Citrix セキュアプライベートアクセス™

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

Contents

Secure Private Access サービス ソリューションの概要 25
アダプティブセキュリティ 25
アプリケーションアクセス 26
シングルサインオン 26
ブラウザセキュリティ 26
デバイスポスチャ 26
TCPおよびUDPアプリケーションのサポート 27
使用例 27
参照記事 27
参考ビデオ 28
関連製品の新機能 28
新機能 29
30 September 2026 29
03 September 2026 29
19 August 2026 30
05 August 2026 30
31 July 2026 31
24 June 2026 31
18 June 2026 32
09 June 2026 32
重要なお知らせ 32
20 May 2026 33
28 April 2026 33
07 April 2026 34
04 March 2026 34
12 February 2026 34

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

05 February 2026 34
18 December 2025 35
16 December 2025 35
11 December 2025 36
30 October 2025 36
17 September 2025 37
13 August 2025 37
14 July 2025 38
03 June 2025 39
15 May 2025 39
24 April 2025 39
22 April 2025 40
20 February 2025 41
08 January 2025 41
07 January 2025 41
02 January 2025 42
03 December 2024 43
25 November 2024 43
14 November 2024 43
08 November 2024 43
07 November 2024 44
23 September 2024 44
15 August 2024 44
16 July 2024 45
11 June 2024 45
13 March 2024 46
12 February 2024 46
23 January 2024 46

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

20 December 2023 46
16 October 2023 46
11 September 2023 47
30 August 2023 47
28 August 2023 47
22 August 2023 48
17 August 2023 48
07 June 2023 48
29 May 2023 48
10 April 2023 49
29 March 2023 49
07 March 2023 49
23 January 2023 49
22 December 2022 50
03 October 2022 50
09 September 2022 51
01 June 2022 52
04 April 2022 52
16 February 2022 55
11 October 2021 55
30 July 2021 56
09 June 2021 56
22 May 2021 56
01 May 2021 57
15 March 2021 57
11 November 2020 57
15 October 2020 58
08 October 2020 58

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

24 September 2020 58
07 July 2020 58
19 June 2020 59
08 May 2020 59
V2019.04.02 59
V2019.04.01 59
V2019.03.01 60
グーグル クローム エンタープライズ プレミアム との統合 61
ソリューションの概要 61
Chrome Enterprise Premiumの高度なセキュリティ機能 62
Chrome Enterprise向けCitrix Secure Accessコントロール 62
統合を成功させるための前提条件 63
Citrix Secure Private Access - サポートされている展開モード 63
法的情報 64
関連トピック 64
統合ソリューションの前提条件 65
ライセンス、アプリのバージョン、および拡張機能 65
Google 管理コンソール 66
セキュア プライベート アクセス サービス 66
グーグル クローム 67
ユーザーの管理 67
必須 - ユーザーのメールアドレスフィールドに入力する 67
必須 - ユーザーグループのメールアドレスフィールドに入力する 68
メールアドレスの欠落または不整合に関するドメインマッピングの考慮事項 68
Citrix Secure Private Accessで構成されたユーザーディレクトリをGoogle Cloudユーザーディレクトリと関連付ける 69
アクティブディレクトリ 69
マイクロソフト Entra ID 69

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

オクタ 70

グーグル クラウド アイデンティティ（グーグル ディレクトリ） 70

TLS検査のバイパス 71

管理者の役割と権限 71

Googleカスタム管理者ロールの権限 72

ロールと権限の作成と割り当て 74

エグレスハブリージョンの構成 74

SaaSアプリケーションのエグレスリージョンパネル 75

リージョンの選択 77

リージョンの選択解除 77

メールアドレスを持たないユーザーグループのドメインマッピング 79

ドメインマッピングの仕組み 79

メールアドレスの構成 82

制限事項 82

管理プロファイルID 83

ユーザー属性タイプを設定する 83

Open ID Connect と Citrix Identity およびアクセス管理 84

概要 84

前提条件 85

OIDC統合の概要 86

Google OIDC SSOプロファイルの作成 87

Citrix OIDCクライアントを作成する 89

OIDC SSOプロファイルの割り当て 90

Citrix OIDCクライアントの更新 91

OIDCクライアントを削除する 92

エンドユーザーエクスペリエンス 92

クローム エンタープライズ プレミアム 用 シトリックス セキュア アクセス 拡張機能 95

Secure Access 拡張機能ログ 95

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

Chrome Enterprise 用 Citrix Secure Access コントロール 95
サポートされているコントロール 98
ポリシー内のユーザーとグループ 99
ユーザーまたはグループを検索 99
同期されたユーザーとグループを使用する 100
キーロギング対策制御 100
前提条件 101
キーロギング対策ポリシーの構成 101
クリップボードコンテナ制御 101
前提条件 102
クリップボードコンテナ制御を有効にする 102
クリップボード共有スコープを有効にする 103
ウェブアプリケーションのドメインサフィックス 105
前提条件 105
DNSサフィックスの構成 105
セッション記録の制御 106
アーキテクチャ 106
前提条件 107
システム要件 107
環境をセットアップする 108
ブラウザセッションの再認証制御 109
前提条件 109
ブラウザセッションの再認証制御を有効にする 110
SSH制御 110
この統合の利点 111
ユースケース 111
システム要件 112
前提条件 112

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

SSHアクセス用にSecure Private Accessを構成する 112
SSHポリシーを構成する 113
リモートデスクトップ制御 113
この統合の利点 114
ユースケース 114
システム要件 115
前提条件 115
RDPアクセス用にSecure Private Accessを構成する 115
リモートデスクトップポリシーを構成する 116
CEP 統合の問題のトラブルシューティング 116
CEP トラブルシューティングのための診断ログ 117
ユーザーが正しいChromeプロファイルにログインしていることを確認します 118
Secure Enterprise Browser拡張機能がインストールされているか確認する 118
ExtensionInstallForcelistポリシーを確認する 118
競合する拡張機能インストールリストポリシーのトラブルシューティング 119
Secure Enterprise Browser拡張機能ポリシーの確認 119
Google 管理コンソール内のユーザー拡張機能構成を確認する 121
ルートがフェッチされているか確認する 122
Secure Private Access管理コンソールでCEP統合を検証する 123
Google Secure Gatewayの到達可能性のトラブルシューティング 123
ルートへのアプリケーションの組み込みを確認する 124
ルーティングされたアプリケーションアクセスのトラブルシューティング 124
IdPとGoogleディレクトリの整合性を確保する 126
Google 管理コンソールでグループのアクセス設定を確認する 126
CEP統合における既知の問題 126
Secure Private Access ユーザーインターフェイス 126
適応型アクセス ポリシー構成 127
Google Chrome ブラウザ 127

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

オープンIDコネクト (OIDC) 128

Citrix Secure Private Access の利用を開始する 129

システム要件 129

仕組み 129

Citrix Secure Private Accessサービスの使用を開始する 130

Secure Private Accessサービス展開モデル 131

Citrix Secure Private Access™ サービス向けPoP (Points of Presence) ロケーション 132

セキュアプライベートアクセス管理 PoPs 132

セキュアプライベートアクセス データPoP 133

Secure Private Access のオンボーディングとセットアップ 134

Secure Private Access にユーザーをオンボーディングする 134

Citrix StoreFront CloudでストアURLを構成する 136

Google Chrome統合のセットアップ 136

SaaS アプリの IP アドレスを追加する 139

プリンシパルアクセス境界ポリシーの構成 139

オンボーディング後のGoogle統合詳細の更新 140

Googleディレクトリ組織部門のCEPを構成する 141

既知の検証の失敗と警告 144

複数のユーザーグループでのプロビジョニング失敗の問題 147

次のステップ 147

データの地域化 148

サポートされる展開 149

構成 149

制限事項 149

アプリケーションの構成と管理 150

エンタープライズWebアプリを構成する 150

システム要件 151

仕組み 151

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

Webアプリを構成する 151
アプリケーション削除時のルーティングエントリの自動クリーンアップ 162
SaaSアプリを構成する 163
Secure Private AccessサービスでSaaSアプリがサポートされる仕組み 163
SaaSアプリを構成する 164
Google Secure Gateway経由のルーティング 173
アプリケーション削除時のルーティングエントリの自動クリーンアップ 173
SaaS アプリサーバー固有の構成 174
エンドツーエンドのアプリ構成 189
エンタープライズWebアプリへのエージェントレスアクセス 189
仕組み 190
エンタープライズWebアプリへのエージェントレスアクセス用にCitrix Secure Private Accessを構成する 190
アプリケーション削除時のルーティングエントリの自動クリーンアップ 203
エージェントレスアクセスアプリとDevice Postureサービス 203
準拠デバイスのみにエージェントレスアクセスを有効にする手順 203
エンドユーザーエクスペリエンス 207
TCP/UDPアプリのサポート 207
前提条件 207
TCP/UDPアプリのSecure Private Accessを構成する 208
管理者設定 – Citrix Secure Access クライアントベースのHTTP/HTTPSアプリへのアクセス 213
前提条件 213
注意事項 214
TCP/UDPおよびHTTP(S)アプリへのアダプティブアクセス 214
アダプティブアクセスポリシーを作成するには 214
ログインおよびログアウトスクリプト構成レジストリ 215
アプリケーションドメインのIPアドレスの競合のトラブルシューティング 215
注意点 217

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

Windowsログオン前のAlways On 218
Always Onはどのように機能しますか? 219
Active DirectoryおよびMicrosoft Entra IDハイブリッドAD構成 219
セキュア プライベート アクセス の構成 221
コネクタアプライアンスの構成 223
Windowsログオン後にAlways Onを構成する（マシン/ユーザー トンネル） 227
制限事項 227
参照 228
TCPおよびUDPサーバー用の予約済みCIDRアドレス 228
予約済みCIDR IPアドレスを構成する 228
FQDNをIPアドレスに解決するためのDNSサフィックス 229
前提条件 230
DNSサフィックスの追加方法 230
ユースケースの例 231
HARファイルを使用して関連ドメインを検出する 233
例 234
前提条件 234
HARファイルをインポートする 235
関連ドメインの管理 235
検証とファイルの要件 236
ルーティング例外を使用したポートベースルーティング - プレビュー 236
ポートベースルーティングのユースケース 237
ポートベースルーティングを示す例 243
Secure Private Access コンソールで証明書を管理する 244
マシン認証証明書を管理する 245
証明書を追加する 245
証明書を無効にする 246
証明書を削除する 246

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

証明書の優先順位を設定する 246
SSL証明書を管理する 246
証明書を追加 246
証明書を検索 247
証明書の変更 247
証明書の削除 248
外部通知 248
Citrix Secure Access™ クライアント 248
Windows 用 Citrix Secure Access クライアント 248
macOS 用 Citrix Secure Access クライアント 248
iOS 用 Citrix Secure Access クライアント 248
Android 用 Citrix Secure Access クライアント 249
Linux 用 Citrix Secure Access クライアント 249
WebおよびSaaSアプリケーション構成のベストプラクティス 249
Secure Private Accessにおける公開済みおよび未公開アプリのアプリケーションアクセス 249
アクセスポリシーの一致と優先順位付け 250
アプリ構成のベストプラクティス 252
IdP ドメインは独自のアプリケーションを持つ必要があります 252
同じ関連ドメインを複数のアプリケーションの一部にすることはできません 254
ディープリンクURL 257
アプリへのアクセスに関するエンドユーザーエクスペリエンスの説明 257
Citrix Secure Access クライアントを介して Web アプリにアクセスする 258
Citrix Secure Access クライアントを介して TCP/UDP アプリにアクセスする 258
Secure Private Access 向けコネクタアプライアンス 259
コネクタアプライアンスを使用したセキュアプライベートアクセスの構成 260
Kerberos構成の検証 266
スケールとサイズに関する考慮事項 267
WebおよびSaaSアプリケーション 267

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

TCPアプリケーション 268
混合トラフィック (Web、SaaS、TCP) 268
コネクタ通知 268
適応型アクセス ポリシーの構成と管理 269
仕組み 269
複数のルールを持つアクセス ポリシーを作成する 270
前提条件 270
ユーザーまたはグループを検索 275
ユーザーとグループの同期を確認する 275
ポリシー作成後の留意事項 276
デバイスに基づく適応型アクセス 277
ロケーションに基づくアダプティブアクセス 277
デバイスポスチャに基づくアダプティブアクセス 279
セッションポリシー 280
ルーティングの優先順位 281
サポートされているCitrix Secure Access™クライアント 281
使用例 281
セッションポリシーを使用して企業ネットワーク内で直接ルーティングを構成する 282
シトリックス エンタープライズ ブラウザ から クローム エンタープライズ プレミアム への移行286
Chrome Enterprise Premium の構成方法 286
メールアドレスのないユーザーグループのポリシーエンリッチメント 287
CEP 互換性分析のためのSecure Private Access構成パーサー 287
ツールの使用方法 288
CEPへの完全移行前の構成変更 292
シングルサインオン構成の変更 293
アクセスポリシーとセッションポリシーの更新 293
アプリケーション全体でのアクションの標準化 293
ポリシー更新のアプリケーション要件 294

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

Webフィルタリングポリシーの更新（オプション） 294
その他のポリシー調整（オプション） 294
セキュリティグループのクリーンアップ（オプション） 295
CEPを組織に展開（完全移行） 295
移行プロセスの概要 296
メールエンリッチメントプロセスの課題 296
ベストプラクティス 297
まとめ 297
高度なSecure Private Access機能 298
Secure Private Accessサービスのためのハイブリッドデータパス 299
ハイブリッドデータパスを使用する主な利点 300
ハイブリッドデータパスの仕組み 300
サポートされているクライアント 301
サポートされているNetScaler Gatewayビルド 301
接続要件 302
送信接続用の許可URLリスト 302
Secure Private Accessアプリケーションのハイブリッドデータパスを設定する 302
接続を確立するためにゲートウェイに接続する 302
NetScaler GatewayをCitrix Cloudに登録する 304
オンプレミスのNetScaler Gatewayを介したデータトラフィックのルーティングを有効にする 305
制限事項 307
Secure Private Access登録スクリプトの問題 307
ネットワーク内のアプリケーション、ドメイン、またはIPアドレスを検出する 309
新しい環境での内部ドメインのアプリケーション検出 310
アプリ検出ページからアプリケーションを作成する 312
既存のアプリケーションを更新する 313
選択したすべての埋め込みドメインを表示 314

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

既知の制限事項 315

コンテキストベースのアプリルーティングとリソースロケーションの選択 315

ユースケース: コンテキストベースのルーティング 316

ユースケース: ユーザーコンテキストに基づくリソースロケーションの選択 317

ルーティングタイプまたはリソースロケーションを変更する手順 318

ユースケース：社内ユーザーをバックエンドアプリケーションに直接ルーティングする 320

Monitor でのコンテキストルーティングのインサイト 320

ローカルLANリソースへのシームレスなアクセス (プリンター、ファイルサーバー) 322

重要な考慮事項 323

ローカルLANアクセス機能を有効にする 323

ポリシーモデリングツール 324

ポリシーモデリングツールにアクセスする 324

ユーザーまたはマシンのセットのポリシーを分析する 325

特定の宛先に対するポリシーを分析する 325

アクセスポリシーの詳細を確認する 326

アプリケーションインポートツール - プレビュー 328

インポートの仕組み 328

CSVファイルの準備 329

CSV ファイルに入力する値 332

CSVベースのツールを使用してアプリケーションを移行する手順 335

CSVファイル使用時のアプリケーションのインポートまたは作成の失敗 338

参照 339

クライアント内部IPアドレスプール - プレビュー 339

クライアント内部IPアドレスプールのユースケース 339

IPアドレスプールの制限事項 340

イントラネットIPアドレスプールを作成する 341

IPアドレスプールを削除する 342

IPアドレス使用状況データを表示する 343

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

一貫した接続を維持する 344
コネクタースティッキネス 345
クライアントIPアドレスのスティッキネス - プレビュー 346
前提条件 347
TCP/UDPアプリケーションのクライアントIPアドレスの固定を有効にする 347
アクティブなセッションを終了し、ユーザー/マシンをブロックリストに追加する 348
ユースケース 349
Chrome Enterprise Premiumを使用している場合のユーザーブロックの前提条件 350
ユーザー/マシンをブロックリストに追加する 350
ユーザー/マシンがブロックリストに追加された後のエンドユーザーエクスペリエンス 352
クラウド経由でアクセスされるアプリケーション 352
オンプレミスNetScaler® Gateway経由でアクセスされるアプリケーション（ハイブリッドデータパス） 352
ユーザーセッションのタイムアウト 352
Webアプリサーバーのタイムアウト 353
Citrix Secure Accessクライアントのタイムアウト 353
構成レポート 354
構成レポートを生成する 354
ADFS と Secure Private Access の統合 355
ADFSにクレームプロバイダートラストを追加する 355
クレームプロバイダー信頼ID 359
リライングパーティ識別子 360
IdP開始フローでリレーステートを有効にする 361
ADFSサーバーでRelayStateパラメーターを有効にするには 362
Citrix Secure Private Accessでのアプリ構成 362
IdP開始フロー 362
SP開始フロー 364
Citrix セキュア プライベート アクセス Terraform プロバイダー 365

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

主な利点 365
ユースケース 366
システム要件 366
前提条件 366
権限 367
インストール 367
Terraformの構成 367
問題のトラブルシューティング 368
制限事項 368
重要な考慮事項 369
参照 369
可視性と監視 370
監視 370
Secure Private Access 使用状況ダッシュボード 370
Secure Private Access アプリケーションおよびセッションの監視 370
Connector Appliance のヘルス監視 371
Secure Private Access 使用状況ダッシュボード 371
診断ログ 372
コネクターステータス 374
起動回数別上位アプリケーション 374
アプリケーション起動回数別上位ユーザー 375
適用別上位アクセスポリシー 376
上位検出アプリケーション 376
チャートからアプリを作成する 377
検索演算子 379
セキュアプライベートアクセス アプリケーション、セッション、およびトレンド 380
アプリケーション、セッション、およびトレンド 380
健全性監視 381

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

コネクタアプライアンス 381
セッションとアプリケーションの傾向 382
セッションとアプリケーションの傾向 382
セッション監視 382
アプリケーションの傾向 383
トリアージとトラブルシューティング 384
アプリ関連の問題のトラブルシューティング 384
DaaS Monitor の Secure Private Access セッションコード 384
Monitor でのセッション関連の問題のトラブルシューティング 384
デバイスポスチャー関連の問題のトラブルシューティング 384
認証関連の問題のトラブルシューティング 385
ログを使用したトラブルシューティング 385
セキュア プライベート アクセス ログ 385
デバイス ポスチャ ログ 385
Monitor を使用したリアルタイムセッションのトラブルシューティング 386
診断ログのエラーコード 386
認証サービスがダウンしているため、アプリの起動に失敗しました 393
アプリケーションのFQDN長が超過したため、アプリの起動に失敗しました 393
バックエンドWebアプリに接続できないため、Webアプリの起動に失敗しました 393
ユーザーの詳細が見つかりません 394
SAMLトークン準備中にユーザー属性が見つからなかったため、Web/SaaSアプリの起動に失敗しました 394
アプリケーションFQDNを識別できなかったため、Web/SaaSアプリの起動に失敗しました 394
SAMLサービスプロバイダーから提供された無効なAppIdにより、Web/SaaSアプリの起動に失敗しました 395
無効なアプリアクセス要求のため、Web/SaaSアプリの起動に失敗しました 395
内部エラーのため、ポリシー評価中にアプリの起動に失敗しました 395

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

ポリシー評価応答の解析中にアプリの起動に失敗しました 395
ポリシー評価中に無効な結果でアプリの起動に失敗しました 396
無効なリソースロケーション構成によりアプリの起動に失敗しました 396
アプリケーション名の長さが長すぎるため、アプリの起動に失敗しました 397
無効なアプリIDのため、プライベートTCPサーバーへの接続確立中にアプリの起動に失敗しました 397
ポリシー評価中にアプリの起動が拒否されました 397
宛先FQDNが長すぎるため、アプリの起動に失敗しました 398
無効な宛先IPのため、アプリの起動に失敗しました 398
Connector Applianceから応答がなかったため、アプリの起動に失敗しました 398
無効なIP/ホスト名またはポートへのリクエストにより、アプリケーションの起動に失敗しました 398
宛先サーバーが接続を拒否したため、アプリケーションの起動に失敗しました 398
宛先が見つからなかったため、アプリケーションの起動に失敗しました 398
宛先ネットワークに到達できなかったため、アプリケーションの起動に失敗しました 398
宛先に接続できなかったため、アプリケーションの起動に失敗しました 399
コネクタからSecure Private Accessサービスへの接続に失敗しました 399
コネクタがプロキシの詳細の読み取りに失敗しました 400
設定されたプロキシに到達できません 400
Connector ApplianceがFR (エッジノード) に到達できません 400
内部接続エラーによりアプリケーションの起動に失敗しました 401
Web/SaaSアプリケーションの起動に失敗しました 401
無効なアプリケーション構成のため、Web/SaaS FormFill SSOに失敗しました 401
Web/SaaS 用 Kerberos SSO が失敗しました 401
内部サーバーエラーにより Web/SaaS SSO が失敗しました 402
構成されたプロキシに到達できないため、Web/SaaS アプリの起動に失敗しました 402
構成されたプロキシでの認証に失敗したため、Web/SaaS アプリの起動に失敗しました 402
Citrix Secure Access™ クライアントが SSO を実行できませんでした 402

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

セッションコード 403

アプリ列挙メッセージコード 403

アプリ起動メッセージコード 405

アプリ起動エラーコード 405

Secure Private Access のログとイベント 409

診断ダッシュボード 409

エラーのリスト 409

監査ログ 409

システムログ 409

デバイスポスチャログ 409

診断ログ 410

FAQ 410

Secure Private Access 診断ログとは何ですか? 410

Secure Private Access ログはどこで確認できますか? 410

Secure Private Access 診断ログを表示するウィジェットはどれですか? 410

Secure Private Access診断ログにはどのような詳細情報がありますか? 411

診断ログをフィルタリングするにはどうすればよいですか? 411

Secure Private Access診断ログにはどのようなイベントが記録されますか? 412

エラーのリスト 413

診断ログ情報コード 413

解決手順 431

クライアントログの収集方法 460

よくある質問 460

参照 462

監査およびシステムログ 463

デバイスポスチャのログとイベント 464

Identity and Access Managementコンソールのデバイスポスチャダッシュボード 464

ログの場所 466

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

Secure Private Accessダッシュボード 466
デバイスポスチャのエラーログ 467
デバイスポスチャデータの書き出し 467
データのエクスポートとサードパーティ統合 468
セキュリティ情報およびイベント管理の統合 468
OData API を使用してカスタムレポートを作成する 468
システムログのエクスポート 469
Kafkaからデータをエクスポートする 469
Secure Private Accessイベント 469
Device Postureサービスイベント 469
監査ログとシステムログのエクスポート 469
SystemLog APIを使用してSecure Private Accessイベントをエクスポートする 470
OData を使用してセッションデータをエクスポートする 470
ロールベースのアクセス制御 472
ロールと権限 474
管理者へのロールベースアクセスを有効にする 475
マルチセッション仮想デスクトップインフラストラクチャのサポート 477
主な機能と利点 477
マルチセッション VDI を有効にする 478
モバイルデバイス用 Citrix Secure Private Access 480
サポートされているバージョンとプラットフォーム 480
サポートされる機能 480
前提条件 481
Citrix Secure Accessクライアントを使用するiOSおよびAndroidユーザーのワークフロー 481
関連トピック 482
iOS Kerberos拡張機能を使用したKerberos認証 482
iOSクライアントの構成 482
前提条件 482

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

iOSデバイスでのMDM登録の検証 483
MDMサーバーの構成 483
Intuneポリシーの構成 483
IIS構成 487
ドメインコントローラー側の構成 489
機能の非推奨化 491
Webアプリアクセスのクライアントレス VPNアクセスの廃止について 492
データガバナンス 494
データレジデンシー 494
データ収集 495
データ転送 496
データ制御 496
データ保持 496
データのエクスポート 497
定義 497
製品認定とコンプライアンス 498
認定と監査 498
証明書と監査レポート 499
index 500
Gateway ConnectorからConnector Applianceへの移行 500
Gateway ConnectorをConnector Applianceに移行するための大まかな手順 501
Connector Applianceをインストールするには 501
よくある質問 501
同じ関連ドメインに起因する競合を解決するためのルートテーブル 502
ルートテーブルの仕組み 502
メインルートテーブル 503
ミニルーティングテーブル 504
ミニルーティングテーブルにルートを追加するには 504

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

Citrix Workspaceアプリ経由でのCitrix Secure Access™クライアントへのシングルサインオン 505
前提条件 505
Windowsの機能要件 506
ADFSとセキュア プライベート アクセスの統合 507
ADFSにクレームプロバイダ信頼を追加する 507
クレームプロバイダートラストID 510
証明書利用者識別子 511
IdP開始フローでリレーステートを有効にする 512
ADFSサーバーでRelayStateパラメータを有効にするには 513
Citrix Secure Private Accessでのアプリ構成 513
IdP開始フロー 513
SP開始フロー 515
シトリックス セキュア プライベート アクセス™ 515
Citrix Secure Private Accessの主な機能 516
セキュアプライベートアクセス REST API 518
アプリケーション固有のリソースロケーションにDNSクエリをルーティングする 518
システム要件 518
機能の有効化 518
DNSクエリのルーティングを構成する 518
G Suite を構成する 521
Jira の構成 521
Citrix Gateway SaaS アプリケーション 522
O365を構成する 526
前提条件 526
ドメインフェデレーションの仕組み 527
Office 365アプリでサポートされている認証方法 528
Secure Private Access サービスで O365 アプリを構成する 529
Microsoft Entra ID から Citrix Workspace へのドメインフェデレーションを構成する 530

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

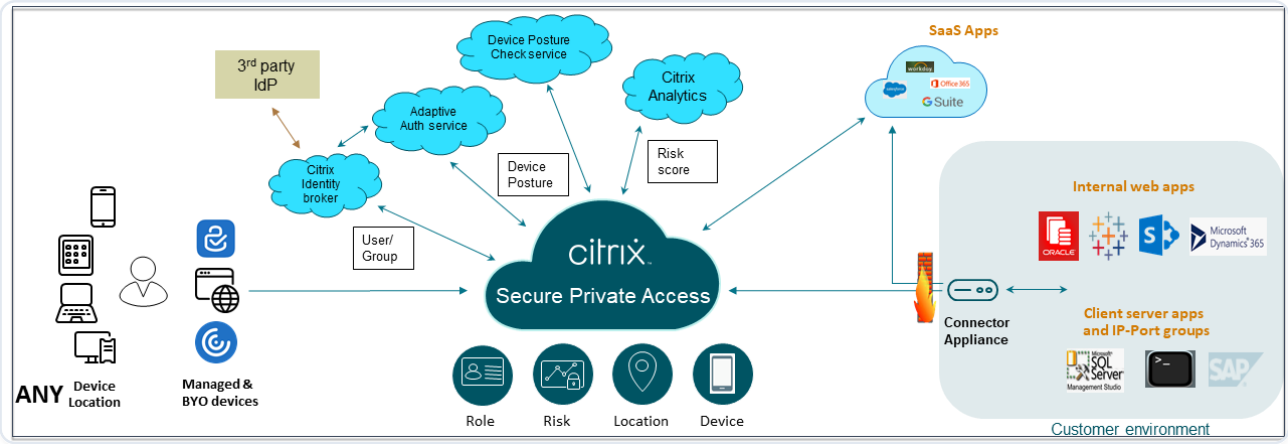
Microsoft Entra ID から Citrix Workspace へのドメインフェデレーションを構成する手順 531
Microsoft Entra ID から Citrix Workspace へのドメインの自動フェデレーション 533
ドメインを自動的にフェデレーションする手順 533
多要素認証 (MFA) の抑制 534
Citrix Workspaceでの個々のOfficeスイートアプリケーションの構成 535
Microsoft Entra ID に統合されたサードパーティ製アプリ 536
参照リンク 538
ERP Cloudを構成する 538
Citrix Gateway SaaSアプリケーション 538
ServiceNow を構成する 540
Tableau を構成する 546
Workday の構成 548
Citrix Gateway SaaS アプリケーション 548
Zoom を構成する 550
Citrix Gateway SaaS アプリケーション 550
アクセスモードベースのポリシー適用 553
仕組み 553
エンドユーザーエクスペリエンス 554
サーバーからクライアントへの接続のサポート - プレビュー 555
サーバーからクライアントへの接続の仕組み 555
サーバーからクライアントへのアプリを作成する 556
前提条件 556
サーバーからクライアントへのTCP/UDPアプリを構成するには、次の手順を実行します 557

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

Secure Private Access サービス ソリューションの概要

従来のVPNソリューションでは、エンドユーザーデバイスの管理、ネットワークレベルでのアクセス提供、静的なアクセス制御ポリシーの適用が必要です。Citrix Secure Private Access™ は、IT部門にBYOデバイスからの脅威から保護するための一連のセキュリティ制御を提供し、ユーザーが管理対象デバイスかBYOデバイスかに関わらず、IT承認済みアプリケーションにアクセスする選択肢を与えます。

Citrix Secure Private Access は、アダプティブ認証、シングルサインオンのサポート、アプリケーション向けの強化されたセキュリティ制御を提供します。Secure Private Access はまた、Device Posture サービスを使用してセッションを確立する前にエンドユーザーデバイスをスキャンする機能も提供します。アダプティブ認証またはデバイスポスチャの結果に基づいて、管理者はアプリの認証方法を定義できます。



アダプティブセキュリティ

アダプティブ認証は、現在のリクエストに対する適切な認証フローを決定します。アダプティブ認証は、デバイスのポスチャ、地理的位置、ネットワークセグメント、ユーザーの組織/部門のメンバーシップを識別できます。取得した情報に基づいて、管理者はIT承認済みアプリへのユーザー認証方法を定義できます。これにより、組織はパブリックSaaSアプリ、プライベートWebアプリ、プライベートクライアントサーバーアプリ、DaaS (Desktops as a Service) を含むすべてのリソースで同じ認証ポリシーフレームワークを実装できます。詳細については、「アダプティブセキュリティ」を参照してください。

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

アプリケーションアクセス

Secure Private Access は、VPNに依存せずにオンプレミスのWebアプリへの接続を作成できます。このVPNレス接続は、オンプレミスに展開されたConnector Applianceを使用します。Connector Appliance は、組織のCitrix Cloudサブスクリプションへのアウトバウンド制御チャネルを作成します。そこから、Secure Private Access はVPNを必要とせずに内部Webアプリへの接続をトンネルできます。詳細については、「アプリケーションアクセス」を参照してください。

シングルサインオン

アダプティブ認証を使用すると、組織は強力な認証ポリシーを提供して、侵害されたユーザーアカウントのリスクを軽減できます。Secure Private Access のシングルサインオン機能は、すべてのSaaS、プライベートWeb、およびクライアントサーバーアプリに同じアダプティブ認証ポリシーを使用します。詳細については、「シングルサインオン」を参照してください。

ブラウザセキュリティ

Secure Private Access は、データ損失防止 (DLP)、マルウェアおよびフィッシング対策、URLフィルタリングなどの機能を含むGoogle Chrome Enterprise Premium (CEP) と統合されています。クライアントマシンでローカルに実行されているGoogle Chromeブラウザは、Chrome管理プロファイルを介したユーザーレベルのポリシー適用を備えたセキュアブラウザとして機能します。詳細については、「Google Chrome Enterprise Premium との統合」を参照してください。

デバイスポスチャ

デバイスポスチャサービスを使用すると、管理者は、企業リソースにリモートでアクセスしようとしているエンドポイントデバイスのポスチャをチェックするポリシーを定義できます。エンドポイントのコンプライアンスステータスに基づいて、デバイスポスチャサービスはアクセスを拒否したり、企業アプリケーションやデスクトップへの制限付き/フルアクセスを提供したりできます。

エンドユーザーがストアから接続を開始すると、Device Posture クライアントはエンドポイントパラメータに関する情報を収集し、この情報をDevice Posture サービスと共有して、エンドポイントのポスチャがポリシー要件を満たしているかどうかを判断します。

Device PostureサービスとCitrix Secure Private Accessの統合により、Citrix Cloudの回復性と拡張性で提供されるSaaS、Web、TCP、UDPアプリへのセキュアなアクセスがどこからでも可能になります。詳細については、Device Postureを参照してください。

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

TCPおよびUDPアプリケーションのサポート

リモートユーザーは、フロントエンドがエンドポイントにあり、バックエンドがデータセンターにあるプライベートなクライアントサーバーアプリへのアクセスを必要とすることがあります。組織は、これらの内部およびプライベートアプリに対して厳格なセキュリティポリシーを正当に適用できますが、これによりリモートユーザーがセキュリティプロトコルを侵害することなくこれらのアプリケーションにアクセスすることが困難になります。

Secure Private Accessサービスは、ZTNAを有効にしてこれらのアプリへのセキュアなアクセスを提供することで、TCPおよびUDPのセキュリティ脆弱性に対処します。ユーザーは、Chromeブラウザを使用するか、またはマシン上で実行されているCitrix Secure Access™クライアントを介してネイティブクライアントアプリケーションを使用することで、TCP、UDP、HTTPSアプリを含むすべてのプライベートアプリにアクセスできるようになりました。

ユーザーは、クライアントデバイスにCitrix Secure Accessクライアントをインストールする必要があります。

- Windowsの場合、クライアントバージョン（22.3.1.5以降）はDownloadsからダウンロードできます。
- macOSの場合、クライアントバージョン（22.02.3以降）はApp Storeからダウンロードできます。

詳細については、クライアントサーバーアプリのサポートを参照してください。

使用例

- ファイアウォールで受信トラフィックを開放することなく、ゼロトラストのアプローチを使用して内部アプリケーション（Web/TCP/UDP）にアクセスする
- ユーザーがアクセスするアプリケーションを検出することで、ゼロトラストのアプローチに移行する
- SaaSアプリケーションへのアクセスを企業所有のパブリックIPアドレスに制限する
- Azure管理SaaSアプリへのセキュリティ強化
- Office 365へのセキュリティ強化
- Oktaアプリへのセキュリティ強化

参照記事

- セキュア プライベート アクセス の概要

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

- 技術概要
- リファレンスアーキテクチャ
- Secure Private Access のオンボーディングとセットアップ

参考ビデオ

- アプリへのゼロトラストネットワークアクセス (ZTNA)
- Citrix Secure Private Access を使用したプライベート Web アプリへのアクセス
- Citrix Secure Private Access を使用したパブリック SaaS アプリへのアクセス
- Citrix セキュア プライベート アクセス を使用したプライベート クライアント/サーバー アプリへのアクセス
- Citrix Secure Private Access を使用したキーロガー保護
- Citrix Secure Private Access を使用した画面共有保護
- Citrix Secure Private Access を使用したエンドユーザーエクスペリエンス
- Citrix Secure Private Access を使用した ZTNA と VPN のログオンエクスペリエンスの比較
- Citrix Secure Private Access を使用した ZTNA と VPN のポートスキャン比較

関連製品の新機能

- Citrix StoreFront Cloud: 新機能
- Citrix DaaS: 新機能
- シトリックス セキュア アクセス: シトリックス セキュア アクセス

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

新機能

30 September 2026

- **新規顧客向けのSecure Private Accessデータ地域化の拡張**

  Secure Private Accessは、新規顧客の管理トラフィックとデータトラフィックを適切な地域のデータPOPとエンドポイントにルーティングするようになりました。詳細については、「データ地域化」を参照してください。

- **アクセスモードベースのポリシー適用**

  アクセスモードベースのポリシー適用により、管理者はユーザーがアプリケーションに接続する方法を制限できます。接続は、ブラウザベースのクライアントまたはCitrix Secure Accessクライアントを介して行うことができます。詳細については、「アクセスモードベースのポリシー適用」を参照してください。

03 September 2026

- **ドメイン、フォレスト、およびIdPタイプ別に表示されるアクセスポリシーのユーザーとグループの詳細:**

  表示名、メールID、またはユーザープリンシパル名でユーザーまたはグループを検索すると、選択したユーザーとグループがグリッドに表示されます。各行には、名前、メールアドレス、IdPタイプ、OID、ドメインなどのIDの詳細が表示されます。異なるドメイン、フォレスト、またはIDプロバイダー（IdP）間で、同じ名前のユーザーまたはグループを明確に区別できます。詳細については、「複数のルールを持つアクセスポリシーの作成」を参照してください。

- **HARファイルを使用した関連ドメインの検出:**

  Secure Private Accessでは、HARファイルをアップロードして、アプリケーションがアクセスするドメインを自動的に検出できるようになりました。検出されたドメインを確認し、アプリケーションの関連ドメイン構成に追加するドメインを選択できます。これにより、関連ドメインを手動で特定して構成する必要が減り、アプリケーションのオンボーディングが簡素化されます。詳細については、「HARファイルを使用した関連ドメインの検出」を参照してください。

- **Chrome Enterprise Premium (CEP) 構成をGoogleディレクトリ組織部門に適用:**

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

すべてのユーザーとGoogleディレクトリユーザーグループに加えて、選択したGoogleディレクトリ組織部門にCEP構成を適用できるようになりました。詳細については、「Googleディレクトリ組織部門のCEPを構成する」を参照してください。

- **条件付き認証のサポート:**

  Citrix CloudをOpenID Connect (OIDC) 認証プロバイダーとして使用するChrome Enterprise Premium (CEP) のシングルサインオン (SSO) が、条件付き認証をサポートするようになりました。詳細については、「Citrix Identity and access managementでのOpen ID Connect」を参照してください。

- **ユーザー属性タイプの設定:**

  Secure Private Access 管理コンソールで、マネージドプロファイルIDページからユーザー属性を設定できるようになりました。詳細については、マネージドプロファイルIDを参照してください。

- **ユーザーとグループの同期を確認する:**

  ユーザーまたはグループを選択する際、管理者は、選択したユーザーディレクトリからのエントリがGoogle Directoryと同期され、正しく構成されているかを確認できます。Secure Private Accessポリシーは、ユーザーとグループが同期されている場合にのみ正しく評価されます。詳細については、ユーザーとグループの同期を確認するを参照してください。

- **アプリケーション削除時のルーティングエントリの自動クリーンアップ:**

  アプリケーションを削除すると、Secure Private Accessはルーティングエントリもクリーンアップするようになりました。詳細については、アプリケーション削除時のルーティングエントリの自動クリーンアップを参照してください。

19 August 2026

- **クローム エンタープライズ プレミアム (CEP) 向けのグーグル クラウド アイデンティティ対応**

  Google Cloud IdentityをCEPのIDプロバイダーとして使用できるようになりました。Google Cloud IdentityがIDプロバイダーである場合、ユーザーとグループはGoogle Cloudディレクトリにネイティブに存在するため、ディレクトリの関連付けは不要です。詳細については、統合ソリューションの前提条件を参照してください。

05 August 2026

- **SaaSアプリケーションにアクセスするための新しいルーティング方法:**

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

SaaSアプリのルーティングタイプを、Google Secure Gateway経由でトラフィックをルーティングする**Google Secure Gateway経由の外部**、またはクライアントからアプリに直接トラフィックをルーティングする**外部**のいずれかに設定できるようになりました。詳細については、SaaSアプリの構成を参照してください。

31 July 2026

- **Chrome Enterprise向けCitrix Secure Accessコントロール:**

  Citrix Secure Private Accessは、Google Chrome Enterprise Premium (CEP) 用のCitrix Secure Access拡張機能によって配信および適用されるセキュリティポリシーをサポートしています。

  Secure Private Accessでサポートされているポリシーは次のとおりです。

  - キーロギング対策
  - クリップボードコンテナ
  - Webアプリケーションのドメインサフィックス
  - セッション記録
  - ブラウザセッションの再認証

24 June 2026

- **エグレスハブリージョンの構成のサポート:**

  Secure Private Access を使用すると、管理者は Chrome Enterprise Premium が SaaS アプリケーションのトラフィックに使用するエグレスリージョンを選択できます。選択された各リージョンは、専用のエグレス IP アドレスセットを提供し、管理者はこれを SaaS アプリケーションの許可リストに追加して、Google Secure Gateway を介してルーティングされるトラフィックを許可できます。この機能は、クラウド展開とハイブリッド展開の両方で利用できます。詳細については、「エグレスハブリージョンの構成」を参照してください。

- **Google ディレクトリの citrix-schema 同期への依存関係の削除:**

  Chrome Enterprise Premium の Google ディレクトリにおける Citrix スキーマ同期への依存関係が削除されました。Google ディレクトリの同期は、ユーザーのメール ID を使用して実行できるようになりました。この機能を有効にするには、Citrix サポートにお問い合わせください。

- **OIDC の SAML 2.0 認証サポート:**

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

OIDC で SAML 2.0 ID プロバイダー (IdP) がサポートされるようになりました。Citrix Identity との OIDC 統合の詳細については、「Citrix Identity との OpenID Connect」を参照してください。

18 June 2026

- **CSV ベースのアプリケーションインポート中にプライマリおよびセカンダリのリソースロケーションを定義:**

CSV ファイルを使用したアプリケーションのインポートで、管理者は一括アプリケーション作成時にプライマリとセカンダリの両方のリソースロケーションを定義できるようになりました。これにより、異なる場所で運用されているエンタープライズ展開の効率的なオンボーディングが可能になります。詳細については、「アプリケーションインポートツール」を参照してください。

09 June 2026

以下のセクションでは、09 June 2026 リリースに関する詳細情報を提供します。

重要なお知らせ

- **シトリックス セキュア プライベート アクセス™ エッジ 構成の更新:**

  Citrix Secure Private Access の継続的なパフォーマンスおよびインフラストラクチャの最適化の一環として、特定の Citrix Secure Private Access エッジ構成の更新がまもなく展開されます。

  > **注:**
  >
  > この通知は、ファイアウォールまたはプロキシレベルで特定のPoPレベルのFQDN許可リストを設定している、または文書化された推奨事項以外のカスタムエントリを設定しているお客様**のみ**を対象としています。

  変更点:

  Citrix Secure Private Access エッジのFQDNは、以下に示す新しい形式に更新されます。

  古いFQDN: `<pop>-rdvz.g.nssvc.net`

  新しいFQDN: `<pop>-spa-rdvz.g.nssvc.net`

  例:

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

`az-us-e-rdvz.g.nssvc.net` が `az-us-e-spa-rdvz.g.nssvc.net` に変更

`az-eu-w-rdvz.g.nssvc.net` が `az-eu-w-spa-rdvz.g.nssvc.net` に変更

対応が必要ですか:

- **対応不要:** 推奨されるワイルドカードドメイン（例: `*.nssvc.net`）を使用している場合、古い名前と新しい名前の両方がすでにカバーされており、対応は不要です。詳細については、「Secure Private Access 用コネクタアプライアンス」を参照してください。
- **対応が必要:** 明示的なPoPレベルのFQDN許可リスト、または文書化された推奨事項以外のカスタムエントリを使用している場合は、必要な対応を実行してください。

必要な操作:

特定のPoPへのアウトバウンドトラフィックを許可しているお客様は、ファイアウォールルールを更新する必要があります。現在許可されている `<pop>-rdvz.g.nssvc.<suffix>` エントリごとに、対応する `<pop>-spa-rdvz.g.nssvc.<suffix>` レコードを追加して、サービスが中断されないようにしてください。PoPのリストについては、「Citrix Secure Private Access サービスのPoP（Points of Presence）の場所」を参照してください。

20 May 2026

- **データ地域化**

  Citrix Secure Private Accessのデータ地域化により、お客様は優先する地理的地域を選択することで、データの保存場所を制御できます。お客様は、グローバル、ヨーロッパ（EU）、APAC（アジア太平洋）、北米（NA）などのオプションから、データの保存地域を選択できます。すべての静止構成データは選択された地域内に留まり、指定された地理的範囲外に出ることはありません。詳細については、「データ地域化」を参照してください。

28 April 2026

- **Secure Private Accessサービス構成の簡素化**

  Secure Private Accessサービスの構成が、単一の統合されたフローに合理化されました。システム構成ページには、Secure Private Accessクラウド展開で使用されるコンポーネントを示すトポロジ図が含まれるようになりました。管理者は、このページから直接Connector ApplianceとGoogle Chrome Enterprise Premiumを構成できます。詳細については、「Secure Private Accessのオンボーディングとセットアップ」を参照してください。

- **テレメトリ目的のGoogle管理者権限の必須化**

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

Google管理コンソールのサービスアカウントに、新しい一連の権限を割り当てる必要があります。これらの権限は、主にテレメトリ目的（DLPアクティビティイベントやセキュリティアラートなど）で使用されます。詳細については、「Google Chrome統合のセットアップ」を参照してください。

- **CEP向けOkta IdPサポート**

  OktaをChrome Enterprise Premium（CEP）のIDプロバイダーとして使用できるようになりました。詳細については、「Citrix OIDCクライアントの作成」を参照してください。詳細については、「Citrix OIDCクライアントの作成」を参照してください。

07 April 2026

- **アプリのオンボーディングを簡素化および高速化するために、最もよく使用される5つのテンプレートをリスト表示**

  アプリケーション構成ページの**テンプレートの選択**セクションに、アプリのオンボーディングを簡素化および高速化するために、最もよく使用される5つのテンプレートがリスト表示されるようになりました。詳細については、「SaaSアプリの構成」を参照してください。

04 March 2026

- **Secure Private Access 管理UIドメインのsecureaccess.cloud.comへの移行**

  Secure Private Access 管理UIドメインは、`secureaccess.cloud.com`に更新されました。現在のURLは引き続き機能し、新しいドメインに自動的にリダイレクトされます。アクションや構成の変更は必要ありません。

12 February 2026

- **ルーティング例外を使用したポートベースルーティング**

  ポートベースルーティング機能を使用すると、管理者はルーティング例外を使用して、TCP/UDPアプリの同じ宛先の異なるポートのトラフィックを異なる方法でルーティングできます。詳細については、ルーティング例外を使用したポートベースルーティングを参照してください。

05 February 2026

- **シトリックス エンタープライズ ブラウザからクローム エンタープライズ プレミアムへの移行**

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

Citrix Enterprise BrowserからChrome Enterprise Premiumへの段階的な移行アプローチにより、組織は両方のブラウザソリューションを並行して実行することで、移行期間中のビジネス継続性を維持できます。段階的な移行により、お客様は既存のアプリケーションとワークフローのChrome Enterprise Premiumとの互換性を検証できます。詳細については、Citrix Enterprise BrowserからChrome Enterprise Premiumへの移行を参照してください。

- **メールアドレスのないユーザーグループのドメインマッピング**

  Googleディレクトリでは、すべてのユーザーおよびグループオブジェクトに検証済みのメールアドレスが必要です。ただし、これはSecure Private Accessでサポートされているディレクトリ、特にActive Directory (AD) およびMicrosoft Entra IDでは常に利用できるわけではありません。ADおよびMicrosoft Entra IDオブジェクトにはメールアドレスがないか、Googleディレクトリが検証できない内部または特殊なドメイン（例: @fabrikam.onmicrosoft.com）を指すメールアドレスがある場合があります。

  通常、メールアドレスはSecure Private AccessとGoogleディレクトリ間の共通識別子として機能するため、検証済みのGoogleメールアドレスを持たないAD/Entraのグループは、Secure Private Accessポリシーでは通常サポートされません。ドメインマッピング機能は、メールアドレスがない場合や、未検証のドメインのメールアドレスを持つ場合でも、管理者がグループに対してポリシーを構成できるようにすることで、この問題を解決します。詳細については、メールアドレスのないユーザーグループのドメインマッピングを参照してください。

18 December 2025

- **ブラウザ内でのSSHおよびRDPアプリケーションへのセキュアなアクセス**

  Citrix Secure Private Accessは、Chrome Enterprise Premiumと統合されており、ブラウザ内で直接セキュアなSSHおよびRDPセッションを有効にします。詳細については、以下のトピックを参照してください。

  - ブラウザ内でのSSHアプリへのセキュアなアクセス(/ja-jp/citrix-secure-private-access/service/spa-cep-ssh-access.html)
  - ブラウザ内でのRDPアプリへのセキュアなアクセス(/ja-jp/citrix-secure-private-access/service/spa-cep-rdp-access.html)

16 December 2025

- **DNSクエリをアプリケーション固有のリソースロケーションにルーティングする**

  管理者は、特定のアプリケーションに対するDNSクエリを、専用のリソースロケーションに直接ルーティングできます。これにより、より正確なDNS解決、インテリジェントなトラフィッ

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

ク管理、およびより良いユーザーエクスペリエンスが可能になります。詳細については、「DNSクエリをアプリケーション固有のリソースロケーションにルーティングする」(/ja-jp/citrix-secure-private-access/service/route-dns-queries-to-application-specific-resource-locations.html)を参照してください。

11 December 2025

- **シトリックス エンタープライズ ブラウザからクローム エンタープライズ プレミアムへの移行**

  既存のSecure Private Accessサービスのお客様は、Citrix Enterprise BrowserからChrome Enterprise Premium (CEP) へ段階的に移行できます。この段階的な移行アプローチにより、組織は移行期間中に両方のブラウザソリューションを並行して実行することで、ビジネスの継続性を維持できます。段階的な移行により、お客様は既存のアプリケーションとワークフローのChrome Enterprise Premiumとの互換性を検証できます。詳細については、「Citrix Enterprise BrowserからChrome Enterprise Premiumへの移行」(/ja-jp/citrix-secure-private-access/service/citrix-enterprise-browser-to-cep-migration.html)を参照してください。

30 October 2025

- **Chrome Enterpriseソリューションと連携したCitrix Secure Private Accessのエージェントレスアクセスリリースの一般提供開始**

  Citrix Secure Private Access™とGoogle Chrome Enterprise Premiumの統合により、エンドユーザーは、Zero Trust Network Access (ZTNA) エージェントを必要とせずに、Google Chromeブラウザをエンタープライズブラウザとして使用して、プライベートWebアプリケーションおよびSaaSアプリケーションに安全にアクセスできるようになりました。また、データ損失防止 (DLP) コントロール、Webフィルタリング、ZTNAポリシー適用によるアプリケーションごとのアクセスを実現できます。詳細については、「Citrix Secure Private AccessとGoogle Chrome Enterprise Premiumの統合」(/ja-jp/citrix-secure-private-access/service/secure-private-access-integration-with-cep.html)を参照してください。

  現在のSecure Private Access / Citrix Enterprise Browserの運用テナントをご利用のお客様への推奨事項

  現在の運用環境のお客様は、運用テナントではなく、別のテナントでエージェントレスアクセスリリースをテストすることをお勧めします。2025年11月下旬に予定されている製品アップデートには、既存のSecure Private Accessのお客様が、既存のアプリ構成とアクセスポリシーを維持したまま、エージェントレスアクセス機能を利用できるようにする機能強化が含まれます。2025年11月のリリースでは、既存のSecure Private Accessのお客様が、現在のWebアプリケーションおよびSaaSアプリケーション (現在はCitrix Enterprise Browser経由で起動) のアプ

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

リ起動をChromeブラウザで起動するように移行できるユーザーインターフェイスも提供されます。

2025年11月のアップデートより前にこのリリースを使用したいお客様は、既存のSecure Private Accessテナントをクリーンな状態にリセットし、その後、Secure Private Accessサービスに再度オンボーディングする必要があります。次の手順を実行します。

a. Secure Private Accessコンソールで、すべてのアクセスポリシー、アプリ、および関連ドメインを削除します。
b. Citrix Cloud コンソール上のSecure Private Accessタイルに戻ります。
c. **Fully Cloud-delivered Service architecture**を選択し、**Continue**をクリックします。詳細については、Secure Private Accessのオンボーディングとセットアップを参照してください。

17 September 2025

- **iOSデバイス向けSecure Private Accessのサポート**

  Secure Private Accessは、iOS版Secure Access Clientバージョン25.08.1以降のモバイルデバイスでサポートされるようになりました。モバイルユーザーは、iOSデバイスから企業アプリケーションにアクセスできます。詳細については、モバイルデバイス向けCitrix Secure Private Accessを参照してください。

13 August 2025

- **Citrix Enterprise Browser™を介してアプリにアクセスするためのカスタムストアURL**

  カスタムストアURL機能により、組織は、デフォルトの*.cloud.comドメインではなく、ブランド化された組織所有のドメイン（例：workspace.company.com）を介して、SaaSおよびプライベートWebアプリケーションへのアクセスをユーザーに提供できます。

- **ポリシーモデリングツールの機能強化**

  ポリシーモデリングツールは、アプリケーションのルーティング決定に影響を与えるルーティングタイプと特定のポリシータイプを表示するようになりました。この機能強化により、管理者はルーティングの問題をトラブルシューティングし、アプリケーションが構成されたポリシーに準拠していることを確認できます。詳細については、ポリシーモデリングツールを参照してください。

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

14 July 2025

- **MonitorでSecure Private Accessエージェントレスアプリを監視およびトラブルシューティングする**

  管理者とヘルプデスク担当者は、MonitorでSecure Private Accessエージェントレスアプリのセッションとイベントを監視およびトラブルシューティングできるようになりました。詳細については、MonitorとのSecure Private Access統合を参照してください。

- **UDPアプリケーションのサーバー-クライアント接続のサポート**

  サーバー-クライアント接続は、TCPアプリケーションに加えてUDPアプリケーションでもサポートされるようになりました。顧客のリソースロケーションにあるサーバーは、リモートクライアントとのUDP接続を確立できます。詳細については、サーバー-クライアント接続のサポートを参照してください。

- **ヘルプデスク担当者向けの新しいロールベースのアクセス制御ロール**

  フルアクセス管理者および読み取り専用管理者のロールに加えて、Secure Private Access 管理者向けに以下のロールが利用可能です。

  - フルモニター管理者
  - ヘルプデスク管理者

  詳細については、「ロールベースのアクセス制御」を参照してください。

- **アプリケーション固有のリソースロケーションへのUDP DNSクエリのルーティング**

  特定のホスト名に対するUDP DNSクエリを、対応するアプリケーションがホストされているリソースロケーションに直接ルーティングできるようになりました。このルーティングにより、DNSクエリが最も関連性の高いリソースロケーションに到達することが保証され、アプリケーションのパフォーマンスが向上します。以前は、すべてのUDP DNSクエリは、アプリケーションの実際の場所に関係なく、デフォルトで地理的に最も近いリソースロケーションにルーティングされていました。

  仕組み:

  a. アプリケーション固有のリソースロケーションへのUDP DNSクエリのルーティングは、デフォルトで無効になっています。この機能を有効にするには、Citrixサポートにお問い合わせください。

  b. この機能が有効になると、DNSクエリはSecure Private Accessにルーティングされ、アプリケーションに関連付けられた特定のリソースロケーションが識別されます。Secure

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

Private Accessからの応答に基づいて、DNSクエリはアプリケーション専用のリソースロケーションにルーティングされます。

c. アプリケーション固有のリソースロケーションが識別されない場合、クエリは利用可能な最も近いリソースロケーションにフォールバックします。

03 June 2025

- **Secure Private Accessコンソール内での証明書の管理**

  Secure Private Access証明書ストアは、管理者向けに、認証局（CA）証明書とSecure Sockets Layer（SSL）証明書の両方を効率的に管理するための一元的な場所を提供するようになりました。この専用ストアにより、管理者は新しい証明書をシームレスに追加し、既存の証明書を変更し、不要になった証明書を削除できるため、証明書管理が簡素化されます。詳細については、「Secure Private Accessコンソールでの証明書の管理」を参照してください。

15 May 2025

- **シトリックス セキュア プライベート アクセス™ と Google Chrome Enterprise Premium の統合**

  Citrix Secure Private Access と Google Chrome Enterprise Premium の統合により、顧客は Google Chrome Enterprise Premium をエンタープライズブラウザソリューションとして使用し、Citrix Secure Private Access が提供するセキュアな接続とともに、プライベート Web アプリや SaaS アプリケーションへのセキュアなアクセスを実現できます。詳細については、「Citrix Secure Private Access と Google Chrome Enterprise Premium の統合」を参照してください。

24 April 2025

- **ハイブリッドデータパスのサポート**

  Secure Private Access サービスのハイブリッドデータパスは、オンプレミスとクラウドの両方のインフラストラクチャを活用して、アプリケーションへのセキュアなアクセスを提供します。組織はハイブリッドデータパスを使用して、すべてのデータトラフィックをオンプレミスの NetScaler Gateway 経由でルーティングできます。詳細については、「Secure Private Access サービスのハイブリッドデータパス」を参照してください。

- **Monitor でのコンテキストルーティングインサイトの表示**

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

コンテキストルーティングにより、アプリケーションのルートが動的に変更される可能性があります。たとえば、ユーザーが社内ネットワーク外にいる場合は Secure Private Access サービス経由でアプリケーションがルーティングされ、社内にいる場合はアプリに直接ルーティングされることがあります。管理者に対してこれらのルーティング決定の可視性を提供することは、ルーティングの問題をトラブルシューティングする上で非常に重要です。詳細については、「Monitor でのコンテキストルーティングインサイト」を参照してください。

- **バックアップリソースロケーションの構成**

  管理者は、セカンダリリソースロケーションを構成するか、「First Available」オプションを使用することで、障害発生時でもアプリケーションの高可用性を確保できます。詳細については、次のトピックを参照してください。

  - エンタープライズ Web アプリのサポート
  - エンタープライズ Web アプリへのエージェントレスアクセス
  - Software as a Service アプリのサポート
  - クライアントサーバーアプリのサポート

- **IP アドレスプールを即時または時間経過とともに段階的に削除する**

  IP アドレスプールを即時または時間経過とともに削除するためのサポートが、次のいずれかのオプションを使用して追加されました。

  - **IPプールを強制的に削除:** 新しいユーザーへのIPアドレスの割り当てを停止し、未使用のIPアドレスを直ちに解放します。削除されたIPアドレスを使用しているアクティブなユーザーセッションは終了する可能性があり、その結果、突然の終了や強制ログアウトが発生します。セッションが終了したユーザーには、別のIPアドレスプールが作成された後にのみ、新しいIPアドレスが割り当てられます。
  - **IPプールを時間経過で削除:** 新しいユーザーへのIPアドレスの割り当てを停止し、未使用のIPアドレスを直ちに解放します。システムは、プールを完全に削除する前に、アクティブなセッションがログアウトまたは期限切れになるのを待ちます。セッションが終了したユーザーには、別のIPアドレスプールが作成された後にのみ、新しいIPアドレスが割り当てられます。

  詳細については、「IPアドレスプールを削除する」を参照してください。

22 April 2025

- **nsconfigファイルを使用したアプリケーションのインポート**

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

Secure Private Access管理コンソールには、管理者がCSVファイルに加えてnsconfigファイルを使用して複数のアプリケーションをシステムに一括インポートできるファイルインポートツールが含まれています。このツールは、従来のVPNからSecure Private Accessのようなより高度なソリューションに移行する組織にとって特に役立ちます。詳細については、「アプリケーションインポートツール」を参照してください。

nsconfigファイル機能を使用したアプリケーションのインポートはプレビュー中です。

20 February 2025

- **管理者監査ログ機能の強化**

  管理者監査ログ機能が強化され、Secure Private Accessサービス内のすべての管理者アクションの詳細なログをキャプチャできるようになりました。詳細については、「監査ログ」を参照してください。

- **UPNとメールアドレスに基づくユーザーの検索と追加**

  Secure Private Accessで、表示名に加えてUPNとメールアドレスに基づいてユーザーを検索および追加できるようになりました。この検索オプションにより、管理者は複数のアカウントを持っている場合でも、正しいユーザーを正確に識別し、アクセスを許可できます。詳細については、「アクセスポリシーを構成する」を参照してください。

08 January 2025

- **セッションポリシーを使用したセッション全体の動的ルーティング**

  管理者はセッションポリシーを構成して、Secure Private Accessを介してトラフィックをトンネリングすることなく、社内ユーザーをバックエンドアプリに直接ルーティングできます。セッションポリシーは、ネットワークロケーションやデバイスのポスチャなどの要因に基づいて動的ルーティングを提供します。詳細については、「社内ユーザーをバックエンドアプリケーションに直接ルーティングする」を参照してください。

07 January 2025

- **コネクタースティッキネスのサポート**

  Secure Private Access はコネクタースティッキネスをサポートしています。コネクタースティッキネスにより、クライアントがコネクターアプライアンスとの接続を確立した後、同じクライアントからの後続のすべてのリクエストが同じソース（コネクターアプライアンス）に

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

転送されるようになります。詳細については、「コネクタースティッキネス」を参照してください。

- **クライアントIPアドレススティッキネスのサポート**

  Secure Private Access はクライアントIPアドレススティッキネスをサポートしています。クライアントIPアドレススティッキネスにより、特定のクライアントIPアドレスからのリクエストが常に同じバックエンドサーバーにルーティングされるようになります。詳細については、「クライアントIPアドレススティッキネス」を参照してください。

  クライアントIPアドレススティッキネス機能はプレビュー中です。

- **クライアント内部IPアドレスプールの作成のサポート**

  クライアント内部IPアドレスプールを作成するためのサポートが追加されました。これらのIPアドレスプールは、ユーザーと関連デバイスに一意のIPアドレスを割り当て、以下のユースケースをサポートするために不可欠です。

  - サーバーからクライアントへの接続
  - クライアントIPアドレススティッキネスのサポート

  詳細については、「クライアント内部IPアドレスプール」を参照してください。

  > **注:**
  >
  > クライアント内部IPアドレスプール機能はプレビュー中です。この機能を有効にするには、Citrixサポートにお問い合わせください。

- **サーバーからクライアントへの接続のサポート**

  Secure Private Access は、顧客のリソースロケーションにあるサーバーがリモートクライアントとTCP接続を確立できるサーバーからクライアントへの接続をサポートしています。サーバーからクライアントへの接続を有効にするために、Secure Private Access はサーバーからクライアントへのアプリを導入しています。このアプリは、クライアントの詳細（ポート、プロトコル）とバックエンドサーバーのIP CIDR範囲で構成できます。詳細については、「サーバーからクライアントへの接続のサポート」を参照してください。

  サーバーからクライアントへのアプリのサポートはプレビュー中です。

02 January 2025

- **CSVベースのアプリケーションインポートツール**

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

Secure Private Access管理コンソールには、管理者がCSVファイルを使用して複数のアプリケーションをシステムに一括インポートできるCSVベースのインポートツールが含まれています。このツールは、従来のVPNからSecure Private Accessのようなより高度なソリューションに移行する組織にとって特に役立ちます。詳細については、CSVベースのアプリケーションインポートツールを参照してください。

03 December 2024

- **クラウドホスト型マルチセッションVDIに対するSecure Private Accessのサポート**

  Windows用Citrix Secure Accessクライアントは、クラウドホスト型マルチセッションVDIから企業リソースへのゼロトラストアクセスを実現するために、Secure Private Accessの使用をサポートするようになりました。詳細については、マルチセッション仮想デスクトップインフラストラクチャのサポートを参照してください。

25 November 2024

- **DaaS MonitorにおけるSecure Private Accessセッションコード**

  Secure Private Accessセッション関連コードがDaaS Monitorに表示されるようになりました。コードのリストについては、MonitorにおけるSecure Private Accessセッション関連コードを参照してください。

14 November 2024

- **ポリシーモデリングツールの機能強化**

  管理者は、各アプリケーションに関連付けられているポリシーの包括的なリストを表示し、ドリルダウン機能を利用して、特定のポリシーの適用ロジック、特定のポリシーが適用された理由、および他のポリシーが適用されなかった理由を理解できるようになりました。詳細については、アクセスポリシーへのドリルダウンを参照してください。

08 November 2024

- **モニターとのセキュアプライベートアクセス統合**

  Secure Private Accessは、Citrix DaaSの監視およびトラブルシューティングコンソールであるMonitorと統合されました。管理者およびヘルプデスク担当者は、DaaS MonitorからWeb/SaaSおよびTCP/UDPアプリのセッションとイベントを監視およびトラブルシューティングできます。詳細については、DaaS Monitorとの統合を参照してください。

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

07 November 2024

- **セキュアプライベートアクセスのグラフィカルユーザーインターフェイスの機能強化**

  セキュアプライベートアクセスサービスは、より良いユーザーエクスペリエンスのために、改善されたグラフィカルユーザーインターフェイス (GUI) を提供するようになりました。プライマリメニューのツリー構造は、より簡単なナビゲーションのためにホバー表示機能に置き換えられました。セカンダリメニュー項目は、ホバーすると表示され、サブメニューが表示されてより迅速な選択が可能になります。

  また、アイコンをクリックすることでメニュー全体を折りたたんだり展開したりできます。

23 September 2024

- **コンテキストベースのアプリルーティングとリソースロケーション選択のサポート**

  アクセスポリシーの動的ドメインルーティング構成により、管理者はユーザーコンテキストに基づいてURLごとの内部ルーティングタイプを編集できるようになりました。管理者はリソースロケーションを変更して、ユーザー要求が最適なデータセンターにルーティングされるようにし、ユーザー要求が効率的に処理され、パフォーマンスが最適化されることを保証できます。詳細については、「コンテキストベースのアプリルーティングとリソースロケーションの選択」を参照してください。

15 August 2024

- **ブロックされたユーザーリストのエントリをパージする期間を構成するオプション**

  管理者は、ブロックされたユーザーリストのエントリをパージする特定の期間 (1〜99日) を設定できるようになりました。詳細については、「アクティブなユーザーセッションを終了し、ユーザーをユーザーブロックリストに追加する」を参照してください。

- **追加のセキュリティ制御**

  アプリケーションアクセスを制限するために、次の追加のセキュリティ制御が利用可能になりました。

  - マイク
  - ウェブカメラ
  - 通知
  - ポップアップ
  - 安全でないコンテンツ

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

- **未承認Webサイト（Webフィルタリング）機能の強化**

  未承認Webサイト（Webフィルタリング）機能を使用すると、管理者はCitrix Enterprise Browserを介して、すべての未承認トラフィックへのアクセスをデフォルトでブロックしたり、デフォルトで許可したりできます。

16 July 2024

- **追加のセキュリティ制御**

  アプリケーションアクセスを制限するために、以下の追加のセキュリティ制御が利用可能です。

  - ファイルタイプによるダウンロード制限
  - ファイルタイプによるアップロード制限
  - 個人データマスキング
  - プリンター管理
  - セキュリティグループのクリップボード制限

- **アプリ検出ページでの埋め込みドメインの表示**

  アプリ検出機能を使用すると、メインドメインまたは埋め込みドメイン（HTTP/HTTPS）、あるいは宛先IPアドレス（TCP/UDP）がアプリケーションに関連付けられていない場合に、管理者は新しいアプリケーションを作成したり、それらのドメインを既存のアプリケーションに追加したりできます。**アプリ検出**ページには、メインドメインとその下にある埋め込みドメインの両方がツリー構造で表示されます。詳細については、「エンドユーザーがアクセスしたドメインまたはIPアドレスを検出する」を参照してください。

11 June 2024

- **ポリシーモデリングツール**

  ポリシーモデリングツール (**アクセスポリシー > ポリシーモデリング**) を使用すると、管理者は管理コンソール内から構成の問題を分析し、トラブルシューティングできます。詳細については、「ポリシーモデリングツール」を参照してください。

- **診断ログチャートにおけるフィルターのサポート**

  診断ログチャートのフィルターオプションは、管理者がログの分析とトラブルシューティングを容易にするために、アプリの種類、カテゴリ、説明などのさまざまな基準に基づいて検索を絞り込むのに役立ちます。詳細については、「診断ログ」を参照してください。

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

13 March 2024

- **アクティブなユーザーセッションを終了し、無効なユーザーリストにユーザーを追加するサポート**

  管理者は、すべてのアクティブなエンドユーザーセッションを直ちに終了し、ユーザーを無効なユーザーリストに追加できるようになりました。この無効なユーザーリストにユーザーを追加すると、すべてのアクティブなSecure Private Accessアプリケーションセッションが終了し、今後のアプリケーションアクセスがブロックされます。詳細については、「アクティブなユーザーセッションを終了し、無効なユーザーリストにユーザーを追加する」を参照してください。

12 February 2024

- **ブラウザおよびウイルス対策スキャンの一般提供**

  Device Postureサービスでサポートされているブラウザおよびウイルス対策スキャンが一般提供されるようになりました。詳細については、「デバイスポスチャでサポートされているスキャン」を参照してください。

23 January 2024

- **Device Postureサービスによるデバイス証明書チェックの一般提供**

  Device Postureサービスによるデバイス証明書チェックが一般提供されるようになりました。詳細については、「Device Postureサービスによるデバイス証明書チェック」を参照してください。

20 December 2023

- **Secure Private Accessオンプレミスの一般提供**

  オンプレミス向けCitrix Secure Private Accessが一般提供されるようになりました。詳細については、「新機能」を参照してください。

16 October 2023

- **Secure Private Accessオンプレミスソリューションのプレビュー機能**

  Secure Private Accessオンプレミスソリューションで、以下の機能が提供されるようになりました。

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

  - 初回セットアップ用の管理UI。
  - アプリケーションとアクセスポリシーの構成用の管理UI。
  - ログダッシュボード。

  詳細については、「Secure Private Access for on-premises」を参照してください。

- **デバイスポスチャサービスのプレビュー機能**

  デバイスポスチャサービスで、以下のチェックがサポートされるようになりました。

  - デバイスポスチャサービスがIGELプラットフォームでサポートされるようになりました。
  - デバイスポスチャサービスで、地理位置情報とネットワーク位置情報のチェックがサポートされるようになりました。

  詳細については、Device Postureを参照してください。

11 September 2023

- **Microsoft Intuneとのデバイスポスチャ統合の一般提供**

  Microsoft Intuneとのデバイスポスチャ統合が一般提供されるようになりました。詳細については、Microsoft Intune integration with Device Postureを参照してください。

30 August 2023

- **Device Postureサービス向けCitrix Endpoint Analysisクライアントの管理**

  EPAクライアントは、NetScalerおよびDevice Postureと組み合わせて使用できます。NetScalerおよびDevice Postureと組み合わせて使用する場合、EPAクライアントを管理するためにいくつかの構成変更が必要です。詳細については、「Device Postureサービス向けCitrix Endpoint Analysisクライアントの管理」を参照してください。

28 August 2023

- **iOSプラットフォームでのDevice Postureサービスサポート**

  Device PostureサービスがiOSプラットフォームでサポートされるようになりました。詳細については、「Device Posture」を参照してください。

  この機能はプレビュー版です。

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

22 August 2023

- **Citrix Device Postureサービスによるデバイス証明書チェック**

  Citrix Device Postureサービスは、エンドデバイスの証明書を企業の認証局と照合して、エンドデバイスが信頼できるかどうかを確認することで、Citrix DaaSおよびSecure Private Accessリソースへのコンテキストアクセス（Smart Access）を有効にできるようになりました。詳細については、「Device Postureサービスによるデバイス証明書チェック」を参照してください。

  この機能はプレビュー版です。

17 August 2023

- **Citrix DaaS™ MonitorでのDevice Postureイベント**

  Device Postureサービスのイベントと監視ログがDaaS Monitorで検索できるようになりました。詳細については、「Citrix DaaS MonitorでのDevice Postureイベント」を参照してください。

07 June 2023

- **オンプレミス向けSecure Private Accessを構成するためのツール**

  オンプレミスソリューション向けSecure Private Accessを構成するための簡素化されたユーザーインターフェイスが利用可能になりました。この構成ツールは、Citrix Virtual Apps and Desktops™デリバリーコントローラーで実行でき、SaaSまたはWebアプリケーションを迅速に作成できます。さらに、このツールを使用して、アプリケーションの制限、トラフィックルーティング、およびNetScaler Gatewayの設定を行うことができます。

29 May 2023

- **複数のルールを持つアクセス ポリシーの作成の一般提供開始**

  単一のポリシー内で、複数のアクセス ルールを作成し、異なるユーザーまたはユーザー グループに対して異なるアクセス条件を構成できます。これらのルールは、HTTP/HTTPS および TCP/UDP アプリケーションの両方に、すべて単一のポリシー内で個別に適用できます。詳細については、「複数のルールを持つアクセス ポリシーの構成」を参照してください。

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

10 April 2023

- **アプリケーション検出**

  アプリケーション検出機能は、管理者が組織内の Web アプリやクライアント サーバー アプリ (TCP および UDP ベースのアプリ) などの内部プライベート アプリケーション、およびそれらのアプリケーションにアクセスするユーザーについて可視性を得るのに役立ちます。管理者は、ドメイン (ワイルドカード ドメイン) または IP サブネットの範囲を指定することで、アプリを検出できます。詳細については、「アプリケーション検出」を参照してください。

29 March 2023

- **オンプレミス展開向け Secure Private Access ソリューション**

  Citrix StoreFront および NetScaler Gateway のお客様は、オンプレミス展開向けの Citrix Secure Private Access ソリューションを使用して、Citrix Virtual Apps および仮想デスクトップとともに Web および SaaS アプリにシームレスにアクセスできるようになりました。詳細については、「Secure Private Access for on-premises」を参照してください。

07 March 2023

- **DNS サフィックスの構成**

  Citrix Secure Private Access サービスの DNS サフィックス機能は、次のユースケースに使用できます。

  - バックエンド サーバーの DNS サフィックス ドメインを追加することで、Citrix Secure Access™ クライアントが非完全修飾ドメイン名 (ホスト名) を完全修飾ドメイン名 (FQDN) に解決できるようにします。
  - 管理者が IP アドレス (IP CIDR/IP 範囲) を使用してアプリケーションを構成できるようにし、エンド ユーザーが DNS サフィックス ドメイン下の対応する FQDN を使用してアプリケーションにアクセスできるようにします。

  詳細については、「FQDN を IP アドレスに解決するための DNS サフィックス」を参照してください。

23 January 2023

- **デバイスポスチャサービス**

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

Citrix Device Postureサービスは、管理者がCitrix DaaS (仮想アプリおよびデスクトップ) またはCitrix Secure Private Accessリソース (SaaS、Webアプリ、TCP、UDPアプリ) へのアクセスを得るためにエンドデバイスが満たす必要のある特定の要件を適用するのに役立つクラウドベースのソリューションです。詳細については、「デバイスポスチャ」を参照してください。

- **Microsoft Endpoint Managerとデバイスポスチャの統合**

  Device Postureサービスが提供するネイティブスキャンに加えて、Device Postureサービスは他のサードパーティソリューションとも統合できます。Device Postureは、WindowsおよびmacOS上のMicrosoft Endpoint Manager (MEM) と統合されています。詳細については、「Microsoft Endpoint Managerとデバイスポスチャの統合」を参照してください。

22 December 2022

- **Citrix Workspace™アプリ経由でログインしたユーザー向けのWorkspace URLのシングルサインオンサポート**

  Citrix Secure Accessクライアントは、Citrix Workspaceアプリ経由で既にログインしている場合、Workspace URLのシングルサインオンをサポートするようになりました。このSSO機能により、複数回の認証を回避することでユーザーエクスペリエンスが向上します。詳細については、「Workspace URLのシングルサインオンサポート」を参照してください。

- **アクセスポリシーを使用したアプリへのアクセスを有効にする**

  ユーザーにアプリへのアクセスを許可するには、管理者はエンドユーザーが利用できるように、アプリの一致するユーザーサブスクリプションリストを使用してアクセスポリシーを作成する必要があります。以前は、管理者はアクセスを有効にするためにユーザーをサブスクライバーとして追加する必要がありました。詳細については、「アクセスポリシーの作成」を参照してください。

03 October 2022

- **アプリへのアクセスを許可するアクセスポリシー**

  構成ウィザードの「アプリケーション」セクションから「アプリサブスクライバー」構成オプションが削除されました。ユーザーにアプリへのアクセスを許可するには、管理者はアクセスポリシーを作成する必要があります。アクセスポリシーでは、管理者はアプリサブスクライ

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

バーを追加し、セキュリティ制御を構成します。詳細については、「アクセスポリシーの作成」を参照してください。

- **UDPアプリのサポート**

  Secure Private Accessサービスは、UDPアプリへのアクセスをサポートするようになりました。詳細については、「プレビュー機能」を参照してください。

09 September 2022

- **ユーザーリスクスコアに基づく適応型アクセス**

  管理者は、Citrix Analytics for Security (CAS) が提供するユーザーリスクスコアを使用して、適応型アクセスポリシーを構成できるようになりました。詳細については、「ユーザーリスクスコアに基づく適応型アクセス」を参照してください。

- **ユーザーのネットワークロケーションに基づく適応型アクセス**

  管理者は、ユーザーがアプリケーションにアクセスしている場所に基づいて、適応型アクセスポリシーを構成できるようになりました。場所は、ユーザーがアプリケーションにアクセスしている国、またはユーザーのネットワークロケーションです。詳細については、「ロケーションに基づく適応型アクセス」を参照してください。

- **強化された適応型アクセスポリシービルダー**

  アプリへのアクセスは、構成された条件が満たされた後にのみ有効になります。アプリのサブスクリプションだけでは、顧客はアプリケーションにアクセスできません。管理者は、アプリのサブスクリプションに加えて、アプリへのアクセスを提供するためにアクセスポリシーを追加する必要があります。また、ユーザーまたはグループは、アプリにアクセスするために満たす必要があるアクセスポリシーの必須条件です。詳細については、「アクセスポリシーの作成」を参照してください。

- **SaaS/Webアプリへのファイルアップロードを制限する**

  この機能により、顧客管理者は、ビジネスに不可欠なアプリケーションにファイルをアップロードできるユーザーを制御（許可または制限）できます。これにより、承認されたユーザーのみがアプリケーションにファイルをアップロードできます。詳細については、「アクセスポリシーの作成」を参照してください。

- **強化されたダッシュボード**

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

Secure Private Accessダッシュボードは、アプリの使用状況、上位のアプリユーザー、アクセスされた上位のアプリ、診断ログなど、いくつかのユーザーメトリックに関する詳細な可視性を提供するようになりました。詳細については、「ダッシュボード」を参照してください。

- **ライブラリの非推奨化**

  Secure Private Accessアプリケーションは、Citrix Cloud™ライブラリ内では表示されなくなりました。構成されたすべてのSecure Private Accessアプリケーションは、Secure Private Accessサービスタイル内のアプリケーションセクションにあります。これにより、管理者はアプリケーションを簡単にナビゲート、編集、構成できます。

- **Secure Private Accessの監査ログ**

  Citrix Secure Private Accessサービス関連イベントは、**Citrix Cloud > システムログ**にキャプチャされるようになりました。詳細については、「監査ログ」を参照してください。

- **エンタープライズWebおよびSaaSアプリアクセスの診断ログ**

  Citrix Secure Private AccessのイベントがCitrix Analyticsと統合されました。Citrix Analyticsは、管理者がイベントにアクセスしてダウンロードできるパブリックエンドポイントを提供します。これらのイベントはPowerShellスクリプトを介してアクセスできます。詳細については、エンタープライズWebおよびSaaSアプリアクセスの診断ログを参照してください。

- **トラブルシューティングガイド**

  管理者はトラブルシューティングガイドを使用して、構成関連の問題を解決できます。詳細については、アプリ関連の問題のトラブルシューティングを参照してください。

01 June 2022

- **アダプティブ認証サービス**

  アダプティブ認証が一般提供（GA）されるようになりました。アダプティブ認証の詳細については、アダプティブ認証サービスを参照してください。

04 April 2022

- **ブランド変更**

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

Citrix Secure Workspace Accessサービスは、Citrix Secure Private Accessサービスにブランド変更されました。

- **簡単なオンボーディングとセットアップのための管理者ガイド付きワークフロー**

  Secure Private Accessには、SaaSアプリ、内部Webアプリ、TCPアプリへのゼロトラストネットワークアクセスを構成するためのステップバイステッププロセスを備えた、新しい合理化された管理者エクスペリエンスが導入されました。これには、アダプティブ認証、ユーザーサブスクリプションを含むアプリケーション、アダプティブアクセスポリシーなどの構成が、単一の管理コンソール内で含まれます。詳細については、簡単なオンボーディングとセットアップのための管理者ガイド付きワークフローを参照してください。

  この機能は一般提供（GA）されるようになりました。

- **Secure Private Accessダッシュボード**

  Secure Private Accessダッシュボードは、管理者に対し、トップアプリ、トップユーザー、コネクタのヘルスステータス、帯域幅使用量などを一箇所で確認できる完全な可視性を提供します。このデータはCitrix Analyticsから取得されます。詳細については、Secure Private Accessダッシュボードを参照してください。

  この機能は一般提供 (GA) が開始されました。

- **エンタープライズWebアプリへの直接アクセス**

  お客様は、Chrome、Firefox、Safari、Microsoft Edgeなどのネイティブ Webブラウザから直接、内部Webアプリへのゼロトラストネットワークアクセス (ZTNA) を有効に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Webアプリへの直接アクセス」を参照してください。

  この機能は一般提供 (GA) が開始されました。

- **TCP/HTTPSアプリへのZTNAエージェントベースアクセス**

  Citrixのお客様は、内部Webアプリに加えて、すべてのクライアントサーバーアプリケーションおよびIP/ポートベースのリソースへのゼロトラストネットワークアクセス (ZTNA) を有効にできるようになりました。詳細については、「クライアントサーバーアプリのサポート」を参照してください。

  この機能は一般提供 (GA) が開始されました。

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

- **エンタープライズWeb、TCP、SaaSアプリケーション向けのアダプティブアクセスとセキュリティ制御**

  Citrix Secure Private Accessサービスのアダプティブアクセス機能は、アプリケーションへのセキュアなアクセスを提供する包括的なゼロトラストネットワークアクセス (ZTNA) アプローチを提供します。アダプティブアクセスにより、管理者はコンテキストに基づいてユーザーがアクセスできるアプリへのきめ細かいレベルのアクセスを提供できます。ここでの「コンテキスト」という用語は、以下を指します。

  - ユーザーとグループ (ユーザーおよびユーザーグループ)
  - デバイス (デスクトップまたはモバイルデバイス)
  - 場所 (地理的位置またはネットワーク上の場所)
  - デバイスのポスチャ (デバイスポスチャチェック)
  - リスク (ユーザーリスクスコア)

  詳細については、「エンタープライズWeb、TCP、SaaSアプリケーション向けのアダプティブアクセスとセキュリティ制御」を参照してください。

  この機能は一般提供 (GA) が開始されました。

- **Secure Private Access の監査ログ**

  Citrix Secure Private Access サービス関連のイベントは、**Citrix Cloud > システムログ**に記録されるようになりました。詳細については、監査ログを参照してください。

  この機能は一般提供 (GA) が開始されました。

- **エンタープライズ Web および SaaS アプリケーションアクセスの診断ログ**

  Citrix Secure Private Access イベントは、Citrix Analytics と統合されました。Citrix Analytics は、管理者がイベントにアクセスしてダウンロードできるパブリックエンドポイントを提供します。これらのイベントは PowerShell スクリプトを介してアクセスできます。詳細については、エンタープライズ Web および SaaS アプリケーションアクセスの診断ログを参照してください。

  この機能は一般提供 (GA) が開始されました。

- **アダプティブ認証サービス**

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

Citrix Cloud のお客様は、Citrix Workspace を使用して、Citrix Virtual Apps and Desktops にアダプティブ認証を提供できるようになりました。アダプティブ認証は、Citrix Workspace にログインするお客様とユーザー向けに高度な認証を可能にする Citrix Cloud サービスです。アダプティブ認証サービスは、Citrix が管理し、Citrix Cloud でホストされる ADC です。詳細については、アダプティブ認証サービスを参照してください。

この機能はプレビュー版です。

16 February 2022

- **クライアント/サーバーアプリのサポート** Citrix Secure Private Access 内のクライアント/サーバーアプリケーションのサポートにより、リモートユーザー向けのすべてのプライベートアプリへのアクセスを提供するための従来の VPN ソリューションへの依存を排除できるようになりました。

  詳細については、クライアント/サーバーアプリのサポート - プレビューを参照してください。

11 October 2021

- **Citrix Gateway サービスタイルを Citrix Cloud の単一の Secure Private Access に統合**

  Citrix Gateway サービスタイルは、Citrix Cloud の単一の Secure Private Access に統合されました。

  - 「Citrix Workspace Essentials™」および「Citrix Workspace Standard」を含むすべての Secure Private Accessのお客様は、SaaSおよびエンタープライズWebアプリ、強化されたセキュリティ制御、コンテキストポリシー、さらにWebフィルタリングポリシーを構成するために、単一のSecure Private Accessタイルを使用できるようになりました。
  - すべてのCitrix DaaSのお客様は、引き続きWorkspace ConfigurationからCitrix Gateway サービスをHDXプロキシとして有効にできます。ただし、ゲートウェイサービスタイルからCitrix Gatewayサービスを有効にするショートカットは削除されました。Citrix Gateway サービスは、**StoreFront Cloud > Access > External Connectivity**から有効にできます。詳細については、「External connectivity」を参照してください。それ以外に機能の変更はありません。

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

30 July 2021

- **ユーザーの地理的位置に基づくエンタープライズWebおよびSaaSアプリのコンテキストアクセスとセキュリティ制御**

  Citrix Secure Private Accessサービスは、ユーザーの地理的位置に基づいて、エンタープライズWebおよびSaaSアプリへのコンテキストアクセスをサポートするようになりました。

- **Citrix Workspaceポータルから特定のWebまたはSaaSアプリを非表示にするオプション**

  管理者は、Citrix Workspaceポータルから特定のWebまたはSaaSアプリを非表示にできるようになりました。アプリがCitrix Workspaceポータルから非表示にされている場合、Citrix Gatewayサービスは列挙中にこのアプリを返しません。ただし、ユーザーは非表示のアプリに引き続きアクセスできます。

09 June 2021

- **アプリトラフィックをルーティングするルールを定義するルートテーブル**

  管理者は、ルートテーブルを使用して、アプリトラフィックをインターネットに直接ルーティングするか、Citrix Gateway Connector経由でルーティングするルールを定義できるようになりました。管理者は、トラフィックフローをどのように定義したいかに応じて、アプリのルートタイプをExternal、Internal、Internal-Bypass Proxy、またはExternal via Gateway Connectorとして定義できます。

22 May 2021

- **エンタープライズWebおよびSaaSアプリケーションへのコンテキストアクセス**

  Citrix Secure Private Accessサービスのコンテキストアクセス機能は、アプリケーションへのセキュアなアクセスを提供する包括的なゼロトラストアクセスアプローチを提供します。コンテキストアクセスにより、管理者は、ユーザーがコンテキストに基づいてアクセスできるアプリに対して、きめ細かなレベルのアクセスを提供できます。ここでの「コンテキスト」という用語は、ユーザー、ユーザーグループ、およびユーザーがアプリケーションにアクセスしているプラットフォーム（モバイルデバイスまたはデスクトップコンピューター）を指します。

- **Citrix Gateway Connectorユーザーインターフェイスのブランド変更**

  Citrix Cloud Gateway Connector™ユーザーインターフェイスは、Citrixのブランディングガイドラインに従ってブランド変更されました。

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

01 May 2021

- **Citrix Secure Private Accessサービスデータストアからの顧客データの削除**

  バックアップを含む顧客データは、サービス利用資格の有効期限が切れてから90日後にCitrix Secure Private Accessサービスデータストアから削除されます。

- **Azure ADからCitrix Workspaceへのドメインフェデレーション手順の簡素化**

  Azure ADからCitrix Workspaceアプリへのドメインフェデレーションの手順が簡素化され、Citrix Workspaceでのオンボーディングが迅速になりました。ドメインフェデレーションは、Citrix Gatewayサービスのユーザーインターフェイスのページから実行できるようになりました。

- **接続テストツールの機能強化**

  Citrix Gateway Connectorの接続テストツールが強化され、タイムアウトエラーの処理と必要なログの生成が可能になりました。

15 March 2021

- **プラットフォームの機能強化**

  お客様の管理者構成をCitrix Gateway Connectorに伝播する際の信頼性を高めるため、さまざまなプラットフォームの機能強化が行われました。

- **Webアプリのパフォーマンス向上**

  クライアントレスVPNを使用してシステムブラウザからWebアプリケーションにアクセスする際のWebアプリのパフォーマンスが向上しました。

- **Citrix Gateway ConnectorでTLS1.2 Grade A以上の暗号スイートを使用可能に**

  Citrix Gateway Connectorは、Citrix Cloudサービスおよびその他のバックエンドサーバーへの接続に、TLS1.2とGrade A以上の暗号スイートを使用するようになりました。

11 November 2020

- **Citrix Access Control™ サービスの名称変更**

  Access Control サービスは、現在 Secure Private Access に名称変更されました。

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

15 October 2020

- **Remote Browser Isolation サービス内で SaaS およびエンタープライズ Web アプリを起動するための強化されたセキュリティオプション**

  管理者は現在、強化されたセキュリティオプションである **Select Launch application always in Citrix Remote Browser Isolation™ service** を使用して、他の強化されたセキュリティ設定に関係なく、Remote Browser Isolation サービスで常にアプリケーションを起動できます。

08 October 2020

- **Citrix Secure Private Access ブラウザ拡張機能のセッションタイムアウトを構成する**

  管理者は現在、Citrix Secure Private Access ブラウザ拡張機能のセッションタイムアウトを構成できます。管理者は、Citrix Gateway サービスのユーザーインターフェイスにある **Manage** タブからこの設定を構成できます。

- **Citrix Secure Private Access ブラウザ拡張機能の管理者設定に対する RBAC 制御**

  Citrix Secure Private Access ブラウザ拡張機能の管理者設定に RBAC 制御が現在適用されています。

24 September 2020

- **ローカルブラウザを介してエンタープライズ Web アプリへの VPN なしのアクセスを有効にする**

  現在、**Citrix Secure Private Access** ブラウザ拡張機能を使用して、ローカルブラウザを介してエンタープライズ Web アプリへの VPN なしのアクセスを有効にできます。**Citrix Secure Private Access** ブラウザ拡張機能は、Google Chrome と Microsoft Edge の両方のブラウザでサポートされています。

07 July 2020

- **Citrix Gateway Connector で Kerberos 構成を検証する**

  Kerberos構成を検証するために、**シングルサインオン**セクションの**テスト**ボタンを使用できるようになりました。

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

19 June 2020

- **Citrix GatewayサービスおよびCitrix Secure Private Accessサービスの管理者への読み取り専用アクセス**

  Citrix Gatewayサービスを使用しているセキュリティ管理者チームは、Citrix GatewayサービスおよびCitrix Secure Private Accessサービスの管理者への読み取り専用アクセスなど、きめ細かな制御を提供できるようになりました。

  - Citrix Gatewayサービスへの読み取り専用アクセス権を持つ管理者は、アプリの詳細のみを表示できます。
  - Citrix Secure Private Accessサービスへの読み取り専用アクセス権を持つ管理者は、コンテンツアクセス設定のみを表示できます。

08 May 2020

- **Citrix Gateway Connector 13.0の新しいトラブルシューティングツール**

  - **ネットワークトレース: トレース**機能を使用して、Citrix Gateway Connectorの登録に関する問題をトラブルシューティングできるようになりました。トレースファイルをダウンロードして、トラブルシューティングのために管理者に共有できます。
  - **接続テスト: 接続テスト**機能を使用して、Gateway Connectorの構成にエラーがなく、Gateway ConnectorがURLに接続できることを確認できるようになりました。

V2019.04.02

- **Citrix Gateway ConnectorからアウトバウンドプロキシへのKerberos認証のサポート**

  Citrix Gateway ConnectorからアウトバウンドプロキシへのトラフィックでKerberos認証がサポートされるようになりました。Gateway Connectorは、構成されたプロキシ資格情報を使用してアウトバウンドプロキシに対して認証を行います。

V2019.04.01

- **Web/SaaSアプリのトラフィックを企業ネットワークでホストされているGateway Connector経由でルーティングできるようになり、2要素認証を回避できます。** 顧客が企業ネットワーク外でホストされているSaaSアプリを公開している場合、そのアプリのトラフィックをオンプレミスのGateway Connector経由で認証するためのサポートが追加されました。

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

例えば、顧客がOktaで保護されたSaaSアプリ（Workdayなど）を持っているとします。顧客は、実際のWorkdayデータトラフィックがCitrix Gatewayサービスを経由しない場合でも、Oktaサーバーへの認証トラフィックはオンプレミスのの Gateway Connectorを介してCitrix Gatewayサービスを経由するようにしたいと考えるかもしれません。これにより、ユーザーが社内ネットワーク内からOktaサーバーに接続しているため、顧客はOktaサーバーからの二要素認証を回避できます。

- **WebサイトリストのフィルタリングとWebサイトのカテゴリ分類の無効化**。管理者が特定の顧客に対してこれらの機能を適用しないことを選択した場合、WebサイトリストのフィルタリングとWebサイトのカテゴリ分類を無効にできます。

- **Remote Browser Isolationサービスのリダイレクトに対する自動地理ルーティング**。Remote Browser Isolationサービスのリダイレクトに対して、自動地理ルーティングが有効になりました。

V2019.03.01

- **「Gateway Connectorの追加」ページに「検出」ボタンが追加されました。** 「**検出**」ボタンは、コネクタのリストを更新するために使用され、新しく追加されたコネクタがWebアプリ接続セクションに反映されるようにします。

- **「アクセス制御Webフィルタリング」カテゴリに新しいカテゴリ「悪意のある危険なサイト」が追加されました。** 「**アクセス制御Webフィルタリング**」カテゴリに、「**悪意のある危険なサイト**」という新しいカテゴリが「**マルウェアとスパム**」グループの下に追加されました。

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

グーグル クローム エンタープライズ プレミアム との統合

以下のセクションでは、統合ソリューションの詳細について説明します。

ソリューションの概要

Citrixのお客様は、世界で最も人気があり安全なWebブラウザであるChromeを、使い慣れたエクスペリエンスで活用し、承認された企業Webアプリケーションにネイティブにアクセスできます。Citrix Secure Private Accessは、Secure Private Accessコンソールを通じて一元的に管理される管理者定義のポリシーに基づいて、アプリケーションごとの最小特権アクセスを適用します。管理者は、Secure Private Accessコンソールでエンタープライズアプリケーションドメインとゼロトラストアクセスポリシーを簡単に構成できます。ポリシーをモデル化してセキュリティの結果を検証およびテストし、適切なレベルのユーザーアクセスとエンドユーザーエクスペリエンスを提供できます。

この統合の利点は、Citrix Secure Private Accessインフラストラクチャを介した自動トラフィックステアリングにより、ChromeブラウザからプライベートWebアプリケーションおよびSaaSアプリケーションへのエージェントレスアクセスを提供することです。ユーザーがChromeを介してアプリケーションにアクセスすると、システムはGoogle Secure Gatewayを介してトラフィックをCitrix Secure Private Accessに自動的に送信します。これにより、ユーザーデバイスに追加のソフトウェアをインストールすることなく、安全で制御されたネットワークアクセスが保証されます。また、展開を簡素化し、IT管理を削減し、ユーザーエクスペリエンスを向上させ、IT運用を合理化します。

統合ソリューションには、次のコンポーネントが含まれています。

- Google Chrome Enterprise Premium (CEP)。これには、データ損失防止 (DLP)、マルウェアおよびフィッシング対策、URLフィルタリング、Google管理コンソールなどの機能が含まれます。
    - クライアントマシンでローカルに実行されているGoogle Chromeブラウザは、Chrome管理プロファイルを介したユーザーレベルごとのポリシー適用により、セキュアブラウザとして機能します。

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

  - Google Cloudポータルを介してアクセスされるGoogle Chrome Enterprise Premiumコンソールは、Chrome Enterprise Premiumセキュリティポリシーの管理、運用、および監視コンソールを提供します。

- Citrix Secure Private Access。これには、クラウドインフラストラクチャ、ZTNAポリシーエンジン、および顧客環境に展開されたコネクタアプライアンスへのアクセスが含まれます。
- プライベートアプリケーションへのゼロトラストアクセスポリシー用のSecure Private Accessコンソールと、監視およびトラブルシューティング用のCitrix Monitorを含むCitrixコンソール。

Citrix Secure Private Accessサービスは、管理者が構成したすべてのアクセスポリシーを適用し、ユーザーが特定のWebアプリケーションにのみアクセスできるようにします。

Chrome Enterprise Premiumの高度なセキュリティ機能

以下は、Chrome Enterprise Premiumが提供する高度なセキュリティ機能の一部です。

- **データ損失防止 (DLP)**: 機密データが漏洩したり誤って共有されたりするのを防ぐために、きめ細かな制御とポリシーを実装します。
- **マルウェアの詳細スキャン**: 高度なスキャン技術を使用して、未知または高リスクのファイルを検出して隔離し、悪意のあるコードの実行を防ぎ、ゼロデイ攻撃から保護します。
- **フィッシング対策**: フィッシングの試みを特定してブロックすることで、ユーザーが有害なWebサイトにアクセスするのを保護し、ログイン資格情報や個人情報の盗難を防ぎます。
- **URLの分類とフィルタリング**: コンテンツカテゴリに基づいてWebサイトへのアクセスを制限し、ユーザーが不適切または悪意のあるコンテンツにアクセスするのを防ぎます。
- **Web使用状況のインサイトと分析**: Webトラフィックに関する詳細なレポートと分析を提供し、管理者がユーザーアクティビティを監視し、潜在的なセキュリティ脅威を特定し、ネットワーク帯域幅を最適化できるようにします。

詳細については、Chrome Enterprise Premiumの概要を参照してください。

Chrome Enterprise向けCitrix Secure Accessコントロール

Secure Private AccessとChrome Enterprise Premiumの統合により、次の付加価値機能がサポートされます。

- **RDP** - ブラウザ内で直接、安全なRDPセッションを有効にします。詳細については、リモートデスクトップコントロールを参照してください。
- **SSH** - ブラウザ内でSSHアプリへの安全なアクセスを有効にします。詳細については、SSHコントロールを参照してください。

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

- **キーロギング対策** - CEPでリソースにアクセスする際のキーロガーを防ぎます。詳細については、キーロギング対策コントロールを参照してください。
- **クリップボードコンテナ** - ブラウザと仮想化アプリケーション間のクリップボード共有を制限または許可します。詳細については、クリップボードコンテナコントロールを参照してください。
- **セッション記録** - ブラウザ内でユーザーセッションを記録します。詳細については、セッション記録コントロールを参照してください。
- **ブラウザセッションの再認証** - 設定された時間間隔の後、ブラウザセッションの定期的な再認証を強制します。詳細については、ブラウザセッション再認証コントロールを参照してください。
- **ドメインサフィックス** - 短いURLにドメインを追加することで、ユーザーエクスペリエンスを最適化します。詳細については、Webアプリケーションのドメインサフィックスを参照してください。

統合を成功させるための前提条件

Citrix Workspace™アプリとChrome Enterprise Premium間の最適な統合を確保するには、以下の前提条件を満たす必要があります。これらの前提条件を正常に完了すると、Citrix Workspaceアプリまたは Webベースのユーザーインターフェイスからアプリケーションを起動する際の効率とシームレスなエクスペリエンスが向上します。

前提条件は、大まかに以下のカテゴリに分類されます。

- ライセンス、アプリのバージョン、および拡張機能
- Google管理コンソール
- セキュアプライベートアクセスサービス
- Chromeブラウザ
- Citrix Workspaceで構成されたユーザーディレクトリとGoogle Cloudユーザーディレクトリの同期

Citrix Secure Private Access - サポートされている展開モード

統合ソリューションは、Citrix Secure Private Accessから以下の展開モードをサポートしています。

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

- **Citrix Secure Private Accessサービス**: この展開モードでは、コントロールプレーンとゲートウェイインフラストラクチャを含むすべてのコンポーネントがCitrix Cloudでホストされます。詳細については、「Citrix Secure Private Access」を参照してください。
- **Citrix Secure Private Accessハイブリッド展開**: この展開により、お客様はオンプレミスのStoreFrontおよびNetScaler Gatewayコンポーネントを使用してZero Trust Network Access (ZTNA) ソリューションを実装し、Citrix Cloudを構成、管理、および監視機能に使用できます。これは、お客様が既存のオンプレミスNetScaler Gatewayを活用してユーザーのトラフィックルーティングを制御しつつ、Citrix Cloudでホストされているを構成とポリシーの管理に使用し、さらにCitrix Cloudでホストされているを監視およびトラブルシューティング機能に使用できることを意味します。詳細については、「Citrix Secure Private Accessハイブリッド展開」を参照してください。

重要:

Chrome Enterprise Premium (CEP) では、HTTPSエンタープライズWebアプリとSaaSアプリのみがサポートされています。HTTPエンタープライズWebアプリとSaaSアプリはサポートされていません。

法的情報

Chrome Enterprise PremiumはGoogle LLCによって提供されており、その使用はGoogleの許容使用ポリシーおよびサービス固有の規約に準拠します。

関連トピック

- Secure Private Access のオンボーディングとセットアップ(/ja-jp/citrix-secure-private-access/service/admin-guided-workflow-for-easy-onboarding-and-setup.html)
- オンボーディング後の Google 統合詳細の更新(/ja-jp/citrix-secure-private-access/service/admin-guided-workflow-for-easy-onboarding-and-setup.html#update-google-integration-details-post-onboarding)
- アプリの構成と管理(/ja-jp/citrix-secure-private-access/service/add-and-manage-apps.html)
- 技術概要: Chrome Enterprise との Citrix Secure Access(https://community.citrix.com/tech-zone/learn/tech-briefs/csa-ce/)

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

統合ソリューションの前提条件

Citrix Workspace™アプリケーションとChrome Enterprise Premium間の最適な統合を確保するには、以下の前提条件を実装する必要があります。これらの前提条件を正常に完了すると、Citrix WorkspaceアプリまたはWebベースのユーザーインターフェイスからアプリケーションを起動する際に、より効率的でシームレスなエクスペリエンスが得られます。

前提条件は、以下のカテゴリに大別されます。

- ライセンス、アプリのバージョン、および拡張機能
- Google 管理コンソール
- セキュア プライベート アクセス サービス
- Chromeブラウザ
- ユーザーの管理
- ユーザーディレクトリの関連付け
- TLSインスペクションのバイパス

ライセンス、アプリのバージョン、および拡張機能

- **Chrome Enterprise Premiumライセンス**: Citrix Cloud Platform License (CPL) プログラムを通じて利用可能な、アクティブなChrome Enterprise Premiumライセンスがあることを確認してください。
- **Citrix Workspaceアプリ (CWA) のバージョン**:
  - Windows: 2025.07以降
  - macOS: 2025.08以降
  - ChromeOS: 25.7.0.25 以降

> **注記:**
>
> Citrix Workspace アプリは、このソリューションのオプション要件です。

- **Citrix Endpoint Analysis (EPA) クライアントバージョン:**
  - Windows: 25.9.1.9 以降
  - macOS: 25.10.3 以降

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

> **注記:**
>
> 定期的なデバイスポスチャスキャンをサポートするために、Windows EPAクライアントを管理者モードでインストールすることをお勧めします。さらに、デバイスポスチャの**設定**ページで定期的なデバイスポスチャスキャンを有効にする必要があります。詳細については、「デバイスの定期スキャン」を参照してください。

- **Chromeブラウザのバージョン**: エンドポイントは、最新のGoogle Chromeバージョンを使用する必要があります。
- **オペレーティングシステム**: Windows、macOS、ChromeOS。

Google 管理コンソール

- **Google顧客ID**: Google 管理コンソールからGoogle顧客IDを取得します。このIDは、Google サービスと統合を構成するために必要です。顧客IDは、Google 管理コンソールの**アカウント > アカウント設定**から取得できます。
- **Google 管理コンソールでカスタムロールを作成する**: Chrome Enterprise Premium (CEP) に顧客をオンボーディングし、Google Chrome統合を有効にするには、管理者はGoogle 管理コンソールでカスタムロールを作成し、適切な権限を割り当てる必要があります。詳細については、「管理者ロールと権限」を参照してください。
- **DevTools拡張機能を制限する**: 機密データの漏洩を防ぐため、強制インストールされた拡張機能のChrome DevToolsは無効にする必要があります。これは、Google 管理コンソールのデフォルトオプションです。

セキュア プライベート アクセス サービス

- **IPv6エンドポイントの制限事項**: Google Cloudエンドポイントと統合されたCitrix Secure Private Accessサービスは、IPv6アドレスを持つエンドユーザーデバイスからトラフィックを受信する場合があります。現在、Secure Private Accessの地理的位置およびネットワーク位置アクセスポリシーはIPv6をサポートしていません。

  その結果、地理的位置またはネットワーク位置の条件を持つアクセスポリシーは、IPv6アドレスを持つエンドユーザーデバイスでは失敗する可能性があります。これらの条件を利用しない他のアクセスポリシーは、IPv4およびIPv6対応のエンドユーザーデバイスの両方で機能します。
- **CEPのアクセス制限はGoogle管理コンソールで設定されるようになりました**: 以前Secure Private Accessコンソールで構成されていたアクセス制限は、Citrix Enterprise Browserにのみ

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

適用されます。Google Chromeがエンタープライズブラウザである場合、アクセス制限はGoogle管理コンソールでポリシーおよびルールとして構成する必要があります。

- ポリシーは、**Google管理コンソール > デバイス > Chrome > 設定**で構成されます。これらの設定により、JavaScriptのブロックやプリンターの許可リストなど、ブラウザの設定を管理できます。
- ルールは、**Google管理コンソール > ルール**で構成されます。これらのルールは、透かしの追加、社会保障番号を含むファイルのダウンロードのブロック、URLフィルタリングなど、DLPに関連する高度な設定です。

Google Workspace管理コンソールでポリシーとルールを作成する方法の詳細については、以下のトピックを参照してください。

- Chrome EnterpriseコネクタポリシーをChrome Enterprise用に設定する
- データ保護ルール

グーグル クローム

管理対象Chromeプロファイル: すべてのエンドユーザーは、管理対象プロファイルを使用してChromeにアクセスする必要があります。管理対象プロファイルにより、Chromeのポリシー、拡張機能、およびセキュリティ設定がユーザーデバイスに適用されます。

ユーザーの管理

シームレスな統合のためには、Citrix Secure Private AccessとGoogle Identity (Directory) で構成されたユーザー間に相関関係が必要です。これにより、承認されたユーザーのみが割り当てられたアプリケーションにアクセスできるようになります。統合でサポートされているユーザーディレクトリは次のとおりです。

- アクティブ ディレクトリ
- マイクロソフト エントラ ID (旧称: アジュール アクティブ ディレクトリ)

必須 - ユーザーのメールアドレスフィールドに入力する

Google Identityにはメールアドレスフィールドの入力が必要です。この目的のために、Secure Private Accessで使用されるディレクトリ内のユーザーオブジェクトは、次のいずれかを持っている必要があります。

- Google管理コンソールで設定および検証されているドメイン部分を持つメールアドレス。たとえば、メールアドレス `alice@example.com` を持つ `Alice` は、Google Identityで `alice@example.com` としてマッピングされます。

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

- Google管理コンソールで設定されていないドメイン部分を持つメールアドレス。たとえば、`Bob` はメールアドレス `bob@example.internal.net` を持っていますが、これはGoogleで設定されていません。この場合、`example.com` が検証済みドメインであるため、彼はGoogle Identityで `bob@example.com` としてマッピングされます。
- ドメインマッピングの目的でメールアドレスがない場合に使用できる別のディレクトリフィールド。一般的なアプローチは、ドメイン置換の有無にかかわらず、ユーザープリンシパル名 (UPN) を活用することです。たとえば、`Charlie` はUPN `charlie@ADdomain.com` を持ち、Google Identityで `charlie@example.com` としてマッピングされます。

Secure Private AccessディレクトリとGoogleディレクトリのメールアドレスが一致しないユーザーには、重大な制限があります。詳細については、ドメインマッピングの考慮事項 セクションを参照してください。

必須 - ユーザーグループのメールアドレスフィールドに入力する

ユーザーと同様に、Secure Private Accessで使用されるディレクトリ内のグループオブジェクトは、次のいずれかを持っている必要があります。

- Google管理コンソールで設定および検証されているドメイン部分を持つメールアドレス。
- Google管理コンソールで設定されていないドメイン部分を持つメールアドレス。
- ドメインマッピングの目的でメールアドレスがない場合に使用できる別のディレクトリフィールド。一般的なアプローチは、共通名 (CN) を活用し、Google Directoryに適切なドメインを追加することです。たとえば、CN `group1` を持つグループは、Google Identityで `group1@example.com` としてマッピングされます。

メールアドレスの欠落または不整合に関するドメインマッピングの考慮事項

ユーザー:

ユーザーのメールアドレスがSecure Private Accessディレクトリにない場合、またはSecure Private AccessディレクトリとGoogle Identityの間で一貫性がない場合、以下の考慮事項が適用されます。

- メールアドレスを持たないユーザーは、Secure Private Accessコンソール内でSecure Private Accessポリシーを設定する際に選択できません。
- Secure Private AccessディレクトリとGoogleディレクトリの間でメールアドレスが一致しないユーザーのSecure Private Accessポリシーは機能しません。
- これらのユーザーに対して、クラウドストアからWebまたはSaaSアプリを起動すること（Citrix WorkspaceアプリまたはWebブラウザを使用）はサポートされていません。

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

グループ:

グループのメールアドレスがSecure Private Accessディレクトリにない場合、またはSecure Private Accessディレクトリと Google Identityの間で一貫性がない場合は、Secure Private Accessのグループレベルポリシーが正しく機能するように、適切なドメインマッピング構成が必要です。

Citrix Secure Private Accessで構成されたユーザーディレクトリをGoogle Cloudユーザーディレクトリと関連付ける

Citrix Secure Private Accessで構成されたユーザーディレクトリをGoogle Cloudディレクトリと関連付ける必要があります。具体的には、以下のユーザーディレクトリがサポートされています。

- アクティブディレクトリ
- マイクロソフト エントラ ID（旧称：アジュール アクティブ ディレクトリ）
- オクタ

アプリケーションアクセスが適切に適用されるように、ユーザーディレクトリの関連付けは定期的に行う必要があることに注意してください。関連付けに必要な属性は最小限のセットのみです。

アクティブディレクトリ

Active Directoryの場合、名前、メールアドレス、オブジェクトグローバル一意識別子 (objectGUID)、およびセキュリティ識別子 (SID) を関連付ける必要があります。パスワードおよびその他のすべての属性は、Google Cloud Directoryと関連付ける必要はありません。

カスタムスキーマ `citrix-schema` の下にカスタムADフィールドを含めるようにADをGoogle Cloudと関連付ける方法の詳細については、「Citrix CloudへのIDプロバイダーとしてのGoogle Cloud Identityの接続」および「Active Directoryユーザーアカウントのプロビジョニング」を参照してください。

マイクロソフト Entra ID

GoogleとMicrosoftの両方のクラウドプラットフォームでユーザーとグループを管理するために、Microsoft Entra IDをGoogle Cloudユーザーディレクトリと同期する必要があります。詳細については、「Microsoft Entra ID (旧Azure AD) ユーザープロビジョニングとシングルサインオン」を参照してください。

同期を構成する際には、以下の要件を考慮する必要があります。

- **メールアドレス:** すべてのユーザーとグループに対して、メールアドレスフィールドが入力されている必要があります。詳細については、「ユーザーの管理」を参照してください。

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

- **objectId属性マッピング:** Entra IDユーザーのobjectId属性は、Google Directoryにマッピングする必要があります。

  このマッピングは、G-Suiteコネクタの設定で行います。

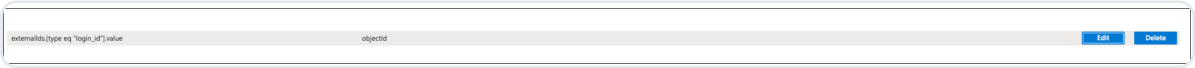
  a. 左側のメニューから、 **>** をクリックします。

  b. 新しいメニューで、 **>** をクリックします。

  c. をクリックします。

  d. objectIdの適切な行を見つけます。

     - をクリックし、 で **externalIds**..value を選択します。
     - 結果として得られる構成が次のスクリーンショットと一致することを確認します。



- **シングルサインオン:** シングルサインオン (SSO) の構成はオプションです。Googleディレクトリで個別のパスワードを設定するか、Entra IDでSSOを設定するか、またはCitrix IdentityによるOpen ID ConnectでSSOを設定できます。

オクタ

OktaからGoogle Cloudユーザーディレクトリ (Cloud Identity / Google Workspace) にユーザーとグループをプロビジョニングすることで、OktaをIDソースとして使用できます。プロビジョニングされると、Secure Private Accessとの関連付けは、他のサポートされているディレクトリと同じモデルに従います。最小限の属性セットのみが必要であり、すべてのユーザーとグループに対してメールアドレスフィールドが入力されている必要があります。

OktaからGoogleへのプロビジョニングの詳細については、「Oktaユーザープロビジョニングとシングルサインオン」を参照してください。同じガイドに従ってOktaに対するSSOを設定するか、「Citrix WorkspaceによるOpen ID Connect」を参照してください。

グーグル クラウド アイデンティティ（グーグル ディレクトリ）

Google Cloud IdentityがすでにIDプロバイダーである場合、ユーザーとグループはGoogle Cloudディレクトリにネイティブに存在します。Googleと照合する別の外部ディレクトリがないため、ディレクトリの関連付けや同期は必要ありません。Googleは、Citrix WorkspaceとChrome管理プロファイルの両方にとってIDのソースです。

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

注:

Chrome Enterprise Premiumのデバイスポスチャサービス統合は、Google Cloudディレクトリがcitrix Workspaceに対して依拠当事者として機能するOpenID Connect (OIDC) フローに依存しています。Google Cloud Identity自体が基盤となるIdPである場合、このフローはサポートされません。したがって、この構成ではデバイスポスチャサービス統合は利用できません。

TLS検査のバイパス

TLS検査（またはSSL検査）を使用するネットワークでChrome Enterprise Premiumエンドポイントが正しく機能するようにするには、以下のホスト名を検査から除外する必要があります。

- `ingress.cloudproxy.app`
- `securegateway.goog`
- `*.securegateway.goog`

多くのTLS検査ソリューション（SSEベンダーやプロキシサーバーなど）は、Chrome Enterprise Premiumが使用するHTTP CONNECTメソッドを完全にサポートしていないため、トラフィックが突然切断される可能性があるため、この除外は不可欠です。

さらに、潜在的なエンドユーザーのパフォーマンス問題や接続遅延を避けるために、以下のホスト名をTLS検査から除外することをお勧めします。

- `safebrowsingrealtime.googleapis.com`
- `secureconnect-pa.clients6.google.com`
- `secureconnect-pa.mtls.clients6.google.com`
- `secureconnect-pa.googleapis.com`
- `chromereporting-pa.googleapis.com`

管理者の役割と権限

Citrixサービスアカウントは、Secure Private Accessによって、ユーザーをChrome Enterprise Premium (CEP) にオンボーディングし、CEP統合を有効にするために使用されます。したがって、Google管理コンソールで、必要な権限を持つ役割をサービスアカウントに割り当てる必要があります。

Google管理コンソールでは、2種類の役割を利用できます。

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

システムロール: これらはGoogleが提供するデフォルトの役割です。スーパー管理者ロールを除き、残りのシステムロールには、Secure Private AccessとのCEP統合に必要なすべての権限は含まれていません。

カスタムロール: これらはAdmin API権限の任意のサブセットを含むことができます。Secure Private AccessとのCEP統合に必要なすべての権限を含むカスタムロールを作成する必要があります。

このタスクを実行するには、スーパー管理者としてGoogle管理コンソールにサインインしている必要があります。

注:

スーパー管理者ロールはサービスアカウントに割り当てることはできません。

Googleカスタム管理者ロールの権限

CEPとSecure Private Accessの統合には、CitrixサービスアカウントがGoogle管理コンソールで以下の特定の権限を持つカスタムロールを持っている必要があります。

必要な管理者権限	この権限が必要な理由
顧客の管理 > 顧客の読み取り	Google顧客組織のフレンドリ名を読み取るため。
組織部門 > 読み取り	設定された組織部門がGoogleディレクトリで利用可能であることを確認するため。
サービス > Chrome管理 > 設定 > ユーザー設定の管理 **注:** トップレベルの権限である **ユーザー設定の管理** と、サブ権限である (**アプリケーション設定の管理** および **Web設定の管理**) を必ず選択してください。	ユーザープロファイルでCEPとSPAの統合に必要な必須の拡張機能とその構成を追加するため。
サービス > Chrome管理 > 管理対象ブラウザの設定 > 読み取り	管理対象のChromeプロファイルと管理対象のブラウザを読み取るため。

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

必要な管理者権限	この権限が必要な理由
ライセンス管理 > 読み取り	組織にプロビジョニングされたChrome Enterprise Premiumが割り当てられたライセンスの総数を照会するため。
レポート	割り当てられたライセンスを積極的に使用しているユーザーを読み取るため。 データ損失防止 (DLP) ルールがトリガーされたときのアクティビティイベントを読み取るため。 失敗イベントを読み取るため。
グループ > 読み取り	構成された統合グループがGoogleディレクトリで利用可能であることを確認するため。
サービス > アラートセンター > フルアクセス > 表示アクセス	データ損失防止のセキュリティアラートとログイン失敗イベントを読み取るため。
デバイスと設定の管理	デバイスのメタデータを読み取り、モニターのネットワークトポロジビューに表示するため。
ユーザー > 読み取り	構成された統合ユーザーがGoogleディレクトリで利用可能であることを確認するため。

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

注:

- これらの管理者権限に対して、同等のOAuthスコープを付与することも必要です。
- すべての管理権限は、**管理者権限**セクションにあります。これには、以前は**管理コンソール権限**および**管理API権限**セクションにリストされていた権限が含まれます。この変更は、権限の割り当て方法には影響せず、既存の権限は以前と同様に機能し続けます。
- 最上位の権限である**ユーザー設定の管理**と、サブ権限（**アプリケーション設定の管理**および**Web設定の管理**）を選択していることを確認してください。サブ権限のみを選択するだけでは不十分です。
- Citrix Secure Private Accessは、構成されたCitrixサービスアカウントを使用して、Googleアカウントに構成を展開します。Citrix Secure Private AccessとGoogle CEPの統合が完了したら、Google管理コンソールを開き、**Chromeブラウザ > アプリと拡張機能**に移動します。いくつかのブラウザ拡張機能がルート組織レベルで構成されていることに注意してください。これらは子OUに継承されます。ユーザーがこのテナントでGoogle Chromeプロファイルをオンボードすると、これらの拡張機能が自動的にプロビジョニングされます。

ロールと権限の作成と割り当て

カスタム管理者ロールを作成し、権限を割り当てるには、次の手順を実行します。

1. Google管理コンソールで、**アカウント** > **管理者ロール**に移動します。
2. **新しいロールを作成**をクリックし、ロールの名前と説明を入力します。
3. Google Chrome統合に必要なすべての権限をこのカスタムロールに追加します。必要な権限のリストについては、「Googleカスタム管理者ロールの権限」を参照してください。

   ロールと権限に関する詳細については、「Googleドキュメント」を参照してください。
4. カスタムロールを保存します。

エグレスハブリージョンの構成

Secure Private Accessを使用すると、管理者はChrome Enterprise PremiumがSaaSアプリケーションのトラフィックに使用するエグレスリージョンを選択できます。選択された各リージョンは、専用のエグレスIPアドレスセットを提供し、管理者はこれをSaaSアプリケーションの許可リストに追加して、Google Secure Gatewayを介してルーティングされるトラフィックを許可できます。この機能は、クラウド展開とハイブリッド展開の両方で利用できます。

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

SaaSアプリケーションのエグレスリージョンパネルには、次のいずれかのパスからアクセスできます。

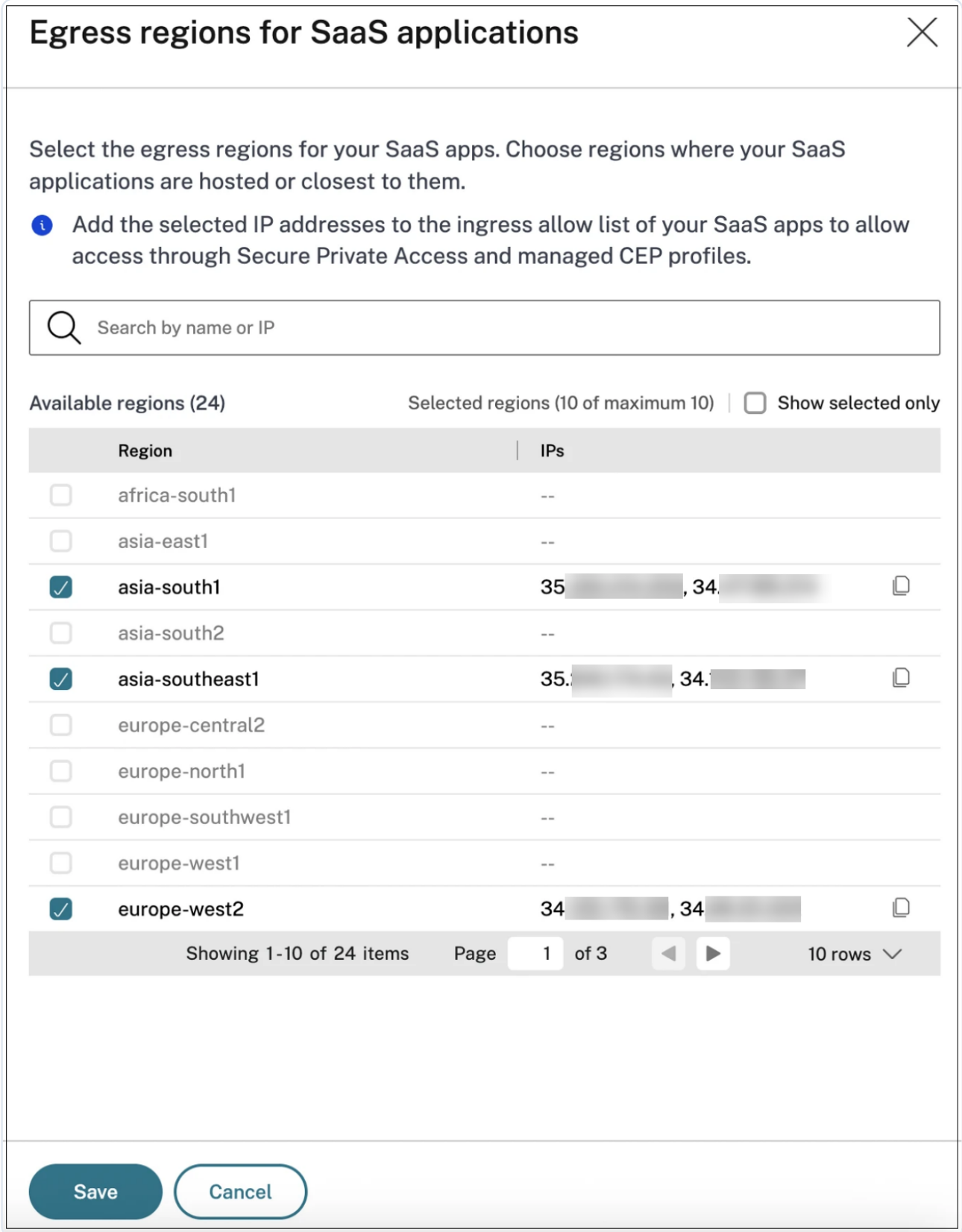
- Chrome Enterprise Premiumセットアップカードの**エグレスリージョンの管理**ボタンをクリックします。

- **ブラウザ設定 > ブラウザ構成 > SaaSアプリケーションのエグレスリージョン**で**編集**をクリックします。

SaaSアプリケーションのエグレスリージョンパネル

SaaSアプリケーションのエグレスリージョンパネルには、利用可能なエグレスリージョンと、選択された各リージョンに関連付けられたIPアドレスが表示されます。リージョンを名前またはIPアドレスで検索し、リージョンのIPアドレスをコピーして、SaaSアプリケーションの許可リストに追加できます。

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



IPアドレスは、リージョンを選択し、変更を保存し、Googleが展開を完了した後にのみ利用可能になります。展開が完了するまで、新しく選択されたリージョンにはIPアドレスが表示されません。展開には通常数分かかりますが、正確な時間は異なる場合があります。

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

リージョンの選択

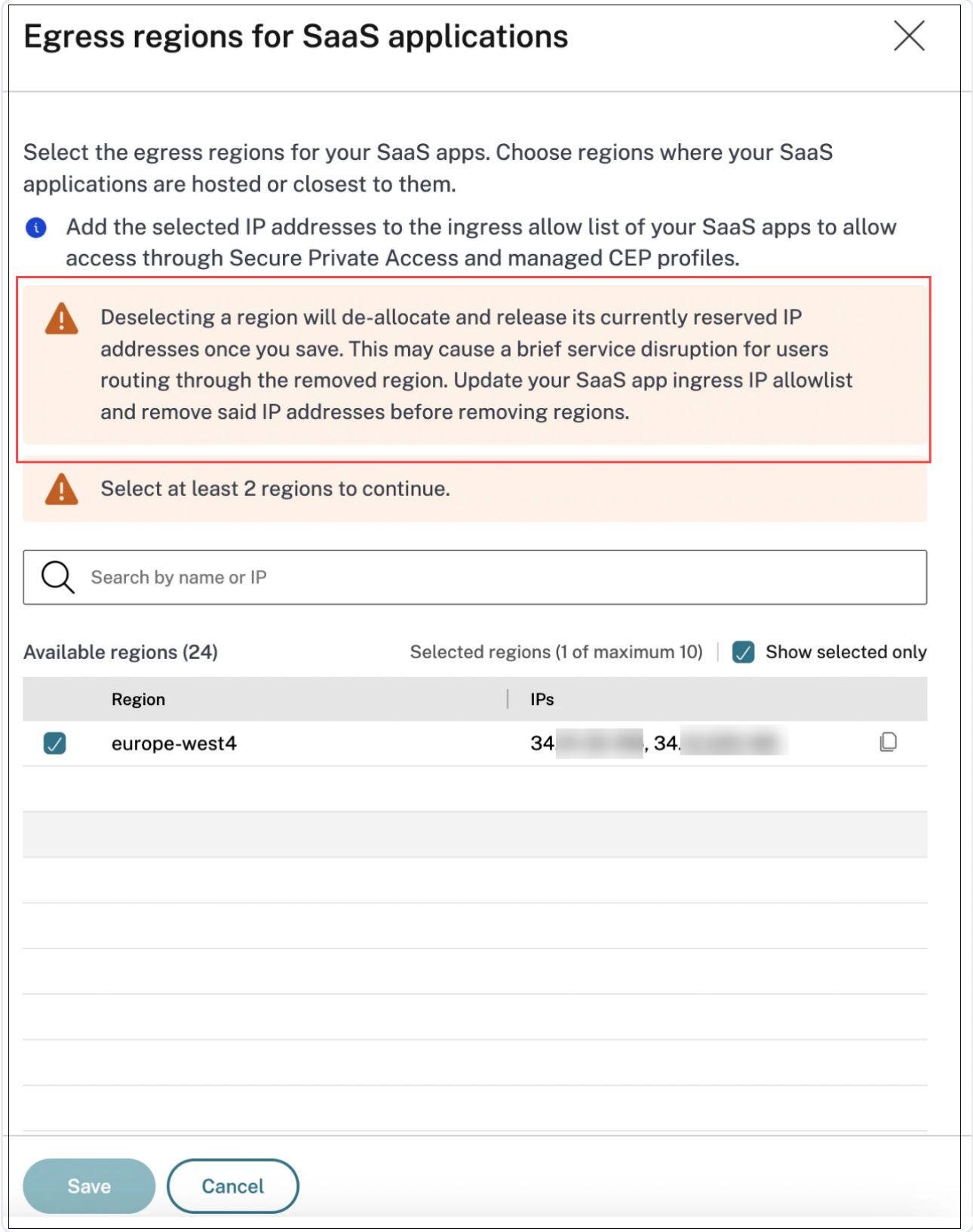
SaaSアプリケーションがホストされているリージョン、またはそれらに最も近いリージョンを選択します。リージョンの障害発生時に冗長性を確保するため、少なくとも2つのリージョンを選択してください。最大10のリージョンを選択できます。

Googleが選択されたリージョンを展開し、関連するIPアドレスが利用可能になったら、それらのIPアドレスをSaaSアプリケーションのイングレス許可リストに追加します。

リージョンの選択解除

リージョンの選択を解除すると、警告メッセージが表示されます。

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



変更を保存する前に、SaaSアプリケーションの許可リストを更新する必要があります。**キャンセル**を選択した場合、すべての変更は破棄されます。

後で同じリージョンの選択を解除して再度選択すると、Googleは新しいエグレスIPアドレスのセットを割り当てます。これらのIPアドレスは通常、以前に割り当てられたものとは異なるため、SaaSアプリケーションの許可リストをそれに応じて更新する必要があります。

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

メールアドレスを持たないユーザーグループのドメインマッピング

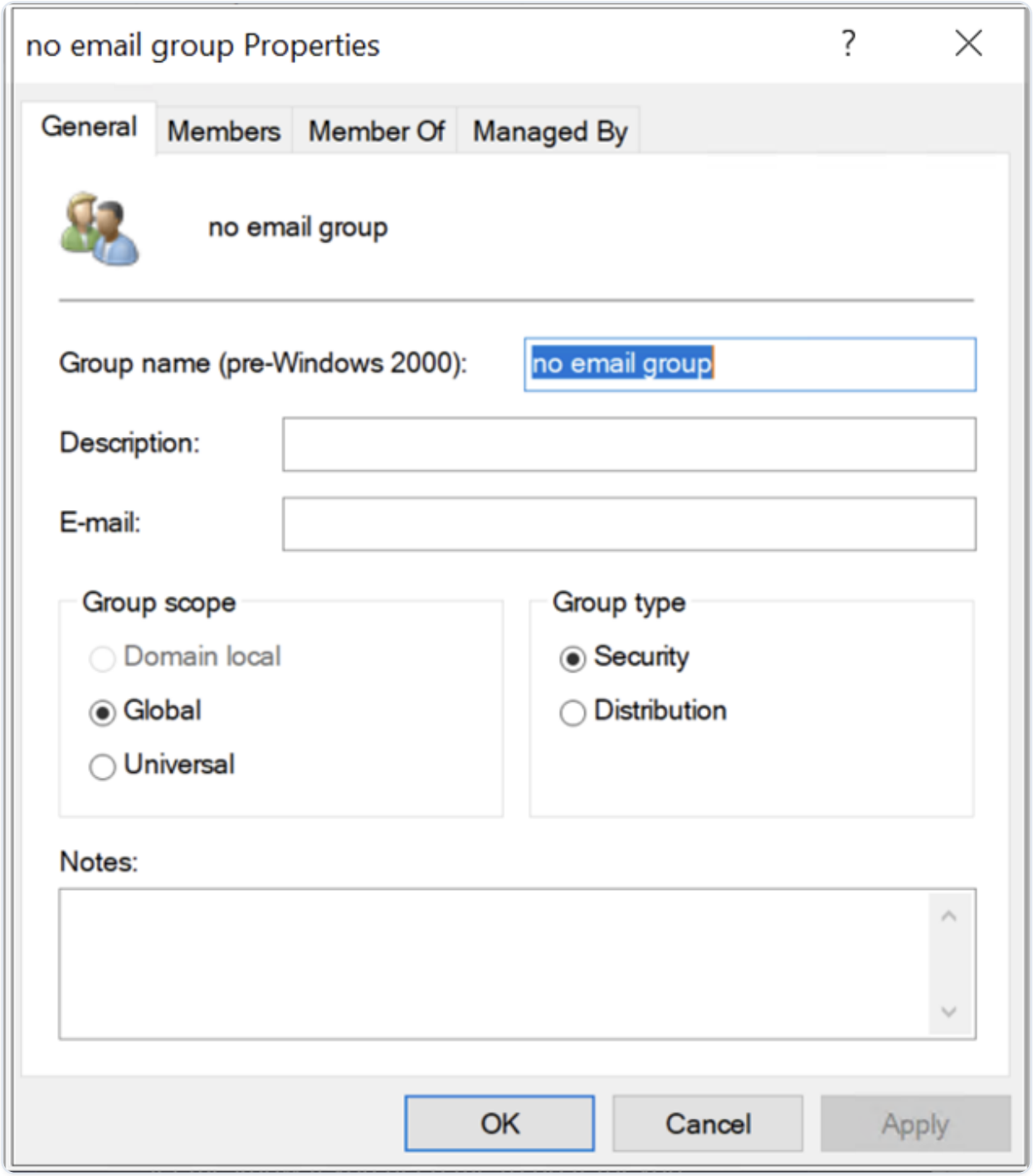
Googleディレクトリでは、すべてのユーザーおよびグループオブジェクトに対して検証済みのメールアドレスが必要です。しかし、Secure Private Accessがサポートするディレクトリ、特にActive Directory (AD) およびMicrosoft Entra IDでは、これが常に利用できるとは限りません。ADおよびMicrosoft Entra IDのオブジェクトにはメールアドレスがないか、Googleディレクトリが検証できない内部ドメインまたは特殊なドメイン（例: @fabrikam.onmicrosoft.com）を指すメールアドレスが設定されている場合があります。

通常、メールアドレスはSecure Private AccessとGoogleディレクトリ間の共通識別子として機能するため、検証済みのGoogleメールアドレスを持たないAD/Entraのグループは、Secure Private Accessポリシーでは通常サポートされません。ドメインマッピング機能は、メールアドレスがないグループや、未検証のドメインを持つメールアドレスを持つグループに対しても管理者がポリシーを設定できるようにすることで、この問題を解決します。

ドメインマッピングの仕組み

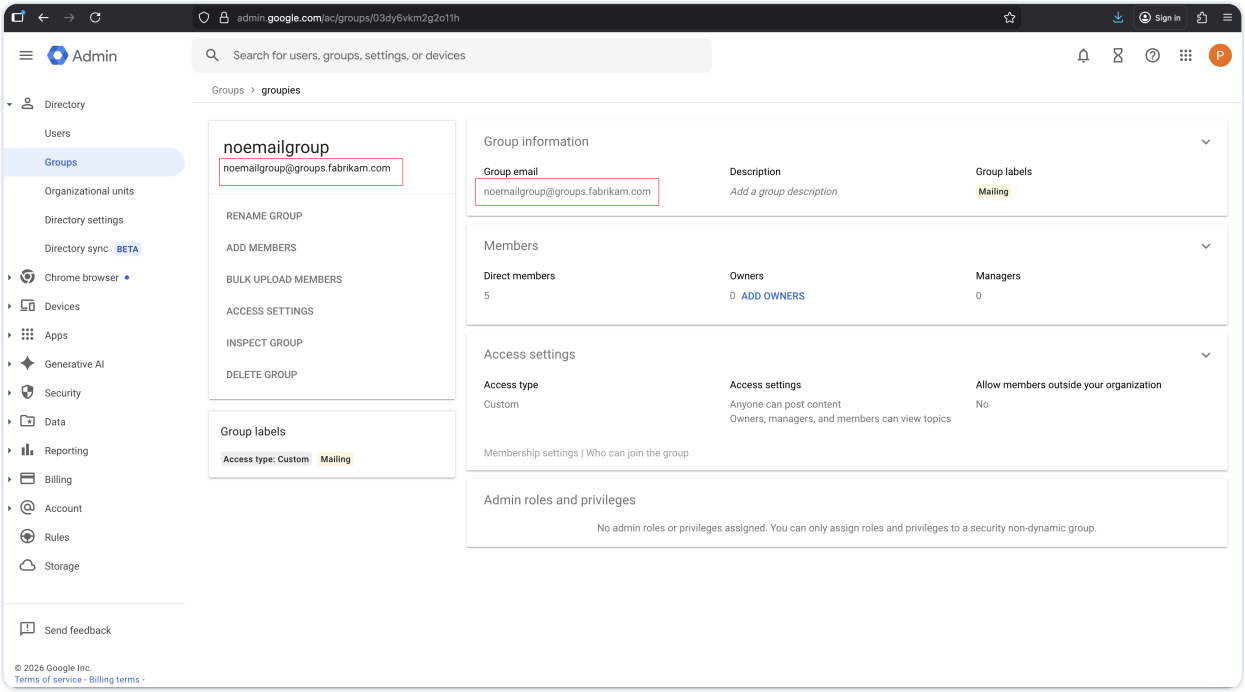
- メールアドレスを持たないAD内のグループを考えてみましょう。

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



- このグループは、グループの共通名（メールアドレスでは「スペース」がサポートされていないため省略されます）と検証済みのGoogleドメイン `@groups.fabrikam.com` によって合成されたメールアドレスでGoogleディレクトリに複製されます。有効なGoogleグループのメールアドレス `noemailgroup@groups.fabrikam.com` は、ソースディレクトリには存在しません。

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



- 管理者は、メールアドレスを持たないグループに対してドメインマッピングを設定できます。

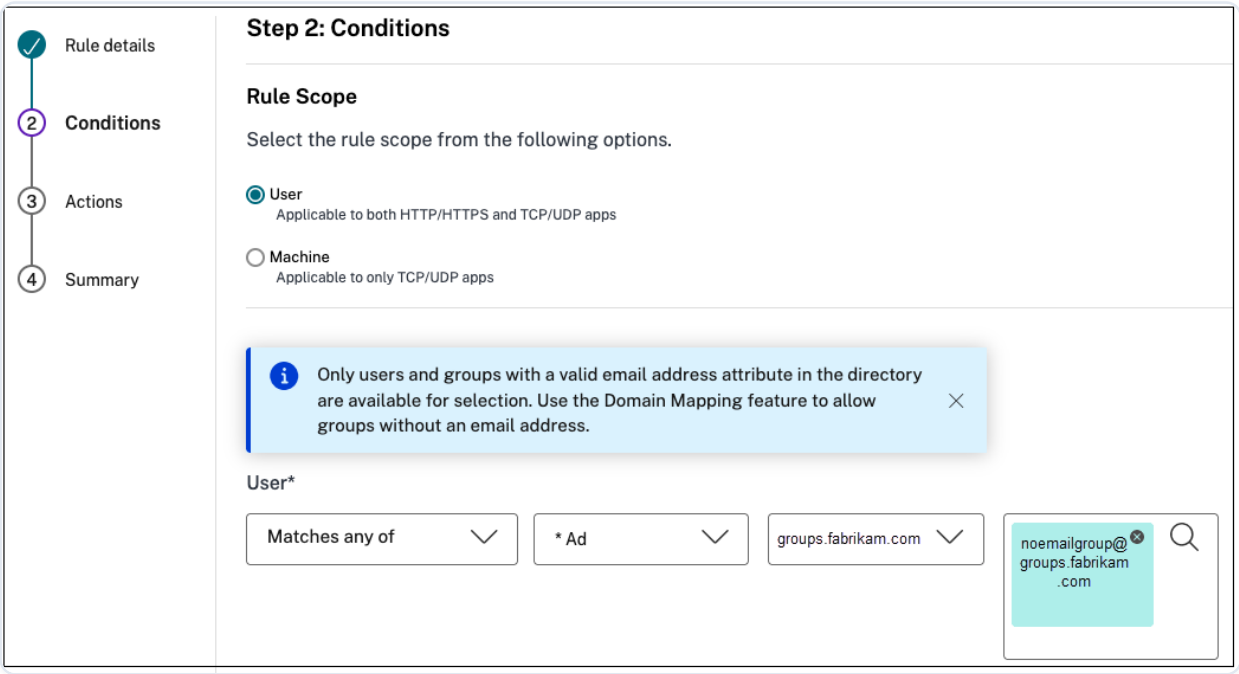
  a. Secure Private Access管理コンソールで、**ブラウザ設定 > ドメインマッピング** に移動します。

  b. **空のドメインを含める** トグルをオンにして、メールアドレスを持たないグループのマッピングを有効にします。

  c. **Googleドメイン > ドメイン** フィールドに、ターゲットグループドメイン（この例では `groups.fabrikam.com`）を入力します。ターゲットグループドメインを追加することで、管理者はポリシーを設定する際に、メールアドレスを持たないグループを適切なGoogleドメインのメールアドレス（`groups.fabrikam.com`）にマッピングできるようになります。

ポリシーにグループを割り当てる際、メールアドレスを持たないグループ（`noemailgroup`）を検索すると、ドメインマッピングの設定に基づいてメールアドレスが合成され、`noemailgroup@groups.fabrikam.com` が利用可能になります。この変換は、事前に定められた変換ロジックに基づいています。詳細については、「メールアドレスの構成」を参照してください。

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



メールアドレスの構成

- 既存のメールアドレスを持たないグループの場合：
  - メールアドレスのローカルパートは、グループの共通名 (cn) の小文字バージョンを使用して入力され、「スペース」文字は省略されます。
  - メールアドレスのドメインパートは、Google ドメイン (google-domain) の小文字バージョンを使用して入力されます。
  - ドメインの選択（複数の Google ドメインが存在する場合）：グループが複数の Google ドメインに関連付けられている場合、管理者はメールアドレスに適切なドメインを選択できます。
- 既存の onmicrosoft.com または未検証ドメイン内のその他のメールアドレスを持つグループの場合：
  - メールアドレスのローカルパート：メールアドレスのローカルパートは、既存のメールアドレスのローカルパートの小文字バージョンを使用して入力されます。
  - ドメインの選択（複数の Google ドメインが存在する場合）：グループが複数の Google ドメインに関連付けられている場合、管理者はメールアドレスに適切なドメインを選択できます。

制限事項

ドメインマッピング機能は、英数字、ダッシュ、アンダースコア、スペースを含むグループのみをサポートします。

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

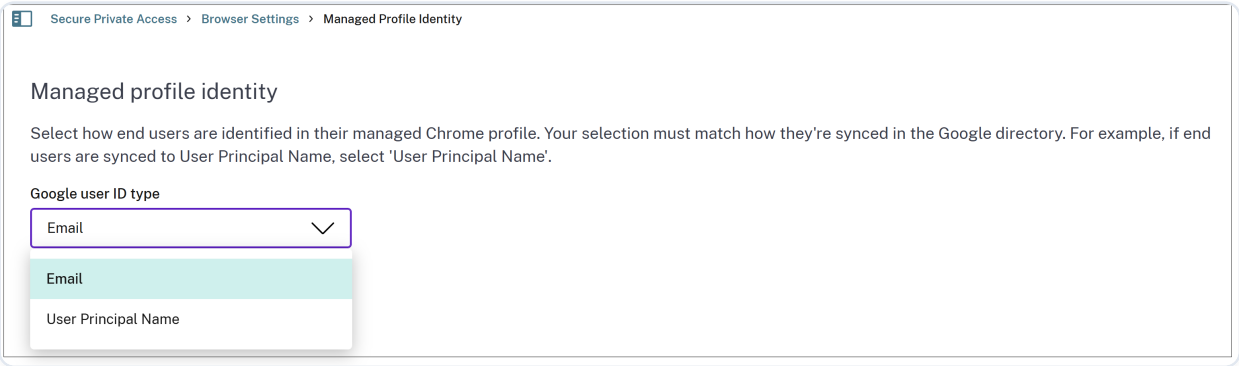
管理プロファイルID

Googleディレクトリは、すべてのユーザーアカウントをプライマリメールアドレスで識別します。組織がActive DirectoryまたはMicrosoft Entra IDからGoogleディレクトリにユーザーを同期する場合、どのソース属性をそのアドレスにするかを選択します。ほとんどの組織はメールアドレスをマッピングします。すべてのユーザーのメール属性を設定しない組織は、代わりにユーザープリンシパル名 (UPN) をマッピングする場合があります。これは、UPNが常にActive Directoryに存在するためです。

Secure Private Accessは、ディレクトリ同期がプライマリアドレスとして使用したのと同じ属性で各ユーザーを検索する必要があります。そうしないと、ユーザーをGoogleディレクトリ内のアカウントと照合できません。属性は、Secure Private Access管理コンソールのページから設定できます。

ユーザー属性タイプを設定する

1. Secure Private Access管理コンソールで、 **>** に移動します。
2. で、Secure Private AccessがCEPエンドユーザーを識別するために使用する属性を選択します。



   - **メール** - Secure Private Accessは、エンドユーザーをメールアドレスで識別します。これはデフォルト値であり、既存の展開で使用されているものです。
   - **ユーザープリンシパル名** - Secure Private Accessは、エンドユーザーをユーザープリンシパル名 (UPN) で識別します。
3. をクリックします。
4. 確認ウィンドウでメッセージを確認し、 をクリックします。

設定が保存されると、確認メッセージが表示されます。

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

注記:

- の設定はユーザーにのみ適用されます。Googleグループにはユーザープリンシパル名がないため、グループIDは影響を受けません。グループにソースディレクトリにメールアドレスがない場合は、「メールアドレスのないユーザーグループのドメインマッピング」を参照してください。
- この設定はテナント全体に適用されます。個々のユーザーに対して異なるID属性を選択することはできません。

Open ID Connect と Citrix Identity およびアクセス管理

Citrix Cloud 向けに、OpenID Connect (OIDC) 認証プロバイダーを使用して、Chrome Enterprise Premium (CEP) のシングルサインオン (SSO) を構成できます。OIDC と Citrix Identity の統合は、次の利点を提供します。

- **Device Posture サービス統合:** Device Posture サービスを Google Chrome Enterprise Premium と統合することで、デバイスコンプライアンスチェックを Chrome ブラウザベースのアクセスシナリオに拡張できます。この統合により、ユーザーが管理対象の Google Chrome プロファイルを通じてアプリケーションにアクセスする際に、組織はデバイスポスチャポリシーを適用できます。この統合に Device Posture サービスを使用するには、定期的なデバイスポスチャスキャンを構成することをお勧めします。

  注:

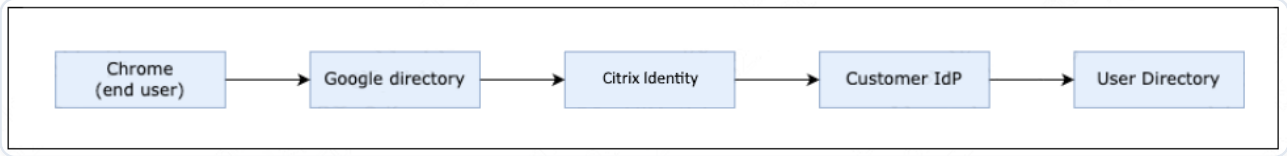
  この統合は、Device Posture サービスが複数ストアモードで構成されている場合には機能しません。

  Device Posture サービスの詳細については、「Device Posture の概要」を参照してください。
- **統合されたサインオンエクスペリエンス:** Chrome の SSO を、Active Directory (AD) および Microsoft Entra (旧 Azure AD) を含むがこれらに限定されない、ほとんどの一般的なIDプロバイダーに対して構成できますが、クラウドストアと CEP の両方で統合されたサインオンエクスペリエンスを選択できます。

概要

OIDC は、Citrix Identity を OIDC 認証プロバイダーとして使用して SSO を可能にします。OIDC に関連するコンポーネントを次の図に示します。

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



Google Chrome は、管理対象プロファイルを作成する際に、常に Google Directory に対して認証を試みます。OIDC を使用すると、Google Directory は実質的に OIDC Connect Provider である Citrix Identity に対するリライングパーティ (RP) となります。その結果、Citrix Identity は次のことを可能にします。

- デバイスポスチャ機能
- Chrome およびクラウドストア向けの、共通の統合されたサインインエクスペリエンス。

前提条件

Citrix Identity との OIDC 認証を構成する前に、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。

- Google Admin consoleへの管理者アクセス権があること。
- ディレクトリ同期を設定し、実行していること。詳細については、「Citrix IDで構成されたユーザーディレクトリをGoogle Cloudユーザーディレクトリと同期する」(/ja-jp/citrix-secure-private-access/service/prerequisites-for-cep-spa-integration.html#synchronize-user-directory-configured-in-citrix-workspace-with-the-google-cloud-user-directory)を参照してください。
- ユーザーIDプロバイダー (IdP) がCitrix Cloud Identity and Access Managementで設定および構成されていること。以下のIDプロバイダーがサポートされています。
  - Active Directory (AD) - 標準的なオンプレミスActive Directory統合
  - トークン付きActive Directory - トークンベース認証によるAD統合
  - Microsoft Entra ID - クラウドベースのIDサービス (旧Azure AD)
  - Okta
  - SAML 2.0

注:

Citrix CloudをOpenID Connect (OIDC) 認証プロバイダーとして使用するChrome Enterprise Premium (CEP) のシングルサインオン (SSO) は、条件付き認証をサポートするようになりました。

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

- Citrix Cloud Identity and Access Managementの詳細については、「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。
- 前述のIDプロバイダーのいずれかを選択して、サブスクライバーがストアに対して認証する方法を構成していること。ストア認証の構成方法については、「認証の構成」(/ja-jp/citrix-workspace/authentication.html)を参照してください。
- Secure Private Accessの初期設定とオンボーディングをすでに完了していること。詳細については、「Secure Private Accessのオンボーディングとセットアップ」(/ja-jp/citrix-secure-private-access/service/admin-guided-workflow-for-easy-onboarding-and-setup.html)を参照してください。

OIDC統合の概要

Google Chromeの管理対象プロファイルログインを構成済みのCitrix Identity Providerと統合するには、Google OIDC SSOプロファイルをCitrix OIDCクライアントに関連付ける必要があります。これを行うには、次の手順を実行します。

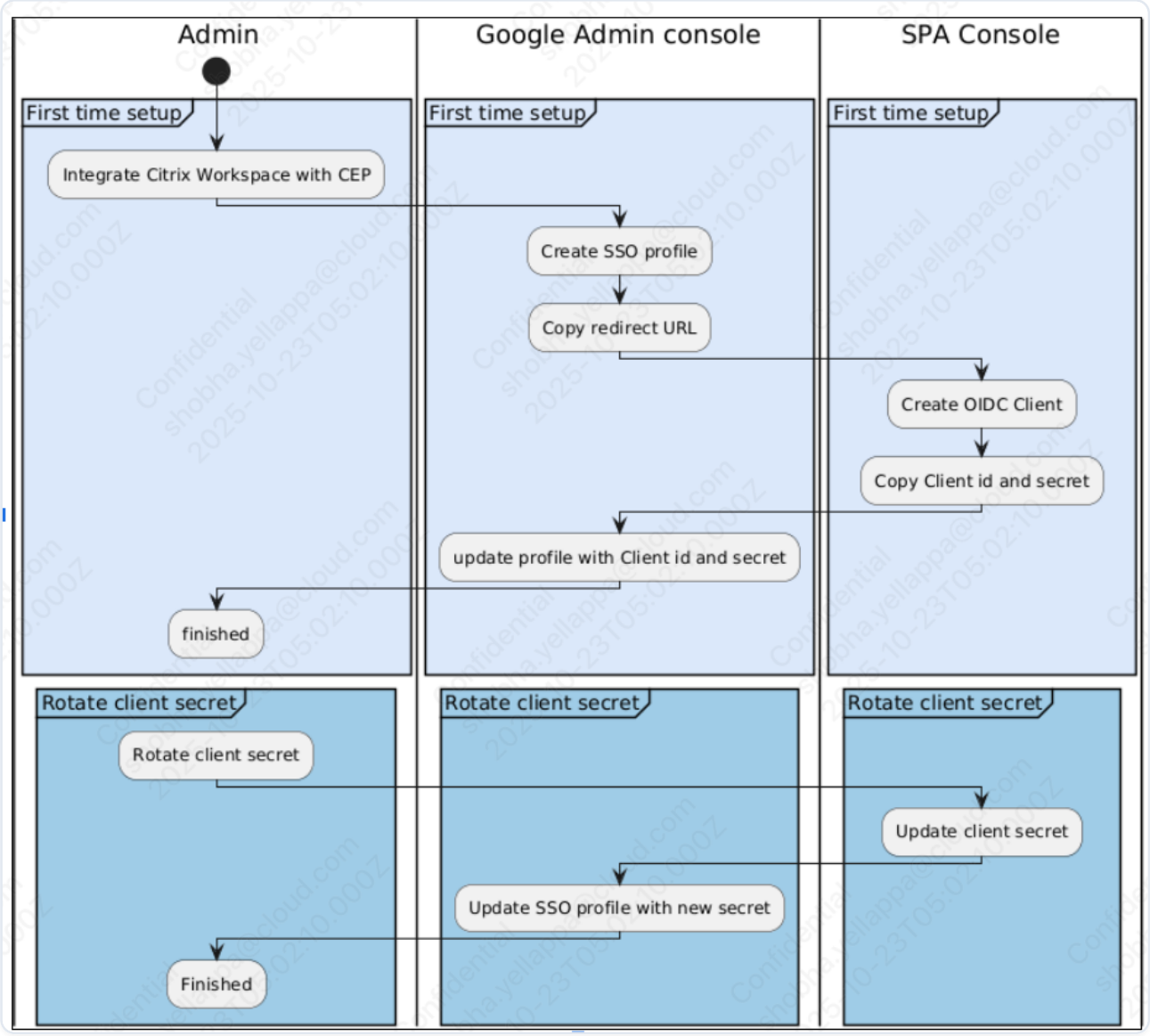
1. Google 管理コンソールで、プロファイル名を入力して新しいSSOプロファイルを作成します。他のフィールドは現時点では空白のままで構いません。新しいSSOプロファイルとリダイレクトURLの作成の詳細については、「Google OIDC SSOプロファイルの作成」を参照してください。
2. SSOプロファイルが作成されたら、このプロファイル用に生成されたリダイレクトURLをコピーします。
3. Secure Private Accessコンソールで、Citrix OIDCクライアントを作成し、（Google SSOプロファイルからの）リダイレクトURLを**リダイレクトURL**フィールドに貼り付けます。Citrix OIDCクライアントの作成の詳細については、「Citrix OIDCクライアントの作成」を参照してください。
4. OIDCクライアントが作成されたら、Secure Private Accessコンソールに表示されるクライアントID、クライアントシークレット、および発行者URLをメモします。
5. Google 管理コンソールに戻り、Secure Private AccessコンソールからのクライアントID、クライアントシークレット、および発行者URLでSSOプロファイルを更新します。
6. **SSOプロファイルの割り当ての管理**で、統合を完了するために構成したGoogle SSOプロファイルを選択します。

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

注：

OIDCクライアントの作成後、Secure Private Accessコンソールでクライアントシークレットをローテーションし、Google 管理コンソールでSSOプロファイルを更新できます。

次の図は、OIDC統合ワークフローを示しています。



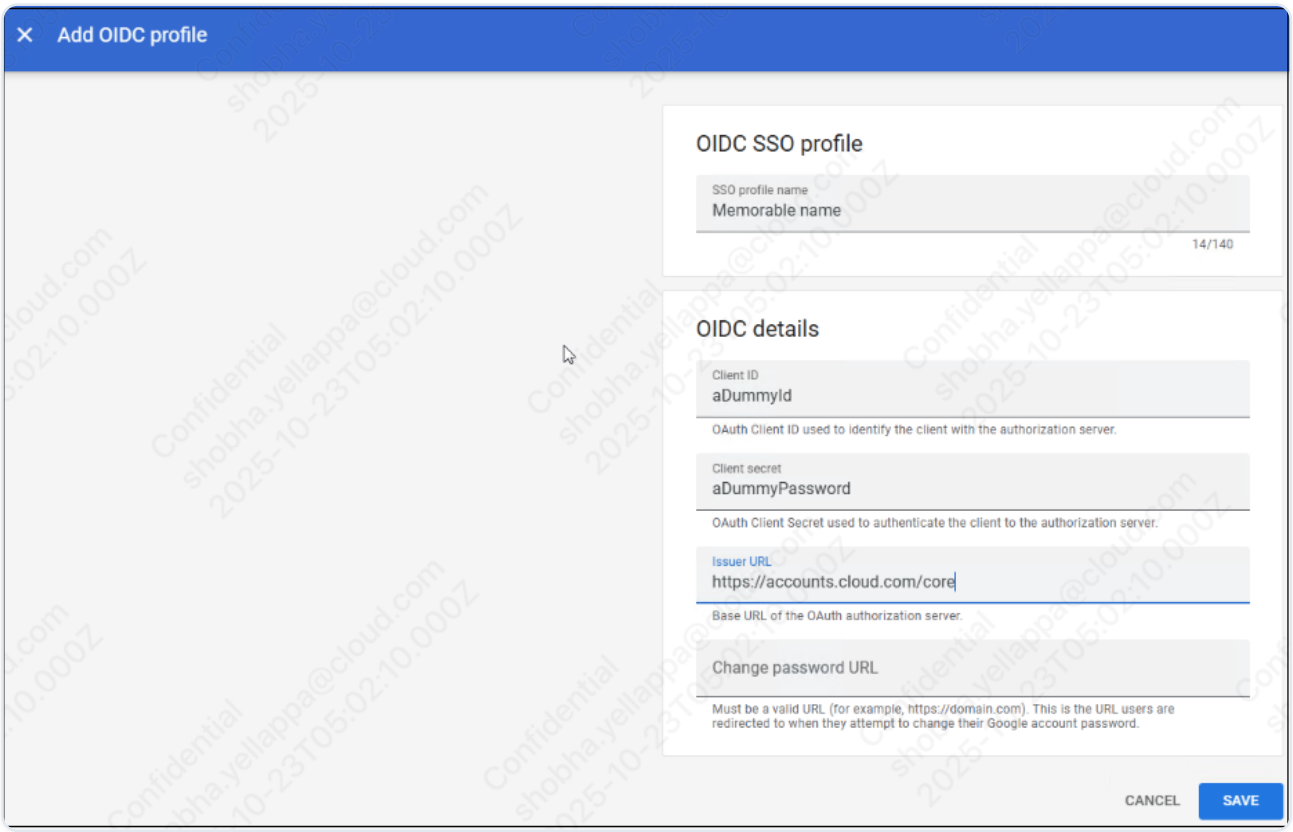
Google OIDC SSOプロファイルの作成

Google 管理コンソールで次の手順を実行します。

1. **セキュリティ > 認証 > サードパーティIdPとのSSO**に移動し、次に**OIDCプロファイルの追加**を選択します。
2. プロファイルの名前を指定します。

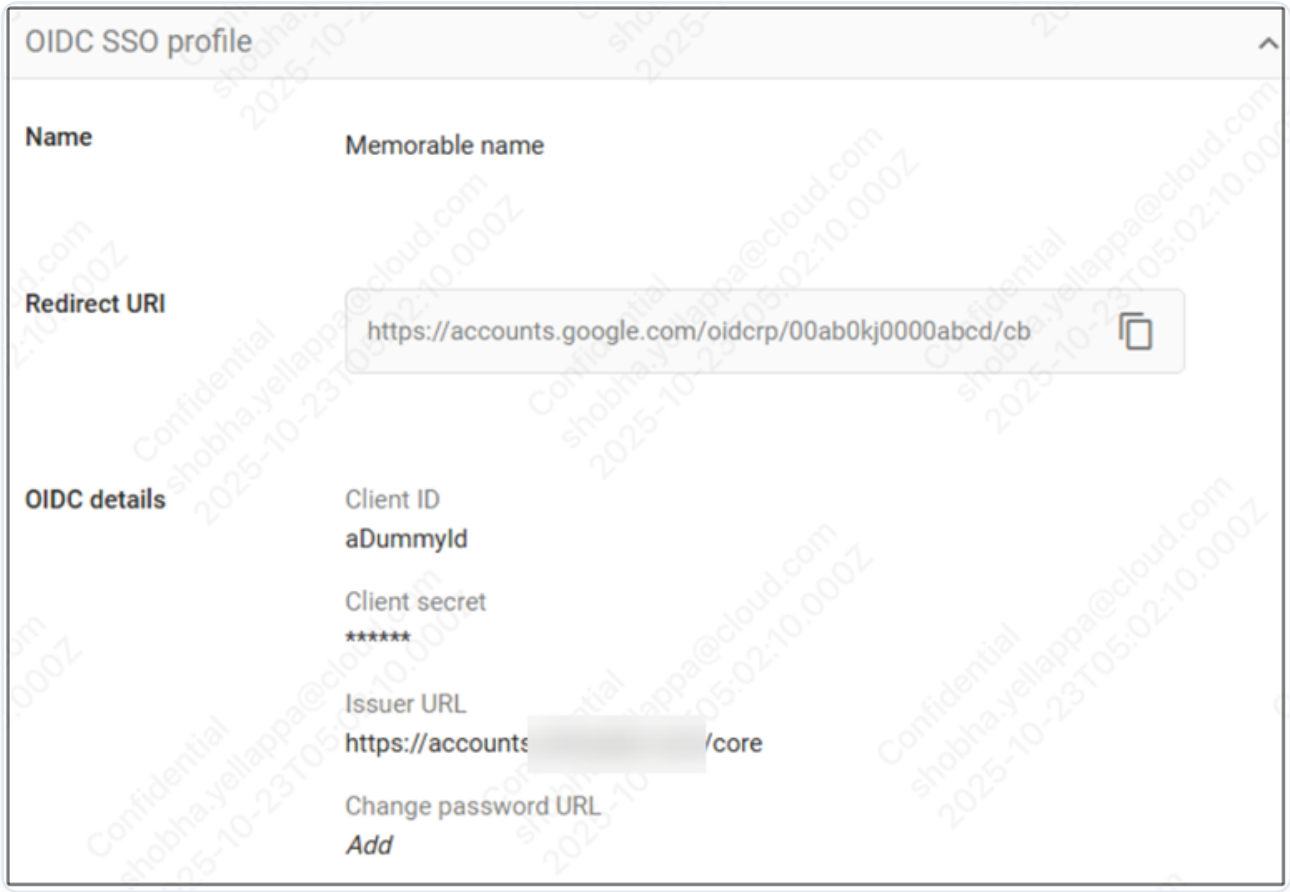
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. クライアントIDとクライアントシークレットにダミー値を割り当てるか、これらを空のままにします。これらのフィールドは後で更新されます。
4. 「**発行者URL**」に「`https://accounts.cloud.com/core`」を入力します。
5. 「**保存**」をクリックします。



プロファイルを作成したら、それをクリックしてリダイレクトURIを取得します。これはOIDCクライアントの作成に必要です。

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



Citrix OIDCクライアントを作成する

Secure Private Access管理コンソールで次の手順を実行します。

1. ナビゲーションペインで、「**ブラウザ設定 > Open ID Connect (OIDC)**」をクリックします。

   「

   注:

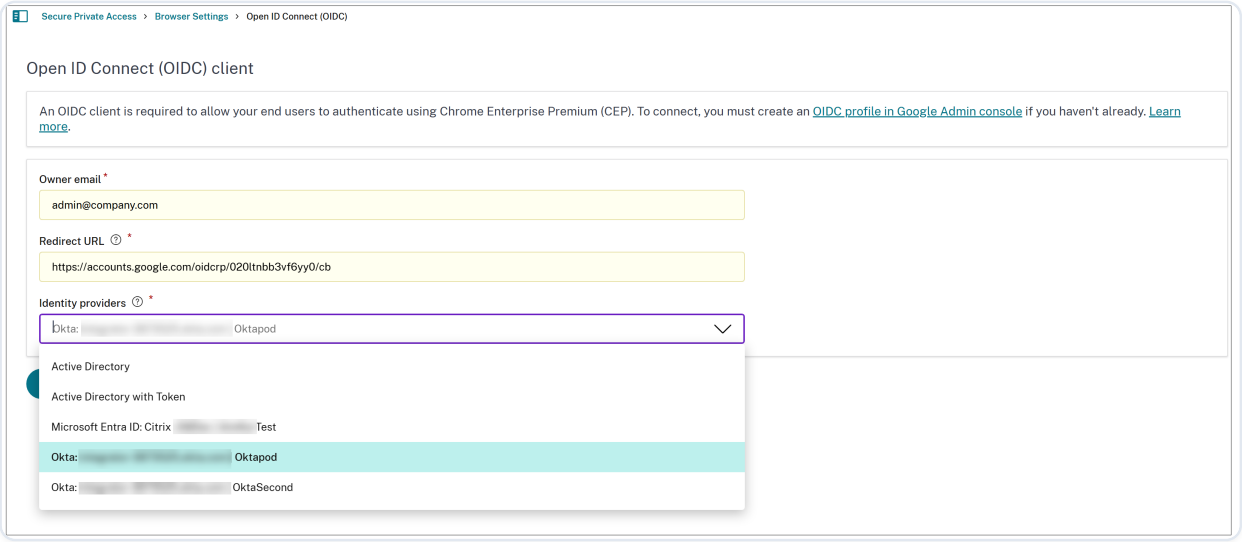
   」.

   「**ブラウザ設定**」メニューの「**Open ID Connect (OIDC)**」オプションは、オンボーディングプロセスが完了した後にのみ利用可能です。

2. 「**所有者のメールアドレス**」にユーザーのメールアドレスを入力します。このメールアドレスは、OIDCクライアントシークレットの有効期限が切れたときにアラートを送信するために必要です。
3. 「**リダイレクトURL**」に、Google OIDC SSOプロファイルを作成したときにGoogle管理コンソールで生成されたリダイレクトURIを入力します。IDプロバイダーは、このURLを使用してユーザー認証要求に応答します。

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

4. 環境で構成されているIDプロバイダーを選択します。
5. 「**作成**」をクリックします。



OIDCクライアントを正常に作成すると、ポップアップウィンドウにクライアントID、クライアントシークレット、および発行者URLが表示されます。これらの詳細をGoogle管理コンソールの設定にコピーする必要があります。資格情報は、次のいずれかの方法で取得できます。

- ポップアップウィンドウから値を直接コピーする
- 詳細をCSVファイルとしてダウンロードし、安全に保存する

重要:

クライアントシークレットは、この初期設定ステップでのみ表示されます。ポップアップウィンドウを閉じるか、次のステップに進む前に、クライアントシークレットを取得する必要があります。ウィンドウが閉じられると、クライアントシークレットは再度表示できなくなり、新しいシークレットを取得するためにシークレットをローテーションする必要があります。

6. **閉じる**をクリックします。

OIDC SSOプロファイルの割り当て

OIDCクライアントが作成され、Google OIDC SSOプロファイルがクライアントIDとシークレットで更新されたら、SSOを有効にするためにOIDC SSOプロファイルをユーザーとグループに割り当てる必要があります。

1. Google管理コンソールで、**セキュリティ > 認証 > サードパーティIdPとのSSO**に移動します。
2. **SSOプロファイルの割り当てを管理**で、**管理**をクリックします。

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

3. 左側のナビゲーションペインから、ルート組織部門（OU）とSSOプロファイルを選択して、組織のすべてのユーザーに対してSSOを有効にします。または、SSOプロファイルを特定のグループまたはOUに割り当てることもできます。

Citrix OIDCクライアントの更新

Citrix OIDCクライアントシークレットのデフォルトの有効期間は2年です。クライアントシークレットをローテーションすることで、OIDCのセキュリティを維持したり、潜在的なセキュリティインシデントに対応したりできます。クライアントシークレットのローテーションは、既存のシークレットの有効期限が近づいている場合、またはプロアクティブなセキュリティメンテナンスの一環として実行する必要がある重要なセキュリティ対策です。 クライアントシークレットをローテーションするたびに、新しいシークレットが生成されます。古いシークレットは、SSO認証の中断なしにスムーズな移行を確実にするために、元の有効期限まで有効です。ローテーション後、できるだけ早くGoogle管理コンソールの設定を新しいクライアントシークレットで更新してください。

クライアントシークレットをローテーションするには、次の手順を実行します。

1. 管理コンソールで、**設定 > Open ID Connect (OIDC) クライアント**ページをクリックします。
2. 「**クライアントシークレットをローテーション**」をクリックして、新しいシークレットを生成します。確認メッセージが表示されます。
3. トグルスイッチを有効にして確認メッセージに同意し、その後「**ローテーション**」をクリックします。

   「

   注：

   」：

   - 古いクライアントシークレットは、有効期限が切れるまで有効です。これにより、認証の中断なしにGoogle Workspaceを更新できます。
   - セキュリティ上の理由からすぐに期限切れにしたい場合は、「**今すぐ期限切れにする**」をクリックします。
   - このプロセス中、クライアントIDは変更されません。

4. 「**閉じる**」をクリックします。
5. Google Workspaceの設定で新しいシークレットをすぐに更新してください。

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

「

重要：

」:

- OIDC認証の中断を防ぐために、以前のシークレットの有効期限が切れる前に、Google OIDC SSOプロファイル構成で新しいクライアントシークレットを更新する必要があります。そのようなタイムリーな方法でシークレットを更新しないと、認証が中断され、ユーザーやサービスにアクセス問題を引き起こす可能性があります。
- 不正アクセスリスクを軽減し、認証システムの整合性を維持するために、クライアントシークレットの定期的なローテーションが推奨されます。
- Google OIDC SSOプロファイルのシークレットを更新したら、古いシークレットを期限切れにすることをお勧めします。

OIDCクライアントを更新(/en-us/citrix-secure-private-access/media/spa-cep-update-oidc-client.png)

OIDCクライアントを削除する

クライアントシークレットは、有効期限が切れるとローテーションできません。クライアントシークレットがローテーションされる前に期限切れになった場合、それは無効になります。この場合、既存のクライアントを削除して新しいものを作成する必要があります。

Secure Private Admin コンソールで次の手順を実行します。

1. Open ID Connect (OIDC) クライアントページで**編集**をクリックします。
2. **クライアントの削除**をクリックします。

   確認メッセージが表示されます。
3. トグルをONにスライドし、その後**クライアントの削除**をクリックします。

エンドユーザーエクスペリエンス

ユーザーは、以下の方法でSecure Private Accessを介してアプリケーションにアクセスできます。各アクセス方法は異なるユーザーエクスペリエンスを提供するため、組織は希望するユーザーエクスペリエンスと展開戦略に基づいて最適なアプローチを選択できます。

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

- **Citrix Workspaceアプリ** - 完全なポリシー適用とシングルサインオン機能を備え、最も安全で機能豊富なアクセスエクスペリエンスを提供するネイティブデスクトップアプリケーションです。
- **Webブラウザでのストア URL** - ユーザーはWebブラウザでストアを開くことができます。
  - Chrome以外のブラウザ（Firefox、Safari、Edgeなど）
  - 管理対象外プロファイルのChrome（エンタープライズポリシーのない個人用Chromeブラウザ）
  - 管理対象プロファイルのChrome（Chrome Enterprise Premiumポリシーが適用されたエンタープライズ管理のChromeブラウザ）
- **Chrome管理対象プロファイル** - ユーザーは、ブックマークを使用するか、Chrome管理対象プロファイルのアドレスバーにアプリケーションURLを手動で入力することで、アプリケーションに直接アクセスします。

次の表は、さまざまな方法でアプリケーションにアクセスした場合のエンドユーザーエクスペリエンスをまとめたものです。

	直接	WEBブラウザでのストアURL	CITRIX WORKSPACEアプリ
Chrome以外のブラウザ	SaaSアプリへのアクセスは拒否されます（SaaSアプリが適切なIPアドレス許可リストで構成されていると仮定した場合）。	アプリはユーザーインターフェイスに列挙されます。	該当なし
	プライベートアプリにアクセスできません。	アプリケーションは、適切なChrome管理プロファイルで起動されます。	
		該当する管理プロファイルがまだ作成されていない場合、プロファイル作成ウィザードが起動されます。	

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

	直接	WEBブラウザでのストアURL	CITRIX WORKSPACEアプリ
Chrome（非管理プロファイル）	SaaSアプリへのアクセスが拒否されました（SaaSアプリが適切なIPアドレス許可リストで構成されていると仮定した場合）。	アプリケーションは、適切なChrome管理プロファイルで起動されます。	該当なし
	プライベートアプリにアクセスできません。	対応する管理プロファイルがまだ作成されていない場合、プロファイル作成ウィザードが起動します。	
Chrome (管理プロファイル)	アプリは、Secure Private Access の構成に応じて許可または拒否されます。	列挙されたアプリは新しいタブで起動されます。	該当なし
Citrix Workspace アプリ	該当なし	該当なし	アプリはユーザーインターフェイスに列挙されます。
			アプリケーションは、適切な Chrome 管理プロファイルで起動されます。
			対応する管理プロファイルがまだ作成されていない場合、プロファイル作成ウィザードが起動します。

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

クローム エンタープライズ プレミアム 用 シトリックス セキュア アクセス 拡張機能

Chrome Enterprise Premium (CEP) 用 Citrix Secure Access 拡張機能は、Chrome ブラウザから直接、内部および外部アプリケーションへの安全なクライアントレスアクセスを可能にします。Citrix Secure Private Access と Chrome Enterprise の機能を組み合わせることで、エンタープライズグレードのセキュリティ、ゼロトラストアクセス、コンテキスト制御、および最新のユーザーエクスペリエンスを提供します。

組織は、この拡張機能を使用して、VPN やネイティブクライアントのインストールを必要とせずに、SaaS アプリケーション、内部 Web アプリ、SSH サーバー、および RDP システムへの安全なアクセスを提供できます。

Secure Private Access を Chrome Enterprise Premium と統合すると、Secure Access ブラウザ拡張機能が自動的にインストールされます。セットアップ手順については、「Google Chrome 統合のセットアップ」を参照してください。インストール後、Chrome ブラウザの右上隅にあるアイコンから拡張機能にアクセスできます。

拡張機能アイコン(/en-us/citrix-secure-private-access/media/chrome-extension-icon.png)

Secure Access 拡張機能ログ

Secure Access ブラウザ拡張機能ログは、監視とトラブルシューティングに不可欠です。エンドユーザーは、問題が発生したときに、ログを確認およびダウンロードして、管理者またはサポートチームと共有できます。

ログを確認またはダウンロードするには:

1. ブラウザ拡張機能アイコンを右クリックします。
    - ログを確認するには、 をクリックします。
    - ログをダウンロードするには、 をクリックします。

拡張機能ログ(/en-us/citrix-secure-private-access/media/chrome-extension-logs.png)

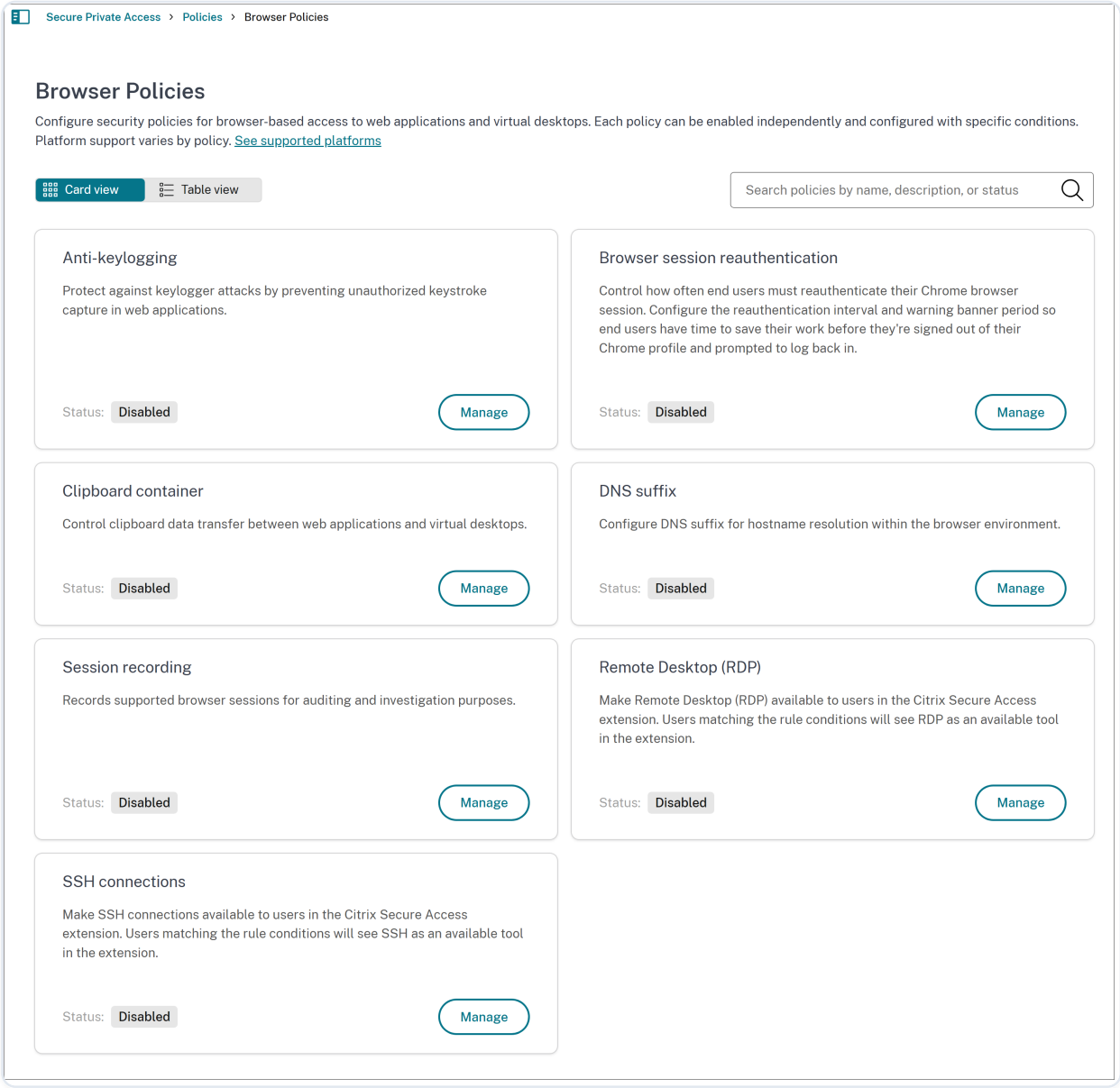
Chrome Enterprise 用 Citrix Secure Access コントロール

Citrix Secure Private Access は、Google Chrome Enterprise Premium (CEP) 用 Citrix Secure Access 拡張機能によって配信および適用されるセキュリティポリシーをサポートしています。詳細については、「サポートされるコントロール」を参照してください。

これらのポリシーは、Secure Private Access 管理コンソールから構成できます。

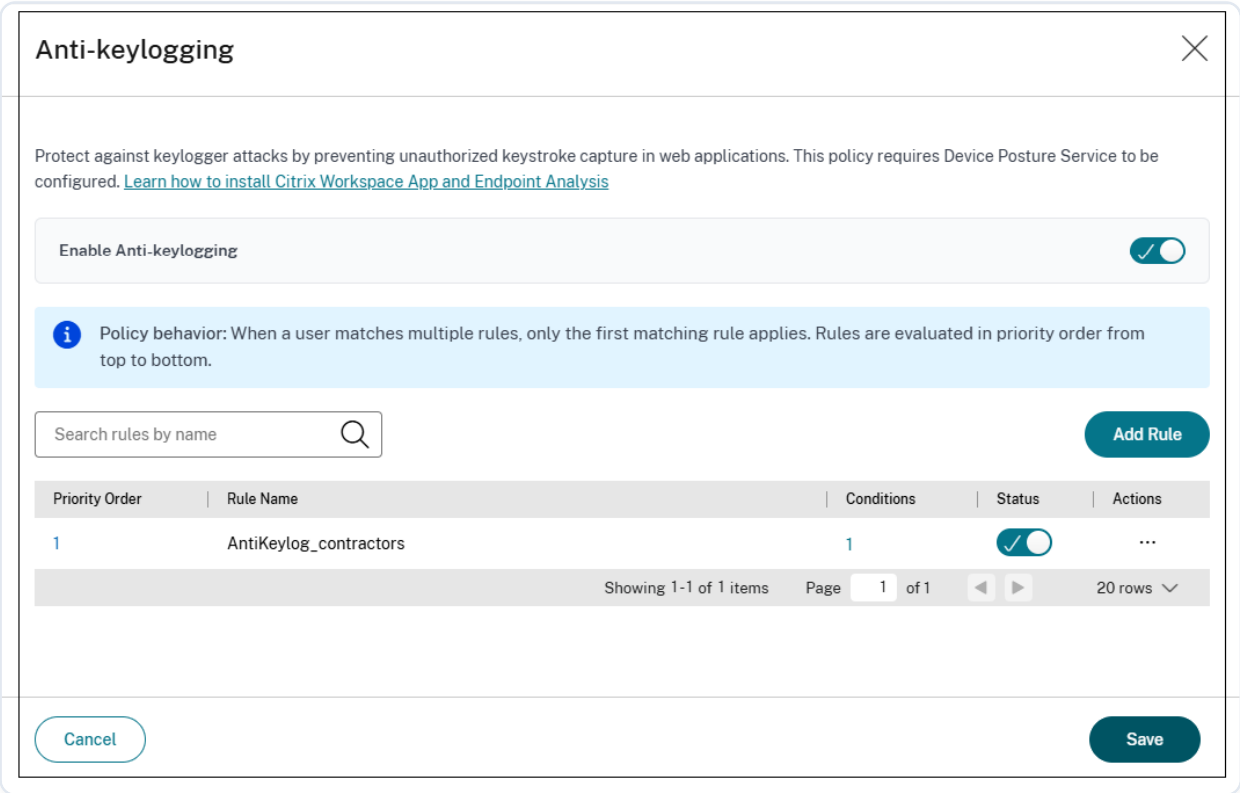
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **ポリシー > ブラウザポリシー**に移動し、**ブラウザポリシーの作成**をクリックします。
2. ポリシーを選択し、**管理**をクリックします。



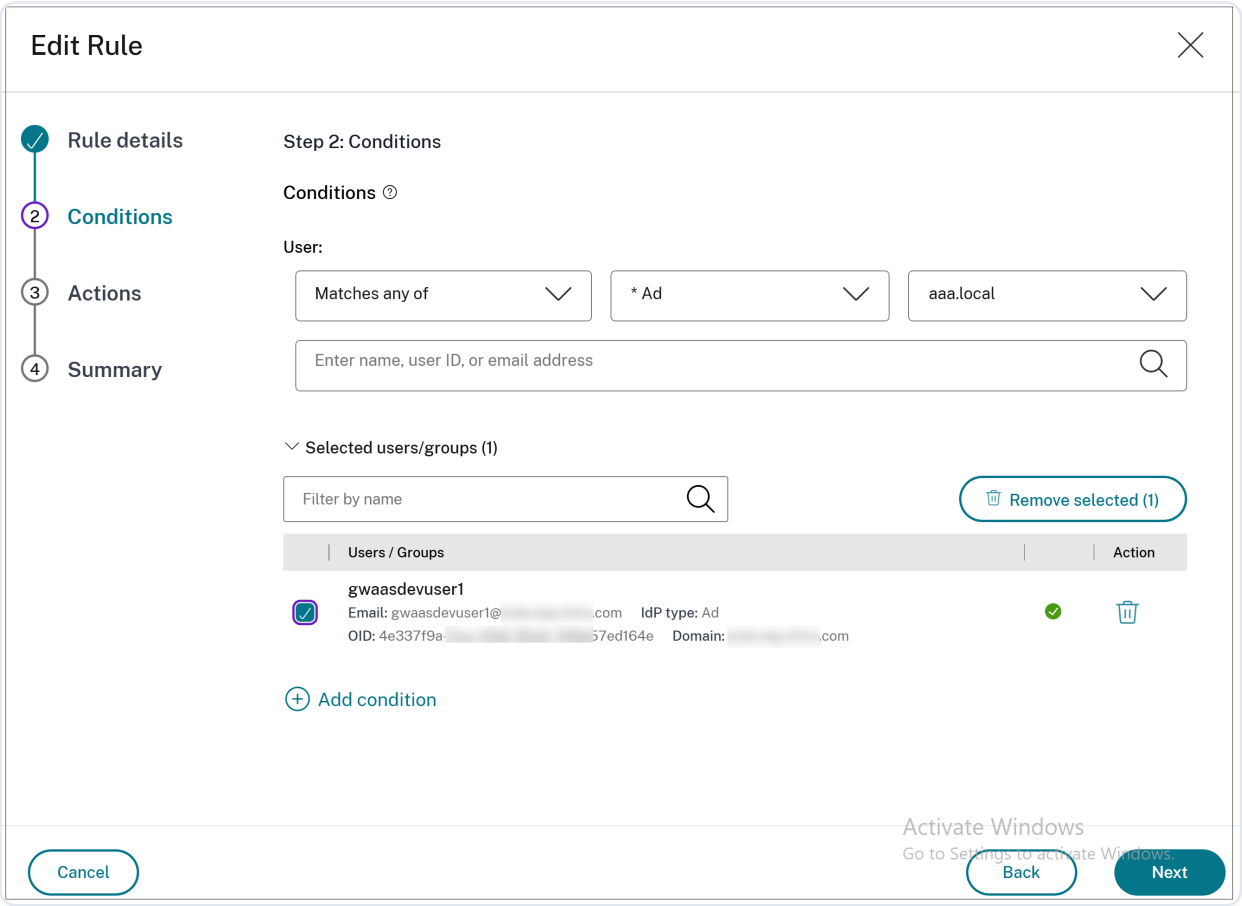
3. ポリシーのルールを追加します。

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



4. ブラウザコントロールをブラウザセッションにスコープするために、**アクセスモード**条件を追加します。ブラウザポリシーの場合、値は通常**ブラウザ**です。アクセスモードの詳細については、「アクセスモードベースのポリシー適用」を参照してください。
5. ポリシーを評価する必要がある条件を選択します。

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



注:

ユーザーまたはグループを選択する際、管理者は、選択したユーザーディレクトリからのエントリがGoogle Directoryと同期され、正しく構成されているかを確認できます。Secure Private Accessポリシーは、同期されたユーザーとグループを使用する場合にのみ正しく評価されます。そうでない場合、警告が表示されることがあります。詳細については、「ユーザーとグループの同期の確認」を参照してください。

詳細な構成手順については、各コントロールのドキュメントを参照してください。

サポートされているコントロール

Citrixは、Secure Private AccessとChrome Enterprise Premiumの統合で、以下のSecure Accessコントロールをサポートしています。

コントロール	機能
キーロギング対策	エンドポイント上のキーロガーマルウェアによるユーザー入力のキャプチャを防ぐために、キーストロークを難読化します。

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

コントロール	機能
クリップボードコンテナ	ユーザーがブラウザと他のアプリの間でコピー＆ペーストできる内容を制御します。
DNSサフィックス	短い内部URL（「wiki/」など）を完全なアドレスに自動的に補完します。
セッション記録	監査およびコンプライアンスのために、ブラウザセッションのアクティビティを記録します。
ブラウザセッションの再認証	設定された時間間隔の後、ブラウザセッションの定期的な再認証を強制します。
SSH接続	ユーザーがターミナルクライアントを必要とせずに、ブラウザタブ内で直接SSH接続を確立できるようにします。
リモートデスクトップ (RDP)	ユーザーがRDPクライアントを必要とせずに、ブラウザタブ内で直接リモートデスクトップセッションを起動できるようにします。

ポリシー内のユーザーとグループ

以下のセクションでは、ユーザーとグループに関する詳細情報を提供します。

ユーザーまたはグループを検索

選択したユーザーとグループはグリッドに表示されます。グリッドの各行には、異なるドメイン、フォレスト、またはIDプロバイダー (IdP) 間で同じ名前のユーザーまたはグループを明確に区別できるように、以下のID詳細が表示されます。

- **名前** – ユーザーまたはグループの表示名。
- **メール** – IDに関連付けられているメールアドレス。
- **IDPタイプ** – Azure AD、Active Directory、Okta、GoogleなどのIDプロバイダー。
- **OID** – IDのオブジェクトIDまたはセキュリティ識別子。
- **ドメイン** – ユーザーまたはグループが属するドメイン。

グリッドを名前でフィルタリングしたり、個々の行を削除したり、複数のエントリを選択して**選択したものを削除**を使用してまとめて削除したりできます。

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

同期されたユーザーとグループを使用する

When selecting users or groups, administrators can verify whether entries from the selected user directory are synchronized with and correctly configured in Google Directory. Secure Private Access policies evaluate correctly only when they use synchronized users and groups. Otherwise, the following warnings might appear:

- **テナントアカウントの権限がありません。**

  対処法: Google管理コンソールで、テナントサービスアカウントに**ユーザー > 読み取り**および**グループ > 読み取り**の権限を割り当てます。SPAは、ユーザーまたはグループが存在することを確認するためにこれらの権限を必要とします。

- **ユーザーまたはグループが同期されていません。**

  対処法: 検索または選択されたユーザーまたはグループは、Googleディレクトリと同期されていません。SPAポリシーで使用する前に、ディレクトリエンティティをGoogleディレクトリと同期してください。

- **グループアクセス設定が不十分です。**

  対処法: Google 管理コンソールで、選択したグループのアクセス設定を開き、**メンバーを表示できるユーザー**で、少なくとも**グループメンバー**オプションが選択されていることを確認します。

> **注:**
>
> この機能は、Google Chrome の統合が正常に完了した後にのみ利用可能です。

キーロギング対策制御

サイバー犯罪者は、パスワード、クレジットカード番号、機密性の高い企業データなどの機密情報を盗むために、キーロガーなどの悪意のあるソフトウェアを使用します。

Chrome Enterprise Premium (CEP) 用のCitrix Secure Accessブラウザ拡張機能は、データの保護に役立つキーロギング対策をサポートしています。この機能はキーストロークをスクランブルするため、悪意のあるプログラムが入力された情報をキャプチャしようとしても、判読不能な文字のみが記録され、実際のテキストは安全に作業アプリケーションに配信されます。

サポートされている展開: Citrix Secure Private Accessサービスおよびハイブリッド展開。

サポートされているプラットフォーム: Windows 11以降。

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

注:

ネイティブRDPセッションでは、キーロギング対策はサポートされていません。

前提条件

キーロギング対策を有効にする前に、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。

- CWAバージョン2603以降がインストールされていること。
- Citrix Secure AccessとChrome Enterprise Premium (CEP) の統合が完了していること。

キーロギング対策ポリシーの構成

1. Secure Private Access管理コンソールにログオンします。
2. **ポリシー > ブラウザポリシー**に移動し、**ブラウザポリシーの作成**をクリックします。
3. **キーロギング対策**を選択し、**管理**をクリックします。
4. アンチキーロギングを有効にするためのルールをユーザーに追加するには、「**ルールを追加**」をクリックします。

   a. ルールの名前を入力し、「**次へ**」をクリックします。

   b. ユーザーまたはグループなど、要件に基づいて条件を選択します。また、「**地理的位置**」、「**ネットワークの場所**」、「**デバイスの姿勢チェック**」などの条件を追加することもできます。

   c. 「**次へ**」をクリックします。

5. 「**保存**」をクリックします。

   アンチキーロギングポリシー用に構成されたルールの数は、「**ブラウザポリシー > アンチキーロギング**」タブに表示されます。

クリップボードコンテナ制御

WebアクセスにChromeを、ネイティブアプリケーションにVDIを使用する展開では、クリップボードコンテナ機能を使用して、ブラウザとVDIセッション間のデータ共有を制御できます。クリップボードデータはCitrixセッション間で直接転送され、ローカルエンドポイントのクリップボードに書き込まれることはありません。 これによりセキュリティが向上し、ユーザーは両方の環境で柔軟に作業できます。

サポートされている展開: Secure Private Accessサービスおよびハイブリッド展開。

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

サポートされているプラットフォーム: Windows。

前提条件

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。

- Citrix Secure AccessとChrome Enterprise Premium (CEP) の統合が完了していること。
- Citrix Workspaceアプリ2603.10以降。
- 2607 LTSR以降を実行しているWindows VDA (Clipboard Sharing ScopeのGAバージョン)。詳細については、「Clipboard Sharing Scope」を参照してください。
- 2507 LTSRを実行しているWindows VDA (Clipboard Sharing Scopeのプレビューバージョン) で、以下を有効にします。
  - **DaaSとのクロス・クリップボード・コンテナ**機能。詳細については、「DaaSとのクロス・クリップボード・コンテナ」を参照してください。この機能は現在、DaaSでプレビューとして利用可能です。
  - **Clipboard Sharing Scope**レジストリ。詳細については、「Clipboard Sharing Scopeレジストリを有効にする」を参照してください。

クリップボードコンテナ制御を有効にする

1. Secure Private Access管理コンソールにログインします。
2. **ポリシー > ブラウザポリシー**に移動し、**ブラウザポリシーの作成**をクリックします。
3. **クリップボードコンテナ**を選択し、**管理**をクリックします。
4. VDAとブラウザ間のクリップボード共有のルールを追加するには、「**ルールを追加**」をクリックします。
   a. ルールの名前を入力し、「**次へ**」をクリックします。
   b. ユーザーやグループなど、要件に基づいて条件を選択します。また、「**地理的位置**」、「**ネットワークの場所**」、「**デバイスの姿勢チェック**」などの条件を追加することもできます。
   c. **次へ**をクリックします。
   d. クリップボード共有を許可するURLとSecure Private Accessアプリケーションを定義します。
   e. ポリシーのスコープを選択します。
   - 「**ブラウザ全体に適用**」 — このポリシーは、管理対象プロファイル内のすべてのクリップボードアクティビティを管理します。

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

- **「特定のアプリケーションとURLに適用」** — このポリシーは、選択されたアプリケーションと入力されたURL/ドメインパターンに限定されます。
  - **「アプリケーションを選択」** — アプリケーションピッカーを使用して、特定の公開アプリケーションを選択します。
  - **「URLまたはドメイン」** - 特定のアプリケーションのURLまたはドメインを入力します。

クリップボードコンテナアクション(/en-us/citrix-secure-private-access/media/spa-cep-clipboard-container-action.png)

5. **「保存」**をクリックします。

   クリップボードコンテナポリシー用に構成されたルールの数は、**「ブラウザポリシー > クリップボードコンテナ」**タブに表示されます。

クリップボード共有スコープを有効にする

VDAバージョン2607の場合:

「仕組み」を参照してください。

VDAバージョン2507の場合:

このレジストリ **Clipboard Sharing Scope** レジストリを有効にします。

1. regedit.exe を使用して Windows レジストリエディターを開きます。
2. HKEY_LOCAL_MACHINE\Software\Citrix\Clipboard\ に移動します。
3. `ClipboardSharingScope` という名前の REG_DWORD 値を作成します。

クリップボードコンテナレジストリ(/en-us/citrix-secure-private-access/media/spa-cep-clipboard-container-registry1.png)

`ClipboardSharingScope` ポリシーは、VDA クリップボードデータを共有できる場所を制御します。新しい DDC ポリシーが利用可能になるまで、この設定は上記のレジストリキーを使用して構成できます。

サポートされている値	スコープ	説明
0	無制限	クリップボードデータはクライアントシステムのクリップボードにコピーされ、クライ

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

サポートされている値	スコープ	説明
		アント、VDA、および CEP からアクセスできます。
1	VDA のみ	クリップボードデータは VDA のみにアクセス可能です。クライアントシステムのクリップボードと CEP はクリップボードコンテンツにアクセスできません。
2	CEP のみ	クリップボードデータは CEP のみにアクセス可能です。クライアントシステムのクリップボードと VDA はクリップボードコンテンツにアクセスできません。
3	VDA と CEP	クリップボードデータは VDA と CEP の両方からアクセス可能です。クライアントシステムのクリップボードはクリップボードコンテンツにアクセスできません。

クリップボードコンテナのレジストリ値(/en-us/citrix-secure-private-access/media/spa-cep-clipboard-container-registry2.png)

注:

- CEPのみ (2) およびVDAとCEP (3) モードは、CEP拡張機能のクリップボードコンテナ機能と連携するように設計されています。
- クリップボードコンテナポリシーが有効になっている場合、管理者が構成したURLのみがVDIとクリップボードデータを交換することが許可されます。

```
>-  Content copied from the approved web applications can be pasted into
the VDI.

>-  Content copied from the VDI can be pasted only into administrator-
```

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

```
configured, paste-allowed URLs.

>-  If a user attempts to paste VDI clipboard content into a website that
is not included in the policy, the paste operation is blocked and an error
message appears.
```

ウェブアプリケーションのドメインサフィックス

ユーザーがブラウザに短い内部ホスト名（例: `sw` または `server001`）を入力するシナリオでは、ドメインサフィックス機能は、オペレーティングシステムのDNSサフィックス設定に依存する代わりに、ブラウザ管理のDNSサフィックスポリシーを使用してDNSサフィックスを自動的に追加し、それらを完全修飾ドメイン名 (FQDN) に変換します。

DNSサフィックス機能は、**Windows** および **macOS** の両プラットフォームでサポートされており、以下を含む一般的なURL入力形式全体にわたって一貫して適用されます。

- `sw`
- `http://sw`
- `https://sw/`
- `sw/`
- `http://sw/`
- `https://sw/`

サポートされている展開: Secure Private Accessサービスおよびハイブリッド展開。

サポートされているプラットフォーム: WindowsおよびmacOS。

前提条件

Citrix Secure AccessとChrome Enterpriseの統合が構成されていることを確認してください。詳細については、「Integration with Google Chrome Enterprise Premium」を参照してください。

DNSサフィックスの構成

1. Secure Private Access管理コンソールにログインします。
2. a. 「**ポリシー > ブラウザポリシー**」に移動し、「**ブラウザポリシーの作成**」をクリックします。
3. 「**DNSサフィックス**」を選択し、「**管理**」をクリックします。
4. 「**ルールの追加**」をクリックして、URLに追加するドメインのルールを追加します。

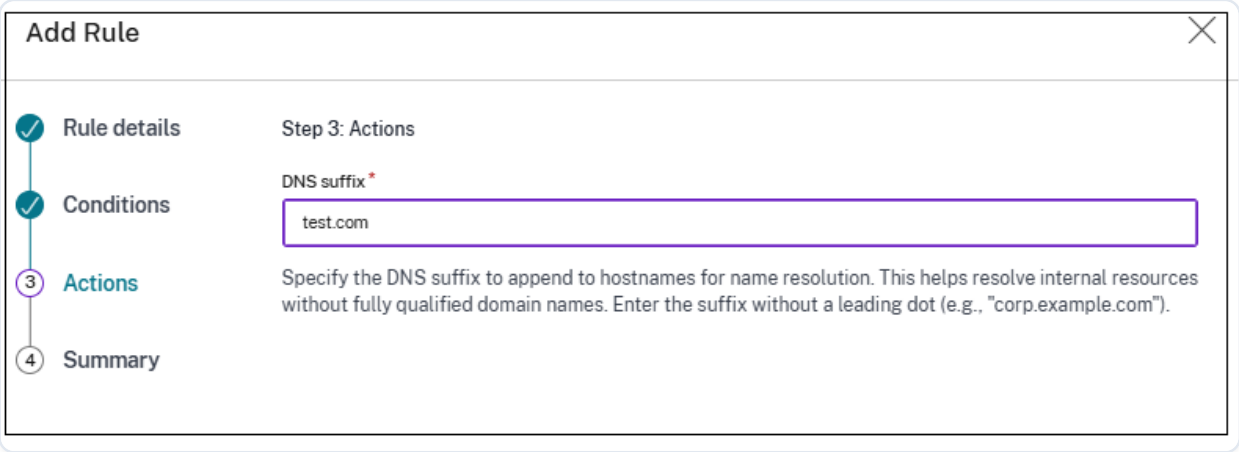
© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. ルールの名前を入力し、「**次へ**」をクリックします。

b. ユーザーやグループなど、要件に基づいて条件を選択します。「**地理的位置**」、「**ネットワークの場所**」、「**デバイスの姿勢チェック**」などの条件を追加することもできます。

c. 「**次へ**」をクリックします。

d. アクセス用に付加するドメインを定義します。



5. 「**保存**」をクリックします。

DNSサフィックスポリシーに設定されているルールの数が、「**ブラウザポリシー > DNSサフィックス**」タブに表示されます。

セッション記録の制御

セッション記録は、セッションを記録、カタログ化、アーカイブして、取得および再生できるようにします。

セッション記録には、次の主な利点があります。

- アプリケーションおよびデスクトップセッションの記録を自動的にトリガーするための柔軟なポリシーを提供します。
- IT担当者がユーザーアクティビティを監視および調査できるようにし、規制遵守およびセキュリティ監視のための内部統制をサポートします。
- 問題の特定を迅速化し、解決までの時間を短縮することで、テクニカルサポートを支援します。

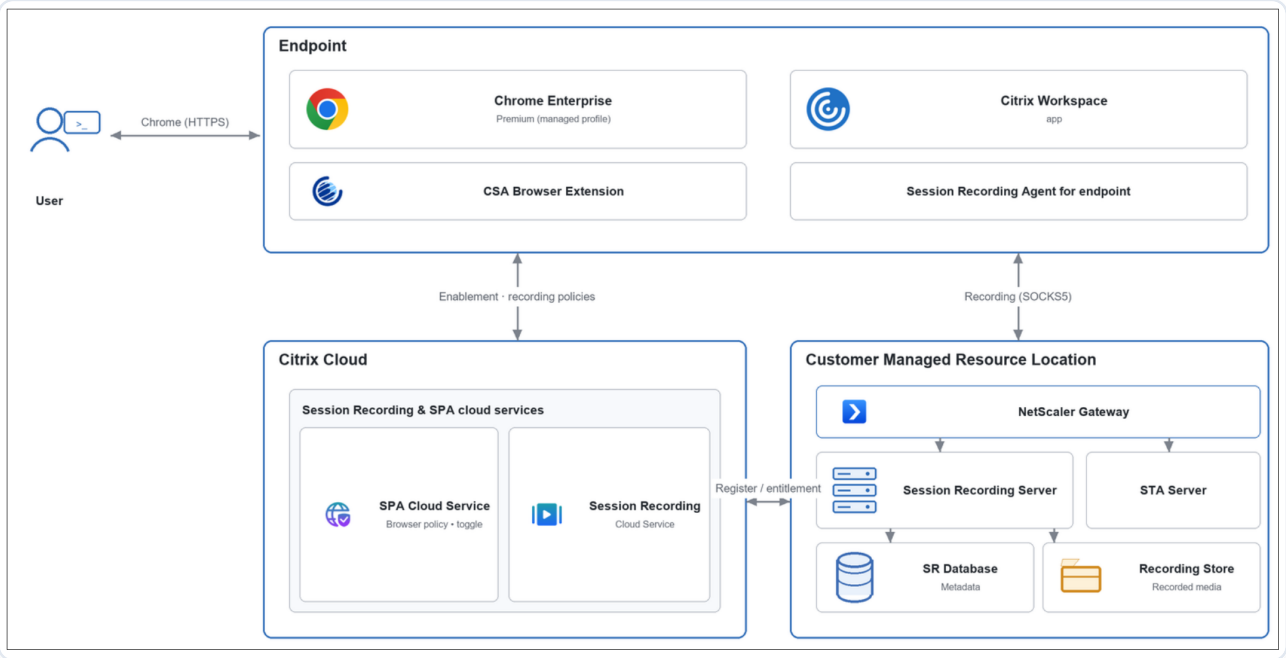
詳細については、「利点」を参照してください。

アーキテクチャ

セッション記録ソリューションは、次の3つのプレーンにまたがっています。

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

- 管理対象のChromeプロファイル、Citrix Secure Access拡張機能、およびエンドポイント用Session Recording Agentを備えたエンドポイント。
- Secure Private AccessおよびSession Recordingクラウドサービスを収容するCitrix Cloudコントロールプレーン。
- NetScaler Gateway、STAサーバー、Session Recordingサーバー、およびそのデータベースと記録ストアを含む、顧客管理のリソースロケーション。



前提条件

- Citrix Workspaceアプリ for Windows 2603.10以降
- Endpoint analysis (EPA) バージョン: 26.5.1.7 以降

システム要件

- Citrix Secure Private Access。サービスモードまたはハイブリッドモードで展開され、Chrome Enterprise Premium（管理プロファイル付き）と組み合わされていること。
- Session Recording Cloud service と Session Recording server 2511 以降。詳細については、「Get started」を参照してください。
- 次のコンポーネントを備えた Windows 64 ビットまたは 32 ビットのエンドポイント:
  - Citrix Endpoint Analysis (EPA) プラグイン 26.5.1.7 以降。
  - Session Recording Endpoint Agent がインストールされた Citrix Workspace app for Windows バージョン 2603.10 以降

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

環境をセットアップする

Chrome Enterprise セッションのエンドポイント録画を有効にして検証するには、次の手順を完了します。

Session Recording サイトを構成する

Configure endpoint recording policies に記載されている手順に従ってください。

注:

エンドポイント録画には NetScaler Gateway が必要です。Secure Private Access の両方の展開タイプで、STA を介して録画トラフィックを Session Recording Server にルーティングします。NetScaler がユーザーからアプリケーションへのアクセスを管理しない Secure Private Access サービスを使用している場合でも、録画トラフィック用の gateway URL を指定する必要があります。

Secure Private Access で Session Recording ブラウザポリシーを構成する

1. Secure Private Access 管理コンソールにログオンします。
2. 「**ポリシー > ブラウザポリシー**」に移動し、「**ブラウザポリシーの作成**」をクリックします。
3. 「**セッション記録**」を選択し、「**管理**」をクリックします。
4. 「**ルールの追加**」をクリックし、ルールの名前を入力して、「**次へ**」をクリックします。
5. 条件（ユーザーとグループ）を設定します。（オプション）「**地理的位置**」、「**ネットワークの場所**」、「**デバイスポスチャチェック**」を追加し、「**次へ**」をクリックします。
6. 「**保存**」をクリックします。ルール数は「**ブラウザポリシー > セッション記録**」タブに表示されます。

エンドポイント用のセッション記録エージェントを含むWorkspaceアプリをインストールする

セッション記録アドオンのサポートに記載されている手順に従ってください。

記録されたセッションを再生する

記録はセッション記録コンソールで表示できます。

- ユーザーのChromeワークプロファイルに関連付けられているすべてのウィンドウが記録されます。
- 1つ以上のモニターにまたがる複数のウィンドウが記録されます。
- フォーカスが外れているウィンドウや、他のアプリケーションによって隠されているウィンドウも、全体が記録されます。

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

- 最小化されたウィンドウや、画面キャプチャ防止が有効になっているウィンドウは、再生中に黒い四角として表示されます。

ベストプラクティス

- **グローバルサイトを1つ維持する**。単一のグローバルエンドポイント記録サイトを使用し、その構成を文書化します。変更すると、他のサイトで構成されているポリシーが意図せず無効になる可能性があります。
- **リージョンを合わせる**。遅延やデータレジデンシーの問題を避けるため、セッションレコーディングのクラウドサービスURL、クラウドクライアント、バックエンドを同じCitrix Cloudリージョンに保持します。
- **ストレージを計画する**。全画面のWeb/SaaSレコーディングは、ストレージを大量に消費する可能性があります。それに応じてサーバー、セッションレコーディングデータベース、およびレコーディングストレージのサイズを決定し、ストレージ消費量を綿密に監視してください。
- **最初にエンタイトルメントとロールを検証する**。Citrix DaaSとCitrix Secure Private Accessのエンタイトルメントの不一致は、展開失敗の最も一般的な原因です。ポリシーを有効にする前に、単一のアクティブな顧客レコードが存在し、必要な管理ロールが割り当てられていることを確認してください。

ブラウザセッションの再認証制御

Citrix Secure Private Access を使用すると、管理者は Chrome Enterprise Premium (CEP) ブラウザセッションのセッションタイムアウトポリシーを適用できます。ユーザーは、ブラウザのアクティビティに関係なく、設定されたセッション期間が経過すると再認証を求められます。これにより、Google Chrome の仕事用プロファイルを通じてアクセスされるアプリケーションのゼロトラストアクセス制御が強化されます。

セッションの有効期限が切れると、ユーザーはエンタープライズ資格情報と多要素認証 (MFA) を使用して再認証する必要があります。再認証が成功すると、最後にアクティブだったページが復元され、セッションタイマーが再開されます。

サポートされている展開: Secure Private Access サービスとハイブリッド展開。

サポートされているプラットフォーム: Windows、macOS、Linux、ChromeOS。

前提条件

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。

- Citrix Secure Access と Chrome Enterprise Premium (CEP) の統合が完了していること。

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

ブラウザセッションの再認証制御を有効にする

1. Secure Private Access 管理コンソールにログインします。
2. **>** に移動し、 をクリックします。
3. を選択し、 をクリックします。
4. をクリックして、ブラウザセッションの再認証を有効にするルールを追加します。

   a. ルールの名前を入力し、 をクリックします。

   b. ユーザーやグループなど、要件に基づいて条件を選択します。また、、、 などの条件を追加することもできます。

   c. 「**次へ**」をクリックします。

   d. 以下を構成します。

   - 「**再認証間隔**」: ユーザーが再認証を求められるまでのブラウザセッションの期間。間隔は5分から14日の間で設定でき、分、時間、または日で構成できます。
   - 「**最初の警告バナー表示時間**」: ユーザーのブラウザセッションが期限切れになる前に表示される、閉じることができる警告バナー。値は期限切れの5分から60分前に設定できます。残り2分になると2番目の警告バナーが表示され、セッション終了時にはセッション期限切れのオーバーレイが続きます。
   - 「**IDプロバイダードメイン**」: コンマ区切りの値として、IDプロバイダーの完全修飾ドメイン名 (FQDN)。1〜25個のドメインを指定できます。認証フローが中断されないように、IdPページではセッションバナーとブロックオーバーレイは非表示になります。古いセッションが完全に削除されるように、セッションの有効期限が切れるとこれらのドメインのCookieがクリアされます。ワイルドカードがサポートされています (例: *.auth0.com)。

   セッション再認証(/en-us/citrix-secure-private-access/media/spa-browser-reauthentication-settings.png)

5. 「**次へ**」をクリックし、「**保存**」をクリックします。

   クリップボードコンテナポリシーに構成されているルールの数は、「**ブラウザポリシー > ブラウザセッション再認証**」タブに表示されます。

SSH制御

Citrix Secure Private Access は Chrome Enterprise Premium と統合されており、ブラウザ内で直接安全な SSH セッションを有効にします。この統合により、管理者とユーザーのセキュリティが強化され、アクセスが合理化されます。

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

組織は、SSH ベースのシステムの安全なリモート管理を必要としています。スタンドアロンの SSH クライアントを使用する従来の方法では、エンドポイントを管理されていない環境に公開し、堅牢なデータ損失防止 (DLP) の適用が不足しているため、リスクが生じ、コンプライアンスが困難になります。

SSH セッションは、スタンドアロンの SSH クライアントではなく Chrome ブラウザ内で起動されるようになり、ローカルインストールへの依存が減り、コンプライアンスが向上します。

注:

- この機能は、ハイブリッドおよびクラウド展開向けの Chrome Enterprise Premium 統合 Secure Private Access セットアップに適用されます。詳細については、次のトピックを参照してください。
- Secure Private Access および Chrome Enterprise Premium ポリシーを構成するには、管理者権限が必要です。
- FreeBSD サーバーへの接続はサポートされていません。

この統合の利点

この統合には、次の主要な利点があります。

- **セキュリティの強化:** 管理されていない SSH クライアントへの依存をなくし、セキュリティリスクへの露出を減らします。
- **アクセスの簡素化:** ブラウザネイティブのアクセスを提供し、追加のソフトウェアインストールの必要性をなくします。
- **コンプライアンス:** ブラウザ内で直接企業の DLP ポリシーを適用し、規制要件への準拠を支援します。
- **運用効率:** エンドポイント管理とクライアント展開に関連する IT オーバーヘッドを削減します。

ユースケース

この機能は、次のようなさまざまなユースケースをサポートします。

- **医療キオスク:** ネイティブクライアントをインストールせずに、デバイスのトラブルシューティングのための安全なSSHアクセスを可能にします。
- **IT管理:** 管理者は、DLPポリシーが適用された管理対象のChromeブラウザからLinuxサーバーに安全にアクセスできます。

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

- **請負業者アクセス:** 組織のセキュリティ体制を損なうことなく、サードパーティベンダーに一時的なSSHアクセスを提供します。

システム要件

環境が次の要件を満たしていることを確認してください。

- Chrome Enterprise Premiumの最新バージョン。
- Citrix Secure Private Accessが統合用に構成されていること。
- SSHトラフィックを許可するアクセスポリシーは、Secure Private Access管理コンソールで作成する必要があります。

前提条件

SSHアプリケーションへのセキュアアクセスを有効にするために、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。

- Citrix Secure Private AccessがGoogle Chrome Enterprise Premium統合で構成されていること。詳細については、「Google Chrome Enterprise Premiumとの統合」を参照してください。
- エンドユーザーが、Citrix Secure Accessブラウザ拡張機能を備えた最新のGoogle Chromeブラウザをインストールしていること。
- 展開固有の前提条件については、次のトピックを参照してください。
  - クラウド展開 - Citrix Secure Private Accessの概要
  - ハイブリッド展開 – システム要件と前提条件

SSHアクセス用にSecure Private Accessを構成する

1. Citrix Cloudにログインし、**Secure Private Access**をクリックします。
2. 管理コンソールで、**Applications > App Configuration**をクリックし、次に**Add an app**をクリックします。
3. セキュア プライベート アクセス内で、SSHアプリをTCP/UDPアプリとして構成します。
   - アプリは、サーバーの正確なIPアドレス、範囲、FQDN、またはホスト名を持つことができます。
   - SSHは、デフォルトポートおよび非デフォルトポートでサポートされています。
4. 関連するユーザーグループにアクセスを割り当てます。

TCP/UDPアプリの作成に関する詳細については、次のトピックを参照してください。

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

- クラウド展開 - TCP/UDPアプリのサポート
- ハイブリッド展開 – TCP/UDPアプリのサポート

SSHポリシーを構成する

1. Secure Private Access管理コンソールにログインします。
2. **Policies > Browser Policies**に移動し、次に**Create browser policy**をクリックします。
3. **SSH**を選択し、次に**Manage**をクリックします。
4. ユーザーがSSHを有効にするためのルールを追加するには、「**ルールを追加**」をクリックします。
5. ルールの名前を入力し、「**次へ**」をクリックします。
6. ユーザーまたはグループなど、要件に基づいて条件を選択します。1. **地理的位置、ネットワークロケーション、デバイスポスチャチェック**などの条件を追加することもできます。
7. 「**次へ**」をクリックします。
8. 「**保存**」をクリックします。

アンチキーロギングポリシー用に構成されたルールの数は、「**ブラウザポリシー > SSH**」タブに表示されます。

リモートデスクトップ制御

Citrix Secure Private Access は Chrome Enterprise Premium と統合されており、ブラウザ内で直接安全な RDP セッションを可能にします。この統合により、管理者とユーザーのセキュリティが強化され、アクセスが合理化されます。

従来のリモートデスクトップアクセスは、多くの場合、ネイティブの RDP クライアントに依存しており、通常、ブラウザベースの DLP 適用機能がありません。この欠陥は、特に管理されていない環境においてセキュリティリスクを高め、コンプライアンスを困難にする可能性があります。組織は、これらの懸念に対処する、安全で準拠した簡素化されたリモートアクセスソリューションを必要としています。

この統合により、管理者はクリップボード制御やスクリーンショット防止などのエンタープライズグレードの DLP 制御を適用できます。

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

注:

- この機能は、ハイブリッドおよびクラウド展開向けの Chrome Enterprise Premium 統合 Secure Private Access セットアップに適用されます。詳細については、以下のトピックを参照してください。
- Secure Private Access および Chrome Enterprise Premium ポリシーを構成するには、管理者権限が必要です。

サポートされていない機能:

以下の機能はサポートされていません。

- クリップボード共有
- オーディオ/Webカメラ/スマートカード/USB リダイレクト
- 2要素認証および生体認証

この統合の利点

この統合は、以下の主要な利点を提供します。

- **セキュリティ:** きめ細かな DLP ポリシーを適用することで、リモートセッション中のデータ漏洩を防ぎます。
- **コンプライアンス:** 堅牢なセキュリティ制御により、機密性の高い環境向けの規制要件の遵守に役立ちます。
- **使いやすさ:** 個別のRDPクライアントをインストールする必要がなくなり、ユーザーアクセスと展開が簡素化されます。
- **柔軟性:** 管理対象のChromeブラウザからの安全なRDPアクセスをサポートし、一貫性のある安全なエクスペリエンスを提供します。

ユースケース

この機能は、次のようなさまざまなユースケースをサポートします。

- **企業請負業者:** 内部セキュリティを損なうことなく、サードパーティベンダーに安全なリモートデスクトップアクセスを提供します。
- **医療スタッフ:** 医療現場のキオスクまたは共有ワークステーションからWindowsシステムへの安全なアクセスを可能にします。

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

- **ITサポート:** 追加のソフトウェアインストールを必要とせずに、IT担当者がリモートデスクトップのトラブルシューティングを行うことを可能にします。

システム要件

環境が次の要件を満たしていることを確認してください。

- Chrome Enterprise Premiumの最新バージョン。
- Citrix Secure Private Accessが統合用に構成されていること。
- RDPトラフィックを許可するアクセスポリシーは、Secure Private Access管理コンソールで作成する必要があります。

前提条件

RDPアプリケーションへの安全なアクセスを有効にするには、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。

- Citrix Secure Private Access は Google Chrome Enterprise Premium 統合で構成されています。詳細については、「Integration with Google Chrome Enterprise Premium」を参照してください。
- エンドユーザーは、Citrix Secure Access ブラウザ拡張機能を備えた最新の Google Chrome ブラウザをインストールしている必要があります。
- 展開固有の前提条件については、次のトピックを参照してください。
  - クラウド展開 - Citrix Secure Private Access の利用を開始する
  - ハイブリッド展開 – System requirements and prerequisites

RDPアクセス用にSecure Private Accessを構成する

1. Citrix Cloud にログインし、**Secure Private Access** をクリックします。
2. 管理コンソールで、**Applications > App Configuration** をクリックし、**Add an app** をクリックします。
3. Secure Private Access 内で RDP アプリを TCP/UDP アプリとして構成します。
   - アプリには、正確な IP アドレスまたは範囲、FQDN、あるいはサーバーのホスト名を設定できます。
   - RDP は、デフォルトポートおよび非デフォルトポートでサポートされています。
4. 関連するユーザーグループにアクセスを割り当てます。

TCP/UDP アプリの作成に関する詳細については、次のトピックを参照してください。

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

- クラウド展開 - Support for TCP/UDP apps
- ハイブリッド展開 – Support for TCP/UDP apps

リモートデスクトップポリシーを構成する

1. Secure Private Access管理コンソールにログインします。
2. **ポリシー > ブラウザポリシー** に移動し、**ブラウザポリシーの作成** をクリックします。
3. **リモートデスクトップ** を選択し、**管理** をクリックします。
4. **ルールの追加** をクリックして、ユーザーがリモートデスクトップを有効にするためのルールを追加します。
5. ルールの名前を入力し、**次へ** をクリックします。
6. ユーザーまたはグループなど、要件に基づいて条件を選択します。 1. **地理的位置、ネットワークロケーション**、および **デバイスポスチャチェック** などの条件を追加することもできます。
7. **次へ** をクリックします。
8. **保存** をクリックします。

アンチキーロギングポリシー用に構成されたルールの数は、**ブラウザポリシー > リモートデスクトップ** タブに表示されます。

CEP 統合の問題のトラブルシューティング

この記事では、Citrix Secure Private Access と Chrome Enterprise Premium (CEP) の統合を完了したが、アプリケーションにアクセスできない顧客管理者向けのトラブルシューティングワークフローについて説明します。

基本的な前提条件:

- 顧客管理者が Google Directory とのディレクトリ同期を完了していること。
- 顧客が Secure Private Access で Chrome Enterprise のオンボーディングを正常に完了していること。
- ユーザーまたはユーザーが属するグループが関連するアプリケーションにアクセスできるように、アプリケーションとアクセスポリシーが Secure Private Access 管理コンソールで構成されていること。
- ユーザーがオンボーディングされたドメインにログインしていること。
- ブラウザがインターネットに接続されていること。

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

CEP 統合のトラブルシューティング(/en-us/citrix-secure-private-access/media/troubleshooting-cep-integration.png)

CEP トラブルシューティングのための診断ログ

調査を効率化するために、サポートケースを開く前に以下の診断情報を収集し、すべての提出物に含めてください。

1. Chrome ポリシーをエクスポートします。
   a. Chrome を開き、chrome://policy/ に移動します。
   b. **その他の操作**をクリックし、**JSON にエクスポート**を選択します。
   c. エクスポートされたファイルをサポートケースに添付します。
2. Secure Enterprise Browser拡張機能の詳細ログを有効にします。
   a. Secure Enterprise Browser拡張機能の横にある省略記号アイコンをクリックします。
   b. オプションをクリックし、**ログレベル**を**すべて**に設定します。
   c. Chromeを閉じて再度開きます。
   d. 拡張機能オプション (省略記号アイコン) に戻り、**ログをダウンロード**をクリックします。
3. 拡張機能ログを収集します。
   a. Chromeを閉じて再度開きます。
   b. ステップ2を繰り返して**拡張機能**オプションにアクセスし、**ログをダウンロード**をクリックします。
   c. ダウンロードしたファイルをサポートケースに添付します。
4. ネットワークログをキャプチャします。
   a. Chromeでchrome://net-export/に移動し、**ディスクへのログ記録を開始**をクリックします(デフォルトのファイル名はchrome-net-export-log.jsonです)。
   b. いくつかのSaaSおよびWebアプリケーションにアクセスし、chrome://net-export/に戻って**ログ記録を停止**をクリックします。
   c. 結果のファイルをサポートケースに添付します。

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

ユーザーが正しいChromeプロファイルにログインしていることを確認します

確認方法: Chromeブラウザの右上隅でプロファイルアイコンをクリックします。アプリケーションにアクセスしようとしているプロファイルに対して、正しいユーザーと正しいドメインが表示されている必要があります。

また、プロファイルが**一時停止**または**サインインをクリック**と表示されていないことを確認してください。表示されている場合は、再認証する必要があります。

- **プロファイルが正しく認証されている場合:** (#check-secure-enterprise-browser-extension-installed)に進みます。
- **プロファイルが正しくないか、認証されていない場合:** 正しいプロファイルでログインまたは再認証してください。ユーザーのメールのドメインサフィックスが、Secure Private Accessがインストールされているグーグル管理アカウントのドメインと一致していることを確認してください。

Secure Enterprise Browser拡張機能がインストールされているか確認する

確認方法: Chromeブラウザの右上隅に、Secure Enterprise Browser拡張機能に対応する緑色の盾のアイコンがあるはずです。すべての拡張機能を表示するには、ジグソーパズルのピースをクリックする必要があるかもしれません。

- **拡張機能が存在する場合:** (#check-secure-enterprise-browser-extension-policy)に進みます。
- **拡張機能が存在しない場合:** (#check-extensioninstallforcelist-policy)に進みます。

ExtensionInstallForcelistポリシーを確認する

確認方法: (chrome://policy/)に移動し、**Chromeポリシー**の下で**ExtensionInstallForcelist**という名前のポリシーを探します。対応する行の末尾にある**詳細を表示**をクリックして、ポリシーの詳細を確認します。

この強制リスト内に、ID: `ekajlcmdfcigmdbphhifahdfjbkciflj`の拡張機能が表示されるはずです。これはSecure Enterprise Browser拡張機能に対応します。

2つの競合するポリシーがあることを示唆する警告が表示される可能性があります。

- **競合の警告と競合するポリシー内の拡張機能:** (#troubleshoot-conflicting-extension-install-list-policies)に進みます。

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

- **ポリシーが見つからない場合:** ポリシーが完全に存在しない場合、ユーザーはSecure Enterprise Browserを使用するように構成されておらず、(#check-user-extension-configuration-within-google-admin-console)を実行する必要があります。
- **ポリシーから拡張機能が見つからない場合:** (#check-user-extension-configuration-within-google-admin-console)に進みます。

競合する拡張機能インストールリストポリシーのトラブルシューティング

競合するポリシーがあることは、必ずしもSecure Private AccessでCEPをサポートする上での障害となるわけではありません。ただし、有効なポリシーは以下の3つの拡張機能のインストールを強制する必要があります。

- セキュア エンタープライズ ブラウザ (`ekajlcmdfcigmdbphhifahdfjbkciflj`)
- シトリックス セキュア アクセス (`loifegnemklkgbmonigcdkmniboielgl`)
- エンドポイント検証 (`callobklhcbilhphinckomhgkigmfocg`)

Secure Private Accessの拡張機能ポリシーの競合を解決するには、Chrome Policy Hierarchy Guideに基づいて、以下の手順に従ってください。

1. **競合の特定:** `chrome://policy`に移動します。**ExtensionInstallForcelist**を見つけて、**Status**と**Source**を確認します。
2. **優先順位の分析:** マシンレベルのポリシー (GPO) は、通常、クラウド/ユーザーレベルのポリシーよりも優先されることに注意してください。
3. **調和:** 最も優先順位の高いポリシーに、必要な3つの拡張機能IDすべてが含まれていることを確認します（追加の拡張機能が含まれていても問題ありません）。あるいは、ブラウザとプロファイルが同じGoogle Workspace組織によって管理されている場合は、ポリシーマージ機能を使用できます。
4. **確認: Reload policies**をクリックします。**Applies to**と**Level**の列で、必要な拡張機能が**Mandatory**であり、有効なレベルでアクティブであることを確認する必要があります。

拡張機能のインストールリストポリシーを修正した後も問題が解決しない場合は、Secure Enterprise Browser拡張機能ポリシーの確認に進んでください。

Secure Enterprise Browser拡張機能ポリシーの確認

確認方法: chrome://policyに移動し、**Secure Enterprise Browser**の下にある**securityGateway**という名前のポリシーを探します。**Show More**をクリックして、完全なポリシー構成を表示します。その値は次の形式であると予想されます。

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

```
{

  "authentication": {},

  "context": {

    "resource": "projects/project-<tenant_id>-<random-hex-characters>/
locations/global/securityGateways/securitygateway-<tenant_id>-<random-hex-
characters>"

  },

  "externalHelper": {

    "id": "com.citrix.device_posture_context_provider",

    "metadata": {

      "action": "device/metadata",

      "input": [

        {

          "key": "tenantId",

          "stringValue": "<tenant_id>"

        }

      ]

    }

  },

  ...

}
```

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

`tenant_id` フィールドに、Citrix CloudテナントIDに対応する値があることを確認してください。この値が異なる場合、2番目のテナントがこのGoogleアカウントと統合するように構成されている可能性があります。

- **ポリシーがない、または空の場合:** ポリシーが完全に存在しない場合、Secure Enterprise Browser拡張機能がSecure Private Accessだけでなく顧客によっても構成されており、ユーザーが以前または手動の構成から空の拡張機能構成を取得していることを示唆しています。Google管理コンソール内でユーザー拡張機能の構成を確認する必要があります。
- **ポリシーに誤ったCitrixテナントIDが入力されている場合:** ポリシーは存在するが、その値が例と一致しない場合、テナントIDが異なるか、2つの競合するポリシーが存在します。Google管理コンソール内でユーザー拡張機能の構成を確認するに進んでください。
- **ポリシーが正しい場合:** ルートがフェッチされているか確認するに進みます。

Google 管理コンソール内のユーザー拡張機能構成を確認する

確認方法: https://admin.google.comに移動します。ここから、**Chrome ブラウザ > アプリと拡張機能**に移動します。このビュー内で、適用されているすべてのポリシー構成を見つける必要があります。

概要タブ（存在する場合）をクリックし、**Secure Enterprise Browser**アプリを選択します。左側の**インストールポリシー**の下には、**\<primary domain\> に強制インストールされ、固定されています**と表示されている必要があります。ここで、\<primary domain\> は Google 管理コンソールの最上位組織部門に対応します。

拡張機能の**展開設定**を表示するためにクリックすると、**拡張機能のポリシー**構成を探します。これは、Secure Enterprise Browser 拡張機能ポリシーの確認セクションで説明されている内容と一致している必要があります。

- **単一のポリシーが正しい場合:** 親 OU のポリシーが正しいように見える場合、テストしているユーザーが該当するアカウントに属していること、およびサブ OU またはグループレベルで親 OU のポリシーを上書きする可能性のある他の構成がないことを確認する必要があります。メンバーシップが確認されても問題が解決しない場合は、Citrix サポートにお問い合わせください。
- **ポリシーが見つからない場合:** ポリシーが完全に存在しない場合、この Google アカウントは Secure Enterprise Browser を使用するように構成されておらず、Secure Private Access 管理コンソールで CEP 統合を検証する必要があります。
- **複数のポリシー - 複数の Citrix アカウント:** Secure Enterprise Browser 拡張機能に複数の構成が表示される場合、これは関連するポリシーの構成が正しくない原因である可能性がありま

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

す。複数の Citrix アカウントを同じ Google アカウントに関連付けることは禁止されていませんが、統合が機能しない原因となる可能性があります。

- **複数のポリシー - 単一の Citrix アカウント:** 1つの Citrix テナントのみを統合している場合、組織内の他の管理機能がこの拡張機能を構成していないことを確認する必要があります。この拡張機能のポリシー構成を提供している人が他にいないと確信できる場合は、Secure Private Access 管理コンソールを通じて統合した Citrix テナントに対応しないポリシー構成を削除することができます。

  不要な拡張機能構成を削除し、ブラウザを再起動してもアプリケーションにアクセスできない場合は、Citrix サポートにお問い合わせください。

ルートがフェッチされているか確認する

確認方法: chrome://extensions/?options=ekajlcmdfcigmdbphhifahdfjbkciflj に移動するか、Secure Enterprise Browser 拡張機能を右クリックして**オプション**を選択します。

ログレベルを**すべて**に設定し、**ログを表示**をクリックします。ログが表示されたら、ブラウザを閉じて、ログページに移動するプロセスを繰り返します。これにより、トラブルシューティングに必要なログの完全なセットが取得されます。

ログ内で、次の内容を含むログ行を検索します。

`Calling 'https://api.prod.securegateway.goog/api/v1/routes'`

これに続いて、次のような応答が表示されるはずです。

`[260220 17:07:51.64] [SG.ApiClient] [DEBUG] Response: {expirationTime: '2026-02-20T15:37:51Z', proxyUrl: 'https://api.prod.securegateway.goog',...`.

- **コンテキストルートのログに403ステータスコードが表示される場合:** この403は、Zscaler、Umbrellaなどの傍受ファイアウォールによって返される可能性があります。
  - この場合、Google Security Gateway宛てのトラフィックが統合ソリューションの前提条件に従って許可されていることを確認してください。
  - そうでない場合は、ユーザープロファイルに認証の問題がある可能性があり、Secure Private AccessとCEPの統合が不完全であることを示唆している可能性があります。Secure Private Access管理コンソールでCEP統合を検証するに進んでください。
- **コンテキストルートでタイムアウト、DNSエラー、または503エラーが表示される場合:** Google Secure Gatewayの到達可能性のトラブルシューティングに進んでください。

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

- **コンテキストルートが成功したように見える場合 (200 OK):** ルートへのアプリケーションの組み込みを確認するに進んでください。

Secure Private Access管理コンソールでCEP統合を検証する

Citrix CloudコンソールのSecure Private Access内にある**ブラウザ設定**セクションにアクセスします。

このセクションで、以下を確認します。

- **Google Chrome統合ステータス**が**完了**と表示されている必要があります。失敗している場合は、ドキュメントに従ってCEP統合の前提条件の手順を完了していることを確認し、再試行してください。問題が解決しない場合は、Citrixサポートにお問い合わせください。
- **顧客ID**には、統合するGoogleアカウントに対応する値が必要です。この値は、Google管理コンソールの**アカウント > アカウント設定**で確認できます。

上記のすべての値が正しいにもかかわらず、Chromeブラウザで正しい拡張機能構成が得られない場合は、Citrixサポートにお問い合わせください。

Google Secure Gatewayの到達可能性のトラブルシューティング

確認方法: URL `https://api.prod.securegateway.goog/api/v1/routes` をコピーし、ブラウザのアドレスバーでこのURLに移動します。HTTP 401エラー応答が表示されるはずです。これは予期される動作であり、Google Secure Gatewayへのネットワーク接続が正常に確立できることを示しています。

- **DNS解決エラー:** これは、貴社がGoogle Security Gateway FQDNのルックアップを妨げるような、制限的なDNS解決設定を導入している可能性があることを示唆しています。ただし、これはこの機能を使用するための前提条件であり、該当するFQDNは解決可能である必要があります。
- **リクエストがハングするか、タイムアウトエラーページが表示される:** これは、ブラウザとインターネット間のファイアウォールが、Googleのセキュリティゲートウェイ宛てのトラフィックを破棄している可能性が高いことを強く示唆しています。統合ソリューションの前提条件に従って、前提条件となるインターネットロケーションがネットワークから到達可能であることを確認してください。

正しいルートがまだ受信されない場合は、Citrixサポートにお問い合わせください。

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

ルートへのアプリケーションの組み込みを確認する

正常なルート応答には、Secure Private Access管理者によって構成されたアプリケーションに対応するFQDNが含まれます。例:

```
[260318 06:42:38.99] [SG.ApiClient] [DEBUG] Response: {expirationTime:
'2026-03-18T14:15:05Z', proxyUrl: 'https://via.prod.securegateway.goog',
endpointMatchers: [{hostname: 'telemetry.netscalergateway.net'},
{hostname: 'www.workday.com'}, {hostname: '*.workday.com'}, {hostname:
'jira.internal.corp'}, {hostname: '*.jira.internal.corp'}]}.
```

この行に、アクセスしようとしているアプリケーションが含まれていますか？

- **アクセスできないアプリケーションがルート応答に含まれている:** ルーティングされたアプリケーションアクセスをトラブルシューティングするに進んでください。
- **ルート応答にtelemetry.netscalergateway.netのみが含まれている:** 追加のアプリケーションと包括的なアプリケーションポリシーを構成してみてください。それでもルートに表示されない場合は、グループメンバーシップの問題、またはCitrixで構成されたIdPとGoogle Directory間のグループの不一致が強く示唆されます。IdPとGoogle Directoryの整合性を確保するに進んでください。
- **アクセスできないアプリケーションがルート応答に含まれていない:** これは、Secure Private Access管理コンソールでアプリケーションが正しく構成されていないことを示唆しています。アプリケーションが存在し、ポリシー（アクセスを許可または拒否するいずれか）が関連付けられていることを確認してください。アプリケーションが構成されていると確信しているにもかかわらず、上記のルートにまだ表示されない場合は、Citrixサポートにお問い合わせください。

ルーティングされたアプリケーションアクセスのトラブルシューティング

アプリケーション（ルートリストに表示されるもの）にアクセスしようとしたとき、どのような動作が観察されますか？

- **ドメイン解決エラー (ERR_NAME_NOT_FOUND) が発生している**

  これは、アプリケーションが正しく構成されていないか、コンテキストルートが正しく受信されていない可能性が高いことを示唆しています。

- **「アクセス拒否」と表示されたクリーム色のページ**

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

これは、Secure Private Accessコンソールでのポリシー構成が、現在のユーザーを含むように設定されていないことを示唆しています。

- **「Oops! Something went wrong.」と表示されたクリーム色のページ**

  このエラーページが表示される最も一般的な原因は、コネクタがターゲットアプリケーションに到達できないことです。この場合、Citrixのドキュメントに従って、内部アプリケーションへのコネクタアクセスをトラブルシューティングしてください。一般的な問題には、次のものがあります。

  - 内部DNSの到達可能性
  - バックエンドサービスがダウンしている
  - ファイアウォールルール

- **大きな赤いフォントで「Service Unavailable」と表示された白いページ**

  これは一時的なエラーである可能性があり、数分後に解決する場合があります。

  問題が解決しない場合は、Citrixサポートにお問い合わせください。

- **タイムアウト**

  - まず、Chromeのアドレスバーに `via.prod.securegateway.goog` を入力して、到達可能であることを確認します。401応答を受信する必要があります。タイムアウトする場合は、中間ファイアウォールまたはプロキシがアクセスをブロックしており、アプリケーションにアクセスする前に解決する必要があります。
  - アプリケーションのタイムアウトのもう1つの潜在的な原因は、インターネットおよび特にGoogle Security Gatewayへのトラフィックをブロックするファイアウォールです。これは、顧客がインターネットにアクセスするために明示的なプロキシを必要とするシナリオでよく見られます。Chrome Enterprise PremiumとのSecure Private Access統合は、このプロキシ構成をサポートしていません。

- **証明書エラー**

  アプリケーションがプライベートCA証明書を使用している場合、ブラウザが「信頼されていない証明書エラー」をスローする可能性があります。Chrome Enterprise Premiumの設定を通じて、顧客は信頼されたルートCAをブラウザにプッシュできます。詳細については、「Chrome Enterprise Premiumを使用してルート証明書構成を管理する」を参照してください。

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

IdPとGoogleディレクトリの整合性を確保する

Chrome Enterprise PremiumとのSecure Private Access統合の場合、ディレクトリとGoogleディレクトリの同期は、「統合ソリューションの前提条件」で説明されているいくつかの仕様に従う必要があります。

ユーザーおよびユーザーグループのメールアドレスが正しく、ソースディレクトリで構成されている内容と一致している場合は、Google 管理コンソールでグループのアクセス設定を確認するに進みます。

Google 管理コンソールでグループのアクセス設定を確認する

Google 管理コンソールで、**ディレクトリ > グループ**に移動し、アクセス ポリシーを構成し、アプリケーションがロードされないグループを選択します。

そこから、**アクセス設定**を選択し、**メンバーを表示できるユーザー**の行で**グループメンバー**オプションが有効になっていることを確認します。この構成は、Secure Private Access でポリシーを作成するすべてのグループに適用する必要があります。

このオプションがすでに有効になっている場合は、Citrix サポートにお問い合わせください。

CEP統合における既知の問題

Chrome Enterprise Premium との Secure Private Access 統合において、以下の既知の問題があります。

Secure Private Access ユーザーインターフェイス

- **問題:** セッションポリシーの設定では、3つの条件が利用可能であるにもかかわらず、現在、ユーザーは2つのシミュレート条件しか追加できません。これにより、ポリシー作成の柔軟性が制限されます。

  回避策: 2つの個別のセッションポリシーを作成します。1つは2つのシミュレート条件を含むもの、もう1つは残りの条件を含むものです。

- **問題:** TCP/UDPのサーバーからクライアントへの構成オプションは、すべての顧客環境のアプリケーション構成UIで利用できません。これにより、サーバーからクライアントへのトラフィック動作を定義する機能が制限されます。

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

適応型アクセス ポリシー構成

- **問題:** ルールでOktaグループが指定されている場合、アクセスポリシーの作成が失敗します。この問題は、Oktaディレクトリに存在するグループにのみ影響します。

  回避策: OktaをIDプロバイダーとして使用できますが、ディレクトリとしては使用できません。OktaをIdPとして使用するには、まずオンプレミスのADをOktaと統合する必要があります。詳細については、「OktaをCitrix CloudへのIDプロバイダーとして接続する」を参照してください。

Google Chrome ブラウザ

- **問題:** Googleプロファイルピッカーが開いていて、既存のプロファイルがない状態でユーザーがCWAまたはChrome以外のブラウザからアプリを起動しようとすると、プロファイル作成ワークフローがトリガーされません。

  回避策: プロファイルピッカーを閉じて、アプリを再起動します。

- **問題:** 管理されたChromeプロファイルでCWAにログインし、アプリを起動しても、プロファイル作成後にユーザーが元の内部アプリURLに移動しません。

  回避策: プロファイル作成後、アプリを再起動します。

- **問題:** Google管理コンソールからグループを同期しても、グループに属するユーザーは自動同期されません。同期中に `whoCanViewGroupMembership` 設定が明示的に `ALL_MANAGERS_CAN_VIEW` に上書きされます。そのため、表示が制限されるのは想定内の動作です。

  回避策: Google 管理コンソールで、または API 経由で usomg を使用して、Google グループの権限を手動で更新します。詳細については、`<https://developers.google.com/workspace/admin/groups-settings/manage>` を参照してください。

- **問題:** 管理対象の Chrome プロファイルを通じて公開された SaaS/Web アプリケーションにアクセスすると、ユーザーはプロキシのポップアップを介してユーザー名とパスワードで認証を求められます。これは通常、一定期間の非アクティブ状態の後に発生します。

  原因:

  - プロキシトークンが利用できないか、プロキシトークンは利用可能だがその後期限切れになっている。
  - 初期化の遅延により、SEB 拡張機能の再初期化が必要になる。

  回避策: 新しいウィンドウで Chrome セッションを再起動します。

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

- **問題:** 管理対象の Chrome プロファイルまたは Citrix Workspace アプリを介して外部 SaaS アプリケーションにアクセスすると、ユーザーは断続的に「Service Unavailable」エラーを経験する可能性があります。この問題は、Google のインフラストラクチャにおける未解決のバックエンドの問題が原因です。

  回避策: サポートについては Google チームにお問い合わせください。

オープンIDコネクト (OIDC)

問題: 顧客が同じ Azure テナントに対して複数の Microsoft Entra ID 接続を持っている場合、OIDC クライアント構成中に Entra ID IdP を確実に区別できません。この問題は、IdP 選択の信頼性にのみ影響します。OIDC クライアント構成と認証動作には影響ありません。

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

Citrix Secure Private Access の利用を開始する

このドキュメントでは、SaaS アプリの配信を初めてオンボーディングして設定する方法について説明します。このドキュメントは、アプリケーション管理者向けです。

システム要件

- **オペレーティングシステムのサポート:** Citrix Workspace アプリは以下をサポートしています。
  - Windows 7、8、10、および 11
  - macOS - 10.11 以降
- **ブラウザのサポート:** Edge、Chrome、Firefox、または Safari の最新バージョンを使用して、クラウドストア URL 経由でアプリにアクセスします。
- **Citrix Workspace™ アプリのサポート:** デスクトッププラットフォーム (Windows、Mac) のいずれか向け Citrix Workspace アプリを使用してストアにアクセスします。
- ユーザーがカスタム URL を使用してストアにアクセスする場合、以下の最小バージョンを使用する必要があります。
  - Windows 向け Citrix Workspace アプリ: 2503.10 以降
  - Mac 向け Citrix Workspace アプリ: 2505.10 以降
  - Mac 向け Citrix Secure Access アプリ: 26.04.1.1 以降
  - iOS 向け Citrix Secure Access アプリ: 26.04.1 以降

仕組み

Citrix Secure Private Access は、IT およびセキュリティ管理者が、承認された SaaS および企業ホスト型 Web アプリへのエンドユーザーアクセスを管理するのに役立ちます。ユーザーの ID と属性はアクセス権限を決定するために使用され、アクセスコントロールポリシーは操作を実行するために必要な権限を決定します。ユーザーが認証されると、アクセスコントロールはそのユーザーの資格情報に関連付けられた適切なレベルのアクセスと許可されたアクションを承認します。

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

Citrix Secure Private Access は、複数の Citrix Cloud™ サービスの要素を組み合わせて、エンドユーザーと管理者向けに統合されたエクスペリエンスを提供します。

機能	機能を提供するサービス/コンポーネント
アプリにアクセスするための一貫したユーザーインターフェイス	ストアフロント クラウド
SaaSおよびWebアプリへのSSO	シトリックス ゲートウェイ サービス スタンダード
Webフィルタリングとカテゴリ分類	Webフィルタリングサービス
SaaS向け強化セキュリティポリシー	クラウドアプリ制御
セキュアブラウジング	リモートブラウザ分離サービス
Webサイトアクセスと危険な行動の可視化	シトリックス アナリティクス

Citrix Secure Private Accessサービスの使用を開始する

1. Citrix Cloudにサインアップします。
2. Secure Private Access サービス資格の要求。
3. 資格が付与されると、Secure Private Access サービスがお客様のアカウントにプロビジョニングされます。
4. Secure Private Access サービス管理 UI にアクセスします。
5. エンドユーザーが StoreFront Cloud でアプリを表示および起動するために使用するストアを構成します。

Citrix Cloud ホームページ(/en-us/citrix-secure-private-access/media/spa-on-citrix-cloud-page.png)

注:

- エンドユーザーがストアを使用し、アプリにアクセスするには、Citrix Workspace アプリをダウンロードして使用するか、Web ブラウザからストアの URL を開く必要があります。Citrix Secure Private Access ソリューションをテストするには、いくつかの SaaS アプリをストアに公開しておく必要があります。Workspace アプリは、ダウンロードからダウンロードできます。**ダウンロードの検索**リストで、**Citrix Workspace アプリ**を選択します。
- アウトバウンドファイアウォールが構成されている場合は、以下のドメインへのアクセスが許可されていることを確認してください。

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

- *.cloud.com
- *.nssvc.net
- *.netscalergateway.net

詳細については、Cloud Connector プロキシとファイアウォール構成およびインターネット接続要件を参照してください。

Secure Private Accessサービス展開モデル

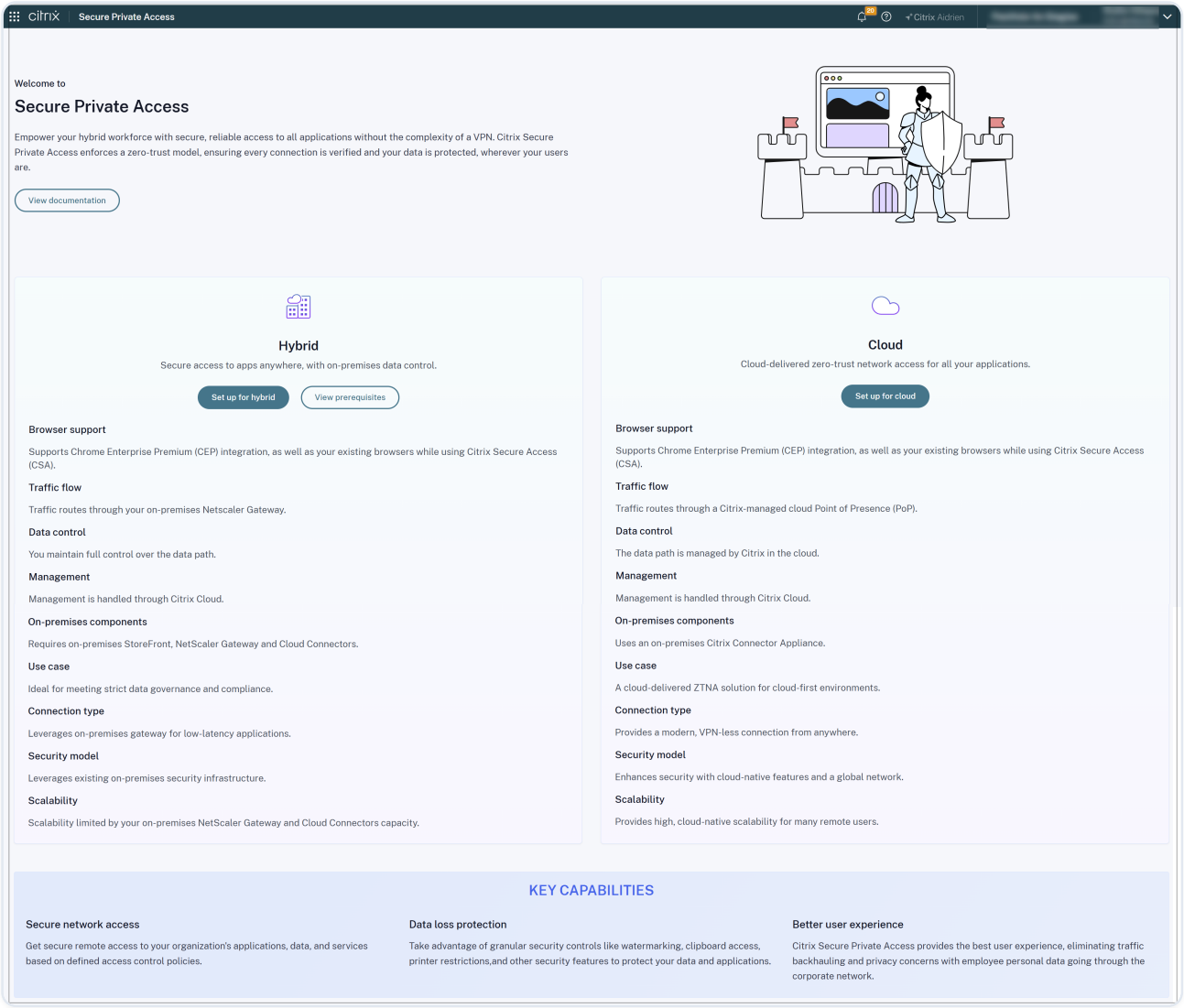
Secure Private Accessサービスは、2つのアーキテクチャオプションでお客様にご利用いただけます。

- **ハイブリッドサービスアーキテクチャ:** ハイブリッドサービスアーキテクチャを使用すると、オンプレミスのStoreFrontおよびNetScaler Gatewayコンポーネントを使用でき、すべてのユーザートラフィックがお客様の管理下に置かれることを保証します。また、サイト管理コンポーネントはCitrixによってホストおよび管理されます。詳細については、ハイブリッド展開を参照してください。
- **クラウドネイティブサービスアーキテクチャ:** クラウドネイティブサービスアーキテクチャは、オンプレミスまたはクラウドに展開されているかに関わらず、IT承認済みアプリケーションへの適応型アクセスを提供するクラウド提供のZTNAソリューションです。詳細については、Citrix Secure Private Accessを参照してください。

Secure Private Accessサービス管理コンソールからこれらのオプションを選択できます。

1. Citrix Cloud™にログインし、その後、**Secure Private Access**をクリックします。
2. 要件に応じて、**ハイブリッドのセットアップ**または**クラウドのセットアップ**を選択します。

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



Citrix Secure Private Access™ サービス向けPoP (Points of Presence) ロケーション

Citrix は、Citrix Secure Private Access のお客様向けに、事業継続性と高品質なサービスを確保するため、グローバルに PoP を追加しています。

セキュアプライベートアクセス管理 PoPs

以下は、Secure Private Access 管理 PoP ロケーションのリストです。

POP 名	ゾーン	リージョン
アズール ヨーロッパ西部 管理	Azure ウェストヨーロッパ	オランダ
アズール インド南部 管理	Azure 南インド	チェンナイ

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

POP 名	ゾーン	リージョン
az-us-e-mgmt	Azure イーストUS	バージニア

セキュアプライベートアクセス データPoP

以下は、Secure Private Access データPoPの場所のリストです。

POP名	ゾーン	リージョン
az-us-東	アジュール eastus	バージニア
az-us-西	アジュール westus	カリフォルニア
az-us-南中央	アジュール southcentralus	テキサス
Azure オーストラリア東部	アジュール オーストラリア東部	ニューサウスウェールズ
Azure ヨーロッパ北部	アジュール 北ヨーロッパ	アイルランド
Azure ヨーロッパ西部	アジュール 西ヨーロッパ	オランダ
Azure 日本東部	アジュール 東日本	東京、埼玉
Azure ブラジル南部	アジュール ブラジル南部	サンパウロ州
az-アジア-南東	Azure 南東アジア	シンガポール
az-UAE-北	Azure アラブ首長国連邦北部	ドバイ
az-インド-南	Azure 南インド	チェンナイ
az-アジア-香港	Azure 東アジア	香港
az-北西ヨーロッパ	Azure ノルウェー東部	ノルウェー

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

Secure Private Access のオンボーディングとセットアップ

Secure Private Access™ 管理コンソールを使用すると、管理者はSaaS、Web、およびTCP/UDPアプリケーションをオンボーディングおよび管理し、ユーザーがそれらのアプリケーションとどのようにやり取りするかを制御する詳細なアクセスポリシーを定義できます。

Citrix Secure Private Access は Google Chrome Enterprise Premium と統合されており、お客様は Google Chrome Enterprise Premium をエンタープライズブラウザとして使用して、プライベートWebアプリケーションやSaaSアプリケーションに安全にアクセスできます。

Secure Private Access をオンボーディングしてセットアップするための大まかな手順は次のとおりです。

1. Secure Private Access にユーザーをオンボーディングする
2. Citrix® StoreFront Cloud でストアURLを構成する
3. Google Chrome 統合をセットアップする。
4. Connector Appliance を構成する
5. ユーザーのアプリを追加する。
6. 必要なアクセスポリシーを作成して、アプリアクセスの権限を割り当てる。

重要：

Google Chrome をエンタープライズブラウザとして設定できます。詳細については、以下のトピックを参照してください。

- Google Chrome をエンタープライズブラウザとして設定する
- ブラウザを切り替える前の考慮事項

Secure Private Access にユーザーをオンボーディングする

Secure Private Access にユーザーをオンボーディングするには、次の手順を実行します。

1. Citrix Cloud™ にログインし、**Secure Private Access** をクリックします。

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

2. **Setup for cloud** を選択し、**Continue** をクリックします。

管理者ガイド付きワークフローの概要(/en-us/citrix-secure-private-access/media/spa-overview1.png)

トポロジ図は、Secure Private Access クラウド展開で使用されるコンポーネントを示しています。ヘルプアイコンをクリックすると、フロー内の各コンポーネントの簡単な説明を表示できます。

トポロジ図(/en-us/citrix-secure-private-access/media/spa-onboarding-topology.png)

- **新規のお客様の場合**、Citrix Cloud コンソールで Secure Private Access サービスを選択すると、セットアップページが開き、Connector Appliance と CEP を構成できます。
  - Connector Appliance を構成するには、**Connector Appliance Configuration** ペインで **Add** をクリックします。詳細については、「Connector Appliance の構成」を参照してください。
  - Google Chrome Enterprise Premium (CEP) を構成するには、**Google Chrome Enterprise Premium** ペインで **Set up** をクリックし、画面の指示に従います。詳細については、「Google Chrome 統合のセットアップ」を参照してください。

  セットアップが完了すると、その後のアクセス時に、管理者が Citrix Cloud コンソールで Secure Private Access をクリックすると、Secure Private Access ダッシュボードにリダイレクトされます。
- **既存のお客様の場合**、システムは以下を確認します。
  - Connector Appliance の可用性
  - Chrome Enterprise Premium のステータス

  Connector Appliance の確認: システムは、1 つ以上の Connector Appliance が構成されているかどうか、および利用可能な数を確認します。この確認は、管理者が、ユーザーが社内アプリケーション (Web、TCP/UDP) に正常に接続するために Connector Appliance の構成が必須であることを理解するのに役立ちます。Connector Appliance は、ネイティブの Citrix Secure Access クライアントを介したエンドユーザー接続を可能にし、顧客が選択した任意のブラウザをサポートします。

  Chrome Enterprise Premium 構成の確認: Chrome Enterprise Premium 構成の確認は、Citrix Secure Private Access と Chrome Enterprise Premium の統合が有効になっているかどうかを管理者が判断するのに役立ちます。この統合により、エンドユーザーはネイティブの Citrix Secure Access クライアントを必要とせずに、Chrome ブラウザを介して企業の Web アプリケーションに安全にアクセスできます。

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

注:

Google Chrome Enterprise Premium のセットアップはオプションであり、スキップできます。

Citrix StoreFront CloudでストアURLを構成する

Secure Private AccessサービスをCitrix® StoreFront Cloudと統合できます。ユーザーには、WebブラウザまたはCitrix Workspace™アプリで開くことができるストアURLを提供します。このストアは、構成されたSaaSアプリ、Webアプリ、仮想アプリ、およびその他の構成されたリソースに対して、統一されたユーザーエクスペリエンスを提供します。

デフォルトでは、ストアはURL `customerid.cloud.com` で作成されます。このURLを変更したり、たとえば `store.company.com` のような独自のカスタムURLを追加したりできます。ストアを構成するには、「ストアへのアクセスを構成する」を参照してください。

Google Chrome統合のセットアップ

Google Chrome統合ページで、次の手順を実行します。

1. 自動生成されたサービスアカウントのメールアドレスをコピーし、Google管理コンソールの適切なフィールドに貼り付けます。

   a. Google管理コンソールで、**管理者ロール**に移動します。

   b. Secure Private Accessサービス用に作成されたロールを選択し、推奨される権限を適用します。権限のリストについては、「管理者ロールと権限」を参照してください。

   c. **管理者**の下で、**サービスアカウントの割り当て**を選択します。

   d. Citrixサービスアカウント (`tenant-sa-<random-string>.iam.gserviceaccount.com`) を貼り付け、**追加**を選択します。その後、**ロールの割り当て**を選択します。

      ロールの詳細については、「管理者ロールについて」を参照してください。

   e. Google管理コンソールで、**ディレクトリ > ユーザー**に移動します。

   f. **新しいユーザーを追加**をクリックし、新しいユーザーを作成します (名: Citrix Service、姓: Account、プライマリメール: caccount)。新しく作成したユーザーのメールアドレスを控えておきます。

   g. 新しいユーザーが作成されたら、そのユーザーを選択し、**ユーザーの詳細**に移動します。**管理者ロールと権限**で、このユーザーに同じロールを選択して割り当てます。

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

h. **セキュリティ > アクセスとデータ制御 > API制御**に移動し、**ドメイン全体の委任を管理**をクリックします。

i. 「**API クライアント**」で「**新規追加**」をクリックし、Google Chrome 統合ページに記載されているそれぞれの情報でクライアント ID と OAuth スコープを入力します。

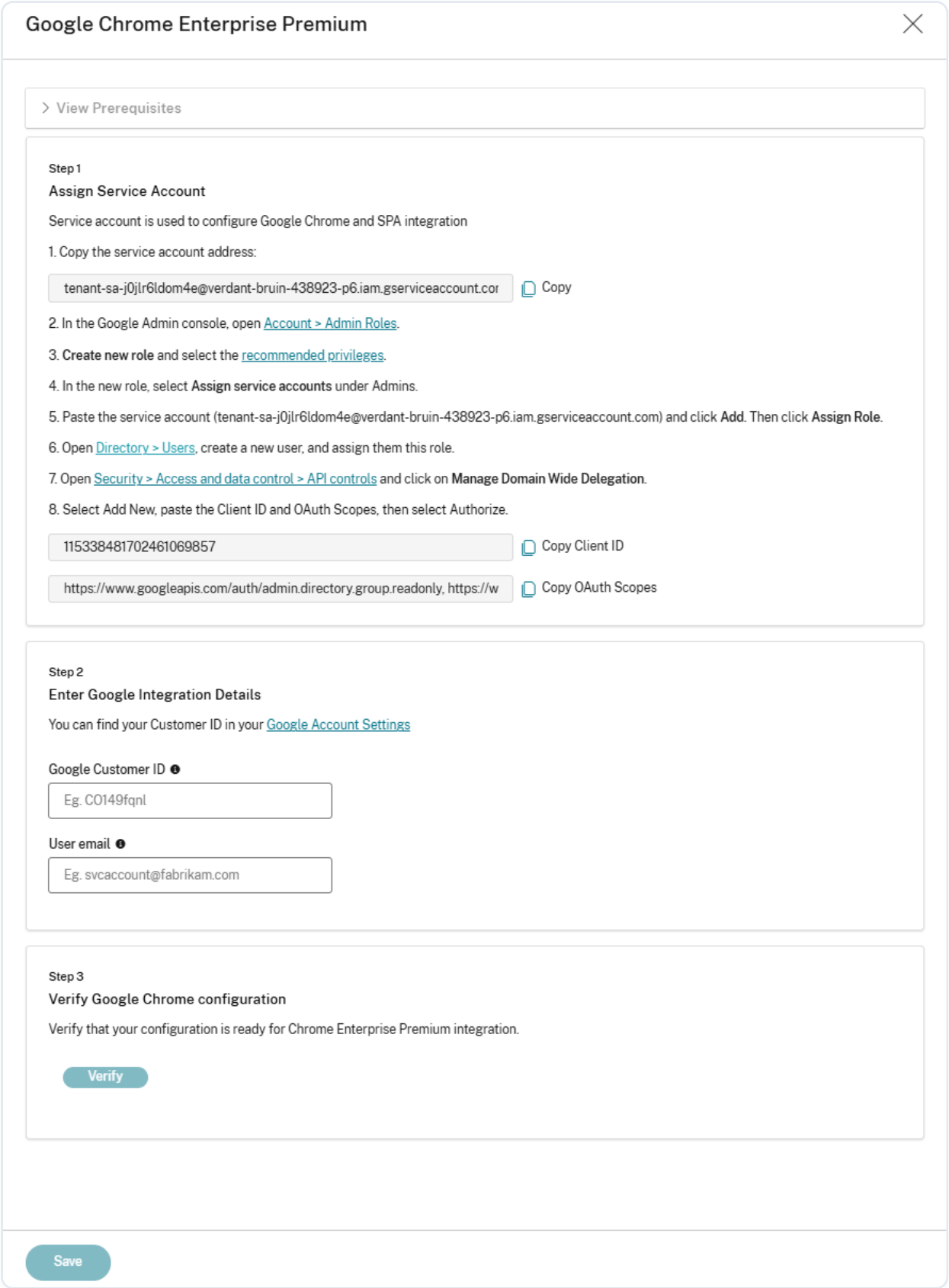
j. Google 管理コンソール内の「**Google アカウント設定**」にある Google 顧客 ID を、「**Google Chrome 統合**」ページの「**Google 顧客 ID**」フィールドにコピーします。

k. Google Chrome 統合ページの「**ユーザーメールフィールド**」に、以前作成したユーザーのメールアドレスを入力します。

2. 「**CEP 検証を実行**」をクリックして Google Workspace の構成を検証し、次のステップに進む前に Chrome Enterprise Premium 統合の準備が整っていることを確認します。

- 検証で失敗または警告が返された場合は、トラブルシューティングのガイダンスについて「既知の検証の失敗と警告」を参照してください。
- CEP 検証が成功すると、Secure Private Access サービスは Google 顧客 ID に正常に接続され、セキュアゲートウェイが作成されます。
- セキュアゲートウェイが正常に作成されると、システムにはそれに割り当てられたエグレス IP アドレスが表示されます。管理者は、Chrome Enterprise Premium が SaaS アプリケーションのトラフィックに使用するエグレスリージョンを選択できます。詳細については、「エグレスハブリージョンの構成」を参照してください。
- ユーザーが SaaS アプリケーションにアクセスしようとすると、リクエストは SaaS プロバイダーに直接送信されません。代わりに、トラフィックはまずパートナーコネクタとして機能するセキュアゲートウェイを経由してルーティングされます。このゲートウェイは仲介役として機能し、すべてのトラフィックが宛先アプリケーションに到達する前に検査および保護します。

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



3. 「**保存**」をクリックします。

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

重要：

- 顧客が CEP にオンボーディングされた後でも、統合の詳細を更新できます。詳細については、「オンボーディング後の Google 統合詳細の更新」を参照してください。
- オンボーディング中に、すべてのユーザーとユーザーグループに加えて、選択した Google Directory 組織部門に CEP 構成を適用できます。詳細については、「Google Directory 組織部門の CEP の構成」を参照してください。

- Google Chrome Enterprise Premium との Secure Private Access 統合の詳細については、「Google Chrome Enterprise Premium との統合」を参照してください。

SaaS アプリの IP アドレスを追加する

Secure Private Access と Chrome Enterprise Premium に顧客をオンボーディングした後、SaaS アプリケーションで使用される IP アドレスのリストを許可する必要があります。この手順は、以下を確実にするために重要です。

- ユーザーがネットワークセキュリティ制御による接続の問題やブロックなしに SaaS アプリケーションにアクセスできること。
- Citrix Secure Private AccessとChrome Enterprise Premiumからのトラフィックは正当なものとして認識され、誤ってフィルタリングされたり拒否されたりすることはありません。

注:

コネクタアプライアンス経由でルーティングされるアプリケーションで、「Internal via Connector」ルーティングタイプを使用する場合、お客様はCitrix IP許可リストを使用する必要があります。

プリンシパルアクセス境界ポリシーの構成

プリンシパルアクセス境界ポリシーは、エンドユーザーがCitrix管理のGoogle Secure Gatewayにアクセスするのを防ぐことができます。

GCP組織に、デフォルトでテナント間リソースへのアクセスをブロックするプリンシパルアクセス境界ポリシーがある場合は、Google Secure Gatewayへのアクセスを許可するプリンシパルアクセス境界ポリシーを作成します。Secure Gateway識別子は、**ブラウザ設定 > ブラウザ**ページから

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

取得できます。適切なポリシーの構成の詳細については、Google Cloud IAM - Principal access boundary policies documentationを参照してください。

オンボーディング後のGoogle統合詳細の更新

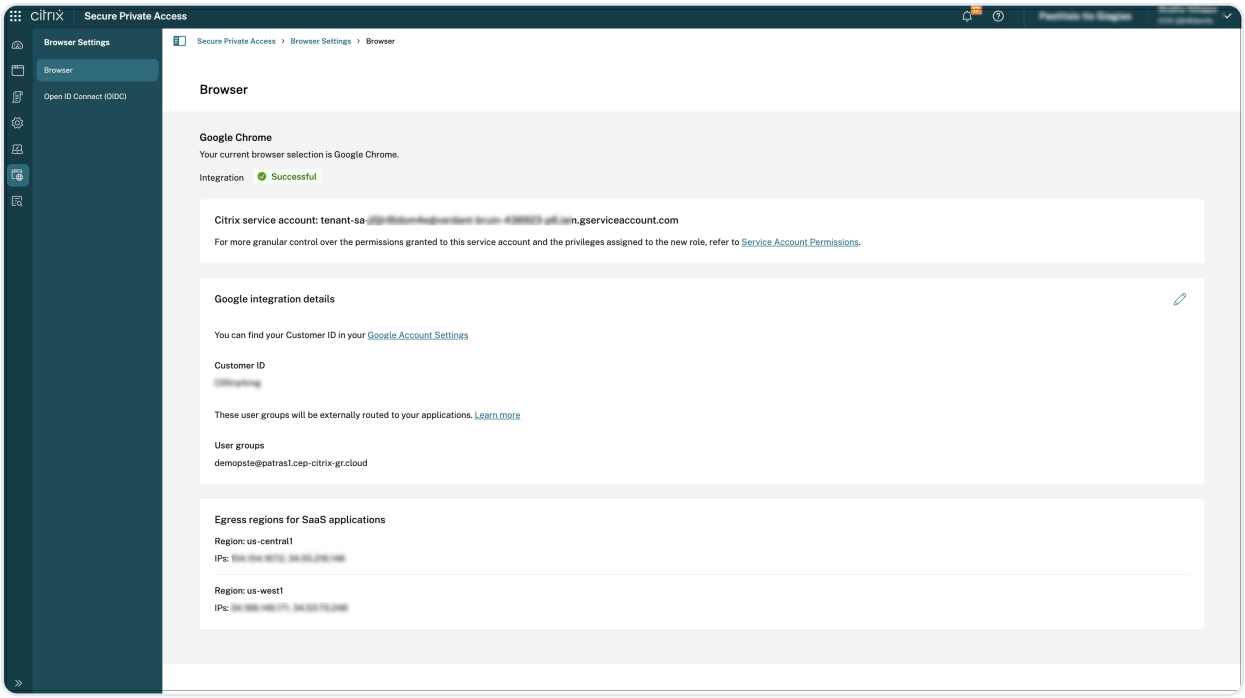
お客様がChrome Enterprise Premiumに正常にオンボーディングされると、Secure Private Accessはオンボーディング後の統合詳細の管理を可能にします。これには、顧客IDなどの重要な識別子を更新したり、関連するユーザーグループを変更したりする機能が含まれます。

オンボーディング後に統合詳細を更新するには、次の手順を実行します。

1. Secure Private Access管理コンソールで、**ブラウザ設定 > ブラウザ**に移動します。

   ブラウザページには、Google Chrome統合の詳細が表示されます。

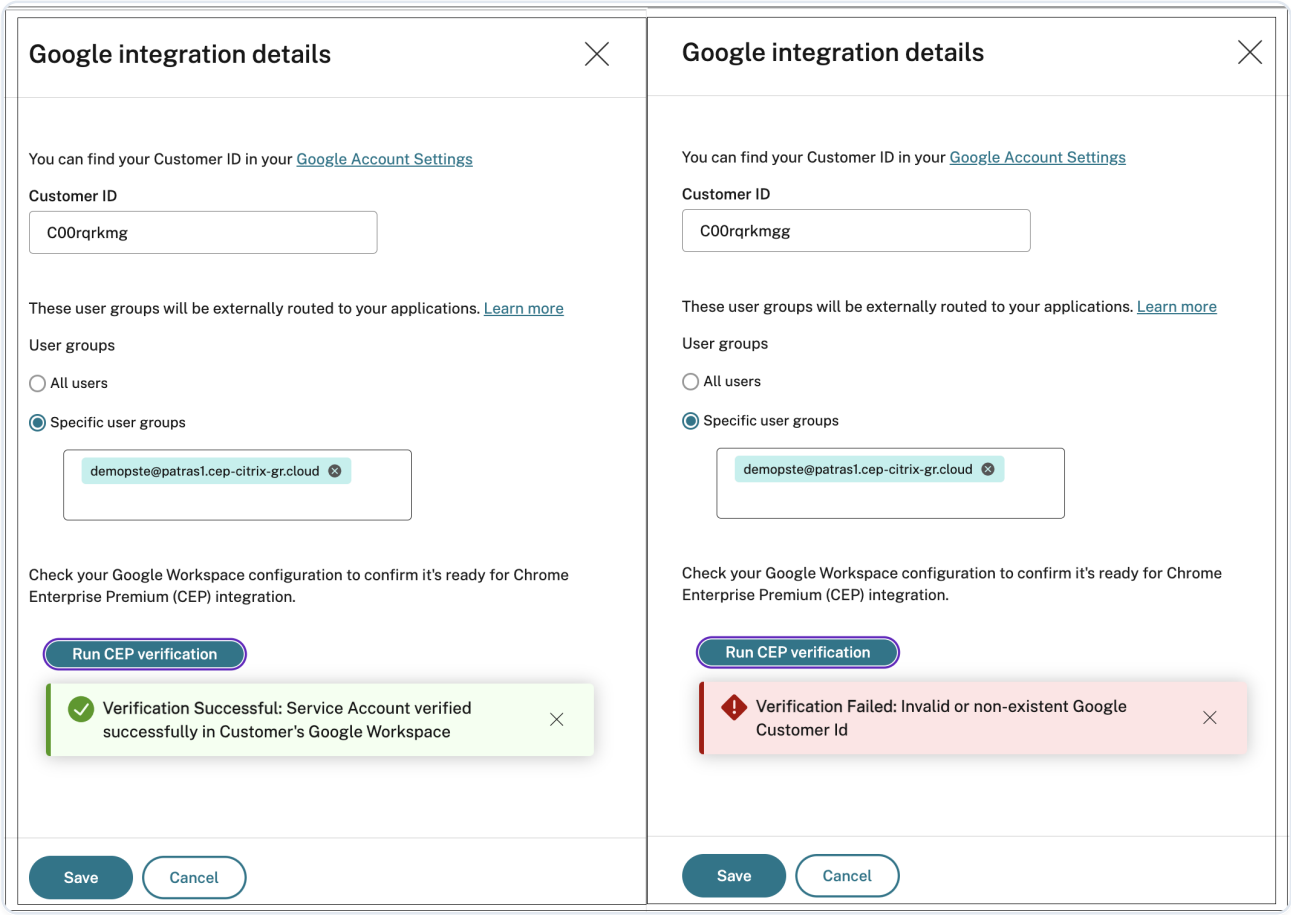
   システムは、Secure Gatewayに関連付けられたエグレスIPアドレスも表示します。ユーザーがこの統合内でサービスとしてのソフトウェア (SaaS) アプリケーションにアクセスしようとするたびに、トラフィックはSaaSアプリケーションに直接接続するのではなく、パートナーコネクタとして機能するGoogle Secure Gatewayを経由してルーティングされます。このゲートウェイはトラフィックを検査および保護し、セキュリティポリシーとアクセス制御を適用し、組織のセキュリティ体制への準拠を保証します。



2. 編集アイコンをクリックして、顧客IDまたはユーザーグループ、あるいはその両方を更新します。
3. **CEP検証を実行**をクリックして、Google Workspaceの構成がChrome Enterprise Premium統合の準備ができていることを確認します。

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

統合の詳細に問題がある場合、CEP検証は、解決に役立つ詳細を含む失敗または警告メッセージを表示します。ガイダンスについては、既知の検証の失敗と警告を参照してください。



Googleディレクトリ組織部門のCEPを構成する

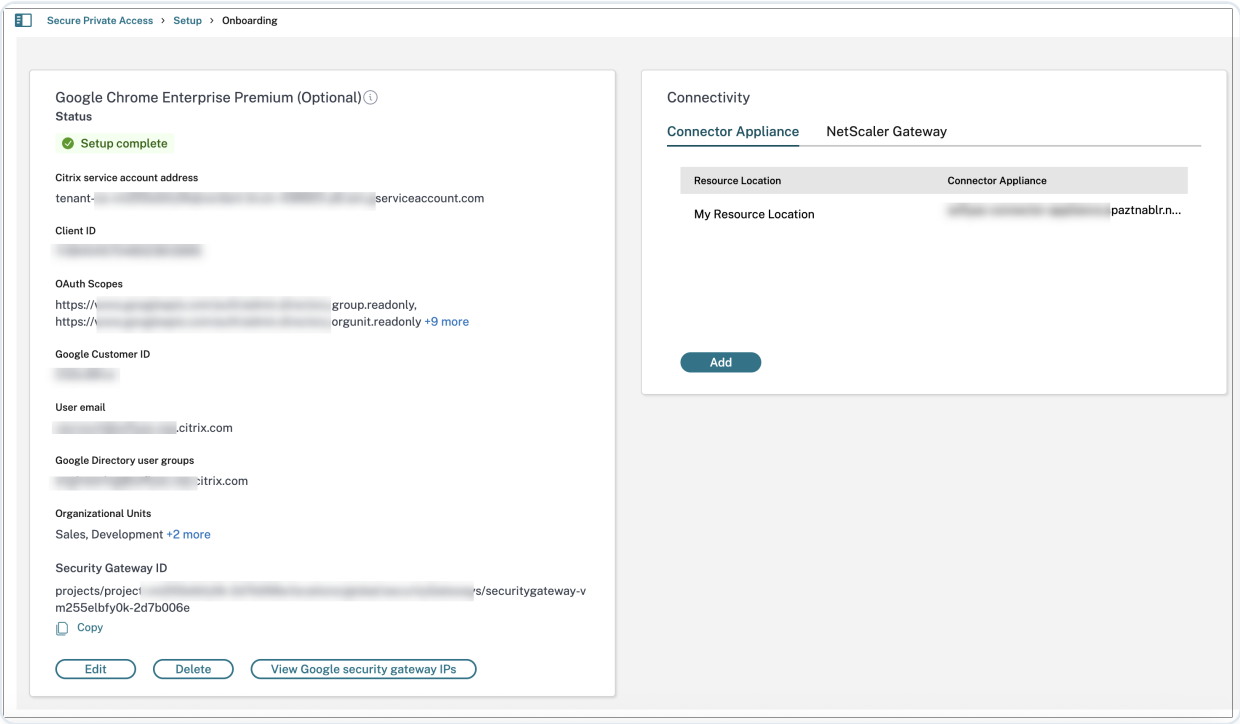
すべてのユーザーとGoogleディレクトリユーザーグループに加えて、選択したGoogleディレクトリ組織部門にChrome Enterprise Premium (CEP) 構成を適用できます。ユーザーグループと組織部門は相互に排他的ではないため、単一の構成で両方をターゲットにできます。また、ユーザーグループを選択せずに、組織部門のみを使用する構成を保存することもできます。このオプションは、Secure Private Accessクラウド展開とハイブリッド展開の両方で利用できます。

選択された組織部門は継承されます。構成はその組織部門のユーザーと、そのすべての子組織部門（後で作成されるものも含む）に適用されます。

組織部門は、Googleディレクトリユーザーグループと同じパネルで選択されます。次の手順を実行します。

1. Chrome Enterprise Premiumセットアップカードで、**編集**をクリックします。

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

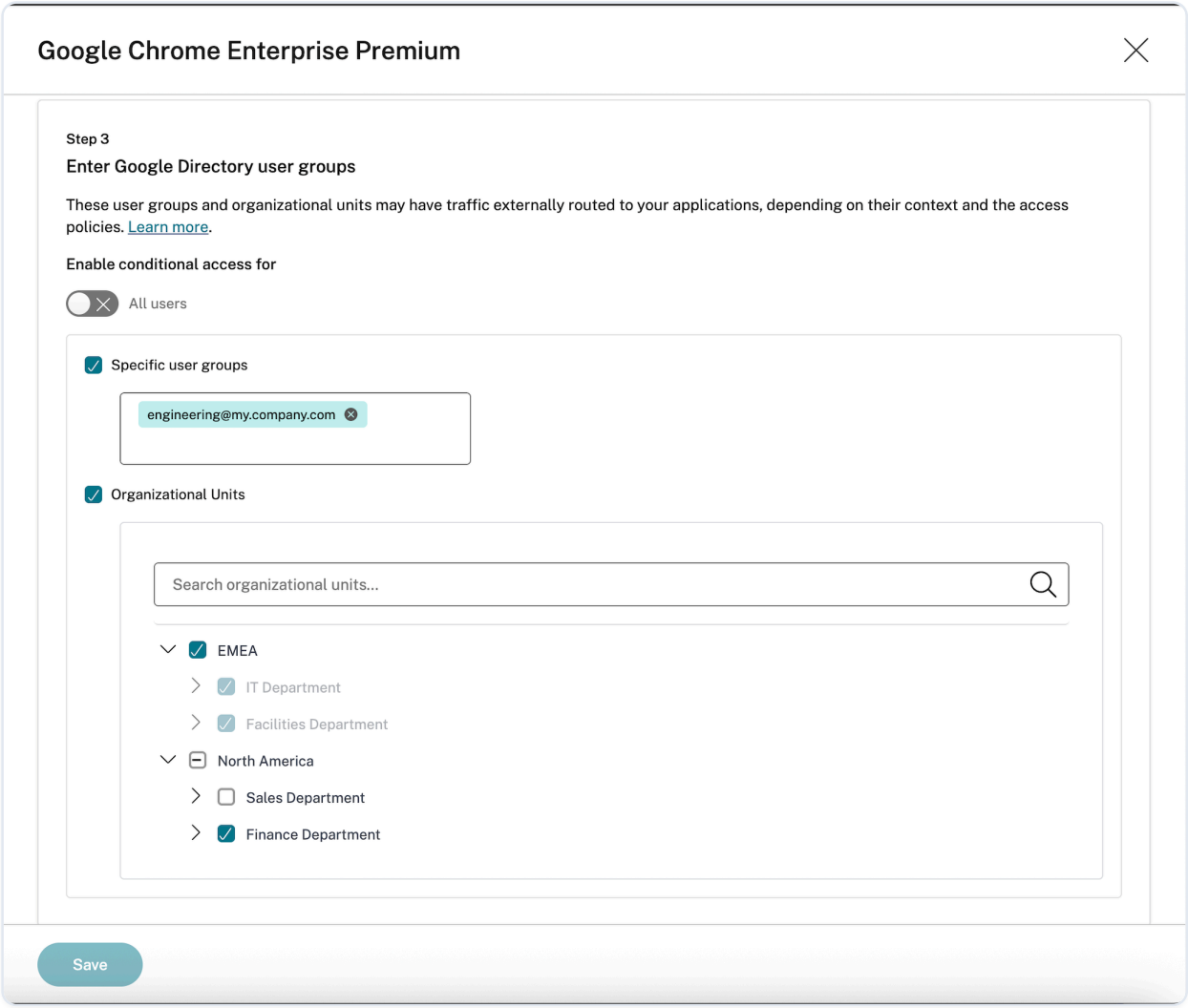


または、Secure Private Access管理コンソールで、**ブラウザ設定 > ブラウザ**に移動し、編集アイコンをクリックします。

カードには、現在選択されている組織部門が一覧表示されます。

2. **組織部門**をクリックして、Googleディレクトリ階層をチェックボックスのツリーとして表示します。

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



注:

- ルート組織部門はツリーに表示されません。全員に対してCEP統合を有効にするには、を選択します。
- 階層は、Citrixサービスアカウントを使用してGoogleディレクトリから読み取られます。サービスアカウントに**組織部門 > 読み取り権限**がない場合、階層を読み込むことができず、ツリーの代わりにエラーが表示されます。詳細については、「Google管理者ロールと権限」を参照してください。

3. 含める組織部門を選択します。

組織部門を選択すると、その子組織部門も選択されます。子ユニットは選択された状態で表示され、グレー表示されます。個別にクリアすることはできません。サブセットのみを含めるには、親をクリアし、必要な特定の子組織部門を選択します。

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

4. 「**CEP検証を実行**」をクリックし、「**保存**」をクリックします。検証が成功した後で選択を変更した場合は、保存する前にもう一度検証を実行してください。検証が報告する失敗と警告については、「既知の検証の失敗と警告」を参照してください。

   パネルを再度開くと、ツリーが展開され、保存された選択内容が表示されます。Google Directoryで削除された組織単位は、パネルから削除されます。

既知の検証の失敗と警告

CEP構成を検証する際、Secure Private Accessは、構成が完了する前に、選択されたセットアップで特定された失敗または警告をフラグ付けします。

構成を続行する前に、特定されたすべての失敗を解決する必要があります。検証中に検出された特定の失敗を特定して修正するには、次の表を使用してください。

失敗メッセージ	アクション
無効なGoogle顧客ID、またはサービスアカウントにGoogle Workspaceへのアクセス権限がありません。	Google顧客IDが正しいことを確認してください。
\^	必要な権限がサービスアカウントに割り当てられていることを確認してください。詳細については、「管理者ロールと権限」を参照してください。
サービスアカウントにChrome拡張機能ポリシーへのアクセス権限がありません。	必要な権限がサービスアカウントに割り当てられていることを確認してください。詳細については、「管理者ロールと権限」を参照してください。
\^サービスアカウントにユーザーグループのChrome拡張機能ポリシーへのアクセス権限がありません。	\^
\^サービスアカウントにChromeクライアント証明書ポリシーへのアクセス権限がありません。	\^
Google Workspace で Null または空のユーザーグループ ID が見つかりました。	これは一時的な問題である可能性があります。問題が解決しない場合は、Google グループに問題がある可能性があります。

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

失敗メッセージ	アクション
\^	複数の Google グループで問題が続く場合は、Citrix サポートにお問い合わせください。
無効または存在しないユーザーグループ	Google グループ名にスペルミスがないか確認してください。
\^	Google 管理コンソールでグループがまだ存在することを確認してください。
サービスアカウントには、組織部門に Chrome 拡張機能ポリシーを適用する権限がありません。	必要な権限がサービスアカウントに割り当てられていることを確認してください。詳細については、「管理者ロールと権限」を参照してください。

特定された警告はすべて記録して調査する必要がありますが、それらが構成の完了を妨げることはありません。以下に、一般的な警告とその対処法を示します。

警告メッセージ	アクション
Google 顧客 ID は既に使用されています	お客様の組織では、Chrome Enterprise Premium 統合に同じ Google 顧客 ID を使用する複数の Citrix Secure Private Access テナントがあります。重複する Google グループ（1 つ以上のテナントで「すべてのユーザー」を選択することを含む）は、他の Citrix テナントの既存の Chrome Enterprise Premium 設定を上書きまたは部分的に上書きする可能性があるため、慎重に設定してください。
重複するGoogleディレクトリユーザーグループが検出されました	指定されたGoogleグループについて、他のCitrixテナントでのChrome Enterprise Premium統合を確認してください。
\^	関連する各Googleグループについて、どのCitrixテナントでChrome Enterprise Premiumを設定する必要があるかを決定します。
\^	他のCitrixテナントから該当する設定を削除します。

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

警告メッセージ	アクション
\^	クリーンアップ中に削除された場合は、選択したCitrixテナントにGoogleグループ設定を再適用します。
「すべてのユーザー」オプションは、このGoogle顧客IDにリンクされている他の顧客と競合する可能性があります	「すべてのユーザー」（ルートGoogle組織単位）に対してChrome Enterprise Premiumを設定すると、同じGoogle顧客IDを使用する他のSecure Private Access設定が上書きされる可能性があります。
\^	この設定は、他のCitrixテナントがユーザーによって積極的に使用されていない場合にのみ使用してください。
「すべてのユーザー」オプションは、このGoogle顧客IDにリンクされている少なくとも1つの顧客によって使用されています	別のCitrixテナントが「すべてのユーザー」（ルートGoogle組織単位）に対してChrome Enterprise Premiumを設定している場合、このCitrixテナントで計画されているGoogleグループ統合が上書きされる可能性があります。
\^	他のCitrixテナントが「すべてのユーザー」統合を必要とするかどうか確認してください。必要としない場合は、そのテナントを特定のGoogleグループに変更してください。
重複するGoogleディレクトリの組織部門が検出されました	このGoogle顧客IDにリンクされている別の顧客が、すでにその組織部門、またはそのパスにある組織部門を使用しています。
\^	重複は、その組織部門とそのすべての子組織部門に適用されます。リストされた組織部門について、他のCitrixテナントでChrome Enterprise Premium統合を確認してください。
サービスアカウントに権限 `Services > Chrome Management > Settings > Managed Browsers > Read` がありません	該当する権限が割り当てられていることを確認してください。割り当てられている場合は、Google管理コンソール（[請求] > [サブスクリプション]）でChrome Enterprise CoreまたはChrome Enterprise Premiumのいずれかのサブスクリプションがあることを確認してください。

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

複数のユーザーグループでのプロビジョニング失敗の問題

Secure Private AccessでChrome Enterprise統合を構成する際（オンボーディング中または**ブラウザ設定**ページから）、8つを超えるユーザーグループを指定すると、プロビジョニングの失敗を引き起こす可能性があります。回避策として、以下を実行してください。

- 必要なすべてのグループを包含する専用のディレクトリ親グループを使用してください。
- オンボーディング中にこの親グループを構成してください。
- ディレクトリでグループメンバーシップが変更された場合は、Googleのディレクトリへの同期プロセスを繰り返してください。

次のステップ

Connector ApplianceとChrome Enterprise Premiumを構成した後、ユーザー向けにアプリケーションとポリシーを構成できます。

- アプリケーションを構成する。
- アクセスポリシーを構成する(/ja-jp/citrix-secure-private-access/service/adaptive-access-to-web-and-saas-apps.html)。

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

データの地域化

Citrix Secure Private Accessにおけるデータの地域化により、お客様は希望する地理的地域を選択することで、データの保存場所を制御できます。お客様は、グローバル、ヨーロッパ (EU)、APAC (アジア太平洋)、北米 (NA) などのオプションから、データの保存地域を選択できます。すべての構成データは、指定された地理的地域から出ることなく、選択された地域内に保持されます。

ユーザーアクセス要求の場合、アプリケーションのトラフィックは選択された地域内で処理され、その地理的地域を通過したり離れたりすることはありません。これはユーザーの場所に関係なく適用されます。ユーザーが世界中に分散している場合でも、各ユーザーのトラフィックは選択された地域を経由してルーティングされ、他の地理的地域を通過することはありません。

データの地域化機能には、次の利点があります。

- すべての構成データを選択された地域内に保持することで、強力なデータレジデンシー制御を保証します。
- 構成データ、および該当する管理データとサポートサービスデータを、顧客の展開に使用される地域データPoPと管理エンドポイントとともに、選択された地域内に保持することで、強力なデータレジデンシー制御を保証します。
- ユーザーの場所に関係なく、ユーザーのトラフィックを特定のPoPに誘導する地理位置情報ベースのルーティングを活用することで、あらゆるアプリケーションのユーザーアクセス要求トラフィックが選択された地域内に留まることを保証します。
- 組織が規制およびデータ主権の要件を満たすのに役立ちます。
- 指定された地理的地域からデータが流出するのを防ぐことで、リスクを軽減します。
- 地域固有のニーズを持つ柔軟なグローバル展開をサポートし、お客様がレジデンシーポリシーに沿ったクラウド提供のセキュアアクセスを安心して導入できるようにします。

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

注:

データの地域化がない場合、複数の地域で事業を展開する組織は、サービスデータの保存場所を制御できない一方で、厳格なデータレジデンシーおよびコンプライアンス要件に直面する可能性があります。地域データ境界がない場合、構成データが必要な地理的地域外に保存される可能性があり、規制リスクが増大し、クラウド提供のセキュアアクセスソリューションの導入が制限されます。

サポートされる展開

この機能は、サービスモデルとハイブリッドモデルの両方を含むすべてのCitrix Secure Private Access展開に適用され、特に地域的なデータレジデンシー、コンプライアンス、および規制要件を持つ組織にとって重要です。

構成

地域の選択は、Secure Private Accessサービスまたはハイブリッド展開のオンボーディング時における1回限りの設定です。設定後は、すべてのデータが選択された地域に保持され、継続的な運用やユーザーワークフローに影響はありません。

1. Citrix Cloudにログインし、**Secure Private Access**をクリックします。
2. 「**クラウドのセットアップ**」または「**ハイブリッド**」を選択し、「**続行**」をクリックします。
3. 「**展開リージョンの選択**」で、データが保存される必要があるリージョンを選択します。利用可能なリージョンは、Citrix Cloudアカウントのリージョンに基づいています。
4. **続行**をクリックします。

制限事項

データリージョン化の制限事項は次のとおりです。

- データリージョン化は、保存されている顧客所有の構成データと、アプリケーションデータに対するユーザーアクセス要求に適用されます。その他のデータタイプ（テレメトリや転送中のデータなど）は、選択されたリージョンに制限されない場合があります。
- グローバルに動作する他のCitrix Cloudサービスには依存関係があり、それらは同じリージョン境界に従わない場合があります。
- これはオンボーディング時の一度限りの構成であり、後で変更することはできません。
- この機能は新規顧客のみが利用できます。

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

アプリケーションの構成と管理

Citrix Secure Private Access は、さまざまなアプリケーション (SaaS/Web および TCP/UDP) へのアクセスを構成および管理するための、ユーザーフレンドリーな集中型プラットフォームを提供します。Secure Private Access コンソールは、さまざまな構成タスクに対して単一の制御ポイントを提供することで、管理を簡素化します。構成ウィザードを使用すると、管理者はアダプティブ認証を簡単に設定し、アプリケーションを構成し、ユーザー権限を制御するアクセス ポリシーを定義し、機密データを保護するためのセキュリティ制限を実装できます。これらすべてを同じコンソール内で行えます。さらに、Secure Private Access は、VPN クライアントをインストールすることなく、エンタープライズ Web アプリへのエージェントレス アクセスをサポートします。

詳細については、次のトピックを参照してください。

- エンタープライズ Web アプリのサポート
- エンタープライズ Web アプリへのエージェントレス アクセス
- サービスとしてのソフトウェア (SaaS) アプリのサポート
- クライアント/サーバー アプリのサポート
- サーバーからクライアントへの接続のサポート
- Citrix Secure Access クライアント
- Web および SaaS アプリケーション構成のベスト プラクティス
- エンドユーザー アプリ アクセス - 解説

エンタープライズWebアプリを構成する

Secure Private Accessサービスを使用したWebアプリ配信により、企業固有のアプリケーションをWebベースのサービスとしてリモートで配信できます。一般的に使用されるWebアプリには、SharePoint、Confluence、OneBugなどがあります。

Secure Private AccessサービスをCitrix® StoreFront Cloudと統合できます。ユーザーはWebブラウザまたはCitrix Workspace™アプリからクラウドストアにアクセスします。このストアは、構成されたSaaSアプリ、構成された仮想アプリ、またはその他のリソースに対して統合されたユーザーエクスペリエンスを提供します。

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

システム要件

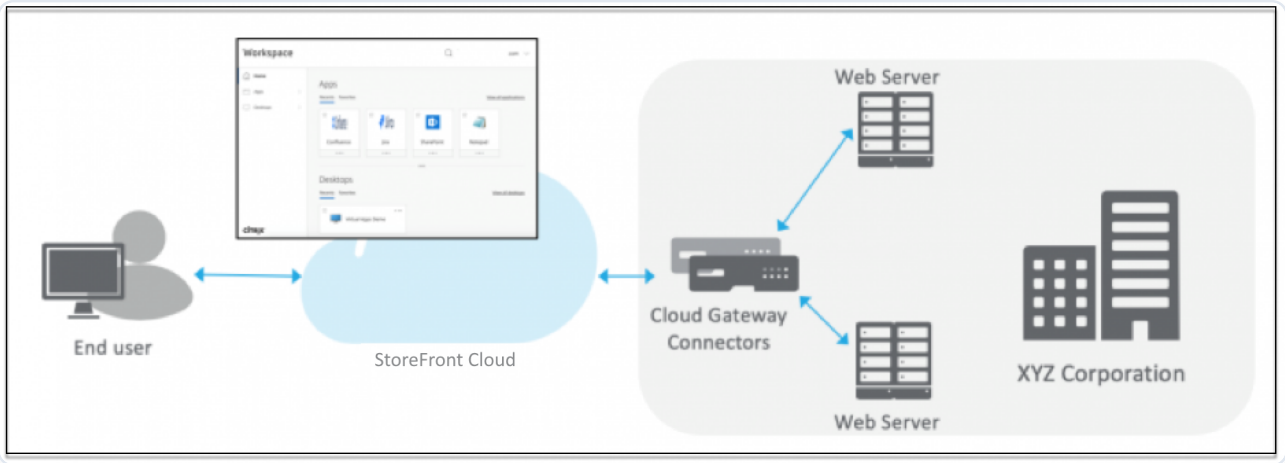
Connector Appliance - Citrix Secure Private AccessサービスでConnector Applianceを使用すると、顧客のデータセンターにあるエンタープライズWebアプリへのVPNレスアクセスをサポートできます。詳細については、「Secure Private Access用Connector Appliance」を参照してください。

仕組み

Citrix Secure Private Access™サービスは、オンプレミスに展開されたコネクタを使用して、オンプレミスデータセンターに安全に接続します。このコネクタは、オンプレミスに展開されたエンタープライズWebアプリとCitrix Secure Private Accessサービス間のブリッジとして機能します。これらのコネクタはHAペアで展開でき、アウトバウンド接続のみが必要です。

Connector Applianceとクラウド内のCitrix Secure Private Accessサービス間のTLS接続により、クラウドサービスに列挙されたオンプレミスアプリケーションが保護されます。Webアプリケーションは、VPNレス接続を使用してストアを介してアクセスおよび配信されます。

次の図は、StoreFront Cloudを使用してストアからWebアプリケーションにアクセスする方法を示しています。



Webアプリを構成する

1. Citrix Cloudにログオンし、**Secure Private Access**を選択します。
2. **Applications > App Configuration**をクリックし、**Add an app**をクリックします。
3. **Choose a template**セクションで、**Skip**をクリックします。テンプレートはSaaSアプリでのみ利用可能です。
4. 「**アプリケーションの場所はどこですか？**」で、「**社内ネットワーク内**」を選択します。

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

- 組織のプライベートネットワークインフラストラクチャ内でホストされ、ファイアウォールの背後にあり、内部ネットワーク接続を介してのみアクセス可能なアプリケーションの場合は、**Inside my corporate network** を選択します。
- 組織のプライベートネットワークインフラストラクチャの外部でホストされているアプリケーションの場合は、**Outside my corporate network (Google Connector)** を選択します。トラフィックルーティングは、Google Cloud Connector を介してユーザーから外部アプリケーションに直接行われます。

5. 「**アプリの詳細**」セクションに以下の詳細を入力し、「**次へ**」をクリックします。

SPAアプリの詳細(/en-us/citrix-secure-private-access/media/spa-web-app-details.png)

- **アプリの種類** – アプリの種類を選択します。

> **注:**
>
> Chrome Enterprise Premium (CEP) では、HTTPSエンタープライズWebアプリとSaaSアプリのみがサポートされています。HTTPエンタープライズWebアプリとSaaSアプリはサポートされていません。

- **アプリ名** – アプリケーションの名前。
- **アプリの説明** - アプリの簡単な説明。この説明は、ストアでユーザーに表示されます。
- **アプリのカテゴリ** - 公開するアプリがストアUIに表示されるカテゴリとサブカテゴリ名（該当する場合）を追加します。各アプリに新しいカテゴリを追加することも、ストアUIの既存のカテゴリを使用することもできます。WebアプリまたはSaaSアプリのカテゴリを指定すると、そのアプリはストアUIの特定のカテゴリの下に表示されます。
  - カテゴリ/サブカテゴリは管理者が構成可能であり、管理者はすべてのアプリに新しいカテゴリを追加できます。
  - 「**アプリのカテゴリ**」フィールドはHTTP/HTTPSアプリに適用され、TCP/UDPアプリでは非表示になります。
  - カテゴリ/サブカテゴリ名はバックスラッシュで区切る必要があります。例: **Business And Productivity\Engineering**。また、このフィールドでは大文字と小文字が区別されます。管理者は、正しいカテゴリが定義されていることを確認する必要があります。ストアUIの名前と、**App category**フィールドに入力されたカテゴリ名との間に不一致がある場合、そのカテゴリは新しいカテゴリとしてリストされます。

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

例えば、「**アプリのカテゴリ**」フィールドに「**Business and Productivity**」カテゴリを誤って「**Business And productivity**」と入力した場合、「**Business And Productivity**」カテゴリに加えて、「**Business and productivity**」という新しいカテゴリがストアUIにリストされます。

- **アプリのアイコン** – アプリのアイコンを変更するには、「**アイコンの変更**」をクリックします。アイコンファイルのサイズは128x128ピクセルである必要があります。アイコンを変更しない場合、デフォルトのアイコンが表示されます。

  アプリケーションアイコンを表示しない場合は、**ユーザーにアプリケーションアイコンを表示しない**を選択します。

- ユーザーがクライアントブラウザから直接アプリにアクセスできるようにするには、**エージェントレスアクセス**を選択します。詳細については、「エンタープライズWebアプリへの直接アクセス」を参照してください。

- **URL** – お客様の顧客IDを含むURL。URLにはお客様の顧客ID (Citrix Cloud™ 顧客ID) が含まれている必要があります。顧客IDの取得については、「Citrix Cloudへのサインアップ」を参照してください。SSOが失敗した場合、またはSSOを使用しない場合、ユーザーはこのURLにリダイレクトされます。

  顧客ドメイン名および**顧客ドメインID** - 顧客ドメイン名とIDは、SAML SSOページでアプリのURLおよびその他の後続のURLを作成するために使用されます。

  たとえば、Salesforceアプリを追加する場合、ドメイン名が`salesforceformyorg`でIDが123754の場合、アプリのURLは`https://salesforceformyorg.my.salesforce.com/?so=123754.`になります。

  顧客ドメイン名と顧客IDのフィールドは、特定のアプリに固有のものです。

- **関連ドメイン** – 関連ドメインは、指定したURLに基づいて自動的に入力されます。関連ドメインは、サービスがURLをアプリの一部として識別し、それに応じてトラフィックをルーティングするのに役立ちます。複数の関連ドメインを追加できます。

  注：

  重複する関連ドメインが追加された場合、または関連ドメインが別のアプリのURLとしても追加された場合、警告メッセージが表示されます。これらの問題を回避するには、「WebおよびSaaSアプリケーション構成のベストプラクティス」を参照してください。

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

- **HARのインポート** – HARファイルをアップロードして、アプリケーションがアクセスするドメインを自動的に検出できます。検出されたドメインを確認し、アプリケーションの関連ドメイン構成に追加するドメインを選択します。これにより、関連ドメインを手動で識別して構成する必要がなくなるため、アプリケーションのオンボーディングが簡素化されます。詳細については、「HARファイルを使用した関連ドメインの検出」を参照してください。
- **一貫した接続を維持** - このチェックボックスをオンにすると、同じコネクタアプライアンスへの一貫した接続が有効になります。一貫した接続の詳細については、「一貫した接続を維持」を参照してください。

> **注：**
>
> **一貫した接続を維持**オプションが選択されている場合、アプリケーションのルーティングタイプは、アプリ接続セクションで**コネクタ経由の内部**に設定する必要があります。

- **アプリケーションをお気に入りWorkspaceアプリに追加**をクリックして、このアプリをCitrix Workspaceアプリのお気に入りアプリとして追加します。
  - **ユーザーがお気に入りから削除することを許可**をクリックすると、アプリのサブスクライバーがCitrix Workspaceアプリのお気に入りアプリリストからアプリを削除できるようになります。このオプションを選択すると、Citrix Workspaceアプリのアプリの左上隅に黄色の星アイコンが表示されます。
  - 「**ユーザーがお気に入りから削除することを許可しない**」をクリックすると、サブスクライバーがCitrix Workspaceアプリのお気に入りアプリリストからアプリを削除するのを防ぐことができます。このオプションを選択すると、Citrix Workspaceアプリのアプリの左上隅に南京錠の付いた星のアイコンが表示されます。

    Secure Private Accessサービスコンソールからお気に入りとしてマークされたアプリを削除した場合、ユーザーはストアのお気に入りリストからアプリを手動で削除する必要があります。Secure Private Accessサービスコンソールから削除しても、アプリはストアから自動的に削除されません。

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

「

重要:

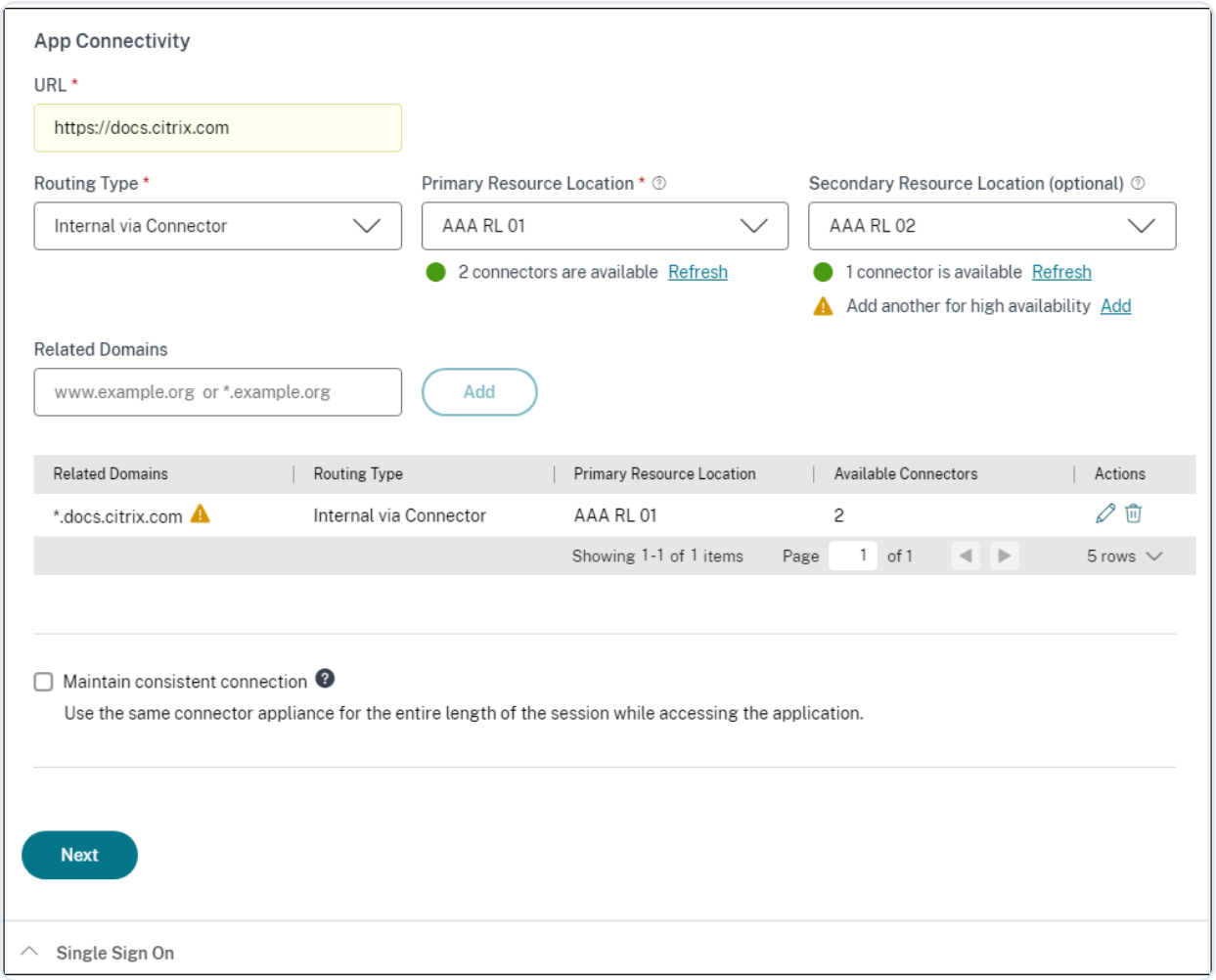
」:

- アプリへのゼロトラストベースのアクセスを有効にするため、アプリへのアクセスはデフォルトで拒否されます。アプリへのアクセスは、アクセスポリシーがアプリケーションに関連付けられている場合にのみ有効になります。
- 複数のアプリが同じFQDNまたはワイルドカードFQDNの何らかのバリエーションで構成されている場合、競合する構成になる可能性があります。
- これらの問題は、いくつかのベストプラクティスに従うことで解決できます。詳細については、「WebおよびSaaSアプリケーション構成のベストプラクティス」を参照してください。

6. 「**アプリ接続**」セクションでは、ドメインをCitrix Connector™ Applianceを介して外部または内部にルーティングする必要がある場合に、アプリケーションの関連ドメインのルーティングを定義します。

「

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



」

- 「**ルーティングタイプ** - 次のいずれかを選択します。」:
  - 「**内部 – プロキシをバイパス** - ドメイントラフィックはConnector Appliance™を介してルーティングされ、Connector Applianceで構成された顧客のWebプロキシをバイパスします。」.
  - 「**コネクタ経由の内部** - アプリは外部のものでもかまいませんが、トラフィックはConnector Applianceを介して外部ネットワークに流れる必要があります。」.
  - 「**外部** – トラフィックはインターネットに直接流れます。」.
- 「**プライマリおよびセカンダリリソースロケーション** - 管理者は、セカンダリリソースロケーションを構成するか、**最初に利用可能**オプションを使用することで、中断時でもアプリケーションの高可用性を確保できます。」.
  - 「**プライマリリソースロケーション:** アプリケーションがホストされているプライマリリソースロケーションを選択します。または、管理者は**プライマリリソースロケーション**で**最初に利用可能**オプションを選択することもできます。」.

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

- 「**最初に利用可能: 最初に利用可能**オプションは、動作中のリソースロケーションが使用されることを保証します。**最初に利用可能**が選択されている場合、システムはトラフィックを最初に利用可能なロケーションに自動的にルーティングします。これにより、手動介入なしで継続的なアプリケーションアクセスが保証されます。たとえば、ResourceLocation1が利用できないがResourceLocation2に到達可能な場合、ResourceLocation2がデフォルトで選択され、アプリケーションのフロントエンドとして機能します。」.
- **セカンダリリソースロケーション** - **セカンダリリソースロケーション**オプションは、プライマリリソースロケーションが明示的に指定されている場合にのみ使用可能になります。コネクタアプライアンスまたはデータセンターの障害などの理由により、プライマリリソースロケーションが利用できなくなった場合、アプリケーションは指定されたセカンダリリソースロケーションにフェールオーバーします。セカンダリリソースロケーションは、アプリケーションが別のデータセンターでホストされている場合でも、フェールオーバーとして機能できます。

関連ドメインごとに、プライマリおよびセカンダリリソースロケーションを設定するか、**First Available**オプションを選択することもできます。

a. 関連ドメインテーブルの**アクション**列にある編集アイコンをクリックします。
b. プライマリおよびセカンダリリソースロケーションを設定するか、**First Available**オプションを選択します。

関連ドメイン(/en-us/citrix-secure-private-access/media/backup-rl-related-domains.png)

注:

- バックアップリソースロケーションの設定と**First Available**オプション機能の使用は、現在プレビュー段階です。
- アプリケーションを削除すると、そのルーティングエントリは自動的に削除されます。詳細については、「アプリケーション削除時のルーティングエントリの自動クリーンアップ」を参照してください。

- **一貫した接続を維持** - このチェックボックスをオンにすると、同じコネクタアプライアンスへの一貫した接続が可能になります。一貫した接続の詳細については、「一貫した接続を維持」を参照してください。

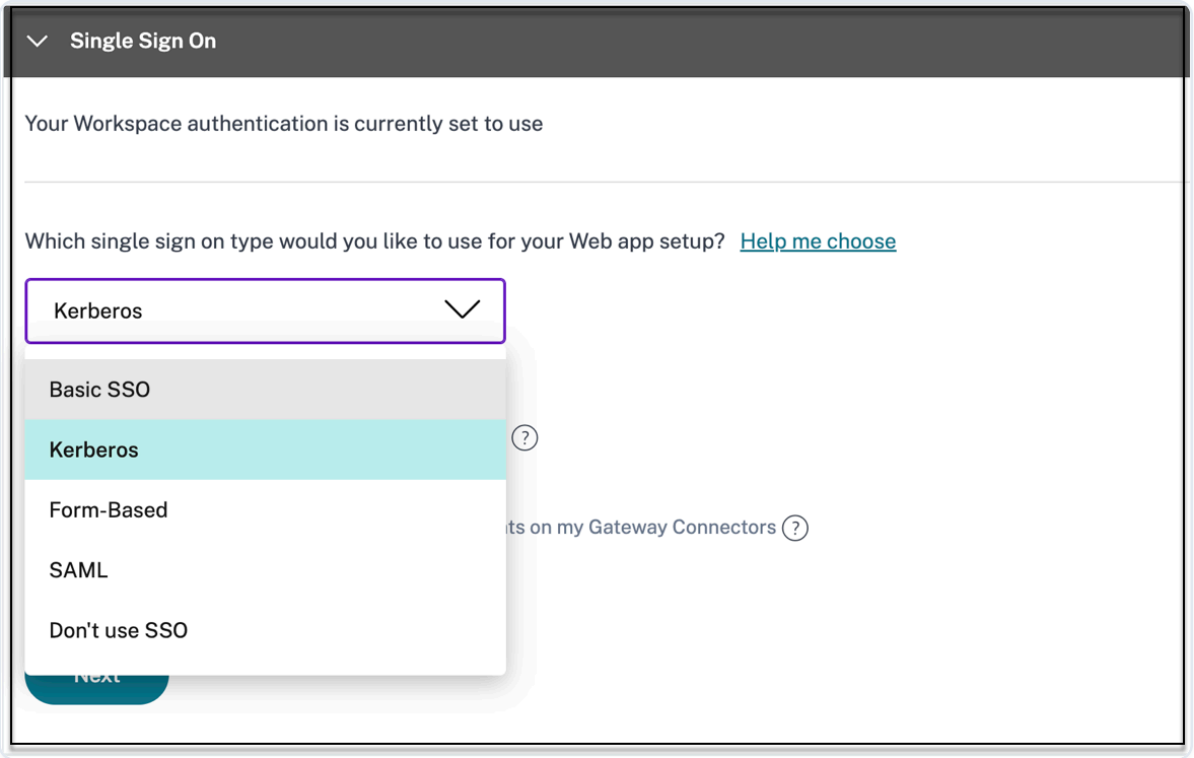
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注:**
>
> **一貫した接続を維持**オプションが選択されている場合、アプリケーションのルーティングタイプは、アプリ接続セクションで**コネクタ経由の内部**に設定する必要があります。

7. 優先するサインオン方法を設定します。

> **注:**
>
> シングルサインオンオプションは、Chrome Enterprise (CEP) を使用するCitrix Secure Accessには適用されません。

   a. **シングルサインオン**セクションで、アプリケーションに使用する優先シングルサインオンタイプを選択し、**保存**をクリックします。以下のシングルサインオンタイプが利用可能です。



   - **Basic** – バックエンドサーバーからbasic-401チャレンジが提示された場合は、**Basic SSO**を選択します。**Basic** SSOタイプには、構成の詳細を指定する必要はありません。

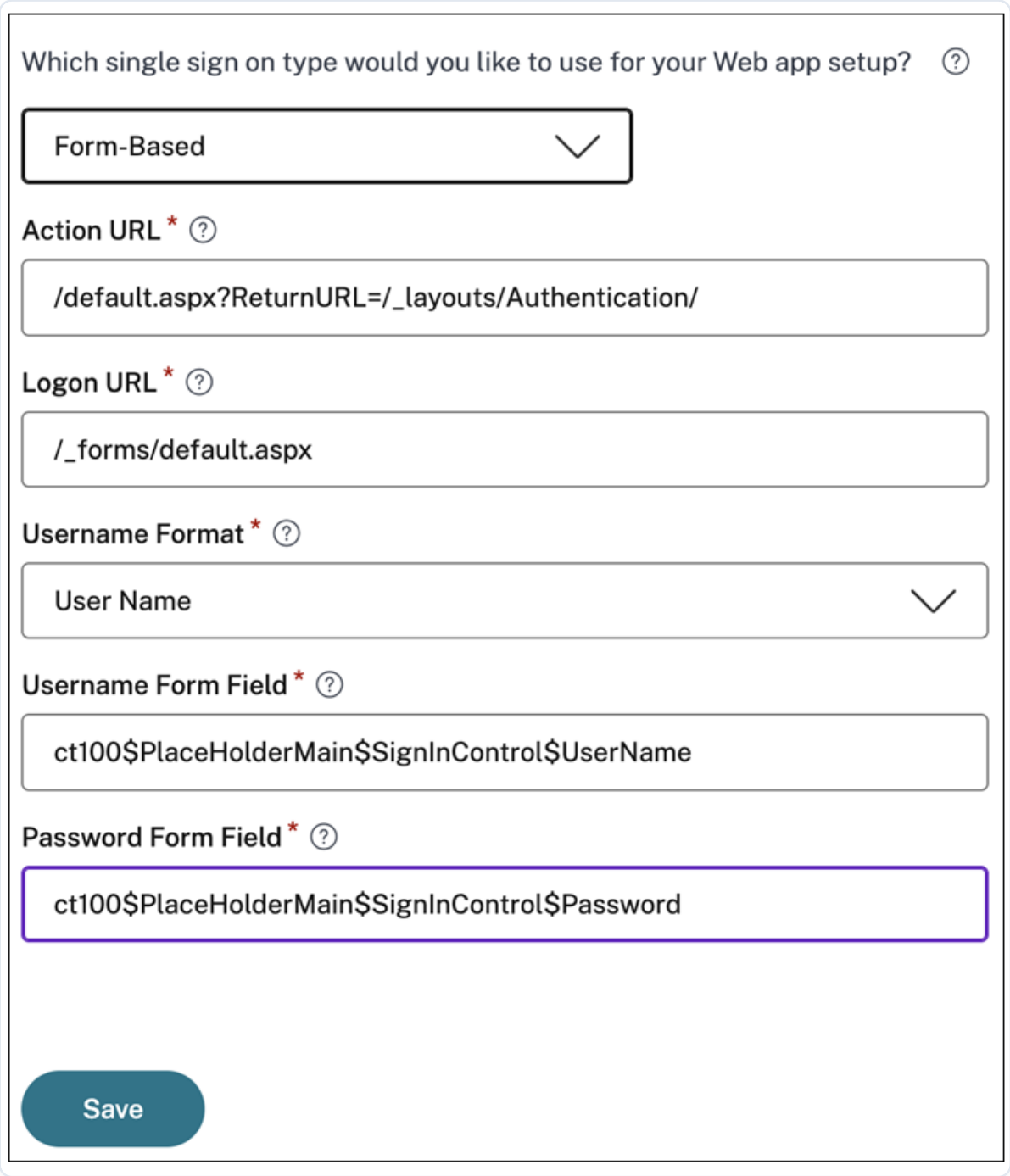
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Kerberos** – バックエンドサーバーからnegotiate-401チャレンジが提示された場合は、**Kerberos**を選択します。**Kerberos** SSOタイプには、構成の詳細を指定する必要はありません。
- **フォームベース** – バックエンドサーバーから認証用のHTMLフォームが提示された場合は、**フォームベース**を選択します。**フォームベース**SSOタイプの構成の詳細を入力します。
- **SAML** - WebアプリケーションへのSAMLベースのSSOには、**SAML**を選択します。**SAML** SSOタイプの構成の詳細を入力します。
- **SSOを使用しない** – バックエンドサーバーでユーザーを認証する必要がない場合は、**SSOを使用しない**オプションを使用します。**SSOを使用しない**オプションが選択されている場合、ユーザーは**アプリの詳細**セクションで構成されたURLにリダイレクトされます。

フォームベースの詳細:

シングルサインオンセクションに以下のフォームベースの構成詳細を入力し、**保存**をクリックします。

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



- **アクションURL** - 完了したフォームが送信されるURLを入力します。
- **ログオンフォームURL** – ログオンフォームが表示されるURLを入力します。
- **ユーザー名形式** - ユーザー名の形式を選択します。
- **ユーザー名フォームフィールド** – ユーザー名属性を入力します。
- **パスワードフォームフィールド** – パスワード属性を入力します。

SAML:

サインオンセクションに以下の詳細を入力し、**保存**をクリックします。

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

設定を保存2(/en-us/citrix-secure-private-access/media/saml-sso-details.png)

- **アサーションの署名** - アサーションまたは応答に署名すると、応答またはアサーションが証明書利用者 (SP) に配信される際のメッセージの整合性が保証されます。**アサーション、応答、両方**、または**なし**を選択できます。
- **アサーションURL** – アサーションURLはアプリケーションベンダーによって提供されます。SAMLアサーションはこのURLに送信されます。
- **リレーステート** – リレーステートパラメーターは、ユーザーがサインインして証明書利用者のフェデレーションサーバーにリダイレクトされた後にアクセスする特定のリソースを識別するために使用されます。リレーステートはユーザー向けに単一のURLを生成します。ユーザーはこのURLをクリックしてターゲットアプリケーションにログオンできます。
- **オーディエンス** – オーディエンスはアプリケーションベンダーによって提供されます。この値は、SAMLアサーションが正しいアプリケーションに対して生成されたことを確認します。
- **名前ID形式** – サポートされている名前識別子形式を選択します。
- **名前ID** – サポートされている名前IDを選択します。

i. **詳細属性 (オプション)** で、アクセス制御の決定のためにアプリケーションに送信されるユーザーに関する追加情報を追加します。

ii. **SAMLメタデータ**の下のリンクをクリックして、メタデータファイルをダウンロードします。ダウンロードしたメタデータファイルを使用して、SaaSアプリサーバーでSSOを構成します。

- **ログインURL**の下にあるSSOログインURLをコピーし、SaaSアプリサーバーでSSOを構成する際にこのURLを使用できます。
- **証明書**リストから証明書をダウンロードし、SaaSアプリサーバーでSSOを構成する際にその証明書を使用することもできます。

8. **保存**をクリックし、次に**完了**をクリックします。

完了をクリックすると、アプリがアプリケーションページに追加されます。アプリケーションを構成した後、アプリケーションページからアプリを編集または削除できます。そのためには、アプリの省略記号ボタンをクリックし、それに応じてアクションを選択します。

- **アプリケーションの編集**
- **削除**

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

重要:

- ユーザーにアプリへのアクセスを許可するには、管理者はアクセスポリシーを作成する必要があります。アクセスポリシーでは、管理者がアプリのサブスクライバーを追加し、セキュリティ制御を構成します。詳細については、「アクセスポリシーの作成」を参照してください。

アプリケーション削除時のルーティングエントリの自動クリーンアップ

アプリケーションを構成すると、その宛先（FQDNまたはアプリケーションドメイン）がルーティングテーブルに追加され、Secure Private Accessがルーティングの決定に使用します。アプリケーションを削除すると、Secure Private Accessは以下のルールに基づいてルーティングエントリをクリーンアップします。

- **参照されていないエントリは削除されます** - 削除されたアプリケーションに関連付けられているルーティングエントリ（FQDNまたはアプリケーションドメイン）が他のどのアプリケーションからも参照されていない場合、Secure Private Accessはルーティングテーブルから自動的に削除します。
- **共有エントリは保持されます** - ルーティングエントリが複数のアプリケーションで使用されている場合、それらのアプリケーションの1つを削除しても、共有エントリは削除されません。そのエントリは、少なくとも1つのアクティブなアプリケーションがそれを参照している限り、ルーティングテーブルに残ります。
- **遡及的な削除はありません** - ルーティングエントリは、アプリケーションの削除の一部としてのみ評価および削除されます。既存のエントリは、どのアプリケーションにも使用されていないことが確認されない限り、遡及的に削除されることはありません。

注:

- アプリケーションページからアプリケーションが削除されると（省略記号（...）メニューを使用して）、クリーンアップは自動的に実行されます。管理者の操作は不要です。
- 共有ルーティングエントリは保持されるため、アプリケーションを削除しても、同じ宛先を共有する他のアプリケーションへのアクセスが中断されることはありません。

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

SaaSアプリを構成する

Software as a Service (SaaS) は、Webベースのサービスとしてソフトウェアをリモートで提供するソフトウェア配信モデルです。一般的に使用されるSaaSアプリには、Salesforce、Workday、Concur、GoToMeetingなどがあります。

Secure Private AccessサービスをCitrix® StoreFront Cloudと統合できます。ユーザーはWebブラウザまたはCitrix Workspace™アプリからクラウドストアにアクセスします。このストアは、構成されたSaaSアプリ、構成された仮想アプリ、またはその他のリソースに対して統一されたユーザーエクスペリエンスを提供します。Secure Private Accessサービスを使用したSaaSアプリの配信は、アプリを管理するための簡単で安全、堅牢、かつスケーラブルなソリューションを提供します。

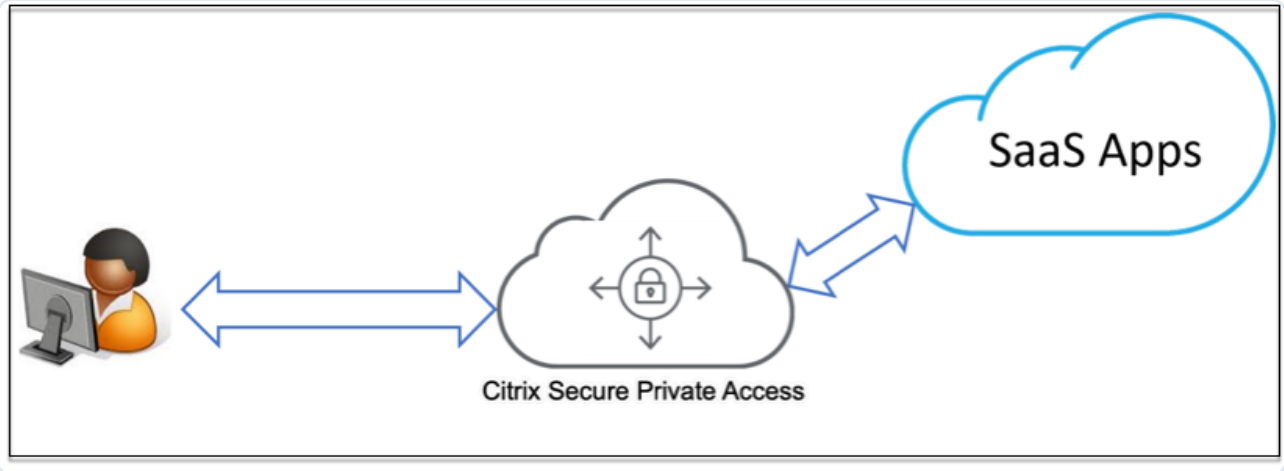
Secure Private AccessサービスでSaaSアプリがサポートされる仕組み

1. 顧客管理者は、Secure Private AccessサービスのUIを使用してSaaSアプリを構成します。
2. 管理者は、エンドユーザーにストアURLを提供します。
3. アプリを起動するには、ユーザーは列挙されたSaaSアプリのアイコンをクリックします。
4. SaaSアプリは、Secure Private Accessサービスによって提供されるSAMLアサーションを信頼し、アプリが起動されます。

注：

- ユーザーにアプリへのアクセスを許可するには、管理者はアクセスポリシーを作成する必要があります。アクセスポリシーでは、管理者はアプリサブスクライバーを追加し、セキュリティ制御を構成します。詳細については、「アクセスポリシーの作成」を参照してください。
- 構成されたSaaSアプリは、仮想アプリやその他のリソースとともにストアに集約され、統一されたユーザーエクスペリエンスを提供します。

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



SaaSアプリを構成する

1. Citrix Cloudにログインし、**Secure Private Access**を選択します。
2. **Applications > App Configuration**をクリックし、**Add an app**をクリックします。

   注:

   アプリは手動で、またはテンプレートを使用して構成できます。テンプレートはほとんどのアプリケーション設定を事前に入力しますが、顧客固有の詳細情報は引き続き提供する必要があります。

   手動構成: テンプレートの選択セクションで**スキップ**をクリックし、**アプリの詳細**セクションでアプリケーションを構成します。ステップ3から開始します。
   テンプレートベースの構成: テンプレートの選択をクリックし、テンプレートを選択して**次へ**をクリックします。必要に応じてアプリの詳細を確認し、更新します。

   - アプリ構成ページでは、アプリのオンボーディングを簡素化し、迅速化するために最もよく使用される5つのテンプレートが強調表示されます。
   - 他のサポートされているSaaSアプリのテンプレートを参照するには、**テンプレートの表示**を選択します。 SaaSアプリのテンプレート(/en-us/citrix-secure-private-access/media/spa-top-5-app-templates.png)

3. **アプリケーションの場所はどこですか?** で、ルーティングパス、ポリシー、および適用する必要があるアクセスメカニズムを決定するために、ターゲットアプリケーションの場所を選択します。SaaSアプリの場合は、**社内ネットワーク外 (Google Connector)** を選択します。

   - **社内ネットワーク外 (Google Connector):** 組織のプライベートネットワークインフラストラクチャの外部でホストされているアプリケーションの場合。トラフィックルーティングは、Citrix Cloudを介してユーザーから外部アプリケーションに直接行われます。

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

- **社内ネットワーク内:** 組織のプライベートネットワークインフラストラクチャ内で、ファイアウォールの背後にホストされ、内部ネットワーク接続を介してのみアクセス可能なアプリケーションの場合。

4. **アプリの詳細**セクションに以下の詳細を入力し、**次へ**をクリックします。

SPAアプリの詳細(/en-us/citrix-secure-private-access/media/spa-saas-app-details.png)

- **アプリ名** – アプリケーションの名前。
- **アプリの説明** - アプリの簡単な説明。この説明は、ストアでユーザーに表示されます。
- **アプリのカテゴリ** - 公開するアプリがストアUIに表示されるカテゴリとサブカテゴリ名 (該当する場合) を追加します。アプリごとに新しいカテゴリを追加することも、ストアUIの既存のカテゴリを使用することもできます。WebアプリまたはSaaSアプリのカテゴリを指定すると、そのアプリはストアUIの特定のカテゴリの下に表示されます。
  - カテゴリ/サブカテゴリは管理者によって設定可能で、管理者はすべてのアプリに新しいカテゴリを追加できます。
  - 「**アプリカテゴリ**」フィールドはHTTP/HTTPSアプリに適用され、TCP/UDPアプリでは非表示になります。
  - カテゴリ/サブカテゴリ名はバックスラッシュで区切る必要があります。例: **Business And Productivity\Engineering**。また、このフィールドは大文字と小文字を区別します。管理者は正しいカテゴリを定義していることを確認する必要があります。ストアUIの名前と「**App category**」フィールドに入力されたカテゴリ名が一致しない場合、そのカテゴリは新しいカテゴリとしてリストされます。

    たとえば、「**アプリカテゴリ**」フィールドに**Business and Productivity**カテゴリを誤って**Business And productivity**と入力した場合、**Business And Productivity**カテゴリに加えて、**Business and productivity**という新しいカテゴリがストアUIにリストされます。
- **アプリのアイコン** – **アイコンの変更** をクリックして、アプリのアイコンを変更します。アイコンファイルのサイズは128x128ピクセルである必要があります。アイコンを変更しない場合、デフォルトのアイコンが表示されます。

  アプリのアイコンを表示したくない場合は、**ユーザーにアプリケーションアイコンを表示しない** を選択します。
- **URL** – お客様の顧客IDを含むURL。URLにはお客様の顧客ID (Citrix Cloud™ 顧客ID) が含まれている必要があります。顧客IDを取得するには、「Citrix Cloudへのサインアップ」を

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

参照してください。SSOが失敗した場合、またはSSOを使用しない場合、ユーザーはこのURLにリダイレクトされます。

- **顧客ドメイン名** および **顧客ドメインID** - 顧客ドメイン名とIDは、SAML SSOページでアプリのURLおよびその他の後続のURLを作成するために使用されます。

  たとえば、Salesforceアプリを追加する場合、ドメイン名は `salesforceformyorg` でIDが123754の場合、アプリのURLは `https://salesforceformyorg.my.salesforce.com/?so=123754.` となります。

  顧客ドメイン名と顧客IDフィールドは、特定のアプリに固有のものです。

- **関連ドメイン** – 関連ドメインは、提供されたURLに基づいて自動的に入力されます。関連ドメインは、サービスがURLをアプリの一部として識別し、それに応じてトラフィックをルーティングするのに役立ちます。複数の関連ドメインを追加できます。

  > **注:**
  >
  > 重複する関連ドメインが追加された場合、または関連ドメインが別のアプリのURLとしても追加された場合、警告メッセージが表示されます。これらの問題を回避するには、「WebおよびSaaSアプリケーション構成のベストプラクティス」を参照してください。

- **HARのインポート** – HARファイルをアップロードして、アプリケーションがアクセスするドメインを自動的に検出できます。検出されたドメインを確認し、アプリケーションの関連ドメイン構成に追加したいものを選択します。これにより、関連ドメインを手動で特定して構成する必要が減り、アプリケーションのオンボーディングが簡素化されます。詳細については、「HARファイルを使用して関連ドメインを検出する」を参照してください。
- **一貫した接続を維持** - SaaSアプリでは、Connector Applianceへの一貫した接続がサポートされています。「**一貫した接続を維持**」チェックボックスを選択し、「**アプリ接続**」セクションで接続タイプとして「**コネクタ経由で内部**」を選択します。一貫した接続の詳細については、「一貫した接続を維持する」を参照してください。
- 「**Workspaceアプリでお気に入りとしてアプリケーションを追加**」をクリックして、このアプリをCitrix Workspaceアプリでお気に入りアプリとして追加します。
  - 「**ユーザーがお気に入りから削除することを許可**」をクリックすると、アプリのサブスクライバーがCitrix Workspaceアプリのお気に入りアプリリストからアプリを削除できるようになります。このオプションを選択すると、Citrix Workspaceアプリのアプリの左上隅に黄色の星アイコンが表示されます。

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

- 「**ユーザーがお気に入りから削除することを許可しない**」をクリックすると、サブスクライバーがCitrix Workspaceアプリのお気に入りアプリリストからアプリを削除できなくなります。このオプションを選択すると、Citrix Workspaceアプリのアプリの左上隅に南京錠の付いた星アイコンが表示されます。

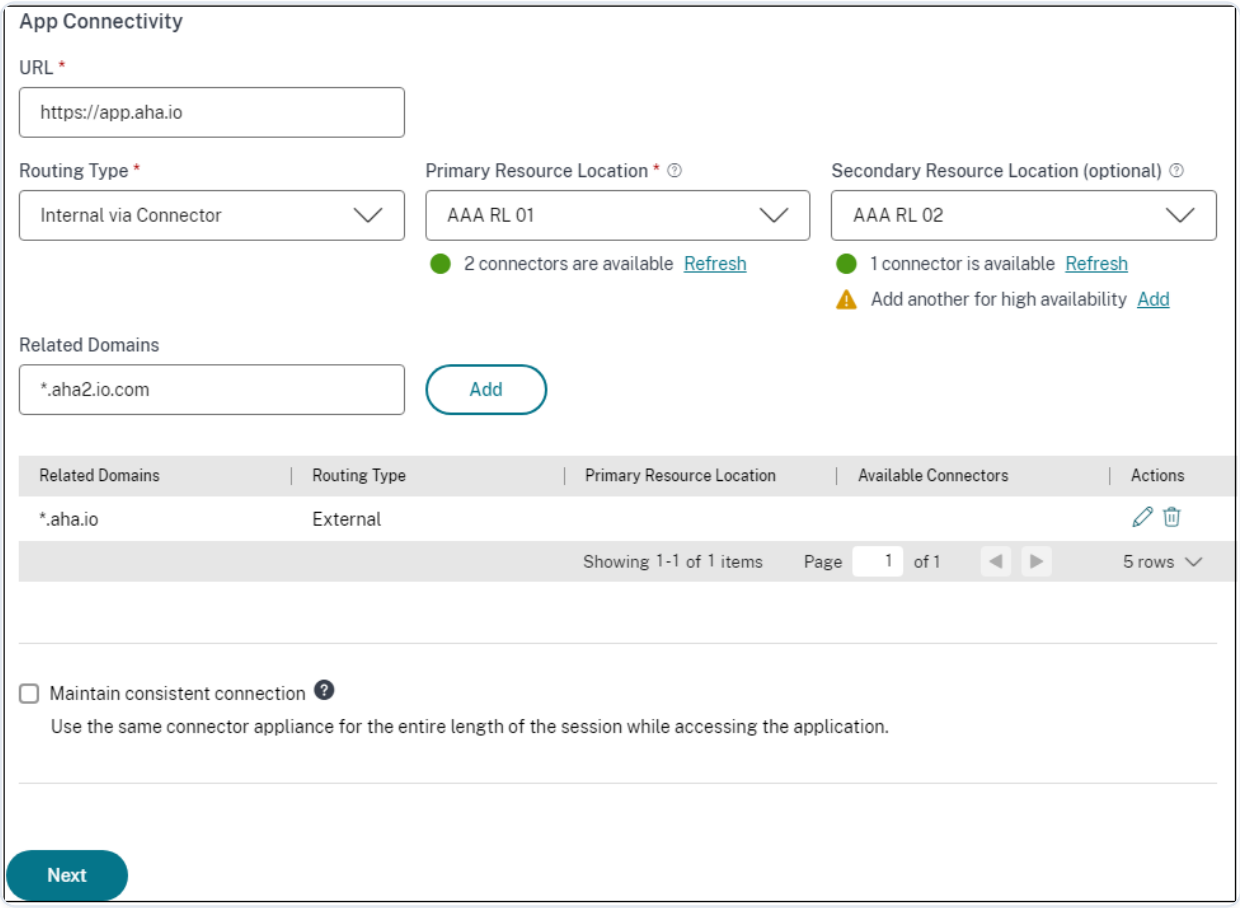
Secure Private Accessサービスコンソールからお気に入りとしてマークされたアプリを削除した場合、ユーザーはストアのお気に入りリストからアプリを手動で削除する必要があります。Secure Private Accessサービスコンソールから削除しても、アプリはストアから自動的に削除されません。

重要:

- SaaSアプリへのアクセスは、そのアクセスポリシーによって管理されます。アプリは、ユーザーに一致するアクセスポリシー規則に基づいて、アクセスが許可されるか、ブロックされるか、または管理されないままになります。ユーザーに一致する規則がない場合、またはアプリに関連付けられているアクセスポリシーがない場合、アプリはブロックされません。管理されないままになり、ブラウザが直接接続します。いずれの規則にも該当しないユーザーのアプリをブロックするには、最も低い優先度で「すべてのユーザー > アクセス拒否」規則を追加します。詳しくは、「デフォルトでSaaSアプリケーションをブロックする」を参照してください。
- 複数のアプリが同じFQDNまたはワイルドカードFQDNのバリエーションで構成されている場合、競合する構成になる可能性があります。
- これらの問題は、いくつかのベストプラクティスに従うことで解決できます。詳しくは、「WebおよびSaaSアプリケーション構成のベストプラクティス」を参照してください。

5. 「**アプリ接続**」セクションで、ドメインをCitrix Connector™ Applianceを介して外部または内部にルーティングする必要がある場合に、アプリケーションの関連ドメインのルーティングを定義します。

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



- 「**ルーティングの種類**」 - 次のいずれかを選択します。
  - 「**内部 – プロキシをバイパス**」 - ドメインのトラフィックは、Connector Appliance™を介してルーティングされ、Connector Applianceで構成された顧客のWebプロキシをバイパスします。
  - 「**コネクタ経由の内部**」 - アプリは外部のものでもかまいませんが、トラフィックはConnector Applianceを介して外部ネットワークに流れる必要があります。
  - 「**外部**」 – トラフィックはインターネットに直接流れます。
  - 「**Google Secure Gateway経由の外部**」 — トラフィックはGoogle Secure Gatewayを介してインターネットに流れます。詳しくは、「Google Secure Gateway経由のルーティング」を参照してください。

  アプリルーティングタイプ(/en-us/citrix-secure-private-access/media/spa-saas-app-routing-type.png)

- **プライマリおよびセカンダリリソースロケーション** - 管理者は、セカンダリリソースロケーションを設定するか、**First Available** オプションを使用することで、障害発生時でもアプリケーションの高い可用性を確保できます。

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

- **プライマリリソースロケーション:** アプリケーションがホストされているプライマリリソースロケーションを選択します。または、管理者は**プライマリリソースロケーション**で**First Available**オプションを選択できます。
- **First available: First Available**オプションは、動作中のリソースロケーションが使用されることを保証します。**First Available**が選択されている場合、システムは自動的にトラフィックを最初に利用可能なロケーションにルーティングします。これにより、手動での介入なしに継続的なアプリケーションアクセスが保証されます。たとえば、ResourceLocation1が利用できないがResourceLocation2に到達可能な場合、ResourceLocation2がデフォルトでアプリケーションのフロントエンドとして選択されます。
- **セカンダリリソースロケーション - セカンダリリソースロケーション**オプションは、プライマリリソースロケーションが明示的に指定されている場合にのみ利用可能になります。プライマリリソースロケーションが、Connector Applianceの障害やデータセンターの障害などの理由で利用できなくなった場合、アプリケーションは指定されたセカンダリリソースロケーションにフェイルオーバーします。セカンダリリソースロケーションは、アプリケーションが別のデータセンターでホストされている場合でも、フェイルオーバーとして機能できます。

関連する各ドメインに対して、プライマリおよびセカンダリリソースロケーションを設定するか、**First Available**オプションを選択することもできます。

a. 関連ドメインテーブルの**アクション**列にある編集アイコンをクリックします。
b. プライマリおよびセカンダリリソースロケーションを設定するか、**First Available**オプションを選択します。

関連ドメイン(/en-us/citrix-secure-private-access/media/backup-rl-related-domains.png)

注:

- バックアップリソースロケーションの設定と**First Available**オプション機能の使用は、現在プレビュー段階です。
- アプリケーションを削除すると、そのルーティングエントリは自動的に削除されます。詳細については、「アプリケーション削除時のルーティングエントリの自動クリーンアップ」を参照してください。

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

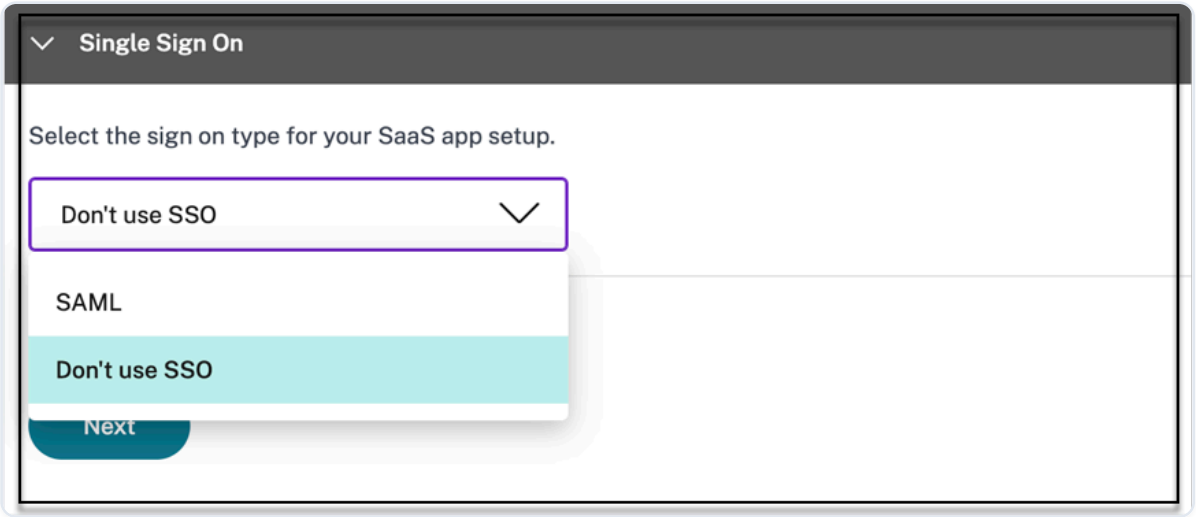
- **一貫した接続を維持** - このチェックボックスをオンにすると、同じConnector Applianceへの一貫した接続が有効になります。一貫した接続の詳細については、「一貫した接続を維持する」を参照してください。

> **注:**
>
> **一貫した接続を維持**オプションが選択されている場合、アプリケーションのルーティングタイプは、セクションで**コネクタ経由の内部**に設定する必要があります。

6. 優先するサインオン方法を設定します。

> **注:**
>
> シングルサインオンオプションは、Chrome Enterprise (CEP) を使用するCitrix Secure Accessには適用されません。

a. **シングルサインオン**セクションで、アプリケーションに使用する優先シングルサインオンタイプを選択し、**保存**をクリックします。以下のシングルサインオンタイプが利用可能です。



- **SSOを使用しない** – バックエンドサーバーでユーザーを認証する必要がない場合は、**SSOを使用しない**オプションを使用します。**SSOを使用しない**オプションが選択されている場合、ユーザーは**アプリの詳細**セクションで構成されたURLにリダイレクトされます。
- **SAML** - WebアプリケーションへのSAMLベースのSSOには**SAML**を選択します。**SAML** SSOタイプの構成詳細を入力します。

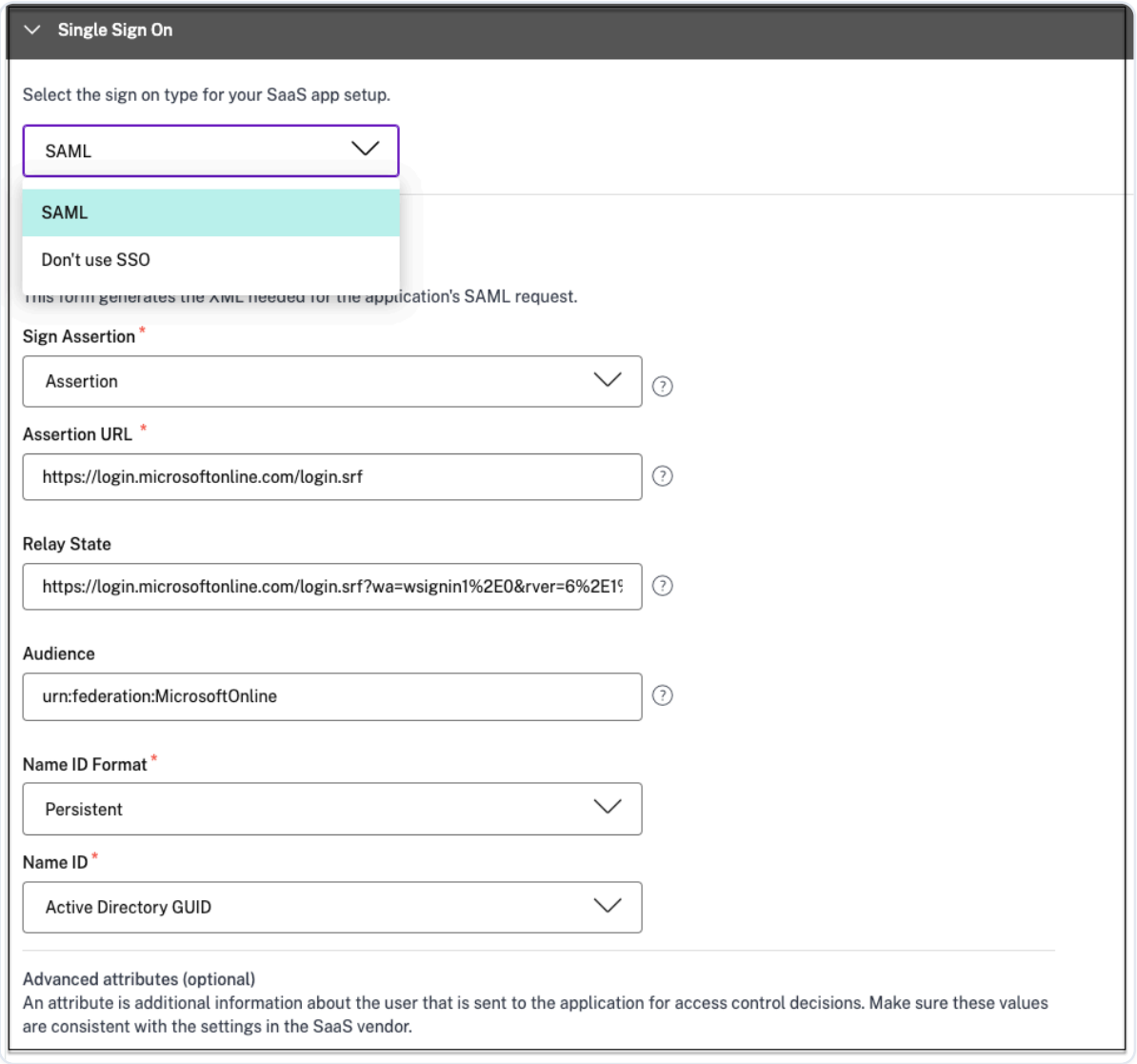
サインオンセクションに以下の詳細を入力し、**保存**をクリックします。

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

- **アサーションの署名** - アサーションまたは応答に署名することで、応答またはアサーションが依拠当事者 (SP) に配信される際のメッセージの整合性が保証されます。**アサーション、応答、両方、またはなし**を選択できます。
- **アサーションURL** – アサーションURLはアプリケーションベンダーによって提供されます。SAMLアサーションはこのURLに送信されます。
- **リレーステート** – リレーステートパラメータは、ユーザーがサインインして依拠当事者のフェデレーションサーバーに誘導された後にアクセスする特定のリソースを識別するために使用されます。リレーステートはユーザー向けに単一のURLを生成します。ユーザーはこのURLをクリックしてターゲットアプリケーションにログオンできます。
- **オーディエンス** – オーディエンスはアプリケーションベンダーによって提供されます。この値は、SAMLアサーションが正しいアプリケーションに対して生成されたことを確認します。
- **名前ID形式** – サポートされている名前識別子形式を選択します。
- **名前ID** – サポートされている名前IDを選択します。
- IDプロバイダーが開始するフローを上書きし、サービスプロバイダーが開始するフローのみを使用するには、**特定のURLを使用してアプリを起動する (SP開始)** を選択します。

b. 「**詳細属性（オプション）**」で、アクセス制御の決定のためにアプリケーションに送信されるユーザーに関する追加情報を追加します。

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



c. **SAMLメタデータ**の下にあるリンクをクリックして、メタデータファイルをダウンロードします。ダウンロードしたメタデータファイルを使用して、SaaSアプリサーバーでSSOを構成します。

- **ログインURL**の下にあるSSOログインURLをコピーし、SaaSアプリサーバーでSSOを構成する際にこのURLを使用できます。
- **証明書**リストから証明書をダウンロードし、SaaSアプリサーバーでSSOを構成する際にその証明書を使用することもできます。

7. **保存**をクリックし、次に**完了**をクリックします。

完了をクリックすると、アプリがアプリケーションページに追加されます。アプリケーションを構成した後、アプリケーションページからアプリを編集または削除できます。そのためには、アプリの省略記号ボタンをクリックし、それに応じてアクションを選択します。

- **アプリケーションの編集**
- **削除**

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

Google Secure Gateway経由のルーティング

SaaSアプリのルーティングタイプを**Google Secure Gateway経由の外部**に設定すると、そのアプリのトラフィックは、クライアントから直接ではなく、Google Secure Gatewayを介してインターネットにルーティングされます。

- アプリケーションの構成中にこのルーティングタイプを設定でき、そのアプリのデフォルトルーティングになります。
- アクセスポリシーでルーティング例外として設定することもでき、そのポリシーのユーザーにのみ適用され、アプリのデフォルトルーティングを上書きします。
- このルーティングタイプは、SaaSアプリと、Google Chrome Enterprise Premiumと統合されたお客様のみが利用できます。内部Webアプリでは利用できません。
- Citrix Secure Accessクライアントでは、このオプションは**外部**と同じように動作します。インポート時に、**ルーティングタイプ**の値を**Google Secure Gateway経由の外部**に設定します。

注:

Citrix Enterprise Browser™ を介してアクセスされる SaaS アプリの場合、**ルーティングタイプ**は、**External** ではなく **External via Google Secure Gateway** と表示されます。これは UI 表示の違いにすぎず、ルーティング動作を変更するものではありません。トラフィックは引き続きインターネットに直接流れます。

アプリケーション削除時のルーティングエントリの自動クリーンアップ

アプリケーションを構成すると、その宛先 (FQDN またはアプリケーションドメイン) がルーティングテーブルに追加され、Secure Private Access はルーティングの決定にそれを使用します。アプリケーションを削除すると、Secure Private Access は次のルールに基づいてルーティングエントリをクリーンアップします。

- **参照されていないエントリは削除されます** - 削除されたアプリケーションに関連付けられているルーティングエントリ (FQDN またはアプリケーションドメイン) が他のどのアプリケーションからも参照されていない場合、Secure Private Access はルーティングテーブルから自動的に削除します。
- **共有エントリは保持されます** - ルーティングエントリが複数のアプリケーションで使用されている場合、それらのアプリケーションのいずれかを削除しても、共有エントリは削除されません。エントリは、少なくとも1つのアクティブなアプリケーションがそれを参照している限り、ルーティングテーブルに残ります。

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

- **遡及的な削除はありません** - ルーティングエントリは、アプリケーションの削除の一部としてのみ評価および削除されます。既存のエントリは、どのアプリケーションにも使用されていないことが確認されない限り、遡及的に削除されることはありません。

注:

- アプリケーションページからアプリケーションが削除されると (省略記号 (...) メニューを使用して)、クリーンアップは自動的に実行されます。管理者の操作は不要です。
- 共有ルーティングエントリは保持されるため、アプリケーションを削除しても、同じ宛先を共有する他のアプリケーションへのアクセスが中断されることはありません。

SaaS アプリサーバー固有の構成

以下は、テンプレートを使用したアプリサーバー固有の構成に関するガイダンスが記載されたドキュメントへのリンクです。Citrix は現在、以下の SaaS アプリをサポートしており、今後もさらに多くのアプリのサポートを追加していきます。

- 15Five - 従業員を指導するための継続的なパフォーマンス管理ツール。
- 10000 ft - 成長を計画するためのプロジェクト管理ツール。
- 4me - 社内、社外、およびアウトソースされたチーム間のコラボレーションのためのサービス管理ツール。
- Abacus - リアルタイム経費報告ソフトウェア。
- Absorb - 学習管理ツール。
- Accompa - 製品開発のための要件管理ツール。
- Adobe Captivate Prime - デバイスを問わずパーソナライズされた学習体験を提供する学習管理システム。
- Aha - 製品を開発し、キャンペーンを開始するための製品ロードマップおよびマーケティング計画ツール。
- AlertOps - ITインシデントを管理するためのコラボレーションインシデント対応ツール。
- Allocadia - 組織のマーケティング計画プロセスを管理するためのマーケティングパフォーマンス管理ツール。`
- Ana plan - データ、人、計画を連携させることで、組織の意思決定を支援する計画ツール。
- &frankly - 職場での変化を推進するためのエンゲージメントツール。

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

- Anodot - 時系列データを監視し、異常を検出し、ビジネスパフォーマンスをリアルタイムで予測するAIプラットフォーム。
- App Follow - グローバルなアプリの成長を加速し、顧客ロイヤルティを高めるための製品管理ツール。
- Assembla - ソフトウェア開発のためのバージョン管理およびソースコード管理ツール。
- Automox - パッチ適用プロセスを追跡、制御、管理するためのパッチ管理ツール。
- Azendoo - チームが会話や共同作業を行うためのコラボレーションツール。
- BambooHR - 従業員データを管理するための人事管理ツール。
- Bananatag - メールを追跡およびスケジュールし、ファイルを追跡し、メールテンプレートを作成するためのツール。
- Base CRM - メール、電話、メモを管理するための営業管理ツール。
- Beekeeper - 複数の運用システムと通信チャネルを、デスクトップおよびモバイルデバイスからアクセスできる1つのセキュアハブに統合するためのツール。
- BitaBIZ - 休暇および欠勤管理のための欠勤・休暇計画およびコミュニケーションツール。
- BlazeMeter - テストスイート。
- Blissbook - 従業員ハンドブックを作成するためのポリシー管理ツール。
- BlueJeans - ビデオ会議ソリューション。
- Bold360 - 顧客エンゲージメントのためのライブチャットツール。
- Bonusly - チームへの貢献を認識するための従業員表彰および報酬管理ツール。
- Box - コンテンツを管理、共有、アクセスするためのコンテンツ管理およびファイル共有ツール。
- Branch - ディープリンクとモバイルを強化するモバイルリンクプラットフォーム。
- Brandfolder - デジタルアセットを保存および共有するためのデジタルアセット管理ツール。
- Breezy HR - 採用ソフトウェアおよび応募者追跡システム。
- `Buddy Punch` - 従業員の勤怠を監視するための時間管理ツール。
- Bugsnag - アプリケーションの安定性を管理し、エラーと診断データを報告するための監視ツール。
- Buildkite - 継続的インテグレーションソフトウェア開発のためのインフラストラクチャツール。
- Bullseye Locations - デバイス上で店舗や販売店を検索するための店舗検索ツール。

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

- CA Flowdock - チームが会話したり共同作業したりするためのコラボレーションツール。
- CakeHR - 勤怠管理とパフォーマンス管理のための人事管理ツール。
- Cardboard - 整理されていない情報を追跡するための共同製品計画ツール。
- Citrix Cedexis - 大規模ウェブサイト向けトラフィック管理ツール。データセンター、クラウドプロバイダー、コンテンツデリバリーネットワークのマルチベンダーソーシングを活用します。
- CipherCloud - クラウドベースのアプリケーションを採用する企業向けに、エンドツーエンドのデータ保護、高度な脅威保護、および包括的なコンプライアンス機能を提供するプラットフォーム。
- Celoxis - プロジェクト計画の作成、作業の自動化、共同作業を行うためのプロジェクト管理ツール。
- CircleHD - 組織内でビデオやスライドを共有するためのトレーニング、学習、コラボレーションツール。
- Circonus - アラート、グラフ、ダッシュボード、機械学習インテリジェンスを提供するデータ分析および監視ツール。
- Cisco Umbrella - インターネット上の脅威に対する最初の防御線を提供するクラウドセキュリティプラットフォーム。
- ClearSlide - 顧客とのやり取りのためにコンテンツや営業資料を共有できる営業エンゲージメントツール。
- Cloudability - クラウド環境全体での可視性、最適化、ガバナンスを向上させるクラウドコスト管理プラットフォーム。
- CloudAMQP - プロセス間および他のシステム間でメッセージを渡すためのメッセージキューツール。
- CloudCheckr - ユーザーがAWSおよびAzureのデプロイメントを最適化するのに役立つコスト管理、セキュリティ、レポート、および分析ツール。
- CloudMonix - クラウドおよびオンプレミスリソースの監視と自動化のためのツール。
- CloudPassage - サイバーリスクを軽減し、コンプライアンスを維持するための可視化および継続的監視ツール。
- CloudRanger - AWSクラウドのバックアップ、災害復旧、サーバー制御を効率化するためのツール。
- Clubhouse - ソフトウェア開発のためのプロジェクト管理ツール。

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

- Coggle - 階層構造のドキュメント（分岐ツリーなど）を作成するためのマインドマッピングWebアプリケーション。
- Comm100 - カスタマーサービスプロフェッショナル向けのカスタマーサービスソフトウェアおよびコミュニケーションツール。
- Confluence - チームが共同作業を行い、知識を共有するのに役立つコンテンツコラボレーションツール。
- ConceptShare - コンテンツをより速く、より迅速に、より安価に提供するための校正ツール。
- Concur - 外出先で経費を管理するための出張・経費管理ツール。
- ConnectWise Control - リモートサポートとアクセスを提供するためのビジネス管理ツール。
- Contactzilla - 最新の連絡先情報にアクセスするための連絡先管理ツール。
- ContractSafe - 契約を追跡、保存、管理するための契約管理ツール。
- Contentful - あらゆるプラットフォームにコンテンツを作成、管理、配信するためのコンテンツソフトウェア。
- Convo - 内部コミュニケーションのためのチームコミュニケーションおよびコラボレーションツール。
- Copper - CRMツール。
- Cronitor - cronジョブの監視ツール。
- Crowdin - 開発者向けにシームレスで継続的なローカリゼーションを提供するソリューション。
- Dashlane - デジタルウォレットも管理するパスワード管理ツール。
- Declaree - 出張用の旅費交通費管理ツール。
- Dell Boomi - クラウドとオンプレミスのアプリケーションおよびデータを接続するための統合ツール。
- Deskpro - チケット管理、顧客のセルフヘルプ、顧客フィードバックを容易にするヘルプデスクツール。
- Deputy - 従業員の時間、タスク、コミュニケーションのスケジュール設定と追跡を行うワークフォース管理ツール。
- DigiCert - WebサイトのSSL証明書用の証明書管理およびトラブルシューティングツール。
- Dmarcian - スパム、マルウェア、フィッシングをフィルタリングするメール監視ツール。
- DocuSign - 保険、医療、不動産などのさまざまなドキュメントに対応するオンライン署名ツール。

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

- DOME9 ARC - パブリッククラウド環境を管理するためのセキュリティおよびコンプライアンスツール。
- Dropbox - 安全なファイル共有と保存のためのクラウドストレージツール。
- Duo - アプリケーションへの安全なアクセスを提供するセキュリティツール。
- Dynatrace - 医療検査サービス。
- Easy Projects - プロジェクト管理ツール。
- EdApp - ワークスペース学習のための学習管理ツール。
- EduBrite - トレーニングプログラムの作成、提供、追跡を行うための学習管理ツール。
- Ekarda - 電子カードデザインツール。
- Envoy - 人員と荷物を管理するための訪問者管理ツール。
- Evernote - メモ作成、整理、タスクリスト、アーカイブのためのアプリケーション。
- Expensify - 経費報告書管理、領収書追跡、出張のための経費管理ツール。
- ezeep - あらゆるデバイス、あらゆる場所からクラウド内のあらゆるプリンターに印刷するための印刷インフラ管理ツール。
- EZOfficeInventory - すべての資産と機器を追跡するための在庫管理ツール。
- EZRentOut - 機器の品質と可用性を追跡するための機器レンタルツール。
- Fastly - ユーザーに近い場所でアプリケーションを提供し、保護するためのエッジクラウドプラットフォーム。
- Favro - 組織のワークフローのための計画およびコラボレーションツール。
- Federated Directory - 異なる企業の企業アドレス帳を検索するための企業間連絡先ディレクトリツール。
- フィーダー
- Feedly - さまざまなソースからのニュースフィードをまとめるためのニュースアグリゲーションツール。
- FileCloud - 組織向けに堅牢で安全なファイルホスティングおよび共有プラットフォームを提供するソフトウェアソリューション。
- Fivetran - アナリストがデータをクラウドウェアハウスに複製するのに役立つツール。
- Flatter Files - 図面やドキュメント用のデジタルフラットファイルキャビネットで、コンテンツへのアクセスを安全かつシンプルに提供します。
- Float - プロジェクトのスケジュール設定とチームの利用状況管理のためのリソース計画ツール。

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

- Flock - コラボレーションツール。
- Formstack - オンラインフォームビルダーおよびデータ収集ツール。
- FOSSA - CI/CDにネイティブに組み込まれた、自動化されたオープンソースライセンススキャンおよび脆弱性管理ツール。
- Freshdesk - 顧客のニーズをサポートするためのカスタマーサポートツール。
- Freshservice - IT運用を簡素化するためのITヘルプデスクツール。
- FrontApp - すべての会話を一元管理するためのコラボレーションツール。
- Frontify - 日々のブランディング、マーケティング、開発業務を促進し、合理化するためのプラットフォーム。
- Fulcrum - モバイルフォームを簡単に構築し、データを収集できるモバイルデータ収集プラットフォーム。
- Fusebill - 請求管理および定期請求ソフトウェア。
- G-Suite - 社内の人々をつなぐインテリジェントなアプリのセット。
- GetGuru - ナレッジ管理ソフトウェア。
- GitBook - ドキュメントを作成および維持するためのツール。
- GitHub - 企業ファイアウォールの内側でホストされているリポジトリに対してGitを使用したバージョン管理のためのWebベースのホスティングサービスです。
- GitLab - 単一のアプリケーションとして提供される、完全なDevOpsプラットフォームです。
- GlassFrog - ホラクラシーの実践のためのソフトウェアです。
- GoodData - 高速で信頼性が高く、使いやすい分析を提供する組み込みBIおよび分析プラットフォームです。
- GotoMeeting - HDビデオ会議機能を備えたオンライン会議ソフトウェアです。
- HackerRank - 消費者および企業向けの競技プログラミング課題を提供します。
- HappyFox - オンラインヘルプデスクソフトウェアおよびWebベースのサポートチケットシステムです。
- Helpjuice - ナレッジベースを作成および維持するためのナレッジ管理ソリューションです。
- Help Scout - カスタマーサービスプロフェッショナル向けのカスタマーサービスソフトウェアおよびナレッジベースツールです。
- Hello sign - いつでも、どこからでも、どのデバイスからでも署名を可能にする電子署名インターフェースです。
- HelpDocs - ユーザーが困ったときにガイドするナレッジベースソフトウェアです。

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

- Honeybadger - アプリケーションの健全性監視ツールです。
- Harness - AWS、GCP、Azure、およびベアメタル環境におけるJava、.NETアプリケーションの継続的デリバリーおよび統合のためのツールです。
- HelpDocs - ユーザーが困ったときにガイドするための信頼できるナレッジベースを作成するツールです。
- Helpmonks - チームコラボレーションのための共同メールプラットフォームです。
- Hoshinplan - 戦略計画を視覚化し、ステータスを1つのキャンバスで追跡するためのツール。
- Hosted Graphite - ウェブサイト、アプリ、サーバー、コンテナのパフォーマンスを監視するためのツール。
- Humanity - シフト、スケジュール、給与、勤怠管理を行うオンライン従業員スケジューリングソフトウェア。
- Igloo - 組織全体のIT課題を解決するためのデジタルワークプレイスおよびイントラネットソリューションプロバイダー。
- iLobby - クラウドベースの訪問者登録管理ソリューション。
- Illumio - データセンターおよびクラウド環境内での侵害の拡散を防ぐセキュリティシステム。
- Image Relay - デジタルファイルを安全に整理および共有するためのデジタルアセット管理およびブランド管理ソフトウェア。
- Informatica - SaaSアプリ統合のためのツールであり、カスタム統合サービスを開発および展開するためのプラットフォーム。
- Intelligent contract - 契約管理ソフトウェア。
- iMeet Central - マーケター、クリエイティブエージェンシー、エンタープライズビジネス向けのプロジェクト管理ソフトウェア。
- InteractGo - システムパフォーマンスに関するリアルタイムおよび履歴データを測定するためのツール。
- iQualify One - 本格的な学習体験を提供するための学習および管理ツール。
- InsideView - 営業、マーケティング、その他のビジネス課題を解決するためのデータおよびインテリジェンスソリューション。
- Insightly - 中小企業向けのクラウドベースの顧客関係管理 (CRM) およびプロジェクト管理ツール。
- ITGlue - MSPがドキュメントを標準化し、ナレッジベースを作成し、パスワードを管理し、デバイスを追跡するのに役立つクラウドベースのITドキュメントプラットフォーム。

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

- Jitbit - 受信したサポートリクエストメールとそれに関連するチケットを管理および追跡するためのヘルプデスクソフトウェアおよびチケットシステム。

JupiterOne - セキュリティプロセス全体を作成および管理するためのソフトウェアプラットフォーム。

- Kanbanize - リーンマネジメントのためのオンラインポートフォリオかんばんソフトウェア。
- Klipfolio - チームや顧客向けの強力なリアルタイムビジネスダッシュボードを構築するためのオンラインダッシュボードプラットフォーム。
- Jira - 課題やプロジェクトを計画、追跡、管理するためのツール。
- Kanban Tool - チームのパフォーマンスを向上させ、生産性を高めるためのビジュアル管理ソフトウェア。
- Keeper Security - パスワードと個人情報を保護するためのパスワードマネージャーおよびセキュリティソフトウェア。
- Kentik - ネットワークおよびパフォーマンス監視、DDoS保護、リアルタイムのアドホックネットワークフロー分析にビッグデータを適用するためのツール。
- Kissflow - ワークフロープロセスを自動化するためのワークフローツールおよびビジネスプロセスワークフロー管理ソフトウェア。
- KnowBe4 - セキュリティ意識向上トレーニングとシミュレートされたフィッシングを提供するツール。
- KnowledgeOwl - ナレッジベースおよびオーサリングツール。
- Kudos - 小売、ジョブ、プロジェクト、およびフルフィルメントプロセスシステム。
- LaunchDarkly - 開発チームと運用チームが機能のライフサイクルを制御できるようにする機能管理プラットフォーム。
- Lifesize - ビデオ会議ソリューション。
- Litmos - 従業員トレーニング、顧客トレーニング、コンプライアンス研修、パートナー研修のための学習管理システム。
- LiquidPlanner - ビジネス向けのオンラインプロジェクト管理ソフトウェア。
- LeanKit - 企業が作業を視覚化し、プロセスを最適化し、より迅速に提供できるようにする、リーンベースのエンタープライズプロセスおよび作業管理ソフトウェア。
- LiveChat - ビジネス向けのライブチャットおよびヘルプデスクソフトウェア。
- LogDNA - すべてのソースからのログを1つの集中型ロギングツールで収集、監視、解析、分析するためのツール。

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

- Mango - サイロ化されたアプリケーションを単一のプラットフォームに統合し、合理化するためのチームコラボレーションソフトウェア。
- Manuscript - 作業の計画、編集、共有を支援するライティングツール。
- Marketo - マーケティングチームがデジタルマーケティングの技術と科学を習得するのに役立つ自動化ソフトウェア。
- Matomo - ウェブサイトを訪れるすべてのユーザーのジャーニー全体を評価するWeb分析プラットフォーム。
- Meisterplan - 組織がプロジェクトポートフォリオを作成するのに役立つソフトウェア。
- Mingle - チーム全体に統合されたワークプレイスを提供するアジャイルプロジェクト管理およびコラボレーションツール。
- MojoHelpdesk - ヘルプデスクソフトウェアおよびチケットシステム。
- Monday - すべての作業を1つのツールで計画、追跡、共同作業するためのチーム管理ソフトウェア。
- Mixpanel - Webおよびモバイルでのユーザーインタラクションを追跡するシステム。
- MuleSoft - クラウドおよびオンプレミスでSaaSおよびエンタープライズアプリケーションを接続するための統合ソフトウェア。
- MyWebTimesheets - さまざまなプロジェクト/ジョブ/アクティビティに費やされた時間を追跡するためのオンライン時間追跡システム。
- New Edge - ハイブリッドIT向けのセキュアなアプリケーションネットワーキングサービス。
- NextTravel - 企業向け出張管理ソフトウェアツール。
- N2F - 業務および出張経費を管理するための経費報告書管理ツール。
- New Relic - アプリケーションとインフラストラクチャのパフォーマンスを測定および監視するためのデジタルインテリジェンスプラットフォーム。
- Nmbrs - 企業向けのクラウドHRおよび給与計算ソフトウェア。
- Nuclino - リアルタイムで共同作業し、情報を共有するためのコラボレーションソフトウェア。
- Office365 - Microsoftのクラウドベースのサブスクリプションサービス。
- OfficeSpace - 組織がワークスペースを割り当てるのに役立つクラウドベースのプラットフォーム。
- OneDesk - 顧客とつながり、サポートするためのプロジェクト管理およびヘルプデスクソフトウェア。
- OpsGenie - DevOpsおよびIT Opsチームがアラートとインシデント解決プロセスを効率化するためのインシデント管理プラットフォーム。

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

- Orginio - 組織構造を視覚化するためのオンライン組織図作成ツール。
- Oomnitza - 資産を追跡および管理するためのIT資産管理プラットフォームソリューション。
- OpenEye - Apexレコーダーでライブおよび録画ビデオを視聴するためのモバイルアプリ。
- Oracle ERP Cloud - 企業機能を管理するためのクラウドベースのソフトウェアアプリケーションスイート。
- Pacific Timesheet - 給与、プロジェクト時間、経費のためのWebベースのタイムシートツール。
- PagerDuty - デジタル運用管理システム。
- PandaDoc - iPhoneユーザーがモバイルデバイスでドキュメント、分析、ダッシュボードに直接アクセスできるモバイルアプリ。
- Panopta - インフラストラクチャ監視ツール。
- Panorama9 - エンタープライズネットワーク監視のためのクラウドベースのIT管理プラットフォーム。
- Papyrs - 独自のイントラネットページを設計するためのエディター。
- ParkMyCloud - AWS、Azure Services、またはGCPに接続するための単一目的のSaaSツール。
- Peakon - 従業員のエンゲージメントを測定し、改善するためのツール。
- People HR - すべての主要な人事機能に対応する人事ソフトウェアシステム。
- Pingboard - チーム編成と人員計画のための組織図を作成するツール。
- Pigeonhole Live - インタラクティブなQ&Aプラットフォーム。
- Pipedrive - 営業CRMおよびパイプライン管理ソフトウェア。
- PlanMyLeave - 従業員の休暇を管理および追跡するための休暇管理システム。
- PlayVox - カスタマーサービス品質監視ツール。
- Podbean - ポッドキャストサービスプロバイダー。
- Podio - プロジェクト管理ワークスペースでチームコミュニケーション、ビジネスプロセス、データ、コンテンツを整理するためのWebベースのツール。
- POPin - 問題解決のためのチームエンゲージメントを運用するクラウドソーシングプラットフォームおよびモバイルアプリ
- Postman - API開発環境。
- Prescreen - 求人情報をオンラインおよびオフラインで公開するための応募者追跡ツール。
- ProductBoard - プロダクト管理ツール。

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

- ProdPad - プロダクト戦略を開発するためのプロダクト管理ソフトウェア。
- Proto.io - 完全にインタラクティブな高忠実度プロトタイプを作成するためのアプリケーションプロトタイピングプラットフォーム。
- Proxyclick - 訪問者を管理し、ブランドイメージを構築し、セキュリティを確保するためのクラウドベースの訪問者管理ソリューション。
- Pulumi - コンテナ、サーバーレス、インフラストラクチャ、Kubernetes向けのクラウドネイティブ開発プラットフォーム。
- PurelyHR - 従業員の休暇データにアクセスするための休暇管理ツール。
- Promapp - ビジネスプロセス管理 (BPM) ツール。
- Prescreen - 求人情報をオンラインおよびオフラインで公開するためのクラウドベースの応募者追跡システム。
- QAComplete - ソフトウェアテスト管理ツール。
- Qualaroo - 顧客からインサイトを得るためのフィードバックツール。
- Quality Built, LLC - 信頼性と革新的な第三者品質保証サービスを提供する保険、金融、建設業界。
- Qubole - Amazon上に構築されたビッグデータ分析用セルフサービスプラットフォーム。
- Questetra BPM Suite - 日常的なワークフローに対応するWebベースのビジネスプロセスプラットフォーム。
- QuestionPro - アンケートや質問票を作成するためのオンラインアンケートソフトウェア。
- Quandora - 質疑応答ベースのナレッジ管理ソリューション。
- Quip - モバイルおよびWeb向けの共同作業生産性ソフトウェアスイート。
- Rackspace - マネージドクラウドコンピューティングサービス。
- ReadCube - Web、デスクトップ、モバイル向けの参照管理ツール。
- RealtimeBoard - 組織がフォーマット、ツール、場所、タイムゾーンを超えて共同作業を行うためのホワイトボードコラボレーションツール。
- Receptive - 顧客、チーム、市場からのフィードバックを一か所に集約するツール。
- Remedyforce - ITサービス管理およびヘルプデスクシステム。
- Retrace - バグ追跡、データ集約、自動アラートを提供するアプリケーションパフォーマンス管理ツール。
- Robin - 会議室やデスクの予約をスケジュールするためのワークプレイスエクスペリエンスツール。
- Rollbar - 開発者向けのリアルタイムエラーアラートおよびデバッグツール。

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

- Really Simple Systems - 中小企業が販売とマーケティングを管理するためのクラウドベースのCRMソフトウェア。
- Reamaze - 単一プラットフォームでチャット、ソーシャル、SMS、FAQ、メールを使用して顧客をサポート、エンゲージ、コンバートするための顧客サポートソフトウェア。
- Resource Guru - 人員、機器、その他のリソースをスケジュールするためのリソース管理ソフトウェア。
- Retrace - コードプロファイリング、エラー追跡、アプリケーションログ、メトリクスを統合するアプリケーションパフォーマンス管理。
- Roadmunk - プロダクトロードマップを作成するためのプロダクトロードマップソフトウェアおよびロードマップツール。
- Runscope - 機能的なAPIテストとモニターを作成、管理、実行するためのツール。
- Salesforce – 顧客連絡先情報の管理、ソーシャルメディアの統合、リアルタイムの顧客コラボレーションを促進するCRMツール。
- SalesLoft - 効率的で収益向上に貢献するセールスエンゲージメントプラットフォーム。
- Salsify - プロダクトエクスペリエンス管理 (PXM) プラットフォーム。
- Samanage - ITサービス管理のためのツール。
- Samepage - オンラインプロジェクトを管理するためのコラボレーションソフトウェア。
- Screencast-O-Matic – スクリーンキャストとビデオ編集のためのツール。
- ScreenSteps –スクリーンキャプチャを中心としたビジュアルドキュメントを作成するためのツール。
- SendSafely – ファイルとメールの安全な交換のための暗号化プラットフォーム。
- Sentry - オープンソースのエラートラッキングソフトウェア。
- ServiceDesk Plus - ITサービスデスクのためのツール。
- ServiceNow - デジタルワークフローを作成するためのクラウドプラットフォーム。
- SharePoint – ドキュメント管理とストレージに使用されるコラボレーションプラットフォーム。
- Shufflrr - プレゼンテーションの作成、更新、共有、およびブロードキャストを行うためのプレゼンテーション管理ツール。
- Sigma Computing – データを探索、分析、視覚化するための分析ツール。
- Signavio – ビジネスプロセスモデリングツール。
- Skeddly - AWSリソースを自動化するツール。

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

- Skills Base - 従業員のパフォーマンスとスキルを追跡および文書化するためのタレント管理ツール。
- Skyprep - 顧客と従業員をトレーニングするための学習管理システム (LMS)。
- Slack - コミュニケーションと情報共有のためのコラボレーションツール。
- Slemma - 複数のデータセットからデータレポートを作成するためのデータ分析ツール。
- Sli.do - 会議、イベント、カンファレンス向けのインタラクションツール。
- SmartDraw - フローチャート、組織図、マインドマップ、プロジェクトチャート、その他のビジネスビジュアルを作成するために使用される図形ツール。
- SmarterU - 顧客と従業員をトレーニングするための学習管理システム (LMS)。
- Smartsheet - タスクの割り当て、プロジェクトの進捗状況の追跡、カレンダーの管理、ドキュメントの共有を行うためのコラボレーションツール。
- SparkPost - メール配信サービス。
- Split - 割り勘アプリケーション。
- Spoke - サービスチケットを登録するためのサービスデスクツール。
- Spotinst - 企業がクラウドインフラストラクチャの容量を購入および管理するのに役立つSaaS最適化プラットフォーム。
- SproutVideo - ビジネスビデオをホストするためのプラットフォーム。
- Stackify - PrefixやRetraceなどのツールスイートでサポートを提供するトラブルシューティングツール。
- StatusCast - ダウンタイムとウェブサイトのメンテナンスについて従業員と顧客に情報を提供するホスト型ページ。
- StatusDashboard - ステータスダッシュボードをホストし、インシデント通知を顧客にブロードキャストするためのコミュニケーションプラットフォーム。
- Status Hero - チームからのステータス更新と日々の目標を追跡するためのツール。
- StatusHub - サービス状態ページをホストするためのプラットフォーム。
- Statuspage - ステータスとインシデントを伝達するためのツール。
- SugarCRM - Salesforce自動化、マーケティングキャンペーン、カスタマーサポート、コラボレーション、モバイルCRM、ソーシャルCRM、レポート作成のためのCRMツール。
- Sumo Logic - セキュリティ、運用、BIのユースケースに焦点を当てたデータ分析ソフトウェア。
- Supermood - 従業員のフィードバックをリアルタイムで収集するためのHRプラットフォーム。

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

- Syncplicity - ファイルを共有および同期するためのツール。
- Tableau - インタラクティブなデータ視覚化を作成するためのツール。
- TalentLMS - オンラインセミナー、コース、その他のトレーニングプログラムを促進するための学習管理システム（LMS）。
- Tallie – 領収書をキャプチャしてアップロードし、経費レポートを生成し、経費の詳細をカスタマイズするためのツール。
- Targetprocess - Scrum、Kanban、SAFeなどのアジャイルプロジェクト管理ソフトウェア。
- Teamphoria - リアルタイムの従業員エンゲージメント指標、従業員レビュー、および表彰を提供するソフトウェア。
- TeamViewer - リモートコントロール、デスクトップ共有、オンライン会議、ウェブ会議、およびコンピューター間のファイル転送のためのプロプライエタリソフトウェアアプリケーション。
- Tenable.io - IT環境における脆弱性や設定ミスを特定、調査し、その修復を優先順位付けするためのデータを提供するツール。
- Testable - 行動実験やアンケートを作成するためのツール。
- TestingBot - ライブテストおよび自動テスト用のさまざまなブラウザバージョンを提供するツール。
- TestFairy - 企業にモバイルセッションのビデオ録画、ログ、クラッシュレポートを提供するモバイルテストプラットフォーム。
- TextExpander - 入力中にメールやその他のコンテンツのリポジトリからテキストスニペットを挿入するコミュニケーションツール。
- TextMagic - 顧客とつながるためのメッセージングサービス。
- ThousandEyes - ネットワークインフラストラクチャを監視し、アプリケーション配信のトラブルシューティングを行い、インターネットパフォーマンスをマッピングするツール。
- Thycotic Secret server - パスワードを管理するためのアカウント管理ソフトウェアツール。
- TimeLive – タイムシートを提供し、時間を追跡するためのツール。
- Tinfoil Security - 脆弱性をチェックするためのセキュリティソリューションソフトウェア。
- Trisotech - 顧客がデジタルエンタープライズを発見、モデル化、分析できるようにするツール。
- Trumba - オンラインでインタラクティブなイベントカレンダーを公開するためのツール。
- TwentyThree - マーケティングスタックに動画を統合して追加するためのビデオマーケティングプラットフォーム。

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

- Twilio - コミュニケーションのための開発者プラットフォーム。
- Ubersmith - 従量課金、見積もり、注文管理、インフラストラクチャ管理、およびヘルプデスクチケットソリューションのためのビジネス管理ソフトウェア。
- UniFi - 音声、ウェブコラボレーション、ビデオ会議機能を備えたコミュニケーションおよびコラボレーションソフトウェア。
- UPTRENDS – ウェブサイトの稼働時間とパフォーマンスを追跡するためのウェブサイト監視ソリューション。
- UserEcho - 企業が顧客からのフィードバックを管理するのに役立つコミュニティフォーラムツール。
- UserVoice - 企業がデータに基づいた製品決定を下せるようにする製品フィードバック管理ソフトウェア。
- VALIMAIL - 正当なメールを認証し、フィッシング攻撃をブロックするためのメール認証ソフトウェア。
- Veracode - サイバー脅威やアプリケーションのバックドアから企業を保護するソースコードアナライザーおよびコードスキャナー。
- Velpic - 職場トレーニングを効率化するために設計された学習管理システム (LMS)。
- VictorOps - DevOpsの可観測性、コラボレーション、リアルタイムアラートを提供するインシデント管理ソフトウェア。
- VIDIZMO - 企業向けライブおよびオンデマンドビデオストリーミングソフトウェア。
- Visual Paradigm - チームコラボレーションのためのビジュアルモデリングおよびダイアグラム作成オンラインプラットフォーム。
- Vtiger - 営業、サポート、マーケティングチームが組織化し、共同作業できるようにするCRMツール。
- WaveMaker – カスタムアプリを構築および実行するためのソフトウェア。
- Weekdone - 企業向けにマネージャーダッシュボードとチーム管理サービスを作成するツール。
- Wepow - モバイルおよびビデオ面接ソリューションを通じて、採用担当者、求職者、雇用主をつなぐツール。
- When I Work - 従業員のスケジュール管理と勤怠管理のためのツール。
- WhosOnLocation – サイトやゾーンを通過する人々の流れを追跡するツール。
- Workable - 応募者追跡システム。
- Workday - 財務管理、人事、計画のためのツール。

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

- Workpath - 組織の目標とパフォーマンスを管理するツール。
- Workplace - Facebookが提供するコラボレーションツールで、従業員が使い慣れたインターフェースを通じてコミュニケーションをとるのに役立ちます。
- Workstars - ソーシャルおよびピア従業員表彰プログラムのためのプラットフォーム。
- Workteam - 従業員の時間と勤怠を追跡するツール。
- Wrike - ソーシャルプロジェクト管理およびコラボレーションソフトウェア。
- XaitPorter - 入札書、提案書、その他のビジネス文書のための共同ドキュメント作成ソフトウェア。
- Ximble - 従業員のスケジュール管理と勤怠管理のためのツール。
- XMatters - 他のツールと統合してシームレスなプロセスと効果的なコミュニケーションを実現するアラートソフトウェアを備えたコラボレーションプラットフォーム。
- Yodeck - Webまたはモバイルを通じて、画面をリモートで管理するツール。
- Zendesk - カスタマーサービスを要求し、サポートチケットを記録するためのソフトウェア。
- Ziflow - クリエイティブ制作チーム向けのツール。
- Zillable – コミュニケーション機能を備えたコラボレーションプラットフォーム。
- Zing tree - インタラクティブな意思決定ツリーとトラブルシューターを作成するためのツールキット。
- ZIVVER - 使い慣れたメールプログラムから安全なメールとファイル転送を可能にするツール。
- Zoho - ビジネスアプリケーションスイート。
- Zoom - 音声、ウェブコラボレーション、ビデオ会議機能を備えたコミュニケーションおよびコラボレーションソフトウェア。
- Zuora - 企業がサブスクリプションビジネスを開始、管理、変革できるようにするサブスクリプションベースのソフトウェア。

エンドツーエンドのアプリ構成

アプリの完全なエンドツーエンド構成については、簡単なオンボーディングとセットアップのための管理者ガイド付きワークフローを参照してください。

エンタープライズWebアプリへのエージェントレスアクセス

SharePoint、JIRA、Confluenceなどの、顧客がオンプレミスまたはパブリッククラウドでホストしているエンタープライズWebアプリケーションに、クライアントブラウザから直接アクセスでき

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

るようになりました。エンドユーザーは、ストアからエンタープライズWebアプリへのアクセスを開始する必要がなくなりました。この機能により、エンドユーザーは電子メール、コラボレーションツール、またはブラウザのブックマークからリンクをクリックしてWebアプリにアクセスすることもできます。これにより、顧客に真のゼロフットプリントソリューションが提供されます。

仕組み

- 構成済みのエンタープライズWebアプリ用に、新しいDNSレコードを追加するか、既存のDNSレコードを変更します。
- IT管理者は、構成済みのエンタープライズWebアプリのFQDNに対して新しいパブリックDNSレコードを追加するか、既存のパブリックDNSレコードを変更して、ユーザーをCitrix Secure Private Access™サービスにリダイレクトします。
- エンドユーザーが構成済みのエンタープライズWebアプリへのアクセスを開始すると、アプリのトラフィックはCitrix Secure Private Accessサービスに誘導され、その後、アプリへのアクセスをプロキシします。
- リクエストがCitrix Secure Private Accessサービスに到達すると、ユーザー認証とアプリケーション承認（コンテキストアクセスポリシーチェックを含む）を確認します。
- 検証が成功すると、Citrix Secure Private Accessサービスは、顧客の環境（オンプレミスまたはクラウドのいずれか）に展開されているCitrix Cloud Connector™アプライアンスと通信し、構成済みのエンタープライズWebアプリへのアクセスを有効にします。

エンタープライズWebアプリへのエージェントレスアクセス用にCitrix Secure Private Accessを構成する

前提条件:

開始する前に、アプリケーションを構成するために以下が必要です。

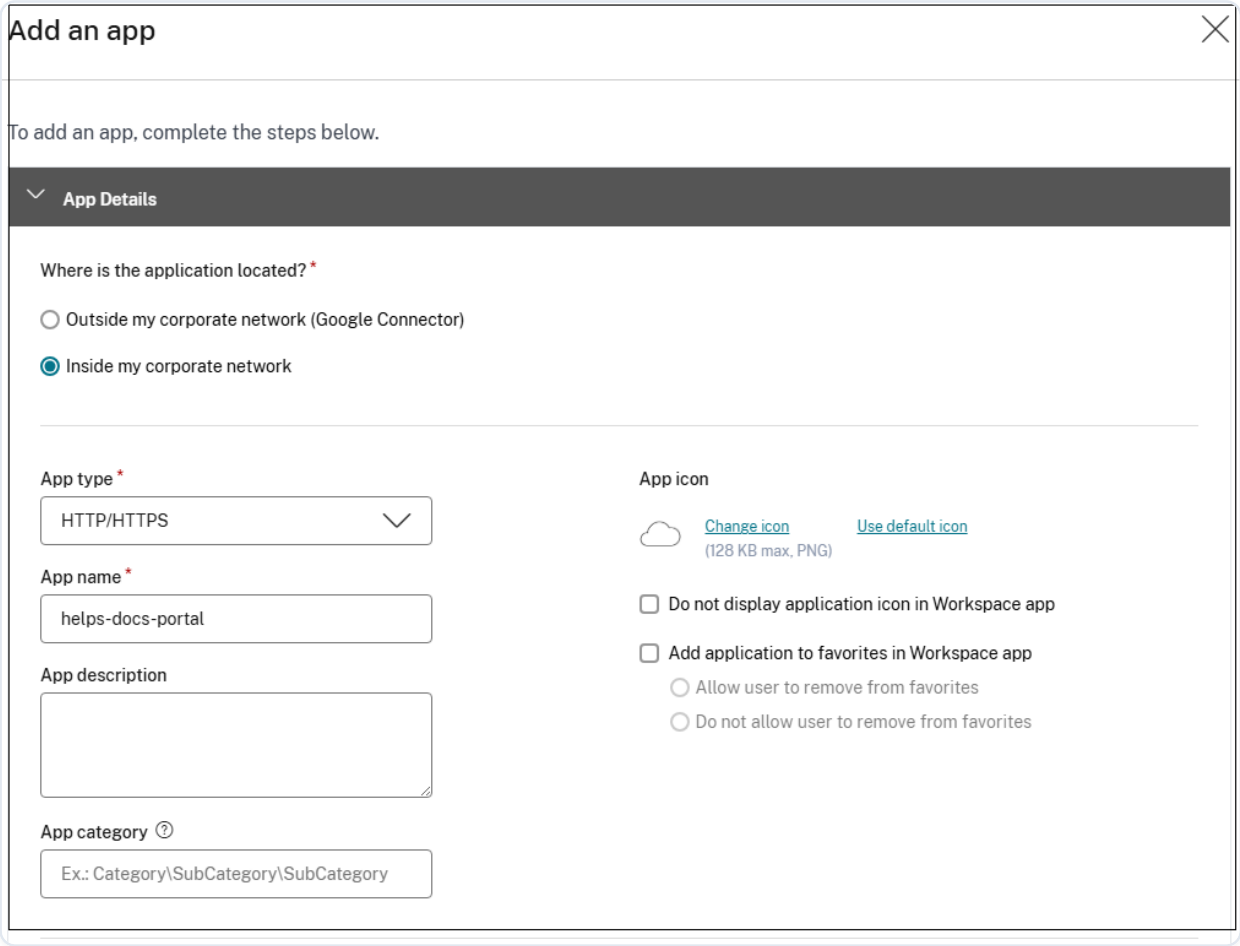
- アプリケーションFQDN
- SSL証明書 – 構成するアプリの公開証明書
- リソースの場所 – Citrix Cloud™ Connectorアプライアンスをインストールする
- アプリケーション構成中にCitrix®から提供される正規名（CNAME）で更新するためのパブリックDNSレコードへのアクセス。

エンタープライズWebアプリへのエージェントレスアクセスを構成する:

1. Citrix Cloudにログインし、**Secure Private Access**を選択します。
2. **Applications > App Configuration**をクリックし、**Add an app**をクリックします。

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

3. **Choose a template**セクションで、**Skip**をクリックします。テンプレートはSaaSアプリでのみ利用可能です。
4. **アプリケーションの場所はどこですか？**で、**社内ネットワーク内**を選択します。
   - 組織のプライベートネットワークインフラストラクチャ内にホストされ、ファイアウォールの背後にあり、内部ネットワーク接続を介してのみアクセス可能なアプリケーションの場合は、**Inside my corporate network**を選択します。
   - **Outside my corporate network (Google Connector):** 組織のプライベートネットワークインフラストラクチャの外部にホストされているアプリケーションの場合。トラフィックルーティングは、Google Cloud Connectorを介してユーザーから外部アプリケーションに直接行われます。
5. **App Details**セクションに以下の詳細を入力し、**Next**をクリックします。



- **App type** – アプリの種類（HTTPまたはHTTPS）を選択します。

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

> **注:**
>
> Chrome Enterprise Premium (CEP) では、HTTPSエンタープライズWebアプリとSaaSアプリのみがサポートされています。HTTPエンタープライズWebアプリとSaaSアプリはサポートされていません。

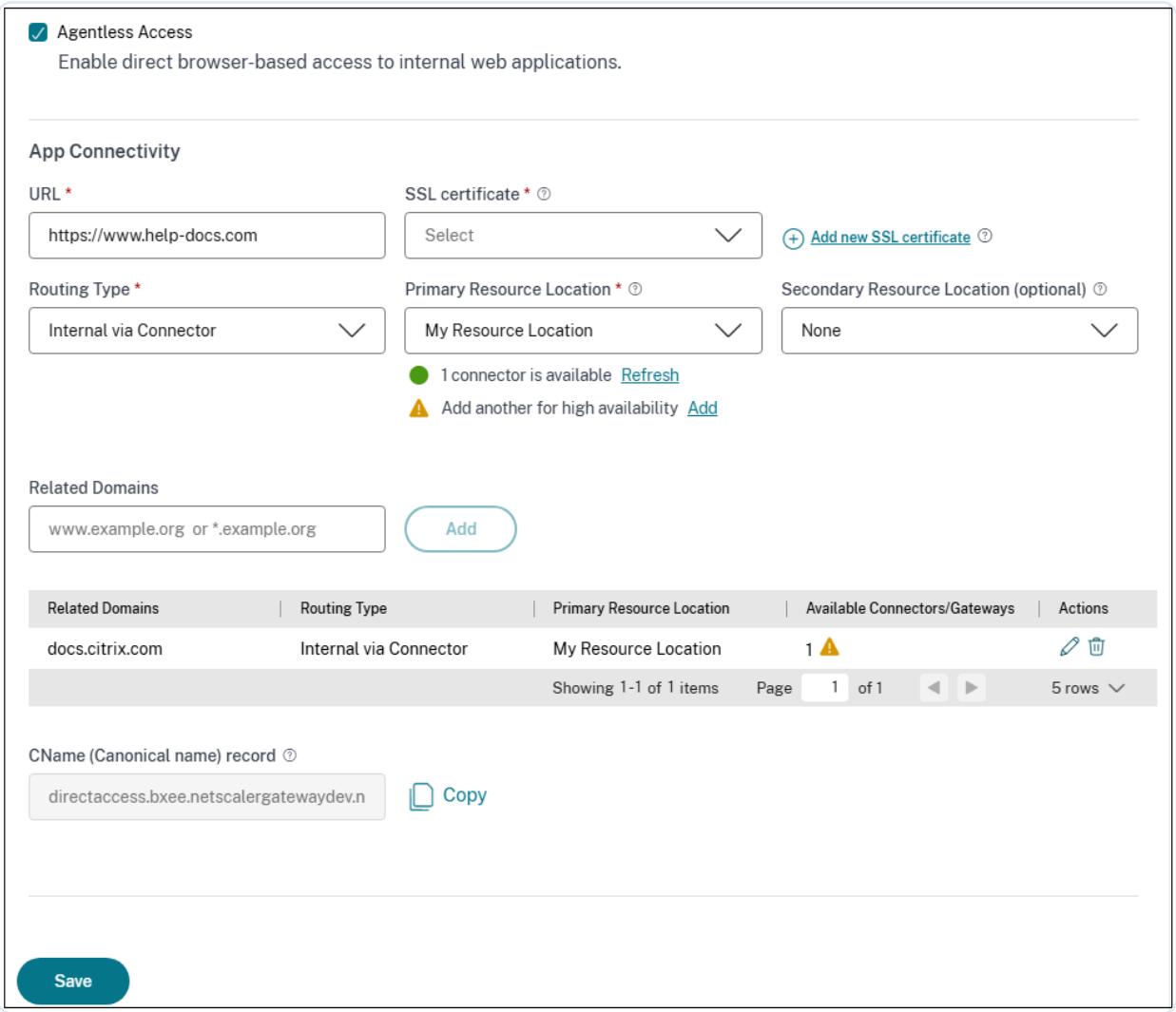
- **App name** – アプリケーションの名前。
- **App description** - アプリの簡単な説明。この説明はストアでユーザーに表示されます。
- **App icon** – アプリのアイコンを変更するには、**Change icon**をクリックします。アイコンファイルのサイズは128x128ピクセルである必要があります。アイコンを変更しない場合、デフォルトのアイコンが表示されます。

  アプリのアイコンを表示しない場合は、**ユーザーにアプリケーションアイコンを表示しない**を選択します。

6. ユーザーがクライアントブラウザから直接アプリにアクセスできるようにするには、**エージェントレスアクセス**を選択します。以下の詳細を入力します。

   エージェントレスアクセスオプションは、エンタープライズWebアプリでのみ利用可能です。

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



- **URL** – バックエンドアプリケーションのURL。URLはHTTPS形式である必要があり、対応するDNSエントリを管理者が追加する必要があります。
- **SSL証明書** – ドロップダウンメニューから既存のSSL証明書を選択するか、**新しいSSL証明書の追加**をクリックして新しいSSL証明書を追加します。
  - パブリックまたは信頼されたCA証明書のみがサポートされています。
  - 証明書の完全なチェーンをアップロードする必要があります。

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

重要:

- Secure Private Accessは独自の証明書ストアを管理しているため、管理者は証明書をSecure Private Accessコンソールに直接アップロードする必要があります。詳細については、「Secure Private Accessコンソールでの証明書の管理」を参照してください。
- NetScaler®コンソールに追加された証明書は、両システム間で同期されないため、Secure Private Accessでは使用できなくなります。

- **関連ドメイン** – 関連ドメインは、提供されたURLに基づいて自動的に入力されます。関連ドメインは、サービスがURLをアプリの一部として識別し、それに応じてトラフィックをルーティングするのに役立ちます。複数の関連ドメインを追加できます。各関連ドメインにSSL証明書をバインドできますが、これはオプションです。

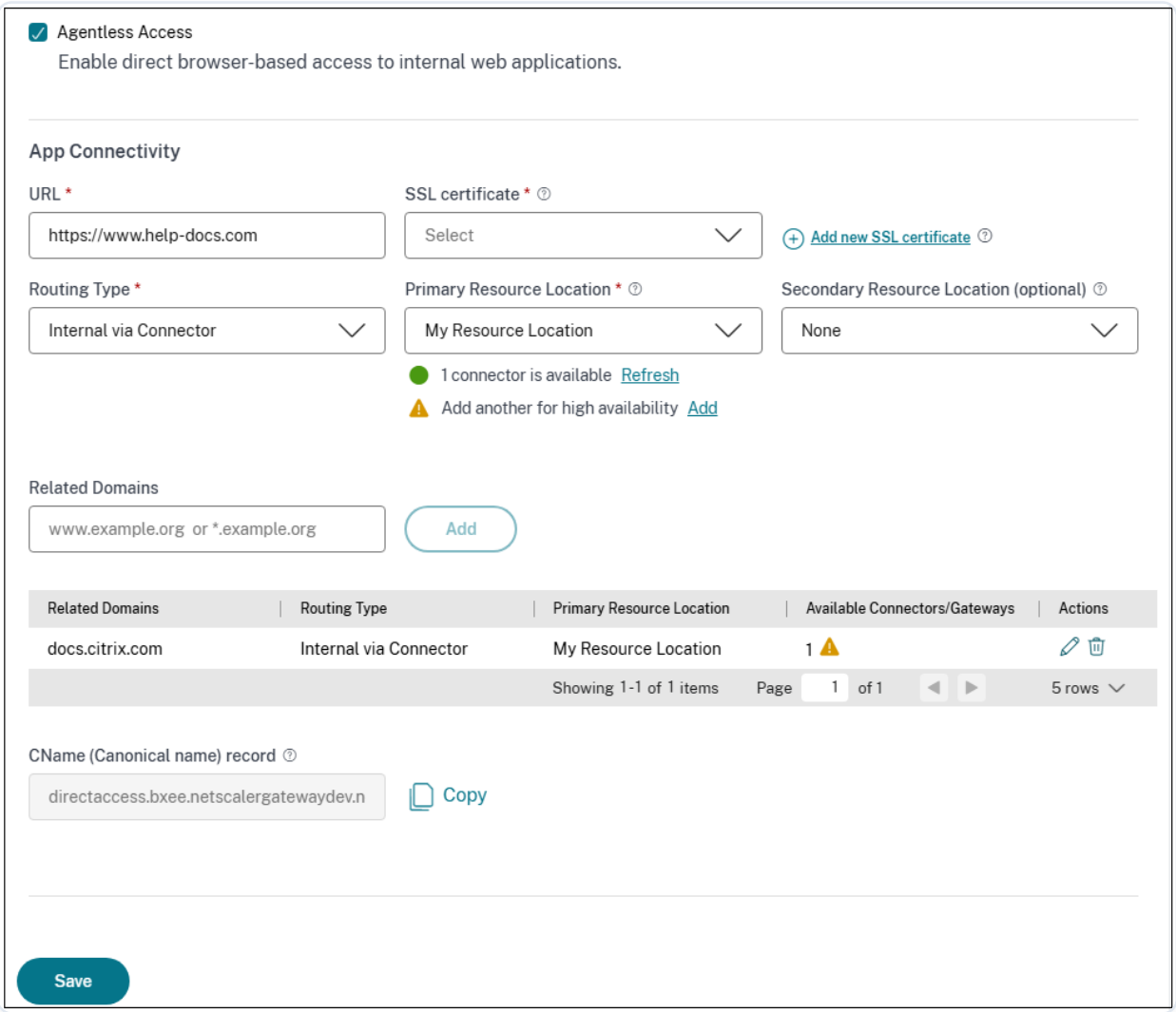
注:

重複する関連ドメインが追加された場合、または関連ドメインが別のアプリのURLとして追加された場合は、警告メッセージが表示されます。これらの問題を回避するには、「WebおよびSaaSアプリケーション構成のベストプラクティス」を参照してください。

- **HARのインポート** – HARファイルをアップロードして、アプリケーションがアクセスするドメインを自動的に検出できます。検出されたドメインを確認し、アプリケーションの関連ドメイン構成に追加するドメインを選択します。これにより、関連ドメインを手動で特定して構成する必要が減り、アプリケーションのオンボーディングが簡素化されます。詳細については、「HARファイルを使用した関連ドメインの検出」を参照してください。
- **CNameレコード** – Secure Private Accessによって自動生成されます。これは、アプリケーションへのエージェントレスアクセスを有効にするためにDNSに入力する必要がある値です。

7. 「**アプリ接続**」セクションでは、ドメインをCitrix Connector™ Applianceを介して外部または内部にルーティングする必要がある場合に、アプリケーションの関連ドメインのルーティングを定義します。

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



- **ルーティングの種類** - 次のいずれかを選択します。
  - **内部 – プロキシをバイパス** - ドメインのトラフィックはConnector Appliance™を介してルーティングされ、Connector Applianceで構成された顧客のWebプロキシをバイパスします。
  - **コネクタ経由の内部** - アプリは外部にある可能性がありますが、トラフィックはConnector Applianceを介して外部ネットワークに流れる必要があります。
  - **外部** – トラフィックはインターネットに直接流れます。
- **プライマリおよびセカンダリリソースロケーション** - 管理者は、セカンダリリソースロケーションを構成するか、「**最初に利用可能なもの**」オプションを使用することによって、中断が発生した場合でもアプリケーションの高可用性を確保できます。
  - **プライマリリソースロケーション:** アプリケーションがホストされているプライマリリソースロケーションを選択します。または、管理者は「**プライマリリソースロケーション**」で「**最初に利用可能なもの**」オプションを選択できます。

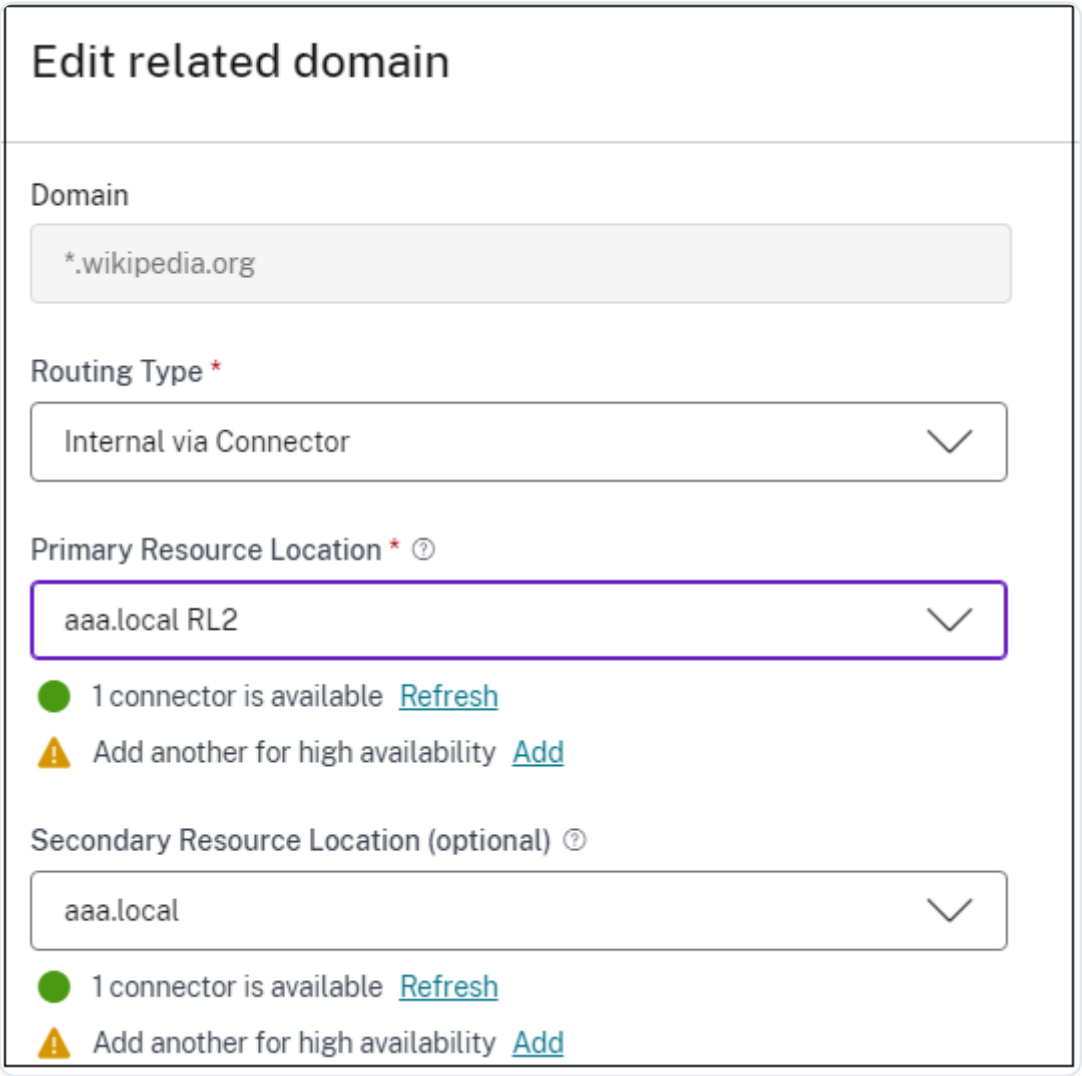
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **最初に利用可能なもの:** 「**最初に利用可能なもの**」オプションは、動作中のリソースロケーションが使用されることを保証します。「**最初に利用可能なもの**」が選択されている場合、システムはトラフィックを最初に利用可能なロケーションに自動的にルーティングします。これにより、手動介入なしで継続的なアプリケーションアクセスが保証されます。たとえば、ResourceLocation1が利用できないがResourceLocation2に到達可能な場合、ResourceLocation2がデフォルトで選択され、アプリケーションのフロントエンドとして機能します。
- **セカンダリリソースロケーション** - 「**セカンダリリソースロケーション**」オプションは、プライマリリソースロケーションが明示的に指定されている場合にのみ利用可能になります。Connector Applianceまたはデータセンターの障害などの理由でプライマリリソースロケーションが利用できなくなった場合、アプリケーションは指定されたセカンダリリソースロケーションにフェイルオーバーします。セカンダリリソースロケーションは、アプリケーションが別のデータセンターでホストされている場合でも、フェイルオーバーとして機能できます。

プライマリおよびセカンダリリソースロケーションを設定することも、関連する各ドメインに対して「**最初に利用可能なもの**」オプションを選択することもできます。

a. 関連ドメインテーブルの「**アクション**」列にある編集アイコンをクリックします。
b. プライマリおよびセカンダリリソースロケーションを設定するか、「**最初に利用可能なもの**」オプションを選択します。

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

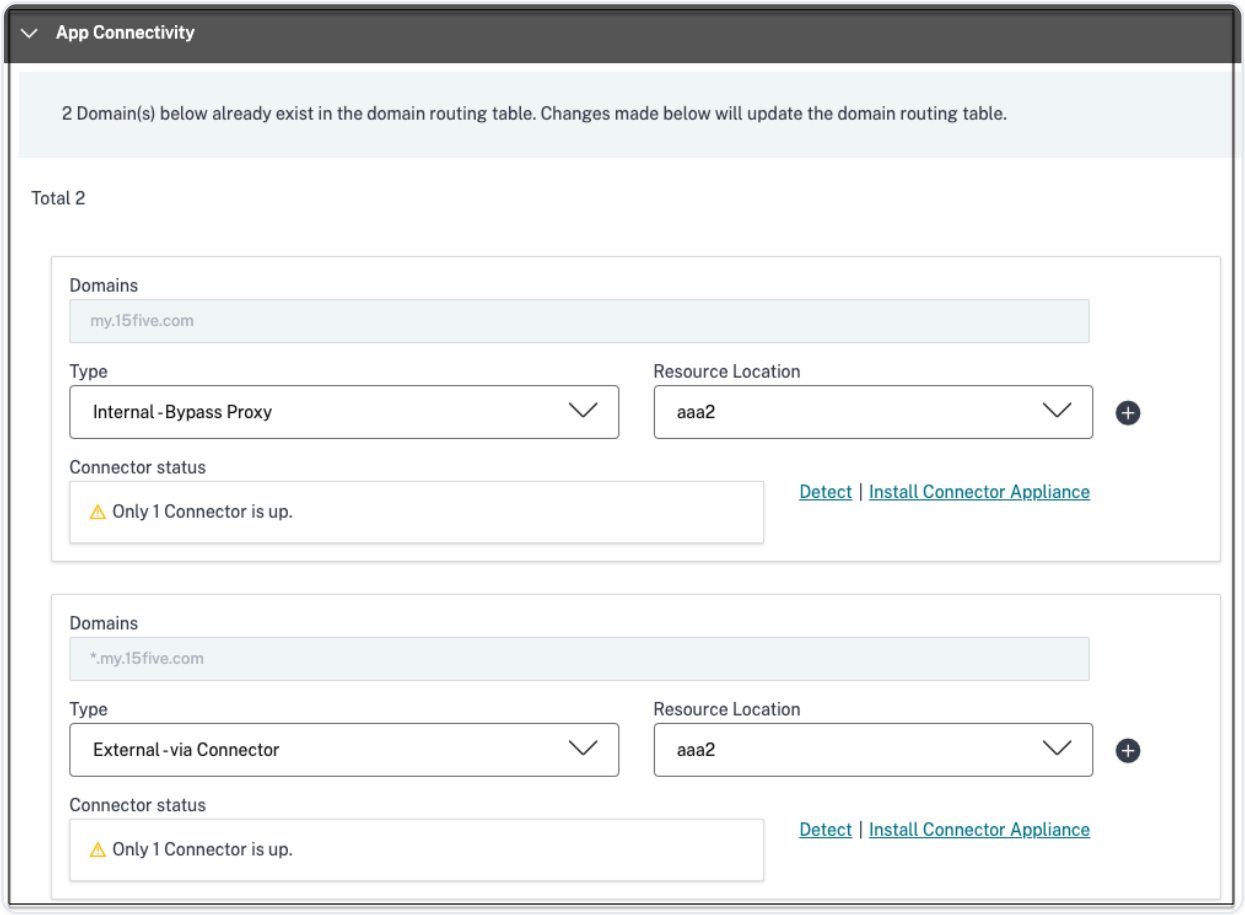


注記:

- バックアップリソースの場所を設定し、「**First Available**」オプション機能を使用することはプレビュー版です。
- アプリケーションを削除すると、そのルーティングエントリは自動的に削除されます。詳細については、アプリケーション削除時のルーティングエントリの自動クリーンアップを参照してください。

8. 「**App Connectivity**」セクションで、ドメインをCitrix Connector™ Applianceを介して外部または内部にルーティングする必要がある場合に、アプリケーションの関連ドメインのルーティングを定義します。

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



9. **一貫した接続を維持** - このチェックボックスをオンにして、同じコネクタアプライアンスへの一貫した接続を有効にします。一貫した接続の詳細については、一貫した接続を維持を参照してください。

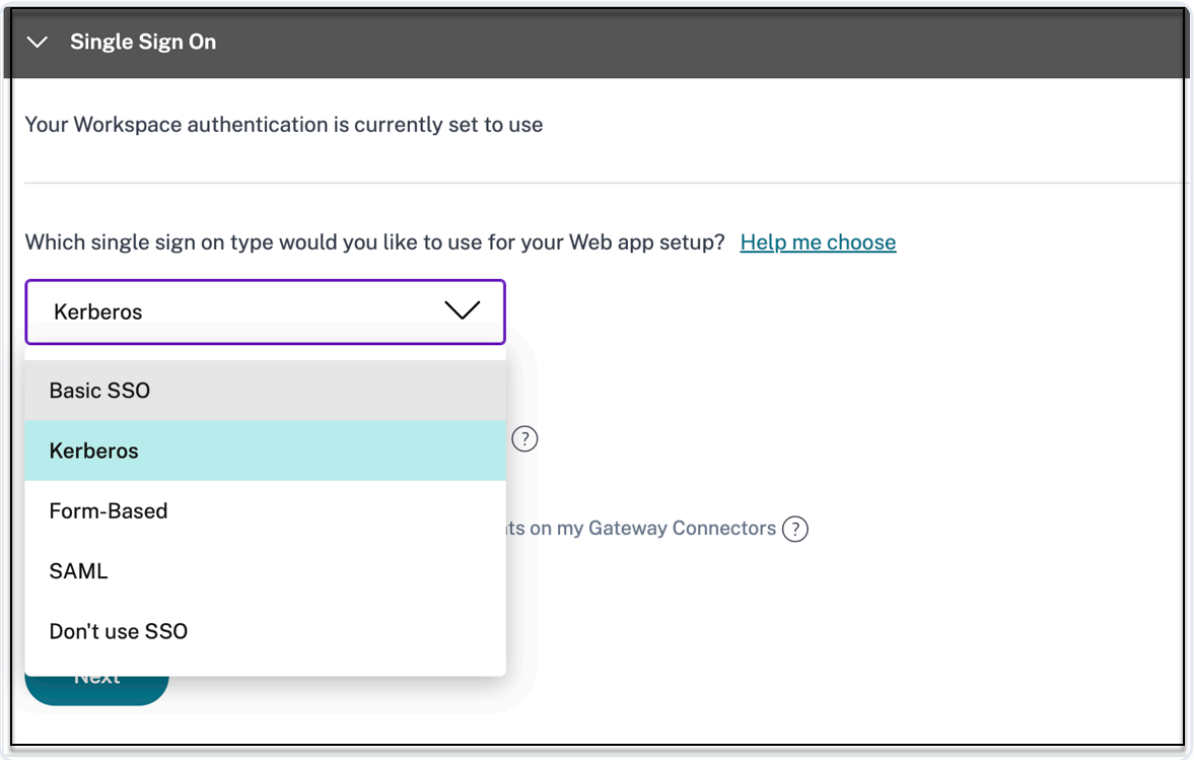
> **注記:**
>
> 「**一貫した接続を維持**」オプションが選択されている場合、アプリケーションのルーティングタイプは「App Connectivity」セクションで「**Internal via Connector**」に設定する必要があります。

10. 優先するサインオン方法を設定します。

> **注記:**
>
> シングルサインオンオプションは、Chrome Enterprise (CEP) を使用するCitrix Secure Accessには適用されません。

a. 「**Single Sign On**」セクションで、アプリケーションに使用する優先シングルサインオンタイプを選択し、「**保存**」をクリックします。次のシングルサインオンタイプが利用可能です。

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

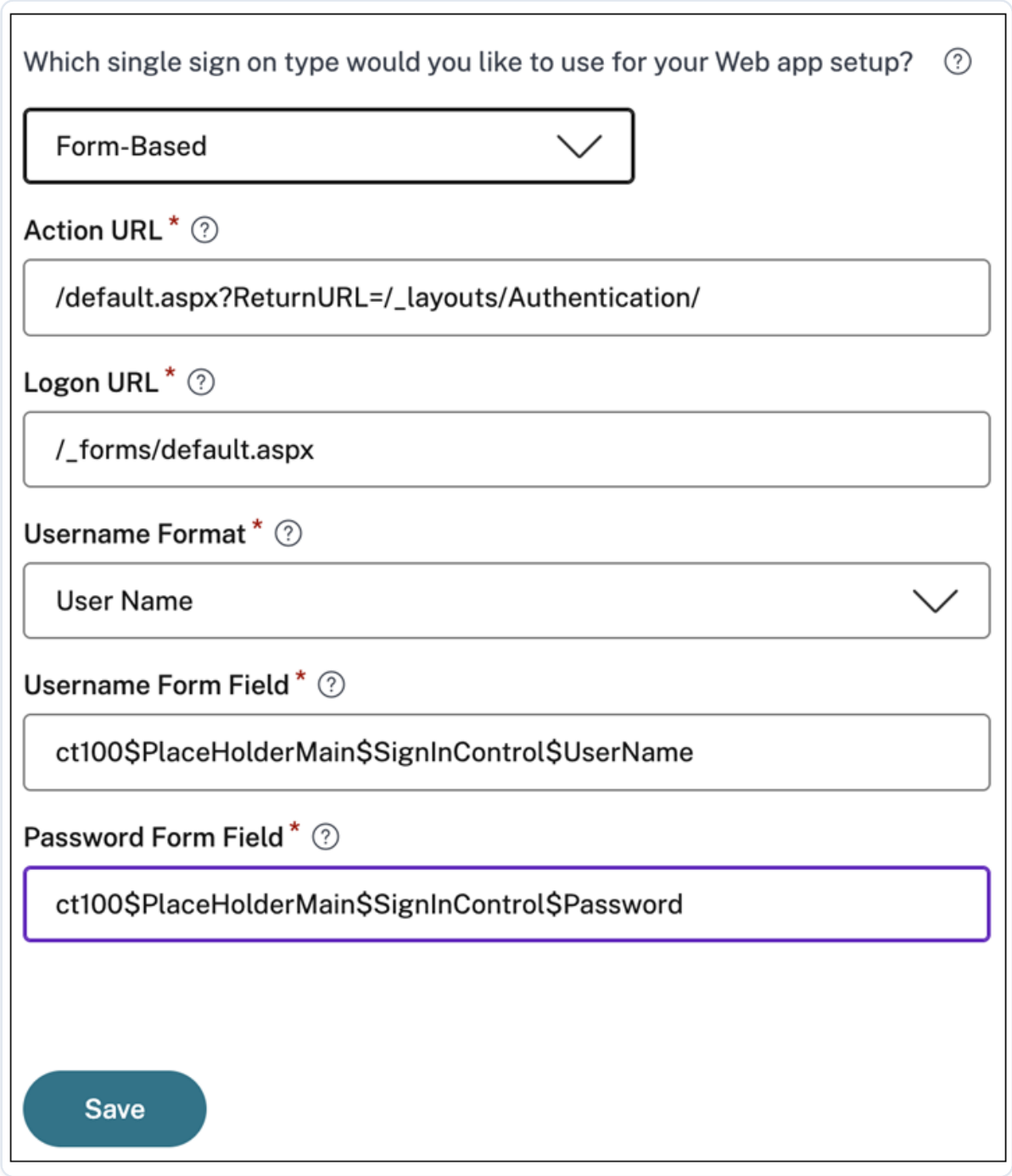


- **Basic** – バックエンドサーバーがbasic-401チャレンジを提示する場合、「**Basic SSO**」を選択します。「**Basic**」SSOタイプには、構成の詳細を指定する必要はありません。
- **Kerberos** – バックエンドサーバーがnegotiate-401チャレンジを提示する場合、「**Kerberos**」を選択します。「**Kerberos**」SSOタイプには、構成の詳細を指定する必要はありません。
- **フォームベース** – バックエンドサーバーが認証のためにHTMLフォームを提示する場合、「**フォームベース**」を選択します。「**フォームベース**」SSOタイプの構成詳細を入力します。
- **SAML** - ウェブアプリケーションへのSAMLベースのSSOには「**SAML**」を選択します。「**SAML**」SSOタイプの構成詳細を入力します。
- **SSOを使用しない** – バックエンドサーバーでユーザーを認証する必要がない場合は、「**SSOを使用しない**」オプションを使用します。「**SSOを使用しない**」オプションが選択されている場合、ユーザーは「**アプリの詳細**」セクションで構成されたURLにリダイレクトされます。

フォームベースの詳細:

シングルサインオンセクションに以下のフォームベースの構成詳細を入力し、「**保存**」をクリックします。

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



- **アクションURL** - 完成したフォームが送信されるURLを入力します。
- **ログオンフォームURL** – ログオンフォームが表示されるURLを入力します。
- **ユーザー名形式** - ユーザー名の形式を選択します。
- **ユーザー名フォームフィールド** – ユーザー名属性を入力します。
- **パスワードフォームフィールド** – パスワード属性を入力します。

SAML:

サインオンセクションに以下の詳細を入力し、「保存.**」をクリックします。

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

Which single sign on type would you like to use for your Web app setup?

SAML

SAML information

This form generates the XML needed for the application's SAML request.

Sign Assertion *

Assertion

Assertion URL *

https://sharepoint.onelogin/saml_assertion

Relay State

&RelayState = /apex/SSO_Redirect?param1=value1

Audience

Name ID Format *

Email Address

Name ID *

User Name

Launch the app using the specified URL (SP initiated)

- **アサーションの署名** - アサーションまたは応答に署名することで、応答またはアサーションが依拠当事者 (SP) に配信される際のメッセージの整合性が保証されます。**アサーション、応答、両方、** または **なし** を選択できます。
- **アサーションURL** – アプリケーションベンダーによって提供されます。SAMLアサーションはこのURLに送信されます。
- **リレーステート** – リレーステートパラメータは、ユーザーがサインインして依拠当事者のフェデレーションサーバーにリダイレクトされた後、アクセスする特定のリソース

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

を識別するために使用されます。リレーステートは、ユーザー向けに単一のURLを生成します。ユーザーはこのURLをクリックして、ターゲットアプリケーションにログオンできます。

- **オーディエンス** – アプリケーションベンダーによって提供されます。この値は、SAMLアサーションが正しいアプリケーションに対して生成されたことを確認します。
- **名前ID形式** – サポートされている名前識別子形式を選択します。
- **名前ID** – サポートされている名前IDを選択します。

i. **詳細属性 (オプション)** で、アクセス制御の決定のためにアプリケーションに送信されるユーザーに関する追加情報を追加します。

ii. **SAMLメタデータ** の下のリンクをクリックして、メタデータファイルをダウンロードします。ダウンロードしたメタデータファイルを使用して、SaaSアプリサーバーでSSOを構成します。

- **ログインURL** の下のSSOログインURLをコピーし、SaaSアプリサーバーでSSOを構成する際にこのURLを使用できます。
- **証明書** リストから証明書をダウンロードし、SaaSアプリサーバーでSSOを構成する際にその証明書を使用することもできます。

11. **保存** をクリックし、次に **完了** をクリックします。アプリが ページに追加されます。アプリケーションを構成した後、 ページからアプリを編集または削除できます。そのためには、アプリの省略記号ボタンをクリックし、それに応じてアクションを選択します。

- **アプリケーションの編集**
- **削除**

重要:

- アプリへのゼロトラストベースのアクセスを有効にするには、デフォルトでアプリへのアクセスが拒否されます。アプリへのアクセスは、アクセスポリシーがアプリケーションに関連付けられている場合にのみ有効になります。アクセスポリシーの作成の詳細については、「アクセスポリシーの作成」を参照してください。
- 複数のアプリが同じFQDNまたはワイルドカードFQDNのいくつかのバリエーションで構成されている場合、競合する構成になる可能性があります。競合する構成を防ぐには、「WebおよびSaaSアプリケーション構成のベストプラクティス」を参照してください。

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

アプリケーション削除時のルーティングエントリの自動クリーンアップ

アプリケーションを構成すると、その宛先 (FQDN またはアプリケーションドメイン) がルーティングテーブルに追加され、Secure Private Access はルーティングの決定にこれを使用します。アプリケーションを削除すると、Secure Private Access は次のルールに基づいてルーティングエントリをクリーンアップします。

- **参照されていないエントリは削除されます** - 削除されたアプリケーションに関連付けられているルーティングエントリ (FQDN またはアプリケーションドメイン) が他のアプリケーションによって参照されていない場合、Secure Private Access はルーティングテーブルから自動的に削除します。
- **共有エントリは保持されます** - ルーティングエントリが複数のアプリケーションで使用されている場合、それらのアプリケーションのいずれかを削除しても、共有エントリは削除されません。エントリは、少なくとも1つのアクティブなアプリケーションがそれを参照している限り、ルーティングテーブルに残ります。
- **遡及的な削除はありません** - ルーティングエントリは、アプリケーションの削除の一部としてのみ評価および削除されます。既存のエントリは、どのアプリケーションによっても使用されていないことが確認されない限り、遡及的に削除されることはありません。

注:

- アプリケーションが ページから削除されると (省略記号 (...) メニューを使用して)、クリーンアップは自動的に実行されます。管理者の操作は必要ありません。
- 共有ルーティングエントリは保持されるため、アプリケーションを削除しても、同じ宛先を共有する他のアプリケーションへのアクセスが中断されることはありません。

エージェントレスアクセスアプリとDevice Postureサービス

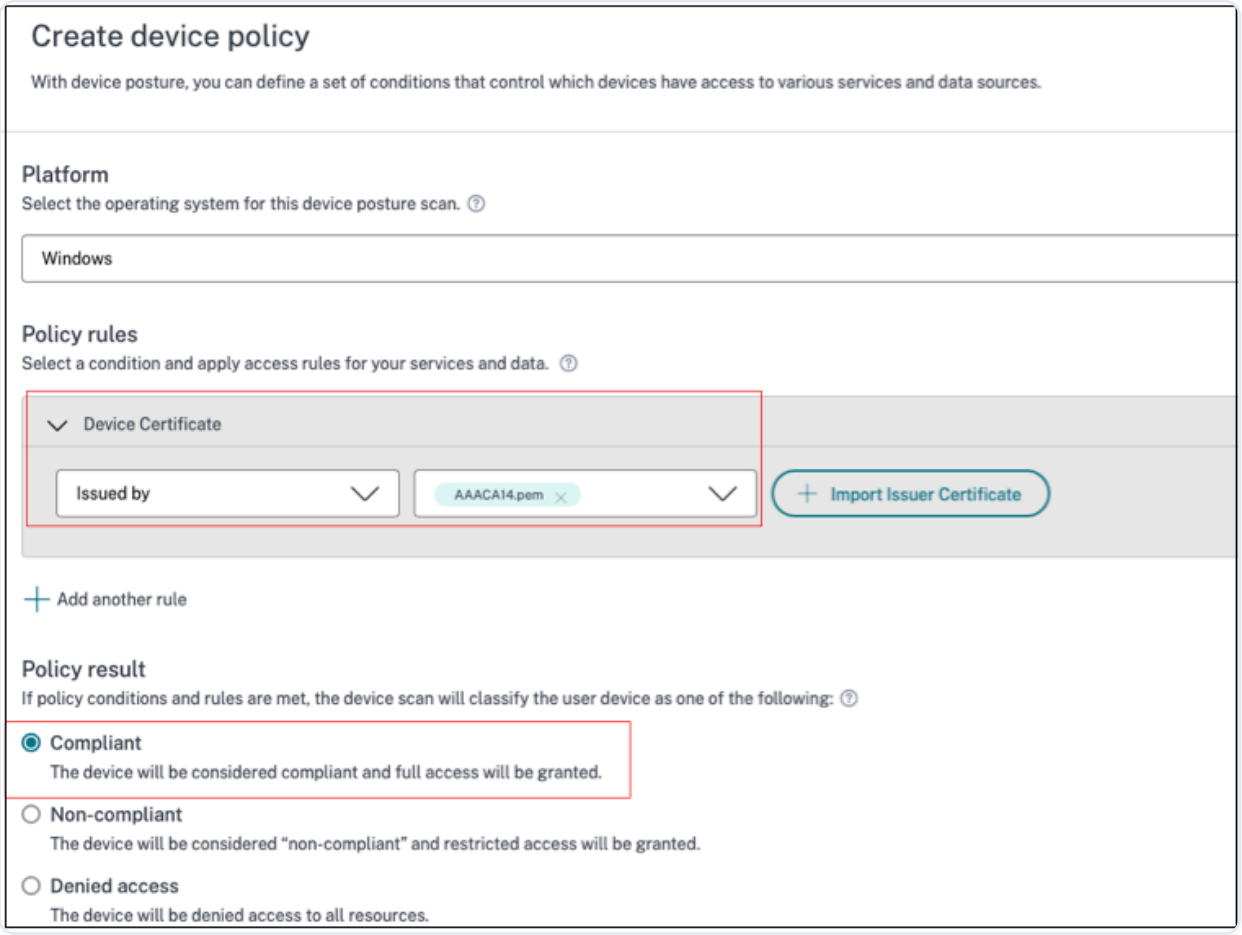
エージェントレスアクセスアプリとDevice Postureサービスを組み合わせたCitrix Secure Private Accessは、準拠デバイスのみがエージェントレスアクセスを介して機密アプリケーションにアクセスできるようにします。管理者は、Device Postureサービスのスキャン結果に基づいて、非準拠または非管理デバイスへのアクセスをブロックできます。

準拠デバイスのみにエージェントレスアクセスを有効にする手順

準拠デバイスのみにエージェントレスアクセスを有効にするには、管理者は次の手順を実行する必要があります。

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

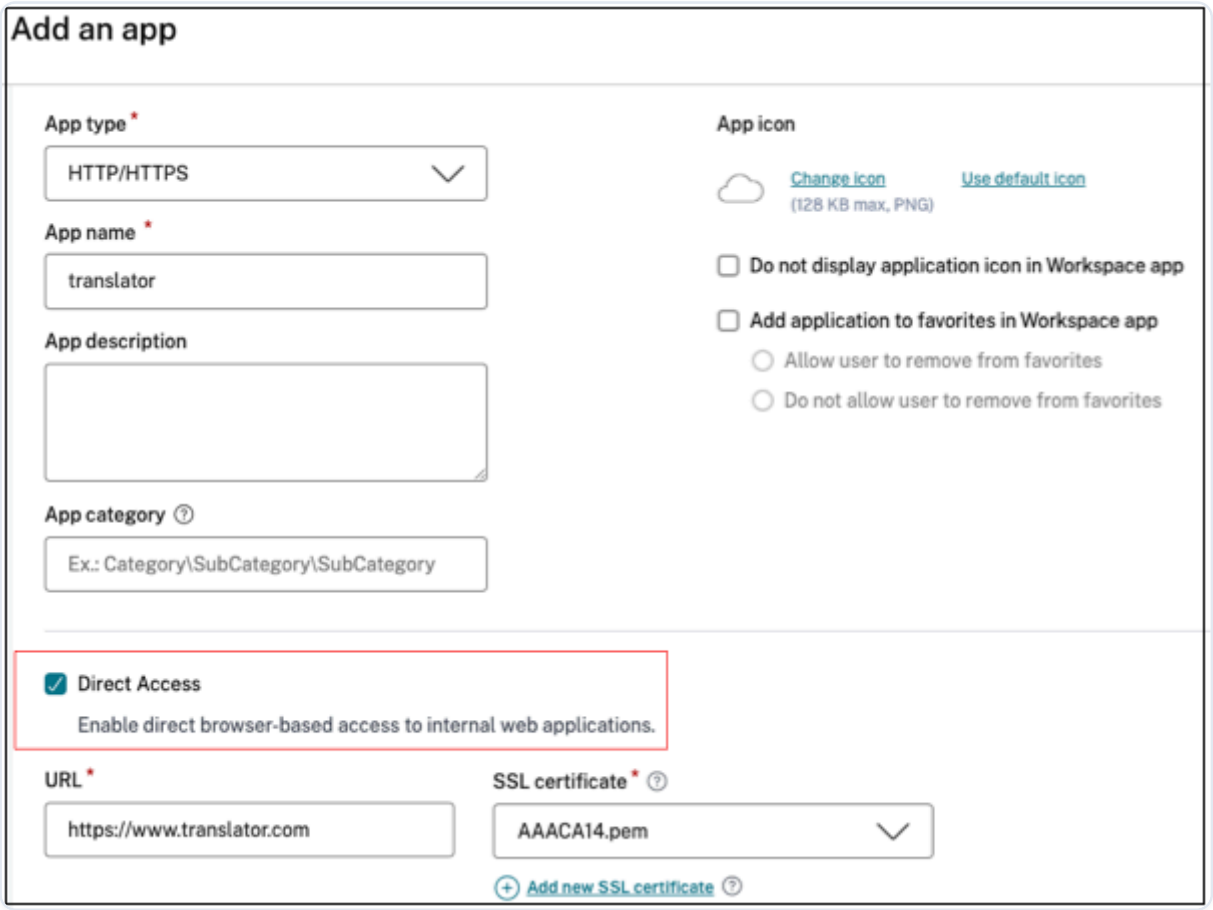
1. Device Postureサービス管理コンソールから、デバイス証明書、ウイルス対策、ブラウザなどのデバイスポスチャスキャン条件を確認するためのデバイスポスチャポリシーを作成し、ポリシー結果アクションとして**準拠**を選択します。詳細については、「デバイスポスチャの構成」を参照してください。



2. Secure Private Access管理コンソールから、次の操作を実行します。

   - エージェントレスアクセスを有効にするアプリケーションを作成します。詳細については、「エンタープライズWebアプリへの直接アクセス」を参照してください。

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

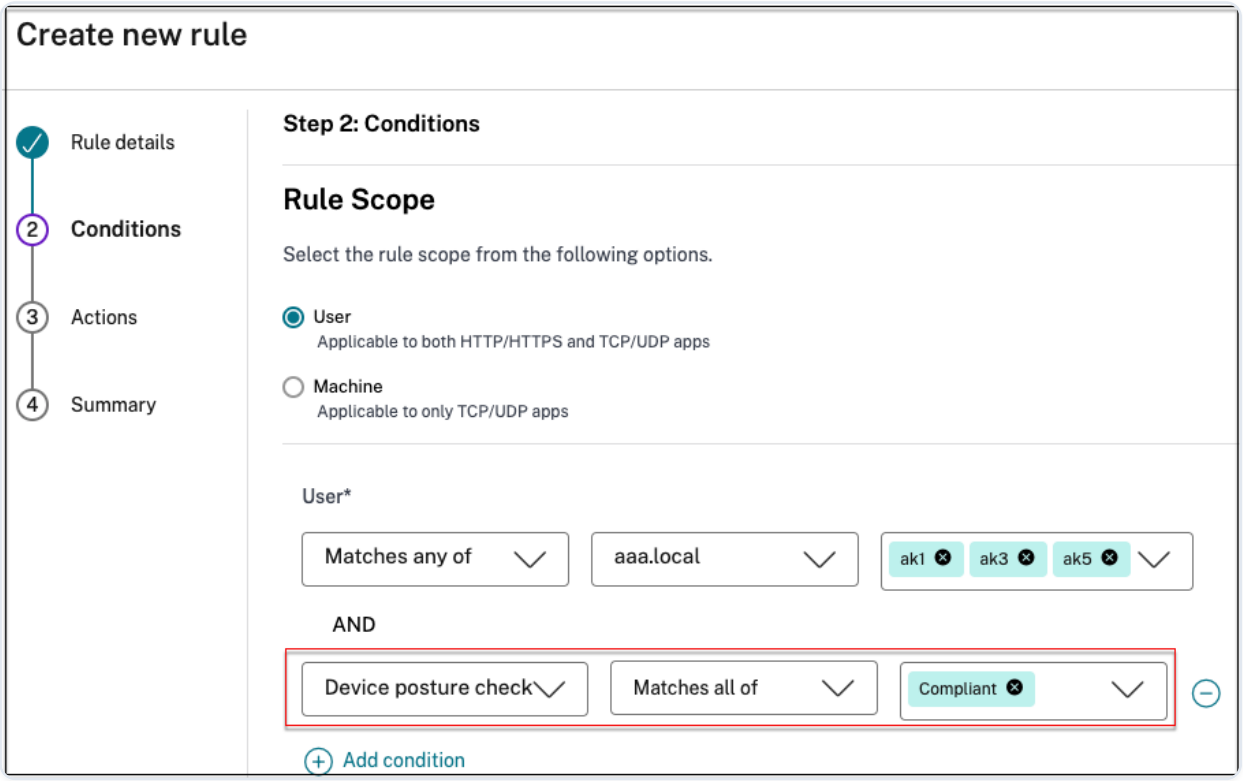


- Secure Private Accessをデバイスポスチャで構成します。**ルールスコープ**で、**デバイスポスチャチェック > 次のいずれかに一致**を選択し、タグ**Compliant**を入力します。このタグはデバイスポスチャサービスから送信されます。

注：

タグは、以前にキャプチャしたとおり、先頭を大文字にして（Compliant）正確に入力する必要があります。そうしないと、デバイスポスチャポリシーは意図したとおりに機能しません。詳細については、「Citrix Secure Private Accessとデバイスポスチャの構成」を参照してください。

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



この構成が実行されると、デバイスポスチャスキャン結果に基づいて、デバイスは準拠、非準拠、またはログイン拒否としてタグ付けされ、それに応じてアプリへのアクセスが有効になります。

例：

エンドポイントデバイス上のデバイス証明書の存在を確認し、そのログインステータスを判断するデバイスポスチャポリシーを作成したとします。デバイスポスチャポリシーが設定され、デバイスポスチャが有効になると、エンドユーザーがストアにログインしたときに次のアクションが発生します。

1. デバイスポスチャスキャンは、エンドポイントデバイスにデバイス証明書が存在するかどうかを確認します。
   - デバイスにデバイス証明書が存在する場合、デバイスは**準拠**としてタグ付けされます。
   - デバイスにデバイス証明書が存在しない場合、デバイスは**非準拠**としてタグ付けされます。
2. この情報はその後、タグとしてCitrix Secure Private Accessサービスに渡されます。
3. アクセスポリシーは、デバイスの分類に基づいて評価されます。
   - デバイスが準拠している場合、アプリへのエージェントレスアクセスが許可されます。
   - デバイスが準拠していない場合、アプリのエージェントレスアクセスは無効になります。

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

エンドユーザーエクスペリエンス

エンドユーザーエクスペリエンスは、デバイスが準拠しているか準拠していないかの分類に基づいています。

- **準拠デバイス:**

  ユーザーは、ストアまたはブラウザからアプリのURLを使用してエージェントレスアクセスアプリを起動できます。

- **非準拠デバイス:**

  - アプリはストアに列挙されません。
  - ユーザーは、ブラウザからアプリのURLを使用してアプリを起動できません。
  - アクセスブロックページがユーザーに表示されます。

TCP/UDPアプリのサポート

Secure Private Accessサービスを使用すると、マシン上で実行されているCitrix Secure Accessクライアントを介して、ネイティブブラウザまたはネイティブクライアントアプリケーションのいずれかを使用して、オンプレミス環境にあるTCP/UDPアプリケーションにアクセスできます。詳細については、以下のセクションを参照してください。

- 前提条件
- TCP/UDPアプリのSecure Private Accessを構成する
- 管理者構成 – Citrix Secure Accessクライアントベースの HTTP/HTTPSアプリへのアクセス
- TCP/UDPおよびHTTP(S)アプリへのアダプティブアクセス
- アプリケーションドメインのIPアドレス競合のトラブルシューティング

前提条件

- Citrix Secure Accessクライアント - 詳細については、Citrix Secure Accessクライアントを参照してください。
- Connector Appliance – Citrixでは、リソースの場所に高可用性セットアップで2つのConnector Applianceをインストールすることをお勧めします。コネクタは、オンプレミス、データセンターのハイパーバイザー、またはパブリッククラウドのいずれかにインストールできます。Connector Applianceとそのインストールについて詳しくは、Connector Appliance for Cloud Servicesを参照してください。TCP/UDPアプリにはConnector Applianceを使用する必要があります。Connector Applianceには、DNS解決のためのDNSサーバー構成が必要です。

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

TCP/UDPアプリのSecure Private Accessを構成する

1. Citrix Cloudにログインし、**Secure Private Access**を選択します。
2. **Applications > App Configuration**をクリックし、**Add an app**をクリックします。
3. **テンプレートの選択**セクションで、**スキップ**をクリックします。テンプレートはSaaSアプリでのみ利用できます。

   アプリは、宛先の論理的なグループ化です。複数の宛先に対して1つのアプリを作成できます。各宛先は、バックエンドの異なるサーバーを意味します。たとえば、1つのアプリに1つのSSH、1つのRDP、1つのデータベースサーバー、および1つのWebサーバーを含めることができます。宛先ごとに1つのアプリを作成する必要はありませんが、1つのアプリに多くの宛先を含めることができます。
4. 「**アプリの詳細**」セクションで、「**社内ネットワーク内**」を選択し、以下の詳細を入力して「**次へ**」をクリックします。

   TCPアプリの詳細(/en-us/citrix-secure-private-access/media/spa-tcp-app-details1.png)

   - **アプリの種類** – TCP/UDPを選択します。
   - **アプリ名** – アプリケーションの名前。
   - **アプリのアイコン** – アプリのアイコンが表示されます。このフィールドはオプションです。
   - **アプリの説明** – 追加するアプリの説明。このフィールドはオプションです。
   - **宛先** – リソースロケーションにあるバックエンドマシンのIPアドレスまたはFQDN。1つ以上の宛先を次のように指定できます。
     - **IPアドレス v4**
     - **IPアドレス範囲** – 例: 10.68.90.10-10.68.90.99
     - **CIDR** – 例: 10.106.90.0/24
     - **マシンのFQDNまたはドメイン名** – 単一またはワイルドカードドメイン。例: ex.destination.domain.com, *.domain.com

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

重要:

管理者がIPアドレスを使用してアプリを設定した場合でも、エンドユーザーはFQDNを使用してアプリにアクセスできます。これは、Citrix Secure Access™クライアントがFQDNを実際のIPアドレスに解決できるためです。 以下の表は、さまざまな宛先の例と、これらの宛先でアプリにアクセスする方法を示しています。

宛先入力	アプリへのアクセス方法
10.10.10.1-10.10.10.100	エンドユーザーは、この範囲のIPアドレスを介してのみアプリにアクセスすることが想定されています。
10.10.10.0/24	エンドユーザーは、IP CIDRで構成されたIPアドレスを介してのみアプリにアクセスすることが想定されています。
10.10.10.101	エンドユーザーは、10.10.10.101を介してのみアプリにアクセスすることが想定されています。
`*.info.citrix.com`	エンドユーザーは、`info.citrix.com` のサブドメインと `info.citrix.com` (親ドメイン) の両方にアクセスすることが想定されています。例えば、`info.citrix.com`, `sub1.info.citrix.com`, `level1.sub1.info.citrix.com` **注:** ワイルドカードは常にドメインの先頭文字である必要があり、*. は1つのみ許可されます。
info.citrix.com	エンドユーザーは `info.citrix.com` のみにアクセスすることが想定されており、サブドメインにはアクセスできません。例えば、`sub1.info.citrix.com` はアクセスできません。

- **ポート** – アプリが実行されているポート。管理者は、宛先ごとに複数のポートまたはポート範囲を構成できます。

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

次の表は、宛先に構成できるポートの例を示しています。

ポート入力	説明
*	デフォルトでは、ポートフィールドは `“*”` (任意のポート) に設定されています。宛先には1から65535までのポート番号がサポートされています。
1300–2400	宛先には1300から2400までのポート番号がサポートされています。
38389	宛先にはポート番号38389のみがサポートされています。
22,345,5678	宛先にはポート22、345、5678がサポートされています。
1300–2400, 42000-43000,22,443	宛先には、ポート番号の範囲1300～2400、42000～43000、およびポート22と443がサポートされています。

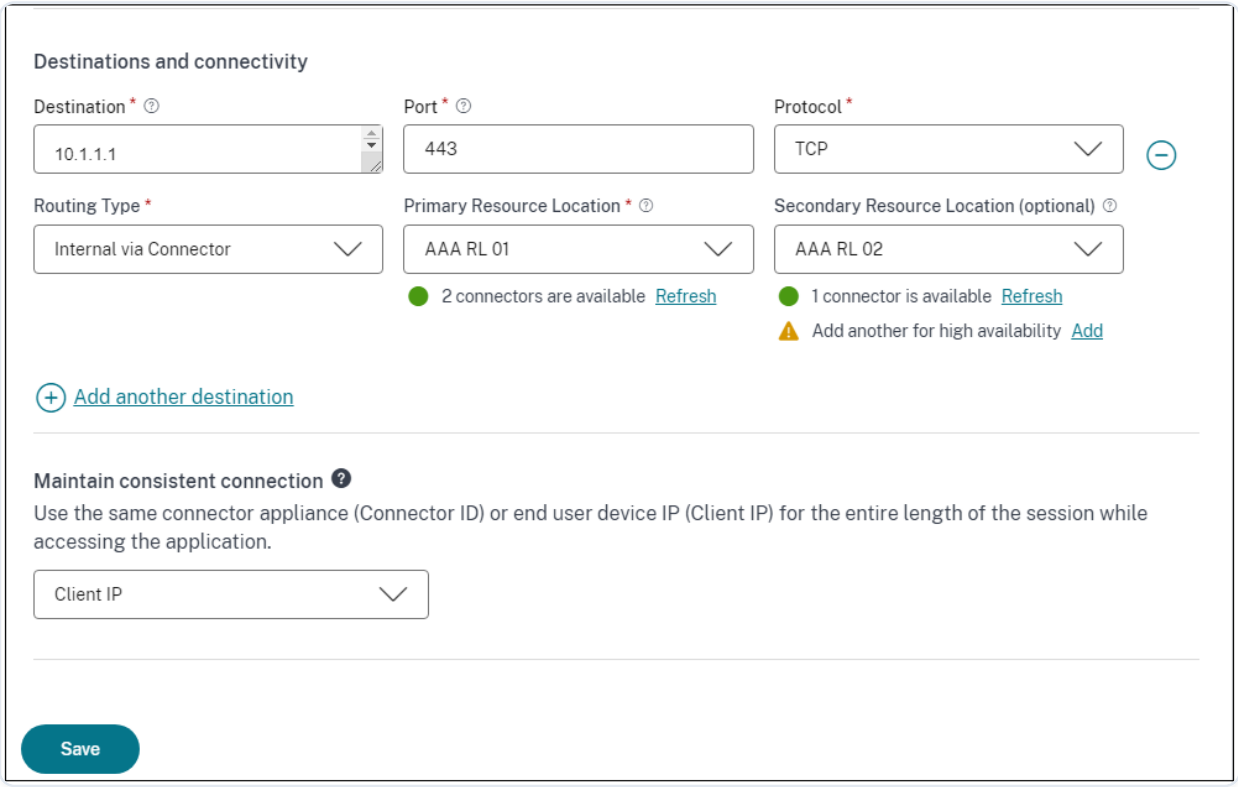
注:

ワイルドカードポート (*) は、ポート番号または範囲と共存できません。

- **プロトコル** – TCP/UDP

5. **アプリ接続**セクションでは、ドメインをCitrix Connector™ Applianceを介して外部または内部にルーティングする必要がある場合に、アプリケーションのルーティングを定義します。

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



- **ルーティングタイプ** - 次のいずれかを選択します。
  - **コネクタ経由の内部** - アプリは外部にある場合がありますが、トラフィックはコネクタアプライアンスを介して外部ネットワークに流れる必要があります。
  - **外部** – トラフィックはインターネットに直接流れます。
- **プライマリおよびセカンダリリソースロケーション** - 管理者は、セカンダリリソースロケーションを構成するか、**First Available** オプションを使用することで、障害発生時でもアプリケーションの高可用性を確保できます。
  - **プライマリリソースロケーション:** アプリケーションがホストされているプライマリリソースロケーションを選択します。または、管理者は**プライマリリソースロケーション**で**First Available**オプションを選択できます。
  - **First available: First Available**オプションは、動作中のリソースロケーションが使用されることを保証します。**First Available**が選択されている場合、システムはトラフィックを自動的に最初に利用可能なロケーションにルーティングします。これにより、手動介入なしで継続的なアプリケーションアクセスが保証されます。たとえば、ResourceLocation1が利用できないがResourceLocation2に到達可能な場合、ResourceLocation2がデフォルトでアプリケーションのフロントエンドとして選択されます。
  - **セカンダリリソースロケーション** - **セカンダリリソースロケーション**オプションは、プライマリリソースロケーションが明示的に指定されている場合にのみ利用可能になりま

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

す。コネクタアプライアンスやデータセンターの障害などの理由でプライマリリソースロケーションが利用できなくなった場合、アプリケーションは指定されたセカンダリリソースロケーションにフェールオーバーします。セカンダリリソースロケーションは、アプリケーションが別のデータセンターでホストされている場合でも、フェールオーバーとして機能できます。

関連する各ドメインに対して、プライマリおよびセカンダリリソースロケーションを設定するか、**First Available**オプションを選択することもできます。

a. 関連ドメインテーブルの**Actions**列にある編集アイコンをクリックします。
b. プライマリおよびセカンダリリソースロケーションを設定するか、**First Available**オプションを選択します。

関連ドメイン(/en-us/citrix-secure-private-access/media/backup-rl-related-domains.png)

> **注:**
>
> バックアップリソースロケーションの設定と**First Available**オプション機能の使用は、現在プレビュー段階です。

- **一貫した接続を維持** - TCP/UDPアプリに対してコネクタスティッキネスまたはクライアントIPスティッキネスを有効にできます。**一貫した接続を維持**チェックボックスを選択し、以下のオプションを選択します。
  - **使用しない:** アプリケーションは永続性を必要としません。アプリケーションは任意の送信元IPアドレスで動作できます。
  - **クライアントIP:** アプリケーションは、各接続でクライアントに対して同じ送信元IPアドレスを使用します。
  - **コネクタID:** アプリケーションは、セッションごとに同じコネクタアプライアンスに接続します。次のいずれかのオプションを選択します。

一貫した接続の詳細については、「一貫した接続の維持」を参照してください。

6. **保存**をクリックし、**完了**をクリックします。

アプリは**アプリケーション**ページに追加されます。アプリケーションを設定した後、**アプリケーション**ページからアプリを編集または削除できます。そのためには、アプリの省略記号ボタンをクリックし、それに応じてアクションを選択します。

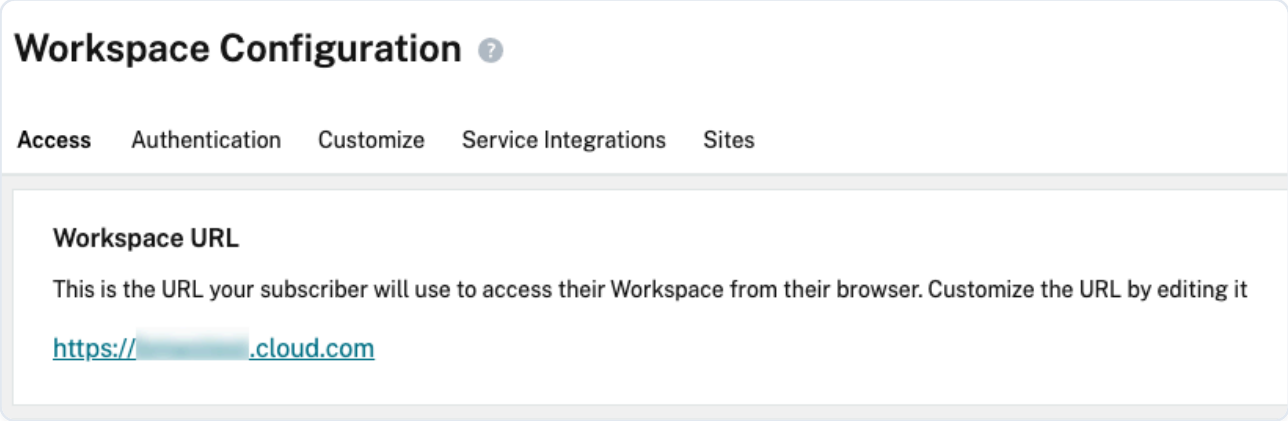
- **アプリケーションの編集**

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

- **削除**

注:

- ユーザーにアプリへのアクセスを許可するには、管理者はアクセスポリシーを作成する必要があります。アクセスポリシーでは、管理者はアプリのサブスクライバーを追加し、セキュリティ制御を設定します。詳細については、「アクセスポリシーの作成」を参照してください。
- ユーザーに必要な認証方法を設定するには、「IDと認証のセットアップ」を参照してください。
- ユーザーと共有するストアURLを取得するには、Citrix Cloud™メニューから**StoreFront Cloud**をクリックし、**アクセス**タブを選択します。



管理者設定 – Citrix Secure Access クライアントベースのHTTP/HTTPSアプリへのアクセス

注:

Citrix Secure Accessクライアントを使用して既存または新規のHTTP/HTTPSアプリにアクセスするには、リソースの場所に少なくとも1つの（高可用性の場合は2つを推奨）コネクタアプライアンスをインストールする必要があります。コネクタアプライアンスは、オンプレミス、データセンターのハイパーバイザー、またはパブリッククラウドにインストールできます。コネクタアプライアンスとそのインストール方法の詳細については、「Cloud Services用コネクタアプライアンス」を参照してください。

前提条件

- Citrix Cloud内のCitrix Secure Private Accessへのアクセス。

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

注意事項

- 強化されたセキュリティ制御が適用されている内部Webアプリは、Citrix Secure Accessクライアントを介してアクセスできません。
- SaaSアプリは、Citrix Secure Accessクライアントを介してアクセスできません。
- 強化されたセキュリティ制御が有効になっているHTTP(S)アプリケーションにアクセスしようとすると、次のポップアップメッセージが表示されます。**「アプリ名」(FQDN) アプリケーションには追加のセキュリティ制御が有効になっています。Citrix Workspaceからアクセスしてください。**

  エラーメッセージ(/en-us/citrix-secure-private-access/media/ztna-agent-based-error-message.png)
- SSOエクスペリエンスを有効にする場合は、Citrix WorkspaceアプリまたはWebポータルを使用してWebアプリにアクセスしてください。

HTTP(S)アプリの設定手順は、エンタープライズWebアプリのサポートで説明されている既存の機能と同じです。

TCP/UDPおよびHTTP(S)アプリへのアダプティブアクセス

アダプティブアクセスにより、管理者は、デバイスのポスチャチェック、ユーザーの地理的位置、ユーザーロール、Citrix Analyticsサービスが提供するリスクスコアなど、複数のコンテキスト要因に基づいて、ビジネスクリティカルなアプリへのアクセスを管理できます。

注：

- TCP/UDPアプリケーションへのアクセスを拒否できます。管理者は、ユーザー、ユーザーグループ、ユーザーがアプリケーションにアクセスするデバイス、およびアプリケーションがアクセスされる場所（国）に基づいてポリシーを作成します。アプリケーションへのアクセスはデフォルトで許可されています。
- アプリケーションに対して行われたユーザーサブスクリプションは、ZTNAアプリケーション用に構成されたすべてのTCP/UDPアプリの宛先に適用されます。

アダプティブアクセスポリシーを作成するには

管理者は、管理者ガイド付きワークフローウィザードを使用して、Secure Private AccessサービスでSaaSアプリ、内部Webアプリ、およびTCP/UDPアプリへのゼロトラストネットワークアクセスを構成できます。

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

注記:

- 適応型アクセス ポリシーの作成について詳しくは、「アクセス ポリシーの作成」を参照してください。
- Secure Private AccessサービスにおけるSaaSアプリ、社内Webアプリ、およびTCP/UDPアプリへのゼロトラストネットワークアクセスのエンドツーエンド構成については、「簡単なオンボーディングとセットアップのための管理者ガイド付きワークフロー」を参照してください。

ログインおよびログアウトスクリプト構成レジストリ

Citrix Secure Accessクライアントは、Citrix Secure Private Accessクラウドサービスに接続するときに、次のレジストリからログインおよびログアウトスクリプト構成にアクセスします。

レジストリ: HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client

- ログインスクリプトパス: SecureAccessLogInScript type REG_SZ
- ログアウトスクリプトパス: SecureAccessLogOutScript type REG_SZ

アプリケーションドメインのIPアドレスの競合のトラブルシューティング

アプリの作成中に追加された宛先は、メインルーティングテーブルに追加されます。 ルーティングテーブルは、接続確立とトラフィックを正しいリソースロケーションに誘導するためのルーティング決定を行うための信頼できる情報源です。

- 宛先IPアドレスは、リソースロケーション全体で一意である必要があります。
- Citrixでは、ルーティングテーブル内のIPアドレスまたはドメインの重複を避けることをお勧めします。重複が発生した場合は、解決する必要があります。

競合シナリオの種類は次のとおりです。**完全な重複**は、競合が解決されるまで管理者の構成を制限する唯一のエラーシナリオです。

競合シナリオ	既存のアプリケーションドメインエントリ	アプリケーション追加からの新規エントリ	動作
サブセットの重複	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL1	許可; 警告情報 - 既存のエントリとのIPド

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

競合シナリオ	既存のアプリケーションドメインエントリ	アプリケーション追加からの新規エントリ	動作
			メインのサブセット重複
サブセットの重複	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL2	許可; 警告情報 - 既存のエントリとのIPドメインのサブセット重複
部分的な重複	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL1	許可; 警告情報 - 既存のエントリとのIPドメインの部分的な重複
部分的な重複	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL2	許可; 警告情報 - IPドメインが既存のエントリと部分的に重複しています
完全な重複	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL1	エラー; `<Completely overlapping IP domain's value>` IPドメインが既存のエントリと完全に重複しています。既存のルーティングIPエントリを変更するか、別の宛先を設定してください
完全な重複	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL2	エラー; `<Completely overlapping IP domain's value>` IPドメインが既存のエントリと完全に重複しています。既存のルーティングIPエントリを変更する

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

競合シナリオ	既存のアプリケーションドメインエントリ	アプリケーション追加からの新規エントリ	動作
			か、別の宛先を設定してください
完全一致	20.20.20.0/29 RL1	20.20.20.0/29	許可; ドメインは既にドメインルーティングテーブルに存在します。変更によりドメインルーティングテーブルが更新されます

注記:

- 追加された宛先が完全に重複する場合、**アプリの詳細**セクションでアプリを構成する際にエラーが表示されます。管理者は、**アプリの接続**セクションで宛先を変更してこのエラーを解決する必要があります。

  アプリの詳細セクションにエラーがない場合、管理者はアプリの詳細を保存できます。ただし、**アプリの接続**セクションで、宛先が相互に、またはメインルーティングテーブルの既存のエントリと部分的に重複している場合、またはそのサブセットである場合、警告メッセージが表示されます。この場合、管理者はエラーを解決するか、構成を続行するかを選択できます。
- Citrixは、クリーンな**アプリケーションドメイン**テーブルを維持することを推奨します。IPアドレスドメインが重複なく適切なチャンクに分割されている場合、新しいルーティングエントリを構成する方が簡単です。

注意点

- 拡張セキュリティが有効になっている既存のWebアプリへのアクセスは、Secure Accessクライアント経由では拒否されます。Citrix Workspaceアプリを使用してログインするよう促すエラーメッセージが表示されます。
- ユーザーリスクスコア、デバイスポスチャチェックなどに基づくWebアプリのポリシー構成は、Citrix Workspaceアプリ経由で、Secure Accessクライアント経由でアプリにアクセスする際に適用されます。

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

- アプリケーションにバインドされたポリシーは、アプリケーション内のすべての宛先に適用されます。

Windowsログオン前のAlways On

Secure Private Access Always On接続により、管理対象デバイスはWindowsログオン前（マシントンネルのみ）およびログオン後も常にエンタープライズネットワークに接続されていることが保証されます。Always On機能は、ユーザーがWindowsシステムにログオンする前に、マシンレベルのVPNトンネルを確立します。ユーザーがログオンすると、マシンレベルのVPNトンネルはユーザーレベルのVPNトンネルに置き換えられます。アプリケーションアクセスは、マシンレベルのトンネルにはマシンに割り当てられたポリシーに基づいて、ユーザーレベルのトンネルにはユーザーに割り当てられたポリシーに基づいて行われます。

Secure Private Access Always On (Windowsログオン前、マシントンネル) 機能は、以下のマシンでサポートされています。

- Active Directoryドメイン参加済みWindowsマシン
- Microsoft Entra IDハイブリッドドメイン参加済みWindowsマシン

Windowsログオン前のAlways Onは、Active Directoryを使用したコンピューターデバイス証明書ベースの認証によって認証されます。

デバイス証明書は、Active Directoryエンタープライズ証明機関 (CA) によって発行されます。デバイス証明書は、ドメイン参加済みWindowsマシンごとに一意です。

注:

- 1層から多層のMicrosoftエンタープライズ証明機関がサポートされています。
- Secure Private Access Always On (Windowsログオン後、ユーザー トンネル) は、Active Directoryの以下の自動ログオン認証方法のいずれかによって実現されます。
  - Windowsログオン時に提供されたActive Directory資格情報を使用したCitrix Secure Access™クライアントへのシングルサインオン (SSO)。第二要素が構成されている場合、SSOは機能しません。
  - Citrix GatewayとのKerberosベースSSO。詳細については、「オンプレミスのCitrix GatewayをCitrix CloudのIDプロバイダーとして接続し、アダプティブ認証をプロビジョニングする」を参照してください。
  - アダプティブ認証の構成。詳細については、「アダプティブ認証のプロビジョニング」を参照してください。

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

- Secure Private Access Always On (Windowsログオン後、ユーザー トンネル) は、Microsoft Entra IDハイブリッド参加済みマシン向けの以下の自動ログオン認証方法、つまりMicrosoft Entra ID認証のプライマリ更新トークン (PRT) を使用したSSOによって実現されます。

  エンドユーザーに常に資格情報の入力を求めるを無効にします。

Always Onはどのように機能しますか?

次の図は、Windowsログオン前のAlways On機能のワークフローを示しています。

Always Onワークフロー(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-how-it-works.png)

- Citrix Identity Brokerはデバイス証明書を検証し、起動直後にデバイスを認証します。デバイス証明書の検証手順は次のとおりです。
  - クライアントは、Secure Private Access管理コンソールにアップロードされたCA証明書に基づいてデバイス証明書を提示します。
  - Citrix IDプロバイダーはデバイス証明書ベースの認証を実行します。
  - Citrix IDプロバイダーは次の詳細を検証します。
    - デバイス証明書の署名
    - CRLベースのデバイス証明書失効チェック
    - Active Directoryコンピューターオブジェクトに対するデバイス証明書の検証
- デバイス証明書の検証が成功すると、アクセスポリシーに基づいて、デバイスと社内リソースの間にセキュアなマシントンネルが確立されます。
- Active Directoryへのアクセスを許可すると、WindowsログオンはActive Directoryでユーザー資格情報を認証し、パスワードの有効期限とパスワード変更をサポートします。
- Windowsログオン後、マシンレベルのトンネルは、自動ログオン付きのユーザートンネルに自動的に置き換えられます。ユーザートンネルの障害/切断時には、接続はマシントンネルにフォールバックします。
- 自動ログイン機能は、Active DirectoryおよびハイブリッドMicrosoft Entra ID環境でサポートされています。

Active DirectoryおよびMicrosoft Entra IDハイブリッドAD構成

Windowsマシンは、Always Onの前提条件として、Active DirectoryまたはMicrosoft Entra IDハイブリッド参加済みである必要があります。Always Onマシン認証用のデバイス証明書を発行するに

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

は、Active Directoryエンタープライズ証明機関が必要です。証明書の失効は、証明機関のLDAP URL構成を持つCDP拡張に基づいて検証されます。

デバイス証明書登録の構成

デバイス証明書の登録には、次の手順が含まれます。

1. Active Directoryエンタープライズ証明機関は、マシン認証用のデバイス証明書を発行します。
2. 証明機関は、CRL配布ポイント (CDP) 拡張機能のLDAP URLを公開している必要があります。

   常にオンのCRL CDP(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-crl-cdp.png)
3. この証明機関に、以下の詳細でデバイス証明書を登録するための証明書テンプレートを作成する必要があります。

   a. 証明書テンプレートスナップインを開き、**コンピューター**または**ワークステーション認証** (推奨) テンプレートのいずれかを複製します。

   b. 証明書に新しい名前を指定します。

   c. **サブジェクト名**タブに切り替え、**サブジェクト名形式**の設定を**共通名**に変更し、代替サブジェクト名に**ユーザープリンシパル名 (UPN)**を含めるようにチェックします。

   常にオンのサブジェクト名(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-common-name-upn.png)

   d. **セキュリティ**タブに切り替え、新しい証明書テンプレートを自動登録するセキュリティグループ (コンピューターアカウントのみを含む) を追加します。追加したグループを選択し、**自動登録**に対して**許可**を選択します。

   常にオンの認証済みユーザー(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-auto-enroll.png)

   > **注:**
   >
   > 上の画像では、**認証済みユーザー** (すべてのコンピューターオブジェクト) が新しい証明書テンプレートの登録/自動登録を許可されています。

   e. (オプション) 自動証明書登録を許可するグループポリシーオブジェクト (GPO) を作成し、それを組織単位 (OU) またはドメインレベルにバインドします。

   常にオンの自動登録証明書(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-autoenroll-certificate.png)

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

セキュア プライベート アクセス の構成

以下のセクションでは、Secure Private Access の構成に関する詳細情報を提供します。

Windows ログオン前のAlways On (マシン トンネル) を構成する

1. Secure Private Access 管理コンソールで、 **>** に移動します。

   注:

   > にある オプションを、 **>** の代わりに使用することをお勧めします。 **>** オプションは、今後のサービスリリースで削除される予定です。

2. ページで、 タブをクリックします。

   トグルスイッチは、Windows ログオン前のAlways On 機能でデフォルトで有効になっています。

3. CA 証明書をアップロードします。 をクリックし、証明書を選択して、 をクリックします。
4. に、証明書の名前を入力します。
5. で、ローカルドライブを参照して証明書ファイルをアップロードします。

   - ルートCAと中間CAの両方の証明書がサポートされています。アップロードする証明書はPEM形式であり、チェーン全体を含める必要があります。証明書は、中間証明書からルートCAまで生成されている必要があります。
   - 証明書がCER形式の場合は、LinuxまたはMacターミナルで次のコマンドを実行して、証明書をPEM形式に変換します。証明書をPEM形式に変換した後、Secure Private Accessユーザーインターフェイスで証明書をアップロードします。

     ```
     openssl x509 -in /Users/t_abhishes2/Downloads/cert12.crt out/Users/t_abhishes2/Downloads/cer_pem12_ao.pem
     ```

6. 「**保存**」をクリックします。

   証明書は、 タブの利用可能な証明書のリストに追加されます。

7. Active Directory に TCP/UDP サーバーとしてアクセスするための TCP/UDP アプリケーションを作成します。例: Active Directory ドメイン、IP アドレス、ポート。これは、AD 資格情報を使用した Windows ユーザーログオン用です。TCP/UDP アプリの作成の詳細については、「管理者構成 – Citrix Secure Access クライアントベースの TCP/UDP アプリへのアクセス」を参照してください。

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

8. Windows ログオン前およびユーザーレベルのトンネル移行前にアクセスする必要がある場合は、追加のアプリケーションを作成します。
9. アクセス ポリシーを作成し、ドメイン参加済みマシンまたはその AD グループにアクセスを提供します。

   a. Secure Private Access 管理コンソールで、 をクリックし、次に をクリックします。
   b. ポリシー名とポリシーの説明を入力します。
   c. で、このポリシーを適用するアプリまたはアプリのセットを選択します。
   d. をクリックして、ポリシーのルールを作成します。

      - ルール名とルールの簡単な説明を入力し、 をクリックします。
      - で、 を選択します。

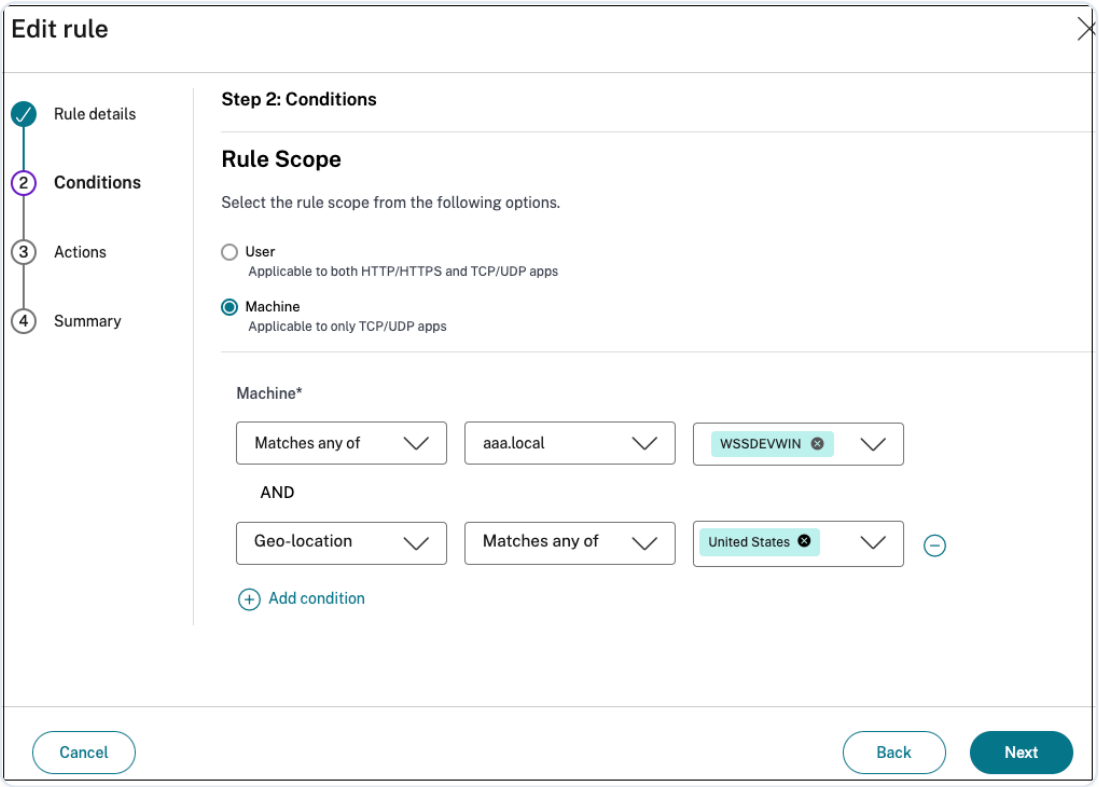
        注:

        マシンを選択すると、マシンレベルのトンネルは単一要素認証に基づいているため、アクセス権限が制限されます。

      - 一致条件とドメインを選択し、ポリシーを適用するマシン/グループを検索します。必要に応じて条件を追加します。完了したら、 をクリックします。

        - **いずれかに一致** – フィールドにリストされている名前のいずれかに一致し、選択したドメインに属するマシン/グループのみがアクセスを許可されます。
        - **いずれにも一致しない** – フィールドにリストされているものおよび選択したドメインに属するもの以外のすべてのマシン/グループがアクセスを許可されます。

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



10. 条件評価に基づいて適用する次のいずれかのアクションを選択します。

    - **アクセスを許可**
    - **アクセスを拒否**

11. 「**次へ**」をクリックし、「**完了**」をクリックします。
12. (オプション) 地理的位置やネットワーク位置などの追加ルールを作成します。詳細については、「アクセスポリシーの構成」を参照してください。

    ポリシーは「アクセスポリシー」ページに表示されます。デフォルトでは、ポリシーに優先順位が割り当てられます。値が小さい優先順位ほど、優先度が高くなります。優先順位番号が最も低いポリシーが最初に評価されます。ポリシーが定義された条件と一致しない場合、次のポリシーが評価されます。条件が一致した場合、他のポリシーはスキップされます。

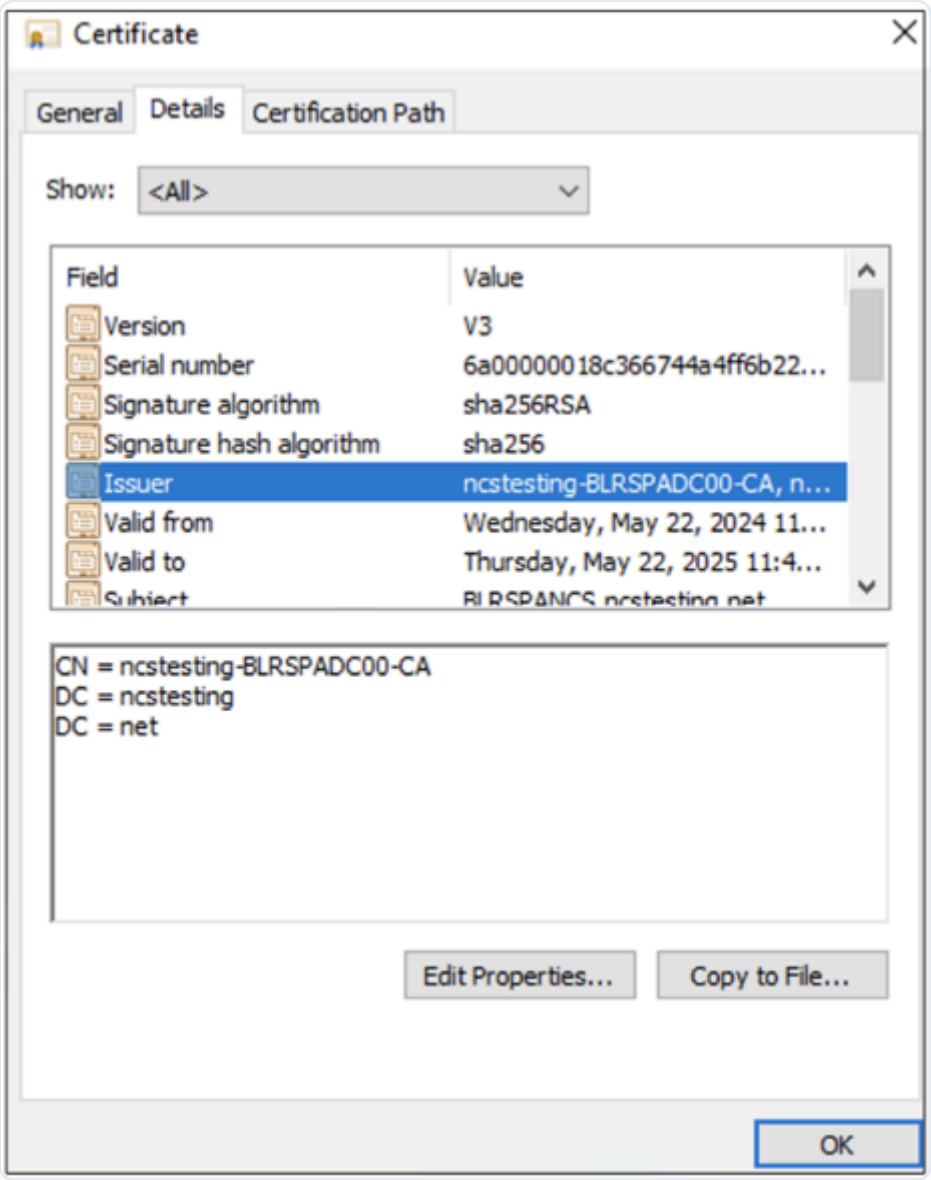
コネクタアプライアンスの構成

Connector Appliance は、Always On デバイス証明書認証のために、デバイス証明書の検証、証明書失効チェック (CRL)、およびデバイスオブジェクトの検証を実行します。デバイス証明書認証をサポートするには、Connector Appliance が Active Directory ドメインにドメイン参加している必要があります。

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

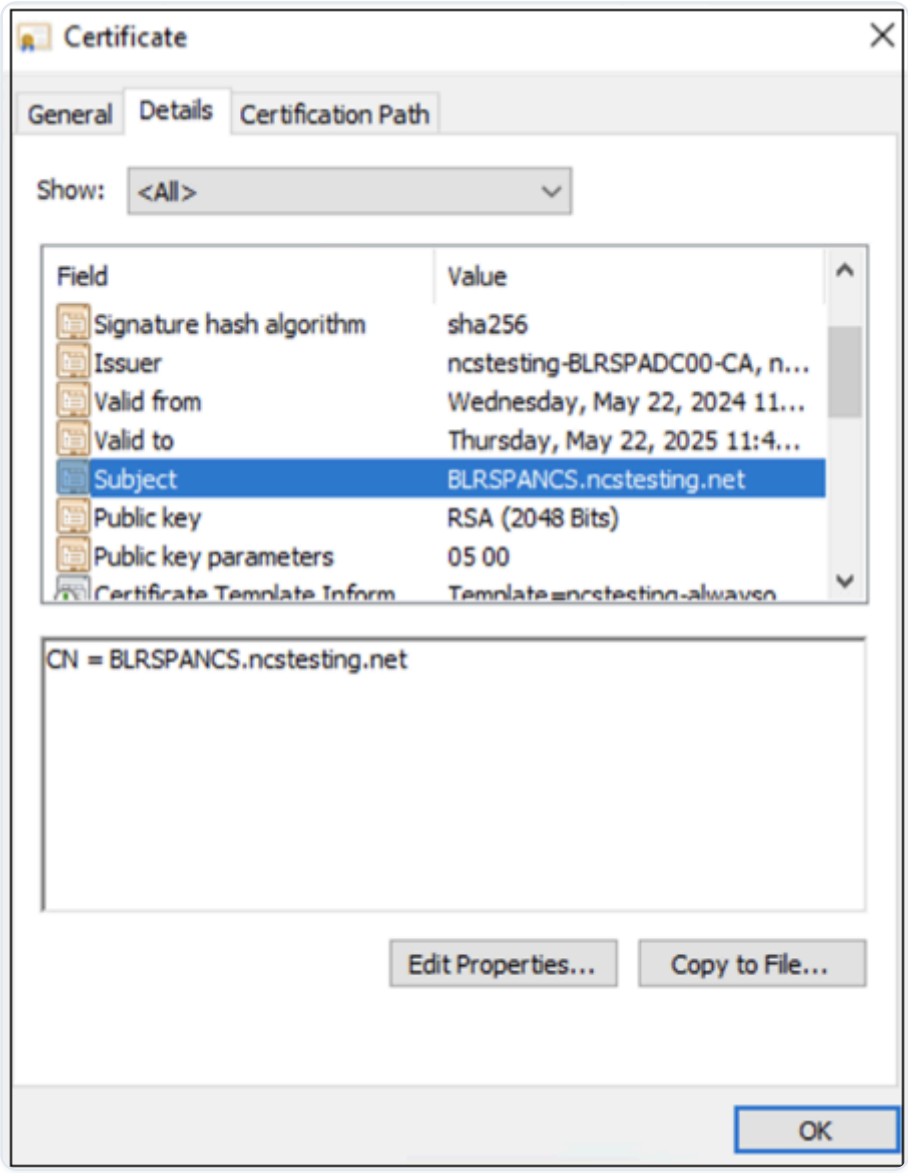
クライアント構成

- Always On をサポートする必要がある Windows マシンは、Active Directory または Entra ID ハイブリッドにドメイン参加している必要があります。
- Windows マシンは、Secure Private Access Always On のために、エンタープライズ証明機関からデバイス証明書を登録する必要があります。
- デバイス証明書の属性には、次の詳細を含める必要があります。
  - デバイス証明書の発行者名は、Secure Private Access 管理コンソールにアップロードされた CA 証明書の共通名と一致する必要があります。



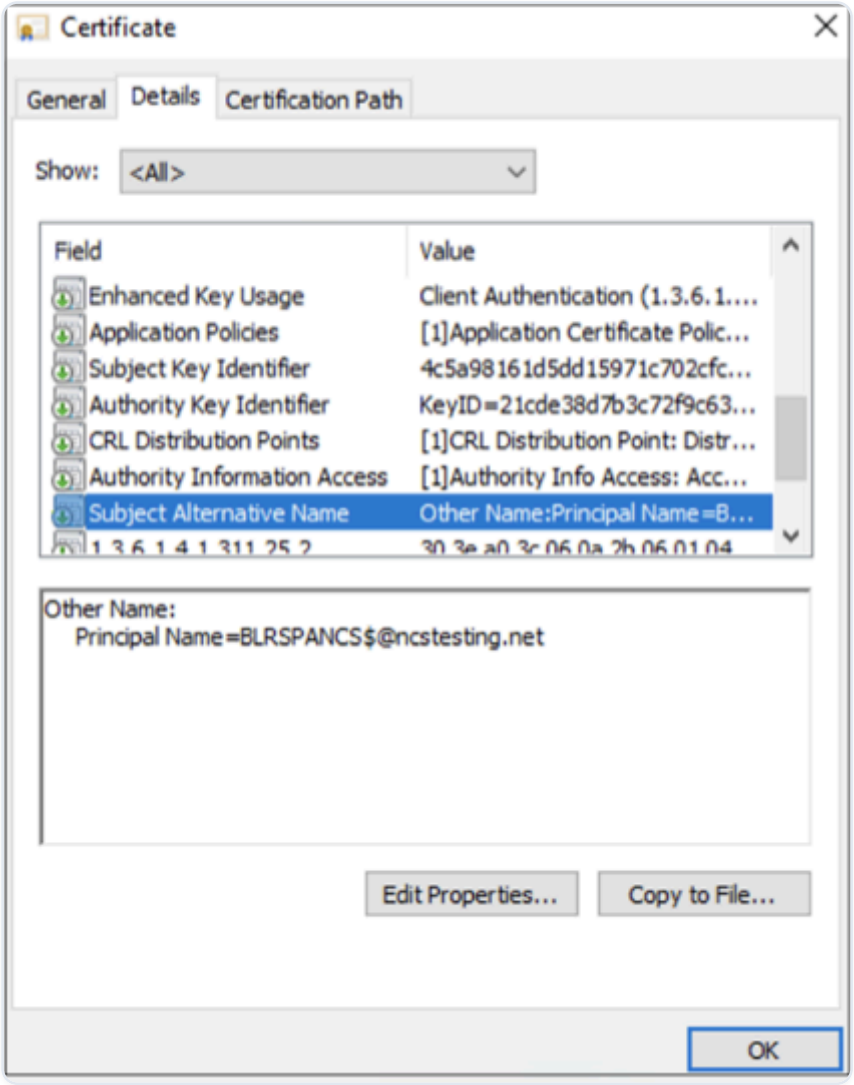
  - サブジェクトには、コンピューターの共通名を含める必要があります。

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



- サブジェクト代替名 (SAN) には、コンピューターの UPN を含める必要があります。

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



- CRL配布ポイントには、適切なLDAP URLが含まれている必要があります。

  常時接続 CRL DP(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-crl-cdp.png)

- 認証パスは、証明機関チェーンに適切である必要があります。

  常時接続 CRL DP(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-cert-path.png)

- Always On 用の Citrix Secure Access クライアントをインストールします。
- Windowsログオン前にAlways Onを有効にするには、クライアントに次のレジストリを作成する必要があります。

  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client のレジストリパスにある **CloudAlwaysOnURL**。

    レジストリの種類 - STRING

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

レジストリ値 - `<Customer store FQDN>` (例: company.cloud.com)

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client にある **AlwaysOnService**。

  レジストリの種類 - DWORD

  レジストリ値 - 0x00000002

Windowsログオン後にAlways Onを構成する（マシン/ユーザー トンネル）

Windowsログオンが成功した後、Citrix Secure Access クライアントでのユーザーログインが成功するまで、マシン トンネルは継続します。

- ユーザーの自動ログインが成功すると、マシン トンネルはユーザー トンネルに移行されます。
- ユーザーの自動ログインが失敗した場合、マシントンネルは継続されます。
- ユーザーのトンネルが切断された場合、接続は自動的にマシントンネルにフォールバックします。

Windowsログオン後のユーザー自動ログオンは、StoreFront Cloud認証構成において以下の認証方法でサポートされています。

- Active Directoryによる認証（第二要素なし） - AD資格情報SSO
- Kerberos SSOで構成されたCitrix Gateway/Adaptive Authによる認証
- Azure Active Directoryによる認証（Microsoft Entra ID認証のプライマリ更新トークン（PRT）によるSSO）。

注:

エンドユーザーに常に資格情報の入力を求めるを無効にします。

制限事項

- コンピューターのUPNホスト名は15文字を超えてはなりません。
- Windows自動ログオン（初回ユーザー（FTU））は、マシンがドメインに参加しており、デバイス証明書が存在する場合にのみサポートされます。
- Windowsログオン前のAlways On機能は、Windows 10以降のバージョンでのみサポートされています。
- Windowsログオン前のAlways On機能は、Windows Serverオペレーティングシステムではサポートされていません。

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

- Windowsログオン前のAlways On機能は、Cloud Connectorではサポートされていません。優先コネクタとしてConnector Applianceを選択していない場合でも、マシントンネルトラフィックはConnector Applianceを経由します。

参照

- セキュア プライベート アクセス コンソールでTCP/UDPアプリケーションを作成する
- TCP/UDPアプリケーションにアクセスポリシーを割り当てる(/ja-jp/citrix-secure-private-access/service/admin-guided-workflow-for-easy-onboarding-and-setup.html#step-3-configure-an-access-policy-with-multiple-rules)
- オンプレミスのCitrix GatewayをCitrix CloudへのIDプロバイダーとして接続する(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/connect-ad-gateway.html)
- 適応型認証のプロビジョニング

TCPおよびUDPサーバー用の予約済みCIDRアドレス

管理者は、TCP/UDPサーバー用に予約済みCIDR IPアドレスを設定できます。これらのIPアドレスは、DNS解決中に実際のIPアドレスの代わりにDNS応答で共有されます。

許可されている予約済みCIDR IPアドレス範囲は次のとおりです。

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

注:

予約済みIPアドレスが以下と競合しないことを確認してください。

- 顧客のリソースロケーションでTCP/UDPアプリケーション用に設定されたIPアドレス。
- クライアントマシンのネットワークサブネット。

予約済みCIDR IPアドレスを構成する

1. **設定**をクリックし、**グローバル構成**をクリックします。

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

2. **Secure Access Agentの予約済みネットワークサブネット**で、**管理**をクリックします。
3. **IP CIDR**で、プライベートIPアドレス範囲を入力します。
4. **保存**をクリックします。

FQDNをIPアドレスに解決するためのDNSサフィックス

DNSサフィックスは、すべてのエンドユーザーに適用されるグローバル設定です。Citrix Secure Private Access™サービスのDNSサフィックス機能は、以下のユースケースで使用できます。

- バックエンドサーバーのDNSサフィックスドメインを追加することで、Citrix Secure Access™クライアントが非完全修飾ドメイン名（ホスト名）を完全修飾ドメイン名（FQDN）に解決できるようにします。
- 管理者がIPアドレス（IP CIDR/IP範囲）を使用してアプリケーションを構成できるようにし、エンドユーザーがDNSサフィックスドメイン下の対応するFQDNを使用してアプリケーションにアクセスできるようにします。

例えば、非完全修飾ドメイン名「workday」を解決する際に、DNSサフィックス「citrix.net」が構成されている場合、オペレーティングシステムはサフィックス「citrix.net」を付加し、「workday.citrix.net」に解決します。

複数のDNSサフィックスが構成されている場合、DNSサフィックスは順序に従って解決されます。例えば、以下のサフィックスが追加されていると仮定します。

- `".citrix.net"`
- `".citrix.com"`
- `".xenserver.com"`

エンドユーザーが「workday」と入力すると、オペレーティングシステムは以下の順序でFQDNを解決しようとします。いずれかのサフィックスで成功した場合、残りのサフィックスはスキップされます。

1. workday.citrix.net
2. workday.citrix.com

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

3. workday.xenserver.com

重要:

- DNSサフィックス設定は、DNSサフィックス機能を使用して構成されたドメインをサフィックスとして付加することで、クライアントが非完全修飾ドメイン名を解決できるようにするだけです。エンドユーザーがDNSサフィックスドメイン下のFQDNにアクセスするには、管理者はIPアドレス、FQDN、またはワイルドカードドメインを使用してアプリケーションを構成する必要があります。詳細については、ユースケースの例の4番目のポイントを参照してください。
- 2つの異なるアプリケーションが設定されており、一方がFQDN、もう一方がIPアドレスで、両方とも同じバックエンドサーバーに対応している場合、IPアドレスを持つアプリケーションのポリシーが優先されます。詳細については、ユースケースの例の5番目の項目を参照してください。

前提条件

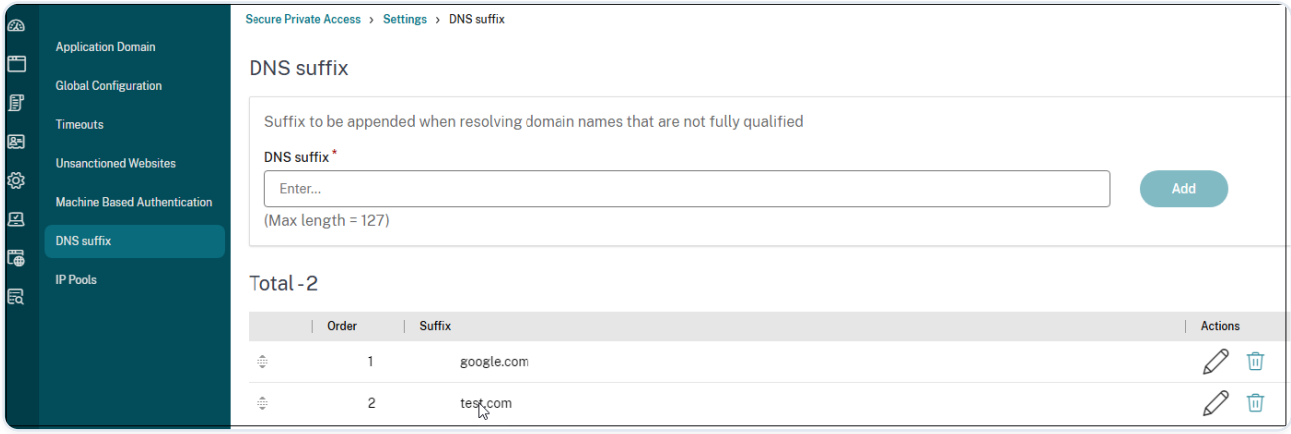
- DNSサフィックス機能を使用するには、Secure Private Access Advancedエディションの利用資格が必要です。
- DNSサフィックス機能フラグを有効にするには、Citrix製品管理チームにお問い合わせください。

DNSサフィックスの追加方法

1. Secure Private Accessタイルで、**「管理」**をクリックします。
2. Secure Private Accessランディングページで、**「設定」**をクリックし、次に**「DNSサフィックス」**をクリックします。
3. **「DNSサフィックス」**フィールドに、完全修飾されていない名前を解決する際に付加する必要があるサフィックスを入力します。
4. **「追加」**をクリックします。

サフィックスは追加された順序で一覧表示されます。管理者はサフィックスを削除または変更できます。

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



ユースケースの例

以下を考慮してください。

- 管理者が顧客ネットワーク内のマシンにIPアドレス192.0.2.1を割り当てました。
- マシン（IPアドレス192.0.2.1）のFQDNは「citrix.net」ドメインに属しています（例: workday.citrix.net）。

	DNSサフィックスとアプリ構成	エンドユーザーエクスペリエンス
1	管理者はDNSサフィックスを「citrix.net」として構成し、IPアドレス192.0.2.1を持つアプリを作成し、user1に対してアクセスポリシーを「許可」に設定します。	user1が「workday」に接続しようとすると、FQDNに「citrix.net」がサフィックスとして追加され（workday.citrix.net）、IPアドレスは192.0.2.1に解決されます。192.0.2.1はuser1に対してアプリが構成されており許可されているため、アクセスが許可されます。
	注: エンドユーザーは、192.0.2.1、workday.citrix.net、または「workday」でWorkdayアプリにアクセスできます。	
	DNSサフィックス構成がない場合、「workday」および「workday.citrix.net」を介したアクセスは拒否されます。	

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

	DNSサフィックスとアプリ構成	エンドユーザーエクスペリエンス
2	管理者はDNSサフィックスを「citrix.net」として構成し、FQDN (workday.citrix.net) を持つアプリを作成し、user1に対してアクセスポリシーを「許可」に設定します。	user1が「workday」に接続しようとすると、「workday」に「citrix.net」がサフィックスとして追加されます (workday.citrix.net)。「workday.citrix.net」でアプリケーションが構成されており、user1に対してアクセスポリシーが「許可」に設定されているため、エンドユーザーはWorkdayにアクセスできます。
	注: エンドユーザーは、workday.citrix.net または「workday」でWorkdayアプリにアクセスできます。	
	このIPアドレスで構成されたアプリがないため、192.0.2.1へのアクセスは拒否されます。	
3	管理者はDNSサフィックスを「citrix.net」として構成し、ワイルドカードドメイン「*.citrix.net」を持つアプリを作成し、user1に対してアクセスポリシーを「許可」に設定します。	user1が「workday」に接続しようとすると、「workday」に「citrix.net」がサフィックスとして追加されます (workday.citrix.net)。「*.citrix.net」でアプリケーションが構成されており、user1に対してアクセスポリシーが「許可」に設定されているため、エンドユーザーはWorkdayにアクセスできます。
	注: エンドユーザーは workday.citrix.net または「workday」で Workday にアクセスできます。	

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

	DNSサフィックスとアプリ構成	エンドユーザーエクスペリエンス
	192.0.2.1 へのアクセスは、このIPアドレスで構成されたアプリがないため拒否されます。	
4	管理者はDNSサフィックスを「citrix.net」として構成します。user1に対して、FQDN (workday.citrix.net) または 192.0.2.1 で構成されたアプリケーションはありません。	user1が「workday」に接続しようとすると、クライアントによって「workday」に「citrix.net」がサフィックスとして追加され、「workday.citrix.net」が192.0.2.1に解決されます。しかし、user1に対して、192.0.2.1、workday.citrix.net、または *.citrix.net で構成されたアプリがないため、プライベートサーバー (workday.citrix.net/192.0.2.1) に接続できません。
5	管理者はDNSサフィックスを「citrix.net」として構成します。IPアドレス192.0.2.1のアプリを追加し、user1のアクセスポリシーを「拒否」に設定します。次に、FQDN (workday.citrix.net) を持ち、192.0.2.1に解決される別のアプリを追加し、user1のアクセスポリシーを「許可」に設定します。	user1が「workday」に接続しようとすると、Workday (workday.citrix.net) に「citrix.net」がサフィックスとして追加され、IPアドレスは192.0.2.1に解決されます。しかし、IP 192.0.2.1で構成されたアプリケーションのポリシーが、FQDNで構成されたアプリよりも優先されるため、Workdayへのアクセスは拒否されます。

HARファイルを使用して関連ドメインを検出する

Secure Private Accessを使用すると、HTTPアーカイブ (HAR) ファイルをアップロードして、アプリケーションがアクセスするドメインを自動的に検出できます。検出されたドメインを確認し、アプリケーションの関連ドメイン構成に追加するドメインを選択できます。これにより、関連ドメイ

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

ンを手動で特定して構成する必要がなくなるため、アプリケーションのオンボーディングが簡素化されます。

以前は、管理者はアプリケーションの関連ドメインをすべて事前に把握しているか、ユーザーがブロックされたURLにアクセスしたときに事後的に検出する必要がありました。構成されていないURLはすべてデフォルトでブロックされるため、この事後的なアプローチはユーザーエクスペリエンスの低下につながります。Secure Private Accessには、アプリケーション内の内部URLや埋め込みURLを特定する方法がありませんでした。

例

プライマリドメインが `example.com` であるアプリケーションを構成しているとします。アプリケーションの使用中に、ブラウザはいくつかの追加ドメインにもアクセスします。例：

- `api.example.com` – アプリケーションのバックエンドAPI呼び出しを処理します。
- `auth.example.com` – サインインと認証を管理します。
- `cdn.example.com` – 画像、スクリプト、スタイルシートなどの静的コンテンツを提供します。
- `login.microsoftonline.com` – サードパーティのID認証を提供します。
- `player.vimeo.com` – 埋め込みビデオコンテンツを読み込みます。

これらのドメインをそれぞれ手動で特定する代わりに：

1. アプリケーションの使用中にHARファイルをキャプチャします。
2. HARファイルをSecure Private Accessにインポートします。
3. Secure Private Accessによって検出されたドメインを確認します。たとえば、インポートによって `api.example.com`、`auth.example.com`、`cdn.example.com` が必要なドメインとして表示される場合があります。また、`player.vimeo.com` のような除外を選択できるドメインも表示されます。
4. アプリケーションに必要なドメインを選択します。
5. 必要に応じてルーティングとリソースの場所を構成します。

これにより、アプリケーション接続に必要なドメインをより迅速に特定し、構成できます。

前提条件

WebまたはSaaSアプリケーションにアクセスする際に、HARファイルをキャプチャしていることを確認してください。HARファイルにはネットワーク要求情報が含まれている必要があり、サイズは50 MB以下である必要があります。

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

HARファイルをインポートする

1. Secure Private Access管理ポータルで、構成するWebまたはSaaSアプリケーションを開きます。
2. **アプリ接続**に移動し、**HARのインポート**をクリックします。

   アプリ接続セクションのHARインポートオプション(/en-us/citrix-secure-private-access/media/har-import-button.png)
3. HARファイルをインポートウィンドウにドラッグアンドドロップするか、デバイスからファイルを選択します。
4. Secure Private AccessはHARファイルを分析し、ネットワーク要求から識別されたドメインを表示します。

   インポートされたHARファイルから検出されたドメイン(/en-us/citrix-secure-private-access/media/har-discovered-domains.png)
5. 検出されたドメインを確認します。
6. アプリケーションに追加するドメインを選択します。
7. **インポート**を選択します。

選択したドメインは、アプリケーションの**関連ドメイン**構成に追加されます。

「関連ドメイン」テーブルに表示されるインポートされたドメイン(/en-us/citrix-secure-private-access/media/har-related-domains-table.png)

> **注:**
>
> 発見されたドメインは、インポートする前に確認してください。HARファイルには、アプリケーションの接続に必要ないドメインが含まれている場合があります。

関連ドメインの管理

ドメインをインポートした後、**関連ドメイン**テーブルから管理できます。

- **ドメインの検索** – 検索フィールドを使用してテーブルをフィルタリングし、特定のドメインをすばやく見つけます。
- **ドメインの選択** – 個々のドメインを選択するか、テーブルヘッダーのチェックボックスを使用して複数のドメインを選択します。選択したドメインに対して、同時に複数のアクションを実行できます。

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

- **ドメイン構成の編集** – ルーティングタイプ、プライマリリソースロケーション、セカンダリリソースロケーションなど、関連ドメインの構成を更新します。
- **ドメインの一括編集** – 複数の対象ドメインを選択し、ルーティングとリソースロケーションの設定を同時に更新します。一括編集は、該当する内部ドメインで利用できます。外部ドメインでは、すべての構成オプションがサポートされていない場合があります。
- **リソースロケーション** – 関連ドメインを構成する際、プライマリリソースロケーションと、該当する場合はセカンダリリソースロケーションを割り当てます。これらの設定を使用して、Secure Private Accessが関連ドメインのトラフィックをどのようにルーティングするか、およびどのリソースロケーションが接続を提供するために使用されるかを定義します。

検証とファイルの要件

HARインポート機能は、アップロードされたファイルを処理する前に検証します。

- ネットワーク要求エントリを含む有効なHARファイルのみをインポートできます。
- サポートされる最大ファイルサイズは**50 MB**です。
- ドメインは、HARファイル内のURLから自動的に抽出されます。
- 重複するドメインは自動的に削除されます。
- ドメインは、関連ドメイン構成に追加される前に正規化されます。

ルーティング例外を使用したポートベースルーティング - プレビュー

ポートベースルーティング機能を使用すると、管理者はルーティング例外を使用して、TCP/UDPアプリの場合、同じ宛先の異なるポートに対してトラフィックを異なる方法でルーティングできます。Secure Private Accessにアプリケーションをオンボーディングする際、管理者は以下のいずれかのオプションを使用して、アプリケーションのトラフィックがどのようにルーティングされるかを定義できます。

- **コネクタ経由の内部**: トラフィックはコネクタを介して安全にトンネルされます。
- **NetScaler Gateway経由の内部**: トラフィックはハイブリッドデータパスを使用してNetScaler Gatewayを介してルーティングされます。
- **外部**: トラフィックはSecure Private Accessを介してトンネルされることなく直接ルーティングされます。

同じ宛先の異なるポートに対してトラフィックを異なる方法でルーティングするには、管理者はアクセスポリシーのルーティング例外を使用する必要があります。個別のルーティング決定を必要

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

とする各宛先とポートの組み合わせは、個別のアプリケーションとして構成され、個別のポリシーにバインドされなければなりません。UIは一意性チェックを強制するため、同じ宛先を持つ異なるアプリケーション内で異なるルートを構成することはできません。

ポートベースルーティングのユースケース

シナリオ: 管理者が同じサーバー (10.102.124.135) 上に2つのアプリケーションをホストしています。

- ポート22でのSSHアクセス
- ポート80、443でのWebアクセス

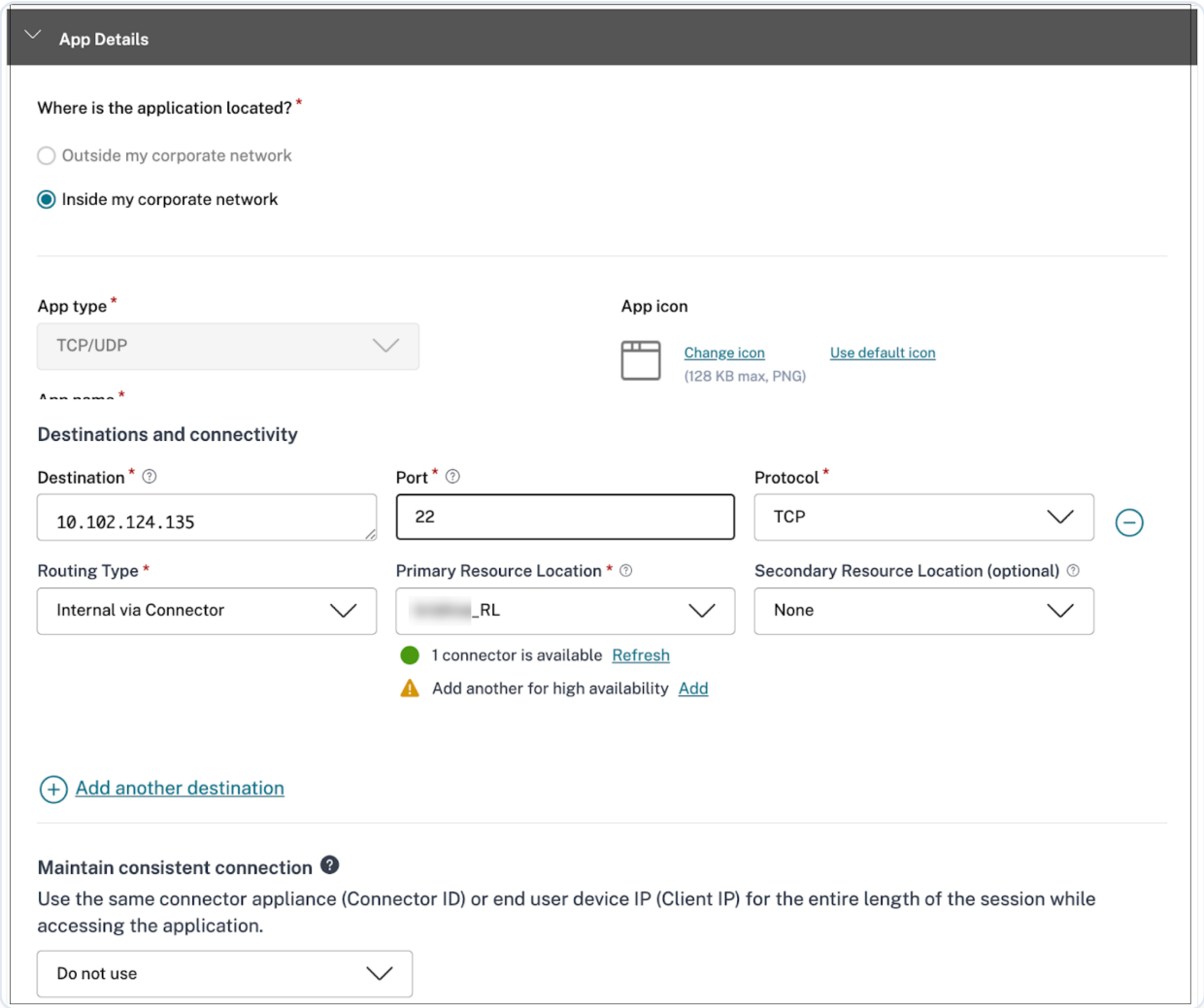
要件:

- 開発者ユーザーグループがコネクタ経由でSSHに内部的にアクセスできるようにする。
- ビジネスユニットユーザーグループが企業ネットワークからWebアプリケーションに直接アクセスできるようにする。

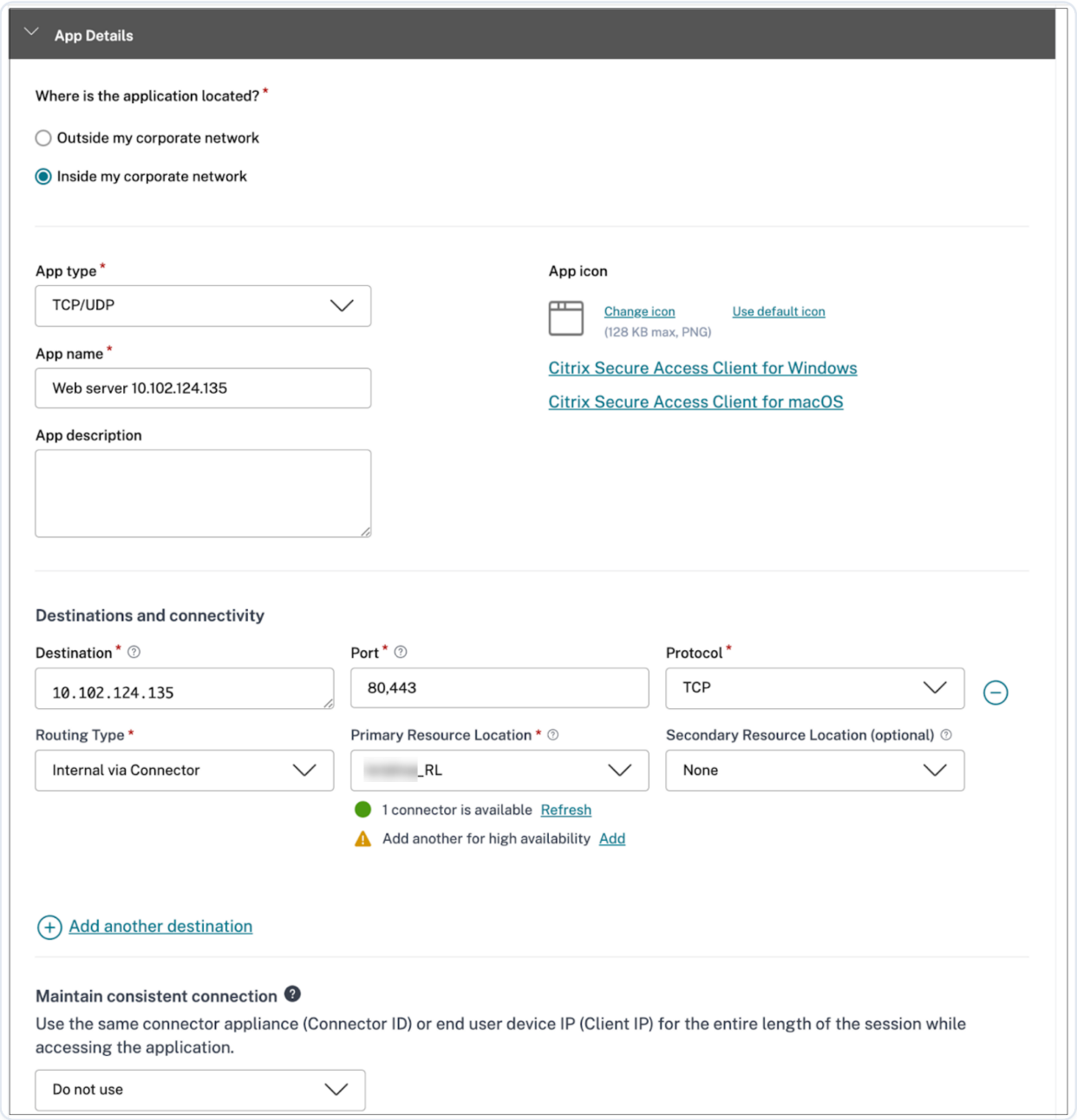
構成:

1. 各要件に対して個別のアプリケーションを作成します。詳細については、「TCP/UDPアプリのサポート」を参照してください。
    - SSHアクセス用のアプリケーションを作成します (宛先:10.102.124.135、ポート 22)。
    - Webアクセス用の別のアプリケーションを作成します (宛先:10.102.124.135、ポート 80,443)。

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



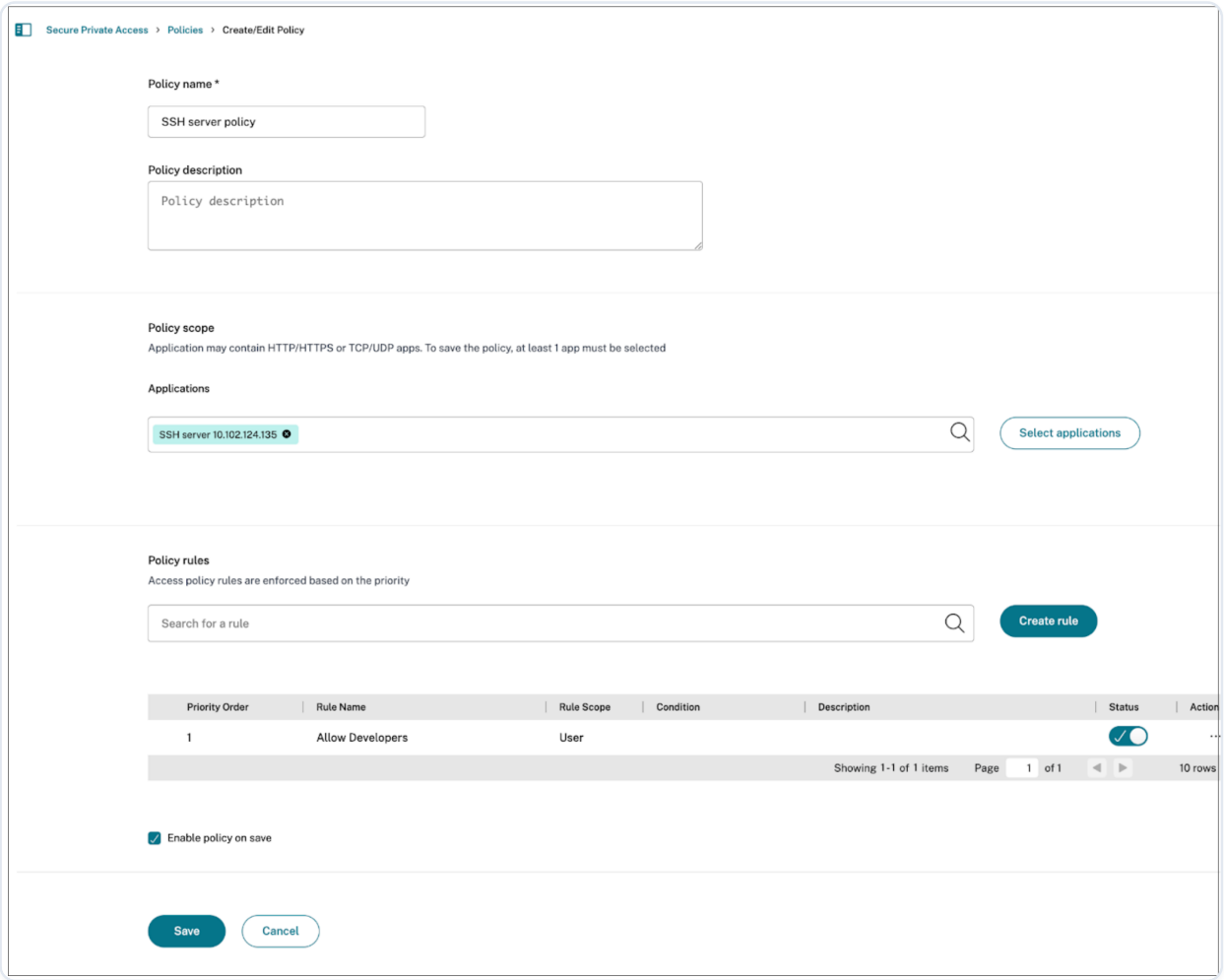
© 1997–2026 Citrix Systems, Inc. All rights reserved.



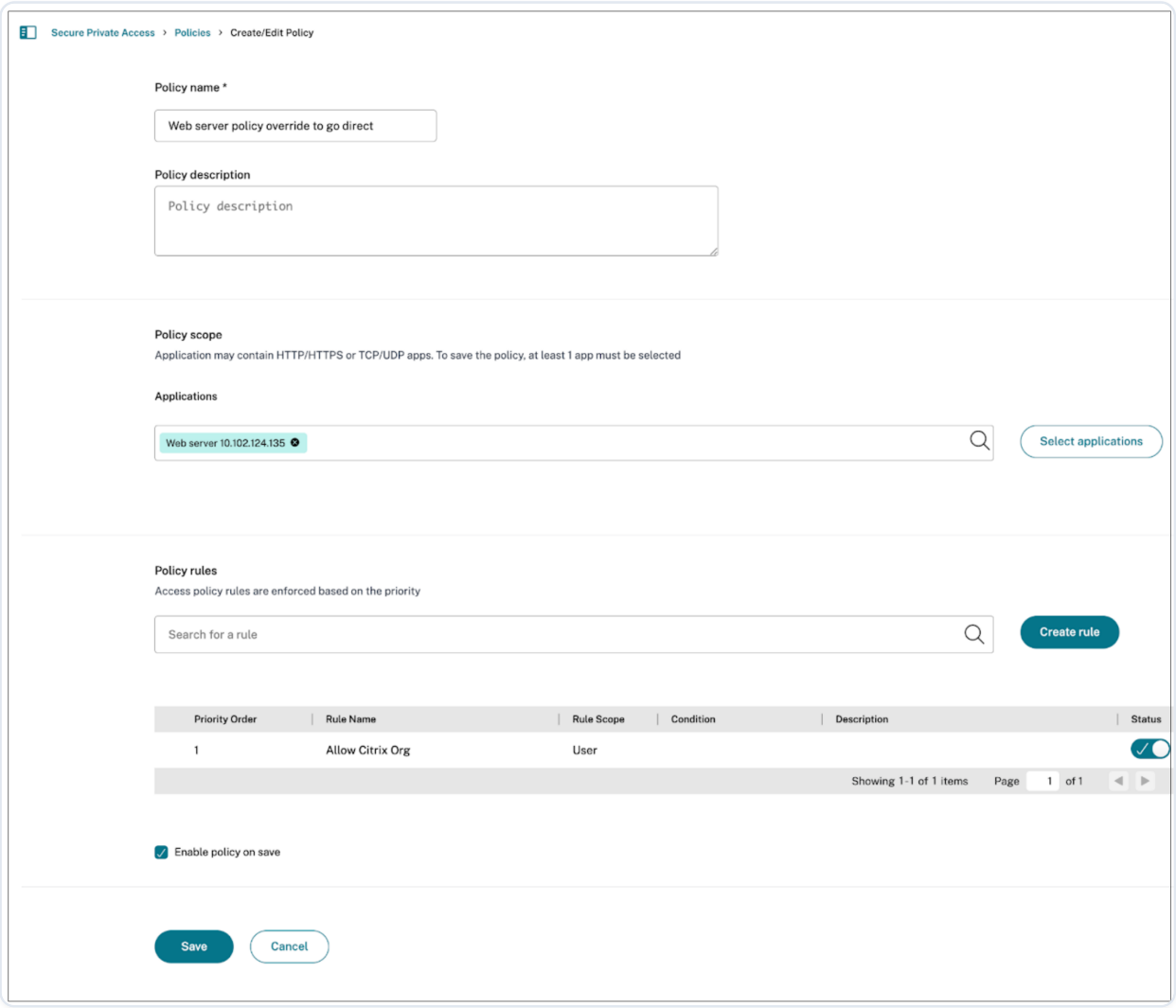
2. 必要に応じて、各アプリケーションのその他の詳細を設定します。
3. 個別のアクセスポリシーを作成します。

   - 各アプリケーションについて個別のポリシーを定義します。
   - ルーティング例外を使用して、設定された各アプリケーションの目的のルーティング動作を指定します。

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

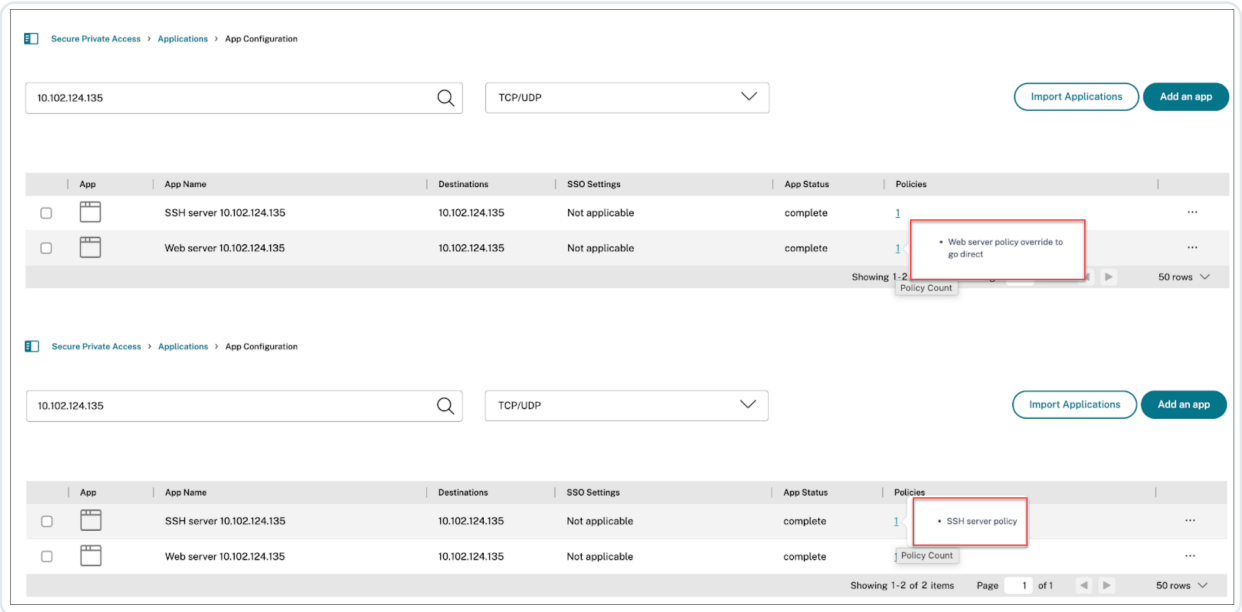


© 1997–2026 Citrix Systems, Inc. All rights reserved.



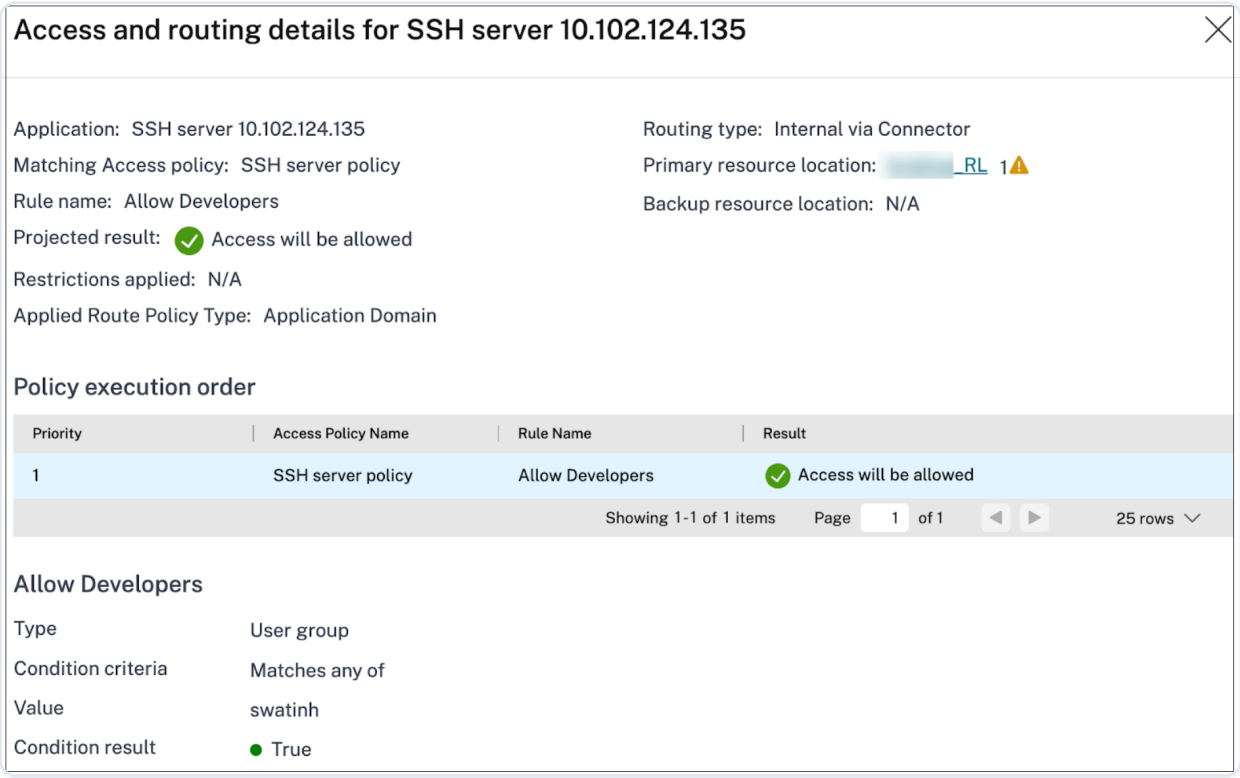
4. ポリシーをアプリケーションにバインドします。

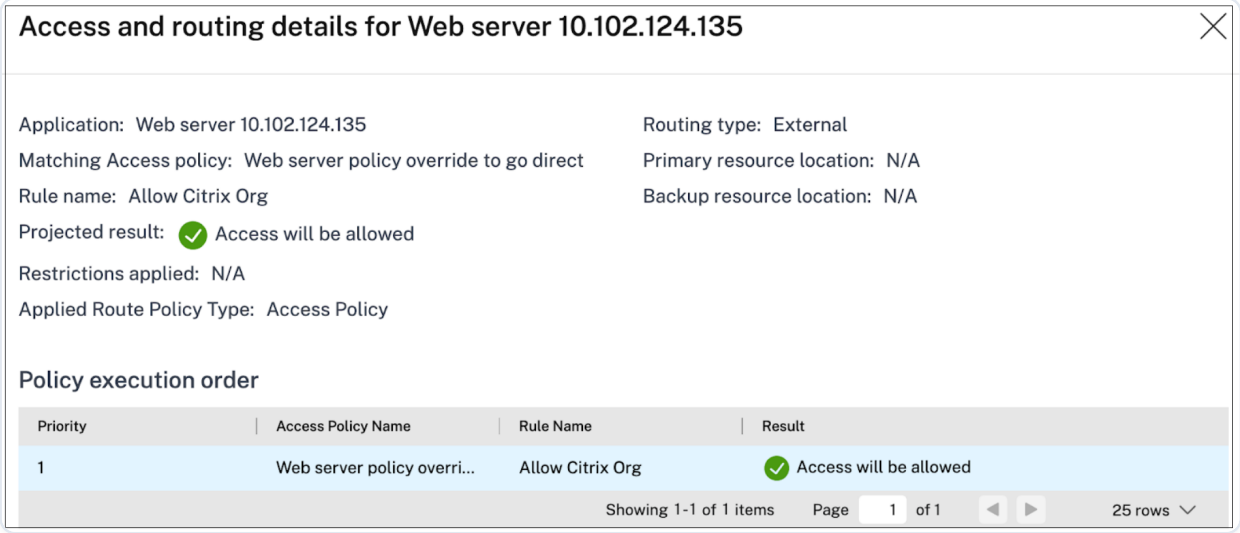
- SSHアクセスポリシーをSSHアプリケーションにバインドします。
- WebアクセスポリシーをWebアプリケーションにバインドします。



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

5. ポリシーモデラーを使用して、アプリケーション、ポリシー、およびルーティングの確認をレビューおよび検証します。





ルーティングオプションの制限事項:

- アクセスポリシーは上から下へ評価されるため、ユーザー、コンテキスト、アプリケーションに一致する最初のポリシーが適用されます。ホスト名ベースのアプリケーションの場合、適用されたポリシーで定義されているルート構成（ルーティングタイプとリソースロケーション）が宛先を解決するために使用されます。
- アクセスポリシーでルート例外が定義されていない場合、アプリケーション構成のルート構成が使用されます。 ルートトンネルとルートダイレクトは相互に排他的です。したがって、ホス

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

ト名ベースの宛先の場合、異なるポートに対してトンネル経由（内部）とダイレクト経由（外部）の両方のルートを持つことはできません。

- 内部ルーティング（コネクタまたはNetScaler Gateway経由）と直接ルーティング（外部）は相互に排他的です。その結果、ホスト名ベースの宛先は内部と外部の両方にルーティングすることはできません。アプリケーションのトラフィックを内部と外部の両方にルーティングする必要がある場合は、IPベースの宛先を使用してアプリケーションをオンボーディングすることをお勧めします。

ポートベースルーティングを示す例

次の図は、ポリシーの優先順位とルーティング例外がエンドユーザーエクスペリエンスにどのように影響するかを示しています。

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

Table	Configured applications and policies for a user	Expected behaviour for the user
App name: LDAP_app Destination URL: example.com Port Number:389 Selected routing in application: 1. Routing Type:Internal via connector 2. Primary resource location: ResourceLocation1 Access policy: LDAP_policy for LDAP_app Routing Exception : None Higher priority	App name: SSH_app Destination URL: example.com Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Lower priority	Both example.com:389 and example.com:22 are resolved via Secure Private Access(Resourcelocation1). example.com:389 is launched successfully. example.com:22 fails to launch as it is supposed to go via External. **Note:** It is not recommended to configure the same domain to go via External and Internal. This limitation is only for FQDN.
App name: LDAP_app Destination URL: example.com Port Number:389 Selected routing in application: • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access Policy :LDAP_policy for LDAP_app Routing Exception : None Lower priority	App name: SSH_app Destination URL: example.com Port Number:22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access Policy:SSH_policy for SSH_app Routing Exception: External Higher priority	Both example.com:389, example.com:22 are launched via External.
App name: LDAP_app Destination URL: 10.0.0.1 Port Number: 389 Selected routing in application: • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: LDAP_policy for LDAP_app Routing Exception: None Higher priority	App name: SSH_app Destination URL: 10.0.0.1 Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Lower priority	10.0.0.1:389 is launched via Secure Private Access (ResourceLocation1). 10.0.0.1:22 is launched via External.
App name: LDAP_app Destination URL: 10.0.0.1 Port Number: 389 Selected routing in application: • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy : LDAP_policy for LDAP_app Routing Exception: None Lower priority	App name: SSH_app Destination URL: 10.0.0.1 Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Higher priority	10.0.0.1:389 is launched via Secure Private Access (ResourceLocation1). 10.0.0.1:22 is launched via External.

Secure Private Access コンソールで証明書を管理する

Secure Private Access 証明書ストアは、管理者が認証局 (CA) 証明書と Secure Sockets Layer (SSL) 証明書の両方を効率的に管理するための一元的な場所を提供します。この専用ストアによ

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

り、管理者は新しい証明書をシームレスに追加し、既存の証明書を変更し、不要になった証明書を削除できるため、証明書管理が簡素化されます。

以前は、Secure Private Access 証明書は NetScaler® Console の証明書ストアに保存されていました。専用の Secure Private Access 証明書ストアが導入されたため、NetScaler Console 内で管理されている証明書は、Secure Private Access 内で自動的に同期されたり、使用できなくなりました。管理者は、必要な証明書を Secure Private Access コンソールに直接アップロードする必要があります。

Secure Private Access で使用される証明書は、 ページ内の 2 つのタブに整理されています。

- **サーバー** - 主にダイレクトアクセス (エージェントレスアクセス) 操作に関連する SSL サーバー証明書を含む証明書のリストです。
- **マシン認証** - Citrix Secure Access™ クライアントから開始されるマシントンネルの管理に関連する証明書のリストです。これらの証明書は、管理者が Citrix Secure Access クライアントにログインするときに使用されます。

  マシン認証証明書は、Always On 機能に不可欠であり、信頼された認証局 (CA) によって発行されたデバイス証明書を利用します。これらの CA 証明書は、 タブ (**設定 > 証明書ストア**) 内で安全にアップロードおよび管理され、Always On 機能のシームレスで堅牢なデバイス認証を保証します。

マシン認証証明書を管理する

以下のセクションでは、マシン認証証明書の管理に関する詳細情報を提供します。

証明書を追加する

マシン認証証明書を追加する手順。

1. **設定 > 証明書ストア** に移動します。

   > **注:**
   >
   > **設定 > マシンベース認証** ではなく、**設定 > 証明書ストア** にある **マシンベース認証** オプションを使用することをお勧めします。**設定 > マシンベース認証** オプションは、今後のサービスリリースで削除される予定です。

2. **マシン認証** タブをクリックし、**証明書の追加** をクリックします。
3. 「**名前**」に証明書の名前を入力します。
4. 「**証明書ファイル**」で、ローカルドライブを参照して証明書ファイルをアップロードします。

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

- ルートCAと中間CAの両方の証明書がサポートされています。
- アップロードする証明書はPEM形式で、チェーン全体を含める必要があります。証明書は、中間証明書からルートCAまで生成されている必要があります。

5. 「**保存**」をクリックします。

証明書は、「**マシン認証**」タブの利用可能な証明書のリストに追加されます。

マシン認証証明書を追加(/en-us/citrix-secure-private-access/media/spa-cert-store-machine-authentication.png)

証明書を無効にする

「**ステータス**」列のトグルスイッチをオフにスライドすると、使用されなくなった証明書を無効にできます。

証明書を削除する

1. 削除アイコンをクリックして証明書を削除します。

証明書の優先順位を設定する

同じマシンで複数の証明書が使用されている場合、「**優先順位**」列の上下ドラッグアイコンを使用して証明書の優先順位を変更できます。

SSL証明書を管理する

以下のセクションでは、SSL証明書の管理に関する詳細情報を提供します。

証明書を追加

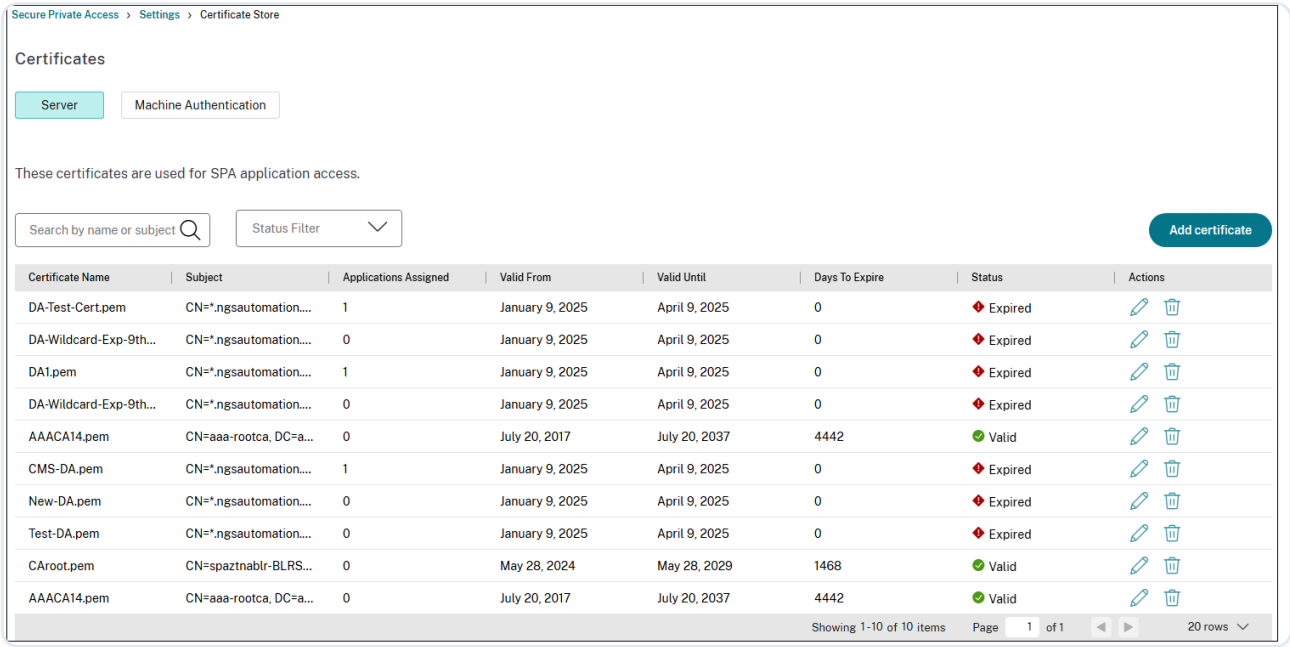
SSL証明書を追加する手順。

1. **設定 > 証明書ストア**に移動します。
2. **サーバー**タブをクリックします。
3. 証明書の名前を入力します。
4. **証明書ファイル**で、ローカルドライブを参照して証明書ファイルをアップロードします。

    - ルートCAと中間CAの両方の証明書がサポートされています。
    - アップロードする証明書はPEM形式で、チェーン全体を含める必要があります。証明書は、中間証明書からルートCAまで生成されている必要があります。

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

5. **パスワード** (オプション) - PFX証明書に適用されます。暗号化されたRSA秘密鍵をお持ちの場合は、秘密鍵の暗号化に使用されたRSAパスフレーズを入力します。
6. **保存**をクリックします。



注:

- 証明書は、**サーバー**タブの下にある利用可能な証明書のリストに追加されます。
- **割り当てられたアプリケーション**列には、証明書が割り当てられているアプリケーションの数が表示されます。

証明書を検索

証明書名またはサブジェクトでSSL証明書を検索できます。証明書のステータスに基づいて証明書を検索することもできます。

SSL証明書の検索(/en-us/citrix-secure-private-access/media/spa-cert-store-server-search.png)

証明書の変更

SSL証明書を変更する手順。

1. 証明書の横にある編集アイコンをクリックします。
2. **証明書ファイル**で、ローカルドライブを参照し、変更された証明書ファイルをアップロードします。

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

更新された証明書が同じドメインまたはワイルドカードドメインのものであることを確認してください。そうしないと、アップロードは失敗します。

3. **保存**をクリックします。

証明書の削除

削除アイコンをクリックして証明書を削除します。

外部通知

顧客アカウント内の証明書の有効期限が近づいている場合、有効期限が切れるまでの30日間の期間内に、特定の顧客管理者に電子メール通知が自動的に送信されます。

Citrix Secure Access™ クライアント

Citrix Secure Private Access を使用すると、マシン上で実行されている Citrix Secure Access クライアントを介して、ネイティブブラウザまたはネイティブクライアントアプリケーションのいずれかを使用して、TCP/UDP および HTTPS アプリを含むすべてのプライベートアプリにアクセスできるようになります。リモートユーザーがすべてのプライベートアプリにアクセスするために、従来の VPN ソリューションへの依存を排除できるようになりました。

Windows 用 Citrix Secure Access クライアント

Windows 用 Citrix Secure Access クライアントのインストールについては、「Windows 用 Citrix Secure Access クライアントのインストール」を参照してください。

Windows 用 Citrix Secure Access クライアントの詳細については、「Windows 用 Citrix Secure Access」を参照してください。

macOS 用 Citrix Secure Access クライアント

macOS 用 Citrix Secure Access クライアントのインストールについては、「macOS 用 Citrix Secure Access クライアントのインストール」を参照してください。

macOS 用 Citrix Secure Access クライアントの詳細については、「macOS 用 Citrix Secure Access」を参照してください。

iOS 用 Citrix Secure Access クライアント

iOS 用 Citrix Secure Access クライアントのセットアップについては、「iOS 用 Citrix Secure Access のセットアップ」を参照してください。

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

iOS 用 Citrix Secure Access クライアントの詳細については、「iOS 用 Citrix Secure Access」を参照してください。

Android 用 Citrix Secure Access クライアント

Android 用 Citrix Secure Access クライアントのセットアップについては、「Android 用 Citrix Secure Access のセットアップ」を参照してください。

Android 用 Citrix Secure Access クライアントの詳細については、「Android 用 Citrix Secure Access」を参照してください。

Linux 用 Citrix Secure Access クライアント

Linux 用 Citrix Secure Access クライアントのインストールについては、Citrix Secure Access クライアントと Citrix EPA クライアントのインストールを参照してください。

Linux 用 Citrix Secure Access クライアントの詳細については、Citrix Secure Access for Linuxを参照してください。

WebおよびSaaSアプリケーション構成のベストプラクティス

公開済みおよび未公開のアプリのアプリケーションアクセスは、Secure Private Accessサービス内で構成されたアプリケーションとアクセスポリシーによって異なります。

Secure Private Accessにおける公開済みおよび未公開アプリのアプリケーションアクセス

- **公開済みWebアプリケーションおよび関連ドメインへのアクセス:**
  - エンドユーザーが公開済みWebアプリに関連付けられているFQDNにアクセスする場合、そのユーザーに対して**許可**または**制限付きで許可**のアクションが明示的に設定されたアクセスポリシーがある場合にのみ、アクセスが許可されます。

> **注:**
>
> 複数のアプリケーションが、完全に一致する同じアプリケーションURLドメインまたは関連ドメインを共有しないことをお勧めします。複数のアプリが同じアプリケーションURLドメインまたは関連ドメインを共有している場合、アクセスは正確なFQDNの一致とポリシーの優先順位に基づいて提供されます。詳細については、「アクセスポリシーの一致と優先順位付け」を参照してください。

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

- 公開済みアプリと一致するアクセスポリシーがない場合、またはアプリがどのアクセスポリシーとも関連付けられていない場合、デフォルトでアプリへのアクセスは拒否されます。アクセスポリシーの詳細については、「アダプティブアクセスポリシーの構成と管理」を参照してください。

- **未公開の内部Webアプリケーションおよび外部インターネットURLへのアクセス:**

  ゼロトラストを有効にするため、Secure Private Accessは、アプリケーションに関連付けられておらず、アプリケーション用にアクセスポリシーが構成されていない内部Webアプリケーションまたはイントラネット URLへのアクセスを拒否します。特定のユーザーへのアクセスを許可するには、イントラネットWebアプリケーション用にアクセスポリシーが構成されていることを確認してください。

  Secure Private Access内でアプリケーションとして構成されていないURLの場合、トラフィックはインターネットに直接流れます。

  - そのような場合、イントラネットWebアプリケーションURLドメインへのアクセスは直接ルーティングされるため、アクセスは拒否されます（ユーザーがすでにイントラネット内にいる場合を除く）。
  - 未公開のインターネットURLの場合、アクセスは、有効になっている場合は未承認アプリ用に構成されたルールに基づきます。デフォルトでは、このアクセスはSecure Private Access内で許可されます。

アクセスポリシーの一致と優先順位付け

Secure Private Accessは、アクセスするアプリケーションを照合する際に、次の処理を行います。

1. アクセスされているドメインを、アプリケーションURLのドメインまたは関連ドメインに完全一致させます。
2. 完全なFQDN一致で構成されたSecure Private Accessアプリケーションが見つかった場合、Secure Private Accessはそのアプリケーション用に構成されたすべてのポリシーを評価します。
   - ユーザーコンテキストが一致するまで、ポリシーは優先順位に従って評価されます。アクション (許可/拒否) は、優先順位で最初に一致したポリシーに従って適用されます。
   - ポリシーが一致しない場合、アクセスはデフォルトで拒否されます。
3. 完全なFQDN一致が見つからない場合、Secure Private Accessは、最長一致 (ワイルドカード一致など) に基づいてドメインを照合し、アプリケーションと対応するポリシーを見つけます。

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

例1: 次のアプリとポリシー構成を考慮してください。

アプリケーション	アプリケーションURL	関連ドメイン
イントラネット	`https://app.intranet.local`	*.cdn.com
ウィキ	`https://wiki.intranet.local`	*.intranet.local

ポリシー名	優先度	ユーザーと関連アプリ
PolicyA	高	Eng-User5 (イントラネット)
PolicyB	低	HR-User4 (ウィキ)

もし `HR-User4` が `app.intranet.local` にアクセスした場合、次のようになります。

a. Secure Private Access は、アクセスされているドメイン (この場合は `app.intranet.local`) の完全一致をすべてのポリシーで検索します。
b. Secure Private Access は `PolicyA` を見つけ、条件が一致するかどうかを確認します。
c. 条件が一致しないため、Secure Private Access はここで停止し、ワイルドカードの一致の確認を続行しません。たとえ `PolicyB` が一致し（`app.intranet.local` は Wiki アプリの関連ドメイン `*.intranet.local` と一致するため）アクセスが許可されたとしても、です。
d. したがって、`HR-User4` は Wiki アプリへのアクセスを拒否されます。

例 2: 複数のアプリケーションで同じドメインが使用されている、以下のアプリとポリシー構成を検討します。

アプリケーション	アプリケーションURL	関連ドメイン
App1	xyz.com	app.intranet.local
App2	app.intranet.local	-

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

ポリシー名	優先度	ユーザーと関連アプリ
PolicyA	高	英語ユーザー5 (アプリ1)
PolicyB	低	HR-ユーザー7 (アプリ2)

ユーザー `Eng-User5` が `app.intranet.local` にアクセスすると、App1 と App2 の両方が正確な FQDN マッチに基づいて一致するため、`Eng-User5` ユーザーは `PolicyA` を介してアクセスできます。

ただし、App1 が関連ドメインとして `*.intranet.local` を持っていた場合、`app.intranet.local` が `PolicyB` に正確に一致し、そのユーザー `Eng-User5` はアクセス権を持たないため、`Eng-User5` へのアクセスは拒否されていたでしょう。

アプリ構成のベストプラクティス

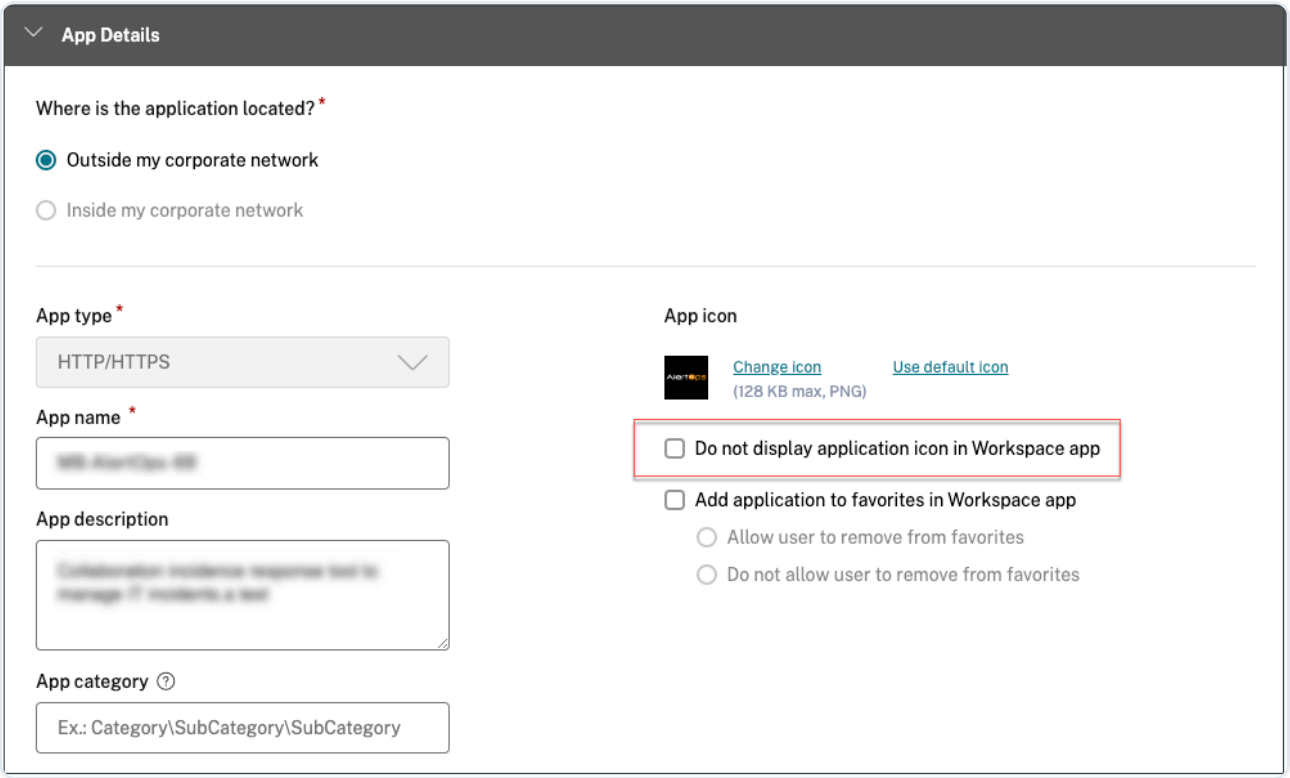
以下のセクションでは、アプリケーション構成のベストプラクティスに関する詳細情報を提供します。

IdP ドメインは独自のアプリケーションを持つ必要があります

イントラネットアプリ構成に関連ドメインとして IdP ドメインを追加する代わりに、以下をお勧めします。

- すべての IdP ドメインに対して個別のアプリケーションを作成します。
- IdP 認証ページへのアクセスを必要とするすべてのユーザーにアクセスを許可するポリシーを作成し、そのポリシーを最優先にします。
- アプリ構成からこのアプリを非表示にします（**ユーザーにアプリケーションアイコンを表示しない**オプションを選択して）、ストアに列挙されないようにします。詳細については、アプリケーションの詳細を構成する を参照してください。

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



注:

このアプリ構成は、IdP 認証ページへのアクセスのみを有効にします。個々のアプリケーションへのさらなるアクセスは、引き続き個々のアプリ構成とそれぞれのアクセスポリシーに依存します。

構成例：

1. すべての共通FQDNをそれぞれのアプリに構成し、該当する場合はグループ化します。

   たとえば、Azure ADをIdPとして使用するいくつかのアプリがあり、`login.microsoftonline.com`およびその他の関連ドメイン（`*.msauth.net`）を構成する必要がある場合は、次の手順を実行します:

   - アプリケーションURLとして`https://login.microsoftonline.com`を、関連ドメインとして`*.login.microsoftonline.com`と`*.msauth.net`を設定した単一の共通アプリケーションを作成します。

2. アプリを構成する際に、**ユーザーにアプリケーションアイコンを表示しない**オプションを選択します。詳細については、「アプリケーションの詳細を構成する」を参照してください。
3. 共通アプリケーションのアクセスポリシーを作成し、すべてのユーザーへのアクセスを有効にします。詳細については、「アクセスポリシーを構成する」を参照してください。

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

4. アクセスポリシーに最高の優先順位を割り当てます。詳細については、「優先順位」を参照してください。
5. 診断ログを検証して、FQDNがアプリと一致し、ポリシーが期待どおりに適用されていることを確認します。

同じ関連ドメインを複数のアプリケーションの一部にすることはできません

関連ドメインはアプリに対して一意である必要があります。構成が競合すると、アプリのアクセスに関する問題が発生する可能性があります。複数のアプリが同じFQDNまたはワイルドカードFQDNの何らかのバリエーションで構成されている場合、次の問題が発生する可能性があります:

- Webサイトの読み込みが停止するか、空白のページが表示されることがあります。
- URLにアクセスしたときに、**アクセスがブロックされました**ページが表示されることがあります。
- ログインページが読み込まれないことがあります。

したがって、一意の関連ドメインを単一のアプリ内で構成することをお勧めします。

誤った構成例：

- **例: 複数のアプリケーションにわたる重複する関連ドメイン**

  Okta (example.okta.com) へのアクセスが必要な2つのアプリがあるとします。

アプリ	アプリケーションURLドメイン	関連ドメイン
App1	`https://code.example.net`	example.okta.com
App2	`https://info.example.net`	example.okta.com

ポリシー名	優先度	ユーザーと関連アプリ
HRへのApp1のアクセスを拒否	高	`App1` のユーザーグループ `HR`
App1への全員のアクセスを許可する	中	App1へのユーザーグループ「全員」のアクセスを有効にする

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

ポリシー名	優先度	ユーザーと関連アプリ
App2への全員のアクセスを許可する	低	App2へのユーザーグループ「全員」のアクセスを有効にする

構成の問題点: App2にすべてのユーザーがアクセスできるようにする意図があったにもかかわらず、ユーザーグループHRはApp2にアクセスできません。ユーザーグループHRはOktaにリダイレクトされますが、App1へのアクセスを拒否した最初のポリシー（App2と同じ関連ドメイン`example.okta.com`を持つ）に基づいてブロックされます。

このシナリオはOktaなどのIDプロバイダーでよく見られますが、共通の関連ドメインを持つ他の密接に統合されたアプリでも発生する可能性があります。ポリシーの一致と優先順位付けの詳細については、「アクセスポリシーの一致と優先順位付け」を参照してください。

上記の構成に関する推奨事項:

a. example.okta.comをすべてのアプリから関連ドメインとして削除します。
b. Okta専用の新しいアプリを作成します（アプリケーションURLは`https://example.okta.com`、関連ドメインは`*.okta.com`）。
c. このアプリをストアから非表示にします。
d. 競合を解消するために、ポリシーに最高の優先順位を割り当てます。

ベストプラクティス:

- あるアプリの関連ドメインは、別のアプリの関連ドメインと重複してはなりません。
- この状況が発生した場合、共有された関連ドメインをカバーするために新しい公開済みアプリを作成し、それに応じてアクセスを設定する必要があります。
- 管理者は、この共有された関連ドメインがストアに実際のアプリとして表示される必要があるかどうかを評価する必要があります。
- アプリをストアに表示しない場合は、アプリの公開時に**ユーザーにアプリケーションアイコンを表示しない**オプションを選択して、ストアから非表示にします。

同じ関連ドメインに起因する競合の解決

あるアプリの関連ドメインが別のアプリのドメインと重複するシナリオでは、管理者は特定の要件に基づいて、これらのアプリケーションを外部またはコネクタアプライアンス経由で内部にルーティングする柔軟性があります。 Secure Private Accessコンソール（**設定 > アプリケーションドメイン**）内のルーティングテーブルには、すべてのアプリケーション用に構成されたすべてのドメ

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

インの包括的なリストが表示されます。このテーブルには、ルーティングタイプを含む各ドメインに関する主要な情報が表示されます。管理者は、対応するドメインエントリの横にある編集アイコンをクリックすることで、ルーティングタイプを簡単に変更できます。

メインルーティングテーブルには、任意のドメインについて次の情報が表示されます。

- **FQDN/IP:** トラフィックルーティングの種類を設定したいFQDNまたはIPアドレス。
- **タイプ:** アプリのタイプ。アプリの追加時に選択された**内部**、**内部 – プロキシバイパス**、または**外部**。
  - **内部** - アプリは外部ですが、トラフィックはコネクタアプライアンスを介して外部ネットワークに流れる必要があります。
  - **内部 – プロキシバイパス** - ドメイントラフィックはCitrix Cloud Connector™を介してルーティングされ、コネクタアプライアンスで構成された顧客のWebプロキシをバイパスします。
  - **外部** – トラフィックはインターネットに直接流れます。

  重要:

  競合がある場合、テーブルの該当する行に警告アイコンが表示されます。競合を解決するには、管理者はそのエントリに関連付けられた三角形のアイコンをクリックして、アプリのタイプを変更する必要があります。

- **リソースロケーション:** 内部タイプのルーティングのリソースロケーション。リソースロケーションが割り当てられていない場合、該当するアプリのリソースロケーション列に三角形のアイコンが表示されます。アイコンにカーソルを合わせると、次のメッセージが表示されます。

  リソースロケーションがありません。このFQDNにリソースロケーションが関連付けられていることを確認してください。

- **ステータス:** ステータス列のトグルスイッチを使用して、アプリを削除せずにルートエントリのルートを無効にできます。トグルスイッチがオフの場合、ルートエントリは有効になりません。また、完全一致のFQDNが存在する場合、管理者は有効または無効にするルートを選択できます。
- **コメント:** コメントがあれば表示されます。
- **アクション:** 編集アイコンは、リソースロケーションを追加したり、ルートエントリのタイプを変更したりするために使用されます。削除アイコンは、ルートを削除するために使用されます。

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

注:

アプリケーション設定中にルーティングの決定を行うために、アプリケーションドメインテーブルのミニバージョンが利用可能です。ミニルートテーブルは、Citrix Secure Private Access™サービス管理コンソールのアプリケーション接続セクションで利用できます。

ディープリンクURL

ディープリンクURLの場合、イントラネットアプリケーションのURLドメインを関連ドメインとして追加する必要があります。

例:

イントラネットアプリのURLは、メインアプリケーションURLドメインとして `https://example.okta.com/deep-link-app-1` が設定されており、関連ドメインにはイントラネットアプリケーションURLドメイン、つまり `*.issues.example.net` があります。

この場合、URL `https://example.okta.com` を持つIdPアプリを個別に作成し、関連ドメインとして `*.example.okta.com` を設定します。

アプリへのアクセスに関するエンドユーザーエクスペリエンスの説明

Citrix Secure Private Access™ アプリには、次の方法でアクセスできます。

- **Citrix Secure Access™ クライアント経由:**
  - Web/SaaS アプリへのアクセス: Citrix Secure Access クライアントにログインした後、エンドユーザーは Chrome などのネイティブブラウザを使用して Web/SaaS アプリにアクセスできます。
  - TCP/UDP アプリへのアクセス: Citrix Secure Access クライアントにログインした後、エンドユーザーはクライアントアプリケーション（例: リモートデスクトッププロトコル (RDP)）を介して TCP/UDP アプリケーションにアクセスできます。
- **エージェントレスアクセス:** クライアントを必要とせずに、ユーザーがエンタープライズ Web アプリにアクセスできるようにします。エンドユーザーは、デバイスに専用クライアントをインストールすることなく、エンタープライズ Web アプリケーションにアクセスできます。エンドユーザーは、ネイティブブラウザにアプリの URL を入力するだけで済みます。

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

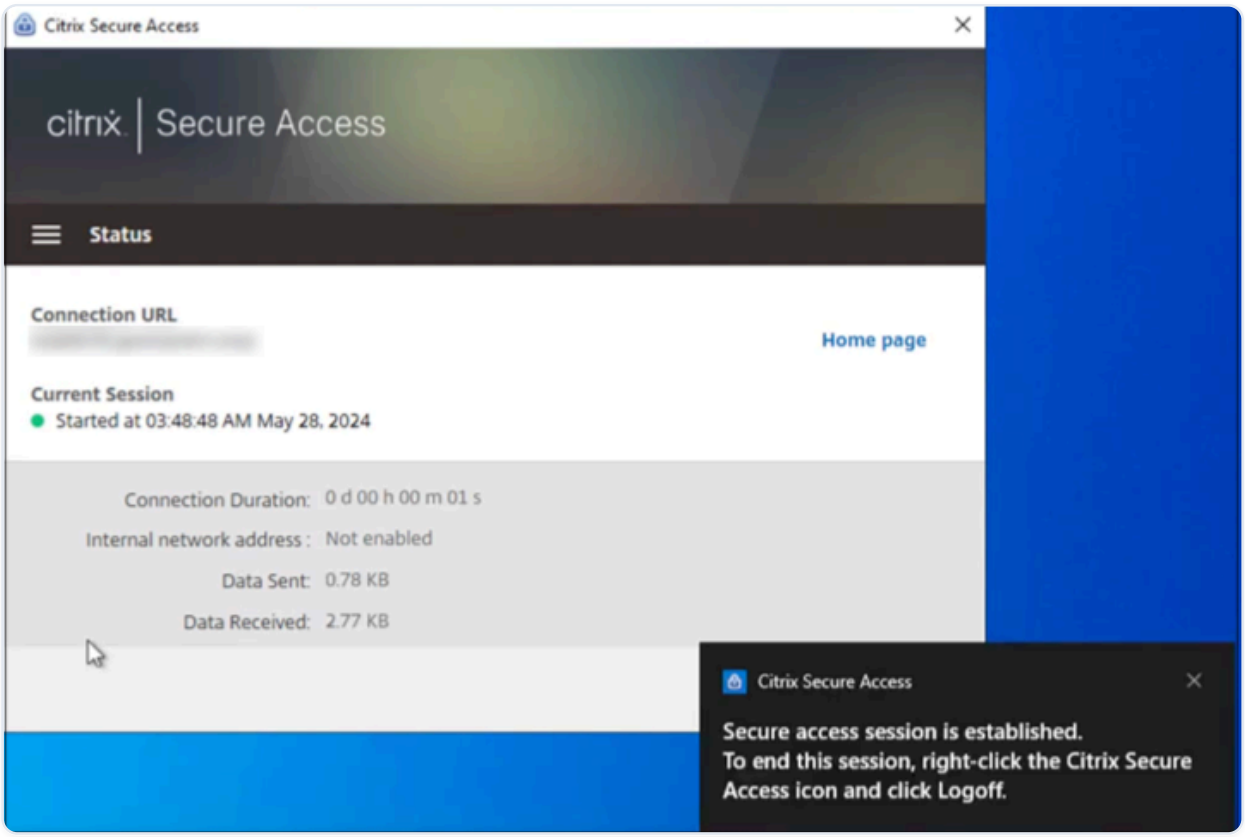
Citrix Secure Access クライアントを介して Web アプリにアクセスする

1. Citrix Secure Access クライアントにログインします。
2. セキュアアクセスセッションが確立されたら、ネイティブブラウザ（例: Chrome）を開きます。
3. ブラウザで、アクセスしたいエンタープライズ Web アプリの URL を入力します。

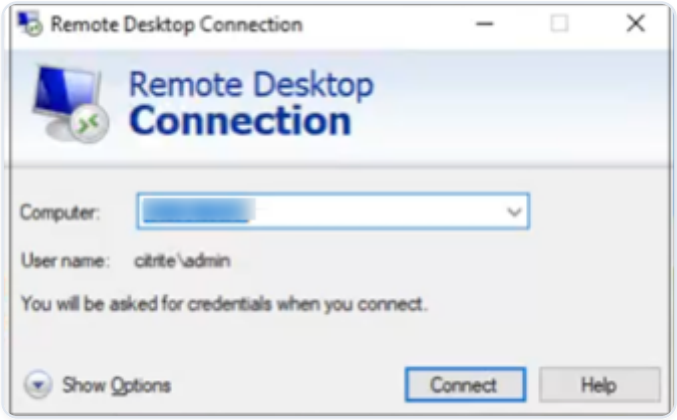
Citrix Secure Access クライアントを介して TCP/UDP アプリにアクセスする

RDP が構成されている場合、エンドユーザーは TCP/UDP アプリにアクセスするために次の手順を実行する必要があります。

1. Citrix Secure Access クライアントにログインします。
2. セキュアアクセスセッションが確立されたら、リモートデスクトップ接続を開始します。



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



a. **Windows**キーを押し、**リモートデスクトップ接続**と入力して、**Enter**キーを押します。

b. 接続しようとしているコンピューターのIPアドレスまたはホスト名を入力します。

c. **接続**をクリックします。資格情報の入力を求められる場合があります。

d. リモートコンピューターのユーザー名とパスワードを入力し、**OK**をクリックします。

これでリモートデスクトップ接続が確立され、エンドユーザーはリモートコンピューターと対話できるようになります。

Citrix Secure Accessクライアントの詳細については、Citrix Secure Accessクライアントを参照してください。

Secure Private Access 向けコネクタアプライアンス

コネクタアプライアンスは、ハイパーバイザーでホストされるCitrixコンポーネントです。これは、Citrix Cloud™ とリソースの場所間の通信チャネルとして機能し、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を可能にします。コネクタアプライアンスを使用すると、ユーザーに価値を提供するリソースを管理し、それらに集中できます。

すべての接続は、標準のHTTPSポート (443) とTCPプロトコルを使用して、コネクタアプライアンスからクラウドへ確立されます。受信接続は許可されません。TCPポート443では、次のFQDNがアウトバウンドで許可されます。

- *.nssvc.net
- *.netscalermgmt.net
- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net
- *.citrix.com
- *.servicebus.windows.net
- *.adm.cloud.com

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

コネクタアプライアンスを使用したセキュアプライベートアクセスの構成

1. リソースの場所に2つ以上のコネクタアプライアンスをインストールします。

   コネクタアプライアンスのセットアップの詳細については、「Connector Appliance for Cloud Services」を参照してください。

2. KCDを使用してオンプレミスのWebアプリに接続するようにセキュアプライベートアクセスを構成するには、次の手順を実行してKCDを構成します。

   a. コネクタアプライアンスをActive Directoryドメインに参加させます。

      Active Directory フォレストに参加すると、Secure Private Access の構成時に Kerberos Constrained Delegation (KCD) を使用できるようになりますが、ID リクエストや認証で Connector Appliance を使用できるようにはなりません。

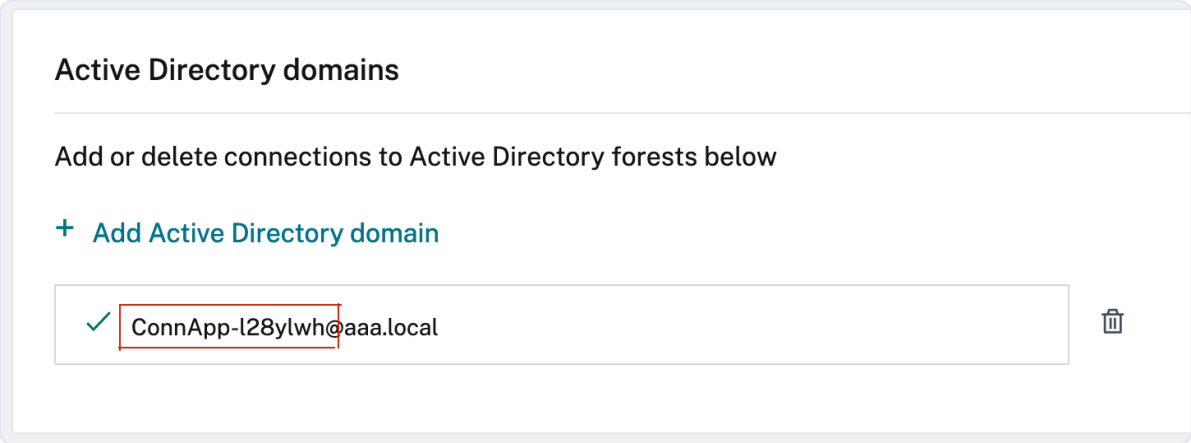
      - Connector Appliance コンソールに表示されている IP アドレスを使用して、ブラウザで Connector Appliance の管理ウェブページに接続します。
      - **Active Directory ドメイン**セクションで、**+ Active Directory ドメインの追加**をクリックします。

        管理ページに**Active Directory ドメイン**セクションがない場合は、Citrix® に連絡してプレビューへの登録をリクエストしてください。
      - **ドメイン名**フィールドにドメイン名を入力します。**追加**をクリックします。
      - Connector Appliance がドメインをチェックします。チェックが成功すると、**Active Directory に参加**ダイアログが開きます。
      - このドメインへの参加権限を持つ Active Directory ユーザーのユーザー名とパスワードを入力します。
      - Connector Appliance がマシン名を提案します。提案された名前を上書きして、最大15文字の独自のマシン名を入力できます。マシンアカウント名をメモしておいてください。

        このマシン名は、Connector Appliance が Active Directory ドメインに参加するときに作成されます。
      - **参加**をクリックします。

   b. ロードバランサーなしでWebサーバーのKerberos Constrained Delegationを構成します。

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



- コネクタアプライアンスのコンピューター名を特定します。この名前は、ホストした場所から、またはコネクタUIから取得できます。
- Active Directory コントローラーで、コネクタアプライアンスのコンピューターを探します。
- Connector Appliance コンピューターアカウントのプロパティに移動し、**委任**タブに移動します。
- **指定されたサービスへの委任に対してこのコンピューターを信頼する**を選択し、次に**任意の認証プロトコルを使用する**を選択します。

  認証プロトコル(/en-us/citrix-secure-private-access/media/connector-appliance-authentication-protocol.png)
- **追加**をクリックします。
- **ユーザーまたはコンピューター**をクリックします。
- ターゲットWebサーバーのコンピューター名を入力し、**名前の確認**をクリックします。上記の画像では、**KCD2K8**がWebサーバーです。 Webサーバーのターゲット(/en-us/citrix-secure-private-access/media/connector-appliance-check-names.png)
- **OK**をクリックします。
- サービスの種類として**http**を選択します。

  HTTPサービスの種類(/en-us/citrix-secure-private-access/media/connector-appliance-service-type.png)
- **OK**をクリックします。
- **適用**をクリックし、次に**OK**をクリックします。

  Webサーバーが追加されました(/en-us/citrix-secure-private-access/media/connector-appliance-webserver-added.png)

これで、Webサーバーの委任を追加する手順は完了です。

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

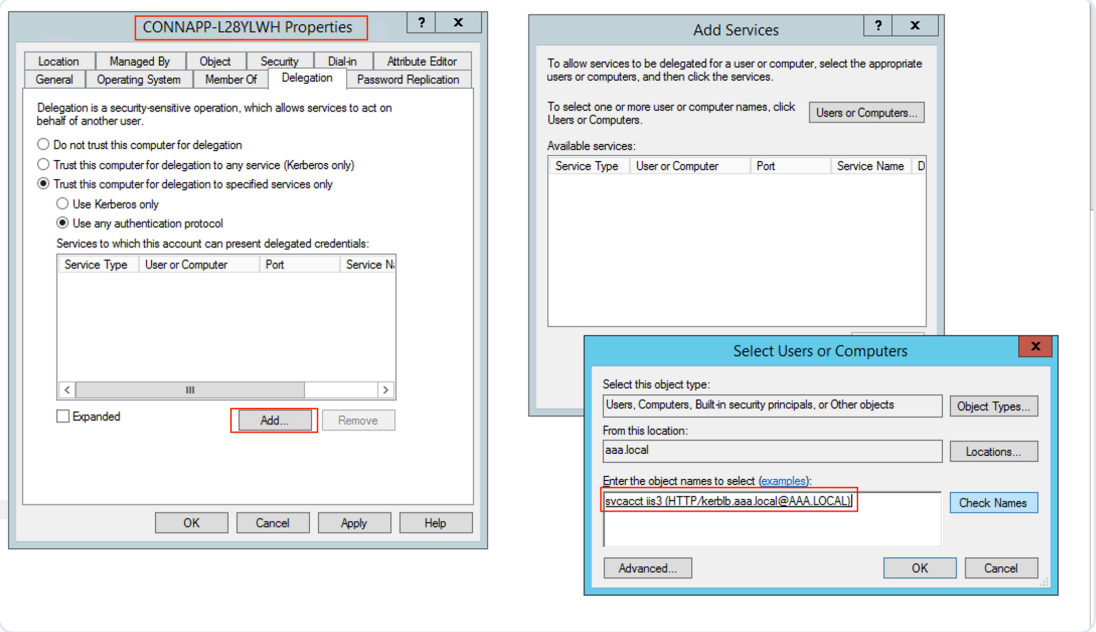
c. ロードバランサーの背後にあるWebサーバーのKerberos制約付き委任（KCD）を構成します。

- 次の `setspn` コマンドを使用して、ロードバランサーのSPNをサービスアカウントに追加します。 `setspn -S HTTP/<web_server_fqdn> <service_account>`

  SPNの設定(/en-us/citrix-secure-private-access/media/connector-appliance-setspn.png)

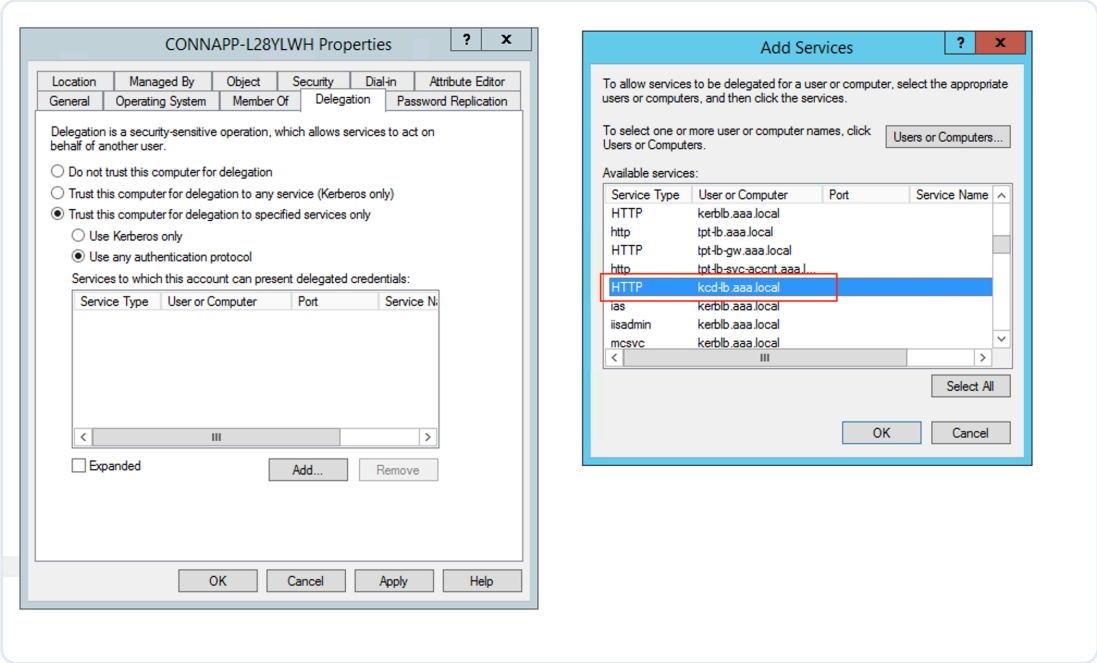
- 次のコマンドを使用して、サービスアカウントのSPNを確認します。 `setspn -l <service_account>`

- コネクタアプライアンスのコンピューターアカウントの委任を作成します。
  - ロードバランサーなしで *Webサーバーの*Kerberos*制約付き委任を構成する* の手順に従って、CAマシンを特定し、委任UIに移動します。
  - **ユーザーとコンピューター**を選択し、サービスアカウント（例: aaa\svc_iis3）を選択します。



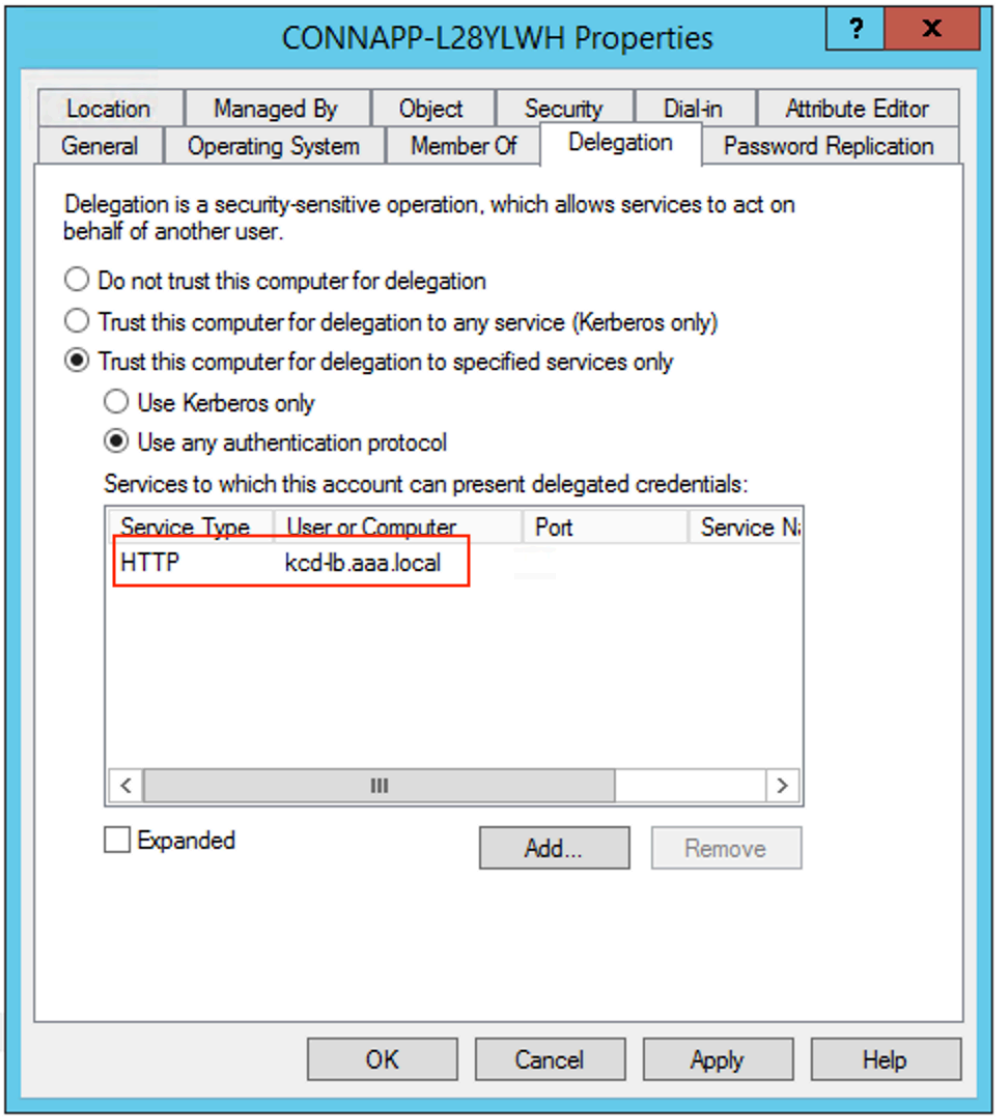
  - サービスで、**ServiceType: HTTP**のエントリとユーザーまたはコンピューター: Webサーバー（例: `kcd-lb.aaa.local` ）を選択します。

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



- **OK**をクリックします。
- **適用**をクリックし、**OK**をクリックします。

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



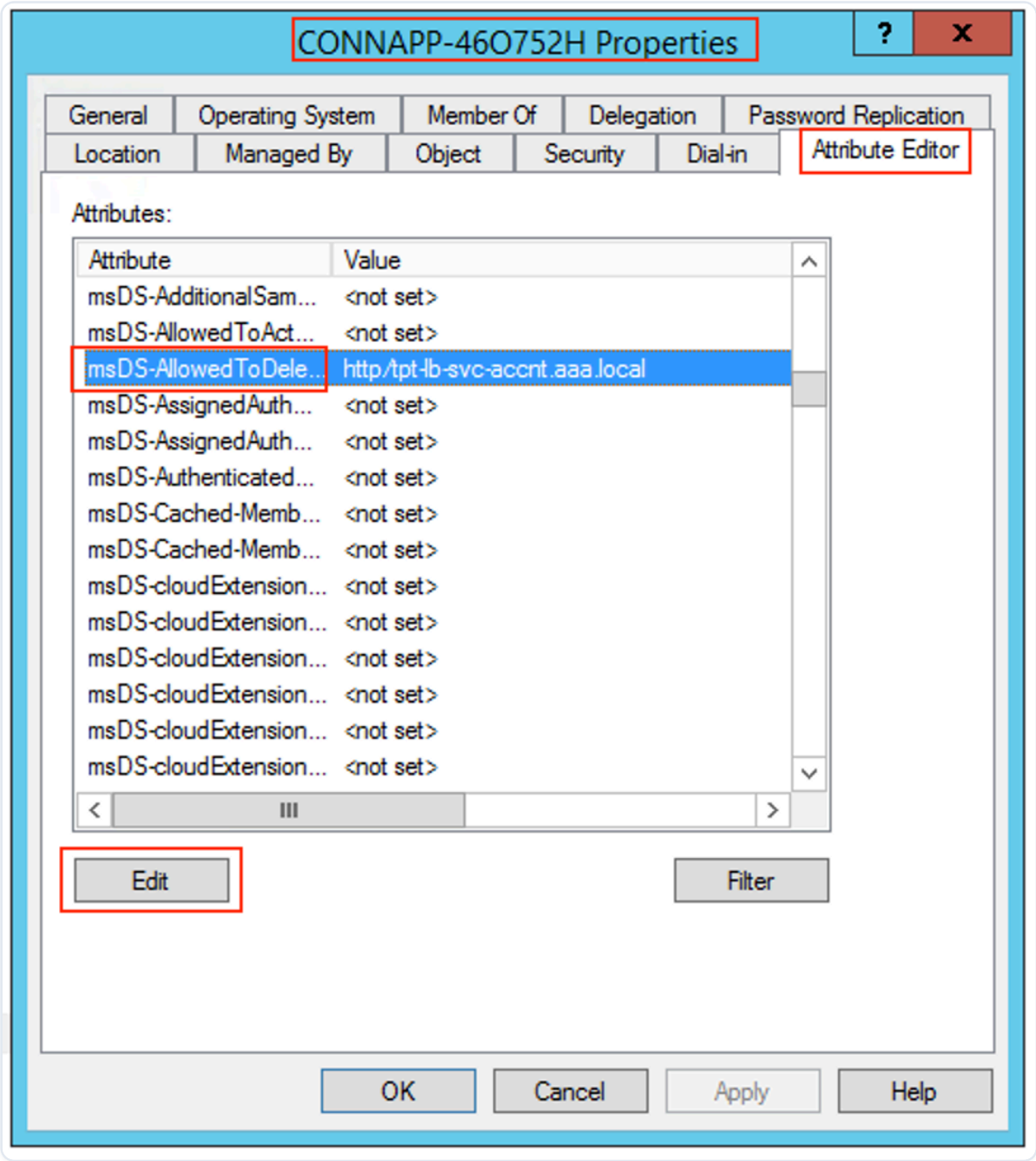
d. グループ管理サービスアカウントのKerberos制約付き委任（KCD）を構成します。

- まだ追加していない場合は、グループ管理サービスアカウントにSPNを追加します。
  `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- 次のコマンドを使用してSPNを確認します。 `setspn -l <group_manged_service_account>`

グループ管理サービスアカウントは、コンピューターアカウントの委任エントリを追加する際に `Users and Computers` 検索に表示されないため、通常の方法でコンピューターアカウントの委任を追加することはできません。したがって、属性エディターを介して、このSPNをCAコンピューターアカウントへの委任エントリとして追加できます。

- Connector Applianceのコンピュータープロパティで、**属性エディター**タブに移動し、`msDA-AllowedToDeleteTo` 属性を探します。
- `msDA-AllowedToDeleteTo attribute` を編集し、SPNを追加します。

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



)

属性エディター2(/en-us/citrix-secure-private-access/media/connector-appliance-attribute-editor-managed-account2.png))

e. シトリックス ゲートウェイ コネクタ™ から シトリックス コネクタ アプライアンス へ移行します。

- ゲートウェイコネクタを構成する際にSPNはすでにサービスアカウントに設定されているため、新しいKerberosアプリが構成されていない場合、サービスアカウントにこれ以上SPNを追加する必要はありません。以下のコマンドでサービスアカウントに割り当てられているすべてのSPNのリストを表示し、それらをCAコンピューターアカウントの委任エントリとして割り当てることができます。

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

```
setspn -l <service_account>
```

SPNを設定(/en-us/citrix-secure-private-access/media/connector-appliance-migration-setspn.png)

この例では、SPN (`kcd-lb.aaa.local, kcd-lb-app1.aaa.local, kcd-lb-app2.aaa.local, kcd-lb-app3.aaa.local`) はKCD用に構成されています。

- 必要なSPNをコネクタアプライアンスのコンピューターアカウントに委任エントリとして追加します。詳細については、「*コネクタアプライアンスのコンピューターアカウントの委任を作成する*」の手順を参照してください。

コンピューターアカウントにSPNを追加(/en-us/citrix-secure-private-access/media/connector-appliance-migration-kcd.png)

この例では、必要なSPNはCAコンピューターアカウントの委任エントリとして追加されています。

注: これらのSPNは、ゲートウェイコネクタを構成する際に、委任エントリとしてサービスアカウントに追加されました。サービスアカウントの委任から移行するため、これらのエントリはサービスアカウントの**委任**タブから削除できます。

f. Citrix Secure Private Access™ サービスをセットアップするには、Citrix Secure Private Access™ のドキュメントに従ってください。セットアップ中に、Citrix Cloud はコネクタアプライアンスの存在を認識し、それらを使用してリソースの場所に接続します。

- Citrix Secure Private Access の使用を開始する
- Citrix Secure Private Access を構成する
- クラウドサービス用コネクタアプライアンス
- インターネット接続要件。
- エンタープライズWebアプリのサポート

Kerberos構成の検証

シングルサインオンにKerberosを使用している場合、**Connector Appliance管理ページ**からActive Directoryコントローラーの構成が正しいことを確認できます。**Kerberos検証**機能を使用すると、Kerberosレルムのみモード構成またはKerberos制約付き委任（KCD）構成を検証できます。

1. **Connector Appliance管理ページ**に移動します。

   a. ハイパーバイザーのConnector Applianceコンソールから、IPアドレスをブラウザのアドレスバーにコピーします。

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

   b. Connector Applianceを登録したときに設定したパスワードを入力します。

2. 右上にある管理者メニューから、**Kerberos検証**を選択します。
3. **Kerberos検証**ダイアログで、**Kerberos検証モード**を選択します。
4. **Active Directoryドメイン**を指定または選択します。
   - Kerberosレルムのみモード構成を検証している場合は、任意のActive Directoryドメインを指定できます。
   - Kerberos制約付き委任構成を検証している場合は、結合されたフォレスト内のドメインのリストから選択する必要があります。
5. **サービスFQDN**を指定します。デフォルトのサービス名は`http`と想定されます。「computer.example.com」を指定した場合、これは`http/computer.example.com`と同じと見なされます。
6. **ユーザー名**を指定します。
7. Kerberosレルムのみモード構成を検証している場合は、そのユーザー名の**パスワード**を指定します。
8. **Kerberosのテスト**をクリックします。

Kerberos の構成が正しい場合、`Successfully validated Kerberos setup` というメッセージが表示されます。Kerberos の構成が正しくない場合、検証の失敗に関する情報を提供するエラーメッセージが表示されます。

スケールとサイズに関する考慮事項

この記事では、単一のリソースロケーションにある単一のConnector Applianceの同時TCP接続制限と同時Webアプリ要求制限を決定するためのガイダンスを詳述します。

WebおよびSaaSアプリケーション

Connector Appliance仮想マシンの最小推奨サイズは2 vCPUおよび4 GB RAMです。高可用性と回復性のために、2つのConnector Applianceを展開することをお勧めします。

展開ガイダンス: 2 vCPU、4 GBメモリ、10 Gbps NICのサイズのConnector Applianceは、以下をサポートできます。

- 1秒あたり最大500件のWebアプリ要求 (Secure Browse)。
- 最大1 Gbpsのデータ転送スループットレート。

これらの数値は、CPU使用率90%およびメモリ使用量80%で算出されました。

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

TCPアプリケーション

Connector Appliance仮想マシンの最小推奨サイズは2 vCPUおよび4 GB RAMです。

展開ガイダンス: 2 vCPU、4 GBメモリ、10 Gbps NICのサイズのConnector Applianceは、以下をサポートできます。

- 最大50,000の同時TCP接続。
- 最大1 Gbpsのデータ転送スループットレート。

これらの数値は、CPU使用率90%およびメモリ使用量80%で算出されました。

混合トラフィック (Web、SaaS、TCP)

展開ガイダンス: 2 vCPU および 4 GB メモリサイズのコネクタアプライアンスは、以下をサポートできます。

- 1秒あたり最大300のWebアプリリクエスト (Secure Browse)。
- 最大10,000の同時TCP接続。
- 最大1 Gbpsの全体的なデータ転送スループットレート。

これらの数値は、CPU使用率90%およびメモリ使用率80%で算出されました。

重要:

1秒あたりのWebアプリリクエスト (Secure Browse)、同時TCP接続、またはスループットの推奨制限を超えるトラフィック要件を管理するには、コネクタアプライアンスを追加して水平方向にスケールする必要があります。

コネクタ通知

コネクタは、1時間のサンプル期間でCPU使用率が80%を超えると通知を生成します。詳細については、「コネクタ通知」を参照してください。

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

適応型アクセス ポリシーの構成と管理

今日の絶えず変化する状況において、アプリケーションセキュリティはあらゆるビジネスにとって不可欠です。コンテキストを認識したセキュリティ決定を行い、アプリケーションへのアクセスを有効にすることで、ユーザーへのアクセスを可能にしながら、関連するリスクを軽減できます。

Citrix Secure Private Access™ サービスの適応型アクセス機能は、アプリケーションへのセキュアなアクセスを提供する包括的なゼロトラストアクセスアプローチを提供します。適応型アクセスにより、管理者はコンテキストに基づいてユーザーがアクセスできるアプリに対して、きめ細かなレベルのアクセスを提供できます。ここでの「コンテキスト」という用語は、以下を指します。

- ユーザーとグループ（ユーザーおよびユーザーグループ）
- デバイス（デスクトップまたはモバイルデバイス）
- 場所（地理的位置またはネットワーク上の場所）
- デバイスのポスチャ（デバイスのポスチャチェック）

適応型アクセス機能は、アクセスされているアプリケーションに適応型ポリシーを適用します。これらのポリシーは、コンテキストに基づいてリスクを判断し、Enterprise Web、SaaS、TCP、および UDP アプリへのアクセスを許可または拒否する動的なアクセス決定を行います。

仕組み

アプリケーションへのアクセスを許可または拒否するために、管理者は、ユーザー、ユーザーグループ、ユーザーがアプリケーションにアクセスするデバイス、およびユーザーがアプリケーションにアクセスしている場所（国またはネットワークの場所）に基づいてポリシーを作成します。

適応型アクセス ポリシーは、次のシナリオで評価されます。

- Secure Private Access サービスからの Web、SaaS、TCP、または UDP アプリの列挙中 – このユーザーに対してアプリケーションアクセスが拒否された場合、ユーザーはこのアプリケーションをストアで確認できません。
- アプリケーションの起動中 – アプリを列挙した後、適応型ポリシーがアクセス拒否に変更された場合、ユーザーは、以前にアプリが列挙されていても、アプリを起動できません。

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

複数のルールを持つアクセス ポリシーを作成する

単一のポリシー内で複数のアクセスルールを作成し、異なるユーザーまたはユーザーグループに対して異なるアクセス条件を構成できます。これらのルールは、HTTP/HTTPS アプリと TCP/UDP アプリの両方に個別に適用でき、すべて単一のポリシー内で設定できます。

アクセス制限は、Secure Private Access インターフェイス内ではなく、Google 管理コンソールを介して構成する必要があります。

ルールは**Google 管理コンソール > ルール**で構成されます。これらのルールは、透かしの追加、社会保障番号を含むファイルのダウンロードのブロック、URLフィルタリングなど、DLPに関連する高度な設定です。

Google 管理コンソールでGoogle Chromeのポリシーとルールを作成する方法の詳細については、次のトピックを参照してください。

- Chrome Enterprise の Chrome Enterprise コネクタポリシーを設定する
- データ保護ルール

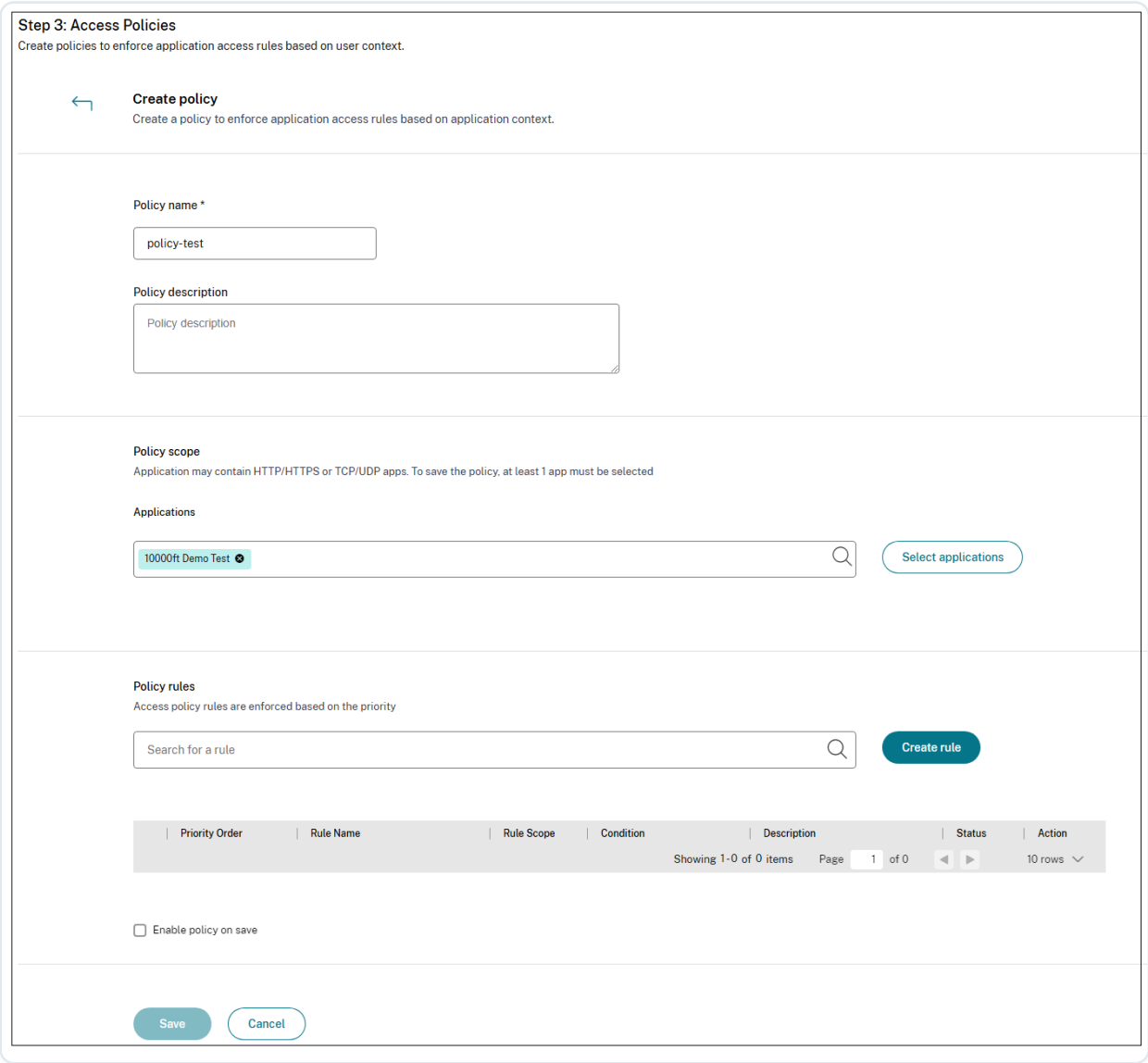
前提条件

ユーザー向けにアプリケーションが構成されていることを確認してください。詳細については、「ユーザー向けにアプリを追加する」を参照してください。

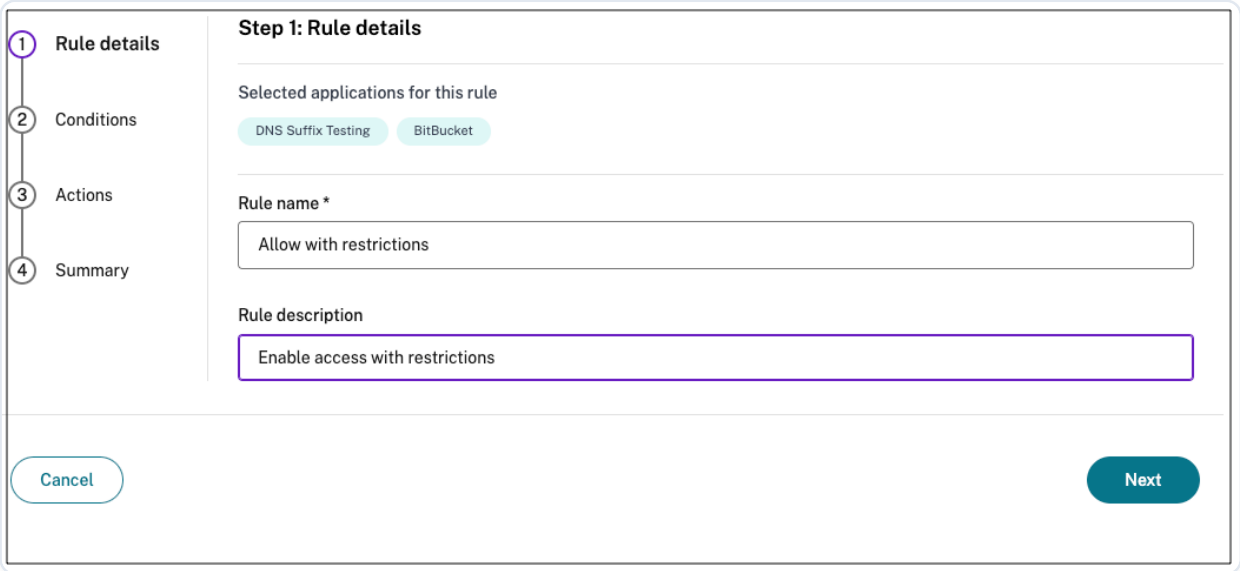
アクセスポリシーを作成する手順:

1. **アクセスポリシー**ページを開き、**ポリシーの作成**をクリックします。
2. ポリシーの名前と説明を入力します。
3. **アプリケーション**で、このポリシーを適用する必要があるアプリまたはアプリのセットを選択します。
4. **ルールの作成**をクリックして、ポリシーのルールを作成します。

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

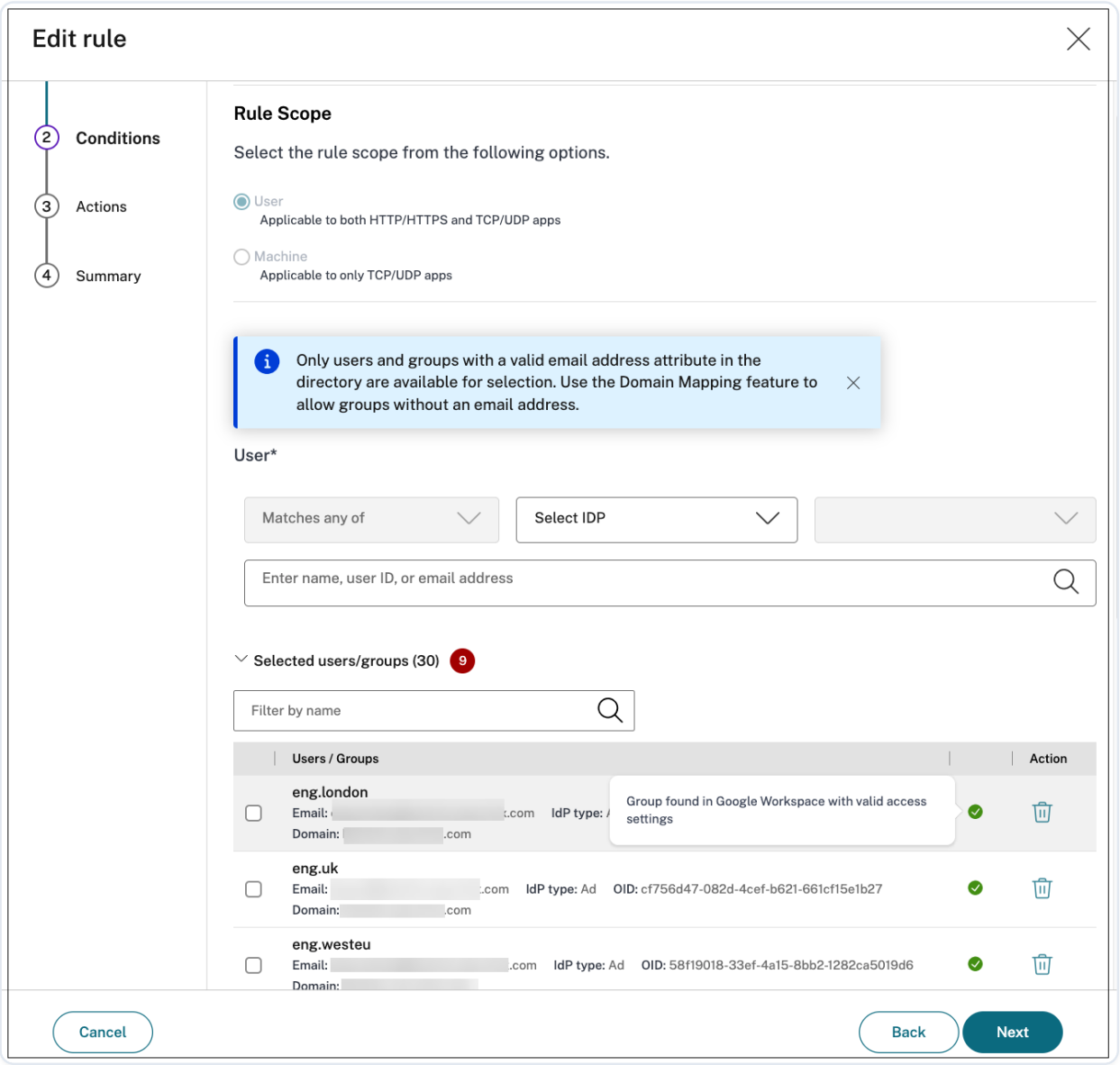


5. ルール名とルールの簡単な説明を入力し、**次へ**をクリックします。



6. ユーザーの条件を選択します。**ユーザー**条件は、ユーザーがアプリにアクセスするために満たす必要がある必須条件です。条件、ドメイン、そしてユーザーの順に選択できます。

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



以下のいずれかを選択します。

- **いずれかに一致** – フィールドにリストされている名前のいずれかに一致し、選択したドメインに属するユーザーまたはグループのみがアクセスを許可されます。
- **いずれにも一致しない** - フィールドにリストされているユーザーまたはグループ、および選択したドメインに属するユーザーまたはグループを除くすべてのユーザーまたはグループがアクセスを許可されます。

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

注:

- 表示名、メールID、またはユーザープリンシパル名でユーザーまたはグループを検索できます。これにより、同じユーザーが複数のアカウントを持っている場合でも、正しいユーザーを正確に特定し、アクセスを許可することができます。詳細については、「ユーザーまたはグループの検索」を参照してください。
- Secure Private Accessポリシーが正しく評価されるように、同期されたユーザーとグループも使用する必要があります。そうしないと、警告メッセージが表示されます。詳細については、「ユーザーとグループの同期の確認」を参照してください。

7. ユーザーがブラウザベースのクライアントまたはCitrix Secure Accessクライアントのどちらを介して接続するかに基づいてアプリケーションアクセスを制限するには、**アクセスモード**条件を追加します。詳細については、「アクセスモードベースのポリシー適用」を参照してください。

注:

アクセスモードを必須の**ユーザー**条件およびその他の条件と組み合わせることができます。

8. (オプション) + をクリックして、コンテキストに基づいて複数の条件を追加します。

   コンテキストに基づいて条件を追加すると、条件にAND演算が適用され、**ユーザー**とオプションのコンテキストベースの条件が満たされた場合にのみポリシーが評価されます。コンテキストに基づいて、次の条件を適用できます。

   - **地理的位置** – 条件と、ユーザーがアプリにアクセスしている地理的位置を選択します。
     - **いずれかに一致:** リストされている地理的位置のいずれかからアプリにアクセスしているユーザーまたはユーザーグループのみが、アプリへのアクセスを許可されます。
     - **いずれにも一致しない:** リストされている地理的位置以外のすべてのユーザーまたはユーザーグループが、アクセスを許可されます。
   - **ネットワークロケーション** – 条件と、ユーザーがアプリにアクセスするために使用するネットワークを選択します。

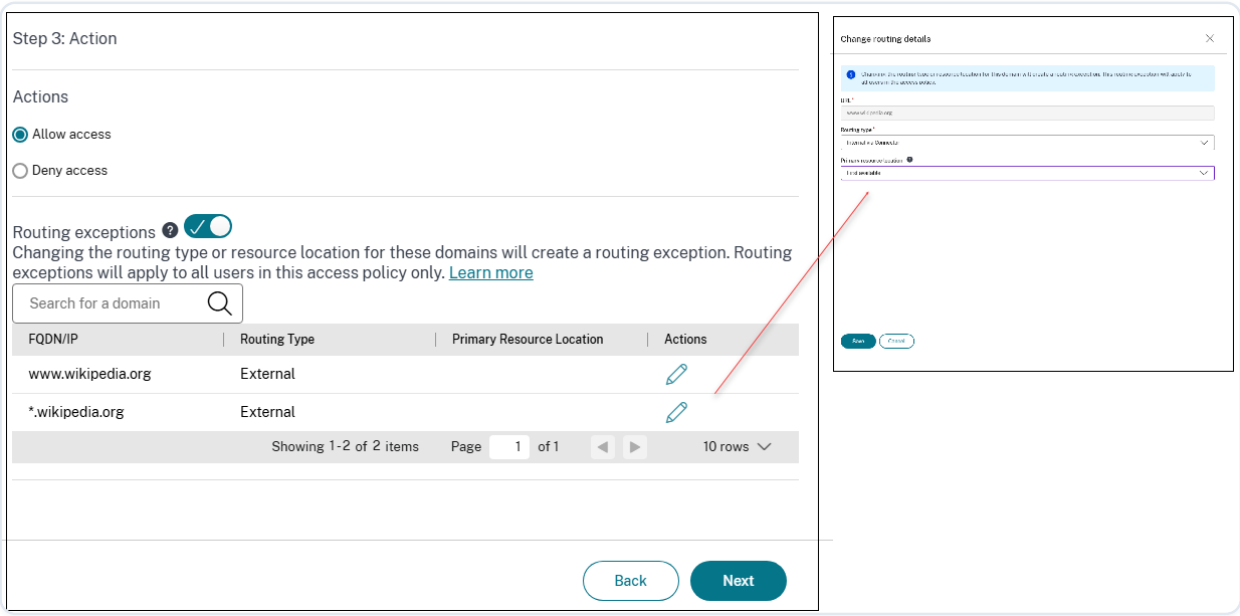
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **いずれかに一致:** リストされているネットワークロケーションのいずれかからアプリにアクセスしているユーザーまたはユーザーグループのみが、アプリへのアクセスを許可されます。
- **いずれにも一致しない:** リストされているネットワークロケーション以外のすべてのユーザーまたはユーザーグループが、アクセスを許可されます。

- **デバイスポスチャチェック** – ユーザーデバイスがアプリにアクセスするために満たす必要がある条件を選択します。

9. **次へ**をクリックします。
10. 条件評価に基づいて適用する必要があるアクションを選択します。

    - **アクセスを許可**
    - **アクセスを拒否**



11. (オプション) 必要に応じて、特定のドメインのルーティングタイプまたはリソースの場所を変更します。「**ルーティング例外**」トグルを使用すると、アクセスポリシーに追加されたアプリのドメインのリソースの場所とルーティング情報を編集できます。

    - **ルーティングタイプ**で、ルーティングタイプを変更します。
        - **内部**: トラフィックはConnector Applianceを介して流れます。Webアプリの場合、トラフィックはデータセンター内を流れます。SaaSアプリの場合、トラフィックはConnector Applianceを介してネットワーク外にルーティングされます。
        - **内部 - プロキシバイパス**: ドメインのトラフィックはCitrix Cloud Connector™アプライアンスを介してルーティングされ、Connector Applianceで構成された顧客のWebプロキシをバイパスします。

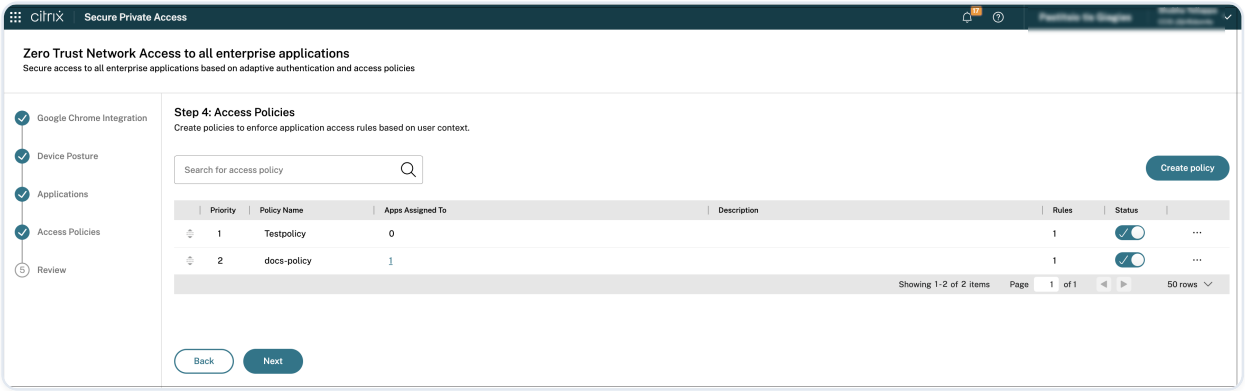
© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **外部**: トラフィックはインターネットに直接流れます。

- **リソースの場所**で、必要に応じてリソースの場所を変更します。このオプションは、内部ルーティングされたドメインにのみ適用されます。

コンテキストルーティングの詳細については、「コンテキストベースのアプリルーティングとリソースの場所の選択」を参照してください。

ポリシーを作成すると、「**アクセスポリシー**」ページに一覧表示されます。



ユーザーまたはグループを検索

選択したユーザーとグループはグリッドに表示されます。グリッドの各行には、異なるドメイン、フォレスト、またはIDプロバイダー (IdP) 間で同じ名前のユーザーまたはグループを明確に区別できるように、次のID詳細が表示されます。

- **名前** – ユーザーまたはグループの表示名。
- **メール** – IDに関連付けられているメールアドレス。
- **IDPタイプ** – Azure AD、Active Directory、Okta、GoogleなどのIDプロバイダー。
- **OID** – IDのオブジェクトIDまたはセキュリティ識別子。
- **ドメイン** – ユーザーまたはグループが属するドメイン。

グリッドを名前でフィルタリングしたり、個々の行を削除したり、複数のエントリを選択して**選択したものを削除**を使用してまとめて削除したりできます。

ユーザーとグループの同期を確認する

When selecting users or groups, administrators can verify whether entries from the selected user directory are synchronized with and correctly configured in Google Directory. Secure Private Access policies evaluate correctly only when the users and groups are synchronized. Otherwise, the following warnings might appear:

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

- **テナントアカウントの権限がありません。**

  回避策:

  Google管理コンソールで、テナントサービスアカウントに**ユーザー > 読み取り**および**グループ > 読み取り**の権限を割り当てます。SPAは、ユーザーまたはグループが存在することを確認するためにこれらの権限を必要とします。

- **ユーザーまたはグループが同期されていません。**

  回避策:

  検索または選択されたユーザーまたはグループはGoogle Directoryと同期されていません。SPAポリシーで使用する前に、ディレクトリエンティティをGoogle Directoryと同期してください。

- **グループアクセス設定が不十分です。**

  回避策:

  Google 管理コンソールで、選択したグループのアクセス設定を開き、**メンバーを表示できるユーザー**に少なくとも**グループメンバー**オプションが選択されていることを確認します。

> **注:**
>
> この機能は、Google Chrome の統合が正常に完了した後にのみ利用できます。

ポリシー作成後の留意事項

- 作成したポリシーは セクションに表示され、デフォルトで有効になっています。必要に応じて規則を無効にできます。ただし、ポリシーをアクティブにするには、少なくとも1つの規則が有効になっていることを確認してください。
- ポリシーにはデフォルトで優先順位が割り当てられます。値が小さい優先順位ほど優先度が高くなります。最も優先順位の低い規則が最初に評価されます。規則 (n) が定義された条件に一致しない場合、次の規則 (n+1) が評価され、以降同様に評価されます。

優先順位による規則の評価例:

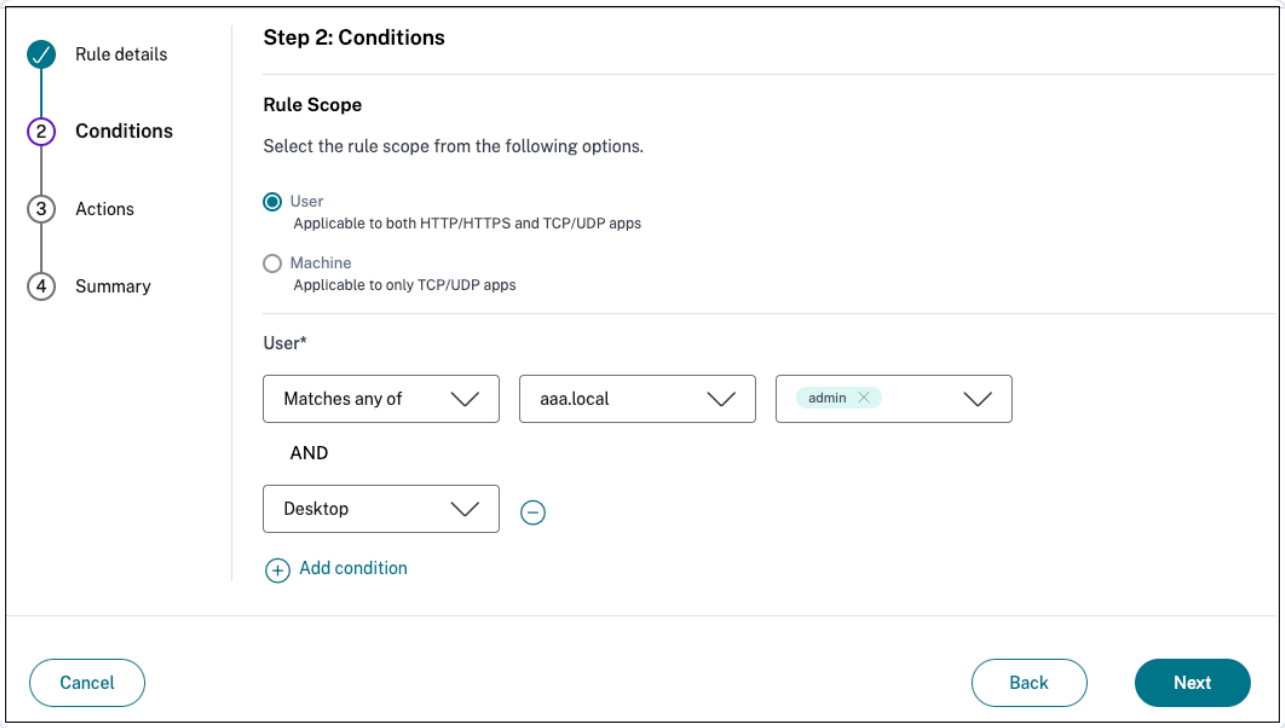
規則1と規則2の2つの規則を作成したとします。 規則1がユーザーAに割り当てられ、規則2がユーザーBに割り当てられている場合、両方の規則が評価されます。 規則1と規則2の両方がユーザーAに割り当てられているとします。この場合、規則1の優先度が高くなります。規則1の条件が満たされた場合、規則1が適用され、規則2はスキップされます。それ以外の場合、規則1の条件が満たされない場合は、規則2がユーザーAに適用されます。

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

デバイスに基づく適応型アクセス

ユーザーがアプリケーションにアクセスしているプラットフォーム（モバイルデバイスまたはデスクトップコンピューター）に基づいて適応型アクセスポリシーを構成するには、「適応型アクセスポリシーの構成と管理」を参照してください。

- **手順2: 条件**ページで、**条件の追加**をクリックします。
- **デスクトップ**または**モバイルデバイス**を選択します。
- ポリシー構成を完了します。



ロケーションに基づくアダプティブアクセス

管理者は、ユーザーがアプリケーションにアクセスしているロケーションに基づいて、アダプティブアクセス ポリシーを構成できます。ロケーションは、ユーザーがアプリケーションにアクセスしている国、またはユーザーのネットワークロケーションです。ネットワークロケーションは、IP アドレス範囲またはサブネットアドレスを使用して定義されます。

ロケーションに基づいてアダプティブアクセス ポリシーを構成するには、次の変更を加えて複数のルールを持つアダプティブアクセス ポリシーを作成する手順を使用します。

- **手順2: 条件**ページで、**条件の追加**をクリックします。
- **地理的位置**または**ネットワークロケーション**を選択します。

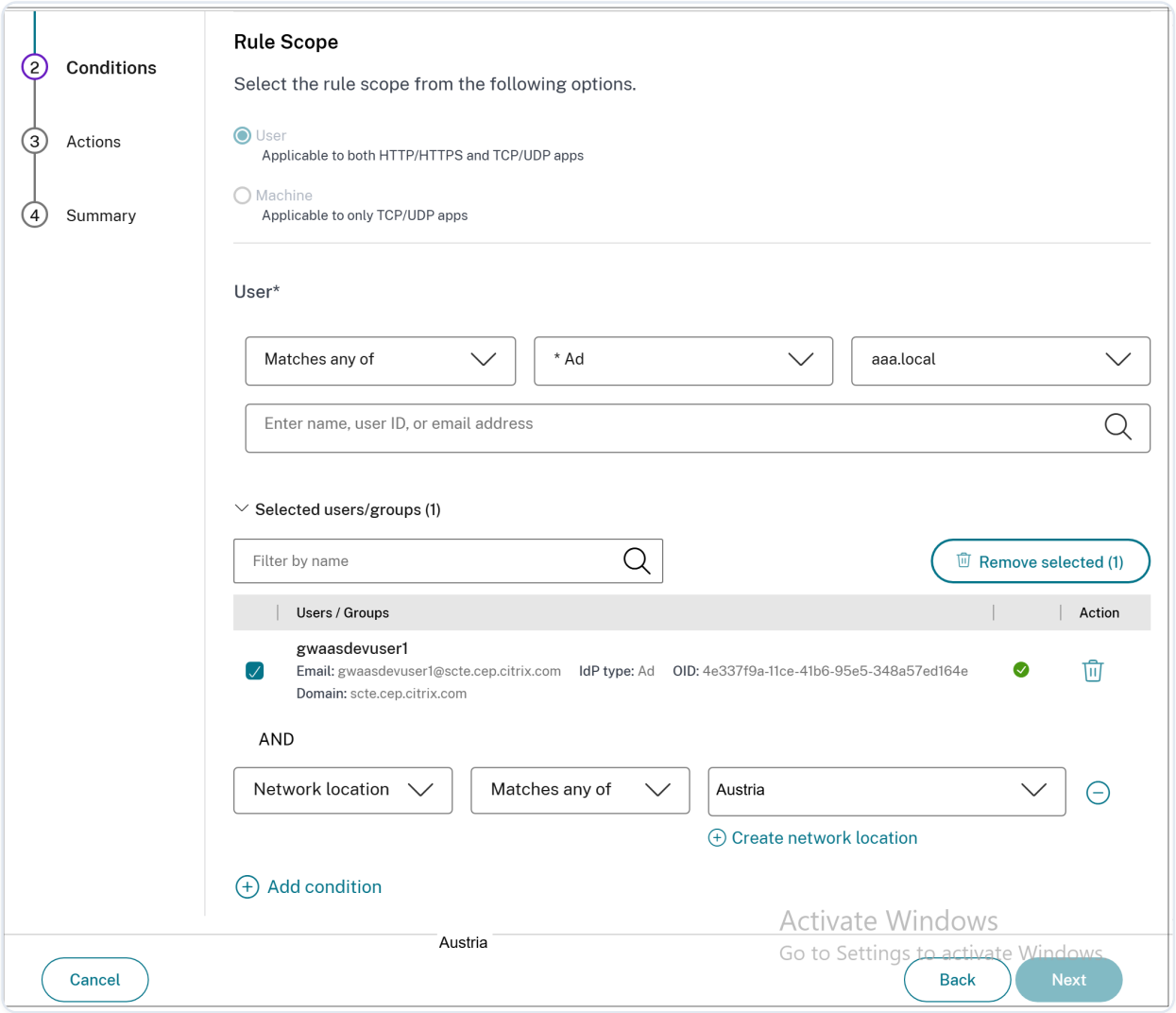
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 複数の地理的位置またはネットワークロケーションを構成している場合は、要件に応じて次のいずれかを選択します。
  - **いずれかに一致** – 地理的位置またはネットワークロケーションが、データベースで構成されている地理的位置またはネットワークロケーションのいずれかに一致します。
  - **いずれにも一致しない** – 地理的位置またはネットワークロケーションが、データベースで構成されている地理的位置またはネットワークロケーションのいずれにも一致しません。

  注:

  - **地理的位置**を選択した場合、ユーザーの送信元IPアドレスは国データベースのIPアドレスと比較評価されます。ユーザーのIPアドレスがポリシー内の国にマッピングされている場合、ポリシーが適用されます。国が一致しない場合、このアダプティブポリシーはスキップされ、次のアダプティブポリシーが評価されます。
  - **ネットワークロケーション**の場合、既存のネットワークロケーションを選択するか、新しいネットワークロケーションを作成できます。新しいネットワークロケーションを作成するには、**ネットワークロケーションの作成**をクリックします。
  - **Citrix Cloud > StoreFront Cloud > アクセス > アダプティブアクセス**からアダプティブアクセスが有効になっていることを確認してください。有効になっていない場合、ロケーションタグを追加できません。詳細については、「アダプティブアクセスを有効にする」を参照してください。
  - Citrix Cloudコンソールからネットワークロケーションを作成することもできます。詳細については、「Citrix Cloudネットワークロケーションの構成」を参照してください。

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



- ポリシー構成を完了します。

デバイスポスチャに基づくアダプティブアクセス

デバイスポスチャータグを使用してアクセス制御を適用するようにSecure Private Accessサービスを構成できます。デバイスポスチャー検証後にデバイスのログインが許可されると、そのデバイスは準拠または非準拠として分類できます。この情報は、Citrix DaaS™サービスおよびCitrix Secure Private Accessサービスにタグとして利用可能であり、デバイスポスチャーに基づいてコンテキストアクセスを提供するために使用されます。

Device Postureサービスの詳細については、「Device Posture」を参照してください。

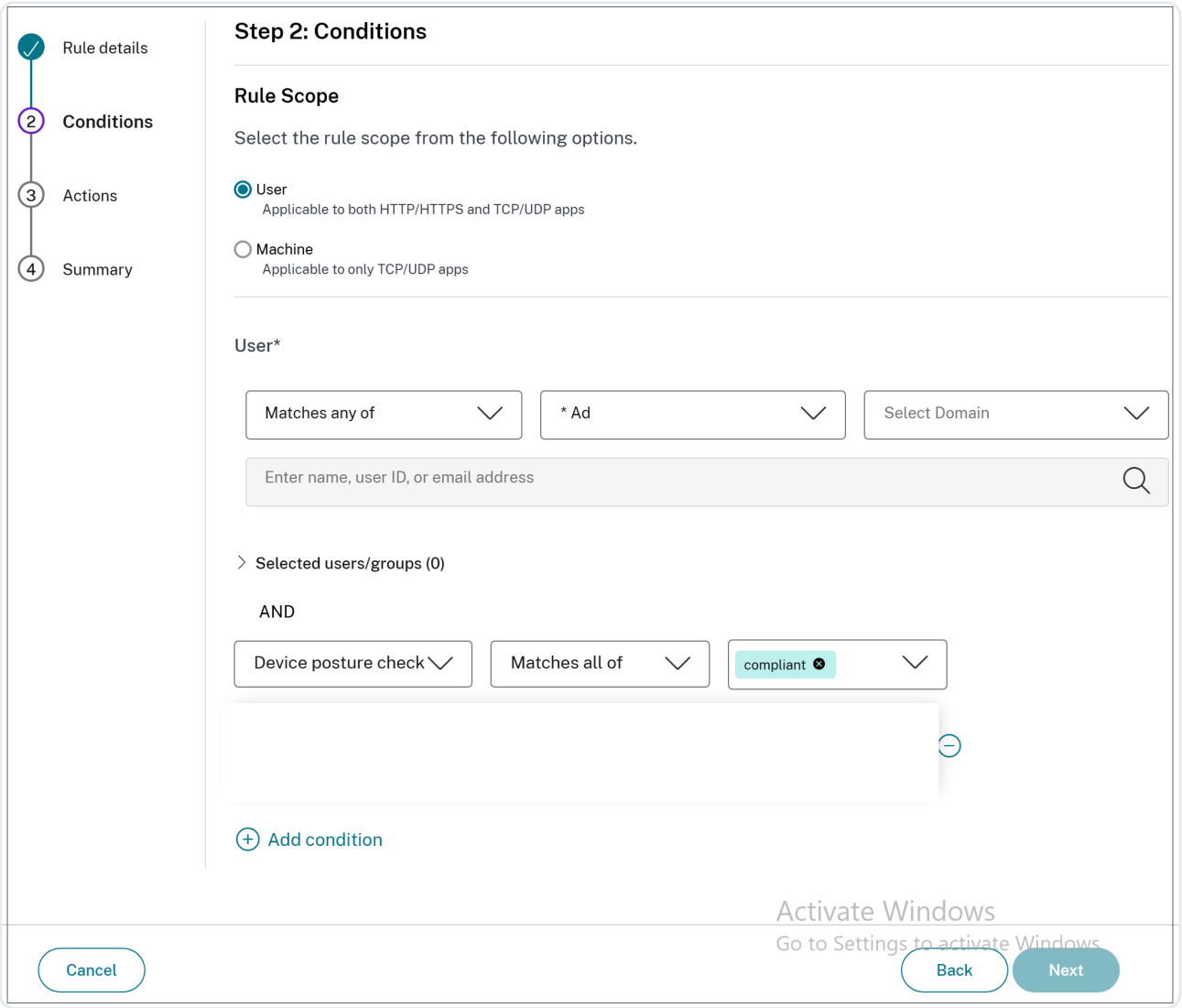
デバイスポスチャーに基づいて適応型アクセスポリシーを構成するには、以下の変更を加えて「複数のルールを持つ適応型アクセスポリシーを作成する」の手順を使用します。

- **手順2: 条件**ページで、**条件の追加**をクリックします。
- ドロップダウンメニューから**デバイスポスチャーチェック**と論理式を選択します。

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

- カスタムタグに次のいずれかの値を入力します。
  - **準拠** - 準拠デバイスの場合
  - **非準拠** - 非準拠デバイスの場合

> **注:**
>
> デバイス分類タグの構文は、以前にキャプチャされた方法、つまり頭文字を大文字（CompliantおよびNon-Compliant）で入力する必要があります。そうしないと、デバイスポスチャーポリシーは意図したとおりに機能しません。



セッションポリシー

管理者は、Secure Private Access を介してトラフィックをトンネリングすることなく、社内ユーザーをバックエンドアプリに直接ルーティングするようにセッションポリシーを構成できます。

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

セッションポリシーは、ネットワークロケーションやデバイスのポスチャなどの要因に基づいて動的なルーティングを提供します。

注:

- セッションポリシー設定は、特定のアプリケーションに紐付けられるのではなく、すべてのアプリケーションに対してセッションレベルで適用されます。
- セッションポリシーは、すべてのユーザーまたはユーザーのサブセットに割り当てることができます。

ルーティングの優先順位

セッションポリシーはアクセスポリシーと連携して機能し、競合がある場合はアクセスポリシーが優先されます。このようなシナリオでは、アクセスポリシーのルーティング例外がセッションポリシーを上書きします。 アクセスポリシーもセッションポリシーも構成されていない場合は、グローバルルーティング設定 (**設定 > アプリケーションドメイン**) が適用されます。

サポートされているCitrix Secure Access™クライアント

以下のバージョンのCitrix Secure Accessクライアントは、ユーザーをバックエンドアプリケーションに直接ルーティングすることをサポートしています。

- macOS - 24.11.1以降
- Windows - 24.11.1.17以降。また、**EnableContextualAccess** VPNクライアントレジストリを有効にする必要があります。詳細については、NetScaler Gateway Windows VPNクライアントレジストリキーを参照してください。

使用例

シナリオ:

組織において、ユーザーが企業ネットワーク「corporate_network1」に接続されている場合、これらのアプリは企業ネットワーク上で直接到達可能であるため、アプリからのトラフィックはバックエンドアプリに直接流れる必要があります。ユーザーが企業ネットワークの外部にいる場合、アプリのトラフィックはトンネリングされる必要があります。

解決策:

1. ルーティングを**Internal via Connector**に設定して、app1、app2を追加します。

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

2. アプリ (app1, app2) へのアクセスを許可するためのアクセスポリシーを追加します。
3. アクセスを許可する際に考慮する必要があるユーザーグループとネットワークロケーションを指定する条件を構成するために、セッションポリシーを追加します。
4. **ユーザー**条件を選択し、**すべてのユーザー**に設定します。
5. **ネットワークロケーション**条件を追加します。これを**いずれかに一致**に設定し、ネットワークロケーション「corporate_network1」を指定します。これにより、「corporate_network1」からのトラフィックがバックエンドアプリに直接流れるようになります。

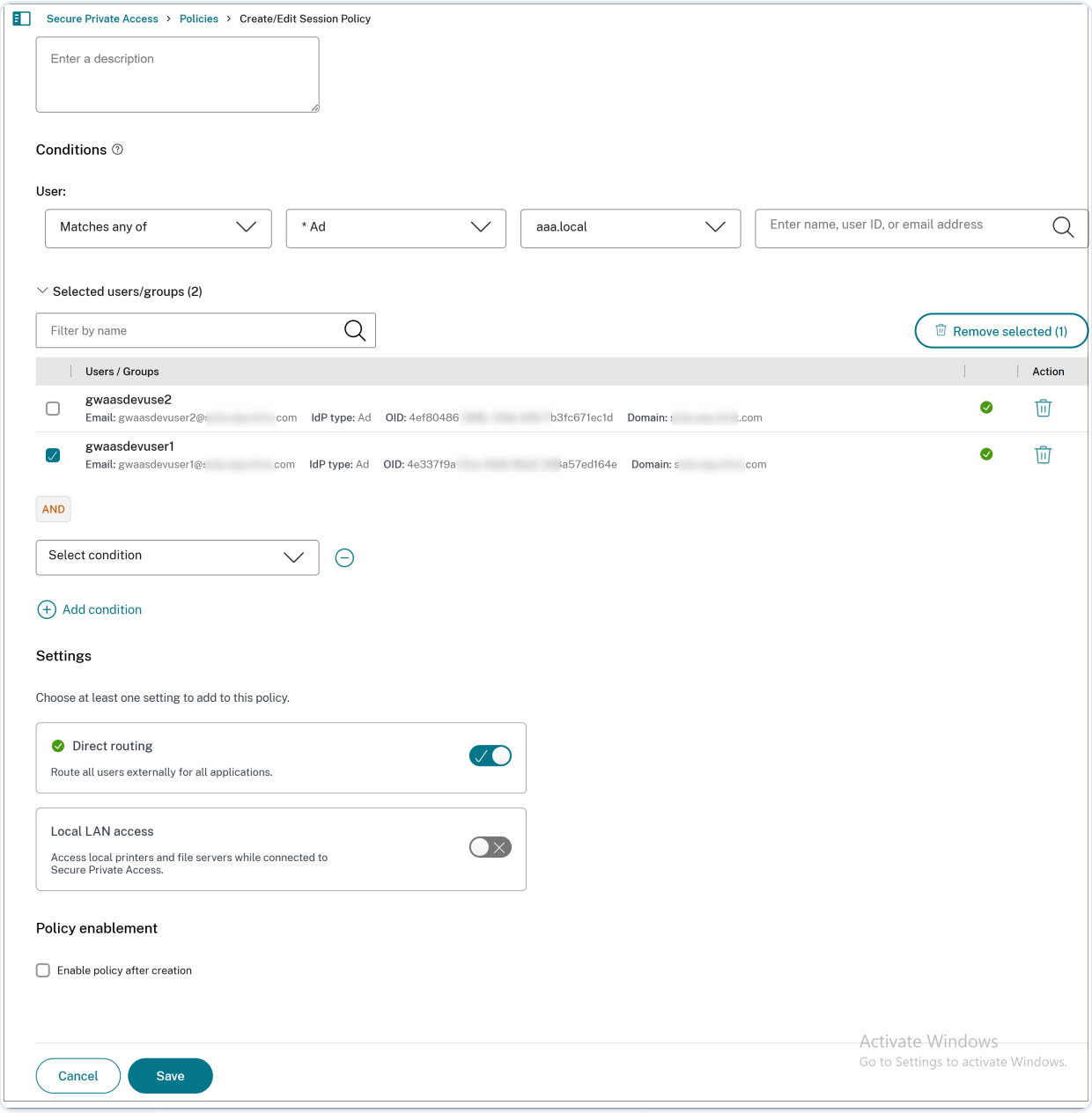
このシナリオでは、ルーティング例外を有効にすることもできます。たとえば、企業ネットワーク上でも常にapp1をトンネル経由にする必要がある場合、アクセスポリシーでapp1のドメインに対してルーティング例外を構成できます。これが完了すると、ルーティング例外がセッションポリシーよりも優先されます。

セッションポリシーを使用して企業ネットワーク内で直接ルーティングを構成する

Secure Private Accessトンネリングをバイパスして、ユーザーがバックエンドアプリケーションに直接アクセスできるようにするには、セッションポリシーを作成する必要があります。これを行うには、まず、このポリシーを適用するユーザーを選択します。次に、「ネットワークロケーション」の下で、企業ネットワークの名前を選択します。これは、ユーザーが社内ネットワーク内にいる場合にのみダイレクトルーティングが有効になるようにするための重要なステップです。

1. **ポリシー > セッションポリシー**に移動し、**セッションポリシーの作成**をクリックします。

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



2. ポリシーの名前とポリシーの説明を入力します。
3. これらの設定を適用するユーザーと条件を選択します。
4. すべてのユーザーに適用する条件を選択するか、ユーザーのサブセットを指定できます。

注:

表示名、メールID、またはユーザープリンシパル名でユーザーまたはグループを検索できます。これにより、同じユーザーが複数のアカウントを持っている場合でも、正しいユーザーを正確に識別し、アクセスを許可することができます。

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

選択したユーザーとグループはグリッドに表示されます。グリッドの各行には、異なるドメイン、フォレスト、またはIDプロバイダー (IdP) 間で同じ名前のユーザーまたはグループを明確に区別できるように、次のID詳細が表示されます。

- **名前** – ユーザーまたはグループの表示名。
- **メール** – ID に関連付けられているメールアドレス。
- **IDP タイプ** – Azure AD、Active Directory、Okta、Google などの ID プロバイダー。
- **OID** – ID のオブジェクト ID またはセキュリティ識別子。
- **ドメイン** – ユーザーまたはグループが属するドメイン。 グリッドを名前でフィルタリングしたり、個々の行を削除したり、複数のエントリを選択して「選択した項目を削除」を使用してまとめて削除したりできます。

5. セッション設定を目的のクライアントタイプにスコープ設定するには、**アクセスモード**条件を追加します。Secure Private Access ルーティング中に評価されるセッションポリシーは、CSA アクセスモードとして扱われます。アクセスモードの詳細については、「アクセスモードベースのポリシー適用」を参照してください。
6. (オプション) + をクリックして、コンテキストに基づいて複数の条件を追加します。
7. セッション全体の動的ルーティングを有効にするには、**ネットワークロケーション**条件を定義します。これにより、ダイレクトルーティングはユーザーが会社の企業ネットワーク内にいる場合にのみ有効になることが確認されます。

   コンテキストに基づいて条件を追加すると、条件に AND 演算が適用され、ユーザーとオプションのコンテキストベースの条件の両方が満たされた場合にのみポリシーが評価されます。条件の詳細については、「アクセスポリシーの構成」を参照してください。
8. すべてのユーザーを外部のバックエンドアプリケーションにルーティングするには、**ダイレクトルーティング**を選択します。
9. ローカル LAN リソースへのシームレスなアクセスを有効にするには、**ローカル LAN アクセス**を選択します。詳細については、「ローカル LAN リソース (プリンター、ファイルサーバー) へのシームレスなアクセス」を参照してください。
10. **作成後にポリシーを有効にする**を選択します。このオプションを選択しない場合、ポリシーは作成されるだけで、アプリケーションには適用されません。または、セッションポリシーページでステータス列のトグルスイッチを使用してポリシーを有効にすることもできます。
11. 「**保存**」をクリックします。

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

注:

ネットワークロケーションの変更はセッションポリシーの更新をトリガーし、エンドクライアントに次のような影響を与える可能性があります。

- **Citrix Secure Access エージェント:** ポリシーの更新によりルーティング構成が変更され、アプリケーションアクセスに影響を与える可能性があります。
- **Citrix Enterprise Browser™:** ポリシーの更新は 30 分ごとに発生します。ユーザーは、アプリケーションにアクセスするためにブラウザを再起動するか、更新を待つ必要があります。

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

シトリックス エンタープライズ ブラウザから クローム エンタープライズ プレミアム への移行

Citrix Enterprise Browser (CEB) から Citrix Enterprise Premium (CEP) への移行は、すべてのアプリケーションに安全で適応性の高い高性能なゼロトラストネットワークアクセス (ZTNA) を提供するための Citrix Secure Private Access の進化における重要な一歩となります。このトピックでは、IT 管理者および Citrix プロフェッショナルが、最小限の混乱と最適なユーザーエクスペリエンスを確保しながら、段階的な移行を計画し実行するための詳細情報を提供します。

この段階的な移行アプローチにより、組織は移行期間中に両方のブラウザソリューションを並行して実行することで、ビジネスの継続性を維持できます。段階的な移行により、お客様は既存のアプリケーションとワークフローの Chrome Enterprise Premium との互換性を検証できます。

CEB から CEP への移行には、次の主要な手順が含まれます。

- クローム エンタープライズ プレミアム の構成
- メールアドレスのないユーザーグループのドメインマッピング
- CEP 互換性分析のための Secure Private Access 構成パーサー
- CEP への完全移行前の構成変更
- 組織への CEP の展開 (完全移行)

Chrome Enterprise Premium の構成方法

既存の Secure Private Access のお客様の場合、Secure Private Access コンソールの移行ウィザードは、CEP のプロビジョニング、ユーザーへの拡張機能のインストール、および段階的なアプリケーションとユーザーの移行パスを容易にします。

1. Secure Private Access 管理コンソールで、**Chrome Enterprise Premium > Configuration** に移動します。

   Google 統合の詳細を表示できます。

   (/en-us/citrix-secure-private-access/media/ceb-cep-integration-details1.png)

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

(/en-us/citrix-secure-private-access/media/ceb-cep-integration-details2.png)

2. 「**Google CEP をセットアップ**」をクリックします。
3. Google WorkSecure Private Access コンソール内でCitrixサービスアカウントの詳細を割り当てます。詳細については、「Google Chrome 統合のセットアップ」を参照してください。
4. 「**保存**」をクリックして閉じます。

Chrome Enterprise Premium のプロビジョニングが開始されます。

メールアドレスのないユーザーグループのポリシーエンリッチメント

Chrome Enterprise Premium のプロビジョニングが正常に完了すると、アクセスポリシーとセッションポリシーのポリシー更新プロセスが自動的にトリガーされます。

この更新プロセスでは、次の処理が行われます。

- 既存のポリシー（アクセスおよびセッション）を確認します。
- ルールにメールアドレスがないユーザーおよびユーザーグループを確認します。
- CC Directory サービスにクエリを実行してメールアドレスを取得し、ポリシーに追加します。

詳細については、「メールアドレスのないユーザーグループのドメインマッピング」を参照してください。

CEP 互換性分析のためのSecure Private Access構成パーサー

次の主要なポリシー要素は、CEP で直接サポートされていません。

- アプリケーション
  - シングルサインオン
- アクセスポリシー
  - 制限付きアクセスを許可
  - 許可/拒否アクションの混在 (HTTP/HTTPS 対 TCP/UDP)
  - ストアURL条件
  - デスクトップ/モバイル条件
- セッションポリシー

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

  - ストアURL条件
  - デスクトップ/モバイル条件

- セキュリティグループ
- Webフィルタリング

これらの非互換性は、CEBからCEPにアプリケーションを移行する前に解決する必要があります。

非互換性の特定プロセスは、Secure Private Access構成パーサー `<parse_citrix_spa_configuration.py>` によって促進されます。このツールは、Citrix Secure Private Access構成エクスポートを分析し、CEPへの移行中に次のような互換性の問題を特定します。

- CEPと互換性のないアプリケーション
- CEPと互換性のないアクセスポリシー
- 構成されたセキュリティグループ
- Webフィルタリング構成

注:

セキュリティグループとWebフィルタリングは、CEPとのCitrix Secure Private Access統合ではサポートされていません。

分析後、ツールはCEPの展開が組織全体で完了しているか（すべてのアプリケーションの移行）に応じて、異なる推奨事項を提供します。

ツールの使用方法

1. スクリプトを以下からダウンロードします: Secure Private Access構成を解析するPythonスクリプト。
2. Secure Private Access管理コンソールで、**「設定」>「グローバル構成」>「レポートの作成」**に移動し、既存のSecure Private Access構成をJSON形式でエクスポートします。
3. Pythonスクリプトをダウンロードし、エクスポートしたレポートを入力として使用してスクリプトを実行します。このスクリプトを実行するには、Python 3がインストールされている必要があります。

   ```
   # python3 parse_citrix_spa_configuration.py <path_to_spa_report>
   ```

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

このスクリプトは、完全移行の前または後に使用でき、異なる推奨アクションを提供します。

注:

このスクリプトは、互換性のないセッションポリシーに関する推奨事項は提供しません。

レポートの例:

```
% python3 parse_citrix_spa_configuration.py
CitrixSpaConfigurationDump.json



Has the CEP rollout to the entire organization been completed?



Enter yes/no (default: no): no



CEP INCOMPATIBLE APPLICATIONS (7 out of 185):



1. Application_1 ⚠


   Reason: Has SSO configuration other than 'Don't use SSO'


2. Application_2 ⚠


   Reason: Has SSO configuration other than 'Don't use SSO'


....
```

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

```
---------------------------------------------------

Mitigation guidance:

---------------------------------------------------

Has SSO configuration other than 'Don't use SSO':

  • Navigate to the application's SSO settings

  • Change the SSO setting to 'Don't use SSO'

===================================================

CEP INCOMPATIBLE POLICIES (15 out of 136):

1. Access_policy_1 ⚠

   Reasons: Contains user(s)/group(s) without email

2. Access_policy_2 ⚠
```

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

```
   Reasons: Mixed actions (HTTP/HTTPS vs TCP/UDP), Contains user(s)/
group(s) without email



...



--------------------------------------------------



Mitigation guidance:



--------------------------------------------------



Platform filter (Desktop/Mobile):



  • Remove the unsupported Desktop/Mobile condition



Workspace URL:



  • Remove the unsupported Workspace URL rule
```

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

```
Access with restrictions:



  • Configure access controls without using restrictions




Mixed actions (HTTP/HTTPS vs TCP/UDP):



  • Ensure both actions have the same value



  • If that's not possible, create separate policies for HTTP/HTTPS and
TCP/UDP applications




Policy contains user(s)/group(s) without email



  • Add email to the user(s)/group(s) without email and update the policy
```

CEPへの完全移行前の構成変更

CEPへの完全移行を開始する前に、Secure Private Access管理者が以下の構成変更を手動で適用する必要があります。これらの更新により、すべてのアプリケーションとポリシー間での互換性と準備が確保されます。

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

シングルサインオン構成の変更

CEPとの互換性を確保するためには、既存のすべてのアプリケーションのシングルサインオン（SSO）構成を更新することが不可欠です。Secure Private Access管理者は、以下の手順を実行する必要があります。

1. アプリケーション構成ページ（**Secure Private Access > アプリ構成**）に移動します。
2. アプリケーションを編集して、シングルサインオン構成を変更します。

   「シングルサインオン」セクションで、「**Webアプリのセットアップに使用するシングルサインオンの種類を選択してください。**」において、「**SSOを使用しない**」を選択します。

重要：

- CEPではSSOステップが削除されるため、この更新は必須です。アプリケーションを「**SSOを使用しない**」に設定することで、継続的な機能と新しい移行フローとの整合性を確保できます。
- 指示どおりにシングルサインオン構成が変更されない場合、CEPへの移行後、アプリケーションにアクセスできなくなります。

アクセスポリシーとセッションポリシーの更新

アクセスポリシーがCEP標準と互換性があることを確認するため、アクセスおよびセッションポリシーに特定の更新が必要です。Secure Private Access管理者は、次の手順を実行する必要があります。

1. 「**Secure Private Access > ポリシー > アクセスポリシー**」に移動します。
2. 関連するポリシーで「**編集**」をクリックし、アクション設定を変更します。

   a. ポリシー内で、「**ポリシー規則**」セクションに移動し、ポリシー規則と同じ行にある省略記号アイコンをクリックして「**編集**」をクリックします。

   b. 「**アクション**」ページに移動し、「**アクション**」設定を変更します。

アプリケーション全体でのアクションの標準化

HTTP/HTTPSおよびTCP/UDPアプリケーションの両方のアクションを構成する際は、以下を確認してください。

- 「**アクセスを許可**」または「**アクセスを拒否**」のいずれかの同じアクションが両方のセクションで選択されていること。

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

- HTTP/HTTPSアプリケーションで「**制限付きアクセスを許可**」オプションが現在有効になっている場合、この設定はCEPでサポートされていないため、削除する必要があります。
- 意図するポリシーの動作に基づいて、「**制限付きアクセスを許可**」を「**アクセスを許可**」または「**アクセスを拒否**」のいずれかに置き換えます。

ポリシー更新のアプリケーション要件

アプリケーションが割り当てられていないアクセスポリシーは更新できません。これらのポリシーを変更するには、まずポリシーにアプリケーションを割り当ててください。

重要：

これらの更新が実行されない場合、混合アクションを含むアクセスポリシーに関連付けられたアプリケーションにアクセスできなくなるか、拒否アクション設定が無視される可能性があります。

Webフィルタリングポリシーの更新（オプション）

新しいCEP移行標準との整合性を維持するため、Secure Private Access内のWebフィルタリング設定を更新する必要があります。Webフィルタリング設定を更新するには、以下の手順を実行します。

1. **Secure Private Access > 設定 > 未承認のWebサイト**に移動します。
2. このセクションに現在リストされているすべてのWebサイトとリモートブラウザ分離（RBI）のエントリを削除します。
3. これらのエントリを削除した後、ページ上部にある**Webフィルタリングが有効**のトグルを無効にします。

これらの設定は、CEPへの移行後は関連性がなくなります。

重要：

これらの手順が完了しなくても、完全な移行後のシステムの運用には影響ありません。ただし、**未承認のWebサイト**ページは表示されなくなります。

その他のポリシー調整（オプション）

未使用の条件を確認して削除します。

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

移行およびポリシー最適化プロセスの一環として、適用されなくなった可能性のある条件がないか、アクセスおよびセッションポリシーを確認することをお勧めします。そのような条件の例としては、次のものがあります。

- ワークスペース URL
- デスクトップおよびモバイルオプション

これらの条件は、現在の環境やビジネス要件に関連しない場合、削除できます。

注:

これらのポリシー調整が行われない場合、システム運用への影響はありません。

セキュリティグループのクリーンアップ（オプション）

Secure Private Access 内のセキュリティグループ設定を確認します。

既存のエントリを評価するには、**Secure Private Access > アプリケーション > セキュリティグループ**に移動します。

移行後、セキュリティグループの設定は利用できなくなります。したがって、このタブに現在リストされているエントリは、移行後の環境には関連性がなくなるため、削除できます。

注:

この設定が更新されない場合でも、システムへの影響はありません。これらのエントリの削除はオプションであり、合理化された環境の維持に役立ちますが、継続的な運用には必須ではありません。

CEPを組織に展開（完全移行）

前述の手順を完了したら、**アプリとユーザーの移行**ページで**組織に展開**をクリックします。これが移行プロセスの最終段階です。

組織に展開(/en-us/citrix-secure-private-access/media/ceb-cep-migration-rollout.png)

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

重要：

展開が完了すると、CEPがデフォルトのエンタープライズブラウザになります。CEBへのロールバックは不可能であり、互換性のない設定はSecure Private Access管理コンソールで非表示になります。

移行プロセスの概要

CEBからCEPにアプリケーションを移行するには、次の手順に従います。

1. Chrome Enterprise Premiumをプロビジョニングします。
2. 特定のユーザーグループ向けに1つのアプリケーションを移行します。
   a. グループにメールアドレスを追加します（存在しない場合）。
   b. 互換性のない部分を修正します。
   c. アプリケーションをCEPに移行します。
   d. アプリケーションがCEP経由でアクセス可能であることを確認します（直接、CWA、WSUI）。
3. ユーザーとユーザーグループにメールアドレスを付与します。
4. さらに多くのアプリケーション、ユーザー、ユーザーグループを移行します。
5. 組織全体にCEPを展開します（完全移行）。
6. 残っている互換性のない部分を修正します。
   a. プロンプトでCEPの展開が完了したことを示して、スクリプトを再度実行します。
   b. 互換性のない部分を修正します。
   c. アプリケーションがCEP経由でアクセス可能であることを確認します（直接、CWA、WSUI）。

メールエンリッチメントプロセスの課題

メールエンリッチメントタスクは複雑になる可能性があり、多くの場合、複数のドメインにわたるさまざまなグループにメールを割り当てるために、複数のチーム間の連携が必要になります。ドメインマッピング機能はこのプロセスを容易にします。詳細については、「メールアドレスを持たないユーザーグループのドメインマッピング」を参照してください。

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

ベストプラクティス

1. 全面的な展開の前に、小規模なユーザーグループを対象としたパイロット移行から開始します。
2. Citrixの公式移行ツールとドキュメントを活用します。
3. すべての変更と構成に関する明確なドキュメントを維持します。
4. 重大な問題が発生した場合に備えて、ロールバック計画を確立します。

まとめ

CEBからCEPへの移行は、強化された機能によりCitrix環境を最新化します。綿密な計画、徹底的なテスト、および積極的なユーザーエンゲージメントにより、CEPへのスムーズな移行が保証されます。

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

高度なSecure Private Access機能

Secure Private Accessでサポートされている高度な機能の一部を以下に示します。

- **アクセスモードベースのポリシー適用:** アクセスモードベースのポリシー適用により、管理者はユーザーがアプリケーションに接続する方法を制限できます。接続はブラウザベースのクライアントまたはCitrix Secure Accessクライアントを介して行うことができます。詳細については、アクセスモードベースのポリシー適用を参照してください。
- **ローカルLANアクセスサポート:** Secure Private Accessは、企業リソースへのセキュアな接続を維持しながら、ローカルLANリソースへのシームレスなアクセスをサポートします。詳細については、ローカルLANリソースへのシームレスなアクセス（プリンター、ファイルサーバー）を参照してください。
- **DNSクエリをアプリケーション固有のリソースロケーションにルーティング:** 管理者は、特定のアプリケーションのDNSクエリを専用のリソースロケーションに直接ルーティングできます。これにより、より正確なDNS解決、インテリジェントなトラフィック管理、およびより良いユーザーエクスペリエンスが可能になります。詳細については、DNSクエリをアプリケーション固有のリソースロケーションにルーティングを参照してください。
- **Secure Private Accessサービス用のハイブリッドデータパス:** Secure Private Accessサービス用のハイブリッドデータパスは、オンプレミスとクラウドの両方のインフラストラクチャを活用して、アプリケーションへのセキュアなアクセスを提供します。組織はハイブリッドデータパスを使用して、すべてのデータトラフィックをオンプレミスのNetScaler Gateway経由でルーティングできます。これにより、機密データが会社のネットワーク内に留まることが保証されます。データトラフィックがオンプレミスのNetScaler Gateway経由でルーティングされる場合でも、Citrix Cloudはアプリケーションとユーザーの監視および管理に引き続き使用できます。詳細については、Secure Private Accessサービス用のハイブリッドデータパスを参照してください。
- **ネットワーク内のアプリケーション、ドメイン、またはIPアドレスを検出:** 管理者が組織内でアクセスされている外部および内部アプリケーション（HTTP/HTTPSおよびTCP/UDPアプリ）を可視化するのに役立ちます。この機能は、公開済みまたは未公開のすべてのドメイン/IPアドレスを検出し、リストします。これにより、管理者はどのドメイン/IPアドレスが誰によってアクセスされているかを確認し、それらをアプリケーションとして公開して、それらのユーザーにアクセスを提供するかどうかを決定できます。詳細については、ネットワーク内のアプリケーション、ドメイン、またはIPアドレスを検出を参照してください。

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

- **コンテキストベースのアプリルーティングとリソースロケーションの選択:** 管理者は、ユーザーコンテキストに基づいて、URLまたはリソースロケーションごとの内部ルーティングタイプを編集できます。詳細については、コンテキストベースのアプリルーティングとリソースロケーションの選択を参照してください。
- **ポリシーモデリングツール:** 管理者は、既存の構成に基づいて、予想されるアプリアクセス結果（許可/制限付きで許可/拒否）を完全に可視化できます。管理者は、デバイスタイプ、デバイスポスチャ、地理的位置、ネットワークロケーション、ワークスペースURLなどの条件に基づいて、任意のユーザーのアクセス結果を確認できます。詳細については、ポリシーモデリングツールを参照してください。
- **アプリケーションインポートツール:** Secure Private Access管理コンソールには、管理者がCSVファイルまたはnsconfigファイルを使用して複数のアプリケーションを一括でシステムにインポートできるファイルインポートツールが含まれています。このツールは、従来のVPNからSecure Private Accessのようなより高度なソリューションに移行する組織にとって特に役立ちます。たとえば、組織はこのツールを使用して、VPN経由で提供されていたアプリケーションをSecure Private Accessに移行し、ZTNAベースのアーキテクチャに移行できます。アプリケーションの一括アップロードにより、組織は手動構成の必要性を排除できます。詳細については、アプリケーションインポートツールを参照してください。
- **アクティブなセッションを終了し、ユーザー/マシンをブロック:** - 管理者はすべてのアクティブなセッションを直ちに終了し、ユーザー/マシンをブロックリストに追加できます。ユーザー/マシンをブロックリストに追加すると、すべてのアクティブなSecure Private Accessアプリケーションセッションが終了し、将来のアプリケーションアクセスがブロックされます。詳細については、アクティブなセッションを終了し、ユーザー/マシンをブロックリストに追加を参照してください。
- **ユーザーセッションのタイムアウト:** 管理者は、WebアプリとCitrix Secure Accessクライアントのタイムアウト期間を設定して、指定された期間ネットワークアクティビティがない場合にユーザーセッションを終了できます。詳細については、ユーザーセッションのタイムアウトを参照してください。

Secure Private Accessサービスのためのハイブリッドデータパス

Secure Private Accessサービスのハイブリッドデータパスは、オンプレミスとクラウドの両方のインフラストラクチャを活用して、アプリケーションへのセキュアなアクセスを提供します。組織はハイブリッドデータパスを使用して、すべてのデータトラフィックをオンプレミスのNetScaler Gateway経由でルーティングできます。これにより、機密データが会社のネットワーク内に留まることが保証されます。データトラフィックがオンプレミスのNetScaler Gateway経由でルーティン

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

グされる場合でも、Citrix Cloud™はアプリケーションとユーザーの監視および管理に引き続き使用できます。

ハイブリッドデータパスを使用する主な利点

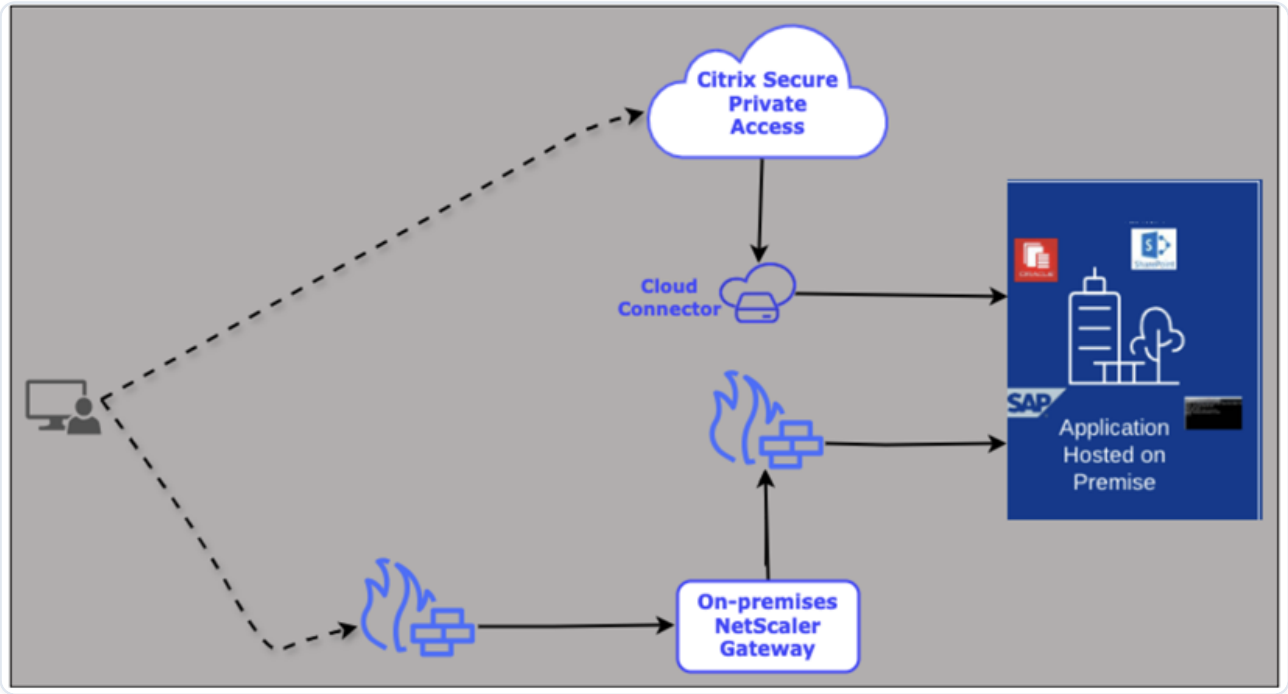
ハイブリッドデータパスを使用する主な利点は次のとおりです。

- オンプレミスゲートウェイによるリーチの拡大:
  - オンプレミスのNetScaler® Gatewayを利用して、クラウドPoPが遠い地域にあるオンプレミスアプリケーションへのアクセスを提供します。
  - 遠隔のクラウドPoPを介したトラフィックルーティングを回避することで、一貫したパフォーマンスを確保します。
- きめ細かなセキュリティと制御:
  - 選択的ルーティングを実装して、機密性の高いアプリケーションを安全なオンプレミス経路経由で誘導し、重要度の低いアプリケーションをクラウド経由でルーティングします。
  - アプリケーションデータの機密性に基づいて、データセキュリティとコンプライアンス要件を満たすためのアプリケーションのカスタムルーティングを可能にします。
- ユーザーエクスペリエンス向上のための直接接続:
  - リモートユーザーと必要なアプリケーション間の直接接続を確立し、クラウドPoPをバイパスします。

ハイブリッドデータパスの仕組み

次の図は、ハイブリッドデータパスのワークフローを示しています。

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



「ハイブリッドデータパス」におけるワークフローを以下に示します。

1. ユーザーがCitrix Secure Access™クライアントにログインします。
2. 認証が成功すると、セッションが確立されます。
3. エンドユーザーがアプリケーションを起動しようとします。
4. アプリケーションに関連付けられたアクセスポリシーが評価され、アプリが起動されます。
    - アプリケーションがSecure Private Accessサービスを介してルーティングされるように構成されている場合、リクエストはCloud Connectorに送信され、その後、特定のアプリが起動されます。
    - アプリケーションがオンプレミスのNetScaler Gatewayを介してルーティングされるように構成されている場合、リクエストはオンプレミスのNetScaler Gatewayに送信され、特定のアプリケーションが起動されます。

サポートされているクライアント

ハイブリッドデータパスは、以下のCitrix Secure Accessクライアントでサポートされています。

- Windows - 25.1.1.17以降
- macOS - 25.02.1以降

サポートされているNetScaler Gatewayビルド

ハイブリッドデータパスは、NetScaler Gatewayバージョン14.1ビルド47.46以降でサポートされています。

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

接続要件

以下のセクションでは、接続要件に関する詳細情報を提供します。

送信接続用の許可URLリスト

NetScaler Gatewayからの送信接続には、以下のURLを許可する必要があります。

- `https://trust.citrixnetworkapi.net`: Citrix Cloudへのゲートウェイ登録用。
- `https://trust.citrixworkspacesapi.net`: Citrix Cloudへのゲートウェイ登録用。
- `https://policy.netscalergateway.net`: ゲートウェイ経由でのアプリ起動リクエストの承認用。
- `https://cacerts.digicert.com`: ポリシーサービスエンジンの証明書検証用。

Secure Private Accessアプリケーションのハイブリッドデータパスを設定する

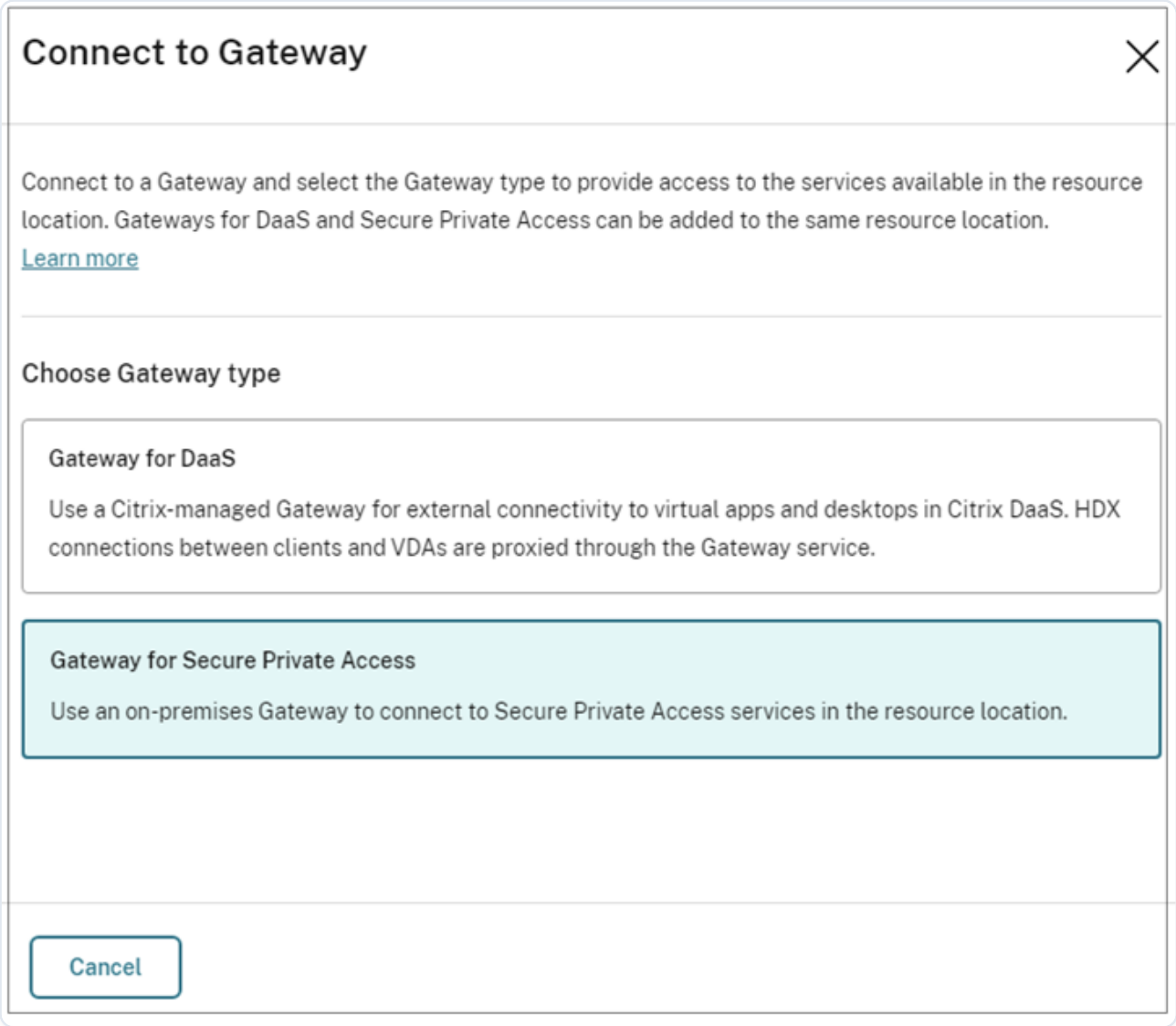
ハイブリッドデータパスの設定には、以下の大まかな手順が含まれます。

1. 接続を確立するためにゲートウェイに接続する
2. NetScaler GatewayをCitrix Cloudに登録する
3. オンプレミスのNetScaler Gatewayを介したデータトラフィックのルーティングを有効にする

接続を確立するためにゲートウェイに接続する

特定のSecure Private Accessリソースロケーションにあるリソースとの接続を確立するには、まずゲートウェイに接続する必要があります。Citrix Cloudを使用すると、特定のDaaSおよびSecure Private Accessリソースロケーションにあるリソースとの接続を確立できます。選択するゲートウェイの種類によって、アクセスできるサービスが決まります。柔軟性を高め、リソース利用を最適化するために、同じリソースロケーション内にDaaSゲートウェイとSecure Private Accessゲートウェイの両方を追加できます。

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



- **DaaS用ゲートウェイ:** Citrixが管理するゲートウェイは、Citrix DaaS™環境内でホストされている仮想アプリケーションおよびデスクトップの外部アクセスポイントとして機能します。このゲートウェイは、セキュアプロキシとして機能し、クライアント（ユーザーデバイス）とCitrix Cloudに存在する仮想デスクトップエージェント（VDA）間のHDX接続を仲介および管理します。

  さまざまなビジネス要件に基づいて、仮想アプリとデスクトップへのアクセスを許可する方法を選択できます。

- **Secure Private Access 用ゲートウェイ:** Secure Private Access 用ゲートウェイは、すべてのデータトラフィックをオンプレミスのNetScaler Gateway経由でルーティングすることで、組織が機密データを制御できるようにし、データが会社のネットワーク境界内に留まるようにします。

  オンプレミスのNetScaler Gatewayがデータトラフィックを処理する一方で、Citrix Cloudは集中管理および監視機能に使用でき、管理者はアプリケーションとユーザーをシームレスに監視および管理できます。

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

ゲートウェイに接続するには、次の手順を実行します。

1. Citrix Cloudにサインインします。
2. **リソースの場所 > 概要** を選択し、**ゲートウェイ** をクリックします。
3. **ゲートウェイタイプの選択** で、**Secure Private Access 用ゲートウェイ** を選択します。
4. ゲートウェイをCitrix Cloudに登録します。詳細については、「NetScaler GatewayをCitrix Cloudに登録する」を参照してください。

NetScaler GatewayをCitrix Cloudに登録する

まず、Secure Private Access 用ゲートウェイを選択し、次にオンプレミスのNetScaler GatewayをCitrix Cloudに登録する必要があります。この登録により、オンプレミスのNetScaler GatewayとCitrix Cloud環境の間で、Secure Private Access サービスのための安全な接続が確立されます。

前提条件:

登録スクリプトを正常に実行するために、次の構成が完了していることを確認してください。

- NetScalerでサブネットIP（SNIP）が構成されている必要があります。
- DNSネームサーバーがまだ存在しない場合は、構成する必要があります。
- 新しいVPN仮想サーバーに指定されたIPアドレスが必要です。
- 新しいVPN仮想サーバーにバインドするためのSSL証明書キー名を指定する必要があります。このSSL証明書キー名は、スクリプト実行前にNetScalerに追加する必要があります。

Citrix Cloudにゲートウェイを登録するには、次の手順を実行します。

1. Citrix Cloudにサインインします。
2. **リソースの場所 > 概要** を選択し、**ゲートウェイ** をクリックします。
3. **ゲートウェイの選択** タイプで、**Secure Private Access 用ゲートウェイ** を選択します。

ゲートウェイの登録(/en-us/citrix-secure-private-access/media/spa-mixed-mode-register-gateway.png)

1. Citrix Cloudに登録するゲートウェイのFQDNを入力します。
2. **メタデータの生成** をクリックします。**メタデータの再生成** をクリックして、メタデータを再生成することもできます。
    - メタデータをクリップボードにコピーします。

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

- オンプレミス環境内にあるNetScaler Gatewayへのセキュアシェル（SSH）接続を確立します。この接続により、NetScalerデバイスでコマンドとスクリプトをリモートで実行できます。
- NetScaler Gatewayへの接続に成功したら、次のコマンドを実行します。

  ```
  python3 /var/spa/scripts/spa_registration.py <copied metadata>
  ```

- `<copied metadata>` を、以前コピーした実際のメタデータに置き換えます。

  スクリプトは8桁の登録コードを生成します。このコードは登録プロセスにとって重要です。

3. **Citrix Cloudへの登録** セクションに8桁のコードを入力します。
4. 「**検証**」をクリックします。

   コードが無効な場合、警告メッセージが表示されます。検証が成功すると、「**登録**」ボタンが表示されます。
5. 「**登録**」をクリックします。
6. スクリプト実行ウィンドウに戻ります。システムは次のステップに進み、構成を完了するために以下の詳細を求めます。

   - VPN仮想サーバーに指定されたIPアドレス。
   - VPN仮想サーバーに関連付けるSSL証明書キー名。

これで、オンプレミスのNetScalerを介したアプリケーションのルーティングを構成できます。

オンプレミスのNetScaler Gatewayを介したデータトラフィックのルーティングを有効にする

オンプレミスのNetScaler Gatewayを介したデータトラフィックのルーティングを有効にするには、次の手順を実行します。

1. アプリを構成します。詳細については、次のトピックを参照してください。

   - エンタープライズWebアプリのサポート
   - エンタープライズWebアプリへのエージェントレスアクセス
   - サービスとしてのソフトウェアアプリのサポート
   - クライアントサーバーアプリのサポート

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

2. 「**アプリ接続**」セクションで、アプリケーションドメインのルーティング設定を定義し、トラフィックを外部にルーティングするか、Citrix Connector™ Applianceを介して内部にルーティングするか、またはオンプレミスのNetScaler Gatewayを介してルーティングするかを指定します。

   「ルーティングを構成」(/en-us/citrix-secure-private-access/media/hybrid-data-path-app-config.png)

3. 「**ルーティングの種類**」で、「**NetScaler Gateway経由の内部**」を選択します。これにより、データトラフィックがオンプレミスのNetScaler Gateway経由でルーティングされるようになります。関連ドメインのルーティングの種類を「**NetScaler Gateway経由の内部**」に更新することもできます。

   - 「**関連ドメイン**」テーブルの「**アクション**」列にある編集アイコンをクリックします。
   - 「**ルーティングの種類**」で、「**NetScaler Gateway経由の内部**」を選択します。
   - 「**保存**」をクリックします。

アクセス ポリシーからルーティングの詳細を変更する

特定のコンテキストに基づいてルーティング動作を変化させるように上書きできます。これらのコンテキストには、ユーザーグループ、地理的な場所、プラットフォーム、その他の関連する基準などの要素を含めることができます。コンテキストに基づいてルーティング動作を変更することで、最適化されたユーザーエクスペリエンスを提供できます。

アクセス ポリシーからオンプレミスのNetScaler Gateway経由でデータトラフィックのルーティングを変更するには、次の手順を実行します。

1. アクセス ポリシーを作成または編集します。詳細については、「アクセス ポリシーの作成」を参照してください。

   「ポリシーからルーティングを構成」(/en-us/citrix-secure-private-access/media/spa-mixed-mode-policy-routing.png)

2. 「**ステップ3: アクション**」ページで、「**ルーティング例外**」トグルを有効にします。「**ルーティング例外**」トグルを使用すると、アクセス ポリシーに追加されたアプリケーションのドメインのリソースの場所とルーティング情報を編集できます。
3. ルーティングの種類を変更したいドメインの横にある編集アイコンをクリックします。
4. 「**ルーティングの種類**」で、「**NetScaler Gateway経由の内部**」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.

制限事項

- サポートされているNetScaler Gatewayの展開タイプ - ハイブリッドデータパスは現在、高可用性セットアップの環境でのみサポートされています。
- フォールバックメカニズム - 現在のリリースでは、オンプレミスゲートウェイが停止したり利用できなくなったりした場合に、トラフィックをクラウドインフラストラクチャに自動的にリダイレクトするフェイルオーバーまたはフォールバックメカニズムはありません。
- 現在のリリースでは、ハイブリッドデータパスで以下の機能はサポートされていません。
  - アプリケーション検出
  - ポリシーモデリング
  - セッションポリシー
  - 可観測性
- `installns` スクリプトを実行してNetScalerビルドをインストールすると、/var/spa/scripts/ フォルダーが作成されます。このフォルダーは、新しく展開されたNetScaler VPXインスタンスには存在しないため、インストールプロセスを通じて作成する必要があります。詳細については、以下のトピックを参照してください。
  - NetScalerスタンドアロンアプライアンスのアップグレード
  - 高可用性ペアのアップグレード

Secure Private Access登録スクリプトの問題

Secure Private Access登録スクリプトは、一部の組み込みコマンドの構成の問題により、Azureに新しく展開されたVPXインスタンスで直接実行されません。この問題を解決するには、次の手順に従ってください。

- Azureに新しいVPXインスタンスをプロビジョニングします。
- 新しい構成を追加しないでください。
- `set system user nsroot <your-password>` コマンドを使用してnsrootユーザーの新しいパスワードを設定します。プロビジョニング中に作成されたカスタムユーザーは、`clear config` コマンドの実行後に削除されるため、この手順は重要です。nsrootとこの新しいパスワードを使用してNetScalerにアクセスできます。
- コマンド `save config` を使用して設定を保存します。
- `show cache policylabel` の出力を確認します。空である必要があります。
- コマンド `clear config basic` を実行し、Y と入力します。

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

- もう一度 `show cache policylabel` の出力を確認します。ラベルとして _reqBuiltinDefaults が表示されるはずです。

```
show cache policylabel



Label Name: _reqBuiltinDefaults

Evaluates: REQ

Number of bound policies: 3

Number of times invoked: 02)  Label Name: _resBuiltinDefaults

Evaluates: RES

Number of bound policies: 8

Number of times invoked: 03)  Label Name: _httpquicReqBuiltinDefaults

Evaluates: HTTPQUIC_REQ

Number of bound policies: 3

Number of times invoked: 04)  Label Name: _httpquicResBuiltinDefaults

Evaluates: HTTPQUIC_RES

Number of bound policies: 8

Number of times invoked: 0Warning: Feature(s) not enabled [IC]
```

- コマンドの出力に _reqBuiltinDefaults が表示されない場合は、Citrix サポートにお問い合わせください。
- SNIP、SSL 証明書キー、および DNS ネームサーバーを構成します。
- コマンド `save config` を使用して設定を保存します。
- Secure Private Access 登録スクリプトをもう一度実行します。

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

ネットワーク内のアプリケーション、ドメイン、またはIPアドレスを検出する

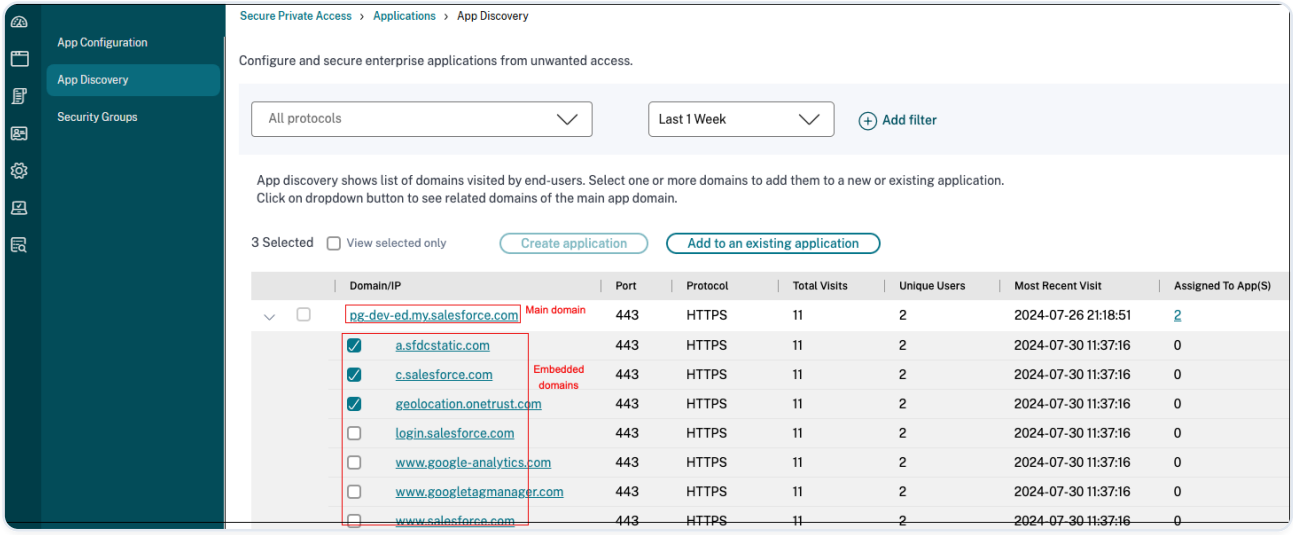
アプリケーション検出機能は、管理者が組織内でアクセスされている外部および内部アプリケーション (HTTP/HTTPSおよびTCP/UDPアプリ) を可視化するのに役立ちます。この機能は、公開済みか未公開かにかかわらず、すべてのドメイン/IPアドレスを検出して一覧表示します。これにより、管理者はどのドメイン/IPアドレスが誰によってアクセスされているかを確認し、それらをアプリケーションとして公開して、それらのユーザーにアクセスを提供するかどうかを決定できます。

アプリケーション検出機能は、管理者に以下の機能を提供します。

- エンドユーザーによってアクセスされる内部または外部のドメイン/IPアドレスの両方に可視性を提供します。
- アクセスされるすべての種類のアプリケーション (HTTP、HTTPS、TCP、UDP) に包括的な可視性を提供します。すべてのアクセス方法がサポートされています。つまり、Citrix Enterprise Browser™、Secure Access Agent、Direct Access、またはストアからのアクセスです。
- エンドユーザーによってアクセスされる公開済みまたは未公開のドメイン/IPアドレスの両方を表示します。
- Citrix Enterprise Browser経由でアクセスするためにアプリケーションを公開する際に、関連ドメインとして構成する必要があるメインドメインとその下層の埋め込みドメインの両方を表示します。
- 埋め込みドメインをツリー構造で表示します。管理者は、メインドメインと同じ行にある展開記号 (**>**) をクリックして、埋め込みドメインを表示できます。
- メインドメインまたは埋め込みドメイン (HTTP/HTTPS) または宛先IPアドレス (TCP/UDP) がアプリケーションに関連付けられていない場合、管理者が新しいアプリケーションを作成したり、それらのドメインを既存のアプリケーションに追加したりできるようにします。

次の図は、サンプル**アプリ検出**ページを示しています。**アプリ検出**ページでは、プロトコル (HTTP/HTTPS、TCP/UDP) およびドメイン/IPアドレスとポート番号に基づいてドメインをフィルタリングできます。また、エンドユーザーによってアクセスされた未公開 (どのアプリにも割り当てられていない) ドメインも表示されます。メインドメインの下に埋め込みドメインのドロップダウンリストが表示されます。これらのドメインは、アプリケーションを公開する際に、関連ドメインとして構成する必要があります。

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



注記：

- 埋め込みドメインは、Citrix Enterprise Browser経由でアクセスされるHTTP/HTTPSアプリの場合のみ、メインドメインの下にグループ化されます。TCP/UDPドメインは1つのメインドメインの下にグループ化されません。
- 埋め込みドメインのグループ化は、Citrix Enterprise Browser (v119以降) からアクセスされるアプリでのみ利用可能です。

新しい環境での内部ドメインのアプリケーション検出

アプリケーション検出機能は、新しいSecure Private Access環境をセットアップし、構成するアプリケーションを可視化したい場合に使用できます。この機能は、エンドユーザーがアクセスするすべてのドメイン/IPアドレスを検出し、リストアップするため、それらをアプリケーションとして構成できます。Secure Private Access環境をセットアップする際に、アプリケーション検出機能を有効にするには、次の手順を使用します。

- 内部Webアプリケーションを検出するには、Secure Private Access内でアプリケーションを構成し、検出したいアプリケーションのドメイン/サブドメインに属するワイルドカード関連ドメインを指定します。

  たとえば、ドメインcitrix.comを持つすべてのアプリケーションを検出したい場合は、関連するワイルドカードドメインとして `*.citrix.com` を持つアプリケーションを作成します。アプリケーション構成を完了させるには、メインのWebアプリURLセクションに任意のテストURLを追加します。

  アプリ検出1の構成(/en-us/citrix-secure-private-access/media/spa-app-discovery-1.png)

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

WebアプリURL: `https://test.citrix.com/` 関連ドメイン: `*.citrix.com`

- 内部TCP/UDPアプリの場合、Secure Private Access内でアプリケーションを構成し、サブネットとTCP/UDPプロトコル、およびポート範囲を指定します（全範囲を含めるには`*`と入力します）。これにより、Citrix Secure Accessエージェントからすべての TCPおよびUDPアプリを検出できます。たとえば、サブネット10.0.0.0/8内のすべてのアプリケーションを検出したい場合は、次の詳細でアプリを構成します。例: 10.0.0.0/8:

  ポート: (*)

  プロトコル: TCP

  アプリ検出2の構成(/en-us/citrix-secure-private-access/media/spa-app-discovery-2.png)

- アプリケーションを作成したら、構成されたドメインとIPサブネットを持つアプリへのアクセスが許可されるユーザーも定義する必要があります。アクセスポリシーを作成し、作成したアプリケーションで構成されたFQDN/IPアドレスへのアクセスを許可したいユーザーを割り当てます。これらは、初期のテストユーザーのセット、または最初にアクセスを許可したい限られた数のユーザーとすることができます。
- アプリケーションと対応するアクセスポリシーを作成した後、ユーザーはCitrix Workspaceアプリからアプリケーションにアクセスし続け、異なるドメインにアクセスできます。エンドユーザーがアクセスするすべてのFQDN/IPアドレスは、アプリケーション検出ページに表示され始めます。

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

注:

- 数日/数週間にわたってほとんどのアプリケーションを検出し特定したら、最初に作成したアプリケーションを削除することをお勧めします。これにより、ワイルドカードドメインとIPサブネットを介して与えられた広範なアクセスを閉じ、検出された特定のアプリケーションURLとIPアドレスのみを新しいアプリケーションを介してアクセスできるようにします。
- アプリ名にプレフィックス `Discover` を追加して、これが検出監視とレポートを有効にするための特別なアプリ構成であることを示します。この命名により、ワイルドカードドメインまたはIPサブネット、あるいはその両方を削除する時期を特定し、数週間または1か月後にアプリ全体のアクセスゾーンを特定のFQDNとIP/ポートの組み合わせのみに減らすことができます。
- TCP/UDPアプリにアクセスするには、ユーザーはCitrix Secure Accessエージェントを使用する必要があります。さまざまなアクセス方法からのアプリアクセスは、アプリのドメインとサブネット構成に基づいて監視され、**アプリ検出**ページ内で報告されます。
- 発見されたアプリケーションを削除した後でも、この機能はユーザーがアクセスしたドメイン/IPアドレスを発見し続けます。そのため、いつでも**アプリ検出**ページに戻って、何がアクセスされているか、そしてアプリケーションとして構成する必要がある新しいドメイン/IPアドレスが発見されていないかを確認できます。

ドメイン、FQDN、またはIPアドレスの追加の詳細については、以下のトピックを参照してください。

- エンタープライズWebアプリのサポート
- Software as a Serviceアプリのサポート
- クライアントサーバーアプリのサポート

アプリ検出ページからアプリケーションを作成する

アプリ検出ページから、埋め込みドメインまたは未公開ドメインのアプリケーションを作成するには、次の手順を実行します。

1. **アプリケーション > アプリ検出**に移動します。
2. リストからドメインを選択します。ドメインに埋め込みドメインがある場合は、メインドメインと同じ行にある展開記号 (**>**) をクリックし、埋め込みドメインを選択します。

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

注:

- 異なるプロトコルに属するドメインを選択してアプリケーションを作成することはできません。異なるプロトコルに属するドメインを選択すると、エラーメッセージが表示されます。
- ドメインがすでにアプリケーションに関連付けられている場合、そのドメインを再度選択してアプリケーションを作成することはできません。そのドメインに対応するチェックボックスはグレー表示され、チェックボックスにマウスを合わせるとツールチップが表示されます。
- 異なるメインドメインの下にグループ化された埋め込みドメインを選択してアプリケーションに追加することはできません。アプリケーション検出機能では、単一のメインドメインの下にグループ化された埋め込みドメインのみをアプリに追加できます。異なるメインドメインからの埋め込みドメインが選択され、同じアプリに追加された場合、エラーメッセージが表示されます。

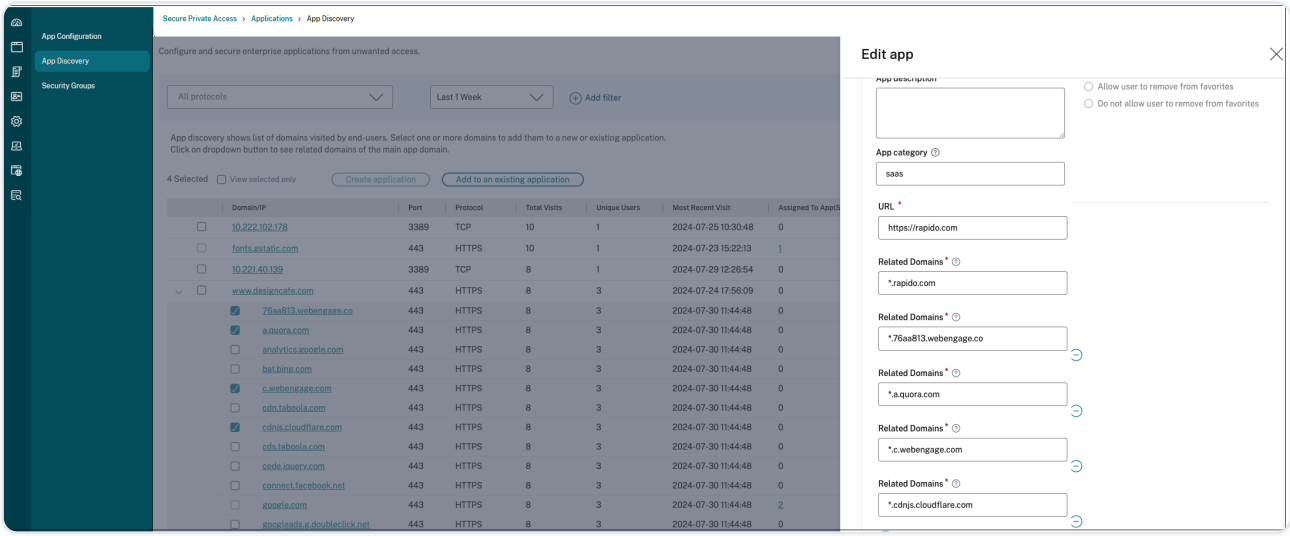
3. **アプリケーションの作成**をクリックします。アプリケーションの作成の詳細については、エンタープライズWebアプリのサポート、Software as a Serviceアプリのサポート、およびクライアントサーバーアプリのサポート](/ja-jp/citrix-secure-private-access/service/spa-support-for-client-server-apps.html)を参照してください。

既存のアプリケーションを更新する

既存のアプリケーションにドメインを追加するには、リストからドメインを選択します。ドメインに埋め込みドメインがある場合は、メインドメインと同じ行にある展開記号 (>) をクリックし、埋め込みドメインを選択します。

1. アプリケーションに追加する必要がある埋め込みドメインを選択します。
2. 「**既存のアプリケーションに追加**」をクリックします。
3. 「**アプリケーション**」で、これらのドメインを追加するアプリケーションを選択します。
4. 「**アプリの詳細を取得**」をクリックします。
5. 「**関連ドメイン**」フィールドに、以前選択したすべての埋め込みドメインが別々の行に表示されます。
6. 「**完了**」をクリックします。

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



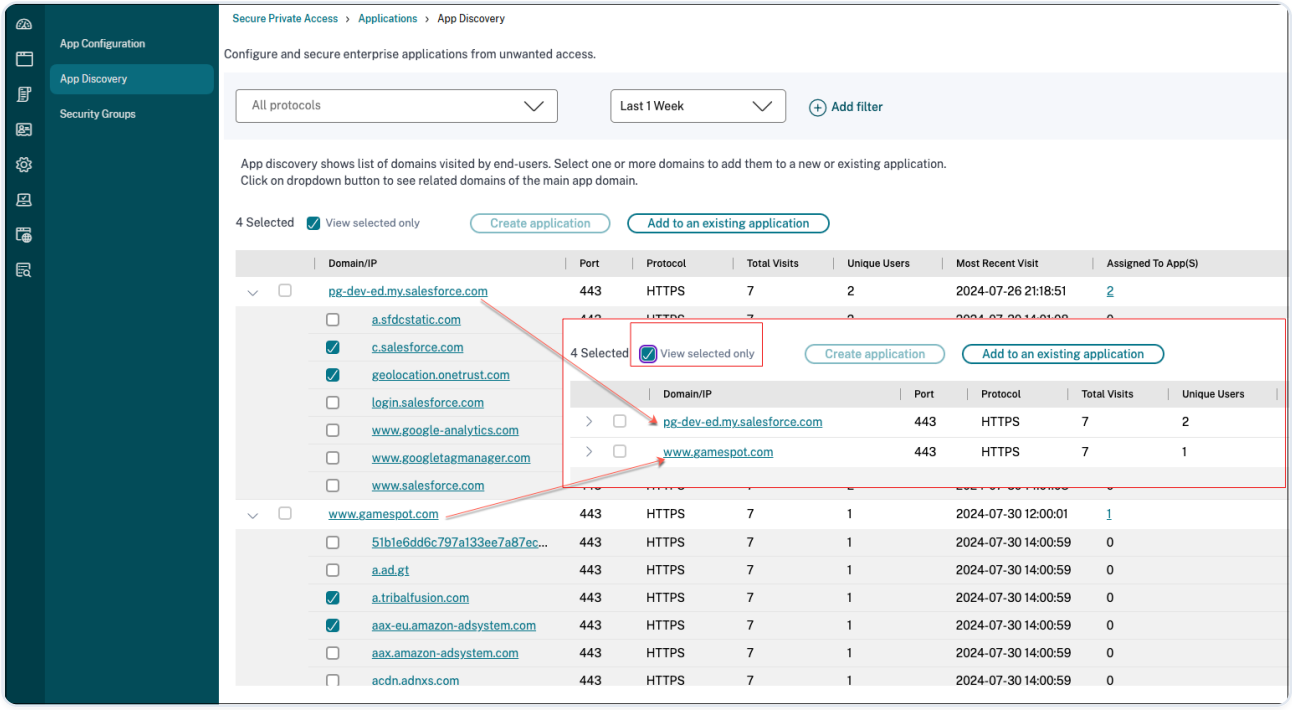
注:

- 既存のTCP/UDPアプリケーションには、TCP/UDP宛先IPアドレスのみを追加できます。「アプリケーション」フィールドには、システムで構成されているTCP/UDPアプリのみが表示されます。
- プロトコルがHTTP/HTTPSであるドメイン（メイン、単一エントリ、または埋め込み）を追加するために、既存のHTTP/HTTPSまたはTCP/UDPアプリを選択できます。
- 既にアプリケーションに関連付けられているドメインを選択することはできません。

選択したすべての埋め込みドメインを表示

ドメインを選択した後、「**選択済みのみ表示**」チェックボックスをクリックして、アプリケーションの作成または更新に進むことができます。また、アプリ検出ページのFQDN/IPアドレスのリストが複数のページにわたる場合、「**選択済みのみ表示**」チェックボックスを使用して、アプリケーションを作成または更新するために選択したすべてのメインドメインと埋め込みドメインを表示できます。このチェックボックスが選択されている場合、選択された埋め込みドメインのすべてのメインドメインが表示されます。

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



既知の制限事項

- Secure Private Accessダッシュボード（**総訪問数別上位検出アプリケーション**チャート）で**アプリケーションの作成**オプションと**既存のアプリケーションに追加**オプションが利用可能ですが、**アプリ検出**ページ（**アプリケーション > アプリ検出**）からアプリケーションを作成または更新することをお勧めします。これは、ダッシュボードからアプリケーションを追加または更新しているときに操作をキャンセルすると、ページが再読み込みされ、その結果、すべての設定がリセットされるためです。
- メインドメインの横に展開記号 (>) が表示されることがありますが、その特定のFQDNの埋め込みドメインがフェッチされない場合があります。この問題は、次の場合に発生する可能性があります。
  - ユーザーに対するアクセス制限により、メインのWebページの読み込みエラーが発生する。
  - Webページの読み込みを妨げるエラー。
  - Citrix Enterprise Browserによる埋め込みドメインリソースのキャッシュにより、埋め込みドメインがソースからフェッチされない。

コンテキストベースのアプリルーティングとリソースロケーションの選択

アプリが構成されると、アプリのURLと関連ドメインはルーティングタイプとリソースロケーションに割り当てられます。これはアプリの構成中に行われます。このアプリルーティングとリソース

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

ロケーションの構成は、そのアプリにアクセスできるすべてのユーザーに適用されます。しかし、次のようなシナリオが考えられます。

- 管理者は、同じアプリを異なるユーザーに対して異なる方法でルーティングしたいと考えています。たとえば、一部のユーザーに対しては、トラフィックがSecure Private Accessサービスにルーティングされるのを防ぐために、内部アプリのURLを外部にルーティングする必要があります。
- パフォーマンスを向上させるために、最適なデータセンターにリクエストをルーティングするために、異なるユーザーに対して異なるリソースロケーションを使用する必要がある。

これは、ルーティング例外を使用してアクセスポリシー内で実行できるようになりました。アクセスポリシーのルーティング例外構成により、管理者はユーザーコンテキストに基づいて、URLまたはリソースロケーションごとの内部ルーティングタイプを編集できます。この設定はアクセスポリシー内にあるため、そのアクセスポリシーの一部であるユーザーにのみ適用されます。

セッションポリシーを使用して、セッション全体を動的にルーティングすることもできます。詳細については、「内部企業ユーザーをバックエンドアプリケーションに直接ルーティングする」を参照してください。

注:

アクセスポリシー内にルーティングとリソースロケーションの構成がある場合、それはアプリの構成を上書きします。

次の例は、ルーティング例外のユースケースを示しています。

- コンテキストベースのルーティング
- ユーザーコンテキストベースのリソースロケーション選択
- 内部企業ユーザーをバックエンドアプリケーションに直接ルーティングする

ユースケース: コンテキストベースのルーティング

シナリオ:

- グループAユーザー: Secure Private Accessを介してOutlookアプリとMicrosoft Teamsアプリにアクセスするabc社の従業員で、内部的にルーティングされます。
- グループBユーザー：ABCと協力しているサードパーティ企業の従業員。彼らは特定のアプリケーション（Outlookを除く）にセキュアプライベートアクセスを介してアクセスします。また、インターネット経由でアクセスする独自のOutlookアプリケーションを持っており、

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

Outlookトラフィックをセキュアプライベートアクセス経由でルーティングしたくありません。

問題点：

- グループBユーザーは、ABCアプリにアクセスするためにセキュアアクセスエージェントにログインします。
- 彼らのネイティブブラウザを介したOutlookへのアクセス要求は、セキュアプライベートアクセス経由でルーティングされ、アクセス拒否につながります。
- Outlookアプリケーションの宛先ドメインは、グループAユーザーとグループBユーザーの両方で同じです。
- アクセスポリシーはグループAユーザーのみにアクセスを許可しているため、グループBユーザーがMicrosoft TeamsまたはOutlookを起動しようとするとアクセスが拒否されます。
- このルーティングの問題により、グループBユーザーは会社のOutlookにアクセスできません。

解決策：

ABC社の管理者は、この問題を解決するために以下の構成変更を行うことができます。

1. Office 365アプリにアクセスするグループBユーザー専用の新しいアクセスポリシーを定義します。
2. アクセスポリシーで、**ルーティング例外**オプションを有効にします。

   管理者は、アクセスポリシーに関連付けられているすべての内部アプリのすべてのURLと関連ドメインのリストを表示できます。
3. すべてのOffice365アプリのURLについて、ルーティングが外部で行われるように構成します。

   これにより、グループBユーザーのOutlookアプリケーションへのアクセス要求がインターネット経由でルーティングされ、セキュアプライベートアクセスをバイパスすることが保証されます。

   これらの変更を実装することで、グループBユーザーは、セキュアプライベートアクセスを経由せずにインターネット経由で会社のOutlookアプリケーションにアクセスできるようになり、必要に応じて他のABCアプリケーションへのアクセスも維持できます。

ユースケース: ユーザーコンテキストに基づくリソースロケーションの選択

シナリオ:

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

- XYZ社: 米国東海岸と米国西海岸にそれぞれユーザーグループがあります。
- データセンター: 東海岸と西海岸にそれぞれ1つずつ、合計2つのデータセンターがあり、どちらも同じJiraアプリケーションをホストしています。
- 目的: 管理者は、最適なパフォーマンスとルーティングを確保するために、ユーザーコンテキスト（地理的位置、ネットワーク位置、ユーザー名、ユーザーグループ）に基づいて、エンドユーザーのアクセス要求を選択されたリソースロケーションにルーティングしたいと考えています。

解決策:

1. Jiraアプリケーションに関連付けられているアクセスポリシーを編集して、新しいルーティング要件に対応します。
2. アクセスポリシー内で、**ルーティング例外**オプションを有効にします。
3. ユーザーコンテキストごとにリソースロケーションを変更します。

管理者は、ユーザーのコンテキストに基づいて最適なデータセンターにユーザー要求がルーティングされるようにすることで、パフォーマンスを向上させ、社内のすべてのユーザーに対してルーティングを効果的に管理できます。

ルーティングタイプまたはリソースロケーションを変更する手順

1. アクセスポリシーを作成または編集します。詳細については、「アクセスポリシーの作成」を参照してください。
2. **手順3: アクション**ページで、**ルーティング例外**トグルスイッチをスライドして、コンテキストルーティングドメイン構成を有効にします。 **ルーティング例外**トグルを使用すると、アクセスポリシーに追加されたアプリケーションのドメインのリソースロケーションとルーティング情報を編集できます。

    - **トグルがオンの場合:** すべてのアプリのURLと関連ドメインのリストが、グローバルルーティングとリソースロケーション構成とともに表形式で表示されます。このリストには、アクセスポリシーに追加されたすべてのアプリケーションのURLと関連ドメインが含まれています。ドメインの横にある編集アイコンをクリックすると、そのリソースロケーションとルーティングタイプを変更できます。このルーティング例外は、アクセスポリシー内のすべてのユーザーにのみ適用されます。
    - **トグルがオフの場合:** ドメインの既存のルーティング例外は削除され、適用されません。エンドユーザーは、アプリケーション設定時に設定されたグローバル構成に基づいてのみルーティングされます。

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

ルーティングタイプの変更(/en-us/citrix-secure-private-access/media/spa-modify-app-routing-type.png)

3. ルーティングタイプを変更するドメインの横にある編集アイコンをクリックします。
4. **ルーティングタイプ**で、ルーティングタイプを変更します。
   - **内部:** トラフィックはコネクタアプライアンスを経由して流れます。
     - Webアプリの場合、トラフィックはデータセンター内で流れます。
     - SaaSアプリの場合、トラフィックはコネクタアプライアンスを介してネットワーク外にルーティングされます。
   - **内部 – プロキシバイパス:** ドメインのトラフィックはCitrix Cloud Connector™アプライアンスを介してルーティングされ、コネクタアプライアンスで構成された顧客のWebプロキシをバイパスします。
   - **外部:** トラフィックはインターネットに直接流れます。
   - **Google Secure Gateway経由の外部:** トラフィックはGoogle Secure Gatewayを介してインターネットに流れます。

   注:

   このルーティングタイプは、Secure Private Accessクラウドおよびハイブリッド展開でGoogle Chrome Enterprise Premiumと統合された顧客のSaaSアプリにのみ適用されます。

5. 必要に応じて、**リソースの場所**でリソースの場所を変更します。このオプションは、内部ルーティングされたドメインにのみ適用されます。

   注:

   アプリがIPアドレスを使用して作成されている場合、**ルーティングタイプ**リストには**コネクタ経由の内部**オプションのみが表示されるため、ルーティングタイプを**外部**に変更することはできません。リソースの場所のみを変更できます。ただし、この制限はFQDNを使用して作成されたアプリには適用されません。

   ルーティングタイプIPの変更(/en-us/citrix-secure-private-access/media/spa-modify-app-routing-type2.png)

6. 「**保存**」をクリックします。

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

「

注記

：」：

- ルーティングとリソースの場所は変更できますが、ルーティングテーブルでルーティングドメインを追加または削除することはできません。
- メインルーティングテーブルからコンテキストルーティングが有効になっているドメインを削除しても、そのドメインはアクセスポリシー内の「**ルーティング例外**」テーブルから削除されません。これは、そのドメインのコンテキストルーティング構成がアクセスポリシー内でそのまま残ることを意味します。
- コンテキストルーティングが有効になっているアプリを削除すると、そのドメインはアクセスポリシー内の「**ルーティング例外**」テーブルから削除されます。これは、そのアプリに関連付けられているすべてのコンテキストルーティング構成がアクセスポリシーから削除されることを意味します。
- このアクセスポリシーの一部であるユーザーの条件が満たされた場合、選択された関連ドメインはデフォルト設定を上書きします。それ以外の場合、デフォルトのルーティングが適用されます。
- ルーティングが変更されていない場合、または「**ルーティング例外**」機能が有効になっていない場合、ルーティングはメインルーティングテーブル（**設定 > アプリケーションドメイン**）のデフォルト設定に基づいて行われます。

ユースケース：社内ユーザーをバックエンドアプリケーションに直接ルーティングする

管理者はセッションポリシーを構成して、Secure Private Access を介してトラフィックをトンネリングすることなく、社内ユーザーをバックエンドアプリに直接ルーティングできます。セッションポリシーは、ネットワークの場所やデバイスのポスチャなどの要因に基づいて動的なルーティングを提供します。詳細については、「セッションポリシー」を参照してください。

Monitor でのコンテキストルーティングのインサイト

コンテキストルーティングは、アプリケーションルートの動的な変更につながる可能性があります。たとえば、ユーザーが社内ネットワーク外にいる場合は Secure Private Access サービスを介してアプリケーションがルーティングされ、ユーザーが社内にいる場合はアプリに直接ルーティン

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

グされることがあります。管理者にこれらのルーティング決定の可視性を提供することは、ルーティングの問題をトラブルシューティングするために不可欠です。

DaaS Monitor の「**アプリケーション トポロジ**」ページでは、Citrix Secure Access クライアントを介してアクセスされる Secure Private Access アプリケーションのルーティングの決定とポリシーの詳細に関する包括的なインサイトが提供されます。これらのインサイトにより、管理者はルーティングの問題を効率的にトラブルシューティングし、ユーザーエクスペリエンスを向上させることができます。

アプリケーションルーティングに関連する以下の詳細が「**アプリケーション トポロジ**」ページにキャプチャされます。

- 「**ルーティングコンテキスト**」：「**概要**」セクションの「**ルーティングコンテキスト**」フィールドは、ルーティング中に適用されるポリシータイプ（アクセスポリシー、セッションポリシー、またはアプリケーションドメイン）を指定します。ルーティングコンテキストは、ルーティングの決定に影響を与える優先順位の階層（アクセスポリシー > セッションポリシー > デフォルトのアプリケーション構成）を特定するのに役立ちます。

  セッションポリシーの場合、「**詳細を表示**」リンクはセッションポリシーに関する追加の詳細を提供します。

- **アクションルーティング: ポリシー評価**セクションの**アクションルーティング**フィールドには、ユーザーのリクエストがSecure Private Accessサービスを介して辿るルーティングパス（**ダイレクト、コネクタ経由の内部、ゲートウェイ経由の内部**）が表示されます。

注:

デフォルトのアプリケーションドメイン（アプリケーション構成）ルーティングが適用される場合、**ポリシー評価**セクションにはポリシーの詳細が表示されますが、このシナリオではポリシーが適用されないため、**アクションルーティング**フィールドには値「**n/a**」が表示されます。

次の図は、ルーティングタイプがダイレクトとして定義されているため、トラフィックがSecure Private Accessサービスを通過しないアプリケーションのトポロジ図を示しています。

アプリケーションのトポロジ(/en-us/citrix-secure-private-access/media/spa-monitor-application-topology-allow-access.png)

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

注:

Citrix Secure Accessクライアントを介してトンネルされるWebアプリの場合、トポロジ図にはリソースロケーション名とコネクタ名が表示されます。

次の図は、コネクタを使用してSecure Private Accessサービスを介してルーティングタイプが内部として定義されているアプリケーションのトポロジ図を示しています。

アプリケーションのトポロジ(/en-us/citrix-secure-private-access/media/spa-monitor-application-topology-allow-access2.png)

詳細については、DaaSモニターとの統合を参照してください。

ローカルLANリソースへのシームレスなアクセス (プリンター、ファイルサーバー)

従業員がCitrix Secure Accessクライアントを使用して自宅またはリモートの場所からSecure Private Access経由で接続している場合、プライベートIPアドレス範囲が公開されている企業アプリと競合すると、ローカルネットワークリソースへのアクセスを失う可能性があります。Secure Private Accessは、企業リソースへの安全な接続を維持しながら、ローカルLANリソースへのシームレスなアクセスをサポートします。

たとえば、ホームプリンターがIPアドレス192.0.2.0で構成され、企業アプリケーションがプライベートIPアドレス192.0.2.0/30の範囲で構成されている場合、ユーザーがプリンターにアクセスしようとすると、プリンターのトラフィックもSPA経由でトンネルされ、エラーが発生します。ローカルLANアクセスを有効にすることで、ユーザーはCitrix Secure Accessクライアントを切断することなく、ローカルLAN経由でプリンターにアクセスできます。

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

注:

- 管理者は、すべてのユーザーまたは特定のユーザーに対して、セッションポリシーでローカルLANアクセス機能を有効にできます。詳細については、「セッションポリシーを使用して企業ネットワーク内で直接ルーティングを構成する」を参照してください。
- ユーザーがCitrix Secure Accessクライアントにログインするときにローカル LANアクセス機能を有効にすると、Secure Private Accessに接続しながら、ホームプリンター、ネットワーク接続ストレージ (NAS) デバイスなどのローカルLANリソースにアクセスできます。これにより、ユーザーは最小限の中断で基本的なローカルタスクを実行できます。

重要な考慮事項

- **すべてのユーザーに対してローカルLANアクセスを有効にする:** セッションポリシーは優先順位に従って評価されます。すべてのユーザーにローカルLANアクセスが必要な場合は、各アクティブなセッションポリシー内で**ローカルLANアクセス**オプションを明示的に有効にする必要があります。ユーザーがセッションポリシーに一致すると、評価は最初に適用されるポリシーで停止します。そのポリシーがローカルLANアクセスを許可しない場合、そのポリシーで**ローカルLANアクセス**オプションが有効になっていても、ユーザーは他の後続のポリシーに対して評価されません。
- **WindowsおよびmacOS用Citrix Secure Accessクライアントによるプリンタートラフィック処理の違い:** Windows用Citrix Secure AccessはローカルLANアクセスを優先します。つまり、プリンターのIPアドレスが企業アプリケーションのIPアドレスと競合する場合、Windows用Citrix Secure Accessクライアントは、Secure Private Access経由で送信する代わりに、アプリケーションのトラフィックをローカルに送信する可能性があります。対照的に、macOS用Citrix Secure Accessクライアントは、Secure Private Access経由でアプリケーションのトラフィックを同時にトンネルしながら、プリンターのトラフィックをローカルLANに送信できます。
- **定期的な更新:** ローカルLANアクセス機能はセッション固有であるため、Windowsフィルター (WFP) のローカルLAN設定に対する構成変更は、ログイン時に有効になり、ログアウトまで維持されます。定期的な更新はサポートされていません。

ローカルLANアクセス機能を有効にする

Secure Private Access管理コンソール:

1. **ポリシー > セッションポリシー**に移動し、セッションポリシーの作成をクリックします。

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

2. セッションポリシーを作成します。詳細については、「セッションポリシーを使用して企業ネットワーク内で直接ルーティングを構成する」を参照してください。
3. **ローカルLANアクセス**オプションが選択されていることを確認します。

SPAコンソールでのローカルLANアクセス(/en-us/citrix-secure-private-access/media/spa-session-policy.png)

Citrix Secure Accessクライアント:

1. Citrix Secure Accessクライアントウィンドウで、**ローカルLANアクセスを許可**を選択します。
2. **接続**をクリックします。

ローカルLANアクセス(/en-us/citrix-secure-private-access/media/spa-local-lan-access.png)

ローカルLANアクセスが有効(/en-us/citrix-secure-private-access/media/spa-local-lan-access-enabled.png)

ポリシーモデリングツール

複数のアプリケーションとアクセスポリシーを管理する場合、管理者にとって、正確なエンドユーザーのアクセス結果を判断するのは困難な場合があります。現在のすべての構成に基づいて、ユーザーがアプリケーションへのアクセスを許可されているか拒否されているか。

アクセスポリシー > ポリシーモデリングにあるポリシーモデリングツールは、現在の構成に基づいて、予想されるアプリのアクセス結果（許可、制限付き許可、または拒否）に関する包括的な可視性を管理者に提供します。管理者は、デバイスの種類、デバイスの姿勢、地理的位置、ネットワークの場所、ストアURLなどの条件に基づいて、任意のユーザーのアクセス結果を確認できます。管理者は、特定のアプリケーションの宛先に対するアクセスポリシーを評価することもできます。

ポリシーモデリングツールにアクセスする

1. Secure Private Accessコンソールで、**アクセスポリシー**をクリックし、次に**ポリシーモデリング**タブをクリックします。
2. ポリシーモデリングツールのユーザーインターフェイスが表示されます。
    - デフォルトでは、**すべてのアプリ**タブが選択されています。このタブは、環境内の複数のユーザー、ユーザーグループ、またはマシンに適用されるポリシーを分析するために使用できます。

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

- 特定のWebサイトドメイン、IPアドレス、またはネットワークポートなどの特定のネットワーク宛先にポリシーがどのように適用されるかを理解するには、**URL**または**IP/ポート**タブを使用して、宛先の詳細を入力する必要があります。

ユーザーまたはマシンのセットのポリシーを分析する

1. **ユーザー**または**マシン**タブを選択し、次の詳細を入力します。

   - **デバイスの種類:** エンドユーザーのデバイスの種類を選択します。（デフォルトではデスクトップが選択されています）。
   - **ドメイン:** ユーザーに関連付けられているドメインを選択します。
   - **ユーザー名またはユーザーグループ:** （**ユーザー**タブを選択した場合にのみ適用可能）アプリケーションと関連ポリシーを分析するユーザー名を選択します。
   - **マシン名:** （**マシン**タブを選択した場合にのみ適用可能）アプリケーションと関連ポリシーを分析する基準となるマシン名を入力します。

2. 正確な結果を検索するには、正確なユーザーまたはマシンの条件を追加します。

   - 「**条件をシミュレート**」をクリックします。
   - 条件（デバイスポスチャ、地理的位置、ネットワークロケーション、ユーザーリスクスコア、ストアURL）を選択し、関連する値を選択します。
   - 「+」記号をクリックして、条件を追加します。
   - 「**適用**」をクリックします。

特定の宛先に対するポリシーを分析する

1. Web/SaaSアプリケーションの場合は「**URL**」タブを、TCP/UDPアプリケーションの場合は「**IP/ポート**」タブをクリックします。
2. 次の詳細を入力します。

   - **URL:** アクセスポリシーを分析するアプリケーションのURL。
   - **IP:ポート:** アクセスポリシーを分析するTCP/UDPアプリのIPアドレスとポート番号。ホスト名の後にポート番号を入力することもできます。

   例: 192.0.2.20:443; example.test.net:443

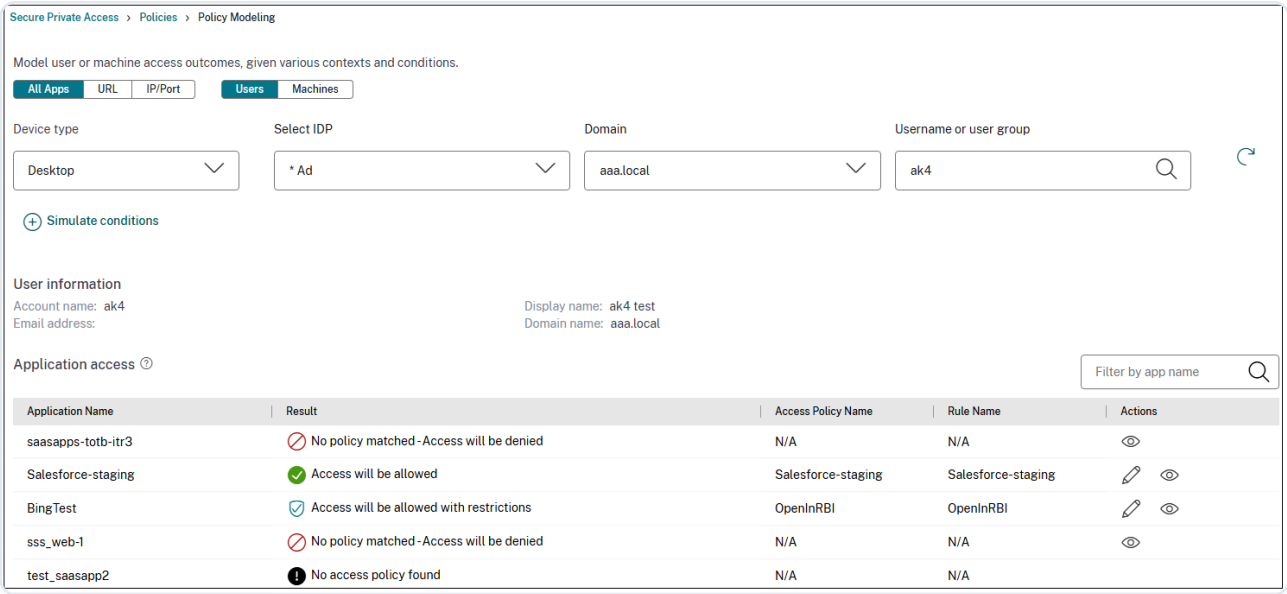
3. 「**適用**」をクリックします。

「**アプリケーションアクセス**」セクションには、検索に基づいてアプリケーションのリストと関連するポリシーが表示されます。正確なポリシーの一致またはポリシーの不一致が発生したアプ

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

リケーションの横には、目のアイコンが表示されます。管理者は、アクセスが許可されている、または制限付きでアクセスが許可されているアプリのポリシーを編集することもできます。

次の図は、すべてのアプリのポリシーアナライザーを示しています。



次の図は、Webアプリのポリシーアナライザーを示しています。

Webアプリのポリシーモデル(/en-us/citrix-secure-private-access/media/spa-policy-model1.png)

次の図は、TCPアプリのポリシーアナライザーを示しています。

TCPアプリのポリシーモデル(/en-us/citrix-secure-private-access/media/spa-policy-model-tcp-app.png)

アクセスポリシーの詳細を確認する

アプリケーションアクセスセクションで、目のアイコンをクリックして、アクセスとルーティングの詳細ページを表示します。**アクセスとルーティングの詳細**ページには、そのアプリケーションのアクセス決定に影響を与えたすべての関連ポリシーの包括的なリストが表示されます。このページには、次の情報が表示されます。

フィールド	説明
アプリケーション	アプリケーションの名前。
一致するアクセスポリシー	アプリケーションと完全に一致するか、主要な一致があるアクセスポリシーの名前。
ルール名	一致するポリシーに関連付けられている特定のルール。

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

フィールド	説明
予測される結果	ポリシー評価に基づいて決定されたアクション（例: 許可、拒否、制限付き許可）。
適用された制限	アプリケーションに適用されるアクセス制限（もしあれば）。
適用されたルートポリシータイプ	アプリケーションのルーティング動作を決定したポリシーのタイプを示します。ポリシータイプは、アクセスポリシー、セッションポリシー、またはアプリケーションドメインです。
	ルーティング決定における階層を識別します。優先順位は、アクセスポリシー（最高優先度）、セッションポリシー、そしてデフォルトのアプリケーションドメイン（最低優先度）の順です。
ルーティングタイプ	ルーティングタイプは、ユーザーのリクエストがSecure Private Accessサービスを介して辿るパスを詳細に示します。
	外部 リクエストは意図された宛先に直接ルーティングされます。
	コネクタ経由の内部 リクエストはコネクタを介してルーティングされます。
	Gateway経由の内部 リクエストはNetScaler Gatewayを介してルーティングされます。このルーティングタイプは、Citrix Secure Access クライアントでサポートされているハイブリッドデータパスにのみ適用されます。詳細については、「Secure Private Accessサービス用のハイブリッドデータパス」を参照してください。
プライマリリソースロケーション	アプリケーションのプライマリロケーションに関連付けられた名前。
バックアップリソースの場所	バックアップロケーションの名前（構成されている場合）。

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

次の図は、アクセスが許可されているTCPアプリのポリシー詳細分析結果を示しています。

ポリシーモデルのアクセスが許可されています(/en-us/citrix-secure-private-access/media/spa-policy-model-tcp-app-2.png)

次の図は、制限付きでアクセスが許可されているWebアプリのポリシー詳細分析結果を示しています。

ポリシーモデルのアクセス制限(/en-us/citrix-secure-private-access/media/spa-policy-model2.png)

次の図は、アクセスが拒否されているWebアプリのポリシー詳細分析結果を示しています。

ポリシーモデルのアクセスが拒否されました(/en-us/citrix-secure-private-access/media/spa-policy-model-access-denied.png)

アプリケーションインポートツール - プレビュー

Secure Private Access管理コンソールには、管理者がCSVファイルまたはnsconfigファイルを使用して複数のアプリケーションをシステムに一括インポートできるファイルインポートツールが含まれています。このツールは、従来のVPNからSecure Private Accessのようなより高度なソリューションに移行する組織にとって特に役立ちます。たとえば、組織はこのツールを使用して、VPN経由で提供されていたアプリケーションをSecure Private Accessに移行し、ZTNAベースのアーキテクチャに移行できます。アプリケーションの一括アップロードにより、組織は手動設定の必要性を排除できます。

- **CSVファイル:** すべての関連するアプリケーションの詳細がCSVに含まれていることを確認する必要があります。これらの詳細には、アプリケーション名、ルーティングタイプ、リソースロケーション、およびその他の必要な構成パラメータが含まれます。
- **NetScalerファイル:** 事前に生成されたCSVファイルを使用してアプリケーションをインポートすることもできます。このCSVファイルは、ns.confおよびns.logファイルから関連するアプリケーション構成を解析および抽出するスクリプトによって作成されます。スクリプトによって生成されたCSVにより、Citrix Secure Private Accessコンソールへのアプリケーション構成の効率的かつ正確なインポートが可能になります。

インポートの仕組み

CSVベースのアプリケーションインポートツールを使用する際に管理者が実行する必要がある大まかな手順は次のとおりです。

1. **CSVファイルの準備:** アプリケーションを手動で追加する場合は、CSVファイルにアプリケーションの詳細を入力します。詳細については、「CSVファイルの準備」を参照してください。

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

2. **CSVファイルのインポート:** 完成したCSVファイルをSecure Private Accessコンソールにインポートします。
3. **アプリケーションの詳細の確認:** インポートされたアプリケーションデータを確認および検証します。
4. **ルーティングとリソースロケーションの更新:** 必要に応じて、ルーティングタイプとリソースロケーションの詳細を確認および更新します。指定されたリソースロケーションで少なくとも1つのコネクタが稼働していることを確認してください。
5. **アプリケーションページでのアプリケーションの表示:** アプリケーションページでインポートされたアプリケーションを表示します。インポート用に選択したすべてのアプリケーションが正常にインポートされたかどうかを確認します。

この構造化されたプロセスにより、Secure Private Access環境内での安全でシームレスなアクセスを実現するための、アプリケーションの徹底的な移行と適切な構成が保証されます。

CSVファイルの準備

Secure Private AccessコンソールからCSVファイルをダウンロードし、アプリケーションの詳細を追加します。

1. **アプリケーション > アプリ構成**に移動します。
2. 「**アプリケーションのインポート**」をクリックします。
3. 「**CSV および NetScaler ファイルを使用したインポート方法**」で、「**CSV**」または「**NetScaler**」をクリックします。

   それに応じて、「**CSV を使用してインポート**」ページまたは「**NetScaler ファイルを使用してインポート**」ページが表示されます。

   - **CSV** - CSV ファイル (CSV テンプレート) をダウンロードし、アプリの詳細を入力します。このページには、入力する必要があるアプリデータのサンプル情報も表示されます。
   - **NetScaler**
     - Python スクリプトをダウンロードし、NetScaler の指定されたフォルダー (/var/spa/scripts) に保存します。
     - ns.conf および ns.log ファイルから CSV ファイルを生成するには、`python3 ztna-migration.py` としてスクリプトを実行します。
     - CSV ファイルが生成されたら、インポートのためにアップロードします。

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

注:

CSV ファイルから多数のアプリケーションをインポートする場合は、50 個のバッチで処理します。CSV をアップロードした後、最初の 50 個のアプリケーションを選択してインポートを完了し、次に次の 50 個を選択して、すべてのアプリケーションがインポートされるまで繰り返します。

「**例をダウンロード**」をクリックして、データを含むサンプル CSV ファイルを表示します。

CSV ファイルを使用してアプリケーションをインポートするためのガイドライン:

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

Import using CSV

Max file size: 5MB

Step 1:

Download the CSV template

Step 2:

Fill in the CSV template with all the necessary details. If any mandatory fields have missing or incorrect information, the import will fail. The following table explains the expected values in the CSV template.Learn more

Field	Description
App Name	Name of the application. Only alpha-numeric characters,spaces,and some special characters(.,_-) are allowed
App location	Network location of the app. Possible value "Inside Corporate Network" or "Outside Corporate Network"
App type	Possible values "HTTP/HTTPS", "TCP/UDP". For SaaS applications we define AppType as HTTP/HTTPS and AppLocation as Outside Corporate Network
URL	Main URL for the application. The URL must include "http://" or "https://"
Related domains	For HTTP/HTTPS applications, if multiple then add related domains comma separated Example *.abc.com, *.xzy.in . For TCP/UDP applications, leave this field blank
Destination/Port/Protocol	For HTTP/HTTPS applications, leave this field blank; for TCP/UDP applications, enter values in the format Destination:Port:Protocol (e.g., X.X.X.X:8080:PROTOCOL_TCP or host.vpn.net:5050:PROTOCOL_TCP), and for multiple entries, separate each with a comma (e.g., X.X.X.X:5050:PROTOCOL_TCP,X.X.X.X:1-65535:PROTOCOL_UDP)
Routing type	Possible values: For Cloud "Internal via connector" or "Internal bypass proxy" or "External". For Hybrid "Internal" or "External"
Primary Resource location	Name of the primary resource location
Secondary Resource location(Optional)	Name of the secondary resource location. Requires primary to be filled.
Description(Optional)	Description of the application
Category(Optional)	Category of the application
UniqueUsers	Number of unique users for the application. If value is not known , Mark the value as 0
TotalVisits	Total number of visits to the application (auto-generated if apps are extracted from ns.log) If value is not known , Mark the value as 0
UniqueUsersperApp	Total number of unique users per application (auto-generated if apps are extracted from ns.log) If value is not known , Mark the value as 0

Download examples

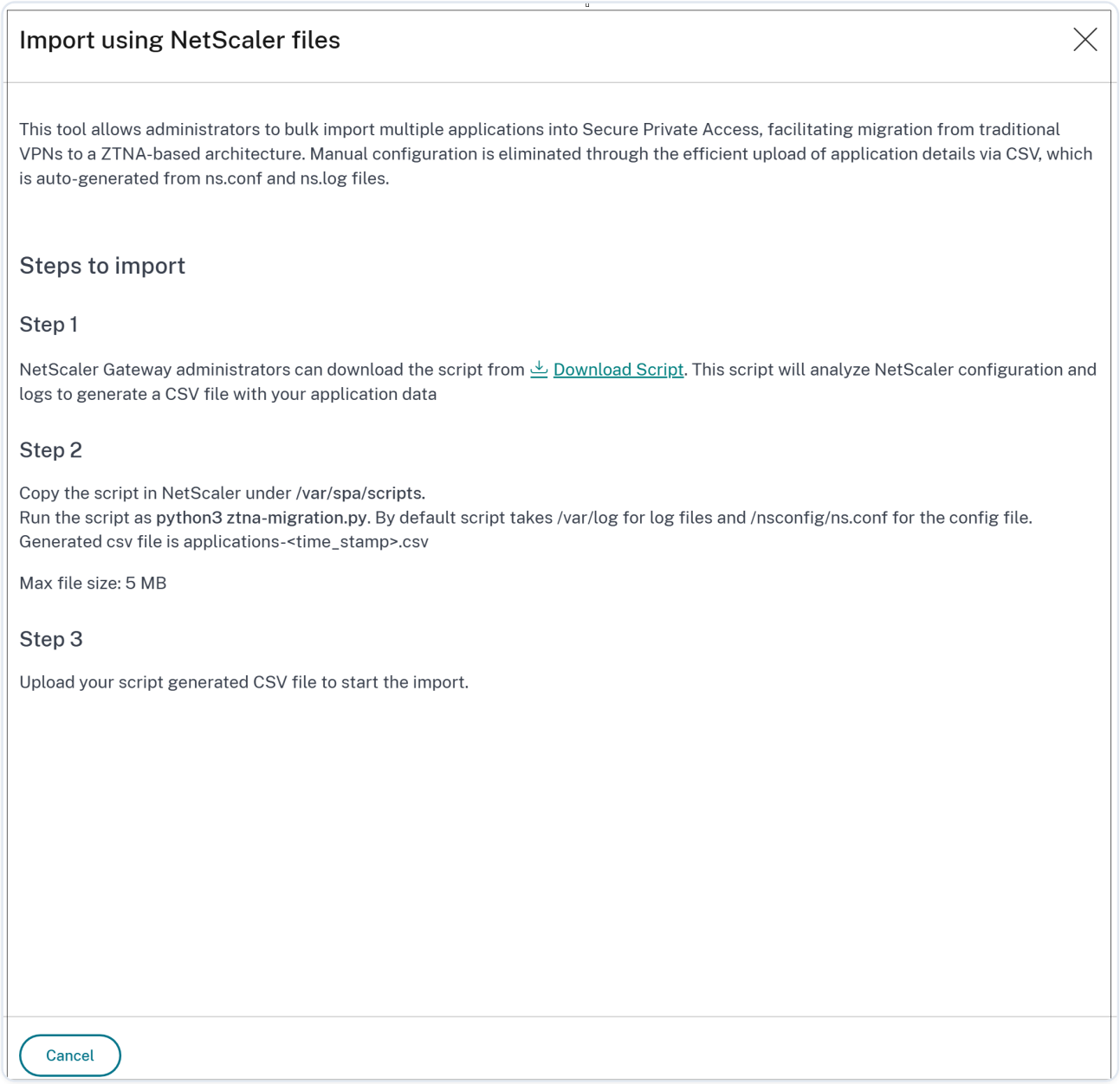
Step 3:

Upload the CSV file to start the import.

Done

NetScaler ファイルを使用してアプリケーションをインポートするためのガイドライン:

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



CSV ファイルに入力する値

アプリケーションを手動で作成する際に、CSVファイルの各列に入力する値に関するガイドラインを以下の表に示します。

列名	値
アプリの場所	社内ネットワーク内 (内部Webアプリ、TCP、UDPアプリの場合)
	社外ネットワーク (SaaSアプリの場合)
アプリの種類	以下のいずれかの値である必要があります。

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

列名	値
	HTTP/HTTPS
	TCP/UDP
URL	HTTP/HTTPSアプリにのみ適用されます。アプリケーションのURLです。URLには「http://」または「https://」を含める必要があります。
関連ドメイン	HTTP/HTTPSアプリにのみ適用されます。複数の関連ドメインをコンマ (,) で区切って追加できます。
	TCP/UDPアプリの場合、このフィールドは空白のままにしてください。
宛先ポートプロトコル	TCP/UDPアプリにのみ適用されます。すべてのIPアドレス、IPアドレス範囲、またはIP/CIDRとポートをコロン (:) で区切ってリストする必要があります。
	HTTP/HTTPSアプリの場合、このフィールドは空白のままにしてください。
	データを手動で入力する場合、宛先、ポート、プロトコルは次のようにフォーマットする必要があります。
	宛先:ポート:プロトコル。例: 192.0.2.254:5050:PROTOCOL_TCP。
	TCP/UDPアプリケーションに複数の宛先がある場合、複数の宛先エントリはそれぞれコンマで区切られます（例: X.X.X.X:5050:PROTOCOL_TCP,X.X.X.X:1-65535:PROTOCOL_UDP）。
	宛先は、IPアドレス、IPアドレス範囲、CIDR、ホスト名、ドメイン、またはFQDNにすることができます。ポートは単一ポート

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

列名	値
	（例: 5050）またはポート範囲（例: 1–65335）にすることができます。
ルーティングタイプ（クラウド環境）	アプリの種類に基づいて、次のいずれかの値を選択します。
	Internal – Bypass Proxy - ドメイントラフィックはCitrix Cloud Connector™を介してルーティングされ、Connector Applianceで構成された顧客のWebプロキシをバイパスします。
	Internal via Connector - アプリは外部または内部のいずれかですが、トラフィックはConnector Applianceを介して流れる必要があります。
	External – トラフィックはインターネットに直接流れます。
ルーティングタイプ（ハイブリッド環境）	**Internal** または **External**。
プライマリリソースロケーション	アプリケーションが存在するプライマリリソースロケーションの名前。
	注: ハイブリッド環境には適用されません。
セカンダリリソースロケーション (オプション)	アプリケーションが存在するセカンダリリソースロケーションの名前。セカンダリリソースロケーションは、プライマリリソースロケーションが明示的に指定されている場合にのみ適用されます。
	注: ハイブリッド環境には適用されません。
説明	(オプション) アプリケーションの説明。
カテゴリ	(オプション) アプリケーションカテゴリ。
UniqueUsers	アプリケーションのユニークユーザー数。

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

列名	値
	アプリがns.logファイルから抽出された場合、この値は自動生成されます。
	CSVファイルを手動で更新する場合は、空白のままにします。
TotalVisits	アプリケーションがアクセスされた合計回数。
	アプリがns.logファイルから抽出された場合、この値は自動生成されます。
	CSVファイルを手動で更新する場合は、空白のままにします。
UniqueUsersperApp	アプリケーションにアクセスしているユニークユーザーの総数。
	この値は、アプリがns.logファイルから抽出された場合に自動生成されます。
	CSVファイルを手動で更新する場合は、空白のままにします。

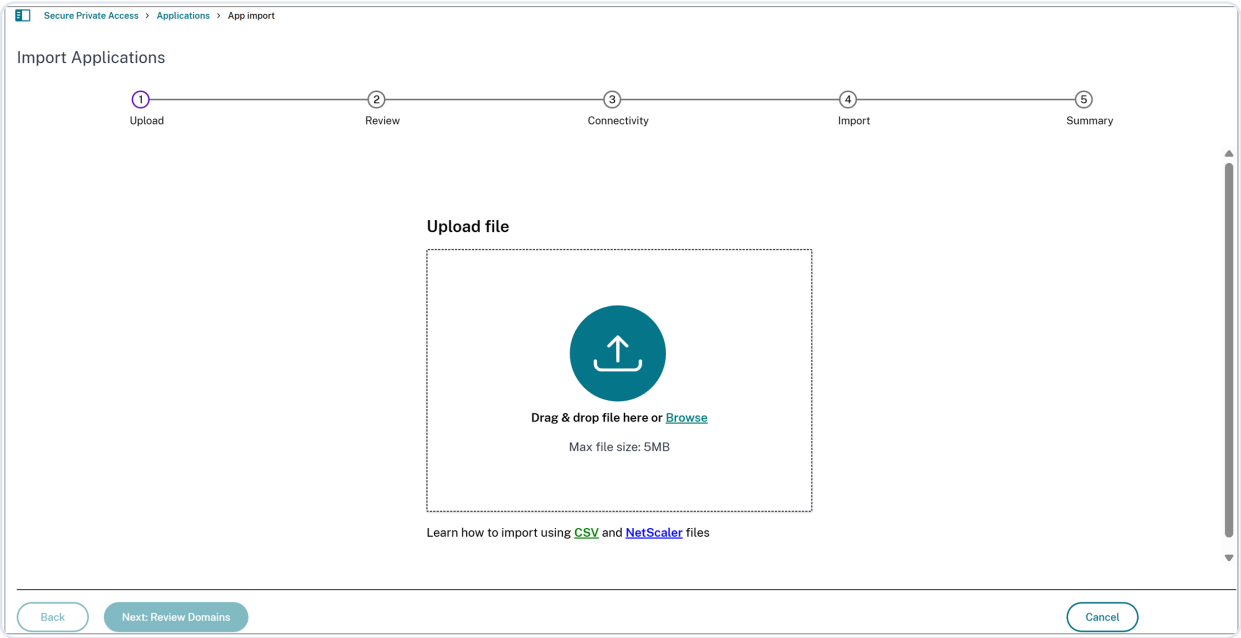
CSVベースのツールを使用してアプリケーションを移行する手順

Secure Private Access の設定中に、または設定完了後にアプリケーションをインポートできます。

1. Secure Private Access サービスタイルで、**管理**をクリックします。
2. 概要ページで、**続行**をクリックします。
3. ユーザーがストアにログインするためのIDと認証を設定します。詳細については、「IDと認証のセットアップ」を参照してください。
4. **ステップ2: アプリケーション**ページで、**アプリケーションのインポート**をクリックします。

   または、Secure Private Access がすでに設定されている場合は、アプリケーションページ (**Secure Private Access > アプリケーション**) から**アプリケーションのインポート**をクリックします。

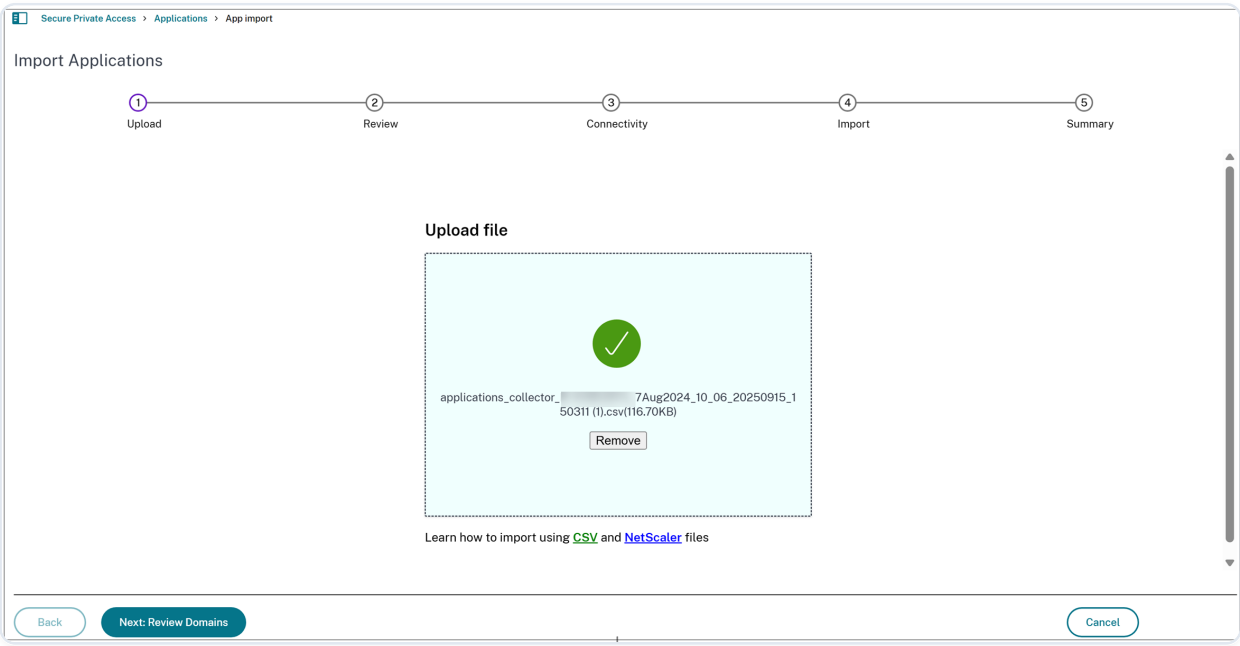
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. CSVファイルをアップロードします。CSVファイルをここにドラッグするか、参照して選択できます。
6. **次へ: ドメインの確認**をクリックします。

注:

- **次へ: ドメインの確認**ボタンは、ファイルにエラーがない場合にのみ有効になります。
- 追加のアプリケーションを含む同じCSV/nsconfigファイルをアップロードした場合、差分のみがインポートされます。



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

7. インポートしたいアプリケーションを選択します。

   アプリケーションを選択(/en-us/citrix-secure-private-access/media/import-applications-select-applications.png)

   注:

   - 同じドメインまたはワイルドカードドメインを持つアプリケーションが既に存在する場合、そのアプリケーションはインポートが無効になります。それらのアプリケーションを選択することはできません。
   - 各アプリケーションの行にある展開アイコンは、アプリに関する追加の詳細を表示します。
   - SaaS/WebおよびTCP/UDPアプリケーションの場合、**アプリケーションのインポート**ページには、アプリケーションへの総アクセス数とユニークユーザー数（アプリケーションにアクセスした個別のユーザー）が表示されます。展開アイコンを使用して、アプリケーションのポートとプロトコルの詳細を表示します。
   - CSV経由で手動でアップロードされたSaaSアプリ（企業ネットワーク外）は、アップロードが成功しても未公開としてマークされ、アプリケーションのインポートUIには表示されません。したがって、CSVファイルにエントリを手動で追加してSaaSアプリケーションを作成するには、**アプリの場所**を**企業ネットワーク外**に、**アプリの種類**を**HTTP/HTTPS**に設定する必要があります。
   - TCP/UDPアプリケーションの場合、このツールは関連するすべての宛先URLとIPアドレスを一覧表示します。デフォルトでは、アプリケーションを選択すると、関連するURLとIPアドレスがインポート用に自動的に選択されます。個々の宛先の選択を解除することはできません。

8. **次へ: 接続の確認**をクリックします。
9. **次へ: 接続の確認**ボタンは、少なくとも1つのアプリケーションが選択されている場合にのみ有効になります。
10. 接続設定を確認および更新します。必要に応じてルーティングタイプとリソースの場所に必要な変更を加え、**完了**をクリックします。

    接続の確認(/en-us/citrix-secure-private-access/media/import-applications-review-connectivity.png)

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

注:

- 指定されたリソースの場所が存在しない場合、顧客に関連付けられているリソースの場所のリストで利用可能な最初のリソースの場所がデフォルトで選択されます。 指定されたリソースの場所のコネクタアプライアンスが起動していない場合、アプリケーションの作成は失敗します。

11. **次へ: インポート**をクリックします。

アプリのインポート(/en-us/citrix-secure-private-access/media/import-applications-import.png)

注:

- **アプリケーションのインポート**ページには、インポートされたアプリケーションの詳細が表示されます。これらのアプリケーションは、**アプリケーション**ページのアプリケーションリストにも追加されます。
- 失敗したアプリケーションのインポートについては、失敗の理由が**理由**列に表示されます。この情報を使用してCSVファイルを修正し、それらのアプリケーションを再インポートしてください。

アプリのインポート(/en-us/citrix-secure-private-access/media/import-applications-page.png)

12. インポートされたアプリケーションを**アプリケーション**ページで表示するには、**アプリケーションに移動**をクリックします。

CSVファイル使用時のアプリケーションのインポートまたは作成の失敗

CSVファイルを使用する際に、以下の問題がインポートまたはアプリケーション作成の失敗を引き起こす可能性があります。

- 列名またはその大文字/小文字の変更。
- CSVファイル内の列の削除または入れ替え。
- CSVファイル内の必須アプリケーションフィールドの欠落。
- 空のCSVファイル、または列名のみを含むCSVファイルがインポートされた場合。空のファイルの場合、エラーメッセージが表示されます。ファイルに列名のみが含まれている場合、**次へ**ボタンは無効のままになります。
- CSVファイルで指定されたリソースの場所にConnector Applianceがありません。

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

- プライマリリソースの場所が欠落しているか空であるにもかかわらず、セカンダリリソースの場所が指定されている。インポートは、プライマリリソースの場所が必要であることを示す検証エラーで失敗します。

参照

Secure Private Accessでのアプリケーション作成に関する情報については、以下のトピックを参照してください。

- エンタープライズWebアプリのサポート
- SaaSアプリのサポート
- TCP/UDPアプリのサポート

クライアント内部IPアドレスプール - プレビュー

クライアント内部IPアドレスプールには、ログインユーザーに割り当てられるIPアドレス範囲が含まれています。各ユーザーとそのデバイスは、Secure Private Access内での識別とセッション管理に必要となる一意の内部IPアドレスを受け取ります。この内部クライアントIPアドレスは、顧客のリソースロケーション内でのみアクセス可能です。

この内部IPアドレスを使用すると、顧客のリソースロケーション内のデバイスは、特定のログインユーザーのデバイスにトラフィックを直接トンネルし、サーバーからクライアントへの接続を可能にします。クライアント内部IPアドレスは、既存のクライアントからサーバーへのトンネルトラフィックに対する送信元IPアドレスの固定化もサポートし、安定した一貫性のある接続を保証します。

注：

クライアント内部IPアドレスプール機能はプレビュー版です。この機能を有効にするには、Citrix®サポートにお問い合わせください。

クライアント内部IPアドレスプールのユースケース

- **サーバーからクライアントへの接続を有効にする：** 構成のプッシュ、リモートアシスタンスの提供、ソフトウェアのインストールなどの特定のタスクでは、サーバーがクライアントデバイスへの接続を開始する必要があります。クライアント内部IPアドレスプールは、クライアントデバイスを識別するために使用される定義済みのIPアドレス範囲を割り当てることで、これを可能にします。これらの内部IPプールは、ユーザーのコンテキストと場所に基づいて割り当て

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

られます。たとえば、特定のIPアドレス範囲を人事チームのようなユーザーグループに割り当てることができます。

サーバーからクライアントへの通信を有効にするには、サーバーからクライアントへのアプリを作成し、クライアントデバイスのポートとプロトコルの詳細、およびクライアントに到達するために使用されるバックエンドIPアドレス範囲を指定する必要があります。詳細については、「サーバーからクライアントへのアプリ構成」を参照してください。

- **クライアント内部IPアドレスの固定化を有効にする：** 一貫した接続を維持するために、一部のアプリケーションでは同じクライアントとの継続的なセッションが必要です。クライアントIPアドレスの永続性を有効にするには、「クライアントIPアドレスの固定化」を参照してください。

> **重要：**
>
> 送信元IPアドレスを内部IPアドレスとして使用する場合、またはサーバー開始接続機能を使用する場合は、以下を確認してください。

  - Connector Applianceのサブネットに接続されているスイッチまたはルーターがGratuitous ARPをサポートしていること。
  - ポートセキュリティおよび動的ARPインスペクション（DAI）構成が、送信元IPアドレスまたはサーバー開始接続機能に影響を与えないこと。

IPアドレスプールの制限事項

IPアドレスプールの制限事項を以下に示します。

- リソースロケーション内のすべてのコネクタアプライアンスは、同じIPサブネット内に存在する必要があります。
- 内部IPアドレスプールは、同じリソースロケーション内のコネクタアプライアンスサブネットからのIPアドレスで構成されている必要があります。
- 内部IPアドレスプール内のIPアドレスは、同じサブネット内のコネクタアプライアンスまたは他のデバイスで使用されているIPアドレスと重複してはなりません。
- プール内のIPアドレスが枯渇した場合、IPアドレスはユーザーに割り当てられず、そのためサーバーからクライアントへの接続およびクライアント内部IPスティッキネス機能は使用できません。
- ユーザーには最大3つの異なるIPアドレスを割り当てることができ、最大3つの異なるデバイスからのログインを許可します。同じユーザーが4番目のデバイスからログインした場合、IPア

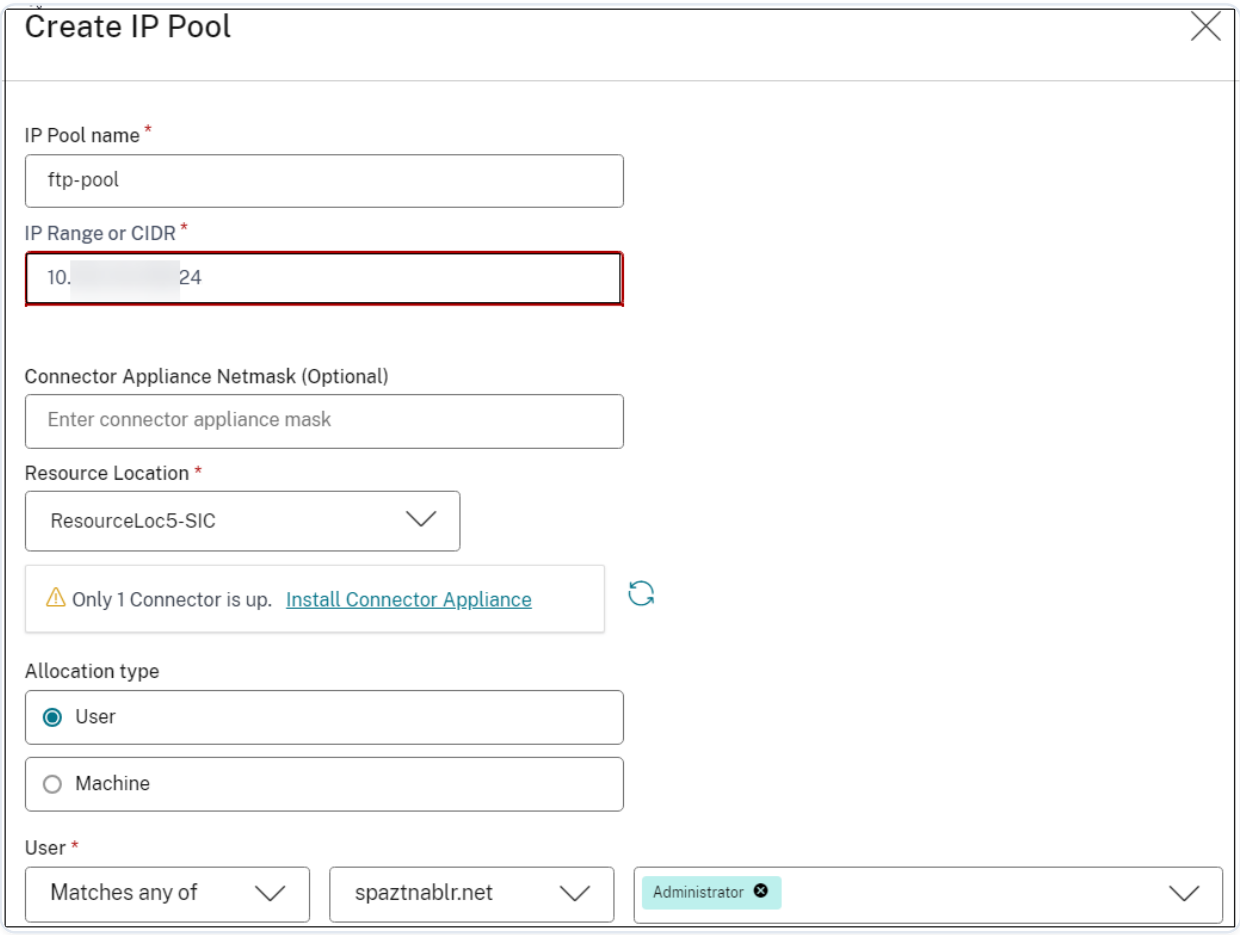
© 1997–2026 Citrix Systems, Inc. All rights reserved.

ドレスは割り当てられず、サーバーからクライアントへの接続およびクライアント内部IPスティッキネスの使用が妨げられます。

- 割り当てられた内部IPアドレスはスティッキーであり、同じデバイスでの毎日のログインとログアウトで同じままです。ただし、ユーザーが15日間連続して非アクティブの場合、そのスティッキーな内部IPアドレスは解放され、別のユーザーに再割り当てされます。

イントラネットIPアドレスプールを作成する

1. **設定 > IPプール** に移動し、**IPプールを作成** をクリックします。



2. **IPプール名**: IPプールの名前を入力します。
3. **IP範囲またはCIDR**: クライアント用に予約されているIPアドレスの範囲を入力します。これらのIPアドレスのいずれかがクライアントマシンに割り当てられます。
4. **コネクタアプライアンスのネットマスク**: (オプション)。コネクタアプライアンスのネットワークサブネットが内部IPアドレスサブネットと異なる場合、コネクタアプライアンスのネットマスクを入力する必要があります。
5. **リソースロケーション**: バックエンドサーバーが配置されているリソースロケーションを選択します。少なくとも1つのコネクタアプライアンスが稼働していることを確認してください。

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

6. **割り当てタイプ**: ユーザーを選択し、このプールが適用される条件、ドメイン、およびユーザーまたはユーザーグループを選択します。
7. **作成** をクリックします。

作成したIPアドレスプールは、IPプールページに表示されます。

IPアドレスプールページ(/en-us/citrix-secure-private-access/media/ip-pools-page.png)

クライアントのログインが成功すると、クライアント内部IPアドレスプールからユーザーにイントラネットIPアドレスが割り当てられます。

前の画像に示すように、管理者は優先順位付けメカニズムを使用してプールの優先順位を制御できます。管理者は、各IPプールに明示的な優先順位レベルを定義できます。Secure Private Accessサービスは、最も高い優先順位から最も低い優先順位（上から下）にIPアドレスを割り当て、予測可能な割り当てと運用制御を保証します。

注：

値が小さい優先順位ほど、優先度が高くなります。

IPアドレスプールを削除する

IPアドレスプールは、次のいずれかのオプションを使用して、すぐに、または時間をかけて削除できます。

- **IPプールを強制的に削除：** 新しいユーザーへのIPアドレスの割り当てを停止し、未使用のIPアドレスを直ちに解放します。削除されたIPアドレスを使用しているアクティブなユーザーセッションは終了され、突然の終了や強制ログアウトにつながる可能性があります。終了したセッションを持つユーザーには、別のIPアドレスプールが作成された後にのみ、新しいIPアドレスが割り当てられます。
- **IPプールを時間をかけて削除：** 新しいユーザーへのIPアドレスの割り当てを停止し、未使用のIPアドレスを直ちに解放します。システムは、プールを完全に削除する前に、アクティブなセッションがログアウトまたは期限切れになるのを待ちます。終了したセッションを持つユーザーには、別のIPアドレスプールが作成された後にのみ、新しいIPアドレスが割り当てられます。

注：

メンテナンス期間をスケジュールし、ユーザーにログアウトを通知してから、IPプールを時間をかけて削除することをお勧めします。スケジュールされた時間後にほとんどのIPアドレスが解放され

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

た場合は、残りの使用中のIPアドレスを強制的に削除できます。ただし、大規模なIPアドレスプールを強制的に削除することはお勧めしません。

IPプールを削除するには、次の手順を実行します。

1. **設定 > IPプール**に移動します。

   IPアドレスプールとその詳細のリストが表示されます。
2. 削除したいアドレスプール名の横にある省略記号（...）をクリックし、「**IPプールを強制的に削除**」または「**IPプールを時間指定で削除**」のいずれかを選択します。

IPアドレスプールの削除(/en-us/citrix-secure-private-access/media/ip-pools-delete.png)

IPプール削除オプション(/en-us/citrix-secure-private-access/media/ip-pools-force-delete.png)

注：

プールが削除された場合、または削除がスケジュールされている場合、管理者はその優先度を下げる必要があります。Secure Private Accessがそのプールから新しいIPアドレスの割り当てを停止するように、このプールの優先度は他のアクティブなプールよりも低くする必要があります。IPアドレスの割り当ては、自動的に優先度の高いプールにフォールバックします。

IPアドレス使用状況データを表示する

IPプール使用状況ページからIPアドレスの使用状況データを監視できます。このページには、IPアドレスのステータスの概要が表示されます。

- ユーザーのリストと、それらのユーザーに割り当てられているIPアドレス。
- 既に割り当てられている利用可能なIPアドレスの割合と、割り当て可能なIPアドレスの総数。

管理者はこのデータを使用してIPアドレスの消費を監視し、ユーザーに十分なIPアドレスが利用可能であることを確認できます。

IPアドレスの使用状況の詳細を表示するには、次の手順を実行します。

1. **設定 > IPプール**に移動します。

   IPアドレスプールのリストとその詳細が表形式で表示されます。
2. アドレスプールの横にある省略記号（...）をクリックし、「**IP使用状況の表示**」をクリックします。

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

一貫した接続を維持する

セッションの継続性が必要なアプリケーションに対して、永続的で一貫した接続を確保するために、管理者はアプリケーションの種類 (Web/SaaS または TCP/UDP) に応じて、コネクタースティッキネスまたはクライアント IP アドレススティッキネスのいずれかを有効にできます。Secure Private Access は、コネクタースティッキネスとクライアント IP アドレススティッキネスの両方をサポートしています。

- **コネクタースティッキネス**は、クライアントがコネクターアプライアンスとの接続を確立した後、そのクライアントからの後続のすべてのリクエストが同じソース (コネクターアプライアンス) に向けられることを保証します。
- **クライアント IP アドレススティッキネス**は、特定のクライアント IP アドレスからのリクエストが、常に同じバックエンドサーバーにルーティングされることを保証します。

コネクターまたはクライアント IP アドレススティッキネスは、アプリケーションの作成中に有効にできます。

- Web/SaaS アプリケーションの場合、管理者は**一貫した接続を維持**オプションを有効にできます。
- TCP/UDP アプリケーションの場合、管理者は要件に応じて、**クライアント IP**スティッキネスと**コネクター ID**スティッキネスのいずれかを選択できます。

詳細については、以下のセクションを参照してください。

- コネクタースティッキネス
- クライアント IP アドレススティッキネス

重要:

- クライアント IP アドレススティッキネス機能はプレビュー版です。
- クライアント IP アドレススティッキネスを有効にするには、管理者はクライアント内部 IP アドレスプールを構成する必要があります。IP アドレスプールは、ユーザーと関連デバイスに一意の IP アドレスを割り当てるために不可欠です。顧客リソースロケーションからのデバイスは、クライアントの内部 IP アドレスを使用して、特定のログイン済みユーザーのデバイスにトラフィックをトンネルできます。詳細については、クライアント内部 IP アドレスプールを参照してください。

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

コネクタースティッキネス

一部のアプリケーションではコネクタースティッキネスが必要です。これは、初期ログインとそれに続くリクエストを含む、ユーザーセッションのすべてのリクエストが同じコネクターアプライアンス (同じ IP アドレス) から送信されることを意味します。リクエストが別のコネクターアプライアンスを経由してルーティングされると、アプリケーションが正しく機能しない可能性があります。

- コネクタのスティッキネスは、特定のユーザーセッションに固有のものです。同じユーザーがアプリを再度開いた場合、トラフィックは別のConnector Applianceにルーティングされる可能性があります。
- Connector Applianceは、特定のリソースロケーションで利用可能なConnector Applianceの中からランダムに選択されます。
- Connector Applianceに障害が発生した場合、接続は同じリソースロケーション内の別のApplianceにリダイレクトされます。

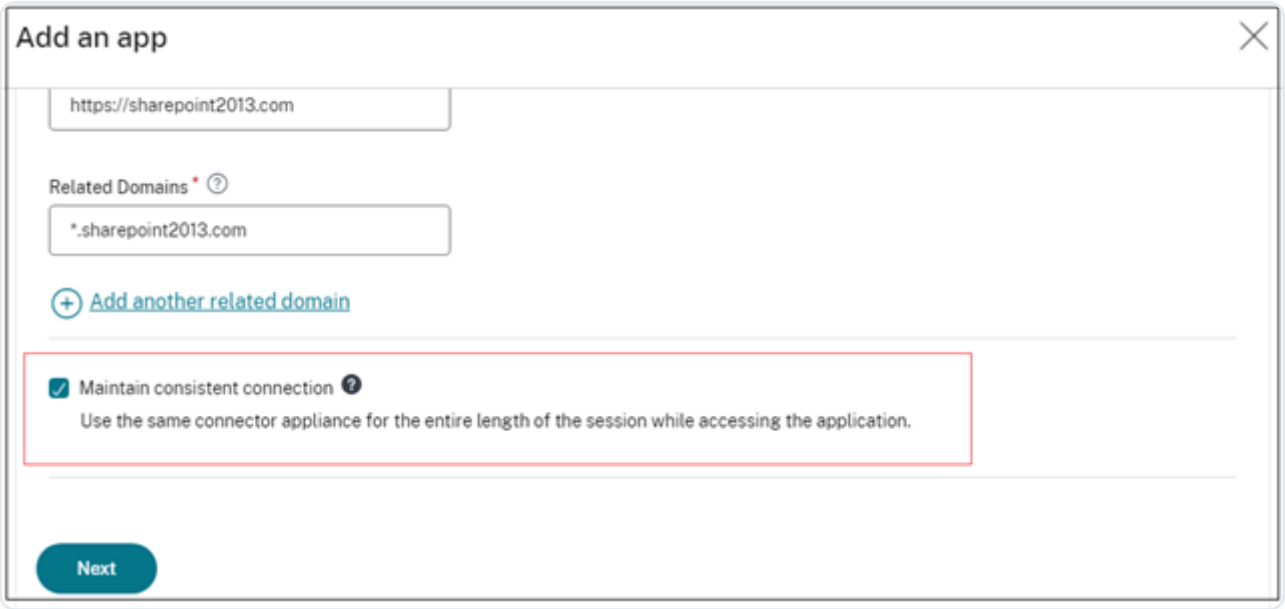
コネクタのスティッキネスは、次のシナリオで重要です。

- NTLMプロトコルは、セッション状態を維持するためにIPアドレスに依存します。要求が別のコネクタを経由してルーティングされると、NTLM認証が失敗し、エラーやログイン失敗につながる可能性があります。
- パッシブFTPに基づくアプリケーションは、制御接続とデータ接続の両方が同じバックエンドサーバーにルーティングされることを保証するために、接続のスティッキネスを必要とします。このスティッキネスがないと、FTPセッションが失敗する可能性があります。

アプリケーションのコネクタのスティッキネスを有効にする方法については、次のトピックを参照してください。

- Webアプリを構成する
- SaaSアプリを構成する
- TCP/UDPアプリを構成する

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



クライアントIPアドレスのスティッキネス - プレビュー

クライアントがリソースロケーション内の複数のConnector Appliance間で負荷分散を介してバックエンドサーバーに接続する場合、トラフィックの送信元IPアドレスが別のConnector AppliceのIPアドレスとして表示されることがあります。このIPアドレスの不一致は、次のような問題につながる可能性があります。

- **TCP/UDPアプリケーション:** 特定のアプリケーションでは、特定のクライアントとサーバー間で一貫したセッションが必要です。送信元IPアドレスが変更されると、これらのアプリケーションは起動に失敗する可能性があります。パッシブFTP、アクティブFTP、一部のWebサーバーなどのアプリケーションは、正しく機能するためにIPアドレスアフィニティ（スティッキネス）に依存しています。
- **セキュリティおよび監視システム:** 送信元IPアドレスが頻繁に変更されると、これらのシステムはトラフィックの追跡と分析が困難になる可能性があります。

ソースIPアドレスのアフィニティ/スティッキネスを維持するために、TCP/UDPアプリケーション(クライアントからサーバーへ) に対してクライアント内部IPアドレスの固定を構成できます。クライアントIPアドレスの固定により、ログイン時にユーザーセッションに一意の内部IPアドレスが割り当てられます。このIPアドレスは、リソースの場所にあるコネクタアプライアンスのIPアドレスの代わりに使用されます。この割り当てにより、クライアントからバックエンドサーバーへのすべての接続で、ログイン時に割り当てられたクライアント内部IPアドレスがソースIPアドレスとして使用されることが保証されます。クライアントIPアドレスの固定は、接続中に使用されるコネクタアプライアンスに関係なく、セッションの永続性を維持します。

クライアントIPアドレスの永続性を有効にするには、「TCP/UDPアプリケーションのクライアントIPアドレスの固定を有効にする」を参照してください。

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

前提条件

IPアドレスプールが作成されていることを確認してください。IPアドレスプールは、ユーザーと関連デバイスに一意のIPアドレスを割り当てるために不可欠です。詳細については、「クライアント内部IPアドレスプール」を参照してください。

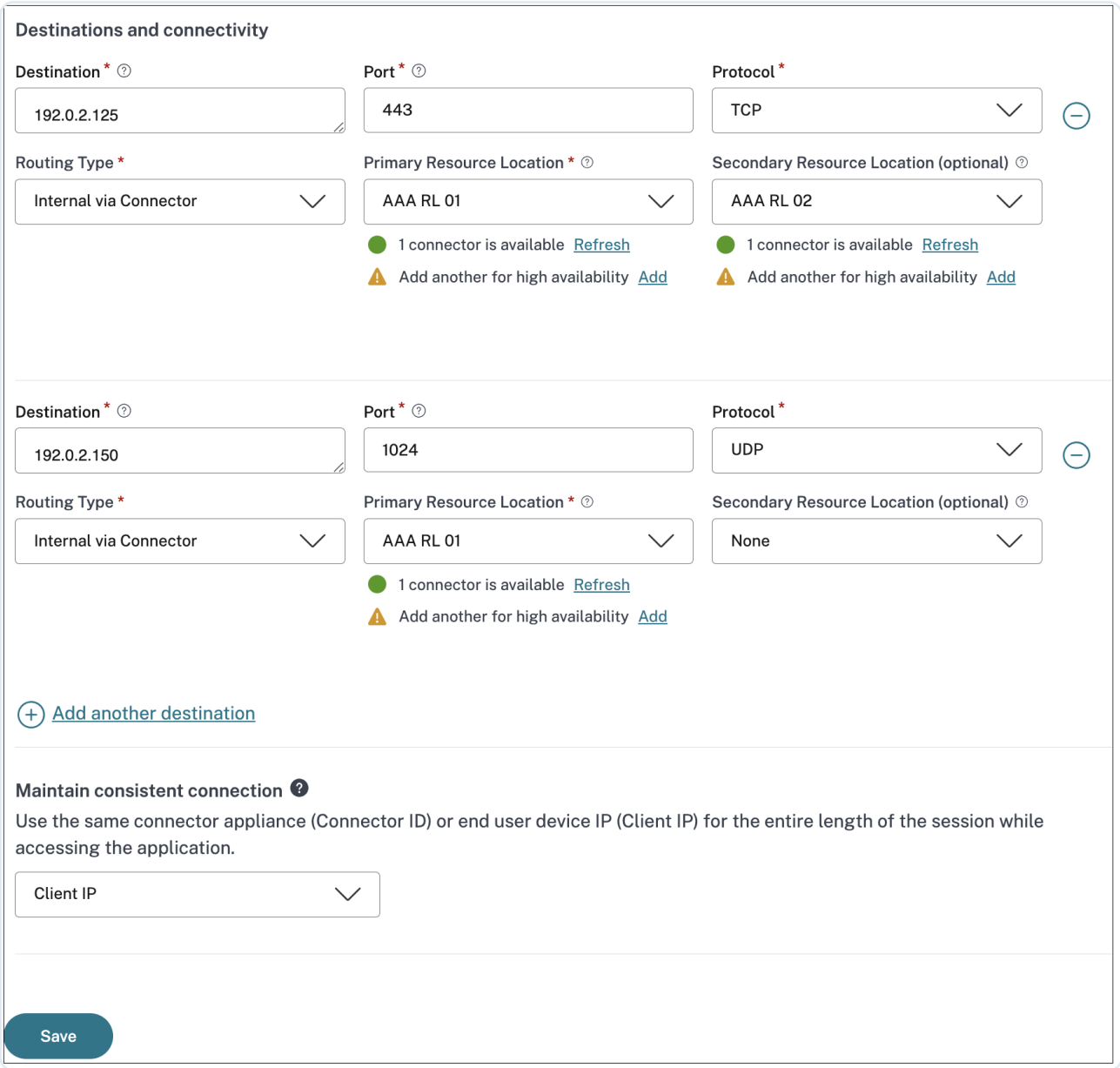
TCP/UDPアプリケーションのクライアントIPアドレスの固定を有効にする

トピック「TCP/UDPアプリのサポート」で概説されている手順を実行します。

アプリの詳細セクションで、**一貫した接続を維持**で次のいずれかの値を選択して、クライアントIPの固定を有効または無効にします。

- **使用しない:** アプリケーションは永続性を必要としません。アプリケーションは任意のソースIPアドレスで動作できます。
- **クライアントIP:** アプリケーションは、接続ごとにクライアントに対して同じソースIPアドレスを使用します。
- **コネクタID:** アプリケーションは、セッションごとに同じコネクタアプライアンスに接続します。

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



注:

クライアントIPアドレスの固定を有効にするには、内部IPアドレスプールを作成したときに使用したのと同じリソースの場所を選択し、アプリ接続セクションで同じリソースの場所が設定されていることを確認してください。

アクティブなセッションを終了し、ユーザー/マシンをブロックリストに追加する

管理者は、すべてのアクティブなセッションを直ちに終了し、ユーザー/マシンをブロックリストに追加できます。ユーザー/マシンをブロックリストに追加すると、すべてのアクティブなSecure

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

Private Accessアプリケーションセッションが終了し、今後のアプリケーションアクセスがブロックされます。

Chrome Enterprise Premiumブラウザ、直接アクセス、HTML5用Citrix Workspaceアプリ、およびSecure Accessエージェントを介したすべてのアクティブなアプリケーションセッションは終了され、ブロックされます。ファイル共有、RDP、SSHセッションなど、Secure Accessエージェントを介して接続されたすべてのリソースも終了され、ブロックされます。ユーザーは、ブロックリストからユーザー/マシンが削除されるまで、新しいアプリケーションを起動できません。

アプリケーションがChrome Enterprise Premiumブラウザを使用してアクセスされる場合、アクティブなブラウザベースのセッションも終了され、無効化されたユーザーからのさらなるアクセス要求は、Secure Private Accessブロックリストポリシーに従って拒否されます。

注:

- ユーザー/マシンをブロックリストに追加しても、構成済みのSecure Private Accessアクセスポリシーが変更または編集されることはありません。アクセスの終了とブロックは、どのようなアクセスポリシーが構成されていても発生します。ユーザー/マシンがリストから削除されると、そのユーザーに対する既存のSecure Private Accessアクセスポリシーが復元されます。
- Internet access via the Citrix Enterprise Premium browser is allowed even after a user is added to the block list. Only access to published Secure Private Access applications is blocked.

ユースケース

この機能は、次のシナリオで使用できます。

- An employee quits the organization or is terminated from the organization. In this case, the admin revokes all Secure Private Access app access by terminating active Secure Private Access sessions and blocking any future app access.
- デバイスが紛失または盗難された場合。この場合、アクセスはブロックされ、すべての現在のセッションが終了します。状況が収拾された後、ユーザーはブロックリストから削除できます。
- ユーザーがアプリアクセスを悪用した場合。この場合、ユーザーのアクセスは直ちに取り消すことができます。ユーザーがリストに追加されるまで、アクセスはブロックされます。

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

Chrome Enterprise Premiumを使用している場合のユーザーブロックの前提条件

Chrome Enterprise PremiumとSecure Private Accessを使用してユーザーをブロックするには、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。

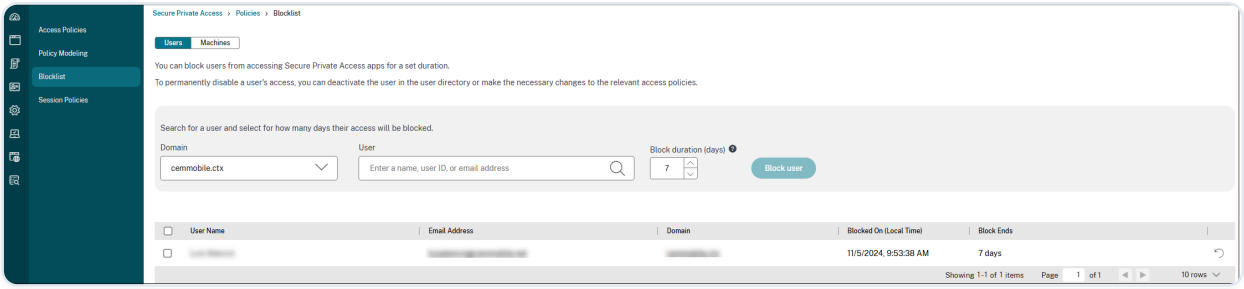
- MicrosoftによるGoogle Cloud / G Suite Connectorを介してMicrosoft Entra IDユーザーを同期する場合、ユーザーIDがCitrix Secure Private Accessユーザーレコードと一致するように、正しい属性マッピングが構成されていることを確認してください。

この設定が行われていない場合、Chrome Enterprise Premiumブラウザを介してアプリケーションにアクセスするユーザーに対して、ユーザーブロックポリシーが適用されない可能性があります。

ユーザー/マシンをブロックリストに追加する

1. **Secure Private Access > ポリシー > ブロックリスト**に移動します。
2. **ドメイン**で、アクセスを無効にするドメインを選択します。
3. **ユーザー**で、ブロックリストに追加する必要があるユーザー名を検索します。検索条件に一致するすべてのユーザー名が表示されます。ユーザーがディレクトリサービスから削除された場合、そのユーザー名は**ユーザー**リストに表示されません。

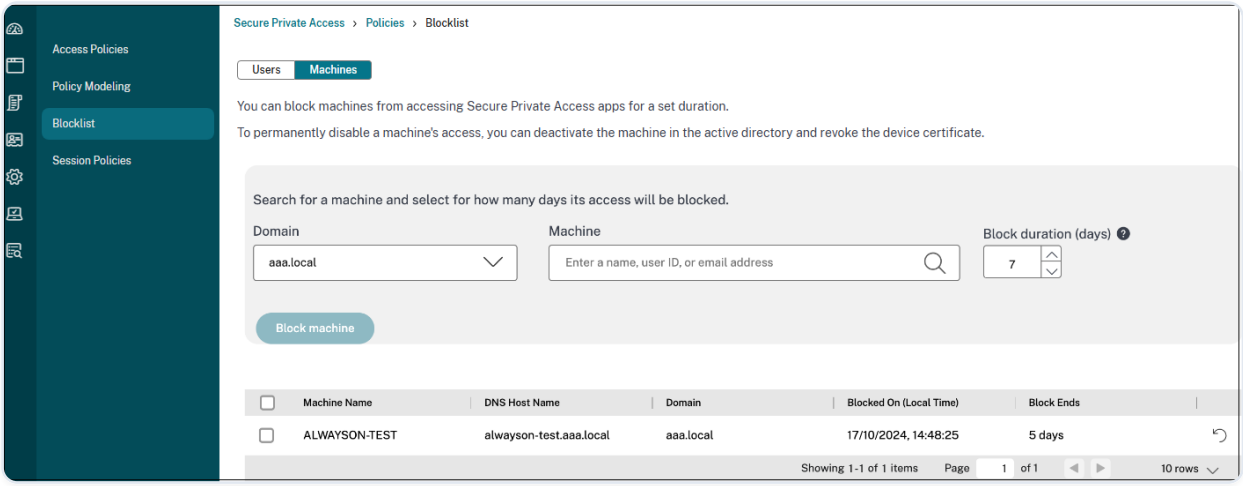
> **注:**
>
> **ユーザー**フィールドは、**ユーザー**タブが選択されている場合にのみ表示されます。



4. **マシン**で、ブロックリストに追加する必要があるマシン名を検索します。検索条件に一致するすべてのマシン名が表示されます。マシンがディレクトリサービスから削除された場合、そのマシン名は**ユーザー**リストに表示されません。

> **注:**
>
> **マシン**フィールドは、**マシン**タブが選択されている場合にのみ表示されます。

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



5. **ブロック期間 (日数)**で、このユーザー/マシンをブロックする日数を入力します。ユーザー/マシンをブロックリストに追加すると、デフォルトで7日間ブロックされます。ただし、期間は1日から99日の間で変更できます。期間が終了すると、ユーザーディレクトリとポリシー構成に基づいてアクセスが復元されます。また、この値は将来の追加のためにユーザーに対して永続的に保持されます。たとえば、管理者がユーザー/マシンのブロック期間を30日に設定した場合、この設定は将来の追加のためにユーザー/マシンに保持されます。
6. **ユーザーをブロック**または**マシンをブロック**を適宜クリックします。

> **注:**
>
> 「**ユーザーをブロック**」または「**マシンをブロック**」フィールドは、選択されているタブ（「**ユーザー**」または「**マシン**」）によって表示されるようです。

ユーザー/マシンがブロックリストに追加されます。

推奨事項:

- ブロック期間が終了する前でも、以下のいずれかの手順を実行することでアクセスを復元できます。
  - アクセスを復元する必要があるアクセスを選択し、「**アクセスを復元**」をクリックします。
  - アクセスを復元したいユーザーと同じ行にある復元アイコンをクリックします。

    どちらの場合も、確認ダイアログが表示されます。
- ユーザー/マシンのアクセスを無期限に失効させるには、Active Directoryなどの該当するディレクトリサービスからユーザー/マシンを削除し、ブロックリストに追加します。これにより、アクティブなSecure Private Accessセッションが終了し、今後のアプリへのアクセスがブロック

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

され、ユーザー/マシンがストアからログアウトすると、非アクティブなディレクトリ資格情報のため、ユーザー/マシンは再度ログインできなくなります。

ユーザー/マシンがブロックリストに追加された後のエンドユーザーエクスペリエンス

以下のセクションでは、ユーザー/マシンがブロックリストに追加された後のエンドユーザーエクスペリエンスに関する詳細情報を提供します。

クラウド経由でアクセスされるアプリケーション

ユーザーがブロックされた場合:

- すべてのアクティブなSecure Private Accessセッションは直ちに終了します。
- すべてのSecure Private Access公開アプリケーションへの今後のアクセスはブロックされます。
- ユーザーがブロックリストに追加された後でも、Citrix Enterprise Premiumブラウザを介したインターネットアクセスは許可されます。公開されたSecure Private Accessアプリケーションへのアクセスのみがブロックされます。

マシンがブロックされた場合：

- マシンがブロックリストに追加されると、ユーザーの現在実行中のすべてのアプリケーションへのアクセスがブロックされます。
- 新しいアプリケーションにアクセスしようとすると、ログアウト要求がトリガーされます。

オンプレミスNetScaler® Gateway経由でアクセスされるアプリケーション（ハイブリッドデータパス）

- クラウドセッションが終了すると（ユーザー操作または取り消しによって）、対応するアクティブなNetScaler Gatewayセッションは自動的に終了します。
- ブロックされたユーザーがNetScaler Gatewayを介して新しいアプリケーションにアクセスしようとすると、システムはログアウト要求をトリガーします。

ユーザーセッションのタイムアウト

WebアプリとCitrix Secure Access™クライアントのタイムアウト期間を設定して、指定された期間ネットワークアクティビティがない場合にユーザーセッションを終了できます。 Citrix Secure Accessクライアントの場合、指定された期間ユーザーアクティビティがない場合にセッションを終了するようにCitrix Secure Accessクライアントを設定することもできます。また、設定された

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

期間が経過すると、ユーザーおよびネットワークアクティビティに関係なく、Citrix Secure Accessクライアントで強制切断を設定できます。

Webアプリサーバーのタイムアウト

1. **>** の順に移動します。
2. で、Webアプリセッションがアイドル状態になる期間を時間と分で選択します。セッションがアイドル状態のままでこの時間が経過すると、Secure Private Accessサービスはセッションを終了します。

   最小期間は1時間、最大期間は168時間です。デフォルト値は2時間です。

Webアプリのタイムアウトを設定する(/en-us/citrix-secure-private-access/media/secure-private-access-timeout-for-webapps.png)

Citrix Secure Accessクライアントのタイムアウト

Citrix Secure Accessクライアントには、次のタイムアウトを設定できます。

- クライアントの非アクティブ
- 強制タイムアウト

1. **>** の順に移動します。

   ZTNAアプリのタイムアウトを設定する(/en-us/citrix-secure-private-access/media/secure-private-access-timeout-for-client-server-appss.png)
2. で、適用するタイムアウトの期間を時間と分で選択します。

   - **クライアント非アクティブタイムアウト**: 設定された期間、ユーザーアクティビティ（マウスまたはキーボード）がない場合に、Citrix Secure Accessクライアントがセッションを終了するまでの期間。このオプションはデフォルトで無効になっています。設定されたタイムアウト期間を適用するには、トグルスイッチを使用してこのオプションを有効にする必要があります。ただし、設定を保存した後にトグルスイッチを無効にすると、クライアントはタイムアウトを開始しません。

     最小期間は5分、最大期間は168時間です。デフォルト値は8時間です。
   - **強制タイムアウト**: ユーザーまたはネットワークアクティビティに関係なく、Citrix Secure Accessクライアントがセッションを終了するまでの期間。このオプションはデフォルトで無効になっています。設定されたタイムアウト期間を適用するには、トグルスイッチを使

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

用してこのオプションを有効にする必要があります。ただし、設定を保存した後にトグルスイッチを無効にすると、クライアントはタイムアウトを開始しません。

セッション終了の15分前に通知メッセージが表示されます。

最小期間は1時間、最大期間は168時間です。デフォルト値は168時間です。

注:

これらの設定を複数有効にした場合、最初に期限切れになるタイムアウト間隔がユーザー接続を閉じます。

構成レポート

顧客管理者は、Secure Private Access の設定に関する洞察を得るために構成レポートを生成できます。構成レポートには、次のカテゴリの情報が含まれます。

- アプリケーションとリソースへのアクセスを管理するアクセスポリシー。
- Secure Private Access 内で構成されたアプリケーション。
- アプリケーション用に設定されたルーティングドメイン。
- 顧客に関連付けられたリソースロケーション。
- ユーザーIDの検証に使用される認証ドメイン。
- ユーザーIDに使用されるIDプロバイダー (IdP)。
- 特定の顧客向けに定義された顧客パラメーター。
- クラウドストアに関連するストア構成。

構成レポートは、次のシナリオで使用できます。

- 構成の問題を特定し、解決する。
- 調査およびトラブルシューティングの目的で Citrix サポートチームと共有する。
- 新しいセットアップの参照として、または既存のセットアップの詳細を変更するためにレポートを使用する。

構成レポートを生成する

設定レポートを生成するには、以下の手順を実行します。

1. Secure Private Access 管理コンソールで、**設定 > グローバル構成**に移動します。

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

2. レポート生成プロセスを開始するには、**レポートの作成**をクリックします。

   レポートが生成されると、**構成レポート**ダイアログに次のステータスが表示されます。

   - **レポート完了:** 必要なすべての詳細がレポートに正常に含まれていることを示します。
   - **レポート一部完了:** 一部の詳細が欠落しているか、生成されていないことを示します。

     ダイアログには、レポート生成が不完全だったカテゴリも表示されます。

   次の図は、完了および一部完了ステータスを示す構成レポートダイアログの例です。

   設定レポート(/en-us/citrix-secure-private-access/media/configuration-report-status-cloud.png)

3. レポートをローカルドライブに手動でエクスポートするには、**ダウンロード**をクリックします。

重要:

構成レポートの生成は、次のSecure Private Accessロールを持つ管理者に限定されます。

- フルアクセス管理者
- 読み取り専用管理者
- フルモニター管理者

ヘルプデスク管理者ロールを持つ管理者は、構成レポートを生成できません。

ADFS と Secure Private Access の統合

クレームパイプラインを介したクレームの流れを制御するには、クレームルールが必要です。クレームルールは、クレームルール実行プロセス中にクレームフローをカスタマイズするためにも使用できます。クレームの詳細については、Microsoftドキュメントを参照してください。

Citrix Secure Private Access™からのクレームを受け入れるようにADFSを設定するには、次の手順を実行する必要があります。

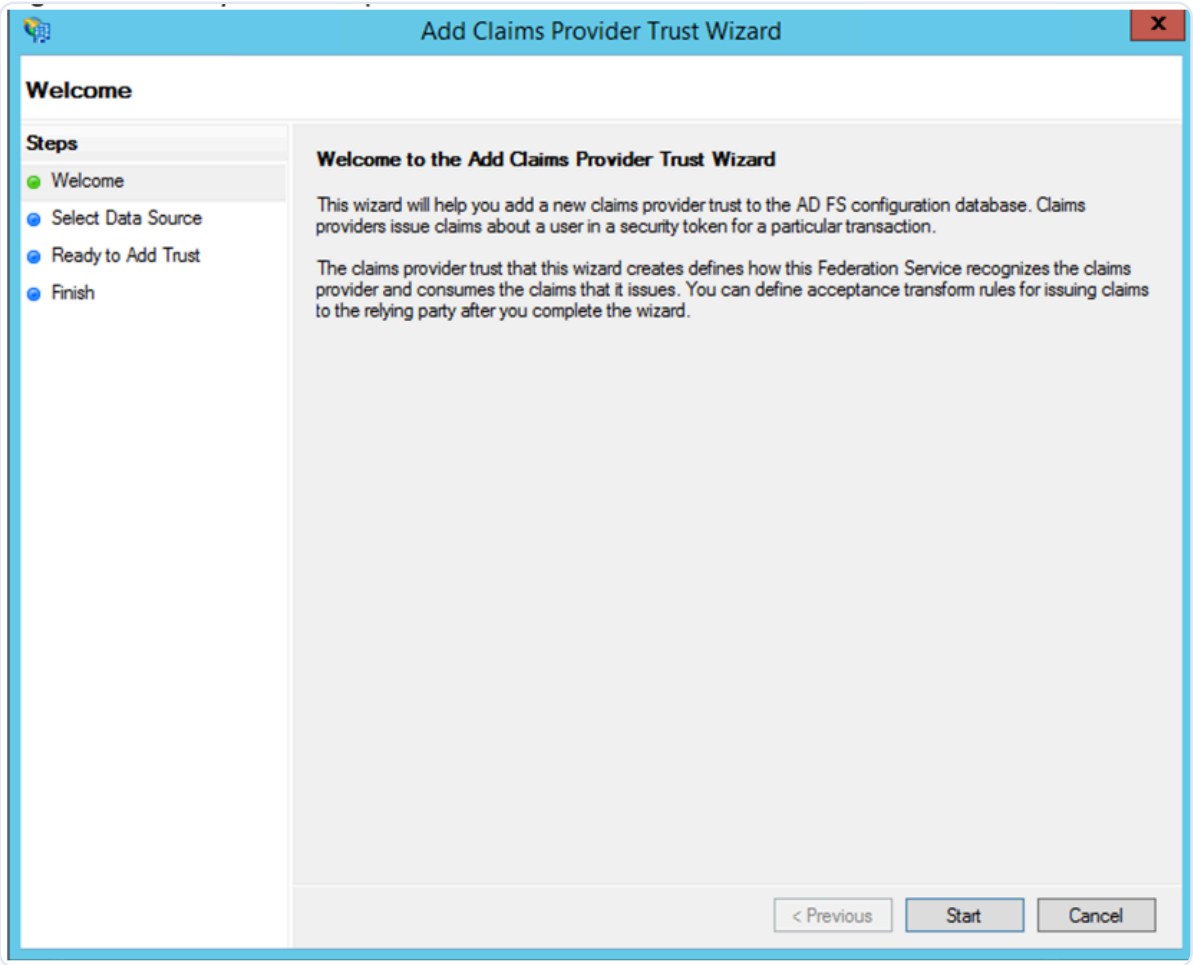
1. ADFSにクレームプロバイダートラストを追加します。
2. Citrix Secure Private Accessでアプリ構成を完了します。

ADFSにクレームプロバイダートラストを追加する

1. ADFS管理コンソールを開きます。**ADFS > 信頼関係 > クレームプロバイダートラスト**に移動します。

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

a. 右クリックして**クレームプロバイダートラストの追加**を選択します。

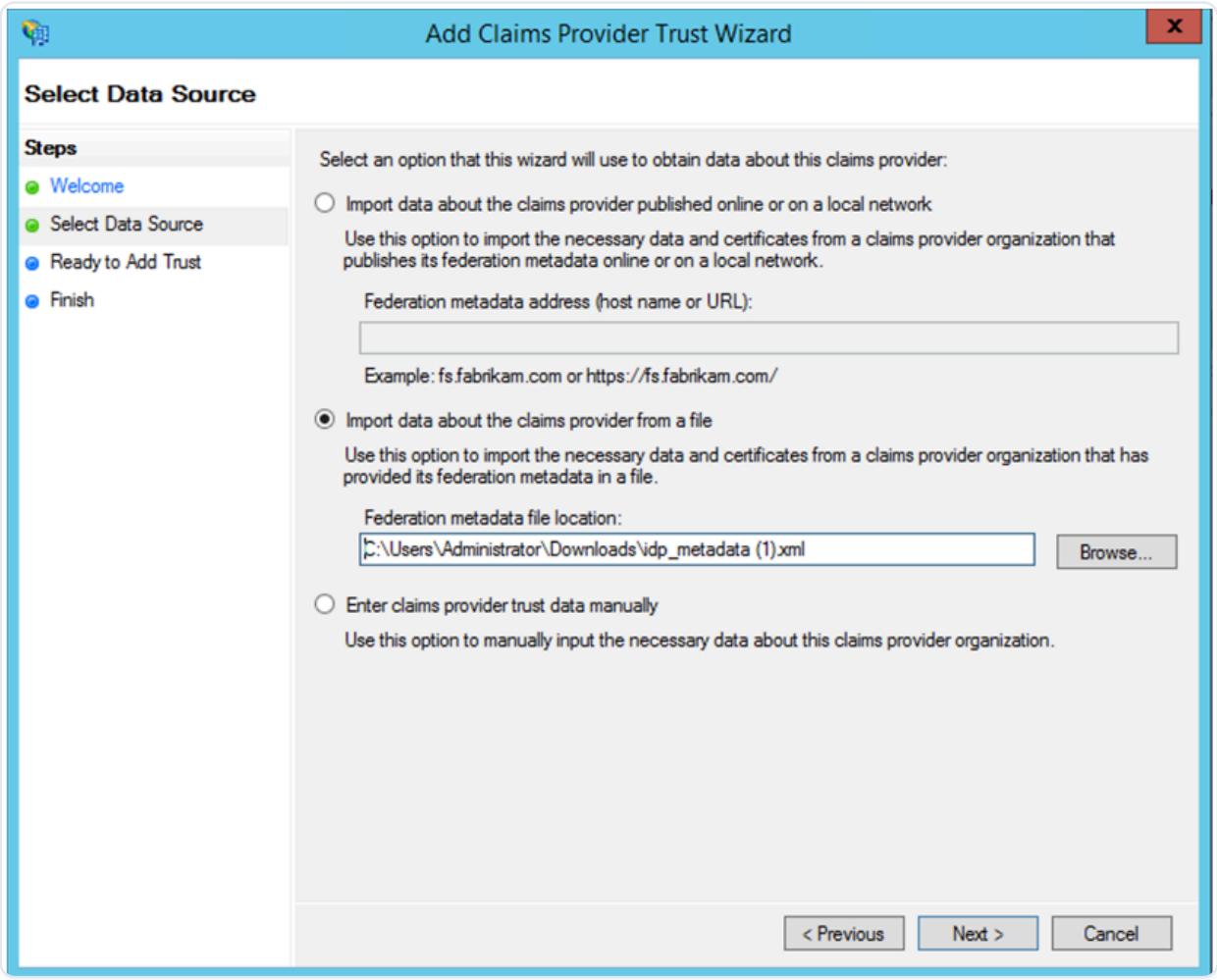


b. ADFSにフェデレーションするために使用されるアプリをSecure Private Accessに追加します。詳細については、Citrix Secure Private Accessでのアプリ構成を参照してください。

注:

まずアプリを追加し、アプリのSSO構成セクションからSAMLメタデータファイルをダウンロードして、そのメタデータファイルをADFSにインポートします。

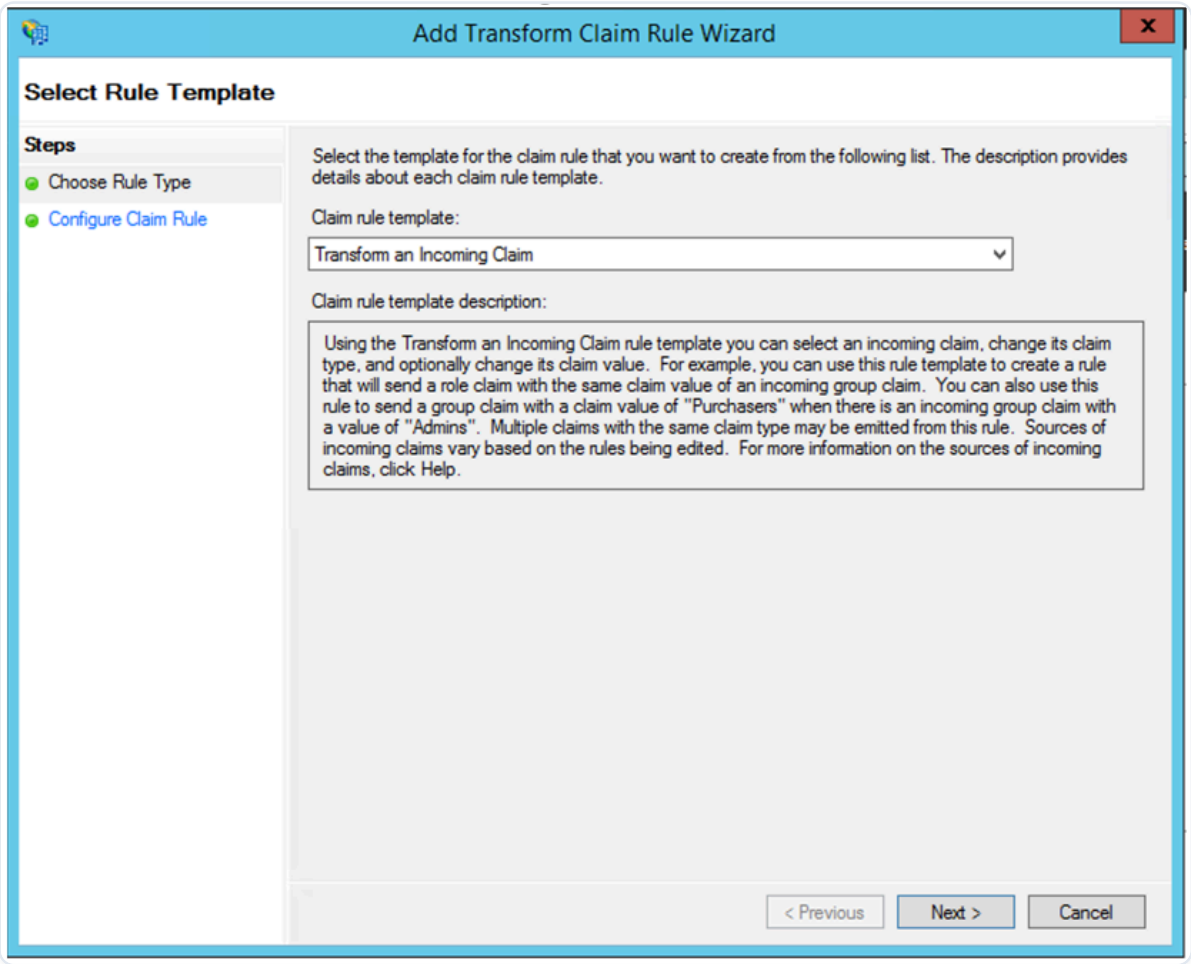
© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. クレームプロバイダートラストの追加を完了するための手順を実行します。クレームプロバイダートラストの追加が完了すると、クレームルールを編集するためのウィンドウが表示されます。

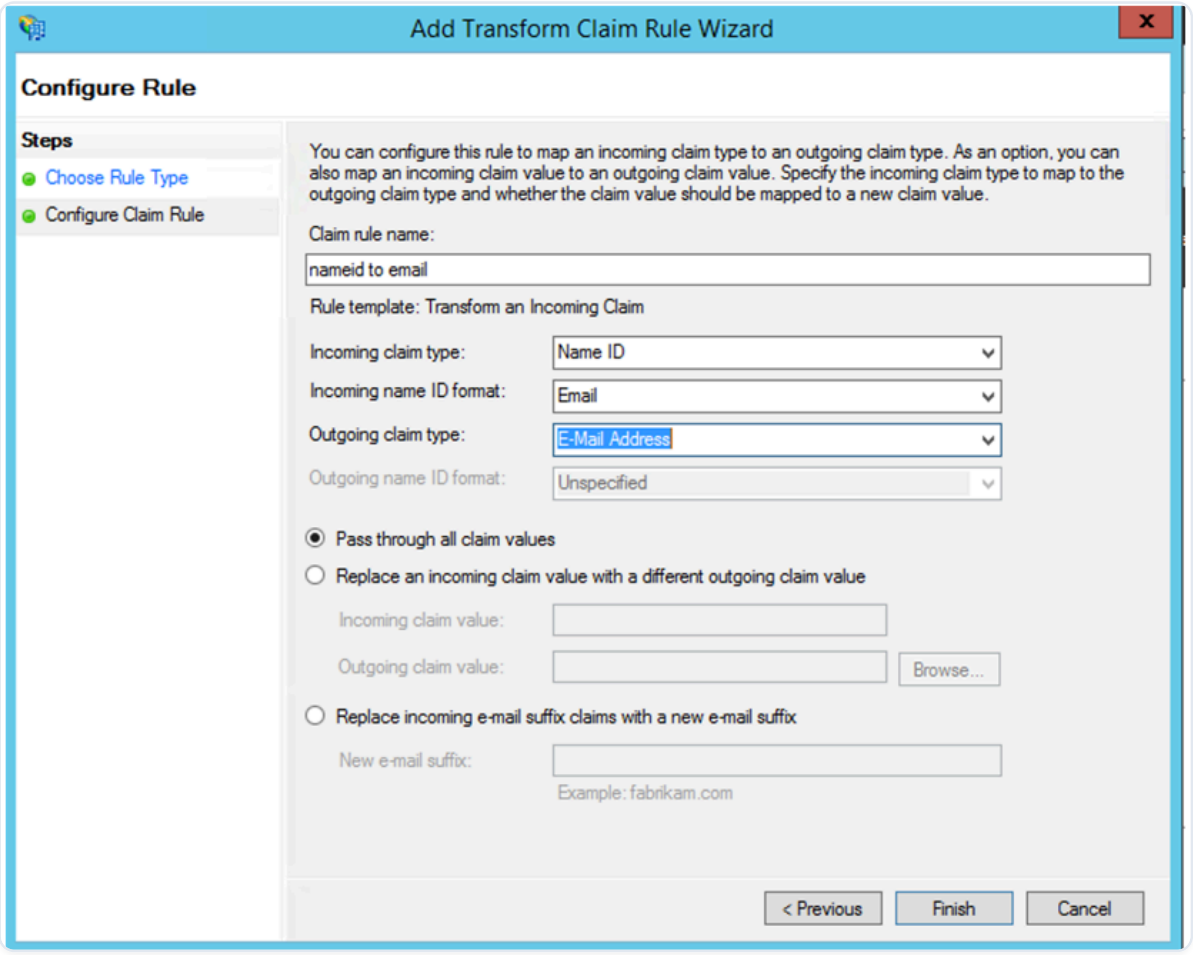
b. **受信クレームの変換**でクレームルールを追加します。

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



c. 次の図に示すように設定を完了します。ADFSが他のクレームを受け入れる場合は、それらのクレームを使用し、Secure Private Accessでもそれに応じてSSOを構成します。

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

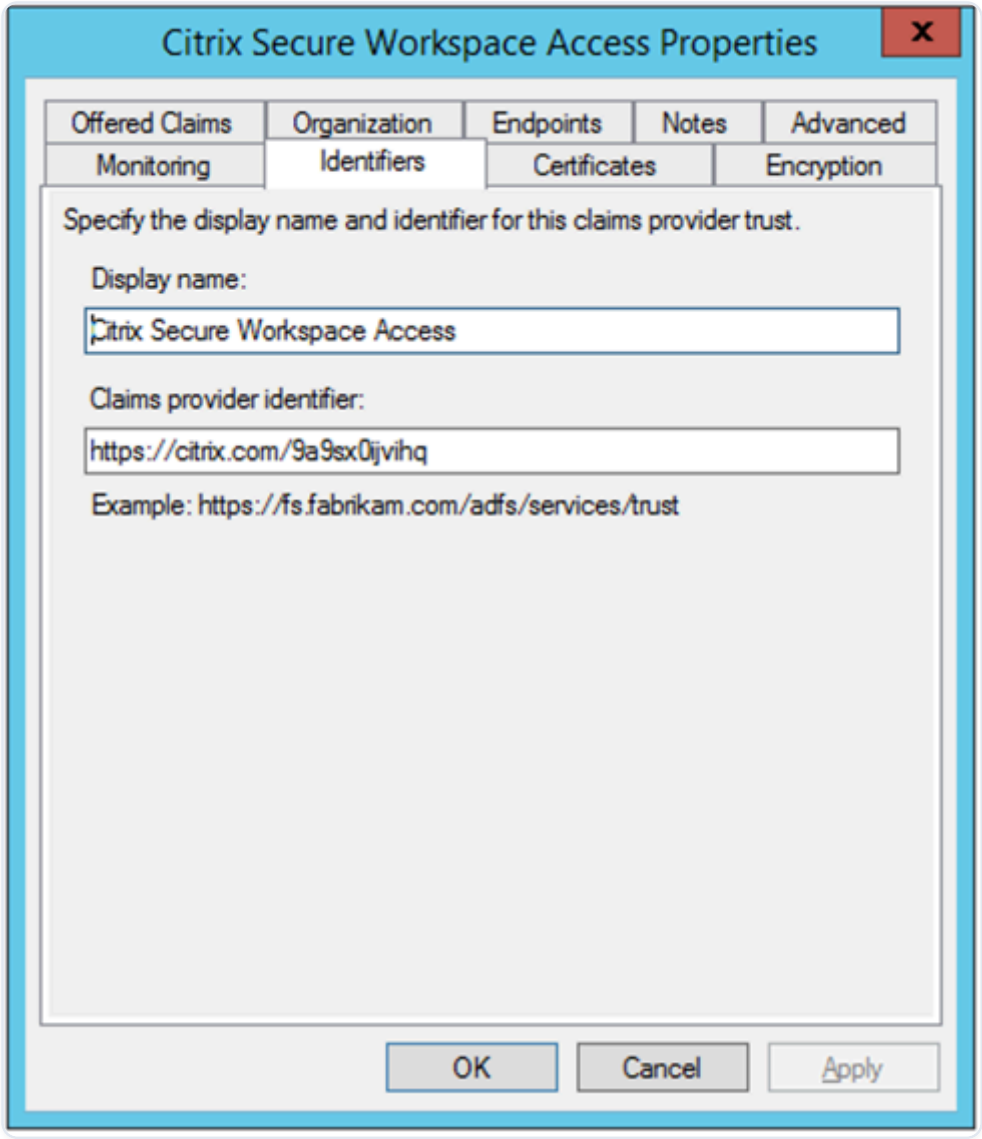


これで、ADFSがSAMLに対してCitrix Secure Private Accessを信頼することを確認するクレームプロバイダートラストが構成されました。

クレームプロバイダー信頼ID

追加したクレームプロバイダー信頼IDをメモしてください。Citrix Secure Private Accessでアプリを設定する際に、このIDが必要です。

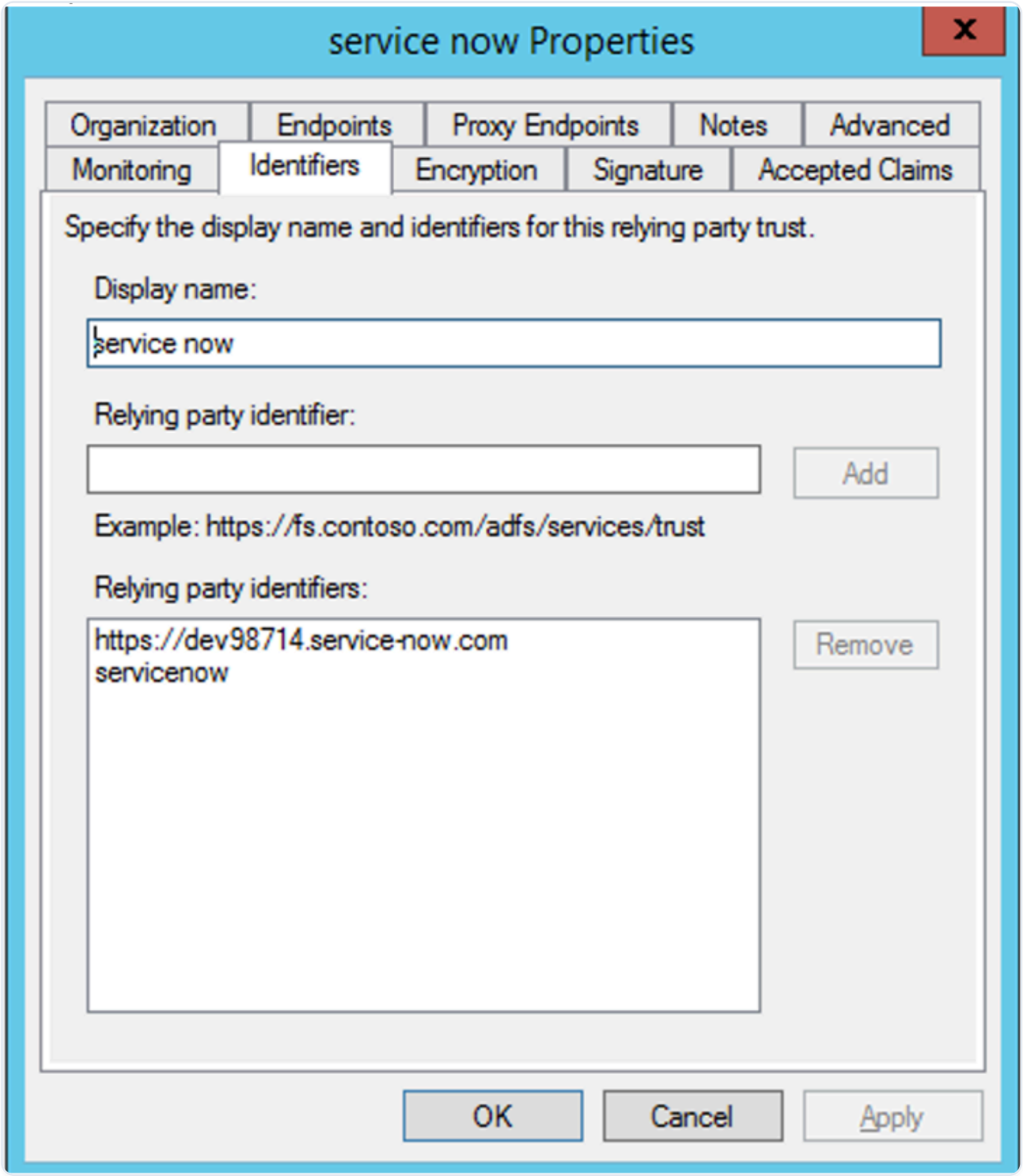
© 1997–2026 Citrix Systems, Inc. All rights reserved.



リライングパーティ識別子

SaaSアプリがADFSを使用してすでに認証されている場合、そのアプリのリライングパーティ信頼がすでに追加されているはずです。Citrix Secure Private Accessでアプリを設定する際に、このIDが必要です。

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



IdP開始フローでリレーステートを有効にする

RelayStateはSAMLプロトコルのパラメーターであり、ユーザーがサインインしてリライングパーティのフェデレーションサーバーに誘導された後、アクセスする特定のリソースを識別するために使用されます。ADFSでRelayStateが有効になっていない場合、それを必要とするリソースプロバイダーに認証した後、ユーザーはエラーを目にします。

ADFS 2.0の場合、RelayStateをサポートするために、更新プログラムKB2681584 (更新プログラムロールアップ2) またはKB2790338 (更新プログラムロールアップ3) をインストールする必要が

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

あります。ADFS 3.0にはRelayStateサポートが組み込まれています。どちらの場合も、RelayStateを有効にする必要があります。

ADFSサーバーでRelayStateパラメーターを有効にするには

1. ファイルを開きます。
   - ADFS 2.0の場合、メモ帳で次のファイルを入力します: %systemroot%\inetpub\adfs\ls\web.config
   - ADFS 3.0の場合、メモ帳で次のファイルを入力します: %systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.config
2. microsoft.identityServer.webセクションで、useRelyStateForIdpInitiatedSignOnの行を次のように追加し、変更を保存します。 `<microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn enabled="true" /> ...</microsoft.identityServer.web>`
   - ADFS 2.0の場合、IISを再起動するには `IISReset` を実行します。
3. 両方のプラットフォームで、Active Directory Federation Services `(adfssrv) service.` を再起動します。 **注:** Windows 2016またはWindows 10を使用している場合は、次のPowerShellコマンドを使用して有効にします。 `Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true`

コマンドへのリンク

Citrix Secure Private Accessでのアプリ構成

IdP開始フローまたはSP開始フローのいずれかを構成できます。Citrix Secure Private AccessでIdPまたはSP開始フローを構成する手順は同じですが、SP開始フローの場合は、UIで**指定されたURLを使用してアプリを起動する（SP開始）**チェックボックスを選択する必要があります。

IdP開始フロー

1. IdP開始フローを設定する際は、以下を構成します。
   - **アプリURL** – アプリURLには次の形式を使用します。 `https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=<rp id>&RedirectToIdentityProvider=<idp id>`
   - **ADFS FQDN** – お使いのADFS設定のFQDN。
   - **RP ID** – RP IDは、証明書利用者信頼から取得できるIDです。これは証明書利用者識別子と同じです。URLの場合、URLエンコードが行われます。

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

- **IDP ID** – IdP IDは、クレームプロバイダー信頼IDと同じです。URLの場合、URLエンコードが行われます。

  例

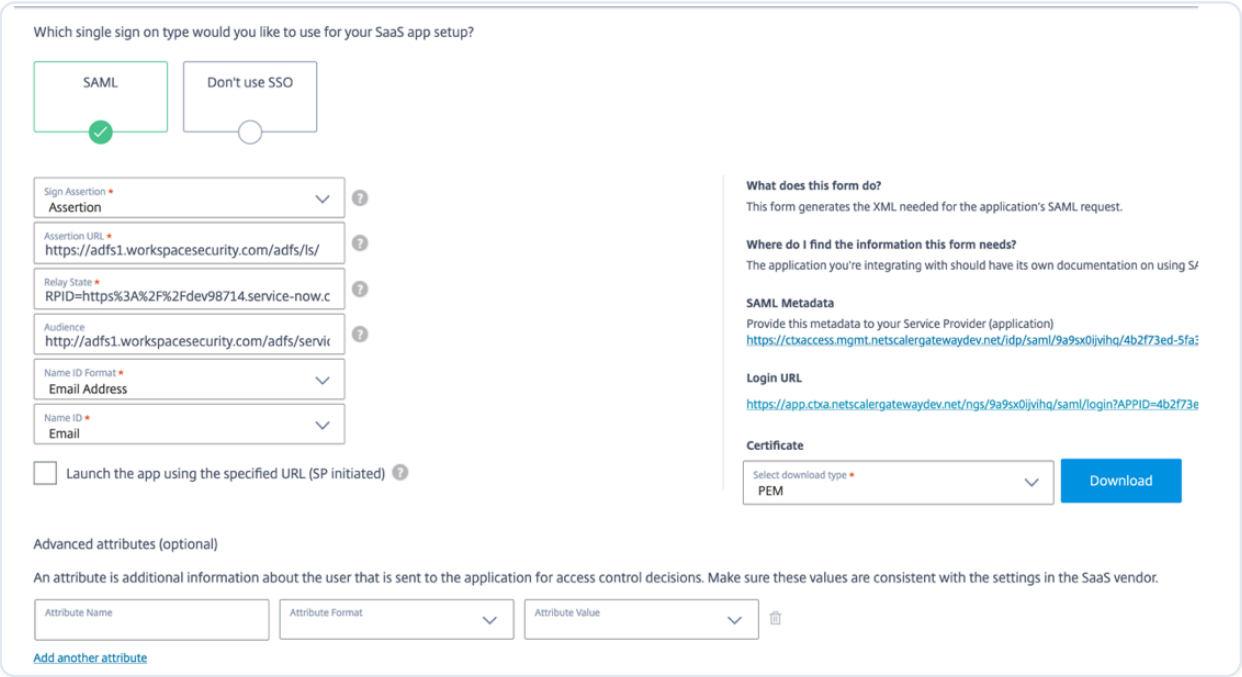
2. SAML SSO構成。

   以下はADFSサーバーのデフォルト値です。いずれかの値が変更された場合は、ADFSサーバーのメタデータから正しい値を取得してください。ADFSサーバーのフェデレーションメタデータは、そのフェデレーションメタデータエンドポイントからダウンロードできます。このエンドポイントは、**ADFS > Service > Endpoints**から確認できます。

   - **アサーションURL** – `https://<adfs fqdn>/adfs/ls/`
   - **リレーステート** – リレーステートはIdP開始フローにとって重要です。正しく構築するには、このリンクに従ってください - リレーステート

     例: RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev98714.service-now.com%2F

   - **対象者** – `http://<adfsfqdn>/adfs/services/trust`
   - その他のSAML SSO構成設定については、以下の画像を参照してください。詳細については、SaaSアプリのサポート。



3. アプリを保存し、ユーザーにサブスクライブします。

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

SP開始フロー

SP開始フローの場合、**IDP開始フロー**セクションに記載されている設定を構成します。さらに、「**指定されたURLを使用してアプリを起動する（SP開始）**」チェックボックスを有効にします。

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

Citrix セキュア プライベート アクセス Terraform プロバイダー

UI を介して Secure Private Access™ の構成を手動で管理することは、時間と手間がかかり、エラーが発生しやすく、環境全体で拡張することが困難です。インフラストラクチャ・アズ・コードのプラクティスを採用しているお客様は、Secure Private Access の構成を自動化し、一貫性を確保し、Secure Private Access の変更を CI/CD パイプラインに統合する方法を必要としています。

Citrix Secure Private Access Terraform プロバイダーを使用すると、お客様は Terraform を使用して Secure Private Access リソースをプログラムでプロビジョニング、構成、管理できます。これにより、Secure Private Access 環境をインフラストラクチャ・アズ・コードのワークフローの一部として、一貫性があり、繰り返し可能で、大規模に管理できるようになります。

Citrix Secure Private Access Terraform プロバイダーは、以下に適用されます。

- Citrix Secure Private Access クラウド展開。
- インフラストラクチャまたは構成管理に Terraform を使用しているお客様。

次の図は、Terraform プロバイダーのアーキテクチャを示しています。

Terraform プロバイダーのアーキテクチャを示す図(/en-us/citrix-secure-private-access/media/spa-terraform-provider.png)

主な利点

Citrix Secure Private Access Terraform プロバイダーは、Secure Private Access リソースを Terraform 管理オブジェクトとして公開します。お客様は、Secure Private Access の構成を宣言的に定義し、アプリケーションインフラストラクチャと並行してバージョン管理し、予測可能な方法で変更を適用できます。

このソリューションを使用する主な利点は次のとおりです。

- Secure Private Access のインフラストラクチャ・アズ・コード管理。
- 環境間（開発、テスト、本番）での一貫した構成。
- 手作業の削減と構成ドリフトの低減。

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

- CI/CD パイプラインおよび GitOps ワークフローとの容易な統合。
- より迅速なオンボーディングと繰り返し可能な展開。

ユースケース

Citrix Secure Private Access Terraformプロバイダーは、次のユースケースで使用できます。

- 新しいアプリケーション/ポリシーのSecure Private Accessへのオンボーディングを自動化します。
- 複数の環境でSecure Private Accessの構成を標準化します。
- バージョン管理されたTerraformステートを使用して、Secure Private Access環境を再作成または復元します。
- Secure Private Accessの構成変更を既存のTerraformワークフローに統合します。
- DevOpsチームがインフラストラクチャと並行してアクセスポリシーを管理できるようにします。
- Secure Private Accessの構成を試用テナントから本番テナントに移行します。
- 買収シナリオのために、2つの顧客のSecure Private Access構成をマージします。

システム要件

次のシステム要件が満たされていることを確認してください。

- Terraform v1.3以降。
- Citrix Secure Private Accessテナントへのアクセス。
- Citrix Cloud™ APIへのネットワーク接続。

前提条件

Citrix Secure Private Access Terraformプロバイダーを使用する前に、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。

- アクティブなCitrix Secure Private Accessサブスクリプションをお持ちであること。
- CitrixテナントでSecure Private Accessリソースを管理する権限があること。
- Terraformが環境にインストールされ、利用可能であること。
- Citrix CloudのAPI資格情報または認証方法が構成されていること。

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

権限

Terraformが使用するサービスプリンシパル認証アカウントには、以下の権限が必要です。

- Secure Private Accessリソースを作成、更新、および削除する。
- 状態の調整のために、既存のSecure Private Access構成を読み取る。

インストール

「TerraformのインストールとCitrix Terraformプロバイダーの構成」を参照してください。

Terraformの構成

Terraformプロバイダーを使用すると、Secure Private Accessの構成をCitrix UIの外部で管理できます。必要に応じてUIを引き続き使用できますが、Terraformは自動化された大規模な展開に推奨されるアプローチです。

Secure Private Access用のTerraformプロバイダーを使用するには、Terraform構成でプロバイダーを次のように定義する必要があります。

```
terraform {

  required_providers {

    citrixspa = {

      source = "citrix/citrixspa"

      version = `<version>`

    }

  }

}



provider "citrixspa" {

  base_url      = "<https://api.cloud.com/accessSecurity>"  # for
commercial deployment
```

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

```
  customer_id   = "xxxxxxxxxxxxx" # the CC customer id

  client_id     = "xxxxxxxxxxxxx" # client id of service principal

  client_secret = "xxxxxxxxxxxxx" # client secret of service principal

}
```

プロバイダーが構成されると、Terraformリソースブロックを使用してSecure Private Accessリソースを定義し、標準のTerraformコマンド（例：）を使用して適用できます。

- `terraform plan`
- `terraform apply`

注:

Terraformプロバイダーは、Terraform構成で宣言され、初期化されると、デフォルトで有効になります。

問題のトラブルシューティング

- **`terraform apply` 操作が認証エラーで失敗します。**

  原因: 無効な、または不足しているCitrix Cloud資格情報。

  解決策: プロバイダーの認証構成と権限を確認してください。

- **`terraform plan` で予期しない変更が検出されました。**

  原因: 手動によるUI変更による構成のずれ。

  解決策: Terraformを介して変更を調整し、必要に応じて状態を更新します。

制限事項

- 最初のプロバイダーリリースでは、すべてのSecure Private Access機能が利用できない場合があります。
- UIで直接行われた変更は、Terraformの状態のずれを引き起こす可能性があります。
- `terraform destroy` 操作では、すべての依存リソースが自動的に削除されない場合があります。

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

重要な考慮事項

- Terraformの状態ファイルには機密性の高い構成データが含まれている可能性があるため、安全に保存する必要があります（例：リモートバックエンド）。
- 導入後は、Secure Private AccessリソースをTerraformのみを使用して管理することをお勧めします。
- 予期せぬ変更を避けるため、プロバイダーのバージョンを固定することを強くお勧めします。
- 変更を適用する前に、必ず `terraform plan` 出力を確認してください。

参照

- Terraform Registry ドキュメント
- Terraform ドキュメント

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

可視性と監視

管理者は、Secure Private Access の可視性と監視のために、以下の機能/リソースを使用できます。

監視

Secure Private Access は、Citrix DaaS の監視およびトラブルシューティングコンソールである Monitor と統合されています。管理者およびヘルプデスク担当者は、Secure Private Access ダッシュボードに加えて、DaaS Monitor から Web/SaaS および TCP/UDP アプリセッションとイベントを監視およびトラブルシューティングできます。詳細については、「DaaS Monitor との統合」を参照してください。

Secure Private Access 使用状況ダッシュボード

Secure Private Access のユーザー、アプリケーション、ポリシー、コネクタのステータスに関する可視性は、Secure Private Access ダッシュボードで確認できます。管理者はダッシュボードを使用してこれらのイベントを監視できます。詳細については、「ダッシュボード」を参照してください。

Secure Private Access アプリケーションおよびセッションの監視

Citrix Monitor を使用して、組織全体の Secure Private Access セッションとアプリケーションの傾向を監視します。詳細については、次のトピックを参照してください。

- Monitor はセッションとアプリケーションのフィルタリング機能を提供し、ユーザーアクティビティの分析とアプリケーションパフォーマンスの問題への対処を容易にします。詳細については、「セッションとアプリケーションの監視」を参照してください。
- 管理者は、Monitor でセッションとエラーの傾向を表示して、パターンを特定し、問題をトラブルシューティングできます。詳細については、「エラーとセッションの傾向」を参照してください。

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

Connector Appliance のヘルス監視

Secure Private Access を展開すると、Connector Appliance コンポーネントがインフラストラクチャ監視の一部として自動的に追加されます。Citrix DaaS サイトに接続されているすべての Connector Appliance は、包括的な監視のために自動的にオンボーディングされ、管理者にこれらの重要なインフラストラクチャコンポーネントの健全性とパフォーマンスに関するリアルタイムの可視性を提供します。

Connector Appliance のヘルス監視の詳細については、「Connector Appliance のヘルス指標」を参照してください。

Secure Private Access 使用状況ダッシュボード

Secure Private Access サービスダッシュボードには、SaaS、Web、TCP、および UDP アプリの診断データと使用状況データが表示されます。このダッシュボードは、管理者に対し、アプリ、ユーザー、コネクタの健全性ステータス、および帯域幅の使用状況を単一の場所で確認できる完全な可視性を提供します。このデータは Citrix Analytics から取得されます。さまざまなエンティティのデータは、プリセットされた時間またはカスタムタイムラインで表示できます。一部のエンティティについては、ドリルダウンして詳細を表示できます。

メトリックは、以下のカテゴリに大別されます。

- **ログとトラブルシューティング**
  - 診断ログ: 認証、アプリケーション起動、アプリ列挙、およびデバイスポスチャチェックに関連するログ。
- **ユーザー**
  - アクティブユーザー: 選択した時間間隔でアプリケーション（SaaS、Web、TCP）にアクセスしている一意のユーザーの総数。
  - アップロード: 選択した時間間隔で Secure Private Access サービスを介してアップロードされたデータ総量。
  - ダウンロード: 選択した時間間隔で Secure Private Access サービスを介してダウンロードされたデータ総量。
- **アプリケーション:**
  - アプリケーション: 現在構成されているアプリケーションの総数（時間間隔に依存しない）。

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

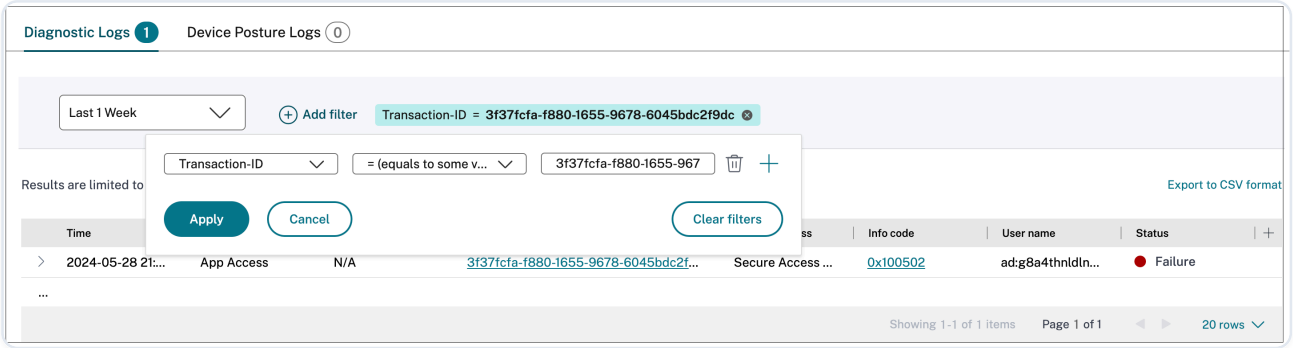
  - アプリケーション起動数: 選択した時間間隔で各ユーザーによって起動されたアプリケーション（アプリセッション）の総数。
  - 構成済みドメイン: 選択した時間間隔で構成されたドメインの総数。
  - 検出されたアプリケーション: アクセスされたものの、どのアプリにも関連付けられていない一意の個別ドメインの総数。

- **アクセスポリシー**
  - アクセス ポリシー: 現在構成されているアクセス ポリシーの総数 (時間間隔とは無関係)。

診断ログ

診断ログチャートを使用して、認証、アプリケーション起動、アプリ列挙、およびデバイスポスチャに関連するログを表示できます。**詳細を表示**リンクをクリックすると、ログの詳細が表示されます。詳細は表形式で表示されます。ログは、事前設定された時間またはカスタムタイムラインで表示できます。ダッシュボードに表示したい情報に応じて、+記号をクリックしてチャートに列を追加できます。ユーザーログをCSV形式でエクスポートできます。

- **フィルターの追加**オプションを使用して、アプリの種類、カテゴリ、説明などのさまざまな条件に基づいて検索を絞り込むことができます。たとえば、検索フィールドで `Transaction ID`、`= (equals to some value)` を選択し、この順序で `7456c0fb-a60d-4bb9-a2a2-edab8340bb15` を入力すると、このトランザクションIDに関連するすべてのログを検索できます。フィルターオプションで使用できる検索演算子の詳細については、検索演算子を参照してください。

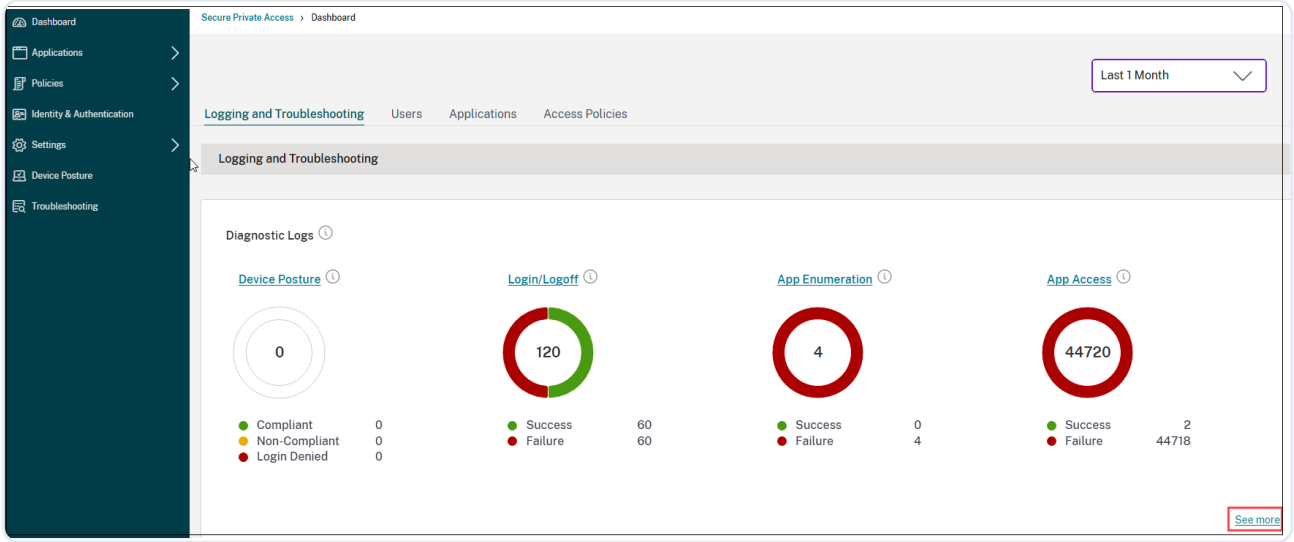


- **デバイスポスチャログ:** ポリシーの結果（**準拠、非準拠、ログイン拒否**）に基づいて検索を絞り込むことができます。デバイスポスチャの詳細については、デバイスポスチャを参照してください。

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

注:

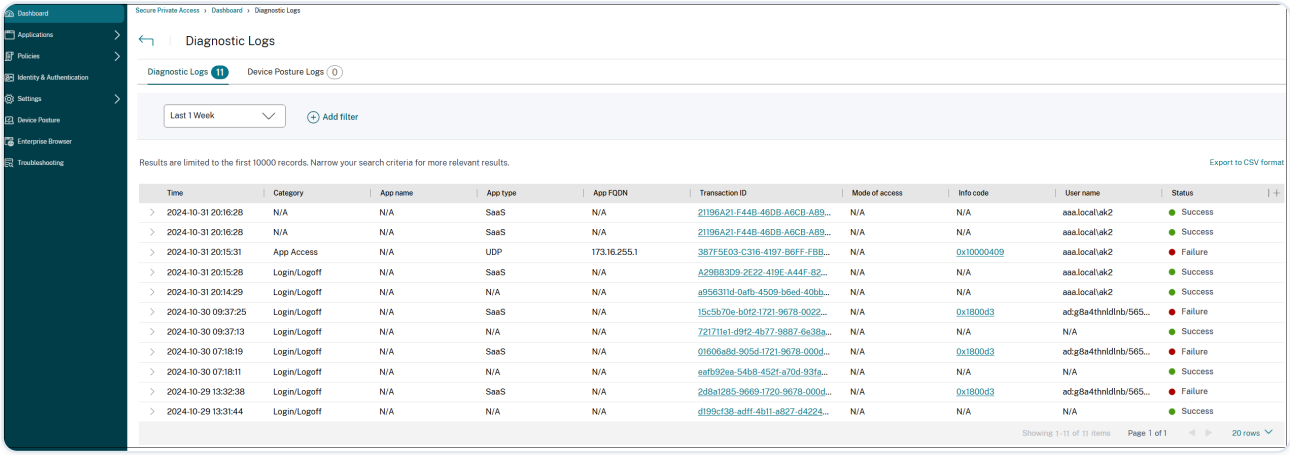
- Secure Private Access診断ログダッシュボード内のすべての失敗イベントには、関連する情報コードがあります。詳細については、情報コードを参照してください。
- トランザクションIDは、アクセス要求のすべてのSecure Private Accessログを関連付けます。詳細については、トランザクションIDを参照してください。



- 展開アイコン (>) をクリックすると、ログの完全な詳細を表示できます。
- **診断ログ**ページには、アクセスされた各メインURLの埋め込みドメインが表示されます。管理者は、メインURLから展開アイコン (>) をクリックして埋め込みドメインを表示できます。管理者は、埋め込みドメインリストを使用して、アプリへのアクセスまたはアプリのレンダリングに関連する問題に対処できます。たとえば、アプリケーション構成でドメインが欠落していた場合、特定のアプリはエンドユーザーによってアクセスできません。この場合、管理者は埋め込みドメインのリストを表示し、欠落しているドメインを特定して、欠落しているドメインでアプリ構成を更新できます。

デフォルトでは、**診断ログ**ページには今週のデータと最新の10000件のレコードのみが表示されます。カスタム日付検索とフィルターを使用して、検索結果をさらに絞り込むことができます。

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

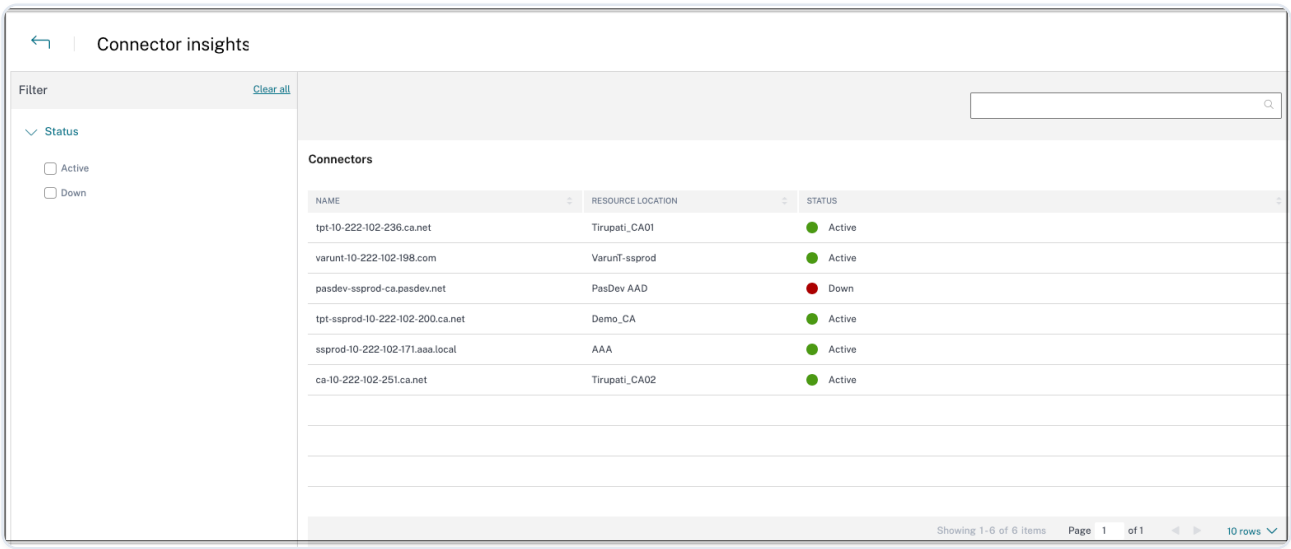


重要:

Secure Private Access サービスの使用中にユーザーが遭遇する可能性のあるエラーの包括的なリストについては、情報コードルックアップテーブルを参照してください。

コネクターステータス

コネクターステータスチャートを使用して、コネクターのステータスとコネクターが展開されているリソースの場所を表示します。詳細を表示するには、**詳細を見る**リンクをクリックします。**コネクターインサイト**ページでは、**アクティブ**または**非アクティブ**フィルターを使用して、ステータスに基づいてコネクターをフィルターできます。

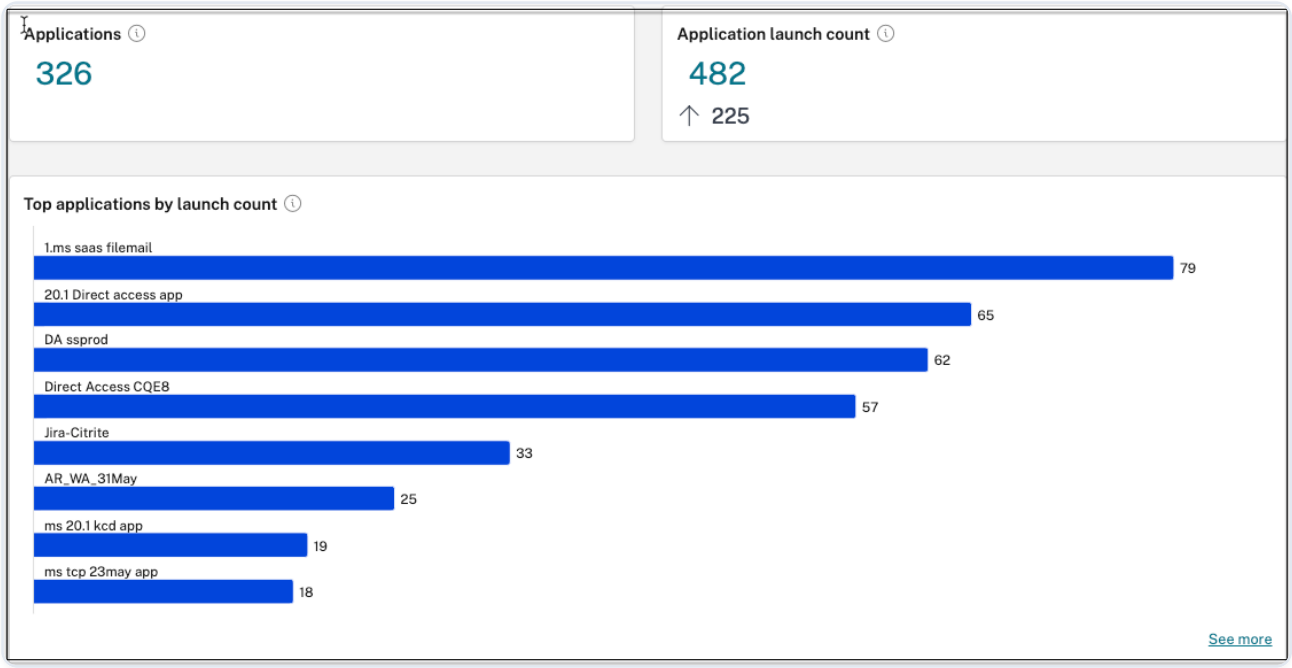


起動回数別上位アプリケーション

起動回数別上位アプリケーションチャートを使用して、アプリの起動回数、アプリサーバーにアップロードされたデータの総量、およびアプリサーバーからダウンロードされたデータの総量に基づいて、上位アプリケーションのリストを表示します。**SaaSアプリ**、**Webアプリ**、または

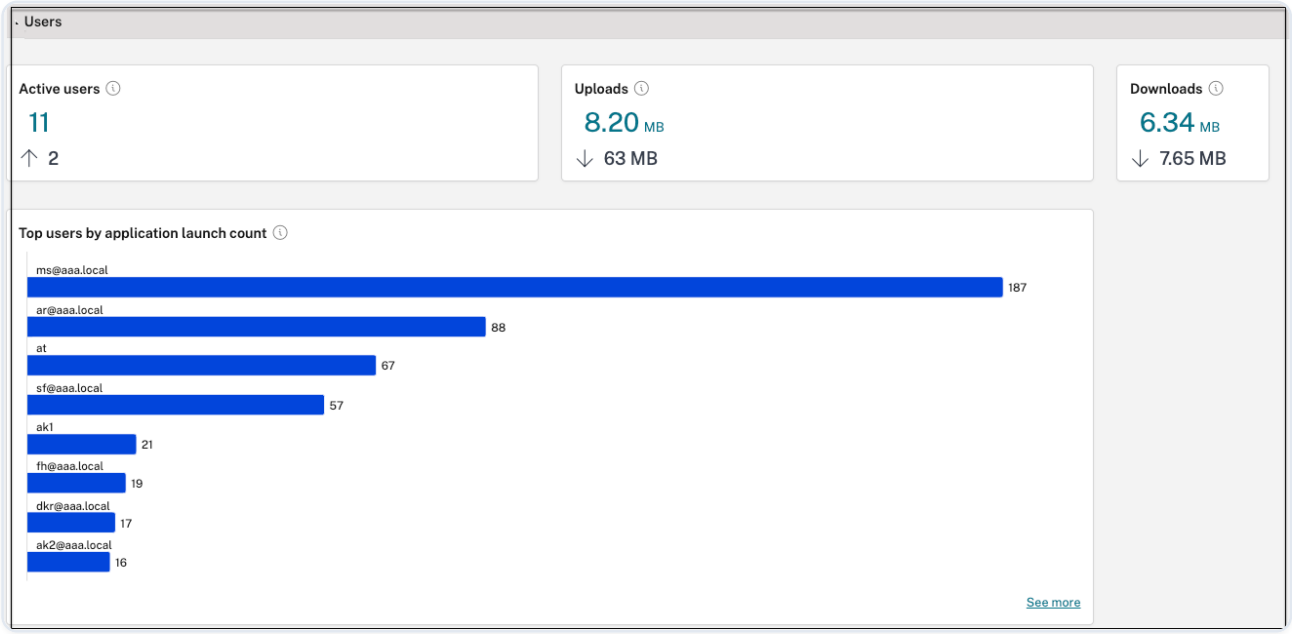
© 1997–2026 Citrix Systems, Inc. All rights reserved.

TCP/UDPアプリのフィルターを適用して、特定のアプリに検索を絞り込むことができます。事前設定されたタイムラインまたはカスタムタイムラインでデータをフィルターできます。



アプリケーション起動回数別上位ユーザー

アプリケーション起動回数別上位ユーザーチャートを使用して、ユーザーごとのデータを表示します。たとえば、ユーザーがTCPアプリを起動した回数、アプリサーバーにアップロードされたデータの総量、およびアプリサーバーからダウンロードされたデータの総量などです。事前設定されたタイムラインまたはカスタムタイムラインでデータをフィルターできます。



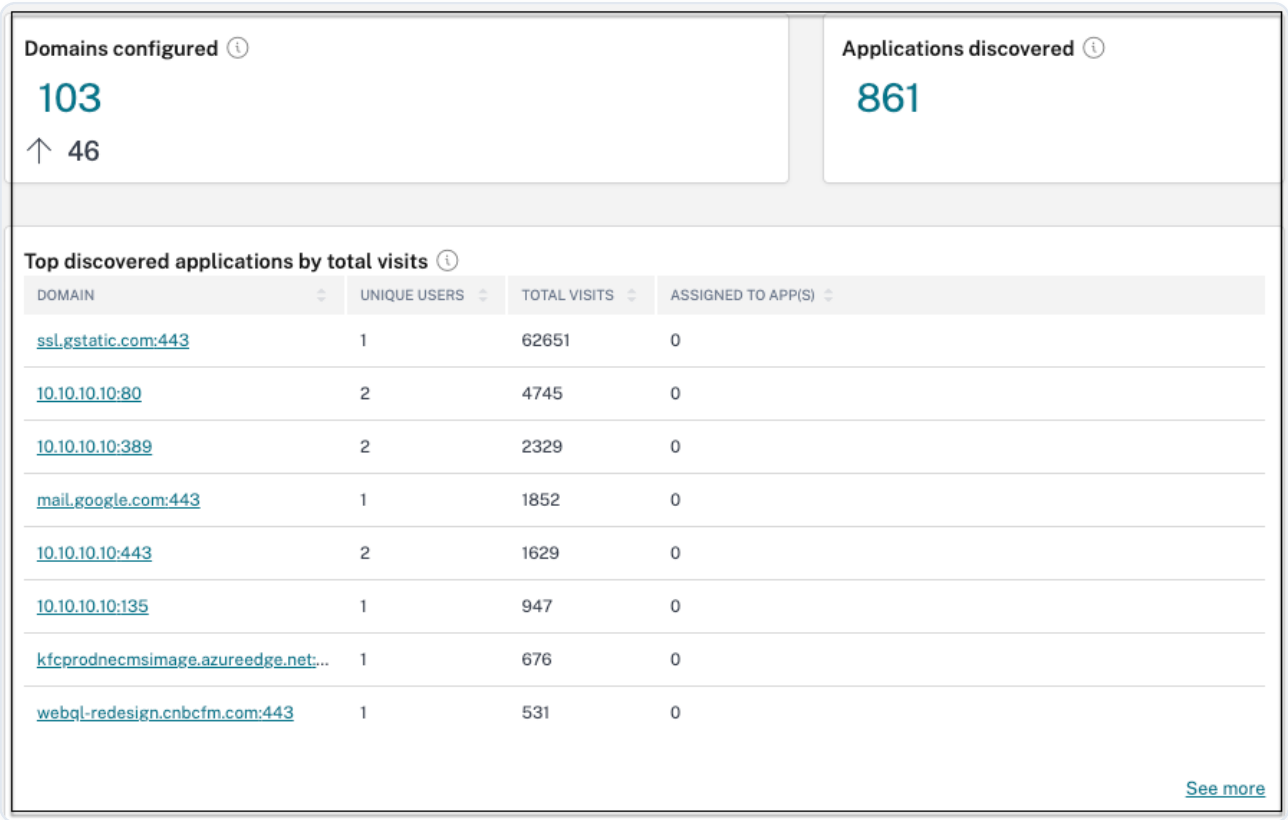
© 1997–2026 Citrix Systems, Inc. All rights reserved.

適用別上位アクセスポリシー

適用別上位アクセスポリシーチャートを使用して、アプリに適用されているアクセスポリシーのリストを表示します。**詳細を見る**リンクをクリックして、アプリに関連付けられているポリシーのリストと、ポリシーが適用された回数を表示します。アクセスポリシーページで**検索**オプションを使用して、ポリシー名に基づいてポリシーをフィルターすることもできます。検索演算子を使用して特定のポリシーを検索し、検索をさらに絞り込むこともできます。詳細については、検索演算子を参照してください。

上位検出アプリケーション

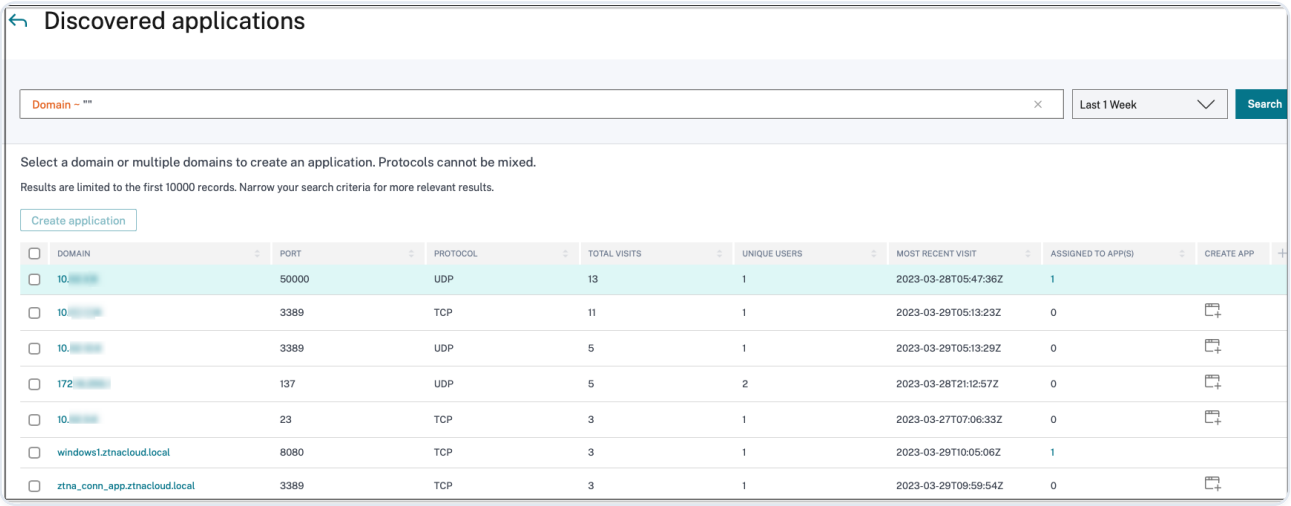
総訪問数別上位検出アプリケーションを使用して、ある時点でアクセスされたがどのアプリにも関連付けられていない、一意の個別のドメインのリストを表示します。これらのドメインは、それらのドメインへの総訪問数に基づいてリストされます。管理者はこのチャートを使用して、特定の関心のあるドメインが多くのユーザーによってアクセスされているかどうかを確認できます。そのような場合、管理者はそのドメインでアプリを作成して、簡単にアクセスできるようにすることができます。



チャートでは、**ASSIGNED TO APPs** 列に、関連URLまたは宛先URLの値の一部としてこのドメインが構成されているアプリケーションの総数が表示されます。この数字をクリックすると、このドメインに割り当てられているアプリが表示されます。

「**See more**」リンクをクリックすると、すべてのドメインに関する詳細を表示できます。

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



「**検出されたアプリケーション**」ページには、ドメイン名、ポート、プロトコル、総訪問数、ユニークユーザー数、最新の訪問日など、ドメインの詳細が表示されます。チャート内のすべての列はソート可能です。検索バーを使用してドメインに基づいて検索できます。

注:

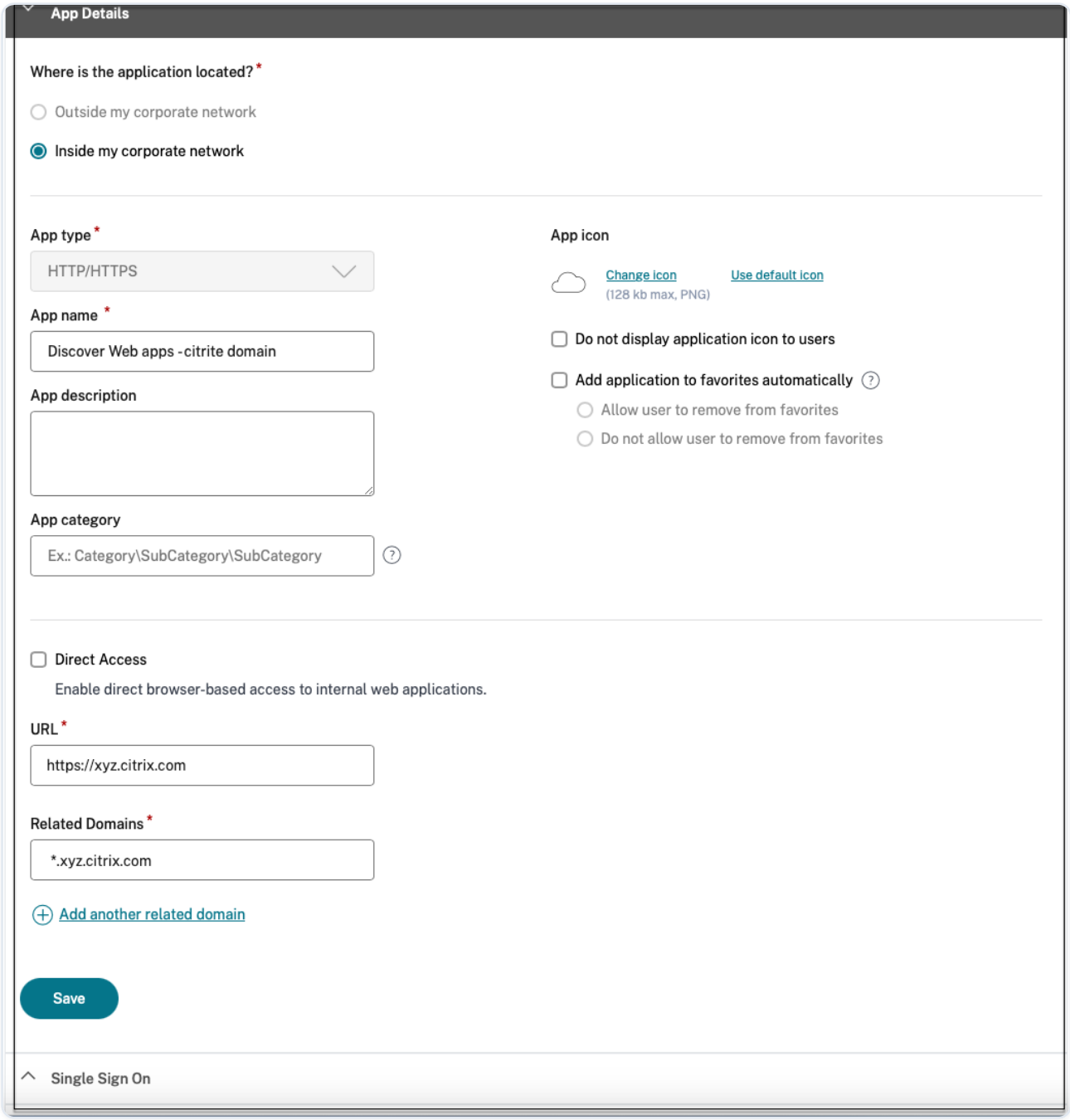
- プロトコルは、お客様が使用する標準ポートに基づいて導出されます。
- 検出されたドメインのリストは10000レコードに制限されています。

チャートからアプリを作成する

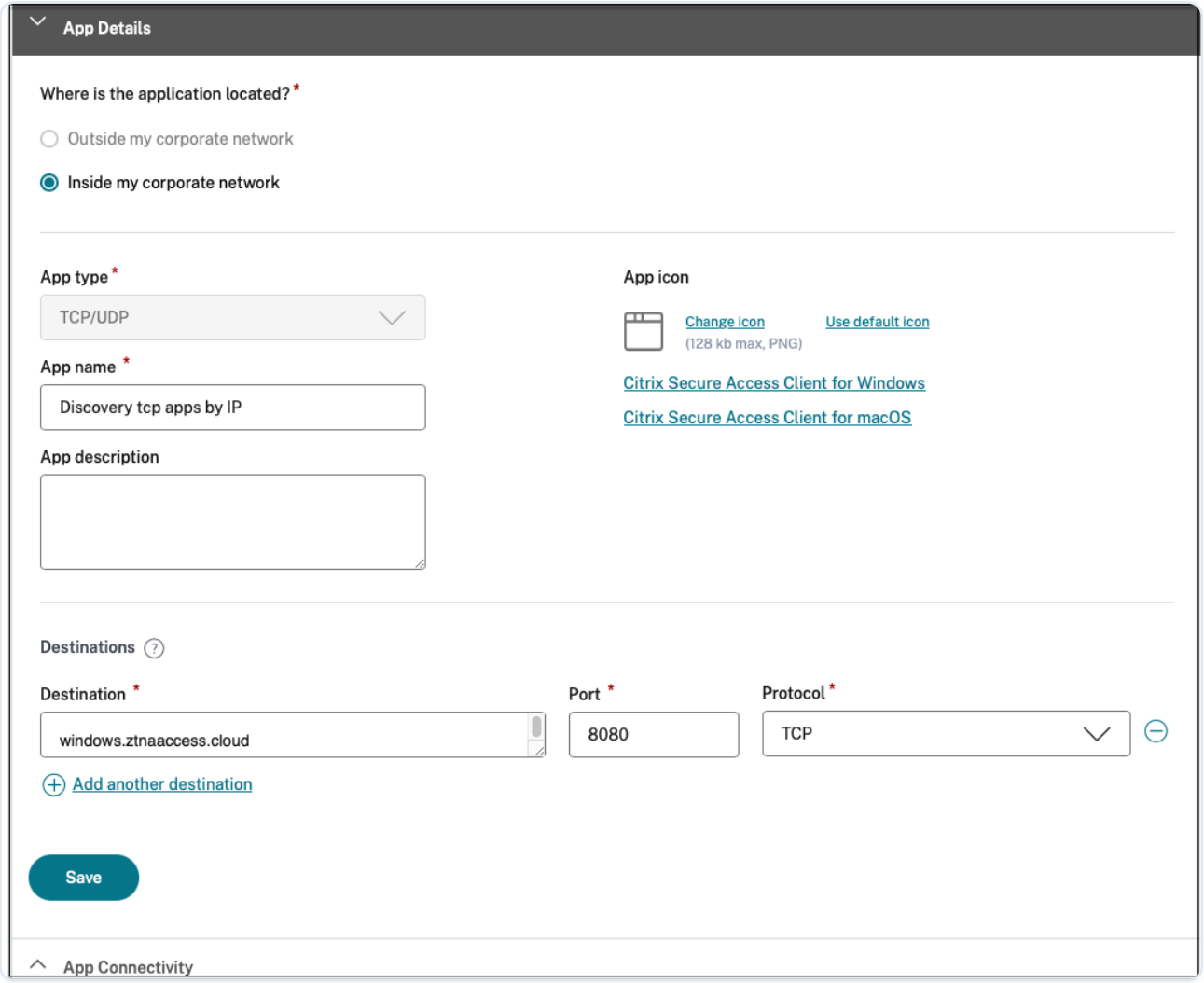
該当するドメインと同じ行にある「**+**」アイコンをクリックしてアプリを作成します。アプリ構成ウィザードがポップアップ表示されます。同じドメイン、ポート、プロトコルの組み合わせでアプリが既に作成されており、完了状態にある行には、アプリ作成アイコンは表示されません。

- アプリの種類は、選択したアプリのプロトコルに基づいて自動入力されます。ただし、必要に応じて種類を変更できます。
- 「**URL、関連ドメイン、宛先、ポート、プロトコル**」フィールドの値はすべて自動入力されます。アプリを追加する手順を完了します。詳細については、簡単なオンボーディングとセットアップのための管理者ガイド付きワークフローを参照してください。

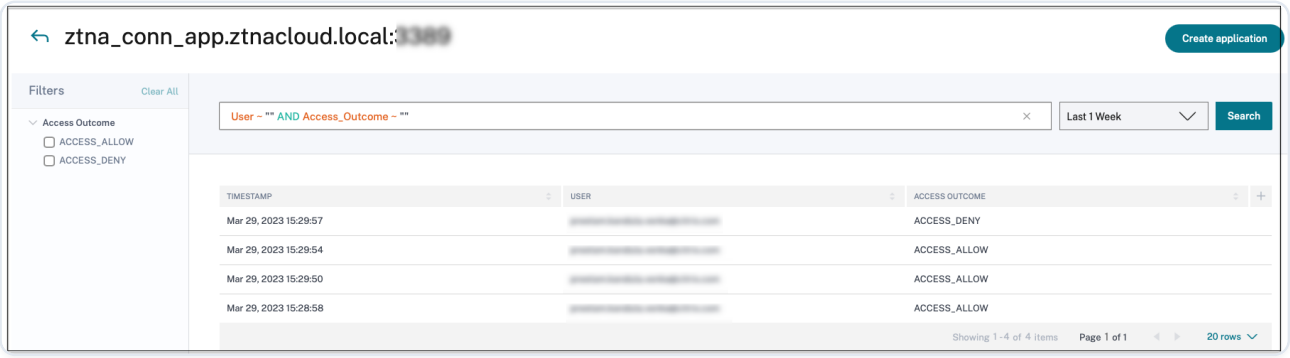
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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



ユニークなドメインリンクをクリックして、詳細を表示し、そのドメインのアプリケーションを作成することもできます。ドメインリンクをクリックすると、そのドメインのユーザー認証ログが表示されます。「**アプリケーションの作成**」ボタンをクリックします。アプリを追加する手順を完了します。



検索演算子

検索を絞り込むために使用できる検索演算子は次のとおりです。

- **= (ある値と等しい)**: 検索条件に完全に一致するログ/ポリシーを検索する場合。

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

- **!= (ある値と等しくない)**: 指定された条件を含まないログ/ポリシーを検索する場合。
- **~ (ある値を含む)**: 検索条件に部分的に一致するログ/ポリシーを検索する場合。
- **!~ (ある値を含まない)**: 指定された条件の一部を含まないログ/ポリシーを検索する場合。

セキュアプライベートアクセス アプリケーション、セッション、およびトレンド

セキュアプライベートアクセスは、Citrix DaaSの監視およびトラブルシューティングコンソールであるMonitorと統合されています。管理者とヘルプデスク担当者は、この統合を使用して、DaaS MonitorコンソールからWeb/SaaSおよびTCP/UDPアプリケーションのセッションとイベントを監視およびトラブルシューティングできます。これにより、セキュアプライベートアクセスダッシュボードを補完する追加の監視機能が提供されます。

セキュアプライベートアクセスでDaaS Monitor機能を使用するには、セキュアプライベートアクセスとDaaSの両方のエンタイトルメントが必要です。

Monitorには、セキュアプライベートアクセスダッシュボード（**Monitorに移動**）またはCitrix DaaSサービスタイルからアクセスできます。

Monitorとの統合の詳細については、セキュアプライベートアクセスを参照してください。

アプリケーション、セッション、およびトレンド

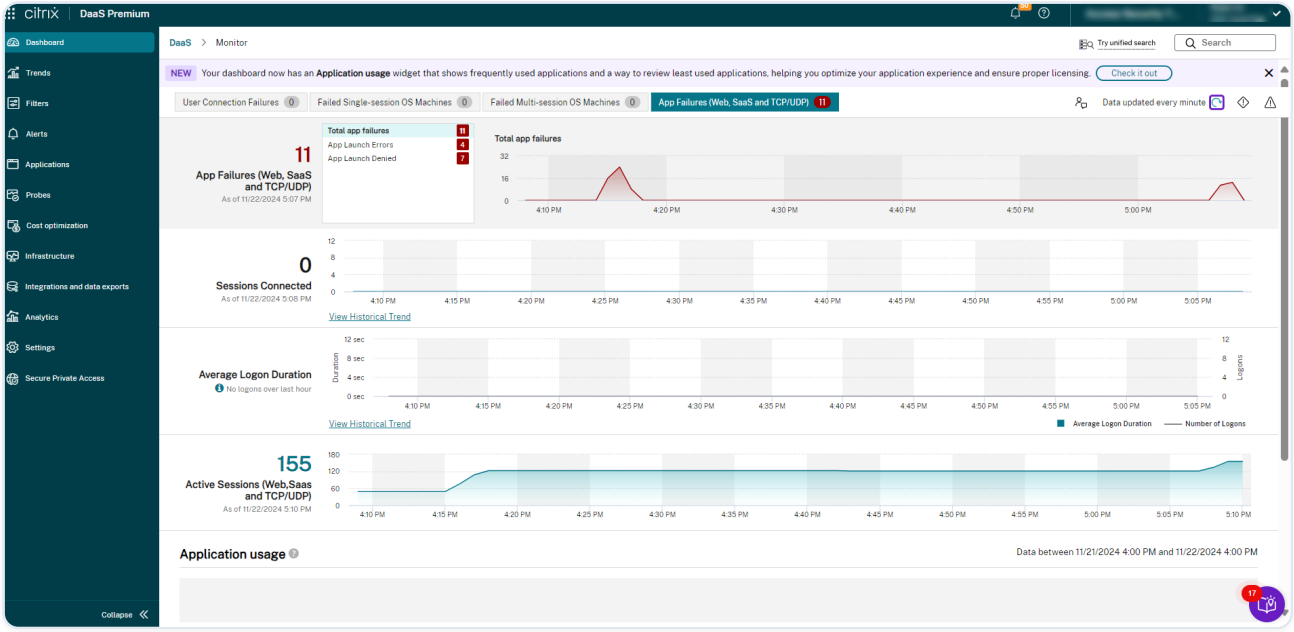
Monitorは、セキュアプライベートアクセスセッションとその関連トレンドに対する可視性を強化します。この包括的な監視機能は、アプリケーションがどのようにアクセスされ使用されているかについて詳細なインサイトを提供し、これらのセッション内での個々のユーザーアクティビティに関する詳細情報も提供します。これにより、管理者はユーザーの行動、アプリケーションのパフォーマンスをより深く理解し、セキュアプライベートアクセス環境のプロアクティブな管理と最適化を可能にします。

セキュアプライベートアクセスのコンテキストにおけるセッション定義を理解するには、セッション定義を参照してください。

ユーザーごとのセキュアプライベートアクセスセッションを表示するには、ユーザーセッションの表示を参照してください。

セッションの詳細を表示するには、セキュアプライベートアクセスサービスの可視性を参照してください。

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



健全性監視

以下のセクションでは、健全性監視に関する詳細情報を提供します。

コネクタアプライアンス

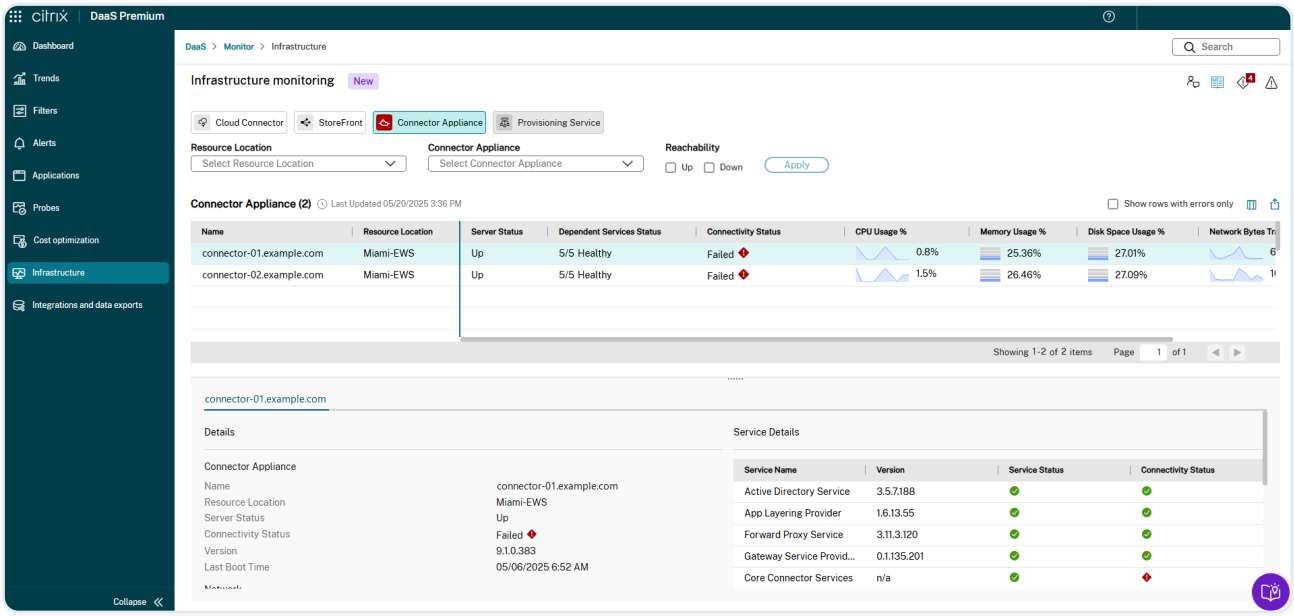
コネクタアプライアンスは、ハイパーバイザーでホストされるCitrixコンポーネントです。これは、Citrix Cloudとリソースの場所間の通信チャネルとして機能し、複雑なネットワークやインフラストラクチャの構成を必要とせずにクラウド管理を可能にします。コネクタアプライアンスを使用すると、ユーザーに価値を提供するリソースを管理し、集中することができます。詳細については、「Secure Private Access用コネクタアプライアンス」を参照してください。

コネクタアプライアンスの健全性メトリック機能は、Citrixインフラストラクチャ内のコネクタアプライアンスコンポーネントの健全性とパフォーマンスを監視するための重要な機能を提供します。このコンポーネントは、Citrix DaaSサイトに接続すると監視のために自動的にオンボーディングされ、インフラストラクチャ監視ダッシュボードへのシームレスな統合が保証されます。

健全性メトリックはインフラストラクチャ監視ダッシュボードに表示され、コネクタアプライアンスのステータスを一元的に表示します。管理者は詳細なメトリックと傾向にアクセスして、問題をプロアクティブに特定し、解決できます。

次の図は、Monitorにおけるコネクタアプライアンスの健全性の例を示しています。

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



セッションとアプリケーションの傾向

管理者は、DaaS Monitorから組織全体のセッションとアプリケーションの傾向を監視できます。これには、ロールアウトの追跡、ポリシーと構成の機能の理解、潜在的な問題の分析が含まれます。

詳細については、「Secure Private Access Serviceの可視性」を参照してください。

セッションとアプリケーションの傾向

Citrix Monitor を使用して、組織全体の Secure Private Access セッションとアプリケーションの傾向を監視します。ロールアウトの進捗状況を追跡し、ポリシーと構成のパフォーマンスを理解し、広範囲にわたるユーザーの問題を引き起こしているかどうかを特定します。Citrix Monitor は、ユーザーアクティビティとアプリケーションの使用パターンを包括的に可視化し、展開を最適化します。

Citrix Monitor は、Secure Private Access 環境に関するリアルタイムおよび過去のインサイトを提供し、管理者がリソース割り当て、ポリシー調整、ユーザーエクスペリエンスの改善についてデータに基づいた意思決定を行えるようにします。監視機能は、セキュリティコンプライアンスを確保しながら最適なパフォーマンスを維持するのに役立ちます。

セッション監視

管理者は、Monitor を使用してアクティブなユーザーセッションをリアルタイムで監視できます。Web/SaaS および TCP/UDP アプリのアプリ障害を監視し、ダッシュボードで Web/SaaS アプリのアクティブなセッションを表示できます。詳細については、「Secure Private Access Service の可視性」を参照してください。

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

アプリケーションの傾向

Secure Private Access アプリケーションのアクセス傾向を監視し、アクティブなアプリケーションセッションを表示し、問題や障害が発生しているアプリケーションを特定します。Citrix Monitor は、アプリケーションの使用パターンを理解し、パフォーマンスを最適化し、組織の重要なアプリケーションへの信頼性の高いアクセスを確保するのに役立つ包括的な分析機能を提供します。

これらの監視機能へのアクセスとデータの解釈に関する詳細については、「Secure Private Access Service の可視性」を参照してください。

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

トリアージとトラブルシューティング

このトピックでは、Citrix Secure Private Access に関連する問題を効果的にトラブルシューティングおよびトリアージするための重要な考慮事項と手順について概説します。管理者はこのドキュメントを、問題の特定、診断、解決のためのガイドとして使用し、ユーザーにシームレスで安全なアクセスを保証できます。

詳細については、以下のトピックを参照してください。

アプリ関連の問題のトラブルシューティング

デバイスポスチャーステータス、ログイン/ログオフステータス、アプリの列挙、アプリアクセスに関連する問題を表示します。詳細については、「アプリ関連の問題のトラブルシューティング」を参照してください。

DaaS Monitor の Secure Private Access セッションコード

Citrix Monitor で、アプリケーションの列挙、アプリケーションの起動、およびセッションに関連するエラーコードのリストを表示します。詳細については、「DaaS Monitor の Secure Private Access セッションコード」を参照してください。

Monitor でのセッション関連の問題のトラブルシューティング

Monitor のヘルプデスクビュー（アクティビティマネージャーページ）を使用して、ユーザーまたはエンドポイントに関する情報を表示します。詳細については、「Monitor でのセッション関連の問題のトラブルシューティング」を参照してください。

デバイスポスチャー関連の問題のトラブルシューティング

ユーザーが Secure Private Access または DaaS を介して接続する際に各セッションで生成されるトランザクション ID を使用して、DaaS Monitor でデバイスポスチャーの問題/エラーをトラブルシューティングできます。トランザクション ID を特定すると、DaaS Monitor にはセッションと適用された関連のデバイスポスチャーポリシーに関する情報が表示されます。Monitor には、デバイ

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

スがポスチャーチェックに合格したか失敗したかを含むポリシー結果も表示されます。詳細については、「デバイスポスチャーサービスのトラブルシューティング」を参照してください。

認証関連の問題のトラブルシューティング

条件付き認証が失敗した場合、失敗メッセージにあるトランザクション ID を使用して、Monitor で失敗の詳細を検索できます。Monitor は、Monitor UI に失敗理由と条件付きポリシーを表示することで、条件付き認証失敗イベントのトラブルシューティングに役立ちます。詳細については、「認証のトラブルシューティング」を参照してください。

ログを使用したトラブルシューティング

Secure Private AccessおよびDevice Postureログは、管理者が構成の問題、接続の問題、ポリシーの誤構成、およびデバイスのコンプライアンスの問題を特定するのに役立ち、問題のより迅速な特定と解決を可能にします。

セキュア プライベート アクセス ログ

Secure Private Accessログは、Secure Private Accessダッシュボードから表示できます。診断ログに記録されるさまざまなイベントについては、「イベント」を参照してください。

Secure Private Access診断ログの詳細については、「診断ログ」を参照してください。

各イベントに関連付けられているさまざまなエラーコードについては、「診断ログ情報コード」を参照してください。

デバイス ポスチャ ログ

Device Postureダッシュボードの診断ログは、デバイスのコンプライアンス（準拠、非準拠、ログイン拒否）に関する洞察を提供します。これらのログにより、管理者はエンドポイントのセキュリティを監視し、組織のポリシーへの準拠を確保し、環境リスクをもたらす可能性のあるデバイスを特定できます。

Device Postureログとイベントは、Secure Private Accessダッシュボードおよび Identity and Access Managementコンソールで表示できます。

詳細については、「Device Postureログとイベント」を参照してください。

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

Monitor を使用したリアルタイムセッションのトラブルシューティング

管理者は、Monitor コンソールを使用して、Secure Private Access セッションをリアルタイムで監視し、トラブルシューティングを行うことができます。

関連情報については、次のトピックを参照してください。

- Secure Private Access と Monitor の統合については、「DaaS Monitor との統合」を参照してください。
- Monitor で Secure Private Access ユーザーセッションを検索して、トラブルシューティングやレポート作成のために特定のセッションをすばやく見つけることができます。詳細については、「ユーザー別の Secure Private Access セッションの表示」を参照してください。
- Monitor の詳細については、「DaaS Monitor」を参照してください。

診断ログのエラーコード

次の表は、Secure Private Access サービスの使用時にユーザーが遭遇する可能性のあるさまざまなエラーと、それに対応する解決策の包括的なリストを示しています。

情報コード	説明	解決策
0x180022	認証サービスがダウンしているため、アプリの起動に失敗しました	認証サービスがダウンしているため、アプリの起動に失敗しました
0x1800B7	アプリの FQDN の長さが超過したため、アプリの起動に失敗しました	「アプリの起動に失敗しました。アプリのFQDNの長さが超過しました。」(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#app-launch-failed-because-app-fqdn-length-exceeded)
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7	バックエンドのWebアプリに接続できなかったため、Webアプリの起動に失敗しました	「バックエンドのWebアプリに接続できなかったため、Webアプリの起動に失敗しました」(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#web-app-launch-

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

情報コード	説明	解決策
		failed-as-unable-to-connect-to-back-end-web-app)
0x18001A, 0x18001B	ユーザーの詳細が見つかりません	「ユーザーの詳細が見つかりません」(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#user-details-not-found)
0x1800AA	SAMLトークン準備中にユーザー属性が見つからなかったため、Web/SaaSアプリの起動に失敗しました	「Web/SaaSアプリの起動に失敗しました」(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#websaas-app-launch-has-failed-due-to-user-attributes-not-found-while-preparing-the-saml-token)
0x180010	アプリケーションのFQDNを特定できなかったため、Web/SaaSアプリの起動に失敗しました	「アプリケーションのFQDNを特定できなかったため、Web/SaaSアプリの起動に失敗しました」(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#websaas-app-launch-has-failed-due-to-inability-to-identify-the-application-fqdn)
0x180040	SAMLサービスプロバイダーから提供されたappIdが無効だったため、Web/SaaSアプリの起動に失敗しました	SAMLサービスプロバイダーによって提供されたapp IDが無効なため、アプリの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#websaas-app-launch-has-failed-due-to-invalid-appid-provided-by-the-saml-service-provider)

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

情報コード	説明	解決策
0x180011, 0x180012, 0x180013, 0x180017, 0x180032, 0x180033, 0x180034, 0x180035, 0x180048	無効なアプリアクセス要求のため、Web/SaaSアプリの起動に失敗しました。	無効なアプリアクセス要求のため、Web/SaaSアプリの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#websaas-app-launch-has-failed-due-to-invalid-app-access-request)
0x1800D4, 0x1800E1, 0x180106, 0x180107, 0x1800EB, 0x1800EC	内部エラーのため、ポリシー評価中にアプリの起動に失敗しました。	内部エラーのため、ポリシー評価中にアプリの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#app-launch-has-failed-during-policy-evaluation-due-to-internal-error)
0x1800D9	ポリシー評価応答の解析中にアプリの起動に失敗しました。	ポリシー評価応答の解析中にアプリの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#app-launch-has-failed-while-parsing-policy-evaluation-response)
0x1800DA	ポリシー評価中に無効な結果が返されたため、アプリの起動に失敗しました。	ポリシー評価中に無効な結果が返されたため、アプリの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#app-launch-has-failed-with-invalid-result-during-policy-evaluation)
0x1800DB	無効なリソースロケーション構成のため、アプリの起動に失敗しました。	アプリケーションの起動に失敗しました。リソースの場所の構成が無効です。

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

情報コード	説明	解決策
0x1800E0	アプリケーション名の長さが長すぎるため、アプリケーションの起動に失敗しました。	アプリケーション名の長さが長すぎるため、アプリケーションの起動に失敗しました。
0x1800EE	無効なアプリケーションIDのため、プライベートTCPサーバーへの接続確立中にアプリケーションの起動に失敗しました。	無効なアプリケーションIDのため、プライベートTCPサーバーへの接続確立中にアプリケーションの起動に失敗しました。
0x1800E3	ポリシー評価中にアプリケーションの起動が拒否されました。	ポリシー評価中にアプリケーションの起動が拒否されました。
0x1800EA	宛先FQDNが長すぎるため、アプリケーションの起動に失敗しました。	宛先FQDNが長すぎるため、アプリケーションの起動に失敗しました。
0x1800ED	無効な宛先IPのため、アプリケーションの起動に失敗しました。	無効な宛先IPのため、アプリの起動に失敗しました(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#app-launch-has-failed-due-to-invalid-destination-ip)
0x180102	Connector Appliance から応答がなかったため、アプリの起動に失敗しました	Connector Appliance から応答がなかったため、アプリの起動に失敗しました(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#app-launch-failed-as-no-response-was-received-from-the-connector-appliance)
0x10000005	バックエンドアプリサーバーとの接続確立に失敗したため、Web/SaaSアプリケーションの起動に失敗しました	バックエンドアプリサーバーとの接続確立に失敗したため、Web/SaaSアプリケーションの起動に失敗しました

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

情報コード	説明	解決策
		(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#websaas-application-launch-failed)
エラーコード: 0x10000101、0x10000102、0x10000103、0x10000104	無効なアプリケーション構成のため、Web/SaaS FormFill SSOに失敗しました	無効なアプリケーション構成のため、Web/SaaS FormFill SSOに失敗しました(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#websaas-formfill-sso-failed-due-to-invalid-application-configuration)
0x10000202	Web/SaaS の Kerberos SSO に失敗しました	Web/SaaS の Kerberos SSO に失敗しました(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#kerberos-sso-for-websaas-failed)
0x10000203	内部サーバーエラーのため、Web/SaaS SSOに失敗しました	Web/SaaS SSO は内部サーバーエラーにより失敗しました(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#websaas-sso-failed-due-to-internal-server-error)
0x10000303, 0x10000304	設定されたプロキシに到達できないため、Web/SaaS アプリの起動に失敗しました	設定されたプロキシに到達できないため、Web/SaaS アプリの起動に失敗しました(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#websaas-app-launch-failed-due-to-the-

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

情報コード	説明	解決策
		configured-proxy-being-unreachable)
0x10000305	設定されたプロキシでの認証に失敗したため、Web/SaaS アプリの起動に失敗しました	設定されたプロキシでの認証に失敗したため、Web/SaaS アプリの起動に失敗しました(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#websaas-app-launch-failed-due-to-a-failure-to-authenticate-with-the-configured-proxy)
0x10000414	無効な IP/ホスト名またはポートでリクエストが送信されたため、アプリケーションの起動に失敗しました	無効な IP/ホスト名またはポートでリクエストが送信されたため、アプリケーションの起動に失敗しました(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#application-launch-failed-due-to-a-request-coming-on-an-invalid-iphostname-or-port)
0x10000415	宛先サーバーが接続を拒否したため、アプリケーションの起動に失敗しました	宛先サーバーが接続を拒否したため、アプリケーションの起動に失敗しました(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#application-launch-failed-as-the-destination-server-refused-the-connection)
0x10000416	宛先が見つからなかったため、アプリケーションの起動に失敗しました	アプリケーションの起動に失敗しました。宛先が見つかりませんでした。(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#application-

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

情報コード	説明	解決策
		launch-failed-as-the-destination-was-not-found)
0x10000417	アプリケーションの起動に失敗しました。宛先ネットワークに到達できませんでした。	アプリケーションの起動に失敗しました。宛先ネットワークに到達できませんでした。(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#application-launch-failed-as-the-destination-network-was-not-reachable)
0x10000405	宛先に接続できなかったため、アプリケーションの起動に失敗しました。	宛先に接続できなかったため、アプリケーションの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#application-launch-failed-due-to-the-inability-to-connect-to-the-destination)
0x10000301	コネクタからSPAサービスへの接続に失敗しました	コネクタからSecure Private Accessサービスへの接続に失敗しました。(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#connector-to-secure-private-access-service-connection-failed)
0x10000302	コネクタがプロキシの詳細を読み取れませんでした	コネクタがプロキシの詳細を読み取れませんでした。(/ja-jp/citrix-secure-private-access/service/spa-daas-monitor-error-codes.html#connector-failed-to-read-the-proxy-details)

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

情報コード	説明	解決策
0x10000306	構成されたプロキシに到達できません	設定されたプロキシに到達できません
0x10000401	コネクタアプライアンスがFRに到達できません	コネクタアプライアンスがFR (エッジノード) に到達できません
0x10000403, 0x10000404, 0x10000407	内部接続エラーによりアプリケーションの起動に失敗しました	内部接続エラーによりアプリケーションの起動に失敗しました
6003, 6007	Citrix Secure AccessクライアントがSSOに失敗しました	Citrix Secure AccessクライアントがSSOに失敗しました

認証サービスがダウンしているため、アプリの起動に失敗しました

情報コード: 0x180022

Secure Private Accessを使用すると、管理者は従来のActive Directory、AAD、Okta、SAMLなどのサードパーティ認証サービスを構成できます。これらの認証サービスの停止がこの問題を引き起こす可能性があります。

サードパーティサーバーが稼働しており、到達可能であることを確認してください。

アプリケーションのFQDN長が超過したため、アプリの起動に失敗しました

情報コード: 0x1800B7

アプリケーションのFQDNは512文字を超えてはなりません。アプリケーション構成ページでアプリケーションのFQDNを確認し、この制限を超えていないことを確認してください。

1. 管理コンソールで**アプリケーション**タブに移動します。
2. FQDNが512文字を超えるアプリケーションを探します。
3. アプリケーションを編集し、アプリケーションのFQDNの長さを修正します。

バックエンドWebアプリに接続できないため、Webアプリの起動に失敗しました

情報コード: 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7

社内ネットワーク内で実行されているWebアプリケーションの閲覧エクスペリエンスが破損しています。

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

1. 解決できないFQDNについて診断ログをフィルタリングします。
2. 社内ネットワーク内からバックエンドサーバーへの到達可能性を確認します。
3. プロキシ設定を確認し、コネクタがバックエンドサーバーへの到達をブロックされていないか確認します。

ユーザーの詳細が見つかりません

情報コード: 0x18001A, 0x18001B

Secure Private Accessサービスがリクエストを処理している間、ドメインユーザーの詳細が見つかりません。この問題は、必要なドメインユーザー属性がCitrix Cloud™から欠落している場合に発生する可能性があります。

1. Citrix Cloud Connector™がユーザーをCitrix Cloudに問題なく同期していることを確認します。
2. **Citrix Cloud > Identity and Access Management** 内のドメインに到達可能であることを確認してください。
3. Citrix Workspace からログアウトし、再度ログインしてください。

SAMLトークン準備中にユーザー属性が見つからなかったため、Web/SaaSアプリの起動に失敗しました

情報コード: 0x1800AA

Secure Private AccessサービスがSAMLトークンを準備している際に、必要なユーザー属性が見つかりません。この問題は、Citrix Cloudからの必要なドメインユーザー属性が不足している場合に発生する可能性があります。

1. Citrix Cloud ConnectorがCitrix Cloudへのユーザー同期に問題がないことを確認してください。
2. **Citrix Cloud > Identity and Access Management** 内のドメインに到達可能であることを確認してください。
3. Citrix Workspace からログアウトし、再度ログインしてください。

アプリケーションFQDNを識別できなかったため、Web/SaaSアプリの起動に失敗しました

情報コード: 0x180010

指定されたドメイン名に対応するアプリケーションが見つかりません。

ドメイン名の長さが構成制限を超えていないことを確認してください。

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

SAMLサービスプロバイダーから提供された無効なAppIdにより、Web/SaaSアプリの起動に失敗しました

情報コード: 0x180040

SAMLサービスプロバイダーから提供されたAppIdが無効です。SAMLサービスプロバイダーによって指定されたApp IDを持つアプリを見つけることができません。

1. SAMLサービスプロバイダーの構成を確認します。
2. SAMLサービスプロバイダーで構成されているIdP URLが適切であることを確認します。
3. このアプリIDは、Secure Private Accessサービスで構成されているアプリとマッピングされている必要があります。

無効なアプリアクセス要求のため、Web/SaaSアプリの起動に失敗しました

情報コード: 0x180011, 0x180012, 0x180013, 0x180017, 0x180032, 0x180033, 0x180034, 0x180035, 0x180048

Secure Private Accessサービスが受信した無効な要求のため、アプリへのアクセスに失敗しました。

Secure Private Accessサービスが受信したアプリケーションを識別できません。受信した要求パラメーターが無効である可能性があります。

1. アプリケーションを再起動するか、Citrix Workspaceからログアウトして再度ログインしてください。
2. 問題が解決しない場合は、Citrixサポートにお問い合わせください。

内部エラーのため、ポリシー評価中にアプリの起動に失敗しました

情報コード: 0x1800D4, 0x1800E1, 0x180106, 0x180107, 0x1800EB, 0x1800EC

トランザクションIDとクライアントが収集したデバッグログを添えてCitrixサポートにお問い合わせください。

ポリシー評価応答の解析中にアプリの起動に失敗しました

情報コード: 0x1800D9

アプリケーション構成に特殊文字が含まれているか、ポリシー構成に問題がある可能性があります。

TCP/UDP/HTTPアプリの設定にサポートされていない文字が含まれていないことを確認してください。

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

1. Secure Private Access管理コンソールで**アプリケーション**をクリックします。
2. アプリケーション名または宛先に特殊文字が含まれていないか確認します。

ポリシーが正しく構成され、適切なアプリケーションに割り当てられているか確認してください。

1. Secure Private Access管理ポータルで**アクセスポリシー**をクリックします。
2. ポリシー構成、ポリシー名、および条件を確認します。
3. ポリシーが適切なアプリケーションに割り当てられているか確認します。

設定が正しい場合は、トランザクションIDとクライアントデバッグログを添えてCitrixサポートにお問い合わせください。

ポリシー評価中に無効な結果でアプリの起動に失敗しました

情報コード: 0x1800DA

アプリケーションまたはポリシーの設定に問題がある可能性があります。TCP/UDP/HTTPアプリの設定にサポートされていない文字が含まれていないことを確認してください。

1. Secure Private Access管理コンソールで**アプリケーション**をクリックします。
2. アプリケーション名または宛先ドメイン/FQDNに特殊文字が含まれていないか確認します。
3. また、宛先IP/IP範囲/IP CIDRが有効であるかどうかも確認します。

アプリケーションドメインテーブル（**Secure Private Access > 設定 > アプリケーションドメイン**）でアプリケーション宛先エントリが有効になっていることを確認してください。

ポリシーが正しく構成され、適切なアプリケーションに割り当てられているかを確認します。

1. Secure Private Access 管理ポータルで をクリックします。
2. ポリシー構成、ポリシー名、および条件を確認します。
3. ポリシーが適切なアプリケーションに割り当てられているかを確認します。

無効なリソースロケーション構成によりアプリの起動に失敗しました

情報コード: 0x1800DB

リソースロケーションと構成に問題がある可能性があります。

リソースロケーションが構成されていることを確認します。

1. Citrix Cloud ポータルにログインし、メニューから をクリックします。

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

2. 予期されるリソースロケーションが構成されているかを確認します。

リソースロケーションが正常でアクティブであることを確認します。

1. Citrix Cloud ポータルにログインし、メニューから をクリックします。
2. 予期されるリソースロケーションがアクティブで正常であるかを確認します。

テーブル (**Secure Private Access > 設定 > アプリケーション ドメイン**) で、宛先に正しいリソースロケーションが選択されていることを確認します。

1. Secure Private Access 管理コンソールで をクリックします。
2. 「**アプリケーションドメイン**」タブをクリックします。
3. アクセスされた宛先に正しいリソースロケーションが構成されているか確認します。
4. アクセスされた宛先エントリが「**アプリケーションドメイン**」テーブルでアクティブになっているか確認します。

   TCP/UDP/HTTPアプリケーションで構成された宛先は、自動的に「**アプリケーションドメイン**」テーブルに追加されます。アクティブなTCP/UDP/HTTPアプリケーションの宛先/URLを削除または無効にしないことをお勧めします。

アプリケーション名の長さが長すぎるため、アプリの起動に失敗しました

情報コード: 0x1800E0

トランザクションIDとクライアントが収集したデバッグログを添えてCitrixサポートにお問い合わせください。

無効なアプリIDのため、プライベートTCPサーバーへの接続確立中にアプリの起動に失敗しました

情報コード: 0x1800EE

トランザクションIDとクライアントが収集したデバッグログを添えてCitrixサポートにお問い合わせください。

ポリシー評価中にアプリの起動が拒否されました

情報コード: 0x1800E3

トランザクションIDとクライアントが収集したデバッグログを添えてCitrixサポートにお問い合わせください。

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

宛先FQDNが長すぎるため、アプリの起動に失敗しました

情報コード: 0x1800EA

FQDNの長さが256文字未満であることを確認してください。

無効な宛先IPのため、アプリの起動に失敗しました

情報コード: 0x1800ED

クライアントから有効なプライベートIPアドレスのみにアクセスしてください。

Connector Applianceから応答がなかったため、アプリの起動に失敗しました

情報コード: 0x180102

Connector Applianceの到達可能性を確認してください。

無効なIP/ホスト名またはポートへのリクエストにより、アプリケーションの起動に失敗しました

情報コード: 0x10000414

ホスト名、IPアドレス、またはポート番号の有効性を確認してください。

宛先サーバーが接続を拒否したため、アプリケーションの起動に失敗しました

情報コード: 0x10000415

宛先サーバーのステータスを確認してください。

宛先が見つからなかったため、アプリケーションの起動に失敗しました

情報コード: 0x10000416

宛先サーバーのホスト名を確認します。

宛先ネットワークに到達できなかったため、アプリケーションの起動に失敗しました

情報コード: 0x10000417

Connector Appliance はバックエンドのプライベート TCP/UDP サーバーとの接続に問題があります。Connector Appliance のネットワーク設定を確認してください。

- エンドユーザーが接続しようとしているバックエンドサーバーが稼働しており、要求を受信できることを確認します。
- 社内ネットワーク内からバックエンドサーバーへの到達可能性を確認します。

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

- コネクタがバックエンドサーバーに到達できないようにブロックされていないか、プロキシ設定を確認します。
- FQDN ベースのアプリに対する要求の場合、DNS サーバーで該当するアプリの DNS エントリを確認します。

宛先に接続できなかったため、アプリケーションの起動に失敗しました

情報コード: 0x10000405

Connector Appliance はバックエンドのプライベート TCP/UDP サーバーとの接続に問題があります。Connector Appliance のネットワーク設定を確認してください。

- エンドユーザーが接続しようとしているバックエンドサーバーが稼働しており、要求を受信できることを確認します。
- 社内ネットワーク内からバックエンドサーバーへの到達可能性を確認します。
- コネクタがバックエンドサーバーに到達できないようにブロックされていないか、プロキシ設定を確認します。
- FQDN ベースのアプリに対する要求の場合、DNS サーバーで該当するアプリの DNS エントリを確認します。

コネクタからSecure Private Accessサービスへの接続に失敗しました

情報コード: 0x10000301

- エラーコードのトランザクションIDを検索します。
- Secure Private Accessダッシュボードで、トランザクションIDに一致するすべてのイベントをフィルタリングします。
- トランザクションIDに一致する他のコンポーネントでエラーが発生したかどうかを確認し、エラーが見つかった場合は、そのエラーコードに一致する適切な回避策を実行します。
- 他のコンポーネントでエラーが見つからない場合は、次の手順を実行します。
  - Connector Appliancesの管理ページに移動します。
  - 診断レポートをダウンロードします。詳細については、「診断レポートの生成」を参照してください。
  - パケットトレースをキャプチャします。詳細については、「ネットワーク接続の確認」を参照してください。
- この診断レポートとパケットトレース、およびエラーコードとトランザクションIDを添えてCitrixサポートに連絡してください。

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

コネクタがプロキシの詳細の読み取りに失敗しました

情報コード: 0x10000302

Connector Applianceは、バックエンドのプライベートTCP/UDPサーバーとの接続に問題があります。Connector Applianceのネットワーク設定を確認してください。

- エンドユーザーが接続しようとしているバックエンドサーバーが稼働しており、リクエストを受信できることを確認します。
- 社内ネットワークからバックエンドサーバーへの到達可能性を確認します。
- プロキシ設定を確認し、コネクタがバックエンドサーバーに到達できないようにブロックされていないか確認します。
- FQDNベースのアプリのリクエストの場合、DNSサーバーで該当するアプリのDNSエントリを確認します。

設定されたプロキシに到達できません

情報コード: 0x10000306

Connector ApplianceがバックエンドのプライベートTCP/UDPサーバーとの接続に問題があります。(/us/en/citrix-cloud/resource-locations/connector-appliance.html#network-settings-for-your-connector-appliance)でネットワーク設定を確認してください。

- エンドユーザーが接続しようとしているバックエンドサーバーが稼働しており、リクエストを受信できる状態にあるか確認してください。
- 社内ネットワーク内からバックエンドサーバーへの到達可能性を確認してください。
- プロキシ設定を確認し、コネクタがバックエンドサーバーに到達できないようにブロックされていないか確認します。
- FQDNベースのアプリのリクエストの場合、DNSサーバーで該当するアプリのDNSエントリを確認します。

Connector ApplianceがFR (エッジノード) に到達できません

情報コード: 0x10000401

Citrix Secure Private Accessサービスとのネットワーク接続を確認してください。

詳細については、(/us/en/citrix-cloud/resource-locations/connector-appliance.html#network-settings-for-your-connector-appliance)を参照してください。

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

内部接続エラーによりアプリケーションの起動に失敗しました

情報コード: 0x10000403, 0x10000404, 0x10000407

- エラーコードのトランザクションIDを調べます。
- Secure Private Accessダッシュボードで、トランザクションIDに一致するすべてのイベントをフィルタリングします。
- トランザクションIDに一致する他のコンポーネントでエラーが発生していないか確認します。エラーが見つかった場合は、そのエラーコードに一致する適切な回避策を実行します。
- 他のコンポーネントでエラーが見つからない場合は、次の手順を実行します。
  - Connector Appliancesの管理者ページに移動します。
  - 診断レポートをダウンロードします。詳細については、「診断レポートの生成」を参照してください。
  - パケットトレースをキャプチャします。詳細については、「ネットワーク接続の確認」を参照してください。
- この診断レポートとパケットトレース、およびエラーコードとトランザクションIDを添えてCitrixサポートに連絡してください。

Web/SaaSアプリケーションの起動に失敗しました

バックエンドアプリサーバーとの接続確立に失敗したため、Web/SaaSアプリケーションの起動に失敗しました。

情報コード： 0x10000005

ターゲットURLを確認するか、Connector Applianceのネットワーク設定を確認してください。詳細については、「Connector Applianceのネットワーク設定」を参照してください。

無効なアプリケーション構成のため、Web/SaaS FormFill SSOに失敗しました

情報コード： 0x10000101、0x10000102、0x10000103、0x10000104

SSOフォームアプリの構成を確認し、ユーザー名、パスワード、アクション、ログインURLの各フィールドがアプリ設定で正しく構成されていることを確認してください。

Web/SaaS 用 Kerberos SSO が失敗しました

情報コード: 0x10000202

Connector Appliance の内部サーバーエラー、またはドメインコントローラーからトークンを取得できなかったため、Web/SaaS 用 Kerberos SSO が失敗しました。

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

バックエンドサーバーとドメインコントローラーの Kerberos SSO 設定を確認してください。フォールバック NTLM 認証設定も確認してください。

詳細については、「Kerberos 構成の検証」を参照してください。

内部サーバーエラーにより Web/SaaS SSO が失敗しました

情報コード: 0x10000203

Secure Private Access サービスとバックエンドサーバーの SSO 設定を確認してください。Secure Private Access サービスについては、「優先サインオン方法の設定」を参照してください。

構成されたプロキシに到達できないため、Web/SaaS アプリの起動に失敗しました

情報コード: 0x10000303, 0x10000304

プロキシサーバーの設定を確認し、Connector Appliance に到達可能であることを確認してください。詳細については、「Citrix Cloud への Connector Appliance の登録」を参照してください。

構成されたプロキシでの認証に失敗したため、Web/SaaS アプリの起動に失敗しました

情報コード: 0x10000305

プロキシサーバーの資格情報を確認し、Connector Appliance で正しく構成されていることを確認してください。詳細については、「Connector Appliance の登録後」を参照してください。

Citrix Secure Access™ クライアントが SSO を実行できませんでした

情報コード: 6003

Broker Agent サービスから Secure Private Access シングルサインオンハンドルの取得中にエラーが発生しました。

Secure Private Access SSO フラグがデリバリーグループで有効になっているか確認してください。詳細については、VDA 上の Citrix Secure Access Client からのシームレスなログオンを参照してください。

情報コード: 6007

Secure Private Access へのログインに失敗しました。

Citrix Secure Access クライアントセッションがタイムアウトした場合は、VDA を再起動してください。

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

セッションコード

コード	ステータス	説明
2101	失敗	セッションの失敗
2102	アクティブ/非アクティブ/失敗	セッションがアクティブであるか、終了しているか、またはセッション内の少なくとも 1 つのアプリ起動が失敗しました
2000	アクティブ	セッションはアクティブです
2001	非アクティブ	セッションは終了/非アクティブです

アプリ列挙メッセージコード

コード	ステータス	説明
1000	成功	列挙は成功しました。少なくとも1つのアプリが列挙されました。
1001	成功	すべてのアプリケーションがポリシーによって拒否されたため、アプリケーションは列挙されませんでした。
1002	成功	一致するポリシーがなかったため、アプリケーションは列挙されませんでした。
1003	成功	一部のアプリケーションが拒否され、その他については一致するポリシーがなかったため、アプリケーションは列挙されませんでした。
1004	成功	評価するポリシーがなかったため、アプリケーションは列挙されませんでした。

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

コード	ステータス	説明
1101	失敗	列挙中に内部エラーが発生しました。
1102	失敗	一部のアプリケーションは列挙されましたが、少なくとも1つのアプリの評価に失敗しました。
1103	失敗	アプリケーションは列挙されず、少なくとも1つのアプリ評価が失敗しました
3000	許可	アプリケーションの列挙が許可されています
3001	拒否	ポリシーによりアプリケーションの列挙が拒否されました
3002	拒否	一致するポリシーがなかったため、アプリケーションは列挙されませんでした
3003	不明	アプリケーションの列挙ステータスは不明です
3004	CEBからのアプリケーション起動	Citrix Enterprise Browser™からのアプリケーション起動試行
3101	失敗	アプリケーションの列挙 - 内部エラーが発生しました (現在未使用)
3102	失敗	ポリシー評価中に例外が発生したため、アプリケーションは列挙されませんでした
3103	失敗	アプリケーションの列挙ステータスがnullです - ポリ

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

コード	ステータス	説明
		シー評価中に内部エラーが発生しました
3104	許可/拒否/失敗	アプリのポリシー詳細の取得中にエラーが発生しました

アプリ起動メッセージコード

コード	ステータス	説明
4000	許可	アプリケーションの起動が許可されています
4001	拒否	ポリシーによりアプリケーションの起動が拒否されました
4002	拒否	一致するポリシーがなかったため、アプリケーションの起動が拒否されました
4101	失敗	アプリケーション起動エラー - アプリケーション起動中に内部エラーが発生しました
4102	失敗	アプリケーション起動エラー (内部)
4103	許可/拒否/失敗	アプリのポリシー詳細の取得中にエラーが発生しました
4104	失敗	アプリケーション起動エラー - アプリケーション構成が見つかりません

アプリ起動エラーコード

コード	説明	解決策/回避策
5001	TCP - 接続失敗	宛先へのネットワーク到達可能性を確認します (NetScaler

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

コード	説明	解決策/回避策
5003	TCP - プローブ失敗	Gateway から `-S <SNIP>` を ping します)。
5002	TCP - プロキシサーバーがダウンしています	プロキシホストが稼働していることを確認してください。
5004	TCP - ゲートウェイでのメモリ割り当てに失敗しました	デバッグレベルのログを有効にし、NetScaler からサポートバンドルを収集します。
5005	TCP - サーバーダウン	宛先へのネットワーク到達可能性を確認し (NetScaler Gateway から `-S <SNIP>` を ping)、サーバーがダウンしているかどうかを確認します。
5006	TCP - プロキシ接続失敗	プロキシホストが稼働しており、接続を受け入れていることを確認します。
5007	TCP - プロキシプローブ失敗	宛先へのネットワーク到達可能性を確認します (NetScaler Gateway から `-S <SNIP>` を ping)。デバッグレベルのログを有効にし、NetScaler からサポートバンドルを収集します。
5008	SPA - サーバーダウン	Secure Private Access サイトの URL が稼働していることを確認します。(NetScaler CLI で `show vpn securePrivateAccessProfile` CLI コマンドを使用して URL ステータスを確認します)。
5009	SPA - コールアウトリクエストエラー	Secure Private Accessサイトの URLが稼働していることを確認します。デバッグレベルのログを有効にし、

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

コード	説明	解決策/回避策
5010	SPA - コールアウト応答エラー	NetScalerからサポートバンドルを収集します。
5011	TCP - セッションの有効期限切れ	これは、ユーザーセッションがアクティブでなくなったときにアプリにアクセスされたことを示します。新しいアクティブなユーザーセッションを開始してください。
5013	TCP - ゲートウェイ内部エラー	デバッグレベルのログを有効にし、NetScalerからサポートバンドルを収集します。
5014	TCP - DNSサーバーがダウンしています	DNSサーバーが稼働していることを確認してください。
5015	TCP - ゲートウェイDNS内部エラー	DNSサーバーが稼働していることを確認してください。デバッグレベルのログを有効にし、NetScalerからサポートバンドルを収集します。
5016	宛先サーバーへの接続に失敗しました	宛先へのネットワーク到達可能性を確認します (NetScaler Gateway から `<SNIP>` を使用して ping を実行)。
5017	宛先サーバーのDNS解決に失敗しました	アプリケーションが使用するホスト名が、意図したDNSサーバー (内部またはパブリック) によって解決されることを確認してください。
5018	ゲートウェイ内部エラー	デバッグレベルのログを有効にし、NetScaler からサポートバンドルを収集してください。
0x1300000C	アプリケーションドメインのDNS解決に失敗しました	アプリケーションが使用するホスト名が、意図したDNS

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

コード	説明	解決策/回避策
		サーバー (内部またはパブリック) によって解決されることを確認してください。

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

Secure Private Access のログとイベント

ログとイベントは、監視、トラブルシューティング、コンプライアンスの確保に不可欠です。Citrix Secure Private Access サービス関連のログとイベントは、次のソースからアクセスできます。

診断ダッシュボード

診断ダッシュボードは、ログとイベントを表示および分析するための一元化されたインターフェイスを提供します。管理者はこのダッシュボードを使用して、Secure Private Access に関連する問題を監視およびトラブルシューティングできます。詳細については、「Secure Private Access ダッシュボード」を参照してください。

エラーのリスト

Secure Private Access サービスの使用中にユーザーが遭遇する可能性のあるエラーの包括的なリストについては、「診断ログ情報コード」を参照してください。

監査ログ

監査ログは、ユーザーアクティビティとシステム変更の詳細な記録をキャプチャします。これらのログは、誰がシステムにアクセスしたか、どのような変更が行われたか、いつこれらのアクションが発生したかを追跡するのに役立つため、コンプライアンスとセキュリティの目的で不可欠です。詳細については、「監査ログとシステムログ」を参照してください。

システムログ

システムログには、Secure Private Access サービスの内部操作に関する情報が含まれています。これらのログは、パフォーマンスの問題やサービス機能のエラーなど、システムレベルの問題を診断するのに役立ちます。詳細については、「システムログ」を参照してください。

デバイスポスチャログ

デバイスポスチャログは、Secure Private Access サービスにアクセスするデバイスのセキュリティポスチャに関する洞察を提供します。これらのログは、アクセスを許可する前にデバイスが必

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

要なセキュリティ標準を満たしていることを確認するのに役立ち、それによって全体的なセキュリティを強化します。詳細については、「デバイスポスチャログ」を参照してください。

診断ログ

以下のセクションでは、診断ログに関する詳細情報を提供します。

FAQ

以下のセクションでは、よくある質問に関する詳細情報を提供します。

Secure Private Access 診断ログとは何ですか?

Secure Private Access 診断ログは、ユーザーが任意のアプリケーション (Web/SaaS/TCP/UDP) にアクセスしたときに発生するすべてのイベントをキャプチャします。これらのログは、デバイスのポスチャ、アプリ認証、アプリ列挙、およびアプリアクセスログをキャプチャします。詳細情報は表形式で表示されます。ログは、事前に設定された時間またはカスタムのタイムラインで表示できます。ダッシュボードに表示したい情報に応じて、+ 記号をクリックしてグラフに列を追加できます。ユーザーログを CSV 形式でエクスポートできます。

Secure Private Access ログはどこで確認できますか?

1. Citrix Cloud にログオンします。
2. Secure Private Access サービスタイルで、**管理**をクリックします。
3. 管理者ユーザーインターフェイスの左側のナビゲーションで、**ダッシュボード**をクリックします。
4. **診断ログ**グラフで、**詳細を表示**リンクをクリックします。

Secure Private Access 診断ログを表示するウィジェットはどれですか?

ログとトラブルシューティングセクションの**診断ログ**ウィジェットは、認証、アプリケーション起動、アプリ列挙に関連するすべての Secure Private Access イベント、およびデバイスポスチャに関連するログの円グラフビューを表示します。Secure Private Access 診断ログは、エンドユーザーがアプリケーションにアクセスしたときにイベントを送信する複数の内部コンポーネントからイベントを取得します。これらのイベントは、**ログイン/ログオフ**、**アプリ列挙**、**アプリアクセス**のカテゴリに分類されます。円グラフは、各カテゴリの全体的な成功/失敗の比率を表示します。いずれかのグラフで色付きの円をクリックすると、適切なイベントを見つけることができる診断ログに移動します。デバイスポスチャサービスが有効になっている場合は、デバイスポスチャログも表示されます。**詳細を表示**リンクをクリックして、完全な診断ログを表示することもできます。

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

診断ログ (/en-us/citrix-secure-private-access/media/spa-troubleshoot-dashboard-diagnostics-logs-chart1.png)

詳細ビュー (/en-us/citrix-secure-private-access/media/spa-troubleshoot-dashboard-diagnostics-logs-chart2.png)

Secure Private Access診断ログにはどのような詳細情報がありますか?

Secure Private Accessユーザーログダッシュボードには、デフォルトで以下の詳細情報が表示されます。

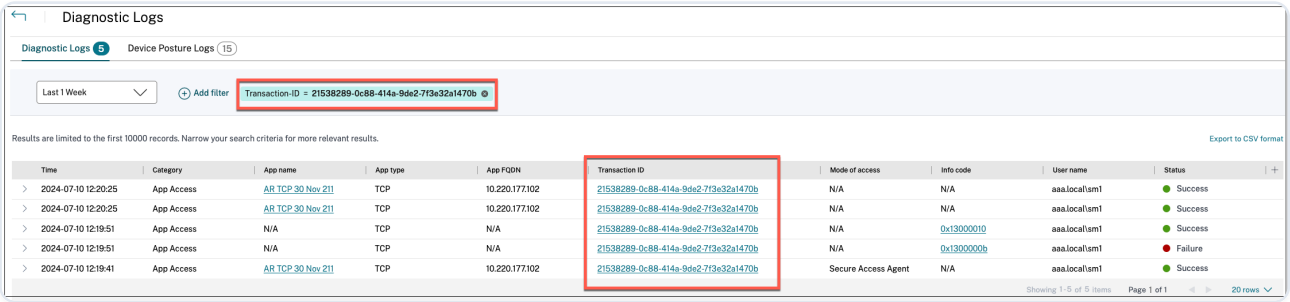
- **タイムスタンプ** - イベントのUTC時刻。
- **ユーザー名** - アプリにアクセスしているエンドユーザーのユーザー名。
- **アプリ名** - アクセスされたアプリの名前。
- **ポリシー情報** - イベント中にトリガーされたアクセスポリシーの名前。
- **ステータス** - イベントのステータス（成功または失敗）。
- **情報コード** - Secure Private Access診断ログダッシュボード内の各失敗イベントに関連付けられたコード。 情報コードの詳細はこちら。
- **説明** - 失敗の理由、またはイベントに関する詳細。
- **アプリFQDN**: アクセスされたアプリケーションのFQDN。
- **イベントタイプ** - 実行された操作に関連付けられたイベントタイプ。
- **操作タイプ** - ログが生成された操作。
- **カテゴリ** - イベントのタイプに応じて利用可能なカテゴリ。利用可能なオプションは、アプリ認証、アプリ列挙、アプリアクセスです。これらのオプションはフィルターオプションとしても利用できます。これらのオプションを使用して、直面している問題のタイプに応じてログをフィルターできます。
- **トランザクションID** - トランザクションIDは、アクセス要求のすべてのSecure Private Accessログを関連付けます。 トランザクションIDの使用方法を学ぶ。 ダッシュボードの右端にある+ボタンをクリックすると、以下の詳細情報を取得できます。
- **SPA PoPロケーション** - アプリアクセス中に使用されたSecure Private AccessサービスPoPロケーションの名前/ID。 Secure Private Access PoPロケーションを参照してください。

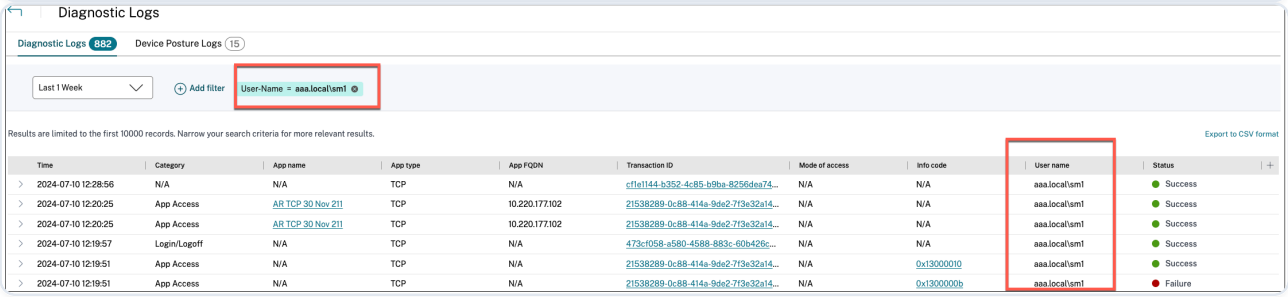
診断ログをフィルタリングするにはどうすればよいですか?

「**フィルターの追加**」オプションを使用して、アプリの種類、カテゴリ、説明など、さまざまな条件に基づいて検索を絞り込むことができます。たとえば、「**検索**」フィールドで、「**トランザクションID、= (特定の値と等しい)、および21538289-0c88-414a-9de2-7f3e32a1470bと入力**」をク

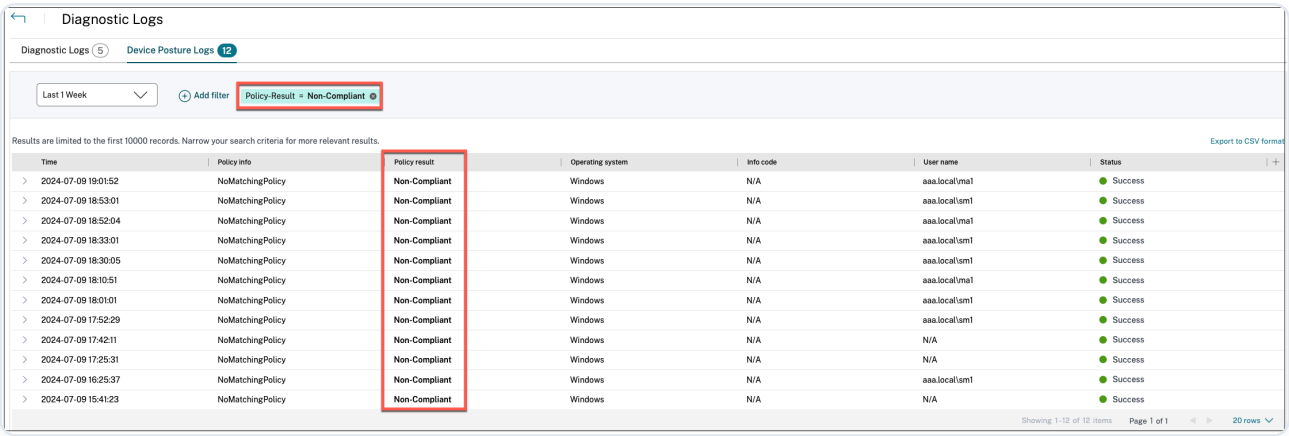
© 1997–2026 Citrix Systems, Inc. All rights reserved.

リックして、このトランザクションIDに関連するすべてのログを検索できます。フィルターオプションで使用できる検索演算子の詳細については、「検索演算子」を参照してください。





デバイスポスチャログの検索を絞り込むために、さまざまなフィルターオプションを使用することもできます。



Secure Private Access診断ログにはどのようなイベントが記録されますか?

Secure Private Access診断ログには、次のイベントが記録されます。

- **デバイスポスチャ:** エンドユーザーデバイスのステータス。これらのログには、デバイスポスチャの結果、つまり、デバイスポスチャポリシーに基づいてデバイスが準拠、非準拠、またはアクセス拒否と見なされたかどうかの情報が記録されます。
- **ログイン/ログオフ**: Citrix Secure Accessクライアントへのエンドユーザーのログオンまたはログオフステータス、およびストア（内部または外部プロバイダー）への認証に関連するイベント。
- **アプリの列挙**: Secure Private Accessサービスでは、管理者が構成したアクセスポリシーによって、どのユーザーがどのアプリにアクセスできるかが決定されます。拒否されたアプリ

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

ケーションは、Citrix Workspaceアプリ内でエンドユーザーには表示されません（列挙されません）。これらのイベントは、Secure Private Accessサービス内で構成されたアクセスポリシーに基づいて、どのアプリケーションがユーザーに許可または拒否されたかを知るのに役立ちます。

- **アプリへのアクセス**: 選択した時間間隔で構成されたアクセスポリシーに従った、エンドユーザーのアプリケーション/エンドポイントアクセス、許可/拒否ステータス、シングルサインオンステータス、および接続ステータスのイベント。

エラーのリスト

Secure Private Accessサービスの使用中にユーザーが遭遇する可能性のあるエラーの包括的なリストについては、「診断ログ情報コード」を参照してください。

診断ログ情報コード

アプリケーション構成、認証とSSO、またはアプリケーションアクセス関連の問題のトラブルシューティングには、このトピックを使用してください。Secure Private Access診断ログの「情報コード」列から情報コードをコピーし、このページでそのコードを検索して、対応するトラブルシューティング手順を見つけてください。このトピックをより効果的に使用するためのFAQを以下に示します。

診断ログの詳細については、診断ログを参照してください。

以下のエラー参照テーブルは、Secure Private Accessサービスの使用中にユーザーが遭遇する可能性のあるさまざまなエラーの包括的な概要を提供します。

情報コード	説明	解決策
0x180006, 0x1800B7	アプリケーションのFQDNの長さが超過したため、アプリケーションの起動に失敗しました	アプリケーションのFQDNの長さが超過したため、アプリケーションの起動に失敗しました
0x180022	認証サービスが停止しているため、アプリケーションの起動に失敗しました	認証サービスが停止しているため、アプリケーションの起動に失敗しました
0x180001, 0x18001A, 0x18001B, 0x18008A	シングルサインオンエラー、Citrix Cloudとオンプレミスコネクタ間の接続確立失敗、	「アプリへのアクセスが拒否されました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-

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

情報コード	説明	解決策
0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC	SAML SSO失敗、無効なアプリケーションFQDN	troubleshooting.html#app-access-is-denied)
0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0		
0x1800B1, 0x1800B2, 0x1800B3, 0x180048		
0x1800EF	コネクタアプライアンスへの接続に関する問題	「コネクタアプライアンスへの接続に関する問題」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#problem-connecting-to-connector-appliance)
0x18009D	DNSルックアップ/接続に失敗しました	「セキュアブラウザサービス - DNSルックアップ/接続エラー」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#secure-browser-service---dns-lookupconnection-failed)
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5	バックエンドWebアプリに接続できなかったため、Webアプリの起動に失敗しました	「バックエンドWebアプリに接続できなかったため、Webアプリの起動に失敗しました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#cwa-web---dns-lookupconnection-errors-for-web-apps)
0x1800A6, 0x1800A7		
0x1800BC, 0x1800BF	ユーザーはWeb/SaaSアプリへのアクセス権がありません	「ユーザーはWeb/SaaSアプリへのアクセス権がありません」(/ja-jp/citrix-secure-private-access/service/

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

情報コード	説明	解決策
		secure-private-access-troubleshooting.html#user-is-not-entitled-to-access-the-websaas-app)
0x1800BD	DirectAccessの場合、ユーザーはWeb/SaaSアプリへのアクセス権がありません	「DirectAccessの場合、ユーザーはWeb/SaaSアプリへのアクセス権がありません」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#user-is-not-entitled-to-access-the-websaas-app-for-directaccess)
0x1800D0	アプリケーション構成の取得中にCitrix Secure Accessエージェントセッションの起動に失敗しました	Citrix Secure Access エージェントのセッション起動が、アプリケーション構成の取得中に失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#citrix-secure-access-agent-session-launch-has-failed-while-fetching-the-application-configuration)
0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA	Citrix Secure Access エージェントのセッション起動が、アプリケーション構成の取得中に失敗しました, Citrix Secure Access エージェントのアプリ起動が、ポリシー評価中に失敗しました, Citrix Secure Access エージェントのアプリ起動が失敗しました	不正な形式のクライアント要求(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#tcpudp-apps---malformed-client-requests)

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

情報コード	説明	解決策
0x1800DE	Citrix Secure Access エージェントのアプリ起動が、ポリシー評価中に失敗しました	Citrix Secure Access エージェントのアプリ起動が、ポリシー評価中に失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#citrix-secure-access-agent-app-launch-has-failed-during-the-policy-evaluation)
0x180055, 0x1800DF, 0x1800E3	コンテキストポリシーによって制限されたアプリ, ポリシー構成によりアクセスが拒否されました	ユーザーダッシュボードに表示されていないアプリが1つ以上あります(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#one-or-more-apps-not-listed-in-the-user-dashboard)
0x1800EB	IPv6がサポートされていないため、Citrix Secure Access エージェントのアプリ起動が失敗しました	IPv6がサポートされていないため、Citrix Secure Access エージェントのアプリ起動が失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#citrix-secure-access-agent-app-launch-has-failed-as-ipv6-is-not-supported)
0x1800EC, 0x1800ED	無効なIPアドレスのため、Citrix Secure Access エージェントのアプリ起動が失敗しました	Citrix Secure Access エージェントアプリの起動は、無効なIPアドレスが原因で失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#citrix-

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

情報コード	説明	解決策
		secure-access-agent-app-launch-has-failed-due-to-invalid-ip-address)
0x10000001, 0x10000002, 0x10000003, 0x10000004	ネットワークの問題によりCitrix Secure Accessクライアントのログインに失敗しました	Citrix Secure Accessクライアントとのネットワーク接続到達性の問題(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#network-connectivity-reachability-issue-with-citrix-secure-access-client)
0x10000006	中間プロキシが原因でCitrix Secure Accessクライアントのログインに失敗しました	プロキシサーバーがサービスとのクライアント接続を妨害しています(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#proxy-server-interfering-client-connectivity-with-service)
0x10000007	信頼されていない認証局が原因でCitrix Secure Accessクライアントのログインに失敗しました	信頼されていないサーバー証明書の問題が確認されました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#untrusted-server-certificate-issue-is-observed)
0x10000008	無効な証明書が原因でCitrix Secure Accessクライアントのログインに失敗しました	無効なサーバー証明書の問題が確認されました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#invalid-

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

情報コード	説明	解決策
		server-certificate-issue-is-observed)
0x1000000A	構成の問題によりCitrix Secure Accessクライアントのログインに失敗しました	ユーザーの構成が空のため、ログインに失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#login-failed-as-configuration-is-empty-for-the-user)
0x1000000B	接続障害によるCitrix Secure Accessクライアントのログイン失敗	ネットワークまたはエンドユーザーによって接続が終了されました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#connection-terminated-by-the-network-and-or-end-user)
0x10000010	セッションの有効期限切れによるCitrix Secure Accessクライアントのログイン失敗	セッションの有効期限が切れているため、構成のダウンロードに失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#configuration-download-failed-as-session-is-expired)
0x10000013	構成リストが大きすぎるため、Citrix Secure Accessクライアントのログインに失敗しました	Citrix Secure Accessクライアントのログインに失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#citrix-secure-access-client-failed-to-log-in)

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

情報コード	説明	解決策
0x11000003	コントロールチャネルの作成失敗によるCitrix Secure Accessクライアントのログイン失敗	セッションの有効期限が切れたため、コントロールチャネルの確立に失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#control-channel-establishment-failed-as-the-session-expired)
0x11000004	コントロールチャネルの作成失敗によるCitrix Secure Accessクライアントのログイン失敗	「コントロールチャネルの確立に失敗しました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#control-channel-establishment-failed)
0x11000005	コントロールチャネル作成の失敗によるCitrix Secure Accessクライアントのログイン失敗	「コントロールチャネルの確立に失敗しました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#control-channel-establishment-failed-1)
0x11000006	コントロールチャネル作成の失敗によるCitrix Secure Accessクライアントのログイン失敗	「ネットワークの問題によりコントロールチャネルの確立に失敗しました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#control-channel-establishment-failed-due-to-network-issue)
0x12000001	セッションがすでに期限切れのため、Citrix Secure Accessクライアントのログアウトに失敗しました	「セッションが終了したためログオフできません」(/ja-jp/citrix-secure-private-access/service/secure-private-

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

情報コード	説明	解決策
		access-troubleshooting.html#unable-to-logoff-as-session-is-terminated)
0x12000002	セッションがすでにタイムアウトしたため、Citrix Secure Accessクライアントのログアウトに失敗しました	「セッションが強制的に終了されました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#session-is-forcefully-terminated)
0x13000001	セッションが期限切れになったため、アプリへのアクセスに失敗しました	セッションの有効期限が切れたため、アプリケーションの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-as-session-is-expired)
0x13000002	ライセンスが不十分なため、アプリへのアクセスに失敗しました。	ライセンスの問題により、アプリケーションの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-because-of-license-issue)
0x13000003, 0x13000008, 0x001800DF	アクセスが禁止されているため、アプリへのアクセスに失敗しました。ポリシーによりTCP/UDPアプリの起動が拒否されました。	サービスによってアクセスが拒否されたため、アプリケーションの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#applicati

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

情報コード	説明	解決策
		on-launch-failed-as-access-is-denied-by-service)
0x13000004, 0x13000005	サーバーが利用できないため、アプリへのアクセスに失敗しました。	クライアントがサービスに到達できないため、アプリケーションの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-as-the-client-is-unable-to-reach-the-service)
0x13000007	アクセス ポリシーが無効になっているか、ユーザーがサブスクライブされていないため、アプリへのアクセスに失敗しました。	ポリシー評価と構成検証に失敗したため、アプリケーションの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-as-policy-evaluation-and-config-validation-failed)
0x13000009	ルーティングエントリが見つからないため、アプリへのアクセスに失敗しました。	アプリケーションドメインテーブルの問題により、アプリケーションの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-because-of-issues-in-application-domain-table)
0x1300000B	クライアントが接続を閉じました	クライアントがSecure Private Accessサービスとの接続を閉じました。(/ja-jp/citrix-secure-private-access/service/secure-private-

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

情報コード	説明	解決策
		access-troubleshooting.html#client-closed-the-connection-with-secure-private-access-service)
0x1300000C	ZTNA経由のFQDN解決に失敗しました	DNSサーバーによるFQDNの解決ができません。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#unable-to-resolve-fqdn-by-the-dns-server)
0x1300000E	Chrome以外のブラウザを使用したため、アプリの起動に失敗しました	Chrome以外のブラウザを使用したため、アプリの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#app-launch-failed-due-to-use-of-non-chrome-browser)
0x001800D3	ログイン中にアプリケーション構成のダウンロードに失敗しました	構成されたアプリケーション宛先リストの取得に失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#failed-to-fetch-configured-application-destinations-list)
0x001800D9, 0x001800DA	ポリシー評価応答の解析中にTCP/UDPアプリの起動に失敗しました。ポリシー評価中に無効な結果でTCP/UDPアプリの起動に失敗しました	アプリケーション構成の問題

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

情報コード	説明	解決策
0x001800DB	TCP/UDPアプリの起動が、無効なリソースロケーション構成のため失敗しました	リソースロケーションの問題
0x13000006, 0x001800DC, 0x001800DD	TCPアプリの起動が、アプリに構成されているサポートされていない拡張セキュリティポリシーのため失敗しました。TCPアプリの起動が、TCPアプリに構成されているサポートされていないセキュアブラウザサービスのリダイレクトのため失敗しました	拡張セキュリティポリシーがHTTPアプリケーションにバインドされています
0x001800DE	TCP/UDPアプリの起動が、宛先に対してアプリケーション構成が見つからないため失敗しました	アプリケーションを見つけられません
0x001800EA	TCPアプリの起動が、宛先FQDNが長すぎるため失敗しました	ホスト名の長さが256文字を超えています
0x001800ED	TCPアプリの起動が、無効な宛先IPのため失敗しました	無効なIPアドレス
0x001800EF	プライベートTCPサーバーへの接続確立中にTCPアプリの起動に失敗しました	エンドツーエンド接続を確立できません
0x001800F5	IPv6アドレスが原因でUDPアプリの起動に失敗しました	アプリのリクエストでIPv6を受信しました
0x001800F9	クライアント接続が失われたため、UDPトラフィックの配信に失敗しました	UDPトラフィックの配信に失敗しました
0x001800FF	UDPデータトラフィックの配信に失敗しました	UDPデータトラフィックの配信に失敗しました

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

情報コード	説明	解決策
0x10000401	Citrix Rendezvousサーバーのダイヤルに失敗しました	ネットワーク接続の問題によりアプリケーションの起動に失敗しました。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#application-launch-failed-due-to-network-connectivity-issues)
0x10000402, 0x1000040C	コネクタアプライアンスを登録できません、UDPネットワーク接続の初期化に失敗しました	コネクタアプライアンスがSecure Private Accessサービスに登録できませんでした。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#connector-appliance-failed-to-register-to-secure-private-access-service)
0x10000403, 0x10000404, 0x10000407, 0x1000040A 0x1000040B, 0x1000040F, 0x10000410	接続エラー、制御パケット送信失敗、ゲートウェイサービスの読み取りエラー、制御パケット解析失敗、ゲートウェイサービスの書き込みエラー	コネクタアプライアンスとの接続の問題(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#connectivity-issue-with-connector-appliance)
0x10000405, 0x10000408, 0x10000409, 0x1000040D 0x1000040E, 0x10000412	バックエンドに到達できません、UDPパケット送信失敗、UDPパケット受信失敗、バックエンドへの書き込みエラー、バックエンドが接続を閉じました	コネクタアプライアンスおよびバックエンドのプライベートTCP/UDPサーバーとの接続の問題(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#connectivity-issues-with-connector-appliance-and-back-end-private-tcpudp-servers)

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

情報コード	説明	解決策
0x10000406	DNS解決に失敗しました	コネクタアプライアンスがFQDNのDNSを解決できません
0x10000411	ゲートウェイサービスが接続を閉じました	プライベートサーバーへの接続が終了しました
0x10000413	接続切断の理由を特定する際にエラーが発生しました	プライベートサービスIPまたはFQDNへの接続またはデータ送信に失敗しました
0x100508	ユーザーコンテキストがアクセスルール条件と一致しません	一致するポリシー条件がありません
0x100509	アクセスポリシーがアプリケーションに関連付けられていません	アプリケーションに関連付けられているアクセスポリシーがありません。(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#no-access-policy-associated-with-the-application)
0x10050C	ユーザーが利用できる可能性のある複数のアプリケーションのポリシー評価結果	アプリケーション列挙情報(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#app-enumeration-information)
0x00180101	アプリケーションドメインテーブルにルーティングエントリがないため、TCP/UDPアプリの起動に失敗しました	アプリケーションドメインテーブルにルーティングエントリがないため、TCP/UDPアプリの起動に失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#tcp-udp-app-launch-failed-as-routing-

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

情報コード	説明	解決策
		entry-is-missing-in-application-domain-table)
0x00180102	コネクタが正常でないため、TCP/UDPアプリの起動に失敗しました	コネクタが正常でないため、TCP/UDPアプリの起動に失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#tcpudp-app-launch-failed-as-connectors-are-not-healthy)
0x00180103	コネクタに到達できないため、UDP/DNSリクエストに失敗しました	コネクタに到達できないため、UDP/DNSリクエストに失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#udpdns-request-failed-as-connector-is-unreachable)
0x20580001	NGS Cookieの有効期限が切れているため、ページの読み込みに失敗しました	「NGS Cookie の有効期限が切れたため、ページを読み込めませんでした」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#failed-to-load-the-page-as-the-ngs-cookie-is-expired)
0x20580002	ネットワーク障害のため、アクセスポリシーの取得に失敗しました	「ネットワーク障害のため、アクセスポリシーの取得に失敗しました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#access-

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

情報コード	説明	解決策
		policy-fetch-failed-because-of-a-network-failure)
0x20580003	JSON Web トークンの解析中にアクセスポリシーの取得に失敗しました	「JSON Web トークンの解析中にアクセスポリシーの取得に失敗しました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#access-policy-fetch-failed-while-parsing-the-json-web-token)
0x20580004	アクセスポリシーの詳細を取得するためのネットワーク障害	「アクセスポリシーの詳細を取得するためのネットワーク障害」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#network-failure-to-fetch-access-policy-details)
0x20580005	公開証明書の取得中にポリシーの取得に失敗しました	「公開証明書の取得中にポリシーの取得に失敗しました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#policy-fetch-failed-while-fetching-the-public-certificate)
0x20580007	JWT の署名を検証中にポリシーの取得に失敗しました	JWTの署名を検証中にポリシーの取得に失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#policy-fetch-failed-while-validating-signature-of-the-json-web-token)

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

情報コード	説明	解決策
0x20580008	公開証明書の検証中にポリシーの取得に失敗しました	公開証明書の検証中にポリシーの取得に失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#policy-fetch-failed-while-validating-the-public-certificate)
0x2058000A	ポリシーURLを形成するためのストア環境の特定に失敗しました	ポリシーURLを形成するためのストア環境の特定に失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#failed-to-determine-the-store-environment-to-form-a-policy-url)
0x2058000B	アクセスポリシー取得リクエストの応答の取得に失敗しました	アクセスポリシー取得リクエストの応答の取得に失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#failed-to-get-a-response-for-access-policy-fetch-request)
0x2058000C	期限切れのセカンダリDS認証トークンが原因でアクセスポリシーの取得に失敗しました	期限切れのセカンダリDS認証トークンが原因でアクセスポリシーの取得に失敗しました(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#access-policy-fetch-failed-due-to-an-expired-secondary-ds-auth-token)
0x10200002	コネクタアプライアンスが登録されていません	コネクタアプライアンスが登録されていません

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

情報コード	説明	解決策
0x10200003	コネクタアプライアンスに接続できません	コネクタアプライアンスに接続できません
0x10000301	Citrix SPAサービスへの接続に失敗しました	Citrix Secure Private Access サービスへの接続に失敗しました
0x10000303, 0x10000304	プロキシサーバーに到達できません	プロキシサーバーに到達できません
0x10000305	プロキシサーバー認証に失敗しました	プロキシサーバー認証に失敗しました
0x10000306	構成されたプロキシサーバーに到達できません	設定されたプロキシサーバーに到達できません
0x10000307	バックエンドサーバーからエラー応答を受信しました	バックエンドサーバーからエラー応答を受信しました
0x10000005	ターゲットURLにリクエストを送信できません	ターゲットURLにリクエストを送信できません
0x10000107	SSOの処理に失敗しました	SSOの処理に失敗しました
0x10000108, 0x1000010B	SSOの処理に失敗しました。SSO設定を特定できません。	SSOの処理に失敗しました。SSO設定を特定できません。
0x10000101, 0x10000102, 0x10000103, 0x10000104	FormFill SSOに失敗しました。フォームアプリの設定が正しくありません。	「フォーム入力SSOに失敗しました。フォームアプリの設定が正しくありません。」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#formfill-sso-failed-incorrect-form-app-configuration)
0x1000010A	フォーム入力SSOに失敗しました。フォームアプリの設定が正しくありません。	「フォーム入力SSOに失敗しました。フォームアプリの設定が正しくありません。」(/ja-jp/citrix-secure-private-access/service/secure-

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

情報コード	説明	解決策
		private-access-troubleshooting.html#formfill-sso-failed-incorrect-form-app-configuration)
0x10000202	Kerberos SSOに失敗しました	「Kerberos SSOに失敗しました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#kerberos-sso-failed)
0x10000203	認証タイプに対するSSOの処理に失敗しました	「認証タイプに対するSSOの処理に失敗しました」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#failed-to-process-sso-for-auth-type)
0x10000204	Kerberos SSOに失敗しましたが、NTLMにフォールバックしています	「Kerberos SSOに失敗しましたが、NTLMにフォールバックしています」(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#kerberos-sso-failed-but-falling-back-to-ntlm)
0x14000001	Citrix Workspaceアプリケーションで複数のZTNAエンタイトルメントアカウントが構成されています	Citrix Workspaceアプリケーションで複数のZTNAエンタイトルメントアカウントが構成されています(/ja-jp/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#multiple-ztna-entitled-accounts-configured-in-citrix-workspace-application)

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

解決手順

以下のセクションでは、ほとんどの情報コードに対する解決手順を説明します。解決手順が記載されていないコードについては、Citrixサポートにお問い合わせください。

ユーザーダッシュボードに表示されないアプリが1つ以上ある

情報コード: 0x180055, 0x1800DF, 0x1800E3

コンテキストポリシー設定により、一部のユーザーまたはデバイスでアプリが表示されない場合があります。信頼要素（デバイスの姿勢やリスクスコアなど）のようなパラメータは、アプリケーションのアクセシビリティに影響を与える可能性があります。

1. 診断ログCSVファイルの、エラーコード `0x18005C` の `reasons` 列からトランザクションIDをコピーします。
2. CSVファイルの `prod` 列フィルターを修正し、 `SWA.PSE` または `SWA.PSE.EVENTS` というコンポーネントからのイベントを表示するようにします。このフィルターは、ポリシー評価に関連するログのみを表示します。
3. `reason` 列で評価されたポリシーペイロードを検索します。このペイロードは、ユーザーがサブスクライブしているすべてのアプリについて、ユーザーのコンテキストで評価されたポリシーを示します。
4. ポリシー評価でユーザーのアプリが拒否されたと示された場合、考えられる理由は次のとおりです。
   - ポリシー内の照合条件が正しくない - Citrix Cloud™でアプリポリシー構成を確認してください
   - ポリシー内の照合ルールが正しくない - Citrix Cloudでアプリポリシー構成を確認してください
   - ポリシー内の照合デフォルトルールが正しくない - これはフォールスルーケースです。条件を適切に調整してください。

ユーザーはWeb/SaaSアプリにアクセスする権限がありません

情報コード: 0x1800BC, 0x1800BF

ユーザーは、サブスクリプションを持っていない可能性のあるアプリリンクをクリックした可能性があります。

ユーザーがアプリケーションのサブスクリプションを持っていることを確認してください。

1. 管理ポータルでアプリケーションに移動します。

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

2. アプリを編集し、**サブスクリプション**タブに移動します。
3. 対象ユーザーがサブスクリプションリストに登録されていることを確認してください。

バックエンドアプリのパフォーマンスが遅い

情報コード:0x18000F

リソースロケーション内のコネクタがダウンしている、またはバックエンドサーバー自体が応答していないために、顧客ネットワークが不安定になる場合があります。

1. ネットワーク遅延を排除するために、コネクタアプライアンスがバックエンドサーバーの地理的に近い場所に配置されていることを確認してください。
2. バックエンドサーバーのファイアウォールがコネクタアプライアンスをブロックしていないか確認してください。
3. クライアントが最寄りのクラウドPOPに接続しているか確認してください。

   例えば、クライアント上の`nslookup nssvc.dnsdiag.net`では、応答の正規名が`aws-us-w.g.nssvc.net.`のような地理固有のサーバーを示します。

アプリケーションFQDNの長さが超過したため、アプリの起動に失敗しました

情報コード: 0x180006, 0x1800B7

アプリケーションFQDNは512文字を超えてはなりません。アプリ構成ページでアプリケーションFQDNを確認してください。長さが512バイトを超えないことを確認してください。

1. 管理コンソールの**アプリケーション**タブに移動します。
2. FQDNが512文字を超えるアプリケーションを探します。
3. アプリケーションを編集し、アプリのFQDNの長さを修正します。

アプリの詳細の長さが超過しました

情報コード: 0x18000E

ポリシーがアプリへのアクセスをブロックしていないか確認します。

1. **アクセスポリシー**に移動します。
2. アプリにエンタイトルメントがあるポリシーを探します。
3. エンドユーザー向けのポリシー規則と条件を確認します。

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

アプリへのアクセスが拒否されました

情報コード: 0x180001, 0x18001A, 0x18001B, 0x18008A, 0x1800A9, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3, 0x180048

これは、特定のユーザーに対してポリシーがアプリを拒否しているコンテキストポリシーに関連しています。

ポリシーがアプリへのアクセスをブロックしていないか確認します

1. **アクセスポリシー**に移動します。
2. アプリにエンタイトルメントがあるポリシーを探します。
3. エンドユーザーのポリシー規則と条件を確認します。

列挙されていないアプリケーション

アプリケーションが列挙されたリストに表示されないのは、ポリシー拒否が原因であるか、Secure Private Access統合が有効になっていないためです。

- 一部のアプリへのアクセスを有効にする必要があるにもかかわらず、アプリが1つも表示されない場合は、Secure Private Access統合を有効にしてみてください。
  - Citrix Cloudにサインインします。
  - ハンバーガーメニューから**StoreFront Cloud**を選択し、**Service Integrations**をクリックします。
  - Secure Private Accessの省略記号ボタンをクリックし、**Enable**をクリックします。
- Secure Private Access統合がすでに有効になっている場合は、一度無効にしてから再度有効にし、アプリが表示されるか確認します。

Connector Applianceへの接続の問題

情報コード: 0x1800EF

オンプレミスコネクタとのTCP接続が利用できないため、アプリのルーティングに失敗します。

コントローラコンポーネントからのイベントを確認する

1. 診断ログCSVファイルで、エラーコード `0x1800EF` の `transaction ID` を検索します。
2. CSVファイル内のトランザクションIDに一致するすべてのイベントをフィルタリングします。
3. また、CSVファイル内で `SWA.GOCTRL` に一致する `prod` 列をフィルタリングします。

   `connectType` メッセージ `multiconnect::success` のイベントが表示された場合、その場合、;

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

- これは、トンネル確立要求がコントローラーに正常に中継されたことを示します。
- ログメッセージ内の `Resource Location` が正しいか確認してください。正しくない場合は、Citrix管理ポータル上のアプリ構成セクションでリソースの場所を修正してください。
- ログメッセージ内の `VDA Ip and Port` が正しいか確認してください。VDA IPとポートは、バックエンドアプリケーションのIPとポートを示します。正しくない場合は、Citrix管理ポータル上のアプリ構成セクションでアプリのFQDNまたはIPアドレスを修正してください。
- 以前に述べた問題が見つからない場合は、コネクタイベントを確認してください。

`connectType` メッセージ `connect::failure` または `multiconnect::success` のイベントが表示された場合、その場合、;

- このログメッセージに対する推奨される修正が `Check if connector is still connected to same pop` と記載されているか確認してください。これは、リソースロケーションのコネクタがダウンした可能性があることを示します。コネクタイベントを確認してください。
- 以前に述べたメッセージが表示されない場合は、Citrixカスタマーサポートに連絡してください。

`connectType` メッセージ `IntraAll::failure` のイベントが表示された場合は、Citrixカスタマーサポートに連絡してください。

コネクタコンポーネントからのイベントを確認する

1. 診断ログCSVファイルで、エラーコード `0x1800EF` について `transaction ID` を調べてください。
2. CSVファイル内のトランザクションIDに一致するすべてのイベントをフィルタリングしてください。
3. また、CSVファイル内の `prod` 列で `SWA.ConnectorAppliance.WebApps` に一致するものをフィルタリングしてください。
4. `status` が `failure` であるイベントが表示された場合、その場合、;
   - これらの失敗イベントのそれぞれについて、 `reason` メッセージを確認してください。
   - `UnableToRegister` は、コネクタがCitrix Cloudに正常に登録できなかったことを示します。Citrixサポートにお問い合わせください。
   - `IsProxyRequiredCheckError` または `ProxyDialFailed` または `ProxyConnectionFailed` または `ProxyAuthenticationFailure` または

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

`ProxiesUnReachable` は、コネクタがプロキシ構成を介してバックエンドURLを解決できなかったことを示します。プロキシ構成が正しいことを確認してください。

- さらなるデバッグについては、コネクタSSOイベントを参照してください。

シングルサインオンエラー

シングルサインオンの場合、アプリ構成から異なるSSO属性が抽出され、アプリ起動時に適用されます。特定のユーザーが属性を持っていない場合、または属性が正しくない場合、シングルサインオンは失敗する可能性があります。構成が正しいことを確認してください。

1. **アクセスポリシー**に移動します。
2. アプリにエンタイトルメントがあるポリシーを探します。
3. エンドユーザーのポリシー規則と条件を確認します。

フォームSSO、Kerberos、NTLMなどのSSOメソッドは、オンプレミスコネクタによって実行されます。コネクタからの以下の診断ログを確認してください。

コネクタコンポーネントからのSSOイベントを確認する

1. `SWA.ConnectorAppliance.WebApps` に一致するcsvファイル内の `component name` をフィルタリングします。
2. ステータスが「failure」のイベントが表示されますか？

   - これらの失敗イベントそれぞれのメッセージを確認します。
   - `IsProxyRequiredCheckError` または `ProxyDialFailed` または `ProxyConnectionFailed` または `ProxyAuthenticationFailure` または `ProxiesUnReachable` は、コネクタがプロキシ構成を介してバックエンドURLを解決できなかったことを示します。プロキシ構成が正しいことを確認してください。
   - `FailedToReadRequest` または `RequestReceivedForNonSecureBrowse` または `UnableToRetrieveUserCredentials` または `CCSPolicyIsNotLoaded` または `FailedToLoadBaseClient` または `ProcessConnectionFailure` または `WebAppUnSupportedAuthType` は、トンネリングの失敗を示します。Citrixサポートにお問い合わせください。
   - `UnableToConnectTargetServer` は、コネクタからバックエンドサーバーに到達できないことを示します。バックエンド構成を再度確認してください。
   - `IncorrectFormAppConfiguration` または `NoLoginFormFound` または `FailedToConstructForLoginActionURL` または `FailedToLoginViaFormBasedAuth` は、フォームベースの認証失敗を示します。Citrix 管理ポータルの「アプリ構成」にある「フォーム SSO 構成」セクションを確認してください。

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

- `NTLMAuthNotFound` は、NTLM ベースの認証失敗を示します。Citrix 管理ポータルのアプリ構成にある「NTLM SSO 構成」セクションを確認してください。
- さらなるデバッグについては、「コネクタイベント」(#review-events-from-the-connector-component) を参照してください。

認証サービスがダウンしているため、アプリの起動に失敗しました

情報コード: 0x180022

Secure Private Access を使用すると、管理者は従来の Active Directory、AAD、Okta、SAML などのサードパーティ認証サービスを構成できます。これらの認証サービスの停止がこの問題を引き起こす可能性があります。

サードパーティサーバーが稼働しており、到達可能であることを確認してください。

SAML SSO の失敗

情報コード: 0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3

IdP 開始の場合、ユーザーはアプリ起動時に認証失敗に直面するか、SP 開始の場合、アクセスできないリンクが表示されることがあります。Secure Private Access サービス側の SAML アプリ構成とサービスプロバイダー構成も確認してください。

セキュア プライベート アクセス の構成:

1. **アプリケーション**タブに移動します。
2. 問題のある SAML アプリを探します。
3. アプリケーションを編集し、**シングルサインオン**タブに移動します。
4. 以下のフィールドを確認してください。
   - アサーションURL
   - リレーステート
   - オーディエンス
   - 名前ID形式、名前ID、およびその他の属性

サービスプロバイダーの構成:

1. サービスプロバイダーにログインします。
2. **SAML設定**に移動します。
3. IdP証明書、オーディエンス、およびIdPログインURLを確認します。

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

構成が正しいように見える場合は、Citrixサポートにお問い合わせください。

無効なアプリFQDN

情報コード: 0x180048

顧客管理者が無効なFQDN、またはバックエンドサーバーでDNS解決が失敗するFQDNを提供した可能性があります。

この場合、エンドユーザーはウェブページにエラーが表示されます。アプリケーション設定を確認してください。

SAASアプリの検証

アプリがネットワークからアクセスできるか確認します。

WEBアプリの検証

1. **アプリケーション**タブに移動します。
2. 問題のあるアプリケーションを編集します。
3. **アプリの詳細**ページに移動します。
4. URLを確認します。URLはイントラネットまたはインターネットのいずれかでアクセス可能である必要があります。

セキュアブラウザサービス - DNSルックアップ/接続失敗

情報コード: 0x18009D

Remote Browser Isolationサービスを介したブラウジングエクスペリエンスが破損しています。エンドユーザーが接続しようとしているバックエンドサーバーを確認してください。

1. バックエンドサーバーに移動し、それが稼働しており、リクエストを受信できることを確認します。
2. プロキシ設定がバックエンドサーバーへの接続を妨げている場合は、それを確認します。

> **注:**
>
> Citrix Remote Browser Isolation™サービスは、以前はSecure Browserサービスとして知られていました。

CWA Web - WebアプリのDNSルックアップ/接続エラー

情報コード: 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7

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

企業ネットワーク内で実行されているWebアプリケーションのブラウジングエクスペリエンスの破損。

1. 解決できないFQDNについて診断ログをフィルタリングします。
2. 企業ネットワーク内からバックエンドサーバーへの到達可能性を確認します。
3. コネクタがバックエンドサーバーへの到達をブロックされていないか、プロキシ設定を確認します。

ダイレクトアクセス - Webアプリとして誤設定されている

Webアプリのトラフィックは常にコネクタ経由でルーティングされるため、それらでダイレクトアクセスを設定すると、アプリのアクセスエラーが発生します。

ルーティングドメインテーブルとアプリ構成の間で競合する設定を確認します。

1. 管理ポータルでアプリケーションに移動します。
2. アプリを編集し、ダイレクトアクセスが有効になっているか確認します。
3. ルーティングドメインテーブル内のアプリのFQDNが内部としてマークされているか確認します。

ユーザーはDirectAccess用のWeb/SaaSアプリにアクセスする権限がありません

情報コード: 0x1800BD

アプリ構成により、ブラウザベースのクライアントから発信されるトラフィックに対してダイレクトアクセスが無効になっています。

ユーザーがアプリケーションへのサブスクリプションを持っていることを確認します。

1. 管理ポータルでアプリケーションに移動します。
2. アプリを編集し、エージェントレスアクセス構成を確認します。

強化されたセキュリティポリシー - Secure Browser Serviceの構成ミス

情報コード: 0x1800C3

ポリシールールで意図されたものとは異なる動作が見られます。コンテキストアクセスポリシーを確認してください。

1. **ポリシー**タブに移動します。
2. アプリケーションに関連付けられているポリシーを確認します。
3. それらのポリシーのルールを確認します。

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

強化されたセキュリティポリシー - ポリシーの構成ミス

ポリシールールで意図されたものとは異なる動作が見られます。強化されたセキュリティ設定を確認してください。

1. アプリケーションに移動します。
2. **アクセスポリシー**タブをクリックします。
3. **利用可能なセキュリティ制限:** セクションの設定を確認します。

アプリケーション構成の取得中にCitrix Secure Access™エージェントセッションの起動に失敗しました

情報コード: 0x1800D0

Citrix Secure AccessアプリがCitrix Cloudへのフルトンネルを正常に確立できません。

1. TCP/UDPアプリのルーティングドメイン構成を確認します。
2. エントリの最大数が16kの制限内に十分収まっていることを確認します。

TCP/UDPアプリ - 不正な形式のクライアント要求

情報コード: 0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA

VPNトンネルが確立されていないか、特定のFQDNがトンネル化されていない可能性があります。

1. 要求が中間プロキシによって偽造または再構築されていないことを確認します。
2. 中間者攻撃の疑い。

TCP/UDPアプリ - Secure Browser Serviceリダイレクトの構成ミス

情報コード: 0x1800DD

Remote Browser Isolationサービスのリダイレクトは、Webアプリにのみ適用でき、TCP/UDPアプリには適用できません。Secure Private AccessサービスGUIでアプリの構成を確認してください。

> **注:**
>
> Citrix Remote Browser Isolationサービスは、以前はSecure Browserサービスとして知られていました。

ポリシー評価中にCitrix Secure Accessエージェントアプリの起動に失敗しました

情報コード: 0x1800DE

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

Citrix Secure Accessクライアントによってトンネル化されるすべての内部FQDNが、ルーティングドメインテーブルに対応するエントリを持っていることを確認します。

Citrix Secure Access エージェントアプリの起動に失敗しました。IPv6はサポートされていません

情報コード: 0x1800EB

ルーティングドメインのエントリを確認してください。テーブルにIPv6エントリがないことを確認してください。

Citrix Secure Access エージェントアプリの起動に失敗しました。IPアドレスが無効です

情報コード:0x1800EC, 0x1800ED

ルーティングドメインのエントリを確認してください。IPアドレスが有効であり、正しいバックエンドを指していることを確認してください。

Citrix Secure Access クライアントとのネットワーク接続到達性の問題

情報コード: 0x10000001, 0x10000002, 0x10000003, 0x10000004

1. クライアントマシンのネットワークに到達可能か確認してください。ネットワークに到達可能な場合は、クライアントのデバッグログを添えてCitrixサポートにお問い合わせください。
2. プロキシまたはファイアウォールがネットワークをブロックしていないか確認してください。

クライアントのデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

プロキシサーバーがサービスとのクライアント接続を妨害している

情報コード: 0x10000006

1. クライアントマシンのネットワークに到達可能か確認してください。
2. クライアントでプロキシが正しく構成されているか確認してください。
3. 両方に問題がない場合は、クライアントデバッグログを添えてCitrixサポートにお問い合わせください。

クライアントデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

信頼されていないサーバー証明書の問題が確認されました

情報コード: 0x10000007

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

サーバー証明書が有効なCAによって正しく生成されているかどうかを確認するには、Citrixサポートにお問い合わせください。

無効なサーバー証明書の問題が確認されました

情報コード: 0x10000008

サーバー証明書が自己署名されているか、期限切れであるか、または信頼できないソースからのものであるかを確認するには、Citrixサポートにお問い合わせください。

ユーザーの構成が空であるため、ログインに失敗しました

情報コード: 0x1000000A

1. 少なくとも1つのTCP/UDP/HTTPアプリが構成されていることを確認してください。詳細については、「アプリケーションの追加と管理」を参照してください。
2. アプリケーションドメインテーブル (**Secure Private Access > Settings > Application Domain**) が空でないこと、またはすべてのエントリが無効になっていないことを確認してください。TCP/UDP/HTTPアプリケーションで構成された宛先は、このテーブルに自動的に追加されます。

アクティブなTCP/UDP/HTTPアプリケーションの宛先またはURLを削除したり無効にしたりしないことをお勧めします。

ネットワークまたはエンドユーザーによって接続が終了されました

情報コード: 0x1000000B

ネットワークが中断されているか、ZTNAセッション接続中にエンドユーザーが接続をキャンセルしたかを確認します。

セッションの有効期限が切れたため、構成のダウンロードに失敗しました

情報コード: 0x10000010

ZTNAセッション構成のダウンロード要求中にVPNセッションの有効期限が切れた可能性があります。Citrix Secure Accessクライアントに再ログインしてみてください。

Citrix Secure Accessクライアントのログインに失敗しました

情報コード: 0x10000013

構成サイズが最大構成制限を超えているため、Citrix Secure Accessクライアントのログインに失敗しました。

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

1. TCP/UDPアプリのルーティングドメイン構成を**Secure Private Access > 設定 > アプリケーションドメイン**で確認します。
2. エントリの数が膨大でないことを確認してください。エントリリストが膨大な場合は、未使用の宛先を無効にするか削除してください。

   宛先リストが1000を超えることが予想される場合は、ConfigSizeレジストリキーを更新して、最大構成ダウンロードサイズを増やしてみてください。詳細については、「Citrix Gateway VPNクライアントレジストリキー」を参照してください。

セッションの有効期限が切れたため、コントロールチャネルの確立に失敗しました

情報コード: 0x11000003

セッションの有効期限が切れたため、DNS要求確立のコントロールチャネルに失敗しました。

コントロールチャネルの設定中にZTNAセッションの有効期限が切れた可能性があります。

Citrix Secure Accessクライアントに再ログインしてみてください。

コントロールチャネルの確立に失敗しました

情報コード: 0x11000004

DNS要求確立のためのコントロールチャネルが失敗しました。

- **リソースの場所を正常に維持する:**

1. Citrix Cloudにログオンします。
2. ハンバーガーメニューから をクリックします。
3. 該当するリソースの場所にあるコネクタアプライアンスのヘルスチェックを実行します。
4. これで問題が解決しない場合は、コネクタ仮想マシンの再起動を試してください。

- **HAコネクタアプライアンスを維持する:**

1. Citrix Cloudにログオンします。
2. ハンバーガーメニューから をクリックします。
3. 予期されるリソースの場所に少なくとも2つのコネクタアプライアンスがあることを確認します。

以下を確認してください。

- リソースの場所のLANが正常に機能していること。

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

- コネクタアプライアンスからサービスまたはバックエンドサーバーへの接続をブロックするファイアウォールまたはプロキシが途中にないこと。
- クライアントネットワークは正常です。
- バックエンドのプライベートサーバーは稼働しています。
- DNSサーバーは稼働しています。
- FQDNは解決可能です。

上記の推奨事項を満たしている場合は、次の手順を実行します。

1. このエラーの診断ログからトランザクションIDを取得します。
2. Secure Private Accessダッシュボードで、トランザクションIDに一致するすべてのイベントをフィルタリングします。
3. クライアント、Connector Appliance、またはサービスの診断ログで、トランザクションIDに一致するエラーが発生していないか確認します。その後、それに応じて適切な措置を講じます。
4. アプリケーションドメインテーブル (**Secure Private Access > 設定 > アプリケーションドメイン**) で、宛先のリソースロケーションが正しく選択されているか確認します。
5. アプリケーションが正しいポート、IP範囲、ドメインで構成されているか確認します。詳細については、「アプリケーションの追加と管理」を参照してください。

問題がまだ解決しない場合は、トランザクションIDとクライアントログに関連するエラーコードを添えてCitrixサポートにお問い合わせください。

クライアントデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

コントロールチャネルの確立に失敗しました

情報コード: 0x11000005

コントロールチャネル (DNSリクエスト用) の確立に失敗しました。

1. Secure Private Access サービスのライセンス資格を確認します。
2. 資格がない場合は、Citrixサポートに連絡してライセンスを確認してください。

詳細については、`<https://www.citrix.com/buy/licensing/product.html>`を参照してください。

ネットワークの問題により、制御チャネルの確立に失敗しました

情報コード: 0x11000006

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

ネットワークの問題により、制御チャネル（DNS要求用）の確立に失敗しました。

1. Secure Private Access サービスに到達可能かどうかを確認します。
2. 到達できない場合は、エラーコードとクライアントログを添えてCitrixサポートに連絡してください。

クライアントデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

IIP不足のため、制御チャネルの確立に失敗しました

情報コード: 0x11000007

IIP不足のため、制御チャネル（DNS要求用）の確立に失敗しました。

エラーコードとクライアントログを添えてCitrixサポートに連絡してください。

クライアントデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

セッションが終了したため、ログオフできません

クライアントマシン（キーボードまたはマウス）が設定されたタイムアウト期間を超えてアイドル状態だったため、この問題が発生した可能性があります。

情報コード: 0x12000001

Citrix Secure Accessクライアントに再ログインしてみてください。

セッションが強制的に終了されました

設定された強制タイムアウトに達したため、セッションが強制的に終了されました。

情報コード: 0x12000002

Citrix Secure Accessクライアントに再ログインしてみてください。

セッションの有効期限が切れたため、アプリケーションの起動に失敗しました

情報コード: 0x13000001

1. アプリケーションの起動中にZTNAセッションの有効期限が切れました。
2. Citrix Secure Accessクライアントに再ログインしてみてください。

ライセンスの問題によりアプリケーションの起動に失敗しました

情報コード: 0x13000002

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

1. Secure Private Accessサービスライセンスのエンタイトルメントを確認してください。
2. エンタイトルメントがない場合は、Citrixサポートに連絡してライセンスを確認してください。

詳細については、`<https://www.citrix.com/buy/licensing/product.html>`を参照してください。

サービスによってアクセスが拒否されたため、アプリケーションの起動に失敗しました

情報コード: 0x13000003, 0x13000008, 0x001800DF

ユーザーおよびアプリケーションのポリシー設定に従って、アプリケーションの起動が拒否されました。

以下を確認してください。

- 複数のアプリケーションで同じ宛先が使用されていないこと (HTTP、HTTPS、TCP、UDP)
- 複数のアプリケーションで宛先が重複していないこと。
- アクセス ポリシーがアプリケーションにバインドされていること。

また、拒否されたアプリケーションに対して構成されているポリシーの条件とアクションも確認してください。その後、ポリシーの条件とアクションを見直してください。

詳細については、アクセス ポリシーを参照してください。

クライアントがサービスに到達できないため、アプリケーションの起動に失敗しました

情報コード: 0x13000004, 0x13000005

1. Secure Private Access Service に到達可能かどうかを確認します。
2. アプリを再度起動します。
3. アプリに長時間到達できない場合は、エラーコードとクライアントログを添えてCitrixサポートに連絡してください。

クライアントデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

ポリシー評価と構成検証が失敗したため、アプリケーションの起動に失敗しました

情報コード: 0x13000007

Secure Private Accessサービスによってポリシー評価と構成検証が失敗したため、アプリケーションの起動に失敗しました。

アクセスされた宛先に対するアプリケーションを特定できません。

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

サービスによってアクセスが拒否されたため、アプリケーションの起動に失敗しました。

アプリケーションドメインテーブルの問題により、アプリケーションの起動に失敗しました

情報コード: 0x13000009

アプリケーションドメインテーブルにアクセスされた宛先のエントリがないため、アプリケーションの起動に失敗しました。

Secure Private Access > 設定 > アプリケーションドメインで、アプリケーションのルートエントリが正しく構成されていることを確認してください。

クライアントがSecure Private Accessサービスとの接続を閉じました

情報コード: 0x1300000B

1. エンドユーザーが手動で接続を閉じたかどうかを確認します。
2. そうでない場合は、エラーコードとクライアントログを添えてCitrixサポートにお問い合わせください。

クライアントデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

DNSサーバーによるFQDNの解決ができません

情報コード: 0x1300000C

この問題は、Connector ApplianceがFQDNのDNS解決に失敗した場合に発生します。

1. DNSサーバーで、該当するアプリのFQDNのDNSエントリを確認します。
2. Connector Applianceに適切なDNSサーバーが構成されていることを確認します。詳細については、「Connector Appliance管理ページでのネットワーク設定の構成」を参照してください。

Chrome以外のブラウザを使用したため、アプリの起動に失敗しました

情報コード: 0x1300000E

ブラウザモードがGoogle Chrome Enterprise Premiumに設定されており、Chrome以外のブラウザが使用されているため、アプリケーションの起動に失敗します。

アプリケーションを起動するには、Chromeブラウザを使用してください。

- ユーザーのシステムでデフォルトのシステムブラウザがChromeに設定されていることを確認します。

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

- ユーザーがChrome以外のブラウザを使用してアプリを手動で起動しようとしていないことを確認します。

アプリケーションが見つかりません

情報コード: 0x001800DE

ユーザーがアクセスした宛先に対応するアプリケーションが見つからない場合があります。これは、アプリケーションドメインテーブルに宛先からリソースロケーションへのマッピングがない場合に発生する可能性があります。

- アクセスされた宛先に対して、TCP/UDPまたはHTTPアプリケーションが構成されていることを確認します。
- ユーザーがアクセスした宛先アプリケーションのサブスクリプションを持っていることを確認します。

1. 管理ポータルでアプリケーションに移動します。
2. アプリを編集し、**サブスクリプション**タブに移動します。
3. 対象ユーザーがサブスクリプションリストにエントリを持っていることを確認します。
4. **アプリケーションドメイン**テーブルに宛先と適切なリソースロケーションがあることを確認します。

構成されたアプリケーション宛先リストの取得に失敗しました

情報コード: 0x001800D3

- 少なくとも1つのTCP/UDP/HTTPアプリが構成されていることを確認します。詳細については、「アプリケーションの追加と管理」を参照してください。
- アプリケーションドメインテーブル (**Secure Private Access > 設定 > アプリケーションドメイン**) ページが空でないこと、またはすべてのエントリが無効になっていないことを確認します。TCP/UDP/HTTPアプリケーションで構成された宛先は、このテーブルに自動的に追加されます。アプリケーションドメインテーブルで、アクティブなTCP/UDP/HTTPアプリケーションの宛先またはURLを削除したり無効にしたりしないことをお勧めします。

アプリケーション構成の問題

アプリケーション構成に特殊文字が含まれているか、ポリシー構成に問題があります。

情報コード: 0x001800D9, 0x001800DA

以下を確認してください。

- アプリ構成にサポートされていない文字が含まれていないこと。

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

- 宛先IPアドレス、IPアドレス範囲、またはIP CIDRが有効であること。
- アプリケーションの宛先は、アプリケーションドメインテーブルで有効になっています（**Secure Private Access > Settings > Application Domain**）。
- ポリシーが構成され、それぞれのアプリケーションにバインドされています。
- アクセスポリシーの構成が正しい。

リソースロケーションに関する問題

情報コード: 0x001800DB

- リソースロケーションが構成されていることを確認してください。
  a. Citrix Cloudのハンバーガーメニューで、**リソースロケーション**を選択します。
  b. 予期されるリソースロケーションが構成されており、リソースロケーションがアクティブな状態であることを確認してください。
- アプリケーションドメインテーブルで、宛先に対して正しいリソースロケーションが選択されていることを確認してください（**Secure Private Access > Settings > Application Domain**）。

TCP/UDP/HTTPアプリケーションで構成された宛先は、このテーブルに自動的に追加されます。アクティブなTCP/UDP/HTTPアプリケーションの宛先またはURLをアプリケーションドメインテーブルで削除または無効にしないことをお勧めします。

強化されたセキュリティポリシーがHTTPアプリケーションにバインドされている

情報コード: 0x001800DC, 0x001800DD, 0x13000006

強化されたセキュリティポリシーがバインドされているHTTPアプリケーションは、Citrix Secure Accessクライアントを介してアクセスされます。

- TCP/UDPアプリケーションとHTTPアプリケーションの両方に同じ宛先が使用されていないことを確認してください。
- HTTP/HTTPSアプリケーションで強化されたセキュリティポリシーが有効になっている場合、アプリへのアクセスはCitrix WorkspaceアプリまたはCitrix Remote Browser Isolationサービスを介してのみ行うことをお勧めします。
- HTTP/HTTPSアプリケーションの拡張セキュリティ制御を無効にして、Citrix Secure Accessクライアント経由でアプリにアクセスします。
  - Secure Private Access管理ポータルに移動します。

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

- **アプリケーション**タブをクリックし、アクセスした宛先HTTP/HTTPSアプリケーションのポリシー名を検索します。
- **アクセスポリシー**タブをクリックし、以前に特定したポリシー名を検索します。
- ポリシーを選択し、**編集**をクリックします。
- アクションを**制限付きアクセスを許可**から**アクセスを許可**に変更します。

構成の詳細については、「アプリケーションの追加と管理」を参照してください。

注：

Citrix Remote Browser Isolationサービスは、以前はSecure Browserサービスとして知られていました。

ホスト名の長さが256文字を超えています

情報コード： 0x001800EA

アプリケーション起動要求で受信したホスト名が256文字を超えています。

FDQN文字は256文字を超えないようにすることをお勧めします。

無効なIPアドレス

情報コード： 0x001800ED

アプリケーション起動リクエストで受信したIPアドレスが無効です。

クライアントからは、有効なプライベートIPアドレスのみにアクセスすることをお勧めします。

エンドツーエンド接続を確立できません

情報コード: 0x001800EF

クライアントとリソースの場所に構成されているサーバーとの間で、エンドツーエンド接続を確立できません。

- リソースの場所がアクティブな状態であることを確認します。
  - Citrix Cloudのハンバーガーメニューで、**リソースの場所**を選択します。
  - 該当するリソースの場所で、Connector Applianceのヘルスチェックを実行します。
  - これで問題が解決しない場合は、コネクタ仮想マシンを再起動します。
- 高可用性Connector Applianceを維持する

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

  - Citrix Cloudのハンバーガーメニューで、**リソースの場所**を選択します。
  - リソースの場所に少なくとも2つのConnector Applianceがあることを確認します。
- 以下を確認します。
  - リソースの場所のLANが正常に機能していること。
  - Connector Applianceからサービスまたはバックエンドサーバーへの接続をブロックするファイアウォールやプロキシが中間で存在しないこと。
  - クライアントネットワークは正常です。
  - バックエンドプライベートサーバーは正常です。
  - DNSサーバーは正常です。
  - FQDNは解決可能です。

これらの問題がない場合は、次の操作を実行します。

1. このエラーの診断ログからトランザクションIDを取得します。
2. Secure Private Accessサービスダッシュボードで、トランザクションIDに一致するすべてのイベントをフィルタリングします。
3. Secure Private Accessサービスダッシュボードからトランザクション IDに対応する診断ログを確認し、それに応じて適切な措置を講じます。
4. アプリケーションドメインテーブル (**Secure Private Access > 設定 > アプリケーションドメイン**) で、正しいリソースロケーションが宛先として選択されていることを確認します。
5. アプリケーションが正しいIPアドレス、ポート、およびFQDNで構成されているか (**Secure Private Access > アプリケーション**) を確認します。

これらの手順のいずれでも問題が解決しない場合は、トランザクションIDに対応するエラーコードを添えてCitrixサポートに連絡し、クライアントログを収集してください。

クライアントデバッグログを収集するには、「クライアントログの収集方法」を参照してください。

アプリケーション要求で受信したIPv6

情報コード: 0x001800F5

アプリケーション要求でサポートされていないIPv6が受信されました。現在、IPv4のみがサポートされています。

アプリケーションを編集して、アプリケーションのIPアドレスの問題を修正します。

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

1. Secure Private Access管理ポータルに移動します。
2. **アプリケーション**タブをクリックします。
3. アプリを検索し、**編集**をクリックします。

詳細については、「アプリの追加と管理」を参照してください。

UDPトラフィックの配信に失敗しました

情報コード: 0x001800F9

クライアント接続が失われたため、UDPトラフィックの配信に失敗しました

1. クライアントセッションがアクティブであるか確認します。
2. ログアウトしてから再ログインします。

UDPデータトラフィックの配信に失敗しました

情報コード: 0x001800FF

- エラーコードのトランザクションIDを検索し、Secure Private Accessサービスダッシュボードでそのトランザクションに一致するすべてのイベントをフィルタリングします。
- トランザクションIDに一致する他のコンポーネントでエラーが発生していないか確認します。他のコンポーネントで問題が見つかった場合は、それに応じて適切な措置を講じてください。
- この方法で問題が解決しない場合は、エラーコードと関連するトランザクションIDを添えてCitrixサポートにお問い合わせください。

ネットワーク接続の問題によりアプリケーションの起動に失敗しました

情報コード: 0x10000401

Connector Appliance と Secure Private Access サービス間のネットワーク接続の問題によるアプリケーション起動の失敗

1. Connector Appliance のパブリックインターネット接続を確認します。
2. プロキシまたはファイアウォールルールが接続をブロックしていないか確認します。
3. プロキシが問題の原因である場合は、プロキシをバイパスしてアプリの起動を再度試してください。
4. Connector Appliance のヘルスステータスを確認します (**Citrix Cloud > リソースの場所**)。

ネットワーク設定の詳細については、「Connector Appliance のネットワーク設定」を参照してください。

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

Connector Appliance が Secure Private Access サービスに登録できませんでした

情報コード: 0x10000402, 0x1000040C

1. Connector Appliances の管理ページに移動し、コネクタの概要を確認します。
2. コネクタのステータスが良好でない場合は、管理ポータルのリソースの場所に移動します。
3. 該当するリソースの場所で Connector Appliances のヘルスチェックを実行します。
4. ヘルスチェックが失敗した場合は、コネクタ仮想マシンを再起動します。
5. コネクタの概要を確認し、ヘルスチェックを再度実行します。

ネットワーク設定の詳細については、Connector Appliance のネットワーク設定を参照してください。

Connector Appliance との接続の問題

情報コード: 0x10000403, 0x10000404, 0x10000407, 0x1000040A, 0x1000040B, 0x1000040F, 0x10000410

- エラーコードのトランザクション ID を調べます。
- Secure Private Access ダッシュボードで、トランザクション ID に一致するすべてのイベントをフィルタリングします。
- トランザクション ID に一致する他のコンポーネントでエラーが発生していないか確認し、エラーが見つかった場合は、そのエラーコードに一致する適切な回避策を実行します。
- 他のコンポーネントでエラーが見つからない場合は、次の操作を行います。
  - Connector Appliances の管理ページに移動します。
  - 診断レポートをダウンロードします。詳細については、診断レポートの生成を参照してください。
  - パケットトレースをキャプチャします。詳細については、ネットワーク接続の確認を参照してください。
- この診断レポートとパケットトレース、およびエラーコードとトランザクション ID を添えて Citrix サポートに連絡してください。

Connector Appliance とバックエンドのプライベート TCP/UDP サーバーとの接続の問題

情報コード: 0x10000405, 0x10000408, 0x10000409, 0x1000040D, 0x1000040E, 0x10000412

Connector Appliance は、バックエンドのプライベート TCP/UDP サーバーとの接続に問題があります。

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

- エンドユーザーが接続しようとしているバックエンドサーバーが稼働しており、リクエストを受信できる状態にあるか確認します。
- 企業ネットワーク内からバックエンドサーバーへの到達可能性を確認します。
- コネクタがバックエンドサーバーに到達できないようにブロックされていないか、プロキシ設定を確認します。
- FQDNベースのアプリのリクエストである場合は、DNSサーバーで該当するアプリのDNSエントリを確認します。

Connector ApplianceがFQDNのDNSを解決できません

情報コード: 0x10000406

- DNSサーバーで該当するアプリのFQDNのDNSエントリを確認します。
- Connector Applianceに適切なDNSサーバーが構成されていることを確認します。詳細については、「Connector Appliance管理ページでのネットワーク設定の構成」を参照してください。

プライベートサーバー接続が終了しました

情報コード: 0x10000411

プライベートサーバーへの接続は、クライアントまたはSecure Private Accessサービスによって終了されました。

1. エンドユーザーがアプリケーションを閉じているかどうかを確認します。
2. このログのトランザクションIDと一致する他の診断ログを確認し、それに応じて適切な措置を講じます。
3. アプリを再度起動します。
4. これで問題が解決しない場合は、エラーコードとトランザクションIDを添えてCitrixサポートに連絡してください。

プライベートサービスIPまたはFQDNへの接続またはデータ送信に失敗しました

情報コード: 0x10000413

- プライベートサーバーへの接続が終了しました
- コネクタアプライアンスとバックエンドのプライベートTCP/UDPサーバーとの接続の問題。ルーティングドメインのエントリを確認してください。IPアドレスが有効であり、正しいバックエンドを指していることを確認してください。

一致するポリシー条件がありません

情報コード: 0x100508

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

ユーザーコンテキストが、アプリに割り当てられているポリシーで定義されているアクセスルール条件と一致しません。

ユーザーのコンテキストと一致するようにポリシー構成を更新します。

アプリケーションに関連付けられているアクセスポリシーがありません

情報コード: 0x100509

1. Citrix Secure Private Access™サービスGUIで、左側のナビゲーションにある**アクセスポリシー**をクリックします。
2. 適切なアプリにアクセスポリシーが関連付けられていることを確認します。
3. アプリにアクセスポリシーが関連付けられていない場合は、アプリのアクセスポリシーを作成します。詳細については、「アクセスポリシーの作成」を参照してください。
4. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

FQDNまたはIPアドレスのアプリケーション構成が見つかりません

情報コード: 0x10050A

受信したFQDNまたはIPアドレス要求に一致するアプリケーションが見つかりませんでした。そのため、アプリは未公開アプリケーションとして分類されます。予期しない場合は、次の操作を実行します。

1. Secure Private Accessサービス管理ポータルに移動します。
2. 左側のナビゲーションで をクリックします。
3. アプリを検索し、 をクリックします。
4. アプリケーションにFQDNまたはIPアドレスを追加します。正確なドメイン、IPアドレス、またはワイルドカードドメインを追加できます。

   注： Secure Private Access > 設定 > アプリケーションドメイン でFQDNまたはIPアドレスを追加しても、この問題は解決しません。アプリケーション構成の一部として追加する必要があります。

アプリケーション列挙情報

情報コード： 0x10050C

このコードは、ユーザーが利用できる可能性のある複数のアプリケーションのポリシー評価結果をキャプチャします。アプリケーションへのアクセスは、次の理由で拒否される場合があります。

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

- ユーザーコンテキストが、アプリに割り当てられているポリシーで定義されているアクセスルール条件と一致しません – 詳細については、「一致するポリシー条件がありません」を参照してください。
- アプリケーションに関連付けられているアクセスポリシーがありません – 詳細については、「アプリケーションに関連付けられているアクセスポリシーがありません」を参照してください。
- アプリケーションに関連付けられているポリシーがアクセスを拒否するように構成されています – この場合、これは意図されたものであるため、アクションは不要です。
- アクセスポリシーの適用中に予期しない内部エラーが発生しました。詳細については、Citrixサポートにお問い合わせください。

アプリケーションドメインテーブルにルーティングエントリがないため、TCP/UDPアプリの起動に失敗しました

情報コード： 0x00180101

アプリケーション構成が存在するにもかかわらず、ルーティングエントリが見つからないか、以前に削除された場合に、この問題が発生する可能性があります。

アクセスされる宛先に対して、ルーティングエントリ（**Secure Private Access > Settings > Application Domain**）を追加します。

コネクタが正常でないため、TCP/UDPアプリの起動に失敗しました

情報コード: 0x00180102

コネクタのいずれも起動しておらず、新しい接続に応答していない場合に、この問題が発生する可能性があります。

該当するリソースの場所で、コネクタアプライアンスのヘルスチェックを実行します。

コネクタに到達できないため、UDP/DNSリクエストに失敗しました

情報コード: 0x00180103

UDP/DNSトラフィックがコネクタに到達できない場合に、この問題が発生する可能性があります。

該当するリソースの場所で、コネクタアプライアンスのヘルスチェックを実行します。

NGSクッキーの有効期限が切れているため、ページの読み込みに失敗しました

情報コード: 0x20580001

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

1. ブラウザを再起動し、アプリを再度開いてみてください。
2. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

ネットワーク障害のため、アクセスポリシーの取得に失敗しました

情報コード: 0x20580002

1. URLとネットワーク接続を確認します。
2. ブラウザを再起動し、アプリをもう一度開いてみてください。
3. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

JSON Webトークンの解析中にアクセスポリシーの取得に失敗しました

情報コード:0x20580003

1. ブラウザを再起動し、アプリをもう一度開いてみてください。
2. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

アクセスポリシーの詳細取得におけるネットワーク障害

情報コード:0x20580004

1. アクセスポリシーが有効になっているか確認します。
2. ブラウザを再起動し、アプリをもう一度開いてみてください。
3. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

公開証明書の取得中にポリシーの取得に失敗しました

情報コード: 0x20580005

1. ブラウザを再起動し、アプリをもう一度開いてみてください。
2. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

JSON Webトークンの署名検証中にポリシーの取得に失敗しました

情報コード: 0x20580007

1. ネットワーク時刻とユーザーデバイス時刻が同期しているか確認してください。
2. ブラウザを再起動し、アプリをもう一度開いてみてください。
3. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

公開証明書の検証中にポリシーの取得に失敗しました

情報コード: 0x20580008

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

1. ブラウザを再起動し、アプリをもう一度開いてみてください。
2. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

ポリシーURLを形成するためのストア環境を特定できませんでした

情報コード: 0x2058000A

1. ブラウザを再起動し、アプリをもう一度開いてみてください。
2. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

アクセス ポリシー取得リクエストへの応答の取得に失敗しました

情報コード: 0x2058000B

1. ブラウザを再起動し、アプリをもう一度開いてみてください。
2. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

セカンダリDS認証トークンの有効期限切れにより、アクセス ポリシーの取得に失敗しました

情報コード: 0x2058000C

1. ブラウザを再起動し、アプリをもう一度開いてみてください。
2. これで問題が解決しない場合は、Citrixサポートにお問い合わせください。

Connector Applianceが登録されていません

情報コード: 0x10200002

Connector Applianceの登録を確認してください。

詳細については、「Citrix CloudへのConnector Applianceの登録」を参照してください。

Connector Applianceに接続できません

情報コード: 0x10200003

Connector Applianceは、Citrix Cloudとリソースの場所の間で通信できません。

コネクタの登録を確認します。

詳細については、「Citrix Cloud に Connector Appliance を登録する」を参照してください。

Citrix Secure Private Access サービスへの接続に失敗しました

情報コード: 0x10000301

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

Connector Appliance のネットワーク設定を確認します。詳細については、「Connector Appliance のネットワーク設定」を参照してください。

プロキシサーバーに到達できません

情報コード: 0x10000303, 0x10000304

プロキシサーバーの設定を確認し、Connector Appliance から到達可能であることを確認します。詳細については、「Citrix Cloud に Connector Appliance を登録する」を参照してください。

プロキシサーバー認証に失敗しました

情報コード: 0x10000305

プロキシサーバーの資格情報を確認し、Connector Appliance で正しく構成されていることを確認します。詳細については、「Connector Appliance の登録後」を参照してください。

構成されたプロキシサーバーに到達できません

情報コード: 0x10000306

Connector Appliance のネットワーク設定、ファイアウォール設定、またはプロキシサーバー設定を確認します。詳細については、次のトピックを参照してください。

- Connector Appliance のネットワーク設定
- Citrix Cloud にコネクタアプライアンスを登録する
- コネクタアプライアンスの通信

バックエンドサーバーからエラー応答を受信しました

情報コード: 0x10000307

予期しないコードの場合は、バックエンドWebサーバーのHTTPステータスコードを確認してください。

ターゲットURLにリクエストを送信できません

情報コード: 0x10000005

ターゲットURLまたはコネクタアプライアンスのネットワーク設定を確認してください。詳細については、「コネクタアプライアンスのネットワーク設定」(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/connector-appliance.html#network-settings-for-your-connector-appliance)を参照してください。

SSOの処理に失敗しました

情報コード: 0x10000107

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

Citrix Cloud からアプリ構成データを取得できませんでした。

コネクタアプライアンスのネットワーク設定を確認し、NTPサーバーが構成されており、タイムストリップの問題がないことを確認してください。詳細については、「コネクタアプライアンスのネットワーク設定」(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/connector-appliance.html#network-settings-for-your-connector-appliance)を参照してください。

Citrix Secure Private Access サービスへの接続に失敗しました

情報コード: 0x10000108, 0x1000010B

コネクタアプライアンスのネットワーク設定を確認してください。詳細については、「コネクタアプライアンスのネットワーク設定」(/ja-jp/citrix-cloud/citrix-cloud-resource-locations/connector-appliance.html#network-settings-for-your-connector-appliance)を参照してください。

SSOの処理に失敗しました。SSO設定を特定できません

情報コード: 0x1000010A

SSO構成を確認し、サーバーがConnector Applianceに到達可能であることを確認してください。

FormFill SSOに失敗しました。フォームアプリの構成が正しくありません

情報コード: 0x10000101, 0x10000102, 0x10000103, 0x10000104

SSOフォームアプリの構成を確認し、ユーザー名、パスワード、アクション、ログインURLの各フィールドがアプリ設定で正しく構成されていることを確認してください。

Kerberos SSOに失敗しました

情報コード: 0x10000202

バックエンドサーバーとドメインコントローラーのKerberos SSO設定を確認してください。また、フォールバックNTLM認証設定も確認してください。

Kerberos SSO設定については、「Kerberos構成の検証」を参照してください。

認証タイプのSSOの処理に失敗しました

情報コード: 0x10000203

Secure Private Accessサービスとバックエンドサーバーのの SSO設定を確認してください。Secure Private Accessサービスについては、「優先サインオン方法の設定」を参照してください。

Kerberos SSOに失敗しましたが、NTLMにフォールバックしています

情報コード: 0x10000204

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

ドメインコントローラーからのKerberosチケットの取得に失敗しました。セカンダリ認証として、Connector ApplianceはフォールバックNTLM認証を試行しました。

Kerberos認証を正常に有効にするには、バックエンドサーバーとドメインコントローラーのKerberos SSO設定を確認してください。

詳細については、「Kerberos構成の検証」を参照してください。

Citrix Workspace™アプリで構成された複数のZTNAエンタイトルアカウント

情報コード: 0x14000001

Citrix Workspaceアプリでは、ZTNAエンタイトルアカウントを1つだけ構成してください。

クライアントログの収集方法

- **Windowsクライアント:**
  a. アプリを開き、ログ記録が有効になっていることを確認します。
  b. Secure Private Accessサービスに接続し、発生している問題を再現します。
  c. アプリで、**ログ記録**に移動し、**ログファイルの収集**をクリックします。これにより、ログファイルが生成されます。
  d. クライアントマシンのデスクトップにログファイルを保存します。
- **Macクライアント:**
  a. アプリを開き、**ログ > 詳細**に移動します。
  b. ログをクリアし、問題の再現に進みます。
  c. 「**ログ > ログのエクスポート**」に戻ります。これにより、ログファイルを含むzipファイルが作成されます。

よくある質問

以下のセクションでは、よくある質問に関する詳細情報を提供します。

診断ログに関する詳細情報はどこで確認できますか?

診断ログの詳細については、トピック「診断ログ」を参照してください。

発生した障害を解決するために、Secure Private Accessのトラブルシューティングトピックをどのように使用しますか?

1. 解決しようとしている障害の情報コードを取得します。
2. エラー参照テーブルで情報コードを見つけます。

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

3. その情報コードに提供されている解決手順に従います。

情報コードとは何ですか どこで確認できますか?

障害などの一部のログイベントには、関連する情報コードがあります。エラー参照テーブル内でこの情報コードを検索して、解決手順またはそのイベントに関する詳細情報を見つけてください。

トランザクションIDとは何ですか どのように使用しますか?

Citrix Enterprise Browserを介したアクセス障害/問題は、エンドユーザーにトランザクションIDを表示します。管理者はエンドユーザーからこのトランザクションIDを取得し、このトランザクションIDを使用して問題の原因となった正確なログをフィルターし、正確な問題を特定できます。管理者がトランザクションIDでイベントをフィルターすると、現在の問題に関連するイベントのみが表示され、障害や問題が発生した理由に関するすべての詳細が管理者に提供されます。管理者は、これらのログのエラーコードを使用して、問題をさらに解決できます。

Secure Private Access PoPの場所はどこですか?

以下は、Secure Private AccessデータPoPの場所のリストです。

POP名	ゾーン	リージョン
アズール-ユーエス-イー	アジュール イーストUS	バージニア
アズール-ユーエス-ダブリュー	アジュール ウェストUS	カリフォルニア
アズール-ユーエス-エスシー	アジュール サウスセントラルUS	テキサス
アズール-エーユーエス-イー	アジュール オーストラリア イースト	ニューサウスウェールズ
アズ-欧州北部	Azure 北ヨーロッパ	アイルランド
アズ-欧州西部	Azure 西ヨーロッパ	オランダ
アズ-日本東部	Azure 東日本	東京、埼玉
アズ-ブラジル南部	Azure ブラジル南部	サンパウロ州
アズ-東南アジア	Azure 東南アジア	シンガポール
アズ-ユーエーイー-エヌ	アジュール UAE北	ドバイ

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

POP名	ゾーン	リージョン
アズ-イン-エス	アジュール 南インド	チェンナイ
アズ-アジア-エイチケー	アジュール 東アジア	香港

以下は、Secure Private Access管理PoPの場所のリストです。

POP名	ゾーン	リージョン
エーダブリューエス-ユーエス-イー-エムジーエムティー	エーダブリューエス us-east-1	ノースバージニア
エーダブリューエス-in-w-mgmt	エーダブリューエス ap-south-1	ムンバイ
エーダブリューエス-eu-c-mgmt	エーダブリューエス eu-central-1	フランクフルト

情報コードとエラー参照テーブルを使用しても障害を解決できない場合はどうすればよいですか?

Citrixサポートにお問い合わせください。

参照

- **Webアプリを追加する**
  - エンタープライズWebアプリのサポート
  - Webアプリへの直接アクセスを構成する
- **SaaSアプリを追加する**
  - サービスとしてのソフトウェアアプリのサポート
  - SaaSアプリサーバー固有の構成
- **クライアント/サーバーアプリの構成**
  - クライアント/サーバーアプリのサポート
- **アクセスポリシーの作成**
  - アクセスポリシーの作成
- **ルートテーブル**

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

- ルートテーブル

監査およびシステムログ

Secure Private Accessサービス関連イベントは、**Citrix Cloud > システムログ**にキャプチャされます。管理者がCitrix Secure Private Access™サービスで実行するすべてのイベントはCitrix Cloudに送信され、**システムログ**にキャプチャされます。管理者イベントには、以下が含まれますが、これらに限定されません。

- アプリの作成または更新
- アプリの削除
- アダプティブアクセスポリシーの設定または削除
- コネクタのアップグレード
- 許可またはブロックされたWebサイトの作成

デフォルトでは、**システムログ**には過去30日間に発生したイベントが表示されます。最新のイベントが最初に表示されます。

ログにはイベントの詳細が表示され、以下でフィルタリングできます。

- **日付と時刻:** イベントが発生した日付と時刻（UTC形式）。
- **アクター:** イベントをトリガーしたユーザーまたはシステム。例: 管理者、セキュアクライアント、サービスプリンシパル。
- **サービス:** イベントがログに記録されたサービス。Secure Private Accessイベントには、サービスとして**Secure Private Access**が設定されている必要があります。
- **イベント:** イベントの簡単な説明。例: SaaSアプリケーションの作成、TCP/UDPアプリケーションの削除、アダプティブアクセスポリシーの更新、アプリケーションドメインの更新。
- **ターゲット:** イベントの結果として影響を受けた、または変更されたオブジェクト。例: アプリケーションに使用されるドメイン。

  ターゲット識別子は人間が判読できる形式であり、実際のIDではありません。

次の図は、**システムログ**におけるSecure Private Accessイベントを表示しています。

システムログ(/en-us/citrix-secure-private-access/media/spa-system-logs.png)

イベントのエクスポート、特定の期間のイベントの取得、ログイベントの転送、データ保持などの詳細については、システムログを参照してください。

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

デバイスポスチャのログとイベント

管理者は、デバイスポスチャダッシュボードを通じてデバイスのコンプライアンスを監視できます。組織のリソースにアクセスするエンドポイントのコンプライアンス要件を定義する、構成済みのすべてのデバイスポスチャポリシーを表示できます。また、すべてのデバイスのリアルタイムのコンプライアンスステータスも表示でき、これには以下のように分類された詳細な評価結果が含まれます。

- **準拠:** 指定されたすべてのセキュリティ要件とポリシー基準を満たすデバイス。
- **非準拠:** 1つ以上のセキュリティ要件を満たさないが、限定的なアクセスが許可される可能性があるデバイス。
- **アクセス拒否:** 重大なセキュリティリスクをもたらし、リソースへのアクセスがブロックされているデバイス。

デバイスポスチャのログとイベントは、Secure Private Accessダッシュボード および Identity and Access Managementコンソールのデバイスポスチャダッシュボード で表示できます。

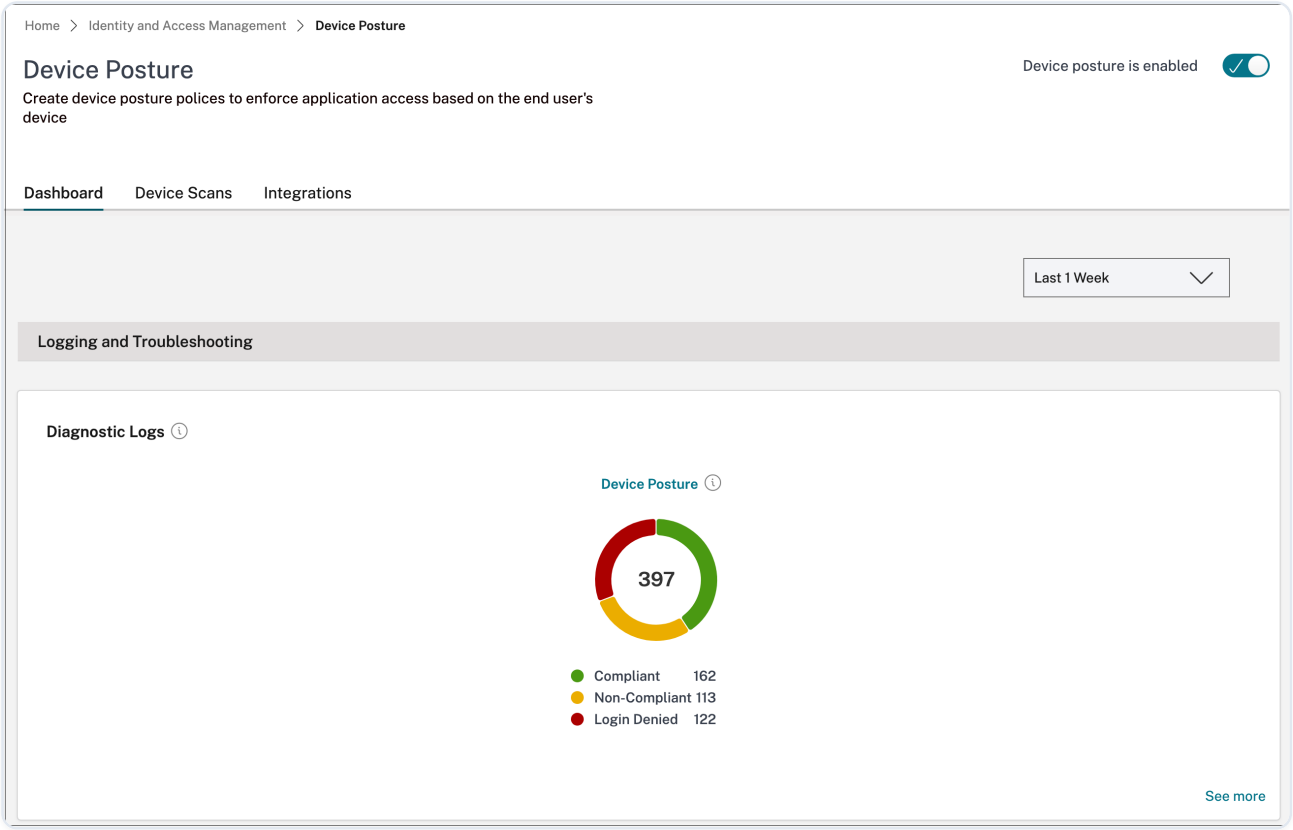
Identity and Access Managementコンソールのデバイスポスチャダッシュボード

Identity and Access Managementコンソールのデバイスポスチャダッシュボードのログとイベントを表示するには、次の手順を実行します。

1. Citrix Cloudにサインインします。
2. Citrix Cloudメニューから、**Identity and Access Management**を選択します。
3. **Device Posture > Manage**をクリックし、次に**Dashboard**をクリックします。

   Logging and Troubleshootingセクションには、デバイスポスチャサービスに関連する診断ログが表示されます。
4. ログの詳細を表示するには、**See more**リンクをクリックします。ポリシー結果（**準拠**、**非準拠**、**ログイン拒否**）に基づいて検索を絞り込むことができます。

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



Add filterオプションを使用して、ポリシー情報、ポリシー結果、オペレーティングシステム、トランザクションID、情報コード、デバイスIDなどのさまざまな基準に基づいて検索を絞り込むことができます。たとえば、検索フィールドで**Device-ID**をクリックし、**~ (contains some value)** を選択して「6273」と入力します。6273を含むデバイスIDに関連するすべてのログが表示されます。

各ログエントリの横にある展開アイコンをクリックすると、スキャンタイプ、クライアントアプリバージョン、クライアントライブラリバージョン、エンドポイント情報などの詳細が表示されます。

デバイスポスチャダッシュボード2(/en-us/device-posture/media/device-posture-dashboard2.png)

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

注:

- **ClientAppVersion**フィールドと**ClientLibraryVersion**フィールドには、それぞれEPAクライアントバージョンとライブラリバージョンが表示されます。
- アクセスが拒否された場合、トランザクションIDもエンドユーザーに表示されます。
- エラーまたはスキャン失敗が発生した場合、Device Postureサービスはトランザクション IDを表示します。このトランザクションIDは、Secure Private Accessサービスダッシュボードで確認できます。ログで問題が解決しない場合、エンドユーザーはCitrixサポートにトランザクションIDを共有して問題を解決できます。

ログの場所

Windowsクライアントログは次の場所にあります。

- %localappdata%\Citrix\EPA\dpaCitrix.txt
- %localappdata%\Citrix\EPA\epalib.txt

macOSクライアントログは次の場所にあります。

- ~/Library/Application Support/Citrix/EPAPlugin/EpaCloud.log
- ~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

Secure Private Accessダッシュボード

Device Postureサービスのログとイベントを表示するには、次の手順を実行します。

1. Citrix Cloudにサインインします。
2. Secure Private Accessタイルで、**Manage**をクリックし、次に**Dashboard**をクリックします。

   Logging and Troubleshootingセクションには、Device Postureサービスに関連する診断ログが表示されます。
3. ログの詳細を表示するには、**See more**リンクをクリックします。ポリシー結果（**Compliant**、**Non-Compliant**、**Login Denied**）に基づいて検索を絞り込むことができます。

ダッシュボード(/en-us/device-posture/media/device-posture-end-user-flow-results33.png)

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

デバイスポスチャのエラーログ

Device Postureサービスに関連する以下のログは、Citrix MonitorおよびSecure Private Accessダッシュボードで表示できます。これらのログについてはすべて、解決のためにCitrixサポートに連絡することをお勧めします。

- 構成されたポリシーの読み取りに失敗しました
- エンドポイントスキャンの評価に失敗しました
- ポリシー/式の処理に失敗しました
- エンドポイントの詳細の保存に失敗しました
- エンドポイントからのスキャン結果の処理に失敗しました

デバイスポスチャデータの書き出し

Device Postureサービスイベント（デバイスポスチャの結果やイベントタイプなど）は、Security Information and Event Management (SIEM) サービスにエクスポートできます。これらのイベントは、Citrix Endpoint Analysis (EPA) クライアントが、Citrix Virtual Apps and Desktops™ または Citrix Secure Private Accessリソースへのアクセスを試みるデバイスに対してポスチャチェックを実行したときに生成されます。

- Device PostureサービスログをSIEMにセットアップ、構成、エクスポートする方法については、「Security Information and Event Management (SIEM) integration」を参照してください。
- Device Postureサービスからエクスポートできるイベントとログの詳細については、「Device Postureサービスイベント」(/ja-jp/security-analytics/siem-integration/siem-messages-schema#device-posture-service-events)を参照してください。
- Device Postureサービスのトランザクションを診断およびトラブルシューティングする方法については、「Device Postureサービストランザクションの診断」(/ja-jp/citrix-daas/monitor/troubleshoot-deployments/user-issues/diagnose-device-posture-service-transactions)を参照してください。

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

データのエクスポートとサードパーティ統合

以下のセクションでは、データのエクスポートとサードパーティ統合に関する詳細情報を提供します。

セキュリティ情報およびイベント管理の統合

Secure Private Access とセキュリティ情報およびイベント管理 (SIEM) の統合により、管理者は重要なログ、ポリシーの結果、およびユーザーアクティビティデータを Kafka プッシュメカニズムを使用してサードパーティの SIEM システムにエクスポートできます。この統合により、Citrix Secure Private Access サービスを使用している組織は、可視性の向上、コンプライアンス追跡、およびセキュリティに関する洞察を得ることができます。

Splunk、Google Chronicle、Microsoft Sentinel、Elastic など、任意の SIEM を使用できます。

SIEM での Secure Private Access および Device Posture サービスに関連するユーザーイベントのリストについては、以下のトピックを参照してください。

- Secure Private Access イベント
- Device Posture サービスイベント

OData API を使用してカスタムレポートを作成する

Secure Private Access Monitor OData REST API を使用すると、管理者はセッションデータをエクスポートし、カスタムレポートを作成できます。この機能は、ロールアウトの追跡、ユーザーアクティビティの分析、および Secure Private Access サービスのパフォーマンスと使用状況に関する洞察を得るのに役立ちます。

エクスポート可能な Secure Private Access データの種類については、以下のトピックを参照してください。

- Secure Private Access セッション
- Secure Private Access アプリケーション
- セキュア プライベート アクセス 列挙

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

システムログのエクスポート

Citrix Cloudの**システムログ**機能は、Secure Private Accessサービス内で発生するイベントのタイムスタンプ付き記録を提供します。管理者は、さらなる分析と検証のために、これらのログをCSVファイルとしてエクスポートできます。詳細については、Citrix CloudからのSyslogを参照してください。

Kafkaからデータをエクスポートする

Kafkaは、リアルタイムのデータ処理と分析のために設計されたオープンソースの分散ストリーミングプラットフォームです。Kafkaを使用することで、組織はストリーミングデータをリアルタイムで分析し、より迅速なインサイトを獲得し、プロアクティブな意思決定を可能にし、高度なセキュリティ監視機能をサポートできます。

Secure Private AccessイベントとDevice Postureサービスイベントを Kafkaからエクスポートして、外部のセキュリティ情報およびイベント管理（SIEM）システム、分析プラットフォーム、カスタム監視ソリューションと統合できます。

Secure Private Accessイベント

ユーザーがCitrix Workspaceアプリ、Citrix Secure Accessクライアント、Citrix Enterprise Browserなどの Citrix Secure Private Accessを介してアプリケーションにアクセスすると、ユーザーイベントはCitrix Analytics for Securityでリアルタイムに受信されます。

詳細については、「Secure Private Accessイベント」を参照してください。

Device Postureサービスイベント

ユーザーイベントは、Citrix Endpoint Analysis（EPA）クライアントがCitrix Virtual Apps and DesktopsまたはCitrix Secure Private Accessリソースへのアクセスを試みるデバイスに対してポスチャチェックを実行したときに生成されます。

詳細については、「Device Postureサービスイベント」を参照してください。

監査ログとシステムログのエクスポート

Citrix Cloudの**システムログ**機能は、Secure Private Accessサービス内で発生するイベントの完全なタイムスタンプ付き記録をキャプチャします。これらの監査ログは、規制遵守、セキュリティ監視、および管理操作のトラブルシューティングに不可欠です。管理者は、詳細な分析、コンプライアンス検証、および外部セキュリティ監視システムとのシームレスな統合のために、ログデータをCSVファイルとしてエクスポートできます。

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

Secure Private Accessサービスの場合、**システムログ**には以下のイベントがキャプチャされます。

- アプリケーション構成の変更（作成、変更、削除を含む）。
- アクセスルール、セキュリティ構成、条件付きアクセス設定などのポリシー更新。
- ユーザーとグループの追加または削除などのユーザーおよびグループ管理操作。
- アプリケーションドメイン関連情報。
- 許可およびブロックされたURLリスト。

SystemLog APIを使用してSecure Private Accessイベントをエクスポートする

SystemLog APIを使用して、Secure Private Accessイベントをエクスポートできます。SystemLog APIを使用すると、指定した期間にCitrix Cloudアカウントで発生したイベントを取得できます。

- SystemLog APIを使用してイベントをエクスポートする方法の詳細については、Citrix DeveloperドキュメントのCitrix Cloud - SystemLogを参照してください。
- Secure Private Accessサービスで**システムログ**がキャプチャするイベントデータを理解するには、システムログイベントリファレンスを参照してください。
- MonitorサービスAPIの詳細については、Citrix Monitor Service APIについてを参照してください。

OData を使用してセッションデータをエクスポートする

Secure Private Access Monitor OData REST API を使用すると、管理者はセッションデータをエクスポートし、カスタムレポートを作成できます。この機能は、ロールアウトの追跡、ユーザーアクティビティの分析、Secure Private Access サービスのパフォーマンスと使用状況に関する洞察の取得に特に役立ちます。

- 管理者は OData REST API を活用して、特定の組織のニーズを満たすカスタムレポートを作成できます。この柔軟性により、セッションデータ、ユーザーアクティビティ、およびアプリケーションの使用状況を詳細に分析できます。
- API はロールアウトの追跡を可能にし、管理者が組織全体での Secure Private Access の構成とポリシーの採用と有効性を監視するのに役立ちます。
- OData API を使用すると、セッションデータを外部ツールやシステムでさらに分析するためにエクスポートできます。

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

Secure Private Access Monitor OData REST API の詳細については、以下のトピックを参照してください。

- Secure Private Access セッション
- Secure Private Access アプリケーション
- セキュアプライベートアクセス列挙

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

ロールベースのアクセス制御

Secure Private Access は、ユーザーの権限とアクセスレベルを管理するために、ロールベースのアクセス制御モデルを使用します。これは、各ユーザーに特定のロールが割り当てられ、そのロールによってシステム内でできることとできないことが決まることを意味します。このモデルは、ユーザーがタスクを実行するために適切なレベルのアクセス権を持つことを保証すると同時に、アクセスしてはならない機密データや機能へのアクセスを防ぐのに役立ちます。

Secure Private Access 管理者には、次の4つの主要なロールが利用可能です。これらの各ロールには、異なる種類のユーザーのニーズに合わせて設計された、異なる権限セットがあります。

- フルアクセス管理者
- 読み取り専用管理者
- フルモニター管理者
- ヘルプデスク管理者

注:

DaaS Monitor を使用して Secure Private Access を監視するには、管理者は Secure Private Access ロールのいずれかに加えて、DaaS ロールを割り当てる必要があります。

次の表は、各ロールの簡単な説明を示しています。

ロール	説明
フルアクセス管理者	Secure Private Access 環境の構成、管理、および運用を完全に制御する必要がある個人を対象としています。フルアクセス管理者には、次の権限があります。
	Secure Private Access のすべての機能へのアクセス。
	Secure Private Access コンソール内で、アプリ、ポリシー、設定を作成、編集、変更する権限。

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

ロール	説明
読み取り専用管理者	Secure Private Access のアクティビティとシステムパフォーマンスを監視および分析する必要がある個人向けです。読み取り専用管理者には、次の権限があります。
	Secure Private Access ダッシュボードへのアクセス。
	すべての Secure Private Access アプリケーション構成と設定を表示する機能。
	読み取り専用管理者には、作成/更新/削除機能のいずれの権限もありません。
フルモニター管理者	Monitor コンソールで Secure Private Access のアクティビティとパフォーマンスを監視する責任があるユーザー向けです。フルモニター管理者には、次の権限があります。
	Secure Private Access 内のすべての監視ダッシュボードとレポートツールへのアクセス。
	すべてのSecure Private Accessの構成と設定を表示する機能。
	フルモニター管理者には、Secure Private Accessの構成、ポリシー、または設定を作成、編集、変更する権限はありません。
ヘルプデスク管理者	ユーザーアクセス問題のトラブルシューティングとトリアージを担当するヘルプデスク担当者向けです。ヘルプデスク管理者には、以下の権限があります。
	Secure Private Accessの構成と設定に対する限定的な可視性。Monitorコンソールでのトラブルシューティングに関連する情報に焦点を当てています。

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

ロール	説明
	Secure Private Accessコンソール内の特定のトラブルシューティングツールおよび診断ユーティリティへのアクセス。
	トラブルシューティングとモニターダッシュボードを表示します。
	ヘルプデスク管理者には、Secure Private Accessの構成またはポリシーを作成、編集、変更する権限はありません。

ロールと権限

以下の表に、ロールと権限をまとめます。

	フルアクセス管理者	読み取り専用管理者	フルモニター管理者	ヘルプデスク管理者
アプリの作成/編集/削除	はい	いいえ	いいえ	いいえ
ポリシーの作成/編集/削除	はい	いいえ	いいえ	いいえ
構成/設定を編集	はい	いいえ	いいえ	いいえ
構成/設定を表示	はい	はい	はい	制限付き
Secure Private Accessダッシュボードでログおよびトラブルシューティングウィジェットを表示	はい	はい	はい	はい
ユーザーを検索	はい	はい	はい	いいえ

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

	フルアクセス管理者	読み取り専用管理者	フルモニター管理者	ヘルプデスク管理者
構成済みドメインを取得	はい	はい	はい	いいえ
Secure Private Accessダッシュボードでユーザー、アプリケーション、アクセスポリシーのウィジェットを表示	はい	はい	はい	いいえ
Monitorダッシュボードでセッションとアプリケーションを表示する	はい	はい	はい	制限付き
レポートツールにアクセスする	はい	いいえ	はい	制限付き

管理者へのロールベースアクセスを有効にする

管理者へのロールベースアクセスを有効にするには、次の手順を実行します。

1. Citrix Cloud™にサインインした後、メニューから**IDおよびアクセス管理**を選択します。
2. **IDおよびアクセス管理**ページで、**管理者**をクリックし、**管理者/グループの追加**をクリックします。コンソールには、アカウント内の現在の管理者がすべて表示されます。
3. **管理者またはグループの追加**で、管理者を選択するIDプロバイダーを選択します。場合によっては、Citrix Cloudから最初にIDプロバイダー（例: Azure Active Directory）にサインインするよう求められることがあります。
4. 「**Citrix Identity**」が選択されている場合は、ユーザーのメールアドレスを入力し、「**次へ**」をクリックします。
5. 「**カスタムアクセス**」を選択し、「**Secure Private Access**」の「**>**」アイコンをクリックします。
6. 次のいずれかの役割を選択し、「次へ」をクリックします。

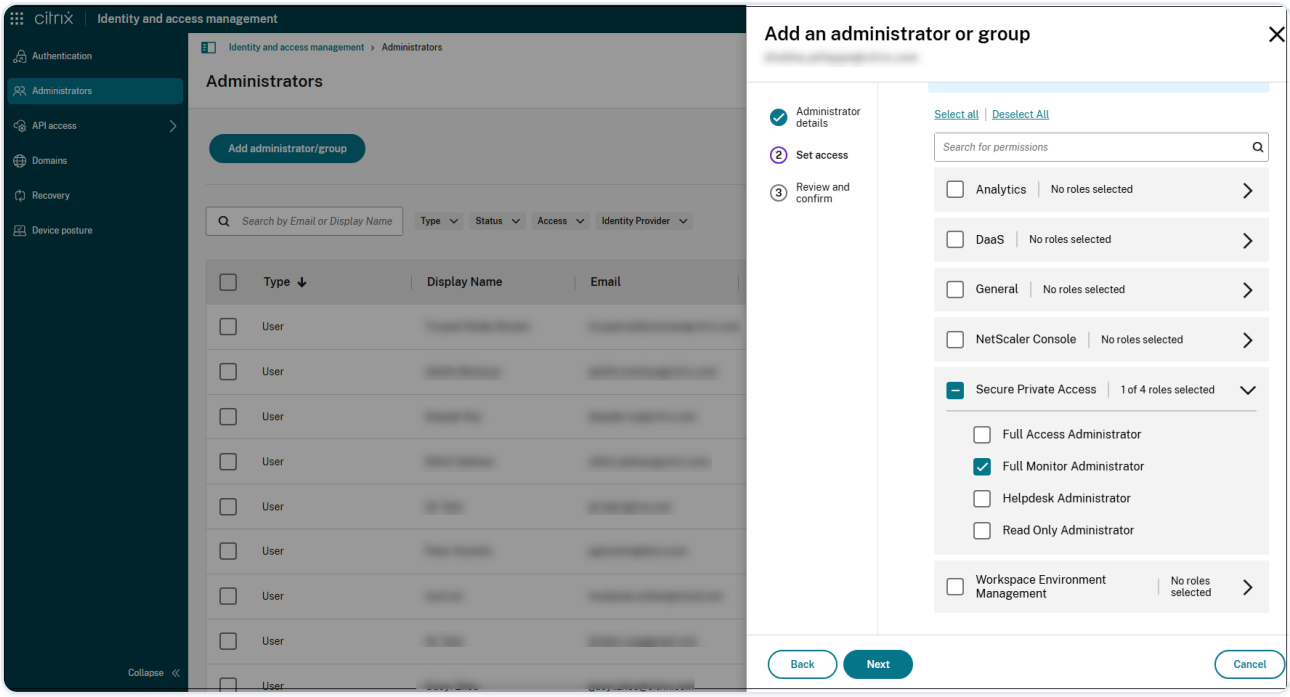
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- フルアクセス管理者
- 読み取り専用管理者
- フルモニター管理者
- ヘルプデスク管理者

7. 「**招待状を送信**」をクリックします。

注：

すべてのSecure Private Accessの役割に対して、**Analytics**サービスと**General**サービスを有効にする必要があります。**Analytics**サービスは監視とレポート作成に必要であり、**General**サービスは認証、ドメイン、承認、トラフィックルーティング、その他の機能に必要です。



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

マルチセッション仮想デスクトップインフラストラクチャのサポート

マルチセッション仮想デスクトップインフラストラクチャ (VDI) では、複数のユーザーが個別のデスクトップ環境を維持しながら仮想マシンを共有します。Citrix Secure Access client for Windows リリース 24.8.1.19 以降、各ユーザーのセッションが分離され、プライベートで保護されていることを確認することで、Secure Private Access の展開向けマルチセッション VDI からエンタープライズアプリケーションにアクセスできます。

マルチセッション VDI ワークフロー(/en-us/citrix-secure-private-access/media/vdi-process.png)

注:

- マルチセッション VDI は、Windows 10 および Windows Server 2019 以降の Windows OS でサポートされています。
- マルチセッション VDI は、Azure ベースの VDI でのみ機能します。

主な機能と利点

- **認証:** 条件ベースの認証を含む、さまざまな認証方法をサポートします。
- **コンテキストアクセス:** 場所、デバイス、グループなどの要因に基づいて、Secure Private Access ポリシーに従って、承認されたアプリケーションのみへのユーザーアクセスを許可します。
- **コスト削減:** 複数のユーザーがコンピューターを共有できるため、組織はハードウェアコストを節約できます。Citrix Secure Access™ client for Windows アプリは、ユーザーがあらゆるデバイスから仮想デスクトップにアクセスできるようにすることで、これらのコスト削減をさらに強化し、エクスプレスルートやレガシー VPN に依存することなく、専用ワークステーションの必要性を低減します。
- **柔軟性の向上:** 承認されたアプリケーションアクセスのみを許可する Secure Private Access ポリシーに従って、エンドユーザーがどこからでも接続できるようにします。

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

マルチセッション VDI を有効にする

Citrix Secure Access client for Windows アプリでマルチセッション VDI サポートを有効にするには、管理者は、Citrix Secure Access client for Windows 24.8.1.19 以降がマルチセッション OS マシンにインストールされていることを確認する必要があります。

管理者は、マルチセッション OS マシンのユーザーにコンテキストアクセスを提供するために、次の手順を実行する必要があります。

1. **レジストリエディター** (**regedit.exe**) を開きます。
2. 「**HKEY_LOCAL_MACHINE\Software\Citrix\Secure Access Client**」に移動します。
3. マルチセッションVDIを有効にするには、`EnableMultiSessionFlow`と`EnableWFP`のレジストリを作成します。詳細については、「NetScaler Gateway Windows VPNクライアントレジストリキー」を参照してください。
4. **レジストリエディター**を閉じます。
5. 設定を有効にするには、マシンを再起動します。

ドメインコントローラーのIPアドレスがDNSのIPアドレスと同じであるドメイン参加済みマシンでは、管理者はマルチセッションVDIを有効にするために次の手順を実行する必要があります。

1. **レジストリエディター** (**regedit.exe**) を開きます。
2. 「**HKEY_LOCAL_MACHINE\Software\Citrix\Secure Access Client**」に移動します。
3. マルチセッションVDIを有効にするには、`EnableMultiSessionFlow`と`AlwaysOnService`のレジストリを作成します。詳細については、「NetScaler Gateway Windows VPNクライアントレジストリキー」を参照してください。
4. タイプ**REG_SZ**の`CloudAlwaysOnUrl`レジストリを作成し、接続URLを指定します。
5. **レジストリエディター**を閉じます。
6. 設定を有効にするには、マシンを再起動します。
7. Secure Private Accessダッシュボードで、ドメインコントローラーとクラウドコネクターのアプリケーションを作成します。

> **注：**
>
> ドメインコントローラーのIPアドレスがDNSのIPアドレスと同じ場合、ドメインコントローラーへのすべての呼び出しは傍受され、破棄されます。ドメインコントローラーのパケットが破棄されるのを避けるため、アプリケーションを作成し、すべてのユーザーへのアクセスを有効にすることをお勧めします。

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

8. DNSサーバーのIPアドレスと一致するドメインコントローラーのIPアドレスを、すべてのTCP/UDPポートを許可した状態でアプリケーションに追加します。
9. すべてのユーザーがドメイン コントローラーにアクセスできるように、アクセス ポリシーを設定します。
10. クラウド コネクタのホスト名がサフィックスと一致する場合 (例: クラウド コネクタのホスト名が cloudconnector.cloud.com で、サフィックスが *.cloud.com の場合)、トンネル化を防ぐために、クラウド コネクタをトラフィックルーティングタイプ **External** に追加します。

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

モバイルデバイス用 Citrix Secure Private Access

Citrix Secure Private Access の展開は、iOS 用 Secure Access Client バージョン 25.08.1 および Android 用 Secure Access Client バージョン 25.11.1 以降のモバイルデバイスでサポートされています。モバイルユーザーは、Secure Private Access のゼロトラストモデルの下で企業アプリケーションやWebリソースにアクセスでき、デスクトップユーザーと同じセキュリティ制御、ポリシー適用、シームレスなエクスペリエンスが提供されます。

サポートされているバージョンとプラットフォーム

iOS デバイス:

- **CSA クライアント**: iOS 25.08.1 (App Store で入手可能)
- **iOS OS バージョン**: 最小 iOS 16
- **展開モデル**
  - クラウド展開用 Secure Private Access
  - ハイブリッド展開用 Secure Private Access

Android デバイス:

- **CSA クライアント**: Android 25.11.1 (Google Play ストアで入手可能)
- **Android OS バージョン**: 最小 Android 12
- **展開モデル**
  - クラウド展開用 Secure Private Access
  - ハイブリッド展開用 Secure Private Access

サポートされる機能

Secure Private Accessの展開では、リソースアクセスはポリシー構成によって制御されます。管理者は、特定の条件の下で、承認されたデバイスまたは場所から、どのユーザーまたはグループが特定のアプリケーションおよびリソースにアクセスできるかを指定するポリシーを定義できます。

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

- セキュアプライベートアクセス ポリシーの条件に従って、ウェブ、SaaS、およびTCP/UDPアプリケーションにアクセスできます。
- セッションセキュリティポリシー: Chrome Enterpriseでサポートされるデータ損失防止 (DLP) コントロール。

サポートされている機能の完全なリストについては、「NetScaler GatewayでサポートされるCitrix Secure Accessクライアントの機能」を参照してください。

前提条件

Secure Private Accessサービスが構成され、最新の状態になっている必要があります。詳細については、以下のトピックを参照してください。

- シトリックス セキュアプライベートアクセス の概要
- Secure Private Accessのオンボーディングとセットアップ
- アプリの構成と管理

Citrix Secure Accessクライアントを使用するiOSおよびAndroidユーザーのワークフロー

次の手順は、Citrix Secure Accessクライアントを使用するiOSおよびAndroidデバイスのユーザー向けのSecure Private Accessフローをまとめたものです。

- **Citrix Secure Accessクライアントのインストール**: Citrix Secure Accessクライアントはモバイルデバイスにインストールする必要があります。これは、企業デバイスの場合はモバイルデバイス管理 (MDM) を介して、またはユーザーがデバイスのアプリストアからアプリケーションを手動でダウンロードすることによって実現できます。
- **ストア/ゲートウェイURLへのアクセス**: ユーザーは指定されたストアまたはゲートウェイURLにアクセスします。このURLは、組織のリソースにアクセスするためのエントリポイントとして機能します。
- ユーザー認証: ユーザーは自身のIDを認証するよう求められます。これには通常、ユーザー名とパスワードなどの資格情報の入力、または多要素認証 (MFA) メソッドの使用が含まれます。
- **ポリシー評価とアクセス許可**:
  - ポリシーが満たされた場合: ユーザーの認証とデバイスのポスチャが定義されたセキュリティポリシーを満たしている場合、アクセスが許可されます。これにより、ユーザーは承認されたWeb、SaaS、およびプライベートWebアプリケーションにアクセスできます。

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

  - ポリシーが失敗した場合: ユーザーがポリシー要件を満たさない場合（例: 古いオペレーティングシステム、未承認のデバイス、誤った資格情報）、ポリシー設定に応じて、アクセスが制限されるか、完全に拒否されます。

- **強制セッション保護**: アクセスが許可されると、Chrome Enterpriseでサポートされているデータ損失防止 (DLP) コントロールが適用されます。例:
  - シークレットモードの無効化
  - 印刷のブロック
  - URLフィルタリング
  - ダウンロードのブロック
  - 構成済み（管理対象）ブックマーク

関連トピック

- クラウド展開向けCitrix Secure Private Access
- ハイブリッド展開向けCitrix Secure Private Access

iOS Kerberos拡張機能を使用したKerberos認証

このトピックでは、Citrix Secure Access for iOSアプリを介して、社内Webアプリ向けにKerberosベースのシングルサインオン (SSO) を有効にするために必要なエンドツーエンドの構成について概説します。

- iOSクライアントの構成
- MDMサーバーの構成
- IISの構成
- ドメインコントローラーの構成

iOSクライアントの構成

以下のセクションでは、iOSクライアントの構成に関する詳細情報を提供します。

前提条件

iOSデバイスがMDMに登録されていることを確認してください。 SSO構成を適用する前に、iOSデバイスがMDMソリューション（例：Microsoft Intune）に登録されている必要があります。MDM登録により、Kerberos SSO拡張プロファイルをデバイスにプッシュできます。

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

iOSデバイスでのMDM登録の検証

1. iOSデバイスで、**設定 > 一般 > VPNとデバイス管理** に移動します。

   デバイス管理の下に、組織のMDMプロファイル（例：Microsoft Intuneまたは会社のMDMプロファイル名）がリストされていることを確認する必要があります。

2. プロファイルをタップして、インストールされていること、およびステータスが **確認済み** または **インストール済み** と表示されていることを確認します。

3. Kerberos SSO拡張機能がMDMによってプッシュされたことを確認するには：

   - 「**設定 > 一般 > VPNとデバイス管理**」に移動します。
   - MDMプロファイルをタップし、プロファイルの詳細で「**シングルサインオン拡張機能**」または「**Kerberos**」を探します。
   - または、「**設定 > 一般 > VPNとデバイス管理 > シングルサインオン**」に移動し、Kerberos拡張機能がリストされていることを確認します。

   デバイスが登録されていないか、プロファイルが見つからない場合は、続行する前にMDM管理者に連絡してデバイスを登録してください。

MDMサーバーの構成

注:

MDM SSO拡張機能ペイロードの構成は、Appleの公式ドキュメントに基づいています。

- Appleデバイスのシングルサインオンデバイス管理ペイロード設定
- AppleデバイスでのKerberosシングルサインオン拡張機能

MDM SSO拡張機能ペイロードで、以下のフィールドが構成されていることを確認してください。

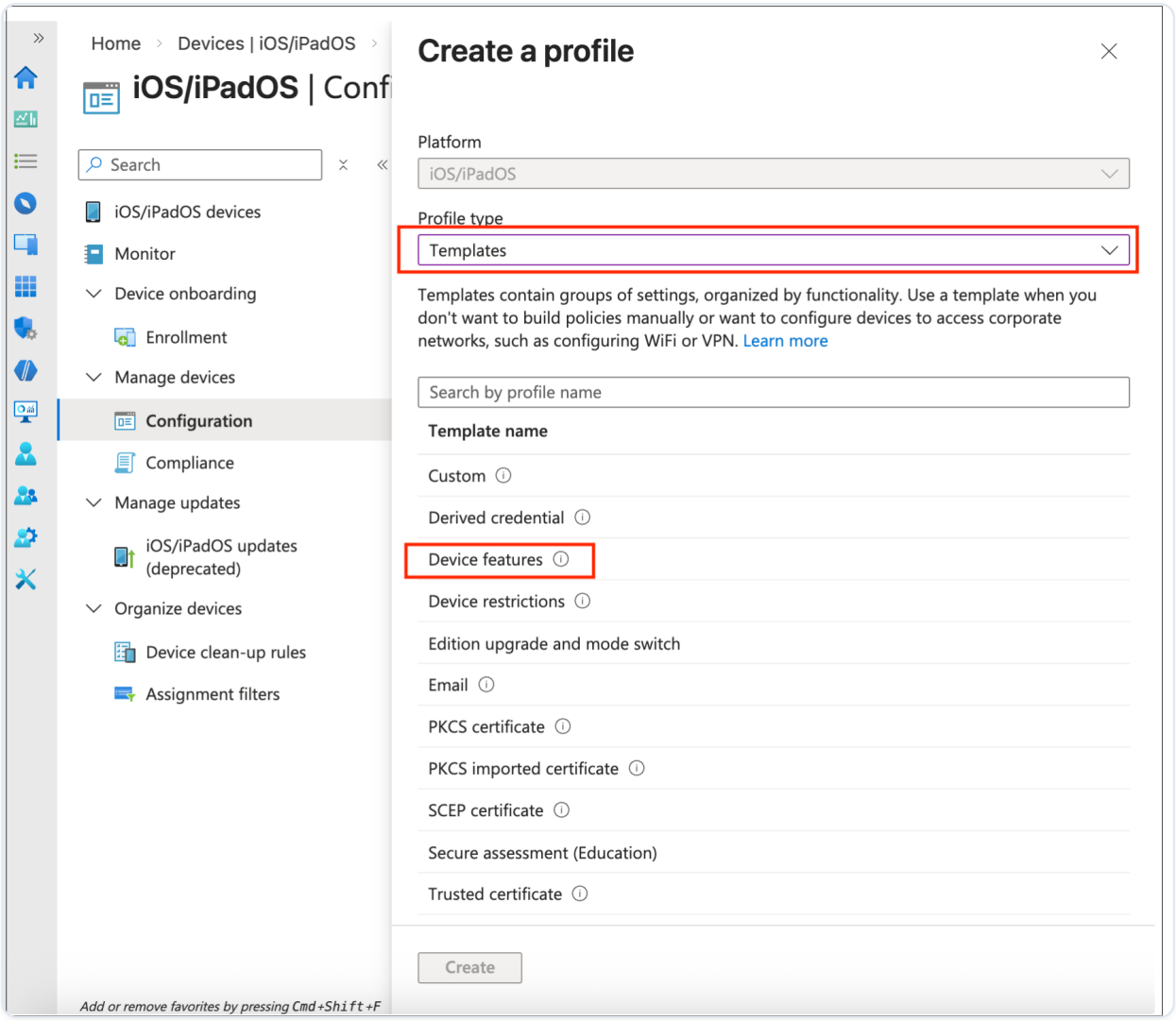
1. **ドメイン:** Kerberosに使用されるURL。
2. **AppBundleIDs:** 使用されるアプリの許可リスト。(例: Chrome: `com.google.chrome.ios`、Citrix Secure Access: `com.citrix.securehub`)
3. **レルム:** データセンターの場所。

Intuneポリシーの構成

前提条件: iOSデバイスがIntuneに登録されていることを確認してください。

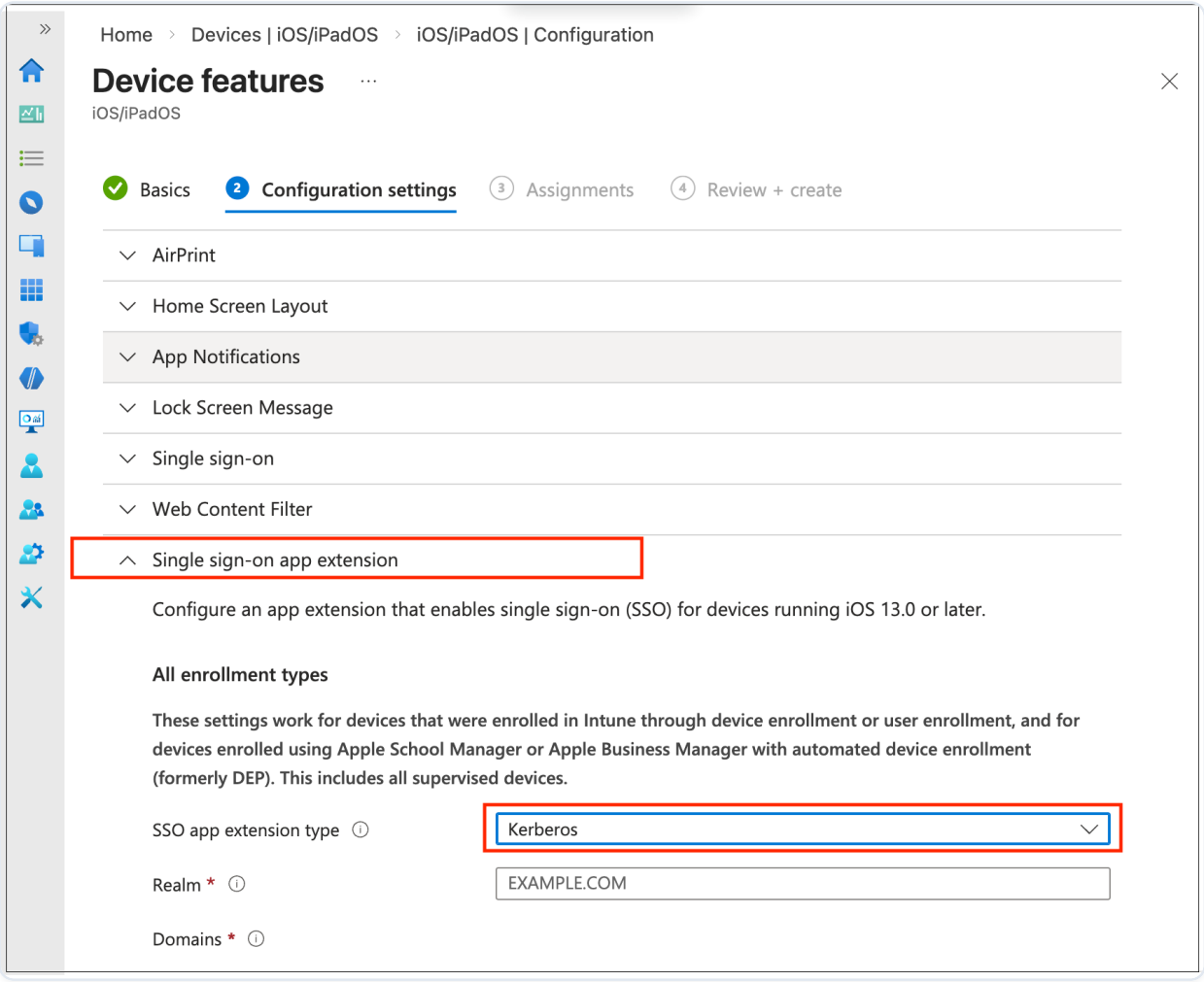
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In the Intune Admin console, go to **ホーム > デバイス | iOS/iPadOS → iOS/iPadOS | 構成**.
2. 新しいポリシーを作成します。
3. **プロファイルの種類**で**テンプレート**を選択し、次に**デバイスの機能**を選択します。



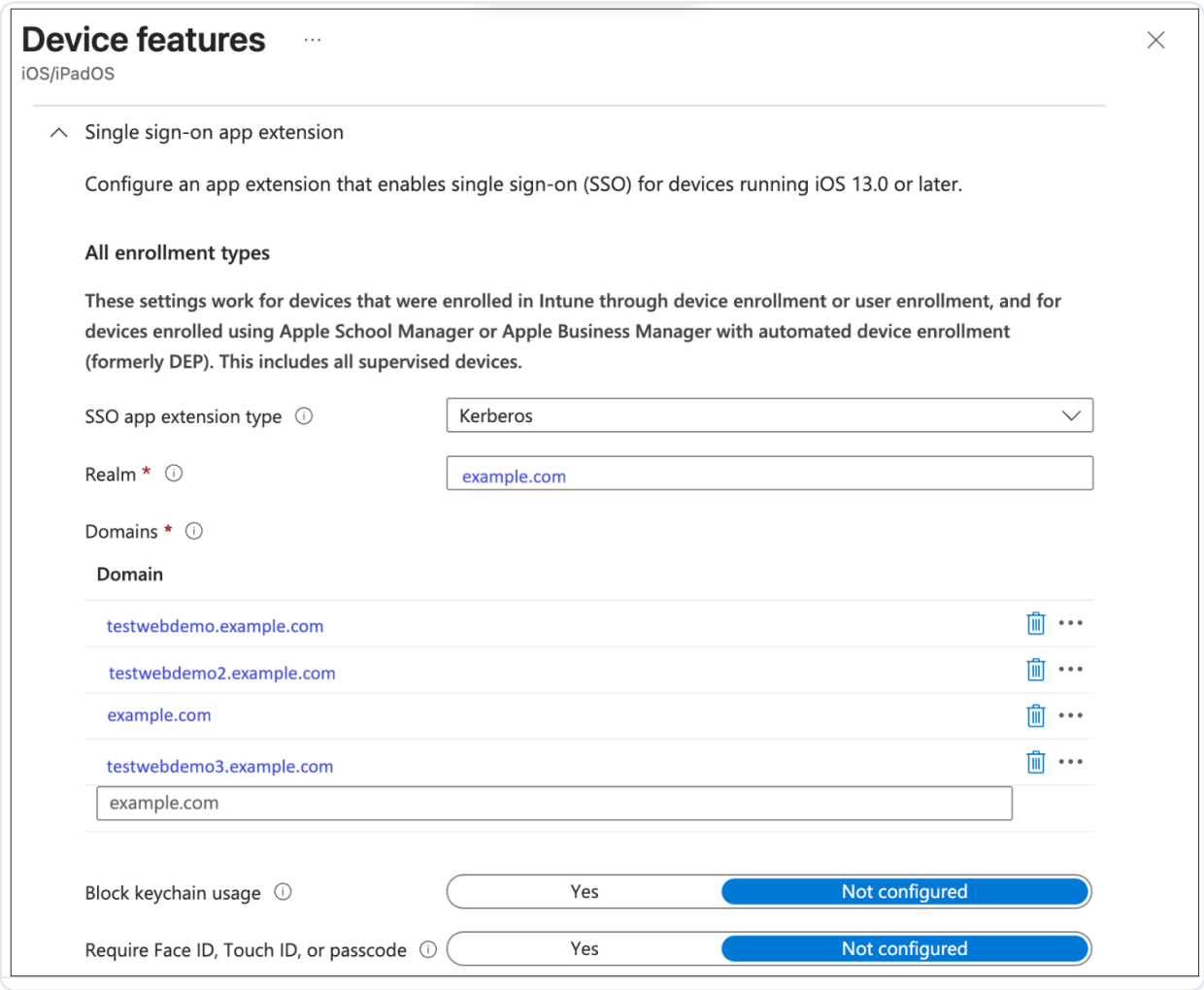
4. **作成**を押します。
5. ポリシーの名前を入力し、**構成設定**に進みます。
6. **シングルサインオンアプリ拡張機能 > SSOアプリ拡張機能の種類**で**Kerberos**を選択します。

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

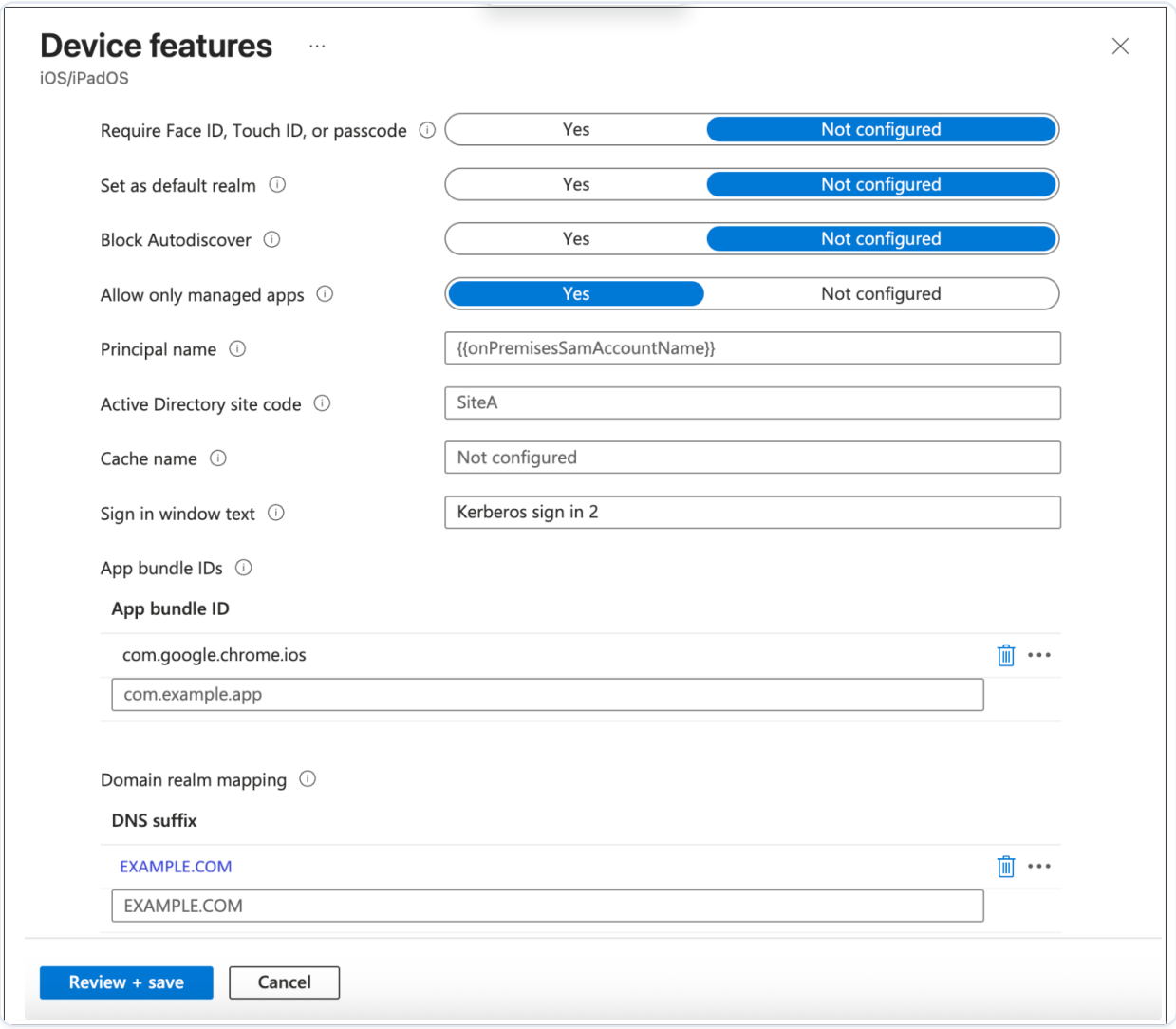


7. セットアップ要件に従って情報を入力します。

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



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



8. **確認 + 保存**を押します。
9. ポリシーをデバイスにバインドします。
   - **ポリシーの編集**に移動し、ポリシーをクリックします。
   - **割り当て**を編集します。
   - デバイスグループを選択します（まだ作成していない場合は、まずデバイスでデバイスグループを作成してください）。
10. デバイスを同期します。

IIS構成

IIS Webサーバーで、Kerberosベースの認証を強制するために、Negotiateプロバイダーを使用して**Windows認証**を有効にし、**匿名認証**を無効にします。

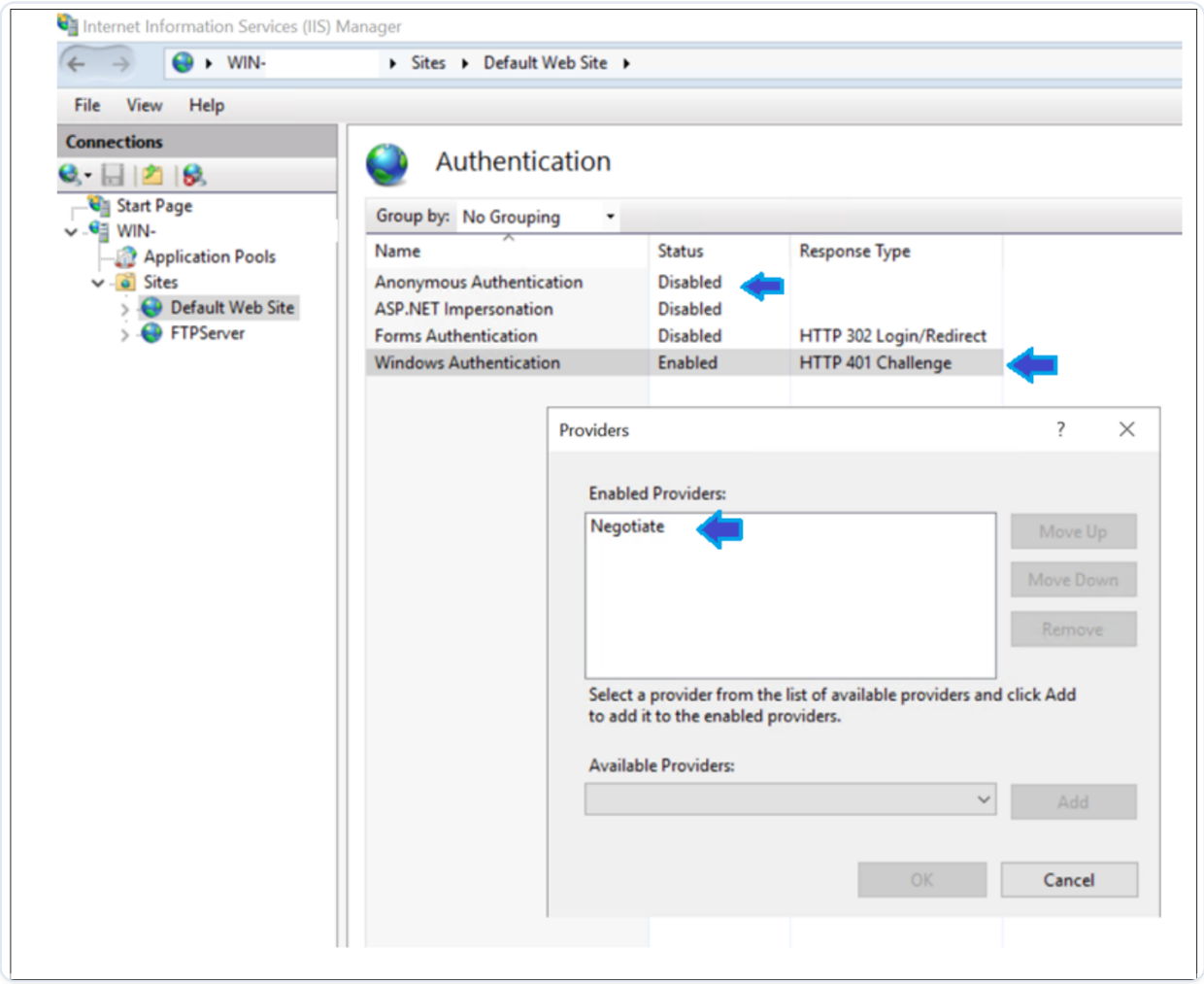
IIS認証を構成する手順：

1. IISマネージャーを開きます（**ファイル名を指定して実行**または**スタート**から**inetmgr**）。

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

2. 「**接続**」ペインで、構成するサイトまたはアプリケーションを選択します。
3. 機能ビューのIISセクションで、**認証**をダブルクリックします。
4. **匿名認証**を無効にします。
   - **匿名認証**を選択し、「**操作**」ペインで**無効**をクリックします。
5. **Windows認証**を有効にします。
   - **Windows認証**を選択し、「**操作**」ペインで**有効**をクリックします。
6. Negotiateプロバイダーを設定します。
   - **Windows認証**が選択されている状態で、「**操作**」ペインで**プロバイダー…**をクリックします。
   - **Negotiate**が最初にリストされていること（NTLMの上）を確認します。不足している場合は追加します。
   - 「**OK**」をクリックします。
7. 変更を保存するには、「**Actions**」ペインで「**Apply**」をクリックします。
8. 必要に応じて、管理者権限のコマンドプロンプトから `iisreset` を実行して、設定をすぐに適用します。

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



ドメインコントローラー側の構成

短縮名とFQDNのSPN登録: Kerberosでは、クライアントが使用するURLとドメイン上の登録済みSPNとの正確な一致が必要です。`http://testwebdemo` にアクセスするクライアントは、`http://testwebdemo.example.com` にアクセスするクライアントとは異なるSPNを使用するため、両方を登録する必要があります。

1. 以下の `<dc-hostname>` をドメインコントローラーのホスト名に置き換えます。
2. 両方の形式を登録します。

   - 短縮ホスト名 (クライアントが短縮名でアクセスする場合に使用されます。例: `http://testwebdemo`)

     ```
     setspn -s HTTP/testwebdemo example.com\<dc-hostname>
     ```

   - FQDN (クライアントが完全修飾ドメイン名でアクセスする場合に使用されます。例: `http://testwebdemo.example.com`)

     ```
     setspn -s HTTP/testwebdemo.example.com example.com\<dc-hostname>
     ```

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

3. 両方が正しいアカウントに登録されていることを確認します
    - setspn -L example.com\<dc-hostname> の設定
4. 期待される出力には両方を含める必要があります:
    - HTTP/testwebdemo の値
    - HTTP/testwebdemo.example.com

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

機能の非推奨化

この記事では、段階的に廃止されるSecure Private Accessサービス機能について事前にお知らせし、お客様がタイムリーなビジネス上の意思決定を行えるようにします。Citrixは、機能がいつ廃止されるかを判断するために、お客様の使用状況とフィードバックを監視しています。発表は、その後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」を参照してください。

次の表に、非推奨または非推奨予定のSecure Private Accessサービス機能を示します。

項目	非推奨の発表時期	非推奨日	代替策
Webアプリアクセス用のクライアントレスVPNアクセス方法	2023年1月	October 17, 2023	ユースケースに応じて、Citrix Enterprise BrowserまたはDirect Accessを使用してください。詳細については、「Webアプリアクセス用のクライアントレスVPNアクセスの非推奨について」を参照してください。
カテゴリベースのWebフィルタリング	2022年12月	December 31, 2022	Secure Private AccessにおけるWebサイトごとの許可、拒否、またはRBIリダイレクト機能は、Citrix Enterprise Browserから業務に関係のないWebサイトへの選択的なアクセスを提供するために維持されます。

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

項目	非推奨の発表時期	非推奨日	代替策
ナビゲーションセキュリティ制御の制限	2022年4月	15 June 2022	NA
Citrix Gateway コネクタ	2022年5月	30 September 2022	Connector Appliance。Gateway ConnectorをConnector Applianceに移行するには、「Gateway ConnectorをConnector Applianceに移行する」を参照してください。

Webアプリアクセスのクライアントレス VPNアクセスの廃止について

- クライアントレスVPN（clientless VPN）アクセス方法とは何ですか？

  Citrix Secure Private Access™は、強化されたセキュリティ制限なしで構成された内部Webアプリが、Webブラウザでストア URLを介してアクセスされる場合に、CVPNベースのアクセス方法を使用します。

  注：

  クライアントレスVPNアクセス方法は、内部アプリがWebブラウザでストアURLを介してアクセスされる場合にのみ使用されます。強化されたセキュリティ制限が構成されていないアプリのみがブロックされます。

- この機能を廃止する理由は何ですか？

  クライアントレスVPN方式は、クライアント側のURL書き換えを使用しており、これには業界全体で特定の技術的制限があります。いくつかのケースでは、Webアプリ内の特定のリンクが書き換えられると、アプリへのアクセス障害を引き起こす可能性があります。これは、エンドユーザーエクスペリエンスの低下につながります。お客様に最高のアプリアクセスエクスペリエンスを提供するために、この機能を廃止し、以下の代替案のいずれかに移行することをお勧めします。

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

- Secure Private Accessが構成されたアプリケーションにアクセスするエンドユーザーにどのような影響がありますか？

  強化されたセキュリティ制限なしで構成されたWebアプリが、Webブラウザからストア URL経由でアクセスされた場合、そのアプリケーションへのアクセスはブロックされます。 Citrix Workspaceアプリ、Direct Access、Remote Browser Isolationサービス (RBI)、またはSecure Access Agentを介してアプリケーションにアクセスするエンドユーザーには影響しません。

- 代替手段は何ですか？管理者は何をすべきですか？

  Citrix Enterprise Browser: Citrix Workspaceアプリを使用して、Citrix Enterprise Browser経由でこれらのアプリケーションにアクセスします。この方法では、強化されたセキュリティ設定（ダウンロード制限、印刷制限、ウォーターマーク、クリップボードアクセス制限など）とブラウザ管理により、最高のエンドユーザーエクスペリエンスが提供されます。 **Direct Access:** Webアプリケーションにクライアントレスでアクセスしたい場合は、Chromeなどのネイティブブラウザから直接アプリにアクセスできるDirect Accessメソッドを使用します。この方法は、エンドデバイスにCitrix Workspaceアプリをインストールできない場合や、管理されていないデバイスのユースケースで使用できます。詳細については、「エンタープライズWebアプリへの直接アクセス」を参照してください。

- Citrix WorkspaceアプリまたはSecure Access Agent経由でアクセスされる既存のアプリケーションに影響はありますか？

  いいえ、Webブラウザで開かれたストアURL経由でアクセスされるWebアプリケーションへのアクセスのみをブロックします。この非推奨化は、Citrix Workspaceアプリまたはエンドデバイスにインストールされているの Secure Accessクライアント経由でアクセスされるアプリには影響しません。強化されたセキュリティ制限が構成されているWebアプリケーションがWebブラウザ経由でアクセスされた場合、それらのアプリケーションへのアクセスはブロックされます。

- 他にご質問がありますか？

  Citrix Supportにお問い合わせください。

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

データガバナンス

このトピックでは、Citrix Secure Private Accessサービスによるログの収集、保存、および保持に関する情報を提供します。定義セクションで定義されていない大文字の用語は、Citrixエンドユーザーサービス契約で指定された意味を持ちます。

データレジデンシー

Citrix Secure Private Accessは、高可用性と冗長性を確保するマルチリージョンアーキテクチャを採用しています。詳細については、Points of Presenceを参照してください。

- 米国東部
- 米国西部
- ブラジル南部
- 東南アジア
- 北ヨーロッパ
- 西ヨーロッパ
- オーストラリア東部
- インド南部

以下は、サービス構成ログとランタイムログの異なる保存先です。

- システム監視およびデバッグログ用のSplunkサービス（米国ロケーションのみ）。
- 診断およびユーザーアクセスログ用のCitrix Analytics Service。詳細については、Citrix Analytics Service Data Governanceを参照してください。
- 集約されたユーザーアクセスログについては、Citrix Application Delivery Management Service、詳細についてはCitrix ADM Data Governanceを参照してください。
- 管理者監査ログについては、Citrix Cloud™ System Logs Service、以下のリンクを参照してください。

Citrix Cloud Servicesに関する一般情報については、Citrix Cloud Services Customer Content and Log HandlingおよびGeographical Considerationsを参照してください。

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

データ収集

Citrix Secure Private Accessを使用すると、管理者は一元化された管理インターフェイスを通じて、サービスおよび関連するConnector Applianceを構成および管理できます。このサービスは、以下の種類の顧客データを処理します。

- Secure Private Accessサービスの場合
  - 顧客のプライベートアプリケーションおよびSaaSアプリケーション
  - Webアプリまたはその両方のFQDNとURL
  - IPアドレス/範囲、ポート、およびプロトコル
  - 関連するリソースの場所
  - WebおよびSaaSアプリのシングルサインオンパラメーター
- アプリのエンタイトルメントのユーザー識別子
- アダプティブアクセス ポリシーの条件
  - ユーザーID
  - ユーザー/デバイスの地理的位置
  - ユーザー/デバイスのネットワークロケーション（Citrix Cloudネットワークロケーション構成による）。詳細については、「Direct Workload Connection を使用してストアへの接続を最適化する」を参照してください。
  - デバイスの種類
- Connector Appliance Platform については、Secure Private Access に関連する「Connector Appliance for Cloud Services」を参照してください。
  - IPアドレスまたはFQDN
  - ユーザー、デバイス、およびリソースロケーション識別子
  - 内部プロキシ構成

サービスコンポーネントによって収集されるランタイムログの主要情報は、次のとおりです。

- ユーザー名
- ユーザーオブジェクトID
- ユーザーのメールアドレス
- ユーザーUPN
- ユーザーグループメンバーシップ

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

- クライアントIPアドレスとポート
- 宛先FQDN/アドレスとポート
- クライアントユーザーエージェント
- アプリケーション名
- アプリケーションURLパス
- アプリケーションのアクセス時間と期間
- リクエストバイト数
- レスポンスバイト数
- 未承認アプリケーションに対するWebフィルタリングの決定
- HTTPトランザクションID

Citrix Analytics Serviceに送信されるデータの包括的なリストについては、Citrix Analytics Service データガバナンスを参照してください。

データ転送

Citrix Secure Private Accessは、トランスポート層セキュリティによって保護された宛先にログを送信します。

データ制御

Citrix Secure Private Accessサービスは現在、顧客がログの送信をオフにしたり、顧客コンテンツがグローバルに複製されるのを防ぐためのオプションを提供していません。

データ保持

Citrix Cloudのデータ保持ポリシーに基づき、顧客の設定データはサブスクリプションの有効期限が切れてから90日後にサービスから削除されます。

ログの宛先は、サービス固有のデータ保持ポリシーを維持します。

- Analyticsログの保持ポリシーの詳細については、データガバナンスを参照してください。
- Citrix Application Delivery Managementに保存されているイベントについては、データガバナンスを参照してください。
- Splunkログはアーカイブされ、90日後に最終的に削除されます。

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

データのエクスポート

ログの種類ごとに異なるデータエクスポートオプションがあります。

- 管理者監査ログは、Citrix Cloudシステムログコンソールからアクセスできます。
- Secure Private Access Serviceの診断ログは、Citrix Analytics ServiceからCSVファイルとしてエクスポートできます。
- Splunkログは、お客様が利用するためのものではありません。これらのイベントは、SplunkからCSVファイルとしてエクスポートすることもできます。

定義

- お客様のコンテンツとは、ストレージのためにお客様のアカウントにアップロードされたデータ、またはCitrixがサービスを実行するためにアクセスを許可されたお客様の環境内のデータを意味します。
- ログとは、パフォーマンス、安定性、使用状況、セキュリティ、サポートを測定する記録を含む、サービスに関連するイベントの記録を意味します。
- サービスとは、Citrix Analyticsの目的のために前述したCitrix Cloudサービスを意味します。

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

製品認定とコンプライアンス

Citrix Secure Private Accessは、組織がネットワークをインターネットに直接公開することなく、ユーザーをアプリケーションに安全に接続できるようにするゼロトラストネットワークアクセス（ZTNA）ソリューションです。Secure Private Accessは、より広範なCitrix CloudおよびハイブリッドサービスポートフォリオのIの一部として提供され、Citrixのクラウドサービスコンプライアンスおよび監査プログラムによって管理されています。

このページでは、Secure Private Accessに適用される認定とコンプライアンス証明を要約しています。

認定と監査

- **SOC 2® タイプ 2:**

  Secure Private Accessは、CitrixのSOC 2 Type 2監査プログラムの対象です。

  SOC 2 Type 2監査では、Secure Private Accessを含むCitrix Cloudサービスに適用されるセキュリティ、可用性、機密性、処理の完全性、およびプライバシー管理が評価されています。

- **ISO 27001 & ISO 27701:**

  Secure Private Accessは、CitrixのISO 27001（情報セキュリティ管理）およびISO 27701（プライバシー情報管理）認定サービスポートフォリオに含まれています。

  これらの世界的に認められた認定は、セキュリティおよびプライバシー管理の実践が正式に確立され、文書化され、継続的に改善されていることを証明しています。

- **HIPAA:**

  Secure Private Accessは、適切に構成および契約された場合、HIPAAコンプライアンスを必要とする環境での使用に適しています。Citrixのクラウドコンプライアンスドキュメントは、Secure Private Accessに対するHIPAAの適用可能性を示しています。

- **PCI DSS 4.0:**

  Secure Private Accessは、該当するクラウドサービスに対するCitrixの年次PCI DSS評価に含まれています。PCIスコープ環境でSecure Private Accessを展開するお客様は、PCI要件を満た

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

すために追加の制御を実装する必要がある場合があります。PCI DSSコンプライアンスは、Citrixとお客様間の共有責任モデルに従います。

- **FIPS / コモンクライテリア:**

  Secure Private Accessは、FIPS認定またはFIPS対応のNetScalerプラットフォームと、Citrix Workspaceアプリで使用されるFIPS認定のCitrix CryptoKitを組み合わせることで、FIPS準拠ソリューションの一部として展開できます。

  Common Criteriaについては、Secure Private AccessはCommon Criteria (NDcPP) 認定のNetScalerプラットフォームおよびCommon Criteria認定のCitrix Workspaceアプリと統合され、ソリューションレベルでCommon Criteria要件に準拠した展開を可能にします。

- **オーストラリア IRAP (情報セキュリティ登録評価者プログラム):**

  Secure Private Accessは、認定されたオーストラリア政府の評価者によるIRAP評価を受けるCitrixのクラウドサービスに含まれています。

  IRAPは、Citrix Cloudサービスがオーストラリア政府情報セキュリティマニュアル (ISM) のセキュリティ管理に準拠していることを独立して検証します。

証明書と監査レポート

利用可能な証明書と監査レポートは、Citrix Trust Centerからダウンロードしてください。

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

index

- Gateway ConnectorからConnector Applianceへの移行
- 同じ関連ドメインに起因する競合を解決するためのルートテーブル
- Citrix Workspaceアプリ経由でのCitrix Secure Access™クライアントへのシングルサインオン
- ADFSとセキュア プライベート アクセスの統合
- シトリックス セキュア プライベート アクセス™
- アプリケーション固有のリソースロケーションにDNSクエリをルーティングする
- G Suite を構成する
- Jira の構成
- O365を構成する
- ERP Cloudを構成する
- ServiceNow を構成する
- Tableau を構成する
- Workday の構成
- Zoom を構成する
- アクセスモードベースのポリシー適用
- サーバーからクライアントへの接続のサポート - プレビュー

Gateway ConnectorからConnector Applianceへの移行

Citrix Gateway Connector™は非推奨になりました。Citrixは、環境でCitrix Gateway Connectorを使用しているお客様に対し、Citrix Gateway Connectorで以前サポートされていたすべてのSecure Private Accessユースケースに Connector Applianceの展開を開始することを推奨します。このトピックでは、Gateway ConnectorをConnector Applianceに移行するためのガイドラインを提供します。

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

Gateway ConnectorをConnector Applianceに移行するための大まかな手順

1. Gateway Connectorに加えて、同じリソースロケーションにConnector Applianceをインストールします。
2. Gateway Connectorをシャットダウンし、既存のWebアプリの接続をテストします。同じリソースロケーションでホストされているWebアプリにアクセスできるか確認します。
3. テストが完了したら、Citrix Gateway Connectorを削除します。

Connector Applianceをインストールするには

Connector Applianceをインストールするには、次の手順を使用します。

1. Citrix Cloudにサインインします。
2. 画面左上のメニューから、**リソースロケーション**を選択します。
3. Connector Applianceを追加するリソースロケーションのConnector Applianceの横にあるプラスアイコンをクリックします。
4. ハイパーバイザーを選択し、**イメージのダウンロード**をクリックします。
5. ハイパーバイザーにConnector Applianceをダウンロードしてインストールします。
6. Web UI（ハイパーバイザーのコンソールに表示されるIPアドレス）にログインし、必要に応じてプロキシを設定します。
7. **登録**ボタンをクリックして、ショートコードを取得します。
8. Connector Applianceをダウンロードする際に使用した（ステップ5）Citrix Cloudユーザーインターフェイスに、ショートコードを貼り付けます。

   Connector Applianceが登録されました。

詳細な手順については、Connector Appliance for Cloud Servicesを参照してください。

よくある質問

- Connector Applianceをダウンロードするにはどうすればよいですか？

  Connector Applianceをダウンロードする。

- Connector Applianceをインストールするにはどうすればよいですか？

  Connector Applianceのインストール。

- Connector Applianceを登録するにはどうすればよいですか？

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

接続機器の登録。

- Connector Applianceの接続要件は何ですか？

  Connector Applianceのインターネット接続要件。

- Connector Applianceのシステム要件は何ですか？

  Connector Applianceのシステム要件。

- Connector Applianceはどのように更新されますか？

  コネクタ アプライアンスの更新

同じ関連ドメインに起因する競合を解決するためのルートテーブル

Citrix Secure Private Access™サービスのアプリケーションドメイン機能により、顧客はアプリケーションの関連ドメインを外部または内部でコネクタアプライアンス経由でルーティングできるようにするルーティング決定を行うことができます。

顧客がSaaSアプリと内部Webアプリの両方で同じ関連ドメインを設定しているとします。 たとえば、OktaがSalesforce（SaaSアプリ）とJira（内部Webアプリ）の両方のSAML IdPである場合、管理者は両方のアプリの設定で `*.okta.com` を関連ドメインとして構成する可能性があります。これにより競合が発生し、エンドユーザーは一貫性のない動作を経験します。このシナリオでは、管理者は要件に応じて、これらのアプリケーションを外部または内部でコネクタアプライアンス経由でルーティングするルールを定義できます。

ルートテーブルの仕組み

管理者は、トラフィックフローをどのように定義したいかに応じて、アプリに対して以下のルートタイプを定義できます。

- **内部 – プロキシバイパス** - ドメイントラフィックはCitrix Cloud Connector™を経由してルーティングされ、コネクタアプライアンスで構成された顧客のWebプロキシをバイパスします。
- **コネクタ経由の内部** - アプリは外部ですが、トラフィックはコネクタアプライアンスを介して外部ネットワークに流れる必要があります。
- **外部** – トラフィックはインターネットに直接流れます。

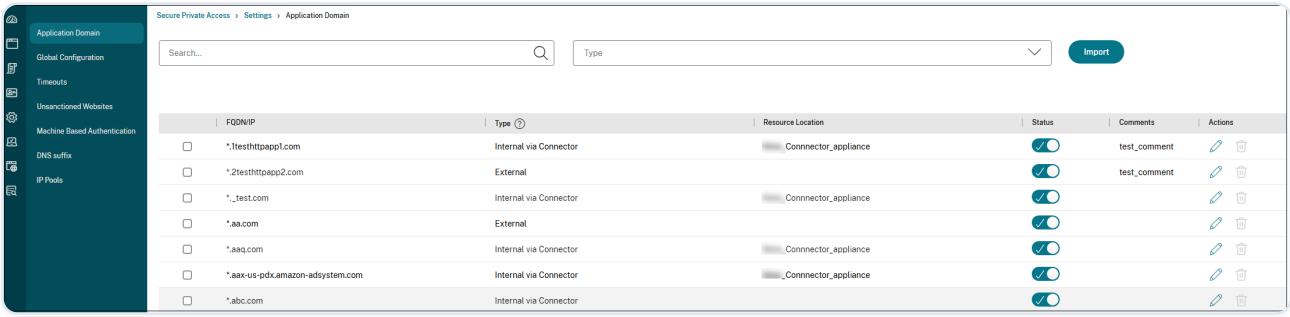
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

- ルートエントリは、アプリに構成されているセキュリティポリシーには影響しません。
- 管理者がルートテーブルのエントリを使用する意図がない場合、または対応するアプリが意図したとおりに動作しない場合、管理者はそのエントリを削除する代わりに無効にすることができます。
- 特定の顧客のすべてのコネクタアプライアンスは、アプリの種類に関係なく、SSO設定を取得します。以前は、特定のアプリのSSO設定はリソースの場所に紐付けられていました。

メインルートテーブル

Secure Private Accessコンソール（**設定 > アプリケーションドメイン**）のメインルーティングテーブルは、すべてのアプリケーションで構成されているドメインに関するすべての詳細を提供する表示専用のダッシュボードです。これは、任意のドメインについて以下の情報を確認するために使用できます。



メインルーティングテーブルを使用して、任意のドメインに関する以下の情報を確認できます。

- **FQDN/IP:** トラフィックルーティングの種類を設定したいFQDNまたはIPアドレス。
- **タイプ**: アプリの種類。アプリの追加時に選択された**内部**、**内部 – プロキシバイパス**、または**外部**。

重要:

競合がある場合、テーブルの該当する行にアラートアイコンが表示されます。競合を解決するには、管理者は三角形のアイコンをクリックし、メインテーブルからアプリの種類を変更する必要があります。

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

- **リソースロケーション: 内部**タイプのルーティングのリソースロケーション。リソースロケーションが割り当てられていない場合、該当するアプリの**リソースロケーション**列に三角形のアイコンが表示されます。アイコンにカーソルを合わせると、次のメッセージが表示されます。

  リソースロケーションがありません。このFQDNにリソースロケーションが関連付けられていることを確認してください。

- **ステータス: ステータス**列のトグルスイッチを使用して、アプリを削除せずにルートエントリのルートを無効にできます。トグルスイッチがオフの場合、ルートエントリは有効になりません。また、完全一致のFQDNが存在する場合、管理者は有効または無効にするルートを選択できます。
- **コメント:** コメントがあれば表示されます。
- **アクション:** 編集アイコンはリソースロケーションを追加したり、ルートエントリの種類を変更したりするために使用されます。削除アイコンはルートを削除するために使用されます。

ミニルーティングテーブル

アプリケーション構成中にルーティングの決定を行うために、アプリケーションドメインテーブルのミニバージョンが利用可能です。ミニルーティングテーブルは、Citrix Secure Private Access サービスのユーザーインターフェイスの**アプリ接続**セクションで利用できます。

ミニルーティングテーブルにルートを追加するには

Citrix Secure Private Accessサービスでアプリを追加する手順は、サービスとしてのソフトウェアアプリのサポート および エンタープライズWebアプリのサポート のトピックで説明されているものと同じですが、以下の2つの変更点があります。

1. 次の手順を完了します。

   - テンプレートを選択します。
   - アプリの詳細を入力します。
   - 必要に応じて、拡張セキュリティの詳細を選択します。
   - 必要に応じて、シングルサインオン方法を選択します。

2. **App Connectivity** をクリックします。- アプリケーション構成中にルーティングの決定を行うために、アプリケーションドメインテーブルのミニバージョンが利用可能です。

   ミニルートテーブル(/en-us/citrix-secure-private-access/media/mini-route-table.png)

   - **ドメイン:** ドメイン列には、特定のアプリに対して1つ以上の行が表示されます。最初の行には、管理者がアプリの詳細を追加する際に入力した実際のアプリURLが表示されます。

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

その他の行はすべて、アプリの詳細を追加する際に入力された関連ドメインです。アプリURLと関連ドメインが同じ場合、それらは1つの行に表示されます。

SAML SSOが選択されている場合、1つの行にSAMLアサーションURLが表示されます。

- **タイプ:** 次のいずれかのオプションを選択します。
  - **内部 – プロキシをバイパス** - ドメイントラフィックはCitrix Cloud™ Connectorを介してルーティングされ、Connector Applianceで構成された顧客のWebプロキシをバイパスします。
  - **コネクタ経由の内部** - アプリは外部ですが、トラフィックはConnector Applianceを介して外部ネットワークに流れる必要があります。
  - **外部** – トラフィックはインターネットに直接流れます。
- **リソースの場所:** アプリのタイプとして「内部」を選択すると自動入力されます。別のリソースの場所が必要な場合は変更します。
- **Connector Applianceのステータス:** アプリのタイプとして「内部」を選択すると、リソースの場所とともに自動入力されます。

Citrix Workspaceアプリ経由でのCitrix Secure Access™クライアントへのシングルサインオン

Citrix Secure Accessクライアントは、Citrix Workspaceアプリ経由で既にログインしている場合、ストアURLのシングルサインオンをサポートするようになりました。このSSO機能により、複数回の認証を回避することでユーザーエクスペリエンスが向上します。

前提条件

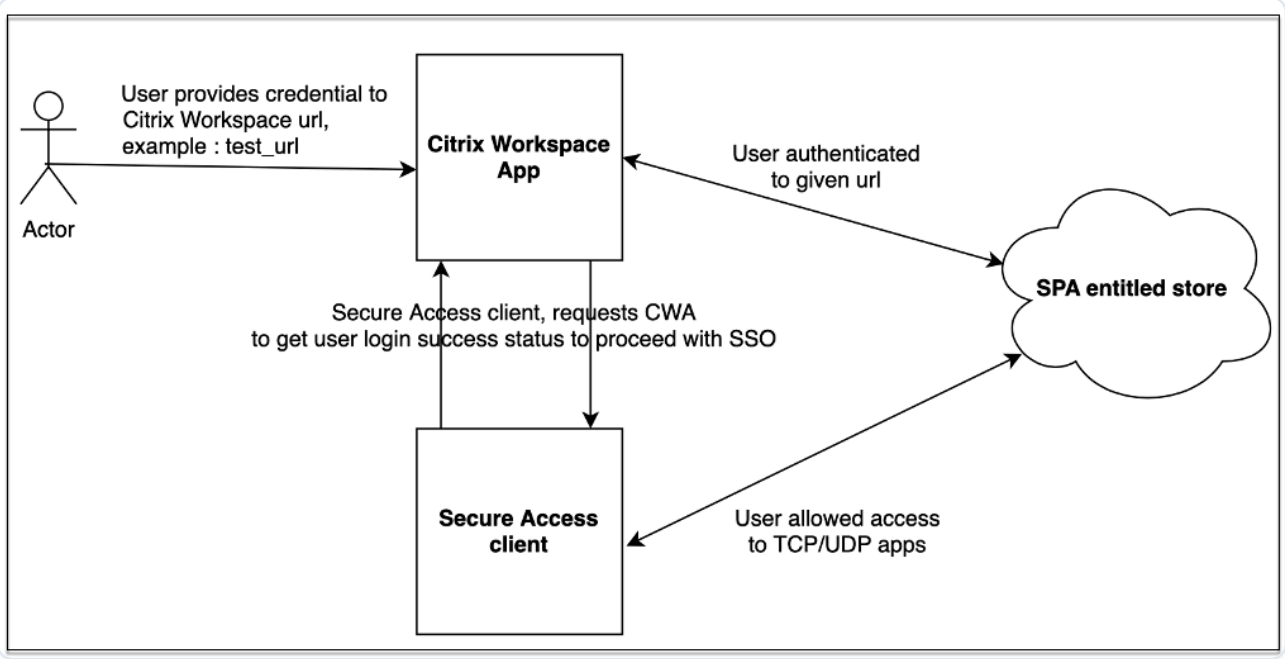
- Citrix WorkspaceアプリとSecure Accessクライアントの両方がデバイスにインストールされている必要があります。
- Citrix Secure Accessクライアントで自動SSOが行われるためには、ユーザーはまずCitrix Workspaceアプリにログインしている必要があります。

注:

シングルサインオン機能は、Citrix Workspaceアプリで構成されているプライマリストアでのみサポートされます。ユーザーがプライマリストア以外のストアにログインした場合、SSOは発生しません。ユーザーはCitrix Secure Accessクライアントに手動でログインする必要があります。

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

次の図は、Citrix WorkspaceアプリとCitrix Secure Accessクライアント間のSSOフローを示しています。



Windowsの機能要件

- Citrix Workspaceアプリのバージョン - **22.10.5.14(2210.5)以降**
- Citrix Secure Accessのバージョン - **22.10.1.9以降**
- Citrix Secure Access Windowsレジストリ - **EnableCWASSO**

SSO機能はデフォルトで無効になっています。この機能を有効にするには、エンドユーザーのマシンに次のレジストリを追加します。

- レジストリ名 - EnableCWASSO
- レジストリパス - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- レジストリの種類 - REG_DWORD
- レジストリ値 - 1

重要:

場合によっては、Citrix Workspaceアプリとのシングルサインオンを正常に確立するために、エンドユーザーのマシンを再起動する必要がある場合があります。

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

ADFSとセキュア プライベート アクセスの統合

クレームパイプラインを介したクレームの流れを制御するには、クレームルールが必要です。クレームルールは、クレームルールの実行プロセス中にクレームフローをカスタマイズするためにも使用できます。クレームの詳細については、Microsoft ドキュメントを参照してください。

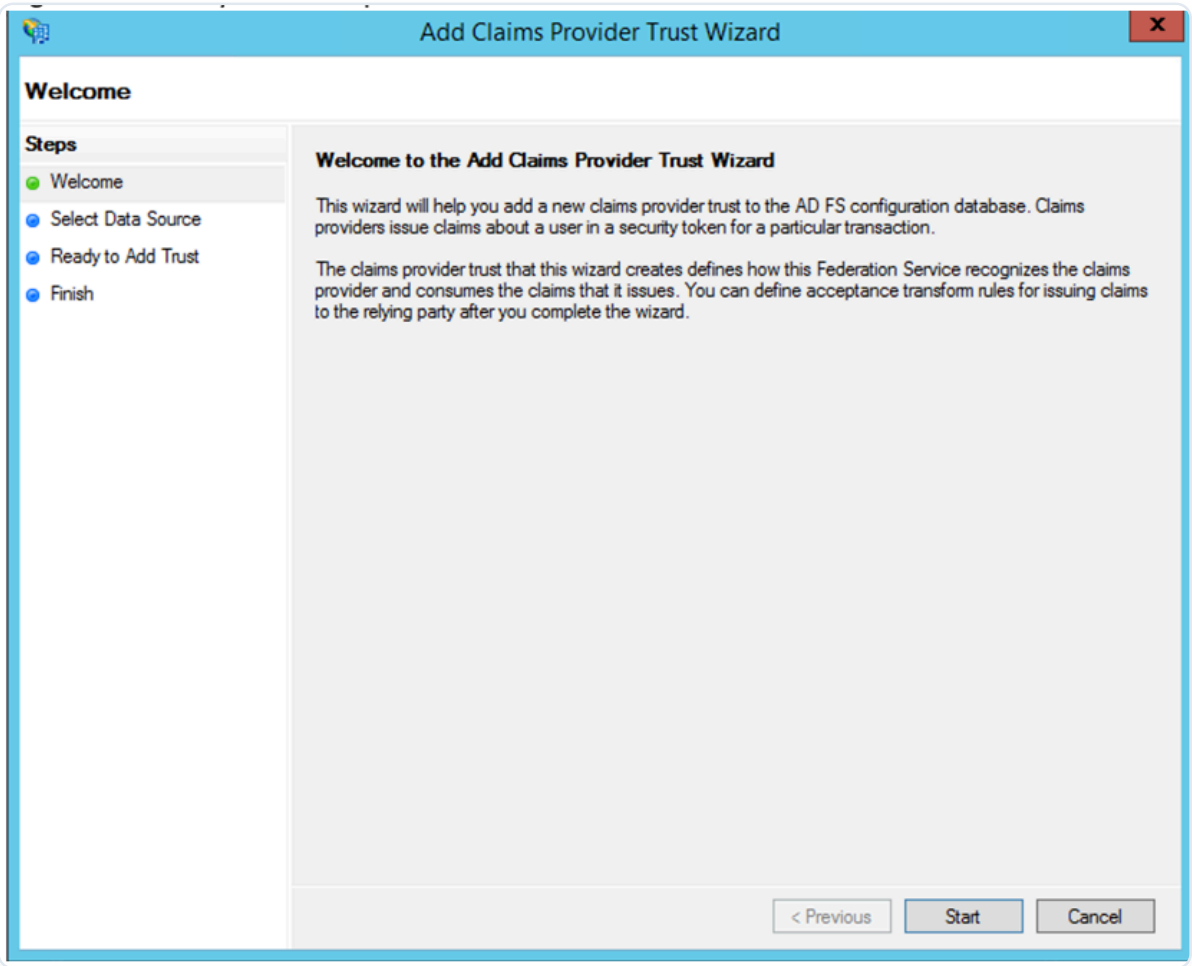
Citrix Secure Private Access™ からのクレームを受け入れるようにADFSを設定するには、次の手順を実行する必要があります。

1. ADFSにクレームプロバイダ信頼を追加します。
2. Citrix Secure Private Accessでアプリの設定を完了します。

ADFSにクレームプロバイダ信頼を追加する

1. ADFS管理コンソールを開きます。**ADFS > 信頼関係 > クレームプロバイダ信頼**に移動します。

   a. 右クリックして、**クレームプロバイダ信頼の追加**を選択します。

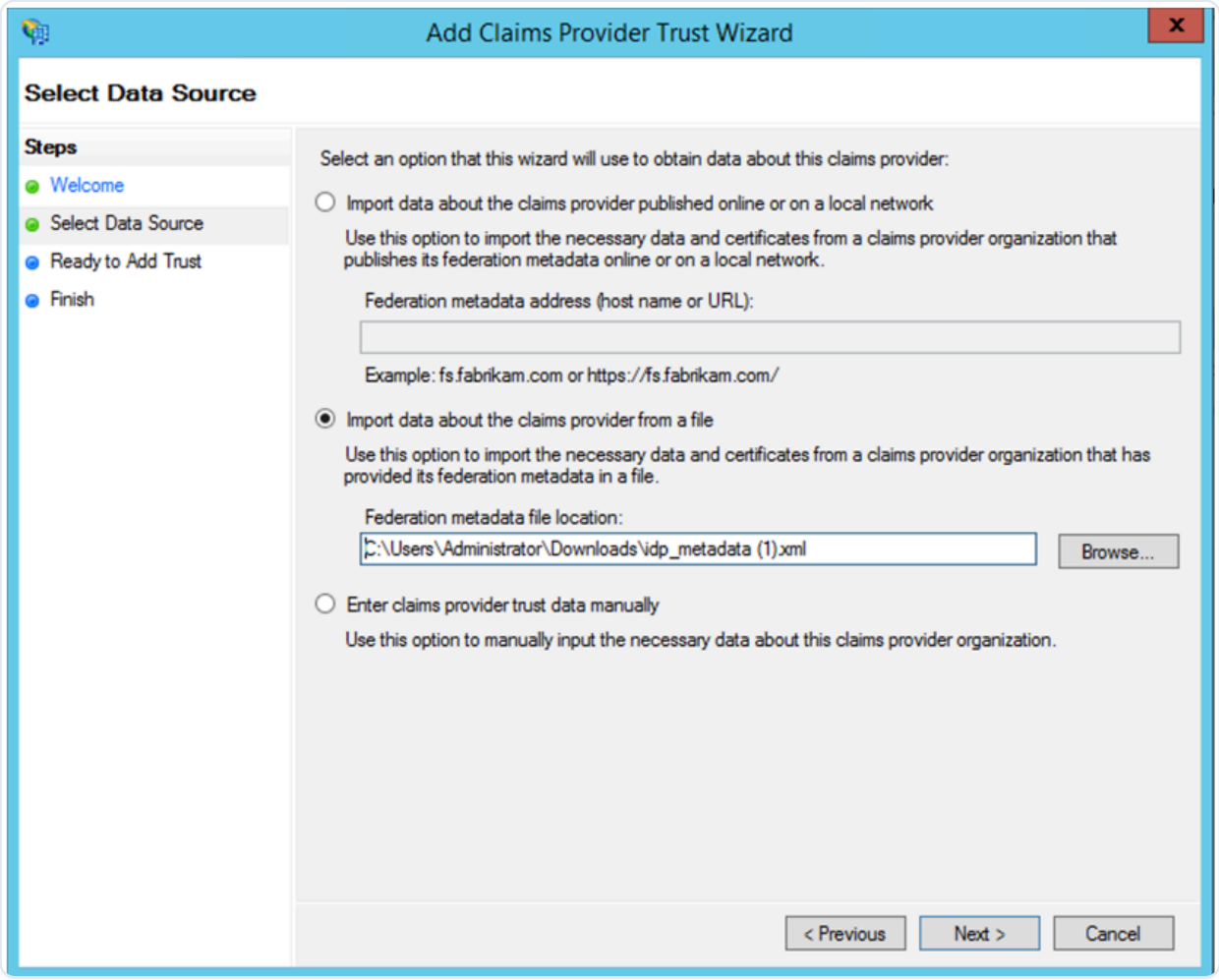


   b. ADFSへのフェデレーションに使用されるアプリをSecure Private Accessに追加します。詳細については、Citrix Secure Private Accessでのアプリ設定を参照してください。

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

注:

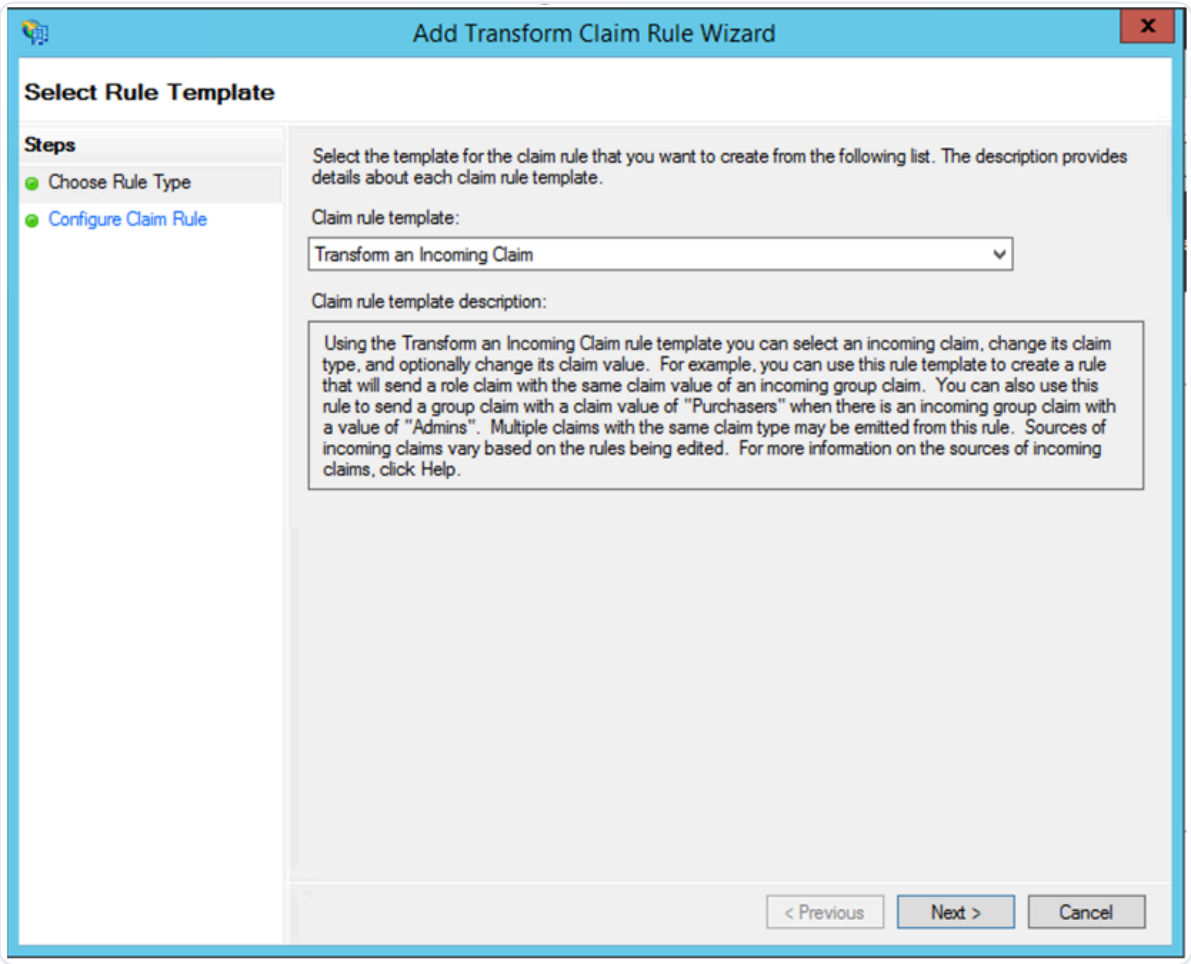
まずアプリを追加し、アプリのSSO構成セクションからSAMLメタデータファイルをダウンロードし、そのメタデータファイルをADFSにインポートします。



a. クレームプロバイダ信頼の追加を完了するための手順を実行します。クレームプロバイダ信頼の追加が完了すると、クレームルールを編集するためのウィンドウが表示されます。

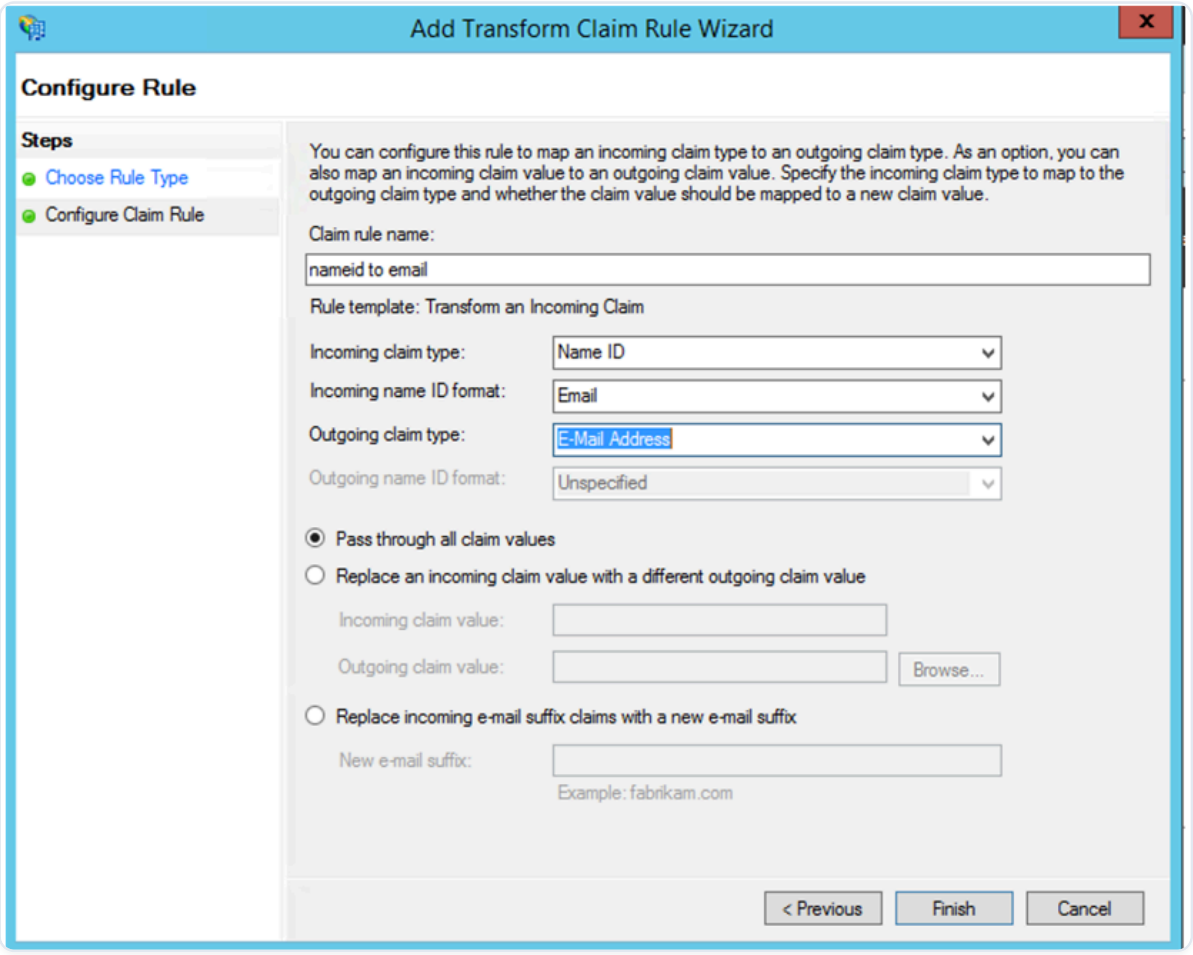
b. **受信クレームの変換**でクレームルールを追加します。

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



c. 次の図に示すように設定を完了します。ADFSが他のクレームを受け入れる場合は、それらのクレームを使用し、Secure Private Accessでもそれに応じてSSOを設定します。

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

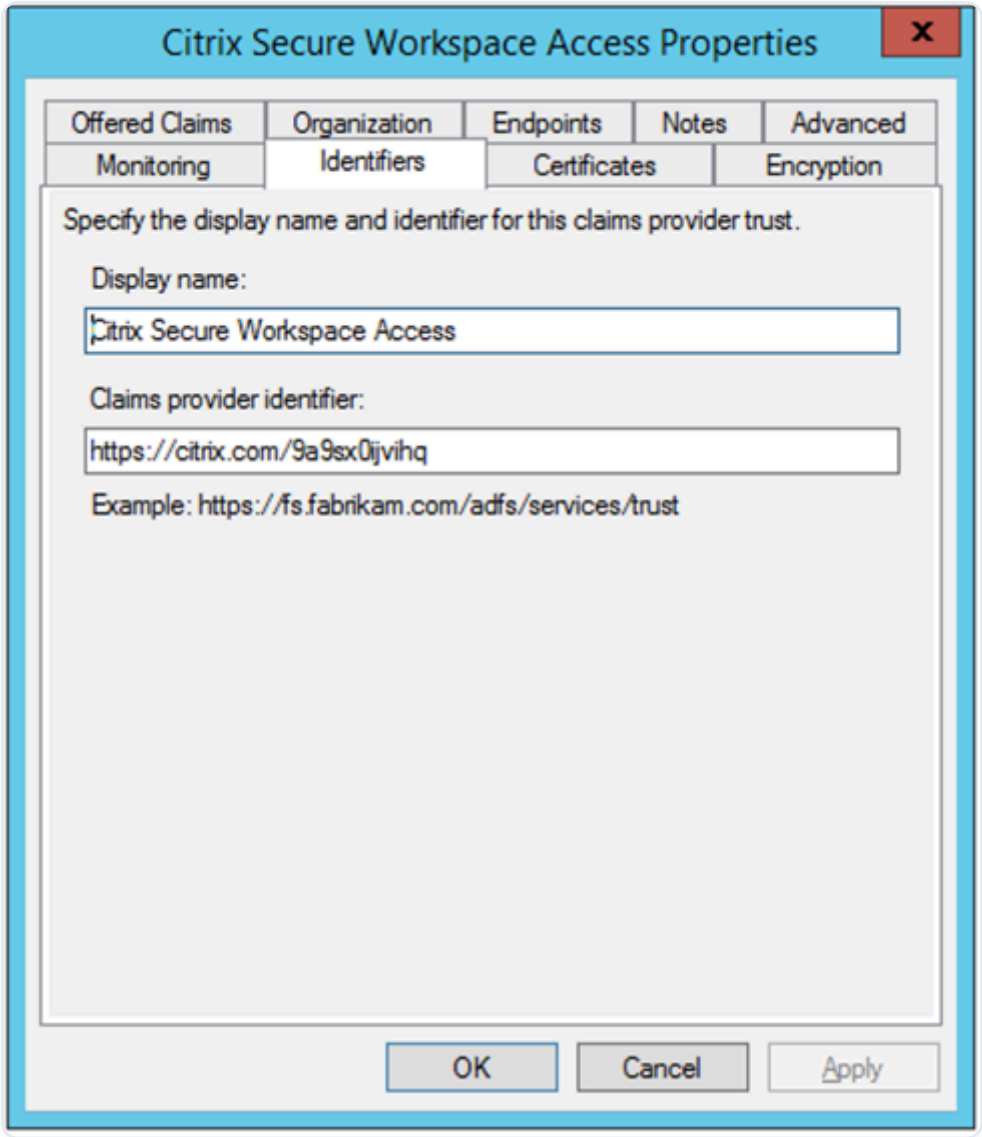


これで、ADFSがSAMLのためにCitrix Secure Private Accessを信頼することを確認するクレームプロバイダートラストが構成されました。

クレームプロバイダートラストID

追加したクレームプロバイダートラストIDをメモしておきます。このIDは、Citrix Secure Private Accessでアプリを構成する際に必要になります。

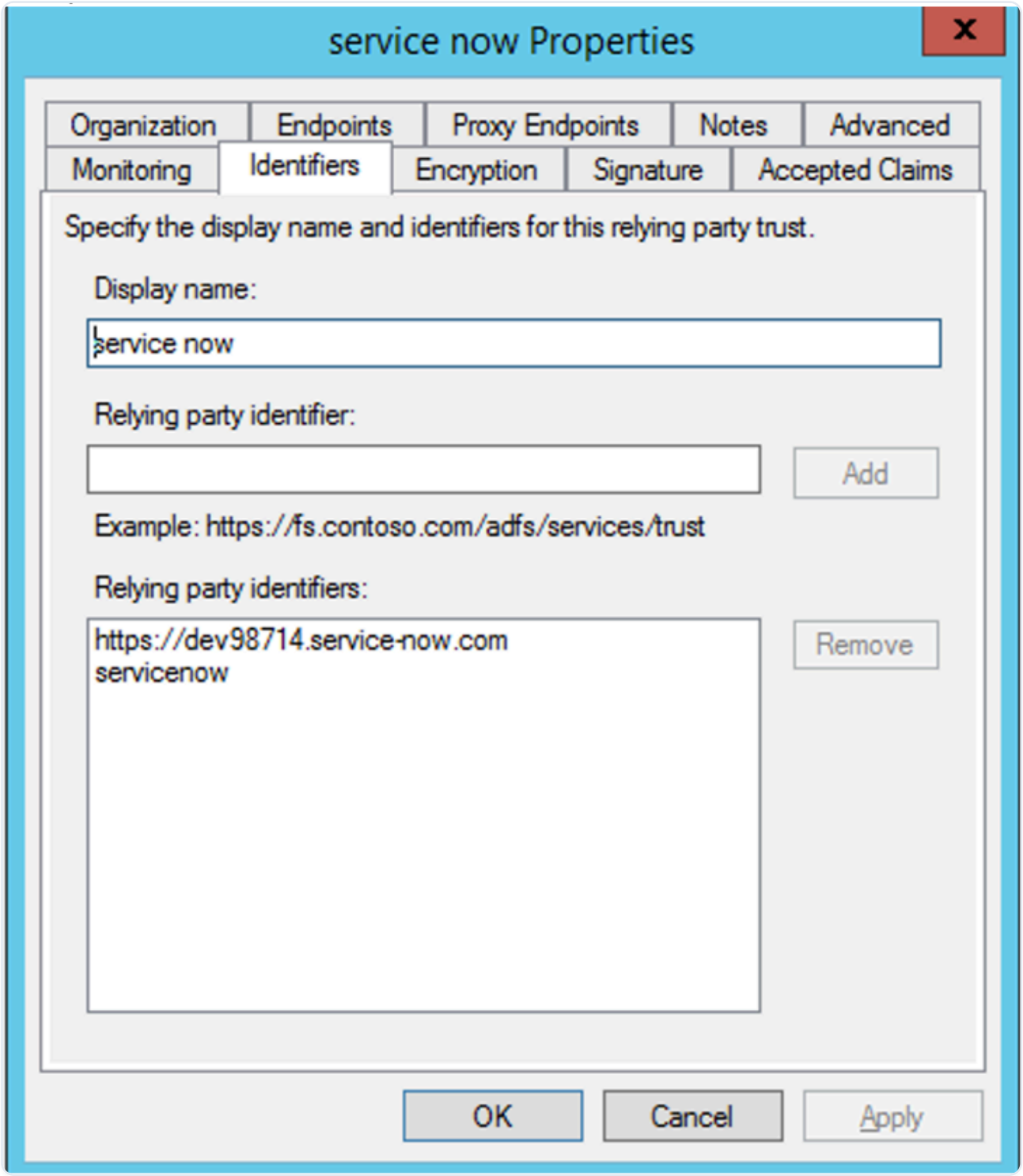
© 1997–2026 Citrix Systems, Inc. All rights reserved.



証明書利用者識別子

SaaSアプリがADFSを使用してすでに認証されている場合、そのアプリの証明書利用者信頼がすでに追加されているはずです。このIDは、Citrix Secure Private Accessでアプリを構成する際に必要になります。

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



IdP開始フローでリレーステートを有効にする

RelayStateはSAMLプロトコルのパラメータであり、ユーザーがサインインして証明書利用者のフェデレーションサーバーにリダイレクトされた後、アクセスする特定のリソースを識別するために使用されます。ADFSでRelayStateが有効になっていない場合、ユーザーはそれを必要とするリソースプロバイダーに認証された後にエラーが表示されます。

ADFS 2.0の場合、RelayStateのサポートを提供するために、更新プログラムKB2681584 (Update Rollup 2) またはKB2790338 (Update Rollup 3) をインストールする必要があります。ADFS 3.0に

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

はRelayStateのサポートが組み込まれています。どちらの場合も、RelayStateは有効にする必要があります。

ADFSサーバーでRelayStateパラメータを有効にするには

1. ファイルを開きます。
   - ADFS 2.0の場合、メモ帳で次のファイルを入力します: %systemroot%\inetpub\adfs\ls\web.config
   - ADFS 3.0の場合、メモ帳で次のファイルを入力します: %systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.config
2. microsoft.identityServer.webセクションで、useRelyStateForIdpInitiatedSignOnの行を次のように追加し、変更を保存します。 `<microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn enabled="true" /> ...</microsoft.identityServer.web>`
   - ADFS 2.0の場合、IISを再起動するために `IISReset` を実行します。
3. 両方のプラットフォームで、Active Directory フェデレーションサービスを再起動します `(adfssrv) service.` **注:** Windows 2016またはWindows 10を使用している場合は、次のPowerShellコマンドを使用して有効にします。 `Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true`

コマンドへのリンク - `<https://docs.microsoft.com/ja-jp/powershell/module/adfs/set-adfsproperties?view=win10-ps>`

Citrix Secure Private Accessでのアプリ構成

IdP開始フローまたはSP開始フローのいずれかを構成できます。Citrix Secure Private AccessでIdPまたはSP開始フローを構成する手順は同じですが、SP開始フローの場合は、UIで**指定されたURLを使用してアプリを起動する（SP開始）**チェックボックスを選択する必要があります。

IdP開始フロー

1. IdP開始フローを設定する際は、以下を構成します。
   - **アプリURL** – アプリURLには次の形式を使用します。 `https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=<rp id>&RedirectToIdentityProvider=<idp id>`
   - **ADFS FQDN** – ADFSセットアップのFQDN。

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

- **RP ID** – RP IDは、証明書利用者信頼から取得できるIDです。これは証明書利用者識別子と同じです。URLの場合、URLエンコードが行われます。
- **IDP ID** – IdP IDは、クレームプロバイダー信頼IDと同じです。URLの場合、URLエンコードが行われます。

  例: `<https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq>`

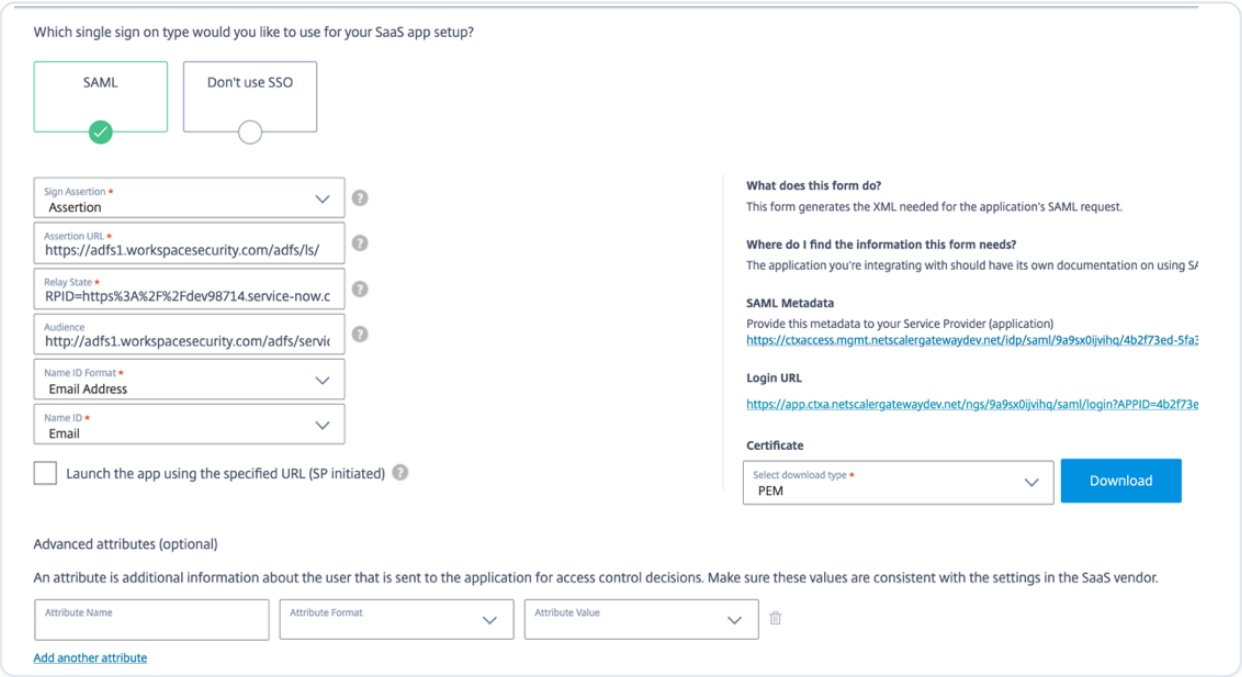
2. SAML SSO構成。

以下はADFSサーバーのデフォルト値です。いずれかの値が変更されている場合は、ADFSサーバーのメタデータから正しい値を取得してください。ADFSサーバーのフェデレーションメタデータは、そのフェデレーションメタデータエンドポイントからダウンロードできます。このエンドポイントは、**ADFS > サービス > エンドポイント**から確認できます。

- **アサーションURL** – `https://<adfs fqdn>/adfs/ls/`
- **リレーステート** – リレーステートは、IdP開始フローにとって重要です。正しく構築するには、このリンクに従ってください - `https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj127245(v=ws.10)`

  例: RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev98714.service-now.com%2F
- **オーディエンス** – `http://<adfsfqdn>/adfs/services/trust`
- その他のSAML SSO構成設定については、次の画像を参照してください。詳細については、SaaSアプリのサポートを参照してください。

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



3. アプリを保存してユーザーに購読させます。

SP開始フロー

SP開始フローの場合、**IDP開始フロー**セクションに記載されている設定を構成します。さらに、**指定されたURLを使用してアプリを起動する（SP開始）**チェックボックスを有効にします。

シトリックス セキュア プライベート アクセス™

Citrix Secure Private Accessサービスにより、管理者はシングルサインオン、リモートアクセス、コンテンツ検査を単一のソリューションに統合し、エンドツーエンドのアクセス制御を実現する一貫したエクスペリエンスを提供できます。IT管理者は、簡素化されたシングルサインオンエクスペリエンスで、承認されたSaaSアプリへのアクセスを管理できます。Citrix Secure Private Accessサービスを使用すると、管理者は特定のWebサイトやWebサイトカテゴリへのアクセスをフィルタリングすることで、組織のネットワークとエンドユーザーデバイスをマルウェアやデータ漏洩から保護することもできます。管理者は、SaaSアプリケーションへのセキュアなアクセスのために、強化されたアクセスセキュリティポリシーを適用できます。認証されると、従業員はオフィス内、自宅、または移動中であるかどうかにかかわらず、あらゆるデバイスからすべての重要なビジネスアプリケーションにアクセスできます。

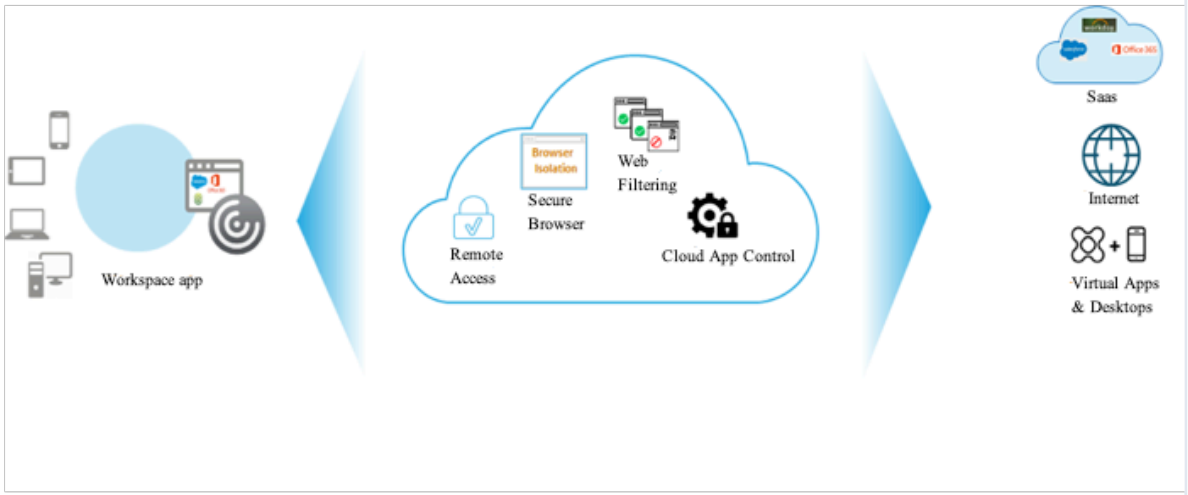
管理者は、アクセスされた悪意のある、危険な、または不明なWebサイト、消費された帯域幅、リスクのあるダウンロードおよびアップロードの動作など、ユーザーアクティビティを監視できます。アクセスされたWebサイトおよびWebサイトカテゴリに関する分析を使用して、管理者は企業ネットワークを保護するための是正措置を講じることができます。同時に、このサービスはエ

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

ンドユーザーに、ホストされているすべてのアプリへのシームレスでセキュアなアクセスを提供します。

管理者は、印刷制限、ダウンロード、クリップボードアクセス（コピー＆ペースト）などのアクションも制限できます。

次の図は、Secure Private Accessサービスの視覚的な表現です。



Citrix Secure Private Accessの主な機能

以下は、Citrix Secure Private Accessサービスで実行できる主要なタスクの一部です。

- **シングルサインオンアクセスでSaaSアプリを公開** - ユーザーがプライマリIDでストアに認証されると、その後のSaaSおよびWebアプリへの認証要求は、SAMLアサーションを使用してCitrix Cloud™のシングルサインオン機能によって自動的に処理されます。

デフォルトでは、SAMLアサーションは、ユーザーのActive Directoryアカウント（IDプロバイダー）に関連付けられたメールアドレスと、ユーザーのSaaSまたはWebアプリのアカウント（サービスプロバイダー）に関連付けられたメールアドレスを利用します。

- **SaaSアプリのセキュリティ強化ポリシーを設定します。(例: 透かし、コピー＆ペースト制限、ダウンロード防止)** - コンテンツを保護するため、組織はSaaSアプリケーション内に強化されたセキュリティポリシーを組み込みます。各ポリシーは、デスクトップ版Workspaceアプリを使用する場合はCitrix Enterprise Browser™に、Web版またはモバイル版Workspaceアプリを使用する場合はSecure Browserに制限を適用します。

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

  - 優先ブラウザ: ローカルブラウザの使用を無効にし、Citrix Enterprise Browserエンジン（Workspaceアプリ - デスクトップ）またはSecure Browser（Workspaceアプリ – モバイルおよびWeb）に依存します。
  - クリップボードアクセスを制限: アプリとエンドポイントのクリップボード間の切り取り/コピー/貼り付け操作を無効にします。
  - 印刷を制限: アプリブラウザ内からの印刷機能を無効にします。
  - ダウンロードを制限: SaaSアプリ内からのユーザーのダウンロード機能を無効にします。
  - ウォーターマークの表示: エンドポイントのユーザー名とIPアドレスを表示する画面ベースのウォーターマークを重ねて表示します。ユーザーが印刷またはスクリーンショットを試みると、ウォーターマークは画面に表示されたとおりに現れます。

- **コンテキストに応じたアクセスを提供する** - 承認されたSaaSアプリは安全と見なされますが、SaaSアプリ内のコンテンツは実際には危険である可能性があり、セキュリティリスクを構成します。ユーザーがSaaSアプリ内のハイパーリンクをクリックすると、トラフィックはWebフィルタリング機能を経由してルーティングされ、ハイパーリンクのリスク評価が提供されます。ハイパーリンクのリスク評価と、カスタマイズされたURLカテゴリのリストに基づいて、Webフィルタリング機能はユーザーからのハイパーリンク要求を次のように許可、拒否、またはリダイレクトします。
  - 承認済み: ハイパーリンクは安全と見なされ、Citrix Enterprise BrowserはWorkspaceアプリ内でハイパーリンクにアクセスします。
  - 拒否済み: ハイパーリンクは危険と見なされ、アクセスは拒否されます。
  - リダイレクト済み: ハイパーリンク要求はRemote Browser Isolationサービスにリダイレクトされ、ユーザーのインターネット閲覧アクティビティはエンドポイントデバイス、企業ネットワーク、およびSaaSアプリから分離されます。
- **セキュリティとパフォーマンスの分析** - ユーザーは、強化されたセキュリティが組み込まれているSaaSアプリに常にアクセスします。Citrix Workspaceアプリ、Secure Private Accessサービス、およびRemote Browser Isolationサービスは、以下のユーザーおよびアプリケーションの動作に関する情報をセキュリティ分析サービスに提供します。これらの分析は、ユーザーの全体的なリスクスコアに影響を与えます。
  - アプリ起動時間
  - アプリ終了時間
  - 印刷アクション
  - クリップボードアクセス
  - URLアクセス

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

- データアップロード
- データダウンロード

Webフィルタリング機能は、SaaSアプリケーション内で選択された各ハイパーリンクのリスクを評価します。これらのサイトにアクセスし、ユーザーの行動の変化を監視すると、エンドポイントデバイスが侵害され、データの感染または暗号化を開始したか、ユーザーとデバイスが知的財産を盗んでいることを示すため、ユーザーの全体的なリスクスコアが増加します。

セキュアプライベートアクセス REST API

Secure Private Access REST API を使用して、複数のアプリケーションとポリシーを直接構成できます。詳細については、Citrix Secure Private Accessを参照してください。

アプリケーション固有のリソースロケーションにDNSクエリをルーティングする

管理者は、特定のアプリケーションに対するDNSクエリを、専用のリソースロケーションに直接ルーティングできます。これにより、より正確なDNS解決、インテリジェントなトラフィック管理、およびより良いユーザーエクスペリエンスが可能になります。以前は、すべてのDNSクエリは、アプリケーションがホストされている場所に関係なく、デフォルトで地理的に最も近い利用可能なDNSサーバーにルーティングされていました。これには、すべてのリソースロケーションのDNSサーバーを同期する必要がありましたが、これは常に実現可能ではありませんでした。

システム要件

Citrix Secure Accessクライアント:

- macOS - バージョンV25.08.1.1 以降 (Citrix Downloads)、バージョンV25.08.1 以降 (App Store)。
- Windows - 25.7.1.11以降。

機能の有効化

アプリケーション固有のDNSルーティング機能は、デフォルトで無効になっています。この機能を組織で有効にするには、Citrixサポートにお問い合わせください。

DNSクエリのルーティングを構成する

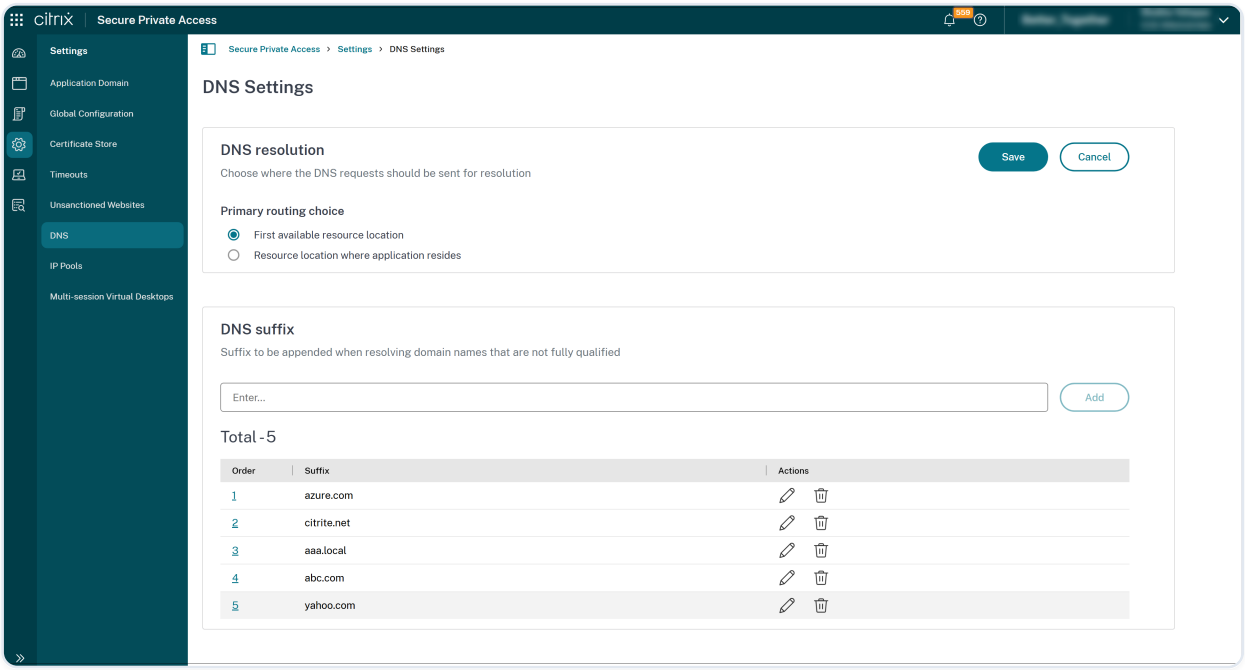
機能が有効になったら、次の2つのオプションのいずれかを使用してDNSクエリをルーティングできます。

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

- **最初に利用可能なリソースロケーション:** すべてのクエリが地理的に最も近いリソースロケーションにルーティングされる従来の動作を維持します。このオプションを使用する場合は、すべてのリソースロケーションのすべてのDNSサーバーが同期されていることを確認してください。
- **アプリケーションが存在するリソースロケーション:** アプリケーション固有のリソースロケーションにルーティングします。ホスト名に基づいて、DNSクエリをアプリケーション専用のリソースロケーションに直接送信できます。

DNSルーティングを構成するには、次の手順を実行します。

1. **設定 > DNS > DNS解決**に移動します。
2. **追加**をクリックします。



3. 次のいずれかのオプションを選択します。
   - **最初に利用可能なリソースロケーション**
   - **アプリケーションが存在するリソースロケーション**
4. **保存**をクリックします。

Secure Private Accessは、サービス継続性を確保するために、堅牢なDNSルーティングフォールバックメカニズムをサポートしています。特定のDNSクエリに対してアプリケーション固有のリソースロケーションを特定できない場合、リクエストは自動的に指定されたフォールバックルートにフォールバックします。

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

注：

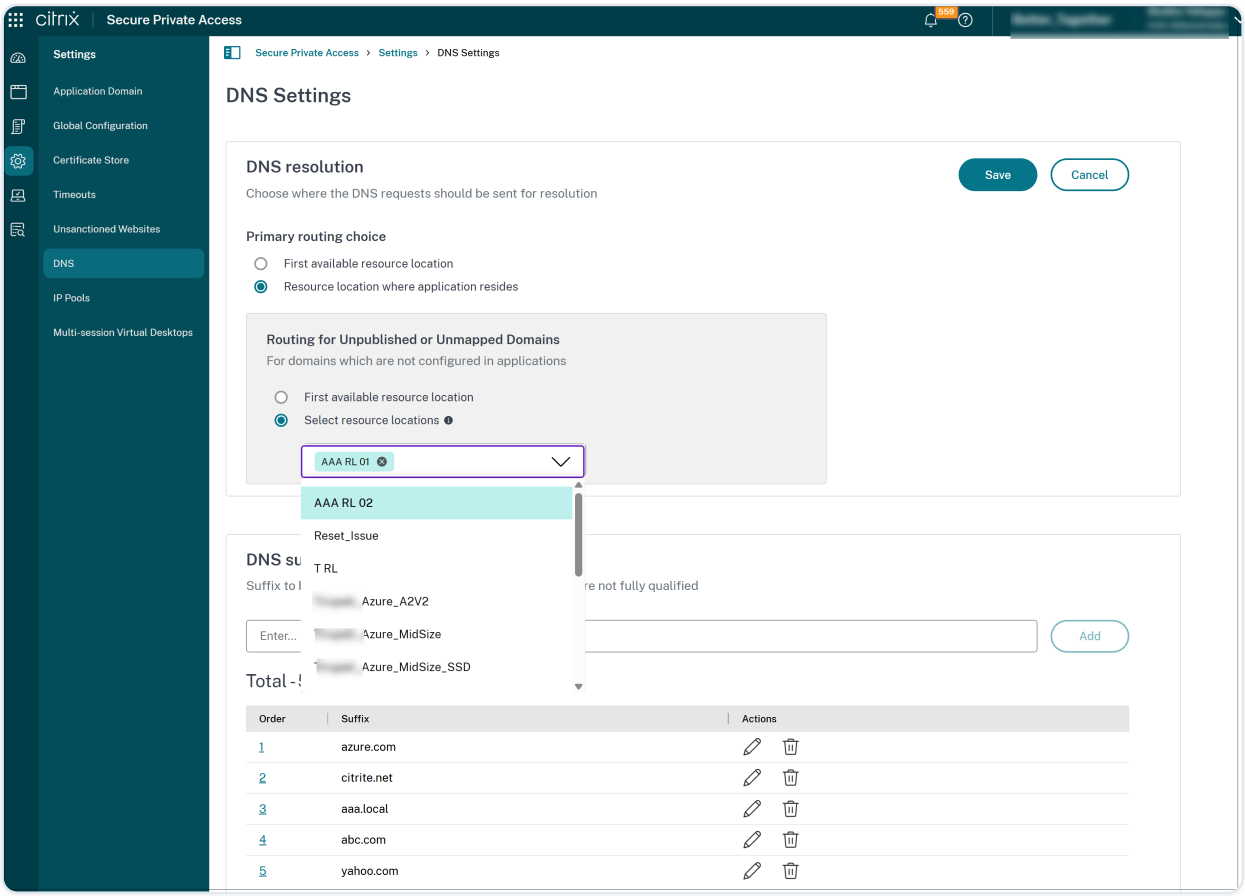
マッピングされていないドメインまたは未公開のドメインのルーティングは、プライマリルーティングの選択肢を**アプリケーションが存在するリソースロケーション**に設定した場合にのみ構成できます。

フォールバックメカニズムは、次のいずれかのオプションに構成できます。

- **最初に利用可能なリソースロケーション:** 最も近い地理的なリソースロケーション。
- **リソースロケーションを選択:** 管理者によって定義された構成済みリソースロケーションのリストからいずれかのロケーション。

DNSクエリのフォールバックルーティングを構成します。

1. **設定 > DNS > DNS解決**に移動します。
2. **追加**をクリックします。



3. 「**プライマリルーティングの選択**」で、「**アプリケーションが存在するリソースロケーション**」を選択します。

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

4. 「**未公開または未マッピングドメインのルーティング**」で、次のいずれかのオプションを選択します。

   - **最初に利用可能なリソースロケーション**
   - **リソースロケーションを選択**

   「**リソースロケーションを選択**」オプションを選択した場合は、リストから目的のリソースロケーションを選択します。複数のリソースロケーションを選択できます。

5. 「**保存**」をクリックします。

G Suite を構成する

SAML を介したシングルサインオンのために G Suite を構成するには、次の手順を実行します。

1. 管理者ユーザーとして G Suite にログオンします。

   G Suite ログオン(/en-us/citrix-secure-private-access/media/gsuite-1.png)

2. **セキュリティ**をクリックします。

   セキュリティ設定(/en-us/citrix-secure-private-access/media/gsuite-2.png)

3. **セキュリティ**ページで、**シングルサインオン (SSO) の設定**をクリックします。

   SSO の設定(/en-us/citrix-secure-private-access/media/gsuite-3.png)

4. **シングルサインオン (SSO) の設定**ページで、**サードパーティの ID プロバイダーで SSO を設定**を選択し、詳細を入力します。

   - **サインインページ URL** - Citrix Cloud ウィザード (**Citrix Gateway Service > Web/SaaS アプリの追加 > シングルサインオン > ログイン URL**) から SAML SSO ログイン URL をコピーできます。
   - **検証証明書** - Citrix Cloud ウィザード (**Citrix Gateway Service > Web/SaaS アプリの追加 > シングルサインオン > 証明書**) から証明書をダウンロードできます。
   - **ドメイン固有の発行者を使用** - チェックボックスをオンにします。

Jira の構成

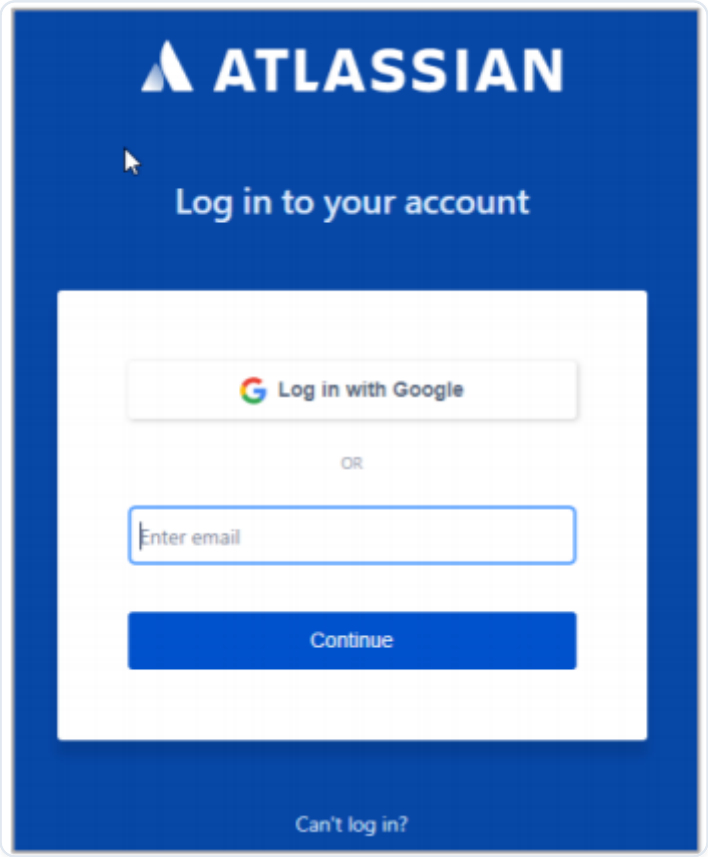
以下のセクションでは、Jira の構成に関する詳細情報を提供します。

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

Citrix Gateway SaaS アプリケーション

Jira を SSO 用に構成すると、管理者は NetScaler を使用してユーザーを管理できます。ユーザーはエンタープライズ資格情報を使用して Jira に安全にログオンできます。 SAML を介して Jira を SSO 用に構成するには、次の手順を実行します。

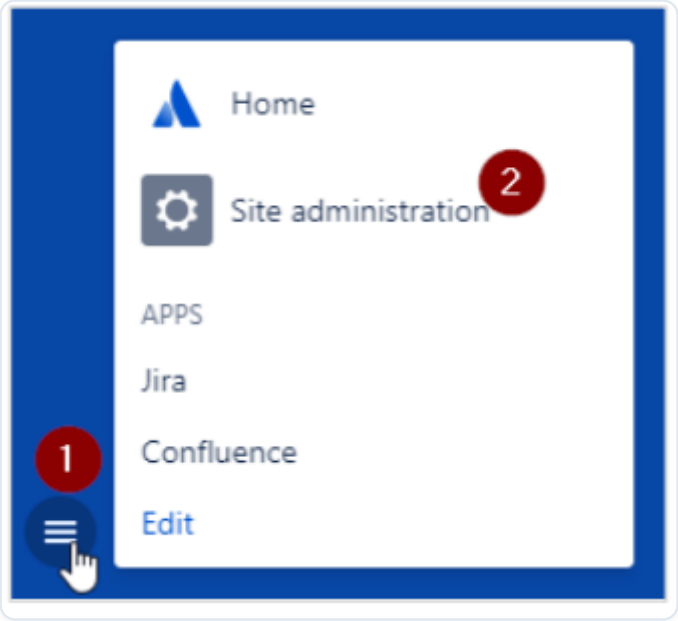
1. ブラウザで、組織の Atlassian クラウド URL を入力し、Enter キーを押します。
2. Atlassian アカウントにログオンします。



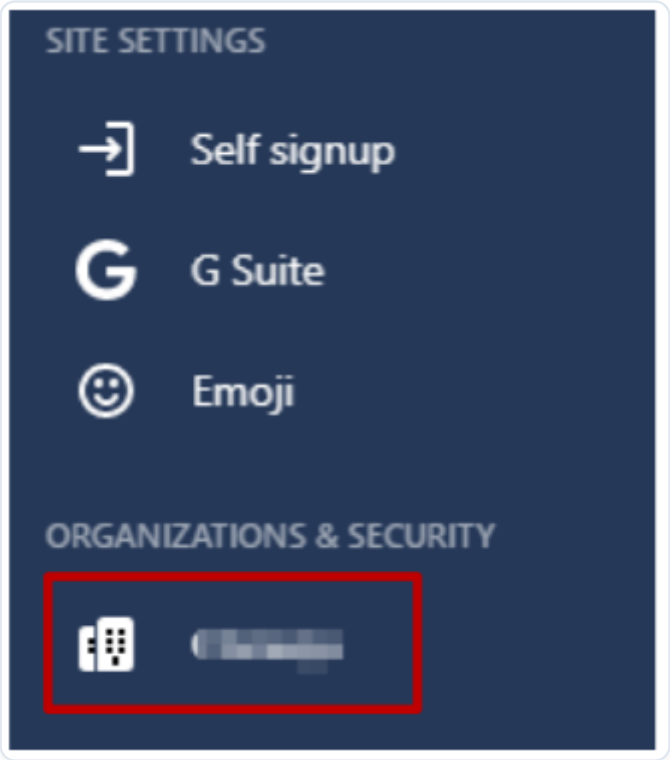
3. ホームページの左下隅にある省略記号アイコンをクリックします。

4. **サイト管理**をクリックします。

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

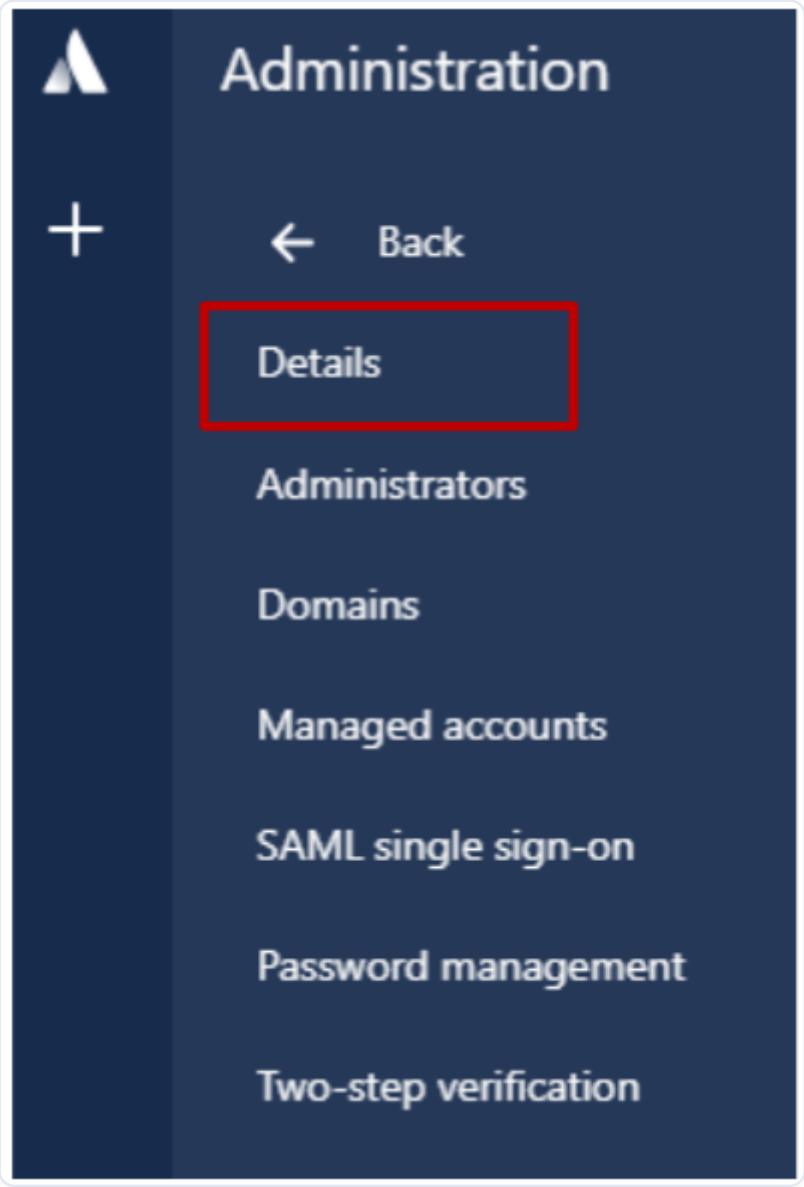


5. 管理ページで、「ORGANIZATION & SECURITY」セクションにある、SAML 認証を構成する組織名をクリックします。



6. **詳細**をクリックし、ドメインを確認します。

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



ドメインを検証するには、以下を実行します。

a. 左下隅にある**アプリを切り替える**アイコンをクリックします。

アプリを切り替えるにはクリックします(/en-us/citrix-secure-private-access/media/jira-6.png)

a. **サイト管理**をクリックします。

サイト管理オプション(/en-us/citrix-secure-private-access/media/jira-7.png)

a. 組織名をクリックします。

組織名(/en-us/citrix-secure-private-access/media/jira-8.png)

a. **ドメイン**をクリックします。

ドメインを選択(/en-us/citrix-secure-private-access/media/jira-9.png)

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

a. DNSまたはHTTPSを使用してドメインを検証できます。ドメイン検証の手順の詳細については、右側のペインの「ドメイン」セクションにある「ドメイン検証の詳細」リンクをクリックしてください。

ドメインを検証する方法(/en-us/citrix-secure-private-access/media/jira-10.png)

a. 手順を完了したら、**ドメインの検証**をクリックします。

ドメインを検証(/en-us/citrix-secure-private-access/media/jira-11.png)

a. 「検証済みドメイン」セクションの「ステータス」列に**検証済み**と表示されます。

ドメイン検証済みステータス(/en-us/citrix-secure-private-access/media/jira-12.png)

7. 「**SAML シングルサインオン**」をクリックします。
8. 右側のペインで、SAML 設定の下にある「**SAML 設定の追加**」をクリックします。

SAML 設定の追加(/en-us/citrix-secure-private-access/media/jira-13.png)

9. 「**SAML 設定の追加**」領域で、次の情報を指定します。

- ID プロバイダーエンティティ ID - 一意のissuer IDを入力します。例: `yourcompany_NS_Jira`
- ID プロバイダー SSO URL - IdP URLを入力します。

  注: Citrix Cloud ウィザード (**Citrix Gateway Service > Add a Web/SaaS App > Single sign on > Login URL**) から URL をコピーできます。

  シングルサインオン URL(/en-us/citrix-secure-private-access/media/jira-14.png)
- 公開 x509 証明書 – SAML IdP 署名証明書をコピーして貼り付けます。

  a. Citrix Cloud ウィザード (**Citrix Gateway Service > Add a Web/SaaS App > Single sign on > Certificate**) から証明書をダウンロードします。

  証明書の例(/en-us/citrix-secure-private-access/media/jira-15.png)

  b. -----BEGIN CERTIFICATE----- と -----END CERTIFICATE----- の間のテキストをコピーします。

  c. テキストエディターにテキストを貼り付け、`your company name`.pem のような適切な形式でファイルを保存します。

10. 「**設定の保存**」をクリックします。

設定の保存(/en-us/citrix-secure-private-access/media/jira-16.png)

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

O365を構成する

以下のセクションでは、O365の構成に関する詳細情報を提供します。

前提条件

Citrix WorkspaceアプリでO365アプリを構成するには、以下を完了していることを確認してください。

- **Microsoft Entra IDで、他のサービスとフェデレーションされていないプライマリドメインが利用可能な場合**、そのドメインを使用してCitrix Secure Private Accessにフェデレーションできます。このドメイン（親ドメインまたは子ドメインのいずれか）がすでにフェデレーションされておらず、その親ドメインがMicrosoft Entra IDにまだ追加されていないことを確認してください。

  たとえば、ユーザーが `user1@demo.citrix.com` を使用してログインする場合、demo.citrix.comがプライマリドメイン、citrix.comが親ドメイン、us.demo.citrix.comが子ドメインです。

- **プライマリドメインをフェデレーションできない場合**、新しいドメインをMicrosoft Entra IDに追加し、Citrix Secure Private Accessにフェデレーションします。ドメインを作成し、検証を完了します。詳細については、`<https://docs.microsoft.com/ja-jp/azure/active-directory/fundamentals/add-custom-domain>` を参照してください。

  または

  Microsoft Entra IDにサブドメインを追加し、SSOのためにCitrix Secure Private Accessにフェデレーションするために活用できます。そのためには、サブドメインを追加してルートドメインに昇格させる必要があります。詳細については、`<https://docs.microsoft.com/ja-jp/azure/active-directory/enterprise-users/domains-verify-custom-subdomain>` を参照してください。

  注: サブドメインをルートドメインに変更するためのPOSTリクエストには、Microsoft Graph Explorerの代わりにMicrosoft Entra ID Graph Explorerを使用する必要がある場合があります。

  フェデレーションドメインが必要な理由の詳細については、ドメインフェデレーションの仕組みを参照してください。

- **追加した新しいドメインまたはサブドメインが、Microsoft Entra IDで「検証済み」状態であることを確認してください。**

- **SAML IDプロバイダーとMicrosoft Entra IDの間に信頼関係を確立します。** 信頼関係を確立するには、Microsoft Entra IDで検証済みのドメインが必要です。ドメインを使用してMicrosoft

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

Entra IDでフェデレーションが構成されている場合、Microsoft Entra IDは、ユーザーがフェデレーションドメインとは異なるドメインからのユーザーであっても、Microsoft Entra IDへのユーザー認証のためにSAMLプロバイダーを信頼します。SP開始フローでMicrosoft Entra IDが認証に使用するIdPを識別する必要がある場合（ユーザーをフェデレーションIdPに誘導する場合）、`whr query param`または`domain_hint`がURL `<https://docs.microsoft.com/ja-jp/azure/active-directory/manage-apps/configure-authentication-for-federated-users-portal>`に渡されることで識別されます。

新しいドメインのフェデレーションを追加しても、既存のセットアップにある既存のフェデレーションには影響しません。ADFSがすでにドメインにフェデレーションされている場合でも、すでにフェデレーションされているドメインのサブドメインでも親ドメインでもない別のドメインにフェデレーションするため、影響はありません。

SSOには以下の2つのフローがあります。

IDP開始フロー: 通常、Microsoft Entra IDポータルにログインする場合に使用されます。Citrix Secure Private Accessサービスは、SAMLアサーションをMicrosoft Entra IDにポストします。Microsoft Entra IDは、以前に設定したフェデレーション設定に基づいてそれを検証します。検証が成功した場合、SAMLの`nameid`属性を抽出します。`nameid`属性は、Microsoft Entra IDに存在するユーザーの`immutableId`と一致する必要があります。

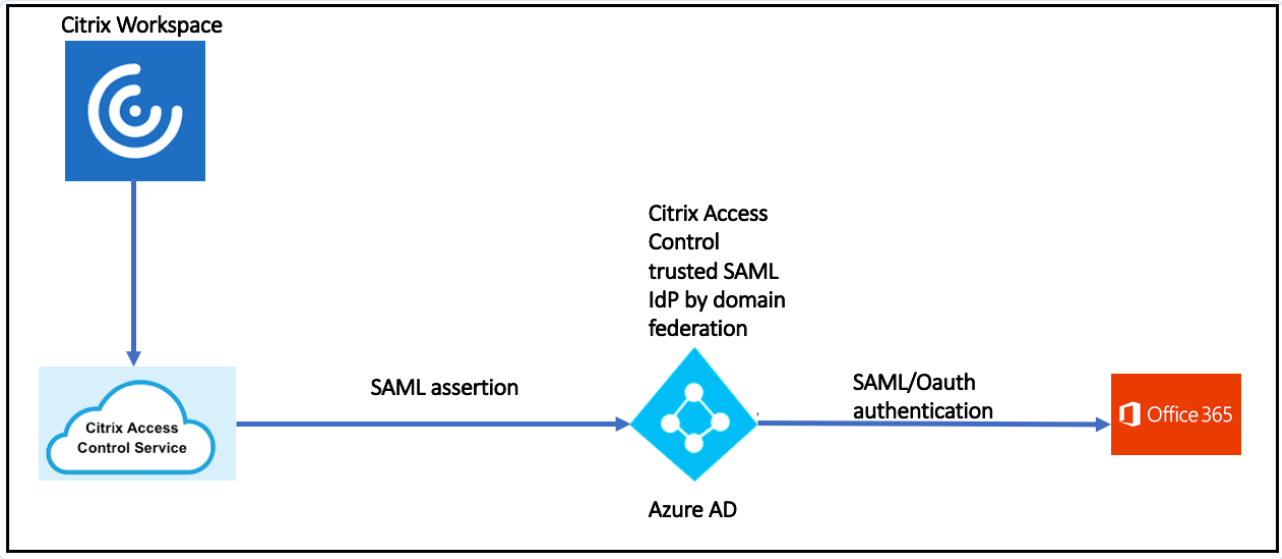
SP開始フロー: 通常、Microsoft Entra IDポータルではなく、アプリに直接アクセスする場合に使用されます。このフローでは、Citrix Secure Private Accessサービスは、アプリ設定で構成されているURLをロードします。URLはMicrosoft Entra IDに送信され、URLにフェデレーションドメインの何らかの表示があるため、ユーザーはSAMLリクエストとリレーステートとともにCitrix Secure Private Accessサービスにリダイレクトされます。Citrix Secure Private Accessサービスは、リクエストで受信したのと同じリレーステートでSAMLアサーションをMicrosoft Entra IDにポストします。SAMLが検証されると、Microsoft Entra IDはユーザーをリレーステート内のコンテキストにリダイレクトし、それによってユーザーはアプリに直接アクセスします。

- **Citrix Secure Private AccessサービスでO365アプリを構成します**。詳細については、「サービスとしてのソフトウェアアプリのサポート」を参照してください。

ドメインフェデレーションの仕組み

次の図は、ドメインフェデレーションが完了した後の一般的なフローを示しています。

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



Office 365アプリをCitrix Workspaceに追加し、透かしを有効にしてダウンロードを制限したいとします。一般的なフローは次のとおりです。

1. Citrix WorkspaceでOffice 365アプリを起動します。
2. リクエストはCitrix Secure Private Accessサービスに送信されます。
3. Citrix Secure Private AccessサービスはSAMLアサーションを作成し、Microsoft Entra IDに転送します。
4. リクエストが信頼されたSAML IdPから来ているため、Microsoft Entra IDは作成されたドメインフェデレーションを通じてそれを識別し、SAMLアサーションをOffice 365アプリに渡します。

   Office 365アプリが起動します。

Office 365アプリでサポートされている認証方法

デフォルトでは、Citrix Cloud™はCitrix IDプロバイダーを使用して、Citrix Cloudアカウントのすべてのユーザーの ID情報を管理します。

Citrix Workspaceは、Office 365に対して次の認証方法をサポートしています。OktaおよびGoogle IdPは現在サポートされていません。

- オンプレミス Active Directory
- Active Directory とトークン
- マイクロソフト Entra ID

注: Microsoft Entra ID を使用してワークスペースに認証する場合、ループが発生するため、プライマリドメイン (ユーザーのログインドメイン) をフェデレーションすることはできません。このような場合は、新しいドメインをフェデレーションする必要があります。

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

- シトリックス セキュア プライベート アクセス
- アクティブ ディレクトリ および RADIUS

詳細については、「ID およびアクセス管理」を参照してください。

Secure Private Access サービスで O365 アプリを構成する

Secure Private Access サービスで O365 アプリを構成するための大まかな手順は次のとおりです。詳細については、「サービスとしてのソフトウェアアプリのサポート」を参照してください。

1. Citrix Cloud の Secure Private Access サービスに移動します。
2. Office 365 を検索し、**Office365** テンプレートを選択します。テンプレートを使用してアプリを構成する方法の詳細については、「サービスとしてのソフトウェアアプリのサポート」を参照してください。

> **注:**
>
> **Office365** テンプレートを選択すると、**アプリの詳細**セクションに次の関連ドメインが自動入力されます。

- *.office.com
- *.office365.com
- *.sharepoint.com
- *.live.com
- *.onenote.com
- *.microsoft.com
- *.powerbi.com
- *.dynamics.com
- *.microsoftstream.com
- *.powerapps.com
- *.yammer.com
- *.windowsazure.com
- *.msauth.net
- *.msauthimages.net
- *.msocdn.com

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

- *.microsoftonline.com
- *.windows.net
- *.microsoftonline-p.com
- *.akamaihd.net
- *.sharepointonline.com
- *.officescriptsservice.com
- *.live.net
- *.office.net
- *.msftauth.net

3. 必要に応じて、拡張セキュリティ制御を有効にします。
4. SSO を構成します。

   注: 唯一の変更点は、「名前 ID」が Active Directory GUID であることを確認することです。

5. 詳細属性も `IDPEmail` を送信することを確認します。

   - 属性名: `IDPEmail`
   - 属性形式: 指定なし
   - 属性値: メール

6. SAML メタデータをクリックして、新しいタブで開きます。

   - 「entityID」をコピー
   - 「ログインURL」をコピー
   - CRT形式で証明書をダウンロード

Microsoft Entra ID から Citrix Workspace へのドメインフェデレーションを構成する

前提条件:

- Microsoft Entra ID で PowerShell を有効にする
- Microsoft MSOnline モジュールをインストールする

以下は、必要なモジュールをインストールするための PowerShell コマンドです。

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

```
`PS> Install-Module AzureAD -Force`



`PS> Import-Module AzureAD -Force`



`PS> Install-Module MSOnline -Force`



`PS> Import-module MSOnline -Force`
```

モジュールがすでにインストールされている場合は、以下のコマンドを実行します。

```
PS> connect-msolservice
```

注: `msolservice` に接続するには Microsoft クラウドアカウントが必要です。例: `admin.user@onmicrosoft.com`。

Microsoft Entra ID から Citrix Workspace へのドメインフェデレーションを構成する手順

1. **フェデレーションを構成するには、PowerShell で以下のコマンドを実行します:**

   - `PS> $dom = "ad-domain.com"`

   注: ad-domain.com は Microsoft Entra ID に追加された新しいドメインです

   - `PS> $IssuerUri = "https://citrix.com/[customerID]"`

   注: customerID は以下の場所から確認できます。

   - **Citrix Cloud > ID およびアクセス管理 > API アクセス**
   - **Citrix Cloud > Citrix Secure Private Access.** customer ID はアプリ構成の詳細 (**シングルサインオン > SAML メタデータファイル > entityID**) で確認できます。
   - `PS> $fedBrandName = “CitrixWorkspace”`
   - `PS> $logoffuri = "https://app.netscalergateway.net/cgi/logout"`

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

- `PS> $uri = "https://app.netscalergateway.net/ngs/[customerID]/saml/login?APPID=[AppID]”`

注: $uri は、**Citrix Secure Private Access Service > Web/SaaS アプリの追加 > シングルサインオン > ログイン URL** または **SAML メタデータ > 場所**からコピーできます。

- `PS> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2(“<location of certificate downloaded from Citrix Secure Private Access service/filename.crt>”)`

  例: `PS> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("c:\cert\saml_idp.crt")`

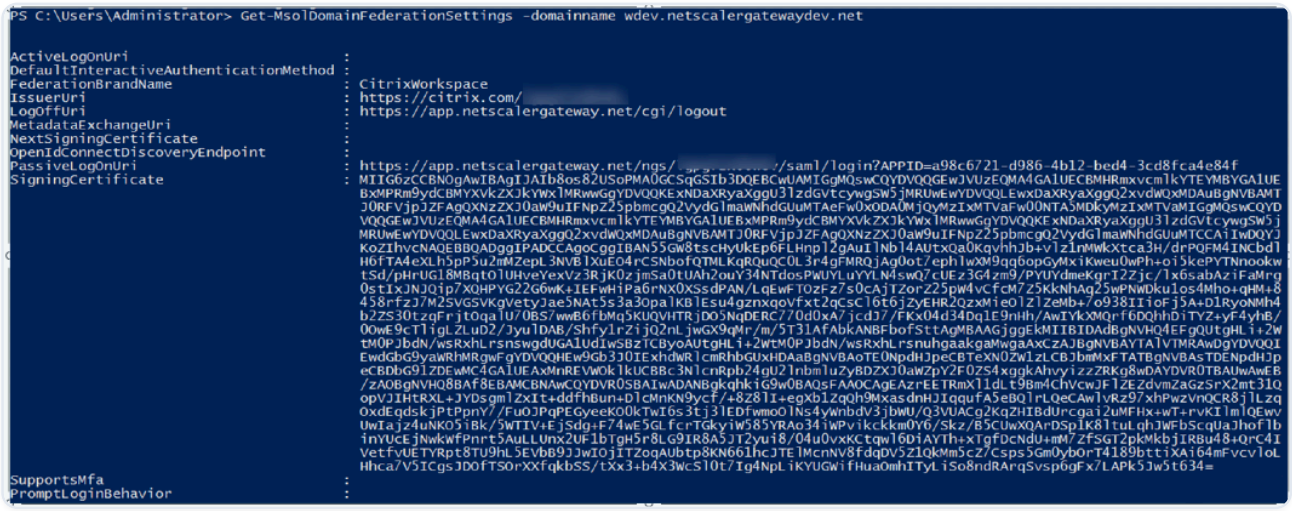
`PS> $certData = [system.convert]::tobase64string($cert.rawdata)`

2. **PS 文字列を実行して、Citrix Secure Private Access へのフェデレーションを完了します。**

   `PS> Set-MsolDomainAuthentication -DomainName $dom –federationBrandName $fedBrandName -Authentication Federated -PassiveLogOnUri $uri -LogOffUri $logoffuri -SigningCertificate $certData -IssuerUri $IssuerUri -PreferredAuthenticationProtocol SAMLP`

3. ドメインフェデレーション設定を確認するには、次のコマンドを実行します。

   `Get-MsolDomainFederationSettings -DomainName <domain name>`



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

Microsoft Entra ID から Citrix Workspace へのドメインの自動フェデレーション

Microsoft Entra ID から Citrix Workspace への手動ドメインフェデレーションでは、ユーザーはクラウドポータルと PowerShell を切り替えてデータをコピーし、スクリプトを実行する必要があります。例:

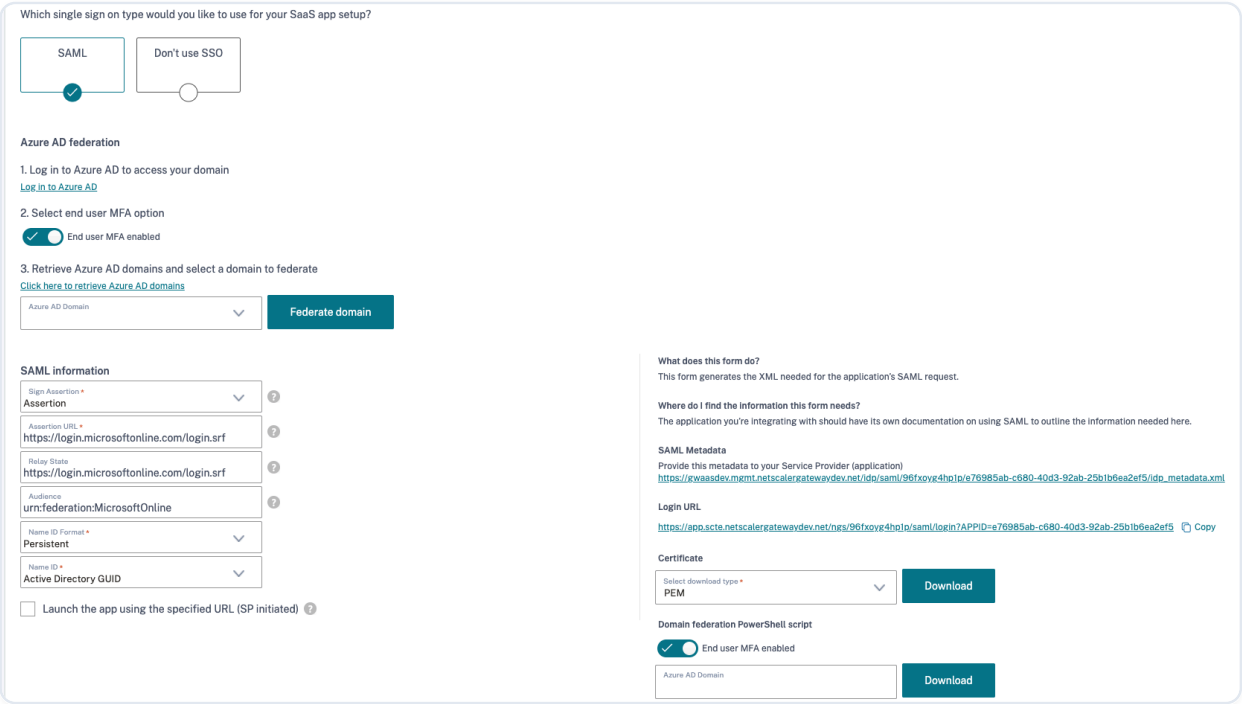
- クラウドポータルから顧客 ID やアプリ ID などのデータをコピーします。
- クラウドポータルから証明書をダウンロードします。
- PowerShell スクリプトを実行します。

この手動のコピー＆ペースト操作はエラーを引き起こす可能性があり、その結果フェデレーションが成功しない場合があります。

ドメインをフェデレーションする手順は、Citrix Secure Private サービスユーザーインターフェイスに統合され、フェデレーションプロセスが自動化されました。ユーザーがインターフェイスの適切なリンクをクリックすると、PowerShell スクリプトがバックエンドで実行されます。ユーザーはクラウドポータルと PowerShell を切り替える必要がありません。

ドメインを自動的にフェデレーションする手順

1. O365 アプリを構成します。詳細については、「Secure Private Access サービスで O365 アプリを構成する」を参照してください。
2. シングルサインオンで、**SAML** を選択します。



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

3. 資格情報を使用して Microsoft Entra ID にログオンします。 **Log in to Entra ID** をクリックすると、認証のために Microsoft Entra ID ログオンポータルにリダイレクトされます。
   - 認証には OAuth プロトコルが使用されます。認証が成功したら、ドメインのフェデレーションに同意する必要があります。
   - **Select end user MFA option** は、デフォルトで有効になっています。
4. すべてのドメインのリストを表示するには、**Click here to retrieve Entra ID Domains** をクリックします。
5. フェデレーションするドメインを選択し、**ドメインのフェデレーション**をクリックします。

> **注：**
>
> - **ドメインのフェデレーション**をクリックすると、PowerShellスクリプトがバックエンドで実行され、ドメインがフェデレーションされます。
> - 必要に応じて、インターフェイスからPowerShellスクリプトをダウンロードすることもできます。**ドメインフェデレーションPowerShellスクリプト**で、**ダウンロード**をクリックします。

多要素認証 (MFA) の抑制

ユーザーがCitrix Workspaceへのユーザー認証中にMFAをすでに入力している場合、MFAを抑制するオプションがO365アプリの高度な属性に追加されます。

- **属性名：**「`http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod`」、,
- **属性値：**「`http://schemas.microsoft.com/claims/multipleauthn`」

Microsoft Entra IDがこのクレームを受け入れるには、次のPowerShellコマンドを使用してフェデレーションします。

```
Set-MsolDomainAuthentication -DomainName $dom –federationBrandName $fedBrandName
-Authentication Federated -PassiveLogOnUri $uri -LogOffUri $logoffuri
-SigningCertificate $certData -IssuerUri $IssuerUri
-PreferredAuthenticationProtocol SAMLP -SupportsMfa $true
```

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

注：

IdP開始フローはリレーステートを尊重しません。SP開始フローを使用して、アプリに直接アクセスしてください。

Citrix Workspaceでの個々のOfficeスイートアプリケーションの構成

個々のOfficeスイートアプリケーションを構成するには、以下を実行します。

1. 前のセクションで詳述されているように、ドメインフェデレーションを完了します。
2. O365テンプレートを選択します。
3. アプリの名前を、たとえばMS Wordに変更します。
4. それに応じてアプリのURLを変更します。

ワード: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2FWord%3 domain>`

パワーポイント: `<https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2Fpowerp domain>`

エクセル: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2FExcel% domain>`

CRM/Dynamics オンライン: `https://<tenant>.crm.dynamics.com/?whr=<federated domain>`

ビジネス向け OneDrive: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2F<tenant>-my.sharepoint.com%2F&whr=<federated domain>`

Outlook カレンダー: `https://outlook.office.com/owa/?realm=<federated domain>&path=/calendar/view/Month`

Exchange Online への アウトルック Web アクセス: `https://outlook.com/owa/<federated domain>`

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

SharePoint オンライン: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2F<tenant>.sharepoint.com%2F&whr=<domain>`

チームズ: `https://login.microsoftonline.com/common/oauth2/authorize?client_id=cc15fd57-2c6c-4117-a88c-83b1d56b4bbe&response_mode=form_post&response_type=code+id_token&scope=openid+profile&domain>`

Microsoft Entra ID に統合されたサードパーティ製アプリ

Box、Salesforce、ServiceNow、Workday などのサードパーティ製アプリケーションを統合している場合は、これらのアプリのスマートリンクをMicrosoft Entra IDから取得できます。

次の手順を実行します。

1. Microsoft Entra ID ポータル `<https://portal.azure.com>` にログインします。
2. **すべてのサービス > Azure Active Directory** を選択し、ディレクトリを選択します。

   すべてのサービスを選択 (/en-us/citrix-secure-private-access/media/all-services-aad.png)
3. **エンタープライズアプリケーション** を選択し、スマートリンクを生成するアプリケーションを選択します。

   エンタープライズアプリケーションを選択 (/en-us/citrix-secure-private-access/media/select-enterprise-application.png)
4. **プロパティ** を選択し、ユーザーアクセスURLをコピーします。

   プロパティを選択 (/en-us/citrix-secure-private-access/media/set-properties-and-copu-user-access-url.png)
5. URLに `whr` を追加すると、例のURLに示されているように `whr` パラメーターが表示されます。

   例のURL: `https://myapps.microsoft.com/signin/Workday/12345678912345678912345678 96d64b&whr=ctxnsqa.net`

   注: Microsoft Entra ID がフェデレーション設定に基づいてユーザーを認証するために使用するIdPを認識し、そのIdPに自動的にリダイレクトするように、URLに `whr` を追加します。
6. 強化されたセキュリティ制御を設定します。
7. SSOを構成します。

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

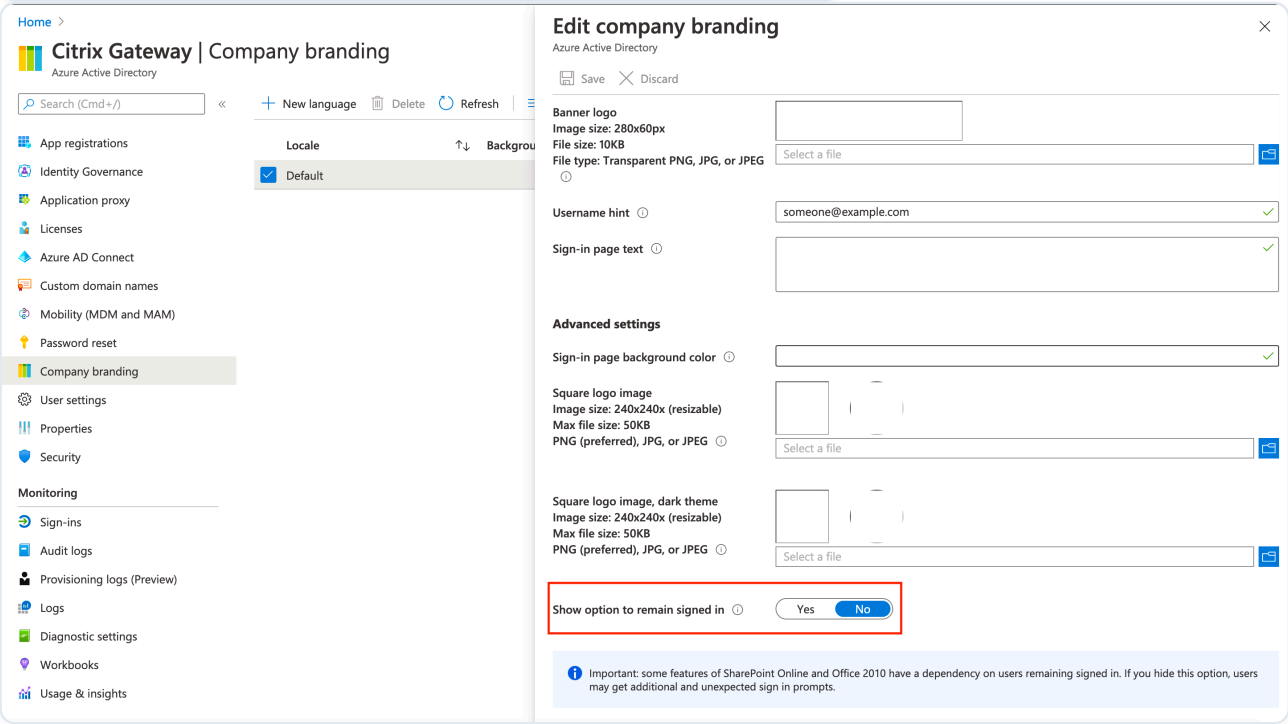
- 名前ID = AD GUID
- SP開始チェックボックスを有効にします
- アサーションURL = ログインURL

IdP開始フローを実行すると、ユーザーはMicrosoft Entra IDポータルページにリダイレクトされます。アプリページに直接アクセスしたい場合は、SAMLアサーションで正しいリレーステートを送信するSP開始フローが必要です。

注：

- プライマリドメインのフェデレーションが有効になっている場合、すべてのMicrosoft Entra IDユーザーは、Office 365アプリケーションへの認証時にCitrix Workspaceにリダイレクトされます。これは、影響を理解せずに実行すると、顧客に障害/インシデントを引き起こす可能性があります。
- ユーザーがMicrosoft Entra IDを使用してCitrix Workspaceにログオンする場合、ログインに使用されるユーザーのプライマリドメインはCitrix Gatewayサービスにフェデレーションされてはなりません。これによりループが発生します。このような場合は、Microsoft Entra IDにログインするユーザーのドメインとは異なる別のドメインを使用して、Citrix Secure Private Accessサービスにフェデレーションしてください。
- プライマリドメインがCitrix Secure Private Accessサービスにフェデレーションされている場合、Microsoft Entra ID内のそのドメインでのすべてのユーザーログインはCitrix Secure Private Accessサービスにリダイレクトされます。POCの場合、必要に応じて、プライマリドメインをフェデレーションする前にテストドメインをフェデレーションできます。
- Microsoft Entra IDでロケーションポリシーが有効になっている場合、ユーザーは企業ネットワークの許可されたIPアドレスのリストからのみアクセスする必要があります。このような場合、O365アプリをWebアプリとして公開し、そのトラフィックをConnector Appliance経由でルーティングできます。
- Microsoft Entra IDにログオンする際に、**サインイン状態を維持しますか？**というプロンプトを回避したい場合は、Microsoft Entra IDを使用してこの設定を変更できます。設定を変更した際に表示される重要なメッセージに注意し、必要に応じて元に戻してください。

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



参照リンク

Azure PowerShellモジュールリファレンス

Microsoft AzureでのOffice 365ディレクトリ同期の展開

ERP Cloudを構成する

以下のセクションでは、ERP Cloudの構成に関する詳細情報を提供します。

Citrix Gateway SaaSアプリケーション

ユーザーは、エンタープライズ資格情報を使用してERP Cloudに安全にログオンできます。

SAMLを介したSSOのためにERP Cloudを構成するには、以下を実行します。

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

1. ブラウザで、`https://<organizationid>.identity.oraclecloud.com/ui/v1/adminconsole/?root=security&security=external-idp` と入力し、Enterキーを押します。
2. ERP Cloudアカウントにログオンします。

   ERPアカウントにログオン(/en-us/citrix-secure-private-access/media/saas-erp-cloud-1.png)
3. ホームページの右上隅で、プロファイルのイニシャルをクリックし、をクリックします。

   ホーム画面の管理コンソール(/en-us/citrix-secure-private-access/media/saas-erp-cloud-2.png)
4. 左上隅にある省略記号をクリックします。
5. をクリックします。

   セキュリティを選択(/en-us/citrix-secure-private-access/media/saas-erp-cloud-3.png)
6. をクリックします。

   IDプロバイダーを追加するにはクリック(/en-us/citrix-secure-private-access/media/saas-erp-cloud-4.png)
7. 「IDプロバイダー」ページで、「SAML IdPの追加」をクリックします。

   SAML IdPの追加(/en-us/citrix-secure-private-access/media/saas-erp-cloud-5.png)
8. 「IDプロバイダー」ページで、次の情報を指定します。

   IdPの詳細(/en-us/citrix-secure-private-access/media/saas-erp-cloud-6.png)

   a. 署名証明書 – PEM証明書を貼り付けます。

      IdP証明書を取得するには、次の手順を実行します。

      - PuTTYを使用してNetScaler®インスタンスにリモートアクセスします。
      - /nsconfig/ssl フォルダーに移動し（シェルコマンド `cd` /nsconfig/ssl を使用）、Enterキーを押します。
      - cat `<certificate-name>` と入力し、Enterキーを押します。
      - -----BEGIN CERTIFICATE----- から -----ENDCERTIFICATE----- までのテキストをコピーします。
      - テキストをテキストエディターに貼り付け、`your organization name`.pem のような適切な形式でファイルを保存します。

        サンプル証明書(/en-us/citrix-secure-private-access/media/saas-erp-cloud-7.png)

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

b. 発行者ID – 一意の名前を入力します。

c. 署名ハッシュアルゴリズム – SAMLメッセージの署名に使用されるハッシュアルゴリズムを選択します。

d. 署名証明書を含める - IdPのメッセージの署名を検証するために署名証明書を含める場合は、このチェックボックスをオンにします。

e. グローバルログアウトが有効化されました - SAMLグローバルログアウトを有効にする場合は、チェックボックスを選択します。

f. SSOサービスURL – IdP URLの後に/saml/loginを付けて入力します。例: `https://<netscalerinstance>.com/saml/ login`

g. SSOサービスバインディング – 認証リクエストを送信するための適切なオプションをクリックします。

h. 要求されたNameID形式 – IdPのユーザー属性値をOracle Identity CloudServiceの対応する属性にマッピングするための適切な形式をクリックします。

i. IDプロバイダーユーザー属性 – ユーザーを一意に識別するために、IdPから受信した適切な属性値をクリックします。

j. Oracle Identity Cloud Serviceユーザー属性 – IdPから受信した属性をマッピングするために使用する適切な属性をクリックします。

9. 変更を保存をクリックします。

ServiceNow を構成する

ユーザーは、エンタープライズ資格情報を使用してServiceNowに安全にログオンできます。

SAML を介して SSO 用に ServiceNow を構成するには、次の手順を実行します。

1. ブラウザで `https://<your-organization>.service-now.com/` と入力し、**Enter** キーを押します。

   たとえば、ServiceNow にアクセスするために使用する URL が `https://myserver.servicenow.com` の場合、`<your-organization>` を `myserver` に置き換える必要があります。

   注:

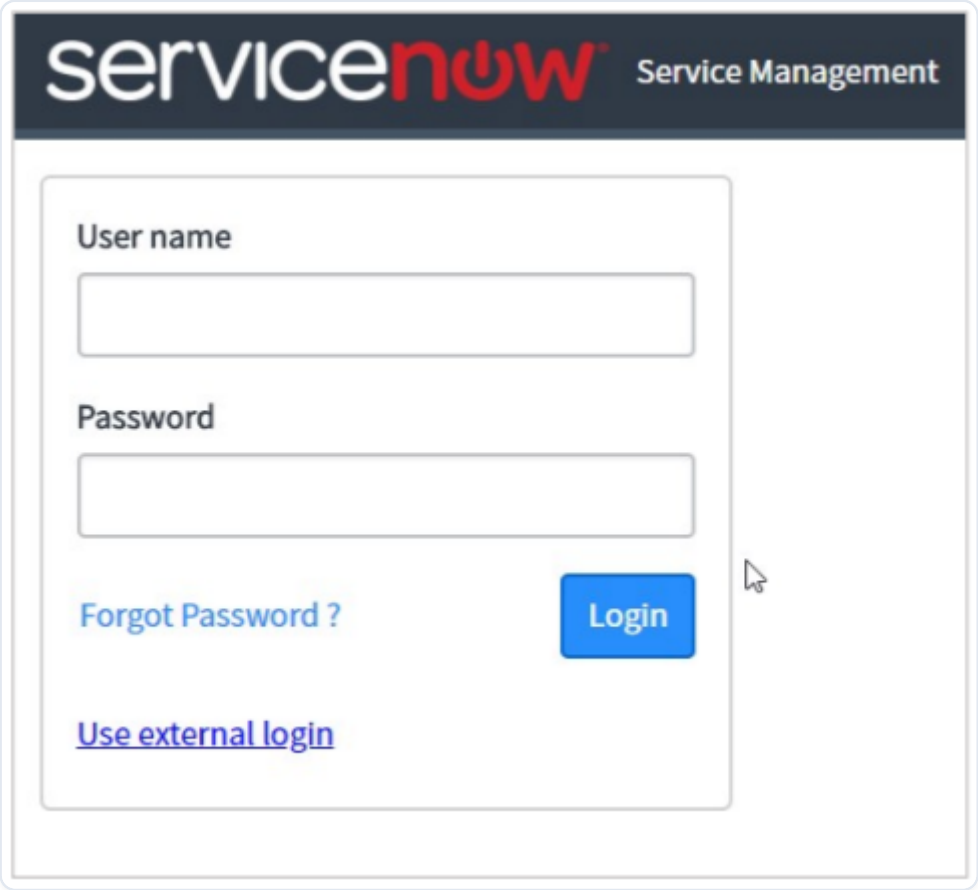
   - ServiceNow アプリを追加する際は、Citrix Gateway サービスユーザーインターフェイスに以下の詳細が入力されていることを確認してください。

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

  - アサーション URL: `https://<your-organizaton>.service-now.com/navpage.do`
  - リレー状態: `https://<your-organizaton>.service-now.com/`
  - オーディエンス: `https://<your-organizaton>.service-now.com/`
  - 名前 ID 形式: 「メールアドレス」を選択
  - 名前 ID: 「ユーザープリンシパル名 (UPN)」を選択

- 名前 ID 形式と名前 ID 属性は、ServiceNow に選択された認証方法によって異なります。

2. 管理者として ServiceNow アカウントにログオンします。



3. 左上隅で、フィルターナビゲーターを使用してプラグインを検索し、検索結果の**プラグイン**をクリックします。

   プラグインを検索(/en-us/citrix-secure-private-access/media/saas-servicenow-2.png)

4. 右側のペインの**システムプラグイン**セクションで、統合を検索します。

   統合プラグイン(/en-us/citrix-secure-private-access/media/saas-servicenow-3.png)

5. 検索結果で、**Integration - Multiple Provider Single Sign-OnInstaller** を右クリックし、**アクティブ化/アップグレード** をクリックします。

   アクティブなプラグイン(/en-us/citrix-secure-private-access/media/saas-servicenow-4.png)

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

6. **アクティブ化**をクリックします。

   進行状況バーにアクティブ化プロセスの完了が表示されます。

7. 左側のペインで、マルチプロバイダーSSOセクションまでスクロールし、**マルチプロバイダーSSO > IDプロバイダー**をクリックします。

   IDプロバイダーを追加(/en-us/citrix-secure-private-access/media/saas-servicenow-5.png)

8. 右側のペインで、**新規**をクリックします。

   SAMLを新しいIDプロバイダーとして追加(/en-us/citrix-secure-private-access/media/saas-servicenow-6.png)

9. **SAML**をクリックします。

   IdPの詳細(/en-us/citrix-secure-private-access/media/saas-servicenow-7.png)

10. メタデータURLがある場合は、**IDプロバイダーの新規レコード**セクションの**IDプロバイダーメタデータのインポート**ポップアップウィンドウで、**URL**をクリックし、メタデータURLを入力して**インポート**をクリックします。

    IDプロバイダーレコードフィールドの値は自動的に入力されます。

    メタデータXMLファイルをお持ちの場合は、XMLをクリックします。IDプロバイダーメタデータXMLデータをコピーしてボックスに貼り付けます。**インポート**をクリックします。

    IDプロバイダーレコードフィールドの値は自動的に入力されます。必要に応じて値を更新できます。

    自動入力されたIdPの詳細(/en-us/citrix-secure-private-access/media/saas-servicenow-8.png)

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

重要:

- Citrixでは、手動で構成するのではなく、メタデータXMLファイルをインポートすることをお勧めします。メタデータXMLファイルは、Citrix Cloudウィザード（**Citrix Gateway Service > Web/SaaSアプリの追加 > シングルサインオン > SAMLメタデータ**）からインポートできます。
- **詳細設定**タブでパラメーターを構成する際は、**ユーザーフィールド**の値がCitrix Gatewayサービスのユーザーインターフェイスで**名前IDフィールド**に構成されている値と一致していることを確認してください。

  ユーザーフィールドと名前IDフィールド(/en-us/citrix-secure-private-access/media/servicenow_user_field.png)

11. **送信**をクリックします。
12. 左側のペインで、x509証明書をクリックしてx509証明書をアップロードします。

    509証明書(/en-us/citrix-secure-private-access/media/saas-servicenow-10.png)
13. 右側のペインで、**新規**をクリックします。

    新しい509証明書を追加(/en-us/citrix-secure-private-access/media/saas-servicenow-11.png)
14. X.509証明書の新規レコードセクションで、次の情報を指定します。

    509証明書の詳細(/en-us/citrix-secure-private-access/media/saas-servicenow-12.png)

    名前 – 証明書の名前を入力します。

    - 形式 – 適切な形式をクリックします。例: PEM。
    - 有効期限通知 – チェックボックスをオンにします。
    - 種類 – 適切な種類をクリックします。
    - 有効期限時に通知 – 通知を受け取るには、 アイコンをクリックします。さらにユーザーを追加するには、 をクリックします。
    - アクティブ – チェックボックスをオンにします。
    - 簡単な説明 – 証明書の説明を入力します。
    - PEM 証明書 – PEM 証明書を貼り付けます。
      - **Citrix Cloud wizard (Citrix Gateway Service > Add a Web/SaaS App > Single sign on > Certificate)** から証明書をダウンロードします。

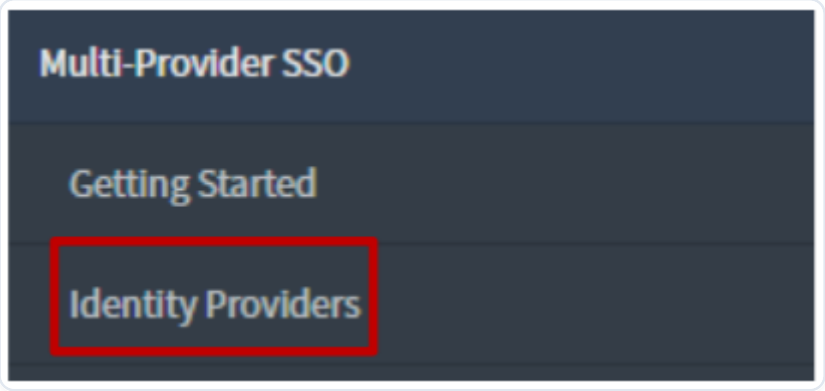
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ——BEGIN CERTIFICATE—— から ——ENDCERTIFICATE—— までのテキストをコピーします。
- テキストをテキストエディターに貼り付け、`<your organization name>.` のような適切な形式でファイルを保存します。

注: IdP の構成に XML ファイルを使用した場合、証明書を構成する必要はありません。

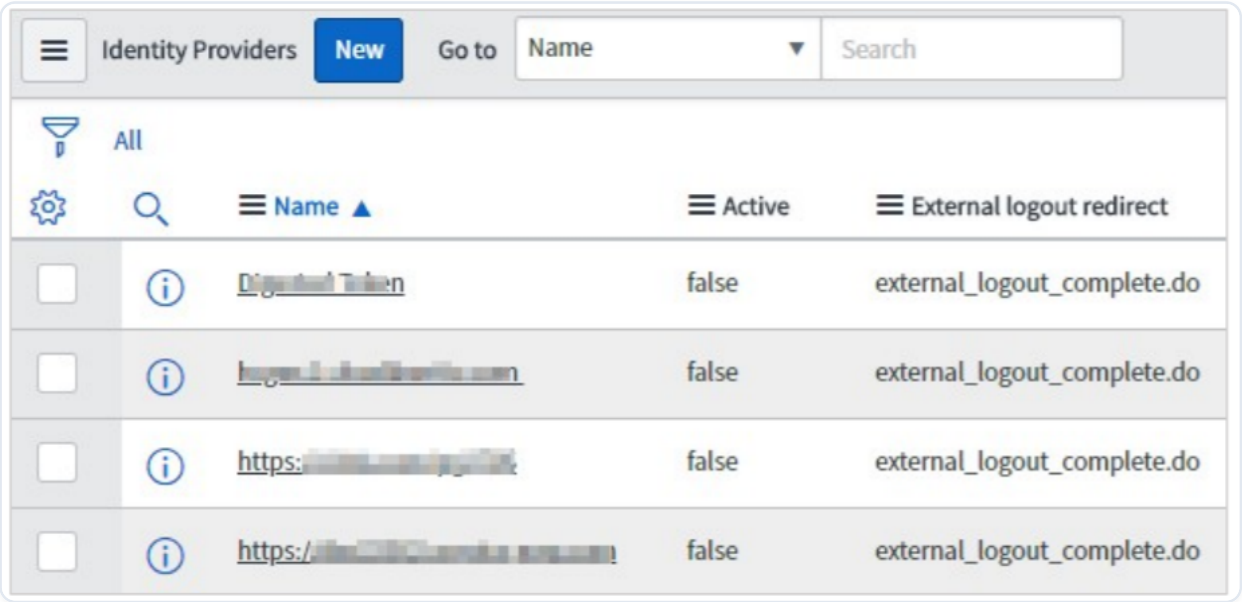
送信 をクリックします。

15. 左側のペインで、**ID プロバイダー** をクリックします。

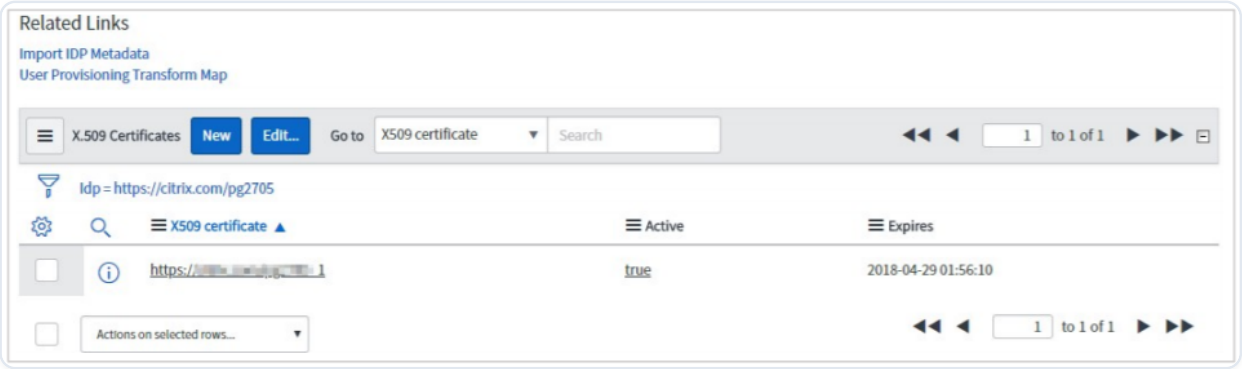


16. 追加したIDプロバイダーをクリックします。

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

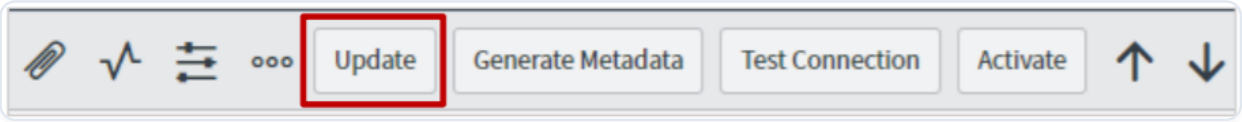


17. IDプロバイダーの詳細ページで、セクションまでスクロールします。行でX.509証明書を検索し、 をクリックして、IDプロバイダーの適切な証明書を追加します。



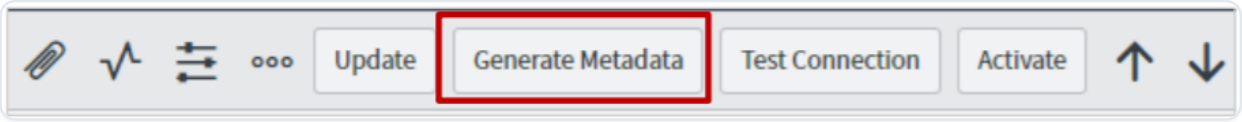
新しいX.509証明書を追加するには をクリックし、証明書を追加または削除するには をクリックします。

18. 変更を保存するには、IDプロバイダーの詳細ページで をクリックします。



19. IdP構成に使用するメタデータを取得するには、 をクリックします。

注： 更新を完了するには、 をクリックする必要があります。



サービスプロバイダーのメタデータが新しいウィンドウに表示されます。このメタデータを使用して、SPとIdPの両方でエンティティを検証できます。

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

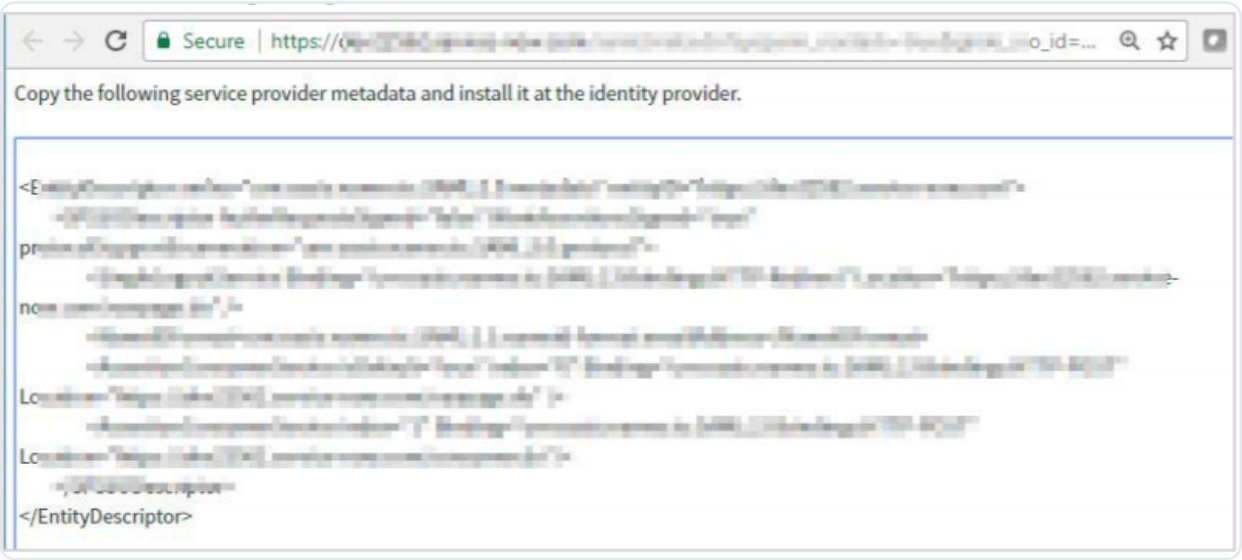


Tableau を構成する

ユーザーは、エンタープライズ資格情報を使用してTableauに安全にログオンできます。

SAML を介した SSO 用に Tableau を構成するには、次の手順を実行します。

1. 管理者として Tableau にログオンします。
2. メニューバーで をクリックします。
3. をクリックします。
4. 認証タイプで を選択し、 をクリックします。

   接続の編集 (/en-us/citrix-secure-private-access/media/tableau-saml-1.png)

   メタデータのエクスポート (/en-us/citrix-secure-private-access/media/tableau-saml-pre1.png)

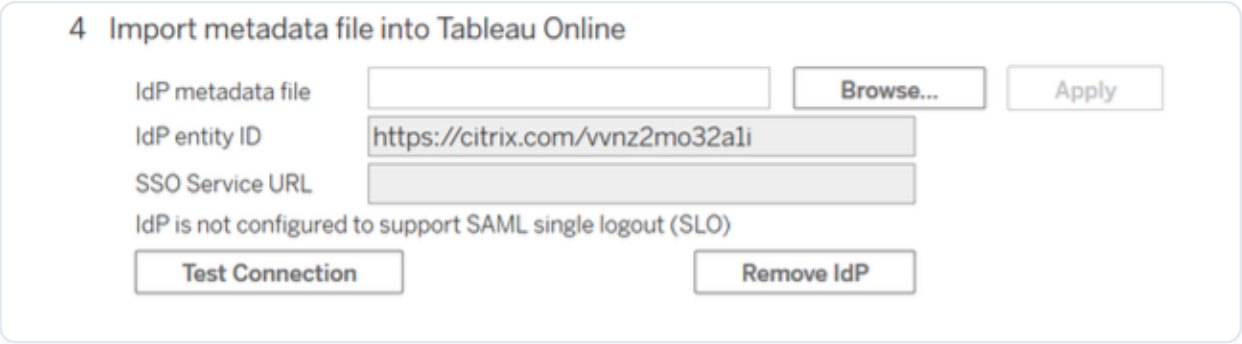
   メタデータのダウンロード (/en-us/citrix-secure-private-access/media/tableau-saml-2.png)
5. Citrix Cloud ウィザードからメタデータファイルをダウンロードします (**Citrix Gateway Service > Web/SaaS アプリの追加 > シングルサインオン > SAML メタデータ**)。

注:

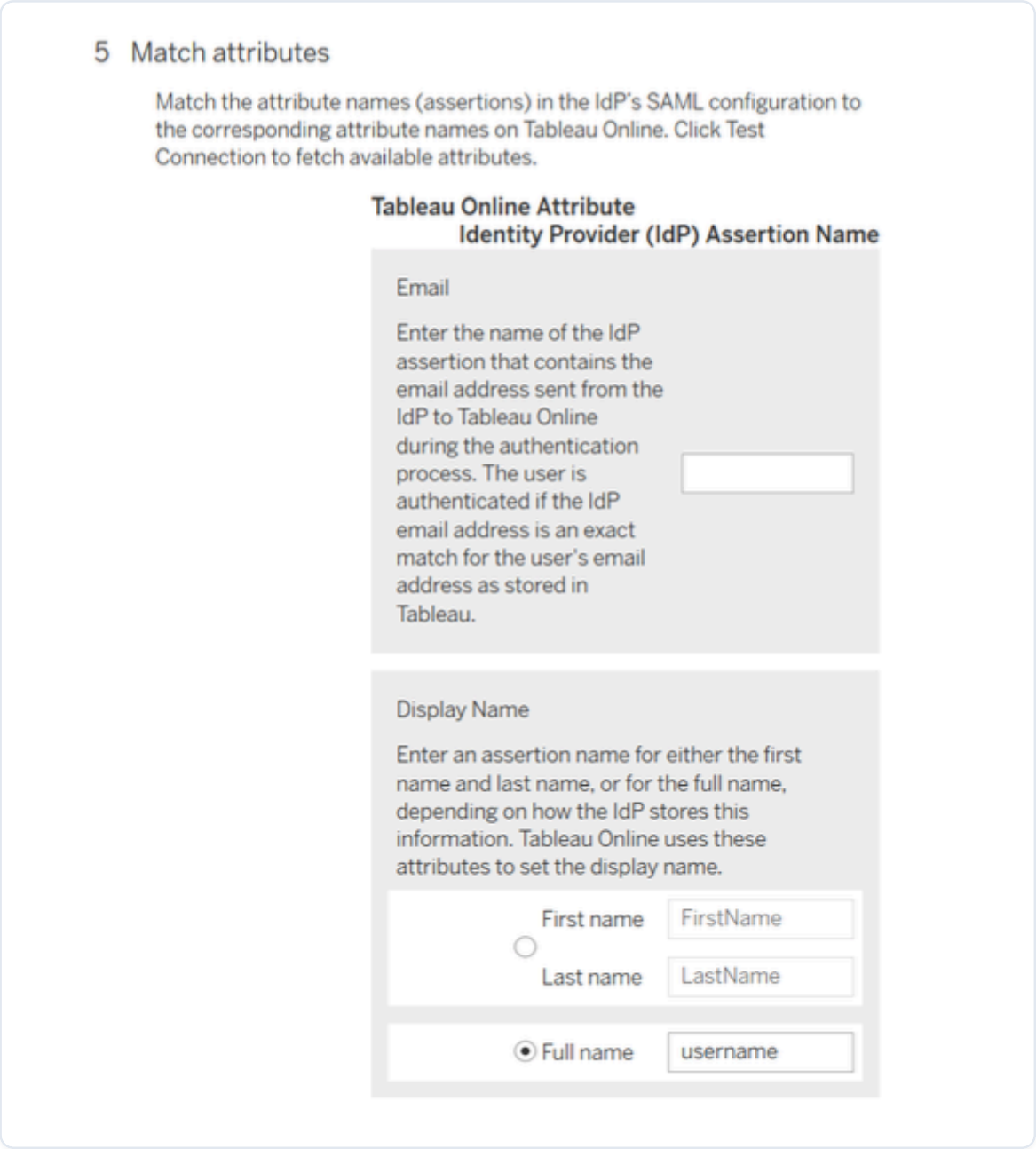
- Citrix® は、メタデータ XML ファイルを手動で構成するのではなく、インポートすることをお勧めします。
- Citrix Cloud ウィザードから証明書をダウンロードできます (**Citrix Gateway Service > Web/SaaS アプリの追加 > シングルサインオン > 証明書**)。

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

6. IdP メタデータファイルを **Tableau Online** にインポートします。

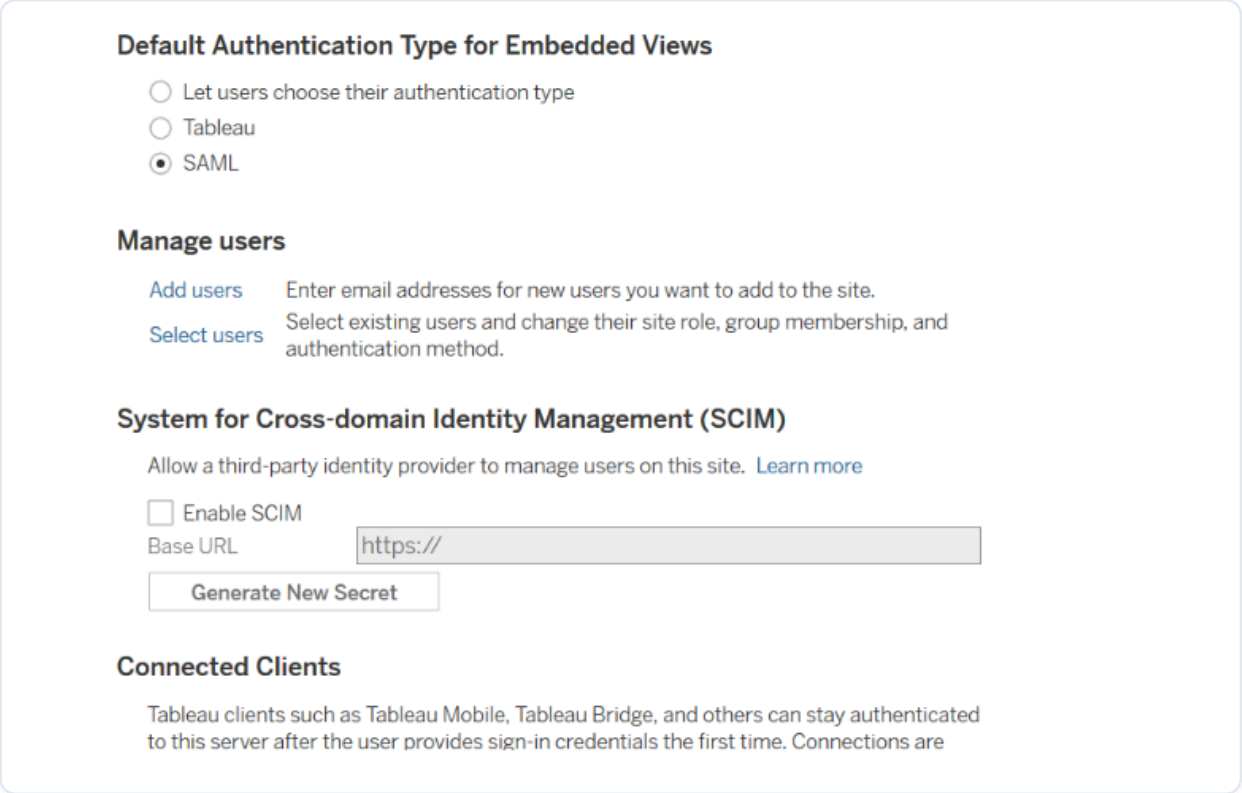


7. IdPエンティティIDを `https://citrix.com/<customerID>` の形式で入力します。
8. **接続テスト**をクリックします。
9. IdP属性をTableau属性と一致させ、**適用**をクリックします。



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

10. 下にスクロールし、埋め込みビューのデフォルト認証タイプとして**SAML**を選択します。



11. 必要に応じて、SSO用のユーザーを追加または選択します。

    - 新しいユーザーを追加するには、**ユーザーの追加**をクリックしてメールアドレスを入力します。
    - 既存のユーザーの場合は、**ユーザーの選択**をクリックし、必要に応じて変更を加えます。

Workday の構成

以下のセクションでは、Workday の構成に関する詳細情報を提供します。

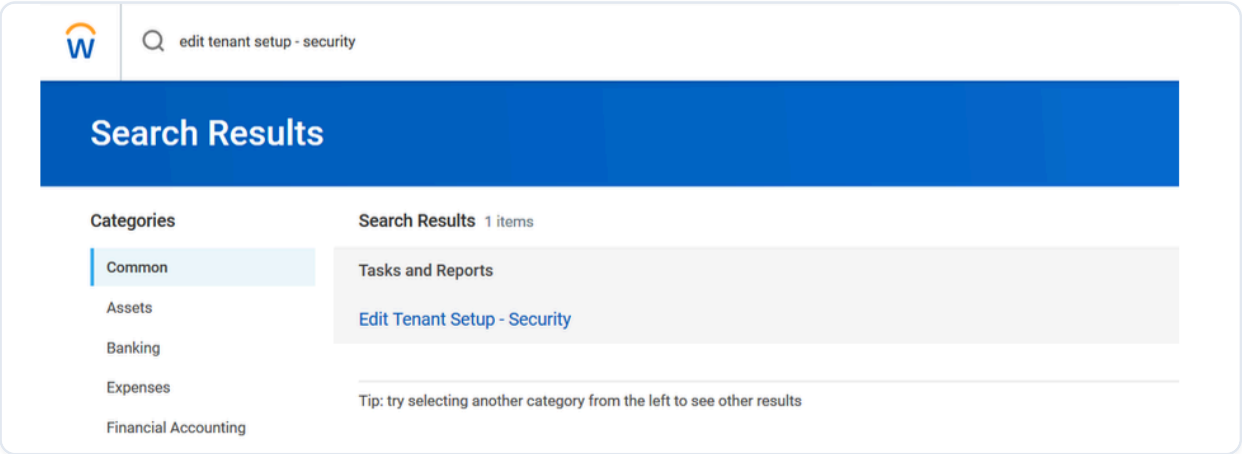
Citrix Gateway SaaS アプリケーション

ユーザーは、エンタープライズ資格情報を使用して Workday に安全にログオンできます。

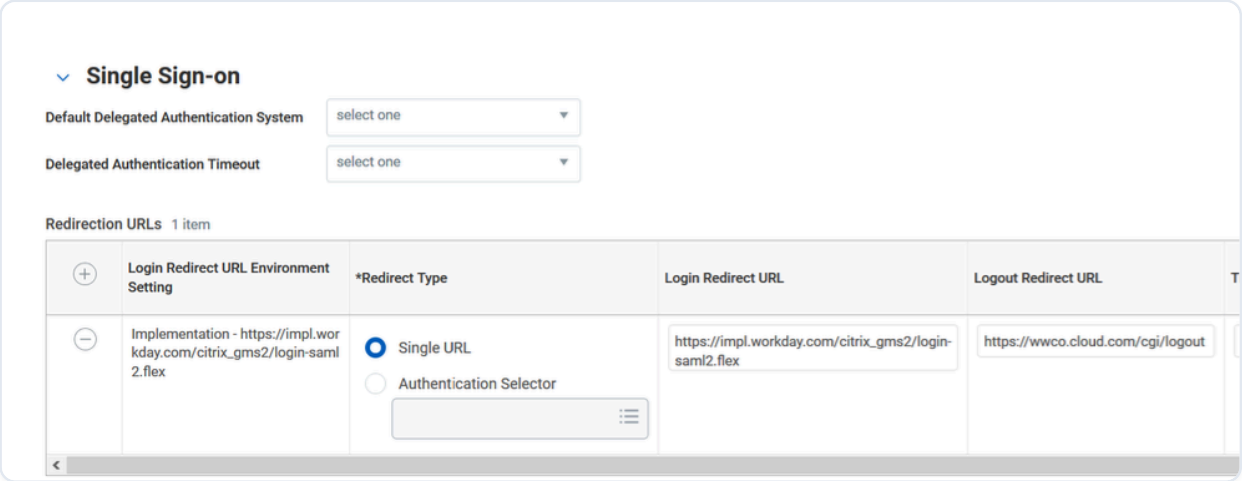
SAML を介した SSO 用に Workday を構成するには、次の手順を実行します。

1. 管理者として Workday にログオンします。
2. **Edit Tenant Setup - Security** に移動し、**Edit Tenant Setup** をクリックします。

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

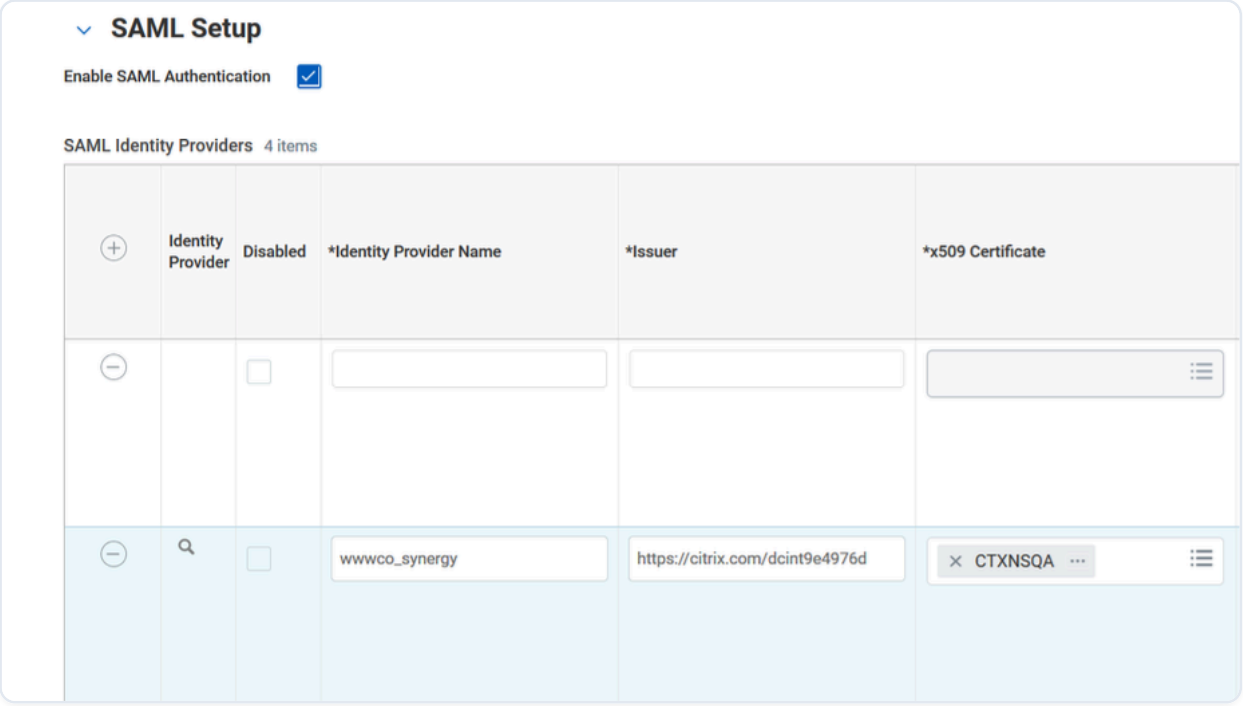


3. **Single Sign-on** をクリックします。



4. リダイレクト URL テーブルのプラスアイコンをクリックします。
5. **Login Redirect URL** に、`https://impl.workday.com/<customer>/login-saml2.flex` の形式で URL を入力します。
6. **Enable SAML Authentication** をクリックします。

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



7. SAML Identity Providers の下のプラス (+) アイコンをクリックして行を追加し、次の情報を指定します。

   a. 「**IDプロバイダー名**」 - Citrix Gatewayと入力します。

   b. 「**発行者**」 - 一意の発行者名を入力します。

8. 「**x509証明書**」で、X509証明書アイコンをクリックし、「**x509公開キーの作成**」をクリックします。

9. Citrix Cloudウィザードから証明書をダウンロードします（**Citrix Gateway Service > Web/SaaSアプリの追加 > シングルサインオン > 証明書**）。

   証明書の作成(/en-us/citrix-secure-private-access/media/workday-4.png)

10. 証明書のテキストを「——BEGIN CERTIFICATE——」から「——ENDCERTIFICATE」までコピーし、証明書フィールドに貼り付けます。

11. 「**OK**」をクリックします。

Zoom を構成する

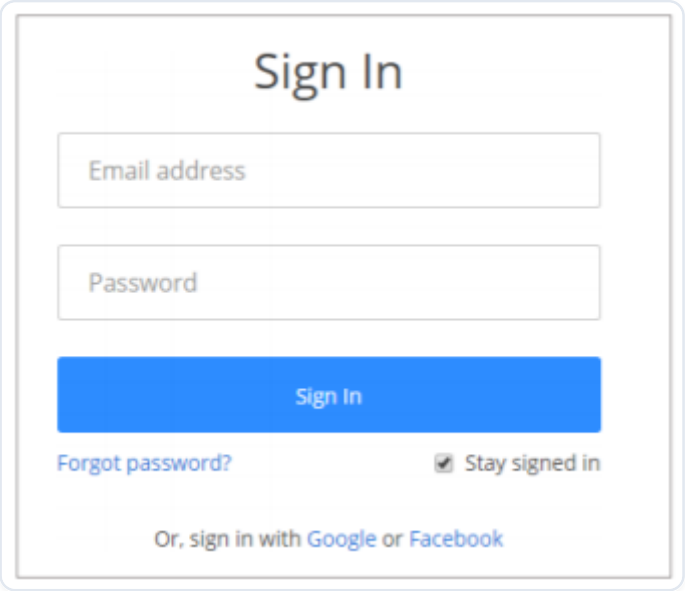
以下のセクションでは、Zoom の構成に関する詳細情報を提供します。

Citrix Gateway SaaS アプリケーション

SSO 用に Zoom を構成すると、管理者は NetScaler を使用してユーザーを管理できるようになります。ユーザーは 企業の資格情報を使用して Zoom に安全にログオンできます。

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

1. ブラウザで `https://zoom.us/signin` と入力し、Enter キーを押します。
2. Zoom アカウントにログオンします



3. **マイプロフィール**ページで、左側のペインの**詳細設定**セクションの下にある**シングルサインオン**をクリックします。

4. SAML タブで、バニティ URL ボックスに表示されている URL をコピーします。この URL は NetScaler の構成に必要です。
5. サインインページ URL ボックスに、NetScaler アプリの IdP URL を入力します: `https://<NetscalerGateway FQDN>/saml/login`
6. サインアウトページ URL ボックスに、https:< NetScaler Gateway FQDN >.com/cgi/tmlogout と入力します。
7. ID プロバイダー証明書ボックスに、ID プロバイダー証明書を貼り付ける必要があります。

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

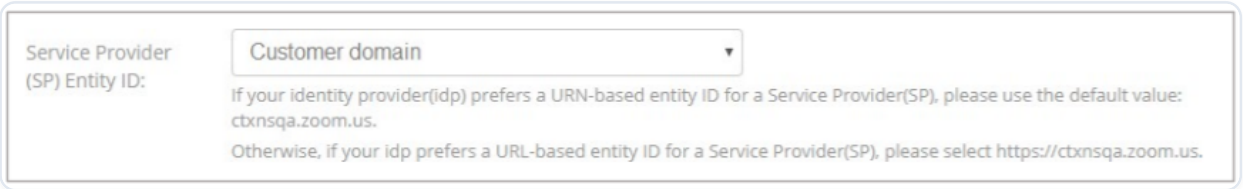
8. IdP 証明書をアップロードするには、以下を実行します。

   - PuTTY を使用して NetScaler インスタンスにリモートでアクセスします。
   - 「/nsconfig/ssl」フォルダー（cd/nsconfig/ssl）に移動し、Enterキーを押します。
   - 「cat certifcate-name.pem」と入力し、Enterキーを押します。

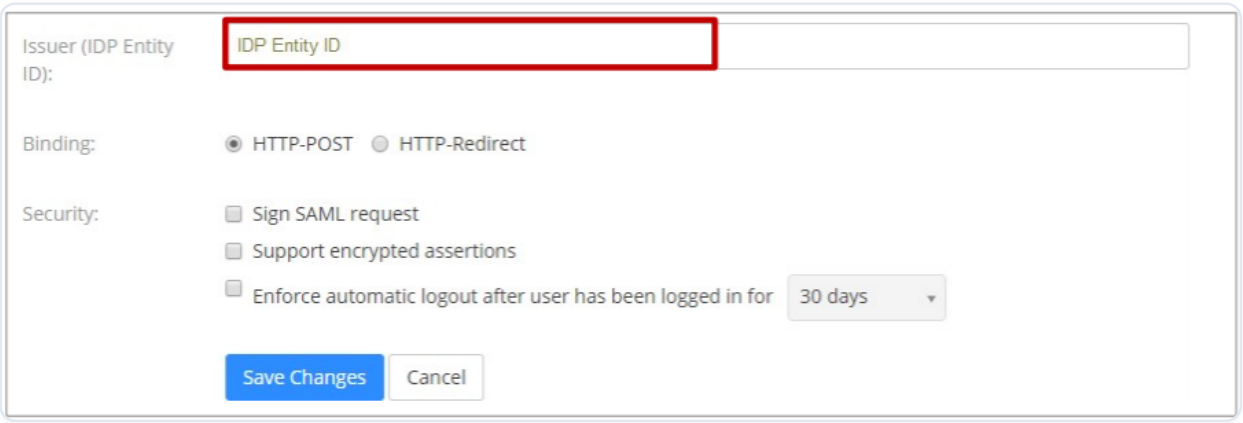
     注: これはSAML IdP署名証明書です。

   - 「-----BEGIN CERTIFICATE-----」と「-----ENDCERTIFICATE-----」の間のテキストをコピーします。

9. サービスプロバイダー (SP) エンティティIDボックスに表示されているURLをコピーします。



10. 発行者 (IdPエンティティID) ボックスに一意の発行者IDを入力し、 をクリックします。



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

アクセスモードベースのポリシー適用

アクセスモードベースのポリシー適用により、管理者はユーザーがアプリケーションに接続する方法を制限できます。接続は、ブラウザベースのクライアントまたはCitrix Secure Accessクライアントを介して行うことができます。以前は、Secure Private Accessには、どのクライアントがセッションを開始するかに基づいてアクセスを制限する方法がありませんでした。アクセスモードはその機能を追加します。

たとえば、管理者は、SSHおよびRDPアプリケーションがChrome Enterprise Premiumなどのブラウザを介してのみ到達可能であり、Citrix Secure Accessクライアントを介してトンネルされないように構成できます。これにより、ブラウザベースのセキュリティ制御が常に適用されるようになります。

注:

アクセスモードは制限条件にすぎません。アクセスを絞り込むことはできますが、それ自体でアクセスを許可することはできません。ポリシー内の他のすべての条件は引き続き評価されます。

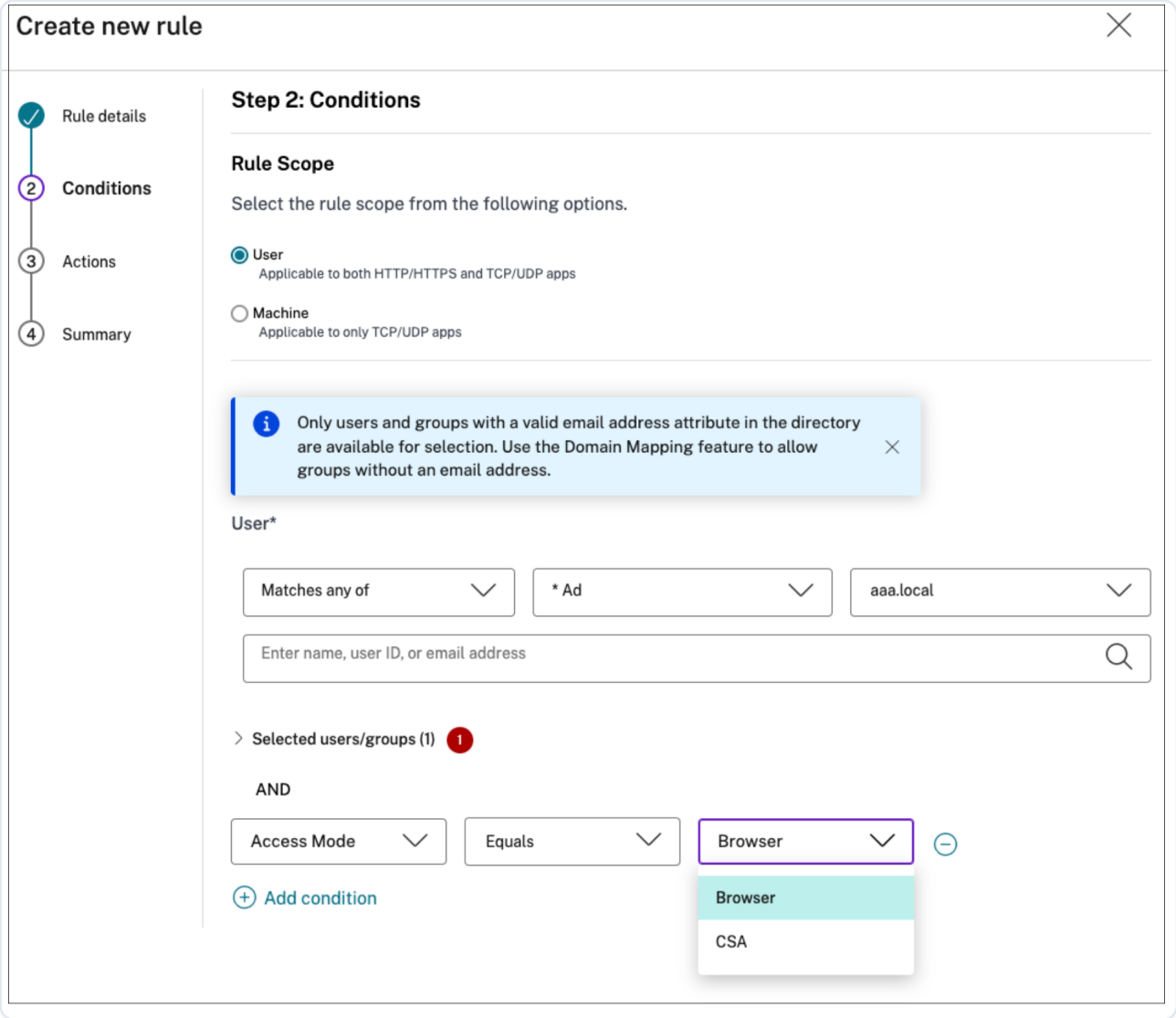
仕組み

アクセスモードはSecure Private Access管理コンソールで構成され、3つのポリシータイプのいずれかのルールに追加できます。

- アダプティブアクセスポリシー
- セッションポリシー
- ブラウザポリシー

次の図は、アクセスポリシーのルール条件の例を示しています。

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



エンドユーザーエクスペリエンス

アクセスモードに基づいて、アプリケーションの列挙と起動が許可または制限されます。

- **一致するクライアント** — アプリケーションが列挙され、正常に起動します。
- **一致しないクライアント** — アプリケーションは列挙中にアプリリストに表示されず、起動試行はブロックされます。ユーザーは標準のアクセス拒否ページに送られます。新しい拒否メッセージは導入されません。
- **判別不能なセッション** — アクセスモードを判別できない場合（たとえば、一部のモバイル Secure Accessセッション）、アクセスモード条件はスキップされ、セッションは影響を受けません。他のすべての条件は引き続き適用されます。

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

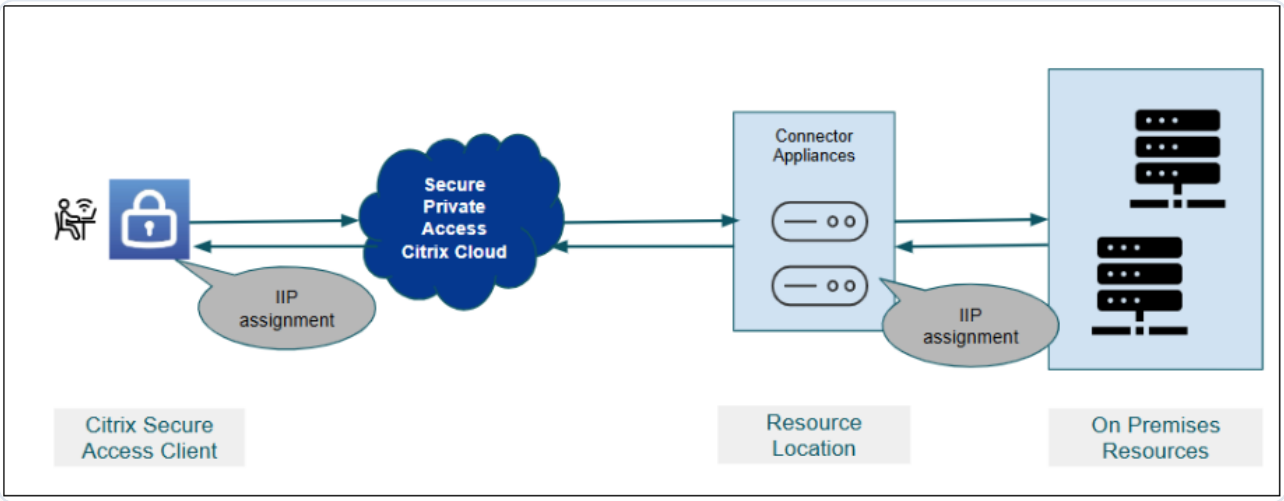
サーバーからクライアントへの接続のサポート - プレビュー

従来のクライアントサーバー設定では、リモートユーザーはHTTP、TCP、UDP接続を使用して顧客のリソースロケーションにあるリソースにアクセスできます。しかし、ユーザーのプライバシーとセキュリティを保護しながら、プッシュ構成、リモートアシスタンス、アプリケーションアクセス、アプリのインストールなどのタスクのために、サーバーまたはバックエンドシステムがリモートクライアントデバイス（例：ラップトップ、スマートフォン、タブレット）との接続を開始する必要があるシナリオがあります。Secure Private Accessは、顧客のリソースロケーションにあるサーバーがリモートクライアントとのTCP/UDP接続を確立できるサーバーからクライアントへの接続をサポートします。

- サーバーからクライアントへの接続を有効にするために、Secure Private Accessはサーバーからクライアントへのアプリを導入します。このアプリは、クライアントの詳細（ポート、プロトコル）とバックエンドサーバーのIP CIDR範囲で構成できます。
- サーバーからクライアントへのアプリタイプが作成された後、サーバーからクライアントへの接続を有効にするために、これらのアプリケーションに適切なアクセスポリシーを構成する必要があります。

サーバーからクライアントへの接続の仕組み

次の図は、サーバーからクライアントへの接続アーキテクチャの例を示しています。



次の手順は、サーバーからクライアントへの接続ワークフローを示しています。

1. ユーザーがCitrix Secure Access™クライアントにログインすると、指定されたクライアント内部IPアドレスプールから内部IPアドレスがユーザーに割り当てられます。この割り当ては、構成されたリソースロケーション、IP CIDR、およびIPアドレスプール構成内のユーザーコンテキストに基づいています。

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

2. この割り当てられたIPアドレスは、構成されたリソースロケーションおよびIPプール内の特定のコネクタアプライアンスに関連付けられます。このコネクタアプライアンスは、バックエンドの顧客リソースロケーションのために、このIPアドレスに関連する接続を所有および管理します。
3. バックエンドサーバーは、サーバーからクライアントへのアプリケーション構成で指定されたクライアントアプリケーションのポートを使用して、割り当てられたクライアント内部IPアドレスを使用してリモートクライアントへのTCP/UDP接続を開始します。
4. コネクタはSecure Private Accessと通信して、クライアントとの接続を確立します。
5. Secure Private Accessは、バックエンドサーバーがサーバーからクライアントへのアプリケーションで構成されているかどうかを確認し、関連するアクセスポリシーを評価して、クライアントマシンへのアクセスを許可するかブロックするかを決定します。
6. ポリシーがアクセスを許可する場合、Secure Private Accessはリモートクライアントマシンに接続します。クライアントマシンがドメイン参加している場合、そのマシンのFQDNはIIPアドレスに登録されます。マシンはFQDNまたは内部IPアドレスのいずれかでアクセスできます。
7. ユーザーがログアウトすると、割り当てられた内部IPアドレスはコネクタアプライアンスとアクティブセッションの両方から解放されます。同じユーザーが15日以内に再度ログインした場合、ユーザーは同じIPアドレスを取得しますが、そうでない場合は他のユーザーの使用のために解放されます。

サーバーからクライアントへのアプリを作成する

以下のセクションでは、サーバーからクライアントへのアプリの作成に関する詳細を説明します。

前提条件

- クライアント内部IPアドレスプールが作成されます。IPアドレスプールは、ユーザーと関連デバイスに一意のIPアドレスを割り当てるために不可欠です。詳細については、「クライアント内部IPアドレスプール」を参照してください。
- お客様の管理者は、リソースロケーションネットワーク用に空いているイントラネットIP CIDRサブネットを割り当てる必要があります。このIP CIDRは、他のリソースIPアドレスと競合してはなりません。
- お客様の管理者は、どのグループ/コンテキストのユーザーがどのリソースロケーションからイントラネットIPアドレスを割り当てられるかを決定する必要があります。ユーザー対IPアドレスの比率を1:3に維持することをお勧めします。つまり、ログインするユーザー数が1000人の場合、クライアントIPプールに3000個のIPアドレスを割り当てることをお勧めします。

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

- 空いているIIPサブネットとコネクタのプライマリIPアドレスは、同じネットワークおよびサブネットに属している必要があります。
- 他の場所（IPプールで構成されていない）のサーバーがクライアントに接続できるように、リソースロケーション間で相互接続を維持する必要があります。
- サーバーからクライアントへのアプリをサポートするCitrix Secure Accessクライアントのバージョンを使用していることを確認してください。
  - Windows 24.11.1.17以降
  - macOS 25.01.1以降
  - Linux 25.2.2以降

サーバーからクライアントへのTCP/UDPアプリを構成するには、次の手順を実行します

1. Citrix Cloudにログインし、**Secure Private Access**を選択します。
2. **アプリケーション > アプリ構成**をクリックし、**アプリの追加**をクリックします。
3. 「**テンプレートの選択**」セクションで、「**スキップ**」をクリックします。テンプレートはSaaSアプリでのみ利用可能です。

   クライアント-サーバーアプリの作成(/en-us/citrix-secure-private-access/media/spa-server-client-app-details1.png)
4. 場所を「**社内ネットワーク内**」に選択します。
5. 次の詳細を入力します。
   - **アプリの種類** – 「**TCP/UDP - サーバーからクライアントへ**」を選択します。
   - **アプリ名** – アプリケーションの名前。
   - **アプリの説明** – 追加するアプリの説明。このフィールドはオプションです。
   - **サーバー** - クライアントマシンとの接続を確立できるバックエンドサーバーのIPアドレス範囲。これにより、この範囲内のIPアドレスを持つサーバーのみがクライアントのポートにアクセスできるようになります。
   - **ポート** – バックエンドサーバーが接続を開始できるクライアントマシンのポート番号。
   - **プロトコル** – TCPまたはUDP。
6. さらにサーバーとポートを追加するには、「**追加**」をクリックします。
7. 「**保存**」をクリックします。アプリが「**アプリ構成**」ページに追加されます。

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

アプリケーションを設定した後、アプリケーションページからアプリを編集または削除できます。そのためには、アプリと同じ行にある省略記号ボタンをクリックし、それに応じてアクションを選択します。

サーバーからクライアントへのアプリを作成したら、要件に応じてアクセスポリシーを作成します。

注:

既存のすべてのアクセスポリシーは、サーバーからクライアントへのアプリケーションでサポートされています。構成されたアクセスポリシーにおいて、コンテキストが「許可」と評価されたユーザーに対して、サーバーからクライアントへのアクセスが許可されます。

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