループを作成するには、 > の順に選択します。

登録プロファイルのリストは、 > ページに表示されます。グローバルプロファイルを編集するか、元のデフォルトにリセットするには、グローバルプロファイルの行を選択して をクリックします。グローバルプロファイルを削除することはできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



通知

Citrix Endpoint Management の通知は、以下の目的で使用できます。

- いくつかのシステム関連機能について、特定のユーザーグループと通信するため。これらの通知は、特定のユーザーを対象にすることもできます。たとえば、iOS デバイスを持つすべてのユーザー、コンプライアンス違反のデバイスを持つユーザー、従業員所有デバイスを持つユーザーなどです。
- ユーザーとそのデバイスを登録するため
- 特定の条件が満たされたときに、ユーザーに自動的に通知するため (自動アクションを使用)。例:
  - コンプライアンスの問題により、ユーザーデバイスが企業ドメインからブロックされようとしている場合
  - デバイスがジェイルブレイクまたはルート化されている場合

自動アクションの詳細については、自動アクションを参照してください。

Citrix Endpoint Management で通知を送信するには、ゲートウェイと通知サーバーを構成する必要があります。Citrix Endpoint Management で通知サーバーをセットアップして、SMTP サーバーを構成できます。これらのサーバーはユーザーにメール通知を送信します。通知を使用して SMTP 経由でメッセージを送信できます。

- SMTP は、メール送信者がメール受信者と通信する、接続指向のテキストベースプロトコルです。メール送信者はコマンド文字列を発行し、通常は TCP 接続経由で必要なデータを提供します。SMTP セッションは、SMTP クライアント (メッセージを送信する人) によって開始されたコマンドと、SMTP サーバーからの対応する応答で構成されます。

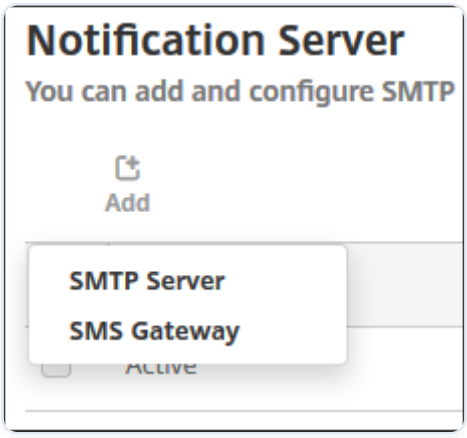
© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

- SMTP 通知サーバーを構成して、ユーザーにメッセージを送信します。サーバーが内部サーバーでホストされている場合は、システム管理者にお問い合わせください。サーバーがホスト型メールサービスである場合は、サービスプロバイダーの Web サイトで適切な構成情報を見つけてください。
- アクティブな SMTP サーバーは 1 つしか使用できません。この通信チャネルでは、アクティブな構成を 1 つしか許可しません。
- ネットワーク DMZ の Citrix Endpoint Management からポート 25 を開いて、内部ネットワーク上の SMTP サーバーに戻るようにします。これにより、Citrix Endpoint Management は通知を正常に送信できるようになります。

SMTP サーバーを構成する

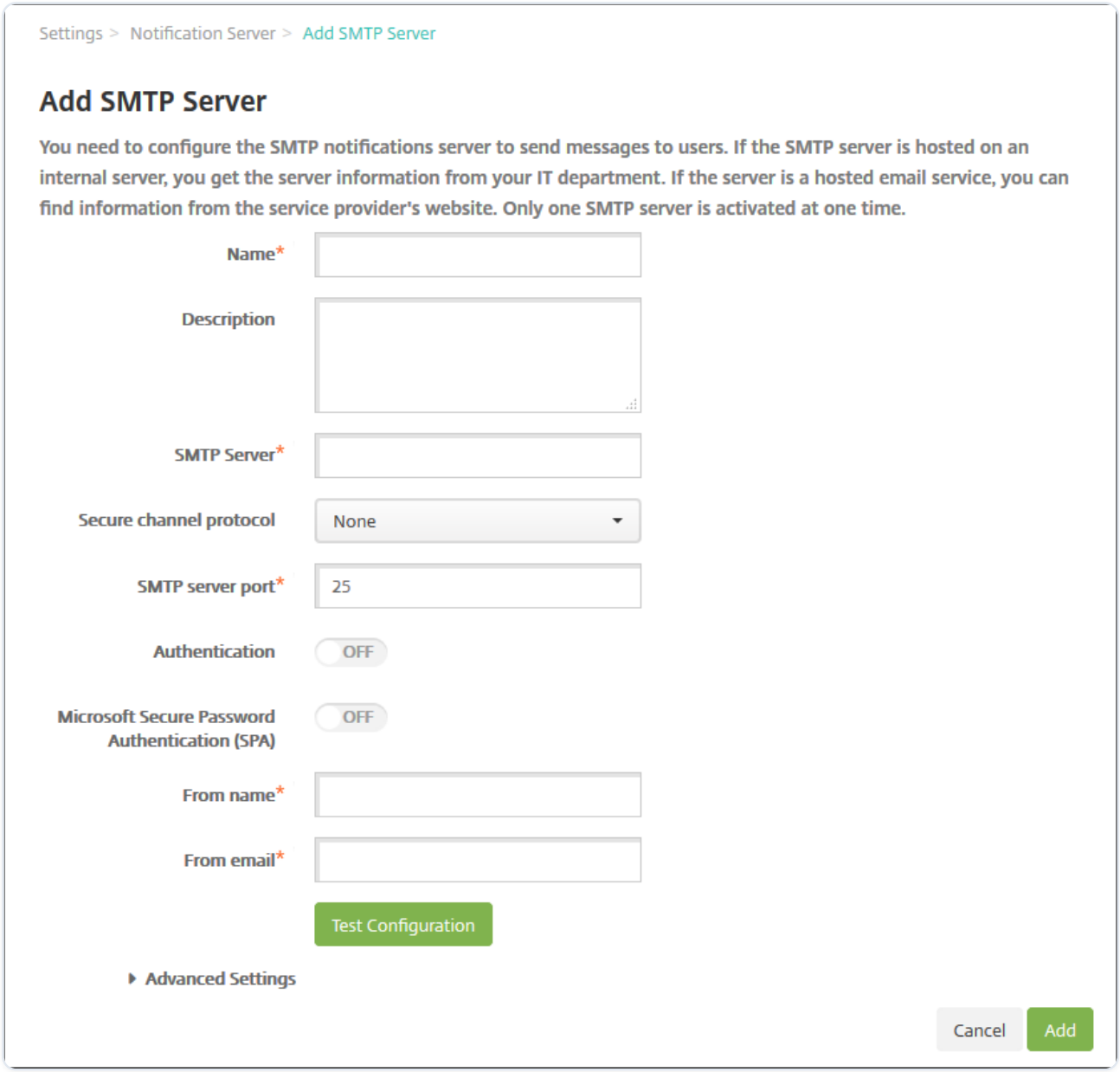
1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **通知**の下で、**通知サーバー**をクリックします。**通知サーバー**ページが表示されます。
3. **追加**をクリックします。SMTPサーバーを構成するためのオプションを含むメニューが表示されます。



   - SMTPサーバーを追加するには、**SMTPサーバー**をクリックし、この設定を構成する手順については、SMTPサーバーの追加を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SMTPサーバーの追加



1. これらの設定を構成します:

   - **名前:** このSMTPサーバーアカウントに関連付けられた名前を入力します。
   - **説明:** オプションで、サーバーの説明を入力します。
   - **SMTPサーバー:** サーバーのホスト名を入力します。完全修飾ドメイン名 (FQDN) またはIPアドレスのいずれかを指定します。
   - **セキュアチャネルプロトコル:** サーバーが使用するセキュアチャネルプロトコル (サーバーがセキュア認証を使用するように構成されている場合) のドロップダウンリストで、**SSL**、**TLS**、または**なし**をクリックします。デフォルトは**なし**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **SMTPサーバーポート:** SMTPサーバーが使用するポートを入力します。デフォルトでは、ポートは25に設定されています。SMTP接続でSSLセキュアチャネルプロトコルを使用する場合は、ポートを465に設定します。
- **認証: オン**または**オフ**を選択します。デフォルトは**オフ**です。
- **認証**を有効にする場合、これらの設定を構成します:
  - **ユーザー名:** 認証用のユーザー名を入力します
  - **パスワード:** 認証ユーザーのパスワードを入力します。

  重要:

  Microsoft Exchange Online で OAuth を使用するには、まず Microsoft Entra ID にアプリケーションを登録する 必要があります。登録後、**認証**と**Microsoft Exchange Online OAuth 2.0**を有効にします。

- **認証**と**Microsoft Exchange Online OAuth 2.0**を有効にする場合は、次の設定を構成します。
  - **ユーザー名:** 認証用のユーザー名を入力します。
  - **テナント ID:** Microsoft Entra ID ディレクトリのテナント ID を入力します。
  - **クライアント ID:** 登録済みアプリケーションのクライアント (アプリケーション) ID を入力します。これは、Azure portal > 登録済みアプリケーション > **アプリケーション (クライアント) ID** で確認できます。
  - **クライアント シークレット:** 登録済みアプリケーションのクライアント シークレットを入力します。これは、Azure portal > 登録済みアプリケーション > **証明書とシークレット** で確認できます。
- **Microsoft Secure Password Authentication (SPA):** SMTP サーバーが SPA を使用している場合は、**オン**をクリックします。デフォルトは**オフ**です。
- **差出人名:** クライアントがこのサーバーから通知メールを受信したときに、**差出人**ボックスに表示される名前を入力します。例: Corporate IT。
- **差出人メール:** メール受信者が SMTP サーバーから送信された通知に返信する場合に使用されるメールアドレスを入力します。

2. **構成のテスト**をクリックして、テストメール通知を送信します。
3. **詳細設定**を展開し、次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **SMTP 再試行回数:** SMTP サーバーから送信された失敗したメッセージを再試行する回数を入力します。デフォルトは 5 です。
- **SMTPタイムアウト:** SMTPリクエストの送信時に待機する期間（秒単位）を入力します。タイムアウトが原因でメッセージ送信が継続的に失敗する場合は、この値を増やしてください。この値を減らすと、タイムアウトして未配信のメッセージ数が増加する可能性があるため、注意してください。デフォルトは30秒です。
- **SMTP受信者の最大数:** SMTPサーバーによって送信されるメールメッセージあたりの受信者の最大数を入力します。デフォルトは100です。

4. **追加**をクリックします。

通知テンプレートの作成と更新

Citrix Endpoint Managementでは、自動アクション、登録、およびユーザーに送信される標準通知メッセージで使用する通知テンプレートを作成または更新できます。通知テンプレートは、Citrix Secure HubまたはSMTPの2つの異なるチャネルを介してメッセージを送信するように構成します。

Citrix Endpoint Managementには、多くの事前定義された通知テンプレートが含まれています。これらのテンプレートは、システム内のすべてのデバイスに対してCitrix Endpoint Managementが自動的に応答するイベントの異なるタイプを反映しています。

注：

SMTPチャネルを使用してユーザーに通知を送信する予定がある場合は、チャネルをアクティブ化する前に設定する必要があります。Citrix Endpoint Managementは、通知テンプレートを追加する際に、チャネルがまだ設定されていない場合に設定を促します。

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **通知テンプレート**をクリックします。**通知テンプレート**ページが表示されます。

   設定通知テンプレート(/en-us/citrix-endpoint-management/media/settings-notification-templates.png)

通知テンプレートの追加

1. **追加**をクリックします。SMTPサーバーが設定されていない場合、SMTP通知の使用に関するメッセージが表示されます。SMTPサーバーを今すぐ設定するか、後で設定するかを選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SMTPサーバー設定を今すぐ設定することを選択した場合、**設定**ページの**通知サーバー**ページにリダイレクトされます。使用したいチャネルを設定した後、**通知テンプレート**ページに戻り、通知テンプレートの追加または変更を続行できます。

重要：

SMTPサーバー設定を後でセットアップすることを選択した場合、通知テンプレートを追加または編集するときにそれらのチャネルをアクティブにすることはできません。結果として、それらのチャネルはユーザー通知の送信に利用できません。

2. 以下の設定を構成します。

- **名前:** テンプレートのわかりやすい名前を入力します。
- **説明:** テンプレートの説明を入力します。
- **種類:** ドロップダウンリストで通知の種類をクリックします。選択した種類でサポートされているチャネルのみが表示されます。APNS証明書有効期限テンプレートは1つのみ許可されており、これは事前定義されたテンプレートです。この種類のテンプレートを追加することはできません。

注:

一部のテンプレートの種類では、種類のすぐ下に「手動送信がサポートされています」というフレーズが表示されます。これらのテンプレートの種類は、**ダッシュボード**の**通知**リストおよび**デバイス**ページで利用できます。これらの場所から、ユーザーに手動で通知を送信できます。件名またはメッセージフィールドで以下のマクロを使用するテンプレートでは、手動送信は利用できません。

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

注:

Citrix Endpoint Managementコンソールには、「blacklist」と「whitelist」という用語が含まれています。今後のバージョンでは、これらの用語を「block list」と「allow list」に変更する予定です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **チャネル**の下で、この通知で使用する各チャネルの情報を構成します。任意のチャネルまたはすべてのチャネルを選択できます。選択するチャネルは、通知を送信する方法によって異なります。

   - **Citrix Secure Hub**を選択した場合、iOSおよびAndroidデバイスのみが通知を受け取り、それらはデバイスの通知トレイに表示されます。
   - **SMTP**を選択した場合、メールアドレスで登録したユーザーがメッセージを受信します。

   シトリックス セキュア ハブ:

   - **アクティブ化:** 通知チャネルを有効にするには、クリックします。
   - **メッセージ:** ユーザーに送信するメッセージを入力します。Citrix Secure Hub を使用している場合、このフィールドは必須です。メッセージでのマクロの使用については、「マクロ」を参照してください。
   - **サウンドファイル:** リストで、通知が受信されたときにユーザーが聞く通知サウンドをクリックします。

   SMTP:

   - **アクティブ化:** 通知チャネルを有効にするには、クリックします。

     SMTPサーバーを設定した後にのみ、SMTP通知をアクティブ化できます。
   - **送信者:** 通知のオプションの送信者を入力します。送信者は、名前、メールアドレス、またはその両方です。
   - **受信者:** このフィールドには、アドホック通知を除くすべての通知に対して、通知が正しいSMTP受信者アドレスに送信されるようにするための事前構築済みマクロがあります。Citrixは、テンプレート内のマクロを変更しないことを推奨します。このフィールドにアドレスを追加することで、さらに受信者（企業管理者など）を追加できます。マクロと他のアドレスを区切るには、セミコロン (;) を使用します。アドホック通知を送信するには、特定の受信者を入力するか、**管理 > デバイス**ページからデバイスを選択して、そこから通知を送信できます。詳細については、「デバイス」を参照してください。
   - **件名:** 通知のわかりやすい件名を入力します。このフィールドは必須です。
   - **メッセージ:** ユーザーに送信するメッセージを入力します。メッセージでのマクロの使用については、「マクロ」を参照してください。

4. **追加**をクリックします。すべてのチャネルが正しく構成されると、**通知テンプレート**ページにSMTPとCitrix Secure Hubの順で表示されます。正しく構成されていないチャネルは、正しく構成されたチャネルの後に表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

通知テンプレートを編集する

1. 通知テンプレートを選択します。そのテンプレートに固有の編集ページが表示されます。**種類**フィールドを除き、テンプレートを編集したり、チャネルをアクティブ化または非アクティブ化したりできます。
2. **保存**をクリックします。

通知テンプレートを削除する

追加した通知テンプレートのみ削除できます。定義済みの通知テンプレートは削除できません。

1. 既存の通知テンプレートを選択します。
2. **削除**をクリックします。確認ダイアログボックスが表示されます。
3. 通知テンプレートを削除するには、**削除**をクリックするか、通知テンプレートの削除をキャンセルするには、**キャンセル**をクリックします。

RBACでロールを構成する

Citrix Endpoint Managementのロールベースのアクセス制御 (RBAC) 機能を使用すると、ユーザーとグループにロールを割り当てることができます。ロールは、ユーザーがシステム機能にアクセスできるレベルを制御する一連の権限です。

Citrix Endpoint Managementには、以下のデフォルトのユーザーロールが付属しています。デフォルトのロールをテンプレートとして使用し、カスタマイズして独自のユーザーロールを作成できます。

- **管理者:** システムへのフルアクセスを許可します。
- **ユーザー:** ユーザーがデバイスを登録し、セルフヘルプポータルにアクセスできるようにします。

Citrix Endpoint ManagementのRBAC機能を使用して、次のことができます。

- ユーザーロールを作成および編集する。
- ローカルユーザーグループおよびActive Directory (AD) グループにロールを割り当てる。
- Citrix Cloudの**IDおよびアクセス管理 > 管理者**を通じて、Citrix Cloudの管理者にロールを割り当てます。を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RBAC機能を使用する

ローカルユーザー、クラウド管理者 (Citrix Cloud内)、ローカルユーザーグループ、およびActive Directoryグループにロールを割り当てることができます。

- **ローカルユーザー: 管理 > ユーザー**を使用して、ローカルユーザーにロールを割り当てます。ローカルユーザーには1つのロールのみを割り当てることができます。ロールを変更するには、ユーザーアカウントを手動で編集します。または、ローカルユーザーのグループを作成し、そのグループにロールを割り当てることもできます。
- **クラウド管理者:** クラウド管理者は、管理者がCitrix Cloudのお客様アカウントに追加されたときにCitrix Cloudが作成する特別なユーザーアカウントです。クラウド管理者アカウントは、Citrix Cloud上の管理者アカウントと同じユーザー名を使用します。Citrix Endpoint ManagementコンソールでRBACロールを作成し、Citrix Cloudの**IDおよびアクセス管理 > 管理者**を通じてこれらのユーザーにロールを割り当てます。
- **Active Directoryグループ:** Active Directoryグループ内のすべてのユーザーは同じ権限を持ちます。ユーザーが複数のActive Directoryグループに属している場合、すべての権限が結合されてそのユーザーの権限が定義されます。たとえば、ADGroupAのユーザーがマネージャーのデバイスを特定でき、ADGroupBのユーザーが従業員のデバイスをワイプできるとします。両方のグループに属するユーザーは、マネージャーと従業員の両方のデバイスを特定およびワイプできます。競合する権限を持つグループにユーザーが属している場合、許可された権限が優先されます。

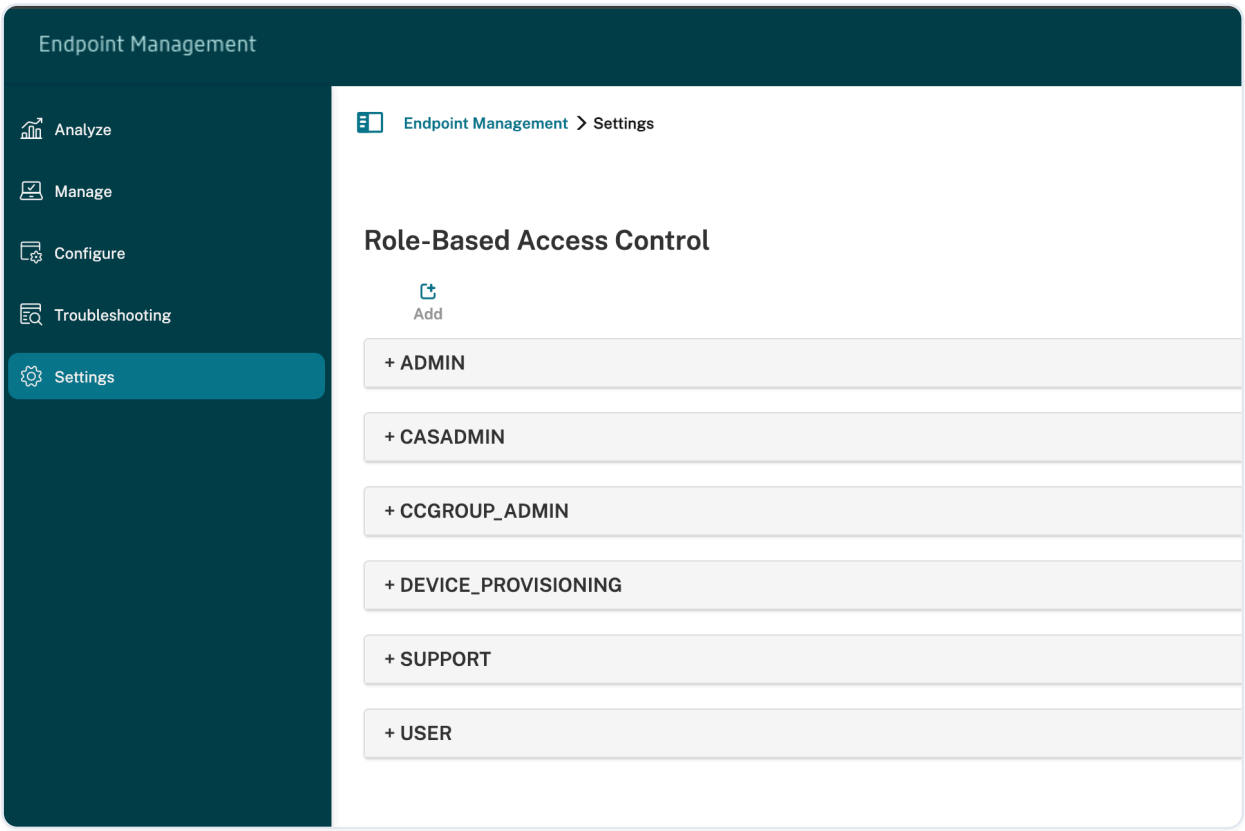
詳細については、「ユーザーアカウントについて」を参照してください。

役割の作成または編集

1. Citrix Endpoint Managementコンソールで、**設定**ページにアクセスするには、右上隅にある歯車アイコンをクリックします。
2. **役割ベースのアクセス制御**をクリックします。**役割ベースのアクセス制御**ページには、デフォルトのユーザー役割と追加した役割が表示されます。

   役割の横にあるプラス記号（+）をクリックすると、その役割のすべての権限が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 役割を追加するには、**追加**をクリックします。または、役割を編集するには、既存の役割の右側にあるペンアイコンをクリックします。

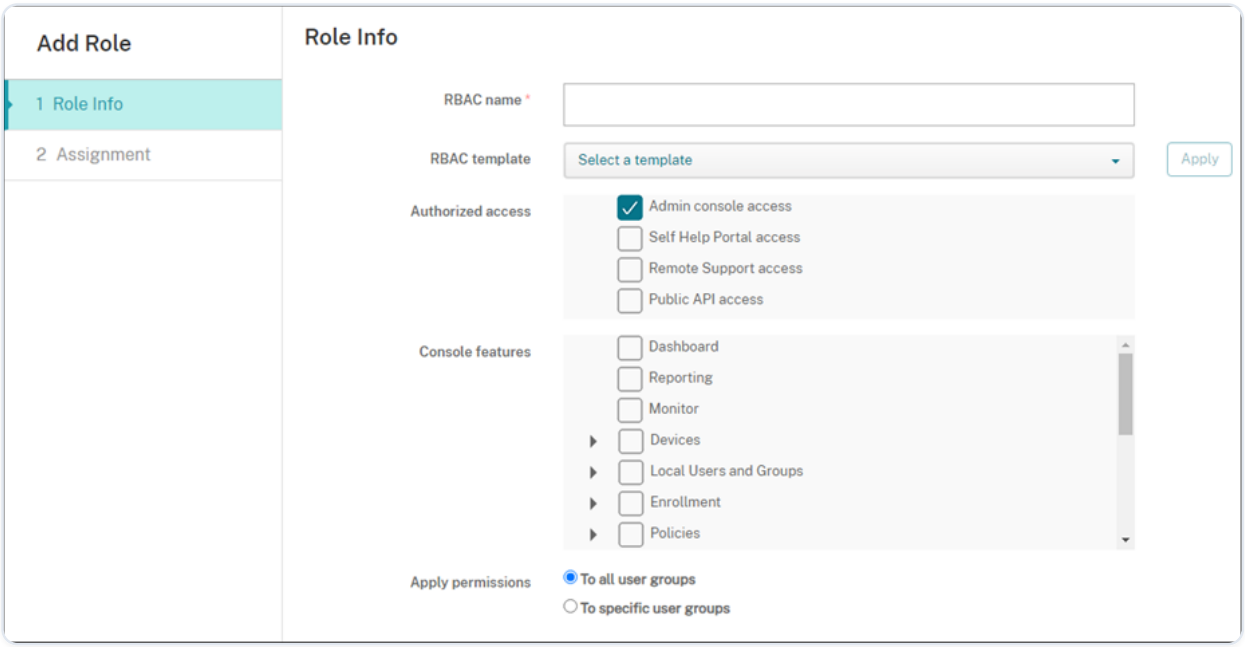
> **注：**
>
> 定義した役割の右側にあるゴミ箱アイコンをクリックすると、役割を削除できます。デフォルトのユーザー役割は削除できません。

4. **役割の追加**ページで、次の情報を入力します。

   - **RBAC名：** 新しいユーザー役割のわかりやすい名前を入力します。既存の役割の名前は変更できません。
   - **RBACテンプレート：** オプションで、新しい役割の開始点としてテンプレートを選択します。（役割を編集している場合、テンプレートを選択または変更することはできません。）RBACテンプレートは、システム機能へのアクセスを定義するデフォルトのユーザー役割です。

   適用ボタンをクリックして、**承認済みアクセス**と**コンソール機能**のチェックボックスに情報を入力します。Citrix Endpoint Managementは、選択したテンプレートの事前定義されたアクセス権と機能権限でこれらのフィールドを埋めます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 役割をカスタマイズするには、**承認済みアクセス**と**コンソール機能**のチェックボックスを選択またはクリアします。

   コンソール機能の横にある三角形をクリックすると、その機能に固有の権限が表示され、選択できます。トップレベルのチェックボックスをクリックしても、個々の権限は選択されません。トップレベルの権限を展開した後、個々のオプションを選択してください。

6. **権限を適用:**「**特定のユーザーグループに**」をクリックして、選択したグループに権限を適用します。

   例えば、RBAC管理者がActiveDirectoryユーザーグループへの権限を持っている場合：

   - 管理者は、ActiveDirectoryグループに属しているユーザーの情報のみにアクセスできます。
   - 管理者は、他のローカルユーザーやADユーザーを表示できません。管理者は、それらのグループのいずれかの子グループのメンバーであるユーザーを表示できます。
   - 管理者は、次の宛先に招待を送信できます。
     - 権限グループとその子グループ
     - 権限グループとその子グループのメンバーであるユーザー

   シトリックス エンドポイント マネジメント RBAC 構成(/en-us/citrix-endpoint-management/media/rbac-apply-permissions.png)

7. 「**次へ**」をクリックし、以下の情報を入力してユーザーグループに役割を割り当てます。

   シトリックス エンドポイント マネジメント RBAC 構成(/en-us/citrix-endpoint-management/media/rbac-assignment-page.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ドメインの選択:** リストからドメインを選択します。
- **ユーザーグループの検索:** 「**検索**」をクリックして、利用可能なすべてのグループのリストを表示します。検索を絞り込むには、グループ名の全部または一部を入力します。
- **ユーザーグループを含める:** 表示されるリストで、役割を割り当てるユーザーグループを選択します。

8. 「**保存**」をクリックします。

Citrix Cloud管理者への役割の追加

Citrix Endpoint Managementコンソールを介してCitrix Cloud管理者にRBACロールを割り当てる代わりに、Citrix Cloudコンソールからロールを割り当てます。

1. Citrix Cloudコンソールで、 **>** に移動します。
2. IDプロバイダーを選択し、メールアドレスを入力して管理者を追加します。 をクリックします。

   既存の管理者行の末尾にある をクリックして、それらの権限を編集します。
3. をクリックします。管理者に権限を割り当てる際に、Citrix Endpoint Managementコンソールで作成されたRBACロールを選択できます。

   Citrix CloudのRBACロール(/en-us/citrix-endpoint-management/media/rbac-roles-citrix-cloud.png)
4. 新しい管理者に招待を送信するには をクリックし、管理者の編集を完了するには をクリックします。

事前定義されたロール

各事前定義されたRBACロールには、特定の関連するアクセス権と機能権限があります。以下の表では、管理者ロールとユーザーロールの各権限について説明します。事前定義されたロールを削除または編集することはできません。

- 各組み込みロールのデフォルト権限の完全なリストについては、ロールベースのアクセス制御のデフォルト をダウンロードしてください。
- Citrix Endpoint Managementユーザーアカウントの詳細については、ユーザーアカウントについて を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

設定権限の下で、RBAC権限は管理者ユーザーに、自身の権限を割り当てる機能を含む完全なアクセス権を与えます。このアクセス権は、Citrix Endpoint Managementシステム内のすべてを操作する能力を与えることを意図しているユーザーにのみ付与してください。

管理者ロール

事前定義された管理者ロールは、Citrix Endpoint Managementで特定のアクセスを提供します。デフォルトでは、 (セルフヘルプポータルを除く)、、および が有効になっています。

「**管理 > ユーザー**」を使用して、管理者ロールが割り当てられているローカルユーザーのロールを変更できます。管理者ロールを持つクラウドユーザーの場合は、Citrix Cloudコンソールを使用してロールを変更します。デフォルトでは、管理者ロールを持つクラウドユーザーとローカルユーザーはフルアクセス権を持っています。

管理者向けの承認済みアクセス

管理コンソールへのアクセス	管理者は、Citrix Endpoint Managementコンソールのすべての機能にアクセスできます。
セルフヘルプポータルへのアクセス	デフォルトでは、管理者はセルフヘルプポータルにアクセスできません。（(/ja-jp/citrix-endpoint-management/users/rbac-roles-and-permissions.html#user-role)を持つユーザーは、セルフヘルプポータルのみにアクセスできます。）
リモートサポートへのアクセス	管理者はリモートサポート機能にアクセスできます。
パブリックAPIへのアクセス	管理者は、Citrix Endpoint Managementコンソールで利用可能なアクションをプログラムで実行するために、パブリックAPIにアクセスできます。これらのアクションには、証明書、アプリ、デバイス、デリバリーグループ、およびローカルユーザーの管理が含まれます。

管理者向けのコンソール機能

管理者は、Citrix Endpoint Managementコンソールへの無制限のアクセス権を持っています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ダッシュボード	**ダッシュボード**は、管理者がCitrix Endpoint Managementコンソールにログオンした後に最初に表示されるページです。**ダッシュボード**には、通知とデバイスに関する基本情報が表示されます。
レポート	「**分析 > レポート**」ページでは、アプリとデバイスの展開を分析できる事前定義レポートが提供されます。
デバイス	「**管理 > デバイス**」ページでは、ユーザーデバイスを管理します。このページで個々のデバイスを追加したり、デバイスプロビジョニングファイルをインポートして複数のデバイスを一度に追加したりできます。
ローカルユーザーとグループ	「**管理 > ユーザー**」ページでは、ローカルユーザーとローカルユーザーグループを追加、編集、または削除できます。
登録	「**管理 > 登録招待**」ページでは、ユーザーがCitrix Endpoint Managementにデバイスを登録するよう招待する方法を管理します。
ポリシー	「**構成 > デバイスポリシー**」ページでは、VPNやネットワークなどのデバイスポリシーを管理します。
アプリ	「**構成 > アプリ**」ページでは、ユーザーがデバイスにインストールできるさまざまなアプリを管理します。
メディア	「**構成 > メディア**」ページでは、ユーザーがデバイスにインストールできるさまざまなメディアを管理します。
アクション	「**構成 > アクション**」ページでは、トリガーイベントへの応答を管理します。
デリバリーグループ	**[構成] > [デリバリーグループ]** ページでは、デリバリーグループとそれに関連付けられているリソースを管理します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

登録プロファイル	**[構成] > [登録プロファイル]** ページでは、ユーザーがデバイスを登録する方法を指定します。
ビジネス向けAlexa	**[設定]** ページでは、Alexa for Business プロファイルを管理します。
設定	**[設定]** ページでは、クライアントおよびサーバーのプロパティ、証明書、資格情報プロバイダーなどのシステム設定を管理します。**重要:** これらの設定には、RBAC 権限が含まれます。RBAC 権限は、管理者自身に権限を割り当てる機能を含め、管理者へのフルアクセスを許可します。このアクセスは、Citrix Endpoint Management システム内のすべてを操作する権限を付与する意図のあるユーザーにのみ付与してください。
サポート	**[トラブルシューティングとサポート]** ページでは、診断の実行やログの生成などのトラブルシューティング活動を行います。

管理者向けのデバイス制限

管理者は、デバイス制限の設定、デバイスへの通知の設定と送信、デバイス上のアプリの管理などによって、コンソール全体でデバイス機能にアクセスします。

デバイスの完全ワイプ	デバイスからすべてのデータとアプリを消去します。デバイスにメモリカードがある場合は、メモリカードも消去されます。
制限のクリア	1つ以上のデバイス制限を削除します。
デバイスの選択的ワイプ	デバイスからすべての企業データとアプリを消去し、個人データとアプリはそのまま残します。
位置の表示	デバイスの位置を確認し、地理的制限を設定します。含まれるもの: デバイスの検索、デバイスの追跡。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスのロック	ユーザーがデバイスを使用できないように、デバイスをリモートでロックします。
デバイスのロック解除	ユーザーがデバイスを使用できるように、デバイスをリモートでロック解除します。
コンテナのロック	デバイス上の企業コンテナをリモートでロックします。
コンテナのロック解除	デバイス上の企業コンテナをリモートでロック解除します。
コンテナパスワードのリセット	企業コンテナのパスワードをリセットします。
ASM/アクティベーションロックのバイパスを有効にする	アクティベーションロックが有効になっている監視対象のiOSデバイスにバイパスコードを保存します。デバイスを消去するには、このコードを使用してアクティベーションロックを自動的に解除します。
常駐ユーザーの取得	現在のデバイスでアクティブなアカウントを持つユーザーを一覧表示します。この操作により、デバイスとCitrix Endpoint Managementコンソールの間で強制的に同期が行われます。
常駐ユーザーのログアウト	現在のユーザーを強制的にログアウトします。
常駐ユーザーの削除	特定のユーザーの現在のセッションを削除します。ユーザーは再度サインインできます。
デバイスを鳴らす	Windowsデバイスをリモートで5分間、最大音量で鳴らします。
デバイスの再起動	Citrix Endpoint ManagementコンソールからWindowsデバイスを再起動します。
デバイスへの展開	アプリ、通知、制限、その他のリソースをデバイスに送信します。
デバイスの編集	デバイスの設定を変更します。
デバイスへの通知	デバイスに通知を送信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスの追加/削除	Citrix Endpoint Managementからデバイスを追加または削除します。
デバイスのインポート	ファイルからデバイスのグループをCitrix Endpoint Managementにインポートします。
デバイステーブルのエクスポート	デバイスページからデバイス情報を収集し、.csvファイルにエクスポートします。
デバイスの取り消し	デバイスがCitrix Endpoint Managementに接続するのを禁止します。
アプリロック	デバイス上のすべてのアプリへのアクセスを拒否します。Androidでは、この制限によりユーザーはCitrix Endpoint Managementにサインインできません。iOSでは、ユーザーはサインインできますが、アプリにアクセスできません。
アプリのワイプ	Androidでは、この制限によりユーザーのCitrix Endpoint Managementアカウントが削除されます。iOSでは、この制限によりユーザーがCitrix Endpoint Management機能にアクセスするために必要な暗号化キーが削除されます。
ソフトウェアインベントリの表示	デバイスにインストールされているソフトウェアを確認します。
AirPlayミラーリングを要求	AirPlayストリーミングの開始を要求します。
AirPlayミラーリングを停止	AirPlayストリーミングを停止します。
紛失モードを有効にする	**管理 > デバイス**ページで、監視対象デバイスを紛失モードに設定して、ロック画面で監視対象デバイスをブロックできます。これにより、デバイスが紛失または盗難されたときにデバイスを特定できます。
紛失モードを無効にする	**管理 > デバイス**ページで、紛失モードに設定されているデバイスの紛失モードを無効にできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OSアップデートデバイス	デバイスにOSアップデートデバイスポリシーを展開できます。
デバイスのシャットダウン	Citrix Endpoint Managementコンソールから iOSデバイスをシャットダウンします。
デバイスの再起動	Citrix Endpoint Management コンソールから iOSデバイスを再起動します。
デバイス登録証明書の更新	デバイスCA証明書を更新します。

ローカルユーザーとグループ

管理者は、Citrix Endpoint Management の **>** ページでローカルユーザーとローカルユーザーグループを管理します。

ローカルユーザーの追加
ローカルユーザーの削除
ローカルユーザーの編集
ローカルユーザーのインポート
ローカルユーザーのエクスポート
ローカルユーザーグループ
ローカルユーザーロックIDの取得
ローカルユーザーロックの削除

登録

管理者は、登録招待の追加と削除、ユーザーへの通知の送信、登録テーブルの.csvファイルへのエクスポートを行うことができます。

登録の追加/削除	ユーザーまたはユーザーグループへの登録招待を追加または削除します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーに通知	ユーザーまたはユーザーグループに登録招待を送信します。
登録招待テーブルのエクスポート	登録ページから登録情報を収集し、.csvファイルにエクスポートします。

ポリシー

ポリシーの追加/削除	デバイスまたはアプリのポリシーを追加または削除します。
ポリシーの編集	デバイスまたはアプリのポリシーを変更します。
ポリシーのアップロード	デバイスまたはアプリのポリシーをアップロードします。
ポリシーのクローン作成	デバイスまたはアプリのポリシーをコピーします。
ポリシーの無効化	既存のアプリポリシーを無効にします。
ポリシーのエクスポート	デバイスポリシーページからデバイスポリシー情報を収集し、.csvファイルにエクスポートします。
ポリシーの割り当て	1つ以上のデリバリーグループにデバイスポリシーを割り当てます。

アプリ

管理者は、Citrix Endpoint Managementの**構成 > アプリ**ページでアプリを管理します。

アプリストアまたはエンタープライズアプリの追加/削除	パブリックアプリストアアプリまたはエンタープライズアプリ（MDX対応ではないもの）を追加または削除します。
アプリストアまたはエンタープライズアプリの編集	パブリックアプリストアアプリまたはエンタープライズアプリ（MDX対応ではないもの）を変更します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDX、Web、およびSaaSアプリの追加/削除	MDX対応アプリ、社内ネットワークからのアプリ（Webアプリ）、またはパブリックネットワークからのアプリ（SaaS）をCitrix Endpoint Managementに追加または削除します。
MDX、Web、およびSaaSアプリの編集	MDX対応アプリ、社内ネットワークのアプリ（Webアプリ）、またはパブリックネットワークのアプリ（SaaS）をCitrix Endpoint Managementに変更します。
カテゴリの追加/削除	アプリがアプリストアに表示されるカテゴリを追加または削除します。
パブリック/エンタープライズアプリをデリバリーグループに割り当てる	パブリックアプリストアのアプリまたはMDX対応アプリを、展開のためにデリバリーグループに割り当てます。
MDX/WebLink/SaaSアプリをデリバリーグループに割り当てる	MDX対応、シングルサインオン不要（WebLink）、またはパブリックネットワーク（SaaS）のアプリをデリバリーグループに割り当てます。
アプリテーブルのエクスポート	アプリページからアプリ情報を収集し、.csvファイルにエクスポートします。

メディア

パブリックアプリストアまたはボリューム購入ライセンスからのメディアを管理します。

アプリストアまたはエンタープライズブックの追加/削除
パブリック/エンタープライズブックをデリバリーグループに割り当てる
アプリストアまたはエンタープライズブックの編集

アクション

アクションの追加/削除	トリガーと関連する応答によって定義されたアクションを追加または削除します。トリガーとは、イベント、デバイスまたはユーザーの

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	プロパティ、あるいはインストールされているアプリ名のことです。
アクションの編集	トリガーと関連する応答によって定義されたアクションを変更します。トリガーとは、イベント、デバイスまたはユーザーのプロパティ、あるいはインストールされているアプリ名のことです。
アクションをデリバリーグループに割り当てる	ユーザーデバイスに展開するために、アクションをデリバリーグループに割り当てます。
アクションのエクスポート	[アクション] ページからアクション情報を収集し、.csv ファイルにエクスポートします。

デリバリーグループ

管理者は、 **>** ページからデリバリーグループを管理します。

デリバリーグループの追加/削除	指定されたユーザーとオプションのポリシー、アプリ、アクションを追加するデリバリーグループを作成または削除します。
デリバリーグループの編集	既存のデリバリーグループを変更します。これにより、ユーザーとオプションのポリシー、アプリ、アクションが変更されます。
デリバリーグループの展開	デリバリーグループを使用可能にする。
デリバリーグループのエクスポート	デリバリーグループページからデリバリーグループ情報を収集し、.csvファイルにエクスポートします。

登録プロファイル

登録プロファイルを管理します。

登録プロファイルの追加/削除
登録プロファイルの編集

© 1997–2026 Citrix Systems, Inc. All rights reserved.

登録プロファイルをデリバリーグループに割り当てる

ビジネス向けALEXA

Alexa for Businessプロファイルを管理します。

ルームの追加/削除/編集
ルームプロファイルの追加/削除/編集
スキルグループの追加/削除/編集

管理者向け設定

管理者は、**設定**ページでさまざまな設定を構成します。

RBAC	RBAC割り当て。**重要:** この権限は、管理者自身に権限を割り当てる機能を含め、管理者に対してフルアクセスを許可します。このアクセスは、Citrix Endpoint Managementシステム内のすべてを操作する権限を与えることを意図しているユーザーにのみ付与してください。
LDAP	Active DirectoryなどのLDAP準拠ディレクトリを1つ以上管理し、グループ、ユーザーアカウント、および関連プロパティをインポートします。
登録	ユーザーおよびセルフヘルプポータル向けに登録セキュリティモードを有効にします。
リリース管理	現在インストールされているリリースを表示します。含まれるもの: リリース管理の更新
証明書	APNS証明書の編集
通知テンプレート	自動アクション、登録、およびユーザーへの標準通知メッセージ配信で使用する通知テンプレートを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ワークフロー	アプリ構成で使用するユーザーアカウントの作成、承認、および削除を管理します。
資格情報プロバイダー	デバイス証明書の発行を許可された1つ以上の資格情報プロバイダーを追加します。資格情報プロバイダーは、証明書の形式と、証明書の更新または失効の条件を制御します。
PKIエンティティ	公開キーインフラストラクチャエンティティ（汎用、Microsoft Certificate Services、または裁量CA）を管理します。
PKI接続のテスト	**設定 > PKIエンティティ**ページで**接続のテスト**ボタンを使用して、サーバーにアクセスできることを確認します。
クライアントプロパティ	パスコードの種類、強度、有効期限など、ユーザーデバイス上のさまざまなプロパティを管理します。
クライアントサポート	ユーザーがサポートサービスに連絡する方法（メール、電話、またはサポートチケットメール）を設定します。
クライアントブランディング	アプリストアのカスタムストア名とデフォルトストアビューを作成します。アプリストアまたはCitrix Secure Hubに表示されるカスタムロゴを追加します。
キャリアSMSゲートウェイ	キャリアSMSゲートウェイを設定して、Citrix Endpoint ManagementがキャリアSMSゲートウェイを介して送信する通知を構成します。
通知サーバー	SMTPゲートウェイサーバーを設定して、ユーザーにメールを送信します。
ActiveSync ゲートウェイ	ルールとプロパティを通じて、ユーザーとデバイスへのユーザーアクセスを管理します。
グーグル クローム	Citrix Endpoint ManagementがGoogle Workspaceアカウントと通信するように構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apple デプロイメントプログラム	Citrix Endpoint ManagementにApple Deployment Programアカウントを追加します。
Apple Configuratorデバイス登録	Citrix Endpoint Managementコンソールで Apple Configuratorの設定を構成します。
iOS/ボリューム購入設定	Apple Volume Purchaseアカウントを追加します。
ネットスケーラー ゲートウェイ	Citrix Endpoint ManagementでNetScaler Gateway（現在はNetScaler Gatewayに名称変更）の設定を構成します。
ネットワークアクセスコントロール	デバイスが非準拠であると判断され、ネットワークにアクセスできないようにする条件を設定します。
サーバープロパティ	サーバープロパティを追加または変更します。すべてのノードでCitrix Endpoint Managementを再起動する必要があります。
バーチャル アプリおよびデスクトップ	ユーザーがCitrix Workspaceアプリを介してCitrix Virtual Apps and Desktopsを追加できるようにします。
シトリックス ファイル	EnterpriseアカウントでCitrix Endpoint Managementを使用する場合: ユーザーアカウント管理のためにShareFileおよび管理者サービスアカウントに接続する設定を構成します。既存のCitrix Filesドメインと管理者資格情報が必要です。ストレージゾーンコネクタでCitrix Endpoint Managementを使用する場合: ストレージゾーンコネクタで定義されているネットワーク共有とSharePointの場所にCitrix Endpoint Managementが接続するように構成します。
アンドロイド エンタープライズ	Android Enterpriseサーバー設定を構成します。
IDプロバイダー (IdP)	IDプロバイダーを構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス エンドポイント マネジメント ツール	Citrix Endpoint Managementツールページにアクセスします。
Windows一括登録	Windows一括登録設定を構成します。

サポート

管理者はさまざまなサポートタスクを実行できます。

NetScaler® Gateway 接続チェック	IPアドレスでNetScaler Gatewayの様々な接続チェックを実行します。ユーザー名とパスワードが必要です。
Citrix Endpoint Management 接続チェック	データベース、DNS、Google Planなど、選択したCitrix Endpoint Management機能の接続チェックを実行します。
Citrix製品ドキュメント	公開されているCitrix Endpoint Managementドキュメントサイトにアクセスします。
Citrix ナレッジセンター	Citrixサポートサイトにアクセスして、ナレッジベース記事を検索します。
ログ	ログファイルを表示およびダウンロードします。
マクロ	プロファイル、ポリシー、通知、または登録テンプレートのテキストフィールドに、ユーザーまたはデバイスのプロパティデータを入力します。単一のポリシーを構成し、そのポリシーを大規模なユーザーベースに展開し、ターゲットとなる各ユーザーにユーザー固有の値を表示させます。
PKI構成	PKI構成情報をインポートおよびエクスポートします。
APNS署名ユーティリティ	Apple Push Network signing (APNs) 証明書のリクエストを送信するか、iOS 用の Citrix Secure Mail APNs 証明書をアップロードします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シトリックス インサイト サービス	さまざまな問題の解決を支援するために、ログを Citrix Insight Services (CIS) にアップロードします。
Exchange ActiveSync ステータス用デバイス NetScaler Gateway コネクタ	Exchange ActiveSync 用コネクタに送信されたデバイスのステータスについて、Citrix Endpoint Management にクエリを実行します。クエリはデバイスの ActiveSync ID に基づいています。

グループアクセスを制限する

管理者ユーザーは、すべてのユーザーグループに権限を適用できます。

デバイスプロビジョニングのコンソール機能

デバイスプロビジョニングユーザーは、Citrix Endpoint Management コンソールへのアクセスが次のように制限されています。デフォルトでは、以下の各機能が有効になっています。

デバイスの制限

デバイスの編集	デバイスの設定を変更します。
デバイスの追加/削除	Citrix Endpoint Management からデバイスを追加または削除します。

デバイスプロビジョニングの設定

デバイスプロビジョニングユーザーは**設定**ページにアクセスできますが、機能を構成する権限はありません。

ユーザーロール

ユーザーロールを持つユーザーは、Citrix Endpoint Managementへのアクセスが次のように制限されています。

ユーザーの承認済みアクセス

セルフヘルプポータル	Citrix Endpoint Managementで、ユーザーにセルフヘルプポータルのみへのアクセスを提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザー向けのコンソール機能

ユーザーはCitrix Endpoint Managementコンソールへの次の制限付きアクセス権を持っています。

ユーザーのデバイス制限付きアクセス

デバイスの完全ワイプ	デバイスからすべてのデータとアプリを消去します。デバイスにメモリカードがある場合は、それらも含まれます。
デバイスの選択的ワイプ	デバイスからすべての企業データとアプリを消去し、個人データとアプリはそのまま残します。
位置の表示	デバイスの位置を確認し、地理的制限を設定します。含まれるもの: デバイスの検索、デバイスの位置の確認、デバイスの追跡、デバイスの位置の経時的な追跡
デバイスをロック	デバイスが使用できないように、リモートでロックします。
デバイスのロックを解除	デバイスが使用できるように、リモートでロックを解除します。
コンテナをロック	デバイス上の企業コンテナをリモートでロックします。
コンテナのロックを解除	デバイス上の企業コンテナをリモートでロック解除します。
コンテナパスワードをリセット	企業コンテナのパスワードをリセットします。
ASMを有効にする/アクティベーションロックをバイパス	アクティベーションロックが有効になっている監視対象のiOSデバイスにバイパスコードを保存します。デバイスを消去するには、このコードを使用してアクティベーションロックを自動的に解除します。
常駐ユーザーを取得	現在のデバイスでアクティブなアカウントを持つユーザーを一覧表示します。このアクションにより、デバイスとCitrix Endpoint Managementコンソール間の同期が強制されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

常駐ユーザーをログアウト	現在のユーザーを強制的にログアウトさせます。
常駐ユーザーの削除	特定のユーザーの現在のセッションを削除します。ユーザーは再度サインインできます。
デバイスを鳴らす	Windowsデバイスを5分間、最大音量でリモートで鳴らします。
デバイスを再起動する	Windowsデバイスを再起動します。
アプリロック	デバイス上のすべてのアプリへのアクセスを拒否します。Androidでは、ユーザーはCitrix Endpoint Managementにサインインできません。iOSでは、ユーザーはサインインできますが、アプリにアクセスできません。
アプリワイプ	Androidでは、この制限によりユーザーのCitrix Endpoint Managementアカウントが削除されます。iOSでは、この制限により、ユーザーがCitrix Endpoint Management機能にアクセスするために必要な暗号化キーが削除されます。
ソフトウェアインベントリの表示	デバイスにインストールされているソフトウェアを確認します。

ユーザーの登録制限

登録の追加/削除	ユーザーまたはユーザーグループへの登録招待を追加または削除します。
ユーザーに通知	ユーザーまたはユーザーグループに登録招待を送信します。

すべての役割のグループアクセスを制限する

デフォルトの役割の場合、この権限はデフォルトで設定されており、すべてのユーザーグループに適用できます。役割を編集することはできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンス

Citrix®ライセンスの使用状況については、以下を参照してください。

- クラウドサービスにおけるライセンスとアクティブな使用状況の監視(/ja-jp/citrix-cloud/citrix-cloud-management/citrix-cloud-service-license-usage.html)
- Citrix Endpoint Managementにおけるライセンスとアクティブな使用状況の監視(/ja-jp/citrix-cloud/citrix-cloud-management/license-usage/endpoint-management-license-usage.html)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイス管理

Citrix Endpoint Managementは、単一の管理コンソール内で、幅広い種類のデバイスをプロビジョニング、管理、保護、およびインベントリできます。

- サポートされているデバイスを管理するために、共通のデバイスポリシーセットを使用します。プラットフォームごとに利用可能なデバイスポリシーを簡単に確認するには：

  a. Citrix Endpoint Managementコンソールに移動し、 > の順に進みます。

  b. をクリックし、表示したいプラットフォームを選択します。

  詳しくは、「追加されたデバイスポリシーのリストをフィルターする」を参照してください。

- ID、会社所有デバイスおよびBYOデバイス、アプリ、データ、ネットワークに対して厳格なセキュリティを適用して、ビジネス情報を保護します。デバイスへの認証に使用するユーザーIDを指定します。デバイス上で企業データと個人データを分離する方法を構成します。
- デバイスやオペレーティングシステムに関係なく、あらゆるアプリをエンドユーザーに配信します。アプリレベルで情報を保護し、エンタープライズグレードのモバイルアプリケーション管理を提供します。
- プロビジョニングおよび構成制御を使用してデバイスをセットアップします。これらの制御には、デバイス登録、ポリシー適用、アクセス権限が含まれます。
- セキュリティおよびコンプライアンス制御を使用して、実行可能なトリガーを備えたカスタマイズされたセキュリティベースラインを作成します。たとえば、定義されたコンプライアンス標準に違反しているデバイスをロック、ワイプ、または通知します。
- OS更新制御を使用して、オペレーティングシステムの更新を防止または強制します。この機能は、標的型オペレーティングシステムの脆弱性に対するデータ損失防止に不可欠です。

サポートされている各プラットフォームに関する記事にアクセスするには、目次リストの「デバイス管理」セクションを展開します。これらの記事には、各デバイスプラットフォームに固有の詳細が記載されています。この記事の残りの部分では、一般的なデバイス管理タスクの実行方法について説明します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイス管理ワークフロー

このセクションのワークフロー図は、デバイス管理タスクの推奨される順序を示しています。

1. **デバイスとアプリを追加するための推奨される前提条件:** 以下のセットアップを事前に実行することで、中断することなくデバイスとアプリを構成できます。

   デバイスとアプリを追加する前の推奨手順(/en-us/citrix-endpoint-management/media/workflow-prereqs-for-adding-devices-apps.png)

   参照:

   リソースを展開する(/ja-jp/citrix-endpoint-management/deploy-resources.html)

   RBACで役割を構成する(/ja-jp/citrix-endpoint-management/users/rbac-roles-and-permissions.html)

   通知テンプレートを作成および更新する(/ja-jp/citrix-endpoint-management/users/notifications.html#create-and-update-notification-templates)

   ワークフローを作成および管理する(/ja-jp/citrix-endpoint-management/users.html#create-and-manage-workflows)
2. **デバイスを追加する:**

   デバイス追加ワークフロー(/en-us/citrix-endpoint-management/media/workflow-add-devices.png)

   参照:

   デバイスを登録し、リソースを配信する準備をする(/ja-jp/citrix-endpoint-management/prepare-to-enroll-devices-and-deliver-resources.html)

   デバイスポリシー(/ja-jp/citrix-endpoint-management/policies.html)

   デリバリーグループに展開する(/ja-jp/citrix-endpoint-management/deploy-resources.html#deploy-to-delivery-groups)

   自動化されたアクション(/ja-jp/citrix-endpoint-management/automated-actions.html)
3. **登録招待を準備する:** iOS、iPadOS、macOS、Android Enterprise、およびレガシーAndroidデバイスのユーザーに登録招待を送信できます。登録招待を使用する予定がある場合は、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

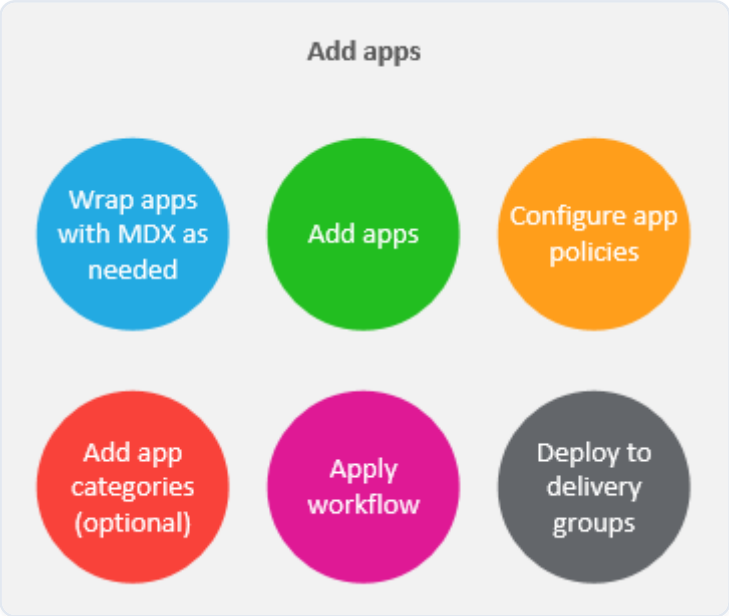
登録招待準備ワークフロー(/en-us/citrix-endpoint-management/media/workflow-enrollment-invitations.png)

参照:

登録セキュリティモードの構成

デバイスへの通知の送信

4. **アプリの追加:**



参照:

MAM SDK

アプリの追加

アプリカテゴリについて

ワークフローの適用

デリバリーグループへの展開

5. **継続的なデバイスおよびアプリの管理の実行:** Citrix Endpoint Managementダッシュボードの使用に加えて、各バージョンの新機能コンテンツを確認することをお勧めします。新機能には、新しいデバイスポリシーの構成など、必要なアクションに関する情報が記載されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



参照:

監視とサポート

レポート

セキュリティアクション

新機能

デバイスポリシー

登録招待

ユーザーデバイスをリモートで安全に管理するには、Citrix Endpoint Management にユーザーデバイスを登録します。ユーザーデバイスに Citrix Endpoint Management クライアントソフトウェアがインストールされ、ユーザーIDが認証されます。その後、Citrix Endpoint Management とユーザープロファイルがインストールされます。サポートされているデバイスプラットフォームの登録の詳細については、このセクションのデバイスに関する記事を参照してください。

Citrix Endpoint Management コンソールで:

- iOS、iPadOS、macOS、Android Enterprise、およびレガシーAndroidデバイスのユーザーに登録招待を送信できます。登録招待はWindowsデバイスでは利用できません。
- iOS、iPadOS、Android Enterprise、またはレガシーAndroidデバイスのユーザーに招待URLを送信できます。招待URLはWindowsデバイスでは利用できません。

登録招待は次のように送信されます:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Active DirectoryユーザーがActive Directoryにメールアドレスを持っている場合、招待を受け取ります。ローカルユーザーは、ユーザープロパティで指定されたメールアドレスで招待を受け取ります。

ユーザーが登録すると、デバイスは **管理 > デバイス** に管理対象として表示されます。招待URLのステータスは **引き換え済み** と表示されます。

前提条件

- LDAPが構成されていること
- ローカルグループとローカルユーザーを使用する場合:
  - 1つ以上のローカルグループ。
  - ローカルグループに割り当てられたローカルユーザー。
  - デリバリーグループはローカルグループに関連付けられています。
- Active Directoryを使用している場合:
  - デリバリーグループはActive Directoryグループに関連付けられています。

登録招待を作成する

1. Citrix Endpoint Managementコンソールで、**管理 > 登録招待**をクリックします。**登録招待**ページが表示されます。

   Citrix Endpoint Managementコンソールの登録招待ページ(/en-us/citrix-endpoint-management/media/manage-enrollment-invitations.png)
2. **追加**をクリックします。登録オプションのメニューが表示されます。

   招待の追加メニュー(/en-us/citrix-endpoint-management/media//manage-enrollment-invitations-add-menu.png)

   - ユーザーまたはグループに登録招待を送信するには、**招待の追加**をクリックします。
   - SMTP経由で受信者リストに登録インストールリンクを送信するには、**インストールリンクの送信**をクリックします。

   登録招待とインストールリンクの送信については、これらの手順の後に説明します。
3. **招待の追加**をクリックします。**登録招待**画面が表示されます。

   登録招待画面(/en-us/citrix-endpoint-management/media/manage-enrollment-invitation-new.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

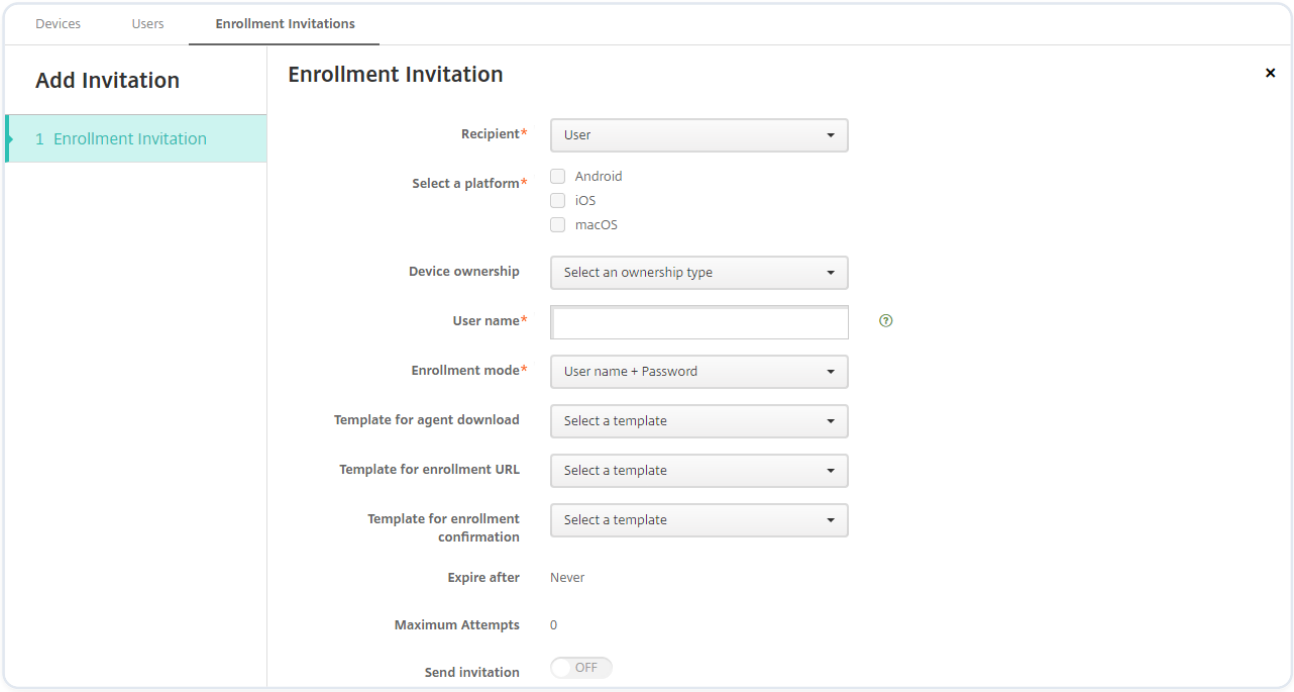
4. 次の設定を構成します。

   - **受信者: グループ**または**ユーザー**を選択します。
   - **プラットフォームの選択: 受信者**が**グループ**の場合、すべてのプラットフォームが選択されます。プラットフォームの選択を変更できます。**受信者**が**ユーザー**の場合、プラットフォームは選択されません。プラットフォームを選択してください。

     Android Enterpriseデバイスの登録招待を作成するには、**Android**を選択します。
   - **デバイスの所有権: 会社所有**または**従業員所有**を選択します。

ユーザーまたはグループの設定は、以下のセクションで説明されているように表示されます。

ユーザーに登録招待を送信するには



1. 次の**ユーザー**設定を構成します。

   - **ユーザー名:** ユーザー名を入力します。ユーザーは、Citrix Endpoint Managementにローカルユーザーまたはは Active Directoryユーザーとして存在している必要があります。ユーザーがローカルの場合、そのユーザーに通知を送信できるように、ユーザーのメールプロパティを設定します。ユーザーがActive Directoryに存在する場合、LDAPが構成されていることを前提とします。
   - **電話番号:** 複数のプラットフォームを選択した場合、またはmacOSのみを選択した場合は、この設定は表示されません。必要に応じて、ユーザーの電話番号を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **キャリア:** 複数のプラットフォームを選択した場合、またはmacOSのみを選択した場合は、この設定は表示されません。ユーザーの電話番号に関連付けるキャリアを選択します。
- **登録モード:** ユーザーの登録セキュリティモードを選択します。デフォルトは**ユーザー名 + パスワード**です。以下のオプションの一部は、すべてのプラットフォームで利用できるわけではありません。
  - **ユーザー名 + パスワード**
  - **招待URL**
  - **招待URL + PIN**
  - **招待URL + パスワード**
  - **2要素認証**
  - **ユーザー名 + PIN**

高セキュリティ登録モードのサポートは廃止されました。登録招待を送信するには、**招待URL**、**招待URL + PIN**、または**招待URL + パスワード**の登録セキュリティモードのみを使用できます。**ユーザー名 + パスワード**、**2要素認証**、または**ユーザー名 + PIN**で登録するデバイスの場合、ユーザーはCitrix Secure Hubをダウンロードし、手動で資格情報を入力する必要があります。

詳細については、「プラットフォーム別の登録セキュリティモード」を参照してください。登録用PINは、ワンタイムPINとも呼ばれます。このようなPINは、ユーザーが登録するときにのみ有効です。

注：

PINを含む登録セキュリティモードを選択すると、**登録PINのテンプレート**フィールドが表示されます。**登録PIN**をクリックします。

- **エージェントダウンロードのテンプレート： ダウンロードリンク**という名前のダウンロードリンクテンプレートを選択します。このテンプレートは、サポートされているすべてのプラットフォーム用です。
- **登録URLのテンプレート： 登録招待**を選択します。
- **登録確認のテンプレート： 登録確認**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **有効期限：** このフィールドは、登録セキュリティモードを構成するときに設定され、登録の有効期限を示します。登録セキュリティモードの構成について詳しくは、「登録セキュリティモードの構成」を参照してください。
- **最大試行回数：** このフィールドは、登録セキュリティモードを構成するときに設定され、登録プロセスが実行される最大回数を示します。
- **招待を送信：** 招待をすぐに送信するには、**オン**を選択します。招待を**登録招待**ページのテーブルに追加するが、送信しない場合は、**オフ**を選択します。

2. **招待を送信**を有効にした場合は、**保存して送信**をクリックします。それ以外の場合は、**保存**をクリックします。招待は、**登録招待**ページのテーブルに表示されます。

「登録招待」ページの表(/en-us/citrix-endpoint-management/media/manage-enrollment-invitation-pending-list.png)

グループに登録招待を送信するには

次の図は、グループへの登録招待を設定するための設定を示しています。

グループへの登録招待ページ(/en-us/citrix-endpoint-management/media/manage-enrollment-invitation-group.png)

1. 次の設定を構成します。

   - **ドメイン:** 招待を受け取るグループのドメインを選択します。
   - **グループ:** 招待を受け取るグループを選択します。Citrix Endpoint Managementは、Active Directoryからユーザーリストを取得します。このリストには、名前に特殊文字が含まれるユーザーが含まれます。
   - **登録モード:** グループ内のユーザーをどのように登録するかを選択します。デフォルトは**ユーザー名 + パスワード**です。次のオプションの一部は、すべてのプラットフォームで利用できるわけではありません。

     - **ユーザー名 + パスワード**
     - **招待URL**
     - **招待URL + PIN**
     - **招待URL + パスワード**
     - **2要素認証**
     - **ユーザー名 + PIN**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高セキュリティ登録モードのサポートは廃止されました。登録招待を送信するには、**招待URL**、**招待URL + PIN**、または**招待URL + パスワード**の登録セキュリティモードのみを使用できます。**ユーザー名 + パスワード**、**2要素認証**、または**ユーザー名 + PIN**で登録するデバイスの場合、ユーザーはCitrix Secure Hubをダウンロードし、手動で資格情報を入力する必要があります。

選択した各プラットフォームに有効な登録セキュリティモードのみが表示されます。詳細については、「プラットフォーム別の登録セキュリティモード」を参照してください。

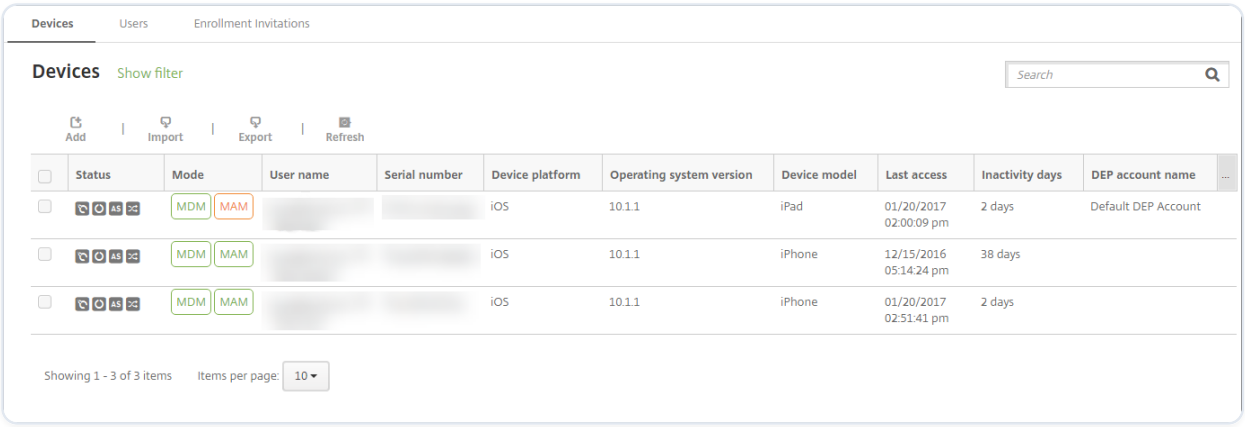
注：

PIN を含む登録セキュリティモードを選択すると、**登録 PIN のテンプレート**フィールドが表示されます。**登録 PIN** をクリックします。

- **エージェントダウンロードのテンプレート： ダウンロードリンク**という名前のダウンロードリンクテンプレートを選択します。このテンプレートは、サポートされているすべてのプラットフォームに対応しています。
- **登録 URL のテンプレート： 登録招待**を選択します。
- **登録確認のテンプレート： 登録確認**を選択します。
- **有効期限：** このフィールドは、登録セキュリティモードを設定するときに設定され、登録の有効期限を示します。登録セキュリティモードの設定の詳細については、「登録セキュリティモードの構成」を参照してください。
- **最大試行回数：** このフィールドは、登録セキュリティモードを設定するときに設定され、登録プロセスが実行される最大回数を示します。
- **招待状を送信：** 招待状をすぐに送信するには、**オン**を選択します。招待状を**登録招待**ページのテーブルに追加するが送信しない場合は、**オフ**を選択します。

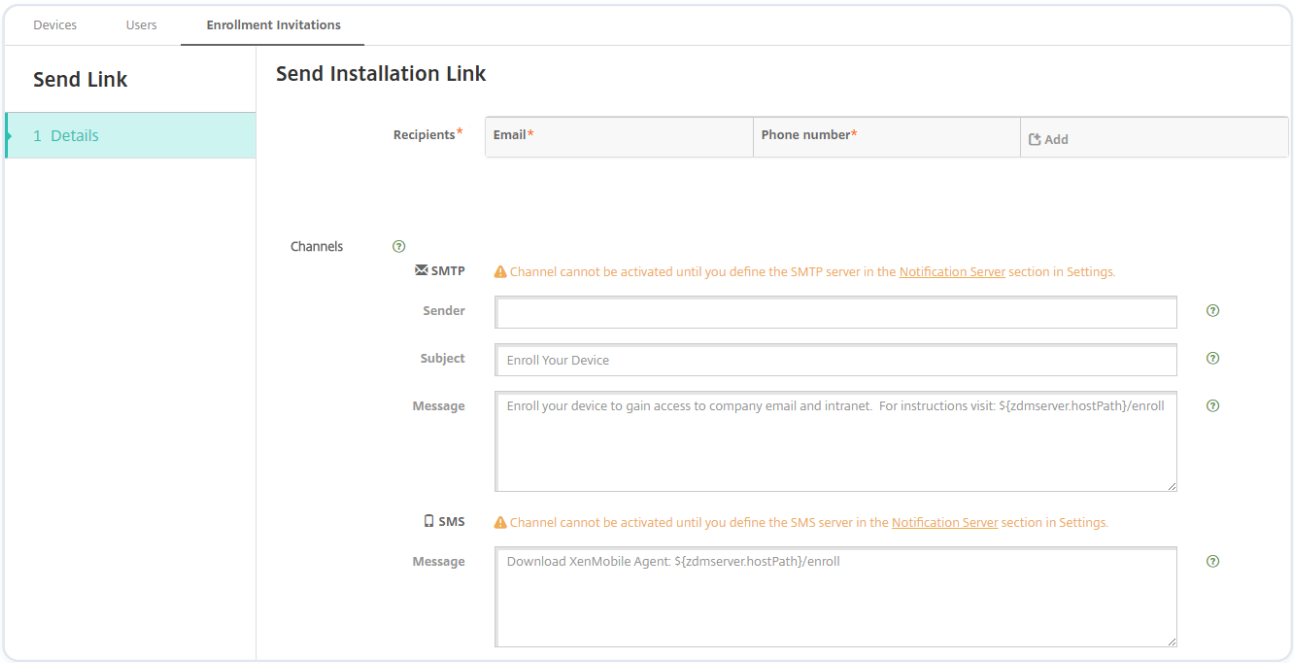
2. **招待状を送信**を有効にした場合は、**保存して送信**をクリックします。それ以外の場合は、**保存**をクリックします。招待状は、**登録招待**ページのテーブルに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



インストールリンクを送信するには

登録インストールリンクを送信する前に、**設定**ページから通知サーバーでチャネル (SMTP) を構成する必要があります。詳細については、「通知」を参照してください。



1. これらの設定を構成し、**保存**をクリックします。

   - **受信者:** 追加したい受信者ごとに、「**追加**」をクリックし、次の操作を行います。
     - **メール:** 受信者のメールアドレスを入力します。このフィールドは必須です。
     - **電話番号:** 受信者の電話番号を入力します。このフィールドは必須です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注：**
>
> 受信者を削除するには、リストのある行にカーソルを合わせ、右側にあるゴミ箱アイコンをクリックします。確認ダイアログボックスが表示されます。リストを削除するには「**削除**」をクリックするか、リストを保持するには「**キャンセル**」をクリックします。

受信者を編集するには、リストのある行にカーソルを合わせます。次に、右側にあるペンアイコンをクリックします。リストを更新し、変更されたリストを保存するには「**保存**」をクリックするか、リストを変更しないままにするには「**キャンセル**」をクリックします。

- **チャネル:** 登録インストールリンクの送信に使用するチャネルを選択します。**SMTP**経由で通知を送信できます。これらのチャネルは、**Notification Server**の**設定**ページでサーバー設定を構成するまでアクティブ化できません。詳細については、「通知」(/ja-jp/citrix-endpoint-management/users/notifications.html)を参照してください。
- **SMTP:** これらのオプション設定を構成します。これらのフィールドに何も入力しない場合、選択したプラットフォーム用に構成された通知テンプレートで指定されたデフォルト値が使用されます。
  - **送信者:** オプションの送信者を入力します。
  - **件名:** メッセージのオプションの件名を入力します。例：「デバイスを登録してください。」
  - **メッセージ:** 受信者に送信するオプションのメッセージを入力します。例：「組織のアプリとメールにアクセスするには、デバイスを登録してください。」

2. 「**送信**」をクリックします。

> **注：**
>
> 環境でsAMAccountNameを使用している場合：ユーザーが招待を受け取り、リンクをクリックした後、認証を完了するためにユーザー名を編集する必要があります。ユーザー名は`sAMAccountName@domainname.com`の形式で表示されます。ユーザーは`@domainname.com`の部分を削除する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プラットフォーム別の登録セキュリティモード

以下の表は、ユーザーデバイスの登録に使用できるセキュリティモードを示しています。表中の**はい**は、特定の登録および管理モードを異なる登録プロファイルでサポートするデバイスプラットフォームを示します。

MDM登録セキュリティモード	NETSCALER GATEWAY上のMAM登録セキュリティモード	管理モード	異なる登録プロファイルをサポート	ANDROID (レガシー)	アンドロイドエンタープライズ	IOS (ユーザー登録モード)	IOS	MACOS	ウィンドウズ
Citrix Cloudを介したIDプロバイダーとしてのAzure ADおよびOkta	クライアント証明書	MDM+MAMまたはMDM	はい	はい	はい	はい	はい	いいえ	いいえ
ユーザー名 + パスワード	LDAP、LDAP + クライアント	MDM+MAM、MDM、またはMAM	はい	はい	はい	はい	はい	はい	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM登録セキュリティモード	NETSCALER GATEWAY上のMAM登録セキュリティモード	管理モード	異なる登録プロファイルをサポート	ANDROID (レガシー)	アンドロイドエンタープライズ	IOS (ユーザー登録モード)	IOS	MACOS	ウィンドウズ
	証明書、およびクライアント証明書のみ	(MAM専用モードはNetScaler Gatewayでクライアント証明書をサポートしていません)							
招待URL	クライアント証明書	MDM+MAM またはMDM	はい	はい	はい	いいえ	はい	いいえ	いいえ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM 登録セキュリティモード	NETSCALER GATEWAY上の MAM 登録セキュリティモード	管理モード	異なる登録プロファイルをサポート	ANDROID (レガシー)	アンドロイドエンタープライズ	IOS (ユーザー登録モード)	IOS	MACOS	ウィンドウズ
招待 URL + PIN	クライアント証明書	MDM +MAM または MDM	はい	はい	はい	いいえ	はい	いいえ	いいえ
招待 URL + パスワード	LDAP、LDAP + クライアント証明書、およびクライアント証明書のみ	MDM +MAM または MDM	はい	はい	はい	いいえ	はい	いいえ	いいえ
2要素認証 (ユーザー名 + パス	LDAP、LDAP + クライア	MDM +MAM または MDM	はい	はい	はい	いいえ	はい	はい	いいえ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM登録セキュリティモード	NETSCALER GATEWAY上のMAM登録セキュリティモード	管理モード	異なる登録プロファイルをサポート	ANDROID (レガシー)	アンドロイドエンタープライズ	IOS (ユーザー登録モード)	IOS	MACOS	ウィンドウズ
ワード + PIN)	ント証明書、およびクライアント証明書のみ								
ユーザー名 + PIN	クライアント証明書	MDM +MAM または MDM	はい	はい	はい	いいえ	はい	はい	いいえ

以下に、iOS、Android、およびAndroid Enterpriseデバイスでの登録セキュリティモードの動作について説明します。

- **ユーザー名 + パスワード** (デフォルト)
    - 登録URLを含む単一の通知をユーザーに送信します。ユーザーがURLをクリックすると、Citrix Secure Hubが開きます。その後、ユーザーはユーザー名とパスワードを入力して、Citrix Endpoint Managementにデバイスを登録します。
- **招待URL**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - 登録URLを含む単一の通知をユーザーに送信します。ユーザーがURLをクリックすると、Citrix Secure Hubが開きます。Citrix Endpoint Managementサーバー名と**はい、登録**ボタンが表示されます。ユーザーは**はい、登録**をタップして、Citrix Endpoint Managementにデバイスを登録します。

- **招待URL + PIN**
  - ユーザーに次のメールを送信します。
    - 登録URLを含むメール。これにより、ユーザーはCitrix Secure Hubを介してCitrix Endpoint Managementにデバイスを登録できます。
    - デバイス登録時にユーザーが入力する必要があるワンタイムPINを含むメール。これには、ユーザーのActive Directory（またはローカル）パスワードも含まれます。
  - このモードでは、ユーザーは通知内の登録URLを使用してのみ登録します。ユーザーが通知招待を紛失した場合、登録できません。ただし、別の招待状を送信できます。
- **招待URL + パスワード**
  - 登録URLを含む単一の通知をユーザーに送信します。ユーザーがURLをクリックすると、Citrix Secure Hubが開きます。Citrix Endpoint Managementサーバー名が表示され、ユーザーがパスワードを入力できるフィールドも表示されます。
- **2要素認証**
  - 登録URLとワンタイムPINを含む単一の通知をユーザーに送信します。ユーザーがURLをクリックすると、Citrix Secure Hubが開きます。Citrix Endpoint Managementサーバー名が表示され、ユーザーがパスワードとPINを入力できる2つのフィールドも表示されます。
- **ユーザー名 + PIN**
  - ユーザーに次のメールを送信します。
    - 登録URLを含むメール。これにより、ユーザーはCitrix Secure Hubをダウンロードしてインストールできます。Citrix Secure Hubが開いた後、ユーザーはCitrix Endpoint Managementにデバイスを登録するためにユーザー名とパスワードを入力するよう求められます。
    - デバイスを登録する際にユーザーが入力する必要があるワンタイムPINと、ユーザーのActive Directory（またはローカル）パスワードを含むメール。
  - ユーザーが通知招待を紛失した場合、登録できません。ただし、別の招待状を送信できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOSデバイスでの登録セキュリティモードの動作は次のとおりです。

- **ユーザー名 + パスワード**
  - 登録URLを含む単一の通知をユーザーに送信します。ユーザーがURLをクリックすると、Safariブラウザが開きます。サインインページが表示され、ユーザーはCitrix Endpoint Managementにデバイスを登録するためにユーザー名とパスワードを入力するよう求められます。
- **2要素認証**
  - 登録URLとワンタイムPINを含む単一の通知をユーザーに送信します。ユーザーがURLをクリックすると、Safariブラウザが開きます。サインインページが表示され、ユーザーがパスワードとPINを入力できる2つのフィールドが表示されます。
- **ユーザー名 + PIN**
  - ユーザーに次のメールを送信します:
    - 登録URLが記載されたメール。ユーザーがURLをクリックすると、Safariブラウザが開きます。サインインページが表示され、ユーザーはCitrix Endpoint Managementにデバイスを登録するためにユーザー名とパスワードを入力するよう求められます。
    - デバイス登録時に入力する必要があるワンタイムPINと、ユーザーのActive Directory（またはローカル）パスワードが記載されたメール。
  - ユーザーが通知招待を紛失した場合、登録できません。ただし、別の招待を送信できます。

Windowsデバイスに登録招待を送信することはできません。Windowsユーザーはデバイスから直接登録します。Windowsデバイスの登録については、「Windowsデバイス」を参照してください。

セキュリティアクション

デバイスおよびアプリのセキュリティアクションは、 **>** ページから実行します。デバイスアクションには、取り消し、ロック、ロック解除、ワイプが含まれます。アプリのセキュリティアクションには、アプリロックとアプリワイプが含まれます。

- **アクティベーションロックバイパス:** デバイスのアクティベーション前に、監視対象のiOSデバイスからアクティベーションロックを解除します。このコマンドでは、ユーザーの個人Apple IDまたはパスワードは必要ありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アプリロック:** デバイス上のすべてのアプリへのアクセスを拒否します。Androidでは、アプリロック後、ユーザーはCitrix Endpoint Managementにサインインできません。iOSでは、ユーザーはサインインできますが、どのアプリにもアクセスできません。
- **アプリワイプ:** Citrix Secure Hubからユーザーアカウントを削除し、デバイスの登録を解除します。**アプリのワイプ解除**アクションを使用するまで、ユーザーは再登録できません。
- **ASM展開プログラムのアクティベーションロック:** Apple School Managerに登録されているiOSデバイスのアクティベーションロックバイパスコードを作成します。
- **証明書の更新:** サポートされているiOS、macOS、およびAndroidデバイスの場合、証明書更新セキュリティアクションにより証明書の更新が開始されます。デバイスが次回Citrix Endpoint Managementに接続するときに、Citrix Endpoint Managementサーバーは新しい証明機関に基づいて新しいデバイス証明書を発行します。
- **制限のクリア:** 監視対象のiOSデバイスでは、このコマンドによりCitrix Endpoint Managementがユーザーによって構成された制限パスワードと制限設定をクリアできます。
- **紛失モードの有効化/無効化:** 監視対象のiOSデバイスを紛失モードにし、表示するメッセージ、電話番号、および脚注をデバイスに送信します。このコマンドを2回目に送信すると、デバイスは紛失モードから解除されます。
- **追跡を有効にする:** AndroidまたはiOSデバイスでは、このコマンドにより、Citrix Endpoint Managementが定義した頻度で特定のデバイスの位置情報をポーリングできます。デバイスの座標と地図上の位置を表示するには、 **>** に移動し、デバイスを選択して、 をクリックします。デバイス情報は、 の下の タブにあります。 を使用して、デバイスを継続的に追跡します。Citrix Secure Hubは、デバイスの実行中に定期的に位置情報を報告します。
- **完全ワイプ:** デバイスからすべてのデータとアプリを、メモリカードを含めて即座に消去します。ワイプされたデバイスは、監査目的で **>** ページのデバイスリストに残ります。ワイプされたデバイスは、デバイスリストから削除できます。

  - Androidデバイスの場合、この要求にはメモリカードをワイプするオプションも含まれることがあります。
  - ワークプロファイルを持つAndroid Enterpriseの完全管理デバイス（COPEデバイス）の場合、選択的ワイプでワークプロファイルを削除した後、完全ワイプを実行できます。
  - iOSおよびmacOSデバイスの場合、デバイスがロックされていても、ワイプは即座に実行されます。

    iOS 11デバイスおよびiPadOS 12デバイス（最小バージョン）の場合：完全ワイプを確定するときに、デバイスのモバイルデータプランを保持するかどうかを選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS 11.3デバイス（最小バージョン）の場合：完全ワイプを確定するときに、iOSデバイスが近接セットアップを実行するのを防ぐことができます。新しいiOSデバイスをセットアップするとき、ユーザーは通常、すでに構成済みのiOSデバイスを使用して自分のデバイスをセットアップできます。Citrix Endpoint Managementで管理され、ワイプされたデバイスでは、近接セットアップをブロックできます。

iOS 17デバイス（最小バージョン）の場合：完全ワイプを確定すると、デバイスはすべてのユーザーデータを自動的にワイプし、指定されたWi-Fiネットワークに接続し、提供された登録プロファイルを使用してMDMサーバーに再登録されます。

- デバイスユーザーがメモリカードのコンテンツが削除される前にデバイスの電源を切った場合、ユーザーはデバイスデータにアクセスできる可能性があります。
- ワイプ要求がデバイスに送信されるまで、ワイプ要求をキャンセルできます。

- **場所の特定:** デバイスを特定し、 **>** ページの **>** の下に、地図を含むデバイスの位置を報告します。場所の特定は1回限りのアクションです。 を使用して、アクションを実行した時点の現在のデバイスの位置を表示します。一定期間デバイスを継続的に追跡するには、 を使用します。
  - このアクションをAndroid（Android Enterpriseを除く）デバイス、またはAndroid Enterprise（会社所有またはBYOD）デバイスに適用する場合、以下の動作に注意してください。
    - **場所の特定** を使用するには、ユーザーが登録時に位置情報の許可を与える必要があります。ユーザーは位置情報の許可を与えないことを選択できます。ユーザーが登録時に許可を与えない場合、Citrix Endpoint Managementは コマンドを送信するときに、再度位置情報の許可を要求します。
  - この機能をiOSまたはAndroid Enterpriseデバイスに適用する場合、以下の制限に注意してください。
    - Android Enterpriseデバイスの場合、位置情報デバイスポリシー でデバイスの位置情報モードが または に設定されていない限り、この要求は失敗します。
    - iOSデバイスの場合、このコマンドはデバイスがMDM紛失モードの場合にのみ成功します。
- **ロック:** デバイスをリモートでロックします。デバイスが盗難され、ロックする必要がある場合に、ロックは役立ちます。Citrix Endpoint ManagementはPINコードを生成し、デバイスに設定します。デバイスにアクセスするには、ユーザーはPINコードを入力します。Citrix Endpoint Managementコンソールからロックを解除するには、**Cancel Lock**を使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ロックしてパスワードをリセット:** デバイスをリモートでロックし、パスコードをリセットします。
  - 次のデバイスではサポートされていません。
    - ワークプロファイルモードでAndroid Enterpriseに登録されており、
    - Android 7.0より前のAndroidバージョンを実行している
  - ワークプロファイルモードでAndroid Enterpriseに登録されており、Android 7.0以降を実行しているデバイスの場合：
    - パスコードはワークプロファイルをロックします。デバイスはロックされません。
    - パスコードが送信されない場合、または送信されたパスコードが要件を満たさず、ワークプロファイルにパスコードがない場合：デバイスはロックされます。
    - パスコードが送信されない場合、または送信されたパスコードが要件を満たさないが、ワークプロファイルにパスコードがある場合：ワークプロファイルはロックされますが、デバイスはロックされません。

  注：

  パスワードリセット機能はBYOD Samsungデバイスでのみサポートされており、コンソール管理者は`DEVICE_ACTION_CONTAINER_PASSWORD_RESET`権限を持っている必要があります。

- **通知（着信音）：** デバイスでサウンドを再生します。

  注：

  この機能はiOSデバイスでのみサポートされています。

- **再起動:** Windows 10およびWindows 11デバイスを再起動します。Windowsタブレットおよび PCの場合、保留中の再起動に関するメッセージが表示されます。再起動は5分後に実行されます。
- **AirPlayミラーリングの要求/停止:** 監視対象のiOSデバイスでAirPlayミラーリングを開始および停止します。
- **再起動/シャットダウン:** 監視対象デバイスを直ちに再起動またはシャットダウンします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注:**
>
> この機能はiOSデバイスでのみサポートされています。

- **取り消し:** デバイスがCitrix Endpoint Managementに接続することを禁止します。
- **取り消し/承認:** 選択的ワイプと同じアクションを実行します。取り消し後、デバイスを再承認して再登録できます。
- **鳴動:** デバイスが紛失モードの場合、「鳴動」は監視対象のiOSデバイスで音を鳴らします。この音は、デバイスを紛失モードから削除するか、ユーザーが音を無効にするまで鳴り続けます。
- **個人用回復キーのローテーション:** FileVaultデバイスポリシーを有効にしている場合、このアクションは新しい個人用回復キーを生成し、古いキーをこの新しいキーに置き換えます。要求が保留中の間は、この要求をキャンセルできます。キャンセルするには、**個人用回復キーのローテーションをキャンセル**をクリックします。
- **選択的ワイプ:** デバイスからすべての企業データとアプリを消去し、個人データとアプリはそのまま残します。選択的ワイプ後、**承認**アクションを使用してデバイスを再承認し、ユーザーが再登録できるようにします。ワイプされたデバイスは、監査目的で**管理 > デバイス**ページのデバイスリストに残ります。ワイプされたデバイスはデバイスリストから削除できます。
  - Androidデバイスを選択的にワイプしても、デバイスがDevice Managerおよび企業ネットワークから切断されることはありません。デバイスがDevice Managerにアクセスするのを防ぐには、デバイス証明書も取り消す必要があります。
  - Androidデバイスを選択的にワイプすると、デバイスも取り消されます。デバイスを再承認するか、コンソールから削除した後にのみ、デバイスを再登録できます。
  - ワークプロファイルを持つAndroid Enterpriseの完全管理デバイス（COPEデバイス）の場合、選択的ワイプでワークプロファイルが削除された後に完全ワイプを実行できます。または、同じユーザー名でデバイスを再登録できます。デバイスを再登録すると、ワークプロファイルが再作成されます。
  - iOSおよびmacOSデバイスの場合、このコマンドはMDMを介してインストールされたプロファイルを削除します。
  - Windowsデバイスでの選択的ワイプは、現在サインオンしているユーザーのプロファイルフォルダーの内容も削除します。選択的ワイプでは、構成を介してユーザーに配信するWebクリップは削除されません。Webクリップを削除するには、ユーザーが手動でデバイスの登録を解除する必要があります。選択的にワイプされたデバイスを再登録することはできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ロック解除:** デバイスがロックされたときに送信されたパスコードをクリアします。このコマンドはデバイスを開きません。

管理 > デバイスで、**デバイスの詳細**ページにはデバイスのセキュリティプロパティも表示されます。これらのプロパティには、強力なID、デバイスのロック、アクティベーションロックのバイパス、およびプラットフォームタイプに関するその他の情報が含まれます。**デバイスの完全ワイプ**フィールドには、ユーザーPINコードが含まれています。デバイスがワイプされた後、ユーザーはそのコードを入力する必要があります。ユーザーがコードを忘れた場合は、ここで確認できます。

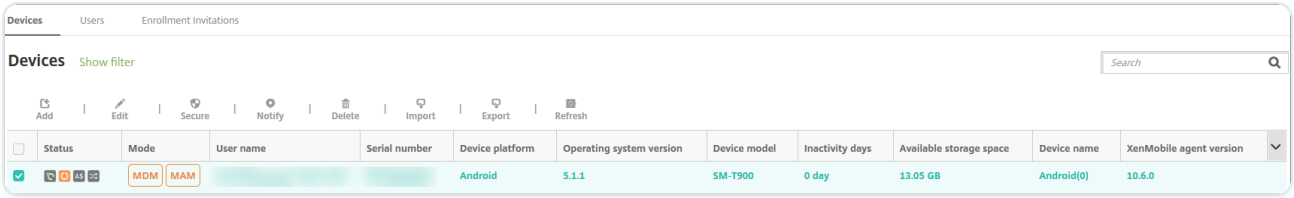
一部のアクションを自動化できます。詳細については、「自動化されたアクション」を参照してください。

Citrix Endpoint Managementコンソールからデバイスを削除する

重要:

Citrix Endpoint Managementコンソールからデバイスを削除しても、管理対象アプリとデータはデバイスに残ります。デバイスから管理対象アプリとデータを削除するには、この記事の後半にある「デバイスを削除する」を参照してください。

Citrix Endpoint Managementコンソールからデバイスを削除するには、**管理 > デバイス**に移動し、管理対象デバイスを選択して、**削除**をクリックします。



デバイスを選択的にワイプする

1. **管理 > デバイス**に移動し、管理対象デバイスを選択して、**セキュリティ保護**をクリックします。
2. **セキュリティアクション**で、**選択的ワイプ**をクリックします。
3. Androidデバイスのみの場合、デバイスを企業ネットワークから切断します。デバイスがワイプされた後、**セキュリティアクション**で**取り消し**をクリックします。

   ワイプが実行される前に選択的ワイプ要求を取り消すには、**セキュリティアクション**で**選択的ワイプのキャンセル**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスを削除する

この手順により、管理対象アプリとデータがデバイスから削除され、Citrix Endpoint Management コンソールのデバイスリストからデバイスが削除されます。Citrix Endpoint Management Public REST APIを使用して、デバイスを一括削除できます。

1. 「**管理 > デバイス**」に移動し、管理対象デバイスを選択して、「**セキュリティ**」をクリックします。
2. 「**選択的ワイプ**」をクリックします。プロンプトが表示されたら、「**選択的ワイプの実行**」をクリックします。
3. ワイプコマンドが成功したことを確認するには、「**管理 > デバイス**」を更新します。「**モード**」列のMDMおよびMAMの琥珀色（アンバーカラー）は、ワイプコマンドが成功したことを示します。

   成功したワイプコマンド(/en-us/citrix-endpoint-management/media/manage-devices-check-wipe-status.png)
4. 「**管理 > デバイス**」でデバイスを選択し、「**削除**」をクリックします。プロンプトが表示されたら、もう一度「**削除**」をクリックします。

アプリのロック、ロック解除、ワイプ、またはワイプ解除

1. 「**管理 > デバイス**」に移動し、管理対象デバイスを選択して、「**セキュリティ**」をクリックします。
2. 「**セキュリティアクション**」で、アプリのアクションをクリックします。

   セキュリティアクションボックスを使用して、Active Directoryからアカウントが無効化または削除されたユーザーのデバイスステータスを確認することもできます。アプリのロック解除またはアプリのワイプ解除アクションの存在は、ロックまたはワイプされたアプリを示します。

アプリのワイプとワイプ解除

1. 「**管理 > デバイス**」に移動します。デバイスを選択します。
2. アプリのワイプ

   - 「**セキュリティ > アプリのワイプ**」をクリックします。次のメッセージが表示されたダイアログボックスが表示されます: 「**このデバイスをアプリワイプしてもよろしいですか？**」「**アプリのワイプ**」をクリックします。
3. アプリのワイプ解除

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**セキュリティ > アプリのワイプ解除**」をクリックします。次のメッセージが表示されたダイアログボックスが表示されます: 「**このデバイスをアプリワイプ解除してもよろしいですか？**」「**デバイスのアプリワイプ解除**」をクリックします。

4. デバイスを同じユーザーとして、同じモードで再登録します。
5. **マイアプリ**ページからMDXアプリを起動します。
6. Citrix Secure Hubを起動します。

デバイスに関する情報の取得

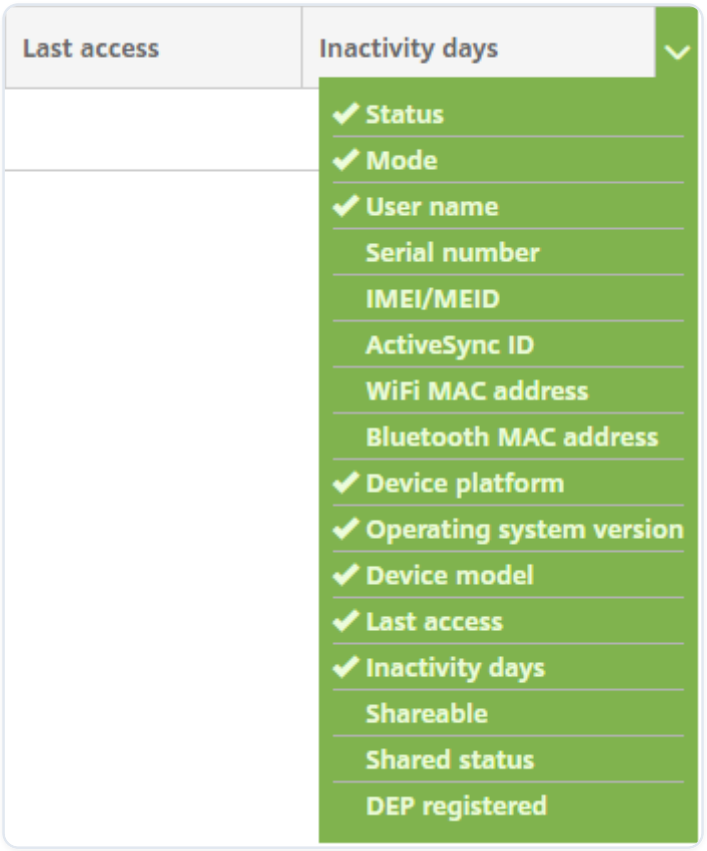
Citrix Endpoint Managementデータベースには、モバイルデバイスのリストが保存されています。Citrix Endpoint Managementコンソールにデバイスを登録するには、デバイスを手動で追加するか、ファイルからデバイスのリストをインポートできます。デバイスプロビジョニングファイル形式の詳細については、この記事の後半にある「デバイスプロビジョニングファイル形式」を参照してください。

Citrix Endpoint Managementコンソールの**管理 > デバイス**ページには、各デバイスと以下の情報が一覧表示されます。

- **状態:** アイコンは、デバイスがジェイルブレイクされているか、管理されているか、ActiveSync Gatewayが利用可能か、および展開状態を示します。
- **モード:** MDMやMDM+MAMなど、デバイスのモードを示します。
- **ユーザー名、デバイスプラットフォーム、最終アクセス、非アクティブ日数**など、デバイスに関するその他の情報。これらの見出しはデフォルトで表示されます。

デバイステーブルをカスタマイズするには、最後の見出しのドロップダウン矢印をクリックします。次に、テーブルに表示したい追加の見出しを選択するか、削除したい見出しのチェックを外します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



デバイスの手動追加、デバイスプロビジョニングファイルからのデバイスのインポート、デバイス詳細の編集、Active Directoryユーザープロパティのカスタマイズ、セキュリティアクションの実行、デバイスへの通知送信が可能です。また、すべてのデバイステーブルデータを.csvファイルにエクスポートして、カスタムレポートを作成することもできます。サーバーはすべてのデバイス属性をエクスポートします。フィルターを適用した場合、Citrix Endpoint Managementは.csvファイルの作成時にそのフィルターを使用します。

プロビジョニングファイルからのデバイスのインポート

携帯電話事業者またはデバイスメーカーから提供されたファイルをインポートすることも、独自のデバイスプロビジョニングファイルを作成することもできます。詳細については、この記事の後半にある「デバイスプロビジョニングファイル形式」を参照してください。

1. **管理 > デバイス**に移動し、**インポート**をクリックします。**プロビジョニングファイルのインポート**ダイアログボックスが表示されます。

   プロビジョニングファイルのインポートダイアログボックス(/en-us/citrix-endpoint-management/media/manage-devices-import-provisioning-file.png)
2. **Choose File** をクリックし、インポートするファイルに移動します。
3. **Import** をクリックします。**デバイス**テーブルにインポートされたファイルが一覧表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. デバイス情報を編集するには、デバイスを選択し、**編集**をクリックします。**デバイスの詳細**ページについては、デバイスに関する情報の取得を参照してください。

デバイスに展開する

1つまたは複数のデバイスをCitrix Endpoint Managementに強制的に接続させることができます。選択されたデバイスは、次回のスケジュールされたチェックインを待つことなく、すぐにリソースを受信します。

デバイスに展開(/en-us/citrix-endpoint-management/media/deploy-devices.png)

1. **管理 > デバイス**に移動し、MDMまたはMDM+MAMで管理されているデバイスを選択し、**展開**をクリックします。
2. ダイアログボックスで、**展開**をクリックして操作を確定します。

デバイスに通知を送信する

デバイスページからデバイスに通知を送信できます。通知の詳細については、通知を参照してください。

1. **管理 > デバイス**ページで、通知を送信するデバイスを選択します。
2. **通知**をクリックします。**通知**ダイアログボックスが表示されます。**受信者**フィールドには、通知を受信するすべてのデバイスが一覧表示されます。

   通知ダイアログボックス(/en-us/citrix-endpoint-management/media/manage-devices-notification.png)
3. これらの設定を構成します。

   - **テンプレート:** ドロップダウンリストで、送信する通知の種類をクリックします。**Ad Hoc**を除く各テンプレートでは、**件名**と**メッセージ**フィールドに、選択したテンプレートに設定されているテキストが表示されます。
   - **チャネル:** メッセージの送信方法を選択します。デフォルトは **SMTP** です。各チャネルのメッセージ形式を表示するには、タブをクリックします。
   - **送信者:** オプションの送信者を入力します。
   - **件名: Ad Hoc** メッセージの件名を入力します。
   - **メッセージ: Ad Hoc** メッセージのメッセージを入力します。
4. **通知**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイステーブルをエクスポートする

1. エクスポートファイルに表示させたい内容に応じて、**デバイス**テーブルをフィルタリングします。
2. **デバイス**テーブルの上にある**エクスポート**ボタンをクリックします。Citrix Endpoint Management は、フィルタリングされた**デバイス**テーブルの情報を抽出し、.csv ファイルに変換します。
3. プロンプトが表示されたら、.csv ファイルを開くか保存します。

ユーザーデバイスを手動でタグ付けする

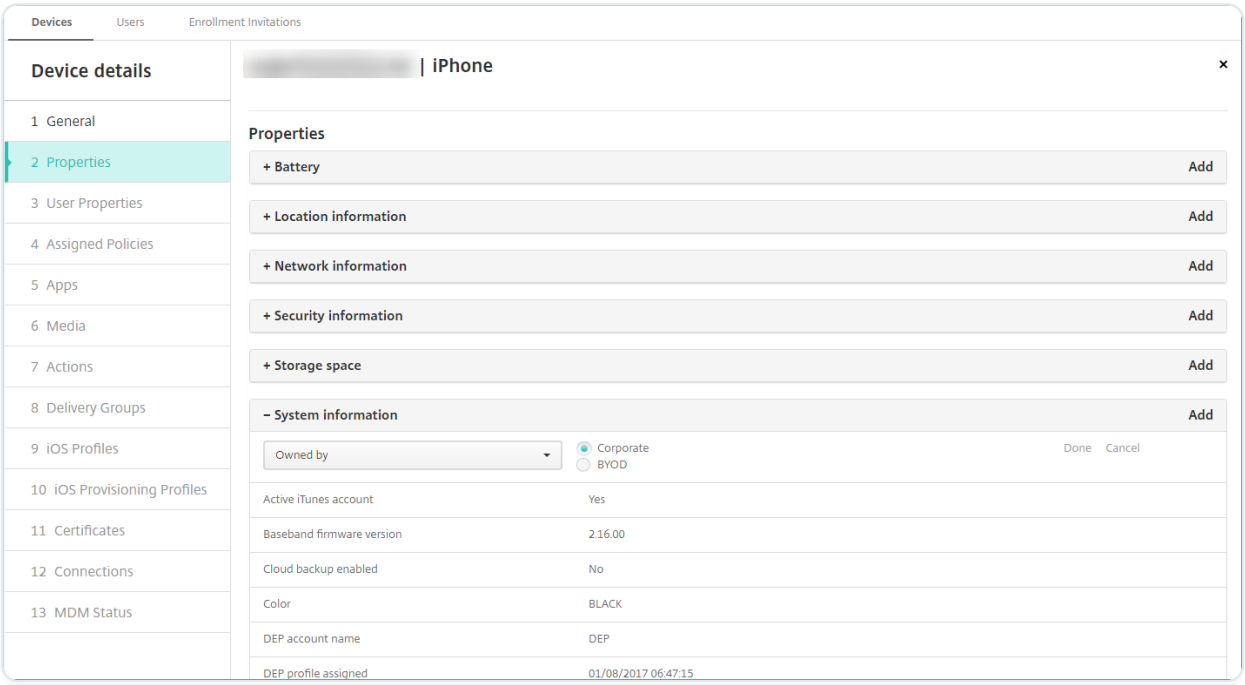
Citrix Endpoint Management でデバイスを手動でタグ付けするには、次の方法があります。

- 招待ベースの登録プロセス中。
- セルフヘルプポータル登録プロセス中。
- デバイスの所有権をデバイスプロパティとして追加する

デバイスを企業所有または従業員所有としてタグ付けするオプションがあります。セルフヘルプポータルを使用してデバイスを自己登録する場合、デバイスを企業所有または従業員所有としてタグ付けできます。また、次のようにデバイスを手動でタグ付けすることもできます。

1. Citrix Endpoint Managementコンソールの**デバイス**タブからデバイスにプロパティを追加します。
2. **Owned by**という名前のプロパティを追加し、**Corporate**または**BYOD** (従業員所有) のいずれかを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Active Directoryユーザー属性をカスタマイズする

Citrix Endpoint Managementがユーザーアカウントを作成するためにアクセスできる属性を定義するために、特定のActive Directoryユーザー属性をカスタマイズできます。

属性のリストを表示するには、**設定 > サーバープロパティ**で`optional.user.identity.attributes`サーバープロパティをカスタムキーとして追加します。**値**フィールドでは、Citrix Endpoint Managementがデフォルトで提供するオプションのActive Directoryユーザー属性を削除し、後で復元できます。詳細については、サーバープロパティを参照してください。

デフォルト値のリストを編集して変更を保存すると、更新されたActive Directoryユーザー属性が**管理 > デバイス > ユーザープロパティ**に表示されます。Citrix Endpoint Managementは、ユーザーがデバイスにサインインした後、または次回のスケジュールされたデバイスチェックイン時にコンソールを更新します。スペルミスをしたり、サポートされていない値を追加したりした場合、Citrix Endpoint Managementは変更を無視します。

オプションのActive Directoryユーザー属性を削除すると、次の機能に影響を与える可能性があります。

- **ユーザーアカウントのプロビジョニング:** 姓と名の値を削除すると、Citrix Endpoint ManagementはShareFileおよびSalesforceのユーザーアカウントをプロビジョニングできません。
- **登録招待:** ユーザーのメールアドレスまたは携帯電話の詳細を削除すると、ユーザーは登録招待を受け取ることができません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **デバイス通知アクション:** ユーザーのメールの詳細を削除すると、ユーザーはSMTP経由で通知を受け取ることができません。
- **Citrix Secure Mailへのシングルサインオン:** 表示名の値を削除すると、ユーザーはシングルサインオンを使用してCitrix Secure Mailにサインインできません。
- **ユーザープロパティと展開ルール:** ユーザープロパティと展開ルールを構成するために使用するオプション属性のいずれかを削除すると、既存の構成に影響を与える可能性があります。
- **アクション: 構成 > アクション**で自動アクションを設定するために使用するオプション属性のいずれかを削除すると、既存の構成に影響を与える可能性があります。
- **カスタムレポート:** カスタムレポートで使用するオプション属性を削除すると、既存の構成に影響を与える可能性があります。

デバイスの検索

高速検索のため、デフォルトの検索スコープには次のデバイスプロパティが含まれます。

- シリアル番号
- IMEI
- Wi-Fi MACアドレス
- Bluetooth MACアドレス
- アクティブ同期ID
- ユーザー名

検索スコープは、デフォルトで **false** に設定されているサーバープロパティ **include.device.properties.during.search** を介して構成できます。デバイス検索にすべてのデバイスプロパティを含めるには、 **>** に移動し、設定を **true** に変更します。

デバイスプロビジョニングファイル形式

多くのモバイル通信事業者またはデバイスメーカーは、承認されたモバイルデバイスのリストを提供しています。これらのリストを使用すると、モバイルデバイスの長いリストを手動で入力する手間を省くことができます。Citrix Endpoint Managementは、Android、iOS、Windowsといったサポートされているデバイスタイプに共通のインポートファイル形式をサポートしています。

手動で作成するプロビジョニングファイルは、次の形式である必要があります。

```
SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propert
propertyNameN;propertyValueN
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の点に注意してください。

- 各プロパティの有効な値については、PDF (/ja-jp/citrix-endpoint-management/downloads/device-property-names-and-values.pdf) を参照してください。
- UTF-8文字セットを使用してください。
- プロビジョニングファイル内のフィールドを区切るには、セミコロン (;) を使用します。
  フィールドの一部にセミコロンが含まれている場合は、バックスラッシュ文字 (\\) でエスケープしてください。

  例として、このプロパティの場合：

  `propertyV;test;1;2`

  次のようにエスケープします。

  `propertyV\;test\;1\;2`
- シリアル番号はiOSデバイスの識別子であるため、iOSデバイスにはシリアル番号が必要です。
- その他のデバイスプラットフォームでは、シリアル番号またはIMEIのいずれかを含める必要があります。
- **OperatingSystemFamily** の有効な値は、**WINDOWS**、**ANDROID**、または **iOS** です。

デバイスプロビジョニングファイルの例：

```
`1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;prop
ertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;prope
rtyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;`
```

ファイル内の各行はデバイスを表します。このサンプルの最初の項目は、次のことを意味します。

- シリアル番号: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`
- OperatingSystemFamily: `WINDOWS`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- プロパティ名: `propertyN`
- プロパティ値: `propertyV\;test\;1\;2;prop 2`

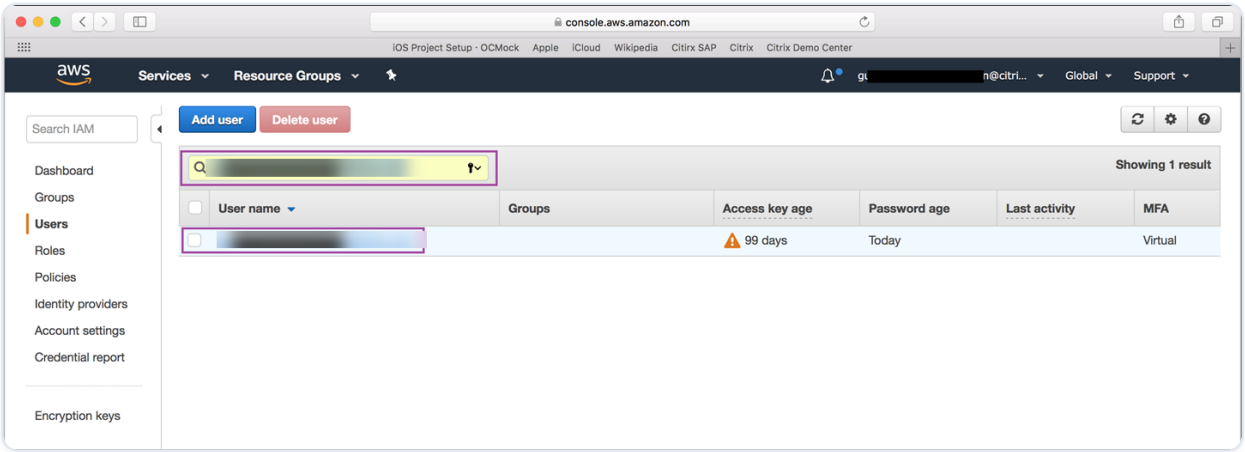
アレクサ フォー ビジネス

Amazon Web Services (AWS) の Alexa for Business サービスを使用すると、会議室アシスタンスなどのビジネス用途で、多数の Alexa 対応デバイスを管理できます。Citrix Endpoint Management を使用すると、Citrix Endpoint Management コンソールでこれらのデバイスを構成および管理できます。Citrix Endpoint Management は、ポリシーを Alexa デバイスに直接展開しません。その代わりに、Citrix Endpoint Management が AWS サービスを更新し、AWS が構成を Alexa デバイスに配信します。

Alexa for Business の使用方法については、Alexa for Business 管理ガイド を参照してください。

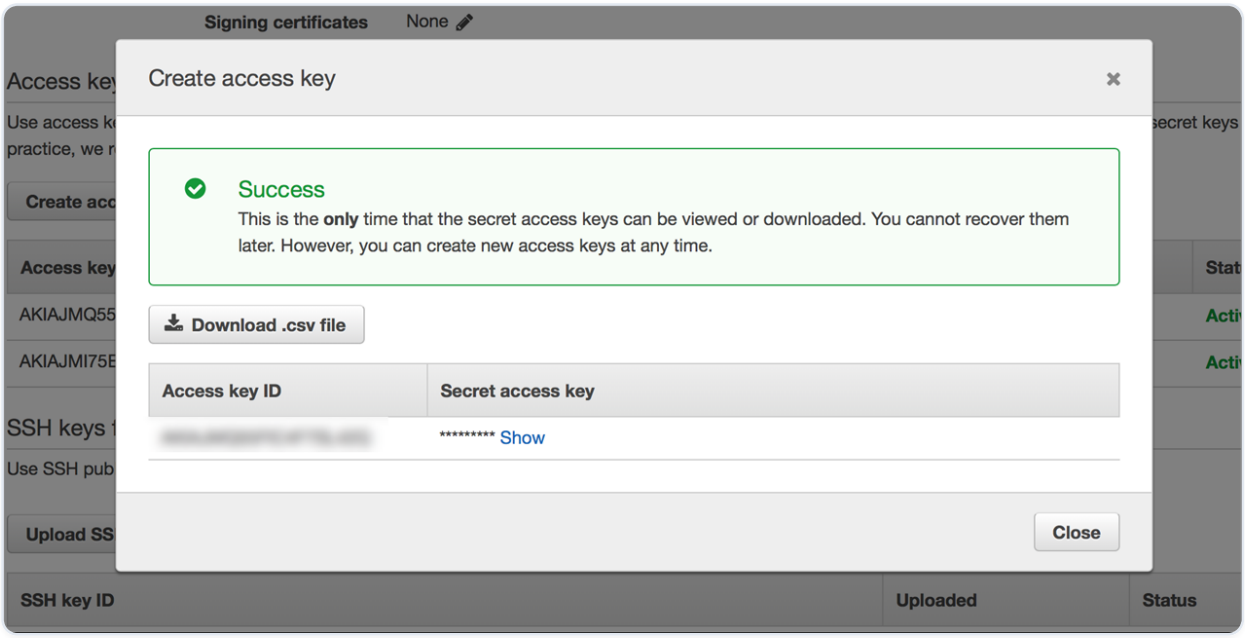
Citrix Endpoint Management への AWS アカウントの認証

1. AWS アカウントの資格情報を取得するには、AWS コンソールにログインし、ユーザーメニューから を選択します。
2. 左側のパネルで を選択します。
3. ユーザー名を検索し、選択します。

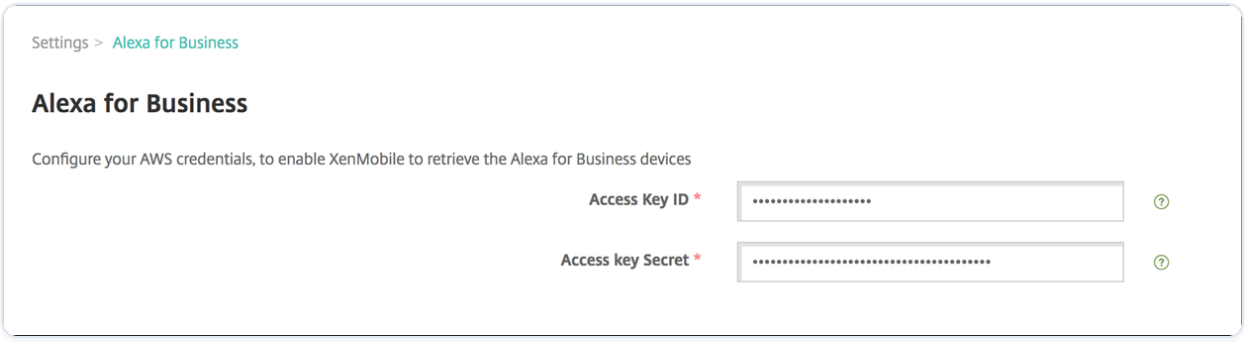


4. タブで、 をクリックして、アクセスキー ID とシークレットアクセスキーを生成します。
5. アクセスキー ID とシークレットアクセスキーをダウンロードします。それらを保存またはメモします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Citrix Endpoint Management コンソールで、歯車アイコンをクリックして に移動します。
7. の下で、 を選択します。
8. アクセスキー ID とシークレットアクセスキーを入力します。 をクリックします。



Citrix Endpoint Management でアレクサ フォー ビジネスを構成する

Citrix Endpoint Management では、以下を構成できます。

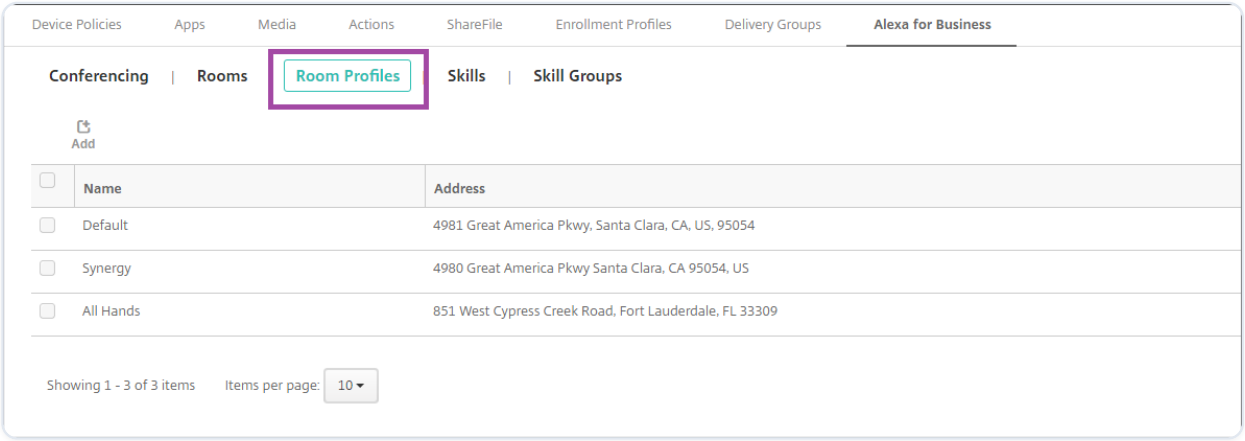
- Alexa デバイスがあるルームに適用する設定のルームプロファイル
- デバイスが設置されている物理的な部屋を表すルーム
- ルームまたはデバイスに割り当てるスキルグループ
- スキルグループに追加できるAlexaスキルストアのAlexaスキル
- 会議プロバイダーを選択し、ルームでの会議のスケジュール設定と参加方法を制御できる会議機能

© 1997–2026 Citrix Systems, Inc. All rights reserved.

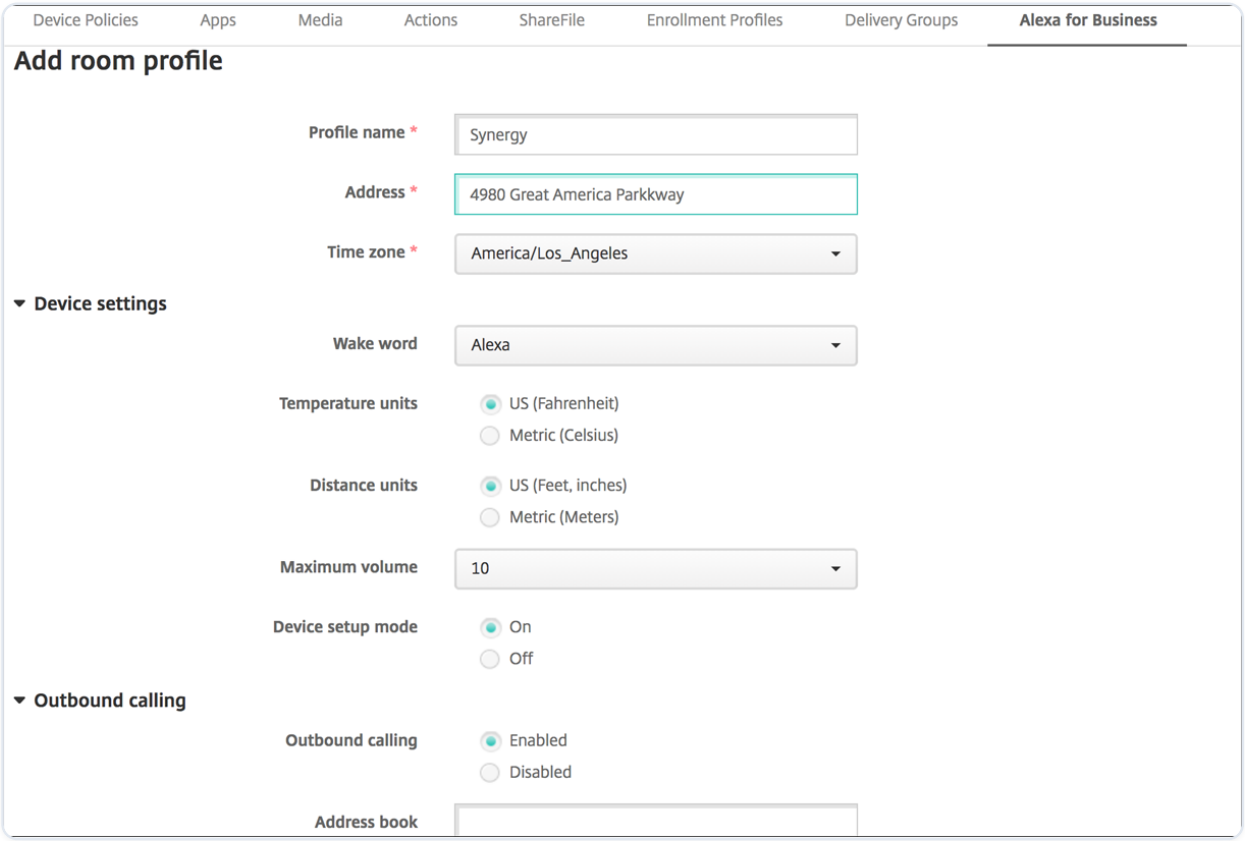
ルームプロファイルの構成

ルームプロファイルは、Alexaデバイスが設置されている複数のルームに適用できる共通構成のセットです。ルームプロファイルを追加、編集、削除できます。

1. Citrix Endpoint Managementコンソールで、**［構成］>［Alexa for Business］>［ルームプロファイル］** の順に選択します。利用可能なルームプロファイルのリストが表示されます。



2. ルームプロファイルを追加するには、**［追加］** をクリックします。ルームプロファイルを編集するには、編集するルームプロファイルを選択し、**［編集］** をクリックします。
3. ルームプロファイル設定を入力します。



- **プロファイル名：** プロファイルの名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

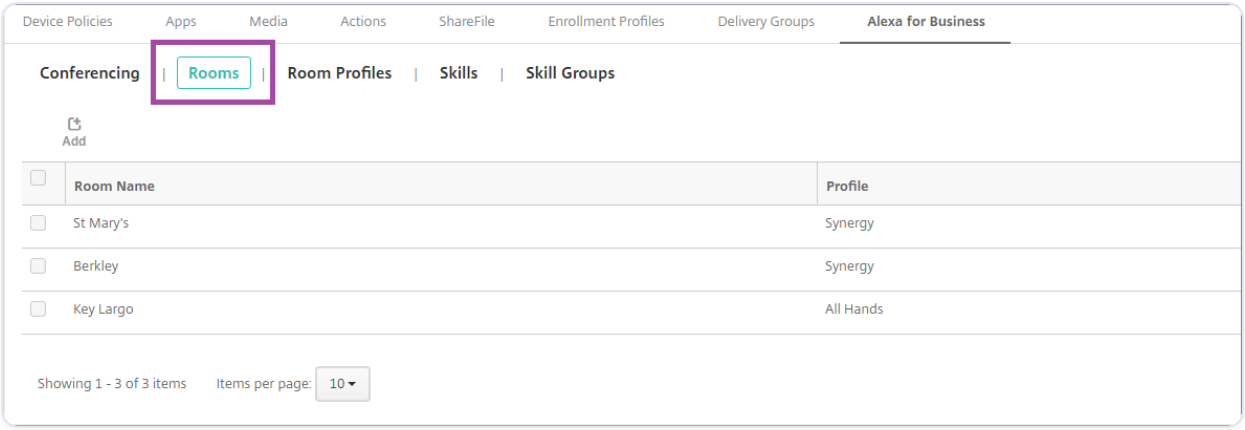
- **アドレス：** Alexaデバイスが設置されている建物の物理的な（番地）アドレスを入力します。
- **タイムゾーン：** 場所のタイムゾーンを選択します。
- **ウェイクワード：** Alexaデバイスが応答するウェイクワードを選択します。
- **温度単位：** Alexaデバイスが温度を報告する単位を選択します。
- **距離単位：** Alexaデバイスが距離を報告する単位を選択します。
- **最大音量:** Alexa の最大音量設定を選択します。
- **デバイスセットアップモード:** Alexa デバイスをデバイスセットアップモードに強制的に移行させることで、再構成できるかどうかを選択します。
- **発信:** Alexa デバイスの発信機能を有効または無効にします。
- **アドレス帳:** Alexa デバイスのアドレス帳設定を行います。

4. **保存**をクリックします。

会議室の構成

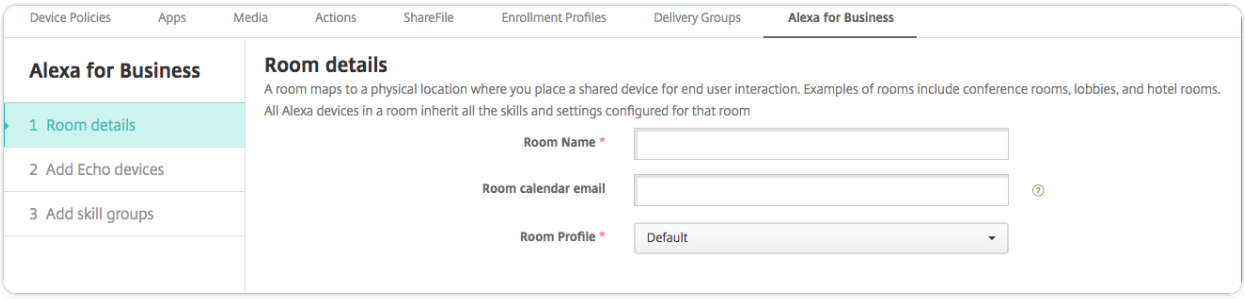
Citrix Endpoint Management コンソールで構成する会議室は、建物内の物理的な会議室、ミーティングルーム、その他の部屋を表します。会議室を構成する際に、その会議室に Alexa デバイスを関連付け、スキルグループをデバイスに追加します。会議室の追加、編集、削除が可能です。

1. Citrix Endpoint Management コンソールで、**構成 > Alexa for Business > 会議室**の順に選択します。利用可能な会議室のリストが表示されます。



2. 会議室を追加するには、**追加**をクリックします。会議室を編集するには、編集する会議室を選択して**編集**をクリックします。
3. これらの会議室設定を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **会議室名:** 会議室、ミーティングルーム、またはその他の部屋の名前を入力します。
- **会議室カレンダーのメールアドレス:** 会議室のカレンダーのメールアドレスを入力します。
- **会議室プロファイル:** 会議室の会議室プロファイル構成の名前を選択します。

4. **次へ**をクリックします。
5. Alexa デバイスを会議室に関連付けるには、**追加**をクリックします。
6. デバイスを選択し、「**追加**」をクリックします。選択したデバイスが「**Echoデバイスの追加**」ページに表示されます。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-7.png)
7. 「**次へ**」をクリックします。
8. 部屋のAlexaデバイスにスキルグループを追加するには、「**追加**」をクリックします。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill-to-room1.png)
9. 部屋のAlexaデバイスに追加するスキルグループを選択します。「**追加**」をクリックします。選択したスキルグループが「**スキルグループの追加**」ページに表示されます。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill-to-room2.png)
10. 「**保存**」をクリックします。

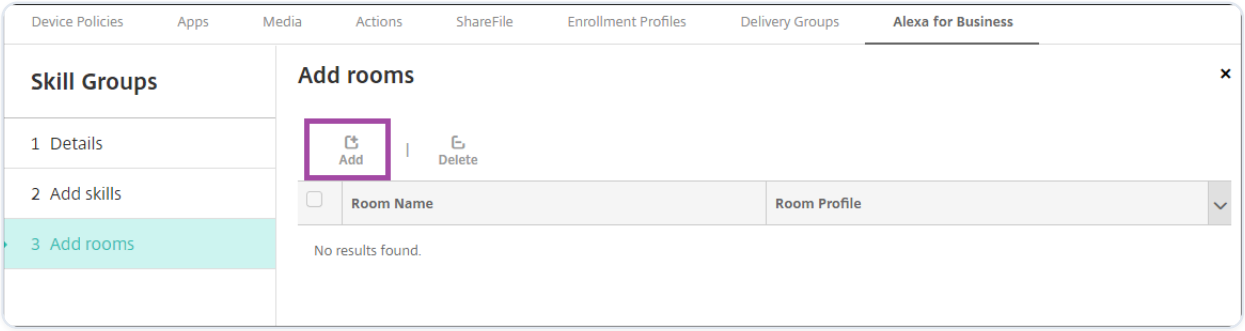
スキルグループを構成する

スキルグループは、部屋に適用できるスキルの集まりです。スキルグループを作成し、それを部屋に割り当てることができます。スキルを使用すると、Alexaデバイスでオンライン会議の開始と終了、議題リストの確認などを行うことができます。スキルグループの追加、編集、削除が可能です。

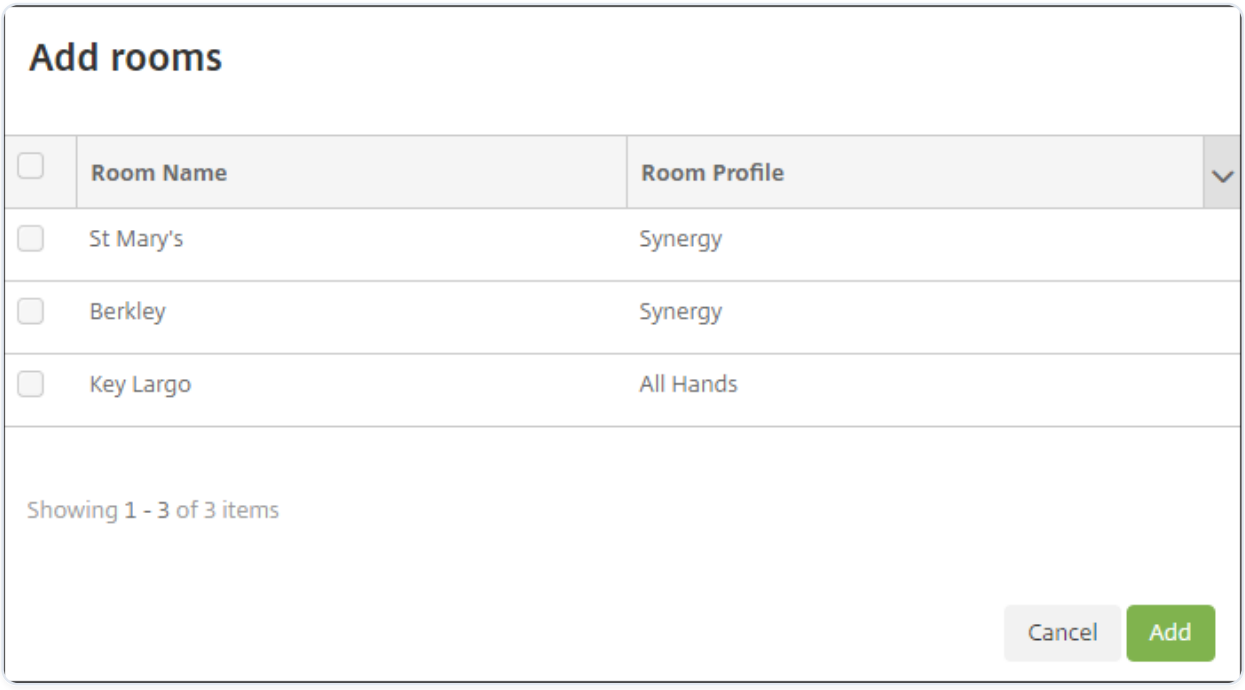
1. Citrix Endpoint Managementコンソールで、「**構成 > Alexa for Business > スキルグループ**」を選択します。利用可能なスキルグループのリストが表示されます。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-11.png)
2. スキルグループを追加するには、「**追加**」をクリックします。スキルグループを編集するには、編集するスキルグループを選択し、「**編集**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. これらのスキルグループ設定を入力します。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill-to-group3.png)
   - **名前:** スキルグループの名前を入力します。
   - **説明:** スキルグループの簡単な説明を入力します。
4. 「**次へ**」をクリックします。
5. スキルグループにスキルを追加するには、「**追加**」をクリックします。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill-to-group3.png)
6. スキルグループに含めるスキルを選択し、「**追加**」をクリックします。選択したスキルが「**スキルの追加**」ページに表示されます。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill-to-group2.png)
7. 指定した部屋のAlexaデバイスにスキルグループを追加するには、**追加**をクリックします。



8. 対象となる部屋を選択してください。



9. **保存**をクリックします。

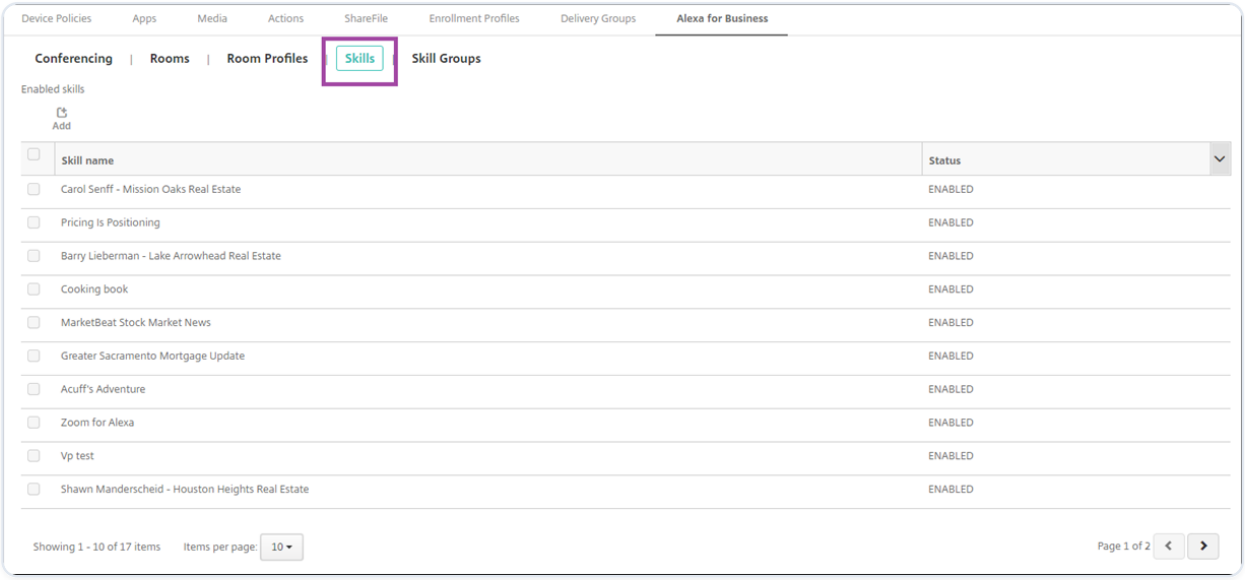
© 1997–2026 Citrix Systems, Inc. All rights reserved.

スキルグループでスキルを利用可能にする

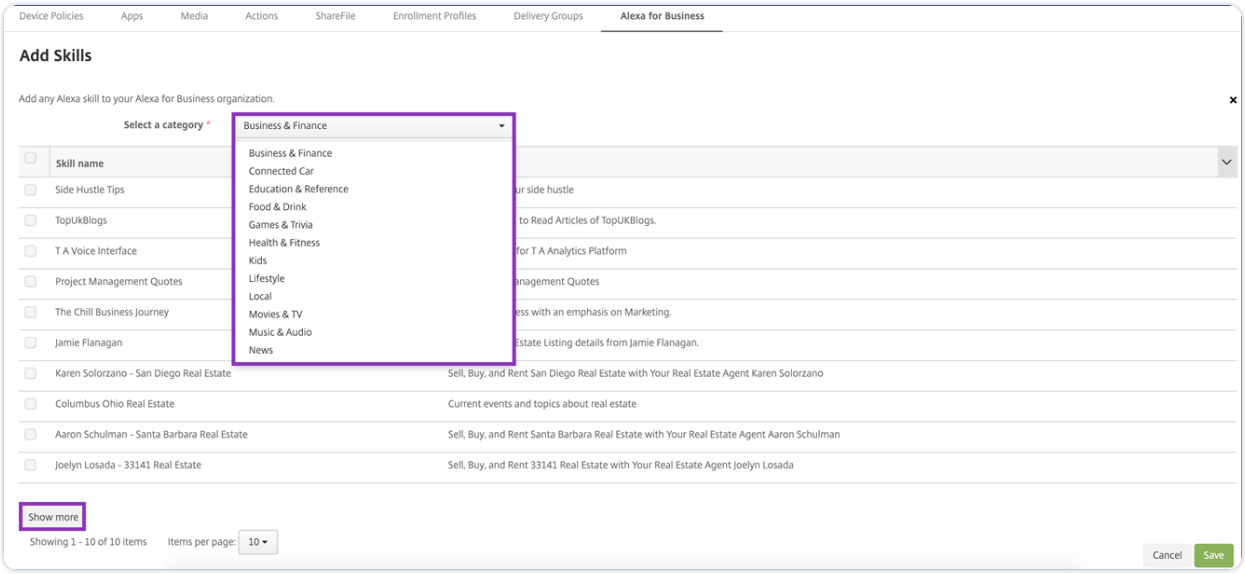
Alexa for Business組織のスキルグループに含めることができるAlexaスキルのリストを構成します。これらのスキルは、パブリックなAlexaスキルストアから、または組織に公開されたプライベートスキルから取得されます。

組織にスキルを追加する

1. Citrix Endpoint Managementコンソールで、**構成 > Alexa for Business > スキル**の順に選択します。有効なスキルのリストが表示されます。



2. スキルを追加するには、**追加**をクリックします。
3. その他のAlexaスキルを表示するには、カテゴリを選択し、**さらに表示**をクリックします。**さらに表示**をクリックすると、組織に追加できるスキルのリストに最大10個のスキルが追加されます。さらにスキルを追加するには、もう一度**さらに表示**をクリックします。

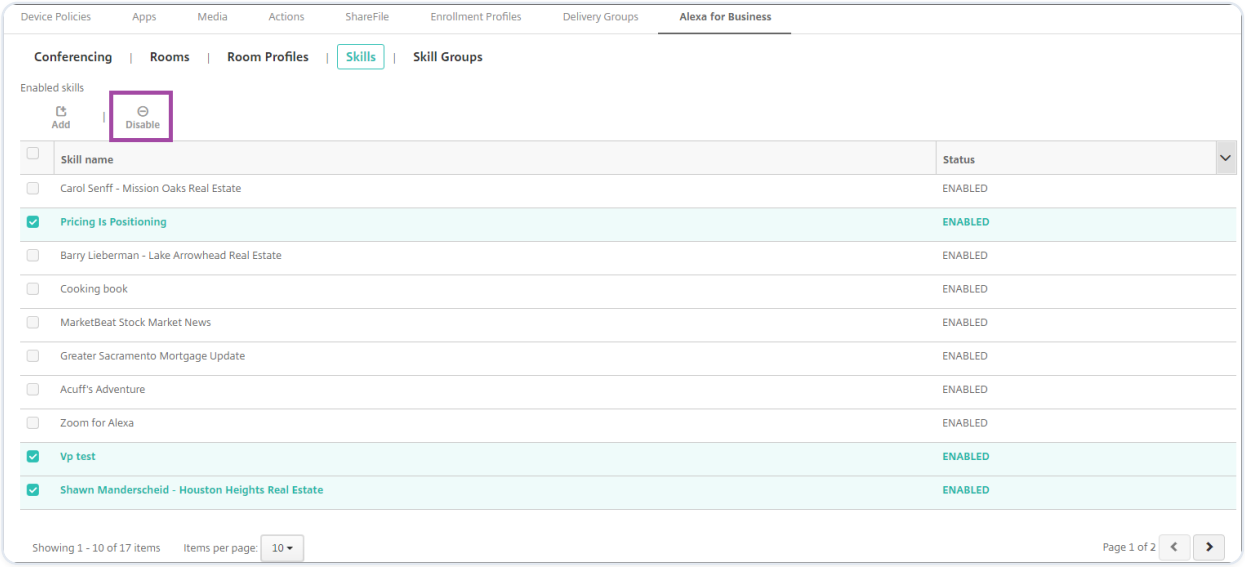


4. 組織に追加するスキルを選択します。
5. **保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

組織からスキルを削除する

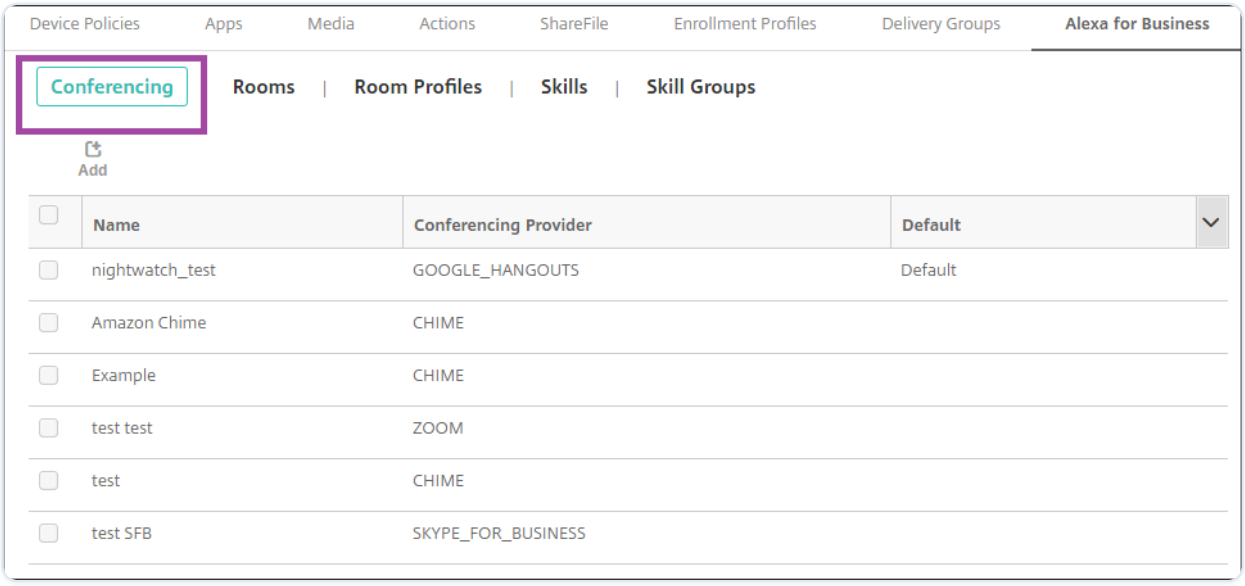
1. Citrix Endpoint Managementコンソールで、**構成 > Alexa for Business > スキル**の順に選択します。有効なスキルのリストが表示されます。
2. 組織から削除するスキルを選択します。
3. 無効にするには、**無効化**をクリックします。



会議設定を構成する

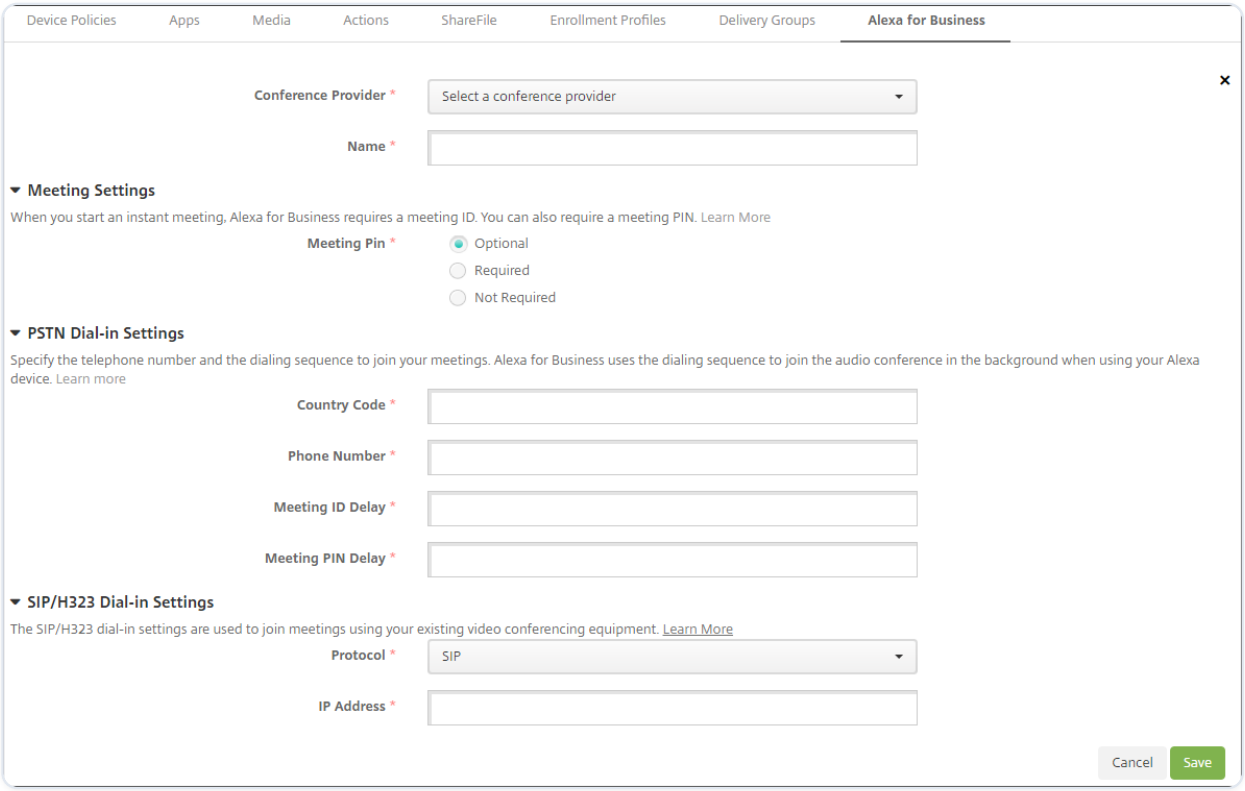
会議機能を使用すると、Google Hangout や Amazon Chime などの会議プロバイダーを構成できます。これらのプロバイダーは、Alexa デバイスが設置されている部屋でユーザーが会議に参加する方法を制御します。会議プロバイダーの追加、編集、削除が可能です。また、既定の会議プロバイダーを設定することもできます。

1. Citrix Endpoint Management コンソールで、 **> >** の順に選択します。利用可能な会議室プロファイルの一覧が表示されます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 会議プロバイダーを追加するには、 をクリックします。会議プロバイダーを編集するには、編集する会議室プロファイルを選択し、 をクリックします。
3. 会議室プロファイルの設定を入力します。



- **会議プロバイダー:** 一覧から会議プロバイダーを選択します。
- **名前:** 会議プロバイダーに付ける名前を入力します。
- **会議 PIN:** 会議に参加するために PIN を要求するかどうかを指定します。
- **PSTN ダイヤルイン設定**
  - **国コード:** 国コードを入力します。
  - **電話番号:** 電話番号を入力します。
  - **会議 ID 遅延:** 会議 ID が送信されるまでの秒数を指定します。
  - **会議 PIN 遅延:** PIN が送信されるまでの秒数を指定します。
- **SIP/H323 ダイヤルイン設定** SIP/H323 ダイヤルイン設定は、既存のビデオ会議機器を使用して会議に参加するために使用されます。
  - **プロトコル:** プロトコルを選択します。
  - **IPアドレス:** IPアドレスを入力します。

4. 「**保存**」をクリックします。

複数の会議プロバイダーを設定する場合は、デフォルトのプロバイダーを設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Citrix Endpoint Managementコンソールで、「**構成 > Alexa for Business > 会議**」を選択します。利用可能な会議室プロファイルのリストが表示されます。
2. デフォルトとして設定する会議プロバイダーを選択します。
3. 「**デフォルトに設定**」をクリックします。

Android

デバイス管理からAndroid Enterpriseへの移行

この記事では、従来のAndroidデバイス管理からAndroid Enterpriseへの移行に関する考慮事項と推奨事項について説明します。GoogleはAndroid Device Administration APIを非推奨にしています。このAPIは、Androidデバイス上のエンタープライズアプリをサポートしていました。Android Enterpriseは、GoogleとCitrixが推奨する最新の管理ソリューションです。

Citrix Endpoint Managementは、Androidデバイスのデフォルトの登録方法としてAndroid Enterpriseに移行しています。GoogleがAPIを非推奨にした後、デバイス管理モードのAndroid Qデバイスでは登録が失敗します。

Android Enterpriseには、完全に管理されたデバイスモードと仕事用プロファイルデバイスモードのサポートが含まれています。Googleの出版物であるAndroid Enterprise Migration Bluebookでは、従来のデバイス管理とAndroid Enterpriseがどのように異なるかについて詳しく説明しています。Googleからの移行情報を読むことをお勧めします。

Citrix Tech Zoneの記事、Citrix Endpoint Managementを使用したAndroidデバイス管理者からAndroid Enterpriseへの移行も参照することをお勧めします。

デバイス管理の非推奨化の影響

GoogleはDevice Administrator APIを非推奨にしており、November 2, 2020以降はサポートしません。Citrix Secure HubをAndroid APIレベル29をターゲットとするようにアップグレードした後、これらのAPIはAndroid 10以降を実行しているデバイスでは機能しません。

- **カメラの無効化:** デバイスカメラへのアクセスを制御します。
- **キーガード機能:** 生体認証やパターンなど、デバイスのロックに関連する機能を制御します。
- **パスワードの有効期限:** 設定可能な期間が経過した後、ユーザーにパスワードの変更を強制します。
- **パスワードの制限:** 制限的なパスワード要件を設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要件と推奨事項

- デバイスをAndroid 10以降にアップグレードできる場合は、そのデバイスをAndroid Enterpriseに登録する必要があります。
    - Android 11デバイスはAndroid Enterpriseに登録する必要があります。
    - September 2020以降、Android 10デバイスの場合: Citrixは、デバイス管理モードへの新規登録またはデバイスの再登録をサポートしていません。すでに登録されているデバイスは、前述のセクションで述べたように、November 2, 2020まで引き続き機能します。
- Android 9以前のデバイスでは、従来のデバイス管理モードをサポートしています。ただし、これらのデバイスはできるだけ早くAndroid Enterpriseに移行することをお勧めします。
- Citrix MAM専用モードに登録されている新規または既存のデバイスについては、何もアクションは必要ありません。非推奨のGoogle APIは、MAM専用モードのデバイスには影響しません。ただし、プラットフォーム暗号化への移行に伴い、MAM専用モードからAndroid Enterpriseワークプロファイルモード（BYOD）への移行を強くお勧めします。ワークプロファイルモードはMAM機能を提供しますが、デバイス上のコンテナ内で動作します。

分析

移行の分析フェーズは以下で構成されます。

- 従来のAndroidセットアップを理解する
- 従来のセットアップを文書化し、従来の機能をAndroid Enterpriseの機能にマッピングできるようにする

推奨される分析

1. Citrix Endpoint ManagementでAndroid Enterpriseを評価する: フルマネージド、ワークプロファイル付きフルマネージド、専用デバイス、ワークプロファイル（BYOD）。
2. 現在のデバイス管理機能をAndroid Enterpriseと比較して分析する。
3. デバイス管理のユースケースを文書化する。

デバイス管理のユースケースを文書化するには：

1. スプレッドシートを作成し、Citrix Endpoint Managementコンソール内の現在のポリシーグループをリストアップします。
2. 既存のポリシーグループに基づいて、個別のユースケースを作成します。
3. 各ユースケースについて、以下を文書化します。
    - 名前

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 事業主
- ユーザーIDモデル
- デバイス要件
  - セキュリティ
  - 管理
  - ユーザビリティ
- デバイスインベントリ
  - メーカーとモデル
  - OSバージョン
- アプリ

4. 各アプリについて、以下をリストアップします。
   - アプリ名
   - パッケージ名
   - ホスティング方法
   - アプリが公開か非公開か
   - アプリが必須であるかどうか（true/false）

要件のマッピング

完了した分析に基づいて、Android Enterpriseの機能要件を決定します。

推奨される要件のマッピング

1. 管理モードと登録方法を決定します。
   - ワークプロファイル (BYOD): 再登録が必要です。工場出荷時設定へのリセットは不要です。
   - 完全に管理されている: 工場出荷時設定へのリセットが必要です。QRコード、近距離無線通信 (NFC) バンプ、デバイスポリシーコントローラー (DPC) 識別子、ゼロタッチを使用してデバイスを登録します。
2. アプリの移行戦略を作成します。
3. ユースケースの要件をAndroid Enterpriseの機能にマッピングします。各デバイス要件について、その要件と対応するAndroidバージョンに最も近い機能を文書化します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 機能要件に基づいて、最小のAndroid OSを決定します (7.0、8.0、9.0)。
5. IDモデルを選択します。
    - 推奨: マネージドGoogle Playアカウント
    - Google Cloud Identityのお客様である場合にのみ、Google Workspaceアカウントを使用してください
6. デバイス戦略を作成します。
    - アクションなし: デバイスが最小OSレベルを満たしている場合
    - アップグレード: デバイスがサポート対象OSに対応しており、かつ更新できる場合
    - 交換: デバイスがサポート対象OSレベルに更新できない場合

推奨されるアプリの移行戦略

要件のマッピングが完了したら、アプリをAndroidプラットフォームからAndroid Enterpriseプラットフォームに移動します。アプリの公開の詳細については、「アプリの追加」を参照してください。

- パブリックストアアプリ
    a. 移行するアプリを選択し、Google Playの設定をクリアするようにアプリを編集し、プラットフォームとして**Android Enterprise**を選択します。
    b. デリバリーグループを選択します。アプリが必須である場合は、そのアプリをデリバリーグループの**必須アプリ**リストに移動します。

    アプリを保存すると、Google Playストアに表示されます。仕事用プロファイルがある場合、アプリは仕事用プロファイルのGoogle Playストアに表示されます。
- プライベート（エンタープライズ）アプリ

    プライベートアプリは、社内またはサードパーティの開発者によって開発されます。プライベートアプリはGoogle Playを使用して公開することをお勧めします。

    a. 移行するアプリを選択し、プラットフォームとして**Android Enterprise**を選択するようにアプリを編集します。
    b. APKファイルをアップロードし、アプリの設定を構成します。
    c. 必須のデリバリーグループにアプリを公開します。
- MDXアプリ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 移行するアプリを選択し、プラットフォームとして**Android Enterprise**を選択するようにアプリを編集します。

b. MDXファイルをアップロードします。アプリの承認プロセスを実行します。

c. MDXポリシーを選択します。

Enterprise MDXアプリの場合、MDX SDKモードでラップされたアプリに変更することをお勧めします。

- オプション1：組織にプライベートに割り当てられた開発者アカウントを使用して、Google PlayでAPKをホストします。Citrix Endpoint ManagementでMDXファイルを公開します。
- オプション2：Citrix Endpoint Managementからエンタープライズアプリとしてアプリを公開します。Citrix Endpoint ManagementでAPKを公開し、MDXファイルのプラットフォームとして**Android Enterprise**を選択します。

Citrixデバイスポリシーの移行

Android (従来のDA) と **Android Enterprise** の両方のプラットフォームで利用可能なポリシーの場合：ポリシーを編集し、プラットフォームとして**Android Enterprise**を選択します。

- Android Enterpriseの場合、デバイスの登録方法を考慮してください。一部のポリシーオプションは、ワークプロファイルモードまたは完全に管理されたモードのデバイスでのみ利用可能です。Android Enterpriseデバイスおよびアプリポリシーの構成を参照してください。
- 従来のDAデバイスにExchangeデバイスポリシーを使用している場合は、代わりにマネージド構成ポリシーデバイスポリシーを作成してメール設定を構成します。
- 意図したデバイス（Android Enterpriseと従来のDA）にポリシーを確実にターゲット設定するには、ポリシーに展開ルールを追加します。たとえば、従来のDAプラットフォームの場合、この展開ルールを使用します。

```
Limit by known device property name Android Enterprise

Enabled Device? Isn’t equal to true
```

その展開ルールは、デバイスがAndroid Enterpriseに対して有効になっていないかどうかを確認し、従来のDAに対して有効になっているデバイスにアプリとともにポリシーを配信します。

概念実証

アプリをAndroid Enterpriseに移行した後、移行テストを設定して、機能が意図どおりに動作していることを確認できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

推奨される概念実証のセットアップ

1. 展開インフラストラクチャをセットアップします。
    - Android Enterpriseテスト用のデリバリーグループを作成します。
    - Citrix エンドポイント管理で Android エンタープライズを構成します。
2. ユーザーアプリを設定します。
3. Android Enterprise機能を構成します。
4. Android Enterpriseデリバリーグループにポリシーを割り当てます。
5. 機能をテストして確認します。
6. 各ユースケースのデバイスセットアップウォークスルーを完了します。
7. ユーザーセットアップ手順を文書化します。

展開

これで、Android Enterpriseのセットアップを展開し、ユーザーを移行に備えさせることができます。

推奨される展開戦略

推奨されるCitrixの展開戦略は、すべての本番システムでAndroid Enterpriseをテストし、その後でデバイスの移行を完了することです。

- このシナリオでは、ユーザーは現在の構成でレガシーデバイスを使い続けます。新しいデバイスはAndroid Enterprise管理用に設定します。
- 既存のデバイスは、アップグレードまたは交換が必要な場合にのみ移行します。
- 既存のデバイスは、通常のライフサイクルの終わりにAndroid Enterprise管理に移行します。または、紛失や破損により交換が必要になったときにそれらのデバイスを移行します。

アンドロイド エンタープライズ

Android Enterprise は、Android デバイス向けのエンタープライズ管理ソリューションとして Google が提供するツールとサービスのセットです。Android Enterprise を使用すると、次のことができます。

- Citrix Endpoint Management を使用して、会社所有および個人所有 (BYOD) の Android デバイスを管理します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- デバイス全体、またはデバイス上の個別のプロファイルを管理できます。個別のプロファイルは、ビジネスアカウント、アプリ、データを個人アカウント、アプリ、データから分離します。
- 在庫管理など、単一の用途に特化したデバイスを管理することもできます。Android Enterprise でできることの概要については、Google の Android Enterprise Management を参照してください。

リソース:

- Android Enterprise に関連する用語と定義のリストについては、Google Android Enterprise 開発者ガイドの記事 Android Enterprise terminology を参照してください。Google はこれらの用語を頻繁に更新します。
- Citrix Endpoint Management でサポートされている Android オペレーティングシステムのリストについては、サポートされているデバイスのオペレーティングシステム を参照してください。
- Android Enterprise のネットワーク環境をセットアップする際に考慮すべきアウトバウンド接続については、Google サポート記事 Android Enterprise Network Requirements を参照してください。
- Android Enterprise の展開については、リソースの展開 を参照してください)。

Android Enterprise の利用開始

重要:

デバイス管理モードはサポートされなくなりました。ユーザーがデバイス管理モードのデバイスを使用している場合は、デバイス管理から Android Enterprise への移行 を参照してください。デバイスが Android Enterprise に移行されたら、次の手順で Android Enterprise デバイスをセットアップします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



初回セットアップ

1. マネージドGoogle Playアカウントを作成します。

   「Citrix Endpoint ManagementでのマネージドGoogle Playの使用」および「要件」を参照してください。

2. Google PlayアカウントをCitrix Endpoint Managementにバインドします。

   「Citrix Endpoint ManagementをGoogle Playに接続する」を参照してください。

3. デバイスの管理方法を計画します。

   「デバイス展開シナリオとプロファイル」を参照してください。

4. ユーザーデバイスの登録セキュリティを計画します。

   「登録セキュリティ」を参照してください。

5. MDX対応アプリを配信する準備をします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリの開発にはMAM SDKを使用します。新しいSDKへの移行準備ができていない場合は、コマンドラインベースのMDX Toolkitを使用してアプリをラップします。

「MAM SDKの概要」を参照してください。

この時点で、Android Enterpriseデバイスをアプリおよびデバイスポリシー、登録プロファイル、アプリで構成する準備が整いました。ガイダンスについては、次のセクションを参照してください。

デバイスを構成する

1. デリバリーグループを作成します。

   誰がどのリソースをいつ取得するかを制御します。「リソースの展開」を参照してください。

   レガシーDAプラットフォーム向けに公開されたアプリのAndroid Enterpriseに登録されているデバイスへの配信を停止します。Android Enterpriseデバイスの場合、Android Enterpriseプラットフォーム向けにアプリを公開します。DAモードのデバイスにレガシーDAアプリを公開し続けるには、それらのアプリ用に個別のデリバリーグループを作成します。「廃止」を参照してください。

2. アプリを追加します。Citrix Endpoint Managementコンソールから直接Google Playのアプリを承認できます。

   Googleサポート記事「組織内のアプリを管理する」を参照してください。

3. 登録プロファイルを作成します。

   デバイスとアプリの管理登録オプションを指定します。「デバイス展開シナリオとプロファイル」および「登録プロファイルの作成」を参照してください。

   - Android Enterpriseの公開アプリストアアプリをAndroidデバイスユーザーに展開すると、そのユーザーは自動的にAndroid Enterpriseに登録されます。
   - ゼロタッチ登録を使用すると、デバイスの電源が初めてオンになったときに自動的に登録されるように構成できます。「ゼロタッチ登録」を参照してください。

4. デバイスとアプリのポリシーを構成します。

   企業セキュリティとユーザーのプライバシーおよびユーザーエクスペリエンスのバランスを取ります。「Android Enterpriseデバイスおよびアプリポリシーの構成」を参照してください。

5. アプリを配布します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

マネージドGoogle Playを使用して、デバイス上のAndroid Enterpriseワークスペースに展開するアプリを追加、購入、および承認します。ユーザーは、管理者が利用可能にしたマネージドGoogle Playのアプリのみをインストールできます。

参照:

- Android Enterpriseアプリの配布
- マネージド構成ポリシー
- アプリ権限ポリシー

6. セキュリティアクションを設定して、コンプライアンスを監視および提供します。

   セキュリティアクションを参照してください。

Citrix Endpoint Managementで管理対象Google Playを使用する

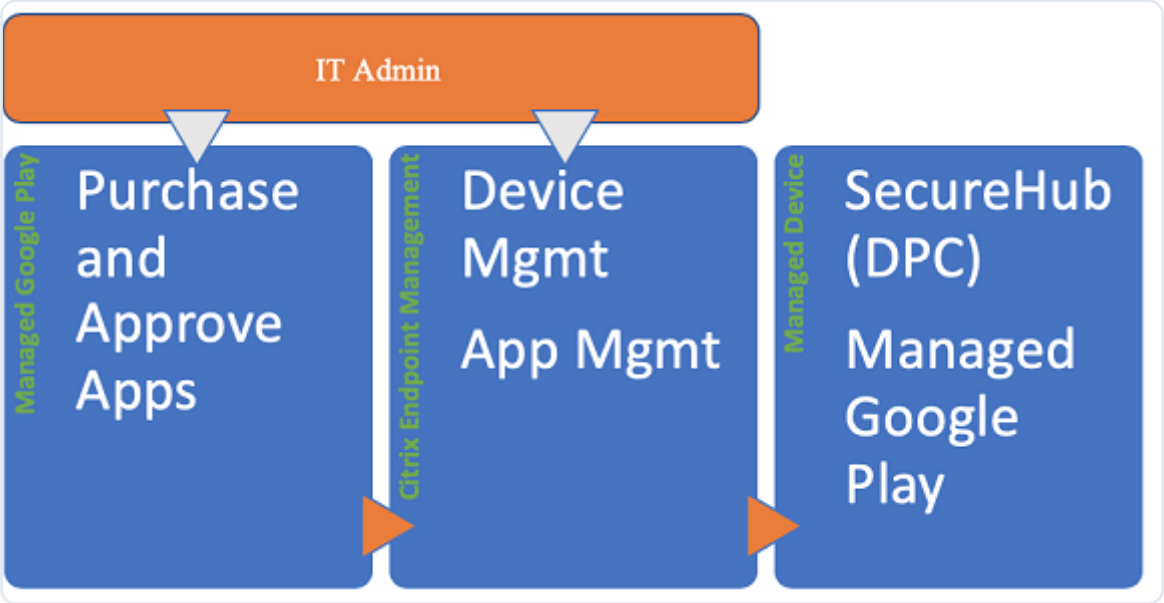
Citrix Endpoint Managementを管理対象Google Playと統合してAndroid Enterpriseを使用すると、エンタープライズが作成されます。Googleは、エンタープライズを組織とエンタープライズモビリティ管理 (EMM) ソリューション間のバインディングと定義しています。組織がソリューションを通じて管理するすべてのユーザーとデバイスは、そのエンタープライズに属します。

Android Enterpriseのエンタープライズには、EMMソリューション、デバイスポリシーコントローラー (DPC) アプリ、Googleエンタープライズアプリプラットフォームの3つのコンポーネントがあります。Citrix Endpoint ManagementをAndroid Enterpriseと統合すると、完全なソリューションには次のコンポーネントが含まれます。

- **Citrix Endpoint Management:** Citrix EMMです。Citrix Endpoint Managementは、安全なデジタルワークスペースのための統合されたCitrix Endpoint Managementです。Citrix Endpoint Managementは、IT管理者が組織のデバイスとアプリを管理する手段を提供します。
- **Citrix Secure Hub:** Citrix DPCアプリです。Citrix Secure Hubは、Citrix Endpoint Managementの起動パッドです。Citrix Secure Hubは、デバイスにポリシーを適用します。
- **管理対象Google Play:** Citrix Endpoint Managementと統合するGoogleエンタープライズアプリプラットフォームです。Google Play EMM APIは、アプリポリシーを設定し、アプリを配布します。

この図は、管理者がこれらのコンポーネントとどのようにやり取りし、コンポーネントが互いにどのようにやり取りするかを示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注：

CitrixをEMMプロバイダーとして登録するには、管理対象Google PlayまたはGoogle Workspace（旧G Suite）のいずれかを使用できます。この記事では、管理対象Google PlayでAndroid Enterpriseを使用する方法について説明します。組織がGoogle Workspaceを使用してアプリへのアクセスを提供している場合は、Android Enterpriseでそれを使用できます。Google Workspaceのお客様向けのレガシーAndroid Enterpriseを参照してください。

管理対象Google Playを使用する場合、デバイスとエンドユーザー向けに管理対象Google Playアカウントをプロビジョニングします。管理対象Google Playアカウントは、管理対象Google Playへのアクセスを提供し、ユーザーが利用可能なアプリをインストールして使用できるようにします。組織がサードパーティのIDサービスを使用している場合は、管理対象Google Playアカウントを既存のIDアカウントとリンクできます。

このタイプのエンタープライズはドメインに紐付けられていないため、単一の組織に対して複数のエンタープライズを作成できます。たとえば、組織内の各部門または地域は、異なるエンタープライズとして登録できます。異なるエンタープライズを使用すると、個別のデバイスとアプリのセットを管理できます。

Citrix Endpoint Management管理者にとって、管理対象Google Playは、Google Playのユーザーエクスペリエンスとアプリストア機能を、エンタープライズ向けに設計された一連の管理機能と組み合わせています。管理対象Google Playを使用して、デバイス上のAndroid Enterpriseワークスペースに展開するアプリを追加、購入、承認します。Google Playを使用して、公開アプリ、プライベートアプリ、サードパーティアプリを展開できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理対象デバイスのユーザーにとって、管理対象のGoogle Playはエンタープライズアプリストアです。ユーザーはアプリを閲覧し、アプリの詳細を表示し、インストールできます。Google Playの公開バージョンとは異なり、ユーザーは管理対象のGoogle Playから、利用可能にしたアプリのみをインストールできます。

デバイス展開シナリオとプロファイル

デバイス展開シナリオとは、展開するデバイスの所有者と、それらをどのように管理するかを指します。デバイスプロファイルとは、DPCがデバイス上でポリシーを管理および適用する方法を指します。

仕事用プロファイルは、ビジネスアカウント、アプリ、データを個人アカウント、アプリ、データから分離します。仕事用プロファイルと個人用プロファイルはOSレベルで分離されています。仕事用プロファイルの詳細は、仕事用プロファイルとはを参照してください。

重要:

Android EnterpriseデバイスがAndroid 11にアップデートされると、Googleは「仕事用プロファイルを持つ完全管理」として管理されているデバイスを、新しいセキュリティ強化された仕事用プロファイルエクスペリエンスに移行します。この新しい登録モードは「企業所有デバイス上の仕事用プロファイル」と呼ばれます。詳細については、Android Enterpriseの仕事用プロファイルを持つ完全管理の今後の変更点を参照してください。 Android 12デバイスについては、仕事用プロファイルのセキュリティとプライバシーの強化を参照してください。

デバイス管理	ユースケース	仕事用プロファイル	個人用プロファイル	備考
会社所有デバイス（完全管理）	仕事専用の会社所有デバイス	いいえ	いいえ	新規デバイスまたは工場出荷時設定にリセットされたデバイスのみ。「Android Enterpriseの完全管理デバイスのプロビジョニング」(#provisioning-android-enterprise-fully-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイス管理	ユースケース	仕事用プロファイル	個人用プロファイル	備考
				managed-devices)を参照してください。
ワークプロファイルによる完全管理 / 会社所有デバイス上のワークプロファイル	仕事用および個人用として使用される会社所有デバイス	はい	はい。これらのデバイスでは、DPCの2つのコピーが実行されます。1つはデバイスオーナーモードでデバイスを管理し、もう1つはプロファイルオーナーモードでワークプロファイルを管理します。デバイスとワークプロファイルに個別のポリシーを適用できます。	「ワークプロファイルによるAndroid Enterpriseの完全管理デバイスのプロビジョニング、または会社所有デバイス上のワークプロファイル」(#provisioning-android-enterprise-fully-managed-devices-with-a-work-profile-or-work-profile-on-corporate-owned-devices)を参照してください。
専用デバイス*	デジタルサイネージやチケット印刷など、単一のユースケース向けに構成された会社所有デバイス	いいえ	いいえ	「Android Enterprise専用デバイスのプロビジョニング」(#provisioning-dedicated-android-enterprise-devices)を参照してください。
BYODワークプロファイル**	ワークプロファイル管理で登録された個人デバ	はい	はい。DPCはワークプロファイルのみを管理	これらのデバイスは新品である必要はなく、工

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイス管理	ユースケース	仕事用プロファイル	個人用プロファイル	備考
	イス（プロファイルオーナーモードとも呼ばれます）		し、デバイス全体は管理しません。	場出荷時の状態にリセットする必要もありません。(#provisioning-android-enterprise-work-profile-devices)「Android Enterpriseワークプロファイルデバイスのプロビジョニング」を参照してください。

* ユーザーは専用デバイスを共有できます。ユーザーが専用デバイス上のアプリにサインオンすると、その作業の状態はデバイスではなくアプリに紐付けられます。

** Citrix Endpoint Managementは、BYODワークプロファイルモードでのZebraデバイスをサポートしていません。Citrix Endpoint Managementは、Android Enterpriseを使用して、完全に管理されたデバイスとしてZebraデバイスをサポートしています。

登録セキュリティ

登録プロファイルは、AndroidデバイスがMAM、MDM、またはMDM+MAMのいずれに登録されるかを決定し、ユーザーがMDMをオプトアウトするオプションを提供します。

セキュリティレベルと必要な登録手順の指定については、(/ja-jp/citrix-endpoint-management/users.html#configure-enrollment-security-modes)「ユーザーアカウント、役割、および登録」を参照してください。

Citrix Endpoint Managementは、MDMまたはMDM+MAMに登録されたAndroidデバイスに対して、以下の認証方法をサポートしています。詳細については、以下の記事を参照してください。

- (/ja-jp/citrix-endpoint-management/authentication/authentication-domain-security-token.html)「ドメインまたはドメインとセキュリティトークン認証」

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- (/ja-jp/citrix-endpoint-management/authentication/client-certificate.html)「クライアント証明書または証明書とドメイン認証」
- IDプロバイダー：
  - (/ja-jp/citrix-endpoint-management/authentication/authentication-with-azure-active-directory-through-citrix-cloud.html)「Citrix Cloudを介したAzure Active Directoryによる認証」（プレビュー）
  - (/ja-jp/citrix-endpoint-management/authentication/authentication-with-okta-through-citrix-cloud.html)「Citrix Cloudを介したOktaによる認証」（プレビュー）

あまり使用されない認証方法として、クライアント証明書とセキュリティトークンがあります。詳細については、`<https://support.citrix.com/article/CTX215200>`を参照してください。

要件

Android Enterpriseの使用を開始する前に、以下が必要です。

- アカウントと資格情報:
  - マネージドGoogle PlayでAndroid Enterpriseをセットアップするには、企業用Googleアカウント
  - 最新のMDXファイルをダウンロードするには、Citrix®カスタマーアカウント
- Firebase Cloud Messaging (FCM)と、Citrix Endpoint Management用に構成された接続スケジューリングデバイスポリシー。詳細については、Firebase Cloud Messagingおよび接続スケジューリングデバイスポリシーを参照してください。

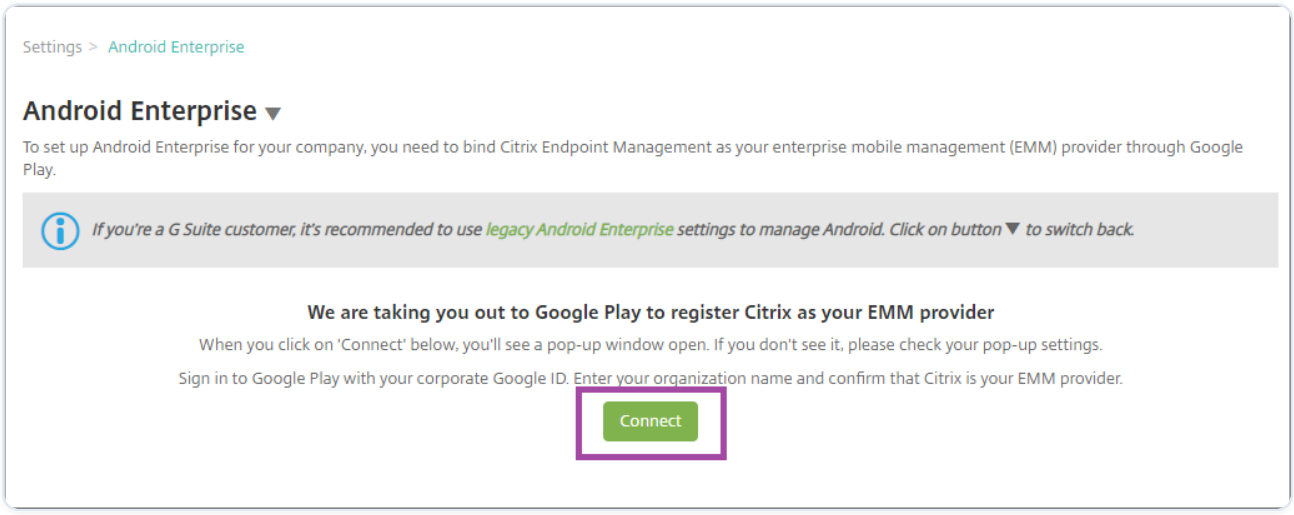
Citrix Endpoint ManagementをGoogle Playに接続する

組織でAndroid Enterpriseをセットアップするには、マネージドGoogle Playを介してCitrixをEMMプロバイダーとして登録します。このセットアップにより、マネージドGoogle PlayがCitrix Endpoint Managementに接続され、Citrix Endpoint Management内にAndroid Enterprise用のエンタープライズが作成されます。

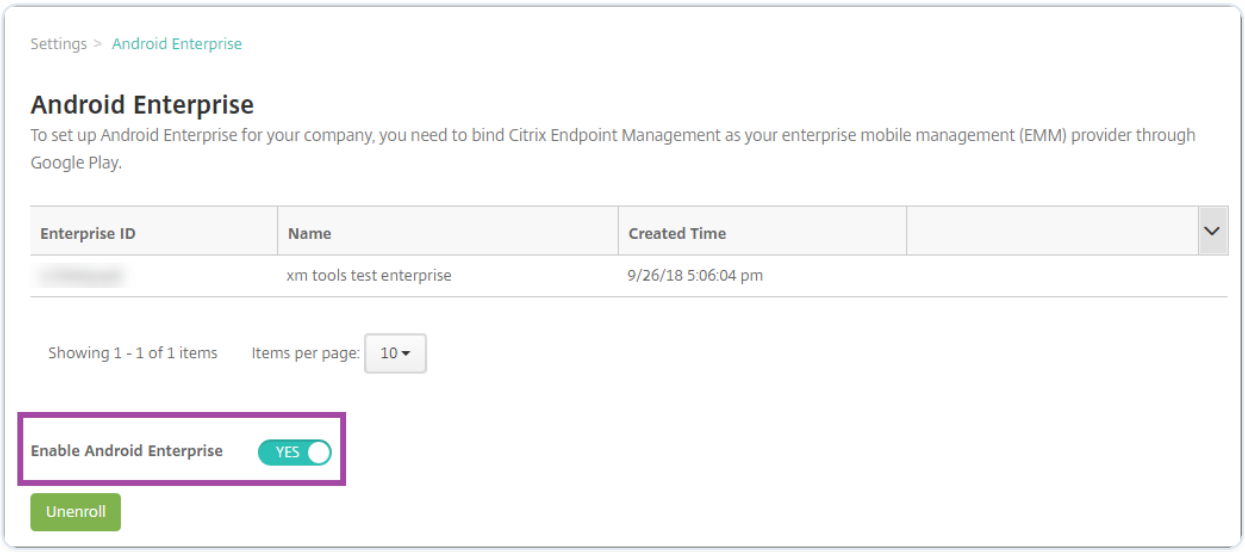
Google Playにサインインするには、企業用Googleアカウントが必要です。

1. Citrix Endpoint Managementコンソールで、**［設定］>［Android Enterprise］**の順に移動します。
2. **［接続］**をクリックします。Google Playが開きます。

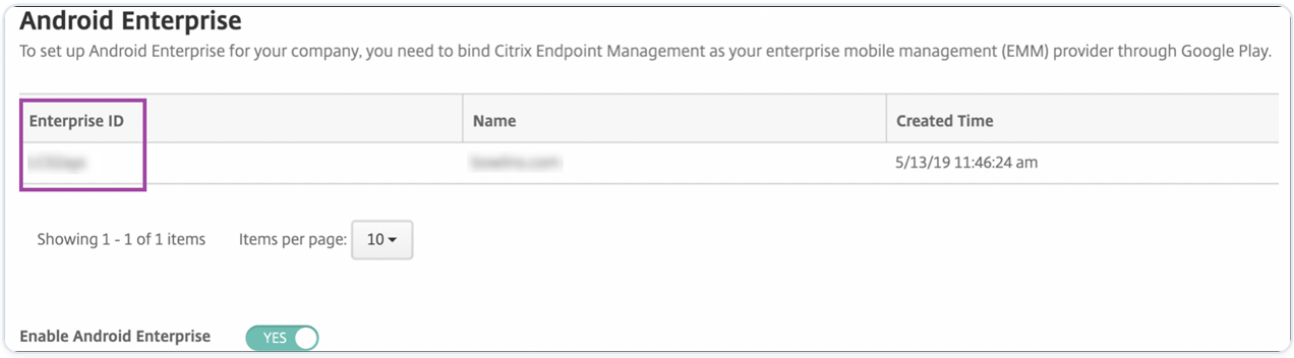
© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. 企業用Googleアカウントの資格情報を使用してGoogle Playにサインインします。組織名を入力し、CitrixがEMMプロバイダーであることを確認します。
2. Android Enterpriseのエンタープライズ**ID**が追加されます。Android Enterpriseを有効にするには、**［Android Enterpriseを有効にする］を［はい］**にスライドします。



エンタープライズ**ID**がCitrix Endpoint Managementコンソールに表示されます。



お使いの環境はGoogleに接続されており、デバイスを管理する準備ができています。これで、ユーザーにアプリを提供できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementは、Citrixモバイル生産性アプリ、MDXアプリ、パブリックアプリストアアプリ、WebおよびSaaSアプリ、エンタープライズアプリ、Webリンクをユーザーに提供できます。これらの種類のアプリをユーザーに提供する方法について詳しくは、「Android Enterpriseアプリの配布」を参照してください。

次のセクションでは、モバイル生産性アプリを提供する方法について説明します。

Android EnterpriseユーザーにCitrixモバイル生産性アプリを提供する

Android EnterpriseユーザーにCitrixモバイル生産性アプリを提供するには、次の手順が必要です。

1. アプリをMDXアプリとして公開します。「MDXアプリとしてアプリを構成する」を参照してください。
2. ユーザーがデバイス上のワークプロファイルにアクセスするために使用するセキュリティチャレンジのルールを構成します。「セキュリティチャレンジポリシーを構成する」を参照してください。

公開したアプリは、Android Enterpriseエンタープライズに登録されているデバイスで利用できます。

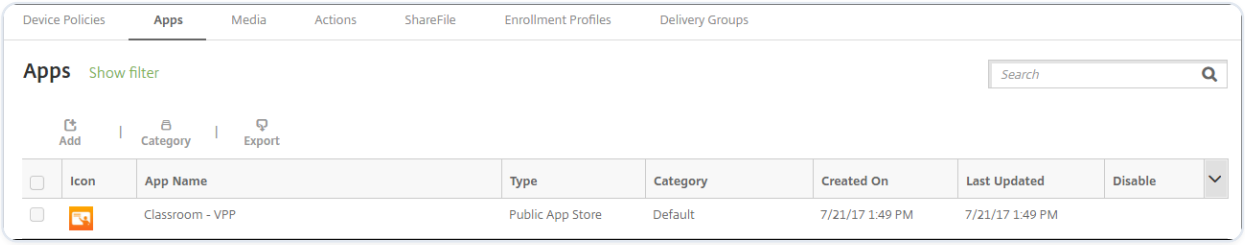
注：

Android EnterpriseパブリックアプリストアアプリをAndroidユーザーに展開すると、そのユーザーは自動的にAndroid Enterpriseに登録されます。

MDXアプリとしてアプリを構成する

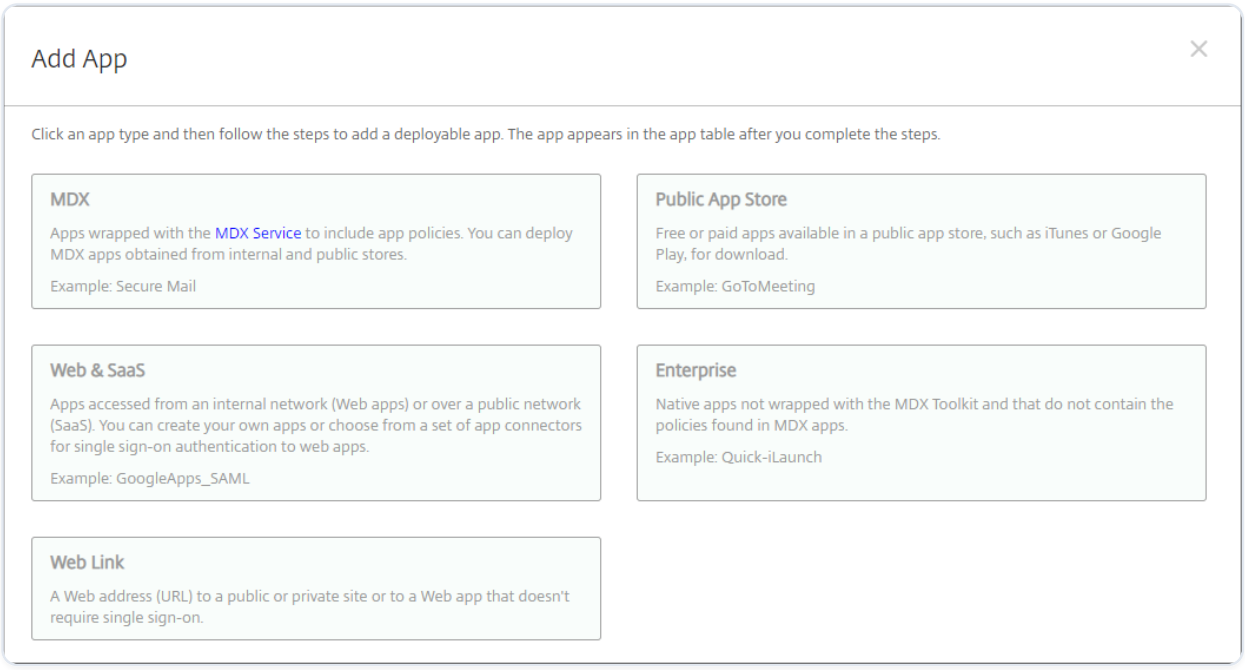
Citrix生産性アプリをAndroid Enterprise用のMDXアプリとして構成するには：

1. Citrix Endpoint Managementコンソールで、**［構成］>［アプリ］** の順にクリックします。**［アプリ］** ページが表示されます。



2. **［追加］** をクリックします。**［アプリの追加］** ダイアログボックスが表示されます。

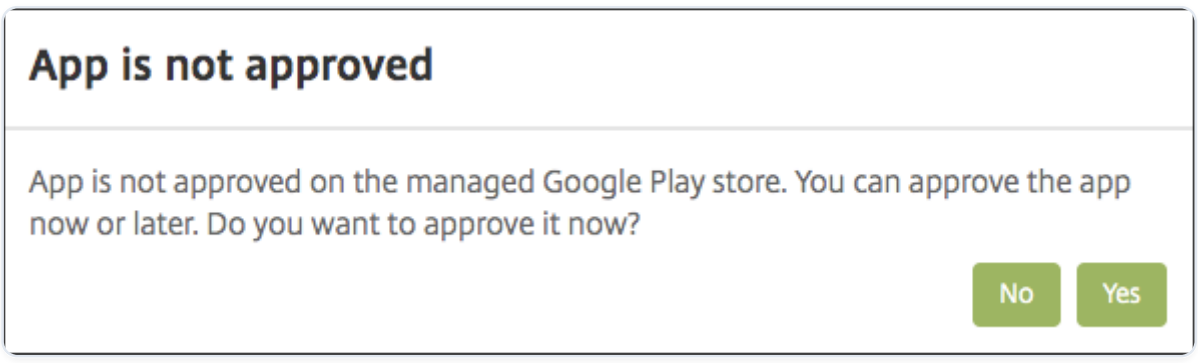
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. **MDX**をクリックします。**アプリ情報**ページが表示されます。
4. ページの左側で、プラットフォームとして**Android Enterprise**を選択します。
5. **アプリ情報**ページで、次の情報を入力します。

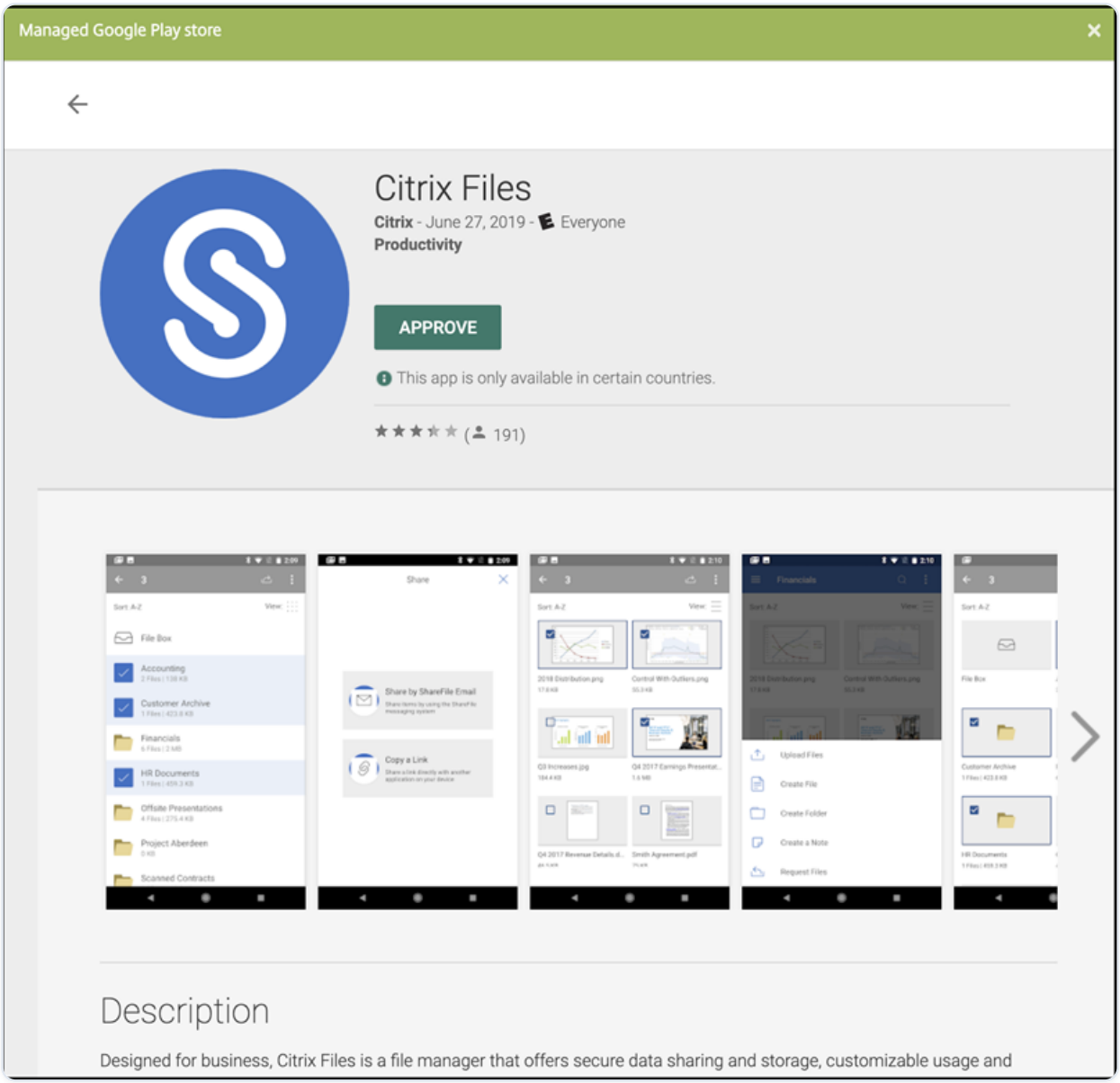
   - **名前:** アプリのわかりやすい名前を入力します。この名前は、**アプリ**テーブルの**アプリ名**の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。

6. **次へ**をクリックします。**Android Enterprise MDXアプリ**ページが表示されます。
7. **アップロード**をクリックし、アプリの.mdxファイルのファイル場所に移動します。ファイルを選択し、**開く**をクリックします。
8. 添付されたアプリケーションが管理対象のGoogle Playストアからの承認を必要とする場合、UIが通知します。Citrix Endpoint Managementコンソールを離れることなくアプリケーションを承認するには、**はい**をクリックします。



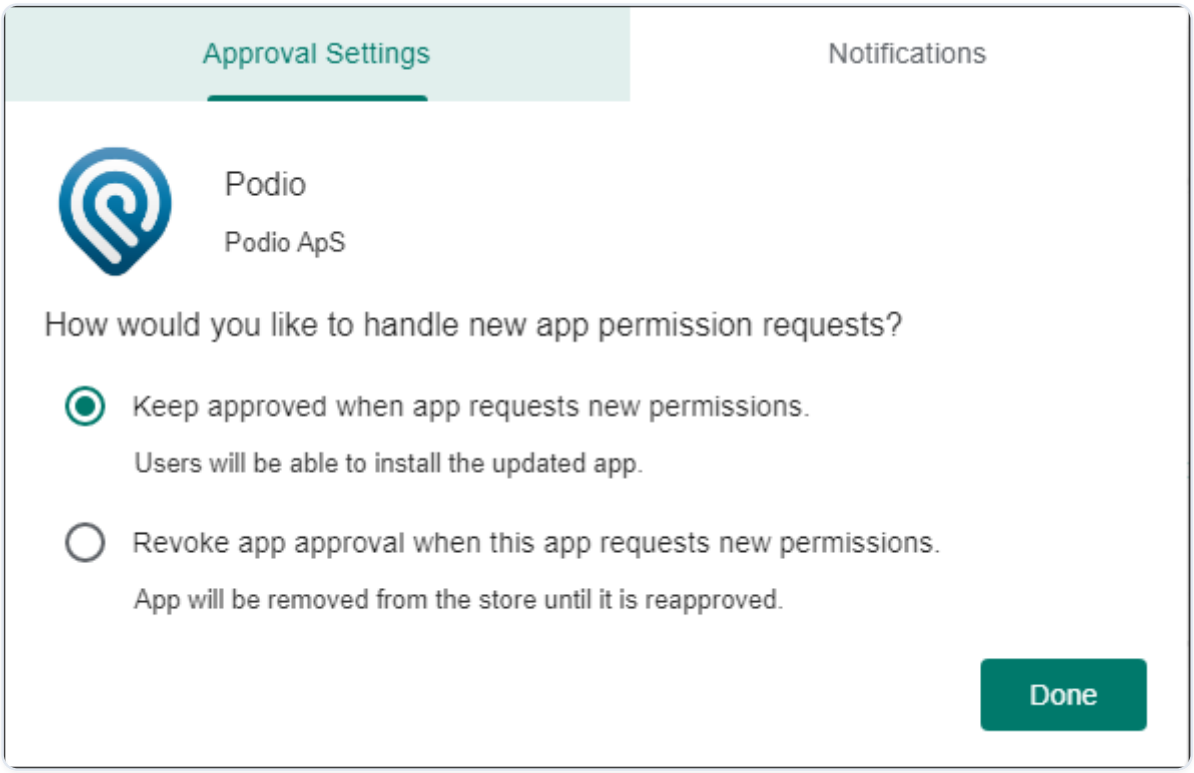
© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. 管理対象のGoogle Playストアページが開いたら、**承認**をクリックします。



10. もう一度**承認**をクリックします。
11. **アプリが新しい権限を要求した場合でも承認を維持する**を選択します。**保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



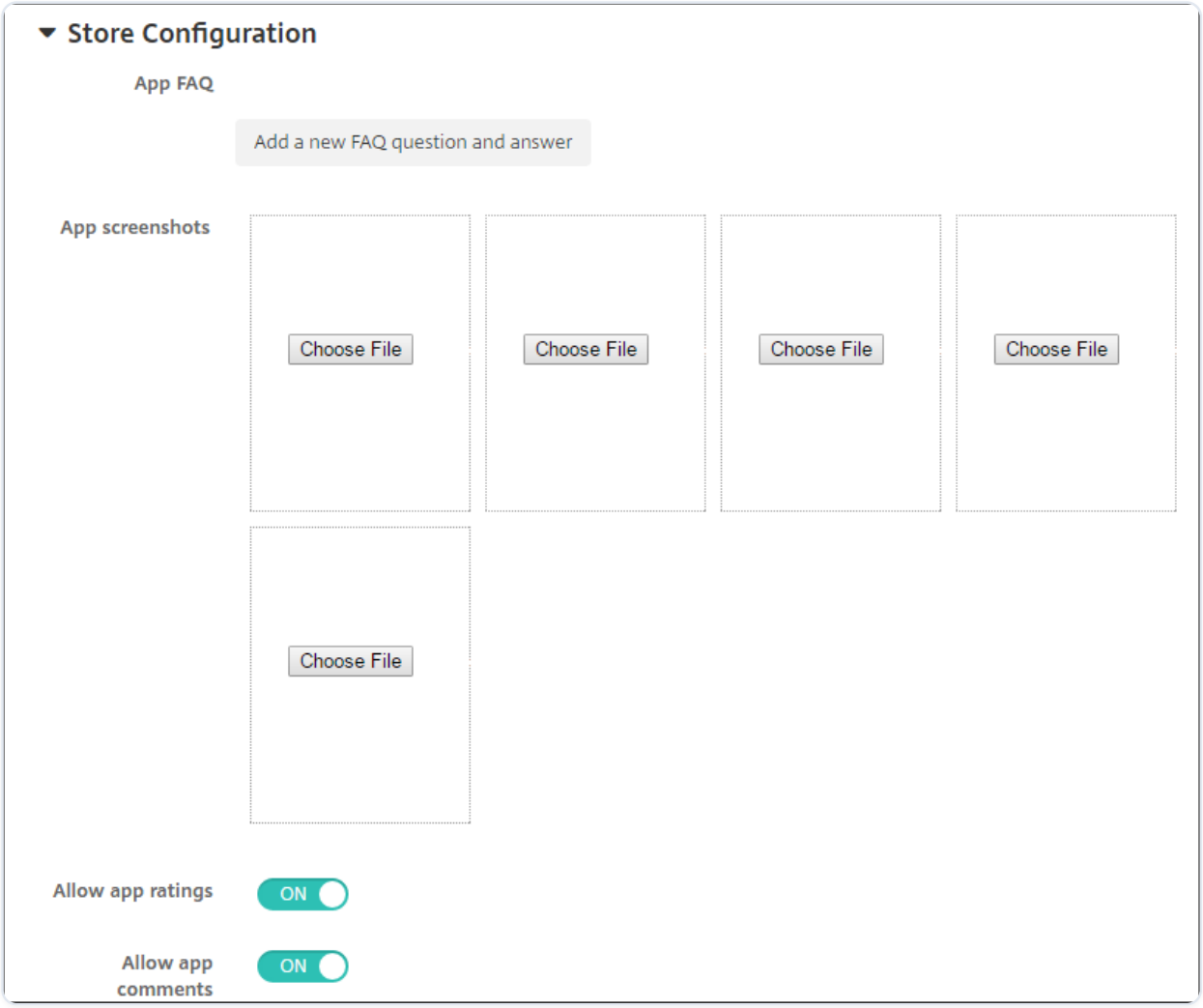
12. アプリが承認されて保存されると、ページにさらに設定が表示されます。これらの設定を構成します。

    - **ファイル名:** アプリに関連付けられているファイル名を入力します。
    - **アプリの説明:** アプリの説明を入力します。
    - **プロダクトトラック:** ユーザーデバイスにプッシュするプロダクトトラックを指定します。テスト用に設計されたトラックがある場合は、それを選択してユーザーに割り当てることができます。デフォルトは「本番」です。
    - **アプリのバージョン:** 必要に応じて、アプリのバージョン番号を入力します。
    - **パッケージID:** Google PlayストアにあるアプリのURL。
    - **最小OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
    - **最大OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
    - **除外デバイス:** 必要に応じて、アプリを実行できないデバイスの製造元またはモデルを入力します。

13. **MDXポリシー**を構成します。MDXアプリのアプリポリシーの詳細については、「MDXポリシーの概要」および「MAM SDKの概要」を参照してください。
14. 展開ルールを構成します。詳細については、「リソースの展開」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

15. **ストア構成**を展開します。この設定は、管理対象のGoogle Playにのみ表示されるAndroid Enterpriseアプリには適用されません。



必要に応じて、アプリのFAQやアプリストアに表示されるスクリーンショットを追加できます。また、ユーザーがアプリを評価したりコメントしたりできるかどうかを設定することもできます。

- これらの設定を構成します。
  - **アプリのFAQ:** アプリのFAQの質問と回答を追加します。
  - **アプリのスクリーンショット:** アプリストアでアプリを分類するのに役立つスクリーンショットを追加します。アップロードするグラフィックはPNGである必要があります。GIFまたはJPEG画像はアップロードできません。
  - **アプリの評価を許可:** ユーザーがアプリを評価することを許可するかどうかを選択します。デフォルトは**オン**です。 **アプリのコメントを許可:** ユーザーが選択したアプリについてコメントすることを許可するかどうかを選択します。デフォルトは**オン**です。

16. **次へ**をクリックします。**承認**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ構成画面(/en-us/citrix-endpoint-management/media/configure-apps-approvals-workflow.png)

ユーザーアカウントを作成する際に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定しない場合は、手順15に進むことができます。

ワークフローを割り当てるか作成するには、次の設定を構成します。

- **使用するワークフロー:** ドロップダウンリストから既存のワークフローをクリックするか、**新しいワークフローの作成**をクリックします。デフォルトは**なし**です。
- **新しいワークフローの作成**を選択した場合は、これらの設定を構成します。詳細については、「ワークフローの作成と管理」を参照してください。
- **名前:** ワークフローの一意の名前を入力します。
- **説明:** 必要に応じて、ワークフローの説明を入力します。
- **メール承認テンプレート:** リストから、割り当てるメール承認テンプレートを選択します。このフィールドの右側にある目のアイコンをクリックすると、テンプレートをプレビューできるダイアログボックスが表示されます。
- **マネージャー承認レベル:** リストから、このワークフローに必要なマネージャー承認レベルの数を選択します。デフォルトは1レベルです。可能なオプションは次のとおりです。
  - 不要
  - 1 レベル
  - 2 レベル
  - 3 レベル
- **Active Directory ドメインの選択:** リストから、ワークフローに使用する適切な Active Directory ドメインを選択します。
- **追加の必須承認者の検索:** 検索フィールドに追加の必須承認者の名前を入力し、**検索**をクリックします。名前は Active Directory に登録されています。
- フィールドに名前が表示されたら、名前の横にあるチェックボックスをオンにします。名前とメールアドレスが**選択された追加の必須承認者**リストに表示されます。
  - **選択された追加の必須承認者**リストからユーザーを削除するには、次のいずれかを実行します。
    - **検索**をクリックして、選択したドメイン内のすべてのユーザーのリストを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 検索ボックスに氏名または部分的な名前を入力し、**検索**をクリックして検索結果を絞り込みます。
- **選択された追加の必須承認者**リストのユーザーには、検索結果リストの名前の横にチェックマークが付いています。リストをスクロールし、削除する各名前の横にあるチェックボックスをオフにします。

17. **次へ**をクリックします。**デリバリーグループの割り当て**ページが表示されます。

アプリ構成画面(/en-us/citrix-endpoint-management/media/configure-apps-delivery-groups.png)

18. **デリバリーグループの選択**の横で、デリバリーグループを検索するためにタイプするか、リストから1つまたは複数のグループを選択します。選択したグループは、**アプリの割り当てを受け取るデリバリーグループ**リストに表示されます。
19. **展開スケジュール**を展開し、次の設定を構成します。

- **展開**の横で、**オン**をクリックして展開をスケジュールするか、**オフ**をクリックして展開を防止します。デフォルトのオプションは**オン**に設定されています。
- 展開スケジュールの横にある「**今すぐ**」または「**後で**」をクリックします。デフォルトオプションは「**今すぐ**」に設定されています。
- 「**後で**」をクリックした場合は、カレンダーアイコンをクリックして、展開の日付と時刻を選択します。
- **展開条件**の横にある「**接続ごとに**」または「**以前の展開が失敗した場合のみ**」をクリックします。デフォルトオプションは「**接続ごとに**」に設定されています。
- **常時接続の展開**の横にある「**オフ**」が選択されていることを確認します。デフォルトオプションは「**オフ**」に設定されています。常時接続は、バージョン10.18.19以降でCitrix Endpoint Managementの使用を開始したお客様のAndroid Enterpriseでは利用できません。バージョン10.18.19より前にCitrix Endpoint Managementの使用を開始したお客様には、この接続をお勧めしません。

  このオプションは、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

  構成する展開スケジュールは、すべてのプラットフォームで同じです。「**常時接続の展開**」を除き、行った変更はすべてのプラットフォームに適用されます。

20. 「**保存**」をクリックします。

各モバイル生産性向上アプリについて、これらの手順を繰り返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

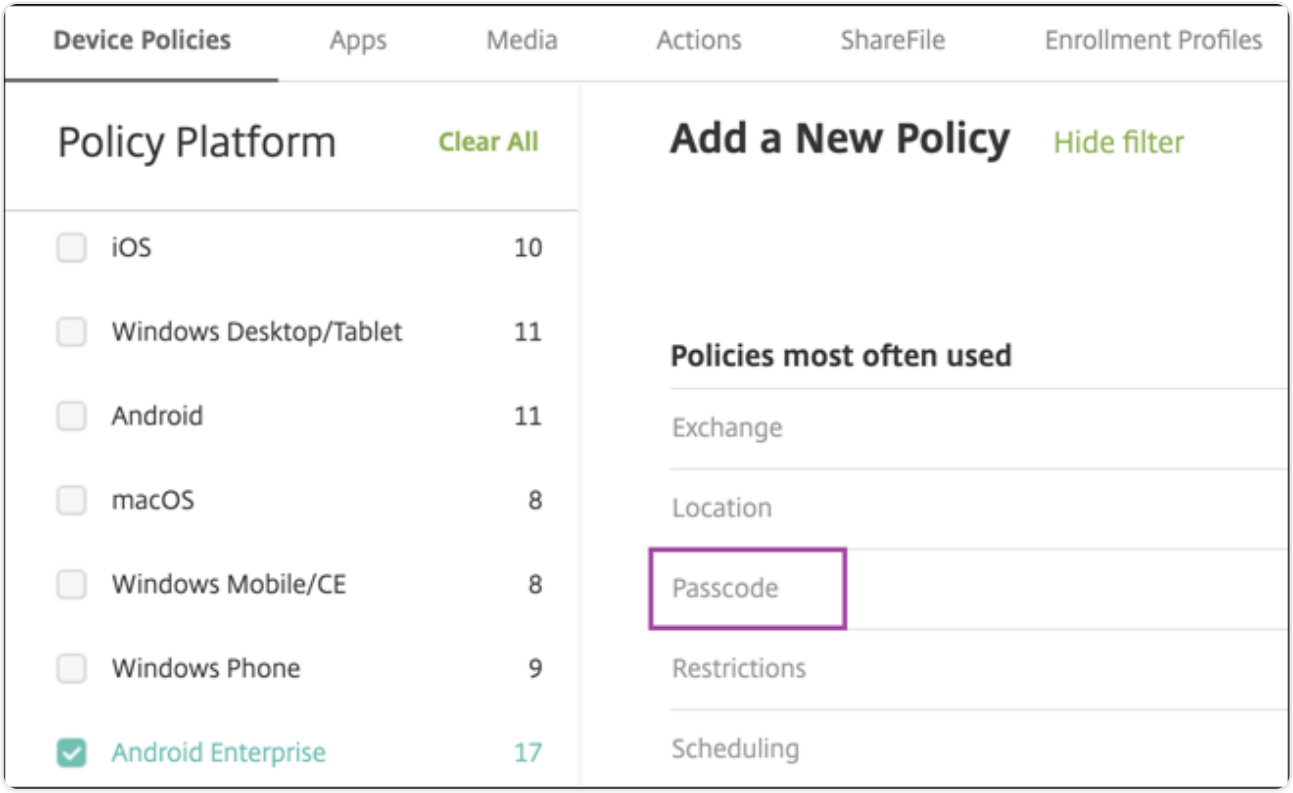
セキュリティチャレンジポリシーを構成する

Citrix Endpoint Managementのパスコードデバイスポリシーは、セキュリティチャレンジルールを構成します。ユーザーがデバイスまたはデバイス上のAndroid Enterpriseワークプロファイルにアクセスすると、チャレンジが表示されます。セキュリティチャレンジは、パスコードまたは生体認証にすることができます。パスコードポリシーについて詳しくは、「パスコードデバイスポリシー」を参照してください。

- Android Enterpriseの展開にBYODデバイスが含まれている場合は、ワークプロファイル用のパスコードポリシーを構成します。
- 展開に会社所有の完全に管理されたデバイスが含まれている場合は、デバイス自体のパスコードポリシーを構成します。
- 展開に両方の種類のデバイスが含まれている場合は、両方の種類のパスコードポリシーを構成します。

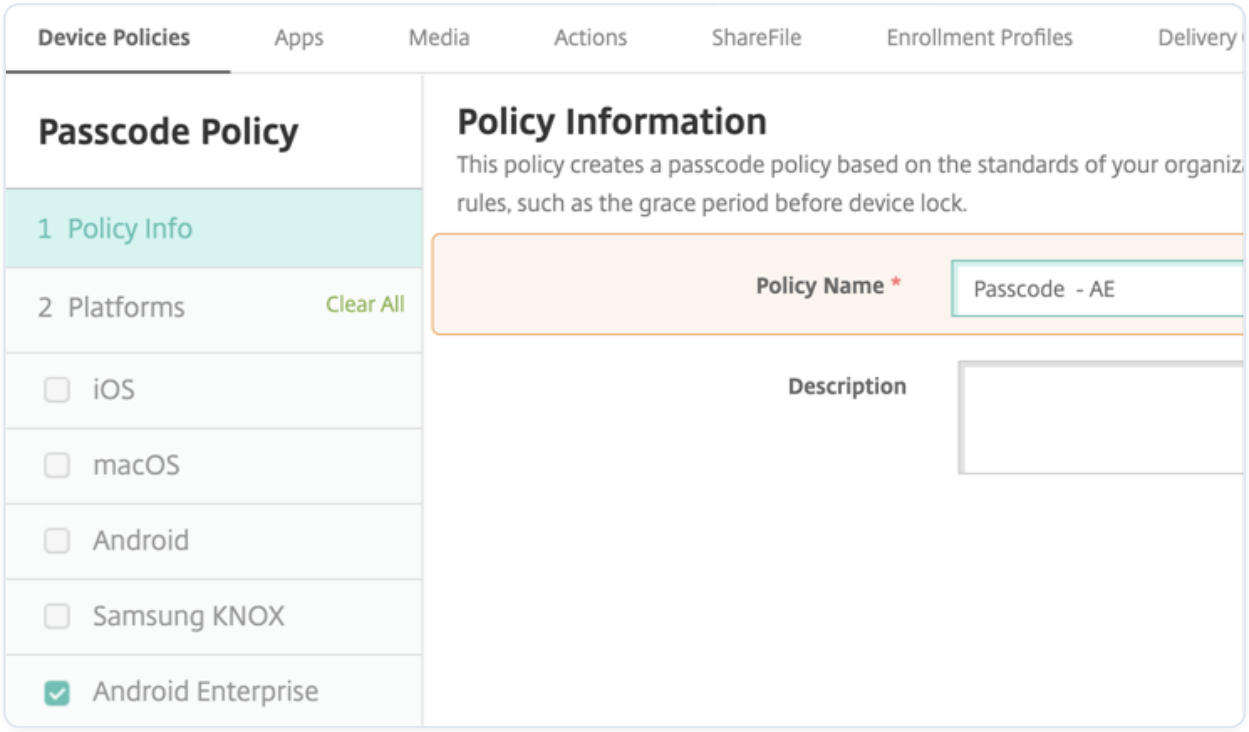
パスコードポリシーを構成するには：

1. Citrix Endpoint Managementコンソールで、**構成 > デバイスポリシー**に移動します。
2. 「**追加**」をクリックします。
3. 「**フィルターの表示**」をクリックして「**ポリシープラットフォーム**」ペインを表示します。「**ポリシープラットフォーム**」ペインで、「**Android Enterprise**」を選択します。
4. 右側のペインで「**パスコード**」をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 「**ポリシー名**」を入力します。「**次へ**」をクリックします。



2. パスコードポリシー設定を構成します。
   - 「**デバイスのパスコードが必要**」を「**オン**」に設定して、デバイス自体のセキュリティチャレンジで利用可能な設定を表示します。
   - 「**仕事用プロファイルのセキュリティチャレンジ**」を「**オン**」に設定して、仕事用プロファイルのセキュリティチャレンジで利用可能な設定を表示します。
3. 「**次へ**」をクリックします。
4. ポリシーを1つ以上のデリバリーグループに割り当てます。
5. 「**保存**」をクリックします。

登録プロファイルの作成

登録プロファイルは、Citrix Endpoint Management展開でAndroid Enterpriseが有効になっている場合に、Androidデバイスがどのように登録されるかを制御します。Android Enterpriseデバイスを登録するための登録プロファイルを作成すると、新規デバイスおよび工場出荷時設定にリセットされたデバイスを次のように登録するように登録プロファイルを構成できます。

- 完全管理対象デバイス
- 専用デバイス
- ワークプロファイルを持つ完全管理対象デバイス/会社所有デバイス上のワークプロファイル

© 1997–2026 Citrix Systems, Inc. All rights reserved.

これらの各Android Enterprise登録プロファイルを、BYOD Androidデバイスをワークプロファイルデバイスとして登録するように構成することもできます。

Citrix Endpoint Management展開でAndroid Enterpriseが有効になっている場合、新しく登録された、または再登録されたすべてのAndroidデバイスはAndroid Enterpriseデバイスとして登録されます。デフォルトでは、グローバル登録プロファイルは、新規および工場出荷時設定にリセットされたAndroidデバイスを完全管理対象デバイスとして登録し、BYOD Androidデバイスを会社所有デバイス上のワークプロファイルとして登録します。

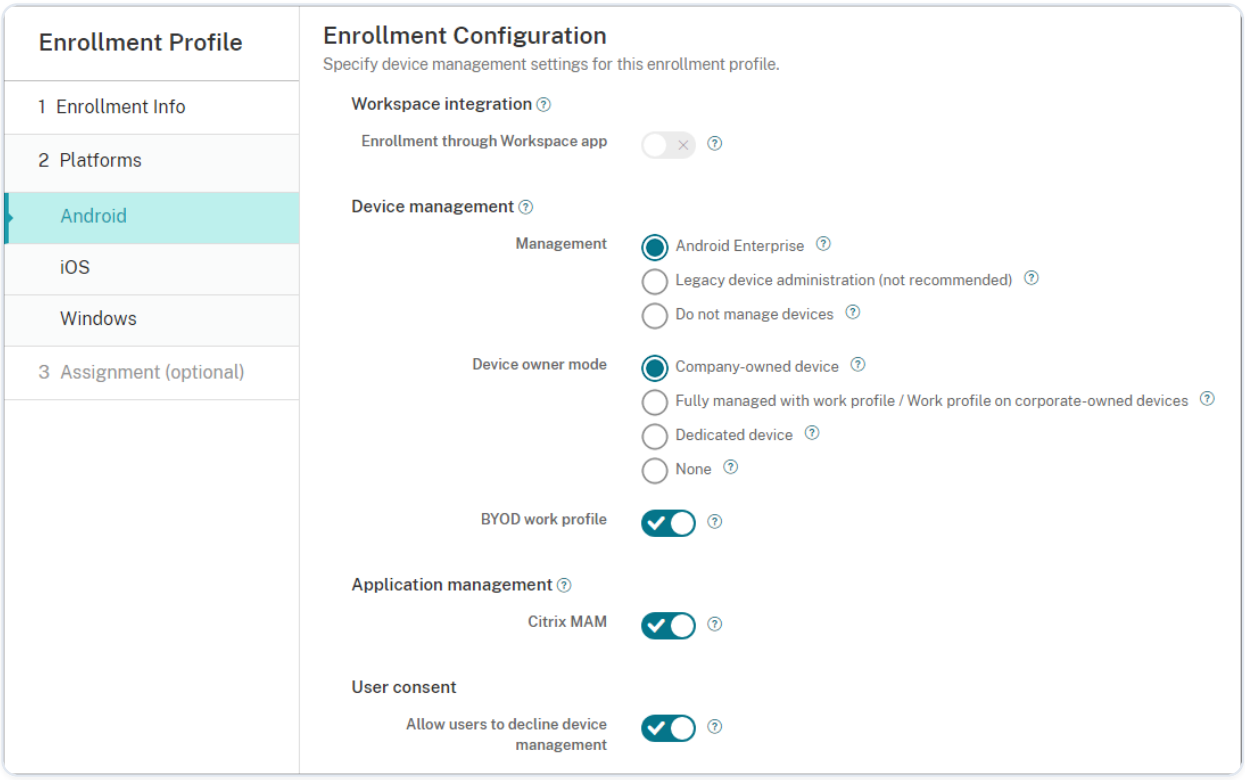
登録プロファイルを作成するときは、それらにデリバリーグループを割り当てます。ユーザーが異なる登録プロファイルを持つ複数のデリバリーグループに属している場合、デリバリーグループの名前によって使用される登録プロファイルが決まります。Citrix Endpoint Managementは、デリバリーグループのアルファベット順リストで最後に表示されるデリバリーグループを選択します。詳細については、「登録プロファイル」を参照してください。

完全管理対象デバイスの登録プロファイルを追加する

グローバル登録プロファイルはデフォルトで完全管理対象デバイスを登録しますが、完全管理対象デバイスを登録するための登録プロファイルをさらに作成できます。

1. Citrix Endpoint Managementコンソールで、**［構成］>［登録プロファイル］**の順に選択します。
2. 登録プロファイルを追加するには、**［追加］**をクリックします。［登録情報］ページで、登録プロファイルの名前を入力します。
3. このプロファイルを持つメンバーが登録できるデバイスの数を設定します。
4. **［プラットフォーム］の下で［Android］を選択するか、［次へ］**をクリックします。［登録構成］ページが表示されます。
5. **［管理］を［Android Enterprise］**に設定します。
6. **［デバイス所有者モード］を［会社所有デバイス］**に設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. **BYODワークプロファイル**を使用すると、BYODデバイスをワークプロファイルデバイスとして登録するように登録プロファイルを構成できます。新規および工場出荷時設定にリセットされたデバイスは、完全管理対象デバイスとして登録されます。BYODデバイスをワークプロファイルデバイスとして登録できるようにするには、**［BYODワークプロファイル］を［オン］に設定します。登録を完全管理対象デバイスに制限するには、［BYODワークプロファイル］を［オフ］に設定します。デフォルトは［オン］**です。
8. Citrix MAMにデバイスを登録するかどうかを選択します。
9. もし**BYODワークプロファイル**を**オン**に設定した場合、ユーザーの同意を設定します。BYODワークプロファイルデバイスのユーザーがデバイスを登録する際にデバイス管理を拒否できるようにするには、**ユーザーがデバイス管理を拒否することを許可する**を**オン**に設定します。

   BYODワークプロファイルが**オン**に設定されている場合、**ユーザーがデバイス管理を拒否することを許可する**のデフォルト値は**オン**です。**BYODワークプロファイル**が**オフ**に設定されている場合、**ユーザーがデバイス管理を拒否することを許可する**は無効になります。
10. **割り当て (オプション)** を選択します。デリバリーグループ割り当て画面が表示されます。
11. フルマネージドデバイスを登録する管理者が所属するデリバリーグループを選択します。次に、**保存**をクリックします。

    追加したプロファイルを含む登録プロファイルページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

専用デバイス登録プロファイルを追加する

Citrix Endpoint Managementの展開に専用デバイスが含まれている場合、1人のCitrix Endpoint Management管理者または少数の管理者グループが多数の専用デバイスを登録します。これらの管理者がすべての必要なデバイスを登録できるようにするには、ユーザーごとに無制限のデバイスを許可する登録プロファイルを作成します。

1. Citrix Endpoint Managementコンソールで、**構成 > 登録プロファイル**に移動します。
2. 登録プロファイルを追加するには、**追加**をクリックします。登録情報ページで、登録プロファイルの名前を入力します。このプロファイルを持つメンバーが登録できるデバイスの数を**無制限**に設定します。
3. **プラットフォーム**の下にある**Android**を選択するか、**次へ**をクリックします。登録構成ページが表示されます。
4. **管理**を**Android Enterprise**に設定します。
5. **デバイス所有者モード**を**専用デバイス**に設定します。

   登録プロファイルページ(/en-us/citrix-endpoint-management/media/android-enterprise-enrollment-profile-dedicated-device.png)
6. **BYODワークプロファイル**を使用すると、BYODデバイスをワークプロファイルデバイスとして登録するように登録プロファイルを構成できます。新規デバイスおよび工場出荷時設定にリセットされたデバイスは、専用デバイスとして登録されます。BYODデバイスをワークプロファイルデバイスとして登録できるようにするには、**BYODワークプロファイル**を**オン**に設定します。登録を会社所有のデバイスに制限するには、**BYODワークプロファイル**を**オフ**に設定します。デフォルトは**オン**です。
7. Citrix MAMにデバイスを登録するかどうかを選択します。
8. **BYODワークプロファイル**を**オン**に設定した場合、ユーザーの同意を設定します。BYODワークプロファイルデバイスのユーザーがデバイスを登録する際にデバイス管理を拒否できるようにするには、**ユーザーがデバイス管理を拒否することを許可する**を**オン**に設定します。

   BYODワークプロファイルが**オン**に設定されている場合、**ユーザーがデバイス管理を拒否することを許可する**のデフォルト値は**オン**です。**BYODワークプロファイル**が**オフ**に設定されている場合、**ユーザーがデバイス管理を拒否することを許可する**は無効になります。
9. **割り当て（オプション）**を選択します。デリバリーグループ割り当て画面が表示されます。
10. 専用デバイスを登録する管理者が所属するデリバリーグループを選択します。次に、**保存**をクリックします。

    追加したプロファイルを含む登録プロファイルページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ワークプロファイルを持つ完全に管理されたデバイス、または会社所有デバイス上のワークプロファイル用の登録プロファイルを追加する

1. Citrix Endpoint Managementコンソールで、**構成 > 登録プロファイル**に移動します。
2. 登録プロファイルを追加するには、**追加**をクリックします。登録情報ページで、登録プロファイルの名前を入力します。
3. このプロファイルを持つメンバーが登録できるデバイスの数を設定します。
4. **プラットフォーム**の下にある**Android**を選択するか、**次へ**をクリックします。登録構成ページが表示されます。
5. **管理**を**Android Enterprise**に設定します。**デバイス所有者モード**を**ワークプロファイルを持つ完全に管理されたデバイス / 会社所有デバイス上のワークプロファイル**に設定します。

   登録プロファイル構成画面(/en-us/citrix-endpoint-management/media/android-enterprise-enrollment-profile-fully-managed-work-profile.png)
6. **BYODワークプロファイル**を使用すると、BYODデバイスをワークプロファイルデバイスとして登録するように登録プロファイルを構成できます。新規デバイスおよび工場出荷時設定にリセットされたデバイスは、ワークプロファイルを持つ完全に管理されたデバイスとして登録されます。BYODデバイスをワークプロファイルデバイスとして登録できるようにするには、**BYODワークプロファイル**を**オン**に設定します。登録を専用デバイスに制限するには、**BYODワークプロファイル**を**オフ**に設定します。デフォルトは**オフ**です。
7. Citrix MAMにデバイスを登録するかどうかを選択します。
8. 「**BYODワークプロファイル**」を「**オン**」に設定する場合は、ユーザーの同意を設定します。BYODワークプロファイルデバイスのユーザーがデバイスを登録する際にデバイス管理を拒否できるようにするには、「**ユーザーによるデバイス管理の拒否を許可**」を「**オン**」に設定します。

   「**BYODワークプロファイル**」が「**オン**」に設定されている場合、「**ユーザーによるデバイス管理の拒否を許可**」のデフォルト値は「**オン**」です。「**BYODワークプロファイル**」が「**オフ**」に設定されている場合、「**ユーザーによるデバイス管理の拒否を許可**」は無効になります。
9. 「**割り当て（オプション）**」を選択します。［デリバリーグループの割り当て］画面が表示されます。
10. ワークプロファイルを使用して完全に管理されたデバイスを登録する管理者がいるデリバリーグループを選択します。次に、**保存**をクリックします。

    追加したプロファイルを含む［登録プロファイル］ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レガシーデバイスの登録プロファイルの追加

Googleは、デバイス管理のデバイス管理者モードを非推奨にしました。Googleは、すべてのAndroidデバイスをデバイス所有者モードまたはプロファイル所有者モードで管理することを推奨しています。（Google Android Enterprise開発者ガイドの「Device admin deprecation」を参照してください）。

この変更をサポートするために、次の対応を行いました。

- Citrixは、Androidデバイスのデフォルトの登録オプションとしてAndroid Enterpriseを採用しました。
- Citrix Endpoint Management展開環境でAndroid Enterpriseが有効になっている場合、新しく登録または再登録されたすべてのAndroidデバイスはAndroid Enterpriseデバイスとして登録されます。

組織によっては、Android Enterpriseを使用してレガシーAndroidデバイスの管理を開始する準備ができていない場合があります。その場合は、デバイス管理者モードで引き続き管理できます。デバイス管理者モードですでに登録されているデバイスの場合、Citrix Endpoint Managementは引き続きデバイス管理者モードでそれらを管理します。

新しいAndroidデバイスの登録でデバイス管理者モードを使用できるように、レガシーデバイスの登録プロファイルを作成します。

レガシーデバイスの登録プロファイルを作成するには：

1. Citrix Endpoint Managementコンソールで、**［構成］>［登録プロファイル］** の順に移動します。
2. 登録プロファイルを追加するには、**［追加］** をクリックします。［登録情報］ページで、登録プロファイルの名前を入力します。
3. このプロファイルを持つメンバーが登録できるデバイスの数を設定します。
4. **Platforms**の下にある**Android**を選択するか、**Next**をクリックします。登録構成ページが表示されます。
5. **Management**を**Legacy device administration (not recommended)**に設定します。**Next**をクリックします。

   登録プロファイル構成画面(/en-us/citrix-endpoint-management/media/android-enterprise-enrollment-profile-legacy.png)
6. Citrix MAMにデバイスを登録するかどうかを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. ユーザーがデバイスを登録する際にデバイス管理を拒否できるようにするには、**Allow users to decline device management**を**On**に設定します。デフォルトは**On**です。
8. **Assignment (options)**を選択します。デリバリーグループ割り当て画面が表示されます。
9. 専用デバイスを登録する管理者が所属するデリバリーグループを選択します。次に、**Save**をクリックします。

追加したプロファイルを含む登録プロファイルページが表示されます。

デバイス管理者モードでレガシーデバイスの管理を続行するには、このプロファイルを使用してデバイスを登録または再登録します。ユーザーにCitrix Secure Hubをダウンロードさせ、登録サーバーURLを提供することで、ワークプロファイルデバイスと同様にデバイス管理者デバイスを登録します。

Android Enterpriseワークプロファイルデバイスのプロビジョニング

Android Enterpriseワークプロファイルデバイスは、プロファイル所有者モードで登録されます。これらのデバイスは新品である必要はなく、工場出荷時の状態にリセットする必要もありません。BYODデバイスはワークプロファイルデバイスとして登録されます。登録エクスペリエンスは、Citrix Endpoint ManagementでのAndroid登録と似ています。ユーザーはGoogle PlayからCitrix Secure Hubをダウンロードし、デバイスを登録します。

デフォルトでは、デバイスをAndroid Enterpriseのワークプロファイルデバイスとして登録すると、デバイスの**USB Debugging and Unknown Sources**設定が無効になります。

Android Enterpriseにデバイスをワークプロファイルデバイスとして登録する場合は、常にGoogle Playにアクセスしてください。そこから、Citrix Secure Hubがユーザーの個人プロファイルに表示されるように有効にします。

Android Enterprise完全管理デバイスのプロビジョニング

前のセクションで設定した展開に、完全に管理されたデバイスを登録できます。完全に管理されたデバイスは会社所有のデバイスであり、デバイス所有者モードで登録されます。新しいデバイスまたは工場出荷時設定にリセットされたデバイスのみが、デバイス所有者モードで登録できます。

次のいずれかの登録方法を使用して、デバイスをデバイス所有者モードで登録できます。

- **DPC識別子トークン:** この登録方法では、デバイスのセットアップ時にユーザーが文字 `afw#xenmobile` を入力します。`afw#xenmobile` はCitrix DPC識別子トークンです。このトークンは、デバイスがCitrix Endpoint Managementによって管理されていることを識別し、Google PlayストアからCitrix Secure Hubをダウンロードします。Citrix DPC識別子トークンを使用したデバイスの登録を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **近距離無線通信（NFC）バンプ:** NFCバンプ登録方法では、近距離無線通信を使用して2つのデバイス間でデータを転送します。新しいデバイスまたは工場出荷時設定にリセットされたデバイスでは、Bluetooth、Wi-Fi、およびその他の通信モードが無効になっています。NFCは、この状態でデバイスが使用できる唯一の通信プロトコルです。NFCバンプを使用したデバイスの登録を参照してください。
- **QRコード:** QRコード登録は、タブレットなど、NFCをサポートしない分散型デバイス群を登録するために使用できます。QRコード登録方法では、セットアップウィザードからQRコードをスキャンすることで、デバイスプロファイルモードを設定および構成します。QRコードを使用したデバイスの登録を参照してください。
- **ゼロタッチ:** ゼロタッチ登録を使用すると、デバイスの電源が初めてオンになったときに自動的に登録されるように構成できます。ゼロタッチ登録は、Android 9.0以降を実行している一部のAndroidデバイスでサポートされています。ゼロタッチ登録を参照してください。
- **Googleアカウント:** ユーザーはGoogleアカウントの資格情報を入力して、プロビジョニングプロセスを開始します。このオプションは、Google Workspaceを使用している企業向けです。

Citrix DPC識別子トークンを使用したデバイスの登録

ユーザーは、新しいデバイスまたは工場出荷時設定にリセットされたデバイスの初期セットアップのために電源をオンにした後、Googleアカウントの入力を求められたときに `afw#xenmobile` を入力します。この操作により、Citrix Secure Hubがダウンロードおよびインストールされます。その後、ユーザーはCitrix Secure Hubのセットアッププロンプトに従って登録を完了します。

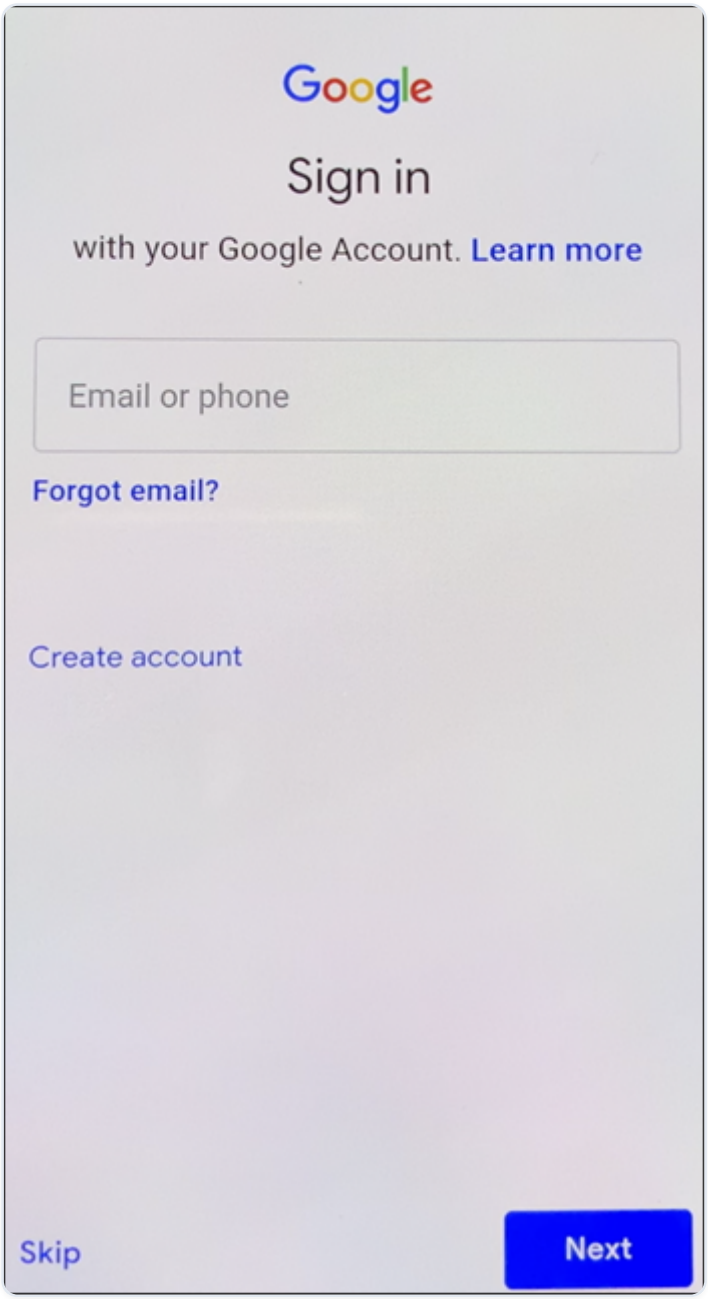
システム要件

- Android OSを実行しているすべてのAndroidデバイスでサポートされています。

デバイスを登録するには

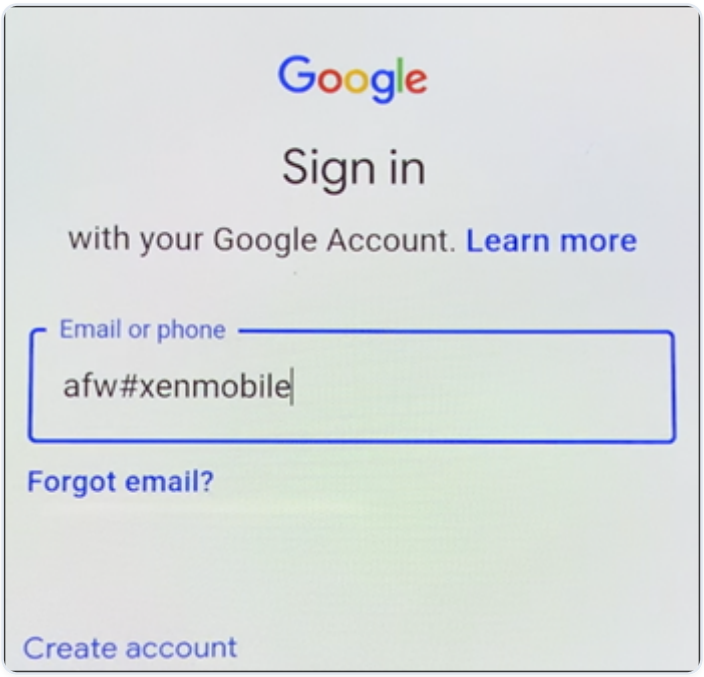
1. 新しいデバイスまたは工場出荷時設定にリセットされたデバイスの電源をオンにします。
2. 初期デバイスセットアップがロードされ、Googleアカウントの入力を求められます。デバイスのホーム画面がロードされた場合は、通知バーに「**セットアップを完了**」通知がないか確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



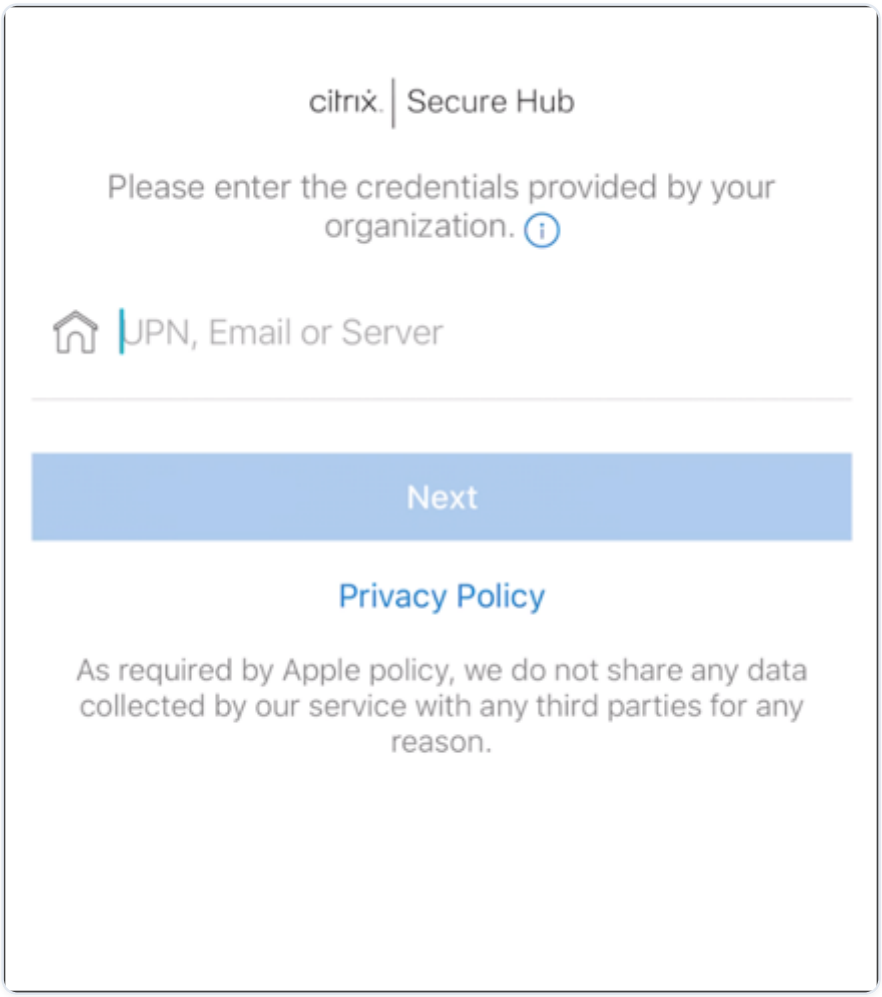
3. 「**メールアドレスまたは電話番号**」フィールドに`afw#xenmobile`を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

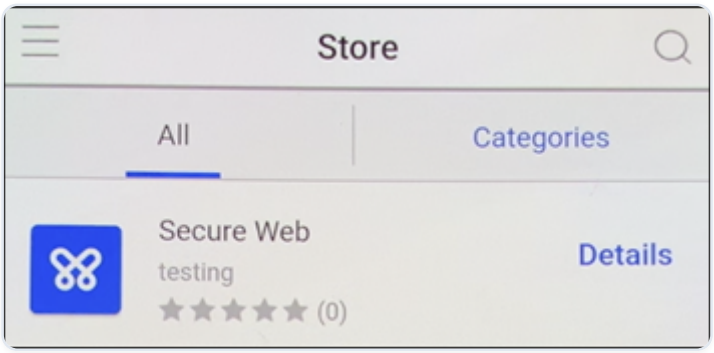


4. Citrix Secure Hubのインストールを促すAndroid Enterprise画面で、 をタップします。
5. Citrix Secure Hubインストーラー画面で、 をタップします。
6. すべてのアプリのアクセス許可要求に対して、 をタップします。
7. Citrix Secure Hubをインストールし、デバイスを管理できるようにするには、 をタップします。
8. Citrix Secure Hubがインストールされ、デフォルトの登録画面が表示されます。この例では、AutoDiscoveryはセットアップされていません。セットアップされている場合は、ユーザーはユーザー名/メールアドレスを入力でき、サーバーが自動的に検出されます。代わりに、環境の登録URLを入力し、 をタップします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. Citrix Endpoint Managementのデフォルト構成では、ユーザーはMAMまたはMDM+MAMのどちらを使用するかを選択できます。このように求められた場合は、 をタップしてMDM+MAMを選択します。
10. ユーザーのメールアドレスとパスワードを入力し、 をタップします。
11. デバイスのパスコードを設定するよう求められます。 をタップしてパスコードを入力します。
12. ユーザーはワークプロファイルのロック解除方法を設定するよう求められます。この例では、 をタップし、 をタップしてPINを入力します。
13. デバイスはCitrix Secure Hubの**** ランディング画面に表示されます。 をタップします。
14. Citrix Secure Webを追加するには、 をタップします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

15. 「**追加**」をタップします。

    Citrix Secure Webストア(/en-us/citrix-endpoint-management/media/secure-web-store.png)

16. Citrix Secure Hubは、Citrix Secure Webをインストールするためにユーザーを Google Playストアに誘導します。「**インストール**」をタップします。

    セキュアアプリのインストール(/en-us/citrix-endpoint-management/media/secure-app-install.png)

17. Citrix Secure Webのインストール後、「**開く**」をタップします。アドレスバーに社内サイトのURLを入力し、ページが読み込まれることを確認します。

    Citrix Secure Webテスト(/en-us/citrix-endpoint-management/media/secure-web-test.png)

18. デバイスで**設定 > アカウント**に移動します。「**管理対象アカウント**」が変更できないことを確認します。画面共有またはリモートデバッグ用の開発者オプションもブロックされます。

    アカウントの変更(/en-us/citrix-endpoint-management/media/account-modification-not-allowed.png)

NFCバンプによるデバイスの登録

NFCバンプを使用してデバイスを完全管理対象デバイスとして登録するには、2つのデバイスが必要です。1つは工場出荷時の設定にリセットされたデバイス、もう1つはCitrix Endpoint Managementプロビジョニングツールを実行しているデバイスです。

システム要件と前提条件

- サポートされているAndroidデバイス。
- NFC機能を備えた新規または工場出荷時設定にリセットされたデバイスで、Android Enterpriseの完全管理対象デバイスとしてプロビジョニングされていること。「Android Enterpriseの完全管理対象デバイスのプロビジョニング」のセクションを参照してください。
- NFC機能を備え、構成済みのプロビジョニングツールを実行している別のデバイス。プロビジョニングツールは、Citrix Secure HubまたはCitrixダウンロードページで入手できます。

各デバイスにはAndroid Enterpriseプロファイルを1つしか設定できません。この場合、プロファイルは管理対象のCitrix Secure Hub用です。2つ目のDPCアプリを追加しようとすると、インストール済みのCitrix Secure Hubが削除されます。

NFCバンプを介して転送されるデータ

初期化されたデバイスをプロビジョニングするには、Android Enterpriseを開始するために、NFCバンプを介して以下のデータを送信する必要があります。

- デバイス所有者として機能するDPCアプリのパッケージ名（この場合はCitrix Secure Hub）。

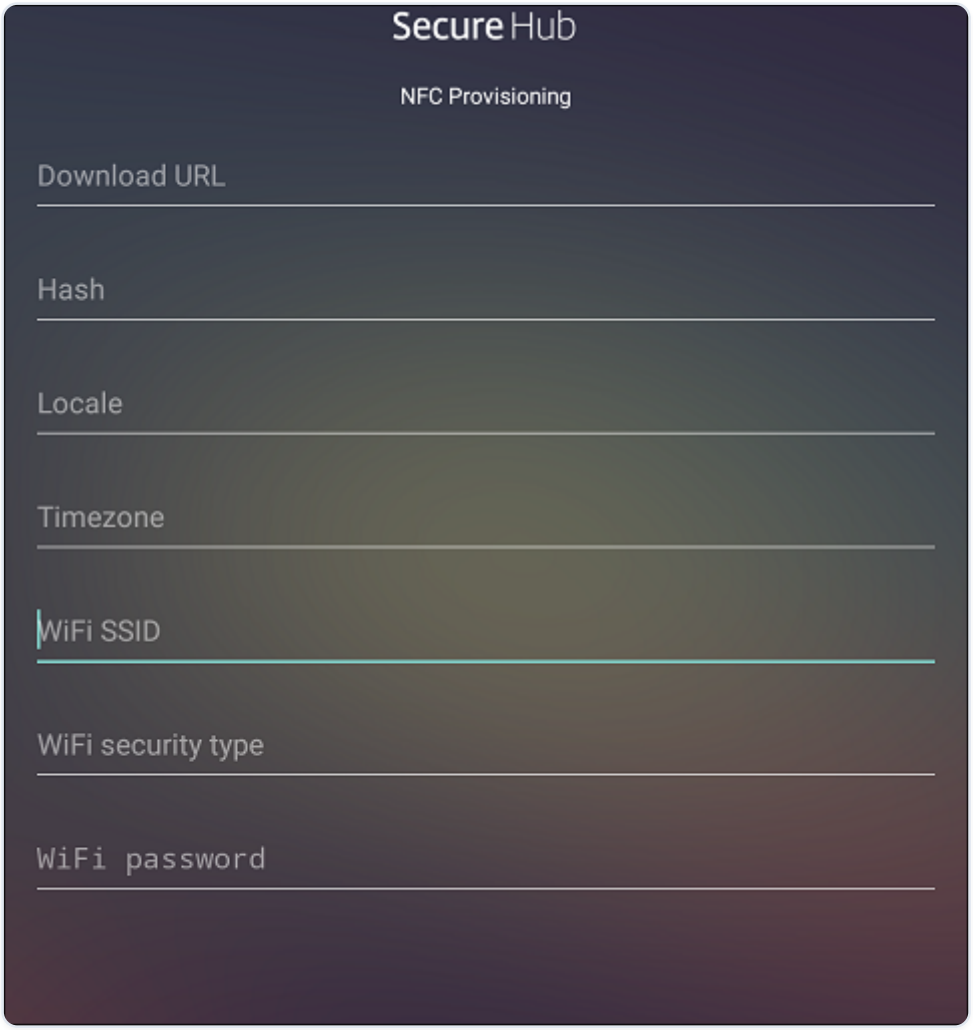
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- デバイスがDPCアプリをダウンロードできるイントラネット/インターネットの場所。
- ダウンロードが成功したかどうかを確認するためのDPCアプリのSHA-256ハッシュ。
- 初期化されたデバイスがDPCアプリに接続してダウンロードできるようにするためのWi-Fi接続の詳細。注：Androidは現在、このステップで802.1x Wi-Fiをサポートしていません。
- デバイスのタイムゾーン（オプション）。
- デバイスの地理的位置（オプション）。

2つのデバイスがバンプされると、プロビジョニングツールからのデータが初期化されたデバイスに送信されます。そのデータは、管理者設定でCitrix Secure Hubをダウンロードするために使用されます。タイムゾーンと場所の値を入力しない場合、Androidは新しいデバイスで値を自動的に構成します。

CITRIX ENDPOINT MANAGEMENTプロビジョニングツールの構成

NFCバンプを行う前に、プロビジョニングツールを構成する必要があります。この構成は、NFCバンプ中に初期化されたデバイスに転送されます。



必要なフィールドにデータを入力するか、テキストファイルを使用してデータを入力できます。次の手順では、各フィールドの説明を含むテキストファイルを構成する方法について説明します。ア

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プリは入力後に情報を保存しないため、将来の使用のために情報を保持するためにテキストファイルを作成することをお勧めします。
テキストファイルを使用してプロビジョニングツールを構成するには
ファイル名をnfcprovisioning.txtとし、デバイスのSDカードの`/sdcard/`フォルダーに配置します。アプリはテキストファイルを読み取り、値を入力できます。

テキストファイルには、次のデータが必要です。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

この行は、EMMプロバイダーアプリのイントラネット/インターネット上の場所です。工場出荷時設定にリセットされたデバイスがNFCバンプ後にWi-Fiに接続すると、ダウンロードのためにこの場所にアクセスできる必要があります。URLは通常のURLであり、特別な書式設定は必要ありません。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>`

この行は、EMMプロバイダーアプリのチェックサムです。このチェックサムは、ダウンロードが成功したことを確認するために使用されます。チェックサムを取得する手順については、この記事の後半で説明します。

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

この行は、プロビジョニングツールが実行されているデバイスの接続済みWi-Fi SSIDです。

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

サポートされている値はWEPとWPA2です。Wi-Fiが保護されていない場合、このフィールドは空にする必要があります。

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

Wi-Fiが保護されていない場合、このフィールドは空にする必要があります。

`android.app.extra.PROVISIONING_LOCALE=<locale>`

言語コードと国コードを入力します。言語コードは、ISO 639-1で定義されている2文字の小文字のISO言語コード（enなど）です。国コードは、ISO 3166-1で定義されている2文字の大文字のISO国コード（USなど）です。たとえば、米国で話されている英語の場合はen_USと入力します。コードを入力しない場合、国と言語は自動的に入力されます。

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスが実行されているタイムゾーン。地域/場所のデータベース名を入力します。たとえば、太平洋時間の場合は**America/Los_Angeles**と入力します。名前を入力しない場合、タイムゾーンは自動的に入力されます。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

このデータは不要です。値がCitrix Secure Hubとしてアプリにハードコードされているためです。ここでは、完全を期すためだけに記載しています。

WPA2で保護されたWi-Fiがある場合、完成したnfcprovisioning.txtファイルは次のようになります。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

保護されていないWi-Fiがある場合、完成したnfcprovisioning.txtファイルは次のようになります。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

CITRIX SECURE HUB のチェックサムを取得するには

Citrix Secure Hub のチェックサムは定数値です: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`。Citrix Secure Hub の APK ファイルをダウ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ンロードするには、次の Google Play ストアリンクを使用してください: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`。

アプリのチェックサムを取得するには

前提条件:

- アンドロイド SDK ビルド ツールからの **apksigner** ツール
- OpenSSL コマンドライン

任意のアプリのチェックサムを取得するには、次の手順に従います。

1. アプリの APK ファイルを Google Play ストアからダウンロードします。
2. OpenSSL コマンドラインで、**apksigner** ツールに移動し: `android-sdk/build-tools/<version>/apksigner`、次のように入力します。

   ```
   apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{(?<=SHA-256 digest:) .*}'  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
   ```

   コマンドは有効なチェックサムを返します。
3. QR コードを生成するには、`PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM` フィールドにチェックサムを入力します。例:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",


"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUth
eu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?
identifier=xenmobile",

  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"

   }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

使用されているライブラリ

プロビジョニングツールは、そのソースコードで以下のライブラリを使用しています。

- Google による Apache License 2.0 の v7 `appcompat` ライブラリ、Design Support ライブラリ、および v7 パレットサポートライブラリ

  詳細については、Support Library Features Guideを参照してください。

- Butter Knife Jake Wharton による Apache License 2.0 のライセンスに基づく

QRコードを使用したデバイスの登録

ユーザーは、生成されたQRコードを使用して、完全に管理されたデバイスを登録できます。

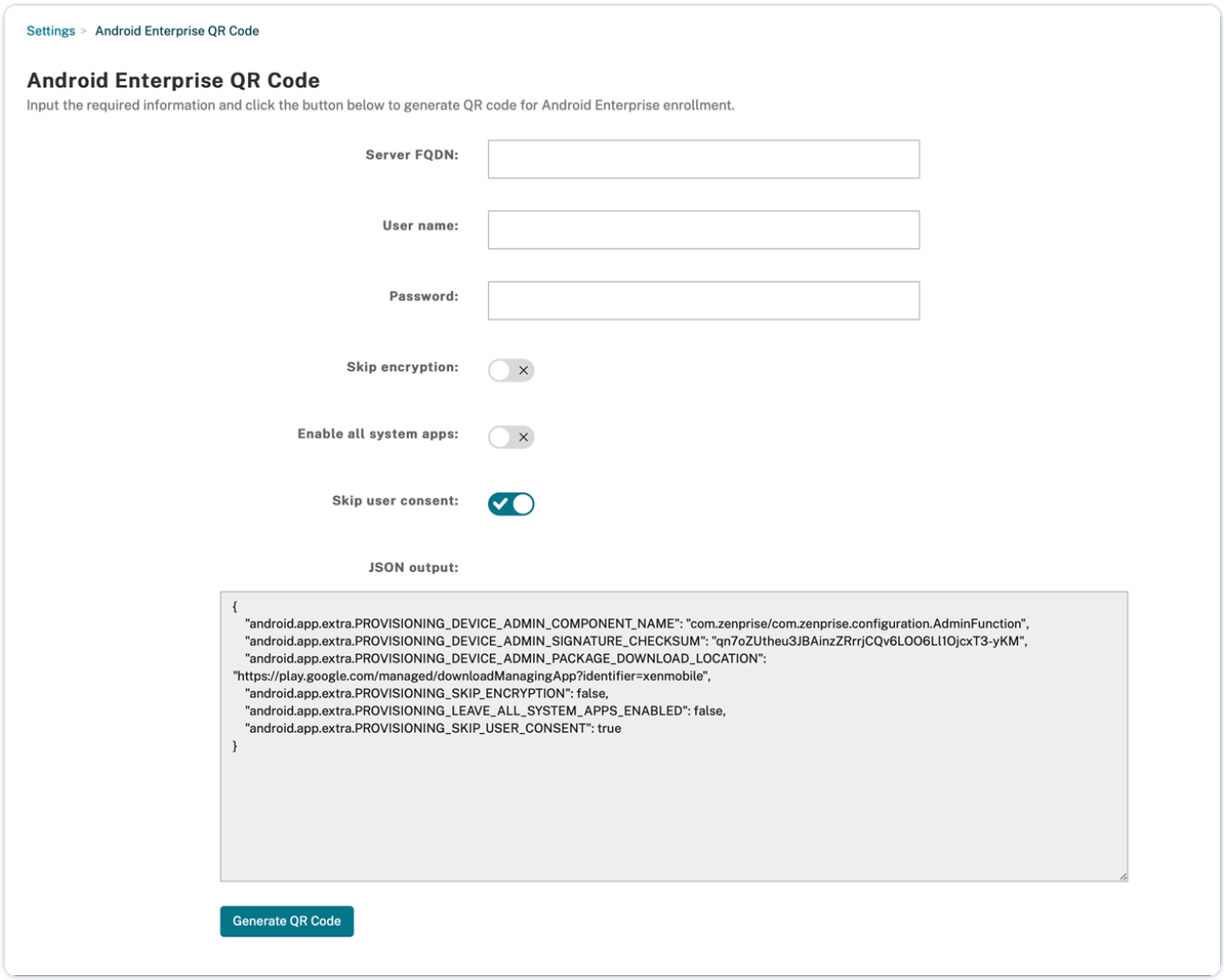
システム要件

Android 7.0以降を実行するAndroidデバイス。

QRコードの作成

必要に応じて登録情報を指定してQRコードを生成します。QRコードを生成したら、ローカルに保存します。Citrix Endpoint ManagementはQRコードを保存しません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. **設定 > Android Enterprise QRコード**に移動します。
2. 必要に応じて、次の登録情報を指定します。

   - **サーバーFQDN:** Citrix Endpoint ManagementサーバーのFQDNを入力します (例: `example.cem.cloud.com`)。このフィールドはオプションです。空のままにした場合、ユーザーは登録時にこの情報を入力する必要があります。
   - **ユーザー名:** 登録に使用するユーザー名を入力します。QRコードを複数のユーザーに配布する予定がある場合は、このフィールドを空のままにすることをお勧めします。ユーザー名とパスワードでQRコードを構成すると、キオスクデバイスの登録に役立ちます。このフィールドを空のままにした場合、ユーザーは登録時にこの情報を入力する必要があります。
   - **パスワード:** 入力したユーザー名に関連付けられているパスワードを入力します。このフィールドを空のままにした場合、ユーザーは登録時にこの情報を入力する必要があります。
   - **暗号化をスキップ: オン**の場合、デバイスは登録中に暗号化されません。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **すべてのシステムアプリを有効にする: オン**の場合、デバイス上のすべてのシステムアプリへのアクセスを許可します。デフォルトは**オフ**です。
- **ユーザーの同意をスキップ: オフ**の場合、ユーザーはデバイス管理をオプトアウトできます。デフォルトは**オフ**です。

JSON出力ボックスには、指定した情報に対応するJSONコンテンツが表示されます。

3. さらに登録情報を追加するには、**JSON出力**ボックスでJSONコンテンツを編集します。
4. **QRコードを生成**をクリックします。QRコードはJSON出力の右側に表示されます。
5. QRコード画像を右クリックし、保存します。
6. デバイス登録のために、画像をユーザーに送信します。

工場出荷時設定にリセットされたデバイスは、このQRコードをスキャンして、完全に管理されたデバイスとして登録します。

デバイスを登録するには

新規または工場出荷時設定にリセットされたデバイスの電源をオンにした後:

1. ウェルカム画面で画面を6回タップして、QRコード登録フローを起動します。
2. プロンプトが表示されたら、Wi-Fiに接続します。QRコード内のCitrix Secure Hubのダウンロード場所は、このWi-Fiネットワーク経由でアクセス可能です。

   デバイスがWi-Fiに正常に接続すると、GoogleからQRコードリーダーをダウンロードし、カメラを起動します。
3. カメラをQRコードに向け、コードをスキャンします。

   Androidは、QRコード内のダウンロード場所からCitrix Secure Hubをダウンロードし、署名証明書の署名を検証し、Citrix Secure Hubをインストールして、デバイス所有者として設定します。

詳細については、Android EMM 開発者向けのこの Google ガイドを参照してください: `<https://developers.google.com/android/work/prov-devices#qr_code_method>`。

ゼロタッチ登録

ゼロタッチ登録を使用すると、デバイスの電源を初めてオンにしたときに、デバイス自体を完全に管理されたデバイスとしてプロビジョニングするように設定できます。

デバイスの再販業者は、デバイスに構成を適用できるオンラインツールである Android ゼロタッチポータルでアカウントを作成します。Android ゼロタッチポータルを使用して、1つ以上のゼロタッチ登録構成を作成し、それらの構成をアカウントに割り当てられたデバイスに適用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーがこれらのデバイスの電源をオンにすると、デバイスはCitrix Endpoint Managementに自動的に登録されます。デバイスに割り当てられた構成によって、自動登録プロセスが定義されます。

システム要件

- ゼロタッチ登録のサポートは Android 9.0 から開始されます。

再販業者からのデバイスとアカウント情報

- ゼロタッチ登録の対象となるデバイスは、エンタープライズ再販業者またはGoogleパートナーから購入されます。Android Enterpriseゼロタッチパートナーのリストについては、Android Webサイトを参照してください。
- 再販業者によって作成されたAndroid Enterpriseゼロタッチポータルアカウント。
- 再販業者から提供されたAndroid Enterpriseゼロタッチポータルアカウントのログイン情報。

ゼロタッチ構成の作成

ゼロタッチ構成を作成するときは、構成の詳細を指定するためにカスタムJSONを含めます。

このJSONを使用して、指定したCitrix Endpoint Managementサーバーにデバイスを登録するように構成します。この例の「URL」には、サーバーのURLを置き換えてください。

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

  {

        "serverURL":"URL"

   }

}
```

追加のパラメーターを含むオプションのJSONを使用して、構成をさらにカスタマイズできます。この例では、Citrix Endpoint Managementサーバーと、この構成を使用するデバイスがサーバーにログオンするために使用するユーザー名およびパスワードを指定します。

```
{

   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
```

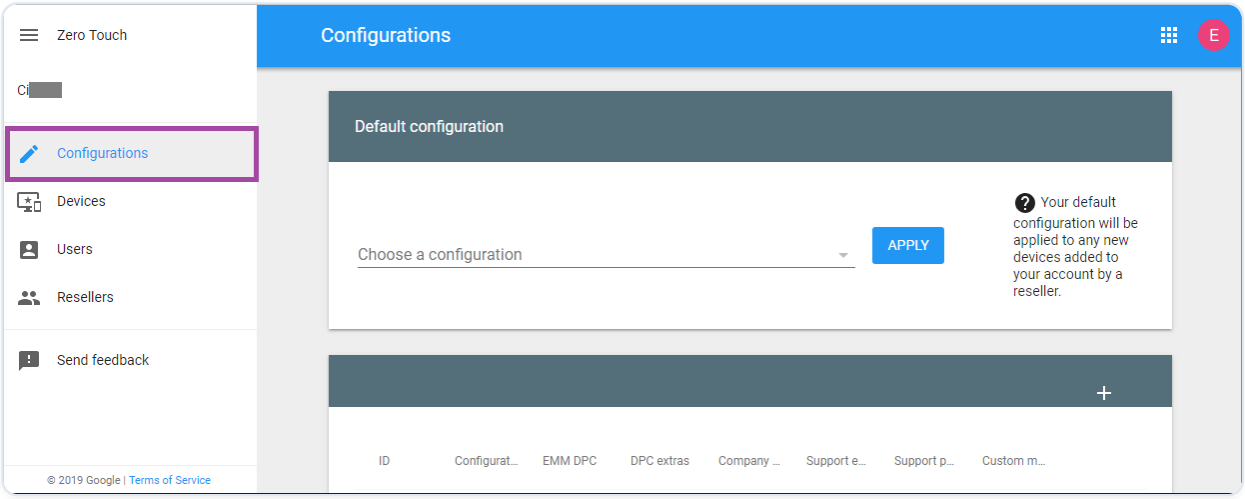
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    {
        "serverURL":"URL",
        "xm_username":"username",
        "xm_password":"password"
    }
      }
```

重要:

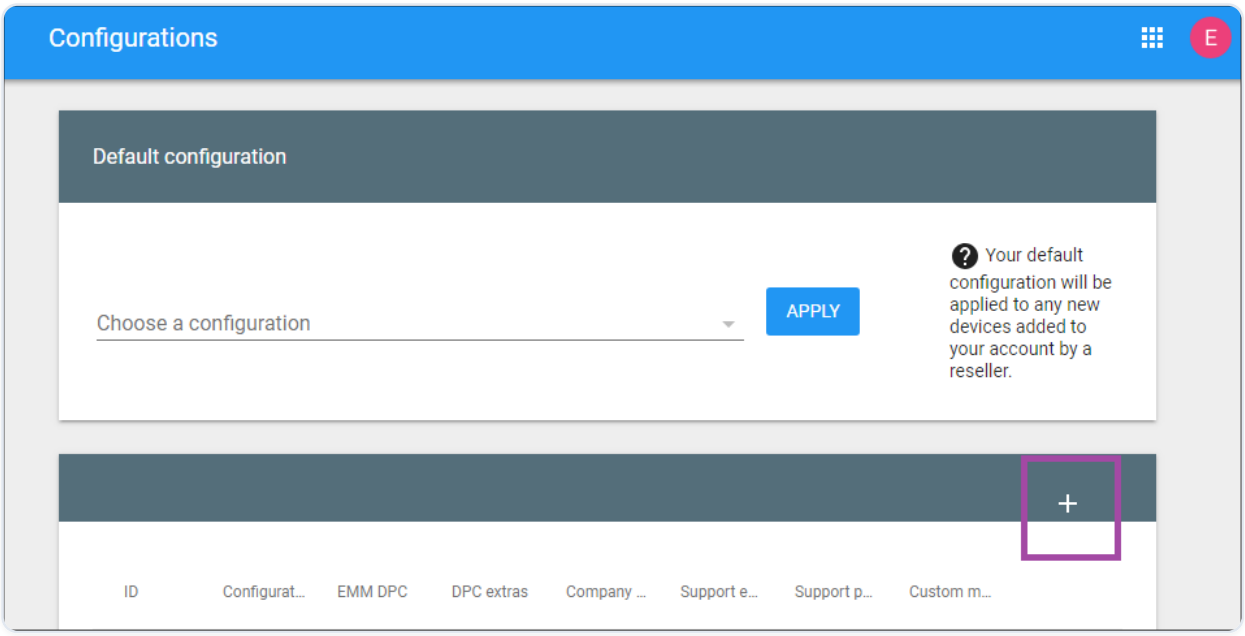
企業所有デバイスモードでデバイスをワークプロファイルに登録するには、`PROVISIONING_ADMIN_EXTRAS_BUNDLE`の下のカスタムJSONに`{"desiredProvisioningMode": "managedProfile"}`を追加します。

1. https://partner.android.com/zerotouchでAndroidゼロタッチポータルにアクセスします。ゼロタッチデバイスの再販業者から提供されたアカウント情報でログインします。
2. **構成**をクリックします。



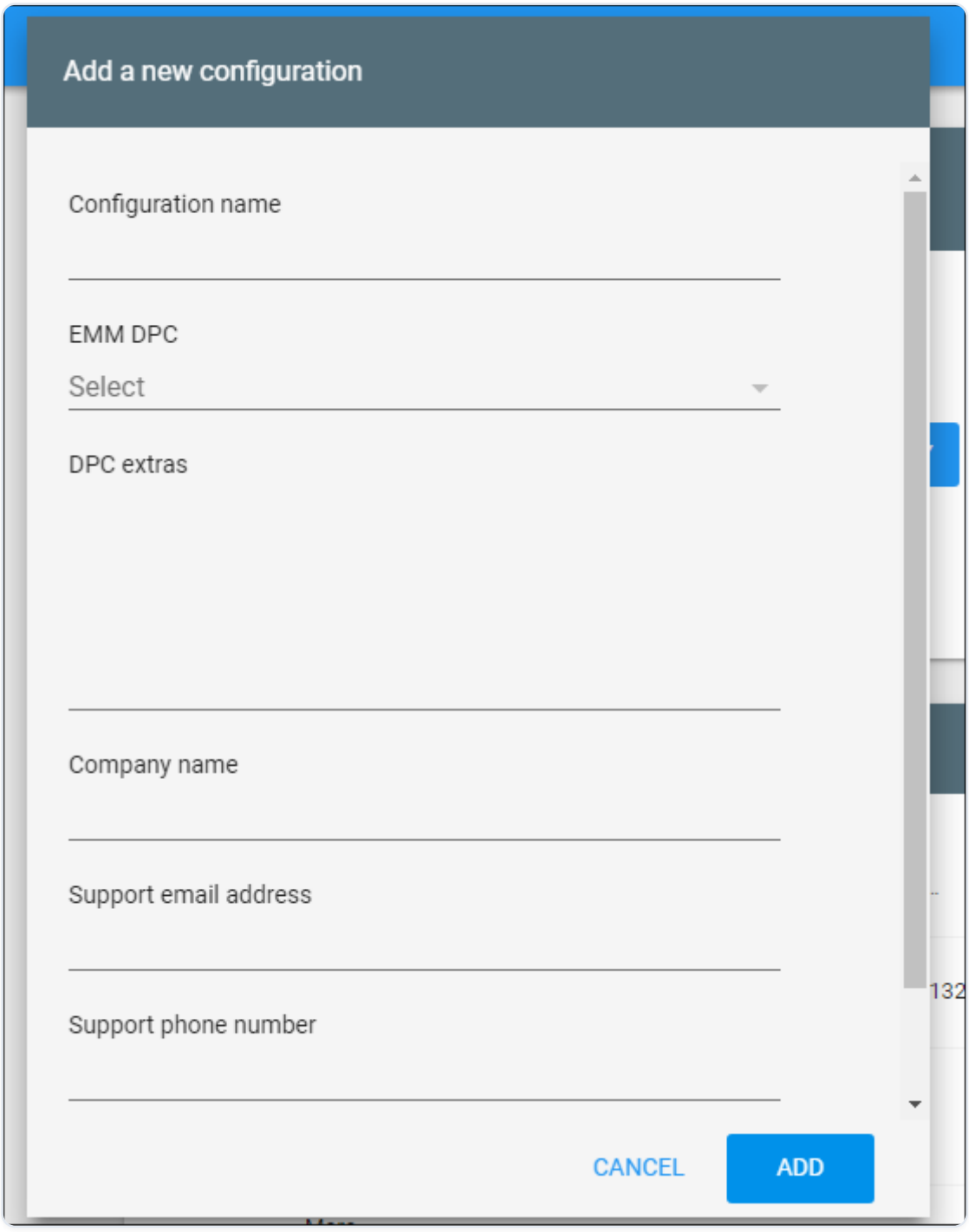
3. 構成テーブルの上にある**+**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 表示される構成ウィンドウに構成情報を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **構成名:** この構成に選択した名前を入力します。
- **EMM DPC: Citrix Secure Hub**を選択します。
- **DPC extras:** このフィールドにカスタムJSONテキストを貼り付けます。
- **会社名:** デバイスプロビジョニング中にAndroid Enterpriseゼロタッチデバイスに表示する名前を入力します。
- **サポートメールアドレス:** ユーザーがヘルプを求めるために連絡できるメールアドレスを入力します。このアドレスは、デバイスプロビジョニング前にAndroid Enterpriseゼロタッチデバイスに表示されます。

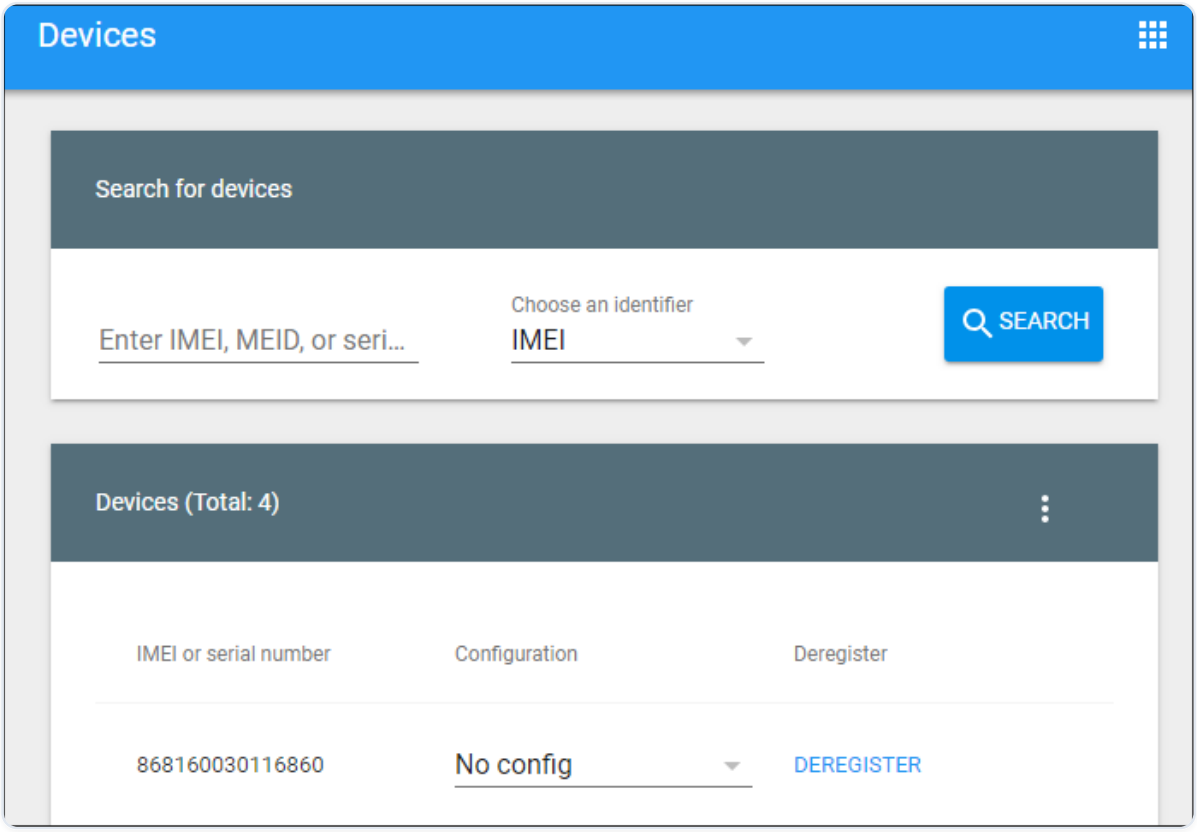
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **サポート電話番号:** ユーザーがヘルプを求めるために連絡できる電話番号を入力します。この電話番号は、デバイスプロビジョニング前にAndroid Enterpriseゼロタッチデバイスに表示されます。
- **カスタムメッセージ:** オプションで、ユーザーが連絡を取りやすくするため、またはデバイスに何が起こっているかについて詳細を伝えるために、1つまたは2つの文を追加します。このカスタムメッセージは、デバイスプロビジョニング前にAndroid Enterpriseゼロタッチデバイスに表示されます。

5. **追加**をクリックします。
6. さらに構成を作成するには、手順2から4を繰り返します。
7. 構成をデバイスに適用するには：

   a. Androidゼロタッチポータルで、「**デバイス**」をクリックします。

   b. デバイスのリストからデバイスを見つけ、それに割り当てる構成を選択します。



   c. 「**更新**」をクリックします。

CSVファイルを使用して、多数のデバイスに構成を適用できます。

多数のデバイスに構成を適用する方法については、「IT管理者向けのゼロタッチ登録」を参照してください。このAndroid Enterpriseのトピックには、構成を管理し、デバイスに適用する方法に関する詳細情報が記載されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

専用のAndroid Enterpriseデバイスのプロビジョニング

専用のAndroid Enterpriseデバイスは、単一のユースケースを満たすために特化した、完全に管理されたデバイスです。これらのデバイスは、このユースケースに必要なタスクを実行するために必要な1つのアプリまたは少数のアプリに制限されます。また、ユーザーが他のアプリを有効にしたり、デバイスで他の操作を行ったりすることを防ぎます。

専用デバイスは、Android Enterpriseの完全に管理されたデバイスのプロビジョニングで説明されているように、他の完全に管理されたデバイスで使用される登録方法のいずれかを使用して登録します。専用デバイスのプロビジョニングには、登録前により多くのセットアップが必要です。

専用デバイスをプロビジョニングするには：

- 専用デバイスを登録することを許可するCitrix Endpoint Management管理者の登録プロファイルを、Citrix Endpoint Management展開に追加します。「登録プロファイルの作成」を参照してください。
- 専用デバイスがアプリにアクセスできるようにするには、それらを許可リストに追加します。
- オプションで、許可されたアプリがロックタスクモードを許可するように設定します。アプリがロックタスクモードの場合、ユーザーがアプリを開くと、アプリはデバイス画面に固定されます。ホームボタンは表示されず、戻るボタンは無効になります。ユーザーは、サインアウトなどのアプリにプログラムされたアクションを使用してアプリを終了します。
- 追加した登録プロファイルに各デバイスを登録します。

システム要件

- 専用デバイスの登録のサポートはAndroid 6.0から開始されます。

アプリを許可し、タスク固定モードを設定する

キオスクデバイスポリシーを使用すると、アプリを許可し、タスク固定モードを設定できます。デフォルトでは、Citrix Secure HubとGoogle Playサービスは許可リストに含まれています。

キオスクポリシーを追加するには：

1. Citrix Endpoint Managementコンソールで、**構成 > デバイスポリシー**をクリックします。**デバイスポリシー**ページが表示されます。
2. **追加**をクリックします。**新しいポリシーの追加**ダイアログボックスが表示されます。
3. **その他**を展開し、セキュリティの下にある**キオスク**をクリックします。**キオスクポリシー**ページが表示されます。
4. プラットフォームで、**Android Enterprise**を選択します。他のプラットフォームの選択を解除します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. ポリシー情報ペインで、**ポリシー名**とオプションの**説明**を入力します。
6. **次へ**をクリックし、**追加**をクリックします。
7. アプリを許可し、そのアプリのタスク固定モードを許可または拒否するには：

   リストから許可するアプリを選択します。

   ユーザーがアプリを起動したときに、アプリをデバイス画面に固定するように設定するには、**許可**を選択します。アプリを固定しないように設定するには、**拒否**を選択します。デフォルトは**許可**です。

   デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/configure-device-policies-kiosk-android-enterprise.png)
8. **保存**をクリックします。
9. 別のアプリを許可し、そのアプリのタスク固定モードを許可または拒否するには、**追加**をクリックします。
10. 展開ルールを設定し、デリバリーグループを選択します。詳細については、「デバイスポリシー」を参照してください。

ワークプロファイルまたは会社所有デバイス上のワークプロファイルを持つAndroid Enterpriseの完全管理対象デバイスのプロビジョニング

Android 9.0〜10.xを実行しているデバイスは、「ワークプロファイル付き完全管理対象」として登録されます。Android 11以降では、デバイスは「会社所有デバイス上のワークプロファイル」として登録されます。これらのデバイスはすべて、仕事と個人の両方の目的で使用される会社所有のデバイスです。組織はデバイス全体を管理します。デバイスには1つのポリシーセットを適用し、ワークプロファイルには別のポリシーセットを適用できます。

Citrix Endpoint Managementコンソールでは、ワークプロファイル付きの完全管理対象デバイスは次の用語で表示されます。

- デバイスの所有権は「会社所有」です。
- デバイスのAndroid Enterpriseインストールタイプは「Corporate Owner Personally Enabled」です。

システム要件

- ワークプロファイル付きの完全管理対象デバイスの登録のサポートは、Android 9.0から開始されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスを登録するには

新規デバイスおよび工場出荷時設定にリセットされたデバイスは、ワークプロファイル付きの完全管理対象デバイスとして登録されます。これらのデバイスは、「Android Enterpriseの完全管理対象デバイスのプロビジョニング」で説明されている、他の完全管理対象デバイスに使用される登録方法のいずれかを使用します。Android 11を実行しているデバイスは、そのセクションで説明されているQRコードまたはゼロタッチ登録方法を使用して、会社所有デバイス上のワークプロファイルモードで登録できます。

重要：

QRコード方式を使用して会社所有デバイス上のワークプロファイルモードでデバイスを登録する場合、`serverURL`フィールドの上に、JSON出力に以下を追加します。

`"desiredProvisioningMode": "managedProfile",`

JSON output

```
{
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
    "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
    "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": false,
    "android.app.extra.PROVISIONING_SKIP_USER_CONSENT": true,
    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
        "desiredProvisioningMode": "managedProfile",
        "serverURL": "https://testServer.xmqa.cloud.com",
        "username": "username",
        "password": "password"
    }
```

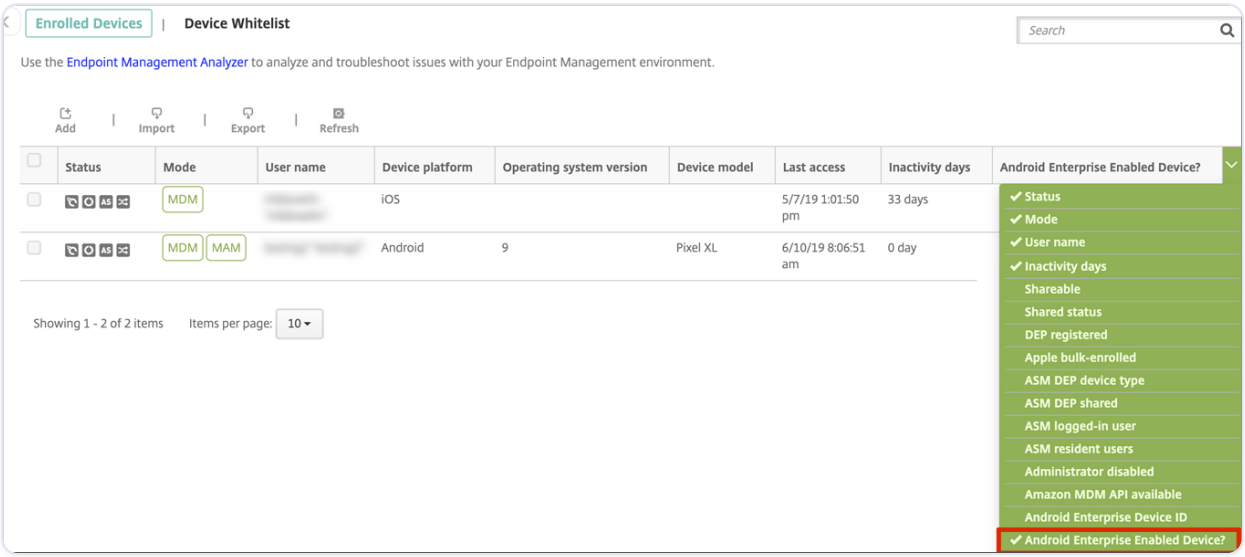
新規デバイスまたは工場出荷時設定にリセットされていないデバイスは、「Android Enterprise ワークプロファイルデバイスのプロビジョニング」で説明されているように、ワークプロファイルデバイスとして登録されます。

Citrix Endpoint ManagementコンソールでのAndroid Enterpriseデバイスの表示

Android Enterpriseの完全管理対象デバイス、専用デバイス、および仕事用プロファイルを持つ完全管理対象デバイスを表示するには：

1. Citrix Endpoint Managementコンソールで、 **>** の順に移動します。
2. テーブルの右端にあるメニューをクリックして、 列を追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 利用可能なセキュリティアクションを表示するには、完全管理対象デバイスを選択し、 をクリックします。デバイスが完全に管理されている場合、 アクションは利用可能ですが、 は利用できません。この違いは、デバイスが管理対象のGoogle Playストアからのアプリのみを許可するためです。ユーザーが公開ストアからアプリケーションをインストールするオプションはありません。組織がデバイス上のすべてのコンテンツを管理します。



Android Enterpriseのデバイスおよびアプリポリシーを構成する

デバイスレベルとアプリレベルの両方で制御されるポリシーの概要については、「Android Enterpriseでサポートされているデバイスポリシーと MDXポリシー」を参照してください。

ポリシーについて知っておくべきこと：

- **デバイス制限：** 数十のデバイス制限により、次のような機能を制御できます。
  - デバイスカメラの使用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 仕事用プロファイルと個人用プロファイル間のコピー＆ペーストの使用

- **アプリごとのVPN：** マネージド構成デバイスポリシーを使用して、Android EnterpriseのVPNプロファイルを構成します。
- **メールポリシー：** アプリを構成するには、マネージド構成デバイスポリシーを使用することをお勧めします。

デバイスポリシー

この表は、Android Enterpriseデバイスで利用可能なすべてのデバイスポリシーを一覧表示します。

重要:

Android Enterpriseに登録し、MDXアプリを使用するデバイスの場合：一部の設定はMDXとAndroid Enterpriseを通じて制御できます。MDXには最も制限の少ないポリシー設定を使用し、ポリシーはAndroid Enterpriseを通じて制御してください。

アプリの権限	アプリのインベントリ	アプリのアンインストール
管理対象アプリの自動更新	接続のスケジュール設定	資格情報
カスタムXML	Citrix Endpoint Management オプション	ファイル
キーガード管理	キオスク	ランチャー構成
位置情報	管理対象構成	ネットワーク
OSアップデート	パスコード	制限

ワークプロファイルを持つ完全管理対象デバイス (COPEデバイス) のデバイスポリシー

ワークプロファイルを持つ完全管理対象デバイスの場合、一部のデバイスポリシーを使用して、デバイス全体とワークプロファイルに個別の設定を適用できます。その他のデバイスポリシーを使用して、デバイス全体にのみ、またはワークプロファイルを持つ完全管理対象デバイスのワークプロファイルにのみ設定を適用できます。企業所有デバイスモードのワークプロファイルに登録されているデバイスの場合、ポリシーはワークプロファイルにのみ適用され、デバイス全体には適用されません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	適用対象
アプリの権限	ワークプロファイル
アプリのインベントリ	ワークプロファイル
アプリのアンインストール	ワークプロファイル
管理対象アプリを自動的に更新	仕事用プロファイル
接続スケジュール	仕事用プロファイル
資格情報	仕事用プロファイル
カスタムXML	該当なし
Citrix Endpoint Managementオプション	仕事用プロファイル
ファイル	仕事用プロファイル
キーガード管理	デバイスと仕事用プロファイル
キオスク	該当なし
ランチャー構成	デバイスとワークプロファイル
位置情報	デバイス (位置情報モードのみ)
管理対象構成	ワークプロファイル
ネットワーク	デバイス
OSアップデート	該当なし
パスコード	デバイスとワークプロファイル
制限	デバイスとワークプロファイル (デバイスとワークプロファイルで個別のポリシーを作成)
「VPN」(/ja-jp/citrix-endpoint-management/policies/vpn-policy.html#android-enterprise-settings)	該当なし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

関連項目: 「Android EnterpriseでサポートされているデバイスポリシーとMDXポリシー」(/ja-jp/mdx-toolkit/policies-platform/android-enterprise-supported-device-and-mdx-policies.html)および「MAM SDKの概要」(/ja-jp/mdx-toolkit/mam-sdk-overview.html)。

セキュリティアクション

Android Enterpriseは、以下のセキュリティアクションをサポートしています。各セキュリティアクションの説明については、「セキュリティアクション」(/ja-jp/citrix-endpoint-management/device-management.html#security-actions)を参照してください。

セキュリティアクション	ワークプロファイル	完全管理
証明書の更新	はい	はい
完全ワイプ	はい（選択的ワイプ後）	はい
検索	はい	はい
ロック	はい	はい
ロックしてパスワードをリセット	いいえ	はい
通知 (着信音)	はい	はい
取り消し	はい	はい
選択的ワイプ	はい	はい

セキュリティアクションに関する注意事項

- 位置特定セキュリティアクションは、位置情報デバイスポリシーがデバイスの位置情報モードを**高精度**または**バッテリー節約**に設定しない限り失敗します。位置情報デバイスポリシーを参照してください。
- Android 9.0より前のバージョンのAndroidを実行している仕事用プロファイルデバイスの場合:
  - ロックおよびパスワードリセットアクションはサポートされていません。
- Android 9.0以降を搭載した仕事用プロファイルデバイスの場合:
  - 送信されたパスコードは仕事用プロファイルをロックします。デバイス自体はロックされません。
  - 仕事用プロファイルにパスコードが設定されていない場合:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - パスコードが送信されない場合、または送信されたパスコードがパスコード要件を満たさない場合: デバイスはロックされます。
  - 仕事用プロファイルにパスコードが設定されている場合:
    - パスコードが送信されない場合、または送信されたパスコードがパスコード要件を満たさない場合: 仕事用プロファイルはロックされますが、デバイス自体はロックされません。

Android Enterpriseエンタープライズの登録解除

Android Enterpriseエンタープライズを使用しなくなった場合は、そのエンタープライズの登録を解除できます。

警告:

エンタープライズの登録を解除すると、そのエンタープライズを通じてすでに登録されているデバイス上のAndroid Enterpriseアプリは、デフォルトの状態にリセットされます。Googleはデバイスを管理しなくなります。新しいAndroid Enterpriseエンタープライズに登録する場合、管理対象Google Playから新しい組織のアプリを承認する必要があります。その後、Citrix Endpoint Managementコンソールからアプリを更新できます。

Android Enterpriseエンタープライズの登録が解除されると、次のようになります。

- エンタープライズを通じて登録されたデバイスとユーザーのAndroid Enterpriseアプリは、デフォルトの状態にリセットされます。以前適用された管理対象構成ポリシーは、操作に影響を与えなくなります。
- Citrix Endpoint Managementは、エンタープライズを通じて登録されたデバイスを管理します。Googleの観点からは、これらのデバイスは管理対象外です。新しいAndroid Enterpriseアプリを追加することはできません。管理対象構成ポリシーを適用することはできません。スケジュール、パスワード、制限などの他のポリシーをこれらのデバイスに適用できます。
- Android Enterpriseにデバイスを登録しようとすると、それらはAndroid Enterpriseデバイスではなく、Androidデバイスとして登録されます。

Citrix Endpoint ManagementサーバーコンソールとCitrix Endpoint Management Toolsを使用して、Android Enterpriseエンタープライズの登録を解除します。

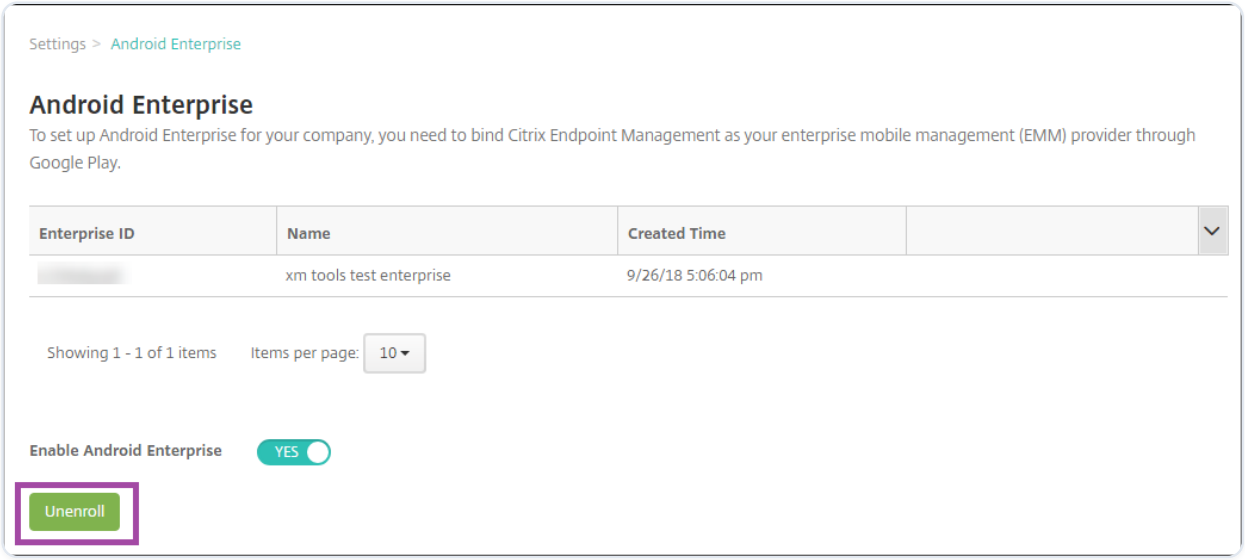
このタスクを実行すると、Citrix Endpoint ManagementはToolsポップアップウィンドウを開きます。開始する前に、ブラウザがポップアップウィンドウを開く権限を持っていることを確認してく

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ださい。Google Chromeなどの一部のブラウザでは、ポップアップブロックを無効にし、Citrix Endpoint Managementサイトのアドレスをポップアップ許可リストに追加する必要があります。

Android Enterpriseエンタープライズの登録を解除するには：

1. Citrix Endpoint Managementコンソールで、右上隅の歯車アイコンをクリックします。ページが表示されます。
2. ページで、 をクリックします。
3. をクリックします。



Android Enterpriseアプリの配布

Citrix Endpoint Managementは、デバイスに展開されたアプリを管理します。以下の種類のAndroid Enterpriseアプリを整理して展開できます。

- **管理対象アプリストアアプリ:** これらのアプリには、管理対象Google Playストアで利用可能な無料アプリが含まれます。例: GoToMeeting。
- **MDX:** MAM SDKで準備された、またはMDX Toolkitでラップされたアプリ。これらのアプリにはMDXポリシーが含まれます。MDXアプリは、内部ソースおよびパブリックストアから入手します。Citrixモバイル生産性アプリをMDXアプリとして展開します。
- **エンタープライズ:** 開発した、または別のソースから入手したプライベートアプリ。これらのアプリは、管理対象Google Playストアを通じてユーザーに提供します。管理対象Google Playストアは、Googleのエンタープライズアプリストアです。
- **MDX対応プライベートアプリ:** MAM SDKで準備された、またはMDX Toolkitでラップされたエンタープライズアプリ。

エンタープライズアプリとMDX対応プライベートアプリは、2つの異なる方法で追加できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- アプリをCitrix Endpoint Managementコンソールにエンタープライズアプリとして追加します。これについては、この記事のエンタープライズアプリおよびMDX対応プライベートアプリのセクションで説明されています。
- Google開発者アカウントを使用して、アプリを管理対象Google Playストアに直接公開します。その後、アプリをCitrix Endpoint Managementコンソールに管理対象アプリストアアプリとして追加します。管理対象アプリストアアプリを参照してください。

Google開発者アカウントを使用してアプリを公開し、その後Citrix Endpoint Managementコンソールを使用するように切り替えた場合、アプリの所有権が異なります。この場合、両方の場所でアプリを管理する必要があります。Citrixは、いずれかの方法を使用してアプリを追加することをお勧めします。

管理対象Google Playストアから自己管理アプリを削除する必要がある場合は、Googleにチケットをオープンしてください。開発者は、管理対象Google Playストアからアプリを無効にすることはできますが、削除することはできません。

以下のセクションでは、Android Enterpriseアプリの構成に関するより詳細な情報を提供します。アプリの配布については、アプリの追加を参照してください。この記事には以下が含まれます。

- Webアプリ、SaaSアプリ、またはWebリンクを追加するための一般的なワークフロー
- エンタープライズアプリおよびパブリックストアアプリに必要なアプリワークフロー
- Citrix Content Delivery Network (CDN) for Enterprise Appsからエンタープライズアプリを配信する方法

マネージドアプリストアアプリ

マネージドGoogle Playストアで利用可能な無料アプリをCitrix Endpoint Managementに追加できます。

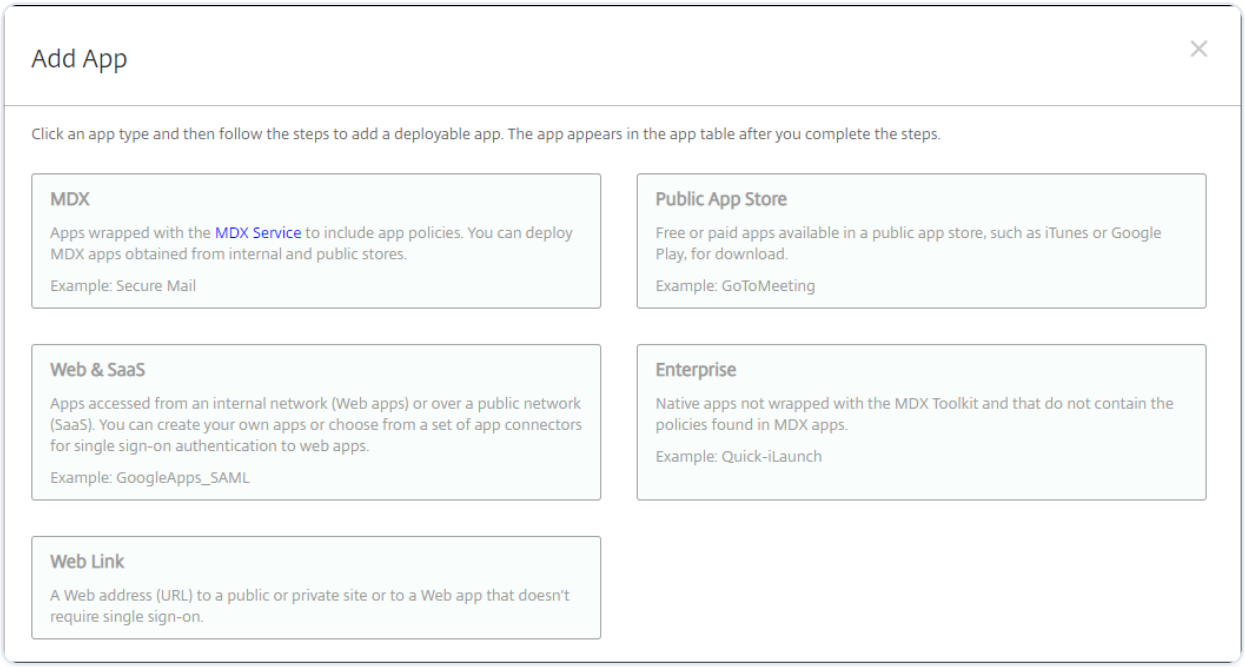
注：

マネージドGoogle PlayからGoogle Playストアのすべてのアプリにアクセスできるようにするには、**Access all apps in the managed Google Play store**サーバープロパティを使用します。「サーバープロパティ」を参照してください。このプロパティを**true**に設定すると、すべてのAndroid Enterpriseユーザーが公開Google Playストアアプリにアクセスできるようになります。その後、制限デバイスポリシーを使用して、これらのアプリへのアクセスを制御できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

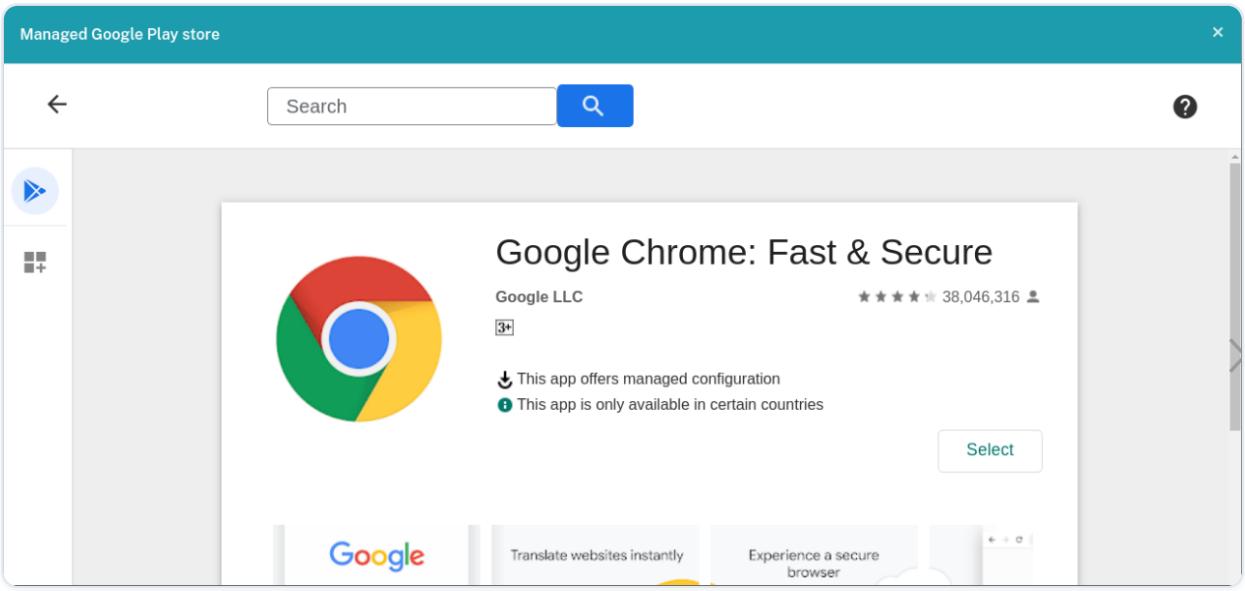
ステップ1：アプリの追加と構成

1. Citrix Endpoint Managementコンソールで、**Configure > Apps**に移動します。**Add**をクリックします。
2. **Public App Store**をクリックします。



3. **App Information**ペインで、次の情報を入力します。
   - **名前：** アプリのわかりやすい名前を入力します。この名前は、**Apps**テーブルの**App Name**の下に表示されます。
   - **説明：** アプリのオプションの説明を入力します。
4. プラットフォームとして**Android Enterprise**を選択します。
5. 検索ボックスにアプリ名またはパッケージIDを入力し、**Search**をクリックします。パッケージIDはGoogle Playストアで確認できます。IDはアプリのURLに含まれています。たとえば、`com.Slack`は`https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`のパッケージIDです。
6. 検索条件に一致するアプリが表示されます。目的のアプリをクリックし、**Select**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. 「**選択**」を再度クリックします。
8. アプリのアイコンをクリックし、アプリの**名前**と**説明**を設定します。

   Android Enterpriseアプリの構成(/en-us/citrix-endpoint-management/media/android-enterprise-public-app-configure.png)

9. アプリにデリバリーグループを割り当て、**保存**をクリックします。詳しくは、「リソースの展開」を参照してください。

手順2：アプリの展開を構成する

1. **構成 > デリバリーグループ**に移動し、構成したデリバリーグループを選択します。**編集**をクリックします。
2. **アプリ**セクションで、目的のアプリを**必須アプリ**ボックスにドラッグします。 アプリを必須としてマークする(/en-us/citrix-endpoint-management/media/required-app-delivery-group.png)
3. **概要**ページで、**保存**をクリックします。
4. **デリバリーグループ**ページで、デリバリーグループを選択し、**展開**をクリックします。

MDXアプリ

MDXファイルをCitrix Endpoint Managementに追加し、アプリの詳細とポリシー設定を構成します。Android Enterprise向けにCitrixモバイル生産性向上アプリを構成するには、それらをMDXアプリとして追加します。各デバイスプラットフォームタイプで利用可能なアプリポリシーについては、以下を参照してください:

- MAM SDKの概要
- MDXポリシーの概要

© 1997–2026 Citrix Systems, Inc. All rights reserved.

手順1：アプリの追加と構成

1. Citrixモバイル生産性向上アプリの場合、パブリックストアのMDXファイルをダウンロードします: `<https://www.citrix.com/downloads>` にアクセスします。**Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**に移動します。

   他の種類のMDXアプリの場合は、MDXファイルを取得します。

2. Citrix Endpoint Managementコンソールで、**Configure > Apps** をクリックします。**Add** をクリックします。**Add App** ダイアログボックスが表示されます。

   アプリ構成画面(/en-us/citrix-endpoint-management/media/configure-apps-add.png)

3. **MDX** をクリックします。**MDX App Information** ページが表示されます。**App Information** ペインに、次の情報を入力します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、**Apps** テーブルの **App Name** の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。

4. プラットフォームとして **Android Enterprise** を選択します。

5. **Upload** をクリックして、MDXファイルに移動します。Android Enterpriseは、MAM SDKまたはMDX Toolkitで準備されたアプリのみをサポートします。

   - 添付されたアプリケーションが管理対象のGoogle Playストアからの承認を必要とする場合、UIが通知します。Citrix Endpoint Managementコンソールを離れることなくアプリケーションを承認するには、**Yes** をクリックします。

     MDXアプリを追加(/en-us/citrix-endpoint-management/media/mdx-app-not-approved.png)

     管理対象のGoogle Playストアが開いたら、指示に従ってアプリを承認して保存します。

     MDXアプリを承認(/en-us/citrix-endpoint-management/media/mdx-approve-app.png)

     アプリが正常に追加されると、**App details** ページが表示されます。

6. 次の設定を構成します。

   - **ファイル名:** アプリに関連付けられているファイル名を入力します。
   - **アプリの説明:** アプリの説明を入力します。
   - **アプリのバージョン:** 必要に応じて、アプリのバージョン番号を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **パッケージID:** マネージドGoogle Playストアから取得したアプリのパッケージIDを入力します。
- **最小OSバージョン:** 必要に応じて、アプリを使用するためにデバイスが実行できる最も古いオペレーティングシステムバージョンを入力します。
- **最大OSバージョン:** 必要に応じて、アプリを使用するためにデバイスが実行する必要がある最新のオペレーティングシステムを入力します。
- **除外デバイス:** 必要に応じて、アプリを実行できないデバイスの製造元またはモデルを入力します。

7. **MDXポリシー**を構成します。MDXポリシーはプラットフォームによって異なり、認証、デバイスセキュリティ、アプリの制限などのポリシー領域のオプションが含まれます。コンソールでは、各ポリシーにポリシーを説明するツールヒントがあります。各デバイスプラットフォームタイプで利用可能なアプリポリシーについては、以下を参照してください。

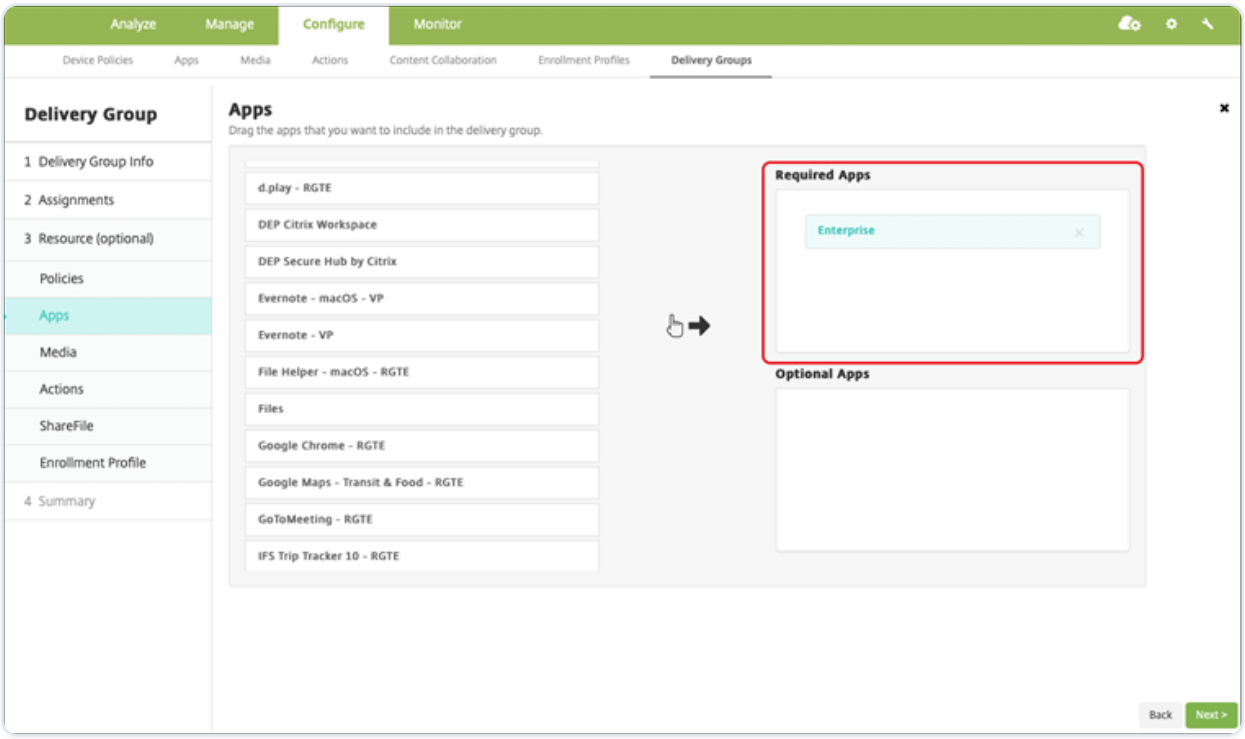
   - MAM SDKの概要
   - MDXポリシーの概要

8. 展開ルールとストア構成を構成します。
9. アプリにデリバリーグループを割り当て、**「保存」**をクリックします。詳細については、「リソースの展開」を参照してください。

ステップ2：アプリの展開を構成する

1. **「構成」>「デリバリーグループ」に移動し、構成したデリバリーグループを選択します。「編集」**をクリックします。
2. **「アプリ」セクションで、目的のアプリを「必須アプリ」**ボックスにドラッグします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 「**概要**」ページで、「**保存**」をクリックします。
4. 「**デリバリーグループ**」ページで、デリバリーグループを選択し、「**展開**」をクリックします。

エンタープライズアプリ

エンタープライズアプリは、MAM SDKまたはMDX Toolkitで準備されていないプライベートアプリを表します。これらのアプリは、自分で開発するか、他のソースから直接入手します。エンタープライズアプリを追加するには、アプリに関連付けられているAPKファイルが必要です。Googleのプライベートアプリのベストプラクティスに従っていることを確認してください。

詳細については、このビデオをご覧ください。

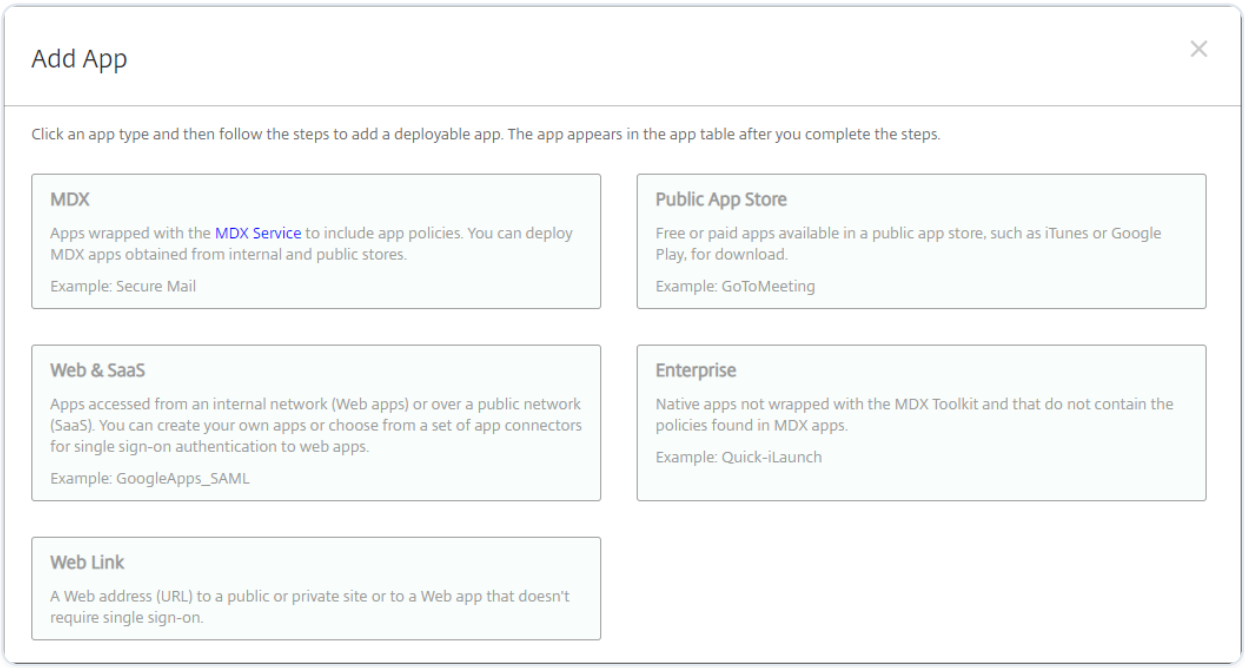
ステップ1：アプリの追加と構成

アプリは次の2つの方法のいずれかで追加します。

- アプリを管理対象Google Playストアに直接公開し、管理対象Playストアアプリとして Citrix Endpoint Managementコンソールに追加します。Googleのドキュメントでプライベートアプリの公開方法に従い、次に管理対象アプリストアアプリセクションの手順に従います。
- アプリをエンタープライズアプリとしてCitrix Endpoint Managementコンソールに追加します。次の手順を実行します。

1. Citrix Endpoint Managementコンソールで、［**構成**］>［**アプリ**］ の順にクリックします。［**追加**］ をクリックします。［**アプリの追加**］ ダイアログボックスが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. **［エンタープライズ］** をクリックします。**［アプリ情報］** ペインで、次の情報を入力します。

   - **名前：** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルのアプリ名の下に表示されます。
   - **説明：** アプリのオプションの説明を入力します。

3. プラットフォームとして**Android Enterprise**を選択します。
4. **アップロード**ボタンをクリックすると、管理対象のGoogle Playストアが開きます。プライベートアプリを公開するために開発者アカウントを登録する必要はありません。続行するには、右下隅にある**プラス**アイコンをクリックします。

   プライベートアプリをアップロードする(/en-us/citrix-endpoint-management/media/upload-enterprise-app.png)

   a. アプリの名前を入力し、.apkファイルをアップロードします。完了したら、**作成**をクリックします。プライベートアプリの公開には最大10分かかる場合があります。

      apkファイルを追加する(/en-us/citrix-endpoint-management/media/add-apk-file.png)

   b. アプリに関する更新情報を受け取るためのメールアドレスを入力します。

      メールアドレスを追加する(/en-us/citrix-endpoint-management/media/add-email-address.png)

   c. アプリケーションが公開されたら、プライベートアプリのアイコンをクリックします。アプリの説明を追加したり、アプリのアイコンを変更したり、その他の操作を行いたい場合

© 1997–2026 Citrix Systems, Inc. All rights reserved.

は、**高度な編集を行う**をクリックします。それ以外の場合は、**選択**をクリックしてアプリ情報ページを開きます。

エンタープライズアプリを公開する(/en-us/citrix-endpoint-management/media/publish-enterprise-app.png)

5. **次へ**をクリックします。プラットフォームのアプリ情報ページが表示されます。
6. プラットフォームの種類の設定を構成します。例:

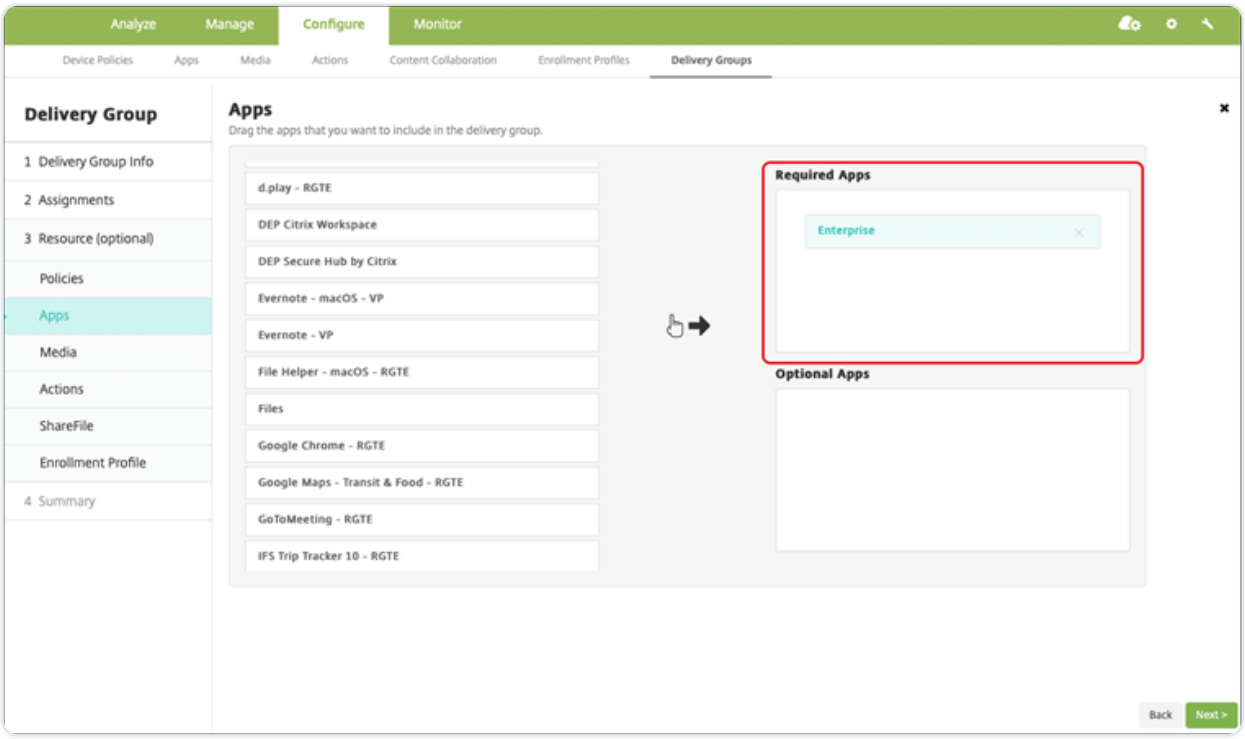
   - **ファイル名:** 必要に応じて、アプリの新しい名前を入力します。
   - **アプリの説明:** 必要に応じて、アプリの新しい説明を入力します。
   - **アプリのバージョン:** このフィールドは変更できません。
   - **パッケージID:** アプリの一意の識別子。
   - **最小OSバージョン:** オプションで、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
   - **最大OSバージョン:** オプションで、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
   - **除外デバイス:** オプションで、アプリを実行できないデバイスの製造元またはモデルを入力します。

7. 展開ルールとストア構成を構成します。
8. アプリにデリバリーグループを割り当て、**保存**をクリックします。詳細については、「リソースの展開」を参照してください。

ステップ2：アプリの展開を構成する

1. **構成 > デリバリーグループ**に移動し、構成したデリバリーグループを選択します。**編集**をクリックします。
2. **アプリ**セクションで、目的のアプリを**必須アプリ**ボックスにドラッグします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. **概要**ページで、**保存**をクリックします。
4. **デリバリーグループ**ページで、デリバリーグループを選択し、**展開**をクリックします。

MDX対応のプライベートアプリ

Android EnterpriseアプリをMDX対応エンタープライズアプリとして追加するには：

1. プライベートAndroid Enterpriseアプリを作成し、そのアプリをMDX対応にします。
2. Citrix Endpoint Managementコンソールにアプリを追加します。
   - アプリを管理対象のGoogle Playストアでホストおよび公開します。
   - アプリをエンタープライズアプリとしてCitrix Endpoint Managementコンソールに追加します。
3. MDXファイルをCitrix Endpoint Managementに追加します。

Google Playストアを通じてアプリをホストおよび公開する場合、Google証明書署名にはオプトインしないでください。MDX対応アプリに使用したのと同じ証明書でアプリに署名します。アプリの公開について詳しくは、GoogleドキュメントのPublishing your appおよびSigning your appを参照してください。MAM SDKはアプリをラップしないため、アプリの開発に使用された証明書以外の証明書は必要ありません。

Google Play Consoleを通じてプライベートアプリを公開する方法について詳しくは、GoogleドキュメントのPublish private apps from the Play Consoleを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementを通じてアプリを公開するには、以下のセクションを参照してください。

Android Enterpriseアプリを準備する

Android Enterpriseアプリを作成する際は、GoogleのBest practices for private appsに従っていることを確認してください。

Android Enterpriseアプリを作成したら、MAM SDKをアプリと統合するか、MDX Toolkitを使用してアプリをラップします。その後、結果のファイルをXenMobileに追加します。

更新された.apkファイルをアップロードすることで、アプリを更新できます。以下の手順では、MDX Toolkitを使用したアプリのラッピングについて説明します。

1. Android Enterpriseアプリを作成し、署名付き.apkファイルを生成します。
2. 以下のサンプルファイルには既知のポリシーがすべて含まれていますが、一部はご使用の環境に適用できない場合があります。使用できない設定はすべて無視されます。以下のパラメーターでXMLファイルを作成します。

```
<?xml version="1.0" encoding="UTF-8"?>

<MobileAppPolicies>

    <PolicySchemaVersion>

        1.0

    </PolicySchemaVersion>

    <Policies>

        <DevicePasscode>false</DevicePasscode>

        <AppPasscode>false</AppPasscode>

        <MaxOfflinePeriod>72</MaxOfflinePeriod>

        <StepupAuthAddress/>

        <RequireUserEntropy>false</RequireUserEntropy>

        <BlockRootedDevices>true</BlockRootedDevices>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        <BlockDebuggerAccess>false</BlockDebuggerAccess>

        <RequireDeviceLock>false</RequireDeviceLock>

        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
NonCompliantDeviceBehavior>

        <WifiOnly>false</WifiOnly>

        <RequireInternalNetwork>false</RequireInternalNetwork>

        <InternalWifiNetworks/>

        <AllowedWifiNetworks/>

        <UpgradeGracePeriod>168</UpgradeGracePeriod>

        <WipeDataOnAppLock>false</WipeDataOnAppLock>

        <ActivePollPeriod>60</ActivePollPeriod>

        <PublicFileAccessLimitsList/>

        <CutAndCopy>Unrestricted</CutAndCopy>

        <Paste>Unrestricted</Paste>

        <DocumentExchange>Unrestricted</DocumentExchange>

        <OpenInExclusionList/>

        <InboundDocumentExchange>Unrestricted</InboundDocumentExchange>

        <InboundDocumentExchangeWhitelist/>

        <connectionSecurityLevel>TLS</connectionSecurityLevel>

        <DisableCamera>false</DisableCamera>

        <DisableGallery>false</DisableGallery>

        <DisableMicrophone>false</DisableMicrophone>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        <DisableLocation>false</DisableLocation>

        <DisableSms>false</DisableSms>

        <DisableScreenCapture>false</DisableScreenCapture>

        <DisableSensor>false</DisableSensor>

        <DisableNFC>false</DisableNFC>

        <BlockLogs>false</BlockLogs>

        <DisablePrinting>false</DisablePrinting>

        <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
MvpnNetworkAccess>

        <MvpnSessionRequired>False</MvpnSessionRequired>

        <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>

        <DisableLocalhostConnections>false</
DisableLocalhostConnections>

        <CertificateLabel/>

        <DefaultLoggerOutput>file,console</DefaultLoggerOutput>

        <DefaultLoggerLevel>15</DefaultLoggerLevel>

        <MaxLogFiles>2</MaxLogFiles>

        <MaxLogFileSize>2</MaxLogFileSize>

        <RedirectSystemLogs>false</RedirectSystemLogs>

        <EncryptLogs>false</EncryptLogs>

        <GeofenceLongitude>0</GeofenceLongitude>

        <GeofenceLatitude>0</GeofenceLatitude>

        <GeofenceRadius>0</GeofenceRadius>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        <EnableGoogleAnalytics>false</EnableGoogleAnalytics>

        <Authentication>OfflineAccessOnly</Authentication>

        <ReauthenticationPeriod>480</ReauthenticationPeriod>

        <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>

    </Policies>

</MobileAppPolicies>
```

3. MDX Toolkitを使用してアプリをラップします。MDX Toolkitの使用方法について詳しくは、Wrapping Android mobile appsを参照してください。

   apptypeパラメーターを**Premium**に設定します。次のコマンドでは、前の手順で作成したXMLファイルを使用します。

   アプリのストアURLがわかっている場合は、**storeURL**パラメーターをそのストアURLに設定します。アプリを公開すると、ユーザーはそのストアURLからアプリをダウンロードします。

   SampleAEappというアプリをラップするために使用されるMDX Toolkitコマンドの例を次に示します。

```
```

 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en
-Duser.variant

 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap

 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk

 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx

 -MinPlatform 5.0

 -keystore /MyKeystore

 -storepass mystorepwd123

 -keyalias key0
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.
```

```
 -keypass mykeypwd123

 -storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"

 -appType Premium

 -premiumMdxPolicies <Path to Premium policy XML>

```
```

アプリをラップすると、ラップされた.apkファイルと.mdxファイルが生成されます。

ラップされた.apkファイルを追加する

アプリを次の2つの方法のいずれかで追加します。

- アプリをマネージドGoogle Playストアに直接公開し、Citrix Endpoint Managementコンソールにマネージドplayストアアプリとして追加します。プライベートアプリを公開する方法についてはGoogleのドキュメントに従い、その後マネージドアプリストアアプリセクションの手順に従ってください。
- Citrix Endpoint Managementコンソールにエンタープライズアプリとしてアプリを追加します。次の手順を実行します。

1. Citrix Endpoint Managementコンソールで、**構成 > アプリ**をクリックします。**アプリ**ページが開きます。
2. **追加**をクリックします。**アプリの追加**ダイアログボックスが表示されます。

   アプリ構成画面(/en-us/citrix-endpoint-management/media/configure-apps-add.png)
3. **エンタープライズ**をクリックします。**アプリ情報**ペインで、次の情報を入力します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルの「アプリ名」の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
4. プラットフォームとして**Android Enterprise**を選択します。
5. **アップロード**ボタンをクリックすると、マネージドGoogle Playストアが開きます。プライベートアプリを公開するために開発者アカウントを登録する必要はありません。続行するには、右下隅にある**プラス**アイコンをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.
```

プライベートアプリのアップロード(/en-us/citrix-endpoint-management/media/upload-enterprise-app.png)

a. アプリの名前を入力し、.apkファイルをアップロードします。完了したら、**作成**をクリックします。プライベートアプリが公開されるまで最大10分かかる場合があります。

   apkファイルを追加(/en-us/citrix-endpoint-management/media/add-apk-file.png)

b. アプリに関する更新情報を受け取るには、メールアドレスを入力します。

   メールアドレスを追加(/en-us/citrix-endpoint-management/media/add-email-address.png)

c. アプリケーションが公開されたら、プライベートアプリのアイコンをクリックし、**選択**をクリックしてアプリ情報ページを開きます。

   エンタープライズアプリを公開(/en-us/citrix-endpoint-management/media/publish-enterprise-app.png)

6. **次へ**をクリックします。プラットフォームのアプリ情報ページが表示されます。
7. プラットフォームの種類に応じて、次のように設定を構成します。

   - **ファイル名:** 必要に応じて、アプリの新しい名前を入力します。
   - **アプリの説明:** 必要に応じて、アプリの新しい説明を入力します。
   - **アプリのバージョン:** このフィールドは変更できません。
   - **パッケージID:** アプリの一意の識別子です。
   - **最小OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
   - **最大OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
   - **除外デバイス:** 必要に応じて、アプリを実行できないデバイスの製造元またはモデルを入力します。

8. デプロイメントルールとストア構成を構成します。
9. **Enterprise App** ページで、**Next** をクリックします。**Approvals** ページが表示されます。

   ユーザーがアプリにアクセスする前に承認を要求するワークフローを使用するには、「ワークフローの適用」を参照してください。承認ワークフローが不要な場合は、手順13に進むことができます。

10. **Next** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. **Delivery Group Assignment** ページが表示されます。このページでは何も操作する必要はありません。.mdxファイルを追加するときに、このアプリのデリバリーグループと展開スケジュールを構成します。**Save** をクリックします。

オプション: ストアURLを追加または変更する

アプリをラップしたときにストアURLがわからなかった場合は、ここでストアURLを追加します。

1. 管理対象のGoogle Playストアでアプリを表示します。アプリを選択すると、ブラウザのアドレスバーにストアURLが表示されます。URL形式からアプリのパッケージ名をコピーします。例: `https://play.google.com/store/apps/details?id=SampleAEappPackage`。コピーしたURLは`https://play.google.com/work/`で始まる場合があります。`work`を`store`に変更してください。
2. MDX Toolkitを使用して、ストアURLを.mdxファイルに追加します。

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \

setinfo \

-in ~/Desktop/SampleApps/Sample.mdx \

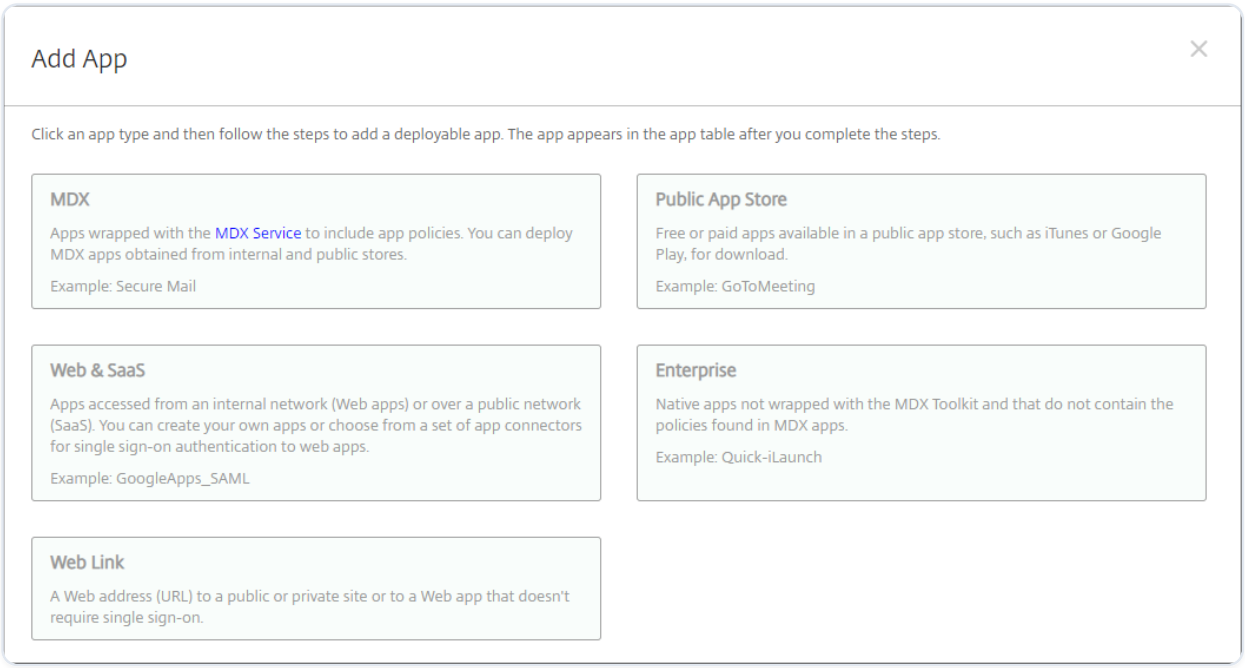
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \

-storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"
```

.mdxファイルを追加する

1. Citrix Endpoint Managementコンソールで、**Configure > Apps** をクリックします。**Add** をクリックします。**Add App** ダイアログボックスが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

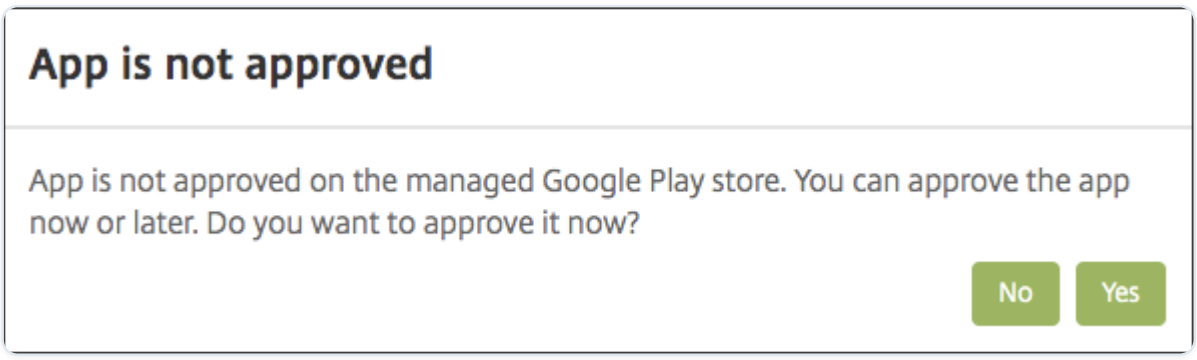


2. **MDX** をクリックします。**MDX App Information** ページが表示されます。**App Information** ペインに、次の情報を入力します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、**Apps** テーブルの**App Name** の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。

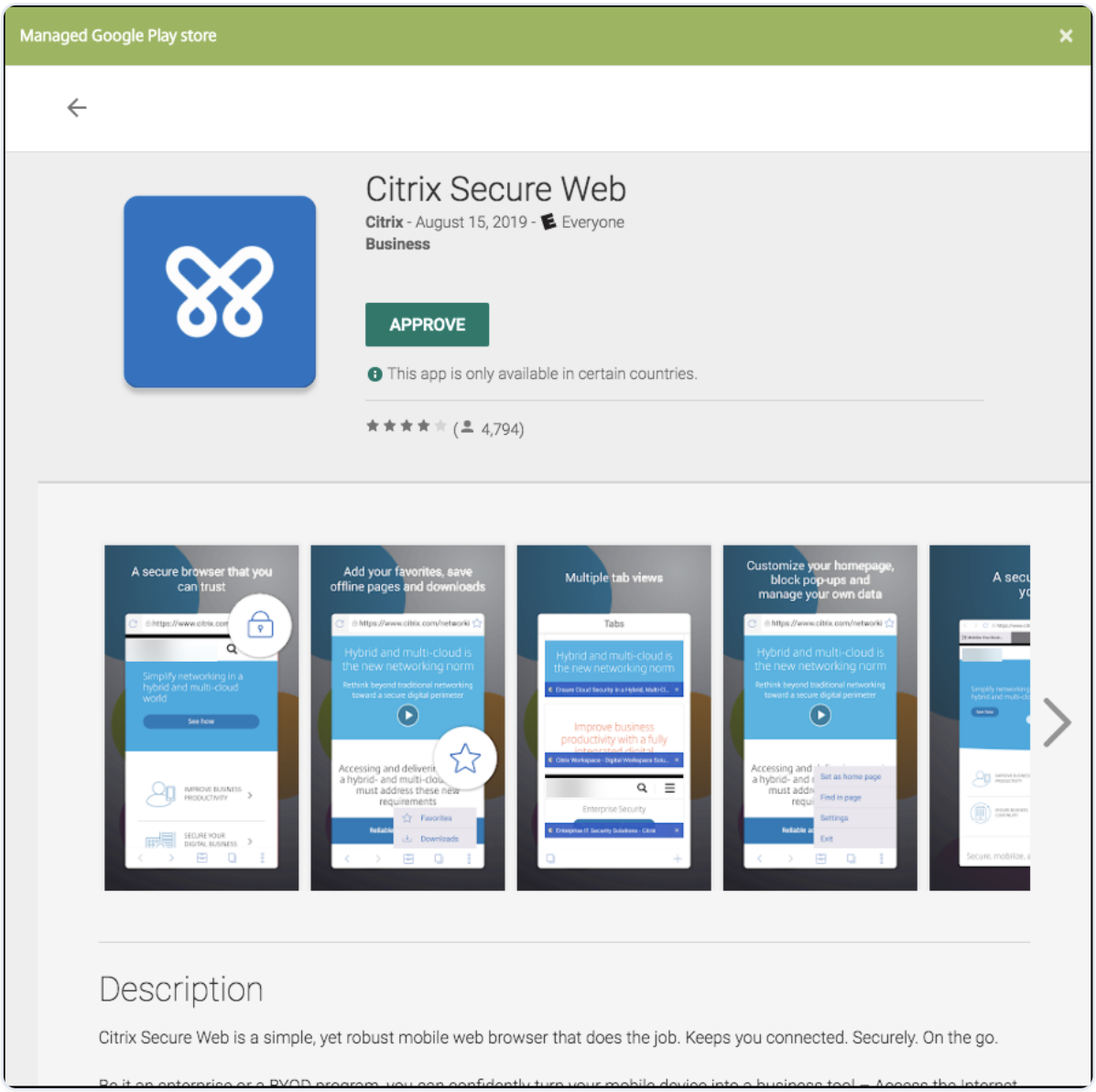
3. プラットフォームとして**Android Enterprise**を選択します。
4. **アップロード**をクリックし、MDXファイルに移動します。Android Enterpriseは、MDX Toolkitでラップされたアプリのみをサポートしています。

   - 添付されたアプリケーションが管理対象のGoogle Playストアからの承認を必要とする場合、UIが通知します。Citrix Endpoint Managementコンソールを離れることなくアプリケーションを承認するには、**はい**をクリックします。

   管理対象のGoogle Playストアが開いたら、指示に従ってアプリを承認して保存します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



アプリが正常に追加されると、**アプリの詳細**ページが表示されます。

5. 次の設定を構成します。

- **ファイル名:** アプリに関連付けられたファイル名を入力します。
- **アプリの説明:** アプリの説明を入力します。
- **アプリのバージョン:** 必要に応じて、アプリのバージョン番号を入力します。
- **パッケージID:** 管理対象のGoogle Playストアから取得したアプリのパッケージIDを入力します。
- **最小OSバージョン:** 必要に応じて、アプリを使用するためにデバイスが実行できる最も古いオペレーティングシステムバージョンを入力します。
- **最大OSバージョン:** 必要に応じて、アプリを使用するためにデバイスが実行する必要がある最新のオペレーティングシステムを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **除外デバイス:** 必要に応じて、アプリを実行できないデバイスのメーカーまたはモデルを入力します。

6. 「**MDXポリシー**」を構成します。MDXポリシーはプラットフォームによって異なり、認証、デバイスセキュリティ、アプリ制限などのポリシー領域のオプションが含まれます。コンソールでは、各ポリシーにポリシーを説明するツールヒントが表示されます。各デバイスプラットフォームタイプで利用可能なアプリポリシーについては、以下を参照してください。

   - MAM SDKの概要
   - MDXサードパーティアプリポリシーの概要

7. 展開ルールとストア構成を構成します。

   「**Deploy for always-on connection**」は、「**Settings > Server Properties**」でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

   常時接続オプション：

   - iOSデバイスでは利用できません
   - バージョン10.18.19以降でCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様は利用できません
   - バージョン10.18.19より前にCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様には推奨されません

   構成する展開スケジュールは、すべてのプラットフォームで同じです。「**Deploy for always-on connection**」を除き、加えた変更はすべてのプラットフォームに適用されます。

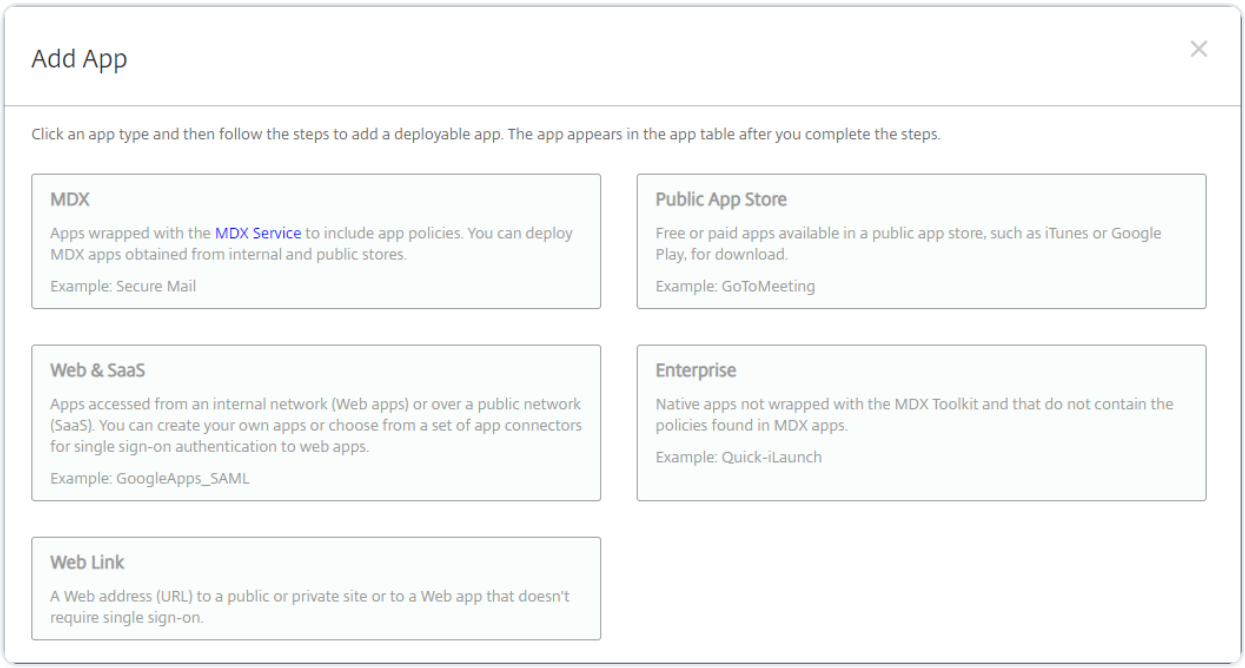
8. アプリにデリバリーグループを割り当て、「**Save**」をクリックします。詳細については、「リソースの展開」を参照してください。

アプリを更新する

Android Enterpriseアプリを更新するには、更新された.apkファイルをラップしてアップロードします。

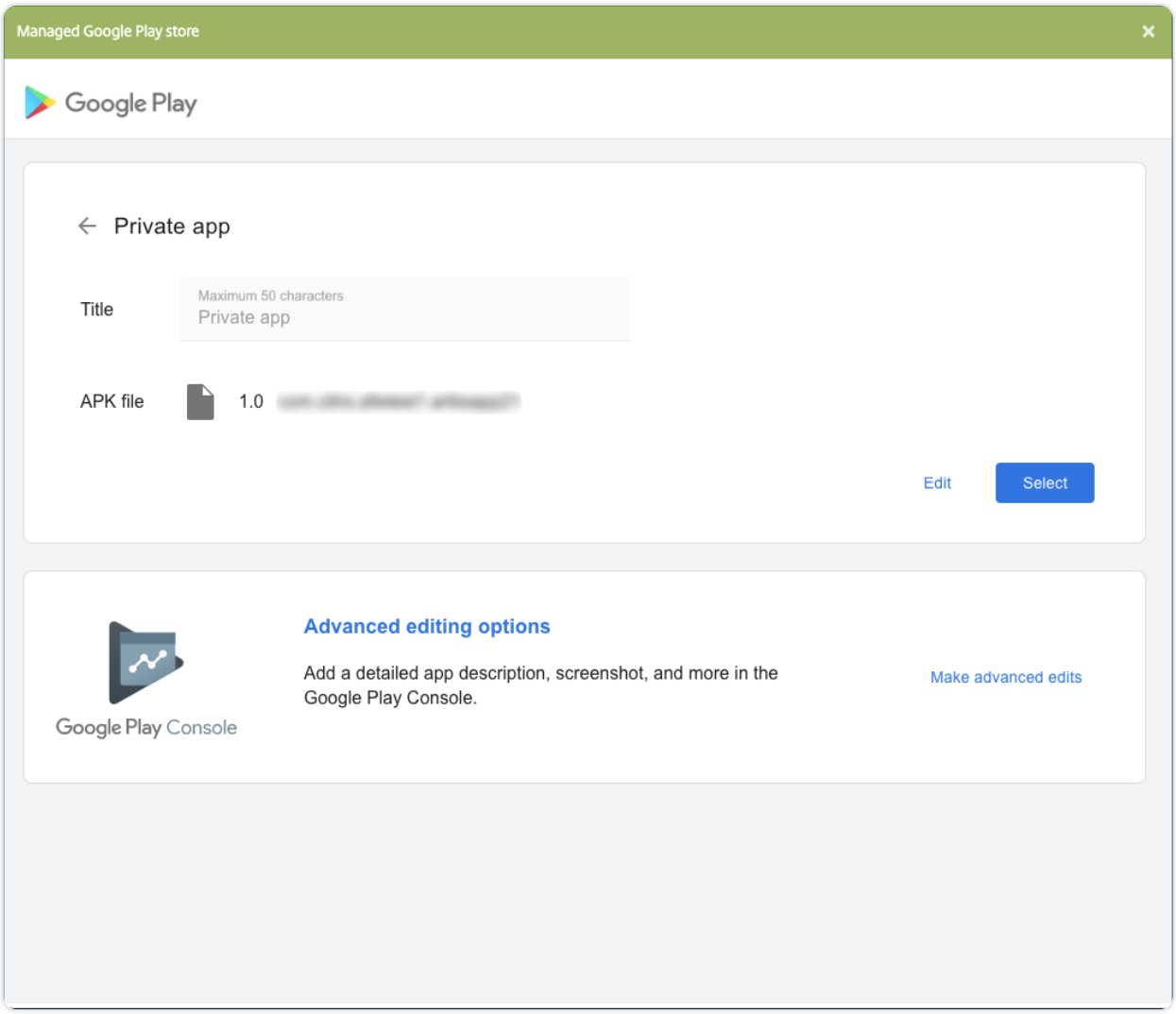
1. 更新されたアプリの.apkファイルをMAM SDKまたはMDX Toolkitを使用してラップします。
2. Citrix Endpoint Managementコンソールで、「**Configure > Apps**」をクリックします。「**Apps**」ページが開きます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. **追加**をクリックします。「**アプリの追加**」ダイアログボックスが表示されます。
4. **エンタープライズ**をクリックします。「**アプリ情報**」ペインで、次の情報を入力します。
   - **名前:** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルの「アプリ名」の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
5. プラットフォームとして「**Android Enterprise**」を選択します。
6. **次へ**をクリックします。「**エンタープライズアプリ**」ページが表示されます。
7. **アップロード**をクリックします。
8. 管理対象のGoogle Playストアページで、更新するアプリを選択します。
9. アプリ情報ページで、.apkファイル名の横にある「**編集**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. 新しい.apkファイルに移動してアップロードします。
11. 管理対象のGoogle Playストアページで、「**保存**」をクリックします。

Google Workspace (旧 G Suite) のお客様向けレガシー Android Enterprise

Google Workspace のお客様は、レガシー Android Enterprise を構成するために、レガシー Android Enterprise 設定を使用する必要があります。Google は最近、G Suite を Google Workspace に名称変更しました。

組織がすでに Google Workspace を使用してユーザーに Google アプリへのアクセスを提供している場合、Google Workspace を使用して Citrix を EMM として登録できます。組織が Google Workspace を使用している場合、既存のエンタープライズ ID とユーザー用の既存の Google アカウントを持っています。Citrix Endpoint Management を Google Workspace とともに使用するには、LDAP ディレクトリと同期し、Google Directory API を使用して Google から Google アカウント情報を取得します。この種類のエンタープライズは既存のドメインに紐付けられているため、各ドメインは1つのエンタープライズしか作成できません。Citrix Endpoint Management にデバイスを登録するには、各ユーザーは既存の Google アカウントで手動でサインインする必要がありま

© 1997–2026 Citrix Systems, Inc. All rights reserved.

す。このアカウントにより、Google Workspace プランで提供される他の Google サービスに加えて、管理対象の Google Play にアクセスできるようになります。

レガシー Android Enterprise の要件:

- 公開アクセス可能なドメイン
- Google 管理者アカウント
- 管理プロファイルのサポートがある Android デバイス
- Google Play がインストールされている Google アカウント
- デバイスに設定されている仕事用プロファイル

レガシー Android Enterprise の構成を開始するには、Citrix Endpoint Management の設定の **Android Enterprise** ページで **レガシー Android Enterprise** をクリックします。

レガシー Android Enterprise オプション(/en-us/citrix-endpoint-management/media/android-enterprise-setup-connect-legacy.png)

Android Enterprise アカウントを作成する

Android Enterprise アカウントを設定する前に、Google でドメイン名を検証する必要があります。

Google でドメイン名をすでに検証している場合、この手順をスキップできます: Android Enterprise サービスアカウントを設定し、Android Enterprise 証明書をダウンロードする。

1. `<https://gsuite.google.com/signup/basic/welcome>` に移動します。

   次のページに、管理者情報と会社情報を入力する画面が表示されます。

   アカウント設定ページ(/en-us/citrix-endpoint-management/media/afw-account-setup-redirect.png)
2. 管理者ユーザー情報を入力します。

   管理者ユーザー情報(/en-us/citrix-endpoint-management/media/afw-enter-admin-user-info.png)
3. 管理者アカウント情報に加えて、会社情報を入力します。

   会社情報画面(/en-us/citrix-endpoint-management/media/afw-enter-company-info.png)

   プロセスの最初のステップが完了し、次のページが表示されます。

   確認ページ(/en-us/citrix-endpoint-management/media/afw-dns-verification-1.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ドメイン所有権の確認

Googleが次のいずれかの方法でドメインを確認できるようにします。

- ドメインホストのWebサイトにTXTまたはCNAMEレコードを追加します。
- HTMLファイルをドメインのWebサーバーにアップロードします。
- ホームページに`<meta>`タグを追加します。Googleは最初の方法を推奨しています。この記事では、ドメイン所有権を確認する手順については説明していませんが、必要な情報は次の場所で見つけることができます: https://support.google.com/a/answer/6248925.

1. **Start**をクリックして、ドメインの確認を開始します。

   Verify domain ownershipページが表示されます。ページの手順に従ってドメインを確認します。
2. 「**確認**」をクリックします。

   確認ボタン(/en-us/citrix-endpoint-management/media/afw-verify-domain-ownership.png)

   確認の確認(/en-us/citrix-endpoint-management/media/afw-domain-verified.png)
3. Googleがドメインの所有権を確認します。

   ドメイン所有権の確認(/en-us/citrix-endpoint-management/media/afw-google-verification.png)
4. 確認が正常に完了すると、次のページが表示されます。「**続行**」をクリックします。

   成功確認ページ(/en-us/citrix-endpoint-management/media/afw-dns-verification-9.png)
5. Googleは、Citrix®に提供し、Android Enterprise設定を構成するときに使用するEMMバインディングトークンを作成します。トークンをコピーして保存してください。セットアップ手順の後半で必要になります。

   バインディングトークン(/en-us/citrix-endpoint-management/media/afw-obtain-token.png)
6. 「**完了**」をクリックして、Android Enterpriseのセットアップを完了します。ドメインが正常に確認されたことを示すページが表示されます。

Android Enterpriseサービスアカウントを作成した後、Google管理コンソールにサインインして、モビリティ管理設定を管理できます。

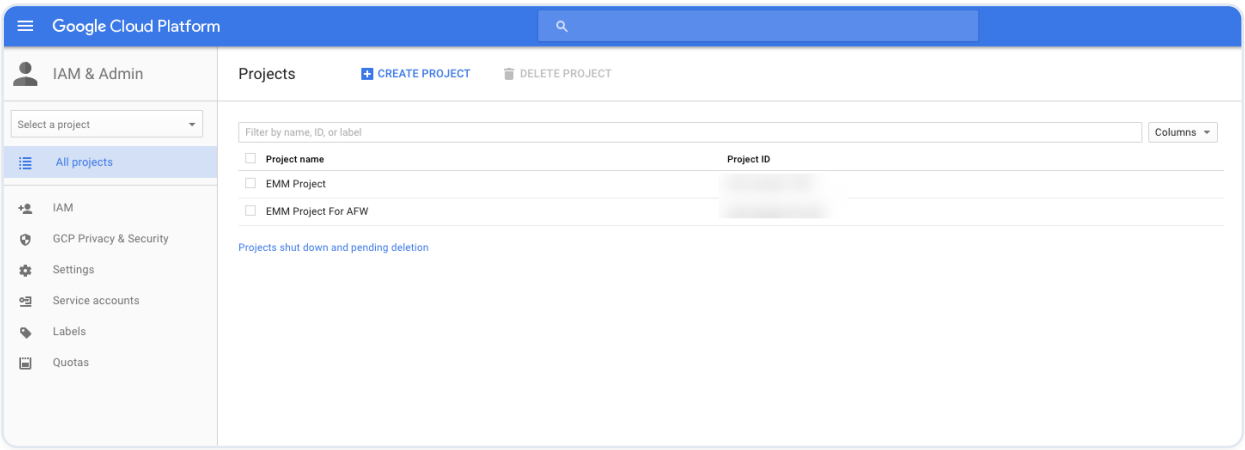
Android Enterpriseサービスアカウントを設定し、Android Enterprise証明書をダウンロードする

Citrix Endpoint ManagementがGoogle PlayおよびDirectoryサービスに接続できるようにするには、開発者向けのGoogle Projectポータルを使用してサービスアカウントを作成する必要がありま

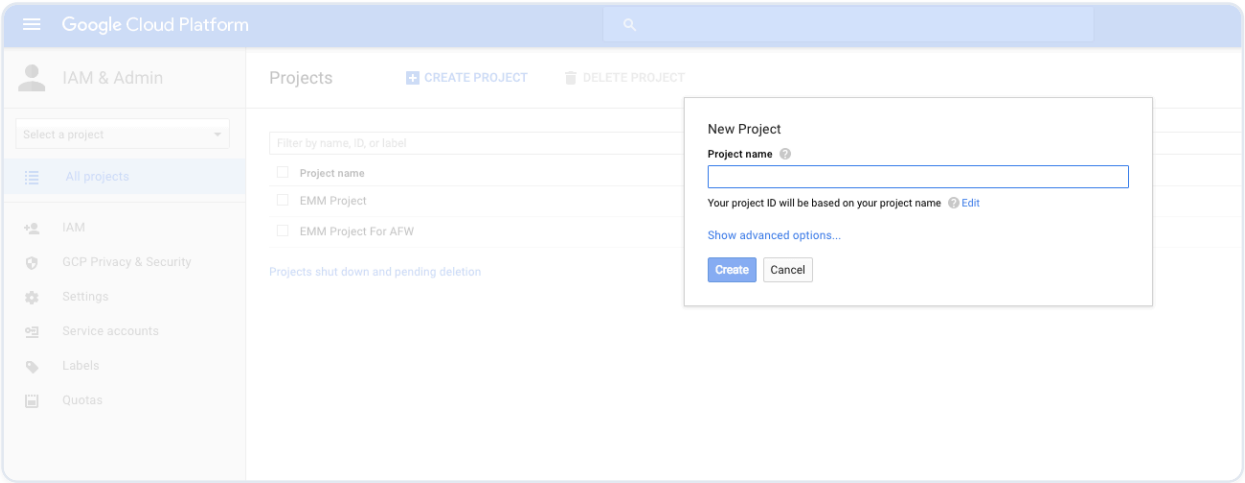
© 1997–2026 Citrix Systems, Inc. All rights reserved.

す。このサービスアカウントは、Citrix Endpoint ManagementとAndroid向けGoogleサービス間のサーバー間通信に使用されます。使用されている認証プロトコルの詳細については、`<https://developers.google.com/identity/protocols/OAuth2ServiceAccount>`にアクセスしてください。

1. Webブラウザで`<https://console.cloud.google.com/project>`にアクセスし、Google管理者資格情報でサインインします。
2. **プロジェクト**リストで、「**プロジェクトを作成**」をクリックします。

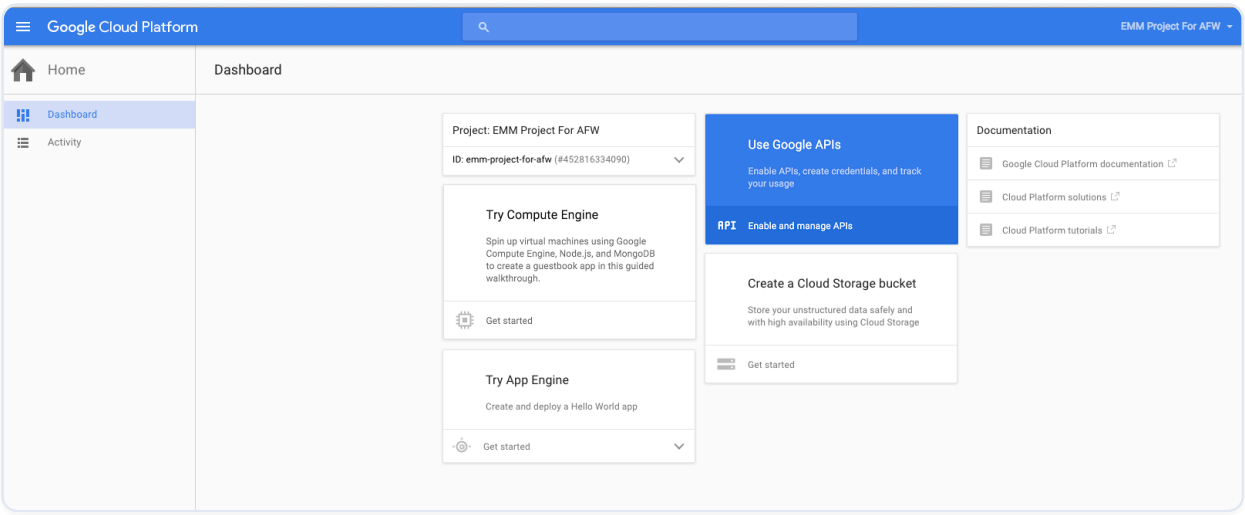


3. **プロジェクト名**に、プロジェクトの名前を入力します。

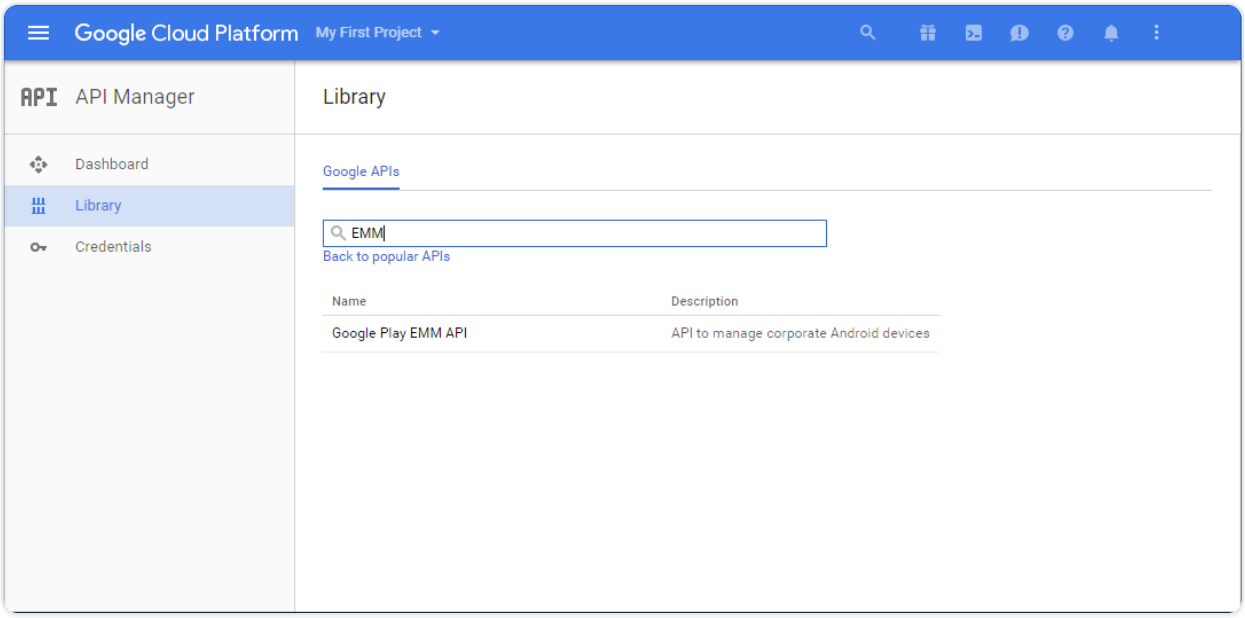


4. ダッシュボードで、**Google API を使用**をクリックします。

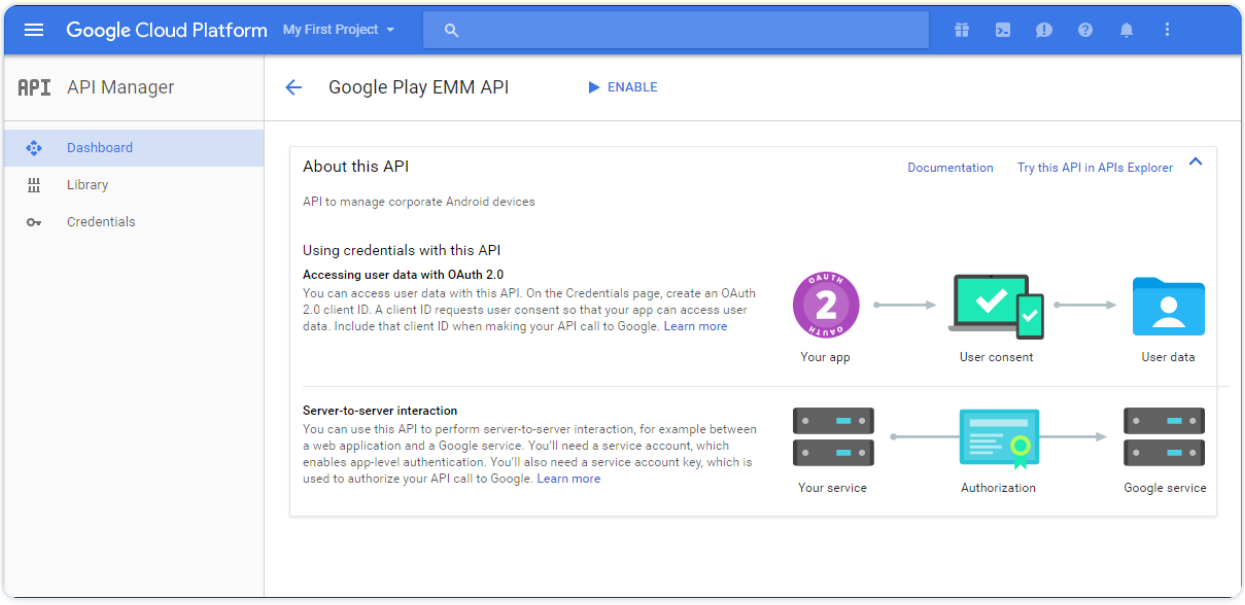
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. **ライブラリ**をクリックし、**検索**に「**EMM**」と入力して、検索結果をクリックします。

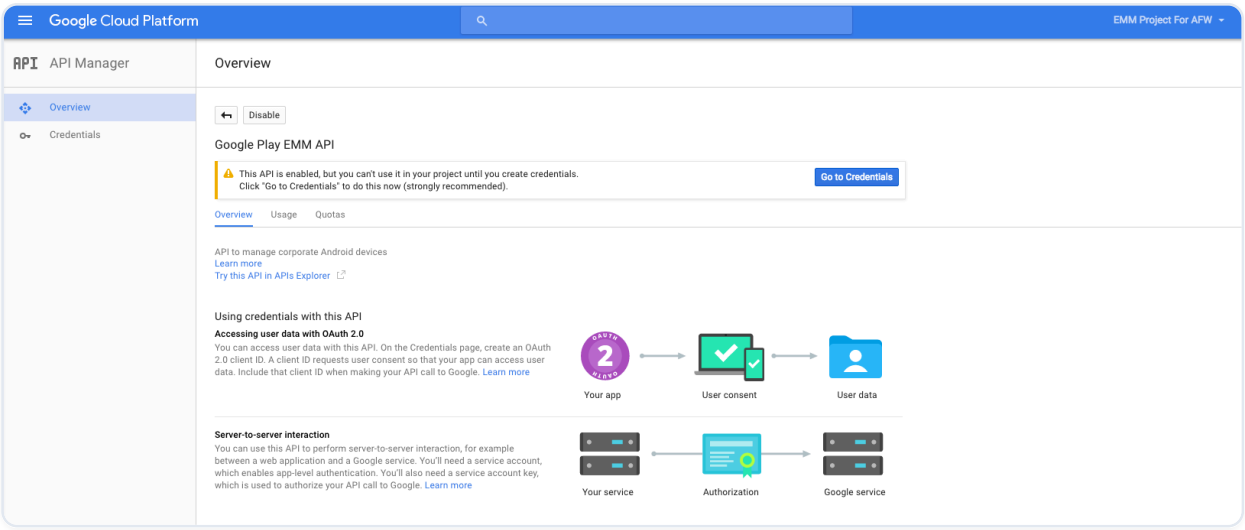


6. **概要**ページで、**有効にする**をクリックします。

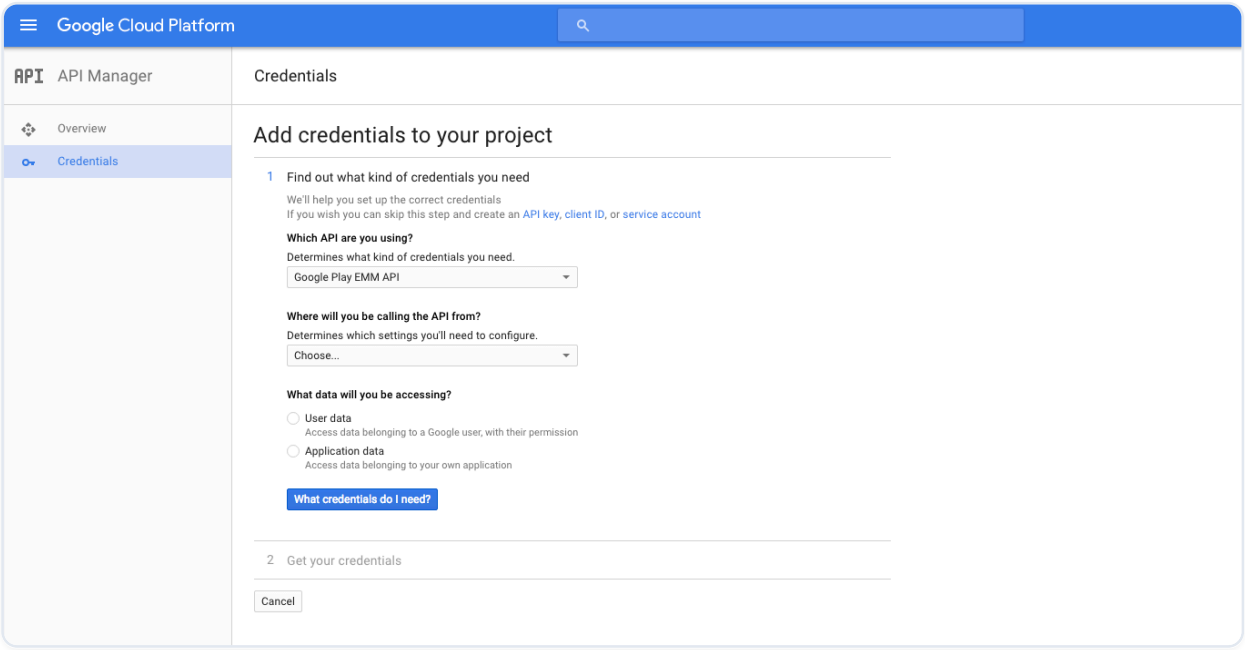


© 1997–2026 Citrix Systems, Inc. All rights reserved.

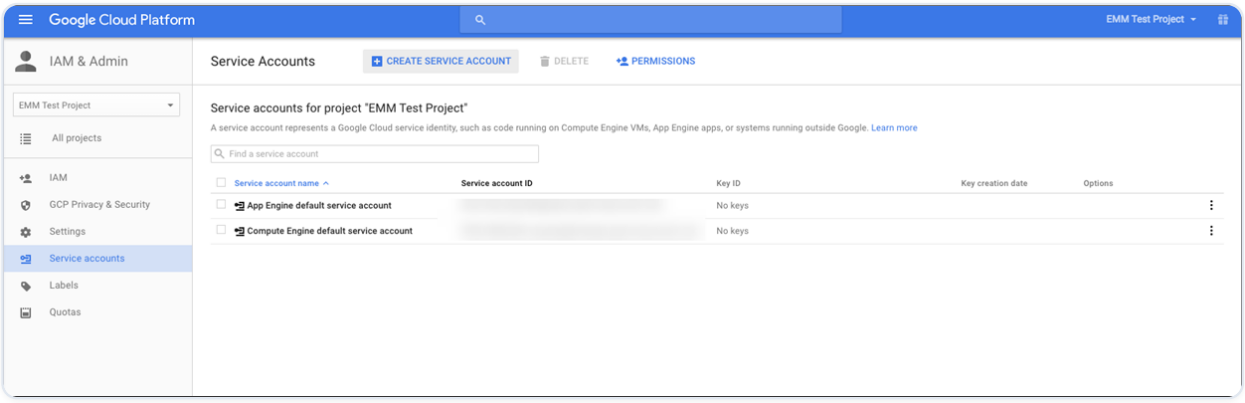
7. **Google Play EMM API**の横にある**認証情報に移動**をクリックします。



8. **プロジェクトに認証情報を追加**リストのステップ1で、**サービスアカウント**をクリックします。

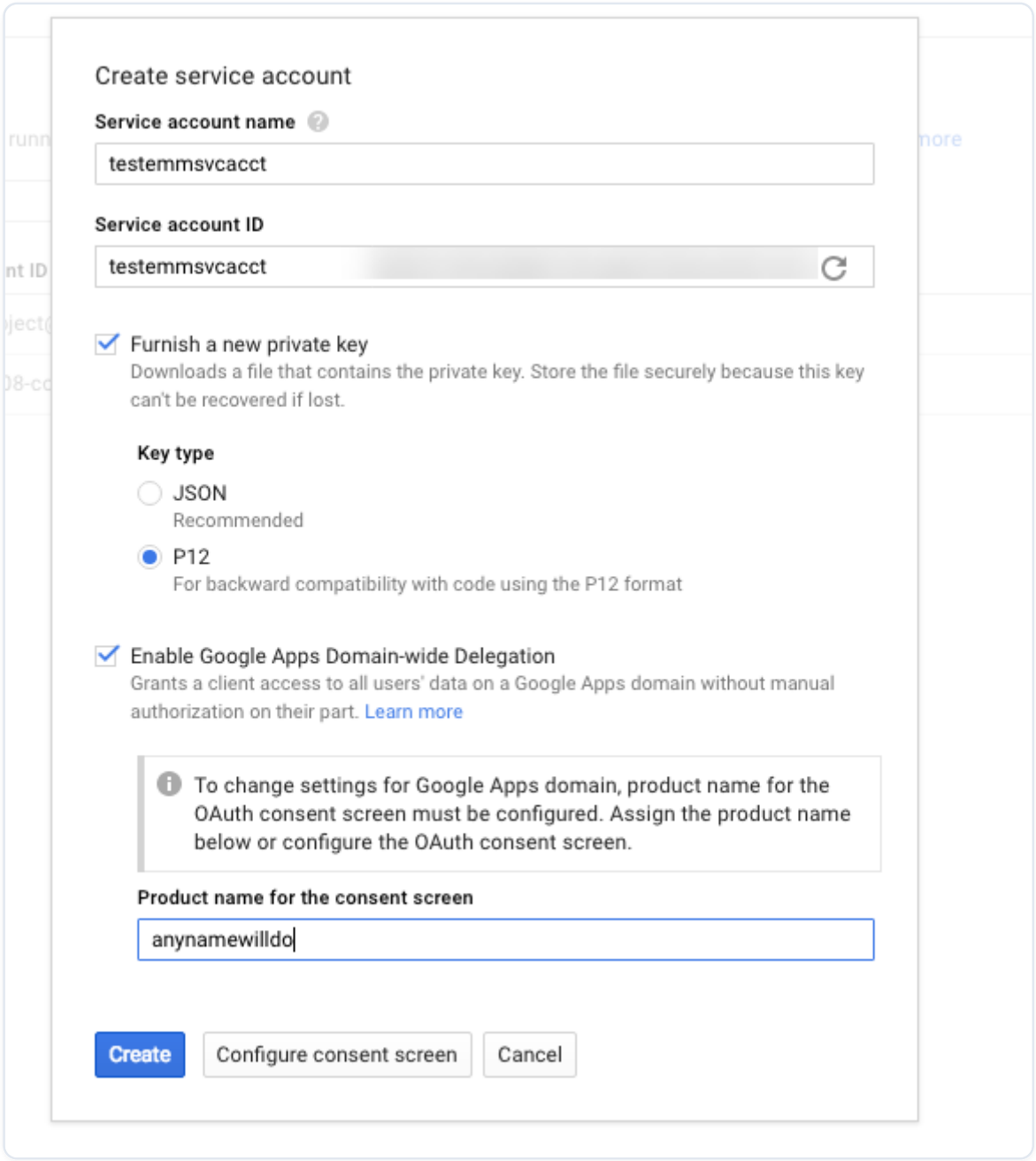


9. **サービスアカウント**ページで、**サービスアカウントを作成**をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

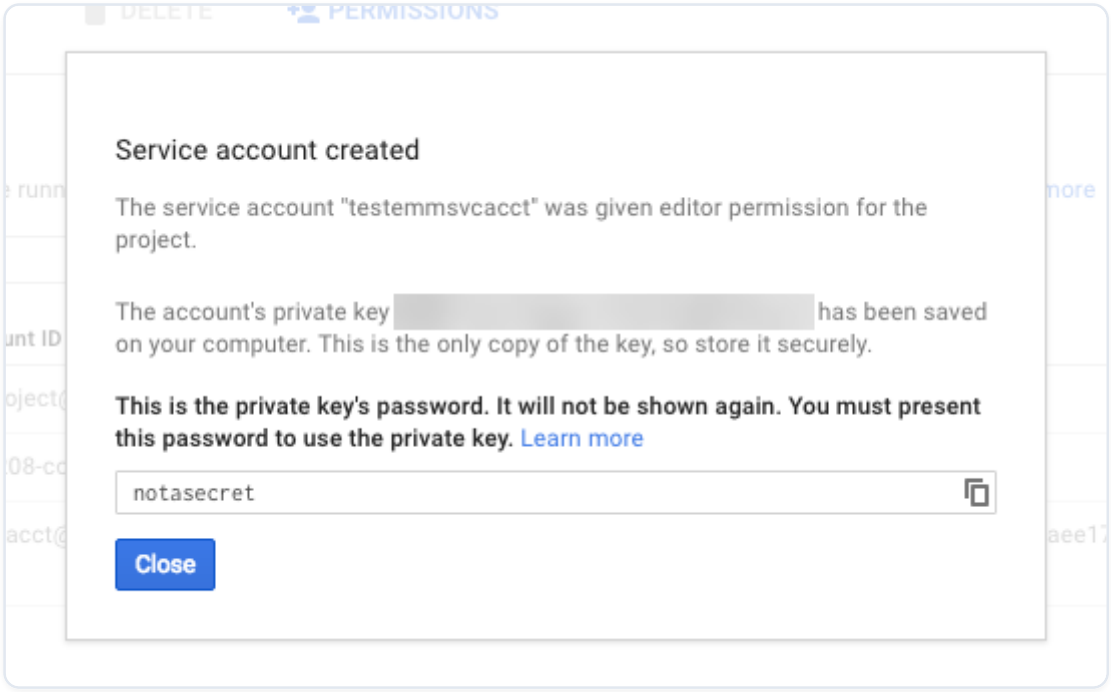
10. 「**サービスアカウントを作成**」で、アカウントに名前を付け、「**新しい秘密鍵を提供する**」チェックボックスをオンにします。「**P12**」をクリックし、「**Google Apps ドメイン全体の委任を有効にする**」チェックボックスをオンにしてから、「**作成**」をクリックします。



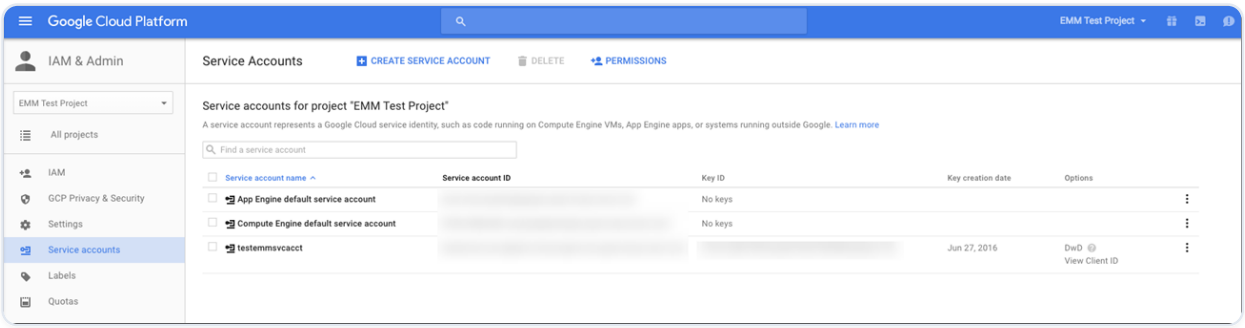
証明書（P12ファイル）がコンピューターにダウンロードされます。証明書は安全な場所に保存してください。

11. 「**サービスアカウントが作成されました**」確認ページで、「**閉じる**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

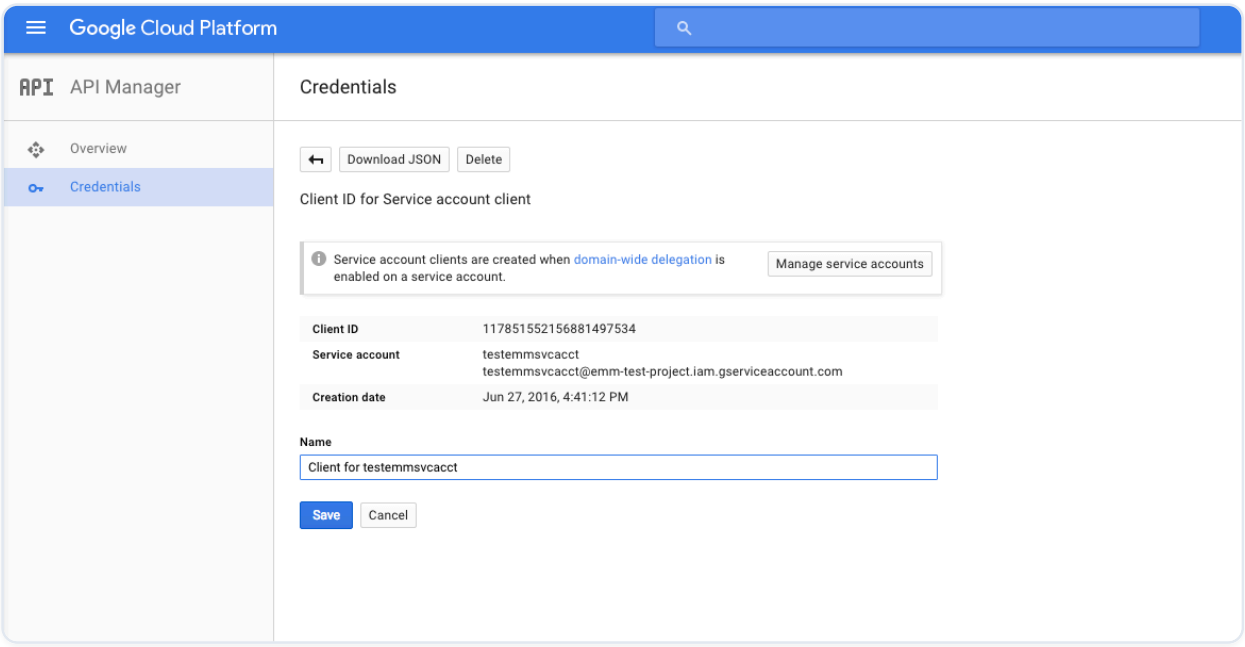


12. 「**権限**」で「**サービスアカウント**」をクリックし、サービスアカウントの「**オプション**」の下にある「**クライアントIDを表示**」をクリックします。

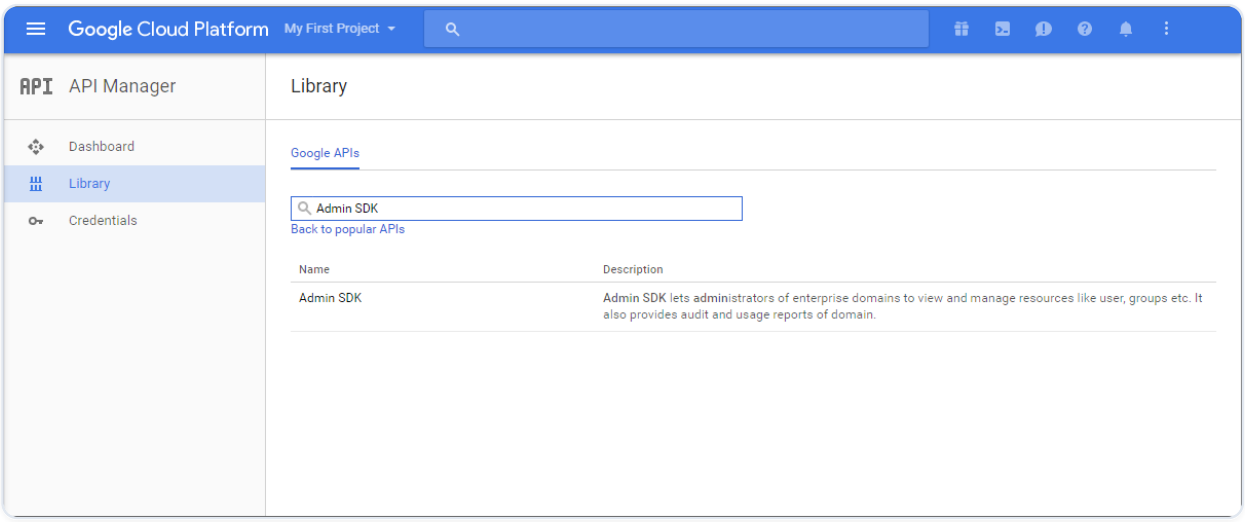


13. Google管理コンソールでのアカウント認証に必要な詳細が表示されます。後で情報を取得できる場所に「**クライアントID**」と「**サービスアカウントID**」をコピーします。この情報とドメイン名をCitrixサポートに送信して、許可リストに追加してもらう必要があります。

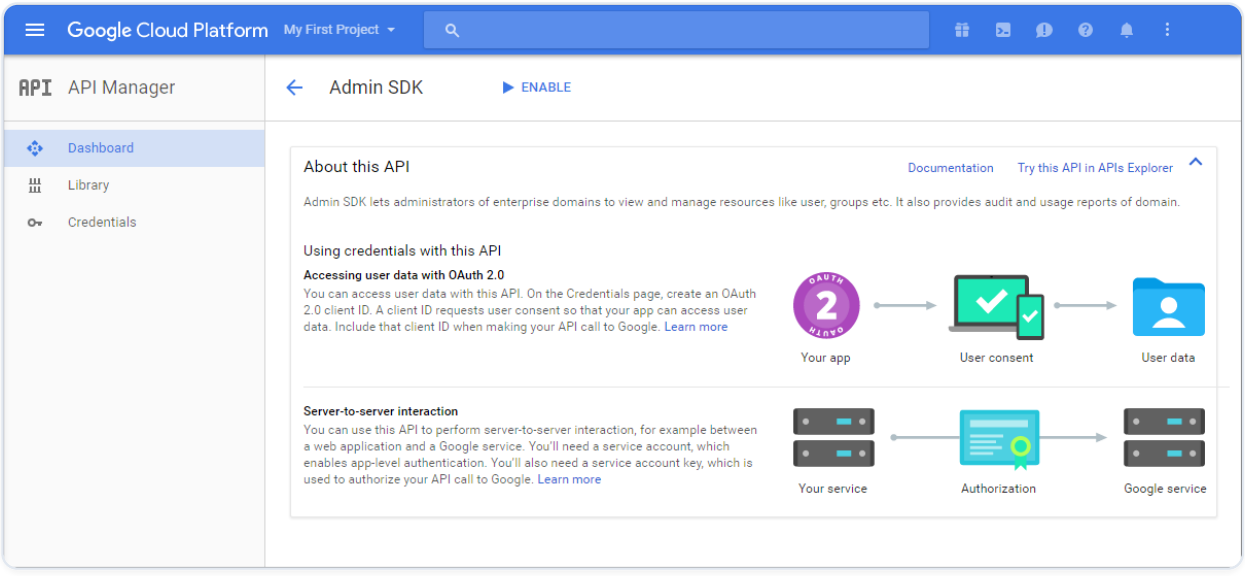
© 1997–2026 Citrix Systems, Inc. All rights reserved.



14. 「**ライブラリ**」ページで、「**Admin SDK**」を検索し、検索結果をクリックします。

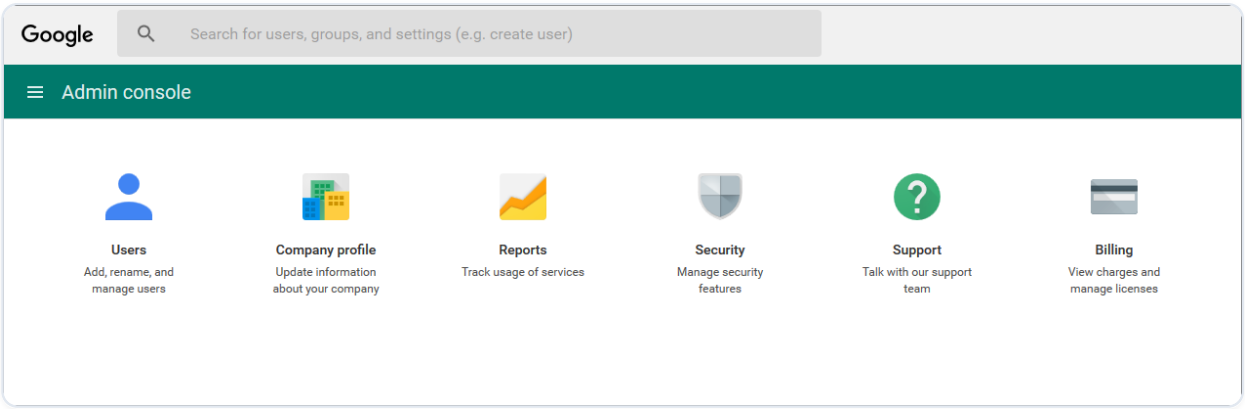


15. 「**概要**」ページで、「**有効にする**」をクリックします。

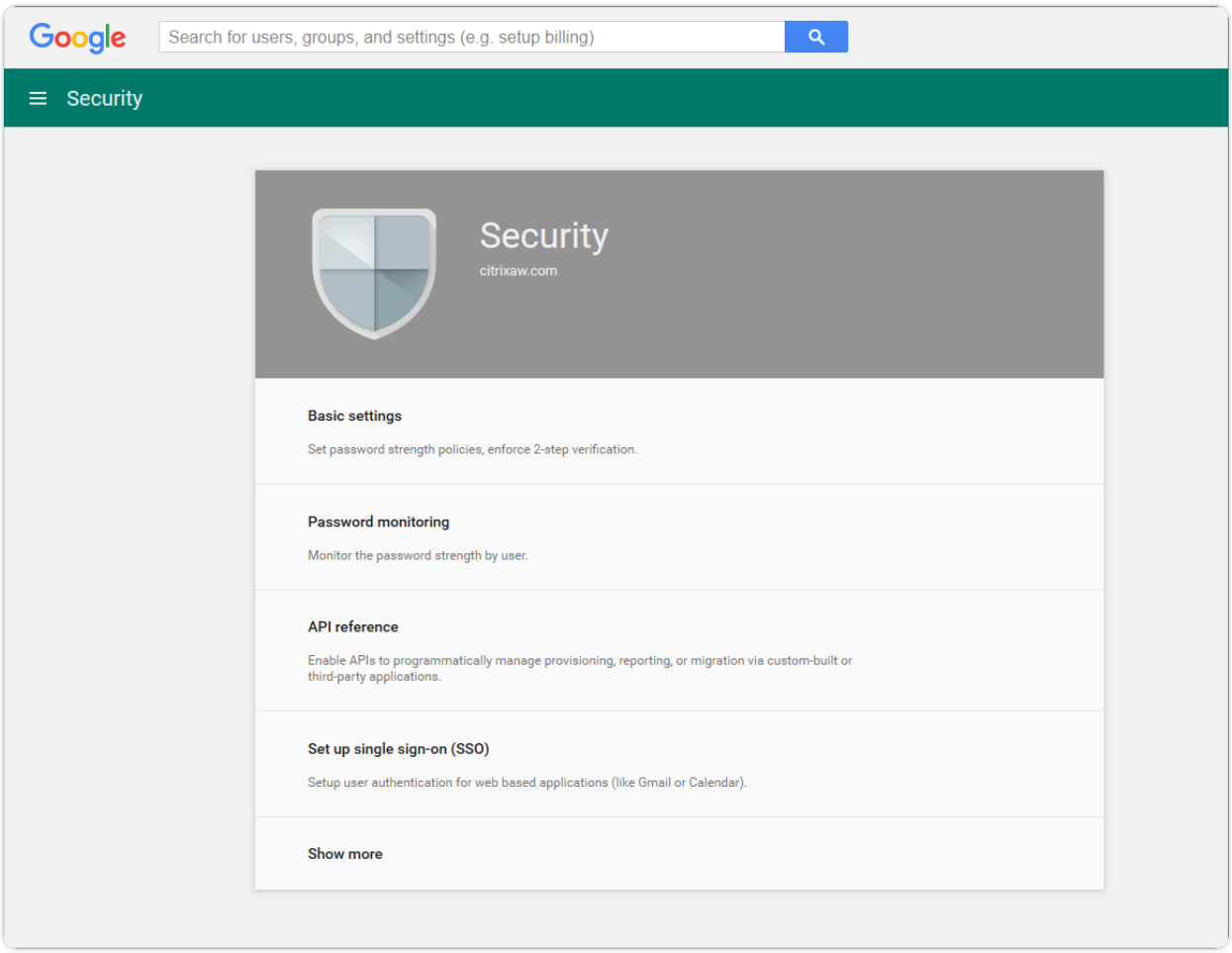


© 1997–2026 Citrix Systems, Inc. All rights reserved.

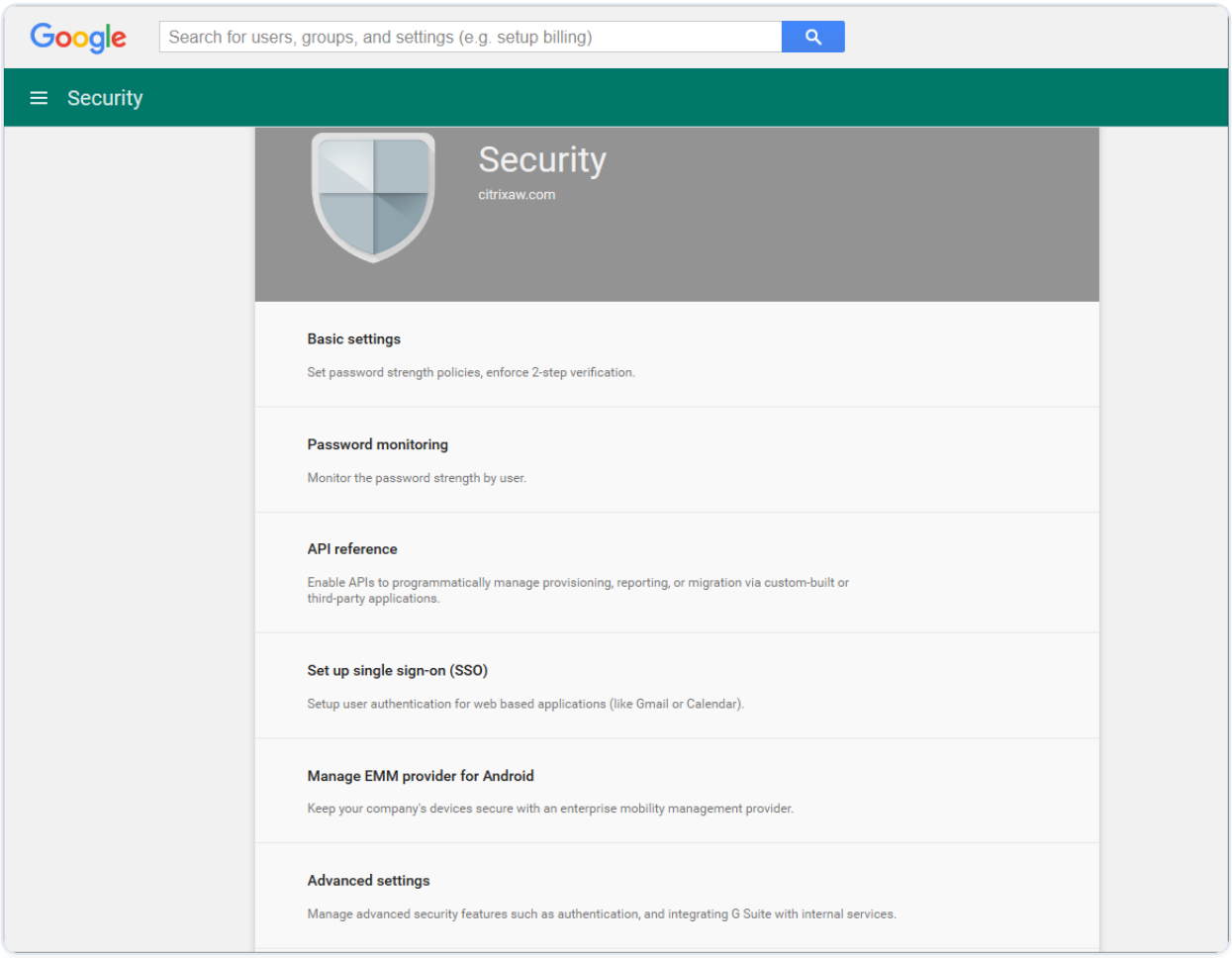
16. ドメインのGoogle管理コンソールを開き、「**セキュリティ**」をクリックします。



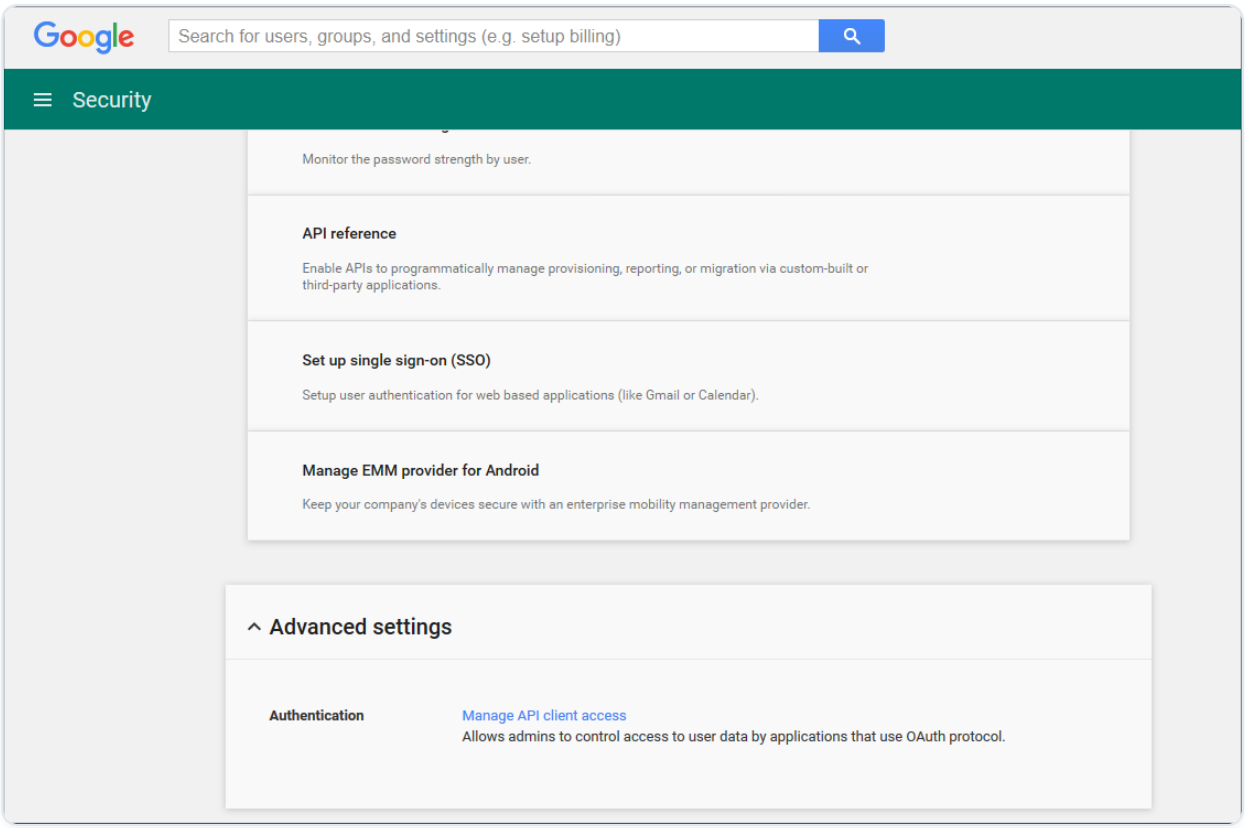
17. 「**設定**」ページで、「**さらに表示**」をクリックし、次に「**詳細設定**」をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

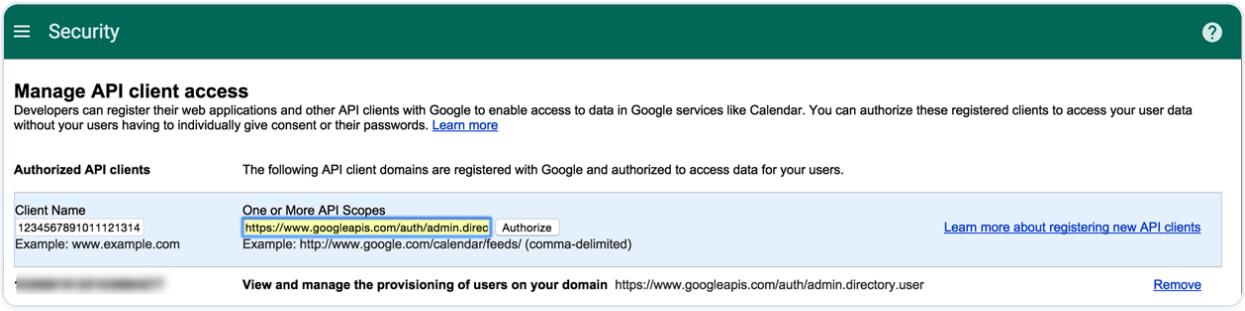


18. 「**APIクライアントアクセスを管理**」をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

19. 「**クライアント名**」に以前保存したクライアントIDを入力し、「**1つ以上のAPIスコープ**」に `https://www.googleapis.com/auth/admin.directory.user` と入力して、「**承認**」をクリックします。



EMMへのバインド

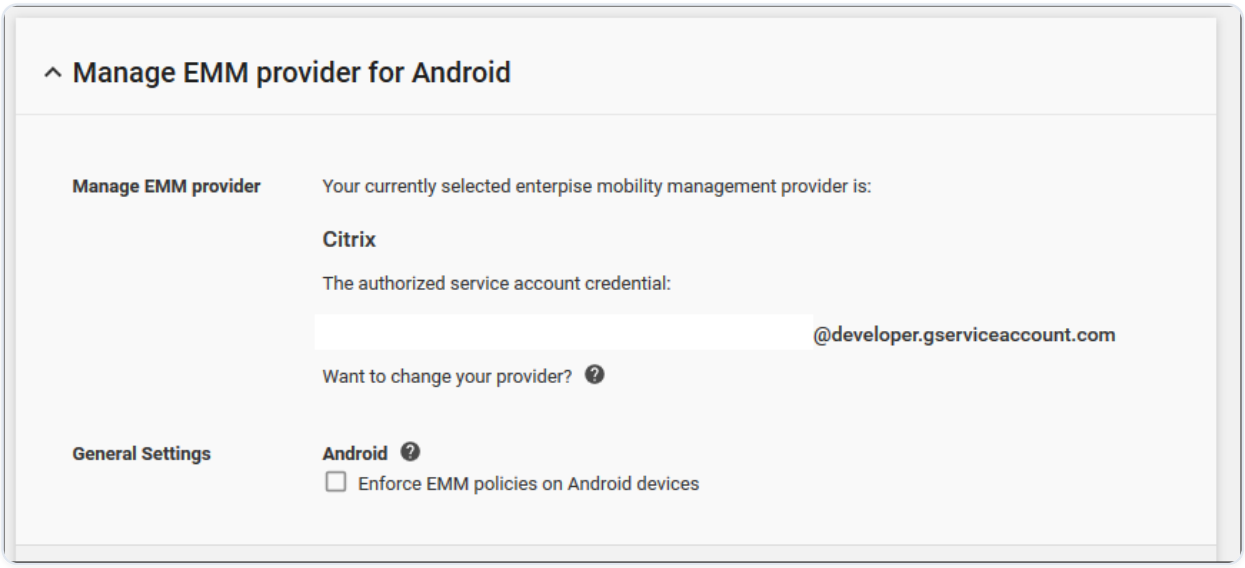
Citrix Endpoint Managementを使用してAndroidデバイスを管理する前に、Citrixテクニカルサポートに連絡し、ドメイン名、サービスアカウント、およびバインドトークンを提供する必要があります。Citrixは、エンタープライズモビリティ管理（EMM）プロバイダーとして、そのトークンをCitrix Endpoint Managementにバインドします。Citrixテクニカルサポートの連絡先については、Citrixテクニカルサポートを参照してください。

1. バインドを確認するには、Google管理ポータルにサインインし、「**セキュリティ**」をクリックします。
2. 「**Android用EMMプロバイダーを管理**」をクリックします。

   Google Android EnterpriseアカウントがEMMプロバイダーとしてCitrixにバインドされていることがわかります。

   トークンのバインドを確認したら、Citrix Endpoint Managementコンソールを使用してAndroidデバイスの管理を開始できます。手順14で生成したP12証明書をインポートします。Android Enterpriseサーバー設定をセットアップし、SAMLベースのシングルサインオン（SSO）を有効にし、少なくとも1つのAndroid Enterpriseデバイスポリシーを定義します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



P12証明書をインポートする

Android Enterprise P12証明書をインポートするには、次の手順に従います。

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックして、**設定**ページを開き、**証明書**をクリックします。**証明書**ページが表示されます。

   証明書ページ(/en-us/citrix-endpoint-management/media/android-enterprise-certs-import.png)

2. **インポート**をクリックします。**インポート**ダイアログボックスが表示されます。

   インポートダイアログボックス(/en-us/citrix-endpoint-management/media/afw-import-certificate-detail.png)

   次の設定を構成します。

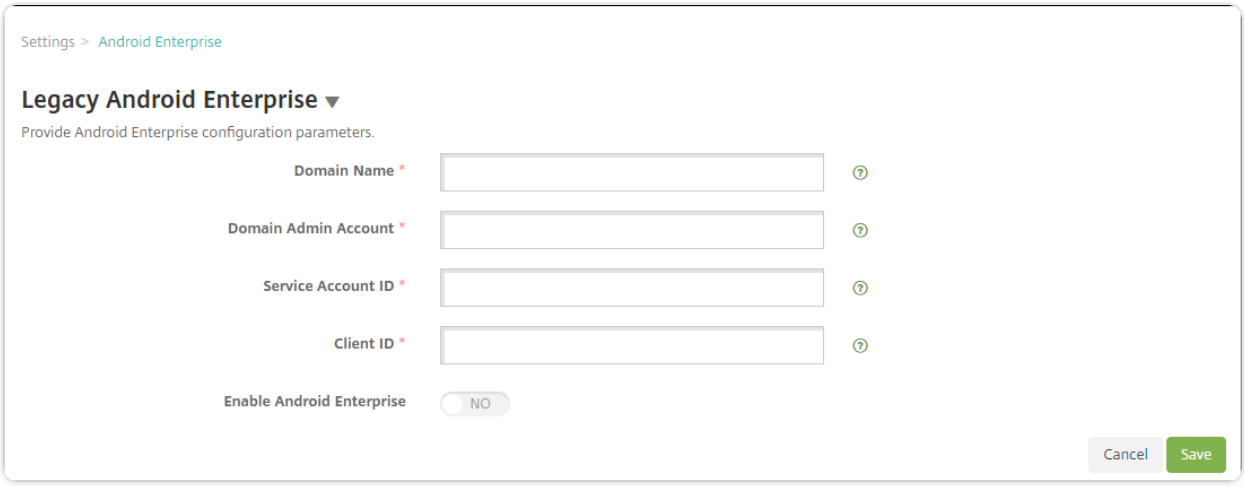
   - **インポート:** ドロップダウンリストで**キーストア**をクリックします。
   - **キーストアの種類:** ドロップダウンリストで**PKCS#12**をクリックします。
   - **用途:** ドロップダウンリストで**サーバー**をクリックします。
   - **キーストアファイル: 参照**をクリックして、P12証明書に移動します。
   - **パスワード:** 証明書のパスワードを入力します。このパスワードは、Android Enterpriseアカウントを設定したときに作成した秘密鍵のパスワードです。
   - **説明:** 必要に応じて、証明書の説明を入力します。

3. **インポート**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android Enterpriseサーバー設定をセットアップする

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. 「**プラットフォーム**」で、「**Android Enterprise**」をクリックします。「**Android Enterprise**」ページが表示されます。



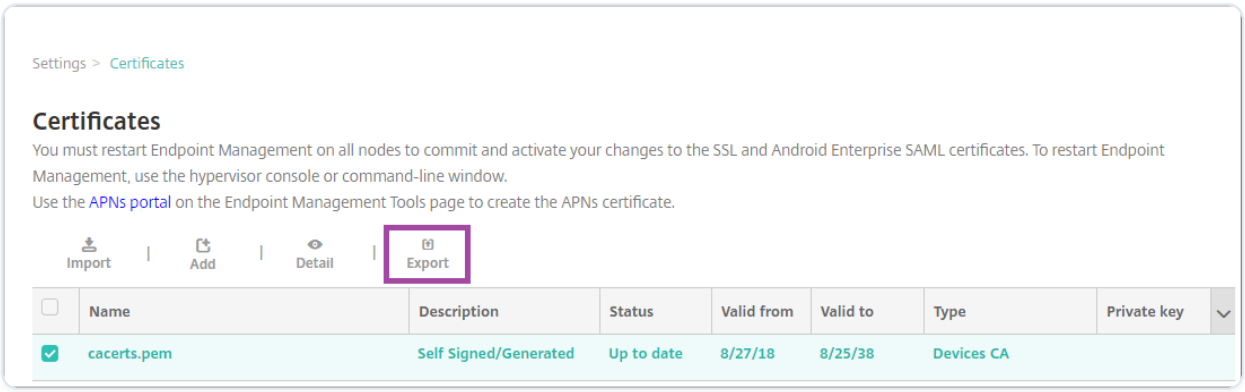
次の設定を構成し、「**保存**」をクリックします。

- **ドメイン名:** Android Enterpriseのドメイン名を入力します。例: domain.com。
- **ドメイン管理者アカウント:** ドメイン管理者のユーザー名を入力します。例: Google Developer Portalで使用されているメールアカウント。
- **サービスアカウントID:** サービスアカウントIDを入力します。例: Googleサービスアカウントに関連付けられているメールアドレス (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`)。
- **クライアントID:** Googleサービスアカウントの数値クライアントIDを入力します。
- **Android Enterpriseを有効にする:** Android Enterpriseを有効または無効にするには、これを選択します。

SAMLベースのシングルサインオンを有効にする

1. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。「**設定**」ページが表示されます。
2. 「**証明書**」をクリックします。「**証明書**」ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 証明書の一覧で、SAML証明書をクリックします。
4. 「**エクスポート**」をクリックし、証明書をコンピューターに保存します。
5. Android Enterprise管理者資格情報を使用してGoogle管理ポータルにサインインします。ポータルへのアクセスについては、Google管理ポータルを参照してください。
6. 「**セキュリティ**」をクリックします。

   セキュリティオプション(/en-us/citrix-endpoint-management/media/afw-admin-console-security-1.png)
7. 「**セキュリティ**」の下で、「**シングルサインオン (SSO) の設定**」をクリックし、次の設定を構成します。

   SSO設定(/en-us/citrix-endpoint-management/media/afw-sso-settings.png)

   - **サインインページURL:** システムおよびGoogle Appsにサインインするユーザーの URLを入力します。例: `https://<Xenmobile-FQDN>/aw/saml/signin`。
   - **サインアウトページURL:** ユーザーがサインアウトしたときにリダイレクトされるURLを入力します。例: `https://<Xenmobile-FQDN>/aw/saml/signout`。
   - **パスワード変更URL:** ユーザーがシステムでパスワードを変更するためのURLを入力します。例: `https://<Xenmobile-FQDN>/aw/saml/changepassword`。このフィールドが定義されている場合、SSOが利用できない場合でも、ユーザーにはこのプロンプトが表示されます。
   - **検証証明書:** 「**ファイルを選択**」をクリックし、Citrix Endpoint Managementからエクスポートされた SAML証明書に移動します。
8. 「**変更を保存**」をクリックします。

Android Enterpriseデバイスポリシーを設定する

ユーザーが最初に登録するときにデバイスにパスコードを設定する必要があるように、パスコードポリシーを設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パスコードポリシーページ(/en-us/citrix-endpoint-management/media/android-enterprise-passcode.png)

デバイスポリシーを設定するための基本的な手順は次のとおりです。

1. Citrix Endpoint Managementコンソールで、「**構成**」をクリックし、次に「**デバイスポリシー**」をクリックします。
2. 「**追加**」をクリックします。
3. **新しいポリシーの追加**ダイアログボックスで、追加するポリシーを選択します。この例では、**パスコード**をクリックします。
4. **ポリシー情報**ページを完了します。
5. **Android Enterprise**をクリックし、ポリシーの設定を構成します。
6. ポリシーをデリバリーグループに割り当てます。

Android Enterpriseアカウント設定を構成する

デバイスでAndroidアプリとポリシーの管理を開始する前に、Citrix Endpoint ManagementでAndroid Enterpriseドメインとアカウント情報を設定する必要があります。まず、GoogleでAndroid Enterpriseのセットアップタスクを完了し、ドメイン管理者を設定して、サービスアカウントIDとバインディングトークンを取得します。

1. Citrix Endpoint Management Webコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **プラットフォーム**の下で、**Android Enterprise**をクリックします。**Android Enterprise**構成ページが表示されます。

Android Enterprise構成ページ(/en-us/citrix-endpoint-management/media/android-enterprise-legacy-settings.png)

1. **Android Enterprise**ページで、次の設定を構成します。
   - **ドメイン名:** ドメイン名を入力します。
   - **ドメイン管理者アカウント:** ドメイン管理者のユーザー名を入力します。
   - **サービスアカウントID:** Googleサービスアカウントを入力します。
   - **クライアントID:** Googleサービスアカウントのクライアントを入力します。
   - **Android Enterpriseを有効にする:** Android Enterpriseを有効にするかどうかを選択します。
2. **保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management向けGoogle Workspaceパートナーアクセスを設定する

Chrome向けCitrix Endpoint Managementの一部の機能は、Citrix Endpoint ManagementとGoogle Workspaceドメイン間の通信にGoogleパートナーAPIを使用します。たとえば、Citrix Endpoint Managementは、シークレットモードやゲストモードなどのChrome機能を管理するデバイスポリシーにAPIを必要とします。

パートナーAPIを有効にするには、Citrix Endpoint Managementコンソールで Google Workspaceドメインを設定し、その後Google Workspaceアカウントを設定します。

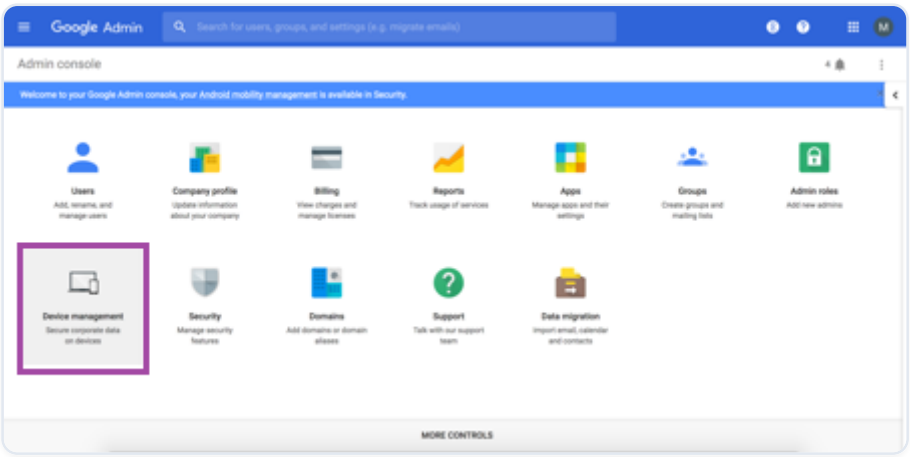
Citrix Endpoint ManagementでGoogle Workspaceドメインを設定する

Citrix Endpoint ManagementがGoogle Workspaceドメイン内のAPIと通信できるようにするには、**設定 > Google Chrome構成**に移動し、設定を構成します。

- **Google Workspaceドメイン:** Citrix Endpoint Managementが必要とするAPIをホストするGoogle Workspaceドメイン。
- **Google Workspace管理者アカウント:** Google Workspaceドメインの管理者アカウント。
- **Google WorkspaceクライアントID:** CitrixのクライアントID。この値を使用して、Google Workspaceドメインのパートナーアクセスを設定します。
- **Google Workspaceエンタープライズ ID:** Googleエンタープライズアカウントから入力される、アカウントのエンタープライズID。

Google Workspaceドメイン内のデバイスとユーザー向けパートナーアクセスを有効にする

1. Google管理コンソールにログインします: `<https://admin.google.com>`
2. **デバイス管理**をクリックします。



3. **Chrome管理**をクリックします。

「Google 管理者コンソール」(/en-us/citrix-endpoint-management/media/google-admin-partner-access2.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「**ユーザー設定**」をクリックします。

   「Google 管理者コンソール」(/en-us/citrix-endpoint-management/media/google-admin-partner-access3.png)

5. 「**Chrome Management - Partner Access**」を検索します。

   「Google 管理者コンソール」(/en-us/citrix-endpoint-management/media/google-admin-partner-access4.png)

6. 「**Chrome Management - Partner Access を有効にする**」チェックボックスをオンにします。
7. パートナーアクセスを理解し、有効にすることに同意します。「**保存**」をクリックします。
8. Chrome 管理ページで、「**デバイス設定**」をクリックします。

   「Google 管理者コンソール」(/en-us/citrix-endpoint-management/media/google-admin-partner-access5.png)

9. 「**Chrome Management - Partner Access**」を検索します。

   「Google 管理者コンソール」(/en-us/citrix-endpoint-management/media/google-admin-partner-access6.png)

10. 「**Chrome Management - Partner Access を有効にする**」チェックボックスをオンにします。
11. パートナーアクセスを理解し、有効にすることに同意します。「**保存**」をクリックします。
12. 「**セキュリティ**」ページに移動し、「**詳細設定**」をクリックします。

    「Google 管理者コンソール」(/en-us/citrix-endpoint-management/media/google-admin-partner-access7.png)

13. 「**Manage API client Access**」をクリックします。
14. Citrix Endpoint Management コンソールで、 **>** に移動し、G Suite クライアント ID の値をコピーします。次に、 ページに戻り、コピーした値を フィールドに貼り付けます。
15. で、次の URL を追加します: `https://www.googleapis.com/auth/chromedevicemanagementapi`

    Google 管理者コンソール(/en-us/citrix-endpoint-management/media/google-admin-partner-access8.png)

16. 「**Authorize**」をクリックします。

    「設定が保存されました」というメッセージが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android Enterprise デバイスの登録

デバイス登録プロセスでユーザーがユーザー名またはユーザー ID を入力する必要がある場合、受け入れられる形式は、Citrix Endpoint Management サーバーがユーザーをユーザープリンシパル名 (UPN) または SAM アカウント名で検索するように構成されている方法によって異なります。

Citrix Endpoint Management サーバーが UPN でユーザーを検索するように構成されている場合、ユーザーは次の形式で UPN を入力する必要があります。

- *ユーザー名@ ドメイン*

Citrix Endpoint Management サーバーが SAM でユーザーを検索するように構成されている場合、ユーザーは次のいずれかの形式で SAM を入力する必要があります。

- *ユーザー名@ ドメイン*
- *domain\username*

Citrix Endpoint Management サーバーがどの種類のユーザー名に構成されているかを判断するには：

1. Citrix Endpoint Management サーバーコンソールで、右上隅にある歯車アイコンをクリックします。 ページが表示されます。
2. 「**LDAP**」をクリックして、LDAP接続の構成を表示します。
3. ページの下部にある「**User search by**」フィールドを表示します。
    - 「**userPrincipalName**」に設定されている場合、Citrix Endpoint Managementサーバーは UPN用に設定されています。
    - 「**sAMAccountName**」に設定されている場合、Citrix Endpoint Managementサーバーは SAM用に設定されています。

Android Enterpriseエンタープライズの登録解除

Citrix Endpoint ManagementサーバーコンソールとCitrix Endpoint Management Toolsを使用して、Android Enterpriseエンタープライズの登録を解除できます。

このタスクを実行すると、Citrix Endpoint ManagementサーバーはCitrix Endpoint Management Toolsのポップアップウィンドウを開きます。開始する前に、Citrix Endpoint Managementサーバーが使用しているブラウザでポップアップウィンドウを開く権限を持っていることを確認してください。Google Chromeなどの一部のブラウザでは、ポップアップブロックを無効にし、Citrix Endpoint Managementサイトのアドレスをポップアップ許可リストに追加する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

警告:

エンタープライズの登録が解除されると、そのエンタープライズを通じてすでに登録されているデバイス上のAndroid Enterpriseアプリは、デフォルトの状態にリセットされます。デバイスはGoogleによって管理されなくなります。Android Enterpriseエンタープライズに再登録しても、追加の構成なしでは以前の機能が復元されない場合があります。

Android Enterpriseエンタープライズの登録が解除された後:

- エンタープライズを通じて登録されたデバイスとユーザーは、Android Enterpriseアプリがデフォルトの状態にリセットされます。以前に適用されたアプリの権限と管理対象構成ポリシーは、もはや効果がありません。
- エンタープライズを通じて登録されたデバイスはCitrix Endpoint Managementによって管理されますが、Googleの観点からは管理対象外となります。新しいAndroid Enterpriseアプリを追加することはできません。アプリの権限や管理対象構成ポリシーを適用することもできません。スケジューリング、パスワード、制限などの他のポリシーは、これらのデバイスに引き続き適用できます。
- Android Enterpriseにデバイスを登録しようとすると、それらはAndroid Enterpriseデバイスではなく、Androidデバイスとして登録されます。

Android Enterpriseエンタープライズの登録を解除するには:

1. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。「設定」ページが表示されます。
2. 「設定」ページで、**Android Enterprise** をクリックします。
3. **Remove Enterprise** をクリックします。

   Remove Enterprise オプション(/en-us/citrix-endpoint-management/media/android-enterprise-remove-ent.png)
4. パスワードを指定します。このパスワードは、次の手順で登録解除を完了するために必要です。次に、**Unenroll** をクリックします。

   Unenroll オプション(/en-us/citrix-endpoint-management/media/android-enterprise-unenroll1.png)
5. Citrix Endpoint Management Tools ページが開いたら、前の手順で作成したパスワードを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パスワードフィールド(/en-us/citrix-endpoint-management/media/android-enterprise-unenroll2.png)

6. **Unenroll** をクリックします。

   Unenroll オプション(/en-us/citrix-endpoint-management/media/android-enterprise-unenroll3.png)

Android Enterprise での完全管理対象デバイスのプロビジョニング

Android Enterprise では、会社所有のデバイスのみが完全管理対象デバイスとなります。完全管理対象デバイスでは、仕事用プロファイルだけでなく、デバイス全体が会社または組織によって制御されます。完全管理対象デバイスは、仕事用管理対象デバイスとも呼ばれます。

Citrix Endpoint Management は、完全管理対象デバイスの登録に次の方法をサポートしています。

- **afw#xenmobile:** この登録方法では、デバイスのセットアップ時にユーザーが `afw#xenmobile` の文字を入力します。このトークンは、デバイスが Citrix Endpoint Management によって管理されていることを識別し、Citrix Secure Hub をダウンロードします。
- **QRコード:** QRコードプロビジョニングは、タブレットなどNFCをサポートしない分散型デバイス群をプロビジョニングする簡単な方法です。QRコード登録方法は、工場出荷時の設定にリセットされたデバイス群で使用できます。QRコード登録方法は、セットアップウィザードからQRコードをスキャンすることで、完全管理対象デバイスをセットアップおよび構成します。
- **近距離無線通信 (NFC) バンプ:** NFCバンプ登録方法は、工場出荷時の設定にリセットされたデバイス群で使用できます。NFCバンプは、近距離無線通信を使用して2つのデバイス間でデータを転送します。工場出荷時の設定にリセットされたデバイスでは、Bluetooth、Wi-Fi、その他の通信モードは無効になります。NFCは、この状態でデバイスが使用できる唯一の通信プロトコルです。

`afw#xenmobile`

新しいデバイスまたは工場出荷時設定にリセットされたデバイスの初期設定後、登録方法が使用されます。ユーザーは、Googleアカウントの入力を求められたときに `afw#xenmobile` を入力します。この操作により、Citrix Secure Hubがダウンロードおよびインストールされます。その後、ユーザーはCitrix Secure Hubのセットアッププロンプトに従って登録を完了します。

Citrix Secure Hubの最新バージョンはGoogle Playストアからダウンロードされるため、この登録方法はほとんどのお客様に推奨されます。他の登録方法とは異なり、Citrix Endpoint Management サーバーからCitrix Secure Hubをダウンロード用に提供する必要はありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件:

- Android OSを実行しているすべてのAndroidデバイスでサポートされています。

QRコード

QRコードを使用してデバイスモードでデバイスを登録するには、JSONを作成し、そのJSONをQRコードに変換してQRコードを生成します。デバイスのカメラがQRコードをスキャンしてデバイスを登録します。

前提条件:

- Android 7.0以降を実行しているすべてのAndroidデバイスでサポートされています。

JSONからQRコードを作成する

次のフィールドを含むJSONを作成します。

これらのフィールドは必須です。

キー: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

値: com.zenprise/com.zenprise.configuration.AdminFunction

キー: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

値: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

キー: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

値: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

これらのフィールドはオプションです:

- **android.app.extra.PROVISIONING_LOCALE:** 言語コードと国コードを入力します。

  言語コードは、ISO 639-1 で定義されている2文字の小文字のISO言語コード（enなど）です。国コードは、ISO 3166-1 で定義されている2文字の大文字のISO国コード（USなど）です。たとえば、米国で話されている英語の場合は en_US と入力します。
- **android.app.extra.PROVISIONING_TIME_ZONE:** デバイスが実行されているタイムゾーン。

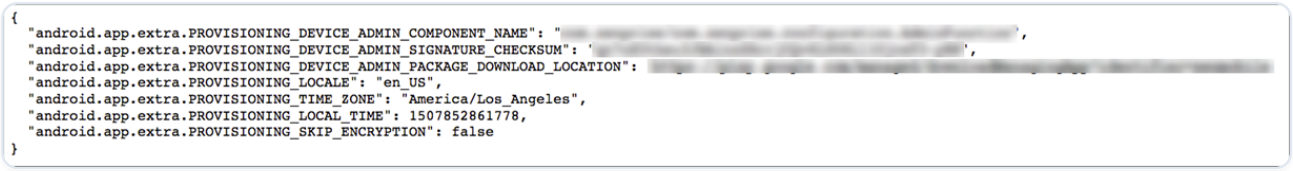
  エリア/場所のデータベース名 を入力します。たとえば、太平洋時間の場合は **America/Los_Angeles** と入力します。名前を入力しない場合、タイムゾーンは自動的に入力されます。
- **android.app.extra.PROVISIONING_LOCAL_TIME:** エポックからのミリ秒単位の時間。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unixエポック（またはUnix時間、POSIX時間、Unixタイムスタンプ）は、January 1, 1970（UTC/GMTの深夜）から経過した秒数です。この時間には閏秒は含まれません（ISO 8601では: 1970-01-01T00:00:00Z）。

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** プロファイル作成時に暗号化をスキップするには **true** に設定します。プロファイル作成時に暗号化を強制するには **false** に設定します。

一般的なJSONは次のようになります:



作成されたJSONは、https://jsonlint.com などのJSON検証ツールを使用して検証します。そのJSON文字列をオンラインQRコードジェネレーターを使用してQRコードに変換します。

このQRコードは、工場出荷時設定にリセットされたデバイスによってスキャンされ、デバイスを完全に管理されたデバイスとして登録します。

デバイスを登録するには

デバイスを完全管理デバイスとして登録するには、デバイスが工場出荷時の状態である必要があります。

1. ようこそ画面で画面を6回タップし、QRコード登録フローを起動します。
2. プロンプトが表示されたら、Wi-Fiに接続します。QRコード（JSONにエンコードされています）内のCitrix Secure Hubのダウンロード場所は、このWi-Fiネットワーク経由でアクセスできます。

   デバイスがWi-Fiに正常に接続すると、GoogleからQRコードリーダーをダウンロードし、カメラを起動します。
3. カメラをQRコードに向け、コードをスキャンします。

   Androidは、QRコード内のダウンロード場所からCitrix Secure Hubをダウンロードし、署名証明書の署名を検証し、Citrix Secure Hubをインストールして、デバイス所有者として設定します。

QRコード方式を使用したデバイスのプロビジョニングの詳細については、Android EMM 開発者向け Google API ドキュメント を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NFCバンプ

NFCバンプを使用してデバイスを完全管理デバイスとして登録するには、2つのデバイスが必要です。1つは工場出荷時の設定にリセットされたデバイス、もう1つはCitrix Endpoint Management Provisioning Toolを実行しているデバイスです。

前提条件:

- サポートされているAndroidデバイス
- Android Enterprise向けに有効化されたCitrix Endpoint Management
- Android Enterprise向けに完全管理デバイスとしてプロビジョニングされた、新規または工場出荷時設定にリセットされたデバイス。この前提条件を完了するための手順は、この記事の後半で確認できます。
- NFC機能を備え、構成済みのProvisioning Toolを実行している別のデバイス。Provisioning Toolは、Citrix Secure HubまたはCitrixダウンロードページで入手できます。

各デバイスには、企業モビリティ管理 (EMM) アプリによって管理されるAndroid Enterpriseプロファイルを1つだけ設定できます。Citrix Endpoint Managementでは、Citrix Secure HubがEMMアプリです。各デバイスで許可されるプロファイルは1つだけです。2つ目のEMMアプリを追加しようとすると、最初のEMMアプリが削除されます。

NFCバンプを介して転送されるデータ

初期化されたデバイスをプロビジョニングするには、Android Enterpriseを初期化するために、NFCバンプを介して以下のデータを送信する必要があります。

- デバイス所有者として機能するEMMプロバイダーアプリのパッケージ名（この場合、Citrix Secure Hub）。
- デバイスがEMMプロバイダーアプリをダウンロードできるイントラネット/インターネットの場所。
- ダウンロードが成功したかどうかを確認するためのEMMプロバイダーアプリのSHA-256ハッシュ。
- 初期化されたデバイスがEMMプロバイダーアプリに接続してダウンロードできるようにするためのWi-Fi接続の詳細。注：現在、Androidはこのステップで802.1x Wi-Fiをサポートしていません。
- デバイスのタイムゾーン（オプション）。
- デバイスの地理的位置（オプション）。

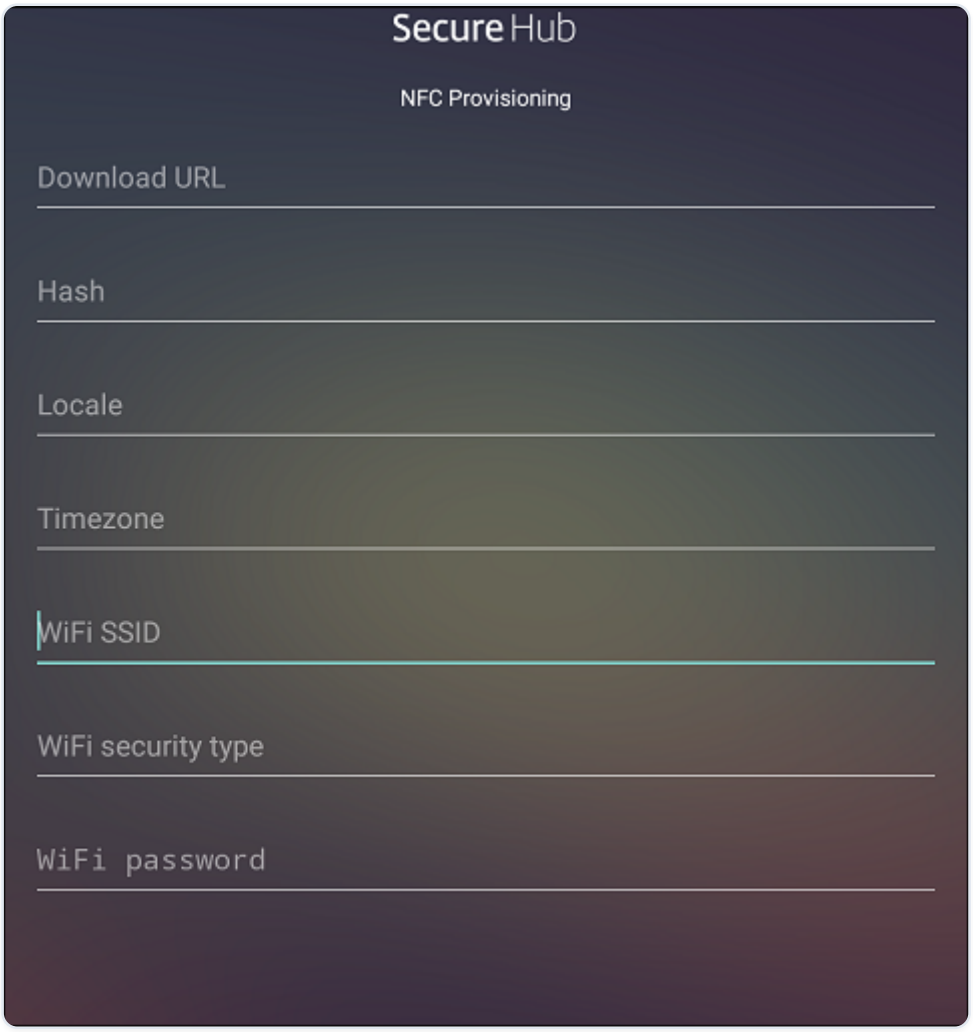
2つのデバイスがバンプされると、プロビジョニングツールからのデータが初期化されたデバイスに送信されます。そのデータは、管理者設定でCitrix Secure Hubをダウンロードするために使用さ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

れます。タイムゾーンと位置情報を入力しない場合、Androidは新しいデバイスで値を自動的に構成します。

CITRIX ENDPOINT MANAGEMENTプロビジョニングツールの構成

NFCバンプを行う前に、プロビジョニングツールを構成する必要があります。この構成は、NFCバンプ中に初期化されたデバイスに転送されます。



必須フィールドにデータを入力するか、テキストファイルを介してデータを入力できます。次の手順では、テキストファイルの構成方法と各フィールドの説明について説明します。アプリは入力後に情報を保存しないため、将来の使用のために情報を保持するためにテキストファイルを作成することをお勧めします。

テキストファイルを使用してプロビジョニングツールを構成するには

ファイル名を nfcprovisioning.txt にして、デバイスのSDカードの **/sdcard/** フォルダーにファイルを配置します。アプリはテキストファイルを読み取り、値を入力できます。

テキストファイルには、次のデータが必要です。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

この行は、EMMプロバイダーアプリのイントラネット/インターネットの場所です。NFCバンプ後に工場出荷時設定にリセットされたデバイスがWi-Fiに接続した後、デバイスはダウンロードのためにこの場所にアクセスできる必要があります。URLは通常のURLであり、特別な書式設定は必要ありません。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>`

この行は、EMMプロバイダーアプリのチェックサムです。このチェックサムは、ダウンロードが成功したことを確認するために使用されます。チェックサムを取得する手順については、この記事の後半で説明します。

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

この行は、プロビジョニングツールが実行されているデバイスの接続済みWi-Fi SSIDです。

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

サポートされている値はWEPとWPA2です。Wi-Fiが保護されていない場合、このフィールドは空にする必要があります。

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

Wi-Fiが保護されていない場合、このフィールドは空にする必要があります。

`android.app.extra.PROVISIONING_LOCALE=<locale>`

言語コードと国コードを入力します。言語コードは、ISO 639-1で定義されている2文字の小文字のISO言語コード（enなど）です。国コードは、ISO 3166-1で定義されている2文字の大文字のISO国コード（USなど）です。たとえば、米国で話されている英語の場合は「en_US」と入力します。コードを入力しない場合、国と言語は自動的に入力されます。

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

デバイスが実行されているタイムゾーンです。地域/場所のデータベース名を入力します。たとえば、太平洋時間の場合は**America/Los_Angeles**と入力します。名前を入力しない場合、タイムゾーンは自動的に入力されます。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

このデータは、値がCitrix Secure Hubとしてアプリにハードコードされているため、必須ではありません。ここでは、完全を期すためにのみ記載されています。

WPA2を使用して保護されたWi-Fiがある場合、完成したnfcprovisioning.txtファイルは次のようになります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name`

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2`

`android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere`

`android.app.extra.PROVISIONING_LOCALE=en_US`

`android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles`

保護されていないWi-Fiがある場合、完成したnfcprovisioning.txtファイルは次のようになります。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name`

`android.app.extra.PROVISIONING_LOCALE=en_US`

`android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles`

CITRIX SECURE HUB のチェックサムを取得するには

Citrix Secure Hub のチェックサムは定数値です: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`。Citrix Secure Hub の APK ファイルをダウンロードするには、次の Google Play ストアのリンクを使用してください: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`。

アプリのチェックサムを取得するには

前提条件:

- Android SDK ビルドツール の **apksigner** ツール
- OpenSSL コマンドライン

任意のアプリのチェックサムを取得するには、次の手順に従います。

1. Google Play ストアからアプリの APK ファイルをダウンロードします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. OpenSSL コマンドラインで、**apksigner** ツールに移動し: `android-sdk/build-tools/<version>/apksigner`、次のように入力します。

   ```
   apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{(?<=SHA-256 digest:) .*}'  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
   ```

   コマンドは有効なチェックサムを返します。

3. QR コードを生成するには、`PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM` フィールドにチェックサムを入力します。例:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",


"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUth
eu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?
identifier=xenmobile",

  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"

   }

}
```

使用されているライブラリ

プロビジョニングツールは、そのソースコードで以下のライブラリを使用しています。

- v7 `appcompat` ライブラリ、Design Support ライブラリ、および v7 パレットサポートライブラリ

  詳細については、Android developers documentation で「Support Library Features Guide」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Jake Wharton 著、Apache ライセンス 2.0 に基づく Butter Knife

Android Enterprise でのワークプロファイルデバイスのプロビジョニング

Android Enterprise のワークプロファイルデバイスでは、デバイス上の企業領域と個人領域を安全に分離します。たとえば、BYOD デバイスはワークプロファイルデバイスにすることができます。ワークプロファイルデバイスの登録エクスペリエンスは、Citrix Endpoint Management での Android 登録と似ています。ユーザーは Google Play から Citrix Secure Hub をダウンロードし、デバイスを登録します。

デフォルトでは、Android Enterprise にワークプロファイルデバイスとして登録されているデバイスでは、USB デバッグと不明なソースの設定は無効になっています。

ヒント:

Android Enterprise にデバイスをワークプロファイルデバイスとして登録する場合は、常に Google Play にアクセスしてください。そこから、Citrix Secure Hub がユーザーの個人プロファイルに表示されるように有効にします。

アンドロイドOS

注：

この記事は、Android Enterprise で管理されているデバイスには適用されません。これらのデバイスに関する情報については、このセクションの他の記事を参照してください。

Citrix Endpoint Management は、Android または Samsung のエンタープライズプログラムを通じて管理されていない Android OS デバイスもサポートしています。Android デバイスが Citrix Endpoint Management サービスに接続する方法とタイミングを制御するには、Firebase Cloud Messaging (FCM) を使用します。詳細については、Firebase Cloud Messaging を参照してください。

登録プロファイルは、Android デバイスが MAM、MDM、または MDM+MAM のいずれに登録されるかを決定し、ユーザーが MDM からオプトアウトするオプションを提供します。Citrix Endpoint Management は、MDM+MAM の Android デバイスに対して以下の認証タイプをサポートしています。詳細については、以下の記事を参照してください。

- ドメインまたはドメインとセキュリティトークン認証
- クライアント証明書または証明書とドメイン認証

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ID プロバイダー：
  - Citrix Cloud を介した Azure Active Directory による認証
  - Citrix Cloud を介した Okta による認証

もう1つのあまり使用されない認証方法は、クライアント証明書とセキュリティトークンです。詳細については、`<https://support.citrix.com/article/CTX215200>` を参照してください。

Android デバイス管理を開始するための一般的なワークフローは次のとおりです。

1. オンボーディングプロセスを完了します。オンボーディングとリソースのセットアップ および デバイスの登録とリソースの配信の準備 を参照してください。
2. 登録方法を選択して構成します。サポートされている登録方法 を参照してください。
3. Android デバイスポリシーの構成。
4. Androidデバイスを登録する。
5. デバイスとアプリのセキュリティアクションを設定します。詳しくは、セキュリティアクションを参照してください。

サポートされているオペレーティングシステムについては、サポートされているデバイスオペレーティングシステムを参照してください。

サポートされている登録方法

次の表に、Citrix Endpoint ManagementがAndroidデバイスでサポートする登録方法を示します。

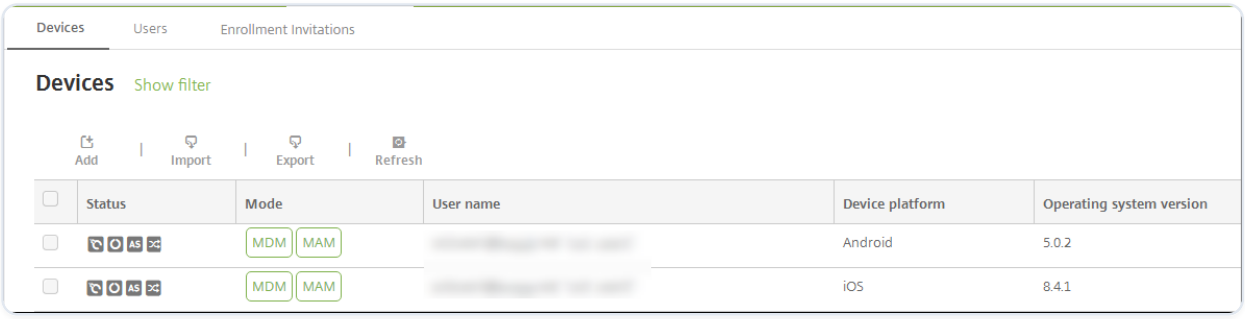
方法	サポート
一括登録	いいえ
手動登録	はい
登録招待	はい

Androidデバイスを手動で追加する

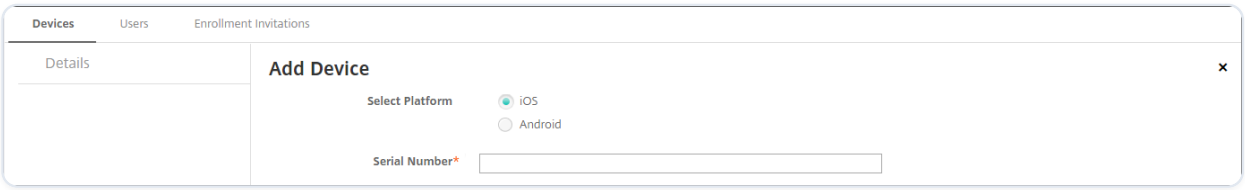
テスト目的などでAndroidまたはiOSデバイスを手動で追加する場合は、次の手順に従ってください。

1. Citrix Endpoint Managementコンソールで、**管理 > デバイス**をクリックします。**デバイス**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. **追加**をクリックします。**デバイスの追加**ページが表示されます。



3. 次の設定を構成します。

   - **プラットフォームの選択: Android**をクリックします。
   - **シリアル番号:** デバイスのシリアル番号を入力します。
   - **IMEI/MEID:** 必要に応じて、デバイスのIMEI/MEID情報を入力します。

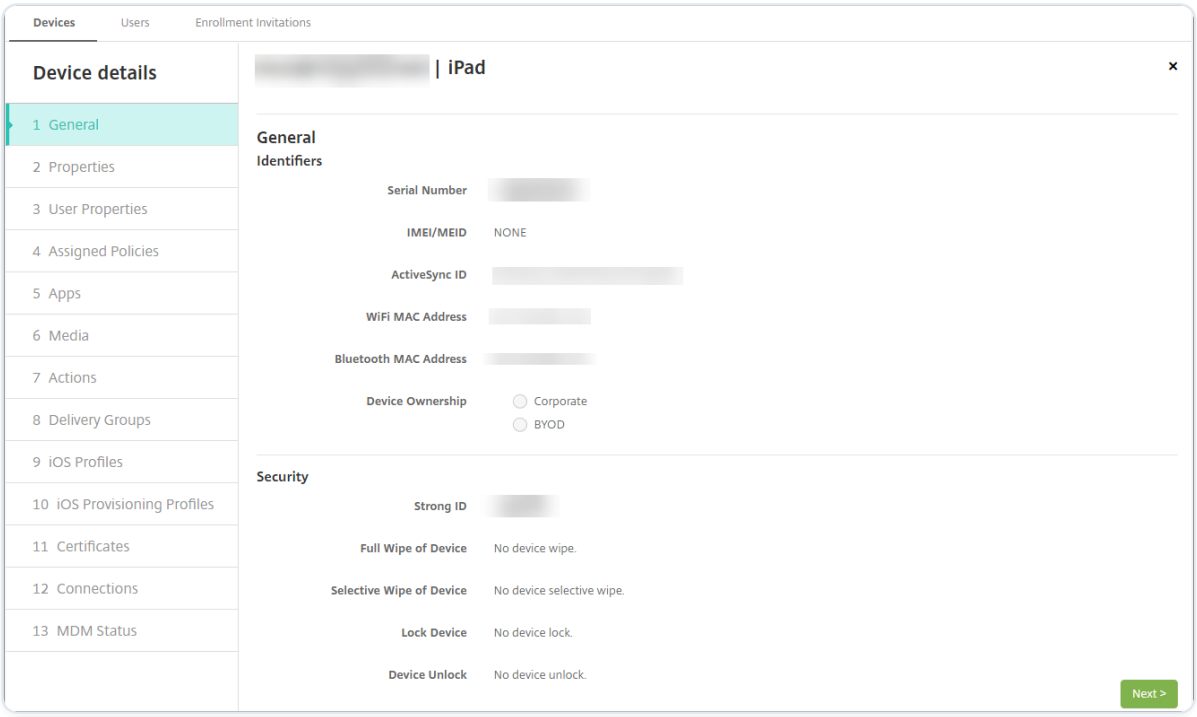
4. **追加**をクリックします。**デバイス**テーブルが表示され、デバイスがリストの一番下に追加されます。デバイスの詳細を表示して確認するには、追加したデバイスを選択し、表示されるメニューで**編集**をクリックします。

   注:

   デバイスの横にあるチェックボックスを選択すると、オプションメニューがデバイスリストの上に表示されます。リスト内の他の場所をクリックすると、オプションメニューがリストの右側に表示されます。

   - LDAPが構成されている
   - ローカルグループとローカルユーザーを使用している場合:
     - 1つ以上のローカルグループ。
     - ローカルグループに割り当てられたローカルユーザー。
     - デリバリーグループはローカルグループに関連付けられています。
   - Active Directoryを使用している場合：
     - デリバリーグループはActive Directoryグループに関連付けられています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. **全般**ページには、シリアル番号やプラットフォームタイプに関するその他の情報など、デバイスの**識別子**が一覧表示されます。**デバイスの所有権**については、**企業所有**または**BYOD**を選択します。

   全般ページには、Strong ID、デバイスのロック、アクティベーションロックバイパスなど、プラットフォームタイプに関するその他の情報など、デバイスの**セキュリティ**プロパティも一覧表示されます。**デバイスの完全ワイプ**フィールドには、ユーザーのPINコードが含まれています。デバイスがワイプされた後、ユーザーはそのコードを入力する必要があります。ユーザーがコードを忘れた場合は、ここで確認できます。

6. **プロパティ**ページには、Citrix Endpoint Managementがプロビジョニングするデバイスプロパティが一覧表示されます。このリストには、デバイスの追加に使用されたプロビジョニングファイルに含まれるすべてのデバイスプロパティが表示されます。プロパティを追加するには、**追加**をクリックし、リストからプロパティを選択します。各プロパティの有効な値については、PDF「デバイスプロパティ名と値」を参照してください。

   プロパティを追加すると、最初に追加したカテゴリの下に表示されます。**次へ**をクリックして**プロパティ**ページに戻ると、プロパティは適切なリストに表示されます。

   プロパティを削除するには、リストにカーソルを合わせ、右側の**X**をクリックします。Citrix Endpoint Managementはすぐに項目を削除します。

7. 残りの**デバイス詳細**セクションには、デバイスの概要情報が含まれています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ユーザープロパティ:** RBACロール、グループメンバーシップ、管理対象Google Playアカウント、およびユーザーのプロパティを表示します。このページから管理対象Google Playアカウントを廃止できます。
- **割り当て済みポリシー:** 展開済み、保留中、失敗したポリシーの数を表示します。各ポリシーのポリシー名、種類、最終展開情報を提供します。展開ステータスを保留中にリセットし、ユーザーが削除したポリシーを再展開できます。
- **アプリ:** 最後のインベントリについて、インストール済み、保留中、失敗したアプリ展開の数を表示します。アプリ名、識別子、種類、およびその他の情報を提供します。**HasUpdateAvailable**などのiOSおよびmacOSインベントリキーの説明については、「モバイルデバイス管理（MDM）プロトコル」を参照してください。
- **メディア:** 最後のインベントリについて、展開済み、保留中、失敗したメディア展開の数を表示します。
- **アクション:** 展開済み、保留中、失敗したアクションの数を表示します。アクション名と最終展開時刻を提供します。
- **デリバリーグループ:** 成功、保留中、失敗したデリバリーグループの数を表示します。各展開について、デリバリーグループ名と展開時間を提供します。デリバリーグループを選択すると、ステータス、アクション、チャネルまたはユーザーを含む詳細情報が表示されます。
- **iOSプロファイル:** 名前、種類、組織、説明を含む、最新のiOSプロファイルインベントリを表示します。
- **iOSプロビジョニングプロファイル:** UUID、有効期限、管理ステータスなどのエンタープライズ配布プロビジョニングプロファイル情報を表示します。
- **証明書:** 有効、期限切れ、または失効した証明書について、種類、プロバイダー、発行者、シリアル番号、有効期限までの残り日数などの情報を表示します。
- **接続:** 最初の接続ステータスと最後の接続ステータスを表示します。各接続について、ユーザー名、最後から2番目の認証時間、および最後の認証時間を提供します。
- **MDMステータス:** MDMステータス、最終プッシュ時間、最終デバイス応答時間などの情報を表示します。

Androidデバイスポリシーを構成する

これらのポリシーを使用して、Citrix Endpoint ManagementがAndroidを実行しているデバイスとどのように連携するかを構成します。この表には、Androidデバイスで利用可能なすべてのデバイスポリシーが一覧表示されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APN	アプリのアクセス	アプリのインベントリ
アプリのロック	アプリのアンインストール	資格情報
Citrix Endpoint Management オプション	Citrix Endpoint Management アンインストール	ファイル
ランチャー構成	位置情報	ネットワーク
パスコード	制限	スケジュール
ストア	利用規約	トンネル
VPN	Webクリップ	

Androidデバイスを登録する

1. AndroidデバイスでGoogle Playストアにアクセスし、Citrix Secure Hubアプリをダウンロードして、アプリをタップします。
2. アプリのインストールを求められたら、**次へ**をクリックし、**インストール**をクリックします。
3. Citrix Secure Hubのインストール後、**開く**をタップします。
4. Android 6.0以降を実行しているデバイスの場合、必要な権限を承認します。
   - Citrix Secure Hubに電話の発信と管理を許可しますか？（必須）
   - Citrix Secure Hubにデバイス上の写真、メディア、ファイルへのアクセスを許可しますか？（必須）
   - Citrix Secure Hubにこのデバイスの位置情報へのアクセスを許可しますか？（任意）
5. Citrix Endpoint Managementサーバー名、ユーザープリンシパル名（UPN）、またはメールアドレスなどの企業資格情報を入力します。次に、**次へ**をクリックします。
6. デバイスの登録方法を選択します。
   - MDM+MAMに登録するには、**はい、登録します**をタップします。
   - MAMに登録するには、**いいえ**をタップします。
7. **デバイス管理者を有効にする**画面で、**有効にする**をタップします。
8. 企業パスワードを入力し、**サインオン**をタップします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Citrix Endpoint Managementの構成方法によっては、Citrix PINの作成を求められる場合があります。このPINは、Citrix Secure Hubや、Citrix Secure Mail、Citrix FilesなどのCitrix Endpoint Management対応アプリにサインオンするために使用できます。Citrix PINは2回入力します。**Citrix PINの作成**画面で、PINを入力します。
10. PINを再入力します。Citrix Secure Hubが開きます。その後、アプリストアにアクセスして、Androidデバイスにインストールできるアプリを表示できます。
11. Citrix Endpoint Managementを構成して、登録後にアプリをデバイスに自動的にプッシュするように設定した場合、ユーザーはアプリのインストールを求められます。また、Citrix Endpoint Managementで構成したポリシーがデバイスに展開されます。アプリをインストールするには、**インストール**をタップします。

Androidデバイスの登録解除と再登録

ユーザーはCitrix Secure Hub内から登録解除できます。以下の手順でユーザーが登録解除しても、デバイスはCitrix Endpoint Managementコンソールのデバイスインベントリに表示されたままになります。ただし、デバイスに対してアクションを実行することはできません。たとえば、デバイスを追跡したり、デバイスのコンプライアンスを監視したりすることはできません。

1. Citrix Secure Hubアプリを開くにはタップします。
2. スマートフォンまたはタブレットのどちらをお持ちかによって、次の操作を行います。

   スマートフォンの場合:

   - 画面の左側からスワイプして設定ペインを開きます。
   - **Preferences**をタップし、**Accounts**をタップしてから、**Delete Account**をタップします。

   タブレットの場合:

   - 右上隅にあるメールアドレスの横の矢印をタップします。
   - **Preferences**をタップし、**Accounts**をタップしてから、**Delete Account**をタップします。

3. **Delete Account?**ウィンドウで、**Yes, delete**をタップします。 Citrix Secure Hubはデバイスの登録を解除します。画面の指示に従ってデバイスを再登録してください。

セキュリティアクション

Androidは次のセキュリティアクションをサポートしています。各セキュリティアクションの説明については、「セキュリティアクション」を参照してください。

アプリロック	アプリワイプ	証明書の更新

© 1997–2026 Citrix Systems, Inc. All rights reserved.

完全ワイプ	検索	ロック
ロックとパスワードのリセット	通知	失効
選択的ワイプ		

注:

Android 6.0以降を実行しているデバイスの場合、検索セキュリティアクションは、登録中にユーザーが位置情報権限を付与する必要があります。ユーザーは位置情報権限を付与しないことを選択できます。ユーザーが登録中に権限を付与しない場合、Citrix Endpoint Managementは、検索コマンドを送信するときに、再度位置情報権限を要求します。

Firebase クラウド メッセージング

注記:

Firebase Cloud Messaging (FCM) は、以前は Google Cloud Messaging (GCM) として知られていました。Citrix Endpoint Management コンソールの一部のラベルとメッセージでは、GCM の用語が使用されています。

Citrix では、Android デバイスが Citrix Endpoint Management に接続する方法とタイミングを制御するために、Firebase Cloud Messaging (FCM) を使用することをお勧めします。FCM 用に構成されている場合、Citrix Endpoint Management は、FCM が有効になっている Android デバイスに接続通知を送信します。セキュリティアクションまたは展開コマンドは、プッシュ通知をトリガーして、ユーザーに Citrix Endpoint Management サーバーへの再接続を促します。

この記事の構成手順を完了し、デバイスがチェックインすると、デバイスは Citrix Endpoint Management の FCM サービスに登録されます。この接続により、Citrix Endpoint Management サービスから FCM を使用してデバイスへのほぼリアルタイムの通信が可能になります。FCM 登録は、新規デバイス登録と以前に登録されたデバイスの両方で機能します。

Citrix Endpoint Management がデバイスへの接続を開始する必要がある場合、FCM サービスに接続します。その後、FCM サービスはデバイスに接続を通知します。この種類の接続は、Apple がプッシュ通知サービスに使用しているものと似ています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

- 最新の Citrix Secure Hub クライアント
- Google 開発者アカウントの資格情報
- FCM が有効な Android デバイスに Google Play サービスがインストールされていること

ファイアウォールポート

- Citrix Endpoint Management でポート 443 を `fcm.googleapis.com` および `Google.com` に開きます。
- デバイスの Wi-Fi 用に、ポート 5228、5229、および 5230 でインターネットへの送信通信を開きます。
- 送信接続を許可するために、FCM は IP 制限なしでポート 5228 から 5230 を許可リストに追加することを推奨しています。ただし、IP 制限が必要な場合は、FCM は IPv4 および IPv6 ブロック内のすべての IP アドレスを許可リストに追加することを推奨しています。これらのブロックは、Google の ASN of 15169 に記載されています。このリストは毎月更新してください。

詳細については、「ポート要件」を参照してください。

アーキテクチャ

この図は、外部ネットワークと内部ネットワークにおけるFCMの通信フローを示しています。

FCMアーキテクチャ](/en-us/citrix-endpoint-management/media/firebase-cloud-messaging-architecture.png)

FCM用にGoogleアカウントを設定するには

1. Google開発者アカウントの資格情報を使用して、次のURLにサインインします。

   `<https://console.firebase.google.com/>`

2. **Add project** をクリックします。

   プロジェクト作成オプション (/en-us/citrix-endpoint-management/media/firebase-cloud-messaging-create.png)

3. プロジェクトを作成したら、**Project settings** をクリックします。

   プロジェクト設定オプション (/en-us/citrix-endpoint-management/media/firebase-cloud-messaging-create-2.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

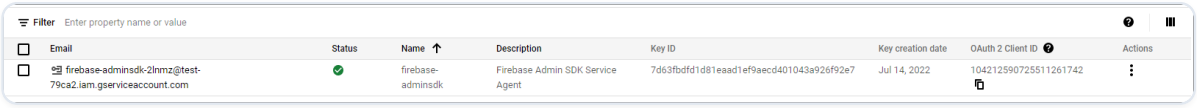
> **注:**
>
> Googleは、現在FCMの実装で使用されているHTTP用のFCMレガシーAPIを非推奨にする予定です。移行期限はJune 21, 2024です。FCMをレガシーFCM APIからHTTP v1 APIに移行する必要があります。詳細については、レガシーFCM APIからHTTP v1への移行を参照してください。

4. **Cloud Messaging** タブをクリックします。Firebase Cloud Messaging APIが有効になっていることを確認し、**Manage Service Accounts** をクリックします。

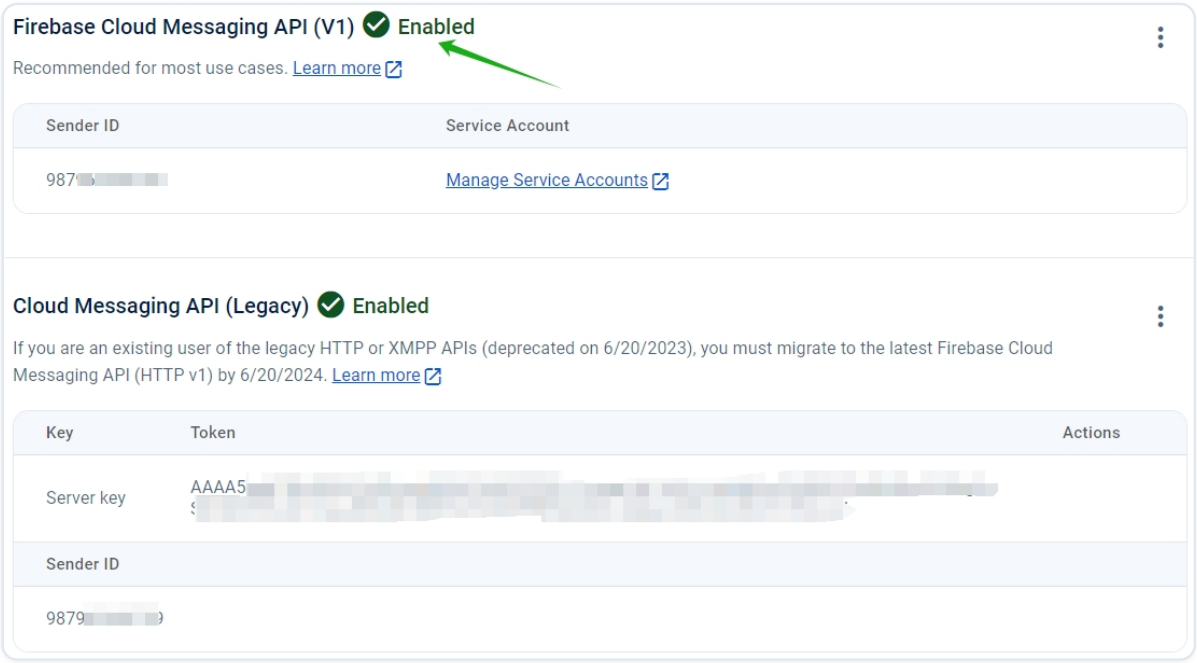
   a. 移行前はレガシーAPIを使用できたため、Cloud Messaging API (Legacy) が有効になっていることを確認してください。**Key** および **Sender ID** フィールドから値をコピーします。

   Cloud Messaging APIを有効にする (/en-us/citrix-endpoint-management/media/enable-legacy.png)

   キーがリストにない場合は、**Actions** の下の省略記号をクリックしてキーを追加します。



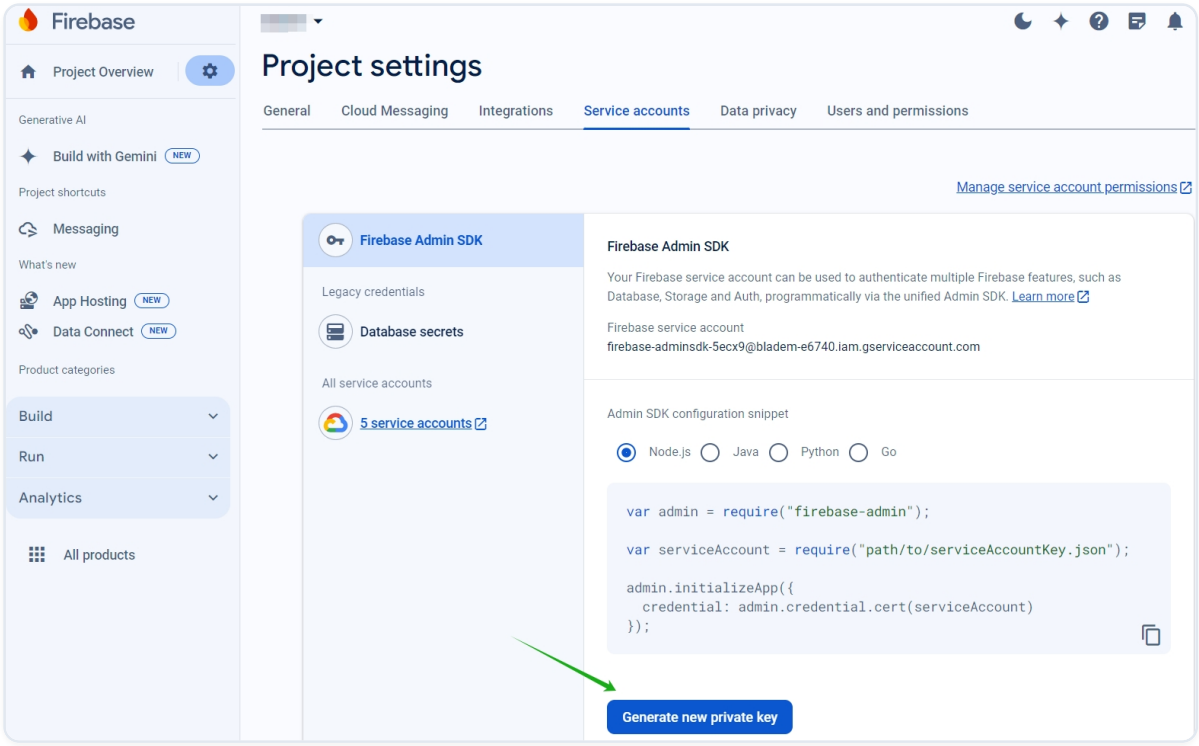
   b. 移行後、レガシーAPIはGoogleから非推奨となります。Firebase Cloud Messaging API(V1)を有効にする必要があります。詳細については、レガシーFCM APIからHTTP v1への移行を参照してください。



   Project settings の下の **Service accounts** からサービスアカウントのJSONファイルをダウンロードします。サービスアカウントの秘密鍵ファイルを生成するには、手動で資格情

© 1997–2026 Citrix Systems, Inc. All rights reserved.

報を提供するセクションを参照してください。**Generate new private key** をクリックして、サービスアカウントキーのJSONファイルをダウンロードします。



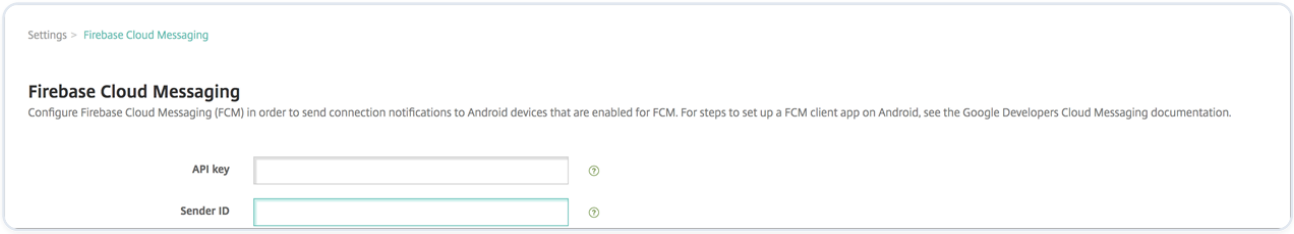
AndroidでFCMクライアントアプリをセットアップする手順については、Google DevelopersのCloud Messagingに関するこの記事を参照してください: `<https://firebase.google.com/docs/cloud-messaging/android/client>`。

FCM用にCitrix Endpoint Managementを構成するには

Citrix Endpoint Managementコンソールで、**Settings > Firebase Cloud Messaging** に移動します。

Cloud Messaging API (レガシー) の場合

1. Firebase Cloud Messaging構成の最後のステップで取得したFirebase Cloud Messaging**Key**を、**API key**フィールドに入力します。
2. 前の手順で取得した**Sender ID**の値を入力します。



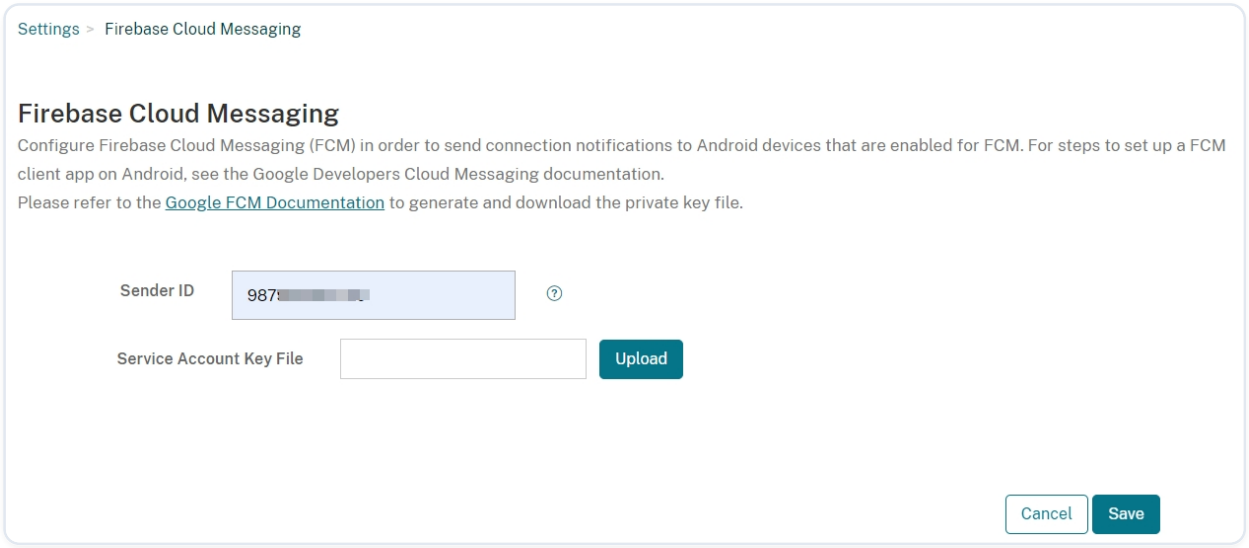
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Firebase クラウド メッセージング API (V1) の場合

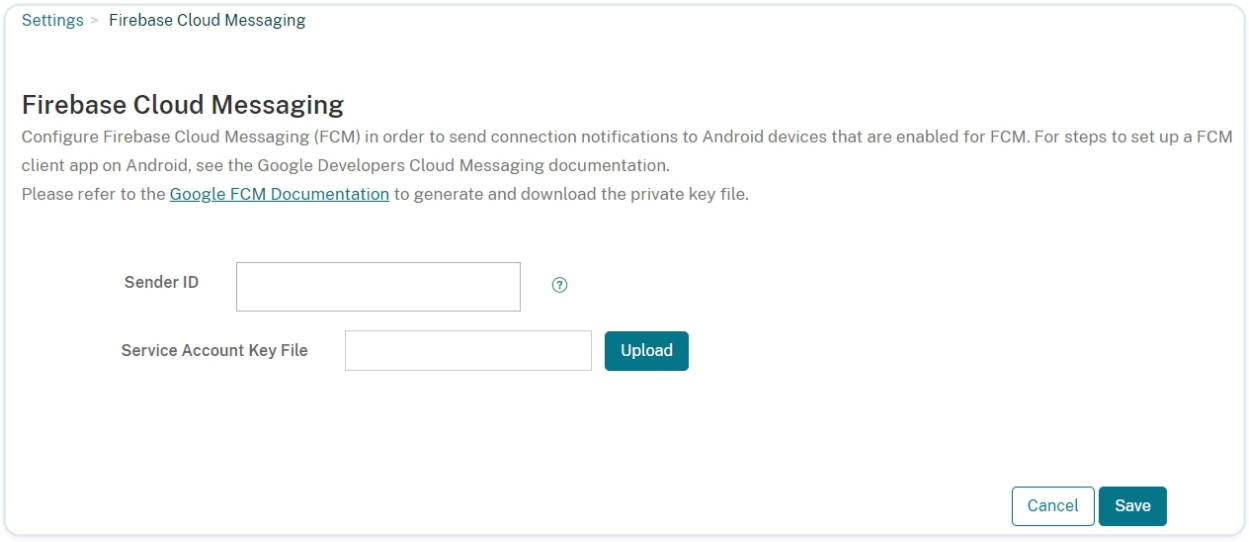
注:

- Citrix Endpoint Management バージョン 24.6.0 以降で FCM API V1 を有効にするには、Knowledge Center の記事 CTX677031 を参照してください。
- 新しい FCM ユーザーの場合は、手順 1 をスキップして手順 2 から進んでください。

1. 既に FCM を使用している場合は、送信者 ID が現在の FCM プロジェクトで自動入力され、**サービスアカウントキーファイル**をアップロードする新しいオプションが表示されます。

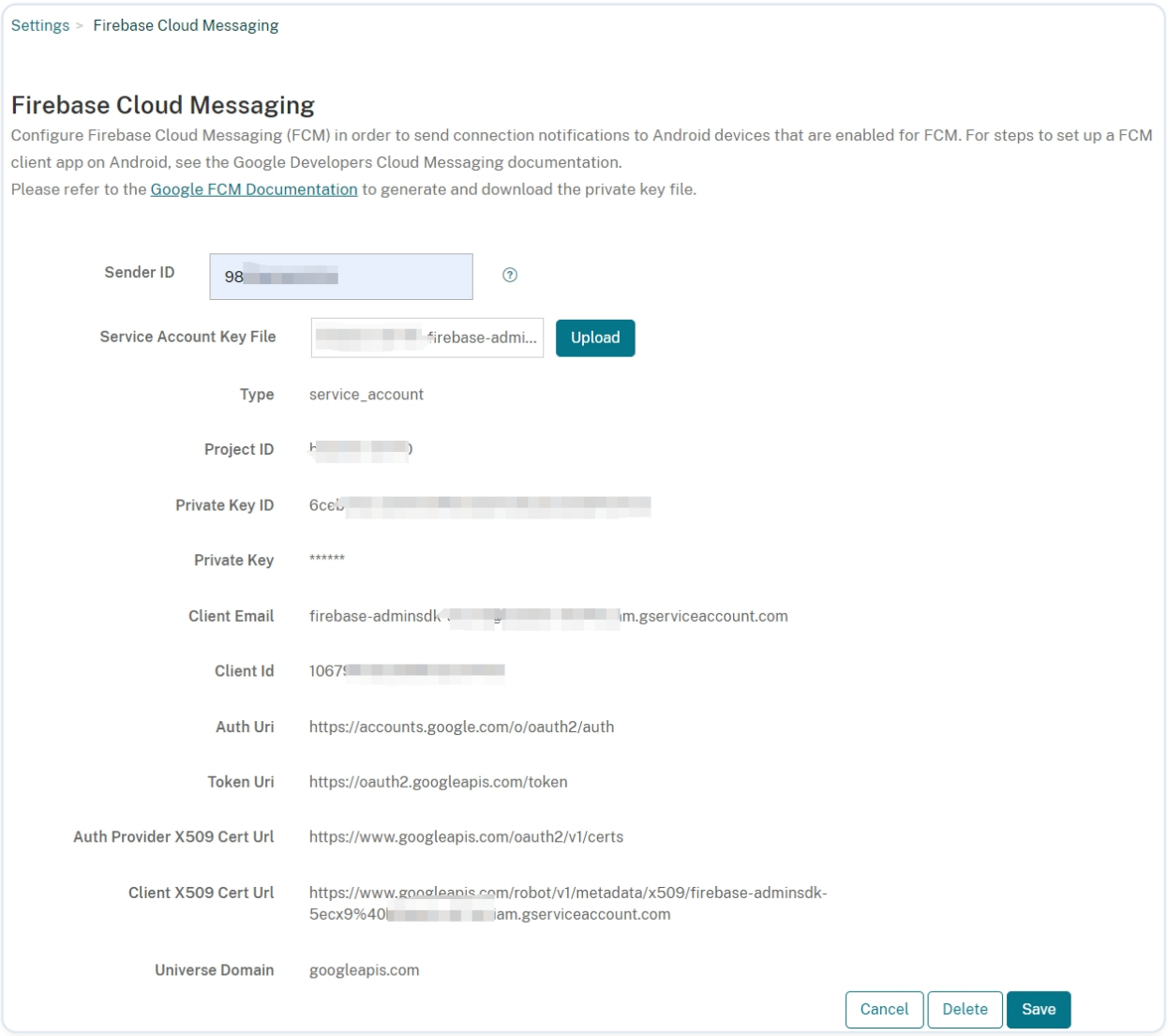


2. 新しい FCM ユーザーの場合は、**送信者 ID** を入力し、前の手順で作成した**サービスアカウントキーファイル**をアップロードします。



3. アップロードされたファイルは解析され、対応するフィールドが自動生成されます。

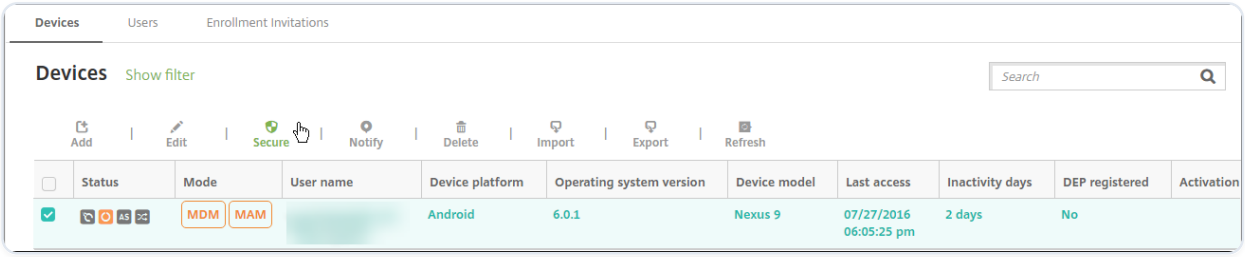
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 情報を確認し、**保存**をクリックします。

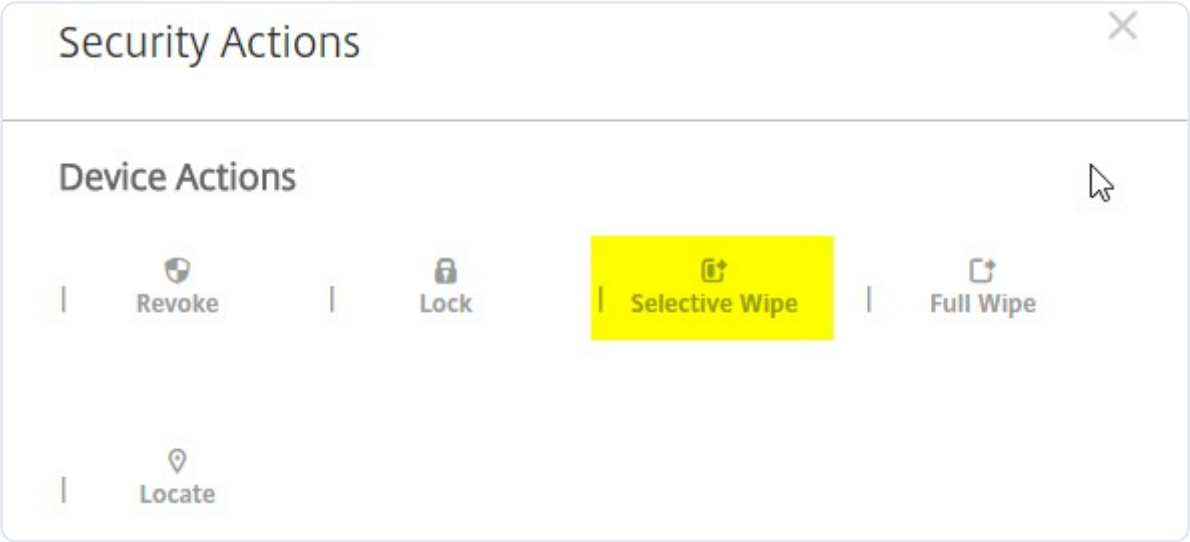
構成をテストするには

1. Android デバイスを登録します。
2. デバイスをしばらくアイドル状態にして、Citrix Endpoint Management から切断されるようにします。
3. Citrix Endpoint Management コンソールで、**管理**をクリックし、Android デバイスを選択してから、**セキュリティ保護**をクリックします。



4. **デバイスアクション**の下で、**選択的ワイプ**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



構成が正常に完了すると、デバイスで選択的ワイプが実行されます。

管理対象構成フィードバックのサポート（テクニカルプレビュー）

注:

テクニカルプレビューの機能は、非本番環境または限定的な本番環境で使用でき、お客様にフィードバックを共有する機会を提供します。Citrix® は、テクニカルプレビューの機能に関するサポートケースは受け付けていませんが、それらを改善するためのフィードバックを歓迎します。この機能に関するフィードバックは、**Send us your feedback** をクリックして提供できます。Citrix は、フィードバックの重大度、重要度、および優先度に基づいて対応する場合があります。

管理対象構成フィードバック機能を使用すると、管理者は管理対象構成ポリシーで構成された Android デバイスからアプリの状態に関するフィードバックを取得できます。このフィードバックは、これらのポリシーの有効性とステータスを監視するために使用できます。

前提条件

1. `App Support`: アプリケーションは管理対象構成ポリシーをサポートしている必要があります。
2. `Keyed App States`: アプリはキー付きアプリの状態もサポートしている必要があります。アプリのフィードバックがどのように機能するかについての詳細は、「EMM にアプリのフィードバックを送信する」を参照してください。

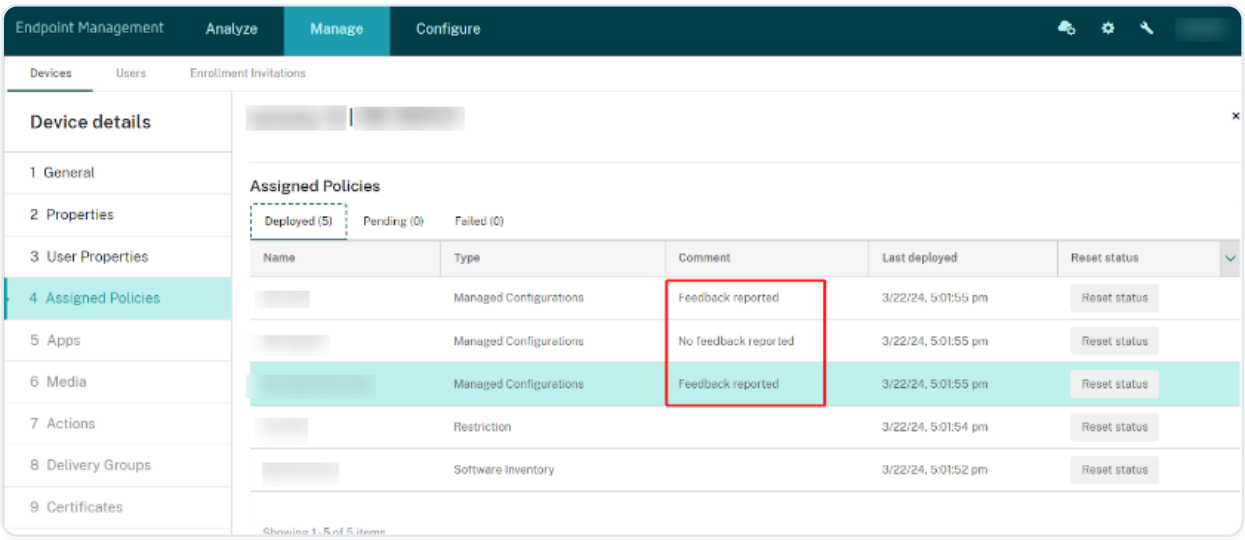
© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成フィードバックを管理および利用する手順

1. 指定された (Citrix Endpoint Management) CEM サーバーで機能フラグ `afw.app_managed_configurations.feedback` を有効にします。
2. 管理対象構成ポリシーを確認します。

   - Android デバイスが登録されており、管理対象構成ポリシーが正常に適用されていることを確認します。
   - **デバイスの詳細** に移動し、**割り当てられたポリシー** をクリックします。管理対象構成ポリシーに関連するコメントが表示されます。

     - **フィードバックが報告されました**: このポリシー関連アプリのフィードバックが利用可能であることを示します。
     - **フィードバックは報告されていません**: このポリシー関連アプリのフィードバックが報告されていないことを示します。



   - 「**デバイスの詳細**」に移動し、「**アプリ**」をクリックします。詳細なフィードバックは、すべてのアプリデータを含む「**管理対象構成フィードバック**」テーブルの下に表示されます。

     管理対象構成フィードバック(/en-us/citrix-endpoint-management/media/manage-config-feedback.png)

注:

上記のスクリーンショットでは、赤いボックスがKnow Service Pluginを強調表示し、緑のボックスが分離されたアプリを示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 単一の管理対象構成ポリシーの場合、割り当てられているすべてのデバイスのフィードバック詳細を確認できます。
  - **情報**: エラーを含まないフィードバックデータが報告されたすべてのデバイス。
  - **エラー**: エラーを含むフィードバックデータが報告されたすべてのデバイス。
  - **空**: フィードバックデータが報告されていないすべてのデバイス。

  フィードバックの詳細(/en-us/citrix-endpoint-management/media/feedback-details.png)
- フィードバックを手動で取得するには、「**管理**」をクリックし、対応するデバイスを見つけるためのチェックボックスを選択します。たとえば、対応するチェックボックスを選択して「**アプリのフィードバック**」をクリックできます。

  アプリのフィードバック(/en-us/citrix-endpoint-management/media/app-feedback.png)
- 「**フィードバックの取得**」をクリックして、選択したデバイスから管理対象構成フィードバックを取得します。

  フィードバックの取得(/en-us/citrix-endpoint-management/media/get-feedback.png)
- 管理対象構成フィードバックレポートから、「**分析**」を選択し、「**レポート**」をクリックして全体的なフィードバックを取得します。すべてのデバイス、構成ポリシー、および関連する構成の失敗に関するレポートを確認できます。

  管理対象構成フィードバックレポート(/en-us/citrix-endpoint-management/media/manage-config-feedback-report.png)

3. フィードバックのスケジュールを調整するために、2つのサーバープロパティが導入されました。クラウド管理ツールを使用してこれらのプロパティを変更し、フィードバックデータがデータベースに保存されるタイミングを制御します。

   a. Android Enterprise管理対象構成フィードバックデータベースを更新するバッチサイズ:
      - キー: `android.managed.configuration.feedback.db.update.batch.size`
      - DBに保存されるレポートのバッチサイズを定義できます。DBに保存されたデータのみがUIに表示されます。デフォルト値は100で、最大値は1000です。

   b. Android Enterprise管理対象構成フィードバックDB更新時間間隔:
      - キー: `android.managed.configuration.feedback.db.update.time.interval`
      - サイズがバッチ制限に達しない場合でも、レポートがデータベースに保存される期間を指定できます。デフォルト値は6時間です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

トラブルシューティング

デフォルトでは、フィードバックレポートは各デバイスのチェックイン時（Secure Hubがサーバーに接続するとき）に取得されます。ただし、アプリフィードバックボタンを使用して、特定のデバイスのレポートを手動で取得することもできます。

Android セーフティネット

Android SafetyNet機能を使用して、Citrix Secure Hubがインストールされているデバイスの互換性とセキュリティを評価できます。Android SafetyNetはMAM展開では利用できません。

この機能が有効になっている場合、SafetyNet Attestation APIは、デバイス上のソフトウェアおよびハードウェア情報を検査し、そのデバイスのプロファイルを作成します。その後、APIはAndroid互換性テストに合格したデバイスモデルのリスト内で同じプロファイルを探します。APIはまた、この情報を使用して、未知のソースがCitrix Secure Hubを変更したかどうかを判断します。

Android SafetyNet機能が有効になっている場合、Citrix Secure HubはSafetyNet Attestation APIリクエストをGoogle Playサービスに送信し、その結果はCitrix Endpoint Managementに報告されます。Citrix Endpoint Managementは、アテステーション結果でデバイス情報を更新します。アテステーション結果を使用してデバイス上でアクションをトリガーする自動アクションを設定できます。

SafetyNet Attestation APIの動作の詳細については、Android開発者向けドキュメントを参照してください。

必要なSafetyNet Attestation APIリクエストの数を推定する

SafetyNet Attestation APIリクエストは、次のときに送信されます。

- デバイスがCitrix Endpoint Managementに登録されている場合
- Citrix Secure Hubのオンライン認証が行われる場合

  オンライン認証は、サーバーセッションの有効期限が切れたとき、またはユーザーがサーバーからサインオフして再度サインオンしたときに発生します。Citrix Secure Hubは、サーバーで認証するための資格情報をユーザーに要求します。
- デバイスが再起動された場合
- 構成した繰り返し時間間隔で（24時間から1,000時間の間）。

Citrix Endpoint Management展開で1日あたり10,000を超えるリクエストが行われる場合、このクォータリクエストフォームに記入してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SafetyNet APIキーを取得する

Citrix Endpoint ManagementでAndroid SafetyNetを有効にするには、**SafetyNet API**キーが必要です。

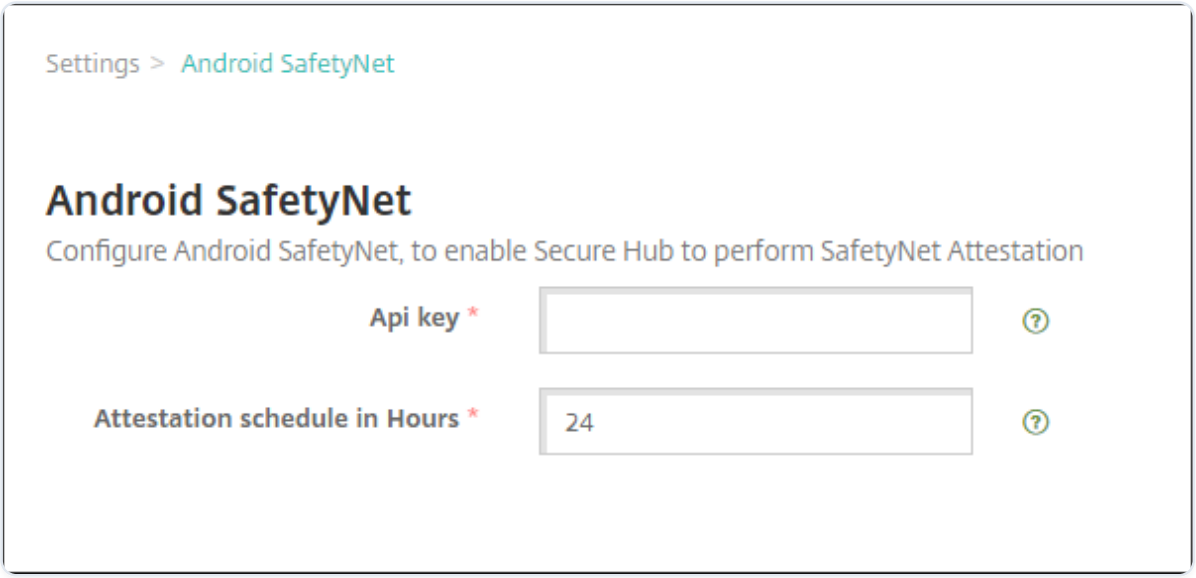
1. Google APIコンソールにGoogle管理者アカウントの資格情報でログインします。
2. ライブラリページに移動します。
3. 「Android Device Verification API」を検索します。 (/en-us/citrix-endpoint-management/media/google-api-search.png)
4. **Android Device Verification API**をクリックします。 (/en-us/citrix-endpoint-management/media/google-api-device-verification.png)
5. APIがまだ有効になっていない場合は、**有効にする**をクリックします。 (/en-us/citrix-endpoint-management/media/google-api-device-verification-enable.png)
6. **管理**をクリックします。
7. APIキーを生成するには、**資格情報の作成**をクリックします。 (/en-us/citrix-endpoint-management/media/google-api-device-verification-create-cred.png)
8. **Android Device Verification**を選択し、**必要な資格情報**をクリックします。次に、**完了**をクリックします。 (/en-us/citrix-endpoint-management/media/google-api-device-verification-create-cred.png)
9. **資格情報**ページで、キーの横にあるコピーアイコンをクリックしてキーをコピーします。 (/en-us/citrix-endpoint-management/media/google-api-device-verification-copy-key.png)
10. Android SafetyNetを有効にする際にCitrix Endpoint Managementコンソールに貼り付けられるように、キーを保存します。

Android SafetyNetを有効にする

1. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **設定**ページで、**Android SafetyNet**をクリックします。 (/en-us/citrix-endpoint-management/media/android-safetynet-settings.png)
3. 次の設定を構成します。

   - **APIキー**。Google APIコンソールから取得したSafetyNet APIキーを貼り付けます。
   - **アテステーションのスケジュール (時間)**。SafetyNet Attestation APIがAndroidデバイスを評価する間隔を時間単位で入力します。最小値は24時間です。最大値は1000時間です。デフォルト値は24時間です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

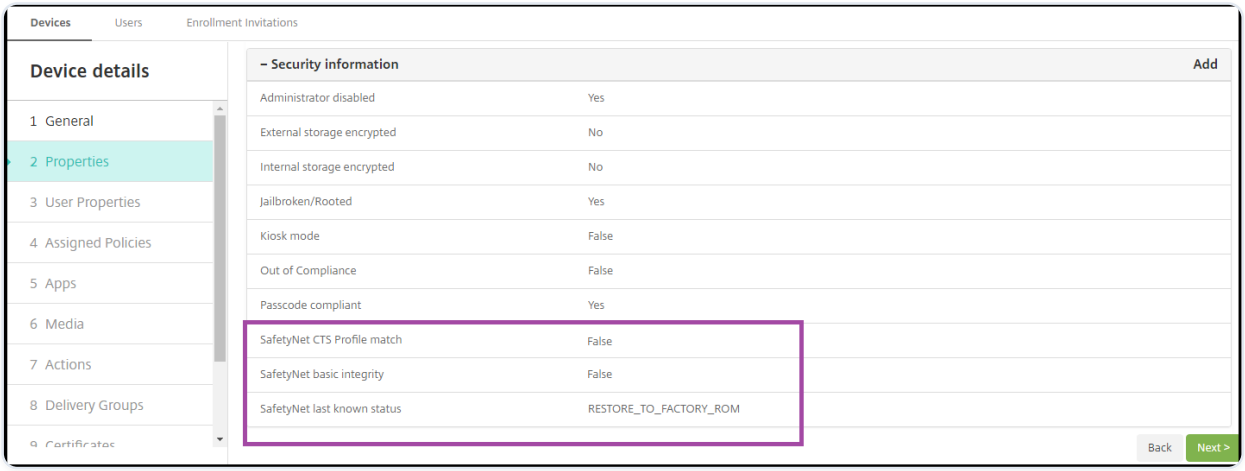


4. **保存**をクリックします。

Android SafetyNetの結果を表示する

デバイスのSafetyNet Attestation API評価の結果を表示するには、次の手順を実行します。

1. Citrix Endpoint Managementコンソールで、**管理 > デバイス**をクリックします。
2. SafetyNet Attestation APIの結果を表示するAndroidデバイスを選択します。次に、**詳細を表示**をクリックします。
3. **デバイスの詳細**ページで、**プロパティ**を選択します。
4. 結果は**セキュリティ**セクションに表示されます。



SafetyNet Attestation APIは、各デバイスについて次のステータスを返します。

- **SafetyNet CTSプロファイルの一致:** この値が**True**の場合、デバイスにはAndroid Compatibility Test Suite (CTS)に合格したプロファイルと一致するプロファイルがあります。この値が**False**に設定されている場合、デバイスにはAndroid CTSに合格したプロファイルと一致するプロファイルがありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **SafetyNetの基本的な整合性:** この値が**True**の場合、SafetyNet Attestation APIは、不明なソースがデバイス上のCitrix Secure Hubを変更したという証拠を見つけませんでした。この値が**False**に設定されている場合、不明なソースがデバイス上のCitrix Secure Hubを変更しました。
- **SafetyNetの最終既知ステータス:** この値は、デバイスの最終既知のSafetyNetステータスを示します。
  - **成功:** SafetyNet Attestation APIは、不明なソースがデバイス上のCitrix Secure Hubを変更したという証拠を見つけませんでした。
  - **LOCK_BOOTLOADER:** ユーザーはデバイスのブートローダーをロックする必要があります。不明なソースがデバイス上のCitrix Secure Hubを変更しました。
  - **RESTORE_TO_FACTORY_ROM:** ユーザーはデバイスをクリーンなファクトリーROMに復元する必要があります。不明なソースがデバイス上のCitrix Secure Hubを変更しました。

プレイ インテグリティ API

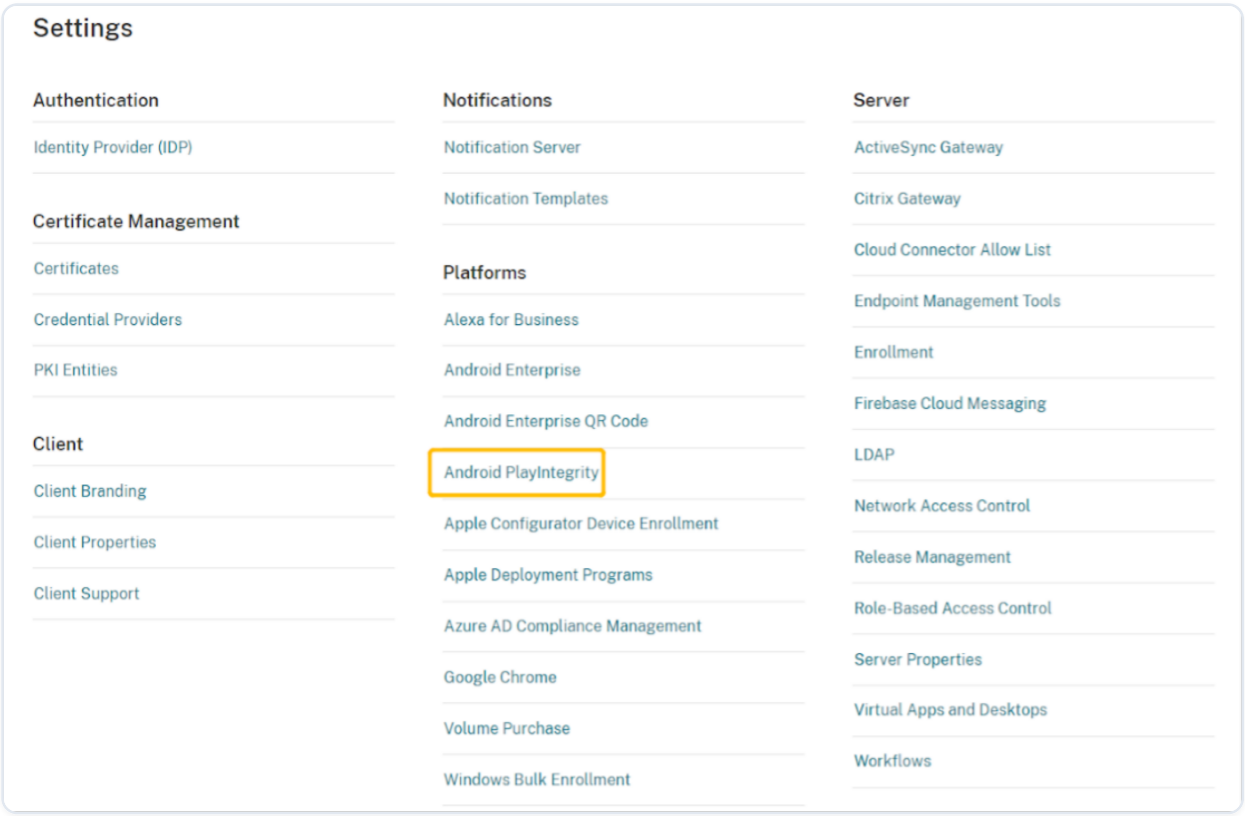
Play Integrity API は、チートや不正アクセスなどの潜在的に危険で不正な操作からアプリやゲームを保護し、適切な対策を講じて攻撃を防ぎ、悪用を減らすのに役立ちます。詳細については、Play Integrity API を参照してください。

Play Integrity API を有効にする

Play Integrity API に切り替えるには、次の手順に従います。

1. 指定された Citrix Endpoint Management サーバーで、*afw.safetynet.attestation.api.* 非推奨機能フラグをオンにします。
2. Citrix Endpoint Management コンソールで、**設定**ページから**Android PlayIntegrity**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

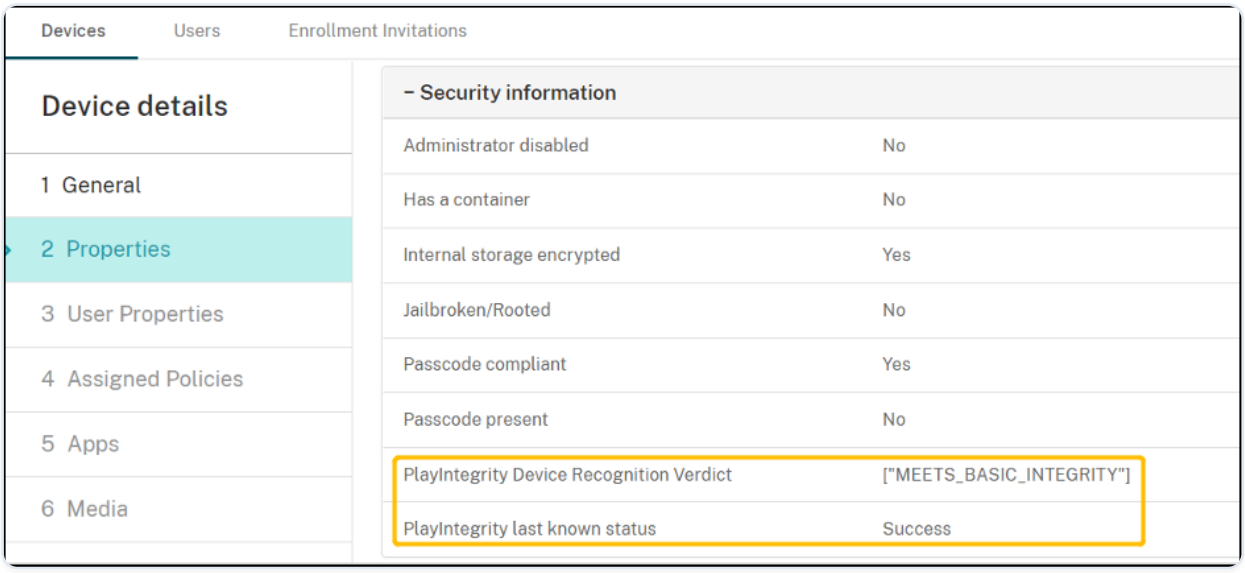


3. 時間フィールドにアッテステーションスケジュール値を入力します。これは、PlayIntegrity Attestation API がデバイスを評価する間隔時間です。最小値は24時間、最大値は1000時間です。デフォルト値は24時間です。**保存**をクリックします。
4. Citrix Secure Hub Android バージョン 23.7.0 にアップグレードします。デバイスからサインオフし、Citrix Secure Hub にサインインして、Play Integrity API 経由のアッテストをトリガーします。

Play Integrity API アッテステーションの結果を表示および分析する

1. Citrix Endpoint Management コンソールで、**管理 > デバイス**に移動します。
2. Play Integrity API アッテステーションの結果を表示したいデバイスを選択します。**詳細を表示**をクリックします。
3. **デバイス**タブで、**プロパティ**を選択します。結果は**セキュリティ情報**セクションに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Play Integrity API アッテステーションは、次のステータスを返します。

   - 「**PlayIntegrity Device Recognition Verdict**」フィールドに「**“MEETS_BASIC_INTEGRITY”**」がある場合、デバイスで実行されているCitrix Secure Hubが少なくとも基本的なシステム整合性を満たしていることを意味します。
   - 「**PlayIntegrity Device Recognition Verdict**」フィールドに「**“MEETS_BASIC_INTEGRITY”**」がない場合、デバイス上のCitrix Secure Hubが認識されていないバージョンのAndroidで実行されているか、ブートローダーがロック解除されているか、または製造元によって認定されていない可能性があることを意味します。
   - 「**PlayIntegrity last known status**」が「**Success**」の場合、PlayIntegrity APIアテステーションが正常に実行されたことを意味します。
   - 「**PlayIntegrity last known status**」が「**Failure**」の場合、PlayIntegrity APIアテステーションの実行に失敗したことを意味します。

注：

管理者は、SafetyNet Attestationの最終的な廃止（2023年11月末）の前に、SafetyNetの使用を許可する機能フラグをクリアできます。

制限事項

1. 新規登録されたCOSUデバイスおよびDOデバイスは、デバイスが準拠している場合でも、非準拠としてマークされます。

   DO登録中の最初のアテステーションでは、Play Integrity APIが空を返すため、デバイスが非準拠に見えます。この制限はGoogleの既知の問題です。この問題を修正するために、DPC Support Lib 20230418が公開されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

この修正はバージョン23.9.0から利用可能です。それまでは、以下の手順を回避策として使用してください。

- 機能フラグをクリアし、SafetyNet APIを引き続き使用してSafetyNet Attestation APIを使い続けます。
- 登録後にアテステーションをトリガーするには、サインオフして再度サインインします。次の定期的なアテステーション（デフォルトは24時間）を待つこともできます。

この問題は登録中にのみ発生します。Play Integrity APIは登録後には正常に動作します。

2. 新規登録されたWPCODデバイスは、デバイスが準拠している場合でも非準拠としてマークされます。Googleはこの問題を調査中です。

サムスン

Samsung は、Citrix Endpoint Management と互換性のあるいくつかのソリューションを提供しています。

Android デバイスが Citrix Endpoint Management サービスに接続する方法とタイミングを制御するには、Firebase Cloud Messaging (FCM) を使用します。詳細については、「Firebase Cloud Messaging」を参照してください。

登録プロファイルは、Android デバイスが MAM、MDM、または MDM+MAM のいずれに登録されるかを決定し、ユーザーは MDM からオプトアウトするオプションを選択できます。Citrix Endpoint Management は、MDM+MAM に登録された Android デバイスに対して、次の認証タイプをサポートしています。詳細については、以下の記事を参照してください。

- ドメインまたはドメインとセキュリティトークン認証
- クライアント証明書または証明書とドメイン認証
- ID プロバイダー:
  - Citrix Cloud を介した Azure Active Directory による認証
  - Citrix Cloud を介した Okta による認証

あまり使用されない別の認証方法として、クライアント証明書とセキュリティトークンがあります。詳細については、`<https://support.citrix.com/article/CTX215200>` を参照してください。

Android デバイス管理を開始するための一般的なワークフローは次のとおりです。

1. オンボーディングプロセスを完了します。「オンボーディングとリソースのセットアップ」および「デバイスの登録とリソースの配信の準備」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 登録方法を選択して構成します。「サポートされている登録方法」を参照してください。
3. Samsung ライセンスキーの展開。
4. Samsung デバイスポリシーの構成。
5. デバイスとアプリのセキュリティアクションを設定します。「セキュリティアクション」(#security-actions)を参照してください。

サポートされているオペレーティングシステムについては、「サポートされているデバイスオペレーティングシステム」(/ja-jp/citrix-endpoint-management/system-requirements/supported-device-platforms.html)を参照してください。

サポートされている登録方法

次の表に、Citrix Endpoint ManagementがAndroidデバイスでサポートする登録方法を示します。

方法	サポート対象
手動登録	はい
登録招待	はい

デバイスの登録については、「Androidデバイスの登録」(/ja-jp/citrix-endpoint-management/device-management/android/android-os.html#enroll-android-devices)を参照してください。

Samsungライセンスキーの展開

SamsungにはKnox Platform Enterpriseキーがあります。詳細については、「Knox Platform for Enterpriseキーデバイスポリシー」(/ja-jp/citrix-endpoint-management/policies/knox-platform-for-enterprise-key-policy.html)を参照してください。

Samsungデバイスポリシーの構成

デバイスポリシー：

アプリの制限	アプリのアンインストール	パスコード
制限	VPN	

セキュリティアクション

Androidは以下のセキュリティアクションをサポートしています。各セキュリティアクションの説明については、セキュリティアクションを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリロック	アプリワイプ	証明書の更新
完全ワイプ	検索	ロック
ロックとパスワードのリセット	通知	取り消し
選択的ワイプ		

注：

Android 6.0以降を実行しているデバイスの場合、**Locate**セキュリティアクションでは、登録時にユーザーが位置情報権限を付与する必要があります。ユーザーは位置情報権限を付与しないことを選択できます。ユーザーが登録時に権限を付与しなかった場合、Citrix Endpoint ManagementはLocateコマンドを送信する際に再度位置情報権限を要求します。

ネットワークアクセスコントロール

ネットワークアクセスコントロール (NAC) ソリューションを使用して、AndroidおよびAppleデバイス向けのCitrix Endpoint Managementデバイスセキュリティ評価を拡張できます。NACソリューションは、Citrix Endpoint Managementセキュリティ評価を使用して認証決定を促進および処理します。NACアプライアンスを構成すると、Citrix Endpoint Managementで構成したデバイスポリシーとNACフィルターが適用されます。

NACソリューションとCitrix Endpoint Managementを併用することで、ネットワーク内部のデバイスに対するQoSとよりきめ細かな制御が追加されます。NACとCitrix Endpoint Managementを統合する利点の概要については、「アクセス制御」を参照してください。

Citrixは、Citrix Endpoint Managementとの統合のために以下のソリューションをサポートしています。

- ネットスケーラー ゲートウェイ
- ForeScout

Citrix®は、他のNACソリューションとの統合を保証しません。

ネットワークにNACアプライアンスがある場合：

- Citrix Endpoint Managementは、iOS、Android Enterprise、およびAndroidデバイスのエンドポイントセキュリティ機能としてNACをサポートしています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Managementでフィルターを有効にして、ルールまたはプロパティに基づいて、NACのデバイスを準拠または非準拠として設定できます。例：
  - Citrix Endpoint Managementで管理されているデバイスが指定された基準を満たさない場合、Citrix Endpoint Managementはそのデバイスを非準拠としてマークします。NACアプライアンスは、ネットワーク上の非準拠デバイスをブロックします。
  - Citrix Endpoint Managementで管理されているデバイスに非準拠アプリがインストールされている場合、NACフィルターはVPN接続をブロックできます。その結果、非準拠のユーザーデバイスはVPNを介してアプリやWebサイトにアクセスできません。
  - NACにNetScaler Gatewayを使用している場合、NetScaler Gatewayプラグインが不要なネットワークトラフィックをNetScaler Gatewayに送信するのを防ぐために、スプリットトンネリングを有効にできます。スプリットトンネリングの詳細については、「スプリットトンネリングの構成」を参照してください。

サポートされているNAC準拠フィルター

Citrix Endpoint Managementは、以下のNAC準拠フィルターをサポートしています。

匿名デバイス： デバイスが匿名モードであるかどうかを確認します。このチェックは、デバイスが再接続しようとしたときにCitrix Endpoint Managementがユーザーを再認証できない場合に利用できます。

禁止されているアプリ： デバイスに、アプリアクセスポリシーで定義されている禁止されているアプリがあるかどうかを確認します。そのポリシーの詳細については、「アプリアクセスのデバイスポリシー」を参照してください。

非アクティブなデバイス： **Server Properties**の**Device Inactivity Days Threshold**設定で定義されているように、デバイスが非アクティブであるかどうかを確認します。詳細については、「サーバープロパティ」を参照してください。

不足している必須アプリ： デバイスに、アプリアクセスポリシーで定義されている必須アプリが不足しているかどうかを確認します。

推奨されないアプリ： デバイスに、アプリアクセスポリシーで定義されている推奨されないアプリがあるかどうかを確認します。

準拠していないパスワード： ユーザーパスワードが準拠しているかどうかを確認します。iOSおよびAndroidデバイスでは、Citrix Endpoint Managementは、現在デバイス上にあるパスワードが、デバイスに送信されたパスコードポリシーに準拠しているかどうかを判断できます。たとえば、iOSでは、Citrix Endpoint Managementがデバイスにパスコードポリシーを送信した場合、ユー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ザーは60分以内にパスワードを設定する必要があります。ユーザーがパスワードを設定する前は、パスコードが準拠していない可能性があります。

準拠していないデバイス： デバイスが、準拠していないデバイスプロパティに基づいて、準拠していないかどうかを確認します。通常、自動化されたアクションまたはCitrix Endpoint Management APIを使用するサードパーティがそのプロパティを変更します。

失効ステータス： デバイス証明書が失効しているかどうかを確認します。失効したデバイスは、再度承認されるまで再登録できません。

ルート化されたAndroidデバイスとジェイルブレイクされたiOSデバイス： AndroidまたはiOSデバイスがジェイルブレイクされているかどうかを確認します。

管理されていないデバイス： Citrix Endpoint Managementがデバイスを管理しているかどうかを確認します。たとえば、MAMに登録されているデバイスや未登録のデバイスは管理されていません。

注：

暗黙的な準拠/非準拠フィルターは、Citrix Endpoint Managementが管理しているデバイスにのみデフォルト値を設定します。たとえば、ブロックされたアプリがインストールされているデバイスや登録されていないデバイスは、非準拠としてマークされます。NACアプライアンスは、これらのデバイスをネットワークからブロックします。

構成の概要

NACコンポーネントは、記載されている順序で構成することをお勧めします。

1. NACをサポートするようにデバイスポリシーを構成します。

   iOSデバイスの場合: NACをサポートするようにVPNデバイスポリシーを構成するを参照してください。

   Android Enterpriseデバイスの場合: Citrix SSOのAndroid Enterprise管理対象構成を作成するを参照してください。

   Androidデバイスの場合: Android向けCitrix SSOプロトコルを構成するを参照してください。
2. Citrix Endpoint ManagementでNACフィルターを有効にする。
3. NACソリューションを構成します:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

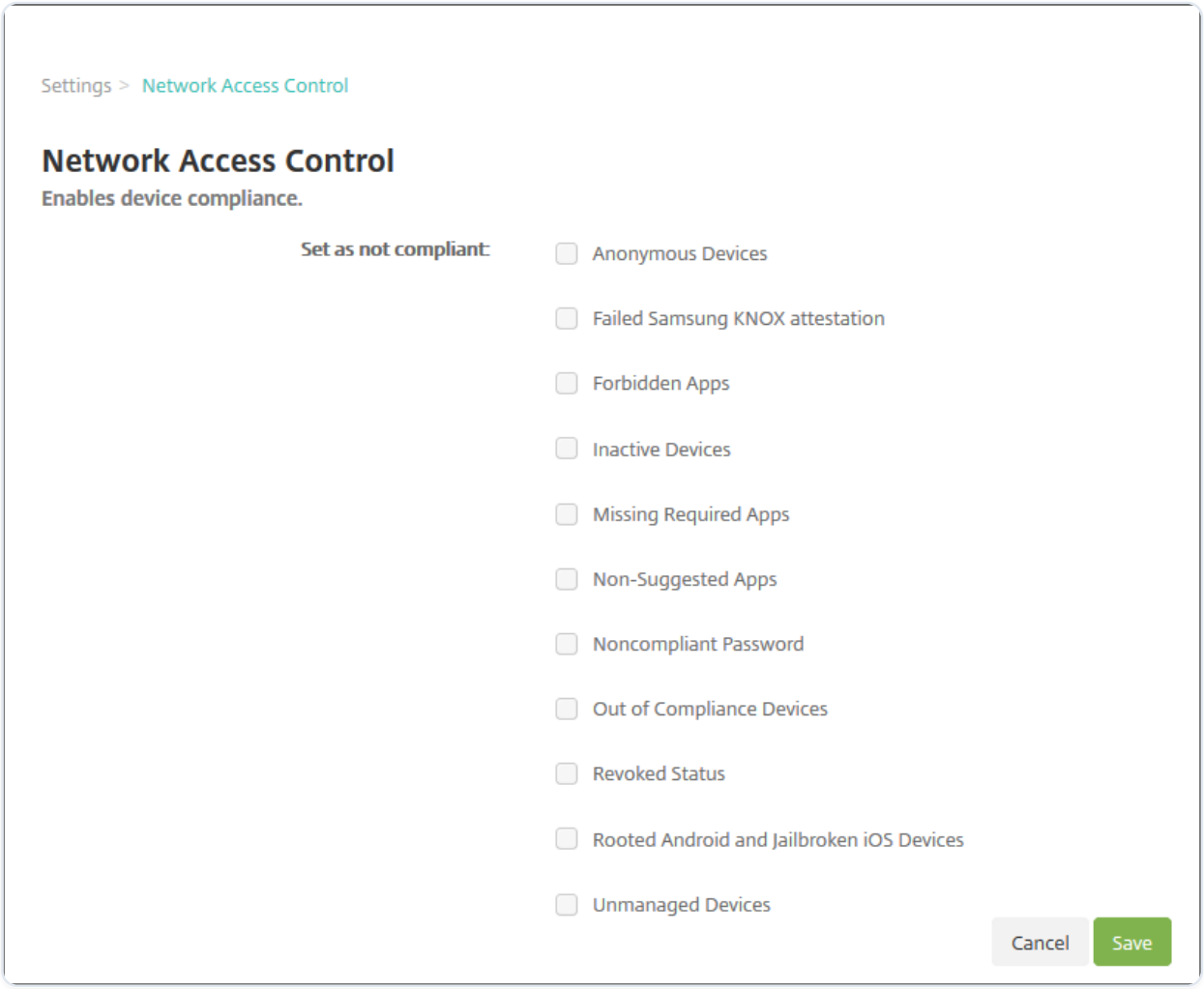
- NetScaler Gateway。NACをサポートするようにNetScaler Gatewayポリシーを更新するに詳述されています。

  デバイスにCitrix SSOをインストールする必要があります。NetScaler Gatewayクライアントを参照してください。

- ForeScout: ForeScoutのドキュメントを参照してください。

Citrix Endpoint ManagementでNACフィルターを有効にする

1. Citrix Endpoint Managementコンソールで、**設定 > ネットワークアクセス制御**に移動します。



2. 有効にする**非準拠として設定**フィルターのチェックボックスをオンにします。
3. **保存**をクリックします。

NACをサポートするようにNetScaler Gatewayポリシーを更新する

VPN仮想サーバーで、高度な（従来の方式ではない）認証およびVPNセッションポリシーを構成する必要があります。

これらの手順は、以下のいずれかの特性を持つNetScaler Gatewayを更新します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Managementと統合されている。
- または、VPN用に設定されており、Citrix Endpoint Management環境の一部ではないが、Citrix Endpoint Managementに到達できる。

コンソールウィンドウから仮想VPNサーバーで、次の操作を行います。コマンドと例のFQDNおよびIPアドレスは架空のものです。

1. VPN仮想サーバーでクラシックポリシーを使用している場合は、すべてのクラシックポリシーを削除してバインドを解除します。確認するには、次のように入力します。

   `show vpn vserver <VPN_VServer>`

   「**Classic**」という単語を含む結果をすべて削除します。例: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   ポリシーを削除するには、次のように入力します。

   `unbind vpn vserver <VPN_VServer> -policy <policy_name>`
2. 次のように入力して、対応する高度なセッションポリシーを作成します。

   `add vpn sessionPolicy <policy_name> <rule> <session action>`

   例: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`
3. 次のように入力して、ポリシーをVPN仮想サーバーにバインドします。

   `bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100`
4. 次のように入力して、認証仮想サーバーを作成します。

   `add authentication vserver <authentication vserver name> <service type> <ip address>`

   例えば: `add authentication vserver authvs SSL 0.0.0.0` この例では、`0.0.0.0` は認証仮想サーバーが公開されていないことを意味します。
5. 次のように入力して、仮想サーバーにSSL証明書をバインドします。

   `bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>`

   例えば: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`
6. VPN仮想サーバーから認証仮想サーバーに認証プロファイルを関連付けます。まず、次のように入力して認証プロファイルを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`add authentication authnProfile <profile name> -authnVsName <authentication vserver name>`

例えば:

`add authentication authnProfile xm_nac_prof -authnVsName authvs`

7. 次のように入力して、認証プロファイルをVPN仮想サーバーに関連付けます。

   `set vpn vserver <vpn vserver name> -authnProfile <authn profile name>`

   例えば:

   `set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof`

8. 次のように入力して、NetScaler Gatewayからデバイスへの接続を確認します。

   `curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"`

   たとえば、このクエリは、環境に登録されている最初のデバイス (`deviceid_1`) のコンプライアンスステータスを取得することで、接続性を検証します。

   `curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"`

   成功した結果は、次の例のようになります。

   ```
   HTTP/1.1 200 OK

   < Server: Apache-Coyote/1.1

   < X-Citrix-Device-State: Non Compliant

   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. 前の手順が成功したら、Citrix Endpoint Management への Web 認証アクションを作成します。まず、iOS VPN プラグインからデバイス ID を抽出するポリシー式を作成します。次のように入力します。

   `add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\', \'&\').VALUE(\"deviceidvalue\")"`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. 次のように入力して、Citrix Endpoint Management にリクエストを送信します。この例では、Citrix Endpoint Management の IP は `10.207.87.82` で、FQDN は `example.em.cloud.com:4443` です。

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort 4443 -fullReqExpr q{"GET /Citrix/Device/v1/Check HTTP/1.1\r\n" + "Host: example.em.cloud.com:4443\r\n" + "X-Citrix-VPN-Device-ID: " + xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\"200\") &&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"
    ```

    Citrix Endpoint Management NAC の成功出力は `HTTP status 200 OK` です。`X-Citrix-Device-State` ヘッダーの値は `Compliant` である必要があります。

11. 次のように入力して、アクションを関連付ける認証ポリシーを作成します。

    ```
    add authentication Policy <policy name> -rule <rule> -action <web authentication action>
    ```

    例: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")" -action xm_nac`

12. 次のように入力して、既存の LDAP ポリシーを高度なポリシーに変換します。

    ```
    add authentication Policy <policy_name> -rule <rule> -action <LDAP action name>
    ```

    例: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. 次のように入力して、LDAP ポリシーを関連付けるポリシーラベルを追加します。

    ```
    add authentication policylabel <policy_label_name>
    ```

    例えば: `add authentication policylabel ldap_pol_label`

14. 次のように入力して、LDAPポリシーをポリシーラベルに関連付けます。

    ```
    bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
    ```

15. 準拠デバイスを接続してNACテストを実行し、LDAP認証が成功したことを確認します。次のように入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END
```

16. 認証仮想サーバーに関連付けるUIを追加します。次のコマンドを入力して、デバイスIDを取得します。

```
add authentication loginSchemaPolicy <schema policy>-rule <rule> -action lschema_single_factor_deviceid
```

17. 次のように入力して、認証仮想サーバーをバインドします。

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100 -gotoPriorityExpression END
```

18. Citrix Secure Hub接続を有効にするLDAP高度認証ポリシーを作成します。次のように入力します。

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\").NOT" -action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -priority 110 -gotoPriorityExpression NEXT
```

Apple

iOS

Citrix Endpoint Management で iOS デバイスを管理するには、Apple から Apple Push Notification service (APNs) 証明書を設定します。詳細については、「APNs 証明書」(/ja-jp/citrix-endpoint-management/authentication/apns.html)を参照してください。

登録プロファイルは、iOS デバイスが MDM+MAM に登録されるかどうかを決定します。ユーザーがモバイルデバイス管理 (MDM) からオプトアウトするオプションがあります。Citrix Endpoint Management は、MDM+MAM の iOS デバイスに対して以下の認証タイプをサポートしています。詳細については、以下の記事を参照してください。

- ドメインまたはドメインとセキュリティトークン認証
- クライアント証明書または証明書とドメイン認証
- ID プロバイダー:
  - Citrix Cloud を介した Azure Active Directory による認証

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Cloud を介した Okta による認証

IOS 13 での信頼された証明書の要件:

Apple は TLS サーバー証明書に関する新しい要件を設けています。すべての証明書が新しい Apple の要件に準拠していることを確認してください。Apple の公開情報 `<https://support.apple.com/ja-jp/HT210176>` を参照してください。証明書の管理については、「証明書のアップロード」(/ja-jp/citrix-endpoint-management/authentication/upload-renew-certificates.html#upload-certificates)を参照してください。

iOS デバイス管理を開始するための一般的なワークフローは次のとおりです。

1. オンボーディングプロセスを完了します。「オンボーディングとリソースのセットアップ」(/ja-jp/citrix-endpoint-management/onboarding-and-resource-setup.html)および「デバイスの登録とリソースの配信の準備」(/ja-jp/citrix-endpoint-management/prepare-to-enroll-devices-and-deliver-resources.html)を参照してください。
2. 登録方法を選択して構成します。「サポートされている登録方法」(#supported-enrollment-methods)を参照してください。
3. iOS デバイスポリシーの構成.
4. iOS デバイスの登録.
5. デバイスとアプリのセキュリティアクションを設定します。セキュリティアクションを参照してください。

サポートされているオペレーティングシステムについては、サポートされているデバイスオペレーティングシステムを参照してください。

iOS 14の互換性

Citrix Endpoint ManagementとCitrixモバイルアプリはiOS 14と互換性がありますが、現在のところ新しいiOS 14の機能はサポートしていません。

監視対象のiOSデバイスの場合、ソフトウェアアップグレードを最大90日間延期できます。iOSの制限デバイスポリシーで、次の設定を使用します。

- **ソフトウェアアップデートの遅延を強制する**
- **ソフトウェアアップデートの遅延を適用する**

iOS設定を参照してください。これらの設定は、ユーザー登録モードまたは非監視（フルMDM）モードのデバイスでは利用できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

開放しておく必要があるAppleホスト名

iOS、macOS、およびApple App Storeが適切に動作するためには、一部のAppleホスト名を開放しておく必要があります。これらのホスト名をブロックすると、iOS、iOSアプリ、MDM操作、デバイスおよびアプリの登録のインストール、更新、および適切な動作に影響を与える可能性があります。詳細については、`<https://support.apple.com/ja-jp/HT201999>`を参照してください。

サポートされている登録方法

登録プロファイルでiOSデバイスの管理方法を指定します。次の登録設定から選択できます。

- **Appleユーザー登録:** BYODデバイスの場合、個人データのプライバシーと企業データのセキュリティのバランスを提供します。この登録モードはパブリックプレビューとして利用可能です。この機能を有効にするには、サポートチームにお問い合わせください。
- **Appleデバイス登録:** 監視対象のiOSデバイスの場合、デバイス上に個別の個人プロファイルと企業プロファイルを作成します。
- **デバイスを管理しない:** アプリのみを管理したい場合は、これらのデバイスをMDMから除外します。

登録プロファイルの作成に関する詳細については、登録プロファイルを参照してください。

Citrix Endpoint Managementは、iOSデバイス向けに以下の登録方法をサポートしています。

方法	サポート
Apple Business Manager (アップルビジネスマネージャー)	はい
Apple School Manager (アップルスクールマネージャー)	はい
アップル コンフィグレータ	はい
手動登録	はい
登録招待	はい

Apple Deployment Programsには、ビジネス組織向けのApple Business Manager (ABM)と、教育機関向けのApple School Manager (ASM)が含まれます。詳細については、Apple Deployment Programsによるデバイスの展開を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apple School Manager は Education Apple Deployment Program の一種です。 Apple Education 機能との統合を参照してください。

Apple Deployment Programs を使用して、iOS、iPadOS、および macOS デバイスを一括登録します。これらのデバイスは、Apple、参加しているApple正規販売店、または通信事業者から直接購入できます。iOSデバイスをAppleから直接購入した場合でも、Apple Configuratorを使用してそれらのデバイスを登録できます。Appleデバイスを一括登録するを参照してください。

管理対象Apple ID

ユーザー登録は、管理対象Apple IDと密接に統合されています。管理対象Apple IDは、ABM/ASMを使用して手動で作成することも、Azure Active Directory (AAD) を使用して動的に作成することもできます。

フェデレーション認証を使用しない場合は、ABM/ASM を使用して管理対象Apple IDを作成し、アカウントを追加します。ABM/ASM でアカウントを追加する方法については、Apple のドキュメント (`https://support.apple.com/guide/apple-business-manager/welcome/web`) と ASM (`https://support.apple.com/guide/apple-school-manager/welcome/web`) を参照してください。ユーザーが登録する際の追加手順を避けるために、以下をお勧めします。

- 管理対象Apple IDを作成する際は、会社のメールアドレスと一致するメールを使用してください。
- ユーザーロールを**スタッフ**に設定します。
- ユーザーには、登録前に手動でパスワードを変更してもらいます。会社のパスワードと同じパスワードを使用することをお勧めすることをユーザーに伝えてください。

管理対象Apple IDを動的に作成するには、Citrix CloudがAADをIDプロバイダーとして使用するように構成します。Citrix CloudがAADを使用するように構成する方法の詳細については、Citrix Cloud を介した Azure Active Directory による認証を参照してください。また、ABM/ASMでフェデレーション認証を構成します。ABMまたはASMでフェデレーション認証を構成する方法の詳細については、Apple Business Managerユーザーガイドと Apple School Managerユーザーガイドを参照してください。

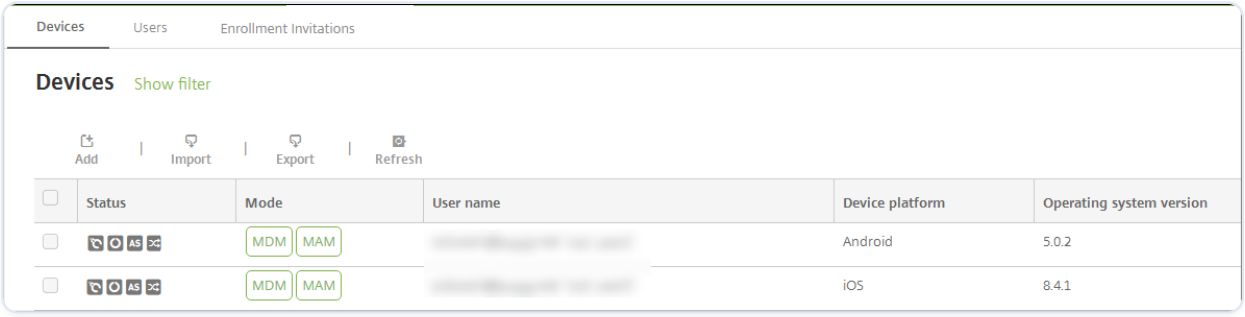
管理対象Apple IDを手動で作成する場合、デフォルトのドメインの代わりにカスタムドメインを使用するように構成できます。構成したカスタムドメインは、既存のドメインを置き換えます。たとえば、会社のメールアドレスは `first.last@company.com` の形式ですが、代わりに管理対象Apple IDのドメインとして `mycompany.website.com` を使用したいとします。ABM/ASMで管理対象Apple IDを作成すると、メールアドレスは `first.last@mycompany.website.com` になります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOSデバイスを手動で追加する

テスト目的などでiOSデバイスを手動で追加する場合は、以下の手順に従ってください。

1. Citrix Endpoint Management コンソールで、**管理 > デバイス**をクリックします。**デバイス**ページが表示されます。



2. **追加**をクリックします。**デバイスの追加**ページが表示されます。

「デバイスの追加」ページ(/en-us/citrix-endpoint-management/media/manage-devices-add-device.png)

3. 次の設定を構成します。

   - **プラットフォームの選択: iOS**をクリックします。
   - **シリアル番号:** デバイスのシリアル番号を入力します。

4. **追加**をクリックします。**デバイス**テーブルが表示され、デバイスがリストの一番下に追加されます。デバイスの詳細を表示して確認するには、追加したデバイスを選択し、表示されるメニューで**編集**をクリックします。

> **注:**
>
> デバイスの横にあるチェックボックスを選択すると、オプションメニューがデバイスリストの上に表示されます。リスト内の他の場所をクリックすると、オプションメニューがリストの右側に表示されます。

   - LDAPが構成されている
   - ローカルグループとローカルユーザーを使用する場合：
     - 1つ以上のローカルグループ。
     - ローカルグループに割り当てられたローカルユーザー。
     - デリバリーグループはローカルグループに関連付けられています。
   - Active Directoryを使用する場合：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- デリバリーグループはActive Directoryグループに関連付けられています。

「デバイスの詳細」リスト(/en-us/citrix-endpoint-management/media/manage-devices-details-general.png)

5. 「**一般**」ページには、シリアル番号やプラットフォームタイプに関するその他の情報など、デバイスの**識別子**が一覧表示されます。「**デバイス所有権**」には、「**企業**」または「**BYOD**」を選択します。

   「**一般**」ページには、強力なID、デバイスのロック、アクティベーションロックのバイパスなど、デバイスの**セキュリティ**プロパティやプラットフォームタイプに関するその他の情報も一覧表示されます。「**デバイスの完全ワイプ**」フィールドには、ユーザーのPINコードが含まれています。デバイスがワイプされた後、ユーザーはそのコードを入力する必要があります。ユーザーがコードを忘れた場合は、ここで確認できます。

6. 「**プロパティ**」ページには、Citrix Endpoint Managementがプロビジョニングするデバイスプロパティが一覧表示されます。このリストには、デバイスの追加に使用されたプロビジョニングファイルに含まれるすべてのデバイスプロパティが表示されます。プロパティを追加するには、「**追加**」をクリックし、リストからプロパティを選択します。各プロパティの有効な値については、PDF「デバイスプロパティ名と値」を参照してください。

   プロパティを追加すると、最初は追加したカテゴリの下に表示されます。「**次へ**」をクリックして「**プロパティ**」ページに戻ると、そのプロパティは適切なリストに表示されます。

   プロパティを削除するには、リストにカーソルを合わせ、右側にある「**X**」をクリックします。Citrix Endpoint Managementはすぐにその項目を削除します。

7. 残りの「**デバイスの詳細**」セクションには、デバイスの概要が表示されます。

   - **ユーザープロパティ:** RBACロール、グループメンバーシップ、ボリューム購入アカウント、およびユーザーのプロパティを表示します。このページからボリューム購入アカウントを廃止できます。
   - **割り当て済みポリシー:** 展開済み、保留中、失敗したポリシーの数を表示します。各ポリシーのポリシー名、タイプ、および最終展開情報を提供します。展開ステータスを保留中にリセットし、ユーザーが削除したポリシーを再展開できます。
   - **アプリ:** 最新のインベントリについて、インストール済み、保留中、失敗したアプリ展開の数を表示します。アプリ名、識別子、タイプ、およびその他の情報を提供します。「**HasUpdateAvailable**」などのiOSおよびmacOSインベントリキーの説明については、「モバイルデバイス管理（MDM）プロトコル」を参照してください。
   - **メディア:** 最新のインベントリについて、展開済み、保留中、失敗したメディア展開の数を表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アクション:** 展開済み、保留中、失敗したアクションの数を表示します。アクション名と最終展開時刻を提供します。
- **デリバリーグループ:** 成功、保留中、失敗したデリバリーグループの数を表示します。各展開について、デリバリーグループ名と展開時刻を提供します。デリバリーグループを選択すると、ステータス、アクション、チャネルまたはユーザーを含む詳細情報が表示されます。
- **iOSプロファイル:** 名前、タイプ、組織、説明を含む最新のiOSプロファイルインベントリを表示します。
- **iOSプロビジョニングプロファイル:** UUID、有効期限、管理ステータスなどのエンタープライズ配布プロビジョニングプロファイル情報を表示します。
- **証明書:** 有効、期限切れ、または失効した証明書について、タイプ、プロバイダー、発行者、シリアル番号、有効期限までの残り日数などの情報を表示します。
- **接続:** 最初の接続ステータスと最後の接続ステータスを表示します。各接続について、ユーザー名、前回の認証時刻、および最後の認証時刻を提供します。
- **MDMステータス:** MDMステータス、最終プッシュ時刻、最終デバイス応答時刻などの情報を表示します。

iOSデバイスポリシーを構成する

これらのポリシーを使用して、Citrix Endpoint ManagementがiOSまたはiPadOSを実行しているデバイスとどのように連携するかを構成します。この表は、iOSおよびiPadOSデバイスで利用可能なすべてのデバイスポリシーを一覧表示します。

AirPlayミラーリング	AirPrint	APN	
アプリのアクセス	アプリの属性	アプリの構成	
アプリのインベントリ	アプリのロック	アプリのアンインストール	
アプリの通知	ブルートゥース	カレンダー (CalDAV)	
モバイルデータ通信	連絡先 (CardDAV)	資格情報	
デバイス名	教育構成	エクスチェンジ	

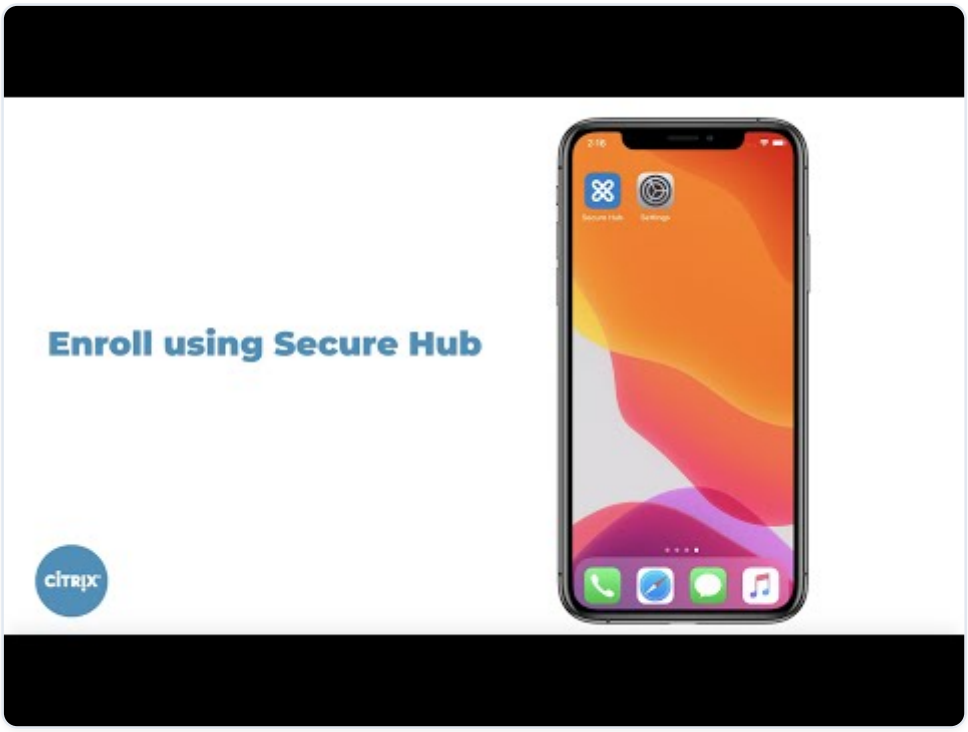
© 1997–2026 Citrix Systems, Inc. All rights reserved.

フォント	ホーム画面のレイアウト	iOS および macOS プロファイルのインポート	
LDAP	位置情報	ロック画面メッセージ	
メール	管理対象ドメイン	最大常駐ユーザー	
MDMオプション	ネットワーク	ネットワーク使用状況	
組織情報	OSアップデート	パスコード	
パスコードロック猶予期間	パーソナルホットスポット	プロファイルの削除	
プロビジョニングプロファイル	プロビジョニングプロファイルの削除	プロキシ	
制限	ローミング	SCEP	
SSOアカウント	ストア	購読カレンダー	
利用規約	VPN	壁紙	
Webコンテンツフィルター	Webクリップ		

iOSデバイスを登録する

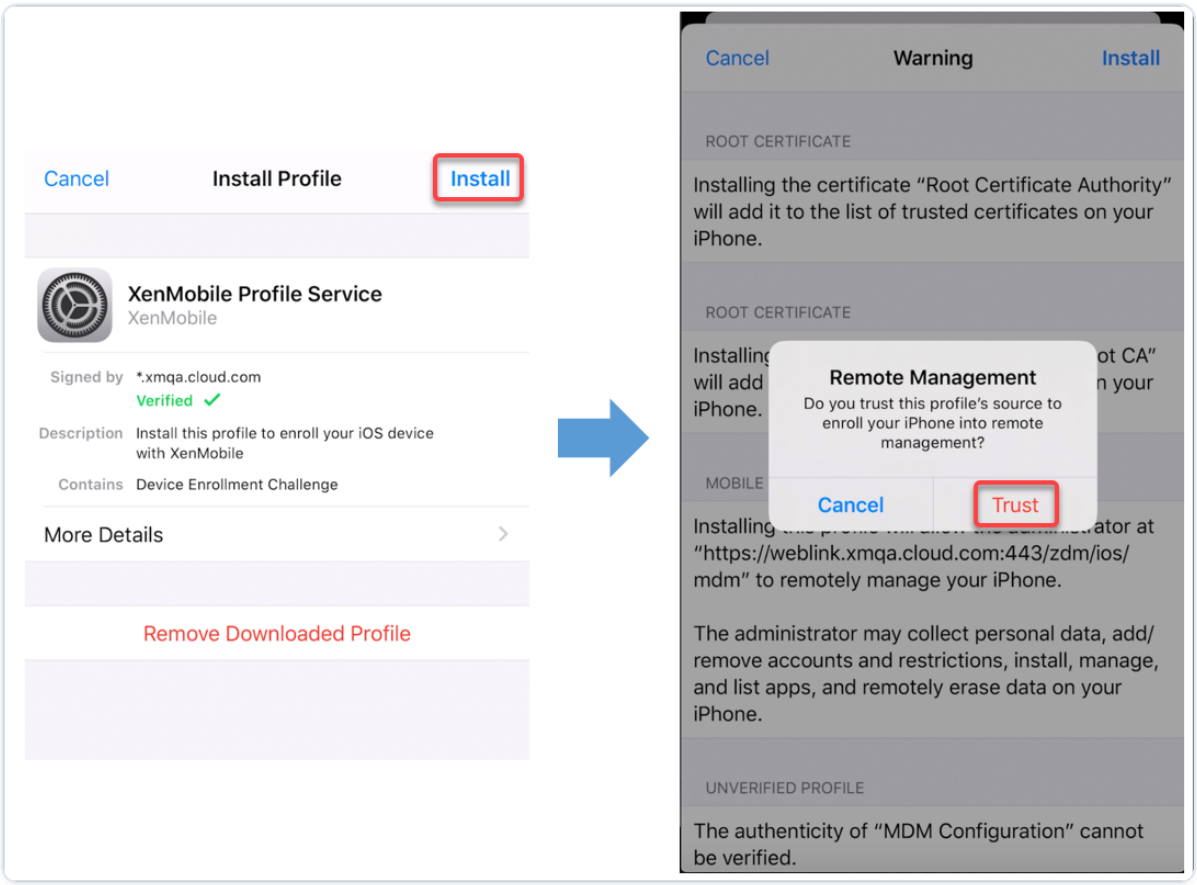
このセクションでは、ユーザーがiOSデバイス（12.2以降）をCitrix Endpoint Managementに登録する方法について説明します。iOS登録の詳細については、次のビデオをご覧ください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. iOSデバイスでApple Storeにアクセスし、Citrix Secure Hubアプリをダウンロードして、アプリをタップします。
2. アプリのインストールを求められたら、**次へ**をタップし、**インストール**をタップします。
3. Citrix Secure Hubのインストールが完了したら、**開く**をタップします。
4. 会社の資格情報（Citrix Endpoint Managementサーバー名、ユーザープリンシパル名（UPN）、メールアドレスなど）を入力します。次に、**次へ**をクリックします。
5. iOSデバイスを登録するには、**はい、登録**をタップします。
6. Citrix Endpoint Managementが収集するデータの一覧が表示されます。**次へ**をクリックします。組織がそのデータをどのように使用するかの説明が表示されます。**次へ**をクリックします。
7. 資格情報を入力したら、プロンプトが表示されたら**許可**をタップして構成プロファイルをダウンロードします。構成プロファイルをダウンロードしたら、**閉じる**をタップします。
8. デバイス設定で、XenMobile®プロファイルをインストールします。
   - **設定 > 一般 > プロファイル > XenMobile Profile Service**に移動し、**インストール**をタップしてプロファイルを追加します。
   - 通知ウィンドウで、**信頼**をタップしてデバイスをリモート管理に登録します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. 登録が成功したら、Citrix Secure Hubを開きます。MDM+MAMに登録する場合：資格情報が検証された後、プロンプトが表示されたらCitrix PINを作成して確認します。
10. ワークフローが完了すると、デバイスが登録されます。その後、アプリストアにアクセスして、iOSデバイスにインストールできるアプリを表示できます。

セキュリティアクション

iOSのデバイス登録では、次のセキュリティアクションがサポートされています。各セキュリティアクションの説明については、「セキュリティアクション」を参照してください。

- アクティベーションロックバイパス
- アプリロック
- アプリワイプ
- ASMアクティベーションロック
- 証明書の更新
- 制限の解除
- 紛失モードの有効化/無効化
- 追跡の有効化/無効化
- 完全ワイプ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 位置特定
- ロック
- 着信音を鳴らす
- AirPlayミラーリングの要求/停止
- 再起動/シャットダウン
- 失効/承認
- 選択的ワイプ
- ロック解除

iOSのユーザー登録では、以下のセキュリティアクションがサポートされています。

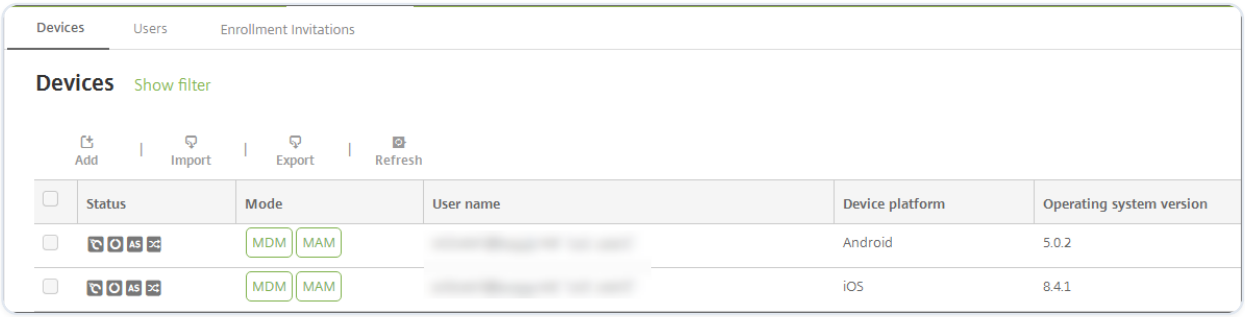
- 失効
- ロック
- 選択的ワイプ
- 証明書の更新

iOSデバイスをロックする

紛失したiOSデバイスをロックし、デバイスのロック画面にメッセージと電話番号を表示できます。

ロックされたデバイスにメッセージと電話番号を表示するには、Citrix Endpoint Management コンソールで パスコード ポリシーを **true** に設定します。代わりに、ユーザーはデバイスでパスコードを手動で有効にできます。

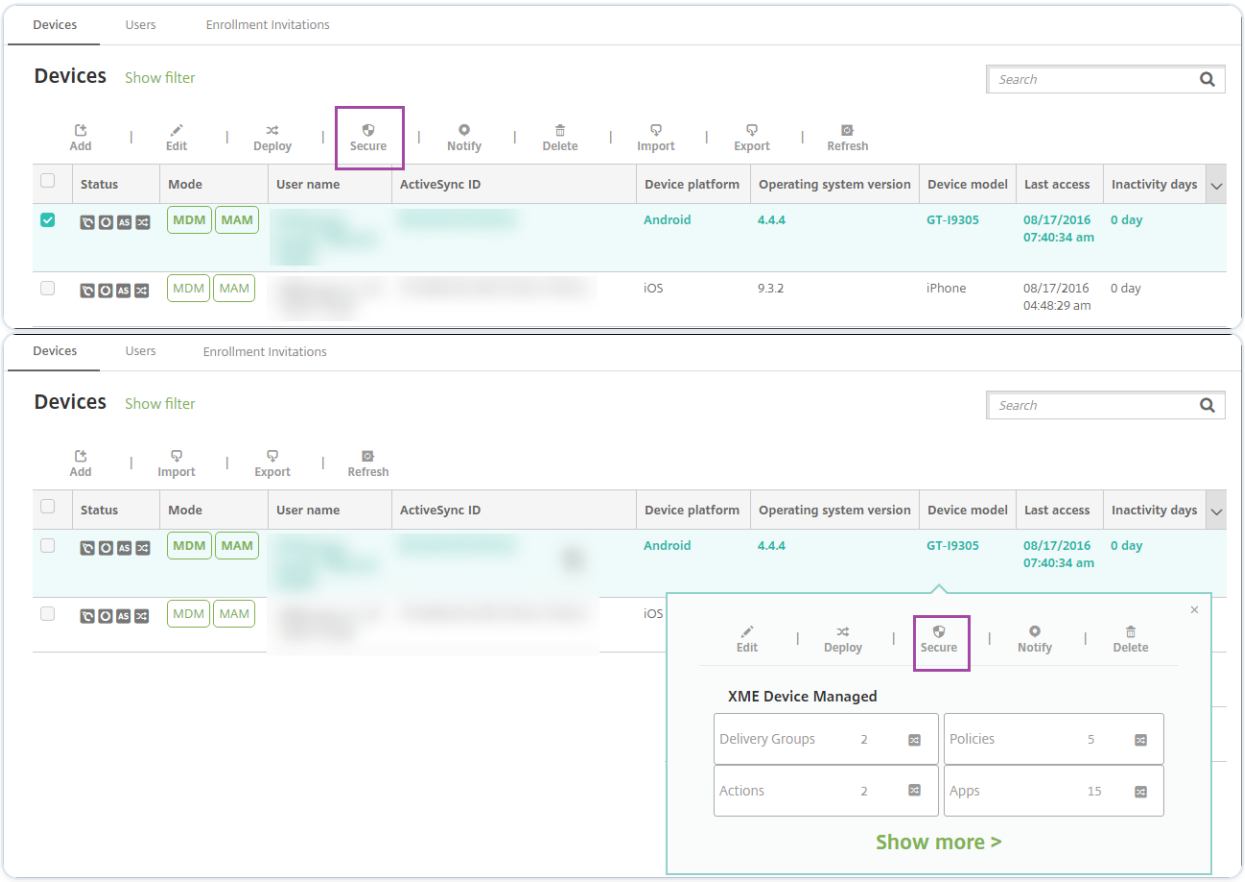
1. **管理 > デバイス** をクリックします。**デバイス** ページが表示されます。



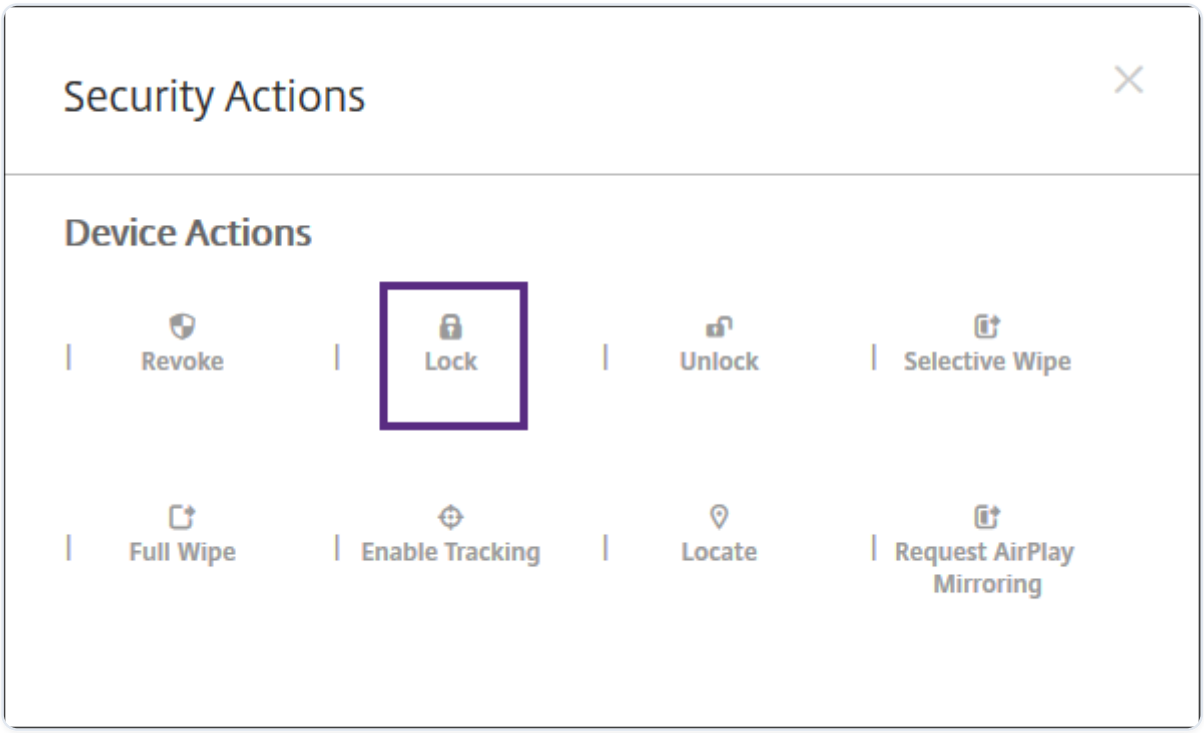
2. ロックするiOSデバイスを選択します。

   デバイスの横にあるチェックボックスを選択して、デバイスリストの上にオプションメニューを表示します。リスト内の他の場所をクリックすると、リストの右側にオプションメニューが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. オプションメニューで、**セキュリティ保護** をクリックします。**セキュリティアクション** ダイアログボックスが表示されます。



4. **ロック** をクリックします。**セキュリティアクション** 確認ダイアログボックスが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「セキュリティアクションの確認」(/en-us/citrix-endpoint-management/media/manage-devices-ios-secure-device-confirm.png)

5. オプションで、デバイスのロック画面に表示されるメッセージと電話番号を入力します。

   iOSは、**メッセージ**フィールドに入力した内容に「Lost iPad」という単語を追加します。

   メッセージフィールドを空のままにして電話番号を提供すると、Appleはデバイスのロック画面に「Call owner」というメッセージを表示します。

6. **デバイスをロック**をクリックします。

iOSデバイスを紛失モードにする

Citrix Endpoint Managementの紛失モードデバイスプロパティは、iOSデバイスを紛失モードにします。Apple Managed Lost Modeとは異なり、Citrix Endpoint Managementの紛失モードでは、ユーザーがデバイスの位置を特定できるようにするために、次のいずれかのアクションを実行する必要はありません。**iPhone/iPadを探す**設定を構成するか、Citrix Secure Hubのロケーションサービスを有効にする。

Citrix Endpoint Managementの紛失モードでは、Citrix Endpoint Managementのみがデバイスのロックを解除できます。（対照的に、Citrix Endpoint Managementのデバイスロック機能を使用する場合、ユーザーは提供されたPINコードを使用してデバイスのロックを直接解除できます。

紛失モードを有効または無効にするには：**管理 > デバイス**に移動し、監視対象のiOSデバイスを選択してから、**セキュリティ**をクリックします。次に、**紛失モードを有効にする**または**紛失モードを無効にする**をクリックします。

「紛失モードのオプション」(/en-us/citrix-endpoint-management/media/manage-devices-enable-lost-mode-button.png)

紛失モードを有効にするをクリックすると、紛失モードのときにデバイスに表示される情報を入力します。

「デバイスに表示される情報」(/en-us/citrix-endpoint-management/media/enable-lost-mode-dialog.png)

紛失モードのステータスを確認するには、次のいずれかの方法を使用します。

- **セキュリティアクション**ウィンドウで、ボタンが**紛失モードを無効にする**に設定されていることを確認します。
- **管理 > デバイス**から、**セキュリティ**の下にある**一般**タブで、最後の紛失モードを有効にするまたは紛失モードを無効にするアクションを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「全般」タブ(/en-us/citrix-endpoint-management/media/manage-devices-ios-lost-mode.png)

- **「管理」>「デバイス」で、「プロパティ」タブの「MDM紛失モード有効」**設定の値が正しいことを確認します。

「MDM紛失モード有効」設定(/en-us/citrix-endpoint-management/media/manage-devices-details-properties.png)

iOSデバイスでCitrix Endpoint Management紛失モードを有効にすると、Citrix Endpoint Managementコンソールも次のように変更されます。

- **「構成」>「アクション」では、「アクション」リストに次の自動アクションは含まれません: 「デバイスの取り消し」、「デバイスの選択的ワイプ」、「デバイスの完全ワイプ」**。
- **「管理」>「デバイス」では、「セキュリティアクション」リストに「取り消し」および「選択的ワイプ」デバイスアクションは含まれなくなります。必要に応じて、セキュリティアクションを使用して「完全ワイプ」**アクションを実行できます。

iOSは、**「セキュリティアクション」画面の「メッセージ」**に入力した内容に「Lost iPad」という単語を追加します。

「メッセージ」を空のままにして電話番号を提供すると、Appleはデバイスのロック画面に「Call owner」というメッセージを表示します。

iOSアクティベーションロックをバイパスする

アクティベーションロックは、「iPhone/iPadを探す」の機能であり、紛失または盗難された監視対象デバイスの再アクティベーションを防止します。アクティベーションロックでは、「iPhone/iPadを探す」をオフにする、デバイスを消去する、またはデバイスを再アクティベートするなどのアクションを実行する前に、ユーザーのApple IDとパスワードが必要です。組織が所有するデバイスの場合、たとえばデバイスをリセットまたは再割り当てするために、アクティベーションロックをバイパスする必要があります。

アクティベーションロックを有効にするには、Citrix Endpoint Management MDMオプションデバイスポリシーを構成して展開します。これにより、ユーザーのApple資格情報なしでCitrix Endpoint Managementコンソールからデバイスを管理できます。アクティベーションロックのApple資格情報要件をバイパスするには、Citrix Endpoint Managementコンソールからアクティベーションロックバイパスセキュリティアクションを発行します。

たとえば、ユーザーが紛失した電話を返却した場合、または完全ワイプの前後にデバイスをセットアップする場合: 電話がApple App Storeアカウントの資格情報を要求したとき、アクティベーションロックバイパスセキュリティアクションを発行してその手順をバイパスします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アクティベーションロックバイパスのデバイス要件

- Apple ConfiguratorまたはApple Deployment Programによって監視されている
- iCloudアカウントで構成されている
- 「iPhone/iPadを探す」が有効
- Citrix Endpoint Managementに登録済み
- アクティベーションロックが有効になっているMDMオプションデバイスポリシーがデバイスに展開されている

デバイスの完全ワイプを実行する前にアクティベーションロックをバイパスするには：

1. > に移動し、デバイスを選択して をクリックし、 をクリックします。
2. デバイスをワイプします。デバイスのセットアップ中にアクティベーションロック画面は表示されません。

デバイスの完全ワイプを実行した後にアクティベーションロックをバイパスするには：

1. デバイスをリセットまたはワイプします。デバイスのセットアップ中にアクティベーションロック画面が表示されます。
2. > に移動し、デバイスを選択して をクリックし、 をクリックします。
3. デバイスの戻るボタンをタップします。ホーム画面が表示されます。

次の点に注意してください。

- ユーザーに「iPhone/iPadを探す」をオフにしないようにアドバイスしてください。デバイスから完全ワイプを実行しないでください。どちらの場合も、ユーザーはiCloudアカウントのパスワードの入力を求められます。アカウントの検証後、すべてのコンテンツと設定を消去しても、ユーザーに「iPhone/iPadをアクティベート」画面は表示されません。
- アクティベーションロックバイパスコードが生成され、アクティベーションロックが有効になっているデバイスの場合：完全ワイプ後に「iPhone/iPadをアクティベート」ページをバイパスできない場合でも、Citrix Endpoint Managementからデバイスを削除する必要はありません。管理者またはユーザーがAppleサポートに直接連絡して、デバイスのブロックを解除できます。
- ハードウェアインベントリ中に、Citrix Endpoint Managementはデバイスにアクティベーションロックバイパスコードを照会します。バイパスコードが利用可能な場合、デバイスはそれをCitrix Endpoint Managementに送信します。その後、デバイスからバイパスコードを削除するには、Citrix Endpoint Managementコンソールからアクティベーションロックバイパスセキュリティアクションを送信します。その時点で、Citrix Endpoint ManagementとAppleはデバイスのブロックを解除するために必要なバイパスコードを保持しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- アクティベーションロックバイパスセキュリティアクションは、Appleサービスの可用性に依存します。アクションが機能しない場合は、次のいずれかの方法でデバイスのブロックを解除できます。
  - デバイスで、iCloudアカウントの資格情報を手動で入力します。
  - ユーザー名フィールドを空のままにし、パスワードフィールドにバイパスコードを入力します。バイパスコードを検索するには、 > に移動し、デバイスを選択し、 をクリックし、をクリックします。 は の下にあります。

macOS

Citrix Endpoint Management で macOS デバイスを管理するには、Apple から Apple Push Notification service (APNs) 証明書をセットアップします。詳しくは、「APNs 証明書」(/ja-jp/citrix-endpoint-management/authentication/apns.html)を参照してください。

Citrix Endpoint Management は、macOS デバイスを MDM に登録します。Citrix Endpoint Management は、MDM の macOS デバイスに対して、次の登録認証タイプをサポートしています。

- ドメイン
- ドメインとワンタイムパスワード
- 招待 URL とワンタイムパスワード

MACOS 15 での信頼された証明書の要件:

Apple は、TLS サーバー証明書に関する新しい要件を設けています。すべての証明書が新しい Apple の要件に準拠していることを確認してください。Apple の公開情報 `<https://support.apple.com/ja-jp/HT210176>` を参照してください。証明書の管理については、「証明書のアップロード」(/ja-jp/citrix-endpoint-management/authentication/upload-renew-certificates.html#upload-certificates)を参照してください。

macOS デバイス管理を開始するための一般的なワークフローは次のとおりです。

1. オンボーディングプロセスを完了します。「オンボーディングとリソースのセットアップ」(/ja-jp/citrix-endpoint-management/onboarding-and-resource-setup.html)および「デバイスの登録とリソースの配信の準備」(/ja-jp/citrix-endpoint-management/prepare-to-enroll-devices-and-deliver-resources.html)を参照してください。
2. 登録方法を選択して構成します。「サポートされている登録方法」(#supported-enrollment-methods)を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 「macOS デバイスポリシーの構成」(#configure-macos-device-policies)。
4. 「macOS デバイスの登録」(#enroll-macos-devices)。
5. デバイスとアプリのセキュリティアクションをセットアップします。「セキュリティアクション」(#security-actions)を参照してください。

サポートされているオペレーティングシステムについては、「サポートされているデバイスオペレーティングシステム」(/ja-jp/citrix-endpoint-management/system-requirements/supported-device-platforms.html)を参照してください。

開放しておく必要があるAppleホスト名

iOS、macOS、およびApple App Storeが適切に動作するためには、一部のAppleホスト名を開放しておく必要があります。これらのホスト名をブロックすると、iOS、iOSアプリ、MDMの操作、デバイスおよびアプリの登録のインストール、更新、および適切な動作に影響を与える可能性があります。詳細については、`<https://support.apple.com/ja-jp/HT201999>`を参照してください。

サポートされている登録方法

次の表に、Citrix Endpoint ManagementがmacOSデバイスでサポートする登録方法を示します。

方法	サポート
Apple導入プログラム	はい
Apple スクールマネージャー	はい
アップルコンフィグレータ	いいえ
手動登録	はい
登録招待	はい

Appleには、ビジネスアカウントと教育機関アカウント向けのデバイス登録プログラムがあります。ビジネスアカウントの場合、Citrix Endpoint Managementでのデバイスの登録と管理にApple Deployment Programを使用するには、Apple Deployment Programに登録します。このプログラムは、iOS、macOS、およびApple TVデバイスに対応しています。「Apple Deployment Programを介したデバイスの展開」(/ja-jp/citrix-endpoint-management/device-management/apple/apple-deployment-program.html)を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

教育機関アカウントの場合、Apple School Managerアカウントを作成します。Apple School Managerは、Deployment ProgramとVolume Purchaseを統合します。Apple School Managerは、Education Apple Deployment Programの一種です。「Apple Education機能との統合」(/ja-jp/citrix-endpoint-management/device-management/apple/integrate-with-apple-education.html)を参照してください。

Apple Deployment Programを使用して、iOS、macOS、およびApple TVデバイスを一括登録できます。これらのデバイスは、Apple、参加しているApple正規販売店、または通信事業者から直接購入できます。

macOSデバイスポリシーを構成する

これらのポリシーを使用して、Citrix Endpoint ManagementがmacOSを実行しているデバイスとどのように連携するかを構成します。この表には、macOSデバイスで利用可能なすべてのデバイスポリシーが一覧表示されています。

AirPlayミラーリング	アプリインベントリ	アプリのアンインストール
カレンダー (CalDAV)	連絡先 (CardDAV)	資格情報
デバイス名	エクスチェンジ	FileVault
ファイアウォール	フォント	iOSおよびmacOSプロファイルのインポート

OSアップデート	パスコード	プロファイルの削除
制限	SCEP	VPN
Webクリップ		

macOSデバイスの登録

Citrix Endpoint Managementは、macOSを実行しているデバイスを登録するための2つの方法を提供します。どちらの方法でも、macOSユーザーはデバイスから直接、ワイヤレスで登録できます。

- **ユーザーに登録招待を送信:** この登録方法では、macOSデバイスに対して以下のいずれかの登録セキュリティモードを設定できます。
    - ユーザー名 + パスワード

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ユーザー名 + PIN
- 2要素認証

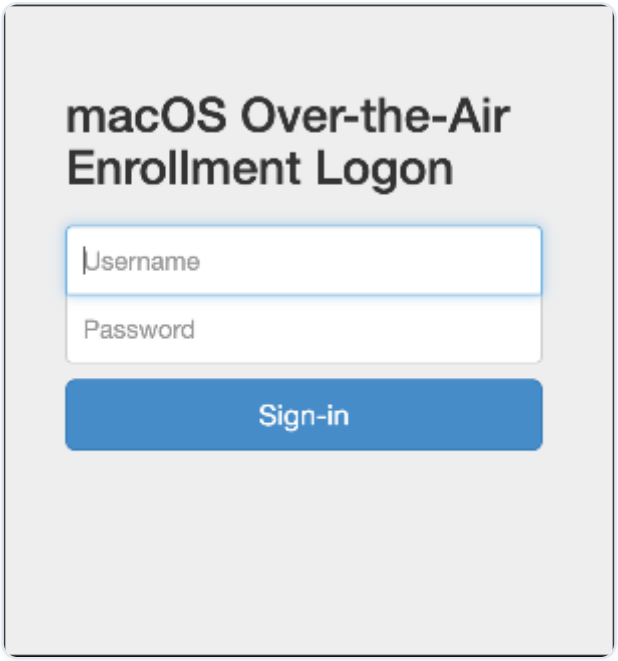
ユーザーが登録招待の指示に従うと、ユーザー名が入力済みのサインオン画面が表示されます。

- **ユーザーに登録リンクを送信:** macOSデバイス向けのこの登録方法では、ユーザーに登録リンクが送信され、ユーザーはそのリンクをSafariまたはChromeブラウザーで開くことができます。その後、ユーザーはユーザー名とパスワードを入力して登録します。

  macOSデバイスで登録リンクの使用を禁止するには、サーバープロパティ **Enable macOS OTAE** を **false** に設定します。その結果、macOSユーザーは登録招待を使用することによってのみ登録できます。

macOSユーザーに登録招待を送信する

1. macOSユーザー登録の招待を追加します。登録招待を参照してください。
2. ユーザーが招待を受け取り、リンクをクリックすると、Safariブラウザーに次の画面が表示されます。Citrix Endpoint Managementがユーザー名を入力します。登録セキュリティモードに **Two Factor** を選択した場合、別のフィールドが表示されます。



3. ユーザーは必要に応じて証明書をインストールします。ユーザーに証明書のインストールを促すプロンプトが表示されるかどうかは、macOS用に以下を設定したかどうかによって異なります：公開されている信頼されたSSL証明書と、公開されている信頼されたデジタル署名証明書。証明書については、証明書と認証を参照してください。
4. ユーザーは要求された資格情報を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Macデバイスポリシーがインストールされます。これで、モバイルデバイスを管理するのと同じように、Citrix Endpoint ManagementでmacOSデバイスの管理を開始できます。

macOSユーザーにインストールリンクを送信する

1. ユーザーがSafariまたはChromeブラウザで開くことができる登録リンク`https://serverFQDN:8443/instanceName/macos/otae`を送信します。

   - **serverFQDN**は、Citrix Endpoint Managementを実行しているサーバーの完全修飾ドメイン名 (FQDN) です。
   - ポート**8443**はデフォルトのセキュアポートです。別のポートを設定した場合は、8443の代わりにそのポートを使用してください。
   - **instanceName**は、多くの場合`zdm`として表示され、サーバーのインストール時に指定された名前です。

   インストールリンクの送信の詳細については、「(/ja-jp/citrix-endpoint-management/device-management.html#to-send-an-installation-link)」を参照してください。
2. ユーザーは必要に応じて証明書をインストールします。iOSおよびmacOS用に公開信頼されたSSL証明書とデジタル署名証明書を設定した場合、ユーザーには証明書をインストールするよう求めるプロンプトが表示されます。証明書に関する情報については、「証明書と認証」を参照してください。
3. ユーザーはMacにサインオンします。

   Macデバイスポリシーがインストールされます。これで、モバイルデバイスを管理するのと同じように、Citrix Endpoint ManagementでmacOSデバイスの管理を開始できます。

セキュリティアクション

macOSは以下のセキュリティアクションをサポートしています。各セキュリティアクションの説明については、「セキュリティアクション」を参照してください。

取り消し	ロック	選択的ワイプ
完全ワイプ	証明書の更新	個人用回復キーをローテーションする

macOSデバイスをロックする

紛失したmacOSデバイスをリモートでロックできます。Citrix Endpoint Managementはデバイスをロックします。その後、PINコードを生成し、デバイスに設定します。デバイスにアクセスするに

© 1997–2026 Citrix Systems, Inc. All rights reserved.

は、ユーザーはPINコードを入力します。Citrix Endpoint Managementコンソールからロックを解除するには、**Cancel Lock**を使用します。

PINコードに関連する詳細設定を構成するには、パスコードデバイスポリシーを使用できます。詳細については、macOS設定を参照してください。

1. **管理 > デバイス**をクリックします。**デバイス**ページが表示されます。

   デバイスページ(/en-us/citrix-endpoint-management/media/manage-devices-macos.png)

2. ロックするmacOSデバイスを選択します。

   デバイスの横にあるチェックボックスを選択すると、デバイスリストの上にオプションメニューが表示されます。リストされた項目の他の場所をクリックして、リストの右側にオプションメニューを表示することもできます。

   オプションメニュー(/en-us/citrix-endpoint-management/media/manage-devices-with-commands-secure-macos.png)

   オプションメニュー(/en-us/citrix-endpoint-management/media/manage-devices-with-commands-secure-macos-2.png)

3. オプションメニューで、**セキュリティ**をクリックします。**セキュリティアクション**ダイアログボックスが表示されます。

   セキュリティアクションダイアログボックス(/en-us/citrix-endpoint-management/media/manage-devices-secure-lock-macos.png)

4. **ロック**をクリックします。**セキュリティアクション**確認ダイアログボックスが表示されます。

   セキュリティアクションの確認(/en-us/citrix-endpoint-management/media/manage-devices-ios-secure-device-confirm-macos.png)

5. **デバイスのロック**をクリックします。

重要:

Citrix Endpoint Managementが生成するコードを使用する代わりに、パスコードを指定することもできます。指定されたコードがデバイスまたは既存のワークプロファイルのコード要件を満たしていない場合、ロックアクションは失敗します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ブートストラップトークン

ブートストラップトークンは、macOSデバイスにサインオンする際に、アカウントにSecureToken macOS属性を付与するのに役立ちます。SecureTokenは、信頼されたアカウントから別のアカウントへと引き継がれます。SecureTokenが有効なアカウントは、デバイス上で暗号化操作を実行できます。ブートストラップトークンがない場合、個々のユーザーアカウントを追加する前に、そのデバイスでアカウントを作成するために複雑なワークフローに従う必要があります。

Citrix Endpoint Managementは、Apple Deployment Programを通じて登録されたmacOSデバイスのブートストラップトークンのエスクローをサポートしています。Apple Deployment Programは、Apple、参加しているApple正規販売店、または通信事業者から直接購入したmacOSデバイスを登録するために使用します。Apple Deployment Programへの登録については、「Apple Deployment Programによるデバイスの展開」を参照してください。

ブートストラップトークンは、設定アシスタントのワークフロー中に生成されます。具体的には、ローカルユーザーアカウントの作成中に生成されます。設定アシスタントは、ユーザーがデバイスを初めて起動したときに実行されます。トークンはCitrix Endpoint Managementデータベースに保存され、管理者やエンドユーザーには表示されません。Citrix Endpoint Managementサイトからデバイスを削除すると、トークンも削除されます。工場出荷時設定にリセットしても、トークンは削除されません。

前提条件:

- macOS 11.0 以降
- Apple T2 Security Chipを搭載したmacOSデバイス
- Apple Deployment Programを通じて登録されたmacOSデバイス

Citrix Endpoint Managementでブートストラップトークンをエスクローする利点の1つは、リモートアカウントでFileVaultを有効にし、FileVaultボリュームのロックを解除できることです。FileVaultの詳細については、「FileVaultデバイスポリシー」を参照してください。

Apple Deployment Programs を介したデバイスの展開

Apple Deployment Programs (ADP) を使用すると、ユーザーがデバイスを受け取る前にデバイスに触れたり準備したりすることなく、Apple デバイスを Citrix Endpoint Management に自動的に登録できます。ユーザーがデバイスを開梱してアクティベートすると、デバイスは自動的に Citrix Endpoint Management に登録され、すべての管理設定、アプリ、およびブックがユーザーのために準備されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ADP には、ビジネス組織向けの Apple Business Manager (ABM) と、教育機関向けの Apple School Manager (ASM) が含まれます。ABM と ASM は、iOS、iPadOS、および macOS デバイスで利用できます。デバイスの適格性の詳細については、「Apple Business Manager ユーザーガイド」および「Apple School Manager ユーザーガイド」を参照してください。

注：

ABM と ASM は、Apple の以前の Device Enroll Program と Volume Purchase Program を統合したものです。

この記事では、ABM または ASM を使用した一般的な展開ワークフローについて説明します。

1. ABM または ASM に登録する
2. ABM または ASM アカウントを Citrix Endpoint Management に接続する
3. デバイスを注文する
4. デバイスを Citrix Endpoint Management に割り当てる
5. コンテンツをまとめて購入し、Citrix Endpoint Management と同期する
6. デバイスポリシーとアプリの展開ルールを構成する
7. ユーザーとリソースが割り当てられているデリバリーグループを追加する

この展開プロセスが完了すると、デバイスは開梱され、自動デバイス登録のためにアクティベートされる準備が整います。

前提条件

Citrix Endpoint ManagementとApple間の接続に必要なポートを開きます。詳細については、「ポート要件」を参照してください。

ABMまたはASMに登録する

Appleでデバイスの展開を開始するには、ABMまたはASMに登録します。

ABMとASMは個人ではなく組織向けに提供されています。アカウントを作成するには、多くの組織の詳細と情報を提供する必要があります。アカウントの申請と承認には時間がかかる場合があります。

ABMに登録する

ABMに登録するには、business.apple.comにアクセスします。**Enroll now**をクリックして、新しいアカウントを申請します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ベストプラクティスは、`deployment@company.com`のような組織のメールアドレスを使用することです。登録プロセスには数日かかる場合があります。ログオン資格情報を受け取ったら、ABMに記載されている手順に従ってアカウントを作成します。

ASMに登録する

ASMアカウントを作成するには、Apple School Managerにアクセスし、登録手順に従います。ASMに初めてログインすると、セットアップアシスタントが開きます。

- ASMの前提条件、セットアップアシスタント、および管理タスクについては、「Apple School Managerユーザーガイド」を参照してください。
- ASMユーザーアカウントを設定する際は、Active Directoryのドメイン名とは異なるドメイン名を使用してください。たとえば、ASMのドメイン名の前に`appleid`のようなものを付けます。
- ASMを名簿データに接続すると、ASMは教員と生徒用にManaged Apple IDを作成します。名簿データには、教員、生徒、クラスが含まれます。ASMに名簿データを追加する方法については、このリストで前述したApple School Managerユーザーガイドを参照してください。
- このリストで前述したApple School Managerユーザーガイドに記載されているように、機関のManaged Apple ID形式をカスタマイズできます。

  重要:

  ASM情報をCitrix Endpoint Managementにインポートした後で、Managed Apple IDを変更しないでください。

- 再販業者または通信事業者を通じてデバイスを購入した場合は、それらのデバイスをASMにリンクしてください。詳細については、このリストで以前にリンクされているApple School Managerユーザーガイドを参照してください。

ABMまたはASMアカウントをCitrix Endpoint Managementに接続する

ABMまたはASMアカウントを作成したら、Citrix Endpoint Managementサーバー展開に接続します。

ステップ1：Citrix Endpoint Managementサーバーから公開キーをダウンロードする

1. Citrix Endpoint Managementコンソールで、 **>** に移動します。

   Apple展開プログラム設定画面のスクリーンショット(/en-us/citrix-endpoint-management/media/settings-apple-dep-enrollment-asm-1.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. で、 をクリックします。

ステップ2：Appleアカウントからサーバートークンファイルを作成してダウンロードする

1. 管理者またはデバイス登録マネージャーアカウントを使用して、Apple Business ManagerまたはApple School Managerにサインインします。
2. サイドバーの下部にある**** をクリックし、次に** > ** をクリックします。
3. 設定で、Citrix Endpoint Managementサーバーの名前を入力します。入力するサーバー名は参照用です。サーバーのURLや名前ではありません。
4. で、 をクリックします。Citrix Endpoint Managementからダウンロードした公開キーをアップロードし、変更を保存します。
5. をクリックして、サーバートークンファイルをコンピューターにダウンロードします。

   ABMまたはASMアカウントをCitrix Endpoint Managementに追加する際に、サーバートークンファイルをアップロードします。トークンファイルをインポートすると、Citrix Endpoint Managementコンソールにトークン情報が表示されます。
6. で、 をクリックします。デバイスの割り当て方法を選択し、要求された情報を提供します。詳細については、ABMユーザーガイドまたはApple School Managerユーザーガイドを参照してください。

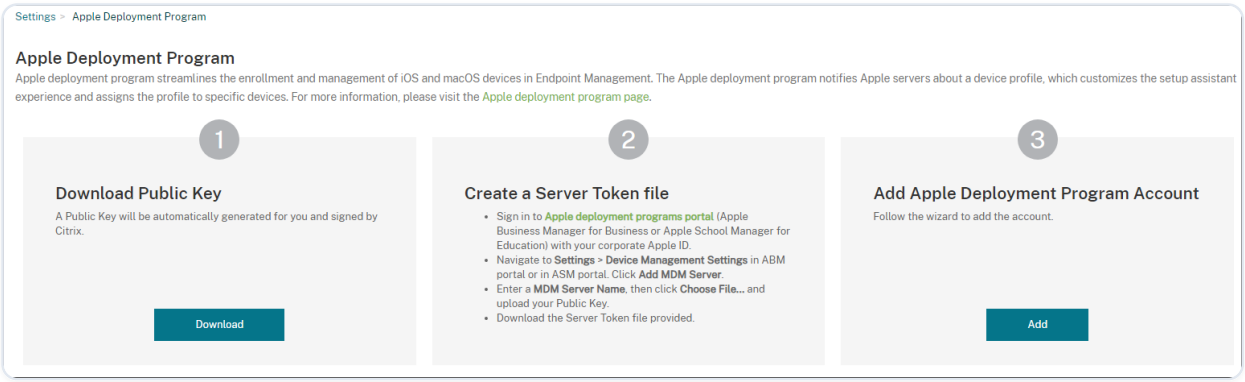
ステップ3：アカウントをCitrix Endpoint Managementに追加する

複数のABMまたはASMアカウントをCitrix Endpoint Managementに追加できます。この機能により、国、部門などに応じて異なる登録設定とセットアップアシスタントオプションを使用できます。その後、ABMまたはASMアカウントを異なるデバイスポリシーに関連付けます。

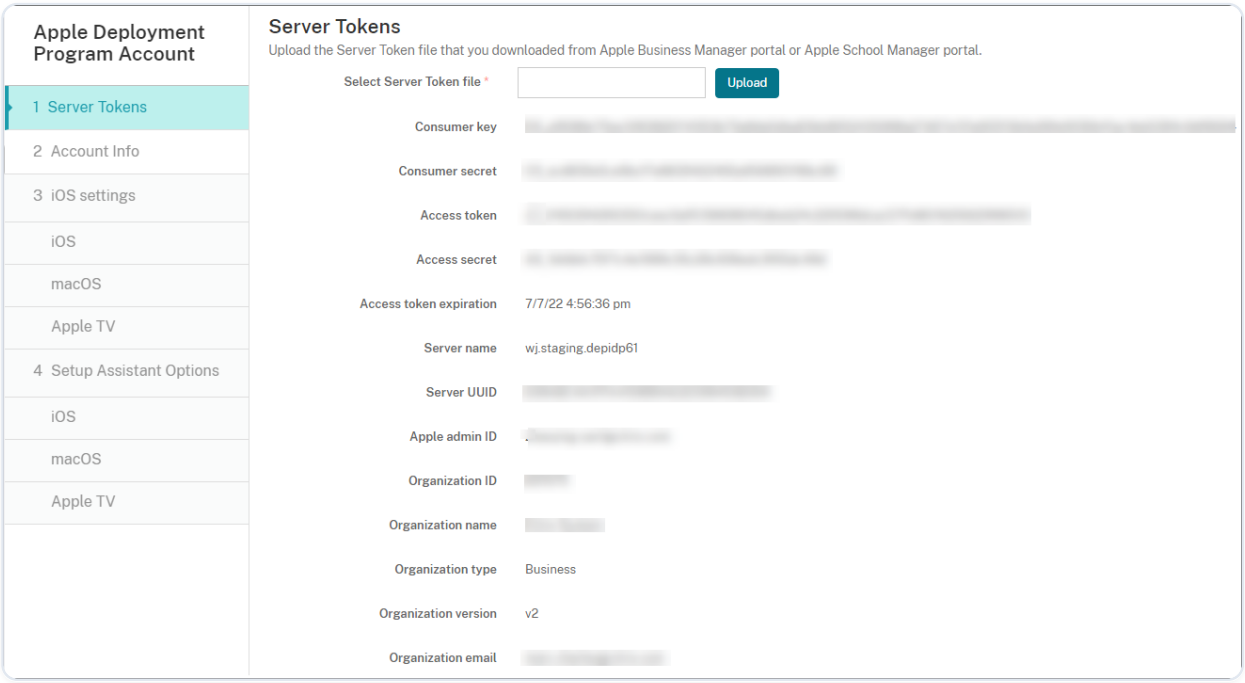
たとえば、異なる国からのすべてのABMまたはASMアカウントを同じCitrix Endpoint Managementサーバーに一元化して、すべてのABMまたはASMデバイスをインポートおよび監視できます。まず、部門、組織階層、またはその他の構造ごとに登録設定とセットアップアシスタントオプションをカスタマイズします。次に、組織全体で適切な機能を提供し、ユーザーが適切な支援を受けられるようにポリシーを構成します。

1. Citrix Endpoint Managementコンソールで、**［設定］>［Apple Deployment Program］**の順に移動し、**［Apple Deployment Programアカウントの追加］**の下にある**［追加］**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



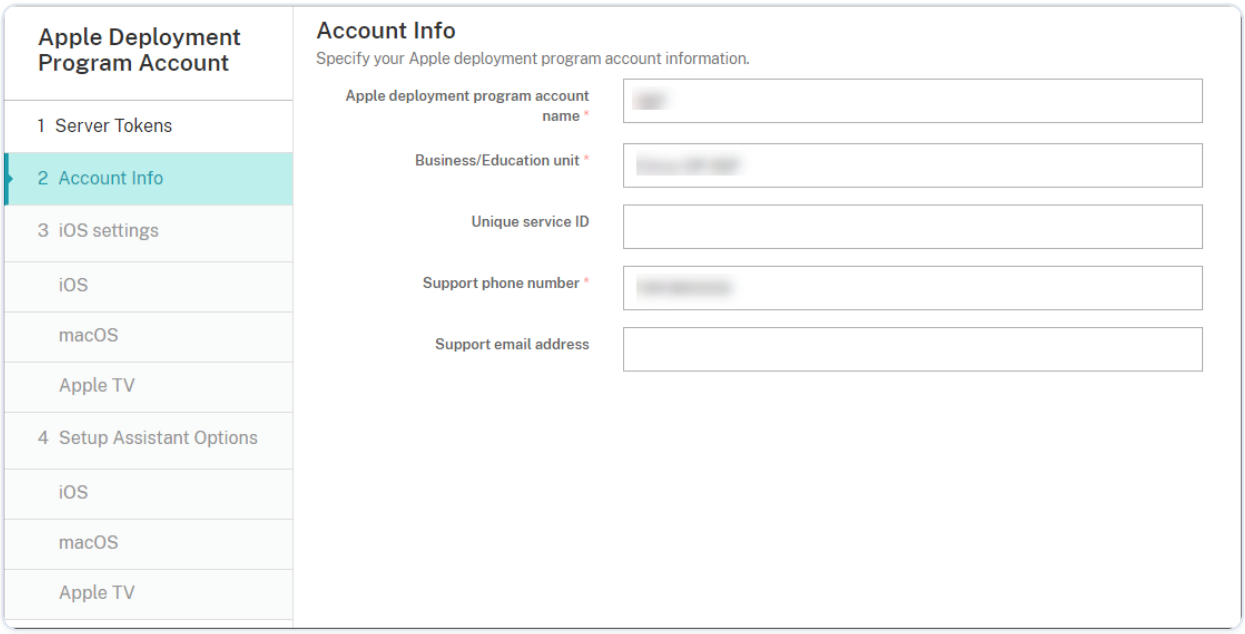
2. **［サーバーのトークン］ページで、サーバーのトークンファイルを指定し、［アップロード］**をクリックします。



サーバーのトークン情報が表示されます。

3. **［アカウント情報］**ページで、次の設定を指定します。

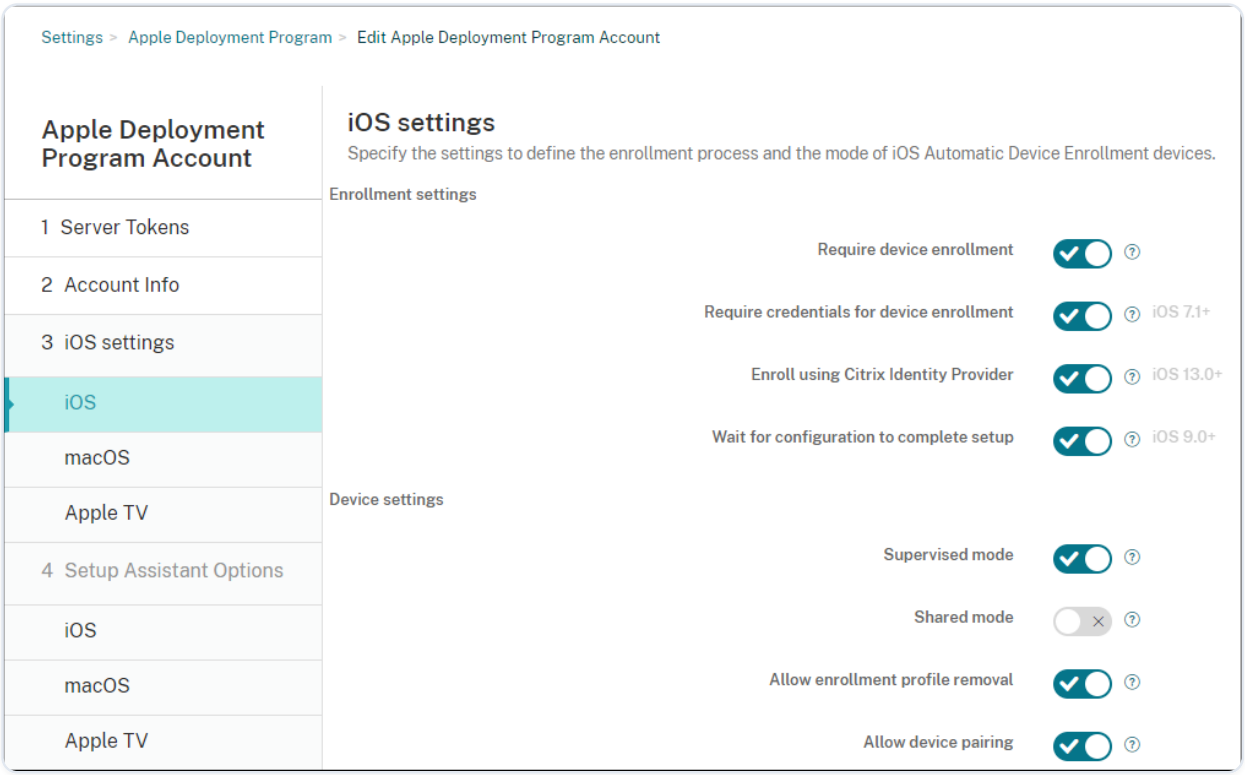
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Apple Deployment Programアカウント名：** このADPアカウントの一意の記述名。国や組織階層など、ADPアカウントをどのように整理するかを識別します。
- **ビジネス/教育ユニット：** デバイスが割り当てられているビジネスユニットまたは部門。このフィールドは必須です。
- **一意のサービスID：** アカウントをさらに識別するのに役立つオプションの一意のID。
- **サポート電話番号：** セットアップ中にユーザーがヘルプを求めるためのサポート電話番号。このフィールドは必須です。
- **サポートメールアドレス：** エンドユーザーが利用できるオプションのサポートメールアドレス。
- **教育サフィックス:** ASMアカウントの場合。このアカウントを通じて登録されたデバイスに割り当てられたサフィックスを入力します。

4. **iOS設定**で、次の設定を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



登録設定:

- **デバイス登録を必須にする:** ユーザーにデバイスの登録を要求するかどうか。デフォルトは**オン**です。
- **デバイス登録に資格情報を要求する:** ABMおよびASMのセットアップ中に、ユーザーに資格情報の入力を要求するかどうか。承認されたユーザーのみがデバイスを登録できるように、すべてのユーザーにデバイス登録中に資格情報を入力するよう要求することをお勧めします。デフォルトは**オン**です。

  初回セットアップの前にABMまたはASMを有効にし、このオプションを選択しない場合、Citrix Endpoint ManagementはABMまたはASMコンポーネントを作成します。この作成には、ユーザー、Citrix Secure Hub、ソフトウェアインベントリ、展開グループなどのコンポーネントが含まれます。このオプションを選択した場合、Citrix Endpoint Managementはコンポーネントを作成しません。その結果、後でこのオプションをクリアした場合、資格情報を入力していないユーザーは、これらのコンポーネントが存在しないため、ABMまたはASMに登録できません。その場合、ABMまたはASMコンポーネントを追加するには、ABMまたはASMアカウントを無効にしてから有効にします。
- **Citrix Identity Providerを使用して登録する:** Citrix Identity Providerを使用して登録するかどうか。この設定はABMアカウントでのみ利用可能です。**オン**の場合、ADPが有効なiOSデバイスはCitrix IDプロバイダーを使用してのみ登録されます。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

この設定をオンにするには、まずCitrix Identity ProviderをIDプロバイダーとして構成する必要があります。**設定 > IDプロバイダー (IDP)** に移動し、**追加**をクリックして、**Citrix Identity Provider**を選択します。

この設定が**オン**に設定されている場合、以下の考慮事項に注意してください。

- **設定 > IDプロバイダー (IDP)** ページで、対応するCitrix Identity Provider構成を削除することはできません。
- 対応するCitrix Identity Provider構成を編集する際、別のIDプロバイダーに切り替えることはできません。

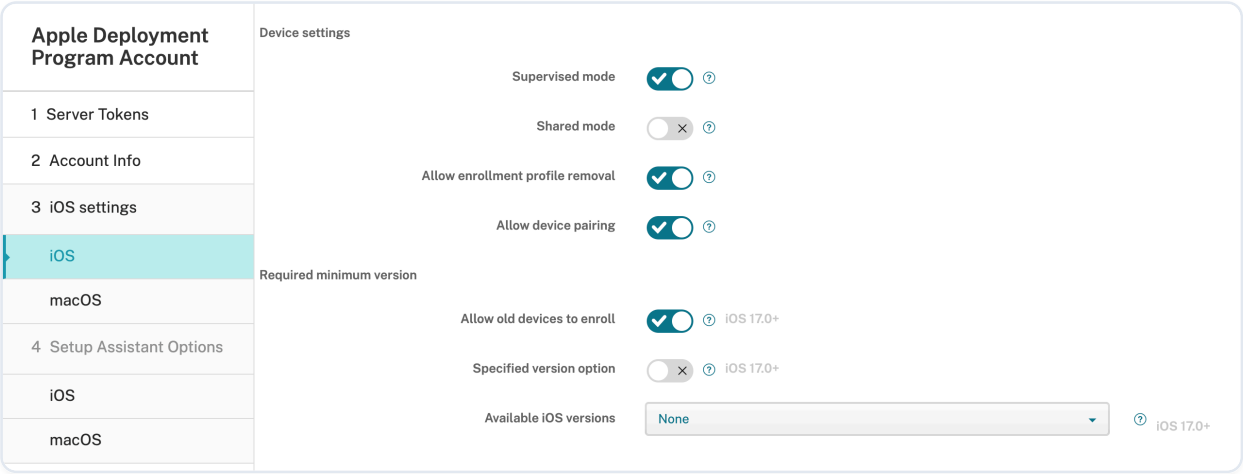
- **構成がセットアップを完了するまで待機する:** すべてのMDMリソースがデバイスに展開されるまで、ユーザーのデバイスをセットアップアシスタントモードにするかどうか。この設定は、監視モードのデバイスで利用できます。デフォルトは**オフ**です。
- Appleのドキュメントによると、デバイスがセットアップアシスタントモードの場合、以下のコマンドが機能しない可能性があります。
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

デバイス設定:

- **監視モード:** 登録済みデバイスの管理にApple Configuratorを使用している場合、または**構成がセットアップを完了するまで待機**が有効になっている場合は、**オン**に設定します。デフォルトは**オン**です。iOSデバイスを監視モードにする方法の詳細については、「Apple Configurator 2を使用してデバイスを展開する」を参照してください。
- **登録プロファイルの削除を許可:** デバイスがリモートで削除できるプロファイルを使用することを許可するかどうか。デフォルトは**オフ**です。
- **デバイスのペアリングを許可:** Apple MusicおよびApple Configuratorを介して登録済みデバイスを管理できるかどうか。デフォルトは**オフ**です。

必須の最小バージョン

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **古いデバイスの登録を許可:** 有効にすると、現在の必須最小バージョンにアップグレードできなかったデバイスでも登録できます。デフォルトはオンです。このオプションはiOS 17.0以降でのみ利用可能です。
- **指定バージョンオプション:** 管理者が指定バージョンを手動で入力することを許可するかどうか。デフォルトは**オフ**です。このオプションはiOS 17.0以降でのみ利用可能です。
- **利用可能なiOSバージョン:** リストから利用可能なiOSバージョンを選択できます。デバイスのiOSバージョンが現在のバージョンよりも低い場合、デバイスで更新プロセスが開始されます。将来的にバージョンが期限切れになった場合、利用可能なバージョンリストの最小バージョンが使用されます。デフォルトはNoneです。Noneに設定した場合、効果はありません。このオプションはiOS 17.0以降でのみ利用可能です。
- **指定バージョン:** デバイスのiOSバージョンが現在のバージョンよりも低い場合、デバイスで更新プロセスが開始されます。将来的にバージョンが期限切れになった場合、利用可能なバージョンリストの最小バージョンが使用されます。正しいバージョン番号を入力してください。そうしないと、不明なエラーが発生する可能性があります。

監視ID

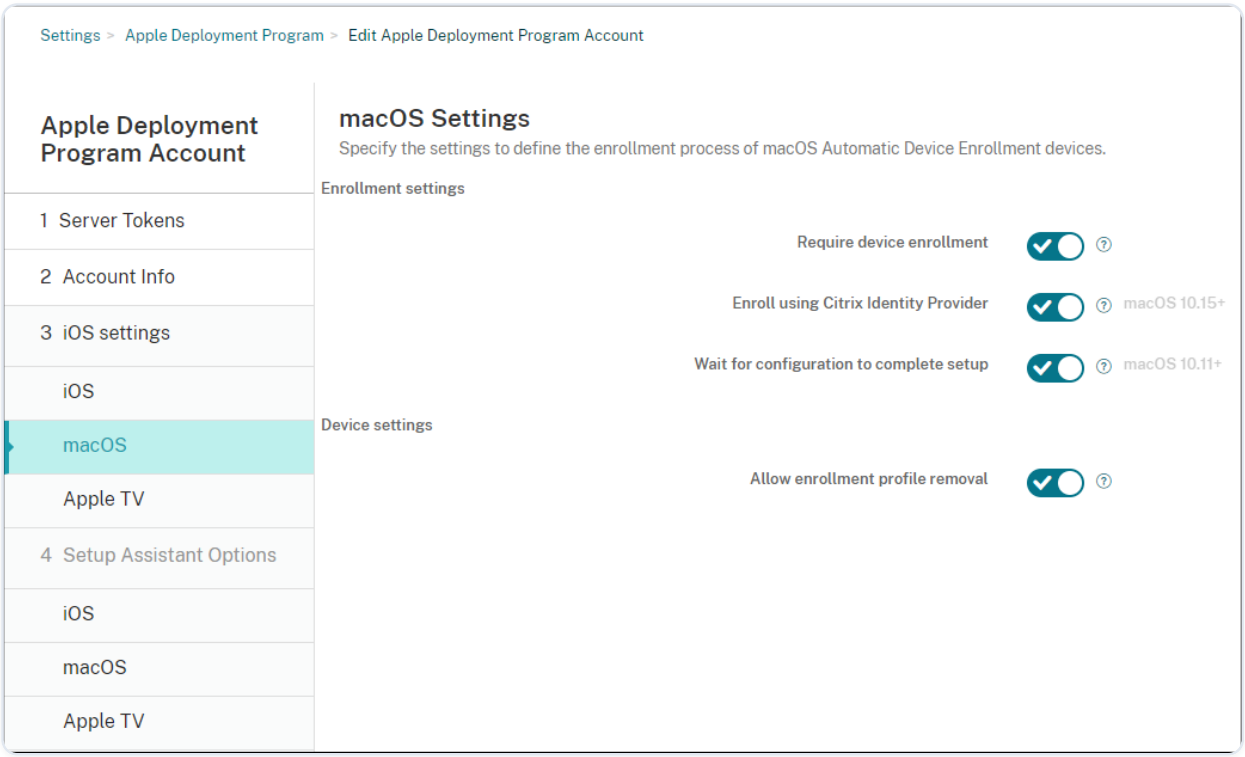
GroundControlツールを使用している場合は、次の操作を行うための証明書を追加できます。

- ペアリング制限を上書きして、「このホストを信頼しますか」というプロンプトを回避します。
- USB経由で管理対象デバイスのアクションをエスカレートし、ユーザー操作なしでプロファイルのインストールなどのアクティビティを実行します。これにより、GroundControlはチェックアウトのためにシングルアプリモードとデバイスロックを有効にできます。
- ABMまたはASMデバイスにバックアップを復元します。

GroundControlの詳細については、GroundControlのWebサイトを参照してください。

5. **macOS設定**で、次の設定を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



登録設定：

- **デバイス登録を必須にする：** ユーザーにデバイスの登録を要求するかどうか。デフォルトは**オン**です。
- **Citrix Identity Providerを使用して登録する：** Citrix Identity Providerを使用して登録するかどうか。この設定はABMアカウントでのみ利用可能です。**オン**の場合、ADP対応のmacOSデバイスはCitrix Identity Providerのみを使用して登録されます。デフォルトは**オフ**です。

  この設定をオンにするには、まずCitrix Identity ProviderをIDプロバイダーとして構成する必要があります。**設定 > IDプロバイダー (IDP)** に移動し、**追加**をクリックして、**Citrix Identity Provider**を選択します。

  この設定が**オン**に設定されている場合、次の考慮事項に注意してください。

  - **設定 > IDプロバイダー (IDP)** ページで、対応するCitrix Identity Provider構成を削除することはできません。
  - 対応するCitrix Identity Provider構成を編集している間は、別のIDプロバイダーに切り替えることはできません。
- **設定完了まで待機: オン**の場合、macOSデバイスは、MDMリソースのパスコードがデバイスに展開されるまで、セットアップアシスタントを続行しません。この展開は、ローカルアカウントの作成前に行われます。この設定は、macOS 10.11以降のデバイスで利用できます。デフォルトは**オフ**です。

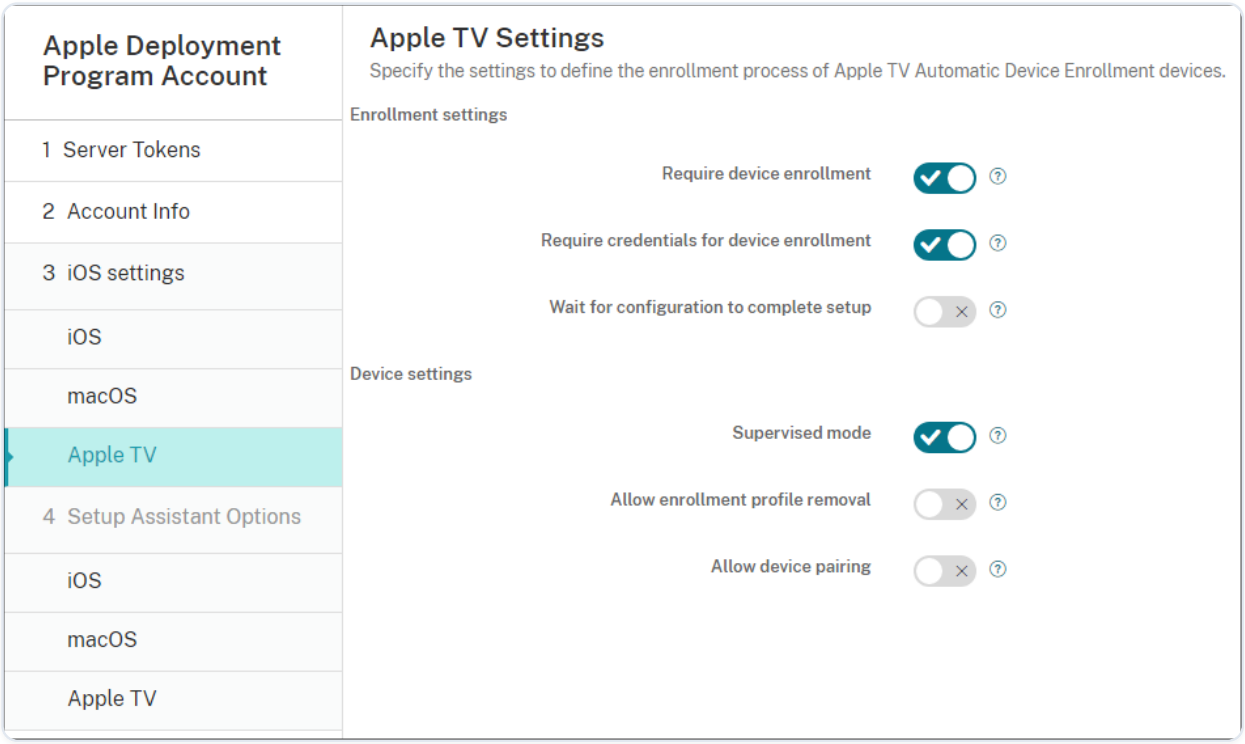
© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイス設定:

- **登録プロファイルの削除を許可:** デバイスがリモートで削除できるプロファイルを使用することを許可するかどうか。デフォルトは**オフ**です。

6. **Apple TV設定**で、次の設定を指定します:

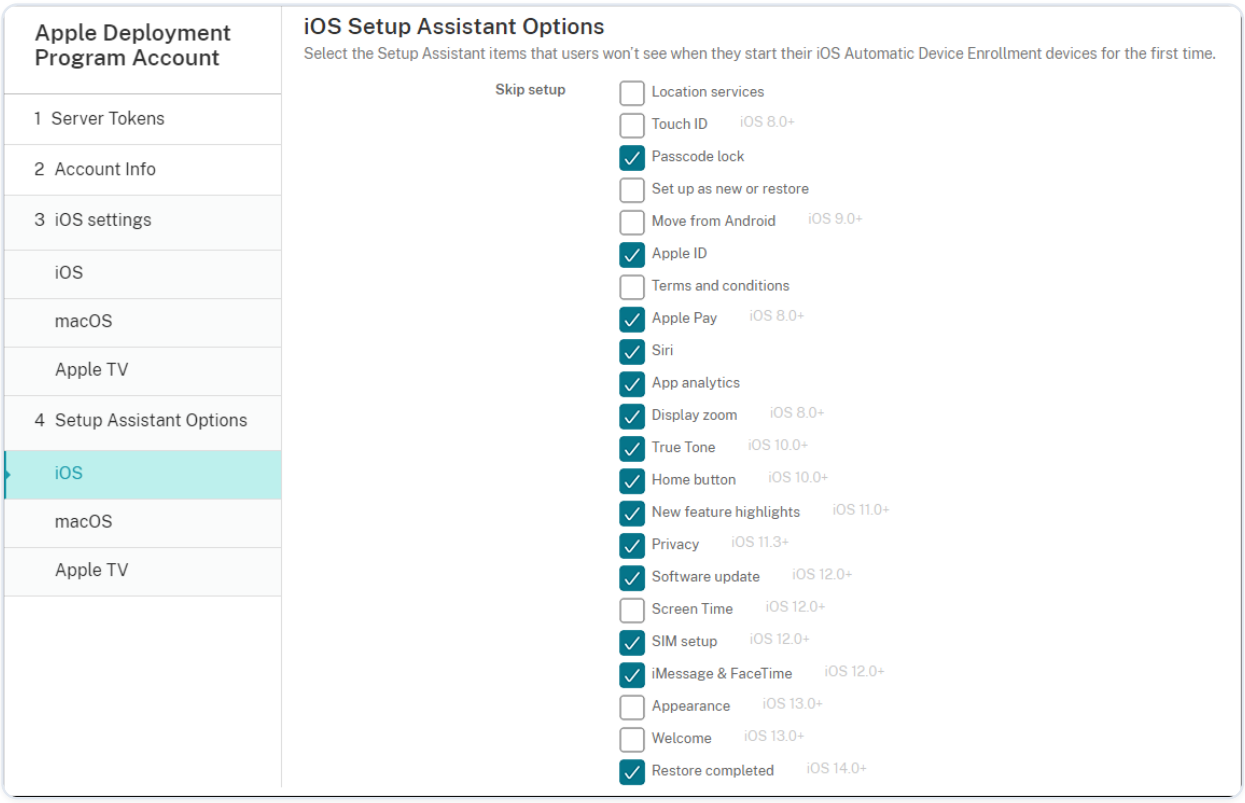
   - **デバイス登録を必須にする:** ユーザーが登録をスキップするのを防ぎます。
   - **デバイス登録に資格情報を要求:** 登録中に資格情報を要求します。この設定がオフの場合、Apple TVはデフォルトの「デバイス登録プログラムユーザー」として登録されます。
   - **設定完了まで待機:** すべてのリソースが展開されるまで、デバイスは**セットアップアシスタント**画面で待機します。
   - **監視モード:** 制限を構成する際に、管理者にさらなる機能を提供します。
   - **登録プロファイルの削除を許可:** ユーザーが登録プロファイルを削除することを許可します。
   - **デバイスペアリングを許可:** デバイス登録プログラムを通じて登録されたデバイスが、Apple App StoreやApple ConfiguratorなどのAppleツールを通じて管理されることを許可します。



7. **iOSセットアップアシスタントオプション**で、ユーザーがデバイスを初めて起動するときにiOSセットアップアシスタントがスキップする手順を選択します。画面がスキップされると、関連する機能はデフォルト設定を使用します。アクセスを完全に制限しない限り、ユーザーはセットアップ完了後にスキップされた機能を構成できます。機能へのアクセス制限の詳細につ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

いては、「制限デバイスポリシー」を参照してください。すべての項目のデフォルトはクリアされています。以下の説明は、設定が選択された場合に何が起こるかを示しています。



- **位置情報サービス:** ユーザーがデバイスで位置情報サービスを設定するのを防ぎます。
- **Touch ID:** ユーザーがiOSデバイスでTouch IDまたはFace IDを設定するのを防ぎます。iOS 15で非推奨になりました。
- **パスコードロック:** ユーザーがデバイスのパスコードを設定するのを防ぎます。パスコードが存在しない場合、ユーザーはTouch IDまたはApple Payを使用できません。
- **新規として設定または復元:** ユーザーがデバイスを新規として設定したり、iCloudまたはApple App Storeのバックアップから復元したりするのを防ぎます。
- **Androidからの移行:** ユーザーがAndroidデバイスからiOSデバイスにデータを転送するのを防ぎます。このオプションは、「**新規として設定または復元**」が選択されている場合（つまり、この手順がスキップされる場合）にのみ利用できます。
- **Apple ID:** ユーザーがデバイスの管理対象Apple IDアカウントを設定するのを防ぎます。
- **利用規約:** ユーザーがデバイスの使用に関する利用規約を読み、同意するのを防ぎます。
- **Apple Pay:** ユーザーがApple Payを設定するのを防ぎます。この設定がオフの場合、ユーザーはTouch IDとApple IDを設定する必要があります。これらの設定がオフになっていることを確認してください。
- **Siri:** ユーザーがSiriを設定するのを防ぎます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アプリ解析:** ユーザーがクラッシュデータと使用状況統計をAppleと共有するかどうかを設定するのを防ぎます。
- **画面表示の拡大:** ユーザーがiOSデバイスで画面解像度（標準または拡大）を設定するのを防ぎます。iOS 17で非推奨になりました。
- **True Tone:** ユーザーが4チャンネルセンサーを設定してディスプレイのホワイトバランスを動的に調整するのを防ぎます。
- **ホームボタン:** ユーザーがホームボタンのフィードバックスタイルを設定するのを防ぎます。iOS 15で非推奨になりました。
- **新機能のハイライト:** ユーザーがAppleソフトウェアの新機能に関する情報を表示する画面を見るのを防ぎます。
- **プライバシー:** ユーザーがデータとプライバシーのペインを見るのを防ぎます。iOS 11.3以降の場合。
- **ソフトウェアアップデート:** ユーザーがiOSを最新バージョンにアップデートするのを防ぎます。iOS 12.0以降の場合。
- **スクリーンタイム:** ユーザーがスクリーンタイムを有効にするのを防ぎます。iOS 12.0以降の場合。
- **SIM設定:** ユーザーが携帯電話プランを設定するのを防ぎます。iOS 12.0以降の場合。
- **iMessageとFaceTime:** ユーザーがiMessageとFaceTimeを有効にするのを防ぎます。iOS 12.0以降の場合。
- **外観:** ユーザーが外観モードを選択するのを防ぎます。iOS 13.0以降の場合。
- **ようこそ:** ユーザーが**はじめに**画面を見るのを防ぎます。iOS 13.0以降の場合。
- **復元完了:** ユーザーがセットアップ中に復元が完了したかどうかを確認するのを防ぎます。iOS 14.0以降の場合。
- **アップデート完了:** ユーザーがセットアップ中にソフトウェアアップデートが完了したかどうかを確認するのを防ぎます。iOS 14.0以降の場合。
- **App Store:** ユーザーがApp Storeを設定するのを防ぎます。iOS 11.1以降の場合。
- **アクションボタン:** ユーザーがアクションボタンの設定ペインを見るのを防ぎます。iOS 17.0以降の場合。
- **ロックダウンモード:** Appleアカウントが設定されている場合、ユーザーがロックダウンモードペインを見るのを防ぎます。iOS 17.1以降の場合。
- **インテリジェンス:** ユーザーがインテリジェンスペインを見るのを防ぎます。iOS 18.0以降の場合。
- **カメラボタン:** ユーザーがカメラボタンペインを見るのを防ぎます。iOS 18.0以降の場合。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アカウントは**設定 > Apple Deployment Program**に表示されます。

8. **macOSセットアップアシスタントオプション**で、ユーザーがデバイスを初めて起動するときにmacOSセットアップアシスタントがスキップする手順を選択します。画面がスキップされると、関連する機能はデフォルト設定を使用します。セットアップが完了した後、それらの機能へのアクセスを完全に制限しない限り、ユーザーはスキップされた機能を構成できます。機能へのアクセスを制限する方法の詳細については、制限デバイスポリシーを参照してください。すべての項目のデフォルトはクリアされています。以下の説明は、設定が選択されたときに何が起こるかを示しています。

   Apple Deployment Programアカウント設定画面(/en-us/citrix-endpoint-management/media/settings-apple-dep-enrollment-11.png)

   - **新規として設定または復元:** ユーザーがデバイスを新規として設定したり、Time Machineバックアップから復元したり、システム移行を行ったりするのを防ぎます。
   - **位置情報サービス:** ユーザーがデバイスで位置情報サービスを設定するのを防ぎます。macOS 10.11以降の場合。
   - **Apple ID:** ユーザーがデバイスの管理対象Apple IDアカウントを設定するのを防ぎます。
   - **利用規約:** ユーザーがデバイスの使用に関する利用規約を読み、同意するのを防ぎます。
   - **Siri:** ユーザーがSiriを設定するのを防ぎます。macOS 10.12以降の場合。
   - **FileVault:** FileVaultを使用して起動ディスクを暗号化します。Citrix Endpoint Managementは、システムに単一のローカルユーザーアカウントがあり、そのアカウントがiCloudにサインインしている場合にのみ、FileVault設定を適用します。

     macOSのFileVaultディスク暗号化機能を使用して、システムボリュームのコンテンツを暗号化することで保護できます (https://support.apple.com/ja-jp/HT204837)。FileVaultがオンになっていない最新モデルのポータブルMacで設定アシスタントを実行すると、この機能をオンにするよう求められる場合があります。このプロンプトは、新しいシステムとOS X 10.10または10.11にアップグレードされたシステムの両方に表示されますが、システムに単一のローカル管理者アカウントがあり、そのアカウントがiCloudにサインインしている場合に限ります。
   - **App解析:** ユーザーがクラッシュデータと使用状況統計をAppleと共有するかどうかを設定するのを防ぎます。
   - **プライバシー:** ユーザーがデータとプライバシーペインを表示するのを防ぎます。macOS 10.13以降の場合。
   - **iCloud解析:** ユーザーが診断用iCloudデータをAppleに送信するかどうかを選択するのを防ぎます。macOS 10.13以降の場合。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **iCloud書類とデスクトップ:** ユーザーがiCloudデスクトップと書類を設定するのを防ぎます。macOS 10.13以降の場合。
- **外観:** ユーザーが外観モードを選択するのを防ぎます。macOS 10.14以降の場合。
- **アクセシビリティ:** ユーザーがVoice Overを自動的に聞くのを防ぎます。デバイスがイーサネットに接続されている場合にのみ利用可能です。macOS 11以降の場合。
- **生体認証:** ユーザーがTouch IDとFace IDを設定するのを防ぎます。macOS 10.12.4以降の場合。
- **True Tone:** ユーザーが4チャンネルセンサーを設定してディスプレイのホワイトバランスを動的に調整するのを防ぎます。macOS 10.13.6以降の場合。
- **Apple Pay:** ユーザーがApple Payを設定するのを防ぎます。この設定がオフの場合、ユーザーはTouch IDとApple IDを設定する必要があります。**Apple ID**と**生体認証**の設定がオフになっていることを確認してください。
- **Screen Time:** ユーザーがScreen Timeを有効にするのを防ぎます。macOS 10.15以降の場合。
- **App Store:** ユーザーがApp Storeを設定するのを防ぎます。macOS 11.1以降の場合。
- **Apple Watchでロック解除:** ユーザーがApple WatchでMacのロックを解除するのを防ぎます。macOS 12以降の場合。
- **ローカルアカウント設定オプション:** デバイスにアカウントを作成するための設定を指定します。Citrix Endpoint Managementは、ここで指定した情報を使用して、まずローカル管理者アカウントを作成します。ユーザーがデバイスをアクティブ化すると、ユーザーアカウントがプライマリアカウントとして作成されます。**プライマリアカウントを標準ユーザーとして作成**オプションは、プライマリアカウントが管理者権限を持つかどうかを決定します。

重要:

macOS設定ページで**構成がセットアップを完了するまで待機**を**オン**に設定した後にのみ、**プライマリアカウントを標準ユーザーとして作成**を選択できます。

- **プライマリアカウントを標準ユーザーとして作成:** 選択すると、Citrix Endpoint Managementは、デバイス上でユーザーに管理者権限を付与するのではなく、標準権限を持つユーザーを作成します。デバイス上でユーザーに管理者権限を付与したい場合は、このオプションをスキップしてください。デフォルトでは、このオプションは選択されていません。
- **管理者のフルネーム:** システムが管理者アカウントに表示する名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **管理者のショートネーム:** デバイスがホームフォルダーとシェルに表示する名前を入力します。
- **管理者のパスワード:** 管理者アカウントの安全なパスワードを入力します。
- **ユーザーとグループに管理者アカウントを表示:** オフにすると、管理者アカウントはmacOS設定の**ユーザーとグループ**に表示されません。プライマリアカウントを標準ユーザーとして作成する場合、Citrix Endpoint Managementが最初に作成する管理者アカウントを非表示にするには、この設定を有効にします。

セキュリティを強化するため、Citrix Endpoint Managementは管理者アカウントのパスワードを毎日ローテーションするかどうかを確認します。デフォルトでは、Citrix Endpoint Managementは7日ごとにパスワードをローテーションします。デフォルトを変更するには、`mac.dep.admin.passwd.rotate`サーバープロパティを更新します。詳細については、サーバープロパティを参照してください。

パスワードの強度とセキュリティを向上させるため、Citrix Endpoint Managementは次のようにパスワードを生成します。

- 12文字
- 3つの大文字
- 小文字3文字
- 数字3桁
- 特殊文字3文字: `! \@ # \$ % \^ * ? + = -`

デバイスの以前のパスワード、現在のパスワード、およびパスワード変更ステータスを表示するには、 **>** に移動します。そのデバイスをクリックし、 をクリックして、 **>** ページを表示します。 セクションには、次の情報が表示されます。

- **以前の管理者パスワード:** 以前のパスワードを表示できます。Citrix Endpoint Managementは、最後のパスワードのみを表示します。パスワードを表示するには、 をクリックします。
- **現在の管理者パスワード:** 現在のパスワードを表示できます。
- **管理者パスワードの変更:** パスワード変更ステータスを表示できます。実際のステータスに応じて、次の情報が表示される場合があります。
  - パスワード変更は\<特定の時刻値\>に要求されました。
  - パスワードは\<特定の時刻値\>に変更されました。
  - パスワード変更の試行は\<特定の時刻値\>に失敗しました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - パスワードはまだ変更されていません。

9. で、ユーザーがデバイスを初めて起動するときにスキップするApple TVセットアップアシスタントの手順を選択します。すべての項目のデフォルトはクリアされています。変更を保存します。

   Apple Deployment Program設定構成画面(/en-us/citrix-endpoint-management/media/settings-dep-apple-tv-setup-assistant.png)

10. アカウントは** > ** に表示されます。Citrix Endpoint ManagementとApple間の接続をテストするには、アカウントを選択し、 をクリックします。

    Apple Deployment Program設定画面(/en-us/citrix-endpoint-management/media/settings-apple-dep-enrollment-6.png)

    ステータスメッセージが表示されます。

    Apple Deployment Program設定画面(/en-us/citrix-endpoint-management/media/settings-apple-dep-enrollment-7.png)

デバイスを注文する

以下のチャネルからデバイスを直接注文できます。

- Apple。販売者にAppleの顧客番号を伝えます。
- 参加しているApple正規販売店または通信事業者。販売者に組織IDを伝え、その販売店IDを取得します。

デバイスサプライヤーの管理について詳しくは、Apple Business Managerユーザーガイドまたは Apple School Managerユーザーガイドを参照してください。

注文が出荷されると、購入したAppleデバイスはABMまたはASMアカウントに追加されます。

デバイスをCitrix Endpoint Managementに割り当てる

ABMまたはASMポータルで、注文番号を検索し、その注文のデバイスをCitrix Endpoint Managementに割り当てるために使用します。また、デバイスの購入場所に関係なく、Apple Configurator 2を使用してiPhone、iPad、iPod touch、およびApple TVデバイスをABMまたはASMに追加することもできます。

詳しくは、Apple Business Managerユーザーガイドまたは Apple School Managerユーザーガイドを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コンテンツを一括購入し、Citrix Endpoint Managementに同期する

ABMとASMを使用すると、単一の組織アカウントからアプリや書籍のライセンスを一括購入、配布、管理できます。Citrix Endpoint ManagementがABMまたはASMと通信して配布用のライセンス情報を取得できるようにするには、次の手順を実行します。

1. ABMまたはASMポータルで、**Apps and Books**から公開アプリと書籍を購入し、**Custom Apps**からCitrix Endpoint Management用に開発されたカスタムアプリを購入します。
2. ABMまたはASMポータルで、Citrix Endpoint Managementに割り当てられているコンテンツトークンをダウンロードします。

   手順1と2の詳細については、Apple Business ManagerユーザガイドまたはApple School Managerユーザガイドを参照してください。
3. Citrix Endpoint Managementコンソールで、ダウンロードしたコンテンツトークンに基づいてボリューム購入アカウントを作成します。

   詳細については、(/ja-jp/citrix-endpoint-management/apps/apple-volume-purchase.html)を参照してください。

   ボリューム購入アカウントが作成されると、購入したアプリとブックは**Manage** > **Apps**に表示され、Citrix Endpoint Managementサーバーに割り当てたデバイスは**Manage > Devices**に表示されます。

デバイスポリシーとアプリの展開ルールを構成する

デバイスポリシーとアプリを構成する際に、ABMまたはASMアカウントを異なるデバイスポリシーやアプリに関連付けることができます。

1. **Configure > Device Policies**および**Configure > Apps**ページで、**Deployment Rules**を展開します。
2. 特定のABMアカウント、または選択したアカウントを除くすべてのABMアカウントに対してポリシーまたはアプリを展開するように指定します。

ABMアカウントのリストには、有効または無効のステータスを持つアカウントのみが含まれます。ABMアカウントが無効になっている場合、ABMデバイスはこのアカウントに属しません。そのため、Citrix Endpoint Managementはアプリまたはポリシーをデバイスに展開しません。

次の例では、デバイスポリシーは「ABM Account NR」というABMアカウント名を持つデバイスにのみ展開されます。

Appleデバイスプログラム設定画面(/en-us/citrix-endpoint-management/media/apple-dep-deployment-rule-policy-example.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Appleデバイスを一括登録する

Citrix Endpoint Managementに多数のiOS、iPadOS、macOSデバイスを登録するには、次の2つの方法があります。

- Apple Deployment Programs (ADP) を使用して、Appleから直接購入した、または参加しているApple正規販売店や通信事業者から購入したAppleデバイスを登録します。

  ADP対応デバイスの展開について詳しくは、「Apple Deployment Programsによるデバイスの展開」を参照してください。この記事では、ユーザーがADP対応デバイスを登録する方法と、デバイスを再登録する方法について説明します。
- Apple Configurator 2を使用して、Appleから直接購入したかどうかにかかわらず、iOSデバイスを登録します。

この記事では、Apple Configurator 2を使用してデバイスを一括展開する方法について説明します。

一括登録について

ADPには、ビジネス向けのApple Business Manager (ABM) と教育機関向けのApple School Manager (ASM) が含まれます。ADPを介した一括登録には、次の特徴があります。

- デバイスに触れたり、準備したりする必要はありません。
- Citrix Endpoint Managementで展開設定を完了すると、デバイスをユーザーに渡し、ユーザーはすぐに使用を開始できます。
- セットアップアシスタントの一部の手順を省略することで、ユーザーのセットアッププロセスを簡素化できます。
- ABMとASMの設定について詳しくは、Apple Business ManagerおよびApple School Managerで入手できるドキュメントを参照してください。

Apple Configurator 2を介した一括登録には、次の特徴があります。

- macOS 10.7.2以降を実行しているMacとApple Configurator 2アプリにiOSデバイスを接続します。Apple Configurator 2を介してiOSデバイスを準備し、ポリシーを構成します。
- セットアッププロセス中にデバイスはCitrix Endpoint Managementに自動的に登録されます。セットアップが完了すると、Citrix Endpoint Managementはポリシー、アプリ、その他のリソースをデバイスにプッシュします。その後、デバイスの管理を開始できます。
- Apple Configurator 2 の使用に関する詳細については、Apple Configurator ヘルプを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーがADP対応デバイスを登録する方法

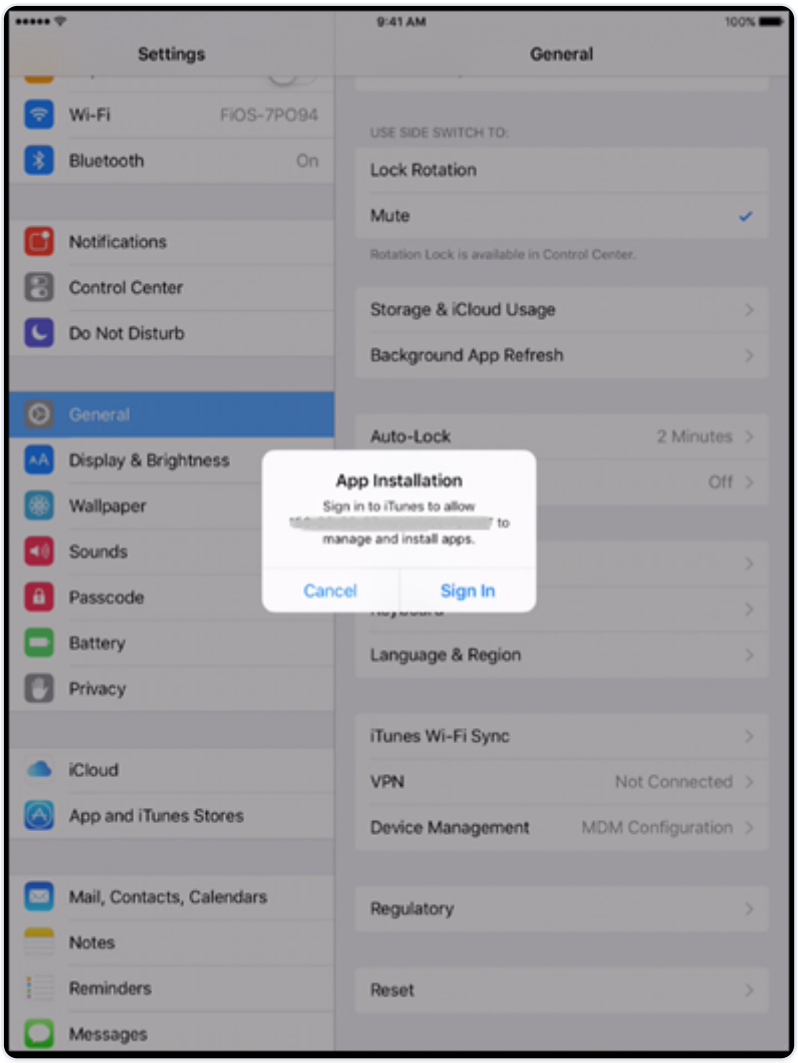
ユーザーは、次のようにCitrix Endpoint Managementにデバイスを登録します。

1. ユーザーはデバイスを起動します。
2. Citrix Endpoint Managementは、**設定 > Apple Deployment Programs**ページで構成したADP設定をデバイスに配信します。
3. ユーザーはデバイスの初期設定を構成します。
4. デバイスは自動的にCitrix Endpoint Managementデバイス登録プロセスを開始します。
5. ユーザーはデバイスの他の初期設定の構成を続行します。
6. ホーム画面で、ユーザーはCitrix Secure Hubをダウンロードするために Apple App Storeにサインインするよう求められる場合があります。

注：

デバイスベースのボリューム購入アプリ割り当てを使用してCitrix Secure Hubアプリを展開するようにCitrix Endpoint Managementを構成した場合、この手順はオプションです。この場合、Apple App Storeアカウントを作成したり、既存のアカウントを使用したりする必要はありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. ユーザーはCitrix Secure Hubを開き、資格情報を入力します。ポリシーで必要とされる場合、ユーザーはCitrix PINを作成して確認するよう求められる場合があります。

   Citrix Endpoint Managementは、残りの必要なアプリをデバイスに展開します。

ADP対応デバイスを再登録する

ADP対応デバイスは、出荷時設定にリセットされた状態から登録されます。ADP対応デバイスを再登録するには、まずデバイスの登録を解除するために完全ワイプを実行する必要があります。詳細な手順は次のとおりです。

1. **管理 > デバイス** ページで、デバイスを選択します。
2. **セキュリティ** をクリックします。
3. **完全ワイプ** をクリックして、デバイスを出荷時設定にリセットされた状態に登録解除します。
4. デバイスを起動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

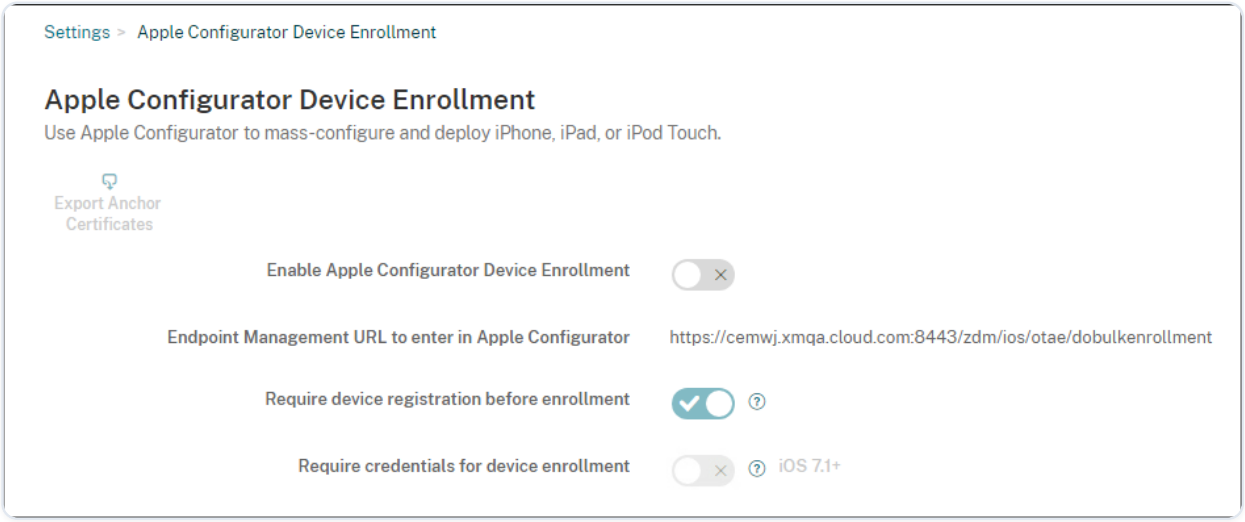
ADP登録では、デバイスが出荷時設定にリセットされた状態である必要があるため、ADP対応デバイスの登録を解除するために **選択的ワイプ** を使用しないでください。

Apple Configurator 2 を使用してデバイスを展開する

Apple Configurator 2 を使用して、設定、アプリ、データを含む多数のデバイスを展開し、これらのデバイスをCitrix Endpoint Managementに登録できます。

ステップ 1: Citrix Endpoint Management で設定を構成する

1. Citrix Endpoint Management コンソールで、**設定 > Apple Configuratorデバイス登録** に移動します。



2. **Apple Configuratorデバイス登録を有効にする** を **はい** に設定します。
3. **Apple Configuratorに入力する登録URL** 設定をコピーし、Apple Configurator 2 で設定を構成するときにこのURLを貼り付けます。この設定は、Appleと通信するCitrix Endpoint ManagementサーバーのURLを提供します。登録URLは、`mdm.server.url.com` のようなCitrix Endpoint Managementサーバーの完全修飾ドメイン名 (FQDN) またはIPアドレスです。
4. 不明なデバイスが登録されないようにするには、**登録前にデバイス登録を要求する** を **はい** に設定します。注: この設定が **はい** に設定されている場合、登録前に構成済みのデバイスをCitrix Endpoint Managementの **管理 > デバイス** に手動で、またはCSVファイルを介して追加する必要があります。
5. iOSデバイスのユーザーが登録時に資格情報を入力するように要求するには、**デバイス登録に資格情報を要求**を**はい**に設定します。デフォルトは**いいえ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注:**
>
> Citrix Endpoint Managementサーバーが信頼されたSSL証明書を使用している場合は、この手順をスキップしてください。**アンカー証明書をエクスポート**をクリックし、certchain.pemファイルをmacOSキーチェーン（ログインまたはシステム）に保存します。

Apple展開プログラム設定画面(/en-us/citrix-endpoint-management/media/settings-apple-dep-enrollment-9.png)

ステップ2：Apple Configurator 2で設定を構成する

1. macOS 10.7.2以降を実行し、Apple Configurator 2がインストールされているMacを準備します。
2. Dockコネクタ-USBケーブルを使用して、AppleデバイスをMacに接続します。最大30台の接続されたデバイスを同時に構成できます。Dockコネクタがない場合は、1つ以上の電源付きUSB 2.0高速ハブを使用してデバイスを接続します。
3. Apple Configurator 2を起動します。コンフィギュレータには、監視用に準備できるすべてのデバイスが表示されます。
4. デバイスを監視用に準備するには：
   - 定期的に構成を再適用してデバイスの制御を維持する予定がある場合は、**デバイスを監視**を選択します。**次へ**をクリックします。

     > **重要:**
     >
     > デバイスを監視モードにすると、選択したバージョンのiOSがデバイスにインストールされ、以前に保存されていたユーザーデータやアプリがデバイスから完全に消去されます。

   - iOSで、インストールしたい最新バージョンのiOSに対して**最新**をクリックします。
5. **MDMサーバーに登録**で、MDMサーバーを選択します。サーバーを追加するには、**次へ**をクリックします。
6. **MDMサーバーを定義**で、サーバーの名前を指定し、Citrix Endpoint ManagementコンソールからMDMサーバーのURLを貼り付けます。
7. 「**組織に割り当てる**」で、デバイスを監視する組織を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apple Configurator 2 を使用したデバイスの準備について詳しくは、Apple Configurator のヘルプページ、デバイスの準備 を参照してください。

8. 各デバイスの準備が完了したら、電源を入れて iOS 設定アシスタントを起動し、デバイスを初回使用に備えて準備します。

Apple Configurator 2 を使用してデバイスを ABM または ASM に追加する

デバイスの購入場所に関係なく、Apple Configurator 2 を使用して iPhone、iPad、Apple TV デバイスを ABM または ASM アカウントに追加できます。 デバイスを追加すると、**デバイス**セクションに表示されます。これらのデバイスには、Apple Configurator 2 を介して割り当てられた登録設定は含まれなくなります。詳しくは、Apple Business Manager ユーザーガイド または Apple School Manager ユーザーガイド を参照してください。

ADP トークンを更新する

ADP トークンの有効期限が切れると、Citrix Endpoint Management にライセンス有効期限の警告が表示されます。ASM または ABM からトークンを置き換えます。

ステップ 1: Citrix Endpoint Management サーバーから公開キーをダウンロードする

1. Citrix Endpoint Management コンソールで、**設定 > Apple Deployment Program** に移動し、新しい公開キーをダウンロードします。

ステップ 2: Apple アカウントからサーバーのトークンファイルを作成してダウンロードする

1. ABM にサインインしてトークンをダウンロードします。
2. **設定**を開き、トークンが必要なサーバーを選択します。**編集**をクリックします。
3. **MDM サーバー設定**で、Citrix Endpoint Management からダウンロードした新しい公開キーをアップロードし、変更を保存します。
4. **トークンをダウンロード**をクリックして、新しいトークンをダウンロードします。

ステップ 3: Citrix Endpoint Management でサーバーのトークンファイルをアップロードする

1. Citrix Endpoint Managementで、 > の順に移動します。
2. Deployment Programアカウントを選択し、 をクリックして、サーバートークンファイルをアップロードします。
3. をクリックして変更を保存します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apple Education機能との統合

Apple Educationを使用する環境で、Citrix Endpoint Managementをモバイルデバイス管理（MDM）ソリューションとして使用できます。Citrix Endpoint Managementは、Apple School Manager（ASM）とiPad用Classroomアプリをサポートしています。Citrix Endpoint ManagementのEducation Configurationデバイスポリシーは、Apple Educationで使用するための教師用および生徒用デバイスを構成します。

構成済みで監視対象のiPadを教師と生徒に提供します。この構成には、Citrix Endpoint ManagementでのASM登録、新しいパスワードで構成されたManaged Apple IDアカウント、および必要なボリューム購入アプリとiBooksが含まれます。

Apple Education機能の詳細については、AppleのEducationサイトおよび同サイトのApple Education Deployment Guideを参照してください。

アップルスクールマネージャー

Citrix Endpoint ManagementをASMと統合するには、次の一般的な手順に従います。

1. ASMで機関のアカウントを作成し、ASMに機関を登録します。
2. Apple School Manager用にEducation Volume Purchaseアカウントを構成します。
3. Apple School Managerユーザーのパスワードを追加します。
4. Citrix Endpoint Managementにリソースとデリバリーグループを計画して追加します。
5. 教師用および生徒用デバイスの登録をテストします。
6. 構成済みのデバイスを教師と生徒に提供します。
7. 教師、生徒、およびクラスのデータを管理する
8. デバイスが紛失または盗難された場合、デバイスをロックして位置を特定できます。

ASMへの登録とCitrix Endpoint Managementへのアカウント接続については、「Deploy devices through the Apple Deployment Program」を参照してください。

前提条件

- NetScaler ゲートウェイ
- MDM+MAM用に構成された登録プロファイル。
- Apple iPad 第3世代（最小バージョン）またはiPad Mini（iOS 9.3 (最小バージョン) を搭載）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

Citrix Endpoint Managementは、ASMユーザーアカウントをLDAPまたはActive Directoryに対して検証しません。ただし、Citrix Endpoint ManagementをLDAPまたはActive Directoryに接続して、ASMの教員や生徒に関係のないユーザーやデバイスを管理できます。たとえば、Active Directoryを使用して、IT管理者やマネージャーなど、他のASMメンバーにCitrix Secure MailおよびCitrix Secure Webを提供できます。

ASMの教員と生徒はローカルユーザーであるため、Citrix Secure Hubをデバイスに展開する必要はありません。
NetScaler Gateway認証を含むMAM登録は、ローカルユーザー（Active Directoryユーザーのみ）をサポートしていません。そのため、Citrix Endpoint Managementは、必要なボリューム購入アプリとiBooksのみを教員および生徒のデバイスに展開します。

iPad用Classroomアプリ

iPad用Classroomアプリを使用すると、教員は生徒のデバイスに接続して管理できます。デバイスの画面を表示したり、iPadでアプリを開いたり、Webリンクを共有して開いたり、生徒の画面をApple TVに表示したりできます。

ClassroomはApp Storeで無料で入手できます。アプリをCitrix Endpoint Managementコンソールにアップロードします。その後、Education Configurationデバイスポリシーを使用してClassroomアプリを構成し、教員デバイスに展開します。

Classroomアプリの展開方法の詳細については、「Appleアプリの配布」を参照してください。

Classroomアプリの要件、セットアップ、および機能の詳細については、Appleサポートサイトの「Classroomユーザーガイド」を参照してください。

Apple School Managerユーザーのパスワードを追加する

ASMアカウントを追加すると、Citrix Endpoint ManagementはASMからクラスとユーザーをインポートします。Citrix Endpoint Managementはクラスをローカルグループとして扱い、コンソールでは「グループ」という用語を使用します。クラスにASMでグループ名が設定されている場合、Citrix Endpoint Managementはそのグループ名をクラスに割り当てます。それ以外の場合、Citrix Endpoint ManagementはソースシステムIDをグループ名として使用します。ASMのコース名は一意ではないため、Citrix Endpoint Managementはコース名をクラス名として使用しません。

Citrix Endpoint Management は、Managed Apple ID を使用して、ユーザータイプが **ASM** のローカルユーザーを作成します。ASM はすべての外部データソースとは独立して資格情報を作成する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ため、ユーザーはローカルです。その結果、Citrix Endpoint Management はこれらの新しいユーザーを認証するためにディレクトリサーバーを使用しません。

ASM は一時的なユーザーパスワードを Citrix Endpoint Management に送信しません。CSV ファイルからインポートするか、手動で追加できます。一時的なユーザーパスワードをインポートするには:

1. Managed Apple ID の一時パスワードを作成するときに ASM によって生成された CSV ファイルを取得します。
2. CSV ファイルを編集し、一時パスワードを、ユーザーが Citrix Endpoint Management に登録するために提供する新しいパスワードに置き換えます。この目的のためのパスワードタイプに制約はありません。

   CSV ファイルのエントリの形式は次のとおりです:
   `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`!

   内訳:

   ユーザー: `user@appleid.citrix.com`

   名: `Firstname`

   ミドルネーム: `Middle`

   姓: `Lastname`

   パスワード: `Password123!`!
3. Citrix Endpoint Management コンソールで、 **>** をクリックします。 ページが表示されます。

   次の **>** 画面のサンプルは、ASM からインポートされたユーザーのリストを示しています。 リストでは:

   - **ユーザー名** には、管理対象の Apple ID が表示されます。
   - ユーザータイプは **ASM** で、アカウントが ASM から作成されたことを示します。
   - **グループ**にはクラスが表示されます。

   「ユーザー画面」(/en-us/citrix-endpoint-management/media/manage-users-asm-filtered.png)
4. 「**ローカルユーザーのインポート**」をクリックします。「**プロビジョニングファイルのインポート**」ダイアログボックスが表示されます。
5. 形式については「**ASMユーザー**」を選択し、手順2で準備したCSVファイルに移動して、「**インポート**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「ユーザー画面」(/en-us/citrix-endpoint-management/media/manage-users-import-passwords.png)

6. ローカルユーザーのプロパティを表示するには、ユーザーを選択して「**編集**」をクリックします。

   「ユーザー画面」(/en-us/citrix-endpoint-management/media/manage-users-asm-properties.png)

   名前のプロパティに加えて、次のASMプロパティを使用できます。

   - **ASMデータソース:** クラスのデータソース（**CSV**や**SFTP**など）。
   - **ASM管理対象Apple ID:** 管理対象Apple IDには、組織名と`appleid`が含まれる場合があります。たとえば、IDはjohnappleseed@appleid.myschool.eduのようになることがあります。Citrix Endpoint Managementでは、認証に管理対象Apple IDが必要です。
   - **ASM組織名:** Citrix Endpoint Managementでアカウントに付けた名前。
   - **ASMパスコードタイプ:** 個人のパスワードポリシー: **複雑**（8文字以上の数字と文字で構成される学生以外のパスワード）、**4桁**（数字）、または**6桁**（数字）。
   - **ASM個人固有ID:** ユーザーの識別子。
   - **ASM個人ステータス:** 管理対象Apple IDが「**アクティブ**」か「**非アクティブ**」かを指定します。このステータスは、ユーザーが管理対象Apple IDアカウントの新しいパスワードを提供した後にアクティブになります。
   - **ASM個人タイトル:** 教員、学生、またはその他。
   - **ASM person unique ID:** ユーザーの一意の識別子。
   - **ASM source system ID:** システムソースの識別子。
   - **ASM student grade:** 学生の学年情報（教員は使用しません）。

Citrix Endpoint Management にリソースとデリバリーグループを計画して追加する

デリバリーグループは、ユーザーのカテゴリに展開するリソースを指定します。たとえば、教員と学生用に1つのデリバリーグループを作成できます。あるいは、複数のデリバリーグループを作成して、さまざまな教員や学生に送信されるアプリ、メディア、ポリシーをカスタマイズすることもできます。クラスごとに1つ以上のデリバリーグループを作成できます。管理者（教育機関の他の職員）用に1つ以上のデリバリーグループを作成することもできます。

ユーザーデバイスに展開するリソースには、デバイスポリシー、Volume Purchaseアプリ、iBooksが含まれます。

- デバイスポリシー:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

教員がClassroomアプリを使用する場合、教育構成デバイスポリシーが必要です。教員と学生のiPadをどのように構成および制限するかを決定するために、他のデバイスポリシーを確認してください。

- Volume Purchaseアプリ:

  Citrix Endpoint Management では、Volume Purchaseアプリを教育ユーザー向けの必須アプリとして展開する必要があります。Citrix Endpoint Management は、このようなVolume Purchaseアプリをオプションとして展開することをサポートしていません。

  Apple Classroomアプリを使用する場合は、教員デバイスにのみ展開してください。

  教員または学生に提供したい他のアプリを展開します。このソリューションはCitrix Secure Hubアプリを使用しないため、教員または学生に展開する必要はありません。

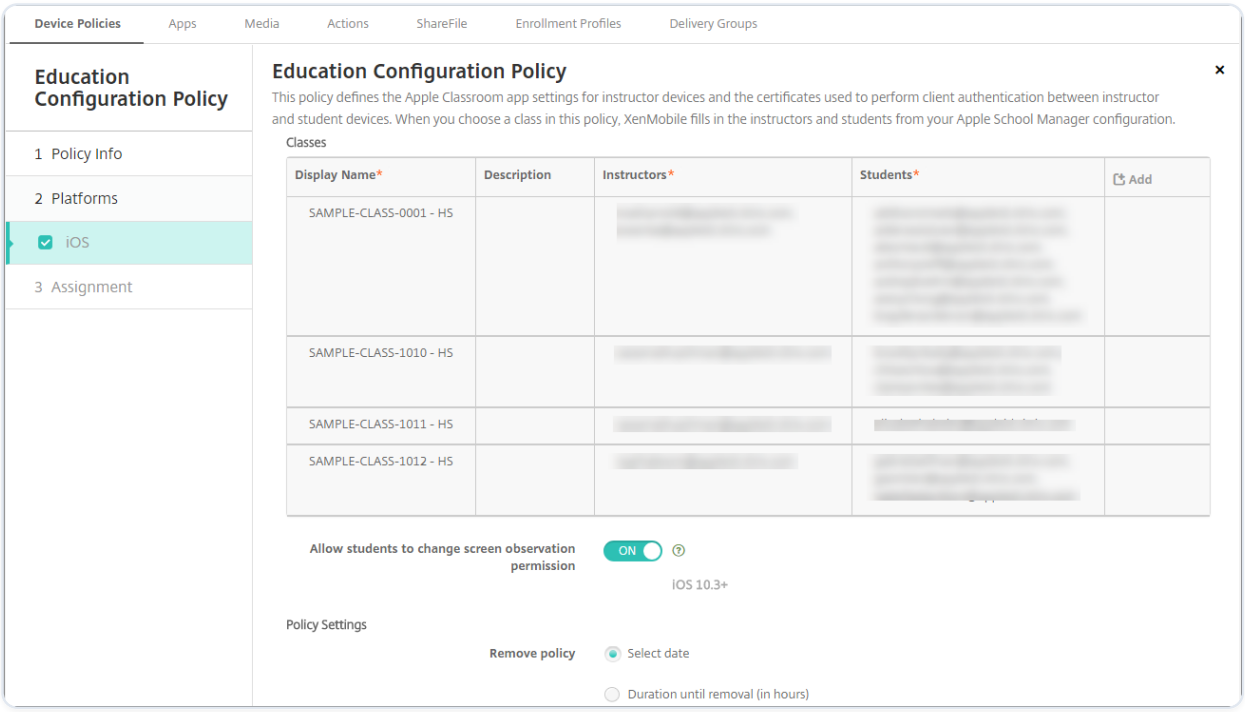
- ボリューム購入 iBooks:

  Citrix Endpoint Management がASMアカウントに接続すると、購入したiBooksがCitrix Endpoint Management コンソールの **構成 > メディア** に表示されます。そのページにリストされているiBooksは、デリバリーグループに追加できます。Citrix Endpoint Management は、iBooksを必須メディアとしてのみ追加することをサポートしています。

教員と学生向けのリソースとデリバリーグループを計画した後、Citrix Endpoint Management コンソールでそれらの項目を作成できます。

1. インストラクターまたは学生のデバイスに展開するデバイスポリシーを作成します。Education Configurationデバイスポリシーについては、Education Configurationデバイスポリシーを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



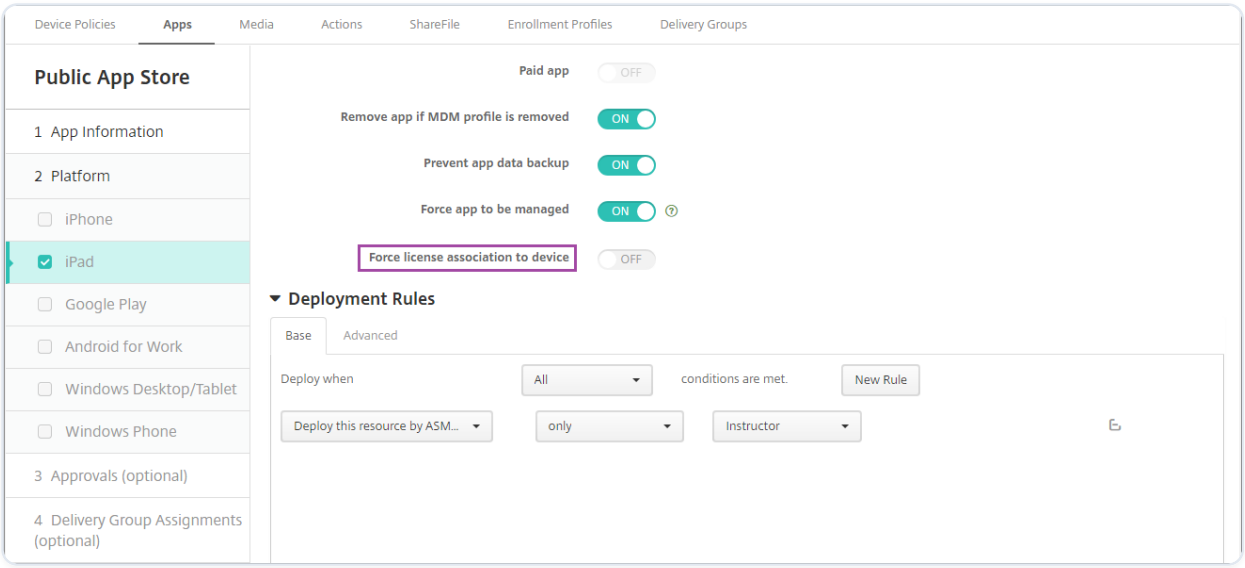
デバイスポリシーについては、デバイスポリシーおよび個別のポリシー記事を参照してください。

2. アプリ (**Configure > Apps**) とiBooks (**Configure > Media**) を構成します。

   - デフォルトでは、Citrix Endpoint ManagementはアプリとiBooksをユーザーレベルで割り当てます。初回展開時に、インストラクターと学生はASMに登録するようプロンプトを受け取ります。招待を承諾すると、ユーザーは次回の展開時（6時間以内）にASMアプリとiBooksを受け取ります。Citrixは、新しいASMユーザーにアプリとiBooksの展開を強制することをお勧めします。そのためには、デリバリーグループを選択し、**Deploy**をクリックします。

     アプリ（iBooksは除く）をデバイスレベルで割り当てることもできます。そのためには、設定 **Force license association to device** を **On** に変更します。アプリをデバイスレベルで割り当てると、ユーザーはVolume Purchaseプログラムへの招待を受け取りません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

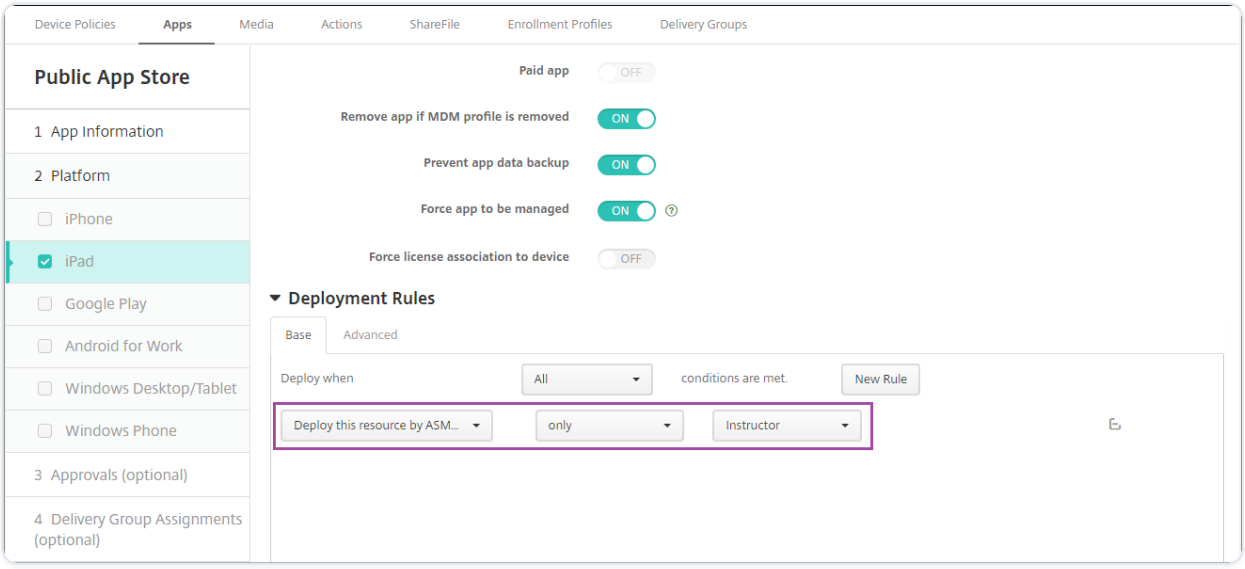


- アプリをインストラクターのみに展開するには、インストラクターのみを含むデリバリーグループを選択するか、次の展開ルールを使用します。

```
Deploy this resource by ASM device type

only

Instructor
```

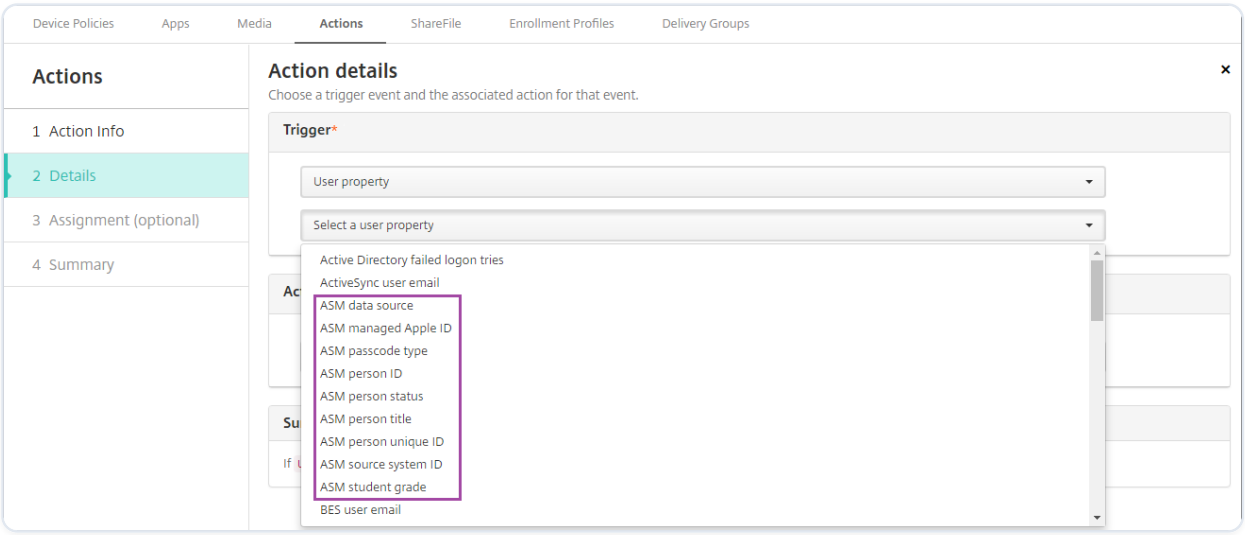


- Volume Purchaseアプリの追加については、パブリックApp Storeアプリの追加を参照してください。

3. オプション。ASMユーザープロパティに基づいてアクションを作成します。たとえば、新しいアプリがインストールされたときに学生デバイスに通知を送信するアクションを作成できま

© 1997–2026 Citrix Systems, Inc. All rights reserved.

す。または、次の例に示すように、ユーザープロパティがトリガーするアクションを作成することもできます。



アクションを作成するには、**Configure > Actions**に移動します。アクションの構成については、自動化されたアクションを参照してください。

4. **Configure > Delivery Groups**で、インストラクター用と学生用のデリバリーグループを作成します。ASMからインポートされたクラスを選択します。また、インストラクターと学生の展開ルールを作成します。

   たとえば、次のユーザー割り当てはインストラクター用です。展開ルールは次のとおりです。

   ```
   Limit by user property

   ASM person title

   is equal to

   Instructor
   ```

   「デリバリーグループ構成画面」(/en-us/citrix-endpoint-management/media/settings-delivery-groups-instructor-assignments.png)

   以下のユーザー割り当ては学生向けです。展開ルールは次のとおりです。

   ```
   Limit by user property

   ASM person title

   is equal to
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Student
```

「デリバリーグループ構成画面」(/en-us/citrix-endpoint-management/media/settings-delivery-groups-student-assignments.png)

ASM組織名に基づいた展開ルールを使用して、デリバリーグループをフィルタリングすることもできます。

「デリバリーグループ構成画面」(/en-us/citrix-endpoint-management/media/configure-delivery-group-filter-by-dep-account.png)

5. リソースをデリバリーグループに割り当てます。次の例は、デリバリーグループ内のiBookを示しています。

   「デリバリーグループ構成画面」(/en-us/citrix-endpoint-management/media/configure-delivery-groups-media.png)

   次の例は、デリバリーグループを選択して**展開**をクリックしたときに表示される確認ダイアログを示しています。

   「デリバリーグループ構成画面」(/en-us/citrix-endpoint-management/media/deploy-delivery-group.png)

   詳しくは、リソースの展開の「デリバリーグループを編集するには」および「デリバリーグループに展開するには」を参照してください。

教員および学生デバイスの登録をテストする

デバイスは、以下のいずれかの方法で登録できます。

- 学校管理者は、Citrix Endpoint Managementコンソールで設定できるユーザーパスワードを使用して、教員および学生のデバイスを登録できます。その結果、アプリとメディアがすでに設定されているデバイスをユーザーに提供できます。
- ユーザーがデバイスを受け取ったら、提供されたユーザーパスワードを使用して登録します。登録が完了すると、Citrix Endpoint Managementはデバイスポリシー、アプリ、およびメディアをデバイスに送信します。

登録をテストするには、ASMにリンクされているApple Deployment Programデバイスを使用します。

1. デバイスがASMにリンクされていない場合は、ハードリセットを実行してデバイスのコンテンツと設定を消去します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. ASMデバイスをインストラクターに登録します。次に、ASMデバイスを生徒に登録します。
3. **Manage > Devices** ページで、両方のASMデバイスがMDMのみに登録されていることを確認します。

   Devices ページは、ASMデバイスのステータス（**ASM registered**、**ASM shared**、**Instructor**、**Student**）でフィルタリングできます。

   デバイス構成画面(/en-us/citrix-endpoint-management/media/manage-devices-asm-filtered.png)
4. 各デバイスにMDMリソースが正しく展開されていることを確認するには：デバイスを選択し、**Edit** をクリックして、さまざまなページを確認します。

   デバイス構成画面(/en-us/citrix-endpoint-management/media/manage-devices-asm-details.png)

デバイスの配布

Appleは、インストラクターと生徒にデバイスを配布するためにイベントを開催することを推奨しています。

事前登録済みのデバイスを配布しない場合は、以下の情報もこれらのユーザーに提供してください。

- 登録用のCitrix Endpoint Managementパスワード
- Managed Apple ID用のASM一時パスワード。

初回ユーザーエクスペリエンスは次のとおりです。

1. ユーザーがハードリセット後に初めてデバイスを起動すると、Citrix Endpoint Managementは登録画面でデバイスの登録を促します。
2. ユーザーは、Citrix Endpoint Managementへの認証に使用するManaged Apple IDとCitrix Endpoint Managementパスワードを提供します。
3. Apple ID設定ステップで、デバイスはユーザーに管理対象Apple IDとASM一時パスワードの入力を求めます。これらの項目は、Appleサービスに対してユーザーを認証します。
4. デバイスは、iCloud内のデータを保護するために使用される、管理対象Apple IDのパスワードを作成するようユーザーに促します。
5. セットアップアシスタントの最後に、Citrix Endpoint Managementはポリシー、アプリ、メディアのデバイスへのインストールを開始します。ユーザーレベルで割り当てられたアプリとiBooksの場合、アシスタントは教師と生徒にボリューム購入への登録を促します。招待を承諾すると、ユーザーは次回の展開時（6時間以内）にボリューム購入のアプリとiBooksを受け取ります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

教師、生徒、クラスのデータを管理する

教師、生徒、クラスのデータを管理する際は、次の点に注意してください。

- ASM情報をCitrix Endpoint Managementにインポートした後で、管理対象Apple IDを変更しないでください。Citrix Endpoint Managementは、ユーザーを識別するためにASMユーザー識別子も使用します。
- 1つ以上の教育構成デバイスポリシーを作成した後でASMのクラスデータを追加または変更した場合は、ポリシーを編集してから再展開します。
- 教育構成デバイスポリシーを展開した後でクラスの教師が変更された場合は、Citrix Endpoint Managementコンソールでポリシーが更新されていることを確認してから、ポリシーを再展開します。
- ASMポータルでユーザープロパティを更新すると、Citrix Endpoint Managementもコンソールでそれらのプロパティを更新します。ただし、Citrix Endpoint Managementは、他のプロパティを受け取るのと同じ方法でASMの人物の役職プロパティ（教師、生徒、その他）を受け取りません。したがって、ASMでASMの人物の役職を変更した場合は、Citrix Endpoint Managementにその変更を反映させるために、次の手順を実行します。

データを管理するには：

1. ASMポータルで、生徒の学年を更新し、教師の学年をクリアします。
2. 生徒アカウントを教師アカウントに変更した場合は、クラスの生徒リストからユーザーを削除します。その後、同じクラスまたは別のクラスの教師リストにユーザーを追加します。

   教師アカウントを生徒アカウントに変更した場合は、クラスからユーザーを削除します。その後、同じクラスまたは別のクラスの生徒リストにユーザーを追加します。更新は、次回の同期時（デフォルトで5分ごと）またはフェッチ時（デフォルトで24時間ごと）にCitrix Endpoint Managementコンソールに表示されます。
3. 教育構成デバイスポリシーを編集して変更を適用し、再展開します。

   - ASMポータルからユーザーを削除すると、Citrix Endpoint Managementもフェッチ後にそのユーザーをCitrix Endpoint Managementコンソールから削除します。

     2つのベースライン間の間隔は、このサーバープロパティ値「**bulk.enrollment.fetchRosterInfoDelay**」を変更することで短縮できます（デフォルトは**1440**分です）。
   - リソースを展開した後: 学生がクラスに参加した場合、その学生のみを含むデリバリーグループを作成し、その学生にリソースを展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 学生または教員が一時パスワードを紛失した場合は、ASM管理者に連絡するよう指示してください。管理者は一時パスワードを提供するか、新しいパスワードを生成できます。

紛失または盗難にあったデバイスの管理

Appleの「iPhone/iPadを探す」サービスには、アクティベーションロック機能が含まれています。アクティベーションロックは、Apple Deployment Programに登録されている紛失または盗難にあったデバイスを、不正なユーザーが使用したり転売したりするのを防ぎます。

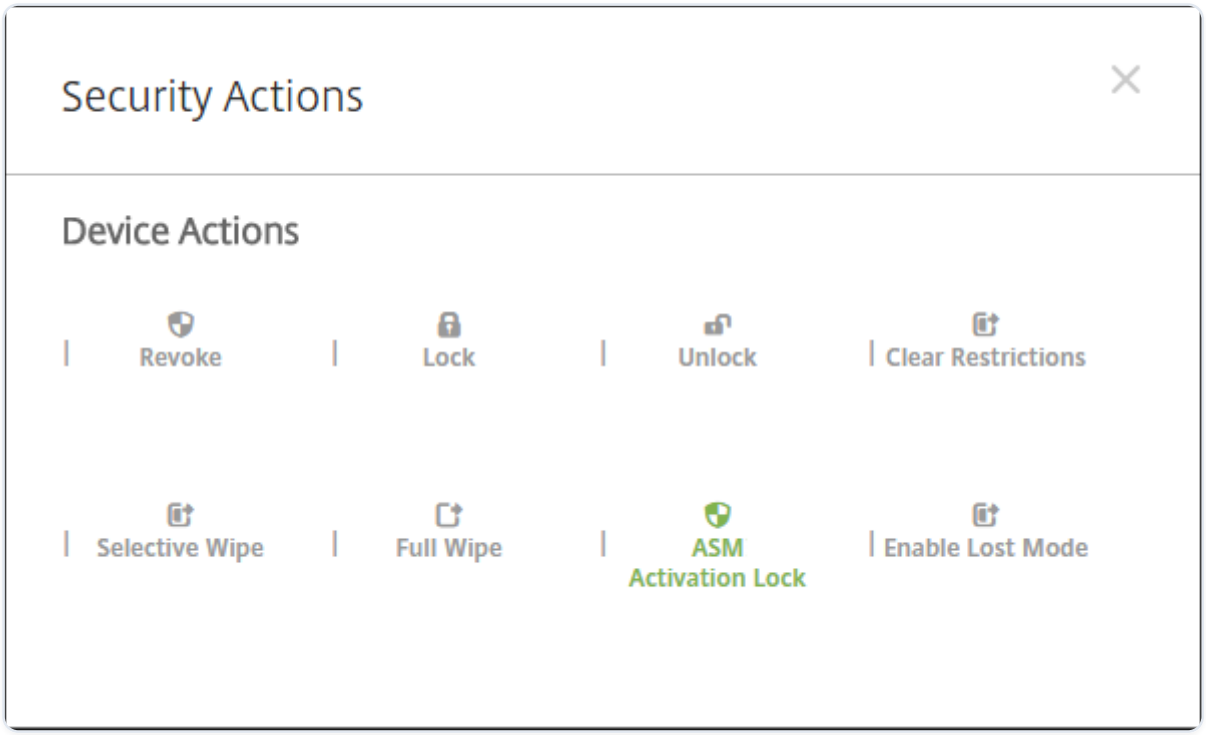
Citrix Endpoint Managementには、ASM Apple Deployment Programに登録されているデバイスにロックコードを送信できる**ASMアクティベーションロック**セキュリティアクションが含まれています。

ASMアクティベーションロックセキュリティアクションを使用すると、Citrix Endpoint Managementは、ユーザーが「iPhone/iPadを探す」サービスを有効にする必要なくデバイスを特定できます。ASMデバイスがハードリセットまたは完全にワイプされた場合、ユーザーはデバイスのロックを解除するためにManaged Apple IDとパスワードを提供します。

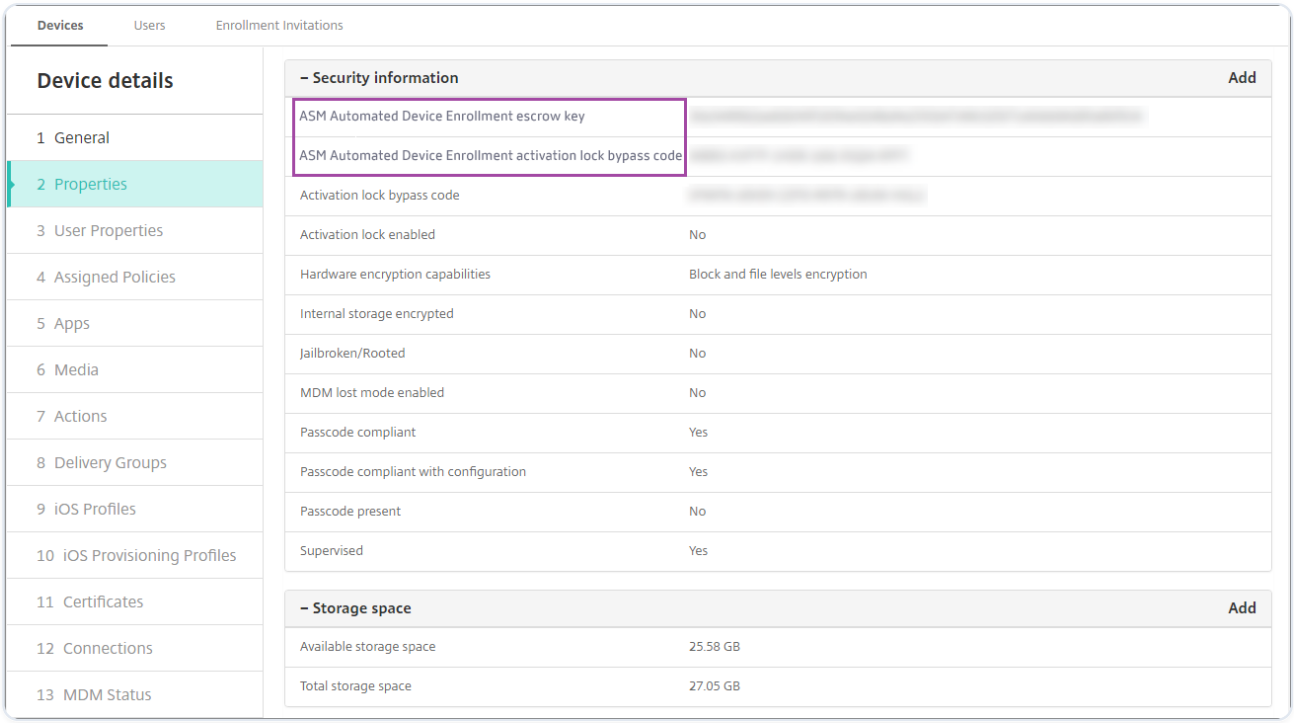
コンソールからロックを解除するには、セキュリティアクションの**アクティベーションロックバイパス**をクリックします。アクティベーションロックのバイパスについては、「iOSアクティベーションロックのバイパス」を参照してください。ユーザーはログインを空白のままにし、パスワードとして**ASMアクティベーションロックバイパスコード**を入力することもできます。この情報は、**デバイスの詳細**の**プロパティ**タブで確認できます。

アクティベーションロックを設定するには、**管理 > デバイス**に移動し、デバイスを選択して**セキュリティ**をクリックし、**ASMアクティベーションロック**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

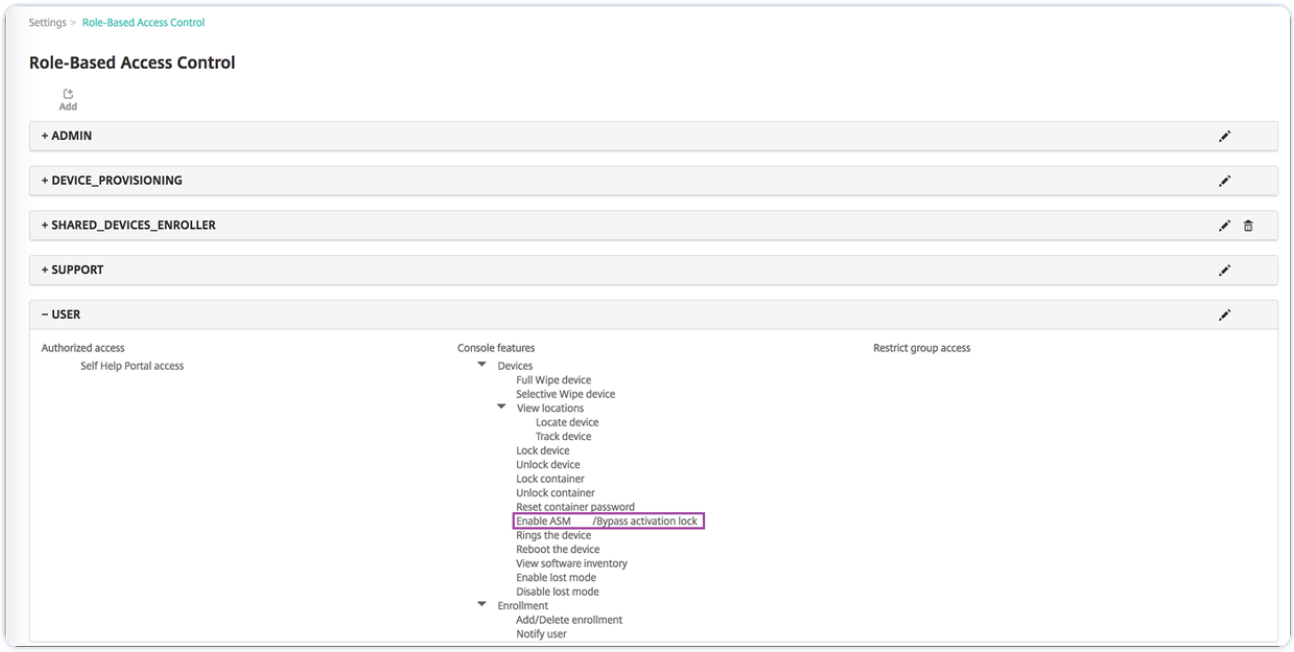


プロパティの**ASMエスクローキー**と**ASMアクティベーションロックバイパスコード**は、**デバイスの詳細**に表示されます。



ASMアクティベーションロックのRBAC権限は、**デバイス > ASMバイパスアクティベーションロックを有効にする**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



共有iPad

共有iPad機能を使用すると、複数のユーザーが1台のiPadを使用できます。デバイスが共有されていても、ユーザーエクスペリエンスをパーソナライズできます。共有iPadは、教育またはビジネス目的で使用できます。Apple School Manager (ASM) は、Apple Business Manager (ABM) がサポートする役割に加えて、教員と生徒の役割をサポートします。

共有iPadの前提条件

- アップルスクールマネージャーまたはアップルビジネスマネージャー
- シトリックス エンドポイントマネージメント
- iPad Pro、iPad 第5世代、iPad Air 2以降、およびiPad mini 4以降のいずれか
- 32 GB以上のストレージ
- 監視対象デバイス

共有iPadを構成する

複数の生徒または従業員が、さまざまな目的でiPadを共有できます。

管理者またはデバイス所有者が共有iPadを登録し、デバイスポリシー、アプリ、メディアをデバイスに展開します。その後、ユーザーは管理対象Apple IDの資格情報を提供して共有iPadにサインインします。以前に生徒に教育構成ポリシーを展開していた場合、彼らはデバイスを共有するために「その他のユーザー」としてサインインする必要がなくなります。

Citrix Endpoint Managementは、共有iPad用に2つの通信チャネルを使用します。デバイス所有者（教員または管理者）用のシステムチャネルと、現在の常駐ユーザー（生徒または従業員）用の

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーチャネルです。Citrix Endpoint Managementは、これらのチャネルを使用して、Appleがサポートするリソースに対して適切なMDMコマンドを送信します。

システムチャネル経由で展開されるリソースは次のとおりです。

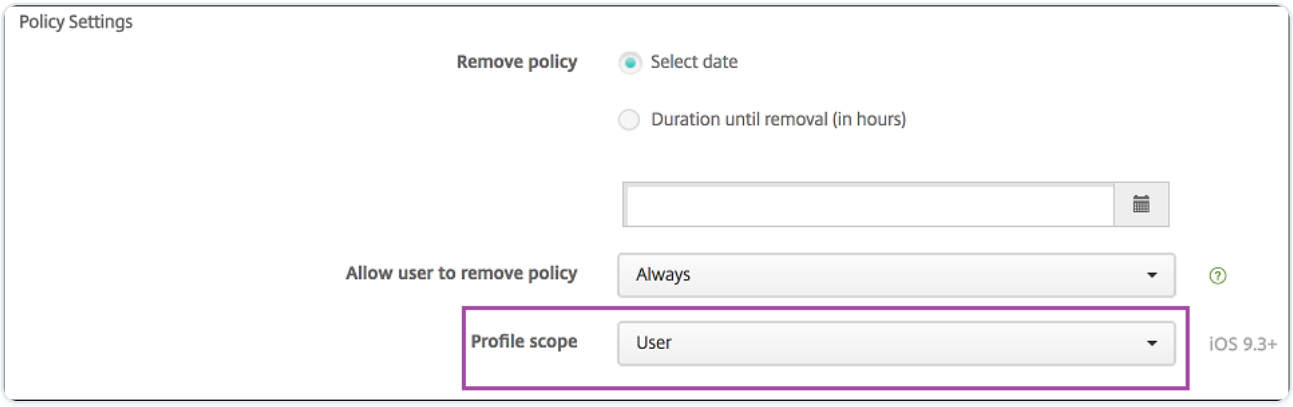
- デバイスポリシー（例: 教育構成、ロック画面メッセージ、最大常駐ユーザー数、パスコードロック猶予期間）
- デバイスベースのボリューム購入アプリ Appleは、共有iPadでエンタープライズアプリまたはユーザーベースのボリューム購入アプリをサポートしていません。共有iPadにインストールされたアプリはデバイス全体に適用され、ユーザーごとではありません。
- ユーザーベースのボリューム購入iBooks Appleは、共有iPadでのユーザーベースのボリューム購入iBooksの割り当てをサポートしています。

ユーザーチャネル経由で展開されるリソースは次のとおりです。

- デバイスポリシー: アプリ通知、ホーム画面レイアウト、制限、Webクリップ。

  Citrix Endpoint Managementは、ユーザーチャネル経由でこれらのデバイスポリシーのみをサポートしています。

デバイスポリシーを構成するときは、ポリシー設定の**プロファイルスコープ**で展開チャネルを指定します。



ユーザーチャネル経由で展開したデバイスポリシーを削除するには、プロファイル削除ポリシーの**展開スコープ**で**ユーザー**を必ず選択してください。

一般的なワークフロー

通常、事前構成済みで監視対象の共有iPadをデバイス所有者に提供します。その後、それらの個人がデバイスを学生や従業員に配布します。事前登録済みの共有iPadを配布しない場合: デバイス所有者がデバイスを登録できるように、Citrix Endpoint Managementサーバーのパスワードを必ず提供してください。

共有iPadを構成および登録するための一般的なワークフローは次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Citrix Endpoint Managementサーバーコンソールを使用して、**共有モード**が有効になっているASMまたはABMアカウント（**設定 > Apple展開プログラム**）を追加します。詳細については、次の「共有iPadのアカウントを管理する」を参照してください。
2. このセクションで説明されているように、必要なデバイスポリシー、アプリ、およびメディアをCitrix Endpoint Managementに追加します。これらのリソースをデリバリーグループに割り当てます。
3. デバイス所有者に共有iPadのハードリセットを実行させます。登録用のリモート管理画面が表示されます。
4. デバイス所有者が共有iPadを登録します。 Citrix Endpoint Managementは、構成されたリソースを登録済みの各共有iPadに展開します。自動再起動後、デバイス所有者はデバイスをユーザーと共有できます。iPadにサインインページが表示されます。
5. デバイスユーザーは、管理対象Apple IDと一時的なASMパスワードを入力します。 共有iPadはASMに対して認証を行い、ユーザーにASMパスワードの作成を促します。次回共有iPadにサインインするときは、デバイスユーザーは新しいASMパスワードを提供します。
6. iPad を共有する別のデバイスユーザーは、前の手順を繰り返してサインインできます。

共有 iPad のアカウントを管理する

Citrix Endpoint Management を Apple Education または Apple Business とすでに使用している場合: デバイス所有者が使用するデバイスなど、共有されていないデバイス用に Citrix Endpoint Management で構成された既存の ASM/ABM アカウントがあります。共有デバイスと非共有デバイスの両方に、同じ ASM/ABM アカウントと Citrix Endpoint Management サーバーを使用できます。

共有 iPad をデバイスグループに整理する

ASM/ABM を使用すると、複数の MDM サーバーを作成することでデバイスをグループに整理できます。共有 iPad を MDM サーバーに割り当てるときは、共有 iPad の各グループに対してデバイスグループを作成します。

- 共有 iPad のグループ 1 > デバイスグループ 1 MDM サーバー
- 共有 iPad のグループ 2 > デバイスグループ 2 MDM サーバー
- 共有 iPad のグループ N > デバイスグループ N MDM サーバー

各デバイスグループの ASM アカウントを追加する

Citrix Endpoint Management サーバーコンソールから複数の ASM/ABM アカウントを作成すると、共有 iPad のグループが自動的にインポートされます。

- デバイスグループ 1 MDM サーバー > デバイスグループ 1 アカウント

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- デバイスグループ 2 MDM サーバー > デバイスグループ 2 アカウント
- デバイスグループ N MDM サーバー > デバイスグループ N アカウント

共有 iPad に固有の要件は次のとおりです。

- これらの設定が有効になっている各デバイスグループの ASM/ABM アカウントを 1 つ:
  - **デバイス登録を必須にする**
  - **監視モード**
  - **共有モード**
- 特定の教育機関では、すべてのASMアカウントに同じ**教育サフィックス**を使用してください。

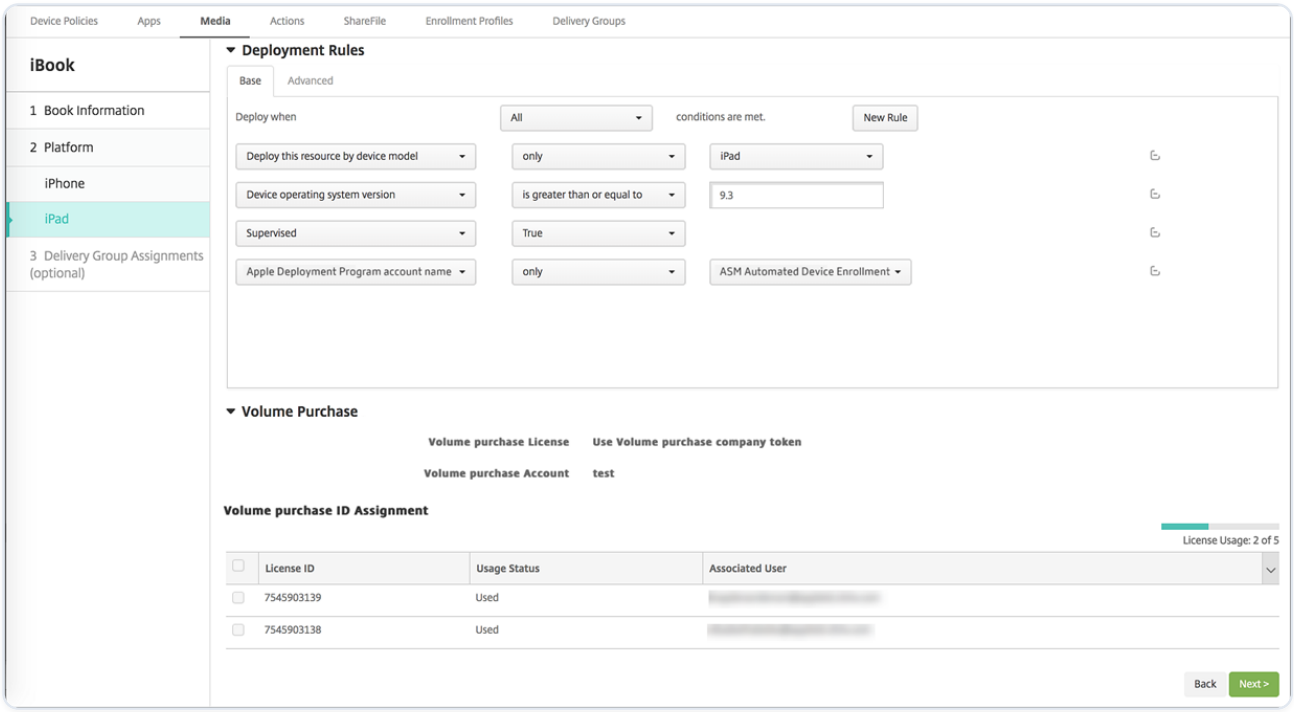
共有iPad用アプリ

共有iPadは、デバイスベースのボリューム購入アプリの割り当てをサポートしています。共有iPadにアプリを展開する前に、Citrix Endpoint ManagementはAppleボリューム購入サーバーにリクエストを送信し、ボリューム購入ライセンスをデバイスに割り当てます。ボリューム購入の割り当てを確認するには、**［構成］>［アプリ］>［iPad］**の順に移動し、［ボリューム購入］**を展開します。

共有iPad用メディア

共有iPadは、ユーザーベースのボリューム購入iBooksの割り当てをサポートしています。共有iPadにiBooksを展開する前に、Citrix Endpoint ManagementはAppleボリューム購入サーバーにリクエストを送信し、ボリューム購入ライセンスをユーザーに割り当てます。ボリューム購入の割り当てを確認するには、**［構成］>［メディア］>［iPad］**の順に移動し、［ボリューム購入］**を展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



共有iPadの展開ルール

共有iPadの展開では、デリバリーグループレベルのルールはユーザープロパティに関連するため適用されません。デバイスの各グループのポリシー、アプリ、メディアをフィルターするには、アカウント名に基づいてリソースの展開ルールを追加します。例：

- デバイスグループ1アカウントの場合、次の展開ルールを設定します。

```
Apple Deployment Program account name

Only

Device Group 1 account
```

- デバイスグループ2アカウントの場合、次の展開ルールを設定します。

```
Apple Deployment Program account name

Only

Device Group 2 account
```

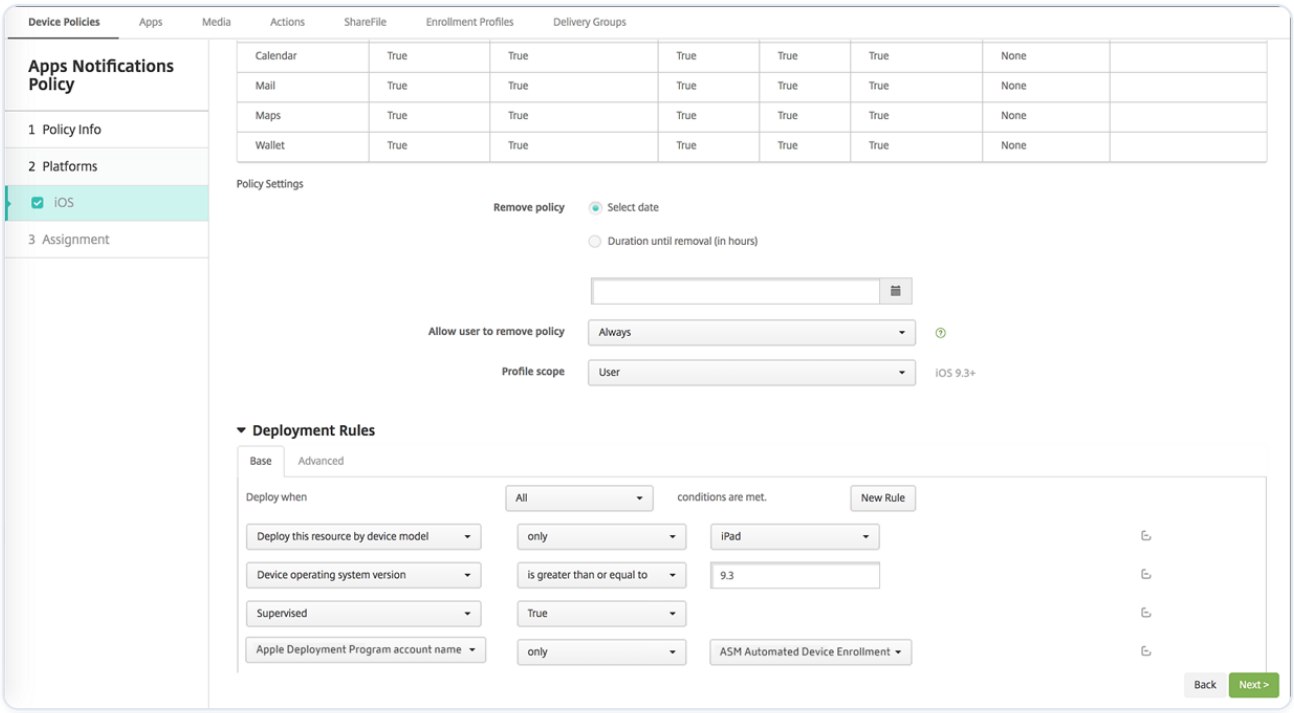
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- デバイスグループNアカウントの場合、次の展開ルールを設定します。

```
Apple Deployment Program account name

Only

Device Group N account
```



Apple Classroomアプリをデバイス所有者 (共有されていないiPadを使用している場合) にのみ展開するには、ASM共有ステータスでリソースをフィルタリングし、次の展開ルールを使用します。

```
Deploy this resource regarding ASM/ABM shared mode

only

unshared
```

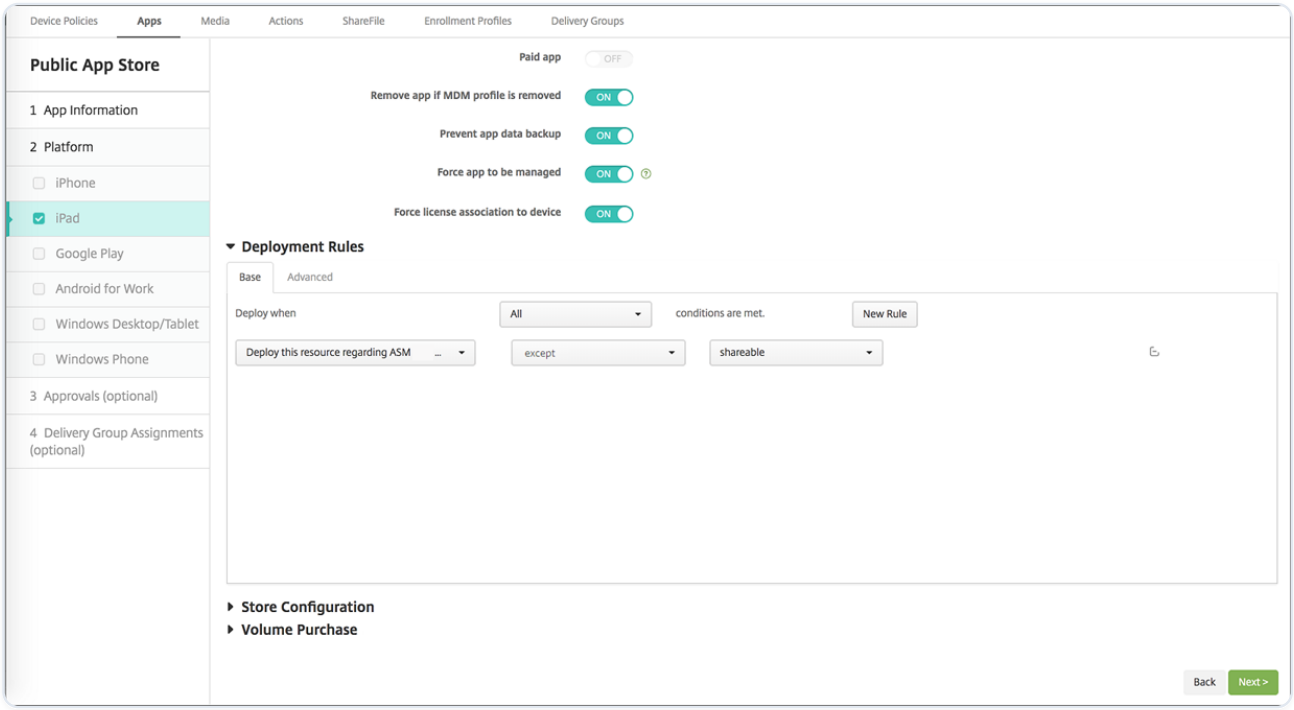
または:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Deploy this resource regarding ASM/ABM shared mode

except

shareable
```

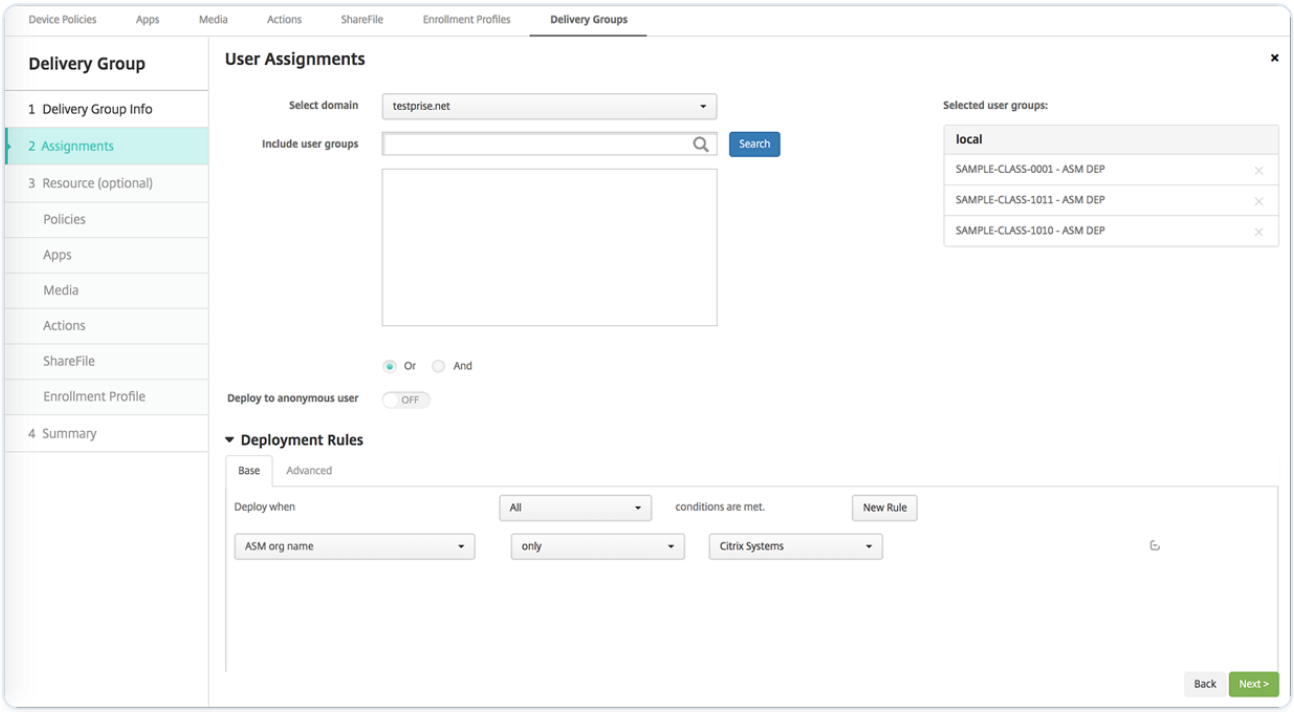


共有iPad用デリバリーグループ

デバイスグループの場合:

- 1つのデリバリーグループを構成します。インストラクターには、Education Configurationポリシーで定義されているすべてのクラスを割り当てます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- そのデリバリーグループには、次のMDMリソースを含める必要があります:
  - デバイスポリシー:
    - 教育設定 (ASM用)
    - ロック画面メッセージ
    - アプリ通知
    - ホーム画面レイアウト
    - 制限
    - 最大常駐ユーザー
    - パスコードロック猶予期間
  - 必須のボリューム購入アプリ
  - 必須のボリューム購入iBooks

デリバリーグループ構成画面(/en-us/citrix-endpoint-management/media/configure-delivery-groups-summary.png)

共有iPadのセキュリティアクション

既存のセキュリティアクションに加えて、共有iPadには以下のセキュリティアクションを使用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **常駐ユーザーの取得:** 現在のデバイスでアクティブなアカウントを持つユーザーを一覧表示します。このアクションにより、デバイスとCitrix Endpoint Managementコンソールの間で同期が強制されます。
- **常駐ユーザーのログアウト:** 現在のユーザーのログアウトを強制します。
- **常駐ユーザーの削除:** 特定のユーザーの現在のセッションを削除します。ユーザーは再度サインインできます。
- **すべてのユーザーを削除:** デバイス上のすべてのユーザーを削除します。

セキュリティアクション画面(/en-us/citrix-endpoint-management/media/security-actions-shared-ipads.png)

常駐ユーザーの削除をクリックした後、ユーザー名を指定できます。

セキュリティアクション画面(/en-us/citrix-endpoint-management/media/force-delete-resident-user-shared-ipad.png)

セキュリティアクションの結果は、**管理 > デバイス > 全般**および**管理 > デバイス > デリバリーグループ**ページに表示されます。

共有iPadに関する情報の取得

「**管理 > デバイス**」ページで、共有iPadに固有の情報を検索します。

- 検索:
  - デバイスが共有されているかどうか（**ASM/ABM共有**）
  - 共有デバイスにログインしているユーザー（**ASM/ABMログインユーザー**）
  - 共有デバイスに割り当てられているすべてのユーザー（**ASM/ABM常駐ユーザー**）

デバイス構成画面(/en-us/citrix-endpoint-management/media/manage-devices-shared-ipad-columns.png)

- デバイスリストを**ASM/ABMデバイスステータス**でフィルタリングします。

デバイス構成画面(/en-us/citrix-endpoint-management/media/manage-devices-shared-ipad-filtered.png)

- 「**管理 > デバイス > ログインユーザープロパティ**」ページで、共有iPadにログインしているユーザーの詳細を表示します。

デバイス構成画面(/en-us/citrix-endpoint-management/media/manage-devices-logged-in-user-properties.png)

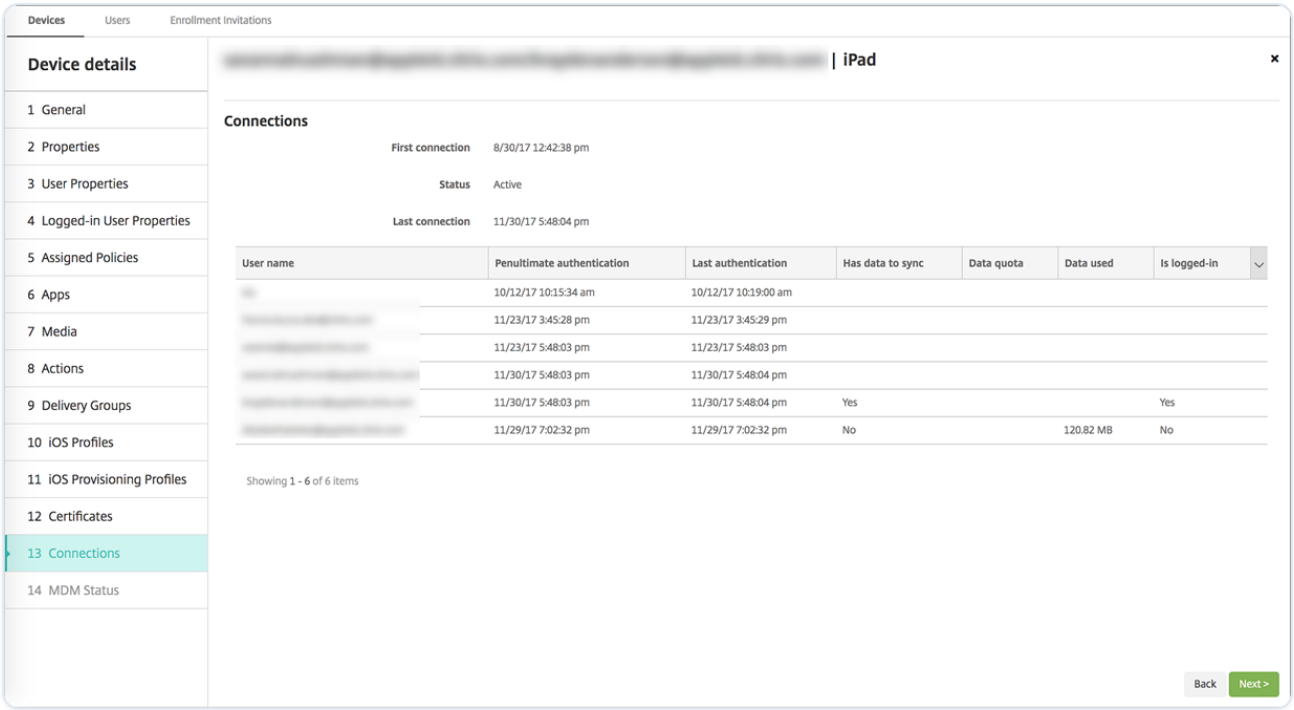
© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイス構成画面(/en-us/citrix-endpoint-management/media/manage-devices-logged-in-user-properties-details.png)

- 「**管理 > デバイス > デリバリーグループ**」ページで、デリバリーグループ内のデバイス所有者とユーザーにリソースを展開するために使用されるチャネルを確認します。「**チャネル/ユーザー**」列には、種類（**システム**または**ユーザー**）と受信者が表示されます。

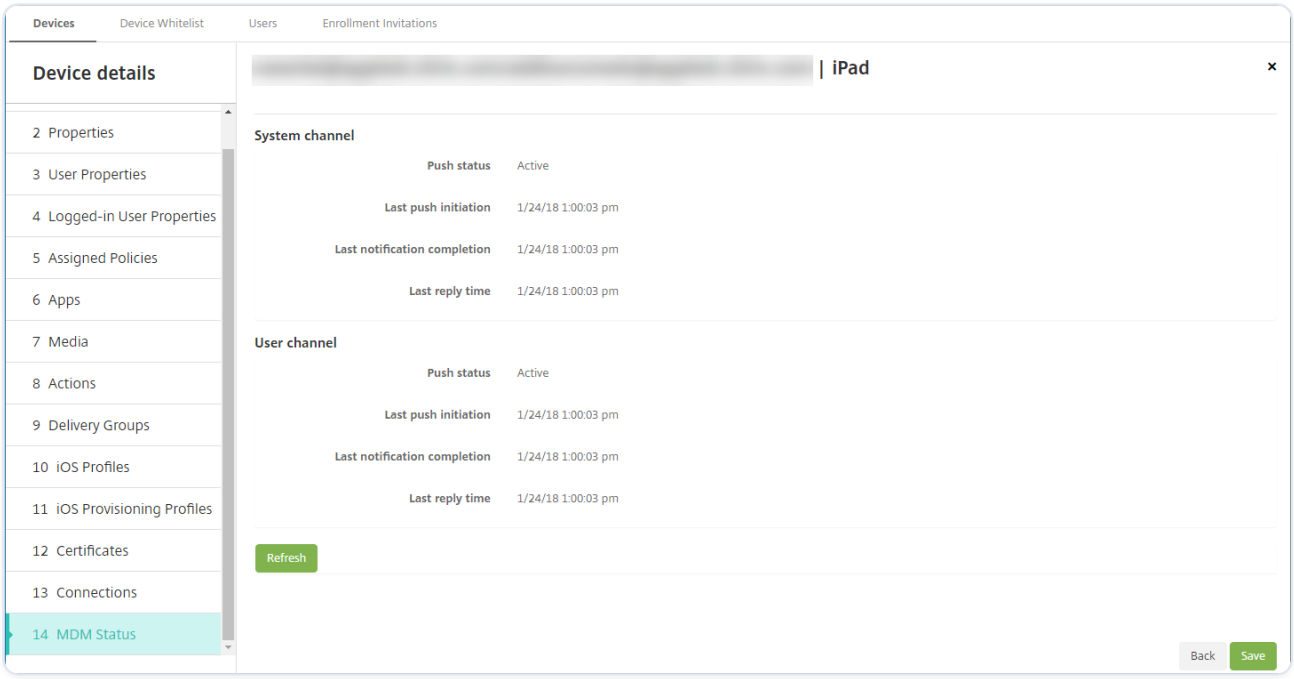
デバイス構成画面(/en-us/citrix-endpoint-management/media/manage-devices-delivery-groups-details.png)

- 常駐ユーザーに関する情報を取得します。
  - **同期するデータがあるか:** ユーザーがクラウドに同期するデータを持っているかどうか。
  - **データクォータ:** ユーザーに設定されたデータクォータ（バイト単位）。ユーザーのクォータが一時的にオフになっているか、ユーザーに適用されていない場合、クォータが表示されないことがあります。
  - **使用済みデータ:** ユーザーが使用したデータ量（バイト単位）。システムが情報を収集する際にエラーが発生した場合、値が表示されないことがあります。
  - **ログイン済み:** ユーザーがデバイスにログインしているかどうか。



- 両方のチャネルのプッシュステータスを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Appleアプリの配布

Citrix Endpoint Management は、デバイスに展開されたアプリを管理します。以下の種類の iOS/iPadOS および macOS アプリを整理して展開できます。

- **パブリックApp Store (iOS/iPadOSのみ):** これらのアプリには、Apple App StoreやGoogle Playなどのパブリックアプリストアで利用可能な無料または有料のアプリが含まれます。例: GoToMeeting。
- **エンタープライズ (iOS/iPadOS/macOS):** MDXが有効になっておらず、MDXアプリに関連付けられたポリシーを持たないネイティブアプリ。
- **MDX (iOS/iPadOSのみ):** MAM SDKで準備されたアプリ、またはMDX Toolkitでラップされたアプリ。これらのアプリにはMDXポリシーが含まれます。MDXアプリは、内部ソースおよびパブリックストアから入手できます。
- **ボリューム購入 (iOS/iPadOS/macOS):** Apple Volume Purchaseプログラムを通じてライセンスが管理されるアプリ。
- **iOSカスタムアプリ (iOS/iPadOSのみ):** 社内またはサードパーティによって開発された独自の企業間アプリ。

さまざまな種類のアプリの詳細については、「アプリの追加」を参照してください。

一部の展開では、Apple Business Management (ABM) またはApple School Management (ASM) アカウントが必要です。詳細については、以下のセクションを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

各アプリの種類と配布方法について、Citrixは一連の構成プラクティスを推奨しています。他のプラットフォーム向けアプリの配布については、「アプリの追加」を参照してください。以下のセクションでは、iOSアプリの構成に関するより詳細な情報を提供します。

アプリ配布の一般的な手順

シナリオ	ステップ1: アカウントのリンク	ステップ2: アプリの追加と構成	ステップ3: デリバリーグループの構成とアプリの展開
「パブリックアプリストアアプリ」(#public-app-store-apps)（Citrixモビリティアプリを含む）	該当なし	**Citrix Endpoint Managementで：** **［構成］** > **［アプリ］** で、iPhoneまたはiPad用の**パブリックアプリストア**アプリを追加します。アプリを構成し、デリバリーグループに割り当てます。	**Citrix Endpoint Managementで：** デリバリーグループを使用してアプリを構成および展開します。
「Apple Volume Purchaseで配信されるパブリックアプリストアアプリ」(#public-app-store-apps-delivered-with-apple-volume-purchase)（Citrixモビリティアプリを含む）	Apple展開プログラムに登録します。**Citrix Endpoint Managementで：** **［設定］** > **［ボリューム購入］** に移動して、ボリューム購入アカウントを追加します。	**ABMまたはASMで：** ［Appとブック］からアプリを購入して追加します。**Citrix Endpoint Managementで：** **［構成］** > **［アプリ］** に移動し、アプリを構成してデリバリーグループに割り当てます。	**Citrix Endpoint Managementで：** デリバリーグループを使用してアプリを構成および展開します。
「エンタープライズアプリ」(#enterprise-apps)	該当なし	**Citrix Endpoint Managementで：** **［構成］** > **［アプリ］** に移動します。**［追加］** をクリックし、**［エンタープライズ］** をクリックします。IPAファイルをアップロードします。アプリを構成	**Citrix Endpoint Managementで：** デリバリーグループを使用してアプリを構成および展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シナリオ	ステップ1: アカウントのリンク	ステップ2: アプリの追加と構成	ステップ3: デリバリーグループの構成とアプリの展開
		し、デリバリーグループに割り当てます。	
「MDXアプリ」(#mdx-apps)	該当なし	**Citrix Endpoint Managementで：**［構成］>［アプリ］ に移動します。［追加］ をクリックし、［MDX］ をクリックします。プラットフォームとして**iPad/iPhone**が選択されていることを確認します。MDXファイルをアップロードします。アプリを構成し、デリバリーグループに割り当てます。	**Citrix Endpoint Managementで:** デリバリーグループを使用してアプリを構成および展開します。
Apple Volume Purchaseを使用して配布されるMDXアプリ	Apple展開プログラムに登録します。**Citrix Endpoint Managementで: 設定 > ボリューム購入** に移動して、ボリューム購入アカウントを追加します。	**ABMで:** 「Appとブック」からMDXアプリを購入して追加します。アプリをABMアカウントにリンクします。**Citrix Endpoint Managementで: 構成 > アプリ**に移動し、アプリを構成してデリバリーグループに割り当てます。	**Citrix Endpoint Managementで:** デリバリーグループを使用してアプリを構成および展開します。
カスタムアプリ	Apple展開プログラムに登録します。**Citrix Endpoint Managementで: 設定 > ボリューム購入** に移動して、ボ	**ABMで:** アプリをプライベートアプリとしてApp Storeに追加します。アプリをABMアカウントにリンクします。**Citrix**	**Citrix Endpoint Managementで:** デリバリーグループを使用してアプリを構

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シナリオ	ステップ1: アカウントのリンク	ステップ2: アプリの追加と構成	ステップ3: デリバリーグループの構成とアプリの展開
	リューム購入アカウントを追加します。	**Endpoint Managementで: 構成 > アプリ**に移動し、アプリを構成してデリバリーグループに割り当てます。	成および展開します。
MDX対応カスタムアプリ	Apple展開プログラムに登録します。**Citrix Endpoint Managementで: 設定 > ボリューム購入**に移動して、ボリューム購入アカウントを追加します。	**ABMで:** アプリをプライベートアプリとしてApp Storeに追加します。アプリをABMアカウントにリンクします。**Citrix Endpoint Managementで: 構成 > アプリ**に移動し、MDXファイルをアップロードします。アプリを構成してデリバリーグループに割り当てます。	**Citrix Endpoint Managementで:** デリバリーグループを使用してアプリを構成および展開します。

公開App Storeアプリ

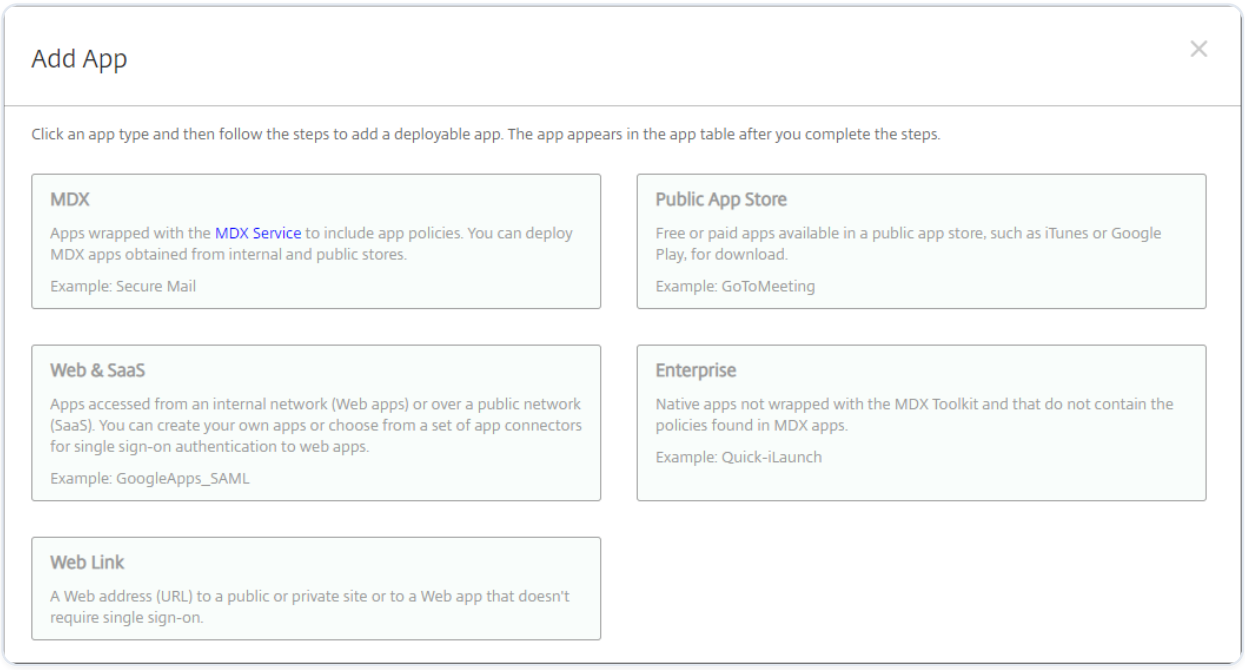
App Storeで利用可能な無料アプリと有料アプリをCitrix Endpoint Managementに追加できます。

機能の利用可能性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	いいえ
利用可能	iOS/iPadOS

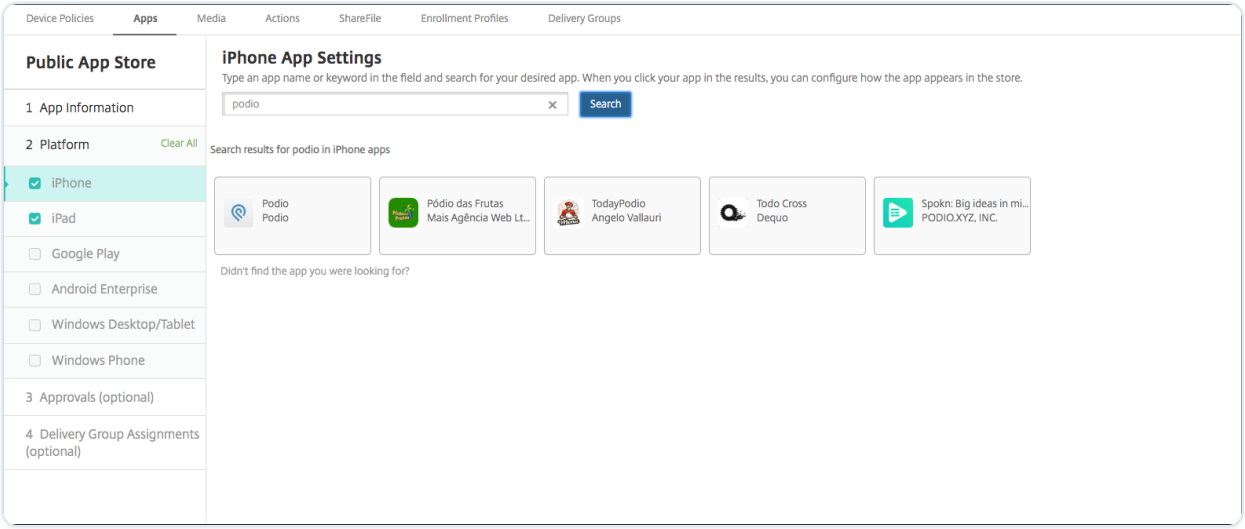
ステップ1：アプリの追加と構成

1. Citrix Endpoint Managementコンソールで、 > に移動します。 をクリックします。
2. をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. プラットフォームとして または を選択します。
4. 検索ボックスにアプリ名を入力し、 をクリックします。



5. 検索条件に一致するアプリが表示されます。目的のアプリをクリックします。
6. アプリにデリバリーグループを割り当て、 をクリックします。

ステップ2：アプリの展開を構成

1. Citrix Endpoint Management コンソールで、**構成 > アプリ**に移動します。
2. 構成するアプリを選択し、**編集**をクリックします。
3. Citrix® は、**アプリの管理を強制**機能を有効にすることを推奨します。
4. デリバリーグループを割り当てて、**保存**をクリックします。
5. **構成 > デリバリーグループ**に移動し、**追加**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. **アプリ**セクションで、目的のアプリを**必須アプリ**ボックスにドラッグします。 アプリを必須としてマークする(/en-us/citrix-endpoint-management/media/required-app-delivery-group-public-app.png)
7. **構成 > デリバリーグループ**に戻ります。
8. デリバリーグループを選択し、**展開**をクリックします。
9. ユーザーはアプリのインストール要求を受け取り、承諾するとアプリはバックグラウンドでインストールされます。 アプリのインストールを要求するメッセージ(/en-us/citrix-endpoint-management/media/ios-app-install.png)

Apple Volume Purchase で配信されるパブリックアプリストアアプリ

Apple Volume Purchase プログラムを通じて、iOS/iPadOS アプリのライセンスを管理できます。Citrix Endpoint Management に Volume Purchase アプリを追加するには、次の手順に従います。

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
利用可能	iOS/iPadOS/macOS

ステップ1：アカウントのリンク

1. Apple Business Manager (ABM) または Apple School Manager (ASM) をセットアップして登録します。これらのプログラムの詳細については、Apple ドキュメント を参照してください。
2. ABM/ASM アカウントを Citrix Endpoint Management にリンクします。ボリューム購入アカウントのリンクの詳細については、Apple ボリューム購入 を参照してください。
3. ボリューム購入アカウントを追加するときに、**App Auto Update** を有効にします。この設定により、Apple Store で更新プログラムが利用可能になったときに、ユーザーデバイス上のアプリが自動的に更新されるようになります。アプリで **Force app to be managed** 設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。更新は、アプリが必要かオプションかに関係なく行われます。

   Force app to be managed および **App Auto Update** 設定を使用するには、`apple.app.force.managed` サーバープロパティを有効にします。サーバープロパティ を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

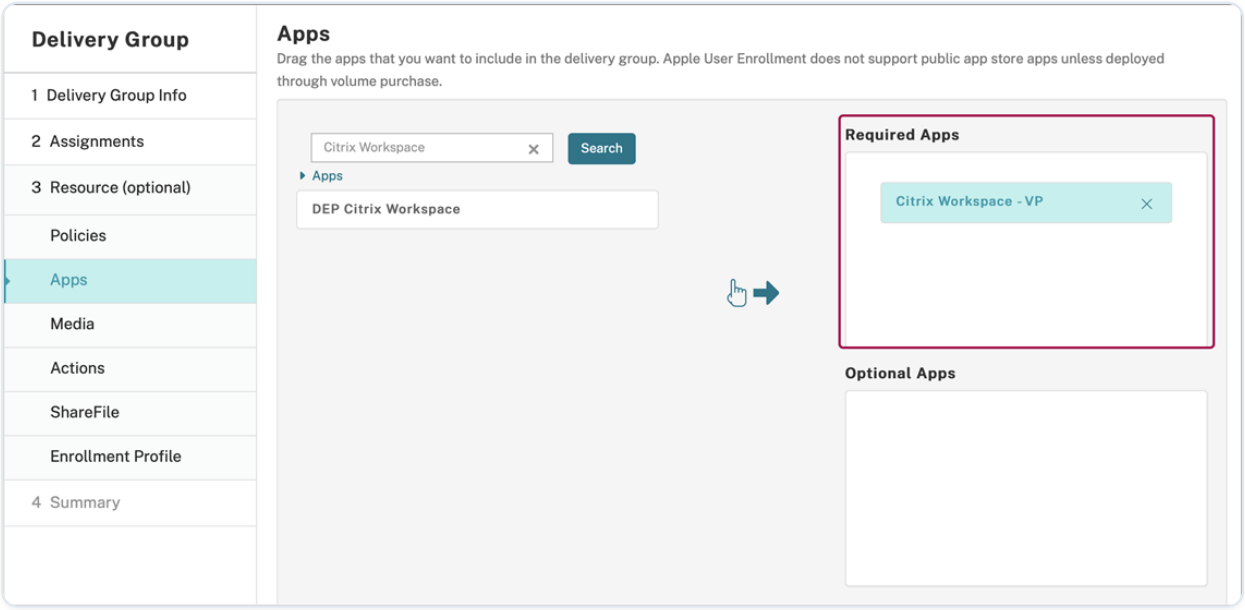
ステップ2：Apple からアプリとライセンスを取得する

ABM/ASM アカウントでアプリを購入します。Apple Books (iOS/iPadOS のみ) および Apple App Store で購入できます。無料のアプリであっても、すべてのアプリを購入する必要があることに注意してください。ABM/ASM でライセンスを購入すると、Citrix Endpoint Management にアプリが自動的に表示されます。

ビジネスでアプリを利用可能にする方法については、Apple ドキュメント を参照してください。

ステップ3：アプリの展開を構成する

1. Citrix Endpoint Management コンソールで、**Configure > Apps** に移動します。
2. 構成するボリューム購入アプリを選択し、**Edit** をクリックします。
3. プラットフォームを選択します: **iPhone**、**iPad**、または **macOS**。
4. Citrix は、**アプリの管理を強制**機能 (iOS/iPadOS のみ) を有効にすることをお勧めします。
5. 任意のデリバリーグループを割り当て、**保存**をクリックします。
6. **構成 > デリバリーグループ**に移動し、**追加**をクリックします。
7. **アプリ**セクションで、目的のアプリを**必須アプリ**ボックスにドラッグします。



8. **構成 > デリバリーグループ**に戻ります。
9. デリバリーグループを選択し、**展開**をクリックします。
10. ユーザーはアプリのインストール要求を受け取り、承諾するとアプリはバックグラウンドでインストールされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



エンタープライズアプリ

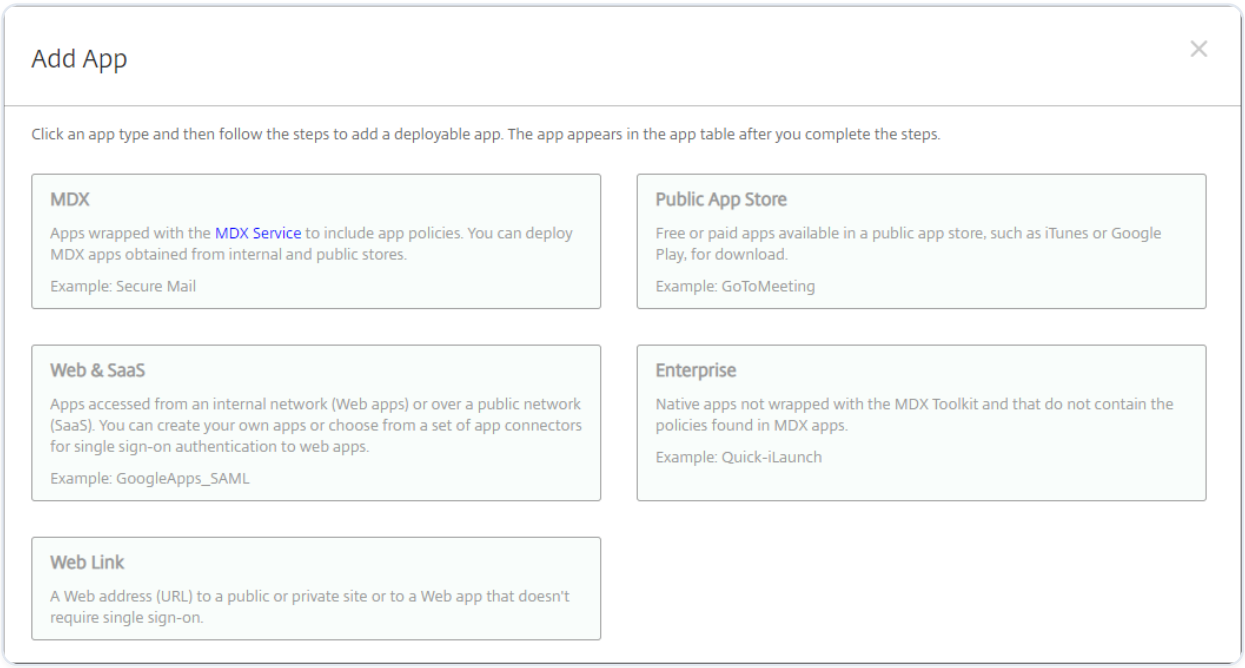
MDXポリシーが関連付けられていないネイティブアプリを追加することもできます。App Storeに存在しないアプリを追加するには、次の手順に従います。

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
OS	iOS/iPadOS/macOS

ステップ1：アプリの追加と構成

1. Citrix Endpoint Managementコンソールで、**構成 > アプリ**に移動します。**追加**をクリックします。
2. **エンタープライズ**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. **アプリ情報**ページで、以下を構成します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルの「アプリ名」の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。

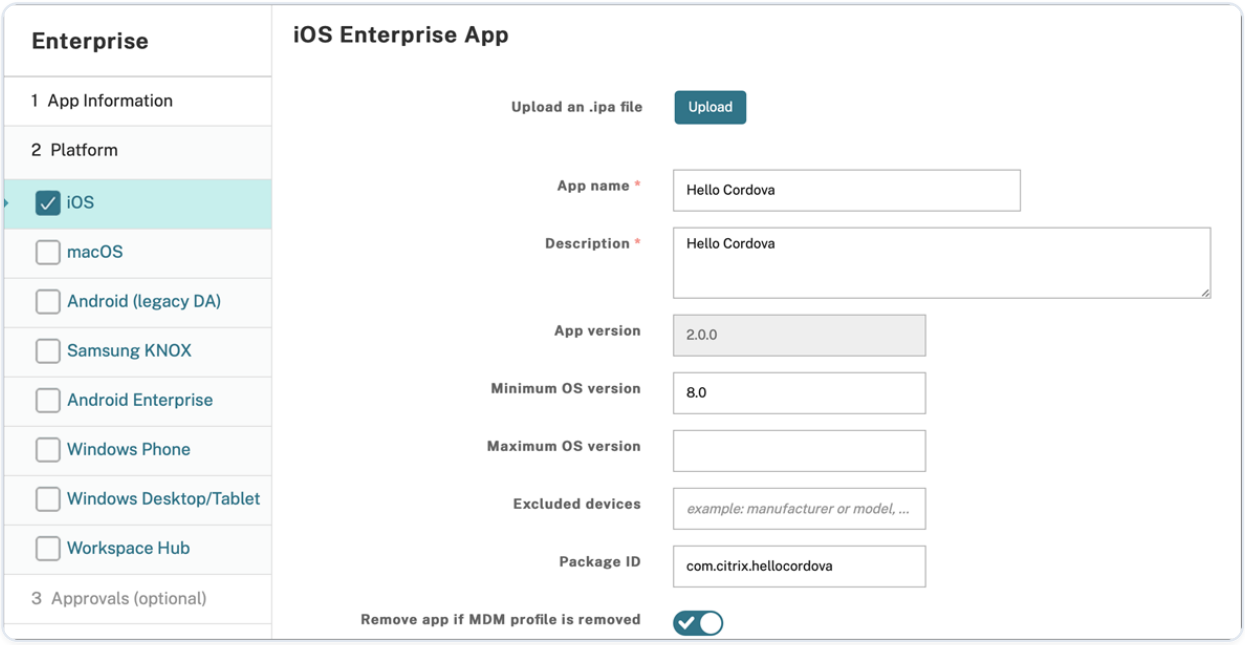
4. **次へ**をクリックします。**アプリプラットフォーム**ページが表示されます。
5. プラットフォームを選択します: **iPhone**、**iPad**、または**macOS**。
6. IPAファイル (iOS/iPadOS) をアップロードするか、PKGファイル (macOS) をアップロードします
7. **次へ**をクリックします。**アプリの詳細**ページが表示されます。
8. これらの設定を構成します:

   - **ファイル名:** オプションで、アプリの新しい名前を入力します。
   - **アプリの説明:** オプションで、アプリの新しい説明を入力します。
   - **アプリのバージョン:** このフィールドは変更できません。
   - **最小OSバージョン:** オプションで、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
   - **最大OSバージョン:** オプションで、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
   - **除外デバイス:** オプションで、アプリを実行できないデバイスの製造元またはモデルを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **MDMプロファイルが削除された場合にアプリを削除:** MDMプロファイルが削除されたときにデバイスからアプリを削除するかどうかを選択します。デフォルトはオンです。(iOS/iPadOSのみ)
- **アプリのデータバックアップを防止:** アプリがデータをバックアップするのを防止するかどうかを選択します。デフォルトはオンです。(iOS/iPadOSのみ)
- **アプリの管理を強制:** 管理されていないアプリをインストールする場合、監視されていないデバイスのユーザーにアプリの管理を許可するプロンプトを表示させたい場合は、**オン**を選択します。ユーザーがプロンプトを受け入れると、アプリは管理されます。アプリで**アプリの管理を強制**設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。更新は、アプリが必要かオプションかに関わらず行われます。(iOS/iPadOSのみ)

アプリの管理を強制および**アプリの自動更新**設定を使用するには、`apple.app.force.managed`サーバープロパティを有効にします。サーバープロパティを参照してください。

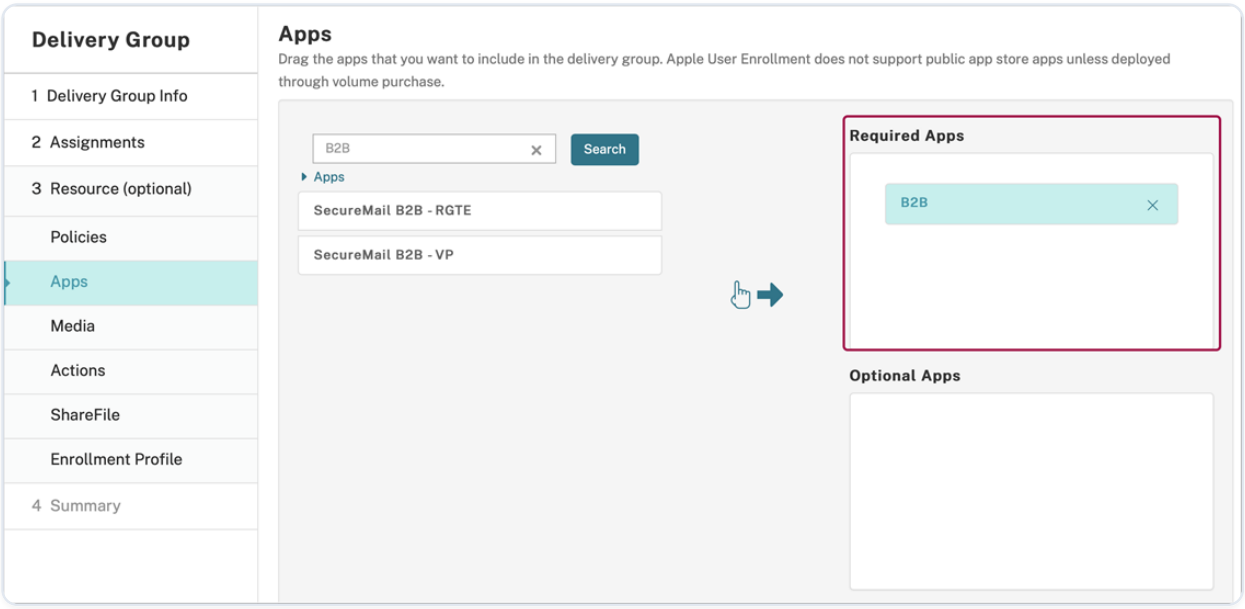


9. アプリにデリバリーグループを割り当て、**保存**をクリックします。

手順2：アプリの展開を構成する

1. Citrix Endpoint Managementコンソールで、**構成 > デリバリーグループ**に移動します。構成するデリバリーグループを選択し、**アプリ**ページをクリックします。
2. 目的のアプリを**必須アプリ**ボックスにドラッグします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. **構成 > デリバリーグループ**に移動します。
4. デリバリーグループを選択し、**展開**をクリックします。
5. ユーザーはアプリのインストール要求を受け取り、承認するとアプリはバックグラウンドでインストールされます。



MDXアプリ

MDXポリシーとセキュリティ機能を使用するには、MAM SDKが有効なアプリまたはMDXでラップされたアプリを追加します。MDXアプリは、ボリューム購入を使用しても、使用しなくても展開できます。

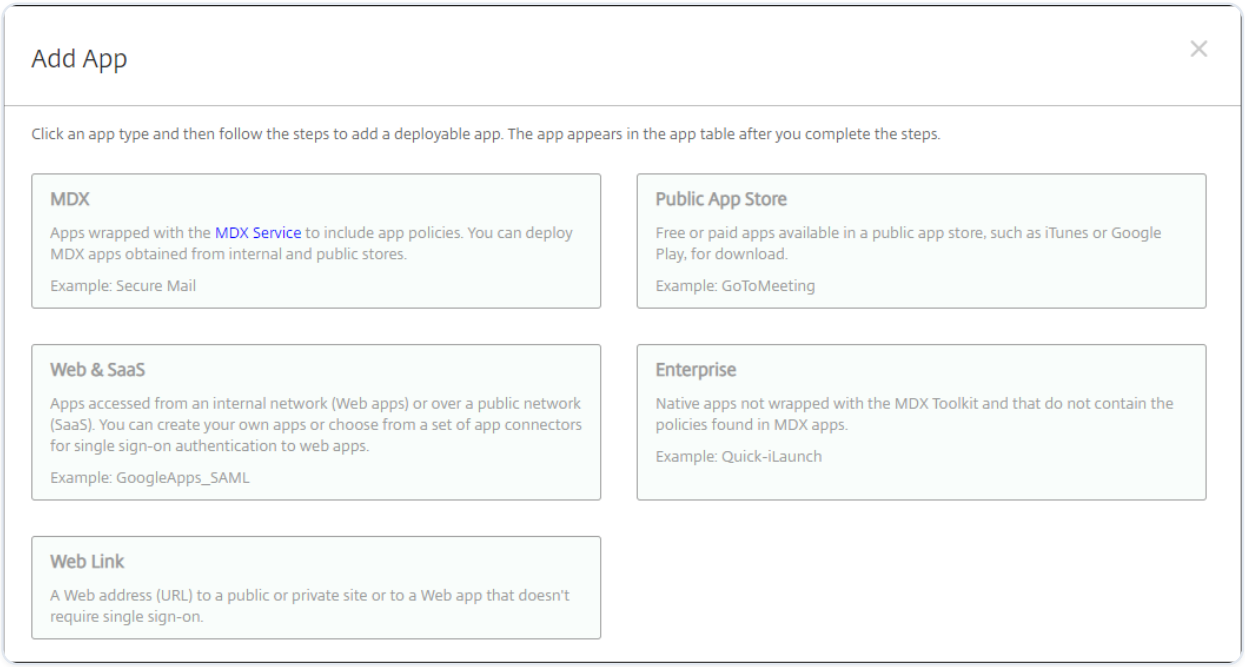
© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
利用可能なプラットフォーム	iOS/iPadOS

パブリックアプリストアアプリのMDXバージョンを追加するには、パブリックアプリストアアプリの手順に従ってから、このセクションの手順に従います。

ステップ1：アプリの追加と構成

1. Citrix Endpoint Managementコンソールで、 > の順に移動します。 をクリックします。
2. をクリックします。



3. プラットフォームとして または を選択します。
4. MDXファイルをアップロードします。
5. アプリの詳細を構成します。「**Volume Purchase経由で展開されたアプリ**」を「**オフ**」に設定します。Citrixは、「**アプリの管理を強制**」機能を有効にすることも推奨しています。 (/en-us/citrix-endpoint-management/media/mdx-app-volume-purchase-off.png)
6. MDXポリシーを構成します。「**必須アップグレードを無効にする**」を「**オン**」に設定します。(/en-us/citrix-endpoint-management/media/mdx-app-disable-required-upgrade.png)
7. アプリにデリバリーグループを割り当て、「**保存**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステップ2：アプリの展開を構成する

1. Citrix Endpoint Managementコンソールで、「**構成 > デリバリーグループ**」に移動し、「**追加**」をクリックします。
2. 「**アプリ**」セクションで、目的のアプリを「**必須アプリ**」ボックスにドラッグします。 (/en-us/citrix-endpoint-management/media/required-app-delivery-group-mdx.png)
3. 「**構成 > デリバリーグループ**」に移動します。
4. デリバリーグループを選択し、「**展開**」をクリックします。
5. ユーザーはアプリのインストール要求を受け取り、承諾するとアプリはバックグラウンドでインストールされます。 (/en-us/citrix-endpoint-management/media/ios-app-install.png)

Apple Volume Purchaseを使用して配布されるMDXアプリ

MDXポリシーとセキュリティ機能を使用するには、MAM SDKが有効になっているアプリまたはMDXでラップされたアプリを追加します。Volume Purchaseを使用してアプリを展開するには、アプリがアプリストアに存在している必要があります。

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
利用可能なプラットフォーム	iOS/iPadOS

ステップ1：アカウントをリンクする

1. Apple Business Manager (ABM) または Apple School Manager (ASM) をセットアップして登録します。これらのプログラムの詳細については、Apple ドキュメントを参照してください。
2. ABM/ASM アカウントを Citrix Endpoint Management にリンクします。ボリューム購入アカウントのリンクの詳細については、Apple Volume Purchaseを参照してください。
3. ボリューム購入アカウントを追加する際に、**App Auto Update** を有効にします。この設定により、Apple Store でアップデートが利用可能になったときに、ユーザーデバイス上のアプリが自動的に更新されるようになります。アプリで **Force app to be managed** 設定が有効になっている場合、ユーザーにプロンプトを表示することなく更新されます。この更新は、アプリが必須であるかオプションであるかに関わらず行われます。

   Force app to be managed および **App Auto Update** の設定を使用するには、`apple.app.force.managed` サーバープロパティを有効にします。サーバープロパティを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

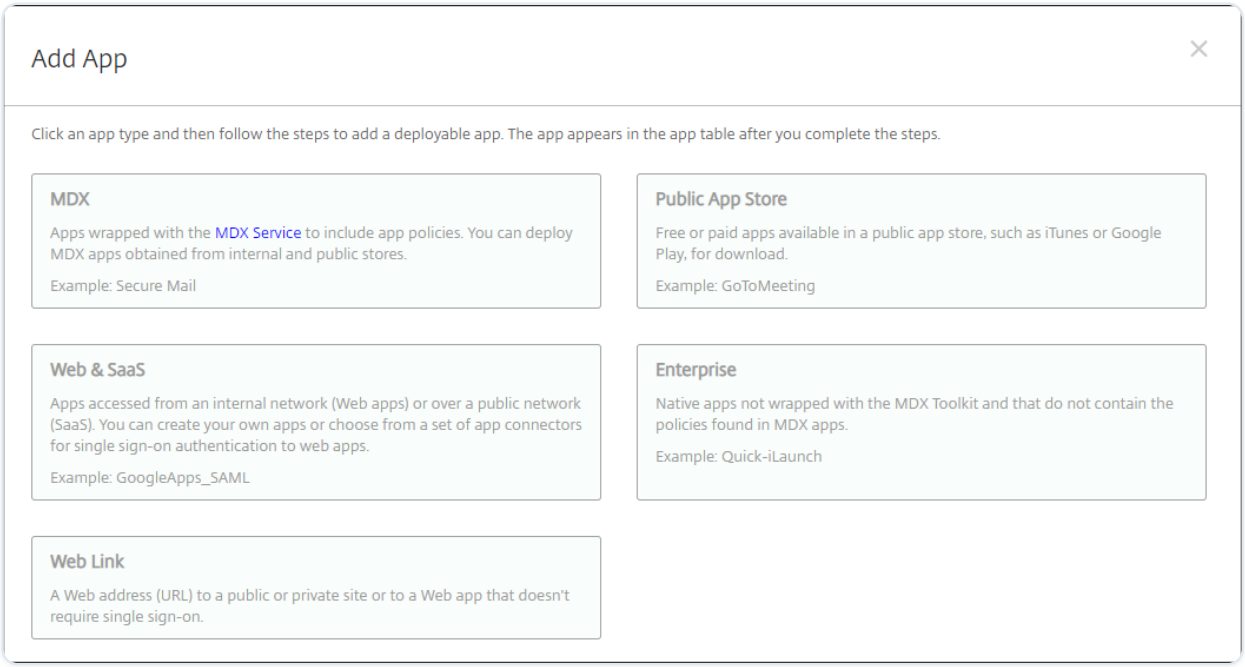
ステップ2：Apple からアプリとライセンスを取得する

ABM/ASM アカウントでアプリを購入します。購入は Apple Books (iOS/iPadOS のみ) および Apple App Store で行うことができます。無料のアプリであっても、すべてのアプリを購入する必要があることに注意してください。ABM/ASM でライセンスを購入すると、Citrix Endpoint Management にアプリが自動的に表示されます。

アプリをビジネスで利用可能にする方法については、Apple ドキュメントを参照してください。

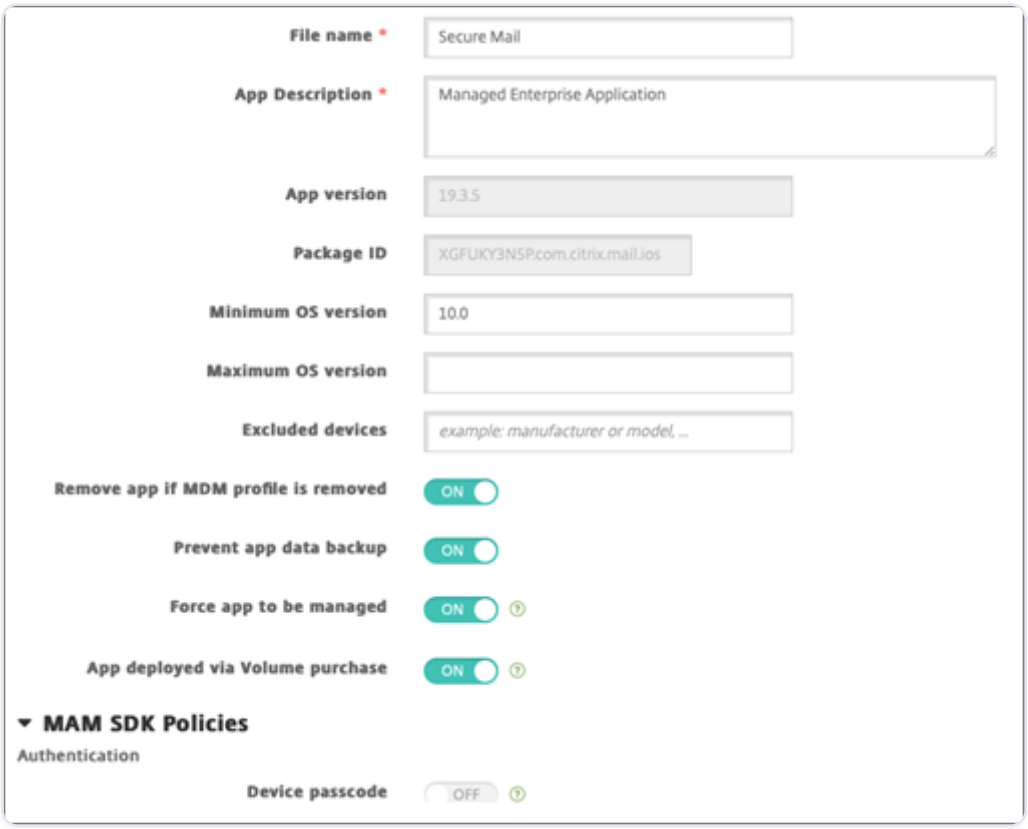
ステップ3：アプリを追加して構成する

1. Citrix Endpoint Management コンソールで、**Configure > Apps** に移動します。**Add** をクリックします。
2. **MDX** をクリックします。

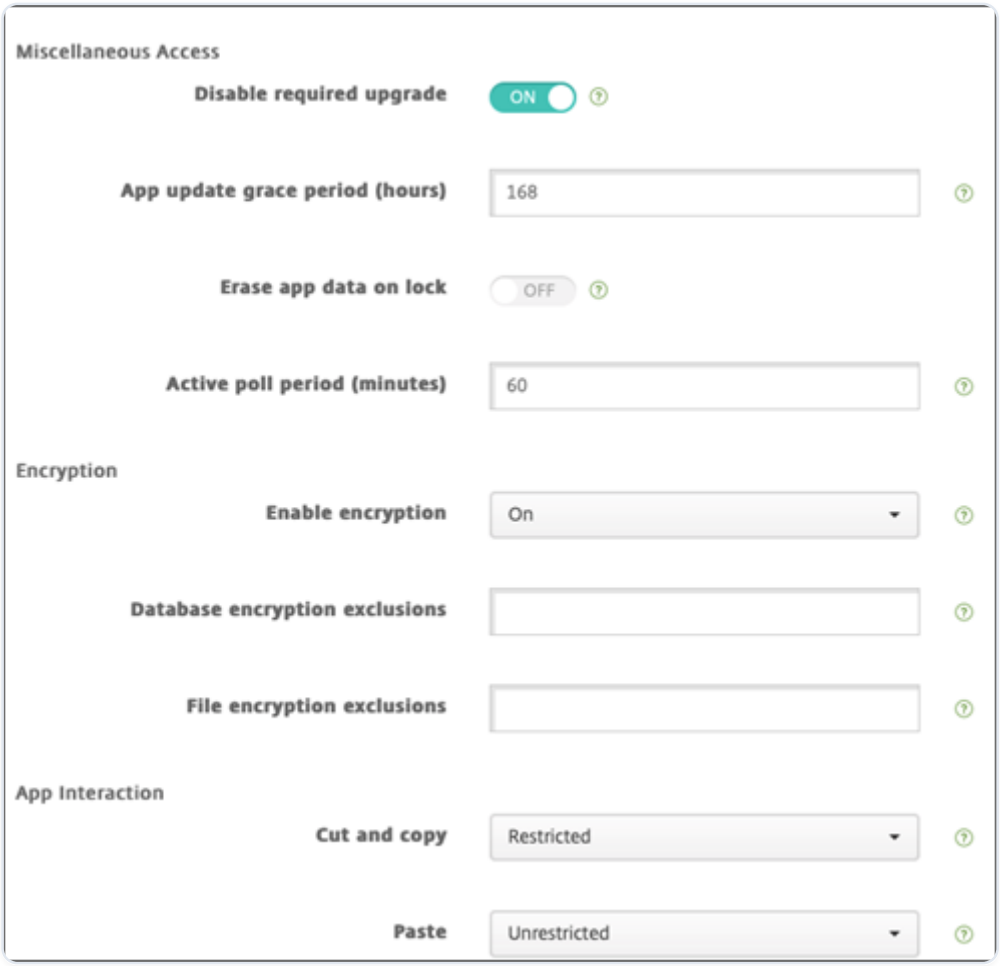


3. プラットフォームには**iPhone**または**iPad**を選択します。
4. MDXファイルをアップロードします。
5. アプリの詳細を構成します。**Volume Purchase経由で展開されたアプリ**を**オン**に設定します。Citrixは、**アプリの管理を強制する**機能を有効にすることも推奨しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. MDXポリシーを構成します。**必須アップグレードを無効にする**を**オン**に設定します。



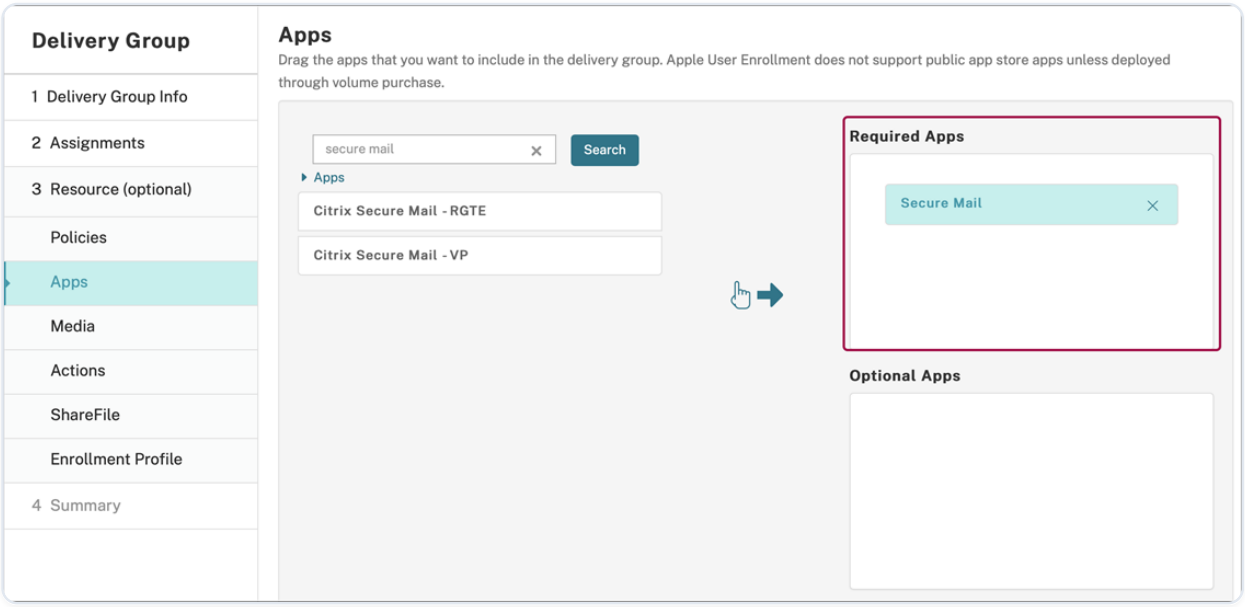
7. 各プラットフォームのアプリにデリバリーグループを割り当て、**保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

この構成により、アプリリストにこのアプリの2つのエントリがリストされます。アプリを構成するためにアプリを選択するときは、**種類**が**MDX**のアプリを選択します。

ステップ4：アプリの展開を構成する

1. Citrix Endpoint Managementコンソールで、**構成 > デリバリーグループ**に移動し、**追加**をクリックします。
2. **アプリ**セクションで、目的のMDXアプリを**必須アプリ**ボックスにドラッグします。



3. **構成 > デリバリーグループ**に移動します。
4. デリバリーグループを選択し、**展開**をクリックします。
5. ユーザーはアプリのインストール要求を受け取り、承諾するとアプリはバックグラウンドでインストールされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



カスタムアプリ

カスタムアプリは、独自の企業間アプリです。Citrix Endpoint ManagementとApple Volume Purchaseを使用して、独自のアプリをプライベートかつ安全に配布できます。アプリは、特定のパートナー、クライアント、フランチャイズ加盟店、および社内従業員に配布できます。

機能の可用性	
デバイスの監視が必要です	いいえ
ユーザー登録モードで利用可能	はい
利用可能	iOS/iPadOS

カスタムアプリの要件

- Apple Business ManagerまたはApple School Managerアカウント
- Apple Volume Purchaseアカウント（iOS 7以降のデバイスが必要）
- 以下のいずれかのApple登録モードを使用して、Citrix Endpoint Managementにデバイスを登録します。
  - 自動デバイス登録
  - デバイス登録

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ユーザー登録

ステップ1：アカウントのリンク

Volume Purchaseを使用してカスタムアプリを展開するには、Volume PurchaseアカウントをCitrix Endpoint Managementにリンクします。

1. Apple Business Manager (ABM) をセットアップして登録します。これらのプログラムの詳細については、Apple ドキュメントを参照してください。
2. ABM アカウントを Citrix Endpoint Management にリンクします。ボリューム購入アカウントのリンクの詳細については、Apple ボリューム購入を参照してください。
3. ボリューム購入アカウントを追加するときに、**App Auto Update** を有効にします。この設定により、Apple Store に更新が表示されたときに、ユーザーデバイス上のアプリが自動的に更新されるようになります。アプリで **Force app to be managed** 設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。更新は、アプリが必要かオプションかに関係なく行われます。

   Force app to be managed および **App Auto Update** 設定を使用するには、`apple.app.force.managed` サーバープロパティを有効にします。サーバープロパティを参照してください。

手順 2：ABM でアプリを構成する

ABM アカウントにアプリを追加します。独自のカスタムアプリをアップロードして配布したり、他の組織からカスタムアプリのライセンスを購入したりできます。ABM でカスタムアプリを追加して有効にする方法の詳細については、Apple ドキュメントを参照してください。

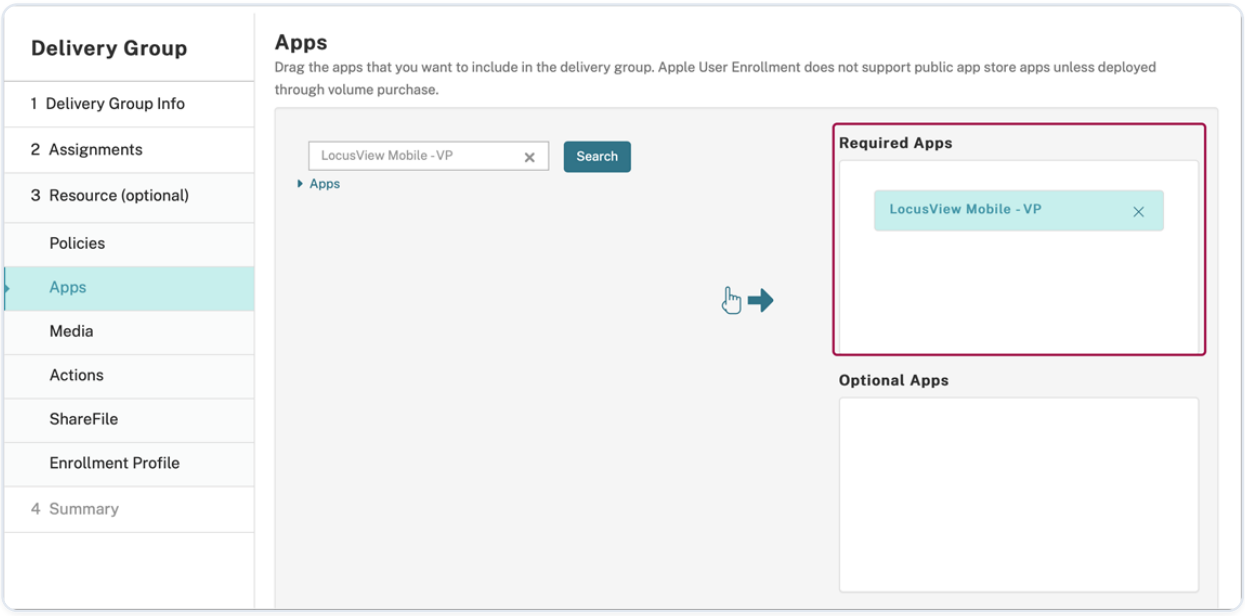
手順 3：Citrix Endpoint Management でアプリを追加および構成する

1. Citrix Endpoint Management コンソールで、［**構成**］>［**アプリ**］ の順に移動します。ボリューム購入アプリがアプリの一覧に表示されます。
2. 構成するアプリを選択します。［**編集**］ をクリックします。
3. プラットフォームを選択します：**iPhone**、**iPad**、または **macOS**。
4. アプリを配布するデリバリーグループを選択します。［**保存**］ をクリックします。

手順 4：アプリの展開を構成する

1. Citrix Endpoint Management コンソールで、［**構成**］>［**デリバリーグループ**］ の順に移動し、［**追加**］ をクリックします。
2. ［**アプリ**］ セクションで、目的のアプリを ［**必須アプリ**］ ボックスにドラッグします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. **［構成］**>**［デリバリーグループ］** に戻ります。
4. 展開するデリバリーグループを選択し、**展開**をクリックします。
5. ユーザーはアプリの展開要求を受け取ります。ユーザーが承認すると、アプリはバックグラウンドでインストールされます。



MDX対応カスタムアプリ

MDXポリシーとセキュリティ機能を使用するには、MAM SDK対応またはMDXでラップされたカスタムアプリを追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
利用可能	iOS/iPadOS

ステップ1：アカウントのリンク

ボリューム購入を使用してカスタムアプリを展開するには、ボリューム購入アカウントをCitrix Endpoint Managementにリンクします。

1. Apple Business Manager (ABM) をセットアップして登録します。これらのプログラムの詳細については、Appleのドキュメントを参照してください。
2. ABMアカウントをCitrix Endpoint Managementにリンクします。ボリューム購入アカウントのリンクの詳細については、Apple Volume Purchaseを参照してください。
3. ボリューム購入アカウントを追加する際に、**アプリの自動更新**を有効にします。この設定により、Apple Storeでアップデートが利用可能になったときに、ユーザーデバイス上のアプリが自動的に更新されるようになります。アプリで**アプリの管理を強制**設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。更新は、アプリが必須であるかオプションであるかに関わらず行われます。

   アプリの管理を強制および**アプリの自動更新**設定を使用するには、`apple.app.force.managed`サーバープロパティを有効にします。サーバープロパティを参照してください。

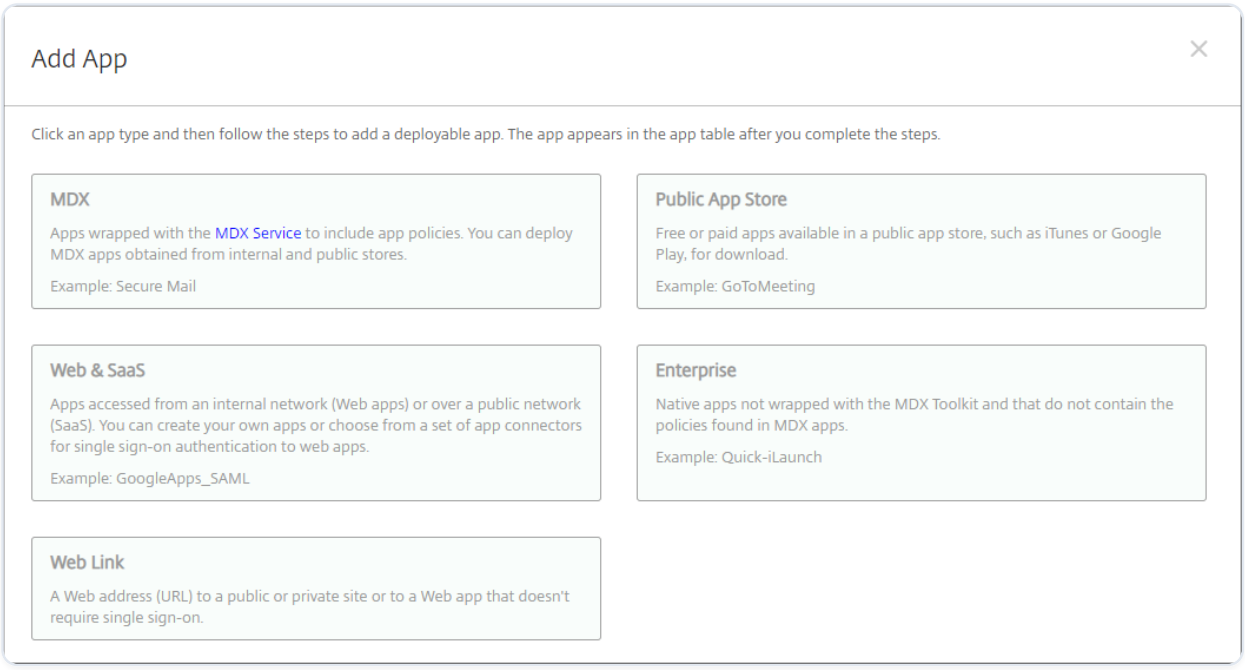
ステップ2：ABMでアプリを構成する

ABMアカウントにアプリを追加します。独自のカスタムアプリをアップロードして配布したり、他の組織からカスタムアプリのライセンスを購入したりできます。ABMでのカスタムアプリの追加と有効化の詳細については、Appleのドキュメントを参照してください。

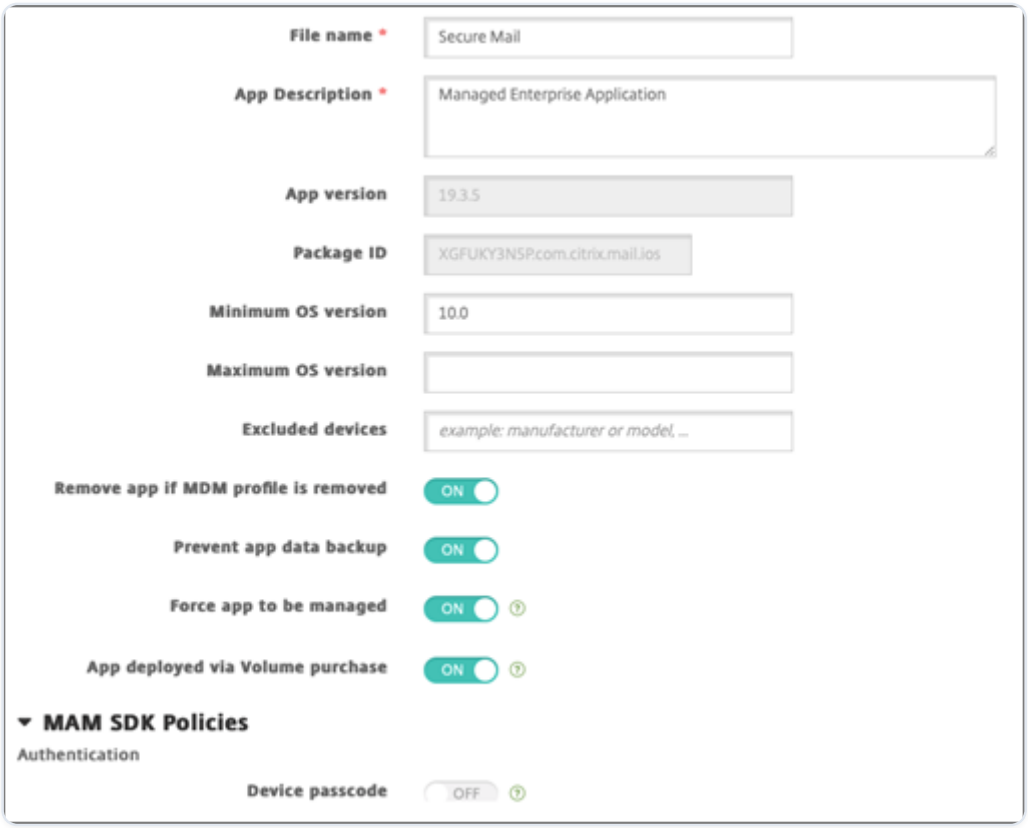
ステップ3：Citrix Endpoint Managementでアプリを追加および構成する

1. Citrix Endpoint Managementコンソールで、**構成 > アプリ**に移動します。**追加**をクリックします。
2. **MDX**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

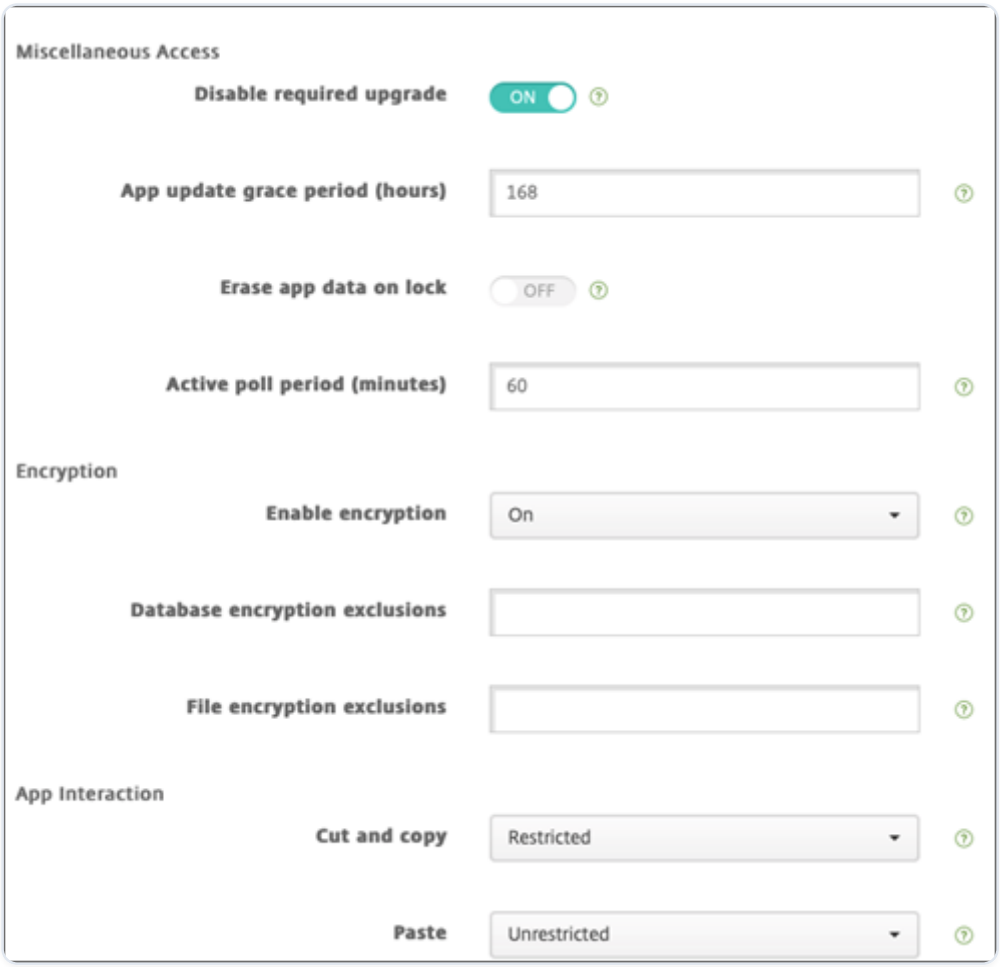


3. **iPhone**または**iPad**プラットフォームを選択します。
4. 追加するアプリのMDXファイルをアップロードします。
5. アプリの詳細を構成します。**ボリューム購入経由で展開されたアプリ**を**オン**に設定します。Citrixは、**アプリの管理を強制**機能を有効にすることも推奨しています。



6. MDXポリシーを構成します。**必須アップグレードを無効にする**を**オン**に設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. アプリにデリバリーグループを割り当て、**保存**をクリックします。

この構成により、アプリリストにこのアプリの2つのエントリが表示されます。構成するアプリを選択するときは、**種類**が**MDX**のアプリを選択します。

ステップ4：アプリの展開を構成する

1. Citrix Endpoint Managementコンソールで、**構成 > アプリ**に移動します。ボリューム購入アプリがアプリのリストに表示されます。
2. 設定したいアプリを選択します。「**編集**」をクリックします。
3. 各プラットフォームでアプリを配信するデリバリーグループを選択します。「**保存**」をクリックします。
4. 「**構成 > デリバリーグループ**」に移動し、「**追加**」をクリックします。
5. 「**アプリ**」セクションで、必要なMDXアプリを「**必須アプリ**」ボックスにドラッグします。 (/en-us/citrix-endpoint-management/media/required-app-delivery-group-mdx-custom.png)
6. 「**構成 > デリバリーグループ**」に戻ります。
7. 展開したいデリバリーグループを選択し、「**展開**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. ユーザーはアプリの展開リクエストを受け取ります。ユーザーが承認すると、アプリはバックグラウンドでインストールされます。 (/en-us/citrix-endpoint-management/media/ios-app-install.png)

オプションアプリ（iOS/iPadOSのみ）

Citrixでは、アプリを「**必須**」として展開することを推奨しています。必須アプリはユーザーデバイスにサイレントインストールされ、ユーザーの操作を最小限に抑えます。この機能を有効にすると、アプリが自動的に更新されるようにもなります。

オプションアプリでは、ユーザーがインストールするアプリを選択できますが、Citrix Secure Hubを介して手動でインストールを開始する必要があります。

オプションアプリをインストールするには、ユーザーはCitrix Secure Hubを起動し、「**ストア**」に移動して、目的のアプリの「**詳細**」を選択し、「**追加**」をクリックする必要があります。 (/en-us/citrix-endpoint-management/media/ios-install-optional-app.png)

ネットワークアクセスコントロール

ネットワークアクセスコントロール (NAC) ソリューションを使用して、AndroidおよびAppleデバイス向けのCitrix Endpoint Managementデバイスセキュリティ評価を拡張できます。NACソリューションは、Citrix Endpoint Managementセキュリティ評価を使用して認証決定を促進および処理します。NACアプライアンスを構成すると、Citrix Endpoint Managementで構成したデバイスポリシーとNACフィルターが適用されます。

NACソリューションとCitrix Endpoint Managementを併用することで、ネットワーク内部のデバイスに対するQoSとよりきめ細かな制御が追加されます。NACとCitrix Endpoint Managementを統合する利点の概要については、「アクセス制御」を参照してください。

Citrixは、Citrix Endpoint Managementとの統合のために以下のソリューションをサポートしています。

- ネットスケーラー ゲートウェイ
- ForeScout

Citrix®は、他のNACソリューションとの統合を保証しません。

ネットワークにNACアプライアンスがある場合：

- Citrix Endpoint Managementは、iOS、Android Enterprise、およびAndroidデバイスのエンドポイントセキュリティ機能としてNACをサポートしています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Managementでフィルターを有効にして、ルールまたはプロパティに基づいて、NACのデバイスを準拠または非準拠として設定できます。例：
  - Citrix Endpoint Managementで管理されているデバイスが指定された基準を満たさない場合、Citrix Endpoint Managementはそのデバイスを非準拠としてマークします。NACアプライアンスは、ネットワーク上の非準拠デバイスをブロックします。
  - Citrix Endpoint Managementで管理されているデバイスに非準拠アプリがインストールされている場合、NACフィルターはVPN接続をブロックできます。その結果、非準拠のユーザーデバイスはVPNを介してアプリやWebサイトにアクセスできません。
  - NACにNetScaler Gatewayを使用している場合、NetScaler Gatewayプラグインが不要なネットワークトラフィックをNetScaler Gatewayに送信するのを防ぐために、スプリットトンネリングを有効にできます。スプリットトンネリングの詳細については、「スプリットトンネリングの構成」を参照してください。

サポートされているNAC準拠フィルター

Citrix Endpoint Managementは、以下のNAC準拠フィルターをサポートしています。

匿名デバイス： デバイスが匿名モードであるかどうかを確認します。このチェックは、デバイスが再接続しようとしたときにCitrix Endpoint Managementがユーザーを再認証できない場合に利用できます。

禁止されているアプリ： デバイスに、アプリアクセスポリシーで定義されている禁止されているアプリがあるかどうかを確認します。そのポリシーの詳細については、「アプリアクセスのデバイスポリシー」を参照してください。

非アクティブなデバイス： **Server Properties**の**Device Inactivity Days Threshold**設定で定義されているように、デバイスが非アクティブであるかどうかを確認します。詳細については、「サーバープロパティ」を参照してください。

不足している必須アプリ： デバイスに、アプリアクセスポリシーで定義されている必須アプリが不足しているかどうかを確認します。

推奨されないアプリ： デバイスに、アプリアクセスポリシーで定義されている推奨されないアプリがあるかどうかを確認します。

準拠していないパスワード： ユーザーパスワードが準拠しているかどうかを確認します。iOSおよびAndroidデバイスでは、Citrix Endpoint Managementは、現在デバイス上にあるパスワードが、デバイスに送信されたパスコードポリシーに準拠しているかどうかを判断できます。たとえば、iOSでは、Citrix Endpoint Managementがデバイスにパスコードポリシーを送信した場合、ユー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ザーは60分以内にパスワードを設定する必要があります。ユーザーがパスワードを設定する前は、パスコードが準拠していない可能性があります。

準拠していないデバイス： デバイスが、準拠していないデバイスプロパティに基づいて、準拠していないかどうかを確認します。通常、自動化されたアクションまたはCitrix Endpoint Management APIを使用するサードパーティがそのプロパティを変更します。

失効ステータス： デバイス証明書が失効しているかどうかを確認します。失効したデバイスは、再度承認されるまで再登録できません。

ルート化されたAndroidデバイスとジェイルブレイクされたiOSデバイス： AndroidまたはiOSデバイスがジェイルブレイクされているかどうかを確認します。

管理されていないデバイス： Citrix Endpoint Managementがデバイスを管理しているかどうかを確認します。たとえば、MAMに登録されているデバイスや未登録のデバイスは管理されていません。

> **注：**
>
> 暗黙的な準拠/非準拠フィルターは、Citrix Endpoint Managementが管理しているデバイスにのみデフォルト値を設定します。たとえば、ブロックされたアプリがインストールされているデバイスや登録されていないデバイスは、非準拠としてマークされます。NACアプライアンスは、これらのデバイスをネットワークからブロックします。

構成の概要

NACコンポーネントは、記載されている順序で構成することをお勧めします。

1. NACをサポートするようにデバイスポリシーを構成します。

   iOSデバイスの場合: NACをサポートするようにVPNデバイスポリシーを構成するを参照してください。

   Android Enterpriseデバイスの場合: Citrix SSOのAndroid Enterprise管理対象構成を作成するを参照してください。

   Androidデバイスの場合: Android向けCitrix SSOプロトコルを構成するを参照してください。
2. Citrix Endpoint ManagementでNACフィルターを有効にする。
3. NACソリューションを構成します:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

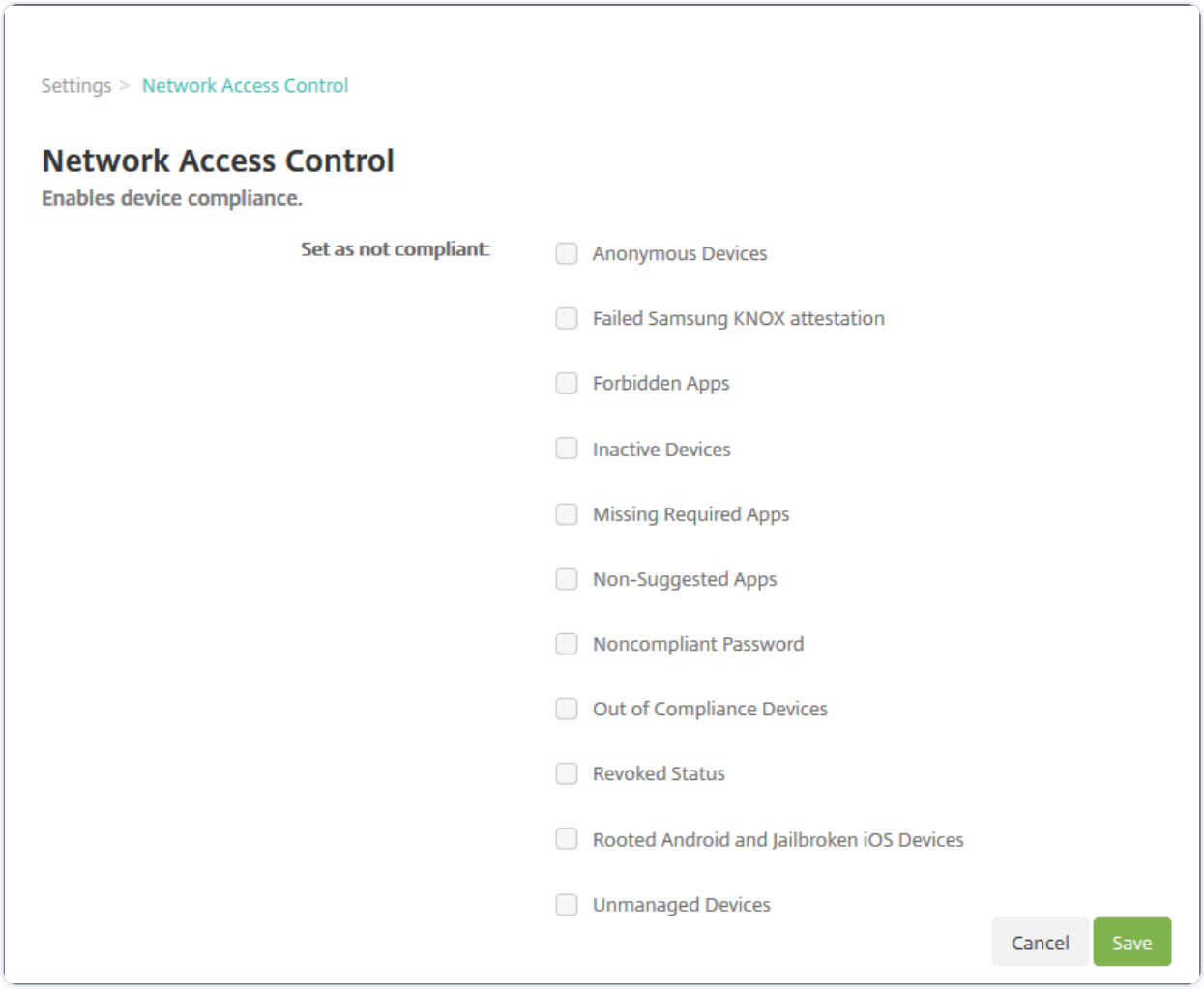
- NetScaler Gateway。NACをサポートするようにNetScaler Gatewayポリシーを更新するに詳述されています。

  デバイスにCitrix SSOをインストールする必要があります。NetScaler Gatewayクライアントを参照してください。

- ForeScout: ForeScoutのドキュメントを参照してください。

Citrix Endpoint ManagementでNACフィルターを有効にする

1. Citrix Endpoint Managementコンソールで、**設定 > ネットワークアクセス制御**に移動します。



2. 有効にする**非準拠として設定**フィルターのチェックボックスをオンにします。
3. **保存**をクリックします。

NACをサポートするようにNetScaler Gatewayポリシーを更新する

VPN仮想サーバーで、高度な（従来の方式ではない）認証およびVPNセッションポリシーを構成する必要があります。

これらの手順は、以下のいずれかの特性を持つNetScaler Gatewayを更新します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Managementと統合されている。
- または、VPN用に設定されており、Citrix Endpoint Management環境の一部ではないが、Citrix Endpoint Managementに到達できる。

コンソールウィンドウから仮想VPNサーバーで、次の操作を行います。コマンドと例のFQDNおよびIPアドレスは架空のものです。

1. VPN仮想サーバーでクラシックポリシーを使用している場合は、すべてのクラシックポリシーを削除してバインドを解除します。確認するには、次のように入力します。

   `show vpn vserver <VPN_VServer>`

   「**Classic**」という単語を含む結果をすべて削除します。例: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   ポリシーを削除するには、次のように入力します。

   `unbind vpn vserver <VPN_VServer> -policy <policy_name>`
2. 次のように入力して、対応する高度なセッションポリシーを作成します。

   `add vpn sessionPolicy <policy_name> <rule> <session action>`

   例: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`
3. 次のように入力して、ポリシーをVPN仮想サーバーにバインドします。

   `bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100`
4. 次のように入力して、認証仮想サーバーを作成します。

   `add authentication vserver <authentication vserver name> <service type> <ip address>`

   例えば: `add authentication vserver authvs SSL 0.0.0.0` この例では、`0.0.0.0` は認証仮想サーバーが公開されていないことを意味します。
5. 次のように入力して、仮想サーバーにSSL証明書をバインドします。

   `bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>`

   例えば: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`
6. VPN仮想サーバーから認証仮想サーバーに認証プロファイルを関連付けます。まず、次のように入力して認証プロファイルを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`add authentication authnProfile <profile name> -authnVsName <authentication vserver name>`

例えば:

`add authentication authnProfile xm_nac_prof -authnVsName authvs`

7. 次のように入力して、認証プロファイルをVPN仮想サーバーに関連付けます。

   `set vpn vserver <vpn vserver name> -authnProfile <authn profile name>`

   例えば:

   `set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof`

8. 次のように入力して、NetScaler Gatewayからデバイスへの接続を確認します。

   `curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"`

   たとえば、このクエリは、環境に登録されている最初のデバイス (`deviceid_1`) のコンプライアンスステータスを取得することで、接続性を検証します。

   `curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"`

   成功した結果は、次の例のようになります。

   ```
   HTTP/1.1 200 OK

   < Server: Apache-Coyote/1.1

   < X-Citrix-Device-State: Non Compliant

   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. 前の手順が成功したら、Citrix Endpoint Management への Web 認証アクションを作成します。まず、iOS VPN プラグインからデバイス ID を抽出するポリシー式を作成します。次のように入力します。

   `add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\', \'&\').VALUE(\"deviceidvalue\")"`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. 次のように入力して、Citrix Endpoint Management にリクエストを送信します。この例では、Citrix Endpoint Management の IP は `10.207.87.82` で、FQDN は `example.em.cloud.com:4443` です。

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort 4443 -fullReqExpr q{"GET /Citrix/Device/v1/Check HTTP/1.1\r\n" + "Host: example.em.cloud.com:4443\r\n" + "X-Citrix-VPN-Device-ID: " + xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\"200\") &&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"
    ```

    Citrix Endpoint Management NAC の成功出力は `HTTP status 200 OK` です。`X-Citrix-Device-State` ヘッダーの値は `Compliant` である必要があります。

11. 次のように入力して、アクションを関連付ける認証ポリシーを作成します。

    ```
    add authentication Policy <policy name> -rule <rule> -action <web authentication action>
    ```

    例: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")" -action xm_nac`

12. 次のように入力して、既存の LDAP ポリシーを高度なポリシーに変換します。

    ```
    add authentication Policy <policy_name> -rule <rule> -action <LDAP action name>
    ```

    例: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. 次のように入力して、LDAP ポリシーを関連付けるポリシーラベルを追加します。

    ```
    add authentication policylabel <policy_label_name>
    ```

    例えば: `add authentication policylabel ldap_pol_label`

14. 次のように入力して、LDAPポリシーをポリシーラベルに関連付けます。

    ```
    bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
    ```

15. 準拠デバイスを接続してNACテストを実行し、LDAP認証が成功したことを確認します。次のように入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END
```

16. 認証仮想サーバーに関連付けるUIを追加します。次のコマンドを入力して、デバイスIDを取得します。

    ```
    add authentication loginSchemaPolicy <schema policy>-rule <rule> -action lschema_single_factor_deviceid
    ```

17. 次のように入力して、認証仮想サーバーをバインドします。

    ```
    bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100 -gotoPriorityExpression END
    ```

18. Citrix Secure Hub接続を有効にするLDAP高度認証ポリシーを作成します。次のように入力します。

    ```
    add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\").NOT" -action 10.200.80.60_LDAP
    ```

    ```
    bind authentication vserver authvs -policy ldap_xm_test_pol -priority 110 -gotoPriorityExpression NEXT
    ```

Windows

Windowsデスクトップおよびタブレット

Citrix Endpoint Managementは、Windows 10およびWindows 11デバイスをMDMに登録します。Citrix Endpoint Managementは、MDMに登録されたWindows 10およびWindows 11デバイスに対して、以下の認証タイプをサポートしています。

- ドメインベースの認証
  - アクティブディレクトリ
  - アジュール アクティブ ディレクトリ
- IDプロバイダー:
  - アジュール アクティブ ディレクトリ
  - Citrix® IDプロバイダー

サポートされている認証タイプの詳細については、証明書と認証を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows 10またはWindows 11デバイス管理を開始するための一般的なワークフローは次のとおりです。

1. オンボーディングプロセスを完了します。オンボーディングとリソースのセットアップおよびデバイスの登録とリソースの配信の準備を参照してください。

   AutoDiscoveryサービスを使用してWindowsデバイスを登録する予定がある場合は、Citrix AutoDiscoveryサービスを構成する必要があります。Citrixテクニカルサポートに支援を依頼してください。詳細については、WindowsデバイスのAutoDiscoveryをリクエストを参照してください。
2. 登録方法を選択して構成します。サポートされている登録方法を参照してください。
3. Windowsデスクトップおよびタブレットデバイスポリシーを構成する。
4. ユーザーはWindows 10およびWindows 11デバイスを登録します。
5. デバイスとアプリのセキュリティアクションを設定します。セキュリティアクションを参照してください。

サポートされているオペレーティングシステムについては、サポートされているデバイスオペレーティングシステムを参照してください。

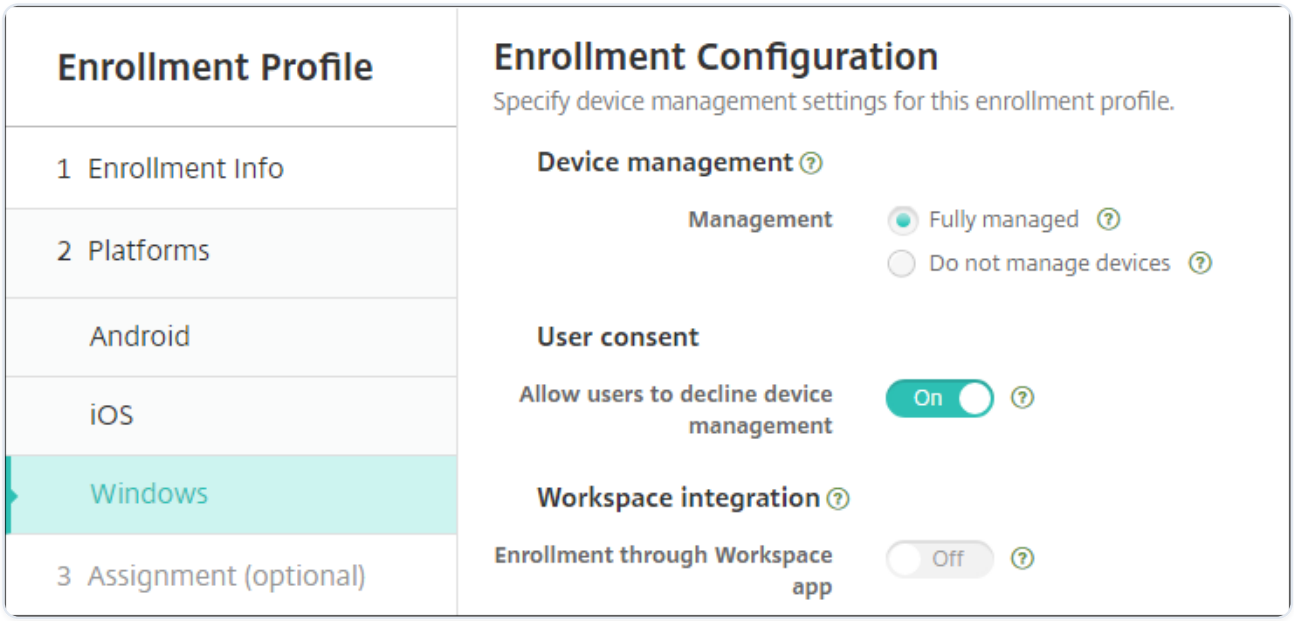
サポートされている登録方法

Windows 10およびWindows 11デバイスの管理方法は、登録プロファイルで指定します。次の2つのオプションがあります。

- フルマネージド (MDM enrollment)
- デバイスを管理しない (no MDM enrollment)

Windows 10およびWindows 11デバイスの登録設定を構成するには、**Configure > Enrollment Profiles > Windows**に移動します。登録プロファイルの詳細は、登録プロファイルを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



次の表に、Citrix Endpoint ManagementがWindows 10およびWindows 11デバイスでサポートする登録方法を示します。

方法	サポート
アジュール アクティブ ディレクトリ 登録	はい
AutoDiscoveryサービス登録	はい
Windowsの一括登録	はい
手動登録	はい
登録招待	いいえ

注：

- 手動登録では、ユーザーがCitrix Endpoint Managementサーバーの完全修飾ドメイン名 (FQDN) を入力する必要があります。手動登録の使用は推奨しません。代わりに、ユーザーの登録プロセスを簡素化するために他の方法を使用してください。
- Windowsデバイスに登録招待を送信することはできません。Windowsユーザーはデバイスから直接登録します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windowsデスクトップおよびタブレットデバイスポリシーの構成

これらのポリシーを使用して、Citrix Endpoint ManagementがWindows 10またはWindows 11を実行しているデスクトップおよびタブレットデバイスとどのように連携するかを構成します。この表には、Windowsデスクトップおよびタブレットデバイスで利用可能なすべてのデバイスポリシーがリストされています。

アプリ構成	アプリインベントリ	アプリロック
アプリのアンインストール	アプリケーションガード	BitLocker
資格情報	カスタムXML	ディフェンダー
デバイスガード	デバイス正常性構成証明	エクスチェンジ
ファイアウォール	キオスク	ネットワーク
オフィス	OSアップデート	パスコード
制限	ストア	利用規約
VPN	Webクリップ	Windowsエージェント
Windows GPO構成	ビジネス向け Windows Hello	

Azure Active Directory を介した Windows 10 および Windows 11 デバイスの登録

重要:

ユーザーが登録する前に、Azure で Azure Active Directory (AD) 設定を構成し、その後 Citrix Endpoint Management を構成する必要があります。詳細については、「Citrix Endpoint Management を Azure AD に接続する」を参照してください。

Windows 10 および Windows 11 デバイスは、AD 認証のフェデレーション手段として Azure に登録できます。この登録には、Azure AD Premium サブスクリプションが必要です。

次のいずれかの方法を使用して、Windows 10 および Windows 11 デバイスを Microsoft Azure AD に参加させることができます。

- 会社所有のデバイスの場合:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - デバイスの電源を初めてオンにしたときに、デバイスを Azure AD に参加させるときに MDM に登録します。このシナリオでは、ユーザーは次の記事で説明されているように登録を完了します: `<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/azuread-joined-devices-frx>`。

    この方法で登録する Windows デバイスの場合、Windows AutoPilot を使用してデバイスをセットアップおよび事前構成できます。詳細については、「Windows AutoPilot を使用してデバイスをセットアップおよび構成する」を参照してください。

  - デバイスの設定後、Windowsの**設定**ページからAzure ADにデバイスを参加させるときにMDMに登録します。このシナリオでは、ユーザーはデバイス設定後にAzure ADに参加するときにMDMに登録するで説明されているように登録を完了します。

- 個人用デバイス（BYODまたはモバイルデバイス）の場合：

  - Microsoftの職場アカウントをWindowsに追加する際にAzure ADに登録するときにMDMに登録します。このシナリオでは、ユーザーはAzure ADに登録するときにMDMに登録するで説明されているように登録を完了します。

デバイス設定後にAzure ADに参加するときにMDMに登録する

1. デバイスで、スタートメニューから**設定 > アカウント > 職場または学校にアクセス**に移動し、**接続**をクリックします。
2. **職場または学校アカウントのセットアップ**ダイアログボックスで、**その他の操作**の下にある**このデバイスをAzure Active Directoryに参加させる**をクリックします。
3. Azure ADの資格情報を入力し、**サインイン**をクリックします。
4. 組織が要求する利用規約に同意します。

   - ユーザーが**拒否**をクリックすると、デバイスはAzure ADに参加せず、Citrix Endpoint Managementにも登録されません。

5. 登録プロセスを続行するには、**参加**をクリックします。
6. 登録プロセスを完了するには、**完了**をクリックします。

Azure ADに登録するときにMDMに登録する

1. デバイスで、スタートメニューから**設定 > アカウント > 職場または学校にアクセス**に移動し、**接続**をクリックします。
2. **職場または学校アカウントのセットアップ**ダイアログボックスで、Azure ADの資格情報を入力し、**サインイン**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 組織が要求する利用規約に同意します。デバイスはAzure ADに登録され、Citrix Endpoint Managementに登録されます。

    - ユーザーが**辞退**をクリックした場合、デバイスはAzure ADに登録されますが、Citrix Endpoint Managementには登録されません。アカウントに**情報**ボタンはありません。

4. **参加**をクリックして、登録プロセスを進めます。
5. **完了**をクリックして、登録プロセスを完了します。

AutoDiscoveryサービスを使用してWindowsデバイスを登録する

WindowsデバイスのAutoDiscoveryサービスを構成するには、Citrixテクニカルサポートに支援を依頼してください。詳細については、「WindowsデバイスのAutoDiscoveryを要求する」を参照してください。

注：

Windowsデバイスを登録するには、SSLリスナー証明書は公開証明書である必要があります。自己署名SSL証明書の場合、登録は失敗します。

ユーザーは、登録を完了するために以下の手順を実行します。

1. デバイスで、スタートメニューから、**設定 > アカウント > 職場または学校にアクセスする**に移動し、**デバイス管理のみに登録**をクリックします。
2. **職場または学校のアカウントを設定する**ダイアログボックスで、会社のメールアドレスを入力し、**次へ**をクリックします。

    ローカルユーザーとして登録するには、正しいドメイン名を持つ存在しないメールアドレス（例：`foo@mydomain.com`）を入力します。この手順により、ユーザーは、Windowsの組み込みデバイス管理が登録を行うという既知のMicrosoftの制限を回避できます。**サービスに接続中**ダイアログボックスで、ローカルユーザーに関連付けられたユーザー名とパスワードを入力します。その後、デバイスはCitrix Endpoint Managementサーバーを見つけて登録プロセスを開始します。

3. 資格情報を入力し、**続行**をクリックします。
4. **利用規約**ダイアログボックスで、デバイスの管理に同意し、**同意**をクリックします。

ドメインポリシーがMDM登録を無効にしている場合、AutoDiscoveryサービスを介したドメイン参加済みWindowsデバイスの登録は失敗します。代わりに、ユーザーは以下のいずれかの方法を使用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- デバイスをドメインから削除し、登録し、その後再参加させます。
- Citrix Endpoint ManagementサーバーのFQDNを入力して続行します。

Windowsの一括登録

Windowsの一括登録を使用すると、デバイスを再イメージ化することなく、MDMサーバーで管理する多くのデバイスをセットアップできます。Windows 10およびWindows 11のデスクトップおよびラップトップデバイスの一括登録には、プロビジョニングパッケージを使用します。詳細については、「Windowsデバイスの一括登録」を参照してください。

セキュリティアクション

Windows 10およびWindows 11デバイスは、次のセキュリティアクションをサポートしています。各セキュリティアクションの説明については、「セキュリティアクション」を参照してください。

検索	ロック	再起動
取り消し	選択的ワイプ	ワイプ

Citrix Endpoint ManagementをAzure ADに接続する

Windows 10およびWindows 11デバイスはAzureに登録できます。Azure ADで作成されたユーザーは、デバイスにアクセスできます。Citrix Endpoint Managementは、MDMサービスとしてMicrosoft Azureに展開されます。Citrix Endpoint ManagementをAzure ADに接続すると、ユーザーはデバイスをAzure ADに登録する際に、Citrix Endpoint Managementに自動的に登録できるようになります。

Citrix Endpoint ManagementをAzure ADに接続するには、次の手順を実行します。

1. Azureポータルで、**Azure Active Directory > モビリティ (MDMおよびMAM) > アプリケーションの追加**に移動し、**オンプレミスMDMアプリケーション**をクリックします。
2. アプリケーションの名前を指定し、**追加**をクリックします。
3. (オプション) Azureでは、cloud.comなどの未検証ドメインをIdP構成に使用できません。Citrix Endpoint Managementの登録FQDNにcloud.comが含まれている場合は、Citrixサポートに連絡し、Azureから取得したTXTレコードを提供してください。Citrixサポートがサブドメインを検証し、構成を続行できるようになります。FQDNが独自のドメイン下にある場合は、Azure内で通常どおり検証できます。
4. 作成したアプリケーションを選択し、以下を構成してから、**保存**をクリックします。
    - **MDMユーザー範囲**。**すべて**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **MDM利用規約URL**。`https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe/tou`の形式で入力します。
- **MDM検出URL**。`https:// <Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe`の形式で入力します。

5. **オンプレミスMDMアプリケーション設定**をクリックします。
   - **プロパティ**ペインで、**APP ID URI**を`https:// < Citrix Endpoint Management Enrollment FQDN>:8443`の形式で設定します。このApp ID URIは、他のどのアプリでも再利用できない一意のIDです。
   - **必要なアクセス許可**ペインで、**Microsoft Graph**と**Windows Azure Active Directory**を選択します。
   - **キー**ペインで、認証キーを作成します。**保存**をクリックしてキーの値を表示します。キーの値は一度しか表示されません。後で使用するためにキーを保存してください。ステップ7でこのキーが必要です。
6. Citrix Endpoint Managementコンソールで、**設定 > IDプロバイダー (IDP)** に移動し、**追加**をクリックします。
7. **検出URL**ページで、以下を構成し、**次へ**をクリックします。
   - **IDP名**。作成するIdP接続を識別するための一意の名前を入力します。
   - **IDPタイプ**。**Azure Active Directory**を選択します。
   - **テナントID**。Azureの**ディレクトリID**です。Azureで**Azure Active Directory > プロパティ**に移動すると表示されます。
8. 「**Windows MDM Info**」ページで、以下を設定し、「**次へ**」をクリックします。
   - **App ID URI**。Azureに入力したAPP ID URIの値。
   - **クライアントID**。Azureの**プロパティ**ペインに表示されるアプリケーションID。
   - **キー**。前の手順4で作成し保存したキーの値。
9. 「**IDP Claims Usage**」ページで、以下を設定し、「次へ」をクリックします。
   - **ユーザー識別子の種類**。「**userPrincipalName**」を選択します。
   - **ユーザー識別子文字列**。`${id_token}.upn`を入力します。
10. 「**保存**」をクリックします。
11. Azure ADユーザーをローカルユーザーとして追加し、ローカルユーザーグループに割り当てます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. 利用規約デバイスポリシーと、そのローカルユーザーグループを含むデリバリーグループを作成します。

Workspace Environment Management™と統合した場合のデバイス管理

Workspace Environment Management (WEM)単独では、MDM展開は不可能です。Citrix Endpoint Management単独では、Windows 10およびWindows 11デバイスの管理に限定されます。両方を統合することで、WEMはMDM機能にアクセスでき、Citrix Endpoint Managementを通じてより広範なWindowsオペレーティングシステムを管理できます。この管理は、Windows GPOの構成という形で行われます。現在、管理者はADMXファイルをCitrix Endpoint Managementにインポートし、Windows 10およびWindows 11のデスクトップとタブレットにプッシュして、特定のアプリケーションを構成しています。Windows GPO構成デバイスポリシーを使用すると、GPOを構成し、WEMサービスに変更をプッシュできます。その後、WEMエージェントがGPOをデバイスとそのアプリに適用します。

MDM管理はWEM統合の要件ではありません。WEMがサポートする任意のデバイスにはGPO構成をプッシュできます。Citrix Endpoint Managementがそのデバイスをネイティブにサポートしていない場合でも可能です。

サポートされているデバイスのリストについては、「オペレーティングシステムの要件」を参照してください。

Windows GPO構成デバイスポリシーを受信するデバイスは、WEMと呼ばれる新しいCitrix Endpoint Managementモードで実行されます。登録済みデバイスの**管理 > デバイス**リストでは、WEM管理デバイスの**モード**列に**WEM**と表示されます。

詳細については、「Windows GPO構成デバイスポリシー」を参照してください。

BitLocker回復キー

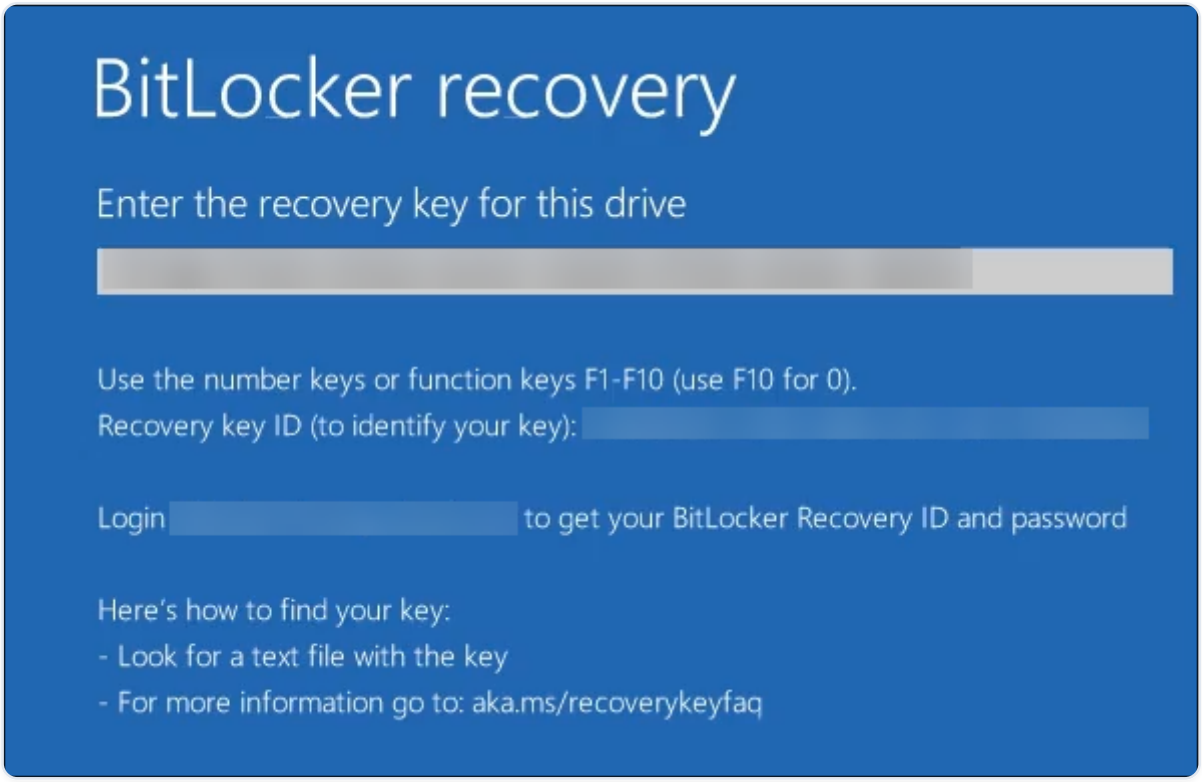
BitLockerを使用してディスクを暗号化することは、便利なセキュリティ機能です。ただし、ユーザーがBitLocker回復キーを紛失した場合、デバイスのロック解除が困難になることがあります。Citrix Endpoint Managementは、ユーザーのBitLocker回復キーを自動的かつ安全に保存できるようになりました。ユーザーは、セルフヘルプポータルでBitLocker回復キーを見つけることができます。BitLocker回復キーを有効にして見つけるには、次の手順を実行します。

1. Citrix Endpoint Managementコンソールで、**［設定］>［サーバープロパティ］**の順に移動します。
2. `shp`を検索し、`shp.console.enable`機能を有効にします。`enable.new.shp`が無効のままであることを確認してください。セルフヘルプポータルの有効化について詳しくは、「登録セキュリティモードの構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **［構成］>［デバイスポリシー］**に移動します。**BitLockerポリシーを見つけるか、新しいポリシーを作成し、**［BitLocker Recovery backup to Citrix Endpoint Management］**設定を有効にします。

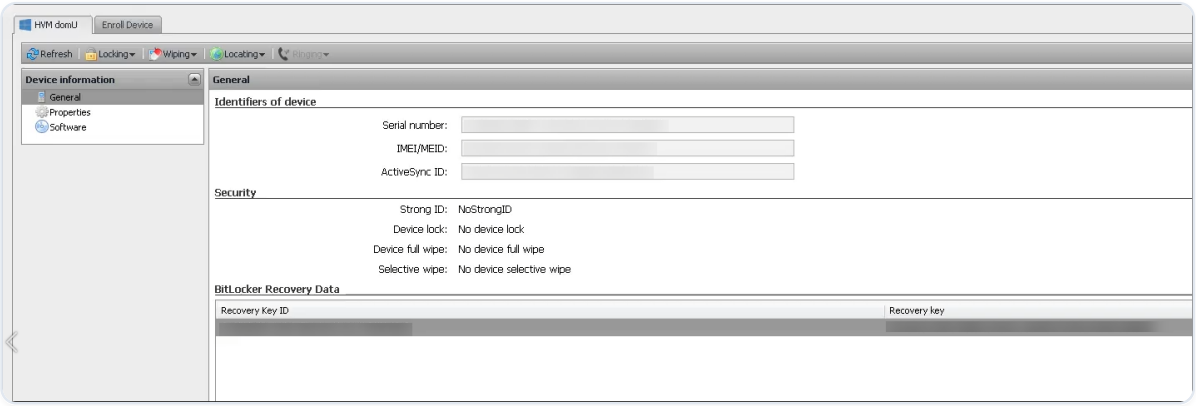
デバイスのロックを解除する際、エンドユーザーにはキーの入力を求めるメッセージが表示されます。このメッセージには、回復キーIDも表示されます。



BitLocker回復キーを見つけるには、ユーザーはセルフヘルプポータルに移動します。

1. **［全般］**の詳細で、**［BitLocker Recovery Data］**を確認します。

   - **回復キーID：** ディスクの暗号化に使用されるBitLocker回復キーの識別子。このIDは、前のメッセージに表示されたキーIDと一致する必要があります。
   - **回復キー：** ユーザーがディスクのロックを解除するために必要なキー。ロック解除プロンプトでこのキーを入力します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

BitLockerデバイスポリシーについて詳しくは、「BitLockerデバイスポリシー」を参照してください。

Windowsデバイスを一括登録する

Citrix Endpoint Managementは、Windows 10およびWindows 11のデスクトップデバイスとタブレットデバイスの一括登録をサポートしています。一括登録を使用すると、デバイスを再イメージングすることなく、Citrix Endpoint Managementで管理する多数のデバイスをセットアップできます。一括登録にはプロビジョニングパッケージを使用します。

Windows 10およびWindows 11デバイスを一括登録するための一般的なワークフローは次のとおりです。

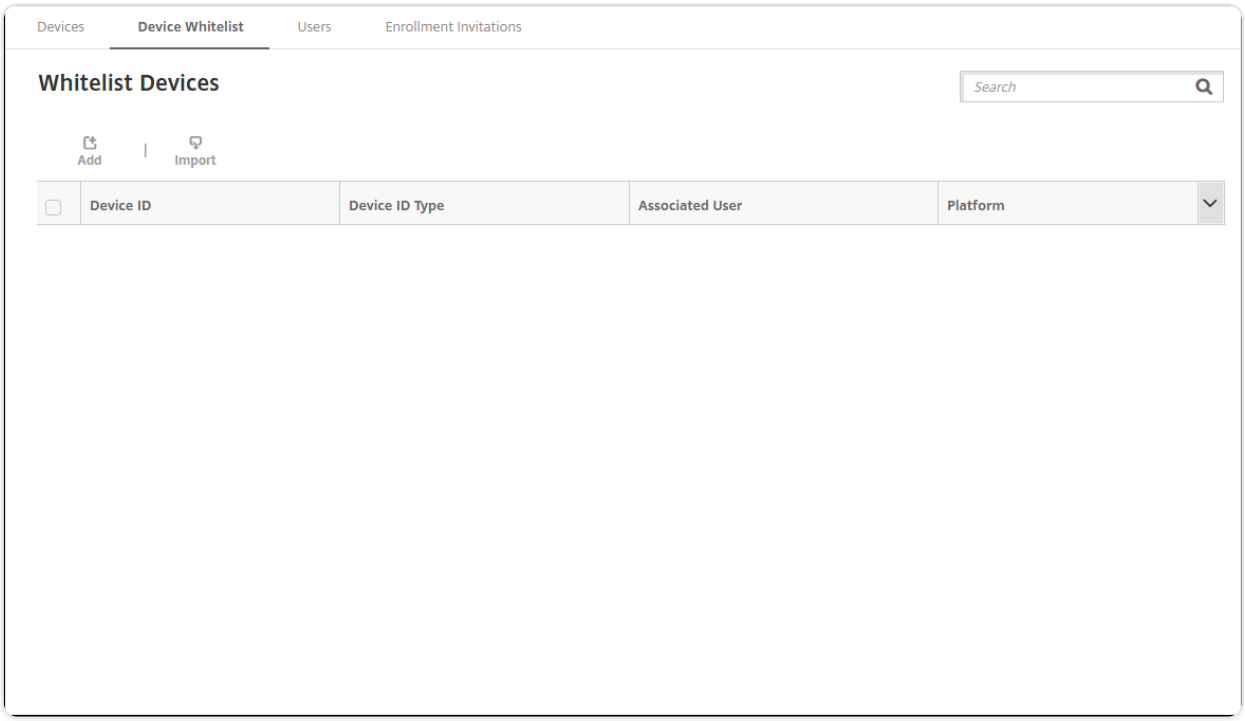
1. デバイスを割り当てます。デバイスは、デバイスごとに割り当てることも、一括で割り当てることもできます。
2. 一括登録を構成します。
3. プロビジョニングパッケージを作成し、そのパッケージをデバイスごとに適用します。

一括登録を実行する前に、すべてのデバイスが正しいユーザーに割り当てられていることを確認してください。この割り当ては、デバイスをデバイスごとに、または一括で追加することによって行います。

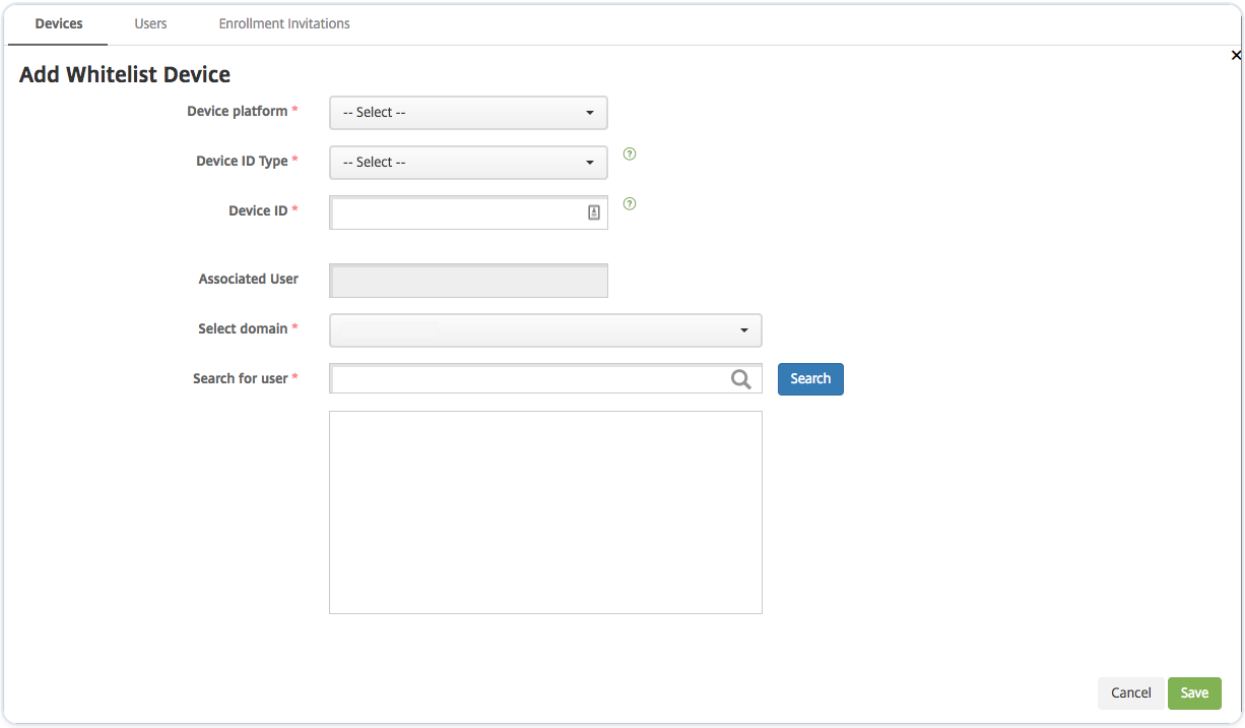
デバイスごとにデバイスを割り当てる

1. Citrix Endpoint Managementコンソールで、**管理** > **デバイス** > **デバイス許可リスト**の順に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 各デバイスを追加するには、**追加**をクリックします。



3. 次の情報を入力します。

- **デバイスプラットフォーム: Windows**を選択します。
- **デバイスIDの種類:** デバイスを識別するIDを選択します。Citrix Endpoint Managementは、Windowsデバイスの**ハードウェアID**と**デバイス名**をサポートしています。
- **デバイスID:** デバイス用に以前選択したタイプに対応するIDを入力します。

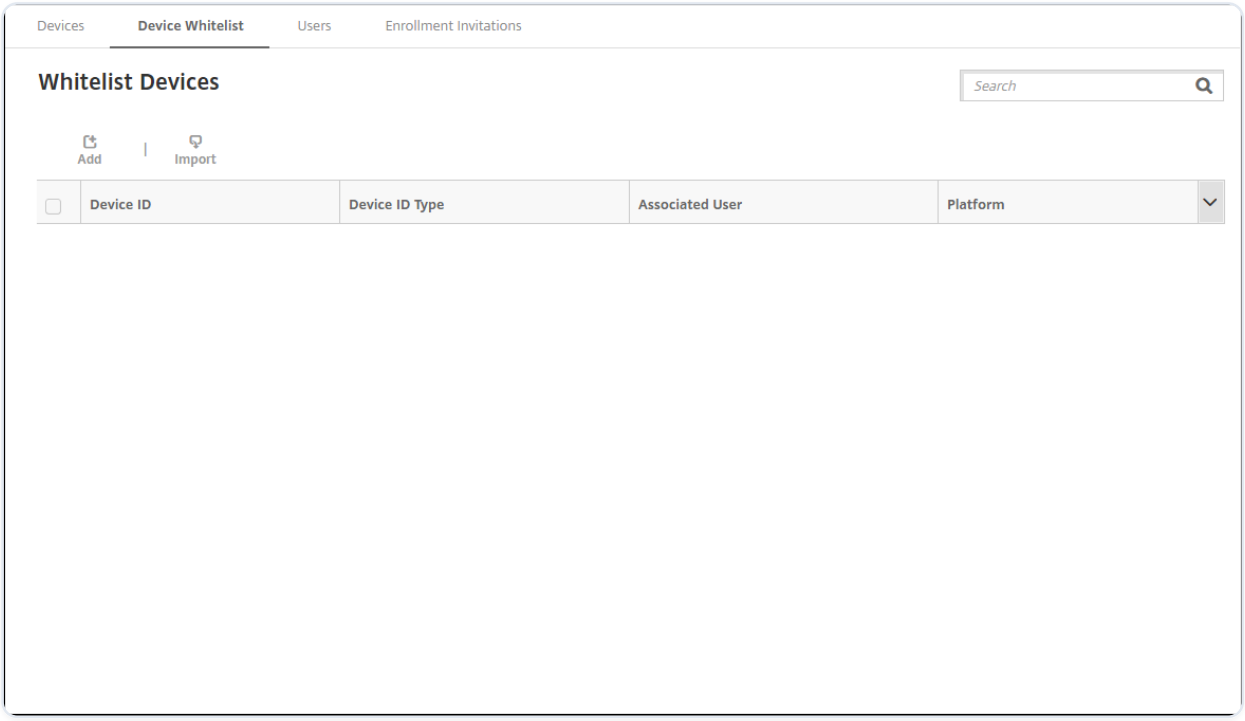
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **関連ユーザー:** このデバイスに関連付けられているユーザーが表示されます。このフィールドには、選択したユーザーが自動的に入力されます。
- **ドメインの選択:** 関連ユーザーを検索したいドメインを選択します。
- **ユーザーの検索** このフィールドにユーザー名の全部または一部を入力し、**検索**をクリックして、このデバイスに関連付けるユーザーを見つけます。

4. **保存**をクリックします。

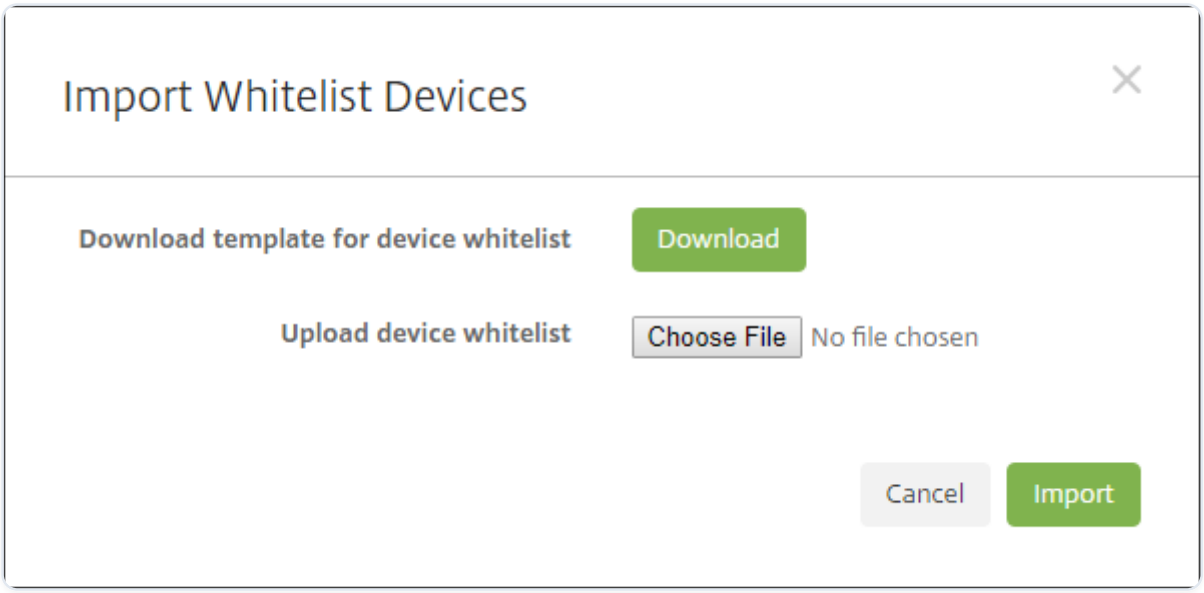
デバイスの一括追加

1. Citrix Endpoint Managementコンソールで、**管理 > デバイス > デバイス許可リスト**に移動します。



2. **インポート**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

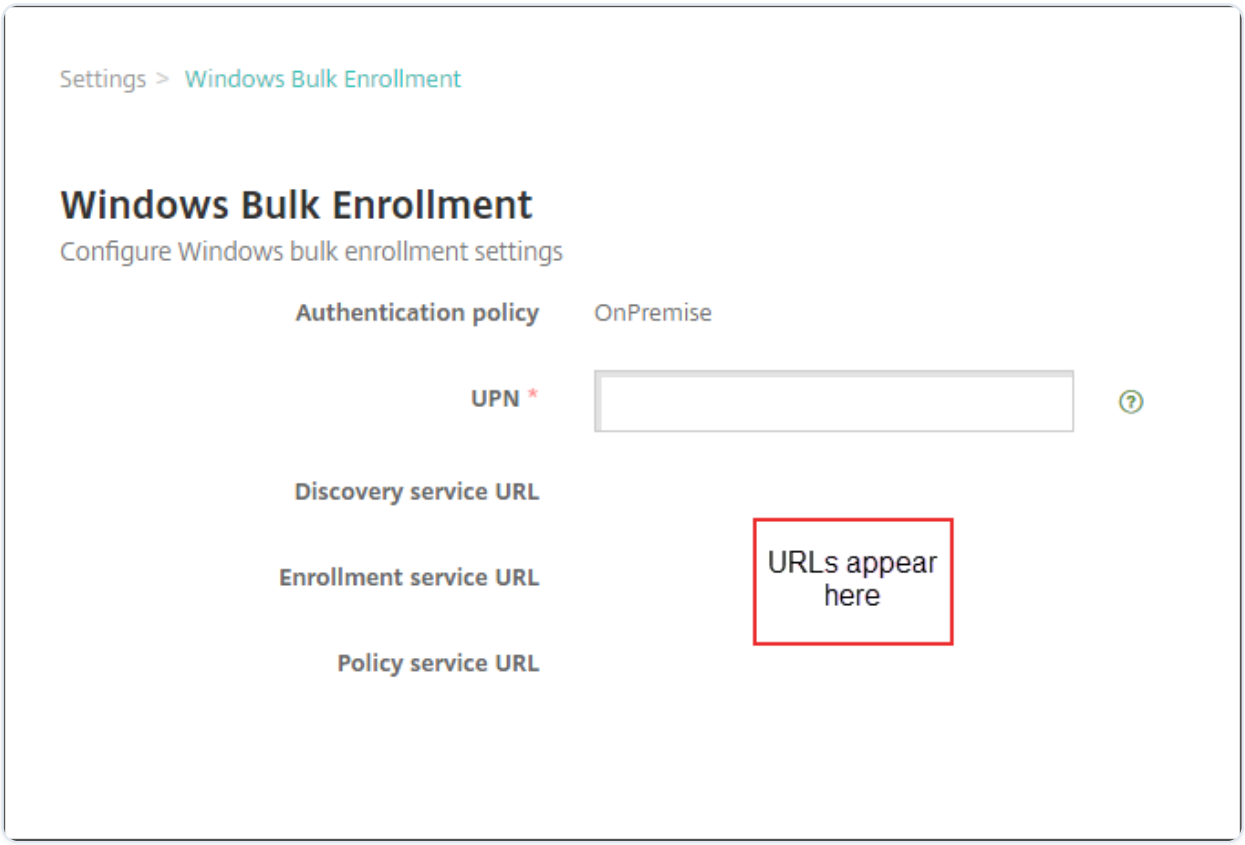


3. **ダウンロード**をクリックして、デバイス許可リストのテンプレート（スプレッドシート）をダウンロードします。そのスプレッドシートに記入し、**ファイルの選択**と**インポート**を使用してスプレッドシートをアップロードします。

一括登録の構成

1. Citrix Endpoint Managementコンソールで、**設定 > Windows一括登録**に移動します。
2. **UPN**フィールドに、すべてのデバイスを展開するためのユーザー名を入力します。UPNは、登録権限を持つCitrix Endpoint Managementの有効なユーザーである必要があります。以前に選択した関連ユーザーとは異なるUPNを指定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Windows Configuration Designerでプロビジョニングパッケージを作成する際に、URLが必要です。

3. **保存**をクリックします。

プロビジョニングパッケージの作成と適用

デバイスを一括プロビジョニングするには、Microsoft StoreからWindows Configuration Designerをダウンロードします。Windows Configuration Designerは、デバイスのイメージングに使用されるプロビジョニングパッケージを作成します。これらのパッケージの一部として、Citrix Endpoint Managementの一括登録構成設定を含めることができ、プロビジョニングされたデバイスがCitrix Endpoint Managementに自動的に登録されるようにします。

プロビジョニングパッケージの使用方法については、`<https://docs.microsoft.com/ja-jp/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-tool>`を参照してください。そのドキュメントの「*オンプレミス認証用のプロビジョニングパッケージを作成して適用する*」セクションに記載されている手順に従ってください。これらの手順に従って、以下のCitrix Endpoint Managementの一括登録構成設定を含め、各デバイスにパッケージを適用します。

- **検出サービスURL**。
- **登録サービスURL**。
- **ポリシーサービスURL**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **シークレット**。UPNのパスワード。以前、UPNフィールドにユーザー名を入力しました。

デバイスをすぐに一括登録する

Citrix Endpoint Managementは、Windowsデバイスのすぐに使える一括登録をサポートしています。一括登録を設定して実行するには、次の手順に従います。

1. Citrix Endpoint Managementコンソールを使用して、デバイスを追加（デバイスごとまたは一括で）し、一括登録を構成します。詳細については、デバイスを一括で追加するおよび一括登録を構成するを参照してください。
2. プロビジョニングパッケージの作成と適用で説明されているように、プロビジョニングパッケージを作成します。

   注：

   プロビジョニングパッケージを作成する際には、各デバイスのデバイス名を構成する必要があります。そのためには、Windows Configuration Designerで、**Runtime settings > Accounts > ComputerAccount > ComputerName**に移動し、デバイス名を指定します。各デバイスに指定するデバイス名は、許可リストデバイスをインポートしたときに使用した名前と一致している必要があります。

3. そのプロビジョニングパッケージをUSBメモリに入れます。
4. ユーザーがデバイスの電源を初めてオンにしたときに、USBメモリをターゲットデバイスに挿入します。

   Windowsデバイスは、USBメモリ上のプロビジョニングパッケージ (.ppkg) を自動的に見つけます。詳細な手順については、Microsoftのドキュメント「初期設定中にプロビジョニングパッケージを適用する方法」を参照してください。

デバイスはCitrix Endpoint Managementに自動的に登録されます。

Windows 10 (バージョン2004以降) またはWindows 11を実行しているデバイスの場合、1つのプロビジョニングパッケージのみを作成することで登録プロセスを簡素化できます。そのパッケージはすべてのデバイスに適用できます。その結果、デバイスごとにプロビジョニングパッケージを作成する必要がなくなります。

登録プロセスを簡素化するには、プロビジョニングパッケージを作成する際に次の手順を実行します。

1. Windows構成デザイナーで、**Runtime settings > Accounts > ComputerAccount > ComputerName**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **ComputerName**フィールドで、デバイス名の一部として次の文字列を含めます: `%SERIAL%`。例: `Surface-%SERIAL%`。この文字列は、各デバイスのBIOSシリアル番号に展開されます。

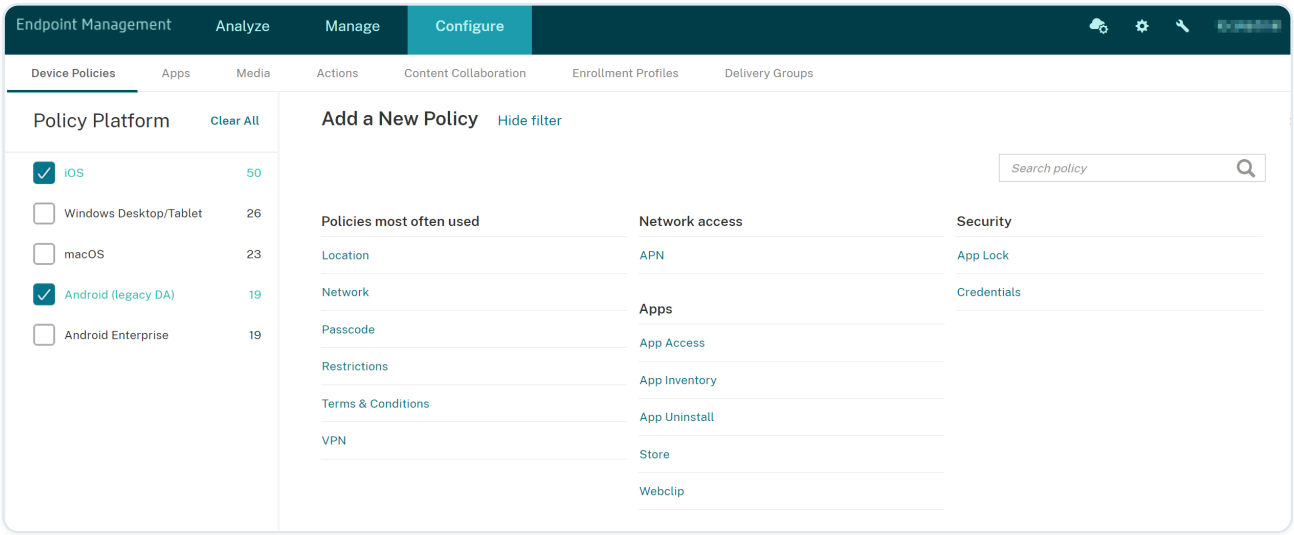
© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー

ポリシーを作成することで、Citrix Endpoint Managementがデバイスとどのように連携するかを設定できます。多くのポリシーはすべてのデバイスに共通していますが、各デバイスにはそのオペレーティングシステムに固有のポリシーセットがあります。そのため、プラットフォーム間、さらにはAndroidデバイスの異なるメーカー間でも違いが見られる場合があります。

プラットフォームごとに利用可能なポリシーを表示するには：

1. Citrix Endpoint Managementコンソールで、**［構成］>［デバイスポリシー］**の順に移動します。
2. **［追加］**をクリックします。
3. 各デバイスプラットフォームは、**［ポリシープラットフォーム］**ペインのリストに表示されます。このペインが開いていない場合は、**［フィルターの表示］**をクリックします。
4. プラットフォームで利用可能なすべてのポリシーのリストを表示するには、そのプラットフォームを選択します。複数のプラットフォームで利用可能なポリシーのリストを表示するには、それらのプラットフォームをそれぞれ選択します。ポリシーは、選択した各プラットフォームに適用される場合にのみリストに表示されます。



各デバイスポリシーの概要については、この記事の「デバイスポリシーの概要」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

環境がグループポリシーオブジェクト（GPO）で構成されている場合：

Windows 10およびWindows 11向けにCitrix Endpoint Managementデバイスポリシーを構成する際は、以下の規則に留意してください。1つ以上の登録済みデバイスでポリシーが競合する場合、GPOに準拠したポリシーが優先されます。
Android Enterpriseコンテナがサポートするポリシーについては、「Android Enterprise」を参照してください。

前提条件

- 使用する予定のデリバリーグループを作成します。
- 必要なCA証明書をインストールします。

デバイスポリシーを追加する

デバイスポリシーを作成する基本的な手順は次のとおりです。

1. ポリシーに名前を付けて説明します。

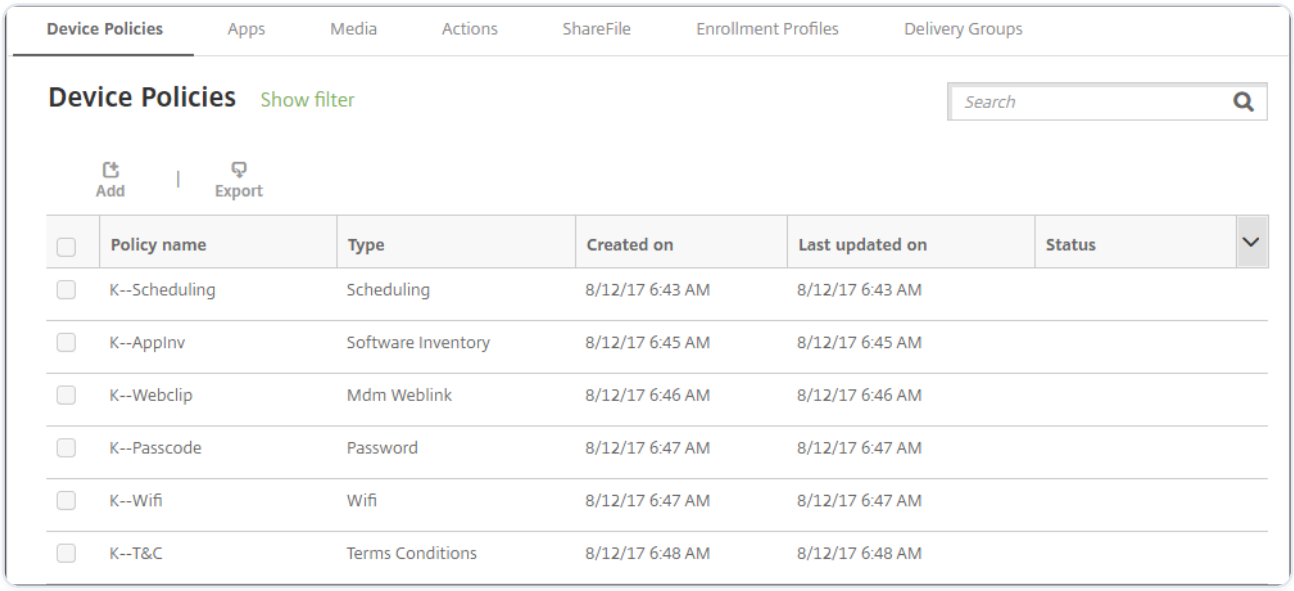
   重要:

   ポリシー名にスラッシュ (/) を使用しないでください。使用すると、後でポリシーを編集するときにエラーが発生する可能性があります。

2. 1つ以上のプラットフォームに対してポリシーを構成します。
3. 展開ルールを作成します (オプション)。
4. デリバリーグループにポリシーを割り当てます。
5. 展開スケジュールを構成します (オプション)。

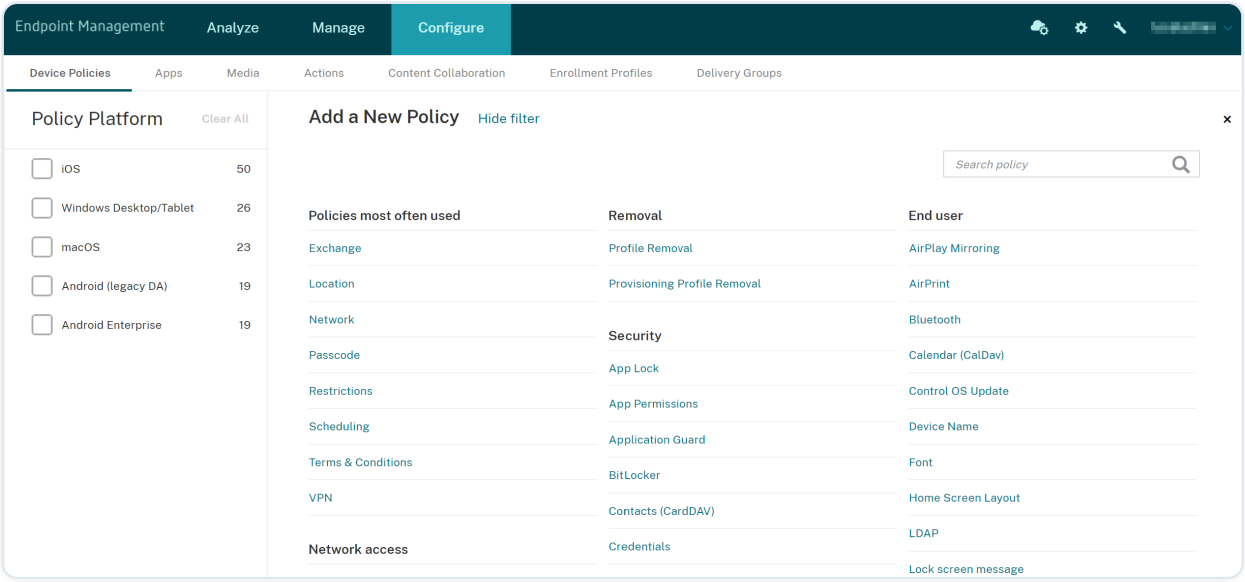
デバイスポリシーを作成および管理するには、 **>** に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



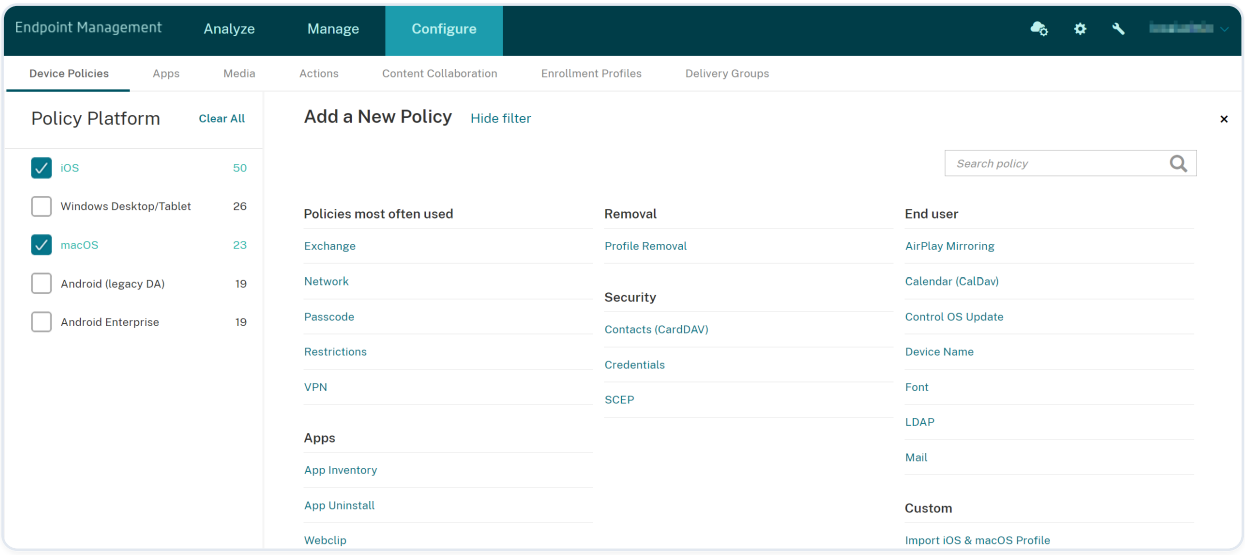
ポリシーを追加するには:

1. ページで、 をクリックします。 ページが表示されます。



2. 1つ以上のプラットフォームをクリックして、選択したプラットフォームのデバイスポリシーのリストを表示します。ポリシーの追加を続行するには、ポリシー名をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



検索ボックスにポリシー名を入力することもできます。入力すると、一致する可能性のある項目が表示されます。ポリシーがリストにある場合は、それをクリックします。選択したポリシーのみが結果に残ります。それをクリックして、そのポリシーの**ポリシー情報**ページを開きます。

3. ポリシーに含めるプラットフォームを選択します。選択したプラットフォームの構成ページは、手順5に表示されます。
4. **ポリシー情報**ページを完了し、**次へ**をクリックします。**ポリシー情報**ページでは、ポリシー名などの情報を収集して、ポリシーを識別および追跡するのに役立ちます。このページは、すべてのポリシーで同様です。
5. プラットフォームページを完了します。手順3で選択した各プラットフォームのプラットフォームページが表示されます。これらのページは、ポリシーごとに異なります。ポリシーはプラットフォームによって異なる場合があります。すべてのポリシーがすべてのプラットフォームに適用されるわけではありません。

   一部のページには、項目のテーブルが含まれています。既存の項目を削除するには、リストがある行にカーソルを合わせ、右側にあるごみ箱アイコンをクリックします。確認ダイアログで、**削除**をクリックします。

   既存の項目を編集するには、リストがある行にカーソルを合わせ、右側にあるペンアイコンをクリックします。

展開ルール、割り当て、およびスケジュールを構成するには

展開ルールの構成について詳しくは、リソースの展開を参照してください。

1. プラットフォームページで、**展開ルール**を展開し、次の設定を構成します。**基本**タブがデフォルトで表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- リストでオプションをクリックして、展開条件を指定します。すべての条件が満たされた場合、またはいずれかの条件が満たされた場合にポリシーを展開することを選択できます。デフォルトのオプションは**すべて**に設定されています。
- **新しいルール**をクリックして条件を定義します。
- リストで、**デバイスの所有権**や**BYOD**などの条件をクリックします。
- さらに条件を追加する場合は、もう一度**新しいルール**をクリックします。必要な数の条件を追加できます。

2. ルールをブールオプションと組み合わせるには、「**Advanced**」タブをクリックします。「**Base**」タブで選択した条件が表示されます。
3. より高度なブール論理を使用して、ルールを結合、編集、または追加できます。

   - 「**AND**」、「**OR**」、または「**NOT**」をクリックします。
   - リストで、ルールに追加する条件を選択します。次に、右側にあるプラス記号（**+**）をクリックして、その条件をルールに追加します。

     いつでも条件をクリックして選択し、その後「**EDIT**」または「**Delete**」をクリックできます。
   - 別の条件を追加するには、「**New Rule**」をクリックします。

4. 次のプラットフォームページに移動するには、「**Next**」をクリックします。すべてのプラットフォームページが完了したら、「**Assignments**」ページに移動します。
5. 「**Assignments**」ページで、ポリシーを適用するデリバリーグループを選択します。デリバリーグループをクリックすると、そのグループが「**Delivery groups to receive app assignment**」ボックスに表示されます。

   「**Delivery groups to receive app assignment**」は、デリバリーグループを選択するまで表示されません。

   デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/device-policies-assignment.png)
6. 「**Assignments**」ページで、「**Deployment Schedule**」を展開し、以下の設定を構成します。

   - 「**Deploy**」の横で、「**On**」をクリックして展開をスケジュールするか、「**Off**」をクリックして展開を防止します。デフォルトのオプションは「**On**」に設定されています。
   - 「**Deployment schedule**」の横で、「**Now**」または「**Later**」をクリックします。デフォルトのオプションは「**Now**」に設定されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

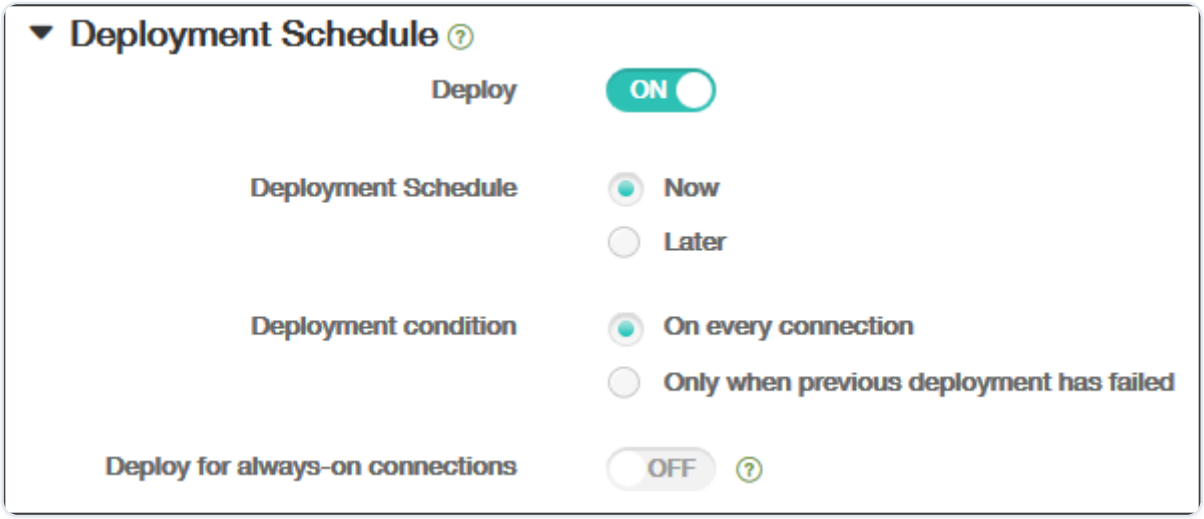
- 「**Later**」をクリックした場合は、カレンダーアイコンをクリックし、展開の日付と時刻を選択します。
- 「**Deployment condition**」の横で、「**On every connection**」または「**Only when previous deployment has failed**」をクリックします。デフォルトのオプションは「**On every connection**」に設定されています。
- 「**常時接続の展開**」の横にある「**オン**」または「**オフ**」をクリックします。デフォルトオプションは「**オフ**」に設定されています。

  注:

  このオプションは、「**設定 > サーバープロパティ**」でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

  常時接続オプション：

  - iOSデバイスでは利用できません
  - バージョン10.18.19以降でCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様は利用できません
  - バージョン10.18.19より前にCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様には推奨されません 構成する展開スケジュールは、すべてのプラットフォームで同じです。「**常時接続の展開**」を除き、行った変更はすべてのプラットフォームに適用されます。



7. 「**保存**」をクリックします。

ポリシーは「**デバイスポリシー**」テーブルに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスからデバイスポリシーを削除する

デバイスからデバイスポリシーを削除する手順は、プラットフォームによって異なります。

- アンドロイド

  Androidデバイスからデバイスポリシーを削除するには、Citrix Endpoint Managementアンインストールデバイスポリシーを使用します。詳細については、「Citrix Endpoint Managementアンインストールデバイスポリシー」を参照してください。

- iOSおよびmacOS

  iOSまたはmacOSデバイスからデバイスポリシーを削除するには、プロファイル削除デバイスポリシーを使用します。iOSおよびmacOSデバイスでは、すべてのポリシーがMDMプロファイルの一部です。そのため、削除したいポリシーのみを対象としたプロファイル削除デバイスポリシーを作成できます。残りのポリシーとプロファイルはデバイスに残ります。詳細については、「プロファイル削除デバイスポリシー」を参照してください。

- Windows 10およびWindows 11

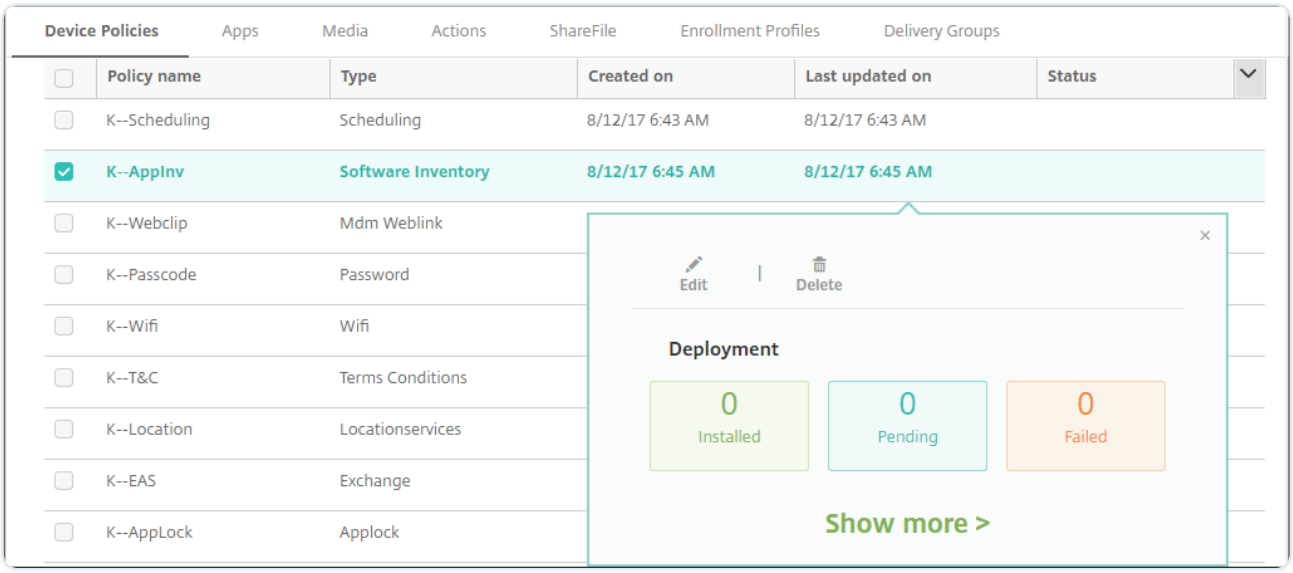
  Windowsデスクトップまたはタブレットデバイスからデバイスポリシーを直接削除することはできません。ただし、次のいずれかの方法を使用できます。

  - デバイスの登録を解除し、新しいポリシーセットをデバイスにプッシュします。ユーザーは続行するために再登録します。
  - 特定のデバイスを選択的にワイプするセキュリティアクションをプッシュします。このアクションにより、すべての企業アプリとデータがデバイスから削除されます。その後、そのデバイスのみを含む配信グループからデバイスポリシーを削除し、その配信グループをデバイスにプッシュします。ユーザーは続行するために再登録します。

デバイスポリシーを編集する

ポリシーを編集するには、ポリシーの横にあるチェックボックスを選択します。オプションメニューがポリシーリストの上に表示されます。または、リスト内のポリシーをクリックして、より多くのコントロールを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



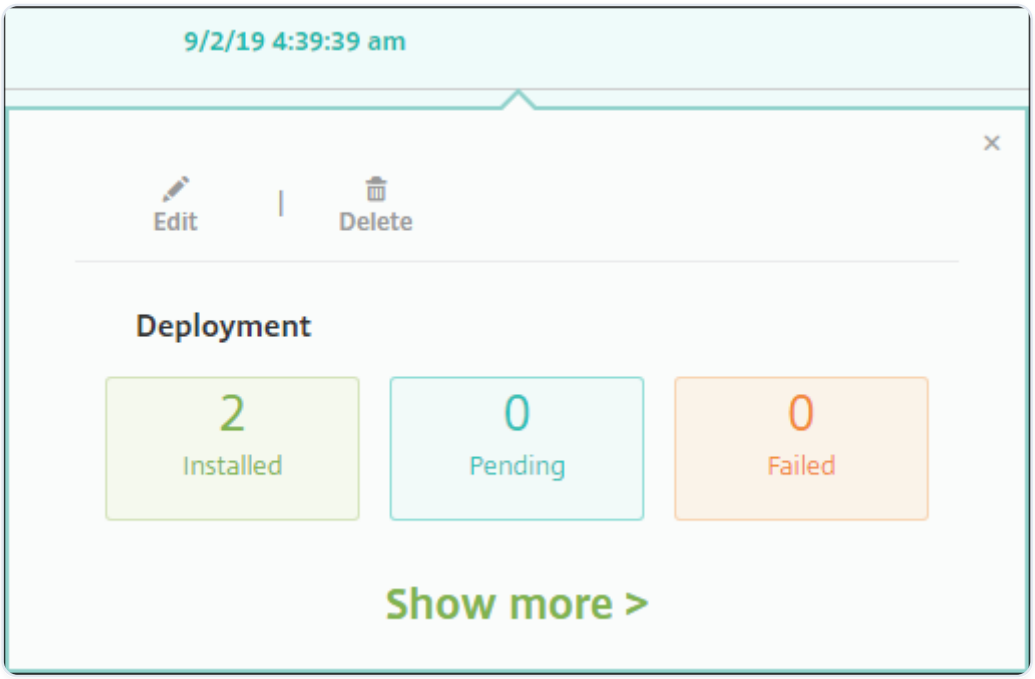
ポリシーの詳細を表示するには、**Show more**をクリックします。

デバイスポリシーのすべての設定を編集するには、**Edit**をクリックします。

Deleteをクリックすると、確認ダイアログボックスが表示されます。ポリシーを削除するには、もう一度**Delete**をクリックします。

ポリシー展開ステータスを確認する

Configure > Device Policiesページでポリシー行をクリックすると、その展開ステータスを確認できます。



ポリシーの展開が保留中の場合、ユーザーは**Preferences > Device Information > Refresh policy**をタップしてCitrix Secure Hubからポリシーを更新できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

追加されたデバイスポリシーのリストをフィルターする

追加されたポリシーのリストを、ポリシーの種類、プラットフォーム、および関連付けられたデリバリーグループでフィルターできます。**Configure > Device Policies**ページで、**Show filter**をクリックします。リストで、表示したい項目のチェックボックスを選択します。

デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/configure-device-policies-filtered.png)

フィルターを保存するには、**SAVE THIS VIEW**をクリックします。フィルターの名前は、**SAVE THIS VIEW**ボタンの下にあるボタンに表示されます。

デバイスポリシーの概要

デバイスポリシー名	デバイスポリシーの説明
AirPlayミラーリング	特定のAirPlayデバイス（Apple TVや別のMacコンピュータなど）をiOSデバイスに追加します。監視対象デバイスの許可リストにデバイスを追加することもできます。このオプションは、ユーザーを許可リスト上のAirPlayデバイスのみに制限します。
AirPrint	AirPrintプリンターをiOSデバイスのAirPrintプリンターリストに追加します。このポリシーにより、プリンターとデバイスが異なるサブネットにある環境をサポートしやすくなります。
APN	特定の電話会社が提供するGPRS（General Packet Radio Service）にデバイスを接続するために使用される設定を決定します。この設定は、ほとんどの新しい電話で既に定義されています。組織がモバイルデバイスからインターネットに接続するために消費者向けAPNを使用しない場合は、このポリシーを使用します。
アプリアクセス	デバイスで必須、オプション、または禁止されているアプリのリストを定義します。その後、そのアプリのリストに対するデバイスのコンプライアンスに対応する自動アクションを作成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー名	デバイスポリシーの説明
アプリの属性	iOSデバイスの管理対象アプリバンドルIDやアプリごとのVPN識別子などの属性を指定します。
アプリの構成	管理対象構成をサポートするアプリのさまざまな設定と動作をリモートで構成します。そのためには、XML構成ファイル（プロパティリスト、または`plist`と呼ばれる）をiOSデバイスに展開します。または、キー/値のペアをWindows 10デスクトップまたはタブレットデバイスに展開します。
アプリのインベントリ	管理対象デバイス上のアプリのインベントリを収集します。Citrix Endpoint Managementは、そのインベントリをそれらのデバイスに展開されているアプリアクセスポリシーと比較します。これにより、アプリアクセスの許可リストまたはブロックリストにあるアプリを検出し、適切に対応できます。
アプリロック	ユーザーがiOSまたは特定のAndroidデバイスで実行できる、または実行できないアプリのリストを定義します。iPadをキオスクに変えることができます。
アプリの権限	ワークプロファイル内のAndroid Enterpriseアプリへの要求が、Googleが「危険」と呼ぶ権限をどのように処理するかを構成します。
アプリのアンインストール	ユーザーデバイスからアプリを削除します。
アプリのアンインストール制限	ユーザーがアンインストールできる、またはできないアプリを指定します。
アプリケーションガード	Microsoft Edgeブラウザのみを対象として、このポリシーはWindows Defender Application Guardの設定を指定します。この設定には、エンタープライズサイトでの外部コンテンツのブロックの有無が含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー名	デバイスポリシーの説明
アプリの通知	iOSユーザーが指定されたアプリから通知を受け取る方法を制御します。
管理対象アプリを自動的に更新	Android Enterpriseデバイスで、インストールされている管理対象アプリが更新される方法を制御します。
BitLocker	Windows 10およびWindows 11デバイスのBitLockerインターフェースで利用可能な設定を構成します。
ブルートゥース	iOSデバイスでBluetoothを有効または無効にします。
ブラウザ	ユーザーデバイスがブラウザを使用できるかどうか、またはデバイスがどのブラウザ機能を使用できるかを定義します。
カレンダー (CalDAV)	iOSまたはmacOSデバイスにカレンダー (CalDAV) アカウントを追加します。CalDAVアカウントにより、ユーザーはCalDAVをサポートする任意のサーバーとスケジュールデータを同期できます。
モバイルデータ通信	携帯ネットワーク設定を構成します。
接続スケジューリング	AndroidデバイスがMDM管理、アプリプッシュ、ポリシー展開のためにCitrix Endpoint Managementに接続し直すために必要です。このポリシーをデバイスに送信せず、Google FCMを有効にしない場合、デバイスはサーバーに接続し直すことができません。
連絡先 (CardDAV)	iOSまたはmacOSデバイスにiOS連絡先 (CardDAV) アカウントを追加します。CardDAVアカウントを使用すると、ユーザーはCardDAVをサポートする任意のサーバーと連絡先データを同期できます。
資格情報	Citrix Endpoint ManagementのPKI構成との統合認証を有効にします。たとえば、PKIエン

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー名	デバイスポリシーの説明
	ティティ、キーストア、資格情報プロバイダー、またはサーバー証明書を使用します。
カスタムXML	デバイスのプロビジョニング、デバイス機能の有効化、デバイスの構成、障害管理などの機能をカスタマイズします。
ディフェンダー	デスクトップおよびタブレット用のWindows 10およびWindows 11のWindows Defender設定を構成します。
デバイスガード	セキュアブート、UEFIロック、仮想化などのセキュリティ機能を有効にします。
デバイス正常性構成証明	Windows 10およびWindows 11デバイスがその正常性の状態を報告することを要求します。そのためには、特定のデータとランタイム情報を分析のためにHealth Attestation Service (HAS) に送信します。HASは、デバイスがCitrix Endpoint Managementに送信するHealth Attestation Certificateを作成して返します。Citrix Endpoint ManagementはHealth Attestation Certificateを受信すると、その証明書の内容に基づいて、構成した自動アクションを展開できます。
デバイス名	iOSおよびmacOSデバイスの名前を設定して、デバイスを識別できるようにします。マクロ、テキスト、またはその両方の組み合わせを使用して、デバイス名を定義できます。
教育構成	Apple Educationで使用するために、教師用デバイスと生徒用デバイスを構成します。教師がClassroomアプリを使用する場合、教育構成デバイスポリシーが必要です。iOS (iPadOS) デバイスでサポートされています。
Citrix Endpoint Managementオプション	AndroidデバイスからCitrix Endpoint Managementに接続する際のCitrix Secure Hubの動作を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー名	デバイスポリシーの説明
Citrix Endpoint Managementのアンインストール	AndroidデバイスからCitrix Endpoint Managementをアンインストールします。展開すると、このポリシーは展開グループ内のすべてのデバイスからCitrix Endpoint Managementを削除します。
エクスチェンジ	デバイス上のネイティブメールクライアントでActiveSyncメールを有効にします。
ファイル	ユーザーのために特定の機能を実行するスクリプトファイルをCitrix Endpoint Managementに追加します。または、Androidデバイスユーザーがデバイスでアクセスできるようにしたいドキュメントファイルを追加することもできます。ファイルを追加する際に、デバイスにファイルを保存するディレクトリも指定できます。
FileVault	このポリシーを使用すると、登録済みのmacOSデバイスでFileVaultデバイス暗号化を有効にできます。また、ユーザーがログイン中にFileVaultのセットアップをスキップできる回数を制御することもできます。macOS 10.7以降で利用可能です。
ファイアウォール	ファイアウォール設定を構成します。デバイスで許可またはブロックするIPアドレス、ポート、ホスト名を提供します。プロキシおよびプロキシの再ルーティング設定も構成できます。
フォント	iOSおよびmacOSデバイスにフォントを追加します。フォントはTrueType (.TTF) またはOpenType (.OFT) フォントである必要があります。Citrix Endpoint Managementはフォントコレクション (.TTC、.OTC) をサポートしていません。
ホーム画面のレイアウト	監視対象のiOSデバイスで、iOSホーム画面のアプリとフォルダーのレイアウトを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー名	デバイスポリシーの説明
iOSおよびmacOSプロファイルのインポート	iOSおよびmacOSデバイスのデバイス構成XMLファイルをCitrix Endpoint Managementにインポートします。このファイルには、Apple Configuratorを使用して準備したデバイスセキュリティポリシーと制限が含まれています。
キーガード管理	ユーザーがデバイスキーガードとワークチャレンジキーガードを解除する前に利用できる機能を制御します。完全に管理された専用デバイスのデバイスキーガード機能も制御できます。たとえば、指紋認証によるロック解除、信頼エージェント、通知などのロック画面機能を無効にできます。
ノックス プラットフォーム フォー エンタープライズ キー	必要なSamsung Knox Platform for Enterprise (KPE) ライセンス情報を提供できます。
ランチャー構成	Androidデバイス上のCitrix Launcherの設定を指定します。たとえば、許可されるアプリや、Launcherアイコンのカスタムロゴ画像などです。
LDAP	iOSデバイスで使用するLDAPサーバーに関する情報を提供します。これには、LDAPサーバーのホスト名などの必要なアカウント情報が含まれます。このポリシーは、LDAPサーバーをクエリする際に使用する一連のLDAP検索ポリシーも提供します。
位置情報	デバイスでCitrix Secure HubのGPSが有効になっている場合、マップ上でデバイスの地理的位置を特定できます。このポリシーをデバイスに展開した後、Citrix Endpoint Managementから位置特定コマンドを送信できます。デバイスは位置座標で応答します。Citrix Endpoint Managementは、ジオフェンシングおよび追跡ポリシーもサポートしています。
ロック画面メッセージ	紛失時に以下のデバイスに表示されるメッセージを設定します。共有iPadのログインウィ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー名	デバイスポリシーの説明
	ンドウと、監視対象iOSデバイスのロック画面。
メール	iOSまたはmacOSデバイスでメールアカウントを構成します。
管理対象構成	Android Enterpriseデバイスのさまざまなアプリ構成オプションとアプリ制限を制御します。
管理対象ドメイン	メールおよびSafariブラウザーに適用される管理対象ドメインを定義します。管理対象ドメインは、Safariを使用してドメインからダウンロードされたドキュメントを開くことができるアプリを制御することで、企業データを保護するのに役立ちます。iOS監視対象デバイスの場合、ユーザーがブラウザーからドキュメント、添付ファイル、ダウンロードを開く方法を制御するために、URLまたはサブドメインを指定できます。
最大常駐ユーザー数	共有iPadの最大ユーザー数を指定します。iOSおよびiPadOSデバイスでサポートされています。
MDMオプション	監視対象iOSデバイスで「iPhoneを探す」とiPadアクティベーションロックを管理します。
ネットワーク	管理者が管理対象デバイスにWi-Fiルーターの詳細を展開できるようにします。ルーターの詳細には、SSID、認証データ、および構成データが含まれます。
ネットワーク使用状況	iOSデバイスで、管理対象アプリが携帯データネットワークなどのネットワークをどのように使用するかを指定するネットワーク使用ルールを設定します。このルールは管理対象アプリにのみ適用されます。管理対象アプリとは、Citrix Endpoint Management を介してユーザーデバイスに展開するアプリのことです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー名	デバイスポリシーの説明
オフィス	Windows 10 (バージョン 1709 以降) または Windows 11 を実行している任意のデバイスに Microsoft Office アプリを展開します。
組織情報	Citrix Endpoint Management が iOS デバイスに展開するアラートメッセージの組織情報を指定します。
OSアップデート	サポートされ、監視されているデバイスに最新のOSアップデートを展開します。
パスコード	管理対象デバイスにPINコードまたはパスワードを強制します。デバイスのパスコードの複雑さとタイムアウトを設定できます。
パスコードロック猶予期間	ユーザーが画面のロックを解除するためにパスコードを入力する必要があるまでに、共有iPadの画面がロックされたままになる分数を示します。iOSおよびiPadOSデバイスでサポートされています。
インターネット共有	ユーザーがWi-Fiネットワークの範囲外にいるときにインターネットに接続できるようにします。ユーザーは、iOSデバイスの携帯データ接続を介して、インターネット共有機能を使用して接続します。
プロファイルの削除	macOSデバイスからアプリプロファイルを削除します。
プロビジョニングプロファイル	デバイスに送信するエンタープライズ配布プロビジョニングプロファイルを指定します。iOSエンタープライズアプリを開発してコード署名する場合、通常はプロビジョニングプロファイルを含めます。Appleは、アプリがiOSデバイスで実行されるためにプロファイルを必要とします。プロビジョニングプロファイルが見つからないか期限切れの場合、ユーザーがアプリを開こうとタップすると、アプリがクラッシュします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー名	デバイスポリシーの説明
プロビジョニングプロファイルの削除	iOSプロビジョニングプロファイルを削除します。
プロキシ	iOSを実行しているデバイスのグローバルHTTPプロキシ設定を指定します。デバイスごとに展開できるグローバルHTTPプロキシポリシーは1つだけです。
制限	管理対象デバイスの機能と機能をロックダウンおよび制御するための何百ものオプションを提供します。制限オプションの例：カメラまたはマイクの無効化、ローミングルールの適用、アプリストアなどのサードパーティサービスへのアクセスの適用。
ローミング	iOSデバイスで音声およびデータローミングを許可するかどうかを設定します。音声ローミングが無効になっている場合、データローミングは自動的に無効になります。
Samsung MDMライセンスキー	デバイスに展開する必要がある組み込みのSamsung Enterprise License Management (ELM) キーを指定します。Citrix Endpoint Managementは、Samsung Enterprise Firmware-Over-The-Air (E-FOTA) サービスもサポートしています。
SCEP	iOSおよびmacOSデバイスが外部SCEPサーバーから証明書を取得するように構成します。Citrix Endpoint Managementに接続されているPKIからSCEPを使用してデバイスに証明書を配信することもできます。そのためには、分散モードでPKIエンティティとPKIプロバイダーを作成します。
シングルサインオン (SSO) アカウント	ユーザーがCitrix Endpoint Managementおよび社内リソースにアクセスするために1回だけサインオンするSSOアカウントを作成します。ユーザーはデバイスに資格情報を保存する必要はありません。Citrix Endpoint Managementは、App Storeのアプリを含む、すべてのアプ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー名	デバイスポリシーの説明
	リでSSOアカウントのエンタープライズユーザー資格情報を使用します。このポリシーはKerberos認証と互換性があります。iOSで利用可能です。
ストレージ暗号化	内部および外部ストレージを暗号化します。一部のデバイスでは、このポリシーにより、ユーザーはデバイスでストレージカードを使用できなくなります。
ストア	アプリストアのWebクリップがユーザーデバイスのホーム画面に表示されるかどうかを指定します。
購読済みカレンダー	iOSデバイスの予定表リストに購読済みカレンダーを追加します。ユーザーデバイスの購読済みカレンダーリストに追加する前に、カレンダーを購読していることを確認してください。
利用規約	企業ネットワークへの接続を管理する会社の特定のポリシーをユーザーが承諾することを要求します。ユーザーがCitrix Endpoint Managementにデバイスを登録する際、デバイスを登録するには利用規約に同意する必要があります。利用規約を拒否すると、登録プロセスはキャンセルされます。
トンネル	あらゆるモバイルデバイスアプリのクライアントコンポーネントとアプリサーバーコンポーネント間のプロキシパラメーターを定義します。
VPN	レガシーVPNゲートウェイテクノロジーを使用するバックエンドシステムへのアクセスを提供します。このポリシーは、デバイスに展開できるVPNゲートウェイ接続の詳細を提供します。Citrix Endpoint Managementは、Cisco AnyConnect、Juniper、Citrix VPNなど、いくつかのVPNプロバイダーをサポートしています。VPNゲートウェイがこのオプションをサポートしている場合、このポリシーをCAにリ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスポリシー名	デバイスポリシーの説明
	ンクして、オンデマンドVPNを有効にすることができます。
壁紙	iOSデバイスのロック画面、ホーム画面、またはその両方に壁紙を設定するために、.pngまたは.jpgファイルを追加します。iPadとiPhoneで異なる壁紙を使用するには、異なる壁紙ポリシーを作成し、適切なユーザーに展開します。
Webクリップ	ユーザーデバイス上のアプリと並んで表示されるように、Webサイトへのショートカット（Webクリップ）を配置します。iOS、macOS、Androidデバイス用のWebクリップを表す独自のアイコンを指定できます。Windowsタブレットでは、ラベルとURLのみが必要です。
Webコンテンツフィルター	iOSデバイス上のWebコンテンツをフィルタリングします。Citrix Endpoint Managementは、Appleの自動フィルター機能と、許可リストおよびブロックリストに追加したサイトを使用します。iOS監視対象デバイスでのみ利用可能です。
Windowsエージェント	このポリシーを有効にすると、アップロードされたPowerShellスクリプトをWindowsデスクトップおよびタブレットで実行できます。
Windows GPO構成	Citrix Workspace Environment Managementでサポートされている任意のWindowsデバイスに対して、グループポリシーオブジェクト (GPO) を構成します。
ビジネス向け Windows Hello	ユーザーがデバイスでWindows Hello for Businessをプロビジョニングできるように、Windows機能を有効にします。このポリシーでは、パスコードの制限やその他のセキュリティ機能も構成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プラットフォーム別のデバイスポリシー

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシー DA)	ウィンドウズ デスクトップ/タブレット	その他
AirPlayミラーリングデバイスポリシー	X	X				
AirPrintデバイスポリシー	X					
APNデバイスポリシー	X			X		
アプリアクセスデバイスポリシー	X			X		
アプリ属性デバイスポリシー	X					
アプリ構成デバイスポリシー	X				X	
アプリインベントリデバイスポリシー	X	X	X	X	X	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシー DA)	ウィンドウズ デスクトップ/タブレット	その他
アプリロックデバイスポリシー	X			X	X	
アプリのアクセス許可デバイスポリシー			X			
アプリのアンインストールデバイスポリシー	X	X	X	X		
アプリのアンインストール制限デバイスポリシー						X
Application Guard デバイスポリシー					X	
アプリの通知デバイスポリシー	X					
管理対象アプリを自動的に更新			X			

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシー DA)	ウィンドウズ デスクトップ/タブレット	その他
BitLocker デバイス ポリシー					X	
Bluetooth デバイス ポリシー	X					
ブラウザ デバイス ポリシー						X
カレンダー (CalDav) デバイス ポリシー	X	X				
セルラー デバイス ポリシー	X					
接続スケジューリングデバイスポリシー			X	X		
連絡先 (CardDAV) デバイス ポリシー	X	X				
Samsung コンテナにアプリをコピーするデバ						X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシー DA)	ウィンドウズ デスクトップ/タブレット	その他
イスポリシー						
資格情報デバイスポリシー	X	X	X	X	X	
カスタム XMLデバイスポリシー			X		X	
Defender デバイスポリシー					X	
Device Guard デバイスポリシー					X	
Device Health Attestation デバイスポリシー					X	
デバイス名デバイスポリシー	X	X				
Education Configuration デバイスポリシー	X					

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシー DA)	ウィンドウズ デスクトップ/タブレット	その他
Citrix Endpoint Management オプションデバイスポリシー			X	X		
Citrix Endpoint Management アンインストールデバイスポリシー				X		
Exchange デバイスポリシー	X	X	X	X	X	
ファイル デバイスポリシー			X	X		
FileVault デバイスポリシー		X				
ファイアウォール デバイスポリシー		X			X	
フォント デバイスポリシー	X	X				

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシー DA)	ウィンドウズ デスクトップ/タブレット	その他
ホーム画面レイアウトデバイスポリシー	X					
デバイス構成のインポートデバイスポリシー						X
iOSおよびmacOSプロファイルのインポートデバイスポリシー	X	X				
キーガード管理デバイスポリシー			X			
キオスクデバイスポリシー			X		X	
ランチャー構成デバイスポリシー			X	X		
LDAPデバイスポリシー	X	X				

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシー DA)	ウィンドウズ デスクトップ/タブレット	その他
位置情報デバイスポリシー	X		X	X		
ロック画面メッセージデバイスポリシー	X					
メールデバイスポリシー	X	X				
管理対象構成デバイスポリシー			X			
管理対象ドメインデバイスポリシー	X					
最大常駐ユーザーデバイスポリシー	X					
MDMオプションデバイスポリシー	X					
ネットワークデバイスポリシー	X		X	X		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシー DA)	ウィンドウズ デスクトップ/タブレット	その他
ネットワーク使用状況デバイスポリシー	X					
Officeデバイスポリシー					X	
組織情報デバイスポリシー	X					
OSアップデートデバイスポリシー	X	X	X		X	
パスコードデバイスポリシー	X	X	X	X	X	
パスコードロック猶予期間デバイスポリシー	X					
パーソナルホットスポットデバイスポリシー	X					
プロファイル削除	X	X				

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシー DA)	ウィンドウズ デスクトップ/タブレット	その他
デバイスポリシー						
プロビジョニングプロファイル デバイスポリシー	X					
プロビジョニングプロファイル削除デバイスポリシー	X					
プロキシ デバイスポリシー	X					
制限デバイスポリシー	X	X		X	X	
ローミング デバイスポリシー	X					
Samsung MDMライセンス キーデバイスポリシー			X			

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシー DA)	ウィンドウズ デスクトップ/タブレット	その他
SCEPデバイスポリシー	X	X				
Siriおよび音声入力ポリシー	X					
SSOアカウントデバイスポリシー	X					
ストレージ暗号化デバイスポリシー						
ストアデバイスポリシー	X			X	X	
購読済みカレンダーデバイスポリシー	X					
利用規約デバイスポリシー	X			X	X	
トンネルデバイスポリシー				X		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー	IOS	MACOS	アンドロイド エンタープライズ	ANDROID (レガシーDA)	ウィンドウズ デスクトップ/タブレット	その他
VPNデバイスポリシー	X	X		X	X	
壁紙デバイスポリシー	X					
Webクリップデバイスポリシー	X	X		X	X	
Webコンテンツフィルターデバイスポリシー	X					
Windowsエージェントデバイスポリシー					X	
Windows GPO構成デバイスポリシー					X	
Windows Hello for Businessデバイスポリシー					X	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AirPlayミラーリングデバイスポリシー

Apple AirPlay機能を使用すると、ユーザーはiOSデバイスからApple TVを介してTV画面にコンテンツをワイヤレスでストリーミングしたり、デバイスのディスプレイに表示されているものをTV画面または別のMacコンピューターに正確にミラーリングしたりできます。

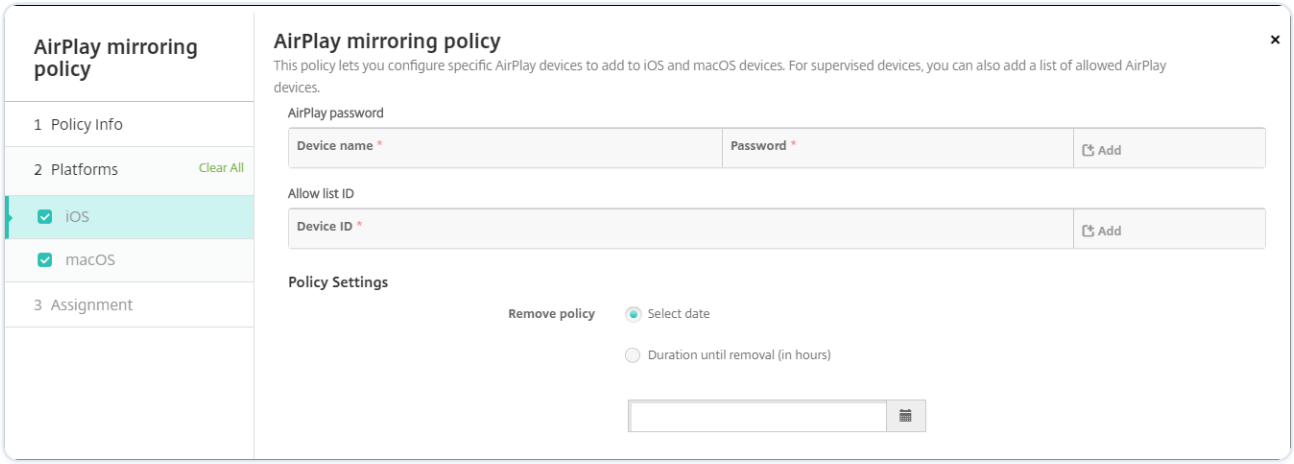
Citrix Endpoint Managementでデバイスポリシーを追加して、特定のAirPlayデバイス（Apple TVや別のMacコンピューターなど）をiOSデバイスに追加できます。また、監視対象デバイスの許可リストにデバイスを追加するオプションもあり、これによりユーザーはそれらのAirPlayデバイスのみに制限されます。デバイスを監視モードにする方法については、「Apple Configurator 2を使用してデバイスを展開する」を参照してください。

注:

続行する前に、追加するすべてのデバイスのデバイスIDとパスワードを準備してください。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

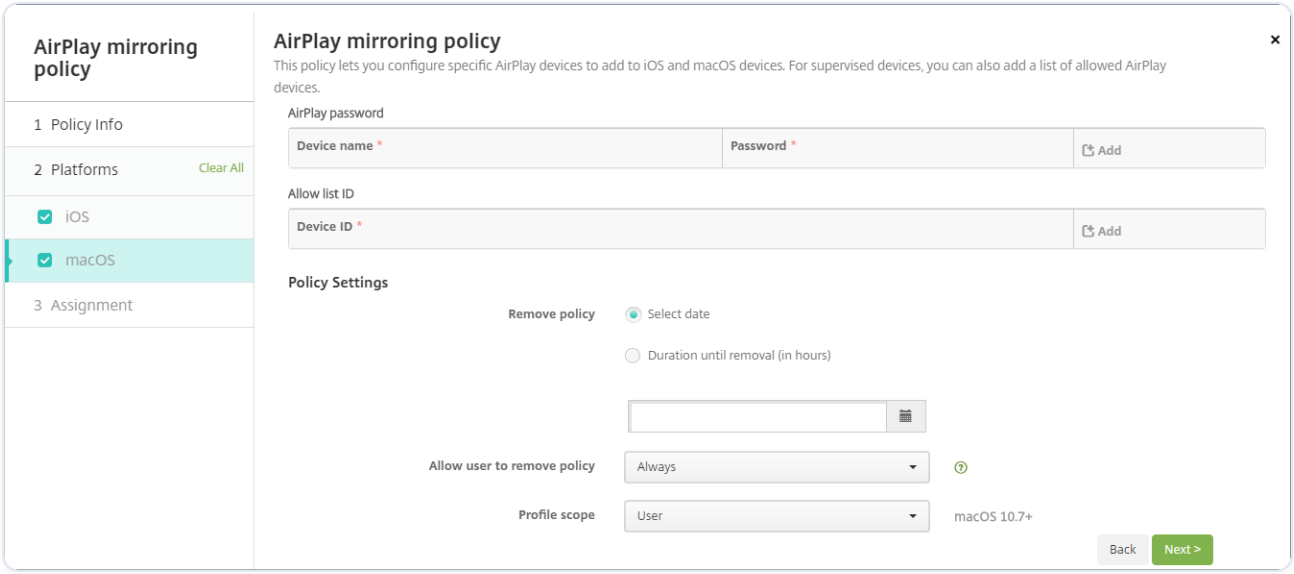


- **AirPlayパスワード:** 追加する各デバイスについて、**追加**をクリックし、次の操作を行います。
  - **デバイス名:** ハードウェアアドレス（MACアドレス）をxx:xx:xx:xx:xx:xx形式で入力します。このフィールドでは大文字と小文字は区別されません。
  - **パスワード:** デバイスのオプションのパスワードを入力します。
  - **追加**をクリックしてデバイスを追加するか、**キャンセル**をクリックしてデバイスの追加をキャンセルします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **許可リストID:** このリストは、監視対象外のデバイスでは無視されます。このリストのデバイスIDは、ユーザーデバイスで利用できる唯一のAirPlayデバイスです。リストに追加する各AirPlayデバイスについて、**追加**をクリックし、次の操作を行います。
    - **デバイスID:** デバイスIDをxx:xx:xx:xx:xx:xx形式で入力します。このフィールドでは大文字と小文字は区別されません。
    - **追加**をクリックしてデバイスを追加するか、**キャンセル**をクリックしてデバイスの追加をキャンセルします。
- **ポリシー設定**
    - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間（時間）**です。
        - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
        - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を数値で入力します。

macOS設定



- **AirPlayパスワード:** 追加するデバイスごとに、**追加**をクリックし、次の操作を行います。
    - **デバイス名:** ハードウェアアドレス（MACアドレス）をxx:xx:xx:xx:xx:xx形式で入力します。このフィールドでは大文字と小文字は区別されません。
    - **パスワード:** デバイスのオプションのパスワードを入力します。
    - デバイスを追加するには**追加**をクリックするか、デバイスの追加をキャンセルするには**キャンセル**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **許可リストID:** このリストは、監視されていないデバイスでは無視されます。このリストのデバイスIDは、ユーザーデバイスで利用可能な唯一のAirPlayデバイスです。リストに追加するAirPlayデバイスごとに、**追加**をクリックし、次の操作を行います。
  - **デバイスID:** デバイスIDをxx:xx:xx:xx:xx:xx形式で入力します。このフィールドでは大文字と小文字は区別されません。
  - デバイスを追加するには**追加**をクリックするか、デバイスの追加をキャンセルするには**キャンセル**をクリックします。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間（時間）**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

AirPrintデバイスポリシー

AirPrintデバイスポリシーは、iOSデバイスのAirPrintプリンターリストにAirPrintプリンターを追加します。このポリシーにより、プリンターとデバイスが異なるサブネットにある環境をサポートしやすくなります。

注:

AirPrintデバイスポリシーを構成するには、各プリンターのIPアドレスとリソースパスが必要です。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、「デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定

- **AirPrint宛先:** 追加するAirPrint宛先ごとに、**追加**をクリックし、次の操作を行います。
  - **IPアドレス:** AirPrintプリンターのIPアドレスを入力します。
  - **リソースパス:** プリンターに関連付けられているリソースパスを入力します。この値は、`_ipps.tcp` Bonjourレコードのパラメーターに対応します。たとえば、`printers/Canon_MG5300_series`または`printers/Xerox_Phaser_7600`です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除をスケジュールする方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間（時間）**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0以降でのみ利用可能です。

アプリの権限デバイスポリシー

ワークプロファイル内にあるAndroid Enterpriseアプリの場合：Googleが「危険な」権限と呼ぶものに対する、それらのアプリからの要求の処理方法を構成できます。アプリからの権限要求をユーザーに許可または拒否するよう促すかどうかを制御します。この機能は、Android 7.0以降を実行しているデバイスに適用されます。

Googleは、危険な権限を次のような権限と定義しています。

- ユーザーの個人情報に関わるデータまたはリソースへのアクセスをアプリに許可する。
- または、ユーザーの保存データや他のアプリの動作に影響を与える可能性がある。たとえば、ユーザーの連絡先を読み取る機能は危険な権限です。

すべての危険な権限要求の動作を制御するために、グローバルステータスを構成できます。この構成の範囲は、ワークプロファイル内にあるAndroid Enterpriseアプリです。また、Googleによって定義されている個々の権限グループに対する危険な権限要求の動作を、アプリごとに制御することもできます。これらの個別の設定は、グローバルステータスを上書きします。

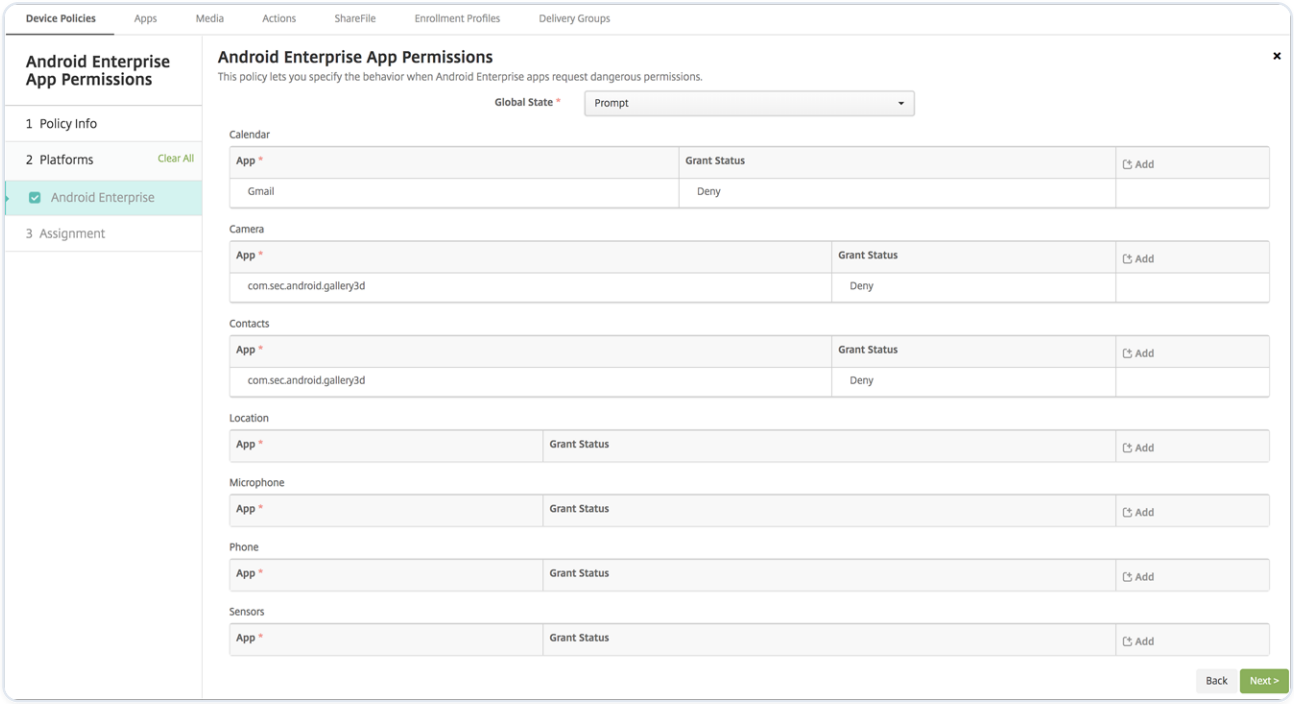
Googleが権限グループをどのように定義しているかについては、Android開発者ガイドを参照してください。

デフォルトでは、ユーザーは危険な権限要求を許可または拒否するよう促されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、デバイスポリシーを参照してください。

Android Enterpriseの設定



- **グローバルステータス：すべての危険な権限要求の動作を制御します。リストで、プロンプト、許可、または拒否**をクリックします。
  - **プロンプト：**ユーザーは危険な権限要求を許可または拒否するよう促されます。
  - **許可：**すべての危険な権限要求が許可されます。ユーザーにはプロンプトが表示されません。
  - **拒否：**すべての危険な権限要求が拒否されます。ユーザーにはプロンプトが表示されません。

  デフォルトは**Prompt**です。
- 各アプリの各権限グループに対して個別の動作を設定します。権限グループの動作を設定するには、**Add**をクリックします。次に、**App**の下で、リストからアプリを選択します。Android Enterpriseシステムアプリを設定する場合は、**Add new**をクリックし、制限デバイスポリシーで有効にしたアプリケーションパッケージ名を入力します。許可ステータスの下で、**Prompt**、**Grant**、または**Deny**を選択します。この許可ステータスはグローバルステータスを上書きします。
  - **Prompt:** ユーザーは、このアプリのこの権限グループからの危険な権限要求を許可または拒否するように求められます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Grant:** このアプリのこの権限グループからの危険な権限要求は許可されます。ユーザーはプロンプト表示されません。

  注:

  Profile Ownerモードで登録されたデバイスの場合、デバイスがAndroid 12以降で実行されている場合、カメラ、位置情報、マイク、センサーに対して**Grant**権限は適用されません。

- **Deny:** このアプリのこの権限グループからの危険な権限要求は拒否されます。ユーザーはプロンプト表示されません。

デフォルトは**Prompt**です。

- アプリと許可ステータスの横にある**Save**をクリックします。
- 権限グループにさらにアプリを追加するには、もう一度**Add**をクリックし、これらの手順を繰り返します。
- 権限グループの**Grant Status**の設定が完了したら、**Next**をクリックします。

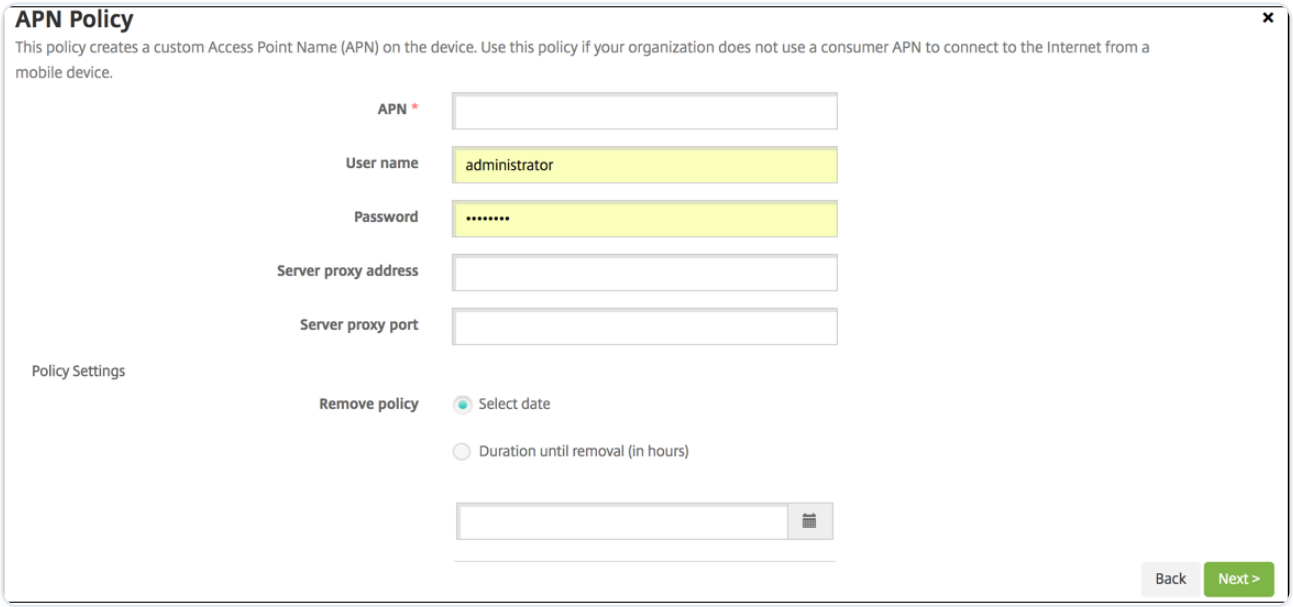
APNデバイスポリシー

iOSおよびAndroidデバイス用のカスタムアクセスポイント名 (APN) デバイスポリシーを追加できます。このポリシーは、組織がモバイルデバイスからインターネットに接続するためにコンシューマーAPNを使用しない場合に使用します。APNポリシーは、デバイスを特定の電話会社のGPRS (General Packet Radio Service) に接続するために使用される設定を決定します。この設定は、ほとんどの新しい電話で既に定義されています。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

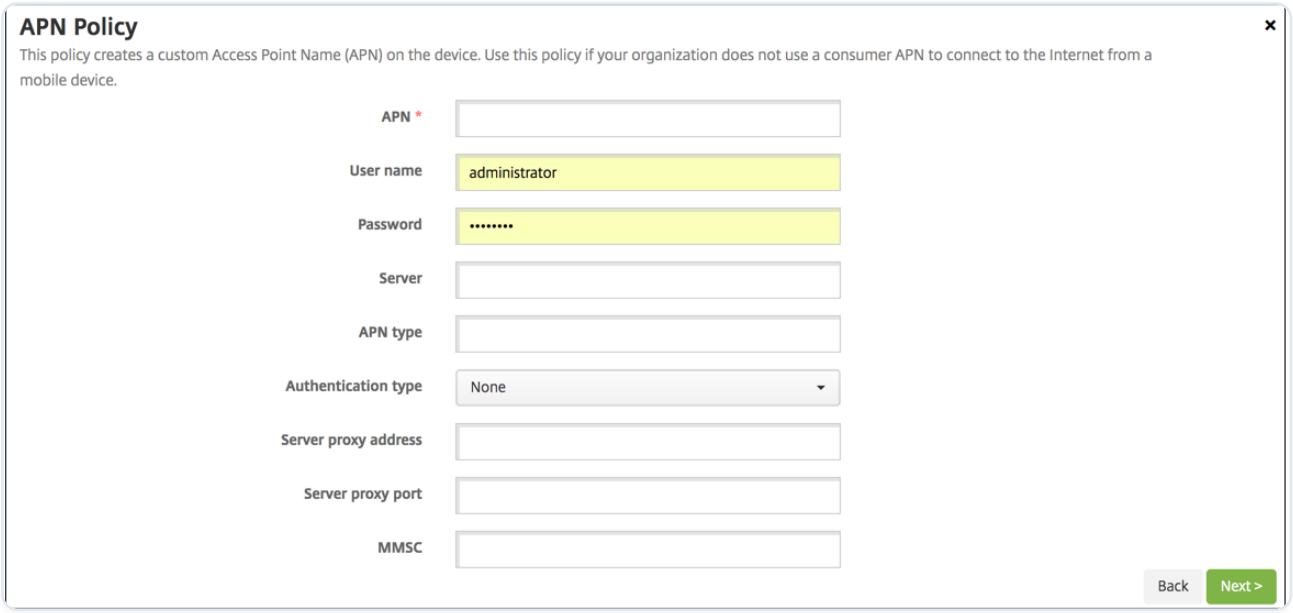
iOS設定



- **APN:** アクセスポイントの名前を入力します。名前は承認されたiOS APNと一致している必要があります。一致しない場合、ポリシーは機能しません。
- **ユーザー名:** この文字列は、このAPNのユーザー名を指定します。ユーザー名が指定されていない場合、プロファイルのインストール中にデバイスが文字列の入力を求めます。
- **パスワード:** このAPNのユーザーのパスワード。難読化のため、パスワードはエンコードされます。ペイロードから欠落している場合、プロファイルのインストール中にデバイスがパスワードの入力を求めます。
- **サーバープロキシアドレス:** APNプロキシのIPアドレスまたはURL。
- **サーバープロキシポート:** APNプロキシのポート番号。サーバープロキシアドレスを入力した場合、ポート番号は必須です。
- で、 の横にある または のいずれかをクリックします。
  - オプションの場合、カレンダーをクリックして、削除する特定の日付を選択します。
  - オプションの場合、パスワードを入力します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、 と です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0以降でのみ利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android設定



- **APN:** アクセスポイントの名前を入力します。名前は承認されたAndroid APNと一致している必要があります。一致しない場合、ポリシーは機能しません。
- **ユーザー名:** この文字列は、このAPNのユーザー名を指定します。ユーザー名が指定されていない場合、プロファイルのインストール中にデバイスが文字列の入力を求めます。
- **パスワード:** このAPNのユーザーのパスワード。難読化のため、パスワードはエンコードされます。ペイロードにパスワードがない場合、プロファイルのインストール中にデバイスがパスワードの入力を求めます。
- **サーバー:** この設定はスマートフォンが登場する以前のもので、通常は空です。標準的なウェブサイトにアクセスしたりレンダリングしたりできない電話機向けのワイヤレスアプリケーションプロトコル (WAP) ゲートウェイサーバーを参照します。
- **APNタイプ:** この設定は、アクセスポイントに対するキャリアの意図する用途と一致している必要があります。これはAPNサービス指定子のコンマ区切り文字列であり、ワイヤレスキャリアが公開している定義と一致している必要があります。例:
  - `*`: すべてのトラフィックがこのアクセスポイントを経由します。
  - `mms`: マルチメディアトラフィックがこのアクセスポイントを経由します。
  - `default`: マルチメディアを含むすべてのトラフィックがこのアクセスポイントを経由します。
  - `supl`: Secure User Plane Locationは、アシストGPSに関連付けられています。
  - `dun`: Dial Up Networkingは古く、ほとんど使用されていません。
  - `hipri.`: 高優先度ネットワーク。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - `fota`: ファームウェアのアップデートを受信するために、ファームウェア無線アップデートが使用されます。

- **認証の種類:** ドロップダウンリストで、使用する認証の種類をクリックします。デフォルトは「なし」です。
- **サーバープロキシアドレス:** キャリアのAPN HTTPプロキシのIPアドレスまたはURL。
- **サーバープロキシポート:** APNプロキシのポート番号。サーバープロキシアドレスを入力した場合は、ポートが必要です。
- **MMSC:** キャリアから提供されるMMSゲートウェイサーバーアドレス。
- **マルチメディアメッセージングサーバー（MMS）プロキシアドレス:** MMSトラフィック用のマルチメディアメッセージングサービスサーバーのアドレス。MMSは、画像や動画などのマルチメディアコンテンツを含むより大きなメッセージを送信するためにSMSの後継として登場しました。これらのサーバーには、特定のプロトコル（MM1、... MM11など）が必要です。
- **MMSポート:** MMSプロキシに使用されるポート。

アプリケーションアクセスデバイスポリシー

アプリケーションアクセスデバイスポリシーを使用すると、インストールが必須、インストール可能、またはインストール禁止のアプリのリストを定義できます。デバイス上のアプリがこのポリシーに違反している場合、Citrix Endpoint Management はそのデバイスを非準拠としてマークします。その後、そのデバイスのコンプライアンスに反応する自動アクションを作成できます。

重要:

アプリケーションアクセスデバイスポリシーは、ユーザーが禁止されているアプリをインストールしたり、必須のアプリをアンインストールしたりするのを防ぐものではありません。

一度に構成できるアクセスポリシーは1種類のみです。各ポリシーには、必須アプリ、推奨アプリ、または禁止アプリのリストが含まれますが、同じアプリケーションアクセスポリシー内でこれらを混在させることはできません。各リストタイプに対してポリシーを作成する場合は、どのポリシーがどのアプリリストに適用されるかをわかるように、各ポリシーに慎重に名前を付けてください。

このポリシーを追加または構成するには、**構成** > **デバイスポリシー** に移動します。詳細については、「デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

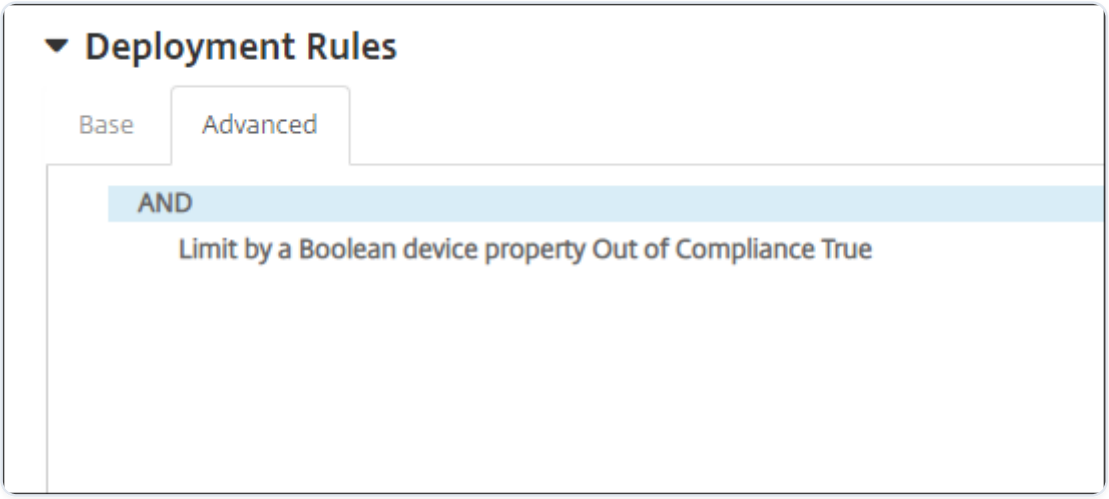
iOSおよびAndroid（レガシーDA）設定

- **アクセスポリシー:** このポリシーで構成するリストのタイプを選択します。
  - **必須:** アプリはデバイス上に存在する必要があります。アプリが存在しない場合、デバイスは非準拠としてマークされます。**必須** がデフォルトのオプションです。
  - **禁止:** アプリはデバイス上に存在してはなりません。アプリが存在する場合、デバイスは非準拠としてマークされます。
- リストに1つ以上のアプリを追加するには：
  a. **追加** をクリックし、以下を構成します。
    - **アプリ名:** アプリ名を入力します。
    - **アプリ識別子:** オプションのアプリ識別子を入力します。
  b. **保存** をクリックします。
  c. 追加したいアプリごとにこれらの手順を繰り返します。

アプリのアクセスコンプライアンスに基づいた自動アクションを構成する

1. アプリを必須または禁止にするためのアプリアクセスポリシーを追加します。
2. 該当するアプリが必須か禁止かに基づいて、2つの自動アクションを構成します。
   - 必須
     - 必須アプリがデバイスに存在しない場合、デバイスを非準拠としてマークします。
     - 必須アプリがインストールされたら、デバイスを準拠としてマークします。
   - 禁止
     - 禁止アプリがデバイスに存在する場合、デバイスを非準拠としてマークします。
     - 禁止アプリがインストールされなくなったら、デバイスを準拠としてマークします。
       自動アクションの設定については、「自動アクション」を参照してください。
3. 非準拠デバイスに適用したい設定で制限ポリシーを作成します。
   a. 制限ポリシーの一部として、**Limit by a Boolean device property**、**Out of Compliance**、**True** のオプションを持つ高度な展開ルールを追加します。「制限デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. デバイスが準拠状態に戻ったら、制限ポリシーを削除するためのプロファイル削除ポリシーを作成します。
5. **Limit by a Boolean device property**、**Out of Compliance**、**False** のオプションを持つ高度な展開ルールを追加します。「プロファイル削除デバイスポリシー」を参照してください。

アプリ属性デバイスポリシー

アプリ属性デバイスポリシーを使用すると、iOSデバイス上のアプリの属性を指定できます。この種類のポリシーを構成することで、次のことが可能になります。

- アプリにアプリごとのVPNを割り当てます。
- ユーザーがミッションクリティカルなアプリをアンインストールするのを防ぎます。iOS 14以降に適用されます。
- 関連ドメイン機能が有効になっている場合、アプリに追加する関連ドメインを指定します。iOS 13以降に適用されます。

  詳細については、「関連ドメインについて」を参照してください。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、「デバイスポリシー」を参照してください。

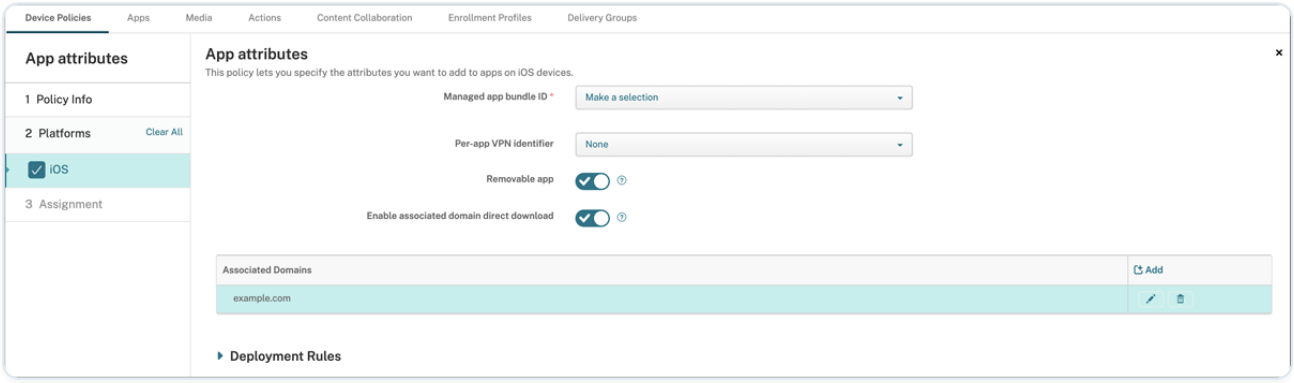
関連ドメインについて

関連ドメインを使用すると、ドメインとアプリの間に安全な関連付けを確立できるため、資格情報を共有したり、Webサイトからアプリの機能を提供したりできます。たとえば、この機能を有効にすると、組織内のアプリとWebサイト間でデータやサインイン資格情報を共有できます。

この機能を有効にする方法の詳細については、AppleのWebサイトの「関連ドメインのサポート」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定



- **管理対象アプリバンドルID:** 次のいずれかの方法でアプリを指定します。
  - アプリバンドルIDを選択します。オプションは、管理対象デバイス上のアプリのインベントリを収集する**アプリインベントリ**デバイスポリシーを有効にした後にのみ利用できます。
  - **新規追加**を選択し、アプリバンドルIDを入力します。 アプリバンドルIDを見つけるには、「App StoreでアプリのバンドルIDを見つける」を参照してください。
- **アプリごとのVPN識別子:** (オプション) このアプリのアプリごとのVPNを選択します。オプションには、**デバイスポリシー > VPNポリシー**ページで構成したアプリごとのVPN接続が含まれます。 詳細については、「アプリごとのVPNを構成する」を参照してください。
- **削除可能なアプリ:** (オプション) このアプリが管理対象アプリである場合に、ユーザーが削除できるかどうかを指定します。ユーザーがこのアプリをアンインストールできないようにするには、このオプションを**オフ**に設定します。デフォルトは**オン**です。
- **関連ドメインの直接ダウンロードを有効にする:** (オプション) デフォルトは**オン**で、このアプリがAppleのサーバーではなくドメインで直接、主張されたサイト関連付けの検証を行うことを示します。このオプションは、インターネットにアクセスできないドメインに対してのみ**オン**に設定してください。
- **関連ドメイン:** (オプション) このアプリに関連ドメインを追加するには、**追加**をクリックし、完全修飾ドメイン名 (FQDN) を入力します。

App StoreでアプリのバンドルIDを見つける

1. App Storeでアプリを見つけ、URLの末尾にある番号をコピーします。たとえば、363501921はCitrix Workspaceアプリのアプリ IDです。
2. `https://itunes.apple.com/lookup?id=`に移動し、そのURLの後に番号を貼り付けます。TXTファイルが自動的にコンピューターにダウンロードされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. TXTファイルで `bundleId` を検索し、アプリのバンドルIDを取得します。例: Citrix Workspaceアプリのバンドルは `com.citrix.ReceiveriPad` です。

アプリ構成デバイスポリシー

管理対象構成をサポートするアプリは、以下を展開することでリモートで構成できます。

- iOSデバイスへのXML構成ファイル（`.plist`、プロパティリストとも呼ばれます）
- Windows 10またはWindows 11を実行している電話、デスクトップ、またはタブレットデバイスのキー/値ペア

この構成は、アプリ内のさまざまな設定と動作を指定します。Citrix Endpoint Managementは、ユーザーがアプリをインストールするときに、構成をデバイスにプッシュします。構成できる実際の設定と動作はアプリによって異なり、この記事の範囲外です。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

注：

各アプリケーションの所有者がアプリ構成変数を定義します。 たとえば、ChromeはChromeのアプリ構成変数を管理および維持します。詳細については、「Chromeアプリ構成変数」を参照してください。

iOS設定

デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/device-policy-appconfig-ios.png)

- **識別子:** ドロップダウンリストで構成するアプリをクリックするか、 をクリックしてリストにアプリを追加します。
    - をクリックした場合は、表示されるフィールドにアプリ識別子を入力します。
- **辞書コンテンツ:** XMLプロパティリスト（`.plist`）の構成情報を入力またはコピー＆ペーストします。
- をクリックします。Citrix Endpoint ManagementがXMLを検証します。エラーがない場合は、コンテンツボックスの下に と表示されます。コンテンツボックスの下に構文エラーが表示された場合は、続行する前にそれらを修正する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

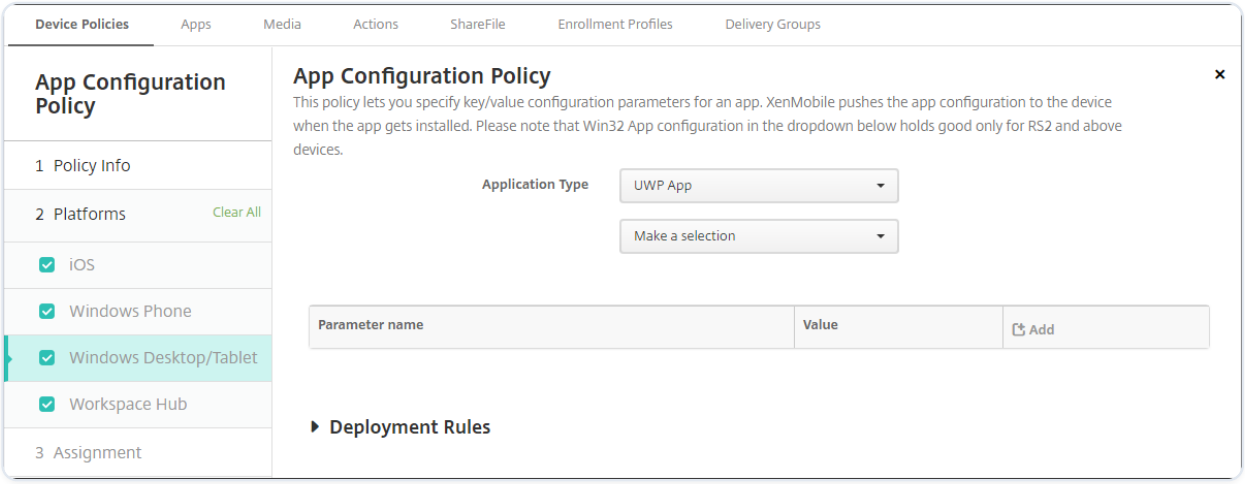
Windowsデスクトップ/タブレット設定

ユニバーサル Windows プラットフォーム (UWP) アプリまたは Win 32 アプリのいずれかを構成できます。Microsoft 管理用テンプレート (ADMX) ポリシー設定をインポートするには、Win 32 アプリを構成します。

注：

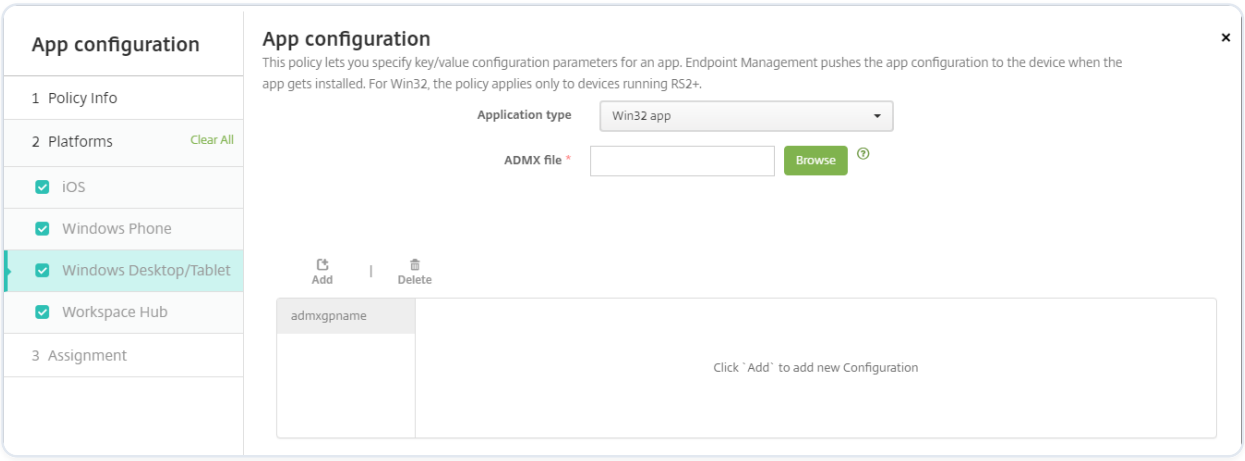
アプリ構成デバイスポリシーは、Office などのサードパーティ製アプリケーション向けのサードパーティ製 ADMX ファイルをサポートしています。`%SystemRoot%\PolicyDefinitions` で利用可能なオペレーティングシステムグループポリシーとして提供される Windows 用の Microsoft ADMX テンプレートはサポートされていません。

- **UWP アプリ**を選択した場合: **選択**リストで、構成するアプリをクリックするか、**新規追加**をクリックしてリストにアプリを追加します。

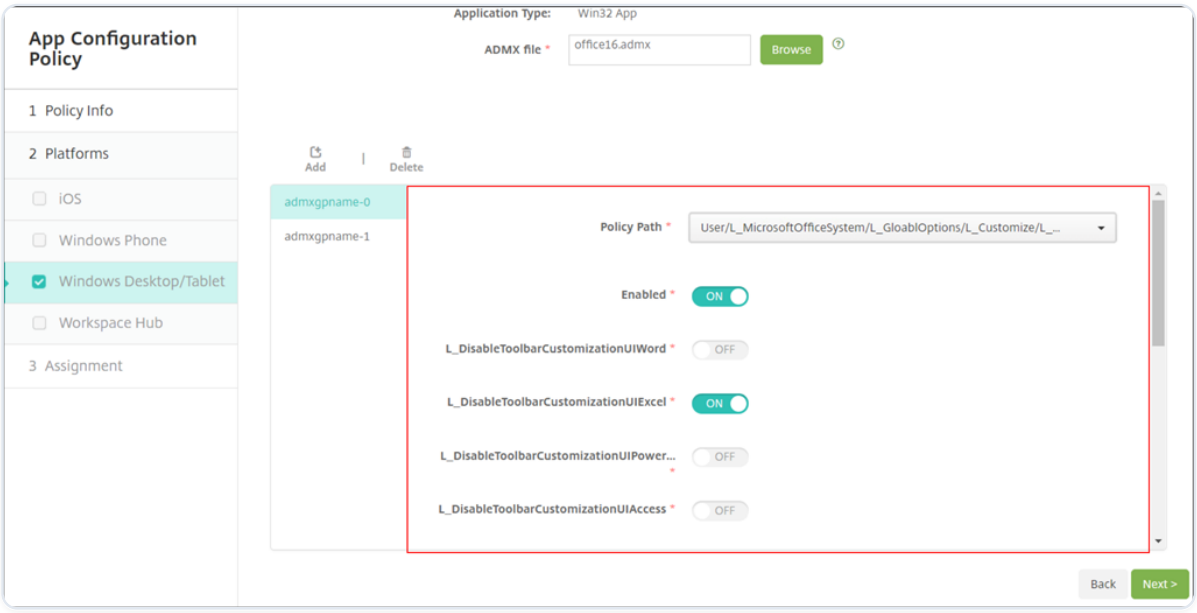


  - **新規追加**をクリックすると、表示されるフィールドにパッケージファミリ名を入力します。
  - 追加する構成パラメータごとに、**追加**をクリックし、次の操作を行います。
    - **パラメータ名:** Windows デバイスのアプリケーション設定のキー名を入力します。Windows アプリ設定の詳細については、Microsoft のドキュメントを参照してください。
    - **値:** 指定されたパラメータの値を入力します。
    - パラメータを追加するには**追加**をクリックするか、パラメータの追加をキャンセルするには**キャンセル**をクリックします。
- **Win32 アプリ**を選択した場合: **参照**をクリックし、ポリシーの構成に使用する ADMX ファイルに移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **追加**をクリックします。ADMX ファイルからの構成オプションがページの右側に表示されます。



- ポリシーパスを選択します。同じパスを複数回選択した場合、最新バージョンに関連付けられた構成が適用されます。
- 「**有効化**」を「**オン**」に設定します。
- 必要なリスト要素の値をキーと値のペアとして入力します。各キーと値のペア、およびペア内の値とキーを区切るには、テキスト文字列「**&#xF000**」を使用します。
- 小数を含む要素の値は、特定の範囲内の値を必要とする場合があります。

アプリインベントリデバイスポリシー

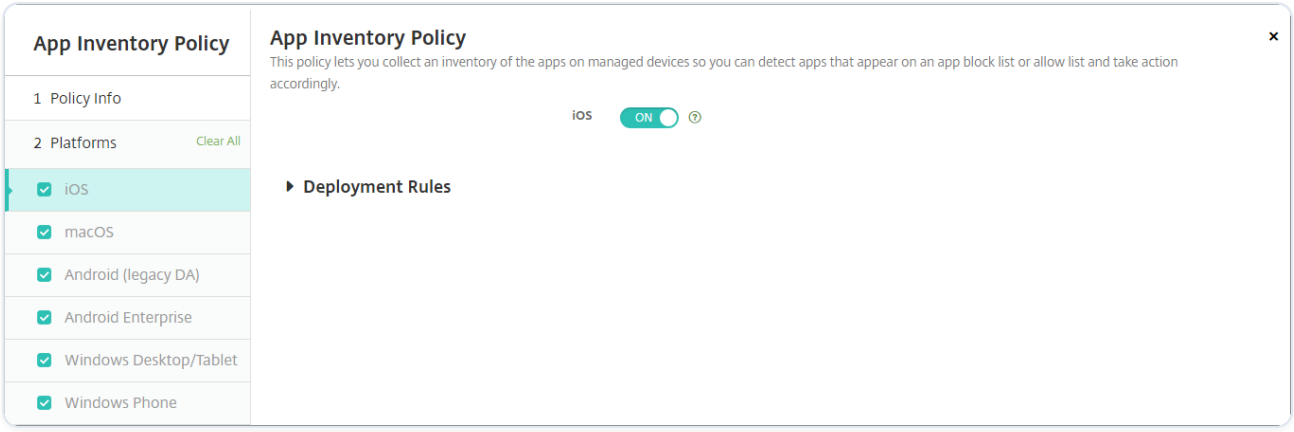
アプリインベントリポリシーを使用すると、管理対象デバイス上のアプリのインベントリを収集できます。Citrix Endpoint Managementは、そのインベントリをそれらのデバイスに展開されているアプリアクセスポリシーと比較できます。これにより、アプリの許可リストまたはブロックリス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

トに表示されるアプリを検出し、適切に対応できます。許可リストまたはブロックリストを定義するには、アプリアクセスポリシーを使用します。

このポリシーを追加または構成するには、**「構成」>「デバイスポリシー」**に移動します。詳しくは、「デバイスポリシー」を参照してください。

iOS、macOS、Android（レガシーDA）、Android Enterprise、およびWindowsデスクトップ/タブレット



- 選択したプラットフォームごとに、デフォルト設定のままにするか、設定を**「オフ」に変更します。デフォルトは「オン」**です。

`Win32`アプリのインベントリと削除

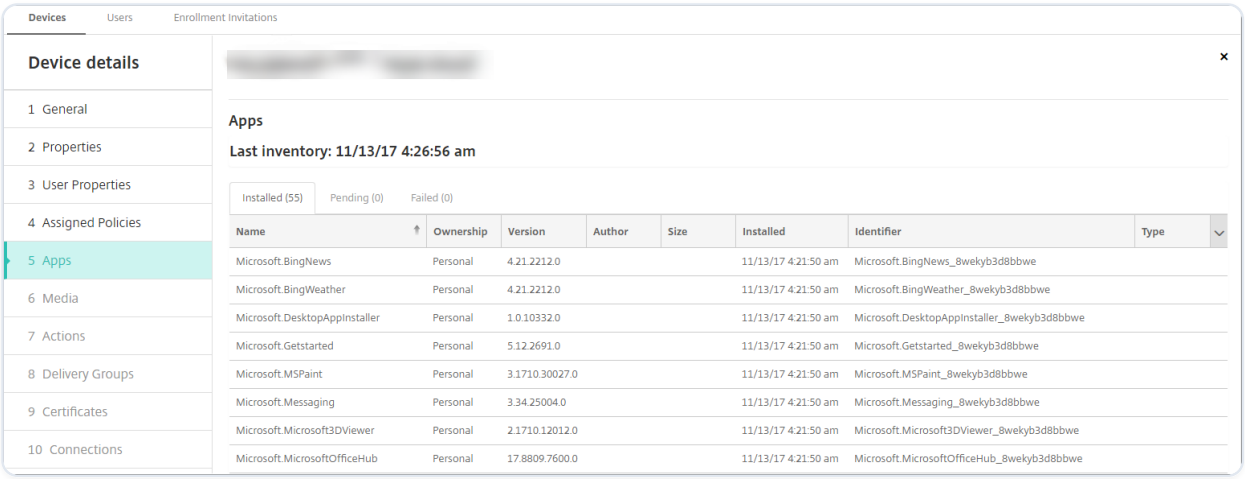
ユーザーデバイス上の`Win32`アプリがアプリアクセスデバイスポリシーに従っているかどうかを判断できます。管理対象のWindows 10およびWindows 11デスクトップおよびタブレットデバイス上の`Win32`アプリのインベントリを表示するには：

1. **「構成」>「デバイスポリシー」**に移動し、**Windowsデスクトップ/タブレット**プラットフォームのアプリインベントリポリシーを追加します。ポリシーを展開します。
2. **「管理」>「デバイス」に移動し、表示するWindows 10およびWindows 11デバイスを選択し、「編集」をクリックしてから、「アプリ」**タブをクリックします。

   インベントリの結果が表示されます。

> **注：**
>
> Windows 11デバイスを構成している場合、Microsoftの設計により、正しいインベントリ結果が得られるまで最大24時間待つ必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. アプリインベントリをアプリアクセスデバイスポリシーと比較します。デバイスにブロックリストにあるアプリがインストールされている場合、それらをデバイスから削除できます。

誤ったプロダクトコードによって引き起こされるアプリのインストールとアンインストールの問題

`Win32`アプリが誤ったプロダクトコードで構成されている場合、アプリは最初にインストールされますが、MicrosoftはアプリのステータスをCitrix Endpoint Managementに返しません。その結果、次のようになります。

- アプリのアンインストールデバイスポリシーでは、アプリがアンインストールされません。
- Citrix Endpoint Managementは、アプリがインストールされたという確認がないため、アプリの展開を継続します。展開のたびに、アプリはすでにインストールされているため、デバイスはエラーコードを生成します。**管理 > デバイス > 配信グループの詳細**に表示されるエラーは次のとおりです: `Msi Application received: Reporting:AppPush id:7z1701-x64.msi: Command execution failed -2147023293`

プロダクトコードを修正するには：

1. デバイスからアプリを手動で削除します。
2. Citrix Endpoint Managementコンソールで、**構成 > アプリ**に移動し、`Win32`アプリのプロダクトコードを修正します。
3. `Win32`アプリを展開します。

Application Guard デバイスポリシー

Application Guard ポリシーは、Windows Defender Application Guard の設定を指定します。設定には、Application Guard を有効にするかどうか、およびクリップボードの動作を制御するものが含まれます。

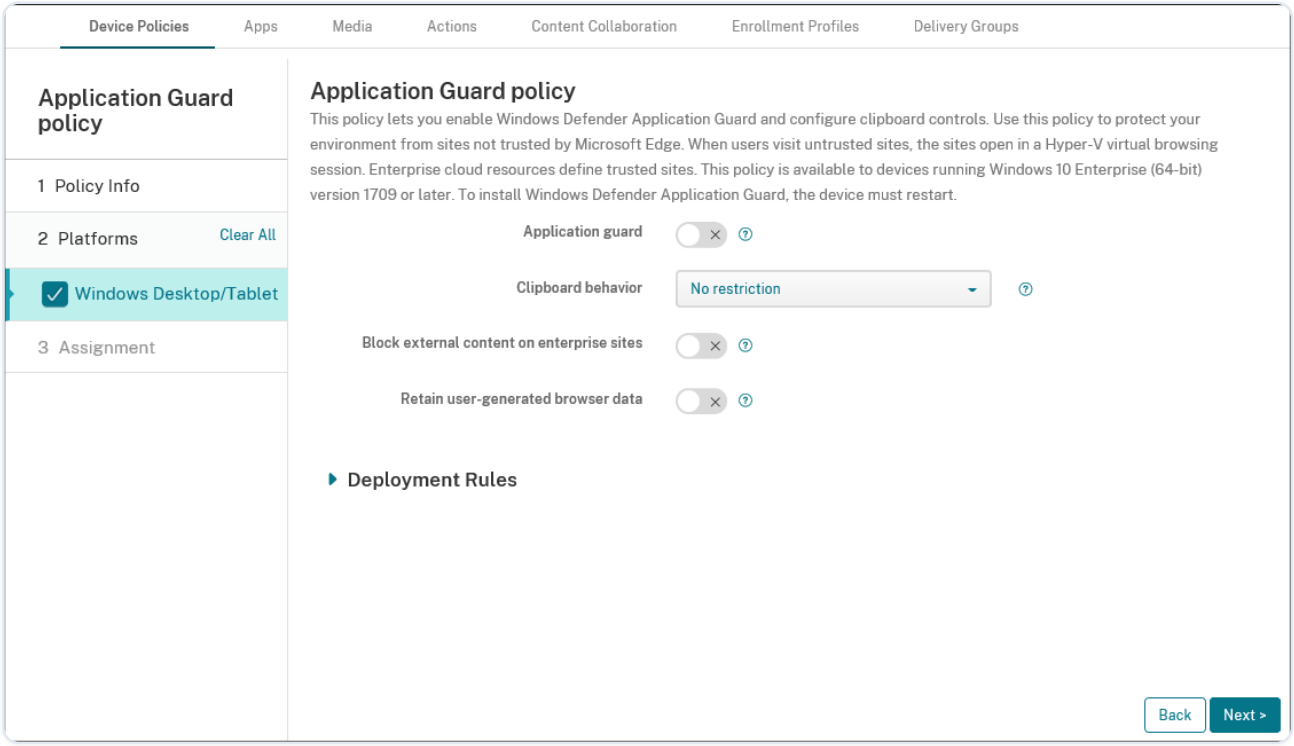
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows Defender Application Guard は、組織によって信頼済みとして定義されていないサイトから環境を保護します。ユーザーが分離されたネットワーク境界にリストされていないサイトにアクセスすると、そのサイトは Hyper-V の仮想ブラウジングセッションで開かれます。エンタープライズクラウドのリソースが信頼済みサイトを定義します。

要件

- Windows 10 Enterprise (64ビット) または Windows 11 Enterprise (64ビット) を実行しているデバイス。Windows Defender Application Guard をインストールするには、デバイスの再起動が必要です。
- Microsoft Edge ブラウザ

Windows デスクトップおよびタブレットの設定



- **Application Guard:** Application Guard を有効にします。デフォルトは**オフ**です。
  - **エンタープライズクラウドのリソース:** エンタープライズクラウドドメインのコンマ区切りリスト。
- **クリップボードの動作:** コンテンツをコピーおよび貼り付けできる方向を制御します。オプションは次のとおりです。
  - **未構成**
  - **ブラウザからPCへのコピーと貼り付けのみを許可:** ユーザーがブラウザからPCにのみコンテンツをコピーして貼り付けることを許可します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **PCからブラウザへのコピーと貼り付けのみを許可:** ユーザーがPCからブラウザにのみコンテンツをコピーして貼り付けることを許可します。
  - **PCとブラウザ間のコピーと貼り付けを許可:** ユーザーがPCとブラウザ間で自由にコンテンツをコピーして貼り付けることを許可します。
  - **PCとブラウザ間のコピーと貼り付けをブロック:** ユーザーがPCとブラウザ間でコンテンツをコピー＆ペーストすることを許可しません。

- **クリップボードのコンテンツ:** ユーザーがコピー＆ペーストできるコンテンツを制御します。オプションは次のとおりです。
  - **制限なし**
  - **テキストのコピーを許可:** ユーザーがテキストのみをコピーできるようにします。
  - **画像のコピーを許可:** ユーザーが画像のみをコピーできるようにします。
  - **テキストと画像の両方のコピーを許可:** ユーザーがテキストと画像の両方をコピーできるようにします。
- **エンタープライズサイトでの外部コンテンツをブロック: オン**の場合、Windows Defender Application Guardは、承認されていないサイトからのコンテンツがエンタープライズサイトにロードされるのを防ぎます。デフォルトは**オフ**です。
- **ユーザー生成のブラウザデータを保持: オン**の場合、Application Guardの仮想ブラウジングセッション中に作成されたユーザーデータを保存できます。このデータには、パスワード、お気に入り、Cookieなどが含まれます。デフォルトは**オフ**です。

アプリロックデバイスポリシー

アプリロックデバイスポリシーは、以下のいずれかのアプリのリストを定義します。

- デバイスでの実行が許可されている。
- デバイスでの実行がブロックされている。

ポリシーの正確な動作は、サポートされているプラットフォームごとに異なります。たとえば、iOSデバイスで複数のアプリをブロックすることはできません。

同様に、iOSデバイスの場合、ポリシーごとに1つのiOSアプリしか選択できません。ユーザーは、デバイスを使用して単一のアプリを実行することしかできません。アプリロックデバイスポリシーが適用されている場合、明示的に許可したオプションを除き、デバイスで他のアクティビティを行うことはできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

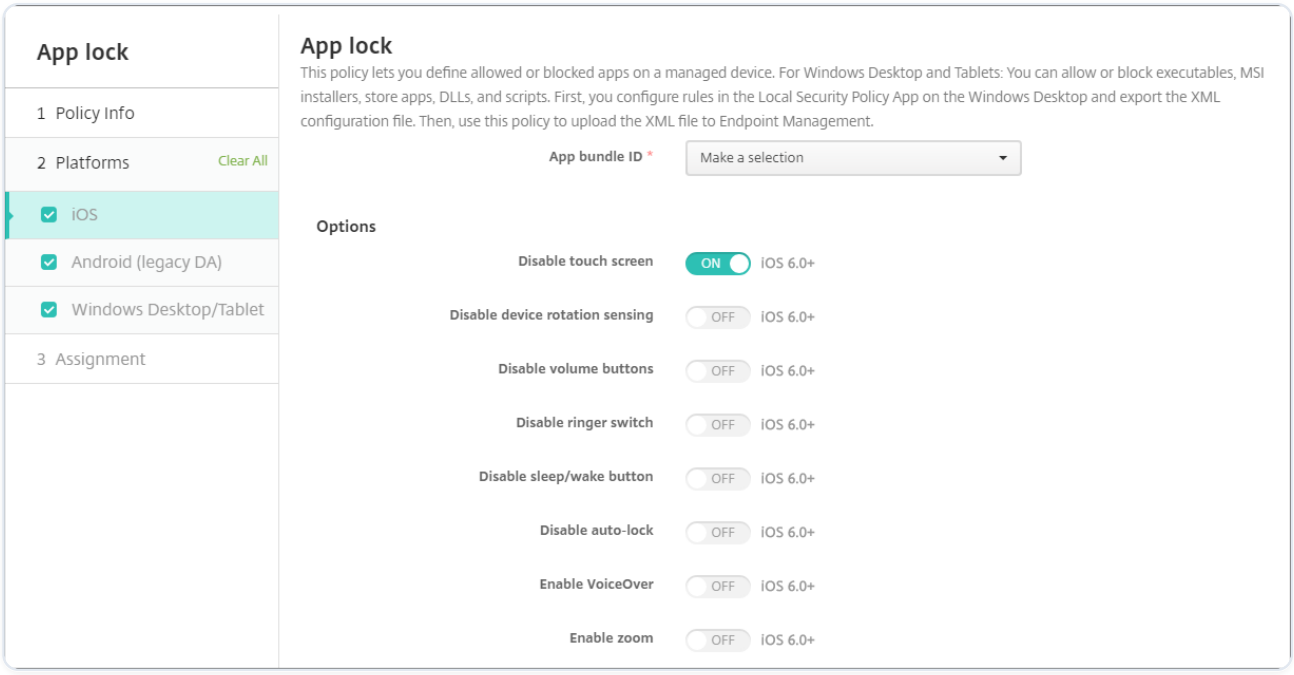
また、アプリロックポリシーをプッシュするには、iOSデバイスが監視されている必要があります。

デバイスポリシーはほとんどのAndroid LおよびMデバイスで機能しますが、アプリロックはAndroid N以降のデバイスでは機能しません。これは、Googleが必要なAPIを非推奨にしたためです。

管理対象のWindowsデスクトップおよびタブレットの場合、許可リストとブロックリスト上のアプリのリストを定義するアプリロックデバイスポリシーを作成できます。実行可能ファイル、MSIインストーラー、ストアアプリ、DLL、およびスクリプトを許可またはブロックできます。

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］**の順に選択します。詳細については、「デバイスポリシー」を参照してください。

iOS設定



- **アプリバンドルID：**このポリシーを適用するアプリをドロップダウンリストからクリックするか、［新規追加］をクリックしてリストにアプリを追加します。**［新規追加］**を選択した場合は、表示されるフィールドにアプリ名を入力します。
- **オプション：**各オプションのデフォルトは［オフ］ですが、［タッチスクリーンを無効にする］のみデフォルトが［オン］**です。
  - タッチスクリーンを無効にする
  - デバイスの回転感知を無効にする
  - 音量ボタンを無効にする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 着信/サイレントスイッチを無効にする

  着信/サイレントスイッチを無効にするが**オン**の場合、着信音の動作は、最初に無効にされたときのスイッチの位置によって異なります。

- スリープ/スリープ解除ボタンを無効にする
- 自動ロックを無効にする
- VoiceOverを無効にする
- ズームを有効にする
- 色を反転を有効にする
- AssistiveTouchを有効にする
- 選択項目の読み上げを有効にする
- モノラルオーディオを有効にする
- 音声コントロールを有効にする

- **ユーザーが有効にするオプション:** 各オプションの既定値は**オフ**です。
  - VoiceOverの調整を許可する
  - ズーム調整を許可
  - 色反転調整を許可
  - AssistiveTouch調整を許可
  - 音声コントロール調整を許可

- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

iPadをキオスクとして構成する

アプリロックデバイスポリシーを使用して、監視対象のiPadをキオスクとして実行できます。Appleはこの機能をシングルアプリモードと呼んでいます。この機能の詳細については、Appleのドキュメントを参照してください。このポリシーを展開する前に、実行したいアプリを展開していることを確認してください。

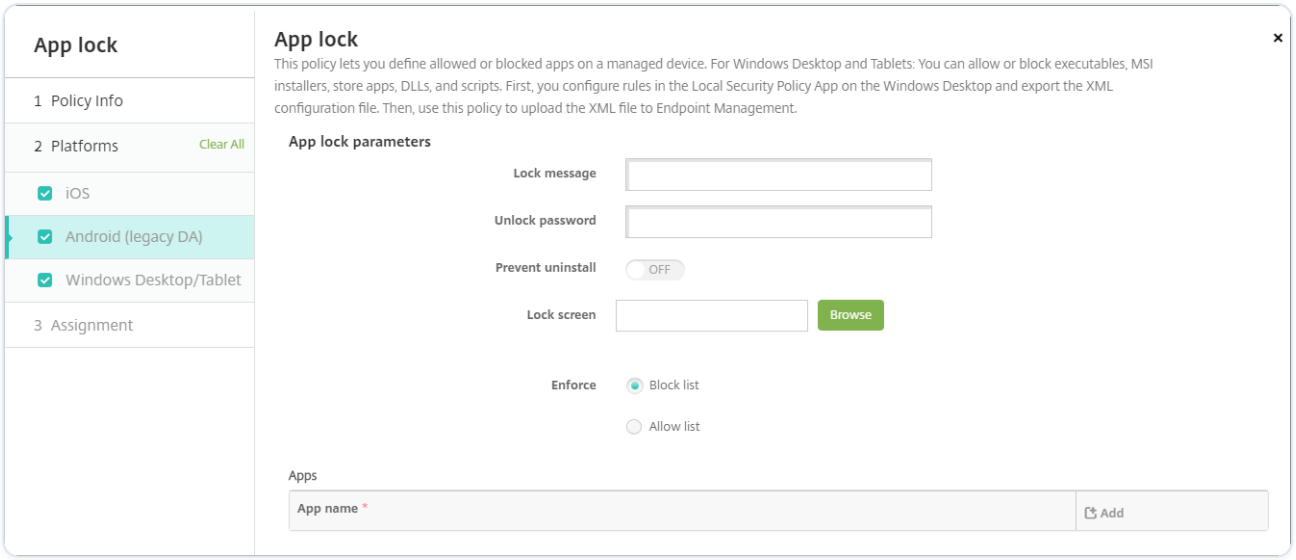
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **構成 > デバイスポリシー**に移動し、**追加**をクリックします。
2. **アプリロック**ポリシーを選択します。
3. **ポリシー名**とオプションの**説明**を入力します。
4. **iOS**プラットフォームのみを選択します。
5. **アプリバンドルID**には、iPadで実行したいアプリを選択します。
6. 以前に説明したとおり、必要なオプションを設定し、ポリシーを保存します。
7. ポリシーをiPadと同じデリバリーグループに追加し、ポリシーを展開します。

Android (レガシーDA) 設定

注:

App Lockデバイスポリシーを使用して、Android設定アプリをブロックすることはできません。



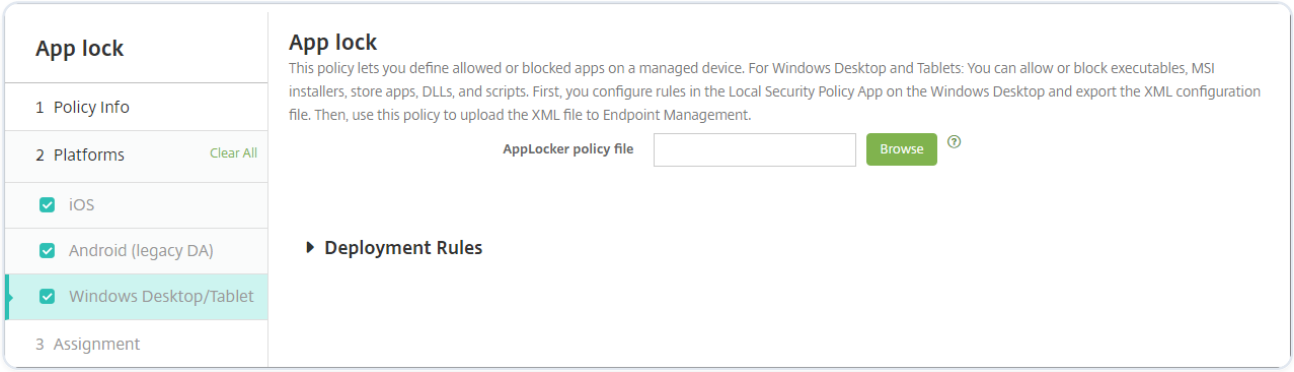
- **App Lockパラメーター**
  - **ロックメッセージ:** ロックされたアプリを開こうとしたときにユーザーに表示されるメッセージを入力します。
  - **ロック解除パスワード:** アプリのロックを解除するためのパスワードを入力します。
  - **アンインストールを防止:** ユーザーがアプリをアンインストールできるかどうかを選択します。デフォルトは**オフ**です。
  - **ロック画面: 参照**をクリックしてファイルの場所に移動し、デバイスのロック画面に表示される画像を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **適用: ブロックリスト**をクリックして、デバイスでの実行が許可されていないアプリのリストを作成します。**許可リスト**をクリックして、デバイスでの実行が許可されているアプリのリストを作成します。

- **アプリ: 追加**をクリックし、次の操作を行います。
  - **アプリ名:** ドロップダウンリストから、許可リストまたはブロックリストに追加するアプリの名前をクリックします。または、**新規追加**をクリックして、利用可能なアプリのリストにアプリを追加します。
  - **新規追加**を選択した場合は、表示されるフィールドにアプリ名を入力します。
  - 「**保存**」または「**キャンセル**」をクリックします。
  - 許可リストまたはブロックリストに追加する各アプリに対して、これらの手順を繰り返します。

Windowsデスクトップおよびタブレットの設定



App Lockの前提条件

- Windowsで、Windows 10またはWindows 11デスクトップのローカルセキュリティポリシーエディターでルールを構成します。
- ポリシーXMLファイルをエクスポートします。Citrix®は、デフォルト構成のロックやデバイスでの問題発生を避けるため、Windowsでデフォルトルールを作成することを推奨します。
- その後、App Lockデバイスポリシーを使用して、XMLファイルをCitrix Endpoint Managementにアップロードします。ルールの作成に関する詳細については、次のMicrosoftの記事を参照してください: `<https://docs.microsoft.com/ja-jp/windows/security/threat-protection/applocker/applocker-overview>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WindowsからポリシーXMLファイルを構成およびエクスポートするには

重要:

Windowsポリシーエディターを通じてポリシーXMLファイルを構成する際は、監査のみモードを使用してください。

1. Windowsコンピューターで、**ローカルセキュリティポリシー**エディターを起動します。「**スタート**」をクリックし、「**ローカルセキュリティポリシー**」と入力して、「**ローカルセキュリティポリシー**」をクリックします。
2. コンソールツリーで、**アプリケーション制御ポリシー**を展開します。
3. **AppLocker**をクリックし、中央ペインで「**ルールの適用を構成**」をクリックします。
4. 「**構成済み**」を選択し、次に「**ルールの適用**」を選択します。ルールを有効にすると、「**ルールの適用**」がデフォルトになります。
5. 「**AppLocker**」を右クリックし、「**ポリシーのエクスポート**」をクリックして、XMLファイルを保存します。

「

注：

」：

「**実行可能ルール**」、「**Windowsインストーラールール**」、「**スクリプトルール**」、および「**パッケージアプリルール**」を作成できます。これを行うには、フォルダーを右クリックし、「**新しいルールの作成**」をクリックします。

ポリシーXMLファイルをCitrix Endpoint Managementにインポートするには

アプリロックポリシーを作成します。「**アプリロックポリシーファイル**」設定の横にある「**参照**」をクリックしてXMLファイルに移動します。

アプリロックポリシーの適用を停止するには

Citrix Endpoint Managementでアプリロックポリシーを展開した後：そのアプリロックポリシーの適用を停止するには、空のXMLファイルを作成します。次に、別のアプリロックポリシーを作成し、ファイルをアップロードして、ポリシーを展開します。アプリロックが有効になっているデバイスは影響を受けません。ポリシーを初めて受信するデバイスには、アプリロックポリシーが適用されません。

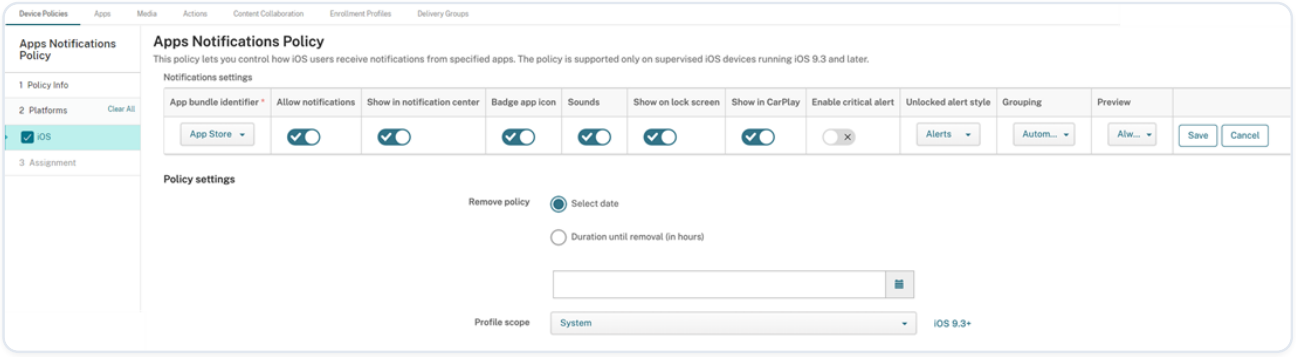
© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ通知デバイスポリシー

アプリ通知ポリシーを使用すると、iOSユーザーが指定されたアプリから通知を受け取る方法を制御できます。このポリシーは、iOS 9.3以降を実行している監視対象のiOSデバイスでのみサポートされています。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定



- **アプリバンドル識別子:** 通知設定を管理するアプリを指定します。
  - アプリバンドルIDを選択します。オプションは、管理対象デバイス上のアプリのインベントリを収集する**アプリインベントリ**デバイスポリシーを有効にした後にのみ利用可能になります。
  - を選択し、アプリバンドルIDを入力します。 アプリバンドルIDを見つけるには、「App Storeでアプリのバンドルを見つける」を参照してください。
- **通知を許可:** 通知を許可するには、 を選択します。
- **通知センターに表示:** ユーザーデバイスの通知センターに通知を表示するには、 を選択します。
- **アプリのアイコンにバッジを表示:** 通知とともにバッジ付きアプリのアイコンを表示するには、 を選択します。
- **サウンド:** 通知にサウンドを含めるには、 を選択します。
- **ロック画面に表示:** ユーザーデバイスのロック画面に通知を表示するには、 を選択します。
- **CarPlayに表示:** Apple CarPlayに通知を表示するには、 を選択します。iOS 12以降に適用されます。デフォルトは**オン**です。
- **重大な通知を有効にする:** アプリが通知を、おやすみモードと着信音設定を無視する重大な通知としてマークできるようにするには、 を選択します。iOS 12以降に適用されます。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ロック解除時のアラートスタイル: なし、バナー**、または**アラート**を選択して、ロック解除時のアラートの外観を構成します。
- **プレビュー:** デバイスがアプリの通知プレビューをどのように表示するかを選択します。iOS 14以降に適用されます。
  - **常に:** デバイスがロックされているかロック解除されているかに関わらず、通知プレビューを表示します。
  - **ロック解除時:** デバイスがロック解除されている場合にのみ、通知プレビューを表示します。
  - **なし:** デバイス上の通知プレビューをクリアします。
- **グループ化:** デバイスがアプリからの通知をどのようにグループ化するかを選択します。iOS 12以降のデバイスに適用されます。
  - **自動:** アプリによって指定されたグループに通知をグループ化します。
  - **アプリ別:** アプリからの通知を1つのグループにまとめます。
  - **オフ:** アプリの通知グループ化をクリアします。デバイスはすべての通知を順番に表示します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。オプションは次のとおりです。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降に適用されます。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。iOS 9.3以降に適用されます。

アプリのアンインストールデバイスポリシー

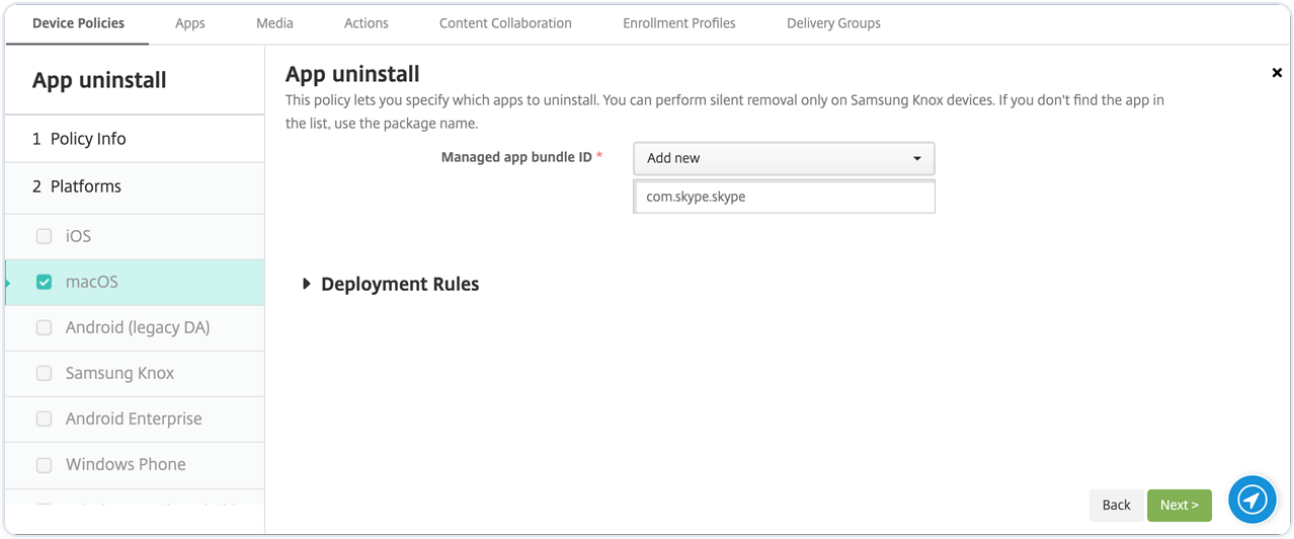
アプリのアンインストールポリシーを使用すると、ユーザーデバイスからアプリを削除できます。サポートを終了したい場合や、別のベンダーの類似アプリに置き換えたい場合に、アプリを削除することがあります。

このポリシーがユーザーデバイスに展開されると、ユーザーはアプリのアンインストールを促すプロンプトを受け取り、その後アプリが削除されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このポリシーを追加または構成するには、 > の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOSおよびmacOSの設定



- **管理対象アプリのバンドルID:** リストから既存の管理対象アプリを選択するか、 を選択します。このプラットフォーム用に構成されたアプリがない場合、リストは空になり、新しい管理対象アプリを追加する必要があります。 を選択すると、管理対象アプリ名を入力できるフィールドが表示されます。iOS 5.0以降およびmacOS 11.0以降で利用可能です。

Android (レガシーDA)、Android Enterprise、およびWindowsデスクトップ/タブレットの設定

- **アンインストールするアプリ:** 追加する各アプリについて、 をクリックし、次の操作を行います。
  - **アプリ名:** ドロップダウンリストから既存のアプリをクリックするか、 をクリックして新しいアプリ名を入力します。このプラットフォーム用に構成されたアプリがない場合、リストは空になり、新しいアプリを追加する必要があります。
  - アプリを追加するには をクリックし、アプリの追加をキャンセルするには をクリックします。

Android Enterpriseアプリの場合、アプリインベントリデバイスポリシーも有効にします。「アプリインベントリデバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

対応するパブリックアプリストアアプリのインストール後にエンタープライズアプリを自動的にアンインストールする

Citrix Endpoint Managementを構成して、パブリックアプリストア版のインストール時にCitrixアプリのエンタープライズ版を削除できます。この機能により、パブリックアプリストア版のインストール後にユーザーデバイスに2つの類似したアプリアイコンが表示されるのを防ぎます。

アプリのアンインストールデバイスポリシーの展開条件により、Citrix Endpoint Managementは新しいバージョンのインストール時にユーザーデバイスから古いアプリを削除します。この機能は、エンタープライズモード (XME) でCitrix Endpoint Managementサーバーに接続されている管理対象iOSデバイスでのみ利用可能です。

「インストール済みアプリ名」条件で展開ルールを構成するには：

- Enterpriseアプリの**管理対象アプリバンドルID**を指定します。
- ルールを追加します: **新しいルール**をクリックし、サンプルに示すように、**インストール済みアプリ名**と**次と等しい**を選択します。パブリックアプリストアアプリのアプリバンドルIDを入力します。

この例では、指定されたデリバリーグループ内のデバイスにパブリックアプリストアアプリ (com.citrix.mail.ios) がインストールされると、Citrix Endpoint Management はEnterpriseバージョン (com.citrix.mail) を削除します。

アプリのアンインストール制限デバイスポリシー

Amazonデバイスでユーザーがアンインストールできるアプリとできないアプリを指定できます。

このポリシーを追加または構成するには、 **>** に移動します。詳しくは、「デバイスポリシー」を参照してください。

Amazonの設定

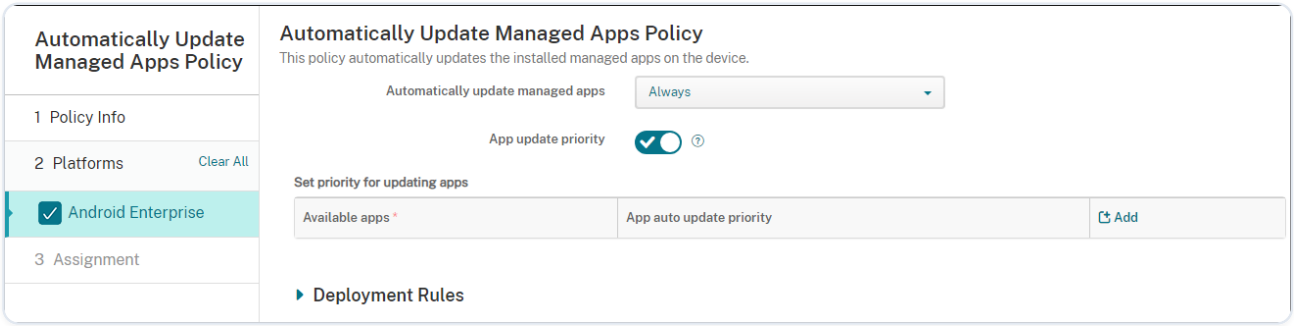
- **アプリのアンインストール制限設定:** 追加するアプリルールごとに、 をクリックして、次の操作を行います。
  - **アプリ名:** ドロップダウンリストからアプリをクリックするか、 をクリックしてアプリを追加します。
  - **ルール:** ユーザーがアプリをアンインストールできるかどうかを選択します。デフォルトではアンインストールが許可されています。
  - または をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

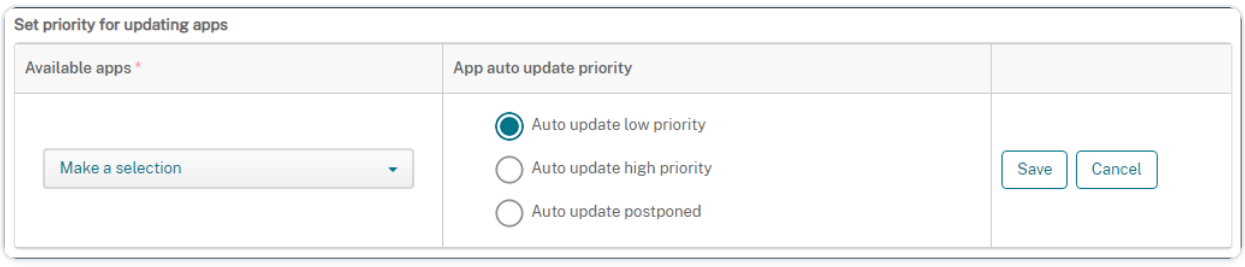
管理対象アプリの自動更新デバイスポリシー

このポリシーは、Android Enterpriseデバイスにインストールされている管理対象アプリがどのように更新されるかを制御します。ユーザーがデバイス上のアプリの自動更新を許可する機能を制限できます。ユーザーがデバイス上のアプリの自動更新を制御できるようにする場合、ユーザーは管理対象のGoogle Playストアで自動アプリ更新ポリシーを設定します。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、デバイスポリシーを参照してください。



- **管理対象アプリを自動更新**
  - **常に:** アプリの自動更新を有効にします。**常に**がデフォルトです。
  - **ユーザーによるポリシー構成を許可:** ユーザーが管理対象のGoogle Playストアでデバイスの自動アプリ更新ポリシーを構成できるようにします。
  - **しない:** アプリの自動更新を無効にします。
  - **デバイスがWi-Fiに接続されている場合のみ:** デバイスがWi-Fiに接続されている場合にのみ、アプリの自動更新を許可します。
- **アプリの更新優先度: オン**の場合、各管理対象アプリの更新優先度レベルを構成できます。
- **アプリの更新優先度を設定: 追加**をクリックして、アプリの更新優先度を構成します。



  - **利用可能なアプリ:** メニューからアプリを選択して、更新優先度を構成します。
  - **アプリの自動更新優先度:** 次の中から更新優先度を選択します。
    - **自動更新低優先度:** デバイスが充電中で、アクティブに使用されておらず、従量制ではないネットワークに接続されている場合にアプリが更新されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **高優先度で自動更新:** アプリは制約なしに、できるだけ早く更新されます。
- **自動更新を延期:** 新しいバージョンが利用可能になってから最大90日間、アプリは自動的に更新されません。90日後、アプリは低優先度で自動的に更新されます。アプリが更新された後、さらに90日間は自動的に更新されません。ユーザーはいつでも手動でアプリを更新できます。

◦ 完了したら、**保存**をクリックします。鉛筆アイコンをクリックして構成を編集できます。ゴミ箱アイコンをクリックして構成を削除します。

BitLockerデバイスポリシー

Windows 10およびWindows 11には、BitLockerと呼ばれるディスク暗号化機能が含まれており、紛失または盗難されたWindowsデバイスへの不正アクセスに対する追加のファイルおよびシステム保護を提供します。さらなる保護のために、BitLockerをTrusted Platform Module (TPM) チップバージョン1.2以降と組み合わせて使用できます。TPMチップは、暗号化操作を処理し、暗号化キーの生成、保存、および使用を制限します。

Windows 10ビルド1703以降、MDMポリシーでBitLockerを制御できます。Citrix Endpoint ManagementのBitLockerデバイスポリシーを使用して、Windows 10およびWindows 11デバイスのBitLockerウィザードで利用可能な設定を構成します。たとえば、BitLockerが有効になっているデバイスでは、BitLockerはユーザーにいくつかのオプションを提示します。

- 起動時にドライブのロックを解除する方法
- 回復キーをバックアップする方法
- 固定ドライブのロックを解除する方法。

BitLockerデバイスポリシー設定では、以下の項目も構成します。

- TPMチップのないデバイスでBitLockerを有効にする。
- BitLockerインターフェイスで回復オプションを表示する。
- BitLockerが有効になっていない場合に、固定ドライブまたはリムーバブルドライブへの書き込みアクセスを拒否する。
- ユーザーがキーを忘れたり紛失したりした場合にアクセスできるように、暗号化されたBitLocker回復キーを安全に保存する。このキーはセルフヘルプポータルで見つけることができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

> デバイスでBitLocker暗号化が開始された後、更新されたBitLockerデバイスポリシーを展開しても、デバイス上のBitLocker設定を変更することはできません。

このポリシーを追加または構成するには、 **>** に移動します。詳しくは、「デバイスポリシー」を参照してください。

要件

- BitLockerデバイスポリシーには、Windows 10 EnterpriseまたはWindows 11 Enterpriseエディションが必要です。
- BitLockerデバイスポリシーを展開する前に、BitLockerを使用するための環境を準備してください。BitLockerのシステム要件やセットアップを含むMicrosoftからの詳細情報については、BitLockerの記事を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windowsデスクトップおよびタブレットの設定

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BitLocker policy

This policy lets you enable BitLocker on an enrolled machine and specify the encryption mechanism to use.

BitLocker settings

Require device to be encrypted — ON

Encryption settings

Configure encryption methods — ON

Operating system drive — XTS AES 128-bit

Fixed drive — XTS AES 128-bit

Removable drive — XTS AES 128-bit

OS drive settings

Require additional authentication at startup — ON

Block BitLocker on devices without TPM chip — ON

TPM startup — Allow TPM

TPM startup PIN — Allow startup PIN with TPM

TPM startup key — Allow TPM key at startup

TPM startup key and PIN — Allow startup key and PIN with TPM

PIN length

Minimum PIN length — 6

BitLocker password recovery settings

BitLocker Recovery backup to Endpoint Management — ON

The Self-Help Portal displays the recovery key on the Devices page. Enable the server property shp.console.enable to provide access to the portal. **Learn more**

OS drive recovery settings

Enable OS drive recovery — ON

Allow certificate based data recovery agent — ON

48-bit recovery password — Allow 48-bit password

256-bit recovery key — Allow 256-bit recovery key

Hide OS drive recovery options — ON

Save recovery info to Active Directory Domain Services — ON

Recovery info stored in Active Directory Domain Services — Backup recovery password

Enable BitLocker after storing recovery info in Active Directory Domain Services — ON

- **BitLocker設定**
  - **デバイスの暗号化を必須にする:** Windowsデスクトップまたはタブレットで BitLocker暗号化を有効にするようユーザーに促すかどうかを決定します。**オン**の場合、登録完了後にデバイスは、企業がデバイスの暗号化を要求していることを示すメッセージを表示します。**オフ**の場合、ユーザーはプロンプト表示されず、BitLockerはポリシー設定を使用します。既定値は**オフ**です。
- **暗号化設定**
  - **暗号化方法の構成:** 特定のドライブタイプに使用する暗号化方法を決定します。**オフ**の場合、BitLockerウィザードは、ドライブタイプに使用する暗号化方法をデバイスユーザーに促します。すべてのドライブの暗号化方法は既定でXTS-AES 128ビットです。リムーバブルドライブの暗号化方法は既定でAES-CBC 128ビットです。**オン**の場合、BitLockerはポリシーで指定された暗号化方法を使用します。**オン**の場合、次の追加設定が表示されます: **オペレーティングシステムドライブ**、**固定ドライブ**、および**リムーバブルドライブ**。各ドライブタイプの既定の暗号化方法を選択します。既定値は**オフ**です。
- **OSドライブ設定**
  - **起動時に追加認証を要求する:** デバイスの起動時に必要な追加認証を指定します。また、TPMチップを持たないデバイスでBitLockerを許可するかどうかも指定します。**オフ**の場合、TPMのないデバイスはBitLocker暗号化を使用できません。TPMに関する情報については、Microsoftの記事「Trusted Platform Module Technology Overview」を参照してください。**オン**の場合、次の追加設定が表示されます。既定値は**オフ**です。
  - **TPMチップのないデバイスでのBitLockerをブロックする:** TPMチップのないデバイスでは、BitLockerはユーザーにロック解除パスワードまたはスタートアップキーの作成を要求します。スタートアップキーはUSBドライブに保存され、ユーザーは起動前にデバイスに接続する必要があります。ロック解除パスワードは最低8文字です。既定値は**オフ**です。
  - **TPMスタートアップ:** TPMを搭載したデバイスには、TPMのみ、TPM + PIN、TPM + キー、TPM + PIN + キーの4つのロック解除モードがあります。TPMスタートアップはTPMのみのモード用で、暗号化キーはTPMチップに保存されます。このモードでは、ユーザーが追加のロック解除データを提供する必要はありません。ユーザーデバイスは、TPMチップからの暗号化キーを使用して、再起動時に自動的にロック解除されます。既定値は**TPMを許可**です。
  - **TPMスタートアップPIN:** この設定はTPM + PINロック解除モードです。PINは最大20桁です。**最小PIN長**設定を使用して、最小PIN長を指定します。ユーザーはBitLockerセットアップ中にPINを構成し、デバイス起動時にPINを提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **TPMスタートアップキー:** この設定はTPM + キーロック解除モードです。スタートアップキーはUSBまたはその他のリムーバブルドライブに保存され、ユーザーは起動前にデバイスに接続する必要があります。
- **TPMスタートアップキーとPIN:** この設定はTPM + PIN + キーロック解除モードです。

  ロック解除が成功すると、オペレーティングシステムがロードを開始します。そうでない場合、デバイスはリカバリモードに入ります。

- **PINの長さ**
  - **最小PIN長:** TPM起動PINの最小の長さ。デフォルトは**6**です。
- **BitLockerパスワード回復設定**
  - **BitLocker回復のCitrix Endpoint Managementへのバックアップ:** このオプションが有効になっている場合、デバイスのロックを解除する必要があるユーザーは、セルフヘルプポータルでBitLocker回復キーを見つけることができます。Citrix Endpoint Management管理者は、ユーザーのBitLocker回復キーを見ることはできません。BitLocker回復キーの表示の詳細については、「BitLocker回復キー」を参照してください。
- **OSドライブ回復設定:** BitLockerで暗号化されたOSドライブのユーザー向け回復オプションを構成します。
  - **OSドライブ回復を有効にする:** ロック解除手順が失敗した場合、BitLockerは構成された回復キーをユーザーに要求します。この設定は、ロック解除パスワードまたはUSB起動キーを持っていないユーザーが利用できるオペレーティングシステムドライブの回復オプションを構成します。デフォルトは**オフ**です。
  - **証明書ベースのデータ回復エージェントを許可する:** 証明書ベースのデータ回復エージェントを許可するかどうかを指定します。グループポリシー管理コンソール (GPMC) またはローカルグループポリシーエディターの公開キーポリシーからデータ回復エージェントを追加します。データ回復エージェントの詳細については、Microsoftの記事「BitLockerグループポリシー設定」を参照してください。デフォルトは**オフ**です。
  - **48ビット回復パスワード:** ユーザーが回復パスワードを使用することを許可するか、または要求するかを指定します。BitLockerはパスワードを生成し、ファイルまたはMicrosoft Cloudアカウントに保存します。デフォルトは**48ビットパスワードを許可**です。
  - **256ビット回復キー:** ユーザーが回復キーを使用することを許可するか、または要求するかを指定します。回復キーはUSBドライブに保存されるBEKファイルです。デフォルトは**256ビット回復キーを許可**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **OSドライブ回復オプションを非表示にする:** BitLockerインターフェイスで回復オプションを表示するか非表示にするかを指定します。**オン**の場合、BitLockerインターフェイスには回復オプションが表示されません。その場合、デバイスをActive Directoryに登録し、回復オプションをActive Directoryに保存し、**回復情報をAD DSに保存**を**オン**に設定します。デフォルトは**オフ**です。
- **回復情報をActive Directory Domain Servicesに保存する:** 回復オプションをActive Directory Domain Servicesに保存するかどうかを指定します。デフォルトは**オフ**です。
- **Active Directory Domain Servicesに保存される回復情報:** BitLocker回復パスワード、または回復パスワードとキーパッケージをActive Directory Domain Servicesに保存するかどうかを指定します。キーパッケージを保存すると、物理的に破損したドライブからデータを回復できます。デフォルトは**回復パスワードをバックアップ**です。
- **Active Directory Domain Servicesに回復情報を保存した後にBitLockerを有効にする:** デバイスがドメインに接続されており、BitLocker回復情報のActive Directoryへのバックアップが成功しない限り、ユーザーがBitLockerを有効にすることを防ぐかどうかを指定します。**オン**の場合、BitLockerを開始する前にデバイスがドメインに参加している必要があります。デフォルトは**オフ**です。
- **プレブート回復メッセージとURL:** BitLockerが回復画面にカスタマイズされたメッセージとURLを表示するかどうかを指定します。**オン**の場合、次の追加設定が表示されます: **デフォルトの回復メッセージとURLを使用**、**空の回復メッセージとURLを使用**、**カスタム回復メッセージを使用**、**カスタム回復URLを使用**、および**Citrix Endpoint Management回復メッセージとURLを使用**。**オフ**の場合、デフォルトの回復メッセージとURLが表示されます。デフォルトは**オフ**です。

- **固定ドライブの回復設定:** BitLockerで暗号化された固定ドライブのユーザー向け回復オプションを設定します。BitLockerは、固定ドライブの暗号化についてユーザーにメッセージを表示しません。起動時にドライブのロックを解除するには、ユーザーはパスワードまたはスマートカードを提供します。このポリシーには含まれていない起動時のロック解除設定は、ユーザーが固定ドライブでBitLocker暗号化を有効にすると、BitLockerインターフェイスに表示されます。関連設定の詳細については、このリストの前の「**OSドライブの回復を構成する**」を参照してください。デフォルトは**オフ**です。
- **固定ドライブの設定**
  - **BitLockerを使用していない固定ドライブへの書き込みアクセスをブロックする: オン**の場合、ユーザーはBitLockerで暗号化されている場合にのみ固定ドライブに書き込むことができます。デフォルトは**オフ**です。
- **リムーバブルドライブの設定**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **BitLockerを使用していないリムーバブルドライブへの書き込みアクセスをブロックする: オン**の場合、ユーザーはBitLockerで暗号化されている場合にのみリムーバブルドライブに書き込むことができます。この設定は、組織が他の組織のリムーバブルドライブへの書き込みアクセスを許可するかどうかに応じて構成してください。デフォルトは**オフ**です。
- **他の組織デバイスへの書き込みアクセスをブロックする: オン**の場合、ユーザーはネットワークドライブなど、組織内の他のデバイスに書き込むことはできません。
- **その他のドライブ設定**
- **その他のディスク暗号化のプロンプト:** デバイス上の他のディスク暗号化に関する警告プロンプトを無効にできます。デフォルトは**オフ**です。

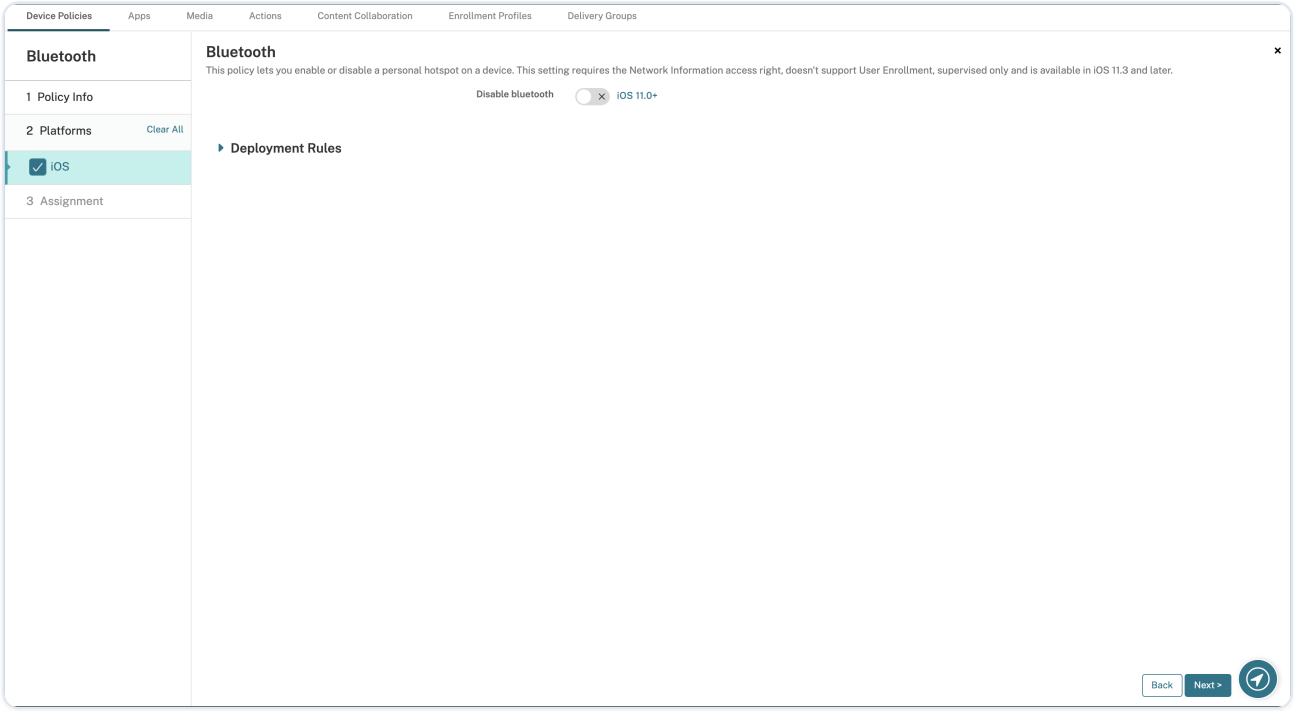
Bluetoothデバイスポリシー

監視対象のiOSデバイスでBluetoothポリシーを構成して、Bluetoothを有効または無効にできます。

この設定にはネットワーク情報アクセス権が必要で、ユーザー登録はサポートされておらず、iOS 11.3以降で利用できます。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、デバイスポリシーを参照してください。

iOS設定



- **Bluetoothを無効にする:** 監視対象デバイスでBluetoothを無効または有効にできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カレンダー (CalDav) デバイスポリシー

Citrix Endpoint Management でデバイスポリシーを追加すると、ユーザーの iOS または macOS デバイスにカレンダー (CalDAV) アカウントを追加し、CalDAV をサポートする任意のサーバーとスケジュールデータを同期できるようになります。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS 設定

- **アカウントの説明:** アカウントの説明を入力します。このフィールドは必須です。
- **ホスト名:** CalDAV サーバーのアドレスを入力します。このフィールドは必須です。
- **ポート:** CalDAV サーバーに接続するポートを入力します。このフィールドは必須です。デフォルトは **8443** です。
- **プリンシパル URL:** ユーザーのカレンダーへのベース URL を入力します。
- **ユーザー名:** ユーザーのログオン名を入力します。このフィールドは必須です。
- **パスワード:** オプションのユーザーパスワードを入力します。
- **SSL を使用:** CalDAV サーバーへの Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは **オン** です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、 と です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0 以降でのみ利用可能です。

macOS設定

- **アカウントの説明:** アカウントの説明を入力します。このフィールドは必須です。
- **ホスト名:** CalDAVサーバーのアドレスを入力します。このフィールドは必須です。
- **ポート:** CalDAVサーバーに接続するポートを入力します。このフィールドは必須です。デフォルトは**8443**です。
- **プリンシパルURL:** ユーザーのカレンダーへのベースURLを入力します。
- **ユーザー名:** ユーザーのログオン名を入力します。このフィールドは必須です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **パスワード:** オプションのユーザーパスワードを入力します。
- **SSLを使用:** CalDAVサーバーへのSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは**オン**です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

携帯電話デバイスポリシー

このポリシーを使用すると、iOSデバイスで携帯電話ネットワーク設定を構成できます。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

プロキシサーバーポートなどの非文字列フィールドでマクロを使用できます。

たとえば、整数に展開される`${device.xyz}`や`${setting.xyz}`のようなマクロを使用できます。また、**iOSおよびmacOSプロファイルのインポート**デバイスポリシーを使用してCitrix Endpoint Managementにインポートするデバイス構成XMLファイルでマクロを使用することもできます。

- **APNの添付**
  - **名前:** この構成の名前。
  - **認証タイプ:** ドロップダウンリストで、チャレンジハンドシェイク認証プロトコル (**CHAP**) またはパスワード認証プロトコル (**PAP**) をクリックします。デフォルトは**PAP**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ユーザー名とパスワード:** 認証に使用するユーザー名とパスワード。

- **APN**
  - **名前:** アクセスポイント名 (APN) 構成の名前。
  - **認証タイプ:** ドロップダウンリストで、**CHAP**または**PAP**をクリックします。デフォルトは**PAP**です。
  - **ユーザー名とパスワード:** 認証に使用するユーザー名とパスワード。
  - **プロキシサーバー:** プロキシサーバーのネットワークアドレス。
  - **プロキシサーバーポート:** プロキシサーバーのポートです。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。

接続スケジューリングデバイスポリシー

重要:

Citrixでは、AndroidおよびAndroid EnterpriseデバイスからCitrix Endpoint Managementへの接続を制御するために、Firebase Cloud Messaging (FCM)を使用することをお勧めします。FCMの使用方法については、「Firebase Cloud Messaging」を参照してください。

FCMを使用しない場合は、ユーザーデバイスがCitrix Endpoint Managementに接続する方法とタイミングを制御する接続スケジューリングポリシーを作成できます。FCMを使用する場合でも、接続スケジューリングポリシーを作成する必要があります。

ユーザーがデバイスを手動で接続するか、デバイスが定義された時間枠内で接続するように指定できます。

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］**の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

AndroidおよびAndroid Enterpriseの設定

- **デバイスの接続を要求:** このスケジュールに設定するオプションをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **しない:** 手動で接続します。ユーザーは、デバイス上のCitrix Endpoint Managementから接続を開始する必要があります。このオプションは、セキュリティポリシーをデバイスに展開できなくなり、ユーザーが新しいアプリやポリシーを受け取ることができなくなるため、Citrixでは本番環境での展開には推奨していません。**［しない］**オプションはデフォルトで有効になっています。
- **毎回:** 指定された間隔で接続します。このオプションが有効なときに、ロックやワイプなどのセキュリティポリシーを送信すると、Citrix Endpoint Managementはデバイスが次回接続したときにデバイス上でアクションを処理します。このオプションを選択すると、**［N分ごとに接続］フィールドが表示され、デバイスが再接続する必要がある分数値を入力する必要があります。デフォルト値および最小値は120**です。
- **スケジュールを定義:** ユーザーデバイス上のCitrix Endpoint Managementは、ネットワーク接続が失われた後、Citrix Endpoint Managementサーバーへの再接続を試みます。Citrix Endpoint Managementは、定義した時間枠内で制御パケットを定期的に送信することで接続を監視します。接続時間枠の定義方法については、次の「接続時間枠の定義」を参照してください。
  - **これらの各範囲内で接続を要求:** ユーザーのデバイスは、定義された時間枠のいずれかで少なくとも1回接続する必要があります。
  - **UTCではなくローカルデバイス時間を使用:** 定義された時間枠を協定世界時 (UTC) ではなくローカルデバイス時間に同期します。

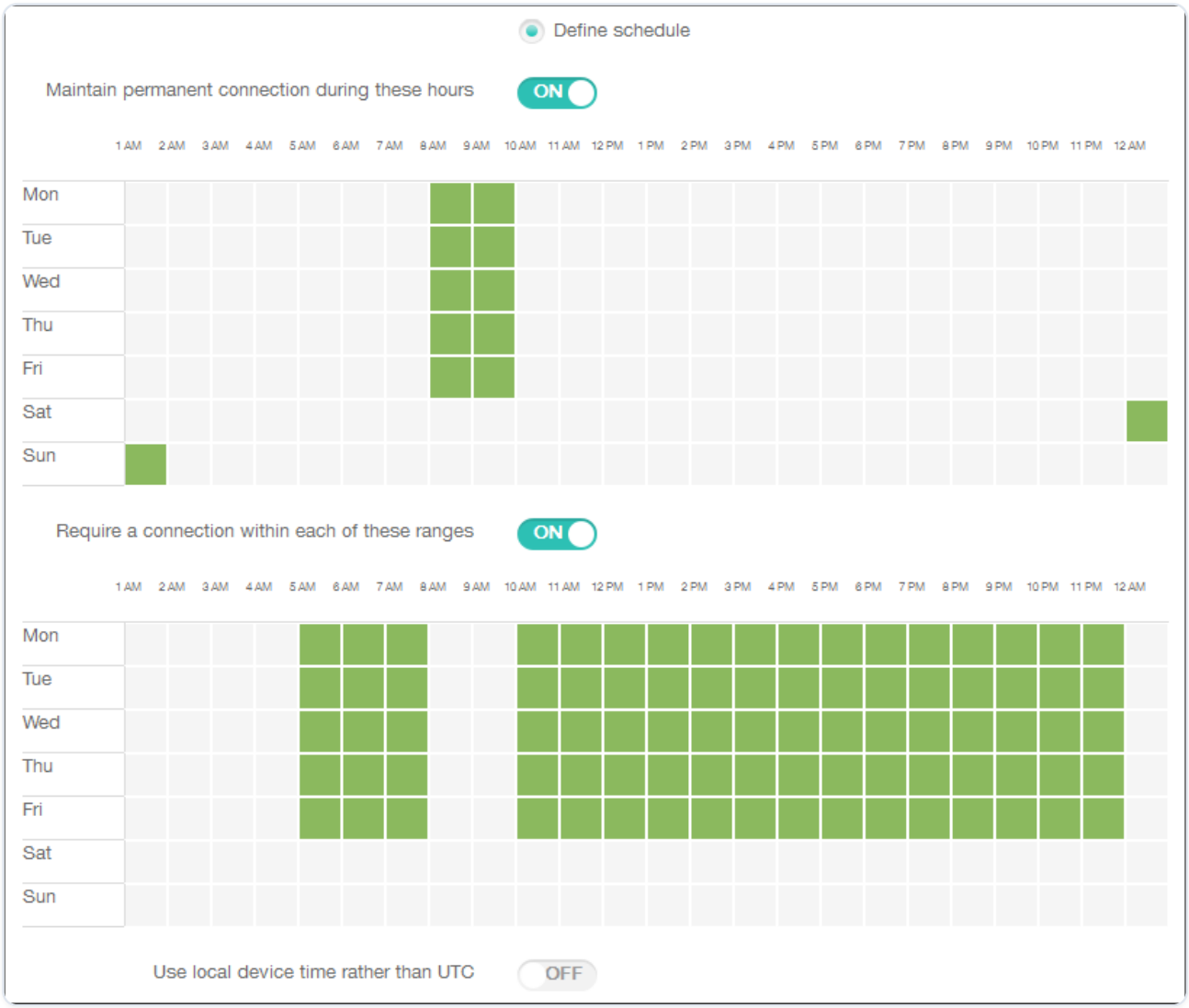
接続時間枠の定義

次のオプションを有効にすると、希望する時間枠を定義できるタイムラインが表示されます。特定の時間帯に永続的な接続を要求するか、特定の時間枠内で接続を要求するために、いずれかまたは両方のオプションを有効にできます。タイムラインの各四角は1時間です。毎週平日の午前8時から午前9時の間に接続を指定するには、タイムライン上の毎週平日の午前8時から午前9時の間の四角をクリックします。

例えば、次の図の2つのタイムラインでは、以下が必要です。

- 毎週平日の午前8時から午前10時までの永続的な接続
- 土曜日の午前1時から日曜日の午前2時までの永続的な接続
- 毎週平日の午前5時から午前8時まで、または午前10時から午前12時までの間に少なくとも1つの接続

© 1997–2026 Citrix Systems, Inc. All rights reserved.



連絡先 (CardDAV) デバイスポリシー

Citrix Endpoint Management でデバイスポリシーを追加して、ユーザーの iOS または macOS デバイスに iOS 連絡先 (CardDAV) アカウントを追加し、CardDAV をサポートする任意のサーバーと連絡先データを同期できるようにします。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS 設定

- **アカウントの説明:** アカウントの説明を入力します。このフィールドは必須です。
- **ホスト名:** CardDAV サーバーのアドレスを入力します。このフィールドは必須です。
- **ポート:** CardDAV サーバーに接続するポートを入力します。このフィールドは必須です。デフォルトは **8443** です。
- **プリンシパル URL:** ユーザーのカレンダーへのベース URL を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ユーザー名:** ユーザーのログオン名を入力します。このフィールドは必須です。
- **パスワード:** オプションのユーザーパスワードを入力します。
- **SSL の使用:** CardDAV サーバーへの Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは **オン** です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除をスケジュールする方法を選択します。利用可能なオプションは、 と です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。

macOS設定

- **アカウントの説明:** アカウントの説明を入力します。このフィールドは必須です。
- **ホスト名:** CardDAVサーバーのアドレスを入力します。このフィールドは必須です。
- **ポート:** CardDAVサーバーに接続するポートを入力します。このフィールドは必須です。デフォルトは**8443**です。
- **プリンシパルURL:** ユーザーのカレンダーへのベースURLを入力します。
- **ユーザー名:** ユーザーのログオン名を入力します。このフィールドは必須です。
- **パスワード:** オプションのユーザーパスワードを入力します。
- **SSLの使用:** CardDAVサーバーへのSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは**オン**です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間（時間）**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

資格情報デバイスポリシー

資格情報デバイスポリシーは、Citrix Endpoint Managementで構成されたPKIを指します。たとえば、PKI構成には、PKIエンティティ、キーストア、資格情報プロバイダー、またはサーバー証明書が含まれる場合があります。資格情報の詳細については、「証明書と認証」を参照してください。

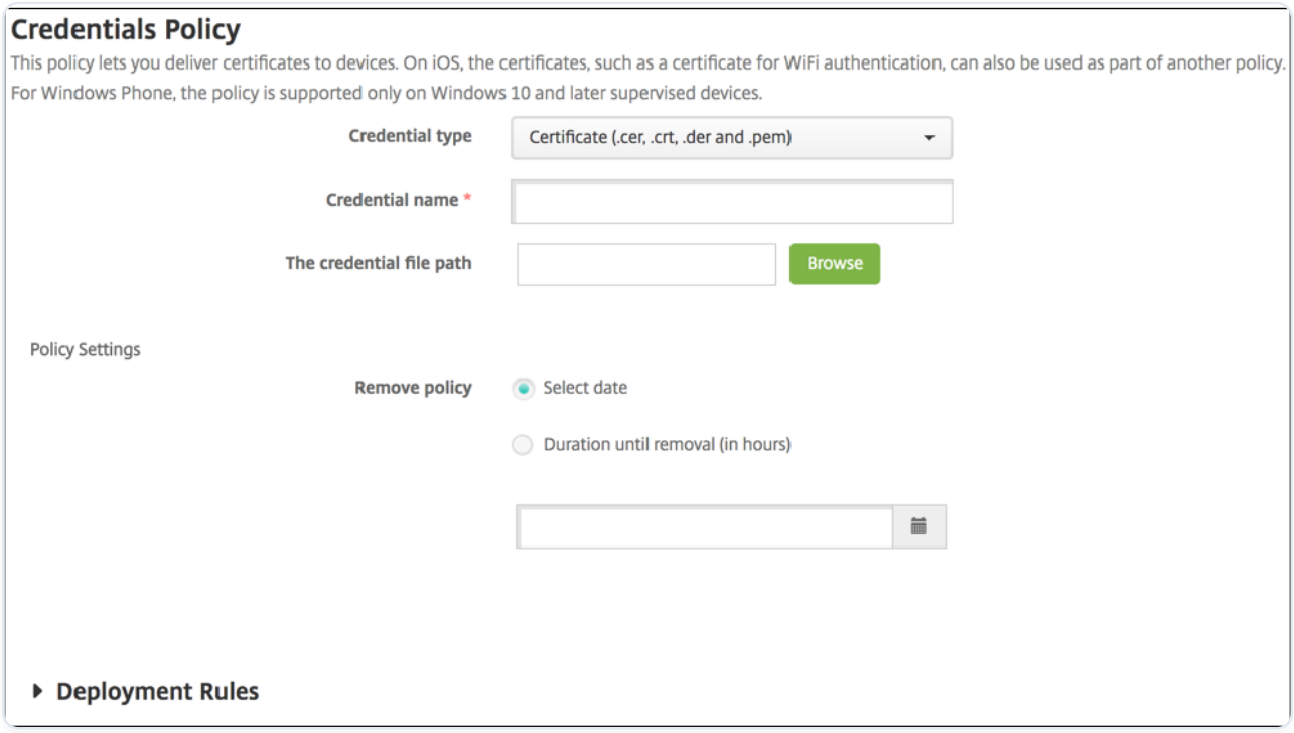
サポートされている各プラットフォームには異なる値のセットが必要であり、それらについてはこの記事で説明します。

注：

このポリシーを作成する前に、各プラットフォームで使用する予定の資格情報、およびすべての証明書とパスワードが必要です。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定



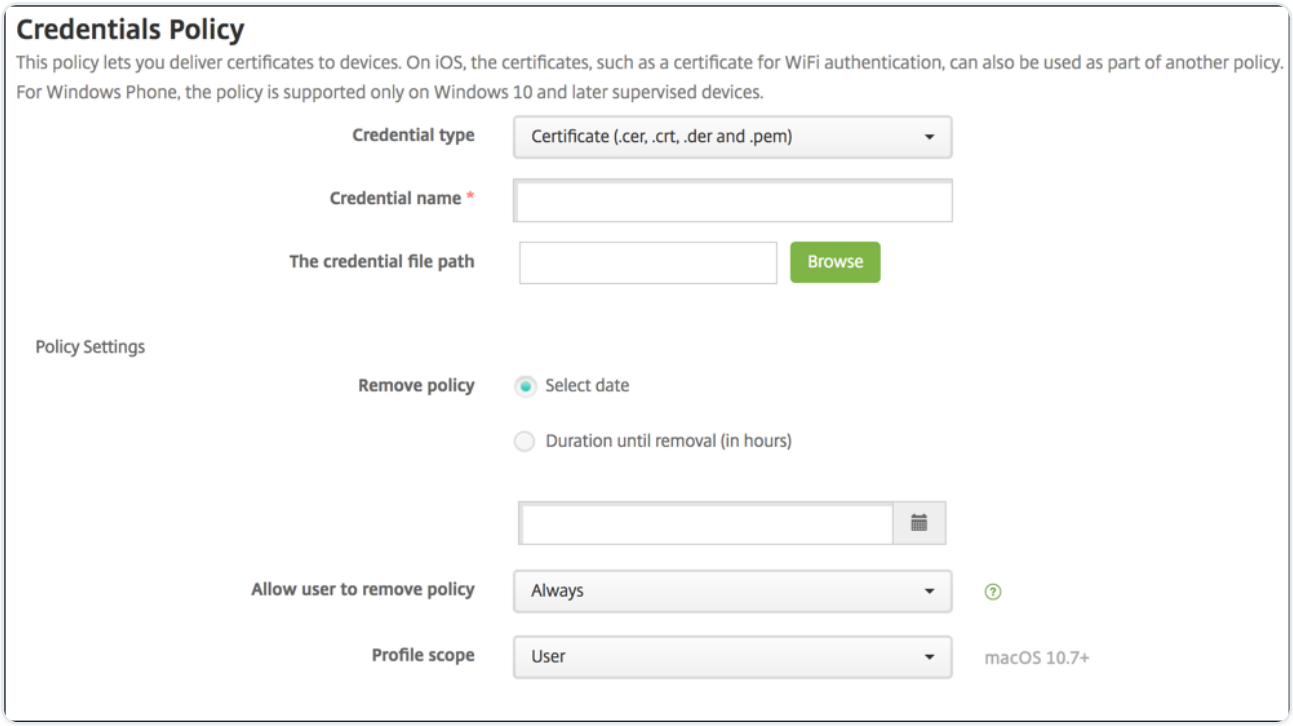
次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **資格情報の種類：** このポリシーで使用する資格情報の種類をドロップダウンリストからクリックし、選択した資格情報について次の情報を入力します。
  - **証明書**
    - **資格情報名：** 資格情報の一意の名前を入力します。
    - **資格情報ファイルのパス：** をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
  - **キーストア**
    - **資格情報名：** 資格情報の一意の名前を入力します。
    - **資格情報ファイルのパス:** 参照をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
    - **パスワード:** 資格情報のキーストアパスワードを入力します。
  - **サーバー証明書**
    - **サーバー証明書:** ドロップダウンリストから使用したい証明書をクリックします。
  - **資格情報プロバイダー**
    - **資格情報プロバイダー:** ドロップダウンリストから資格情報プロバイダーの名前をクリックします。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択** と **削除までの期間 (時間)** です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから **常に**、**パスコードが必要**、または **なし** を選択します。**パスコードが必要** を選択した場合は、**削除パスコード** フィールドにパスコードを入力します。iOSでは利用できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS設定



次の設定を構成します。

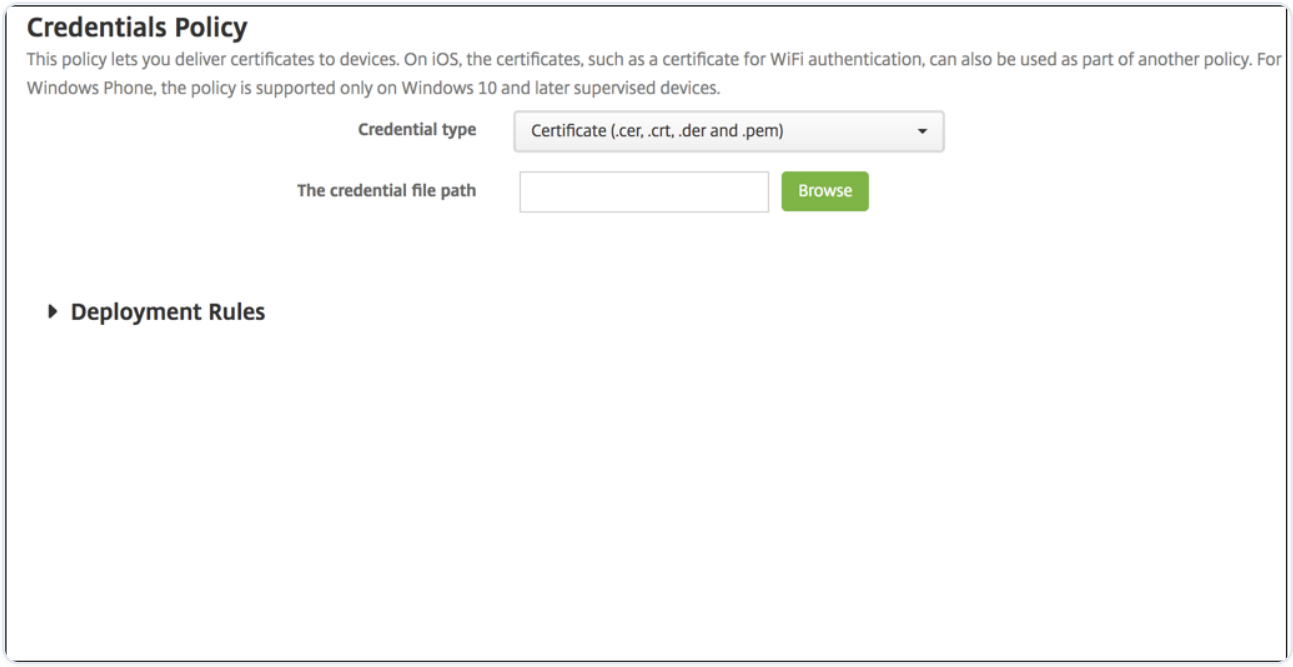
- **資格情報タイプ:** このポリシーで使用したい資格情報の種類をドロップダウンリストからクリックし、選択した資格情報について次の情報を入力します。
  - **証明書**
    - **資格情報名:** 資格情報の一意の名前を入力します。
    - **資格情報ファイルのパス: 参照**をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
  - **キーストア**
    - **資格情報名:** 資格情報の一意の名前を入力します。
    - **資格情報ファイルのパス: 参照**をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
    - **パスワード:** 資格情報のキーストアパスワードを入力します。
  - **サーバー証明書**
    - **サーバー証明書:** ドロップダウンリストから使用する証明書をクリックします。
  - **資格情報プロバイダー**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **資格情報プロバイダー:** ドロップダウンリストから資格情報プロバイダーの名前をクリックします。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションは、macOS 10.7以降でのみ利用可能です。

Android設定



次の設定を構成します。

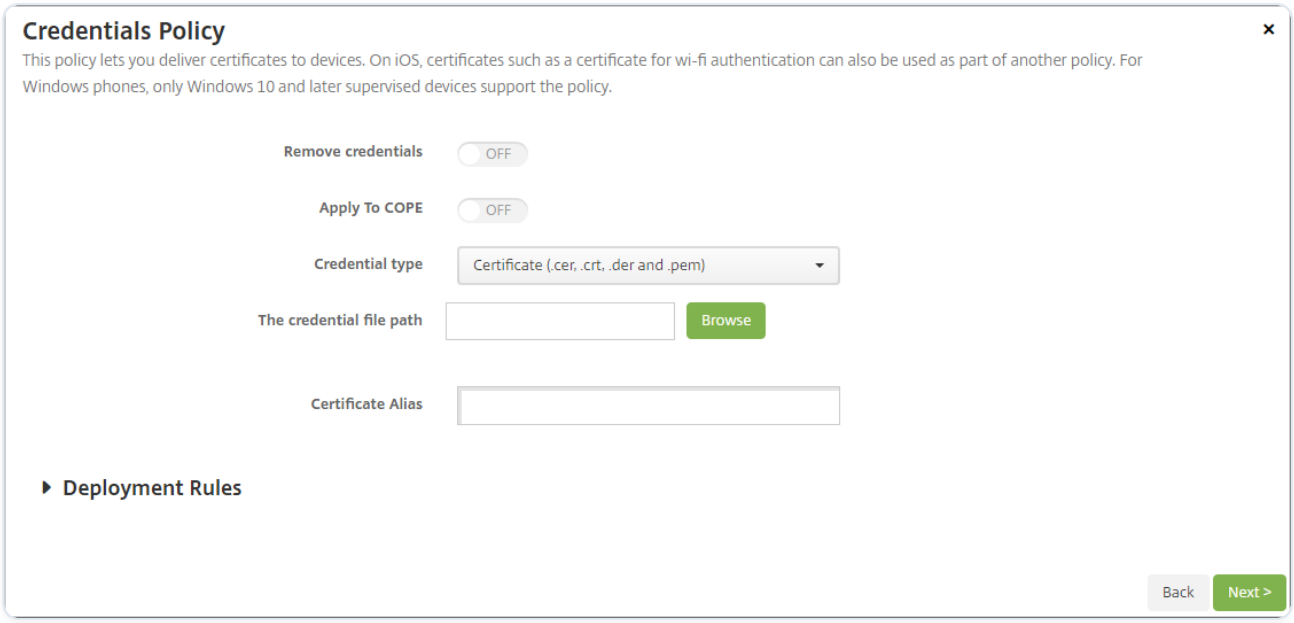
- **資格情報の種類:** このポリシーで使用する資格情報の種類をドロップダウンリストからクリックし、選択した資格情報について次の情報を入力します。
  - **証明書**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **資格情報名:** 資格情報の一意の名前を入力します。
- **資格情報ファイルのパス:** をクリックして資格情報ファイルを選択し、ファイルの場所に移動します。

- **キーストア**
  - **資格情報名:** 資格情報の一意の名前を入力します。
  - **資格情報ファイルのパス: 参照**をクリックして資格情報ファイルを選択し、ファイルの場所に移動します。
  - **パスワード:** 資格情報のキーストアパスワードを入力します。
- **サーバー証明書**
  - **サーバー証明書:** ドロップダウンリストから使用する証明書をクリックします。
- **資格情報プロバイダー**
  - **資格情報プロバイダー:** ドロップダウンリストから資格情報プロバイダーの名前をクリックします。

Android エンタープライズ設定



資格情報設定がどのように適用されるかを決定するために、これらの設定を構成します。

- **資格情報の削除:** 以下の設定を構成するには、**オン**に設定します。デフォルトは**オフ**です。
  - **ユーザー資格情報の削除:** 管理対象のキーストアから証明書を削除します。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **信頼されたルート証明書の削除:** すべての非システムCA証明書をアンインストールします。デフォルトは**オフ**です。

- **仕事用プロファイルを持つ完全に管理されたデバイス/会社所有デバイスの仕事用プロファイルに適用:** 仕事用プロファイルを持つ完全に管理されたデバイスの資格情報ポリシー設定を構成できます。この設定が**オン**に設定されている場合、これらの設定のいずれかを選択します。このポリシーは、デバイス上の仕事用プロファイルにのみ適用されます。

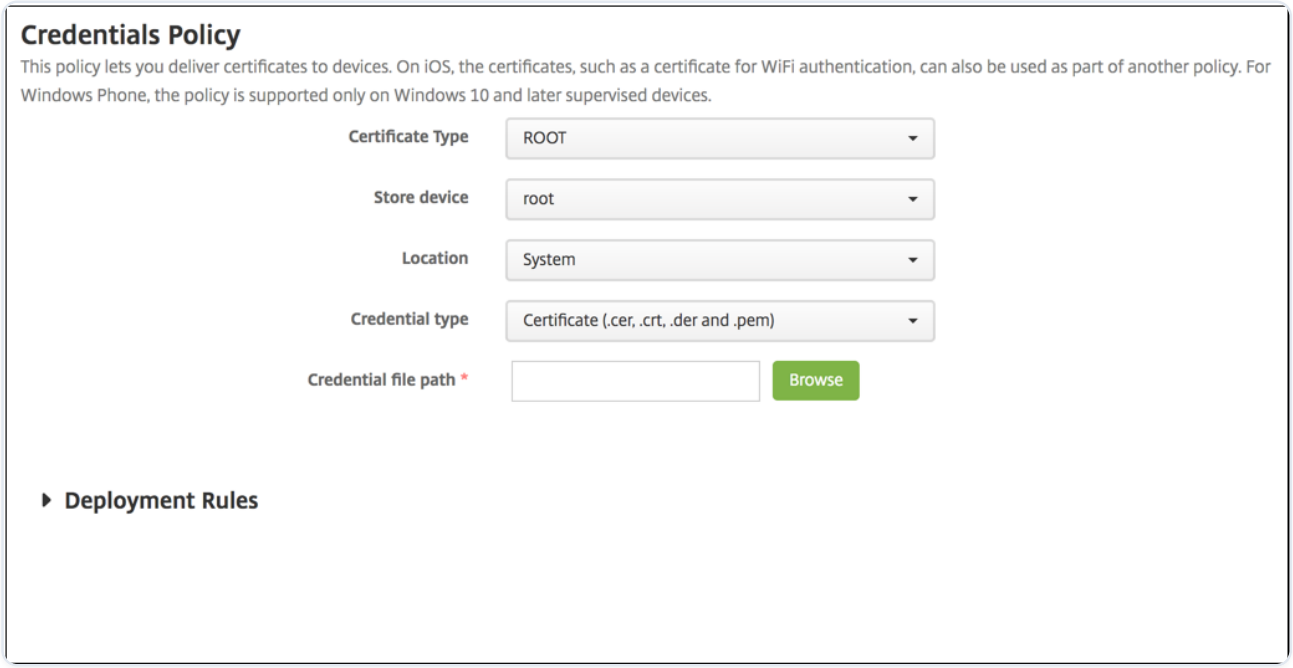
資格情報設定を構成します。

- **資格情報タイプ:** このポリシーで使用する資格情報の種類をドロップダウンリストからクリックし、選択した資格情報について以下の情報を入力します。
    - **証明書**
        - **資格情報名:** 資格情報の一意の名前を入力します。
        - **資格情報ファイルのパス: 参照**をクリックしてファイルパスに移動し、資格情報ファイルを選択します。
    - **キーストア**
        - **資格情報名:** 資格情報の一意の名前を入力します。
        - **資格情報ファイルのパス: 参照**をクリックしてファイルが保存されている場所に移動し、資格情報ファイルを選択します。
        - **パスワード:** 資格情報のキーストアパスワードを入力します。
        - **証明書エイリアス:** 証明書エイリアスを使用すると、アプリが証明書にアクセスしやすくなります。Android Enterpriseの管理対象構成デバイスポリシーで証明書エイリアスを構成します。次に、資格情報デバイスポリシーの**証明書エイリアス**フィールドにエイリアスを入力します。アプリは、ユーザーによる操作なしで証明書を取得し、VPNを認証します。
    - **サーバー証明書**
        - **サーバー証明書:** ドロップダウンリストから使用する証明書をクリックします。
    - **資格情報プロバイダー**
        - **資格情報プロバイダー:** ドロップダウンリストから資格情報プロバイダーの名前をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **証明書を使用するアプリ:** このプロバイダーからの資格情報にサイレントアクセスできるアプリを指定するには、**追加**をクリックし、アプリを選択して、**保存**をクリックします。
- **証明書エイリアス:** 証明書エイリアスを使用すると、アプリが証明書にアクセスしやすくなります。Android Enterpriseの管理対象構成デバイスポリシーで証明書エイリアスを構成します。次に、資格情報デバイスポリシーの**証明書エイリアス**フィールドにエイリアスを入力します。アプリは、ユーザーによる操作なしで証明書を取得し、VPNを認証します。

Windowsデスクトップ/タブレット設定



- **証明書の種類:** ドロップダウンリストで、**ROOT**または**CLIENT**のいずれかをクリックします。
- **ROOT**をクリックした場合は、次の設定を構成します。
  - **デバイスの保存:** 資格情報の証明書ストアの場所について、ドロップダウンリストで**root**、**My**、または**CA**をクリックします。**My**は、証明書をユーザーの証明書ストアに保存します。
  - **場所:** Windows 10およびWindows 11タブレットの場合、**システム**のみが場所として利用可能です。
  - **資格情報タイプ:** Windows 10およびWindows 11タブレットの場合、**証明書**のみが資格情報タイプとして利用可能です。
  - **資格情報ファイルパス: 参照**をクリックしてファイルの場所に移動し、証明書ファイルを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **クライアント**をクリックした場合、以下の設定を構成します。
- **場所:** Windows 10およびWindows 11タブレットの場合、**システム**のみが場所として利用可能です。
- **資格情報タイプ:** Windows 10およびWindows 11タブレットの場合、**キーストア**のみが資格情報タイプとして利用可能です。
- **資格情報名:** 資格情報の名前を入力します。このフィールドは必須です。
- **資格情報ファイルパス: 参照**をクリックしてファイルの場所に移動し、証明書ファイルを選択します。
- **パスワード:** 資格情報に関連付けられたパスワードを入力します。このフィールドは必須です。

カスタムXMLデバイスポリシー

Citrix Endpoint Managementでは、カスタムXMLポリシーを作成して、サポートされているWindowsデバイスで次の機能をカスタマイズできます。

- プロビジョニング（デバイスの構成、機能の有効化または無効化を含む）
- デバイス構成（ユーザーによる設定およびデバイスパラメーターの変更を許可することを含む）
- ソフトウェアアップグレード（アプリやシステムソフトウェアを含む、デバイスにロードされる新しいソフトウェアまたはバグ修正の提供を含む）
- 障害管理（デバイスからのエラーおよびステータスレポートの受信を含む）

注：

XMLコンテンツを作成する際は、\%文字の使用に注意してください。\%文字はXMLの予約文字であり、XMLの特殊文字をエスケープするためにのみ使用されます。名前に\%を使用するには、\%25としてエンコードします。

Windowsデバイスの場合：WindowsのOpen Mobile Alliance Device Management（OMA DM）APIを使用して、カスタムXML構成を作成します。OMA DM APIを使用したカスタムXMLの作成は、このトピックの範囲外です。OMA DM APIの使用について詳しくは、Microsoft Developer NetworkサイトのOMA DM プロトコルのサポートを参照してください。

Android Enterpriseデバイスの場合：MX Management System（MXMS）を使用して、カスタムXML構成を作成します。MXMS APIを使用したカスタムXMLの作成は、この記事の範囲外です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］**の順に選択します。詳しくは、(/ja-jp/citrix-endpoint-management/policies.html)を参照してください。

Windowsデスクトップ/タブレットの設定

XMLコンテンツ： ポリシーに追加するカスタムXMLコードを入力またはコピー＆ペーストします。

［次へ］をクリックすると、Citrix Endpoint ManagementはXMLコンテンツの構文をチェックします。構文エラーはコンテンツボックスの下に表示されます。続行する前に、すべてのエラーを修正してください。

構文エラーがない場合、**［カスタムXMLポリシー］**の割り当てページが表示されます。

Windows AutoPilot を使用してデバイスをセットアップおよび構成する

Windows AutoPilot は、新しいデバイスをセットアップおよび事前構成し、生産的な使用に備えるために使用されるテクノロジーのコレクションです。Windows AutoPilot を使用して、デバイスをリセット、再利用、および回復できます。AutoPilot は、現在のオペレーティングシステム展開の複雑さの一部を取り除くのに役立ちます。AutoPilot を使用すると、タスクがシンプルな設定と操作のセットに削減され、デバイスを迅速かつ効率的に使用できるようになります。

Citrix Endpoint Management で Windows AutoPilot を使用することの概要については、このビデオをご覧ください。

<iframe src="https://www.youtube.com/embed/DFCeF68NXM0" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

前提条件

- Azure Active Directory ポータルで構成された会社のブランド設定。
- 会社が Azure Active Directory Premium P1 または P2 サブスクリプションを所有していること。
- Citrix Endpoint Management の IdP タイプとして Azure Active Directory を構成します。Citrix Endpoint Management コンソールで、 **>** に移動します。
- Windows AutoPilot で使用されるクラウドサービスへのネットワーク接続。
- Windows 10 Professional、Enterprise、または Education (バージョン 1703 以降) または Windows 11 Professional、Enterprise、または Education がプレインストールされているデバイス。
- デバイスがインターネットにアクセスできること。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件の構成の詳細については、AutoPilot に関する Microsoft Windows のドキュメントを参照してください: `<https://docs.microsoft.com>`。

AutoPilot デバイス向けに Citrix Endpoint Management で Windows 自動再展開を構成するには

1. カスタム XML デバイスポリシーでカスタム XML ポリシーを追加する手順に従います。 に以下を追加します。

```
<Add>

<CmdID>_cmdid_</CmdID>

<Item>

<Target>

<LocURI>./Vendor/MSFT/Policy/Config/CredentialProviders/
DisableAutomaticReDeploymentCredentials</LocURI>

</Target>

<Meta>

<Format xmlns="syncml:metinf">int</Format>

</Meta>

<Data>0</Data>

</Item>

</Add>
```

2. Windows のロック画面で、キーボードショートカット **CTRL + Windows キー + R** を入力します。
3. Azure Active Directory アカウントでログインします。
4. デバイスは、ユーザーがデバイスを再展開する権限を持っていることを確認します。その後、デバイスは再展開されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. デバイスがAutoPilot構成で更新された後、ユーザーは新しく構成されたデバイスにログインできます。

Windows 11デバイスにシングルアプリキオスクを展開する

注:

Windows 11デバイスは、シングルアプリキオスクモードのみをサポートしています。

XML content テキストボックスに、次のXMLスクリプトをコピーして貼り付け、以下の文字列を独自の設定に置き換えます。

- `your_username_here` (2つのインスタンス): デバイス上に作成するユーザー名。両方のインスタンスで同じ設定を維持します。
- `your password_here`: ユーザーのパスワード。
- `your_UWP_app_id_here`: デバイスに展開するUMPアプリのAUMID。

XMLスクリプト:

```
<Add>
    <CmdID>_cmdid_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/Accounts/Users/
your_username_here/Password</LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data>your_password_here</Data>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    </Item>
</Add>
<Replace>
    <CmdID>_cmdid_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/AssignedAccess/Configuration</
LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data><![CDATA[<AssignedAccessConfiguration
        xmlns="http://schemas.microsoft.com/AssignedAccess/2017/config"
        xmlns:rs5="http://schemas.microsoft.com/AssignedAccess/201810/
config">
            <Profiles>
                <Profile Id="{AFF9DA33-AE89-4039-B646-3A5706E92957}">
                    <KioskModeApp AppUserModelId="your_UWP_app_id_here"/>
                </Profile>
            </Profiles>
            <Configs>
                <Config>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    <Account>your_username_here</Account>

                    <DefaultProfile Id="{AFF9DA33-AE89-4039-
B646-3A5706E92957}"/>

                </Config>

            </Configs>

        </AssignedAccessConfiguration>]]></Data>

    </Item>

</Replace>
```

宣言型デバイス管理ポリシー

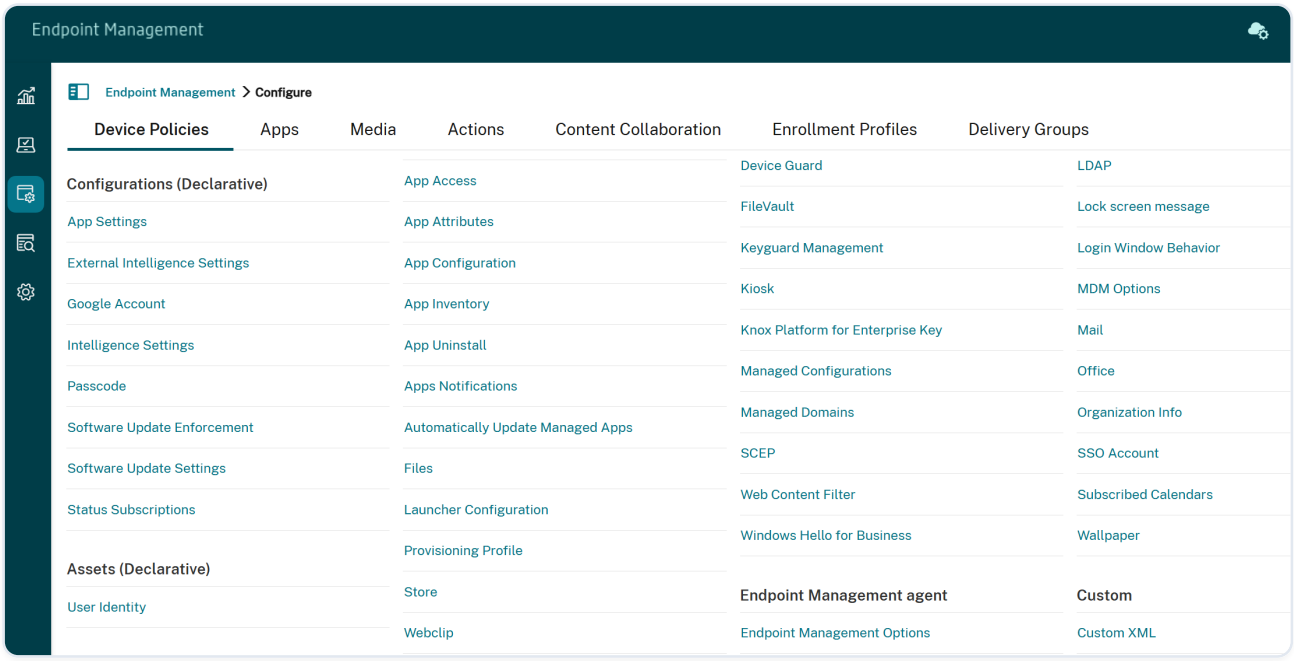
Appleは、iOS 15で宣言型データモデルパラダイムを使用した宣言型デバイス管理 (DDM) を発表しました。このパラダイムにより、サーバーは、コマンドのシリアル化やMDMを介したデバイスのポーリングに通常関連する一般的なパフォーマンスとスケーラビリティの問題を回避できます。詳細については、「宣言型管理データモデルを活用してデバイスを拡張する」を参照してください。

Citrix Endpoint Management™は、Appleが提供する最新の機能を導入するためにDDMをサポートするようになりました。

DDM機能を有効にすると、次の宣言型デバイスポリシーがサポートされます。

- アプリ設定
- 外部インテリジェンス設定
- Googleアカウント
- インテリジェンス設定
- パスコードデバイスポリシー
- ソフトウェア更新の適用
- ソフトウェア更新設定
- ステータスサブスクリプション
- ユーザーID

© 1997–2026 Citrix Systems, Inc. All rights reserved.



アプリ設定デバイスポリシー

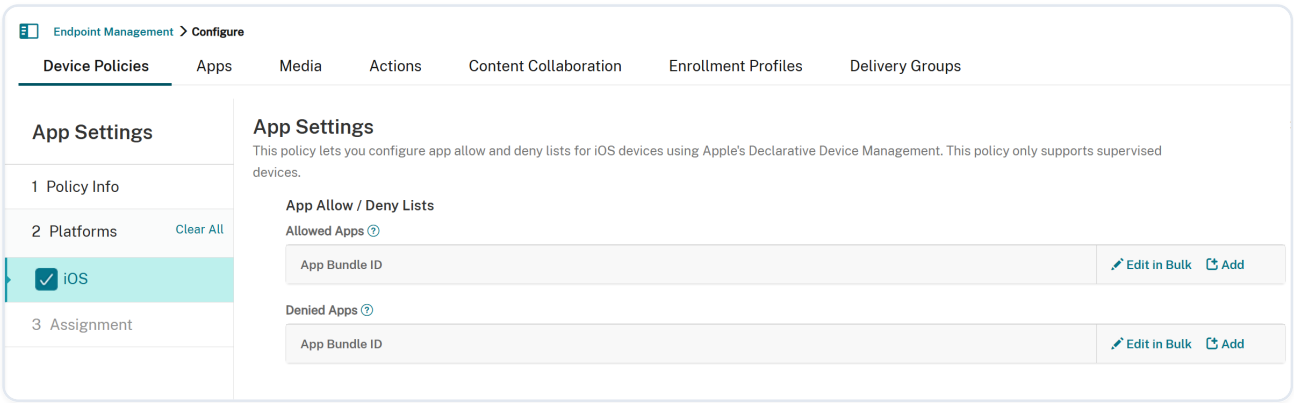
アプリ設定デバイスポリシーを使用すると、Appleの宣言型デバイス管理を使用してアプリの許可リストと拒否リストを設定できます。これは、非推奨の`allowListedAppBundleIDs`および`blockedAppBundleIDs`制限キーを置き換えます。このポリシーは、監視対象デバイスのみをサポートします。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、 デバイスポリシー を参照してください。

前提条件

- CEMのバージョンが**26.8.0**以上であること。
- **iOS 27**以降および**iPadOS 27**以降で利用可能で、監視対象デバイスのみをサポートします。

iOS設定



- アプリの許可/拒否リスト

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **許可されたアプリ:** 存在する場合、デバイスはリスト内のバンドルIDを持つアプリのみを表示または起動します。すべてのWebクリップを許可するには、値`com.apple.webapp`を含めます。これは、App Storeアプリ、マーケットプレイスアプリ、およびローカルにインストールされたアプリ（Configurator、Xcodeなどを使用）に適用されます。
  - **アプリバンドルID:** アプリバンドルIDを追加するには、 をクリックし、アプリバンドルIDを入力して、 をクリックします。追加する各アプリバンドルIDに対してこのプロセスを繰り返します。または、 をクリックし、アプリバンドルIDを1行に1つずつ、またはコンマで区切って入力または貼り付け、 をクリックすることもできます。
- **拒否されたアプリ:** 存在する場合、デバイスはリスト内のバンドルIDを持つアプリの表示または起動を防止します。すべてのWebクリップを制限するには、値`com.apple.webapp`を含めます。これは、App Storeアプリ、マーケットプレイスアプリ、およびローカルにインストールされたアプリ（Configurator、Xcodeなどを使用）に適用されます。

注:

システムアプリを拒否すると、他の機能が無効になる場合があります。たとえば、App Storeアプリを拒否すると、ユーザーはユーザーベースのボリューム購入プログラム（VPP）の利用規約に同意できなくなる可能性があります。アプリの許可リストまたはアプリの拒否リストのいずれかを構成することをお勧めします。両方を構成することはお勧めしません。

外部インテリジェンス設定デバイスポリシー

外部インテリジェンス設定デバイスポリシーを使用すると、Appleの宣言型デバイス管理を使用して外部AI統合（例：ChatGPT）を管理できます。このポリシーは、非推奨の外部インテリジェンス制限キーを置き換えます。このポリシーは監視対象デバイスのみをサポートします。

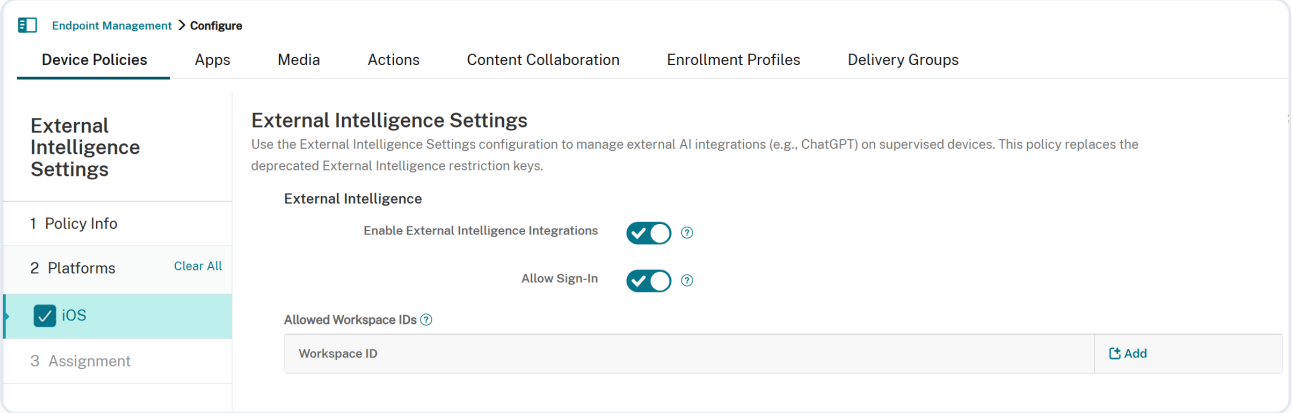
このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、以下を参照してください。 デバイスポリシー。

前提条件

- CEMバージョンが**26.8.0**以上であること。
- **iOS 26.4**以降および**iPadOS 26.4**以降で利用可能で、監視対象デバイスのみをサポートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定



- **外部インテリジェンス**
  - **外部インテリジェンス統合を有効にする: オフ**の場合、外部インテリジェンス統合を無効にします。デフォルトは**オン**です。
  - **サインインを許可: オフ**の場合、外部インテリジェンス統合のサインインを無効にします。デフォルトは**オン**です。
  - **許可されたワークスペースID:** 文字列の配列ですが、現在は単一の要素に制限されています。存在する場合、Apple Intelligenceは指定された外部統合ワークスペースIDのみの使用を許可し、リクエストを行うにはサインインが必要です。ユーザーはサインインをサポートする統合にサインインする必要があります。複数の値は交差演算を使用して結合されます。
    - **ワークスペースID:** 外部インテリジェンスワークスペースIDを追加するには、**追加**をクリックし、ワークスペースIDを入力して、**保存**をクリックします。追加したいワークスペースIDごとにこのプロセスを繰り返します。

Googleアカウントデバイスポリシー

Googleアカウントデバイスポリシーを使用すると、iOSデバイスのGoogleアカウント設定を構成できます。設定には、アカウント名と、メールアドレスおよびユーザーのフルネームを構成するユーザーIDアセットが含まれます。

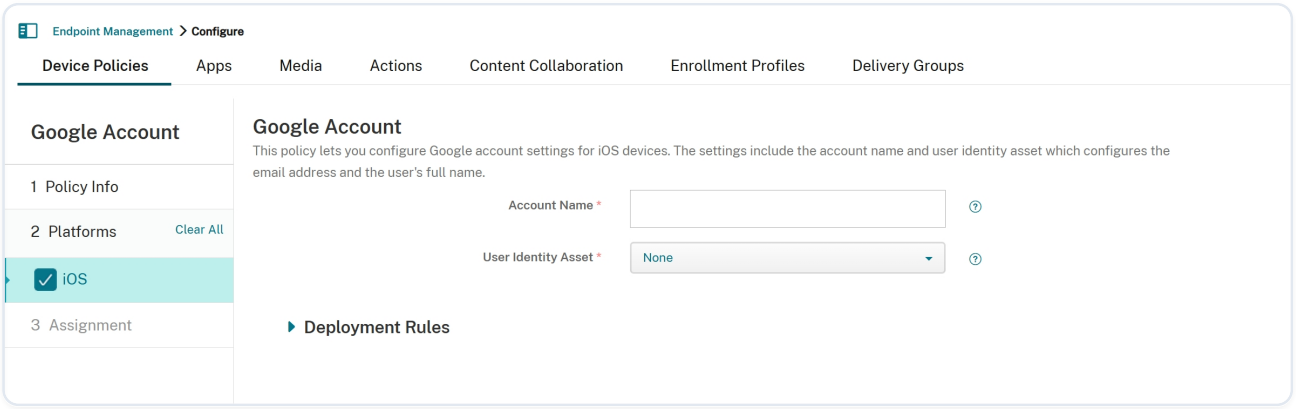
このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

前提条件

- CEMのバージョンが**25.5.0**以上であること。
- ユーザーIDポリシーが構成されていること。「ユーザーIDデバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定



- **アカウント名:** Googleアカウントの名前を入力します。
- **ユーザーIDアセット:** リストから、ユーザーのメールアドレスとフルネームを含む、ユーザーIDポリシーによって作成されたユーザーIDアセットを選択します。デフォルトは**なし**です。

インテリジェンス設定デバイスポリシー

インテリジェンス設定デバイスポリシーを使用すると、Appleの宣言型デバイス管理を使用してApple Intelligence機能を管理できます。このポリシーは、非推奨のインテリジェンス制限キーに代わるものです。このポリシーは、監視対象デバイスのみをサポートします。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、 デバイスポリシー を参照してください。

前提条件

- CEMのバージョンが**26.8.0**以上であること。
- **iOS 26.4**以降および**iPadOS 26.4**以降で利用可能で、監視対象デバイスのみをサポートします。

iOS設定

インテリジェンス設定デバイスポリシーの画像(/en-us/citrix-endpoint-management/media/intelligence-settings-ios-settings.png)

- **許可**
  - **Genmoji: オフ**の場合、Genmojiを無効にします。デフォルトは**オン**です。
  - **Image Playground: オフ**の場合、Image Playgroundを無効にします。デフォルトは**オン**です。
  - **Image Wand: オフ**の場合、Image Wandを無効にします。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Writing Tools: オフ**の場合、Apple Intelligence Writing Toolsを無効にします。デフォルトは**オン**です。
- **パーソナライズされた手書き結果: オフ**の場合、パーソナライズされた手書き結果を無効にし、システムがユーザーの手書きでテキストを生成するのを防ぎます。デフォルトは**オン**です。
- **ビジュアルインテリジェンスの要約: オフ**の場合、ビジュアルインテリジェンスの要約を無効にします。デフォルトは**オン**です。
- **Apple Intelligence Report:** 「**オフ**」の場合、Apple Intelligence Report を無効にします。デフォルトは「**オン**」です。

- **アプリ設定**
  - **メール概要:** 「**オフ**」の場合、メール概要を無効にします。デフォルトは「**オン**」です。
  - **メールスマートリプライ:** 「**オフ**」の場合、メールスマートリプライを無効にします。デフォルトは「**オン**」です。
  - **メモの文字起こし:** 「**オフ**」の場合、メモの文字起こしを無効にします。デフォルトは「**オン**」です。
  - **メモの文字起こし概要:** 「**オフ**」の場合、メモの文字起こし概要を無効にします。デフォルトは「**オン**」です。
  - **Safari概要:** 「**オフ**」の場合、Safari概要を無効にします。デフォルトは「**オン**」です。

- **強制**
  - **デバイス上のみの音声入力の強制:** 「**オン**」の場合、デバイス上のみの音声入力を強制します。デフォルトは「**オフ**」です。
  - **デバイス上のみの翻訳の強制:** 「**オン**」の場合、デバイス上のみの翻訳を強制します。デフォルトは「**オフ**」です。

パスコードデバイスポリシー

パスコードデバイスポリシーは、組織の標準に基づいてパスコード要件を作成します。デバイスにコードを要求したり、書式設定ルールや、デバイスロックまでの猶予期間などの他のパスコードルールを設定したりできます。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、 デバイスポリシー を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

- CEMのバージョンが**25.5.0**以上であること。

iOS設定

パスコードデバイスポリシー(/en-us/citrix-endpoint-management/media/passcode-ios-settings1.png)

- **パスコードを要求:** このオプションを選択すると、パスコードが要求され、iOSパスコードデバイスポリシーの構成オプションが表示されます。 の場合、パスコードの長さや品質に関する要件なしにユーザーにパスコードの設定を要求し、パスコード要件とパスコードセキュリティの設定を構成できるようにページが展開されます。デフォルトは****です。
- **パスコード要件**
  - **英数字パスコードを要求:** パスコードに少なくとも1つの英字と少なくとも1つの数字を含める必要があるかどうかを選択します。デフォルトは****です。
  - **複雑なパスコードを要求:** 複雑なパスコードを要求するかどうかを選択します。複雑なパスコードとは、繰り返し文字や増加/減少する文字（123やCBAなど）を含まず、少なくとも1つの非数字および非英字文字を含むパスコードです。デフォルトは****です。
  - **パスコードの最小長:** パスコードに含めることができる最小文字数を選択します。デフォルトは**6**です。
  - **最小複雑文字数:** パスワード内の複雑な文字の最小数を選択します。複雑な文字とは、数字や文字以外の文字（&、%、$、#など）です。デフォルトは**0**です。
- **パスコードセキュリティ**
  - **最大失敗試行回数:** iOSがデバイスを消去するまでにシステムがユーザーに許可するパスコード失敗試行回数を選択します。この設定を変更しない場合、6回の失敗試行後、ユーザーが再度パスコードを入力できるようになるまでにデバイスは時間遅延を課します。時間遅延は失敗試行ごとに増加します。最後の失敗試行後、システムはiOSデバイスからすべてのデータと設定を安全に消去します。パスコードの時間遅延は6回目の試行後に開始されるため、この値が6以下の場合、システムは時間遅延なしで、ユーザーが制限を超えるとすぐに消去またはロックをトリガーします。デフォルトは**11**です。
  - **最大猶予期間:** ユーザーがパスコードなしでデバイスのロックを解除できる最大期間を選択します。猶予期間を設けない場合は**すぐに**を選択すると、デバイスはすぐにパスコードを要求します。デフォルトは**なし**で、ユーザーは任意の期間を選択できます。
  - **デバイスの自動ロック:** システムがデバイスを自動的にロックするまでの、デバイスがアイドル状態であることができる最大期間を選択します。デバイスがこの制限に達すると、デ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

バイスはロックされ、ユーザーはロックを解除するためにパスコードを入力する必要があります。デフォルトは**なし**で、ユーザーは任意の期間を選択できます。

- **パスコードの最大有効期間:** パスコードを変更せずに維持できる最大日数を指定します。この日数を超えると、システムはデバイスのロックを解除する前にユーザーにパスコードの変更を強制します。有効な値は0～730です。**0**の値は、パスコードの即時変更を強制します。デフォルトは空で、パスコードの有効期間の制限がないことを意味します。
- **パスコードの再利用制限:** 新しいパスコードを検証する際にシステムがチェックする過去のパスコードエントリの数を選択します。指定されたパスコード履歴の範囲内で以前使用されたパスコードと一致する場合、デバイスは新しいパスコードを拒否します。有効な値は1～50です。デフォルトは**空**で、システムが履歴チェックを実行しないことを意味します。

注:

同じ設定がMDMプロファイルおよび宣言型構成としてデバイスに送信された場合、設定が複数のプロファイルによって配信された場合と同じルールが適用されます。たとえば、パスコードポリシーがプロファイル（パスコードポリシー経由）と構成（宣言型パスコードポリシー経由）によって構成されている場合、ポリシーはマージされ、最も厳格な設定が適用されます。

ソフトウェアアップデート強制デバイスポリシー

特定のOSリリース向けのソフトウェアアップデート強制デバイスポリシーにより、IT管理者はiOSデバイスのアップデートを管理し、適用されるアップデートを制御したり、すべてのアップデートを完了するための期限を設定したりできます。これらの設定は、Appleの宣言型デバイス管理機能で使用される宣言を構成します。これらの設定は以前のMDM設定とは別であり、宣言型管理が有効になっているデバイスにのみ適用されます。同じ設定の「OSアップデートの制御」ポリシーよりも優先されます。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、 デバイスポリシーを参照してください。

前提条件

- CEMバージョンが**25.5.0**以上であること。
- **iOS 17.0**以降および**iPadOS 17.0**以降で利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定

ソフトウェアアップデート強制デバイスポリシー(/en-us/citrix-endpoint-management/media/software-update-enforcement-ios-settings1.png)

- **ターゲットOSバージョンタイプ:** ターゲットOSバージョンの構成方法を指定します。デフォルトは**利用可能なiOSバージョン**です。
  - **利用可能なiOSバージョン: オン**の場合、**ターゲットOSバージョン**で利用可能なターゲットOSバージョンを一覧表示します。
  - **指定されたバージョン: オン**の場合、推奨される形式でOSバージョンを手動で入力します。
- **ターゲットOSバージョン: (必須)** 適切な時期までにデバイスをアップデートするターゲットOSバージョンを選択または入力します。これはOSのバージョン番号です (例: 17.7)。補足的なバージョン識別子 (例: 17.7.2) を含む場合もあります。
- **ターゲットビルドバージョン:** 適切な時期までにデバイスをアップデートするターゲットビルドバージョンを入力します (例: 20A242)。システムは、シード期間中のテストにビルドバージョンを使用します。ビルドバージョンには、補足的なバージョン識別子 (例: 20A242a) を含めることができます。ビルドバージョンがTargetOSVersionキーで指定されたターゲットOSバージョンと一致しない場合、ターゲットOSバージョンが優先されます。
- **ターゲットローカル日時: (必須)** ソフトウェアアップデートを強制的にインストールする日時を指定するローカル日時値を入力します。RFC3339から派生したyyyy-mm-ddThh:mm:ss形式を使用します。ただし、タイムゾーンオフセットは含まれません。ユーザーがこの時刻までにソフトウェアアップデートをトリガーしない場合、デバイスは強制的にインストールします。
- **詳細URL:** 組織が強制アップデートについて提供する詳細を示すWebページのURLを入力します。

注記:

「ソフトウェア更新適用ポリシー」と「OS更新制御ポリシー」の両方で、デバイスのOS更新を管理できます。ただし、「ソフトウェア更新適用ポリシー」は「OS更新制御ポリシー」よりも優先されます。両方のポリシーが同じ設定で展開されている場合、「OS更新制御ポリシー」の設定は上書きされ、適用されません。詳細については、「宣言型デバイス管理への移行」を参照してください。

さらに、「ソフトウェア更新適用ポリシー」と「OS更新制御ポリシー」にはいくつかの違いがあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシーの種類	ソフトウェア更新適用	OS更新制御
デバイスの種類	監視対象または非監視対象デバイス	監視対象デバイス
更新期限の適用	✓	✕
ヘルプURLの入力	✓	✕
ビルドバージョン番号を指定	✓	✕
最新のアップデートを自動展開	✕	✓
サポートされる最小バージョン	iOS 17.0	iOS 10.3 (監視対象)

ソフトウェアアップデート設定デバイスポリシー

ソフトウェアアップデート設定デバイスポリシーは、OSアップデートを延期し、システム設定でユーザーがソフトウェアアップデートと手動でやり取りする方法を制御するために使用できます。このポリシーは監視対象デバイスのみをサポートします。

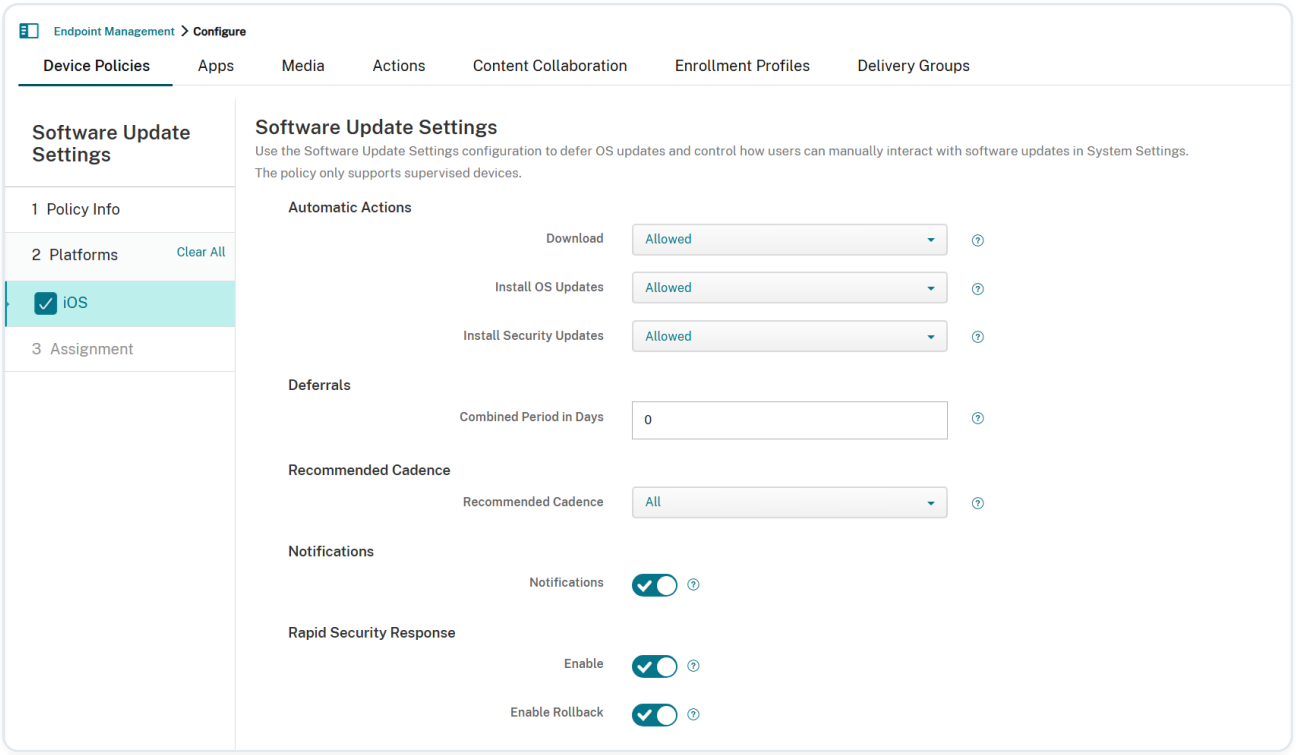
このポリシーを追加または構成するには、 **>** に移動します。詳細については、 デバイスポリシー を参照してください。

前提条件

- CEMのバージョンが**25.5.0**以上であること。
- **iOS 18.0**以降および**iPadOS 18.0**以降で利用可能で、監視対象デバイスのみをサポートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定



- **自動アクション**
  - **ダウンロード:** ユーザーが利用可能なアップデートの自動ダウンロードを制御できるかどうかを指定します。デフォルトは**許可**です。
    - **許可** - ユーザーは自動ダウンロードを有効または無効にできます。
    - **常にオン** - 自動ダウンロードは常に有効になります。
    - **常にオフ** - 自動ダウンロードは常に無効になります。
  - **OSアップデートのインストール:** ユーザーが利用可能なアップデートの自動インストールを制御できるかどうかを指定します。デフォルトは**許可**です。
    - **許可** - ユーザーは自動インストールを有効または無効にできます。
    - **AlwaysOn** - 自動インストールは常に有効です。
    - **AlwaysOff** - 自動インストールは常に無効です。
  - **セキュリティアップデートのインストール:** ユーザーが利用可能なセキュリティアップデートの自動インストールを制御できるかどうかを指定します。デフォルトは**Allowed**です。
    - **Allowed** - ユーザーは自動インストールを有効または無効にできます。
    - **AlwaysOn** - 自動インストールは常に有効です。
    - **AlwaysOff** - 自動インストールは常に無効です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **延期**
  - **合計日数:** デバイスでのメジャーまたはマイナーOSソフトウェアアップデートを延期する日数を指定します。設定すると、ソフトウェアアップデートのリリース後、指定された遅延期間が経過した後にのみソフトウェアアップデートが表示されます。iOS 18以降で利用可能です。有効な値は0～90です。デフォルトは**0**で、これは遅延がないことを意味します。
- **推奨される頻度**
  - **推奨される頻度:** デバイスがユーザーにソフトウェアアップデートを表示する方法を指定します。複数のアップデートが利用可能な場合、デバイスは次のように動作します。デフォルトは**All**です。
    - **All** - すべてのソフトウェアアップデートバージョンを表示します。
    - **Oldest** - 最も古い（番号の小さい）ソフトウェアアップデートバージョンのみを表示します。
    - **Newest** - 最も新しい（番号の大きい）ソフトウェアアップデートバージョンのみを表示します。
- **通知**
  - **通知: On**の場合、デバイスはすべてのソフトウェアアップデート強制通知を表示します。**Off**の場合、デバイスは強制期限の1時間前にトリガーされる通知と、再起動カウントダウン通知のみを表示します。デフォルトは**On**です。
- **迅速なセキュリティ対応**
  - **有効にする: オフ**の場合、ユーザーによるインストール向けに迅速なセキュリティ対応は提供されません。システムは、`com.apple.configuration.softwareupdate.enforcement.specific`構成で迅速なセキュリティ対応をインストールできます。**オン**の場合、システムはユーザーに迅速なセキュリティ対応を提供します。デフォルトは**オン**です。
  - **ロールバックを有効にする: オフ**の場合、システムはユーザーに迅速なセキュリティ対応のロールバックを提供しません。**オン**の場合、システムはユーザーに迅速なセキュリティ対応のロールバックを提供します。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステータスサブスクリプションデバイスポリシー

ステータスサブスクリプションデバイスポリシーを使用すると、オペレーティングシステムのバージョン/ビルド、バッテリーの状態、ソフトウェア更新ステータスなどのプロパティを含む、デバイスのステータスサブスクリプションを構成できます。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、 デバイスポリシー を参照してください。

前提条件

- CEMのバージョンが**25.5.0**以上であること。

iOS設定

](/en-us/citrix-endpoint-management/media/status-subscriptions-ios-settings1.png)

- **デバイスプロパティ**
  - **システムバージョン: オン**の場合、デバイスはオペレーティングシステムのバージョン（例：18.0）を報告し、これはデバイスプロパティのシステム情報セクションに表示されます。バージョンアップグレードが発生したときにデバイスが自動的に報告するため、これは便利です。デフォルトは**オン**です。iOS 15以降で利用可能です。
  - **システムビルド: オン**の場合、デバイスはオペレーティングシステムのビルドバージョン（例：18F132）を報告し、これはデバイスプロパティのシステム情報セクションに表示されます。バージョンアップグレードが発生したときにデバイスが自動的に報告するため、これは便利です。デフォルトは**オン**です。iOS 15以降で利用可能です。
  - **バッテリーの状態: オン**の場合、新しい設定**バッテリーの状態**がデバイスプロパティに追加されます。この設定により、管理者は** > > > > ** に移動して、登録済みiOSデバイスのバッテリーの状態を表示できます。デフォルトは**オン**です。iOS 17以降で利用可能です。
- **ソフトウェアアップデート**
  - **失敗理由: オン**の場合、デバイスはOSアップデートの失敗理由を報告し、これはデバイスプロパティのソフトウェアアップデート情報セクションに表示されます。デフォルトは**オフ**です。iOS 17以降で利用可能です。

ユーザーIDデバイスポリシー

ユーザーIDデバイスポリシーを使用すると、iOSデバイスのユーザーIDアセットを構成できます。設定には、ユーザーのメールアドレスと氏名が含まれます。

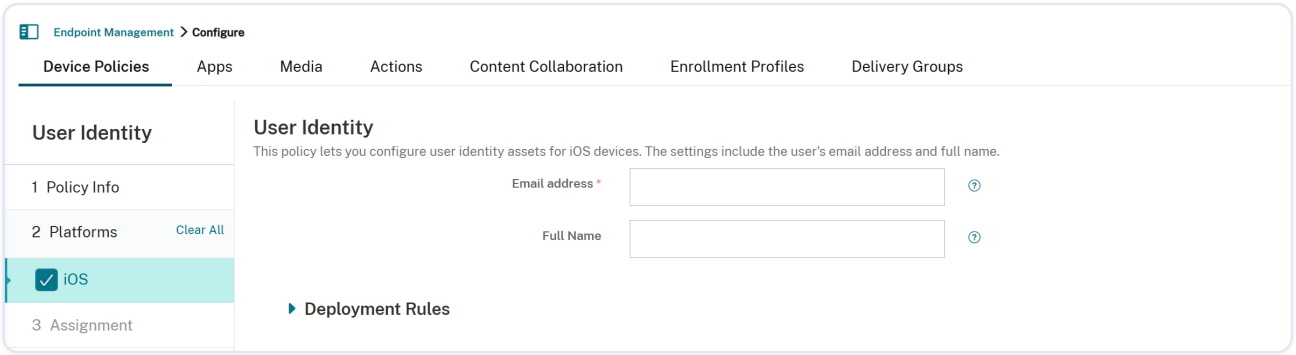
© 1997–2026 Citrix Systems, Inc. All rights reserved.

このポリシーを追加または構成するには、 > に移動します。詳細については、 デバイスポリシー を参照してください。

前提条件

- CEMバージョンが**25.5.0**以上であること。

iOS設定



- **メールアドレス:** ユーザーのメールアドレスを入力します。このフィールドは必須です。
- **氏名:** ユーザーの氏名を入力します。

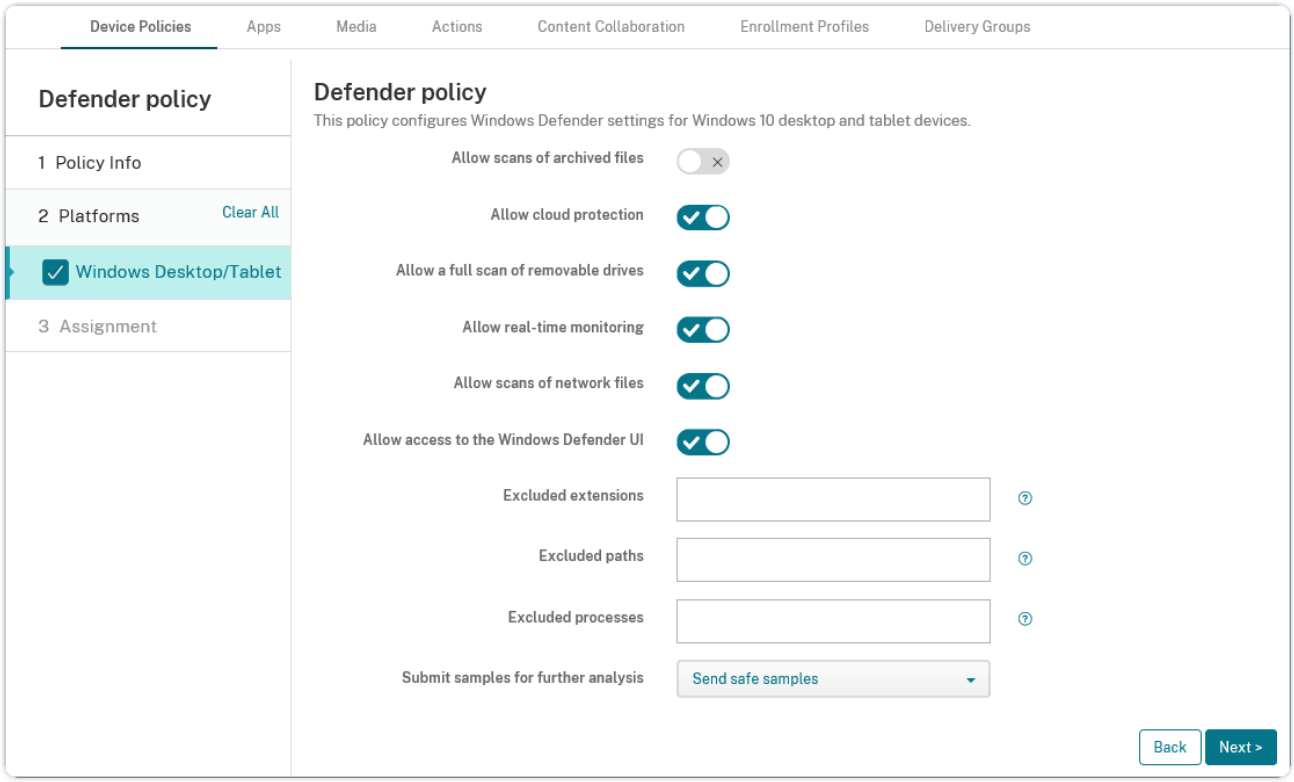
Defenderデバイスポリシー

Windows Defenderは、Windows 10およびWindows 11に付属するマルウェア対策機能です。Citrix Endpoint ManagementデバイスポリシーのDefenderを使用して、Windows 10およびWindows 11のデスクトップおよびタブレットデバイス向けMicrosoft Defenderポリシーを構成できます。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、デバイスポリシーを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windowsデスクトップおよびタブレットの設定



- **アーカイブファイルのスキャンを許可:** Defenderがアーカイブファイルをスキャンすることを許可またはブロックします。既定値は**オフ**です。
- **クラウド保護を許可:** Defenderがマルウェア活動に関する情報をMicrosoftに送信することを許可またはブロックします。既定値は**オン**です。
- **リムーバブルドライブのフルスキャンを許可:** DefenderがUSBスティックなどのリムーバブルドライブをスキャンすることを許可またはブロックします。既定値は**オン**です。
- **リアルタイム監視を許可:** 既定値は**オン**です。
- **ネットワークファイルのスキャンを許可:** Defenderがネットワークファイルをスキャンすることを許可またはブロックします。既定値は**オン**です。
- **Windows Defender UIへのアクセスを許可:** ユーザーがWindows Defenderユーザーインターフェイスにアクセスできるかどうかを指定します。この設定は、ユーザーデバイスが次回起動したときに有効になります。この設定が**オフ**の場合、ユーザーはWindows Defenderの通知を受け取りません。既定値は**オン**です。
- **除外する拡張子:** リアルタイムスキャンまたはスケジュールスキャンから除外する拡張子。拡張子を区切るには、`|`文字を使用します。例: `lib\|obj`。
- **除外するパス:** リアルタイムスキャンまたはスケジュールスキャンから除外するパス。パスを区切るには、`|`文字を使用します。例: `C:\Example|C:\Example1`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **除外するプロセス:** リアルタイムスキャンまたはスケジュールスキャンから除外するプロセス。プロセスを区切るには、`|`文字を使用します。例: `C:\Example.exe|C:\Example1.exe`。
- **詳細分析のためにサンプルを送信:** 悪意のあるファイルであるかどうかを判断するために、さらに分析が必要なファイルをMicrosoftに送信するかどうかを制御します。オプション: **常にプロンプトを表示、安全なサンプルを送信、送信しない、すべてのサンプルを送信**。既定値は**安全なサンプルを送信**です。

Device Guard デバイスポリシー

Device Guard は、Windows 10 および Windows 11 で利用できるセキュリティ機能です。この機能は、**Windows Hypervisor** を使用してデバイス上のセキュリティサービスをサポートすることで、仮想化ベースのセキュリティを有効にします。Device Guard ポリシーは、セキュアブート、UEFI ロック、仮想化などのセキュリティ機能を有効にします。

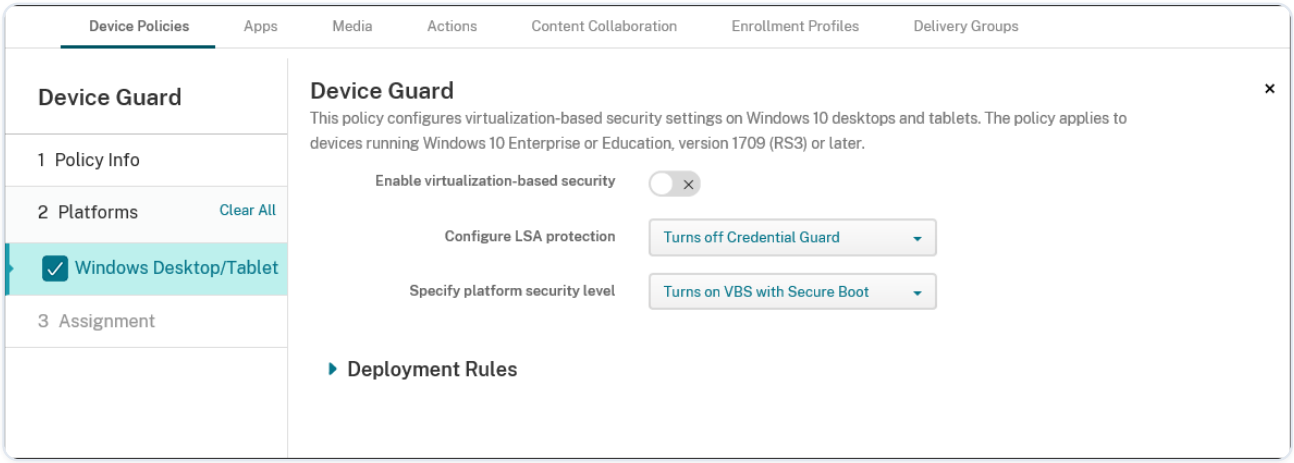
前提条件

- Windows 10 および Windows 11 デスクトップおよびタブレット (Enterprise または Education ライセンスを持つ)
- Windows で Device Guard が有効になっていること

  Device Guard の詳細については、`<https://docs.microsoft.com/ja-jp/windows/access-protection/credential-guard/credential-guard-manage>` を参照してください。

このポリシーを追加または構成するには、**Configure > Device Policies** に移動します。詳細については、デバイスポリシー を参照してください。

Windows デスクトップおよびタブレットの設定



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **仮想化ベースのセキュリティを有効にする:** 仮想化ベースのセキュリティ機能を無効または有効にします。仮想化ベースのセキュリティは、Windows Hypervisor を使用してセキュリティサービスをサポートします。
- **LSA 保護を構成する:** Credential Guard を構成できます。この設定により、ユーザーは仮想化ベースのセキュリティで Credential Guard を有効にし、次回の再起動時に資格情報を保護できます。オプションは、**Credential Guard をオフにする**、**UEFI ロックで Credential Guard をオンにする**、および **UEFI ロックなしで Credential Guard をオンにする** です。デフォルトは **Credential Guard をオフにする** です。
- **プラットフォームセキュリティレベルを指定する:** 次回の再起動時にプラットフォームセキュリティレベルを指定できます。オプションは、**セキュアブートで VBS をオンにする** および **セキュアブートとダイレクトメモリアクセスで VBS をオンにする** です。デフォルトは **セキュアブートで VBS をオンにする** です。

Citrix Endpoint Management は、仮想化ベースのセキュリティ設定がサーバー上の設定と一致するかどうかを判断するためにデバイスを照会します。セキュリティ設定が一致する場合、Citrix Endpoint Management はこのポリシーをデバイスに展開しません。セキュリティ設定が一致しない場合、Citrix Endpoint Management はポリシーを展開します。

デバイス正常性構成証明デバイスポリシー

Citrix Endpoint Management では、Windows 10 および Windows 11 デバイスにその正常性の状態を報告させることができます。正常性の状態を報告するために、デバイスは特定のデータとランタイム情報を Health Attestation Service (HAS) に送信して分析します。HAS は、デバイスが Citrix Endpoint Management に送信する Health Attestation Certificate を作成して返します。Citrix Endpoint Management は、Health Attestation Certificate の内容を使用して、設定した自動アクションを展開します。

HAS によって検証されるデータは次のとおりです。

- AIK プレゼンス
- BitLocker の状態
- ブートデバッグが有効
- ブートマネージャー改訂リストバージョン
- コード整合性が有効
- コード整合性改訂リストバージョン
- Apple 展開プログラムポリシー
- ELAM ドライバーがロード済み

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 発行日時
- カーネルデバッグが有効
- PCR
- リセット回数
- 再起動回数
- セーフモード有効
- SBCPハッシュ
- セキュアブート有効
- テスト署名有効
- VSM有効
- WinPE有効

詳細については、Microsoft のDevice HealthAttestation CSPページを参照してください。

DHAは、Microsoft CloudまたはオンプレミスのWindows DHAサーバーを使用して、次のように構成できます。

- Microsoft Cloudを使用してDHAを構成するには：デバイス正常性構成証明ポリシーを追加し、この記事で説明されているとおりに構成します。
- オンプレミスのWindows DHAサーバーを使用してDHAを構成するには：DHAサーバーを構成します。次に、デバイス正常性構成証明ポリシーを追加し、この記事で説明されているとおりに構成します。

  DHAサーバーを構成するには、Windows Server 2016 Technical Preview 5以降を実行しているマシンにDHAサーバーの役割をインストールします。手順については、「オンプレミスのデバイス正常性構成証明サーバーを構成する」を参照してください。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、「デバイスポリシー」を参照してください。

Windowsデスクトップ/タブレット設定

Microsoft Cloudを使用してDHAを構成する場合

- **デバイス正常性構成証明を有効にする:** デバイス正常性構成証明を必須にするかどうかを選択します。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

オンプレミスのWindows DHAサーバーを使用してDHAを構成する場合

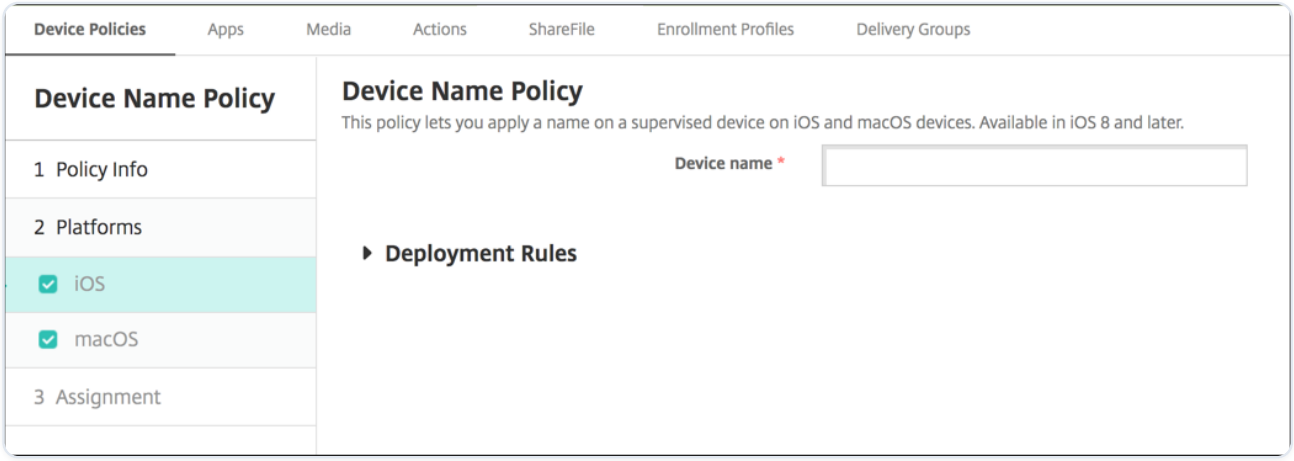
- **デバイス正常性構成証明を有効にする:** オンに設定します。
- **オンプレミス正常性構成証明サービスを構成する:** オンに設定します。
- **オンプレミスDHAサービスFQDN:** 設定したDHAサーバーの完全修飾ドメイン名を入力します。
- **オンプレミスDHA APIバージョン:** DHAサーバーにインストールされているDHAサービスのバージョンを選択します。

デバイス名デバイスポリシー

監視対象のiOSおよびmacOSデバイスに名前を設定して、デバイスを簡単に識別できるようにすることができます。デバイス名を定義するには、マクロ、テキスト、またはその両方の組み合わせを使用できます。たとえば、デバイス名をデバイスのシリアル番号として設定するには、${device.serialnumber}を使用できます。デバイス名をユーザー名とドメインの組み合わせとして設定するには、${user.username}@example.comを使用できます。マクロの詳細については、「Citrix Endpoint Managementのマクロ」を参照してください。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOSおよびmacOSの設定



- **デバイス名:** 各デバイスに一意の名前を付けるには、マクロ、マクロの組み合わせ、またはマクロとテキストの組み合わせを入力します。たとえば、${device.serialnumber}を使用してデバイス名を各デバイスのシリアル番号に設定したり、${device.serialnumber} ${ user.username } を使用してユーザーのApple IDをデバイス名に含めたりします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

教育構成デバイスポリシー

教育構成デバイスポリシーは以下を定義します。

- インストラクターデバイス用のApple Classroomアプリ設定。
- インストラクターデバイスと生徒デバイス間のクライアント認証に使用される証明書。

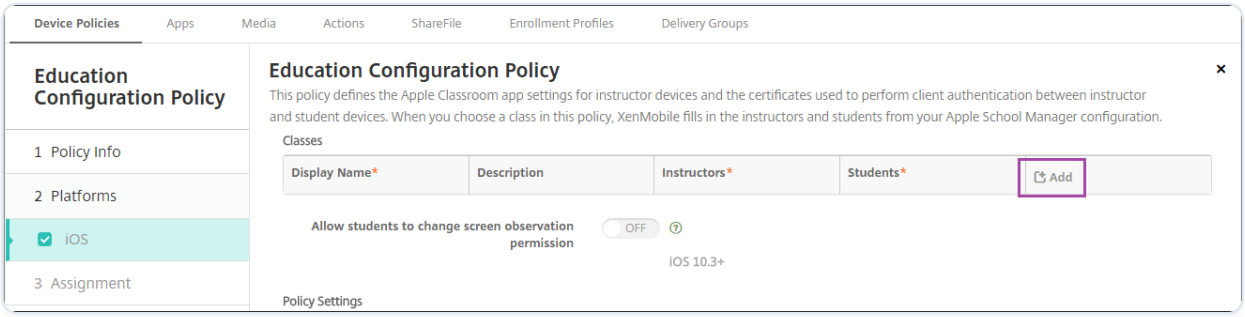
教育構成デバイスポリシーは、iOS (iPadOS) デバイスでサポートされています。

このポリシーでクラスを選択すると、Citrix Endpoint Managementコンソールは、Apple School Manager構成からインストラクターと生徒を自動入力します。このポリシーのApple Classroomアプリ設定がすべてのクラスで同じである場合は、1つのポリシーを作成します。

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］** の順に移動します。詳しくは、「デバイスポリシー」を参照してください。

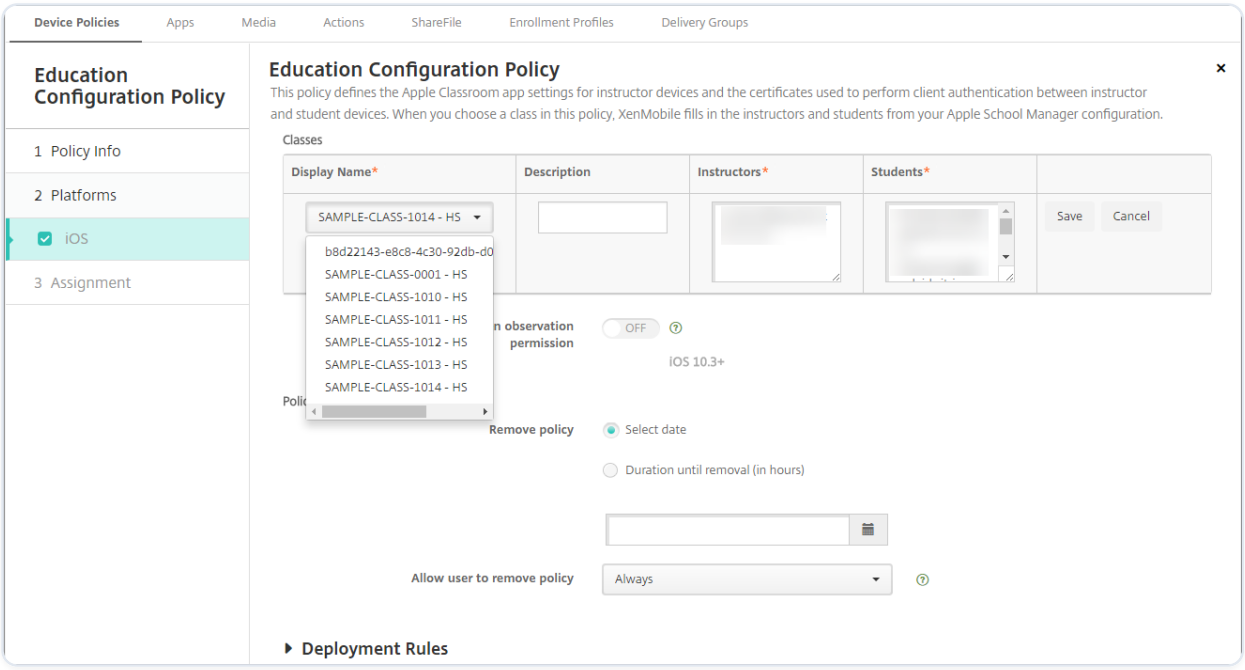
iOS設定

- **クラス：** クラスを追加するには、**［追加］** をクリックします。

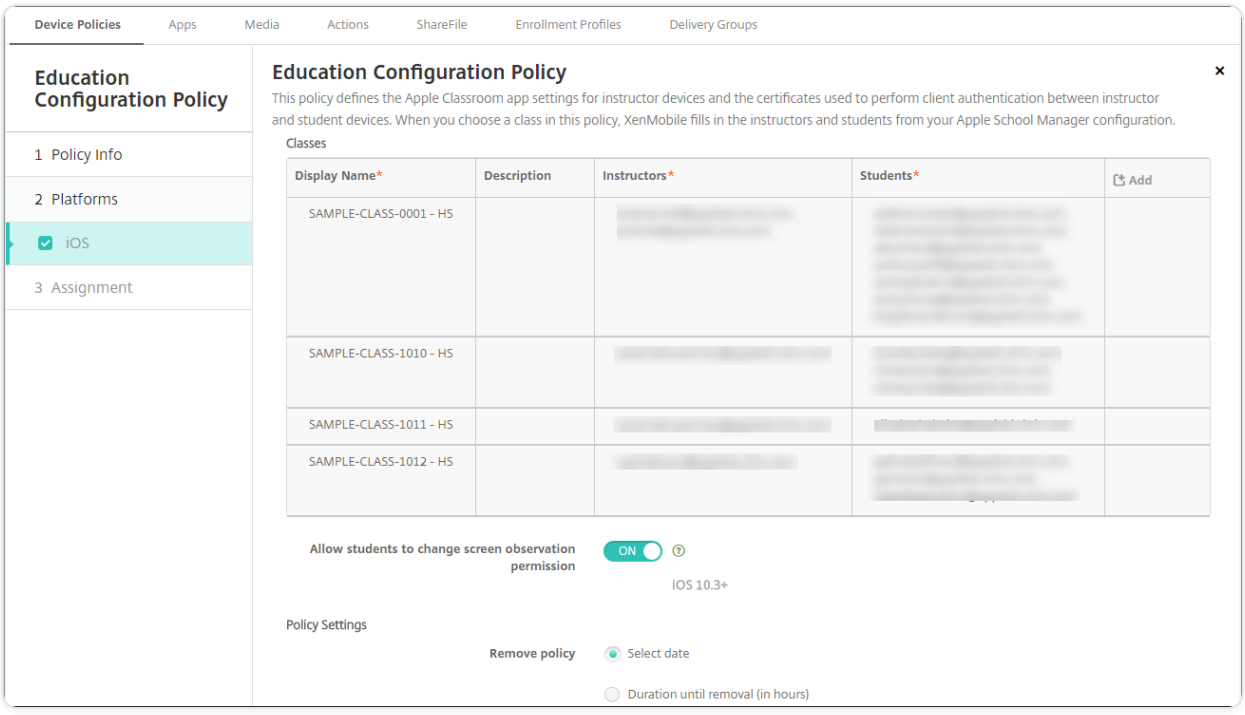


次に、**［表示名］** リストをクリックします。接続されているApple School Managerアカウントから取得されたクラスのリストが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



［**表示名**］ からクラスを選択すると、Citrix Endpoint Managementはインストラクターと生徒を自動入力します。引き続きクラスを追加します。



- **生徒による画面監視権限の変更を許可：** ［**オン**］ の場合、管理対象クラスに登録されている生徒は、教師が自分のデバイス画面を監視することを許可するかどうかを選択できます。デフォルトは**［オフ］**です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択** と **削除までの期間 (時間)** です。

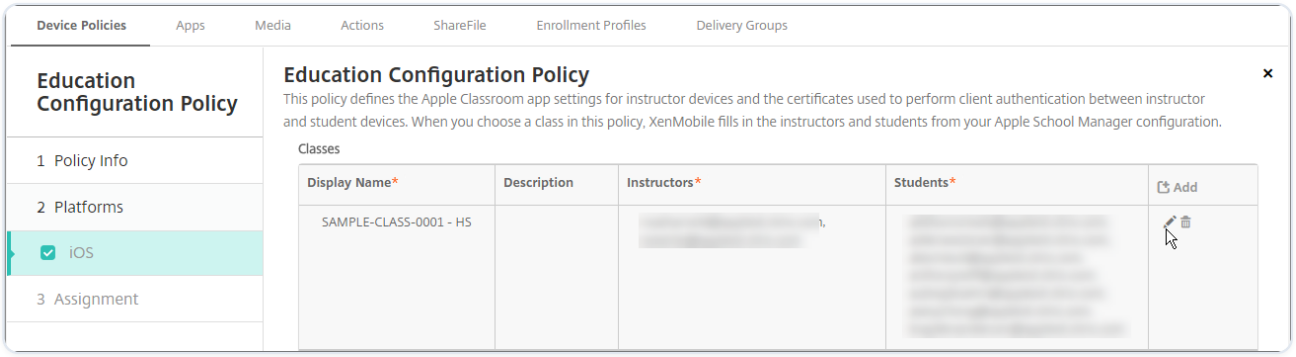
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
- **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。

ポリシー内のクラス情報を編集するには

クラスに説明を追加できます (Classroom アプリの「Display name」)。また、教員や生徒を追加または削除することもできます。Citrix Endpoint Management は、これらの変更を Apple School Manager アカウントに保存しません。詳細については、「Apple Education 機能との統合」の「教員、生徒、およびクラスデータの管理」を参照してください。

編集したいクラスの **Add** 列にマウスオーバーし、鉛筆アイコンをクリックします。



ポリシーからクラスを削除するには、削除したいクラスの **Add** 列にマウスオーバーし、ゴミ箱アイコンをクリックします。

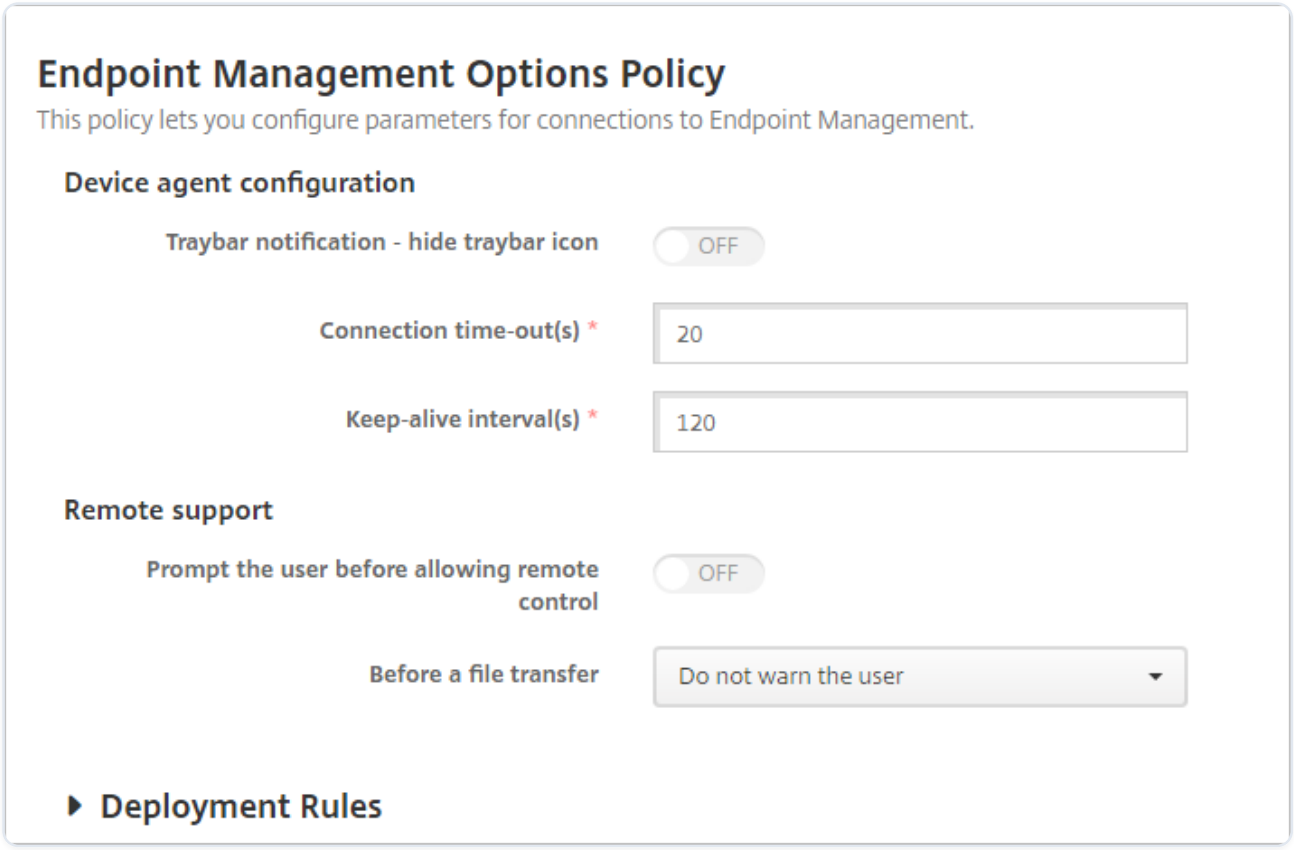
Endpoint Managementオプションデバイスポリシー

AndroidデバイスからCitrix Endpoint Managementに接続する際のCitrix Secure Hubの動作を構成するために、Endpoint Managementオプションポリシーを追加します。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、デバイスポリシーを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

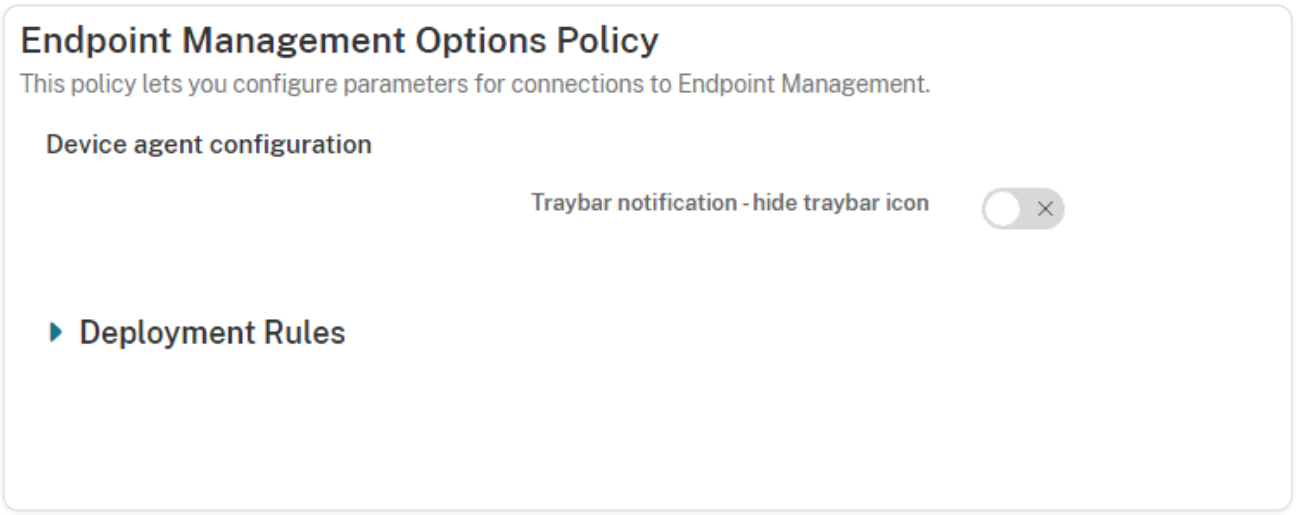
Android設定



- **トレイバー通知 - トレイバーアイコンを非表示にする:** トレイバーアイコンを非表示にするか表示するかを選択します。デフォルトは**オフ**です。
- **接続: タイムアウト:** 接続がタイムアウトするまでにアイドル状態を維持できる時間を秒単位で入力します。デフォルトは20秒です。
- **キープアライブ間隔:** 接続を開いたままにする時間を秒単位で入力します。デフォルトは120秒です。
- **リモートコントロールを許可する前にユーザーにプロンプトを表示する:** リモートサポートコントロールを許可する前にユーザーにプロンプトを表示するかどうかを選択します。デフォルトは**オフ**です。
- **ファイル転送前:** ドロップダウンリストで、ファイル転送についてユーザーに警告するか、ユーザーに許可を求めるかをクリックします。利用可能な値: **ユーザーに警告しない**、**ユーザーに警告する**、**ユーザーの許可を求める**。デフォルトは**ユーザーに警告しない**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アンドロイド エンタープライズ 設定



Androidバージョン7以降でサポートされています。

トレイバー通知 - トレイバーアイコンを非表示にする: トレイバーアイコンを非表示にするか表示するかを選択します。デフォルトは**オフ**です。

注:

Android Enterpriseで動作するデバイス向けにVPNサービスを有効にする場合は、**VPNデバイスポリシー**で**Enable Always-On VPN**オプションを有効にできます。以前のバージョンで**Endpoint Management Optionsデバイスポリシー**の**Enable Always-On VPN**オプションをすでに有効にしている場合は、**VPNデバイスポリシー**で再度有効にしてください。

Citrix Endpoint Management アンインストールデバイスポリシー

Citrix Endpoint Managementで、AndroidデバイスからCitrix Endpoint Managementをアンインストールするデバイスポリシーを追加できます。展開すると、このポリシーは展開グループ内のすべてのデバイスからCitrix Endpoint Managementを削除します。

このポリシーを追加または構成するには、**「構成」>「デバイスポリシー」**の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android設定

- **デバイスからCitrix Endpoint Managementをアンインストールする：** このポリシーを展開するすべてのデバイスからCitrix Endpoint Managementをアンインストールするかどうかを選択します。デフォルトは**「オフ」**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

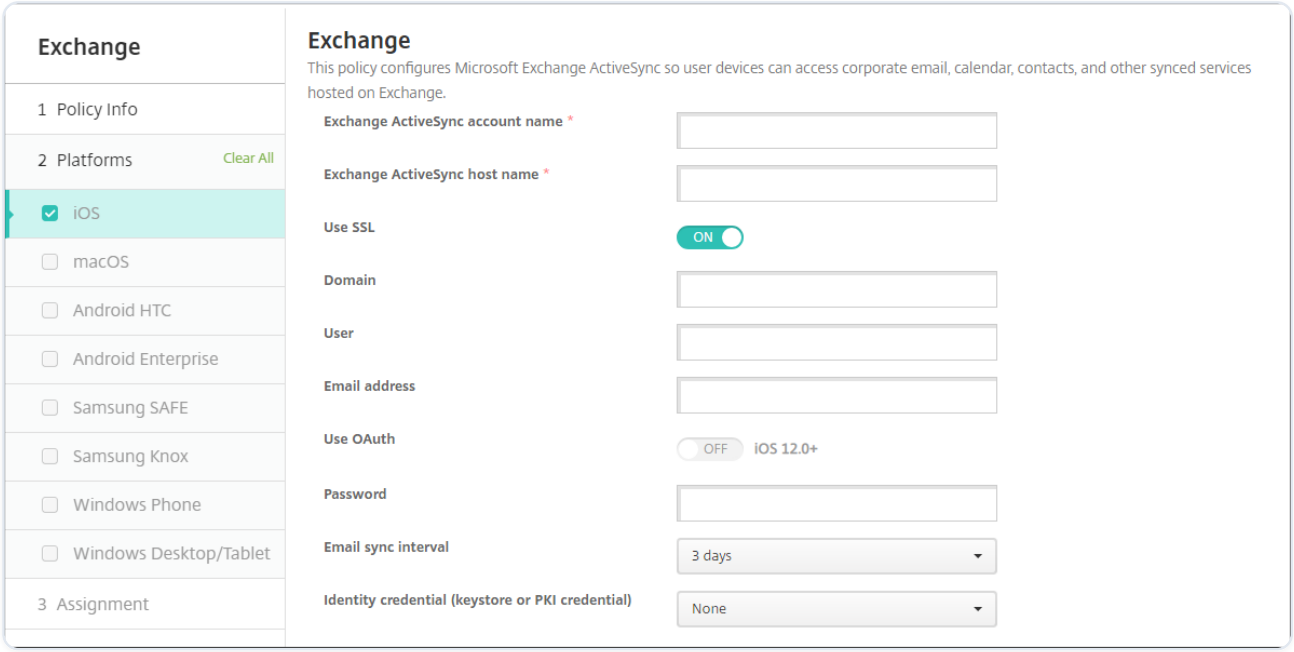
Exchangeデバイスポリシー

Exchange ActiveSyncデバイスポリシーを使用して、ユーザーデバイス上のメールクライアントを構成し、Exchangeでホストされている会社のメールにアクセスできるようにすることができます。各プラットフォームには異なる値のセットが必要であり、これについては以下のセクションで詳しく説明します。

このポリシーを作成するには、Exchange Serverのホスト名またはIPアドレスが必要です。ActiveSync設定の詳細については、Microsoftの記事「ActiveSync CSP」を参照してください。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定



- **Exchange ActiveSyncアカウント名:** ユーザーデバイスに表示されるメールアカウントの説明を入力します。
- **Exchange ActiveSyncホスト名:** メールサーバーのアドレスを入力します。
- **SSLを使用:** ユーザーデバイスとExchange Server間の接続を保護するかどうかを選択します。デフォルトは**オン**です。
- **ドメイン:** Exchange Serverが存在するドメインを入力します。このフィールドでシステムマクロ`$user.domainname`を使用すると、ユーザーのドメイン名を自動的に検索できます。
- **ユーザー:** Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ`$user.username`を使用すると、ユーザー名を自動的に検索できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **メールアドレス:** 完全なメールアドレスを指定します。このフィールドでシステムマクロ `$user.mail` を使用すると、ユーザーのメールアカウントを自動的に検索できます。
- **OAuthを使用: オン**に設定すると、接続は認証にOAuthを使用します。デフォルトは**オフ**です。このオプションはiOS 12.0以降に適用されます。
- **パスワード:** Exchangeユーザーアカウントのオプションのパスワードを入力します。この設定は、 が**オン**の場合には表示されません。
- **メール同期間隔:** リストから、メールがExchange Serverと同期される頻度を選択します。デフォルトは**3日**です。
- **識別情報資格情報 (キーストアまたはPKI):** Citrix Endpoint Management 用にIDプロバイダーを構成している場合は、ドロップダウンリストからオプションの識別情報資格情報をクリックします。このフィールドは、Exchange がクライアント証明書認証を要求する場合にのみ必要です。デフォルトは **None** です。
- **アカウント間のメール移動を許可する:** ユーザーに以下を許可するかどうかを選択します。
  - このアカウントから別のメールアカウントにメールを移動する
  - 別のメールアカウントからメールを転送する
  - 別のメールアカウントから返信する。

  デフォルトは **Off** です。
- **メールアプリからのみメールを送信する:** ユーザーがメール送信にiOSメールアプリのみを使用するように制限するかどうかを選択します。デフォルトは **Off** です。
- **ユーザーが最近のアドレスを同期するのを防ぐ:** ユーザーが最近のアドレスを同期するのを防ぐかどうかを選択します。デフォルトは **Off** です。
- **Mail Dropを許可する:** アカウントがMail Dropを使用することを許可するかどうかを選択します。デフォルトは **Off** です。
- **S/MIME署名を有効にする:** このアカウントがS/MIME署名をサポートするかどうかを選択します。デフォルトは **On** です。**On** に設定すると、以下のフィールドが表示されます。
  - **署名識別情報資格情報:** 使用する署名資格情報を選択します。
  - **ユーザーはS/MIME署名を上書きできる: On** に設定すると、ユーザーはデバイスの設定でS/MIME署名をオン/オフできます。デフォルトは **Off** です。このオプションはiOS 12.0以降に適用されます。
  - **ユーザーはS/MIME署名証明書UUIDを上書きできる: On** に設定すると、ユーザーはデバイスの設定で、使用する署名資格情報を選択できます。デフォルトは **Off** です。このオプションはiOS 12.0以降に適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **S/MIME暗号化を有効にする:** このアカウントがS/MIME暗号化をサポートするかどうかを選択します。デフォルトは **Off** です。**On** に設定すると、以下のフィールドが表示されます。
  - **暗号化識別情報資格情報:** 使用する暗号化資格情報を選択します。
  - **メッセージごとのS/MIMEスイッチを有効にする: オン**に設定すると、ユーザーが作成する各メッセージのS/MIME暗号化をオンまたはオフに切り替えるオプションが表示されます。デフォルトは**オフ**です。
  - **ユーザーはS/MIME暗号化を上書きできます: オン**に設定すると、ユーザーはデバイスの設定でS/MIMEをデフォルトでオンにするかどうかを選択できます。デフォルトは**オフ**です。このオプションはiOS 12.0以降に適用されます。
  - **ユーザーはS/MIME暗号化証明書UUIDを上書きできます: オン**に設定すると、ユーザーはデバイスの設定でS/MIME暗号化IDと暗号化をオン/オフに切り替えることができます。デフォルトは**オフ**です。このオプションはiOS 12.0以降に適用されます。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは**日付を選択**と**削除までの期間（時間）**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を時間単位で入力します。

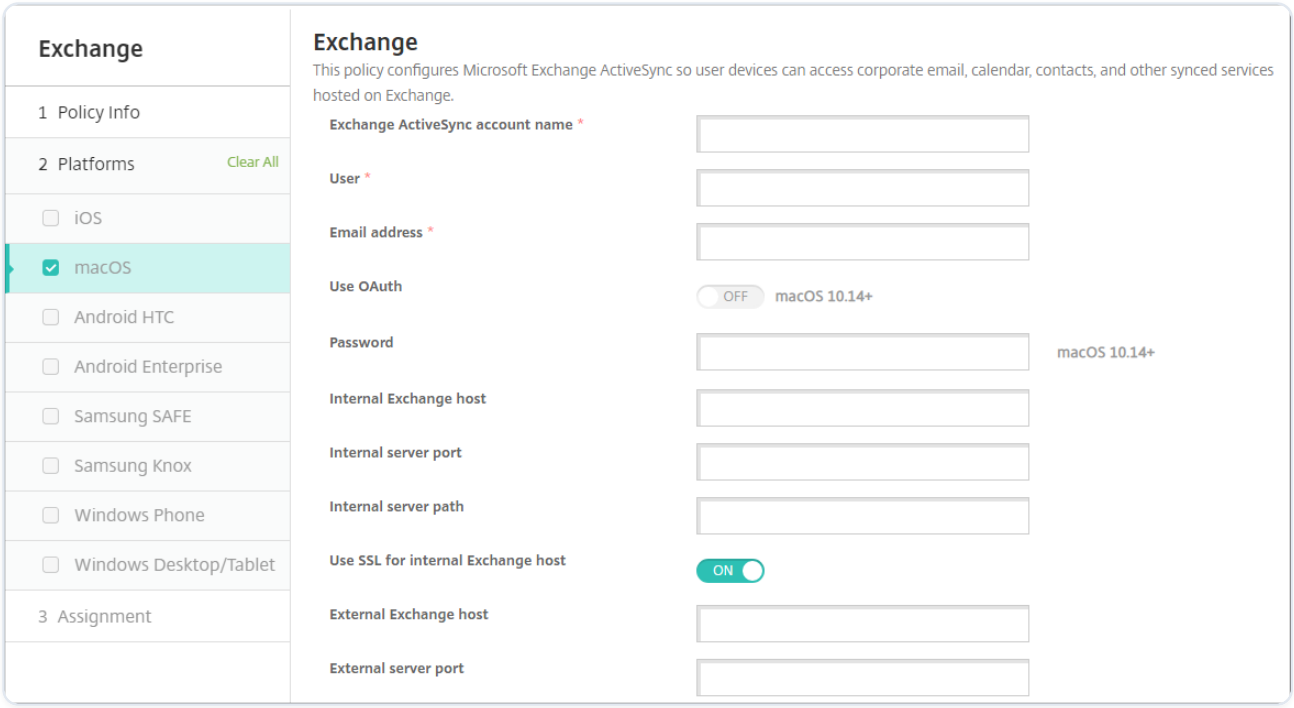
同期されたExchangeサービス

同期されたExchangeサービスの各設定では、以下の機能を同期するかどうかを選択できます。

- カレンダー
- 連絡先
- メール
- メモ
- リマインダー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS設定



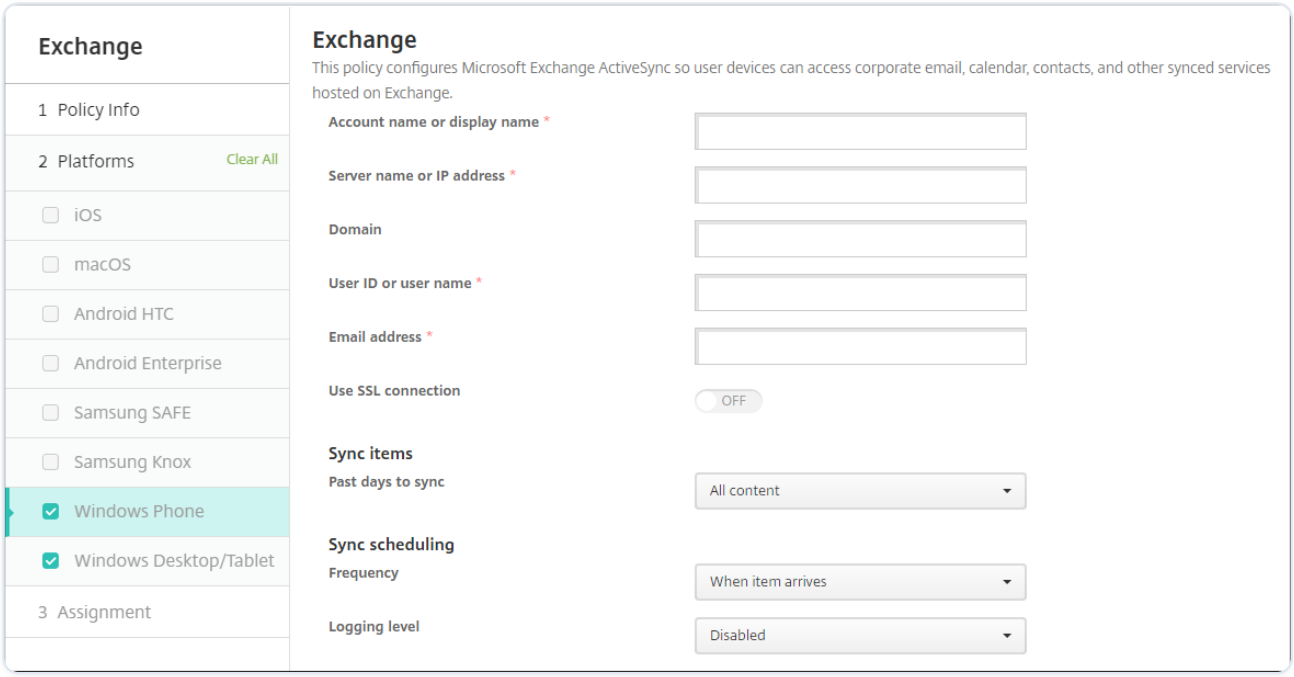
- **Exchange ActiveSyncアカウント名:** ユーザーデバイスに表示されるメールアカウントの説明を入力します。
- **ユーザー:** Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ `$user.username` を使用して、ユーザー名を自動的に検索できます。
- **メールアドレス:** 完全なメールアドレスを指定します。このフィールドでシステムマクロ `$user.mail` を使用して、ユーザーのメールアカウントを自動的に検索できます。
- **OAuthを使用: オン**に設定されている場合、接続は認証にOAuthを使用します。デフォルトは**オフ**です。このオプションはmacOS 10.14以降に適用されます。
- **OAuthサインインURL:** AutoDiscoveryサービスを使用しない場合に、OAuthを使用して認証するためにウェブビューにロードするURLを指定します。このフィールドは、**OAuthを使用**が**オン**に設定されている場合に表示されます。
- **パスワード:** Exchangeユーザーアカウントのオプションのパスワードを入力します。この設定は、**OAuthを使用**が**オン**の場合には表示されません。
- **内部Exchangeホスト:** 内部と外部のExchangeホスト名を異なるものにする場合は、オプションの内部Exchangeホスト名を入力します。
- **内部サーバーポート:** 内部と外部のExchangeサーバーポートを異なるものにする場合は、オプションの内部Exchangeサーバーポート番号を入力します。
- **内部サーバーパス:** 内部と外部のExchangeサーバーパスを異なるものにする場合は、オプションの内部Exchangeサーバーパスを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **内部ExchangeホストにSSLを使用:** ユーザーデバイスと内部Exchangeホスト間の接続を保護するかどうかを選択します。デフォルトは**オン**です。
- **外部Exchangeホスト:** 内部と外部のExchangeホスト名を異なるものにする場合は、オプションの外部Exchangeホスト名を入力します。
- **外部サーバーポート:** 内部と外部のExchangeサーバーポートを異なるものにする場合は、オプションの外部Exchangeサーバーポート番号を入力します。
- **外部サーバーパス:** 内部と外部のExchangeサーバーパスを異なるものにする場合は、オプションの外部Exchangeサーバーパスを入力します。
- **外部ExchangeホストにSSLを使用:** ユーザーデバイスと内部Exchangeホスト間の接続を保護するかどうかを選択します。デフォルトは**オン**です。
- **Mail Dropを許可:** 既存のネットワークに接続することなく、ユーザーが2台のMac間でファイルをワイヤレスで共有することを許可するかどうかを選択します。デフォルトは**オフ**です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**しない**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windowsデスクトップ/タブレット設定



注：

このポリシーでは、ユーザーパスワードを設定できません。ユーザーは、ポリシーをプッシュした後、自分のデバイスからそのパラメーターを設定する必要があります。

- **アカウント名または表示名:** Exchange ActiveSyncアカウント名を入力します。
- **サーバー名またはIPアドレス:** Exchange Serverのホスト名またはIPアドレスを入力します。
- **ドメイン:** Exchange Serverが存在するドメインを入力します。このフィールドでシステムマクロ`$user.domainname`を使用すると、ユーザーのドメイン名を自動的に検索できます。
- **ユーザーIDまたはユーザー名:** Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ`$user.username`を使用すると、ユーザー名を自動的に検索できます。
- **メールアドレス:** 完全なメールアドレスを指定します。このフィールドでは、システムマクロ`$user.mail`を使用して、ユーザーのメールアカウントを自動的に検索できます。
- **SSL接続を使用:** ユーザーデバイスとExchange Server間の接続を保護するかどうかを選択します。デフォルトは**オフ**です。
- **同期する過去の日数:** リストで、デバイス上のすべてのコンテンツをExchange Serverと同期する過去の日数を選択します。デフォルトは**すべてのコンテンツ**です。
- **頻度:** ドロップダウンリストで、Exchange Serverからデバイスに送信されるデータを同期するときに使用するスケジュールをクリックします。デフォルトは**アイテム到着時**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ログレベル:** ドロップダウンリストで、Exchangeアクティビティをログに記録する際の詳細レベルを指定するために、**無効**、**基本**、または**詳細**をクリックします。デフォルトは**無効**です。

ファイルデバイスポリシー

ユーザーがAndroidおよびAndroid Enterpriseデバイスでアクセスできるようにファイルを追加および展開できます。ファイルをデバイスに保存するディレクトリを指定します。たとえば、ユーザーに会社のドキュメントまたは.pdfファイルを配布したい場合などです。ファイルをデバイスに展開し、ファイルの場所をユーザーに知らせます。

Androidデバイスはスクリプトのネイティブ実行をサポートしていません。ユーザーはスクリプトを実行するためにサードパーティ製ソフトウェアが必要です。

このポリシーで追加できるファイルの種類は次のとおりです。

- テキストベースのファイル（.xml、.html、.pyなど）
- ドキュメント、画像、スプレッドシート、プレゼンテーションなどのその他のファイル

このポリシーを追加または構成するには、**「構成」>「デバイスポリシー」**の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

アンドロイド エンタープライズ 設定

- **インポートするファイル：**インポートするファイルを選択するには、［参照］**をクリックしてファイルの場所に移動します。
- **宛先フォルダー：**リストからアップロードしたファイルを保存する場所を選択するか、［新規追加］**を選択してファイルの場所を指定します。アップロードしたファイルを保存する場所を示すには、`%Flash Storage%\`または`%XenMobile Storage%\`マクロを選択します。マクロは、各デバイスの該当する場所に展開されます。
  - `%XenMobile Storage%\`は、内部ストレージディレクトリの`Android/data/com.zenprise/`に展開されます。
  - Android 9.0以前の場合、`%Flash Storage%\`はファイルを外部ストレージディレクトリに保存します。
  - Android 10.0以降の場合、`%Flash Storage%\`はファイルを内部ストレージディレクトリの**Downloads**フォルダーに保存します。
  - Android 11.0以降の場合、Googleがターゲットロケーションへのアクセスに課す制限のため、`%XenMobile Storage%\`は適用されなくなりました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **宛先ファイル名：**オプション。デバイスに展開する前にファイル名を変更する必要がある場合は、ファイル名を入力します。
- **ファイルが存在する場合:** リストから、既存のファイルをコピーするかどうかを選択します。デフォルトは「**異なる場合のみファイルをコピー**」です。

重要:

ファイルデバイスポリシーは、Android Enterpriseでのスクリプトの追加をサポートしなくなりました。既存のポリシーにスクリプトが含まれている場合、そのポリシーを選択するとエラーメッセージが表示され、ポリシーを再追加することで問題を解決できます。

Android設定

- **インポートするファイル:** インポートするファイルを選択するには、「**参照**」をクリックしてファイルの場所に移動します。
- **ファイルの種類:** 「**ファイル**」または「**スクリプト**」のいずれかを選択します。
- **すぐに実行:** 「**スクリプト**」を選択すると、「**すぐに実行**」オプションが表示されます。この設定を有効にしても何も起こりません。ユーザーはスクリプトを手動で実行する必要があります。
- **マクロ式を置換:** スクリプト内のマクロトークン名をデバイスまたはユーザープロパティに置き換えるかどうかを選択します。マクロ構文については、「マクロ」を参照してください。デフォルトは「**オフ**」です。
- **保存先フォルダー:** リストから、アップロードしたファイルを保存する場所を選択するか、「**新規追加**」を選択してファイルの場所を指定します。アップロードしたファイルを保存する場所を示すには、`%Flash Storage%\`または`%XenMobile Storage%\`マクロを選択します。マクロは、各デバイスの該当する場所に展開されます。
  - `%XenMobile Storage%\`は内部ストレージディレクトリの`Android/data/com.zenprise/`に展開されます。
  - Android 9.0以前の場合、`%Flash Storage%\`はファイルを外部ストレージディレクトリに保存します。
  - Android 10.0以降の場合、`%Flash Storage%\`はファイルを内部ストレージディレクトリの「**ダウンロード**」フォルダーに保存します。
  - Android 11.0以降の場合、Googleがターゲットロケーションへのアクセスに課す制限のため、`%XenMobile Storage%\`は適用されなくなりました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **保存先ファイル名:** オプション。デバイスに展開する前にファイル名を変更する必要がある場合は、ファイル名を入力します。
- **ファイルが存在する場合:** リストから、既存のファイルをコピーするかどうかを選択します。デフォルトは「**異なる場合のみファイルをコピー**」です。

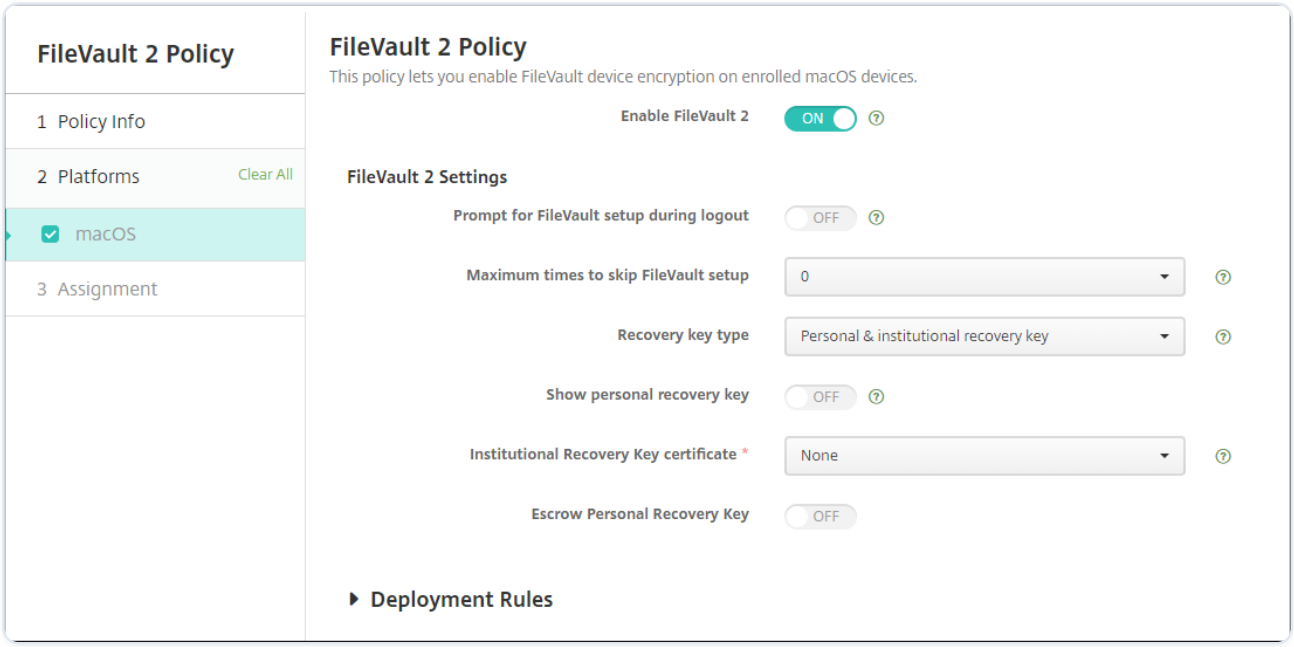
FileVaultデバイスポリシー

macOSのFileVaultフルディスク暗号化（FileVault 2）機能は、システムボリュームのコンテンツを暗号化することで保護します。ユーザーは、デバイスが起動するたびに、アカウントパスワードを使用してFileVaultが有効なmacOSデバイスにログインします。パスワードを忘れた場合、回復キーを使用してディスクのロックを解除し、パスワードをリセットできます。

このデバイスポリシーは、FileVaultのユーザー設定画面を有効にし、回復キーなどの設定を構成します。FileVaultの詳細については、Appleサポートサイトを参照してください。

FileVaultポリシーを追加するには、**Configure > Device Policies**に移動します。

macOS設定



- **FileVaultを有効にする:** この設定が**オン**の場合、**FileVaultセットアップをスキップできる最大回数**オプションで指定された次のN回のログアウト時に、ユーザーにFileVaultを有効にするよう促します。**オフ**の場合、ユーザーはFileVaultを有効にするプロンプトを受け取りませんが、自分でFileVaultを有効にすることはできます。
- **ログアウト時にFileVaultセットアップを促す: オン**の場合、ユーザーはログアウト時にFileVaultを有効にするよう求めるプロンプトを表示されます。

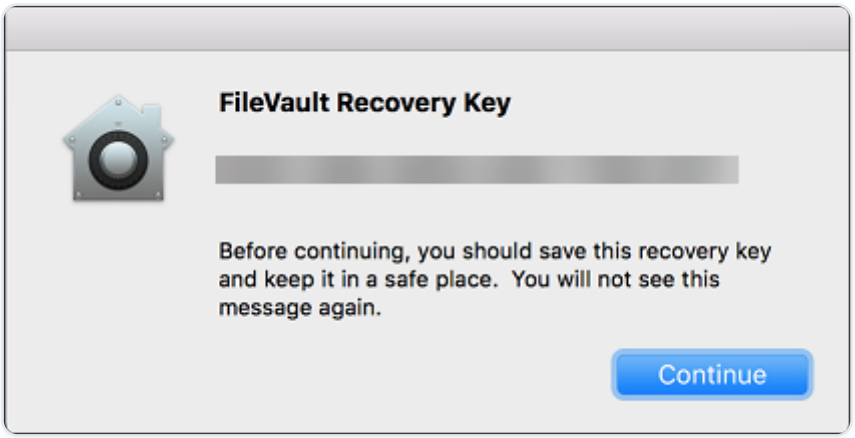
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **FileVaultセットアップをスキップできる最大回数:** ユーザーがFileVaultセットアップをスキップできる最大回数です。ユーザーが最大回数に達すると、ログインするためにFileVaultをセットアップする必要があります。**0**の場合、ユーザーは最初のログイン試行時にFileVaultを有効にする必要があります。デフォルトは**0**です。
- **回復キーの種類:** パスワードを忘れたユーザーは、回復キーを入力してディスクのロックを解除し、パスワードをリセットできます。回復キーのオプション:
  - **個人用回復キー:** 個人用回復キーはユーザー固有のものです。FileVaultのセットアップ中に、ユーザーは回復キーを作成するか、iCloudアカウントでディスクのロックを解除することを許可するかを選択します。FileVaultのセットアップ完了後にユーザーに回復キーを表示するには、**個人用回復キーを表示**を有効にします。キーを表示することで、ユーザーは将来の使用のためにキーを記録できます。ユーザーがキーを紛失した場合にキーを検索できるようにするには、**個人用回復キーをエスクローする**を有効にします。

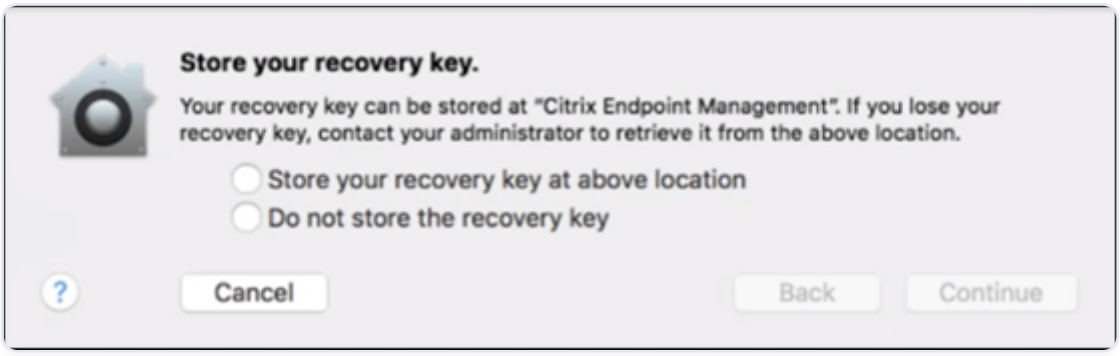
    セキュリティアクションを通じて個人用回復キーをローテーションできます。個人用回復キーのローテーションの詳細については、セキュリティアクションを参照してください。

    回復キー管理の詳細については、Appleサポートサイトを参照してください。
  - **機関用回復キー:** 機関用（またはメイン）回復キーとFileVault証明書を作成し、それを使用してユーザーデバイスのロックを解除できます。詳細については、Appleサポートサイトを参照してください。Citrix Endpoint Managementを使用してFileVault証明書をデバイスに展開します。詳細については、証明書と認証を参照してください。
  - **個人用および機関用回復キー:** 両方の種類の回復キーを有効にすることで、ユーザーが個人用回復キーを紛失した場合にのみ、ユーザーデバイスのロックを解除する必要があります。
- **機関リカバリキー証明書: リカバリキーの種類**として**機関リカバリキー**または**個人および機関リカバリキー**を選択した場合、そのキーのリカバリキー証明書を選択します。
- **個人リカバリキーを表示: オン**の場合、ユーザーデバイスは、FileVault設定後に個人リカバリキーをユーザーに表示します。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



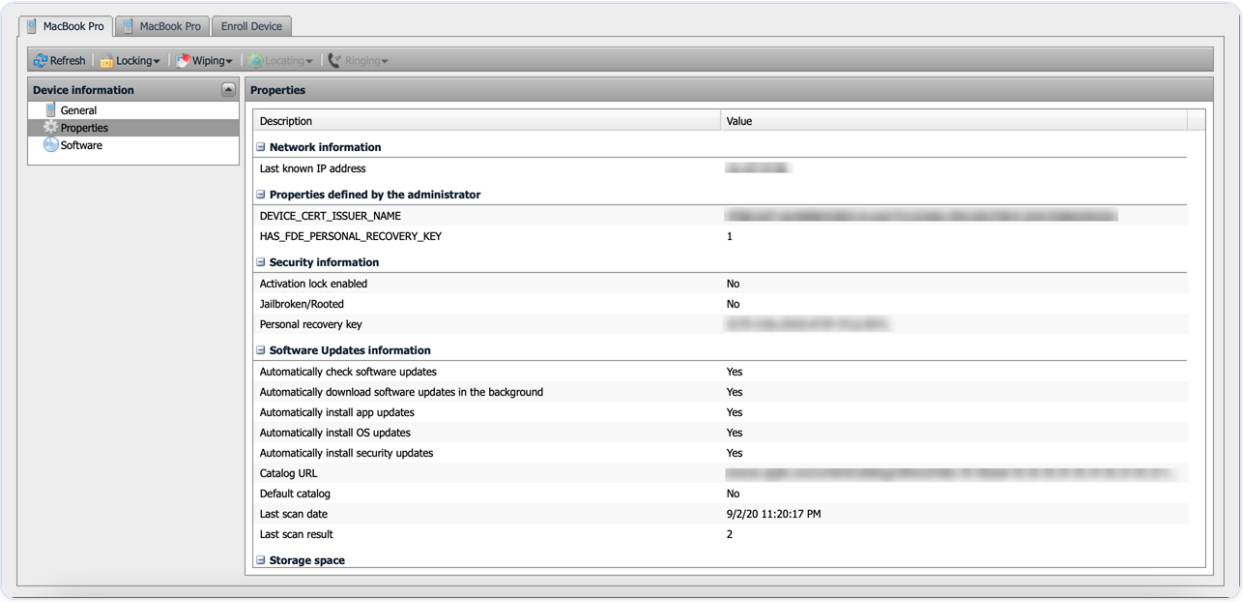
- **個人リカバリキーのエスクロー:** 有効にすると、ユーザーは各デバイスの個人リカバリキーのコピーをCitrix Endpoint Managementに保存できます。



Citrix Endpoint Managementからキーにアクセスするには、**管理 > デバイス**に移動し、macOSデバイスを選択して**編集**をクリックします。次に、**デバイスの詳細 > 全般**に移動し、**個人リカバリキー**を見つけます。

ユーザーがセルフヘルプポータルからリカバリキーを表示できるようにするには、**個人リカバリキーのエスクロー**と**個人リカバリキーをユーザーに表示**を有効にします。キーは、セルフヘルプポータルの**プロパティ**ページの**セキュリティ情報**の下に表示されます。セルフヘルプポータルの詳細については、「セルフヘルプポータル」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



FileVaultを有効にする設定を有効にしない場合でも、**個人リカバリキーのエスクロー**設定を有効にできます。**FileVaultを有効にする**設定を無効にした場合でも、ユーザーは自分でFileVaultを有効にできます。この状況では、ユーザーがキーのコピーをCitrix Endpoint Managementに保存できるように、**個人リカバリキーのエスクロー**を有効にします。

ユーザーがCitrix Endpoint Managementにデバイスを登録する前にFileVaultを有効にした場合、Citrix Endpoint Managementはリカバリキーを保存しません。デバイスはコンソールでFileVaultが有効になっていると表示されます。

ファイアウォールデバイスポリシー

このポリシーを使用すると、Samsung、macOS、およびWindowsデバイスのファイアウォール設定を構成できます。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

macOS設定

macOS 10.12以降が必要です。

デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/configure-device-policies-macos-firewall.png)

- **ファイアウォールを有効にする**。ファイアウォールを有効にするには、このオプションを に設定します。
- **すべての受信接続をブロックする**。このオプションを に設定すると、基本サービスに必要な接続を除くすべての受信接続がブロックされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ステルスモードを有効にする**。ステルスモードでは、デバイスはPingなどのICMPを使用するテストアプリケーションによるネットワークからのアクセス試行に応答したり、認識したりしません。ステルスモードを有効にするには、このオプションを に設定します。
- **アプリ固有の受信接続設定**。特定のアプリが接続を受信できるようにするには、アプリを追加し、 を に設定します。

Windowsデスクトップおよびタブレットの設定

Windows 10 (バージョン1709以降) またはWindows 11を実行しているWindowsデスクトップおよびタブレットデバイスが必要です。

デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/firewall-device-policy-windows.png)

- **機能の有効化:** このポリシーが展開されているコンピューターの送受信トラフィックを制御します。デフォルトは です。
- **パブリックプロファイル:** コンピューターが空港やコーヒーショップなどの公共の場所で信頼されていないネットワークに接続されている間、Windowsファイアウォールを制御します。デフォルトは です。
- **プライベートプロファイル:** コンピューターがホームネットワークなどの信頼できるネットワークに接続されている間のWindowsファイアウォールを制御します。デフォルトは**オン**です。
- **ドメインプロファイル:** コンピューターが職場などのドメインネットワークに接続されている間のWindowsファイアウォールを制御します。デフォルトは**オン**です。
- **許可されたプログラムのリストにあるものを含め、すべての受信接続をブロックする:** デフォルトは**オフ**です。
- **ファイアウォールが新しいプログラムをブロックしたときにユーザーへの通知を無効にする:** デフォルトは**オフ**です。

フォントデバイスポリシー

Citrix Endpoint Managementでデバイスポリシーを追加して、iOSおよびmacOSデバイスにフォントを追加できます。フォントはTrueType (`.ttf`) またはOpenType (`.oft`) フォントである必要があります。フォントコレクション (`.ttc` または `.otc`) はサポートされていません。

このポリシーを追加または構成するには、**Configure > Device Policies**に移動します。詳細については、「デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定

- **ユーザーに表示される名前:** ユーザーがフォントリストで確認する名前を入力します。
- **フォントファイル:** ユーザーデバイスに追加するフォントファイルを選択するには、**参照**をクリックしてファイルの場所に移動します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。

macOS設定

- **ユーザーに表示される名前:** ユーザーがフォントリストで確認する名前を入力します。
- **フォントファイル:** ユーザーデバイスに追加するフォントファイルを選択するには、**参照**をクリックしてファイルの場所に移動します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから、**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションは、macOS 10.7以降でのみ利用可能です。

ホーム画面レイアウトデバイスポリシー

ホーム画面レイアウトデバイスポリシーを使用すると、監視対象のiOSデバイスのiOSホーム画面のアプリとフォルダのレイアウトを指定できます。

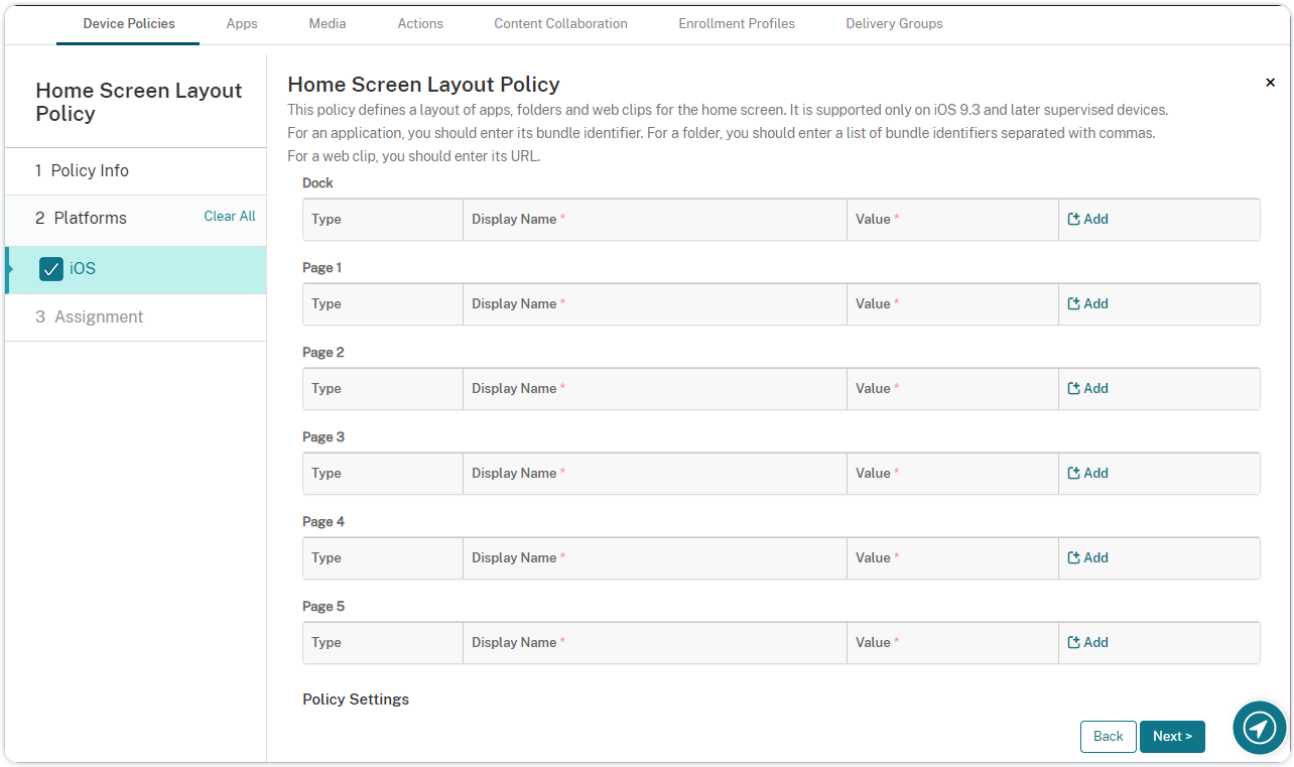
© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

複数のホーム画面レイアウトポリシーをデバイスに展開すると、デバイスでiOSエラーが発生します。この制限は、Citrix Endpoint Managementポリシーを通じてホーム画面を定義する場合でも、Apple Configuratorを通じて定義する場合でも適用されます。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、デバイスポリシーを参照してください。

iOS設定

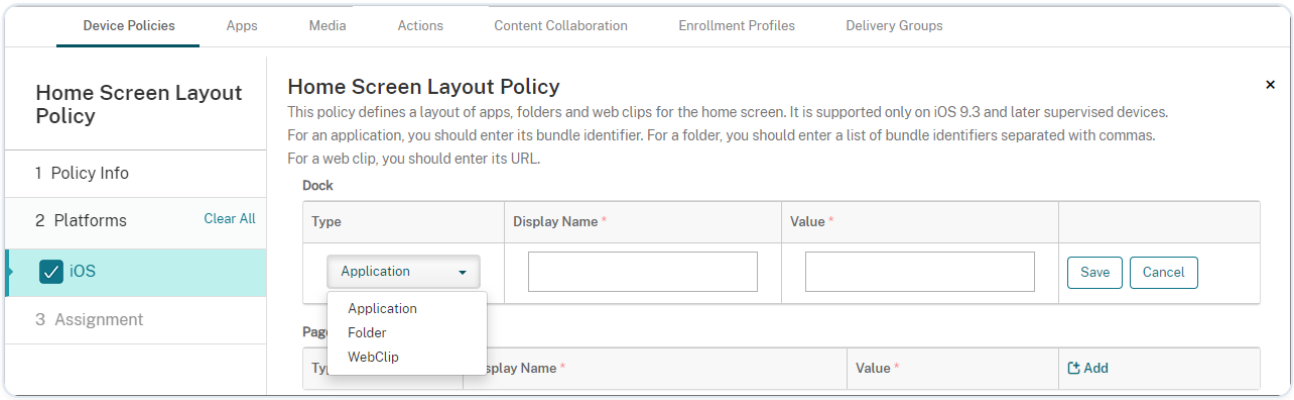


- 構成する画面領域（**Dock**や**Page 1**など）ごとに、**追加**をクリックします。
- **種類: アプリケーション**、**フォルダ**、または**Webクリップ**を選択します。

  制限デバイスポリシーの**制限付きアプリ使用 > 一部のアプリのみを許可**設定により、Webクリップがホーム画面に適切に表示されない場合があります。Webクリップを適切に表示するには、次のいずれかを実行します。

  - **制限付きアプリ使用**を**すべてのアプリを許可**または**一部のアプリを許可しない**に設定します。
  - **制限付きアプリ使用**が**一部のアプリのみを許可**に設定されている場合、Webクリップを許可するには、バンドルID `com.apple.webapp` のアプリを追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **表示名:** アプリまたはフォルダのホーム画面に表示される名前。
- **値:** アプリの場合はバンドル識別子を入力します。フォルダの場合は、コンマで区切られたバンドル識別子のリストを入力します。Webクリップの場合は、バンドルID `com.apple.webClip.managed` を入力し、WebクリップポリシーでWebクリップのURLを構成します。同じURLを持つWebクリップ値が複数存在する場合、iOS 11.3以降のデバイスでは動作が未定義です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間単位)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間単位):** ポリシーが削除されるまでの時間を数値で入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションは、iOS 9.3以降でのみ利用可能です。

iOSおよびmacOSプロファイルデバイスポリシーのインポート

iOSおよびmacOSデバイス用のデバイス構成XMLファイルをCitrix Endpoint Managementにインポートできます。このファイルには、Apple Configurator 2またはProfile Creatorで準備したデバイスセキュリティポリシーと制限が含まれています。構成XMLファイルにはマクロを含めることができます。詳細については、「マクロ」を参照してください。

ユースケース

Profile Creatorを使用してmacOSデバイス向けにCitrix Endpoint Managementの外部で作成された次の構成をインポートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **システムポリシー制御:** このポリシーは、認定されたApple開発者によって署名されたアプリを識別し、ユーザーがMac App Storeから検証済みアプリをダウンロードできるようにします。

  ポリシーを構成する際:

  - ユーザーが検証済みで信頼できるソフトウェアのみを実行するように、**Gatekeeperを有効にする**を選択します。
  - ユーザーが認定されたApple開発者によって署名されたアプリのみをインストールするように、**識別された開発者を許可する**を選択します。

- **プライバシー設定ポリシー制御:** このポリシーを使用すると、位置情報サービス、カメラ、画面キャプチャなど、特定のファイルや機能へのアプリケーション間のアクセスを許可または制限できます。

  展開する予定の設定を構成します。詳細については、「プライバシー設定ポリシー制御ペイロード設定」を参照してください。

- **カーネル拡張ポリシー:** このポリシーを使用すると、ユーザーはオペレーティングシステムのネイティブ機能を拡張するアプリ拡張機能をインストールできます。カーネル拡張機能はカーネルレベルで実行されます。

  展開する予定の設定を構成します。詳細については、「カーネル拡張ポリシーペイロード設定」を参照してください。

- **イーサネット設定ポリシー:** このポリシーを使用すると、イーサネットネットワーク接続を管理できます。

  展開する予定の設定を構成します。詳細については、「イーサネット設定」を参照してください。

Apple Configurator 2またはProfile Creatorのいずれかを使用して、macOSおよびiOSデバイス向けに次のポリシーを構成します。

- **Wi-Fiポリシー:** このポリシーを使用すると、ユーザーがデバイスをWi-Fiネットワークに接続する方法を管理できます。

  ポリシーを構成する場合:

  - ターゲットSSIDを優先順位リストの先頭に追加します。
  - ユーザーがネットワークに参加するときに使用する接続モードを選択します。**システム**を選択した場合、デバイスはシステム資格情報を使用してユーザーを認証します。**ログインウィンドウ**を選択した場合、デバイスはログインウィンドウで入力されたのと同じ資格情報を使用してユーザーを認証します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

詳細については、Wi-Fi設定を参照してください。

- **制限ポリシー:** このポリシーは、ユーザーデバイスでの特定の機能の使用を許可または制限します。

  展開する設定を構成します。詳細については、制限の概要を参照してください。

- **VPNポリシー:** このポリシーは、プライベートネットワークへのデバイスレベルの暗号化された接続を提供します。

  展開する設定を構成します。詳細については、VPNの概要を参照してください。

Apple Configurator 2を使用して構成プロファイルを作成する

1. Apple App StoreからApple Configurator 2をインストールします。
2. Apple Configurator 2を起動し、**ファイル > 新規プロファイル**に移動します。新しい構成ウィンドウが表示されます。
3. **一般**設定ペインで、プロファイルの名前と識別子を入力し、追加のペイロードオプションを追加します。
4. 左側のペインでペイロードを選択し、**構成**をクリックして設定を入力します。署名されたプロファイルはサポートされていないため、プロファイルに署名しないでください。

   単一のプロファイル内に複数のペイロードを追加するには、ペイロードを選択し、右上隅にある**ペイロードを追加**ボタンをクリックします。
5. 「**ファイル > 保存**」に移動し、XMLファイルを保存する名前と場所を選択して、「**保存**」をクリックします。

Profile Creator を使用して構成プロファイルを作成する

1. GitHub から Profile Creator をインストールします。
2. Profile Creator を起動し、「**ファイル > 新規**」に移動します。新しい構成ウィンドウが表示されます。
3. 「**一般**」設定ペインで、プロファイルの名前と説明を入力し、追加のペイロードオプションを追加します。

   - 推奨事項: 「**ユーザーがこのプロファイルを削除できないようにする**」を選択します。
   - 「**ペイロードスコープ**」を「**システム**」または「**ユーザー**」に設定します。
4. 左ペインでポリシーを選択し、設定を構成して、右上隅の「**追加**」をクリックします。

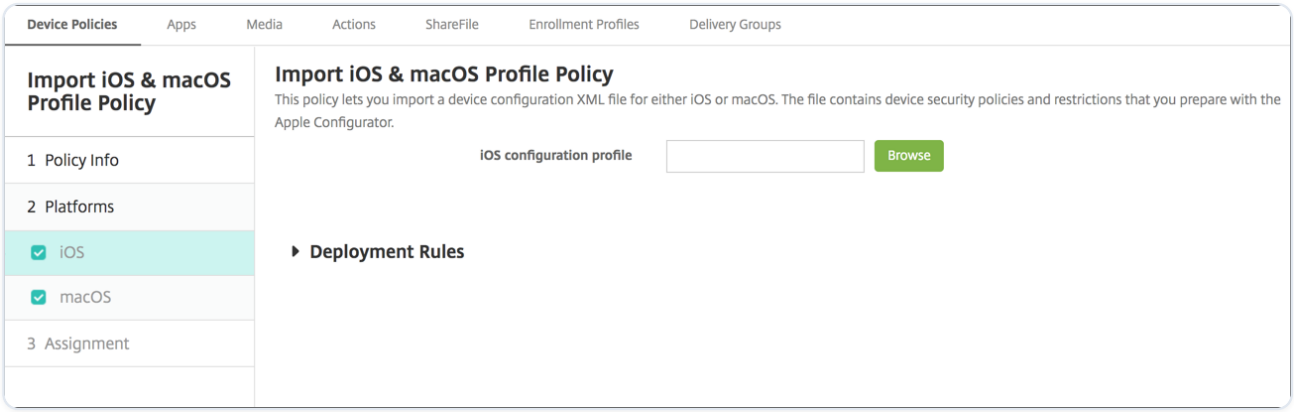
© 1997–2026 Citrix Systems, Inc. All rights reserved.

単一のプロファイル内で複数のポリシーを構成するには、ポリシーを選択し、「**追加**」ボタンをクリックします。

5. 「**ファイル > エクスポート**」に移動し、XMLファイルを保存する名前と場所を選択して、「**保存**」をクリックします。

Citrix Endpoint Management コンソールで iOS および macOS プロファイルデバイスポリシーの構成ファイルをインポートするには、「**構成 > デバイスポリシー**」に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS および macOS の設定



- **iOS 構成プロファイル**または**macOS 構成プロファイル:** インポートする構成ファイルを選択するには、「**参照**」をクリックし、ファイルの場所に移動します。

Androidデバイスのコンプライアンス強制 (テクニカルプレビュー)

注:

テクニカルプレビューの機能は、非本番環境または限定的な本番環境で使用でき、お客様がフィードバックを共有する機会を提供します。Citrix®はテクニカルプレビューの機能に関するサポートケースを受け付けていませんが、改善のためのフィードバックを歓迎します。この機能に関するフィードバックは、**フィードバックを送信**をクリックして提供できます。Citrixは、その重大度、重要性、および緊急性に基づいてフィードバックに対応する場合があります。

*デバイスオーナー*モードで登録されたAndroidデバイスの場合、顧客管理者はデバイスのコンプライアンスを管理できます。これには、コンプライアンスを評価するためのカスタムルールを定義できます。以下が含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- デバイスのパスワード強度が指定された基準を満たしていることを確認する。
- 必要なすべてのアプリのインストールを確認する。
- 禁止されているアプリがすべて削除されていることを確認する。

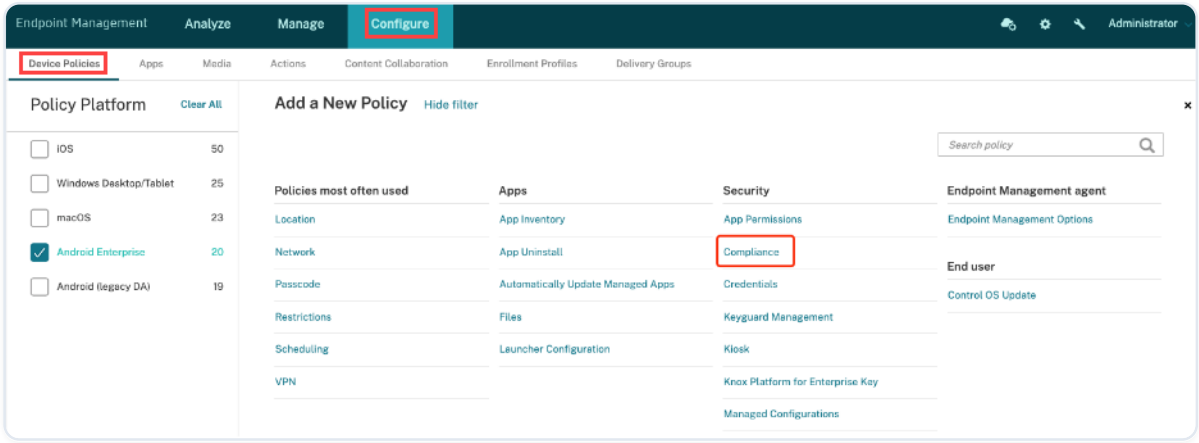
デバイスが非準拠と判断された場合、顧客はユーザーに問題を修正するよう促すことができます。さらに、コンプライアンスが達成されるまでユーザーアクセスを制限するために、デバイス上のアプリをフリーズするなどのより厳格な措置も利用できます。 この機能を有効にするには、サーバー側とクライアント側の両方で変更が必要なため、2つの前提条件が必要です。

- CEMサーバーをバージョン24.8.0にアップグレードする。
- Secure Hubをバージョン24.8.0にアップグレードする。

Androidデバイスのコンプライアンス管理手順

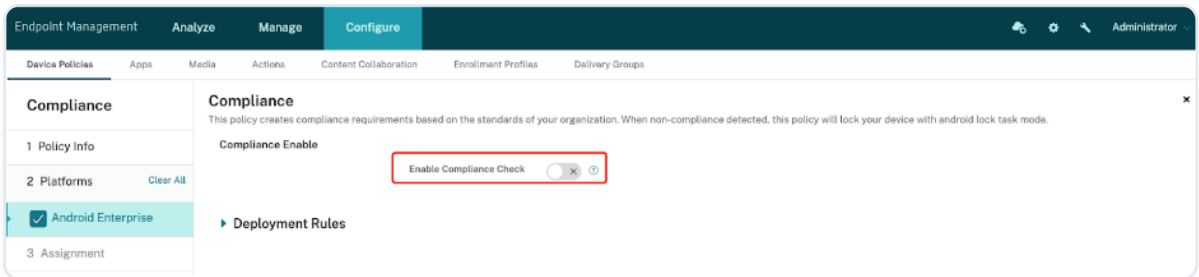
1. 特にCEMサーバー向けに機能フラグ `afw.policy.compliance` をアクティブ化します。
2. コンプライアンスポリシーを追加して展開します。

   a. **構成**タブから**デバイスポリシー**を選択し、**コンプライアンス**をクリックします。



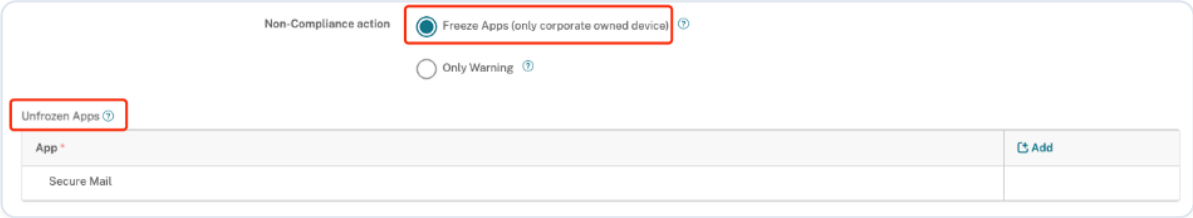
   b. 以下の設定でポリシーを構成します。

   - **コンプライアンスチェック**を有効にする: この設定は、デバイスがコンプライアンスチェックを受けるかどうかを制御します。展開済みのコンプライアンスポリシーを取り消すには、このオプションを無効にしてポリシーを再展開します。デリバリーグループからポリシーを削除するだけでは効果がありません。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

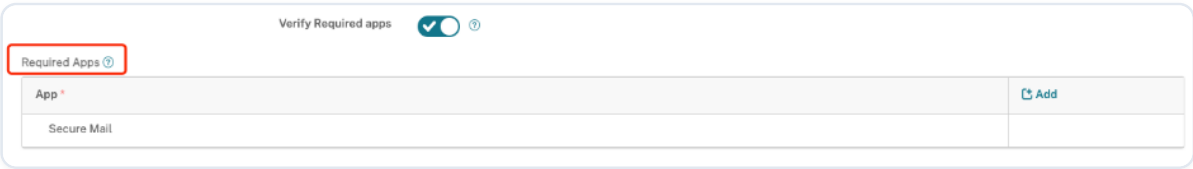
- 非準拠アクション: **警告のみ**と**アプリのフリーズ (企業所有デバイスのみ)**のいずれかを選択します。**警告のみ**を選択すると、Secure Hubでユーザーに非準拠項目が通知され、これらの問題に対処するよう求められます。**アプリのフリーズ (企業所有デバイスのみ)**を選択すると、デバイス上のすべてのアプリがロックされますが、管理者はSecure Hub (非準拠項目の表示と解決のため)、Google Playストア (必要なアプリのインストールのため)、設定 (工場出荷時設定へのリセットのため)、SMS (緊急連絡のため) など、特定のアプリを除外するフリーズ解除アプリリストをカスタマイズできます。**アプリのフリーズ (企業所有デバイスのみ)**は、企業所有デバイスにのみ適用されます。



- パスコードの準拠を確認: デバイスのパスコードが指定された標準を満たしているかを確認します。通常、パスコードポリシーとともに使用されます。
- 必須アプリを確認: 必須アプリのリストを表示します。これらのアプリがデバイスにインストールされていることを確認します。

注:

- **必須アプリ**の下にリストされているアプリは、その機能を確保するために、デリバリーグループの必須アプリセクションにも含める必要があります。そうしないと、効果がありません。
- 必須アプリが管理対象のGoogle Playで利用できない場合、エンドユーザーはロックされたモードのままになります。



- 禁止アプリを確認: 禁止されているアプリのリストを表示します。これらのアプリがインストールされていないことを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注:**
>
> 管理者は、システムにプリインストールされているアプリを**禁止アプリ**リストに追加するのを控えるべきです。エンドユーザーにはそれらを削除する権限がないためです。

3. ポリシーを展開します。

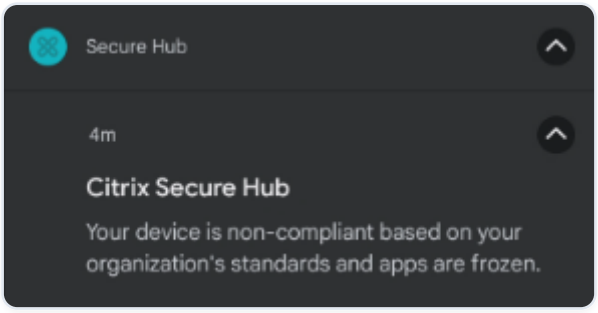
   a. Secure Hubで、ポリシーの更新をクリックするか、6時間ごとの定期的な同期を待ってポリシーをデバイスに展開します。

   b. 展開後、コンプライアンスチェックがすぐにトリガーされます。アプリ凍結モードの非準拠デバイスは、コンプライアンスが満たされるまで、デバイスとそのアプリの両方を制限します。

   デバイスポリシー(/en-us/citrix-endpoint-management/media/device-policy.png)

   管理者が非準拠アクションを「アプリ凍結」に設定した場合、Secure Hubとデバイス自体の両方でアプリの使用が制限されます。具体的には次のとおりです。

   - アプリが凍結されていることをユーザーに通知する永続的な通知が通知バーに表示されます。

   - デフォルトで許可されているアプリ、または**凍結解除されたアプリ**リストにあるアプリを除き、アプリは凍結され、クリックしても応答しなくなります。
   - この状態は、デバイスがコンプライアンスを達成するまで継続します。再起動またはシステムアップグレード後も、デバイスはすぐにこの凍結状態に戻ります（Secure Hubのアップグレード中は例外で、ユーザーによる手動起動が必要です）。

4. 非準拠の解決策:

   - デバイスが非準拠の場合、Secure Hubは通常のメソッド（**デバイス情報**ページで**ポリシーの更新**ボタンをクリックする）によるポリシーの更新がブロックされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

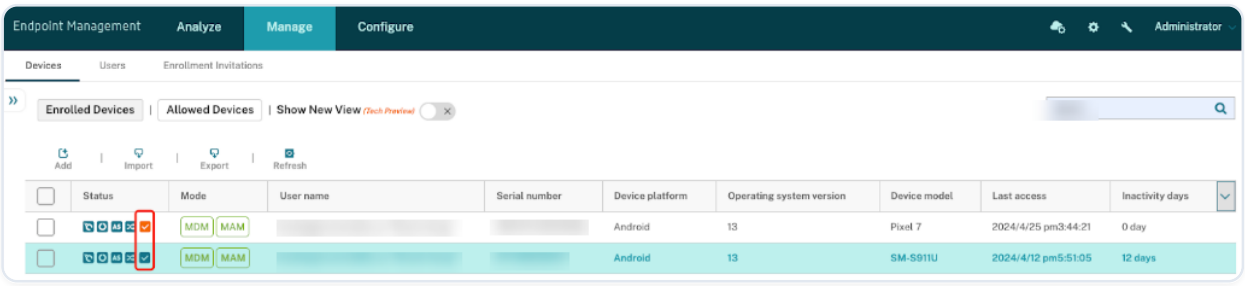
- 代わりに、非準拠項目を表示するページをプルダウンすることで代替ソリューションが提供され、更新結果はトースト通知を通じて伝えられます。

更新リクエストが成功しました(/en-us/citrix-endpoint-management/media/refresh-request-succeeded.png)

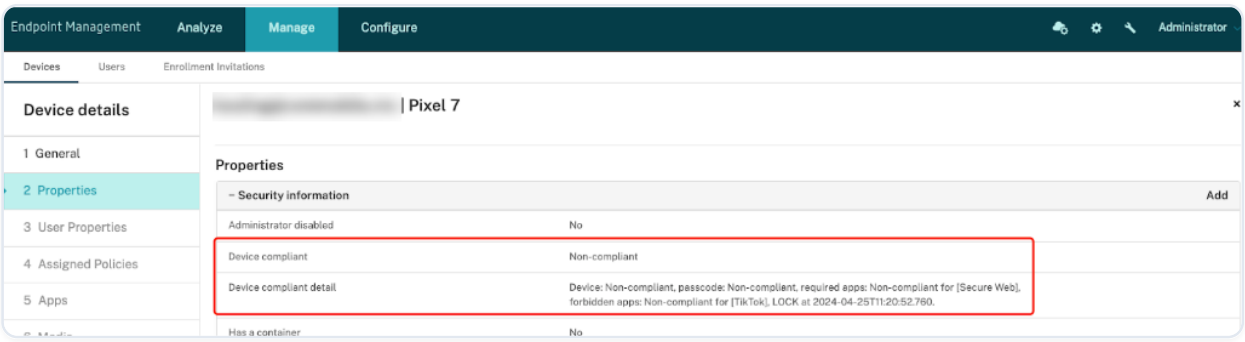
- ユーザー向けの具体的なアクション:
  - 基準を満たすためにより複雑なパスコードを設定します。
  - Google Playストアから必要なアプリをインストールします。
  - 禁止されているアプリをアンインストールします。

5. コンプライアンスの監視

- コンプライアンスステータスの表示: **管理** -> **デバイス** -> **ステータス**に新しいコンプライアンスステータスアイコンが表示されます。緑は準拠、オレンジは非準拠を示します。



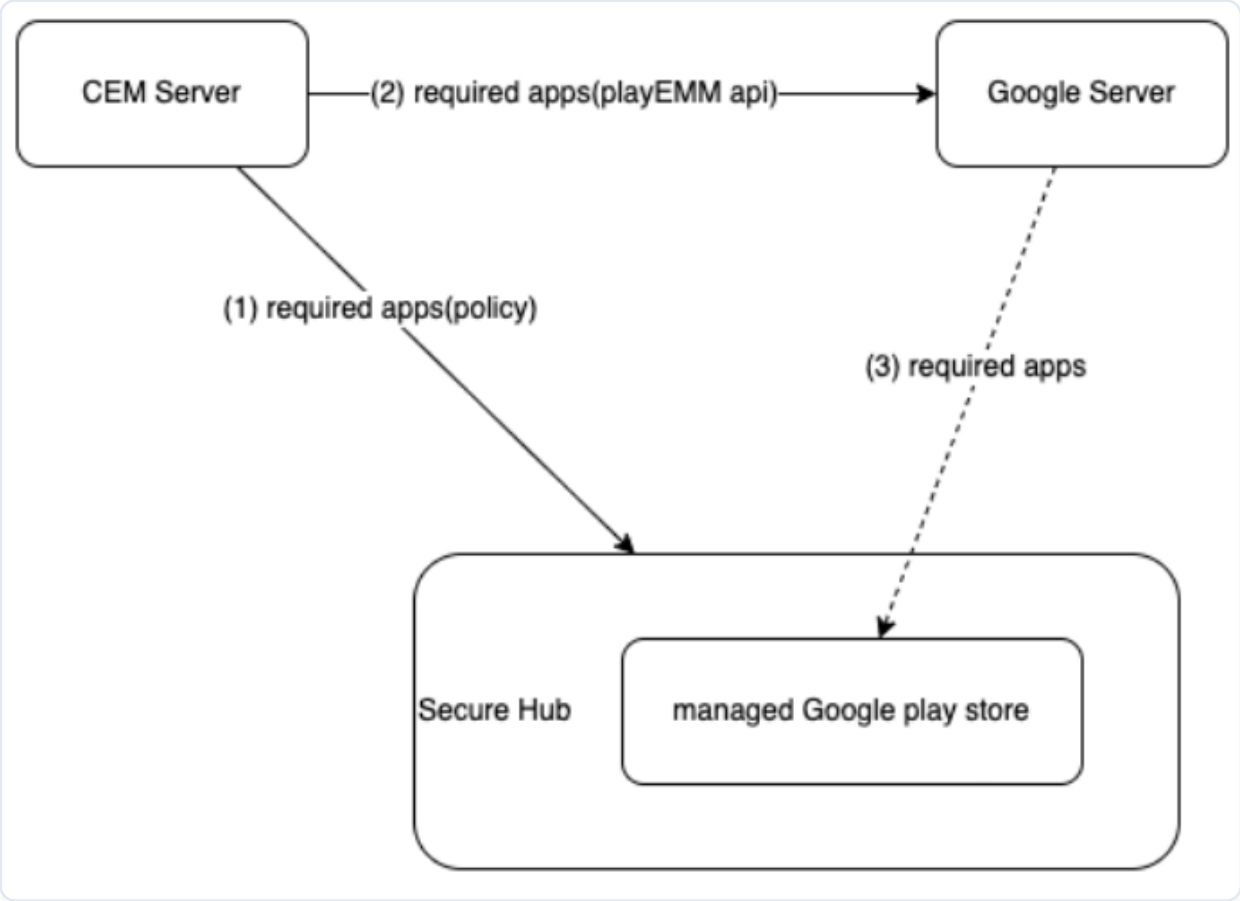
- 詳細なコンプライアンスステータスは、**管理** -> **デバイス** -> **デバイスの詳細** -> **プロパティ** -> **セキュリティ情報**で確認できます。



トラブルシューティング

1. 構成された必須アプリがGoogle Playストアで見つからないため、デバイスが非準拠になり、問題を解決できません。これは設計上の欠陥です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



CEMサーバーは、リンク1と2を介して必須アプリをSecure HubとGoogleサーバーにプッシュしますが、リンク3は当社の管理外です。Secure Hubがリンク1を使用して必須アプリをチェックする際、管理対象のGoogle Playストアにこれらのアプリが利用可能であることを保証できません。この不一致は、コンプライアンスポリシーがSecure Hubにこれらのアプリのインストールを要求しているにもかかわらず、ストアにすぐに見つからない可能性があることを意味します。通常、Googleサーバーはリンク3を使用して24時間以内に必須アプリをデバイスにプッシュします。

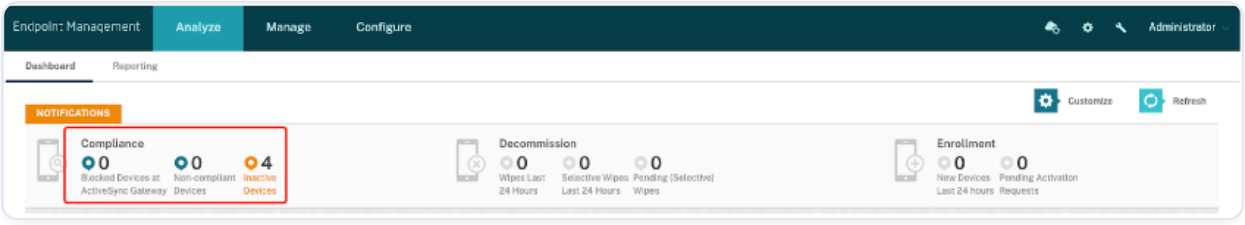
2. Secure Hubをアップグレードする前は、デバイスは非準拠で、アプリはフリーズしていました。しかし、Secure Hubのアップグレード後、すべてのアプリがフリーズ解除されました。これは、アップグレードプロセス中にSecure Hubの操作が終了し、アプリのフリーズ状態を維持できなかったために発生しました。 この問題は既知であり、現在解決策はありません。Googleと協力してこの問題に対処しており、将来のバージョンでの改善を期待しています。アップグレード完了後、ユーザーはSecure Hubを手動で起動してプロセスを開始し、アプリをフリーズ状態に戻すことができます。
3. アプリのフリーズを解除する方法 最も一般的な方法は、ユーザーがすべての非準拠の問題を解決し、デバイスを準拠状態にして、すべてのアプリを自動的にフリーズ解除することです。迅速に準拠状態にすることが難しい場合は、以下の手順を実行できます。

    - 関連アプリを「フリーズ解除されたアプリ」リストに追加し、プルダウンして更新します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 非準拠アクションを「警告」に変更し、プルダウンして更新します。
- 非準拠項目に対応するチェックスイッチまたはマススイッチを無効にし、プルダウンして更新します。
- 上記の方法のいずれも機能しない場合は、特定のCEMサーバーで機能フラグ `afw.locktaskmode.disable` を有効にし、プルダウン更新を実行します。このアクションにより、すべてのアプリが強制的にフリーズ解除されますが、非準拠アクションが**警告**に設定されている場合と同様に、Secure Hubはブロックされたままになります。
- 特定のCEMサーバーで機能フラグ `afw.policy.compliance` を無効にし、プルダウン更新を実行します。
- Secure HubがCEMサーバーに接続できない最悪のシナリオでは、設定から工場出荷時設定へのリセットを実行します。

4. -> に表示されるコンプライアンスステータスは、このポリシーで参照されているものとは異なる種類のCitrix Endpoint Management™のコンプライアンスです。この機能はまだ開発されておらず、今後のバージョンで強化される予定です。



5. この機能は、COSU/WPCOD/BYODモードで登録されたデバイスには適用されません。現在、デバイス所有者 (DO) モードで登録されたデバイスのみをサポートしています。

キーガード管理デバイスポリシー

Androidのキーガードは、デバイスと仕事用チャレンジロック画面を管理します。このポリシーを使用すると、Android Enterpriseの仕事用プロファイルキーガードと高度なデバイスキーガードの機能を管理できます。制御できるのは次のとおりです。

- 仕事用プロファイルデバイスでのキーガード管理。デバイスキーガードと仕事用チャレンジキーガードを解除する前に、ユーザーが利用できる機能を指定できます。たとえば、デフォルトでは、ユーザーは指紋認証によるロック解除を使用したり、ロック画面で編集されていない通知を表示したりできます。
- 完全に管理された専用デバイスでのキーガード管理。信頼エージェントやセキュアカメラなど、キーガード画面を解除する前に利用できる機能を指定できます。または、すべてのキーガード機能を無効にすることもできます。

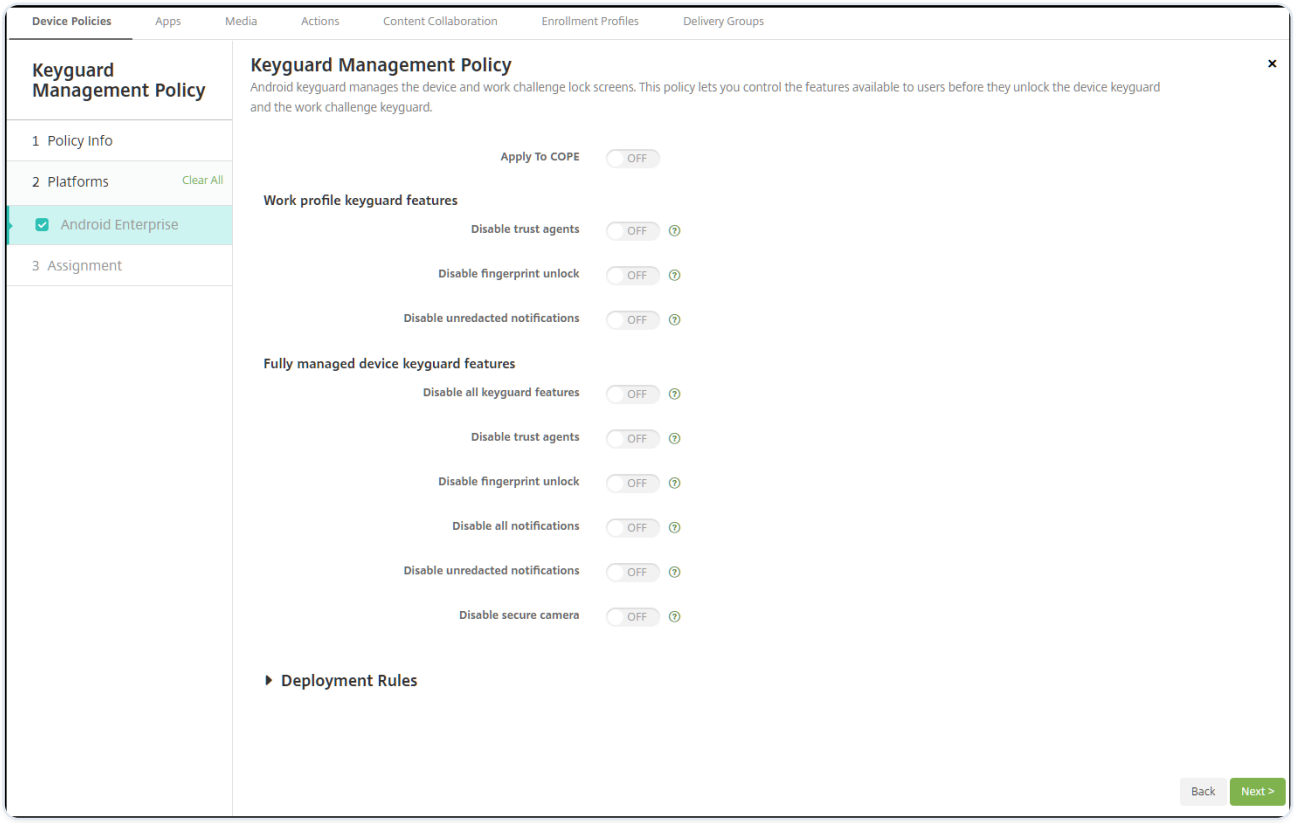
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 仕事用プロファイルを持つ完全に管理されたデバイスでのキーガード管理。これらのデバイスは、以前はCOPE（企業所有個人利用可能）デバイスとして知られていました。1つのキーガード管理ポリシーを使用して、デバイスと仕事用プロファイルに個別の設定を適用できます。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、デバイスポリシーを参照してください。

詳細については、このビデオをご覧ください。

Android Enterpriseの設定



- **COPEに適用:** 仕事用プロファイルを持つ完全に管理されたデバイスのキーガード管理デバイスポリシー設定を構成できます。

  この設定が**オン**の場合、仕事用プロファイルを持つ完全に管理されたデバイスで、デバイスと仕事用プロファイルに個別の設定を適用できます。

  この設定が**オフ**の場合、仕事用プロファイルデバイスまたは完全に管理されたデバイスに設定を適用できます。仕事用プロファイル用に構成した設定は仕事用プロファイルデバイスにのみ適用されます。完全に管理されたデバイス用に構成した設定は完全に管理されたデバイスにのみ適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デフォルトは**オフ**です。

- **仕事用プロファイルキーガード機能:** ユーザーが仕事用プロファイルキーガード（ロック画面）を解除する前に、以下の機能が利用可能かどうかを制御します。
  - **トラストエージェントを無効にする:** 「**オフ**」の場合、ワークプロファイルにチャレンジが設定されているときに、トラストエージェントはセキュアなキーガード画面で動作できます。「**オン**」に設定すると、ワークプロファイル上のすべてのトラストエージェントが無効になります。デフォルトは「**オフ**」です。
  - **生体認証を無効にする:** 「**オフ**」の場合、ワークプロファイルにチャレンジが設定されているときに、セキュアなキーガード画面で生体認証が利用できます。「**オン**」に設定すると、ワークプロファイル上の生体認証が無効になります。この設定により、指紋認証ロック解除、顔認証、虹彩認証が無効になります。デフォルトは「**オフ**」です。Android 9.0以降の場合。
  - **指紋認証ロック解除を無効にする:** 「**オフ**」の場合、ワークプロファイルにチャレンジが設定されているときに、セキュアなキーガード画面で指紋認証ロック解除が利用できます。「**オン**」に設定すると、ワークプロファイル上の指紋認証ロック解除が無効になります。デフォルトは「**オフ**」です。
  - **顔認証を無効にする:** 「**オフ**」の場合、ワークプロファイルにチャレンジが設定されているときに、セキュアなキーガード画面で顔認証が利用できます。「**オン**」に設定すると、ワークプロファイル上の顔認証が無効になります。デフォルトは「**オフ**」です。Android 9.0以降の場合。
  - **虹彩認証を無効にする:** 「**オフ**」の場合、ワークプロファイルにチャレンジが設定されているときに、セキュアなキーガード画面で虹彩認証が利用できます。「**オン**」に設定すると、ワークプロファイル上の虹彩認証が無効になります。デフォルトは「**オフ**」です。Android 9.0以降の場合。
  - **編集されていない通知を無効にする:** 「**オフ**」の場合、編集済みと編集されていない両方の通知がセキュアなキーガード画面に表示されます。「**オン**」に設定すると、編集されていない通知が無効になり、編集済みの通知のみが表示されます。デフォルトは「**オフ**」です。
- **フルマネージドデバイスのキーガード機能:** ユーザーがデバイスのキーガード（ロック画面）を解除する前に、以下の機能が利用可能かどうかを制御します。これらの機能は、フルマネージドデバイスまたは専用デバイスに適用されます。
  - **すべてのキーガード機能を無効にする:** 「**オフ**」の場合、現在および将来のすべてのキーガードカスタマイズがセキュアなキーガード画面で利用できます。「**オン**」に設定すると、すべてのキーガードカスタマイズが無効になります。デフォルトは「**オフ**」です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **トラストエージェントを無効にする:** 「**オフ**」の場合、トラストエージェントはセキュアなキーガード画面で動作できます。「**オン**」に設定すると、トラストエージェントが無効になります。デフォルトは「**オフ**」です。
- **生体認証を無効にする:** 「**オフ**」の場合、デバイスにチャレンジが設定されているときに、セキュアなキーガード画面で生体認証が利用できます。「**オン**」に設定すると、デバイス上の生体認証が無効になります。無効になる生体認証機能は、指紋認証ロック解除、顔認証、および虹彩認証です。デフォルトは「**オフ**」です。Android 9.0以降の場合。
- **指紋認証ロック解除を無効にする:** 「**オフ**」の場合、デバイスにチャレンジが設定されているときに、セキュアなキーガード画面で指紋認証ロック解除が利用できます。「**オン**」に設定すると、デバイス上の指紋認証ロック解除が無効になります。デフォルトは「**オフ**」です。
- **顔認証を無効にする:** 「**オフ**」の場合、デバイスにチャレンジが設定されているときに、セキュアなキーガード画面で顔認証が利用できます。「**オン**」に設定すると、デバイス上の顔認証が無効になります。デフォルトは「**オフ**」です。Android 9.0以降の場合。
- **虹彩認証を無効にする:** 「**オフ**」の場合、デバイスにチャレンジが設定されているときに、セキュアなキーガード画面で虹彩認証が利用できます。「**オン**」に設定すると、デバイス上の虹彩認証が無効になります。デフォルトは「**オフ**」です。Android 9.0以降の場合。
- **すべての通知を無効にする:** 「**オフ**」の場合、すべての通知がセキュアなキーガード画面に表示されます。「**オン**」に設定すると、すべての通知が表示されます。デフォルトは「**オフ**」です。
- **編集されていない通知を無効にする:** 「**オフ**」の場合、編集済みと編集されていない両方の通知がセキュアなキーガード画面に表示されます。「**オン**」に設定すると、編集されていない通知が無効になり、編集済みの通知のみが表示されます。デフォルトは「**オフ**」です。
- **セキュアカメラを無効にする: オフ**の場合、セキュアキーガード画面でセキュアカメラが利用可能です。**オン**に設定すると、セキュアカメラが無効になります。デフォルトは**オフ**です。

キオスクデバイスポリシー

キオスクポリシーを使用すると、実行できるアプリを制限することで、デバイスをキオスクモードに制限できます。Citrix Endpoint Managementは、デバイスのどの部分がキオスクモードでロックされるかを制御しません。ポリシーを展開した後、デバイスがキオスクモードの設定を管理します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iPadをキオスクモードで実行するように設定するには、アプリロックデバイスポリシーを使用します。iPadをキオスクとして設定する方法については、「iPadをキオスクとして構成する」を参照してください。iPadを単一のWebサイトのみを開くように構成することもできます。詳細については、「Webクリップポリシー」を参照してください。

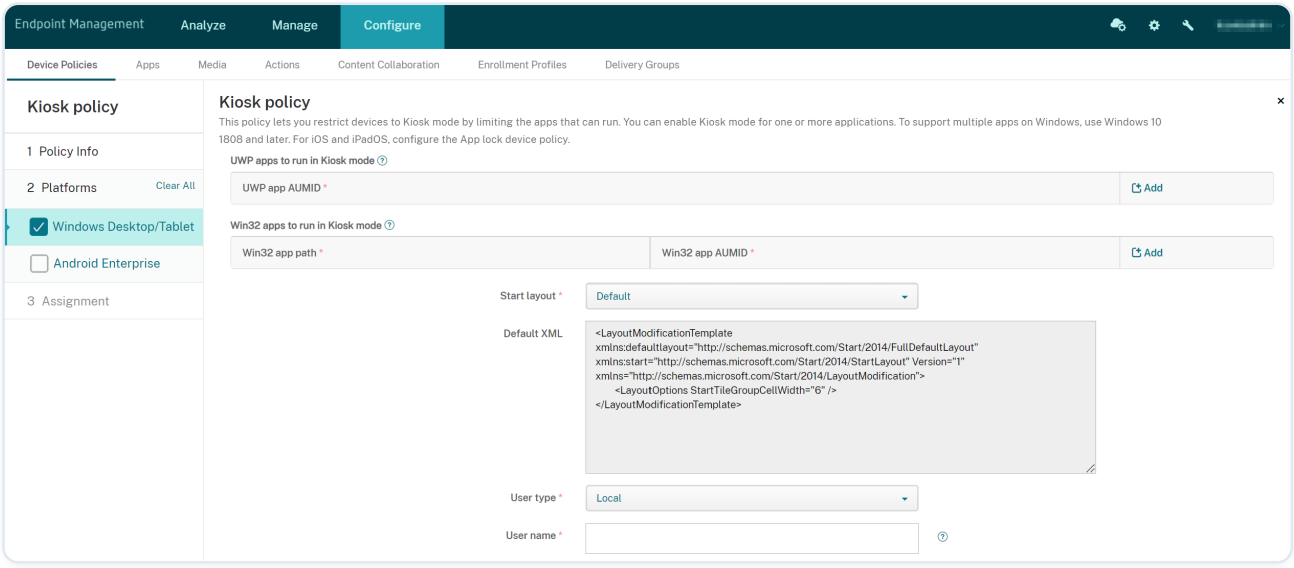
Windowsデスクトップおよびタブレットの設定

Windowsデスクトップおよびタブレットデバイスの場合、キオスクポリシーはローカルユーザーとAzure ADに登録されているユーザーにのみ適用されます。

Windowsデスクトップおよびタブレットデバイスでは、単一のアプリまたは複数のアプリをキオスクモードで実行できます。

注：

キオスクデバイスポリシーは、Windows 10デバイスにのみ適用されます。 Windows 11デバイスにシングルアプリキオスクを展開するには、カスタムXMLデバイスポリシーを使用して、提供されているXMLスクリプトをデバイスに展開できます。詳細については、「Windows 11デバイスにシングルアプリキオスクを展開する」を参照してください。



- **UWPアプリAUMID：** をクリックし、ユニバーサルWindowsプラットフォーム（UWP）アプリを選択し、各UWPアプリのアプリケーションユーザーモデルID（AUMID）を入力します。たとえば、次のAUMIDを入力します。
  - `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Win32アプリパス** および **Win32アプリAUMID**： をクリックし、Windowsデスクトップ (`Win32`) アプリを選択し、各 `Win32` アプリのパスとAUMIDを入力します。たとえば、次のパスとAUMIDを入力します。
  - `%windir%\system32\mspaint.exe` または `C:\Windows\System32\mspaint.exe`
  - `{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe`
- **スタートレイアウト:** アプリの既定のスタート画面のみが利用可能です。
- **既定のXML:** 既定のXMLスクリプトのみが利用可能です。
- **ユーザータイプの選択:** キオスクポリシーを受け取るユーザータイプを指定します。オプションは次のとおりです。
  - **ローカル:** Citrix Endpoint Managementは、ターゲットデバイスのユーザーを作成するか、既存のユーザーを追加します。
  - **Azure AD:** Citrix Endpoint Managementは、Azure ADに登録されているユーザーを追加します。
- **ユーザー名:** キオスクポリシーを受け取るユーザー名を入力します。
  - ターゲットデバイスにローカルユーザー名を作成するには、名前を入力します。ローカルユーザー名にドメインが含まれていないことを確認してください。既存の名前を入力した場合、Citrix Endpoint Managementはユーザーを作成したり、現在のパスワードを変更したりしません。
  - Azure ADユーザーを追加するには、`azuread\user`の形式で名前を入力します。`user` の部分は、Azure ADでユーザーを作成する際に入力した**名前**、またはAzure ADでユーザーを作成する際に入力した**ユーザー名**のいずれかです。割り当てられたユーザーはAzure AD管理者にはなれません。
- **パスワード:** Azure ADユーザーにはパスワード設定はありません。ローカルユーザー名にのみパスワードを入力してください。
- **タスクバーの表示:** タスクバーを有効にすると、ユーザーはアプリケーションを簡単に表示および管理できます。既定は**オフ**です。
- **次へ**をクリックして変更を保存します。

キオスクモードで許可したいUWPアプリの場合、AUMIDを提供する必要があります。現在のデバイスユーザー用にインストールされているすべてのMicrosoft StoreアプリのAUMIDのリストを取得するには、次のPowerShellコマンドを実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$installedapps = get-AppxPackage



$aumidList = @()

foreach ($app in $installedapps)

{

    foreach ($id in (Get-AppxPackageManifest
$app).package.applications.application.id)

    {

        $aumidList += $app.packagefamilyname + "!"+ $id

    }

}



$aumidList
```

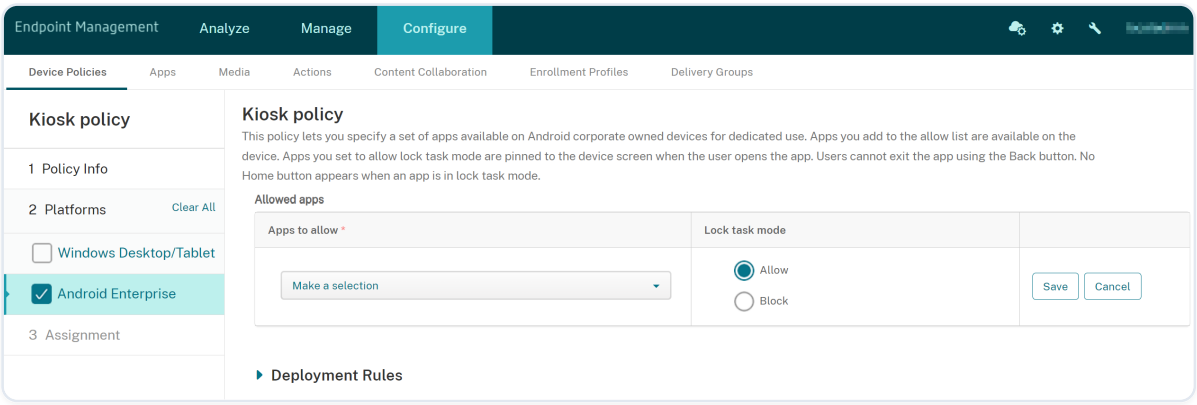
Android Enterpriseの設定

専用のAndroid Enterpriseデバイス（企業所有の単一用途（COSU）デバイスとも呼ばれます）に対して、アプリを許可し、タスクロックモードを設定できます。

アプリを許可するには、**追加**をクリックします。許可リストに複数のアプリを追加できます。詳細については、Android Enterpriseを参照してください。

- **許可するアプリ:** 許可するアプリのパッケージ名を入力するか、リストからアプリを選択します。
    - **新規追加**をクリックして、許可するアプリのパッケージ名をリストに入力します。
    - リストから既存のアプリを選択します。このリストには、Citrix Endpoint Managementにアップロードされているアプリが表示されます。デフォルトでは、Citrix Secure HubとGoogle Play開発者サービスは許可リストに含まれています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **タスク固定モード:** ユーザーがアプリを起動したときに、アプリをデバイス画面に固定するには、**許可**を選択します。アプリを固定しないようにするには、**ブロック**を選択します。デフォルトは**許可**です。

アプリがタスク固定モードの場合、ユーザーがアプリを開くと、アプリはデバイス画面に固定されます。ホームボタンは表示されず、**戻る**ボタンは無効になります。ユーザーは、サインアウトなどのアプリにプログラムされたアクションを使用してアプリを終了します。

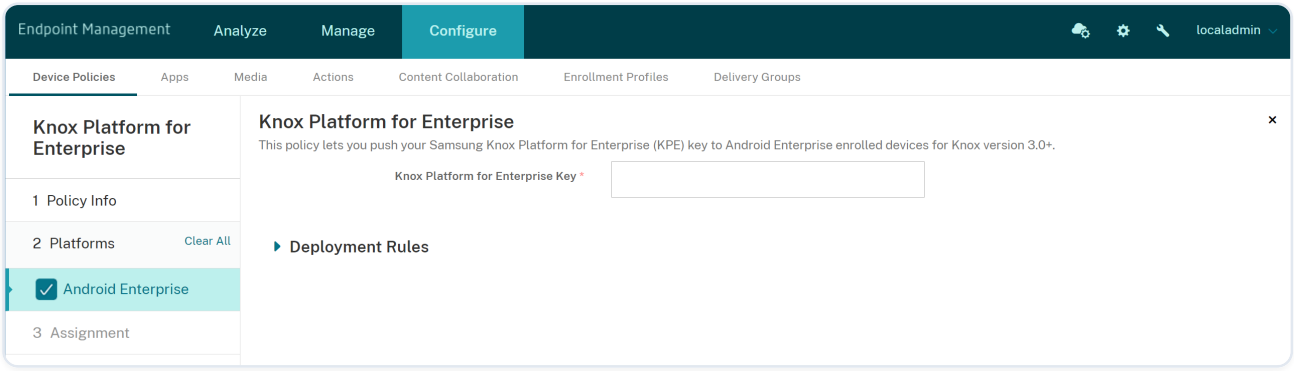
Knox Platform for Enterprise Key デバイスポリシー

このポリシーを使用すると、必要なSamsung Knox Platform for Enterprise (KPE) ライセンス情報を提供できます。

このポリシーを追加または構成するには、**構成** > **デバイスポリシー**に移動します。詳細については、デバイスポリシーを参照してください。

アンドロイド エンタープライズ 設定

このポリシーは、必要なSamsung Knox Platform for Enterprise (KPE) ライセンス情報を提供します。Android 12以前の場合、Knoxプレミアム機能を使用するにはKPEプレミアムライセンスを要求する必要があります。Android 13以降の場合、KPEプレミアムライセンスはデフォルトで提供されます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Knox Platform for Enterprise Key: Android Enterpriseデバイスにプッシュするサムスン Knox Platform for Enterprise (KPE) キーを入力します。KPEライセンスキーはSamsung Knox Platform for Enterprise (KPE) keyで申請してください。

ランチャー構成デバイスポリシー

Citrix Launcher を使用すると、Citrix Endpoint Management によって展開された Android Enterprise デバイスおよびレガシー Android デバイスのユーザーエクスペリエンスをカスタマイズできます。

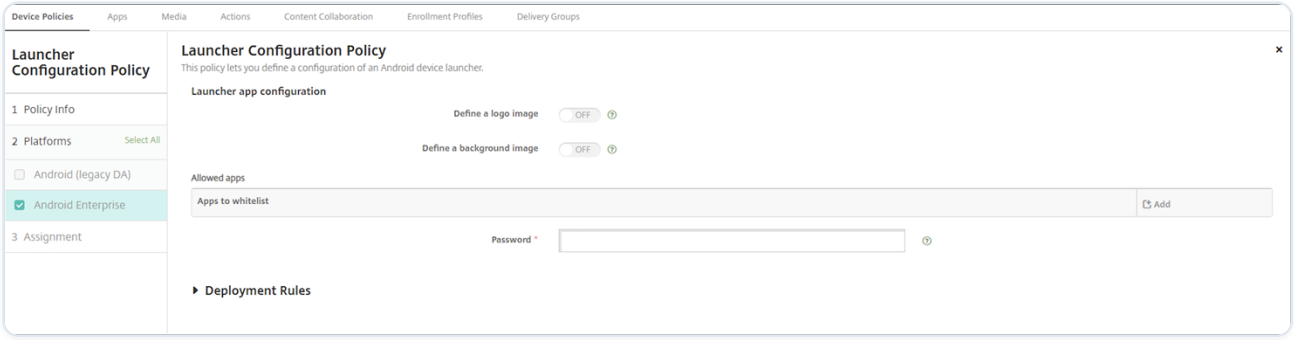
ランチャー構成ポリシーを使用して、次の Citrix Launcher 機能を制御します。

- ユーザーが指定したアプリのみにアクセスできるように、Android Enterprise デバイスとレガシー Android デバイスを管理します。
- 必要に応じて、Citrix Launcher アイコンのカスタムロゴ画像と、Citrix Launcher のカスタム背景画像を指定します。
- ユーザーがランチャーを終了するために必要なパスワードを指定します。

Citrix Launcher は、デバイスプラットフォームがすでに提供しているセキュリティの上に、追加のセキュリティレイヤーとして機能することを意図していません。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

Android Enterprise および Android の設定



- **ロゴ画像を定義:** Citrix Launcher アイコンにカスタムロゴ画像を使用するかどうかを選択します。デフォルトは **オフ** です。
- **ロゴ画像: ロゴ画像を定義** を有効にすると、**参照** をクリックしてファイルの場所に移動し、画像ファイルを選択します。サポートされているファイルの種類は、PNG、JPG、JPEG、GIF です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **背景画像を定義:** Citrix Launcher の背景にカスタム画像を使用するかどうかを選択します。デフォルトは **オフ** です。
- **背景画像: 背景画像を定義** を有効にすると、**参照** をクリックしてファイルの場所に移動し、画像ファイルを選択します。サポートされているファイルの種類は、PNG、JPG、JPEG、GIF です。
- **許可されたアプリ:** Citrix Launcher で許可する各アプリについて、**追加** をクリックし、次の操作を行います。
  - **追加する新しいアプリ:** 追加するアプリの完全な名前を入力します。たとえば、Androidカレンダーアプリの場合はcom.android.calendarです。
  - アプリを追加するには、**保存**をクリックするか、アプリの追加をキャンセルするには、**キャンセル**をクリックします。
- **パスワード:** ユーザーがCitrix Launcherを終了するために必要なパスワード。

LDAPデバイスポリシー

Citrix Endpoint ManagementでiOSデバイス用のLDAPポリシーを作成し、必要なアカウント情報を含む、使用するLDAPサーバーに関する情報を提供します。このポリシーは、LDAPサーバーを照会する際に使用する一連のLDAP検索ポリシーも提供します。

このポリシーを構成する前に、LDAPホスト名が必要です。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **アカウントの説明:** オプションのアカウントの説明を入力します。
- **アカウントのユーザー名:** オプションのユーザー名を入力します。
- **アカウントのパスワード:** オプションのパスワードを入力します。このフィールドは、暗号化されたプロファイルでのみ使用してください。
- **LDAPホスト名:** LDAPサーバーのホスト名を入力します。このフィールドは必須です。
- **SSLを使用:** LDAPサーバーへのSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは**オン**です。
- **検索設定:** LDAPサーバーを照会する際に使用する検索設定を追加します。必要な数の検索設定を入力できますが、アカウントを有効にするには少なくとも1つの検索設定を追加する必要があります。**追加**をクリックし、次の操作を行います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **説明:** 検索設定の説明を入力します。このフィールドは必須です。
- **スコープ:** LDAPツリーをどの深さまで検索するかを定義するために、**Base**、**One level**、または**Subtree**を選択します。デフォルトは**Base**です。
  - **Base**は、検索ベースが指すノードを検索します。
  - **One level**は、Baseノードとその1レベル下を検索します。
  - **サブツリー**は、深さに関係なく、ベースノードとそのすべての子を検索します。
- **検索ベース:** 検索を開始するノードへのパスを入力します。例: ou=people または 0=example corp。このフィールドは必須です。
- **保存**をクリックして検索設定を追加するか、**キャンセル**をクリックして検索設定の追加をキャンセルします。
- 追加する検索設定ごとにこれらの手順を繰り返します。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。

macOS設定

- **アカウントの説明:** オプションのアカウントの説明を入力します。
- **アカウントのユーザー名:** オプションのユーザー名を入力します。
- **アカウントのパスワード:** オプションのパスワードを入力します。このフィールドは、暗号化されたプロファイルでのみ使用します。
- **LDAPホスト名:** LDAPサーバーのホスト名を入力します。このフィールドは必須です。
- **SSLを使用:** LDAPサーバーへのSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは**オン**です。
- **検索設定:** LDAPサーバーを照会するときに使用する検索設定を追加します。必要な数の検索設定を入力できますが、アカウントを有効にするには少なくとも1つの検索設定を追加する必要があります。**追加**をクリックし、次の操作を行います。
  - **説明:** 検索設定の説明を入力します。このフィールドは必須です。
  - **スコープ:** LDAPツリーをどの深さまで検索するかを定義するために、**Base**、**One level**、または**Subtree**を選択します。デフォルトは**Base**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **Base**は、検索ベースで指定されたノードを検索します。
    - **One level**は、Baseノードとその1つ下のレベルを検索します。
    - **Subtree**は、Baseノードとそのすべての子を、深さに関係なく検索します。
  - **検索ベース:** 検索を開始するノードへのパスを入力します。たとえば、ou=peopleまたは0=example corpです。このフィールドは必須です。
  - 検索設定を追加するには**保存**をクリックし、検索設定の追加をキャンセルするには**キャンセル**をクリックします。
  - 追加する各検索設定について、これらの手順を繰り返します。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

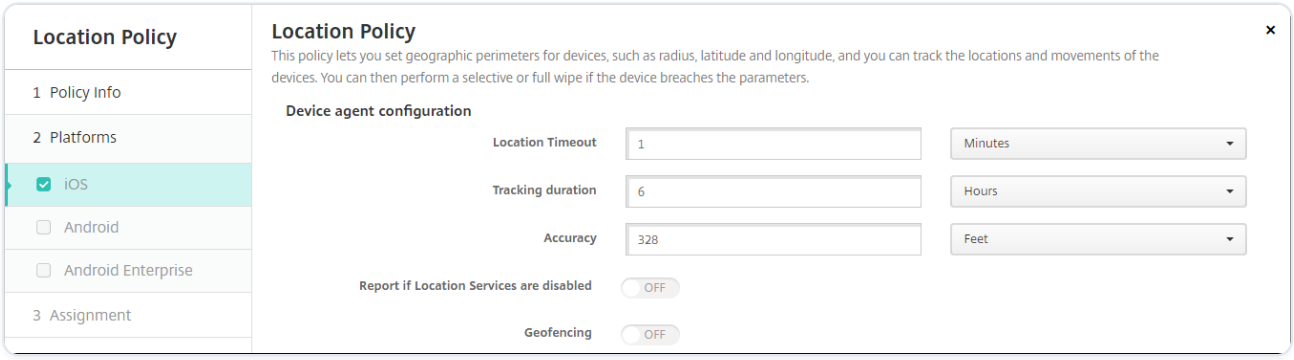
ロケーションデバイスポリシー

地理的境界を適用するために、Citrix Endpoint Management でロケーションデバイスポリシーを作成します。ユーザーが定義された境界（*ジオフェンス*とも呼ばれます）を越えた場合、Citrix Endpoint Management は特定のアクションを実行できます。たとえば、定義された境界を越えたときにユーザーに警告メッセージを発行するようにポリシーを構成できます。また、境界を越えたときに、すぐに、または遅延後にユーザーの企業データをワイプするようにポリシーを構成することもできます。デバイスの追跡と位置特定を有効にするなどのセキュリティアクションについては、「セキュリティアクション」を参照してください。

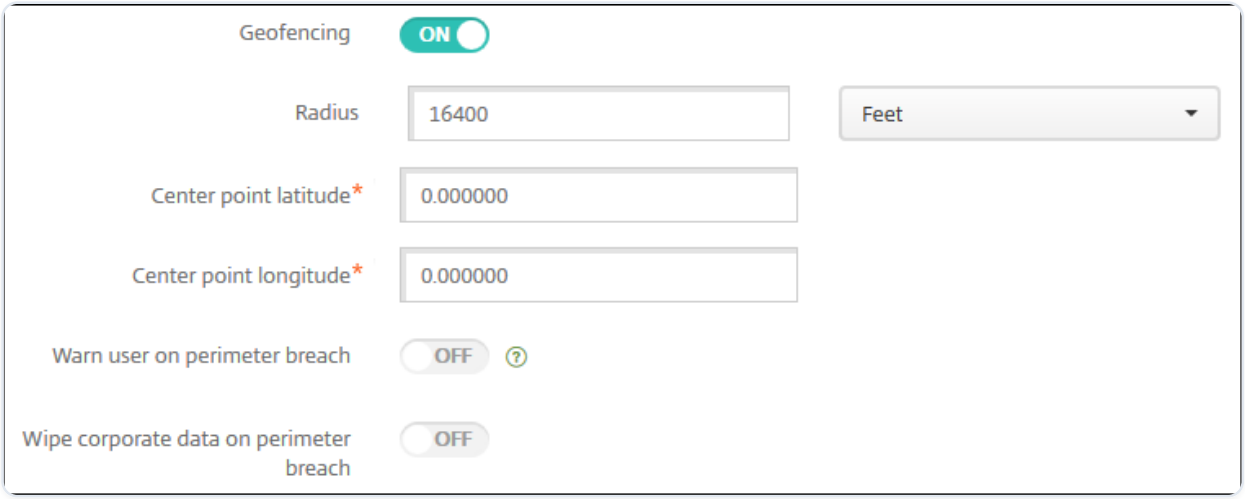
このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］**の順に移動します。詳しくは、「デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定



- **ロケーションタイムアウト:** 数値を入力し、［秒］または［分］をクリックして、**Citrix Endpoint Management がデバイスの位置を特定しようとする頻度を設定します。有効な値は、60～900秒または1～15分です。デフォルトは1分**です。
- **追跡期間:** 数値を入力し、［時間］または［分］をクリックして、**Citrix Endpoint Management がデバイスを追跡する期間を設定します。有効な値は、1～10時間または10～600分です。デフォルトは6時間**です。
- **精度:** 数値を入力し、［メートル］、［フィート］、または**［ヤード］をクリックして、**Citrix Endpoint Management がデバイスを追跡する際のデバイスへの近さを設定します。有効な値は、10～5000ヤード、30～15000フィート、または10～5000メートルです。デフォルトは**328フィート**（100メートル）**です。
- **位置情報サービスが無効な場合にレポートする:** ユーザーがGPSをオフにしたときに、デバイスがCitrix Endpoint Management にレポートを送信するかどうかを選択します。デフォルトは**オフ**です。
- **ジオフェンシング**



ジオフェンシングを有効にすると、次の設定を構成します。

- **半径:** 数値を入力し、半径の測定に使用する単位をクリックします。デフォルトは**16400フィート（5000メートル）**です。半径の有効な値は次のとおりです。

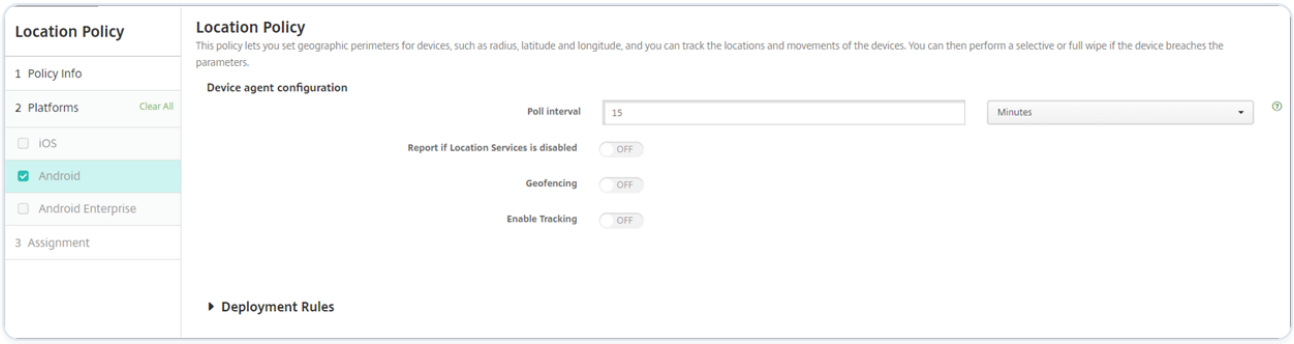
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 164〜16400フィート
- 50〜50000メートル
- 54–54680 ヤード
- 1–31 マイル

- **中心点の緯度:** 37.787454などの緯度を入力して、ジオフェンスの中心点の緯度を定義します。
- **中心点の経度:** 122.402952などの経度を入力して、ジオフェンスの中心点の経度を定義します。
- **境界侵害時にユーザーに警告:** ユーザーが定義された境界を侵害したときに警告メッセージを発行するかどうかを選択します。デフォルトは**オフ**です。警告メッセージを表示するためにCitrix Endpoint Managementへの接続は必要ありません。
- **境界侵害時に企業データをワイプ:** ユーザーが境界を侵害したときにデバイスをワイプするかどうかを選択します。デフォルトは**オフ**です。このオプションを有効にすると、**ローカルワイプの遅延**フィールドが表示されます。
  - 数値を入力し、**秒**または**分**をクリックして、ユーザーデバイスから企業データをワイプするまでの遅延時間を設定します。この遅延により、Citrix Endpoint Managementがデバイスを選択的にワイプする前に、ユーザーは許可された場所に戻る機会を得られます。デフォルトは**0秒**です。

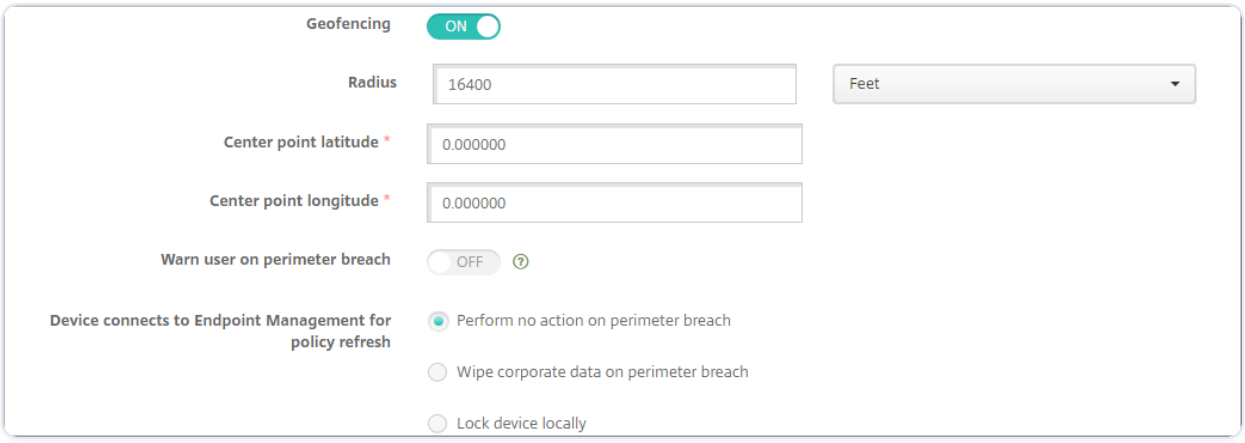
Android (レガシーDA) 設定

Androidの位置情報追跡にはAndroid 9以降が必要です。



- **ポーリング間隔:** 数値を入力し、**分**、**時間**、または**日**をクリックして、Citrix Endpoint Managementがデバイスの位置を特定しようとする頻度を設定します。有効な値は15〜1440分、1〜24時間、または任意の日数です。デフォルトは**15分**です。
- **位置情報サービスが無効な場合に報告:** ユーザーがGPSをオフにしたときに、デバイスがCitrix Endpoint Managementにレポートを送信するかどうかを選択します。デフォルトは**オフ**です。
- **ジオフェンシング**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



ジオフェンシングを有効にすると、次の設定を構成します。

- **半径:** 数値を入力し、半径の測定に使用する単位をクリックします。デフォルトは **16400 フィート** (**5000 メートル**) です。半径の有効な値は次のとおりです。
  - 164～164000 フィート
  - 1～50 キロメートル
  - 50～50000 メートル
  - 54～54680 ヤード
  - 1～31 マイル
- **中心点の緯度:** ジオフェンスの中心点の緯度を定義するために、37.787454 などの緯度を入力します。
- **中心点の経度:** ジオフェンスの中心点の経度を定義するために、122.402952 などの経度を入力します。
- **境界侵害時にユーザーに警告:** ユーザーが定義された境界を侵害したときに警告メッセージを発行するかどうかを選択します。デフォルトは **オフ** です。警告メッセージを表示するために Citrix Endpoint Management への接続は必要ありません。
- **ポリシー更新のためにデバイスが Citrix Endpoint Management に接続する:** ユーザーが境界を侵害した場合の次のオプションのいずれかを選択します。
  - **境界侵害時にアクションを実行しない:** 何もしません。これがデフォルトです。
  - **境界侵害時に企業データをワイプする:** 指定された時間後に企業データをワイプします。このオプションを有効にすると、**ローカルワイプの遅延** フィールドが表示されます。
    - 数値を入力し、**秒** または **分** をクリックして、ユーザーデバイスから企業データをワイプするまでの遅延時間を設定します。この遅延により、Citrix Endpoint Management がデバイスを選択的にワイプする前に、ユーザーは許可された場所に戻る機会を得られます。デフォルトは **0 秒** です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

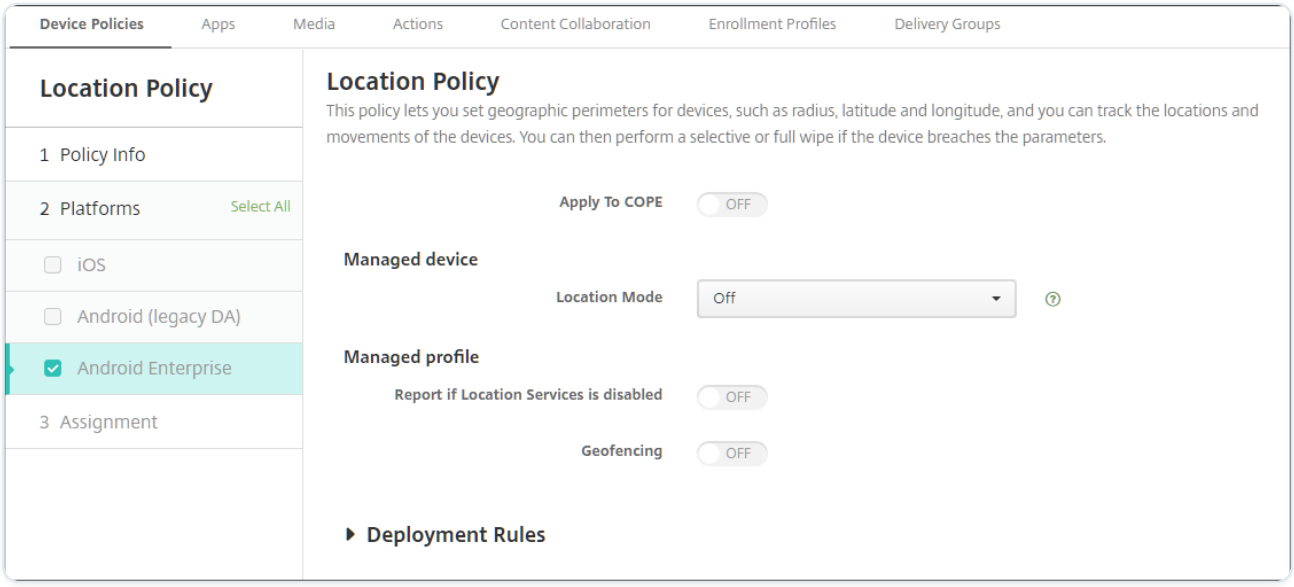
    - **デバイスをローカルでロックする:** 指定された時間後にユーザーのデバイスをロックします。このオプションを有効にすると、**ロックの遅延** フィールドが表示されます。
        - 数値を入力し、**秒** または **分** をクリックして、ユーザーデバイスをロックするまでの遅延時間を設定します。この遅延により、Citrix Endpoint Management がデバイスをロックする前に、ユーザーは許可された場所に戻る機会を得られます。デフォルトは **0 秒** です。

- **追跡を有効にする:** デバイスがユーザーの位置を追跡するかどうかを選択します。デフォルトは**オフ**です。

Android Enterpriseの設定

Androidの位置追跡が機能するためには、以下の要件が満たされていることを確認してください。

- Android 9以降
- Android Enterpriseの制限デバイスポリシーで「位置情報共有を許可」設定が有効になっていること
- 接続スケジューリング（Firebase Cloud Messagingを推奨）



ワークプロファイルを持つ完全に管理されたデバイスに適用

ワークプロファイルを持つ完全に管理されたデバイス（以前はCOPEデバイスとして知られていました）の場合、位置情報モード設定のみが利用可能です。

- **ワークプロファイルを持つ完全に管理されたデバイス/企業所有デバイス上のワークプロファイルに適用:** ワークプロファイルを持つ完全に管理されたデバイスの位置情報モードを構成できます。この設定がオンの場合、ワークプロファイルの設定を構成します。

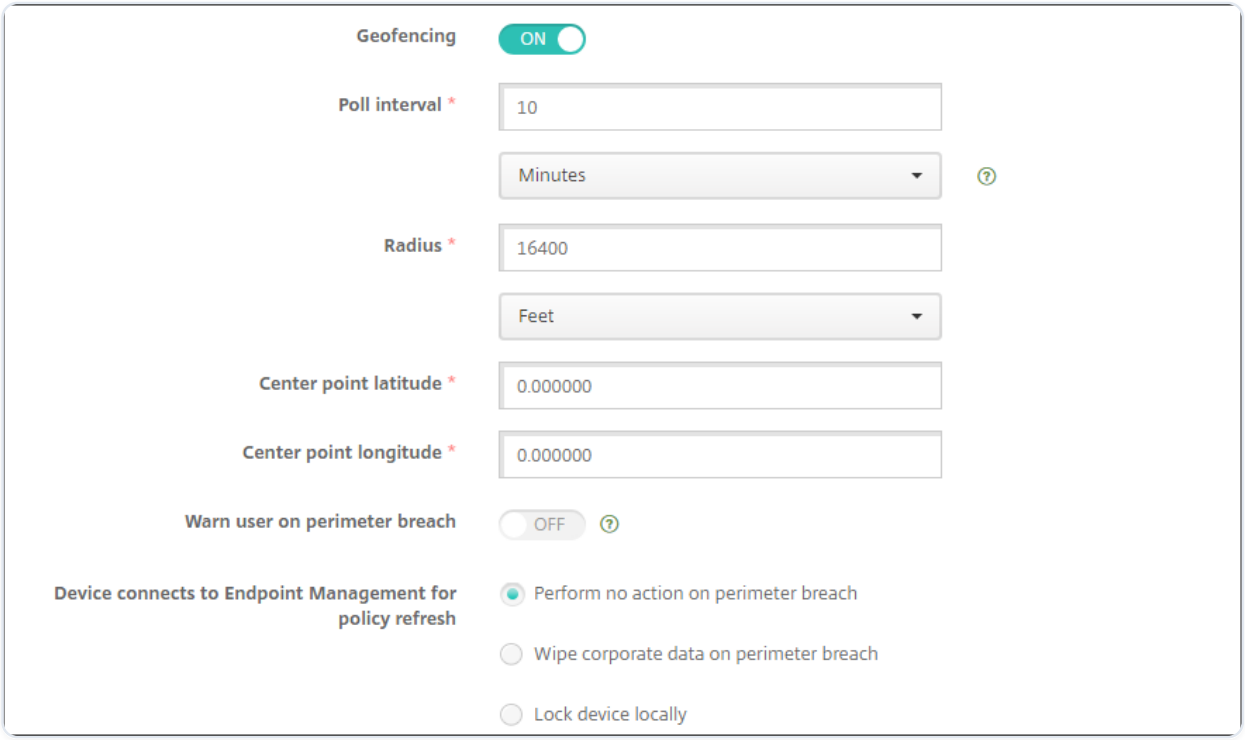
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **位置情報サービスが無効な場合に報告:** ユーザーがGPSをオフにしたときに、デバイスがCitrix Endpoint Managementにレポートを送信するかどうかを選択します。デフォルトは**オフ**です。
- **ジオフェンシング:** この記事の管理対象デバイスの下にある設定を参照してください。

ワークプロファイルを持つ完全に管理されたデバイス/企業所有デバイス上のワークプロファイルに適用がオフの場合、設定は以下のセクションに示すように、管理対象デバイスとワークプロファイルに適用されます。デフォルトは**オフ**です。

管理対象デバイス

- **位置情報モード:** 有効にする位置検出の精度を指定します。位置情報モードが**高精度**または**バッテリー節約**に設定されている場合にのみ、位置特定セキュリティアクションを使用できます。デフォルトは**高精度**です。
  - **高精度:** GPS、ネットワーク、その他のセンサーを含む、すべての位置検出方法を有効にします。
  - **センサーのみ:** GPSとその他のセンサーのみを有効にします。
  - **バッテリー節約:** ネットワーク位置情報プロバイダーのみを有効にします。
  - **オフ:** 位置検出を無効にします。
- **ジオフェンシング:**



ジオフェンシングを有効にすると、次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ポーリング間隔:** 数値を入力し、**分**、**時間**、または**日**をクリックして、Citrix Endpoint Managementがデバイスの位置を特定しようとする頻度を設定します。有効な値は、1〜1440分、1〜24時間、または任意の日数です。デフォルトは**10分**です。この値を10分未満に設定すると、デバイスのバッテリー寿命に悪影響を及ぼす可能性があります。
- **半径:** 数値を入力し、半径の測定に使用する単位をクリックします。デフォルトは**16400フィート** (**5000メートル**) です。半径の有効な値は次のとおりです。
  - 164〜164000フィート
  - 1〜50キロメートル
  - 50〜50000メートル
  - 54〜54680ヤード
  - 1〜31マイル
- **中心点の緯度:** ジオフェンスの中心点の緯度を定義するために、37.787454などの緯度を入力します。値を確認するには、**管理 > デバイス**に移動し、デバイスを選択して、**セキュリティ保護**をクリックし、**検索**をクリックします。デバイスを検索した後、Citrix Endpoint Managementは**セキュリティ**の下の**デバイスの詳細 > 全般**ページでデバイスの位置を報告します。
- **中心点の経度:** ジオフェンスの中心点の経度を定義するために、122.402952などの経度を入力します。
- **境界侵害時にユーザーに警告:** ユーザーが定義された境界を侵害したときに警告メッセージを発するかどうかを選択します。デフォルトは**オフ**です。警告メッセージを表示するためにCitrix Endpoint Managementへの接続は必要ありません。
- **ポリシー更新のためにデバイスがCitrix Endpoint Managementに接続:** ユーザーが境界を侵害したときの次のオプションのいずれかを選択します。
  - **境界侵害時にアクションを実行しない:** 何もしません。この設定がデフォルトです。
  - **境界侵害時に企業データをワイプ:** 指定された時間後に企業データをワイプします。このオプションを有効にすると、**ローカルワイプの遅延**フィールドが表示されます。
    - 数値を入力し、**秒**または**分**をクリックして、ユーザーデバイスから企業データをワイプするまでの遅延時間を設定します。この遅延により、Citrix Endpoint Managementがデバイスを選択的にワイプする前に、ユーザーは許可された場所に戻る機会を得られます。デフォルトは**0秒**です。
  - **デバイスをローカルでロック:** 指定された時間後にユーザーのデバイスをロックします。このオプションを有効にすると、**ロックの遅延フィールド**が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 数値を入力し、**秒**または**分**をクリックして、ユーザーデバイスをロックするまでの遅延時間を設定します。この遅延により、Citrix Endpoint Managementがデバイスをロックする前に、ユーザーは許可された場所に戻る機会を得られます。デフォルトは**0秒**です。

ワークプロファイル

- **位置情報サービスが無効な場合に報告:** ユーザーがGPSをオフにしたときに、デバイスがCitrix Endpoint Managementにレポートを送信するかどうかを選択します。デフォルトは**オフ**です。
- **ジオフェンシング:** この記事の管理対象デバイスの下の設定を参照してください。

ロック画面メッセージデバイスポリシー

ロック画面メッセージポリシーを使用すると、紛失した以下のiOSデバイスに表示されるメッセージを設定できます。

- 共有iPadのログインウィンドウ
- 監視対象iOSデバイスのロック画面

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **デバイスのアセットタグ情報:** デバイスのアセットタグ。Appleデバイスは長い文字列を切り詰めるため、ポリシーを本番環境に展開する前に文字列をテストしてください。文字列の長さは、AppleデバイスのモデルとAppleの設定によって異なり、変更される可能性があります。
- **ログインウィンドウとロック画面のフッター:** デバイスを返却するのに役立つ情報（住所やその他の連絡先情報など）。たとえば、メッセージは「紛失した場合は、〜に返却してください」という形式になる場合があります。Appleデバイスは長い文字列を切り詰めるため、ポリシーを本番環境に展開する前に文字列をテストしてください。文字列の長さは、AppleデバイスのモデルとAppleの設定によって異なり、変更される可能性があります。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間（時間）**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0以降でのみ利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メールデバイスポリシー

Citrix Endpoint Managementでメールデバイスポリシーを追加して、iOSまたはmacOSデバイスでメールアカウントを設定できます。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」(/ja-jp/citrix-endpoint-management/policies.html) を参照してください。

iOSおよびmacOSの設定

デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/device-policy-mail-ios.png)

- **アカウントの説明:** メールおよび設定アプリに表示されるアカウントの説明を入力します。このフィールドは必須です。
- **アカウントの種類:** ユーザーアカウントに使用するプロトコルとして、**IMAP** または **POP** のいずれかを選択します。デフォルトは **IMAP** です。**POP** を選択すると、以下の **パス** プレフィックスオプションは表示されなくなります。
- **パスプレフィックス: INBOX** またはIMAPメールアカウントのパスプレフィックスを入力します。このフィールドは必須です。
- **ユーザー表示名:** メッセージやその他の目的に使用する完全なユーザー名を入力します。このフィールドは必須です。
- **メールアドレス:** アカウントの完全なメールアドレスを入力します。このフィールドは必須です。
- **受信メール設定**
  - **メールサーバーホスト名:** 受信メールサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
  - **メールサーバーポート:** 受信メールサーバーのポート番号を入力します。デフォルトは **143** です。このフィールドは必須です。
  - **ユーザー名:** メールアカウントのユーザー名を入力します。この名前は通常、メールアドレスの「@」記号より前の部分と同じです。このフィールドは必須です。
  - **認証の種類:** 使用する認証の種類を選択します。デフォルトは **パスワード** です。**なし** を選択すると、以下の **パスワード** フィールドは表示されなくなります。
  - **パスワード:** 受信メールサーバーのオプションのパスワードを入力します。
  - **SSLを使用:** 受信メールサーバーがSecure Socket Layer認証を使用するかどうかを選択します。デフォルトは**オフ**です。
- **送信メール設定**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **メールサーバーのホスト名:** 送信メールサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
- **メールサーバーのポート:** 送信メールサーバーのポート番号を入力します。ポート番号を入力しない場合、指定されたプロトコルのデフォルトポートが使用されます。
- **ユーザー名:** メールアカウントのユーザー名を入力します。この名前は通常、@文字までのメールアドレスと同じです。このフィールドは必須です。
- **認証タイプ:** 使用する認証タイプを選択します。デフォルトは**パスワード**です。
- **パスワード:** 送信メールサーバーのオプションのパスワードを入力します。
- **送信パスワードは受信と同じ:** 受信パスワードと送信パスワードが同じかどうかを選択します。デフォルトは**オフ**で、パスワードが異なることを意味します。
- **SSLを使用:** 送信メールサーバーがSecure Socket Layer認証を使用するかどうかを選択します。デフォルトは**オフ**です。

- **ポリシー**
  - **アカウント間のメール移動を許可:** ユーザーに以下を許可するかどうかを選択します。
    - このアカウントから別のメールアカウントへメールを移動する
    - 別のメールアカウントからメールを転送する
    - 別のメールアカウントから返信する。

    デフォルトは**オフ**です。
  - **メールアプリからのみメールを送信:** ユーザーがメール送信にiOSメールアプリのみを使用するように制限するかどうかを選択します。
  - **メールの最近の同期を無効にする:** ユーザーが最近のアドレスを同期するのを防ぐかどうかを選択します。デフォルトは**オフ**です。このオプションはiOS 6.0以降にのみ適用されます。
  - **Mail Dropを許可:** iOS 9.2以降を実行しているデバイスでApple Mail Dropの使用を許可するかどうかを選択します。デフォルトは**オフ**です。
  - **S/MIME署名を有効にする:** このアカウントがS/MIME署名をサポートするかどうかを選択します。デフォルトは**オン**です。**オン**に設定すると、以下のフィールドが表示されます。
    - **署名ID資格情報:** 使用する署名資格情報を選択します。
    - **S/MIME署名ユーザーによる上書き可能: オン**に設定すると、ユーザーはデバイスの設定でS/MIME署名をオン/オフできます。デフォルトは**オフ**です。このオプションはiOS 12.0以降に適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **S/MIME署名証明書UUIDユーザーによる上書き可能: オン**に設定すると、ユーザーはデバイスの設定で、使用する署名資格情報を選択できます。デフォルトは**オフ**です。このオプションはiOS 12.0以降に適用されます。

  - **S/MIME暗号化を有効にする:** このアカウントがS/MIME暗号化をサポートするかどうかを選択します。デフォルトは**オフ**です。**オン**に設定すると、以下のフィールドが表示されます。

    - **暗号化ID資格情報:** 使用する暗号化資格情報を選択します。
    - **メッセージごとのS/MIMEスイッチを有効にする: オン**に設定すると、ユーザーが作成する各メッセージに対してS/MIME暗号化をオンまたはオフにするオプションが表示されます。デフォルトは**オフ**です。
    - **S/MIMEデフォルト暗号化ユーザーによる上書き可能: オン**に設定すると、ユーザーはデバイスの設定で、S/MIMEがデフォルトでオンになっているかどうかを選択できます。デフォルトは**オフ**です。このオプションはiOS 12.0以降に適用されます。
    - **S/MIME暗号化証明書UUIDユーザーによる上書き可能: オン**に設定すると、ユーザーはデバイスの設定でS/MIME暗号化IDと暗号化をオン/オフできます。デフォルトは**オフ**です。このオプションはiOS 12.0以降に適用されます。

- **ポリシー設定**

  - **ポリシーの削除:** 後でポリシーを削除するには、この設定を構成して、**日付を選択**してポリシーを削除するか、**削除までの期間（時間）**を設定します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがメールポリシーを**常に**、**パスコードが必要**な場合のみ、または**許可しない**のいずれかの方法で削除することを許可します。macOSでのみ利用可能です。
  - **プロファイルスコープ:** macOSのみの場合、ポリシーを**ユーザー**レベルで適用するか、**システム**全体に適用するかを選択します。

マネージド構成ポリシー

マネージド構成デバイスポリシーは、さまざまなアプリ構成オプションとアプリ制限を制御します。このポリシーは、制御したいAndroid Enterpriseアプリごとに作成します。

アプリ開発者が、アプリで利用できるオプションとツールヒントを定義します。ツールヒントに「テンプレート値」の使用が記載されている場合は、代わりに、対応するCitrix Endpoint Managementマクロを使用してください。詳細については、リモート構成の概要 (Android開発者サイト上) およびマクロを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ構成設定には、次のような項目が含まれる場合があります。

- メールアプリの設定
- WebブラウザーのURLを許可またはブロックする
- 携帯電話接続またはWi-Fi接続のみによるアプリコンテンツ同期を制御するオプション

アプリに表示される設定については、アプリ開発者にお問い合わせください。

注：

Android版Citrix SSOは、Citrix Secure Accessに名称変更されました。この名称変更を反映するために、ドキュメントを更新しています。

前提条件

- GoogleでAndroid Enterpriseのセットアップタスクを完了し、Android EnterpriseをマネージドGoogle Playに接続します。詳細については、Android Enterpriseを参照してください。
- Android EnterpriseアプリをCitrix Endpoint Managementに追加します。詳細については、Citrix Endpoint Managementへのアプリの追加を参照してください。

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］** に移動します。詳細については、デバイスポリシーを参照してください。

アプリごとのVPNの要件

AE用のアプリごとのVPNを作成するには、マネージド構成デバイスポリシーの設定に加えて、追加の手順を実行する必要があります。また、以下の前提条件が満たされていることを確認する必要があります。

- オンプレミスNetScaler Gateway
- 以下のアプリケーションがデバイスにインストールされています。
  - シトリックス エスエスオー
  - シトリックス セキュアハブ

AEデバイス用のアプリごとのVPNを構成する一般的なワークフローは次のとおりです。

1. この記事で説明されているように、VPNプロファイルを構成します。
2. アプリごとのVPNからのトラフィックを受け入れるようにCitrix ADCを構成します。詳細については、「NetScaler Gatewayでの完全なVPNセットアップ」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

制限事項

Android 11以降のデバイスのAndroid Enterprise環境におけるアプリごとのVPNの制限事項は、Android 11で導入されたパッケージの可視性制限のため、次のとおりです。

- VPNセッションが開始された後に、許可/拒否リストの一部であるアプリがデバイスに展開された場合、エンドユーザーはアプリがVPNセッションを介してトラフィックをルーティングするためにVPNセッションを再起動する必要があります。
- アプリごとのVPNがAlways On VPNセッションを介して使用されている場合、デバイスに新しいアプリをインストールした後、エンドユーザーはアプリのトラフィックがVPNセッションを介してルーティングされるように、ワークプロファイルを再起動するか、デバイスを再起動する必要があります。

注：

Android 23.8.1以降のバージョンのCitrix SSOを使用している場合、これらの制限は適用されません。詳細については、「Always On VPNの自動再起動」を参照してください。

Android Enterprise の設定

管理対象構成デバイスポリシーを追加することを選択すると、アプリを選択するプロンプトが表示されます。Citrix Endpoint Management に Android Enterprise アプリが追加されていない場合、続行できません。

アプリを選択したら、ポリシー設定を構成します。設定はアプリごとに異なります。

デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/android-enterprise-managed-configurations-device-policy-dropbox.png)

Android Enterprise 用の VPN プロファイルを構成する

管理対象構成デバイスポリシーで Citrix SSO アプリを使用して、Android Enterprise デバイスで VPN プロファイルを利用できるようにします。

まず、Citrix SSO を Google Play ストアアプリとして Citrix Endpoint Management コンソールに追加します。「パブリックアプリストアアプリを追加する」を参照してください。

コンソール内の SSO アプリ(/en-us/citrix-endpoint-management/media/citrixsso-app-added.png)

詳細については、このビデオをご覧ください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android デバイスで高度な VPN 管理を構成する方法(/en-us/citrix-endpoint-management/media/shared-video-placeholder.png)

Citrix SSO 用の Android Enterprise 管理対象構成を作成する

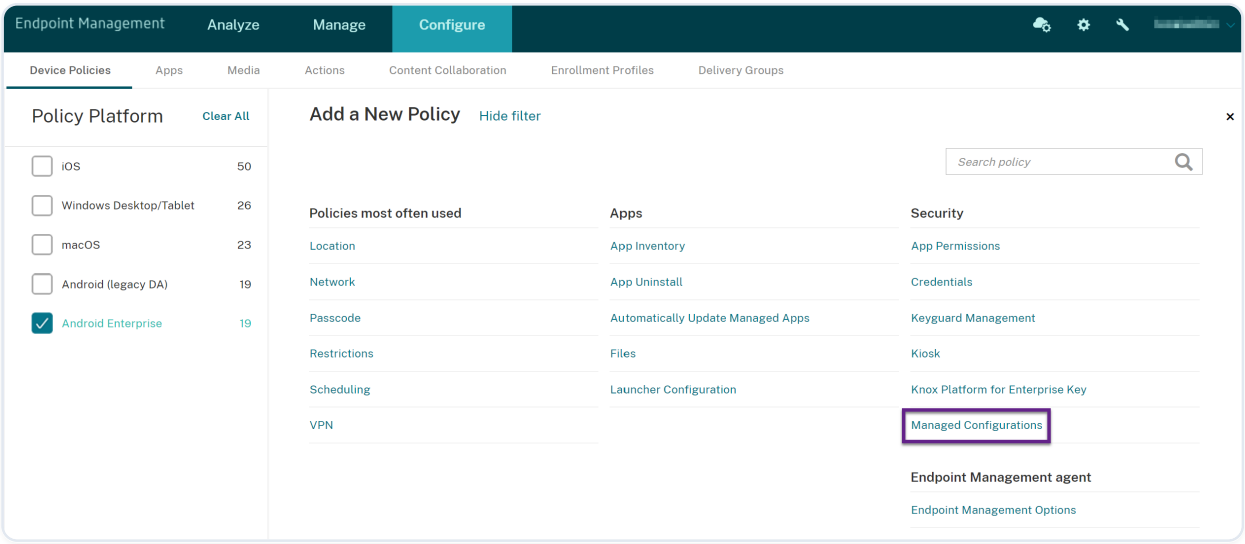
Citrix SSO の管理対象構成デバイスポリシーを構成して、VPN プロファイルを作成します。Citrix SSO アプリがインストールされ、ポリシーが展開されているデバイスは、作成した VPN プロファイルにアクセスできます。

Citrix Endpoint Management は、次の場合にデバイスキーストアのユーザー証明書を使用します。

- NetScaler Gateway が証明書ベースの認証用に構成されている。
- Citrix Endpoint Management ページの **>** で、 が有効になっている。

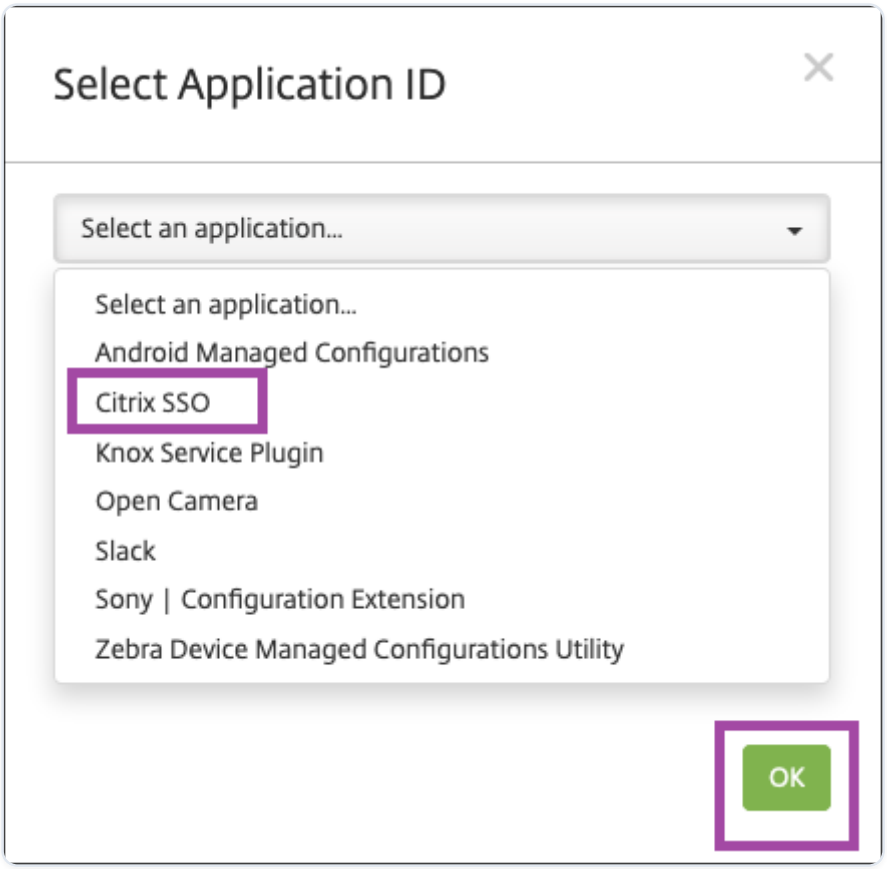
NetScaler Gateway の FQDN とポートが必要です。

1. Citrix Endpoint Managementコンソールで、 **>** の順にクリックします。 をクリックします。
2. を選択します。 をクリックします。

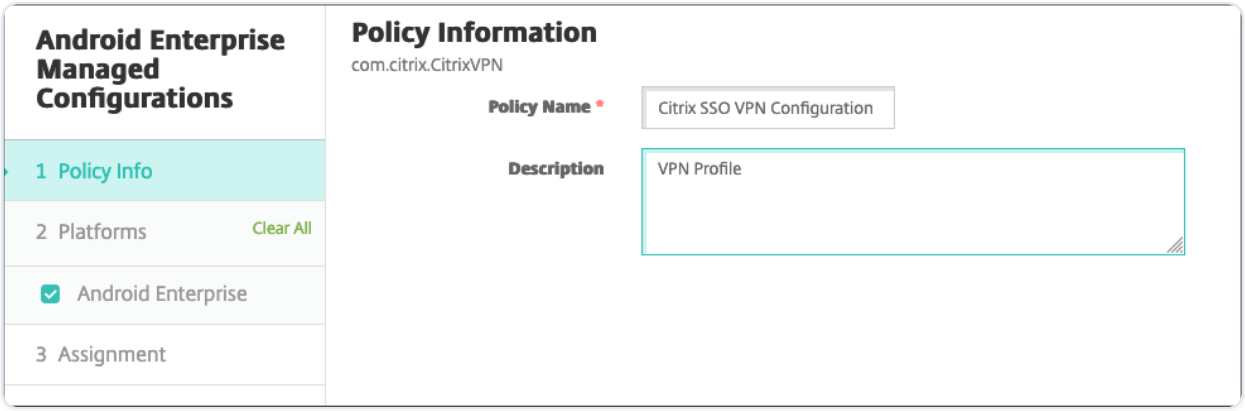


3. ウィンドウが表示されたら、リストから を選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Citrix SSO VPN構成の名前と説明を入力します。 をクリックします。



5. VPNプロファイルパラメーターを構成します。

- **VPNプロファイル名:** VPNプロファイルの名前を入力します。複数のVPNプロファイルを作成する場合は、それぞれに一意の名前を使用します。名前を指定しない場合、 フィールドに入力したアドレスがVPNプロファイル名として使用されます。
- **サーバーアドレス(*):** NetScaler GatewayのFQDNを入力します。NetScaler Gatewayのポートが443でない場合は、ポートも入力します。URL形式を使用します。例： `https://gateway.mycompany.com:8443`。
- **ユーザー名（オプション）：**エンドユーザーがNetScaler Gatewayへの認証に使用するユーザー名を入力します。このフィールドには、Citrix Endpoint Managementマクロ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

{user.username} を使用できます。（マクロを参照）。ユーザー名を指定しない場合、ユーザーがNetScaler Gatewayに接続するときにユーザー名の入力を求められます。

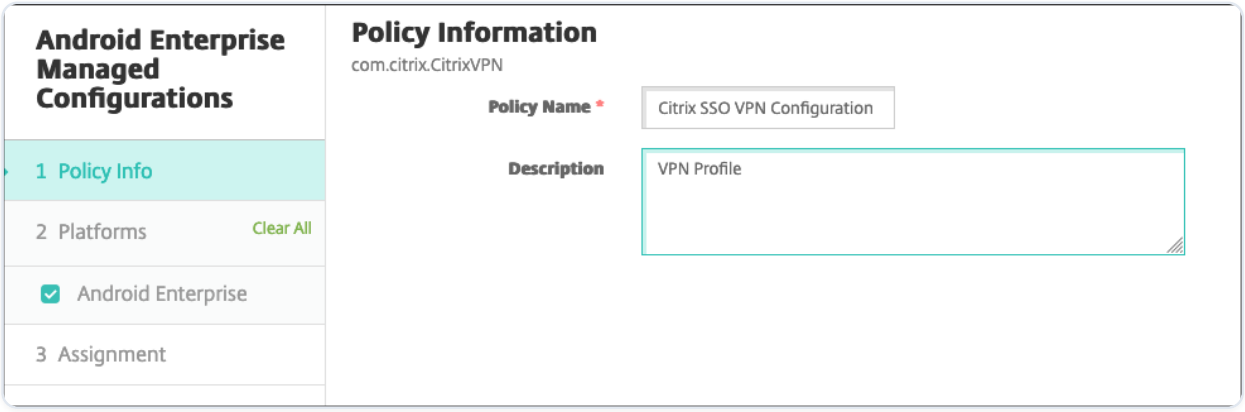
- **パスワード（オプション）：**エンドユーザーがNetScaler Gatewayへの認証に使用するパスワードを入力します。パスワードを指定しない場合、ユーザーがNetScaler Gatewayに接続するときにパスワードの入力を求められます。
- **証明書エイリアス（オプション）：**証明書エイリアスを入力します。証明書エイリアスを使用すると、アプリが証明書にアクセスしやすくなります。資格情報デバイスポリシーで同じ証明書エイリアスを使用すると、アプリは証明書を取得し、ユーザーによる操作なしでVPNを認証します。
- **ゲートウェイ証明書ピン（オプション）：**NetScaler Gatewayに使用される証明書ピンを記述するJSONオブジェクト。値の例：`{"hash-alg" : "sha256", "pinset" : ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="]}`。詳しくは、「Android Citrix SSOでのNetScaler Gateway証明書ピンニング」を参照してください。
- **アプリごとのVPNの種類（オプション）：**アプリごとのVPNを使用して、このVPNを使用するアプリを制限する場合は、この設定を構成できます。 を選択すると、 にリストされているアプリパッケージ名のネットワークトラフィックはVPN経由でルーティングされます。その他のすべてのアプリのネットワークトラフィックはVPN外にルーティングされます。 を選択すると、 にリストされているアプリパッケージ名のネットワークトラフィックはVPN外にルーティングされます。その他のすべてのアプリのネットワークトラフィックはVPN経由でルーティングされます。デフォルトは です。
- **PerAppVPNアプリリスト:** VPNでトラフィックが許可またはブロックされるアプリのリストです。これは**Per-App VPN Type**の値によって異なります。アプリのパッケージ名をコンマまたはセミコロンで区切ってリストします。アプリのパッケージ名は大文字と小文字を区別し、Google Playストアに表示されているとおりにこのリストに正確に記載する必要があります。このリストはオプションです。デバイス全体のVPNをプロビジョニングする場合は、このリストを空のままにします。
- **デフォルトVPNプロファイル:** ユーザーが特定のプロファイルではなくCitrix SSOアプリの接続スイッチをタップしたときに使用するVPNプロファイルの名前を入力します。このフィールドが空の場合、メインプロファイルが接続に使用されます。プロファイルが1つしか構成されていない場合、それはデフォルトプロファイルとしてマークされます。常時接続VPNの場合、このフィールドには常時接続VPNを確立するために使用されるVPNプロファイルの名前を設定する必要があります。
- **常時接続VPN（オプション）：**この属性は、VPNプロファイルが常時接続VPNプロファイルとして構成されているかどうかを示します。**true**に設定すると、VPNプロファイルが常

© 1997–2026 Citrix Systems, Inc. All rights reserved.

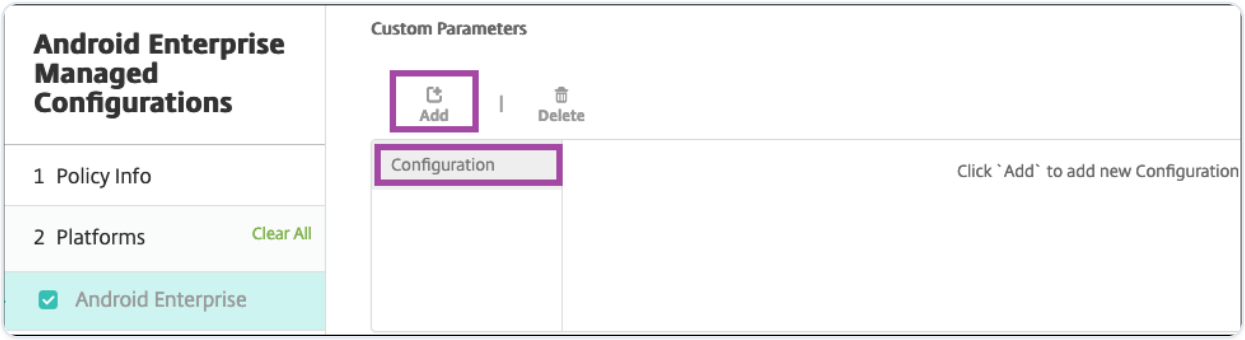
時接続VPNプロファイルであることを意味します。デフォルト値は**false**です。このプロパティは、メインVPNプロファイルにのみ割り当てることができます。このプロパティを有効にすることは、常時接続VPNの信頼性の高い機能性を確保するために不可欠です。

- **ユーザープロファイルの無効化:** この設定がオンの場合、ユーザーは自分のデバイスで独自のVPNを作成できません。この設定がオフの場合、ユーザーは自分のデバイスで独自のVPNを作成できます。デフォルトはオフです。
- **信頼できないサーバーをブロック:** この設定は、以下のいずれかのシナリオでオフになります。
  - NetScaler Gatewayに自己署名証明書を使用する場合
  - NetScaler Gateway証明書を発行するCAのルート証明書がシステムCAリストにない場合。

  この設定がオンの場合、AndroidオペレーティングシステムはNetScaler Gateway証明書を検証します。検証に失敗した場合、接続は許可されません。デフォルト値はオンです。



6. 必要に応じて、カスタムパラメーターを作成します。カスタムパラメーター**XenMobileDeviceId**と**UserAgent**がサポートされています。現在のVPN構成を選択し、**追加**をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメーター名	説明	値
XenMobileDeviceId	このフィールドは、Citrix Endpoint Managementでのデバイス登録に基づくネットワークアクセスチェックに使用するデバイスIDです。Citrix Endpoint Managementがデバイスを登録および管理している場合、VPN接続は許可されます。それ以外の場合、VPN確立時に認証は拒否されます。	Citrix Endpoint Managementがデバイスの登録および管理状態を判断するには、XenMobileDeviceIDの値を `DeviceID_${device.id}` に設定します。
UserAgent	このテキストは、NetScaler Gatewayで追加のチェックを行うためにUser-Agent HTTPヘッダーに追加されます。このテキストの値は、NetScaler Gatewayとの通信中にCitrix SSOアプリによってUser-Agent HTTPヘッダーに追加されます。	User-Agent HTTPヘッダーに追加するテキストを入力します。このテキストは、HTTP User-Agentの仕様に準拠している必要があります。
EnableDebugLogging	Always On VPNの場合にVPN接続の問題のトラブルシューティングに役立つように、Citrix SSOアプリでデバッグログを有効にします。管理対象VPN構成のいずれかで有効にできます。デバッグログは、管理対象構成が処理されるときに有効になります。	**True**: デバッグログを有効にします。デフォルト値: **False**
DisableLogoutFromStoreOnExplicitDisconnect	エンドユーザーがアプリUIからVPNセッションを明示的に切断したときのストアからのログアウトを制御します。Citrix Secure Private	**True**: Secure Private Accessストアからのログアウトを無効にし、Secure Private Accessセッションをそのまま維持し、Citrix Secure Accessアプリセッションの

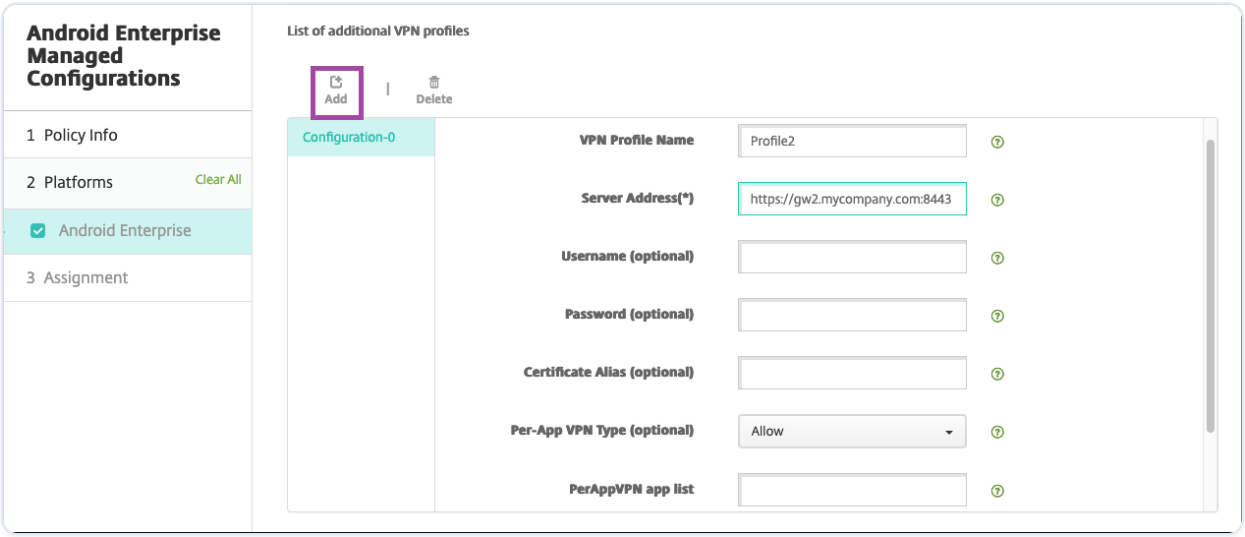
© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメーター名	説明	値
	Access展開にのみ適用されます。	みを切断します。デフォルト値: **False**。



別のカスタムパラメータを作成するには、もう一度 **追加** をクリックします。

7. 必要に応じて、さらにVPNプロファイル構成を作成します。構成リストの下にある **追加** をクリックします。新しい構成がリストに表示されます。新しい構成を選択し、手順5を繰り返し、必要に応じて手順6も繰り返します。



8. 必要なVPNプロファイルをすべて作成したら、**次へ**をクリックします。
9. Citrix SSO のこの管理対象構成の展開規則を構成します。
10. **保存**をクリックします。

Citrix SSO のこの管理対象構成が、構成済みデバイスポリシーのリストに表示されます。

構成したVPNプロファイルで常時接続を有効にするには、(/ja-jp/citrix-endpoint-management/policies/options-policy.html#android-enterprise-settings)を設定します。

注：

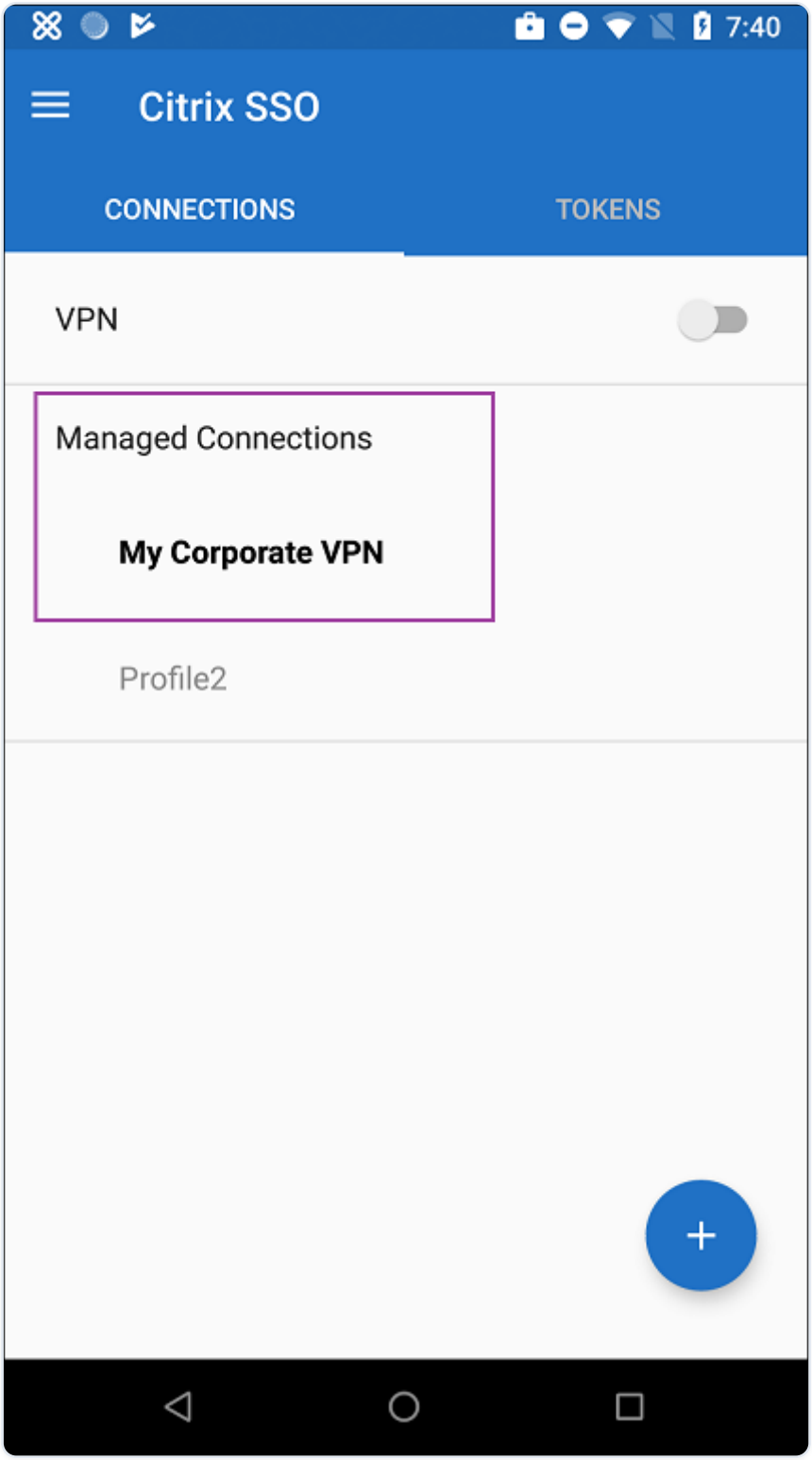
Android Enterprise の常時接続VPNには、Citrix Secure Hub 19.5.5以降が必要です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスからのVPNプロファイルへのアクセス

作成したVPNプロファイルにアクセスするには、Android Enterpriseユーザーは管理対象のGoogle PlayストアからCitrix SSOをインストールします。

構成したVPNプロファイルは、アプリの**管理対象接続**領域に表示されます。ユーザーはVPNプロファイルをタップして、そのVPNプロファイルを使用して接続します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーが認証して接続すると、VPNプロファイルの横にチェックマークが表示されます。キーアイコンは、VPNが接続されていることを示します。

Zebra OEMConfig を使用したZebra Androidデバイスの管理

Zebra Technologies OEMConfig 管理ツールを使用して、Zebra Androidデバイスを管理します。Zebra OEMConfig アプリケーションの詳細については、Zebra Technologies のWebサイトを参照してください。

Citrix Endpoint Management は、Zebra OEMConfig バージョン9.2以降をサポートしています。デバイスにZebra OEMConfig をインストールするためのシステム要件については、Zebra Technologies WebサイトのOEMConfig セットアップを参照してください。

現在、以下のZebraデバイスをサポートしています。

- EC50, EC55, ET56
- TC52x、TC52x-HC モデル
- TC52ax、TC52ax-HC モデル
- TC57x

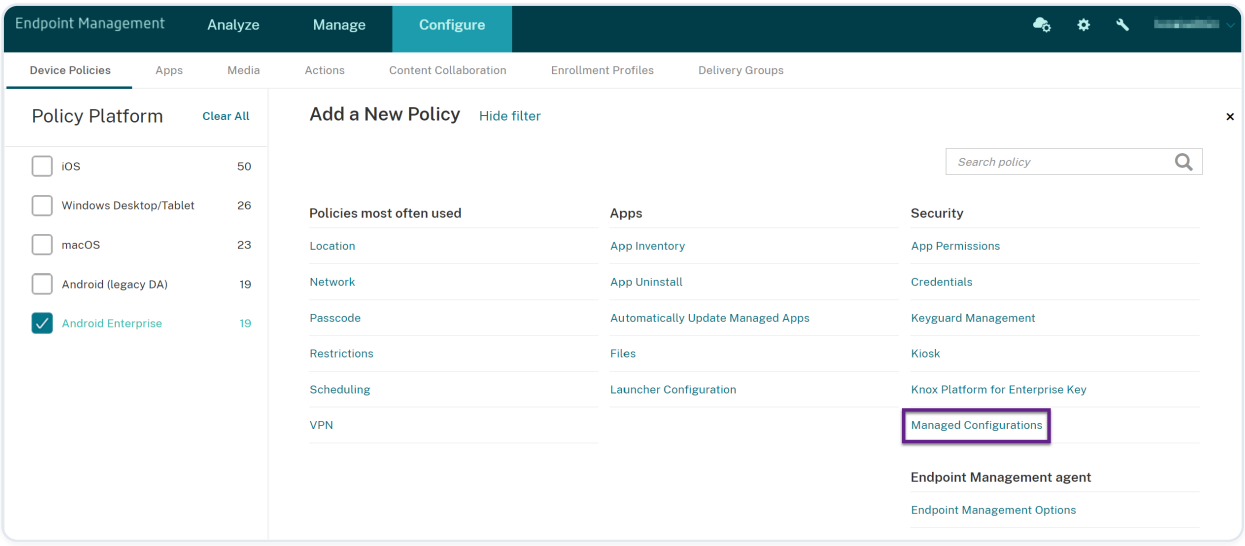
まず、Citrix Endpoint Managementコンソールで、Zebra OEMConfigアプリをGoogle Playストアアプリとして追加します。「パブリックアプリストアアプリの追加」を参照してください。

Zebra OEMConfigアプリのAndroid Enterprise管理対象構成を作成する

Zebra OEMConfigアプリの管理対象構成デバイスポリシーを構成します。このポリシーは、Zebra OEMConfigアプリがインストールされ、ポリシーが展開されているZebraデバイスに適用されます。

1. Citrix Endpoint Managementコンソールで、 > の順にクリックします。 をクリックします。
2. を選択します。 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. ウィンドウが表示されたら、リストから を選択し、 をクリックします。
4. Zebra OEMConfig構成の名前と説明を入力します。 をクリックします。
5. Zebra OEMConfig構成の名前を入力します。
6. 利用可能なパラメーターを構成します。例:

   - デバイス前面のカメラを無効にするには、**カメラ構成**を選択し、**前面カメラの使用**を**オフ**に設定します。
   - デバイスの時刻形式を変更するには、**クロック構成**を選択し、**時刻形式**を**12** (12時間形式) または **24** (24時間形式) に設定します。

利用可能なすべての構成のリストと説明については、Zebra TechnologiesのWebサイトでZebra Managed Configurationsを参照してください。

1. 必要に応じて、Zebra OEMConfig構成をさらに作成します。構成のリストの下にある**追加**をクリックします。新しい構成がリストに表示されます。新しい構成を選択し、パラメーターを設定します。
2. 必要なZebra OEMConfig構成をすべて作成したら、**次へ**をクリックします。
3. Zebra OEMConfigのこの管理対象構成の展開ルールを構成します。
4. **保存**をクリックします。

事前定義されたブックマークでChromeブラウザを管理する

事前定義されたブックマークでChromeブラウザを管理する方法の例を次に示します。

```
[
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{ "toplevel_name": "My managed bookmarks folder" }

,



{ "name": "Google", "url": "[google.com|http://google.com/]" }

,



{ "name": "Youtube", "url": "[youtube.com|http://youtube.com/]" }

,

{

"nested_links": [



{ "name": "Chromium", "url": "[chromium.org|http://chromium.org/]" }

,



{ "name": "Chromium Developers", "url": "[dev.chromium.org|http://
dev.chromium.org/]" }

],

"name": "Chrome links"

}

]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理対象構成フィードバックのサポート (テクニカルプレビュー)

管理対象構成フィードバック機能のサポートの詳細については、Support managed configurations feedbackを参照してください。

マネージド ドメイン デバイス ポリシー

メールとSafariブラウザに適用されるマネージド ドメインを定義できます。マネージド ドメインは、Safariを使用してドメインからダウンロードされたドキュメントをどのアプリで開くことができるかを制御することで、企業データを保護するのに役立ちます。

iOS監視対象デバイスの場合、以下を指定します。

- ユーザーがブラウザからドキュメント、添付ファイル、ダウンロードを開く方法を制御するためのURLまたはサブドメイン。
- ユーザーがSafariでパスワードを保存できるURL。

iOSデバイスを監視モードに設定する手順については、「Apple Configurator 2を使用してデバイスを展開する」を参照してください。

ユーザーがマネージド メール ドメイン リストにないドメインの受信者にメールを送信すると、そのメッセージはユーザーのデバイスでフラグが立てられ、企業ドメイン外の相手にメッセージを送信していることが警告されます。

ドキュメント、添付ファイル、ダウンロードなどの項目について：ユーザーがマネージド Web ドメイン リストにある Web ドメインから Safari を使用して項目を開くと、適切な企業アプリがその項目を開きます。項目がマネージド Web ドメイン リストにある Web ドメインからのものでない場合、ユーザーは企業アプリでその項目を開くことができません。個人用の管理されていないアプリを使用する必要があります。

監視対象デバイスの場合、Safariのパスワード自動入力ドメインを指定しない場合でも、デバイスが一時的なマルチユーザーとして構成されている場合、ユーザーはパスワードを保存できません。ただし、デバイスが一時的なマルチユーザーとして構成されていない場合、ユーザーはすべてのパスワードを保存できます。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイス ポリシー」を参照してください。

iOS設定

ドメインを指定するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

形式	説明
`example.com`	`example.com`以下の任意のパスを管理対象としますが、`site.example.com/`は管理対象としません。
`foo.example.com`	`foo.example.com`以下の任意のパスを管理対象としますが、`example.com/`または`bar.example.com/`は管理対象としません。
`*.example.com`	`foo.example.com`または`bar.example.com`以下の任意のパスを管理対象としますが、`example.com/`は管理対象としません。
`example.com/sub`	`example.com/sub`とその下の任意のパスを管理対象としますが、`example.com/`は管理対象としません。
`foo.example.com/sub`	`foo.example.com/sub`以下の任意のパスを管理対象としますが、`example.com`、`example.com/sub`、`foo.example.com/`、または`bar.example.com/sub`は管理対象としません。
`*.example.com/sub`	`foo.example.com/sub`または`bar.example.com/sub`以下の任意のパスを管理対象としますが、`example.com`または`foo.example.com/`は管理対象としません。

ルール:

- ドメインを比較する際、URLの先頭の「www.」と末尾のスラッシュは無視されます。
- エントリにポート番号がある場合、そのポート番号を指定するアドレスのみが管理対象と見なされます。それ以外の場合、標準ポート（httpの場合はポート80、httpsの場合はポート443）のみが管理対象と見なされます。たとえば、パターン`*.example.com:8080`は`https://site.example.com:8080/page.html`に一致しますが、`https://site.example.com/page.html`には一致しません。しかし、パターン`*.example.com`は`https://site.example.com/page.html`と`https://site.example.com/page.html`に一致しますが、`https://site.example.com:8080/page.html`には一致しません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 管理対象のSafari Webドメイン定義は累積的です。すべての管理対象Safari Webドメインペイロードによって定義されたパターンは、URLリクエストを照合するために使用されます。

設定:

- **管理対象ドメイン**
  - **マークなしのメール ドメイン:** リストに含める各メール ドメインについて、**追加**をクリックしてから、次の操作を行います。
    - **管理対象メール ドメイン:** メール ドメインを入力します。
    - **保存**をクリックしてメール ドメインを保存するか、**キャンセル**をクリックしてメール ドメインを保存しないようにします。
  - **管理対象 Safari Web ドメイン:** リストに含める各 Web ドメインについて、**追加**をクリックしてから、次の操作を行います。
    - **管理対象 Web ドメイン:** Web ドメインを入力します。
    - **保存**をクリックして Web ドメインを保存するか、**キャンセル**をクリックして Web ドメインを保存しないようにします。
  - **Safari パスワード自動入力ドメイン:** リストに含める各自動入力ドメインについて、**追加**をクリックしてから、次の操作を行います。
    - **Safari パスワード自動入力ドメイン:** 自動入力ドメインを入力します。
    - **保存**をクリックして自動入力ドメインを保存するか、**キャンセル**をクリックして自動入力ドメインを保存しないようにします。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

最大常駐ユーザーデバイスポリシー

最大常駐ユーザーデバイスポリシーは、iOS (iPadOS) を実行している共有デバイス用です。共有iPadの詳細については、「Apple Education機能との統合」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

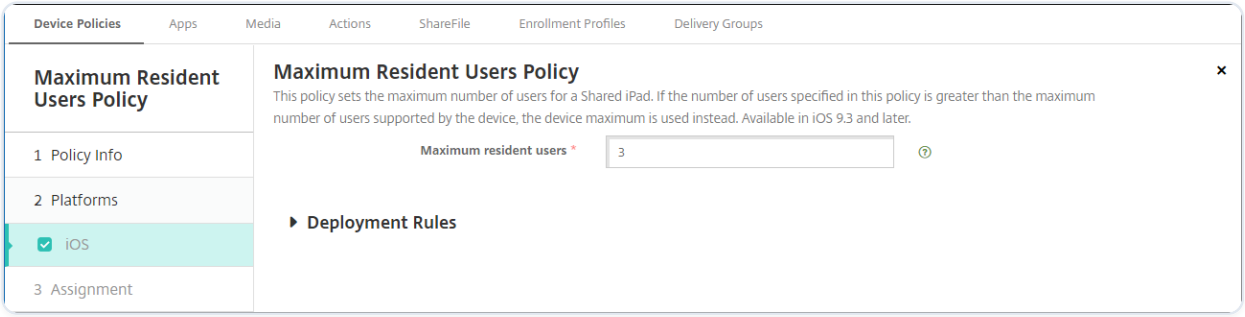
このポリシーは、iPadがセットアップアシスタント中に「構成待ち」フェーズにあるときに展開する必要があります。Appleは、共有iPadが登録された後にこのポリシーを展開することを許可していません。

このポリシーを追加または構成するには、**「構成」>「デバイスポリシー」**に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **最大常駐ユーザー数:** 共有iPadの最大ユーザー数。このポリシーで指定されたユーザー数がデバイスでサポートされる最大ユーザー数よりも多い場合、Citrix Endpoint Managementは代わりにデバイスの最大値を使用します。デフォルトは**5**ユーザーです。

  Appleは、最大常駐ユーザーの値を可能な限り低く保つことを推奨しています。値が低いほど、各ユーザーのiPadストレージ容量が最大化されます。また、値が低いほどiCloudとの通信が最小限に抑えられ、サインインエクスペリエンスが高速になります。AppleがiPadで共有ストレージを処理する方法については、`<https://developer.apple.com/education/shared-ipad/>`を参照してください。



MDMオプションデバイスポリシー

MDMオプションデバイスポリシーは、監視対象のiOSデバイスで「iPhoneを探す/iPadを探す」のアクティベーションロックを管理します。iOSデバイスを監視モードに設定する手順については、「Apple Configurator 2を使用してデバイスを展開する」(/ja-jp/citrix-endpoint-management/device-management/apple/ios-bulk-enrollment.html#deploy-devices-using-apple-configurator-2)を参照してください。

アクティベーションロックは、「iPhoneを探す/iPadを探す」の機能で、紛失または盗難された監視対象デバイスの再アクティベーションを防止します。アクティベーションロックは、誰かが「iPhoneを探す/iPadを探す」をオフにしたり、デバイスを消去したり、デバイスを再アクティベートしたりする前に、ユーザーのApple IDとパスワードを要求します。組織が所有するデバイス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

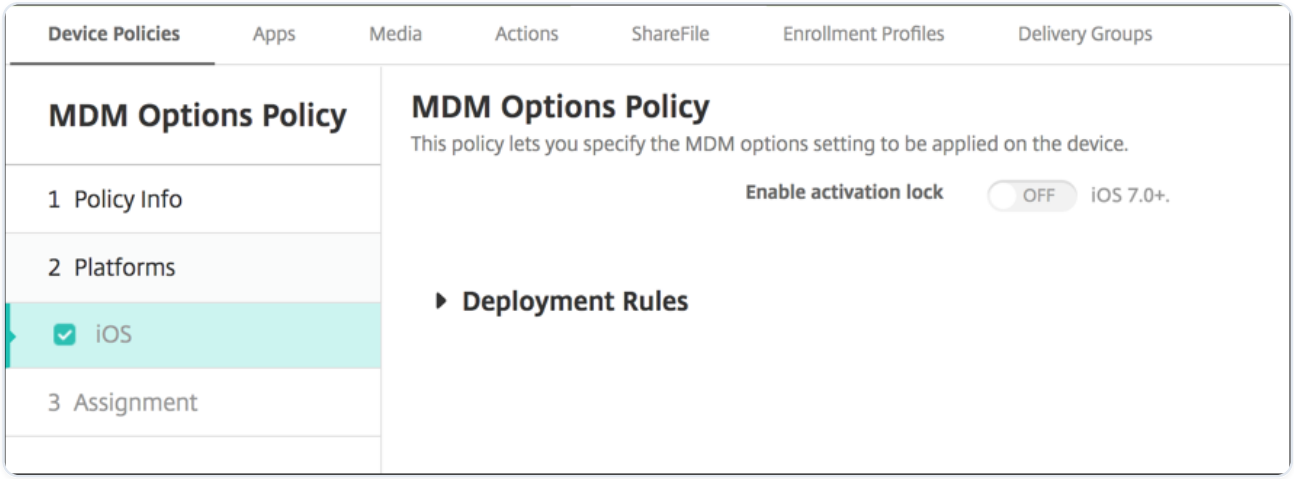
の場合、例えばデバイスをリセットしたり再割り当てしたりするために、アクティベーションロックをバイパスする必要があります。

アクティベーションロックを有効にするには、Citrix Endpoint Management MDMオプションデバイスポリシーを構成して展開します。その後、ユーザーのApple資格情報なしでCitrix Endpoint Managementコンソールからデバイスを管理できます。アクティベーションロックのApple資格情報要件をバイパスするには、Citrix Endpoint Managementコンソールから「アクティベーションロックバイパス」セキュリティアクションを発行します。

例えば、ユーザーが紛失した電話を返却した場合や、完全ワイプの前後にデバイスを設定する場合：電話がApple App Storeアカウントの資格情報を要求したときに、Citrix Endpoint Managementコンソールから「アクティベーションロックバイパス」セキュリティアクションを発行することで、その手順をバイパスできます。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」(/ja-jp/citrix-endpoint-management/policies.html)を参照してください。

iOS設定



- **アクティベーションロックを有効にする：** このポリシーを展開するデバイスでアクティベーションロックを有効にするかどうかを選択します。デフォルトは です。

MDMオプションデバイスポリシーを展開してアクティベーションロックを有効にすると、 > ページでそれらのデバイスを選択し、 をクリックすると、セキュリティアクション が表示されます。アクティベーションロックバイパスを使用すると、デバイスユーザーのApple IDとパスワードを知らなくても、デバイスのアクティベーション前に監視対象デバイスからアクティベーションロックを解除できます。完全ワイプの前後にデバイスにアクティベーションロックバイパスを送信できます。詳細については、「iOSアクティベーションロックをバイパスする」(/ja-jp/citrix-endpoint-management/device-management/apple/ios.html#bypass-an-ios-activation-lock)を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネットワークデバイスポリシー

ネットワークデバイスポリシーを使用すると、以下の項目を定義することで、ユーザーがデバイスをWi-Fiネットワークに接続する方法を管理できます。

- ネットワーク名と種類
- 認証およびセキュリティポリシー
- プロキシサーバーの使用
- その他のWi-Fi関連の詳細

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］**の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

前提条件

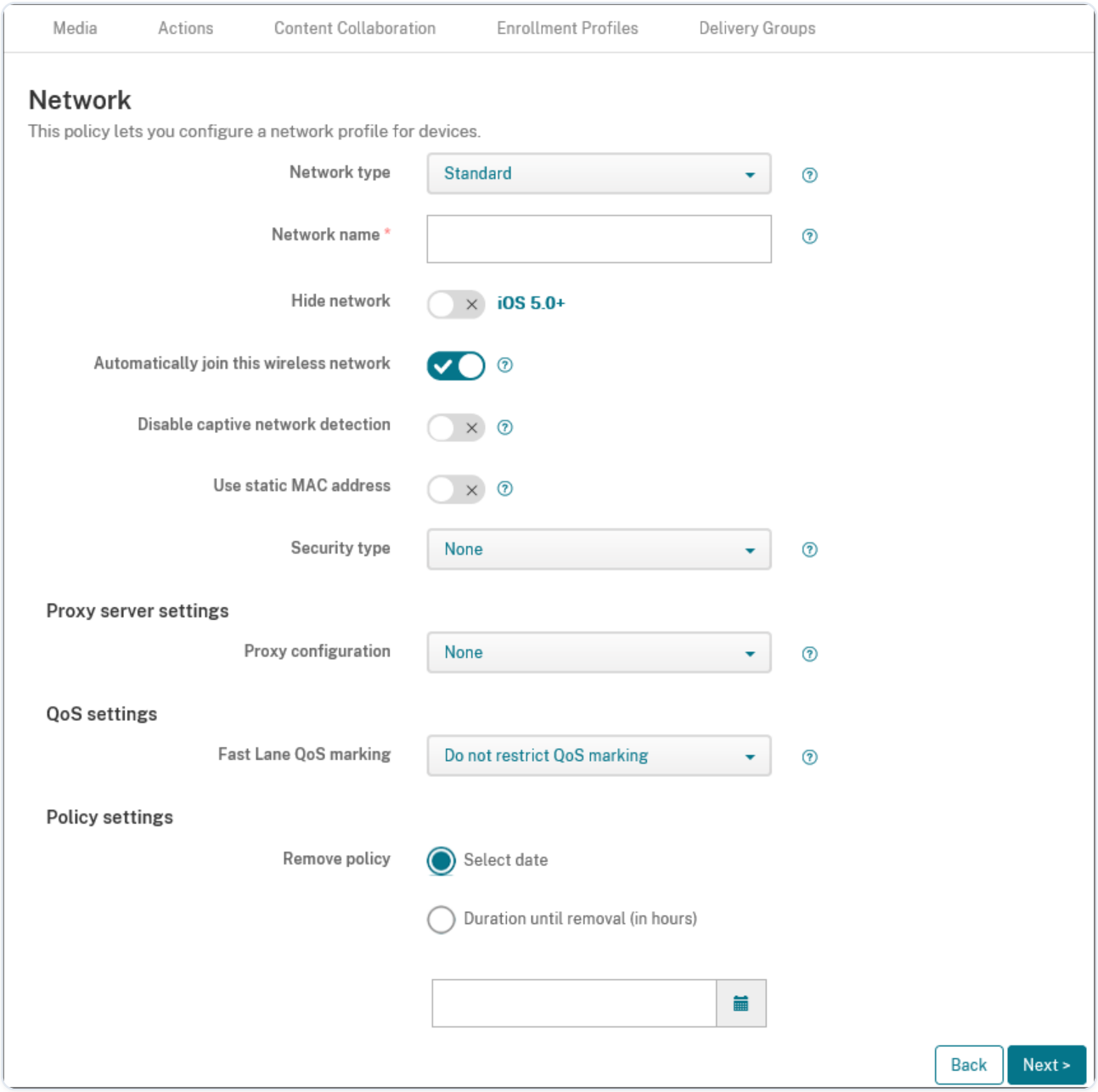
ポリシーを作成する前に、以下を完了してください。

- 使用する予定のデリバリーグループを作成します。
- ネットワーク名と種類を把握します。
- 使用する予定の認証またはセキュリティの種類を把握します。
- 必要となる可能性のあるプロキシサーバー情報を把握します。
- 必要なCA証明書をインストールします。
- 必要な共有キーを用意します。
- 証明書ベースの認証用のPKIエンティティを作成します。
- 資格情報プロバイダーを構成します。

詳細については、認証とそのサブ記事を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定



- **ネットワークの種類:** リストから、使用する予定のネットワークの種類として、**Standard**、**Legacy Hotspot**、または**Hotspot 2.0**を選択します。
- **ネットワーク名:** デバイスで利用可能なネットワークのリストに表示されるSSIDを入力します。**Hotspot 2.0**には適用されません。
- **ネットワークを非表示にする:** ネットワークを非表示にするかどうかを選択します。
- **このワイヤレスネットワークに自動的に参加する:** デバイスがネットワークに自動的に参加するかどうかを選択します。デバイスが別のネットワークに接続されている場合、このネットワークには参加しません。デバイスが自動的に接続する前に、ユーザーは以前のネットワークから切断する必要があります。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **キャプティブネットワーク検出を無効にする:** キャプティブネットワークアシスタントは、ユーザーがサブスクリプションまたはWi-Fiホットスポットネットワークにアクセスするのに役立ちます。これらのネットワークは通常、コーヒーショップ、ホテル、その他の公共の場所で見られます。**オン**の場合、デバイスはキャプティブネットワークに接続できますが、ユーザーはブラウザを開いて手動でログインする必要があります。デフォルトは**オフ**です。
- **静的MACアドレスを使用する:** MACアドレスは、デバイスがネットワーク内で送信する一意の識別子です。プライバシーを強化するために、iOSおよびiPadOSデバイスは、ネットワークに接続するたびに異なるMACアドレスを使用できます。**オン**の場合、デバイスはこのネットワークに接続するときに常に同じMACアドレスを使用します。**オフ**の場合、デバイスはこのネットワークに接続するたびに異なるMACアドレスを使用します。デフォルトは**オフ**です。
- **セキュリティの種類:** リストから、使用する予定のセキュリティの種類を選択します。**Hotspot 2.0**には適用されません。
  - なし - それ以上の構成は不要です。
  - WEP
  - WPA/WPA2/WPA3パーソナル
  - 任意 (個人用)
  - WEPエンタープライズ
  - WPA/WPA2/WPA3 Enterprise: Windows 10の最新リリースでは、WPA-2 Enterpriseを使用するようにSimple Certificate Enrollment Protocol (SCEP) を構成します。その後、Citrix Endpoint Managementは、Wi-Fiサーバーへの認証のために証明書をデバイスに送信できます。SCEPを構成するには、**［設定］>［資格情報プロバイダー］**の［配信］ページに移動します。詳しくは、「資格情報プロバイダー」を参照してください。
  - 任意 (エンタープライズ)

次のセクションでは、上記の各接続タイプに対して構成するオプションを一覧表示します。

- **プロキシサーバー設定**
  - **プロキシ構成:** リストで、VPN接続がプロキシサーバーを介してルーティングされる方法を設定するために、**［なし］**、**［手動］**、または**［自動］を選択し、追加のオプションを構成します。デフォルトは**［なし］**で、これ以上構成する必要はありません。
  - **［手動］**を選択した場合は、次の設定を構成します。
    - **ホスト名またはIPアドレス:** プロキシサーバーのホスト名またはIPアドレスを入力します。
    - **ポート:** プロキシサーバーのポート番号を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **ユーザー名:** プロキシサーバーへの認証に使用するオプションのユーザー名を入力します。
    - **パスワード:** プロキシサーバーへの認証に使用するオプションのパスワードを入力します。
  - **［自動］**を選択した場合は、次の設定を構成します。
    - **サーバーURL:** プロキシ構成を定義するPACファイルのURLを入力します。
    - **PACに到達できない場合に直接接続を許可:** PACファイルに到達できない場合に、ユーザーが宛先に直接接続することを許可するかどうかを選択します。デフォルトは**［オン］**です。

- **Fast Lane QoSマーキング:** Cisco Fast Lane QoSをサポートするWi-FiネットワークでQoSマーキングを制限しない場合、すべてのアプリがL2およびL3マーキングを使用できます。QoSマーキングを制限する場合は、L2およびL3マーキングを使用できるアプリを指定します。
  - **QoSマーキングを有効にする:** QoSマーキングを制限する場合、この設定を使用して完全に無効にするか、特定のアプリのみをマーキングします。**オフ**の場合、QoSマーキングは完全に無効になります。**オン**の場合、QoSマーキングを使用できるアプリのリストを設定します。デフォルトは**オン**です。
  - **Appleオーディオ/ビデオ通話を許可する:** オーディオおよびビデオ通話アプリがQoSマーキングを使用できるかどうかを選択します。**オフ**の場合、ビデオ通話とオーディオ通話の品質が低下する可能性があります。
  - **特定のアプリを許可する:** アプリがQoSマーキングを使用できるように、このリストにアプリパッケージIDを追加します。

- **Hotspot 2.0設定**
  - **表示されるオペレーター名:** Hotspotデバイスによってブロードキャストされるフレンドリ名。ユーザーは利用可能なWi-Fiネットワークのリストでこの名前を確認します。
  - **ドメイン名:** Hotspot 2.0ネゴシエーションに使用されるドメイン名。
  - **ローミングパートナーネットワークへの接続を許可する: オン**の場合、ホームネットワークからローミングしているデバイスはパートナーネットワークに接続できます。
  - **ローミングコンソーシアム組織識別子 (OI):** デバイスがアクセスできる組織識別子のリストを追加します。ローミングコンソーシアムOIは、共有認証方法を持つ組織に属します。設定したHotspotが利用できない場合、デバイスはここにリストされているローミングコンソーシアムOIに接続します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ネットワークアクセス識別子 (NAI) レルム名:** ローミングネットワークのユーザーを識別するために使用されるレルム名のリストを設定します。NAIは`user@realm`の形式で送信されます。
- **モバイル国コード (MCC) およびモバイルネットワーク構成 (MNC):** モバイル国コードは、ネットワークの国を識別する3桁の数字で構成されます。モバイルネットワークコードは、2桁または3桁の一意の数字で構成されます。MCC/MNCを一緒に使用すると、モバイルネットワークオペレーターまたはキャリアを一意に識別できます。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除の特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから、**常に許可**、**パスコードが必要**、または**許可しない**を選択します。**パスコードが必要**を選択した場合、**削除パスコード**フィールドにパスコードを入力します。iOSでは利用できません。

iOSにおけるWPA、WPA Personal、Any (Personal) の構成設定

パスワード: オプションのパスワードを入力します。このフィールドを空白のままにすると、ユーザーはログオン時にパスワードの入力を求められる場合があります。

iOS向けWEP Enterprise、WPA Enterprise、WPA2 Enterprise、WPA3 Enterprise、任意の (エンタープライズ) の設定

これらのセキュリティタイプのいずれかを選択すると、**QoS設定**の後に**EAP**設定が表示されます。

重要:

WPA2 Enterpriseセキュリティタイプを選択した場合、少なくとも1つのEAPプロトコルを許可する必要があります。

- **許可されるEAPプロトコル:** サポートするEAPタイプを有効にし、関連する設定を構成します。利用可能な各EAPタイプのデフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

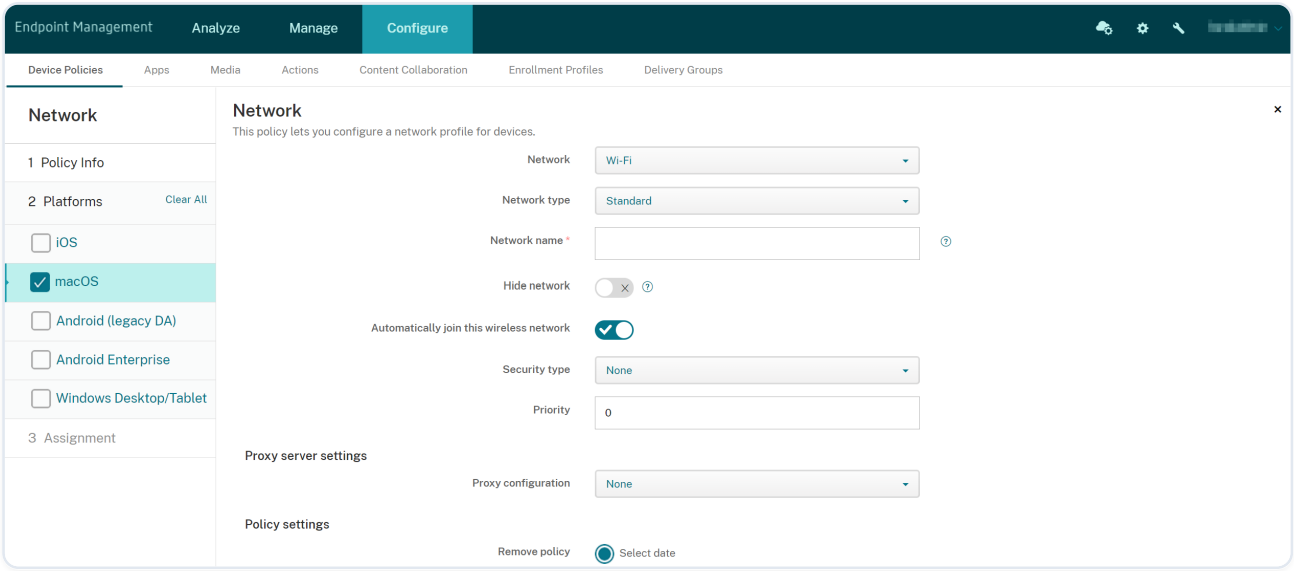
- **内部認証 (TTLS):** *TTLSを有効にした場合にのみ必要*。リストから、使用する内部認証方法を選択します。オプションは、**PAP**、**CHAP**、**MSCHAP**、または**MSCHAPv2**です。デフォルトは**MSCHAPv2**です。
- **PACを使用したEAP-FAST:** 保護されたアクセス資格情報 (PAC) を使用するかどうかを選択します。
  - **PACを使用**を選択した場合、プロビジョニングPACを使用するかどうかを選択します。
    - **プロビジョニングPAC**を選択した場合、エンドユーザークライアントとCitrix Endpoint Managementの間で匿名TLSハンドシェイクを許可するかどうかを選択します。
      - **匿名でPACをプロビジョニング**
- **認証:**
  - **ユーザー名:** ユーザー名を入力します。
  - **接続ごとのパスワード:** ユーザーがログオンするたびにパスワードを要求するかどうかを選択します。
  - **パスワード:** オプションのパスワードを入力します。このフィールドを空白のままにすると、ユーザーはログオン時にパスワードの入力を求められる場合があります。
  - **ID資格情報 (キーストアまたはPKI資格情報):** リストからID資格情報の種類を選択します。デフォルトは**なし**です。
  - **外部ID: PEAP**、**TTLS**、*または* **EAP-FAST***を有効にした場合にのみ必要です*。外部から見えるユーザー名を入力します。ユーザー名が見えないように「anonymous」のような一般的な用語を入力することで、セキュリティを強化できます。
  - **TLS証明書を要求する:** TLS証明書を要求するかどうかを選択します。
- **信頼**
  - **信頼された証明書:** 信頼された証明書を追加するには、**追加**をクリックし、追加する各証明書について以下を実行します。
    - **アプリケーション:** リストから追加するアプリケーションを選択します。
    - **保存**をクリックして証明書を保存するか、**キャンセル**をクリックします。
  - **信頼されたサーバー証明書名:** 信頼されたサーバー証明書の共通名を追加するには、**追加**をクリックし、追加する各名前について以下を実行します。
    - **証明書:** サーバー証明書の名前を入力します。wpa.*.example.com のようにワイルドカードを使用して名前を指定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **保存**をクリックして証明書名を保存するか、**キャンセル**をクリックします。

- **信頼例外を許可する:** 証明書が信頼されていない場合に、ユーザーデバイスに証明書の信頼ダイアログが表示されるかどうかを選択します。デフォルトは**オン**です。

macOS設定



- **ネットワーク**：リストから、使用するネットワークオプションを選択します。デフォルトは**Wi-Fi**です。
  - ワイファイ
  - グローバルイーサネット
  - 最初のアクティブイーサネット
  - 2番目のアクティブイーサネット
  - 3番目のアクティブイーサネット
  - 最初のイーサネット
  - 2番目のイーサネット
  - 3番目のイーサネット
- **ネットワークの種類**：リストから、使用するネットワークの種類を設定するために、**Standard**、**Legacy Hotspot**、または**Hotspot 2.0**を選択します。
- **ネットワーク名**：デバイスで利用可能なネットワークのリストに表示されるSSIDを入力します。**Hotspot 2.0**には適用されません。
- **ネットワークを非表示にする**：ネットワークを非表示にするかどうかを選択します。
- **このワイヤレスネットワークに自動的に参加する**：ネットワークに自動的に参加するかどうかを選択します。デバイスがすでに別のネットワークに接続されている場合、このネットワーク

© 1997–2026 Citrix Systems, Inc. All rights reserved.

には参加しません。デバイスが自動的に接続する前に、ユーザーは以前のネットワークから切断する必要があります。デフォルトは**オン**です。

- **セキュリティの種類**：リストから、使用するセキュリティの種類を選択します。**Hotspot 2.0** には適用されません。
  - なし - それ以上の設定は不要です。
  - WEP
  - WPA/WPA2 パーソナル
  - 任意 (パーソナル)
  - WEP エンタープライズ
  - WPA/WPA2 エンタープライズ
  - 任意 (エンタープライズ)

  以下のセクションでは、上記の各接続タイプに対して構成するオプションを一覧表示します。
- **優先度:** 複数のネットワークの場合、ネットワーク接続の優先度を定義する数値を入力します。デバイスは、最も低い優先度番号のネットワークに最初に接続します。負の数も使用できます。デフォルトは **0** です。
- **プロキシサーバー設定**
  - **プロキシ構成:** リストから **なし**、**手動**、または **自動** を選択して、VPN 接続がプロキシサーバー経由でルーティングされる方法を設定し、追加のオプションを構成します。デフォルトは **なし** で、それ以上の構成は不要です。
  - **手動** を選択した場合、以下の設定を構成します。
    - **ホスト名またはIPアドレス:** プロキシサーバーのホスト名またはIPアドレスを入力します。
    - **ポート:** プロキシサーバーのポート番号を入力します。
    - **ユーザー名:** プロキシサーバーへの認証に使用するオプションのユーザー名を入力します。
    - **パスワード:** プロキシサーバーへの認証に使用するオプションのパスワードを入力します。
  - **Automatic** を選択した場合、以下の設定を構成します。
    - **サーバーURL:** プロキシ構成を定義するPACファイルのURLを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **PACに到達できない場合に直接接続を許可する:** PACファイルに到達できない場合に、ユーザーが宛先に直接接続することを許可するかどうかを選択します。デフォルトは **On** です。

- **Hotspot 2.0設定**

    - **表示されるオペレーター名:** ホットスポットデバイスによってブロードキャストされるフレンドリ名。ユーザーは利用可能なWi-Fiネットワークのリストでこの名前を確認します。
    - **ドメイン名:** Hotspot 2.0ネゴシエーションに使用されるドメイン名。
    - **ローミングパートナーネットワークへの接続を許可する: On** の場合、ホームネットワークからローミングしているデバイスはパートナーネットワークに接続できます。
    - **ローミングコンソーシアム組織識別子 (OI):** デバイスがアクセスできる組織識別子のリストを追加します。ローミングコンソーシアムOIは、共有認証方法を持つ組織に属します。構成したホットスポットが利用できない場合、デバイスはここにリストされているローミングコンソーシアムOIに接続します。
    - **ネットワークアクセス識別子 (NAI) レルム名:** ローミングネットワークにユーザーを識別するために使用されるレルム名のリストを構成します。NAIは `user@realm` の形式で送信されます。
    - **モバイル国コード (MCC) およびモバイルネットワーク構成 (MNC):** モバイル国コードは、ネットワークの国を識別する3桁の数字で構成されます。モバイルネットワークコードは、2桁または3桁の一意の数字で構成されます。これらを一緒に使用すると、MCC/MNCはモバイルネットワークオペレーターまたはキャリアを一意に識別します。

- **ポリシー設定**

    - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは **日付を選択** と **削除までの期間 (時間)** です。
        - **日付を選択:** カレンダーをクリックして、削除の特定の日付を選択します。
        - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。
    - **ユーザーによるポリシーの削除を許可する:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから **常に**、**パスコードが必要**、または **しない** を選択します。**パスコードが必要** を選択した場合は、**削除パスコード** フィールドにパスコードを入力します。
    - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、システム全体 (**システム**) に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOSのWPA、WPAパーソナル、WPA 2パーソナル、任意（パーソナル）設定

- **パスワード:** オプションのパスワードを入力します。このフィールドを空白のままにすると、ユーザーはログオン時にパスワードの入力を求められる場合があります。

macOSのWEPエンタープライズ、WPAエンタープライズ、WPA2エンタープライズ、任意（エンタープライズ）設定

- **接続モード: オン**の場合、ユーザーがネットワークに参加するときに使用する接続モードを選択します。デフォルトは**オフ**です。
  - **システム:** チェックされている場合、デバイスはシステム資格情報を使用してユーザーを認証します。デフォルトはクリアされています。
  - **ログインウィンドウ:** チェックされている場合、デバイスはログインウィンドウで入力されたのと同じ資格情報を使用してユーザーを認証します。デフォルトはクリアされています。

これらのセキュリティタイプのいずれかを選択すると、**QoS設定**の後に**EAP**設定が表示されます。

重要:

WPA2 Enterpriseセキュリティタイプを選択した場合、少なくとも1つのEAPプロトコルを許可する必要があります。

- **許可されるEAPプロトコル:** サポートするEAPタイプを有効にし、関連する設定を構成します。利用可能な各EAPタイプのデフォルトは**オフ**です。
- **内部認証 (TTLS):** *TTLSを有効にした場合にのみ必要です。*リストから使用する内部認証方法を選択します。オプションは、**PAP**、**CHAP**、**MSCHAP**、または**MSCHAPv2**です。デフォルトは**MSCHAPv2**です。
- **PACを使用したEAP-FAST:** 保護されたアクセス資格情報 (PAC) を使用するかどうかを選択します。
  - **PACを使用**を選択した場合、プロビジョニングPACを使用するかどうかを選択します。
    - **プロビジョニングPAC**を選択した場合、エンドユーザークライアントとCitrix Endpoint Managementの間で匿名TLSハンドシェイクを許可するかどうかを選択します。
      - **PACを匿名でプロビジョニング**
- **認証:**

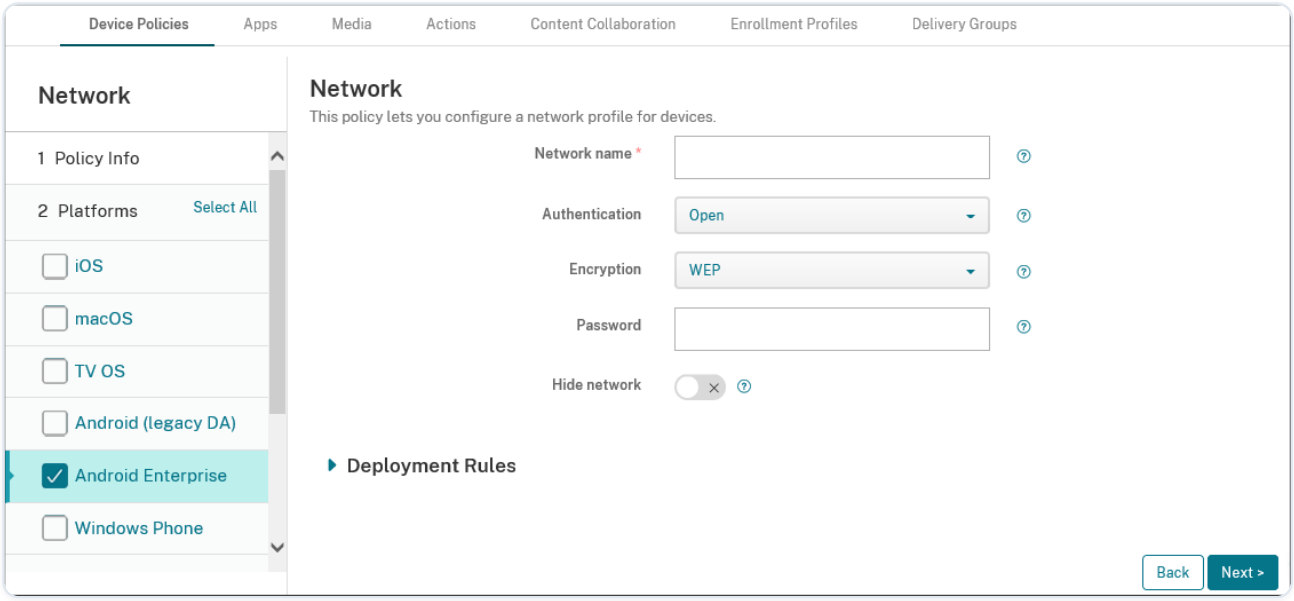
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Active Directory認証を使用:** Active Directory認証を有効にするかどうかを選択します。macOS 10.7以降で利用可能です。このオプションを有効にするには、以下を完了してください:
  - EAPプロトコルとして**PEAP**を設定します。
  - プロファイルスコープを**システム**に設定します。この設定オプションは、ポリシーをシステム全体に適用する場合にのみ使用できます。
- **ユーザー名:** ユーザー名を入力します。
- **接続ごとのパスワード:** ユーザーがログオンするたびにパスワードを要求するかどうかを選択します。
- **パスワード:** オプションのパスワードを入力します。このフィールドを空白のままにすると、ユーザーはログオン時にパスワードの入力を求められることがあります。
- **ID資格情報（キーストアまたはPKI資格情報）:** リストからID資格情報の種類を選択します。デフォルトは**なし**です。
- **外部ID:** *有効にした場合にのみ必要です* **PEAP**、**TTLS**、*または* **EAP-FAST**。外部から見えるユーザー名を入力します。「anonymous」のような一般的な用語を入力することで、ユーザー名が見えないようにしてセキュリティを強化できます。
- **TLS証明書を要求:** TLS証明書を要求するかどうかを選択します。

- **信頼**
  - **信頼された証明書:** 信頼された証明書を追加するには、**追加**をクリックし、追加する各証明書について以下を実行します:
    - **アプリケーション:** リストから追加するアプリケーションを選択します。
    - **保存**をクリックして証明書を保存するか、**キャンセル**をクリックします。
  - **信頼されたサーバー証明書名:** 信頼されたサーバー証明書の共通名を追加するには、**追加**をクリックし、追加する各名前について、以下を実行します。
    - **証明書:** 追加するサーバー証明書の名前を入力します。wpa.*.example.com のように、ワイルドカードを使用して名前を指定できます。
    - 証明書名を保存するには**保存**をクリックするか、**キャンセル**をクリックします。
- **信頼例外を許可:** 証明書が信頼されていない場合に、ユーザーデバイスに証明書の信頼ダイアログが表示されるかどうかを選択します。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アンドロイド エンタープライズ 設定



- **ネットワーク名:** ユーザーデバイスの利用可能なネットワークのリストにあるSSIDを入力します。
- **認証:** リストから、Wi-Fi接続で使用するセキュリティの種類を選択します。
  - オープン
  - 共有
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下のセクションでは、前述の各接続タイプに対して構成するオプションを一覧表示します。デフォルトは**Open**です。

Android EnterpriseのOpen、共有設定

- **暗号化:** リストから、**Disabled**または**WEP**を選択します。デフォルトは**WEP**です。
- **パスワード:** オプションのパスワードを入力します。
- **ネットワークを非表示:** ネットワークを非表示にするかどうかを選択します。

Android Enterprise の WPA、WPA-PSK、WPA2、WPA2-PSK 設定

- **暗号化:** リストから、**TKIP**または**AES**を選択します。デフォルトは**TKIP**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **パスワード:** オプションのパスワードを入力します。
- **ネットワークを非表示:** ネットワークを非表示にするかどうかを選択します。

Android Enterprise 向け 802.1x 設定

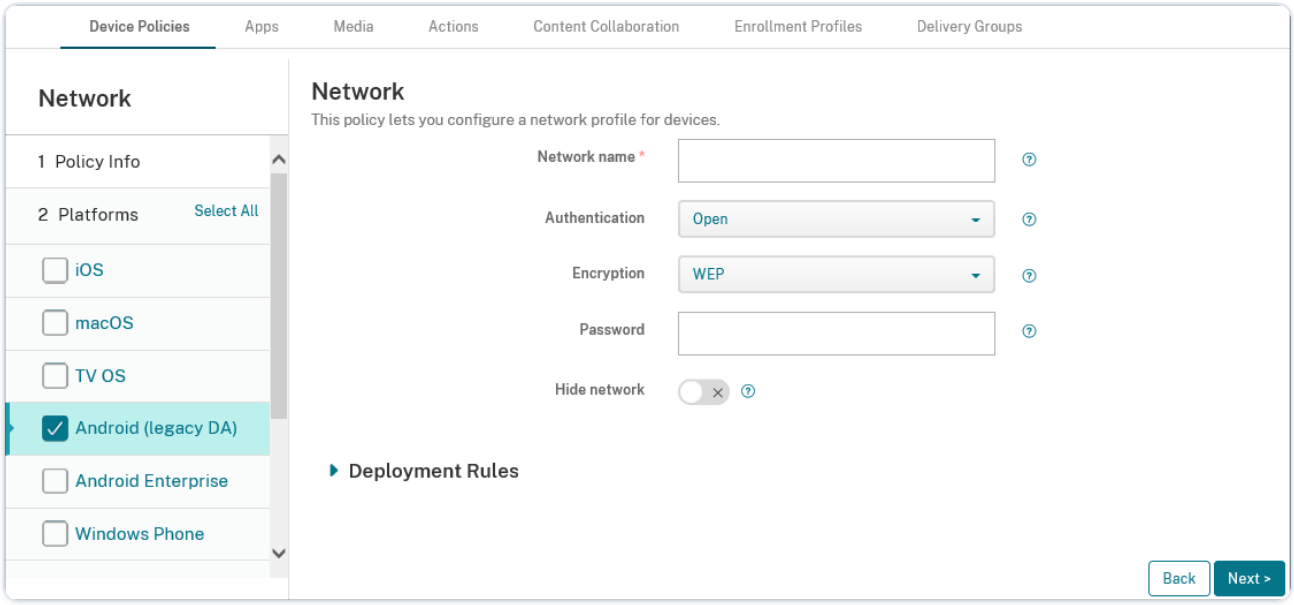
- **EAPタイプ:** リストから、**PEAP**、**TLS**、または**TTLS**を選択します。デフォルトは**PEAP**です。
- **パスワード:** オプションのパスワードを入力します。
- **認証フェーズ2:** リストから、**None**、**PAP**、**MSCHAP**、**MSCHAPPv2**、または**GTC**を選択します。デフォルトは**PAP**です。
- **ID:** オプションのユーザー名とドメインを入力します。
- **匿名:** オプションの、外部から見えるユーザー名を入力します。「anonymous」のような一般的な用語を入力することで、ユーザー名が表示されないようにセキュリティを強化できます。
- **CA 証明書:** リストから、使用する証明書を選択します。
- **ドメイン:** 必要なドメイン名を入力します。詳しくは、「ドメイン」を参照してください。

> **注:**
>
> Android 13 以降を実行しているデバイスで Wi-Fi ポリシーを構成する場合、**CA 証明書**と**ドメイン**のフィールドは必須で更新する必要があります。更新しない場合、構成は失敗します。

- **ID 資格情報:** リストから、使用する ID 資格情報を選択します。デフォルトは**なし**です。
- **ネットワークを非表示にする:** ネットワークを非表示にするかどうかを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android (レガシー DA) 設定



- **ネットワーク名:** ユーザーデバイスで利用可能なネットワークのリストにある SSID を入力します。
- **認証:** リストから、Wi-Fi 接続で使用するセキュリティの種類を選択します。
  - オープン
  - 共有 (Android Enterprise のみ)
  - WPA (アンドロイド エンタープライズ のみ)
  - WPA-PSK (アンドロイド エンタープライズ のみ)
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下のセクションでは、前述の各接続タイプについて構成するオプションを一覧表示します。

Android のオープン、共有設定

- **暗号化:** リストから、**無効**または**WEP**のいずれかを選択します。デフォルトは**WEP**です。
- **パスワード:** オプションのパスワードを入力します。
- **ネットワークを非表示:** ネットワークを非表示にするかどうかを選択します。

Android の WPA、WPA-PSK、WPA2、WPA2-PSK 設定

- **暗号化:** リストから、**TKIP**または**AES**のいずれかを選択します。デフォルトは**TKIP**です。
- **パスワード:** オプションのパスワードを入力します。

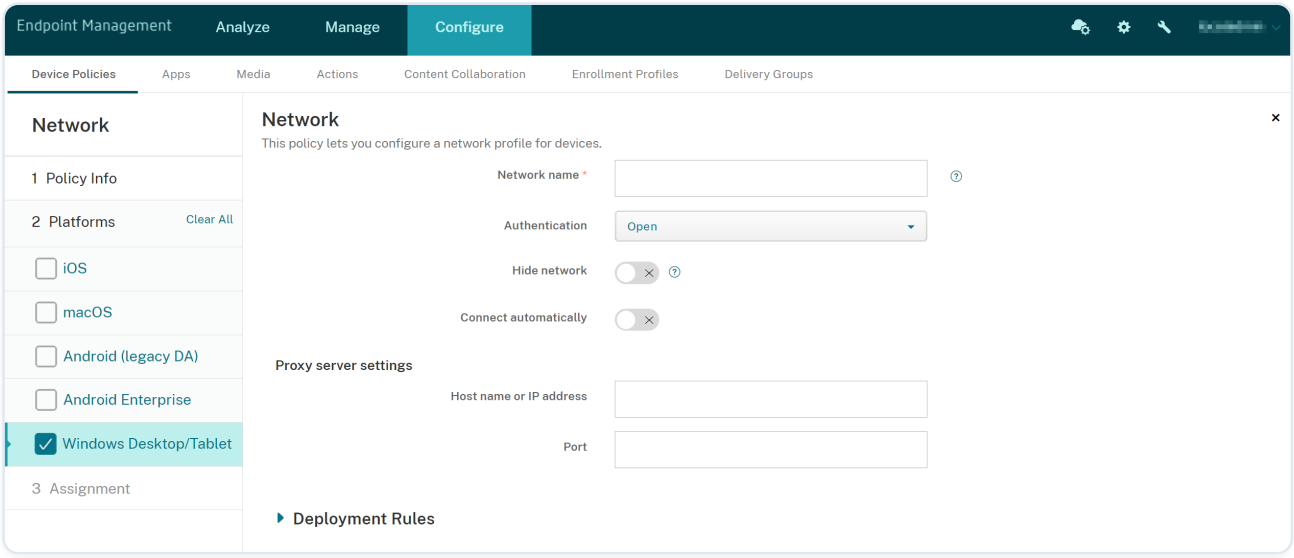
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ネットワークを非表示:** ネットワークを非表示にするかどうかを選択します。

Android の 802.1x 設定

- **EAP タイプ:** リストから、**PEAP**、**TLS**、または**TTLS**を選択します。デフォルトは**PEAP**です。
- **パスワード:** オプションのパスワードを入力します。
- **認証フェーズ 2:** リストから、**なし**、**PAP**、**MSCHAP**、**MSCHAPPv2**、または**GTC**を選択します。デフォルトは**PAP**です。
- **ID:** オプションのユーザー名とドメインを入力します。
- **匿名:** オプションの、外部から見えるユーザー名を入力します。「anonymous」のような一般的な用語を入力することで、ユーザー名が見えないようにしてセキュリティを強化できます。
- **CA証明書:** リストから使用する証明書を選択します。
- **ID資格情報:** リストから使用するID資格情報を選択します。デフォルトは**なし**です。
- **ネットワークを非表示:** ネットワークを非表示にするかどうかを選択します。

Windowsデスクトップ/タブレットの設定



- **ネットワーク名:** 利用可能なネットワークのリストに表示されるSSID。
- **認証:** ドロップダウンリストから、Wi-Fi接続で使用するセキュリティの種類をクリックします。
  - オープン
  - WPAパーソナル
  - WPA-2パーソナル

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- WPAエンタープライズ
- WPA-2エンタープライズ: Windows 10の最新リリースでは、WPA-2エンタープライズを使用するようにSCEPを構成します。SCEP構成により、Citrix Endpoint Managementは証明書をデバイスに送信し、Wi-Fiサーバーに対して認証を行うことができます。SCEPを構成するには、**設定 > 資格情報プロバイダー**の**配布**ページに移動します。詳細については、資格情報プロバイダーを参照してください。

以下のセクションでは、上記の各接続タイプに対して構成するオプションを一覧表示します。

Windows 10およびWindows 11のオープン設定

- **ネットワークを非表示にする:** ネットワークを非表示にするかどうかを選択します。
- **自動的に接続する:** ネットワークに自動的に接続するかどうかを選択します。

Windows 10およびWindows 11のWPA Personal、WPA-2 Personal設定

- **暗号化:** リストから**AES**または**TKIP**を選択して、暗号化の種類を設定します。デフォルトは**AES**です。
- **共有キー:** 選択した方式の暗号化キーを入力します。
- **ネットワークを非表示にする:** ネットワークを非表示にするかどうかを選択します。
- **自動的に接続する:** ネットワークに自動的に接続するかどうかを選択します。

Windows 10およびWindows 11のWPA-2 Enterprise設定

- **暗号化:** リストから**AES**または**TKIP**を選択して、暗号化の種類を設定します。デフォルトは**AES**です。
- **EAPタイプ:** リストから**PEAP-MSCHAPv2**または**TLS**を選択して、EAPタイプを設定します。デフォルトは**PEAP-MSCHAPv2**です。
- **ネットワークを非表示にする:** ネットワークを非表示にするかどうかを選択します。
- **自動的に接続する:** ネットワークに自動的に接続するかどうかを選択します。
- **SCEPを有効にする?:** SCEPを使用してユーザーデバイスに証明書をプッシュするかどうかを選択します。
- **SCEPの資格情報プロバイダー:** リストからSCEP資格情報プロバイダーを選択します。デフォルトは**None**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネットワーク使用状況デバイスポリシー

iOSデバイスがセルラーデータネットワークなどのネットワークをどのように使用するかを指定するネットワーク使用状況ルールを設定できます。このルールは、管理対象アプリと指定されたSIMに適用されます。管理対象アプリとは、Citrix Endpoint Managementを介してユーザーのデバイスに展開するアプリです。ユーザーがCitrix Endpoint Managementを介して展開されていない場合に、デバイスに直接ダウンロードしたアプリは含まれません。また、デバイスがCitrix Endpoint Managementに登録されたときにすでにデバイスにインストールされていたアプリも含まれません。このポリシーは、iOS 13デバイスのSIMに適用されます。アプリルール、SIMルール、またはその両方を構成できます。SIMルールは、そのデバイス上のすべての管理対象アプリに適用されます。

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］**の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS設定

- **アプリケーションルール**
  - **ローミング中のセルラーデータを許可：** 指定されたアプリがローミング中にセルラーデータ接続を使用できるかどうかを選択します。デフォルトは**オフ**です。
  - **セルラーデータを許可：** 指定されたアプリがセルラーデータ接続を使用できるかどうかを選択します。デフォルトは**オフ**です。
  - **アプリ識別子の照合：** リストに追加する各アプリについて、**［追加］**をクリックし、以下を構成します。
    - **アプリ識別子：** アプリ識別子を入力します。
  - アプリをリストに保存するには**［保存］**をクリックし、保存しない場合は［キャンセル］**をクリックします。
- **SIMルール**
  - **SIM Wi-Fiアシストポリシー：** **［低品質Wi-Fiからの切り替え］**を有効にすると、Wi-Fiアシストポリシーが低品質Wi-Fiからセルラー接続へより積極的に切り替わるようになります。この設定により、セルラーデータ使用量が増加し、バッテリー寿命に影響を与える可能性があります。
  - **SIM ICCID：** リストに追加する各SIMについて、**［追加］**をクリックし、以下を構成します。
    - **ICCID：** 追加するSIMカードの19桁または20桁の番号を入力します。

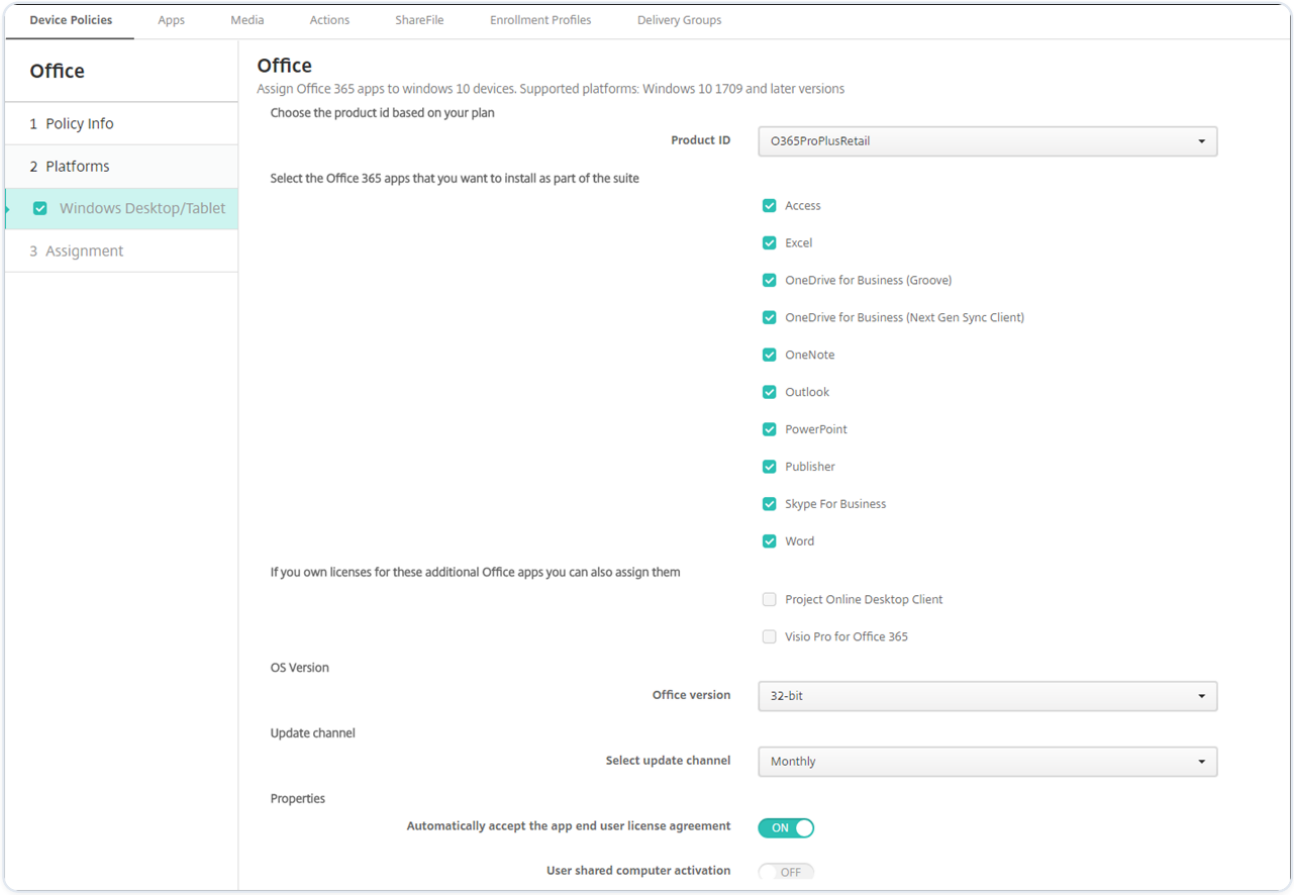
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Officeデバイスポリシー

Citrix Endpoint Managementでは、Office構成サービスプロバイダー (CSP) を使用してMicrosoft Office 365製品を展開できます。Officeデバイスポリシーを構成することで、Windows 10 (バージョン1709以降) またはWindows 11を実行している任意のデバイスにMicrosoft Officeアプリを展開できます。

このポリシーを追加または構成するには、**「構成」>「デバイスポリシー」**に移動します。詳しくは、「デバイスポリシー」(/ja-jp/citrix-endpoint-management/policies.html)を参照してください。

Windowsデスクトップ/タブレット設定



- **製品ID：** Office 365プランに基づいて製品IDを選択します。オプションは、**O365ProPlusRetail、O365BusinessRetail、またはO365SmallBusPremRetail**です。
- **Office 365アプリ：** 展開するOffice 365アプリを選択します。デフォルトではすべてのアプリが選択されています。
- **追加のOfficeアプリ：** **Project Online Desktop Client**または**Visio Pro for Office 365**のライセンスを所有している場合は、これらのアプリを選択してインストールできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Officeバージョン：** Officeの**32ビット**または**64ビット**バージョンのどちらをインストールするかを選択します。
- **更新チャネル：** 更新の頻度を選択します。オプションは、**月次、月次（ターゲット指定）、半期**、または**半期（ターゲット指定）**です。
- **プロパティ：**
  - **アプリのエンドユーザーライセンス契約を自動的に承諾する：** **「オン」**または**「オフ」**を選択します。**デフォルトは**「オン」**です。
  - **ユーザー共有コンピューターのライセンス認証：** コンピューターが共有されているかどうかを選択します。オプションは**「オン」**または**「オフ」**です。**デフォルトは**「オフ」**です。
- **Office言語：** Officeは、Windowsに既にインストールされているすべての言語で自動的にインストールされます。追加の言語を選択してインストールできます。

組織情報デバイスポリシー

組織情報デバイスポリシーは、Citrix Endpoint ManagementからiOSデバイスにプッシュされるアラートメッセージ用の組織情報を指定します。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **名前:** Citrix Endpoint Managementを実行している組織の名前を入力します。
- **アドレス:** 組織のアドレスを入力します。
- **電話:** 組織のサポート電話番号を入力します。
- **メール:** サポートメールアドレスを入力します。
- **マジック:** 組織によって管理されるサービスを説明する単語またはフレーズを入力します。

OS更新デバイスポリシー

OS更新デバイスポリシーを使用すると、以下を展開できます。

- 監視対象のiOSデバイスへの最新のOSアップデート。

  OS更新デバイスポリシーは、Apple Deployment Programに登録されている監視対象デバイスでのみ機能します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Apple Deployment Programに登録されているmacOS 10.11.5以降を実行しているmacOSデバイスへの最新のOSおよびアプリのアップデート。

注：

Appleは現在、OSアップデートをメジャーバージョンのみに制限しています。管理者はマイナーバージョンを更新できません。詳細については、Appleのドキュメントにあるこの記事を参照してください。

- Windows 10またはWindows 11を実行している監視対象のデスクトップおよびタブレットデバイスへの最新のOSアップデート。

  OS更新ポリシーを使用して、Windows 10（バージョン1607以降）またはWindows 11を実行しているデスクトップおよびタブレットの配信最適化設定を管理することもできます。配信最適化は、MicrosoftがWindows 10およびWindows 11のアップデート用に提供するピアツーピアクライアント更新サービスです。配信最適化の目的は、更新プロセス中の帯域幅の問題を軽減することです。帯域幅の削減は、ダウンロードタスクを複数のデバイス間で共有することによって実現されます。詳細については、Microsoft の記事「Windows 10 の更新プログラムの配信の最適化を構成する」を参照してください。
- 管理対象のAndroid Enterpriseデバイス（Android 7.0以降）への最新のOSアップデート。

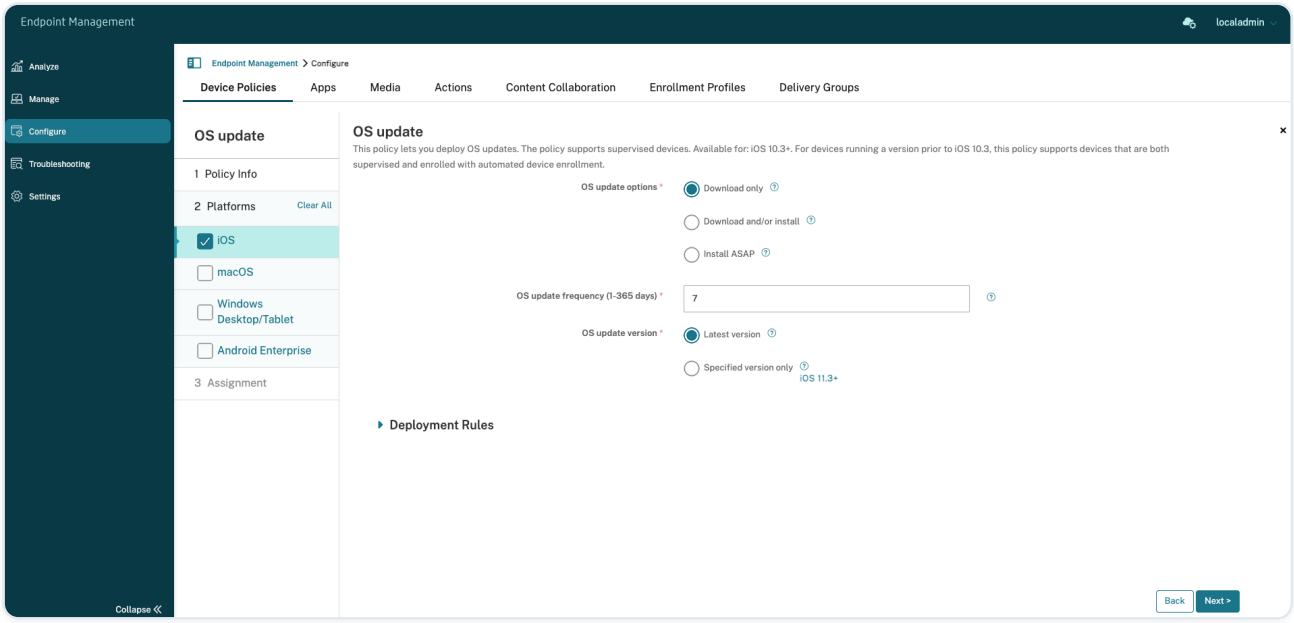
重要：

OS更新ポリシーでは、更新を完全に無効にすることはできません。更新を最大90日間遅延させるには、制限ポリシーを作成します。(/ja-jp/citrix-endpoint-management/policies/restrictions-policy.html)を参照してください。

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］**に移動します。詳細については、(/ja-jp/citrix-endpoint-management/policies.html)を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定

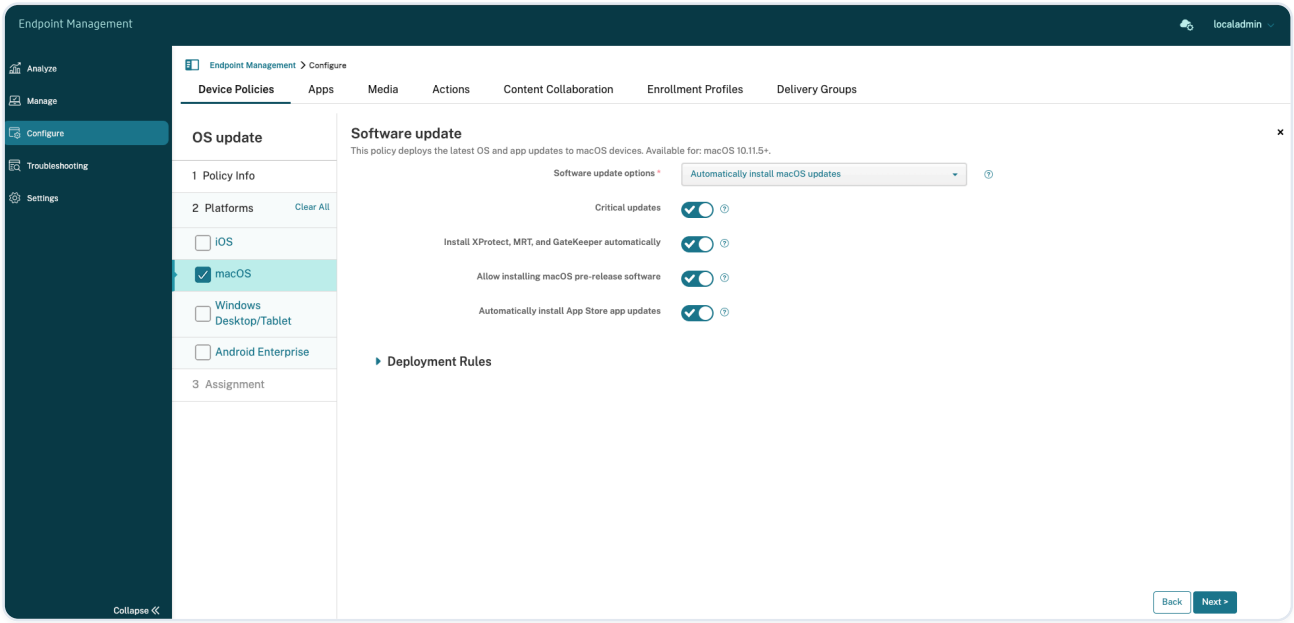


以下の設定は、監視対象のiOSデバイス用です。

- **OSアップデートオプション:** どちらのオプションも、**OSアップデート頻度**に従って、最新のOSアップデートを監視対象デバイスにダウンロードします。デバイスはユーザーにアップデートのインストールを促します。プロンプトは、ユーザーがデバイスのロックを解除した後に表示されます。
- **OSアップデート頻度:** Citrix Endpoint Managementがデバイスの OSをチェックし、アップデートする頻度を決定します。デフォルトは**7**日です。
- **OSアップデートバージョン:** 監視対象のiOSデバイスをアップデートするために使用するバージョンを指定します。デフォルトは**最新バージョン**です。
  - **最新バージョン:** 最新のOSバージョンにアップデートするには、これを選択します。
  - **特定のバージョンのみ:** 特定のOSバージョンにアップデートするには、これを選択し、バージョン番号を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOSの設定



- **ソフトウェアアップデートオプション:** macOSデバイスがアップデートをチェックし、インストールする方法を制御します。以下のオプションから選択します。
  - **macOSアップデートを自動的にインストール:** アップデートは自動的にダウンロードされ、インストールされます。
  - **利用可能な場合は新しいアップデートをダウンロード:** アップデートはダウンロードされますが、手動でのインストールが必要です。
  - **アップデートを確認:** アップデートが存在するかどうかを確認しますが、アップデートを自動的にダウンロードまたはインストールしません。
  - **アップデートを確認しない:** 新しいアップデートの確認、アップデートのダウンロード、またはアップデートの自動インストールを行いません。ユーザーは引き続き手動でアップデートをインストールできます。
- **重要なアップデート:** 重要なmacOSアップデートの自動インストールを許可します。
- **xProtect、MRT、およびGateKeeperアップデートを自動的にインストール:** macOSデバイスがセキュリティソフトウェアのアップデートを自動的にインストールすることを許可します。
- **macOSプレリリースソフトウェアのインストールを許可:** ユーザーがmacOSソフトウェアのプレリリースバージョンをインストールできるようにします。
- **App Storeアプリのアップデートを自動的にインストール:** App Storeアプリが自動的にアップデートされるようにします。

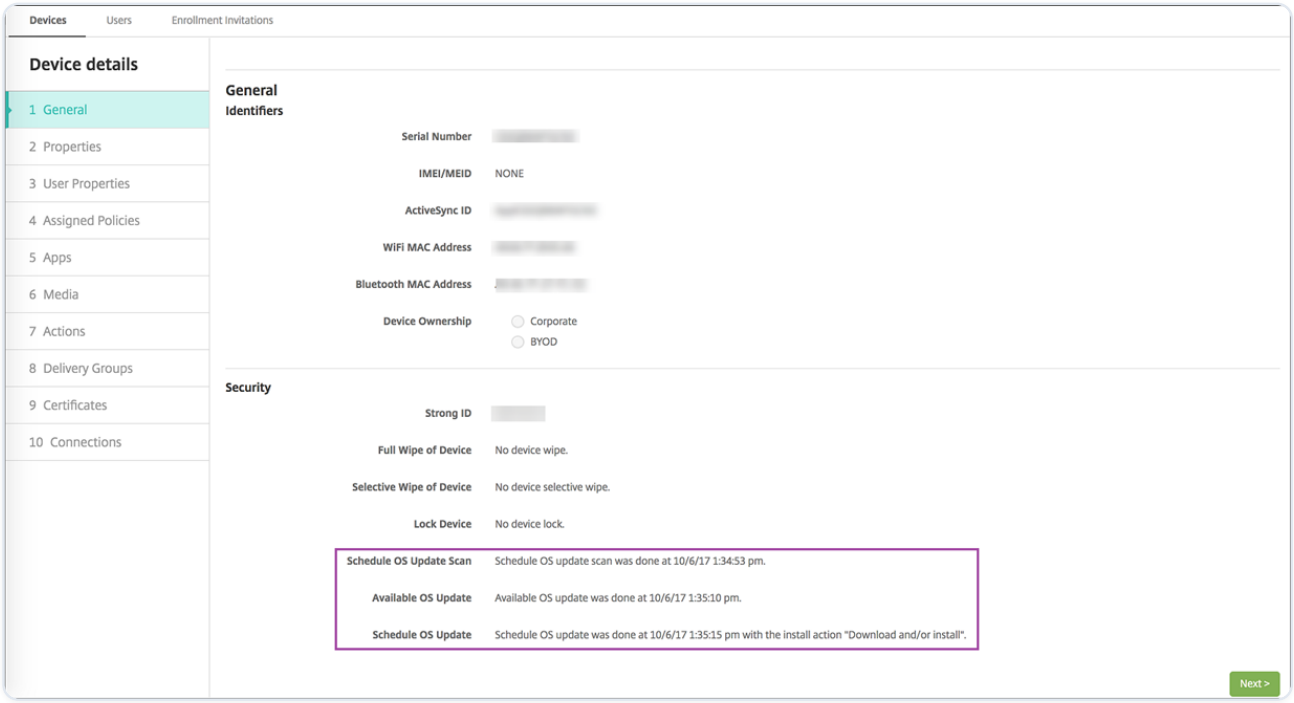
© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOSおよびmacOSのアップデートアクションのステータスを取得

iOSおよびmacOSの場合、Citrix Endpoint ManagementはOSアップデート制御ポリシーをデバイスに展開しません。代わりに、Citrix Endpoint Managementはポリシーを使用して、以下のMDMコマンドをデバイスに送信します。

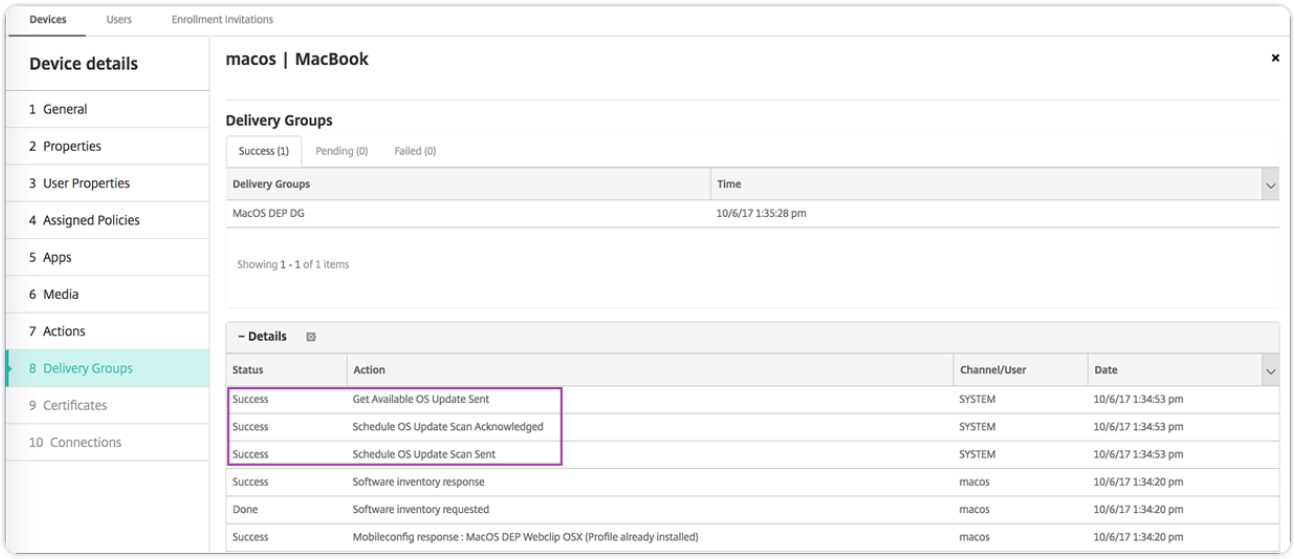
- OSアップデートスキャンをスケジュール: デバイスがOSアップデートのバックグラウンドスキャンを実行するように要求します。(iOSではオプション)
- 利用可能なOSアップデート: 利用可能なOSアップデートのリストをデバイスに照会します。
- OSアップデートをスケジュール: デバイスがmacOSアップデート、アプリのアップデート、またはその両方を行うように要求します。したがって、デバイスのOSがOSおよびアプリのアップデートをダウンロードまたはインストールするタイミングを決定します。

Manage > Devices > Device details (General)ページには、スケジュールされた利用可能なOSアップデートスキャン、およびスケジュールされたmacOSとアプリのアップデートのステータスが表示されます。

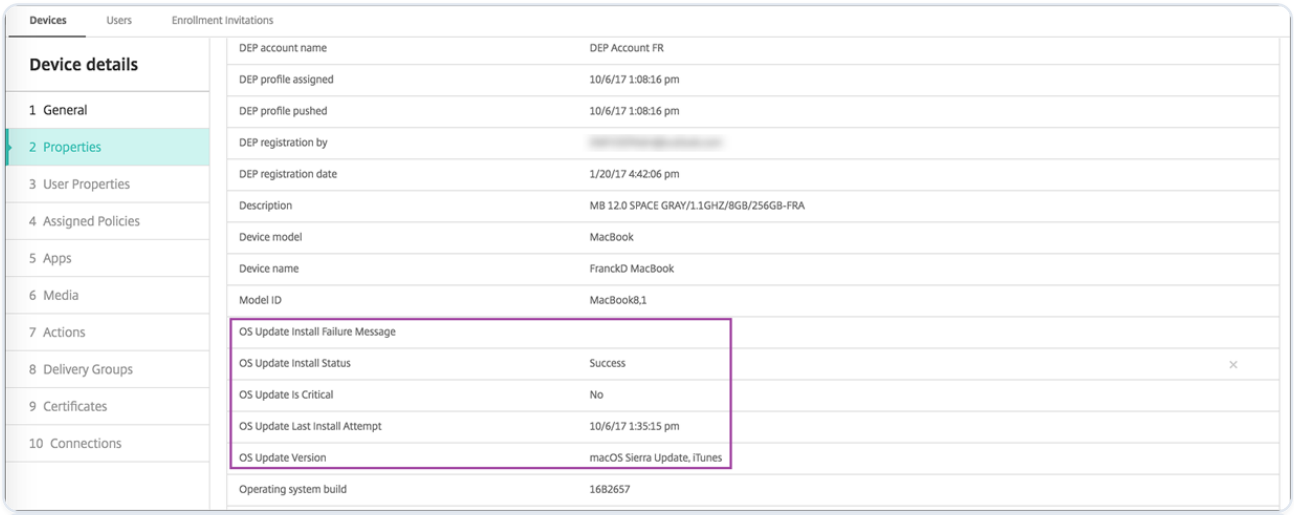


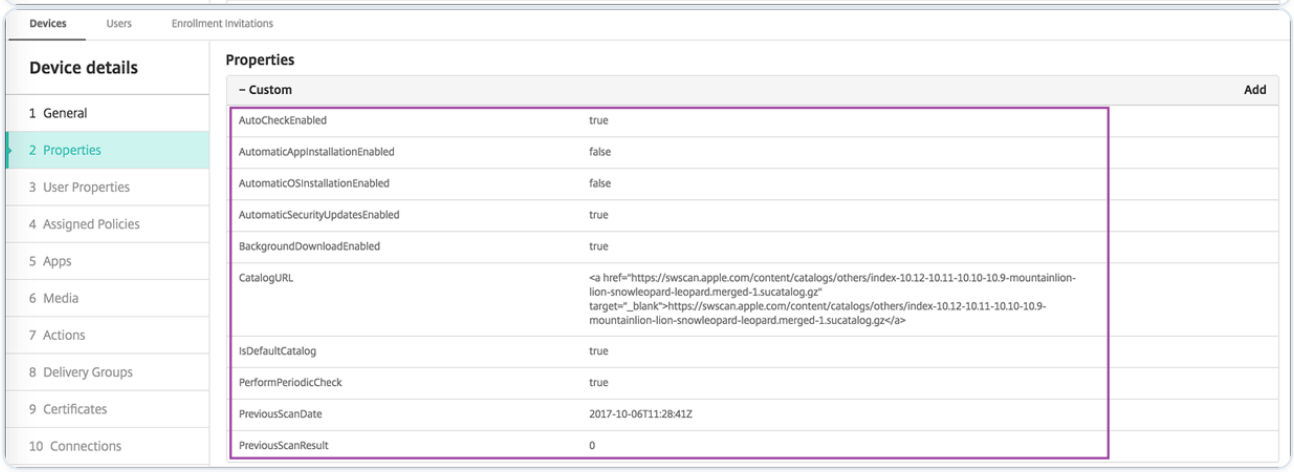
アップデートアクションのステータスの詳細については、**Manage > Devices > Device details (Delivery Groups)**ページに移動してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



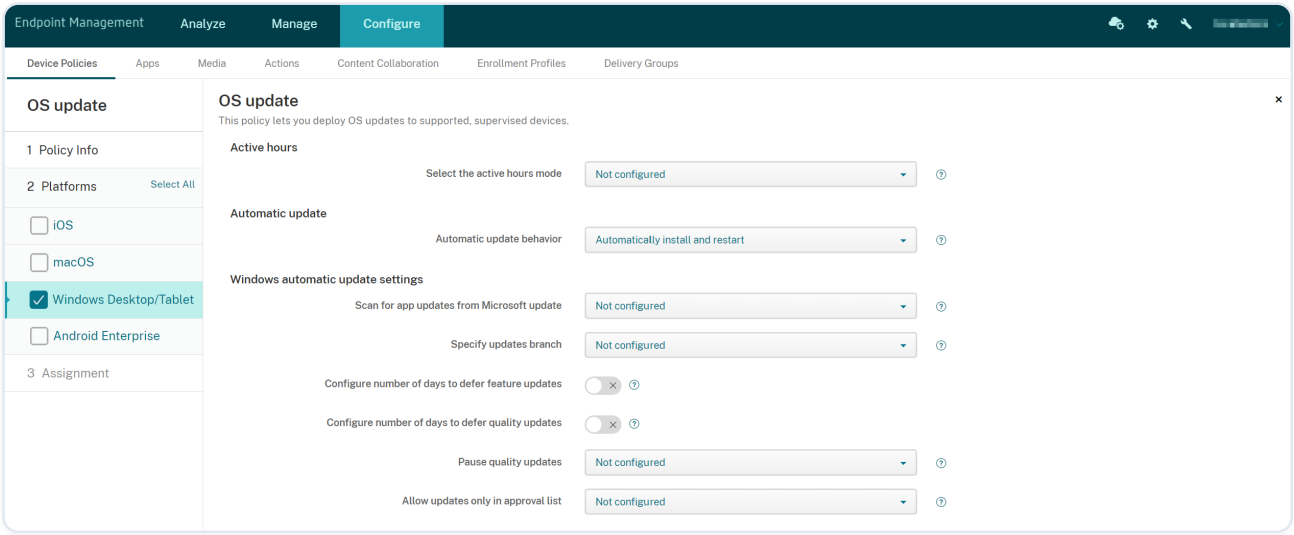
利用可能なOSアップデートや最終インストール試行などの詳細については、**Manage > Devices > Device details (Properties)**ページに移動してください。





© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windowsデスクトップおよびタブレットの設定



- **アクティブ時間モードの選択:** OSアップデートを行うアクティブ時間を構成するモードを選択します。時間範囲、または開始時刻と終了時刻を指定できます。モードを選択すると、追加の設定が表示されます。**アクティブ時間の最大範囲を指定**、または**アクティブ時間の開始**と**アクティブ時間の終了**。**未構成**を選択すると、WindowsはいつでもOSアップデートを実行できます。既定値は**未構成**です。
- **自動更新の動作:** ユーザーデバイス上のWindows更新サービスのダウンロード、インストール、および再起動の動作を構成します。既定値は**自動インストールと再起動**です。
  - **更新プログラムのダウンロード前にユーザーに通知:** Windowsは、更新プログラムが利用可能になったときにユーザーに通知します。Windowsは、更新プログラムを自動的にダウンロードおよびインストールしません。ユーザーがダウンロードおよびインストール操作を開始する必要があります。
  - **自動インストールとデバイス再起動のスケジュール設定を通知:** Windowsは、従量制課金接続ではないネットワークで更新プログラムを自動的にダウンロードします。Windowsは、デバイスが使用中でなく、バッテリー電源で動作していないときに、自動メンテナンス中に更新プログラムをインストールします。自動メンテナンスが2日間更新プログラムをインストールできない場合、Windows Updateはすぐに更新プログラムをインストールします。インストールに再起動が必要な場合、Windowsはユーザーに再起動時刻をスケジュールするよう促します。ユーザーは最大7日間、再起動をスケジュールできます。7日後、Windowsはデバイスの再起動を強制します。ユーザーが開始時刻を制御できるようにすることで、再起動時に適切にシャットダウンしないアプリによって引き起こされる偶発的なデータ損失のリスクが軽減されます。
  - **自動インストールと再起動:** 既定の設定です。Windowsは、従量制課金接続ではないネットワークで更新プログラムを自動的にダウンロードします。Windowsは、デバイスが使用中でなく、バッテリー電源で動作していないときに、自動メンテナンス中に更新プログラム

© 1997–2026 Citrix Systems, Inc. All rights reserved.

をインストールします。自動メンテナンスが2日間更新プログラムをインストールできない場合、Windows Updateはすぐに更新プログラムをインストールします。インストールに再起動が必要な場合、Windowsはデバイスが非アクティブなときに自動的にデバイスを再起動します。

- **指定した時刻に自動インストールと再起動:** このオプションを選択すると、日付と時刻を指定するための追加の設定が表示されます。既定値は毎日午前3時です。自動インストールは指定された時刻に行われ、デバイスの再起動は15分間のカウントダウン後に発生します。Windowsが再起動の準備ができたとき、ログインしているユーザーは15分間のカウントダウンを中断して再起動を遅らせることができます。
- **エンドユーザー制御なしで自動インストールと再起動:** Windowsは、従量制課金接続ではないネットワークで更新プログラムを自動的にダウンロードします。Windowsは、デバイスが使用中でなく、バッテリー電源で動作していないときに、自動メンテナンス中に更新プログラムをインストールします。自動メンテナンスが2日間更新プログラムをインストールできない場合、Windows Updateはすぐに更新プログラムをインストールします。インストールに再起動が必要な場合、Windowsはデバイスが非アクティブなときに自動的にデバイスを再起動します。このオプションは、ユーザーコントロールパネルも読み取り専用に設定します。
- **自動更新をオフにする:** デバイス上のWindows自動更新を無効にします。

- **Microsoft Updateからのアプリ更新プログラムのスキャン:** WindowsがMicrosoft Updateサービスから他のMicrosoftアプリの更新プログラムを受け入れるかどうかを指定します。既定値は**未構成**です。
  - **未構成:** 動作を構成したくない場合は、この設定を使用します。Windowsは、ユーザーデバイス上の関連UIを変更しません。ユーザーは、他のMicrosoftアプリの更新プログラムを受け入れるか拒否することができます。
  - **はい:** Windowsは、Windows更新サービスからアプリの更新プログラムがインストールされることを許可します。ユーザーデバイス上の関連設定は非アクティブであるため、ユーザーはその設定を変更できません。
  - **いいえ:** Windowsは、Windows更新サービスからアプリの更新プログラムがインストールされることを許可しません。ユーザーデバイス上の関連設定は非アクティブであるため、ユーザーはその設定を変更できません。
- **更新ブランチの指定:** 更新プログラムに使用するWindows更新サービスブランチを指定します。既定値は**未構成**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **未構成:** 動作を構成したくない場合は、この設定を使用します。Windowsは、ユーザーデバイス上の関連UIを変更しません。ユーザーはWindows更新サービスブランチを選択できます。
  - **Current Branch:** Windows は Current Branch から更新プログラムを受け取ります。ユーザーデバイスの関連設定は非アクティブであるため、ユーザーはその設定を変更できません。
  - **Current Branch for Business:** Windows は Current Branch for Business から更新プログラムを受け取ります。ユーザーデバイスの関連設定は非アクティブであるため、ユーザーはその設定を変更できません。

- **機能更新プログラムの延期日数設定: オン**の場合、Windows は指定された日数だけ機能更新プログラムを延期し、ユーザーはその設定を変更できません。**オフ**の場合、ユーザーは機能更新プログラムを延期する日数を変更できます。既定値は**オフ**です。
- **品質更新プログラムの延期日数設定: オン**の場合、Windows は指定された日数だけ品質更新プログラムを延期し、ユーザーはその設定を変更できません。**オフ**の場合、ユーザーは品質更新プログラムを延期する日数を変更できます。既定値は**オフ**です。
- **品質更新プログラムの一時停止:** 品質更新プログラムを 35 日間一時停止するかどうかを指定します。既定値は**未構成**です。
  - **未構成:** 動作を構成しない場合は、この設定を使用します。Windows はユーザーデバイスの関連 UI を変更しません。ユーザーは品質更新プログラムを 35 日間一時停止することを選択できます。
  - **はい:** Windows は、Windows Update サービスからの品質更新プログラムのインストールを 35 日間一時停止します。ユーザーデバイスの関連設定は非アクティブであるため、ユーザーはその設定を変更できません。
  - **いいえ:** Windows は、Windows Update サービスからの品質更新プログラムのインストールを一時停止しません。ユーザーデバイスの関連設定は非アクティブであるため、ユーザーはその設定を変更できません。
- **承認リスト内の更新プログラムのみを許可:** MDM サーバーが承認した更新プログラムのみをインストールするかどうかを指定します。Citrix Endpoint Management は、承認済み更新プログラムのリストの構成をサポートしていません。既定値は**未構成**です。
  - **未構成:** 動作を構成しない場合は、この設定を使用します。Windows はユーザーデバイスの関連 UI を変更しません。ユーザーは許可する更新プログラムを選択できます。
  - **はい、承認済み更新プログラムのみをインストール:** 承認済み更新プログラムのみのインストールを許可します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **いいえ、適用可能なすべての更新プログラムをインストール:** デバイス上の適用可能なすべての更新プログラムのインストールを許可します。

- **内部更新サーバーを使用:** Windows Update サービスから更新プログラムを取得するか、Windows Server Update Services (WSUS) を介して内部更新サーバーから更新プログラムを取得するかを指定します。**オフ**の場合、デバイスは Windows Update サービスを使用します。**オン**の場合、デバイスは指定された WSUS サーバーに接続して更新プログラムを取得します。既定値は**オフ**です。

    - **Microsoft 以外のエンティティによって署名された更新プログラムを受け入れる:** Microsoft 以外のサードパーティエンティティによって署名された更新プログラムを受け入れるかどうかを指定します。この機能には、デバイスがサードパーティベンダーの証明書を信頼している必要があります。既定値は**オフ**です。
    - **Microsoft 更新サービスへの接続を許可:** デバイスが WSUS サーバーから更新プログラムを取得するように構成されている場合でも、デバイス上の Windows Update が定期的に Microsoft 更新サービスに接続することを許可します。既定値は**オン**です。
    - **WSUSサーバー:** WSUSサーバーのサーバーURLを指定します。
    - **更新プログラムをホストする代替イントラネットサーバー:** 更新プログラムをホストし、レポート情報を受信する代替イントラネットサーバーのURLを指定します。

- **配信の最適化を構成する:** Windows 10およびWindows 11の更新プログラムに配信の最適化を使用するかどうか。既定値は**オフ**です。
- **キャッシュサイズ:** 配信の最適化キャッシュの最大サイズ。値が**0**の場合、キャッシュは無制限です。既定値は**10** GBです。
- **VPNピアキャッシュを許可する:** VPN経由でドメインネットワークに接続されている場合に、デバイスがピアキャッシュに参加することを許可するかどうか。**オン**の場合、デバイスはVPNまたは企業ドメインネットワーク上の他のドメインネットワークデバイスからダウンロードまたはアップロードできます。既定値は**オフ**です。
- **ダウンロード方法:** 配信の最適化がWindows Update、アプリ、およびアプリの更新プログラムのダウンロードに使用できるダウンロード方法。既定値は**HTTP blended with peering behind the same NAT**です。オプションは次のとおりです。

    - **HTTPのみ、ピアリングなし:** ピアツーピアキャッシュを無効にしますが、配信の最適化がWindows UpdateサーバーまたはWindows Server Update Services (WSUS) サーバーからコンテンツをダウンロードすることを許可します。
    - **HTTP blended with peering behind the same NAT:** 同じネットワーク上でのピア共有を有効にします。配信の最適化クラウドサービスは、ターゲットクライアントと同じパブ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リックIPを使用してインターネットに接続する他のクライアントを検索します。これらのクライアントは、プライベートサブネットIPを使用して同じネットワーク上の他のピアに接続しようとします。

- **HTTP blended with peering across a private group:** デバイスのActive Directory Domain Services (AD DS) サイトまたはデバイスが認証するドメインに基づいてグループを自動的に選択します。ピアリングは、リモートオフィス内のデバイスを含む、同じグループに属するデバイス間の内部サブネット全体で発生します。
- **HTTP blended with Internet peering:** 配信の最適化のインターネットピアソースを有効にします。
- **ピアリングなしのシンプルダウンロードモード:** 配信の最適化クラウドサービスの使用を無効にします。配信の最適化は、配信の最適化クラウドサービスが利用できない、到達できない、またはコンテンツファイルサイズが10 MB未満の場合に、自動的にこのモードに切り替わります。このモードでは、配信の最適化はピアツーピアキャッシュなしで信頼性の高いダウンロードエクスペリエンスを提供します。
- **配信の最適化を使用せず、代わりにBITSを使用する:** クライアントがBranchCacheを使用できるようにします。詳細については、Microsoftの記事「BranchCache」を参照してください。

- **最大ダウンロード帯域幅:** 1秒あたりの最大ダウンロード帯域幅 (KB/秒)。既定値は**0**で、動的な帯域幅調整を意味します。
- **最大ダウンロード帯域幅の割合:** 配信の最適化がすべての同時ダウンロードアクティビティで使用できる最大ダウンロード帯域幅。この値は、利用可能なダウンロード帯域幅の割合です。既定値は**0**で、動的な調整を意味します。
- **最大アップロード帯域幅:** 1秒あたりの最大アップロード帯域幅 (KB/秒)。既定値は**0**です。値が**0**の場合、帯域幅は無制限です。
- **月間アップロードデータ上限:** 各暦月において、配信最適化がインターネットピアにアップロードできる最大サイズ（GB単位）。デフォルトは20 GBです。値が**0**の場合、月間アップロードは無制限を意味します。

Citrix Endpoint ManagementがWindowsデスクトップおよびタブレットデバイスへの承認済みアップデートを処理する方法

承認済みの更新プログラムのみをインストールするかどうかを指定できます。Citrix Endpoint Managementは、更新プログラムを次のように処理します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Windows Defenderの定義などのセキュリティ更新プログラムの場合、Citrix Endpoint Managementは更新プログラムを自動的に承認し、次回の同期時にデバイスにインストールコマンドを送信します。
- その他のすべての更新プログラムの種類については、Citrix Endpoint Managementは承認を待ってからデバイスにインストールコマンドを送信します。

前提条件

- Microsoftルート証明書をCitrix Endpoint Managementサーバーにサーバー証明書としてアップロードする必要があります。
- サーバー証明書のインポートについては、証明書と認証の「証明書をインポートするには」を参照してください。

承認済みの更新プログラムのみをインストールするには

1. **構成 > デバイスポリシー**に移動し、OS更新デバイスポリシーを開きます。
2. **承認リスト内の更新プログラムのみを許可**設定を**はい、承認済みの更新プログラムのみをインストール**に変更します。

更新プログラムを承認するには

1. OS更新デバイスポリシーで、**保留中の更新プログラム**テーブルまでスクロールします。Citrix Endpoint Managementは、テーブルにリストされている更新プログラムをデバイスから取得します。
2. **承認ステータス**が**保留中**の更新プログラムを検索します。
3. 承認したい更新プログラムの行をクリックし、その行の編集アイコン（**追加**列内）をクリックします。

   「デバイスポリシー設定画面」(/en-us/citrix-endpoint-management/media/pending-approved-windows-updates.png)
4. 更新を承認するには、**承認済み**をクリックし、次に**保存**をクリックします。

   「デバイスポリシー設定画面」(/en-us/citrix-endpoint-management/media/change-approval-status.png)

注：

「保留中の更新」テーブルには追加および削除コマンドが含まれていますが、これらのコマンドはCitrix Endpoint Managementデータベースに変更をもたらしません。承認ステータスの編集は、保留中の更新に対して利用可能な唯一のアクションです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスのWindows更新ステータスを表示するには、**管理 > デバイス > プロパティ**に移動します。

「デバイス設定画面」(/en-us/citrix-endpoint-management/media/device-details-win-updates-approved-to-install.png)

更新が公開されると、最初の列にステータス（成功または失敗）とともに**更新ID**が表示されます。失敗した更新があるデバイスに対してレポートまたは自動アクションを作成できます。公開日時も表示されます。

初回展開とそれ以降の展開での更新の仕組み

OS更新デバイスポリシーがデバイスに与える影響は、初回展開と、デバイスが更新を取得した後の展開とでは異なります。

- Citrix Endpoint Managementがデバイスに更新を照会するには、少なくとも1つのOS更新デバイスポリシーを構成し、デリバリーグループに割り当てる必要があります。

  Citrix Endpoint Managementは、デバイスのMDM同期中に、インストール可能な更新についてデバイスを照会します。
- 最初のOS更新デバイスポリシーが展開された後、まだデバイスが報告していないため、Windows更新のリストは空になります。
- 割り当てられたデリバリーグループ内のデバイスが更新を報告すると、Citrix Endpoint Managementはそれらの更新をデータベースに保存します。報告された更新を承認するには、ポリシーを再度編集します。

  更新の承認は、編集しているポリシーにのみ適用されます。あるポリシーで承認された更新は、別のポリシーでは承認済みとして表示されません。デバイスが次回同期するときに、Citrix Endpoint Managementは更新が承認されたことを示すコマンドをデバイスに送信します。
- 2番目のOS更新デバイスポリシーの場合、更新リストにはCitrix Endpoint Managementデータベースに保存されている更新が含まれます。各ポリシーの更新を承認します。

  各デバイス同期中に、Citrix Endpoint Managementは、デバイスが更新のインストールを報告するまで、承認された更新状態についてデバイスにクエリを実行します。インストール後に再起動が必要な更新の場合、Citrix Endpoint Managementは、デバイスが更新のインストールを報告するまで、更新の状態をクエリします。
- Citrix Endpoint Managementは、ポリシー構成ページに表示される更新をデリバリーグループまたはデバイスによって制限しません。デバイスによって報告されたすべての更新がリストに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android Enterpriseの設定

デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/device-policies-control-os-updates-android-enterprise.png)

- **システム更新ポリシー:** システム更新がいつ行われるかを決定します。
  - **自動:** 更新が利用可能になったときにインストールします。
  - **時間枠指定: 開始時刻**と**終了時刻**で指定された日次メンテナンス時間枠内で更新を自動的にインストールします。
    - **開始時刻:** メンテナンス時間枠の開始時刻。デバイスの現地時間の深夜からの分数（**0**～**1440**）で測定されます。デフォルトは**0**です。
    - **終了時刻:** メンテナンス時間枠の終了時刻。デバイスの現地時間の深夜からの分数（**0**～**1440**）で測定されます。デフォルトは**120**です。
  - **延期:** ユーザーが更新を最大30日間延期できるようにします。
  - **デフォルト:** 更新ポリシーをシステムデフォルトに設定します。
- **無線アップグレードを許可:** 無効にすると、ユーザーデバイスはワイヤレスでソフトウェア更新を受信できません。デフォルトは**オン**です。
- **フリーズ期間: オン**の場合、**自動**、**延期**、**時間枠指定**の更新ポリシーで指定された日付範囲中は、OS更新がデバイスにインストールされません。デバイスに設定できるフリーズ期間は一度に1つだけです。フリーズ期間の長さは90日を超えることはできません。
  - **開始日/終了日: フリーズ期間**が有効な場合にOS更新がインストールされない日付範囲。
- **フリーズ期間：オン**」の場合、「**自動**」、「**延期**」、「**期間指定**」の各更新ポリシーで指定された日付範囲中は、デバイスにOSアップデートがインストールされません。デバイスごとに設定できるフリーズ期間は1つだけです。フリーズ期間の長さは90日を超えることはできません。
  - **開始日/終了日：フリーズ期間**」が有効になっている場合にOSアップデートがインストールされない日付範囲。

パスコードデバイスポリシー

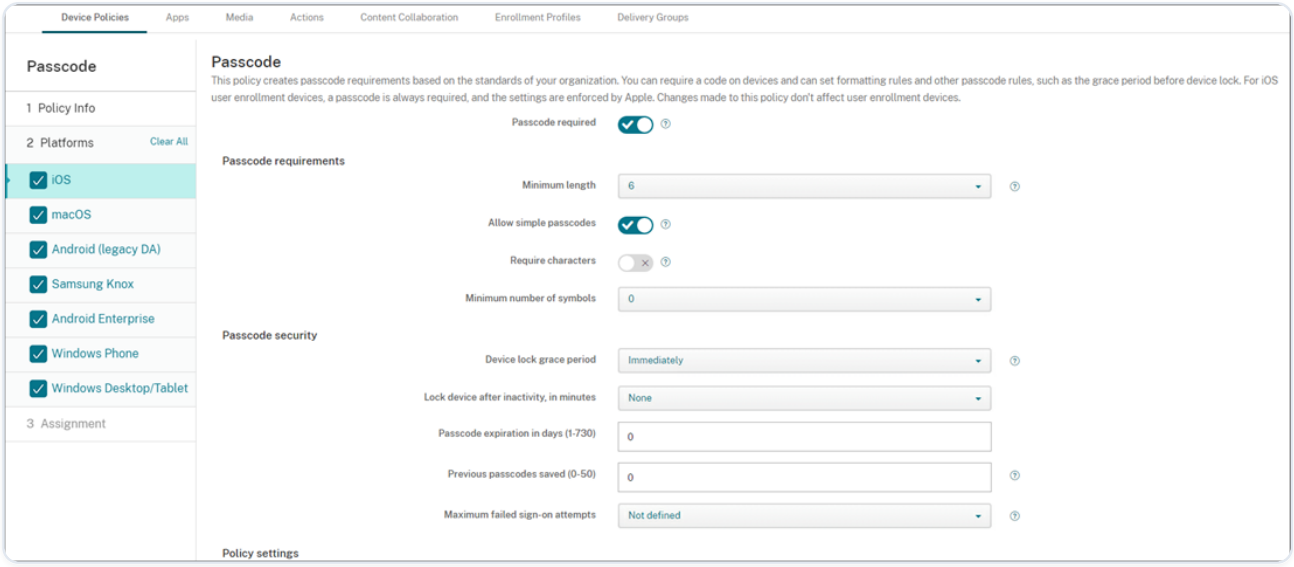
組織の基準に基づいて、Citrix Endpoint Management でパスコードポリシーを作成します。ユーザーのデバイスにパスコードを要求し、さまざまな書式設定とパスコードルールを設定できます。iOS、macOS、Android、Android Enterprise、および Windows デスクトップ/タブレット用の

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシーを作成します。各プラットフォームには異なる値のセットが必要であり、それらについてはこの記事で説明します。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、デバイスポリシーを参照してください。

iOS設定



- **パスコードが必要:** パスコードを要求し、iOSパスコードデバイスポリシーの構成オプションを表示するには、このオプションを選択します。ページが展開され、パスコード要件、パスコードセキュリティ、およびポリシー設定を構成できるようになります。
- **パスコードの要件**
  - **最小長:** ドロップダウンリストで最小パスコード長をクリックします。デフォルトは**6**です。
  - **簡単なパスコードを許可:** 簡単なパスコードを許可するかどうかを選択します。簡単なパスコードとは、繰り返しまたは連続した文字のセットです。デフォルトは**オン**です。
  - **必須文字:** パスコードに少なくとも1つの文字を含める必要があるかどうかを選択します。デフォルトは**オフ**です。
  - **記号の最小数:** リストで、パスコードに含める必要のある記号の数をクリックします。デフォルトは**0**です。
- **パスコードのセキュリティ**
  - **デバイスロック猶予期間:** リストで、ロックされたデバイスのロックを解除するためにユーザーがパスコードを入力する必要があるまでの時間を選択します。デフォルトは**即時**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

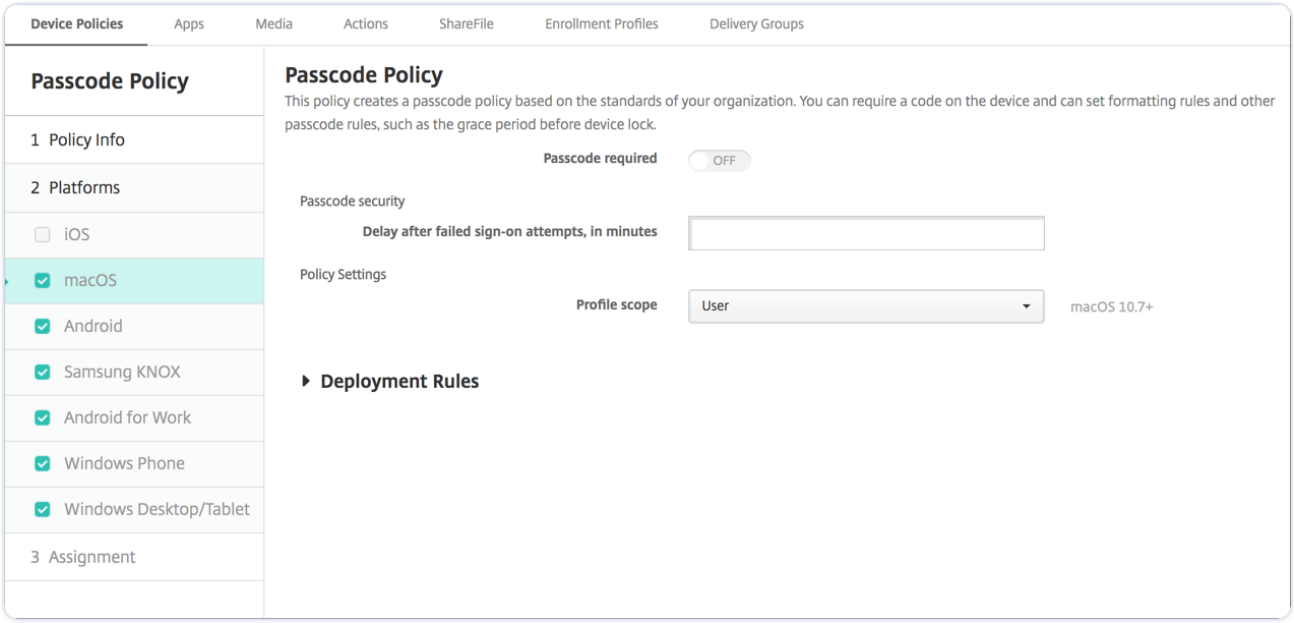
- **非アクティブ後にデバイスをロック:** ボックスに、デバイスがロックされるまでの非アクティブな時間を入力します。値は1分から15分の間です。ポリシーを無効にするには、値を**なし**に設定します。デフォルトは**なし**です。
- **パスコードの有効期限 (日数) (1-730):** パスコードの有効期限が切れるまでの日数を入力します。有効な値は1～730です。デフォルトは**0**で、これはパスコードの有効期限がないことを意味します。
- **保存された以前のパスワード (0-50):** 保存する使用済みパスワードの数を入力します。ユーザーはこのリストにあるパスワードを使用できません。有効な値は0～50です。デフォルトは**0**で、ユーザーはパスワードを再利用できます。
- **サインオン失敗の最大試行回数:** リストで、ユーザーがサインインに失敗できる回数をクリックします。
  - この数値を6より大きく設定した場合、6回目の試行後、デバイスは試行間に時間遅延を課します。時間遅延は、試行が失敗するたびに増加します。最終試行後、すべてのデータと設定は安全に消去されます。
  - 数値を6以下に設定した場合、デバイスは時間遅延なしで消去されます。
  - **未定義**を選択した場合、6回の試行後、デバイスは試行間に時間制限を徐々に長く課しますが、ワイプされません。

  デフォルトは**未定義**です。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除をスケジュールする方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS設定



- **パスコードが必要:** このオプションを選択すると、パスコードが必要になり、iOSパスコードデバイスポリシーの構成オプションが表示されます。ページが展開され、パスコード要件、パスコードセキュリティ、およびポリシー設定を構成できるようになります。
- **パスコードが必要**が無効になっている場合、**サインオン失敗後の遅延 (分)**の横に、ユーザーがパスコードを再入力できるようになるまでの遅延時間（分）を入力します。
- **パスコードが必要**を有効にした場合、次の設定を構成します。
- **パスコードの要件**
  - **最小の長さ：** ドロップダウンリストで、パスコードの最小の長さをクリックします。デフォルトは**6**です。
  - **簡易パスコードを許可：** 簡易パスコードを許可するかどうかを選択します。簡易パスコードとは、繰り返しまたは連続した文字のセットです。デフォルトは**オン**です。
  - **必須文字：** パスコードに少なくとも1つの文字を含めることを必須とするかどうかを選択します。デフォルトは**オフ**です。
  - **記号の最小数：** リストで、パスコードに含める必要のある記号の数をクリックします。デフォルトは**0**です。
- **パスコードのセキュリティ**
  - **デバイスロックの猶予期間：** リストで、ロックされたデバイスのロックを解除するためにユーザーがパスコードを入力する必要があるまでの時間をクリックします。デフォルトは**なし**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **非アクティブ後にデバイスをロック：** リストで、デバイスがロックされるまでに非アクティブでいられる時間をクリックします。値は1～5分の間です。ポリシーを無効にするには、値を**なし**に設定します。デフォルトは**なし**です。
- **パスコードの有効期限（日数）（1～730）：** パスコードの有効期限が切れるまでの日数を入力します。有効な値は1～730です。デフォルトは**0**で、これはパスコードの有効期限がないことを意味します。
- **保存された以前のパスワード（0～50）：** 保存する使用済みパスワードの数を入力します。ユーザーはこのリストにあるパスワードを使用できません。有効な値は0～50です。デフォルトは**0**で、これはユーザーがパスワードを再利用できることを意味します。
- **サインオン失敗の最大回数：** リストで、ユーザーがサインインに失敗できる回数をクリックします。
  - この数値を6より高く設定した場合、6回目の試行後、デバイスは試行間に時間遅延を課します。時間遅延は、試行が失敗するたびに増加します。最終試行後、デバイスはロックされます。
  - この数値を6以下に設定した場合、デバイスは時間遅延を実装せずにロックされます。
  - **未定義**を選択した場合、6回の試行後、デバイスは試行間に増加する時間制限を課しますが、ロックはされません。

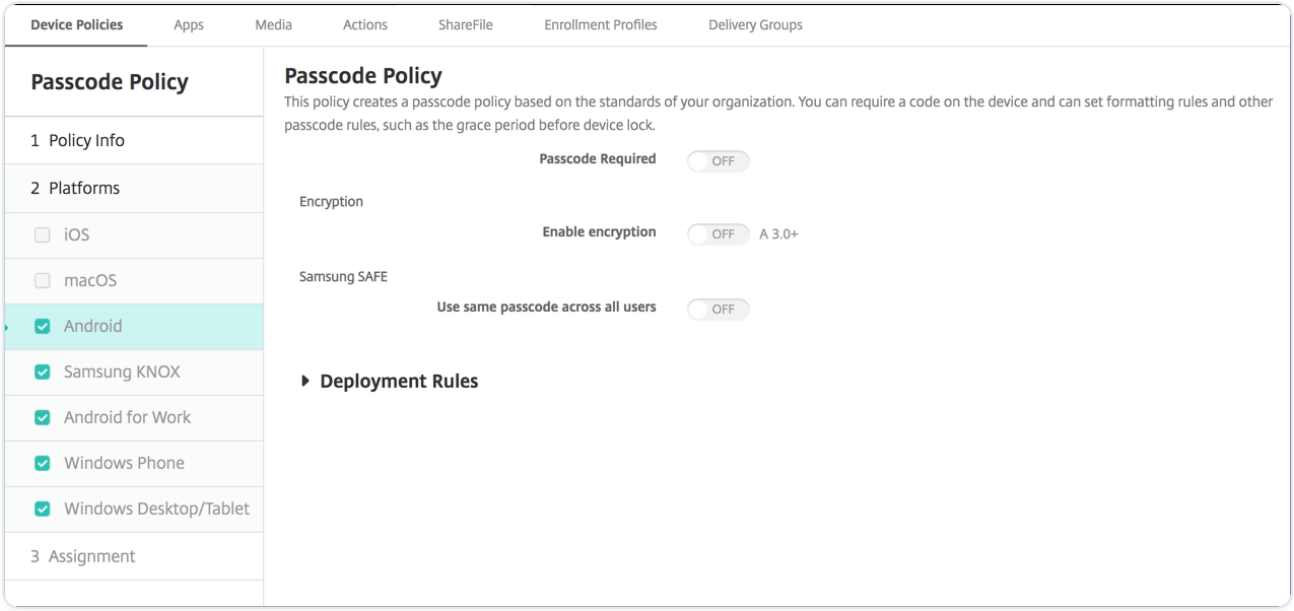
  デフォルトは**未定義**です。
- **ログイン試行失敗後の遅延（分）：** ユーザーが最大試行回数に達した後、ログインウィンドウが表示されるまでの分数を入力します。
- **パスコードのリセットを強制： オフ**の場合、ユーザーはデバイスがこのポリシーを受信した後、次回認証時にパスコードをリセットする必要はありません。デフォルトは**オン**です。

- **ポリシー設定**
  - **ポリシーの削除：** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間（時間）**です。
    - **日付を選択：** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）：** ポリシーが削除されるまでの時間を入力します。
  - **ユーザーによるポリシーの削除を許可：** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **プロファイルスコープ：** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

Android (レガシーDA) 設定



注：

Androidのデフォルト設定は**オフ**です。

- **パスコードが必要：** パスコードを要求し、Androidパスコードデバイスポリシーの構成オプションを表示するには、このオプションを選択します。ページが展開され、パスコード要件、パスコードセキュリティ、および暗号化の設定を構成できるようになります。
- **パスコード要件**
  - **最小の長さ：** ドロップダウンリストで最小パスコード長をクリックします。デフォルトは6です。
  - **生体認証:** 生体認証を有効にするかどうかを選択します。このオプションを有効にすると、「Required characters」フィールドは非表示になります。デフォルトは**オフ**です。
  - **必須文字:** リストで、パスコードの構成方法を設定するために、**制限なし**、**数字と文字の両方**、**数字のみ**、または**文字のみ**をクリックします。デフォルトは**制限なし**です。
  - **詳細ルール:** 詳細なパスコードルールを適用するかどうかを選択します。デフォルトは**オフ**です。
  - **詳細ルール**を有効にすると、以下の各リストから、パスコードに含める必要がある各文字タイプの最小数をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **記号:** 記号の最小数。
- **文字:** 文字の最小数。
- **小文字:** 小文字の最小数。
- **大文字:** 大文字の最小数。
- **数字または記号:** 数字または記号の最小数。
- **数字:** 数字の最小数。

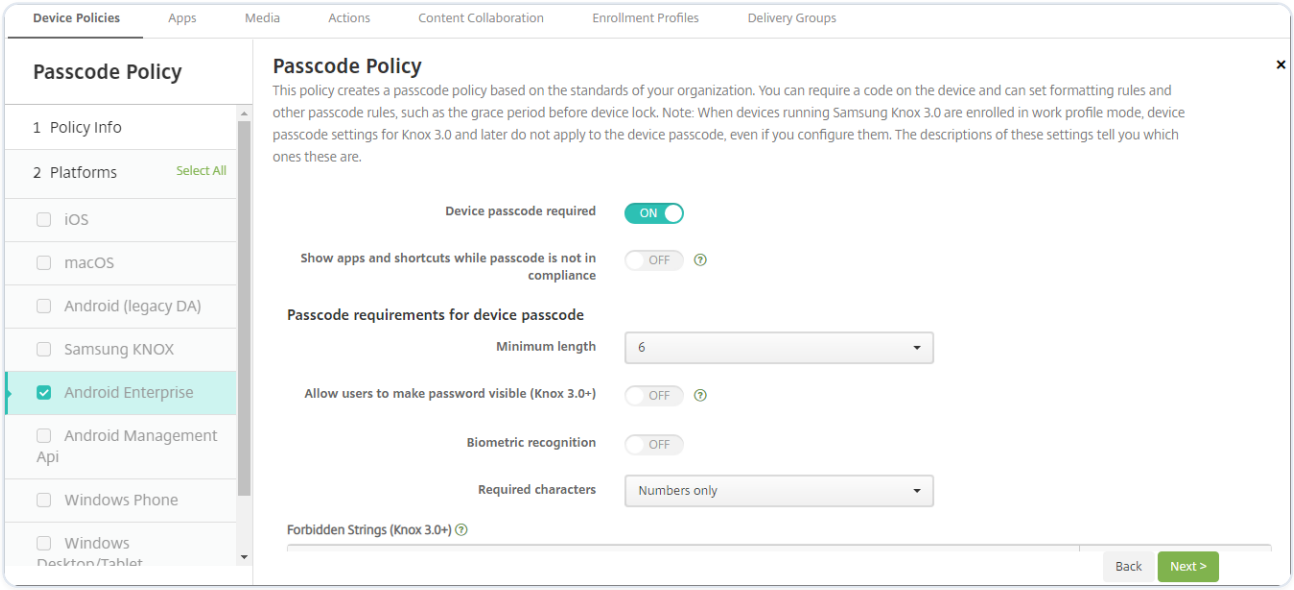
- **パスコードのセキュリティ**
  - **非アクティブ後のデバイスロック:** リストで、デバイスがロックされるまでの非アクティブ期間をクリックします。デフォルトは**なし**です。
  - **パスコードの有効期限（日数、1〜730）:** パスコードの有効期限が切れるまでの日数を入力します。有効な値は1〜730です。デフォルトは**0**で、これはパスコードの有効期限がないことを意味します。
  - **保存された以前のパスワード（0〜50）:** 保存する使用済みパスワードの数を入力します。ユーザーはこのリストにあるパスワードを使用できません。有効な値は0〜50です。デフォルトは**0**で、これはユーザーがパスワードを再利用できることを意味します。
  - **サインオン失敗の最大試行回数:** リストで、ユーザーがサインインに失敗できる回数をクリックします。この回数を超えるとデバイスがワイプされます。デフォルトは**未定義**です。

- **暗号化**
  - **暗号化を有効にする:** 暗号化を有効にするかどうかを選択します。このオプションは、**パスコードが必要**の設定に関係なく利用できます。

    デバイスを暗号化するには、ユーザーはバッテリーを充電した状態から開始し、暗号化が完了するまでデバイスを接続したままにする必要があります。このプロセスには1時間以上かかる場合があります。暗号化プロセスを中断すると、デバイス上の一部のデータまたはすべてのデータが失われる可能性があります。デバイスが暗号化されると、工場出荷時設定にリセットしてデバイス上のすべてのデータを消去しない限り、プロセスを元に戻すことはできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android Enterpriseの設定



Android Enterpriseデバイスの場合、デバイスにパスコードを要求したり、Android Enterpriseの仕事用プロファイルにセキュリティチャレンジを要求したり、その両方を要求したりできます。

- **デバイスパスコードが必要:** デバイスにパスコードを要求します。この設定が**オン**の場合、**デバイスパスコードのパスコード要件**と**デバイスパスコードのパスコードセキュリティ**の設定を構成します。デフォルトは**オフ**です。
- **パスコードが準拠していないときにアプリとショートカットを表示する:** この設定が**オン**の場合、パスコードが準拠していなくても、デバイス上のアプリとショートカットは非表示になりません。この設定が**オフ**の場合、パスコードが準拠していないときにアプリとショートカットは非表示になります。この設定を有効にする場合、Citrix®は、パスコードが準拠していないときにデバイスを非準拠としてマークする自動アクションを作成することをお勧めします。デフォルトは**オフ**です。
- **デバイスパスコードのパスコード要件:**
  - **最小の長さ:** 最小パスコード長を指定します。デフォルトは6です。
  - **生体認証:** 生体認証を有効にします。この設定が**オン**の場合、**必要な文字**フィールドは非表示になります。デフォルトは**オフ**です。
  - **必要な文字:** パスコードに必要な文字の種類を指定します。リストから、**制限なし**、**数字と文字の両方**、**数字のみ**、または**文字のみ**を選択します。**制限なし**は、Android 7.0を実行しているデバイスでのみ使用してください。Android 7.1以降では、**制限なし**の設定は適用されません。デフォルトは**数字と文字の両方**です。
  - **詳細ルール:** パスコードで使用できる文字の種類に関する詳細ルールを適用します。この設定が**オン**の場合、**最小数**と**最大数**の設定を構成します。この設定は、Android 5.0より前のAndroidデバイスでは利用できません。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **最小数:**
  - **記号:** 記号の最小数を指定します。デフォルトは**0**です。
  - **文字:** 最小文字数を指定します。デフォルトは**0**です。
  - **小文字:** 最小小文字数を指定します。デフォルトは**0**です。
  - **大文字:** 最小大文字数を指定します。デフォルトは**0**です。
  - **数字または記号:** 最小数字または記号の数を指定します。デフォルトは**0**です。
  - **数字:** 最小数字数を指定します。デフォルトは**0**です。
  - **変更された文字:** 有効なKnoxライセンスキーが構成されているSamsung Knox 3.0以降を実行しているデバイスの場合。フルマネージドデバイスのみ。この設定は、ワークプロファイルデバイスとして登録されているデバイスには適用されません。ユーザーが以前のパスコードから変更する必要がある文字数を指定します。デフォルトは**0**です。
- **最大数:** 有効なKnoxライセンスキーが構成されているSamsung Knox 3.0以降を実行しているデバイスの場合。フルマネージドデバイスのみ。この設定は、ワークプロファイルデバイスとして登録されているデバイスには適用されません。
  - **文字の出現回数:** パスコード内で文字が出現できる最大回数を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。
  - **英字シーケンスの長さ:** パスコード内の英字シーケンスの最大長を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。
  - **数字シーケンスの長さ:** パスコード内の数字シーケンスの最大長を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。

- **デバイスパスコードのパスコードの複雑さ (Android 12+):**
  - **パスコードの複雑さを適用:** カスタムパスワード要件ではなく、プラットフォームによって定義された複雑さレベルのパスワードを要求します。Android 12以降のデバイスで、Citrix Secure Hub 22.9以降を使用している場合にのみ適用されます。
  - **複雑さレベル:** 事前定義されたパスワードの複雑さレベル。
    - **なし:** パスワードは不要です。
    - **低:** パスワードは次のいずれかです。
      - パターン
      - 4桁以上の数字のPIN
    - **中:** パスワードは次のいずれかです:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 繰り返しシーケンス (4444) または順序付きシーケンス (1234) を含まない4桁以上の数字のPIN
    - 4文字以上の英字
    - 4文字以上の英数字
  - **高:** パスワードは次のいずれかです:
    - 繰り返しシーケンス (4444) または順序付きシーケンス (1234) を含まない8桁以上の数字のPIN
    - 6文字以上の英字
    - 6文字以上の英数字

> **注:**
>
> BYODデバイスの場合、最小の長さ、必須文字、生体認証、詳細ルールなどのパスコード設定はAndroid 12以降では適用されません。代わりにパスコードの複雑さを使用してください。

- **デバイスパスコードのパスコードセキュリティ:**
  - **デバイスをワイプするまでの回数 (サインオン失敗回数):** ユーザーがサインオンに失敗できる回数を指定します。この回数を超えると、デバイスは完全にワイプされます。デフォルトは**未定義**です。
  - **非アクティブ後にデバイスをロックする:** デバイスがロックされるまでの非アクティブな時間を分単位で指定します。ポリシーを無効にするには、値を0に設定します。
  - **パスコードの有効期限 (日数) (1〜730):** パスコードの有効期限が切れるまでの日数を指定します。有効な値は1〜730です。デフォルトは**0**で、パスコードの有効期限がないことを意味します。
  - **保存された以前のパスワード (0〜50):** 保存する使用済みパスワードの数を指定します。ユーザーはこのリストにあるパスワードを使用できません。有効な値は0〜50です。デフォルトは**0**で、ユーザーがパスワードを再利用できることを意味します。
- **仕事用プロファイルのセキュリティチャレンジ:** Android Enterpriseの仕事用プロファイルで実行されているアプリにアクセスするために、ユーザーにセキュリティチャレンジの完了を要求します。Android 7.0以降を実行しているデバイス向けです。この設定が**オン**の場合、**仕事用プロファイルのセキュリティチャレンジのパスコード要件**および**仕事用プロファイルのセキュリティチャレンジのパスコードセキュリティ**の設定を構成します。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **仕事用プロファイルのセキュリティチャレンジのパスコード要件:**
  - **最小の長さ:** パスコードの最小の長さを指定します。デフォルトは6です。
  - **生体認証:** 生体認証を有効にします。この設定が**オン**の場合、**必須文字**フィールドは非表示になります。デフォルトは**オフ**です。
  - **必須文字:** パスコードに必要な文字の種類を指定します。リストから、**制限なし**、**数字と文字の両方**、**数字のみ**、または**文字のみ**を選択します。**制限なし**は、Android 7.0を実行しているデバイスでのみ使用してください。Android 7.1以降では、**制限なし**設定は適用されません。デフォルトは**数字と文字の両方**です。
  - **詳細ルール:** パスコードに含めることができる文字の種類に関する詳細ルールを適用します。この設定が**オン**の場合、**最小数**および**最大数**の設定を構成します。この設定は、Android 5.0より前のAndroidデバイスでは利用できません。デフォルトは**オフ**です。
  - **最小数:**
    - **記号:** 記号の最小数を指定します。デフォルトは**0**です。
    - **文字:** 文字の最小数を指定します。デフォルトは**0**です。
    - **小文字:** 小文字の最小数を指定します。デフォルトは**0**です。
    - **大文字:** 大文字の最小数を指定します。デフォルトは**0**です。
    - **数字または記号:** 数字または記号の最小数を指定します。デフォルトは**0**です。
    - **数字:** 数字の最小数を指定します。デフォルトは**0**です。
    - **変更する文字数:** 有効なKnoxライセンスキーが構成されているKnox 3.0以降を実行しているデバイスの場合。ユーザーが以前のパスコードから変更する必要がある文字数を指定します。デフォルトは**0**です。
  - **最大数:** 有効なKnoxライセンスキーが構成されているKnox 3.0以降を実行しているデバイスの場合。
    - **文字の出現回数:** パスコード内で文字が出現できる最大回数を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。
    - **アルファベット順の長さ:** パスコード内のアルファベット順の最大長を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。
    - **数字順の長さ:** パスコード内の数字順の最大長を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。
- **仕事用プロファイルのセキュリティチャレンジのパスコードの複雑さ (Android 12+):**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **パスコードの複雑さを適用:** カスタムパスワード要件ではなく、プラットフォームによって定義された複雑さレベルのパスワードを要求します。Android 12以降のデバイスで、Citrix Secure Hub 22.9以降を使用している場合にのみ適用されます。
- **複雑さのレベル:** パスワードの複雑さの事前定義されたレベル。
  - **なし:** パスワードは不要です。
  - **低:** パスワードは次のいずれかです。
    - パターン
    - 最低4桁のPIN
  - **中:** パスワードは次のいずれかです。
    - 繰り返しシーケンス (4444) や順序付きシーケンス (1234) がなく、最低4桁のPIN
    - 最低4文字のアルファベット
    - 4文字以上の英数字
  - **高:** パスワードは次のいずれかです。
    - 繰り返しシーケンス (4444) や順序付きシーケンス (1234) がなく、8桁以上のPIN
    - 6文字以上の英字
    - 6文字以上の英数字

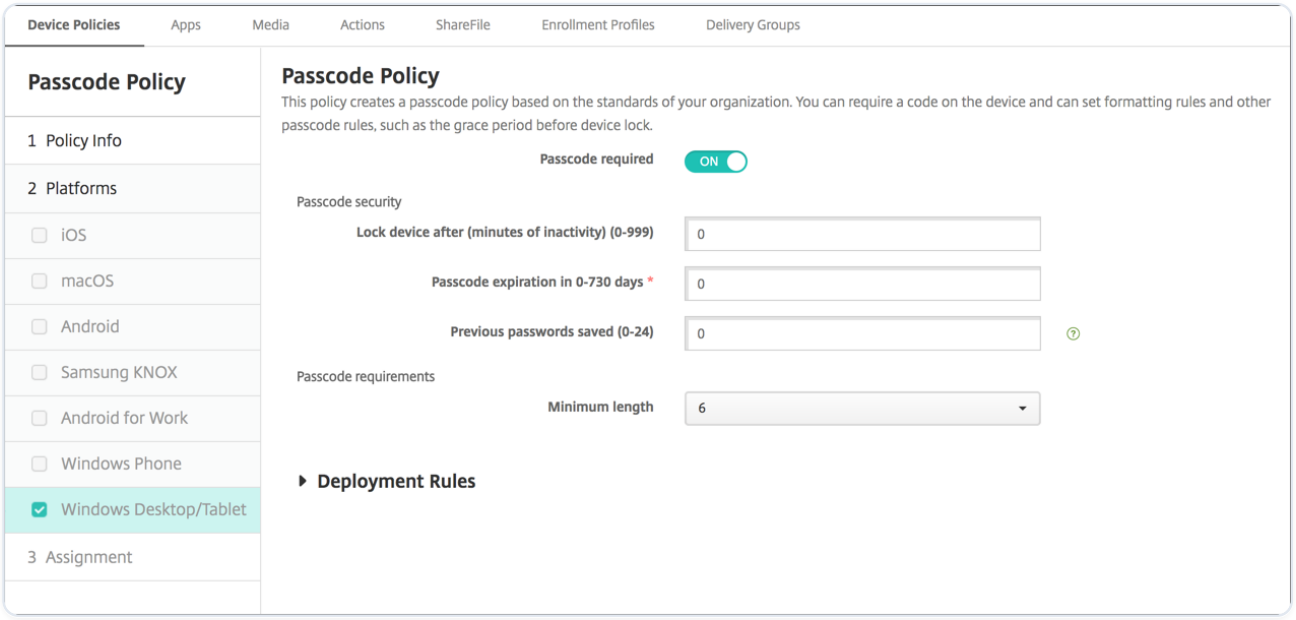
> **注:**
>
> ワークプロファイルのパスコードの複雑さを有効にする場合は、デバイスでも有効にする必要があります。

- **ワークプロファイルのセキュリティチャレンジのパスコードセキュリティ**
  - **コンテナをワイプするまでの回数（サインオン失敗回数）：** ユーザーがサインオンに失敗できる回数を指定します。この回数を超えると、ワークプロファイルとそのデータがデバイスからワイプされます。ワイプ後、ユーザーはワークプロファイルを再初期化する必要があります。デフォルトは**未定義**です。
  - **非アクティブ後にコンテナをロックする：** ワークプロファイルがロックされるまでにデバイスが非アクティブでいられる分数を示します。値は0～999分の間です。ポリシーを無効にするには、値を0に設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **パスコードの有効期限（日数）（1〜730）：** パスコードが期限切れになるまでの日数を指定します。有効な値は1〜730です。デフォルトは**0**で、パスコードは期限切れになりません。
- **保存された以前のパスワード（0〜50）：** 保存する使用済みパスワードの数を指定します。ユーザーはこのリストにあるパスワードを使用できません。有効な値は0〜50です。デフォルトは**0**で、ユーザーはパスワードを再利用できます。

Windowsデスクトップ/タブレットの設定



- **パスコードが必要：** Windowsデスクトップ/タブレットデバイスにパスコードを要求しない場合は、このオプションを選択します。デフォルト設定は**オン**で、パスコードが必要です。この設定を無効にすると、ページが折りたたまれ、以下のオプションが非表示になります。
- **パスコードセキュリティ**
  - **非アクティブ状態の後でデバイスをロック:** デバイスがロックされるまでに非アクティブ状態を維持できる分数を入力します。デフォルトは**0**です。
  - **パスコードの有効期限 (日数) (0-730):** パスコードの有効期限が切れるまでの日数を入力します。有効な値は0〜730です。デフォルトは**0**で、これはパスコードの有効期限がないことを意味します。
  - **以前に保存されたパスワード (0-24):** 保存する使用済みパスコードの数を入力します。ユーザーは、このリストにあるパスコードを使用できません。有効な値は1〜24です。このフィールドに1から24までの数値を入力します。デフォルトは**0**です。
- **パスコードの要件**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **最小の長さ:** ドロップダウンリストで最小パスコードの長さをクリックします。デフォルトは**6**です。

パスコードロック猶予期間デバイスポリシー

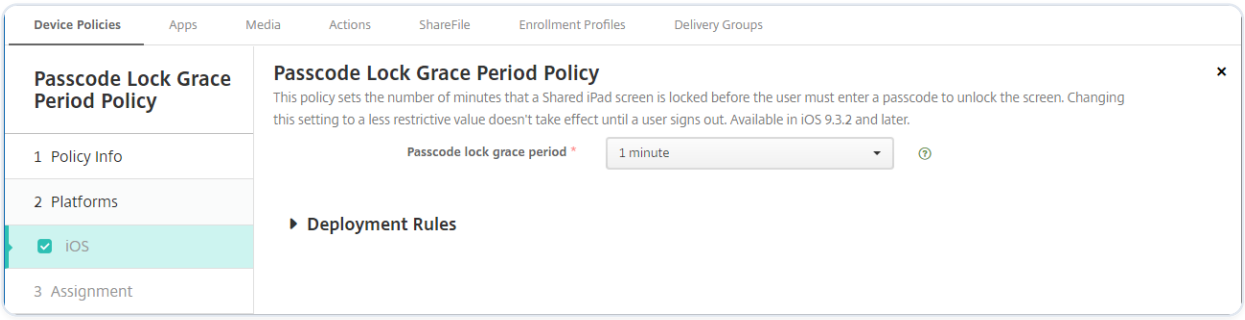
パスコードロック猶予期間デバイスポリシーは、iOS (iPadOS) を実行している共有デバイス用です。共有iPadの詳細については、「Apple Education機能との統合」を参照してください。

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］**の順に選択します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **パスコードロック猶予期間:** 共有iPadの画面がロックされたままになり、ユーザーが画面のロックを解除するためにパスコードを入力する必要があるまでの分数。この設定をより制限の少ない値に変更しても、ユーザーがサインアウトするまで有効になりません。デフォルトは**［即時］**です。

  デフォルトでは、共有iPadは2分間操作がないと自動的にロックされます。



パーソナルホットスポットデバイスポリシー

ユーザーがWi-Fiネットワークの範囲外にいる場合でも、iOSデバイスのパーソナルホットスポット機能を通じてセルラーデータ接続を使用することで、インターネットに接続できるようにすることができます。

このポリシーを追加または構成するには、**Configure > Device Policies** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **パーソナルホットスポットを無効にする:** ユーザーデバイスでパーソナルホットスポット機能を無効にするかどうかを選択します。デフォルトは**オフ**で、ユーザーデバイスのパーソナルホットスポットをオフにします。このポリシーは機能を無効にするものではありません。ユー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

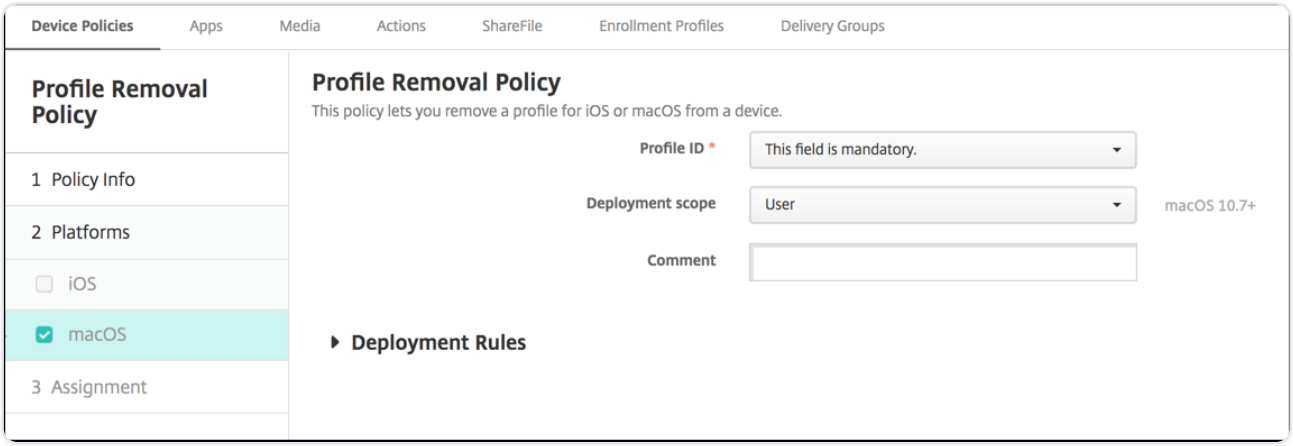
ザーは引き続きデバイスでパーソナルホットスポットを使用できますが、ポリシーが展開されると、パーソナルホットスポットはデフォルトでオンにならないようにオフになります。

プロファイル削除デバイスポリシー

Citrix Endpoint Managementでアプリプロファイル削除デバイスポリシーを作成できます。このポリシーを展開すると、ユーザーのiOSまたはmacOSデバイスからアプリプロファイルが削除されます。

このポリシーを追加または構成するには、 > に移動します。詳しくは、「デバイスポリシー」を参照してください。

macOS設定



- **プロファイルID:** ドロップダウンリストでアプリプロファイルIDをクリックします。このフィールドは必須です。
- **展開スコープ:** ドロップダウンリストで または をクリックします。デフォルトは です。このオプションはmacOS 10.7以降でのみ利用可能です。
- **コメント:** オプションのコメントを入力します。

プロビジョニングプロファイルデバイスポリシー

iOSエンタープライズアプリを開発し、コード署名する際、通常、AppleがiOSデバイスでアプリを実行するために必要とするエンタープライズ配布プロビジョニングプロファイルを含めます。プロビジョニングプロファイルが見つからないか期限切れの場合、ユーザーがアプリを開こうとタップすると、アプリがクラッシュします。

プロビジョニングプロファイルの主な問題は、Apple Developer Portalで生成されてから1年で期限切れになることです。そのため、ユーザーが登録したすべてのiOSデバイス上のすべてのプロビジョニングプロファイルの有効期限を追跡する必要があります。有効期限を追跡するには、実際

© 1997–2026 Citrix Systems, Inc. All rights reserved.

の有効期限だけでなく、どのユーザーがどのバージョンのアプリを使用しているかも把握する必要があります。2つの解決策として、プロビジョニングプロファイルをユーザーにメールで送信するか、ダウンロードしてインストールできるようにWebポータルに配置する方法があります。これらの解決策は機能しますが、ユーザーがメールの指示に対応したり、Webポータルにアクセスして正しいプロファイルをダウンロードしてインストールしたりする必要があるため、エラーが発生しやすいです。

このプロセスをユーザーにとって透過的にするために、Citrix Endpoint Managementでは、デバイスポリシーを使用してプロビジョニングプロファイルをインストールおよび削除できます。不足しているプロファイルや期限切れのプロファイルは必要に応じて削除され、最新のプロファイルがユーザーのデバイスにインストールされるため、アプリをタップするだけで使用できるようになります。

プロビジョニングプロファイルポリシーを作成する前に、プロビジョニングプロファイルファイルを作成する必要があります。詳細については、Apple Developerサイトで開発プロビジョニングプロファイルを作成する方法に関するAppleの記事を参照してください。

iOS設定

- **iOSプロビジョニングプロファイル: 参照**をクリックしてファイルが保存されている場所に移動し、インポートするプロビジョニングプロファイルファイルを選択します。

プロビジョニングプロファイル削除デバイスポリシー

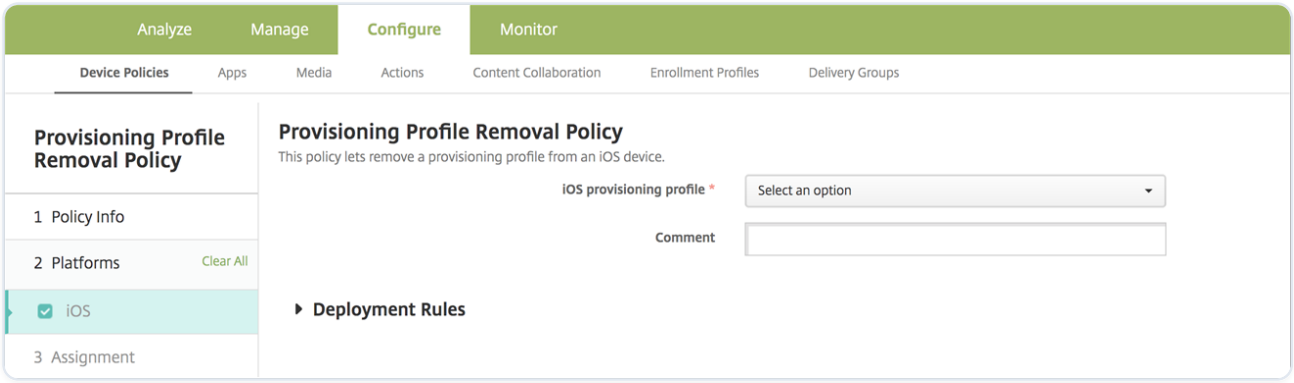
プロビジョニングプロファイルを使用すると、iOSアプリをユーザーデバイスに配布できます。Appleは、iOSデバイスでアプリを実行することを承認するために、プロビジョニングプロファイルを使用してアプリに署名することを要求しています。詳細については、「プロビジョニングプロファイルデバイスポリシー」を参照してください。

古いプロビジョニングプロファイルを削除または置き換えるには、プロビジョニングプロファイル削除デバイスポリシーを使用します。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定



- **iOSプロビジョニングプロファイル:** 削除するプロビジョニングプロファイルをドロップダウンリストでクリックします。
- **コメント:** 必要に応じて、コメントを追加します。

プロキシデバイスポリシー

プロキシデバイスポリシーは、サポートされているiOSデバイスのグローバルHTTPプロキシ設定を指定します。デバイスごとに展開できるグローバルHTTPプロキシポリシーは1つだけです。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

前提条件

このポリシーを展開する前に、グローバルHTTPプロキシを設定するすべてのiOSデバイスを監視モードに設定してください。詳細については、「Apple Configurator 2を使用してデバイスを展開する」または「Apple Deployment Programを通じてデバイスを展開する」を参照してください。

デバイスにプロキシポリシーを送信する前に、デバイスを登録するための展開ルールを設定します。

iOS設定

- **プロキシ構成:** ユーザーのデバイスでプロキシを構成する方法として、 または をクリックします。
    - をクリックした場合は、次の設定を構成します。
        - **プロキシサーバーのホスト名またはIPアドレス:** プロキシサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **プロキシサーバーのポート:** プロキシサーバーのポート番号を入力します。このフィールドは必須です。
    - **ユーザー名:** プロキシサーバーに認証するためのオプションのユーザー名を入力します。
    - **パスワード:** プロキシサーバーに認証するためのオプションのパスワードを入力します。
  - をクリックした場合は、次の設定を構成します。
    - **プロキシPAC URL:** プロキシ構成を定義するPACファイルのURLを入力します。
    - **PACに到達できない場合に直接接続を許可する:** PACファイルに到達できない場合に、ユーザーが直接宛先に接続することを許可するかどうかを選択します。デフォルトは**オン**です。

- **キャプティブネットワークにアクセスするためにプロキシをバイパスすることを許可する:** キャプティブネットワークにアクセスするためにプロキシをバイパスすることを許可するかどうかを選択します。デフォルトは**オフ**です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

制限デバイスポリシー

注:

アップグレードに新しい制限デバイスポリシー設定が含まれている場合、ポリシーを編集して保存する必要があります。Citrix Endpoint Managementは、保存するまでアップグレードされた制限デバイスポリシーを展開しません。

制限デバイスポリシーでは、カメラなど、ユーザーデバイス上の特定の機能や機能を許可または制限します。セキュリティ制限やメディアコンテンツの制限を設定できます。また、ユーザーがインストールできるアプリとできないアプリの種類に制限を設定することもできます。ほとんどの制

© 1997–2026 Citrix Systems, Inc. All rights reserved.

限設定はデフォルトで**オン**、つまり*許可*されています。主な例外は、iOSセキュリティ - 強制機能とすべてのWindowsタブレット機能で、これらはデフォルトで**オフ**、つまり*制限*されています。

オンを選択したオプションはすべて、ユーザーがその操作を実行したり、その機能を使用したりできることを意味します。例:

- **カメラ: オン**の場合、ユーザーはデバイスのカメラを使用できます。**オフ**の場合、ユーザーはデバイスのカメラを使用できません。
- **スクリーンショット: オン**の場合、ユーザーはデバイスでスクリーンショットを撮ることができます。**オフ**の場合、ユーザーはデバイスでスクリーンショットを撮ることができません。

制限デバイスポリシーとキオスクデバイスポリシーの両方が構成されている場合、制限デバイスポリシーが優先されます。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定



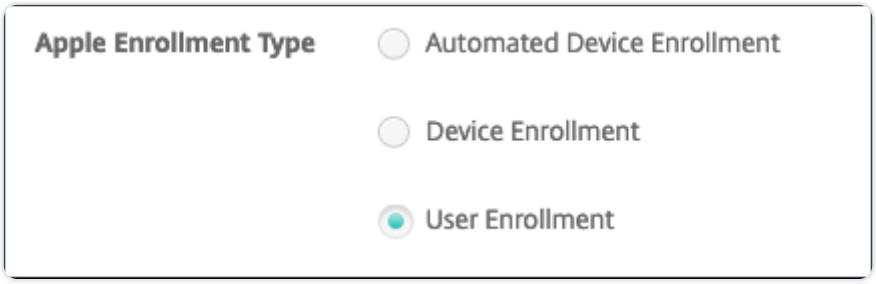
一部のiOS制限ポリシー設定は、ここに記載されているとおり、またCitrix Endpoint Managementコンソールの制限ポリシーページに記載されているとおり、特定のバージョンのiOSにのみ適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

これらの設定は、デバイスがユーザー登録モード、非監視（完全MDM）モード、または監視モードで登録されている場合に適用されます。次の表は、iOS 13以降の各設定で利用可能な登録モードを示しています。

- **自動デバイス登録:** 監視対象デバイス。これらは一括登録によって登録されるデバイスです。
- **デバイス登録:** 非監視対象デバイス。これらのデバイスは個別に登録され、デバイス全体が完全なMDMです。
- **ユーザー登録:** 特定のユーザーのみが管理されるデバイス。ユーザー登録の詳細については、Appleのドキュメントを参照してください。

iOS制限ポリシー設定は、デバイスがユーザー登録モード、非監視（フルMDM）モード、または監視モードで登録されている場合に適用されることがあります。次の表は、iOS 13以降の各制限ポリシー設定で利用可能な登録モードを示しています。



表に示されているように、以前は非監視モードと監視モードで利用可能だった一部の設定は、iOS 13以降では監視モードでのみ利用可能です。以下のルールが適用されます。

- 監視対象のiOS 13以降のデバイスがCitrix Endpoint Managementに登録されている場合、設定はデバイスに適用されます。
- 非監視対象のiOS 13以降のデバイスがCitrix Endpoint Managementに登録されている場合、設定はデバイスに適用されません。
- iOS 12（またはそれ以前）のデバイスがすでにCitrix Endpoint Managementに登録されており、その後iOS 13にアップグレードしても、変更はありません。設定は、アップグレード前と同様にデバイスに適用されます。

iOSデバイスを監視モードに設定する方法については、Apple Configurator 2を使用してデバイスを展開するを参照してください。

設定	ユーザー登録	非監視	監視
ハードウェア制御を許可			
カメラ	いいえ	はい	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
FaceTime	いいえ	いいえ	はい
FaceTimeリモートコントロールを許可する	いいえ	いいえ	はい
画面キャプチャ	はい	いいえ	はい
Classroomアプリが学生の画面をリモートで監視することを許可する	いいえ	いいえ	はい
Classroomアプリがプロンプトなしで AirPlayと画面表示を実行できるようにする	いいえ	いいえ	はい
フォトストリーム	いいえ	はい	はい
共有フォトストリーム	いいえ	はい	はい
共有iPadの一時セッションを許可	いいえ	いいえ	はい
音声ダイヤル	いいえ	はい	はい
Siri (シリ)	はい	はい	はい
デバイスロック中に許可	はい	はい	はい
Siriの不適切な言葉のフィルター	いいえ	いいえ	はい
アプリのインストール	いいえ	いいえ	はい
代替アプリマーケットプレイス	いいえ	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
Web配布アプリ	いいえ	いいえ	はい
ローミング中にグローバルバックグラウンドフェッチを許可する	いいえ	はい	はい
アプリを許可する			
iTunes ストア	いいえ	いいえ	はい
アプリ内購入	いいえ	はい	はい
購入時にiTunes Storeのパスワードを要求する	いいえ	はい	はい
サファリ	いいえ	いいえ	はい
自動入力	いいえ	いいえ	はい
詐欺警告を強制する	はい	はい	はい
JavaScriptを有効にする	いいえ	はい	はい
ポップアップをブロックする	いいえ	はい	はい
Cookieを許可する	いいえ	はい	はい
ネットワーク - iCloudアクションを許可する			
iCloudの書類とデータ	いいえ	いいえ	はい
iCloudバックアップ	いいえ	はい	はい
iCloud写真キーチェーン	いいえ	はい	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
iCloud写真ライブラリ	いいえ	はい	はい
セキュリティ - 強制			
暗号化されたバックアップ	はい	はい	はい
広告追跡の制限	いいえ	はい	はい
初回AirPlayペアリング時のパスコード	はい	はい	はい
手首検出を使用するペアリングされたApple Watch	はい	はい	はい
AirDrop を使用した管理対象ドキュメントの共有	はい	はい	はい
セキュリティ - 許可			
信頼されていないSSL 証明書の受け入れ	いいえ	はい	はい
証明書信頼設定の自動更新	いいえ	はい	はい
管理されたペーストボードを要求する	はい	はい	はい
管理対象外アプリ内の管理対象アプリからのドキュメント	はい	はい	はい
管理対象外アプリが管理対象の連絡先を読み取る	いいえ	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
管理対象アプリが管理対象外の連絡先に書き込む	いいえ	いいえ	はい
管理対象アプリ内の管理対象外アプリからのドキュメント	はい	はい	はい
Appleへの診断情報の送信	はい	はい	はい
Touch IDによるデバイスのロック解除	いいえ	はい	はい
自動ロック解除	いいえ	はい	はい
ロック時のWallet通知	いいえ	はい	はい
ハンドオフ	いいえ	はい	はい
管理対象アプリのiCloud同期	はい	はい	はい
エンタープライズブックのバックアップ	はい	はい	はい
エンタープライズブックのメモとハイライトの同期	はい	はい	はい
Spotlightでのインターネット検索結果	いいえ	はい	はい
エンタープライズアプリの信頼	いいえ	はい	はい
Appleのパーソナライズされた広告を許可する	いいえ	はい	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
監視対象デバイスのみの設定 - 許可			
eSIMの変更を許可する	いいえ	いいえ	はい
消去時にeSIMを保持する	いいえ	いいえ	はい
すべてのコンテンツと設定を消去する	いいえ	いいえ	はい
スクリーンタイム	いいえ	いいえ	はい
ポッドキャスト	いいえ	いいえ	はい
構成プロファイルのインストール	いいえ	いいえ	はい
Touch IDおよびFace IDの変更	いいえ	いいえ	はい
デバイスからのアプリのインストール	いいえ	いいえ	はい
キーボードショートカット	いいえ	いいえ	はい
ペアリングされたApple Watch	いいえ	いいえ	はい
パスコードの変更	いいえ	いいえ	はい
デバイス名の変更	いいえ	いいえ	はい
壁紙の変更	いいえ	いいえ	はい
アプリの自動ダウンロード	いいえ	いいえ	はい
AirDrop	いいえ	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
iMessage	いいえ	いいえ	はい
Siriユーザー生成コンテンツ	いいえ	いいえ	はい
iBooks	いいえ	いいえ	はい
アプリの削除	いいえ	はい	はい
ゲームセンター	いいえ	いいえ	はい
友達を追加	いいえ	いいえ	はい
マルチプレイヤーゲーム	いいえ	いいえ	はい
アカウント設定の変更	いいえ	いいえ	はい
アプリのモバイルデータ設定の変更	いいえ	いいえ	はい
アプリのモバイルデータ設定の変更	いいえ	いいえ	はい
ネットワークドライブ接続を許可	いいえ	いいえ	はい
USBデバイス接続を許可	いいえ	いいえ	はい
「デバイスを探す」を許可	いいえ	いいえ	はい
「友達を探す」設定を許可	いいえ	いいえ	はい
「友達を探す」設定の変更	いいえ	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
Configurator以外のホストとのペアリング	いいえ	いいえ	はい
予測キーボード	いいえ	いいえ	はい
キーボードの自動修正	いいえ	いいえ	はい
キーボードのスペルチェック	いいえ	いいえ	はい
QuickPathキーボードを許可	いいえ	いいえ	はい
定義の検索	いいえ	いいえ	はい
単一アプリのバンドルID	いいえ	いいえ	はい
ニュース	いいえ	いいえ	はい
Apple Musicサービス	いいえ	いいえ	はい
Apple Musicラジオ	いいえ	いいえ	はい
通知の変更	いいえ	いいえ	はい
制限付きアプリの使用	いいえ	いいえ	はい
診断提出の変更	いいえ	いいえ	はい
Bluetoothの変更	いいえ	いいえ	はい
音声入力を許可する	いいえ	いいえ	はい
Wi-Fiのオン/オフを変更する	いいえ	いいえ	はい
ネットワークポリシーによってインス	いいえ	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
トールされたWi-Fi ネットワークのみに参加する			
Classroomアプリがプロンプトなしで AirPlayと画面表示を実行することを許可する	いいえ	いいえ	はい
Classroomアプリがプロンプトなしでアプリにロックし、デバイスをロックすることを許可する	いいえ	いいえ	はい
Classroomアプリのクラスにプロンプトなしで自動的に参加する	いいえ	いいえ	はい
AirPrintを許可する	いいえ	いいえ	はい
AirPrintの資格情報をキーチェーンに保存することを許可する	いいえ	いいえ	はい
iBeacon を使用した AirPrint プリンターの検出を許可する	いいえ	いいえ	はい
信頼された証明書を持つ宛先への AirPrint のみを許可する	いいえ	いいえ	はい
VPN 構成の追加	いいえ	いいえ	はい
携帯電話プラン設定の変更	いいえ	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
システムアプリの削除	いいえ	いいえ	はい
新しい近くのデバイスのセットアップ	いいえ	いいえ	はい
USB制限モードを許可	いいえ	いいえ	はい
ソフトウェアアップデートの遅延を強制する	いいえ	いいえ	はい
強制されたソフトウェアアップデートの遅延	いいえ	いいえ	はい
クラスを離れるための教室リクエスト許可を強制する	いいえ	いいえ	はい
自動入力前の認証を強制する	いいえ	いいえ	はい
日付と時刻の自動設定を強制する	いいえ	いいえ	はい
パスワードの自動入力	いいえ	いいえ	はい
パスワードの近接リクエスト	いいえ	いいえ	はい
パスワード共有	いいえ	いいえ	はい
パーソナルホットスポットの変更を許可する	いいえ	いいえ	はい
ペアリングされていないデバイスによる	いいえ	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
リカバリへの起動を許可する			
迅速なセキュリティ対応をインストールする	いいえ	いいえ	はい
迅速なセキュリティ対応を削除	いいえ	いいえ	はい
メールプライバシー保護を許可	いいえ	いいえ	はい
NFC	いいえ	いいえ	はい
App Clipを許可	いいえ	いいえ	はい
ゲン文字	いいえ	いいえ	はい
イメージプレイグラウンド	いいえ	いいえ	はい
イメージワンド	いいえ	いいえ	はい
iPhoneミラーリング	いいえ	いいえ	はい
パーソナライズされた手書きの結果	いいえ	いいえ	はい
手書きツール	いいえ	いいえ	はい
通話録音	いいえ	いいえ	はい
非表示にするアプリ	いいえ	いいえ	はい
ロックするアプリ	いいえ	いいえ	はい
メールサマリー	いいえ	いいえ	はい
RCSメッセージング	いいえ	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
外部インテリジェンス統合を許可	いいえ	いいえ	はい
外部インテリジェンス統合へのサインインを許可	いいえ	いいえ	はい
メールスマートリプライを許可	いいえ	いいえ	はい
メモの文字起こしを許可	いいえ	いいえ	はい
Safariの要約を許可	いいえ	いいえ	はい
ビジュアルインテリジェンスの要約を許可	いいえ	いいえ	はい
メモの文字起こし要約を許可	いいえ	いいえ	はい
Apple Intelligenceレポートを許可	いいえ	いいえ	はい
デフォルトの通話アプリの変更を許可	いいえ	いいえ	はい
デフォルトのメッセージングアプリの変更を許可	いいえ	いいえ	はい
外部インテリジェンスワークスペースIDを許可	いいえ	いいえ	はい
デフォルトブラウザの変更	いいえ	いいえ	はい
ライブ留守番電話を許可	いいえ	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	ユーザー登録	非監視	監視
セキュリティ - ロック画面に表示			
コントロールセンター	はい	はい	はい
通知	はい	はい	はい
今日の表示	はい	はい	はい
メディアコンテンツ - 許可			
露骨な音楽、ポッドキャスト、iTunes Uコンテンツ	いいえ	いいえ	はい
iBooks内の露骨な性的コンテンツ	いいえ	はい	はい
レーティング地域	いいえ	はい	はい
映画	いいえ	はい	はい
テレビ番組	いいえ	はい	はい
アプリ	いいえ	はい	はい

- **ハードウェア制御を許可**
  - **カメラ:** ユーザーがデバイスでカメラを使用することを許可します。
    - **FaceTime:** ユーザーがデバイスでFaceTimeを使用することを許可します。監視対象のiOSデバイスの場合。
    - **FaceTimeリモートコントロールを許可:** リモートFaceTimeセッションがデバイスの制御を要求することを許可します。監視対象のiOSデバイスの場合。iOS 18.4以降で利用可能です。
  - **スクリーンキャプチャ:** ユーザーがデバイスでスクリーンショットを撮ることを許可します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **Classroomアプリが学生の画面をリモートで監視することを許可:** この制限が選択されていない場合、インストラクターはClassroomアプリを使用して学生の画面をリモートで監視できません。デフォルト設定は選択されており、インストラクターはClassroomアプリを使用して学生の画面を監視できます。**ClassroomアプリがプロンプトなしでAirPlayと画面表示を実行することを許可**の設定は、学生がインストラクターに許可を与えるためのプロンプトを受け取るかどうかを決定します。監視対象のiOSデバイスの場合。
    - **ClassroomアプリがプロンプトなしでAirPlayと画面表示を実行することを許可:** この制限が選択されている場合、インストラクターは許可を求めるプロンプトなしで、学生のデバイスでAirPlayと画面表示を実行できます。デフォルト設定は選択されていません。監視対象のiOSデバイスの場合。

- **フォトストリーム:** ユーザーがMyPhotoStreamを使用して、iCloud経由で写真をすべてのiOSデバイスに共有することを許可します。
- **共有フォトストリーム:** ユーザーがiCloud写真共有を使用して、同僚、友人、家族と写真を共有することを許可します。
- **共有iPadの一時セッションを許可:** 共有iPadの一時セッションへのアクセスを防止します。
- **音声ダイヤル:** ユーザーデバイスでの音声ダイヤルを有効にします。
- **Siri:** ユーザーがSiriを使用することを許可します。
    - **デバイスロック中に許可:** ユーザーがデバイスロック中にSiriを使用することを許可します。
    - **Siri不適切表現フィルター:** Siri不適切表現フィルターを有効にします。デフォルトではこの機能は制限されており、不適切表現のフィルタリングは行われません。

      Siriとセキュリティの詳細については、Siriと音声入力ポリシーを参照してください。
- **アプリのインストール:** ユーザーがアプリをインストールできるようにします。監視対象のiOSデバイスの場合。
- **代替アプリマーケットプレイス:** Webからの代替マーケットプレイスアプリのインストールを防止し、インストール済みの代替マーケットプレイスアプリがアプリをインストールするのを防止します。この機能はiOS 17.4以降のバージョンで利用可能です。デフォルトは**オン**です。監視対象のiOSデバイスの場合。
- **Web配布アプリ:** 顧客管理者がiOSデバイス上のWeb配布されたサードパーティアプリをブロックできるようにします。これはiOSバージョン17.5以降に適用されます。詳細については、制限を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ローミング中のグローバルバックグラウンドフェッチを許可:** デバイスがローミング中に、メールアカウントをiCloudに自動的に同期できるようにします。**オフ**の場合、iOSフォンがローミング中のグローバルバックグラウンドフェッチアクティビティを無効にします。デフォルトは**オン**です。

- **アプリを許可**
  - **iTunes Store:** ユーザーがiTunes Storeにアクセスできるようにします。監視対象のiOSデバイスの場合。
  - **アプリ内課金:** ユーザーがアプリ内課金を行えるようにします。
    - **購入にiTunes Storeのパスワードを要求:** アプリ内課金にパスワードを要求します。デフォルトではこの機能は制限されており、アプリ内課金にパスワードは不要です。
  - **Safari:** ユーザーがSafariにアクセスできるようにします。監視対象のiOSデバイスの場合。
    - **自動入力:** ユーザーがSafariでユーザー名とパスワードの自動入力を設定できるようにします。
    - **詐欺警告を強制:** この設定が有効で、ユーザーがフィッシングの疑いのあるWebサイトにアクセスした場合、Safariはユーザーに警告します。デフォルトではこの機能は制限されており、警告は発行されません。
    - **JavaScriptを有効にする:** SafariでJavaScriptを実行できるようにします。
    - **ポップアップをブロック:** Webサイトの閲覧中にポップアップをブロックします。デフォルトではこの機能は制限されており、ポップアップはブロックされません。
  - **Cookieを許可:** Cookieがどの程度許可されるかを設定します。リストから、Cookieを許可または制限するオプションを選択します。デフォルトオプションは**常に**で、すべてのWebサイトがSafariにCookieを保存することを許可します。その他のオプションは、**現在のWebサイトのみ**、**しない**、**訪問済みのサイトからのみ**です。

- **ネットワーク - iCloudアクションを許可**
  - **iCloud書類とデータ:** ユーザーが書類とデータをiCloudに同期できるようにします。監視対象のiOSデバイスの場合。
  - **iCloudバックアップ:** ユーザーがデバイスをiCloudにバックアップできるようにします。
  - **iCloudキーチェーン:** ユーザーがパスワード、Wi-Fiネットワーク、クレジットカード、その他の情報をiCloudキーチェーンに保存できるようにします。
  - **クラウド写真ライブラリ:** ユーザーがiCloud写真ライブラリにアクセスできるようにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **セキュリティ - 強制**

  デフォルトでは、以下の機能が制限されます。これは、セキュリティ機能が有効になっていないことを意味します。

  - **暗号化されたバックアップ:** iCloudへのバックアップを暗号化するように強制します。
  - **広告追跡の制限:** ターゲット広告の追跡をブロックします。
  - **初回AirPlayペアリング時のパスコード:** AirPlay対応デバイスがAirPlayを使用する前に、1回限りの画面上のコードで認証されるように要求します。
  - **手首検出を使用するペアリングされたApple Watch:** ペアリングされたApple Watchが**手首検出**を使用するように要求します。
  - **AirDropを使用した管理対象ドキュメントの共有:** このオプションを**オン**に設定すると、AirDropが管理対象外のドロップターゲットとして表示されます。

- **セキュリティ - 許可**

  - **信頼できないSSL証明書の受け入れ:** ユーザーがWebサイトの信頼できないSSL証明書を受け入れることを許可します。
  - **証明書信頼設定の自動更新:** 信頼された証明書が自動的に更新されることを許可します。
  - **管理対象ペーストボードの要求:** コピー＆ペースト機能が、**管理対象外アプリ内の管理対象アプリからのドキュメント**および**管理対象アプリ内の管理対象外アプリからのドキュメント**に適用するのと同じ制限に従うことを許可します。 たとえば、次のように構成します。

    - **管理対象ペーストボードを要求:** オン
    - **管理対象アプリから非管理対象アプリへのドキュメント:** オフ
    - **非管理対象アプリから管理対象アプリへのドキュメント:** オン ポリシーをiOSデバイスに展開すると、ユーザーは管理対象アプリから非管理対象アプリにデータをコピー＆ペーストできなくなりますが、非管理対象アプリから管理対象アプリにデータをコピー＆ペーストすることはできます。

  - **管理対象アプリから非管理対象アプリへのドキュメント:** ユーザーが管理対象（企業）アプリから非管理対象（個人）アプリにデータを移動することを許可します。
  - **非管理対象アプリから管理対象アプリへのドキュメント:** ユーザーが非管理対象（個人）アプリから管理対象（企業）アプリにデータを移動することを許可します。
  - **Appleへの診断データ送信:** ユーザーのデバイスに関する匿名の診断データをAppleに送信することを許可します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Touch IDまたはFace IDによるデバイスのロック解除:** ユーザーがTouch IDまたはFace IDを使用してデバイスのロックを解除することを許可します。
- **自動ロック解除: オフ**の場合、ユーザーはApple Watchを使用してペアリングされたiPhoneのロックを解除できません。デフォルトは**オン**です。iOS 14.5以降で利用可能です。
- **ロック時のWallet通知:** ロック画面にWallet通知が表示されることを許可します。
- **Handoff:** ユーザーが1つのiOSデバイスから近くの別のiOSデバイスにアクティビティを転送することを許可します。
- **管理対象アプリのiCloud同期:** ユーザーが管理対象アプリをiCloudに同期することを許可します。
- **エンタープライズブックのバックアップ:** エンタープライズブックをiCloudにバックアップすることを許可します。
- **エンタープライズブックのメモとハイライトの同期:** ユーザーがエンタープライズブックに追加したメモとハイライトをiCloudに同期することを許可します。
- **エンタープライズアプリの信頼:** エンタープライズアプリケーションを信頼することを許可します。エンタープライズアプリとは、組織向けにカスタム作成されたアプリのことです。これらのアプリは社内で作成することも、外部ベンダーによって開発および購入することもできます。詳細については、「iOSにカスタムエンタープライズアプリをインストールする」を参照してください。
- **Spotlightでのインターネット検索結果:** Spotlightがデバイスに加えてインターネットからの検索結果を表示することを許可します。
- **管理対象外アプリによる管理対象連絡先の読み取り:** オプション。**管理対象アプリのドキュメントを管理対象外アプリで利用**が無効になっている場合にのみ利用可能です。このポリシーが有効な場合、管理対象外アプリは管理対象アカウントの連絡先からデータを読み取ることができます。デフォルトは**オフ**です。iOS 12以降で利用可能です。
- **管理対象アプリによる管理対象外連絡先への書き込み:** オプション。有効にすると、管理対象アプリが管理対象外アカウントの連絡先に連絡先を書き込むことができます。**管理対象アプリのドキュメントを管理対象外アプリで利用**が有効になっている場合、この制限は無効になります。デフォルトは**オフ**です。iOS 12以降で利用可能です。
- **Appleパーソナライズド広告を許可: オフ**の場合、Apple広告プラットフォームはユーザーのデータを使用してパーソナライズされた広告を配信できません。デフォルトは**オン**です。iOS 14.0以降で利用可能です。

- **監視対象デバイスのみの設定 - 許可**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

これらの設定は、監視対象デバイスにのみ適用されます。iOSデバイスを監視モードに設定する手順については、「Apple Configurator 2を使用してデバイスを展開する」を参照してください。

- **eSIMの変更を許可:** ユーザーがデバイスのeSIM設定を変更できるようにします。
- **消去時にeSIMを保持: オン**の場合、パスワードの試行回数超過または**設定 > 一般 > リセット**の「すべてのコンテンツと設定を消去」オプションによりデバイスが消去されたときに、システムはeSIMを保持します。デフォルトは**オフ**です。

> **注：**
>
> **探す**がデバイスの消去を開始した場合、システムはeSIMを保持しません。

- **すべてのコンテンツと設定を消去:** ユーザーがデバイスからすべてのコンテンツと設定を消去できるようにします。
- **スクリーンタイム:** ユーザーがスクリーンタイムを有効にできるようにします。
- **ポッドキャスト:** ユーザーがポッドキャストをダウンロードおよび同期できるようにします。
- **構成プロファイルのインストール:** ユーザーが、展開した以外の構成プロファイルをインストールできるようにします。
- **Touch IDおよびFace IDの変更:** ユーザーがTouch IDまたはFace IDを変更または削除できるようにします。
- **デバイスからのアプリのインストール:** ユーザーがアプリをインストールできるようにします。この設定を無効にすると、エンドユーザーは新しいアプリをインストールできなくなります。App Storeは無効になり、そのアイコンはホーム画面から削除されます。
- **キーボードショートカット:** ユーザーが頻繁に使用する単語やフレーズのカスタムキーボードショートカットを作成できるようにします。
- **ペアリングされたApple Watch:** ユーザーが監視対象デバイスにApple Watchをペアリングできるようにします。
- **パスコードの変更:** ユーザーが監視対象デバイスのパスコードを変更できるようにします。
- **デバイス名の変更:** ユーザーがデバイスの名前を変更できるようにします。
- **壁紙の変更:** ユーザーがデバイスの壁紙を変更できるようにします。
- **アプリの自動ダウンロード:** アプリをダウンロードできるようにします。
- **AirDrop:** ユーザーが近くのiOSデバイスと写真、ビデオ、ウェブサイト、位置情報などを共有できるようにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **iMessage:** ユーザーがiMessageでWi-Fi経由でテキストメッセージを送信できるようにします。
- **Siriのユーザー生成コンテンツ:** SiriがWebからユーザー生成コンテンツを照会できるようにします。従来のジャーナリストではなく、消費者がユーザー生成コンテンツを作成します。たとえば、TwitterやFacebookで見つかるコンテンツはユーザー生成コンテンツです。
- **iBooks:** ユーザーがiBooksアプリを使用できるようにします。
- **アプリの削除:** ユーザーがデバイスからアプリを削除できるようにします。
- **Game Center:** ユーザーがデバイスでGame Centerを介してオンラインゲームをプレイできるようにします。
  - **友達の追加:** ユーザーが友達にゲームをプレイするための通知を送信できるようにします。
  - **マルチプレイヤーゲーム:** ユーザーがデバイスでマルチプレイヤーゲームを開始できるようにします。
- **アカウント設定の変更:** ユーザーがデバイスのアカウント設定を変更できるようにします。
- **アプリのモバイルデータ設定の変更:** ユーザーがアプリのモバイルデータ使用方法を変更できるようにします。
- **ネットワークドライブ接続を許可:** ファイルアプリでのネットワークドライブへの接続を禁止します。
- **USBデバイス接続を許可:** ファイルアプリで接続されているUSBデバイスへの接続を禁止します。
- **デバイスを探すを許可:** 「探す」アプリの**デバイスを探す**オプションを無効にします。
- **友達を探す設定を許可:** 「探す」アプリの**友達を探す**オプションを無効にします。
- **友達を探す設定の変更:** ユーザーが友達を探す設定を変更できるようにします。
- **Configurator以外のホストとのペアリング:** 管理者がユーザーデバイスをどのデバイスとペアリングできるかを制御できるようにします。この設定を無効にすると、Apple Configuratorを実行している監視ホストとのペアリングを除き、ペアリングが禁止されます。監視ホスト証明書が構成されていない場合、すべてのペアリングが無効になります。
- **予測キーボード:** ユーザーデバイスが入力時に単語を提案するために予測キーボードを使用できるようにします。ユーザーに提案された単語へのアクセスを許可したくない標準テストの実施などの状況では、このオプションを無効にしてください。
- **キーボードの自動修正:** ユーザーデバイスがキーボードの自動修正を使用できるようにします。ユーザーに自動修正へのアクセスを許可したくない標準テストの実施などの状況では、このオプションを無効にしてください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **キーボードのスペルチェック:** ユーザーデバイスが入力中にスペルチェックを使用できるようにします。ユーザーにスペルチェッカーへのアクセスを許可したくない標準テストの実施などの状況では、このオプションを無効にしてください。
- **定義の検索:** ユーザーデバイスが入力中に定義の検索を使用できるようにします。ユーザーが入力中に定義を検索することを望まない標準テストの実施などの状況では、このオプションを無効にしてください。
- **シングルアプリバンドルID:** デバイスの制御を維持し、他のアプリや機能とのやり取りを防止できるアプリのリストを作成します。 アプリを追加するには、**追加**をクリックし、**アプリ名**を入力して、**保存**をクリックします。追加したいアプリごとにこのプロセスを繰り返します。
- **ニュース:** ユーザーがニュースアプリを使用できるようにします。
- **Apple Musicサービス:** ユーザーがApple Musicサービスを使用できるようにします。Apple Musicサービスを許可しない場合、ミュージックアプリはクラシックモードで実行されます。デフォルトは**オン**です。iOS 9.3以降で利用可能です。
- **Apple Music Radio:** ユーザーがApple Music Radioを使用できるようにします。デフォルトは**オン**です。iOS 9.3以降で利用可能です。
- **通知の変更:** ユーザーが通知設定を変更できるようにする。
- **アプリの使用制限:** ユーザーがすべてのアプリを使用できるようにするか、指定したバンドルIDに基づいてアプリを使用または使用しないようにするかを許可します。監視対象デバイスにのみ適用されます。**一部のアプリのみを許可**を選択した場合、Webクリップを許可するには、バンドルID `com.apple.webapp` のアプリを追加します。

  注:

  iOS 11以降、Appleはアプリの制限に利用できるポリシーに変更を加えました。Appleは、適切なiOSアプリケーションバンドルを制限することによって、設定アプリと電話アプリへのアクセスを削除することを許可しなくなりました。

  一部のアプリをブロックするように制限デバイスポリシーを構成し、そのポリシーを展開した後: 後でそれらのアプリの一部またはすべてを許可したい場合でも、制限デバイスポリシーを変更して展開しても、制限は変更されません。この場合、iOSは変更をiOSプロファイルに適用しません。続行するには、プロファイル削除ポリシーを使用してiOSプロファイルを削除し、更新された制限デバイスポリシーを展開します。

  この設定を**一部のアプリのみを許可**に変更した場合: このポリシーを展開する前に、Apple Deployment Programを使用して登録されたデバイスのユーザーに、セットアップアシスタ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ントからAppleアカウントにサインインするようアドバイスしてください。そうしないと、ユーザーはAppleアカウントにサインインして許可されたアプリにアクセスするために、デバイスで2要素認証を無効にする必要がある場合があります。

- **診断送信の変更:** ユーザーが**設定 > 診断と使用状況**ペインで診断送信とアプリ分析の設定を変更できるようにする。
- **Bluetoothの変更:** ユーザーがBluetooth設定を変更できるようにする。
- **音声入力の許可:** 監視対象のみ。この制限が**オフ**に設定されている場合、音声入力（音声テキスト変換を含む）は許可されません。デフォルト設定は**オン**です。
- **Wi-Fiのオン/オフの変更:** 設定またはコントロールセンターでWi-Fiをオンまたはオフにすることを防ぎます。機内モードにしても効果はありません。この制限は、使用するWi-Fiネットワークを選択することを妨げません。
- **ネットワークポリシーによってインストールされたWi-Fiネットワークのみに参加:** オプション。監視対象のみ。この制限が**オン**に設定されている場合、デバイスは構成プロファイルを通じて設定されたWi-Fiネットワークにのみ参加できます。デフォルト設定は**オフ**です。
- **ClassroomアプリがプロンプトなしでAirPlayと画面表示を実行することを許可:** この制限が選択されている場合、インストラクターは許可を求めるプロンプトなしで、学生のデバイスでAirPlayと画面表示を実行できます。デフォルト設定は選択されていません。監視対象のiOSデバイス向け。
- **Classroomアプリがプロンプトなしでアプリにロックし、デバイスをロックすることを許可:** この制限が**オン**に設定されている場合、Classroomアプリはユーザーにプロンプトを表示することなく、ユーザーデバイスをアプリに自動的にロックし、デバイスをロックします。デフォルト設定は**オフ**です。iOS 11（最小バージョン）を実行している監視対象デバイス向け。
- **Classroomアプリのクラスにプロンプトなしで自動的に参加:** この制限が**オン**に設定されている場合、Classroomアプリはユーザーにプロンプトを表示することなく、ユーザーをクラスに自動的に参加させます。デフォルト設定は**オフ**です。iOS 11（最小バージョン）を実行している監視対象デバイス向け。
- **AirPrintを許可:** この制限が**オフ**に設定されている場合、ユーザーはAirPrintで印刷できません。デフォルト設定は**オン**です。この制限が**オン**の場合、これらの追加制限が表示されます。iOS 11（最小バージョン）を実行している監視対象デバイス向け。
  - **AirPrint資格情報をキーチェーンに保存することを許可する:** この制限が選択されていない場合、AirPrintのユーザー名とパスワードはキーチェーンに保存されません。デ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

フォルト設定は選択されています。iOS 11（最小バージョン）を実行している監視対象デバイス向け。

- **iBeaconを使用してAirPrintプリンターの検出を許可する:** この制限が選択されていない場合、iBeaconによるAirPrintプリンターの検出は無効になります。この設定により、偽のAirPrint Bluetoothビーコンがネットワークトラフィックをフィッシングするのを防ぎます。デフォルト設定は選択されています。iOS 11（最小バージョン）を実行している監視対象デバイス向け。
- **信頼された証明書を持つ宛先へのAirPrintのみを許可する:** この制限が選択されている場合、ユーザーは信頼された証明書を持つ宛先にのみAirPrintを使用して印刷できます。デフォルト設定は選択されていません。iOS 11（最小バージョン）を実行している監視対象デバイス向け。

- **VPN構成の追加:** この制限が**オフ**に設定されている場合、ユーザーはVPN構成を作成できません。デフォルト設定は**オン**です。iOS 11（最小バージョン）を実行している監視対象デバイス向け。
- **モバイルデータ通信プラン設定の変更:** この制限が**オフ**に設定されている場合、ユーザーはモバイルデータ通信プラン設定を変更できません。デフォルト設定は**オン**です。iOS 11（最小バージョン）を実行している監視対象デバイス向け。
- **システムアプリの削除:** この制限が**オフ**に設定されている場合、ユーザーはデバイスからシステムアプリを削除できません。デフォルト設定は**オン**です。iOS 11（最小バージョン）を実行している監視対象デバイス向け。
- **近くの新しいデバイスのセットアップ:** この制限がオフに設定されている場合、ユーザーは近くの新しいデバイスをセットアップできません。デフォルト設定はオンです。iOS 11（最小バージョン）を実行している監視対象デバイス向け。
- **USB制限モードを許可する: オフ**の場合、デバイスはロックされている間も常にUSBアクセサリに接続できます。デフォルトは**オン**です。監視対象のiOS 11.3以降のデバイスでのみ利用可能です。
- **ソフトウェアアップデートの遅延を強制する: オン**の場合、ユーザーへのソフトウェアアップデートの表示を遅らせます。この制限が適用されている場合、ユーザーはソフトウェアアップデートのリリース日から指定された日数が経過するまでソフトウェアアップデートを確認できません。デフォルトは**オフ**です。監視対象のiOS 11.3以降のデバイスでのみ利用可能です。OSアップデートポリシーには、デバイスがアップデートを受信する頻度を制御するための詳細な設定があります。(/ja-jp/citrix-endpoint-management/policies/control-os-updates.html)を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **強制的なソフトウェアアップデート遅延（日数）:** デバイスでのソフトウェアアップデートを遅延させる日数を指定できます。最大遅延日数は**90**日です。デフォルトは**30**日です。監視対象のiOS 11.3以降のデバイスでのみ利用可能です。
- **クラスを離れるためのClassroomリクエスト許可を強制する: オン**の場合、Classroomで管理されていないコースに登録している生徒は、コースを離れようとするときに教師に許可を求める必要があります。デフォルトは**オフ**です。監視対象のiOS 11.3以降のデバイスでのみ利用可能です。
- **自動入力の前に認証を強制する:** 自動入力機能を使用する前に、ユーザーに認証を強制します。
- **日付と時刻の自動設定を強制する:** 監視対象デバイスで日付と時刻を自動的に設定できるようにします。**オン**の場合、デバイスユーザーは**一般 > 日付と時刻**の下にある**自動設定**をオフにできません。デバイスのタイムゾーンは、デバイスがその位置を特定できる場合にのみ更新されます。つまり、デバイスがモバイルデータ通信接続を持っているか、位置情報サービスが有効なWi-Fi接続を持っている場合です。デフォルトは**オフ**です。監視対象のiOS 12以降のデバイスでのみ利用可能です。
- **パスワードの自動入力:** オプション。無効にすると、ユーザーはパスワードの自動入力または強力なパスワードの自動生成機能を使用できません。デフォルトは**オン**です。iOS 12以降で利用可能です。
- **パスワードの近接リクエスト:** オプション。無効にすると、ユーザーのデバイスは近くのデバイスからパスワードをリクエストしません。デフォルトは**オン**です。iOS 12以降で利用可能です。
- **パスワード共有:** オプション。無効にすると、ユーザーはAirDropパスワード機能を使用してパスワードを共有できません。デフォルトは**オン**です。iOS 12以降で利用可能です。
- **パーソナルホットスポットの変更を許可:** ユーザーがパーソナルホットスポットの設定を変更するのを防ぎます。
- **ペアリングされていないデバイスによるリカバリへの起動を許可: オン**の場合、ペアリングされていないデバイスによるリカバリへのデバイスの起動を許可します。デフォルトは**オフ**です。iOS 14.5以降で利用可能です。
- **緊急セキュリティ対応のインストール: オフ**の場合、緊急セキュリティ対応のインストールを禁止します。デフォルトは**オン**です。
- **緊急セキュリティ対応の削除: オフ**の場合、緊急セキュリティ対応の削除を禁止します。デフォルトは**オン**です。
- **メールプライバシー保護を許可: オフ**の場合、デバイス上のメールプライバシー保護を無効にします。デフォルトは**オン**です。iOS 15.2以降で利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **NFC: オフ**の場合、NFCを無効にします。デフォルトは**オン**です。iOS 14.2以降で利用可能です。
- **App Clipを許可**: **オフ**の場合、ユーザーがApp Clipを追加するのを防ぎ、デバイス上の既存のApp Clipをすべて削除します。デフォルトは**オン**です。iOS 14.0以降で利用可能です。
- **Genmoji: オフ**の場合、新しいGenmojiの作成を禁止します。デフォルトは**オン**です。iOS 18以降で利用可能です。
- **Image Playground: オフ**の場合、画像生成の使用を禁止します。デフォルトは**オン**です。iOS 18以降で利用可能です。
- **Image Wand: オフ**の場合、Image Wandの使用を禁止します。デフォルトは**オン**です。iOS 18以降で利用可能です。
- **iPhoneミラーリング: オフ**の場合、iPhoneミラーリングの使用を禁止し、iPhoneがMacにミラーリングするのを防ぎます。デフォルトは**オン**です。iOS 18以降で利用可能です。
- **パーソナライズされた手書き結果: オフ**の場合、システムがユーザーの手書きでテキストを生成するのを防ぎます。デフォルトは**オン**です。iOS 18以降で利用可能です。
- **ライティングツール: オフ**の場合、Apple Intelligenceライティングツールを無効にします。デフォルトは**オン**です。iOS 18以降で利用可能です。
- **通話録音: オフ**の場合、通話録音を無効にします。デフォルトは**オン**です。iOS 18以降で利用可能です。
- **非表示にするアプリ: オフ**の場合、ユーザーがアプリを非表示にすることを禁止します。ホーム画面からアプリを削除しながら、Appライブラリにアプリを残す機能には影響しません。デフォルトは**オン**です。iOS 18以降で利用可能です。
- **ロックするアプリ: オフ**の場合、ユーザーがアプリをロックする機能を無効にします。アプリを非表示にするにはロックが必要なため、ロックを無効にすると非表示も無効になります。デフォルトは**オン**です。iOS 18以降で利用可能です。
- **メールの要約: オフ**の場合、メールメッセージの要約を手動で作成する機能を無効にします。これは自動要約生成には影響しません。デフォルトは**オン**です。iOS 18.1以降で利用可能です。
- **RCSメッセージング: オフ**の場合、RCSメッセージングの使用を禁止します。デフォルトは**オン**です。iOS 18.1以降で利用可能です。
- **外部インテリジェンス統合を許可: オフ**の場合、Siriで外部のクラウドベースのインテリジェンスサービスを使用することを無効にします。デフォルトは**オン**です。iOS 18.2以降で利用可能です。
- **外部インテリジェンス統合へのサインインを許可: オフ**の場合、外部インテリジェンスプロバイダーを匿名モードに強制します。ユーザーがすでに外部インテリジェンスプロバイ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ダーにサインインしている場合、この制限を適用すると、次回の要求が試行されたときにサインアウトされます。デフォルトは**オン**です。iOS 18.2以降で利用可能です。

- **メールのスマートリプライを許可: オフ**の場合、メールでのスマートリプライを無効にします。デフォルトは**オン**です。iOS 18.2以降で利用可能です。
- **メモの文字起こしを許可: オフ**の場合、メモでの文字起こしを無効にします。デフォルトは**オン**です。iOS 18.2以降で利用可能です。
- **Safariの要約を許可: オフ**の場合、システムはSafariでコンテンツを要約する機能を無効にします。デフォルトは**オン**です。iOS 18.4以降で利用可能です。
- **ビジュアルインテリジェンスの要約を許可: オフ**の場合、システムはビジュアルインテリジェンスの要約を無効にします。デフォルトは**オン**です。iOS 18.3以降で利用可能です。
- **メモの文字起こし要約を許可: オフ**の場合、メモでの文字起こし要約を無効にします。デフォルトは**オン**です。iOS 18.3以降で利用可能です。
- **Apple Intelligenceレポートを許可: オフ**の場合、システムはApple Intelligenceレポートを無効にします。デフォルトは**オン**です。iOS 18.4以降で利用可能です。
- **デフォルトの通話アプリの変更を許可: オフ**の場合、デフォルトの通話アプリ設定の変更を無効にします。この設定が適用されている場合でも、デフォルトの通話アプリ設定を設定するMDM設定コマンドは引き続き機能します。デフォルトは**オン**です。iOS 18.4以降で利用可能です。
- **デフォルトのメッセージングアプリの変更を許可: オフ**の場合、デフォルトのメッセージングアプリ設定の変更を無効にします。この設定が適用されている場合でも、デフォルトのメッセージングアプリ設定を設定するMDM設定コマンドは引き続き機能します。デフォルトは**オン**です。iOS 18.4以降で利用可能です。
- **外部インテリジェンスワークスペースIDを許可:** 文字列の配列ですが、現在は単一の要素に制限されています。存在する場合、Apple Intelligenceは指定された外部統合ワークスペースIDのみを使用することを許可し、リクエストを行うにはサインインが必要です。ユーザーはサインインをサポートする統合にサインインする必要があります。複数のペイロードは交差演算を使用して結合されます。これは、複数のペイロードで競合する値が指定された場合、許可されるワークスペースIDのセットが空になる可能性があることを意味します。iOS 18.3以降で利用可能です。

  - **外部インテリジェンスワークスペースID:** 外部インテリジェンスワークスペースIDを追加するには、**追加**をクリックし、**外部インテリジェンスワークスペースID**を入力して、**保存**をクリックします。追加したいワークスペースIDごとにこのプロセスを繰り返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

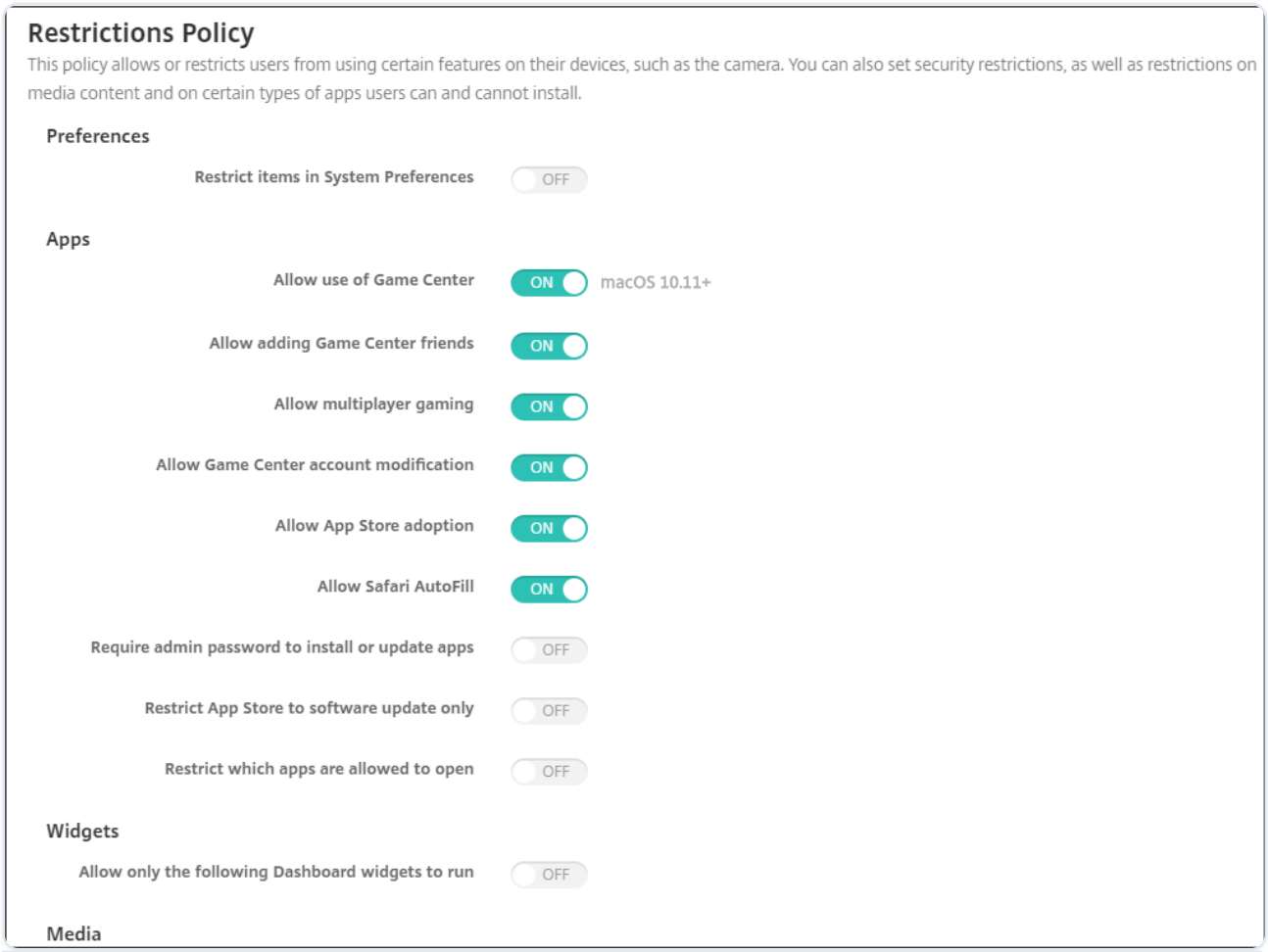
- **デフォルトブラウザの変更: オフ**の場合、デフォルトブラウザ設定の変更を無効にします。これが適用されても、デフォルトブラウザ設定を設定するMDM設定コマンドは引き続き機能します。デフォルトは**オン**です。iOS 18.2以降で利用可能です。
- **ライブボイスメールを許可: オフ**の場合、システムはデバイス上のライブボイスメールを無効にします。デフォルトは**オン**です。iOS 17.2以降で利用可能です。

- **セキュリティ - ロック画面に表示**
  - **コントロールセンター:** ロック画面でのコントロールセンターへのアクセスを許可します。コントロールセンターを使用すると、ユーザーは機内モード、Wi-Fi、Bluetooth、おやすみモード、画面回転ロックの設定を簡単に変更できます。
  - **通知:** ロック画面での通知を許可します。
  - **今日の表示:** 天気やその日のカレンダー項目などの情報を集約する「今日の表示」をロック画面で許可します。
- **メディアコンテンツ - 許可**
  - **露骨な表現を含む音楽、ポッドキャスト、iTunes Uコンテンツ:** ユーザーのデバイスで露骨な表現を含むコンテンツを許可します。
  - **iBooksの露骨な性的コンテンツ:** iBooksから露骨な表現を含むコンテンツをダウンロードすることを許可します。
  - **レーティング地域:** 保護者による制限のレーティングが取得される地域を設定します。リストから国をクリックしてレーティング地域を設定します。デフォルトは**米国**です。
  - **映画:** ユーザーのデバイスで映画を許可するかどうかを設定します。映画が許可されている場合、オプションで映画のレーティングレベルを設定します。リストからオプションをクリックして、デバイスでの映画を許可または制限します。デフォルトは「すべての映画を許可」です。
  - **テレビ番組:** ユーザーのデバイスでテレビ番組を許可するかどうかを設定します。テレビ番組が許可されている場合、オプションでテレビ番組のレーティングレベルを設定します。リストからオプションをクリックして、デバイスでのテレビ番組を許可または制限します。デフォルトは「すべてのテレビ番組を許可」です。
  - **アプリ:** ユーザーのデバイスでアプリを許可するかどうかを設定します。アプリが許可されている場合、オプションでアプリのレーティングレベルを設定します。リストからオプションをクリックして、デバイスでのアプリを許可または制限します。デフォルトは「すべてのアプリを許可」です。
- **ポリシー設定**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
  - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
  - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を入力します。iOS 6.0以降でのみ利用可能です。
- **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはiOS 9.3以降でのみ利用可能です。

macOS設定



設定	非監視	監視
アプリ		
Game Centerの使用を許可する	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	非監視	監視
Game Centerの友達追加を許可する	いいえ	はい
マルチプレイヤーゲームを許可する	いいえ	はい
Game Centerアカウントの変更を許可する	はい	はい
App Storeの利用を許可する	はい	はい
Safariの自動入力を許可する	いいえ	はい
アプリのインストールまたは更新に管理者パスワードを要求する	はい	はい
App Storeをソフトウェアアップデートのみに制限する	はい	はい
開くことを許可するアプリを制限する	はい	はい
メディア		
AirDropを許可する	いいえ	はい
機能		
デスクトップピクチャをロックする	いいえ	はい
カメラの使用を許可	いいえ	はい
Apple Musicを許可	いいえ	はい
Spotlightの提案を許可	はい	はい
調べる機能を許可	はい	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	非監視	監視
ローカルアカウントでのiCloudパスワードの使用を許可	はい	はい
iCloud書類とデータを許可	はい	はい
iCloudデスクトップと書類を許可	いいえ	はい
iCloudキーチェーンの同期を許可	いいえ	はい
iCloudメールを許可	はい	はい
iCloud連絡先を許可	はい	はい
iCloudカレンダーを許可	はい	はい
iCloudリマインダーを許可	はい	はい
iCloudブックマークを許可	はい	はい
iCloudメモを許可	はい	はい
iCloud写真を許可	はい	はい
自動ロック解除を許可	はい	はい
Touch IDによるMacのロック解除を許可	はい	はい
ソフトウェアアップデートの遅延を強制	いいえ	はい
パスワードの自動入力	いいえ	はい
パスワードの近接要求	いいえ	はい
パスワード共有	はい	はい
イメージプレイグラウンド	いいえ	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	非監視	監視
iPhoneミラーリング	いいえ	はい
書き込みツール	いいえ	はい
メディア共有の変更を許可	はい	はい

- **環境設定**
  - **システム環境設定の項目を制限:** ユーザーのシステム環境設定へのアクセスを許可または制限します。デフォルトは**オフ**で、ユーザーはシステム環境設定に完全にアクセスできます。有効にした場合、次の設定を構成します。
    - **システム環境設定ペイン:** 選択した設定を有効にするか無効にするかを選択します。デフォルトではすべての設定が有効になっており、既定で**オン**になっています。
      - ユーザーとグループ
      - 一般
      - アクセシビリティ
      - App Store (アップストア)
      - ソフトウェアアップデート
      - ブルートゥース
      - CDとDVD
      - 日付と時刻
      - デスクトップとスクリーンセーバ
      - ディスプレイ
      - ドック
      - 省エネルギー
      - 機能拡張
      - FibreChannel
      - iCloud
      - インク
      - インターネットアカウント
      - キーボード

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 言語とテキスト
    - ミッションコントロール
    - マウス
    - ネットワーク
    - 通知
    - ペアレンタルコントロール
    - プリンタとスキャナ
    - プロファイル
    - セキュリティとプライバシー
    - 共有
    - サウンド
    - 音声入力とスピーチ
    - スポットライト
    - 起動ディスク
    - タイムマシン
    - トラックパッド
    - エックスサン

- **アプリ**
    - **Game Centerの使用を許可:** ユーザーがGame Centerを介してオンラインゲームをプレイすることを許可します。デフォルトは**オン**です。
    - **Game Centerの友達追加を許可:** ユーザーが友達にゲームをプレイするための通知を送信することを許可します。デフォルトは**オン**です。
    - **マルチプレイヤーゲームを許可:** ユーザーがマルチプレイヤーゲームプレイを開始することを許可します。デフォルトは**オン**です。
    - **Game Centerアカウントの変更を許可:** ユーザーがGame Centerアカウント設定を変更することを許可します。デフォルトは**オン**です。
    - **App Storeの採用を許可:** App StoreがOS Xに既存のアプリを採用することを許可または制限します。デフォルトは**オン**です。
    - **Safariの自動入力を許可:** Safariが保存しているパスワード、アドレス、その他の基本情報でウェブサイトのフィールドを自動的に入力することを許可します。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アプリのインストールまたは更新に管理者パスワードを要求する:** アプリのインストールまたは更新に管理者パスワードを要求します。デフォルトは**オフ**で、管理者パスワードは不要です。
- **App Storeをソフトウェアアップデートのみに制限する:** App Storeをアップデートのみに制限し、App Store内の「アップデート」以外のすべてのタブを無効にします。デフォルトは**オフ**で、App Storeへのフルアクセスが許可されます。
- **起動を許可するアプリを制限する:** ユーザーが使用できるアプリを制限または許可します。デフォルトはオフで、すべてのアプリの使用が許可されます。有効にした場合、次の設定を構成します。
  - **許可されたアプリ: 追加**をクリックし、起動を許可するアプリの名前とバンドルIDを入力して、**保存**をクリックします。Citrixモバイル生産性アプリの場合、アプリを追加する際に**パッケージID**フィールドのIDを使用します。起動を許可する各アプリについて、この手順を繰り返します。
  - **許可されていないフォルダー: 追加**をクリックし、ユーザーアクセスを制限したいフォルダーのファイルパス（例: /Applications/Utilities）を入力して、**保存**をクリックします。ユーザーにアクセスさせたくないすべてのフォルダーについて、この手順を繰り返します。
  - **許可されたフォルダー: 追加**をクリックし、ユーザーアクセスを許可したいフォルダーのファイルパスを入力して、**保存**をクリックします。ユーザーにアクセスさせたいすべてのフォルダーについて、この手順を繰り返します。

- **ウィジェット**
  - **次のDashboardウィジェットのみ実行を許可する: オン**の場合、ユーザーはこの設定で構成されたDashboardウィジェットのみを実行できます。デフォルトは**オフ**で、すべてのウィジェットの実行が許可されます。有効にした場合、次の設定を構成します。
    - **許可されたウィジェット: 追加**をクリックし、実行を許可するウィジェットの名前とIDを入力して、**保存**をクリックします。Dashboardで実行したい各ウィジェットについて、この手順を繰り返します。

- **メディア**
  - **AirDropを許可する:** ユーザーが写真、ビデオ、Webサイト、位置情報などを近くのiOSデバイスと共有できるようにします。

- **共有**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **新しい共有サービスを自動的に有効にする:** 共有サービスを自動的に有効にするかどうかを選択します。
- **メール:** 共有メールボックスを許可するかどうかを選択します。
- **Facebook:** 共有Facebookアカウントを許可するかどうかを選択します。
- **ビデオサービス - Flickr、Vimeo、Tudou、Youku:** 共有ビデオサービスを許可するかどうかを選択します。
- **Apertureに追加:** Apertureに追加する共有機能を許可するかどうかを選択します。
- **Sina Weibo:** 共有Sina Weiboアカウントを許可するかどうかを選択します。
- **Twitter:** 共有Twitterアカウントを許可するかどうかを選択します。
- **メッセージ:** メッセージへの共有アクセスを許可するかどうかを選択します。
- **iPhotoに追加:** iPhotoに追加する共有機能を許可するかどうかを選択します。
- **リーディングリストに追加:** リーディングリストに追加する共有機能を許可するかどうかを選択します。
- **AirDrop:** 共有AirDropアカウントを許可するかどうかを選択します。

- **機能**
  - **デスクトップピクチャをロック:** ユーザーがデスクトップピクチャを変更できるかどうかを選択します。デフォルトは**オフ**で、ユーザーはデスクトップピクチャを変更できます。
  - **カメラの使用を許可:** ユーザーがMacでカメラを使用できるかどうかを選択します。デフォルトは**オフ**で、ユーザーはカメラを使用できません。
  - **Apple Musicを許可:** ユーザーがApple Musicサービスを使用できるようにします（macOS 10.12以降）。Apple Musicサービスを許可しない場合、ミュージックアプリはクラシックモードで実行されます。監視対象デバイスにのみ適用されます。デフォルトは**オン**です。
  - **Spotlightの提案を許可:** ユーザーがSpotlightの提案を使用してMacを検索したり、インターネットやApp StoreからSpotlightの提案を提供したりできるかどうかを選択します。デフォルトは**オフ**で、ユーザーがSpotlightの提案を使用することを禁止します。
  - **調べるを許可:** ユーザーがコンテキストメニューまたはSpotlight検索メニューで単語の定義を調べることができるかどうかを選択します。デフォルトはオフで、ユーザーがMacで調べる機能を使用することを禁止します。
  - **ローカルアカウントでのiCloudパスワードの使用を許可:** ユーザーがApple IDとiCloudパスワードを使用してMacにサインオンできるかどうかを選択します。このポリシーを有効にすると、ユーザーはMacの *すべて*のログイン画面で1つのIDとパスワードのみを使用するこ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

とになります。デフォルトは**オン**で、ユーザーがApple IDとiCloudパスワードを使用してMacにアクセスすることを許可します。

- **iCloud書類とデータを使用を許可:** ユーザーがMacでiCloudに保存されている書類やデータにアクセスすることを許可するかどうかを選択します。デフォルトは**オン**で、ユーザーがMacでiCloud書類とデータを使用することを禁止します。
  - **iCloudデスクトップと書類を許可:** (macOS 10.12.4以降) デフォルトは選択されています。
- **iCloudキーチェーン同期を許可:** iCloudキーチェーンの同期を許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloudメールを許可:** ユーザーがiCloudメールを使用することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloud連絡先を許可:** ユーザーがiCloud連絡先を使用することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloudカレンダーを許可:** ユーザーがiCloudカレンダーを使用することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloudリマインダーを許可:** ユーザーがiCloudリマインダーを使用することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloudブックマークを許可:** ユーザーがiCloudブックマークと同期することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloudメモを許可:** ユーザーがiCloudメモを使用することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloud写真を許可:** この設定を**オフ**に変更すると、iCloud写真ライブラリから完全にダウンロードされていない写真は、ローカルデバイスストレージから削除されます (macOS 10.12以降)。デフォルトは**オン**です。
- **自動ロック解除を許可:** このオプションとApple Watchの詳細については、https://www.imore.com/auto-unlockを参照してください (macOS 10.12以降)。デフォルトは**オン**です。
- **Touch IDによるMacのロック解除を許可:** (macOS 10.12.4以降)。デフォルトは**オン**です。
- **ソフトウェアアップデートの遅延を強制: オン**の場合、この設定はソフトウェアアップデートのユーザーへの表示を遅延させます。ユーザーは、ソフトウェアアップデートのリリース日から指定された日数が経過するまで、ソフトウェアアップデートを表示しません。デフォルトは**オフ**です。macOS 10.13.4以降を実行している監視対象デバイスでのみ利用可能です。OSアップデートポリシーには、デバイスがアップデートを受信する頻度を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

制御するための詳細な設定があります。OSアップデートデバイスポリシーを参照してください。

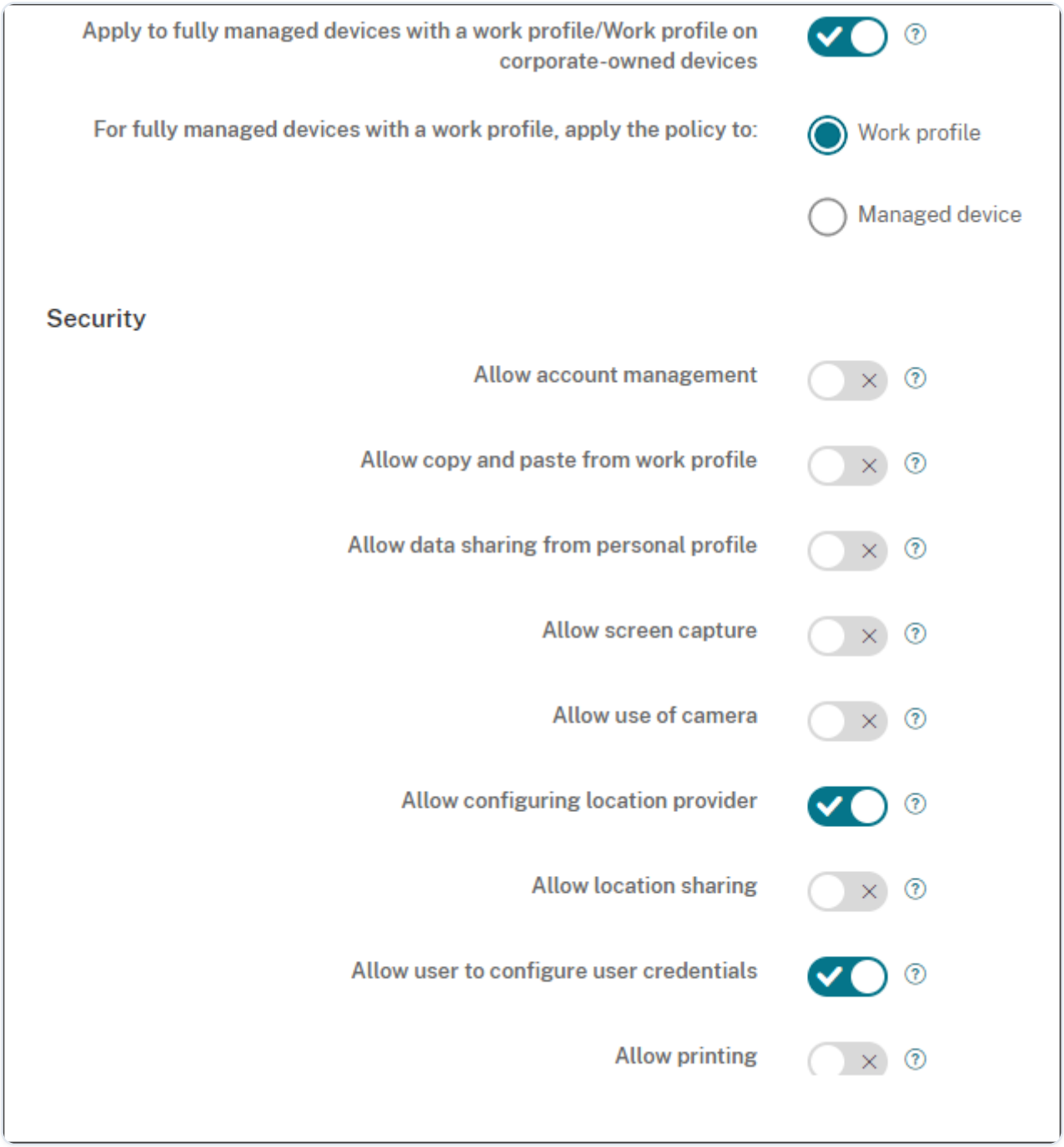
- **強制的なソフトウェアアップデート遅延 (日数):** デバイスでのソフトウェアアップデートを遅延させる日数を指定します。最大は90日です。デフォルトは**30**です。macOS 10.13.4以降を実行している監視対象デバイスでのみ利用可能です。
- **パスワードの自動入力:** オプション。無効にすると、ユーザーはパスワードの自動入力または強力なパスワードの自動生成機能を使用できません。デフォルトは**オン**です。(macOS 10.14以降)
- **パスワード近接リクエスト:** オプション。無効にすると、ユーザーのデバイスは近くのデバイスからパスワードを要求しません。デフォルトは**オン**です。(macOS 10.14以降)
- **パスワード共有:** オプション。無効にすると、ユーザーはAirDropパスワード機能を使用してパスワードを共有できません。デフォルトは**オン**です。(macOS 10.14以降)
- **Image Playground: オフ**の場合、画像生成の使用を禁止します。デフォルトは**オン**です。macOS 15以降を実行している監視対象デバイスでのみ利用可能です。
- **iPhoneミラーリング: オフ**の場合、iPhoneミラーリングの使用を禁止します。macOSで使用する場合、これによりMacがiPhoneをミラーリングするのを防ぎます。デフォルトは**オン**です。macOS 15以降を実行している監視対象デバイスでのみ利用可能です。
- **ライティングツール: オフ**の場合、Apple Intelligenceライティングツールを無効にします。デフォルトは**オン**です。macOS 15以降を実行している監視対象デバイスでのみ利用可能です。
- **メディア共有の変更を許可: オフ**の場合、メディア共有設定の変更を禁止します。デフォルトは**オン**です。macOS 15.1以降で利用可能です。

Android設定

- **カメラ:** ユーザーがデバイスのカメラを使用できるようにします。**オフ**の場合、カメラは無効になります。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アンドロイド エンタープライズ 設定



新規または工場出荷時設定にリセットされたAndroidデバイスがワークプロファイルモードで登録されると、Android 9.0～10.xを実行しているデバイスはワークプロファイルを持つ完全に管理されたデバイスとして登録されます。Android 11以降を実行しているデバイスは、企業所有デバイス上のワークプロファイルとして登録されます。制限ポリシーは、デバイス上のワークプロファイルまたは管理対象デバイスのいずれかに適用できます。

企業所有デバイス上のワークプロファイルモードで登録されたデバイスでは、以下の制限は機能しません。

- バックアップサービスを許可

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- システムアプリを有効にする
- キーガードによるデバイスのロックを防止
- ステータスバーの使用を許可する
- デバイスの画面をオンのままにする
- アプリケーション設定のユーザー制御を許可する
- ユーザーがユーザー資格情報を構成することを許可する
- VPN構成を許可する
- USB大容量ストレージを許可する
- 出荷時設定へのリセットを許可する
- アプリのアンインストールを許可する
- Google Play以外のアプリを許可する
- プロファイル間のコピーアンドペーストを許可する
- アプリの検証を有効にする
- アカウント管理を許可する
- 印刷を許可する
- NFCを許可する
- ユーザーの追加を許可する

デフォルトでは、デバイスがAndroid Enterpriseのワークプロファイルモードに登録されている場合、**USBデバッグと不明なソース**の設定は無効になります。

詳細については、このビデオをご覧ください。



- **ワークプロファイルを持つ完全に管理されたデバイス/企業所有デバイス上のワークプロファイルに適用:** ワークプロファイルを持つ完全に管理されたデバイスに対して、制限ポリシー設定を構成できるようにします。これらのデバイスは、COPE (corporate owned personally enabled) デバイスとも呼ばれます。この設定が**オン**の場合、次のいずれかの設定を選択します。
  - **ワークプロファイル:** 構成する制限設定は、デバイス上のワークプロファイルにのみ適用されます。
  - **管理対象デバイス:** 構成する制限設定は、デバイスにのみ適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

この設定が**オフ**の場合、構成する資格情報設定は、ワークプロファイルに明示的に適用される設定を除き、デバイスに適用されます。デフォルトは**オフ**です。

ワークプロファイルを持つ完全に管理されたデバイス/企業所有デバイス上のワークプロファイルに適用がオフの場合、次の設定を構成します。

- **セキュリティ**
  - **アカウント管理を許可:** ワークプロファイルおよび管理対象デバイスにアカウントを追加できるようにします。デフォルトは**オフ**です。
  - **ワークプロファイルからのコピーと貼り付けを許可: オン**の場合、ユーザーはワークプロファイルのアプリから個人プロファイルのアプリにデータをコピーして貼り付けることができます。デフォルトは**オフ**です。
  - **個人プロファイルからのデータ共有を許可: オン**の場合、ユーザーは個人プロファイルのアプリからワークプロファイルのアプリにファイルやデータをコピー、貼り付け、共有できます。デフォルトは**オフ**です。
  - **画面キャプチャを許可:** ユーザーがデバイス画面を録画または画面キャプチャできるようにします。デフォルトは**オフ**です。
  - **カメラの使用を許可:** ユーザーがデバイスのカメラで写真やビデオを撮影できるようにします。デフォルトは**オフ**です。
  - **VPN構成を許可:** ユーザーがVPN構成を作成できるようにします。Android 6以降を実行しているワークプロファイルデバイスおよび完全に管理されたデバイスに適用されます。デフォルトは**オン**です。
  - **バックアップサービスを許可:** ユーザーがデバイス上のアプリケーションデータとシステムデータをバックアップできるようにします。デフォルトは**オン**です。
  - **NFCを許可:** ユーザーがNFC（近距離無線通信）を使用して、デバイスから別のデバイスにウェブページ、写真、ビデオ、またはその他のコンテンツを送信できるようにします。MDM 4.0以降の場合。デフォルトは**オン**です。
  - **位置情報プロバイダーの設定を許可:** ユーザーがデバイスでGPSをオンにできるようにします。Android API 28以降の場合。デフォルトは**オン**です。
  - **位置情報共有を許可:** 管理対象プロファイルの場合、デバイス所有者がこの設定を上書きできます。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **ヒント:**
>
> Citrix Endpoint Managementで位置情報デバイスポリシーを作成し、地理的境界を適用できます。「位置情報デバイスポリシー」を参照してください。

- **ユーザーがユーザー資格情報を構成することを許可:** ユーザーが管理対象キーストアで資格情報を構成できるかどうかを指定します。デフォルトは**オン**です。
- **印刷を許可:** **オン**の場合、ユーザーはユーザーデバイスからアクセス可能な任意のプリンターに印刷できます。デフォルトは**オフ**です。対象：Android 9以降。
- **USBデバッグを許可:** デフォルトは**オフ**です。

- **アプリ**
  - **システムアプリを有効にする:** ユーザーがプリインストールされたデバイスアプリを実行できるようにします。デフォルトは**オフ**です。特定のアプリを有効にするには、**システムアプリリスト**テーブルで**追加**をクリックします。
    - **システムアプリリスト:** デバイスで有効にするシステムアプリのリスト。**システムアプリを有効にする**を**オン**に設定し、アプリのパッケージ名を追加します。システムアプリのパッケージ名を調べるには、Android Debug Bridge (`adb`) を使用してAndroidパッケージマネージャー (`pm`) コマンドを呼び出すことができます。たとえば、`adb shell "pm list packages -f name"`（「name」はパッケージ名の一部）です。詳しくは、`<https://developer.android.com/studio/command-line/adb>`を参照してください。Android Enterpriseデバイスの場合、Android Enterpriseアプリの権限ポリシーを使用してアプリの権限を制限できます。
  - **アプリケーションを無効にする:** 指定されたアプリのリストがデバイスで実行されないようにブロックします。デフォルトは**オフ**です。インストールされているアプリを無効にするには、設定を**オン**に変更し、**アプリケーションリスト**テーブルで**追加**をクリックします。
    - **アプリケーションリスト:** ブロックするアプリのリスト。**アプリケーションを無効にする**を**オン**に設定し、アプリを追加します。アプリのパッケージ名を入力します。アプリリストを変更して展開すると、以前のアプリリストが上書きされます。例：com.example1とcom.example2を無効にし、後でリストをcom.example1とcom.example3に変更した場合、Citrix Endpoint Managementはcom.example.2を有効にします。
  - **資格情報マネージャーアプリケーション:** アプリケーションが資格情報プロバイダーとして機能できるかどうかを制御します。デフォルトは**オフ**です。この設定が**オン**の場合、ユー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ザーはパッケージポリシータイプを選択し、**資格情報プロバイダーアプリリスト**テーブルで**追加**をクリックして、パッケージ名でアプリを追加できます。この機能はAndroid 14以降で利用可能であり、Secure Hubバージョン26.5.0以降が必要です。

- **パッケージポリシータイプ:** 許可またはブロックされる資格情報プロバイダーを指定します。デフォルトオプションは**許可リストとシステムパッケージ**で、OEMデフォルトの資格情報プロバイダーと資格情報プロバイダーの許可リストからのアクセスを許可します。その他のオプションは、ユーザーが使用できる資格情報プロバイダーをポリシー内のパッケージに制限する**許可リストのみ**と、ポリシーにリストされている資格情報プロバイダーがユーザーによって使用されるのをブロックする**ブロックリスト**です。
- **資格情報プロバイダーアプリリスト:** パッケージポリシータイプに基づいて、アプリケーションを資格情報プロバイダーとして許可またはブロックするには、**追加**をクリックし、アプリパッケージ名を入力して、**保存**をクリックします。追加したいアプリごとに繰り返します。

- **アプリの検証を有効にする:** OSがアプリをスキャンして悪意のある動作を検出できるようにします。デフォルトは**オン**です。
- **Googleアプリを有効にする:** ユーザーがGoogleモバイルサービスからデバイスにアプリをダウンロードできるようにします。デフォルトは**オン**です。
- **Google Play以外のアプリを許可する:** Google Play以外のストアからのアプリのインストールを許可します。デフォルトは**オフ**です。
- **すべてのプロファイルでGoogle Play以外のアプリを許可する: オン**の場合、ユーザーはデバイス上のすべてのプロファイルでGoogle Play以外のストアからアプリをインストールできます。デフォルトは**オフ**です。
- **アプリケーション設定のユーザー制御を許可する:** ユーザーがアプリをアンインストールしたり、アプリを無効にしたり、キャッシュとデータをクリアしたり、任意のアプリを強制停止したり、デフォルトをクリアしたりできるようにします。ユーザーはこれらのアクションを「設定」アプリから実行します。デフォルトは**オフ**です。
- **アプリのアンインストールを許可する:** ユーザーが管理対象Google Playストア内からアプリをアンインストールできるようにします。デフォルトは**オフ**です。

- **BYODワークプロファイル**
  - **接続されたアプリを有効にする:** 有効にすると、ユーザーは仕事用と個人用の両方のデータを使用して、仕事用プロファイルと個人用プロファイル間で通信できるアプリを選択できます。有効にした後、**追加**をクリックし、目的のアプリを選択して、**保存**をクリックします。この機能を有効にするには、ワークプロファイルが必要です。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ホーム画面にワークプロファイルアプリウィジェットを許可する:** この設定が**オン**の場合、ユーザーはデバイスのホーム画面にワークプロファイルアプリウィジェットを配置できます。この設定が**オフ**の場合、ユーザーはデバイスのホーム画面にワークプロファイルアプリウィジェットを配置できません。デフォルトは**オフ**です。
  - **ウィジェットが許可されているアプリ:** ホーム画面で許可したいアプリのリストです。**ホーム画面にワークプロファイルアプリウィジェットを許可する**を**オン**に設定し、アプリを追加します。**追加**をクリックし、リストからホーム画面でウィジェットを許可したいアプリを選択します。**保存**をクリックします。さらにアプリウィジェットを許可するには、このプロセスを繰り返します。
- **デバイスの連絡先にワークプロファイルの連絡先を許可する:** 着信時に、管理対象のAndroid Enterpriseプロファイルからの連絡先を親プロファイルに表示します（Android 7.0以降）。デフォルトは**オフ**です。

- **完全に管理されたデバイスのみ**
  - **ユーザーの追加を許可する:** ユーザーがデバイスに新しいユーザーを追加できるようにします。デフォルトは**オン**です。
  - **データローミングを許可:** ユーザーがローミング中に携帯データを使用できるようにします。デフォルトはオフで、ユーザーのデバイスでのローミングを無効にします。デフォルトは**オフ**です。
  - **SMSを許可:** ユーザーがSMSメッセージを送受信できるようにします。デフォルトは**オフ**です。
  - **ステータスバーの使用を許可: オン**の場合、この設定は管理対象デバイスおよび専用デバイス（COSUデバイスとも呼ばれます）でステータスバーを有効にします。この設定は、通知、クイック設定、および全画面モードからの脱出を可能にするその他の画面オーバーレイを無効にします。ユーザーはシステム設定に移動して通知を確認できます。Android 6.0以降の場合。デフォルトは**オフ**です。
  - **Bluetoothを許可:** ユーザーがBluetoothを使用できるようにします。デフォルトは**オン**です。
    - **Bluetooth共有を許可:** 選択されていない場合、ユーザーはデバイスでBluetoothによる送信共有を確立できません。デフォルトは選択されています。
  - **日付と時刻の設定を許可:** ユーザーがデバイスの日付と時刻を変更できるようにします。デフォルトは**オン**です。
  - **工場出荷時設定へのリセットを許可:** ユーザーがデバイスを工場出荷時設定にリセットできるようにします。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **デバイス画面をオンのままにする:** この設定が**オン**の場合、デバイスが接続されている間、デバイス画面はオンのままになります。デフォルトは**オフ**です。
- **USB大容量ストレージを許可:** ユーザーのデバイスとコンピューター間でUSB接続を介した大容量データファイルの転送を許可します。デフォルトは**オン**です。
- **マイクを許可:** ユーザーがデバイスのマイクを使用できるようにします。デフォルトは**オン**です。
- **テザリングを許可:** ユーザーがポータブルホットスポットを設定し、データをテザリングできるようにします。デフォルトは**オフ**です。
- **キーガードによるデバイスのロックを防止: オン**の場合、この設定は管理対象デバイスおよび専用デバイス（COSUデバイスとも呼ばれます）のロック画面でキーガードを無効にします。デフォルトは**オフ**です。
- **Wi-Fiの変更を許可: オン**の場合、ユーザーはWi-Fiをオンまたはオフにしたり、Wi-Fiネットワークに接続したりできます。デフォルトは**オン**です。
- **ファイル転送を許可:** USB経由でのファイル転送を許可します。デフォルトは**オフ**です。

- **サムスン**
  - **TIMAキーストアを有効にする:** TIMAキーストアは、TrustZoneベースの対称鍵用のセキュアな鍵ストレージを提供します。RSA鍵ペアと証明書は、ストレージのためにデフォルトのキーストアプロバイダーにルーティングされます。デフォルトは**オフ**です。
  - **共有リストを許可する:** ユーザーが「共有」リスト内のアプリ間でコンテンツを共有できるようにします。デフォルトは**オン**です。
  - **監査ログを有効にする:** デバイスのフォレンジック分析のためにイベント監査ログの作成を有効にします。デフォルトは**オフ**です。
- **Samsung: 完全管理対象デバイスのみ**
  - **緊急通報のみを許可する:** ユーザーがデバイスで緊急通報のみモードを有効にできるようにします。デフォルトは**オフ**です。
  - **ファームウェアの回復を許可する:** ユーザーがデバイスのファームウェアを回復できるようにします。デフォルトは**オン**です。
  - **高速暗号化を許可する:** 使用中のメモリ領域のみを暗号化できるようにします。この暗号化は、すべてのデータを暗号化するフルディスク暗号化とは対照的です。このデータには、設定、アプリケーションデータ、ダウンロードされたファイルとアプリケーション、メディア、その他のファイルが含まれます。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Common Criteriaモードを有効にする:** デバイスをCommon Criteriaモードにします。Common Criteria構成は、厳格なセキュリティプロセスを強制します。デフォルトは**オン**です。
- **再起動バナーを有効にする:** ユーザーのデバイスが再起動されたときに、DoD承認のシステム使用通知メッセージまたはバナーを表示します。デフォルトは**オフ**です。
- **設定変更を許可する:** ユーザーが完全管理対象デバイスの設定を変更できるようにします。デフォルトは**オン**です。
- **バックグラウンドデータ使用を有効にする:** アプリがバックグラウンドでデータを同期できるようにします（完全管理対象デバイスの場合）。デフォルトは**オン**です。
- **クリップボードを許可する:** ユーザーがデバイスのクリップボードにデータをコピーできるようにします。
  - **クリップボード共有を許可する:** ユーザーがデバイスとコンピューター間でクリップボードコンテンツを共有できるようにします（MDM 4.0以降）。
- **ホームキーを許可する:** ユーザーが完全管理対象デバイスで**ホーム**キーを使用できるようにします。デフォルトは**オン**です。
- **モックロケーションを許可する:** ユーザーがGPS位置情報を偽装できるようにします。完全管理対象デバイスの場合。デフォルトは**オフ**です。
- **NFC:** ユーザーが完全に管理されたデバイス (MDM 3.0 以降) で NFC を使用できるようにします。デフォルトは**オン**です。
- **電源オフを許可:** ユーザーが完全に管理されたデバイス (MDM 3.0 以降) の電源をオフにできるようにします。デフォルトは**オン**です。
- **Wi-Fi Direct を許可:** ユーザーが Wi-Fi 接続を介して別のデバイスに直接接続できるようにします。デフォルトは**オン**です。**オン**の場合、**Wi-Fi 変更を許可**設定を有効にする必要があります。
- **SD カードを許可:** ユーザーが利用可能な場合、デバイスで SD カードを使用できるようにします。デフォルトは**オン**です。
- **USB ホストストレージを許可:** USB デバイスがユーザーのデバイスに接続されたときに、ユーザーのデバイスが USB ホストとして機能できるようにします。その後、ユーザーのデバイスは USB デバイスに電力を供給します。デフォルトは**オン**です。
- **音声ダイヤラーを許可:** ユーザーがデバイス (MDM 4.0 以降) で音声ダイヤラーを使用できるようにします。デフォルトは**オン**です。
- **S ビームを許可:** ユーザーが NFC および Wi-Fi Direct を使用して他のユーザーとコンテンツを共有できるようにします (MDM 4.0 以降)。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **S Voice を許可:** ユーザーがデバイス (MDM 4.0 以降) でインテリジェントパーソナルアシスタントおよび知識ナビゲーターを使用できるようにします。デフォルトは**オン**です。
- **USB テザリングを許可:** ユーザーが USB 接続を使用してモバイルデータ接続を別のデバイスと共有できるようにします。デフォルトは**オフ**です。**オン**の場合、**テザリングを許可**設定も**オン**にする必要があります。
- **Bluetooth テザリングを許可:** ユーザーが Bluetooth 接続を使用してモバイルデータ接続を別のデバイスと共有できるようにします。デフォルトは**オフ**です。**オン**の場合、**テザリングを許可**設定も**オン**にする必要があります。
  - **Bluetooth 共有を許可:** 選択されていない場合、ユーザーはデバイスで Bluetooth による送信共有を確立できません。デフォルトは選択されています。
- **Wi-Fi テザリングを許可:** ユーザーが Wi-Fi 接続を使用してモバイルデータ接続を別のデバイスと共有できるようにします。デフォルトは**オフ**です。**オン**の場合、**テザリングを許可**設定も**オン**にする必要があります。
- **MMS 受信を許可:** ユーザーが MMS メッセージを受信できるようにします。デフォルトは**オフ**です。**オン**の場合、**SMS を許可**設定をオンにする必要があります。
- **MMS 送信を許可:** ユーザーが MMS メッセージを送信できるようにします。デフォルトは**オフ**です。**オン**の場合、**SMS を許可**設定をオンにする必要があります。
- **SMS 受信を許可:** ユーザーが SMS メッセージを受信できるようにします。デフォルトは**オフ**です。**オン**の場合、**SMS を許可**設定をオンにする必要があります。
- **SMS送信を許可:** ユーザーがSMSメッセージを送信できるようにします。デフォルトは**オフ**です。**オン**の場合、**SMSを許可**設定をオンにする必要があります。
- **モバイルネットワークを構成:** ユーザーが携帯データ接続を使用できるようにします。デフォルトは**オフ**です。
- **1日あたりの制限 (MB):** ユーザーが毎日使用できるモバイルデータのMB数を入力します。デフォルトは0で、この機能は無効になります (MDM 4.0以降)。
- **1週間あたりの制限 (MB):** ユーザーが毎週使用できるモバイルデータのMB数を入力します。デフォルトは0で、この機能は無効になります (MDM 4.0以降)。
- **1か月あたりの制限 (MB):** ユーザーが毎月使用できるモバイルデータのMB数を入力します。デフォルトは0で、この機能は無効になります (MDM 4.0以降)。
- **セキュアなVPN接続のみを許可:** ユーザーがセキュアな接続のみを使用できるようにします (MDM 4.0以降)。デフォルトは**オン**です。
- **音声録音を許可:** ユーザーがデバイスで音声を録音できるようにします (MDM 4.0以降)。デフォルトは**オン**です。**オン**の場合、**マイクを許可**設定をオンにする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ビデオ録画を許可:** ユーザーがデバイスでビデオを録画できるようにします (MDM 4.0以降)。デフォルトは**オフ**です。**オン**の場合、**カメラの使用を許可**設定をオンにする必要があります。
- **ローミング時のプッシュメッセージを許可:** ユーザーがプッシュのために携帯データを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。
- **ローミング時の自動同期を許可:** ユーザーが同期のために携帯データを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。
- **ローミング時の音声通話を許可:** ユーザーが音声通話のために携帯データを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。

ワークプロファイルを持つ完全に管理されたデバイス/企業所有デバイス上のワークプロファイルに適用がオンで、**ワークプロファイルを持つ完全に管理されたデバイスの場合、ポリシーを適用する対象**が**ワークプロファイル**に設定されている場合、以下の設定を構成します。

- **セキュリティ**
  - **アカウント管理を許可:** ワークプロファイルおよび管理対象デバイスにアカウントを追加できるようにします。デフォルトは**オフ**です。
  - **プロファイル間のコピーと貼り付けを許可: オン**の場合、ユーザーはAndroid Enterpriseプロファイルのアプリと個人領域のアプリ間でコピーと貼り付けを行うことができます。デフォルトは**オフ**です。
  - **画面キャプチャを許可する:** ユーザーがデバイス画面を記録またはスクリーンキャプチャすることを許可します。デフォルトは**オフ**です。
  - **カメラの使用を許可する:** ユーザーがデバイスのカメラで写真やビデオを撮影することを許可します。デフォルトは**オフ**です。
  - **位置情報プロバイダーの設定を許可する:** ユーザーがデバイスでGPSをオンにすることを許可します。Android API 28以降の場合。デフォルトは**オン**です。
  - **位置情報の共有を許可する:** 管理対象プロファイルの場合、デバイス所有者がこの設定を上書きできます。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **ヒント:**
>
> Citrix Endpoint Managementで位置情報デバイスポリシーを作成して、地理的境界を適用できます。位置情報デバイスポリシーを参照してください。

- **ユーザーがユーザー資格情報を構成することを許可する:** ユーザーが管理対象キーストアで資格情報を構成できるかどうかを指定します。デフォルトは**オン**です。
- **印刷を許可する:** **オン**の場合、ユーザーデバイスからアクセス可能な任意のプリンターへの印刷をユーザーに許可します。デフォルトは**オフ**です。対象: Android 9以降。

- **アプリ**
  - **システムアプリを有効にする:** ユーザーがプリインストールされたデバイスアプリを実行することを許可します。デフォルトは**オフ**です。特定のアプリを有効にするには、**システムアプリリスト**テーブルで**追加**をクリックします。
    - **システムアプリリスト:** デバイスで有効にするシステムアプリのリストです。**システムアプリを有効にする**を**オン**に設定し、アプリのパッケージ名を追加します。システムアプリのパッケージ名を調べるには、Android Debug Bridge (`adb`) を使用してAndroidパッケージマネージャー (`pm`) コマンドを呼び出すことができます。たとえば、`adb shell "pm list packages -f name"` のように、「name」はパッケージ名の一部です。詳細については、`<https://developer.android.com/studio/command-line/adb>` を参照してください。Android Enterpriseデバイスの場合、Android Enterpriseアプリのアクセス許可ポリシーを使用してアプリのアクセス許可を制限できます。
  - **アプリケーションを無効にする:** 指定されたアプリのリストがデバイスで実行されないようにブロックします。デフォルトは**オフ**です。インストールされているアプリを無効にするには、設定を**オン**に変更し、**アプリケーションリスト**テーブルで**追加**をクリックします。
    - **アプリケーションリスト:** ブロックするアプリのリストです。**アプリケーションを無効にする**を**オン**に設定し、アプリを追加します。アプリのパッケージ名を入力します。アプリリストを変更して展開すると、以前のアプリリストが上書きされます。例: com.example1とcom.example2を無効にし、後でリストをcom.example1とcom.example3に変更すると、Citrix Endpoint Managementはcom.example.2を有効にします。
  - **資格情報マネージャーアプリケーション:** アプリケーションが資格情報プロバイダーとして機能できるかどうかを制御します。デフォルトは**オフ**です。この設定が**オン**の場合、ユーザーはパッケージポリシータイプを選択し、**資格情報プロバイダーアプリリスト**テーブル

© 1997–2026 Citrix Systems, Inc. All rights reserved.

で**追加**をクリックして、パッケージ名でアプリを追加できます。この機能はAndroid 14以降で利用可能であり、Secure Hubバージョン26.5.0以降が必要です。

- **パッケージポリシータイプ:** どの資格情報プロバイダーが許可またはブロックされるかを指定します。デフォルトのオプションは**許可リストとシステムパッケージ**で、OEMデフォルトの資格情報プロバイダーと資格情報プロバイダーの許可リストからのアクセスを許可します。その他のオプションは、ユーザーが使用できる資格情報プロバイダーをポリシー内のパッケージに制限する**許可リストのみ**と、ポリシーにリストされている資格情報プロバイダーがユーザーによって使用されるのをブロックする**ブロックリスト**です。
- **資格情報プロバイダーアプリリスト:** パッケージポリシータイプに基づいて、アプリケーションを資格情報プロバイダーとして許可またはブロックするには、**追加**をクリックし、アプリのパッケージ名を入力して、**保存**をクリックします。追加する各アプリについて繰り返します。

- **アプリの検証を有効にする:** OSがアプリをスキャンして悪意のある動作を検出できるようにします。デフォルトは**オン**です。
- **Googleアプリを有効にする:** ユーザーがGoogleモバイルサービスからデバイスにアプリをダウンロードできるようにします。デフォルトは**オン**です。
- **Google Play以外のアプリを許可する:** Google Play以外のストアからのアプリのインストールを許可します。デフォルトは**オフ**です。
- **アプリケーション設定のユーザー制御を許可する:** ユーザーがアプリのアンインストール、アプリの無効化、キャッシュとデータのクリア、任意のアプリの強制停止、デフォルトのクリアを行えるようにします。ユーザーはこれらのアクションをアプリから実行します。デフォルトは**オフ**です。
- **アプリのアンインストールを許可する:** ユーザーがManaged Google Playストア内からアプリをアンインストールできるようにします。デフォルトは**オフ**です。

- **BYODワークプロファイル**
  - **ホーム画面でのワークプロファイルアプリウィジェットを許可する:** この設定が**オン**の場合、ユーザーはワークプロファイルアプリウィジェットをデバイスのホーム画面に配置できます。この設定が**オフ**の場合、ユーザーはワークプロファイルアプリウィジェットをデバイスのホーム画面に配置できません。デフォルトは**オフ**です。
    - **ウィジェットが許可されているアプリ:** ホーム画面で許可するアプリのリストです。**ホーム画面でのワークプロファイルアプリウィジェットを許可する**を**オン**に設定し、アプリを追加します。**追加**をクリックし、ホーム画面でウィジェットを許可するアプリ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

をリストから選択します。**保存**をクリックします。このプロセスを繰り返して、さらに多くのアプリウィジェットを許可します。

- **デバイスの連絡先でのワークプロファイル連絡先を許可する:** 管理対象のAndroid Enterpriseプロファイルからの連絡先を、親プロファイルに着信通話用として表示します（Android 7.0以降）。デフォルトは**オフ**です。

- **サムスン**

  - **TIMAキーストアを有効にする:** TIMAキーストアは、対称鍵用のTrustZoneベースの安全な鍵ストレージを提供します。RSA鍵ペアと証明書は、ストレージのためにデフォルトのキーストアプロバイダーにルーティングされます。デフォルトは**オフ**です。
  - **共有リストを許可する:** ユーザーが「共有」リスト内のアプリ間でコンテンツを共有できるようにします。デフォルトは**オン**です。
  - **監査ログを有効にする:** デバイスのフォレンジック分析のためにイベント監査ログの作成を有効にします。デフォルトは**オフ**です。

ワークプロファイルを持つ完全に管理されたデバイス/企業所有デバイス上のワークプロファイルに適用がオンで、**ワークプロファイルを持つ完全に管理されたデバイスの場合、ポリシーを適用する対象**が**管理対象デバイス**に設定されている場合、これらの設定を構成します。

- **セキュリティ**

  - **アカウント管理を許可:** アカウントをワークプロファイルおよび管理対象デバイスに追加できるようにします。デフォルトは**オフ**です。
  - **プロファイル間のコピーと貼り付けを許可: オン**の場合、ユーザーはAndroid Enterpriseプロファイルのアプリと個人領域のアプリの間でコピーと貼り付けを行うことができます。デフォルトは**オフ**です。
  - **画面キャプチャを許可:** ユーザーがデバイス画面を録画またはスクリーンキャプチャできるようにします。デフォルトは**オフ**です。
  - **カメラの使用を許可:** ユーザーがデバイスのカメラで写真やビデオを撮影できるようにします。デフォルトは**オフ**です。
  - **VPN構成を許可:** ユーザーがVPN構成を作成できるようにします。Android 6以降を実行しているワークプロファイルデバイスおよび完全に管理されているデバイスの場合。デフォルトは**オン**です。
  - **バックアップサービスを許可:** ユーザーがデバイス上のアプリケーションデータとシステムデータをバックアップできるようにします。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **NFCを許可:** ユーザーがNFC (Near Field Communication) を使用して、Webページ、写真、ビデオ、またはその他のコンテンツを自分のデバイスから別のデバイスに送信できるようにします。MDM 4.0以降の場合。デフォルトは**オン**です。
- **位置情報プロバイダーの構成を許可:** ユーザーがデバイスでGPSをオンにできるようにします。Android API 28以降の場合。デフォルトは**オン**です。
- **位置情報共有を許可:** 管理対象プロファイルの場合、デバイス所有者がこの設定を上書きできます。デフォルトは**オフ**です。

  ヒント:

  Citrix Endpoint Managementで位置情報デバイスポリシーを作成して、地理的境界を適用できます。位置情報デバイスポリシーを参照してください。

- **ユーザーがユーザー資格情報を構成することを許可:** ユーザーが管理対象キーストアで資格情報を構成できるかどうかを指定します。デフォルトは**オン**です。
- **印刷を許可:** **オン**の場合、ユーザーはユーザーデバイスからアクセス可能な任意のプリンターに印刷できます。デフォルトは**オフ**です。利用可能: Android 9以降。
- **USBデバッグを許可:** デフォルトは**オフ**です。

- **アプリ**
  - **システムアプリを有効にする:** ユーザーがプリインストールされているデバイスアプリを実行できるようにします。デフォルトは**オフ**です。特定のアプリを有効にするには、**システムアプリリスト**テーブルで**追加**をクリックします。
    - **システムアプリリスト:** デバイスで有効にするシステムアプリのリストです。**システムアプリを有効にする**を**オン**に設定し、アプリのパッケージ名を追加します。システムアプリのパッケージ名を調べるには、Android Debug Bridge (`adb`) を使用してAndroidパッケージマネージャー (`pm`) コマンドを呼び出すことができます。たとえば、`adb shell "pm list packages -f name"` のように、「name」はパッケージ名の一部です。詳しくは、`<https://developer.android.com/studio/command-line/adb>` を参照してください。Android Enterpriseデバイスの場合、Android Enterpriseアプリのアクセス許可 ポリシーを使用してアプリのアクセス許可を制限できます。
  - **アプリケーションを無効にする:** 指定されたアプリのリストがデバイスで実行されないようにブロックします。デフォルトは**オフ**です。インストールされているアプリを無効にするには、設定を**オン**に変更し、**アプリケーションリスト**テーブルで**追加**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **アプリケーションリスト:** ブロックするアプリのリストです。**アプリケーションを無効にする**を**オン**に設定し、アプリを追加します。アプリのパッケージ名を入力します。アプリリストを変更して展開すると、以前のアプリリストが上書きされます。例：com.example1とcom.example2を無効にし、後でリストをcom.example1とcom.example3に変更した場合、Citrix Endpoint Managementはcom.example.2を有効にします。

  - **アプリの検証を有効にする:** OSがアプリをスキャンして悪意のある動作を検出できるようにします。デフォルトは**オン**です。
  - **Googleアプリを有効にする:** ユーザーがGoogle Mobile Servicesからデバイスにアプリをダウンロードできるようにします。デフォルトは**オン**です。
  - **Google Play以外のアプリを許可する:** Google Play以外のストアからのアプリのインストールを許可します。デフォルトは**オフ**です。
  - **ユーザーによるアプリケーション設定の制御を許可する:** ユーザーがアプリのアンインストール、アプリの無効化、キャッシュとデータのクリア、任意のアプリの強制停止、およびデフォルトのクリアを行えるようにします。ユーザーはこれらのアクションをアプリから実行します。デフォルトは**オフ**です。
  - **アプリのアンインストールを許可する:** ユーザーがManaged Google Playストア内からアプリをアンインストールできるようにします。デフォルトは**オフ**です。

- **完全に管理されたデバイスのみ**
  - **ユーザーの追加を許可する:** ユーザーがデバイスに新しいユーザーを追加できるようにします。デフォルトは**オン**です。
  - **データローミングを許可する:** ユーザーがローミング中にモバイルデータを使用できるようにします。デフォルトはオフで、ユーザーのデバイスでのローミングを無効にします。デフォルトは**オフ**です。
  - **SMSを許可する:** ユーザーがSMSメッセージを送受信できるようにします。デフォルトは**オフ**です。
  - **ステータスバーの使用を許可する: オン**の場合、この設定は管理対象デバイスおよび専用デバイス（COSUデバイスとも呼ばれる）でステータスバーを有効にします。この設定は、通知、クイック設定、および全画面モードからの脱出を可能にするその他の画面オーバーレイを無効にします。ユーザーはシステム設定に移動して通知を確認できます。Android 6.0以降の場合。デフォルトは**オフ**です。
  - **Bluetoothを許可:** ユーザーがBluetoothを使用できるようにします。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **Bluetooth共有を許可:** 選択されていない場合、ユーザーはデバイスでBluetoothによる発信共有を確立できません。デフォルトは選択されています。

  - **日付と時刻の設定を許可:** ユーザーがデバイスの日付と時刻を変更できるようにします。デフォルトは**オン**です。
  - **出荷時設定へのリセットを許可:** ユーザーがデバイスを出荷時設定にリセットできるようにします。デフォルトは**オン**です。
  - **出荷時設定へのリセット保護を許可:** **オン**に設定されている場合、リカバリモードを使用してデバイスがリセットされると、ユーザーはリセット前にデバイスにあったアカウントの資格情報を入力する必要があります。リセット前に設定されていた場合は、デバイスロックを提供することもできます。**オフ**に設定されている場合、リセット後に認証は不要です。デフォルトは**オン**です。
  - **デバイス画面をオンのままにする:** この設定が**オン**に設定されている場合、デバイスが接続されている間、デバイス画面はオンのままになります。デフォルトは**オフ**です。
  - **USB大容量記憶装置を許可:** ユーザーのデバイスとコンピューター間でUSB接続を介した大容量データファイルの転送を許可します。デフォルトは**オン**です。
  - **マイクを許可:** ユーザーがデバイスのマイクを使用できるようにします。デフォルトは**オン**です。
  - **テザリングを許可:** ユーザーがポータブルホットスポットを設定し、データをテザリングできるようにします。デフォルトは**オフ**です。この設定がオンの場合、Samsungデバイスでは次の設定が利用可能です。
  - **キーガードによるデバイスのロックを防止:** **オン**の場合、この設定は、管理対象デバイスおよび専用デバイス（COSUデバイスとも呼ばれる）のロック画面でキーガードを無効にします。デフォルトは**オフ**です。
  - **Wi-Fiの変更を許可:** **オン**の場合、ユーザーはWi-Fiをオンまたはオフにしたり、Wi-Fiネットワークに接続したりできます。デフォルトは**オン**です。
  - **ファイル転送を許可:** USB経由でのファイル転送を許可します。デフォルトは**オフ**です。

- **サムスン**

  - **TIMAキーストアを有効にする:** TIMAキーストアは、対称鍵用のTrustZoneベースの安全な鍵ストレージを提供します。RSA鍵ペアと証明書は、ストレージのためにデフォルトのキーストアプロバイダーにルーティングされます。デフォルトは**オフ**です。
  - **共有リストを許可:** ユーザーが「共有」リスト内のアプリ間でコンテンツを共有できるようにします。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **監査ログを有効にする:** デバイスのフォレンジック分析のためのイベント監査ログの作成を有効にします。デフォルトは**オフ**です。

- **Samsung: フルマネージドデバイスのみ**
  - **緊急通話のみを許可:** ユーザーがデバイスで緊急通話のみモードを有効にできるようにします。デフォルトは**オフ**です。
  - **ファームウェアの回復を許可:** ユーザーがデバイスのファームウェアを回復できるようにします。デフォルトは**オン**です。
  - **高速暗号化を許可:** 使用済みメモリ領域のみの暗号化を許可します。この暗号化は、すべてのデータを暗号化するフルディスク暗号化とは対照的です。そのデータには、設定、アプリケーションデータ、ダウンロードされたファイルとアプリケーション、メディア、その他のファイルが含まれます。デフォルトは**オン**です。
  - **コモンクライテリアモードを有効にする:** デバイスをコモンクライテリアモードにします。コモンクライテリア構成は、厳格なセキュリティプロセスを強制します。デフォルトは**オン**です。
  - **再起動バナーを有効にする:** ユーザーのデバイスが再起動されたときに、DoD承認のシステム使用通知メッセージまたはバナーを表示します。デフォルトは**オフ**です。
  - **設定変更を許可:** ユーザーがフルマネージドデバイスの設定を変更できるようにします。デフォルトは**オン**です。
  - **バックグラウンドデータ使用を有効にする:** フルマネージドデバイスの場合、アプリがバックグラウンドでデータを同期できるようにします。デフォルトは**オン**です。
  - **クリップボードを許可:** ユーザーがデバイスのクリップボードにデータをコピーできるようにします。デフォルトは**オン**です。
    - **クリップボード共有を許可:** ユーザーがデバイスとコンピューター間でクリップボードコンテンツを共有できるようにします (MDM 4.0以降)。
  - **ホームキーを許可:** ユーザーがフルマネージドデバイスで**ホーム**キーを使用できるようにします。デフォルトは**オン**です。
  - **擬似ロケーションを許可:** ユーザーがGPS位置情報を偽装できるようにします。フルマネージドデバイスの場合。デフォルトは**オフ**です。
  - **NFC:** ユーザーがフルマネージドデバイスでNFCを使用できるようにします (MDM 3.0以降)。デフォルトは**オン**です。
  - **電源オフを許可:** ユーザーがフルマネージドデバイスの電源をオフにできるようにします (MDM 3.0以降)。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

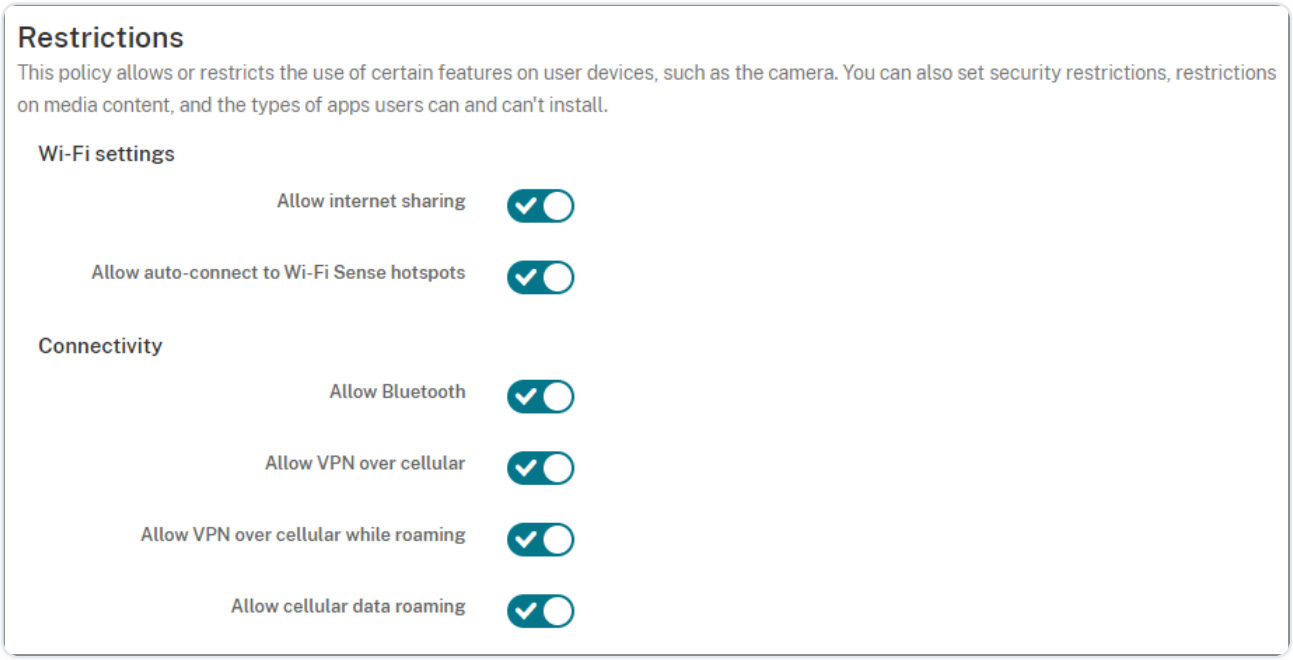
- **Wi-Fi Directを許可:** ユーザーがWi-Fi接続を介して別のデバイスに直接接続できるようにします。デフォルトは**オン**です。**オン**の場合、「**Wi-Fi変更を許可**」設定を有効にする必要があります。
- **SDカードを許可:** ユーザーが利用可能なSDカードをデバイスで使用できるようにします。デフォルトは**オン**です。
- **USBホストストレージを許可:** USBデバイスがユーザーのデバイスに接続されたときに、ユーザーのデバイスがUSBホストとして機能できるようにします。ユーザーのデバイスはUSBデバイスに電力を供給します。デフォルトは**オン**です。
- **音声ダイヤラーを許可:** ユーザーがデバイスで音声ダイヤラーを使用できるようにします (MDM 4.0以降)。デフォルトは**オン**です。
- **Sビームを許可:** ユーザーがNFCとWi-Fi Directを使用して他のユーザーとコンテンツを共有できるようにします (MDM 4.0以降)。デフォルトは**オン**です。
- **Sボイスを許可:** ユーザーがデバイスでインテリジェントパーソナルアシスタントと知識ナビゲーターを使用できるようにします (MDM 4.0以降)。デフォルトは**オン**です。
- **USBテザリングを許可:** ユーザーがUSB接続を使用してモバイルデータ接続を別のデバイスと共有できるようにします。デフォルトは**オフ**です。**オン**の場合、「**テザリングを許可**」設定も**オン**にする必要があります。
- **Bluetoothテザリングを許可:** ユーザーがBluetooth接続を使用してモバイルデータ接続を別のデバイスと共有できるようにします。デフォルトは**オフ**です。**オン**の場合、「**テザリングを許可**」設定も**オン**にする必要があります。
- **Wi-Fiテザリングを許可:** ユーザーがWi-Fi接続を使用してモバイルデータ接続を別のデバイスと共有できるようにします。デフォルトは**オフ**です。**オン**の場合、「**テザリングを許可**」設定も**オン**にする必要があります。
- **MMS受信を許可:** ユーザーがMMSメッセージを受信できるようにします。デフォルトは**オフ**です。**オン**の場合、「**SMSを許可**」設定をオンにする必要があります。
- **MMS送信を許可:** ユーザーがMMSメッセージを送信できるようにします。デフォルトは**オフ**です。**オン**の場合、「**SMSを許可**」設定をオンにする必要があります。
- **SMS受信を許可:** ユーザーがSMSメッセージを受信できるようにします。デフォルトは**オフ**です。**オン**の場合、「**SMSを許可**」設定をオンにする必要があります。
- **SMS送信を許可:** ユーザーがSMSメッセージを送信できるようにします。デフォルトは**オフ**です。**オン**の場合、「**SMSを許可**」設定をオンにする必要があります。
- **モバイルネットワークを構成:** ユーザーが携帯データ接続を使用できるようにします。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **1日あたりの制限 (MB):** ユーザーが1日に使用できるモバイルデータのMB数を入力します。デフォルトは0で、この機能は無効になります (MDM 4.0以降)。
- **週ごとの制限 (MB):** ユーザーが毎週使用できるモバイルデータのMB数を入力します。デフォルトは0で、この機能は無効になります (MDM 4.0以降)。
- **月ごとの制限 (MB):** ユーザーが毎月使用できるモバイルデータのMB数を入力します。デフォルトは0で、この機能は無効になります (MDM 4.0以降)。
- **安全なVPN接続のみを許可:** ユーザーが安全な接続のみを使用できるようにします (MDM 4.0以降)。デフォルトは**オン**です。
- **音声録音を許可:** ユーザーがデバイスで音声を録音できるようにします (MDM 4.0以降)。デフォルトは**オン**です。**オン**の場合、**マイクを許可**設定をオンにする必要があります。
- **ビデオ録画を許可:** ユーザーがデバイスでビデオを録画できるようにします (MDM 4.0以降)。デフォルトは**オフ**です。**オン**の場合、**カメラの使用を許可**設定をオンにする必要があります。
- **ローミング中のプッシュメッセージを許可:** ユーザーがプッシュのためにセルラーデータを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。
- **ローミング中の自動同期を許可:** ユーザーが同期のためにセルラーデータを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。
- **ローミング中の音声通話を許可:** ユーザーが音声通話のためにセルラーデータを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windowsデスクトップ/タブレット設定



- **Wi-Fi設定**
  - **インターネット共有を許可:** デバイスがWi-Fiホットスポットになることで、他のデバイスとインターネット接続を共有できるようにします。
- **接続**
  - **Bluetoothを許可:** デバイスがBluetooth経由で接続できるようにします。
  - **セルラー経由のVPNを許可:** デバイスがVPN経由でセルラーネットワークに接続できるようにします。
  - **ローミング中にセルラー経由のVPNを許可:** デバイスがセルラーネットワークでローミング中にVPN経由で接続することを許可します。
  - **セルラーデータローミングを許可:** ユーザーがローミング中にセルラーデータを使用することを許可します。
- **アカウント**
  - **Microsoftアカウント接続を許可:** デバイスが、メール以外の接続認証およびサービスにMicrosoftアカウントを使用することを許可します。
  - **Microsoft以外のメールを許可:** ユーザーがMicrosoft以外のメールアカウントを追加することを許可します。
- **システム**
  - **ストレージカードを許可:** デバイスがストレージカードを使用することを許可します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **テレメトリ:** ドロップダウンリストからオプションをクリックして、デバイスがテレメトリ情報を送信することを許可または制限します。デフォルトは**許可**です。その他のオプションは、**許可しない**および**セカンダリデータ要求を除く許可**です。
  - **アプリによる位置情報サービスへのアクセスを許可:** アプリによる位置情報サービスへのアクセスを許可します。
  - **内部ビルドのプレビューを許可:** ユーザーがMicrosoftの内部ビルドをプレビューすることを許可します。

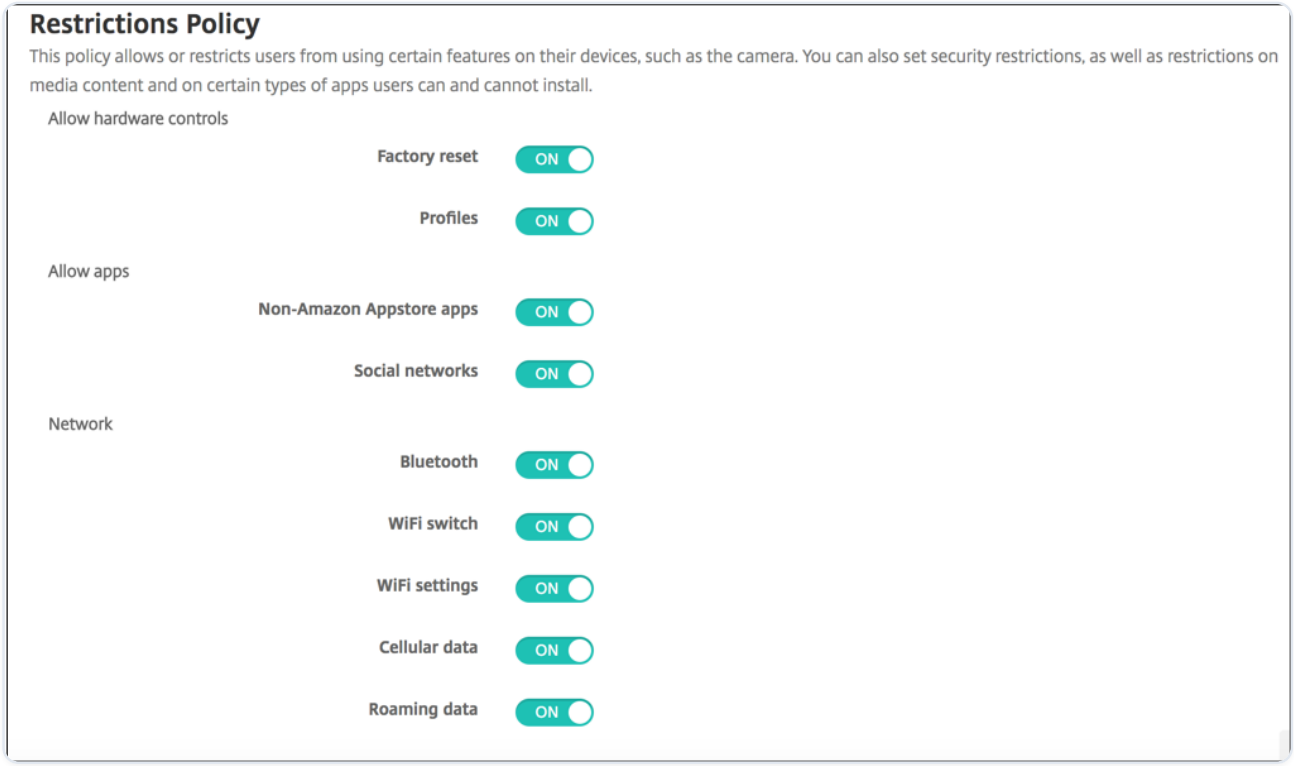
- **カメラ:** Windowsデスクトップ/タブレットのみ
  - **カメラの使用を許可:** ユーザーがデバイスのカメラを使用することを許可します。
- **ブルートゥース:** Windows デスクトップ/タブレットのみ
  - **検出可能モードを許可:** Bluetoothデバイスがローカルデバイスを検出することを許可します。
  - **ローカルデバイス名:** ローカルデバイスの名前。
- **エクスペリエンス:** Windows デスクトップ/タブレットのみ
  - **Cortana を許可:** ユーザーがインテリジェントなパーソナルアシスタントおよび知識ナビゲーターである Cortana にアクセスすることを許可します。
  - **デバイスの検出を許可:** デバイスのネットワーク検出を許可します。
  - **MDM の手動登録解除を許可:** ユーザーが Citrix Endpoint Management MDM からデバイスを手動で登録解除することを許可します。
  - **デバイス設定の同期を許可:** ユーザーがローミング中に Windows 10 デバイスと Windows 11 デバイス間で設定を同期することを許可します。
- **ロック画面の上:** Windows デスクトップ/タブレットのみ
  - **ロック画面でのトースト通知を許可:** ロック画面でのトースト通知を許可します。Windows デスクトップ/タブレットのみ
- **アプリ**
  - **アプリストアからの自動更新を許可:** アプリストアからのアプリが自動的に更新されることを許可します。Windows デスクトップ/タブレットのみ。
- **プライバシー:** Windows デスクトップ/タブレットのみ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **入力のパーソナライズを許可:** 入力パーソナライズサービスを実行することを許可します。入力パーソナライズサービスは、ユーザーが入力した内容に基づいて、ペンやタッチキーボードなどの予測入力を改善します。

- **設定:** Windows デスクトップ/タブレットのみ。
  - **自動再生を許可:** ユーザーが自動再生設定を変更することを許可します。
  - **データセンスを許可:** ユーザーがデータセンス設定を変更することを許可します。
  - **日付と時刻を許可:** ユーザーが日付と時刻の設定を変更することを許可します。
  - **言語を許可:** ユーザーが言語設定を変更できるようにします。
  - **電源スリープを許可:** ユーザーが電源とスリープの設定を変更できるようにします。
  - **地域を許可:** ユーザーが地域設定を変更できるようにします。
  - **サインインオプションを許可:** ユーザーがサインイン設定を変更できるようにします。
  - **職場を許可:** ユーザーが職場設定を変更できるようにします。
  - **アカウントを許可:** ユーザーがアカウント設定を変更できるようにします。

Amazon の設定



- **ハードウェア制御を許可**
  - **工場出荷時設定へのリセット:** ユーザーがデバイスを工場出荷時設定にリセットできるようにします

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **プロファイル:** ユーザーがデバイスのハードウェアプロファイルを変更できるようにします。

- **アプリを許可**

  - **Amazon Appstore 以外のアプリ:** ユーザーがデバイスに Amazon Appstore 以外のアプリをインストールできるようにします。
  - **ソーシャルネットワーク:** ユーザーがデバイスからソーシャルネットワークにアクセスできるようにします。

- **ネットワーク**

  - **Bluetooth:** ユーザーがBluetoothを使用できるようにします。
  - **Wi-Fiスイッチ:** アプリがWi-Fi接続状態を変更できるようにします。
  - **Wi-Fi設定:** ユーザーがWi-Fi設定を変更できるようにします。
  - **モバイルネットワークの構成:** ユーザーが携帯データ接続を使用できるようにします。
  - **ローミングデータ:** ユーザーがローミング中に携帯データを使用できるようにします。
  - **位置情報サービス:** ユーザーがGPSを使用できるようにします。

- **USBアクション:**

  - **デバッグ:** ユーザーのデバイスがUSB経由でコンピューターに接続してデバッグできるようにします。

ローミングデバイスポリシー

Citrix Endpoint Managementでデバイスポリシーを追加し、サポートされているiOSデバイスで音声およびデータローミングを許可するかどうかを設定できます。音声ローミングが無効になっている場合、データローミングは自動的に無効になります。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **音声ローミングを無効にする:** 音声ローミングを無効にするかどうかを選択します。このオプションが有効になっている場合、データローミングは自動的に無効になります。デフォルトは**オフ**で、音声ローミングが許可されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

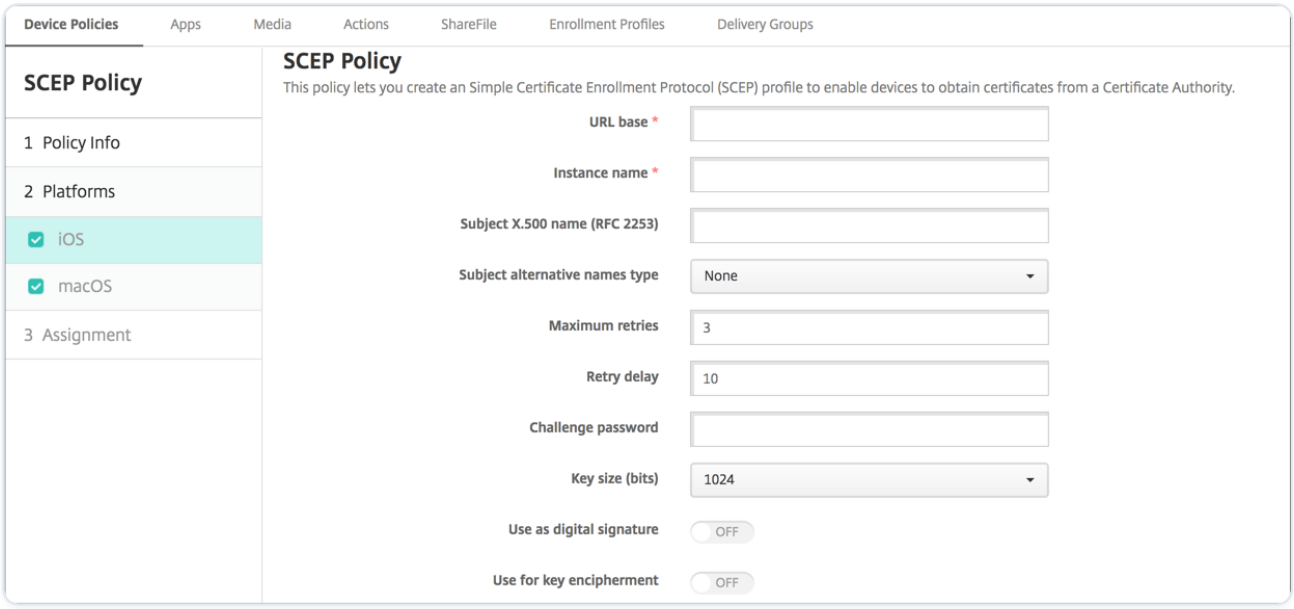
- **データローミングを無効にする:** データローミングを無効にするかどうかを選択します。このオプションは、音声ローミングが有効になっている場合にのみ使用できます。デフォルトは**オフ**で、データローミングが許可されます。

SCEP デバイスポリシー

このポリシーを使用すると、iOS および macOS デバイスが Simple Certificate Enrollment Protocol (SCEP) を介して外部 SCEP サーバーから証明書を取得するように構成できます。Citrix Endpoint Management に接続されている PKI から SCEP を使用してデバイスに証明書を配信するには、分散モードで PKI エンティティと PKI プロバイダーを作成します。詳細については、「PKI エンティティ」を参照してください。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS 設定



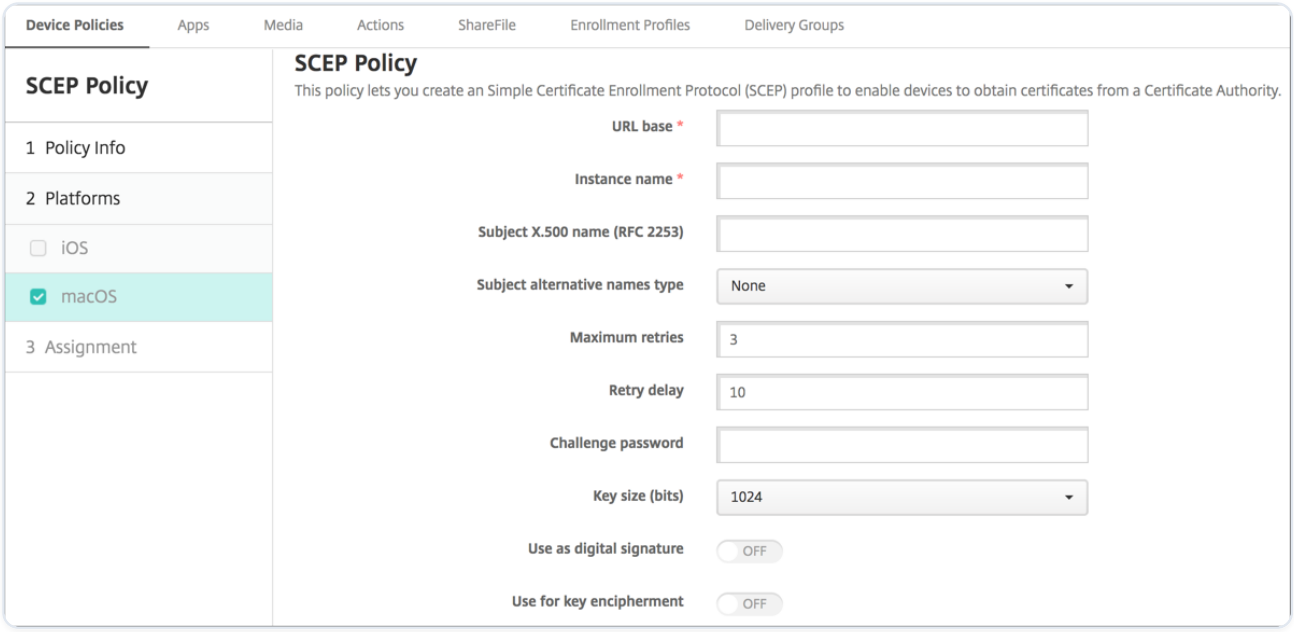
- **URL ベース:** SCEP リクエストを HTTP または HTTPS 経由で送信する場所を定義するために、SCEP サーバーのアドレスを入力します。秘密鍵は証明書署名要求 (CSR) と一緒に送信されないため、リクエストを暗号化せずに送信しても安全な場合があります。ワンタイムパスワードが再利用できるように構成されている場合は、HTTPS を使用してパスワードを保護してください。この手順は必須です。
- **インスタンス名:** SCEP サーバーが認識する任意の文字列を入力します。たとえば、example.org のようなドメイン名でも構いません。CA に複数の CA 証明書がある場合、このフィールドを使用して必要なドメインを区別できます。この手順は必須です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **サブジェクト X.500 名 (RFC 2253):** X.500 名をオブジェクト識別子 (OID) と値の配列として表現したものを入力します。たとえば、`/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar` は `[ [ [“C”, “US”] ], [ [“O”, “Apple Inc.”] ], …, [ [“1.2.5.3”, “bar” ] ] ]` に変換されます。OID は、国 (C)、地域 (L)、州 (ST)、組織 (O)、組織単位 (OU)、共通名 (CN) のショートカットを含むドット区切りの数値として表現できます。
- **サブジェクトの別名タイプ:** 別名タイプを選択します。オプションの別名タイプは、CA が証明書を発行するために必要な値を提供できます。、、、または を指定できます。
- **最大再試行回数:** SCEP サーバーが PENDING 応答を送信したときに、デバイスが再試行する回数を入力します。デフォルトは **3** です。
- **再試行遅延:** 後続の再試行間の待機時間を秒単位で入力します。最初の再試行は遅延なしで試行されます。デフォルトは **10** です。
- **チャレンジパスワード:** 事前共有シークレットを入力します。
- **キーサイズ (ビット):** キーサイズをビット単位で **2048** 以上に選択します。
- **デジタル署名として使用:** 証明書をデジタル署名として使用するかどうかを選択します。SCEP サーバーは、公開鍵を使用してハッシュを復号化する前に、証明書がデジタル署名として使用されていることを確認します。
- **鍵の暗号化に使用:** 証明書を鍵の暗号化に使用するかどうかを選択します。サーバーはまず、クライアントから提供された証明書が鍵の暗号化に許可されているかどうかを確認します。次に、サーバーは証明書内の公開鍵を使用して、データが秘密鍵で暗号化されたことを検証します。そうでない場合、操作は失敗します。
- **SHA-256 フィンガープリント (16 進数文字列):** CA が HTTP を使用している場合は、このフィールドを使用して CA 証明書のフィンガープリントを指定します。デバイスは、登録中に CA 応答の信頼性を確認するためにフィンガープリントを使用します。SHA-256 フィンガープリントを指定するか、証明書を選択してその署名をインポートできます。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0 以降でのみ利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS の設定



- **URL ベース:** SCEP リクエストが HTTP または HTTPS 経由で送信される場所を定義するために、SCEP サーバーのアドレスを入力します。秘密鍵は証明書署名要求 (CSR) と一緒に送信されないため、リクエストを暗号化せずに送信しても安全な場合があります。ワンタイムパスワードが再利用可能に構成されている場合は、HTTPS を使用してパスワードを保護してください。この手順は必須です。
- **インスタンス名:** SCEP サーバーが認識する任意の文字列を入力します。たとえば、example.org のようなドメイン名でも構いません。CA が複数の CA 証明書を持っている場合、このフィールドを使用して必要なドメインを区別できます。この手順は必須です。
- **サブジェクト X.500 名 (RFC 2253):** X.500 名をオブジェクト識別子 (OID) と値の配列として表現したものを入力します。たとえば、`/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar` は次のように翻訳されます: `[ [ [“C”, “US”] ], [ [“O”, “Apple Inc.”] ], …, [ [“1.2.5.3”, “bar” ] ] ]`。OID は、国 (C)、地域 (L)、州 (ST)、組織 (O)、組織単位 (OU)、共通名 (CN) のショートカットを含むドット区切りの数値として表現できます。
- **サブジェクト代替名タイプ:** 代替名タイプを選択します。オプションの代替名タイプは、証明書の発行に CA が必要とする値を提供できます。**なし**、**RFC 822 名**、**DNS 名**、または**URI**を指定できます。
- **最大再試行回数:** SCEP サーバーが PENDING 応答を送信したときに、デバイスが再試行する回数を入力します。デフォルトは**3**です。
- **再試行遅延:** 後続の再試行間の待機時間を秒単位で入力します。最初の再試行は遅延なしで試行されます。デフォルトは**10**です。
- **チャレンジパスワード:** 事前共有シークレットを入力します。
- **キーサイズ (ビット):** キーサイズをビット単位で**2048**以上に選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **デジタル署名として使用:** 証明書をデジタル署名として使用するかどうかを選択します。SCEPサーバーは、公開鍵を使用してハッシュを復号化する前に、証明書がデジタル署名として使用されていることを確認します。
- **鍵の暗号化に使用:** 証明書を鍵の暗号化に使用するかどうかを選択します。サーバーはまず、クライアントから提供された証明書が鍵の暗号化に許可されているかどうかを確認します。次に、サーバーは証明書内の公開鍵を使用して、データが秘密鍵で暗号化されたことを検証します。そうでない場合、操作は失敗します。
- **SHA-256フィンガープリント (16進数文字列):** CAがHTTPを使用している場合、このフィールドを使用してCA証明書のフィンガープリントを指定します。デバイスは、登録中にCA応答の信頼性を確認するためにフィンガープリントを使用します。SHA-256フィンガープリントを指定するか、証明書を選択してその署名をインポートできます。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**しない**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

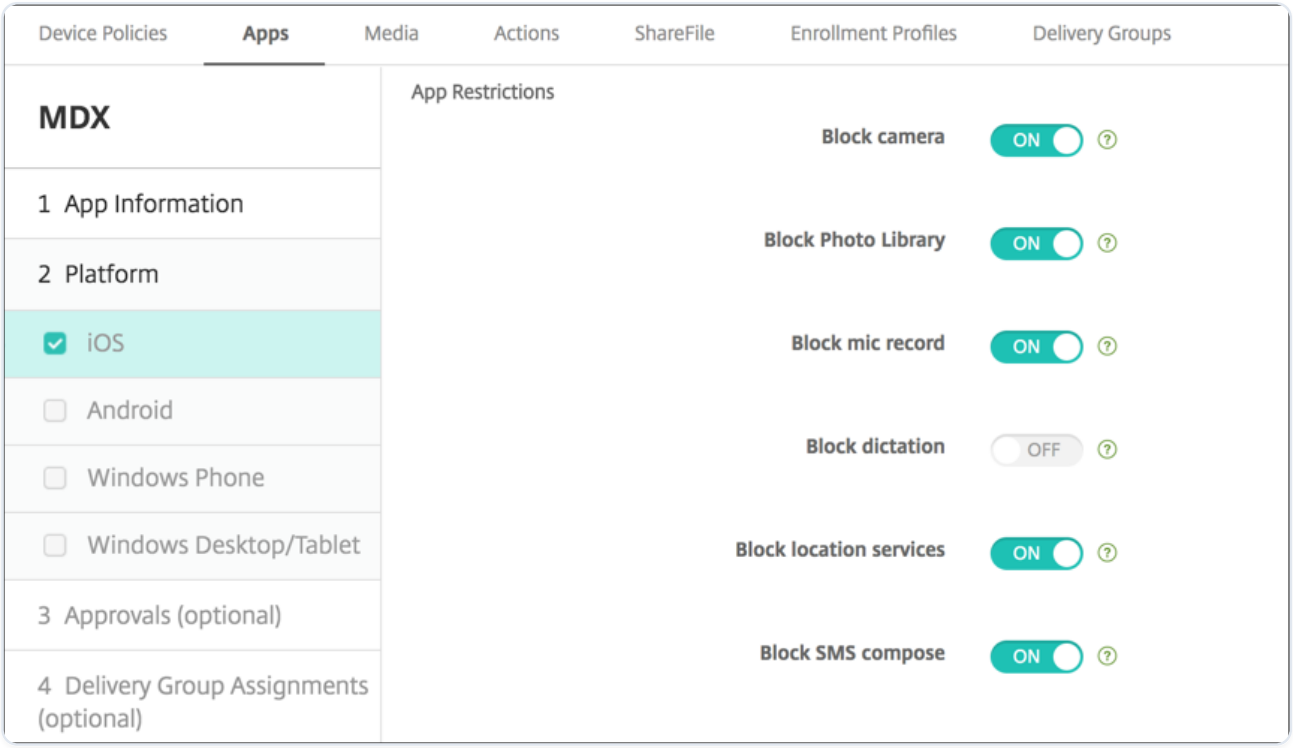
Siriと音声入力のポリシー

ユーザーが管理対象のiOSデバイスでSiriに質問したり、テキストを音声入力したりすると、AppleはSiriの改善のために音声データを収集します。音声データはAppleのクラウドベースサービスを経由するため、セキュアなCitrix Endpoint Managementコンテナの外部に存在します。ただし、音声入力によって生成されたテキストはコンテナ内に残ります。

Citrix Endpoint Managementでは、セキュリティ要件に応じてSiriおよび音声入力サービスをブロックできます。

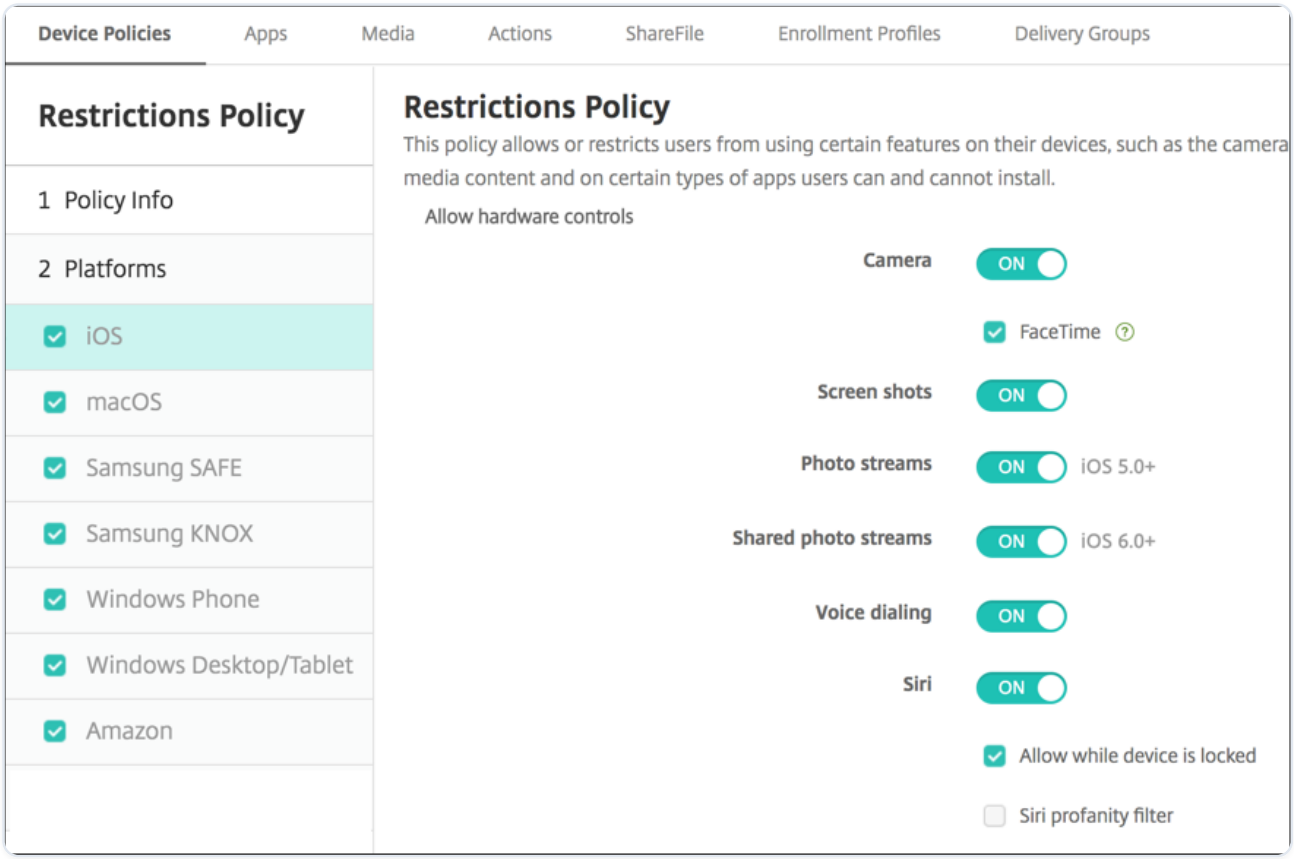
© 1997–2026 Citrix Systems, Inc. All rights reserved.

MAM展開では、各アプリの**音声入力のブロック**ポリシーはデフォルトで**オン**になっており、デバイスのマイクが無効になります。音声入力を許可する場合は、**オフ**に設定します。このポリシーは、Citrix Endpoint Managementコンソールの**構成 > アプリ**で確認できます。アプリを選択し、**編集**をクリックしてから、**iOS**をクリックします。



MDM展開では、**構成 > デバイスポリシー**にあるSiriポリシーを使用してSiriを無効にすることもできます。Siriの使用はデフォルトで許可されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Siriと音声入力を許可するかどうかを決定する際に留意すべき点がいくつかあります。

- Appleが公開している情報によると、AppleはSiriと音声入力の音声クリップデータを最大2年間保持します。データにはユーザーを表すランダムな番号が割り当てられ、音声ファイルはこのランダムな番号に関連付けられます。
- Appleのプライバシーポリシーは、任意のiOSデバイスで**設定 > 一般 > キーボード**に移動し、**音声入力を有効にする**の下にあるリンクをタップすることで確認できます。

SSOアカウントデバイスポリシー

SSOアカウントデバイスポリシーを使用すると、Citrix Endpoint Managementでシングルサインオン (SSO) アカウントを作成できます。これらのアカウントにより、ユーザーは一度サインオンするだけで、さまざまなアプリからCitrix Endpoint Managementおよび社内リソースにアクセスできます。ユーザーはデバイスに資格情報を保存する必要はありません。SSOアカウントのエンタープライズユーザー資格情報は、App Storeのアプリを含む、複数のアプリで利用されます。このポリシーは、Kerberos認証バックエンドと連携するように設計されています。

このポリシーを追加または構成するには、 > の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定

- **アカウント名:** ユーザーのデバイスに表示されるKerberos SSOアカウント名を入力します。このフィールドは必須です。
- **Kerberosプリンシパル名:** Kerberosプリンシパル名を入力します。このフィールドは必須です。
- **ID資格情報 (キーストアまたはPKI資格情報):** ドロップダウンリストから、ユーザーの操作なしでKerberos資格情報を更新するために使用できるオプションのID資格情報をクリックします。
- **Kerberosレルム:** このポリシーのKerberosレルムを入力します。この値は通常、すべて大文字のドメイン名です (例: EXAMPLE.COM)。このフィールドは必須です。
- **許可されるURL:** SSOを必須にする各URLについて、 をクリックし、次の操作を行います。
  - **許可されるURL:** ユーザーがiOSデバイスからURLにアクセスしたときにSSOを必須にするURLを入力します。

    たとえば、ユーザーがサイトを閲覧しようとして、WebサイトがKerberosチャレンジを開始した場合、そのサイトがURLリストにない場合、iOSデバイスは、以前のKerberosログオンからデバイスにキャッシュされている可能性のあるKerberosトークンを提供してSSOを試行しません。URLのホスト部分は完全に一致する必要があります。たとえば、`https://shopping.apple.com` は有効ですが、`https://*.apple.com` は無効です。

    また、ホストの一致に基づいてKerberosがアクティブ化されていない場合でも、URLは標準のHTTP呼び出しにフォールバックします。これは、標準のパスワードチャレンジや、URLがKerberosを使用したSSOのみに構成されている場合のHTTPエラーなど、ほぼすべてのことを意味する可能性があります。
  - をクリックしてURLを追加するか、 をクリックしてURLの追加をキャンセルします。
- **アプリ識別子:** このログインの使用が許可されている各アプリについて、 をクリックし、次の操作を行います。
  - **アプリ識別子:** このログインの使用が許可されているアプリのアプリ識別子を入力します。アプリ識別子を追加しない場合、このログインは**すべて**のアプリ識別子に一致します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

ストアデバイスポリシー

Citrix Endpoint Managementでポリシーを作成し、デバイスがホーム画面にアプリストアのWebクリップを表示するかどうかを指定できます。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「」(/ja-jp/citrix-endpoint-management/policies.html)を参照してください。

iOS、Android、およびWindowsデスクトップ/タブレットの設定

構成する各プラットフォームについて、アプリストアのWebクリップがユーザーデバイスに表示されるかどうかを選択します。デフォルトは**オン**です。

購読済みカレンダーデバイスポリシー

Citrix Endpoint Managementでデバイスポリシーを追加して、iOSデバイスのカレンダーリストに購読済みカレンダーを追加できます。購読できる公開カレンダーのリストは、Appleサポートサイトのダウンロードで入手できます。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

前提条件

ユーザーデバイスの購読済みカレンダーリストに追加する前に、カレンダーを購読している必要があります。

iOS設定

- **説明:** カレンダーの説明を入力します。このフィールドは必須です。
- **URL:** カレンダーのURLを入力します。`webcal://` URLまたはiCalendarファイル (.ics) への `https://` リンクを入力できます。このフィールドは必須です。
- **ユーザー名:** ユーザーのログオン名を入力します。このフィールドは必須です。
- **パスワード:** オプションのユーザーパスワードを入力します。
- **SSLを使用:** カレンダーへのSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは**オフ**です。
- **ポリシー設定**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、 と です。
  - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
  - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を入力します。iOS 6.0以降でのみ利用可能です。

利用規約デバイスポリシー

企業ネットワークへの接続を管理する会社の特定のポリシーをユーザーに承諾させたい場合、Citrix Endpoint Management で利用規約デバイスポリシーを作成します。ユーザーがデバイスを Citrix Endpoint Management に登録する際、利用規約が表示され、デバイスを登録するにはそれらを受け入れる必要があります。利用規約を拒否すると、登録プロセスはキャンセルされます。

会社に国際的なユーザーがいて、彼らが母国語で利用規約を受け入れることを望む場合、異なる言語で利用規約のポリシーを作成できます。展開を計画しているプラットフォームと言語の組み合わせごとにファイルを提供する必要があります。Android および iOS デバイスの場合、PDF ファイルを提供する必要があります。Windows デバイスの場合、テキスト (.txt) ファイルと付随する画像ファイルを提供する必要があります。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS および Android の設定

- **インポートするファイル:** をクリックしてファイルの場所へ移動し、インポートする利用規約ファイルを選択します。
- **デフォルトの利用規約:** このファイルが、異なる利用規約を持つ複数のグループのメンバーであるユーザーのデフォルトドキュメントであるかどうかを選択します。デフォルトは です。

注:

デバイス登録プログラム (DEP) を介して iOS デバイスが登録されている場合、利用規約は表示されません。

Windows タブレットの設定

- **インポートするファイル:** をクリックしてファイルの場所へ移動し、インポートする利用規約ファイルを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **画像:** をクリックしてファイルの場所へ移動し、インポートする画像ファイルを選択します。
- **デフォルトの利用規約:** このファイルが、異なる利用規約を持つ複数のグループのメンバーであるユーザーのデフォルトドキュメントであるかどうかを選択します。デフォルトは です。

トンネルデバイスポリシー

アプリケーショントンネル（アプリトンネル）は、モバイルアプリのサービス継続性とデータ転送の信頼性を向上させるように設計されています。アプリトンネルは、モバイルデバイスアプリのクライアントコンポーネントとアプリサーバーコンポーネント間のプロキシパラメータを定義します。Androidデバイスのトンネルポリシーを構成できます。

このポリシーで定義したトンネルを介して送信されるアプリトラフィックはすべて、アプリを実行しているサーバーにリダイレクトされる前に、Citrix Endpoint Management を経由します。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

Android設定

デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/device-policy-tunnel-android.png)

- **接続開始元:** 接続を開始するソースを指定するには、 または をクリックします。
- **デバイスあたりの最大接続数:** アプリが確立できる同時TCP接続の数を指定する数値を入力します。このフィールドは、デバイスが開始する接続にのみ適用されます。
- **接続タイムアウトの定義:** トンネルが閉じられるまでにアプリがアイドル状態になる時間を設定するかどうかを選択します。
    - **接続タイムアウト:** を に設定した場合、トンネルが閉じられるまでにアプリがアイドル状態になる秒数を入力します。
- **このトンネルを通過する携帯電話接続をブロックする:** ローミング中にこのトンネルがブロックされるかどうかを選択します。Wi-FiおよびUSB接続はブロックされません。
- **クライアントポート:** クライアントポート番号を入力します。通常、この値はサーバーポートと同じです。
- **IPアドレスまたはサーバー名:** アプリサーバーのIPアドレスまたは名前を入力します。このフィールドは、デバイスが開始する接続にのみ適用されます。
- **サーバーポート:** サーバーポート番号を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VPNデバイスポリシー

VPNデバイスポリシーは、ユーザーデバイスが企業リソースに安全に接続できるようにする仮想プライベートネットワーク (VPN) 設定を構成します。以下のプラットフォーム向けにVPNデバイスポリシーを構成できます。各プラットフォームには異なる値のセットが必要であり、それらについてはこの記事で詳しく説明します。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳細については、デバイスポリシーを参照してください。

注：

AndroidおよびiOS版Citrix SSOは、現在Citrix Secure Accessと呼ばれています。この名称変更を反映するために、ドキュメントを更新しています。

アプリごとのVPNの要件

以下のプラットフォーム向けに、VPNポリシーを介してアプリごとのVPN機能を構成します。

- iOS
- macOS
- Android (レガシーDA)

Android Enterpriseの場合、管理対象構成デバイスポリシーを使用してVPNプロファイルを構成します。

アプリごとのVPNオプションは、特定の接続タイプで利用できます。次の表は、アプリごとのVPNオプションが利用可能な場合を示しています。

プラットフォーム	接続タイプ	備考
iOS	シスコ レガシー エニーコネクト、ジュニパー SSL、F5 SSL、ソニックウォール モバイル コネクト、アリバ VIA、シトリックス SSO、またはカスタム SSL。	
macOS	シスコ エニーコネクト、ジュニパー SSL、F5 SSL、ソニックウォール モバイル コ	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プラットフォーム	接続タイプ	備考
	ネクト、アリバ VIA、または カスタム SSL。	
Android (レガシーDA)	シトリックス SSO	

Citrix SSOアプリを使用してiOSおよびAndroid (レガシーDA) デバイス用のアプリごとのVPNを作成するには、VPNポリシーの構成に加えて、追加の手順を実行する必要があります。また、以下の前提条件が満たされていることを確認する必要があります。

- オンプレミスNetScaler Gateway
- 以下のアプリケーションがデバイスにインストールされていること:
  - シトリックス SSO
  - シトリックス セキュア ハブ

Citrix SSOアプリを使用してiOSおよびAndroidデバイス用のアプリごとのVPNを構成する一般的なワークフローは次のとおりです。

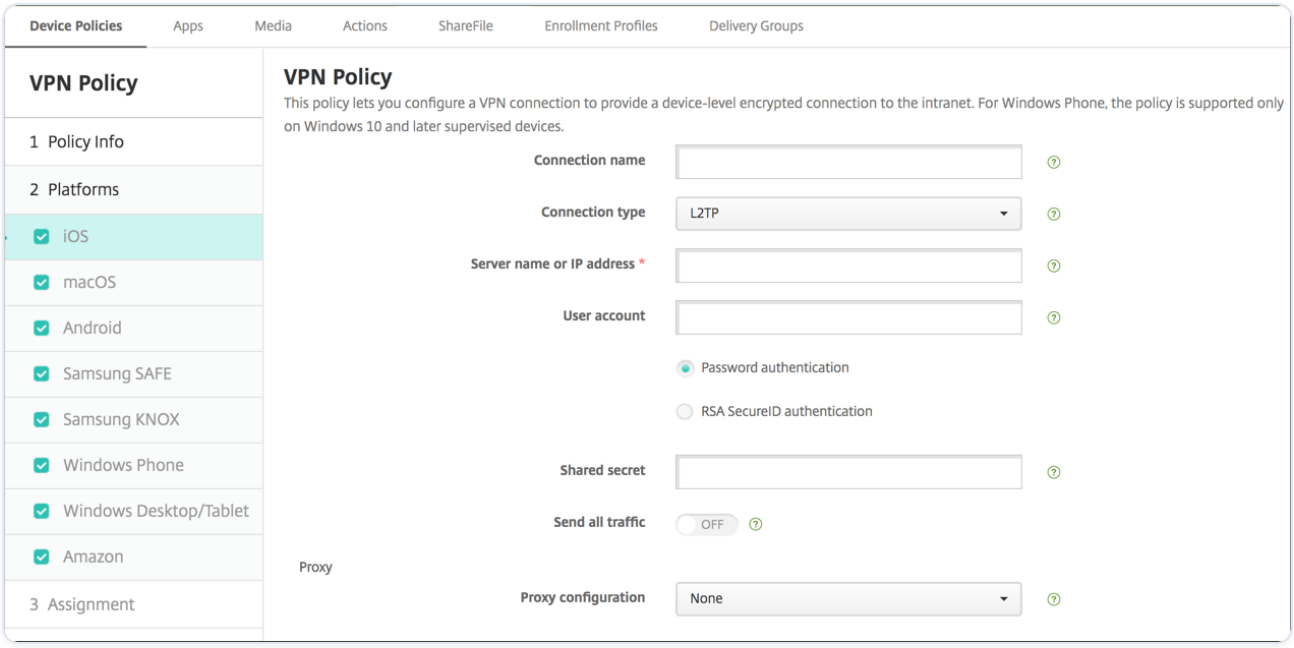
1. この記事で説明されているように、VPNデバイスポリシーを構成します。
   - iOSの場合、iOS向けCitrix SSOプロトコルの構成を参照してください。VPNデバイスポリシーを介してiOS向けCitrix SSOプロトコルを構成した後、アプリをアプリごとのVPNポリシーに関連付けるためにアプリ属性ポリシーも作成する必要があります。詳細については、アプリごとのVPNの構成を参照してください。
     - 「**接続の認証タイプ**」フィールドで「**証明書**」を選択した場合、まずCitrix Endpoint Management向けに証明書ベースの認証を構成する必要があります。クライアント証明書または証明書とドメイン認証を参照してください。
   - Android (レガシーDA) の場合は、Citrix SSO プロトコルを Android 用に構成する を参照してください。
     - **接続の認証タイプ**フィールドで、**証明書**または**パスワードと証明書**を選択した場合、まずCitrix Endpoint Managementの証明書ベースの認証を構成する必要があります。クライアント証明書または証明書とドメイン認証 を参照してください。
2. アプリごとのVPNからのトラフィックを受け入れるようにCitrix ADCを構成します。詳細については、NetScaler Gatewayでの完全なVPNセットアップ を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS設定

iOS用VPNデバイスポリシーのCitrix VPN接続タイプはiOS 12をサポートしていません。既存のVPNデバイスポリシーを削除し、Citrix SSO接続タイプでVPNデバイスポリシーを作成するには、次の手順を実行します。

1. iOS用VPNデバイスポリシーを削除します。
2. 次の設定でiOS用VPNデバイスポリシーを追加します。
    - **接続タイプ: Citrix SSO**
    - **アプリごとのVPNを有効にする: オン**
    - **プロバイダータイプ: パケットトンネル**
3. iOS用アプリ属性デバイスポリシーを追加します。**アプリごとのVPN識別子**には、**iOS_VPN**を選択します。



- **接続名:** 接続の名前を入力します。
- **接続タイプ:** リストから、この接続に使用するプロトコルを選択します。デフォルトは**L2TP**です。
    - **L2TP:** 事前共有キー認証を使用するレイヤー2トンネリングプロトコル。
    - **PPTP:** ポイントツーポイントトンネリング。
    - **IPSec:** 企業のVPN接続。
    - **Cisco Legacy AnyConnect:** この接続タイプでは、ユーザーデバイスにCisco Legacy AnyConnect VPNクライアントがインストールされている必要があります。シスコは、現

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在非推奨となっているVPNフレームワークに基づいていたCisco Legacy AnyConnectクライアントを段階的に廃止しています。

現在のCisco AnyConnectクライアントを使用するには、**接続タイプ**として**Custom SSL**を使用します。必要な設定については、このセクションの「Custom SSLプロトコルの構成」を参照してください。

- **Juniper SSL:** Juniper Networks SSL VPNクライアント。
- **F5 SSL:** F5 Networks SSL VPNクライアント。
- **SonicWALL Mobile Connect:** iOS用Dell統合VPNクライアント。
- **Ariba VIA:** アリバネットワークスの仮想インターネットアクセス クライアント。
- **IKEv2 (iOS only):** iOS専用のInternet Key Exchangeバージョン2。
- **AlwaysOn IKEv2:** IKEv2を使用した常時接続アクセス。
- **AlwaysOn IKEv2 Dual Configuration:** IKEv2デュアル構成を使用した常時接続アクセス。
- **Citrix SSO:** iOS 12以降用のCitrix SSOクライアント。
- **Custom SSL:** カスタムSecure Socket Layer。この接続タイプは、バンドルIDが**com.cisco.anyconnect**であるCisco AnyConnectクライアントに必要です。**接続名**として**Cisco AnyConnect**を指定します。VPNポリシーを展開し、iOSデバイスのネットワークアクセスコントロール（NAC）フィルターを有効にすることもできます。このフィルターは、非準拠アプリがインストールされているデバイスのVPN接続をブロックします。この構成には、以下のiOSセクションで説明されているように、iOS VPNポリシーの特定の設定が必要です。NACフィルターを有効にするために必要なその他の設定の詳細については、「ネットワークアクセスコントロール」を参照してください。

以下のセクションでは、上記の各接続タイプの構成オプションを一覧表示します。

iOS用L2TPプロトコルの構成

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **パスワード認証**または**RSA SecurID認証**のいずれかを選択します。
- **共有シークレット:** IPsec共有シークレットキーを入力します。
- **すべてのトラフィックを送信:** VPN経由ですべてのトラフィックを送信するかどうかを選択します。デフォルトは**オフ**です。

iOS用PPTPプロトコルの構成

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **パスワード認証**または**RSA SecurID認証**のいずれかを選択します。
- **暗号化レベル:** リストから暗号化レベルを選択します。デフォルトは**なし**です。
  - **なし:** 暗号化を使用しません。
  - **自動:** サーバーでサポートされている最も強力な暗号化レベルを使用します。
  - **最大 (128ビット):** 常に128ビット暗号化を使用します。
- **すべてのトラフィックを送信:** VPN経由ですべてのトラフィックを送信するかどうかを選択します。デフォルトは**オフ**です。

iOS用IPsecプロトコルの構成

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**共有シークレット**または**証明書**のいずれかを選択します。デフォルトは**共有シークレット**です。
- **共有シークレット**を有効にする場合は、以下の設定を構成します。
  - **グループ名:** オプションのグループ名を入力します。
  - **共有シークレット:** オプションの共有シークレットキーを入力します。
  - **ハイブリッド認証を使用:** ハイブリッド認証を使用するかどうかを選択します。ハイブリッド認証では、まずサーバーがクライアントに対して認証を行い、次にクライアントがサーバーに対して認証を行います。デフォルトは**オフ**です。
  - **パスワードの入力を求める:** ユーザーがネットワークに接続する際にパスワードの入力を求めるかどうかを選択します。デフォルトは**オフ**です。
- **証明書**を有効にする場合は、以下の設定を構成します。
  - **ID資格情報:** リストから、使用するID資格情報を選択します。デフォルトは**なし**です。
  - **接続時にPINの入力を求める:** ユーザーがネットワークに接続する際にPINの入力を要求するかどうかを選択します。デフォルトは**オフ**です。
  - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「iOS向けVPNオンデマンド設定の構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。
- **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされたアプリがネットワーク通信を開始したときに、アプリごとのVPN接続が自動的にトリガーされるかどうかを選択します。デフォルトは**オフ**です。
- **Safariドメイン: 追加**をクリックしてSafariドメイン名を追加します。

iOS 用 Cisco レガシー AnyConnect プロトコルの構成

Cisco レガシー AnyConnect クライアントから新しい Cisco AnyConnect クライアントに移行するには、カスタム SSL プロトコルを使用します。

- **プロバイダーバンドル識別子:** レガシー AnyConnect クライアントの場合、バンドル ID は com.cisco.anyconnect.gui です。
- **サーバー名または IP アドレス:** VPN サーバーのサーバー名または IP アドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **グループ:** オプションのグループ名を入力します。
- **接続の認証タイプ:** この接続の認証タイプとして、リストから または を選択します。デフォルトは です。
  - を有効にする場合は、 フィールドにオプションの認証パスワードを入力します。
  - を有効にする場合は、次の設定を構成します。
    - **ID 資格情報:** リストから使用する ID 資格情報を選択します。デフォルトは です。
    - **接続時に PIN の入力を求める:** ユーザーがネットワークに接続するときに PIN の入力を求めるかどうかを選択します。デフォルトは です。
    - **VPN オンデマンドを有効にする:** ユーザーがネットワークに接続したときに VPN 接続をトリガーすることを有効にするかどうかを選択します。デフォルトは です。 が の場合の設定の構成については、「iOS 用の VPN オンデマンド設定の有効化を構成する」を参照してください。
- **すべてのネットワークを含める:** すべてのネットワークでこの接続を使用できるようにするかどうかを選択します。デフォルトは です。
- **ローカルネットワークを除外する:** ローカルネットワークを接続の使用から除外するか、ネットワークを許可するかを選択します。デフォルトは です。
- **アプリごとの VPN を有効にする:** アプリごとの VPN を有効にするかどうかを選択します。デフォルトは です。このオプションを有効にする場合は、次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされたアプリがネットワーク通信を開始したときに、アプリごとのVPN接続を自動的にトリガーするかどうかを選択します。デフォルトは**オフ**です。
- **プロバイダーの種類:** アプリごとのVPNを**アプリプロキシ**として提供するか、**パケットトンネル**として提供するかを選択します。デフォルトは**アプリプロキシ**です。
- **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして以下を実行します。
  - **ドメイン:** 追加するドメインを入力します。
  - **保存**をクリックしてドメインを保存するか、**キャンセル**をクリックしてドメインを保存しないようにします。

iOS 用の Juniper SSL プロトコルを構成する

- **プロバイダーバンドル識別子:** アプリごとのVPNプロファイルに、同じ種類の複数のVPNプロバイダーを持つアプリのバンドル識別子がある場合は、ここで使用するプロバイダーを指定します。
- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **レルム:** オプションのレルム名を入力します。
- **ロール:** オプションのロール名を入力します。
- **接続の認証タイプ:** この接続の認証タイプとして、リストから**パスワード**または**証明書**のいずれかを選択します。デフォルトは**パスワード**です。
- **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
- **証明書**を有効にする場合は、次の設定を構成します。
  - **識別情報:** 使用する識別情報をリストから選択します。デフォルトは**なし**です。
  - **接続時にPINを要求:** ユーザーがネットワークに接続する際にPINを要求するかどうかを選択します。デフォルトは**オフ**です。
  - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「iOS向けVPNオンデマンド設定の構成」を参照してください。
  - **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションを有効にする場合は、以下の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされたアプリがネットワーク通信を開始したときに、アプリごとのVPN接続を自動的にトリガーするかどうかを選択します。デフォルトは**オフ**です。
- **プロバイダーの種類:** アプリごとのVPNを**アプリプロキシ**として提供するか、**パケットトンネル**として提供するかを選択します。デフォルトは**アプリプロキシ**です。
- **Safariドメイン:** アプリごとのVPN接続をトリガーできるSafariドメインごとに、**追加**をクリックして以下を実行します。
- **ドメイン:** 追加するドメインを入力します。

- **保存**をクリックしてドメインを保存するか、**キャンセル**をクリックしてドメインを保存しないようにします。

iOS向けF5 SSLプロトコルの構成

- **プロバイダーバンドル識別子:** アプリごとのVPNプロファイルに、同じ種類の複数のVPNプロバイダーを持つアプリのバンドル識別子がある場合は、ここで使用するプロバイダーを指定します。
- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **接続の認証の種類:** この接続の認証の種類として、リストから**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にする場合は、以下の設定を構成します。
    - **識別情報資格情報:** リストから、使用する識別情報資格情報を選択します。デフォルトは**なし**です。
    - **接続時にPINの入力を求める:** ユーザーがネットワークに接続するときにPINの入力を求めるかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「iOS向けVPNオンデマンド設定の構成」を参照してください。
- **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションを有効にする場合は、次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとのVPN接続を自動的にトリガーするかどうかを選択します。
- **プロバイダーの種類:** アプリごとのVPNが**アプリプロキシ**として提供されるか、**パケットトンネル**として提供されるかを選択します。デフォルトは**アプリプロキシ**です。
- **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして、次の操作を行います。
  - **ドメイン:** 追加するドメインを入力します。
  - **保存**をクリックしてドメインを保存するか、**キャンセル**をクリックしてドメインを保存しないようにします。

iOS向けSonicWALLプロトコルの構成

- **プロバイダーバンドル識別子:** アプリごとのVPNプロファイルに、同じ種類の複数のVPNプロバイダーを持つアプリのバンドル識別子がある場合は、ここで使用するプロバイダーを指定します。
- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **ログオングループまたはドメイン:** オプションのログオングループまたはドメインを入力します。
- **接続の認証の種類:** リストから、この接続の認証の種類として**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。
  - 「**パスワード**」を有効にする場合、「**認証パスワード**」フィールドにオプションの認証パスワードを入力します。
  - 「**証明書**」を有効にする場合、以下の設定を構成します。
    - **ID資格情報:** リストから使用するID資格情報を選択します。デフォルトは**なし**です。
    - **接続時にPINを要求:** ユーザーがネットワークに接続する際にPINを要求するかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。「**VPNオンデマンドを有効にする**」が**オン**の場合の設定については、「iOS向けVPNオンデマンド設定を構成する」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションをオンに設定した場合、以下の設定を構成します。
  - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされたアプリがネットワーク通信を開始したときに、アプリごとのVPN接続が自動的にトリガーされるようにするかどうかを選択します。
  - **プロバイダーの種類:** アプリごとのVPNが**アプリプロキシ**として提供されるか、**パケットトンネル**として提供されるかを選択します。デフォルトは**アプリプロキシ**です。
  - **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして以下を実行します。
    - **ドメイン:** 追加するドメインを入力します。
    - ドメインを保存するには**保存**をクリックし、保存しない場合は**キャンセル**をクリックします。

iOS向けAriba VIAプロトコルを構成する

- **プロバイダーバンドル識別子:** アプリごとのVPNプロファイルに、同じ種類の複数のVPNプロバイダーを持つアプリのバンドル識別子がある場合、ここで使用するプロバイダーを指定します。
- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**パスワード**または**証明書**のいずれかを選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にする場合は、以下の設定を構成します。
    - **ID資格情報:** リストから、使用するID資格情報を選択します。デフォルトは**なし**です。
    - **接続時にPINを要求:** ユーザーがネットワークに接続する際にPINを要求するかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「iOS向けVPNオンデマンド設定を構成する」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションを有効にする場合は、以下の設定を構成します。
  - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされたアプリがネットワーク通信を開始したときに、アプリごとのVPN接続が自動的にトリガーされるかどうかを選択します。
  - **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして以下を実行します。
    - **ドメイン:** 追加するドメインを入力します。
    - ドメインを保存するには**保存**をクリックし、保存しない場合は**キャンセル**をクリックします。

iOS向けIKEv2プロトコルの構成

このセクションには、IKEv2、Always On IKEv2、およびAlways On IKEv2 Dual Configurationプロトコルで使用される設定が含まれています。Always On IKEv2 Dual Configurationプロトコルの場合、これらの設定はすべてセルラーネットワークとWi-Fiネットワークの両方に対して構成します。

- **ユーザーによる自動接続の無効化を許可:** Always Onプロトコル用。ユーザーがデバイスでネットワークへの自動接続を無効にすることを許可するかどうかを選択します。デフォルトは**オフ**です。
- **サーバーのホスト名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ローカル識別子 (Local Identifier):** IKEv2クライアントのFQDNまたはIPアドレス。このフィールドは必須です。
- **リモート識別子 (Remote Identifier):** VPNサーバーのFQDNまたはIPアドレス。このフィールドは必須です。
- **デバイス認証 (Device Authentication):** この接続の認証タイプとして、**共有シークレット (Shared Secret)**、**証明書 (Certificate)**、または**デバイス識別子に基づくデバイス証明書 (Device Certificate Based on Device Identifier)** を選択します。デフォルトは**共有シークレット (Shared Secret)** です。
  - **共有シークレット (Shared Secret)** を選択した場合は、オプションの共有シークレットキーを入力します。
  - **証明書 (Certificate)** を選択した場合は、使用する**ID資格情報 (Identity credential)** を選択します。デフォルトは**なし (None)** です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **デバイス識別子に基づくデバイス証明書 (Device Certificate Based on Device Identifier)** を選択した場合は、使用する**デバイスIDタイプ (Device identity type)** を選択します。デフォルトは**IMEI**です。このオプションを使用するには、REST APIを使用して証明書を一括インポートします。「REST APIを使用した証明書の一括アップロード」を参照してください。**Always On IKEv2**を選択した場合にのみ利用可能です。

- **拡張認証を有効にする (Extended Authentication Enabled):** 拡張認証プロトコル (EAP) を有効にするかどうかを選択します。**オン (On)** の場合は、**ユーザーアカウント (User account)** と **認証パスワード (Authentication password)** を入力します。
- **Dead Peer Detection間隔 (Dead Peer Detection Interval):** ピアデバイスが到達可能であることを確認するために、ピアデバイスにどのくらいの頻度で連絡するかを選択します。デフォルトは**なし (None)** です。オプションは次のとおりです。
  - **なし (None):** Dead Peer Detectionを無効にします。
  - **低 (Low):** 30分ごとにピアに連絡します。
  - **中 (Medium):** 10分ごとにピアに連絡します。
  - **高 (High):** 1分ごとにピアに連絡します。
- **モビリティとマルチホーミングを無効にする (Disable Mobility and Multihoming):** この機能を無効にするかどうかを選択します。
- **IPv4/IPv6内部サブネット属性を使用する (Use IPv4/IPv6 internal subnet attributes):** この機能を有効にするかどうかを選択します。
- **リダイレクトを無効にする (Disable redirects):** リダイレクトを無効にするかどうかを選択します。
- **フォールバックを有効にする:** 有効にすると、この設定により、Wi-Fiアシストの対象となり、VPNを必要とするトラフィックをセルラーデータ経由でトンネルが伝送できるようになります。デフォルトは**オフ**です。
- **デバイスがスリープ状態のときにNATキープアライブを有効にする:** Always Onプロトコル用です。キープアライブパケットは、IKEv2接続のNATマッピングを維持します。デバイスが起動しているとき、チップはこれらのパケットを定期的に送信します。この設定がオンの場合、デバイスがスリープ状態であってもチップはキープアライブパケットを送信します。デフォルトの間隔は、Wi-Fi経由で20秒、セルラー経由で110秒です。NATキープアライブ間隔パラメーターを使用して間隔を変更できます。
- **NATキープアライブ間隔 (秒):** デフォルトは20秒です。
- **Perfect Forward Secrecyを有効にする:** この機能を有効にするかどうかを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **DNSサーバーIPアドレス:** オプション。DNSサーバーIPアドレス文字列のリストです。これらのIPアドレスには、IPv4アドレスとIPv6アドレスが混在していてもかまいません。**追加**をクリックしてアドレスを入力します。
- **ドメイン名:** オプション。トンネルのプライマリドメインです。
- **検索ドメイン:** オプション。単一ラベルのホスト名を完全に修飾するために使用されるドメイン文字列のリストです。
- **補足一致ドメインをリゾルバーのリストに追加する:** オプション。補足一致ドメインリストをリゾルバーの検索ドメインリストに追加するかどうかを決定します。デフォルトは**オン**です。
- **補足一致ドメイン:** オプション。DNSサーバーアドレスにあるDNSリゾルバー設定を使用するDNSクエリを決定するために使用されるドメイン文字列のリストです。このキーは、特定のドメイン内のホストのみがトンネルのDNSリゾルバーを使用して解決されるスプリットDNS構成を作成します。このリストのドメインのいずれにも含まれないホストは、システムのデフォルトリゾルバーを使用して解決されます。

このパラメーターが空の文字列の場合、その文字列がデフォルトドメインになります。その結果、スプリットトンネル構成は、プライマリDNSサーバーの前にすべてのDNSクエリをVPN DNSサーバーに転送できます。VPNトンネルがネットワークのデフォルトルートである場合、リストされたDNSサーバーがデフォルトのリゾルバーになります。その場合、補足一致ドメインリストは無視されます。

- **IKE SAパラメーター**と**子SAパラメーター:** 各セキュリティアソシエーション (SA) パラメーターオプションについて、これらの設定を構成します。
  - **暗号化アルゴリズム:** リストから、使用するIKE暗号化アルゴリズムを選択します。デフォルトは**3DES**です。
  - **整合性アルゴリズム:** リストから、使用する整合性アルゴリズムを選択します。デフォルトは**SHA-256**です。
  - **Diffie Hellmanグループ:** リストから、Diffie Hellmanグループ番号を選択します。デフォルトは**2**です。
  - **IKEライフタイム (分):** SAライフタイム (再キー間隔) を表す10から1440までの整数を入力します。デフォルトは**1440**分です。
- **サービス例外:** Always Onプロトコル用です。サービス例外は、Always On VPNの対象外となるシステムサービスです。これらのサービス例外設定を構成します。
  - **ボイスメール:** リストから、ボイスメール例外の処理方法を選択します。デフォルトは**トンネル経由のトラフィックを許可**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **AirPrint:** リストから、AirPrint例外の処理方法を選択します。デフォルトは**トンネル経由のトラフィックを許可**です。
- **VPNトンネル外のキャプティブWebシートからのトラフィックを許可:** ユーザーがVPNトンネル外のパブリックホットスポットに接続することを許可するかどうかを選択します。デフォルトは**オフ**です。
- **VPNトンネル外のすべてのキャプティブネットワークアプリからのトラフィックを許可:** VPNトンネル外のすべてのホットスポットネットワークアプリを許可するかどうかを選択します。デフォルトは**オフ**です。
- **キャプティブネットワークアプリのバンドル識別子:** ユーザーがアクセスを許可されているホットスポットネットワークアプリのバンドル識別子ごとに、**追加**をクリックし、ホットスポットネットワークアプリの**バンドル識別子**を入力します。アプリのバンドル識別子を保存するには、**保存**をクリックします。

- **アプリごとのVPN:** IKEv2接続タイプに対してこれらの設定を構成します。
  - **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。
  - **オンデマンド一致アプリが有効:** アプリごとのVPNサービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとのVPN接続を自動的にトリガーするかどうかを選択します。デフォルトは**オフ**です。
  - **Safariドメイン: 追加**をクリックしてSafariドメイン名を追加します。
- **プロキシ構成:** VPN接続がプロキシサーバー経由でルーティングされる方法を選択します。デフォルトは**なし**です。

iOS向けCitrix SSOプロトコルの構成

Citrix SSOクライアントはApple Storeで入手できます。

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にする場合は、次の設定を構成します。
    - **ID資格情報:** リストから、使用するID資格情報を選択します。デフォルトは**なし**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **接続時にPINの入力を求める:** ユーザーがネットワークに接続するときにPINの入力を求めるかどうかを選択します。デフォルトは**オフ**です。
  - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続のトリガーを有効にするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定の構成については、「iOS向けVPNオンデマンド設定の構成」を参照してください。

- **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションをオンに設定する場合は、次の設定を構成します。
  - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとのVPN接続が自動的にトリガーされるかどうかを選択します。
  - **プロバイダーの種類:** アプリごとのVPNが**アプリプロキシ**として提供されるか、**パケットトンネル**として提供されるかを選択します。デフォルトは**アプリプロキシ**です。
  - **プロバイダーの種類: パケットトンネル**に設定します。
  - **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできるSafariドメインごとに、**追加**をクリックして次の操作を行います。
    - **ドメイン:** 追加するドメインを入力します。
    - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。

- **カスタムXML:** 追加するカスタムXMLパラメーターごとに、**追加**をクリックしてキーと値のペアを指定します。使用可能なパラメーターは次のとおりです。
  - **disableL3:** システムレベルのVPNを無効にします。アプリごとのVPNのみを許可します。**値**は不要です。
  - **ユーザーエージェント：** このデバイスポリシーを、VPNプラグインクライアントをターゲットとするNetScaler Gatewayポリシーに関連付けます。プラグインによって開始された要求の場合、このキーの**値**はVPNプラグインに自動的に追加されます。

iOS用のカスタムSSLプロトコルを構成する

Cisco Legacy AnyConnectクライアントからCisco AnyConnectクライアントへ移行するには：

1. カスタムSSLプロトコルでVPNデバイスポリシーを構成します。そのポリシーをiOSデバイスに展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. `<https://apps.apple.com/us/app/cisco-secure-client/id1135064690>`からCisco AnyConnectクライアントをアップロードし、アプリをCitrix Endpoint Managementに追加し、その後、アプリをiOSデバイスに展開します。
3. 古いVPNデバイスポリシーをiOSデバイスから削除します。

設定：

- **カスタムSSL識別子（逆引きDNS形式）：** バンドル識別子に設定します。Cisco AnyConnectクライアントの場合は、**com.cisco.anyconnect**を使用します。
- **プロバイダーバンドル識別子： カスタムSSL識別子**で指定されたアプリに、同じタイプ（アプリプロキシまたはパケットトンネル）の複数のVPNプロバイダーがある場合は、このバンドル識別子を指定します。Cisco AnyConnectクライアントの場合は、**com.cisco.anyconnect**を使用します。
- **サーバー名またはIPアドレス：** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント：** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ：** この接続の認証タイプとして、リストから**パスワード**または**証明書**のいずれかを選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にした場合、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にした場合、これらの設定を構成します。
    - **ID資格情報：** リストから使用するID資格情報を選択します。デフォルトは**なし**です。
    - **接続時にPINを要求:** ユーザーがネットワークに接続する際にPINを要求するかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定構成については、「iOS向けVPNオンデマンド設定の構成」を参照してください。
- **すべてのネットワークを含める:** すべてのネットワークがこの接続を使用できるようにするかどうかを選択します。デフォルトは**オフ**です。
- **ローカルネットワークを除外する:** ローカルネットワークが接続を使用しないようにするか、または使用できるようにするかを選択します。デフォルトは**オフ**です。
- **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションをオンに設定した場合、次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとのVPN接続が自動的にトリガーされるようにするかどうかを選択します。
- **プロバイダーの種類:** プロバイダーの種類は、プロバイダーがVPNサービスであるかプロキシサービスであるかを示します。VPNサービスの場合は、**パケットトンネル**を選択します。プロキシサービスの場合は、**アプリプロキシ**を選択します。Cisco AnyConnectクライアントの場合は、**パケットトンネル**を選択します。
- **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできるSafariドメインごとに、**追加**をクリックして、次の操作を行います。
  - **ドメイン:** 追加するドメインを入力します。
  - ドメインを保存するには**保存**をクリックし、保存しない場合は**キャンセル**をクリックします。

- **カスタムXML:** 追加するカスタムXMLパラメーターごとに、**追加**をクリックして、次の操作を行います。
  - **パラメーター名:** 追加するパラメーターの名前を入力します。
  - **値: パラメーター名**に関連付けられている値を入力します。
  - パラメーターを保存するには**保存**をクリックし、保存しない場合は**キャンセル**をクリックします。

NACをサポートするようにVPNデバイスポリシーを構成する

1. NACフィルターを構成するには、**接続タイプ**として**カスタムSSL**が必要です。
2. **接続名**に**VPN**を指定します。
3. **カスタムSSL識別子**には、**com.citrix.NetScalerGateway.ios.app**と入力します。
4. **プロバイダーバンドル識別子**には、**com.citrix.NetScalerGateway.ios.app.vpnplugin**と入力します。

手順3と4の値は、NACフィルタリングに必要なCitrix SSOのインストールから取得されます。認証パスワードは構成しません。NAC機能の使用に関する詳細については、「ネットワークアクセス制御」を参照してください。

iOSのVPNオンデマンドオプションを有効にするように構成する

- **オンデマンドドメイン:** ユーザーが接続したときに実行する各ドメインと関連付けられたアクションについて、**追加**をクリックして、次の操作を行います。
- **ドメイン:** 追加するドメインを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アクション:** リストから可能なアクションのいずれかを選択します。
  - **常に確立:** ドメインは常にVPN接続をトリガーします。
  - **確立しない:** ドメインはVPN接続をトリガーしません。
  - **必要に応じて確立:** ドメイン名解決が失敗した場合、ドメインはVPN接続の試行をトリガーします。失敗は、DNSサーバーがドメインを解決できない場合、別のサーバーにリダイレクトされる場合、またはタイムアウトした場合に発生します。
  - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。
- **オンデマンドルール**
  - **アクション:** リストから実行するアクションを選択します。デフォルトは**EvaluateConnection**です。可能なアクションは次のとおりです。
    - **許可:** トリガーされたときにオンデマンドVPNの接続を許可します。
    - **接続:** 無条件にVPN接続を開始します。
    - **切断:** VPN接続を削除し、ルールが一致する限りオンデマンドで再接続しません。
    - **接続の評価:** 各接続のActionParameters配列を評価します。
    - **無視:** 既存のVPN接続を維持しますが、ルールが一致する限りオンデマンドで再接続しません。
  - **DNSドメインの一致:** デバイスの検索ドメインリストが一致する可能性のある、追加したい各ドメインについて、**追加**をクリックして以下を実行します。
    - **DNSドメイン:** ドメイン名を入力します。複数のドメインに一致させるには、ワイルドカード「*」プレフィックスを使用できます。たとえば、*.example.comはmydomain.example.com、yourdomain.example.com、およびherdomain.example.comに一致します。
    - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。
  - **DNSサーバーアドレスの一致:** ネットワークの指定されたDNSサーバーのいずれかが一致する可能性のある、追加したい各IPアドレスについて、**追加**をクリックして以下を実行します。
    - **DNSサーバーアドレス:** 追加したいDNSサーバーアドレスを入力します。DNSサーバーに一致させるには、ワイルドカード「*」サフィックスを使用できます。たとえば、17.*はクラスAサブネット内の任意のDNSサーバーに一致します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - DNSサーバーアドレスを保存するには**保存**をクリックし、DNSサーバーアドレスを保存しない場合は**キャンセル**をクリックします。

- **インターフェースタイプの一致:** リストで、使用中のプライマリネットワークインターフェースハードウェアのタイプを選択します。デフォルトは**指定なし**です。可能な値は次のとおりです。

    - **指定なし:** 任意のネットワークインターフェースハードウェアに一致します。このオプションがデフォルトです。
    - **イーサネット:** イーサネットネットワークインターフェースハードウェアのみに一致します。
    - **Wi-Fi:** Wi-Fiネットワークインターフェースハードウェアのみに一致します。
    - **Cellular:** セルラーネットワークインターフェイスハードウェアのみに一致します。

- **SSIDMatch:** 追加する現在のネットワークと照合する各SSIDについて、**Add** をクリックして以下を実行します。

    - **SSID:** 追加するSSIDを入力します。ネットワークがWi-Fiネットワークでない場合、またはSSIDが表示されない場合、一致は失敗します。任意のSSIDに一致させるには、このリストを空のままにします。
    - **Save** をクリックしてSSIDを保存するか、**Cancel** をクリックしてSSIDを保存しないようにします。

- **URLStringProbe:** 取得するURLを入力します。このURLがリダイレクトなしで正常に取得された場合、このルールは一致します。
- **ActionParameters : Domains:** EvaluateConnectionがチェックする追加したい各ドメインについて、**Add** をクリックして以下を実行します。

    - **Domain:** 追加するドメインを入力します。
    - **Save** をクリックしてドメインを保存するか、**Cancel** をクリックしてドメインを保存しないようにします。

- **ActionParameters : DomainAction:** リストから、指定された **ActionParameters : Domains** ドメインの **VPN behavior** を選択します。デフォルトは **ConnectIfNeeded** です。可能なアクションは次のとおりです。

    - **ConnectIfNeeded:** ドメイン名解決が失敗した場合、ドメインはVPN接続試行をトリガーします。失敗は、DNSサーバーがドメインを解決できない場合、別のサーバーにリダイレクトされる場合、またはタイムアウトした場合に発生します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **NeverConnect:** ドメインはVPN接続をトリガーしません。
  - **Action Parameters: RequiredDNSServers:** 指定されたドメインの解決に使用する各DNSサーバーについて、**Add** をクリックして以下を実行します。
    - **DNS Server: ActionParameters** : **DomainAction** = **ConnectIfNeeded** の場合にのみ有効です。DNSサーバーのIPアドレスを入力します。このサーバーは、デバイスの現在のネットワーク構成の外部にある場合があります。DNSサーバーに到達できない場合、応答としてVPN接続が確立されます。DNSサーバーが内部DNSサーバーまたは信頼できる外部DNSサーバーのいずれかであることを確認してください。
    - **Save** をクリックしてDNSサーバーを保存するか、**Cancel** をクリックしてDNSサーバーを保存しないようにします。
  - **ActionParameters : RequiredURLStringProbe:** オプションで、GETリクエストを使用してプローブするHTTPまたはHTTPS（推奨）URLを入力します。URLのホスト名を解決できない場合、サーバーに到達できない場合、またはサーバーが応答しない場合、VPN接続が確立されます。**ActionParameters** : **DomainAction** = **ConnectIfNeeded** の場合にのみ有効です。
  - **OnDemandRules : XMLコンテンツ:** XML構成オンデマンドルールを入力またはコピーアンドペーストします。
    - XMLコードを検証するには、 をクリックします。XMLが有効な場合、 テキストボックスの下に が表示されます。無効な場合は、エラーメッセージにエラーが記述されます。

- **プロキシ**
  - **プロキシ構成:** リストから、VPN接続がプロキシサーバー経由でルーティングされる方法を選択します。デフォルトは です。
    - を有効にした場合は、次の設定を構成します。
      - **プロキシサーバーのホスト名またはIPアドレス:** プロキシサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
      - **プロキシサーバーのポート:** プロキシサーバーのポート番号を入力します。このフィールドは必須です。
      - **ユーザー名:** オプションのプロキシサーバーユーザー名を入力します。
      - **パスワード:** オプションのプロキシサーバーパスワードを入力します。
    - を構成する場合は、次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **プロキシサーバーURL:** プロキシサーバーのURLを入力します。このフィールドは必須です。

- **ポリシー設定**
    - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、 と です。
        - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
        - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

アプリごとのVPNを構成する

iOSのアプリごとのVPNオプションは、Cisco Legacy AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix VPN、Citrix SSO、Custom SSLの接続タイプで利用できます。

アプリごとのVPNを構成するには:

1. **構成 > デバイスポリシー**で、VPNポリシーを作成します。例:

   デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/configure-device-policies-vpn-per-app-ios-example.png)

   デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/configure-device-policies-vpn-per-app-ios-example2.png)
2. **構成 > デバイスポリシー**で、アプリをアプリごとのVPNポリシーに関連付けるためのアプリ属性ポリシーを作成します。**アプリごとのVPN識別子**には、ステップ1で作成したVPNポリシーの名前を選択します。**管理対象アプリバンドルID**には、アプリリストから選択するか、アプリバンドルIDを入力します。(iOSアプリインベントリポリシーを展開すると、アプリリストにアプリが表示されます。)

   デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/configure-device-policies-app-attributes-per-app.png)

macOS設定

デバイスポリシー構成画面(/en-us/citrix-endpoint-management/media/configure-device-policies-vpn-macos-example.png)

- **接続名:** 接続の名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **接続タイプ:** リストから、この接続に使用するプロトコルを選択します。デフォルトはL2TPです。
  - **L2TP:** 事前共有キー認証を使用するレイヤー2トンネリングプロトコル。
  - **PPTP:** ポイントツーポイントトンネリング。
  - **IPSec:** 会社のVPN接続。
  - **Cisco AnyConnect:** Cisco AnyConnect VPNクライアント。
  - **Juniper SSL:** Juniper Networks SSL VPNクライアント。
  - **F5 SSL:** F5 Networks SSL VPNクライアント。
  - **SonicWALL Mobile Connect:** iOS用Dell統合VPNクライアント。
  - **Ariba VIA:** Ariba Networks 仮想インターネットアクセス クライアント。
  - **Citrix VPN:** Citrix VPNクライアント。
  - **Custom SSL:** カスタム セキュアソケットレイヤー。

以下のセクションでは、上記の各接続タイプの構成オプションを一覧表示します。

macOS用L2TPプロトコルの構成

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **パスワード認証**、**RSA SecurID認証**、**Kerberos認証**、または**CryptoCard認証**を選択します。デフォルトは**パスワード認証**です。
- **共有シークレット:** IPsec共有シークレットキーを入力します。
- **すべてのトラフィックを送信:** すべてのトラフィックをVPN経由で送信するかどうかを選択します。デフォルトは**オフ**です。

macOS用PPTPプロトコルの構成

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **パスワード認証**、**RSA SecurID認証**、**Kerberos認証**、または**CryptoCard認証**を選択します。デフォルトは**パスワード認証**です。
- **暗号化レベル:** 目的の暗号化レベルを選択します。デフォルトは**なし**です。
  - **なし:** 暗号化を使用しません。
  - **自動:** サーバーでサポートされている最も強力な暗号化レベルを使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **最大** (128ビット): 常に128ビット暗号化を使用します。

- **すべてのトラフィックを送信:** すべてのトラフィックをVPN経由で送信するかどうかを選択します。デフォルトは**オフ**です。

macOS 用 IPsec プロトコルを構成する

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**共有シークレット**または**証明書**のいずれかを選択します。デフォルトは**共有シークレット**です。
    - **共有シークレット**認証を有効にする場合は、次の設定を構成します。
        - **グループ名:** オプションのグループ名を入力します。
        - **共有シークレット:** オプションの共有シークレットキーを入力します。
        - **ハイブリッド認証を使用:** ハイブリッド認証を使用するかどうかを選択します。ハイブリッド認証では、まずサーバーがクライアントに対して認証を行い、次にクライアントがサーバーに対して認証を行います。既定値は**オフ**です。
        - **パスワードの入力を求める:** ユーザーがネットワークに接続するときにパスワードの入力を求めるかどうかを選択します。既定値は**オフ**です。
    - **証明書**認証を有効にする場合は、次の設定を構成します。
        - **ID資格情報:** リストから使用するID資格情報を選択します。既定値は**なし**です。
        - **接続時にPINの入力を求める:** ユーザーがネットワークに接続するときにPINの入力を要求するかどうかを選択します。既定値は**オフ**です。
        - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続のトリガーを有効にするかどうかを選択します。既定値は**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定の構成については、「VPNオンデマンドオプションの有効化を構成する」を参照してください。

macOS 用の Cisco AnyConnect プロトコルを構成する

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **グループ:** オプションのグループ名を入力します。
- **接続の認証の種類:** この接続の認証の種類として、リストから**パスワード**または**証明書**のいずれかを選択します。既定値は**パスワード**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
- **証明書**を有効にする場合は、次の設定を構成します。
  - **ID資格情報:** リストから使用するID資格情報を選択します。既定値は**なし**です。
  - **接続時にPINの入力を求める:** ユーザーがネットワークに接続するときにPINの入力を求めるかどうかを選択します。既定値は**オフ**です。
  - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続のトリガーを有効にするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「VPNオンデマンドオプションの構成」を参照してください。
- **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションを有効にする場合は、次の設定を構成します。
  - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとのVPN接続が自動的にトリガーされるかどうかを選択します。デフォルトは**オフ**です。
  - **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして、次の操作を行います。
    - **ドメイン:** 追加するドメインを入力します。
    - **保存**をクリックしてドメインを保存するか、**キャンセル**をクリックしてドメインを保存しないようにします。

macOS 用 Juniper SSL プロトコルの構成

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **レルム:** オプションのレルム名を入力します。
- **役割:** オプションの役割名を入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**パスワード**または**証明書**のいずれかを選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にする場合は、次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **ID資格情報:** リストから、使用するID資格情報を選択します。デフォルトは**なし**です。
    - **接続時にPINを要求:** ユーザーがネットワークに接続する際にPINを要求するかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを有効にするかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「VPNオンデマンド設定の構成」を参照してください。

- **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションを有効にする場合は、次の設定を構成します。
    - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされたアプリがネットワーク通信を開始したときに、アプリごとのVPN接続が自動的にトリガーされるかどうかを選択します。デフォルトは**オフ**です。
    - **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできるSafariドメインごとに、**追加**をクリックして、次の操作を行います。
        - **ドメイン:** 追加するドメインを入力します。
        - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。

macOS 用 F5 SSLプロトコルの構成

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**パスワード**または**証明書**のいずれかを選択します。デフォルトは**パスワード**です。
    - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
    - **証明書**を有効にする場合は、次の設定を構成します。
        - **ID資格情報:** リストから、使用するID資格情報を選択します。デフォルトは**なし**です。
        - **接続時にPINを要求:** ユーザーがネットワークに接続する際にPINを要求するかどうかを選択します。デフォルトは**オフ**です。
        - **VPNオンデマンドを有効にする**：ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

効にするが**オン**の場合の設定については、「VPNオンデマンド設定の構成」を参照してください(#configure-enable-vpn-on-demand-options)。

- **アプリごとのVPNを有効にする**：アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションを有効にする場合は、以下の設定を構成します。
  - **オンデマンド一致アプリを有効にする**：アプリごとのVPNサービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとのVPN接続を自動的にトリガーするかどうかを選択します。デフォルトは**オフ**です。
  - **Safariドメイン**：含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして以下を実行します。
    - **ドメイン**：追加するドメインを入力します。
    - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。

macOS 用 SonicWALL Mobile Connect プロトコルの構成

- **サーバー名またはIPアドレス**：VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント**：オプションのユーザーアカウントを入力します。
- **ログオングループまたはドメイン**：オプションのログオングループまたはドメインを入力します。
- **接続の認証タイプ**：リストから、この接続の認証タイプとして**パスワード**または**証明書**のいずれかを選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にした場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にした場合は、以下の設定を構成します。
    - **ID資格情報**：リストから、使用するID資格情報を選択します。デフォルトは**なし**です。
    - **接続時にPINを要求する**：ユーザーがネットワークに接続するときにPINを要求するかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続のトリガーを有効にするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「VPNオンデマンド設定の構成」を参照してください。
- **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションを有効にする場合は、次の設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされたアプリがネットワーク通信を開始したときに、アプリごとのVPN接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは**オフ**です。
- **Safariドメイン:** アプリごとのVPN接続をトリガーできるSafariドメインごとに、**追加**をクリックして次の操作を行います。
  - **ドメイン:** 追加するドメインを入力します。
  - **保存**をクリックしてドメインを保存するか、**キャンセル**をクリックしてドメインを保存しないようにします。

macOS 用のAriba VIAプロトコルを構成する

- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
- **接続の認証の種類:** リストから、この接続の認証の種類として**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にする場合は、次の設定を構成します。
    - **ID資格情報:** リストから、使用するID資格情報を選択します。デフォルトは**なし**です。
    - **接続時にPINの入力を求める:** ユーザーがネットワークに接続するときにPINの入力を求めるかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続のトリガーを有効にするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「VPNオンデマンド設定の構成」を参照してください。
- **アプリごとのVPNを有効にする:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションを有効にする場合は、次の設定を構成します。
  - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとのVPN接続が自動的にトリガーされるかどうかを選択します。デフォルトは**オフ**です。
  - **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして次の操作を行います。
    - **ドメイン:** 追加するドメインを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **保存**をクリックしてドメインを保存するか、**キャンセル**をクリックしてドメインを保存しないようにします。

macOS用のカスタムSSLプロトコルを構成する

- **カスタムSSL識別子 (逆引きDNS形式):** 逆引きDNS形式でSSL識別子を入力します。このフィールドは必須です。
- **サーバー名またはIPアドレス:** VPNサーバーのサーバー名またはIPアドレスを入力します。このフィールドは必須です。
- **ユーザーアカウント:** オプションのユーザーアカウントを入力します。
    - **接続の認証タイプ:** リストから、この接続の認証タイプとして**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。
    - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
    - **証明書**を有効にする場合は、次の設定を構成します。
        - **ID資格情報:** リストから、使用するID資格情報を選択します。デフォルトは**なし**です。
        - **接続時にPINを要求する:** ユーザーがネットワークに接続するときにPINを要求するかどうかを選択します。デフォルトは**オフ**です。
        - **オンデマンドVPNを有効にする:** ユーザーがネットワークに接続したときにVPN接続のトリガーを有効にするかどうかを選択します。デフォルトは**オフ**です。**オンデマンドVPNを有効にする**が**オン**の場合の設定の構成については、「オンデマンドVPNを有効にする設定を構成する」を参照してください。
    - **アプリごとのVPN:** アプリごとのVPNを有効にするかどうかを選択します。デフォルトは**オフ**です。このオプションを有効にする場合は、次の設定を構成します。
        - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされたアプリがネットワーク通信を開始したときに、アプリごとのVPN接続が自動的にトリガーされるかどうかを選択します。
        - **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできるSafariドメインごとに、**追加**をクリックして、次の操作を行います。
            - **ドメイン:** 追加するドメインを入力します。
            - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **カスタムXML:** 追加するカスタムXMLパラメーターごとに、**追加**をクリックして、次の操作を行います。
  - **パラメーター名:** 追加するパラメーターの名前を入力します。
  - **値: パラメーター名**に関連付けられた値を入力します。
  - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。

VPNオンデマンドオプションの有効化を構成する

- **オンデマンドドメイン:** 追加する、ユーザーが接続したときに実行される各ドメインと関連付けられたアクションごとに、**追加**をクリックして、次の操作を行います。
  - **ドメイン:** 追加するドメインを入力します。
  - **アクション:** リストから可能なアクションのいずれかを選択します。
    - **常に確立:** ドメインは常にVPN接続をトリガーします。
    - **確立しない:** ドメインはVPN接続をトリガーしません。
    - **必要に応じて確立:** ドメイン名解決に失敗した場合、ドメインはVPN接続を試行します。失敗は、DNSサーバーがドメインを解決できない場合、別のサーバーにリダイレクトされる場合、またはタイムアウトした場合に発生します。
  - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。
- **オンデマンドルール**
  - **アクション:** リストから実行するアクションを選択します。デフォルトは**EvaluateConnection**です。可能なアクションは次のとおりです。
    - **許可:** トリガーされたときにオンデマンドVPNの接続を許可します。
    - **接続:** 無条件にVPN接続を開始します。
    - **切断:** VPN接続を削除し、ルールが一致する限りオンデマンドで再接続しません。
    - **EvaluateConnection:** 各接続の**ActionParameters**配列を評価します。
    - **無視:** 既存のVPN接続を維持しますが、ルールが一致する限りオンデマンドで再接続しません。
  - **DNSDomainMatch:** デバイスの検索ドメインリストが一致する可能性のあるドメインについては、**追加**をクリックして、以下を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **DNSドメイン:** ドメイン名を入力します。複数のドメインに一致させるには、ワイルドカード「*」プレフィックスを使用できます。たとえば、*.example.comはmydomain.example.com、yourdomain.example.com、およびherdomain.example.comに一致します。
- ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。

- **DNSServerAddressMatch:** 追加したい、ネットワークの指定されたDNSサーバーのいずれかに一致する各IPアドレスについて、**追加**をクリックして、以下を実行します。
  - **DNSサーバーアドレス:** 追加したいDNSサーバーアドレスを入力します。DNSサーバーに一致させるには、ワイルドカード「*」サフィックスを使用できます。たとえば、17.*はクラスAサブネット内の任意のDNSサーバーに一致します。
  - DNSサーバーアドレスを保存するには**保存**をクリックし、DNSサーバーアドレスを保存しない場合は**キャンセル**をクリックします。
- **InterfaceTypeMatch:** リストで、使用中のプライマリネットワークインターフェイスハードウェアの種類をクリックします。デフォルトは「**Unspecified**」です。可能な値は次のとおりです。
  - **Unspecified:** 任意のネットワークインターフェイスハードウェアに一致します。このオプションがデフォルトです。
  - **Ethernet:** イーサネットネットワークインターフェイスハードウェアのみに一致します。
  - **WiFi:** Wi-Fiネットワークインターフェイスハードウェアのみに一致します。
  - **Cellular:** セルラーネットワークインターフェイスハードウェアのみに一致します。
- **SSIDMatch:** 追加する現在のネットワークと照合する各SSIDについて、「**Add**」をクリックして以下を実行します。
  - **SSID:** 追加するSSIDを入力します。ネットワークがWi-Fiネットワークでない場合、またはSSIDが表示されない場合、一致は失敗します。任意のSSIDに一致させるには、このリストを空のままにします。
  - SSIDを保存するには「**Save**」をクリックし、SSIDを保存しない場合は「**Cancel**」をクリックします。
- **URLStringProbe:** 取得するURLを入力します。このURLがリダイレクトなしで正常に取得された場合、このルールは一致します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ActionParameters : Domains:** 追加するEvaluateConnectionがチェックする各ドメインについて、「**Add**」をクリックして以下を実行します。
  - **Domain:** 追加するドメインを入力します。
  - ドメインを保存するには「**Save**」をクリックし、ドメインを保存しない場合は「**Cancel**」をクリックします。
- **ActionParameters : DomainAction:** リストで、指定された「**ActionParameters : Domains**」ドメインの「**VPN behavior**」を選択します。デフォルトは「**ConnectIfNeeded**」です。可能なアクションは次のとおりです。
  - **ConnectIfNeeded:** ドメイン名解決が失敗した場合、ドメインはVPN接続試行をトリガーします。失敗は、DNSサーバーがドメインを解決できない場合、別のサーバーにリダイレクトされる場合、またはタイムアウトした場合に発生します。
  - **NeverConnect:** ドメインはVPN接続をトリガーしません。
- **アクションパラメータ: RequiredDNSServers:** 指定されたドメインの解決に使用する各DNSサーバーについて、**追加**をクリックし、以下を実行します。
  - **DNSサーバー: ActionParameters** : **DomainAction** = **ConnectIfNeeded**の場合にのみ有効です。追加するDNSサーバーのIPアドレスを入力します。このサーバーは、デバイスの現在のネットワーク構成の外部に配置できます。DNSサーバーに到達できない場合、VPN接続が確立されます。このDNSサーバーは、内部DNSサーバーまたは信頼できる外部DNSサーバーのいずれかである必要があります。
  - DNSサーバーを保存するには、**保存**をクリックするか、DNSサーバーを保存しない場合は**キャンセル**をクリックします。
- **ActionParameters : RequiredURLStringProbe:** オプションで、GETリクエストを使用してプローブするHTTPまたはHTTPS（推奨）URLを入力します。URLのホスト名を解決できない場合、サーバーに到達できない場合、またはサーバーが応答しない場合、VPN接続が確立されます。**ActionParameters** : **DomainAction** = **ConnectIfNeeded**の場合にのみ有効です。
- **OnDemandRules : XMLコンテンツ:** XMLのオンデマンド構成ルールを入力またはコピーして貼り付けます。
  - XMLコードを検証するには、**辞書をチェック**をクリックします。XMLが有効な場合、**XMLコンテンツ**テキストボックスの下に**有効なXML**が表示されます。有効でない場合は、エラーメッセージにエラーが記述されます。

- **プロキシ**

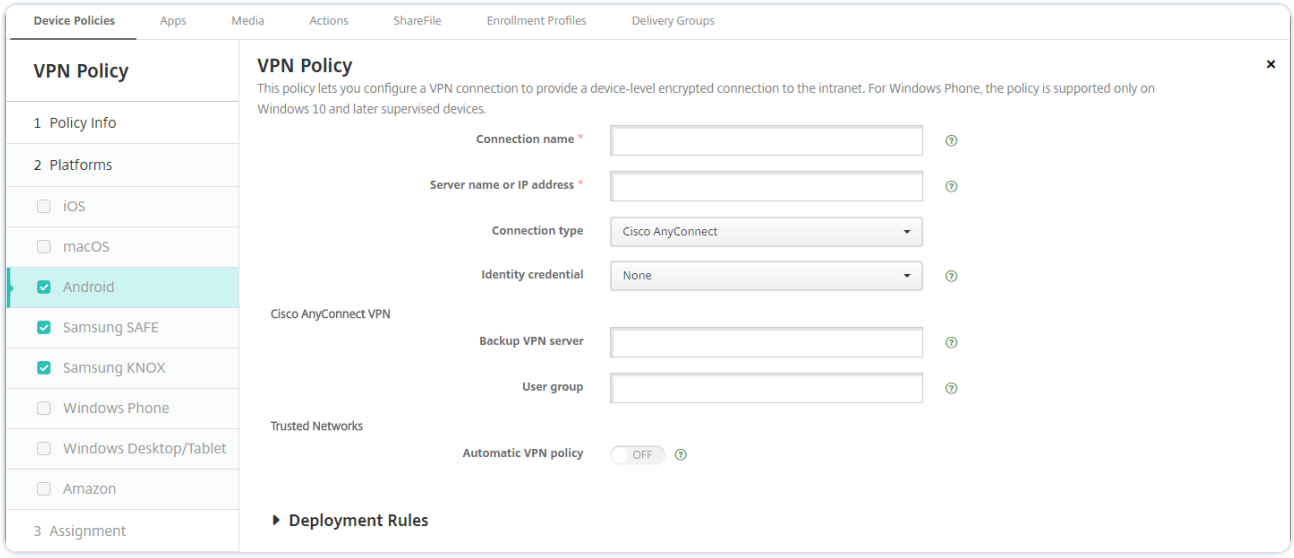
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **プロキシ構成:** リストから、VPN接続がプロキシサーバーを介してルーティングされる方法を選択します。デフォルトは**なし**です。
  - **手動**を有効にする場合、次の設定を構成します。
    - **プロキシサーバーのホスト名またはIPアドレス:** プロキシサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
    - **プロキシサーバーのポート:** プロキシサーバーのポート番号を入力します。このフィールドは必須です。
    - **ユーザー名:** オプションのプロキシサーバーユーザー名を入力します。
    - **パスワード:** オプションのプロキシサーバーパスワードを入力します。
  - **自動**を構成する場合、次の設定を構成します。
    - **プロキシサーバーURL:** プロキシサーバーのURLを入力します。このフィールドは必須です。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android (レガシーDA) 設定



Android 用 Cisco AnyConnect VPN プロトコルの構成

- **接続名:** Cisco AnyConnect VPN 接続の名前を入力します。このフィールドは必須です。
- **サーバー名またはIPアドレス:** VPNサーバーの名前またはIPアドレスを入力します。このフィールドは必須です。
- **ID資格情報:** リストからID資格情報を選択します。
- **バックアップVPNサーバー:** バックアップVPNサーバー情報を入力します。
- **ユーザーグループ:** ユーザーグループ情報を入力します。
- **信頼できるネットワーク**
    - **自動VPNポリシー:** このオプションを有効または無効にして、VPNが信頼済みネットワークと信頼されていないネットワークにどのように反応するかを設定します。有効にした場合、以下の設定を構成します。
        - **信頼済みネットワークポリシー:** リストから目的のポリシーを選択します。デフォルトは**切断**です。選択可能なオプションは次のとおりです。
            - **切断:** クライアントは信頼済みネットワークでVPN接続を終了します。この設定がデフォルトです。
            - **接続:** クライアントは信頼済みネットワークでVPN接続を開始します。
            - **何もしない:** クライアントは何もアクションを実行しません。
            - **一時停止:** ユーザーが信頼済みネットワーク外でVPNセッションを確立し、その後信頼済みとして構成されたネットワークに入ると、VPNセッションは一時停止されます。ユーザーが再び信頼済みネットワークを離れると、セッションは再開されま

© 1997–2026 Citrix Systems, Inc. All rights reserved.

す。この設定により、信頼済みネットワークを離れた後に新しいVPNセッションを確立する必要がなくなります。

- **信頼されていないネットワークポリシー:** リストから目的のポリシーを選択します。デフォルトは**接続**です。選択可能なオプションは次のとおりです。
  - **接続:** クライアントは信頼されていないネットワークでVPN接続を開始します。
  - **何もしない:** クライアントは信頼されていないネットワークでVPN接続を開始します。このオプションは常時接続VPNを無効にします。

- **信頼済みドメイン:** クライアントが信頼済みネットワークにいるときにネットワークインターフェイスが持つ各ドメインサフィックスについて、**追加**をクリックして以下を実行します。
  - **ドメイン:** 追加するドメインを入力します。
  - ドメインを保存するには**保存**をクリックするか、ドメインを保存しない場合は**キャンセル**をクリックします。
- **信頼済みサーバー:** クライアントが信頼済みネットワークにいるときにネットワークインターフェイスが持つ各サーバーアドレスについて、**追加**をクリックして以下を実行します。
  - **サーバー:** 追加するサーバーを入力します。
  - サーバーを保存するには**保存**をクリックするか、サーバーを保存しない場合は**キャンセル**をクリックします。

Android 用 Citrix SSO プロトコルを構成する

- **接続名:** VPN 接続の名前を入力します。このフィールドは必須です。
- **サーバー名または IP アドレス:** NetScaler Gateway の FQDN または IP アドレスを入力します。
- **接続の認証タイプ:** 認証タイプを選択し、そのタイプに表示されるフィールドをすべて入力します。
  - **ユーザー名**と**パスワード: 認証タイプ**が**パスワード**または**パスワードと証明書**の場合、VPN 資格情報を入力します。オプションです。VPN 資格情報を提供しない場合、Citrix VPN アプリはユーザー名とパスワードの入力を求めます。
  - **ID 資格情報: 認証タイプ**が**証明書**または**パスワードと証明書**の場合に表示されます。リストから ID 資格情報を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アプリごとの VPN を有効にする:** アプリごとの VPN を有効にするかどうかを選択します。アプリごとの VPN を有効にしない場合、すべてのトラフィックは Citrix VPN トンネルを通過します。アプリごとの VPN を有効にする場合、以下の設定を指定します。デフォルトは**オフ**です。
  - **許可リスト**または**ブロックリスト: 許可リスト**の場合、許可リスト内のすべてのアプリがこの VPN を介してトンネル接続されます。**ブロックリスト**の場合、ブロックリスト上のアプリを除くすべてのアプリがこの VPN を介してトンネル接続されます。
  - **アプリケーションリスト:** 許可リストまたはブロックリスト上のアプリ。**追加**をクリックし、アプリパッケージ名をコンマ区切りで入力します。
- **カスタム XML: 追加**をクリックし、カスタムパラメータを入力します。Citrix Endpoint Management は、Citrix VPN に対して以下のパラメータをサポートしています。
  - **DisableUserProfiles:** オプション。このパラメータを有効にするには、**値**に**はい**と入力します。有効にすると、Citrix Endpoint Management はユーザーが追加した VPN 接続を表示せず、ユーザーは接続を追加できません。この設定はグローバルな制限であり、すべての VPN プロファイルに適用されます。
  - **userAgent:** 文字列値。各 HTTP リクエストで送信するカスタムユーザーエージェント文字列を指定できます。指定されたユーザーエージェント文字列は、既存の Citrix VPN ユーザーエージェントに追加されます。
  - **IsAlwaysOnVpn:** オプション。このプロパティは、VPN プロファイルが Always On VPN プロファイルであるかどうかを決定します。VPN プロファイルが Always On VPN プロファイルであることを示すには**はい**に設定します。デフォルトは**いいえ**です。Always On VPN が確実に機能するためには、このプロパティが**はい**に設定されている VPN プロファイルは 1 つだけである必要があります。

NAC をサポートするように VPN を構成する

1. NAC フィルターを構成するには、**接続タイプ**として**カスタム SSL**を使用します。
2. 「**接続名**」を「**VPN**」と指定します。
3. 「**カスタムXML**」で、「**追加**」をクリックし、以下を実行します。
   - **パラメーター名:** 「**XenMobileDeviceId**」と入力します。このフィールドは、Citrix Endpoint ManagementへのデバイスNACチェックに使用するデバイスIDです。Citrix Endpoint Managementがデバイスを登録および管理している場合、VPN接続は許可されます。それ以外の場合、VPN確立時に認証は拒否されます。

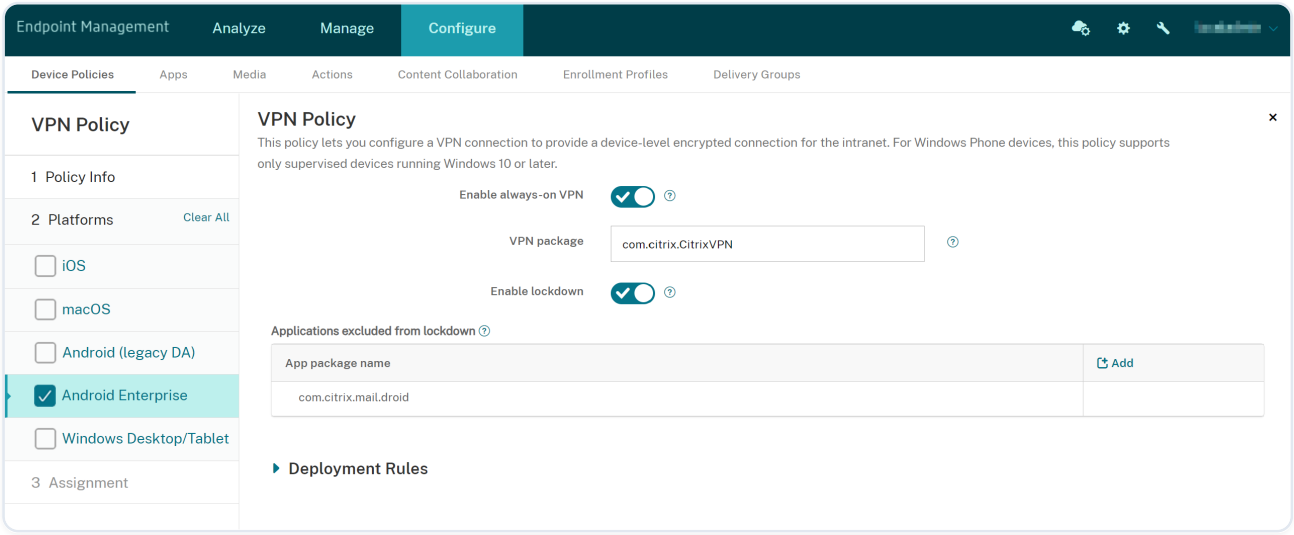
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **値:** パラメーター「**XenMobileDeviceId**」の値である「**DeviceID_${device.id}**」と入力します。
- パラメーターを保存するには、「**保存**」をクリックします。

Android Enterprise向けVPNの構成

Android Enterpriseデバイス向けVPNを構成するには、Citrix SSOアプリ用のAndroid Enterprise管理対象構成デバイスポリシーを作成します。「Android Enterprise向けVPNプロファイルの構成」を参照してください。

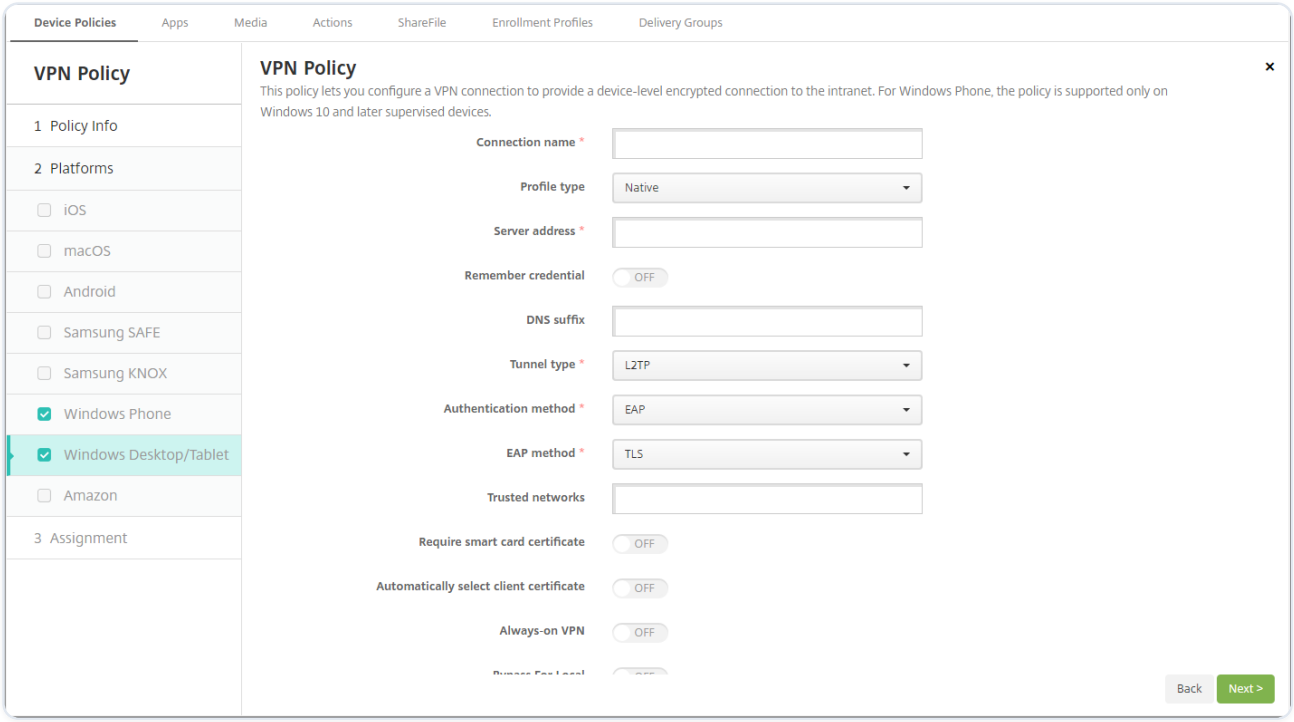
Android Enterpriseの設定



- **常時接続VPNを有効にする:** VPNを常時接続にするかどうかを選択します。デフォルトは**オフ**です。有効にすると、ユーザーが手動で切断するまでVPN接続は維持されます。
- **VPNパッケージ** デバイスが使用するVPNアプリのパッケージ名を入力します。
- **ロックダウンを有効にする:** 無効になっている場合、VPN接続が存在しないと、どのアプリもネットワークにアクセスできません。有効になっている場合、以下の設定で構成したアプリは、VPN接続が存在しない場合でもネットワークにアクセスできます。Android 10以降のデバイスで利用可能です。
- **ロックダウンから除外されるアプリケーション:** 「**追加**」をクリックして、ロックダウン設定をバイパスするアプリのパッケージ名を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windowsデスクトップ/タブレットの設定



- **接続名:** 接続の名前を入力します。このフィールドは必須です。
- **プロファイルの種類:** リストから、**ネイティブ**または**プラグイン**を選択します。デフォルトは**ネイティブ**です。
- **ネイティブプロファイルの種類を構成:** これらの設定は、ユーザーのWindowsデバイスに組み込まれているVPNに適用されます。
  - **サーバーアドレス:** VPNサーバーのFQDNまたはIPアドレスを入力します。このフィールドは必須です。
  - **資格情報を記憶:** 資格情報をキャッシュするかどうかを選択します。デフォルトは**オフ**です。有効にすると、可能な限り資格情報がキャッシュされます。
  - **DNSサフィックス:** DNSサフィックスを入力します。
  - **トンネルの種類:** リストから、使用するVPNトンネルの種類を選択します。デフォルトは**L2TP**です。選択可能なオプションは次のとおりです。
    - **L2TP:** 事前共有キー認証を使用するレイヤー2トンネリングプロトコル。
    - **PPTP:** ポイントツーポイントトンネリング。
    - **IKEv2:** インターネットキー交換バージョン2。
  - **認証方法:** リストから、使用する認証方法を選択します。デフォルトは**EAP**です。選択可能なオプションは次のとおりです。
    - **EAP:** 拡張認証プロトコル。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **MSChapV2:** 相互認証にMicrosoftチャレンジハンドシェイク認証プロトコルを使用します。このオプションは、トンネルの種類に**IKEv2**を選択した場合は使用できません。

  - **EAPメソッド:** リストから、使用するEAPメソッドを選択します。デフォルトは**TLS**です。MSChapV2認証が有効な場合、このフィールドは使用できません。選択可能なオプションは次のとおりです。

    - **TLS:** トランスポート層セキュリティ
    - **PEAP:** 保護された拡張認証プロトコル

  - **信頼されたネットワーク:** VPN接続を必要としないネットワークのリストをコンマで区切って入力します。たとえば、ユーザーが社内ワイヤレスネットワークにいる場合、保護されたリソースに直接アクセスできます。
  - **スマートカード証明書を要求:** スマートカード証明書を要求するかどうかを選択します。デフォルトは**オフ**です。
  - **クライアント証明書を自動的に選択:** 認証に使用するクライアント証明書を自動的に選択するかどうかを選択します。デフォルトは**オフ**です。このオプションは、**スマートカード証明書を要求**を有効にしている場合は使用できません。
  - **常時接続VPN:** VPNを常時接続にするかどうかを選択します。デフォルトは**オフ**です。有効にすると、ユーザーが手動で切断するまでVPN接続は維持されます。
  - **ローカルのバイパス:** ローカルリソースがプロキシサーバーをバイパスできるように、アドレスとポート番号を入力します。

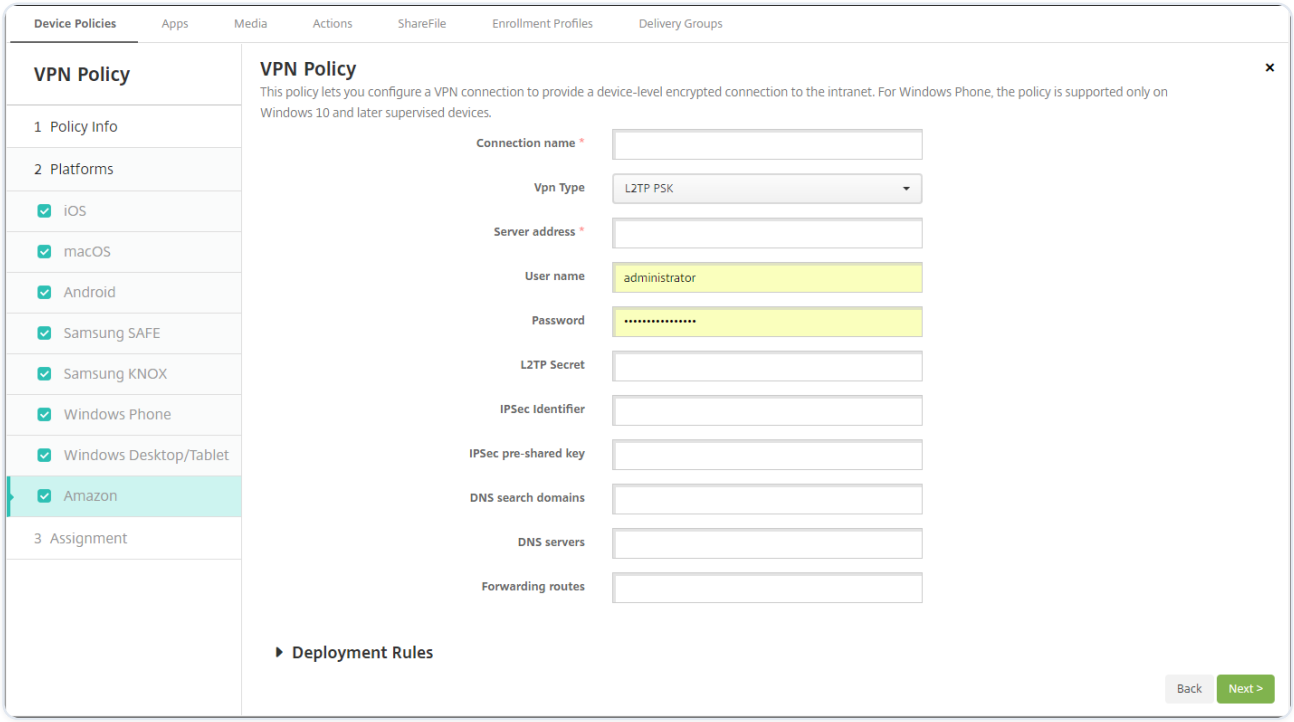
- **プラグインプロファイルタイプを構成:** これらの設定は、Windowsストアから入手し、ユーザーのデバイスにインストールされたVPNプラグインに適用されます。

  - **サーバーアドレス:** VPNサーバーのFQDNまたはIPアドレスを入力します。このフィールドは必須です。
  - **資格情報を記憶:** 資格情報をキャッシュするかどうかを選択します。デフォルトは**オフ**です。有効にすると、可能な限り資格情報がキャッシュされます。
  - **DNSサフィックス:** DNSサフィックスを入力します。
  - **クライアントアプリID:** VPNプラグインのパッケージファミリー名を入力します。
  - **プラグインプロファイルXML:** **参照**をクリックしてファイルの場所へ移動し、使用するカスタムVPNプラグインプロファイルを選択します。形式と詳細については、プラグインプロバイダーにお問い合わせください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **信頼されたネットワーク:** VPN接続を必要としないネットワークのリストをコンマで区切って入力します。たとえば、ユーザーが社内ワイヤレスネットワークにいる場合、保護されたリソースに直接アクセスできます。
- **常時接続VPN:** VPNを常時接続にするかどうかを選択します。デフォルトは**オフ**です。有効にすると、ユーザーが手動で切断するまでVPN接続は維持されます。
- **ローカルのバイパス:** ローカルリソースがプロキシサーバーをバイパスできるように、アドレスとポート番号を入力します。

Amazon の設定



- **接続名:** 接続の名前を入力します。
- **VPN タイプ:** 接続タイプを選択します。選択可能なオプションは次のとおりです。
  - **L2TP PSK:** 事前共有キー認証を使用するレイヤー2トンネリングプロトコル。この設定がデフォルトです。
  - **L2TP RSA:** RSA認証を使用するレイヤー2トンネリングプロトコル。
  - **IPSEC XAUTH PSK:** 事前共有キーと拡張認証を使用するインターネットプロトコルセキュリティ。
  - **IPSEC HYBRID RSA:** ハイブリッドRSA認証を使用するインターネットプロトコルセキュリティ。
  - **PPTP:** ポイントツーポイントトンネリング。

以下のセクションでは、上記の各接続タイプの構成オプションを一覧表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Amazon の L2TP PSK 設定を構成する

- **サーバーアドレス:** VPNサーバーのIPアドレスを入力します。
- **ユーザー名:** オプションのユーザー名を入力します。
- **パスワード:** オプションのパスワードを入力します。
- **L2TP シークレット:** 共有シークレットキーを入力します。
- **IPSec識別子:** ユーザーが接続時にデバイスで確認するVPN接続の名前を入力します。
- **IPSec事前共有キー:** シークレットキーを入力します。
- **DNS検索ドメイン:** ユーザーデバイスの検索ドメインリストが一致する可能性のあるドメインを入力します。
- **DNSサーバー:** 指定されたドメインの解決に使用するDNSサーバーのIPアドレスを入力します。
- **転送ルート:** 企業VPNサーバーが転送ルートをサポートしている場合、使用する各転送ルートについて、**追加**をクリックして以下を実行します。
  - **転送ルート:** 転送ルートのIPアドレスを入力します。
  - ルートを保存するには**保存**をクリックし、ルートを保存しない場合は**キャンセル**をクリックします。

AmazonのL2TP RSA設定を構成する

- **サーバーアドレス:** VPNサーバーのIPアドレスを入力します。
- **ユーザー名:** オプションのユーザー名を入力します。
- **パスワード:** オプションのパスワードを入力します。
- **L2TPシークレット:** 共有シークレットキーを入力します。
- **DNS検索ドメイン:** ユーザーデバイスの検索ドメインリストが一致する可能性のあるドメインを入力します。
- **DNSサーバー:** 指定されたドメインの解決に使用するDNSサーバーのIPアドレスを入力します。
- **サーバー証明書:** リストから使用するサーバー証明書を選択します。
- **CA証明書:** リストから、使用するCA証明書を選択します。
- **ID資格情報:** リストから、使用するID資格情報を選択します。
- **転送ルート:** 社内VPNサーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに**追加**をクリックして、次の操作を行います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **転送ルート:** 転送ルートのIPアドレスを入力します。
- **保存**をクリックしてルートを保存するか、**キャンセル**をクリックしてルートを保存しないようにします。

AmazonのIPSEC XAUTH PSK設定を構成する

- **サーバーアドレス:** VPNサーバーのIPアドレスを入力します。
- **ユーザー名:** オプションのユーザー名を入力します。
- **パスワード:** オプションのパスワードを入力します。
- **IPSec識別子:** ユーザーが接続時にデバイスで確認するVPN接続の名前を入力します。
- **IPSec事前共有キー:** 共有シークレットキーを入力します。
- **DNS検索ドメイン:** ユーザーデバイスの検索ドメインリストが一致する可能性のあるドメインを入力します。
- **DNSサーバー:** 指定されたドメインの解決に使用するDNSサーバーのIPアドレスを入力します。
- **転送ルート:** 社内VPNサーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに**追加**をクリックして、次の操作を行います。
  - **転送ルート:** 転送ルートのIPアドレスを入力します。
  - 「**保存**」をクリックしてルートを保存するか、ルートを保存しない場合は「**キャンセル**」をクリックします。

Amazon の IPSEC AUTH RSA 設定を構成する

- **サーバーアドレス:** VPNサーバーのIPアドレスを入力します。
- **ユーザー名:** オプションのユーザー名を入力します。
- **パスワード:** オプションのパスワードを入力します。
- **DNS検索ドメイン:** ユーザーデバイスの検索ドメインリストが一致するドメインを入力します。
- **DNSサーバー:** 指定されたドメインの解決に使用するDNSサーバーのIPアドレスを入力します。
- **サーバー証明書:** リストから使用するサーバー証明書を選択します。
- **CA証明書:** リストから使用するCA証明書を選択します。
- **ID資格情報:** リストから使用するID資格情報を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **転送ルート:** 企業VPNサーバーが転送ルートをサポートしている場合、使用する各転送ルートについて「**追加**」をクリックし、以下を実行します。
  - **転送ルート:** 転送ルートのIPアドレスを入力します。
  - 「**保存**」をクリックしてルートを保存するか、ルートを保存しない場合は「**キャンセル**」をクリックします。

Amazon の IPSEC HYBRID RSA 設定を構成する

- **サーバーアドレス:** VPNサーバーのIPアドレスを入力します。
- **ユーザー名:** オプションのユーザー名を入力します。
- **パスワード:** オプションのパスワードを入力します。
- **DNS検索ドメイン:** ユーザーデバイスの検索ドメインリストが一致するドメインを入力します。
- **DNSサーバー:** 指定されたドメインの解決に使用するDNSサーバーのIPアドレスを入力します。
- **サーバー証明書:** リストから使用するサーバー証明書を選択します。
- **CA証明書:** リストから使用するCA証明書を選択します。
- **転送ルート:** 企業VPNサーバーが転送ルートをサポートしている場合、使用する各転送ルートについて、**追加**をクリックして以下を実行します。
  - **転送ルート:** 転送ルートのIPアドレスを入力します。
  - **保存**をクリックしてルートを保存するか、**キャンセル**をクリックしてルートを保存しません。

AmazonのPPTP設定を構成する

- **サーバーアドレス:** VPNサーバーのIPアドレスを入力します。
- **ユーザー名:** オプションのユーザー名を入力します。
- **パスワード:** オプションのパスワードを入力します。
- **DNS検索ドメイン:** ユーザーデバイスの検索ドメインリストが一致するドメインを入力します。
- **DNSサーバー:** 指定されたドメインの解決に使用するDNSサーバーのIPアドレスを入力します。
- **PPP暗号化 (MPPE):** Microsoft Point-to-Point Encryption (MPPE) を使用したデータ暗号化を有効にするかどうかを選択します。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **転送ルート:** 企業VPNサーバーが転送ルートをサポートしている場合、使用する各転送ルートについて、**追加**をクリックして以下を実行します。
  - **転送ルート:** 転送ルートのIPアドレスを入力します。
  - ルートを保存するには**保存**をクリックするか、ルートを保存しない場合は**キャンセル**をクリックします。

壁紙デバイスポリシー

壁紙デバイスポリシーを使用すると、.png または .jpg ファイルを追加して、iOS デバイスのロック画面、ホーム画面、またはその両方に壁紙を設定できます。このポリシーは、監視対象デバイスでのみ利用可能です。iPad と iPhone で異なる壁紙を使用するには、異なる壁紙ポリシーを作成し、適切なユーザーに展開する必要があります。

次の表に、iOS デバイス向けに Apple が推奨する画像寸法を示します。

iPhone

デバイス	ピクセル単位の画像寸法
アイフォーン 12 プロ マックス	2778 x 1284
iPhone 12 および iPhone 12 Pro	2532 x 1170
アイフォーン 12 ミニ	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
アイフォーン XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 第2世代	1334 x 750
アイフォーン 7 Plus, 8 Plus	2208 x 1242
iPhone 7, 8	1334 x 750

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイス	ピクセル単位の画像寸法
アイフォーン 8 プラス	1334 x 750
iPhone 8	1334 x 750

iPad

デバイス	ピクセル単位の画像寸法
iPad Pro (第1世代、第2世代、第3世代 12.9インチ)	2732 x 2048
iPad Pro 10.5インチ	2224 x 1668
iPad Pro (9.7インチ)	1536 x 2048
iPad Air 2	2048 x 1536

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **適用先:** リストで、壁紙を表示する場所を設定するために、、、または を選択します。
- **壁紙ファイル:** 壁紙ファイルを選択するには、 をクリックし、ファイルの場所を参照します。

Webコンテンツフィルターデバイスポリシー

許可リストまたはブロックリストに追加する特定のサイトでAppleの自動フィルター機能を使用すると、iOSデバイスのWebコンテンツをフィルター処理できます。Webコンテンツフィルターデバイスポリシーは、監視モードのiOSデバイスでのみ使用できます。iOSデバイスを監視モードにする方法については、「Apple Configurator 2を使用してデバイスを展開する」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

- AndroidデバイスはWebコンテンツフィルタリングをサポートしていません。
- iOSバージョン16.5以降、Webコンテンツフィルターデバイスポリシーは許可リスト内の `https://localhost` を認識しなくなります。これにより、一部のアプリが応答しなくなることがあります。また、`http://localhost:`、`http://localhost:*` などのURLの派生を許可リストに追加しても、問題は解決しません。

このポリシーを追加または構成するには、**構成** > **デバイスポリシー**の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS設定

- **フィルターの種類：** ドロップダウンリストで**［組み込み］**または**［プラグイン］**をクリックし、選択したオプションの手順に従います。デフォルトは**［組み込み］**です。

組み込みフィルターの種類

- **Webコンテンツフィルター**
  - **自動フィルターを有効にする：** 不適切なコンテンツがないかWebサイトを分析するためにAppleの自動フィルター機能を使用するかどうか。デフォルトは**［オフ］**です。
  - **許可されたURL：** **［自動フィルターを有効にする］**が**［オフ］**に設定されている場合、このリストは無視されます。**［自動フィルターを有効にする］**が**［オン］**に設定されている場合、自動フィルターがアクセスを許可するかどうかにかかわらず、このリストの項目には常にアクセスできます。許可リストに追加する各URLについて、**［追加］**をクリックして、次の操作を行います。
    - 許可されたWebサイトのURLを入力します。Webアドレスの前に `https://` または `https://` を追加する必要があります。
    - Webサイトを許可リストに保存するには**［保存］**をクリックし、保存しない場合は**［キャンセル］**をクリックします。
  - **ブロックされたURL：** このリストの項目は常にブロックされます。ブロックリストに追加する各URLについて、**［追加］**をクリックして、次の操作を行います。
    - ブロックするWebサイトのURLを入力します。Webアドレスの前に `https://` または `https://` を追加する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **保存**をクリックしてWebサイトをブロックリストに保存するか、**キャンセル**をクリックして保存しないようにします。

- **ブックマーク許可リスト**
    - **ブックマーク許可リスト:** ユーザーがアクセスできるサイトを指定します。Webサイトへのアクセスを有効にするには、そのURLを追加します。
        - **URL:** ユーザーがアクセスできる各WebサイトのURL。たとえば、Citrix Secure Hubストアへのアクセスを有効にするには、Citrix Endpoint ManagementサーバーのURLを**URL**リストに追加します。Webアドレスの前に`https://`または`https://`を追加する必要があります。このフィールドは必須です。
        - **ブックマークフォルダー:** オプションのブックマークフォルダー名を入力します。このフィールドを空白のままにすると、ブックマークはデフォルトのブックマークディレクトリに追加されます。
        - **タイトル:** Webサイトのわかりやすいタイトルを入力します。たとえば、URL`https://google.com`には「Google」と入力します。
        - **保存**をクリックしてWebサイトを許可リストに保存するか、**キャンセル**をクリックして保存しないようにします。

プラグインフィルターの種類

- **フィルター名:** フィルターの一意の名前を入力します。
- **識別子:** フィルタリングサービスを提供するプラグインのバンドルIDを入力します。
- **サービスアドレス:** オプションのサーバーアドレスを入力します。有効な形式は、IPアドレス、ホスト名、またはURLです。
- **ユーザー名:** サービス用のオプションのユーザー名を入力します。
- **パスワード:** サービス用のオプションのパスワードを入力します。
- **証明書:** ドロップダウンリストから、ユーザーをサービスに認証するために使用する必要があるオプションのID証明書をクリックします。デフォルトは**なし**です。
- **WebKitトラフィックをフィルタリング:** WebKitトラフィックをフィルタリングするかどうかを選択します。
- **ソケットトラフィックをフィルタリング:** ソケットトラフィックをフィルタリングするかどうかを選択します。
- **カスタムデータ:** Webフィルターに追加するカスタムキーごとに、**追加**をクリックし、次の操作を行います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **キー:** カスタムキーを入力します。
- **値:** カスタムキーの値を入力します。
- カスタムキーを保存するには**保存**をクリックし、保存しない場合は**キャンセル**をクリックします。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除をスケジュールする方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

Webクリップデバイスポリシー

ユーザーデバイス上のアプリと並んで表示されるように、Webサイトへのショートカット（Webクリップ）を配置できます。iOS、iPadOS、macOS、Androidデバイス用のWebクリップを表す独自のアイコンを指定できます。Windowsタブレットでは、ラベルとURLのみが必要です。iOSおよびiPadOSデバイスの場合、作成したWebクリップを整理するには、ホーム画面レイアウトデバイスポリシーを構成します。iOSでアプリへのアクセスを制限する場合は、Webクリップを許可するように制限デバイスポリシーを構成してください。これらのポリシーの構成については、「ホーム画面レイアウトデバイスポリシー」および「制限デバイスポリシー」を参照してください。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **ラベル:** Webクリップとともに表示されるラベルを入力します。
- **URL:** Webクリップに関連付けられているURLを入力します。URLはプロトコルで始まる必要があります（例: `https://server`）。
- **削除可能:** ユーザーがWebクリップを削除できるかどうかを選択します。デフォルトは**オフ**です。このオプションは共有iPadではサポートされていません。
- **更新するアイコン:** をクリックしてファイルの場所に移動し、Webクリップに使用するアイコンを選択します。
- **プリコンポーズアイコン:** アイコンに効果（角丸、ドロップシャドウ、反射光沢）が適用されているかどうかを選択します。デフォルトは**オフ**で、効果が追加されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **全画面表示:** リンクされたWebページが全画面モードで開くかどうかを選択します。この設定により、iPadで単一のWebサイトのみを開くことも可能になります。または、iPadをキオスクモードで実行するように設定するには、アプリロックデバイスポリシーを使用します。詳細については、「iPadをキオスクとして構成する」を参照してください。デフォルトは**オフ**です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、 と です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。
  - **プロファイルスコープ:** ポリシーがユーザーに適用されるか、システム全体に適用されるかを選択します。デフォルト値は**システム**です。iOS 9.3以降でのみ利用可能です。

macOS設定

- **ラベル:** Webクリップに表示するラベルを入力します。
- **URL:** Webクリップに関連付けられているURLを入力します。URLは、たとえば`https://server`のようにプロトコルで始まる必要があります。
- **更新するアイコン:** 参照をクリックしてファイルの場所に移動し、Webクリップに使用するアイコンを選択します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間（時間）**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を数値で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。

Android設定

- **ルール:** このポリシーがWebクリップを追加するか削除するかを選択します。デフォルトは**追加**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ラベル:** Webクリップに表示するラベルを入力します。
- **URL:** Webクリップに関連付けられているURLを入力します。
- **アイコンを定義:** アイコンファイルを使用するかどうかを選択します。デフォルトは**オフ**です。
- **アイコンファイル: アイコンを定義**が**オン**の場合、**参照**をクリックしてファイルの場所に移動し、使用するアイコンファイルを選択します。

ウィンドウズ デスクトップ/タブレットの設定

- **名前:** Webクリップに表示されるラベルを入力します。
- **URL:** Webクリップに関連付けられているURLを入力します。

Windows Agentデバイスポリシー

Windows Agentデバイスポリシーを使用して、管理対象のWindowsデスクトップおよびタブレットでPowerShellスクリプトを実行します。Citrix Endpoint Managementにエンタープライズアプリとしてアップロードされたスクリプトファイルや、スクリプトをホストする他のサーバーを指すことができます。エンタープライズアプリの追加については、「アプリの追加」を参照してください。

すべてのスクリプトは特権ステータスで実行されるため、管理者としてスクリプトを実行する必要はありません。

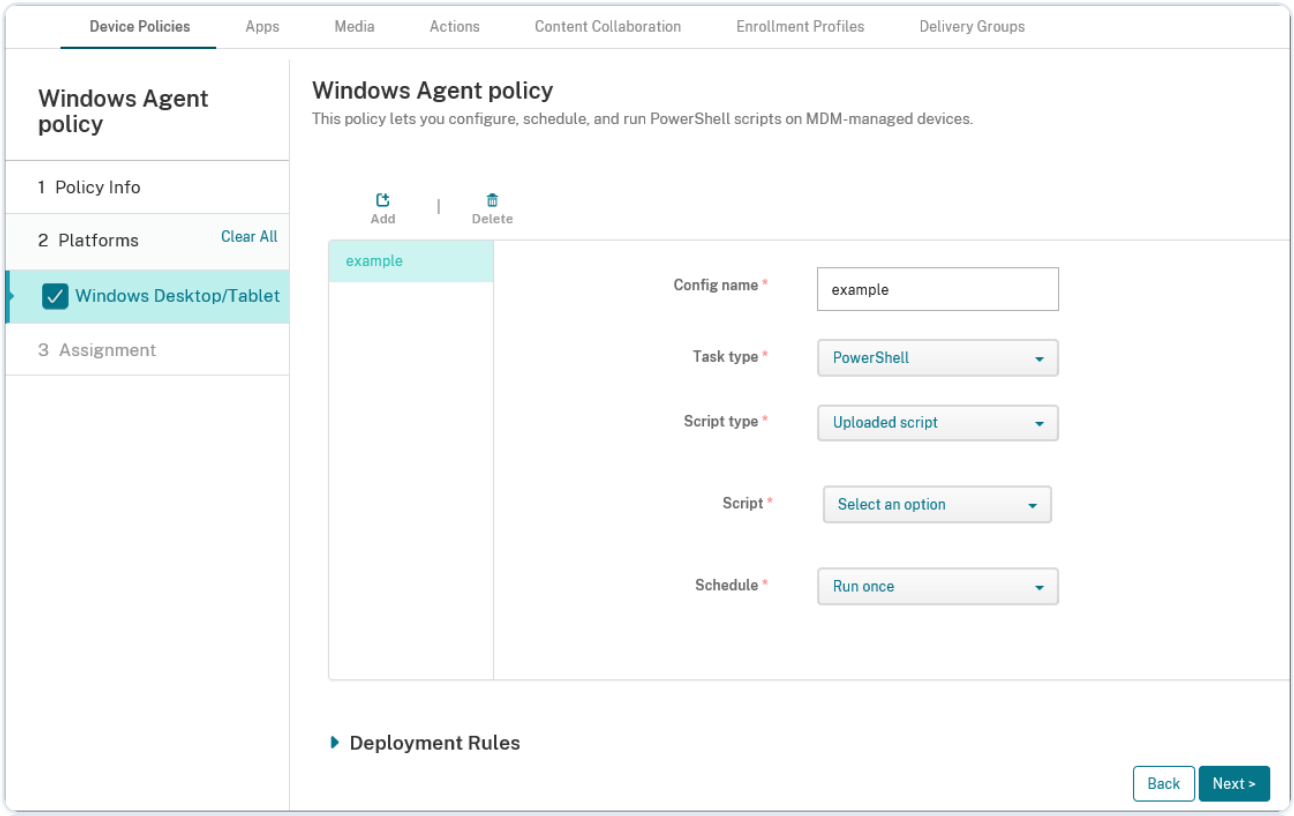
スクリプトを展開して実行した後、スクリプトの結果に基づいて自動アクションを構成できます。たとえば、レジストリキーを監視して結果を返すスクリプトを実行します。返された結果に基づいて、自動アクションが実行されます。このアクションは、アプリへのアクセスを許可または拒否したり、デバイスをコンプライアンス違反としてマークしたり、その他の影響を与えたりします。

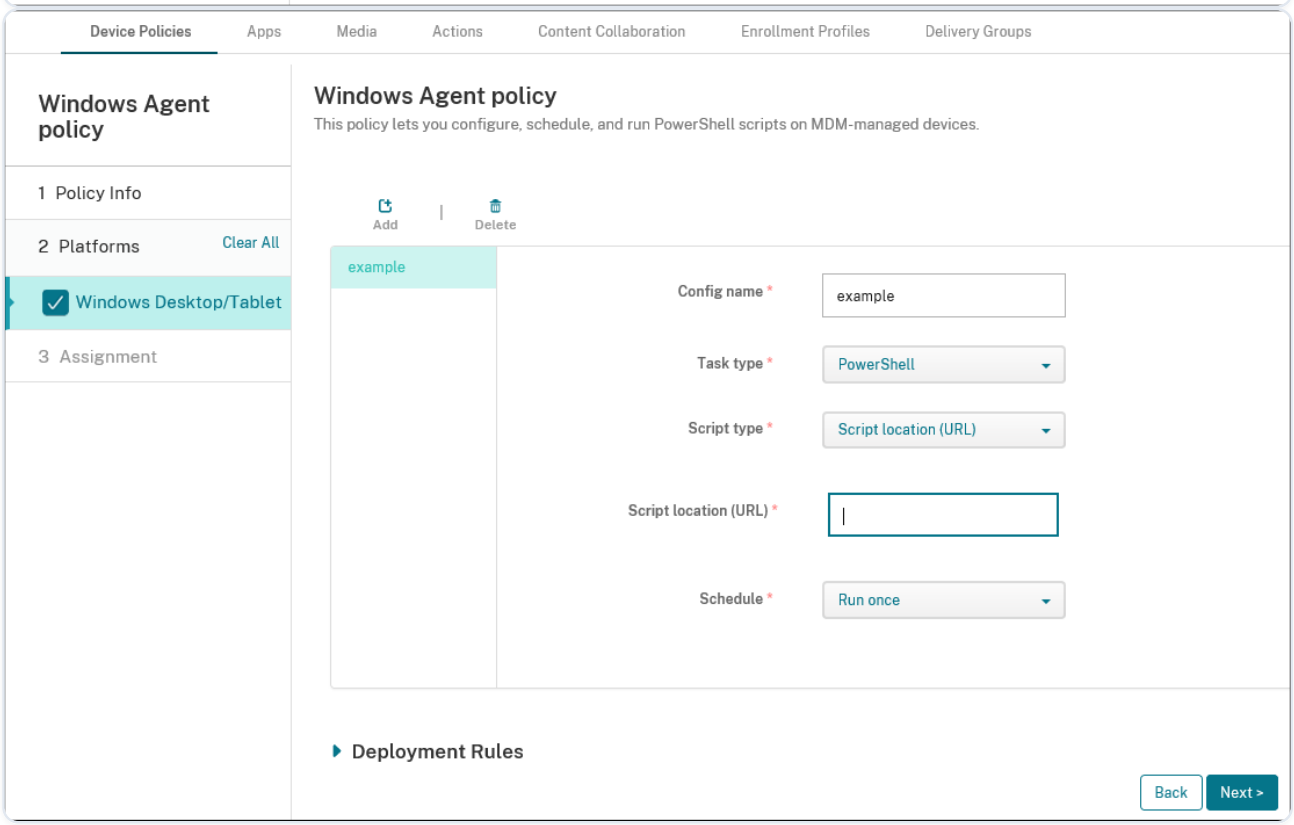
このポリシーを使用して、.msiファイルと.mstファイルを指すPowerShellスクリプトを構成することで、カスタマイズされたMSIインストーラーを展開することもできます。

このポリシーを追加または構成するには、［**構成**］>［**デバイスポリシー**］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windowsデスクトップおよびタブレットの設定





- **構成名：** 構成のわかりやすい名前を入力します。
- **タスクの種類：** ［PowerShell］ を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **スクリプトの種類：** Citrix Endpoint Managementにアップロードしたスクリプトの場合は **［アップロードされたスクリプト］** を選択し、外部でホストされているスクリプトの場合は **［スクリプトの場所（URL）］** を選択します。Citrix Endpoint Managementにスクリプトをアップロードする方法について詳しくは、「エンタープライズアプリとして`Win32`アプリを追加する」を参照してください。
    - **スクリプトの選択：** **［アップロードされたスクリプト］** を選択した場合は、実行するスクリプトを選択します。
    - **スクリプトの場所（URL）：** **［スクリプトの場所（URL）］** を選択した場合は、実行するスクリプトの場所を入力します。このURLは、スクリプトをペイロードとして配信する必要があります。Citrix Endpoint Managementは、JavaScriptダウンロードとしてスクリプトを配信するURLをサポートしていません。スクリプトは公開されている必要があります。
- **スケジュール：** 選択したスクリプトを1回実行するには **［1回実行］** を選択し、定期的に実行するには **［定期的に実行］** を選択します。
    - **実行間隔 (時間):** スクリプト実行間の時間数を入力します。

スクリプトのステータスを確認するには、コンソールで **>** に移動します。スクリプトのステータスを確認するデバイスを選択し、 をクリックします。 で、 の見出しの下にある をクリックすると、スクリプトのステータスを確認できます。

自動アクションをトリガーするPowerShellスクリプトを展開する

1. レジストリキーを監視するPowerShellスクリプトを作成します。次のPowerShellスクリプトは、ファイアウォールが有効になっているかどうかを確認します。

```
$body = @{}

$firewallEnabled = Get-ItemPropertyValue HKLM:
\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPoli
cy\StandardProfile -Name EnableFirewall

if($firewallEnabled -eq 1){

$body["firewallEnabled"]="true"

} else {

$body["firewallEnabled"]="false"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}

$body | ConvertTo-Json -Depth 10
```

このスクリプトは、次のいずれかの値を返します。

```
{

    "firewallEnabled":  "true"

}
```

または

```
{

    "firewallEnabled":  "false"

}
```

2. スクリプトをエンタープライズアプリとしてCitrix Endpoint Managementコンソールにアップロードするか、アクセス可能なURLでスクリプトをホストします。
3. この記事で説明されているWindows Agentデバイスポリシーを構成します。スクリプトがすぐに実行されるようにスケジュールされていることを確認してください。
4. スクリプトの実行後、スクリプトのステータスを判断します。
    a. コンソールで **>** に移動します。
    b. スクリプトのステータスを確認するデバイスを選択し、 をクリックします。
    c. の見出しの下にある をクリックします。
5. 受信したステータスに基づいて自動アクションを構成します。自動アクションの構成の詳細については、「Windows Agentデバイスポリシーの結果に基づく自動アクションの作成」を参照してください。そのセクションでは、サンプルスクリプトとWindows Agentデバイスポリシー用に作成された特定の自動アクションが示されています。

Windows GPO構成デバイスポリシー

Windows GPO構成デバイスポリシーでは、次のことができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

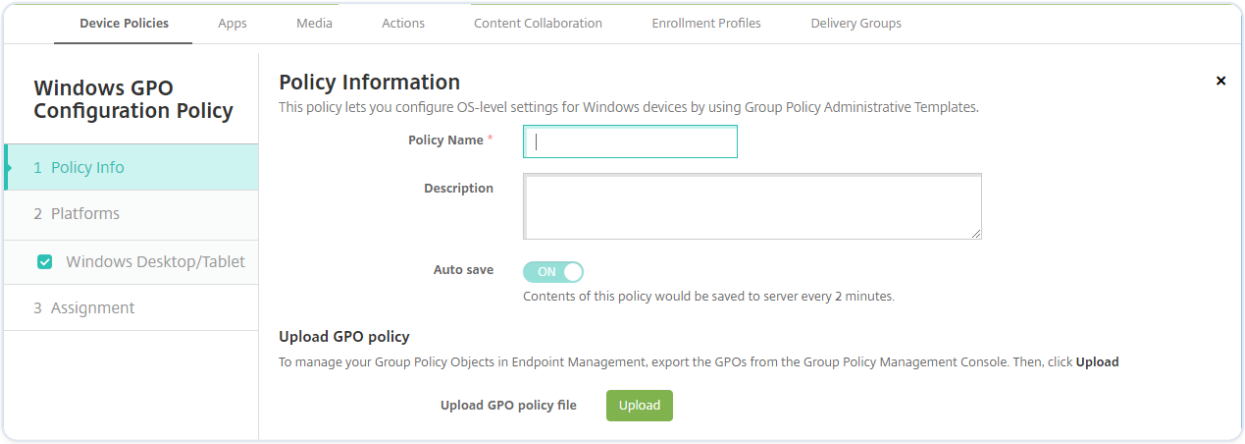
- Citrix Endpoint Managementコンソールを使用して、グループポリシーオブジェクト (GPO) をインポートし、Windows 10およびWindows 11デバイスに展開します。
- Citrix Workspace Environment Managementでサポートされている任意のWindowsデバイス向けにGPOを構成します。
- デバイスレベルおよびユーザーレベルでGPOを構成します。

Windows 10およびWindows 11デバイスに展開するためのGPOをインポートする

AD管理者がグループポリシー管理コンソールを使用してGPOを管理するのではなく、Citrix Endpoint Managementコンソールを通じてGPOをインポートおよび展開できます。

Citrix Endpoint ManagementでGPOのバックアップを作成するには：

1. AD管理者に、グループポリシー管理コンソールからGPOをエクスポートし、そのファイルをあなたに提供するよう依頼します。
2. Citrix Endpoint Managementコンソールで、**構成 > デバイスポリシー**に移動し、**Windows GPO構成**ポリシーを作成します。
3. **アップロード**をクリックし、ファイルを見つけて、**開く**をクリックしてファイルをインポートします。



GPOの構成については、この記事のWindowsデスクトップおよびタブレット設定を参照してください。

Citrix Workspace Environment Managementに展開するためのGPOを構成する

Windows GPO構成デバイスポリシーを使用すると、Citrix Workspace Environment Management (WEM) でサポートされている任意のWindowsデバイス向けにGPOを構成できます。Citrix Endpoint Managementは、ポリシーをCitrix WEMサービスにプッシュします。その後、WEMサー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ビスは、デバイスにインストールされているWEMエージェントを使用して、GPOをデバイスとそのアプリに適用します。

Workspace Environment Managementエージェントのインストールについては、「インストールと構成」を参照してください。

このポリシーは、すべてのWindows OS ADMXファイルを使用します。サードパーティのADMXファイルをアップロードする場合は、アプリ構成デバイスポリシーを使用します。サードパーティのADMXファイルのアップロードについて詳しくは、「アプリケーション構成デバイスポリシー」を参照してください。

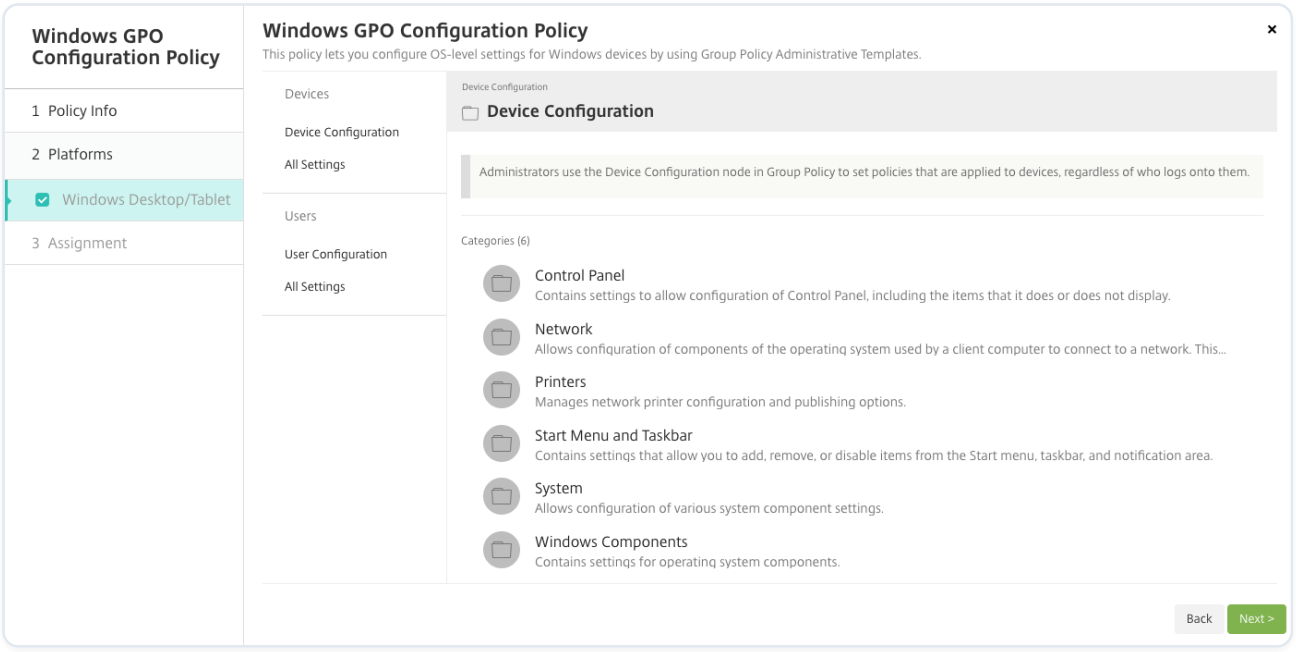
- Citrix Endpoint Managementがデバイスをネイティブでサポートしていない場合でも、WEMがサポートする任意のデバイスにGPO構成をプッシュできます。サポートされているデバイスのリストについては、「オペレーティングシステムの要件」を参照してください。
- このポリシーでは、デバイスにWEMエージェントがインストールされ、構成されている必要があります。デバイスをMDMまたはMAMに登録する必要はありません。
- Citrix Endpoint Managementは、WEMチャネルを介してGPO設定をプッシュします。（Microsoftは、MDMチャネルを介したデバイスレベル設定のプッシュをサポートしていません。）Windows GPO構成デバイスポリシーを受信するデバイスは、WEMと呼ばれるCitrix Endpoint Managementモードで実行されます。登録済みデバイスの**管理 > デバイス**リストでは、WEM管理デバイスの**モード**列に**WEM**と表示されます。

このポリシーを追加または構成するには、**構成 > デバイスポリシー**に移動します。詳しくは、「デバイスポリシー」を参照してください。

Windowsデスクトップおよびタブレットの設定

このポリシーを使用すると、デバイスレベルとユーザーレベルでGPOを構成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Windowsデバイスに展開するWindows GPOを選択して構成します。**デバイス構成**と**ユーザー構成**を変更できます。ポリシーはツリー構造で表示されます。すべての設定を表示するには、**すべての設定**をクリックします。設定の詳細については、MicrosoftからGPOリファレンスシートをダウンロードしてください。

設定を構成するには、まずそれを有効にします。構成中に、Citrix Endpoint Managementは変更を自動保存し、その設定が保持されるようにします。設定が保存される前にページを離れようとすると、未保存の変更があることを示すポップアップメッセージが表示されます。

設定に2つのオプションがある場合は、ラジオボタンの選択が表示されます。3つ以上のオプションがある場合は、メニューが表示されます。

注：

構成した設定を確認する必要がある場合は、次の操作を実行できます。

1. Citrix Endpoint Managementコンソールで、編集する**Windows GPO構成**ポリシーを開きます。
2. 「**デバイス**」または「**ユーザー**」の下で、「**すべての設定**」を選択します。
3. テーブルを「**ステータス**」で昇順に並べ替えます。未構成のポリシーはすべて「**未構成**」のステータスになります。構成したポリシーが一番上に表示されます。

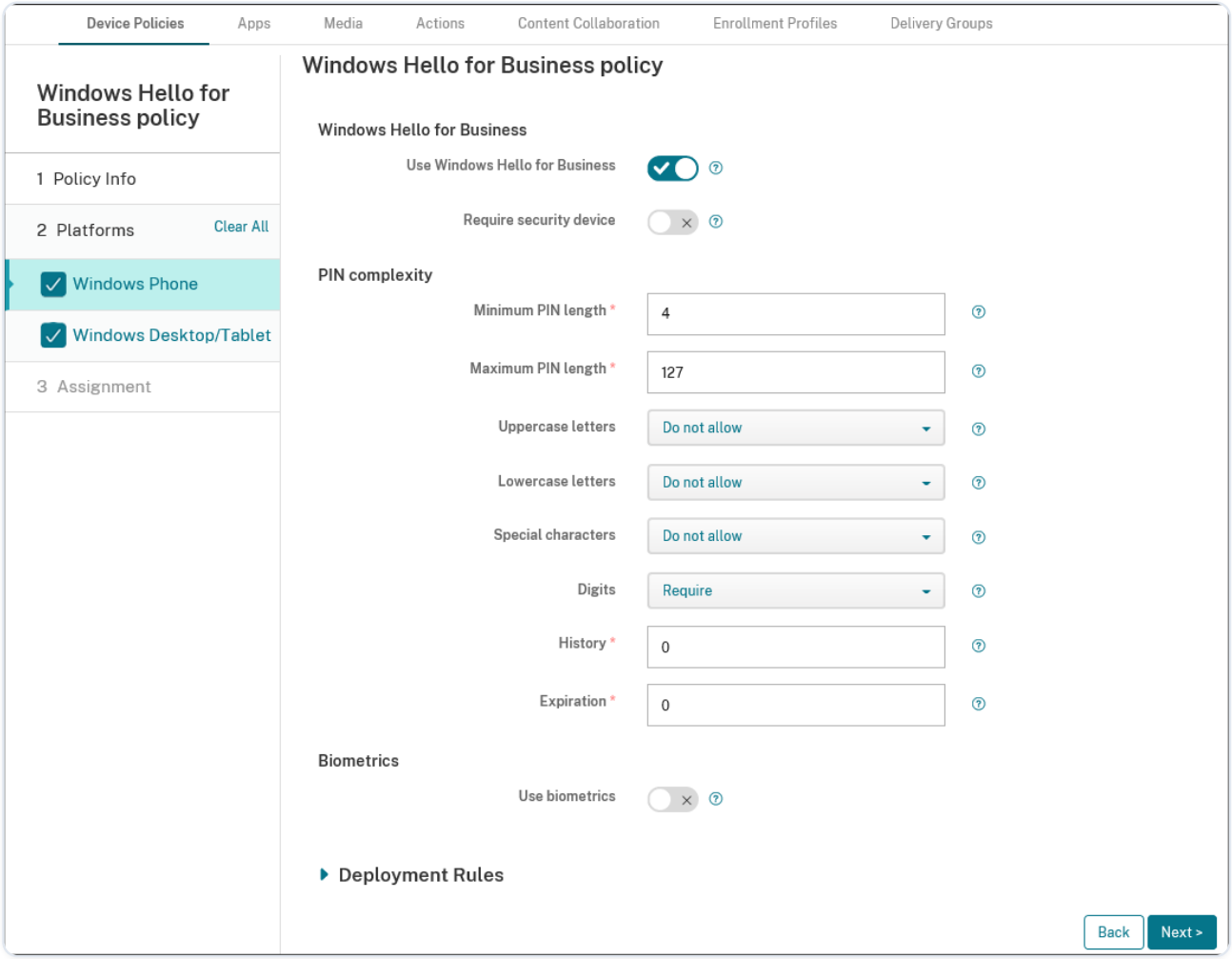
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows Hello for Business デバイスポリシー

Windows Hello for Businessを使用すると、ユーザーはActive DirectoryまたはAzure Active Directoryアカウントを使用してWindowsデバイスにサインオンできます。**Windows Hello for Business**デバイスポリシーを使用してこの機能を有効にすると、ユーザーはデバイスでWindows Hello for Businessをプロビジョニングできるようになります。このポリシーでは、パスコードの制限やその他のセキュリティ機能も構成できます。

構成 > デバイスポリシーに移動して、**Windows Hello for Business**デバイスポリシーを追加します。次の設定を構成します。

Windowsデスクトップ/タブレットの設定



- **Windows Hello for Businessを使用する:** 機能を有効にして、ユーザーがデバイスでWindows Hello for Businessをプロビジョニングできるようにします。
- **セキュリティデバイスを要求する:** サインオンするには、ユーザーがトラステッドプラットフォームモジュール（TPM）を持っていることを要求します。
- **PINの最小/最大長:** ユーザーPINの最小および最大長。**PINの最小長**のデフォルトは**4**です。**PINの最大長**のデフォルトは**127**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **大文字、小文字、特殊文字:** 各文字タイプを**許可**、**必須**、または**許可しない**のいずれにするかを選択します。デフォルトは**許可しない**です。
- **数字:** 数字を**許可**、**必須**、または**許可しない**のいずれにするか。デフォルトは**必須**です。
- **履歴:** ユーザーが再利用できない過去のPINの数。デフォルトは**0**で、これはユーザーがすべてのPINを再利用できることを意味します。
- **有効期限:** ユーザーがPINを変更する必要があるまでの日数。デフォルトは**0**で、これはPINが期限切れにならないことを意味します。
- **生体認証を使用する:** ユーザーサインオンにPINの代わりに生体認証の使用を許可します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリの追加

Citrix Endpoint Managementにアプリを追加すると、モバイルアプリケーション管理 (MAM) 機能が提供されます。Citrix Endpoint Managementは、アプリケーションの配信、ソフトウェアライセンス、構成、およびアプリケーションライフサイクル管理を支援します。

アプリをMDX対応にすることは、一部の種類のアプリをユーザーデバイスに配布するために準備する上で重要な部分です。MDXの概要については、Citrix Endpoint Managementコンポーネントおよび MAM SDKの概要を参照してください。

- Citrixでは、MAM SDKを使用してアプリをMDX対応にすることをお勧めします。または、MDX Toolkitが非推奨になるまで、アプリのMDXラッピングを継続することもできます。非推奨を参照してください。
- MDX Toolkitを使用してCitrixモバイル生産性向上アプリをラップすることはできません。Citrixダウンロードからモバイル生産性向上アプリのMDXファイルを入手してください。

Citrix Endpoint Managementコンソールにアプリを追加すると、次のことができます。

- アプリ設定の構成
- 必要に応じて、Citrix Secure Hubで整理するためにアプリをカテゴリに配置する
- 必要に応じて、ユーザーがアプリにアクセスする前に承認を要求するワークフローを定義する
- ユーザーへのアプリの展開

この記事では、アプリを追加するための一般的なワークフローについて説明します。プラットフォーム固有の情報については、以下の記事を参照してください。

- Android Enterpriseアプリの配布
- Appleアプリの配布

重要：

Citrix Endpoint Managementは、最大300個のアプリの追加と保守をサポートしています。この制限を超えると、システムが不安定になります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリの種類と機能

次の表は、Citrix Endpoint Management で展開できるアプリの種類をまとめたものです。

アプリの種類	ソース	注	参照
MDX	ユーザー向けに開発するiOSおよびAndroidアプリ。Citrixモバイル生産性アプリ。	MAM SDKを使用してiOSまたはAndroidアプリを開発するか、MDX Toolkitでラップします。モバイル生産性アプリの場合は、Citrixダウンロードからパブリックストアのファイルをダウンロードします。その後、Citrix Endpoint Managementにアプリを追加します。	MDXアプリを追加する
パブリックアプリストア	Google PlayやApple App Storeなどのパブリックアプリストアからの無料または有料アプリ。	アプリをアップロードし、MDXを有効にしてから、Citrix Endpoint Managementにアプリを追加します。	パブリックアプリストアアプリを追加する
WebおよびSaaS	内部ネットワーク (Webアプリ) またはパブリックネットワーク (SaaS)。	Citrix Endpoint Managementは、MDMに登録されているiOSおよびAndroidデバイスからネイティブSaaSアプリへのモバイルシングルサインオンを提供します。または、Security Assertion Markup Language (SAML) アプリケーションコネクタを使用します。	WebアプリまたはSaaSアプリを追加する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリの種類	ソース	注	参照
エンタープライズ	MDXが有効になっていないWin32アプリを含むプライベートアプリ。MDXが有効になっているプライベートAndroid Enterpriseアプリ。エンタープライズアプリは、コンテンツ配信ネットワークの場所またはCitrix Endpoint Managementサーバーにあります。	アプリをCitrix Endpoint Managementに追加します。	エンタープライズアプリを追加する
Webリンク	インターネットWebアドレス、イントラネットWebアドレス、またはシングルサインオンを必要としないWebアプリ。	Citrix Endpoint ManagementでWebリンクを構成します。	Webリンクを追加する

アプリの配布を計画する際は、次の機能を考慮してください。

- サイレントインストールについて
- 必須アプリとオプションアプリについて
- アプリケーションカテゴリについて
- Citrix CDN からエンタープライズアプリを配信
- Microsoft 365 アプリを有効にする
- ワークフローを適用する
- アプリストアと Citrix Secure Hub のブランディング
- アプリストアを介した Citrix Virtual Apps and Desktops™

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サイレントインストールについて

Citrix は、iOS、Android Enterprise、Samsung アプリのサイレントインストールとアップグレードをサポートしています。サイレントインストールとは、デバイスに展開するアプリのインストールをユーザーに促さないことを意味します。アプリはバックグラウンドで自動的にインストールされます。

サイレントインストールを実装するための前提条件:

- iOS の場合、管理対象の iOS デバイスを監視モードにします。詳細については、「iOS および macOS プロファイルデバイスポリシーのインポート」を参照してください。
- Android Enterprise の場合、アプリはデバイスの Android 仕事用プロファイルにインストールされます。詳細については、「Android Enterprise」を参照してください。
- Samsung デバイスの場合、デバイスで Samsung Knox を有効にします。

  そのためには、Samsung MDM ライセンスキーデバイスポリシーを設定して、Samsung ELM および Knox ライセンスアクセスコードを生成します。詳細については、「Samsung MDM ライセンスキーデバイスポリシー」を参照してください。

必須アプリとオプションアプリについて

デリバリーグループにアプリを追加するときに、オプションにするか必須にするかを選択します。Citrix は、アプリを**必須**として展開することをお勧めします。

- 必須アプリはユーザーデバイスにサイレントインストールされ、ユーザーの操作を最小限に抑えます。この機能を有効にすると、アプリが自動的に更新されるようにもなります。
- オプションアプリでは、ユーザーがインストールするアプリを選択できますが、ユーザーは Citrix Secure Hub を介して手動でインストールを開始する必要があります。

必須としてマークされたアプリの場合、ユーザーは次のような状況で迅速に更新を受け取ることができます。

- 新しいアプリをアップロードし、必須としてマークする。
- 既存のアプリを必須としてマークする。
- ユーザーが必須アプリを削除する。
- Citrix Secure Hub の更新が利用可能になる。

必須アプリの強制展開の要件

- iOS 用 Citrix Secure Hub 10.5.15 および Android 用 10.5.20 (最小バージョン)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- MAM SDK または MDX Toolkit 10.6 (最小バージョン)
- Citrix Endpoint Management と Citrix Secure Hub をアップグレードした後: 登録済みデバイスのユーザーは、必須アプリの展開更新を取得するために、Citrix Secure Hub からサインオフしてからサインオンする必要があります。

例

次の例は、Secure Tasks という名前のアプリをデリバリーグループに追加し、そのデリバリーグループを展開する手順を示しています。

デリバリーグループ構成画面(/en-us/citrix-endpoint-management/media/configure-delivery-groups-required-apps.png)

デリバリーグループ構成画面(/en-us/citrix-endpoint-management/media/delivery-groups-deploy.png)

サンプルアプリ Secure Tasks がユーザーデバイスに展開されると、Citrix Secure Hub はユーザーにアプリのインストールを促します。

シトリックス セキュア ハブ 画面(/en-us/citrix-endpoint-management/media/secure-hub-app-installation-message.png)

シトリックス セキュア ハブ 画面(/en-us/citrix-endpoint-management/media/secure-hub-app-installed.png)

重要:

エンタープライズアプリやパブリックアプリストアアプリを含むMDX対応の必須アプリは、直ちにアップグレードされます。アプリの更新猶予期間のMDXポリシーを構成し、ユーザーが後でアプリをアップグレードすることを選択した場合でも、このアップグレードは実行されます。

エンタープライズアプリおよびパブリックストアアプリ向けのiOS必須アプリのワークフロー

1. 初期登録時にモバイル生産性向上アプリを展開します。必須アプリがデバイスにインストールされます。
2. Citrix Endpoint Managementコンソールでアプリを更新します。
3. Citrix Endpoint Managementコンソールを使用して必須アプリを展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. ホーム画面のアプリが更新されます。また、パブリックストアアプリの場合、アップグレードは自動的に開始されます。ユーザーに更新を促すプロンプトは表示されません。
5. ユーザーはホーム画面からアプリを開きます。アプリの更新猶予期間を設定し、ユーザーが後でアプリをアップグレードするようにタップした場合でも、アプリは直ちにアップグレードされます。

エンタープライズアプリ向けのAndroid必須アプリのワークフロー

1. 初期登録時にモバイル生産性向上アプリを展開します。必須アプリがデバイスにインストールされます。
2. Citrix Endpoint Managementコンソールを使用して必須アプリを展開します。
3. アプリがアップグレードされます。（Nexusデバイスではインストール更新のプロンプトが表示されますが、Samsungデバイスではサイレントインストールが実行されます。）
4. ユーザーはホーム画面からアプリを開きます。アプリの更新猶予期間を設定し、ユーザーが後でアプリをアップグレードするようにタップした場合でも、アプリは直ちにアップグレードされます。（Samsungデバイスではサイレントインストールが実行されます。）

パブリックストアアプリのAndroid必須アプリワークフロー

1. 初期登録時にモバイル生産性アプリを展開します。必須アプリがデバイスにインストールされます。
2. Citrix Endpoint Managementコンソールでアプリを更新します。
3. Citrix Endpoint Managementコンソールを使用して必須アプリを展開します。または、デバイスでCitrix Secure Hubストアを開きます。更新アイコンがストアに表示されます。
4. アプリのアップグレードが自動的に開始されます。（Nexusデバイスはユーザーに更新のインストールを促します。）
5. ホーム画面でアプリを開きます。アプリがアップグレードされます。ユーザーは猶予期間を求められません。（Samsungデバイスはサイレントインストールを実行します。）

必須として構成されているアプリをアンインストールする

必須として構成されているアプリをユーザーがアンインストールできるようにすることができます。**［構成］>［デリバリーグループ］** に移動し、アプリを **［必須アプリ］** から **［オプションアプリ］** に移動します。

推奨： 特定のユーザーがアプリをアンインストールできるように、特別なデリバリーグループを使用してアプリを一時的にオプションに変更します。既存の必須アプリをオプションに変更し、そのデリバリーグループにアプリを展開してから、それらのデバイスからアプリをアンインストー

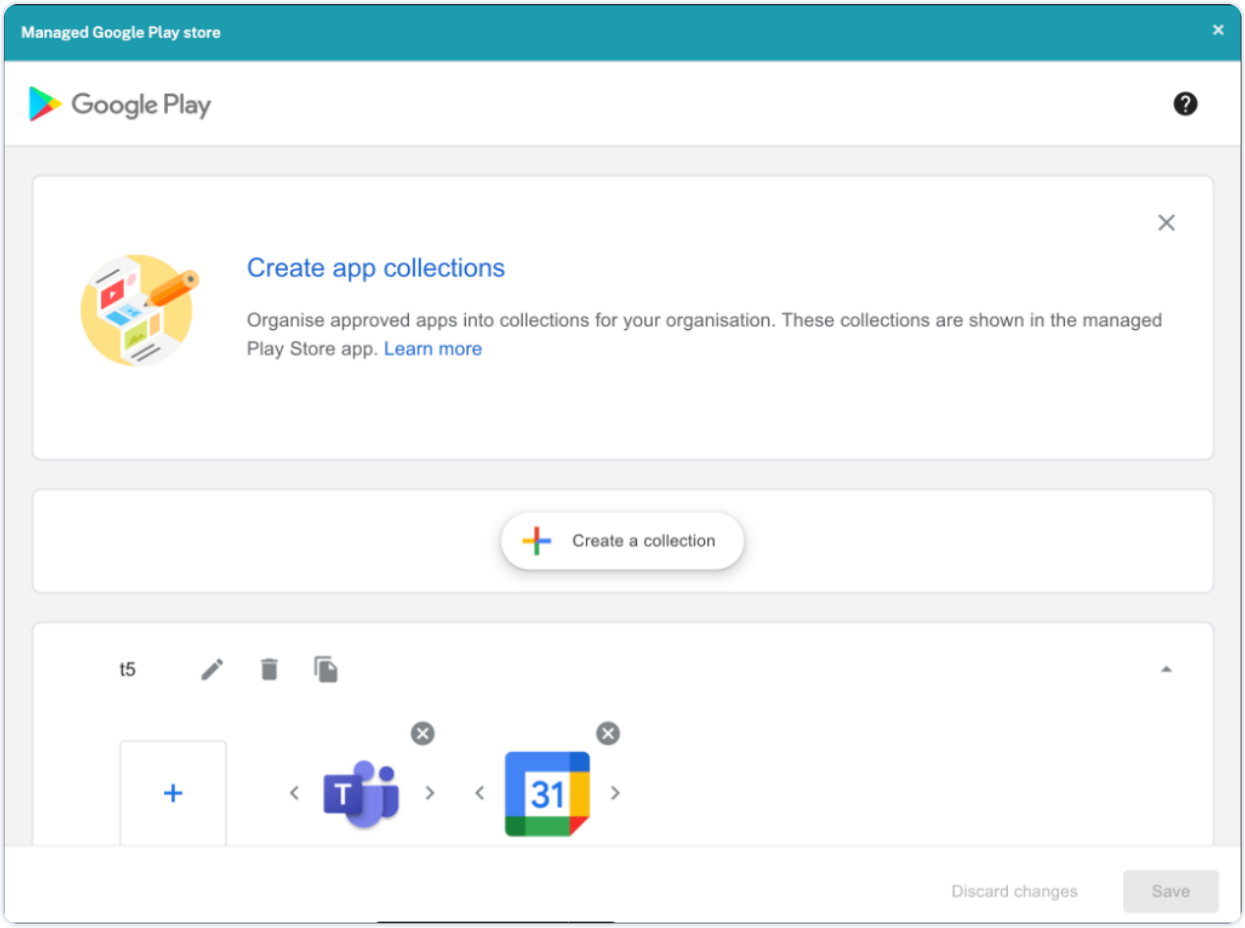
© 1997–2026 Citrix Systems, Inc. All rights reserved.

ルできます。その後、そのデリバリーグループの将来の登録でアプリを必須にする場合は、アプリを必須に戻すことができます。

アプリを整理する（Android Enterprise）

ユーザーがCitrix Secure Hubにログオンすると、Citrix Endpoint Managementで設定したアプリ、Webリンク、ストアのリストが表示されます。Android Enterpriseでは、これらのアプリをコレクションに整理して、ユーザーが特定のアプリ、ストア、またはWebリンクのみにアクセスできるようにすることができます。たとえば、財務コレクションを作成し、財務に関連するアプリのみをそのコレクションに追加します。または、営業アプリを割り当てる営業コレクションを構成することもできます。

1. Citrix Endpoint Managementコンソールで、**［構成］>［アプリ］>［アプリの整理］** をクリックします。**［Managed Google Playストア］** ウィンドウが表示されます。



2. 「**コレクションを作成**」をクリックし、そのコレクションに追加するアプリを選択します。
3. コレクションの追加が完了したら、**［保存］** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

IT管理者は、Managed Google Playウィンドウのコレクションにアプリを追加する前に、そのアプリを承認する必要があります。IT管理者は、`<https://play.google.com/work>`に移動してアプリを承認できます。今後のリリースでは、コレクションにアプリを追加する前に承認する必要はありません。

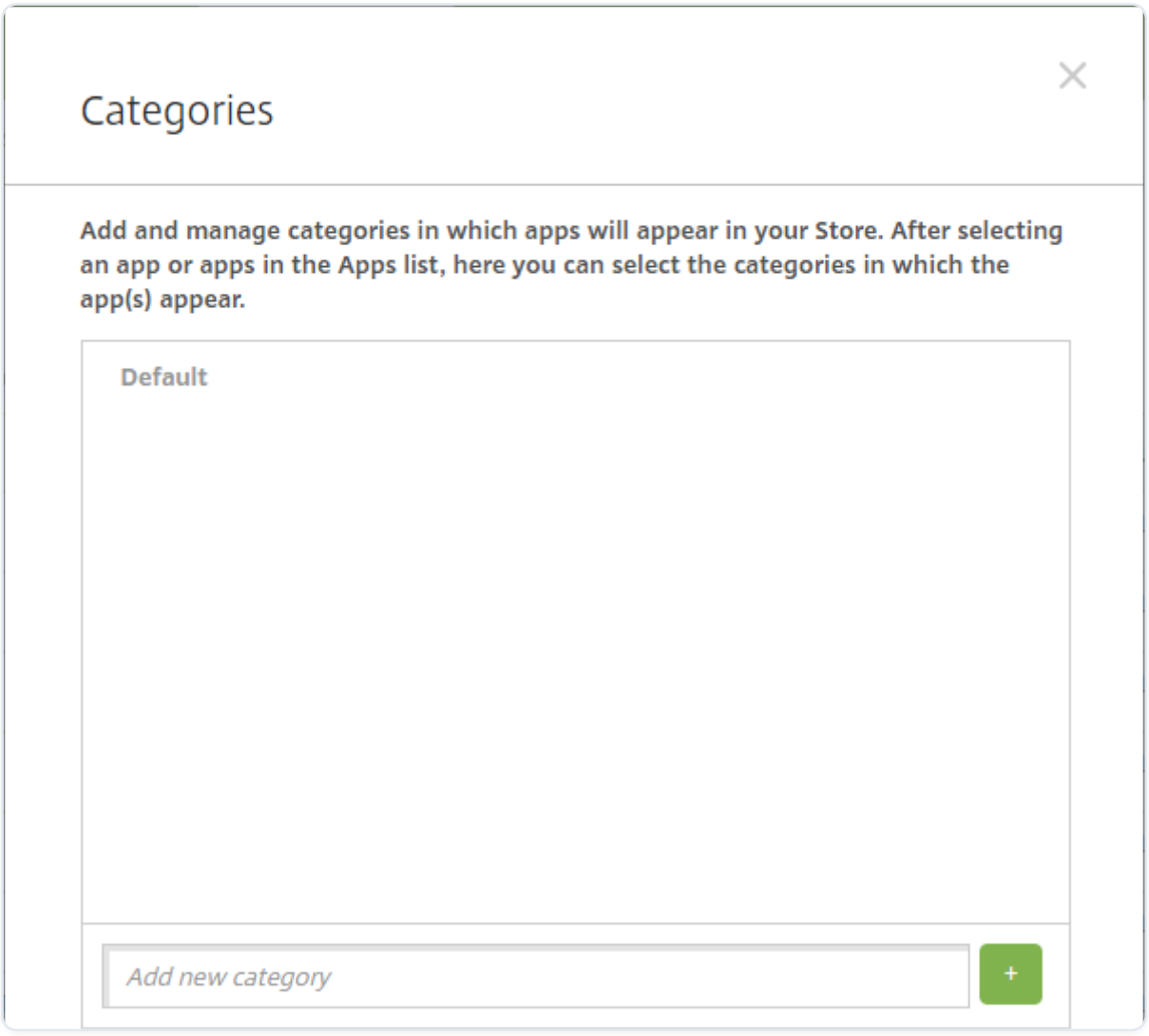
アプリカテゴリについて（iOSおよびMDX）

ユーザーがCitrix Secure Hubにログオンすると、Citrix Endpoint Managementで設定したアプリ、Webリンク、ストアのリストが表示されます。iOSまたはMDXでは、アプリカテゴリを使用して、特定のアプリ、ストア、またはWebリンクのみにユーザーがアクセスできるようにすることができます。たとえば、「財務」カテゴリを作成し、財務に関連するアプリのみをそのカテゴリに追加できます。または、「営業」カテゴリを設定し、営業アプリを割り当てることもできます。

アプリ、Webリンク、またはストアを追加または編集するときに、構成済みのカテゴリの1つ以上にアプリを追加できます。

1. Citrix Endpoint Managementコンソールで、**［構成］>［アプリ］>［カテゴリ］**の順にクリックします。［カテゴリ］**ダイアログボックスが表示されます。

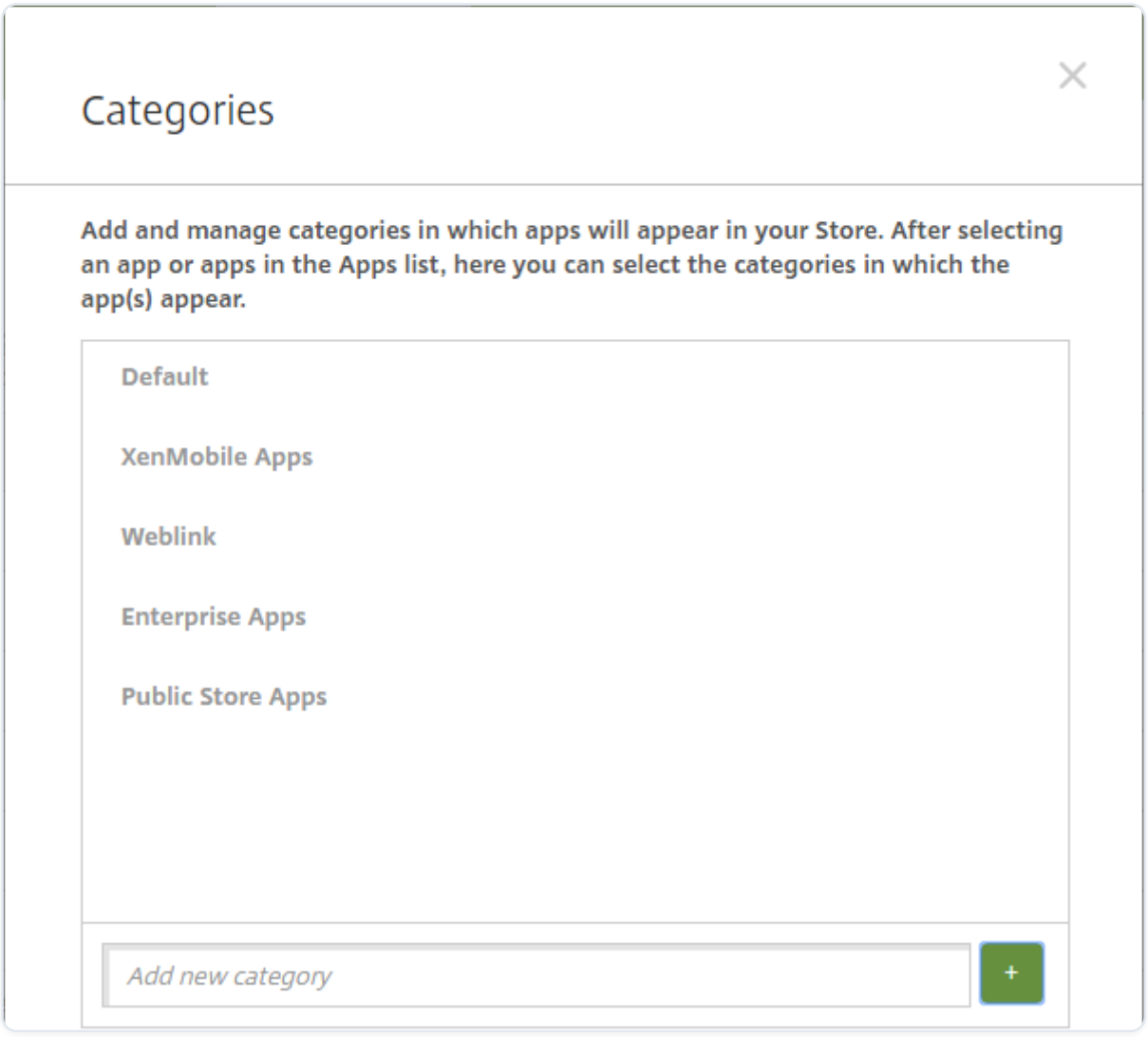
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 追加するカテゴリごとに、次の操作を行います。

   - ダイアログボックスの下部にある**［新しいカテゴリの追加］**フィールドに、追加するカテゴリの名前を入力します。たとえば、「Enterprise Apps」と入力して、エンタープライズアプリのカテゴリを作成できます。
   - プラス記号（+）をクリックしてカテゴリを追加します。新しく作成されたカテゴリが追加され、**［カテゴリ］**ダイアログボックスに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. カテゴリの追加が完了したら、**［カテゴリ］**ダイアログボックスを閉じます。
4. **［アプリ］**ページで、既存のアプリを新しいカテゴリに配置できます。

   - カテゴリ分けするアプリを選択します。
   - **［編集］をクリックします。**［アプリ情報］**ページが表示されます。
   - 「**アプリカテゴリ**」リストで、カテゴリチェックボックスを選択して新しいカテゴリを適用します。アプリに適用したくない既存のカテゴリのチェックボックスはすべてオフにします。
   - **配信グループの割り当て**タブをクリックするか、以降の各ページで**次へ**をクリックして、残りのアプリ設定ページに進みます。
   - **配信グループの割り当て**ページで**保存**をクリックして、新しいカテゴリを適用します。新しいカテゴリはアプリに適用され、**アプリ**テーブルに表示されます。

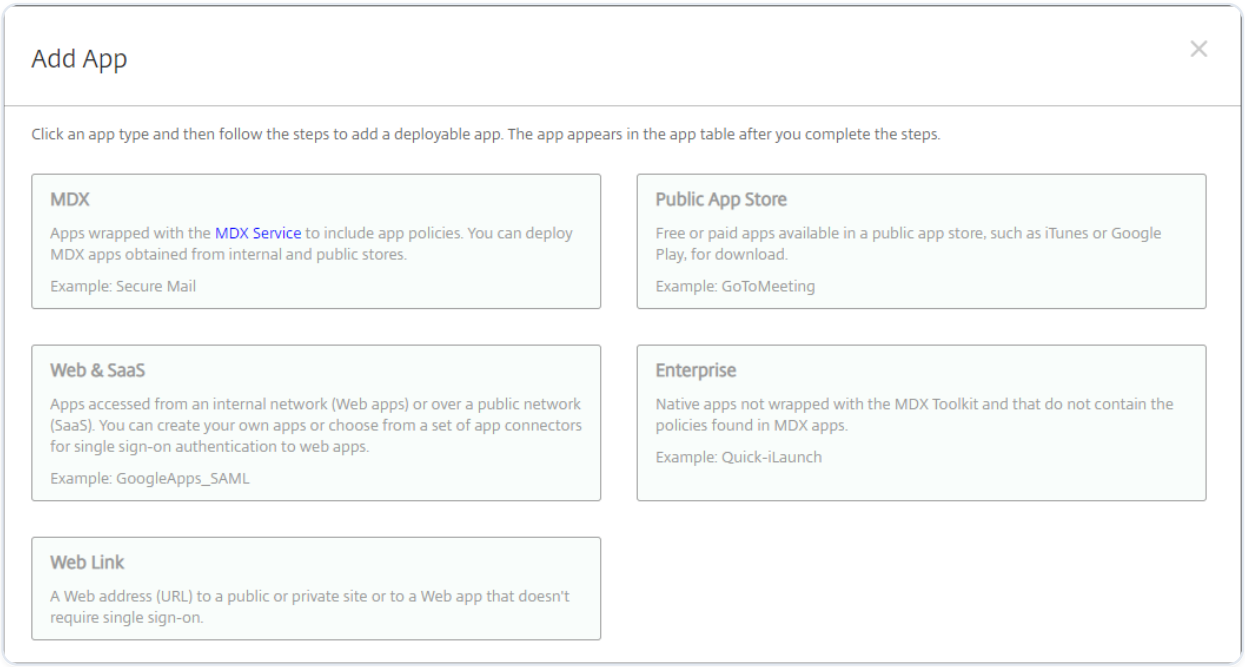
© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDXアプリを追加する

iOSまたはAndroidアプリ用のMDXファイルを受け取ったら、そのアプリをCitrix Endpoint Managementにアップロードできます。アプリをアップロードした後、アプリの詳細とポリシー設定を構成できます。各デバイスプラットフォームタイプで利用可能なアプリポリシーについては、以下を参照してください。

- MAM SDKの概要
- MDXポリシーの概要

1. Citrixモバイル生産性向上アプリの場合は、パブリックストアのMDXファイルをダウンロードします。`<https://www.citrix.com/downloads>`にアクセスします。**Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**に移動します。
2. その他の種類のMDXアプリについては、MDXファイルを入手してください。
3. Citrix Endpoint Managementコンソールで、**構成 > アプリ > 追加**をクリックします。**アプリの追加**ダイアログボックスが表示されます。



4. **MDX**をクリックします。**MDXアプリ情報**ページが表示されます。
5. **アプリ情報**ペインで、次の情報を入力します。
   - **名前:** アプリのわかりやすい名前を入力します。この名前は、**アプリ**テーブルの**アプリ名**の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

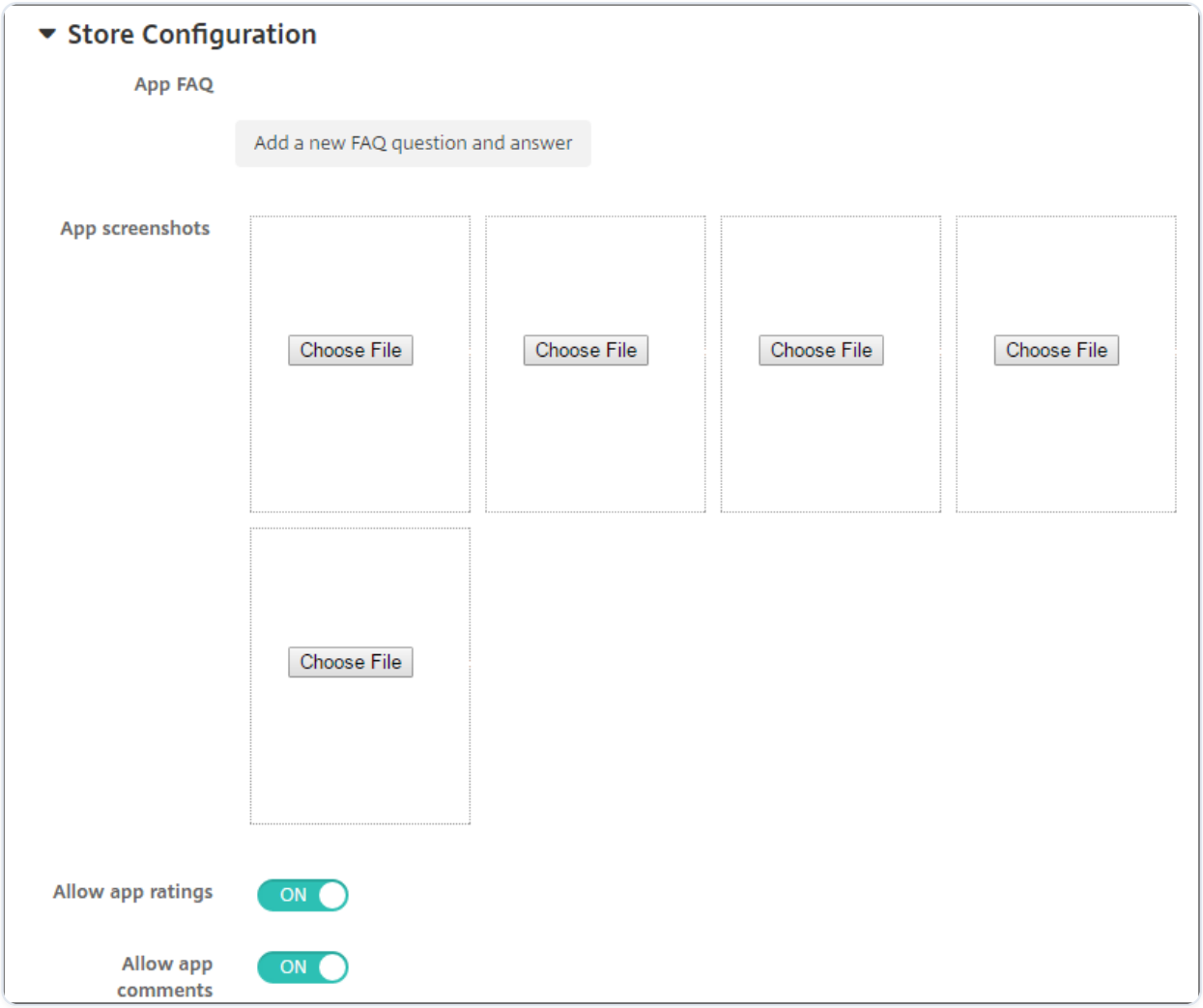
- **アプリカテゴリ:** リストから、アプリを追加するカテゴリを任意でクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。

6. 「**次へ**」をクリックします。「**アプリプラットフォーム**」ページが表示されます。
7. 「**プラットフォーム**」で、追加するプラットフォームを選択します。1つのプラットフォームのみを構成する場合は、他のプラットフォームの選択を解除します。
8. アップロードするMDXファイルを選択するには、「**アップロード**」をクリックしてファイルの場所に移動します。
9. 「**アプリの詳細**」ページで、次の設定を構成します。

- **ファイル名:** アプリに関連付けられているファイル名を入力します。
- **アプリの説明:** アプリの説明を入力します。
- **アプリのバージョン:** 必要に応じて、アプリのバージョン番号を入力します。
- **パッケージID:** 管理対象のGoogle Playストアから、アプリのパッケージIDを入力します。
- **最小OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
- **最大OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
- **除外されるデバイス:** 必要に応じて、アプリを実行できないデバイスの製造元またはモデルを入力します。
- **MDMプロファイルが削除された場合にアプリを削除する:** MDMプロファイルが削除されたときに、iOSデバイスからアプリを削除するかどうかを選択します。デフォルトは「**オン**」です。
- **アプリデータのバックアップを防止する:** ユーザーがiOSデバイスでアプリデータをバックアップするのを防止するかどうかを選択します。デフォルトは「**オン**」です。
- **プロダクトトラック:** iOSデバイスにプッシュするプロダクトトラックを指定します。テスト用に設計されたトラックがある場合は、それを選択してユーザーに割り当てることができます。デフォルトは「**Production**」です。
- **アプリの管理を強制:** 管理対象外としてインストールされるアプリの場合、監視対象外のiOSデバイスでアプリの管理を許可するようユーザーに促すかどうかを選択します。デフォルトは**オン**です。
- **ボリューム購入で展開されるアプリ:** Appleボリューム購入を使用してアプリを展開するかどうかを選択します。**オン**の場合で、アプリのMDXバージョンを展開し、ボリューム購入を使用してアプリを展開すると、Citrix Secure Hubはボリューム購入インスタンスのみを表示します。デフォルトは**オフ**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. **MDXポリシー**を構成します。MDXポリシーはプラットフォームによって異なり、認証、デバイスセキュリティ、アプリ制限などのポリシー領域のオプションが含まれます。コンソールでは、各ポリシーにポリシーを説明するツールヒントがあります。
11. 展開ルールを構成します。詳細については、「展開ルールを構成する」を参照してください。
12. **ストア構成**を展開します。

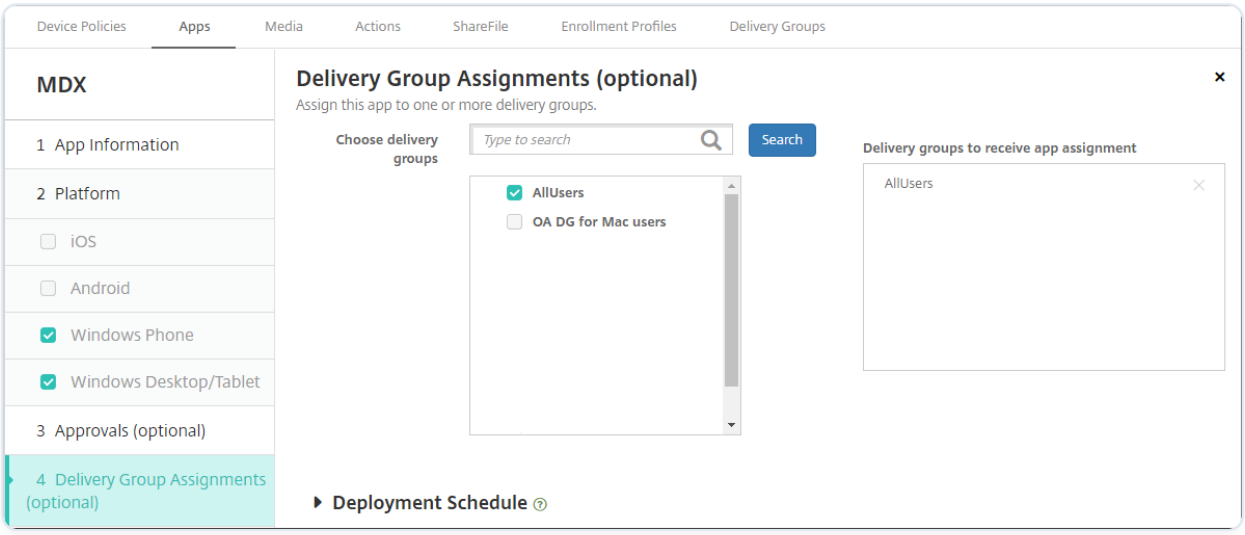


必要に応じて、以下を構成できます。

- **アプリFAQ: 新しいFAQの質問と回答を追加**をクリックして、アプリのFAQを作成します。
- **電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。
- **アプリの評価を許可:** ユーザーがアプリストアでアプリを評価できるようにします。
- **アプリのコメントを許可:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

13. **次へ**をクリックします。**デリバリーグループの割り当て**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



14. **デリバリーグループの選択**の横で、デリバリーグループを検索するためにタイプするか、リストから1つまたは複数のグループを選択します。選択したグループは、**アプリの割り当てを受け取るデリバリーグループ**リストに表示されます。
15. **展開スケジュール**を展開し、次の設定を構成します。

    - **展開:** アプリをデバイスに展開するかどうかを選択します。既定値は**オン**です。
    - **展開スケジュール:** アプリを**今すぐ**展開するか、**後で**展開するかを選択します。「**後で**」を選択した場合は、アプリを展開する日付と時刻を設定します。既定値は**今すぐ**です。
    - **展開条件:** デバイスが接続するたびにアプリを展開するには、「**接続ごとに**」を選択します。以前にデバイスがアプリを受信できなかった場合にアプリを展開するには、「**以前の展開が失敗した場合のみ**」を選択します。既定値は**接続ごとに**です。

    常時接続用に展開オプションは、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

    常時接続オプションは次のとおりです。

    - iOSデバイスでは利用できません
    - バージョン10.18.19以降でCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様は利用できません
    - バージョン10.18.19より前にCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様には推奨されません

    構成する展開スケジュールは、すべてのプラットフォームで同じです。行った変更は、**常時接続用に展開**を除き、すべてのプラットフォームに適用されます。
16. **保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パブリックアプリストアアプリを追加する

Apple App Storeなどのパブリックアプリストアで利用可能な無料または有料のアプリをCitrix Endpoint Managementに追加できます。

Apple App Storeからアプリ名と説明を取得するように設定を構成できます。ストアからアプリ情報を取得すると、Citrix Endpoint Managementは既存の名前と説明を上書きします。Google Playストアのアプリ情報は手動で構成してください。

注:

Android Enterprise Managed Google Playを介したAndroid向け有料アプリは、Googleによってサポートされなくなりました。詳細については、Managed Google Playヘルプドキュメントを参照してください。

アプリ情報を構成し、アプリを配信するプラットフォームを選択します。

1. Citrix Endpoint Managementコンソールで、 **> >** の順にクリックします。 ダイアログボックスが表示されます。

   アプリ構成画面(/en-us/citrix-endpoint-management/media/configure-apps-add.png)
2. をクリックします。 ページが表示されます。
3. ペインで、次の情報を入力します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、 テーブルの の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。
4. をクリックします。 ページが表示されます。
5. で、追加するプラットフォームを選択します。1つのプラットフォームのみを構成する場合は、他のプラットフォームの選択を解除します。

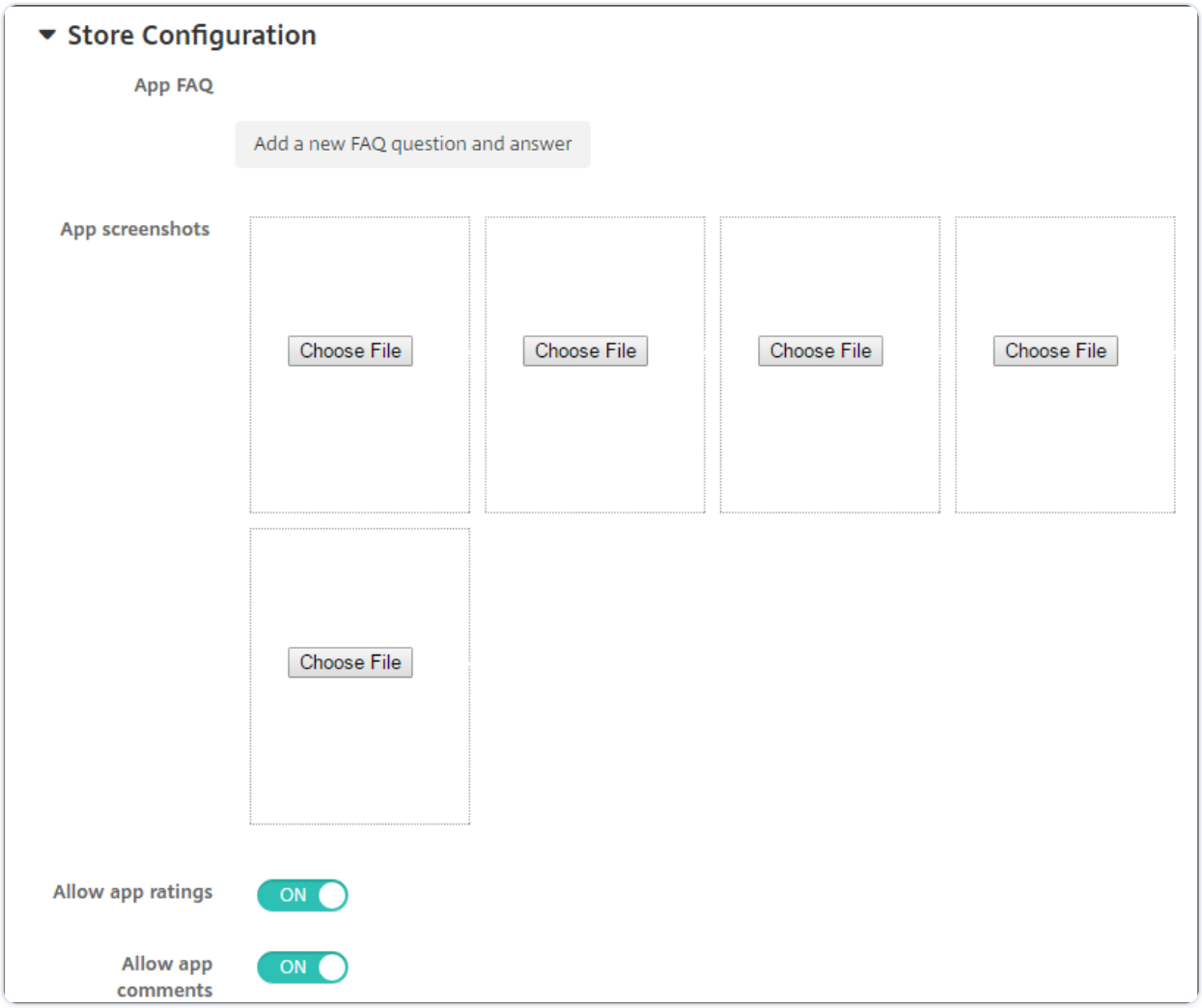
次に、各プラットフォームのアプリ設定を構成します。参照:

- Google Playアプリのアプリ設定を構成する
- 管理対象アプリストアアプリ
- iOSアプリのアプリ設定を構成する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プラットフォームの設定の構成が完了したら、プラットフォームの展開ルールとアプリストア構成を設定します。

1. デプロイ規則を構成します。詳細については、「デプロイ規則の構成」を参照してください。
2. **Store Configuration**を展開します。



必要に応じて、以下を構成できます。

- **App FAQ: Add a new FAQ question and answer**をクリックして、アプリのFAQを作成します。
- **Add screenshots for phones/tablets:** アプリストアに表示されるスクリーンショットを追加します。
- **Allow app ratings:** ユーザーがアプリストアでアプリを評価できるようにします。
- **Allow app comments:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

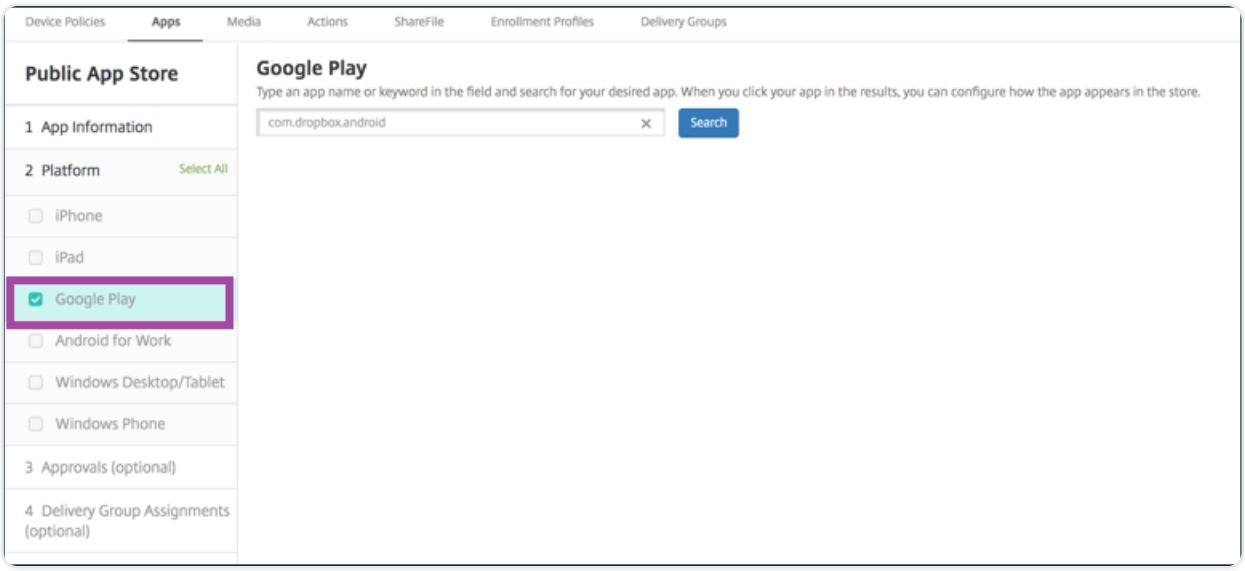
Google Playアプリのアプリ設定を構成する

注：

管理対象Google PlayからGoogle Playストアのすべてのアプリにアクセスできるようにするには、**Access all apps in the managed Google Play store**サーバープロパティを使用します。(「サーバープロパティ」を参照してください。) このプロパティを**true**に設定すると、すべてのAndroid Enterpriseユーザーが公開Google Playストアアプリにアクセスできるようになります。その後、制限デバイスポリシーを使用して、これらのアプリへのアクセスを制御できます。

Google Playストアアプリの設定を構成するには、他のプラットフォームのアプリとは異なる手順が必要です。Google Playストアアプリの情報を手動で構成します。

1. **Platforms**の下で**Google Play**が選択されていることを確認します。



2. Google Playストアに移動します。Google PlayストアからパッケージIDをコピーします。IDはアプリのURLにあります。

   「アプリを検索中」(/en-us/citrix-endpoint-management/media/app-id-search1.png)

3. Citrix Endpoint Managementコンソールでパブリックストアアプリを追加する場合、検索バーにパッケージIDを貼り付けます。**検索**をクリックします。

   「アプリを検索中」(/en-us/citrix-endpoint-management/media/app-id-search2.png)

4. パッケージIDが有効な場合、アプリの詳細を入力できるUIが表示されます。

   「アプリを検索中」(/en-us/citrix-endpoint-management/media/app-id-search3.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. ストアでアプリと一緒に表示される画像のURLを構成できます。Google Playストアの画像を使用するには：

   a. Google Playストアにアクセスします。アプリの画像を右クリックし、画像アドレスをコピーします。

   b. 画像アドレスを**画像URL**フィールドに貼り付けます。

   c. **画像をアップロード**をクリックします。画像が**画像**の横に表示されます。

画像を構成しない場合、汎用Android画像がアプリとともに表示されます。

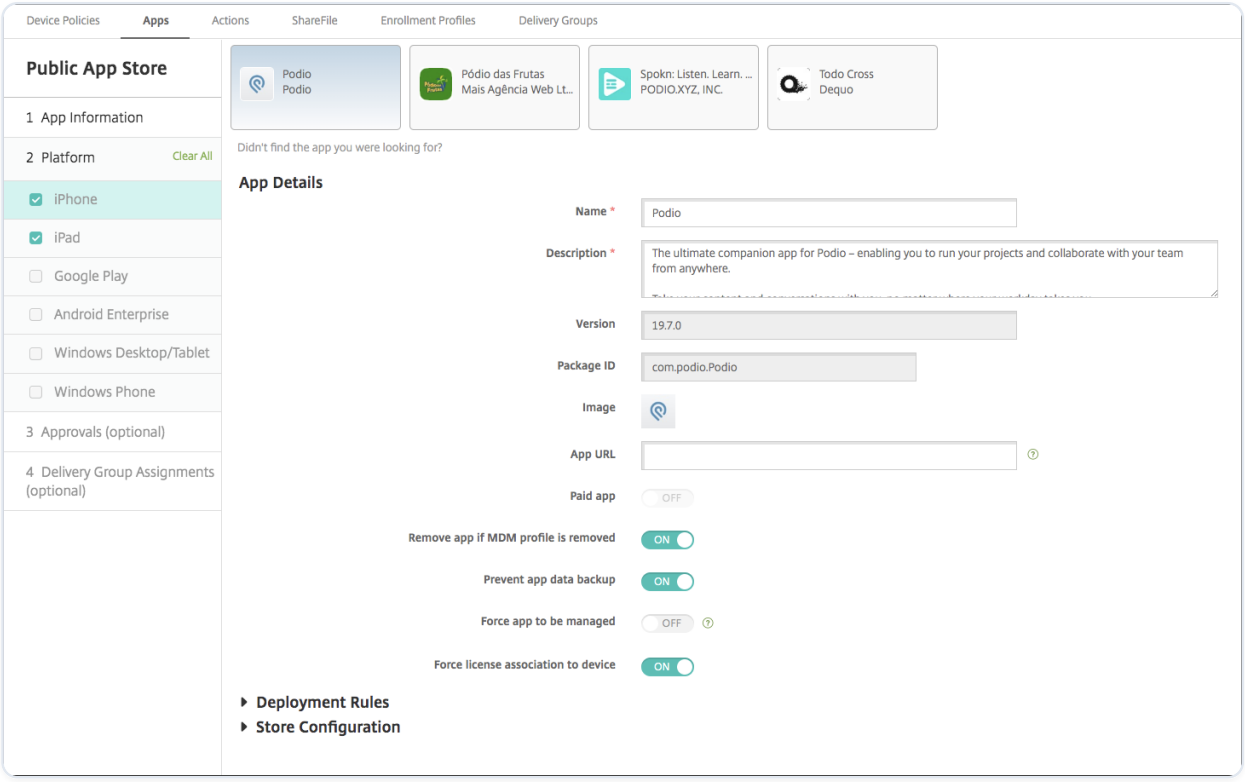
iOSアプリのアプリ設定を構成する

1. 検索ボックスにアプリ名を入力し、**検索**をクリックします。検索条件に一致するアプリが表示されます。検索条件に一致するアプリが表示されます。

   次の図は、iPhoneのアプリで**podio**を検索した結果を示しています。

   「アプリ構成画面」(/en-us/citrix-endpoint-management/media/configure-apps-search-public-app-store.png)

2. 追加したいアプリをクリックします。
3. 「**アプリの詳細**」フィールドには、選択したアプリに関連する情報（名前、説明、バージョン番号、関連画像など）が事前に入力されます。



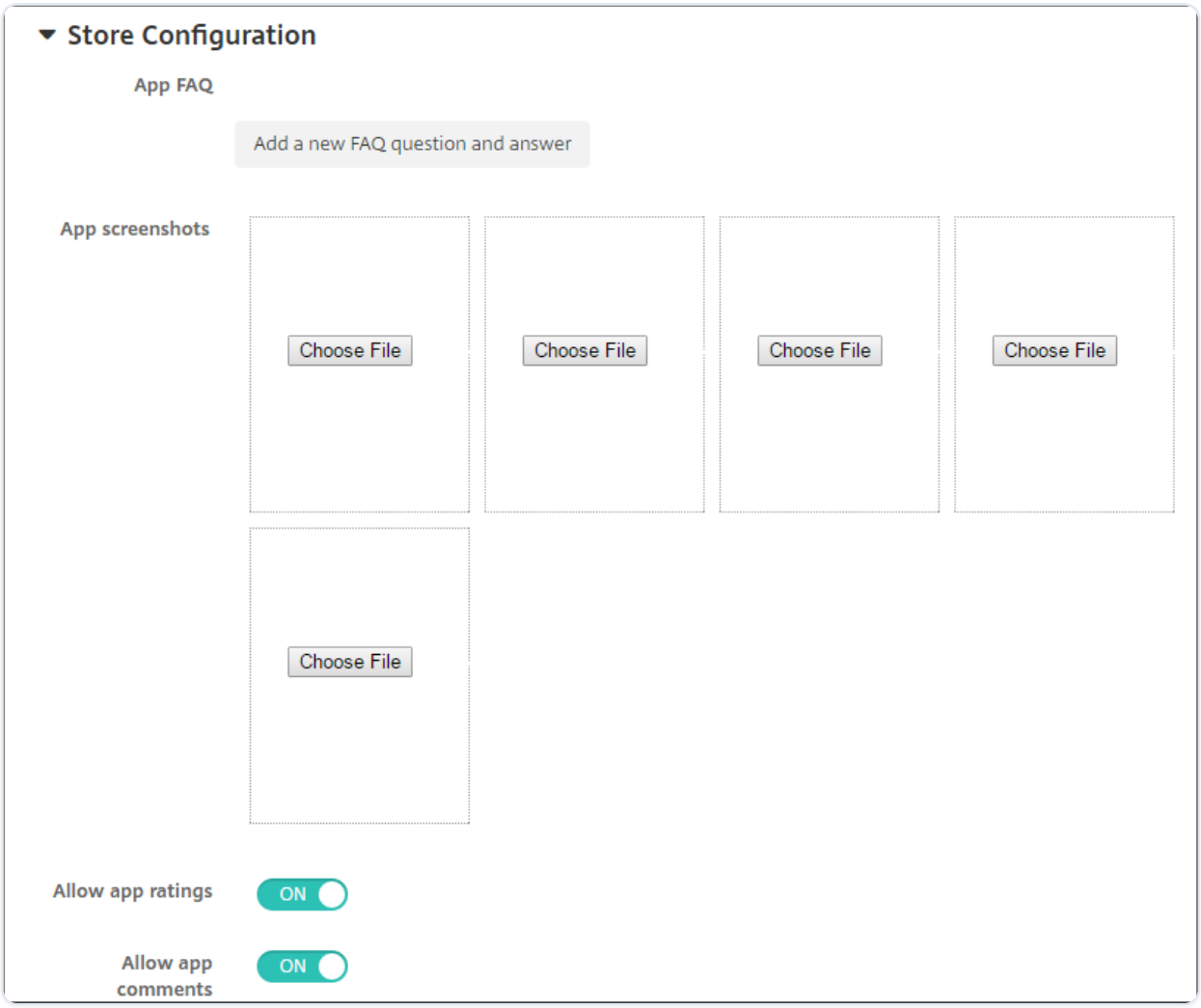
4. 設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 必要に応じて、アプリの名前と説明を変更します。
- **アプリのURL:** Citrix Workspaceアプリからアプリを起動するためのURLをコンマ区切りで入力します。このフィールドは、iPhoneおよびiPadデバイスでのみ使用できます。
- **有料アプリ:** このフィールドは事前構成されており、変更できません。
- **MDMプロファイルが削除された場合にアプリを削除:** MDMプロファイルが削除された場合にアプリを削除するかどうかを選択します。デフォルトは**オン**です。
- **アプリのデータバックアップを防止:** アプリがデータをバックアップするのを防止するかどうかを選択します。デフォルトは**オン**です。
- **製品トラック:** ユーザーデバイスにプッシュする製品トラックを指定します。テスト用に設計されたトラックがある場合は、それを選択してユーザーに割り当てることができます。デフォルトは**本番**です。
- **アプリの管理を強制:** 管理対象外としてインストールされるアプリの場合、監視対象外のiOSデバイスでアプリの管理を許可するようにユーザーにプロンプトを表示するかどうかを選択します。デフォルトは**オフ**です。ユーザー登録を通じて登録されたiOSデバイスの場合、Citrix Endpoint Managementはこの設定を適用せず、アプリの管理を許可するようにユーザーにプロンプトを表示しません。
- **ライセンスをデバイスに関連付けることを強制:** アプリ（デバイス関連付けが有効な状態で開発されたもの）をユーザーではなくデバイスに関連付けるかどうかを選択します。選択したアプリがデバイスへの割り当てをサポートしていない場合、この設定は変更できません。

5. 展開ルールを構成します。詳しくは、「展開ルールの構成」を参照してください。
6. **ストア構成**を展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



必要に応じて、以下を構成できます。

- **アプリのFAQ: 新しいFAQの質問と回答を追加**をクリックして、アプリのFAQを作成します。
- **電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。
- **アプリの評価を許可:** ユーザーがアプリストアでアプリを評価できるようにします。
- **アプリのコメントを許可:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

7. iPhoneまたはiPadの場合、「**ボリューム購入**」を展開します。

   a. Citrix Endpoint Managementでアプリのボリューム購入ライセンスを適用できるようにするには、「**ボリューム購入ライセンス**」リストで「**ボリューム購入ライセンスをアップロード**」をクリックします。

   b. 表示されるダイアログボックスで、ライセンスをインポートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンス割り当てテーブルには、利用可能な合計ライセンス数に対して、アプリで使用中のライセンス数が表示されます。

個々のユーザーのボリューム購入ライセンスの関連付けを解除できます。これにより、ライセンス割り当てが終了し、ライセンスが解放されます。

c. ボリューム購入アカウントを追加するときに、「**アプリの自動更新**」を有効にします。この設定により、Apple Storeでアップデートが利用可能になったときに、ユーザーデバイス上のアプリが自動的に更新されるようになります。アプリで「**アプリの管理を強制**」設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。この更新は、アプリが必須であるかオプションであるかに関わらず行われます。

8. 「**ボリューム購入**」設定を完了したら、「**次へ**」をクリックします。「**承認**」ページが表示されます。

ワークフローを使用して、ユーザーがアプリにアクセスする前に承認を要求するには、「ワークフローの適用」を参照してください。承認ワークフローが不要な場合は、次の手順に進みます。

9. 「**次へ**」をクリックします。「**デリバリーグループの割り当て**」ページが表示されます。
10. 「**デリバリーグループの選択**」の横で、デリバリーグループを検索するためにタイプ入力するか、リストから1つまたは複数のグループを選択します。選択したグループは、「**アプリの割り当てを受け取るデリバリーグループ**」リストに表示されます。
11. 「**展開スケジュール**」を展開し、次の設定を構成します。

- **展開:** アプリをデバイスに展開するかどうかを選択します。デフォルトは**オン**です。
- **展開スケジュール:** アプリを**今すぐ**展開するか、**後で**展開するかを選択します。**後で**を選択した場合は、アプリを展開する日時を設定します。デフォルトは**今すぐ**です。
- **展開条件:** デバイスが接続するたびにアプリを展開するには、**接続ごとに**を選択します。以前の展開が失敗した場合にのみアプリを展開するには、**以前の展開が失敗した場合のみ**を選択します。デフォルトは**接続ごとに**です。

常時接続用に展開オプションは、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

常時接続オプション:

- iOSデバイスでは利用できません
- バージョン10.18.19以降でCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様は利用できません

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- バージョン10.18.19より前にCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様には推奨されません

構成する展開スケジュールは、すべてのプラットフォームで同じです。行った変更は、**常時接続用に展開**を除き、すべてのプラットフォームに適用されます。

12. **保存**をクリックします。

WebアプリまたはSaaSアプリを追加する

Citrix Endpoint Managementコンソールを使用して、エンタープライズ、Web、SaaSアプリへのシングルサインオン (SSO) 認証をユーザーに付与できます。

WebアプリまたはSaaSアプリを追加する際に、Citrix Endpoint Managementで独自のコネクタを構築できます。Citrix Endpoint Managementで利用可能なコネクタタイプの一覧については、「アプリケーションコネクタの種類」を参照してください。

アプリがSSOのみで利用可能な場合: 設定を保存すると、Citrix Endpoint Managementコンソールの**アプリ**タブにアプリが表示されます。

1. Citrix Endpoint Managementコンソールで、**構成 > アプリ > 追加**をクリックします。**アプリの追加**ダイアログボックスが表示されます。

   「アプリ構成画面」(/en-us/citrix-endpoint-management/media/configure-apps-add.png)

2. **Web & SaaS**をクリックします。**App Information**ページが表示されます。

   「アプリ構成画面」(/en-us/citrix-endpoint-management/media/configure-apps-web-saas.png)

3. 既存または新規のアプリコネクタを次のように構成します。

既存のアプリコネクタを構成するには

1. **App Information**ページで、**Choose from existing connectors**がすでに選択されています（前述のとおり）。**App Connectors**リストで、使用するコネクタをクリックします。アプリコネクタ情報が表示されます。
2. 次の設定を構成します。

   - **アプリ名:** 事前入力された名前を受け入れるか、新しい名前を入力します。
   - **アプリの説明:** 事前入力された説明を受け入れるか、独自の説明を入力します。
   - **URL:** 事前入力されたURLを受け入れるか、アプリのWebアドレスを入力します。選択したコネクタによっては、このフィールドにプレースホルダーが含まれている場合があり、次のページに進む前に置き換える必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ドメイン名:** 該当する場合、アプリのドメイン名を入力します。このフィールドは必須です。
- **アプリは内部ネットワークでホストされています:** アプリが内部ネットワーク内のサーバーで実行されているかどうかを選択します。ユーザーがリモートの場所から内部アプリに接続する場合、NetScaler Gatewayを介して接続する必要があります。このオプションを**On**に設定すると、アプリにVPNキーワードが追加され、ユーザーはNetScaler Gatewayを介して接続できるようになります。デフォルトは**Off**です。
- **アプリカテゴリ:** ドロップダウンリストからオプションのカテゴリをクリックして、アプリに適用します。
- **ユーザーアカウントプロビジョニング:** アプリのユーザーアカウントを作成するかどうかを選択します。Globoforce_SAMLコネクタを使用する場合、シームレスなSSO統合を提供するには、このオプションを有効にする必要があります。
- **ユーザーアカウントプロビジョニング**を有効にする場合は、次の設定を構成します。
  - **サービスアカウント**
    - **ユーザー名:** アプリケーション管理者の名前を入力します。このフィールドは必須です。
    - **パスワード:** アプリケーション管理者のパスワードを入力します。このフィールドは必須です。
  - **ユーザーアカウント**
    - **ユーザーエンタイトルメントの終了時:** ユーザーがアプリへのアクセスを許可されなくなったときに実行するアクションをドロップダウンリストからクリックします。デフォルトは**アカウントを無効にする**です。
  - **ユーザー名ルール**
    - 追加するユーザー名ルールごとに、次の操作を行います。
      - **ユーザー属性:** ドロップダウンリストからルールに追加するユーザー属性をクリックします。
      - **長さ (文字数):** ユーザー名ルールで使用するユーザー属性の文字数をドロップダウンリストからクリックします。デフォルトは**すべて**です。
      - **ルール:** 追加する各ユーザー属性は、ユーザー名ルールに自動的に追加されます。
- **パスワード要件**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **長さ:** ユーザーパスワードの最小長を入力します。デフォルトは**8**です。

- **パスワードの有効期限**

    - **有効期間 (日数):** パスワードが有効な日数を入力します。有効な値は**0〜90**です。デフォルトは90です。
    - **有効期限が切れた後にパスワードを自動的にリセットする:** パスワードの有効期限が切れたときに自動的にリセットするかどうかを選択します。デフォルトは**オフ**です。このフィールドを有効にしない場合、ユーザーはパスワードの有効期限が切れた後にアプリを開くことができません。

新しいアプリコネクタを構成するには

1. **App Information**ページで、**Create a new connector**を選択します。アプリコネクタのフィールドが表示されます。

   アプリ構成画面(/en-us/citrix-endpoint-management/media/configure-apps-web-saas-add-app-connector.png)

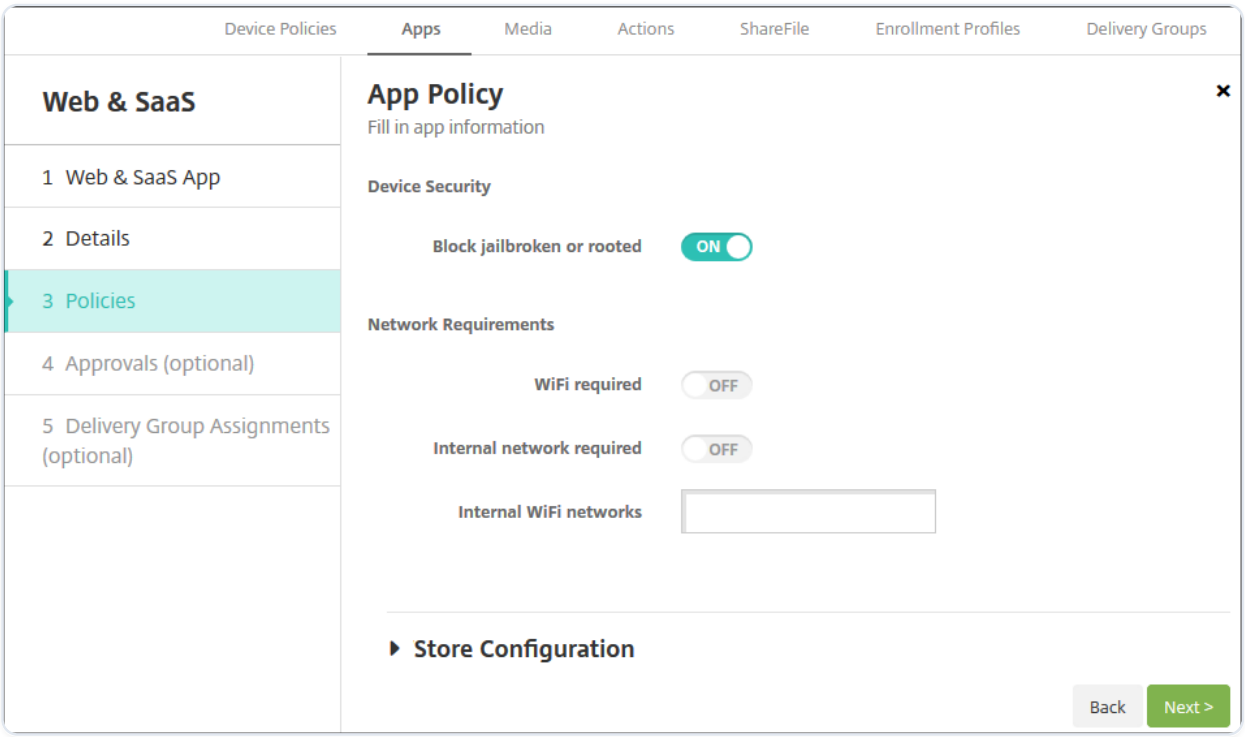
2. 次の設定を構成します。

    - **名前:** コネクタの名前を入力します。このフィールドは必須です。
    - **説明:** コネクタの説明を入力します。このフィールドは必須です。
    - **ログオンURL:** ユーザーがサイトにログオンするURLを入力またはコピーして貼り付けます。たとえば、追加するアプリにログオンページがある場合、Webブラウザを開いてそのアプリのログオンページに移動します。例えば、`https://www.example.com/logon`のようになります。このフィールドは必須です。
    - **SAMLバージョン: 1.1**または**2.0**のいずれかを選択します。デフォルトは**1.1**です。
    - **エンティティID:** SAMLアプリのIDを入力します。
    - **リレーステートURL:** SAMLアプリケーションのWebアドレスを入力します。リレーステートURLは、アプリからの応答URLです。
    - **名前ID形式: Email Address**または**Unspecified**のいずれかを選択します。デフォルトは**Email Address**です。
    - **ACS URL:** IDプロバイダーまたはサービスプロバイダーのアサーションコンシューマーサービスURLを入力します。ACS URLは、ユーザーにSSO機能を提供します。
    - **画像:** デフォルトのCitrix画像を使用するか、独自のアプリ画像をアップロードするかを選択します。デフォルトは「デフォルトを使用」です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 独自の画像をアップロードするには、**参照**をクリックしてファイルの場所に移動します。ファイルは.PNGファイルである必要があります。JPEGまたはGIFファイルはアップロードできません。カスタムグラフィックを追加すると、後で変更することはできません。

3. 完了したら、**追加**をクリックします。**詳細**ページが表示されます。
4. 「**次へ**」をクリックします。「**アプリポリシー**」ページが表示されます。

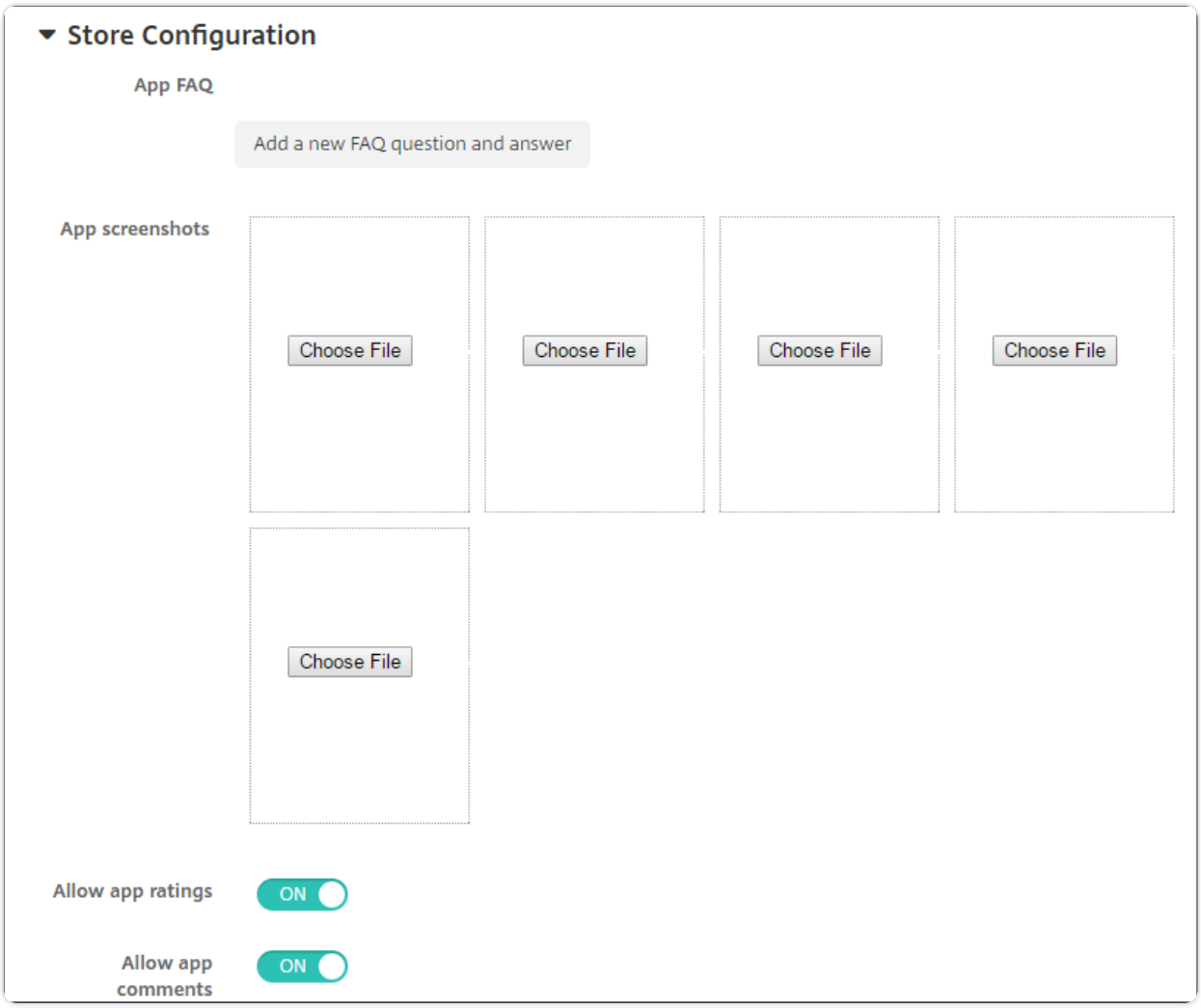


5. 次の設定を構成します。

- **デバイスセキュリティ**
- **ジェイルブレイクまたはルート化されたデバイスをブロック:** ジェイルブレイクまたはルート化されたデバイスがアプリにアクセスするのをブロックするかどうかを選択します。デフォルトは**オン**です。
- **ネットワーク要件**
- **Wi-Fi必須:** アプリを実行するためにWi-Fi接続が必要かどうかを選択します。デフォルトは**オフ**です。
- **内部ネットワーク必須:** アプリを実行するために内部ネットワークが必要かどうかを選択します。デフォルトは**オフ**です。
- **内部Wi-Fiネットワーク: Wi-Fi必須**を有効にした場合は、使用する内部Wi-Fiネットワークを入力します。

6. 「**ストア構成**」を展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

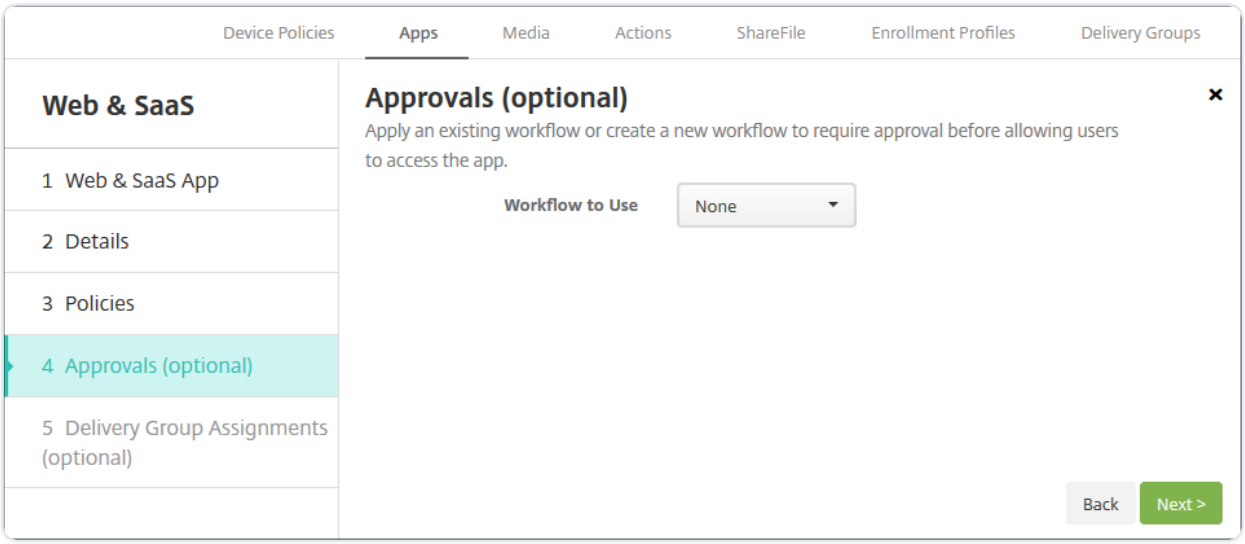


必要に応じて、次の項目を構成できます。

- **アプリFAQ:** アプリのFAQを作成するには、「**新しいFAQの質問と回答を追加**」をクリックします。
- **電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。
- **アプリの評価を許可:** ユーザーがアプリストアでアプリを評価できるようにします。
- **アプリのコメントを許可:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

7. **次へ**をクリックします。**承認**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



ユーザーがアプリにアクセスする前に承認を要求するワークフローを使用するには、「ワークフローの適用」を参照してください。承認ワークフローが不要な場合は、次の手順に進みます。

8. **次へ**をクリックします。**デリバリーグループの割り当て**ページが表示されます。
9. **デリバリーグループの選択**の横で、デリバリーグループを検索するためにタイプ入力するか、1つまたは複数のグループを選択します。選択したグループは、**アプリの割り当てを受け取るデリバリーグループ**リストに表示されます。
10. **展開スケジュール**を展開し、次の設定を構成します。

    - **展開:** デバイスにアプリを展開するかどうかを選択します。デフォルトは**オン**です。
    - **展開スケジュール:** アプリを**今すぐ**展開するか、**後で**展開するかを選択します。**後で**を選択した場合は、アプリを展開する日付と時刻を構成します。デフォルトは**今すぐ**です。
    - **展開条件:** デバイスが接続するたびにアプリを展開するには、**接続ごとに**を選択します。以前にデバイスがアプリの受信に失敗した場合にアプリを展開するには、**以前の展開が失敗した場合のみ**を選択します。デフォルトは**接続ごとに**です。

    常時接続用に展開オプションは、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

    常時接続オプションは次のとおりです。

    - iOSデバイスでは利用できません
    - バージョン10.18.19以降でCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様は利用できません
    - バージョン10.18.19より前にCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様には推奨されません

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成する展開スケジュールはすべてのプラットフォームで同じです。**Deploy for always-on connection** を除き、加えた変更はすべてのプラットフォームに適用されます。

11. **保存**をクリックします。

エンタープライズアプリを追加する

Citrix Endpoint Management のエンタープライズアプリは、開発した、または他のソースから取得したプライベートアプリです。MDX対応アプリとして配信されるプライベートなAndroid Enterpriseアプリを除き、エンタープライズアプリはMAM SDKまたはMDX Toolkitで準備されません。Citrix Endpoint Management コンソールの**アプリ**タブでエンタープライズアプリをアップロードできます。エンタープライズアプリは、以下のプラットフォーム（および対応するファイルタイプ）をサポートしています。

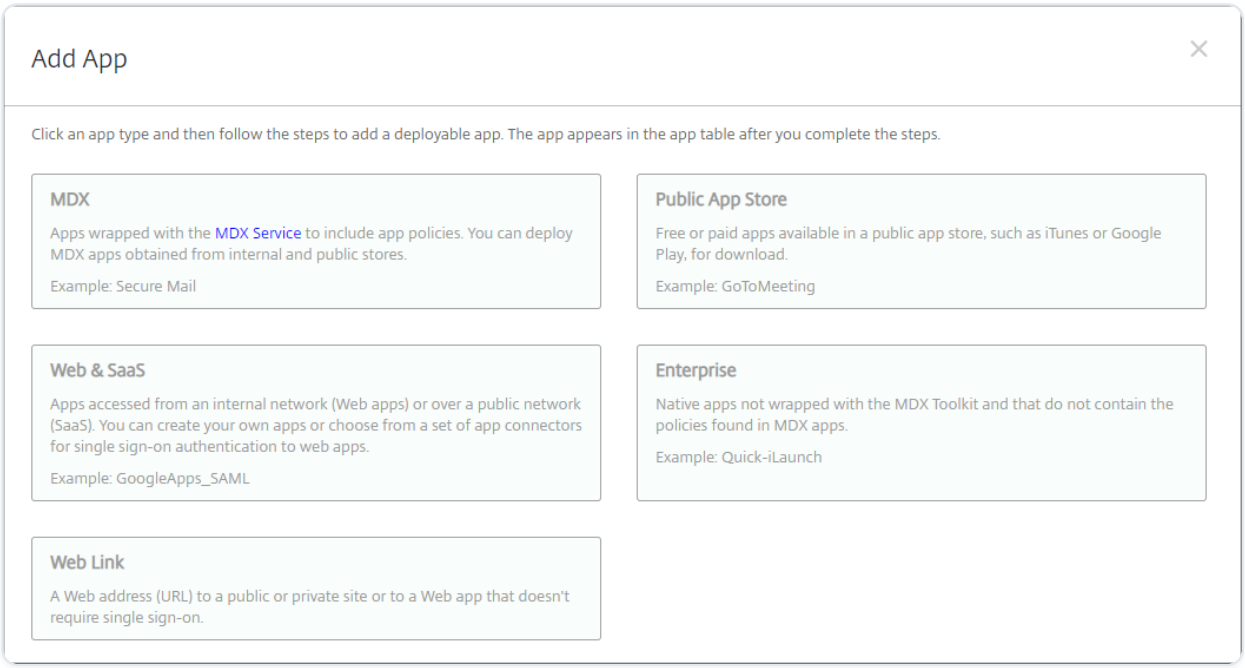
- iOS (.ipa ファイル)
- macOS (.pkg ファイル)

  Citrix Endpoint Management は、アップロードするPKGファイルのサイズを制限しませんが、ファイルのアップロード時間を制限します。デフォルトでは、100秒以内にアップロードを完了する必要があります。詳細については、「サーバープロパティ」を参照してください。
- Android (.apk ファイル)
- Android Enterprise (.apk ファイル)
- 関連項目: Win32アプリをエンタープライズアプリとして追加する
- 関連項目: MDX対応プライベートアプリ

Google Playストアからダウンロードしたアプリをエンタープライズアプリとして追加することはサポートされていません。代わりに、Google Playストアのアプリをパブリックアプリストアアプリとして追加してください。パブリックアプリストアアプリを追加するを参照してください。

1. Citrix Endpoint Management コンソールで、**構成 > アプリ > 追加**をクリックします。**アプリの追加**ダイアログボックスが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. **エンタープライズ**をクリックします。**アプリ情報**ページが表示されます。
3. 「**アプリ情報**」ペインで、次の情報を入力します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルの「アプリ名」の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。

4. **次へ**をクリックします。「**アプリプラットフォーム**」ページが表示されます。
5. **プラットフォーム**で、追加するプラットフォームを選択します。1つのプラットフォームのみを設定する場合は、他のプラットフォームの選択を解除します。
6. 選択した各プラットフォームについて、**アップロード**をクリックしてファイルの場所に移動し、アップロードするファイルを選択します。
7. **次へ**をクリックします。プラットフォームのアプリ情報ページが表示されます。
8. 次のようなプラットフォームタイプの構成を設定します。

   - **ファイル名:** オプションで、アプリの新しい名前を入力します。
   - **アプリの説明:** オプションで、アプリの新しい説明を入力します。
   - **アプリバージョン:** このフィールドは変更できません。
   - **最小OSバージョン:** オプションで、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **最大OSバージョン:** オプションで、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
- **除外デバイス:** オプションで、アプリを実行できないデバイスの製造元またはモデルを入力します。
- **パッケージID:** アプリの一意の識別子。
- **MDMプロファイルが削除された場合にアプリを削除する:** MDMプロファイルが削除されたときに、デバイスからアプリを削除するかどうかを選択します。デフォルトは**オン**です。この設定はmacOSには適用されません。
- **アプリデータのバックアップを防止する:** アプリがデータをバックアップするのを防止するかどうかを選択します。デフォルトは**オン**です。この設定はmacOSには適用されません。
- **アプリを強制的に管理対象にする:** 監視対象外のデバイスにアプリを管理対象アプリとしてインストールするかどうかを選択します。デバイスの種類によって、この設定が有効になっている場合のCitrix Endpoint Managementによる処理方法が決まります。この設定を有効にすると、ユーザーにプロンプトを表示せずにアプリが更新されます。更新は、アプリが必要かオプションかに関わらず行われます。デフォルトは**オフ**です。
  - iOSデバイスの場合、アプリがすでにインストールされていると、ユーザーはアプリの管理を許可するよう求めるプロンプトを受け取ります。アプリが存在しないデバイスにアプリを展開すると、この設定の状態に関わらず、アプリは管理対象アプリとしてインストールされます。iOS 9.0以降で利用可能です。ユーザー登録を通じて登録されたiOSデバイスの場合、Citrix Endpoint Managementはこの設定を適用せず、ユーザーにアプリ管理を許可するよう求めるプロンプトも表示しません。
  - macOSデバイスの場合、設定を有効にしてから、アプリをデバイスに展開します。アプリは自動的に管理対象アプリとしてインストールされます。ユーザーにプロンプトは表示されません。アプリが存在しないデバイスにアプリを展開すると、この設定の状態に関わらず、アプリは管理対象アプリとしてインストールされます。macOS 11.0以降で利用可能です。

9. 展開ルールを構成します。詳細については、「展開ルールの構成」を参照してください。
10. **Store Configuration**を展開します。

    アプリ構成画面(/en-us/citrix-endpoint-management/media/configure-apps-store-configuration.png)

    必要に応じて、以下を構成できます。

    - **アプリFAQ: 新しいFAQの質問と回答を追加**をクリックして、アプリのFAQを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。
- **アプリの評価を許可する:** ユーザーがアプリストアでアプリを評価できるようにします。
- **アプリのコメントを許可する:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

11. **次へ**をクリックします。**承認**ページが表示されます。

    ユーザーがアプリにアクセスする前に承認を要求するワークフローを使用するには、「ワークフローの適用」を参照してください。承認ワークフローが不要な場合は、次の手順に進みます。

12. **次へ**をクリックします。**デリバリーグループの割り当て**ページが表示されます。
13. **デリバリーグループの選択**の横で、デリバリーグループを検索するためにタイプ入力するか、リストから1つまたは複数のグループを選択します。選択したグループは、**アプリの割り当てを受け取るデリバリーグループ**リストに表示されます。
14. **展開スケジュール**を展開し、次の設定を構成します。

    - **展開:** アプリをデバイスに展開するかどうかを選択します。デフォルトは**オン**です。
    - **展開スケジュール:** アプリを**今すぐ**展開するか、**後で**展開するかを選択します。**後で**を選択した場合は、アプリを展開する日時を構成します。デフォルトは**今すぐ**です。
    - **展開条件:** デバイスが接続するたびにアプリを展開するには、**接続ごとに**を選択します。以前にデバイスがアプリを受信できなかった場合にアプリを展開するには、**以前の展開が失敗した場合のみ**を選択します。デフォルトは**接続ごとに**です。

    常時接続用に展開オプションは、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

    常時接続オプション:

    - iOSデバイスでは利用できません
    - Citrix Endpoint Managementをバージョン10.18.19以降で使い始めたAndroidおよびAndroid Enterpriseのお客様には利用できません
    - Citrix Endpoint Managementをバージョン10.18.19より前に使い始めたAndroidおよびAndroid Enterpriseのお客様には推奨されません

    構成する展開スケジュールは、すべてのプラットフォームで同じです。行った変更は、**常時接続用に展開**を除き、すべてのプラットフォームに適用されます。

15. **保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Win32アプリをエンタープライズアプリとして追加する

Win32アプリ用のMSI、APPX、AppxBundle、PS1、またはEXEファイルをCitrix Endpoint Managementにアップロードして、管理対象のWindows 10およびWindows 11デスクトップおよびタブレットデバイスに展開できます。Citrix Endpoint Managementを使用してファイルを展開すると、Windowsデバイスは次のようにアプリをインストールします。

- アップグレードされたアプリがインストール中に古いバージョンを削除する場合、デバイスにはアップグレードされたアプリのみが含まれます。
- アップグレードされたアプリが古いバージョンを削除できないが、新しいバージョンをインストールできる場合、デバイスには両方のバージョンのアプリが含まれます。Citrix Endpoint Managementには、古いバージョンの情報がなくなります。
- 古いバージョンが存在する場合にアップグレードされたアプリをインストールできない場合、新しいアプリはインストールされません。その場合、まずApp Uninstallデバイスポリシーを展開して古いバージョンを削除します。その後、新しいバージョンを展開します。

要件

- Windows 10 (バージョン1607以降) または Windows 11
- Windows 10 プロフェッショナル または Windows 11 プロフェッショナル
- Windows 10 エンタープライズ または Windows 11 エンタープライズ
- /quietオプションでインストールされたスタンドアロンのWin32 MSIアプリ。この展開ユースケースでは、Microsoftは複数のアプリを含むMSI、ネストされたMSI、または対話型インストールをサポートしていません。

メタデータの検索

Win32アプリをCitrix Endpoint Managementに追加する際は、そのアプリのメタデータを指定します。メタデータを検索するには、WindowsコンピューターでOrcaアプリケーションを使用し、次の情報をメモしてください。

- プロダクトコード
- プロダクト名
- プロダクトバージョン
- パッケージのインストールタイプ（ユーザーごとまたはマシンごと）

Citrix Endpoint Management に Win32 アプリを追加する

1. 「**構成 > アプリ**」に移動し、「**エンタープライズ**」をクリックして、「**アプリ情報**」ページでアプリの名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Windows デスクトップ/タブレット** 以外のすべてのプラットフォームチェックボックスをオフにします。
3. **Windows デスクトップ/タブレットエンタープライズアプリ** ページで、**アップロード** をクリックしてファイルに移動します。
4. 次の設定を構成します。

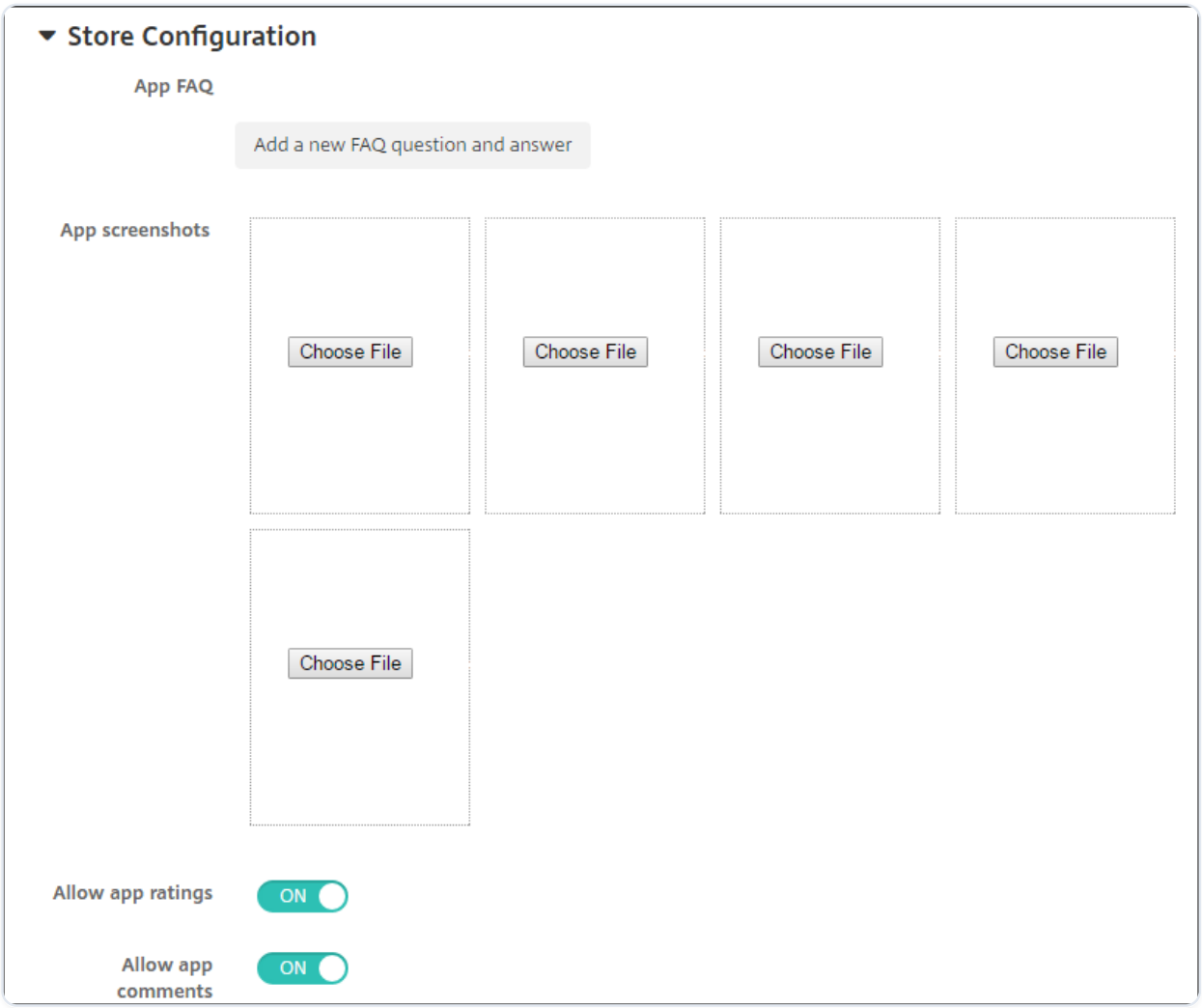
   アプリ構成画面(/en-us/citrix-endpoint-management/media/configure-win32-msi-apps.png)

   - **アプリ名:** アプリのメタデータからのアプリの名前。
   - **説明:** アプリの説明。
   - **アプリのバージョン:** アプリのメタデータからのアプリのバージョン番号。
   - **最小 OS バージョン:** オプション。デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョン。
   - **最大 OS バージョン:** オプション。デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステム。
   - **除外デバイス:** オプション。アプリを実行できないデバイスの製造元またはモデル。
   - **製品コード:** アプリのメタデータからの、UUID 形式の MSI アプリ製品コード。
   - **インストールコンテキスト:** アプリのメタデータに基づいて、アプリをデバイスまたはユーザーのどちらにインストールするかを選択します。この設定は EXE ファイルでは使用できません。
   - **コマンドライン:** MSIEXEC.exe を呼び出すときに使用するコマンドラインオプション。
   - 「**インストールコマンドライン:** EXEファイルをサイレントインストールするためのコマンドライン引数を追加します。」.
   - 「**アンインストールコマンドライン:** EXEファイルをサイレントアンインストールするためのコマンドライン引数を追加します。」.
   - 「**再試行回数:** ダウンロードおよびインストール操作を、インストールが失敗したとマークされるまでに再試行できる回数。」.
   - 「**タイムアウト:** インストーラーがインストールを失敗と解釈し、プロセスを監視しなくなるまでに、インストールプロセスが実行される分数。」.
   - 「**再試行間隔:** 再試行操作間の分数。」.

5. 「展開ルールを構成します。詳細については、「」を参照してください。(/ja-jp/citrix-endpoint-management/deploy-resources.html#configure-deployment-rules)」.
6. 「**ストア構成**を展開します。」.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「



」

「必要に応じて、以下を構成できます。」:

- 「**アプリFAQ: 新しいFAQの質問と回答を追加**をクリックして、アプリのFAQを作成します。」.
- 「**電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。」.
- 「**アプリの評価を許可:** ユーザーがアプリストアでアプリを評価できるようにします。」.
- 「**アプリのコメントを許可:** ユーザーがアプリストアでアプリにコメントを残せるようにします。」.

7. 「**次へ**をクリックして**概要**ページに進み、**保存**をクリックします。」.
8. 「**構成 > デリバリーグループ**に移動し、Win32アプリを必須アプリとして追加します。」.
9. アプリを展開した後、ユーザーにアプリが利用可能になったことを知らせます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Win32アプリのアップグレード

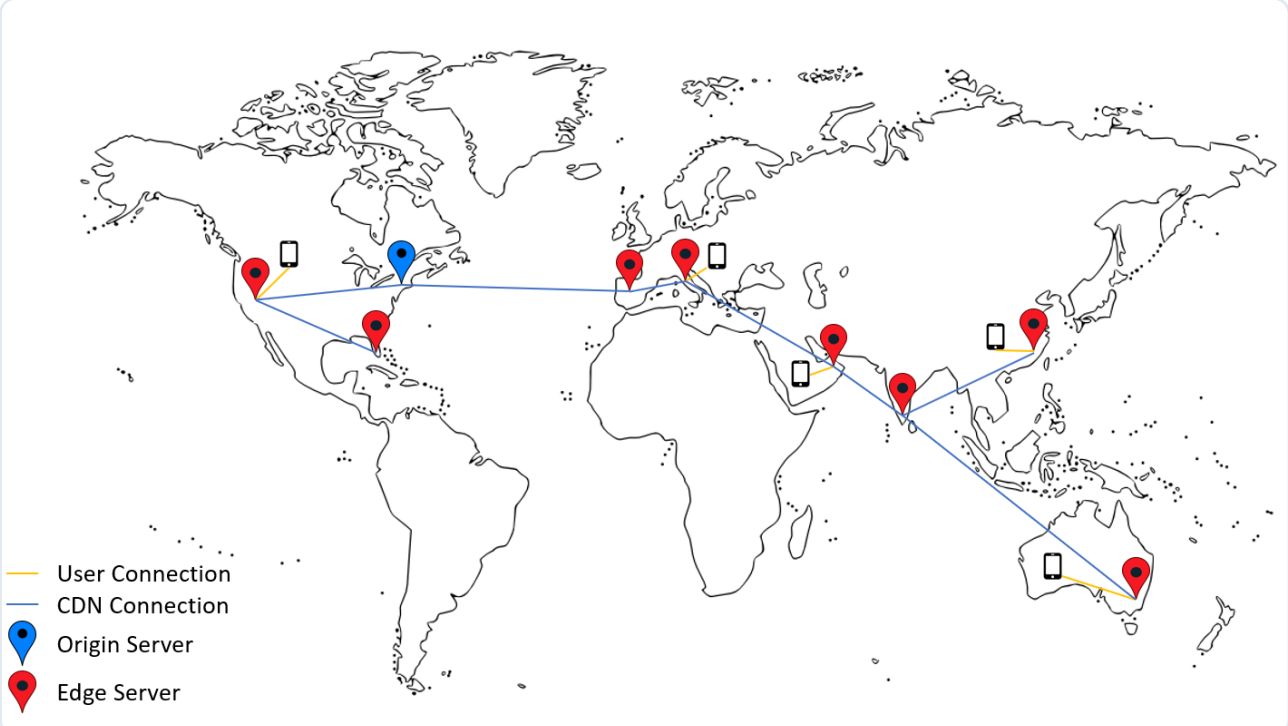
1. 「メタデータの検索」で前述したように、アプリのメタデータを検索します。
2. **構成 > アプリ**に移動して、アプリの新しいバージョンをアップロードします。**アプリのバージョン**を更新します。アプリの新しいバージョンに異なる**製品コード**がある場合は、その設定を更新します。
3. 変更を送信してアプリを展開します。

Citrix CDNからエンタープライズアプリとMDXアプリを配信する

Citrix Content Delivery Network (CDN) からエンタープライズアプリとMDXアプリを配信できます。CDNとは、アプリケーションコンテンツを安全かつ高速に配信するために連携する、地理的に分散したサーバーグループを指します。ローカルサーバーがアプリをモバイルデバイスに配信します。

CDNは、近くのCDN配信ポイントを介してモバイルデバイスに地理的に近いコンテンツを配布することで、アプリのダウンロード時間を改善します。CDNは、ユーザーに最も近いPoint of Presence (POP) ロケーションからアプリを配信します。

次の図は、CDNがモバイルデバイスユーザーに最も近いエッジサーバーにアプリを配信する方法の例を示しています。エッジサーバーは、モバイルデバイスがアプリを要求したときに、元のサーバーからコンテンツをキャッシュします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーはCitrix Secure Hubを使用してアプリに接続できます。アプリを追加すると、Citrix Endpoint Managementはそのアプリのコネクタを作成します。

エンタープライズアプリ向けのCitrix CDNサポートは、以下のプラットフォームで利用できます。

- iOS (MDMまたはMAM登録)
- Android (MDMまたはMAM登録)
- Windowsデスクトップまたはタブレット (MDM登録)
- macOS (MDM登録)

MDXアプリのCitrix CDNサポートは、次のプラットフォームで利用できます。

- iOS (MDMまたはMAM登録)
- Android (MDMまたはMAM登録)

CDNの仕組み

CDNサービスの核となる部分では、アプリをより高速に配信するという目標を達成するためにサーバーが連携しています。この目標は、アプリを世界中のさまざまな配信ポイントに安全に配置することによって達成されます。Citrix Endpoint Managementサーバーへの初期接続時に使用されるモバイルデバイスのDNSサーバーによって、配信ポイントが決定されます。

例: モバイルデバイスのDNSサーバーIPがフロリダ州フォートローダーデールにあると仮定します。CDNは、その場所に最も近いローカル配信ポイントを使用して、アプリをモバイルデバイスに配信します。このCDNの使用により、アプリのダウンロード時間が短縮されます。

モバイルデバイスがエンタープライズアプリを最初に要求またはプッシュすると、Citrix Endpoint Managementはアプリをローカル配信ポイントにコピーし、他のローカルデバイスのダウンロードのために、そのアプリを24時間そこに保持します。

Citrix CDNからエンタープライズアプリを配信する

Citrix Endpoint Managementリリース19.4.1では、すべての新規マルチテナンシー顧客に対して、エンタープライズアプリの配信はデフォルトでCDN配信になります。このリリース以前の既存の顧客については、このセクションの手順に従ってください。

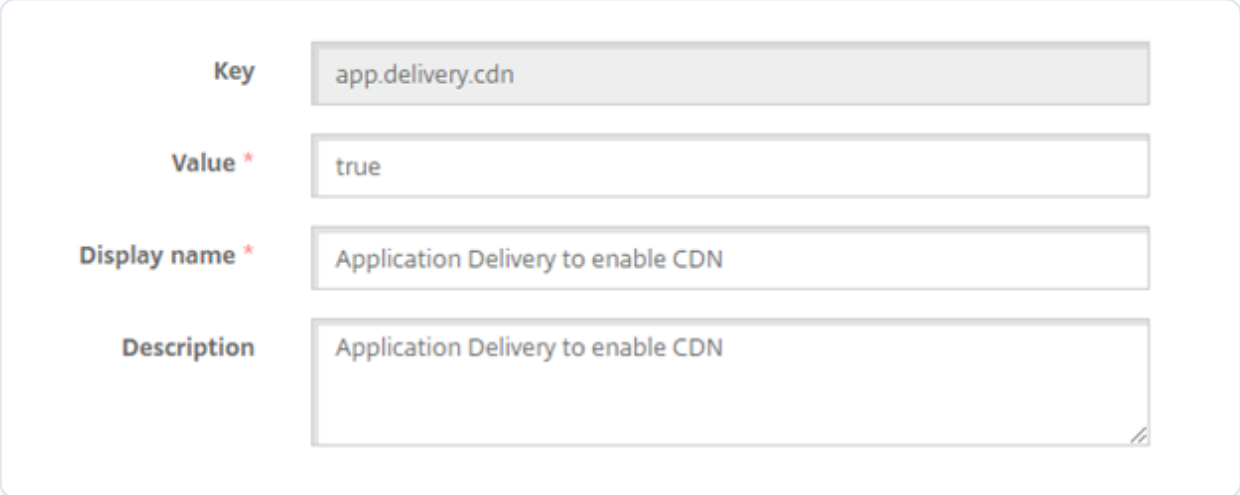
Citrix Endpoint Managementサーバーに既に存在するエンタープライズアプリについては、Citrix Endpoint Managementは、以下の手順を完了してそれらのアプリが再アップロードされるまで、引き続きサーバーからそれらのアプリを配信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

Citrix Cloud管理者のみがアカウントのCDNを有効にできます。サーバープロパティ `app.delivery.cdn` は、Citrix Cloud管理者としてログオンした場合にのみCitrix Endpoint Managementに表示されます。Citrix Cloud管理者については、「Manage Citrix Cloud administrators」を参照してください。

1. アカウントのCDNを有効にするには: Citrix Endpoint Managementコンソールで、 **>** の順に移動します。
2. `app.delivery.cdn` を検索し、 をクリックします。
3. 値を**true**に変更します。



4. Citrix Endpoint Managementコンソールで、エンタープライズアプリを再度アップロードします。
   a. **Configure > Apps**に移動し、アプリリストを**Type** (**Enterprise**)と**Platform**でフィルタリングします。
   b. アプリを選択し、**Edit**をクリックし、**Next**をクリックし、**Upload**をクリックします。
   c. 各エンタープライズアプリについて、前の手順を繰り返します。

Citrix CDNからMDXアプリを配信する

Citrix Endpoint Managementリリース20.12.0では、すべての新規マルチテナンシー顧客に対して、MDXアプリの配信はデフォルトでCDN配信になります。このリリース以前の既存の顧客は、このセクションの手順に従ってください。

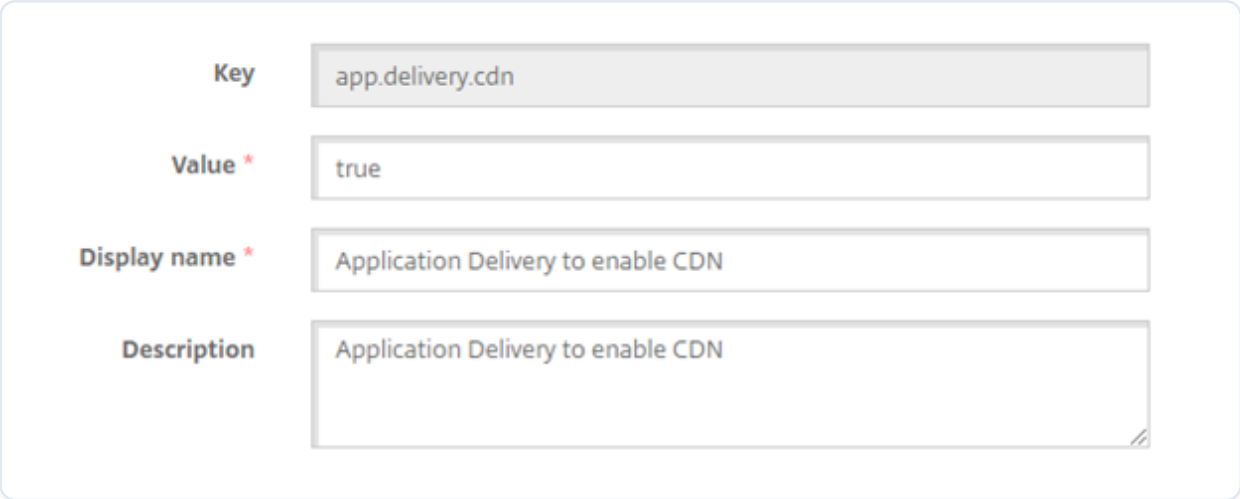
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementサーバーにすでに存在するMDXアプリについては、以下の手順を完了してアプリが再アップロードされるまで、Citrix Endpoint Managementは引き続きサーバーからそれらのアプリを配信します。

重要:

Citrix Cloud管理者のみがアカウントのCDNを有効にできます。サーバープロパティ `app.delivery.cdn` は、Citrix Cloud管理者としてログオンした場合にのみCitrix Endpoint Managementで表示されます。Citrix Cloud管理者については、Citrix Cloud管理者の管理を参照してください。

1. アカウントのCDNを有効にするには: Citrix Endpoint Managementコンソールで、**Settings > Server Properties**に移動します。
2. `app.delivery.cdn` を検索し、**Edit**をクリックします。
3. 値を**true**に変更します。



4. Citrix Endpoint Managementコンソールで、MDXアプリを再度アップロードします。
   a. **［構成］> ［アプリ］** に移動し、アプリリストを **［種類］** (**MDX**) と **［プラットフォーム］** でフィルターします。
   b. アプリを選択し、**［編集］** をクリックし、**［次へ］** をクリックし、**［アップロード］** をクリックします。
   c. 各MDXアプリについて、前の手順を繰り返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Webリンクを追加する

Webリンクは、インターネットまたはイントラネットサイトへのWebアドレスです。Webリンクは、SSOを必要としないWebアプリケーションを指すこともできます。Webリンクの構成が完了すると、そのリンクはアプリストアにアイコンとして表示されます。ユーザーがCitrix Secure Hubでログオンすると、そのリンクは利用可能なアプリとデスクトップのリストとともに表示されます。

Citrix Endpoint Managementコンソールの **［アプリ］** タブからWebリンクを構成できます。Webリンクの構成が完了すると、そのリンクは **［アプリ］** テーブルのリストにリンクアイコンとして表示されます。ユーザーがCitrix Secure Hubでログオンすると、そのリンクは利用可能なアプリとデスクトップのリストとともに表示されます。

詳細については、このビデオをご覧ください。

リンクを追加するには、次の情報を提供します。

- リンクの名前
- リンクの説明
- Webアドレス（URL）
- カテゴリ
- ロール
- .png 形式の画像 (オプション)

1. Citrix Endpoint Management コンソールで、 **> >** の順にクリックします。 ダイアログボックスが表示されます。

   アプリ構成画面(/en-us/citrix-endpoint-management/media/configure-apps-add.png)
2. をクリックします。 ページが表示されます。
3. ペインで、次の情報を入力します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルの の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。
4. をクリックします。 ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

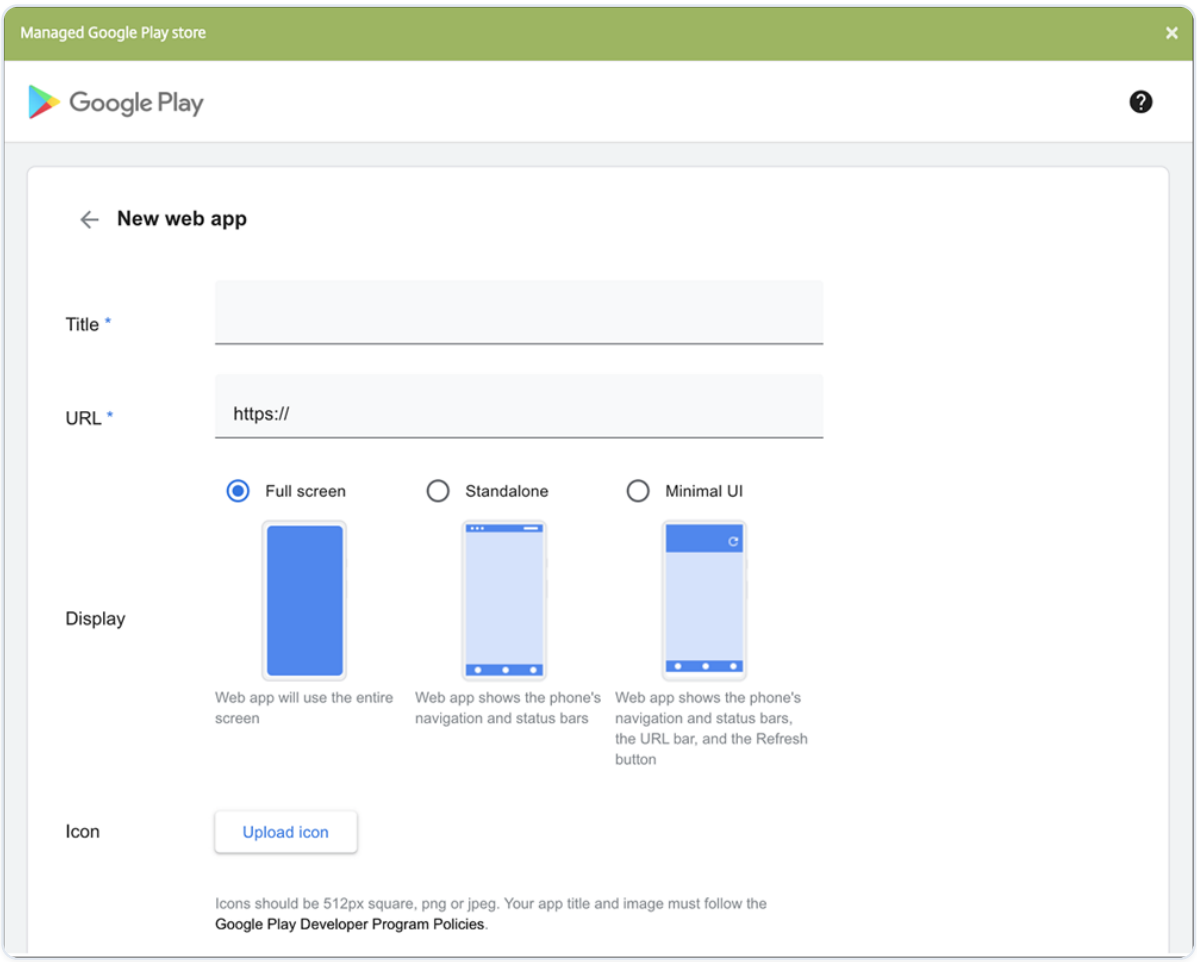
5. で、iOS、Android (レガシーDA)、およびWindows 8用のWebアプリを追加するには**** を選択するか、 を選択します。含めたくないプラットフォームのチェックボックスはオフにします。

   - を選択した場合は、次の手順に進んで設定を構成します。
   - を選択した場合は、 ボタンをクリックして管理対象のGoogle Playストアを開きます。Webアプリを公開するために開発者アカウントを登録する必要はありません。続行するには、右下隅にある**** アイコンをクリックします。

     Webアプリの作成(/en-us/citrix-endpoint-management/media/create-web-apps.png)

     次の設定を構成します。

     - **タイトル:** Webアプリの名前を入力します。
     - **URL:** アプリのWebアドレスを入力します。
     - **Display:** ユーザーデバイスにWebアプリを表示する方法を選択します。利用可能なオプションは、**全画面表示**、**スタンドアロン**、**最小限のUI**です。
     - **Icon:** Webアプリ用の独自の画像をアップロードします。



   完了したら、**作成**をクリックします。Webアプリが公開されるまでに最大10分かかる場合があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

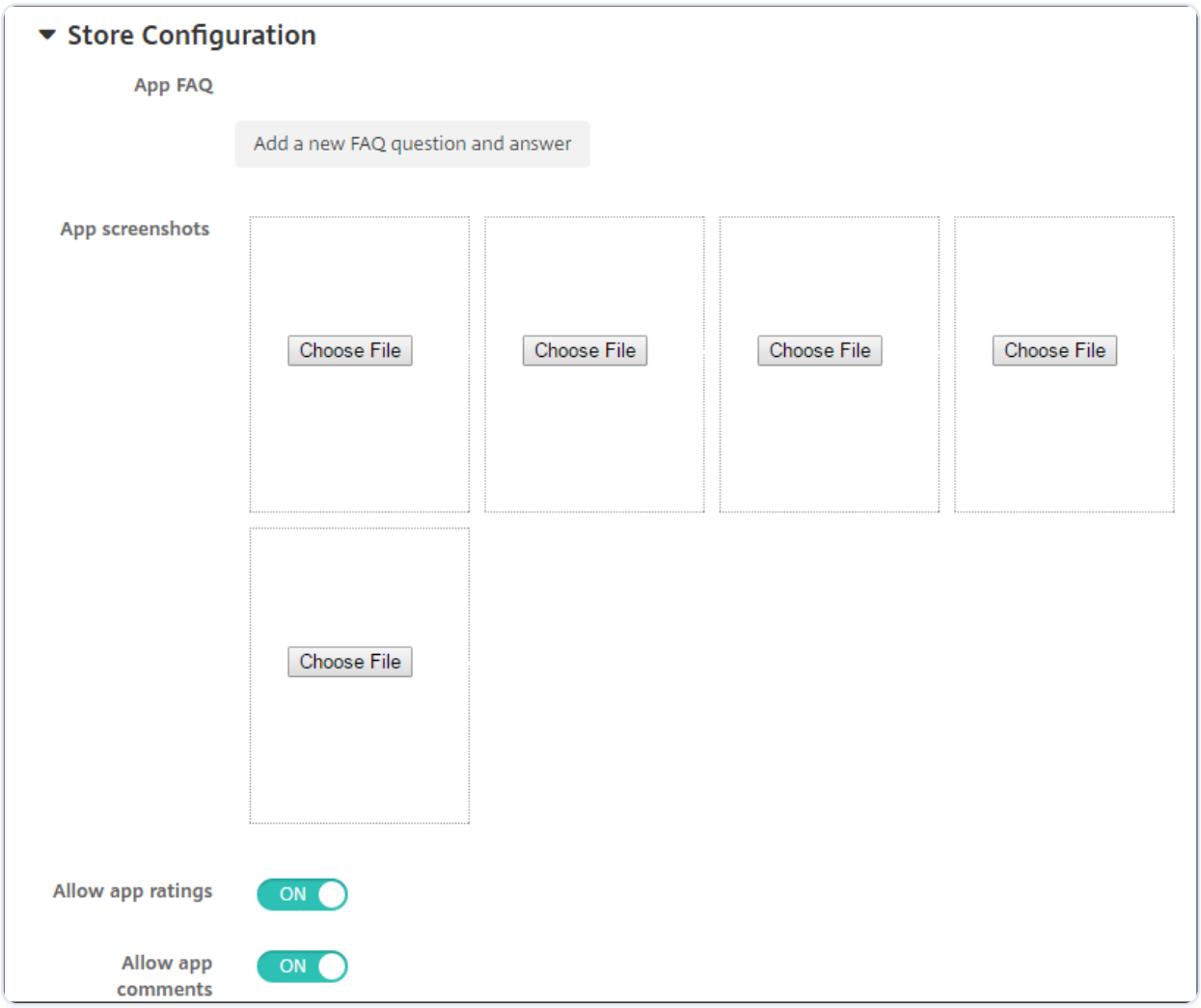
6. Android Enterprise以外のプラットフォームでは、以下の設定を構成します。

    - **App name:** 事前入力された名前を受け入れるか、新しい名前を入力します。
    - **App description:** 事前入力された説明を受け入れるか、独自の説明を入力します。
    - **URL:** 事前入力されたURLを受け入れるか、アプリのWebアドレスを入力します。選択したコネクタによっては、このフィールドにプレースホルダーが含まれている場合があり、次のページに進む前にそれを置き換える必要があります。
    - **App is hosted in internal network:** アプリが内部ネットワーク内のサーバーで実行されているかどうかを選択します。ユーザーがリモートの場所から内部アプリに接続する場合、NetScaler Gatewayを介して接続する必要があります。このオプションを**オン**に設定すると、アプリにVPNキーワードが追加され、ユーザーはNetScaler Gatewayを介して接続できるようになります。デフォルトは**オフ**です。
    - **App category:** ドロップダウンリストでオプションのカテゴリをクリックして、アプリに適用します。
    - **Image:** デフォルトのCitrix画像を使用するか、独自のアプリ画像をアップロードするかを選択します。デフォルトは「デフォルトを使用」です。

        - 独自の画像をアップロードするには、**参照**をクリックしてファイルの場所に移動します。ファイルは.PNGファイルである必要があります。JPEGまたはGIFファイルはアップロードできません。カスタムグラフィックを追加すると、後で変更することはできません。

7. 展開ルールを構成します。詳細については、展開ルールの構成を参照してください。
8. **ストア構成**を展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



必要に応じて、以下を構成できます。

- **アプリのFAQ: 新しいFAQの質問と回答を追加**をクリックして、アプリのFAQを作成します。
- **電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。
- **アプリの評価を許可:** ユーザーがアプリストアでアプリを評価できるようにします。
- **アプリのコメントを許可:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

9. **次へ**をクリックします。**デリバリーグループの割り当て**ページが表示されます。
10. **デリバリーグループの選択**の横で、入力してデリバリーグループを検索するか、リストから1つ以上のグループを選択します。選択したグループは、**アプリの割り当てを受け取るデリバリーグループ**リストに表示されます。
11. **展開スケジュール**を展開し、以下の設定を構成します。

- **展開:** アプリをデバイスに展開するかどうかを選択します。デフォルトは**オン**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **展開スケジュール:** アプリを**今すぐ**展開するか、**後で**展開するかを選択します。**後で**を選択した場合は、アプリを展開する日付と時刻を構成します。デフォルトは**今すぐ**です。
- **展開条件:** デバイスが接続するたびにアプリを展開するには、**接続ごとに**を選択します。以前にデバイスがアプリを受信できなかった場合にアプリを展開するには、**以前の展開が失敗した場合のみ**を選択します。デフォルトは**接続ごとに**です。

常時接続の展開オプションは、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

常時接続オプション：

- iOSデバイスでは利用できません
- バージョン10.18.19以降でCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様には利用できません
- バージョン10.18.19より前にCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様には推奨されません

構成する展開スケジュールは、すべてのプラットフォームで同じです。行った変更は、**Deploy for always-on connection** を除き、すべてのプラットフォームに適用されます。

12. **保存** をクリックします。

Microsoft 365アプリを有効にする

MDXコンテナを開いて、Citrix Secure Mail、Citrix Secure Web、およびCitrix Filesがドキュメントとデータを Microsoft Office 365アプリに転送できるようにすることができます。詳細については、「Office 365アプリとの安全な対話を許可する」を参照してください。

ワークフローを適用する

ワークフローを割り当てるか作成するには、次の設定を構成します。

- **使用するワークフロー:** ドロップダウンリストで既存のワークフローをクリックするか、**新しいワークフローを作成** をクリックします。デフォルトは **なし** です。

  新しいワークフローを作成 を選択した場合は、次の設定を構成します。

  - **名前:** ワークフローの一意の名前を入力します。
  - **説明:** 必要に応じて、ワークフローの説明を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **メール承認テンプレート:** リストから、割り当てるメール承認テンプレートを選択します。このフィールドの右側にある目のアイコンをクリックすると、テンプレートをプレビューできるダイアログボックスが表示されます。
- **マネージャー承認レベル:** リストから、このワークフローに必要なマネージャー承認レベルの数を選択します。デフォルトは1レベルです。可能なオプションは次のとおりです。
  - 不要
  - 1レベル
  - 2レベル
  - 3レベル
- **Active Directoryドメインの選択:** リストから、ワークフローに使用する適切なActive Directoryドメインを選択します。
- **追加の必須承認者を見つける:** 検索フィールドに追加の必須承認者の名前を入力し、**検索**をクリックします。名前はActive Directoryから取得されます。
- フィールドに名前が表示されたら、名前の横にあるチェックボックスを選択します。名前とメールアドレスは「**選択された追加の必須承認者**」リストに表示されます。

  「**選択された追加の必須承認者**」リストからユーザーを削除するには、次のいずれかを実行します。
  - **検索**をクリックして、選択したドメイン内のすべてのユーザーのリストを表示します。
  - 検索ボックスに氏名または部分的な名前を入力し、**検索**をクリックして検索結果を絞り込みます。
  - 「**選択された追加の必須承認者**」リストのユーザーは、検索結果リストの名前の横にチェックマークが付いています。リストをスクロールし、削除する各名前の横にあるチェックボックスをオフにします。

アプリストアとCitrix Secure Hubのブランディング

ストアでのアプリの表示方法を設定し、Citrix Secure Hubとアプリストアにロゴを追加できます。これらのブランディング機能は、iOSおよびAndroidデバイスで利用できます。

開始する前に、カスタムイメージが準備され、アクセス可能であることを確認してください。

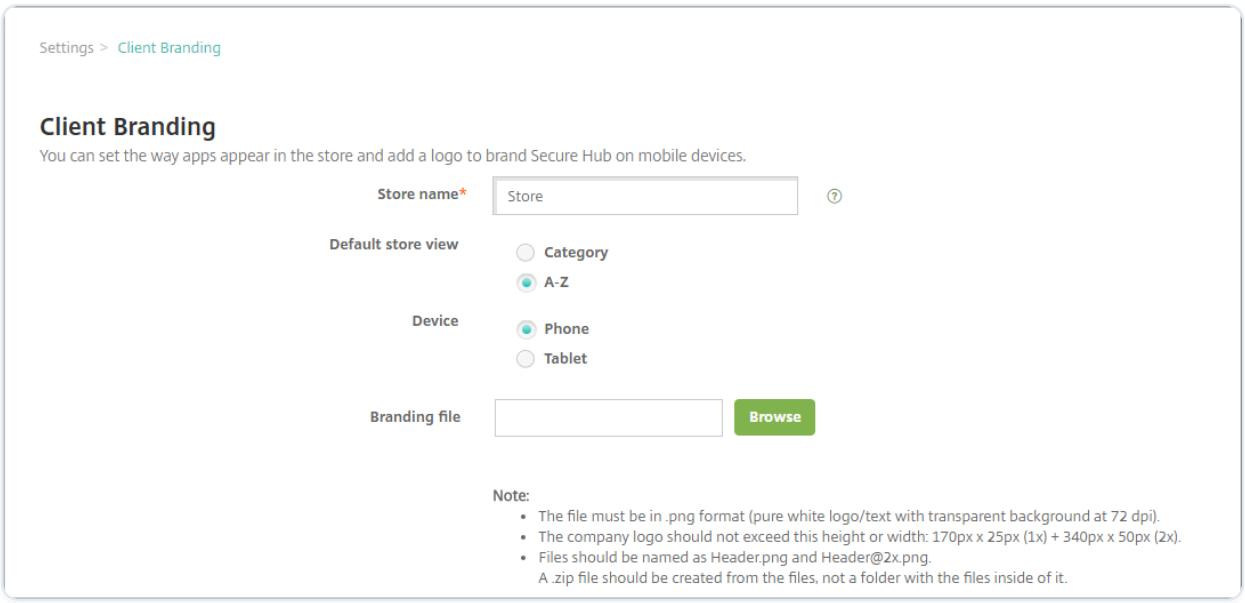
カスタムイメージは次の要件を満たす必要があります。

- ファイルは.png形式である必要があります

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 72 dpiで、透明な背景の純粋な白のロゴまたはテキストを使用します。
- 会社のロゴは、高さまたは幅が170 px x 25 px (1x) および 340 px x 50 px (2x) を超えることはできません。
- ファイル名を `Header.png` および `Header@2x.png` にします。
- ファイルを格納したフォルダーではなく、ファイルから.zipファイルを作成します。

1. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **クライアント**の下で、**クライアントブランディング**をクリックします。**クライアントブランディング**ページが表示されます。



次の設定を構成します。

- **ストア名:** ストア名はユーザーのアカウント情報に表示されます。名前を変更すると、ストアサービスへのアクセスに使用されるURLも変更されます。通常、デフォルト名を変更する必要はありません。

  重要:

  ストア名には英数字のみを使用できます。

- **デフォルトのストアビュー: カテゴリ**または**A-Z**のいずれかを選択します。デフォルトは**A-Z**です。
- **デバイスオプション: 電話**または**タブレット**のいずれかを選択します。デフォルトは**電話**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ブランディングファイル:** ブランディング画像または画像の.zipファイルを選択するには、**参照**をクリックしてファイルの場所に移動します。

3. **保存**をクリックします。

このパッケージをユーザーデバイスに展開するには、展開パッケージを作成し、そのパッケージを展開します。

アプリストアを介したCitrix Virtual Apps and Desktops

Citrix Endpoint Managementは、Citrix Virtual Apps and Desktopsからアプリを収集し、アプリストアでモバイルデバイスユーザーが利用できるようにすることができます。ユーザーはアプリストア内で直接アプリを購読し、Citrix Workspaceから起動します。アプリを起動するには、Citrix Workspaceアプリがユーザーデバイスにインストールされている必要があります。

この設定を構成するには、オンプレミスのStoreFrontの完全修飾ドメイン名 (FQDN) またはIPアドレスとポート番号が必要です。

1. Citrix Endpoint Management Webコンソールで、右上隅にある歯車アイコンをクリックします。「**設定**」ページが表示されます。
2. 「**Virtual Apps and Desktops**」をクリックします。「**Virtual Apps and Desktops**」ページが表示されます。

   Virtual Apps and Desktops設定画面(/en-us/citrix-endpoint-management/media/settings-virtual-apps-and-desktops.png)
3. 次の設定を構成します。

   - **ホスト:** StoreFrontの完全修飾ドメイン名 (FQDN) またはIPアドレスを入力します。
   - **ポート:** StoreFrontのポート番号を入力します。デフォルトは80です。
   - **相対パス:** パスを入力します。例：/Citrix/PNAgent/config.xml
   - **HTTPSの使用:** StoreFrontとクライアントデバイス間のセキュアな認証を有効にするかどうかを選択します。デフォルトは**オフ**です。
   - **Cloud Connectorの使用:** StoreFrontサーバーへの接続にCloud Connectorを使用するには、「**オン**」を選択します。次に、接続の「**リソースの場所**」と「**許可される相対パス**」を指定します。
     - **リソースの場所:** Citrix Cloud Connectorで定義されているリソースの場所から選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **許可される相対パス:** 指定されたリソースの場所で許可される相対パス。1行に1つのパスを指定します。アスタリスク (*) のワイルドカードを使用できます。

リソースの場所が `https://StoreFront.company.com` であり、次のURLへのアクセスを提供したいとします。

- `https://StoreFront.company.com/Citrix/PNAgent/Config.xml`
- `https://StoreFront.company.com/Citrix/PNAgent/enum.aspx`
- `https://StoreFront.company.com/Citrix/PNAgent/launch.aspx`

URL `https://StoreFront.company.com/Citrix/PNAgent/*` を持つすべてのリクエストを許可するには、このパスを入力します: `/Citrix/PNAgent/*`

Citrix Endpoint Management は、他のすべてのパスをブロックします。

4. **接続テスト** をクリックして、Citrix Endpoint Management が指定されたStoreFrontサーバーに接続できることを確認します。
5. **保存** をクリックします。

アプリコネクタの種類

以下の表に、WebアプリまたはSaaSアプリを追加する際にCitrix Endpoint Managementで利用可能なコネクタとコネクタの種類を示します。WebアプリまたはSaaSアプリを追加する際に、Citrix Endpoint Managementにコネクタを追加することもできます。

この表は、コネクタがユーザーアカウント管理をサポートしているかどうかを示しています。これにより、アカウントを自動的に、またはワークフローを使用して作成できます。

コネクタ名	SSO SAML	ユーザーアカウント管理をサポート
EchoSign_SAML	はい	はい
Globoforce_SAML		**注:** このコネクタを使用する場合、シームレスなSSO統合を確実にするために、プロビジョニングのためにユーザー管理を有効にする必要があります。
GoogleApps_SAML	はい	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コネクタ名	SSO SAML	ユーザーアカウント管理をサポート
GoogleApps_SAML_IDP	はい	はい
Lynda_SAML	はい	はい
Office365_SAML	はい	はい
Salesforce_SAML	はい	はい
Salesforce_SAML_SP	はい	はい
SandBox_SAML	Y	
SuccessFactors_SAML	Y	
ShareFile_SAML	Y	
ShareFile_SAML_SP	Y	
WebEx_SAML_SP	Y	Y

Citrix ランチャー

Citrix Launcherを使用すると、Android EnterpriseデバイスおよびCitrix Endpoint Managementによって展開されたレガシーAndroidデバイスのユーザーエクスペリエンスをカスタマイズできます。Citrix Launcherを使用すると、ユーザーが特定のデバイス設定にアクセスするのを防ぎ、デバイスを1つのアプリまたは少数のアプリに制限できます。

Citrix LauncherのCitrix Secure Hub管理でサポートされる最小Androidバージョンは Android 6.0です。

これらのCitrix Launcher機能を制御するには、**Launcher構成ポリシー**を使用します。

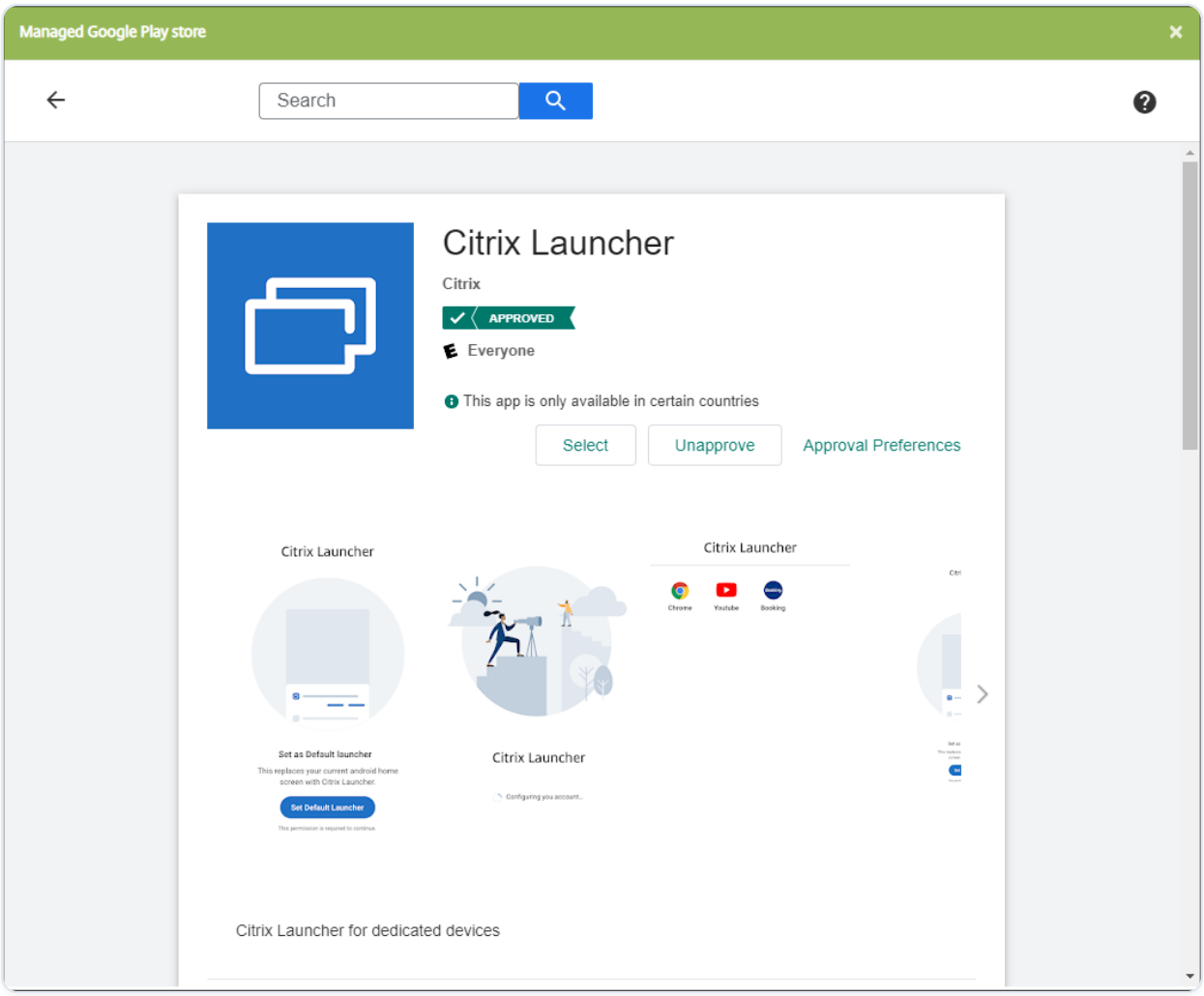
- Android Enterpriseデバイスとレガシー Androidデバイスを管理し、ユーザーが指定したアプリのみにアクセスできるようにします。
- オプションで、Citrix Launcherアイコンのカスタムロゴ画像とCitrix Launcherのカスタム背景画像を指定します。
- ユーザーがランチャーを終了するためにタイプする必要があるパスワードを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Launcherは、デバイスプラットフォームがすでに提供しているものの上に、追加のセキュリティ層となることを意図していません。

Android Enterpriseデバイス向けCitrix Launcherのセットアップ

1. Citrix Launcherアプリ (com.citrix.launcher.droid) をパブリックストアアプリとしてCitrix Endpoint Managementに追加します。**構成 > アプリ**で、**追加**をクリックし、次に**パブリックアプリストア**をクリックします。詳細については、「パブリックアプリストアアプリの追加」を参照してください。



2. キオスクデバイスポリシーで、専用用途の会社所有デバイス (Android企業所有シングルユース (COSU) デバイスとも呼ばれる) で利用可能にする必要があるアプリを指定します。**構成 > デバイスポリシー**に移動し、**追加**をクリックして**キオスク**を選択します。次に、Citrix Launcherアプリと許可リスト内の追加アプリを選択します。以前にアプリをリストに追加している場合、アプリを再度アップロードする必要はありません。詳細については、「Android Enterprise設定」を参照してください。
3. Launcher構成デバイスポリシーを追加します。**構成 > デバイスポリシー**に移動し、**追加**をクリックして**Launcher構成**を選択します。Launcher構成ポリシーで、キオスクポリシーで指定

© 1997–2026 Citrix Systems, Inc. All rights reserved.

したアプリを追加します。キオスクポリシーで指定したすべてのアプリを追加する必要はありません。Citrix Launcherアプリはキオスクポリシーでのみ追加する必要があります。詳細については、「Launcher構成ポリシー」を参照してください。

4. デリバリーグループを作成し、リソースを展開します。詳細については、この記事の「デリバリーグループを追加してリソースを展開する」セクションを参照してください。

専用用途の会社所有Android EnterpriseデバイスにCitrix Launcherを展開すると、Citrix Endpoint Managementはアプリをインストールし、デフォルトの Citrix Secure Hubランチャーを置き換えます。Citrix Launcherアプリを終了すると、Citrix Secure Hubが再びデフォルトのランチャーになります。

レガシーAndroidデバイス向けCitrix Launcherのセットアップ

注:

2020年8月、CitrixはレガシーAndroidデバイス向けのCitrixLauncher.apkのサポートを非推奨としました。新しい機能更新を受け取ることなく、レガシーCitrix Launcherアプリ (com.citrix.launcher) をAndroidデバイスで引き続き使用できます。

1. Citrix Launcherアプリを見つけるには、Citrix Endpoint Managementダウンロードページにアクセスし、**Citrix Launcher**を検索します。最新ファイルをダウンロードしてください。このファイルはCitrix Endpoint Managementへのアップロード準備ができており、ラッピングは不要です。
2. Launcher構成デバイスポリシーを追加します。**構成 > デバイスポリシー**に移動し、**追加**をクリックして、**Launcher構成**を選択します。詳細については、「Launcher構成ポリシー」を参照してください。
3. Citrix LauncherアプリをエンタープライズアプリとしてCitrix Endpoint Managementに追加します。**構成 > アプリ**で、**追加**をクリックし、次に**エンタープライズ**をクリックします。詳細については、「エンタープライズアプリの追加」を参照してください。
4. デリバリーグループを作成し、リソースを展開します。詳細については、この記事の「デリバリーグループを追加してリソースを展開する」セクションを参照してください。

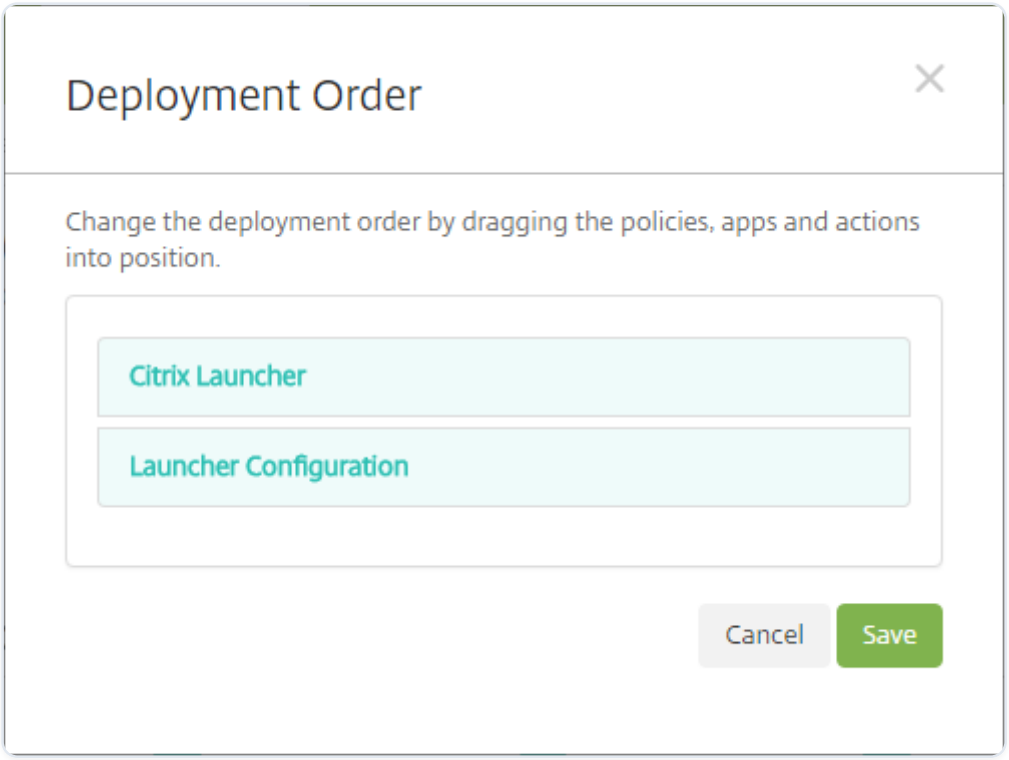
デリバリーグループを追加してリソースを展開する

1. **構成 > デリバリーグループ**で、以下の構成でCitrix Launcherのデリバリーグループを作成します。

    - **ポリシー**ページで、**Launcher構成ポリシー**を追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アプリ**ページで、**Citrix Launcher**を**必須アプリ**にドラッグします。
- **概要**ページで、**展開順序**をクリックし、**Citrix Launcher**アプリが**Launcher構成**ポリシーより前にあることを確認します。



2. デリバリーグループ内のすべてのユーザーにプッシュ通知を送信して、デリバリーグループにリソースを展開します。デリバリーグループへのリソースの追加について詳しくは、「リソースの展開」を参照してください。

Citrix Launcherなしでデバイスを管理する

Citrix Launcher を使用する代わりに、既存の機能を使用できます。

専用デバイスをプロビジョニングするには：

1. **デバイス所有者モード**を**専用デバイス**に設定して、登録プロファイルを作成します。詳細については、「専用の Android Enterprise デバイスのプロビジョニング」および「登録プロファイル」を参照してください。
2. アプリを許可リストに追加し、タスクロックモードを設定するために、キオスクデバイスポリシーを作成します。以前にアプリをリストに追加した場合は、再度アプリをアップロードする必要はありません。詳しくは、「Android Enterprise の設定」を参照してください。
3. 作成した登録プロファイルに各デバイスを登録します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apple Volume Purchase を使用してアプリを追加する

Apple Business Manager (ABM) および Apple School Manager (ASM) を使用すると、アプリとブックのライセンスをまとめて購入し、Volume Purchase の情報を Citrix Endpoint Management と同期できます。その後、Citrix Endpoint Management を使用して、これらのアプリとブックを iOS および macOS デバイスに展開できます。コンテンツをまとめて購入することで、組織向けのアプリやブックの検索、購入、配布プロセスが簡素化されます。

ABM または ASM を使用したコンテンツの購入について詳しくは、Apple Business Managerユーザーガイドまたは Apple School Managerユーザーガイドを参照してください。この記事では、ABM および ASM から Citrix Endpoint Management にまとめて購入したライセンスを同期する方法と、ライセンスを管理する方法について説明します。

注：

Apple Volume Purchase Program (VPP) は、January 14, 2021 をもって利用できなくなりました。Volume Purchase 機能は ABM および ASM に統合されました。現在 Device Enrollment Program (DEP) または VPP を使用している場合は、ABM または ASM にアップグレードできます。詳しくは、Apple のドキュメント Apple Deployment Programs からのアップグレード を参照してください。

Apple Volume Purchase について

ABM または ASM を使用してコンテンツをまとめて購入する場合、次の点に注意してください。

- 次のコンテンツのライセンスを購入できます。
  - 一般公開されているアプリとブック
  - 組織向けに特別に開発されたカスタムアプリ
- まとめて購入したアプリとブックは、組織所有デバイスと BYO デバイスに展開できます。ABM または ASM を介して登録された組織所有デバイスは、MDM または MDM+MAM 登録をサポートしますが、MAM 登録はサポートしません。
- アプリの配布について詳しくは、(/ja-jp/citrix-endpoint-management/device-management/apple/distribute-apple-apps.html)を参照してください。
- 既知の問題のリストについては、Knowledge Center の記事CTX222633を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

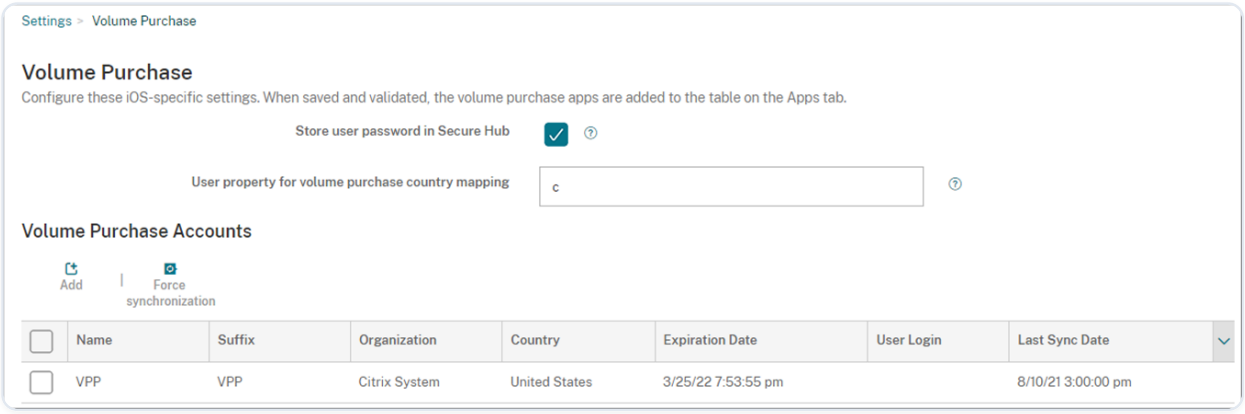
Volume Purchase アカウントを追加する

ABM または ASM ポータルでコンテンツを購入した後、ポータルから Citrix Endpoint Management に関連付けられたコンテンツトークンをダウンロードします。次に、Citrix Endpoint Management で、このコンテンツコードに基づいて Volume Purchase アカウントを作成します。このコードにより、Citrix Endpoint Management は ABM または ASM からコンテンツライセンスを同期できます。

Volume Purchaseを使用すると、管理ライセンスを使用してコンテンツを購入し、デバイスに展開できます。現在引き換えコードを使用しており、管理ライセンスに変更する場合は、Appleサポートドキュメントを参照してください。

Citrix Endpoint ManagementでVolume Purchaseアカウントを追加するには

1. ABMまたはASMポータルで、必要に応じてコンテンツを購入し、コンテンツコードファイルを安全な場所にダウンロードします。
2. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
3. **Volume Purchase**をクリックします。**Volume Purchase**構成ページが表示されます。



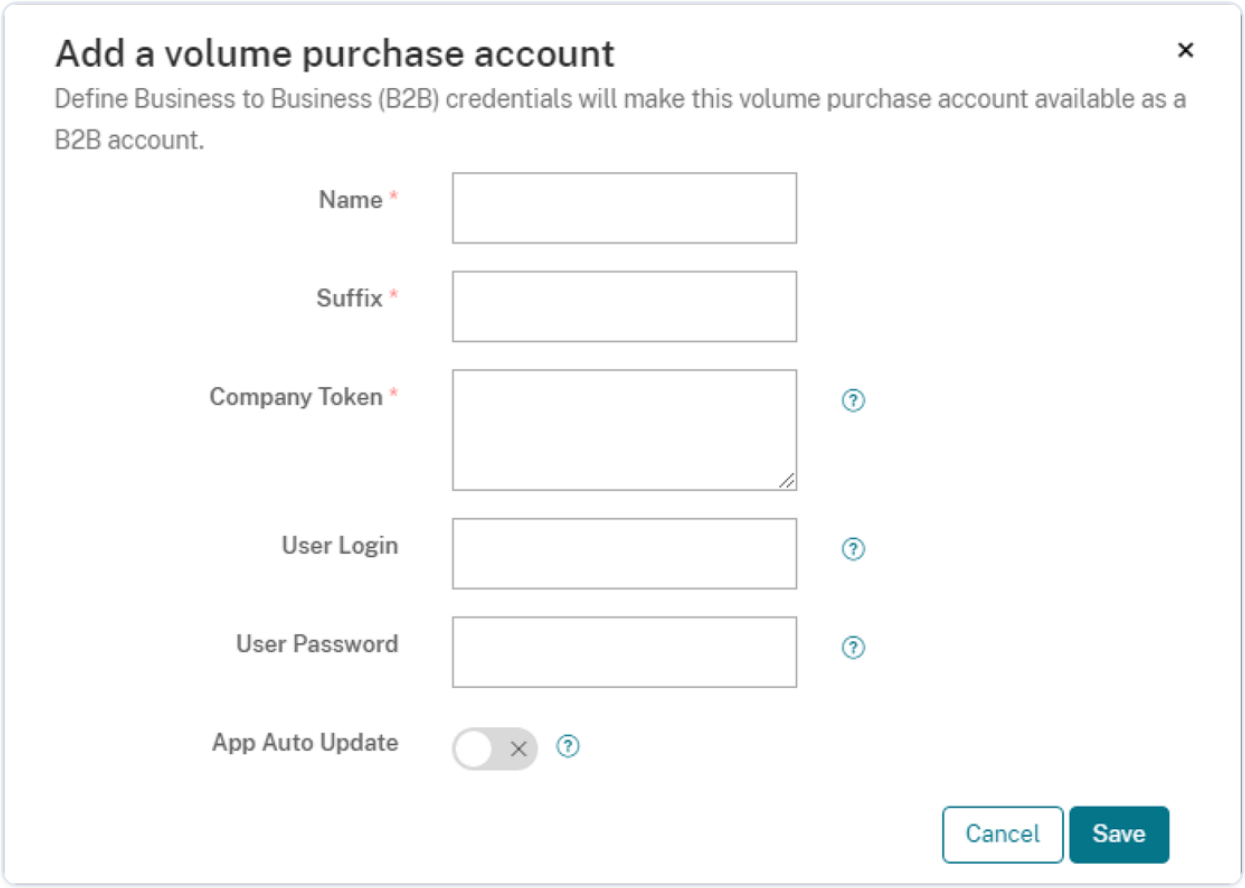
4. 次の設定を構成します:

   - **Citrix Secure Hubにユーザーパスワードを保存:** Citrix Endpoint Management認証のために、ユーザー名とパスワードをCitrix Secure Hubに保存するかどうかを選択します。デフォルトは**オン**です。
   - **Volume Purchaseの国マッピングのユーザープロパティ:** 国マッピングコードを入力して、ユーザーが国固有のアプリストアからアプリをダウンロードできるようにします。このコードについては、コンテンツマネージャーにお問い合わせください。

     Citrix Endpoint Managementは、国マッピングコードを使用してVolume Purchaseのプロパティプールを選択します。たとえば、ユーザープロパティが米国の場合、マッピングコードが英国のものであれば、ユーザーはアプリをダウンロードできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. **追加**をクリックします。**Volume Purchaseアカウントの追加**ダイアログボックスが表示されます。



6. 次のアカウント設定を構成します:

注:

Apple Configurator 1を使用している場合は、次のようにライセンスファイルをアップロードします。**構成 > アプリ**をクリックし、アプリのプラットフォームページに移動して、**Volume Purchase**を展開します。

- **名前:** アカウントのわかりやすい名前を入力します。
- **サフィックス:** Appleストアから継承されるアプリ名に表示されるサフィックスを入力します。たとえば、**VP**と入力すると、アプリリストには**Citrix Secure Mail - VP**として**Citrix Secure Mail**アプリが表示されます。
- **会社トークン:** 手順1でダウンロードしたコンテンツトークンをコピーして貼り付けます。
- **ユーザーログイン:** (オプション) このボリューム購入アカウントの管理者のユーザー名を入力します。設定されている場合、Citrix Endpoint Managementにボリューム購入したカスタムアプリを同期するには、ユーザー名とパスワードが必要です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ユーザーパスワード:** (オプション) 入力したユーザー名のパスワードを入力します。
- **アプリの自動更新: オン**にすると、Citrix Endpoint Managementコンソール内のボリューム購入アプリおよびオプションアプリは、新しいバージョンが利用可能になったときに自動的に更新されます。エンタープライズアプリおよびパブリックアプリストアアプリは、Citrix Endpoint Managementコンソールで手動で更新する必要があります。この設定が**オフ**の場合でも、Citrix Endpoint Managementコンソールでボリューム購入アプリを手動で更新できます。コンソールでアプリが更新されると、そのアプリがインストールされているデバイスもその更新を受け取ります。デフォルトは**オフ**です。

ボリュームアカウントが正常に追加されると、次の内容を通知するメッセージが表示されます。

- **構成 > アプリ**ページに、ボリューム購入したアプリがアプリリストに表示されます。アプリ名には、構成したサフィックスが表示されます。
- **構成 > メディア**ページに、ボリューム購入したブックがメディアリストに表示されます。ブック名には、構成したサフィックスが表示されます。

ボリューム購入アプリの構成

ボリューム購入アカウントを追加すると、アプリ情報がCitrix Endpoint Managementに同期され、**構成 > アプリ**ページに表示されます。これで、これらのアプリを構成し、デリバリーグループを調整し、iOSおよびmacOSデバイスのデバイスポリシー設定を調整できます。構成が完了すると、ユーザーはデバイスを登録できます。

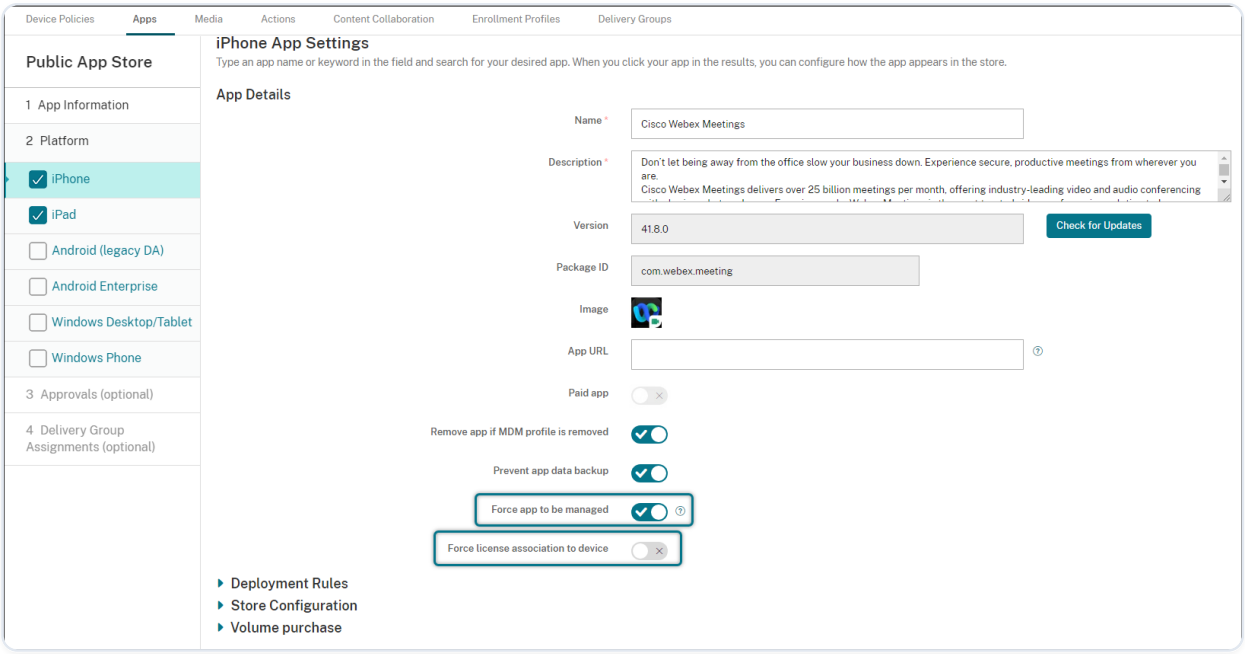
ボリューム購入アプリを構成する際は、次の設定に注意してください。

- **構成 > アプリ**ページで:
  - Citrix Endpoint Managementがアプリをユーザーではなくデバイスに展開できるようにするには、**ライセンスをデバイスに強制的に関連付ける**をオンにします。この設定がオンの場合、ユーザーはApple IDを使用する必要がなく、App Storeアカウントにサインインせずにアプリをダウンロードできます。
  - アプリが管理対象アプリとして自動的にインストールされるように、**アプリを管理対象にする**をオンにすることをお勧めします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

「**Force app to be managed**」設定を有効にするには、**Settings > Server Properties**ページで`apple.app.force.managed`サーバープロパティを**True**に構成する必要があります。詳細については、「サーバープロパティ」を参照してください。



- **設定 > デリバリーグループ**ページで:

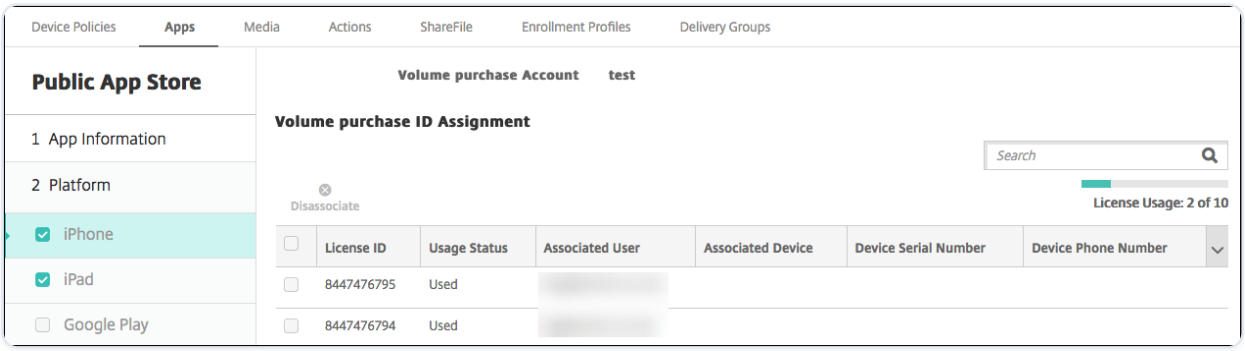
  ユーザーの操作を最小限に抑えてアプリをユーザーデバイスにサイレントインストールするには、**Apps**ページに移動し、アプリを**Required Apps**リストにドラッグします。デフォルトでは、Citrix Secure Hubを除くアプリは**Optional Apps**であり、ユーザーはCitrix Secure Hubを介してアプリのインストールを手動で開始する必要があります。

アプリライセンスの使用状況を追跡および管理する

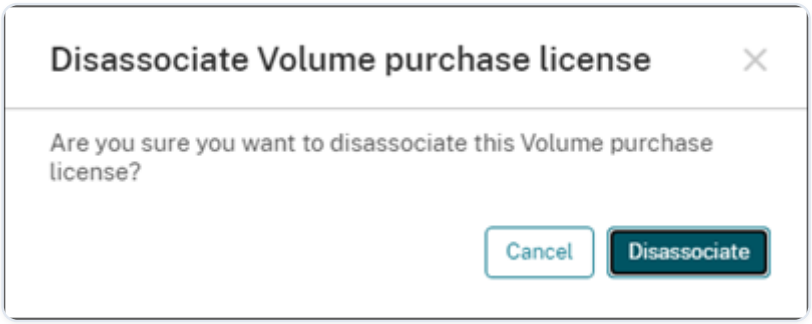
アプリのライセンス使用状況を追跡できます。必要に応じて、使用済みのライセンスを回収し、別のユーザーまたはデバイスで利用できるようにすることができます。

1. **Configure > Apps**をクリックします。
2. アプリを選択し、**Edit**をクリックします。
3. **Platform**ページに移動し、**Volume purchase**を展開します。 **Volume purchase ID Assignment**テーブルで、使用されているライセンスの数と、どのユーザーまたはデバイスによって使用されているかを追跡できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. ライセンスを回収するには、ライセンスを選択し、**Disassociate**をクリックします。



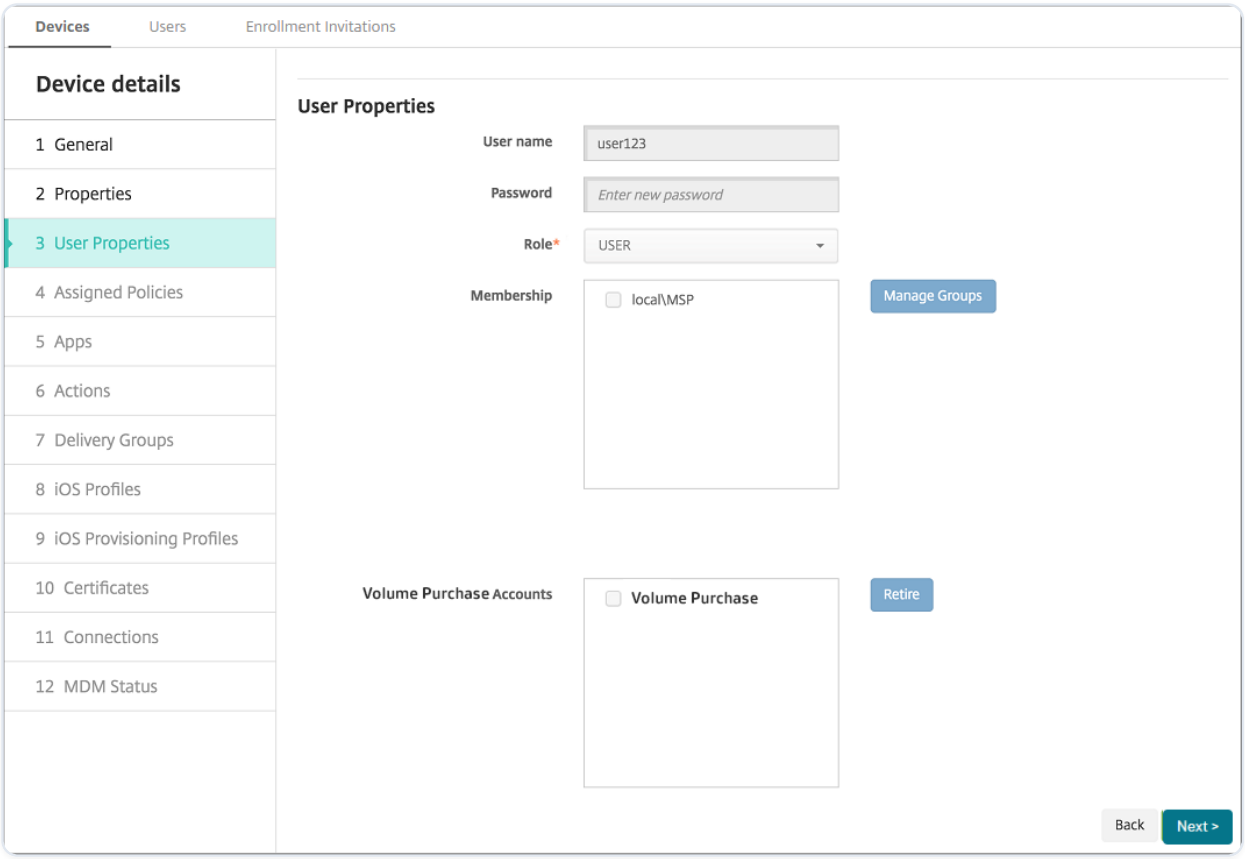
5. **Disassociate**をクリックして、アクションを確定します。

ボリューム購入アカウントからユーザーを廃止する

アプリライセンスをユーザーに関連付けている場合、ボリューム購入アカウントからユーザーをリタイアさせて、そのユーザーに割り当てられているすべてのライセンスを回収できます。ユーザーが組織を離れる場合などがユースケースとして挙げられます。

1. **「管理」>「デバイス」** をクリックします。
2. 対象ユーザーに属するデバイスを選択し、**「編集」** をクリックします。
3. **「ユーザープロパティ」** ページに移動し、必要に応じてボリューム購入アカウントを選択します。
4. **「リタイア」** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix Endpoint Managementは、選択したボリューム購入アカウントのアプリライセンスをユーザーから取り消します。

アプリ情報の同期

Citrix Endpoint Managementは、ABMまたはASMとアプリ情報を定期的に同期します。必要に応じて、アプリ情報を手動で同期できます。同期により、アプリライセンスやその他のアプリ情報がすべての変更を反映していることが保証されます。このような変更には、ボリューム購入アカウントからアプリを手動で削除した場合などが含まれます。

デフォルトの同期間隔を変更する

デフォルトでは、Citrix Endpoint Managementはボリューム購入ライセンスのベースラインを少なくとも1440分（24時間）ごとに更新します。Citrix Cloud管理者は、サーバープロパティ `vpp.baseline` を介してデフォルトの間隔を変更できます。詳しくは、「サーバープロパティ」を参照してください。

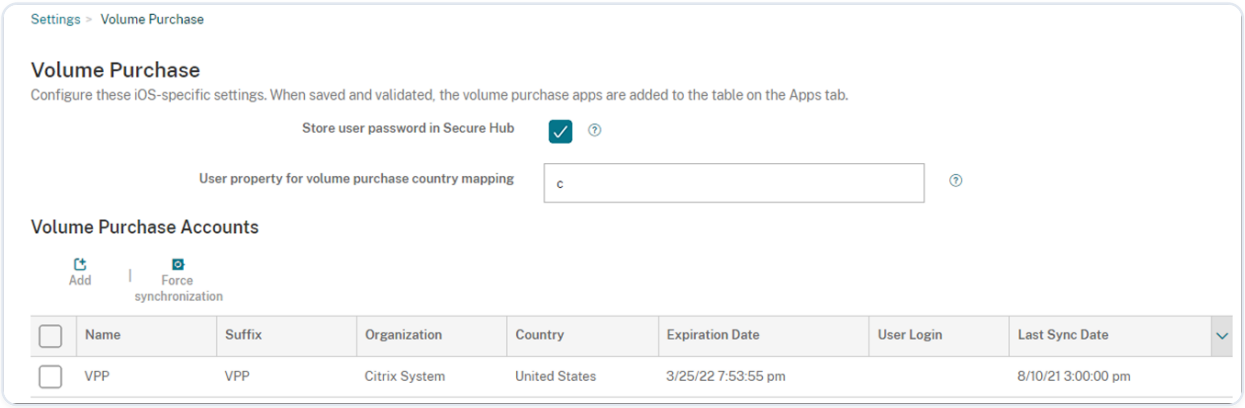
アプリ情報を手動で同期する

ABMまたはASMとの同期を強制して、最新のアプリ情報をすぐに取得できます。

1. **「設定」>「ボリューム購入」** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. ボリューム購入アカウントを選択し、**「同期を強制」** をクリックします。または、ボリューム購入アカウントを選択せずに**「同期を強制」** をクリックして、すべてのアカウントを同期します。



3. 同期アクションを確認します。同期が開始されます。

   同期には、ボリューム購入ライセンスの数に応じて数分かかる場合があります。同期が完了すると、Citrix Endpoint Managementは**「ボリューム購入」** ページを更新し、新しい**「最終同期日」** 列に同期日時を更新します。

アプリの更新を確認する

Volume Purchaseアカウントを追加する際に、**アプリの自動更新**設定をオンにすると、Citrix Endpoint Managementは、ボリューム購入アプリおよびオプションアプリの新しいバージョンを定期的に確認し、更新を行います。必要に応じて、任意のアプリの新しいバージョンを手動で確認し、Citrix Endpoint Managementにアプリの更新を適用できます。

Citrix Endpoint Managementが必須アプリの新しいバージョンを受信すると、ユーザーにプロンプトを表示することなく、新しいバージョンをデバイスにプッシュしてサイレントインストールします。

アプリの新しいバージョンを確認して適用するには

1. **構成 > アプリ**をクリックします。**アプリ**ページが表示されます。
2. アプリを選択し、**編集**をクリックします。
3. **プラットフォーム**ページに移動し、**バージョン**の横にある**更新の確認**をクリックします。
4. 表示される**更新**ダイアログボックスで、新しいバージョンが利用可能な場合は更新を適用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Volume Purchaseアカウントのコンテンツトークンを更新する

コンテンツトークンは毎年期限切れになります。トークンの有効期限が近づくと、Citrix Endpoint Managementはライセンス有効期限の警告を表示します。ユーザーの中断を防ぐために、コンテンツトークンを期限内に更新してください。

1. ABMまたはASMポータルから、更新されたトークンをダウンロードします。
2. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
3. **Volume Purchase**をクリックします。Volume Purchase構成ページが表示されます。
4. 更新されたトークン情報でVolume Purchaseアカウントを編集します。

Citrix Endpoint Management で ShareFile を使用する

免責事項:

ShareFile (現 Progress) がサポートを中止した場合、この機能は非推奨になります。

Citrix Endpoint Management には、ShareFile と統合するための2つのオプションがあります。それらは Citrix Files とストレージゾーンコネクタです。

シトリックス ファイル

Citrix Endpoint Management を構成して、ShareFile アカウントへのアクセスを提供できます。その構成では、次のことが可能です。

- ファイル共有、ファイル同期、ストレージゾーンコネクタなど、ShareFile の全機能セットにモバイルユーザーがアクセスできるようにします。
- モバイル生産性アプリユーザーの Citrix Files へのシングルサインオン認証と、包括的なアクセス制御ポリシーを提供できます。
- Citrix Endpoint Management コンソールを通じて、ShareFile の構成、サービスレベル監視、およびライセンス使用状況監視を提供します。

Enterprise アカウント向け Citrix Endpoint Management の構成の詳細については、「Citrix Files でのシングルサインオンのための SAML」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ストレージゾーンコネクタ

Citrix Endpoint Management を構成して、Citrix Endpoint Management コンソールを通じて作成したストレージゾーンコネクタにのみアクセスを提供できます。その構成では、次のことが可能です。

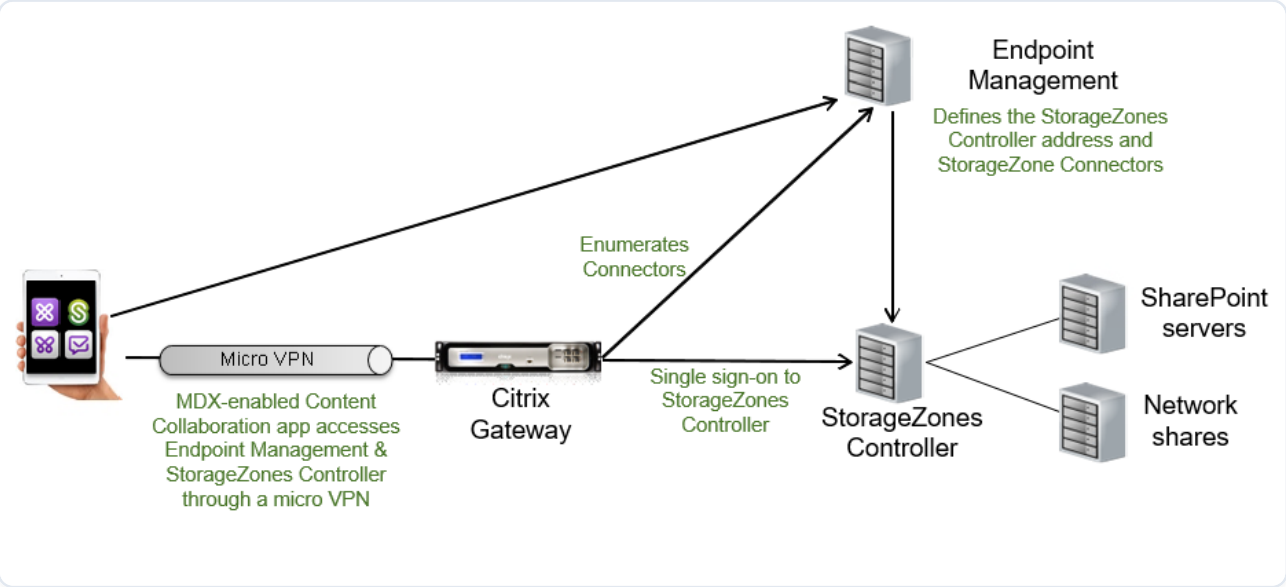
- SharePoint サイトやネットワークファイル共有など、既存のオンプレミスストレージリポジトリへの安全なモバイルアクセスを提供します。
- ShareFile サブドメインの設定や Citrix Files データのホストは不要です。
- iOS および Android 用 Citrix Files 向けの Citrix モバイル生産性アプリを通じて、ユーザーにデータへのモバイルアクセスを提供します。ユーザーは Microsoft Office ドキュメントを編集できます。また、モバイルデバイスから Adobe PDF ファイルをプレビューおよび注釈付けすることもできます。
- 企業ネットワーク外へのユーザー情報漏洩に対するセキュリティ制限に準拠します。
- Citrix Endpoint Managementコンソールを通じて、ストレージゾーンコネクタの簡単なセットアップを提供します。後でCitrix Endpoint ManagementでCitrix Filesの全機能を使用することにした場合、Citrix Endpoint Managementコンソールで構成を変更できます。

ストレージゾーンコネクタのみを使用するCitrix Endpoint Management統合の場合：

- ShareFileは、NetScaler Gatewayへのシングルサインオン構成を使用して、ストレージゾーンコントローラーで認証します。
- Citrix Filesコントロールプレーンが使用されないため、Citrix Endpoint ManagementはSAMLを介して認証しません。

次の図は、ストレージゾーンコネクタと連携したCitrix Endpoint Managementの使用に関する高レベルのアーキテクチャを示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



要件

- 最小コンポーネントバージョン：
  - iOS版シェアファイル (MDX) 5.3
  - Android版シェアファイル (MDX) 5.3
  - ストレージゾーンコントローラー 5.11.20 この記事には、ストレージゾーンコントローラー 5.0 の構成方法に関する手順が記載されています。
- ストレージゾーンコントローラーを実行するサーバーがシステム要件を満たしていることを確認してください。要件については、システム要件を参照してください。

Citrix Files Data用ストレージゾーンおよび制限付きストレージゾーンの要件は、ストレージゾーンコネクタのみを使用するCitrix Endpoint Management統合には適用されません。

Citrix Endpoint ManagementはDocumentumコネクタをサポートしていません。

- PowerShellスクリプトを実行するには:
  - PowerShellの32ビット (x86) バージョンでスクリプトを実行します。

インストールタスク

ストレージゾーンコントローラーをインストールしてセットアップするには、以下のタスクを提示された順序で完了してください。これらの手順は、Citrix Endpoint Managementとストレージゾーンコネクタの統合にのみ特化しています。これらの記事の一部は、ストレージゾーンコントローラーのドキュメントに記載されています。

1. ストレージゾーンコントローラー用にNetScalerを構成する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gatewayをストレージゾーンコントローラーの DMZプロキシとして使用できます。

2. SSL証明書をインストールする

   標準ゾーンをホストするストレージゾーンコントローラーにはSSL証明書が必要です。制限付きゾーンをホストし、内部アドレスを使用するストレージゾーンコントローラーにはSSL証明書は必要ありません。

3. サーバーを準備する

   ストレージゾーンコネクタには、IISとASP.NETのセットアップが必要です。

4. ストレージゾーンコントローラーをインストールする
5. ストレージゾーンコネクタ専用のストレージゾーンコントローラーを使用するための準備
6. ストレージゾーンのプロキシサーバーを指定する

   ストレージゾーンコントローラーコンソールを使用すると、ストレージゾーンコントローラーのプロキシサーバーを指定できます。他の方法でプロキシサーバーを指定することもできます。

7. 委任のためにドメインコントローラーがストレージゾーンコントローラーを信頼するように構成する

   ドメインコントローラーを構成して、ネットワーク共有またはSharePointサイトでのNTLMまたはKerberos認証をサポートするようにします。

8. セカンダリのストレージゾーンコントローラーをストレージゾーンに参加させる(#join-a-secondary-storage-zones-controller-to-a-storage-zone)

   高可用性のためにストレージゾーンを構成するには、少なくとも2つのストレージゾーンコントローラーを接続します。

ストレージゾーンコントローラーをインストールする

1. ストレージゾーンコントローラーソフトウェアをダウンロードしてインストールします。

   a. ShareFile Tool/App Downloadsからログオンし、最新のストレージゾーンコントローラーインストーラーをダウンロードします。

   b. ストレージゾーンコントローラーをインストールすると、サーバー上のデフォルトのWebサイトがコントローラーのインストールパスに変更されます。デフォルトのWebサイトで**匿名認証**を有効にします。

2. ストレージゾーンコントローラーをインストールするサーバーで、StorageCenter.msiを実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ストレージゾーンコントローラーのセットアップウィザードが起動します。

3. プロンプトに応答します。

   - **Destination Folder**ページで、Internet Information Services (IIS)がデフォルトの場所にインストールされている場合は、デフォルトのままにします。そうでない場合は、IISのインストール場所に移動します。
   - インストールが完了したら、**Launch Storage Zones Controller Configuration Page**のチェックボックスをオフにして、**Finish**をクリックします。

   セットアップウィザード(/en-us/citrix-endpoint-management/media/setup-wizard-clear-launch.png)

4. プロンプトが表示されたら、ストレージゾーンコントローラーを再起動します。
5. インストールが成功したことをテストするには、`https://localhost/`に移動します。(証明書エラーが発生した場合は、代わりにHTTPで接続することを検討してください。)インストールが成功すると、Citrix Filesのロゴが表示されます。

   Citrix Files のロゴが表示されない場合は、ブラウザのキャッシュをクリアして再試行してください。

   重要:

   ストレージゾーンコントローラーをクローンする予定がある場合は、ストレージゾーンコントローラーの構成を続行する前にディスクイメージをキャプチャしてください。

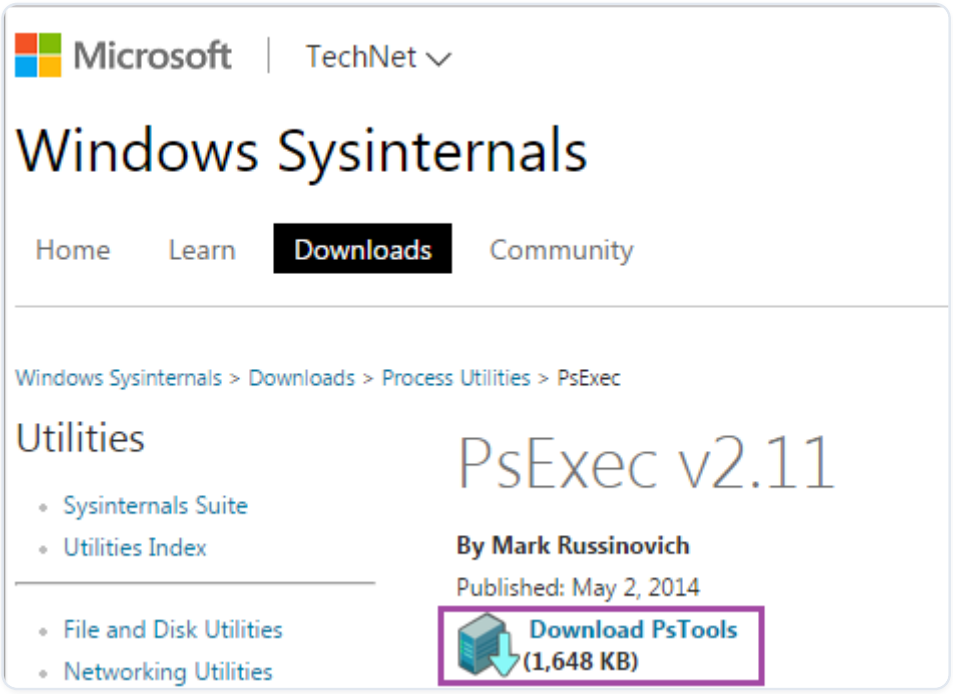
ストレージゾーンコネクタのみで使用するためのストレージゾーンコントローラーの準備

ストレージゾーンコネクタのみとの統合の場合、ストレージゾーンコントローラーの管理コンソールは使用しません。そのインターフェイスには Citrix Files 管理者アカウントが必要ですが、このソリューションでは不要です。そのため、Citrix Files コントロールプレーンなしで使用できるようにストレージゾーンコントローラーを準備するために PowerShell スクリプトを実行します。スクリプトは次のことを行います。

- 現在のストレージゾーンコントローラーをプライマリストレージゾーンコントローラーとして登録します。後でセカンダリストレージゾーンコントローラーをプライマリコントローラーに参加させることができます。
- ゾーンを作成し、そのパスフレーズを設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. ストレージゾーンコントローラーサーバーから PsExec ツールをダウンロードします。Microsoft Windows Sysinternals に移動し、**Download PsTools** をクリックします。ツールを C ドライブのルートに展開します。



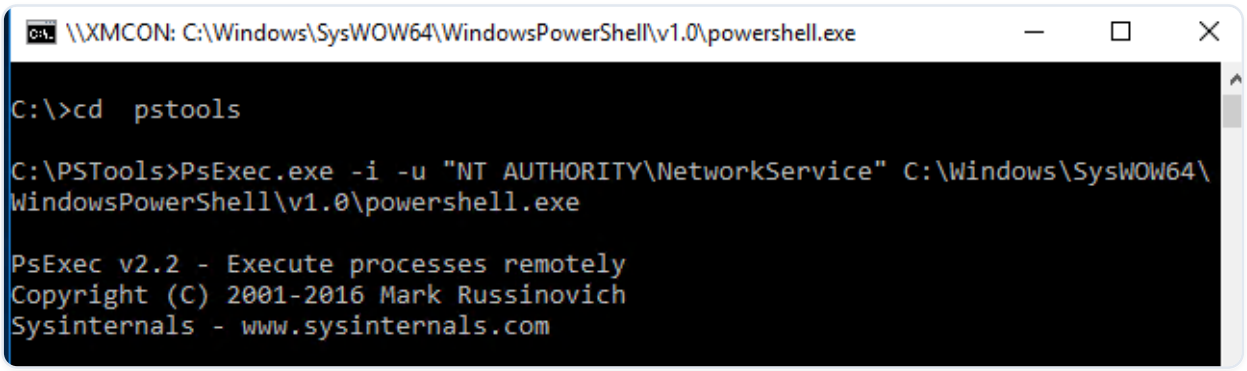
2. PsExec ツールを実行します。コマンドプロンプトを管理者ユーザーとして開き、次のように入力します。

```
```

cd c:\pstools

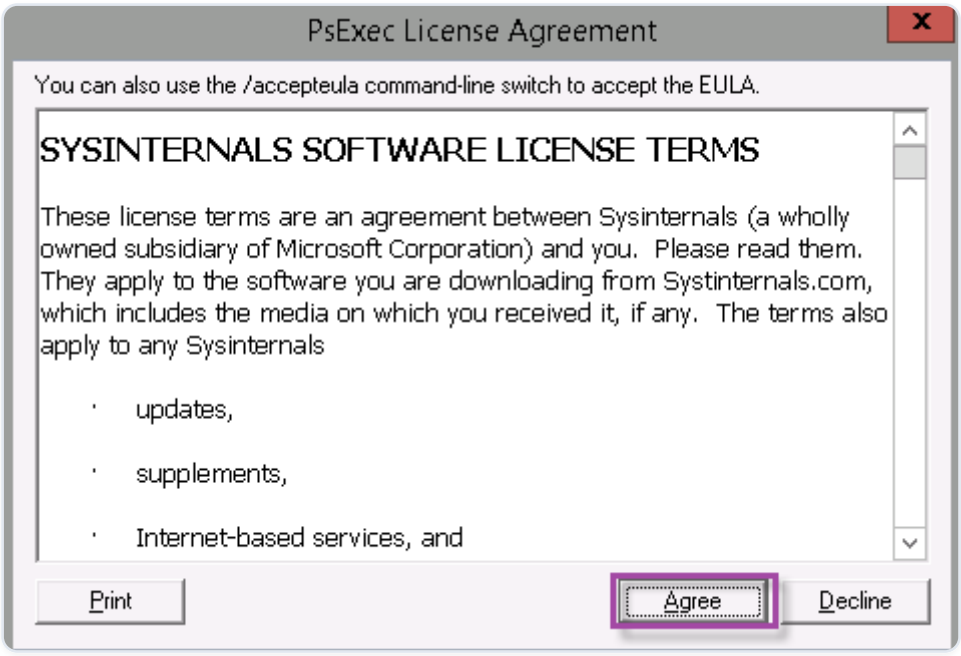
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:
\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

```
```



3. プロンプトが表示されたら、**Agree** をクリックして Sysinternals ツールを実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



PowerShell ウィンドウが開きます。

4. PowerShell ウィンドウで、次のように入力します。

```
```

Import-Module "C:
\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com

```
```

場所:

パスフレーズ: サイトに割り当てるパスフレーズです。メモしておいてください。コントローラーからパスフレーズを回復することはできません。パスフレーズを紛失した場合、ストレージゾーンを再インストールしたり、ストレージゾーンにストレージゾーンコントローラーを追加したり、サーバー障害時にストレージゾーンを回復したりすることはできません。

ExternalAddress: ストレージゾーンコントローラーサーバーの外部完全修飾ドメイン名です。

PowerShellコマンド(/en-us/citrix-endpoint-management/media/powershell-commands-create-primary-zone.png)

プライマリストレージゾーンコントローラーの準備ができました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementにログインしてストレージゾーンコネクタを作成する前に、必要に応じて以下の構成を完了してください。

ストレージゾーンのプロキシサーバーを指定する

委任のためにドメインコントローラーがストレージゾーンコントローラーを信頼するように構成する

セカンダリストレージゾーンコントローラーをストレージゾーンに参加させる

ストレージゾーンコネクタを作成するには、「Citrix Endpoint Managementでストレージゾーンコントローラー接続を定義する」を参照してください。

セカンダリストレージゾーンコントローラーをストレージゾーンに参加させる

高可用性のためにストレージゾーンを構成するには、少なくとも2つのストレージゾーンコントローラーを接続します。セカンダリストレージゾーンコントローラーをゾーンに参加させるには、2台目のサーバーにストレージゾーンコントローラーをインストールします。次に、そのコントローラーをプライマリコントローラーのゾーンに参加させます。

1. プライマリサーバーに参加させたいストレージゾーンコントローラーサーバーでPowerShellウィンドウを開きます。
2. PowerShellウィンドウで、次のように入力します。

```
Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
```

例:

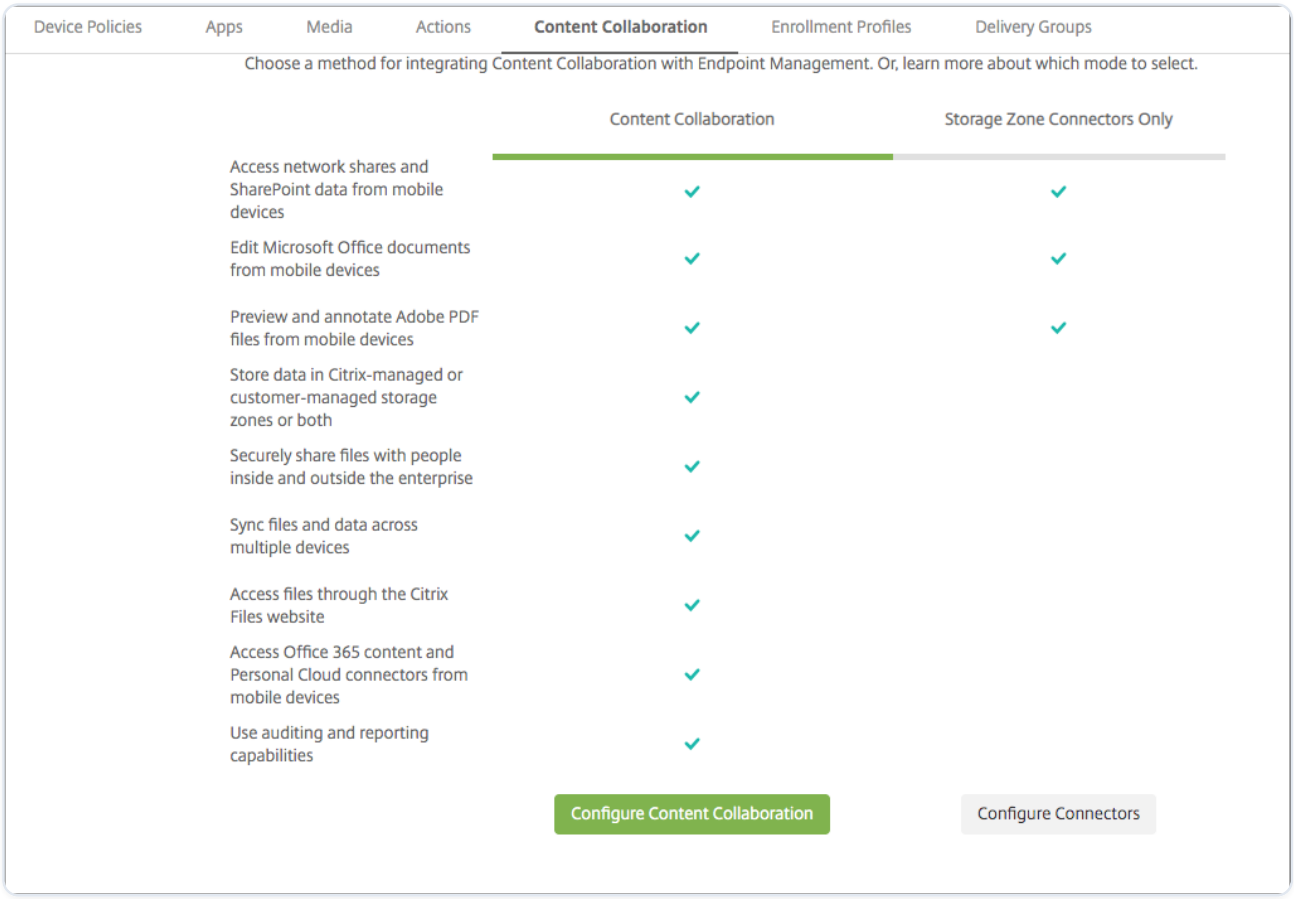
```
Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
```

Citrix Endpoint Management でストレージゾーンコントローラー接続を定義する

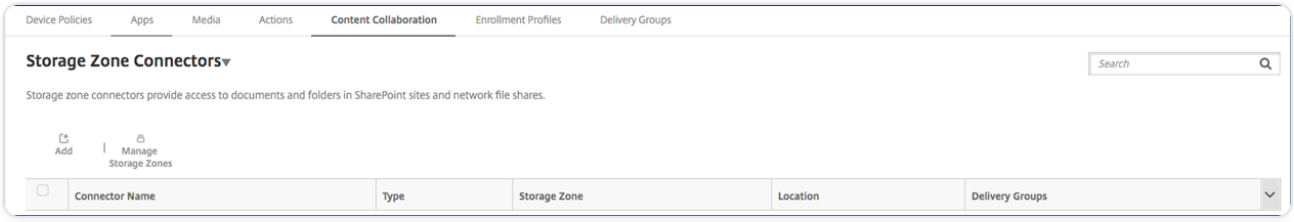
ストレージゾーンコネクタを追加する前に、ストレージゾーンコネクタに対して有効になっている各ストレージゾーンコントローラーの接続情報を構成します。ストレージゾーンコントローラーは、このセクションで説明するように定義することも、コネクタを追加するときに定義することもできます。

構成 > ShareFile ページに初めてアクセスすると、エンタープライズアカウントに Citrix Endpoint Management を使用する場合とストレージゾーンコネクタを使用する場合の違いがページに要約されます。

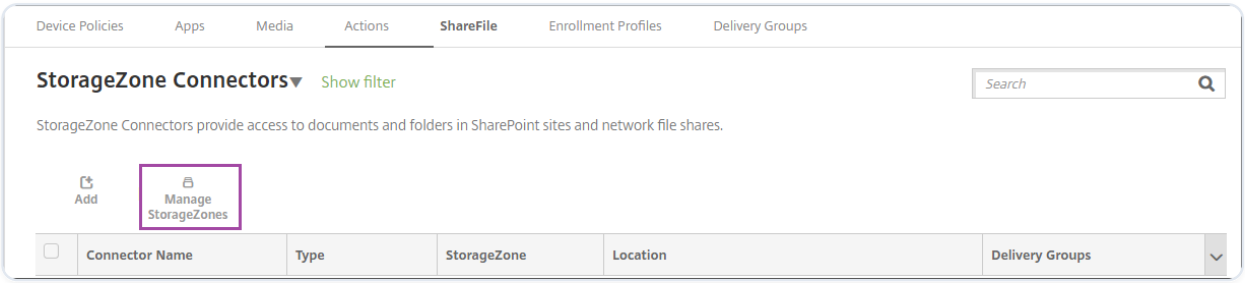
© 1997–2026 Citrix Systems, Inc. All rights reserved.



コネクタの構成をクリックして、この記事の構成手順を続行します。

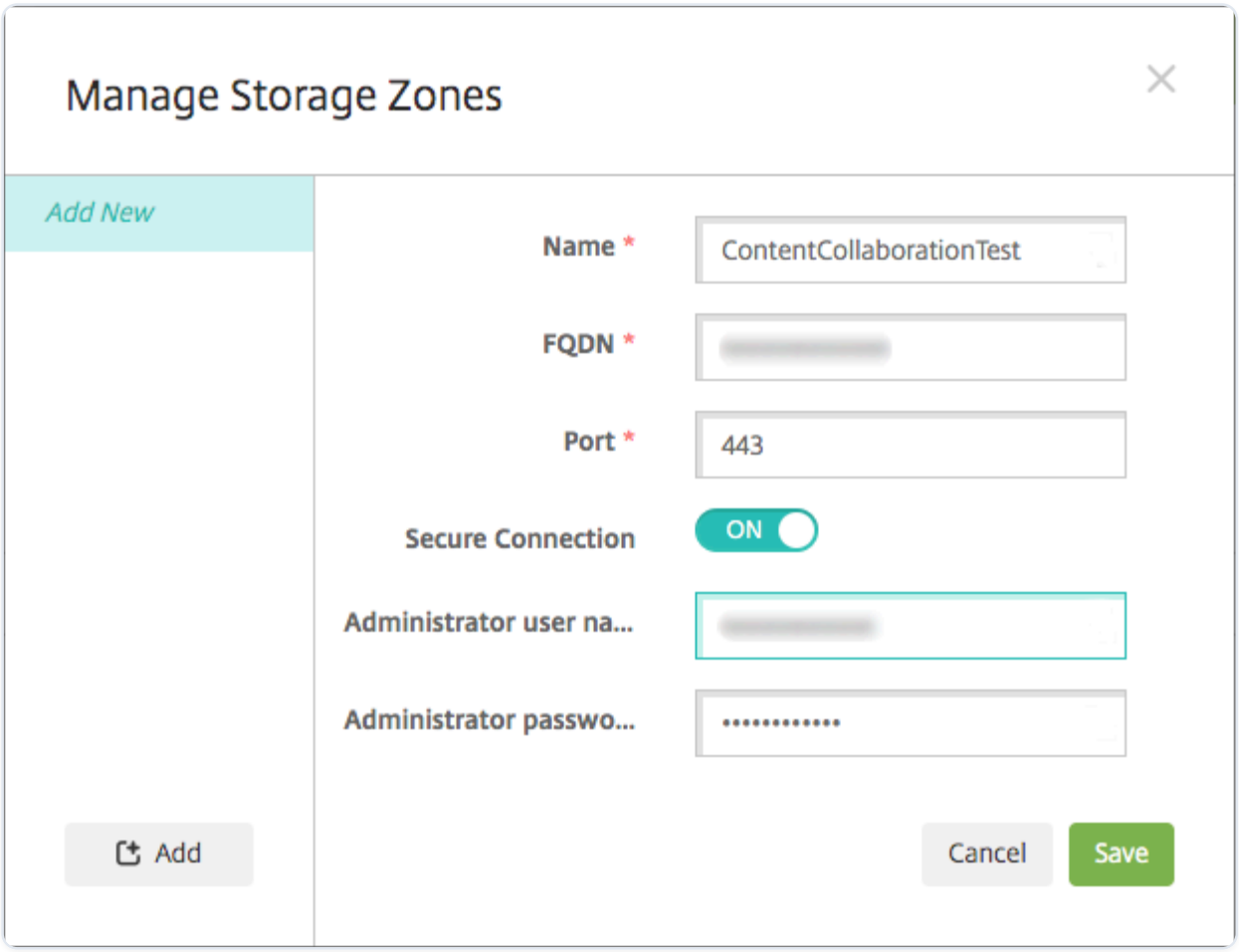


1. **構成 > ShareFile** で、**ストレージゾーンの管理**をクリックします。



2. **ストレージゾーンの管理**で、接続情報を追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **名前:** Citrix Endpoint Management でストレージゾーンを識別するために使用される、ストレージゾーンのわかりやすい名前。名前にスペースや特殊文字を含めないでください。
- **FQDNとポート:** Citrix Endpoint Management サーバーから到達可能なストレージゾーンコントローラーの完全修飾ドメイン名とポート番号。
- **セキュア接続:** ストレージゾーンコントローラーへの接続にSSLを使用する場合は、デフォルト設定の「オン」を使用します。接続にSSLを使用しない場合は、この設定を「オフ」に変更します。
- **管理者ユーザー名**と**管理者パスワード:** 管理者サービスアカウントのユーザー名（domain\\adminの形式）とパスワード。または、ストレージゾーンコントローラーに対する読み取りおよび書き込み権限を持つユーザーアカウント。

3. 「**保存**」をクリックします。
4. 接続をテストするには、Citrix Endpoint Managementサーバーがポート443でストレージゾーンコントローラーの完全修飾ドメイン名に到達できることを確認します。
5. 別のストレージゾーンコントローラー接続を定義するには、「**ストレージゾーンの管理**」で「**追加**」ボタンをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ストレージゾーンコントローラー接続の情報を編集または削除するには、「**ストレージゾーンの管理**」で接続名を選択します。次に、「**編集**」または「**削除**」をクリックします。

Citrix Endpoint Managementでストレージゾーンコネクタを追加する

1. 「**構成 > ShareFile**」に移動し、「**追加**」をクリックします。

   「ShareFile構成」(/en-us/citrix-endpoint-management/media/configure-sharefile-storagezone-connectors-no-list.png)

2. 「**コネクタ情報**」ページで、次の設定を構成します。

   「ShareFile構成」(/en-us/citrix-endpoint-management/media/configure-sharefile-add-storagezone-connector.png)

   - **コネクタ名:** Citrix Endpoint Managementでストレージゾーンコネクタを識別する名前。
   - **説明:** このコネクタに関するオプションのメモ。
   - **種類:** 「**SharePoint**」または「**ネットワーク**」のいずれかを選択します。
   - **ストレージゾーン:** コネクタに関連付けられているストレージゾーンを選択します。ストレージゾーンが一覧にない場合は、「**ストレージゾーンの管理**」をクリックしてストレージゾーンコントローラーを定義します。
   - **場所:** SharePointの場合、SharePointのルートレベルサイト、サイトコレクション、またはドキュメントライブラリのURLを`https://sharepoint.company.com`の形式で指定します。ネットワーク共有の場合、Uniform Naming Convention (UNC) パスの完全修飾ドメイン名を\\server\\shareの形式で指定します。

3. 「**デリバリーグループの割り当て**」ページで、必要に応じてコネクタをデリバリーグループに割り当てます。または、「**構成 > デリバリーグループ**」を使用してコネクタをデリバリーグループに関連付けることもできます。

ShareFile構成(/en-us/citrix-endpoint-management/media/configure-sharefile-edit-storagezone-connector-delivery-group.png)

1. 「**概要**」ページで、構成したオプションを確認できます。構成を調整するには、「**戻る**」をクリックします。
2. コネクタを保存するには、「**保存**」をクリックします。
3. コネクタをテストします。

   a. Citrix Filesクライアントをラップする場合、ネットワークアクセスポリシーを**トンネル化 - Web SSO**に設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このトンネルモードでは、MDXフレームワークがMDXアプリからのSSL/HTTPトラフィックを終端します。その後、MDXはユーザーの内部接続への新しい接続を開始します。このポリシー設定により、MDXフレームワークはWebサーバーによって発行された認証チャレンジを検出して応答できるようになります。

b. Citrix FilesクライアントをCitrix Endpoint Managementに追加します。詳細については、「Citrix FilesクライアントをCitrix Endpoint Managementに追加するには」を参照してください。

c. サポートされているデバイスから、Citrix Filesおよびコネクタへのシングルサインオンを確認します。

次のサンプルでは、SharefileDevはコネクタの名前です。

ShareFile構成(/en-us/citrix-endpoint-management/media/connector-app-1.png)

ShareFile構成(/en-us/citrix-endpoint-management/media/connector-app-2.png)

ストレージゾーンコネクタリストをフィルターする

ストレージゾーンコネクタのリストは、コネクタの種類、割り当てられたデリバリーグループ、およびストレージゾーンでフィルターできます。

1. 「**構成 > ShareFile**」に移動し、「**フィルターの表示**」をクリックします。

   「ShareFile構成」(/en-us/citrix-endpoint-management/media/configure-sharefile-storagezone-connectors-show-filter.png)

2. 選択を行うには、フィルターの見出しを展開します。フィルターを保存するには、**Save This View** をクリックし、フィルター名を入力して、**Save** をクリックします。

   「ShareFile構成」(/en-us/citrix-endpoint-management/media/configure-sharefile-filter-storagezone-connectors.png)

3. フィルターの名前を変更または削除するには、フィルター名の横にある矢印アイコンをクリックします。

   「ShareFile構成」(/en-us/citrix-endpoint-management/media/configure-sharefile-save-filter.png)

Enterpriseアカウントに切り替える

Citrix Endpoint Managementとストレージゾーンコネクタを統合した後、後で完全なEnterprise機能セットに切り替えることができます。Citrix Endpoint Managementは、既存のストレージゾーンコネクタ統合設定を保持します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure > ShareFile に移動し、**Storage Zone Connectors** ドロップダウンメニューをクリックし、次に **Configure ShareFile** をクリックします。

「ShareFile構成」(/en-us/citrix-endpoint-management/media/configure-sharefile-switch-to-enterprise.png)

Enterpriseアカウントの構成については、Citrix FilesでのシングルサインオンのためのSAML を参照してください。

HDX™アプリ向けSmartAccess

この機能を使用すると、デバイスのプロパティ、デバイスのユーザープロパティ、またはデバイスにインストールされているアプリケーションに基づいて、HDXアプリへのアクセスを制御できます。この機能は、自動アクションを設定してデバイスを非準拠としてマークし、そのデバイスへのアクセスを拒否することで使用します。この機能で使用されるHDXアプリは、非準拠デバイスへのアクセスを拒否するSmartAccessポリシーを使用して、Citrix Virtual Apps and Desktopsで構成されます。Citrix Endpoint Managementは、署名され暗号化されたタグを使用して、デバイスのステータスをStoreFrontに伝達します。その後、StoreFrontはアプリのアクセスコントロールポリシーに基づいてアクセスを許可または拒否します。

この機能を使用するには、展開環境で以下が必要です。

- シトリックス バーチャルアプリおよびデスクトップ™
- シトリックス エンドポイント管理
- タグの署名と暗号化に使用するSAML証明書で構成されたCitrix Endpoint Management。同じ証明書（秘密鍵なし）がStoreFrontサーバーにアップロードされます。

この機能の使用を開始するには：

- Citrix Endpoint Managementサーバー証明書をStoreFrontストアに構成する
- 必要なSmartAccessポリシーを使用して、少なくとも1つのCitrix Virtual Apps and Desktopsデリバリーグループを構成する
- Citrix Endpoint Managementで自動アクションを設定する

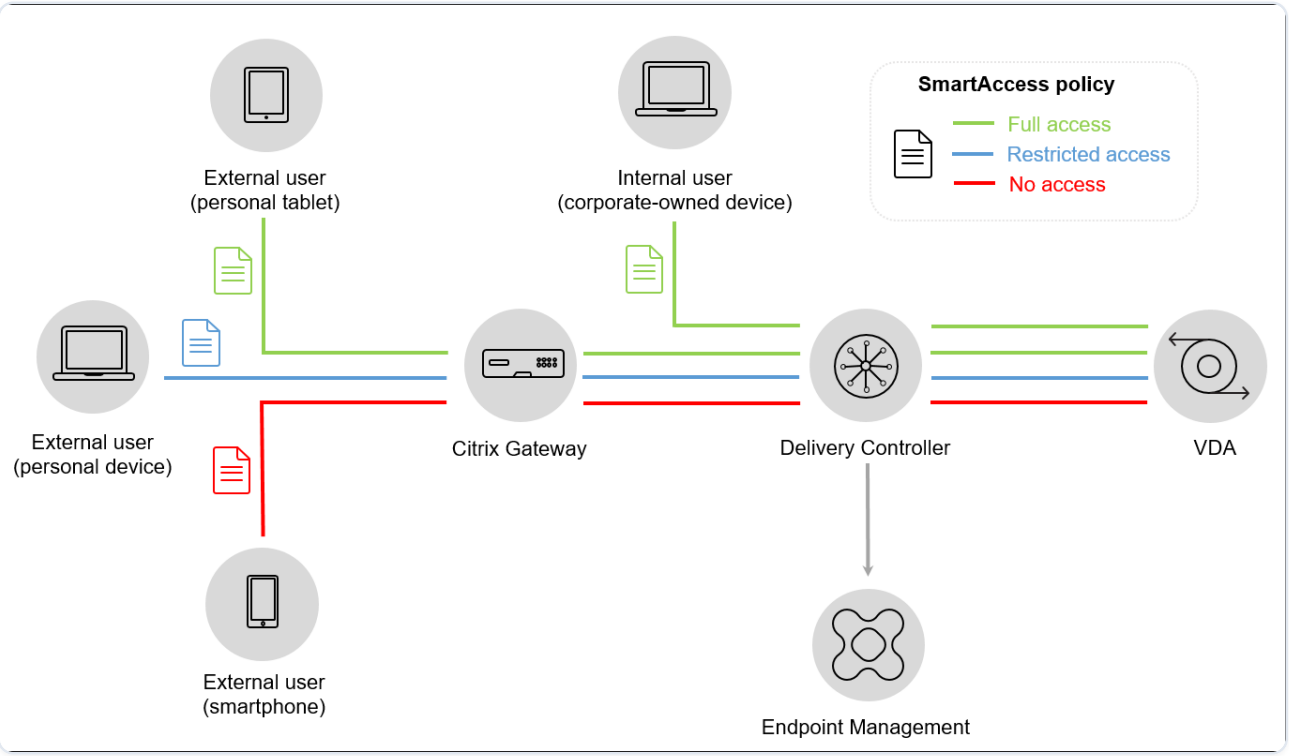
エンドポイント向けHDXアプリのSmartAccess

この機能を使用すると、ポリシーベースのアクセスコントロールを適用して、デバイスのHDXアプリへのアクセスを制限できます。HDXアプリには、次のアクセスレベルを適用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **フルアクセス**。デバイスは、Citrix Secure Hubストアが提供するすべてのHDXアプリにアクセスできます。
- **制限付きアクセス**。デバイスは、1つ以上のHDXアプリにアクセスできますが、すべてではありません。
- **アクセスなし**。デバイスは、どのHDXアプリにもアクセスできません。

次の図は、アクセス制御の仕組みを示しています。Citrix Secure HubでHDXアプリを起動しようとすると、Delivery Controllerにリクエストがトリガーされます。その後、Delivery Controllerは検証のためにCitrix Endpoint Managementサーバーにリクエストを転送します。検証の結果によって、デバイスが持つアクセスレベルが決まります。たとえば、デバイスがジェイルブレイクされている場合、HDXアプリへのアクセスは拒否されます。



Citrix Endpoint Managementサーバー証明書をエクスポートして構成し、StoreFrontストアにアップロードする

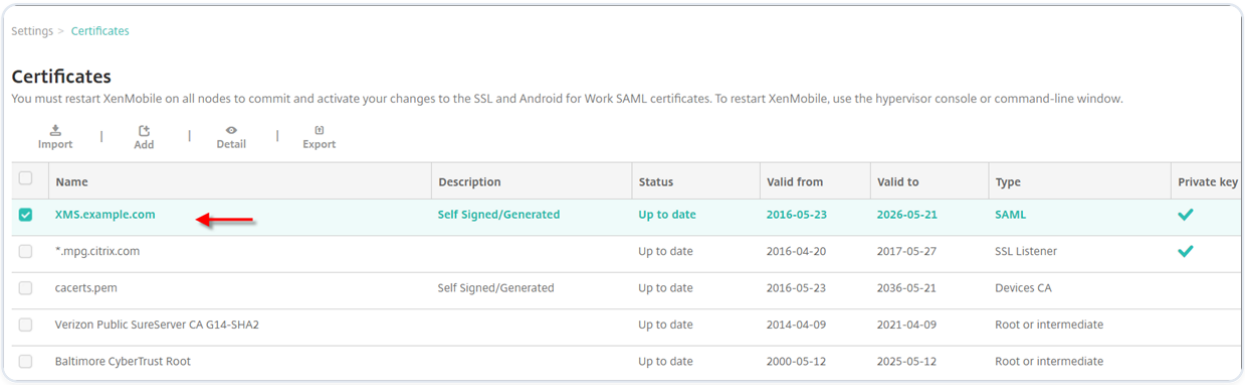
SmartAccessは、署名および暗号化されたタグを使用して、Citrix Endpoint ManagementサーバーとStoreFrontサーバー間で通信します。その通信を有効にするには、Citrix Endpoint Managementサーバー証明書をStoreFrontストアに追加します。

Citrix Endpoint Managementでドメインおよび証明書ベースの認証が有効になっている場合のStoreFrontとCitrix Endpoint Managementの統合の詳細については、サポート知識センターを参照してください。

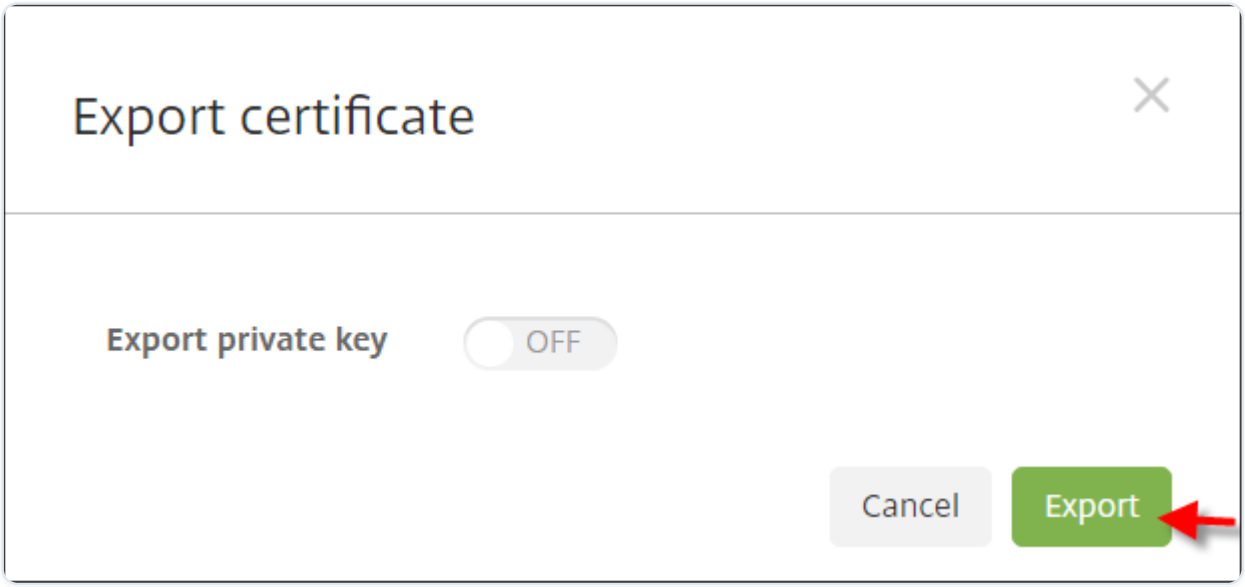
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint ManagementからSAML証明書をエクスポートする

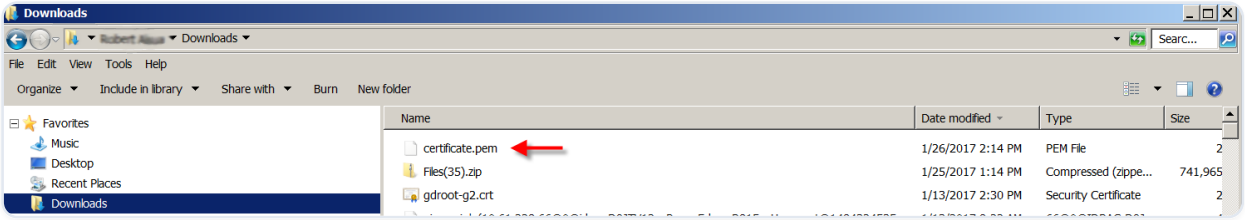
1. Citrix Endpoint Managementコンソールで、右上隅の歯車アイコンをクリックします。**設定**ページが表示されます。**証明書**をクリックします。
2. Citrix Endpoint ManagementサーバーのSAML証明書を見つけます。



3. **秘密キーのエクスポート**が**オフ**に設定されていることを確認します。**エクスポート**をクリックして、証明書をダウンロードディレクトリにエクスポートします。



4. ダウンロードディレクトリで証明書を見つけます。証明書はPEM形式です。



証明書をPEMからCERに変換する

1. Microsoft管理コンソール (MMC) を開き、**証明書 > すべてのタスク > インポート**を右クリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-import-certificate.png)

2. 証明書のインポートウィザードが表示されたら、「**次へ**」をクリックします。

   「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-import-certificate-wizard.png)

3. ダウンロードディレクトリ内の証明書を参照します。

   「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-browse-certificate.png)

4. 「**すべての証明書を次のストアに配置する**」を選択し、証明書ストアとして「**個人**」を選択します。「**次へ**」をクリックします。

   「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-import-certificate-store.png)

5. 選択内容を確認し、「**完了**」をクリックします。確認ウィンドウを閉じるには、「**OK**」をクリックします。
6. MMCで証明書を右クリックし、「**すべてのタスク > エクスポート**」を選択します。

   「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-export-certificate.png)

7. 証明書のエクスポートウィザードが表示されたら、「**次へ**」をクリックします。

   「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-export-certificate-wizard.png)

8. 形式として「**DER encoded binary X.509 (.CER)**」を選択します。「**次へ**」をクリックします。

   「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-convert-certificate.png)

9. 証明書を参照します。証明書の名前を入力し、「**次へ**」をクリックします。

   「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-export-certificate-browse.png)

10. 証明書を保存します。

    「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-export-certificate-save.png)

11. 証明書を参照し、**次へ**をクリックします。

    「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-export-certificate-browse.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. 選択内容を確認し、**完了**をクリックします。**OK**をクリックして確認ウィンドウを閉じます。

    「SmartAccess構成」(/en-us/citrix-endpoint-management/media/mmc-export-certificate-summary.png)

13. ダウンロードディレクトリで証明書を見つけます。証明書はCER形式です。

    「SmartAccess構成」(/en-us/citrix-endpoint-management/media/certificate-in-download-folder.png)

証明書をStoreFrontサーバーにコピーする

1. StoreFrontサーバーで、**SmartCert**という名前のフォルダーを作成します。
2. 証明書を**SmartCert**フォルダーにコピーします。

    「SmartAccess構成」(/en-us/citrix-endpoint-management/media/certificate-in-smartcert-folder.png)

StoreFrontストアで証明書を構成する

StoreFrontサーバーで、このPowerShellコマンドを実行して、変換されたCitrix Endpoint Managementサーバー証明書をストアに構成します。

```
Grant-STFStorePnaSmartAccess –StoreService $store –CertificatePath  “C:\xms\xms.cer” –ServerName “XMS server”
```

SmartAccess構成(/en-us/citrix-endpoint-management/media/upload-cert-storefront.png)

StoreFrontストアに既存の証明書がある場合は、このPowerShellコマンドを実行してそれらを失効させます。

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```

SmartAccess構成(/en-us/citrix-endpoint-management/media/revoke-certs-storefront.png)

または、StoreFrontサーバーで次のいずれかのPowerShellコマンドを実行して、StoreFrontストアの既存の証明書を失効させることができます。

- 名前で失効:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM
Server"
```

- サムプリントで失効:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –
CertificateThumbprint "[Thumbprint]
```

- サーバーオブジェクトで失効:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    $access = Get-STFStorePnaSmartAccess –StoreService $store



    Revoke-STFStorePnaSmartAccess –StoreService $store –SmartAccess
$access.AccessConditionsTrusts[0]
```

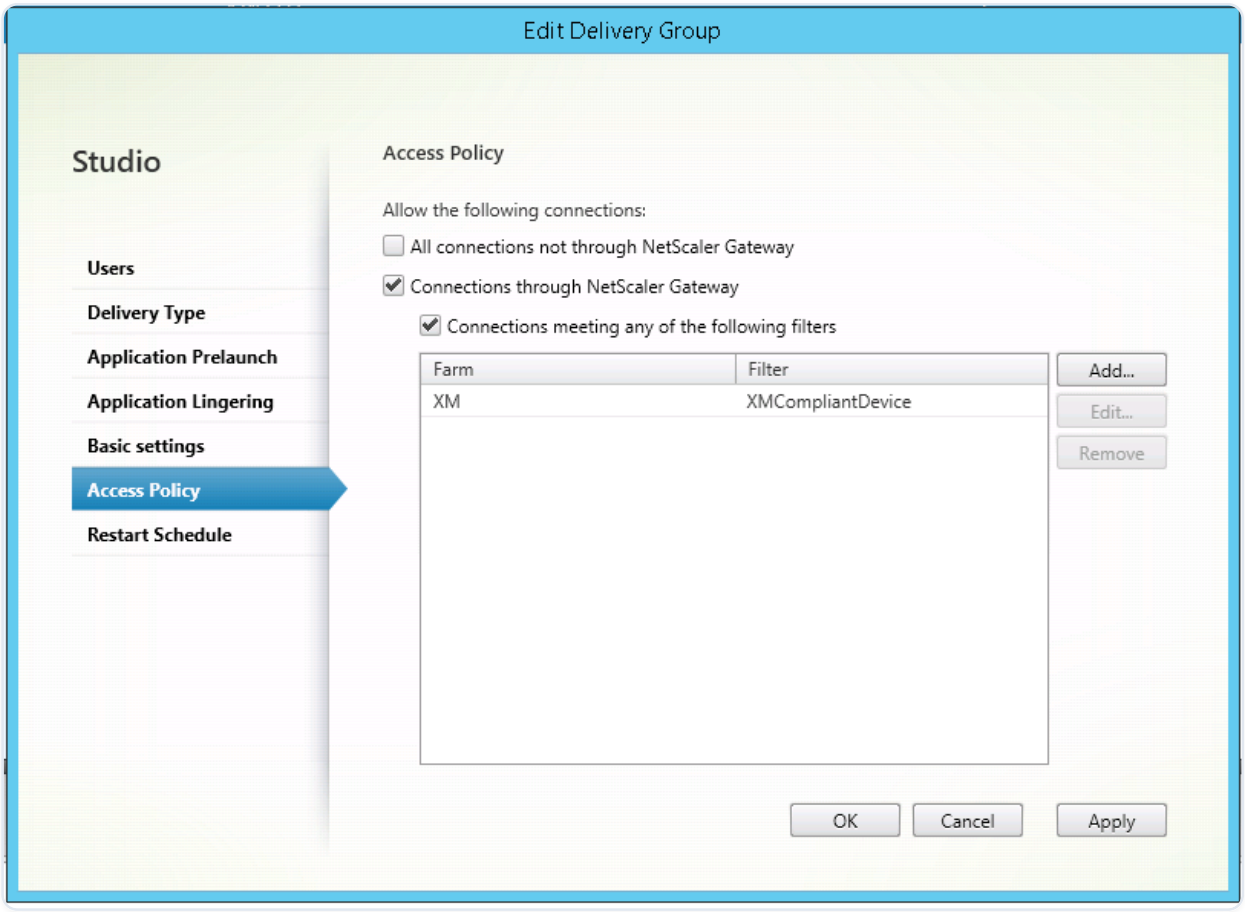
Citrix Virtual Apps and Desktops のSmartAccessポリシーを構成する

HDXアプリを配信するデリバリーグループに、必要なSmartAccessポリシーを追加するには:

1. Citrix CloudコンソールからCitrix Studioを開きます。
2. Studioナビゲーションペインで****を選択します。
3. アクセスを制御するアプリを配信するグループを選択します。次に、**ペインで**を選択します。
4. **ページで、と**を選択します。
5. ****をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

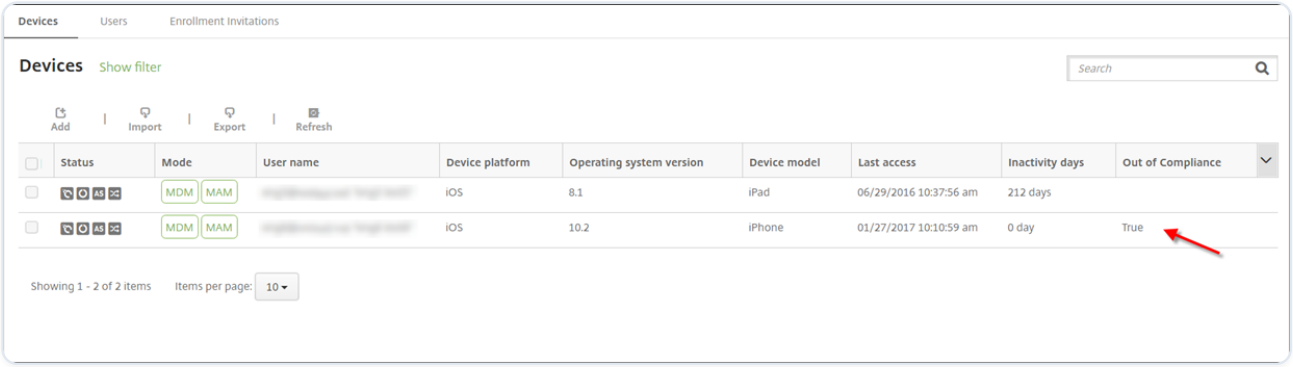
6. **がXM**で、**がXMCompliantDevice**であるアクセスポリシーを追加します。



7. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**OK**をクリックします。

Citrix Endpoint Managementで自動アクションを設定する

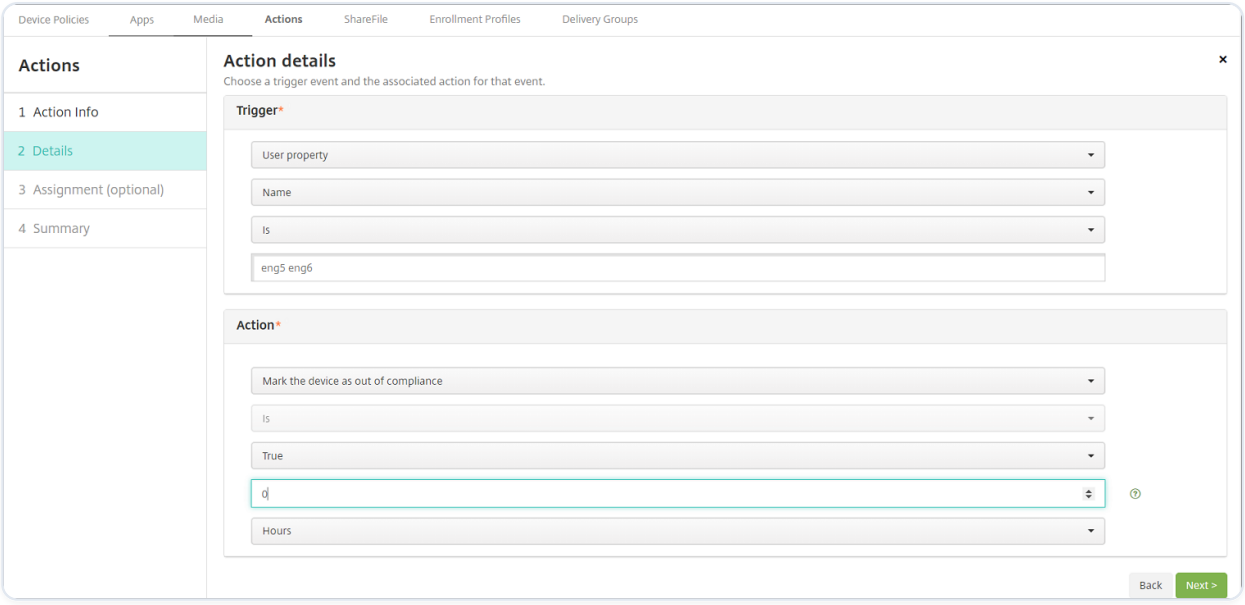
HDXアプリのデリバリーグループで設定したSmartAccessポリシーは、デバイスがコンプライアンス違反の場合、そのデバイスへのアクセスを拒否します。自動アクションを使用して、デバイスをコンプライアンス違反としてマークします。



1. Citrix Endpoint Managementコンソールで、**構成 > アクション**をクリックします。**アクション**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. アクションを追加するには、**追加**をクリックします。**アクション情報**ページが表示されます。
3. **アクション情報**ページで、アクションの名前と説明を入力します。
4. **次へ**をクリックします。**アクションの詳細**ページが表示されます。次の例では、ユーザープロパティ名が**eng5**または**eng6**であるデバイスを直ちにコンプライアンス違反としてマークするトリガーが作成されます。



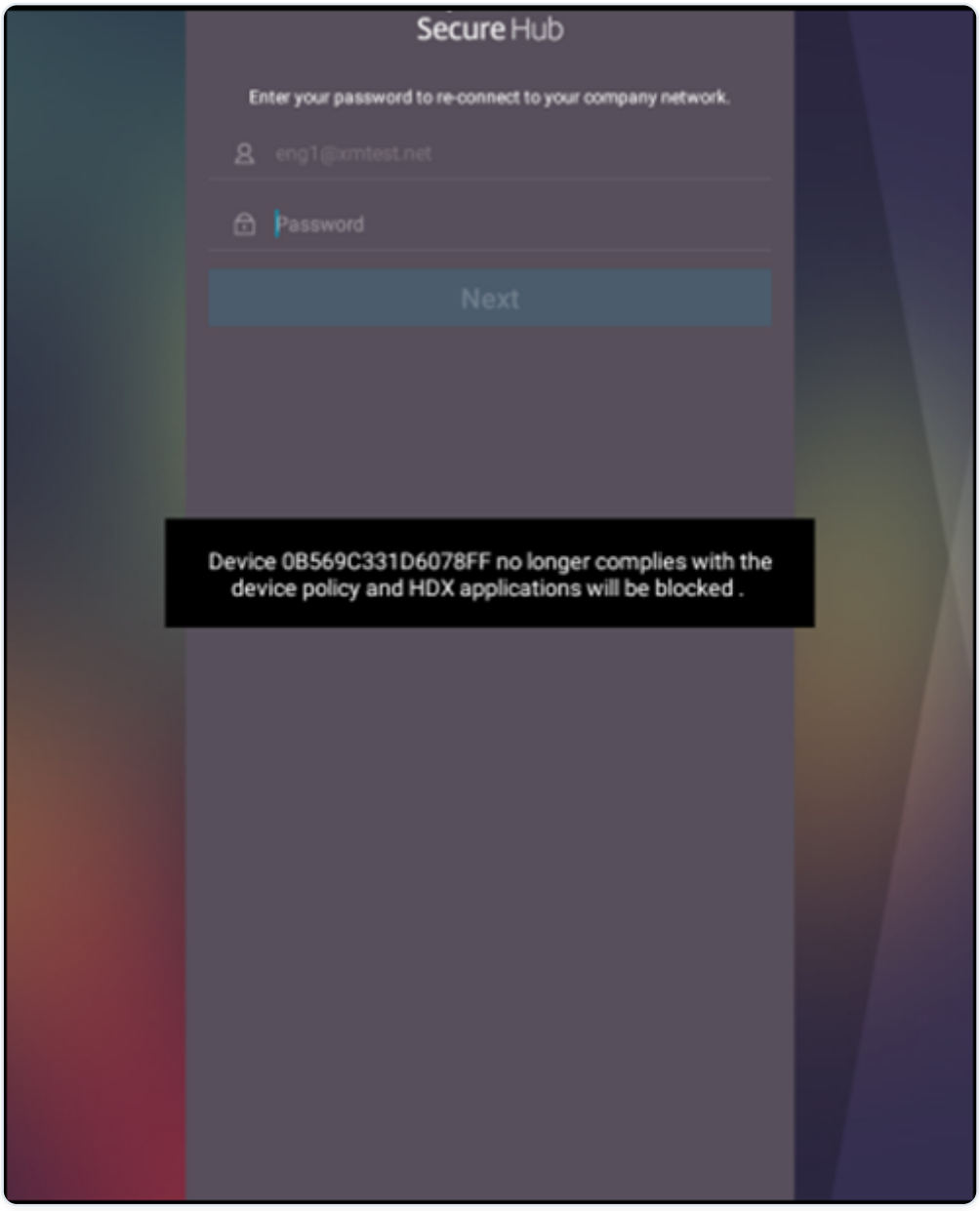
5. **トリガー**リストで、**デバイスプロパティ**、**ユーザープロパティ**、または**インストール済みアプリ名**を選択します。SmartAccessはイベントトリガーをサポートしていません。
6. **アクション**リストで：
   - **デバイスをコンプライアンス違反としてマーク**を選択します。
   - **次と等しい**を選択します。
   - **True**を選択します。
   - トリガー条件が満たされたときにデバイスをすぐに非準拠としてマークするアクションを設定するには、時間枠を**0**に設定します。
7. このアクションを適用するCitrix Endpoint Managementデリバリーグループを選択します。
8. アクションの概要を確認します。
9. **次へ**をクリックし、**保存**をクリックします。

デバイスが非準拠としてマークされると、HDXアプリはCitrix Secure Hubストアに表示されなくなります。ユーザーはアプリのサブスクライブを解除されます。デバイスに通知は送信されず、Citrix Secure HubストアにはHDXアプリが以前利用可能であったことを示すものは何もありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスが非準拠としてマークされたときにユーザーに通知したい場合は、通知を作成し、その通知を送信する自動アクションを作成します。

この例では、デバイスが非準拠としてマークされたときに、次の通知を作成して送信します。「デバイスのシリアル番号または電話番号がデバイスポリシーに準拠しなくなったため、HDXアプリケーションはブロックされました。」



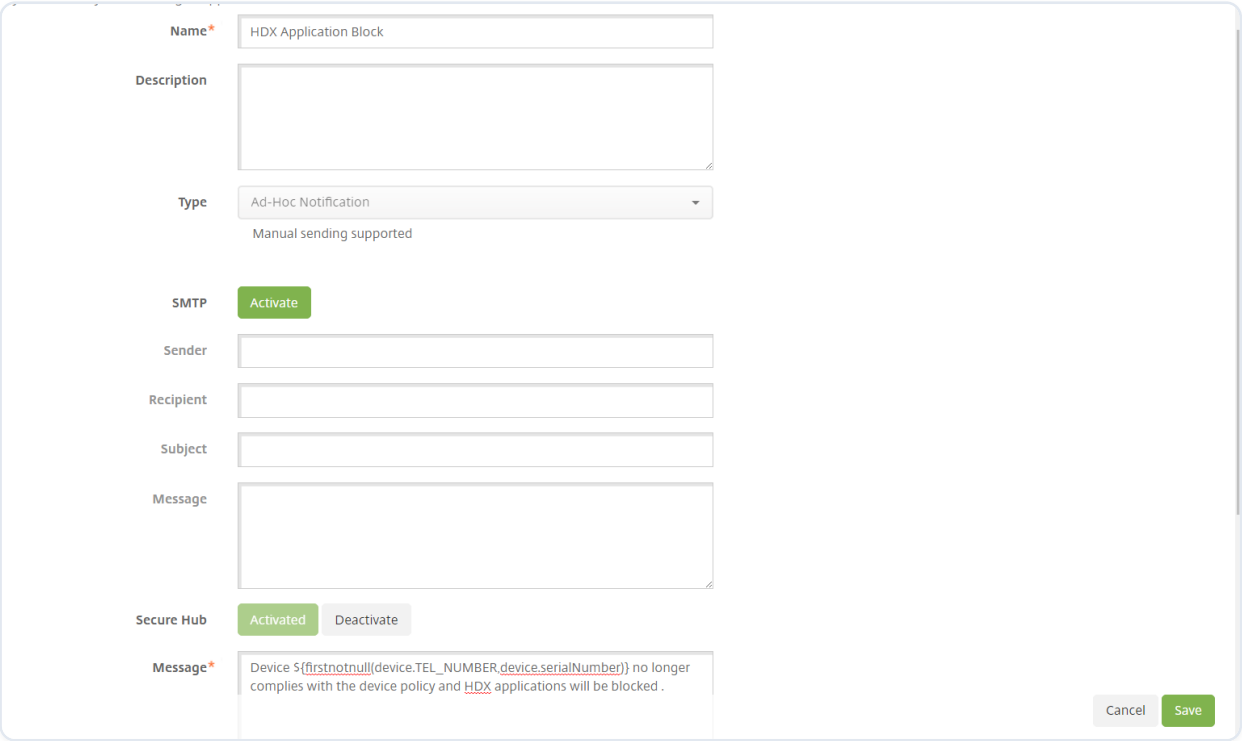
デバイスが非準拠としてマークされたときにユーザーに表示される通知を作成する

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **通知テンプレート**をクリックします。**通知テンプレート**ページが表示されます。
3. **通知テンプレート**ページで**追加**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 次の設定を構成します。

   - **名前:** HDXアプリケーションブロック
   - **説明:** デバイスが非準拠の場合のエージェント通知
   - **種類:** アドホック通知
   - **Citrix Secure Hub:** アクティブ化済み
   - **メッセージ:** デバイス `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` がデバイスポリシーに準拠しなくなり、HDXアプリケーションがブロックされました。



5. **保存**をクリックします。

デバイスが非準拠とマークされたときに通知を送信するアクションを作成します

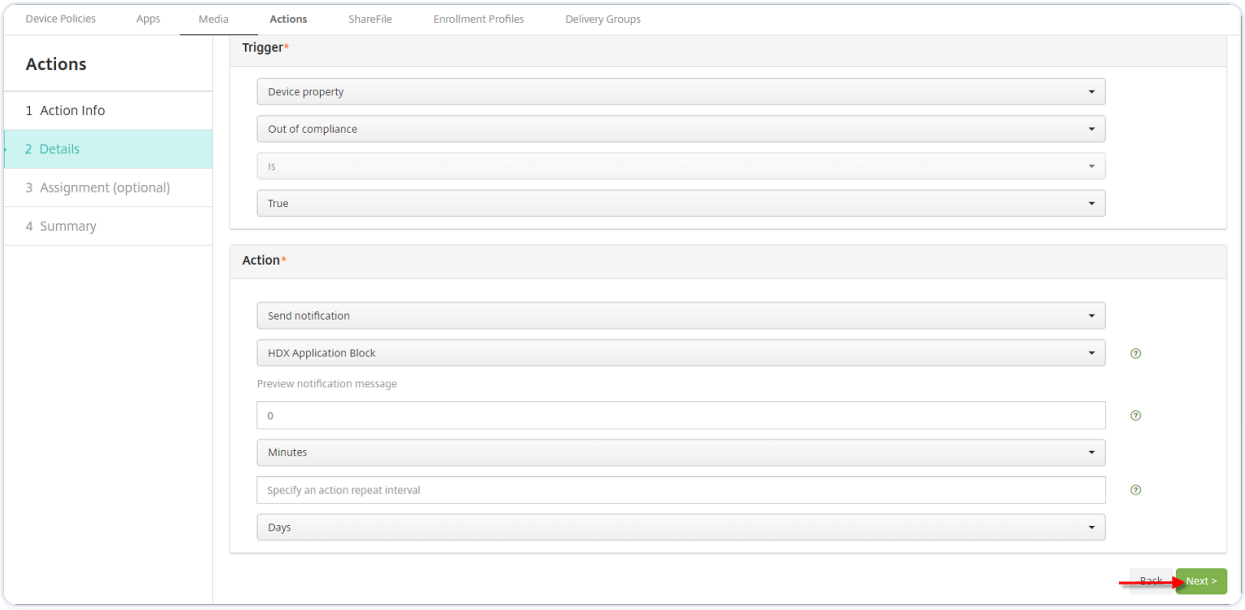
1. Citrix Endpoint Managementコンソールで、**構成 > アクション**をクリックします。**アクション**ページが表示されます。
2. **追加**をクリックしてアクションを追加します。**アクション情報**ページが表示されます。
3. **アクション情報**ページで、アクションの名前と説明を入力します。

   - 名前: HDXブロック通知
   - **説明:** デバイスが非準拠であるためHDXブロック通知

4. **次へ**をクリックします。**アクションの詳細**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. **トリガー**リストで:
    - **デバイスプロパティ**を選択します。
    - **非準拠**を選択します。
    - 「**Is**」を選択します。
    - 「**True**」を選択します。



6. **アクション**リストで、トリガーが満たされたときに実行されるアクションを指定します。
    - 「**通知を送信**」を選択します。
    - 「**HDX Application Block, 作成した通知**」を選択します。
    - 「**0**」を選択します。この値を0に設定すると、トリガー条件が満たされたときに通知が送信されます。
7. このアクションを適用する Citrix Endpoint Management デリバリーグループを選択します。この例では、「**AllUsers**」を選択します。
8. アクションの概要を確認します。
9. 「**次へ**」をクリックし、「**保存**」をクリックします。

自動アクションの設定の詳細については、「自動アクション」を参照してください。

ユーザーが HDX アプリへのアクセスを回復する方法

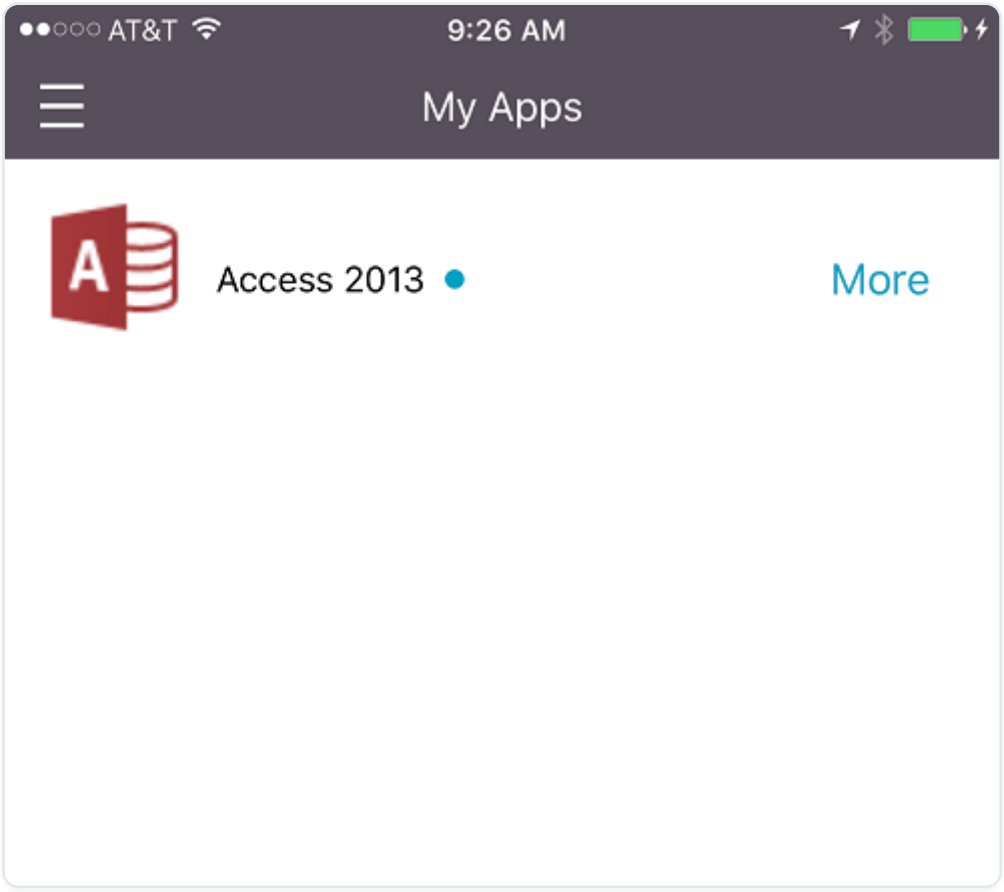
デバイスがコンプライアンスに準拠した状態に戻った後、ユーザーは HDX アプリに再度アクセスできるようになります。

1. デバイスで、Citrix Secure Hub ストアに移動して、ストア内のアプリを更新します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. アプリに移動し、アプリの「**追加**」をタップします。

アプリが追加されると、新しくインストールされたアプリであるため、My Appsに青い点が付いて表示されます。



MDXまたはエンタープライズアプリをアップグレードする

Citrix Endpoint ManagementでMDXまたはエンタープライズアプリをアップグレードするには、Citrix Endpoint Managementコンソールでアプリを無効にし、その後、アプリの新しいバージョンをアップロードします。

1. Citrix Endpoint Managementコンソールで、**Configure > Apps**をクリックします。**Apps**ページが表示されます。
2. 管理対象デバイス（モバイルデバイス管理のためにCitrix Endpoint Managementに登録されているデバイス）の場合、手順3に進みます。非管理対象デバイス（エンタープライズアプリ管理目的でのみCitrix Endpoint Managementに登録されているデバイス）の場合、次の操作を行います。

    a. **Apps**テーブルで、アプリの横にあるチェックボックスをオンにするか、更新するアプリがある行をクリックします。

    b. 表示されるメニューで**Disable**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリメニュー(/en-us/citrix-endpoint-management/media/configure-apps-disable-app.png)

c. 確認ダイアログボックスで**Disable**をクリックします。アプリの**Disable**列に*Disabled*と表示されます。

無効化されたアプリ(/en-us/citrix-endpoint-management/media/configure-apps-disable-app-disabled.png)

> **注：**
>
> アプリが無効になっている間、ユーザーはログオフ後にアプリに再接続できません。アプリの無効化は任意ですが、アプリの機能に関する問題を回避するために、アプリを無効にすることをお勧めします。たとえば、新しいバージョンをアップロードしているときにユーザーがアプリのダウンロードを要求すると、問題が発生する可能性があります。

3. **Apps**テーブルで、アプリの横にあるチェックボックスをクリックするか、更新するアプリがある行をクリックします。
4. 表示されるメニューで**Edit**をクリックします。**App Information**ページが表示され、アプリ用に最初に選択したプラットフォームが選択されています。
5. 次の設定を構成します:

   - **名前：** 必要に応じて、アプリ名を変更します。
   - **説明:** 必要に応じて、アプリの説明を変更します。
   - **アプリカテゴリ:** 必要に応じて、アプリカテゴリを変更します。

6. **次へ**をクリックします。最初に選択したプラットフォームページが表示されます。選択した各プラットフォームについて、以下を実行します。

   a. **アップロード**をクリックしてファイルの場所に移動し、アップロードする置換ファイルを選択します。アプリがCitrix Endpoint Managementにアップロードされます。

   Android Enterprise用アプリをアップロードしている場合、管理対象Google Playウィンドウが表示されます。ここでアプリの新しいバージョンをアップロードします。詳細については、「Android Enterpriseアプリの配布」を参照してください。

   b. 必要に応じて、プラットフォームのアプリの詳細とポリシー設定を変更します。

   c. 必要に応じて、展開ルールとアプリストアを構成します。詳細については、「MDXアプリの追加」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. **保存**をクリックします。**アプリ**ページが表示されます。
8. 手順2でアプリを無効にした場合は、以下を実行します。

    a. **アプリ**テーブルで、更新したアプリをクリックして選択し、表示されるメニューで**有効にする**をクリックします。

    b. 表示される確認ダイアログボックスで、**有効にする**をクリックします。これでユーザーはアプリにアクセスできるようになり、アプリのアップグレードを促す通知を受け取ります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メディアを追加

Citrix Endpoint Managementにメディアを追加して、ユーザーデバイスに展開できます。Apple Volume Purchaseを通じて入手したApple BooksをCitrix Endpoint Managementを使用して展開できます。

Citrix Endpoint ManagementでVolume Purchaseアカウントを構成すると、購入済みおよび無料の書籍が**構成** > **メディア**に表示されます。**メディア**ページから、配信グループを選択し、展開ルールを指定することで、iOSデバイスに展開する書籍を構成します。

ユーザーが初めて書籍を受け取り、Volume Purchaseライセンスを承諾すると、展開された書籍がデバイスにインストールされます。書籍はApple Bookアプリに表示されます。書籍ライセンスをユーザーから関連付け解除したり、デバイスから書籍を削除したりすることはできません。Citrix Endpoint Managementは、書籍を必須メディアとしてインストールします。ユーザーがインストール済みの書籍をデバイスから削除しても、その書籍はApple Bookアプリに残ったままで、ダウンロード準備ができています。

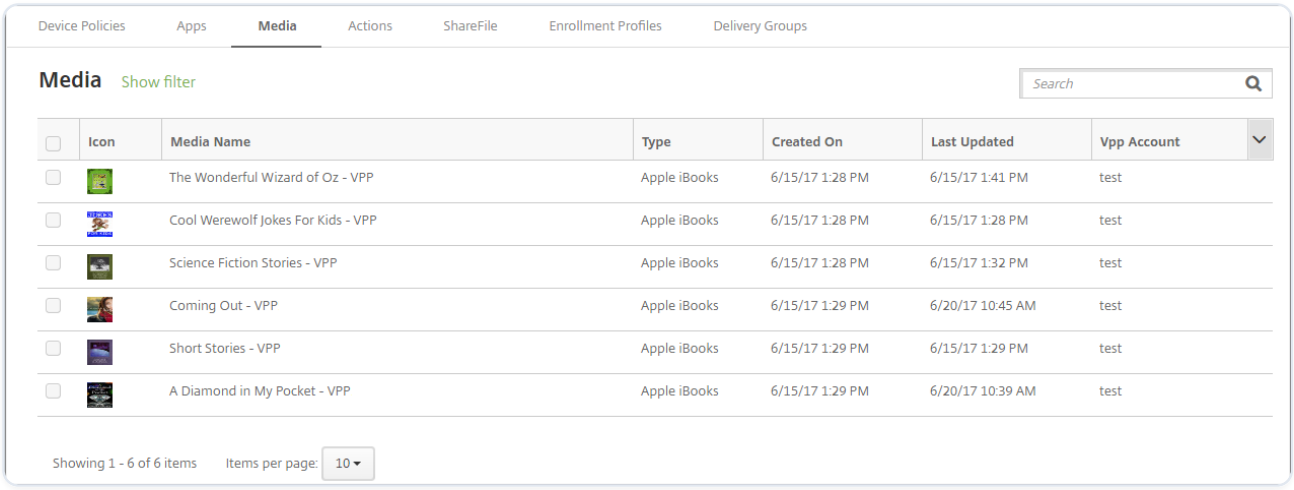
前提条件

- iOSデバイス
- (/ja-jp/citrix-endpoint-management/apps/apple-volume-purchase.html)で説明されているように、Citrix Endpoint ManagementでApple Volume Purchaseを構成します。

書籍の構成

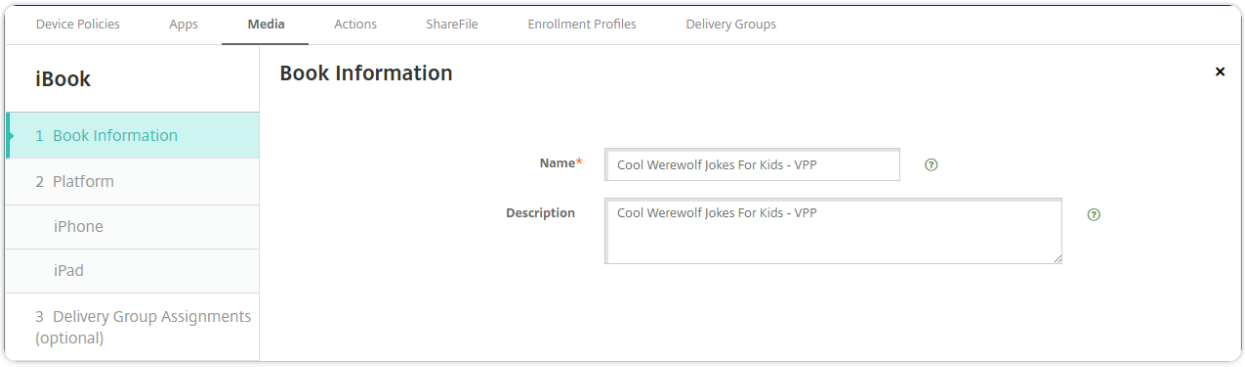
Volume Purchaseを通じて入手したApple Booksは、**構成** > **メディア**ページに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Apple Bookを展開用に構成するには

1. **構成 > メディア**で、書籍を選択し、**編集**をクリックします。**書籍情報**ページが表示されます。



名前と**説明**は、Citrix Endpoint Managementコンソールとログにのみ表示されます。

2. **iPhone iBook設定**および**iPad iBook設定**ページで：書籍の名前と説明は任意で変更できますが、Citrix®はこれらの設定を変更しないことを推奨します。画像は情報提供のみを目的としており、編集できません。**有料iBook**は、書籍がApple Volume Purchaseを通じて購入されたことを示します。

   「書籍の構成」(/en-us/citrix-endpoint-management/media/configure-media-ibooks-vp-iphone.png)

   デプロイ規則を指定したり、ボリューム購入情報を表示したりすることもできます。

   「書籍の構成」(/en-us/citrix-endpoint-management/media/configure-media-ibooks-vp-settings.png)

3. 必要に応じて、書籍をデリバリーグループに割り当て、展開スケジュールを設定します。

   「書籍の構成」(/en-us/citrix-endpoint-management/media/configure-media-ibooks-vp-delivery-groups.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure > Delivery Groupsの**Media**タブから、書籍をデリバリーグループに割り当てることもできます。Citrix Endpoint Managementは、必須の書籍展開のみをサポートしています。

「書籍の構成」(/en-us/citrix-endpoint-management/media/configure-delivery-groups-media-ibooks-vp.png)

4. **Manage > Devices**の**Media**タブを使用して、展開ステータスを表示します。

「書籍の構成」(/en-us/citrix-endpoint-management/media/manage-devices-media-ibook-vp.png)

> **注：**
>
> **Configure** > **Media**ページで書籍を選択して**Delete**をクリックすると、Citrix Endpoint Managementはリストから書籍を削除します。ただし、Citrix Endpoint Managementが次回Apple Volume Purchaseと同期するときに、Apple Volume Purchaseから削除されていない限り、その書籍はリストに再表示されます。リストから書籍を削除しても、デバイスから書籍が削除されるわけではありません。

書籍は、次の例に示すようにユーザーデバイスに表示されます。

「書籍の構成」(/en-us/citrix-endpoint-management/media/store-ibooks-samples.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リソースを展開する

デバイスの構成と管理には通常、Citrix Endpoint Managementコンソールでリソース（ポリシー、アプリ、メディア）とアクションを作成し、それらをデリバリーグループを使用してパッケージ化する作業が含まれます。デリバリーグループはユーザーのカテゴリを定義するため、指定されたポリシー、アプリ、メディア、およびアクションをデバイスに展開できます。Citrix Endpoint Managementコンソールを使用して、次のことができます。

- デリバリーグループを追加、管理、展開する。
- Citrix Endpoint Management がデリバリーグループ内のリソースとアクションをデバイスにプッシュする順序を変更します。この順序は *展開順序* と呼ばれます。

  Citrix Endpoint Managementコンソールで展開順序を指定できます。ただし、ユーザーが重複または競合するポリシーを持つ複数のデリバリーグループに属している場合、Citrix Endpoint Managementが展開順序を決定します。「計算手順」を参照してください。

デリバリーグループについて

デリバリーグループへの包含は通常、会社、国、部署、オフィス住所、役職などのユーザー特性に基づいています。デリバリーグループを使用すると、誰がどのリソースをいつ取得するかをより詳細に制御できます。デリバリーグループをすべてのユーザーに展開することも、定義されたユーザーグループに展開することもできます。

Citrix Endpoint Managementをインストールして構成すると、デフォルトのデリバリーグループであるAllUsersが作成されます。このグループには、すべてのローカルユーザーとActive Directoryユーザーが含まれます。AllUsersグループを削除することはできませんが、すべてのユーザーにリソースをプッシュしたくない場合は無効にできます。詳細については、「AllUsersデリバリーグループを有効または無効にする」を参照してください。

デリバリーグループにリソースを展開すると、そのデリバリーグループ内のすべてのユーザーにプッシュ通知が送信されます。Appleデバイスの場合、Apple Push Notificationサービス（APNs）を使用して通知を送信します。詳細については、「APNs証明書」を参照してください。Androidデバイスの場合、Firebase Cloud Messaging（FCM）を使用します。詳細については、「Firebase Cloud Messaging」を参照してください。Windowsデバイスの場合、Windows Push Notification Service（WNS）を使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リソースの展開について

デバイスにリソースをプッシュする際には、次の点を考慮してください。

- 展開順序: 展開順序とは、Citrix Endpoint Managementがリソース（ポリシー、アプリ、メディア）とアクションをデバイスにプッシュする順序のことです。展開順序は、デバイス管理（MDM）またはアプリケーション管理（MAM）とMDMの組み合わせ用に登録プロファイルが構成されているデリバリーグループ内のデバイスに適用されます。
- 展開ルール: Citrix Endpoint Managementは、ユーザーおよびデバイスのプロパティに対して指定した展開ルールを使用して、ポリシー、アプリ、メディア、アクション、およびデリバリーグループをフィルタリングします。たとえば、展開ルールでは、ドメイン名が特定の値と一致する場合に展開パッケージをプッシュするように指定できます。

  デリバリーグループ内で、ユーザーおよびデバイスのプロパティに基づいてリソースを受け取るユーザーとデバイスのサブセットを指定できます。デリバリーグループ内のユーザーおよびデバイスのプロパティによるフィルタリングは、リソースに設定された展開ルールよりも優先されます。
- **展開スケジュール:** Citrix Endpoint Managementは、ポリシー、アプリ、メディア、およびアクションに対して指定した展開スケジュールを使用して、これらのアイテムの展開を制御します。展開が今すぐ、設定された日時、または展開条件が満たされたときに発生するように指定できます。ルールを作成するときにスケジュールを指定します。「展開ルールを構成する」を参照してください。

デリバリーグループを追加する前に、展開順序、ルール、およびスケジュールが展開目標とどのように関連するかを検討してください。

展開順序

展開順序とは、Citrix Endpoint Management がリソースをデバイスにプッシュする順序のことです。リソースに前提条件がある場合や、リソース間に依存関係がある場合、展開順序は重要です。リソースには、ポリシー、アプリ、アクション、デリバリーグループが含まれます。

たとえば、証明書ベースの認証を持つ Wi-Fi ポリシーをプッシュする場合、Wi-Fi ポリシーの前に証明書ポリシーをプッシュする必要があります。そうしないと、エラーが発生します。逆に、一部のポリシー（利用規約、ソフトウェアインベントリ、アクションなど）では、展開順序は関係ありません。

デリバリーグループを追加するときに、リソースがデバイスに展開される順序を指定できます。ただし、Citrix Endpoint Management は、ユーザーが重複または競合するポリシーを持つ複数のデリバリーグループに属している状況を常に識別します。これらの場合、Citrix Endpoint

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Management は、デバイスに配信するオブジェクトと実行するアクションの両方について、展開順序を計算します。

展開順序を決定する際、Citrix Endpoint Management は、展開ルールや展開スケジュールなどのフィルターと制御基準をリソースに適用します。次の表は、これらの基準のどれを各リソースタイプに適用できるかを示しています。

リソース	デバイスプラットフォーム	展開ルール	展開スケジュール	ユーザー/グループ
デバイスポリシー	Y	Y	Y	-
アプリ	Y	Y	Y	-
メディア	Y	Y	Y	-
アクション	-	Y	Y	-
デリバリーグループ	-	Y	-	Y

計算手順

Citrix Endpoint Managementが展開順序を計算する必要がある場合、以下の手順を実行します。

注：

デバイスプラットフォームは計算手順に影響しません。

1. ユーザー、グループ、および展開規則のフィルターに基づいて、特定のユーザーに対するすべてのデリバリーグループを決定します。
2. 選択したデリバリーグループ内のすべてのリソース（ポリシー、アプリ、メディア、アクション）の順序付きリストを作成します。このリストは、デバイスプラットフォーム、展開規則、および展開スケジュールに基づいて作成されます。順序付けアルゴリズムは次のとおりです。

    a. 管理者が定義した展開順序を持つデリバリーグループのリソースを、そうでないデリバリーグループのリソースよりも前に配置します。詳細については、「ユーザー定義の順序による計算例」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. デリバリーグループ間のタイブレーカーとして、デリバリーグループ名で逆アルファベット順にリソースを並べ替えます。たとえば、Citrix Endpoint Managementは、デリバリーグループBのリソースをデリバリーグループAのリソースよりも前に配置します。

c. 並べ替え中に、デリバリーグループのリソースに対して管理者が定義した展開順序が指定されている場合は、その順序を維持します。それ以外の場合は、そのデリバリーグループ内のリソースをリソース名でアルファベット順に並べ替えます。

d. 同じリソースが複数回出現する場合は、重複するリソースを削除します。これらのリソースのうち、最初のものだけを配信します。

管理者定義の順序に関連付けられたリソースは、管理者定義の順序がないリソースよりも先に展開されます。

管理者定義の順序による計算の例

2つのデリバリーグループがあるとします。

- デリバリーグループ Account Managers 1: リソースの順序は *未指定* です。ポリシーは **Network** と **Passcode** です。
- Delivery group Account Managers 2: With *specified* order for resources. Has the policies **Connection scheduling**, **Restrictions**, **Passcode**, and **Network**, in order.

計算アルゴリズムがデプロイグループを名前のみで順序付けした場合、Citrix Endpoint Managementは、デリバリーグループ Account Managers 1から開始して、**Network**、**Passcode**、**Connection scheduling**、**Restrictions**の順で展開する可能性があります。Citrix Endpoint Managementは、Account Managers 2デリバリーグループからの重複する**Passcode**と**Network**を無視する可能性があります。

しかし、Account Managers 2グループには管理者指定の展開順序があります。そのため、計算アルゴリズムはAccount Managers 2デリバリーグループのリソースをAccount Managers 1デリバリーグループのリソースよりもリストの上位に配置します。結果として、Citrix Endpoint Managementはポリシーを**Connection scheduling**、**Restrictions**、**Passcode**、**Network**の順で展開します。Citrix Endpoint Managementは、Account Managers 1デリバリーグループからのポリシー**Network**と**Passcode**を重複しているため無視します。このアルゴリズムは、Citrix Endpoint Management管理者が指定した順序を尊重します。

展開ルールの構成

特定の条件が満たされたときにリソースを配信するように展開ルールを構成します。基本または高度な展開ルールを構成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

展開ルールの基本構成(/en-us/citrix-endpoint-management/media/deployment-rules.png)

基本エディターを使用して展開ルールを追加するときは、まずリソースを展開するタイミングを選択します。

- **すべて:** ユーザーまたはデバイスが構成したすべての条件を満たした場合にリソースを配信します。
- **いずれか:** ユーザーまたはデバイスが構成した条件の少なくとも1つを満たした場合にリソースを配信します。

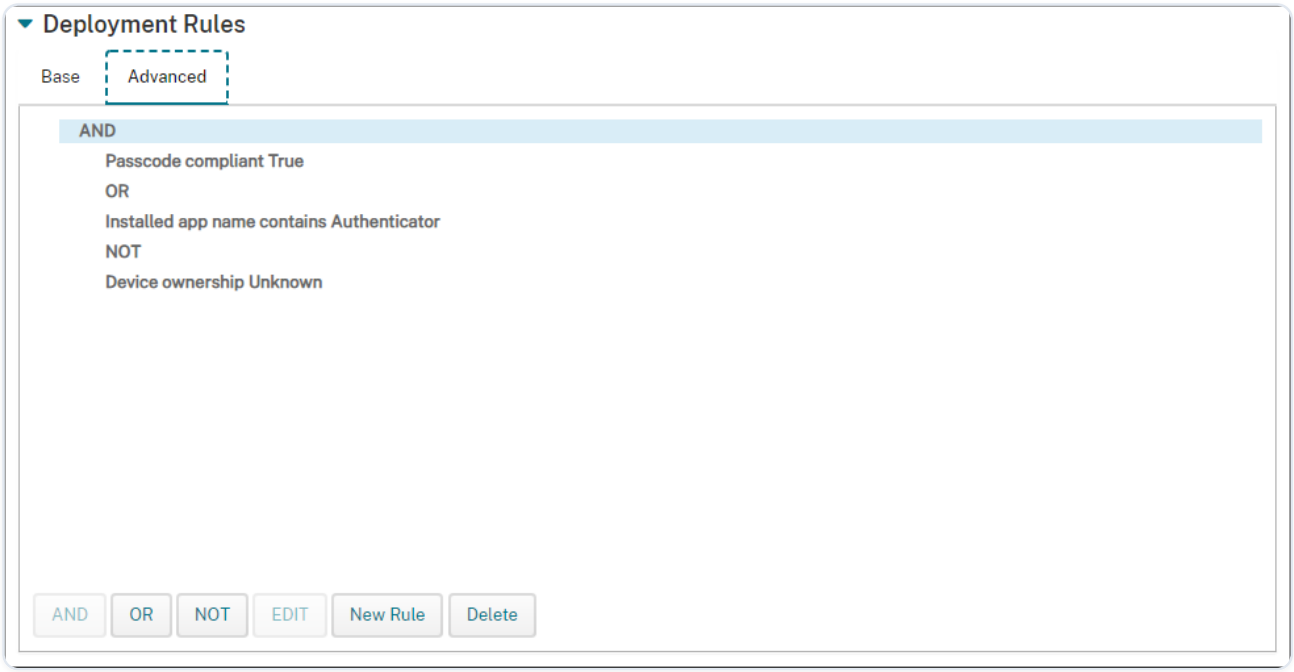
新しいルールをクリックして、追加する利用可能なルールの一覧からルールを選択します。利用可能なルールは、展開されるリソースと、リソースを構成するプラットフォームによって異なります。各ルール内には条件があります。

リソースを展開するように指定できます。

- 選択したプロパティが存在する場合のみ、または選択したプロパティが存在する場合を除く。
- プロパティが入力したテキストと完全に一致する場合、プロパティが入力したテキストを含む場合、またはプロパティが入力したテキストと一致しない場合。
- デバイスまたはユーザーが選択したプロパティに準拠している場合、または選択したプロパティに準拠していない場合。
- デバイスまたはユーザーのプロパティが、定義済みリストから選択した条件と一致する場合。

高度なエディターを使用して、より複雑な展開ルールを作成できます。高度なルールを作成する際には、より多くのルールから選択し、さまざまなブール論理演算子を組み合わせることができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



デリバリーグループの操作

デリバリーグループは、次の方法で操作できます。

- デリバリーグループを追加する
- デリバリーグループに展開する
- デリバリーグループを削除する
- デリバリーグループを編集する
- AllUsers デリバリーグループを有効または無効にする。

デリバリーグループを追加する

デリバリーグループを作成する際、ユーザー割り当てをCitrix Endpoint Managementで管理するか、Citrix Cloudで管理するかを指定します。デリバリーグループの作成後、この指定を変更することはできません。

デリバリーグループを他のCitrix Cloudサービスに提供する予定がある場合は、Citrix Cloudでユーザー割り当てを管理するように指定します。その他のCitrix Cloudサービスには、Citrix Virtual Apps and Desktops、ShareFile、またはSecure Browser Serviceが含まれます。Citrix Cloudで管理されているデリバリーグループにのみ、Active Directoryユーザーを追加できます。

ユーザーとアプリのデリバリーグループに対してモビリティ管理のみが必要な場合は、**ユーザー割り当ての管理**を**Citrix Endpoint Managementで**に設定します。Citrix Endpoint Managementでユーザーが管理されているデリバリーグループはCitrix Cloudでは表示されません。そのため、

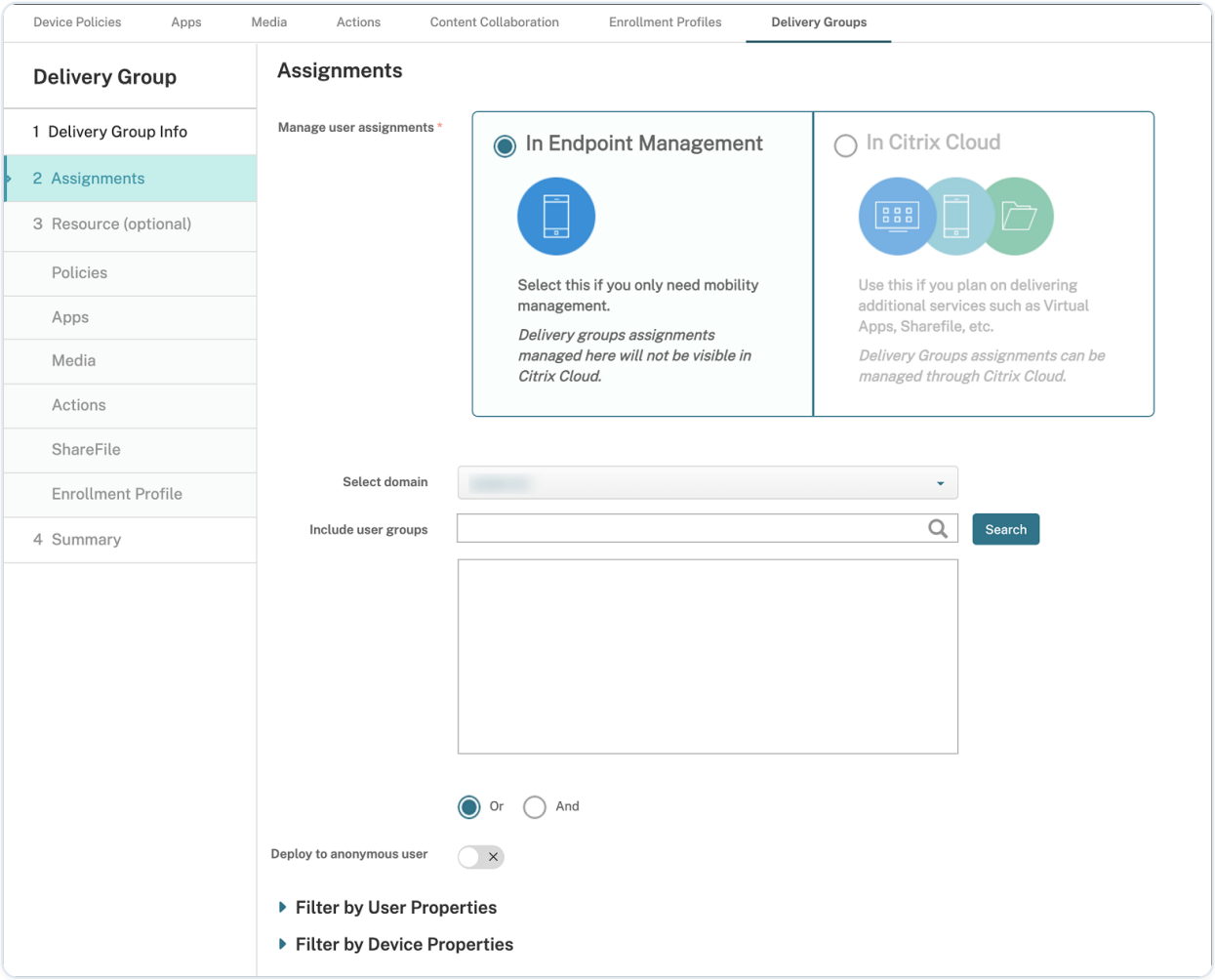
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementで管理されているデリバリーグループを他のサービスの提供に使用することはできません。

注：

デバイスポリシーと登録プロファイルを作成する前に、デリバリーグループを追加することをお勧めします。それらの作成方法については、「デバイスポリシー」および「登録プロファイル」を参照してください。

1. Citrix Endpoint Managementコンソールで、**構成 > デリバリーグループ**をクリックします。
2. **デリバリーグループ**ページで、**追加**をクリックします。
3. **デリバリーグループ情報**ページで、デリバリーグループの名前と説明を入力し、**次へ**をクリックします。
4. **割り当て**ページで、デリバリーグループの割り当てを管理する方法を指定します。



- **ユーザー割り当ての管理：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Citrix Endpoint Managementで：** モビリティ管理のみが必要なユーザーとアプリのデリバリーグループを作成する予定がある場合は、このオプションを選択します。Citrix Endpoint Managementでユーザー割り当てが管理されているデリバリーグループはCitrix Cloudでは表示されず、他のサービスの提供に使用することはできません。
- **Citrix Cloudで：** デリバリーグループを他のサービスの提供に使用する予定がある場合は、このオプションを選択します。これらのサービスには、Citrix Virtual Apps and DesktopsやShareFileが含まれる場合があります。

5. デリバリーグループにユーザーを追加します。

> **重要：**
>
> デリバリーグループの作成後、**ユーザー割り当ての管理**設定を変更することはできません。

- **ドメインの選択:** リストから、ユーザーを選択するドメインを選択します。
- **ユーザーグループを含める:** 次のいずれかを実行します。
  - ユーザーグループのリストで、追加するグループをクリックします。選択したグループは、**選択したユーザーグループ**リストに表示されます。
  - **検索**をクリックすると、選択したドメイン内のすべてのユーザーグループのリストが表示されます。検索ボックスにグループ名の全部または一部を入力し、**検索**をクリックして検索を絞り込むこともできます。

  選択したユーザーグループリストからユーザーグループを削除するには、次のいずれかを実行します。

  - **選択したユーザーグループ**リストで、削除する各グループの横にある**X**をクリックします。
  - **検索**をクリックすると、選択したドメイン内のすべてのユーザーグループのリストが表示されます。または、**検索**をクリックする前にグループ名の全部または一部を入力して検索を絞り込みます。削除する各グループのチェックボックスをオフにします。
- **または/および:** リソースが展開されるユーザーが、いずれかのグループに属しているか (Or)、すべてのグループに属している必要があるか (And) を選択します。
- **匿名ユーザーに展開:** デリバリーグループ内の認証されていないユーザーに展開するかどうかを選択します。認証されていないユーザーとは、認証できないものの、Citrix Endpoint Managementへのデバイス接続を許可したユーザーのことです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. **ユーザープロパティでフィルター**または**デバイスプロパティでフィルター**を展開して、デリバリーグループがリソースを管理する方法を指定します。

   - **デバイスプロパティでフィルター**を選択した場合は、デバイスプラットフォームを展開して展開ルールを構成します。

     - **デバイスプロパティ - Android** (「Androidデバイスにリソースを展開するルールを作成する」を参照)
     - **デバイスプロパティ - iOS**
     - **デバイスプロパティ - Windowsデスクトップ/タブレットのみ**

   - 「**Base**」タブがデフォルトで表示されます。「**Base**」タブで、ポリシーを展開するタイミングを指定します。**すべての**条件が満たされたときにポリシーを展開するか、**いずれかの**条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは「**すべて**」に設定されています。

     - 「**新しいルール**」をクリックして条件を定義します。
     - リストから条件を選択します。たとえば、「デバイス所有権」と「BYOD」を選択します。
     - 追加する条件ごとに「**新しいルール**」をクリックします。

   - 「**詳細設定**」タブをクリックして、ルールをブールオプションと組み合わせます。「**Base**」タブで選択した条件が表示されます。

     - 「**AND**」、「**OR**」、または「**NOT**」をクリックし、次に「**新しいルール**」をクリックします。
     - リストからルールに追加する条件を選択し、右側のプラス記号（+）をクリックします。

       いつでも条件をクリックして選択し、「**編集**」をクリックして条件を変更するか、「**削除**」をクリックして条件を削除できます。

7. 「**次へ**」をクリックして「**ポリシー**」ページに移動します。ここでは、必要に応じてデリバリーグループのポリシー、アプリ、メディア、またはアクションを追加できます。詳細については、以下を参照してください。

   - デリバリーグループにポリシーを追加する
   - デリバリーグループにアプリを追加する
   - デリバリーグループにメディアを追加する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- デリバリーグループにアクションを追加する

8. デリバリーグループの設定に問題がなければ、「**概要**」をクリックして構成の概要を表示します。
9. 「**保存**」をクリックします。新しいデリバリーグループが「**デリバリーグループ**」ページに表示されます。

デリバリーグループにポリシーを追加する

1. **リソース (オプション)** リストから、**ポリシー**をクリックします。
2. 追加するポリシーごとに、次の操作を行います。

   - 利用可能なポリシーのリストをスクロールして、追加するポリシーを見つけます。または、検索ボックスにポリシーの完全名または部分名を入力し、**検索**をクリックします。
   - 追加したいポリシーを右側のボックスにドラッグします。

   ボックスからポリシーを削除するには、ポリシー名の横にある**X**をクリックします。
3. **次へ**をクリックして、**アプリ**ページに移動します。

デリバリーグループにアプリを追加する

1. 追加するアプリごとに、次の操作を行います。

   - 利用可能なアプリのリストをスクロールして、追加するアプリを見つけます。または、検索ボックスにアプリの完全名または部分名を入力し、**検索**をクリックします。
   - アプリを**必須アプリ**ボックスまたは**オプションアプリ**ボックスのいずれかにドラッグします。

   必須としてマークされたアプリの場合、ユーザーは次のような状況で迅速に更新を受け取ることができます。

   - 新しいアプリをアップロードし、それを必須としてマークした場合。
   - 既存のアプリを必須としてマークした場合。
   - ユーザーが必須アプリを削除した場合。
   - Citrix Secure Hub のアップデートが利用可能です。

   必須アプリの強制展開に関する情報 (機能の有効化方法を含む) については、「必須アプリとオプションアプリについて」を参照してください。

   ボックスからアプリを削除するには、アプリ名の横にある **X** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **次へ** をクリックして、**メディア** ページに移動します。

デリバリーグループにメディアを追加する

1. 追加する各ブックについて、以下を実行します。

   - 利用可能なブックのリストをスクロールして、追加したいブックを見つけます。または、検索ボックスにブックの完全な名前または部分的な名前を入力し、**検索** をクリックします。
   - 追加したいブックを **必須ブック** ボックスにドラッグします。

   必須としてマークされたブックの場合、ユーザーは次のような状況で速やかにアップデートを受け取ります。

   - 新しいブックをアップロードし、それを必須としてマークした場合。
   - 既存のブックを必須としてマークした場合。
   - ユーザーが必須ブックを削除した場合。
   - Citrix Secure Hub のアップデートが利用可能です。

   ボックスからブックを削除するには、ブック名の横にある **X** をクリックします。
2. **次へ** をクリックして、**アクション** ページに移動します。

デリバリーグループにアクションを追加する

1. 追加するアクションごとに、次の操作を行います。

   - 利用可能なアクションのリストをスクロールして、追加したいアクションを見つけます。または、検索ボックスにアクションの完全な名前または部分的な名前を入力し、**検索**をクリックします。
   - 追加したいアクションを右側のボックスにドラッグします。

   ボックスからアクションを削除するには、アクション名の横にある**X**をクリックします。
2. **次へ**をクリックして、**ShareFile**ページに移動します。

ShareFile構成を適用する

ShareFileページは、Citrix Endpoint Management (**構成 > ShareFile**) をエンタープライズアカウント用に構成したか、ストレージゾーンコネクタ用に構成したかによって異なります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

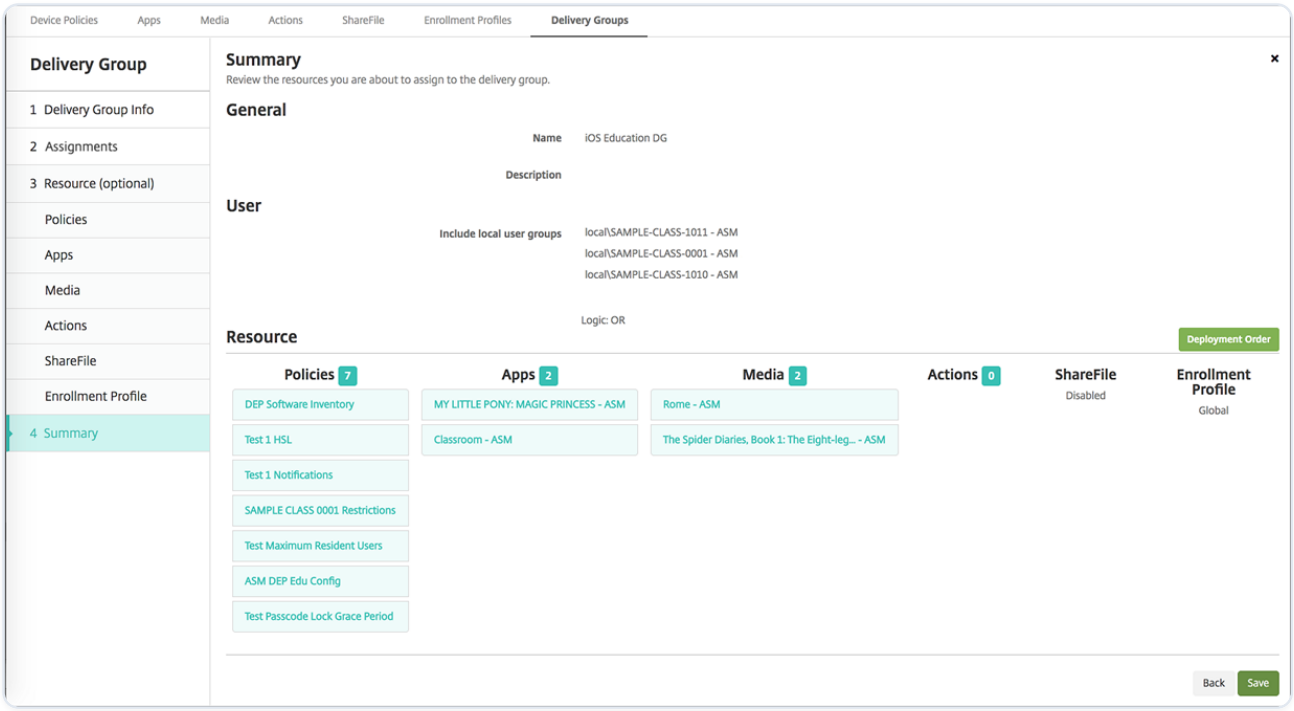
- Citrix Endpoint Managementで使用するためにエンタープライズアカウントを構成した場合は、**ShareFileを有効にする**を**オン**に設定します。この設定により、デリバリーグループはShareFileのコンテンツとデータにシングルサインオンでアクセスできるようになります。
- Citrix Endpoint Managementで使用するためにストレージゾーンコネクタを構成した場合は、デリバリーグループに含めるストレージゾーンコネクタを右側のボックスにドラッグします。

構成されたオプションを確認し、展開順序を変更する

概要ページでは、デリバリーグループ用に構成したオプションを確認し、リソースの展開順序を変更できます。概要ページには、カテゴリ別にリソースが表示されます。概要ページには展開順序は表示されません。

注：

戻るをクリックして前のページに戻り、構成を変更します。



デプロイ順序を表示または変更するには：

1. をクリックします。
2. ダイアログボックスで、リソースをデプロイしたい順序の場所にドラッグします。リソースは上から下の順序でデプロイされます。
3. をクリックしてデプロイ順序を保存します。

デリバリーグループの設定が完了したら、 ページで をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android Enterpriseにリソースをデプロイするルールを作成する

Androidデバイスプロパティルールを使用して、Android Enterpriseデバイスへのデリバリーグループの展開を管理できます。同じユーザーに複数のデバイスを登録する場合、デバイスの登録モードまたはデバイスアプリケーションパッケージIDに基づいて、Android Enterpriseの高度なフィルターを作成できます。

Android Enterpriseデバイスにデリバリーグループをデプロイする(/en-us/citrix-endpoint-management/media/deploy-delivery-group-android-enterprise.png)

デバイス登録モードを使用してAndroid Enterpriseデバイスにデリバリーグループをデプロイするには：

1. デリバリーグループを作成します。
2. ページで、 を展開します。
3. で、 **タブ**を開き、 をクリックします。
4. リストから、ルールに追加する条件を選択します。
    - 新しいAndroid Enterpriseデバイスの場合、 を選択し、最初の値フィールドに **GOOGLE_AW_INSTALL_TYPE** と入力します。次に、条件をいずれかの登録モードと等しくなるように設定する必要があります。
    - 既存のAndroid Enterpriseデバイスの場合、 を選択し、最初の値フィールドで を選択します。次に、条件をいずれかの登録モードと等しくなるように設定する必要があります。
5. 2番目のフィールドに、Android Enterpriseデバイスの登録モードを入力します。
    - **DeviceAdministrator:** 会社所有のデバイスで、仕事でのみ使用することを指定します（デバイス所有者モードとも呼ばれます）。
    - **ManagedProfile:** BYOD（個人所有のデバイスで、仕事用プロファイル管理に登録されているもの）を指定します（プロファイル所有者モードとも呼ばれます）。
    - **CorporateOwnedSingleUse:** 専用デバイスを指定します（以前は企業所有の単一用途デバイスとして知られていました）。
    - **CorporateOwnedPersonallyEnabled:** 仕事用プロファイルを持つ完全に管理されたデバイスを指定します（以前は企業所有の個人利用可能デバイスとして知られていました）。
6. デリバリーグループの追加で説明されているように、デリバリーグループの設定を完了します。

    詳しくは、デバイス展開シナリオとプロファイルを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスアプリケーションパッケージIDを使用して、Android Enterpriseデバイスにデリバリーグループを展開するには：

1. **デバイスプロパティ – Android**で、**詳細タブ**を開き、**新しいルール**をクリックします。
2. リストから**インストール済みアプリ名**を選択し、アプリケーションパッケージIDを入力します。

デリバリーグループを編集する

既存のデリバリーグループの名前は変更できません。その他の設定を更新するには、**構成 > デリバリーグループ**に移動し、編集したいグループを選択して、**編集**をクリックします。

AllUsersデリバリーグループを有効/無効にする

AllUsersは、有効または無効にできる唯一のデリバリーグループです。他のデリバリーグループのようにAllUsersを削除することはできません。

デリバリーグループページで、**AllUsers**の横にあるチェックボックスを選択するか、**AllUsers**を含む行をクリックして、AllUsersデリバリーグループを選択します。次に、以下のいずれかを実行します。

- AllUsersデリバリーグループを無効にするには、「**無効化**」をクリックします。このコマンドは、AllUsersグループが有効になっている場合（デフォルト）にのみ使用できます。デリバリーグループテーブルの「**無効**」見出しの下に「**無効**」と表示されます。
- AllUsersデリバリーグループを有効にするには、「**有効化**」をクリックします。このコマンドは、AllUsersグループが無効になっている場合にのみ使用できます。デリバリーグループテーブルの「**無効**」見出しの下に「**無効**」と表示されなくなります。

デリバリーグループへの展開

デリバリーグループに展開するとは、Apple、Android、Windowsタブレットデバイスを使用しているすべてのユーザーにプッシュ通知を送信することです。

その他のプラットフォームデバイスを使用しているユーザーの場合、それらのデバイスがすでにCitrix Endpoint Managementに接続されている場合は、すぐにリソースを受け取ります。そうでない場合は、スケジューリングポリシーに基づいて、次回接続時にリソースを受け取ります。

Androidデバイスのアプリストアの「更新可能なアプリ」リストに更新されたアプリを表示するには、まず、App Inventoryポリシーをユーザーデバイスに展開します。

1. 「**デリバリーグループ**」ページで、次のいずれかを実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 複数のデリバリーグループに一度に展開するには、展開するグループの横にあるチェックボックスをオンにします。
- 単一のデリバリーグループに展開するには、その名前の横にあるチェックボックスをオンにするか、その名前を含む行をクリックします。

2. 「**展開**」をクリックします。

   単一のデリバリーグループを選択する方法に応じて、「**展開**」コマンドがデリバリーグループの上または右に表示されます。

   アプリ、ポリシー、およびアクションを展開するグループが一覧表示されていることを確認します。次に、「**展開**」をクリックします。アプリ、ポリシー、およびアクションは、デバイスプラットフォームとスケジューリングポリシーに基づいて、選択したグループに展開されます。

   「**デリバリーグループ**」ページで展開ステータスを確認するには、次のいずれかの方法を使用します。

   - デリバリーグループの「**ステータス**」見出しの下にある展開アイコンを確認します。これは展開の失敗を示します。
   - デリバリーグループがある行をクリックして、「**インストール済み**」、「**保留中**」、「**失敗**」の展開を示すオーバーレイを表示します。

   デリバリーグループ構成画面(/en-us/citrix-endpoint-management/media/configure-delivery-groups-check-deployment.png)

デリバリーグループのクローンを作成する

既存のデリバリーグループに似たデリバリーグループを作成したい場合は、デリバリーグループのクローンを作成します。クローンを新しいデリバリーグループの開始点として使用します。その後、登録プロファイルの追加や新しいADユーザーセットの追加など、クローンに変更を加えます。

1. Citrix Endpoint Managementコンソールで、**［構成］**をクリックし、［デリバリーグループ］**タブを選択します。
2. デリバリーグループの一覧から、新しいグループのベースとして使用するものを選択します。
3. **［クローン］**を選択します。
4. ［デリバリーグループのクローン作成］ダイアログボックスで、新しいグループの名前を入力し、必要に応じて説明を入力します。
5. **［クローン］**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デリバリーグループを削除する

AllUsersデリバリーグループは削除できませんが、すべてのユーザーにリソースをプッシュしたくない場合は無効にできます。「AllUsersデリバリーグループを有効または無効にする」を参照してください。

重要：

削除は元に戻せません。

1. **［デリバリーグループ］**ページで、次のいずれかを実行します。
   - 複数のデリバリーグループを一度に削除するには、削除するグループの横にあるチェックボックスをオンにします。
   - 単一のデリバリーグループを削除するには、その名前の横にあるチェックボックスをオンにするか、その名前を含む行をクリックします。
2. **削除**」をクリックします。

   単一のデリバリーグループを選択する方法に応じて、「**削除**」コマンドがデリバリーグループの上または右側に表示されます。
3. 「**削除**」ダイアログボックスで、「**削除**」をクリックします。

デリバリーグループテーブルをエクスポートする

1. 「**デリバリーグループ**」テーブルの上にある「**エクスポート**」をクリックします。Citrix Endpoint Management は、「**デリバリーグループ**」テーブルの情報を抽出し、.csv ファイルに変換します。
2. ブラウザの通常の手順に従って、.csv ファイルを開くか保存します。

マクロ

Citrix Endpoint Managementは、以下の項目のテキストフィールド内でユーザーまたはデバイスのプロパティデータを入力する方法として、マクロを提供します。

- ポリシー
- 通知
- 登録テンプレート
- デバイス構成XMLファイル

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 自動アクション
- 資格情報プロバイダーの証明書署名要求

Citrix Endpoint Managementは、マクロを対応するユーザーまたはシステムの値に置き換えます。たとえば、数千人のユーザーにわたる単一のExchangeプロファイルで、ユーザーのメールボックス値を事前に入力できます。

マクロの構文

マクロは次の形式をとることができます。

- `${type.PROPERTYNAME}`
- `${type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)]}`

ドル記号 ($) に続くすべての構文を中括弧 ({ }) で囲みます。

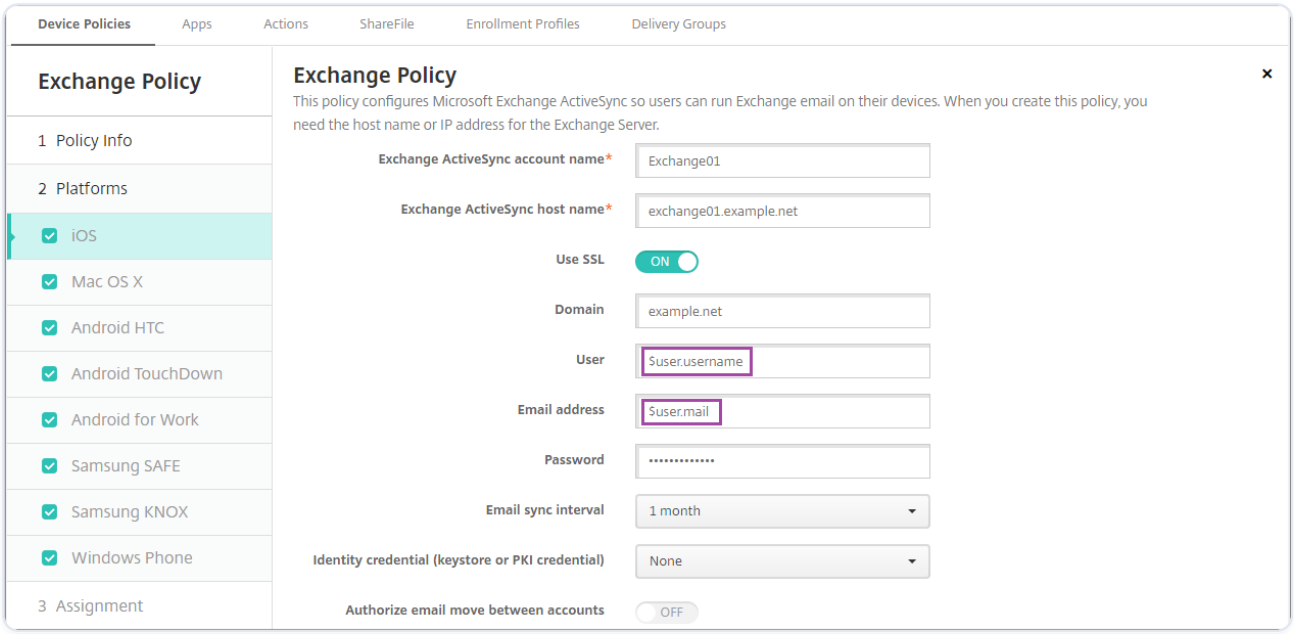
- 修飾プロパティ名は、ユーザープロパティ、デバイスプロパティ、またはカスタムプロパティのいずれかを参照します。
- 修飾プロパティ名は、プレフィックスと実際のプロパティ名で構成されます。
- ユーザープロパティは`${user.[PROPERTYNAME] (prefix="user.")}`の形式を取ります。
- デバイスプロパティは`${device.[PROPERTYNAME] (prefix="device.")}`の形式を取ります。
- プロパティ名は大文字と小文字を区別します。
- 関数は、限定されたリストであるか、関数を定義するサードパーティのリファレンスへのリンクである場合があります。通知メッセージ用のこのマクロには、関数`firstnotnull`が含まれています。

デバイス`${firstnotnull(device.TEL_NUMBER,device.serialNumber)}`はブロックされました…

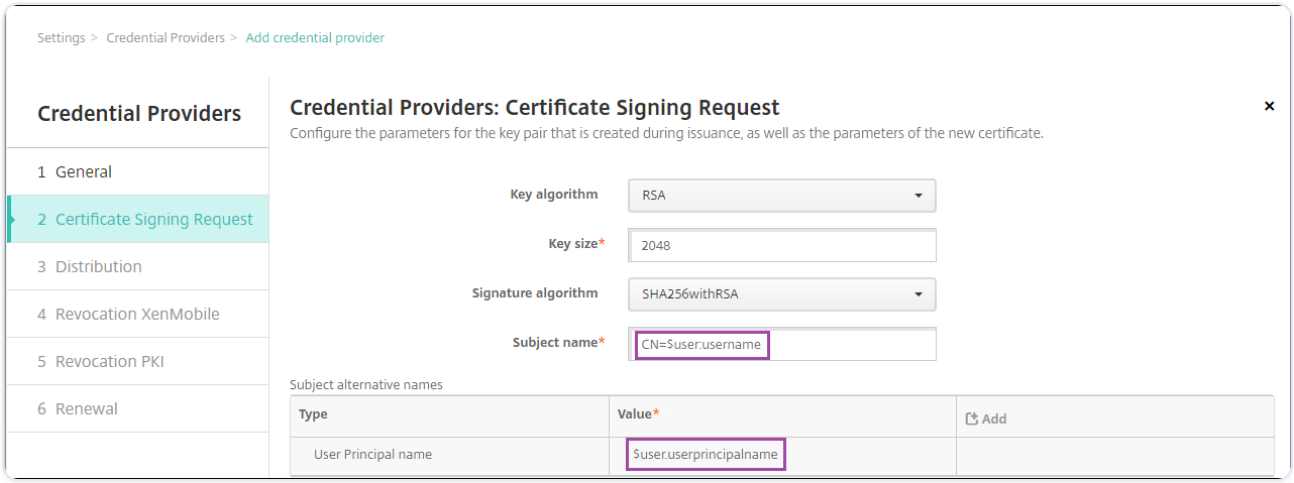
- カスタムマクロ（定義するプロパティ）の場合、プレフィックスは`${custom}`です。プレフィックスを省略することもできます。

ポリシーのテキストフィールドにユーザー名の値を入力する、一般的に使用されるマクロ`${user.username}`の例を次に示します。このマクロは、Exchange ActiveSyncプロファイルや、多くのユーザーが使用するその他のプロファイルを構成するのに役立ちます。次の例は、Exchangeポリシーでマクロを使用する方法を示しています。**ユーザー**のマクロは`${user.username}`です。**メールアドレス**のマクロは`${user.mail}`です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



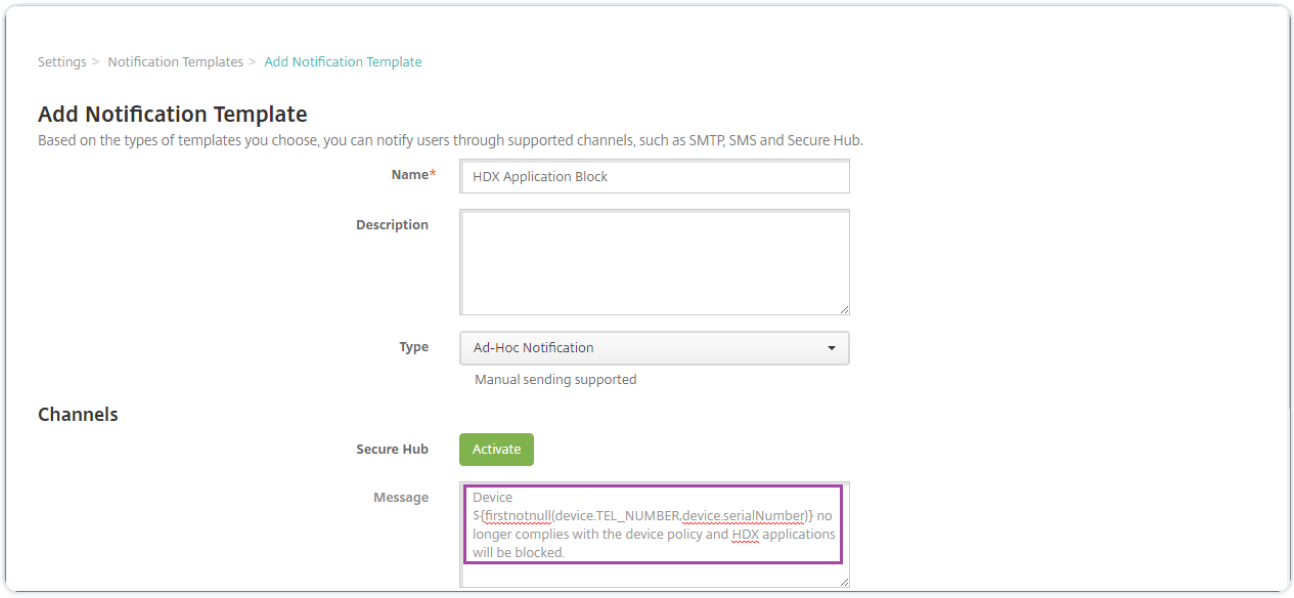
次の例は、証明書署名要求にマクロを使用する方法を示しています。**サブジェクト名**のマクロは**CN=$user.username**です。**サブジェクトの別名**の**値**のマクロは**$user.userprincipalname**です。



次の例は、通知テンプレートでマクロを使用する方法を示しています。このテンプレートの例では、非準拠デバイスのためにHDX™アプリケーションがブロックされたときにユーザーに送信されるメッセージを定義しています。**メッセージ**のマクロは次のとおりです。

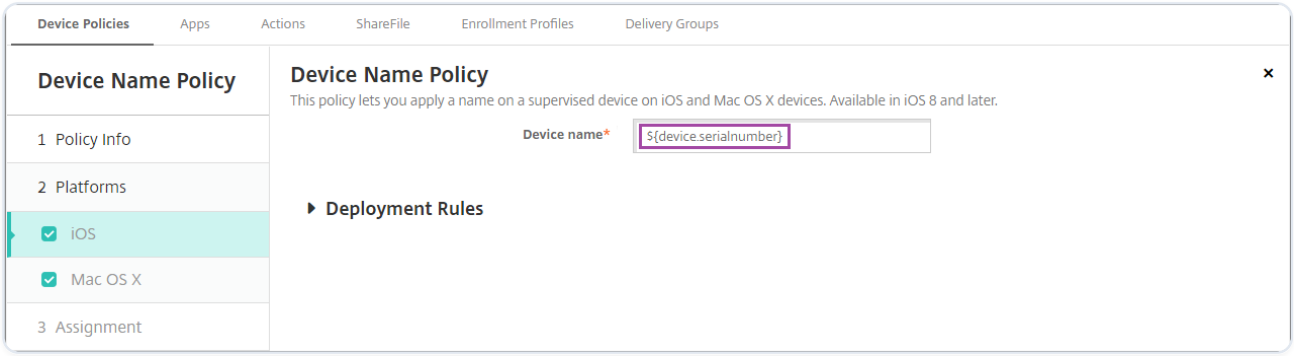
デバイス`${firstnotnull(device.TEL_NUMBER,device.serialNumber)}`はデバイスポリシーに準拠しなくなり、HDXアプリケーションはブロックされました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



通知で使用されるマクロのその他の例については、**設定 > 通知テンプレート**に移動し、定義済みのテンプレートを選択して、**編集**をクリックします。

以下の例は、デバイス名デバイスポリシーにおけるマクロを示しています。各デバイスに一意の名前を付けるために、マクロ、マクロの組み合わせ、またはマクロとテキストの組み合わせを入力できます。たとえば、`${device.serialnumber}` を使用して、デバイス名を各デバイスのシリアル番号に設定します。`${device.serialnumber} ${ user.username }` を使用して、デバイス名にユーザー名を含めます。デバイス名デバイスポリシーは、監視対象のiOSおよびmacOSデバイスで機能します。



デフォルト通知テンプレート用のマクロ

デフォルト通知テンプレートでは、以下のマクロを使用できます。

- `${account.SUPPORT_EMAIL}`
- `${applicationName}`
- `${enrollment.andriod.agent.download.url}`
- `${enrollment.ios.agent.download.url}`
- `${enrollment.pin}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `${enrollment.url}`
- `${enrollment.urls}`
- `${enrollment.ios.url}`
- `${enrollment.macos.url}`
- `${enrollment.android.url}`
- `${enrollment.ios.platform}`
- `${enrollment.macos.platform}`
- `${enrollment.android.platform}`
- `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${outofcompliance.reason(smg_block)}`
- `${outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `${vpp.account}`
- `${vpp.appname}`
- `${vpp.url}`
- `${zdmserver.hostPath}/enroll`

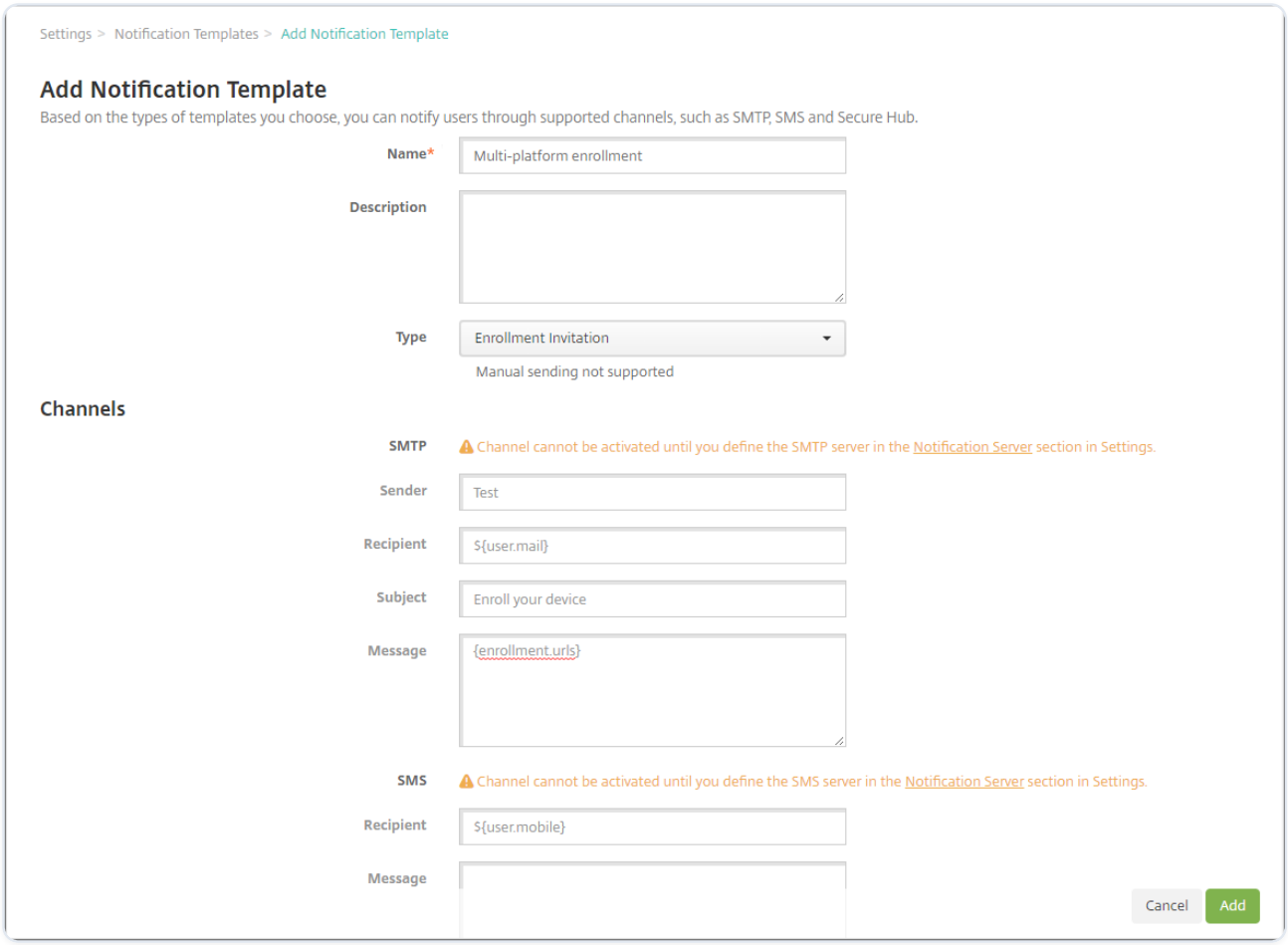
注:

Citrix Endpoint Management コンソールには、「blacklist」と「whitelist」という用語が含まれています。今後のバージョンでは、これらの用語を「block list」と「allow list」に変更する予定です。

この例では、多くのデバイスプラットフォームの登録URLを含む通知を作成する方法を示します。**メッセージ**のマクロは次のとおりです。

${enrollment.urls}

© 1997–2026 Citrix Systems, Inc. All rights reserved.



これらの例は、ユーザーが自分のデバイスプラットフォームの登録URLをクリックするように促す通知メッセージを作成する方法を示しています。

例1：

```
To enroll, click the link below that applies to your device platform:


${enrollment.ios.platform} - ${enrollment.ios.url}


${enrollment.macos.platform} - ${enrollment.macos.url}


${enrollment.android.platform} - ${enrollment.android.url}
```

例2：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
To enroll an iOS device, click the link ${enrollment.ios.url}.


To enroll a macOS device, click the link ${enrollment.macos.url}.


To enroll an Android device, click the link ${enrollment.android.url}.
```

特定のポリシーのマクロ

デバイス名デバイスポリシー（iOSおよびmacOS用）の場合、**デバイス名**にこれらのマクロを使用できます。

- `${device.serialnumber}`
- `${user.username}@example.com`
- `${device.serialnumber}`
- `${device.serialnumber}`
- `${user.username}`
- `${enrollment.pin}`
- `${user.dnsroot}`

セルラーデバイスポリシー（iOS用）の場合、プロキシサーバーポートなどの非文字列フィールドの値にマクロを使用できます。たとえば、`${device.xyz}` や `${setting.xyz}` のようなマクロを使用できるようになり、これらは整数に展開されます。

iOSおよびmacOSプロファイルのインポートデバイスポリシーを使用してCitrix Endpoint Managementにインポートするデバイス構成XMLファイルの場合、非文字列フィールドの値にマクロを使用できます。

Samsung MDMライセンスキーデバイスポリシーの場合、**ELMライセンスキー**にこのマクロを使用できます。

- `${elm.license.key}`

ウェブクリップデバイスポリシーの場合、このマクロを**URL:**に使用できます。

- `${webeas-url}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

組み込みデバイスプロパティを取得するためのマクロ

表示名	マクロ
デバイスID	`$device.id`
デバイスGUID	`$device.uniqueid`
デバイスIMEI	`$device.imei`
OSファミリー	`$device.OSFamily`
シリアル番号	`$device.serialNumber`

すべてのデバイスプロパティのマクロ

表示名: アカウントは停止されていますか？

- **Web要素:** `GOOGLE_AW_DIRECTORY_SUSPENDED`
- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_SUSPENDED}`

表示名: アクティベーションロックバイパスコード

- **Web要素:** `ACTIVATION_LOCK_BYPASS_CODE`
- **マクロ:** `${device.ACTIVATION_LOCK_BYPASS_CODE}`

表示名: アクティベーションロックが有効

- **Web要素:** `ACTIVATION_LOCK_ENABLED`
- **マクロ:** `${device.ACTIVATION_LOCK_ENABLED}`

表示名: アクティブなApple App Storeアカウント

- **Web要素:** `ACTIVE_ITUNES`
- **マクロ:** `${device.ACTIVE_ITUNES}`

表示名: 管理者が無効

- **Web要素:** `ADMIN_DISABLED`
- **マクロ:** `${device.ADMIN_DISABLED}`

表示名: AIKは存在しますか？

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web要素:** `WINDOWS_HAS_AIK_PRESENT`
- **マクロ:** `${device.WINDOWS_HAS_AIK_PRESENT}`

表示名: Amazon MDM APIが利用可能

- **Web要素:** `AMAZON_MDM`
- **マクロ:** `${device.AMAZON_MDM}`

表示名: Android Enterpriseデバイス ID

- **Web要素:** `GOOGLE_AW_DEVICE_ID`
- **マクロ:** `${device.GOOGLE_AW_DEVICE_ID}`

表示名: Android Enterpriseが有効なデバイス？

- **Web要素:** `GOOGLE_AW_ENABLED_DEVICE`
- **マクロ:** `${device.GOOGLE_AW_ENABLED_DEVICE}`

表示名: Android Enterpriseインストールタイプ

- **Web要素:** `GOOGLE_AW_INSTALL_TYPE`
- **マクロ:** `${device.GOOGLE_AW_INSTALL_TYPE}`

表示名: アンチスパイウェア署名ステータス

- **Web要素:** `ANTI_SPYWARE_SIGNATURE_STATUS`
- **マクロ:** `${device.ANTI_SPYWARE_SIGNATURE_STATUS}`

表示名: アンチスパイウェアステータス

- **Web要素:** `ANTI_SPYWARE_STATUS`
- **マクロ:** `${device.ANTI_SPYWARE_STATUS}`

表示名: アンチウイルス署名ステータス

- **Web要素:** `ANTI_VIRUS_SIGNATURE_STATUS`
- **マクロ:** `${device.ANTI_VIRUS_SIGNATURE_STATUS}`

表示名: アンチウイルスステータス

- **Web要素:** `ANTI_VIRUS_STATUS`
- **マクロ:** `${device.ANTI_VIRUS_STATUS}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名: ASM展開プログラムのアクティベーションロックバイパスコード

- **Web要素:** `DEP_ACTIVATION_LOCK_BYPASS_CODE`
- **マクロ:** `${device.DEP_ACTIVATION_LOCK_BYPASS_CODE}`

表示名: ASM展開プログラムエスクローキー

- **Web要素:** `DEP_ESCROW_KEY`
- **マクロ:** `${device.DEP_ESCROW_KEY}`

表示名: 資産タグ

- **Web要素:** `ASSET_TAG`
- **マクロ:** `${device.ASSET_TAG}`

表示名: ソフトウェアアップデートを自動的に確認

- **Web要素:** `AutoCheckEnabled`
- **マクロ:** `${device.AutoCheckEnabled}`

表示名: バックグラウンドでソフトウェアアップデートを自動的にダウンロード

- **Web要素:** `BackgroundDownloadEnabled`
- **マクロ:** `${device.BackgroundDownloadEnabled}`

表示名: アプリのアップデートを自動的にインストール

- **Web要素:** `AutomaticAppInstallationEnabled`
- **マクロ:** `${device.AutomaticAppInstallationEnabled}`

表示名: OSアップデートを自動的にインストール

- **Web要素:** `AutomaticOSInstallationEnabled`
- **マクロ:** `${device.AutomaticOSInstallationEnabled}`

表示名: セキュリティアップデートを自動的にインストール

- **Web要素:** `AutomaticSecurityUpdatesEnabled`
- **マクロ:** `${device.AutomaticSecurityUpdatesEnabled}`

表示名: 自動更新ステータス

- **Web要素:** `AUTOUPDATE_STATUS`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **マクロ:** `${device.AUTOUPDATE_STATUS}`

表示名: 利用可能なRAM

- **Web要素:** `MEMORY_AVAILABLE`
- **マクロ:** `${device.MEMORY_AVAILABLE}`

表示名: 利用可能なソフトウェアアップデート

- **Web要素:** `AVAILABLE_OS_UPDATE_HUMAN_READABLE`
- **マクロ:** `${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE}`

表示名: 利用可能なストレージ容量

- **Web要素:** `FREEDISK`
- **マクロ:** `${device.FREEDISK}`

表示名: バックアップバッテリー

- **Web要素:** `BACKUP_BATTERY_PERCENT`
- **マクロ:** `${device.BACKUP_BATTERY_PERCENT}`

表示名: ベースバンドファームウェアバージョン

- **Web要素:** `MODEM_FIRMWARE_VERSION`
- **マクロ:** `${device.MODEM_FIRMWARE_VERSION}

表示名: バッテリー充電中

- **Web要素:** `BATTERY_CHARGING_STATUS`
- **マクロ:** `${device.BATTERY_CHARGING_STATUS}`

表示名: バッテリー充電中

- **Web要素:** `BATTERY_CHARGING`
- **マクロ:** `${device.BATTERY_CHARGING}`

表示名: バッテリー残量

- **Web要素:** `BATTERY_ESTIMATED_CHARGE_REMAINING`
- **マクロ:** `${device.BATTERY_ESTIMATED_CHARGE_REMAINING}`

表示名: バッテリー稼働時間

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web要素:** `BATTERY_RUNTIME`
- **マクロ:** `${device.BATTERY_RUNTIME}`

表示名: バッテリーの状態

- **Web要素:** `BATTERY_STATUS`
- **マクロ:** `${device.BATTERY_STATUS}`

表示名: BES PIN

- **Web要素:** `BES_PIN`
- **マクロ:** `${device.BES_PIN}`

表示名: BES server agent ID

- **Web要素:** `AGENT_ID`
- **マクロ:** `${device.AGENT_ID}`

表示名: BESサーバー名

- **Web要素:** `BES_SERVER`
- **マクロ:** `${device.BES_SERVER}`

表示名: BESサーバーバージョン

- **Web要素:** `BES_VERSION`
- **マクロ:** `${device.BES_VERSION}`

表示名: BIOS情報

- **Web要素:** `BIOS_INFO`
- **マクロ:** `${device.BIOS_INFO}`

表示名: BitLockerステータス

- **Web要素:** `WINDOWS_HAS_BIT_LOCKER_STATUS`
- **マクロ:** `${device.WINDOWS_HAS_BIT_LOCKER_STATUS}`

表示名: Bluetooth MACアドレス

- **Web要素:** `BLUETOOTH_MAC`
- **マクロ:** `${device.BLUETOOTH_MAC}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名: ブートデバッグは有効ですか？

- **Web要素:** `WINDOWS_HAS_BOOT_DEBUGGING_ENABLED`
- **マクロ:** `${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED}`

表示名: ブートマネージャー改訂リストバージョン

- **Web要素:** `WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION`
- **マクロ:** `${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION}`

表示名: キャリアコード

- **Web要素:** `CARRIER_CODE`
- **マクロ:** `${device.CARRIER_CODE}`

表示名: キャリア設定バージョン

- **Web要素:** `CARRIER_SETTINGS_VERSION`
- **マクロ:** `${device.CARRIER_SETTINGS_VERSION}`

表示名: カタログURL

- **Web要素:** `CatalogURL`
- **マクロ:** `${device.CatalogURL}`

表示名: セルラー高度

- **Web要素:** `GPS_ALTITUDE_FROM_CELLULAR`
- **マクロ:** `${device.GPS_ALTITUDE_FROM_CELLULAR}`

表示名: セルラーコース

- **Web要素:** `GPS_COURSE_FROM_CELLULAR`
- **マクロ:** `${device.GPS_COURSE_FROM_CELLULAR}`

表示名: セルラー水平精度

- **Web要素:** `GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR`
- **マクロ:** `${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR}`

表示名: セルラー緯度

- **Web要素:** `GPS_LATITUDE_FROM_CELLULAR`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **マクロ:** `${device.GPS_LATITUDE_FROM_CELLULAR}`

表示名: セルラー経度

- **Web要素:** `GPS_LONGITUDE_FROM_CELLULAR`
- **マクロ:** `${device.GPS_LONGITUDE_FROM_CELLULAR}`

表示名: セルラー速度

- **Web要素:** `GPS_SPEED_FROM_CELLULAR`
- **マクロ:** `${device.GPS_SPEED_FROM_CELLULAR}`

表示名: セルラーテクノロジー

- **Web要素:** `CELLULAR_TECHNOLOGY`
- **マクロ:** `${device.CELLULAR_TECHNOLOGY}`

表示名: セルラータイムスタンプ

- **Web要素:** `GPS_TIMESTAMP_FROM_CELLULAR`
- **マクロ:** `${device.GPS_TIMESTAMP_FROM_CELLULAR}`

表示名: セルラー垂直精度

- **Web要素:** `GPS_VERTICAL_ACCURACY_FROM_CELLULAR`
- **マクロ:** `${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}`

表示名: 次回のログイン時にパスワードを変更しますか？

- **Web要素:** `GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`
- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

表示名: クライアントデバイスID

- **Web要素:** `CLIENT_DEVICE_ID`
- **マクロ:** `${device.CLIENT_DEVICE_ID}`

表示名: クラウドバックアップが有効

- **Web要素:** `CLOUD_BACKUP_ENABLED`
- **マクロ:** `${device.CLOUD_BACKUP_ENABLED}`

表示名: コード整合性は有効ですか？

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web要素:** `WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- **マクロ:** `${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED}`

表示名: コード整合性失効リストバージョン

- **Web要素:** `WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`
- **マクロ:** `${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION}`

表示名: 色

- **Web要素:** `COLOR`
- **マクロ:** `${device.COLOR}`

表示名: CPUクロック速度

- **Web要素:** `CPU_CLOCK_SPEED`
- **マクロ:** `${device.CPU_CLOCK_SPEED}`

表示名: CPUタイプ

- **Web要素:** `CPU_TYPE`
- **マクロ:** `${device.CPU_TYPE}`

表示名: 作成時刻

- **Web要素:** `GOOGLE_AW_DIRECTORY_CREATION_TIME`
- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_CREATION_TIME}`

表示名: 重要なソフトウェア更新

- **Web要素:** `AVAILABLE_OS_UPDATE_IS_CRITICAL`
- **マクロ:** `${device.AVAILABLE_OS_UPDATE_IS_CRITICAL}`

表示名: 現在のキャリアネットワーク

- **Web要素:** `CARRIER`
- **マクロ:** `${device.CARRIER}`

表示名: 現在のモバイル国コード

- **Web要素:** `CURRENT_MCC`
- **マクロ:** `${device.CURRENT_MCC}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名: 現在のモバイルネットワークコード

- **Web要素:** `CURRENT_MNC`
- **マクロ:** `${device.CURRENT_MNC}`

表示名: データローミングを許可

- **Web要素:** `DATA_ROAMING_ENABLED`
- **マクロ:** `${device.DATA_ROAMING_ENABLED}`

表示名: 最後のiCloudバックアップの日付

- **Web要素:** `LAST_CLOUD_BACKUP_DATE`
- **マクロ:** `${device.LAST_CLOUD_BACKUP_DATE}`

表示名: デフォルトカタログ

- **Web要素:** `IsDefaultCatalog`
- **マクロ:** `${device.IsDefaultCatalog}`

表示名: Apple Deployment Programアカウント名

- **Web要素:** `BULK_ENROLLMENT_DEP_ACCOUNT_NAME`
- **マクロ:** `${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME}`

表示名: Apple Deployment Programポリシー

- **Web要素:** `WINDOWS_HAS_DEP_POLICY`
- **マクロ:** `${device.WINDOWS_HAS_DEP_POLICY}`

表示名: Apple Deployment Programプロファイル割り当て済み

- **Web要素:** `PROFILE_ASSIGN_TIME`
- **マクロ:** `${device.PROFILE_ASSIGN_TIME}`

表示名: Apple Deployment Programプロファイルプッシュ済み

- **Web要素:** `PROFILE_PUSH_TIME`
- **マクロ:** `${device.PROFILE_PUSH_TIME}`

表示名: Apple Deployment Programプロファイル削除済み

- **Web要素:** `PROFILE_REMOVE_TIME`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **マクロ:** `${device.PROFILE_REMOVE_TIME}`

表示名: Apple Deployment Program登録者

- **Web要素:** `DEVICE_ASSIGNED_BY`
- **マクロ:** `${device.DEVICE_ASSIGNED_BY}`

表示名: Apple Deployment Program登録日

- **Web要素:** `DEVICE_ASSIGNED_DATE`
- **マクロ:** `${device.DEVICE_ASSIGNED_DATE}`

表示名: 説明

- **Web要素:** `DESCRIPTION`
- **マクロ:** `${device.DESCRIPTION}`

表示名: デバイスモデル

- **Web要素:** `SYSTEM_OEM`
- **マクロ:** `${device.SYSTEM_OEM}`

表示名: デバイス名

- **Web要素:** `DEVICE_NAME`
- **マクロ:** `${device.DEVICE_NAME}`

表示名: デバイスの種類

- **Web要素:** `DEVICE_TYPE`
- **マクロ:** `${device.DEVICE_TYPE}`

表示名: おやすみモードが有効

- **Web要素:** `DO_NOT_DISTURB`
- **マクロ:** `${device.DO_NOT_DISTURB}`

表示名: ELAMドライバーがロードされましたか？

- **Web要素:** `WINDOWS_HAS_ELAM_DRIVER_LOADED`
- **マクロ:** `${device.WINDOWS_HAS_ELAM_DRIVER_LOADED}`

表示名: 暗号化コンプライアンス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web要素:** `ENCRYPTION_COMPLIANCE`
- **マクロ:** `${device.ENCRYPTION_COMPLIANCE}`

表示名: ENROLLMENT_KEY_GENERATION_DATE

- **Web要素:** `ENROLLMENT_KEY_GENERATION_DATE`
- **マクロ:** `${device.ENROLLMENT_KEY_GENERATION_DATE}`

表示名: エンタープライズID

- **Web要素:** `ENTERPRISEID`
- **マクロ:** `${device.ENTERPRISEID}`

表示名: 外部ストレージ 1: 利用可能な領域

- **Web要素:** `EXTERNAL_STORAGE1_FREE_SPACE`
- **マクロ:** `${device.EXTERNAL_STORAGE1_FREE_SPACE}`

表示名: 外部ストレージ 1: 利用可能な領域

- **Web要素:** `EXTERNAL_STORAGE1_FREE_SPACE`
- **マクロ:** `${device.EXTERNAL_STORAGE1_FREE_SPACE}`

表示名: 外部ストレージ 1: 名前

- **Web要素:** `EXTERNAL_STORAGE1_NAME`
- **マクロ:** `${device.EXTERNAL_STORAGE1_NAME}`

表示名: 外部ストレージ 1: 合計領域

- **Web要素:** `EXTERNAL_STORAGE1_TOTAL_SPACE`
- **マクロ:** `${device.EXTERNAL_STORAGE1_TOTAL_SPACE}`

表示名: 外部ストレージ 2: 利用可能な領域

- **Web要素:** `EXTERNAL_STORAGE2_FREE_SPACE`
- **マクロ:** `${device.EXTERNAL_STORAGE2_FREE_SPACE}`

表示名: 外部ストレージ 2: 名前

- **Web要素:** `EXTERNAL_STORAGE2_NAME`
- **マクロ:** `${device.EXTERNAL_STORAGE2_NAME}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名: 外部ストレージ 2: 合計領域

- **Web要素:** `EXTERNAL_STORAGE2_TOTAL_SPACE`
- **マクロ:** `${device.EXTERNAL_STORAGE2_TOTAL_SPACE}`

表示名: 外部ストレージの暗号化

- **Web要素:** `EXTERNAL_ENCRYPTION`
- **マクロ:** `${device.EXTERNAL_ENCRYPTION}`

表示名: FileVaultが有効

- **Web要素:** `IS_FILEVAULT_ENABLED`
- **マクロ:** `${device.IS_FILEVAULT_ENABLED}`

表示名: ファイアウォールの状態

- **Web要素:** `DEVICE_FIREWALL_STATUS`
- **マクロ:** `${device.DEVICE_FIREWALL_STATUS}`

表示名: ファイアウォールの状態

- **Web要素:** `DEVICE_FIREWALL_STATUS`
- **マクロ:** `${device.DEVICE_FIREWALL_STATUS}`

表示名: ファイアウォールの状態

- **Web要素:** `FIREWALL_STATUS`
- **マクロ:** `${device.FIREWALL_STATUS}`

表示名: ファームウェアバージョン

- **Web要素:** `FIRMWARE_VERSION`
- **マクロ:** `${device.FIRMWARE_VERSION}`

表示名: 初回同期

- **Web要素:** `ZMSP_FIRST_SYNC`
- **マクロ:** `${device.ZMSP_FIRST_SYNC}`

表示名: Google Directory エイリアス

- **Web要素:** `GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}`

表示名: Google Directory 姓

- **Web要素:** `GOOGLE_AW_DIRECTORY_FAMILY_NAME`
- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}`

表示名: Google Directory 名

- **Web要素:** `GOOGLE_AW_DIRECTORY_NAME`
- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_NAME}`

表示名: Google Directory プライマリメール

- **Web要素:** `GOOGLE_AW_DIRECTORY_PRIMARY`
- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_PRIMARY}`

表示名: Google Directory ユーザーID

- **Web要素:** `GOOGLE_AW_DIRECTORY_USER_ID`
- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_USER_ID}`

表示名: GPS高度

- **Web要素:** `GPS_ALTITUDE_FROM_GPS`
- **マクロ:** `${device.GPS_ALTITUDE_FROM_GPS}`

表示名: GPSコース

- **Web要素:** `GPS_COURSE_FROM_GPS`
- **マクロ:** `${device.GPS_COURSE_FROM_GPS}`

表示名: GPS水平精度

- **Web要素:** `GPS_HORIZONTAL_ACCURACY_FROM_GPS`
- **マクロ:** `${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS}`

表示名: GPS緯度

- **Web要素:** `GPS_LATITUDE_FROM_GPS`
- **マクロ:** `${device.GPS_LATITUDE_FROM_GPS}`

表示名: GPS経度

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web要素:** `GPS_LONGITUDE_FROM_GPS`
- **マクロ:** `${device.GPS_LONGITUDE_FROM_GPS}`

表示名: GPS速度

- **Web要素:** `GPS_SPEED_FROM_GPS`
- **マクロ:** `${device.GPS_SPEED_FROM_GPS}`

表示名: GPSタイムスタンプ

- **Web要素:** `GPS_TIMESTAMP_FROM_GPS`
- **マクロ:** `${device.GPS_TIMESTAMP_FROM_GPS}`

表示名: GPS垂直精度

- **Web要素:** `GPS_VERTICAL_ACCURACY_FROM_GPS`
- **マクロ:** `${device.GPS_VERTICAL_ACCURACY_FROM_GPS}`

表示名: ハードウェアデバイスID

- **Web要素:** `HW_DEVICE_ID`
- **マクロ:** `${device.HW_DEVICE_ID}`

表示名: ハードウェア暗号化機能

- **Web要素:** `HARDWARE_ENCRYPTION_CAPS`
- **マクロ:** `${device.HARDWARE_ENCRYPTION_CAPS}`

表示名: HAS_CONTAINER

- **Web要素:** `HAS_CONTAINER`
- **マクロ:** `${device.HAS_CONTAINER}`

表示名: 現在ログインしているApple App Storeアカウントのハッシュ

- **Web要素:** `ITUNES_STORE_ACCOUNT_HASH`
- **マクロ:** `${device.ITUNES_STORE_ACCOUNT_HASH}`

表示名: ホームキャリアネットワーク

- **Web要素:** `SIM_CARRIER_NETWORK`
- **マクロ:** `${device.SIM_CARRIER_NETWORK}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名: ホームモバイル国コード

- **Web要素:** `SIM_MCC`
- **マクロ:** `${device.SIM_MCC}`

表示名: ホームモバイルネットワークコード

- **ウェブ要素:** `SIM_MNC`
- **マクロ:** `${device.SIM_MNC}`

表示名: ICCID

- **ウェブ要素:** `ICCID`
- **マクロ:** `${device.ICCID}`

表示名: ID

- **ウェブ要素:** `AS_DEVICE_IDENTITY`
- **マクロ:** `${device.AS_DEVICE_IDENTITY}`

表示名: IMEI/MEID 番号

- **ウェブ要素:** `IMEI`
- **マクロ:** `${device.IMEI}`

表示名: IMSI

- **ウェブ要素:** `SIM_ID`
- **マクロ:** `${device.SIM_ID}`

表示名: 内部ストレージの暗号化済み

- **Web要素:** `LOCAL_ENCRYPTION`
- **マクロ:** `${device.LOCAL_ENCRYPTION}`

表示名: IPロケーション

- **Web要素:** `IP_LOCATION`
- **マクロ:** `${device.IP_LOCATION}`

表示名: IPV4アドレス

- **Web要素:** `IP_ADDRESSV4`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **マクロ:** `${device.IP_ADDRESSV4}`

表示名: IPV6アドレス

- **Web要素:** `IP_ADDRESSV6`
- **マクロ:** `${device.IP_ADDRESSV6}`

表示名: 発行日時

- **Web要素:** `WINDOWS_HAS_ISSUED_AT`
- **マクロ:** `${device.WINDOWS_HAS_ISSUED_AT}`

表示名: ジェイルブレイク/ルート化

- **Web要素:** `ROOT_ACCESS`
- **マクロ:** `${device.ROOT_ACCESS}`

表示名: カーネルデバッグが有効ですか？

- **Web要素:** `WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED`
- **マクロ:** `${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED}`

表示名: キオスクモード

- **Web要素:** `IS_KIOSK`
- **マクロ:** `${device.IS_KIOSK}`

表示名: 最後に確認されたIPアドレス

- **Web要素:** `LAST_IP_ADDR`
- **マクロ:** `${device.LAST_IP_ADDR}`

表示名: 最終ポリシー更新時刻

- **Web要素:** `LAST_POLICY_UPDATE_TIME`
- **マクロ:** `${device.LAST_POLICY_UPDATE_TIME}`

表示名: 最終スキャン日

- **Web要素:** `PreviousScanDate`
- **マクロ:** `${device.PreviousScanDate}`

表示名: 最終スキャン結果

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web要素:** `PreviousScanResult`
- **マクロ:** `${device.PreviousScanResult}`

表示名: 最終スケジュール済みソフトウェア更新

- **Web要素:** `AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME`
- **マクロ:** `${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}`

表示名: 最終スケジュール済みソフトウェア更新失敗メッセージ

- **Web要素:** `AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG`
- **マクロ:** `${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG}`

表示名: 最終スケジュール済みソフトウェア更新ステータス

- **Web要素:** `AVAILABLE_OS_UPDATE_INSTALL_STATUS`
- **マクロ:** `${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS}`

表示名: 最終同期

- **Web要素:** `ZMSP_LAST_SYNC`
- **マクロ:** `${device.ZMSP_LAST_SYNC}`

表示名: ロケーターサービスが有効

- **Web要素:** `DEVICE_LOCATOR`
- **マクロ:** `${device.DEVICE_LOCATOR}`

表示名: MACアドレス

- **Web要素:** `MAC_ADDRESS`
- **マクロ:** `${device.MAC_ADDRESS}`

表示名: MACアドレスネットワーク接続

- **Web要素:** `MAC_NETWORK_CONNECTION`
- **マクロ:** `${device.MAC_NETWORK_CONNECTION}`

表示名: MACアドレスの種類

- **Web要素:** `MAC_ADDRESS_TYPE`
- **マクロ:** `${device.MAC_ADDRESS_TYPE}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名: メールボックス設定

- **Web要素:** `GOOGLE_AW_DIRECTORY_MAILBOX_SETUP`
- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP}`

表示名: メインバッテリー

- **Web要素:** `MAIN_BATTERY_PERCENT`
- **マクロ:** `${device.MAIN_BATTERY_PERCENT}`

表示名: MDM紛失モード有効

- **Web要素:** `IS_MDM_LOST_MODE_ENABLED`
- **マクロ:** `${device.IS_MDM_LOST_MODE_ENABLED}`

表示名: MDX_SHARED_ENCRYPTION_KEY

- **Web要素:** `MDX_SHARED_ENCRYPTION_KEY`
- **マクロ:** `${device.MDX_SHARED_ENCRYPTION_KEY}`

表示名: MEID

- **Web要素:** `MEID`
- **マクロ:** `${device.MEID}`

表示名: 携帯電話番号

- **Web要素:** `TEL_NUMBER`
- **マクロ:** `${device.TEL_NUMBER}`

表示名: モデルID

- **Web要素:** `MODEL_ID`
- **マクロ:** `${device.MODEL_ID}`

表示名: モデル番号

- **Web要素:** `MODEL_NUMBER`
- **マクロ:** `${device.MODEL_NUMBER}`

表示名: ネットワークアダプターの種類

- **Web要素:** `NETWORK_ADAPTER_TYPE`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **マクロ:** `${device.NETWORK_ADAPTER_TYPE}`

表示名: オペレーティングシステムビルド

- **Web要素:** `SYSTEM_OS_BUILD`
- **マクロ:** `${device.SYSTEM_OS_BUILD}`

表示名: オペレーティングシステムエディション

- **Web要素:** `OS_EDITION`
- **マクロ:** `${device.OS_EDITION}`

表示名: オペレーティングシステム言語 (ロケール)

- **Web要素:** `SYSTEM_LANGUAGE`
- **マクロ:** `${device.SYSTEM_LANGUAGE}`

表示名: オペレーティングシステムバージョン

- **Web要素:** `SYSTEM_OS_VERSION`
- **マクロ:** `${device.SYSTEM_OS_VERSION}`

表示名: 組織の住所

- **Web要素:** `ORGANIZATION_ADDRESS`
- **マクロ:** `${device.ORGANIZATION_ADDRESS}`

表示名: 組織のメール

- **Web要素:** `ORGANIZATION_EMAIL`
- **マクロ:** `${device.ORGANIZATION_EMAIL}`

表示名: 組織のMagic

- **Web要素:** `ORGANIZATION_MAGIC`
- **マクロ:** `${device.ORGANIZATION_MAGIC}`

表示名: 組織名

- **Web要素:** `ORGANIZATION_NAME`
- **マクロ:** `${device.ORGANIZATION_NAME}`

表示名: 組織の電話番号

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web要素:** `ORGANIZATION_PHONE`
- **マクロ:** `${device.ORGANIZATION_PHONE}`

'**表示名:** コンプライアンス違反

- **Web要素:** `OUT_OF_COMPLIANCE`
- **マクロ:** `${device.OUT_OF_COMPLIANCE}`

表示名: 所有者

- **Web要素:** `CORPORATE_OWNED`
- **マクロ:** `${device.CORPORATE_OWNED}`

表示名: パスコード準拠

- **Web要素:** `PASSCODE_IS_COMPLIANT`
- **マクロ:** `${device.PASSCODE_IS_COMPLIANT}`

表示名: 構成に準拠したパスコード

- **Web要素:** `PASSCODE_IS_COMPLIANT_WITH_CFG`
- **マクロ:** `${device.PASSCODE_IS_COMPLIANT_WITH_CFG}`

表示名: パスコードあり

- **Web要素:** `PASSCODE_PRESENT`
- **マクロ:** `${device.PASSCODE_PRESENT}`

表示名: PCR0

- **Web要素:** `WINDOWS_HAS_PCR0`
- **マクロ:** `${device.WINDOWS_HAS_PCR0}`

表示名: 境界侵害

- **Web要素:** `GPS_PERIMETER_BREACH`
- **マクロ:** `${device.GPS_PERIMETER_BREACH}`

表示名: 定期チェック

- **Web要素:** `PerformPeriodicCheck`
- **マクロ:** `${device.PerformPeriodicCheck}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名: パーソナルホットスポットが有効

- **Web要素:** `PERSONAL_HOTSPOT_ENABLED`
- **マクロ:** `${device.PERSONAL_HOTSPOT_ENABLED}`

表示名: ジオフェンスのPINコード

- **Web要素:** `PIN_CODE_FOR_GEO_FENCE`
- **マクロ:** `${device.PIN_CODE_FOR_GEO_FENCE}`

表示名: プラットフォーム

- **Web要素:** `SYSTEM_PLATFORM`
- **マクロ:** `${device.SYSTEM_PLATFORM}`

表示名: プラットフォームAPIレベル

- **Web要素:** `API_LEVEL`
- **マクロ:** `${device.API_LEVEL}`

表示名: ポリシー名

- **Web要素:** `POLICY_NAME`
- **マクロ:** `${device.POLICY_NAME}`

表示名: プライマリ電話番号

- **Web要素:** `IDENTITY1_PHONENUMBER`
- **マクロ:** `${device.IDENTITY1_PHONENUMBER}`

表示名: プライマリSIMキャリアオペレーター

- **Web要素:** `IDENTITY1_CARRIER_NETWORK_OPERATOR`
- **マクロ:** `${device.IDENTITY1_CARRIER_NETWORK_OPERATOR}`

表示名: プライマリSIM ICCID

- **Web要素:** `IDENTITY1_ICCID`
- **マクロ:** `${device.IDENTITY1_ICCID}`

表示名: プライマリSIM IMEI

- **Web要素:** `IDENTITY1_IMEI`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **マクロ:** `${device.IDENTITY1_IMEI}`

表示名: プライマリSIM IMSI

- **Web要素:** `IDENTITY1_IMSI`
- **マクロ:** `${device.IDENTITY1_IMSI}`

表示名: プライマリSIMローミング

- **Web要素:** `IDENTITY1_ROAMING`
- **マクロ:** `${device.IDENTITY1_ROAMING}`

表示名: プライマリSIMローミング

- **Web要素:** `IDENTITY1_ROAMING_COMPLIANCE`
- **マクロ:** `${device.IDENTITY1_ROAMING_COMPLIANCE}`

表示名: 製品名

- **Web要素:** `PRODUCT_NAME`
- **マクロ:** `${device.PRODUCT_NAME}`

表示名: パブリッシャーデバイスID

- **Web要素:** `PUBLISHER_DEVICE_ID`
- **マクロ:** `${device.PUBLISHER_DEVICE_ID}`

表示名: リセット回数

- **Web要素:** `WINDOWS_HAS_RESET_COUNT`
- **マクロ:** `${device.WINDOWS_HAS_RESET_COUNT}`

表示名: 再起動回数

- **Web要素:** `WINDOWS_HAS_RESTART_COUNT`
- **マクロ:** `${device.WINDOWS_HAS_RESTART_COUNT}`

表示名: セーフモードが有効ですか？

- **Web要素:** `WINDOWS_HAS_SAFE_MODE`
- **マクロ:** `${device.WINDOWS_HAS_SAFE_MODE}`

表示名: SBCP Hash

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web要素:** `WINDOWS_HAS_SBCP_HASH`
- **マクロ:** `${device.WINDOWS_HAS_SBCP_HASH}`

表示名: 画面: 高さ

- **Web要素:** `SCREEN_HEIGHT`
- **マクロ:** `${device.SCREEN_HEIGHT}`

表示名: 画面: 色数

- **Web要素:** `SCREEN_NB_COLORS`
- **マクロ:** `${device.SCREEN_NB_COLORS}`

表示名: 画面: サイズ

- **Web要素:** `SCREEN_SIZE`
- **マクロ:** `${device.SCREEN_SIZE}`

表示名: 画面: 幅

- **Web要素:** `SCREEN_WIDTH`
- **マクロ:** `${device.SCREEN_WIDTH}`

表示名: 画面: X軸解像度

- **Web要素:** `SCREEN_XDPI`
- **マクロ:** `${device.SCREEN_XDPI}`

表示名: 画面: Y軸解像度

- **Web要素:** `SCREEN_YDPI`
- **マクロ:** `${device.SCREEN_YDPI}`

表示名: 副電話番号

- **Web要素:** `IDENTITY2_PHONENUMBER`
- **マクロ:** `${device.IDENTITY2_PHONENUMBER}`

表示名: セカンダリSIMキャリアオペレーター

- **Web要素:** `IDENTITY2_CARRIER_NETWORK_OPERATOR`
- **マクロ:** `${device.IDENTITY2_CARRIER_NETWORK_OPERATOR}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名: セカンダリSIM ICCID

- **Web要素:** `IDENTITY2_ICCID`
- **マクロ:** `${device.IDENTITY2_ICCID}`

表示名: セカンダリSIM IMEI

- **Web要素:** `IDENTITY2_IMEI`
- **マクロ:** `${device.IDENTITY2_IMEI}`

表示名: セカンダリSIM IMSI

- **Web要素:** `IDENTITY2_IMSI`
- **マクロ:** `${device.IDENTITY2_IMSI}`

表示名: セカンダリSIMローミング

- **Web要素:** `IDENTITY2_ROAMING`
- **マクロ:** `${device.IDENTITY2_ROAMING}`

表示名: セカンダリSIMローミングコンプライアンス

- **Web要素:** `IDENTITY2_ROAMING_COMPLIANCE`
- **マクロ:** `${device.IDENTITY2_ROAMING_COMPLIANCE}`

表示名: セキュアブートは有効ですか？

- **Web要素:** `WINDOWS_HAS_SECURE_BOOT_ENABLED`
- **マクロ:** `${device.WINDOWS_HAS_SECURE_BOOT_ENABLED}`

表示名: セキュアブートステータス

- **Web要素:** `SECURE_BOOT_STATE`
- **マクロ:** `${device.SECURE_BOOT_STATE}`

表示名: SecureContainerが有効

- **Web要素:** `DLP_ACTIVE`
- **マクロ:** `${device.DLP_ACTIVE}`

表示名: セキュリティパッチレベル

- **Web要素:** `SYSTEM_SECURITY_PATCH_LEVEL`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **マクロ:** `${device.SYSTEM_SECURITY_PATCH_LEVEL}`

表示名: シリアル番号

- **Web要素:** `SERIAL_NUMBER`
- **マクロ:** `${device.SERIAL_NUMBER}`

表示名: SMS対応

- **Web要素:** `IS_SMS_CAPABLE`
- **マクロ:** `${device.IS_SMS_CAPABLE}`

表示名: 監視対象

- **Web要素:** `SUPERVISED`
- **マクロ:** `${device.SUPERVISED}`

表示名: サスペンド理由

- **Web要素:** `GOOGLE_AW_DIRECTORY_SUSPENTION_REASON`
- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON}`

表示名: 改ざんステータス

- **Web要素:** `TAMPERED_STATUS`
- **マクロ:** `${device.TAMPERED_STATUS}`

表示名: 利用規約

- **Web要素:** `TERMS_AND_CONDITIONS`
- **マクロ:** `${device.TERMS_AND_CONDITIONS}`

表示名: 利用規約に同意済みか？

- **Web要素:** `GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS`
- **マクロ:** `${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS}`

表示名: テスト署名が有効か？

- **Web要素:** `WINDOWS_HAS_TEST_SIGNING_ENABLED`
- **マクロ:** `${device.WINDOWS_HAS_TEST_SIGNING_ENABLED}`

表示名: 合計RAM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Web要素:** `MEMORY`
- **マクロ:** `${device.MEMORY}`

表示名: 合計ストレージ容量

- **Web要素:** `TOTAL_DISK_SPACE`
- **マクロ:** `${device.TOTAL_DISK_SPACE}`

表示名: TPMバージョン

- **Web要素:** `TPM_VERSION`
- **マクロ:** `${device.TPM_VERSION}`

表示名: UDID

- **Web要素:** `UDID`
- **マクロ:** `${device.UDID}`

表示名: ユーザーアカウント制御の状態

- **Web要素:** `UAC_STATUS`
- **マクロ:** `${device.UAC_STATUS}`

表示名: ユーザーエージェント

- **Web要素:** `USER_AGENT`
- **マクロ:** `${device.USER_AGENT}`

表示名: ユーザー定義 #1

- **Web要素:** `USER_DEFINED_1`
- **マクロ:** `${device.USER_DEFINED_1}`

表示名: ユーザー定義 #2

- **Web要素:** `USER_DEFINED_2`
- **マクロ:** `${device.USER_DEFINED_2}`

表示名: ユーザー定義 #3

- **Web要素:** `USER_DEFINED_3`
- **マクロ:** `${device.USER_DEFINED_3}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名: ユーザー言語 (ロケール)

- **Web要素:** `USER_LANGUAGE`
- **マクロ:** `${device.USER_LANGUAGE}`

表示名: ベンダー

- **Web要素:** `VENDOR`
- **マクロ:** `${device.VENDOR}`

表示名: 音声対応

- **Web要素:** `IS_VOICE_CAPABLE`
- **マクロ:** `${device.IS_VOICE_CAPABLE}`

表示名: 音声ローミングを許可

- **Web要素:** `VOICE_ROAMING_ENABLED`
- **マクロ:** `${device.VOICE_ROAMING_ENABLED}`

表示名: VSMが有効ですか？

- **Web要素:** `WINDOWS_HAS_VSM_ENABLED`
- **マクロ:** `${device.WINDOWS_HAS_VSM_ENABLED}`

表示名: Wi-Fi MACアドレス

- **Web要素:** `WIFI_MAC`
- **マクロ:** `${device.WIFI_MAC}`

表示名: WINDOWS_ENROLLMENT_KEY

- **Web要素:** `WINDOWS_ENROLLMENT_KEY`
- **マクロ:** `${device.WINDOWS_ENROLLMENT_KEY}`

表示名: WinPEが有効ですか？

- **Web要素:** `WINDOWS_HAS_WINPE`
- **マクロ:** `${device.WINDOWS_HAS_WINPE}`

表示名: WNS通知ステータス

- **Web要素:** `PROPERTY_WNS_PUSH_STATUS`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **マクロ:** `${device.PROPERTY_WNS_PUSH_STATUS}`

表示名: WNS通知URL

- **Web要素:** `PROPERTY_WNS_PUSH_URL`
- **マクロ:** `${device.PROPERTY_WNS_PUSH_URL}`

表示名: WNS通知URL有効期限

- **Web要素:** `PROPERTY_WNS_PUSH_URL_EXPIRY`
- **マクロ:** `${device.PROPERTY_WNS_PUSH_URL_EXPIRY}`

表示名: Citrix Endpoint ManagementエージェントID

- **Web要素:** `ENROLLMENT_AGENT_ID`
- **マクロ:** {device.ENROLLMENT_AGENT_ID}`

表示名: Citrix Endpoint Managementエージェントリビジョン

- **Web要素:** `EW_REVISION`
- **マクロ:** `${device.EW_REVISION}`

表示名: Citrix Endpoint Managementエージェントバージョン

- **Web要素:** `EW_VERSION`
- **マクロ:** `${device.EW_VERSION}`

表示名: Zebra APIが利用可能

- **Web要素:** `ZEBRA_MDM`
- **マクロ:** `${device.ZEBRA_MDM}`

表示名: Zebra MXMFバージョン

- **Web要素:** `ZEBRA_MDM_VERSION`
- **マクロ:** `${device.ZEBRA_MDM_VERSION}`

表示名: Zebraパッチバージョン

- **Web要素:** `ZEBRA_PATCH_VERSION`
- **マクロ:** `${device.ZEBRA_PATCH_VERSION}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

組み込みユーザープロパティを取得するためのマクロ

表示名	マクロ
`domainname` (ドメイン名; デフォルトドメイン)	`${user.domainname}`
`loginname` (ユーザー名とドメイン名)	`${user.loginname}`
`username` (ドメインを除くログイン名 (存在する場合))	`${user.username}`

すべてのユーザープロパティのマクロ

表示名	WEB要素	マクロ
Active Directoryのログオン失敗試行回数	`badpwdcount`	`${user.badpwdcount}`
ActiveSyncユーザーメール	`asuseremail`	`${user.asuseremail}`
ASMデータソース	`aspersonsource`	`${user.aspersonsource}`
ASM展開プログラムアカウント名	`asmdepaccount`	`${user.asmdepaccount}`
ASM管理対象Apple ID	`aspersonmanagedappleid`	`${user.aspersonmanagedappleid}`
ASMパスコードタイプ	`aspersonpasscodetype`	`${user.aspersonpasscodetype}`
ASM 個人ID	`aspersonid`	`${user.aspersonid}`
ASM 個人ステータス	`aspersonstatus`	`${user.aspersonstatus}`
ASM 個人役職	`aspersontitle`	`${user.aspersontitle}`
ASM 個人一意ID	`aspersonuniqueid`	`${user.aspersonuniqueid}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名	WEB要素	マクロ
ASM ソースシステムID	`asmpersonsourcesystemid`	`${user.asmpersonsourcesystemid}`
ASM 学生の学年	`asmpersongrade`	`${user.asmpersongrade}`
BES ユーザーのメールアドレス	`besuseremail`	`${user.besuseremail}`
会社	`company`	`${user.company}`
会社名	`companyname`	`${user.companyname}`
国	`c`	`${user.c}`
部署	`department`	`${user.department}`
説明	`description`	`${user.description}`
無効なユーザー	`disableduser`	`${user.disableduser}`
表示名	`displayname`	`${user.displayname}`
識別名	`distinguishedname`	`${user.distinguishedname}`
ドメイン名	`domainname`	`${user.domainname}`
メール	`mail`	`${user.mail}`
名	`givenname`	`${user.givenname}`
自宅住所	`homestreetaddress`	`${user.homestreetaddress}`
自宅の市	`homecity`	`${user.homecity}`
居住国	`homecountry`	`${user.homecountry}`
自宅FAX	`homefax`	`${user.homefax}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名	WEB要素	マクロ
自宅電話	`homephone`	`${user.homephone}`
居住州/地域	`homestate`	`${user.homestate}`
自宅の郵便番号	`homezip`	`${user.homezip}`
IP電話	`ipphone`	`${user.ipphone}`
ミドルネームの頭文字	`middleinitial`	`${user.middleinitial}`
ミドルネーム	`middlename`	`${user.middlename}`
携帯電話	`mobile`	`${user.mobile}`
名前	`cn`	`${user.cn}`
勤務先住所	`physicaldeliveryofficename`	`${user.physicaldeliveryofficename}`
勤務先都市	`l`	`${user.l}`
勤務先FAX番号	`facsimiletelephonenumber`	`${user.facsimiletelephonenumber}`
勤務先都道府県	`st`	`${user.st}`
勤務先番地	`officestreetaddress`	`${user.officestreetaddress}`
会社の電話番号	`telephonenumber`	`${user.telephonenumber}`
会社の郵便番号	`postalcode`	`${user.postalcode}`
私書箱	`postofficebox`	`${user.postofficebox}`
ポケットベル	`pager`	`${user.pager}`
プライマリグループID	`primarygroupid`	`${user.primarygroupid}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示名	WEB要素	マクロ
SAM アカウント	`samaccountname`	`${user.samaccountname}`
住所	`streetaddress`	`${user.streetaddress}`
姓	`sn`	`${user.sn}`
役職	`title`	`${user.title}`
ユーザーログオン名	`userprincipalname`	`${user.userprincipalname}`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

自動アクション

Citrix Endpoint Management で自動アクションを作成し、以下の事柄に対する反応をプログラムします。

- イベント
- ユーザーまたはデバイスのプロパティ
- ユーザーデバイス上のアプリの存在

自動アクションを作成すると、そのアクションに定義されたトリガーによって、Citrix Endpoint Management に接続されたユーザーデバイスで何が起こるかが決定されます。イベントがトリガーされた場合、より深刻なアクションが実行される前に、問題を修正するようユーザーに通知を送信できます。

自動的に実行されるように設定する効果には、次のものがあります。

- デバイスの完全または選択的なワイプ。
- デバイスを非準拠に設定する。
- デバイスの取り消し。
- より深刻なアクションが実行される前に、問題を修正するようユーザーに通知を送信する。

MAM専用モードの場合、アプリロックおよびアプリワイプアクションを構成できます。

自動アクションを使用して、Azure Active Directory (AD) に参加している Windows 10 および Windows 11 デバイスを Azure AD で非準拠としてマークできます。

注：

ユーザーに通知する前に、Citrix Endpoint Management がメッセージを送信できるように、Citrix Endpoint Management の SMTP 設定で通知サーバーを構成する必要があります。詳細については、「通知」を参照してください。続行する前に、使用する予定の通知テンプレートを設定してください。詳細については、「通知」を参照してください。設定については、「通知テンプレートの作成と更新」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アクションの例

自動化されたアクションの使用例を次に示します。

例1

- 以前にブロックしたアプリ（例: 「Words with Friends」）を検出したいとします。「Words with Friends」アプリを検出した後、ユーザーデバイスを非準拠状態にするトリガーを指定できます。その後、アクションは、デバイスを準拠状態に戻すためにアプリを削除する必要があることをユーザーに通知します。ユーザーが準拠するまで待機する時間制限を設定することもできます。その時間制限が過ぎると、デバイスの選択的ワイプなど、定義されたアクションが実行されます。

例2

- 顧客が最新のファームウェアを使用しているかどうかを確認し、ユーザーがデバイスを更新する必要がある場合にリソースへのアクセスをブロックしたいとします。ユーザーデバイスが最新バージョンでない場合に、ユーザーデバイスを非準拠状態にするトリガーを指定できます。自動化されたアクションを使用して、リソースをブロックし、顧客に通知します。

例3

- ユーザーデバイスが非準拠状態になり、ユーザーがデバイスを修正したとします。デバイスを準拠状態にリセットするパッケージを展開するポリシーを構成できます。

例4

- 特定の期間非アクティブだったユーザーデバイスを非準拠としてマークしたいとします。非アクティブなデバイスに対して、次のように自動化されたアクションを作成できます。

  a. Citrix Endpoint Managementコンソールで、 > の順に移動し、 を選択します。 設定の詳細については、「ネットワークアクセス制御」を参照してください。

  b. アクションの追加と管理 に記載されているアクションを追加する手順に従います。唯一の違いは、 ページで次のように設定を構成することです。

     - 。、、、および を選択します。
     - 。 を選択し、 の を使用して作成したテンプレートを選択します。次に、アクションを実行するまでの遅延を日、時間、または分で設定します。ユーザーがトリガーとなる問題に対処するまでアクションが繰り返される間隔を設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ヒント:

非アクティブなデバイスを一括削除するには、(/ja-jp/citrix-endpoint-management/downloads/public-rest-api.pdf)を使用します。まず、削除したい非アクティブなデバイスのデバイスIDを手動で取得し、その後、削除APIを実行してそれらを一括削除します。

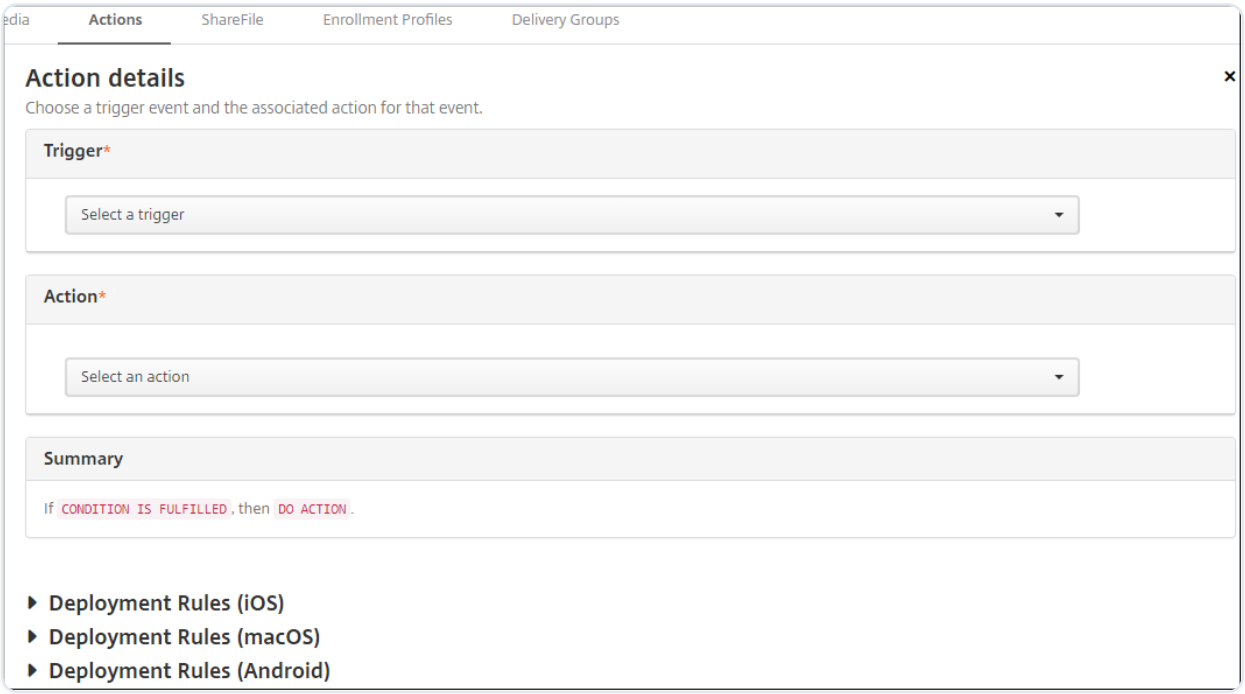
アクションの追加と管理

自動アクションを追加、編集、フィルタリングするには：

1. Citrix Endpoint Managementコンソールで、**構成 > アクション**をクリックします。**アクション**ページが表示されます。
2. **アクション**ページで、次のいずれかを実行します。
   - **追加**をクリックしてアクションを追加します。
   - 既存のアクションを選択して編集または削除します。使用したいオプションをクリックします。
3. **アクション情報**ページが表示されます。
4. **アクション情報**ページで、次の情報を入力または変更します。
   - **名前:** アクションを識別するための名前を入力します。このフィールドは必須です。
   - **説明:** アクションの目的を説明します。
5. **次へ**をクリックします。**アクションの詳細**ページが表示されます。

   次の例は、**イベント**トリガーを設定する方法を示しています。別のトリガーを選択した場合、表示されるオプションはここに示されているオプションとは異なります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. **アクションの詳細**ページで、次の情報を入力または変更します。

   「**トリガー**」リストで、このアクションのイベントトリガーの種類をクリックします。次のいずれかのトリガーを選択します。

   - 「**イベント**」: 選択した非準拠イベントにデバイスの状態が一致するかどうかを確認し、それに対応します。
   - 「**デバイスプロパティ**」: MDMで管理されているデバイスのデバイス属性の特定の値をチェックし、それに対応します。詳しくは、「デバイスプロパティ名と値」PDFを参照してください。
   - 「**ユーザープロパティ**」: 通常、Active Directoryからのユーザー属性の特定の値に対応します。
   - 「**インストール済みアプリ名**」: アプリがインストールされたことに対応します。MAM専用モードには適用されません。デバイスでアプリインベントリポリシーが有効になっている必要があります。アプリインベントリポリシーは、すべてのプラットフォームでデフォルトで有効になっています。詳しくは、「アプリインベントリデバイスポリシー」を参照してください。
   - 「**ポリシーの戻り値**」: PowerShellスクリプトから返された値が特定のロジック基準を満たしているかどうかを確認します。Windowsエージェントポリシーを有効にして構成する必要があります。Windowsエージェントポリシーについて詳しくは、「Windowsエージェントデバイスポリシー」を参照してください。

7. 次のリストで、トリガーへの応答をクリックします。

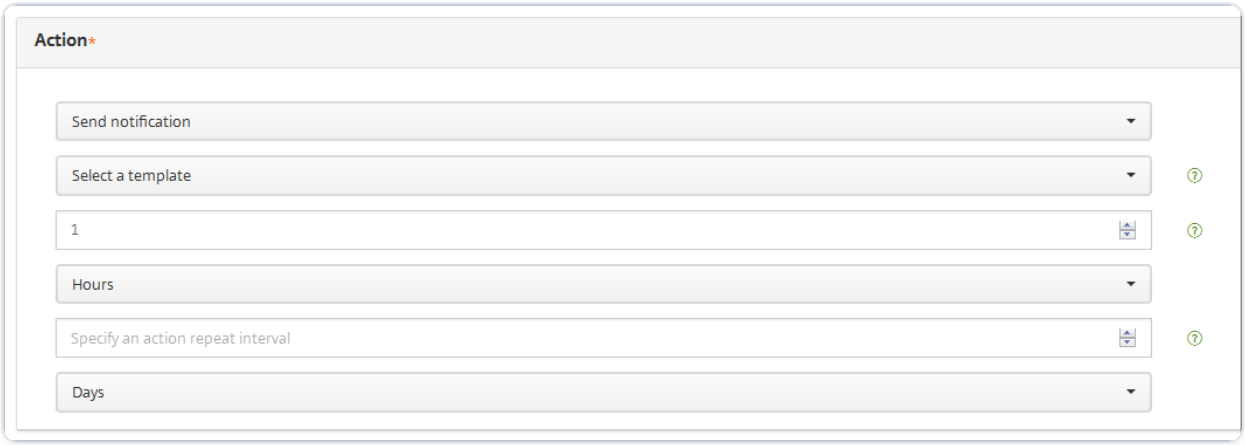
© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. 「**アクション**」リストで、トリガー条件が満たされたときに実行するアクションをクリックします。「**通知の送信**」アクションを除き、ユーザーがトリガーの原因となった問題を解決できる期間を選択します。その期間内に問題が解決されない場合、選択したアクションが実行されます。アクションの定義については、「セキュリティアクション」を参照してください。

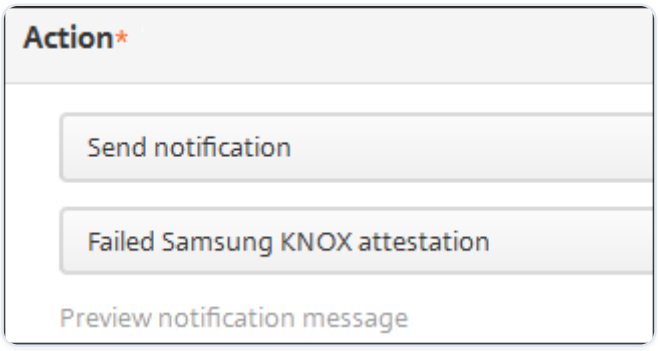
   「**通知の送信**」を選択した場合、次の手順で通知アクションを送信します。

9. 次のリストで、通知に使用するテンプレートを選択します。選択したイベントに関連する通知テンプレートが表示されます。通知の種類にテンプレートがない場合は、「このイベントタイプにはテンプレートがありません。**設定**の**通知テンプレート**を使用してテンプレートを作成してください。」というメッセージでテンプレートを構成するように求められます。

   ユーザーに通知するには、Citrix Endpoint Managementがメッセージを送信できるように、**設定 > 通知サーバー**を使用してSMTPの設定を構成します。「通知」を参照してください。また、続行する前に、**設定 > 通知テンプレート**を使用して、使用する予定の通知テンプレートを設定してください。「通知テンプレートの作成と更新」を参照してください。



   テンプレートを選択したら、「**通知メッセージのプレビュー**」をクリックします。



10. 次のフィールドで、アクションを実行するまでの遅延を日、時間、または分で設定します。ユーザーがトリガーとなる問題に対処するまで、アクションが繰り返される間隔を設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



11. **概要**で、意図したとおりに自動アクションが作成されたことを確認します。



12. アクションの詳細を構成したら、各プラットフォームの展開ルールを個別に構成できます。これを行うには、選択した各プラットフォームについて手順13を完了します。
13. 展開ルールを構成します。展開ルールの構成に関する一般情報については、「リソースの展開」を参照してください。

    この例では：

    - デバイスの所有権は**BYOD**である必要があります。
    - デバイスはパスコードに準拠している必要があります。
    - デバイスのモバイル国コードはアンドラのみにすることはできません。

14. アクションのプラットフォーム展開ルールの構成が完了したら、**次へ**をクリックします。**アクションの割り当て**ページが表示され、そこでアクションを1つまたは複数のデリバリーグループに割り当てます。この手順はオプションです。
15. **デリバリーグループの選択**の横で、入力してデリバリーグループを検索するか、リストからグループを選択します。選択したグループは、**アプリの割り当てを受け取るデリバリーグループ**リストに表示されます。
16. **展開スケジュール**を展開し、次の設定を構成します。

    - **展開**の横で、**オン**をクリックして展開をスケジュールするか、**オフ**をクリックして展開を防止します。デフォルトのオプションは**オン**に設定されています。**オフ**を選択した場合、他のオプションは不要です。
    - **展開スケジュール**の横で、**今すぐ**または**後で**をクリックします。デフォルトのオプションは**今すぐ**に設定されています。
    - **後で**をクリックした場合は、カレンダーアイコンをクリックし、展開の日付と時刻を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**展開条件**」の横で、「**接続ごとに**」または「**前回の展開が失敗した場合のみ**」をクリックします。デフォルトオプションは「**接続ごとに**」に設定されています。
- 「**常時接続の展開**」の横で、「**オン**」または「**オフ**」をクリックします。デフォルトオプションは「**オフ**」に設定されています。

  このオプションは、「**設定 > サーバープロパティ**」でバックグラウンド展開のスケジュールキーを設定した場合に適用されます。

  注:

  このオプションは、「**設定 > サーバープロパティ**」でバックグラウンド展開のスケジュールキーを設定した場合に適用されます。

  常時接続オプション:

  - iOSデバイスでは利用できません
  - バージョン10.18.19以降でCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様は利用できません
  - バージョン10.18.19より前にCitrix Endpoint Managementの使用を開始したAndroidおよびAndroid Enterpriseのお客様には推奨されません

構成する展開スケジュールは、すべてのプラットフォームで同じです。行った変更は、「**常時接続の展開**」を除き、すべてのプラットフォームに適用されます。

17. 「**次へ**」をクリックします。「**概要**」ページが表示され、アクション構成を確認できます。
18. 「**保存**」をクリックしてアクションを保存します。

MAM専用モードのアプリロックおよびアプリワイプアクション

Citrix Endpoint Managementコンソールにリストされている4つのトリガーカテゴリ（イベント、デバイスプロパティ、ユーザープロパティ、インストール済みアプリ名）すべてについて、デバイス上のアプリをワイプまたはロックできます。

自動アプリワイプまたはアプリロックを構成するには

1. Citrix Endpoint Management コンソールで、 > をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. ページで、 をクリックします。
3. ページで、アクションの名前とオプションの説明を入力します。
4. ページで、目的のトリガーを選択します。
5. で、アクションを選択します。

この手順では、以下の条件に注意してください。

トリガーの種類が**に設定されており、値がではない場合、および**アクションは表示されません。

トリガーの種類が**に設定されており、値が**である場合、次のアクションは表示されません。

- デバイスを選択的にワイプする
- デバイスを完全にワイプする
- デバイスを取り消す

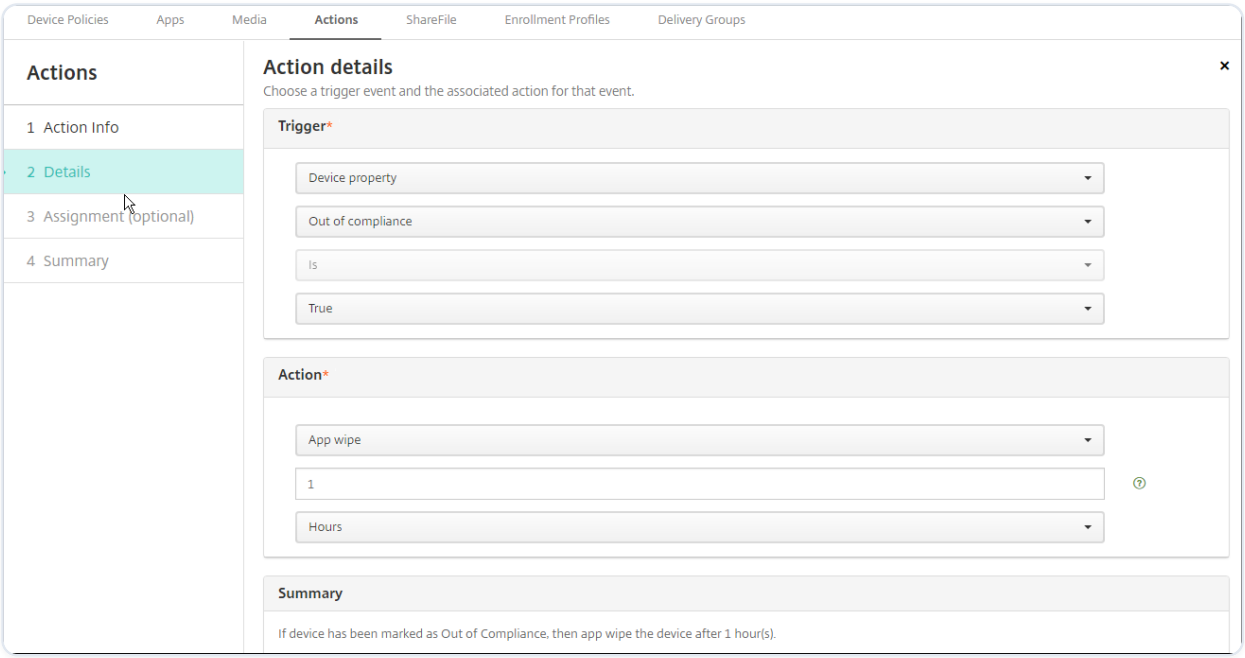
各オプションについて、1時間の遅延が自動的に設定されますが、遅延期間を分、時間、または日で選択できます。遅延の目的は、アクションが実行される前にユーザーが問題を解決する時間を与えることです。アプリのワイプとアプリのロックアクションの詳細については、セキュリティアクションを参照してください。

注：

トリガーを****に設定すると、繰り返し間隔は自動的に最低1時間になります。通知を受信するには、デバイスがポリシーを更新してサーバーと同期する必要があります。通常、デバイスはユーザーがサインオンしたとき、またはCitrix Secure Hubを介してポリシーを手動で更新したときにサーバーと同期します。

Active DirectoryデータベースがCitrix Endpoint Managementと同期できるように、アクションが実行される前に約1時間の追加遅延が発生する場合があります。

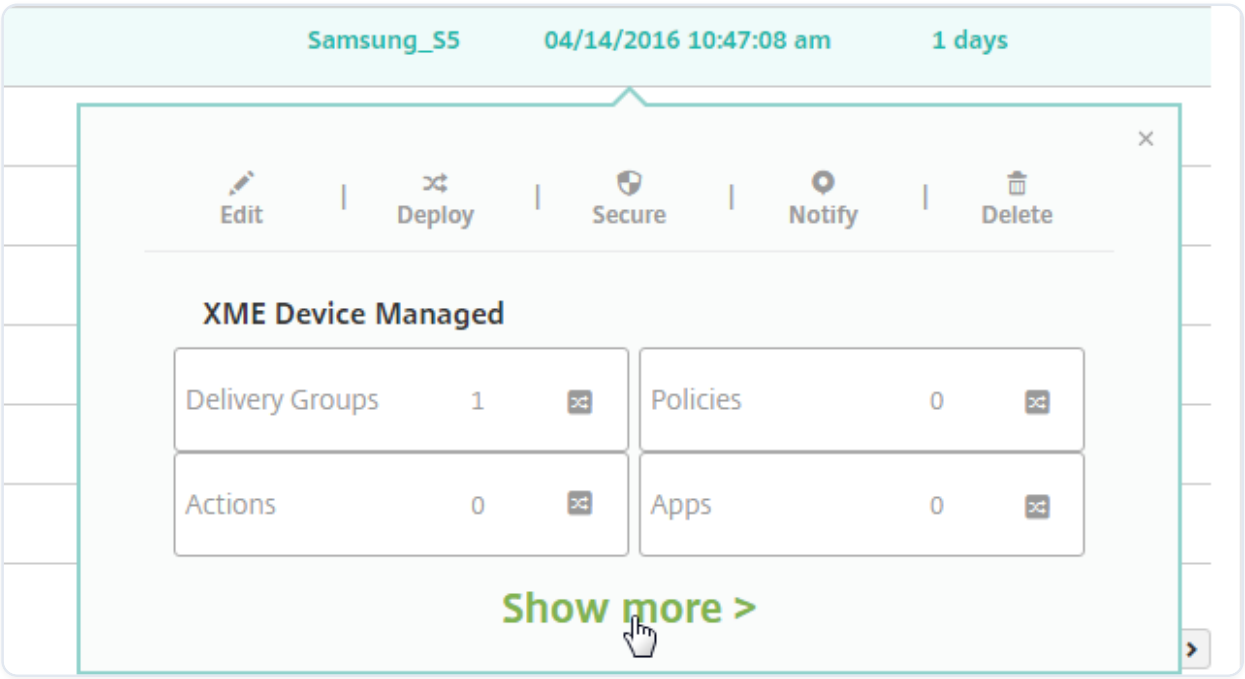
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 展開ルールを設定し、**次へ**をクリックします。
7. デリバリーグループの割り当てと展開スケジュールを設定し、**次へ**をクリックします。
8. **保存**をクリックします。

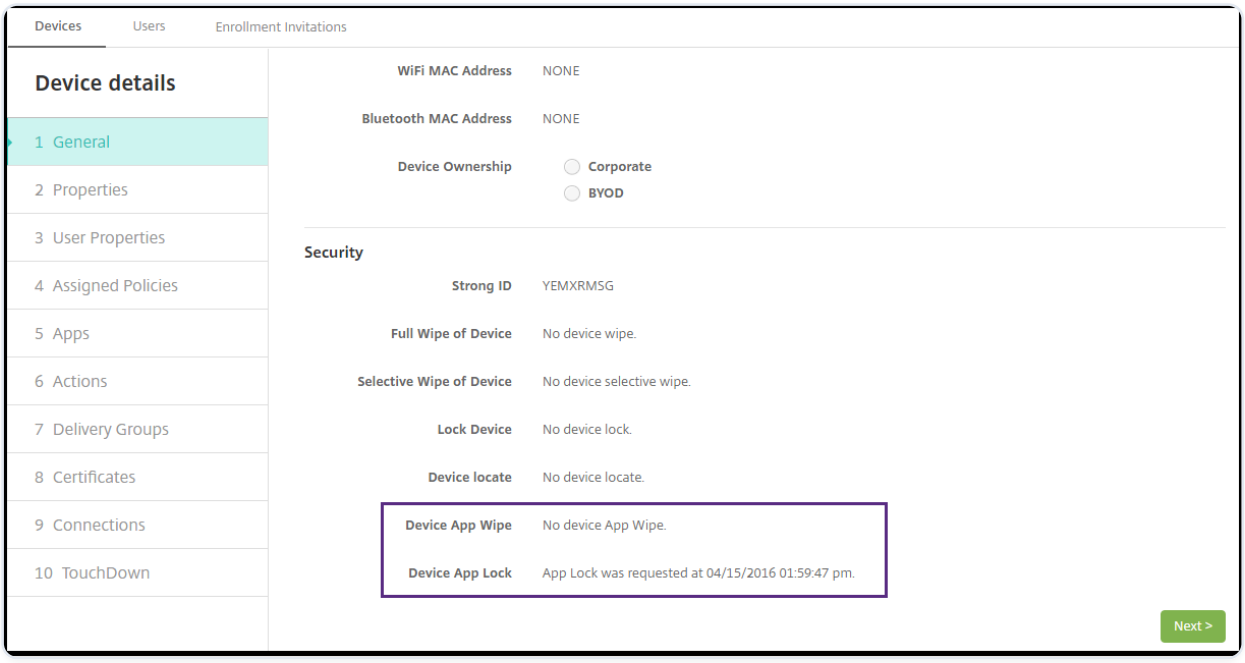
アプリロックまたはアプリワイプのステータスを確認するには

1. **管理 > デバイス**に移動し、デバイスをクリックして、**詳細を表示**をクリックします。

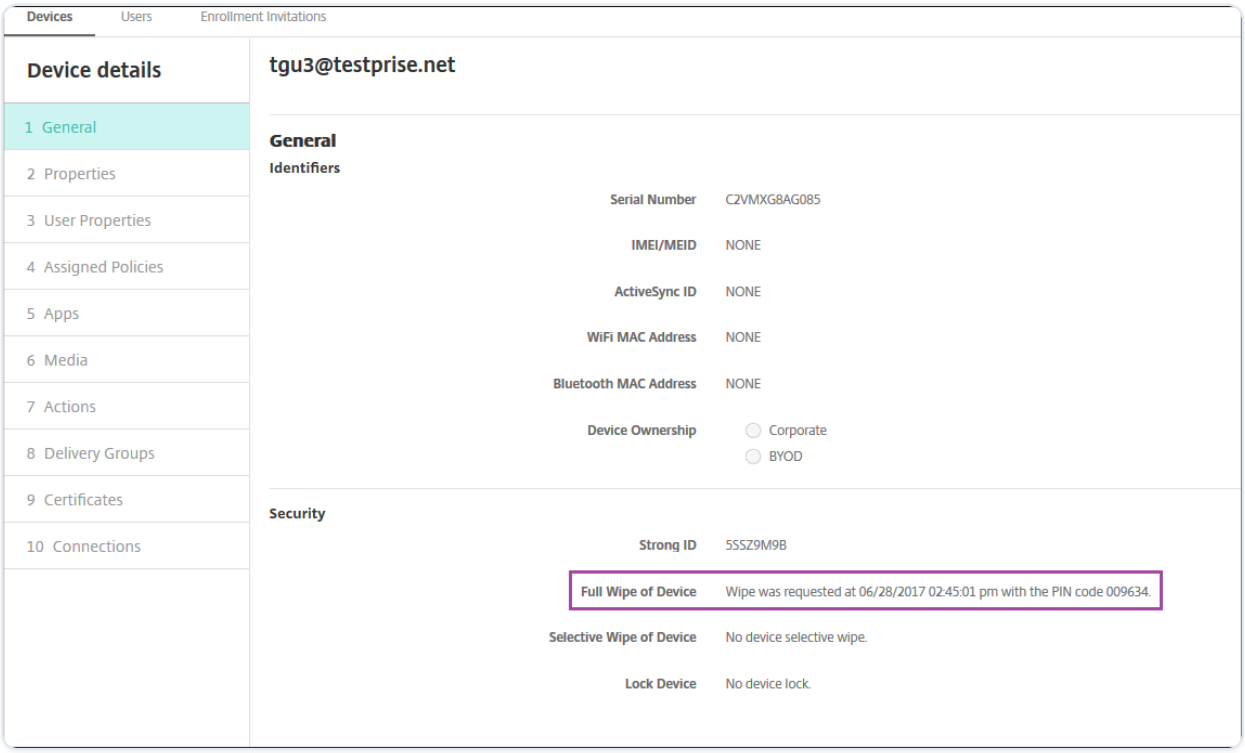


2. **デバイスアプリワイプ**と**デバイスアプリロック**までスクロールします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



デバイスがワイプされると、ユーザーはPINコードの入力を求められます。ユーザーがコードを忘れた場合は、デバイスの詳細で確認できます。



Azure ADでWindows 10およびWindows 11デバイスを非準拠としてマークする

Azure ADに参加しているWindows 10およびWindows 11デバイスがCitrix Endpoint Managementによって非準拠とマークされた場合、Azure ADでも非準拠とマークできます。この機能を有効にす

© 1997–2026 Citrix Systems, Inc. All rights reserved.

るには、Azure ADポータルでオンプレミスMDMアプリケーションにMicrosoft Graph APIへのアクセス許可を追加します。

1. Azure AD管理者資格情報を使用してAzure ADポータルにログインします。
2. Azure ADポータルで、**Azure Active Directory > モビリティ (MDM および MAM)** に移動します。**オンプレミスMDMアプリケーション**を選択します。
3. 「**オンプレミスアプリケーション設定 > 必要なアクセス許可 > 追加 > APIの選択 > Microsoft Graph**」をクリックします。「**選択**」をクリックして保存します。
4. 「**必要なアクセス許可**」で「**Microsoft Graph**」を選択します。「**アクセスを有効にする**」で「**ディレクトリデータの読み取りと書き込み**」を選択します。
5. 「**必要なアクセス許可**」で「**Microsoft Graph**」を選択します。次に、「**アクセス許可の付与**」をクリックします。
6. アクセス許可を付与するには、「**はい**」をクリックします。

Windows 10またはWindows 11を実行しているAzure AD登録済みデバイスが非準拠である場合、Citrix Endpoint ManagementはAzure ADでもそのデバイスを非準拠としてマークします。

Windowsエージェントデバイスポリシーの結果に基づいて自動アクションを作成する

Windowsエージェントデバイスポリシーを使用して、管理対象のWindowsデスクトップおよびタブレットでレジストリ値を監視するスクリプトを展開します。スクリプトから返された値に基づいて、自動アクションを実行するように構成できます。

1. Windowsエージェントデバイスポリシーを構成し、スクリプトによって返される値を確認します。Windowsエージェントデバイスポリシーの詳細については、Windowsエージェントデバイスポリシーを参照してください。

   その記事とこのセクションには、`EntApp_2019_checkFirewall`という名前のスクリプトに基づいたサンプルが含まれています。関連するWindowsエージェントデバイスポリシーは、`cName_checkFirewall`という名前の構成を定義します。その構成はサンプルスクリプトを実行します。

   スクリプトがデバイスで実行された後、Windowsエージェントデバイスポリシーで説明されているように、アクションを作成するために必要な情報が得られます。
2. Citrix Endpoint Managementコンソールで、「**構成 > アクション**」をクリックします。
3. **アクション**ページで、「**追加**」をクリックします。
4. **アクション情報**ページで、アクションの名前とオプションの説明を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. **アクションの詳細**ページで、「**ポリシーが返した値**」トリガーを選択します。

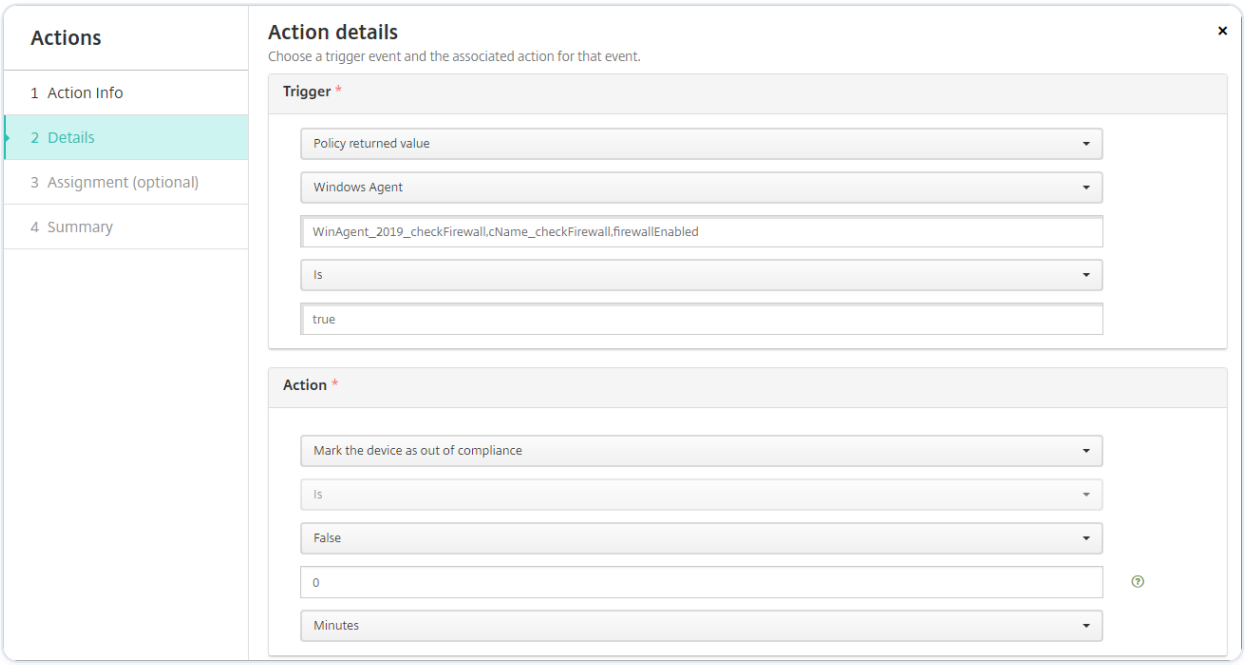


6. 表示されるフィールドで、トリガーとアクションを定義します。

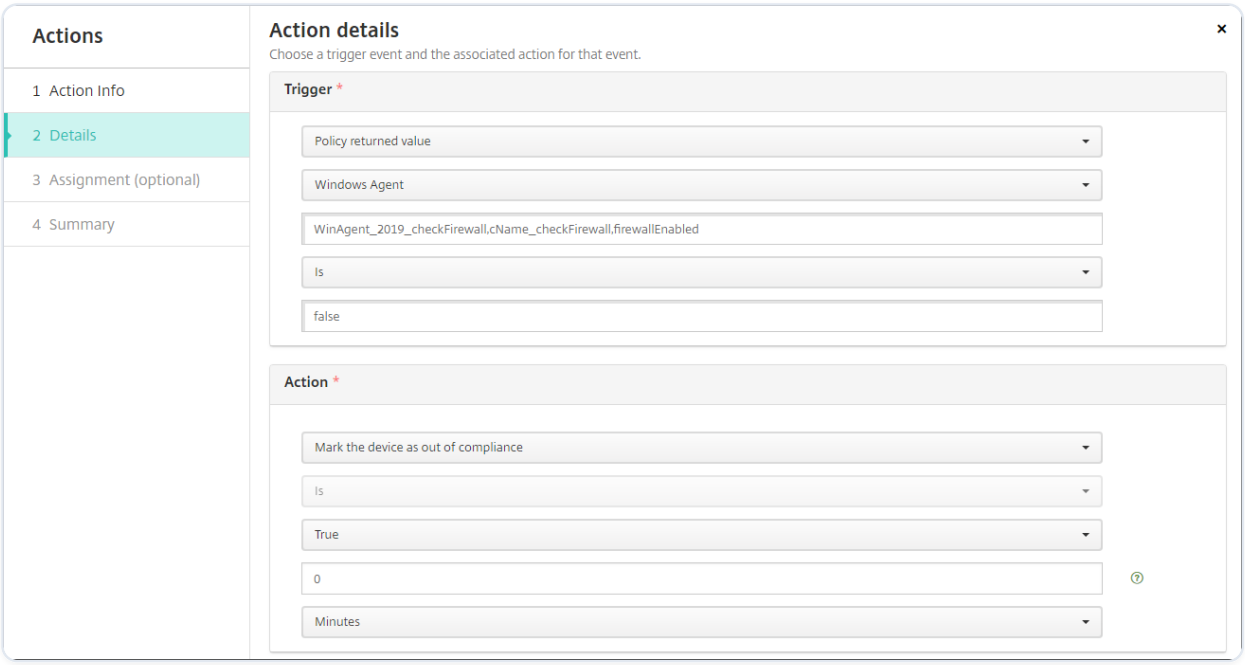
   - **Windows Agent設定:** 作成したWindows Agentポリシーのポリシー名、構成名、およびキー名を入力します。
   - **ドロップダウンメニュー: Is、Is Not、Contains、またはDoes Not Contain**のロジックを選択します。このロジックは次のフィールドに適用され、ロジックが適用されるとアクションがトリガーされます。
   - **文字列を入力:** ポリシーでアップロードしたPowerShellスクリプトの実行結果として得られた文字列を入力します。その文字列を見つける方法については、「Windows Agentデバイスポリシー」を参照してください。
   - **アクション:** アクション、アクションの値を選択し、アクションを解決するための期間を選択します。

   例: キー名`firewallEnabled`が値`true`を返す場合、次のアクションはデバイスを準拠としてマークします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



キー名`firewallEnabled`が値`false`を返す場合、次のアクションはデバイスを非準拠としてマークします。



7. 必要に応じて、展開スケジュールを設定し、デリバリーグループを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

監視とサポート

Citrix Endpoint ManagementダッシュボードとCitrix Endpoint Managementサポートページを使用して、Citrix Endpoint Managementサーバーを監視およびトラブルシューティングできます。Citrix Endpoint Managementサポートページを使用して、サポート関連の情報やツールにアクセスできます。

Citrix Endpoint Managementコンソールで、右上隅にあるレンチアイコンをクリックします。

サポートアイコン(/en-us/citrix-endpoint-management/media/select-support-wrench.png)

トラブルシューティングとサポートページが表示されます。

Citrix Endpoint Managementの**トラブルシューティングとサポート**ページを使用して、次のことができます。

- 診断にアクセスする。
- Citrix製品ドキュメントおよびナレッジセンターへのリンクにアクセスする。
- ログ操作にアクセスする。
- 高度な構成オプションを使用する。
- 一連のツールとユーティリティにアクセスする。

Citrix Endpoint Managementコンソールダッシュボードにアクセスすると、情報を一目で確認することもできます。この情報により、ウィジェットを使用して問題や成功をすばやく確認できます。

分析ダッシュボード(/en-us/citrix-endpoint-management/media/analyze-dashboard.png)

ダッシュボードは通常、Citrix Endpoint Managementコンソールにサインオンしたときに最初に表示されるページです。コンソールの他の場所からダッシュボードにアクセスするには、**Analyze**をクリックします。ダッシュボードで**Customize**をクリックすると、ページのレイアウトや表示されるウィジェットを編集できます。

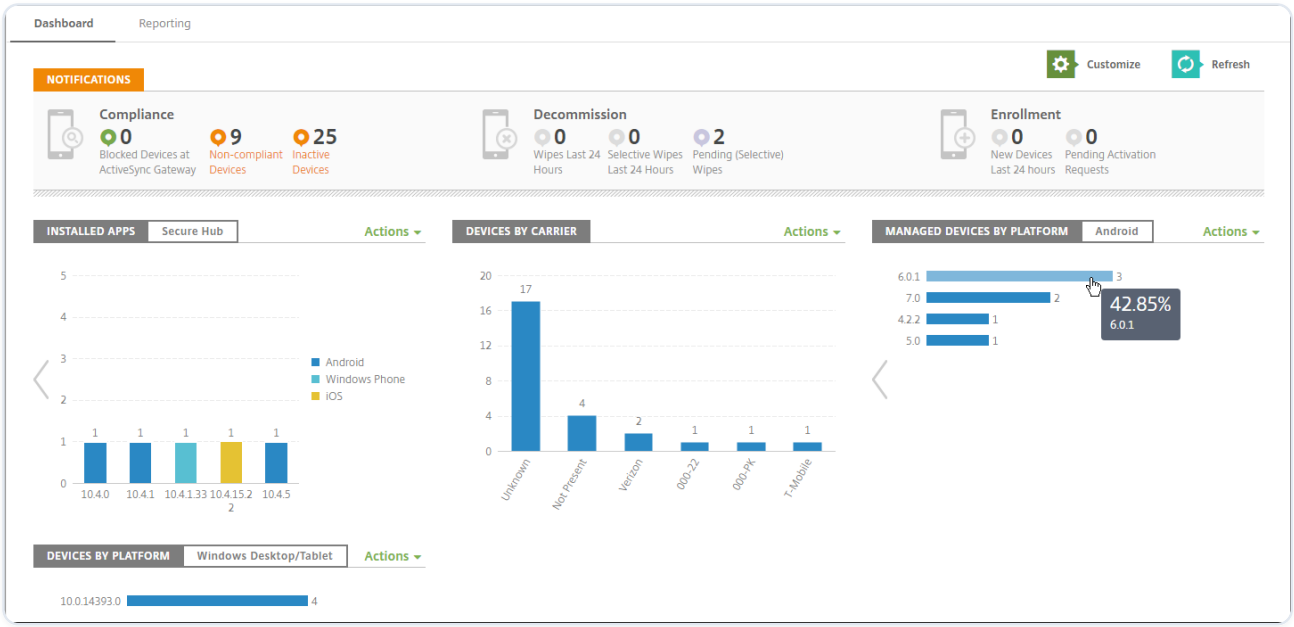
- **マイダッシュボード:** 最大4つのダッシュボードを保存できます。これらのダッシュボードは個別に編集でき、保存されたダッシュボードを選択してそれぞれを表示できます。
- **レイアウトスタイル:** この行では、ダッシュボードに表示されるウィジェットの数と、ウィジェットのレイアウト方法を選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ウィジェットの選択:** ダッシュボードに表示する情報を選択できます。
  - **通知:** ウィジェットの上に通知バーを追加するには、左側の数字の上にあるチェックボックスをオンにします。このバーには、準拠デバイス、非アクティブデバイス、および過去24時間以内にワイプまたは登録されたデバイスの数が表示されます。
  - **プラットフォーム別デバイス:** プラットフォーム別に管理対象デバイスと非管理対象デバイスの数を表示します。
  - **キャリア別デバイス:** キャリア別に管理対象デバイスと非管理対象デバイスの数を表示します。各バーをクリックすると、プラットフォーム別の内訳が表示されます。
  - **プラットフォーム別管理対象デバイス:** プラットフォーム別に管理対象デバイスの数を表示します。
  - **プラットフォーム別非管理対象デバイス:** プラットフォーム別に非管理対象デバイスの数を表示します。このグラフに表示されるデバイスは、エージェントがインストールされている可能性がありますが、その権限が取り消されているか、デバイスがワイプされています。
  - **ActiveSync Gatewayステータス別デバイス:** ActiveSync Gatewayステータス別にグループ化されたデバイスの数を表示します。情報には、ブロック済み、許可済み、または不明のステータスが表示されます。各バーをクリックすると、プラットフォーム別にデータを内訳できます。
  - **所有権別デバイス:** 所有権ステータス別にグループ化されたデバイスの数を表示します。情報には、会社所有、従業員所有、または不明の所有権ステータスが表示されます。
  - **失敗したデリバリーグループ展開:** パッケージごとの失敗した展開の総数を表示します。展開に失敗したパッケージのみが表示されます。
  - **ブロック理由別デバイス:** ActiveSyncによってブロックされたデバイスの数を表示します。
  - **インストール済みアプリ:** アプリ情報のグラフを表示するには、アプリ名を入力します。
  - **ボリューム購入アプリのライセンス使用状況:** Appleボリューム購入アプリのライセンス使用状況統計を表示します。

各ウィジェットで、個々の部分をクリックして詳細情報をドリルダウンできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Actionメニューをクリックして、情報を.csvファイルとしてエクスポートすることもできます。

分析ダッシュボードメニュー(/en-us/citrix-endpoint-management/media/analyze-dashboard-actions-menu.png)

ヘルプデスク管理者向けのモニターページ

MonitorページでCitrix Endpoint Managementを監視およびトラブルシューティングできます。このインターフェイスは、ヘルプデスク管理者がユーザーベースのトラブルシューティングを効率的に実行できるようにカスタマイズされています。

ヘルプデスク管理者は、**Monitor**ページと利用可能なすべてのワークフローにアクセスするために、次の権限を持っている必要があります。

- 承認されたアクセス
  - 管理コンソールアクセス
  - パブリックAPIアクセス
- コンソール機能
  - モニター
  - デバイス
  - デバイスの完全ワイプ
  - 位置の表示
    - デバイスの検索

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - デバイスの追跡
  - デバイスをロック
  - デバイスのロック解除
  - アプリロック
  - アプリワイプ
  - アプリ

監視ページでは、デバイスポリシーと構成の統合ビューが表示されます。このビューには、アプリのロック/ロック解除、アプリのワイプ、デバイスのロック/ロック解除、デバイスのワイプなどのトラブルシューティングアクションが含まれます。

Citrix Cloud Monitor画面のスクリーンショット(/en-us/citrix-endpoint-management/media/monitor-tab-xenmobile-cloud.png)

監視ページを使用して、次の操作を行います。

- トラブルシューティングするActive Directory (AD)ユーザーとデバイスを検索します。
- 次の情報を含む**デバイスの詳細**ページを分析します。
  - **ポリシー:** 選択したデバイスとアプリのデバイスおよびアプリポリシーを表示します。ポリシーの変更については、デバイスポリシーおよびアプリの追加を参照してください。
  - **構成:** デバイスの構成を表示します。このパネルには、デバイスで位置情報サービスが有効になっているか、ジェイルブレイクされているか、MDMまたはMAMで管理されているかを示すアイコンが含まれています。また、ストレージ暗号化の状態も表示されます。
  - **実行中のアプリケーション**テーブル: デバイスで現在実行されているアプリケーションの詳細を表示します。
- デバイスのトラブルシューティングを行います。このページで利用できるセキュリティアクションは、デバイスの登録と、ログインしている管理者に利用可能な権限に基づいています。
  - デバイスのロック/ロック解除
  - デバイスワイプ
  - アプリのロック/ロック解除 (デバイスがMAMに登録されている場合に利用可能)
  - アプリのワイプ (デバイスがMAMに登録されている場合に利用可能)

実行できるアクションの詳細については、セキュリティアクションを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

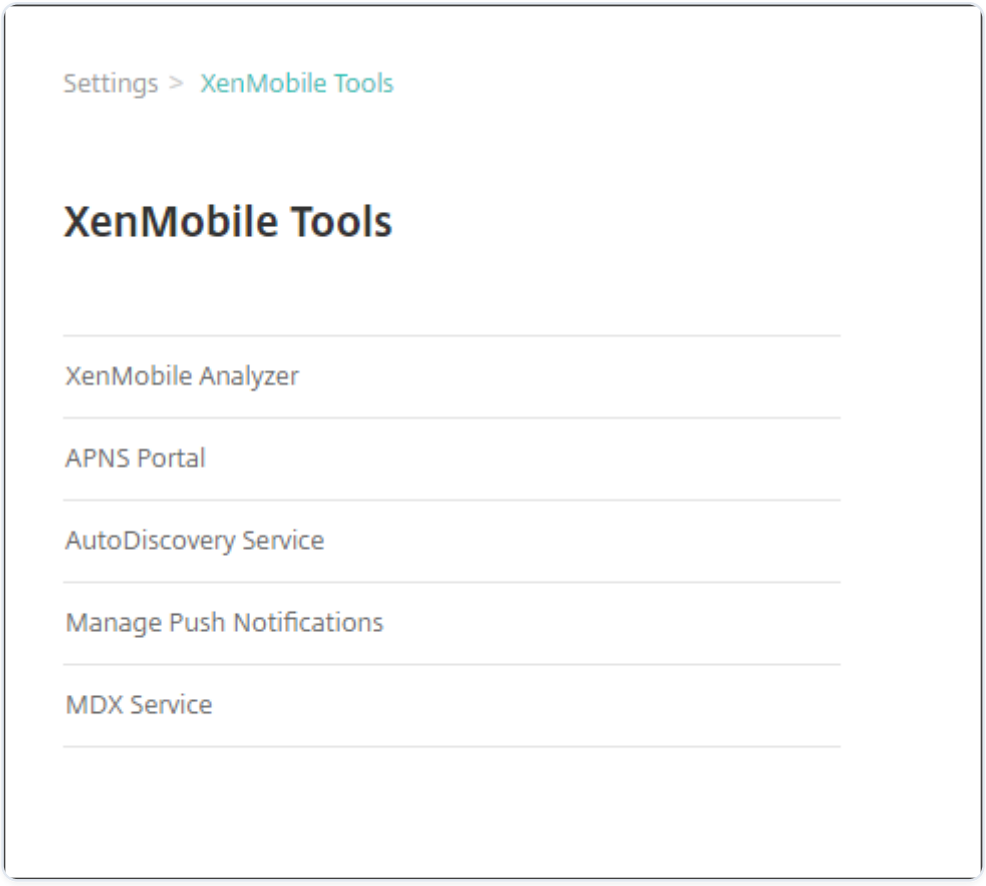
監視ページは、ログインセッションの更新を処理しないため、最後に読み込まれてから60分後に予期したとおりに動作しない場合があります。回避策として、ページを再読み込みしてトークンを更新してください。サービスコンソールで**Citrix Cloud**リンクをクリックし、**Citrix Endpoint Management > Manage > Monitor**をクリックします。

コンソールからのCitrix Endpoint Managementツールへのアクセス

Citrix Endpoint Managementコンソールから、以下のCitrix Endpoint Managementツールにアクセスできます。

- **APNsポータル** – APNs証明書に署名するようCitrixにリクエストを送信し、その証明書をAppleに提出します。
- **自動検出サービス** – ドメイン内のCitrix Endpoint Managementの自動検出をリクエストおよび構成します。
- **プッシュ通知の管理** – iOSおよびWindowsモバイルアプリのプッシュ通知を管理します。

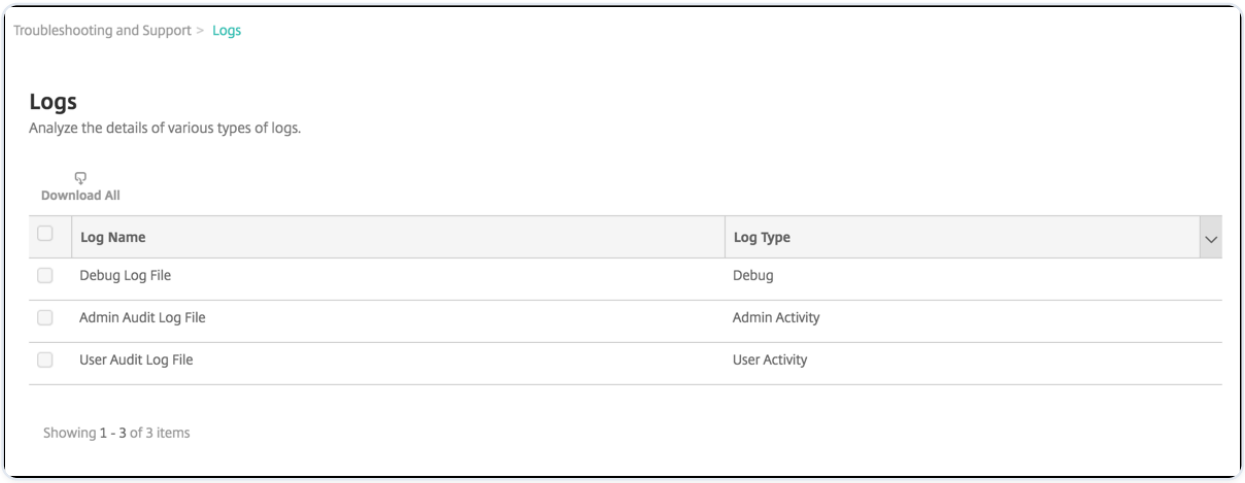
これらのツールにアクセスするには、**設定 > Citrix Endpoint Managementツール**に移動します。このページは、Cloud AdminまたはCustomer Adminの役割を持つユーザーが利用できます。



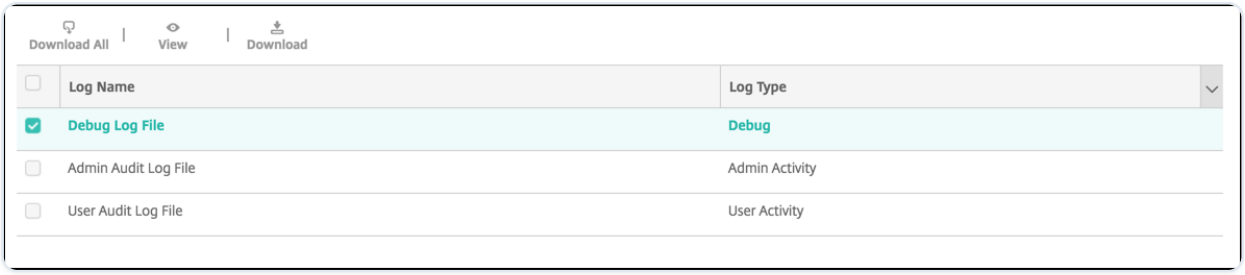
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementでのログファイルの表示と分析

1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にあるレンチアイコンをクリックします。**トラブルシューティングとサポート**ページが開きます。
2. **ログ操作**で、**ログ**をクリックします。**ログ**ページが表示されます。個々のログがテーブルに表示されます。



3. 表示したいログを選択します:
   - デバッグログファイルには、エラーメッセージやサーバー関連のアクションなど、Citrixサポートに役立つ情報が含まれています。
   - 管理者監査ログファイルには、Citrix Endpoint Managementコンソールでのアクティビティに関する監査情報が含まれています。
   - ユーザー監査ログファイルには、設定されたユーザーに関連する情報が含まれています。
4. テーブルの上部にあるアクションを使用して、すべてのログをダウンロード、表示、または単一のログをダウンロードします。



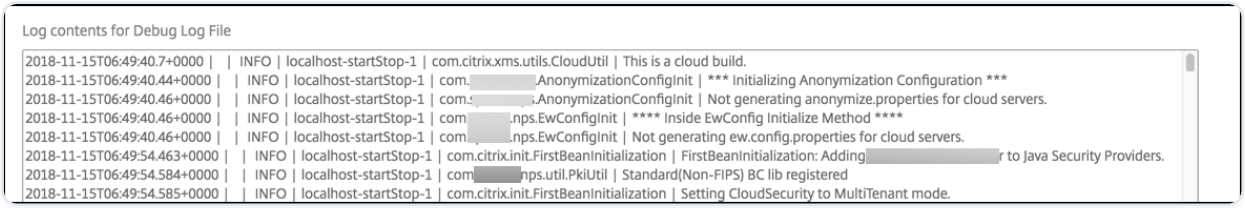
注:

複数のログファイルを選択した場合、**すべてダウンロード**のみが利用可能です。

5. 次のいずれかを実行します:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **すべてダウンロード:** コンソールは、システムに存在するすべてのログ (デバッグ、管理者監査、ユーザー監査、サーバーログなど) をダウンロードします。
- **表示:** 選択したログの内容をテーブルの下に表示します。
- **ダウンロード:** コンソールは、選択された単一のログファイルタイプのみをダウンロードします。コンソールは、同じタイプのアーカイブされたログもダウンロードします。



Citrix Endpoint Managementは、log4j syslogアペンダーを使用してRFC5424形式のsyslogメッセージを送信します。syslogメッセージデータは、特定の形式を持たないプレーンテキストです。

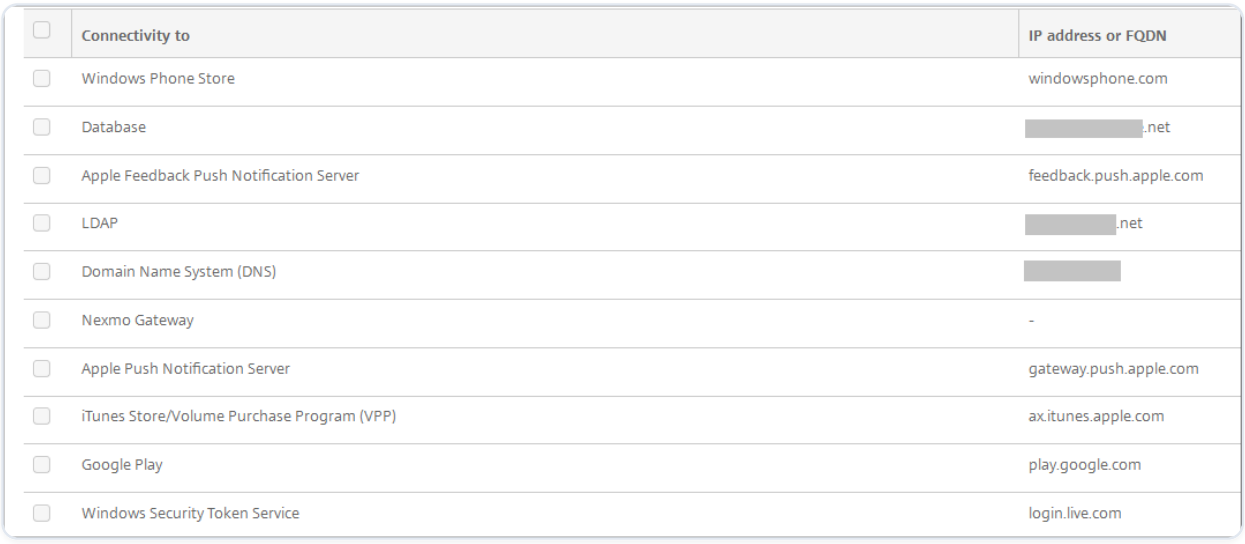
接続性チェック

Citrix Endpoint Managementの**トラブルシューティングとサポート**ページから、NetScaler Gatewayおよびその他のサーバーや場所へのCitrix Endpoint Managementの接続を確認できます。Citrix Endpoint Managementの接続性チェックを実行するには、サポートまたは管理者ロールが必要です。このロールは、ロールベースのアクセス制御 (RBAC) を使用して設定します。ロールの割り当ての詳細については、「RBACでロールを構成する」を参照してください。

Citrix Endpoint Managementの接続性チェックを実行する

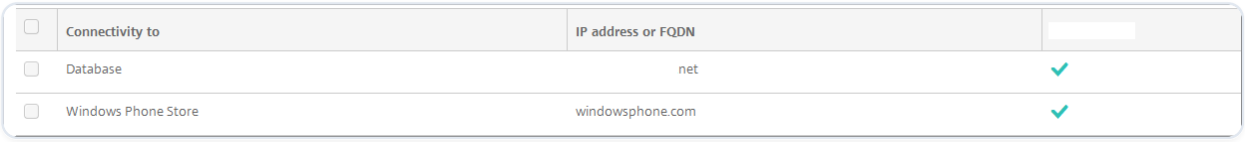
1. Citrix Endpoint Managementコンソールで、コンソールの右上隅にあるレンチアイコンをクリックします。**トラブルシューティングとサポート**ページが表示されます。
2. **診断**の下にある**Citrix Endpoint Management接続性チェック**をクリックします。**Citrix Endpoint Management接続性チェック**ページが表示されます。Citrix Endpoint Management環境にクラスター化されたノードがある場合、すべてのノードが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



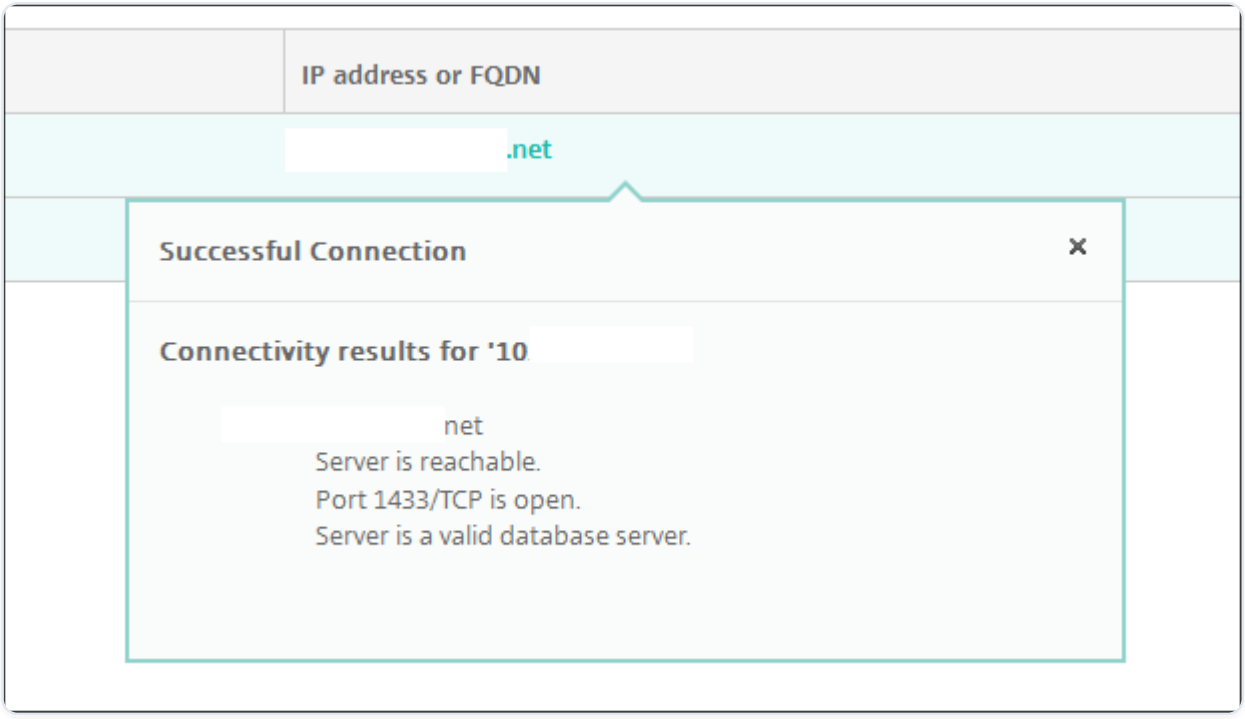
Connectivity to	IP address or FQDN
Windows Phone Store	windowsphone.com
Database	.net
Apple Feedback Push Notification Server	feedback.push.apple.com
LDAP	.net
Domain Name System (DNS)	
Nexmo Gateway	-
Apple Push Notification Server	gateway.push.apple.com
iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
Google Play	play.google.com
Windows Security Token Service	login.live.com

3. 接続性テストに含めるサーバーを選択し、**接続性のテスト**をクリックします。テスト結果ページが表示されます。



Connectivity to	IP address or FQDN	
Database	net	✓
Windows Phone Store	windowsphone.com	✓

4. テスト結果テーブルでサーバーを選択すると、そのサーバーの詳細な結果が表示されます。

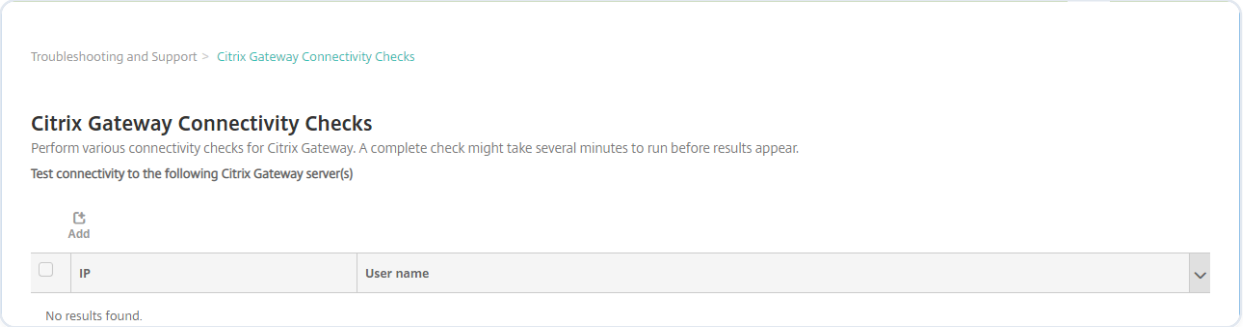


Citrix Endpoint Managementが実行できる接続性チェックとその詳細については、「接続性チェックの詳細」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gatewayの接続性チェックの実行

1. **トラブルシューティングとサポート**ページで、**診断**の下にある**NetScaler Gateway接続性チェック**をクリックします。**NetScaler Gateway接続性チェック**ページが表示されます。Citrix Endpoint ManagementとNetScaler Gatewayの間に接続がない場合、テーブルは空になります。



2. **追加**をクリックします。**NetScaler Gatewayサーバーの追加**ダイアログボックスが表示されます。

   NetScaler Gateway 接続チェック(/en-us/citrix-endpoint-management/media/add-gateway-from-connectivity.png)

3. **NetScaler Gateway 管理 IP** に、テストする NetScaler Gateway を実行しているサーバーの管理 IP アドレスを入力します。

   以前に追加済みの NetScaler Gateway サーバーの接続チェックを実行している場合、IP アドレスが提供されます。

4. この NetScaler Gateway の管理者資格情報を入力します。

   以前に追加済みの NetScaler Gateway サーバーの接続チェックを実行している場合、ユーザー名が提供されます。

5. **追加**をクリックします。NetScaler Gateway が、**NetScaler Gateway 接続チェック**ページのテーブルに追加されます。

6. NetScaler Gateway サーバーを選択し、**接続のテスト**をクリックします。結果はテスト結果テーブルに表示されます。

7. テスト結果テーブルでサーバーを選択すると、そのサーバーの詳細な結果が表示されます。

接続チェックの詳細

次の表に、Citrix Endpoint Management が実行できるさまざまな接続チェックと、各チェックの詳細を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

接続先	IP アドレスまたは FQDN	詳細
Apple プッシュ通知サーバー	api.push.apple.com	Apple Push Notification Server と Citrix Endpoint Management ノード間の接続をチェックします。Apple Push Notification Server は、iOS および macOS デバイスにメッセージを送信するために必要です。
Apple フィードバックプッシュ通知サーバー	feedback.push.apple.com	Apple フィードバックサーバーと Citrix Endpoint Management ノード間の接続をチェックします。Apple フィードバックプッシュ通知サーバーは、iOS および macOS デバイスに送信されたリモート通知の失敗に関する情報を提供します。
Citrix ライセンスサーバー	ライセンスサーバーの IP アドレス	Citrix ライセンスサーバーと Citrix Endpoint Management ノード間の接続をチェックします。Citrix 製品を実行しているサーバーは、ライセンスを取得するために Citrix ライセンスサーバーに接続します。
ネットスケーラー ゲートウェイ	Citrix Endpoint Management で構成されている NetScaler Gateway の FQDN	NetScaler Gateway と Citrix Endpoint Management ノード間の接続をチェックします。NetScaler Gateway は、Citrix Endpoint Management クライアントアプリ (Citrix Secure Mail や Citrix Secure Web など) が VPN サーバー経由で内部ネットワークにアクセスするために使用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

接続先	IP アドレスまたは FQDN	詳細
データベース	データベースサーバーの IP アドレスまたは FQDN	Citrix Endpoint Management データベースと Citrix Endpoint Management ノード間の接続をチェックします。
ドメインネームシステム (DNS)	Citrix Endpoint Management で構成されている IP アドレス	DNSサーバーとCitrix Endpoint Managementノード間の接続を確認します。
セキュア チケット オーソリティ サービス	ローカルホスト	Citrix Endpoint Management ノードの認証サービス、STA (Secure Ticket Authority) サービス、およびクラスターサービスへの接続を確認します。
ファイアベース クラウド メッセージング (FCM) サーバー		FCMサーバーとCitrix Endpoint Managementノード間の接続を確認します。FCMを使用すると、新しいメールやその他のデータが同期可能であることをクライアントアプリに通知できます。通知メッセージを送信して、ユーザーエンゲージメントと定着率を高めることができます。FCMはGoogle Cloud Messaging (GCM) の後継です。
グーグルプレイ	play.google.com	Google StoreサーバーとCitrix Endpoint Managementノード間の接続を確認します。Google Playは、管理されたプライベートエンタープライズアプリ配信ストアを含むサービスを提供するために使用されます。
iTunes Store/ボリューム購入	vpp.itunes.apple.com	Apple StoreサーバーとCitrix Endpoint Managementノード

© 1997–2026 Citrix Systems, Inc. All rights reserved.

接続先	IP アドレスまたは FQDN	詳細
		間の接続を確認します。Apple Storeは、管理されたプライベートエンタープライズアプリ配信ストアを含むサービスを提供するために使用されます。
LDAP	Citrix Endpoint Managementで構成されたLDAPのIPアドレスまたはFQDN	LDAPサーバーとCitrix Endpoint Managementノード間の接続を確認します。
Microsoft プッシュ通知サーバー	sin.notifiy.windows.com	Windows Notification Server と Citrix Endpoint Management ノード間の接続をチェックします。Windows Notification Server は、Windows デバイスにメッセージを送信するために使用されます。
ShareFile サービス	Citrix Endpoint Managementで構成されている ShareFile サービスの IP アドレスまたは FQDN	ShareFile サービスと Citrix Endpoint Management 間の接続をチェックします。ShareFile サービスは、企業が大きなファイルを保存および共有するための安全なクラウドベースのプラットフォームです。
Windows デスクトップ/タブレット ストア	windows.microsoft.com	Windows デスクトップ/タブレット ストアと Citrix Endpoint Management ノード間の接続をチェックします。Windows デスクトップ/タブレット ストアは、管理されたプライベートエンタープライズアプリ配信ストアを含むサービスを提供するために使用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

接続先	IP アドレスまたは FQDN	詳細
Windows セキュリティトークンサービス	login.live.com	Windows Security Token Server と Citrix Endpoint Management ノード間の接続をチェックします。Windows Security Token Service は、Windows デバイスの二要素認証（ドメインとセキュリティトークン）をサポートします。

モバイルサービスプロバイダー

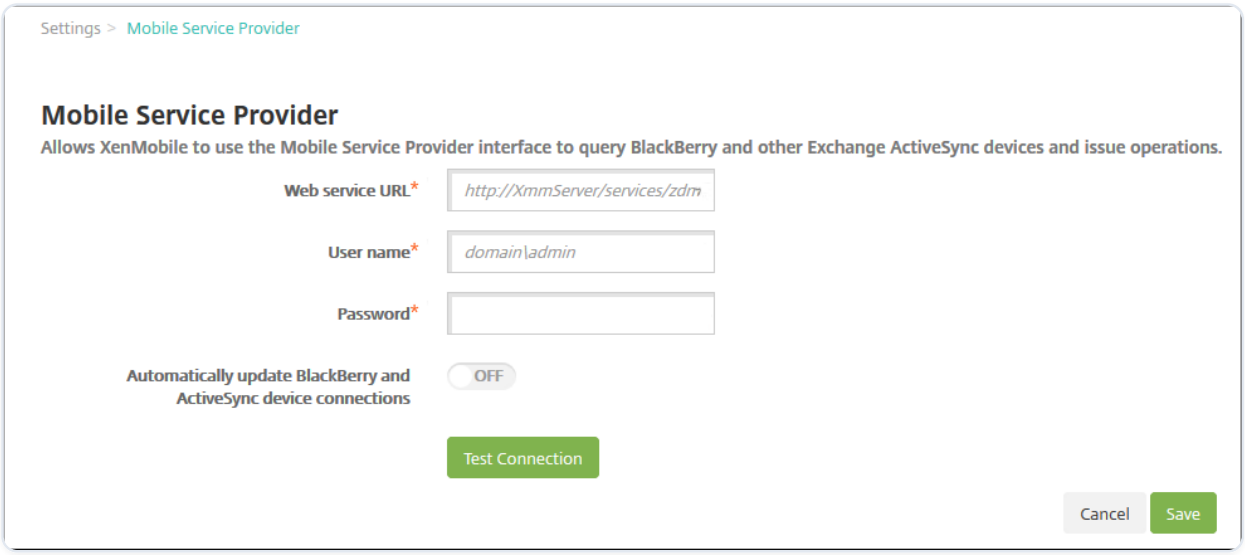
Citrix Endpoint Management でモバイルサービスプロバイダーインターフェイスを使用できるようにして、BlackBerry および Exchange ActiveSync デバイスを照会し、操作を発行できます。

たとえば、組織に 1,000 人のユーザーがいて、各ユーザーが 1 つ以上のデバイスを使用しているとします。すべてのユーザーにデバイスを Citrix Endpoint Management に登録するよう指示した後、Citrix Endpoint Management コンソールには、ユーザーが登録したデバイスの数が表示されます。この設定を構成することで、Exchange Server に接続しているデバイスの数を特定できます。このようにして、次のことができます。

- まだデバイスを登録する必要があるユーザーがいるかどうかを判断する。
- Exchange Server に接続しているユーザーデバイスにコマンドを発行する（データ消去など）。

1. Citrix Endpoint Management コンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **サーバー**の下で、**モバイルサービスプロバイダー**をクリックします。**モバイルサービスプロバイダー**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 次の設定を構成します。

   - **Web サービス URL:** Web サービスの URL を入力します。例: `https://XmmServer/services/xdmservice`。
   - **ユーザー名:** `domain\\admin` の形式でユーザー名を入力します。
   - **パスワード:** パスワードを入力します。
   - **BlackBerry および ActiveSync デバイス接続を自動的に更新:** デバイス接続を自動的に更新するかどうかを選択します。デフォルトは**オフ**です。
   - **接続のテスト**をクリックして接続を確認します。

4. **保存**をクリックします。

レポート

Citrix Endpoint Managementは、アプリとデバイスの展開を分析できる以下の事前定義されたレポートを提供します。各レポートはテーブルとグラフとして表示されます。テーブルは列で並べ替えたりフィルタリングしたりできます。グラフの要素を選択して、より詳細な情報を表示できます。

- **アプリの展開試行合計:** ユーザーがデバイスにインストールしようとした展開済みアプリを一覧表示します。
- **プラットフォーム別アプリ:** デバイスのプラットフォームとバージョン別にアプリとアプリのバージョンを一覧表示します。
- **タイプ別アプリ:** バージョン、タイプ、カテゴリ別にアプリを一覧表示します。
- **デバイス登録:** 登録されているすべてのデバイスを一覧表示します。
- **デバイスとアプリ:** 管理対象アプリを実行しているデバイスを一覧表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **非アクティブなデバイス:** Citrix Endpoint Managementサーバープロパティ `device.inactivity.days.threshold` で指定された日数、アクティビティがなかったデバイスのリスト。
- **ジェイルブレイク/ルート化されたデバイス:** ジェイルブレイクされたiOSデバイスとルート化されたAndroidデバイスを一覧表示します。
- **利用規約:** 利用規約に同意または拒否したユーザーを一覧表示します。グラフの領域を選択して、詳細を表示できます。
- **失敗した展開トップ10:** 展開に失敗したアプリを最大10個一覧表示します。
- **デバイスとユーザー別のブロックされたアプリ**: ユーザーがデバイスに持っているブロックリスト上のアプリを一覧表示します。
- **非準拠デバイス:** コンプライアンス基準を満たさないデバイスを一覧表示します。基準には、デバイスがジェイルブレイクされているか、実行中のOSバージョン、およびデバイスにパスコードがあるかどうかが含まれます。レポートには、デバイスに関連付けられたユーザー名と、デバイスが暗号化されているかどうかも表示されます。iOSデバイスの場合、暗号化列にはN/Aと表示されます。

各テーブルのデータは.csv形式でエクスポートでき、Microsoft Excelなどのプログラムで開くことができます。各レポートのグラフはPDF形式でエクスポートできます。

レポートタブには、シリアル番号、IMEI/MEID、アプリ、接続などのデバイスの詳細が含まれています。特定のデバイスに関するより包括的なレポートについては、**管理 > デバイス**に移動し、そのデバイスをクリックし、**詳細を表示**をクリックして、**デバイスの詳細**ページを表示します。**デバイスの詳細**ページには、デバイスのセキュリティプロパティ、デバイスプロパティ、割り当てられたポリシー、アプリ、アクション、証明書などが一覧表示されます。**デバイスの詳細**ページについては、「デバイスに関する情報を取得する」を参照してください。

Citrix Endpoint Management が管理対象デバイスに展開またはインストールされたアプリに関する情報を収集する方法は、以下の側面によって決定されます。

- デバイスの種類
- 登録方法
- アプリインベントリデバイスポリシー が展開されているかどうか

Android デバイスの場合、動作はデバイスの種類と登録方法によって異なります。以下の表は、**Android Enterprise** のアプリがどこに表示されるか（**デバイスの詳細**ページ、レポート、または利用不可）を示しています。特に指定がない限り、アプリリストにはすべてのアプリが含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	MDM+MAM (すべてのアプリ)	MDM (すべてのアプリ)
必須アプリ（アプリインベントリポリシーが展開されていない場合）	**デバイスの詳細**ページとレポート	パブリックアプリ。**デバイスの詳細**ページとレポート
オプションアプリ（アプリインベントリポリシーが展開されていない場合）	利用不可	利用不可
必須アプリ（アプリインベントリポリシーが展開されている場合）	**デバイスの詳細**ページとレポート	「**デバイスの詳細**」ページおよびレポート
オプションのアプリ (アプリインベントリポリシーが展開されている場合)	エンタープライズ、MDX、パブリック、およびWebリンクアプリ；レポート	「**デバイスの詳細**」ページおよびレポート

次の表は、**Android (レガシーDA)** のアプリがどこに一覧表示されるかを示します (「**デバイスの詳細**」ページ、レポート、または利用不可)。アプリリストには、特に指定がない限り、すべてのアプリが含まれます。

	MDM+MAM (すべてのアプリ)	MDM (パブリックおよびエンタープライズアプリ)	MAM
必須アプリ (アプリインベントリポリシーが展開されていない場合)	「**デバイスの詳細**」ページおよびレポート	「**デバイスの詳細**」ページおよびレポート	N/A
オプションのアプリ (アプリインベントリポリシーが展開されていない場合)	「**デバイスの詳細**」ページおよびレポート	「**デバイスの詳細**」ページおよびレポート	利用不可
必須アプリ（アプリインベントリポリシーが展開されている場合）	**デバイスの詳細**ページとレポート	**デバイスの詳細**ページとレポート	該当なし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	MDM+MAM (すべてのアプリ)	MDM (パブリックおよびエンタープライズアプリ)	MAM
オプションアプリ（アプリインベントリポリシーが展開されている場合）	**デバイスの詳細**ページとレポート	**デバイスの詳細**ページとレポート	利用不可

iOSデバイスの場合、動作は登録方法によって異なります。以下の表は、アプリが一覧表示される場所（**デバイスの詳細**ページまたはレポート）を示しています。特に指定がない限り、アプリリストにはすべてのアプリが含まれます。

	MDM+MAM（すべてのアプリ）	MDM（公開アプリとエンタープライズアプリ）	MAM（すべてのアプリ）
必須アプリ（アプリインベントリポリシーが展開されていない場合）	**デバイスの詳細**ページとレポート	**デバイスの詳細**ページとレポート	**デバイスの詳細**ページとレポート。これらのアプリは、保留状態 (インストールされていない場合でも) で表示されるか、手動でインストールされた後も保留状態のままになります。
オプションアプリ (アプリインベントリポリシーが展開されていない場合)	**デバイスの詳細**ページとレポート	**デバイスの詳細**ページとレポート	Web、SaaS、およびWebリンクアプリは、「**デバイスの詳細**」ページにインストール済みアプリとして表示されます。これらはレポートには表示されません。Enterprise、MDX、およびパブリックアプリは、手動でインストールされた後、「**デバイスの詳細**」ページには表示され

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	MDM+MAM（すべてのアプリ）	MDM（公開アプリとエンタープライズアプリ）	MAM（すべてのアプリ）
			ません。アプリは、手動でインストールされた後、レポートには表示されません。
必須アプリ (アプリインベントリポリシーが展開されている場合)	**デバイスの詳細**ページとレポート	**デバイスの詳細**ページとレポート	アプリインベントリポリシーはデバイスに展開できません。アプリは「**デバイスの詳細**」ページとレポートに表示されます。これらのアプリは、保留状態 (インストールされていない場合でも) で表示されるか、手動でインストールされた後も保留状態のままになります。
オプションアプリ (アプリインベントリポリシーが展開されている場合)	**デバイスの詳細**ページとレポート	**デバイスの詳細**ページとレポート	アプリインベントリポリシーはデバイスに展開できません。Web、SaaS、およびWebリンクアプリは、「**デバイスの詳細**」ページにインストール済みアプリとして表示されます。これらはレポートには表示されません。Enterprise、MDX、およびパブリックアプリは、手動でインストールされた後、「**デバイスの詳細**」ページには表示されません。アプリは、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	MDM+MAM（すべてのアプリ）	MDM（公開アプリとエンタープライズアプリ）	MAM（すべてのアプリ）
			手動でインストールされた後、レポートには表示されません。

macOSおよびWindowsデバイスの場合、Citrix Endpoint Managementは、アプリインベントリポリシーが展開されている場合にのみアプリのインベントリを収集します。

レポートを生成するには

1. Citrix Endpoint Managementコンソールで、**［分析］> ［レポート］** の順にクリックします。**［レポート］** ページが表示されます。
2. 生成するレポートをクリックします。

   レポートの生成(/en-us/citrix-endpoint-management/media/reporting-total-apps.png)

レポートの詳細を表示するには

1. グラフの領域をクリックしてドリルダウンし、詳細情報を表示します。

   レポートの詳細(/en-us/citrix-endpoint-management/media/reporting-total-apps-drilldown.png)

テーブルの列を並べ替え、フィルター、または検索するには、列見出しをクリックします

レポートの列の並べ替え、フィルター、および検索(/en-us/citrix-endpoint-management/media/reporting-click-column-heading.png)

日付でレポートをフィルターするには

1. 列見出しをクリックして、フィルター設定を表示します。

   日付によるレポートのフィルター(/en-us/citrix-endpoint-management/media/analyze-reporting-date-filter.png)
2. **［フィルター条件］** から、レポートされる日付を制限する方法を選択します。

   日付によるレポートのフィルター(/en-us/citrix-endpoint-management/media/analyze-reporting-date-filter-condition.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 日付選択ツールを使用して日付を指定します。

   日付でレポートをフィルタリング(/en-us/citrix-endpoint-management/media/analyze-reporting-date-filter-choose-date.png)

4. 日付フィルターのある列は、次の例に示すように表示されます。

   日付でレポートをフィルタリング(/en-us/citrix-endpoint-management/media/analyze-reporting-date-filter-indicator.png)

5. フィルターを削除するには、列ヘッダーをクリックし、次に**フィルターを削除**をクリックします。

   フィルターの削除(/en-us/citrix-endpoint-management/media/analyze-reporting-date-filter-remove.png)

グラフまたはテーブルをエクスポートするには

- グラフをPDF形式でエクスポートするには、**アクション**をクリックし、次に**グラフをPDFとしてエクスポート**をクリックします。
- テーブルデータをCSV形式でエクスポートするには、**アクション**をクリックし、次に**データをCVSとしてエクスポート**をクリックします。

グラフまたはテーブルのエクスポート(/en-us/citrix-endpoint-management/media/reporting-export-snip.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REST API

Citrix Endpoint Management REST API を使用すると、次のことができます。

- Citrix Endpoint Management コンソールに表示されるサービスを呼び出す
- 任意の REST クライアントを使用して REST サービスを呼び出す

API は、サービスを呼び出すために Citrix Endpoint Management コンソールにサインオンする必要はありません。

利用可能な API の完全な現在のセットについては、REST サービス用パブリック API PDF をダウンロードしてください。

モバイルおよびデスクトップのエンドポイントデバイスを管理し、Workspace apps の設定を構成するための API が利用可能です。`<https://developer.cloud.com/citrixworkspace>` にアクセスし、**Citrix Endpoint Management > Mobile Application Integration** に移動してください。

REST API にアクセスするために必要な権限

REST API へのアクセスには、次のいずれかの権限が必要です。

- Citrix Cloud 管理者
- ロールベースのアクセス構成の一部として設定されたパブリック API アクセス権限。詳細については、RBAC を使用したロールの構成 を参照してください。
- スーパーユーザー権限

Citrix Cloud アカウントを使用して REST API にアクセスするには、**API** キーを生成します。

1. Citrix Cloud メニューから、**Identity and Access Management** を選択します。
2. **API Access > Secure Clients** を選択します。
3. セキュアクライアントの名前を入力し、「**クライアントの作成**」をクリックします。

Citrix Cloudは、セキュアクライアントIDとクライアントシークレットを作成します。この情報のコピーをダウンロードし、参照用に安全なオフライン環境に保存してください。ダイアログボックスを閉じると、Citrix Cloudは一意の識別子を保存しません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REST APIサービスを呼び出すには

RESTクライアントまたはcURLコマンドを使用して、REST APIサービスを呼び出すことができます。次の例では、Chrome用のAdvanced RESTクライアントを使用しています。

注：

次の例では、ホスト名とポート番号を環境に合わせて変更してください。

ログイン

ここに示されている例では、Citrix Cloud APIを介して取得したトークンを使用してログインする方法について説明します。

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login/cloud`

メソッドタイプ: POST

コンテンツタイプ: application/json

リクエストの例:

```
{

 "bearerToken":
"eyJ0eOiJSUzJiibGcI1AiONiJ9.eyJkIjoMDExN1c2VIXiMzNDc1OTk4...qf0iQ"

}
```

Citrix Cloud API `https://trust.citrixworkspacesapi.net/Help/Api/POST-customer-tokens-clients` を使用してベアラートークンを取得する必要があります。詳細については、開発者向けドキュメント を参照してください。

レスポンスの例:

```
{

 "auth_token": "q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

関連情報

- シトリックス エンドポイント マネジメント REST API

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メールアクセス制限

ActiveSync ゲートウェイ

ActiveSyncは、Microsoftが開発したモバイルデータ同期プロトコルです。ActiveSyncは、ハンドヘルドデバイスとデスクトップ（またはラップトップ）コンピューター間でデータを同期します。

Citrix Endpoint ManagementでActiveSync Gatewayルールを構成できます。ActiveSync Gatewayは、Citrix Endpoint Managementで構成されているすべてのデバイスのActiveSync IDのリストを保持します。構成したルールに基づいて、これらのActiveSync IDに基づいて、デバイスのActiveSyncデータへのアクセスを許可または拒否できます。たとえば、**必要なアプリの不足**ルールをアクティブ化すると、Citrix Endpoint Managementは必要なアプリのアプリアクセスポリシーをチェックします。必要なアプリが見つからない場合、ポリシーはActiveSyncデータへのアクセスを拒否します。各ルールについて、**許可**または**拒否**のいずれかを選択できます。デフォルト設定は**許可**に設定されています。

アプリアクセスデバイスポリシーについて詳しくは、「アプリアクセスデバイスポリシー」を参照してください。

Citrix Endpoint Managementは、次のルールをサポートしています。

匿名デバイス： デバイスが匿名モードであるかどうかを確認します。このチェックは、デバイスが再接続しようとしたときにCitrix Endpoint Managementがユーザーを再認証できない場合に利用できます。

禁止アプリ： アプリアクセスポリシーで定義されている禁止アプリがデバイスにあるかどうかを確認します。

暗黙的な許可と拒否： このアクションは、ActiveSync Gatewayのデフォルトです。ゲートウェイは、他のどのフィルター条件も満たさないすべてのデバイスのデバイスリストを作成します。その後、ゲートウェイはそのリストに基づいて接続を許可または拒否します。ルールが一致しない場合、デフォルトは**暗黙的な許可**に設定されます。

非アクティブなデバイス： サーバープロパティの**デバイス非アクティブ日数しきい値**設定で定義されているように、デバイスが非アクティブであるかどうかを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

必要なアプリの不足： アプリアクセスポリシーで定義されているように、デバイスに必要なアプリが不足しているかどうかを確認します。

推奨されないアプリ： アプリアクセスポリシーで定義されているように、デバイスに推奨されないアプリがあるかどうかを確認します。

非準拠パスワード： ユーザーパスワードが準拠しているかどうかを確認します。iOSおよびAndroidデバイスでは、Citrix Endpoint Managementは、デバイスに現在設定されているパスワードが、デバイスに送信されたパスコードポリシーに準拠しているかどうかを判断できます。たとえば、iOSでは、Citrix Endpoint Managementがパスコードポリシーをデバイスに送信した場合、ユーザーは60分以内にパスワードを設定する必要があります。ユーザーがパスワードを設定する前は、パスコードが非準拠である可能性があります。

非準拠デバイス： 非準拠デバイスプロパティに基づいて、デバイスが非準拠であるかどうかを確認します。通常、自動アクションまたはCitrix Endpoint Management APIを使用するサードパーティがこのプロパティを変更します。

失効ステータス： デバイス証明書が失効しているかどうかを確認します。失効したデバイスは、再度承認されるまで再登録できません。

ルート化されたAndroidおよびジェイルブレイクされたiOSデバイス： AndroidまたはiOSデバイスがジェイルブレイクされているかどうかを確認します。

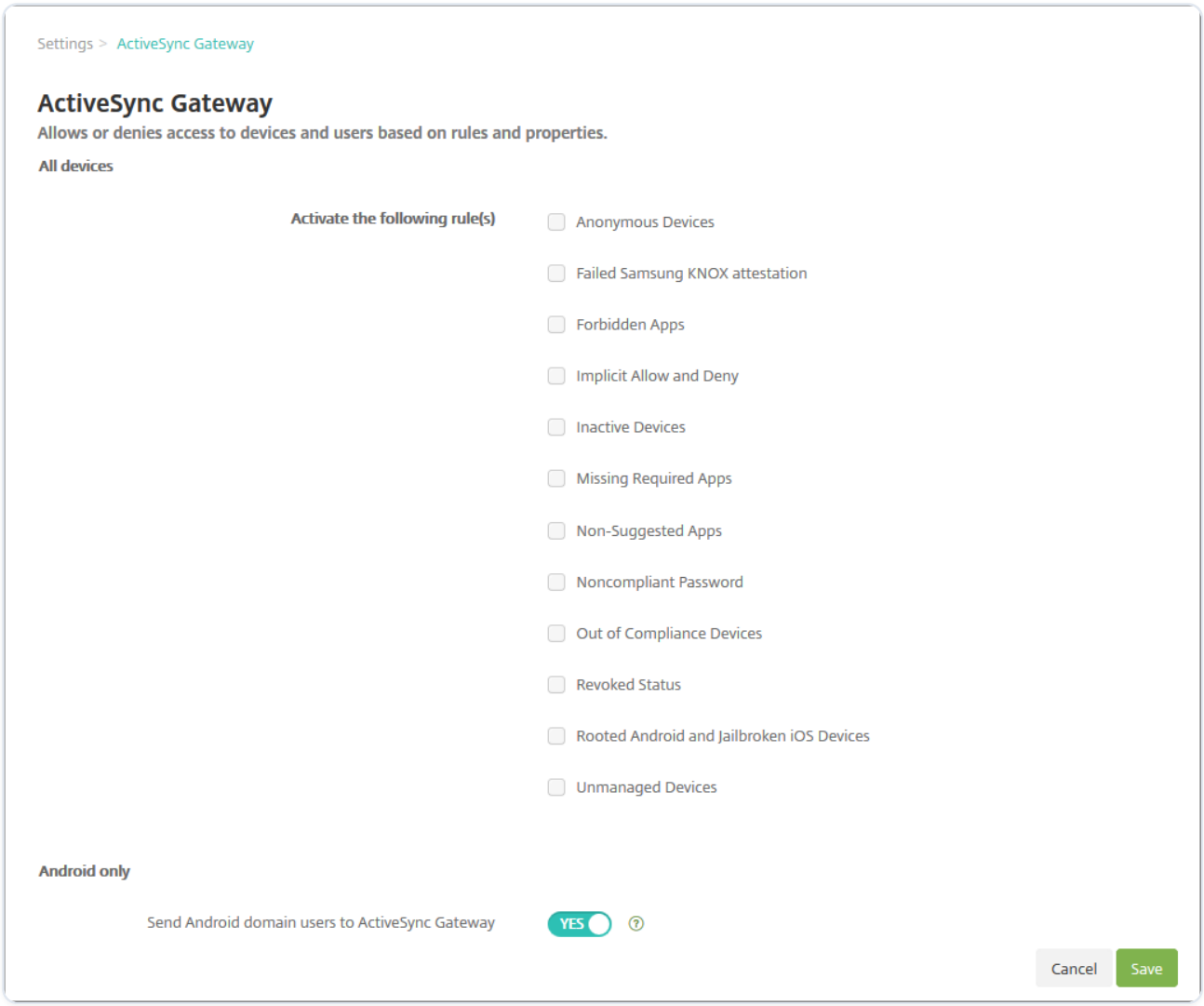
管理対象外デバイス: デバイスがCitrix Endpoint Managementによって制御される管理状態にあるかどうかを確認します。たとえば、MAMに登録されているデバイスや登録解除されたデバイスは管理対象ではありません。

AndroidドメインユーザーをActiveSync Gatewayに送信: はいをクリックすると、Citrix Endpoint ManagementがAndroidデバイス所有者のユーザー名とActiveSync IDをActiveSync Gatewayに送信するようになります。レガシー構成を実行している場合を除き、この機能をオフにしてください。より新しい構成では、この機能により、デバイスに関連付けられたユーザー名がGatewayに存在するかぎり、どのデバイスでもActiveSyncデータにアクセスできるようになります。

ActiveSync Gateway設定を構成するには

1. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **サーバー**で、**ActiveSync Gateway**をクリックします。**ActiveSync Gateway**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. **次のルールをアクティブ化**で、アクティブ化するルールを1つ以上選択します。
2. **AndroidのみのAndroidドメインユーザーをActiveSync Gatewayに送信**で、**はい**をクリックして、Citrix Endpoint ManagementがAndroidデバイス情報をActiveSync Gatewayに送信するようにします。
3. **保存**をクリックします。

エクスチェンジ アクティブシンク 用 シトリックス エンドポイント マネジメント コネクタ

XenMobile Mail Manager は、Exchange ActiveSync 用 Citrix Endpoint Management コネクタになりました。Citrix の統合ポートフォリオの詳細については、Citrix 製品ガイドを参照してください。

このコネクタは、Citrix Endpoint Management の機能を次の方法で拡張します。

- Exchange Active Sync (EAS) デバイスの動的アクセス制御。EAS デバイスは、Exchange サービスへのアクセスを自動的に許可またはブロックできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Management が Exchange によって提供される EAS デバイスのパートナーシップ情報にアクセスする機能。
- Citrix Endpoint Management が EAS ステータスに基づいてモバイルデバイスをワイプする機能。
- Citrix Endpoint Management が Blackberry デバイスに関する情報にアクセスし、ワイプやパスワードのリセットなどの制御操作を実行する機能。

EAS ステータスに基づいてデバイスをワイプするには、ActiveSync トリガーを使用して自動アクションを構成します。自動アクションを参照してください。

重要：

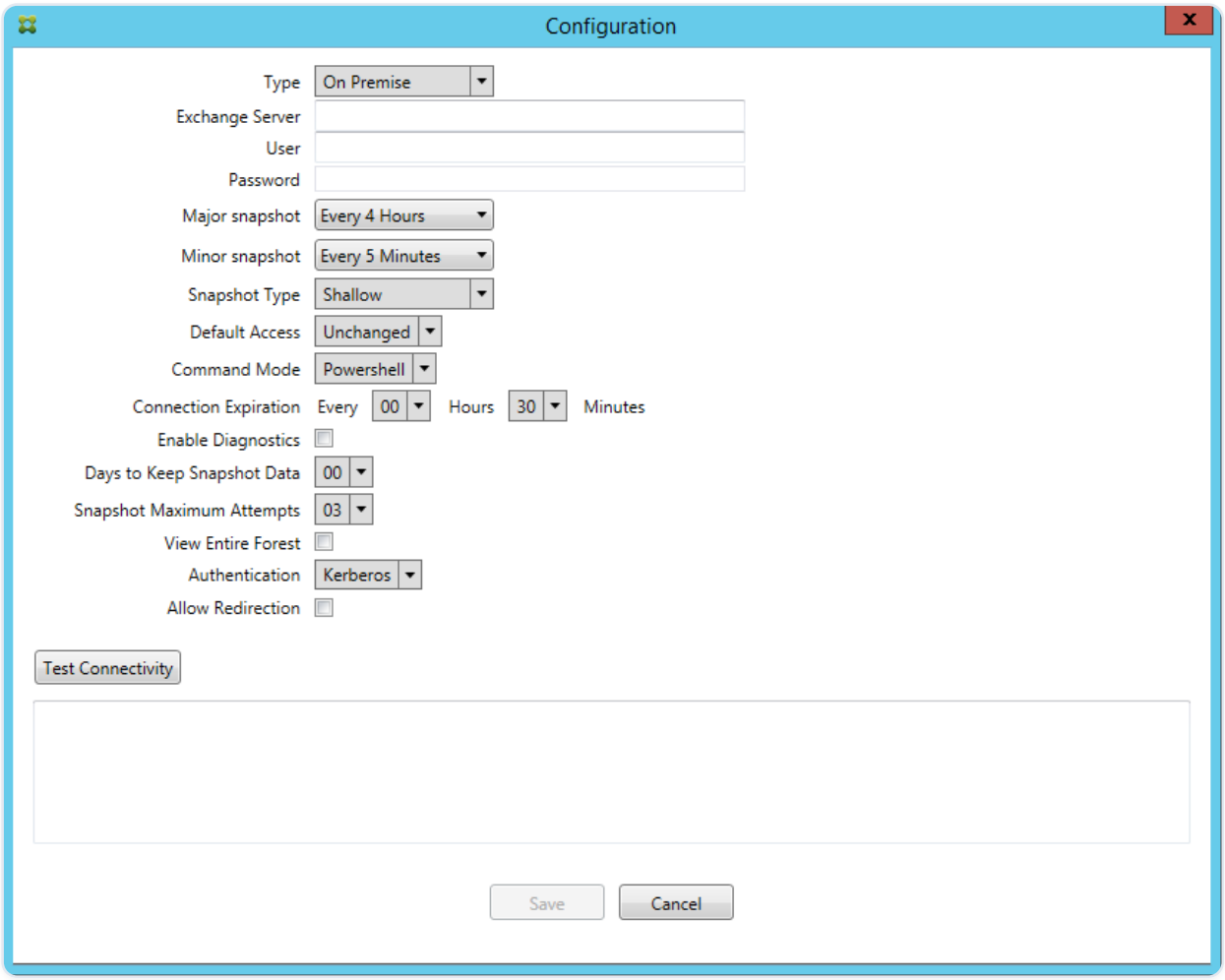
2022 年 10 月以降、Microsoft がこちらで発表した認証の変更により、Exchange ActiveSync 用の Citrix Endpoint Management および NetScaler Gateway コネクタは Exchange Online をサポートしなくなりました。Exchange 用 Citrix Endpoint Management コネクタは、Microsoft Exchange Server (オンプレミス) で引き続き動作します。

バージョン 10.1.10 の新機能

バージョン 10.1.10 では、以下の問題が修正されています。

- 頻繁にネットワークの問題が発生するお客様は、以前提供されていた 3 回の試行でスナップショットを完了できない場合があります。このリリースでは、管理者が最大試行回数 (1 ～ 10 回) を構成できます。この修正により、スナップショットプロセスを完全に中断することなく、通信の複数の切断が発生してもスナップショットを続行できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 以前のバージョンでは、スナップショットタイプが Exchange 構成のリストに表示されませんでした。今回のバージョンでは、スナップショットタイプが表示されるようになりました。
- PowerShell によって報告される PSRemotingTransport 例外は、Exchange へのセッションがもはや有効ではないことを示します。このステータスは、デフォルトで構成ファイルのクリティカルエラーリストに追加されます。これにより、PSRemotingTransportException が検出されると、接続は後で破棄するためにエラーとしてマークされます。次の通信では、有効な接続を使用するか、新しい接続を作成します。
- 構成変更が保存されると、新しい構成をロードする前に、以前に構成されたすべての内部コンポーネントが適切に破棄されなかった可能性があります。この問題は、予測できない動作につながる可能性があります。動作は、特定の変更と、その変更が以前の構成と競合したかどうかに依存します。このリリースでは、新しい構成をロードする前にすべての内部コンポーネントが破棄されます。

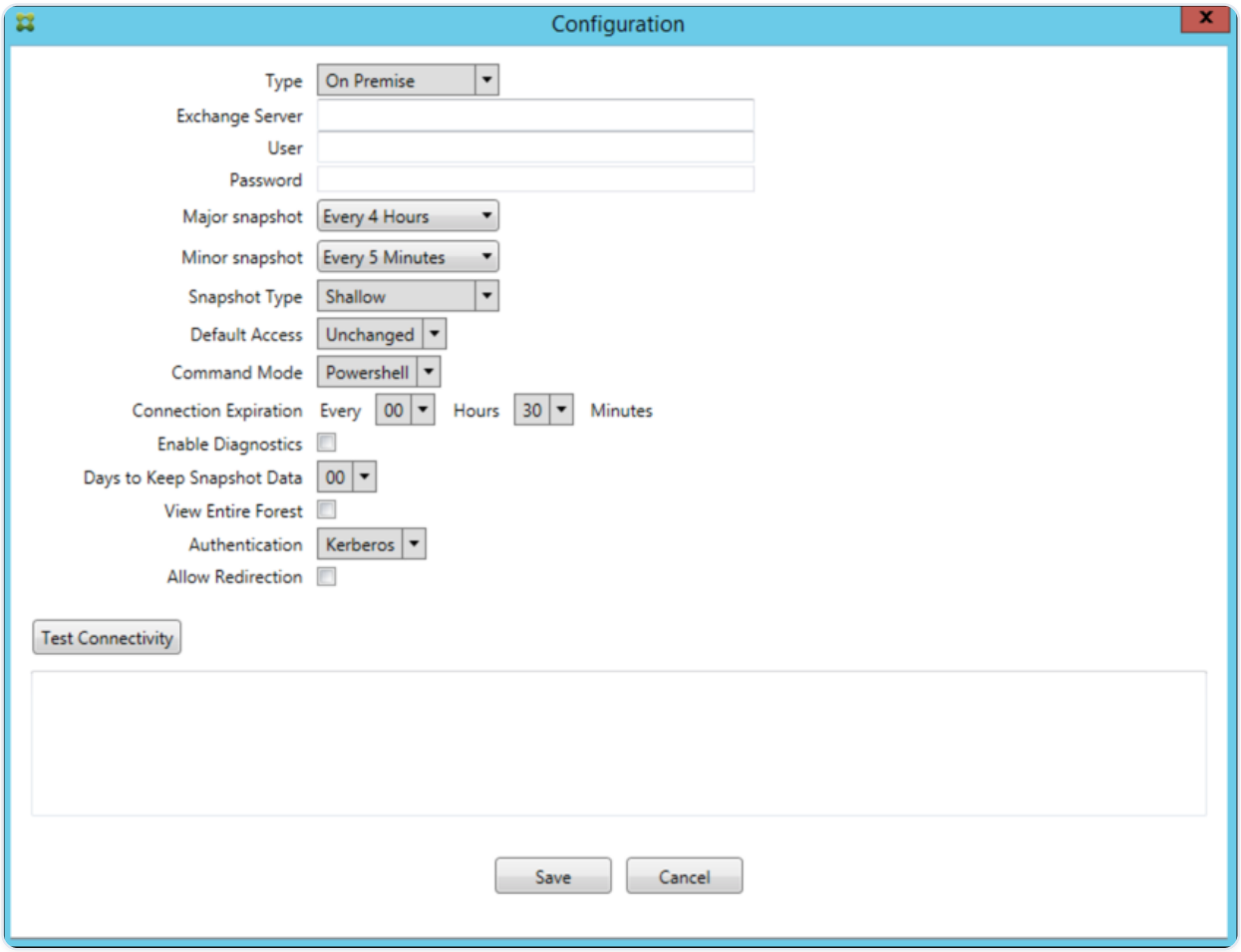
バージョン10.1.9の新機能

バージョン10.1.9で修正された問題は次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 構成変更は、より一貫した方法で処理されるようになりました。サービスが構成の変更を検出すると、各内部サブシステムが停止され、アクティブまたはスケジュールされた処理が中断されます。次に、新しい構成がロードされ、サブシステムが再度開始されます。これにより、すべてのスケジュールとその他の内部インフラストラクチャが新しい設定で再確立されます。この問題は、バージョン10.1.8の既知の問題を修正します。
- アップグレード中に、既存のデータベース構成が新しい構成ファイルにマージされませんでした。データベース構成は、アップグレードされた構成ファイルにマージされるようになりました。
- スナップショット関連の診断ファイルで、列ヘッダーが欠落していました。ヘッダーは復元されました。
- 以前のバージョンからアップグレードする際、構成ファイルのデフォルトセクションが、使用中の構成ファイルの類似セクションによって上書きされていました。この問題により、アップグレード後にデフォルトセクションへの追加や改善がサービスによってロードされなくなっていました。このバージョン以降、デフォルトセクションは常に最新の構成を反映します。
- 管理者は、アプリケーションの実行中にShiftキーを押しても特定のオプションにアクセスできなくなりました。これらのオプションは以前、Citrix®の許可があれば利用可能でした。一部のオプション（「リダイレクトを許可」など）は完全に利用可能になり、その他のオプション（「ハング検出」や「カウント修正」など）は非推奨になりました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



以前のバージョンの新機能

次のセクションでは、以前のバージョンのCitrix Endpoint Management connector for Exchange ActiveSyncの新機能と修正された問題について説明します。

バージョン10.1.8の新機能

- Exchangeが、Exchange ActiveSyncサービス用のCitrix Endpoint Managementコネクタがコマンドを頻繁に発行しすぎないようにスロットリングする可能性があります。この問題は、Office 365への接続でよく発生します。スロットリングの影響により、サービスは次のコマンドを送信する前に指定された期間一時停止する必要があります。Configureコンソールに、一時停止の残り時間が表示されるようになりました。
- 構成ファイル (config.xml) の「Watchdog」セクションおよび/または「SpecialistsDefaults」セクションに変更が加えられても、アップグレード後にその変更が構成ファイルに反映されませんでした。このリリースでは、変更が新しい構成ファイルに正しくマージされるようになりました。
- Google Analyticsに送信される分析情報に、特にスナップショットに関する詳細が追加されました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Exchangeの接続テスト機能は、接続を一度だけ初期化しようとします。Office 365の接続はスロットリングされる可能性があるため、スロットリング時に接続テストが失敗したように見えることがありました。Citrix Endpoint Management connector for Exchange ActiveSyncは、接続を最大3回試行するようになりました。
- Exchangeでポリシーを適用するには、Citrix Endpoint Management connector for Exchange ActiveSyncが、各メールボックスに関連するすべてのデバイスを許可リストとブロックリストの2つのリストに含める**Set-CASMailbox**コマンドをコンパイルする必要があります。デバイスがどちらのリストにも含まれていない場合、Exchangeはデフォルトのアクセス状態に戻ります。そのデフォルトのアクセス状態がデバイスの望ましい状態と異なる場合、そのデバイスはコンプライアンス違反になります。したがって、Exchangeのデフォルトのアクセス状態がブロックされており、許可されるべきである場合、ユーザーはメールへのアクセスを失う可能性があります。または、メールへのアクセスがブロックされるべきユーザーがアクセスを許可される可能性があります。Citrix Endpoint Management connector for Exchange ActiveSyncは、有効な望ましい状態を持つすべてのデバイスが各**Set-CasMailbox**コマンドに含まれるようにします。

バージョン10.1.8で以下の問題が確認されています。

管理者が構成データを変更するConfigureアプリケーションで変更を行う際に、サービスがスナップショットやポリシー評価などの長時間にわたる操作を実行していると、サービスが不定状態になることがあります。考えられる症状としては、ポリシーの変更が処理されない、またはスナップショットが開始されないなどがあります。サービスを動作状態に戻すには、サービスを再起動する必要があります。サービスを開始する前に、Windowsサービスマネージャーを使用してサービスプロセスを終了する必要がある場合があります。

バージョン10.1.7の新機能

- XenMobile Mail Manager は、Citrix Endpoint Management の Exchange ActiveSync 用コネクタとなりました。
- Exchange構成ダイアログボックスの**Disable Pipelining**オプションは非推奨になりました。config.xmlファイルで各コマンドに複数のステップを設定することで、同じ機能を実現できます。

バージョン10.1.7で以下の問題が修正されました。

- スナップショット履歴ウィンドウでは、エラーメッセージがほとんどコンテキストなしで表示されることがありました。現在では、エラーメッセージには発生した場所のコンテキストがプレフィックスとして付加されます。
- XmmGoogleAnalytics .dllには、リリースに対応するファイルバージョンがありませんでした。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 診断を改善するため、メールボックスの許可/ブロック状態を設定するために使用されるデバイスIDのリストの文字列形式を最近変更しました。しかし、あまりにも多くのデバイスを指定すると、最大文字列サイズを超えてしまいました。現在では、内部配列データ構造を使用しています。この構造にはサイズ制限がなく、診断目的にも適切にデータをフォーマットします。
- Exchangeと同期していないデバイスポリシーが検出された場合、そのコマンドには関連するメールボックスに属さないデバイスが含まれることがあります。Citrix Endpoint Management connector for Exchange ActiveSyncは、Exchangeへのコマンドがそれぞれのメールボックスに属するデバイスのみを表すようにします。
- 一部の環境では、Microsoftアセンブリが利用できませんでした。必要なアセンブリは、アプリケーションとともに明示的にインストールされるようになりました。
- デバイスまたはメールボックスの識別名（Distinguished Names）に、属性名と等号の間にスペースがある場合、または等号の後と値の前にスペースがある場合、Citrix Endpoint Management connector for Exchange ActiveSyncはデバイスとそのメールボックスを適切に照合できない、またはその逆の状況が発生する可能性があります。その結果、スナップショットの調整中に一部のデバイスやメールボックスが拒否される可能性があります。

注:

以下の「新機能」セクションでは、Citrix Endpoint Management connector for Exchange ActiveSyncを旧称のXenMobile Mail Managerとして参照しています。名称はバージョン10.1.7から変更されました。

バージョン10.1.6.20での更新

10.1.6への更新には、バージョン10.1.6.20で以下の修正が含まれています。

- Exchangeと同期していないデバイスポリシーが検出された場合、そのコマンドには、関連するメールボックスに属さないデバイスが含まれることがあります。XenMobile® Mail Managerは、Exchangeへのコマンドがそれぞれのメールボックスに属するデバイスのみを表すようにします。

バージョン10.1.6の新機能

XenMobile Mail Managerバージョン10.1.6には、以下の修正された問題と機能強化が含まれています。

- スナップショット履歴ウィンドウが、時として更新されなくなる状態になることがあります。ウィンドウの更新メカニズムが改善され、より確実に更新されるようになりました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- パーティション化されたスナップショットとパーティション化されていないスナップショットには、2つの異なるモードとコードパスが使用されていました。パーティション化されていないスナップショットは、単一の「*」パーティションを使用する構成のパーティション化されたスナップショットと同等であるため、パーティション化されていないスナップショットモードは廃止されました。デフォルトのスナップショットモードは、36個のパーティション（0〜9、A〜Z）を持つパーティション化されたスナップショットになりました。
- スナップショット履歴ウィンドウでは、エラーメッセージがステータスメッセージによって上書きされていました。現在、XenMobile Mail Managerは2つの別々のフィールドを提供し、ユーザーがステータスとエラーを同時に表示できるようにしています。
- Exchange Online (Office 365) に接続すると、スナップショット関連のクエリによってデータセットが切り詰められる可能性があります。この問題は、XenMobile Mail Managerがマルチコマンドパイプラインスクリプトを実行するときに発生する可能性があります。アップストリームコマンドがダウンストリームコマンドにデータを十分に速く渡すことができず、ダウンストリームコマンドが時期尚早に作業を完了してしまいます。その結果、不完全なデータが発生します。XenMobile Mail Managerは、パイプライン自体を模倣し、アップストリームコマンドが完了するまで待ってからダウンストリームコマンドを呼び出すことができるようになりました。この変更により、すべてのデータが処理およびキャプチャされるはずです。
- Exchangeへのポリシー更新コマンドで解決不能なエラーが発生した場合、同じコマンドが長期間にわたって繰り返しワークキューに戻されます。この状況により、コマンドが何度もExchangeに送信されていました。このバージョンのXenMobile Mail Managerでは、エラーが発生したコマンドは、ワークキューに特定の回数だけ戻されるようになりました。
- 特定のメールボックスに対するポリシー更新で、すべてのデバイスの許可またはブロックが含まれる場合、発行された **Set-CASMailbox** コマンドは、空のリストが **NULL** ではなく空の文字列に変換されるため、失敗していました。適切なデータが送信されるようになりました。
- 新しいデバイスを処理する際、Exchangeはしばらくの間（通常15分間）状態を「DeviceDiscovery」として返すことがあります。XenMobile Mail Managerはこの状態を特別に処理していませんでした。XenMobile Mail Managerはこの状態を処理するようになりました。UIの監視タブで、ユーザーはこの状態のデバイスをフィルタリングできます。
- XenMobile Mail Managerは、XenMobile Mail Managerデータベースへの書き込み権限をチェックしていませんでした。そのため、権限が制限されている場合、動作が予測できない可能性がありました。XenMobile Mail Managerは、データベースから必要な権限を取得し、検証するようになりました。XenMobile Mail Managerは、接続テスト時（メッセージが表示されます）またはメインの構成ウィンドウの下部にあるデータベースインジケーター（メッセージを表示するにはホバーします）で、権限が削減されていることを示します。
- 現在のワークロードによっては、指示されたときにXenMobile Mail Managerサービスがすぐに停止しない場合があります。そのため、サービスが応答しない状態に見えることがあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

改善により、進行中のタスクを中断できるようになり、より正常なシャットダウンが可能になりました。

バージョン 10.1.5 の新機能

XenMobile Mail Manager バージョン 10.1.5 では、以下の問題が修正されています。

- Exchange が XenMobile Mail Manager のアクティビティにスロットリングを適用している場合、スロットリングが発生していることを示す表示 (ログ以外) はありません。このリリースでは、ユーザーがアクティブなスナップショットにカーソルを合わせると、「スロットリング」状態が表示されます。また、XenMobile Mail Manager がスロットリングされている間は、Exchange がスロットリングの制限を解除するまで、メジャースナップショットの開始は禁止されます。
- メジャースナップショット中に XenMobile Mail Manager が Exchange によってスロットリングされている場合、次のスナップショット試行を実行するまでに十分な時間が経過しない可能性があります。この問題により、さらにスロットリングが発生し、スナップショットが失敗します。XenMobile Mail Manager は、スナップショット試行間の待機時間として Exchange が指定する最小時間だけ待機するようになりました。
- 診断が有効になっている場合、コマンドファイルには、各プロパティ名の前にハイフンが欠落している **Set-CasMailbox** コマンドが表示されます。この問題は、診断ファイルのフォーマットでのみ発生し、Exchange への実際のコマンドでは発生しません。ハイフンが欠落していると、ユーザーはコマンドを切り取って PowerShell プロンプトに直接貼り付けてテストや検証を行うことができません。ハイフンが追加されました。
- メールボックスのIDが `lastname, firstname` の形式である場合、Exchange はクエリからデータを返すときにコンマの前にバックスラッシュを追加します。XenMobile Mail Manager がそのIDを使用してさらにデータをクエリする場合、このバックスラッシュは削除する必要があります。

既知の制限事項

注:

以下の制限事項はバージョン 10.1.6 で解決されています。

XenMobile Mail Manager には、Exchange へのコマンドが失敗する可能性がある既知の制限事項があります。Exchange にポリシー変更を適用するために、XenMobile Mail Manager によって **Set_CASMailbox** コマンドが発行されます。このコマンドは、2つのデバイスリスト（許可するリ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ストとブロックするリスト）を受け取ることができます。このコマンドは、メールボックスと連携しているデバイスに適用されます。

これらのリストは、Microsoft API によってそれぞれ256文字に制限されています。これらのリストのいずれかが制限を超えると、コマンド全体が失敗し、そのメールボックスのデバイスに対するポリシーが設定されなくなります。XenMobile Mail Manager のログに表示されるエラーは、次のようになります。この例はブロックされたリストに関するものです。

“メッセージ:'パラメーター 'ActiveSyncBlockedDeviceIDs' をターゲットにバインドできません。"ActiveSyncBlockedDeviceIDs" の設定中に例外が発生しました: "プロパティの長さが長すぎます。最大長は 256 で、指定された値の長さは…"

デバイスIDの長さは異なる場合がありますが、同時に許可またはブロックされるデバイスが約10台以上になると、制限を超える可能性があるという目安があります。特定のメールボックスにこれほど多くのデバイスが関連付けられていることは稀ですが、可能性はあります。このようなシナリオを処理できるように Mail Manager が改善されるまで、ユーザーとメールボックスに関連付けられるデバイスの数を10台以下に制限することをお勧めします。

バージョン 10.1.4 の新機能

XenMobile Mail Manager バージョン 10.1.4 では、以下の問題が修正されています。

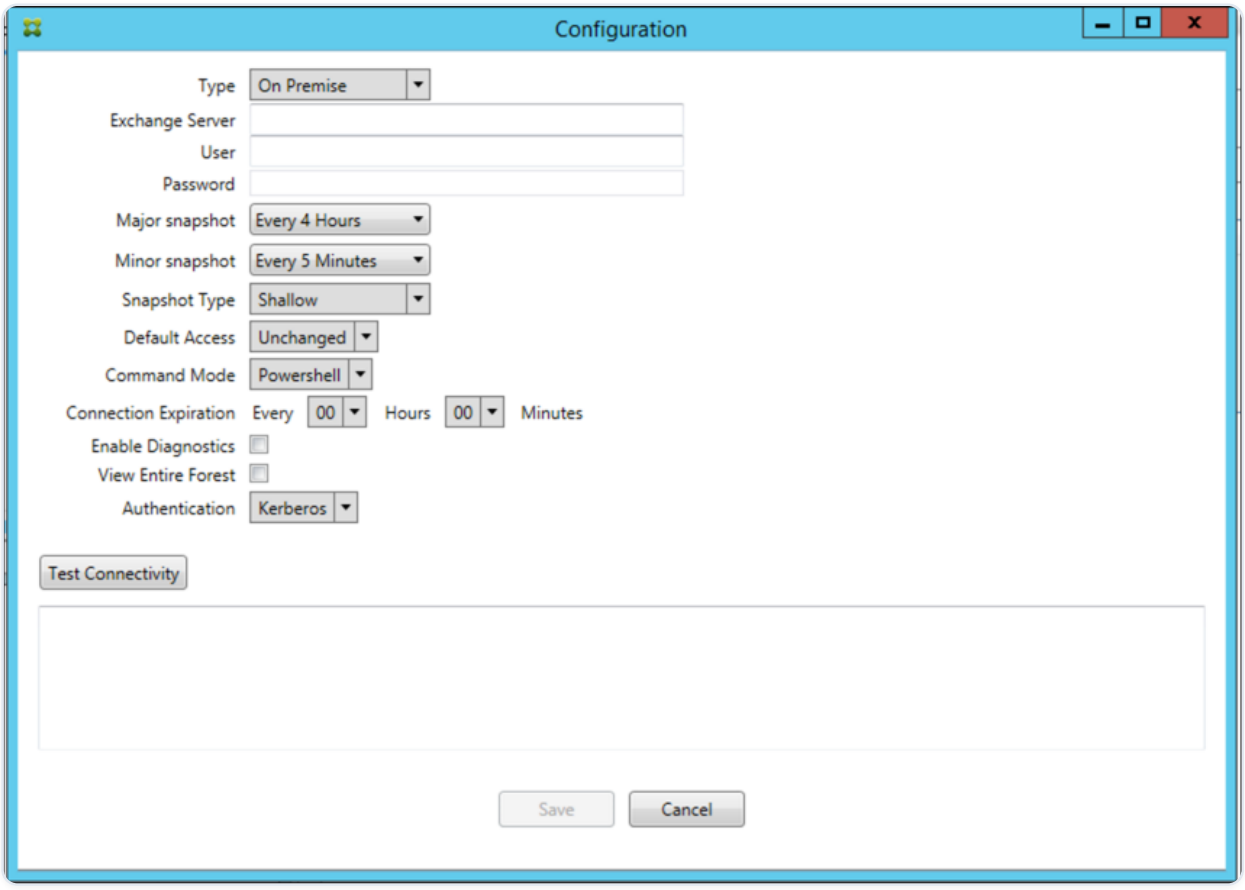
- セキュリティの脆弱化のため、PCI Council は TLS 1.0 および TLS 1.1 を非推奨にしています。XenMobile Mail Manager に 1.2 のサポートが追加されました。
- XenMobile Mail Manager には新しい診断ファイルが含まれています。Exchange の仕様で が選択されている場合、新しいスナップショット履歴ファイルが生成されます。スナップショットの試行ごとに、スナップショットの結果がファイルに行として追加されます。
- コマンド診断ファイルでは、**Set-CASMailbox** コマンドに対して許可またはブロックされたデバイスのリストが表示されませんでした。代わりに、関連する引数に対して内部クラス名がファイルに表示されていました。XenMobile Mail Manager は、デバイス ID のリストをコンマ区切りのリストとして表示するようになりました。
- 不適切な仕様が原因で Exchange への接続の取得に失敗した場合、「すべての接続が使用中です」という誤ったメッセージがエラーメッセージを上書きしていました。現在では、「すべての接続が動作不能です」、「接続プールが空です」、「すべての接続がスロットルされています」、「利用可能な接続がありません」などの、より詳細なメッセージが表示されるようになりました。
- 許可/ブロック/ワイプコマンドが XenMobile Mail Manager の内部キャッシュに複数回キューイングされることがあります。この問題により、コマンドが Exchange に送信されるのが遅延し

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ます。XenMobile Mail Manager は、各コマンドのインスタンスを 1 つだけキューイングするようになりました。

バージョン 10.1.3 の新機能

- **Google Analytics のサポート:** XenMobile Mail Manager の使用状況を把握し、製品を改善できる点に注力したいと考えています。
- **診断を有効にする設定:** ダイアログボックスの構成コンソールに チェックボックスが表示されます。



バージョン 10.1.3 で修正された問題

- ウィンドウで、スナップショットの現在の状態を示すツールヒントが実際の状態を反映していません。 まれに、XenMobile Mail Manager がコマンド診断ファイルに書き込めないことがあります。この場合、コマンド履歴が完全にログに記録されません。
- 接続でエラーが発生した場合、その接続が「エラー状態」としてマークされないことがあります。その結果、後続のコマンドがその接続を使用しようとして、別のエラーを引き起こす可能性があります。
- Exchange Server からのスロットリングが発生すると、Check Health ルーチンで例外がスローされることがあります。その結果、エラーが発生した接続や期限切れになった接続がパージさ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

れない可能性があります。また、XenMobile Mail Manager は、スロットリング時間が期限切れになるまで接続を作成しない場合があります。.

- Exchange の最大セッション数を超過すると、XenMobile Mail Manager は「デバイスキャプチャに失敗しました」というエラーを報告しますが、これは正確なメッセージではありません。代わりに、XenMobile Mail Manager が通常 Exchange 通信に使用する 2 つのセッションが使用中であることを示すメッセージが表示されるべきです。

バージョン 10.1.2 の新機能

- **Exchange への接続の改善:** XenMobile Mail Manager は、Exchange と通信するために PowerShell セッションを使用します。PowerShell セッションは、特に Office 365 を扱う場合、しばらくすると不安定になり、その後のコマンドの成功を妨げる可能性があります。XenMobile Mail Manager は、接続の有効期限を設定できるようになりました。接続が有効期限に達すると、XenMobile Mail Manager は PowerShell セッションを正常にシャットダウンし、新しいセッションを作成します。これにより、PowerShell セッションが不安定になる可能性が低くなり、スナップショットの失敗の可能性が大幅に減少します。
- **スナップショットワークフローの改善:** メジャーなスナップショットは、時間とプロセスを大量に消費する操作です。スナップショット中にエラーが発生した場合、XenMobile Mail Manager はスナップショットを完了するために複数回（最大3回）試行するようになりました。その後の試行は最初から開始されません。XenMobile Mail Manager は中断したところから続行します。この機能強化により、スナップショットの進行中に一時的なエラーを許容することで、スナップショット全体の成功率が向上します。
- **診断機能の改善:** スナップショット中にオプションで生成される3つの新しい診断ファイルにより、スナップショット操作のトラブルシューティングが容易になりました。これらのファイルは、PowerShell コマンドの問題、情報が不足しているメールボックス、およびメールボックスに関連付けられないデバイスの特定に役立ちます。管理者はこれらのファイルを使用して、Exchange で正しくない可能性のあるデータを特定できます。
- **メモリ使用量の改善:** XenMobile Mail Manager は、メモリの使用においてより効率的になりました。管理者は、システムをクリーンな状態にするために、XenMobile Mail Manager を自動的に再起動するようにスケジュールできます。
- **Microsoft .NET Framework 4.6 の前提条件:** Microsoft .NET Framework の前提条件バージョンは、バージョン 4.6 になりました。

修正された問題

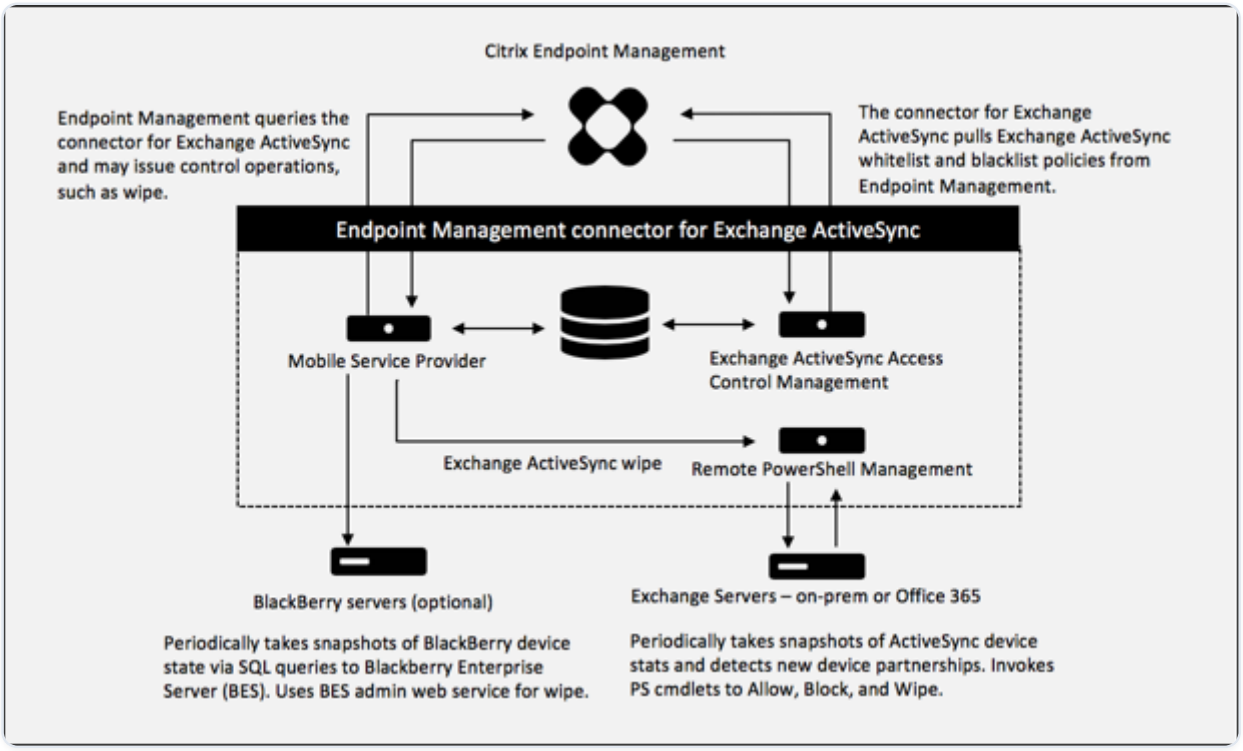
- 資格情報のプロンプトエラー: Office 365 セッションの不安定性がこのエラーを引き起こすことがよくありました。Exchange への接続の改善機能がこの問題に対処します。(XMHELP-293, XMHELP-311, XMHELP-801)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- メールボックスとデバイスのカウントの不正確さ: XenMobile Mail Manager には、改善されたメールボックスとデバイスの関連付けアルゴリズムが搭載されています。診断機能の改善は、XenMobile Mail Manager がその責任範囲内ではないと見なすメールボックスとデバイスの特定に役立ちます。(XMHELP-623)
- 許可/ブロック/ワイプコマンドが認識されない: 時折、XenMobile Mail Manager の許可/ブロック/ワイプコマンドが認識されないというバグが修正されました。(XMHELP-489)
- メモリ管理: より良いメモリ管理と軽減策。(XMHELP-419)

アーキテクチャ

次の図は、Exchange ActiveSync 用 Citrix Endpoint Management コネクタの主要コンポーネントを示しています。詳細な参照アーキテクチャ図については、アーキテクチャを参照してください。



2つの主要コンポーネントは次のとおりです。

- **Exchange ActiveSync アクセス制御管理:** Citrix Endpoint Management と通信して Citrix Endpoint Management から Exchange ActiveSync ポリシーを取得し、このポリシーをローカルで定義されたポリシーとマージして、Exchange へのアクセスを許可または拒否すべき Exchange ActiveSync デバイスを決定します。ローカルポリシーにより、ポリシー規則を拡張して、Active Directory グループ、ユーザー、デバイスタイプ、またはデバイスユーザーエージェント（通常はモバイルプラットフォームのバージョン）によるアクセス制御を許可できます。
- **リモート PowerShell 管理:** Exchange ActiveSync アクセス制御管理によってコンパイルされたポリシーを実行するために、リモート PowerShell コマンドのスケジュール設定と呼び出し

© 1997–2026 Citrix Systems, Inc. All rights reserved.

を担当します。定期的に Exchange ActiveSync データベースのスナップショットを取得し、新規または変更された Exchange ActiveSync デバイスを検出します。

システム要件と前提条件

Citrix Endpoint Management connector for Exchange ActiveSync を使用するには、以下の最小システム要件が必要です。

- Windows Server 2016、Windows Server 2012 R2、または Windows Server 2008 R2 Service Pack 1。英語ベースのサーバーである必要があります。Windows Server 2008 R2 Service Pack 1 のサポートは January 14, 2020 に終了し、Windows Server 2012 R2 のサポートは October 10, 2023 に終了します。
- Microsoft SQL Server 2016 サービスパック 2、SQL Server 2014 サービスパック 3、または SQL Server 2012 サービスパック 4。
- マイクロソフト .NET Framework 4.6。
- Blackberry Enterprise Service、バージョン 5 (オプション)。

Microsoft Exchange Server の最小サポートバージョン:

- マイクロソフト オフィス 365
- エクスチェンジ サーバー 2016
- Exchange Server 2013 (サポートは April 11, 2023 に終了)
- Exchange Server 2010 Service Pack 3 (サポートは January 14, 2020 に終了)

前提条件

- Windows Management Framework がインストールされている必要があります。
    - PowerShell V5、V4、および V3
- PowerShell実行ポリシーは、Set-ExecutionPolicy RemoteSigned を介して RemoteSigned に設定する必要があります。
- Exchange ActiveSync 用コネクタを実行しているコンピューターとリモートの Exchange Server の間で、TCP ポート 80 が開いている必要があります。

デバイスのメールクライアント: すべてのメールクライアントが、デバイスに対して常に同じ ActiveSync ID を返すわけではありません。Exchange ActiveSync 用コネクタは、各デバイスに対して一意の ActiveSync ID を期待するため、各デバイスに対して常に同じ一意の ActiveSync ID を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

生成するメールクライアントのみがサポートされます。Citrix によってテストされ、エラーなく動作したメールクライアントは次のとおりです。

- Samsung ネイティブメールクライアント
- iOS ネイティブメールクライアント

Exchange: Exchange を実行しているオンプレミスコンピューターの要件は次のとおりです。

Exchange 構成 UI で指定された資格情報には、Exchange Server に接続し、以下の Exchange 固有の PowerShell コマンドレットを実行するためのフルアクセス権が必要です。

- **Exchange Server 2010 SP2 の場合:**
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-ActiveSyncDevice`
  - `Get-ActiveSyncDeviceStatistics`
  - `Clear-ActiveSyncDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- **Exchange Server 2013 および Exchange Server 2016 の場合:**
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Exchange ActiveSync 用コネクタがフォレスト全体を表示するように構成されている場合、**Set-AdServerSettings -ViewEntireForest $true** を実行する権限が付与されている必要があります。
- 指定された資格情報には、リモートシェルを介してExchange Serverに接続する権限が付与されている必要があります。デフォルトでは、Exchangeをインストールしたユーザーがこの権限を持っています。
- リモート接続を確立し、リモートコマンドを実行するには、資格情報がリモートマシンの管理者であるユーザーに対応している必要があります。Set-PSSessionConfiguration を使用して管理要件をなくすことができますが、そのコマンドの説明はこのドキュメントの範囲外です。詳細については、Microsoft の記事「About Session Configurations」を参照してください。
- Exchange Serverは、HTTP経由のリモートPowerShell要求をサポートするように構成する必要があります。通常、Exchange Serverで次のPowerShellコマンド「WinRM QuickConfig」を実行するだけで十分です。
- Exchangeには多くのスロットリングポリシーがあります。そのポリシーの1つは、ユーザーごとに許可される同時PowerShell接続の数を制御します。Exchange 2010では、ユーザーに許可される同時接続のデフォルト数は18です。接続制限に達すると、Exchange ActiveSync用コネクタはExchange Serverに接続できなくなります。PowerShellを介して許可される同時接続の最大数を変更する方法がありますが、それはこのドキュメントの範囲外です。興味がある場合は、PowerShellによるリモート管理に関連するExchangeのスロットリングポリシーを調べてください。

Office 365 Exchangeの要件

- **権限:** Exchange構成UIで指定された資格情報は、Office 365に接続でき、次のExchange固有のPowerShellコマンドレットを実行するためのフルアクセス権が付与されている必要があります。
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Get-ManagementRoleAssignment`

- **特権:** 提供された資格情報には、リモートシェルを介してOffice 365サーバーに接続する権限が付与されている必要があります。デフォルトでは、Office 365のオンライン管理者が必要な特権を持っています。
- **スロットリングポリシー:** Exchangeには多くのスロットリングポリシーがあります。そのポリシーの1つは、ユーザーごとに許可される同時PowerShell接続の数を制御します。Office 365では、ユーザーに許可される同時接続のデフォルト数は3です。接続制限に達すると、Exchange ActiveSync用コネクタはExchange Serverに接続できなくなります。PowerShellを介して許可される同時接続の最大数を変更する方法がありますが、それはこのドキュメントの範囲外です。興味がある場合は、PowerShellによるリモート管理に関連するExchangeのスロットリングポリシーを調べてください。

インストールと構成

1. XmmSetup.msi ファイルをクリックし、インストーラーの指示に従って Citrix Endpoint Management connector for Exchange ActiveSync をインストールします。
2. セットアップウィザードの最後の画面で、 が選択されたままにします。または、 メニューから Exchange ActiveSync 用コネクタを開きます。
3. 次のデータベースプロパティを構成します。

   - **>** タブを選択します。
   - SQL Server の名前を入力します (デフォルトは localhost)。
   - データベースはデフォルトの **CitrixXmm** のままにします。

4. SQL に使用する次の認証モードのいずれかを選択します。

   - **SQL:** 有効な SQL ユーザーのユーザー名とパスワードを入力します。
   - **Windows 統合:** このオプションを選択した場合、XenMobile Mail Manager Service のログオン資格情報を、SQL Server にアクセスする権限を持つ Windows アカウントに変更する必要があります。これを行うには、 **> >** を開き、XenMobile Mail Manager Service エントリを右クリックして、 タブをクリックします。

   BlackBerry データベース接続にも Windows 統合が選択されている場合、ここで指定された Windows アカウントにも BlackBerry データベースへのアクセス権を付与する必要があります。

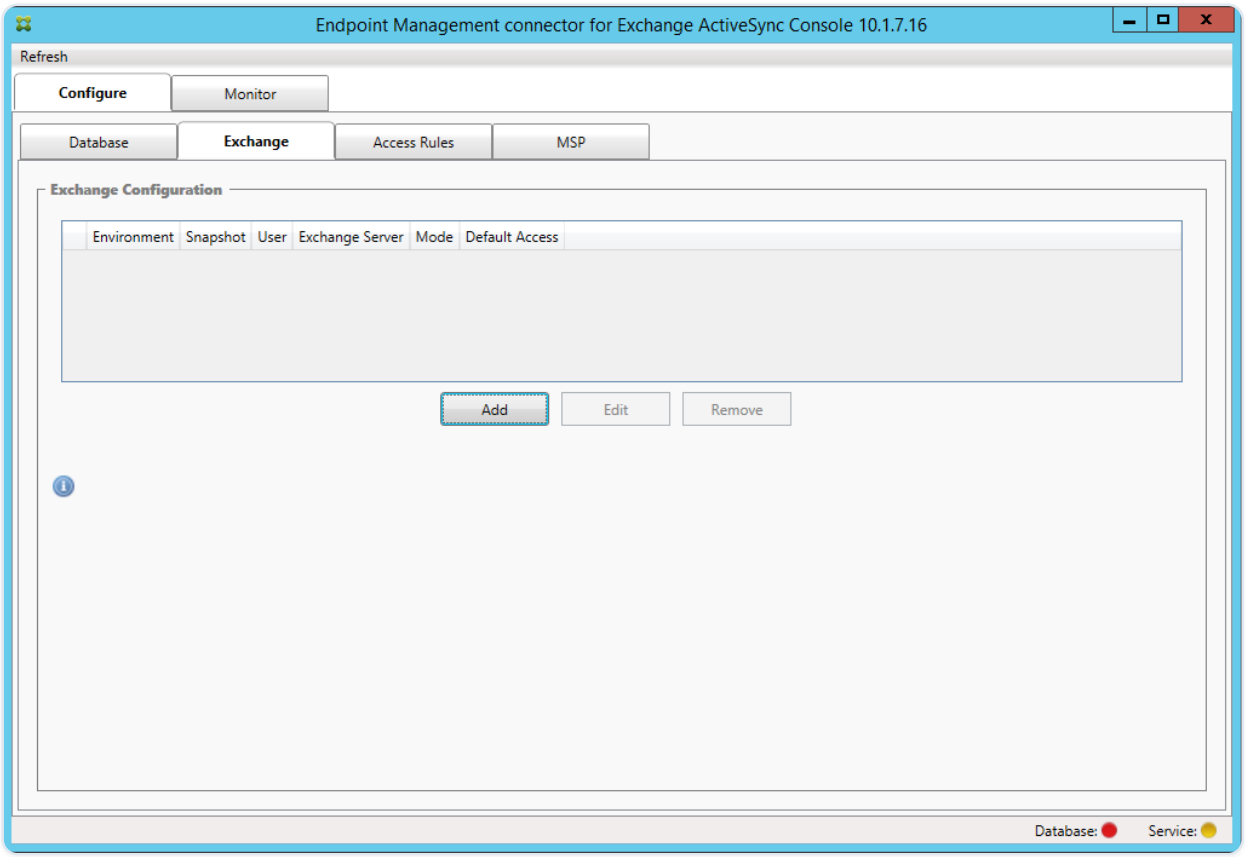
5. をクリックして SQL Server への接続が可能であることを確認し、 をクリックします。
6. サービスを再起動するよう促すメッセージが表示されます。 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exchange ActiveSync セットアップ画面用コネクタ(/en-us/citrix-endpoint-management/media/connector-configuration-change.png)

7. 1つ以上の Exchange Server を構成します。

   - 単一のExchange環境を管理している場合は、サーバーは1つのみ指定します。複数のExchange環境を管理している場合は、各Exchange環境にExchange Serverを1つ指定します。
   - 「**構成 > Exchange**」タブをクリックし、**追加**をクリックします。



8. Exchange Server環境の種類を選択します。**オンプレミス**または**Office 365**。

   - **オンプレミス**を選択した場合、リモートPowerShellコマンドに使用するExchange Serverの名前を入力します。
   - 要件セクションで指定されているように、Exchange Serverに対する適切な権限を持つWindows IDの**ユーザー名**を入力し、そのユーザーの**パスワード**を入力します。
   - メジャースナップショットを実行するスケジュールを選択します。メジャースナップショットは、すべてのExchange ActiveSyncパートナーシップを検出します。
   - マイナースナップショットを実行するスケジュールを選択します。マイナースナップショットは、新しく作成されたExchange ActiveSyncパートナーシップを検出します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- スナップショットの種類を選択します。**ディープ**または**シャロー**。シャロースナップショットは通常はるかに高速で、Exchange ActiveSync用コネクタのすべてのExchange ActiveSyncアクセス制御機能を実行するのに十分です。
- デフォルトのアクセスを選択します。**許可**、**ブロック**、または**変更なし**。この設定は、明示的なCitrix Endpoint Managementまたはローカルルールによって識別されたデバイス以外のすべてのデバイスがどのように扱われるかを制御します。**許可**を選択すると、そのようなすべてのデバイスへのActiveSyncアクセスが許可されます。**ブロック**を選択すると、アクセスが拒否されます。**変更なし**を選択すると、変更は行われません。
- ActiveSyncコマンドモードを選択します。**PowerShell**または**シミュレーション**。
- **PowerShell**モードでは、Exchange ActiveSync用コネクタは、目的のアクセス制御を実行するためにPowerShellコマンドを発行します。シミュレーションモードでは、Exchange ActiveSync用コネクタはPowerShellコマンドを発行しませんが、意図されたコマンドと意図された結果をデータベースにログ記録します。シミュレーションモードでは、ユーザーは**監視**タブを使用して、PowerShellモードが有効になっていた場合に何が起こったかを確認できます。
- **接続の有効期限**で、接続の有効期間を時間と分で設定します。接続が指定された期間に達すると、その接続は期限切れとしてマークされ、二度と使用されなくなります。期限切れの接続が使用されなくなると、Exchange ActiveSync用コネクタは接続を正常にシャットダウンします。接続が再度必要になった場合、利用可能な接続がない場合は新しい接続が初期化されます。指定がない場合、デフォルトの30分が使用されます。
- **フォレスト全体を表示**を選択して、Exchange環境内のActive Directoryフォレスト全体を表示するようにExchange ActiveSync用コネクタを構成します。
- 認証プロトコルを選択します。**Kerberos**または**基本**。Exchange ActiveSync用コネクタは、オンプレミス展開の基本認証をサポートしています。これにより、コネクタサーバーがExchangeサーバーが存在するドメインのメンバーではない場合でも、コネクタを使用できます。
- 「**Test Connectivity**」をクリックして、Exchange Serverへの接続が可能であることを確認し、「**Save**」をクリックします。
- サービスを再起動するよう促すメッセージが表示されます。「**Yes**」をクリックします。

9. アクセスルールを構成します。「**Configure > Access Rules**」タブを選択し、「**Citrix Endpoint Management Rules**」タブをクリックして、「**Add**」をクリックします。

   アクセスルール(/en-us/citrix-endpoint-management/media/connector-access-rules.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. 「**Citrix Endpoint Management server Service Properties**」ページで、URL文字列をCitrix Endpoint Managementサーバーを指すように変更します。たとえば、インスタンス名が`zdm`の場合、`https://<XdmHostName>/zdm/services/MagConfigService`と入力します。この例では、`XdmHostName`をCitrix Endpoint ManagementサーバーのIPまたはDNSアドレスに置き換えます。

    メールマネージャーコンソール(/en-us/citrix-endpoint-management/media/connector-service-properties.png)

    - サーバーの承認済みユーザーを入力します。
    - ユーザーのパスワードを入力します。
    - 「**Baseline Interval**」、「**Delta Interval**」、および「**Timeout**」の値はデフォルトのままにします。
    - 「**Test Connectivity**」をクリックしてサーバーへの接続を確認し、「**OK**」をクリックします。

    「**Disabled**」チェックボックスが選択されている場合、Citrix Endpoint Management Mail ServiceはCitrix Endpoint Managementからポリシーを収集しません。

11. 「**Local Rules**」タブをクリックします。

    ローカルルールタブ(/en-us/citrix-endpoint-management/media/connector-access-rules-local.png)

    - ActiveSyncデバイスID、デバイスタイプ、ADグループ、ユーザー、またはデバイスのUserAgentに基づいてローカルルールを追加できます。リストから適切なタイプを選択します。
    - テキストボックスにテキストまたはテキストフラグメントを入力します。必要に応じて、クエリボタンをクリックして、フラグメントに一致するエンティティを表示します。

    Group以外のすべてのタイプでは、システムはスナップショットで見つかったデバイスに依存します。したがって、開始したばかりでスナップショットを完了していない場合、エンティティは利用できません。

    - テキスト値を選択し、**許可**または**拒否**をクリックして、右側の**ルールリスト**ペインに追加します。**ルールリスト**ペインの右側にあるボタンを使用して、ルールの順序を変更したり、削除したりできます。順序は重要です。特定のユーザーとデバイスの場合、ルールは表示されている順序で評価され、上位のルール（上部に近いルール）が一致すると、それ以降のルールは無効になります。たとえば、すべてのiPadデバイスを許可するルールがあ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

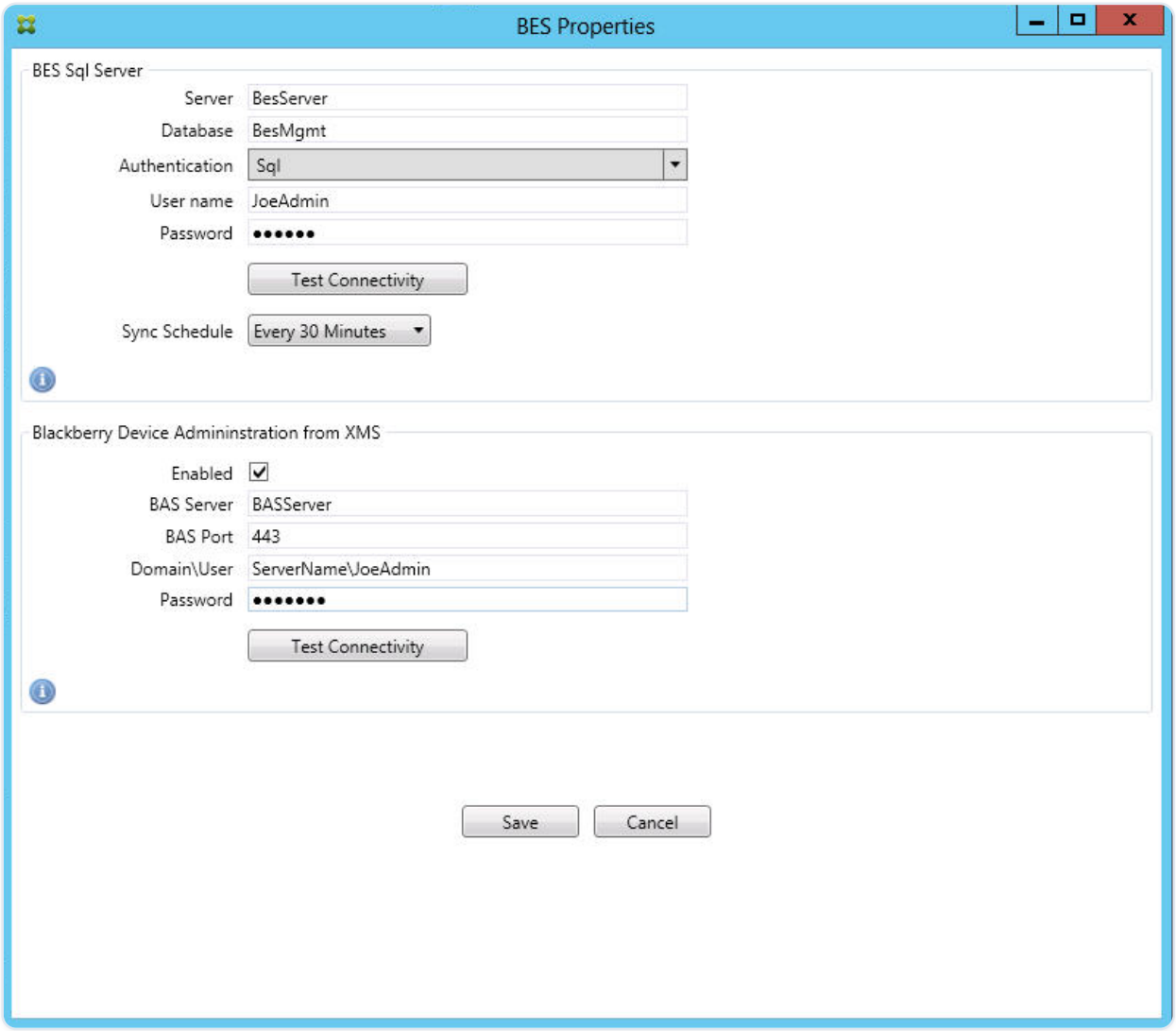
り、その後にユーザーMattをブロックするルールがある場合、iPadルールがMattルールよりも実質的な優先度が高いため、MattのiPadは引き続き許可されます。

- ルールリスト内のルールを分析して、潜在的なオーバーライド、競合、または補足的な構成を見つけるには、**分析**をクリックし、次に**保存**をクリックします。

12. Active Directoryグループで動作するローカルルールを構築する場合は、**LDAPの構成**をクリックし、LDAP接続プロパティを構成します。

    LDAP構成(/en-us/citrix-endpoint-management/media/xmm-install-8.png)

13. 必要に応じて、BlackBerry Enterprise Server (BES) のインスタンスを1つ以上構成します。**追加**をクリックし、BES SQL Serverのサーバー名を入力します。



- BES管理データベースのデータベース名を入力します。
- **認証**モードを選択します。Windows統合認証を選択した場合、Exchange ActiveSyncサービス用コネクタのユーザーアカウントが、BES SQL Serverへの接続に使用されるアカウントになります。コネクタデータベース接続にもWindows統合を選択した場合、ここで指定

© 1997–2026 Citrix Systems, Inc. All rights reserved.

されたWindowsアカウントにもコネクタデータベースへのアクセス権を付与する必要があります。

- **SQL認証**を選択した場合は、ユーザー名とパスワードを入力します。
- **同期スケジュール**を設定します。これは、BES SQL Serverに接続し、デバイスの更新を確認するために使用されるスケジュールです。
- **接続テスト**をクリックして、SQL Serverへの接続を確認します。Windows統合を選択した場合、このテストは現在ログオンしているユーザーを使用し、コネクタサービスユーザーは使用しないため、SQL認証を正確にテストするものではありません。
- Citrix Endpoint ManagementからBlackBerryデバイスのリモートワイプとパスワードリセットをサポートするには、**有効**チェックボックスを選択します。
- BESの完全修飾ドメイン名 (FQDN) を入力します。
- 管理Webサービスに使用されるBESポートを入力します。
- BESサービスで必要とされる完全修飾ユーザーとパスワードを入力します。
- BESへの接続をテストするには、**Test Connectivity** をクリックし、次に **Save** をクリックします。

ActiveSync IDでメールポリシーを適用する

企業のメールポリシーにより、特定のデバイスが企業メールの使用を承認されていない場合があります。このポリシーに従うため、従業員がそのようなデバイスから企業メールにアクセスできないようにする必要があります。Citrix Endpoint Management connector for Exchange ActiveSync と Citrix Endpoint Management は連携して、このようなメールポリシーを適用します。Citrix Endpoint Management は企業メールアクセスに関するポリシーを設定します。未承認のデバイスがCitrix Endpoint Managementに登録されると、Exchange ActiveSync用コネクタがポリシーを適用します。

デバイス上のメールクライアントは、デバイスを識別するために使用されるデバイスID（ActiveSync IDとも呼ばれる）を使用して、Exchange Server（またはOffice 365）に自身を通知します。Citrix Secure Hub は同様の識別子を取得し、デバイスが登録されるとCitrix Endpoint Managementにその識別子を送信します。2つのデバイスIDを比較することで、Exchange ActiveSync用コネクタは特定のデバイスが企業メールアクセスを持つべきかどうかを判断できます。次の図はこの概念を示しています。

ActiveSync ID検出ワークフロー(/en-us/citrix-endpoint-management/media/connector-identifydevices-diagram.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementが、デバイスがExchangeに公開するIDとは異なるActiveSync IDをExchange ActiveSync用コネクタに送信した場合、コネクタは、そのデバイスをどうすべきかをExchangeに指示できません。

ActiveSync IDの一致は、ほとんどのプラットフォームで確実に機能します。しかし、Citrixは、一部のAndroid実装では、デバイスからのActiveSync IDが、メールクライアントがExchangeに通知するIDと異なることを発見しました。この問題を軽減するために、次のことができます。

- Androidプラットフォームでは、CitrixはCitrix Secure Mailの使用を推奨します。

企業メールアクセスポリシーが適切に適用されることを保証するために、防御的なセキュリティ体制を採用できます。Citrix Endpoint Management connector for Exchange ActiveSync を構成し、静的ポリシーをデフォルトで **Deny** に設定してメールをブロックします。これは、従業員がAndroidデバイスで別のメールクライアントを構成し、ActiveSync ID検出が機能しない場合、企業メールがその従業員へのアクセスを拒否することを意味します。

アクセス制御ルール

Citrix Endpoint Management connector for Exchange ActiveSync は、Exchange ActiveSyncデバイスのアクセス制御を動的に構成するためのルールベースのアプローチを提供します。コネクタのアクセス制御ルールは、一致式と目的のアクセス状態（許可またはブロック）の2つの部分で構成されます。ルールは、特定のExchange ActiveSyncデバイスに対して評価され、そのルールがデバイスに適用されるか、またはデバイスと一致するかを判断します。一致式には複数の種類があります。たとえば、ルールは特定のデバイスタイプに属するすべてのデバイス、特定のExchange ActiveSyncデバイスID、または特定のユーザーのすべてのデバイスなどに一致する場合があります。

ルールリスト内のルールの追加、削除、再配置のどの時点でも、**Cancel** ボタンをクリックすると、ルールリストは最初に開いたときの状態に戻ります。**Save** をクリックしない限り、Configureツールを閉じると、このウィンドウで行われた変更はすべて失われます。

Citrix Endpoint Management connector for Exchange ActiveSync には、ローカルルール、Citrix Endpoint Managementサーバールール（XDMルールとも呼ばれる）、およびデフォルトアクセスルールの3種類のルールがあります。

ローカルルール: ローカルルールは最も高い優先度を持ちます。デバイスがローカルルールに一致した場合、ルール評価は停止します。Citrix Endpoint Managementサーバールールもデフォルトアクセスルールも参照されません。ローカルルールは、**Configure > Access Rules > Local Rules** タブを介して、Exchange ActiveSync用コネクタにローカルで構成されます。サポートマッチング

© 1997–2026 Citrix Systems, Inc. All rights reserved.

は、特定のActive Directoryグループ内のユーザーのメンバーシップに基づいています。サポートマッチングは、次のフィールドの正規表現に基づいています。

- Active SyncデバイスID
- ActiveSyncデバイスの種類
- ユーザープリンシパル名 (UPN)
- ActiveSyncユーザーエージェント (通常はデバイスプラットフォームまたはメールクライアント)

メジャースナップショットが完了してデバイスが検出された場合、通常ルールまたは正規表現ルールを追加できます。メジャースナップショットが完了していない場合は、正規表現ルールのみを追加できます。

Citrix Endpoint Managementサーバーのルール: Citrix Endpoint Managementサーバーのルールは、管理対象デバイスに関するルールを提供する外部のCitrix Endpoint Managementサーバーへの参照です。Citrix Endpoint Managementサーバーは、デバイスがジェイルブレイクされているか、禁止されているアプリがあるかなど、Citrix Endpoint Managementに認識されているプロパティに基づいて、許可またはブロックするデバイスを識別する独自の高レベルルールで構成できます。Citrix Endpoint Managementは高レベルルールを評価し、許可またはブロックされたActiveSyncデバイスIDのセットを生成し、それらはXenMobile Mail Managerに配信されます。

デフォルトのアクセスルール: デフォルトのアクセスルールは、すべてのデバイスに一致する可能性があり、常に最後に評価されるという点でユニークです。このルールは包括的なルールであり、特定のデバイスがローカルまたはCitrix Endpoint Managementサーバーのルールに一致しない場合、デバイスの目的のアクセス状態はデフォルトのアクセスルールの目的のアクセス状態によって決定されます。

- **デフォルトアクセス – 許可:** ローカルまたはCitrix Endpoint Managementサーバーのルールのいずれにも一致しないデバイスは許可されます。
- **デフォルトアクセス – ブロック:** ローカルまたはCitrix Endpoint Managementサーバーのルールのいずれにも一致しないデバイスはブロックされます。
- **デフォルトアクセス - 変更なし:** ローカルまたはCitrix Endpoint Managementサーバーのルールのいずれにも一致しないデバイスは、Exchange ActiveSync用コネクタによってアクセス状態が一切変更されません。デバイスがExchangeによって検疫モードに置かれている場合、アクションは実行されません。たとえば、デバイスを検疫モードから削除する唯一の方法は、明示的なローカルまたはXDMルールで検疫を上書きすることです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ルール評価について

ExchangeがExchange ActiveSync用コネクタに報告する各デバイスについて、ルールは次のように優先度の高いものから低いものへと順に評価されます。

- ローカルルール
- Citrix Endpoint Managementサーバーのルール
- デフォルトのアクセスルール

一致が見つかると、評価は停止します。たとえば、ローカルルールが特定のデバイスに一致する場合、そのデバイスはCitrix Endpoint Managementサーバーのルールやデフォルトのアクセスルールに対して評価されません。これは、特定のルールタイプ内でも同様です。たとえば、ローカルルールリストで特定のデバイスに対して複数のマッチがある場合、最初の一致が満たされた時点で評価は停止します。

Exchange ActiveSync用コネクタは、デバイスのプロパティが変更された場合、デバイスが追加または削除された場合、あるいはルール自体が変更された場合に、現在定義されているルールセットを再評価します。メジャースナップショットは、設定可能な間隔でデバイスプロパティの変更と削除を検出します。マイナースナップショットは、設定可能な間隔で新しいデバイスを検出します。

Exchange ActiveSyncにもアクセスを管理するルールがあります。これらのルールがExchange ActiveSync用コネクタのコンテキストでどのように機能するかを理解することが重要です。Exchangeは、個人免除、デバイスルール、組織設定の3つのレベルのルールで構成できます。Exchange ActiveSync用コネクタは、Remote PowerShellリクエストをプログラムで発行して個人免除リストに影響を与えることにより、アクセス制御を自動化します。これらは、特定のメールボックスに関連付けられた、許可またはブロックされたExchange ActiveSyncデバイスIDのリストです。展開されると、Exchange ActiveSync用コネクタは、Exchange内の免除リスト機能の管理を効果的に引き継ぎます。Microsoftの記事「Exchange および Configuration Manager を使用したデバイス管理」を参照してください。

分析は、同じフィールドに対して複数のルールが定義されている状況で役立ちます。ルール間の関係をトラブルシューティングできます。ルールフィールドの観点から分析を行います。たとえば、ActiveSyncデバイスID、ActiveSyncデバイスタイプ、ユーザー、ユーザーエージェントなど、一致するフィールドに基づいてルールがグループで分析されます。

ルールの用語

- **オーバーライドルール:** オーバーライドは、複数のルールが同じデバイスに適用できる場合に発生します。ルールはリスト内の優先順位によって評価されるため、後で適用される可能性のあるルールインスタンスは評価されない場合があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

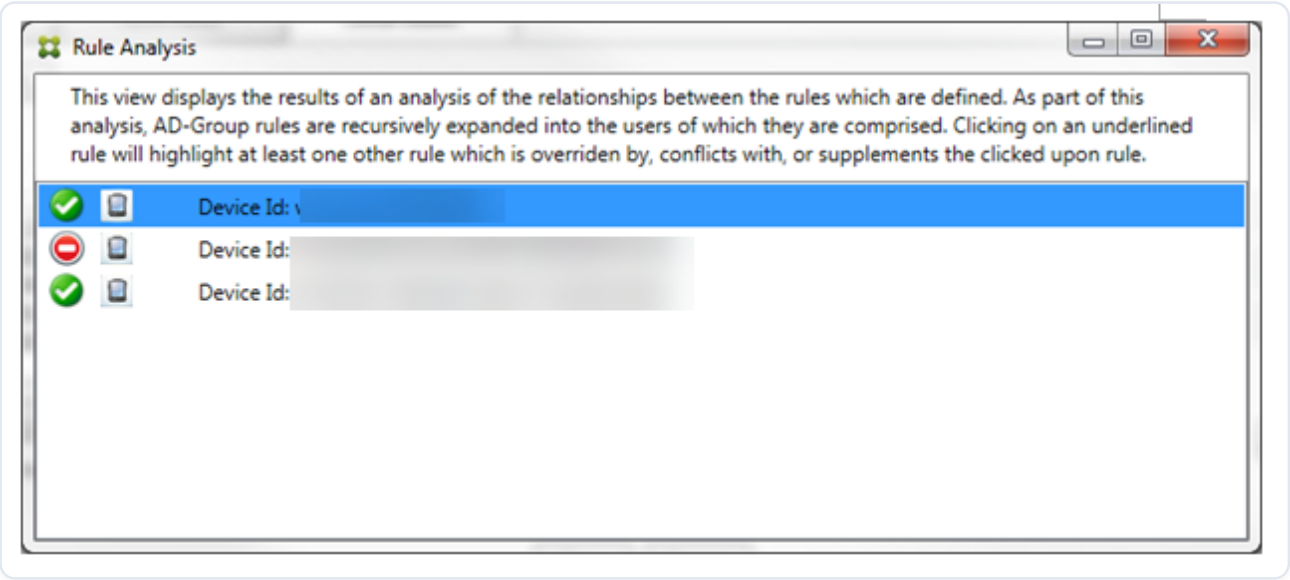
- **競合ルール:** 競合は、複数のルールが同じデバイスに適用できるが、アクセス（許可/ブロック）が一致しない場合に発生します。競合するルールが正規表現ルールでない場合、競合は常に暗黙的にオーバーライドを意味します。
- **補足ルール:** 補足は、複数のルールが正規表現ルールであり、2つ（またはそれ以上）の正規表現を単一の正規表現ルールに結合できるか、または機能が重複していないことを確認する必要がある場合に発生します。補足ルールは、そのアクセス（許可/ブロック）において競合する可能性もあります。
- **プライマリルール:** プライマリルールは、ダイアログボックス内でクリックされたルールです。このルールは、周囲を囲む実線の境界線によって視覚的に示されます。また、ルールには上または下を指す1つまたは2つの緑色の矢印が表示されます。矢印が上を指している場合、その矢印はプライマリルールの前に補助ルールがあることを示します。矢印が下を指している場合、これはプライマリルールの後に補助ルールがあることを示します。一度にアクティブにできるプライマリルールは1つだけです。
- **補助ルール:** 補助ルールは、オーバーライド、競合、または補足関係のいずれかを通じて、プライマリルールと何らかの形で関連しています。これらのルールは、周囲を囲む破線の境界線によって視覚的に示されます。各プライマリルールには、1つから多数の補助ルールが存在する可能性があります。下線が引かれたエントリをクリックすると、強調表示される補助ルールは常にプライマリルールの観点からのものです。たとえば、補助ルールがプライマリルールによってオーバーライドされる、補助ルールがプライマリルールとのアクセスで競合する、または補助ルールがプライマリルールを補足する、といった場合です。

ルール分析ダイアログボックスでのルールの種類の表示方法

競合、オーバーライド、または補足がない場合、**ルール分析**ダイアログボックスには下線付きのエントリはありません。いずれかの項目をクリックしても影響はありません。たとえば、通常の選択された項目の視覚表示が発生します。

ルール分析ウィンドウにはチェックボックスがあり、これを選択すると、競合、オーバーライド、冗長性、または補足であるルールのみが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



オーバーライドが発生すると、プライマリルールと補助ルール（複数可）の少なくとも2つのルールに下線が引かれます。少なくとも1つの補助ルールは、より薄いフォントで表示され、そのルールがより高い優先順位のルールによってオーバーライドされたことを示します。オーバーライドされたルールをクリックすると、どのルールがそのルールをオーバーライドしたかを確認できます。オーバーライドされたルールがプライマリルールまたは補助ルールであるために強調表示されるたびに、その横に黒い丸が表示され、そのルールが非アクティブであることをさらに視覚的に示します。たとえば、ルールをクリックする前のダイアログボックスは次のようになります。

「上書き」(/en-us/citrix-endpoint-management/media/xenmobilemailmanager-accessrules13.png)

最も優先度の高いルールをクリックすると、ダイアログボックスは次のように表示されます。

「最も優先度の高いルールダイアログボックス」(/en-us/citrix-endpoint-management/media/xenmobilemailmanager-accessrules14.png)

この例では、正規表現ルール `WorkMail.*` がプライマリルール（実線枠で示される）であり、通常ルール `workmailc633313818` が補助ルール（破線枠で示される）です。補助ルールの横にある黒い点は、その前にある優先度の高い正規表現ルールのため、そのルールが非アクティブ（評価されることはありません）であることをさらに示す視覚的な合図です。上書きされたルールをクリックすると、ダイアログボックスは次のように表示されます。

「上書きされたルールダイアログボックス」(/en-us/citrix-endpoint-management/media/xenmobilemailmanager-accessrules15.png)

前の例では、正規表現ルール `WorkMail.*` が補助ルール（破線枠で示される）であり、通常ルール `workmailc633313818` がプライマリルール（実線枠で示される）です。この簡単な例では、大きな違いはありません。より複雑な例については、このトピックの後半にある複雑な式の例を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参照してください。多くのルールが定義されているシナリオでは、上書きされたルールをクリックすると、どのルールがそれを上書きしたかをすばやく特定できます。

競合が発生すると、プライマリルールと補助ルールまたは複数のルールを含む、少なくとも2つのルールに下線が引かれます。競合するルールは赤い点で示されます。互いにのみ競合するルールは、2つ以上の正規表現ルールが定義されている場合にのみ可能です。他のすべての競合シナリオでは、競合だけでなく、上書きも作用します。簡単な例でいずれかのルールをクリックする前に、ダイアログボックスは次のように表示されます。

「ルール分析」(/en-us/citrix-endpoint-management/media/xenmobilemailmanager-accessrules16.png)

2つの正規表現ルールを検査すると、最初のルールは「App」を含むデバイスIDを持つすべてのデバイスを許可し、2番目のルールは `Appl` を含むデバイスIDを持つすべてのデバイスを拒否することが明らかです。また、2番目のルールが `Appl` を含むデバイスIDを持つすべてのデバイスを拒否するにもかかわらず、許可ルールの優先度が高いため、その一致条件を持つデバイスが拒否されることはありません。最初のルールをクリックすると、ダイアログボックスは次のように表示されます。

「ルール分析」(/en-us/citrix-endpoint-management/media/xenmobilemailmanager-accessrules17.png)

前のシナリオでは、プライマリルール（正規表現ルール `App.*`）と補助ルール（正規表現ルール `Appl.*`）の両方が黄色で強調表示されています。これは、単一の一致可能なフィールドに複数の正規表現ルールを適用したことを警告する単なる視覚的な警告であり、冗長性の問題やより深刻な問題を示している可能性があります。

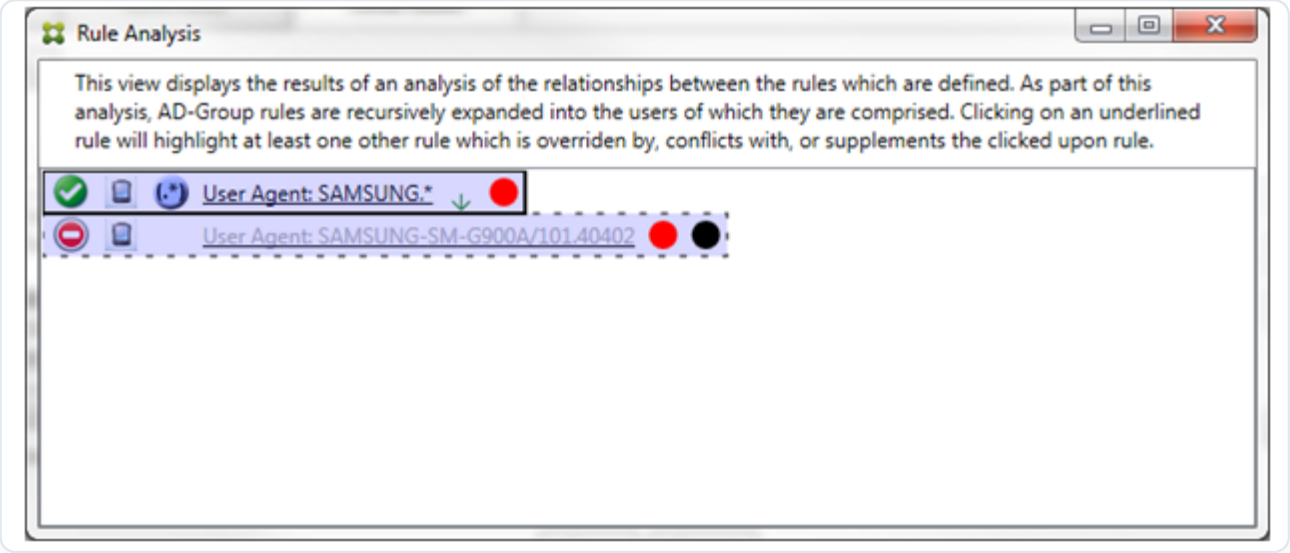
競合と上書きの両方があるシナリオでは、プライマリルール（正規表現ルール `App.*`）と補助ルール（正規表現ルール `Appl.*`）の両方が黄色で強調表示されます。これは、単一の一致可能なフィールドに複数の正規表現ルールを適用したことを警告する単なる視覚的な警告であり、冗長性の問題やより深刻な問題を示している可能性があります。

「競合と上書きのシナリオ」(/en-us/citrix-endpoint-management/media/xenmobilemailmanager-accessrules18.png)

前の例では、最初のルール（正規表現ルール `SAMSUNG.*`）が次のルール（通常ルール `SAMSUNG-SM-G900A/101.40402`）を上書きするだけでなく、2つのルールがアクセスにおいて異なる（プライマリは許可を指定し、補助はブロックを指定する）ことが簡単にわかります。2番目のルール（通常ルール `SAMSUNG-SM-G900A/101.40402`）は、上書きされて非アクティブであることを示すために、薄いテキストで表示されます。

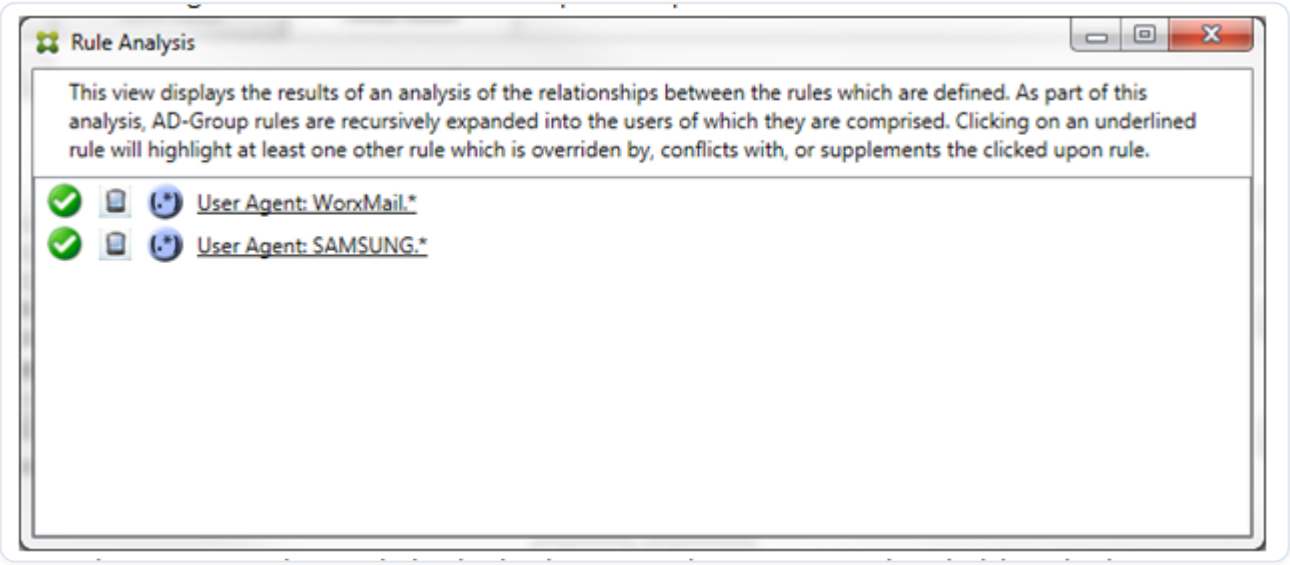
© 1997–2026 Citrix Systems, Inc. All rights reserved.

正規表現ルールをクリックすると、ダイアログボックスは次のように表示されます。



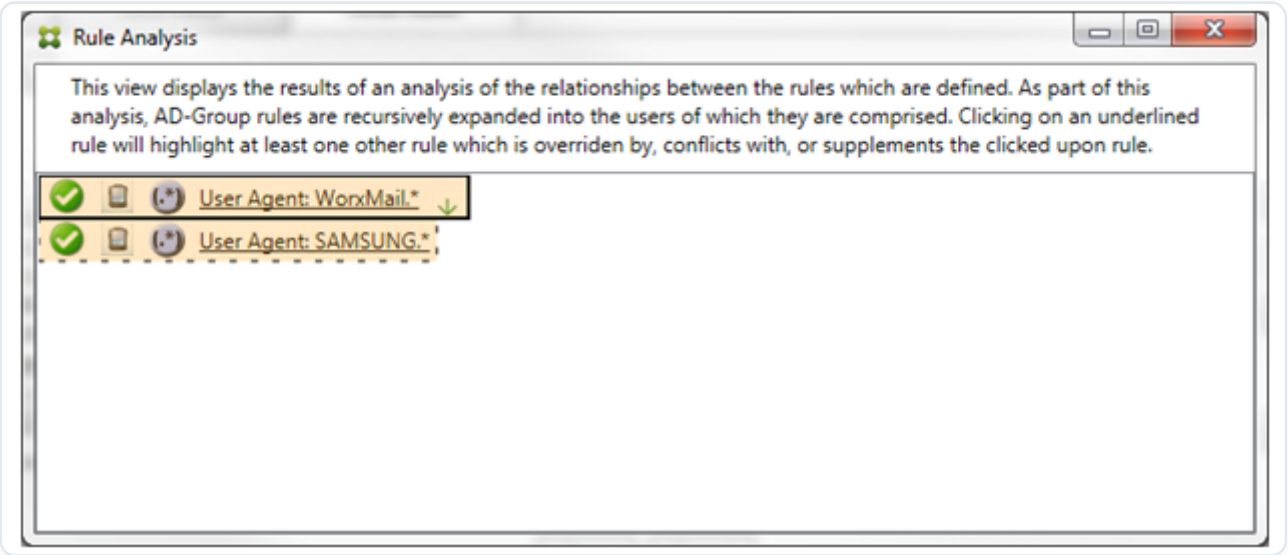
プライマリルール（正規表現ルール `SAMSUNG.*`）の後には赤い点が表示され、そのアクセス状態が1つ以上の補助ルールと競合していることを示します。補助ルール（通常ルール `SAMSUNG-SM-G900A/101.40402`）の後には赤い点が表示され、そのアクセス状態がプライマリルールと競合していることを示します。そのルールには黒い点も表示され、それがオーバーライドされて非アクティブになっていることを示します。

少なくとも2つのルール（プライマリルールと補助ルール）が下線で示されます。互いに補完し合うルールは、正規表現ルールのみとなります。ルールが互いに補完し合う場合、黄色のオーバーレイで示されます。簡単な例では、いずれかのルールをクリックする前のダイアログボックスは次のようになります。



視覚的に確認すると、両方のルールが正規表現ルールであり、Citrix Endpoint Management connector for Exchange ActiveSync の ActiveSync デバイスIDフィールドに適用されていることが簡単にわかります。最初のルールをクリックすると、ダイアログボックスは次のようになります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



プライマリルール（正規表現ルール `WorkMail.*`）は黄色のオーバーレイで強調表示され、正規表現である補助ルールが少なくとも1つ存在することを示します。補助ルール（正規表現ルール `SAMSUNG.*`）は黄色のオーバーレイで強調表示され、このルールとプライマリルールの両方が、Exchange ActiveSync コネクタ内の同じフィールドに適用される正規表現ルールであることを示します。この場合、そのフィールドはActiveSyncデバイスIDです。正規表現は重複する場合としない場合があります。正規表現が適切に作成されているかどうかは、お客様が判断してください。

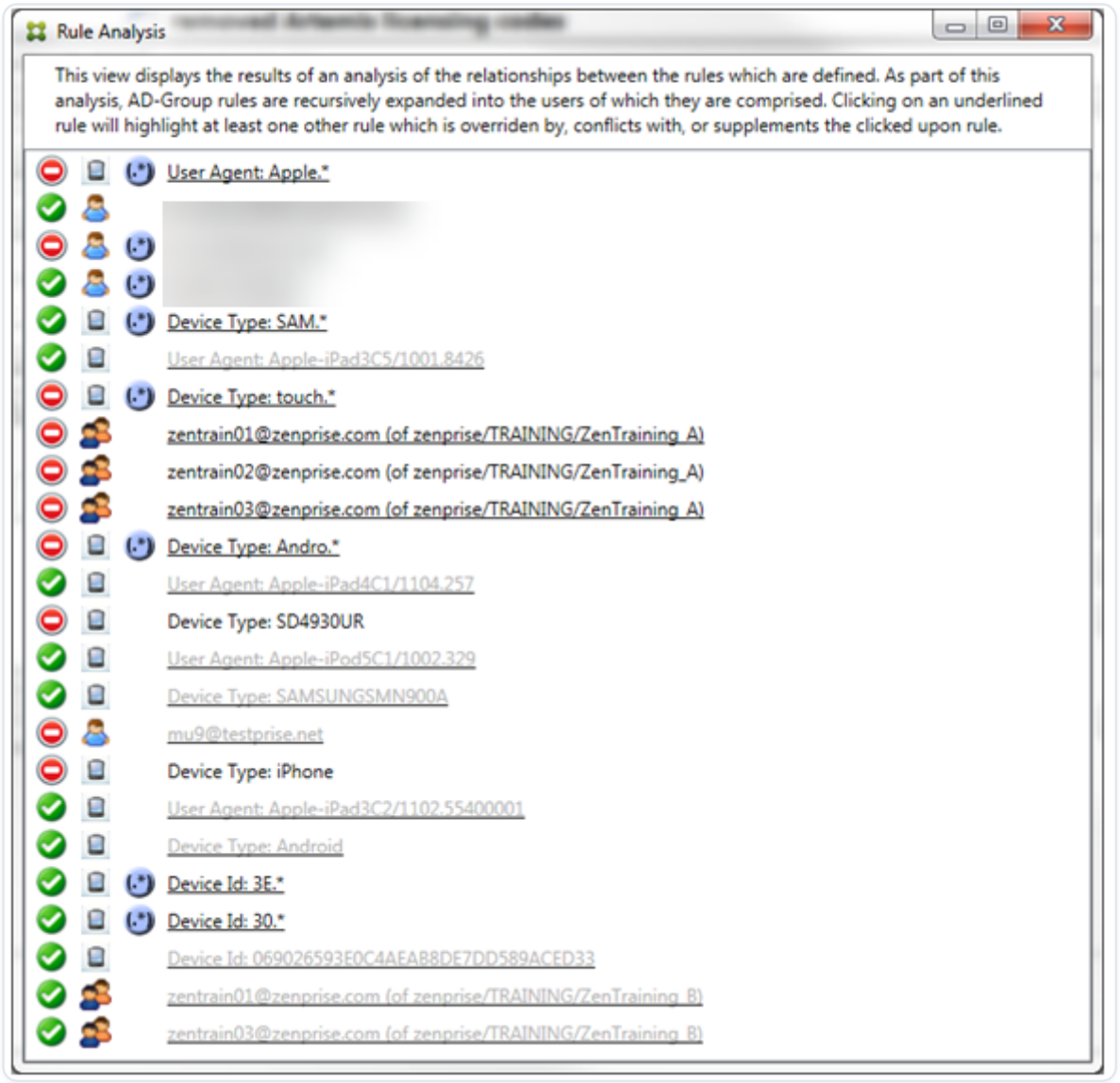
複雑な式の例

多くの潜在的なオーバーライド、競合、または補完が発生する可能性があり、すべての可能なシナリオの例を示すことは不可能です。次の例では、実行すべきでないことについて説明するとともに、ルール分析の視覚的構成の全機能を示す役割も果たします。次の図では、ほとんどの項目に下線が引かれています。多くの項目が薄いフォントで表示されており、これは、該当するルールが何らかの形でより優先度の高いルールによってオーバーライドされていることを示しています。



アイコンで示されているように、いくつかの正規表現ルールもリストに含まれています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

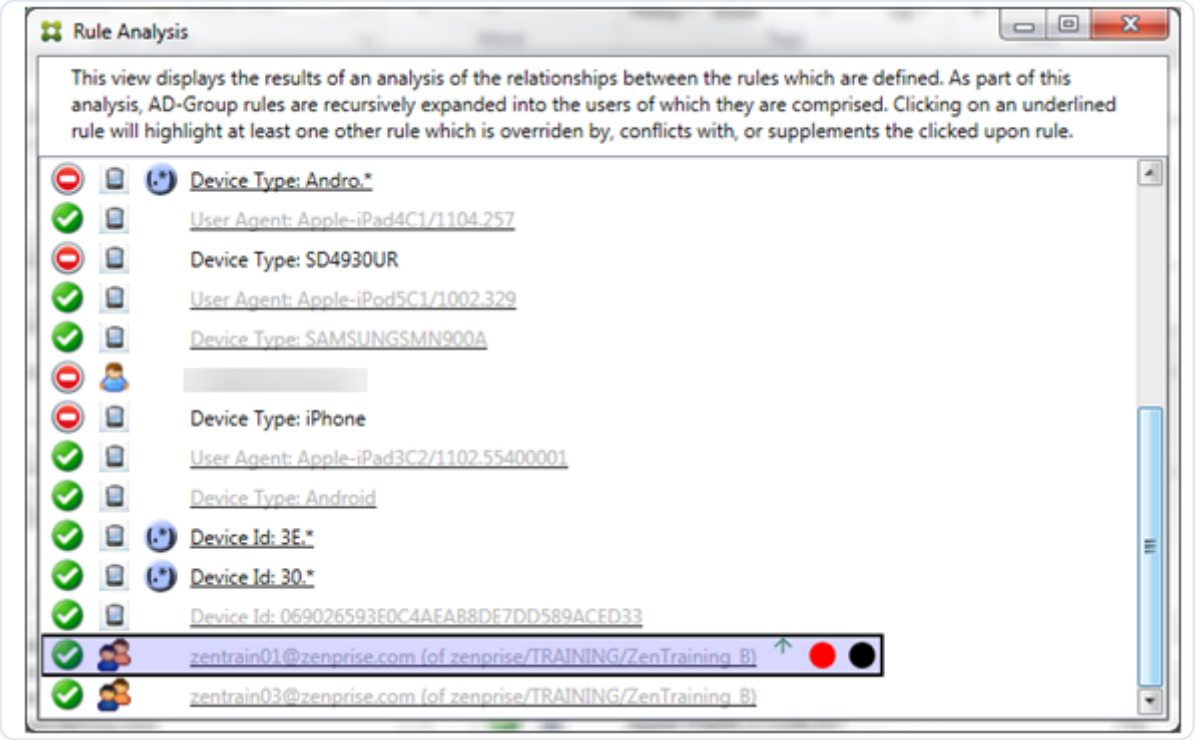


オーバーライドを分析する方法

特定のルールをオーバーライドしたルールを確認するには、そのルールをクリックします。

例1： この例では、`zentrain01@zenprise.com` がオーバーライドされた理由を調べます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

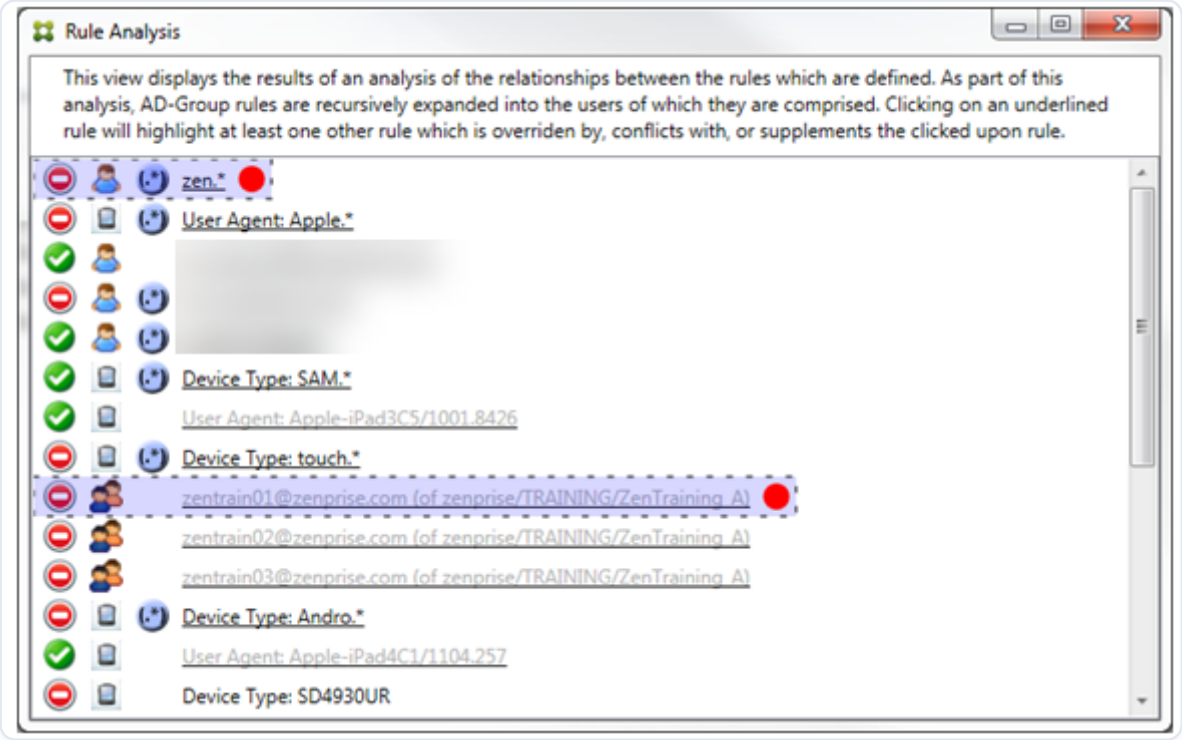


プライマリルール（ADグループルール `zenprise/TRAINING/ZenTraining B`、`zentrain01@zenprise.com` がそのメンバー）には、次の特性があります。

- 青色で強調表示され、実線の境界線があります。
- 上向きの緑色の矢印があります（補助ルールがすべてその上にあることを示します）。
- 赤い丸と黒い丸の両方が続き、それぞれ1つ以上の補助ルールがそのアクセスと競合していること、およびプライマリルールがオーバーライドされて非アクティブになっていることを示します。

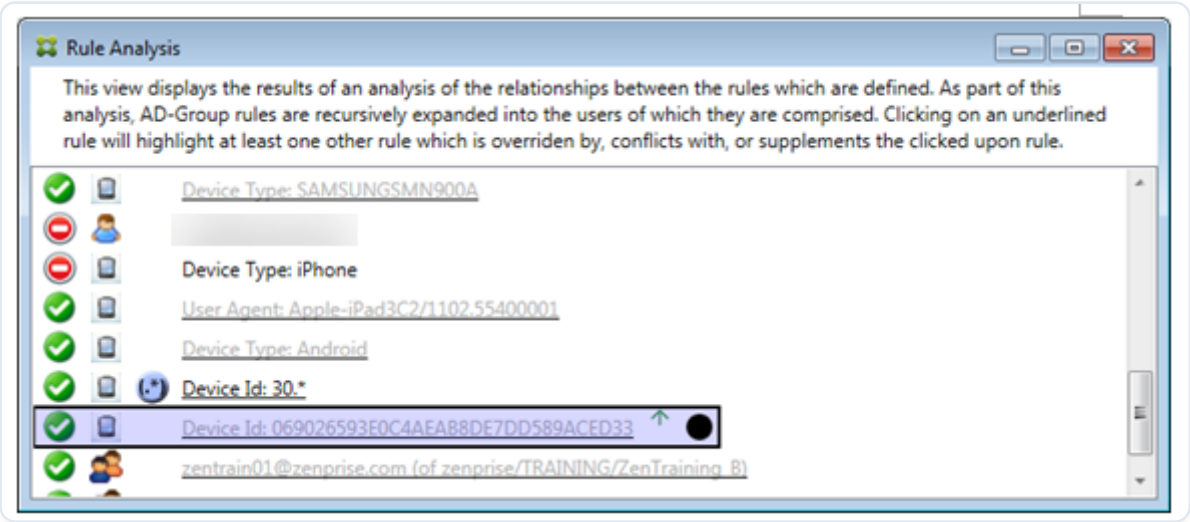
上にスクロールすると、次の内容が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



この場合、プライマリルールをオーバーライドする2つの補助ルールがあります。正規表現ルール `zen.*` と通常ルール `zentrain01@zenprise.com` （`zenprise/TRAINING/ZenTraining A` の）です。後者の補助ルールの場合、Active Directoryグループルール `ZenTraining A` にユーザー `zentrain01@zenprise.com` が含まれ、Active Directoryグループルール `ZenTraining B` にもユーザー `zentrain01@zenprise.com` が含まれています。しかし、補助ルールはプライマリルールよりも優先順位が高いため、プライマリルールはオーバーライドされています。プライマリルールのアクセスは「許可」であり、両方の補助ルールのアクセスが「ブロック」であるため、すべてに赤い丸が続き、アクセス競合をさらに示しています。

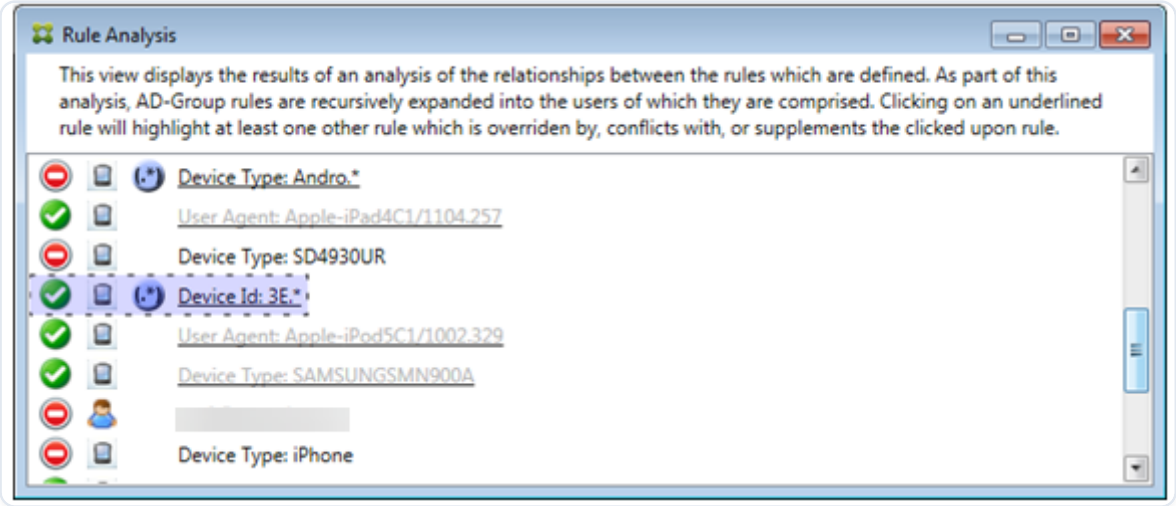
例2： この例は、ActiveSyncデバイスIDが `069026593E0C4AEAB8DE7DD589ACED33` のデバイスがオーバーライドされた理由を示しています。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

プライマリルール（通常のデバイスIDルール `069026593E0C4AEAB8DE7DD589ACED33`）には、次の特徴があります。

- 青色で強調表示され、実線の境界線があります。
- 上向きの緑色の矢印があります（補助ルールがその上にあることを示します）。
- 黒い丸が続き、補助ルールがプライマリルールをオーバーライドして非アクティブになっていることを示します。



この場合、単一の補助ルールがプライマリルールをオーバーライドします。正規表現ActiveSyncデバイスIDルールは `3E.*` です。正規表現 `3E.*` が `069026593E0C4AEAB8DE7DD589ACED33` に一致するため、プライマリルールは評価されません。

補足と競合を分析する方法

この場合、プライマリルールは正規表現のActiveSyncデバイスタイプルール `touch.*` です。特性は次のとおりです。

- 特定のルールフィールド（この場合はActiveSyncデバイスタイプ）に対して、単一の正規表現ルールだけでなく複数のルールが適用されていることを警告する、黄色のオーバーレイが付いた実線で示されます。
- それぞれ上向きと下向きの2つの矢印は、優先度の高い補助ルールが少なくとも1つと、優先度の低い補助ルールが少なくとも1つ存在することを示しています。
- その隣の赤い丸は、少なくとも1つの補助ルールのアクセスが**許可**に設定されており、プライマリルールのアクセスである**ブロック**と競合していることを示しています。
- 2つの補助ルールがあります。正規表現のActiveSyncデバイスタイプルール `SAM.*` と、正規表現のActiveSyncデバイスタイプルール `Andro.*` です。
- 両方の補助ルールは、補助であることを示すために破線で囲まれています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 両方の補助ルールは、ActiveSyncデバイスタイプのルールフィールドにも適用されていることを示すために、黄色でオーバーレイされています。
- このようなシナリオでは、正規表現ルールが冗長にならないようにする必要があります。

ルールシナリオ(/en-us/citrix-endpoint-management/media/xenmobilemailmanager-accessrules27.png)

ルールの詳細な分析方法

この例では、ルール間の関係が常にプライマリルールの視点からどのように見られるかを探ります。前の例では、値が `touch.*` のデバイスタイプのルールフィールドに適用される正規表現ルールをクリックするとどうなるかを示しました。補助ルール `Andro.*` をクリックすると、異なる補助ルールのセットが強調表示されます。

ルール分析(/en-us/citrix-endpoint-management/media/xenmobilemailmanager-accessrules28.png)

この例では、ルール関係に含まれるオーバーライドされたルールを示しています。このルールは通常のActiveSyncデバイスタイプルール `Android` であり、オーバーライドされており（薄くなったフォントとその隣の黒い丸で示されます）、そのアクセスはプライマリルールの正規表現ActiveSyncデバイスタイプルール `Andro.*` とも競合しています。このルールは、クリックされる前は補助ルールでした。前の例では、通常のActiveSyncデバイスタイプルール `Android` は、当時のプライマリルール（正規表現ActiveSyncデバイスタイプルール `touch.*`）の視点からは関連性がなかったため、補助ルールとして表示されませんでした。

通常の式ローカルルールを構成するには

1. **アクセスルール**タブをクリックします。

   アクセスルールタブ(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-local-rule.png)

2. **Device ID**リストで、ローカルルールを作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドの一意の一致をすべて表示します。この例では、**Device Type**フィールドが選択されており、選択肢は次のリストボックスに表示されます。

   一意の一致(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-localrules-unique.png)

4. 結果リストボックス内のいずれかの項目をクリックし、次のいずれかのオプションをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Allow**は、一致するすべてのデバイスに対してActiveSyncトラフィックを許可するようにExchangeが構成されることを意味します。
- **Deny**は、一致するすべてのデバイスに対してActiveSyncトラフィックを拒否するようにExchangeが構成されることを意味します。

この例では、デバイスの種類がSamsungSPhl720であるすべてのデバイスのアクセスが拒否されます。

Samsungの例(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-accessrules-deny-samsung.png)

正規表現を追加するには

正規表現ローカルルールは、その横に表示されるアイコン - 
で区別できます。正規表現ルールを追加するには、特定のフィールドの結果リストから既存の値に基づいて正規表現ルールを作成するか（メジャースナップショットが完了している限り）、目的の正規表現を直接入力することができます。

既存のフィールド値から正規表現を作成するには

1. **アクセスルール**タブをクリックします。

   アクセスルールタブ(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-local-rule.png)
2. **Device ID**リストで、正規表現ローカルルールを作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドの一意の一致をすべて表示します。この例では、**デバイスタイプ**フィールドが選択されており、選択肢は次のリストボックスに表示されます。

   デバイスタイプの選択肢(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-magnifier.png)
4. 結果リストのいずれかの項目をクリックします。この例では、**SAMSUNGSPHL720**が選択されており、**デバイスタイプ**の横のテキストボックスに表示されます。

   ルール分析(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-localrules-samsung-regex.png)
5. デバイスタイプ値に「Samsung」を含むすべてのデバイスタイプを許可するには、次の手順に従って正規表現ルールを追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 選択した項目テキストボックス内をクリックします。

b. テキストを**SAMSUNGSPHL720**から**SAMSUNG.***に変更します。

c. 正規表現チェックボックスが選択されていることを確認します。

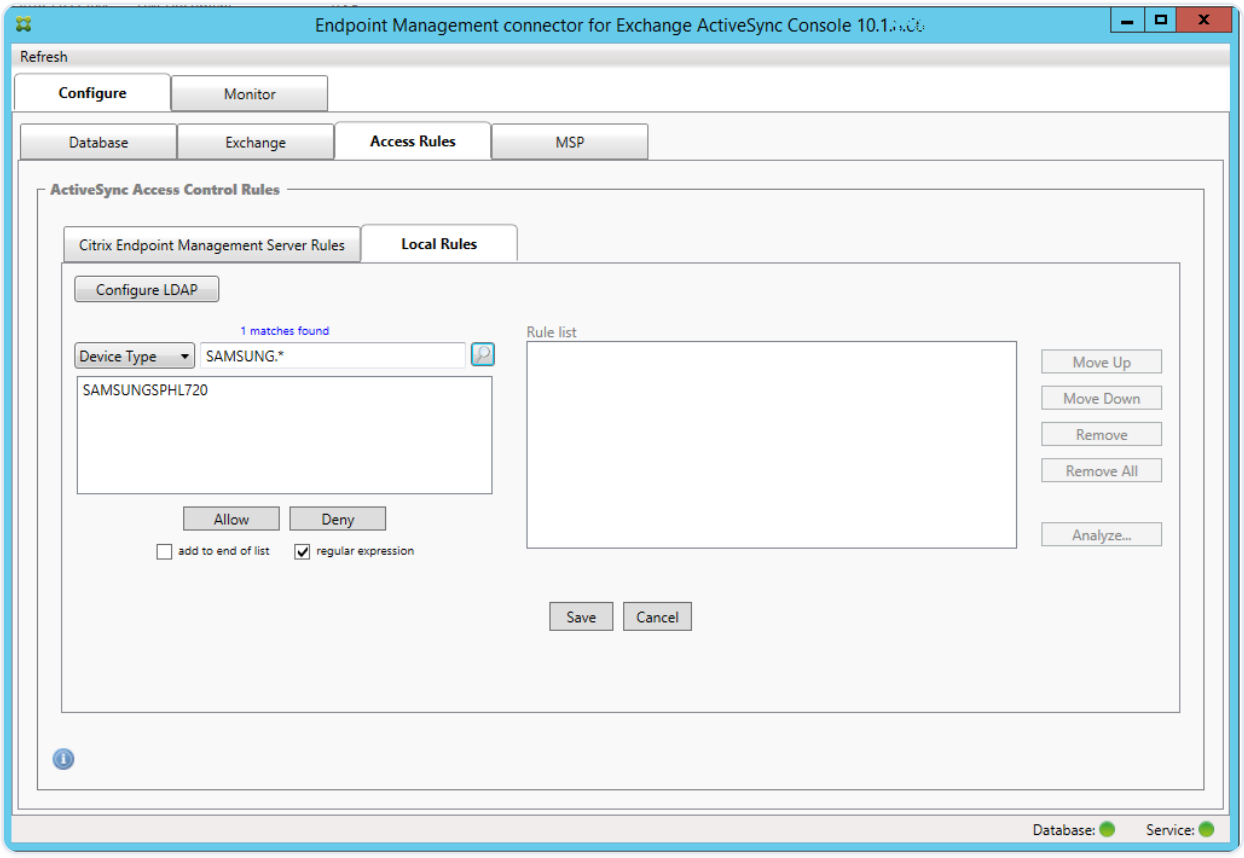
d. **許可**をクリックします。

許可メッセージ(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-accessrules-allow-samsung.png)

アクセスルールを作成するには

1. **ローカルルール**タブをクリックします。
2. 正規表現を入力するには、デバイスIDリストと選択した項目テキストボックスの両方を使用する必要があります。

   アクセスルール(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-local-rule.png)
3. 照合するフィールドを選択します。この例では、**デバイスタイプ**を使用します。
4. 正規表現を入力します。この例では `samsung.*` を使用します。
5. 正規表現のチェックボックスが選択されていることを確認し、**許可**または**拒否**をクリックします。この例では、選択は**許可**に設定されています。最終結果は次のとおりです。

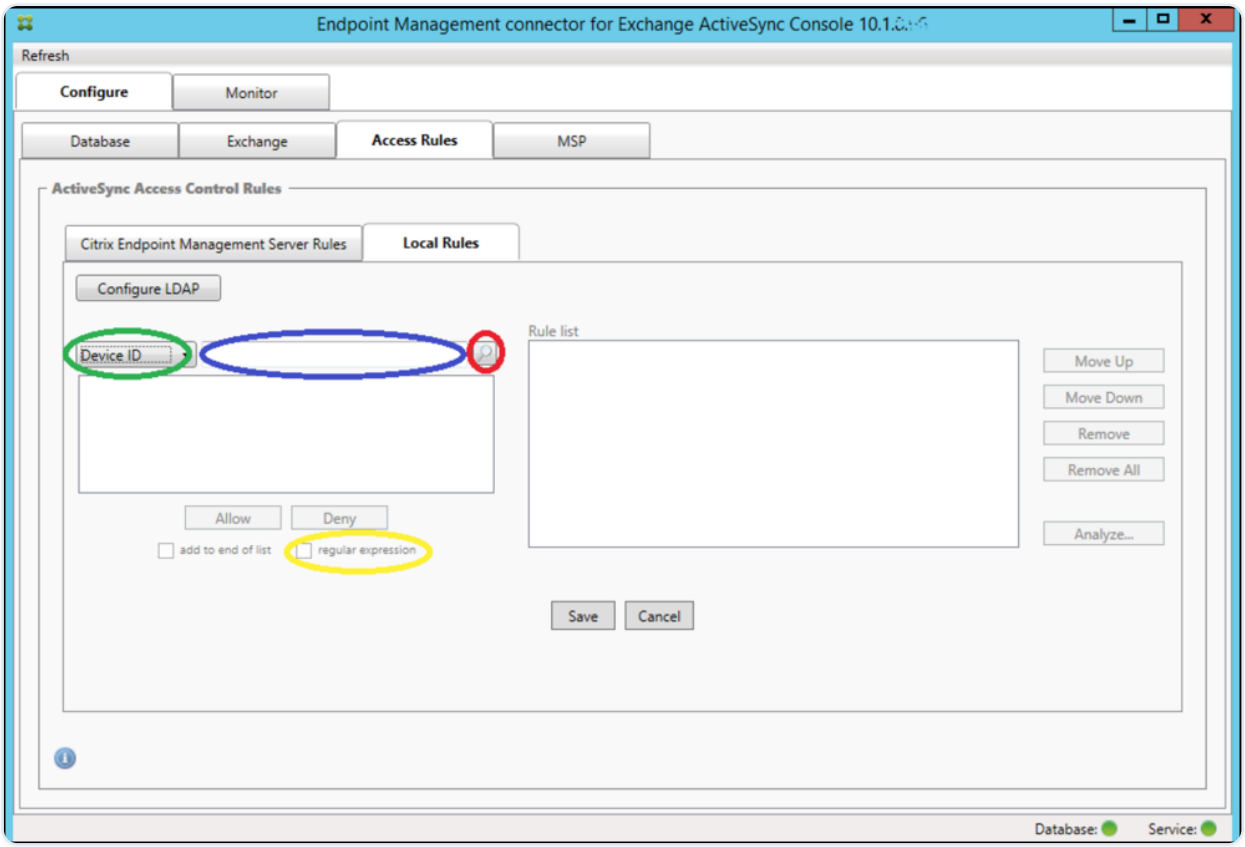


© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスを検索するには

正規表現のチェックボックスを選択すると、指定された表現に一致する特定のデバイスを検索できます。この機能は、メジャースナップショットが正常に完了した場合にのみ利用可能です。正規表現ルールを使用する予定がない場合でも、この機能を使用できます。たとえば、ActiveSyncデバイスIDにテキスト `workmail` を含むすべてのデバイスを検索したいとします。これを行うには、次の手順に従います。

1. **アクセスルール**タブをクリックします。
2. デバイス一致フィールドセレクターが「デバイスID」（デフォルト）に設定されていることを確認します。



3. 選択した項目テキストボックス内（前の図で青色で示されている部分）をクリックし、`workmail.*` と入力します。
4. 正規表現のチェックボックスが選択されていることを確認し、虫眼鏡アイコンをクリックして、次図に示すように一致するものを表示します。

   ](/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-accessrules-localrules-regex.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

個々のユーザー、デバイス、またはデバイスタイプを静的ルールに追加するには

ActiveSyncデバイスタブで、ユーザー、デバイスID、またはデバイスタイプに基づいて静的ルールを追加できます。

1. **ActiveSyncデバイス**タブをクリックします。
2. リストで、ユーザー、デバイス、またはデバイスタイプを右クリックし、選択を許可するか拒否するかを選択します。

   次の画像は、user1が選択されている場合の許可/拒否オプションを示しています。

   許可/拒否オプション(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-devices-allowdeny.png)

デバイスの監視

Citrix Endpoint Management connector for Exchange ActiveSyncの**監視**タブでは、検出されたExchange ActiveSyncおよびBlackBerryデバイスと、発行された自動PowerShellコマンドの履歴を参照できます。**監視**タブには、次の3つのタブがあります。

- **ActiveSyncデバイス:**
  - **エクスポート**ボタンをクリックすると、表示されているActiveSyncデバイスのパートナーシップをエクスポートできます。
  - **ユーザー**、**デバイスID**、または**タイプ**の列を右クリックし、適切な許可またはブロックルールタイプを選択することで、ローカル（静的）ルールを追加できます。
  - 展開された行を折りたたむには、展開された行をCtrlキーを押しながらクリックします。
- **Blackberryデバイス**
- **自動化履歴**

構成タブには、すべてのスナップショットの履歴が表示されます。スナップショット履歴には、スナップショットがいつ実行されたか、かかった時間、検出されたデバイスの数、および発生したエラーが表示されます。

- **Exchange**タブで、目的のExchange Serverの「情報」アイコンをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

トラブルシューティングと診断

Citrix Endpoint Management connector for Exchange ActiveSyncは、エラーおよびその他の運用情報をログファイル *インストールフォルダー*\log\XmmWindowsService.log に記録します。Exchange ActiveSync用コネクタは、重要なイベントをWindowsイベントログにも記録します。

ログレベルを変更するには

Citrix Endpoint Management connector for Exchange ActiveSync には、次のログレベルが含まれています: Error、Info、Warn、Debug、および Trace。

注:

各レベルが上がるごとに、より詳細な情報 (より多くのデータ) が生成されます。たとえば、Error レベルは最も詳細度が低く、Trace レベルは最も詳細度が高くなります。

ログレベルを変更するには、次の手順を実行します。

1. `C:\Program Files\Citrix\Citrix` Citrix Endpoint Management connector で、nlog.config ファイルを開きます。
2. `<rules>` セクションで、*minilevel* パラメーターを希望のログレベルに変更します。例:

```
<rules >



<logger name="*" writeTo="file" minlevel="Debug" />



</rules>
```

3. ファイルを保存します。

   変更はすぐに有効になります。Exchange ActiveSync 用コネクタを再起動する必要はありません。

一般的なエラー

次の一覧には、一般的なエラーが含まれています。

- Exchange ActiveSync サービス用コネクタが起動しない

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ログファイルと Windows イベントログでエラーを確認してください。一般的な原因は次のとおりです。

- Exchange ActiveSync サービス用コネクタが SQL Server にアクセスできません。これは、次の問題が原因である可能性があります。
  - SQL Server サービスが実行されていません。
  - 認証の失敗。

  Windows統合認証が構成されている場合、Exchange ActiveSyncサービス用コネクタのユーザーアカウントは、許可されたSQLログオンである必要があります。Exchange ActiveSyncサービス用コネクタのアカウントはデフォルトでローカルシステムですが、ローカル管理者権限を持つ任意のアカウントに変更できます。SQL認証が構成されている場合、SQLログオンはSQLで適切に構成されている必要があります。

トラブルシューティングツール

トラブルシューティング用のPowerShellユーティリティー式は、**Support\PowerShell**フォルダーにあります。

トラブルシューティングツールは、ユーザーのメールボックスとデバイスの詳細な分析を行い、エラー状態と潜在的な障害領域を検出し、ユーザーの詳細なRBAC分析を行います。すべてのコマンドレットの生出力をテキストファイルに保存できます。

Exchange ActiveSync 用 NetScaler Gateway コネクタ

XenMobile NetScaler Connector は、Exchange ActiveSync 用 NetScaler Gateway コネクタになりました。Citrix 統合ポートフォリオの詳細については、Citrix 製品ガイドを参照してください。

Exchange ActiveSync 用コネクタは、Exchange ActiveSync プロトコルのリバースプロキシとして機能する NetScaler Gateway に対して、ActiveSync クライアントのデバイスレベルの認証サービスを提供します。認証は、以下の組み合わせによって制御します。

- Citrix Endpoint Management で定義するポリシー
- Exchange ActiveSync 用 NetScaler Gateway コネクタによってローカルで定義されるルール

詳しくは、ActiveSync Gatewayを参照してください。

詳細なリファレンスアーキテクチャ図については、アーキテクチャを参照してください。

Exchange ActiveSync 用 NetScaler Gateway コネクタの現在のバージョンは 8.5.3 です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コネクタをダウンロードするには：

1. `<https://www.citrix.com/downloads>` にアクセスします。
2. **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (オンプレミス) > プロダクト ソフトウェア > XenMobile Server 10 > サーバー コンポーネント** に移動します。
3. **NetScaler Gateway Connector** タイルで、**Download File** をクリックします。

コネクタをインストールするには、Exchange ActiveSync 用 NetScaler Gateway コネクタのインストールを参照してください。

重要：

2022年10月以降、Microsoft がこちらで発表した認証変更により、Citrix Endpoint Management および Exchange ActiveSync 用 NetScaler Gateway コネクタは Exchange Online をサポートしなくなります。Exchange 用 Citrix Endpoint Management コネクタは、Microsoft Exchange Server (オンプレミス) で引き続き動作します。

バージョン 8.5.3 の新機能

- このリリースでは、ActiveSync プロトコル 16.0 および 16.1 のサポートが追加されました。
- Google Analytics に送信される分析情報、特にスナップショットに関する詳細が追加されました。

以前のバージョンの新機能

注：

以下の「新機能」セクションでは、Exchange ActiveSync 用 NetScaler Gateway コネクタを旧称の XenMobile NetScaler Connector と呼んでいます。この名称はバージョン 8.5.2 から変更されました。

バージョン 8.5.2 の新機能

- XenMobile NetScaler Connector は、Exchange ActiveSync 用 NetScaler Gateway コネクタになりました。

このバージョンでは、以下の問題が修正されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ポリシー規則の定義に複数の条件が使用され、その条件にユーザー ID が含まれる場合、次の問題が発生する可能性があります。ユーザーが複数のエイリアスを持っている場合、規則の適用時にエイリアスもチェックされません。

バージョン 8.5.1.11 の新機能

- **システム要件の変更:** 現在のバージョンの NetScaler Connector には、Microsoft .NET Framework 4.5 が必要です。
- **Google Analytics のサポート:** お客様がコネクタをどのように使用しているかを知ることで、製品をより良くできる点に注力したいと考えています。
- **TLS 1.1 および 1.2 のサポート:** セキュリティの脆弱化のため、PCI Council は TLS 1.0 および TLS 1.1 を非推奨にしています。XenMobile NetScaler Connector に TLS 1.2 のサポートが追加されました。

Exchange ActiveSync 用 NetScaler Gateway コネクタの監視

Exchange ActiveSync 用 NetScaler Gateway コネクタの構成ユーティリティは、詳細なログを提供します。ログを使用して、Secure Mobile Gateway が許可またはブロックする、Exchange Server を通過するすべてのトラフィックを表示できます。

ログタブを使用して、承認のために Exchange ActiveSync 用コネクタに転送された ActiveSync リクエストの履歴を表示します。

また、Exchange ActiveSync Web サービス用コネクタが実行されていることを確認するには、コネクタサーバーのブラウザに次の URL を読み込みます `https://<host:port>/services/ActiveSync/Version`。URL が製品バージョンを文字列として返した場合、Web サービスは応答しています。

Exchange ActiveSync 用コネクタで ActiveSync トラフィックをシミュレートするには

NetScaler Gateway connector for Exchange ActiveSync を使用して、ポリシーで ActiveSync トラフィックをシミュレートできます。コネクタ構成ユーティリティで、**シミュレーター**タブをクリックします。結果には、構成したルールに従ってポリシーがどのように適用されるかが表示されます。

Exchange ActiveSync 用コネクタのフィルターを選択する

NetScaler Gateway connector for Exchange ActiveSync のフィルターは、特定のポリシー違反またはプロパティ設定についてデバイスを分析することで機能します。デバイスが基準を満たしている場合、そのデバイスはデバイスリストに配置されます。このデバイスリストは、許可リストでも

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ブロックリストでもありません。定義された基準を満たすデバイスのリストです。Citrix Endpoint Management 内の Exchange ActiveSync 用コネクタには、次のフィルターが利用可能です。各フィルターの2つのオプションは、**許可**または**拒否**です。

- **匿名デバイス:** Citrix Endpoint Management に登録されているが、ユーザーのIDが不明なデバイスを許可または拒否します。たとえば、登録済みユーザーのActive Directoryパスワードの期限が切れている場合や、資格情報が不明な場合、そのユーザーのIDは不明です。
- **禁止アプリ:** ポリシーのブロックリストで定義されたデバイスリストと、ブロックリスト上のアプリの存在に基づいてデバイスを許可または拒否します。
- **暗黙的な許可/拒否:** 他のどのフィルター規則の基準も満たさないすべてのデバイスのデバイスリストを作成し、そのリストに基づいて許可または拒否します。暗黙的な許可/拒否オプションは、 タブの Exchange ActiveSync 用コネクタのステータスが有効になっており、デバイスのコネクタステータスが表示されることを確認します。暗黙的な許可/拒否オプションは、選択されていない他のすべてのコネクタフィルターも制御します。たとえば、コネクタはブロックリスト上のアプリを拒否します。ただし、暗黙的な許可/拒否オプションが**許可**に設定されているため、コネクタは他のすべてのフィルターを許可します。
- **非アクティブなデバイス:** 指定された時間内に Citrix Endpoint Management と通信していないデバイスのデバイスリストを作成します。これらのデバイスは非アクティブと見なされます。フィルターは、それに応じてデバイスを許可または拒否します。
- **不足している必須アプリ:** ユーザーが登録すると、インストールする必要がある必須アプリのリストを受け取ります。不足している必須アプリフィルターは、1つ以上のアプリが存在しなくなったことを示します。たとえば、ユーザーが1つ以上のアプリを削除した場合などです。
- **推奨されないアプリ:** ユーザーが登録すると、インストールするアプリのリストを受け取ります。推奨されないアプリフィルターは、そのリストにないアプリをデバイスで確認します。
- **非準拠パスワード:** デバイスにパスコードがないすべてのデバイスのデバイスリストを作成します。
- **コンプライアンス違反デバイス:** 独自の内部ITコンプライアンス基準を満たすデバイスを拒否または許可できます。コンプライアンスは、**True**または**False**のいずれかになるブール型フラグである「Out of Compliance」という名前のデバイスプロパティによって定義される任意の設置です。（このプロパティは手動で作成して値を設定できます。または、自動アクションを使用して、デバイスが特定の基準を満たしているかどうかに基づいて、デバイス上にこのプロパティを作成することもできます。）
    - **準拠違反 = True:** デバイスがIT部門によって設定された準拠基準およびポリシー定義を満たしていない場合、そのデバイスは準拠違反となります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **準拠違反 = False:** デバイスがIT部門によって設定された準拠基準およびポリシー定義を満たしている場合、そのデバイスは準拠しています。

- **取り消し済みステータス:** 取り消し済みのすべてのデバイスのデバイスリストを作成し、取り消し済みステータスに基づいて許可または拒否します。
- **ルート化されたAndroid/ジェイルブレイクされたiOSデバイス:** ルート化済みとしてフラグ付けされたすべてのデバイスのデバイスリストを作成し、ルート化済みステータスに基づいて許可または拒否します。
- **管理対象外デバイス:** Citrix Endpoint Managementデータベース内のすべてのデバイスのデバイスリストを作成します。モバイルアプリケーションゲートウェイをブロックモードで展開します。

Exchange ActiveSync 用 NetScaler Gateway コネクタへの接続を構成するには

Exchange ActiveSync 用 NetScaler Gateway コネクタは、Citrix Secure Web Services を介して Citrix Endpoint Management およびその他のリモート構成プロバイダーと通信します。

1. Exchange ActiveSync 構成ユーティリティのコネクタで、**Config Providers** タブをクリックし、**Add** をクリックします。
2. **Config Providers** ダイアログボックスの **Name** に、管理者権限を持ち、Citrix Endpoint Managementサーバーとの基本的なHTTP認証に使用されるユーザー名を入力します。
3. **Url** に、Citrix Endpoint Management GCS の Web アドレスを入力します。通常、形式は `https://<FQDN>/<instanceName>/services/<MagConfigService>` です。*MagConfigService* の名前は大文字と小文字を区別します。
4. **Password** に、Citrix Endpoint Managementサーバーとの基本的なHTTP認証に使用するパスワードを入力します。
5. **Managing Host** に、Exchange ActiveSync サーバー名のコネクタを入力します。
6. **Baseline Interval** に、Citrix Endpoint Management から新しく更新された動的ルールセットをプルする期間を指定します。
7. **Delta interval** に、動的ルールの更新をプルする期間を指定します。
8. **Request Timeout** に、サーバー要求のタイムアウト間隔を指定します。
9. 「**Config Provider**」で、構成プロバイダーサーバーインスタンスがポリシー構成を提供しているかどうかを選択します。
10. 「**Events Enabled**」で、Exchange ActiveSync 用コネクタがデバイスがブロックされたときに Citrix Endpoint Management に通知するようにする場合は、このオプションを有効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management の自動アクションでコネクタルールを使用している場合、このオプションは必須です。

11. 「**Save**」をクリックし、次に「**Test Connectivity**」をクリックして、ゲートウェイと構成プロバイダー間の接続をテストします。接続に失敗した場合は、ローカルファイアウォール設定が接続を許可しているか確認するか、管理者に問い合わせてください。
12. 接続が成功したら、「**Disabled**」チェックボックスをオフにして、「**Save**」をクリックします。

構成プロバイダーを追加すると、Exchange ActiveSync 用コネクタは、そのプロバイダーに関連付けられた1つ以上のポリシーを自動的に作成します。`NewPolicyTemplate` セクションの `config\policyTemplates.xml` に含まれるテンプレート定義がポリシーを定義します。このセクション内で定義されているポリシー要素ごとに、新しいポリシーが作成されます。

次の条件が満たされている場合、オペレーターはポリシー要素を追加、削除、または変更できます。ポリシー要素がスキーマ定義に準拠しており、標準の置換文字列（中括弧で囲まれたもの）が変更されていないこと。次に、プロバイダーの新しいグループを追加し、新しいグループを含めるようにポリシーを更新します。

Citrix Endpoint Management からポリシーをインポートするには

1. Exchange ActiveSync 構成ユーティリティのコネクタで、「**Config Providers**」タブをクリックし、「**Add**」をクリックします。
2. 「**Config Providers**」ダイアログボックスの「**Name**」に、Citrix Endpoint Management との基本 HTTP 認証用のユーザー名を入力します。このユーザーは管理者権限を持っている必要があります。
3. 「**Url**」に、Citrix Endpoint Management Gateway Configuration Service (GCS) の Web アドレスを入力します。通常、形式は `https://<xdmHost>/xdm/services/<MagConfigService>` です。MagConfigService の名前は大文字と小文字を区別します。
4. 「**Password**」に、Citrix Endpoint Management サーバーとの基本 HTTP 認証に使用するパスワードを入力します。
5. 「**Test Connectivity**」をクリックして、ゲートウェイと構成プロバイダー間の接続をテストします。接続に失敗した場合は、ローカルファイアウォール設定が接続を許可しているか確認するか、管理者に確認してください。
6. 接続が正常に確立されたら、「**Disabled**」チェックボックスをオフにして、「**Save**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. 「**Managing Host**」では、ローカルホストコンピューターのデフォルトの DNS 名をそのままにします。この設定は、複数の Forefront Threat Management Gateway (TMG) サーバーがアレイで構成されている場合に、Citrix Endpoint Management との通信を調整するために使用されます。

   設定を保存したら、GCS を開きます。

NetScaler Gateway connector for Exchange ActiveSync のポリシーモードの構成

NetScaler Gateway connector for Exchange ActiveSync は、次の6つのモードで実行できます。

- **すべて許可:** このポリシーモードは、Exchange ActiveSync 用コネクタを通過するすべてのトラフィックへのアクセスを許可します。他のフィルタリングルールは使用されません。
- **すべて拒否:** このポリシーモードは、Exchange ActiveSync 用コネクタを通過するすべてのトラフィックへのアクセスをブロックします。他のフィルタリングルールは使用されません。
- **静的ルール: ブロックモード:** このポリシーモードは、最後に暗黙的な拒否またはブロックステートメントを含む静的ルールを実行します。Exchange ActiveSync 用コネクタは、他のフィルタールールによって許可または許可されていないデバイスをブロックします。
- **静的ルール: 許可モード:** このポリシーモードは、最後に暗黙的な許可ステートメントを含む静的ルールを実行します。他のフィルタールールによってブロックまたは拒否されていないデバイスは、Exchange ActiveSync 用コネクタを介して許可されます。
- **静的 + ZDM ルール**: ブロックモード。このポリシーモードは、最初に静的ルールを実行し、次にCitrix Endpoint Managementからの動的ルールを、最後に暗黙的な拒否またはブロックステートメントとともに実行します。デバイスは、定義されたフィルターとCitrix Endpoint Managementルールに基づいて許可または拒否されます。定義されたフィルターとルールに一致しないデバイスはすべてブロックされます。
- **静的 + ZDM ルール**: 許可モード。このポリシーモードは、最初に静的ルールを実行し、次にCitrix Endpoint Managementからの動的ルールを、最後に暗黙的な許可ステートメントとともに実行します。デバイスは、定義されたフィルターとCitrix Endpoint Managementルールに基づいて許可または拒否されます。定義されたフィルターとルールに一致しないデバイスはすべて許可されます。

Exchange ActiveSync プロセス用コネクタは、Citrix Endpoint Management から受信した iOS および Windows ベースのモバイルデバイスの一意の ActiveSync ID に基づいて、動的ルールを許可またはブロックします。Android デバイスは製造元によって動作が異なり、一意の ActiveSync ID を容易に公開しないものもあります。これを補うため、Citrix Endpoint Management は Android デバイスのユーザー ID 情報を送信して、許可またはブロックの決定を行います。その結果、ユー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ザーが Android デバイスを1台しか持っていない場合、許可とブロックは正常に機能します。ユーザーが複数の Android デバイスを持っている場合、Android デバイスを区別できないため、すべてのデバイスが許可されます。既知の場合、ActiveSyncID によってこれらのデバイスを静的にブロックするようにゲートウェイを構成できます。また、デバイスの種類またはユーザーエージェントに基づいてブロックするようにゲートウェイを構成することもできます。

ポリシーモードを指定するには、SMG Controller Configuration ユーティリティで、次の手順を実行します。

1. **Path Filters** タブをクリックし、次に **Add** をクリックします。
2. **Path Properties** ダイアログボックスで、**Policy** リストからポリシーモードを選択し、次に **Save** をクリックします。

構成ユーティリティの **Policies** タブでルールを確認できます。ルールは、Exchange ActiveSync用コネクタで上から下へ処理されます。許可ポリシーは緑色のチェックマークで表示されます。拒否ポリシーは、線が引かれた赤い丸で表示されます。画面を更新して最新のルールを表示するには、**Refresh** をクリックします。config.xml ファイルでルールの順序を変更することもできます。

ルールをテストするには、**Simulator** タブをクリックします。フィールドに値を指定します。値はログから取得できます。結果メッセージには、許可またはブロックが指定されます。

静的ルールを構成するには

ActiveSync接続のHTTPリクエストのISAPIフィルタリングが読み取る値で静的ルールを入力します。静的ルールにより、Exchange ActiveSync用コネクタは次の基準でトラフィックを許可またはブロックできます。

- **ユーザー:** Exchange ActiveSync用コネクタは、デバイス登録中に取得された認証済みユーザーの値と名前の構造を使用します。この構造は、LDAP経由でActive Directoryに接続されたCitrix Endpoint Managementを実行しているサーバーによって参照される`domain\username`として一般的に見られます。コネクタ構成ユーティリティの**ログ**タブには、コネクタを通過する値が表示されます。コネクタが値の構造を決定する必要がある場合、または構造が異なる場合に、値が渡されます。
- **DeviceID (ActiveSyncID):** 接続されているデバイスのActiveSyncIDとしても知られています。この値は、Citrix Endpoint Managementコンソールの特定のデバイスプロパティページで一般的に見られます。この値は、Exchange ActiveSync構成ユーティリティのコネクタの**ログ**タブからも確認できます。
- **DeviceType:** Exchange ActiveSync用コネクタは、デバイスがiPhone、iPad、またはその他のデバイスタイプであるかを判断し、その基準に基づいて許可またはブロックできます。他の値

© 1997–2026 Citrix Systems, Inc. All rights reserved.

と同様に、コネクタ構成ユーティリティは、ActiveSync接続のために処理されているすべての接続済みデバイスタイプを明らかにできます。

- **UserAgent:** 使用されているActiveSyncクライアントに関する情報が含まれます。通常、指定された値は、モバイルデバイスプラットフォームの特定のオペレーティングシステムのビルドとバージョンに対応します。

サーバー上で実行されているExchange ActiveSync構成ユーティリティのコネクタが、常に静的ルールを管理します。

1. SMG Controller Configurationユーティリティで、**Static Rules**タブをクリックし、**Add**をクリックします。
2. **Static Rule Properties**ダイアログボックスで、基準として使用する値を指定します。たとえば、ユーザー名（例：AllowedUser）を入力してアクセスを許可するユーザーを入力し、**Disabled**チェックボックスをオフにすることができます。
3. **Save**をクリックします。

   静的ルールが有効になりました。また、正規表現を使用して値を定義することもできますが、その場合はconfig.xmlファイルでルール処理モードを有効にする必要があります。

動的ルールを構成するには

Citrix Endpoint Managementのデバイスポリシーとプロパティは動的ルールを定義し、Exchange ActiveSyncフィルター用の動的コネクタをトリガーできます。トリガーは、ポリシー違反またはプロパティ設定の有無に基づいています。Exchange ActiveSync用コネクタフィルターは、特定のポリシー違反またはプロパティ設定についてデバイスを分析することで機能します。デバイスが基準を満たしている場合、そのデバイスはデバイスリストに配置されます。このデバイスリストは、許可リストでもブロックリストでもありません。定義された基準を満たすデバイスのリストです。以下の構成オプションを使用すると、Exchange ActiveSync用コネクタを使用して、デバイスリスト内のデバイスを許可するか拒否するかを定義できます。

注：

動的ルールを構成するには、Citrix Endpoint Managementコンソールを使用します。

1. Citrix Endpoint Managementコンソールで、右上隅の歯車アイコンをクリックします。**Settings**ページが表示されます。
2. 「**サーバー**」の下で、「**ActiveSync Gateway**」をクリックします。ActiveSync Gatewayページが表示されます。
3. 「**次のルールをアクティブ化**」で、アクティブ化するルールを1つ以上選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Androidのみの場合、「**AndroidドメインユーザーをActiveSync Gatewayに送信**」で「**はい**」をクリックして、Citrix Endpoint ManagementがAndroidデバイス情報をSecure Mobile Gatewayに送信するようにします。

   このオプションを有効にすると、Citrix Endpoint Managementがデバイスユーザーの ActiveSync識別子を持っていない場合、Citrix Endpoint ManagementはAndroidデバイス情報をコネクタに送信します。

Exchange ActiveSync XMLファイルのコネクタを編集してカスタムポリシーを構成するには

Exchange ActiveSync構成ユーティリティのコネクタの「**ポリシー**」タブで、デフォルト構成の基本ポリシーを表示できます。カスタムポリシーを作成する場合は、Exchange ActiveSync XML構成ファイル (config\config.xml) のNetScaler Gatewayコネクタを編集できます。

1. ファイル内の「**PolicyList**」セクションを見つけ、新しい「**Policy**」要素を追加します。
2. 新しいグループも必要な場合（たとえば、別の静的グループや別のGCPをサポートするグループなど）は、新しい「**Group**」要素を「**GroupList**」セクションに追加します。
3. 必要に応じて、「**GroupRef**」要素を並べ替えることで、既存のポリシー内のグループの順序を変更できます。

Exchange ActiveSync XMLファイルのコネクタの構成

Exchange ActiveSync用コネクタは、コネクタの動作を指示するためにXML構成ファイルを使用します。他のエントリの中でも、このファイルは、HTTPリクエストを評価する際にフィルターが実行するグループファイルと関連アクションを指定します。デフォルトでは、ファイル名はconfig.xmlで、次の場所にあります: ..\Program Files\Citrix\XenMobile NetScaler Connector\config\.

GroupRefノード

GroupRefノードは論理グループ名を定義します。デフォルトはAllowGroupとDenyGroupです。

注：

GroupRefListノードに表示されるGroupRefノードの順序は重要です。

GroupRefノードのID値は、特定のユーザーアカウントまたはデバイスを照合するために使用されるメンバーの論理コンテナまたはコレクションを識別します。アクション属性は、フィルターがコレクション内のルールに一致するメンバーをどのように処理するかを指定します。たとえば、AllowGroupセットのルールに一致するユーザーアカウントまたはデバイスは「パス」します。パスするとは、Exchange CASへのアクセスが許可されることを意味します。DenyGroupセットの

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ルールに一致するユーザーアカウントまたはデバイスは「拒否」されます。拒否されるとは、Exchange CASへのアクセスが許可されないことを意味します。

特定のユーザーアカウント/デバイスまたはその組み合わせが両方のグループのルールを満たす場合、リクエストの結果を決定するために優先順位の規則が使用されます。優先順位は、config.xmlファイル内のGroupRefノードの順序（上から下）に具現化されます。GroupRefノードは優先順位順にランク付けされます。Allowグループ内の特定の条件に対するルールは、常にDenyグループ内の同じ条件に対するルールよりも優先されます。

グループノード

また、config.xmlはグループノードを定義します。これらのノードは、論理コンテナであるAllowGroupとDenyGroupを外部XMLファイルにリンクします。外部ファイルに保存されているエントリは、フィルター規則の基礎となります。

注：

このバージョンでは、外部XMLファイルのみがサポートされています。

デフォルトのインストールでは、構成に2つのXMLファイル（allow.xmlとdeny.xml）が実装されます。

Exchange ActiveSync 用 NetScaler Gateway コネクタの構成

Exchange ActiveSync 用 NetScaler Gateway コネクタを構成して、次のプロパティに基づいてActiveSyncリクエストを選択的にブロックまたは許可できます。**Active Sync Service ID**、**デバイスの種類**、**ユーザーエージェント**（デバイスのオペレーティングシステム）、**承認済みユーザー**、および**ActiveSyncコマンド**。

デフォルトの構成では、静的グループと動的グループの組み合わせがサポートされています。静的グループは、SMG Controller Configurationユーティリティを使用して維持します。静的グループは、特定のユーザーエージェントを使用するすべてのデバイスなど、既知のデバイスカテゴリで構成できます。

Gateway Configuration Providerと呼ばれる外部ソースが動的グループを維持します。Exchange ActiveSync用コネクタは、定期的にグループを接続します。Citrix Endpoint Managementは、許可されたデバイスとブロックされたデバイスおよびユーザーのグループをExchange ActiveSync用コネクタにエクスポートできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway Configuration Providerと呼ばれる外部ソースが動的グループを維持します。Exchange ActiveSync用コネクタは、動的グループを定期的に収集します。Citrix Endpoint Managementは、許可されたデバイスとブロックされたデバイスおよびユーザーのグループをコネクタにエクスポートできます。

ポリシーは、各グループに関連付けられたアクション（許可またはブロック）とグループメンバーのリストを持つ、順序付けられたグループのリストです。ポリシーには任意の数のグループを含めることができます。ポリシー内のグループの順序は重要です。なぜなら、一致が見つかるとそのグループのアクションが実行され、後続のグループは評価されないためです。

メンバーは、リクエストのプロパティを照合する方法を定義します。デバイスIDなどの単一のプロパティ、またはデバイスタイプやユーザーエージェントなどの複数のプロパティを照合できます。

Exchange ActiveSync 用 NetScaler Gateway コネクタのセキュリティモデルの選択

セキュリティモデルの確立は、あらゆる規模の組織にとって、モバイルデバイスの展開を成功させるために不可欠です。デフォルトでユーザー、コンピューター、またはデバイスへのアクセスを許可するために、保護されたネットワーク制御または隔離されたネットワーク制御を使用するのが一般的です。この方法は常に理想的であるとは限りません。ITセキュリティを管理するすべての組織は、モバイルデバイスのセキュリティに対して、わずかに異なる、またはカスタマイズされたアプローチを持っている可能性があります。

同じ論理がモバイルデバイスのセキュリティにも当てはまります。許可モデルを使用することは、多数のモバイルデバイスと種類、ユーザーあたりのモバイルデバイス、および利用可能なオペレーティングシステムプラットフォームとアプリがあるため、弱い選択肢です。ほとんどの組織では、制限モデルが最も論理的な選択肢です。

CitrixがExchange ActiveSync用コネクタをCitrix Endpoint Managementと統合するために許可する構成シナリオは次のとおりです。

許可モデル (許可モード)

許可セキュリティモデルは、デフォルトですべてが許可されるか、アクセスが許可されるという前提で動作します。ルールとフィルタリングによってのみ、何かがブロックされ、制限が適用されます。許可セキュリティモデルは、モバイルデバイスに関するセキュリティ上の懸念が比較的緩い組織に適しています。このモデルは、適切な場合にのみアクセスを拒否するための制限的な制御を適用します (ポリシー規則が失敗した場合)。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

制限モデル (ブロックモード)

制限セキュリティモデルは、デフォルトでは何も許可されない、またはアクセスが許可されないという前提に基づいています。セキュリティチェックポイントを通過するすべてのものはフィルタリングおよび検査され、アクセスを許可するルールが通過しない限り、アクセスは拒否されます。制限セキュリティモデルは、モバイルデバイスに関するセキュリティ基準が比較的厳しい組織に適しています。このモードは、アクセスを許可するすべてのルールが通過した場合にのみ、ネットワークサービスでの使用と機能へのアクセスを許可します。

Exchange ActiveSync用NetScaler Gatewayコネクタの管理

Exchange ActiveSync 用 NetScaler Gateway コネクタを使用して、アクセス制御ルールを構築できます。これらのルールは、管理対象デバイスからの ActiveSync 接続要求へのアクセスを許可またはブロックします。アクセスは、デバイスの状態、アプリの許可/ブロックリスト、およびその他のコンプライアンス条件に基づいています。

Exchange ActiveSync構成ユーティリティ用コネクタを使用すると、企業の電子メールポリシーを適用する動的および静的ルールを構築できます。これらのルールとポリシーにより、コンプライアンス基準に違反しているユーザーをブロックできます。また、電子メール添付ファイルの暗号化を設定して、Exchange Serverを介して管理対象デバイスに渡されるすべての添付ファイルが暗号化されるようにすることもできます。暗号化された添付ファイルは、管理対象デバイスを持つ承認されたユーザーのみが表示できます。

XNCをアンインストールするには

1. 管理者アカウントでXncInstaller.exeを実行します。
2. 画面の指示に従ってアンインストールを完了します。

Exchange ActiveSync用コネクタをインストール、アップグレード、またはアンインストールするには

1. 管理者アカウントでXncInstaller.exeを実行して、Exchange ActiveSync用コネクタをインストールするか、既存のコネクタのアップグレードまたは削除を許可します。
2. 画面の指示に従って、インストール、アップグレード、またはアンインストールを完了してください。

Exchange ActiveSync 用コネクタをインストールした後、Citrix Endpoint Management 構成サービスと通知サービスを手動で再起動する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exchange ActiveSync 用 NetScaler Gateway コネクタのインストール

Exchange ActiveSync 用コネクタは、専用のサーバーにインストールすることも、Citrix Endpoint Management をインストールしたサーバーと同じサーバーにインストールすることもできます。

次の理由により、Exchange ActiveSync 用コネクタを専用のサーバー (Citrix Endpoint Management とは別) にインストールすることを検討できます。

- Citrix Endpoint Management サーバーがクラウドにリモートでホストされている場合 (物理的な場所)
- Citrix Endpoint Management サーバーの再起動が Exchange ActiveSync 用コネクタに影響を与えないようにしたい場合 (可用性)
- サーバーのシステムリソースをすべて Exchange ActiveSync 用コネクタに割り当てたい場合 (パフォーマンス)

Exchange ActiveSync 用コネクタがサーバーにかける CPU 負荷は、管理されるデバイスの数によって異なります。コネクタが Citrix Endpoint Management と同じサーバーに展開されている場合、CPU コアをもう 1 つ追加することが一般的な推奨事項です。多数のデバイス (50,000 を超える) の場合、クラスター環境がない場合は、より多くのコアをプロビジョニングする必要があるかもしれません。コネクタのメモリフットプリントは、より多くのメモリを必要とするほど重要ではありません。

Exchange ActiveSync 用 NetScaler Gateway コネクタのシステム要件

Exchange ActiveSync 用 NetScaler Gateway コネクタは、NetScaler Gateway アプライアンスで構成された SSL ブリッジを介して NetScaler Gateway と通信します。このブリッジにより、アプライアンスはすべてのセキュアなトラフィックを Citrix Endpoint Management に直接ブリッジできます。Exchange ActiveSync 用コネクタの最小システム構成は次のとおりです。

コンポーネント	要件
コンピューターとプロセッサー	733 MHz Pentium III 733 MHz 以上のプロセッサー。2.0 GHz Pentium III 以上のプロセッサー (推奨)
シトリックス ゲートウェイ	ソフトウェアバージョン10のCitrix Gatewayアプライアンス
メモリ	1 GB

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コンポーネント	要件
ハードディスク	150 MBの空きハードディスク容量を持つNTFSフォーマットのローカルパーティション
オペレーティングシステム	Windows Server 2016、Windows Server 2012 R2、またはWindows Server 2008 R2 Service Pack 1。英語ベースのサーバーである必要があります。Windows Server 2008 R2 Service Pack 1のサポートはJanuary 14, 2020に終了し、Windows Server 2012 R2のサポートはOctober 10, 2023に終了します。
その他のデバイス	内部ネットワークとの通信のためのホストオペレーティングシステムと互換性のあるネットワークアダプター
マイクロソフト .NET Framework	バージョン8.5.1.11にはMicrosoft .NET Framework 4.5が必要です。
ディスプレイ	VGAまたはそれ以上の解像度のモニター

Exchange ActiveSync用コネクタのホストコンピューターには、以下の最小空きハードディスク容量が必要です。

- **アプリケーション:** 10〜15 MB (100 MBを推奨)
- **ログ:** 1 GB (20 GBを推奨)

Exchange ActiveSync用コネクタのプラットフォームサポートについては、「サポートされているデバイスのオペレーティングシステム」を参照してください。

デバイスのメールクライアント

すべてのメールクライアントが、デバイスに対して常に同じActiveSync IDを返すわけではありません。Exchange ActiveSync用コネクタは、各デバイスに対して一意のActiveSync IDを期待するため、次のことが言えます。各デバイスに対して常に同じ一意のActiveSync IDを生成するメールクライアントのみがサポートされます。Citrixはこれらのメールクライアントをテストしており、エラーなしで動作しました。

- Samsungネイティブメールクライアント
- iOSネイティブメールクライアント

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネットスケーラー ゲートウェイ コネクタ Exchange ActiveSync 用の展開

NetScaler Gateway connector for Exchange ActiveSyncを使用すると、NetScaler Gatewayを使用して、Citrix Endpoint Management管理対象デバイスとのCitrix Endpoint Managementサーバー通信をプロキシおよび負荷分散できます。Exchange ActiveSync用コネクタは、Citrix Endpoint Managementと定期的に通信してポリシーを同期します。Exchange ActiveSync用コネクタとCitrix Endpoint Managementを、まとめて、または個別にクラスター化できます。

Exchange ActiveSync用コネクタのコンポーネント

- **Exchange ActiveSync用コネクタサービス:** このサービスは、NetScaler Gatewayが呼び出して、デバイスからのActiveSync要求が承認されているかどうかを判断できるREST Webサービスインターフェイスを提供します。
- **Citrix Endpoint Management構成サービス:** このサービスはCitrix Endpoint Managementと通信し、Citrix Endpoint Managementのポリシー変更をExchange ActiveSync用コネクタと同期します。
- **Citrix Endpoint Management通知サービス:** このサービスは、不正なデバイスアクセスに関する通知をCitrix Endpoint Managementに送信します。この方法により、Citrix Endpoint Managementは、デバイスがブロックされた理由をユーザーに通知するなどの適切な措置を講じることができます。
- **Exchange ActiveSync用コネクタ構成ユーティリティ:** このアプリケーションを使用すると、管理者はExchange ActiveSync用コネクタを構成および監視できます。

NetScaler Gateway connector for Exchange ActiveSyncのリスニングアドレスを設定するには

NetScaler Gateway connector for Exchange ActiveSyncがNetScaler GatewayからのActiveSyncトラフィックを承認するリクエストを受信するには、次の手順を実行します。Exchange ActiveSync用コネクタがNetScaler Gateway Webサービスコールをリッスンするポートを指定します。

1. 「**スタート**」メニューから、Exchange ActiveSync構成ユーティリティ用のコネクタを選択します。
2. 「**Web Service**」タブをクリックし、コネクタWebサービスのリッスンアドレスを入力します。「**HTTP**」または「**HTTPS**」のいずれか、あるいは両方を選択できます。Exchange ActiveSync用コネクタがCitrix Endpoint Managementと共存している（同じサーバーにインストールされている）場合は、Citrix Endpoint Managementと競合しないポート値を選択してください。
3. 値を設定したら、「**Save**」をクリックし、次に「**Start Service**」をクリックしてWebサービスを開始します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway connector for Exchange ActiveSyncでデバイスアクセスコントロールポリシーを構成するには

管理対象デバイスに適用するアクセスコントロールポリシーを構成するには、次の手順を実行します。

1. Exchange ActiveSync構成ユーティリティのコネクタで、「**Path Filters**」タブをクリックします。
2. 最初の行「**Microsoft-Server-ActiveSync is for ActiveSync**」を選択し、「**Edit**」をクリックします。
3. 「**Policy**」リストから、目的のポリシーを選択します。Citrix Endpoint Managementポリシーを含むポリシーの場合は、「**Static + ZDM: Permit Mode or Static + ZDM: Block Mode**」を選択します。これらのポリシーは、ローカル（または静的）ルールとCitrix Endpoint Managementからのルールを組み合わせたものです。Permit Modeは、ルールによって明示的に識別されていないすべてのデバイスがActiveSyncへのアクセスを許可されることを意味します。Block Modeは、そのようなデバイスがブロックされることを意味します。
4. ポリシーを設定したら、「**Save**」をクリックします。

Citrix Endpoint Managementとの通信を構成するには

NetScaler Gateway connector for Exchange ActiveSyncおよびNetScaler Gatewayで使用するCitrix Endpoint Managementサーバーの名前とプロパティを指定します。

> **注：**
>
> このタスクは、Citrix Endpoint Managementをすでにインストールおよび構成していることを前提としています。Exchange ActiveSync構成ユーティリティでは、Citrix Endpoint ManagementをConfig Providerという用語で表します。

1. Exchange ActiveSync構成ユーティリティのコネクタで、「**Config Providers**」タブをクリックし、「**Add**」をクリックします。
2. この展開で使用しているCitrix Endpoint Managementサーバーの名前とURLを入力します。マルチテナント展開で複数のCitrix Endpoint Managementサーバーを展開している場合、この名前は各サーバーインスタンスで一意である必要があります。
3. **URL** に、Citrix Endpoint Management GlobalConfig Provider (GCP) のWebアドレスを入力します。通常、形式は `https://<FQDN>/<instanceName>/services/<MagConfigService>` です。*MagConfigService* の名前は大文字と小文字を区別します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. **パスワード** に、Citrix Endpoint Management Webサーバーとの基本的なHTTP認証に使用するパスワードを入力します。
5. **管理ホスト** に、Exchange ActiveSync 用コネクタをインストールしたサーバー名を入力します。
6. **ベースライン間隔** に、Citrix Endpoint Management から新しい更新された動的ルールセットがプルされる期間を指定します。
7. **要求タイムアウト** に、サーバー要求のタイムアウト間隔を指定します。
8. **構成プロバイダー** で、構成プロバイダーサーバーインスタンスがポリシー構成を提供するかどうかを選択します。
9. **イベント有効** で、デバイスがブロックされたときにSecure Mobile GatewayがCitrix Endpoint Managementに通知するようにする場合は、このオプションを有効にします。このオプションは、Citrix Endpoint Managementの自動アクションでSecure Mobile Gatewayルールを使用している場合に必要です。
10. サーバーを構成したら、**接続テスト** をクリックしてCitrix Endpoint Managementへの接続をテストします。
11. 接続が確立されたら、**保存** をクリックします。

冗長性とスケーラビリティのためのExchange ActiveSync用NetScaler Gatewayコネクタの展開

Exchange ActiveSync用NetScaler GatewayコネクタとCitrix Endpoint Management展開をスケーリングするには、複数のWindows ServerにExchange ActiveSync用コネクタのインスタンスをインストールできます。すべてのコネクタインスタンスは同じCitrix Endpoint Managementインスタンスを指します。その後、NetScaler Gatewayを使用してサーバーの負荷分散を行うことができます。

Exchange ActiveSync用コネクタの構成には、次の2つのモードがあります。

- 非共有モードでは、Exchange ActiveSyncインスタンスの各コネクタはCitrix Endpoint Managementサーバーと通信し、結果として得られるポリシーの独自のプライベートコピーを保持します。たとえば、Citrix Endpoint Managementサーバーのクラスターの場合、各Citrix Endpoint Managementサーバーでコネクタインスタンスを実行できます。コネクタは、ローカルのCitrix Endpoint Managementインスタンスからポリシーを取得します。
- 共有モードでは、Exchange ActiveSyncノードの1つのコネクタがプライマリノードとして指定されます。コネクタはCitrix Endpoint Managementと通信します。他のノードは、Windows ネットワーク共有またはWindows（またはサードパーティ）レプリケーションを介して結果の構成を共有します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exchange ActiveSync 用のコネクタ構成全体は、単一のフォルダー (いくつかの XML ファイルで構成される) に格納されています。コネクタプロセスは、このフォルダー内のファイルの変更を検出し、自動的に構成を再ロードします。共有モードでは、プライマリノードのフェールオーバーはありません。ただし、システムはプライマリサーバーが数分間ダウンしても (たとえば、再起動のためなど) 許容できます。最後に正常に動作した構成は、コネクタプロセスにキャッシュされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高度な概念

Citrix Endpoint Managementの高度な概念に関する記事は、Citrix Endpoint Managementに関する製品情報をより深く掘り下げて説明しています。その目的は、専門的な手法を通じて展開時間を短縮することです。これらの記事では、コンテンツを作成した技術専門家が引用されている場合があります。

Citrix Endpoint Management環境における意思決定ポイント、推奨事項、よくある質問、およびユースケースについては、このセクションのCitrix Endpoint Managementの展開を参照してください。

Citrix Endpoint Managementに関するコミュニティサポートフォーラムについては、Citrix Discussionsを参照してください。

Citrix Endpoint Management のデプロイメント

Citrix Endpoint Management の展開を計画する際には、考慮すべき点がたくさんあります。どのデバイスを選択しますか？それらをどのように管理しますか？優れたユーザーエクスペリエンスを提供しながら、ネットワークのセキュリティを確保するにはどうすればよいですか？どのようなハードウェアが必要で、どのようにトラブルシューティングしますか？このセクションの記事は、そのような疑問に答えることを目的としています。展開に関する懸念事項をカバーするトピックのユースケースと推奨事項が含まれています。

ガイドラインや推奨事項がすべての環境やユースケースに適用されるとは限らないことに留意してください。Citrix Endpoint Management の展開を本稼働させる前に、必ずテスト環境をセットアップしてください。

このセクションの記事では、次の領域について説明します。

- **評価:** 展開を計画する際に考慮すべき一般的なユースケースと質問。
- **設計と構成:** 環境の設計と構成に関する推奨事項
- **運用と監視:** 稼働中の環境がスムーズに動作することを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

評価

どのような展開でもそうですが、ニーズの評価が最優先事項です。Citrix Endpoint Management の主なニーズは何ですか？環境内のすべてのデバイスを管理する必要がありますか、それともアプリのみ、あるいはその両方ですか？Citrix Endpoint Management 環境にはどの程度のセキュリティが必要ですか？展開を計画する際に考慮すべき一般的なユースケースと質問を見てみましょう。

- 管理モード
- デバイス要件
- セキュリティとユーザーエクスペリエンス
- アプリ
- ユーザーコミュニティ
- メール戦略
- シトリックス エンドポイント マネジメント の統合

設計と構成

展開のニーズの評価が完了したら、環境の設計方法と構成方法を決定できます。計画する項目には、次のものがあります。

- サーバーのハードウェアの選択
- アプリとデバイスのポリシーの設定
- ユーザーの登録

このセクションでは、これらの各シナリオなどに関するユースケースと推奨事項について説明します。

- NetScaler Gateway および Citrix ADC との統合
- MDX アプリの SSO とプロキシに関する考慮事項
- 認証
- サーバープロパティ
- デバイスとアプリのポリシー
- ユーザー登録オプション

© 1997–2026 Citrix Systems, Inc. All rights reserved.

運用と監視

Citrix Endpoint Management 環境が稼働を開始したら、スムーズな運用を確保するために監視する必要があります。監視セクションでは、Citrix Endpoint Management とそのコンポーネントが生成するさまざまなログとメッセージの場所、およびそれらのログの読み取り方法について説明します。このセクションには、カスタマーサポートへのフィードバック時間を短縮するために実行できる、さまざまな一般的なトラブルシューティング手順も含まれています。

- アプリのプロビジョニングとプロビジョニング解除
- ダッシュボードベースの操作
- ロールベースのアクセス制御および Citrix Endpoint Management のサポート
- 監視とサポート
- Citrix サポートプロセス

管理モード

管理モードとは、モバイルデバイス管理 (MDM) とモバイルアプリ管理 (MAM) を含む用語です。以下を構成できます。

- AndroidおよびiOSデバイスをMDM、MAM、またはその両方 (MDM+MAM) に登録するための登録プロファイル。MDM+MAMを選択した場合、ユーザーにMDMからのオプトアウトを許可できます。
- Windows 10およびWindows 11デバイスをMDMに登録するための登録プロファイル。

登録オプションは、デリバリーグループにアタッチする登録プロファイルで指定します。登録オプションについて詳しくは、「登録プロファイル」を参照してください。以下のセクションでは、デバイスとアプリの管理に関する考慮事項に焦点を当てます。

モバイルデバイス管理 (MDM)

MDMを使用すると、モバイルデバイスの構成、セキュリティ保護、およびサポートを行うことができます。MDMを使用すると、システムレベルでデバイスとデバイス上のデータを保護できます。ポリシー、アクション、およびセキュリティ機能を構成できます。たとえば、デバイスが紛失、盗難、またはコンプライアンス違反になった場合、デバイスを選択的にワイプできます。

デバイス上のアプリを管理しない場合でも、パブリックアプリストアアプリやエンタープライズアプリなどのモバイルアプリを配信できます。

MDMの一般的なユースケースは次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- MDMは、デバイスレベルの管理ポリシーや特定の制限が必要な企業所有デバイスの検討事項です。これらの制限には、完全ワイプ、選択的ワイプ、または地理的位置情報が含まれます。
- 顧客が実際のデバイスの管理を必要とするが、MDXポリシーを必要としない場合。
- ユーザーがモバイルデバイス上のネイティブメールクライアントにメールを配信するだけでよく、Exchange ActiveSyncまたはクライアントアクセスサーバーがすでに外部からアクセス可能な場合。このユースケースでは、MDMを使用してメール配信を構成できます。
- ネイティブエンタープライズアプリ (非MDX)、パブリックアプリストアアプリ、またはパブリックストアから配信されるMDXアプリを展開する場合。MDMソリューションだけでは、デバイス上のアプリ間での機密情報のデータ漏洩を防げない可能性があることに注意してください。データ漏洩は、Office 365アプリでのコピー＆ペーストや名前を付けて保存の操作で発生する可能性があります。

モバイルアプリ管理 (MAM)

MAMはアプリデータを保護し、アプリデータの共有を制御できます。MAMはまた、個人データとは別に企業データとリソースの管理を可能にします。MAM用に構成されたCitrix Endpoint Managementを使用すると、MDX対応モバイルアプリを使用して、アプリごとのコンテナ化と制御を提供できます。

MDXポリシーを使用することで、Citrix Endpoint Managementは、ネットワークアクセス（マイクロVPNなど）、アプリとデバイスの相互作用、およびアプリへのアクセスに対するアプリレベルの制御を提供します。

MAMは、デバイスが管理されていない場合でも企業データが保護されるため、BYO (bring-your-own) デバイスに適していることがよくあります。MDXには、MDM制御を必要としないMAM専用ポリシーが多数あります。

MAMは、Citrixモバイル生産性向上アプリもサポートしています。このサポートには以下が含まれます。

- Citrix Secure Mailへの安全な電子メール配信
- 保護されたCitrixモバイル生産性向上アプリ間でのデータ共有
- Citrix Filesでの安全なデータストレージ。

詳細については、「モバイル生産性向上アプリ」を参照してください。

MAMは、以下の例に適していることがよくあります。

- MDXアプリなどのモバイルアプリを、アプリレベルで管理して配信します。
- デバイスをシステムレベルで管理する必要はありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM+MAM

Citrix Endpoint Managementでは、ユーザーがデバイス管理をオプトアウトできるかどうかを指定できます。この柔軟性は、さまざまなユースケースが混在する環境で役立ちます。このような環境では、MAMリソースにアクセスするために、MDMポリシーによるデバイスの管理が必要になる場合があります。

MDM+MAMは、以下の例に適しています。

- MDMとMAMの両方が必要な単一のユースケースがあります。MAMリソースにアクセスするにはMDMが必要です。
- 一部のユースケースではMDMが必要ですが、そうでないユースケースもあります。
- 一部のユースケースではMAMが必要ですが、そうでないものもあります。

デバイス管理とMDM登録

Citrix Endpoint Management Enterprise環境には、さまざまなユースケースが含まれる場合があります。その中には、MAMリソースへのアクセスを許可するためにMDMポリシーによるデバイス管理を必要とするものもあります。

ユーザーにCitrixモバイル生産性向上アプリを展開する前に、ユースケースを完全に評価し、MDM登録を必須とするかどうかを決定してください。後でMDM登録の要件を変更することにした場合、ユーザーはデバイスを再登録する必要がある場合があります。詳細については、「登録プロファイル」を参照してください。

登録とNetScaler Gatewayの詳細については、「NetScaler GatewayおよびCitrix ADCとの統合」を参照してください。

以下は、MDM登録を必須とすることの利点と欠点（およびその軽減策）の概要です。

MDM登録がオプションの場合

利点

- ユーザーは、デバイスをMDM管理下に置くことなくMAMリソースにアクセスできます。このオプションは、ユーザーの採用を増やすことができます。
- 企業データを保護するためにMAMリソースへのアクセスを保護する機能。
- **アプリパスコード**などのMDXポリシーは、各MDXアプリのアプリアクセスを制御できます。
- NetScaler Gateway、Citrix Endpoint Management、およびアプリケーションごとのタイムアウトをCitrix PINとともに構成することで、追加の保護層が提供されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- MDMアクションはデバイスに適用されませんが、MAMアクセスを拒否するために一部のMDXポリシーが利用可能です。拒否は、ジェイルブレイクされたデバイスやルート化されたデバイスなどのシステム設定に基づいています。
- ユーザーは、初回使用時にデバイスをMDMに登録するかどうかを選択できます。

欠点

- MAMリソースは、MDMに登録されていないデバイスでも利用できます。
- MDMポリシーとアクションは、MDMに登録されているデバイスでのみ利用できます。

軽減策のオプション

- ユーザーに、コンプライアンス違反を選択した場合に責任を負う会社の利用規約に同意させます。管理者に、管理されていないデバイスを監視させます。
- アプリケーションタイマーを使用して、アプリケーションのアクセスとセキュリティを管理します。タイムアウト値を短縮するとセキュリティは向上しますが、ユーザーエクスペリエンスに影響を与える可能性があります。

MDM登録が必要な場合

利点

- MAMリソースへのアクセスをMDM管理デバイスのみに制限する機能。
- MDMポリシーとアクションは、希望どおりに環境内のすべてのデバイスに適用できます。
- ユーザーはデバイスの登録をオプトアウトできません。

欠点

- すべてのユーザーがMDMに登録する必要があります。
- 個人デバイスの企業管理に反対するユーザーの導入を妨げる可能性があります。

軽減策のオプション

- Citrix Endpoint Managementがデバイス上で実際に何を管理しているか、および管理者がどのような情報にアクセスできるかについて、ユーザーを教育します。

デバイス要件

あらゆる展開において考慮すべき重要な点は、展開を計画しているデバイスのセットです。iOS、Android、Windowsプラットフォームでは、多くの選択肢があります。Citrix Endpoint

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Managementがサポートするデバイスのリストについては、サポートされるデバイスプラットフォームを参照してください。

BYOD (Bring Your Own Device) 環境では、サポートされているプラットフォームが混在する可能性があります。ただし、ユーザーが登録できるデバイスについて通知する際には、「サポートされるデバイスプラットフォーム」の記事にある制限事項を考慮してください。環境内で1つまたは2つのデバイスしか許可しない場合でも、Citrix Endpoint ManagementはiOS、Android、Windowsデバイスでわずかに異なる動作をします。各プラットフォームで異なる機能セットが利用可能です。

また、すべてのアプリデザインがタブレットとスマートフォンの両方のフォームファクターを対象としているわけではありません。広範な変更を行う前に、展開したいデバイスの画面にアプリが適合することを確認するためにテストしてください。

登録要素も考慮できます。AppleとGoogleは、企業向け登録プログラムを提供しています。Apple Deployment ProgramとGoogle Android Enterpriseを通じて、事前設定済みで従業員がすぐに使用できるデバイスを購入できます。

登録の詳細については、ユーザー登録オプションを参照してください。

セキュリティとユーザーエクスペリエンス

セキュリティはどの組織にとっても重要ですが、セキュリティとユーザーエクスペリエンスのバランスを取る必要があります。たとえば、ユーザーが使いにくいほど高度に保護された環境になっている場合があります。あるいは、環境が非常にユーザーフレンドリーで、アクセス制御がそれほど厳しくない場合もあります。この仮想ハンドブックの他のセクションでは、セキュリティ機能について詳しく説明しています。この記事の目的は、一般的なセキュリティ上の懸念事項と、Citrix Endpoint Management で利用できるセキュリティオプションの概要を説明することです。

各ユースケースで留意すべき重要な考慮事項を以下に示します。

- 特定のアプリ、デバイス全体、またはその両方を保護しますか？
- ユーザーにどのように身元を認証させたいですか？LDAP、証明書ベースの認証、またはその両方の組み合わせを使用しますか？
- ユーザーのセッションがタイムアウトするまで、どのくらいの期間継続させたいですか？バックグラウンドサービス、Citrix ADC、およびオフライン中にアプリにアクセスできる場合では、タイムアウト値が異なることに注意してください。
- ユーザーにデバイスレベルのパスコードとアプリレベルのパスコードを設定させたいですか？許可するサインイン試行回数は何回ですか？MAM で実装される可能性のある追加のアプリごとの認証要件と、ユーザーがそれらをどのように認識するかを考慮してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ユーザーにどのような他の制限を課したいですか？Siri などのクラウドサービスへのアクセスをユーザーに許可しますか？提供する各アプリで何ができ、何ができないようにしますか？オフィス内から携帯電話データプランが使用されるのを防ぐために、企業ネットワーク (Wi-Fi) ポリシーを展開しますか？

アプリとデバイス

最初に考慮すべきことの1つは、何を保護したいかということです。

- 特定のアプリのみ（モバイルアプリ管理、または MAM）
- デバイス全体（モバイルデバイス管理、または MDM）。
- MDM+MAM

最も一般的なのは、デバイスレベルの制御を必要としない場合、特に組織が Bring Your Own Device (BYOD) をサポートしている場合は、モバイルアプリのみを管理すればよいということです。

Citrix Endpoint Management が管理しないデバイスを持つユーザーは、アプリストアを通じてアプリをインストールできます。選択的または完全なワイプなどのデバイスレベルの制御の代わりに、アプリポリシーを通じてアプリへのアクセスを制御します。設定した値に応じて、ポリシーはデバイスが定期的に Citrix Endpoint Management をチェックし、アプリが引き続き実行を許可されていることを確認することを要求します。

MDMは、デバイス上のすべてのソフトウェアのインベントリを取得する機能を含め、デバイス全体を保護することを可能にします。MDMは、デバイスがジェイルブレイクされている、ルート化されている、または安全でないソフトウェアがインストールされている場合に、登録を防止することを可能にします。しかし、このレベルの制御を行うと、ユーザーは自分の個人デバイスに対してそれほどの権限を与えることに警戒心を抱き、登録率が低下する可能性があります。

認証

認証は、ユーザーエクスペリエンスの大部分を占める部分です。組織がすでにActive Directoryを実行している場合、Active Directoryを使用することが、ユーザーがシステムにアクセスするための最も簡単な方法です。

認証ユーザーエクスペリエンスのもう1つの重要な部分は、タイムアウトです。セキュリティの高い環境では、ユーザーがシステムにアクセスするたびにサインオンを求める場合があります。このオプションは、すべての組織やユースケースにとって理想的ではないかもしれません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーエントロピー

セキュリティを強化するために、*ユーザーエントロピー*と呼ばれる機能を有効にできます。Citrix Secure Hubやその他のいくつかのアプリは、すべてが適切に機能するように、パスワード、PIN、証明書などの共通データを共有することがよくあります。この情報は、Citrix Secure Hub内の汎用ボールトに保存されます。**Encrypt Secrets**オプションを通じてユーザーエントロピーを有効にすると、Citrix Endpoint ManagementはUserEntropyというボールトを作成します。Citrix Endpoint Managementは、汎用ボールトからこの新しいボールトに情報を移動します。Citrix Secure Hubまたは別のアプリがデータにアクセスするには、ユーザーはパスワードまたはPINを入力する必要があります。

ユーザーエントロピーを有効にすると、いくつかの場所で認証レイヤーが追加されます。その結果、アプリがUserEntropyボールト内の共有データ（パスワード、PIN、証明書を含む）へのアクセスを必要とするたびに、ユーザーは認証する必要があります。

ユーザーエントロピーの詳細については、MDX Toolkitについてを参照してください。ユーザーエントロピーを有効にするには、関連する設定をクライアントプロパティで見つけることができます。

ポリシー

MDXとMDMの両方のポリシーは、組織に大きな柔軟性をもたらしますが、ユーザーを制限することもできます。特定の状況ではその制限が必要な場合もありますが、ポリシーによってはシステムが使用できなくなることもあります。たとえば、機密データを外部に送信する可能性のあるSiriやiCloudなどのクラウドアプリケーションへのアクセスをブロックしたい場合があります。これらのサービスへのアクセスをブロックするポリシーを設定できますが、そのようなポリシーには意図しない結果が生じる可能性があることに留意してください。たとえば、iOSキーボードのマイクはクラウドアクセスに依存しています。

アプリ

エンタープライズモビリティ管理 (EMM) は、モバイルデバイス管理 (MDM) とモバイルアプリケーション管理 (MAM) に分かれます。MDMは組織がモバイルデバイスを保護および制御できるようにする一方、MAMはアプリケーションの配信と管理を容易にします。BYODの採用が増加するにつれて、Citrix Endpoint ManagementのようなMAMソリューションを導入して、以下のことを支援できます。

- アプリの配信
- ソフトウェアライセンス
- 構成
- アプリケーションライフサイクル管理

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management を使用すると、特定の MAM ポリシーと VPN 設定を構成して、データ漏洩やその他のセキュリティ脅威を防ぐことで、これらのアプリのセキュリティを強化できます。Citrix Endpoint Management は、MDM と MAM の両方の機能を同じ環境に含める柔軟性を組織に提供します。

モバイルデバイスにアプリを配信する機能に加えて、Citrix Endpoint Management は MDX テクノロジーによるアプリのコンテナ化を提供します。MDX は、プラットフォームが提供するデバイスレベルの暗号化とは別の暗号化によってアプリを保護します。アプリをワイプまたはロックできます。アプリは、きめ細かなポリシーベースの制御の対象となります。独立系ソフトウェアベンダー (ISV) は、Mobile Apps SDK を使用してこれらの制御を適用できます。

企業環境では、ユーザーは職務を支援するためにさまざまなモバイルアプリを使用します。アプリには、パブリックアプリストアのアプリ、社内開発アプリ、またはネイティブアプリが含まれます。Citrix Endpoint Management は、これらのアプリを次のように分類します。

パブリックアプリ: これらのアプリには、Apple App Store や Google Play などのパブリックアプリストアで入手できる無料または有料のアプリが含まれます。組織外のベンダーは、多くの場合、パブリックアプリストアでアプリを提供しています。このオプションにより、顧客はインターネットから直接アプリをダウンロードできます。ユーザーのニーズに応じて、組織内で多くのパブリックアプリを使用する場合があります。このようなアプリの例としては、GoToMeeting、Salesforce、EpicCare アプリなどがあります。

Citrix® は、パブリックアプリストアからアプリのバイナリを直接ダウンロードし、それを MDX Toolkit でラップしてエンタープライズ配布することをサポートしていません。サードパーティアプリケーションを MDX 対応にするには、アプリベンダーに連絡してアプリのバイナリを入手してください。MDX Toolkit を使用してバイナリをラップするか、MAM SDK をバイナリと統合することができます。

社内アプリ: 多くの組織には、特定の機能を提供し、組織内で独自に開発および配布されるアプリを作成する社内開発者がいます。場合によっては、ISV が提供するアプリを持つ組織もあります。このようなアプリはネイティブアプリとして展開することも、Citrix Endpoint Management などの MAM ソリューションを使用してアプリをコンテナ化することもできます。たとえば、医療機関は、医師がモバイルデバイスで患者情報を表示できる社内アプリを作成できます。組織は、患者情報を保護し、バックエンドの患者データベースサーバーへの VPN アクセスを有効にするために、MAM SDK を有効にするか、アプリを MDM ラップすることができます。

Web および SaaS アプリ: これらのアプリには、内部ネットワークからアクセスするアプリ (Web アプリ) またはパブリックネットワーク経由でアクセスするアプリ (SaaS) が含まれます。Citrix Endpoint Management では、アプリコネクタのリストを使用してカスタムの Web および SaaS アプリを作成することもできます。これらのアプリコネクタは、既存の Web アプリへのシングル

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サインオン (SSO) を容易にすることができます。詳細については、「アプリコネクタの種類」を参照してください。たとえば、Google Apps SAML を使用して、Security Assertion Markup Language (SAML) に基づく Google Apps への SSO を行うことができます。

モバイル生産性アプリ: モバイル生産性アプリは、Citrix Endpoint Management ライセンスに含まれる Citrix 開発のアプリです。詳細については、「モバイル生産性アプリについて」を参照してください。Citrix は、その他のビジネス対応アプリも提供しています。ISV は、Mobile Apps SDK を使用してビジネス対応アプリを開発します。

HDX アプリ: HDX アプリは、StoreFront で公開する Windows ホスト型アプリです。Citrix Virtual Apps and Desktops 環境がある場合は、アプリを Citrix Endpoint Management と統合して、登録済みユーザーがアプリを利用できるようにすることができます。

Citrix Endpoint Management で展開および管理するモバイルアプリの種類によって、基盤となる構成とアーキテクチャは異なります。さまざまなレベルの権限を持つ多くのユーザーグループが単一のアプリを使用するとします。その場合、アプリの 2 つのバージョンを展開するために、個別のデリバリーグループを作成できます。ユーザーデバイスでのポリシーの不一致を避けるために、ユーザーグループのメンバーシップが相互に排他的であることを確認してください。

Apple Volume Purchase を使用して iOS アプリケーションのライセンスを管理することもできます。このオプションでは、Apple Volume Purchase プログラムに登録する必要があります。また、Citrix Endpoint Management コンソールを使用して Volume Purchase 設定を構成する必要があります。この構成により、Volume Purchase ライセンスでアプリを配布できます。このようなさまざまなユースケースがあるため、Citrix Endpoint Management 環境を実装する前に MAM 戦略を評価し、計画することが重要です。MAM 戦略の計画は、以下を定義することから開始できます。

アプリの種類: サポートする予定のさまざまな種類のアプリをリストアップします。次に、パブリック、ネイティブ、Citrix モバイル生産性アプリ、Web、社内、ISV アプリなど、アプリを分類します。また、iOS や Android など、異なるデバイスプラットフォームのアプリも分類します。この分類は、各種類のアプリに必要な Citrix Endpoint Management 設定を調整するのに役立ちます。たとえば、特定のアプリはラッピングの対象とならない場合があります。または、一部のアプリでは、他のアプリとの対話のために特別な API を有効にするために Mobile Apps SDK の使用が必要になる場合があります。

ネットワーク要件: 特定のネットワークアクセス要件を持つアプリを適切な設定で構成します。たとえば、特定のアプリは VPN を介して内部ネットワークへのアクセスを必要とする場合があります。一部のアプリは、DMZ 経由でアクセスをルーティングするためにインターネットアクセスを必要とする場合があります。このようなアプリが必要なネットワークに接続できるようにするには、それに応じてさまざまな設定を構成する必要があります。アプリごとのネットワーク要件を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

定義して、事前にアーキテクチャの決定を確定するのに役立てます。この作業により、全体的な実装プロセスが合理化されます。

セキュリティ要件: 個々のアプリまたはすべてのアプリに適用されるセキュリティ要件を定義します。MDX ポリシーなどの一部の設定は、個々のアプリに適用されます。セッションおよび認証設定は、すべてのアプリに適用されます。一部のアプリには、特定の暗号化、コンテナ化、ラッピング、認証、ジオフェンシング、パスコード、またはデータ共有の要件がある場合があります。展開を簡素化するために、これらの要件を事前に概説してください。

展開要件: ポリシーベースの展開を使用して、準拠しているユーザーのみが公開されたアプリをダウンロードできるようにしたい場合があります。たとえば、特定のアプリで次の要件を満たす必要がある場合があります。

- デバイスプラットフォームベースの暗号化が有効になっている
- デバイスが管理されている
- デバイスが最小オペレーティングシステムバージョンを満たしている
- 特定のアプリが企業ユーザーのみに提供されている

適切な展開ルールまたはアクションを設定できるように、このような要件を事前に概説してください。

ライセンス要件: アプリ関連のライセンス要件を記録します。これらのメモは、ライセンスの使用状況を効果的に管理し、ライセンスを容易にするためにCitrix Endpoint Managementで特定の機能を構成する必要があるかどうかを判断するのに役立ちます。たとえば、無料または有料のiOSアプリを展開する場合、AppleはユーザーがApple Storeアカウントにサインオンすることでアプリにライセンス要件を適用します。Apple Volume Purchaseに登録して、Citrix Endpoint Managementを通じてこれらのアプリを配布および管理できます。Volume Purchaseを使用すると、ユーザーはApple Storeアカウントにサインインすることなくアプリをダウンロードできます。また、Samsung Knoxなどのツールには特別なライセンス要件があり、これらの機能を展開する前に完了する必要があります。

許可リストとブロックリストの要件: ユーザーが一部のアプリをインストールまたは使用するのを防ぎたいと考えるでしょう。デバイスを非準拠にするアプリの許可リストを作成します。次に、デバイスが非準拠になったときにトリガーされるポリシーを設定します。一方、アプリは使用可能であっても、何らかの理由でブロックリストに該当する場合があります。その場合、アプリを許可リストに追加し、そのアプリは使用可能であるが、必須ではないことを示すことができます。また、新しいデバイスにプリインストールされているアプリには、オペレーティングシステムの一部ではない一般的に使用されるアプリが含まれる場合があることに注意してください。これらのアプリは、ブロックリスト戦略と競合する可能性があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリのユースケース

医療機関は、モバイルアプリのMAMソリューションとして機能するようにCitrix Endpoint Managementを展開する予定です。モバイルアプリは、企業ユーザーとBYODユーザーに提供されます。IT部門は、次のアプリを提供および管理することを決定しました。

- **モバイル生産性アプリ:** Citrixが提供するiOSおよびAndroidアプリ。
- **Citrix Files:** 共有データにアクセスし、ファイルを共有、同期、編集するためのアプリ。

パブリックアプリストア

- **Citrix Secure Hub:** すべてのモバイルデバイスがCitrix Endpoint Managementと通信するために使用するクライアント。IT部門は、Citrix Secure Hubクライアントを介してセキュリティ設定、構成、およびモバイルアプリをモバイルデバイスにプッシュします。AndroidおよびiOSデバイスは、Citrix Secure Hubを介してCitrix Endpoint Managementに登録します。
- **Citrix Workspaceアプリ:** ユーザーがCitrix Virtual Appsによってホストされているアプリをモバイルデバイスで開くことができるモバイルアプリ。
- **GoToMeeting:** オンライン会議、デスクトップ共有、ビデオ会議クライアントであり、ユーザーがインターネット経由で他のコンピューターユーザー、顧客、クライアント、または同僚とリアルタイムで会議を行うことができます。
- **SalesForce1:** Salesforce1を使用すると、ユーザーはモバイルデバイスからSalesforceにアクセスでき、すべてのChatter、CRM、カスタムアプリ、およびビジネスプロセスを、あらゆるSalesforceユーザーにとって統一されたエクスペリエンスにまとめます。
- **RSA SecurID:** 2要素認証用のソフトウェアベースのトークン。
- **EpicCare apps:** これらのアプリは、医療従事者に患者のカルテ、患者リスト、スケジュール、メッセージングへの安全でポータブルなアクセスを提供します。
  - **Haiku:** iPhoneおよびAndroidフォン用のモバイルアプリ。
  - **Canto:** iPad用のモバイルアプリ
  - **Rover:** iPhoneおよびiPad用のモバイルアプリ。

HDX: Citrix Virtual Appsは、Citrix WorkspaceにHDXアプリを配信します。

- **Epic Hyperspace:** 電子カルテ管理用のEpicクライアントアプリケーション。

ISV

- **Vocera:** HIPAA準拠のボイスオーバーIPおよびメッセージングモバイルアプリであり、iPhoneおよびAndroidスマートフォンを介して、いつでもどこでもVocera音声テクノロジーの利点を拡張します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

社内アプリ

- **HCMail:** 暗号化されたメッセージを作成し、社内メールサーバーのアドレス帳を検索し、電子メールクライアントを使用して暗号化されたメッセージを連絡先に送信するのに役立つアプリ。

社内WEBアプリ

- **PatientRounding:** さまざまな部門が患者の健康情報を記録するために使用するWebアプリケーション。
- **Outlook Web Access:** Webブラウザ経由でメールへのアクセスを許可します。
- **SharePoint:** 組織全体でのファイルおよびデータ共有に使用されます。

次の表に、MAM構成に必要な基本情報を示します。

アプリ名	アプリの種類	MDXラッピング	IOS	アンドロイド
シトリックス セキュア メール	モバイル生産性アプリ	バージョン10.4.1以降はいいえ	はい	はい
シトリックス セキュア ウェブ	モバイル生産性アプリ	バージョン10.4.1以降はいいえ	はい	はい
シトリックス ファイル	モバイル生産性アプリ	バージョン10.4.1以降はいいえ	はい	はい
シトリックス セキュア ハブ	パブリックアプリ	該当なし	はい	はい
Citrix Workspaceアプリ	パブリックアプリ	N/A	はい	はい
GoToMeeting	公開アプリ	N/A	はい	はい
SalesForce1	公開アプリ	N/A	はい	はい
RSA SecurID	公開アプリ	該当なし	はい	はい
エピック ハイク	パブリックアプリ	該当なし	はい	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ名	アプリの種類	MDXラッピング	IOS	アンドロイド
エピック カント	パブリックアプリ	該当なし	はい	いいえ
エピック ローバー	パブリックアプリ	該当なし	はい	いいえ
エピック ハイパースペース	HDX™ App	該当なし	はい	はい
ボセラ	ISV アプリ	はい	はい	はい
エイチシーメール	社内アプリ	はい	はい	はい
PatientRounding	Webアプリ	該当なし	はい	はい
アウトルック ウェブ アクセス	Webアプリ	該当なし	はい	はい
SharePoint	Webアプリ	該当なし	はい	はい

以下の表は、Citrix Endpoint ManagementでMAMポリシーを構成する際に参照できる特定の要件を示しています。

アプリ名	VPN必須	相互作用 (コンテナ外のアプリとの)	相互作用 (コンテナ外のアプリからの)	デバイスプラットフォームベースの暗号化
シトリックス セキュア メール	はい	選択的に許可	許可	不要
シトリックス セキュア ウェブ	はい	許可	許可	不要
シトリックス ファイルズ	はい	許可	許可	不要
シトリックス セキュア ハブ	はい	該当なし	該当なし	該当なし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ名	VPN必須	相互作用 (コンテナ外のアプリとの)	相互作用 (コンテナ外のアプリからの)	デバイスプラットフォームベースの暗号化
Citrix Workspaceアプリ	はい	該当なし	該当なし	該当なし
GoToMeeting	いいえ	該当なし	該当なし	該当なし
SalesForce1	いいえ	該当なし	該当なし	該当なし
RSA SecurID	N	N/A	N/A	N/A
エピック ハイク	Y	N/A	N/A	N/A
エピック カント	Y	N/A	N/A	N/A
エピック ローバー	はい	該当なし	該当なし	該当なし
エピック ハイパースペース	はい	該当なし	該当なし	該当なし
ボセラ	はい	ブロック済み	ブロック済み	不要
エイチシーメール	はい	ブロック済み	ブロック済み	必須
PatientRounding	はい	N/A	N/A	必須
アウトルック ウェブ アクセス	はい	N/A	N/A	不要
SharePoint	はい	N/A	N/A	不要

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ名	プロキシフィルタリング	ライセンス	ジオフェンシング	モバイルアプリSDK	最小オペレーティングシステムバージョン
シトリックス セキュアメール	必須	N/A	選択的に必須	N/A	適用済み
シトリックス セキュアウェブ	必須	該当なし	不要	該当なし	適用済み
セキュアノーツ	必須	該当なし	不要	該当なし	適用済み
シトリックス ファイルズ	必須	N/A	不要	N/A	適用済み
シトリックス セキュアハブ	不要	ボリューム購入	不要	N/A	適用されていません
シトリックス ワークスペース アプリ	不要	ボリューム購入	不要	N/A	強制されません
GoToMeeting	不要	ボリューム購入	不要	該当なし	強制されません
SalesForce1	不要	ボリューム購入	不要	該当なし	強制されません
RSA SecurID	不要	ボリューム購入	不要	該当なし	適用されません
エピック・ハイク	不要	ボリューム購入	不要	該当なし	適用されません
エピック・カント	不要	ボリューム購入	不要	該当なし	適用されません

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ名	プロキシフィルタリング	ライセンス	ジオフェンシング	モバイルアプリSDK	最小オペレーティングシステムバージョン
エピック ローバー	不要	ボリューム購入	不要	該当なし	適用されません
エピック ハイパースペース	不要	該当なし	不要	該当なし	適用されません
ボセラ	必須	該当なし	必須	必須	適用済み
エイチシーメール	必須	該当なし	必須	必須	適用済み
PatientRound-ing	必須	該当なし	不要	該当なし	適用されません
Outlook Web アクセス	必須	N/A	不要	N/A	適用されません
SharePoint	必須	N/A	不要	N/A	適用されません

ユーザーコミュニティ

すべての組織は、さまざまな機能的役割を担う多様なユーザーコミュニティで構成されています。これらのユーザーコミュニティは、ユーザーデバイスを介して提供されるさまざまなリソースを使用して、異なるタスクやオフィス機能を実行します。ユーザーは、提供されたモバイルデバイスを使用して、自宅やリモートオフィスで作業する場合があります。あるいは、ユーザーは自身のモバイルデバイスを所有しており、特定のセキュリティコンプライアンス規則の対象となるツールにアクセスできる場合があります。

ユーザーコミュニティが業務でモバイルデバイスを使用するようになるにつれて、データ漏洩を防ぐためにエンタープライズモビリティ管理 (EMM) が不可欠になります。EMM は、組織のセキュリティ制限を適用するためにも重要です。効率的でより高度なモバイルデバイス管理のために、ユーザーコミュニティを分類できます。これにより、ユーザーとリソースのマッピングが簡素化され、適切なセキュリティポリシーがユーザーに適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の例は、医療機関のユーザーコミュニティが EMM 向けにどのように分類されているかを示しています。

ユーザーコミュニティのユースケース

この医療機関の例では、ネットワークおよび関連会社の従業員やボランティアを含む多くのユーザーにテクノロジーリソースとアクセスを提供しています。この組織は、EMM ソリューションを非管理職ユーザーのみに展開することを選択しました。

この組織のユーザーの役割と機能は、臨床、非臨床、契約社員などのサブグループに分類できます。選択されたユーザーには会社のモバイルデバイスが支給され、その他のユーザーは個人のデバイスから限られた会社の情報にアクセスできます。適切なレベルのセキュリティ制限を適用し、データ漏洩を防ぐために、組織は登録された各デバイスを企業 IT が管理することを決定しました。これらのデバイスは、会社所有であるか、BYOD (Bring Your Own Device) である可能性があります。また、ユーザーは単一のデバイスのみを登録できます。

次のセクションでは、各サブグループの役割と機能の概要を説明します。

臨床

- 看護師
- 医師 (内科医、外科医など)
- 専門医 (栄養士、麻酔科医、放射線科医、心臓病専門医、腫瘍専門医など)
- 外部医師 (従業員ではない医師および遠隔オフィスで働く事務員)
- 在宅医療サービス (患者の自宅訪問で医師サービスを行うオフィスおよびモバイルワーカー)
- 研究専門家 (医学の問題に対する答えを見つけるために臨床研究を行う6つの研究機関のナレッジワーカーおよびパワーユーザー)
- 教育と研修 (教育と研修における看護師、医師、専門家)

非臨床

- 共有サービス (人事、給与計算、買掛金、サプライチェーンサービスなど、さまざまなバックオフィス業務を行うオフィスワーカー)
- 医師サービス (管理サービス、分析およびビジネスインテリジェンス、ビジネスシステム、クライアントサービス、財務、マネージドケア管理、患者アクセスソリューション、収益サイクルソリューションなど、プロバイダー向けにさまざまなヘルスケア管理、管理サービス、ビジネスプロセスソリューションを行うオフィスワーカー)
- サポートサービス (福利厚生管理、臨床統合、コミュニケーション、報酬および業績管理、施設および資産サービス、人事テクノロジーシステム、情報サービス、内部監査およびプロセス改善など、さまざまな非臨床業務を行うオフィスワーカー)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 慈善プログラム (慈善プログラムを支援するためにさまざまな業務を行うオフィスおよびモバイルワーカー)

請負業者

- 製造業者およびベンダーパートナー (サイト間VPN経由でオンサイトおよびリモート接続され、さまざまな非臨床サポート機能を提供する)

上記の情報に基づいて、組織は以下のエンティティを作成しました。Citrix Endpoint Management のデリバリーグループの詳細については、リソースの展開を参照してください。

ACTIVE DIRECTORY組織単位 (OU) およびグループ

OU = Citrix Endpoint Managementリソースの場合:

- OU = 臨床; グループ =
  - XM-看護師
  - XM-医師
  - XM-専門医
  - XM-外部医師
  - XM-在宅医療サービス
  - XM-調査スペシャリスト
  - XM-教育・研修
- OU = 非臨床; Groups =
  - XM-共有サービス
  - XM-医師サービス
  - XM-サポートサービス
  - XM-慈善プログラム

CITRIX ENDPOINT MANAGEMENT ローカルユーザーとグループ

Group= 契約者の場合、ユーザー=

- ベンダー1
- ベンダー2
- ベンダー3
- … ベンダー10

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CITRIX ENDPOINT MANAGEMENT デリバリーグループ

- 臨床-看護師
- 臨床-医師
- 臨床-専門家
- 臨床-外部医師
- 臨床-在宅医療サービス
- 臨床-研究専門家
- 臨床-教育およびトレーニング
- 非臨床-共有サービス
- 非臨床-医師サービス
- 非臨床-サポートサービス
- 非臨床-慈善プログラム

デリバリーグループとユーザーグループのマッピング

ACTIVE DIRECTORY グループ	CITRIX ENDPOINT MANAGEMENT デリバリーグループ
XM-看護師	臨床-看護師
XM-医師	Clinical-医師
XM-専門医	Clinical-専門医
XM-外部医師	Clinical-外部医師
XM-在宅医療サービス	Clinical-在宅医療サービス
XM-研究専門家	Clinical-研究専門家
XM-教育およびトレーニング	Clinical-教育およびトレーニング
XM-共有サービス	Non-Clinical-共有サービス
XM-医師サービス	非臨床-医師サービス
XM-サポートサービス	非臨床-サポートサービス
XM-慈善プログラム	非臨床-慈善プログラム

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デリバリーグループとリソースのマッピング

次の表は、このユースケースにおける各デリバリーグループに割り当てられたリソースを示しています。最初の表はモバイルアプリの割り当てを示し、2番目の表はパブリックアプリ、HDXアプリ、およびデバイス管理リソースを示しています。

CITRIX ENDPOINT MANAGEMENT デリバリーグループ	CITRIX モバイルアプリ	パブリックモバイルアプリ	HDX モバイルアプリ
臨床-看護師	X		
臨床-医師			
臨床-専門家			
臨床 - 外部医師	X		
臨床 - 在宅医療サービス	X		
臨床 - 研究スペシャリスト	X		
臨床 - 教育およびトレーニング		X	X
非臨床 - 共有サービス		X	X
非臨床 - 医師サービス		X	X
非臨床サポートサービス	X	X	X
非臨床慈善プログラム	X	X	X
契約社員	X	X	X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CITRIX ENDPOINT MANAGEMENT デリバリーグループ	パブリックアプリ: RSA SECURID	パブリックアプリ: EPICCARE HAIKU	HDXアプリ: EPIC HYPERSPACE	パスコードポリシー	デバイス制限	自動アクション	ネットワークポリシー
臨床 - 看護師							X
臨床 - 医師					X		
臨床 - 専門医							
臨床 - 外部医師							
臨床 - 在宅医療サービス							
臨床 - 研究専門家							
臨床 - 教育およびトレーニング		X	X				
非臨床 - 共有サービス		X	X				
非臨床 - 医師		X	X				

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CITRIX ENDPOINT MANAGEMENT デリバリーグループ	パブリックアプリ: RSA SECURID	パブリックアプリ: EPICCARE HAIKU	HDXアプリ: EPIC HYPERSPACE	パスコードポリシー	デバイス制限	自動アクション	ネットワークポリシー
サービス							
非臨床 - サポートサービス		X	X				

注意事項と考慮事項

- Citrix Endpoint Management は、初期設定時に All Users という名前のデフォルトのデリバリーグループを作成します。このデリバリーグループを無効にしない場合、すべての Active Directory ユーザーは Citrix Endpoint Management に登録する権利を持ちます。
- Citrix Endpoint Management は、LDAP サーバーへの動的接続を使用して、Active Directory ユーザーとグループをオンデマンドで同期します。
- ユーザーが Citrix Endpoint Management にマッピングされていないグループに属している場合、そのユーザーは登録できません。同様に、ユーザーが多数のグループのメンバーである場合、Citrix Endpoint Management は、Citrix Endpoint Management にマッピングされているグループの一部としてのみユーザーを分類します。

セキュリティ要件

Citrix Endpoint Management環境に関連するセキュリティ上の考慮事項の範囲は、すぐに手に負えなくなる可能性があります。多くの相互に関連する要素と設定があります。許容できるレベルの保護が利用可能であることを確認するために、どこから始めればよいか、何を選択すればよいかわからないかもしれません。これらの選択を簡単にするために、Citrixは以下の表に示すように、高、より高、最高のセキュリティに関する推奨事項を提供しています。

セキュリティ上の懸念は、デバイスの登録モード（MAM、MDM+MAM（MDMオプション）、またはMDM+MAM（MDM必須））を検討する唯一の要素ではありません。ユースケースの要件も確認し、管理モードを選択する前にセキュリティ上の懸念を軽減できるかどうかを判断することが重要です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高: これらの設定を使用すると、ほとんどの組織で許容される基本的なセキュリティレベルを維持しながら、最適なユーザーエクスペリエンスを提供できます。

より高: これらの設定は、セキュリティと使いやすさのより強力なバランスを生み出します。

最高: これらの推奨事項に従うと、使いやすさやユーザーの採用を犠牲にして、高いレベルのセキュリティが提供されます。

管理モードのセキュリティに関する考慮事項

次の表は、各セキュリティレベルの管理モードを示しています。

高セキュリティ	より高セキュリティ	最高セキュリティ
MAM、MDM+MAM	MDM+MAM	MDM+MAM

注記:

- ユースケースによっては、MAMのみの展開でセキュリティ要件を満たし、良好なユーザーエクスペリエンスを提供できます。
- BYODのようなユースケースで、すべてのビジネス要件とセキュリティ要件がアプリのコンテナ化のみで満たされる場合、CitrixはMAM-onlyモードを推奨します。
- 高セキュリティ環境（および企業支給デバイス）の場合、Citrixは利用可能なすべてのセキュリティ機能を活用するためにMDM+MAMを推奨します。

Citrix ADCとNetScaler Gatewayのセキュリティに関する考慮事項

次の表は、各セキュリティレベルにおけるCitrix ADCとNetScaler Gatewayの推奨事項を示しています。

高セキュリティ	より高いセキュリティ	最高セキュリティ
Citrix ADCを推奨します。NetScaler GatewayはMAMおよびMDM+MAMに必要です。	Citrix Endpoint ManagementがDMZにある場合、SSLブリッジを使用したXenMobileウィザード構成用の標準NetScaler。	エンドツーエンド暗号化によるSSLオフロード

注:

- NATまたは既存のサードパーティ製プロキシ/ロードバランサーを介してCitrix Endpoint Managementサーバーをインターネットに公開することは、MDMのオプションとなる場合があ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ります。ただし、その場合、SSLトラフィックはCitrix Endpoint Managementサーバーで終端され、潜在的なセキュリティリスクをもたらします。

- 高セキュリティ環境の場合、デフォルトのCitrix Endpoint Management構成を持つNetScaler Gatewayは、通常、セキュリティ要件を満たすか、それを上回ります。
- 最高のセキュリティ要件を持つMDM登録の場合、NetScaler GatewayでのSSL終端により、エンドツーエンドのSSL暗号化を維持しながら、境界でトラフィックを検査できます。
- SSL/TLS暗号を定義するオプション。
- 詳細については、NetScaler GatewayおよびCitrix ADCとの統合を参照してください。

登録のセキュリティに関する考慮事項

次の表に、各セキュリティレベルにおけるCitrix ADCおよびNetScaler Gatewayの推奨事項を示します。

高セキュリティ	より高いセキュリティ	最高セキュリティ
Active Directoryグループのメンバーシップのみ。すべてのユーザー配信グループは無効。	招待制の登録セキュリティモード。Active Directoryグループのメンバーシップのみ。すべてのユーザー配信グループは無効	デバイスIDに紐付けられた登録セキュリティモード。Active Directoryグループのメンバーシップのみ。すべてのユーザー配信グループは無効

注：

- Citrixでは通常、登録を事前定義されたActive Directoryグループのユーザーのみに制限することを推奨しています。この制限には、組み込みの「すべてのユーザー」配信グループを無効にする必要があります。
- 登録招待を使用して、招待状を持つユーザーに登録を制限できます。登録招待はWindowsデバイスでは利用できません。
- ワンタイムPIN（OTP）登録招待を二要素認証ソリューションとして使用し、ユーザーが登録できるデバイスの数を制御できます。（OTP招待はWindowsデバイスでは利用できません。）

デバイスパスコードのセキュリティに関する考慮事項

次の表に、各セキュリティレベルにおけるデバイスパスコードの推奨事項を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高いセキュリティ	より高いセキュリティ	最高のセキュリティ
推奨。デバイスレベルの暗号化には高いセキュリティが必要です。MDMで適用できます。MDXポリシーの「非準拠デバイスの動作」を使用して、MAMのみに必須として設定できます。	MDM、MAM、またはMDM+MAMポリシーを使用して適用されます。	MDMおよびMDXポリシーを使用して適用されます。MDMの複雑なパスコードポリシー。

注記:

- Citrixはデバイスパスコードの使用を推奨しています。
- MDMポリシーを介してデバイスパスコードを適用できます。
- MDXポリシーを使用して、管理対象アプリの使用にデバイスパスコードを必須とすることができます。たとえば、BYODのユースケースなどです。
- Citrixは、MDM+MAM登録のセキュリティを強化するために、MDMとMDXのポリシーオプションを組み合わせることを推奨しています。
- 最高のセキュリティ要件を持つ環境では、複雑なパスコードポリシーを設定し、MDMで適用できます。デバイスがパスコードポリシーに従わない場合に、管理者に通知したり、選択的/完全なデバイスワイプを実行したりする自動アクションを設定できます。

アプリ

エンタープライズモビリティ管理 (EMM) は、モバイルデバイス管理 (MDM) とモバイルアプリケーション管理 (MAM) に分かれます。MDMは組織がモバイルデバイスを保護および制御できるようにする一方、MAMはアプリケーションの配信と管理を支援します。BYODの採用が増加するにつれて、Citrix Endpoint ManagementのようなMAMソリューションを通常実装できます。Citrix Endpoint Managementは、アプリケーションの配信、ソフトウェアライセンス、構成、およびアプリケーションライフサイクル管理を支援します。ユーザーにMDM管理への参加を要求または許可できます。

Citrix Endpoint Managementを使用すると、データ漏洩やその他のセキュリティ脅威を防ぐために、MAMポリシーとVPN設定を構成することでアプリを保護できます。Citrix Endpoint Managementは、デバイスをMAMのみまたはMDM+MAMとして登録する柔軟性を組織に提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

モバイルデバイスにアプリを配信する機能に加えて、Citrix Endpoint Managementは、MDXテクノロジを介したアプリのコンテナ化を提供します。アプリには、きめ細かなポリシーベースの制御が適用されます。独立系ソフトウェアベンダー (ISV) は、Mobile Apps SDKを使用してこれらの制御を適用できます。

企業環境では、ユーザーは職務を支援するためにさまざまなモバイルアプリを使用します。アプリには、パブリックアプリストアのアプリ、社内開発アプリ、またはネイティブアプリが含まれる場合があります。Citrix Endpoint Managementは、これらのアプリを次のように分類します。

- **パブリックアプリ:** これらのアプリには、Apple App StoreやGoogle Playなどのパブリックアプリストアで利用可能な無料または有料のアプリが含まれます。組織外のベンダーは、多くの場合、自社のアプリをパブリックアプリストアで利用できるようにします。このオプションにより、顧客はインターネットから直接アプリをダウンロードできます。ユーザーのニーズに応じて、組織内で多くのパブリックアプリを使用する場合があります。このようなアプリの例には、GoToMeeting、Salesforce、EpicCareアプリなどがあります。
    - **MAM SDKを使用する場合:** アプリベンダーからアプリバイナリを入手します。その後、MAM SDKをアプリに統合します。
    - **MDX Toolkitを使用する場合:** Citrix®は、パブリックアプリストアからアプリバイナリを直接ダウンロードし、それをMDX Toolkitでラップしてエンタープライズ配布することをサポートしていません。サードパーティアプリケーションをラップするには、アプリベンダーと協力してアプリバイナリを入手してください。その後、MDX Toolkitを使用してバイナリをラップできます。
- **社内アプリ:** 多くの組織には、特定の機能を提供し、組織内で独自に開発および配布されるアプリを作成する社内開発者がいます。特定のケースでは、一部の組織はISVが提供するアプリも持っている場合があります。そのようなアプリをネイティブアプリとして展開することも、Citrix Endpoint ManagementのようなMAMソリューションを使用してアプリをコンテナ化することもできます。

  たとえば、医療機関は、医師がモバイルデバイスで患者情報を表示できる社内アプリを作成する場合があります。組織は、以下のいずれかを使用して患者情報を保護し、患者データベースへのVPNアクセスを有効にできます。

    - MAM SDK
    - MDX ツールキット
- **WebアプリとSaaSアプリ:** これらのアプリには、内部ネットワークからアクセスするアプリ (Webアプリ) またはパブリックネットワーク経由でアクセスするアプリ (SaaS) が含まれます。Citrix Endpoint Managementでは、アプリコネクタのリストを使用してカスタムWebアプ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リとSaaSアプリを作成することもできます。これらのアプリコネクタは、既存のWebアプリへのシングルサインオン (SSO) を容易にすることができます。詳細については、「アプリコネクタの種類」を参照してください。たとえば、Security Assertion Markup Language (SAML) に基づくSSOのためにGoogle Apps SAMLをGoogle Appsに使用できます。

- **モバイル生産性アプリ:** モバイル生産性アプリは、Citrix Endpoint Managementライセンスに含まれるCitrix開発のアプリです。詳細については、「モバイル生産性アプリについて」を参照してください。Citrixは、ISVがMobile Apps SDKを使用して開発するその他のビジネス対応アプリも提供しています。
- **HDXアプリ:** HDXアプリは、StoreFrontで公開するWindowsホスト型アプリです。Citrix Virtual Apps and DesktopsおよびCitrix Workspaceを使用している場合、HDXアプリは登録済みユーザーが利用できます。

Citrix Endpoint Managementで展開および管理するモバイルアプリの種類によって、基盤となる構成が異なる場合があります。たとえば、異なる権限レベルを持つ多くのユーザーグループが1つのアプリを使用する場合があります。その場合、同じアプリの2つの異なるバージョンを展開するために、個別のデリバリーグループを作成できます。また、ユーザーのデバイスでのポリシーの不一致を避けるために、ユーザーグループのメンバーシップが相互に排他的であることを確認する必要があります。

Apple Volume Purchaseを使用して、iOSアプリケーションのライセンスを管理することもできます。このオプションを使用するには、Volume Purchaseプログラムに登録し、Citrix Endpoint ManagementコンソールでVolume Purchase設定を構成する必要があります。この構成により、Volume Purchaseライセンスを使用してアプリを配布できます。さまざまなユースケースがあるため、Citrix Endpoint Management環境を実装する前にMAM戦略を評価し、計画することが重要です。MAM戦略の計画は、以下を定義することから始められます。

- **アプリの種類:** サポートを計画しているさまざまな種類のアプリをリストアップし、パブリック、ネイティブ、Web、社内、ISVアプリなどのカテゴリに分類します。また、iOSやAndroidなどの異なるデバイスプラットフォーム向けにアプリを分類します。この分類は、各種類のアプリに必要なさまざまなCitrix Endpoint Management設定を調整するのに役立ちます。たとえば、一部のアプリでは、他のアプリとの対話のための特別なAPIを有効にするために、モバイルアプリSDKの使用が必要になる場合があります。
- **ネットワーク要件:** 特定のネットワークアクセス要件を持つアプリの設定を構成します。たとえば、特定のアプリはVPNを介して内部ネットワークへのアクセスを必要とする場合があります。一部のアプリは、DMZを介してアクセスをルーティングするためにインターネットアクセスを必要とする場合があります。このようなアプリが必要なネットワークに接続できるようにするには、それに応じてさまざまな設定を構成する必要があります。アプリごとのネットワー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ク要件を定義することは、アーキテクチャ上の決定を早期に完了するのに役立ち、全体的な実装プロセスを効率化します。

- **セキュリティ要件:** 個々のアプリまたはすべてのアプリに適用するセキュリティ要件を定義できます。
  - MDXポリシーなどの設定は、個々のアプリに適用されます。
  - セッションおよび認証設定は、すべてのアプリに適用されます。
  - 一部のアプリには、特定のコンテナ化、MDX、認証、ジオフェンシング、パスコード、またはデータ共有の要件がある場合があります。

  展開を簡素化するために、これらの要件を事前に概説してください。Citrix Endpoint Managementのセキュリティの詳細については、「セキュリティとユーザーエクスペリエンス」を参照してください。
- **展開要件:** ポリシーベースの展開を使用して、準拠しているユーザーのみが公開されたアプリをダウンロードできるようにしたい場合があります。たとえば、特定のアプリでは、デバイスが管理されていること、またはデバイスが最小オペレーティングシステムバージョンを満たしていることが必要になる場合があります。また、特定のアプリを企業ユーザーのみが利用できるようにしたい場合もあります。適切な展開ルールまたはアクションを構成できるように、これらの要件を事前に概説してください。
- **ライセンス要件:** アプリ関連のライセンス要件を記録しておきます。メモは、ライセンスの使用状況を効果的に管理し、ライセンスを容易にするためにCitrix Endpoint Managementで特定の機能を構成するかどうかを決定するのに役立ちます。たとえば、無料または有料のiOSアプリを展開する場合、Appleはアプリにライセンス要件を適用します。その結果、ユーザーはApple App Storeアカウントにサインインする必要があります。

  ただし、Apple Volume Purchaseに登録することで、Citrix Endpoint Managementを使用してこれらのアプリを配布および管理できます。Volume Purchaseを使用すると、ユーザーはApple App Storeアカウントにサインインすることなくアプリをダウンロードできます。

  一部のプラットフォームでは、それらの機能を展開する前に完了する必要がある特別なライセンス要件があります。
- **許可リストとブロックリストの要件:** ユーザーにインストールまたは使用させたくないアプリを特定する場合があります。ブロックリストを作成すると、コンプライアンス違反イベントが定義されます。その後、イベントが発生したときにトリガーされるポリシーを設定できます。一方、アプリは使用可能であるにもかかわらず、何らかの理由でブロックリストに含まれる場合があります。その場合、アプリを許可リストに追加し、そのアプリは使用可能であるが必須ではないことを示すことができます。また、新しいデバイスにプリインストールされているアプリには、オペレーティングシステムの一部ではない一般的なアプリが含まれる場合があるこ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

とに注意してください。このようなアプリは、ブロックリスト戦略と競合する可能性があります。

ユースケース

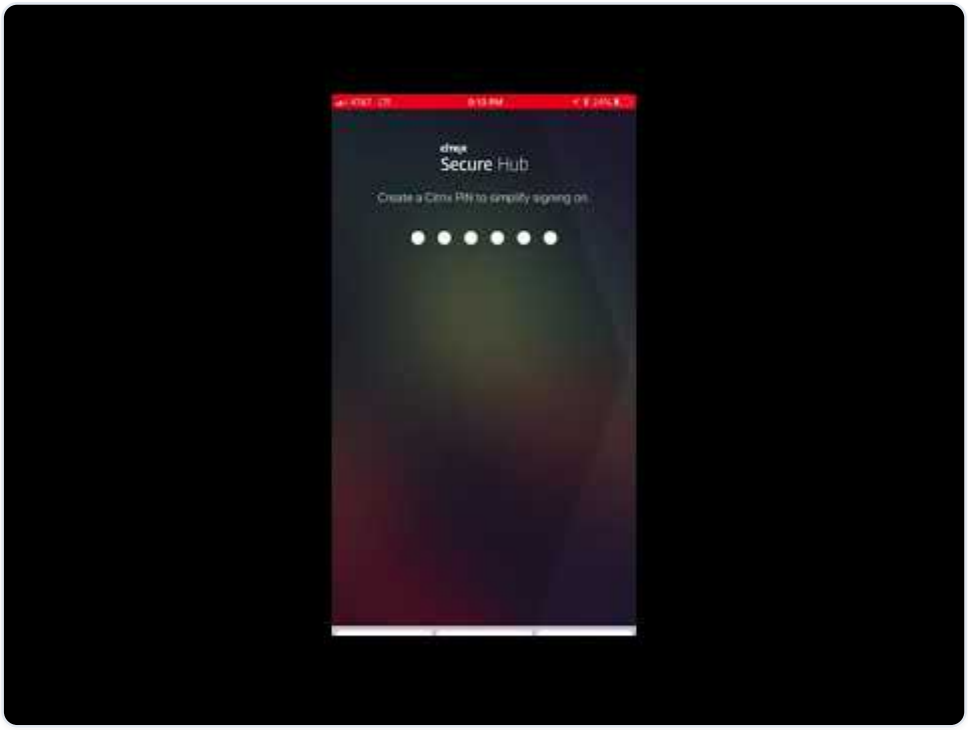
医療機関は、モバイルアプリのMAMソリューションとして機能させるためにCitrix Endpoint Managementを展開する予定です。モバイルアプリは、企業ユーザーとBYODユーザーに配信されます。IT部門は、以下のアプリを配信および管理することを決定しました。

モバイル生産性アプリ: Citrixが提供するiOSおよびAndroidアプリ。詳細については、「モバイル生産性アプリ」を参照してください。

Citrix Secure Hub: Citrix Endpoint Management 10.18.14より前にオンボーディングしたお客様の場合: Citrix Secure Hubを使用して、セキュリティ設定、構成、およびモバイルアプリをモバイルデバイスにプッシュします。AndroidおよびiOSデバイスは、Citrix Secure Hubを介してCitrix Endpoint Managementに登録されます。

Citrix Endpoint Management 10.18.14以降の新規のお客様の場合: Citrix Secure HubはWorkspaceアプリストアの使用をサポートしています。Citrix Secure Hubを開くと、ユーザーはCitrix Secure Hubストアを表示しなくなります。現在、「アプリの追加」ボタンをクリックすると、ユーザーはWorkspaceアプリストアに移動します。

以下は、Citrix Workspaceアプリを使用してiOSデバイスがCitrix Endpoint Managementに登録する様子を示すビデオです。



.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspaceアプリ: Citrix Workspaceアプリは、既存のCitrix Receiverテクノロジー、Citrix Secure Hub、およびその他のCitrix Workspaceクライアントテクノロジーを統合しています。Citrix Workspaceアプリは、エンドユーザーに統一されたコンテキストに応じたエクスペリエンスを提供します。

GoToMeeting: ユーザーがインターネットを介して他のコンピューターユーザー、顧客、クライアント、または同僚とリアルタイムで会議できるようにする、オンライン会議、デスクトップ共有、ビデオ会議クライアント。

SalesForce1: Salesforce1を使用すると、ユーザーはモバイルデバイスからSalesforceにアクセスでき、すべてのChatter、CRM、カスタムアプリ、およびビジネスプロセスを、あらゆるSalesforceユーザー向けの統一されたエクスペリエンスにまとめます。

RSA SecurID: 2要素認証用のソフトウェアベースのトークン。

EpicCareアプリ: これらのアプリは、医療従事者に患者のカルテ、患者リスト、スケジュール、およびメッセージングへの安全でポータブルなアクセスを提供します。

Haiku: iPhoneおよびAndroidフォン用のモバイルアプリ。

Canto: iPad用のモバイルアプリ

Rover: iPhoneおよびiPad用のモバイルアプリ。

HDX: これらのアプリは、Citrix WorkspaceのCitrix Virtual Appsを介して配信されます。

- **Epic Hyperspace:** 電子カルテ管理用のEpicクライアントアプリケーション。

ISV:

- **Vocera:** HIPAA準拠のVoIPおよびメッセージングモバイルアプリで、iPhoneおよびAndroidスマートフォンを介して、いつでもどこでもVocera音声テクノロジーの利点を拡張します。

社内アプリ:

- **HCMail:** 暗号化されたメッセージを作成し、社内メールサーバーのアドレス帳を検索し、メールクライアントを使用して暗号化されたメッセージを連絡先に送信するのに役立つアプリ。

社内Webアプリ:

- **PatientRounding:** さまざまな部署が患者の健康情報を記録するために使用するWebアプリケーション。
- **Outlook Web Access:** Webブラウザを介したメールへのアクセスを可能にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **SharePoint:** 組織全体のファイルおよびデータ共有に使用されます。

次の表に、MAM構成に必要な基本情報を示します。

アプリ名	アプリの種類	MDX対応	IOS	アンドロイド
シトリックス セキュア メール	モバイル生産性アプリ	いいえ	はい	はい
シトリックス セキュア ウェブ	モバイル生産性アプリ	いいえ	はい	はい
シトリックス ファイル	モバイル生産性アプリ	いいえ	はい	はい
シトリックス セキュア ハブ	公開アプリ	N/A	はい	はい
Citrix Workspaceアプリ	公開アプリ	N/A	はい	はい
GoToMeeting	公開アプリ	N/A	はい	はい
SalesForce1	公開アプリ	N/A	はい	はい
RSA SecurID	公開アプリ	N/A	はい	はい
エピック ハイク	公開アプリ	N/A	はい	はい
エピック カント	公開アプリ	該当なし	はい	いいえ
エピック ローバー	公開アプリ	該当なし	はい	いいえ
エピック ハイパースペース	HDXアプリ	該当なし	はい	はい
ヴォセーラ	ISV アプリ	はい	はい	はい
エイチシーメール	社内アプリ	はい	はい	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ名	アプリの種類	MDX対応	IOS	アンドロイド
PatientRounding	Web アプリ	該当なし	はい	はい
アウトルック ウェブ アクセス	Webアプリ	N/A	はい	はい
SharePoint	Webアプリ	N/A	はい	はい

以下の表に、Citrix Endpoint Management で MAM ポリシーを構成する際に参照できる特定の要件を示します。

アプリ名	VPNが必要	相互作用 (コンテナ外のアプリとの)	相互作用 (コンテナ外のアプリからの)	プロキシフィルタリング	ライセンス	ジオフェンシング	モバイルアプリSDK	最小オペレーティングシステムバージョン
シトリックス セキュアメール	Y	選択的に許可	許可	必須	N/A	選択的に必須	N/A	強制
Citrix セキュアウェブ	はい	許可	許可	必須	該当なし	不要	該当なし	強制
Citrix ファイル	はい	許可	許可	必須	該当なし	不要	該当なし	強制
シトリックス セキュアハブ	はい	該当なし	該当なし	不要	ボリューム購入	不要	該当なし	強制なし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ名	VPNが必要	相互作用 (コンテナ外のアプリとの)	相互作用 (コンテナ外のアプリからの)	プロキシフィルタリング	ライセンス	ジオフェンシング	モバイルアプリSDK	最小オペレーティングシステムバージョン
Citrix Workspace アプリ	はい	該当なし	該当なし	不要	ボリューム購入	不要	該当なし	強制されない
GoTo Meeting	N	該当なし	該当なし	不要	ボリューム購入	不要	該当なし	強制されない
Sales Force 1	N	N/A	N/A	不要	ボリューム購入	不要	N/A	適用されません
RSA SecurID	N	N/A	N/A	不要	ボリューム購入	不要	該当なし	適用されない
エピック ハイク	はい	該当なし	該当なし	不要	ボリューム購入	不要	該当なし	適用されない
エピック カント	はい	該当なし	該当なし	不要	ボリューム購入	不要	N/A	適用されません
エピック ローバー	Y	N/A	N/A	不要	ボリューム購入	不要	N/A	適用されません
エピック ハイパースペース	はい	該当なし	該当なし	不要	該当なし	不要	該当なし	強制なし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリ名	VPNが必要	相互作用 (コンテナ外のアプリとの)	相互作用 (コンテナ外のアプリからの)	プロキシフィルタリング	ライセンス	ジオフェンシング	モバイルアプリSDK	最小オペレーティングシステムバージョン
ボセラ	はい	ブロック済み	ブロック済み	必須	該当なし	必須	必須	強制
エイチシーメール	Y	ブロック済み	ブロック済み	必須	N/A	必須	必須	強制
PatientRound-ing	Y	N/A	N/A	必須	該当なし	不要	該当なし	強制されない
Outlook Web アクセス	はい	該当なし	該当なし	必須	該当なし	不要	該当なし	強制されない
SharePoint	はい	該当なし	該当なし	必須	該当なし	不要	該当なし	適用なし

ユーザーコミュニティ

組織はそれぞれ、異なる機能的役割を担う多様なユーザーコミュニティで構成されています。これらのユーザーコミュニティは、ユーザーのモバイルデバイスを通じて提供されるさまざまなリソースを使用して、異なるタスクやオフィス機能を実行します。ユーザーは、提供されたモバイルデバイスを使用して自宅や遠隔地のオフィスで作業する場合があります。または、個人用モバイルデバイスを使用して、特定のセキュリティコンプライアンス規則の対象となるツールにアクセスすることもあります。

モバイルデバイスを使用するユーザーコミュニティが増えるにつれて、データ漏洩を防ぎ、組織のセキュリティ制限を適用するために、Enterprise Mobility Management (EMM) が不可欠になります。効率的でより高度なMobile Device Managementを実現するために、ユーザーコミュニティを分類できます。これにより、ユーザーとリソースのマッピングが簡素化され、適切なセキュリティポリシーが適切なユーザーに適用されるようになります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーコミュニティの分類には、次のコンポーネントの使用が含まれます。

- Active Directoryの組織単位 (OU) とグループ

  Users added to specific Active Directory security groups can receive policies and resources such as apps. Removing users from the Active Directory security groups removes access to previously allowed Citrix Endpoint Management resources.

- Citrix Endpoint Management local users and groups

  For users who don't have an account in Active Directory, you can create the users as local Citrix Endpoint Management users. You can add local users to delivery groups and provision resources to them in the same manner as Active Directory users.

- Citrix Endpoint Management delivery groups

  異なるレベルの権限を持つ多数のユーザーグループが単一のアプリを使用する場合、個別のデリバリーグループを作成することをお勧めします。個別のデリバリーグループを使用すると、同じアプリの2つの異なるバージョンを展開できます。Citrix®は、デバイスポリシーを作成する前にデリバリーグループを作成することを推奨しています。

- デリバリーグループとユーザーグループのマッピング

  デリバリーグループとActive Directoryグループのマッピングは、1対1または1対多のいずれかです。基本ポリシーとアプリは1対多のデリバリーグループマッピングに割り当てます。機能固有のポリシーとアプリは1対1のデリバリーグループマッピングに割り当てます。

- デリバリーグループとアプリのリソースマッピング

  各デリバリーグループに特定のアプリを割り当てます。

- デリバリーグループとMDMリソースのリソースマッピング

  各デリバリーグループにアプリと特定のデバイス管理リソースを割り当てます。たとえば、次の任意の組み合わせでデリバリーグループを構成します。アプリの種類（パブリック、HDX™など）、アプリの種類ごとの特定のアプリ、およびデバイスポリシーや自動アクションなどのリソース。

次の例は、医療機関のユーザーコミュニティがEMM向けにどのように分類されているかを示しています。

ユースケース

この医療機関の例では、ネットワークおよび関連会社の従業員やボランティアを含む多くのユーザーにテクノロジーリソースとアクセスを提供しています。この組織は、EMMソリューションを非管理職ユーザーにのみ展開することを選択しました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

この組織のユーザーの役割と機能は、臨床、非臨床、契約社員などのサブグループに分けることができます。一部のユーザーは会社のモバイルデバイスを受け取り、他のユーザーは個人のデバイス（BYOD）から限られた会社の情報にアクセスできます。適切なレベルのセキュリティ制限を適用し、データ漏洩を防ぐため、組織は登録された各デバイスを企業ITが管理することを決定しました。また、ユーザーは1つのデバイスしか登録できません。

以下のセクションでは、各サブグループの役割と機能の概要を説明します。

臨床

- 看護師
- 医師（内科医、外科医など）
- 専門医（栄養士、麻酔科医、放射線科医、循環器科医、腫瘍内科医など）
- 外部医師（非従業員の医師およびリモートオフィスで働く事務員）
- 在宅医療サービス（患者宅への往診を行う事務員およびモバイルワーカー）
- 研究専門家（6つの研究所で医学の問題に対する答えを見つけるための臨床研究を行うナレッジワーカーおよびパワーユーザー）
- 教育と研修（教育と研修に携わる看護師、医師、専門家）

非臨床

- 共有サービス（人事、給与、買掛金、サプライチェーンサービスなど、さまざまなバックオフィス業務を行うオフィスワーカー）
- 医師サービス（管理サービス、分析およびビジネスインテリジェンス、ビジネスシステム、クライアントサービス、財務、マネージドケア管理、患者アクセスソリューション、収益サイクルソリューションなど、医療管理、管理サービス、ビジネスプロセスソリューションをプロバイダーに提供するオフィスワーカー）
- サポートサービス（福利厚生管理、臨床統合、コミュニケーション、報酬および業績管理、施設および不動産サービス、人事テクノロジーシステム、情報サービス、内部監査およびプロセス改善など、さまざまな非臨床業務を行うオフィスワーカー）
- 慈善プログラム（慈善プログラムを支援するためにさまざまな業務を行うオフィスワーカーおよびモバイルワーカー）

請負業者

- 製造元およびベンダーパートナー（オンサイトおよびサイト間VPN経由でリモート接続し、さまざまな非臨床サポート機能を提供）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

上記の情報に基づき、組織は以下のエンティティを作成しました。Citrix Endpoint Management のデリバリーグループの詳細については、Citrix Endpoint Management 製品ドキュメントの「リソースの展開」を参照してください。

Active Directory 組織単位 (OU) およびグループ

OUの場合 = Citrix Endpoint Management リソース

- OU = 臨床; グループ =
  - XM-ナース
  - XM-フィジシャン
  - XM-スペシャリスト
  - XM-外部フィジシャン
  - XM-ホームヘルスサービス
  - XM-研究スペシャリスト
  - XM-教育およびトレーニング
- OU = 非臨床; グループ =
  - XM-共有サービス
  - XM-医師サービス
  - XM-サポートサービス
  - XM-慈善プログラム

Citrix Endpoint Management のローカルユーザーとグループ

グループ = 請負業者、ユーザー =

- ベンダー1
- ベンダー2
- ベンダー3
- … ベンダー10

Citrix Endpoint Management のデリバリーグループ

- 臨床看護師
- 臨床 - 医師
- 臨床 - 専門医

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 臨床 - 外部医師
- 臨床 - 在宅医療サービス
- 臨床 - 研究専門家
- 臨床 - 教育および研修
- 非臨床 - 共有サービス
- 非臨床 - 医師サービス
- 非臨床 - サポートサービス
- 非臨床 - 慈善プログラム

デリバリーグループとユーザーグループのマッピング

ACTIVE DIRECTORY グループ	CITRIX ENDPOINT MANAGEMENT デリバリーグループ
XM-看護師	臨床 - 看護師
XM-医師	臨床-医師
XM-専門医	臨床-専門医
XM-外部医師	臨床-外部医師
XM-在宅医療サービス	臨床-在宅医療サービス
XM-研究専門家	臨床-研究専門家
XM-教育および研修	臨床-教育および研修
XM-共有サービス	非臨床-共有サービス
XM-医師サービス	非臨床 - 医師サービス
XM - サポートサービス	非臨床 - サポートサービス
XM - 慈善プログラム	非臨床 - 慈善プログラム

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリのデリバリーグループとリソースマッピング

	セキュアメール	セキュアウェブ	CITRIX ファイルズ	WORKSPACEアプリ	SALESFORCE1	RSA SECURID	エピックケアハイク	エピック ハイパースペース
臨床 - 看護師	X	X	X					
臨床医								
臨床専門医								
臨床-外部医師	X		X					
臨床-在宅医療サービス	X		X					
臨床-研究専門家	X		X					
臨床-教育および研修							X	X
非臨床 - 共有サービス							X	X
非臨床 - 医師サービス							X	X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	セキュアメール	セキュアウェブ	CITRIX ファイルズ	WORKSPACEアプリ	SALESFORCE1	RSA SECURID	エピックケアハイク	エピック ハイパースペース
非臨床 - サポートサービス	X		X				X	X
非臨床 - 慈善プログラム	X		X				X	X
契約社員	X		X	X	X		X	X

MDMリソースのデリバリーグループとリソースマッピング

	MDM: パスコードポリシー	MDM: デバイス制限	MDM: 自動アクション	MDM: ネットワークポリシー
臨床 - 看護師				X
臨床 - 医師		X		
臨床 - 専門家				
臨床 - 外部医師				
臨床 - 在宅医療サービス				
臨床 - 研究専門家				
臨床 - 教育および研修				
非臨床 - 共有サービス				

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	MDM: パスコードポリシー	MDM: デバイス制限	MDM: 自動アクション	MDM: ネットワークポリシー
非臨床 - 医師サービス				
非臨床 - サポートサービス				
非臨床 - 慈善プログラム				
契約者				X

注意事項と考慮事項

- Citrix Endpoint Managementは、初期構成時にAll Usersという名前のデフォルトのデリバリーグループを作成します。このデリバリーグループを無効にしない場合、すべてのActive DirectoryユーザーはCitrix Endpoint Managementに登録する権利を持ちます。
- Citrix Endpoint Managementは、LDAPサーバーへの動的接続を使用して、Active Directoryユーザーとグループをオンデマンドで同期します。
- ユーザーがCitrix Endpoint Managementにマッピングされていないグループに属している場合、そのユーザーは登録できません。同様に、ユーザーが多数のグループのメンバーである場合、Citrix Endpoint Managementは、そのユーザーをCitrix Endpoint Managementにマッピングされているグループに属しているものとしてのみ分類します。

メール戦略

モバイルデバイスからのメールへのセキュアなアクセスは、あらゆる組織のモビリティ管理イニシアチブの主要な推進要因の1つです。適切なメール戦略を決定することは、Citrix Endpoint Managementの設計において重要な要素となることがよくあります。Citrix Endpoint Managementは、セキュリティ、ユーザーエクスペリエンス、統合要件に基づいて、さまざまなユースケースに対応するためのいくつかのオプションを提供します。この記事では、クライアントの選択からメールトラフィックフローまで、適切なソリューションを選択するための一般的な設計決定プロセスと考慮事項について説明します。

メールクライアントの選択

クライアントの選択は、通常、全体的なメール戦略設計において最優先事項です。Citrix Secure Mail、特定のモバイルプラットフォームのオペレーティングシステムに付属するネイティブメール、または公開アプリストアを通じて利用可能なその他のサードパーティクライアントなど、い

© 1997–2026 Citrix Systems, Inc. All rights reserved.

くつかのクライアントから選択できます。ニーズに応じて、単一の（標準）クライアントでユーザーコミュニティをサポートすることも、複数のクライアントを組み合わせて使用する必要がある場合もあります。

次の表は、利用可能なさまざまなクライアントオプションに関する設計上の考慮事項の概要を示しています。

トピック	シトリックス セキュア メール	ネイティブ (例: iOS メール)	サードパーティメール
構成	MDXポリシーを介して構成されたExchangeアカウントプロファイル。	MDMポリシーを介して構成されたExchangeアカウントプロファイル。Androidのサポートは Android Enterpriseに限定されます。その他のすべてのクライアントはサードパーティクライアントと見なされます。	通常、ユーザーによる手動構成が必要です。
セキュリティ	設計上セキュアであり、最高のセキュリティを提供します。データ暗号化レベルが追加されたMDXポリシーを使用します。Citrix Secure Mailは、MDXポリシーを介して完全に管理されるアプリです。Citrix PINによる認証の追加レイヤーがあります。	ベンダー/アプリの機能セットに基づく。より高いセキュリティを提供する。デバイスの暗号化設定を使用する。アプリへのアクセスにはデバイスレベルの認証に依存する。	ベンダー/アプリの機能セットに基づく。高いセキュリティを提供する。
統合	デフォルトで管理対象 (MDX) アプリとの連携を可能にする。Citrix Secure Web で Web URL を開く。Citrix Files にファイ	デフォルトでは、他の非管理対象 (非MDX) アプリとのみ連携できる。	デフォルトでは、他の非管理対象 (非MDX) アプリとのみ連携できる。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	ルを保存したり、Citrix Files からファイルを添付したりする。GoToMeeting に直接参加したり、ダイヤルインしたりする。		
展開/ライセンス	Citrix Secure Mail は、MDM を介して、またはパブリックアプリストアから直接プッシュできます。Citrix Endpoint Management Advanced および Enterprise ライセンスに含まれています。	プラットフォームのオペレーティングシステムに含まれるクライアントアプリ。追加のライセンス要件なし。	MDM を介して、エンタープライズアプリとして、またはパブリックアプリストアから直接プッシュできます。関連するライセンスモデル/コストはアプリベンダーに基づきます。
サポート	クライアントとEMMソリューション（Citrix）に対する単一ベンダーサポート。Citrix Secure Hub/アプリデバッグログ機能にサポート連絡先情報が埋め込まれている。サポートするクライアントは1つ。	ベンダー定義のサポート（Apple/Google）。デバイスプラットフォームに基づいて異なるクライアントをサポートする必要がある場合があります。	ベンダー定義のサポート。サードパーティ製クライアントがすべての管理対象デバイスプラットフォームでサポートされていると仮定した場合、サポートするクライアントは1つ。

メールトラフィックフローとフィルタリングに関する考慮事項

このセクションでは、Citrix Endpoint Management のコンテキストにおけるメール (ActiveSync) トラフィックの流れに関する3つの主要なシナリオと設計上の考慮事項について説明します。

シナリオ1：公開されたExchange

外部クライアントをサポートする環境では、通常、Exchange ActiveSyncサービスがインターネットに公開されています。モバイルActiveSyncクライアントは、リバースプロキシ（例：NetScaler Gateway）またはEdge Serverを介して、この外部に面したパス経由で接続します。このオプショ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ンは、ネイティブまたはサードパーティのメールクライアントを使用するために必要であり、これらのクライアントがこのシナリオで一般的な選択肢となっています。一般的な方法ではありませんが、このシナリオでCitrix Secure Mailクライアントを使用することもできます。そうすることで、MDXポリシーの使用とアプリの管理によって提供されるセキュリティ機能の恩恵を受けることができます。

シナリオ2：NetScaler Gateway経由のトンネル接続（マイクロVPNおよびSTA）

このシナリオは、Citrix Secure Mailクライアントを使用する場合のデフォルトです。これは、そのマイクロVPN機能によるものです。この場合、Citrix Secure MailクライアントはNetScaler GatewayをActiveSyncへのセキュアな接続を確立します。本質的に、Citrix Secure Mailは内部ネットワークからActiveSyncに直接接続するクライアントと見なすことができます。Citrixのお客様は、モバイルActiveSyncクライアントとしてCitrix Secure Mailを標準化することがよくあります。この決定は、最初のシナリオで説明したように、公開されたExchange Server上でActiveSyncサービスをインターネットに公開することを避けるための取り組みの一部です。

MAM SDKが有効になっているアプリ、またはMDXでラップされたアプリのみがマイクロVPN機能を使用できます。MDXラッピングを使用する場合、このシナリオはネイティブクライアントには適用されません。MDX Toolkitでサードパーティクライアントをラップすることは可能かもしれませんが、この方法は一般的ではありません。ネイティブまたはサードパーティクライアントのトンネルアクセスを許可するためにデバイスレベルのVPNクライアントを使用することは、煩雑であり、実現可能なソリューションではないことが証明されています。

シナリオ3：クラウドホスト型Exchangeサービス

Microsoft Office 365などのクラウドホスト型Exchangeサービスは、ますます普及しています。Citrix Endpoint Managementのコンテキストでは、ActiveSyncサービスもインターネットに公開されているため、このシナリオは最初のシナリオと同じように扱われる可能性があります。この場合、クラウドサービスプロバイダーの要件がクライアントの選択を決定します。選択肢には通常、Citrix Secure Mailやその他のネイティブまたはサードパーティクライアントなど、ほとんどのActiveSyncクライアントのサポートが含まれます。

このシナリオにおいて、Citrix Endpoint Managementは3つの領域で価値を付加できます。

- MDXポリシーとCitrix Secure Mailによるアプリ管理を備えたクライアント
- サポートされているネイティブメールクライアントでのMDMポリシーを使用したクライアント構成
- Exchange ActiveSync用Citrix Endpoint Managementコネクタを使用したActiveSyncフィルタリングオプション

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メールトラフィックフィルタリングの考慮事項

インターネットに公開されるほとんどのサービスと同様に、パスを保護し、認証されたアクセスに対してフィルタリングを提供する必要があります。Citrix Endpoint Managementソリューションには、ネイティブおよびサードパーティクライアント向けのActiveSyncフィルタリング機能を提供するために特別に設計された2つのコンポーネントが含まれています。それは、Exchange ActiveSync用NetScaler GatewayコネクタとExchange ActiveSync用Citrix Endpoint Managementコネクタです。

エクスチェンジ アクティブシンク用ネットスケーラー ゲートウェイ コネクタ

NetScaler GatewayのExchange ActiveSync用コネクタは、NetScaler GatewayをActiveSyncトラフィックのプロキシとして使用することで、境界でのActiveSyncフィルタリングを提供します。その結果、フィルタリングコンポーネントはメールトラフィックフローの経路に位置し、メールが環境に出入りする際に傍受します。Exchange ActiveSync用コネクタは、NetScaler GatewayとCitrix Endpoint Management間の仲介役として機能します。デバイスがNetScaler Gateway上のActiveSync仮想サーバーを介してExchangeと通信すると、NetScaler GatewayはExchange ActiveSyncサービス用コネクタにHTTPコールアウトを実行します。そのサービスは、Citrix Endpoint Managementでデバイスのステータスを確認します。デバイスのステータスに基づいて、Exchange ActiveSync用コネクタはNetScaler Gatewayに接続を許可するか拒否するかを応答します。ユーザー、エージェント、デバイスの種類、またはIDに基づいてアクセスをフィルタリングするための静的ルールを設定することもできます。

この設定により、Exchange ActiveSyncサービスをインターネットに公開し、不正アクセスを防ぐためのセキュリティ層を追加できます。設計上の考慮事項は次のとおりです。

- **Windows Server:** Exchange ActiveSyncコンポーネント用コネクタにはWindows Serverが必要です。
- **フィルタリングルールセット:** Exchange ActiveSync用コネクタは、ユーザー情報ではなく、デバイスの状態と情報に基づいてフィルタリングするように設計されています。ユーザーIDでフィルタリングするための静的ルールを設定することはできますが、たとえばActive Directoryグループメンバーシップに基づいてフィルタリングするオプションはありません。Active Directoryグループフィルタリングの要件がある場合は、代わりにCitrix Endpoint ManagementのExchange ActiveSync用コネクタを使用できます。
- **NetScaler Gatewayのスケーラビリティ:** NetScaler Gatewayを介してActiveSyncトラフィックをプロキシする必要があるため、すべてのActiveSync SSL接続の追加ワークロードをサポートするには、NetScaler Gatewayインスタンスの適切なサイジングが不可欠です。
- **NetScaler Gateway統合キャッシュ:** NetScaler Gateway上のExchange ActiveSync構成用コネクタは、統合キャッシュ機能を使用してコネクタからの応答をキャッシュします。この構成に

© 1997–2026 Citrix Systems, Inc. All rights reserved.

より、NetScaler Gatewayは特定のセッション内のすべてのActiveSyncトランザクションに対してコネクタにリクエストを発行する必要がありません。この構成は、適切なパフォーマンスと拡張性のためにも重要です。統合キャッシュはNetScaler Gateway Platinum Editionで利用可能です。

- **カスタムフィルタリングポリシー:** 標準のネイティブモバイルクライアント以外の特定のActiveSyncクライアントを制限するために、カスタムのNetScaler Gatewayポリシーを作成する必要がある場合があります。この構成には、ActiveSync HTTPリクエストとNetScaler Gatewayレスポンダーポリシーの作成に関する知識が必要です。
- **Citrix Secure Mailクライアント:** Citrix Secure MailにはマイクロVPN機能があり、境界でのフィルタリングの必要がありません。Citrix Secure Mailクライアントは、NetScaler Gatewayを介して接続されている場合、一般的に内部（信頼された）ActiveSyncクライアントとして扱われることがあります。ネイティブクライアントとサードパーティクライアント（Exchange ActiveSync用コネクタを使用）、およびCitrix Secure Mailクライアントの両方のサポートが必要な場合、CitrixはCitrix Secure Mailトラフィックがコネクタに使用されるNetScaler Gateway仮想サーバーを介して流れないようにすることを推奨します。このトラフィックフローはDNSを介して実現でき、コネクタポリシーがCitrix Secure Mailクライアントに影響を与えないようにすることができます。

Citrix Endpoint Management展開におけるNetScaler GatewayのExchange ActiveSync用コネクタの図については、アーキテクチャを参照してください。

シトリックス エンドポイント マネジメントのExchange ActiveSync用コネクタ

Citrix Endpoint ManagementのExchange ActiveSync用コネクタは、Exchangeサービスレベルで ActiveSyncフィルタリングを提供するCitrix Endpoint Managementコンポーネントです。その結果、フィルタリングはメールがCitrix Endpoint Management環境に入る時ではなく、Exchange サービスに到達した後にのみ行われます。Mail ManagerはPowerShellを使用してExchange ActiveSyncからデバイスのパートナーシップ情報を照会し、デバイスの隔離アクションを通じてアクセスを制御します。これらのアクションは、Citrix Endpoint ManagementのExchange ActiveSync用コネクタのルール基準に基づいてデバイスを隔離したり、隔離から解除したりします。

NetScaler GatewayのExchange ActiveSync用コネクタと同様に、Exchange ActiveSync用コネクタはCitrix Endpoint Managementでデバイスのステータスを確認し、デバイスのコンプライアンスに基づいてアクセスをフィルタリングします。デバイスの種類またはID、エージェントバージョン、およびActive Directoryグループメンバーシップに基づいてアクセスをフィルタリングするための静的ルールを設定することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このソリューションはNetScaler Gatewayの使用を必要としません。既存のActiveSyncトラフィックのルーティングを変更することなく、Exchange ActiveSync用コネクタを展開できます。設計上の考慮事項は次のとおりです。

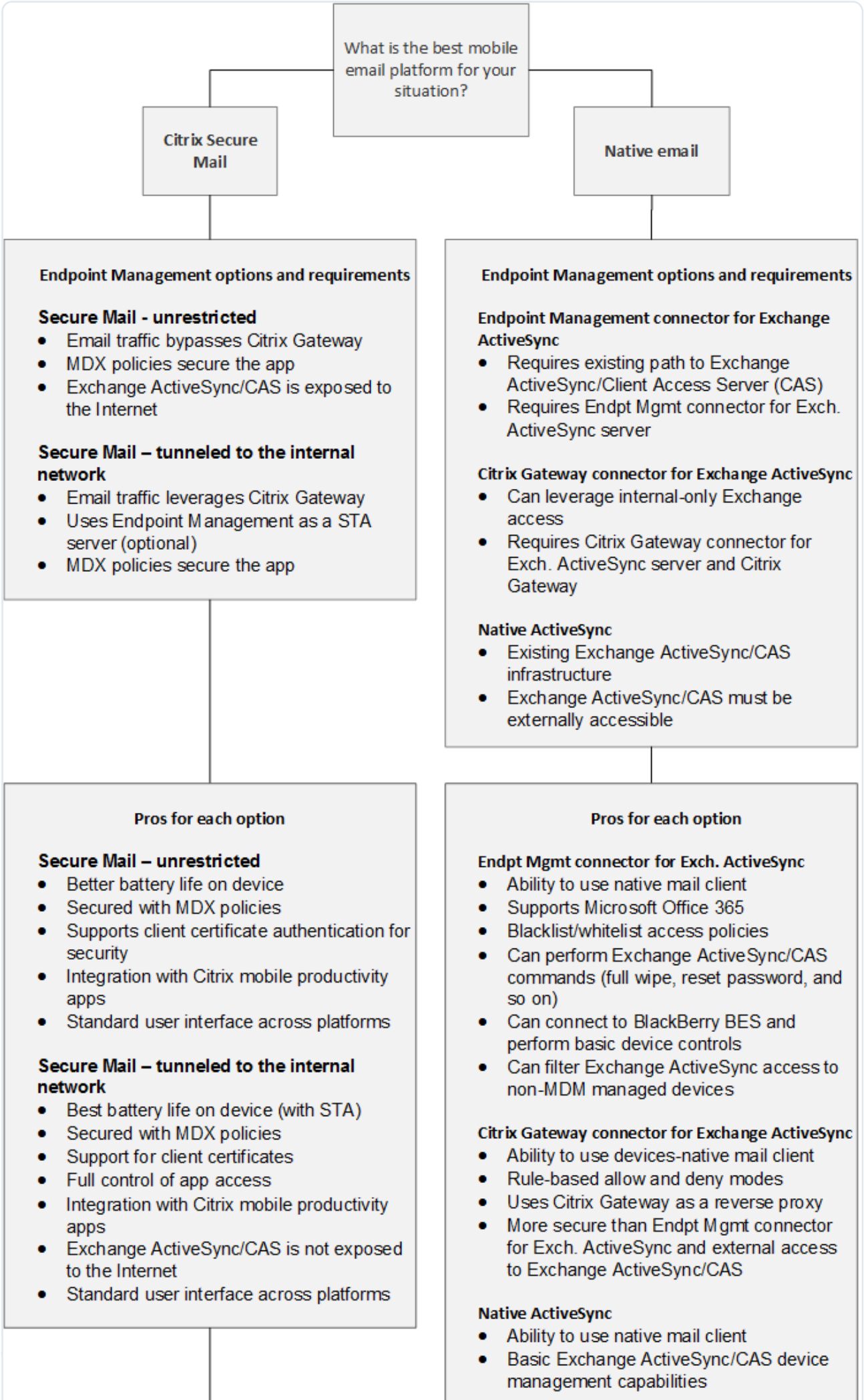
- **Windows Server:** Exchange ActiveSync用コネクタを展開するにはWindows Serverが必要です。
- **フィルタリングルールセット:** NetScaler GatewayのExchange ActiveSync用コネクタと同様に、Exchange ActiveSync用コネクタにはデバイスの状態を評価するためのフィルタリングルールが含まれています。また、Exchange ActiveSync用コネクタは、Active Directoryグループメンバーシップに基づいてフィルタリングするための静的ルールもサポートしています。
- **Exchange の統合:** Exchange ActiveSync 用コネクタは、ActiveSync ロールをホストする Exchange クライアントアクセスサーバー (CAS) への直接アクセスと、デバイスの隔離アクションの制御を必要とします。この要件は、環境のアーキテクチャとセキュリティ体制によっては課題となる可能性があります。この技術要件を事前に評価することが重要です。
- **その他の ActiveSync クライアント:** Exchange ActiveSync 用コネクタは ActiveSync サービスレベルでフィルタリングを行うため、Citrix Endpoint Management 環境外の他の ActiveSync クライアントを考慮してください。Exchange ActiveSync 用コネクタの静的ルールを構成して、他の ActiveSync クライアントへの意図しない影響を回避できます。
- **拡張された Exchange 機能:** Exchange ActiveSync との直接統合により、Exchange ActiveSync 用コネクタは、Citrix Endpoint Management がモバイルデバイスで Exchange ActiveSync ワイプを実行する機能を提供します。Exchange ActiveSync 用コネクタは、Citrix Endpoint Management が Blackberry デバイスに関する情報にアクセスし、その他の制御操作を実行することも可能にします。

Citrix Endpoint Management 展開における Exchange ActiveSync 用 Citrix Endpoint Management コネクタの図については、「アーキテクチャ」を参照してください。

メールプラットフォームの意思決定ツリー

次の図は、Citrix Endpoint Management 展開でネイティブメールソリューションと Citrix Secure Mail ソリューションのどちらを使用するかについて、それぞれの長所と短所を区別するのに役立ちます。各選択肢では、サーバー、ネットワーク、データベースへのアクセスを可能にするための関連する Citrix Endpoint Management オプションと要件が考慮されます。長所と短所には、セキュリティ、ポリシー、ユーザーインターフェイスに関する考慮事項が含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.


What is the best mobile email platform for your situation?
Citrix Secure Mail
Native email
Endpoint Management options and requirements
Secure Mail - unrestricted
Email traffic bypasses Citrix Gateway
MDX policies secure the app
Exchange ActiveSync/CAS is exposed to the Internet
Secure Mail – tunneled to the internal network
Email traffic leverages Citrix Gateway
Uses Endpoint Management as a STA server (optional)
MDX policies secure the app
Endpoint Management options and requirements
Endpoint Management connector for Exchange ActiveSync
Requires existing path to Exchange ActiveSync/Client Access Server (CAS)
Requires Endpt Mgmt connector for Exch. ActiveSync server
Citrix Gateway connector for Exchange ActiveSync
Can leverage internal-only Exchange access
Requires Citrix Gateway connector for Exch. ActiveSync server and Citrix Gateway
Native ActiveSync
Existing Exchange ActiveSync/CAS infrastructure
Exchange ActiveSync/CAS must be externally accessible
Pros for each option
Secure Mail – unrestricted
Better battery life on device
Secured with MDX policies
Supports client certificate authentication for security
Integration with Citrix mobile productivity apps
Standard user interface across platforms
Secure Mail – tunneled to the internal network
Best battery life on device (with STA)
Secured with MDX policies
Support for client certificates
Full control of app access
Integration with Citrix mobile productivity apps
Exchange ActiveSync/CAS is not exposed to the Internet
Standard user interface across platforms
Pros for each option
Endpt Mgmt connector for Exch. ActiveSync
Ability to use native mail client
Supports Microsoft Office 365
Blacklist/whitelist access policies
Can perform Exchange ActiveSync/CAS commands (full wipe, reset password, and so on)
Can connect to BlackBerry BES and perform basic device controls
Can filter Exchange ActiveSync access to non-MDM managed devices
Citrix Gateway connector for Exchange ActiveSync
Ability to use devices-native mail client
Rule-based allow and deny modes
Uses Citrix Gateway as a reverse proxy
More secure than Endpt Mgmt connector for Exch. ActiveSync and external access to Exchange ActiveSync/CAS
Native ActiveSync
Ability to use native mail client
Basic Exchange ActiveSync/CAS device management capabilities

シトリックス エンドポイント マネジメントの統合

この記事では、Citrix Endpoint Management を既存のネットワークおよびソリューションと統合する方法を計画する際に考慮すべき事項について説明します。たとえば、Citrix Virtual Apps and Desktops に NetScaler Gateway をすでに使用している場合:

- 既存の NetScaler Gateway インスタンスを使用しますか、それとも新しい専用インスタンスを使用しますか?
- StoreFront を使用して公開されている HDX アプリを Citrix Endpoint Management と統合しますか?
- Citrix Endpoint Management と Citrix Files を併用する予定ですか?
- Citrix Endpoint Management に統合したいネットワークアクセスコントロールソリューションをお持ちですか?

ネットスケーラー ゲートウェイ

NetScaler Gateway は Citrix Endpoint Management に必要です。NetScaler Gateway は、すべての企業リソースへのアクセスにマイクロ VPN パスを提供し、強力な多要素認証をサポートします。

既存の NetScaler Gateway インスタンスを使用することも、Citrix Endpoint Management 用に新しいインスタンスをセットアップすることもできます。以下のセクションでは、既存または新規の専用 NetScaler Gateway インスタンスを使用する利点と欠点について説明します。

Citrix Endpoint Management 用に作成された NetScaler Gateway VIP を持つ共有 NetScaler Gateway MPX

利点:

- すべての Citrix リモート接続 (Citrix Virtual Apps、フル VPN、クライアントレス VPN) に共通の NetScaler Gateway インスタンスを使用します。
- 証明書認証や、DNS、LDAP、NTP などのサービスへのアクセスなど、既存の NetScaler Gateway 構成を使用します。
- 単一の NetScaler Gateway プラットフォームライセンスを使用します。

欠点:

- 同じNetScaler Gatewayで2つの異なるユースケースを処理する場合、スケールの計画がより困難になります。
- Citrix Virtual Appsのユースケースでは、特定のNetScaler Gatewayバージョンが必要になる場合があります。その同じバージョンがCitrix Endpoint Managementで既知の問題を抱えている

© 1997–2026 Citrix Systems, Inc. All rights reserved.

可能性や、Citrix Endpoint ManagementがそのNetScaler Gatewayバージョンで既知の問題を抱えている可能性があります。

- NetScaler Gatewayが既に存在する場合、Citrix Endpoint Management用のNetScaler Gateway構成を作成するために、NetScaler for XenMobileウィザードを再度実行することはできません。
- NetScaler Gateway 11.1以降でPlatinumライセンスが使用されている場合を除き、NetScaler Gatewayにインストールされ、VPN接続に必要となるユーザーアクセスライセンスはプールされます。これらのライセンスはすべてのNetScaler Gateway仮想サーバーで利用できるため、Citrix Endpoint Management以外のサービスがそれらを消費する可能性があります。

専用のNetScaler Gateway VPX/MPXインスタンス

利点:

Citrixでは、NetScaler Gatewayの専用インスタンスを使用することをお勧めします。

- スケールの計画が容易になり、リソースが既に制約されている可能性のあるNetScaler GatewayインスタンスからCitrix Endpoint Managementトラフィックを分離できます。
- Citrix Endpoint ManagementとCitrix Virtual Appsで異なるNetScaler Gatewayソフトウェアバージョンが必要な場合に発生する問題を回避します。一般的に、Citrix Endpoint Managementには最新の互換性のあるNetScaler Gatewayバージョンとビルドを使用することをお勧めします。
- 組み込みのNetScaler for XenMobileウィザードを介したNetScaler GatewayのCitrix Endpoint Management構成を可能にします。
- サービスの仮想的および物理的な分離。

欠点:

- Citrix Endpoint Management構成をサポートするために、NetScaler Gatewayに追加のサービスを設定する必要があります。
- 別のNetScaler Gatewayプラットフォームライセンスが必要です。各NetScaler GatewayインスタンスにNetScaler Gatewayのライセンスを付与します。

Citrix Endpoint Management管理モードでNetScaler GatewayとCitrix ADCを統合する際に考慮すべき事項については、「NetScaler GatewayとCitrix ADCとの統合」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFront

Citrix Virtual Apps and Desktops 環境をお持ちの場合、StoreFront を使用して HDX アプリケーションを Citrix Endpoint Management と統合できます。HDX アプリを Citrix Endpoint Management と統合すると、次のようになります。

- アプリは、Citrix Endpoint Management に登録されているユーザーが利用できます。
- アプリは、他のモバイルアプリとともにアプリストアに表示されます。
- Citrix Endpoint Management は、StoreFront 上で Citrix Receiver を使用します。
- デバイスに Citrix Workspace アプリがインストールされている場合、HDX アプリはそのアプリを使用して起動します。

StoreFront には、StoreFront インスタンスごとに1つのサービスサイトという制限があります。多数のストアがあり、他の本番環境での使用から分離したいとします。その場合、Citrix は通常、Citrix Endpoint Management 用に新しい StoreFront インスタンスとサービスサイトを検討することを推奨します。

考慮事項は次のとおりです。

- StoreFront に異なる認証要件はありますか？StoreFront サービスサイトでは、ログオンに Active Directory 資格情報が必要です。証明書ベースの認証のみを使用しているお客様は、同じ NetScaler Gateway を使用して Citrix Endpoint Management 経由でアプリケーションを列挙することはできません。
- 同じストアを使用しますか、それともストアを作成しますか？
- 同じ StoreFront サーバーを使用しますか、それとも別の StoreFront サーバーを使用しますか？

以下のセクションでは、Citrix Workspace と Citrix モバイル生産性アプリに個別のまたは結合されたストアフロントを使用することの利点と欠点について説明します。

既存の StoreFront インスタンスを Citrix Endpoint Management と統合する

利点:

- 同じストア: HDX アクセスに同じ NetScaler Gateway VIP を使用することを前提として、Citrix Endpoint Management に追加の StoreFront 構成は不要です。同じストアを使用し、Citrix Workspace アクセスを新しい NetScaler Gateway VIP に誘導したいとします。その場合、適切な NetScaler Gateway 構成を StoreFront に追加します。
- 同じStoreFrontサーバー: 既存のStoreFrontのインストールと構成を使用します。

デメリット:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 同じストア: Citrix Virtual Apps and DesktopsのワークロードをサポートするためのStoreFrontの再構成は、Citrix Endpoint Managementに悪影響を及ぼす可能性があります。
- 同じStoreFrontサーバー: 大規模な環境では、アプリの列挙と起動のためにCitrix Receiverを使用するCitrix Endpoint Managementからの追加負荷を考慮してください。

Citrix Endpoint Managementとの統合に新しい専用のStoreFrontインスタンスを使用する

メリット:

- 新しいストア: Citrix Endpoint Management用のStoreFrontストアの構成変更は、既存のVirtual Apps and Desktopsワークロードに影響を与えません。
- 新しいStoreFrontサーバー: サーバー構成の変更は、Virtual Apps and Desktopsのワークフローに影響を与えません。また、アプリの列挙と起動のためにCitrix Receiverを使用するCitrix Endpoint Management以外の負荷は、スケーラビリティに影響を与えません。

デメリット:

- 新しいストア: StoreFrontストアの構成。
- 新しいStoreFrontサーバー: 新しいStoreFrontのインストールと構成が必要です。

詳細については、「アプリストアを介したCitrix Virtual Apps and Desktops」を参照してください。

シェアファイルとシトリックスファイル

免責事項:

ShareFile（現Progress）がサポートを中止した場合、この機能は非推奨になります。

ShareFile を使用すると、ドキュメントを簡単かつ安全に交換したり、大容量のドキュメントを電子メールで送信したり、サードパーティへのドキュメント転送を安全に処理したりできます。Citrix Files アプリを使用すると、ユーザーはあらゆるデバイスからすべてのデータにアクセスして同期できます。Citrix Files を使用すると、ユーザーは組織内外のユーザーとデータを安全に共有できます。

Citrix Endpoint Management は、Citrix Files に以下を提供します。

- モバイル生産性向上アプリユーザー向けのシングルサインオン認証。
- Active Directory ベースのユーザーアカウントプロビジョニング。
- 包括的なアクセス制御ポリシー。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

モバイルユーザーは、Enterprise アカウントの全機能セットを利用できます。

または、Citrix Endpoint Management を構成して、ストレージゾーンコネクタとのみ統合することもできます。ストレージゾーンコネクタを介して、Citrix Files は以下へのアクセスを提供します。

- ドキュメントとフォルダ
- ネットワークファイル共有
- SharePoint サイト内: サイトコレクションとドキュメントライブラリ。

接続されたファイル共有には、Citrix Virtual Apps and Desktops 環境で使用されるものと同じネットワークホームドライブを含めることができます。Citrix Endpoint Management コンソールを使用して、Enterprise アカウントまたはストレージゾーンコネクタとの統合を構成します。詳細については、「Citrix Files for Citrix Endpoint Management」を参照してください。

以下のセクションでは、Citrix Files の設計上の決定を行う際に考慮すべき質問について説明します。

Citrix Files またはストレージゾーンコネクタのみと統合する

考慮すべき質問:

- Citrix が管理するストレージゾーンにデータを保存しますか？
- ユーザーにファイル共有および同期機能を提供しますか？
- ユーザーがCitrix Files Webサイト上のファイルにアクセスできるようにしますか？それとも、モバイルデバイスからOffice 365コンテンツやパーソナルクラウドコネクタにアクセスできるようにしますか？

設計上の決定事項:

- これらの質問のいずれかに対する回答が「はい」の場合、エンタープライズアカウントと統合します。
- ストレージゾーンコネクタのみとの統合により、iOSユーザーはSharePointサイトやネットワークファイル共有などの既存のオンプレミスストレージリポジトリに安全にモバイルアクセスできます。この構成では、Citrix Filesサブドメインを設定したり、ユーザーをCitrix Filesにプロビジョニングしたり、Citrix Filesデータをホストしたりすることはありません。Citrix Endpoint Managementでストレージゾーンコネクタを使用すると、企業ネットワーク外へのユーザー情報の漏洩に対するセキュリティ制限が遵守されます。

ストレージゾーンコントローラーサーバーの場所

質問事項:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- オンプレミスストレージまたはストレージゾーンコネクタなどの機能が必要ですか？
- Citrix Filesのオンプレミス機能を使用する場合、ストレージゾーンコントローラーはネットワーク内のどこに配置されますか？

設計上の決定事項:

- ストレージゾーンコントローラーサーバーをCitrix Filesクラウド、オンプレミスのシングルテナントストレージシステム、またはサポートされているサードパーティのクラウドストレージのどこに配置するかを決定します。
- ストレージゾーンコントローラーは、Citrix Filesコントロールプレーンと通信するためにインターネットアクセスを必要とします。直接アクセスやNAT/PAT構成など、いくつかの方法で接続できます。

ストレージゾーンコネクタ

質問事項:

- CIFS共有パスは何ですか？
- SharePoint の URL は何ですか？

設計上の決定事項:

- それらの場所にアクセスするために、オンプレミスのストレージゾーンコントローラーが必要かどうかを判断します。
- ファイルリポジトリ、CIFS共有、SharePointなどの内部リソースとのストレージゾーンコネクタ通信のため、CitrixはストレージゾーンコントローラーをDMZファイアウォールの背後にある内部ネットワークに配置し、NetScaler Gatewayを前面に配置することを推奨します。

シトリックス エンドポイント マネジメント との SAML 統合

質問事項:

- Citrix Files に Active Directory 認証は必要ですか？
- Citrix Endpoint Management 用の Citrix Files アプリを初めて使用する場合、SSO は必要ですか？
- 現在の環境に標準の IdP はありますか？
- SAML を使用するには、いくつのドメインが必要ですか？
- Active Directory ユーザーに多くのメールエイリアスがありますか？
- Active Directory ドメインの移行が進行中または近日中に予定されていますか？

設計上の決定事項:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Files の認証メカニズムとして SAML を使用することを選択できます。認証オプションは次のとおりです。

- Citrix Endpoint Management サーバーを SAML の ID プロバイダー (IdP) として使用する

  このオプションは、優れたユーザーエクスペリエンスを提供し、Citrix Filesアカウントの作成を自動化し、モバイルアプリのSSO機能を有効にすることができます。

  Citrix Endpoint Managementサーバーはこのプロセス向けに強化されており、Active Directoryの同期は不要です。

  ユーザープロビジョニングには、Citrix Filesユーザー管理ツールを使用します。

- SAMLのIdPとして、サポートされているサードパーティベンダーを使用します。

  既存のサポートされているIdPがあり、モバイルアプリのSSO機能が不要な場合は、このオプションが最適かもしれません。このオプションでは、アカウントプロビジョニングのためにCitrix Filesユーザー管理ツールを使用することも必要です。

  ADFSなどのサードパーティIdPソリューションを使用すると、Windowsクライアント側でSSO機能を提供できる場合もあります。Citrix Files SAML IdPを選択する前に、ユースケースを必ず評価してください。

- または、両方のユースケースを満たすには、「デュアルIDプロバイダー向けShareFileシングルサインオン構成ガイド」を参照してください。

モバイルアプリ

質問事項:

- どのCitrix Filesモバイルアプリを使用する予定ですか（パブリック、MDM、MDX）？

設計上の決定事項:

- Citrixモバイル生産性向上アプリは、Apple App StoreおよびGoogle Playストアから配布します。そのパブリックアプリストア配布により、Citrixダウンロードページからラップされたアプリを入手できます。
- セキュリティ要件が低く、コンテナ化が不要な場合、パブリックCitrix Filesアプリは適さない可能性があります。
- 詳しくは、「アプリ」および「Citrix Endpoint Management向けCitrix Files」を参照してください。

セキュリティ、ポリシー、およびアクセス制御

質問事項:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- デスクトップ、Web、モバイルユーザーに対してどのような制限が必要ですか？
- ユーザーに対してどのような標準アクセス制御設定を希望しますか？
- どのようなファイル保持ポリシーを使用する予定ですか？

設計上の決定事項:

- Citrix Files を使用すると、従業員の権限を管理できます。詳細については、「従業員の権限」を参照してください。
- 一部の Citrix Files デバイスセキュリティ設定と MDX ポリシーは、同じ機能を制御します。これらの場合、Citrix Endpoint Management ポリシーが優先され、その後に Citrix Files デバイスセキュリティ設定が適用されます。例: Citrix Files で外部アプリを無効にしても、Citrix Endpoint Management で有効にした場合、外部アプリは Citrix Files で無効になります。Citrix Endpoint Management が PIN/パスコードを要求しないようにアプリを設定できますが、Citrix Files アプリは PIN/パスコードを要求します。

標準ストレージゾーンと制限付きストレージゾーン

質問事項:

- 制限付きストレージゾーンが必要ですか？

設計上の決定事項:

- 標準ストレージゾーンは、機密性の低いデータを対象としており、従業員が非従業員とデータを共有できるようにします。このオプションは、ドメイン外でのデータ共有を伴うワークフローをサポートします。
- 制限付きストレージゾーンは機密データを保護します。ゾーンに保存されているデータには、認証されたドメインユーザーのみがアクセスできます。

アクセス制御

企業は、ネットワークの内外でモバイルデバイスを管理できます。Citrix Endpoint Management のようなエンタープライズモビリティ管理ソリューションは、場所に関係なくモバイルデバイスにセキュリティと制御を提供するのに優れています。ただし、これらをネットワークアクセスコントロール (NAC) ソリューションと組み合わせると、ネットワーク内部のデバイスに QoS とよりきめ細かい制御を追加できます。この組み合わせにより、NAC ソリューションを通じて Citrix Endpoint Management デバイスセキュリティ評価を拡張できます。その後、NAC ソリューションは Citrix Endpoint Management セキュリティ評価を使用して、認証の決定を容易にし、処理できます。

NACポリシーを適用するために、以下のいずれかのソリューションを使用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ネットスケーラー ゲートウェイ
- ForeScout

Citrixは、他のNACソリューションとの統合を保証しません。

Citrix Endpoint ManagementとNACソリューションを統合する利点は次のとおりです。

- エンタープライズネットワーク上のすべてのエンドポイントに対するセキュリティ、コンプライアンス、および制御の向上。
- NACソリューションは次のことができます。
  - デバイスがネットワークに接続しようとした瞬間に検出する。
  - Citrix Endpoint Managementにデバイス属性を照会する。
  - そのデバイス情報を使用して、それらのデバイスを許可、ブロック、制限、またはリダイレクトするかどうかを決定する。これらの決定は、適用することを選択したセキュリティポリシーによって異なります。
- NACソリューションは、IT管理者に未管理および非準拠デバイスのビューを提供します。

Citrix Endpoint ManagementでサポートされているNACコンプライアンスフィルターの説明と構成の概要については、ネットワークアクセス制御を参照してください。

NetScaler Gateway と Citrix ADC との統合

Citrix Endpoint Management と統合すると、NetScaler Gateway は MAM デバイスの内部ネットワークへのリモートデバイスアクセス用の認証メカニズムを提供します。この統合により、Citrix モバイル生産性向上アプリは、マイクロ VPN を介してイントラネット内の企業サーバーに接続できます。Citrix Endpoint Management は、デバイス上のアプリから NetScaler Gateway へのマイクロ VPN を作成します。NetScaler Gateway は、すべての企業リソースへのアクセスにマイクロ VPN パスを提供し、強力な多要素認証をサポートします。

ユーザーが MDM 登録をオプトアウトすると、デバイスは NetScaler Gateway FQDN を使用して登録されます。

Citrix Cloud Operations が Citrix ADC の負荷分散を管理します。

設計上の決定事項

以下のセクションでは、NetScaler Gateway と Citrix Endpoint Management の統合を計画する際に考慮すべき多くの設計上の決定事項を要約します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書

決定の詳細:

- Citrix Endpoint Management 環境への登録とアクセスに、より高度なセキュリティが必要ですか？
- LDAP は選択肢ではありませんか？

設計ガイダンス:

Citrix Endpoint Management のデフォルト設定は、ユーザー名とパスワード認証です。Citrix Endpoint Management 環境への登録とアクセスに別のセキュリティ層を追加するには、証明書ベースの認証の使用を検討してください。証明書を LDAP と組み合わせて二要素認証に使用することで、RSA サーバーを必要とせずに、より高度なセキュリティを提供できます。

LDAP を許可せず、スマートカードまたは類似の方法を使用する場合、証明書を構成することで、スマートカードを Citrix Endpoint Management に提示できます。ユーザーは、Citrix Endpoint Management が生成する一意の PIN を使用して登録します。ユーザーがアクセス権を取得すると、Citrix Endpoint Management は、後で Citrix Endpoint Management 環境への認証に使用される証明書を作成および展開します。

Citrix Endpoint Management は、サードパーティの認証局に対してのみ証明書失効リスト (CRL) をサポートします。Microsoft CA を構成している場合、Citrix Endpoint Management は NetScaler Gateway を使用して失効を管理します。クライアント証明書ベースの認証を構成する際は、NetScaler Gateway の証明書失効リスト (CRL) 設定である **Enable CRL Auto Refresh** を構成する必要があるかどうかを検討してください。この手順により、MAM にのみ登録されているデバイスのユーザーが、デバイス上の既存の証明書を使用して認証できないようにします。Citrix Endpoint Management は、証明書が失効した場合にユーザーがユーザー証明書を生成することを制限しないため、新しい証明書を再発行します。この設定は、CRL が期限切れの PKI エンティティをチェックする際に、PKI エンティティのセキュリティを向上させます。

専用または共有の NetScaler Gateway VIP

決定の詳細:

- 現在、Citrix Virtual Apps and Desktops に NetScaler Gateway を使用していますか?
- Citrix Endpoint Management は、Citrix Virtual Apps and Desktops と同じ NetScaler Gateway を使用しますか?
- 両方のトラフィックフローの認証要件は何ですか?

設計ガイダンス:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix 環境に Citrix Endpoint Management と Virtual Apps and Desktops の両方が含まれている場合、両方に同じ NetScaler Gateway 仮想サーバーを使用できます。バージョン競合の可能性と環境分離のため、Citrix Endpoint Management 環境ごとに専用の NetScaler Gateway を使用することをお勧めします。

LDAP 認証を使用する場合、Citrix Secure Hub は問題なく同じ NetScaler Gateway に認証できます。証明書ベースの認証を使用する場合、Citrix Endpoint Management は MDX コンテナに証明書をプッシュし、Citrix Secure Hub はその証明書を使用して NetScaler Gateway で認証します。

2つの NetScaler Gateway VIP に同じ FQDN を使用できるこの回避策を検討できます。同じ IP アドレスを持つ2つの NetScaler Gateway VIP を作成できます。Citrix Secure Hub 用は標準のポート 443 を使用し、Citrix Virtual Apps and Desktops (Citrix Workspace アプリを展開する) 用はポート 444 を使用します。その後、1つの FQDN が同じ IP アドレスに解決されます。この回避策では、StoreFront を構成して、デフォルトのポート 443 ではなくポート 444 の ICA ファイルを返すようにする必要がある場合があります。この回避策では、ユーザーがポート番号を入力する必要はありません。

NetScaler Gateway のタイムアウト

決定の詳細:

- Citrix Endpoint Management トラフィックの NetScaler Gateway タイムアウトをどのように構成しますか?

設計ガイダンス:

NetScaler Gateway には、セッションタイムアウトと強制タイムアウトの設定が含まれています。詳細については、推奨される構成 を参照してください。バックグラウンドサービス、NetScaler Gateway、およびオフラインでのアプリケーションアクセスには、異なるタイムアウト値があることに注意してください。

登録 FQDN

重要:

登録FQDNを変更するには、新しいSQL ServerデータベースとCitrix Endpoint Management サーバーの再構築が必要です。

Citrix Secure Webトラフィック

決定の詳細:

- Citrix Secure Webを内部Webブラウジングのみに制限しますか？

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Secure Webを内部および外部Webブラウジングの両方で有効にしますか？

設計ガイダンス:

Citrix Secure Webを内部Webブラウジングのみに使用する予定の場合、NetScaler Gatewayの構成は簡単です。ただし、Citrix Secure Webがデフォルトですべての内部サイトに到達できない場合、ファイアウォールとプロキシサーバーを構成する必要があるかもしれません。

Citrix Secure Webを内部および外部ブラウジングの両方で使用する予定の場合、SNIPでアウトバウンドインターネットアクセスを有効にする必要があります。IT部門は通常、登録済みデバイス（MDXコンテナを使用）を企業ネットワークの拡張と見なします。そのため、IT部門は通常、Citrix Secure Web接続がNetScaler Gatewayに戻り、プロキシサーバーを経由してインターネットにアクセスすることを望んでいます。デフォルトでは、Citrix Secure Webアクセスは内部ネットワークにトンネル接続します。Citrix Secure Webは、すべてのネットワークアクセスに対して内部ネットワークへのアプリケーションごとのVPNトンネルを使用し、NetScaler Gatewayはスプリットトンネル設定を使用します。

Citrix Secure Web接続の詳細については、「ユーザー接続の構成」を参照してください。

Citrix Secure Mailのプッシュ通知

決定の詳細:

- プッシュ通知を使用しますか？

iOSの設計ガイダンス:

NetScaler Gatewayの構成にSecure Ticket Authority (STA)が含まれており、スプリットトンネリングがオフの場合: NetScaler Gatewayは、Citrix Secure MailからCitrixリスナーサービスURLへのトラフィックを許可する必要があります。これらのURLは、iOS版Citrix Secure Mailのプッシュ通知で指定されています。

Androidの設計ガイダンス:

Firebase Cloud Messaging (FCM) を使用して、Android デバイスが Citrix Endpoint Management に接続する方法とタイミングを制御します。FCM が構成されている場合、セキュリティアクションまたは展開コマンドは、Citrix Secure Hub にプッシュ通知をトリガーし、ユーザーに Citrix Endpoint Management サーバーへの再接続を促します。

HDX™ STA

決定の詳細:

- HDX アプリケーションアクセスを統合する場合、どの STA を使用しますか?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設計ガイダンス:

HDX STA は StoreFront の STA と一致している必要があり、Virtual Apps and Desktops サイトに対して有効である必要があります。

シトリックス ファイル と シェアファイル

決定の詳細:

- 環境でストレージゾーンコントローラーを使用しますか?
- どの Citrix Files VIP URL を使用しますか?

設計ガイダンス:

環境にストレージゾーンコントローラーを含める場合は、以下を正しく構成していることを確認してください。

- Citrix Files コンテンツスイッチ VIP (Citrix Files コントロールプレーンがストレージゾーンコントローラーサーバーと通信するために使用)
- Citrix Files ロードバランシング VIP
- 必要なすべてのポリシーとプロファイル

詳細については、Storage zones controller のドキュメントを参照してください。

SAML IdP

決定の詳細:

- Citrix Files で SAML が必要な場合、Citrix Endpoint Management を SAML IdP として使用しますか？

設計ガイダンス:

推奨されるベストプラクティスは、Citrix Files を Citrix Endpoint Management と統合することです。これは、SAML ベースのフェデレーションを構成するよりも簡単な方法です。Citrix Endpoint Management は、Citrix Files に以下を提供します。

- Citrix モバイル生産性アプリユーザーのシングルサインオン (SSO) 認証
- Active Directory に基づくユーザーアカウントプロビジョニング
- 包括的なアクセス制御ポリシー。

Citrix Endpoint Management コンソールを使用すると、Citrix Files の構成、サービスレベルの監視、ライセンス使用状況の確認を行うことができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Files クライアントには、Citrix Endpoint Management 用 Citrix Files (ラップされた Citrix Files とも呼ばれます) と Citrix Files モバイルクライアント (ラップされていない Citrix Files とも呼ばれます) の2種類があります。違いを理解するには、「Citrix Endpoint Management 用 Citrix Files クライアントと Citrix Files モバイルクライアントの違い」を参照してください。

Citrix Endpoint Management と Citrix Files を構成して、SAML を使用して以下の SSO アクセスを提供できます。

- MAM SDK が有効になっている、または MDX Toolkit を使用してラップされている Citrix Files アプリ
- Web サイト、Outlook プラグイン、同期クライアントなどの、ラップされていない Citrix Files クライアント

Citrix Endpoint Management を Citrix Files の SAML IdP として使用する場合は、適切な構成が設定されていることを確認してください。詳細については、「Citrix Files での SSO 用 SAML」を参照してください。

ShareConnect ダイレクト接続

決定の詳細:

- ユーザーは、ShareConnect を実行しているコンピューターまたはモバイルデバイスから、ダイレクト接続を使用してホストコンピューターにアクセスしますか？

設計ガイダンス:

ShareConnect を使用すると、ユーザーは iPad、Android タブレット、Android フォンを介して自分のコンピューターに安全に接続し、ファイルやアプリケーションにアクセスできます。ダイレクト接続の場合、Citrix Endpoint Management は NetScaler Gateway を使用して、ローカルネットワーク外のリソースへの安全なアクセスを提供します。構成の詳細については、「ShareConnect」を参照してください。

各管理モードの登録FQDN

管理モード	登録FQDN
MDM登録が必須のMDM+MAM	シトリックス エンドポイント マネジメント サーバーのFQDN
MDM登録がオプションのMDM+MAM	シトリックス エンドポイント マネジメント サーバーのFQDN

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理モード	登録FQDN
MAMのみ	Citrix Endpoint Managementサーバーの完全修飾ドメイン名

展開の概要

テスト、開発、本番環境など、Citrix Endpoint Managementのインスタンスが多数ある場合は、追加の環境に対してNetScaler Gatewayを手動で構成する必要があります。動作する環境が整ったら、Citrix Endpoint Management用にNetScaler Gatewayを手動で構成する前に、設定をメモしておいてください。

Citrix Endpoint Managementサーバーへの通信にHTTPSを使用するかHTTPを使用するかは、重要な決定事項です。HTTPSは、NetScaler GatewayとCitrix Endpoint Management間のトラフィックが暗号化されるため、安全なバックエンド通信を提供します。再暗号化はCitrix Endpoint Managementサーバーのパフォーマンスに影響を与えます。HTTPはCitrix Endpoint Managementサーバーのパフォーマンスを向上させます。NetScaler GatewayとCitrix Endpoint Management間のトラフィックは暗号化されません。以下の表は、NetScaler GatewayとCitrix Endpoint ManagementのHTTPおよびHTTPSポート要件を示しています。

HTTPS

Citrixは通常、NetScaler Gateway MDM仮想サーバー構成にはSSL Bridgeを推奨しています。MDM仮想サーバーでNetScaler Gateway SSL Offloadを使用する場合、Citrix Endpoint Managementはバックエンドサービスとしてポート80のみをサポートします。

管理モード	NETSCALER GATEWAYの負荷分散方法	SSL再暗号化	CITRIX ENDPOINT MANAGEMENTサーバーのポート
MAM	SSLオフロード	有効	8443
MDM+MAM	MDM: SSLブリッジ	N/A	443, 8443
MDM+MAM	MAM: SSLオフロード	有効	8443

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HTTP

管理モード	NETSCALER GATEWAYの負荷分散方法	SSL再暗号化	シトリックス エンドポイント マネジメント サーバーポート
MAM	SSLオフロード	有効	8443
MDM+MAM	MDM: SSLオフロード	サポートされていません	80
MDM+MAM	MAM: SSLオフロード	有効	8443

Citrix Endpoint Management展開におけるNetScaler Gatewayの図については、Architectureを参照してください。

MDXアプリのSSOとプロキシに関する考慮事項

Citrix Endpoint ManagementとNetScaler Gatewayの統合により、すべてのバックエンドHTTP/HTTPSリソースへのシングルサインオン (SSO) をユーザーに提供できます。SSO認証の要件に応じて、MDXアプリのユーザー接続をSecure Browse (トンネル化 - Web SSO) を使用するように構成します。これはクライアントレスVPNの一種です。

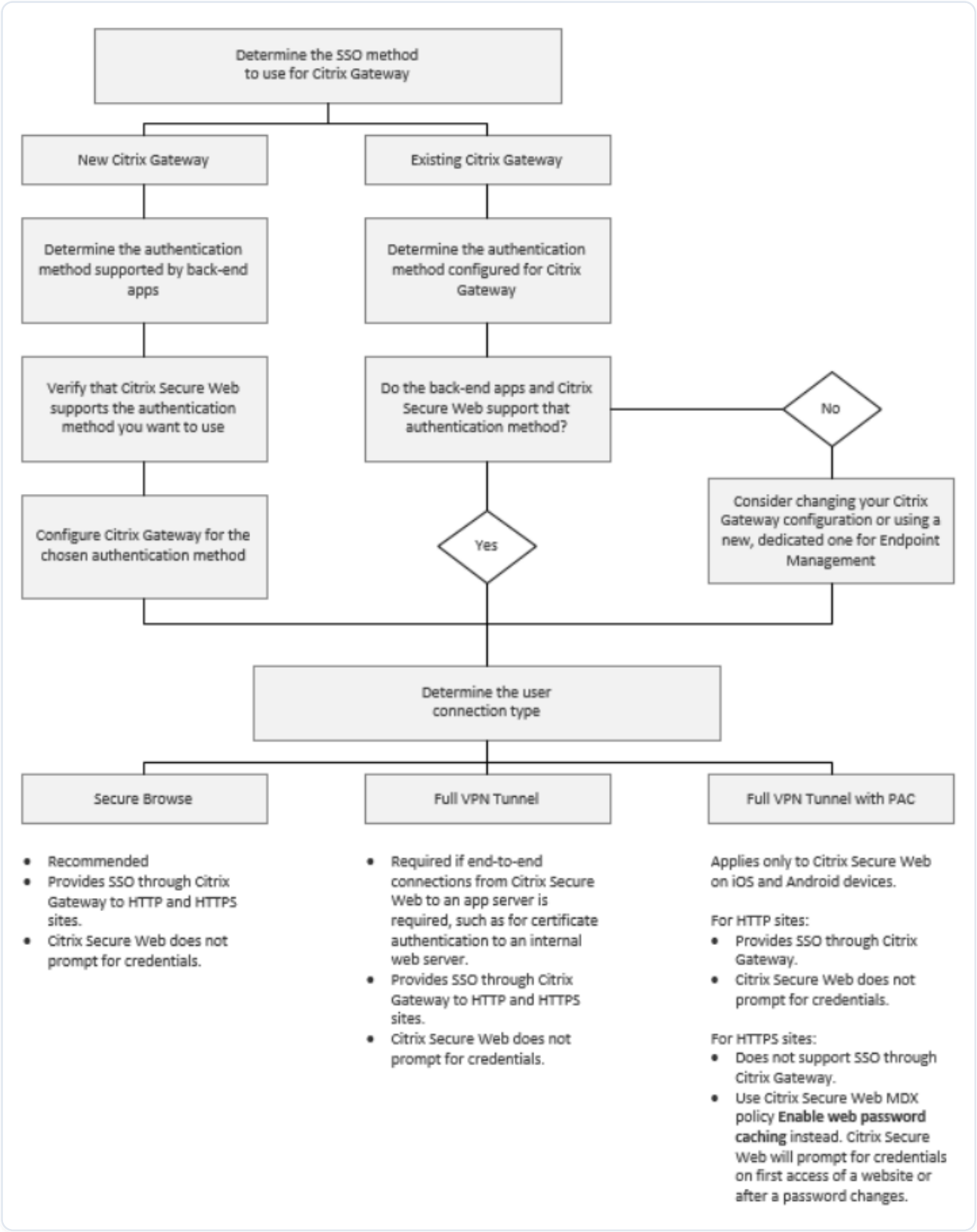
重要:

Citrixは、iOSおよびAndroidデバイス向けのフルVPNトンネルと、フルVPNトンネル展開でのプロキシ自動構成 (PAC) ファイルのサポートを非推奨としました。詳細については、「非推奨」を参照してください。

環境内でNetScaler GatewayがSSOを提供する最適な方法でない場合、ポリシーベースのローカルパスワードキャッシュを使用してMDXアプリをセットアップできます。この記事では、Citrix Secure Webに焦点を当てて、さまざまなSSOおよびプロキシオプションについて説明します。これらの概念は他のMDXアプリにも適用されます。

次のフローチャートは、SSOとユーザー接続の決定フローをまとめたものです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler Gatewayの認証方法

このセクションでは、NetScaler Gatewayでサポートされている認証方法に関する一般的な情報を提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SAML認証

NetScaler GatewayをSecurity Assertion Markup Language (SAML) 用に構成すると、ユーザーはSAMLプロトコルをサポートするWebアプリにシングルサインオンで接続できます。NetScaler Gatewayは、SAML WebアプリのIDプロバイダー (IdP) シングルサインオンをサポートします。

必要な構成:

- NetScaler Gatewayトラフィックプロファイルで SAML SSOを構成します。
- 要求されたサービスに対してSAML IdPを構成します。

NTLM認証

セッションプロファイルでWebアプリへのSSOが有効になっている場合、NetScaler GatewayはNTLM認証を自動的に実行します。

必要な構成:

- NetScaler Gatewayのセッションプロファイルまたはトラフィックプロファイルで SSOを有効にします。

Kerberosインパーソネーション

Citrix Endpoint Managementは、Citrix Secure Webに対してのみKerberosをサポートします。NetScaler GatewayをKerberos SSO用に構成すると、ユーザーパスワードがNetScaler Gatewayで利用可能な場合、NetScaler Gatewayはインパーソネーションを使用します。インパーソネーションとは、NetScaler Gatewayがユーザー資格情報を使用して、Citrix Secure Webなどのサービスへのアクセスに必要なチケットを取得することを意味します。

必要な構成:

- NetScaler Gatewayの `Worx` セッションポリシーを構成して、接続からKerberosレルムを識別できるようにします。
- NetScaler GatewayでKerberos Constrained Delegation (KCD) アカウントを構成します。そのアカウントをパスワードなしで構成し、Citrix Endpoint Managementゲートウェイのトラフィックポリシーにバインドします。
- これらの構成およびその他の詳細については、Citrixブログ「WorxWeb and Kerberos Impersonation SSO」を参照してください。

Kerberos 制限付き委任

Citrix Endpoint Managementは、Citrix Secure Webに対してのみKerberosをサポートします。NetScaler GatewayをKerberos SSO用に構成すると、ユーザーパスワードがNetScaler Gatewayで利用できない場合、NetScaler Gatewayは制約付き委任を使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

制約付き委任では、NetScaler Gatewayは指定された管理者アカウントを使用して、ユーザーおよびサービスのチケットを取得します。

必要な構成:

- 必要な権限を持つKCDアカウントをActive Directoryに構成し、NetScaler GatewayにKDCアカウントを構成します。
- NetScaler Gatewayのトラフィックプロファイルで SSOを有効にします。
- バックエンドのWebサイトをKerberos認証用に構成します。

フォーム入力認証

NetScaler Gatewayをフォームベースのシングルサインオン用に構成すると、ユーザーは1回ログオンするだけで、ネットワーク内のすべての保護されたアプリにアクセスできます。この認証方法は、トンネル化されたWeb SSOモードを使用するアプリに適用されます。

必要な構成:

- NetScaler Gatewayトラフィックプロファイルでフォームベースの SSOを構成します。

ダイジェストHTTP認証

セッションプロファイルでWebアプリへのSSOを有効にすると、NetScaler Gatewayはダイジェストの HTTP認証を自動的に実行します。この認証方法は、トンネル化されたWeb SSOモードを使用するアプリに適用されます。

必要な構成:

- NetScaler Gatewayセッションプロファイルまたはトラフィックプロファイルで SSOを有効にします。

基本HTTP認証

セッションプロファイルでWebアプリへのSSOを有効にすると、NetScaler Gatewayは基本HTTP認証を自動的に実行します。この認証方法は、トンネル化されたWeb SSOモードを使用するアプリに適用されます。

必要な構成:

- NetScaler Gatewayセッションプロファイルまたはトラフィックプロファイルで SSOを有効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セキュアトンネル化 - Web SSO

このセクションでは、Citrix Secure Webの**トンネル化されたWeb SSO**ユーザー接続の種類について説明します。

内部ネットワークにトンネル接続する接続では、Tunneled - Web SSO と呼ばれるクライアントレス VPN のバリエーションを使用できます。Tunneled - Web SSO は、Citrix Secure Web の **Preferred VPN mode** ポリシーに指定されているデフォルト構成です。Citrix は、シングルサインオン (SSO) を必要とする接続に Tunneled - Web SSO を推奨します。

Tunneled - Web SSO モードでは、NetScaler Gateway は HTTPS セッションを2つの部分に分割します。

- クライアントからNetScaler Gatewayへ
- NetScaler Gatewayからバックエンドのリソースサーバーへ。

このようにして、NetScaler Gateway はクライアントとサーバー間のすべてのトランザクションを完全に可視化し、SSO を提供できるようにします。

Tunneled - Web SSO モードで使用する場合、Citrix Secure Web 用のプロキシサーバーも構成できます。詳細については、ブログ「Citrix Endpoint Management WorxWeb Traffic Through Proxy Server in Secure Browse Mode」を参照してください。

注:

Citrix は、PAC を使用したフル VPN トンネルの非推奨を発表しました。「非推奨」を参照してください。

Citrix Endpoint Management は、NetScaler Gateway が提供するプロキシ認証をサポートしています。PAC ファイルには、Web ブラウザーが特定の URL にアクセスするためにプロキシを選択する方法を定義するルールが含まれています。PAC ファイルのルールは、内部サイトと外部サイトの両方の処理を指定できます。Citrix Secure Web は PAC ファイルのルールを解析し、プロキシサーバー情報を NetScaler Gateway に送信します。NetScaler Gateway は PAC ファイルまたはプロキシサーバーを認識しません。

HTTPS Web サイトへの認証の場合: Citrix Secure Web MDX ポリシーの **Web パスワードキャッシュを有効にする** は、Citrix Secure Web が MDX を介してプロキシサーバーに認証し、SSO を提供できるようにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway のスプリットトンネリング

SSO とプロキシの構成を計画する際には、NetScaler Gateway のスプリットトンネリングを使用するかどうかも決定する必要があります。Citrix は、必要な場合にのみ NetScaler Gateway のスプリットトンネリングを使用することを推奨します。このセクションでは、スプリットトンネリングの仕組みについて概要を説明します。NetScaler Gateway は、ルーティングテーブルに基づいてトラフィックパスを決定します。NetScaler Gateway のスプリットトンネリングがオンの場合、Citrix Secure Hub は内部 (保護された) ネットワークトラフィックとインターネットトラフィックを区別します。Citrix Secure Hub は、DNS サフィックスとイントラネットアプリケーションに基づいてその判断を行います。その後、Citrix Secure Hub は内部ネットワークトラフィックのみを VPN トンネル経由でトンネルします。NetScaler Gateway のスプリットトンネリングがオフの場合、すべてのトラフィックは VPN トンネルを通過します。

セキュリティ上の考慮事項からすべてのトラフィックを監視したい場合は、NetScaler Gateway のスプリットトンネリングを無効にしてください。その結果、すべてのトラフィックが VPN トンネルを通過します。

NetScaler Gateway には、マイクロ VPN リバーススプリットトンネルモードもあります。この構成は、NetScaler Gateway にトンネルされない IP アドレスの除外リストをサポートします。代わりに、これらのアドレスはデバイスのインターネット接続を使用して送信されます。リバーススプリットトンネリングの詳細については、NetScaler Gateway のドキュメントを参照してください。

Citrix Endpoint Management には、**リバーススプリットトンネル除外リスト** が含まれています。特定の Web サイトが NetScaler Gateway を介してトンネルされるのを防ぐには: 代わりに LAN を使用して接続する完全修飾ドメイン名 (FQDN) または DNS サフィックスのコンマ区切りリストを追加します。このリストは、リバーススプリットトンネリング用に構成された NetScaler Gateway を使用する Tunneled - Web SSO モードにのみ適用されます。

認証

Citrix Endpoint Management展開では、認証を構成する方法を決定する際に、いくつかの考慮事項が発生します。このセクションでは、認証に影響を与えるさまざまな要因について説明します。

- 認証に関連する主要なMDXポリシー、Citrix Endpoint Managementクライアントプロパティ、およびNetScaler Gateway設定。
- これらのポリシー、クライアントプロパティ、および設定がどのように相互作用するか。
- 各選択肢のトレードオフ。

この記事には、セキュリティレベルを高めるための推奨される構成の3つの例も含まれています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

大まかに言えば、セキュリティが強化されると、ユーザーはより頻繁に認証する必要があるため、ユーザーエクスペリエンスは最適ではなくなります。これらの懸念をどのようにバランスさせるかは、組織のニーズと優先順位によって異なります。さまざまな認証オプションの相互作用を理解するために、3つの推奨構成を確認してください。

認証モード

オンライン認証: ユーザーをCitrix Endpoint Managementネットワークに許可します。インターネット接続が必要です。

オフライン認証: デバイス上で発生します。ユーザーはセキュアボールトをロック解除し、ダウンロードされたメール、キャッシュされたウェブサイト、メモなどのアイテムにオフラインでアクセスできます。

認証方法

シングルファクター

LDAP: Citrix Endpoint Managementで、Lightweight Directory Access Protocol (LDAP) に準拠する1つ以上のディレクトリへの接続を構成できます。この方法は、企業環境向けにシングルサインオン (SSO) を提供するために一般的に使用されます。LDAPでのユーザーエクスペリエンスを向上させるために、Active Directoryパスワードキャッシュを使用したCitrix PINを選択する場合があります。同時に、登録時の複雑なパスワード、パスワードの有効期限、およびアカウントロックアウトのセキュリティを提供できます。

詳細については、「ドメインまたはドメインとセキュリティトークン認証」を参照してください。

クライアント証明書: Citrix Endpoint Managementは業界標準の認証局と統合し、オンライン認証の唯一の方法として証明書を使用できます。Citrix Endpoint Managementはユーザー登録後にこの証明書を提供します。これにはワンタイムパスワード、招待URL、またはLDAP資格情報のいずれかが必要です。クライアント証明書を主要な認証方法として使用する場合、デバイス上の証明書を保護するために、クライアント証明書のみの環境ではCitrix PINが必要です。

Citrix Endpoint Managementは、サードパーティの認証局に対してのみ証明書失効リスト (CRL) をサポートします。Microsoft CAが構成されている場合、Citrix Endpoint ManagementはNetScaler Gatewayを使用して失効を管理します。クライアント証明書ベースの認証を構成する際は、NetScaler Gatewayの証明書失効リスト (CRL) 設定である「CRL自動更新を有効にする」を構成する必要があるかどうかを検討してください。この手順により、MAMにのみ登録されているデバイスが、デバイス上の既存の証明書を使用して認証できないようにします。Citrix Endpoint Managementは、証明書が失効した場合でもユーザーがユーザー証明書を生成することを制限しな

© 1997–2026 Citrix Systems, Inc. All rights reserved.

いため、新しい証明書を再発行します。この設定は、CRLが期限切れのPKIエンティティをチェックする際に、PKIエンティティのセキュリティを向上させます。

証明書ベースの認証に必要な展開、またはエンタープライズ認証局 (CA) を使用したデバイス証明書の発行を示す図については、アーキテクチャを参照してください。

二要素認証

LDAP + クライアント証明書: この構成は、Citrix Endpoint Managementにとってセキュリティとユーザーエクスペリエンスの最適な組み合わせです。LDAPとクライアント証明書認証の両方を使用すると、次のようになります。

- NetScaler Gatewayでの二要素認証によって提供されるセキュリティと相まって、最高のSSOの可能性を秘めています。
- ユーザーが知っているもの（Active Directoryパスワード）と、ユーザーが持っているもの（デバイス上のクライアント証明書）の両方でセキュリティを提供します。

Citrix Secure Mailは、クライアント証明書認証を使用して、シームレスな初回ユーザーエクスペリエンスを自動的に構成および提供できます。この機能には、適切に構成されたExchangeクライアントアクセスサーバー環境が必要です。

最適な使いやすさのために、LDAPとクライアント証明書認証をCitrix PINおよびActive Directoryパスワードキャッシュと組み合わせることができます。

LDAP + トークン: この構成では、RADIUSプロトコルを使用して、LDAP資格情報とワンタイムパスワードの従来の構成が可能です。最適な使いやすさのために、このオプションをCitrix PINおよびActive Directoryパスワードキャッシュと組み合わせることができます。

認証に関する重要なポリシー、設定、およびクライアントプロパティ

以下のポリシー、設定、およびクライアントプロパティは、次の3つの推奨構成で適用されます。

MDXポリシー

アプリのパスコード: オンの場合、アプリの起動時または一定期間の非アクティブ状態からの再開時に、Citrix PINまたはパスコードがアプリのロック解除に必要です。デフォルトは**オン**です。

すべてのアプリの非アクティブタイマーを構成するには、Citrix Endpoint Managementコンソールの**設定**タブにある**クライアントプロパティ**で、INACTIVITY_TIMERの値を分単位で設定します。デフォルトは15分です。非アクティブタイマーを無効にして、アプリの起動時にのみPINまたはパスコードのプロンプトが表示されるようにするには、値をゼロに設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

micro VPNセッションが必要: オンの場合、ユーザーはエンタープライズネットワークへの接続とアクティブなセッションを持っている必要があります。デバイス上のアプリにアクセスするには、アクティブなセッションが必要です。**オフ**の場合、デバイス上のアプリにアクセスするためにアクティブなセッションは必要ありません。デフォルトは**オフ**です。

最大オフライン期間（時間）： アプリがCitrix Endpoint Managementからアプリの資格を再確認し、ポリシーを更新することなく実行できる最大期間を定義します。iOSアプリは、以下の条件を満たした後、ユーザーに中断を与えることなく、Citrix Endpoint ManagementからMDXアプリの新しいポリシーを取得します。

- 最大オフライン期間を設定していること、および
- iOS版Citrix Secure Hubが有効なNetScaler Gatewayトークンを持っていること。

Citrix Secure Hubが有効なNetScaler Gatewayトークンを持っていない場合、アプリのポリシーを更新する前に、ユーザーはCitrix Secure Hubを介して認証する必要があります。NetScaler Gatewayトークンは、NetScaler Gatewayセッションの非アクティブまたは強制セッションタイムアウトポリシーのために無効になることがあります。ユーザーがCitrix Secure Hubに再度サインオンすると、アプリの実行を継続できます。

期間が終了する30分前、15分前、5分前に、ユーザーにサインオンするよう通知されます。期限切れ後、ユーザーがサインオンするまでアプリはロックされます。デフォルトは**72時間（3日間）**です。最小期間は1時間です。

注：

ユーザーが頻繁に移動し、国際ローミングを使用するシナリオでは、デフォルトの72時間（3日間）では短すぎる可能性があることに留意してください。

バックグラウンドサービスチケットの有効期限： バックグラウンドネットワークサービスチケットが有効である期間。Citrix Secure MailがNetScaler Gatewayを介してActiveSyncを実行しているExchange Serverに接続すると、Citrix Endpoint Managementはトークンを発行します。Citrix Secure Mailはそのトークンを使用して内部Exchange Serverに接続します。このプロパティ設定は、Citrix Secure Mailが認証およびExchange Serverへの接続のために新しいトークンを必要とせずにトークンを使用できる期間を決定します。制限時間が経過すると、ユーザーは新しいトークンを生成するために再度ログオンする必要があります。デフォルトは**168時間（7日間）**です。このタイムアウトが期限切れになると、メール通知は停止します。

micro VPNセッションの猶予期間： オンラインセッションが検証されるまで、ユーザーがアプリをオフラインで使用できる分数。デフォルトは**0**（猶予期間なし）です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

認証ポリシーの詳細については、以下を参照してください。

- MAM SDKを使用する場合：MAM SDKの概要
- MDX Toolkitを使用する場合：iOS向けCitrix Endpoint Management MDXポリシーおよびAndroid向けCitrix Endpoint Management MDXポリシー

Citrix Endpoint Managementクライアントプロパティ

> **注：**
>
> クライアントプロパティは、Citrix Endpoint Managementに接続するすべてのデバイスに適用されるグローバル設定です。

Citrix PIN: シンプルなサインオンエクスペリエンスのために、Citrix PINを有効にすることを選択できます。PINを使用すると、ユーザーはActive Directoryのユーザー名やパスワードなどの他の資格情報を繰り返し入力する必要がありません。Citrix PINは、スタンドアロンのオフライン認証としてのみ構成することも、PINとActive Directoryパスワードキャッシュを組み合わせて、最適な使いやすさのために認証を合理化することもできます。Citrix Endpoint Managementコンソールで、**> >** でCitrix PINを構成します。

以下は、いくつかの重要なプロパティの概要です。詳細については、「クライアントプロパティ」を参照してください。

ENABLE_PASSCODE_AUTH

表示名: Citrix PIN認証を有効にする

このキーを使用すると、Citrix PIN機能をオンにできます。Citrix PINまたはパスコードを使用すると、ユーザーはActive Directoryパスワードの代わりにPINを定義するように求められます。**ENABLE_PASSWORD_CACHING**が有効になっている場合、またはCitrix Endpoint Managementが証明書認証を使用している場合は、この設定を有効にします。

設定可能な値: true または **false**

デフォルト値: false

ENABLE_PASSWORD_CACHING

表示名: ユーザーパスワードのキャッシュを有効にする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このキーを使用すると、ユーザーのActive Directoryパスワードをモバイルデバイスにローカルでキャッシュできます。このキーをtrueに設定すると、ユーザーはCitrix PINまたはパスコードを設定するように求められます。このキーを**true**に設定する場合、**ENABLE_PASSCODE_AUTH**キーもtrueに設定する必要があります。

設定可能な値: true または **false**

デフォルト値: false

PASSCODE_STRENGTH

表示名: PINの強度要件

このキーは、Citrix PINまたはパスコードの強度を定義します。この設定を変更すると、ユーザーは次回認証を求められたときに新しいCitrix PINまたはパスコードを設定するように求められます。

指定可能な値: 低、中、または**高**

デフォルト値: 中

INACTIVITY_TIMER

表示名: 非アクティビティタイマー

このキーは、ユーザーがデバイスを非アクティブなままにしておき、Citrix PINまたはパスコードの入力を求められることなくアプリにアクセスできる時間を分単位で定義します。MDXアプリでこの設定を有効にするには、**App Passcode**設定を**On**にする必要があります。**App Passcode**設定が**Off**の場合、ユーザーはCitrix Secure Hubにリダイレクトされ、完全な認証を行うことになります。この設定を変更すると、ユーザーが次回認証を求められたときに値が有効になります。デフォルトは15分です。

ENABLE_TOUCH_ID_AUTH

表示名: Touch ID認証を有効にする

オフライン認証に指紋リーダー（iOSのみ）の使用を許可します。オンライン認証には、引き続き主要な認証方法が必要です。

ENCRYPT_SECRETS_USING_PASSCODE

表示名: パスコードを使用してシークレットを暗号化する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このキーを使用すると、機密データをiOSキーチェーンなどのプラットフォームベースのネイティブストアではなく、秘密の保管庫にモバイルデバイスに保存できます。この構成キーは、キーアーティファクトの強力な暗号化を可能にするだけでなく、ユーザーエントロピー（ユーザーのみが知っているユーザー生成のランダムなPINコード）も追加します。

指定可能な値: true または **false**

デフォルト値: false

NetScaler Gatewayの設定

セッションタイムアウト: この設定を有効にすると、NetScaler Gatewayが指定された間隔でネットワークアクティビティを検出しない場合、NetScaler Gatewayはセッションを切断します。この設定は、NetScaler Gateway Plug-in、Citrix Secure Hub、またはWebブラウザを介して接続するユーザーに適用されます。デフォルトは**1440分**です。この値をゼロに設定すると、この設定は無効になります。

強制タイムアウト: この設定を有効にすると、ユーザーが何をしていても、タイムアウト間隔が経過するとNetScaler Gatewayはセッションを切断します。タイムアウト間隔が経過すると、ユーザーは切断を防ぐためのいかなる操作もできません。この設定は、NetScaler Gateway Plug-in、Citrix Secure Hub、またはWebブラウザ経由で接続するユーザーに適用されます。Citrix Secure Mailが特別なNetScaler GatewayモードであるSTAを使用している場合、この設定はCitrix Secure Mailセッションには適用されません。デフォルトは値なしで、これは任意のアクティビティでセッションが延長されることを意味します。

NetScaler Gatewayのタイムアウト設定の詳細については、NetScaler Gatewayのドキュメントを参照してください。

ユーザーがデバイスに資格情報を入力してCitrix Endpoint Managementで認証するよう促されるシナリオの詳細については、「認証プロンプトのシナリオ」を参照してください。

デフォルトの構成設定

これらの設定は、以下によって提供されるデフォルトです。

- NetScaler® for XenMobileウィザード
- MAM SDKまたはMDX Toolkit
- シトリックス エンドポイント マネジメント コンソール

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	設定の場所	デフォルト設定
セッションタイムアウト	ネットスケーラー ゲートウェイ	1440分
強制タイムアウト	ネットスケーラー ゲートウェイ	値なし (オフ)
最大オフライン期間	MDXポリシー	72時間
バックグラウンドサービスチケットの有効期限	MDXポリシー	168時間 (7日間)
micro VPNセッションが必要	MDXポリシー	オフ
micro VPNセッションの猶予期間が必要	MDXポリシー	0
アプリパスコード	MDXポリシー	オン
パスコードを使用してシークレットを暗号化	Citrix Endpoint Management クライアントプロパティ	いいえ
Citrix PIN認証を有効にする	Citrix Endpoint Management クライアントプロパティ	いいえ
PINの強度要件	Citrix Endpoint Management クライアントプロパティ	中
PINの種類	Citrix Endpoint Management クライアントプロパティ	数字
ユーザーパスワードのキャッシュを有効にする	Citrix Endpoint Management クライアントプロパティ	無効
非アクティビティタイマー	Citrix Endpoint Management クライアントプロパティ	15
Touch ID認証を有効にする	Citrix Endpoint Management クライアントプロパティ	無効

© 1997–2026 Citrix Systems, Inc. All rights reserved.

推奨される構成

このセクションでは、最低限のセキュリティと最適なユーザーエクスペリエンスから、最高のセキュリティとより煩わしいユーザーエクスペリエンスまで、3つのCitrix Endpoint Management構成の例を示します。これらの例は、独自の構成をどのレベルに設定するかを決定するための役立つ参照点となります。これらの設定を変更すると、他の設定も変更する必要がある場合があります。たとえば、最大オフライン期間はセッションタイムアウトを超えてはなりません。

最高のセキュリティ

この構成は最高レベルのセキュリティを提供しますが、使いやすさとの間で大きなトレードオフがあります。

設定	設定の場所	推奨設定	動作への影響
セッションタイムアウト	ネットスケーラーゲートウェイ	1440	ユーザーは、オンライン認証が必要な場合（24時間ごと）にのみCitrix Secure Hubの資格情報を入力します。
強制タイムアウト	ネットスケーラーゲートウェイ	値なし	アクティビティがある場合、セッションは延長されます。
最大オフライン期間	MDXポリシー	23	毎日ポリシーの更新が必要です。
バックグラウンドサービスのチケット有効期限	MDXポリシー	72時間	STAのタイムアウト。これにより、NetScaler Gatewayセッショントークンなしで長期間のセッションが可能になります。Citrix Secure Mailの場合、STAタイムアウトをセッションタイムアウトよりも長く設定すると、メール通知が停止するのを防ぐことができます。その場

© 1997–2026 Citrix Systems, Inc. All rights reserved.

			合、ユーザーがセッションの有効期限が切れる前にアプリを開かないと、Citrix Secure Mailはユーザーにプロンプトを表示しません。
マイクロVPNセッションが必要	MDXポリシー	オフ	アプリを使用するための有効なネットワーク接続とNetScaler Gatewayセッションを提供します。
マイクロVPNセッションの猶予期間が必要	MDXポリシー	0	猶予期間なし（マイクロVPNセッションが必要を有効にした場合）。
アプリのパスコード	MDXポリシー	オン	アプリケーションにパスコードを要求します。
パスコードを使用してシークレットを暗号化	Citrix Endpoint Management クライアントプロパティ	はい	ユーザーエントロピーから派生したキーがボールトを保護します。
Citrix PIN認証を有効にする	Citrix Endpoint Management クライアントプロパティ	はい	簡素化された認証エクスペリエンスのためにCitrix PINを有効にします。
PINの強度要件	Citrix Endpoint Management クライアントプロパティ	強	高いパスワードの複雑さの要件。
PINの種類	Citrix Endpoint Management クライアントプロパティ	英数字	PINは英数字のシーケンスです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パスワードキャッシュを有効にする	Citrix Endpoint Management クライアントプロパティ	無効	Active Directory のパスワードはキャッシュされず、オフライン認証には Citrix PIN が使用されます。
非アクティブタイマー	Citrix Endpoint Management クライアントプロパティ	15	ユーザーがこの期間中に MDX アプリまたは Citrix Secure Hub を使用しない場合、オフライン認証を要求します。
Touch ID 認証を有効にする	Citrix Endpoint Management クライアントプロパティ	無効	iOS のオフライン認証ユースケースで Touch ID を無効にします。

セキュリティの強化

より中道的なアプローチとして、この構成では、ユーザーは（7日ごとではなく）最大3日ごとに、より頻繁に認証を行う必要があり、より強力なセキュリティが提供されます。認証回数が増えることで、コンテナがより頻繁にロックされ、デバイスが使用されていないときのデータセキュリティが確保されます。

設定	設定の場所	推奨設定	動作への影響
セッションタイムアウト	ネットスケーラーゲートウェイ	4320	ユーザーは、オンライン認証が必要な場合（3日ごと）にのみCitrix Secure Hubの資格情報を入力します。
強制タイムアウト	ネットスケーラーゲートウェイ	値なし	アクティビティがある場合、セッションは延長されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

最大オフライン期間	MDXポリシー	71	3日ごとにポリシーの更新が必要です。1時間の差は、セッションタイムアウトより前に更新を許可するためです。
バックグラウンドサービスチケットの有効期限	MDXポリシー	168時間	NetScaler Gatewayセッショントークンなしで長期間のセッションを可能にするSTAのタイムアウト。Citrix Secure Mailの場合、STAタイムアウトをセッションタイムアウトよりも長く設定することで、ユーザーにプロンプトを表示せずにメール通知が停止するのを防ぎます。
micro VPNセッションが必要	MDXポリシー	オフ	アプリを使用するための有効なネットワーク接続とNetScaler Gatewayセッションを提供します。
micro VPNセッションが必要な猶予期間	MDXポリシー	0	猶予期間なし（micro VPNセッションが必要を有効にした場合）。
アプリのパスコード	MDXポリシー	オン	アプリケーションにパスコードを要求する。
パスコードを使用してシークレットを暗号化する	Citrix Endpoint Managementクライアントプロパティ	いいえ	ボールトを暗号化するためにユーザーエ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

			ントロピーを要求しない。
Citrix PIN認証を有効にする	Citrix Endpoint Managementクライアントプロパティ	はい	認証エクスペリエンスを簡素化するためにCitrix PINを有効にする。
PINの強度要件	Citrix Endpoint Managementクライアントプロパティ	中	中程度のパスワード複雑性ルールを適用します。
PINの種類	Citrix Endpoint Managementクライアントプロパティ	数値	PINは数値シーケンスです。
パスワードキャッシュを有効にする	Citrix Endpoint Managementクライアントプロパティ	真	ユーザーPINはActive Directoryパスワードをキャッシュし、保護します。
非アクティブタイマー	Citrix Endpoint Managementクライアントプロパティ	30	ユーザーがこの期間にMDXアプリまたはCitrix Secure Hubを使用しない場合、オフライン認証を要求します。
Touch ID認証を有効にする	Citrix Endpoint Managementクライアントプロパティ	真	iOSでのオフライン認証ユースケースにTouch IDを有効にします。

高セキュリティ

この構成は、ユーザーにとって最も便利であり、ベースレベルのセキュリティを提供します。

設定	**設定の場所**	**推奨設定**	**動作への影響**
セッションタイムアウト	ネットスケーラーゲートウェイ	10080	ユーザーは、オンライン認証が必要な場合（7日ごと）にの

© 1997–2026 Citrix Systems, Inc. All rights reserved.

			みCitrix Secure Hubの資格情報を入力します。
強制タイムアウト	ネットスケーラーゲートウェイ	値なし	アクティビティがある場合、セッションは延長されます。
最大オフライン期間	MDXポリシー	167	毎週（7日ごと）ポリシーの更新が必要です。時間差は、セッションタイムアウト前に更新を許可するためです。
バックグラウンドサービスのチケットの有効期限	MDXポリシー	240	STAのタイムアウト。これにより、NetScaler Gatewayセッショントークンなしで長期間のセッションが可能になります。Citrix Secure Mailの場合、STAのタイムアウトをセッションタイムアウトよりも長く設定することで、メール通知が停止するのを防ぎます。その場合、ユーザーがセッションの有効期限が切れる前にアプリを開かなければ、Citrix Secure Mailはユーザーにプロンプトを表示しません。
マイクロVPNセッションが必要	MDXポリシー	オフ	アプリを使用するための有効なネットワーク接続とNetScaler Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

			セッションを提供します。
マイクロVPNセッションの猶予期間が必要	MDXポリシー	0	猶予期間なし（マイクロVPNセッションが必要を有効にした場合）。
アプリのパスコード	MDXポリシー	オン	アプリケーションにパスコードを要求する。
パスコードを使用してシークレットを暗号化する	Citrix Endpoint Managementクライアントプロパティ	いいえ	ボールトの暗号化にユーザーエントロピーを要求しない。
Citrix PIN認証を有効にする	Citrix Endpoint Managementクライアントプロパティ	はい	簡素化された認証エクスペリエンスのためにCitrix PINを有効にする。
PINの強度要件	Citrix Endpoint Managementクライアントプロパティ	低	パスワードの複雑さの要件なし
PINの種類	Citrix Endpoint Managementクライアントプロパティ	数値	PINは数値のシーケンスです。
パスワードキャッシュを有効にする	Citrix Endpoint Managementクライアントプロパティ	はい	ユーザーPINはActive Directoryパスワードをキャッシュして保護します。
非アクティブタイマー	Citrix Endpoint Managementクライアントプロパティ	90	ユーザーがこの期間MDXアプリまたはCitrix Secure Hubを使用しない場合、オフライン認証を要求します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Touch ID認証を有効にする	Citrix Endpoint Managementクライアントプロパティ	はい	iOSでのオフライン認証のユースケースでTouch IDを有効にします。

ステップアップ認証の使用

一部のアプリでは、強化された認証が必要になる場合があります。たとえば、トークンや積極的なセッションタイムアウトなどの二次認証要素です。この認証方法はMDXポリシーを通じて制御します。この方法では、認証方法を制御するための個別の仮想サーバーも必要になります（同じNetScaler Gatewayアプライアンス上でも、別々のアプライアンス上でも可能です）。

設定	設定の場所	推奨設定	動作への影響
代替ネットスケーラー ゲートウェイ	MDXポリシー	セカンダリNetScaler GatewayアプライアンスのFQDNとポートが必要です。	セカンダリNetScaler Gatewayアプライアンスの認証およびセッションポリシーによって制御される、強化された認証を可能にします。

ユーザーが代替NetScaler Gatewayを使用するアプリを開くと、他のすべてのアプリはそのNetScaler Gatewayインスタンスを使用して内部ネットワークと通信します。セッションは、強化されたセキュリティを持つNetScaler Gatewayインスタンスからのセッションがタイムアウトした場合にのみ、より低いセキュリティのNetScaler Gatewayインスタンスに戻ります。

マイクロVPNセッションの必須化

Citrix Secure Webなどの特定のアプリケーションでは、ユーザーが認証済みセッションを持っている場合にのみアプリを実行するように設定できます。このポリシーはそのオプションを強制し、ユーザーが作業を完了できるように猶予期間を設けます。

設定	設定の場所	推奨設定	動作への影響
micro VPNセッションが必要	MDXポリシー	オン	デバイスがオンラインであり、有効な認証トークンを持っていることを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定	設定の場所	推奨設定	動作への影響
micro VPNセッションが必要な猶予期間	MDXポリシー	15	ユーザーがアプリを使用できなくなるまでに15分間の猶予期間を許可します。

サーバープロパティ

サーバープロパティは、Citrix Endpoint Managementインスタンス全体にわたる操作、ユーザー、デバイスに適用されるグローバルプロパティです。Citrixでは、この記事で説明されているサーバープロパティを環境に合わせて評価することをお勧めします。その他のサーバープロパティを変更する前に、必ずCitrixにご相談ください。

サーバープロパティを更新するには、 > の順に移動します。

サーバープロパティの追加、編集、または削除

Citrix Endpoint Managementでは、サーバーにプロパティを適用できます。

1. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。 ページが表示されます。
2. で、 をクリックします。 ページが表示されます。このページからサーバープロパティを追加、編集、または削除できます。

   サーバープロパティ(/en-us/citrix-endpoint-management/media/settings-server-server-properties.png)

サーバープロパティを追加するには

1. をクリックします。 ページが表示されます。

   サーバープロパティ(/en-us/citrix-endpoint-management/media/settings-server-server-properties-add.png)
2. 次の設定を構成します。

   - キー: リストから適切なキーを選択します。キーは大文字と小文字を区別します。プロパティ値を編集したり、特別なキーを要求したりする前に、Citrixサポートに連絡してください。
   - 値: 選択したキーに応じて値を入力します。
   - 表示名: テーブルに表示される新しいプロパティ値の名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 説明: 必要に応じて、新しいサーバープロパティの説明を入力します。

3. **保存**をクリックします。

サーバープロパティを編集するには

1. **サーバープロパティ**テーブルで、編集するサーバープロパティを選択します。

   サーバープロパティの横にあるチェックボックスを選択すると、サーバープロパティリストの上にオプションメニューが表示されます。リスト内の他の場所をクリックすると、リストの右側にオプションメニューが開きます。

2. **編集**をクリックします。**新しいサーバープロパティの編集**ページが表示されます。

   サーバープロパティ(/en-us/citrix-endpoint-management/media/settings-server-server-properties-edit.png)

3. 必要に応じて、以下の情報を変更します。

   - キー: このフィールドは変更できません。
   - 値: プロパティの値。
   - 表示名: プロパティ名。
   - 説明: プロパティの説明。

4. 変更を保存するには**保存**をクリックし、プロパティを変更しないままにするには**キャンセル**をクリックします。

サーバープロパティを削除するには

1. **サーバープロパティ**テーブルで、削除するサーバープロパティを選択します。
2. 「**削除**」をクリックします。確認ダイアログボックスが表示されます。もう一度「**削除**」をクリックします。

サーバープロパティの定義

マネージドGoogle Playストア内のすべてのアプリにアクセス

- **true**の場合、Citrix Endpoint Managementは、パブリックGoogle PlayストアのすべてのアプリをマネージドGoogle Playストアからアクセスできるようにします。これらのアプリへのアクセスを制御するには、制限デバイスポリシーを使用できます。デフォルトは**false**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

常にデバイスを追加

- **true**の場合、Citrix Endpoint Managementは、登録に失敗した場合でも、デバイスをCitrix Endpoint Managementコンソールに追加します。その結果、どのデバイスが登録を試みたかを確認できます。デフォルトは**false**です。

AGクライアント証明書発行スロットリング間隔

- 証明書生成間の猶予期間です。この間隔により、Citrix Endpoint Managementが短期間にデバイスに対して多数の証明書を生成するのを防ぎます。Citrixでは、この値を変更しないことをお勧めします。デフォルトは**30**分です。

指定された期間非アクティブとマークされたデバイスの削除を許可する

- **true**の場合、指定された期間（日数）非アクティブだったデバイスは、Citrix Endpoint Managementから削除されます。アクティビティ期間は、**Length of Time Device Can Be Inactive Before Being Automatically Removed From CEM**サーバープロパティによって設定されます。デフォルトは**true**です。このプロパティの値を変更するには、Citrix担当者にご相談ください。

監査ロガー

- **False**の場合、ユーザーインターフェイス（UI）イベントはログに記録されません。デフォルトは**False**です。

ルート化されたAndroidデバイスおよびジェイルブレイクされたiOSデバイスの登録をブロックする

このプロパティが**true**に設定されている場合、Citrix Endpoint Managementは、ルート化されたAndroidデバイスおよびジェイルブレイクされたiOSデバイスの登録をブロックします。すべてのセキュリティレベルで推奨される設定は**true**です。デフォルトは**true**です。

cdn.s3.retry.intervalおよびcdn.s3.max.retry

`cdn.s3.retry.interval` と `cdn.s3.max.retry` のサーバープロパティは連携して、すべてのmacOS PKG ファイルアップロードの最大時間制限を設定します。デフォルトでは、Citrix Endpoint Management はファイルアップロード時間を 100 秒に制限しています。ファイルアップロードがこの制限を超えると、アップロードは失敗します。デフォルトを変更するには、`cdn.s3.retry.interval` と `cdn.s3.max.retry` のキーを次のように構成します。

- `cdn.s3.retry.interval`。Citrix Endpoint Management がファイルアップロードが正常に完了したかどうかを確認する間隔をミリ秒単位で定義できます。デフォルトは `10000` です。
- `cdn.s3.max.retry`。アップロードが失敗するまでに許可される検証の最大再試行回数を定義できます。デフォルトは `10` です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

これら2つのキーは連携して、ファイルアップロード時間を制限します。デフォルトでは、時間制限は100秒（10000*10ミリ秒）です。

秒単位での証明書の更新

- 証明書の有効期限が切れる何秒前に Citrix Endpoint Management が証明書の更新を開始するか。たとえば、証明書が12月30日に期限切れになり、このプロパティが30日に設定されている場合、デバイスが12月1日から12月30日の間に接続すると、Citrix Endpoint Management は証明書の更新を試みます。デフォルトは **2592000** 秒（30日）です。

接続タイムアウト

- セッションの非アクティブタイムアウト（分単位）。この時間が経過すると、Citrix Endpoint Management はデバイスへの TCP 接続を閉じます。セッションは開いたままです。Android デバイスに適用されます。デフォルトは **5** 分です。

デフォルトの展開チャネル

- シトリックス エンドポイント マネジメント がリソースをデバイスに展開する方式を決定します。ユーザーレベル（**DEFAULT_TO_USER**）またはデバイスレベルで展開されます。既定値は **DEFAULT_TO_DEVICE** です。

モバイルサービスプロバイダーの非推奨化

- Blackberry およびその他の Exchange ActiveSync デバイスのクエリに使用されるモバイルサービスプロバイダーインターフェイスのサポートを非推奨にします。有効にすると、**Mobile Service Provider** インターフェイスはコンソールから非表示になります。デフォルトは **true** です。

デバイスのタグ付け

- `enable.device.tagging` を **true** に設定すると、Citrix Endpoint Management はデバイスタイプ別にデバイスを自動的にタグ付けします。デバイスタグを使用して、ポリシーやアプリを展開したり、デリバリーグループを構成したりできます。Citrix Endpoint Management は、以下の目的でデバイスにタグを適用します。
    - BYODタグ
        - iOS ユーザー登録
        - Android Enterprise ワークプロファイル
    - 企業タグ
        - Android Enterprise 完全管理対象企業デバイス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 一括登録
  - Apple Business Manager デバイス
  - Apple School Manager デバイス
  - Windows AutoPilot デバイス
  - Android Enterprise 一括登録

ホスト名検証を無効にする

- デフォルトでは、Microsoft PKI サーバーを除く送信接続でホスト名検証が有効になっています。ホスト名検証が失敗すると、サーバーログに「Unable to connect to the Volume Purchase Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer」のようなエラーが含まれます。ホスト名検証によって展開が中断される場合は、このプロパティを **true** に変更してください。デフォルトは **false** です。

SSLサーバー検証を無効にする

- **True** の場合、以下のすべての条件が満たされたときにSSLサーバー証明書の検証を無効にします。
  - Citrix Endpoint Management で証明書ベースの認証を有効にしている
  - Microsoft CA サーバーが証明書発行者である
  - Citrix Endpoint Managementがルートを信頼していない内部CAが、証明書に署名しました。

  デフォルトは**True**です。

クラッシュレポートを有効にする

- **true**の場合、CitrixはCitrix Secure Hub for iOSおよびAndroidの問題のトラブルシューティングに役立つクラッシュレポートと診断を収集します。**false**の場合、データは収集されません。デフォルト値は**true**です。

診断のためのHibernate統計ログを有効/無効にする

- **True**の場合、アプリケーションのパフォーマンス問題のトラブルシューティングを支援するために、Hibernate統計ログを有効にします。Hibernateは、Citrix Endpoint ManagementがMicrosoft SQL Serverに接続するために使用されるコンポーネントです。ログはアプリケーションのパフォーマンスに影響を与えるため、デフォルトでは無効になっています。巨大なログファイルの作成を避けるため、短期間のみログを有効にしてください。Citrix Endpoint Managementはログを/opt/sas/logs/hibernate_stats.logに書き込みます。デフォルトは**False**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS OTAEを有効にする

- **false**の場合、macOSデバイスの登録リンクの使用が防止され、macOSユーザーは登録招待状を使用することによってのみ登録できるようになります。デフォルトは**true**です。

通知トリガーを有効にする

- Citrix Secure Hubクライアントの通知を有効または無効にします。値が**true**の場合、通知が有効になります。デフォルトは**true**です。

ActiveSyncの許可ユーザーと拒否ユーザーの完全プル

- Citrix Endpoint ManagementがActiveSyncの許可ユーザーと拒否ユーザーの完全なリスト（ベースライン）をプルする間隔（秒単位）。デフォルトは**28800**秒です。

テレメトリが有効かどうかを識別します

- テレメトリが有効かどうかを識別します。テレメトリは、カスタマーエクスペリエンス向上プログラム（CEIP）とも呼ばれます。Citrix Endpoint Managementをインストールまたはアップグレードする際に、CEIPにオプトインできます。Citrix Endpoint Managementで15回連続してアップロードが失敗した場合、テレメトリは無効になります。デフォルトは**false**です。

非アクティブタイムアウト（分）

- Citrix Endpoint Management が非アクティブなユーザーをログアウトするまでの分数。ユーザーは、Citrix Endpoint Management コンソールまたはサードパーティ製アプリにアクセスするために、Citrix Endpoint Management Public API を使用している必要があります。タイムアウト値が **0** の場合、非アクティブなユーザーはログインしたままになります。API にアクセスするサードパーティ製アプリの場合、ログイン状態を維持することが通常必要です。デフォルト値は **5** に設定されています。
- **WebServices timeout type** サーバープロパティが **INACTIVITY_TIMEOUT** の場合：このプロパティは、Citrix Endpoint Management が以下の操作を行った非アクティブな管理者をログアウトするまでの分数を示します。
  - REST Services 用 Public API を使用して Citrix Endpoint Management コンソールにアクセスした
  - REST Services 用 Public API を使用してサードパーティ製アプリにアクセスした。タイムアウトが **0** の場合、非アクティブなユーザーはログインしたままになります。

include.device.properties.during.search

- デバイス検索にすべてのデバイスプロパティを含めます。デフォルトは **Off** で、検索範囲を高速検索のために以下のデバイスプロパティに制限します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- シリアル番号
- IMEI
- Wi-Fi MAC アドレス
- Bluetooth MAC アドレス
- アクティブ同期ID
- ユーザー名

このプロパティが **On** に設定されている場合、デバイス検索に時間がかかることがあります。

ios.delayBeforeDeclareUnreachable; macos.delayBeforeDeclareUnreachable

- オフラインの iOS または macOS デバイスが到達不能と見なされるまでの日数を指定します。iOS または macOS デバイスが指定された制限に達すると、Citrix Endpoint Management との通信を停止します。両方のプロパティのデフォルトは **45** 日です。

iOSデバイス管理登録 必要に応じてルートCAをインストール

- サーバープロパティ **ios.mdm.enrollment.installRootCaIfRequired** は、すべてのCitrix Endpoint Management環境で **False** に設定されています。Citrix Endpoint Managementは公開された信頼できる証明書チェーンを使用するため、ルートCAをデバイスにプッシュする必要はありません。(このプロパティはオンプレミス環境でのみ使用されます。)

iOSデバイス管理登録 最終ステップの遅延

- デバイス登録中、このプロパティ値は、MDMプロファイルのインストールとデバイス上でのエージェントの起動の間に待機する時間を指定します。Citrixは、ネットワークの遅延や速度の問題がある場合にのみ、このプロパティを編集することを推奨します。その場合、値を5000ミリ秒（5秒）を超えて設定しないでください。デフォルトは **1000** ミリ秒（1秒）です。

iOSデバイス管理ID 配信モード

- Citrix Endpoint ManagementがMDM証明書をデバイスに配布する際に、**SCEP** (セキュリティ上の理由から推奨) または **PKCS12** のどちらを使用するかを指定します。PKCS12モードでは、キーペアはサーバー上で生成され、ネゴシエーションは行われません。デフォルトは **SCEP** です。

iOSデバイス管理ID キーサイズ

- MDM ID、iOSプロファイルサービス、およびCitrix Endpoint Management iOSエージェントIDの秘密鍵のサイズを定義します。デフォルトは **2048** です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOSデバイス管理ID 更新日数

- Citrix Endpoint Managementが証明書の更新を開始する、証明書の有効期限が切れるまでの日数を指定します。例: 証明書が10日後に期限切れになり、このプロパティが **10** 日の場合、デバイスが期限切れの9日前に接続すると、Citrix Endpoint Managementは新しい証明書を発行します。デフォルトは **30** 日です。

iOS MDM APNS秘密鍵パスワード

- このプロパティにはAPNsパスワードが含まれており、Citrix Endpoint ManagementがAppleサーバーに通知をプッシュするために必要です。

デバイスが切断されるまでの非アクティブ期間

- Citrix Endpoint Managementがデバイスを切断するまでの、最終認証を含むデバイスが非アクティブでいられる期間を指定します。デフォルトは **7** 日です。

CEMから自動的に削除されるまでの、デバイスが非アクティブでいられる期間

- Citrix Endpoint Managementからデバイスが自動的に削除されるまでの非アクティブ期間（日数）。最小値は**14**日、デフォルトは**30**日です。このプロパティを有効にするには、**Allows The Removal of Devices That Have Been Marked Inactive For A Specified Period Of Time** サーバープロパティを**true**に設定する必要があります。

local.user.account.lockout.time

- ロックアウト制限を超過した後、ユーザーが待機する必要がある分数。サポートされる値は0～999です。デフォルトは**30**分です。

local.user.account.lockout.limit

- ユーザーあたりの連続した無効なログイン試行の最大数を指定します。サポートされる値は0～999です。デフォルト値は**6**に設定されています。

mac.dep.admin.passwd.rotate

このサーバープロパティを使用すると、Apple Deployment Programを通じて登録されたmacOSデバイスの管理者パスワードのローテーション間隔を構成できます。Citrix Endpoint Managementは、管理者アカウントのパスワードを毎日ローテーションするかどうかを確認します。デフォルトでは、Citrix Endpoint Managementは10,080分（7日）ごとにパスワードをローテーションします。`mac.dep.admin.passwd.rotate`キーを次のように構成します。

- 値: *管理者定義* Citrix Endpoint Managementがパスワードをローテーションする間隔（分）。360（6時間）以上の値を入力してください。Citrix Endpoint Managementは360未満の値を無視し、代わりに360分（6時間）ごとにパスワードをローテーションします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 表示名: *管理者定義*
- 説明: *管理者定義*

MAMのみのデバイスの最大数

- このカスタムキーは、各ユーザーが登録できるMAM専用デバイスの数を制限します。キーを次のように構成します。**値**を**0**にすると、デバイスの登録が無制限になります。
- Key = **number.of.mam.devices.per.user**
- 値 = **5**
- 表示名 = **MAM Only Device Max**
- 説明 = **各ユーザーが登録できるMAMデバイスの数を制限します。**

MaxNumberOfWorker

- 多数のボリューム購入ライセンスをインポートする際に使用されるスレッドの数。デフォルトは **3** です。さらに最適化が必要な場合は、スレッド数を増やすことができます。ただし、スレッド数が多いとCPU使用率が高くなります。

NetScaler Gateway (NetScaler) シングルサインオン

- **False** の場合、NetScaler Gateway から Citrix Endpoint Management へのシングルサインオン中に Citrix Endpoint Management のコールバック機能を無効にします。NetScaler Gateway の構成にコールバックURLが含まれている場合、Citrix Endpoint Management はコールバック機能を使用して NetScaler Gateway セッションIDを検証します。デフォルトは **False** です。

連続して失敗したアップロードの数

- カスタマーエクスペリエンス向上プログラム (CEIP) のアップロード中に連続して失敗した回数を表示します。アップロードが失敗すると、Citrix Endpoint Management は値をインクリメントします。15回のアップロード失敗後、Citrix Endpoint Management はテレメトリとも呼ばれるCEIPを無効にします。詳細については、サーバープロパティ **Identifies if telemetry is enabled or not** を参照してください。アップロードが成功すると、Citrix Endpoint Management は値を **0** にリセットします。

デバイスあたりのユーザー数

- MDMで同じデバイスを登録できるユーザーの最大数。値が **0** の場合、無制限の数のユーザーが同じデバイスを登録できます。デフォルトは **0** です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

optional.user.identity.attributes

- このサーバープロパティを使用すると、オプションのActive Directoryユーザー属性をカスタマイズできます。

  カスタムキーを作成し、**Values** フィールドでユーザー属性を編集して、Citrix Endpoint Management がユーザーアカウントを作成するためにアクセスできる属性を定義します。詳細については、ユーザープロパティのカスタマイズ を参照してください。

  - キー: **カスタムキー**
  - キー: **optional.user.identity.attributes**
  - 値: **共通名, 名, 姓, 表示名, 番地, 市, 都道府県, 国, 勤務先電話番号, 自宅電話番号, 携帯電話番号, 会社, 部署, 説明, 従業員ID, FAX番号, イニシャル, IP電話, マネージャー, 自宅郵便番号, その他の携帯電話, ポケットベル, 配送先オフィス名, 郵便番号, 私書箱, 役職, 組織, 優先言語**
  - 表示名: **optional.user.identity.attributes**
  - 説明: **オプションのActive Directoryユーザー属性**

macOSおよびiOS/iPadOS登録プロファイル用組織名

- `apple.mdm.enrollment.profile.organization.name`に入力する値は、登録プロファイルを提供する組織の名前に対応します。この名前は、ユーザーがデバイスをCitrix Endpoint Managementに登録する際に表示されます。表示されるデフォルト名は**Citrix Workspace**です。

許可および拒否されたユーザーの増分変更のプル

- ActiveSyncデバイスの差分を取得するためにPowerShellコマンドを実行する際に、Citrix Endpoint Managementがドメインからの応答を待機する秒数。デフォルトは**60**秒です。

Microsoft証明書サーバーへの読み取りタイムアウト

- 読み取り時にCitrix Endpoint Managementが証明書サーバーからの応答を待機する秒数。証明書サーバーが遅く、トラフィックが多い場合は、この値を60秒以上に増やすことができます。120秒後に応答しない証明書サーバーはメンテナンスが必要です。デフォルトは**15000**ミリ秒（15秒）です。

REST Webサービス

- REST Webサービスを有効にします。デフォルトは**true**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指定されたサイズのチャンクでデバイス情報を取得します

- この値は、デバイスのエクスポート時のマルチスレッド処理に内部的に使用されます。値が高いほど、単一のスレッドがより多くのデバイスを解析します。値が低いほど、より多くのスレッドがデバイスを取得します。値を減らすと、エクスポートとデバイスリストの取得のパフォーマンスが向上する可能性がありますが、利用可能なメモリが減少する可能性があります。デフォルトは**1000**です。

shp.console.enable

- **False**の場合、セルフヘルプポータルへのアクセスを防止します。ポート4443でポータルにアクセスするユーザーには、「アクセス拒否」メッセージが表示されます。**True**の場合、ポート443経由でセルフヘルプポータルへのアクセスを提供します。

  デフォルトは**False**です。

enable.new.shp

- **False**の場合、ユーザーがセルフヘルプポータルからデバイスを有効にすることを防ぎます。**True**の場合、ユーザーはセルフヘルプポータルからデバイスを有効にできます。

  BitLocker回復キー機能を使用するには、このプロパティを**False**に設定し、`shp.console.enable`プロパティを**True**に設定する必要があります。

  デフォルトは**False**です。

セッションログのクリーンアップ (日数)

- Citrix Endpoint Managementがセッションログを保持する日数。デフォルトは**7**です。

ShareFile構成タイプ

- Citrix Filesのストレージタイプを指定します。**ENTERPRISE**はCitrix Files Enterpriseモードを有効にします。**CONNECTORS**は、Citrix Endpoint Managementコンソールを通じて作成したストレージゾーンコネクタへのアクセスのみを提供します。デフォルトは**NONE**で、これは**構成 > Citrix Files**画面の初期ビューを表示し、Citrix Files Enterpriseとコネクタのどちらかを選択できます。デフォルトは**NONE**です。

静的タイムアウト (分)

- **WebServices timeout type**サーバープロパティが**STATIC_TIMEOUT**の場合：このプロパティは、Citrix Endpoint Managementが以下を使用した後に管理者をログアウトさせるまでの分数を定義します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Endpoint Managementコンソールにアクセスするための RESTサービス用パブリックAPI。
- 任意のサードパーティ製アプリにアクセスするためのRESTサービス用パブリックAPI。

デフォルトは**60**です。

トリガーエージェントメッセージの抑制

- Citrix Secure Hubクライアントメッセージングを有効または無効にします。値が**false**の場合、メッセージングが有効になります。デフォルトは**true**です。

エージェントのサウンド抑制をトリガー

- Citrix Secure Hubクライアントのサウンドを有効または無効にします。値が**false**の場合、サウンドが有効になります。デフォルトは**true**です。

Androidデバイスの非認証アプリダウンロード

- **True**の場合、Android Enterpriseを実行しているAndroidデバイスにセルフホスト型アプリをダウンロードできます。Google PlayストアでダウンロードURLを静的に提供するAndroid Enterpriseオプションが有効になっている場合、Citrix Endpoint Managementはこのプロパティを必要とします。その場合、ダウンロードURLには認証トークンを持つワンタイムチケット（**XAM One-Time Ticket server**プロパティで定義）を含めることはできません。デフォルトは**False**です。

Windowsデバイスの非認証アプリダウンロード

- ワンタイムチケットを検証しない古いCitrix Secure Hubバージョンでのみ使用されます。**False**の場合、Citrix Endpoint ManagementからWindowsデバイスに非認証アプリをダウンロードできます。デフォルトは**False**です。

ActiveSync IDを使用してActiveSyncデバイスワイプを実行する

- **true**の場合、Exchange ActiveSync用Citrix Endpoint Managementコネクタは、ActiveSync識別子を**asWipeDevice**メソッドの引数として使用します。デフォルトは**false**です。

Exchangeからのユーザーのみ

- **true**の場合、ActiveSync Exchangeユーザーのユーザー認証を無効にします。デフォルトは**false**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ボリューム購入ベースライン間隔

- Citrix Endpoint ManagementがAppleからボリューム購入ライセンスを再インポートする最小間隔。ライセンス情報を更新することで、ボリューム購入からインポートされたアプリを手動で削除した場合など、すべての変更がCitrix Endpoint Managementに反映されるようになります。デフォルトでは、Citrix Endpoint Managementはボリューム購入ライセンスのベースラインを最低**1440**分ごとに更新します。
    - 多数のボリューム購入ライセンス（たとえば50,000以上）がインストールされている場合、Citrixはライセンスのインポート頻度とオーバーヘッドを削減するために、ベースライン間隔を長くすることをお勧めします。
    - Appleからのボリューム購入ライセンスの変更が頻繁に発生すると予想される場合、Citrixは変更をCitrix Endpoint Managementに反映させるために、値を低くすることをお勧めします。
    - 2つのベースライン間の最小間隔は60分です。また、Citrix Endpoint Managementは、最後のインポート以降の変更をキャプチャするために、60分ごとに差分インポートを実行します。したがって、ボリューム購入ベースライン間隔が60分の場合、ベースライン間の間隔は最大119分遅れる可能性があります。

WebServices タイムアウトタイプ

- パブリックAPIから取得した認証トークンの有効期限をどのように設定するかを指定します。
    - **STATIC_TIMEOUT**の場合: Citrix Endpoint Managementは、サーバープロパティ**Static Timeout in Minutes**の値に基づいて、トークンの有効期限が切れたと見なします。
    - **INACTIVITY_TIMEOUT**の場合: Citrix Endpoint Managementは、サーバープロパティ**Inactivity Timeout in Minutes**の値に基づいて、トークンの有効期限が切れたと見なします。デフォルトは**STATIC_TIMEOUT**です。

WindowsタブレットMDM証明書の有効期間延長 (5年)

- WindowsタブレットにMDMが発行するデバイス証明書の有効期間。デバイスは、デバイス管理中にMDMサーバーへの認証にデバイス証明書を使用します。**true**の場合、有効期間は5年です。**false**の場合、有効期間は2年です。デフォルトは**true**です。

Windows WNSチャネル - 更新までの日数

- ChannelURIの更新頻度。デフォルトは**10**日です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows WNSハートビート間隔

- Citrix Endpoint Managementが、デバイスに3分ごとに5回接続した後、次に接続するまでに待機する時間。デフォルトは**6**時間です。

XAMワンタイムチケット

- ワンタイム認証トークン (OTT) がアプリのダウンロードに有効なミリ秒数。このプロパティと、**Unauthenticated App download for Android**および**Unauthenticated App download for Windows**プロパティは連携して動作します。これらのプロパティは、認証されていないアプリのダウンロードを許可するかどうかを指定します。デフォルトは**3600000**です。

Citrix Endpoint Management MDMセルフヘルプポータルコンソールの最大非アクティブ間隔(分)

- このプロパティ名は、以前のCitrix Endpoint Managementバージョンを反映しています。このプロパティは、Citrix Endpoint Managementコンソールの最大非アクティブ間隔を制御します。この間隔は、Citrix Endpoint Managementが非アクティブなユーザーをCitrix Endpoint Managementコンソールからログアウトさせるまでの分数です。タイムアウトが**0**の場合、非アクティブなユーザーはログインしたままになります。デフォルトは**30**です。

ABM MDMサーバーから割り当て解除されたときに、ABMデバイスをCEMから削除する

- もし `remove.unassigned.abm.devices` が **true** の場合、CEM はこのサーバーに割り当てられなくなったデバイスを削除します。デフォルトは **false** です。

デバイスとアプリのポリシー

Citrix Endpoint Management のデバイスおよびアプリのポリシーを使用すると、次のような要素間のバランスを最適化できます。

- エンタープライズセキュリティ
- 企業データと資産の保護
- ユーザーのプライバシー
- 生産的でポジティブなユーザーエクスペリエンス

これらの要素間の最適なバランスは異なる場合があります。たとえば、金融などの厳しく規制されている組織では、ユーザーの生産性が主な考慮事項となる教育や小売などの他の業界よりも、より厳格なセキュリティ制御が必要です。

ユーザーのID、デバイス、場所、接続タイプに基づいてポリシーを一元的に制御および構成し、企業コンテンツの悪意のある使用を制限できます。デバイスが紛失または盗難された場合、ビジネスアプリケーションとデータをリモートで無効化、ロック、またはワイプできます。全体とし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

て、従業員の満足度と生産性を向上させながら、セキュリティと管理制御を確保するソリューションとなります。

この記事の主な焦点は、セキュリティに関連する多くのデバイスおよびアプリのポリシーです。

セキュリティリスクに対処するポリシー

Citrix Endpoint Management のデバイスおよびアプリのポリシーは、次のようなセキュリティリスクをもたらす可能性のある多くの状況に対処します。

- ユーザーが信頼できないデバイスや予測不能な場所からアプリやデータにアクセスしようとする場合
- ユーザーがデバイス間でデータをやり取りする場合
- 不正なユーザーがデータにアクセスしようとする場合
- 退職したユーザーが自身のデバイス (BYOD) を使用した場合
- ユーザーがデバイスを紛失する
- ユーザーは常に安全にネットワークにアクセスする必要があります
- ユーザーは自分のデバイスを管理しており、仕事のデータと個人のデータを分離する必要があります
- デバイスがアイドル状態になり、ユーザー資格情報の再検証が必要になる
- ユーザーが機密性の高いコンテンツを保護されていないメールシステムにコピー＆ペーストする
- ユーザーが、個人アカウントと会社アカウントの両方を持つデバイスで、機密データを含むメール添付ファイルやWebリンクを受信する

これらの状況は、企業データを保護する上で懸念される2つの主要な領域に関連しています。それは、データが次の状態にある場合です。

- 保存されている状態
- 転送中の状態

Citrix Endpoint Managementが保存データを保護する方法

モバイルデバイスに保存されているデータは「保存データ」と呼ばれます。Citrix Endpoint Managementは、iOSおよびAndroidプラットフォームが提供するデバイス暗号化を使用します。Citrix Endpoint Managementは、Citrix MAM SDKを通じて利用できるコンプライアンスチェックなどの機能で、プラットフォームベースの暗号化を補完します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementのモバイルアプリケーション管理（MAM）機能により、Citrixモバイル生産性アプリ、MDX対応アプリ、およびそれらに関連するデータの完全な管理、セキュリティ、および制御が可能になります。

Mobile Apps SDKは、Citrix MDXアプリコンテナテクノロジーを使用することで、Citrix Endpoint Management展開用のアプリを有効にします。このコンテナテクノロジーは、ユーザーデバイス上の企業アプリとデータを個人アプリとデータから分離します。このデータ分離により、カスタム開発されたサードパーティ製またはBYOモバイルアプリを、包括的なポリシーベースの制御で保護できます。

Citrix Endpoint Managementには、アプリレベルの暗号化も含まれています。Citrix Endpoint Managementは、デバイスのパスコードを要求したり、ポリシーを適用するためにデバイスを管理したりすることなく、MDX対応アプリ内に保存されているデータを個別に暗号化します。

- iOSデバイスでは、Citrix Endpoint Managementは、キーチェーンなどの強力なFIPS検証済み暗号化サービスとライブラリを使用します。
- OpenSSL はさまざまなデバイスプラットフォーム向けに FIPS 検証済みモジュールを提供します。OpenSSL は、転送中のデータと、デバイスの管理および登録に必要な証明書をさらに保護します。
- Citrix Endpoint Management は、MAM SDK 共有ボールト API を使用して、同じキーチェーンアクセスグループを持つアプリ間で管理対象コンテンツを共有します。たとえば、登録済みアプリを介してユーザー証明書を共有し、アプリがセキュアボールトから証明書を取得できるようにすることができます。
- Citrix Endpoint Management は、プラットフォームが提供するデバイス暗号化を使用します。
- Citrix Endpoint Management のアプリレベルの MAM コントロールは、アプリを起動するたびにデバイス暗号化が有効になっていることを検証するためのコンプライアンスチェックを実行します。

Citrix Endpoint Management が転送中のデータを保護する方法

ユーザーのモバイルデバイスと社内ネットワーク間で移動するデータは、転送中のデータと呼ばれます。MDX アプリコンテナテクノロジーは、NetScaler Gateway を介して社内ネットワークへのアプリケーション固有の VPN アクセスを提供します。

従業員がモバイルデバイスからセキュアなエンタープライズネットワーク内にある以下のリソースにアクセスしたい状況を考えてみましょう。

- 企業のメールサーバー
- 企業イントラネットでホストされている SSL 対応の Web アプリケーション

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ファイルサーバーまたは Microsoft SharePoint に保存されているドキュメント

MDX は、アプリケーション固有のマイクロ VPN を介して、モバイルデバイスからこれらすべてのエンタープライズリソースへのアクセスを可能にします。各デバイスには、専用のマイクロ VPN トンネルがあります。

マイクロ VPN 機能は、信頼できないモバイルデバイスのセキュリティを危険にさらす可能性のあるデバイス全体の VPN を必要としません。その結果、社内ネットワークは、企業システム全体に感染する可能性のあるマルウェアや攻撃にさらされることはありません。企業のモバイルアプリと個人のモバイルアプリは、1つのデバイス上で共存できます。

さらに強力なレベルのセキュリティを提供するために、MDX 対応アプリを代替 NetScaler Gateway ポリシーで構成できます。このポリシーは、認証とアプリとのマイクロ VPN セッションに使用されます。マイクロ VPN セッション必須ポリシーで代替 NetScaler Gateway を使用して、アプリに特定のゲートウェイへの再認証を強制することができます。このようなゲートウェイは通常、異なる（より高い保証の）認証要件とトラフィック管理ポリシーを持つ場合があります。

セキュリティ機能に加えて、マイクロ VPN 機能は、圧縮アルゴリズムを含むデータ最適化技術も提供します。圧縮アルゴリズムは、次のことを保証します。

- 最小限のデータのみが転送される
- 転送は可能な限り最速で行われます。速度はユーザーエクスペリエンスを向上させ、これはモバイルデバイス導入における主要な成功要因です。

次のような状況で、デバイスポリシーを定期的に再評価してください。

- デバイスのオペレーティングシステムアップデートのリリースにより、Citrix Endpoint Managementの新しいバージョンに新規または更新されたポリシーが含まれる場合
- デバイスタイプを追加する場合：

  多くのポリシーはすべてのデバイスに共通していますが、各デバイスにはそのオペレーティングシステムに固有のポリシーセットがあります。その結果、iOS、Android、Windowsデバイス間、さらには異なるメーカーのAndroidデバイス間でも違いが見られる場合があります。
- 新しい企業セキュリティポリシーやコンプライアンス規制など、企業または業界の変化に合わせてCitrix Endpoint Managementの運用を同期させるため
- MAM SDKの新しいバージョンに新規または更新されたポリシーが含まれる場合
- アプリを追加または更新する場合
- 新しいアプリや新しい要件により、ユーザー向けに新しいワークフローを統合するため

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリポリシーとユースケースシナリオ

Citrix Secure Hubを通じて利用可能なアプリを選択できますが、それらのアプリがCitrix Endpoint Managementとどのように連携するかを定義したい場合もあるでしょう。アプリポリシーは次の場合に使用します：

- 一定期間が経過した後にユーザーに認証を要求する場合。
- ユーザーに情報へのオフラインアクセスを提供したい場合。

以下のセクションでは、いくつかのポリシーと使用例について説明します。

- MAM SDKを使用してiOSおよびAndroidアプリに統合できるサードパーティポリシーのリストについては、MAM SDKの概要を参照してください。
- 各プラットフォームのすべてのMDXポリシーのリストについては、MDX Policies at a Glanceを参照してください。

認証ポリシー

- **デバイスパスコード**

  このポリシーを使用する理由: デバイスパスコードポリシーを有効にすると、デバイスにデバイスパスコードが有効になっている場合にのみ、ユーザーがMDXアプリにアクセスできるようになります。この機能により、デバイスレベルでのiOS暗号化の使用が保証されます。

  ユーザーの例: このポリシーを有効にすると、ユーザーはMDXアプリにアクセスする前に、iOSデバイスにパスコードを設定する必要があります。

- **アプリパスコード**

  このポリシーを使用する理由: アプリパスコードポリシーを有効にすると、Citrix Secure Hubは、ユーザーがアプリを開いてデータにアクセスする前に、管理対象アプリへの認証を要求します。ユーザーは、Citrix Endpoint Managementコンソールの**Settings > Client Properties**で設定した内容に応じて、Active Directoryパスワード、Citrix PIN、またはiOS TouchIDで認証する場合があります。Client Propertiesで非アクティブタイマーを設定すると、タイマーが期限切れになるまでCitrix Secure Hubが管理対象アプリへの再認証をユーザーに要求しないようにすることができます。

  アプリパスコードはデバイスパスコードとは異なります。デバイスにプッシュされたデバイスパスコードポリシーを使用すると、Citrix Secure Hubはユーザーにパスコードまたは PINの設定を要求します。ユーザーは、デバイスの電源を入れたとき、または非アクティブタイマーが期限切れになったときに、デバイスのロックを解除する必要があります。詳細については、Authentication in Citrix Endpoint Managementを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーの例: デバイスでCitrix Secure Webアプリケーションを開く際、非アクティブ期間が期限切れになっている場合、ユーザーはウェブサイトを閲覧する前にCitrix PINを入力する必要があります。

- **micro VPNセッションが必要**

  このポリシーを使用する理由: アプリケーションの実行にWebアプリ（Webサービス）へのアクセスが必要な場合は、このポリシーを有効にします。Citrix Endpoint Managementは、アプリを使用する前に、ユーザーにエンタープライズネットワークへの接続またはアクティブなセッションの確立を要求します。

  ユーザーの例: micro VPNセッション必須ポリシーが有効になっているMDXアプリをユーザーが開こうとすると、ネットワークに接続するまでアプリを使用できません。接続には、セルラーまたはWi-Fiサービスを使用する必要があります。

- **最大オフライン期間**

  このポリシーを使用する理由: このポリシーは、追加のセキュリティオプションとして使用します。このポリシーにより、指定された期間オフラインでアプリを実行するユーザーは、アプリの資格を再確認し、ポリシーを更新する必要があります。

  ユーザーの例: MDXアプリを最大オフライン期間で構成した場合、ユーザーはオフラインタイマー期間が期限切れになるまで、アプリをオフラインで開いて使用できます。その時点で、ユーザーはセルラーまたはWi-Fiサービスを介してネットワークに再接続し、プロンプトが表示された場合は再認証する必要があります。

その他のアクセス ポリシー

- **アプリ更新猶予期間 (時間)**

  このポリシーを使用する理由: アプリ更新猶予期間とは、アプリストアで新しいバージョンが利用可能になったアプリをユーザーが更新しなければならないまでの期間です。猶予期間が終了すると、ユーザーはアプリ内のデータにアクセスする前にアプリを更新する必要があります。この値を設定する際は、モバイルワーカー、特に海外旅行中に長期間オフラインになる可能性のあるユーザーのニーズを考慮してください。

  ユーザーの例: アプリストアにCitrix Secure Mailの新しいバージョンをロードし、アプリ更新猶予期間を6時間に設定します。Citrix Secure Hubユーザーは、アプリストアにリダイレクトされる前に、Citrix Secure Mailをアップグレードするために6時間の猶予があります。

- **アクティブポーリング期間 (分)**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このポリシーを使用する理由: アクティブポーリング期間とは、Citrix Endpoint ManagementがApp LockやApp Wipeなどのセキュリティアクションを実行するタイミングをアプリで確認する間隔です。

ユーザーの例: アクティブポーリング期間ポリシーを60分に設定し、App Lockコマンドを送信すると、最後のポーリングから60分以内にロックが実行されます。

非準拠デバイスの動作ポリシー

デバイスが最小限のコンプライアンス要件を下回った場合、非準拠デバイスの動作ポリシーにより、実行するアクションを選択できます。詳細については、「非準拠デバイスの動作」を参照してください。

アプリの対話ポリシー

これらのポリシーを使用する理由: アプリの対話ポリシーを使用して、MDXアプリからデバイス上の他のアプリへのドキュメントとデータのフローを制御します。たとえば、ユーザーが次のことを行うのを防ぐことができます。

- コンテナ外の個人用アプリにデータを移動する
- コンテナ外からコンテナ化されたアプリにデータを貼り付ける

ユーザーの例: アプリの対話ポリシーを「制限付き」に設定すると、ユーザーはCitrix Secure MailからCitrix Secure Webにテキストをコピーできます。ユーザーは、そのデータをコンテナ外の個人用SafariまたはChromeブラウザにコピーすることはできません。また、ユーザーはCitrix Secure Mailから添付ドキュメントをCitrix FilesまたはQuickEditで開くことができます。ユーザーは、コンテナ外の個人用ファイル表示アプリで添付ドキュメントを開くことはできません。

アプリ制限ポリシー

これらのポリシーを使用する理由: アプリ制限ポリシーを使用して、MDXアプリの実行中にユーザーがアクセスできる機能を制御します。この制限により、アプリの実行中に悪意のあるアクティビティが発生しないようにします。アプリ制限ポリシーは、iOSとAndroidで若干異なります。たとえば、iOSではMDXアプリの実行中にiCloudへのアクセスをブロックできます。Androidでは、MDXアプリの実行中にNFCの使用を停止できます。

ユーザーの例: MDXアプリでiOSのディクテーションをブロックするアプリ制限ポリシーを有効にしたとします。その結果、MDXアプリの実行中にユーザーはiOSキーボードのディクテーション機能を使用できません。そのため、ユーザーがディクテーションしたデータは、安全でないサードパーティのクラウドディクテーションサービスに渡されません。ユーザーがコンテナ外で個人用アプリを開くと、個人間の通信のためにディクテーションオプションは引き続き利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリネットワークアクセスポリシー

これらのポリシーを使用する理由: アプリネットワークアクセスポリシーを使用して、デバイス上のコンテナ内のMDXアプリから企業ネットワーク内のデータへのアクセスを提供します。トンネル化 - Web SSOオプションは、HTTPおよびHTTPSトラフィックのトンネル化のみを許可します。このオプションは、HTTPおよびHTTPSトラフィックのシングルサインオン（SSO）とPKINIT認証を提供します。

ユーザーの例: ユーザーがトンネル化が有効になっているMDXアプリを開くと、ブラウザはユーザーがVPNを開始することなくイントラネットサイトを開きます。アプリはマイクロVPNテクノロジーを使用して内部サイトに自動的にアクセスします。

アプリの地理位置情報およびジオフェンシングポリシー

これらのポリシーを使用する理由: アプリの地理位置情報とジオフェンシングを制御するポリシーには、中心点の経度、中心点の緯度、および半径が含まれます。これらのポリシーは、MDXアプリ内の特定の地理的エリアのデータにアクセスできます。ポリシーは、緯度と経度の座標の半径によって地理的エリアを定義します。ユーザーが定義された半径外でアプリを使用しようとすると、アプリはロックされたままになり、ユーザーはアプリデータにアクセスできません。

ユーザーの例: ユーザーはオフィスにいる間、合併買収データにアクセスできます。オフィスから離れると、この機密データにはアクセスできなくなります。

Citrix Secure Mailアプリポリシー

- **バックグラウンドネットワークサービス**

  このポリシーを使用する理由: Citrix Secure Mailのバックグラウンドネットワークサービスは、NetScaler Gatewayを介して接続するために、実質的にSOCKS5プロキシであるSecure Ticket Authority（STA）を使用します。STAは長期間の接続をサポートし、マイクロVPNと比較してバッテリー寿命を向上させます。そのため、STAは常に接続するメールに最適です。Citrixは、Citrix Secure Mailにこれらの設定を構成することを推奨しています。NetScaler for XenMobileウィザードは、Citrix Secure Mail用にSTAを自動的にセットアップします。

  ユーザーの例: STAが有効になっていない場合、AndroidユーザーがCitrix Secure Mailを開くと、VPNを開くように求められ、VPNはデバイス上で開いたままになります。STAが有効になっている場合、AndroidユーザーがCitrix Secure Mailを開くと、Citrix Secure MailはVPNを必要とせずにシームレスに接続します。

- **デフォルトの同期間隔**

  このポリシーを使用する理由: この設定は、ユーザーがCitrix Secure Mailに初めてアクセスしたときに、Citrix Secure Mailに同期されるメールのデフォルトの日数を指定します。2週間分

© 1997–2026 Citrix Systems, Inc. All rights reserved.

のメールは、3日分のメールよりも同期に時間がかかります。同期するデータが多いほど、ユーザーのセットアッププロセスが長くなります。

ユーザーの例: ユーザーがCitrix Secure Mailを初めてセットアップしたときに、デフォルトの同期間隔が3日に設定されているとします。ユーザーは、現在から過去3日間に受信したメールをすべて受信トレイで確認できます。ユーザーが3日よりも古いメールを確認したい場合は、検索を実行できます。Citrix Secure Mailは、サーバーに保存されている古いメールを表示します。Citrix Secure Mailをインストールした後、各ユーザーはこの設定を自分のニーズに合わせて変更できます。

デバイスポリシーとユースケースの動作

デバイスポリシーは、MDMポリシーと呼ばれることもあり、Citrix Endpoint Managementがデバイスを管理する方法を決定します。多くのポリシーはすべてのデバイスに共通ですが、各デバイスにはそのオペレーティングシステムに固有のポリシーセットがあります。次のリストには、いくつかのデバイスポリシーが含まれており、それらの使用方法について説明しています。すべてのデバイスポリシーのリストについては、「デバイスポリシー」の記事を参照してください。

- **アプリインベントリポリシー**

  このポリシーを使用する理由: ユーザーがインストールしたアプリを確認するには、アプリインベントリポリシーをデバイスに展開します。このポリシーを展開しない場合、ユーザーがアプリストアからインストールしたアプリのみが表示され、個人でインストールしたアプリは表示されません。アプリインベントリポリシーを使用して、特定のアプリが企業デバイスで実行されないようにブロックできます。

  ユーザーの例: MDM管理対象デバイスのユーザーは、この機能を無効にできません。ユーザーが個人でインストールしたアプリケーションは、Citrix Endpoint Management管理者から参照できます。

- **アプリロックポリシー**

  このポリシーを使用する理由: Android向けのアプリロックポリシーを使用すると、アプリを許可リストまたはブロックリストに配置できます。たとえば、許可されたアプリの場合、キオスクデバイスを構成できます。通常、アプリロックポリシーは、ユーザーがインストールできるアプリを制限するため、企業所有のデバイスにのみ展開します。ブロックされたアプリへのユーザーアクセスを提供するために、上書きパスワードを設定できます。

  ユーザーの例: Angry Birdsアプリをブロックするアプリロックポリシーを展開したとします。ユーザーはGoogle PlayからAngry Birdsアプリをインストールできますが、アプリを開くと、管理者がアプリをブロックしたことを通知するメッセージが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **接続スケジュールポリシー**

  このポリシーを使用する理由: 接続スケジュールポリシーにより、Windows Mobileデバイスは MDM管理、アプリプッシュ、およびポリシー展開のためにCitrix Endpoint Managementに接続できます。AndroidおよびAndroid Enterpriseデバイスの場合は、代わりにGoogle Firebase Cloud Messaging (FCM) を使用します。FCMはCitrix Endpoint Managementへの接続を制御します。スケジューリングオプションは次のとおりです。

  - **しない:** 手動で接続します。ユーザーは、デバイス上のCitrix Endpoint Managementから接続を開始する必要があります。このオプションは、デバイスにセキュリティポリシーを展開できなくなるため、Citrixは本番環境での展開には推奨しません。その結果、ユーザーは新しいアプリやポリシーを受け取ることができません。**しない**オプションはデフォルトで有効になっています。
  - **毎回:** 選択した間隔で接続します。ロックやワイプなどのセキュリティポリシーを送信すると、Citrix Endpoint Managementはデバイスが次回接続したときにデバイス上でポリシーを処理します。
  - **スケジュールを定義:** Citrix Endpoint Managementは、ネットワーク接続が失われた後、ユーザーのデバイスをCitrix Endpoint Managementサーバーに再接続しようとします。Citrix Endpoint Managementは、定義した時間枠内で定期的に制御パケットを送信することで接続を監視します。

  ユーザーの例: 登録済みデバイスにパスコードポリシーを展開したいとします。スケジューリングポリシーにより、デバイスは定期的にサーバーに接続して新しいポリシーを収集するようになります。

- **資格情報ポリシー**

  このポリシーを使用する理由: ネットワークポリシーと組み合わせて使用されることが多い資格情報ポリシーを使用すると、証明書認証を必要とする内部リソースへの認証用の証明書を展開できます。

  ユーザーの例: デバイスにワイヤレスネットワークを構成するネットワークポリシーを展開します。Wi-Fiネットワークには認証用の証明書が必要です。資格情報ポリシーは、オペレーティングシステムのキーストアに保存される証明書を展開します。ユーザーは、内部リソースに接続したときに証明書を選択できます。

- **Exchangeポリシー**

  このポリシーを使用する理由: Citrix Endpoint Managementでは、Microsoft Exchange ActiveSyncメールを配信するための2つのオプションがあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Citrix Secure Mailアプリ:** パブリックアプリストアまたはアプリストアから配布するCitrix Secure Mailアプリを使用してメールを配信します。
- **ネイティブメールアプリ:** デバイス上のネイティブメールクライアントでActiveSyncメールを有効にします。マクロを使用して、ユーザーのActive Directory属性からユーザーデータを入力できます。たとえば、ユーザー名を入力するには`${user.username}`、ユーザーのドメインを入力するには`${user.domain}`を使用します。

ユーザーの例: Exchangeポリシーをプッシュすると、Exchange Serverの詳細がデバイスに送信されます。Citrix Secure Hubはユーザーに認証を促し、メールの同期が開始されます。

- **位置情報ポリシー**

  このポリシーを使用する理由: デバイスでCitrix Secure HubのGPSが有効になっている場合、位置情報ポリシーを使用すると、マップ上でデバイスの地理的位置を特定できます。このポリシーを展開し、Citrix Endpoint Managementから位置特定コマンドを送信すると、デバイスは位置座標を返します。

  ユーザーの例: 位置情報ポリシーを展開し、デバイスでGPSが有効になっている場合: ユーザーがデバイスを紛失した場合、Citrix Endpoint Managementセルフヘルプポータルにログオンし、位置特定オプションを選択してマップ上でデバイスの位置を確認できます。ユーザーは、Citrix Secure Hubが位置情報サービスを使用することを許可するかどうかを選択します。ユーザーが自分でデバイスを登録する場合、位置情報サービスの使用を強制することはできません。このポリシーを使用する際のもう1つの考慮事項は、バッテリー寿命への影響です。

- **パスコードポリシー**

  このポリシーを使用する理由: パスコードポリシーを使用すると、管理対象デバイスにPINコードまたはパスワードを強制できます。このパスコードポリシーを使用すると、デバイスのパスコードの複雑さとタイムアウトを設定できます。

  ユーザーの例: 管理対象デバイスにパスコードポリシーを展開すると、Citrix Secure Hubはユーザーにパスコードまたは PINの構成を促します。パスコードまたはPINは、起動時または非アクティブタイマーの期限切れ時に、ユーザーがデバイスにアクセスできるようにします。

- **プロファイル削除ポリシー**

  このポリシーを使用する理由: ユーザーグループにポリシーを展開し、後でそのポリシーをユーザーの一部から削除する必要があるとします。プロファイル削除ポリシーを作成することで、選択したユーザーのポリシーを削除できます。次に、展開ルールを使用して、指定したユーザーにのみプロファイル削除ポリシーを展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーの例: プロファイル削除ポリシーをユーザーデバイスに展開しても、ユーザーはその変更に気づかない場合があります。たとえば、プロファイル削除ポリシーがデバイスカメラを無効にする制限を削除した場合、ユーザーはその変更について知りません。変更がユーザーエクスペリエンスに影響を与える場合は、ユーザーに知らせることを検討してください。

- **制限ポリシー**

  このポリシーを使用する理由: 制限ポリシーは、管理対象デバイスの機能や動作をロックダウンして制御するための多くのオプションを提供します。サポートされているデバイスに対して、数百もの制限オプションを有効にできます。たとえば、デバイスのカメラやマイクを無効にしたり、ローミングルールを適用したり、アプリストアなどのサードパーティサービスへのアクセスを強制したりできます。

  ユーザーの例: iOSデバイスに制限を展開した場合、ユーザーはiCloudやApple App Storeにアクセスできない可能性があります。

- **利用規約ポリシー**

  このポリシーを使用する理由: デバイスが管理されることの法的影響についてユーザーに助言する必要がある場合があります。また、企業データがデバイスにプッシュされる際のセキュリティリスクについてユーザーが認識していることを確認したい場合もあります。利用規約ドキュメントを使用すると、ユーザーが登録する前にルールと通知を公開できます。

  ユーザーの例: ユーザーは登録プロセス中に利用規約情報を確認します。提示された条件の受け入れを拒否した場合、登録プロセスは終了し、企業データにアクセスできません。誰が条件を受け入れたか、または拒否したかを示すレポートを人事/法務/コンプライアンスチームに提供できます。

- **VPNポリシー**

  このポリシーを使用する理由: VPNポリシーを使用して、古いVPNゲートウェイテクノロジーを使用するバックエンドシステムへのアクセスを提供します。このポリシーは、Cisco AnyConnect、Juniper、Citrix VPNなど、さまざまなVPNプロバイダーをサポートしています。VPNゲートウェイがこのオプションをサポートしている場合、このポリシーをCAにリンクしてオンデマンドVPNを有効にすることも可能です。

  ユーザーの例: VPNポリシーが有効になっている場合、ユーザーが内部ドメインにアクセスすると、ユーザーのデバイスはVPN接続を開きます。

- **Webクリップポリシー**

  このポリシーを使用する理由: Webサイトに直接開くアイコンをデバイスにプッシュしたい場合は、Webクリップポリシーを使用します。WebクリップにはWebサイトへのリンクがあり、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カスタムアイコンを含めることができます。デバイス上では、Webクリップはアプリアイコンのように見えます。

ユーザーの例: ユーザーはWebクリップアイコンをクリックしてインターネットサイトを開き、必要なサービスにアクセスできます。ブラウザでリンクアドレスを入力するよりも、Webリンクを使用する方が便利です。

- **ネットワークポリシー**

  このポリシーを使用する理由: ネットワークポリシーを使用すると、SSID、認証データ、構成データなどのWi-Fiネットワークの詳細を管理対象デバイスに展開できます。

  ユーザーの例: ネットワークポリシーを展開すると、デバイスは自動的にWi-Fiネットワークに接続し、ユーザーを認証するため、ネットワークにアクセスできるようになります。

- **エンドポイント管理ストアポリシー**

  このポリシーを使用する理由: アプリストアは、管理者がユーザーに必要なすべての企業アプリとデータリソースを公開できる、統合されたアプリストアです。管理者は以下を追加できます。

  - Webアプリ、SaaSアプリ、MAM SDK対応アプリ、またはMDXでラップされたアプリ
  - Citrixモバイル生産性向上アプリ
  - ネイティブモバイルアプリ（.ipaファイルや.apkファイルなど）
  - Apple App StoreおよびGoogle Playアプリ
  - Webリンク
  - Citrix StoreFrontを使用して公開されたCitrix Virtual Apps

  ユーザーの例: ユーザーがデバイスをCitrix Endpoint Managementに登録すると、Citrix Secure Hubアプリを介してアプリストアにアクセスします。ユーザーは、利用可能なすべての企業アプリとサービスを確認できます。ユーザーはアプリをクリックしてインストールしたり、データにアクセスしたり、アプリを評価およびレビューしたり、アプリストアからアプリの更新をダウンロードしたりできます。

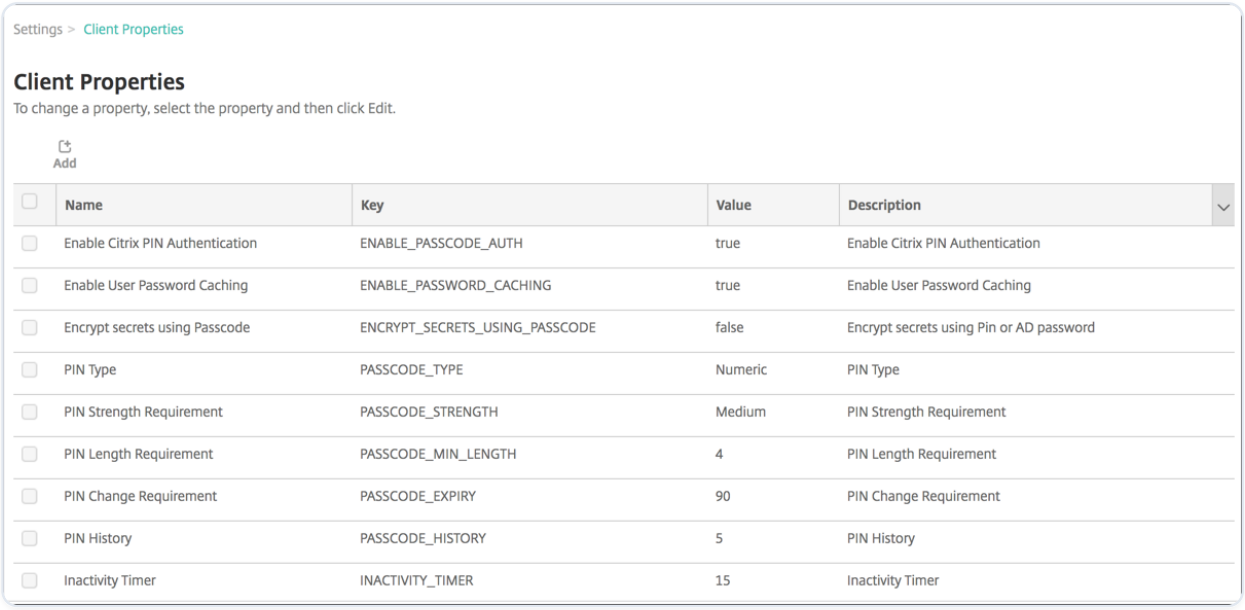
クライアントプロパティ

クライアントプロパティには、ユーザーデバイス上のCitrix Secure Hubに直接提供される情報が含まれています。これらのプロパティを使用して、Citrix PINなどの高度な設定を構成できます。クライアントプロパティはCitrixサポートから入手できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クライアントプロパティは、Citrix Secure Hubのリリースごとに、またクライアントアプリによっては変更される場合があります。より一般的に構成されるクライアントプロパティの詳細については、この記事の後半にある「クライアントプロパティのリファレンス」を参照してください。

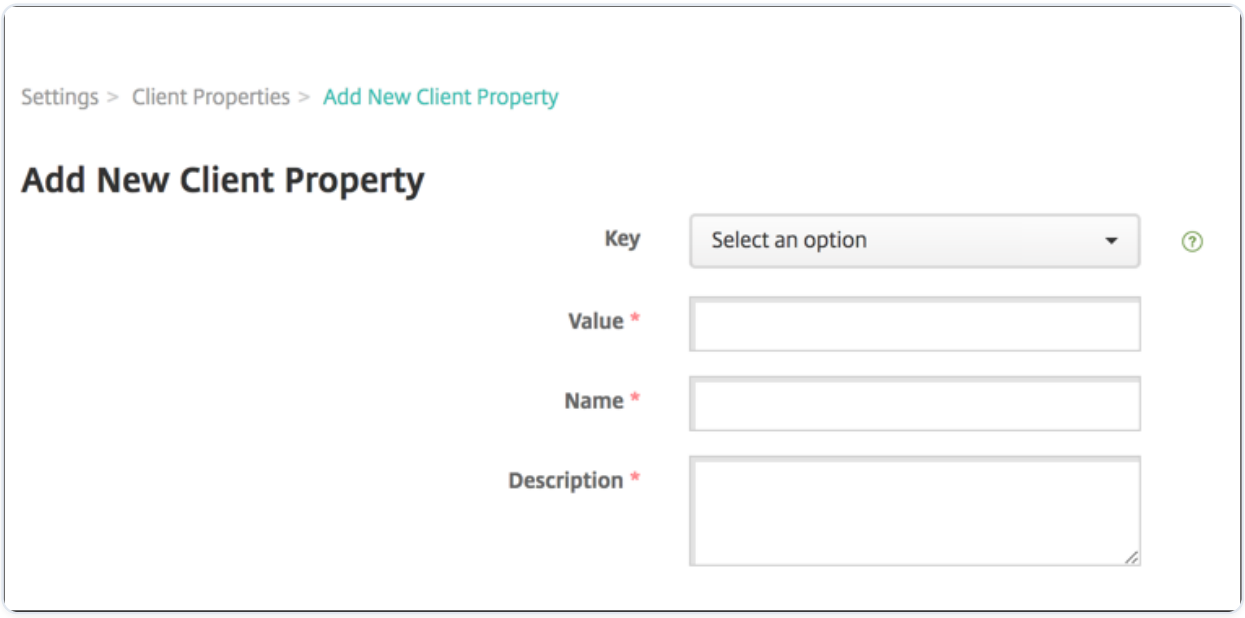
1. Citrix Endpoint Managementコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **クライアント**の下で、**クライアントプロパティ**をクリックします。**クライアントプロパティ**ページが表示されます。このページからクライアントプロパティを追加、編集、削除できます。



Name	Key	Value	Description
Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	true	Enable Citrix PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	true	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
PIN Type	PASSCODE_TYPE	Numeric	PIN Type
PIN Strength Requirement	PASSCODE_STRENGTH	Medium	PIN Strength Requirement
PIN Length Requirement	PASSCODE_MIN_LENGTH	4	PIN Length Requirement
PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
PIN History	PASSCODE_HISTORY	5	PIN History
Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer

クライアントプロパティを追加するには

1. **追加**をクリックします。**新しいクライアントプロパティの追加**ページが表示されます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 次の設定を構成します。

   - **キー:** ドロップダウンリストから追加するプロパティキーをクリックします。**重要:** 設定を更新する前にCitrixサポートに連絡してください。特別なキーを要求できます。
   - **値:** 選択したプロパティの値。
   - **名前:** プロパティの名前。
   - **説明:** プロパティの説明。

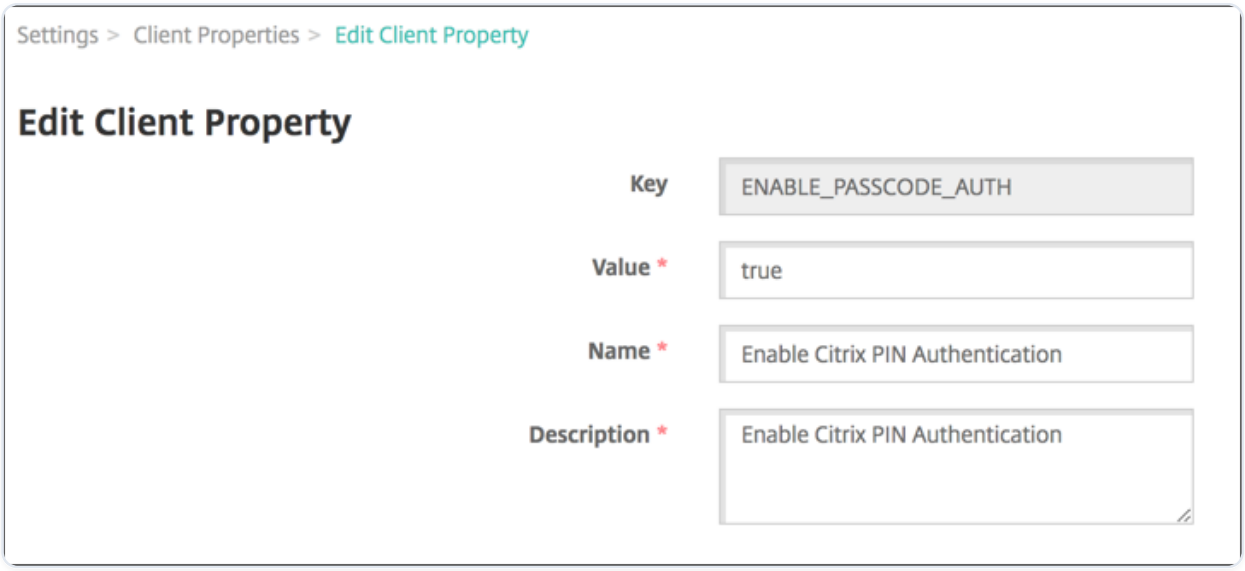
3. **保存**をクリックします。

クライアントプロパティを編集するには

1. **クライアントプロパティ**テーブルで、編集するクライアントプロパティを選択します。

   クライアントプロパティの横にあるチェックボックスを選択すると、クライアントプロパティリストの上にあるオプションメニューが開きます。リスト内の他の場所をクリックすると、リストの右側にあるオプションメニューが開きます。

2. **編集**をクリックします。**クライアントプロパティの編集**ページが表示されます。



3. 必要に応じて、次の情報を変更します。

   - **キー:** このフィールドは変更できません。
   - **値:** プロパティ値。
   - **名前:** プロパティ名。
   - **説明:** プロパティの説明。

4. **保存**をクリックして変更を保存するか、**キャンセル**をクリックしてプロパティを変更せずに終了します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クライアントプロパティを削除するには

1. **クライアントプロパティ**テーブルで、削除するクライアントプロパティを選択します。

   各プロパティの横にあるチェックボックスを選択すると、複数のプロパティを選択して削除できます。

2. **削除**をクリックします。確認ダイアログボックスが表示されます。もう一度**削除**をクリックします。

クライアントプロパティのリファレンス

Citrix Endpoint Management の事前定義されたクライアントプロパティとそのデフォルト設定は次のとおりです。

- **ALLOW_CLIENTSIDE_PROXY**
  - 表示名: ALLOW_CLIENTSIDE_PROXY
  - ユーザーが iOS フォンで構成したプロキシを使用したい場合は、このカスタムポリシーをデフォルト値の **true** のままにします。

    一部のユーザーは、デバイスの **> >** でプロキシをすでに構成している場合があります。Citrix Secure Hub がそれらのユーザーに対して開かない場合は、次のいずれかの操作を実行します。

    - デバイスからプロキシ構成を削除し、Citrix Secure Hub を再起動します。
    - デバイスを別の Wi-Fi ネットワークに接続します。Citrix Secure Hub が再認証されると、**ALLOW_CLIENTSIDE_PROXY** プロパティを取得して開きます。
  - **ALLOW_CLIENTSIDE_PROXY** が **false** で、ユーザーがデバイスでプロキシを構成した場合、Citrix Endpoint Management はプロキシを検出します。ただし、Citrix Secure Hub はプロキシを使用せず、エラーメッセージを表示します。プロキシが有効になっているアクセスポイントまたはルーターにデバイスが接続されている場合、Citrix Endpoint Management はプロキシを検出しません。最高のセキュリティのために、証明書ピンニングを使用することをお勧めします。Citrix Secure Hub の証明書ピンニングを有効にする方法については、「証明書ピンニング」を参照してください。
  - このカスタムクライアントポリシーを構成するには、 **>** に移動し、カスタムキー **ALLOW_CLIENTSIDE_PROXY** を追加して、 を設定します。
- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - 表示名: MDXコンテナ自己破壊期間

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 自己破壊は、指定された日数にわたる非アクティブ状態の後、Citrix Secure Hub および管理対象アプリへのアクセスを防止します。制限時間を過ぎると、アプリは使用できなくなります。データのワイプには、アプリキャッシュとユーザーデータを含む、インストールされている各アプリのアプリデータのクリアが含まれます。

  非アクティブ時間とは、サーバーが特定の期間にわたってユーザーを検証するための認証要求を受信しない期間です。このプロパティが 30 日であると仮定します。ユーザーが 30 日以上アプリを使用しない場合、ポリシーが有効になります。

  このグローバルセキュリティポリシーは、iOS および Android プラットフォームに適用され、既存のアプリロックおよびワイプポリシーの機能強化です。
- このグローバルポリシーを設定するには、**Settings > Client Properties** に移動し、カスタムキー **CONTAINER_SELF_DESTRUCT_PERIOD** を追加します。
- 値: 日数

- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - 表示名: デバイスログをITヘルプデスクに送信
  - このプロパティは、ITヘルプデスクにログを送信する機能を有効または無効にします。
  - 設定可能な値: **true** または **false**
  - デフォルト値: **false**
- **DISABLE_LOGGING**
  - 表示名: ログ記録を無効にする
  - このプロパティを使用して、ユーザーがデバイスからログを収集およびアップロードするのを防ぎます。このプロパティは、Citrix Secure Hub およびインストールされているすべてのMDXアプリのログ記録を無効にします。ユーザーはサポートページからどのアプリのログも送信できません。メール作成ダイアログボックスが表示されても、ログは添付されません。ログ記録が無効になっていることを示すメッセージが表示されます。この設定により、Citrix Endpoint Management コンソールでCitrix Secure Hub およびMDXアプリのログ設定を更新することもできなくなります。

    このプロパティが **true** に設定されている場合、Citrix Secure Hub は **Block application logs** を **true** に設定します。その結果、新しいポリシーが適用されるとMDXアプリはログ記録を停止します。
  - 設定可能な値: **true** または **false**
  - デフォルト値: **false** (ログ記録は無効になっていません)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ENABLE_CRASH_REPORTING**
  - 表示名: クラッシュレポートを有効にする
  - 「**true**」の場合、Citrix は、iOS および Android 用 Citrix Secure Hub の問題のトラブルシューティングに役立つクラッシュレポートと診断情報を収集します。「**false**」の場合、データは収集されません。
  - 指定可能な値: **true** または **false**
  - デフォルト値: **true**
- **ENABLE_CREDENTIAL_STORE**
  - 表示名: 資格情報ストアを有効にする
  - 資格情報ストアを有効にすると、Android または iOS ユーザーは Citrix モバイル生産性向上アプリにアクセスする際にパスワードを一度入力するだけで済みます。Citrix PIN を有効にするかどうかにかかわらず、資格情報ストアを使用できます。Citrix PIN を有効にしない場合、ユーザーは Active Directory パスワードを入力します。Citrix Endpoint Management は、Citrix Secure Hub およびパブリックストアアプリでのみ、資格情報ストアでの Active Directory パスワードの使用をサポートします。資格情報ストアで Active Directory パスワードを使用する場合、Citrix Endpoint Management は PKI 認証をサポートしません。
  - Citrix Secure Mail への自動登録には、このプロパティを **true** に設定する必要があります。
  - このカスタムクライアントポリシーを構成するには、**［設定］>［クライアントプロパティ］** に移動し、カスタムキー **ENABLE_CREDENTIAL_STORE** を追加して、**［値］** を **true** に設定します。
- **ENABLE_PASSCODE_AUTH**
  - 表示名: Citrix PIN 認証を有効にする
  - このプロパティを使用すると、Citrix PIN 機能を有効にできます。Citrix PIN またはパスコードを使用すると、ユーザーは Active Directory パスワードの代わりに PIN を定義するように求められます。この設定は、ENABLE_PASSWORD_CACHING が有効になっている場合、または Citrix Endpoint Management が証明書認証を使用している場合に自動的に有効になります。

    オフライン認証の場合、Citrix PIN はローカルで検証され、ユーザーは要求したアプリまたはコンテンツにアクセスできます。オンライン認証の場合、Citrix PIN またはパスコードによって Active Directory パスワードまたは証明書のロックが解除され、それが Citrix Endpoint Management で認証するために送信されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ENABLE_PASSCODE_AUTH が true で ENABLE_PASSWORD_CACHING が false の場合、Citrix Secure Hub はパスワードを保存しないため、オンライン認証では常にパスワードの入力が求められます。

- 指定可能な値: **true** または **false**
- デフォルト値: **false**

- **ENABLE_PASSWORD_CACHING**
  - 表示名: ユーザーパスワードのキャッシュを有効にする
  - このプロパティは、Active Directoryパスワードをモバイルデバイスにローカルでキャッシュできるようにします。このプロパティを**true**に設定する場合、**ENABLE_PASSCODE_AUTH**プロパティも**true**に設定する必要があります。ユーザーパスワードのキャッシュが有効になっている場合、Citrix Endpoint ManagementはユーザーにCitrix PINまたはパスコードの設定を促します。
  - 指定可能な値: **true**または**false**
  - デフォルト値: **false**
- **ENABLE_TOUCH_ID_AUTH**
  - 表示名: Touch ID認証を有効にする
  - Touch ID認証をサポートするデバイスの場合、このプロパティはデバイスでのTouch ID認証を有効または無効にします。要件:

    ユーザーデバイスでは、Citrix PINまたはLDAPが有効になっている必要があります。LDAP認証が無効になっている場合（たとえば、証明書ベースの認証のみが使用されているため）、ユーザーはCitrix PINを設定する必要があります。この場合、クライアントプロパティ**ENABLE_PASSCODE_AUTH**が**false**であっても、Citrix Endpoint ManagementはCitrix PINを要求します。

    ユーザーがアプリを起動したときにTouch IDの使用を促すプロンプトに応答する必要があるように、**ENABLE_PASSCODE_AUTH**を**false**に設定します。
  - 指定可能な値: **true**または**false**
  - デフォルト値: **false**
- **ENABLE_WORXHOME_CEIP**
  - 表示名: Citrix Secure Hub CEIPを有効にする
  - このプロパティは、カスタマーエクスペリエンス向上プログラムを有効にします。この機能は、匿名の構成データと使用状況データを定期的にCitrixに送信します。このデータは、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CitrixがCitrix Endpoint Managementの品質、信頼性、およびパフォーマンスを向上させるのに役立ちます。

- 値: **true** または **false**
- 既定値: **false**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - 表示名: パスコードを使用してシークレットを暗号化
  - このプロパティは、iOSキーチェーンなどのプラットフォームベースのネイティブストアではなく、シークレットボールトに機密データをデバイスに保存します。このプロパティは、キーアーティファクトの強力な暗号化を可能にし、ユーザーエントロピーを追加します。ユーザーエントロピーとは、ユーザーのみが知っているユーザー生成のランダムなPINコードです。

    Citrixは、ユーザーデバイスのセキュリティを向上させるために、このプロパティを有効にすることを推奨します。その結果、ユーザーはCitrix PINの認証プロンプトをより多く経験することになります。
  - 指定可能な値: **true** または **false**
  - 既定値: **false**

- **INACTIVITY_TIMER**
  - 表示名: 非アクティブタイマー
  - このプロパティは、ユーザーがデバイスを非アクティブな状態にしてから、Citrix PINまたはパスコードのプロンプトなしでアプリにアクセスできる時間を定義します。MDXアプリでこの設定を有効にするには、 設定を に設定します。 設定が に設定されている場合、ユーザーはCitrix Secure Hubにリダイレクトされ、完全な認証を行います。この設定を変更すると、ユーザーが認証を求められた次回のときに値が有効になります。

    iOSでは、非アクティブタイマーはMDXおよび非MDXアプリのCitrix Secure Hubへのアクセスも管理します。
  - 指定可能な値: 任意の正の整数
  - 既定値: **15** (分)

- **ON_FAILURE_USE_EMAIL**
  - 表示名: 失敗時にメールを使用してデバイスログをITヘルプデスクに送信する
  - このプロパティは、メールを使用してデバイスログをIT部門に送信する機能を有効または無効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 指定可能な値: **true** または **false**
- デフォルト値: **true**

- **PASSCODE_EXPIRY**
  - 表示名: PIN変更要件
  - このプロパティは、Citrix PINまたはパスコードが有効な期間を定義します。この期間が過ぎると、ユーザーはCitrix PINまたはパスコードの変更を強制されます。この設定を変更した場合、新しい値は現在のCitrix PINまたはパスコードの有効期限が切れたときにのみ設定されます。
  - 指定可能な値: **1**～**99**を推奨。PINのリセットをなくすには、値を大きな数値（例: 100,000,000,000）に設定します。有効期限を最初に1～99日の間に設定し、その期間中に大きな数値に変更した場合: PINは最初の期間の終わりには期限切れになりますが、その後は二度と期限切れになりません。
  - デフォルト値: **90** (日)

- **PASSCODE_HISTORY**
  - 表示名: PIN履歴
  - このプロパティは、ユーザーがCitrix PINまたはパスコードを変更する際に再利用できない、以前使用したCitrix PINまたはパスコードの数を定義します。この設定を変更した場合、新しい値はユーザーがCitrix PINまたはパスコードをリセットする次回に設定されます。
  - 指定可能な値: **1**～**99**
  - デフォルト値: **5**

- **PASSCODE_MAX_ATTEMPTS**
  - 表示名: PIN試行回数
  - このプロパティは、ユーザーが完全な認証を求められるまでに、Citrix PINまたはパスコードを何回間違って試行できるかを定義します。ユーザーが完全な認証に成功すると、Citrix PINまたはパスコードの作成を求められます。
  - 指定可能な値: 任意の正の整数
  - デフォルト値: **15**

- **PASSCODE_MIN_LENGTH**
  - 表示名: PINの長さの要件

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- このプロパティは、Citrix PINの最小長を定義します。
- 指定可能な値: **4～10**
- デフォルト値: **6**

- **PASSCODE_STRENGTH**
  - 表示名: PINの強度要件
  - このプロパティは、Citrix PINまたはパスコードの強度を定義します。この設定を変更すると、次回認証を求められたときに、ユーザーはCitrix PINまたはパスコードの作成を求められます。
  - 指定可能な値: **低**、**中**、**高**、または**強**
  - デフォルト値: **中**
  - PASSCODE_TYPE設定に基づく各強度設定のパスワードルールは次のとおりです:

数値パスコードのルール:

パスコードの強度	数値パスコードの種類のルール	許可	不許可
低	すべての数字、任意のシーケンスが許可されます	444444, 123456, 654321	
中 (デフォルト設定)	すべての数字を同じにしたり、連続させたりすることはできません。	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
高	隣接する数字を同じにすることはできません。	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
強力	同じ数字を2回以上使用しないでください。3つ以上の連続した数字を続けて使用しないでください。3つ以上の連続した数字を逆順で使	102983, 085085, 824673, 132312	132132, 131313, 902030

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パスコードの強度	数値パスコードの種類のルール	許可	不許可
	用しないでください。		

英数字パスコードのルール:

パスコードの強度	英数字パスコードの種類のルール	許可	不許可
低	少なくとも1つの数字と1つの文字を含める必要があります	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef
中 (デフォルト設定)	「低パスコード強度」のルールに加え、文字とすべての数字を同じにすることはできません。文字を連続させることも、数字を連続させることもできません。	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, または aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, または cba123
高	少なくとも1つの大文字と1つの小文字を含めます。	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
強	少なくとも1つの数字、1つの特殊記号、1つの大文字、および1つの小文字を含めます。	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

- **PASSCODE_TYPE**
  - 表示名: PINタイプ
  - このプロパティは、ユーザーが数値のCitrix PINを定義できるか、英数字のパスコードを定義できるかを決定します。**数値**を選択すると、ユーザーは数字のみを使用できます (Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PIN)。**英数字**を選択すると、ユーザーは文字と数字の組み合わせを使用できます (パスコード)。

この設定を変更すると、ユーザーは次回認証を求められたときに新しいCitrix PINまたはパスコードを設定する必要があります。

- 可能な値: **数値** または **英数字**
- デフォルト値: **数値**

- **REFRESHINTERVAL**
  - 表示名: REFRESHINTERVAL
  - 既定では、Citrix Endpoint Managementは3日ごとにAutoDiscovery Server (ADS)にピン留めされた証明書をpingします。更新間隔を変更するには、 **>** に移動し、カスタムキー **REFRESHINTERVAL** を追加し、 を時間数に設定します。
  - デフォルト値: **72** 時間 (3 日)
- **SEND_LDAP_ATTRIBUTES**
  - Android、iOS、またはmacOSデバイスのMAM専用展開の場合: Citrix Endpoint Managementを構成して、メール資格情報でCitrix Secure Hubに登録したユーザーがCitrix Secure Mailに自動的に登録されるようにすることができます。その結果、ユーザーはCitrix Secure Mailに登録するために追加情報を提供したり、追加の手順を実行したりする必要がありません。
  - このグローバルクライアントポリシーを構成するには、 **>** に移動し、カスタムキー **SEND_LDAP_ATTRIBUTES** を追加し、 を次のように設定します。
  - 値: `userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}`
  - 属性値は、MDMポリシーと同様にマクロとして指定されます。
  - このプロパティのサンプルアカウントサービス応答を次に示します。

    ```
    <property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,em
    name="SEND_LDAP_ATTRIBUTES"/>
    ```

  - このプロパティの場合、Citrix Endpoint Managementはコンマ文字を文字列ターミネータとして扱います。したがって、属性値にコンマが含まれる場合は、その前にバックスラッシュを付けます。バックスラッシュは、クライアントが埋め込まれたコンマを属性値の終わりとして解釈するのを防ぎます。バックスラッシュ文字は`"\\"`で表します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **HIDE_THREE_FINGER_TAP_MENU**
  - このプロパティが設定されていないか、**false** に設定されている場合、ユーザーはデバイスで3本指タップを行うことで隠し機能メニューにアクセスできます。隠し機能メニューでは、ユーザーがアプリケーションデータをリセットできました。このプロパティを **true** に設定すると、ユーザーは隠し機能メニューにアクセスできなくなります。
  - このグローバルクライアントポリシーを設定するには、**Settings > Client Properties** に移動し、カスタムキー **HIDE_THREE_FINGER_TAP_MENU** を追加して、**Value** を設定します。
- **TUNNEL_EXCLUDE_DOMAINS**
  - 表示名: トンネル除外ドメイン
  - デフォルトでは、MDXは、モバイルアプリSDKとアプリがさまざまな機能に使用する一部のサービスエンドポイントをマイクロVPNトンネリングから除外します。たとえば、これらのエンドポイントには、Google Analytics、Citrix Cloud™サービス、Active Directory サービスなど、エンタープライズネットワークを介したルーティングを必要としないサービスが含まれます。このクライアントプロパティを使用して、除外されるドメインのリストに追加のドメインを追加します。
  - このグローバルクライアントポリシーを設定するには、**Settings > Client Properties** に移動し、カスタムキー **TUNNEL_EXCLUDE_DOMAINS** を追加して、**Value** を設定します。
  - 値: トンネリングから除外する追加のドメイン。ドメインサフィックスのコンマ区切りリストを入力します。例:

    ```
    app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com
    hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com,features.netscalergatewaystaging.net,features.n
    ```

Citrix Endpoint Management のカスタムクライアントプロパティは次のとおりです。

ENABLE_MAM_NFACTOR_SSO:

- このプロパティを使用すると、NetScaler® Gateway で高度な認証ポリシーを使用しているときに、Secure Hub の MAM 登録またはログイン中に MAM nFactor SSO を有効または無効にできます。値が **true** に設定されている場合、Secure Hub の MAM 登録またはログイン中に MAM nFactor SSO が有効になります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- このプロパティを設定するには、**Settings > Client Properties** に移動し、**Add** をクリックします。**Key** ドロップダウンメニューで **Custom Key** を選択し、必要に応じて以下の情報を更新します。
  - キー - ENABLE_MAM_NFACTOR_SSO
  - 値 - true または false
  - 名前 - ENABLE_MAM_NFACTOR_SSO
  - 説明 - 関連する説明を追加します

MICROSOFT_CERTIFICATE_STRONG_MAPPING:

- このプロパティは、Microsoft 公開キーインフラストラクチャ (PKI) で Secure Mail を使用する際に、セキュリティ識別子 (SID) をサブジェクト代替名 (SAN) に追加することで、既存のクライアント証明書が証明書の強力なマッピング機能をサポートするために更新されるかどうかを制御します。値が **true** に設定されている場合、既存のクライアント証明書は SAN SID を含むように更新されます。
- このプロパティは Microsoft PKI にのみ適用されます。
- このプロパティを設定するには、 **>** に移動し、 をクリックします。 ドロップダウンメニューで を選択し、必要に応じて以下の情報を更新します。
  - キー - MICROSOFT_CERTIFICATE_STRONG_MAPPING
  - 値 - true または false
  - 名前 - MICROSOFT_CERTIFICATE_STRONG_MAPPING
  - 説明 - SAN SID を含むようにクライアント証明書を更新する

aeDeviceCertRenewSupport:

- このプロパティは、エンドユーザーが Citrix Secure Hub アプリからデバイス証明書の健全性ステータスを表示し、証明書の問題を自動的に修正できるかどうかを制御します。値が **true** に設定されている場合、この機能が有効になります。
- このプロパティを設定するには、 **>** に移動し、 をクリックします。 ドロップダウンメニューで を選択し、必要に応じて以下の情報を更新します。
  - キー - aeDeviceCertRenewSupport
  - 値 - true または false
  - 名前 - aeDeviceCertRenewSupport
  - 説明 - デバイス証明書の健全性ステータスと証明書の問題の自動修正を有効にする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザー登録オプション

ユーザーはいくつかの方法でCitrix Endpoint Managementにデバイスを登録できます。詳細を検討する前に、MDM+MAM、MDM、またはMAMのいずれに登録するデバイスを決定してください。これらの管理モードの詳細については、「管理モード」を参照してください。

最も高いレベルでは、4つの登録オプションがあります。

- **登録招待:** 登録招待または招待URLをユーザーに送信します。登録招待およびURLは、Windowsデバイスでは利用できません。
- **セルフヘルプポータル:** ユーザーがCitrix Secure Hubをダウンロードし、登録をリクエストし、デバイス情報を表示できるポータルを設定します。
- **手動登録:** システムが稼働しており、登録できることをユーザーに知らせるメール、ハンドブック、またはその他の連絡を送信します。その後、ユーザーはCitrix Secure Hubをダウンロードし、デバイスを手動で登録します。
- **エンタープライズ:** デバイス登録のもう1つのオプションは、Apple Deployment ProgramとGoogle Android Enterpriseを介することです。これらの各プログラムを通じて、従業員がすぐに使用できる事前構成済みのデバイスを購入できます。詳細については、Apple SupportのApple Deployment Programの記事と、Android Enterprise websiteのGoogle Android Enterpriseドキュメントを参照してください。

登録招待

iOS、macOS、Android Enterprise、およびレガシーAndroidデバイスのユーザーに登録招待をメールで送信できます。登録招待はWindowsデバイスでは利用できません。

また、iOS、macOS、Android Enterprise、Android、またはWindowsデバイスのユーザーにに SMTP経由でインストールリンクを送信することもできます。詳細については、「デバイスの登録」を参照してください。

登録招待方法を使用することを選択した場合、次のことができます。

- **招待URL**、**招待URL + PIN**、または**招待URL + パスワード**の登録セキュリティモードを選択します。
- これらのモードの任意の組み合わせを使用します。
- Citrix Endpoint Managementの**設定**ページからモードを有効または無効にします。

各登録セキュリティモードの詳細については、「登録セキュリティモードの構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

招待は多くの目的に役立ちます。招待の最も一般的な用途は、システムが利用可能であり、ユーザーが登録できることをユーザーに通知することです。招待URLは一意です。ユーザーが招待URLを使用すると、そのURLは利用できなくなります。このプロパティを使用して、システムに登録するユーザーまたはデバイスを制限できます。

登録プロファイルを構成する際、Active Directoryグループに基づいて、特定のユーザーが登録できるデバイスの数を制御できます。たとえば、財務部門にはユーザーあたり1台のデバイスのみを許可することができます。

特定の登録オプションには、追加のコストと落とし穴があることに注意してください。SMTPを使用して招待を送信するには、追加のインフラストラクチャが必要です。このオプションの詳細については、「通知」を参照してください。

また、メールで招待を送信するには、ユーザーがCitrix Secure Hubの外部でメールにアクセスする方法があることを確認してください。MDM登録のActive Directoryパスワードの代替として、ワンタイムパスワード (OTP) 登録セキュリティモードを使用できます。

セルフヘルプポータル

セルフヘルプポータルは、管理者がCitrix Endpoint Managementコンソールにアクセスするのと同じURLでアクセスできます。エンドユーザーは、管理コンソールの代わりにセルフヘルプポータルを表示します。ユーザーは、セルフヘルプポータルでCitrix Secure Hubをダウンロードし、登録を要求し、デバイス情報を表示できます。

ポータルを設定するには、 **>** で以下のサーバープロパティを更新します。

- `shp.console.enable`: セルフヘルプポータルへのアクセスを提供するには、**True** に設定します。
- `enable.new.shp`: ユーザーがセルフヘルプポータルからデバイスを有効にできるようにするには、**True** に設定します。

手動登録

手動登録では、ユーザーはAutoDiscoveryを介して、またはサーバー情報を入力してCitrix Endpoint Managementに接続します。AutoDiscoveryを使用する場合、ユーザーはメールアドレスまたはユーザープリンシパル名形式のActive Directory資格情報のみでログオンします。AutoDiscoveryを使用しない場合、ユーザーはサーバーアドレスとActive Directory資格情報を入力する必要があります。AutoDiscoveryの設定の詳細については、「Citrix Endpoint Management AutoDiscoveryサービスのセットアップ」を参照してください。

手動登録はいくつかの方法で促進できます。ガイドを作成してユーザーに配布し、ユーザー自身で登録させることもできます。IT部門に特定の時間帯にユーザーグループを手動で登録させることも

© 1997–2026 Citrix Systems, Inc. All rights reserved.

できます。ユーザーが資格情報またはサーバー情報を入力する必要がある、同様の任意の方法を使用できます。

ユーザーオンボーディング

環境をセットアップしたら、ユーザーを環境に取り込む方法を決定する必要があります。この記事の前のセクションでは、ユーザー登録セキュリティモードの詳細について説明しました。このセクションでは、ユーザーに連絡する方法について説明します。

オープン登録と選択的招待

ユーザーをオンボーディングする際、次の2つの基本的な方法で登録を許可できます。

- オープン登録。デフォルトでは、LDAP資格情報とCitrix Endpoint Management環境情報を持つすべてのユーザーが登録できます。
- 制限付き登録。招待状を持つユーザーのみが登録できるようにすることで、ユーザー数を制限できます。また、Active Directoryグループによってオープン登録を制限することもできます。

招待方法を使用すると、ユーザーが登録できるデバイスの数を制限することもできます。ほとんどの場合、オープン登録は許容されますが、考慮すべき点がいくつかあります。

- MAM登録の場合、Active Directoryグループメンバーシップを通じてオープン登録を簡単に制限できます。
- MDM登録の場合、Active Directoryグループメンバーシップに基づいて登録できるデバイスの数を制限できます。環境内で企業デバイスのみを許可している場合、通常、その制限は問題になりません。ただし、BYOD環境でデバイスの数を制限したい場合は、この方法を検討することをお勧めします。

選択的招待は、オープン登録よりも手間がかかるため、通常はあまり行われません。ユーザーがデバイスを環境に登録するには、各ユーザーに固有の招待状を送信する必要があります。登録招待状の送信方法については、「登録招待状」を参照してください。

環境に登録したい各ユーザーまたはグループに招待状を送信します。このプロセスは、組織の規模によっては時間がかかる場合があります。Active Directoryグループを使用して招待状を一括作成することも可能ですが、このアプローチは段階的に実行する必要があります。

ユーザーとの最初の連絡

オープン登録と選択的招待のどちらを使用するかを決定し、それらの環境を設定したら、ユーザーに登録オプションについて通知します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

選択的招待方法を使用する場合、電子メールメッセージはそのプロセスの一部です。オープン登録の場合も、Citrix Endpoint Managementコンソールを通じて電子メールを送信できます。詳細については、「登録招待状」を参照してください。

いずれの場合も、電子メールにはSMTPサーバーが必要であることに留意してください。これらのサーバーは、決定を下す際に考慮すべき追加費用となる可能性があります。新しいユーザーが情報にアクセスする方法をどのように期待するかを検討してください。すべてのユーザーがCitrix Endpoint Managementを通じて電子メールにアクセスすることを望む場合、招待電子メールを送信することは問題になる可能性があります。

オープン登録環境の場合、Citrix Endpoint Management以外の別の手段で通信を送信することもできます。そのオプションを選択する場合は、関連するすべての情報を含めるようにしてください。ユーザーにCitrix Secure Hubアプリの入手先と登録に使用する方法を知らせてください。検出をオフにしている場合は、Citrix Endpoint Managementサーバーアドレスもユーザーに提供してください。検出の詳細については、「Citrix Endpoint Management AutoDiscoveryサービスのセットアップ」を参照してください。

アプリのプロビジョニングとプロビジョニング解除

アプリケーションのプロビジョニングは、モバイルアプリのライフサイクル管理を中心に展開されます。Citrix Endpoint Management環境内でのモバイルアプリの準備、構成、配信、および管理です。場合によっては、アプリケーションコードの開発や変更もプロビジョニングプロセスの一部となることがあります。Citrix Endpoint Managementには、アプリのプロビジョニングに使用できるさまざまなツールとプロセスが備わっています。

アプリのプロビジョニングに関するこの記事を読む前に、アプリとユーザーコミュニティを読むことをお勧めします。組織がユーザーに提供するアプリの種類を決定したら、アプリのライフサイクル全体にわたる管理プロセスを概説できます。

アプリのプロビジョニングプロセスを定義する際に、次の点を考慮してください。

- **アプリのプロファイリング:** 組織は限られた数のアプリから始めるかもしれません。しかし、ユーザーの採用率が増加し、環境が拡大するにつれて、管理するアプリの数は急速に増加する可能性があります。アプリのプロビジョニングを管理しやすくするために、事前に特定のアプリプロファイルを定義してください。アプリのプロファイリングは、非技術的な観点からアプリを論理的なグループに分類するのに役立ちます。たとえば、次の要素に基づいてアプリプロファイルを作成できます。
    - バージョン: 追跡用のアプリバージョン

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- インスタンス: さまざまなユーザーセットに展開される多数のインスタンス（たとえば、異なるアクセスレベルを持つもの）
- プラットフォーム: iOS、Android、またはWindows
- ターゲットオーディエンス: 標準ユーザー、部門、Cレベルの役員
- 所有権: アプリを所有する部門
- 種類: MDX、パブリック、WebおよびSaaS、またはWebリンク
- アップグレードサイクル: アプリがアップグレードされる頻度
- ライセンス: ライセンス要件と所有権
- MAM SDKまたはMDXポリシー: モバイルアプリにMDX機能適用するため
- ネットワークアクセス: シングルサインオンでHTTPおよびHTTPSトラフィックをトンネリングするなどのアクセスタイプ（トンネル化 - Web SSO）。

例:

要素	シトリックス セキュアメール	メール	社内	エピック ローバー
バージョン	10.1	10.1	X.x	X.x
インスタンス	VIP	医師	臨床	臨床
プラットフォーム	iOS	iOS	iOS	iOS
ターゲットユーザー	VIPユーザー	医師	臨床ユーザー	臨床ユーザー
所有権	IT	IT	IT	IT
種類	MDX	MDX	ネイティブ	公開
アップグレードサイクル	四半期ごと	四半期ごと	毎年	N/A
ライセンス	N/A	N/A	N/A	ボリューム購入
MDXポリシー	はい	はい	はい	いいえ
ネットワークアクセス	VPN	VPN	VPN	パブリック

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アプリのバージョン管理:** アプリのバージョンを維持および追跡することは、プロビジョニングプロセスにおいて非常に重要です。バージョン管理は通常、ユーザーには透過的です。ユーザーは、新しいバージョンのアプリがダウンロード可能になったときにのみ通知を受け取ります。あなたの視点から見ると、本番環境に影響を与えないように、各アプリのバージョンを非本番環境でレビューおよびテストすることも重要です。

  特定のアップグレードが必要かどうかを評価することも重要です。アプリのアップグレードには通常2つの種類があります。特定のバグの修正などのマイナーアップグレードと、大幅な変更を導入するメジャーリリースです。いずれの場合も、アップグレードが必要かどうかを評価するために、アプリのリリースノートを注意深く確認してください。

- **アプリ開発:** 開発するモバイルアプリにMAM SDKを統合すると、それらのアプリにMDX機能が適用されます。MAM SDKの概要を参照してください。

  MAM SDKは、2023年7月に廃止予定のMDX Toolkitに代わるものです。アプリのラッピングに関する情報については、MDX Toolkitを参照してください。ラップされたアプリのアプリプロビジョニングプロセスは、標準の非ラップアプリのプロビジョニングプロセスとは異なります。

- **アプリのセキュリティ:** プロビジョニングプロセスの一部として、個々のアプリまたはアプリプロファイルのセキュリティ要件を定義します。アプリを展開する前に、セキュリティ要件を特定のMDMまたはMAMポリシーにマッピングできます。この計画により、アプリの展開が簡素化され、高速化されます。例：

  - 特定のアプリを異なる方法で展開する場合があります。
  - Citrix Endpoint Management環境にアーキテクチャ上の変更を加える必要がある場合があります。変更は、アプリが必要とするセキュリティコンプライアンスの種類によって異なります。たとえば、特定のアプリではエンドツーエンドのSSL暗号化やジオフェンシングが必要になる場合があります。

- **アプリの配信:** Citrix Endpoint Managementでは、アプリをMDMアプリまたはMAMアプリとして配信できます。MDMアプリはアプリストアに表示されます。このストアを使用すると、パブリックアプリまたはネイティブアプリをユーザーに便利に配信できます。デバイスレベルの制限を適用する以外に、他のアプリ制御は必要ありません。ただし、MAMを使用してアプリを配信すると、アプリの配信とアプリ自体を完全に制御できます。MAMを介してアプリを配信する方が、通常はより適しています。

- **アプリケーションのメンテナンス:**

  - 初期監査の実施：本番環境に存在するアプリのバージョンと、最後のアップグレードサイクルを追跡します。アップグレードが必要となった特定の機能やバグ修正に注意してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ベースラインの確立：各アプリの最新の安定版リリースのリストを維持します。アップグレード後に予期しない問題が発生した場合に備えて、以前のアプリバージョンにフォールバックできるように準備します。ロールバック計画を策定します。本番環境に展開する前に、テスト環境でアプリのアップグレードをテストします。可能であれば、最初に本番ユーザーの一部にアップグレードを展開し、次に全ユーザーベースに展開します。
- Citrix®ソフトウェア更新通知およびサードパーティソフトウェアベンダー通知の購読：アプリの最新リリースを常に把握しておくことは非常に重要です。早期アクセスリリース（EAR）ビルドは、事前にテストのために利用できる場合があります。
- ユーザーに通知する戦略の考案：アプリのアップグレードが利用可能になったときにユーザーに通知する戦略を定義します。展開前にトレーニングでユーザーを準備します。アプリを更新する前に複数の通知を送信することを検討してください。アプリによっては、最適な通知方法はメール通知またはWebサイトである場合があります。

アプリのライフサイクル管理には、アプリの初期展開から廃止までの完全なライフサイクルが含まれます。アプリのライフサイクルには、次のフェーズがあります。

1. 仕様の要件：ビジネスケースとユーザー要件から始めます。
2. 開発：アプリがビジネスニーズを満たしていることを検証します。
3. テスト：テストユーザー、問題、バグを特定します。
4. 展開：アプリを本番ユーザーに展開します。
5. メンテナンス：アプリのバージョンを更新します。本番環境でアプリを更新する前に、テスト環境でアプリを展開します。

ダッシュボードベースの操作

Citrix Endpoint Managementコンソールのダッシュボードにアクセスすると、情報を一目で確認できます。この情報により、ウィジェットを使用して問題や成功をすばやく把握できます。

ダッシュボードは通常、Citrix Endpoint Managementコンソールに初めてサインオンしたときに表示される画面です。コンソールの他の場所からダッシュボードにアクセスするには、 をクリックします。ダッシュボードで をクリックすると、ページのレイアウトや表示されるウィジェットを編集できます。

- **マイダッシュボード:** 最大4つのダッシュボードを保存できます。これらのダッシュボードは個別に編集でき、保存したダッシュボードを選択してそれぞれを表示できます。
- **レイアウトスタイル:** この行では、ダッシュボードに表示されるウィジェットの数と、ウィジェットのレイアウト方法を選択できます。
- **ウィジェットの選択:** ダッシュボードに表示する情報を選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **通知:** 左側の数字の上にあるチェックボックスをオンにすると、ウィジェットの上に通知バーが追加されます。このバーには、準拠デバイス、非アクティブデバイス、および過去24時間以内にワイプまたは登録されたデバイスの数が表示されます。
- **プラットフォーム別デバイス:** プラットフォームごとの管理対象デバイスと非管理対象デバイスの数を表示します。
- **キャリア別デバイス:** キャリアごとの管理対象デバイスと非管理対象デバイスの数を表示します。各バーをクリックすると、プラットフォーム別の内訳が表示されます。
- **プラットフォーム別管理対象デバイス:** プラットフォームごとの管理対象デバイスの数を表示します。
- **プラットフォーム別非管理対象デバイス:** プラットフォームごとの非管理対象デバイスの数を表示します。このグラフに表示されるデバイスにはエージェントがインストールされている可能性がありますが、権限が取り消されているか、ワイプされています。
- **ActiveSync Gatewayステータス別デバイス:** ActiveSync Gatewayステータス別にグループ化されたデバイスの数を表示します。情報は、ブロック済み、許可済み、または不明のステータスを示します。各バーをクリックすると、プラットフォーム別にデータを内訳表示できます。
- **所有権別デバイス:** 所有権ステータス別にグループ化されたデバイスの数を表示します。情報は、会社所有、従業員所有、または不明な所有権ステータスを示します。
- **失敗したデリバリーグループ展開:** パッケージごとの失敗した展開の合計数を表示します。展開に失敗したパッケージのみが表示されます。
- **ブロック理由別デバイス:** ActiveSyncによってブロックされたデバイスの数を表示します。
- **インストール済みアプリ:** このウィジェットを使用すると、アプリ名を入力でき、そのアプリに関する情報がグラフに表示されます。
- **ボリューム購入アプリのライセンス使用状況:** Appleボリューム購入アプリのライセンス使用状況統計を表示します。

ユースケース

ダッシュボードウィジェットを使用して環境を監視できる多くの方法の例をいくつか示します。

- Citrixモバイル生産性向上アプリを展開しており、モバイル生産性向上アプリがデバイスにインストールできないというサポートチケットを受け取っています。**コンプライアンス違反デバイス**および**インストール済みアプリ**ウィジェットを使用して、Citrixモバイル生産性向上アプリがインストールされていないデバイスを確認します。
- 非アクティブなデバイスを監視して、環境からデバイスを削除し、ライセンスを再利用したいと考えています。**非アクティブデバイス**ウィジェットを使用して、この統計を追跡します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- データが適切に同期されないというサポートチケットを受け取っています。**ActiveSync Gatewayステータス別デバイス**および**ブロック理由別デバイス**ウィジェットを使用して、問題がActiveSync関連であるかどうかを判断することをお勧めします。

レポート

環境がセットアップされ、ユーザーが登録されたら、レポートを実行して展開について学ぶことができます。Citrix Endpoint Managementには、環境で実行されているデバイスの全体像を把握するのに役立つさまざまなレポートが組み込まれています。詳細については、レポートを参照してください。

ロールベースのアクセス制御とCitrix Endpoint Managementのサポート

Citrix Endpoint Managementは、ロールベースのアクセス制御（RBAC）を使用して、Citrix Endpoint Managementコンソール、セルフヘルプポータル、パブリックAPIなどのCitrix Endpoint Managementシステム機能へのユーザーおよびグループのアクセスを制限します。この記事では、Citrix Endpoint Managementに組み込まれているロールについて説明し、RBACを使用するCitrix Endpoint Managementのサポートモデルを決定するための考慮事項を含みます。

組み込みロール

以下の組み込みロールに付与されているアクセスを変更したり、ロールを追加したりできます。各ロールに関連付けられているアクセス権と機能権限の完全なセットおよびそれらのデフォルト設定については、ロールベースのアクセス制御のデフォルトをダウンロードしてください。各機能の定義については、RBACでロールを構成するを参照してください。

管理者ロール

付与されるデフォルトのアクセス権:

- セルフヘルプポータルを除くすべてのシステムアクセス。
- デフォルトでは、管理者は接続の確認やサポートバンドルの作成など、一部のサポートタスクを実行できます。

考慮事項:

- 一部またはすべての管理者がセルフヘルプポータルへのアクセスを必要としますか？その場合、管理者ロールを編集するか、管理者ロールを追加できます。
- 一部の管理者または管理者グループのアクセスをさらに制限するには、管理者テンプレートに基づいてロールを追加し、権限を編集します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザー

付与されるデフォルトのアクセス権:

- 認証されたユーザーが登録リンクを生成できるセルフヘルプポータルへのアクセス。このリンクにより、デバイスを登録したり、登録招待状を自分自身に送信したりできます。
- Citrix Endpoint Managementコンソールへの制限付きアクセス: デバイス機能（ワイプ、デバイスのロック/ロック解除、コンテナのロック/ロック解除、位置情報の表示と地理的制限の設定、デバイスの呼び出し、コンテナパスワードのリセットなど）。登録招待状の追加、削除、送信。

考慮事項:

- ユーザーロールを使用すると、ユーザーが自分で問題を解決できるようになります。
- 共有デバイスをサポートするには、共有デバイス登録用のユーザーロールを作成します。

Citrix Endpoint Managementサポートモデルに関する考慮事項

採用できるサポートモデルは多岐にわたり、レベル1および2のサポートをサードパーティが担当し、レベル3および4のサポートを従業員が担当する場合があります。サポートの負荷をどのように分散するかに関わらず、Citrix Endpoint Managementの展開とユーザーベースに特化した、このセクションの考慮事項を念頭に置いてください。

ユーザーは会社所有のデバイスを使用していますか、それともBYOデバイスを使用していますか？ サポートに影響を与える主な質問は、Citrix Endpoint Management環境でユーザーデバイスを誰が所有しているかということです。ユーザーが会社所有のデバイスを使用している場合、デバイスをロックダウンする方法として、より低いレベルのサポートを提供する可能性があります。その場合、デバイスの問題やデバイスの使用方法についてユーザーを支援するヘルプデスクを提供するかもしれません。サポートする必要があるデバイスの種類に応じて、ヘルプデスクでRBACのデバイスプロビジョニングおよびサポートロールをどのように使用できるかを検討してください。

ユーザーがBYOデバイスを使用している場合、組織はユーザーがデバイスサポートの独自のソースを見つけることを期待するかもしれません。その場合、組織が提供するサポートは、Citrix Endpoint Management固有の問題に焦点を当てた管理的な役割になります。

デスクトップのサポートモデルはどうなっていますか？ デスクトップのサポートモデルが他の会社所有デバイスにも適切であるかどうかを検討してください。同じサポート組織を使用できますか？どのような追加トレーニングが必要になる可能性がありますか？

ユーザーにCitrix Endpoint Managementセルフヘルプポータルへのアクセスを許可しますか？ ― 部の組織はユーザーにCitrix Endpoint Managementへのアクセスを許可しないことを好みますが、ユーザーにセルフサポート機能を提供することで、サポート組織の負担を軽減できます。RBACの

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デフォルトのユーザーロールに付与したくない権限が含まれている場合は、含めたい権限のみを持つロールを作成することを検討してください。要件を満たすために必要な数のロールを作成できます。

Citrixサポートプロセス

Citrix製品に関する問題の解決には、Citrixテクニカルサポートサービスをご利用いただけます。このグループは、回避策と解決策を提供し、開発チームと協力してソリューションを提供します。

Citrix ConsultingSM ServicesまたはCitrix Education Servicesは、製品トレーニング、製品の使用方法に関するアドバイス、構成、インストール、または環境の設計とアーキテクチャに関するサポートを提供します。

Citrix Consultingは、以下のCitrix製品関連プロジェクトを支援します。

- 概念実証
- 経済的影響評価
- インフラストラクチャのヘルスチェック
- 設計要件分析
- アーキテクチャ設計の検証
- 統合
- 運用プロセス開発

Citrix EducationSMは、Citrixの仮想化、クラウド、およびネットワークテクノロジーに関する最高レベルのITトレーニングと認定を提供します。

Citrixでは、サポートケースを作成する前に、Citrixのセルフヘルプリソースと推奨事項を最大限に活用することをお勧めします。たとえば、Citrixの技術専門家が執筆した記事や速報にアクセスしたり、Citrixソリューションとテクノロジーの製品ドキュメントを参照したり、Citrixの役員、製品チーム、技術専門家からの直接的な意見を読んだりできる場所がいくつかあります。それぞれ、Knowledge Center、Product documentation、Blogsのページを参照してください。

よりインタラクティブな支援が必要な場合は、ディスカッションフォーラムに参加して質問し、他の顧客から実際の回答を得たり、ユーザーグループや関心のあるグループ内でアイデア、意見、技術情報、ベストプラクティスを共有したり、Citrixサポートのソーシャルネットワーキングサイトを監視しているCitrixサポートエンジニアと交流したりできます。それぞれ、Support ForumsおよびCitrix Communityのページを参照してください。

スキルを向上させるためのトレーニングコースや認定コースも利用できます。Citrix Educationを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Insight Servicesは、Citrix環境向けのシンプルでオンラインのトラブルシューティングプラットフォームとヘルスチェッカーを提供します。Citrix Endpoint Management、Citrix Virtual Apps and Desktops、Citrix Hypervisor、およびNetScaler Gatewayで利用可能です。分析ツールを参照してください。

テクニカルサポートを求めるには、電話またはWeb経由でサポートケースを作成できます。Webは低および中程度の重大度の問題に、電話オプションは高重大度の問題に使用できます。Citrix Endpoint Managementの問題に関するサポートに連絡するには、Citrixサポートサービスを参照してください。

Citrixソリューションの提供において豊富な経験を持つ、高度な訓練を受けた単一の連絡窓口を求める場合、Citrix Servicesはテクニカルリレーションシップマネージャーを提供します。Citrixサービス製品と利点の詳細については、Citrix Worldwide Servicesを参照してください。

Citrix Endpoint Management でグループ登録招待を送信する

Citrix Endpoint Management では、グループおよびネストされたグループに登録招待を送信できます。登録招待は Windows デバイスでは利用できません。

グループ招待を設定する際、1つ以上のデバイスプラットフォームを指定できます。また、デバイスにタグを付けて、例えば会社所有のデバイスと従業員所有のデバイスを区別することもできます。その後、ユーザーデバイスの認証タイプを設定します。

注:

カスタム通知テンプレートを使用する予定がある場合は、登録セキュリティモードを構成する前にテンプレートを設定する必要があります。通知テンプレートの詳細については、「通知テンプレートの作成と更新」を参照してください。

ユーザーアカウント、役割、登録セキュリティモード、および招待に関する基本的な構成の詳細については、「ユーザーアカウント、役割、および登録」を参照してください。

一般的な手順

1. Citrix Endpoint Management コンソールで、 > の順に移動します。
2. 画面左上の をクリックし、次に をクリックします。
3. メニューから をクリックします。

   この手順では、1つ以上のプラットフォームを選択できます。会社内で異なるオペレーティングシステムプラットフォームが混在している場合は、すべてのプラットフォームを選択しま

© 1997–2026 Citrix Systems, Inc. All rights reserved.

す。特定のプラットフォームを使用しているユーザーがいないと確信できる場合にのみ、プラットフォームの選択を解除してください。

4. 招待プロセス中にデバイスにタグを付けることができます。 または を選択します。

   タグ付けにより、会社所有のデバイスと従業員所有のデバイスを簡単に区別できます。

5. リストで、グループが存在するドメインを選択します。
6. リストで、招待を送信する Active Directory グループを選択します。
7. 「**登録モード**」では、ユーザーが希望する登録セキュリティの種類を設定できます。

   - ユーザー名 + パスワード
   - 高セキュリティ
   - 招待URL
   - 招待URL + PIN
   - 招待URL + パスワード
   - 2要素認証
   - ユーザー名 + PIN

   注:

   「**高セキュリティ**」登録セキュリティモードは非推奨になりました。登録招待を送信するには、「**招待URL**」、「**招待URL + PIN**」、または「**招待URL + パスワード**」の登録セキュリティモードのみを使用できます。「**ユーザー名 + パスワード**」、「**2要素認証**」、または「**ユーザー名 + PIN**」で登録するデバイスの場合、ユーザーはCitrix Secure Hubをダウンロードし、手動で資格情報を入力する必要があります。

8. 「**エージェントダウンロード**」、「**登録URL**」、「**登録PIN**」、および「**登録確認**」テンプレートについては、以前に作成したカスタム通知テンプレートを選択します。または、表示されているデフォルトを選択します。

   これらの通知テンプレートには、Citrix Endpoint Management内で構成したSMTPサーバー設定を使用します。続行する前に、まずSMTP情報を設定してください。

   注:

   「**有効期限**」と「**最大試行回数**」のオプションは、選択した「**登録モード**」オプションに基づいて変更されます。これらのオプションは変更できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. 「**招待を送信**」で「オン」を選択し、「**保存して送信**」をクリックしてプロセスを完了します。

ネストされたグループのサポート

ネストされたグループを使用して招待状を送信できます。通常、ネストされたグループは、同様の権限を持つグループが互いにバインドされている大規模な環境で使用されます。

設定 > LDAP に移動し、**ネストされたグループのサポート**オプションを有効にします。

トラブルシューティングと既知の制限事項

問題: Active Directoryグループから削除されたにもかかわらず、ユーザーに招待状が送信されています。

解決策: Active Directory環境の規模によっては、変更がすべてのサーバーに伝播するまでに最大6時間かかる場合があります。ユーザーまたはネストされたグループが最近削除された場合でも、Citrix Endpoint Managementはそれらのユーザーをまだグループの一部と見なす可能性があります。

したがって、ユーザーに別のグループ招待状を送信する前に、最大6時間待つのが最善です。

Citrix Secure Mailプッシュ通知用のEWSによる証明書ベース認証の構成

Citrix Secure Mailプッシュ通知を機能させるには、以下を実行する必要があります。

- 証明書ベース認証用にExchange Serverを構成します。この要件は、Citrix Secure Hubが証明書ベース認証でCitrix Endpoint Managementに登録されている場合に特に必要です。
- ExchangeメールサーバーバーAction上のActive SyncおよびExchange Web Services (EWS) 仮想ディレクトリを証明書ベース認証で構成します。

これらの構成を完了しないと、Citrix Secure Mailプッシュ通知のサブスクリプションが失敗し、Citrix Secure Mailでバッジの更新が行われません。

この記事では、証明書ベース認証を構成する手順について説明します。これらの構成は、特にExchange Server上のEWS仮想ディレクトリに対して行われます。

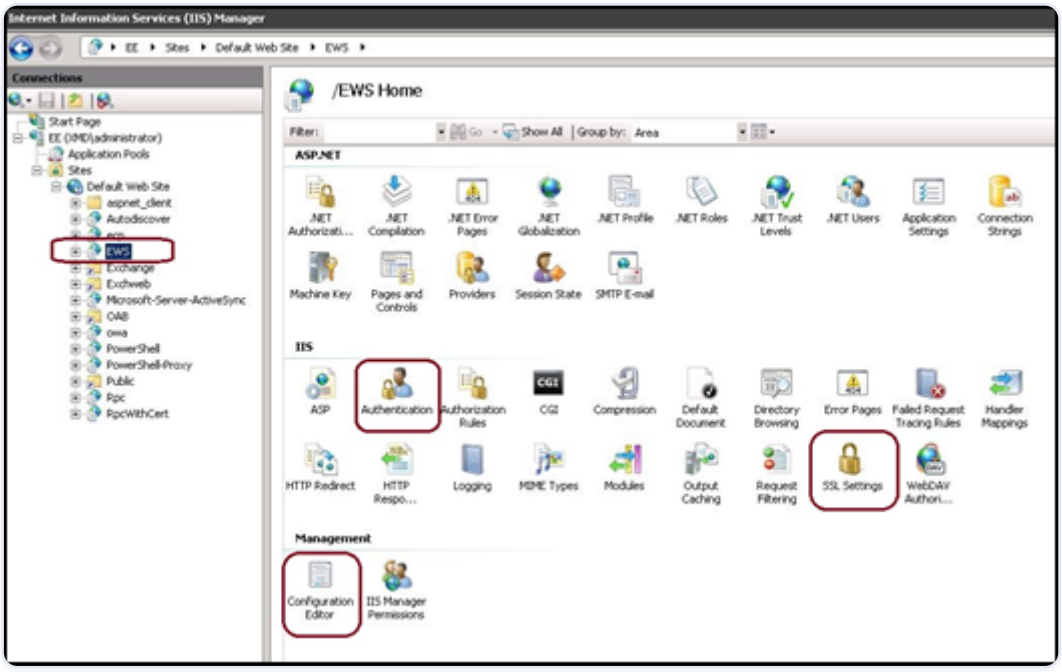
構成を開始するには、以下を実行します。

1. EWS仮想ディレクトリがインストールされているサーバーにログオンします。
2. IISマネージャーコンソールを開きます。

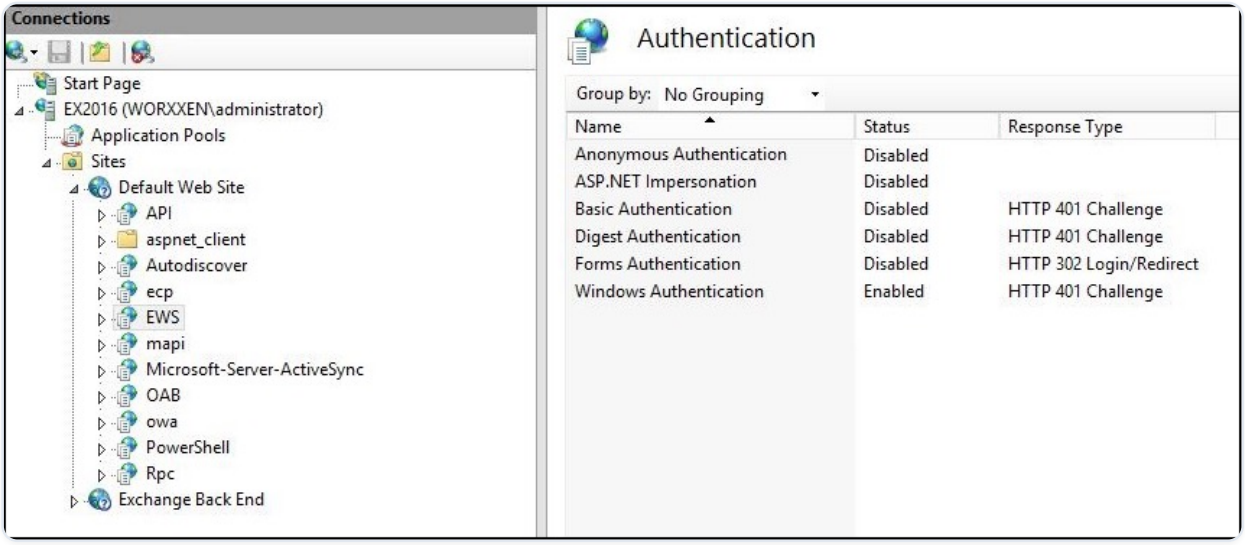
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Default Web Site**の下で、EWS仮想ディレクトリをクリックします。

   認証、SSL、構成エディターのスナップインは、IISマネージャーコンソールの右側にあります。



4. EWSの**認証**設定が次の図に示すように構成されていることを確認します。

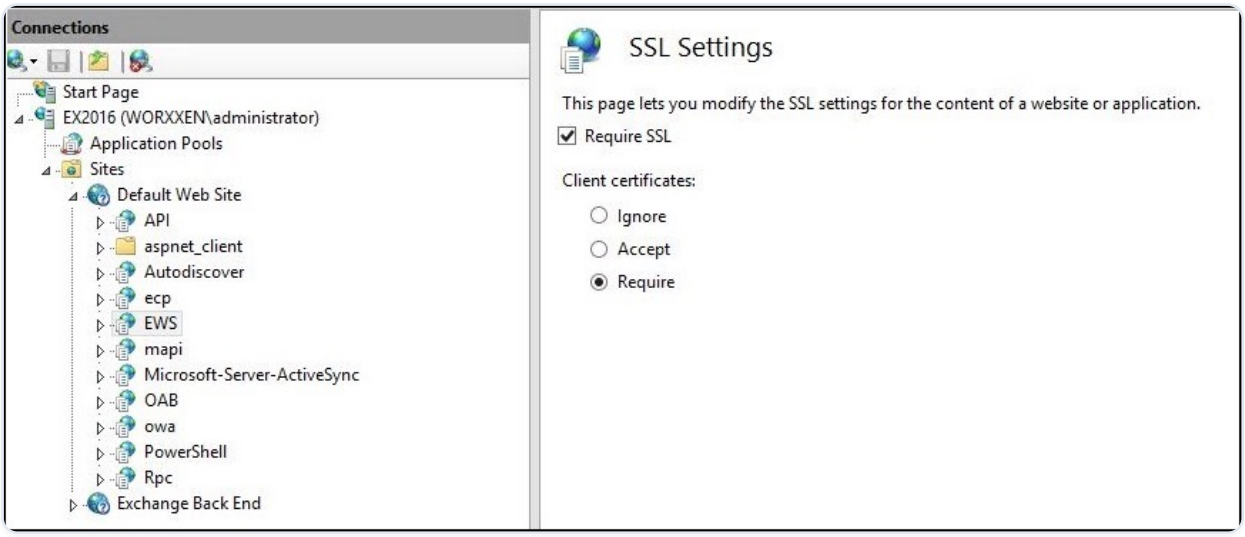


5. EWS仮想ディレクトリの**SSL設定**を構成します。

   a. 「**Require SSL**」チェックボックスを選択します。

   b. **Client Certificates**の下で、**Require**をクリックします。または、他のEWSメールクライアントがユーザー名とパスワードを使用してExchange Serverに認証する場合、**Accept**をクリックします。

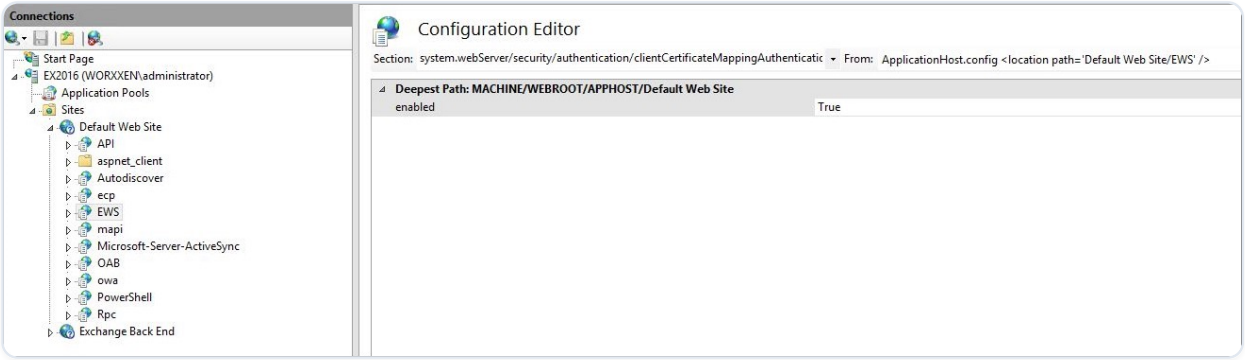
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. **Configuration Editor**をクリックします。**Section**ドロップダウンリストで、次のセクションに移動します。

   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. **enabled**の値を**True**に設定します。



8. **Configuration Editor**をクリックします。**Section**ドロップダウンリストで、次のセクションに移動します。

   - **system.webServer/serverRuntime**

9. **uploadReadAheadSize**の値を**10485760** (10 MB) または**20971520** (20 MB)、または組織の要件に応じて設定します。

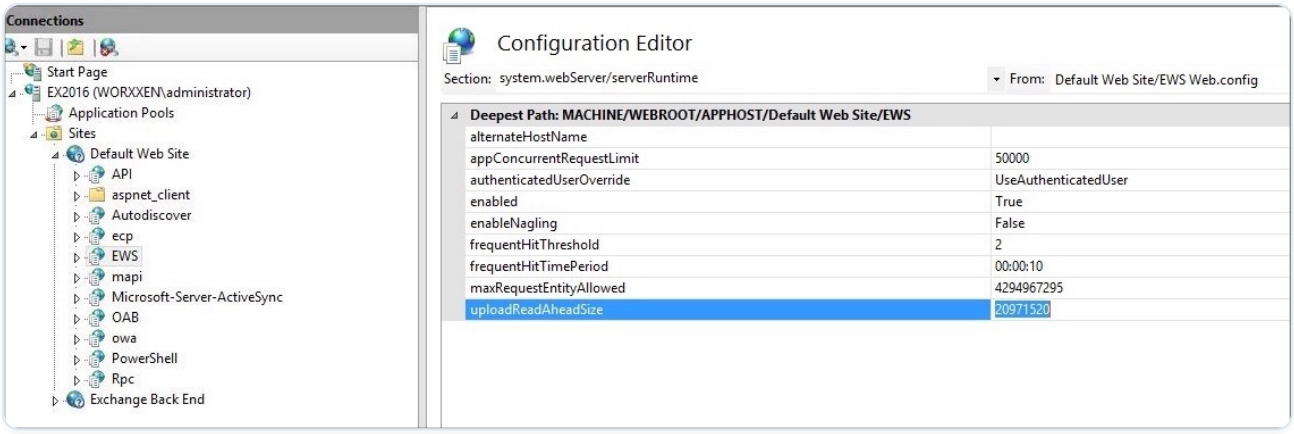
   重要:

   この値を正しく設定しないと、EWSプッシュ通知の購読中に証明書ベースの認証がエラーコード413で失敗する可能性があります。

   この値を**0**に設定しないでください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

詳細については、Microsoftの記事「Microsoft IIS server runtime」を参照してください。



iOSプッシュ通知に関するCitrix Secure Mailの問題のトラブルシューティングの詳細については、このCitrixサポート技術情報センターの記事を参照してください。

関連情報

iOS版Citrix Secure Mailのプッシュ通知

オンプレミスのデバイス正常性構成証明サーバーの構成

オンプレミスのWindowsサーバーを介して、Windows 10およびWindows 11モバイルデバイス向けにデバイス正常性構成証明 (DHA) を有効にできます。DHAをオンプレミスで有効にするには、まずDHAサーバーを構成します。

DHAサーバーを構成した後、オンプレミスのDHAサービスを有効にするCitrix Endpoint Managementポリシーを作成します。詳しくは、「デバイス正常性構成証明デバイスポリシー」を参照してください。

DHAサーバーの前提条件

- Desktop Experienceインストールオプションを使用してインストールされた、Windows Server Technical Preview 5以降を実行しているサーバー。
- 1台以上のWindows 10およびWindows 11クライアントデバイス。これらのデバイスは、最新バージョンのWindowsを実行しているTPM 1.2または2.0を搭載している必要があります。
- 次の証明書：
    - **DHA SSL証明書：** エクスポート可能な秘密キーを持つ、エンタープライズ信頼済みルートにチェーンするx.509 SSL証明書。この証明書は、DHAデータ通信を転送中に保護します。これには以下が含まれます。
        - サーバー間（DHAサービスとMDMサーバー）の通信

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - サーバーとクライアント間（DHAサービスとWindows 10またはWindows 11デバイス）の通信

  - **DHA署名証明書：** エクスポート可能な秘密キーを持つ、エンタープライズ信頼済みルートにチェーンするx.509証明書。DHAサービスはこの証明書をデジタル署名に使用します。
  - **DHA暗号化証明書：** エクスポート可能な秘密キーを持つ、エンタープライズ信頼済みルートにチェーンするx.509証明書。DHAサービスはこの証明書を暗号化にも使用します。

- 次の証明書検証モードのいずれかを選択します。

  - **EKCert：** EKCert検証モードは、インターネットに接続されていない組織内のデバイス向けに最適化されています。EKCert検証モードで実行されているDHAサービスに接続するデバイスは、インターネットに直接アクセスできません。
  - **AIKCert：** AIKCert検証モードは、インターネットにアクセスできる運用環境向けに最適化されています。AIKCert検証モードで実行されているDHAサービスに接続するデバイスは、インターネットに直接アクセスでき、MicrosoftからAIK証明書を取得できる必要があります。

WindowsサーバーにDHAサーバーの役割を追加する

1. Windowsサーバーで、サーバーマネージャーがまだ開いていない場合は、**「スタート」をクリックし、次に**「サーバーマネージャー」**をクリックします。
2. **「役割と機能の追加」**をクリックします。
3. **「開始する前に」ページで、**「次へ」**をクリックします。
4. **「インストールの種類の選択」ページで、**「役割ベースまたは機能ベースのインストール」**をクリックし、次に**「次へ」**をクリックします。
5. **「対象サーバーの選択」ページで、**「サーバープールからサーバーを選択」**をクリックし、サーバーを選択して、**「次へ」**をクリックします。
6. **「サーバーの役割の選択」ページで、**「デバイス正常性構成証明」**チェックボックスをオンにします。
7. オプション：**「機能の追加」**をクリックして、その他の必要な役割サービスと機能をインストールします。
8. **「次へ」**をクリックします。
9. **「機能の選択」ページで、**「次へ」**をクリックします。
10. **「Webサーバーの役割 (IIS)」ページで、**「次へ」**をクリックします。
11. **「役割サービスの選択」ページで、**「次へ」**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. **「デバイス正常性構成証明サービス」**ページで、**「次へ」**をクリックします。
13. **「インストール選択の確認」**ページで、**「インストール」**をクリックします。
14. インストールが完了したら、**「閉じる」**をクリックします。

サーバーの証明書ストアにSSL証明書を追加します

1. SSL証明書ファイルに移動して選択します。
2. ストアの場所として、**現在のユーザー**を選択し、**次へ**をクリックします。

   Windows サーバーマネージャー(/en-us/citrix-endpoint-management/media/configuredha-addcert1.png)
3. 秘密キーのパスワードを入力します。
4. インポートオプションの**すべての拡張プロパティを含める**が選択されていることを確認します。**次へ**をクリックします。

   Windows サーバーマネージャー(/en-us/citrix-endpoint-management/media/configuredha-addcert2.png)
5. このウィンドウが表示されたら、**はい**をクリックします。

   Windows サーバーマネージャー(/en-us/citrix-endpoint-management/media/configuredha-addcert3.png)
6. 証明書がインストールされていることを確認します。

   a. コマンドプロンプトウィンドウを開きます。
   b. `mmc`と入力し、**Enter**キーを押します。ローカルコンピューターのストアで証明書を表示するには、管理者ロールである必要があります。
   c. ファイルメニューで、**スナップインの追加と削除**をクリックします。
   d. **追加**をクリックします。
   e. スタンドアロンスナップインの追加ダイアログボックスで、**証明書**を選択します。
   f. **「追加」**をクリックします。
   g. 「証明書スナップイン」ダイアログボックスで、**「マイユーザーアカウント」**を選択します。(サービスアカウントホルダーとしてサインインしている場合は、**「サービスアカウント」**を選択します。)
   h. 「コンピューターの選択」ダイアログボックスで、**「完了」**をクリックします。

      Windows サーバーマネージャー(/en-us/citrix-endpoint-management/media/configuredha-thumbprint5.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. **サーバーマネージャー > IIS** に移動し、アイコンのリストから「**サーバー証明書**」を選択します。

   Windows サーバーマネージャー(/en-us/citrix-endpoint-management/media/configuredha-addcert5.png)

8. 「操作」メニューから「**インポート...**」を選択して、SSL証明書をインポートします。

   Windows サーバーマネージャー(/en-us/citrix-endpoint-management/media/configuredha-addcert6.png)

証明書のサムプリントを取得して保存する

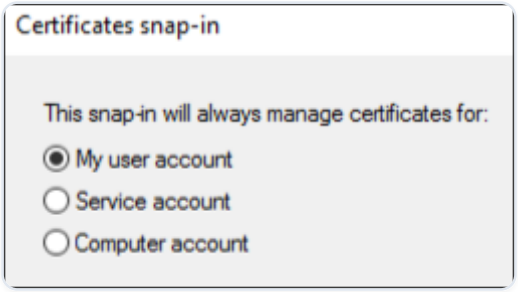
1. ファイルエクスプローラーの検索バーに「`mmc`」と入力します。
2. 「コンソールルート」ウィンドウで、「**ファイル > スナップインの追加と削除**」をクリックします。

   Windowsファイルエクスプローラー (/en-us/citrix-endpoint-management/media/configuredha-thumbprint1.png)

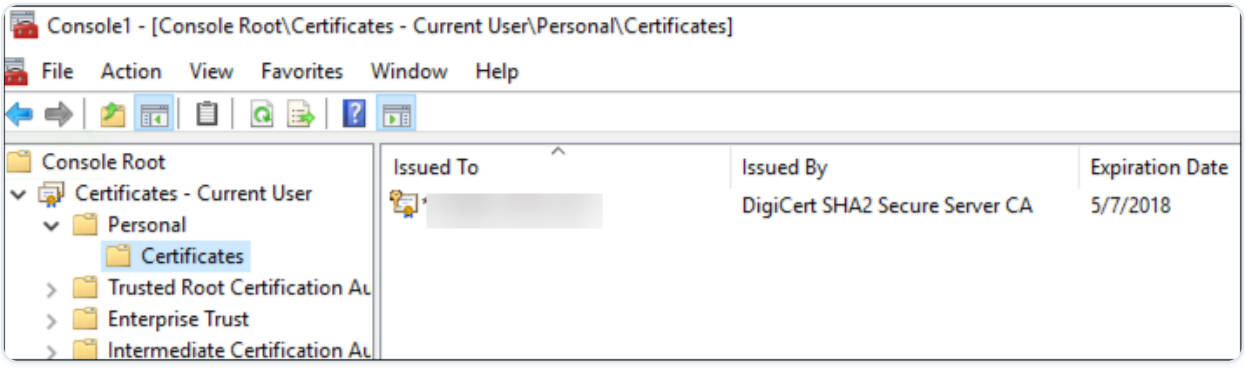
3. 利用可能なスナップインから証明書を選択し、選択したスナップインに追加します。

   Windows スナップインの追加と削除 (/en-us/citrix-endpoint-management/media/configuredha-thumbprint2.png)

4. 「**マイユーザーアカウント**」を選択します。

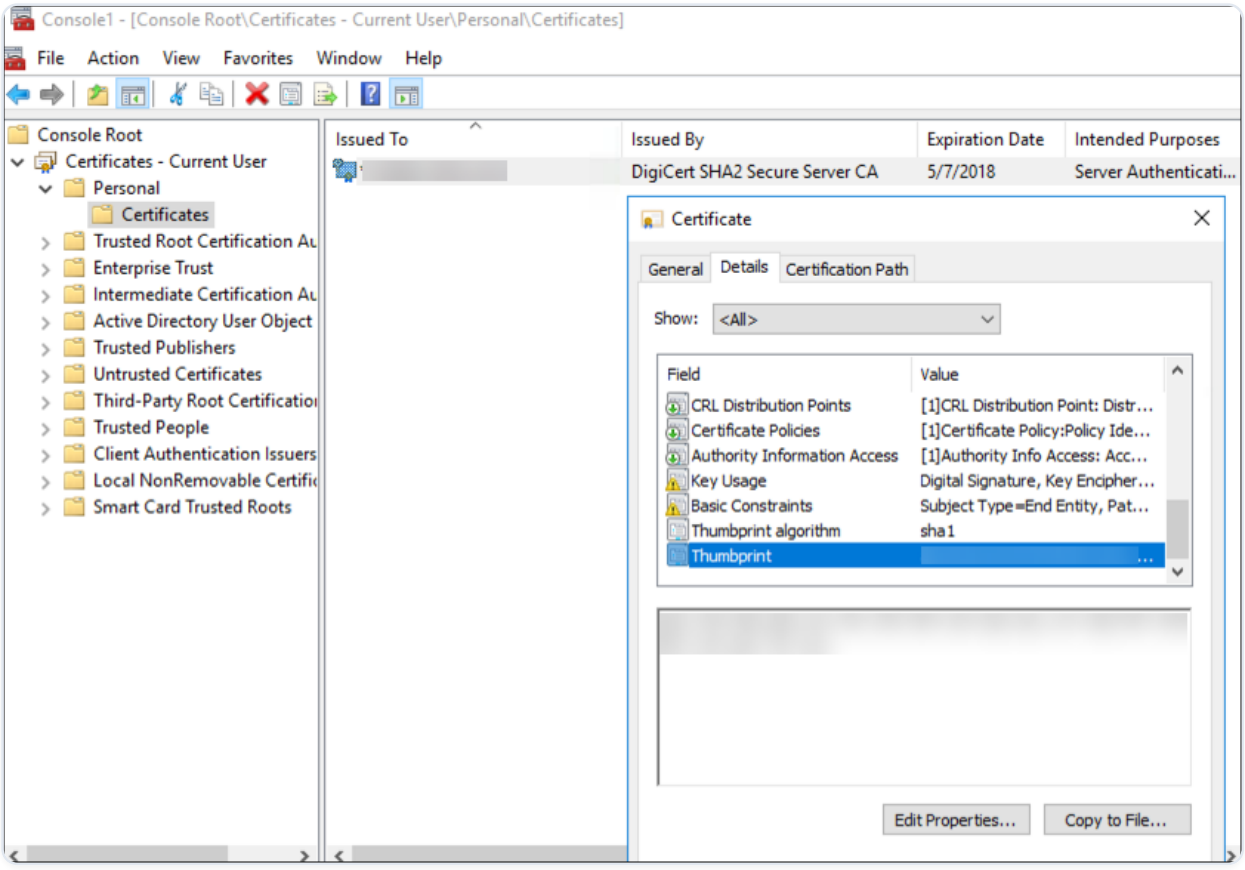


5. 証明書を選択し、**OK**をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. 証明書をダブルクリックし、**詳細**タブを選択します。スクロールして証明書のサムプリントを確認します。



7. サムプリントをファイルにコピーします。PowerShellコマンドでサムプリントを使用する際は、スペースを削除してください。

署名証明書と暗号化証明書をインストールする

署名証明書と暗号化証明書をインストールするには、Windowsサーバーでこれらの PowerShellコマンドを実行します。

プレースホルダー ReplaceWithThumbprint を、示されているように二重引用符で囲んで置き換えます。

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.Thumbprint
-like "ReplaceWithThumbprint"}



$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" +
$keyname icacls $keypath /grant IIS_IUSRS`:R
```

TPMルート証明書を抽出し、信頼された証明書パッケージをインストールする

Windowsサーバーで次のコマンドを実行します。

```
mkdir .\TrustedTpm



expand -F:\* .\TrustedTpm.cab .\TrustedTpm



cd .\TrustedTpm



.\setup.cmd
```

DHAサービスを構成する

DHAサービスを構成するには、Windowsサーバーでこのコマンドを実行します。

プレースホルダー ReplaceWithThumbprint を置き換えます。

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
ReplaceWithThumbprint



-SigningCertificateThumbprint ReplaceWithThumbprint



-SslCertificateStoreName My -SslCertificateThumbprint
ReplaceWithThumbprint
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-SupportedAuthenticationSchema "AikCertificate"
```

DHAサービスの証明書チェーンポリシーを設定するには、Windowsサーバーで次のコマンドを実行します。

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

これらのプロンプトに次のように応答します。

```
  Confirm

    Are you sure you want to perform this action?

    Performing the operation "Install-DeviceHealthAttestation" on target
"[Machine Name]".

    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): A

    Adding SSL binding to website 'Default Web Site'.

    Add SSL binding?
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

    Add application pool?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding web application 'DeviceHealthAttestation' to website 'Default
Web Site'.

    Add web application?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding firewall rule 'Device Health Attestation Service' to allow
inbound connections on port(s) '443'.

    Add firewall rule?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    Setting initial configuration for Device Health Attestation Service.


    Set initial configuration?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Registering User Access Logging.


    Register User Access Logging?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

構成を確認する

DHASActiveSigningCertificate がアクティブであるかどうかを確認するには、サーバーでこのコマンドを実行します。

`Get-DHASActiveSigningCertificate`

証明書がアクティブな場合、証明書の種類 (署名) とサムプリントが表示されます。

DHASActiveSigningCertificate がアクティブであるかどうかを確認するには、サーバーでこれらのコマンドを実行します。

プレースホルダー ReplaceWithThumbprint を置き換え、示されているように二重引用符で囲みます。

```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
-Force
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-DHASActiveEncryptionCertificate
```

証明書がアクティブな場合、サムプリントが表示されます。

最終確認を行うには、次の URL にアクセスします。

`https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate/v1`

DHA サービスが実行されている場合、「Method not allowed」と表示されます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

index

- エンタープライズハブデバイスポリシー
- マップデバイスポリシー

エンタープライズハブデバイスポリシー

Windows Phoneのエンタープライズハブデバイスポリシーでは、エンタープライズハブの業務用ストアを通じてアプリを配布できます。

このポリシーを作成するには以下が必要です。

- DigiCertからのAET（`.aetx`）署名証明書
- Microsoftのアプリ署名ツール（XapSignTool.exe）を使用して署名されたCitrix Company Hubアプリ

注：

Endpoint Managementでは、Windows Phone Secure Hubの1つのモードについて、1つのエンタープライズハブポリシーだけがサポートされています。たとえば、Windows Phone Secure Hub for Endpoint Managementをアップロードする場合、複数のエンタープライズハブポリシーをさまざまなバージョンのSecure Hub用に作成しないでください。デバイスの登録中に最初のエンタープライズハブポリシーを展開するだけです。

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］** の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows Phoneの設定

- **`.aetx`ファイルのアップロード：** **［参照］** をクリックして`.aetx`ファイルの場所に移動し、そのファイルを選択します。
- **署名済みエンタープライズハブアプリをアップロード：** **［参照］** をクリックしてエンタープライズハブアプリの場所へ移動し、そのアプリを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

マップデバイスポリシー

Windows 10の電話デバイスでは、オフラインマップがサポートされています。［マップ］デバイスポリシーを使用して、デバイスにダウンロードするマップを指定します。Microsoft Maps構成サービスプロバイダー（CSP）では、ドイツ、英国、および米国のマップのみがサポートされています。

このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］** の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows Phoneの設定

マップを追加するには、**［追加］** をクリックし、**国** と **州** を選択します。これらの手順を繰り返して、さらにマップを追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Managementドキュメント履歴

次の表に、Citrix Endpoint Management製品のドキュメントに対する重要な変更点を示します。 これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

日付	変更	説明
05 May 2025	Citrix Endpoint Management 25.5.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 25.5.0」を参照してください。
26 Feb 2025	Citrix Endpoint Management 25.3.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 25.3.0」を参照してください。
13 Jan 2025	Citrix Endpoint Management 25.1.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 25.1.0」を参照してください。
21 Nov 2024	Citrix Endpoint Management 24.10.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 24.10.0」を参照してください。
09 Aug 2024	Citrix Endpoint Management 24.8.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 24.8.0」を参照してください。
03 Jun 2024	Citrix Endpoint Management 24.6.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
		Endpoint Management 24.6.0」を参照してください。
16 Apr 2024	Citrix Endpoint Management 24.4.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 24.4.0」を参照してください。
07 Feb 2024	Citrix Endpoint Management 24.1.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 24.1.0」を参照してください。
06 Dec 2023	Citrix Endpoint Management 23.12.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 23.12.0」を参照してください。
04 Dec 2023	Citrix Endpoint Management 23.9.0リリースのロールバック	詳しくは、「Citrix Endpoint Management 23.9.0」を参照してください。
11 Oct 2023	Citrix Endpoint Management 23.9.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 23.9.0」を参照してください。
22 Sep 2023	Citrix Endpoint Management Governmentに関連したリファレンスを削除しました	Citrix Endpoint Managementのサポートは廃止されました。
22 Aug 2023	ChromeOSおよびtvOSに関連した記事およびリファレンスは削除されました	ChromeOSおよびtvOSのサポートは廃止されました。
28 Jul 2023	Citrix Endpoint Management 23.7.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 23.7.0」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
20 Jul 2023	ビジネス向けMicrosoft Storeに関連する記事と参照を削除しました	ビジネス向けMicrosoft Storeのサポートは廃止されました。 Microsoftは、このプラットフォームをサポートしなくなりました。 詳しくは、Microsoftのドキュメントを参照してください。
14 Jun 2023	Citrix Endpoint Management 23.6.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 23.6.0」を参照してください。
08 May 2023	Citrix Endpoint Management 23.4.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 23.4.0」を参照してください。
13 Mar 2023	Citrix Endpoint Management 23.2.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 23.2.0」を参照してください。
23 Jan 2023	Citrix Endpoint Management 23.1.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 23.1.0」を参照してください。
13 Dec 2022	Citrix Endpoint Management 22.12.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 22.12.0」を参照してください。
01 Nov 2022	Citrix Endpoint Management 22.10.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 22.10.0」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
14 Sep 2022	Citrix Endpoint Management 22.9.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 22.9.0」を参照してください。
11 Aug 2022	Citrix Endpoint Management 22.7.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 22.7.0」を参照してください。
06 Jun 2022	Citrix Endpoint Management 22.6.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 22.6.0」を参照してください。
02 May 2022	Citrix Endpoint Management 22.5.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 22.5.0」を参照してください。
28 Mar 2022	Citrix Endpoint Management 22.4.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 22.4.0」を参照してください。
01 Mar 2022	Citrix Endpoint Management 22.3.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 22.3.0」を参照してください。
07 Feb 2022	Citrix Endpoint Management 22.2.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 22.2.0」を参照してください。
06 Jan 2022	Citrix Endpoint Management 22.1.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 22.1.0」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
30 Nov 2021	Citrix Endpoint Management 21.12.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.12.0」を参照してください。
05 Nov 2021	Citrix Endpoint Management 21.11.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.11.0」を参照してください。
22 Oct 2021	Citrix Endpoint Management 21.10.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.10.1」を参照してください。
21 Oct 2021	Windows 10デバイスでの［Wi-Fiセンサーホットスポットへの自動接続の許可］に関する制限の廃止を発表	詳しくは、「廃止」とMicrosoft社のドキュメントを参照してください。
05 Oct 2021	Citrix Endpoint Management 21.10.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.10.0」を参照してください。
24 Sep 2021	Cloud Connectorを使用しないIDプロバイダー認証の公開プレビューを発表	この機能について詳しくは、「IDプロバイダー認証」を参照してください。
15 Sep 2021	Citrix Endpoint Management 21.9.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.9.1」を参照してください。
06 Sep 2021	Citrix Endpoint Management 21.9.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
		Endpoint Management 21.9.0」を参照してください。
18 Aug 2021	Citrix Endpoint Management 21.8.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.8.0」を参照してください。
22 Jul 2021	Citrix Endpoint Management 21.7.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.7.1」を参照してください。
09 Jul 2021	Self Help Portalで高セキュリティ登録モードと登録招待の設定の廃止を発表しました	詳しくは、「廃止」を参照してください。
06 Jul 2021	Citrix Endpoint Management 21.7.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.7.0」を参照してください。
23 Jun 2021	Android for Workspaceプラットフォームは、パブリックプレビューとして利用できます。 Android for Workspaceを構成すると、ユーザーはCitrix Workspaceアプリを使用してCitrix Endpoint Managementに登録できます。	詳しくは、「Android for Workspace」を参照してください。
14 Jun 2021	Citrix Endpoint Management 21.6.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.6.0」を参照してください。
24 May 2021	Citrix Endpoint Management 21.5.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.5.1」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
11 May 2021	MDX共有デバイスのサポートを廃止する日付の更新	詳しくは、「廃止」を参照してください。
06 May 2021	Citrix Endpoint Management 21.5.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.5.0」を参照してください。
03 May 2021	既知の問題CXM-89333のドキュメント追加	詳しくは、「Citrix Endpoint Management 21.4.0の既知の問題」を参照してください。
26 Apr 2021	セキュリティの検索操作の説明を更新しました	「セキュリティ操作」を参照してください。
22 Apr 2021	操作の例を追加しました	「自動化された操作」を参照してください。
21 Apr 2021	デバイスのIMEIまたはシリアル番号を使用した招待URL生成の廃止の発表	詳しくは、「廃止」を参照してください。
20 Apr 2021	Azure AD条件付きアクセスとの統合の追加	詳しくは、「Azure ADの条件付きアクセス（プレビュー）と統合します」を参照してください。
15 Apr 2021	共有iPadに関する記事の追加	「共有iPad」を参照してください。
13 Apr 2021	Citrix Endpoint Management 21.4.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.4.0」を参照してください。
31 Mar 2021	Per-App VPNの要件に関する説明を追加	「VPNデバイスポリシー」および「管理対象の構成デバイスポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
09 Mar 2021	Citrix Endpoint Management 21.3.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.3.0」を参照してください。
09 Mar 2021	AutoDiscoveryサービスレコードの移行に関する情報の追加	「AutoDiscoveryサービスレコードの移行」を参照してください。
24 Feb 2021	エンドポイントをiOS 14.5にアップグレードする前に必要な準備に関する情報の追加	「エンドポイントのiOS 14.5へのアップグレード準備」を参照してください。
12 Feb 2021	Citrix Endpoint Management 21.2.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.2.0」を参照してください。
25 Jan 2021	Citrix Endpoint Management 21.1.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.1.1」を参照してください。
06 Jan 2021	Citrix Endpoint Management 21.1.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 21.1.0」を参照してください。
09 Dec 2020	IDプラットフォームとしてAzure Active DirectoryとOktaを使用したAndroid Enterpriseデバイスの登録に関するプレビューコンテンツの追加	変更について詳しくは、「Citrix Endpoint Management 20.12.0」を参照してください。
04 Dec 2020	Citrix Endpoint Management 20.12.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.12.0」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
10 Nov 2020	Citrix Endpoint Managementが実行できるさまざまな接続チェックの表を追加	「接続チェックの詳細」を参照してください。
06 Nov 2020	Citrix Endpoint Management 20.11.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.11.0」を参照してください。
28 Oct 2020	最新バージョンのCitrix ADCにアップグレードする場合に必要な回避策を追加	「オンプレミスのCitrix ADCを13.0-64.35+にアップグレードする前に」を参照してください。
23 Oct 2020	Citrix Endpoint Management 20.10.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.10.1」を参照してください。
22 Oct 2020	Android Enterpriseセットアップの概要レベルのワークフローを追加	「Android Enterpriseの使用開始」を参照してください。
22 Oct 2020	Android Enterpriseアプリを配布するためのさまざまな方法を詳しく説明した記事を追加	「Android EnterpriseアプリとAndroid for Workspaceアプリの配布」を参照してください。
07 Oct 2020	Citrix Endpoint Management 20.10.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.10.0」を参照してください。
22 Sep 2020	Citrix Endpoint Management 20.9.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.9.1」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
04 Sep 2020	Citrix Endpoint Management 20.9.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.9.0」を参照してください。
20 Aug 2020	Citrix Endpoint Management 20.8.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.8.0」を参照してください。
14 Aug 2020	追加設定のないWindowsデバイス一括登録プロセスの簡素化に関する説明を追加	「デバイスを追加設定なしで一括登録」を参照してください。
31 Jul 2020	Windowsデバイスの一括登録に関する記事を更新	「Windowsデバイスの一括登録」を参照してください。
23 Jul 2020	Citrix Endpoint Management 20.7.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.7.1」を参照してください。
10 Jul 2020	Citrix Endpoint Management 20.7.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.7.0」を参照してください。
02 Jul 2020	MDX暗号化の廃止予定のタイムラインとアクションプランを追加	「今後の変更に備えてAndroidデバイスを準備する」を参照してください。
25 Jun 2020	Citrix Endpoint Management 20.6.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.6.0」を参照してください。
19 Jun 2020	ドキュメントの「ブラックリスト」と「ホワイトリスト」という用語に対処。「禁止リスト」と「許可リスト」に変更。	Citrix Endpoint Management コンソールには、現在、「ブラックリスト」、「ホワイトリスト」という用語が含まれています。ドキュメントを更

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
		新しました。 今後のリリースの製品コンソールでこれらの用語を変更していきます。
18 Jun 2020	Samsung SEAMSコンテナの廃止を発表	「廃止」を参照してください。
09 Jun 2020	Citrix Cloud ConnectorがCitrix Endpoint Managementで使用するためにサポートする、フォレストおよびドメインの機能レベルの表を追加。	「サポートされるActive Directoryの機能レベル」を参照してください。
05 Jun 2020	AndroidおよびiOSデバイスの登録についてCitrix Cloud Connectorの負荷テスト結果を提供する記事を追加	「Cloud Connectorのスケールおよびサイズの考慮事項」を参照してください。
02 Jun 2020	Citrix Endpoint Management 20.5.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.5.0」を参照してください。
27 May 2020	Intune管理対象アプリの公開に関するコンテンツを増補。サードパーティアプリのラップに関連するコンテンツを削除。	「Citrix Endpoint ManagementとMicrosoft Endpoint Managerとの統合」を参照してください。
13 May 2020	Citrix Endpoint Managementのユーザーの役割と権限に関する情報を増補	「RBAC機能の使用」を参照してください。
05 May 2020	Citrix Endpoint Management 20.4.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.4.1」を参照してください。
04 May 2020	iOS、iPadOS、およびmacOSの信頼できる証明書	「証明書」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
	の新しいTLS証明書要件に関する注を追加	
30 Apr 2020	認証にAzure Active Directoryを使用することに関するプレビューコンテンツを追加	「Citrix Cloudを介したAzure Active Directoryでの認証」を参照してください。
29 Apr 2020	Citrix Endpoint ManagementでのOkta資格情報を使用した認証のサポートに関するプレビュードキュメントを追加	「Citrix Cloudを介したOktaでの認証」を参照してください。
13 Apr 2020	Citrix Endpoint Management 20.4.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.4.0」を参照してください。
26 Mar 2020	Citrix Endpoint Management 20.3.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.3.0」を参照してください。
20 Mar 2020	異なる種類のiOSアプリを配布する手順の詳細に関する記事を追加	「Appleアプリの配布」を参照してください。
13 Mar 2020	高度なサイバー攻撃に対するエンタープライズモバイルデバイスの保護に関するセクションを追加	「Mobile Threat Defenseソフトウェアとの統合」を参照してください。
13 Feb 2020	Citrix Endpoint Management 20.2.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.2.1」を参照してください。
08 Jan 2020	Citrix Endpoint Management 20.1.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 20.1.0」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
03 Dec 2019	Citrix Endpoint Management 19.12.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.12.0」を参照してください。
08 Nov 2019	Citrix Endpoint Management 19.11.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.11.0」を参照してください。
16 Oct 2019	Citrix Endpoint Management 19.10.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.10.0」を参照してください。
16 Oct 2019	Android EnterpriseへのGoogle移行に関するセクションを追加	「登録プロファイルの作成」を参照してください。
25 Sep 2019	Citrix Endpoint Management 19.9.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.9.1」を参照してください。
10 Sep 2019	Citrix Endpoint Management 19.9.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.9.0」を参照してください。
08 Aug 2019	Citrix Endpoint Management 19.8.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.8.0」を参照してください。
07 Aug 2019	Android Enterpriseの概念を明確にするために、Android Enterpriseの記事を更新しました。 Android Enterpriseへ	「Android Enterprise」および「Device AdministrationからAndroid Enterpriseへの移行」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
	の移行に関する記事に、移行に関連した推奨事項を追加	
31 Jul 2019	従来のAndroidデバイス管理からAndroid Enterpriseへの移行に関する記事を追加しました	「Device AdministrationからAndroid Enterpriseへの移行」を参照してください。
16 Jul 2019	Citrix Endpoint Management 19.7.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.7.1」を参照してください。
27 Jun 2019	Citrix Endpoint Management 19.6.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.6.1」を参照してください。
06 Jun 2019	Citrix Endpoint Management 19.6.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.6.0」を参照してください。
24 May 2019	現在のGoogle Android Enterpriseのドキュメントと一致するように、Android Enterpriseの用語を更新しました。	「Android Enterprise」の記事を更新しました。
20 May 2019	iOSおよびAndroidデバイスからネイティブSaaSアプリへのモバイルSSOのサポートに関する新しいセクション	「アプリの追加」の記事に、モバイルSSOの構成方法に関するセクションを追加しました。
20 May 2019	Citrix GatewayサービスとCitrix Endpoint Managementとの統合に関する新しいセクション	Citrix Gatewayサービスのプレビューは、Citrix Gatewayサービスのサブスクリプション対象者で、ワークスペースを有効にしているお客様が利用できます。 「Citrix Endpoint Managementで使用するCitrix Gatewayの構成」

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
		記事に「オンボードとリソースのセットアップ」のセクションを追加しました。
10 May 2019	Entrust PKIに関する新しいセクション	「PKIエンティティ」の記事にEntrust PKIに関するセクションを追加しました。
09 May 2019	Citrix Endpoint Management 19.5.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.5.0」を参照してください。
01 May 2019	Android Enterprise用にVPNを構成する方法に関する新しいセクション：Citrix SSOアプリの管理対象構成デバイスポリシーを作成する	「管理対象の構成ポリシー」の記事にセクション：「Android Enterpriseに対するVPNプロファイルの構成」を追加しました。
17 Apr 2019	Citrix Endpoint Management 19.4.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.4.1」を参照してください。
04 Apr 2019	ゼロタッチ構成に関する新しいセクション	「ゼロタッチ登録」の記事に「Android Enterprise」のセクションを追加しました。
02 Apr 2019	Gatewayコネクタ：Exchange ActiveSync用8.5.3リリースの記事の更新	新機能および変更された機能の概要については、「バージョン8.5.3の新機能」を参照してください。
02 Apr 2019	Citrix Endpoint Management 19.3.1リリースで新しく解決された問題	詳しくは、「Citrix Endpoint Management 19.3.1」で解決された問題を参照してください。
26 Mar 2019	アップグレード手順が追加され更新されたFCMセクション	FCMについて詳しくは、「Firebase Cloud Messaging」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日付	変更	説明
26 Mar 2019	Citrix Secure Hubストア名の構文を更新	「アプリストアおよびCitrix Secure Hubのブランド設定」でストア名の英数字の要件に関する注意が追加されました。
11 Mar 2019	Citrix Endpoint Management 19.3.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.3.0」を参照してください。
22 Feb 2019	Citrix Endpoint Management 19.2.1リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.2.1」を参照してください。
11 Feb 2019	Citrix Endpoint Management 19.2.0リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.2.0」を参照してください。
25 Jan 2019	Citrix Endpoint Management 19.1.2リリースの記事の更新	新機能および変更された機能の概要については、「Citrix Endpoint Management 19.1.2」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.