

モバイル生産性アプリ

Contents

モバイル生産性アプリのリリーススケジュール	21
Secure MailおよびSecure Webの段階的リリースプロセスについて	21
機能フラグ管理の前提条件	21
モバイル生産性アプリのサポート	23
サポートされているオペレーティングシステム	23
その他の考慮事項と制限	24
セキュアメール	24
セキュアウェブ	25
QuickEdit	25
シトリックス コンテンツ コラボレーション™ エンドポイント管理向け	25
ShareConnect	25
シトリックス セキュア ノーツ および シトリックス セキュア タスク	25
管理者のタスクと考慮事項	26
機能フラグの管理	26
以下のURLへのトラフィックを有効にする	26
ドメインによる許可リストの作成	26
許可リストにIPアドレスを記載する	27
LaunchDarklyのシステム要件	27
サポートされているアプリストア	27
公開アプリストア配信の有効化	28
Appleプッシュ通知	29
パブリックアプリストアに関するFAQ	29
アンドロイド	29
iOS	30
モバイル生産性向上アプリの MDX ポリシー	33
Android版Secure Mailのデュアルモード	33

前提条件	34
制限事項	34
内部ネットワークへのユーザー接続	35
ネットワークアクセス制限	36
Endpoint Managementクライアントプロパティ	36
ユーザーパスワードのキャッシュ	36
非アクティブタイマー	37
Citrix PIN認証	37
指紋認証またはTouch ID認証	37
指紋認証の要件	37
指紋認証を構成するには	38
Google アナリティクス	38
Google Analyticsを無効にする	38
モバイル生産性アプリのMDXポリシーの概要	39
認証	39
デバイスのパスコード	39
アプリのパスコード	39
オンラインセッションの猶予期間 (分)	39
最大オフライン期間	40
代替シトリックス ゲートウェイ	40
デバイスセキュリティ	40
ジェイルブレイクまたはルート化されたデバイスをブロックする	40
デバイスロックを必須	40
ネットワーク要件	41
Wi-Fiを必須	41
許可されたWi-Fiネットワーク	41
その他のアクセス	41
アプリ更新猶予期間 (時間)	41

必須アップグレードの無効化	42
ロック時にアプリデータを消去	42
アクティブポーリング期間 (分)	42
暗号化	42
暗号化の種類	42
非準拠デバイスの動作	43
MDX暗号化を有効にする	43
暗号化キー	43
プライベートファイルの暗号化	43
プライベートファイルの暗号化の除外	43
パブリックファイルのアクセス制限	43
公開ファイルの暗号化	44
公開ファイルの暗号化除外	44
公開ファイルの移行	44
暗号化を有効にする	44
データベース暗号化の除外	45
ファイル暗号化の除外	45
アプリのインタラクション	45
セキュリティグループ	45
切り取りとコピー	45
貼り付け	45
ドキュメント交換 (Open in)	46
フィルタリングから除外されるURLドメイン	46
許可されたセキュアWebドメイン	46
接続セキュリティレベル	46
受信ドキュメント交換 (Open In)	46
制限付きOpen In例外リスト	46
アプリのURLスキーム	47

許可されたURL	47
明示的なログオフ通知	47
アプリの操作 (アウトバウンドURL)	47
URLフィルタリングから除外されるドメイン	47
許可されるURL	47
許可されたセキュアWebドメイン	48
アプリの制限	48
カメラをブロック	48
ギャラリーをブロック	48
写真ライブラリをブロック	48
マイク録音をブロック	48
音声入力をブロック	48
位置情報サービスをブロック	49
SMS作成をブロック	49
画面キャプチャをブロック	49
デバイスセンサーをブロック	49
NFCをブロック	49
iCloud をブロック	49
Look Up をブロック	49
ファイルバックアップをブロック	50
AirPrint をブロック	50
印刷をブロック	50
AirDropをブロック	50
ファイル添付をブロック	50
メール作成をブロック	50
Facebook および Twitter API をブロックする	51
画面コンテンツを不明瞭にする	51
サードパーティ製キーボードをブロックする	51

アプリログをブロック	51
ShareFileを有効にする	51
ファイルからの添付を有効にする	51
アプリのネットワークアクセス	52
ネットワークアクセス	52
マイクロVPNセッションが必要	52
マイクロVPNセッションの猶予期間（分）	52
除外リスト	52
localhost 接続をブロックする	52
証明書ラベル	52
アプリログ	53
デフォルトのログ出力	53
デフォルトのログレベル	53
最大ログファイル数	53
最大ログファイルサイズ	53
アプリログのリダイレクト	53
ログの暗号化	53
アプリのジオフェンス	54
中心点の経度	54
中心点の緯度	54
半径	54
アプリ設定	54
セキュアメール エクスチェンジサーバー	54
Secure Mail ユーザー ドメイン	55
バックグラウンドネットワークサービス	55
バックグラウンドサービスチケットの有効期限	55
バックグラウンドネットワークサービスゲートウェイ	55
連絡先のエクスポート	56

エクスポートする連絡先フィールド	56
すべてのSSL証明書を承認する	56
ロック画面の通知を制御する	56
セキュア接続の使用	56
既定のメール通知	56
既定の同期間隔	56
メールの検索制限	57
最大同期間隔	57
週番号を有効にする	57
Wi-Fi経由での添付ファイルのダウンロードを有効にする	57
オフラインドキュメントを許可	57
情報権限管理	58
メール分類	58
メール分類マーク	58
メール分類名前空間	58
メール分類バージョン	58
デフォルトのメール分類	58
下書きメールの自動保存を有効にする	58
iOSデータ保護を有効にする	59
プッシュ通知EWSホスト名	59
プッシュ通知	59
プッシュ通知の地域	59
セキュアメールの初回起動時にS/MIMEを有効にする	59
初回認証メカニズム	59
初回認証資格情報	60
週番号を有効にする	60
カレンダーのWebおよびオーディオオプション	60
S/MIME公開証明書ソース	60

LDAPサーバーアドレス	60
LDAPベースDN	60
LDAPに匿名でアクセス	60
許可されたメールドメイン	61
認証失敗時にユーザー名の移行を試行する	61
フィッシングメールアドレスを報告する	61
フィッシング報告メカニズム	61
Skype for Business会議ドメイン	61
カレンダーのエクスポート	61
Slack を有効にする	62
Slack ワークスペース名	62
発信者ID	62
分析	62
Google Analytics を有効にする	62
Google Analytics の詳細レベル	62
レポート	63
Citrix レポート	63
アップロードトークン	63
Wi-Fi 経由でのみレポートを送信	63
レポートファイルキャッシュの最大値	63
Office 365 の OAuth サポート	63
Office 365 にモダン認証を使用する	63
Office 365 認証メカニズム	64
信頼できる Exchange Online ホスト名	64
信頼されたAD FSホスト名	64
最新の認証用のカスタムユーザーエージェント	64
メールリダイレクト	64
メールリダイレクト	64

Slack連携	65
Slackを有効にする	65
Slackワークスペース名	65
Android向けモバイル生産性アプリのMDXポリシー	65
認証	65
アプリのパスコード	65
最大オフライン期間（時間）	66
代替 シトリックス ゲートウェイ	66
デバイスのセキュリティ	66
ジェイルブレイクまたはルート化されたデバイスをブロック	66
デバイスの暗号化を必須にする	66
デバイスロックを必須にする	67
ネットワーク要件	67
Wi-Fiを必須にする	67
許可されたWi-Fiネットワーク	67
その他のアクセス	67
アプリ更新猶予期間（時間）	67
必須アップグレードを無効にする	68
ロック時にアプリデータを消去	68
アクティブポーリング期間 (分)	68
暗号化	69
暗号化の種類	69
非準拠デバイスの動作	69
暗号化キー	69
プライベートファイルの暗号化	69
プライベートファイルの暗号化の除外	70
公開ファイルのアクセス制限	70
公開ファイルの暗号化	71

公開ファイルの暗号化除外	71
公開ファイルの移行	71
アプリの相互作用	72
セキュリティグループ	72
切り取りとコピー	72
貼り付け	72
ドキュメント交換 (Open In)	73
フィルタリングから除外されるURLドメイン	73
許可されたSecure Webドメイン	73
制限付きOpen-In例外リスト	73
受信ドキュメント交換 (Open In)	74
受信ドキュメント交換ホワイトリスト	74
接続セキュリティレベル	74
アプリの制限	74
カメラをブロック	75
ギャラリーをブロック	75
マイク録音をブロック	75
位置情報サービスをブロック	75
SMS作成をブロック	75
画面キャプチャをブロック	75
デバイスセンサーをブロック	76
NFCをブロック	76
アプリログをブロック	76
印刷をブロック	76
ShareFileを有効にする	76
アプリのネットワークアクセス	76
ネットワークアクセス	76
Micro VPNセッションが必要	77

除外リスト	77
localhost接続をブロック	77
証明書ラベル	78
アプリログ	78
デフォルトのログ出力	78
デフォルトのログレベル	78
最大ログファイル数	78
最大ログファイルサイズ	78
アプリログのリダイレクト	79
ログの暗号化	79
アプリのジオフェンス	79
中心点の経度	79
中心点の緯度	79
半径	79
分析	80
Google Analyticsの詳細	80
アプリ設定	80
セキュアメール Exchangeサーバー	80
Secure Mailユーザー ドメイン	80
バックグラウンドネットワークサービス	80
バックグラウンドサービスチケットの有効期限	81
バックグラウンドネットワークサービスゲートウェイ	81
連絡先のエクスポート	81
エクスポートする連絡先フィールド	81
すべてのSSL証明書を承認する	82
セキュア接続を使用する	82
情報権限管理	82
ロック画面通知を制御する	82

デフォルトの同期間隔	82
Wi-Fi経由での添付ファイルのダウンロードを有効にする	82
オフラインドキュメントを許可する	83
メール下書きの自動保存を有効にする	83
初回認証メカニズム	83
初回認証資格情報	83
週番号を有効にする	83
メール分類	83
メール分類マーキング	83
メール分類ネームスペース	84
メール分類バージョン	84
デフォルトのメール分類	84
メール検索制限	84
最大同期間隔	84
カレンダーのWebおよびオーディオオプション	85
S/MIME公開証明書のソース	85
LDAPサーバーアドレス	85
LDAPベースDN	85
LDAPに匿名でアクセス	85
許可されたメールアドレスドメイン	85
プッシュ通知	85
プッシュ通知EWSホスト名	86
プッシュ通知リージョン	86
認証失敗時にユーザー名移行を試行	86
フィッシングメールアドレスの報告	86
フィッシング報告メカニズム	86
Skype for Business会議ドメイン	86
カレンダーのエクスポート	87

Office 365のOAuthサポート	87
O365に最新の認証を使用	87
信頼されたExchange Onlineホスト名	87
信頼されたAD FSホスト名	88
最新の認証用のカスタムユーザーエージェント	88
Slack連携	88
Slackを有効にする	88
Slackワークスペース名	88
iOS向けモバイル生産性アプリのMDXポリシー	88
認証	89
デバイスパスコード	89
アプリパスコード	89
最大オフライン期間（時間）	89
代替シトリックス ゲートウェイ	89
デバイスセキュリティ	90
ジェイルブレイクまたはルート化されたデバイスをブロック	90
ネットワーク要件	90
Wi-Fiを必須にする	90
許可されたWi-Fiネットワーク	90
その他のアクセス	90
必須アップグレードを無効にする	90
アプリ更新猶予期間（時間）	90
ロック時にアプリデータを消去	91
アクティブポーリング期間（分）	91
暗号化	92
暗号化の種類	92
非準拠デバイスの動作	92
MDX暗号化を有効にする	92

データベース暗号化の除外	92
ファイル暗号化の除外	93
アプリの操作	93
切り取りとコピー	93
貼り付け	93
ドキュメント交換 (Open In)	93
制限付きOpen-In例外リスト	94
接続セキュリティレベル	94
受信ドキュメント交換 (Open In)	94
アプリのURLスキーム	94
アプリ連携 (送信URL)	96
URLフィルタリングから除外されるドメイン	96
許可されたURL	96
許可されたSecure Webドメイン	98
アプリの制限	99
カメラをブロック	99
写真ライブラリをブロック	99
マイク録音をブロック	99
音声入力をブロック	99
位置情報サービスをブロック	99
SMS作成をブロック	99
メール作成をブロック	99
iCloudをブロック	99
ルックアップをブロック	100
ファイルバックアップをブロック	100
AirPrintをブロック	100
AirDropをブロック	100
ファイル添付をブロック	100

FacebookおよびTwitter APIをブロック	100
画面コンテンツを隠す	101
サードパーティ製キーボードをブロックする (iOS 11以降のみ)	101
アプリログをブロックする	101
ShareFileを有効にする	101
ファイルから添付を有効にする	101
アプリのネットワークアクセス	101
ネットワークアクセス	101
Micro VPNセッションが必要	102
Micro VPNセッションの猶予期間 (分)	102
証明書ラベル	102
除外リスト	102
アプリログ	103
デフォルトのログ出力	103
デフォルトのログレベル	103
最大ログファイル数	103
ログファイルの最大サイズ	103
アプリのジオフェンス	103
中心点の経度	103
中心点の緯度	104
半径	104
Google Analyticsを有効にする	104
分析	104
Google Analytics の詳細レベル	104
レポート	104
Citrix レポート	104
アップロードトークン	105
Wi-Fi 経由でのみレポートを送信	105

レポートファイルキャッシュの最大値	105
アプリの操作	105
明示的なログオフ通知	105
アプリ設定	105
セキュアメール Exchange サーバー	105
Secure Mail ユーザー ドメイン	105
バックグラウンドネットワークサービス	106
バックグラウンドサービスチケットの有効期限	106
バックグラウンドネットワークサービスゲートウェイ	106
連絡先のエクスポート	106
エクスポートする連絡先フィールド	107
すべてのSSL証明書を承認する	107
ロック画面通知の制御	107
デフォルトのメール通知	107
デフォルトの同期間隔	107
メール検索制限	108
最大同期間隔	108
週番号を有効にする	108
Wi-Fi 経由での添付ファイルのダウンロードを有効にする	108
オフラインドキュメントを許可する	108
情報権限管理	108
メール分類	108
メール分類マーキング	109
メール分類名前空間	109
メール分類バージョン	109
デフォルトのメール分類	109
メール下書きの自動保存を有効にする	109
初回認証メカニズム	109

初回認証資格情報	110
ユーザー名の自動入力の有効化	110
iOSデータ保護を有効にする	110
プッシュ通知EWSホスト名	110
プッシュ通知	110
プッシュ通知リージョン	110
S/MIME公開証明書ソース	110
最初のSecure Mail起動時にS/MIMEを有効にする	111
カレンダーのWebおよびオーディオオプション	111
S/MIME公開証明書ソース	111
LDAPサーバーアドレス	111
LDAPベースDN	111
LDAPに匿名でアクセス	112
許可されたメールドメイン	112
認証失敗時のユーザー名移行を試行	112
フィッシングメールアドレスを報告	112
フィッシング報告メカニズム	112
Skype for Business会議ドメイン	113
カレンダーのエクスポート	113
発信者識別	114
Office 365のOAuthサポート	114
Office 365認証メカニズム	114
信頼できるExchange Onlineホスト名	114
信頼されたAD FSホスト名	114
メールリダイレクト	115
メールリダイレクト	115
Slack連携	115
Slackを有効にする	115

Slackワークスペース名	115
プラットフォーム別の機能	116
シトリックス セキュアハブ™	116
シトリックス セキュアメール	117
シトリックス セキュアウェブ™	129
機能フラグ管理	131
IPアドレス	131
システム要件	131
シトリックス セキュアハブ™	133
Secure Hubの管理	133
シトリックス PIN	133
証明書ピンニング	134
Secure Hub の証明書 + ワンタイムパスワード認証の構成	135
AndroidデバイスのADS接続のポート要件	138
Secure Hub の機能	140
Secure Mail の概要	143
シトリックス セキュアウェブ™	146
Secure Webの統合と配信	146
ユーザー接続の構成	147
Secure Webポリシー	148
許可またはブロックされたWebサイト	148
ポップアップをブロック	149
事前読み込みされたブックマーク	149
ホームページURL	150
ブラウザのユーザーインターフェイス	150
オプション	150
Web パスワードキャッシュを有効にする	150
プロキシサーバー	151

DNS サフィックス	151
Secure Web 用のイントラネットサイトの準備	151
イントラネットサイトのトラブルシューティング	152
ウェブアーカイブファイルを作成するには	153
Secure Webの機能	154
エンドポイント管理向け Citrix Content Collaboration™	157
Endpoint Management 向け Citrix Content Collaboration クライアントが Citrix Files モバイルクライアントと異なる点	158
ユーザーアクセス	158
SSO	158
マイクロVPN	159
2要素認証	159
フォルダーのアクセス許可	159
ドキュメントアクセス保護	159
Citrix Filesアカウントへのアクセス	160
デバイスポリシー	160
MDXポリシー	160
データ暗号化	160
可用性	161
Endpoint Managementクライアント向けCitrix Content Collaborationの統合と提供	161
SSOのためにEndpoint ManagementでCitrix Filesアカウント情報を構成するには	162
Endpoint ManagementにEndpoint Managementクライアント用のCitrix Content Collaborationを追加するには	163
前提条件	163
Citrix Content Collaboration for Endpoint Managementクライアントを検証するには	164
EOLおよび非推奨のアプリ	166
Office 365アプリとの安全な対話を許可する	168
iOSでのOffice 365の有効化	168

AndroidでのOffice 365の有効化	169
サポートされているファイル形式	169
業務用モバイルアプリのドキュメント履歴	170

モバイル生産性アプリのリリーススケジュール

Citrix® モバイル生産性アプリのリリースは2週間ごとに行われます。正確な日付は変更される可能性があります。このリリース周期を把握しておくことで、事前に計画を立てることができます。また、アプリの展開と更新をより簡単に管理できるようにしたいと考えています。

Secure MailおよびSecure Webの段階的リリースプロセスについて

Secure MailおよびSecure Webの新しいバージョンが利用可能になると、リリースは以下の段階的なアプローチで展開されます。

- iOSおよびAndroidユーザー向けに、Secure MailおよびSecure Webのアップデートは、App StoreおよびGoogle Playストアで、1週間（7日間）にわたって利用可能なユーザーの割合を増やしながら提供されます。
- iOS版Secure MailおよびSecure Webの新規ダウンロードでは、この1週間以内に新しいバージョンが提供されます。Android版Secure MailおよびSecure Webの新規ダウンロードでは、新しいリリースの展開が全ユーザーの100%に達するまで、その週は以前のバージョンが実行されます。
- ユーザー向けに、一部の機能は段階的にリリースされます。

機能フラグ管理の前提条件

本番環境でSecure HubまたはSecure Mailに問題が発生した場合、アプリコード内の影響を受ける機能を無効にすることができます。そのためには、機能フラグとLaunchDarklyというサードパーティサービスを使用します。ファイアウォールまたはプロキシがアウトバウンドトラフィックをブロックしている場合を除き、LaunchDarklyへのトラフィックを有効にするための設定は不要です。その場合は、ポリシー要件に応じて、特定のURLまたはIPアドレスを介してLaunchDarklyへのトラフィックを有効にします。モバイル生産性アプリ10.6.15以降のMDXにおける、トンネリングからのドメイン除外のサポートに関する詳細は、[MDX Toolkitドキュメント](#)を参照してください。機能フラグとLaunchDarklyに関するFAQについては、この[サポート知識センターの記事](#)を参照してください。

注： 段階的に廃止されるCitrix Endpoint Management機能の事前通知については、[廃止予定](#)を参照してください。

モバイル生産性アプリのサポート

自動更新が有効になっているユーザーは、アプリストアから最新バージョンを受け取ります。モバイル生産性アプリの最新バージョンは次のとおりです。

- 23.10.0 (Secure Web アンドロイド版)
- 23.9.0 (iOS版Secure MailおよびSecure Web)
- 23.8.2 (Secure Mail アンドロイド版)

Citrix®は、モバイル生産性アプリの過去2バージョンからのアップグレードをサポートしています。モバイル生産性アプリの過去2バージョンは次のとおりです。

- 23.8.1 (Secure Mail アンドロイド版)
- 23.8.0 (Secure Web アンドロイド版)
- 23.7.0 (Secure Mail アンドロイド版およびSecure Mail アイオーエス版)
- 23.5.0 (Secure Mail アイオーエス版およびSecure Web アンドロイド版)
- 23.2.0 (Secure Web アイオーエス版)
- 22.9.1 (Secure Web アイオーエス版)

重要:

MDX暗号化は、September 1, 2020にサポート終了（EOL）となりました。レガシーデバイス管理（DA）に登録されているデバイスの場合：

- MDX暗号化を使用しない場合、アクションは不要です。
- MDX暗号化を使用している場合は、AndroidデバイスをAndroid Enterpriseに移行してください。Android 10を実行しているデバイスは、Android Enterpriseを使用して登録または再登録する必要があります。これには、MAM専用モードのAndroidデバイスも含まれます。詳細については、[デバイス管理をAndroid Enterpriseに移行する](#)を参照してください。

サポートされているオペレーティングシステム

モバイル生産性向上アプリは、以下のオペレーティングシステムをサポートしています。

製品名	オペレーティングシステム	最小展開バージョン	利用可能な最新バージョン
セキュアハブ	アンドロイド	7.x	14.x
	iOS	12.x	17.x
セキュアメール	アンドロイド	8.x	14.x
	iOS	13.x	17.x
セキュアウェブ	アンドロイド	8.x	14.x
	iOS	13.x	17.x

モバイル生産性アプリの最新バージョンは、Citrix Endpoint Managementの最新バージョンおよびその2つ前のバージョンと互換性があります。Citrix Endpoint Managementでサポートされているオペレーティングシステムの詳細については、[サポートされているデバイスオペレーティングシステム](#)を参照してください。

モバイル生産性アプリの最新バージョンには、Secure Hubの最新バージョンが必要です。Secure Hubを常に最新の状態に保つようにしてください。

注：

Citrixは常に、AndroidおよびiOSオペレーティングシステムの最新バージョンと、その2つ前のバージョン (N、N-1、N-2) のみをサポートします。

その他の考慮事項と制限

段階的に廃止されるCitrix Endpoint Managementの機能の事前通知については、[廃止予定](#)を参照してください。

セキュアメール

- Endpoint Managementは現在、Secure Ticket Authority (STA) とSecure Mailに関する問題のため、NetScaler 12.0.41.16をサポートしていません。この問題はNetScaler 12.0ビルド41.22で修正されています。
- Secure MailでのExchange 2007およびLotus Notes 8.5.3のサポートは、September 30, 2017にEnd of Life (EOL) に達しました。

- Citrix Filesの添付ファイルを送信する際の最高のパフォーマンスを得るには、Citrix Filesの最新バージョンが推奨されます。Citrix FilesはWindowsではサポートされていません。
- IBM Notes環境では、IBM Domino Travelerサーバーバージョン9.0を構成する必要があります。詳細については、「Integrating Exchange Server or IBM Notes Traveler Server」を参照してください。

注：

- Citrix Files for XenMobileは、July 1, 2023にEOLに達しました。詳細については、[EOLおよび廃止されたアプリ](#)を参照してください。

セキュアウェブ

デバイスにAndroid WebViewの最新バージョンをインストールします。ユーザーはGoogle PlayストアからAndroid WebViewをダウンロードできます。

QuickEdit

QuickEditは引き続きモバイル生産性アプリとして利用可能です。以前通知されたように、End of Life (EOL) ステータスはSeptember 1, 2018には適用されません。

シトリックス コンテンツ コラボレーション™ エンドポイント管理向け

ユーザーはバージョン6.5以降、パブリックアプリストアからCitrix Content Collaboration for Endpoint Managementにアクセスします。

ShareConnect

ShareConnectはJune 30, 2020にEnd of Life (EOL) に達しました。詳細については、[EOLおよび非推奨アプリ](#)を参照してください。

シトリックス セキュア ノーツ およびシトリックス セキュア タスク

Citrix Secure NotesおよびCitrix Secure Tasksは、December 31, 2018にEnd of Life (EOL) ステータスに達しました。詳細については、[EOLおよび非推奨アプリ](#)を参照してください。

管理者のタスクと考慮事項

この記事では、モバイル生産性アプリの管理者に関連するタスクと考慮事項について説明します。

機能フラグの管理

モバイル生産性アプリで問題が発生した場合、アプリコード内の影響を受ける機能を無効にできます。iOSおよびAndroid版のSecure Hub、Secure Mail、Secure Webの機能を無効にできます。そのためには、機能フラグとLaunchDarklyというサードパーティサービスを使用します。ファイアウォールまたはプロキシがアウトバウンドトラフィックをブロックしている場合を除き、LaunchDarklyへのトラフィックを有効にするための設定は不要です。その場合は、ポリシー要件に応じて、特定のURLまたはIPアドレスを介してLaunchDarklyへのトラフィックを有効にします。トンネリングからのドメイン除外に関するサポートの詳細については、[MAM SDKドキュメント](#)を参照してください。

LaunchDarklyへのトラフィックと通信は、以下の方法で有効にできます。

以下のURLへのトラフィックを有効にする

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `firehose.launchdarkly.com`

ドメインによる許可リストの作成

以前は、社内ポリシーでIPアドレスのみをリストに含める必要がある場合に、使用するIPアドレスのリストを提供していました。現在、Citrix®がインフラストラクチャの改善を行ったため、July 16, 2018よりパブリックIPアドレスの段階的な廃止を進めています。可能な場合は、ドメインによる許可リストを作成することをお勧めします。

許可リストにIPアドレスを記載する

許可リストにIPアドレスを記載する必要がある場合は、現在のすべてのIPアドレス範囲のリストについて、この[LaunchDarklyパブリックIPリスト](#)を参照してください。このリストを使用して、インフラストラクチャの更新に合わせてファイアウォール構成が自動的に更新されるようにすることができます。インフラストラクチャ変更のステータスに関する詳細については、[LaunchDarkly ステータスページ](#)を参照してください。

注:

公開アプリストアアプリは、初めて展開する際に新規インストールが必要です。現在のエンタープライズラップ版アプリから公開ストア版へアップグレードすることはできません。

公開アプリストア配信では、MDX Toolkitを使用してCitrix開発のアプリに署名したりラップしたりすることはありません。MDX Toolkitを使用して、サードパーティ製アプリやエンタープライズアプリをラップできます。

LaunchDarklyのシステム要件

- エンドポイントマネジメント 10.7 以降。
- Citrix ADCでスプリットトンネリングが**OFF**に設定されている場合、アプリが以下のサービスと通信できることを確認してください。
 - LaunchDarklyサービス
 - APNsリスナーサービス

サポートされているアプリストア

モバイル生産性向上アプリは、Apple App StoreおよびGoogle Playで利用できます。

中国ではGoogle Playが利用できないため、Android版Secure Hubは以下のアプリストアで利用できます。

- [<https://shouji.baidu.com>](https://shouji.baidu.com)
- [<http://apk.hiapk.com>](http://apk.hiapk.com)
- [<https://apk.91.com>](https://apk.91.com)

公開アプリストア配信の有効化

1. iOSとAndroidの両方について、公開ストア版の.mdxファイルを[Endpoint Managementダウンロードページ](#)からダウンロードしてください。
2. .mdxファイルをEndpoint Managementコンソールにアップロードします。モバイル生産性アプリのパブリックストアバージョンは、引き続きMDXアプリケーションとしてアップロードされます。アプリをサーバー上のパブリックストアアプリとしてアップロードしないでください。手順については、「[アプリの追加](#)」を参照してください。
3. セキュリティポリシーに基づいて、ポリシーをデフォルトから変更します（オプション）。
4. アプリを必須アプリとしてプッシュします（オプション）。この手順には、モバイルデバイス管理が有効になっている環境が必要です。
5. App Store、Google Play、またはEndpoint Managementアプリストアからデバイスにアプリをインストールします。
 - Androidでは、ユーザーはPlayストアに誘導されてアプリをインストールします。iOSでは、MDMが展開されている場合、ユーザーがアプリストアに移動することなくアプリがインストールされます。
 - App StoreまたはPlayストアからアプリがインストールされると、次のアクションが発生します。対応する.mdxファイルがサーバーにアップロードされている限り、アプリは管理対象アプリに移行します。管理対象アプリに移行する際、アプリはCitrix PINの入力を求めます。ユーザーがCitrix PINを入力すると、Secure Mailにアカウント構成画面が表示されます。
6. アプリは、Secure Hubに登録されており、対応する.mdxファイルがサーバー上にある場合にのみアクセス可能です。いずれかの条件が満たされない場合、ユーザーはアプリをインストールできますが、アプリの使用はブロックされます。

現在、パブリックアプリストアにあるCitrix Ready Marketplace™のアプリを使用している場合、展開プロセスにはすでに慣れているでしょう。モバイル生産性アプリは、多くのISVが現在使用しているのと同じアプローチを採用しています。アプリをパブリックストア対応にするには、MDX SDKをアプリ内に埋め込みます。

注：

iOSとAndroidの両方に対応するCitrix Filesアプリのパブリックストアバージョンは、現在ユニバーサルです。Citrix Filesアプリは、電話とタブレットで同じです。

Appleプッシュ通知

プッシュ通知の構成について詳しくは、「[Secure Mailのプッシュ通知の構成](#)」を参照してください。

パブリックアプリストアに関するFAQ

- パブリックストアアプリの複数のコピーを異なるユーザーグループに展開できますか？たとえば、異なるユーザーグループに異なるポリシーを展開したい場合です。

各ユーザーグループに異なる.mdxファイルをアップロードします。ただし、この場合、単一のユーザーが複数のグループに属することはできません。ユーザーが複数のグループに属している場合、同じアプリの複数のコピーがそのユーザーに割り当てられます。アプリIDは変更できないため、パブリックストアアプリの複数のコピーを同じデバイスに展開することはできません。

- 公開ストアアプリを必須アプリとしてプッシュできますか？

はい。アプリをデバイスにプッシュするにはMDMが必要です。MAMのみの展開ではサポートされていません。

- ユーザーエージェントに基づいたトラフィックポリシーやExchange Serverルールを更新する必要がありますか？

プラットフォームごとのユーザーエージェントベースのポリシーおよびルールの文字列は以下のとおりです。

重要:

Secure NotesおよびSecure Tasksは、December 31, 2018にサポート終了（EOL）ステータスに達しました。詳細については、[EOLおよび非推奨アプリ](#)を参照してください。

アンドロイド

アプリ	サーバー	ユーザーエージェント文字列
シトリックス セキュアメール TM	エクスチェンジ	WorxMail
	ロータス ノーツ トラベラー	アップル - アイフォン ワークスメール

アプリ	サーバー	ユーザーエージェント文字列
Citrix セキュアウェブ™		WorxMail
シトリックス セキュア タスク	エクスチェンジ	WorxMail
シトリックス セキュア ノーツ	エクスチェンジ	WorxMail
	シトリックス ファイル	セキュア ノーツ

iOS

アプリ	サーバー	ユーザーエージェント文字列
シトリックス セキュア メール	エクスチェンジ	WorxMail
	ロータス ノーツ トラベラー	アップル - iPhone ワークス メール
シトリックス セキュアウェブ		com.citrix.browser
シトリックス セキュアタスク	エクスチェンジ	WorxTasks
シトリックス セキュアノート	エクスチェンジ	WorxNotes
	シトリックス ファイル	セキュアノート

- アプリのアップグレードを防ぐことはできますか？

いいえ。パブリックアプリストアに更新が投稿されると、自動更新が有効になっているすべてのユーザーが更新を受け取ります。

- アプリのアップグレードを強制できますか？

はい、アップグレードはアップグレード猶予期間ポリシーによって強制されます。このポリシーは、アプリの更新バージョンに対応する新しい.mdxファイルがEndpoint Managementにアップロードされたときに設定されます。

- 更新のタイムラインを制御できない場合、更新がユーザーに届く前にアプリをテストするにはどうすればよいですか？

Secure Hubの場合と同様に、EAR期間中、iOSではTestFlightで、AndroidではGoogle Playベータプログラムを通じてアプリをテストできます。この期間中にアプリの更新をテストできます。

- 自動更新がユーザーデバイスに届く前に、新しい.mdxファイルを更新しなかった場合、どうなりますか？

更新されたアプリは、古い.mdxファイルとの互換性を維持します。新しいポリシーに依存する新機能は有効になりません。

- Secure Hubがインストールされている場合、アプリは管理対象に移行しますか、それともアプリを登録する必要がありますか？

パブリックストアアプリを管理対象アプリ（MDXで保護）としてアクティブ化し、使用可能にするには、ユーザーがSecure Hubに登録されている必要があります。Secure Hubがインストールされていても登録されていない場合、ユーザーはパブリックストアアプリを使用できません。

- パブリックストアアプリにApple Enterprise開発者アカウントは必要ですか？

いいえ。Citrixがモバイル生産性向上アプリの証明書とプロビジョニングプロファイルを維持しているため、アプリをユーザーに展開するためにApple Enterprise開発者アカウントは必要ありません。

- エンタープライズ配布の終了は、展開したすべてのラップされたアプリケーションに適用されますか？

いいえ、これはモバイル生産性向上アプリ（Secure Mail、Secure Web、Endpoint Management用Citrix Content Collaboration™、QuickEdit、ShareConnect）にのみ適用されます。社内で開発された、またはサードパーティによって開発された展開済みのエンタープライズラップアプリは、引き続きエンタープライズラッピングを使用できます。MDX Toolkitは、アプリ開発者向けのエンタープライズラッピングを引き続きサポートします。

- Google Playからアプリをインストールすると、エラーコード505のAndroidエラーが発生します。

注:

Android 5.x のサポートは、December 31, 2018 に終了しました。

これは、Google Play および Android 5.x バージョンで発生する既知の問題です。このエラーが発生した場合は、以下の手順に従って、アプリのインストールを妨げるデバイス上の古いデータをクリアできます。

1. デバイスを再起動します。
2. デバイス設定から Google Play のキャッシュとデータをクリアします。
3. 最終手段として、デバイスの Google アカウントを削除してから再度追加します。

詳細については、次のキーワード「Fix Google Play Store Error 505 in Android: Unknown Error Code」を使用してこの[サイト](#)を検索してください。

- Google Play のアプリは製品版としてリリースされており、新しいベータ版リリースは利用できませんが、Google Play のアプリタイトルの後に「Beta」と表示されるのはなぜですか？

早期アクセスリリース (EAR) プログラムに参加している場合、アプリタイトルの横に常に「Beta」と表示されます。この名前は、特定のアプリに対するユーザーのアクセスレベルを通知するものです。「Beta」という名前は、ユーザーが利用可能なアプリの最新バージョンを受け取れることを示します。最新バージョンは、製品版トラックまたはベータ版トラックに公開された最新バージョンである場合があります。

- アプリをインストールして開いた後、.mdx ファイルが Endpoint Management コンソールにあるにもかかわらず、「App Not Authorized」というメッセージが表示されます。

この問題は、ユーザーが App Store または Google Play から直接アプリをインストールした場合、および Secure Hub が更新されていない場合に発生する可能性があります。Secure Hub は、非アクティブタイマーが期限切れになったときに更新する必要があります。ポリシーは、ユーザーが Secure Hub を開いて再認証したときに更新されます。アプリは、ユーザーが次回アプリを開いたときに承認されます。

- アプリを使用するためにアクセスコードが必要ですか？ App Store または Play ストアからアプリをインストールすると、アクセスコードの入力を求める画面が表示されます。

アクセスコードを要求する画面が表示される場合、Secure Hub を介して Endpoint Management に登録されていません。Secure Hub に登録し、アプリの .mdx ファイルがサーバーに展開されていることを確認してください。また、アプリが使用可能であることを確認してください。アクセスコードは Citrix 社内でのみ使用が制限されています。アプリをアクティブ化するには、Endpoint Management の展開が必要です。

- VPP または DEP を介して iOS パブリックストアアプリを展開できますか？

Endpoint Management は、MDX が有効になっていないパブリックストアアプリの VPP 配布用に最適化されています。Endpoint Management パブリックストアアプリを VPP で配布することはできますが、Endpoint Management と Secure Hub ストアにさらなる機能強化を加えて制限に対処するまでは、展開は最適ではありません。VPP を介して Endpoint Management パブリックストアアプリを展開する際の既知の問題のリストと、潜在的な回避策については、[Citrix ナレッジセンター](#)のこの記事を参照してください。

モバイル生産性向上アプリの MDX ポリシー

MDXポリシーを使用すると、Endpoint Managementが適用する設定を構成できます。これらのポリシーは、認証、デバイスセキュリティ、ネットワーク要件とアクセス、暗号化、アプリの相互作用、アプリの制限などを対象とします。多くのMDXポリシーは、すべてのモバイル生産性向上アプリに適用されます。一部のポリシーはアプリ固有です。

ポリシーファイルは、モバイル生産性向上アプリのパブリックストアバージョン向けに.mdxファイルとして提供されます。アプリを追加する際に、Endpoint Managementコンソールでポリシーを構成することもできます。

MDXポリシーの詳細については、このセクションの以下の記事を参照してください。

- [モバイル生産性向上アプリのMDXポリシーの概要](#)
- [Android向けモバイル生産性向上アプリのMDXポリシー](#)
- [iOS向けモバイル生産性向上アプリのMDXポリシー](#)

以下のセクションでは、ユーザー接続に関連するMDXポリシーについて説明します。

Android版Secure Mailのデュアルモード

モバイルアプリケーション管理（MAM）SDKは、iOSおよびAndroidプラットフォームでカバーされていないMDX機能の領域を置き換えるために利用可能です。MDXラッピングテクノロジーは、2021年9月にサポート終了（EOL）を迎える予定です。エンタープライズアプリケーションの管理を継続するには、MAM SDKを組み込む必要があります。

バージョン20.8.0以降、Androidアプリは、前述のMDX EOL戦略に備えるため、MDXおよびMAM SDKとともにリリースされます。MDXデュアルモードは、現在のMDX Toolkitから新しいMAM SDKへの移行方法を提供することを目的としています。デュアルモードを使用すると、次のいずれかを行うことができます。

- MDX Toolkitを使用してアプリの管理を継続する（Endpoint Managementコンソールでは現在「Legacy MDX」と表示されています）
- 新しいMAM SDKを組み込んだアプリを管理する。

注：

MAM SDKを使用する場合、アプリをラップする必要はありません。

MAM SDKに切り替えた後で、追加の手順は必要ありません。

MAM SDK の詳細については、以下の記事を参照してください。

- [MAM SDK の概要](#)
- [MAM SDK の最新リリース](#)
- Citrix Developer の [デバイス管理](#) セクション
- [Citrix のブログ投稿](#)

前提条件

デュアルモード機能を正常に展開するには、以下を確認してください。

- Citrix Endpoint Management をバージョン 10.12 RP2 以降、または 10.11 RP5 以降に更新します。
- モバイルアプリをバージョン 20.8.0 以降に更新します。
- ポリシーファイルをバージョン 20.8.0 以降に更新します。
- 組織でサードパーティ製アプリを使用している場合は、Citrix モバイル生産性向上アプリの MAM SDK オプションに切り替える前に、MAM SDK をサードパーティ製アプリに組み込むようにしてください。管理対象アプリはすべて、一度に MAM SDK に移行する必要があります。

注:

MAM SDK は、すべてのクラウドベースのお客様でサポートされています。

制限事項

- MAM SDK は、Citrix Endpoint Management™ 展開で Android Enterprise プラットフォームの下で公開されたアプリのみをサポートします。新しく公開されたアプリの場合、デフォルトの暗号化はプラットフォームベースの暗号化です。
- MAM SDK はプラットフォームベースの暗号化のみをサポートし、MDX 暗号化はサポートしません。
- Citrix Endpoint Management を更新せず、ポリシーファイルがモバイルアプリのバージョン 20.8.0 以降で実行されている場合、Secure Mail 用のネットワークポリシーの重複エントリが作成されます。

Citrix Endpoint Management で Secure Mail を構成すると、デュアルモード機能により、MDX Toolkit (現在は Legacy MDX) を使用してアプリの管理を継続するか、新しい MAM SDK に切り替えてアプリを管理することができます。Citrix は MAM SDK への切り替えを推奨しています。MAM

SDK はよりモジュール性が高く、組織が使用する MDX 機能のサブセットのみを使用できるようにすることを目的としているためです。

MDX または MAM SDK ポリシーコンテナのポリシー設定には、以下のオプションがあります。

- MAM SDK
- レガシー MDX

The screenshot shows the Citrix Cloud Endpoint Management console. The left sidebar lists navigation options: Device Policies, Apps, Media, Actions, Content Collaboration, Enrollment Profiles, and Delivery Groups. The 'Apps' section is expanded, showing a list of applications under the 'MDX' category. The 'iOS' application is selected. The main panel displays the configuration for the 'Secure Mail' application. Fields include File name, App Description, App version, Minimum OS version, Maximum OS version, and Excluded devices. There are also toggle switches for 'Remove app if MDM profile is removed', 'Prevent app data backup', 'Force app to be managed', and 'App deployed via Volume purchase'. At the bottom, the 'MDX or MAM SDK policy container' is set to 'Legacy MDX'.

MDX または MAM SDK ポリシーコンテナポリシーでは、オプションをLegacy MDXからMAM SDKに変更することのみ可能です。MAM SDKからLegacy MDXへの切り替えは許可されておらず、アプリを再公開する必要があります。デフォルト値はLegacy MDXです。同じデバイスで実行されている Secure Mail と Secure Web の両方に同じポリシーモードを設定してください。同じデバイスで2つの異なるモードを実行することはできません。

内部ネットワークへのユーザー接続

内部ネットワークにトンネル接続する接続は、フルVPNトンネルまたはクライアントレスVPNのバリエーションである「トンネル化 - Web SSO」を使用できます。優先VPNモードポリシーがその動作を制御します。デフォルトでは、接続は「トンネル化 - Web SSO」を使用します。これはSSOを必要とする接続に推奨されます。フルVPNトンネル設定は、クライアント証明書または内部ネットワーク内のリソースへのエンドツーエンドSSLを使用する接続に推奨されます。この設定はTCP上のあらゆるプロトコルを処理し、WindowsおよびMacコンピューター、iOSおよびAndroidデバイスで使用できます。

VPNモード切り替え許可ポリシーは、必要に応じてフルVPNトンネルモードとトンネル化 - Web SSOモード間の自動切り替えを許可します。デフォルトでは、このポリシーはオフです。このポリシーがオンの場合、優先VPNモードで処理できない認証要求が原因で失敗したネットワーク要求は、代替モードで再試行されます。たとえば、クライアント証明書のサーバーチャレンジはフルVPNトンネルモードで対応できますが、トンネル化 - Web SSOモードでは対応できません。同様に、HTTP認証チャレンジは、トンネル化 - Web SSOモードを使用する場合、SSOで処理される可能性が高くなります。

ネットワークアクセス制限

ネットワークアクセスポリシーは、ネットワークアクセスに制限が課されるかどうかを指定します。デフォルトでは、Secure Mail のアクセスは無制限であり、ネットワークアクセスに制限はありません。アプリは、デバイスが接続されているネットワークに無制限にアクセスできます。デフォルトでは、Secure Web のアクセスは内部ネットワークにトンネル接続されます。これは、すべてのネットワークアクセスにアプリケーションごとの VPN トンネルが内部ネットワークに戻って使用され、Citrix ADC のスプリットトンネル設定が使用されることを意味します。また、ブロックされたアクセスを指定して、アプリがデバイスにネットワーク接続がないかのように動作させることもできます。

AirPrint、iCloud、Facebook および Twitter API などの機能を許可したい場合は、ネットワークアクセスポリシーをブロックしないでください。

ネットワークアクセスポリシーは、バックグラウンドネットワークサービスポリシーとも連携します。詳細については、「[Exchange Server または IBM Notes Traveler Server の統合](#)」を参照してください。

Endpoint Managementクライアントプロパティ

クライアントプロパティには、ユーザーデバイス上のSecure Hubに直接提供される情報が含まれています。クライアントプロパティは、Endpoint Managementコンソールの >> にあります。

クライアントプロパティは、次のような設定を構成するために使用されます。

ユーザーパスワードのキャッシュ

ユーザーパスワードのキャッシュにより、ユーザーのActive Directoryパスワードをモバイルデバイスにローカルでキャッシュできます。ユーザーパスワードのキャッシュを有効にすると、ユーザーはCitrix PINまたはパスコードを設定するように求められます。

非アクティブタイマー

非アクティブタイマーは、ユーザーがデバイスを非アクティブなままにしておき、Citrix PINまたはパスコードの入力を求められることなくアプリにアクセスできる時間を分単位で定義します。

MDXアプリでこの設定を有効にするには、アプリパスコードポリシーを に設定する必要があります。アプリパスコードポリシーが の場合、ユーザーは完全な認証を実行するためにSecure Hubにリダイレクトされます。この設定を変更すると、次回ユーザーが認証を求められたときに値が有効になります。

Citrix PIN認証

Citrix PINは、ユーザー認証エクスペリエンスを簡素化します。PINは、クライアント証明書を保護したり、Active Directory資格情報をデバイスにローカルで保存したりするために使用されます。PIN設定を構成すると、ユーザーのサインオンエクスペリエンスは次のようになります。

1. ユーザーがSecure Hubを初めて起動すると、PINの入力を求めるプロンプトが表示され、Active Directory資格情報がキャッシュされます。
2. ユーザーが次にSecure Mailなどのモバイル生産性アプリを起動すると、PINを入力してサインオンします。

クライアントプロパティを使用してPIN認証を有効にし、PINの種類を指定し、PINの強度、長さ、および変更要件を指定します。

指紋認証またはTouch ID認証

iOSデバイスの指紋認証（Touch ID認証とも呼ばれる）は、Citrix PINの代替手段です。この機能は、Secure Hubを除くラップされたアプリが、非アクティブタイマーの期限切れ時など、オフライン認証を必要とする場合に役立ちます。この機能は、次の認証シナリオで有効にできます。

- Citrix PIN + クライアント証明書構成
- Citrix PIN + キャッシュされたADパスワード構成
- Citrix PIN + クライアント証明書構成およびキャッシュされたADパスワード構成
- Citrix PINが無効

指紋認証が失敗した場合、またはユーザーが指紋認証プロンプトをキャンセルした場合、ラップされたアプリはCitrix PINまたはADパスワード認証にフォールバックします。

指紋認証の要件

- 指紋認証をサポートし、少なくとも1つの指紋が構成されているiOSデバイス（最小バージョン8.1）。

- ユーザーエントロピーはオフである必要があります。

指紋認証を構成するには

重要:

ユーザーエントロピーがオンの場合、Enable Touch ID Authenticationプロパティは無視されます。ユーザーエントロピーは、Encrypt secrets using the Passcodeキーを介して有効になります。

1. Endpoint Managementコンソールで、**Settings > Client > Client Properties**に移動します。
2. **Add**をクリックします。

新しいクライアントプロパティの追加画面の画像(/en-us/mobile-productivity-apps/media/add-client-property-endpointmanagement.png)

3. キー**ENABLE_TOUCH_ID_AUTH**を追加し、その**Value**を**True**に設定し、次にポリシー名を**Enable Fingerprint Authentication**に設定します。

指紋認証を構成した後、ユーザーはデバイスを再登録する必要はありません。

パスコードキーを使用したシークレットの暗号化とクライアントプロパティ全般に関する詳細については、Endpoint Managementのに関する記事(/ja-jp/citrix-endpoint-management/advanced-concepts/deployment/client-properties.html)を参照してください。

Google アナリティクス

Citrix Secure Mailは、製品品質を向上させるために、アプリの統計情報と利用状況分析データを収集するためにGoogle Analyticsを使用しています。Citrixは、その他の個人ユーザー情報を収集または保存しません。

Google Analyticsを無効にする

管理者は、カスタムクライアントプロパティ**DISABLE_GA**を構成することで、Google Analyticsを無効にできます。Google Analyticsを無効にするには、次の手順を実行します。

1. Citrix Endpoint Managementコンソールにサインインし、**Settings > Client Properties > Add New Client Property**の順に移動します。
2. **Key**フィールドに値**DISABLE_GA**を追加します。
3. クライアントプロパティの値を**true**に設定します。

注：

Citrix Endpoint Managementコンソールで値**DISABLE_GA**を構成しない場合、Google Analyticsデータはアクティブになります。

モバイル生産性アプリのMDXポリシーの概要

この記事では、iOSおよびAndroid向けCitrixモバイル生産性アプリのMDXアプリポリシーと、そのデフォルト値について説明します。ポリシー設定は、Citrix Endpoint Managementコンソールで変更します。詳細については、「[アプリの追加](#)」を参照してください。

注：

Secure Hubは、特定のアクション中にポリシーを更新します。詳細については、「[Secure Hubの管理](#)」を参照してください。

認証

デバイスのパスコード

- iOS：はい
- Android：いいえ
- デフォルト設定：オフ

注：

このポリシーは、Citrix®がサポートしなくなったiOS 9デバイスにのみ適用されています。

アプリのパスコード

- iOS：はい
- Android：はい
- デフォルト設定：オン

オンラインセッションの猶予期間 (分)

- iOS: はい

- Android: いいえ
- デフォルト設定: 0

最大オフライン期間

- iOS: はい
- Android: はい
- デフォルト設定: 168時間 (7日間)

代替シトリックス ゲートウェイ

注:

Endpoint Managementコンソールでのこのポリシー名は、Alternate NetScaler® Gatewayです。

- iOS: はい
- Android: はい
- デフォルト設定: 空

デバイスセキュリティ

ジェイルブレイクまたはルート化されたデバイスをブロックする

- iOS: はい
- Android: はい
- デフォルト設定: オン

デバイスロックを必須

- iOS: いいえ
- Android: はい
- デフォルト設定: オフ

注:

Android Mデバイスでは、デバイスのPINまたはパスコード、およびデバイスのパターン画面ロックオプションは同じ効果があります。これらのオプションのいずれかを使用すると、デバイスにPIN、パスコード、またはパターン画面ロックが設定されていない場合、アプリはロックされます。

ネットワーク要件

Wi-Fiを必須

- iOS: はい
- Android: はい
- デフォルト設定: オフ

許可されたWi-Fiネットワーク

- iOS: はい
- Android: はい
- デフォルト設定: 空

その他のアクセス

アプリ更新猶予期間 (時間)

- iOS: はい
- Android: はい
- デフォルト設定: 168時間 (7日間)

注:

Citrixでは、ゼロ (0) 以外の値を使用することをお勧めします。ゼロ値にすると、ユーザーは警告なしに、更新をダウンロードしてインストールするまで実行中のアプリを使用できなくなります。この設定により、ユーザーがアプリを強制終了させられ、作業内容が失われる可能性がある状況につながる場合があります。

必須アップグレードの無効化

- iOS: はい
- Android: はい
- デフォルト設定: オン

ロック時にアプリデータを消去

- iOS: はい
- Android: はい
- デフォルト設定: オフ

アクティブポーリング期間 (分)

- iOS: はい
- Android: はい
- デフォルト設定: 60分 (1時間)

注:

高リスクのアプリの場合のみ、この値をデフォルトよりも低く設定してください。そうしないと、パフォーマンスに影響が出る可能性があります。

暗号化

暗号化の種類

- iOS: はい
- Android: はい
- デフォルト設定: MDX暗号化

注意:

新しく追加されたアプリの場合、**Platform encryption with compliance enforcement**から**MDX encryption**に変更すると、アプリを削除して再インストールする必要があります。新しく追加されたアプリのデフォルト設定は**Platform encryption with compliance enforcement**です。

非準拠デバイスの動作

- iOS: はい
- Android: はい
- デフォルト設定: 警告後にアプリを許可

MDX暗号化を有効にする

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

注意:

アプリを展開した後にこのポリシーを変更した場合、ユーザーはアプリを再インストールする必要があります。

暗号化キー

- iOS: いいえ
- Android: はい
- デフォルト設定: オフラインアクセス許可のみが利用可能なオプションです。

プライベートファイルの暗号化

- iOS: いいえ
- Android: はい
- デフォルト設定: SecurityGroup

プライベートファイルの暗号化の除外

- iOS: いいえ
- Android: はい
- デフォルト設定: 空

パブリックファイルのアクセス制限

- iOS: いいえ
- Android: はい

- デフォルト設定: 空

注:

パブリックファイルの暗号化ポリシーを有効にすると、このポリシーが適用されます（無効オプションからSecurityGroupまたはアプリケーションオプションに変更されます）。このポリシーは、既存の暗号化されていないパブリックファイルにのみ適用され、ファイルを暗号化するタイミングを指定します。

公開ファイルの暗号化

- iOS: いいえ
- Android: はい
- デフォルト設定: SecurityGroup

公開ファイルの暗号化除外

- iOS: いいえ
- Android: はい
- デフォルト設定: 空

公開ファイルの移行

- iOS: いいえ
- Android: はい
- デフォルト設定: 書き込み (RO/RW)

注:

既存の公開ファイルを暗号化すると、同じ暗号化キーを持たない他のアプリからそのファイルにアクセスできなくなります。

暗号化を有効にする

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

注:

既存のアプリに対してこのポリシーを変更する場合、ユーザーはポリシーの変更を適用するためにアプリを削除して再インストールする必要があります。

データベース暗号化の除外

- iOS: はい
- Android: いいえ
- デフォルト設定: 空

ファイル暗号化の除外

- iOS: はい
- Android: いいえ
- デフォルト設定: 空

アプリのインタラクション

セキュリティグループ

- iOS: いいえ
- Android: はい
- デフォルト設定: 空

注:

既存のアプリに対してこのポリシーを変更した場合、ポリシーの変更を適用するには、ユーザーがアプリを削除して再インストールする必要があります。

切り取りとコピー

- iOS: はい
- Android: はい
- デフォルト設定: 制限付き

貼り付け

- iOS: はい

- Android: はい
- デフォルト設定: 無制限

ドキュメント交換 (Open in)

- iOS: はい
- Android: はい
- デフォルト設定: 制限付き

フィルタリングから除外されるURLドメイン

- iOS: いいえ
- Android: はい
- デフォルト設定: 空

許可されたセキュアWebドメイン

- iOS: いいえ
- Android: はい
- デフォルト設定: 空

接続セキュリティレベル

- iOS: はい
- Android: はい
- デフォルト設定: TLS

受信ドキュメント交換 (Open In)

- iOS: はい
- Android: はい
- デフォルト設定: 無制限

制限付きOpen In例外リスト

- iOS: はい
- Android: はい
- デフォルト設定: 空 (Androidの場合); Office 365アプリ (iOSの場合)

注:

Androidでは、このポリシーは以前「Open In除外」という名前でした。iOSでは、このポリシーは非表示です。詳細については、[iOSアプリのMDXポリシー](#)を参照してください。

アプリのURLスキーム

- iOS: はい
- Android: いいえ
- デフォルト設定: 空。登録されているすべてのアプリURLスキームはブロックされます。

許可されたURL

- iOS: はい
- Android: いいえ
- デフォルト設定: デフォルト設定の詳細については、「iOSアプリ用MDXポリシー」の「アプリの操作」セクションを参照してください。

明示的なログオフ通知

- iOS: はい
- Android: いいえ
- デフォルト設定: Secure Mailの場合のみ、共有デバイス

アプリの操作 (アウトバウンドURL)

URLフィルタリングから除外されるドメイン

- iOS: はい
- Android: いいえ
- デフォルト設定: 空

許可されるURL

- iOS: はい
- Android: いいえ
- デフォルト設定: デフォルト設定の詳細については、「iOSアプリ用MDXポリシー」の「アプリの操作 (アウトバウンドURL)」セクションを参照してください。

許可されたセキュアWebドメイン

- iOS: はい
- Android: いいえ
- デフォルト設定: 空

アプリの制限

カメラをブロック

- iOS: はい
- Android: はい
- デフォルト設定: iOSではオフ、Androidではオン

ギャラリーをブロック

- iOS: いいえ
- Android: はい
- デフォルト設定: オフ

写真ライブラリをブロック

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

マイク録音をブロック

- iOS: はい
- Android: はい
- デフォルト設定: オン

音声入力をブロック

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

位置情報サービスをブロック

- iOS: はい
- Android: はい
- デフォルト設定: Androidの場合: Secure Mailではデフォルト値はオフです。その他のアプリではデフォルト値はオンです。

SMS作成をブロック

- iOS: はい
- Android: はい
- デフォルト設定: オン

画面キャプチャをブロック

- iOS: いいえ
- Android: はい
- デフォルト設定: オン

デバイスセンサーをブロック

- iOS: いいえ
- Android: はい
- デフォルト設定: オン

NFCをブロック

- iOS: いいえ
- Android: はい
- デフォルト設定: オン

iCloud をブロック

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

Look Up をブロック

- iOS: はい

- Android: いいえ
- デフォルト設定: オン

ファイルバックアップをブロック

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

AirPrint をブロック

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

印刷をブロック

- iOS: いいえ
- Android: はい
- デフォルト設定: オン

AirDropをブロック

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

ファイル添付をブロック

- iOS: はい
- Android: いいえ
- デフォルト設定: オフ

メール作成をブロック

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

Facebook および Twitter API をブロックする

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

画面コンテンツを不明瞭にする

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

サードパーティ製キーボードをブロックする

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

注

iOS 11以降

アプリログをブロック

- iOS: はい
- Android: はい
- デフォルト設定: オフ

ShareFileを有効にする

- iOS:
- Android: はい
- デフォルト設定: オン

ファイルからの添付を有効にする

- iOS: はい
- Android: いいえ

- デフォルト設定: オン

アプリのネットワークアクセス

ネットワークアクセス

- iOS: はい
- Android: はい
- デフォルト設定: 新しくアップロードされたアプリの場合、Secure Mail を除くすべてのアプリで、デフォルトは**ブロック済み**です。Intune にはブロック状態がないため、Secure Mail のデフォルトは**無制限**です。

マイクロVPNセッションが必要

- iOS: はい
- Android: はい
- デフォルト設定: 以前の設定を使用。新しくアップロードされたアプリの場合、デフォルト値は「いいえ」です。

マイクロVPNセッションの猶予期間（分）

- iOS: はい
- Android: はい
- デフォルト設定: 0（猶予期間なし）

除外リスト

- iOS: はい
- Android: はい
- デフォルト設定: 空

localhost 接続をブロックする

- iOS: いいえ
- Android: はい
- デフォルト設定: オフ

証明書ラベル

- iOS: はい

- Android: はい
- デフォルト設定: 空

アプリログ

デフォルトのログ出力

- iOS: はい
- Android: はい
- デフォルト設定: ファイル

デフォルトのログレベル

- iOS: はい
- Android: はい
- デフォルト設定: 4 (情報メッセージ)

最大ログファイル数

- iOS: はい
- Android: はい
- デフォルト設定: 2

最大ログファイルサイズ

- iOS: はい
- Android: はい
- デフォルト設定: 2 MB

アプリログのリダイレクト

- iOS: いいえ
- Android: はい
- デフォルト設定: オン

ログの暗号化

- iOS: いいえ
- Android: はい

- デフォルト設定: オフ

アプリのジオフェンス

中心点の経度

- iOS: はい
- Android: はい
- デフォルト設定: 0

中心点の緯度

- iOS: はい
- Android: はい
- デフォルト設定: 0

半径

- iOS: はい
- Android: はい
- デフォルト設定: 0 (無効)

注:

半径をメートル単位で設定します。ゼロに設定すると、ジオフェンスは無効になります。

アプリ設定

セキュアメール エクスチェンジサーバー

- iOS: はい
- Android: はい
- デフォルト設定: 空

注:

既存のアプリに対してこのポリシーを変更した場合、ユーザーはポリシーの変更を適用するためにアプリを削除して再インストールする必要があります。

Secure Mail ユーザー ドメイン

- iOS: はい
- Android: はい
- デフォルト設定: 空

バックグラウンドネットワークサービス

- iOS: はい
- Android: はい
- デフォルト設定: 空

注:

このポリシーを構成する場合は、ネットワークアクセスポリシーを「内部ネットワークへのトンネル」に設定してください。その後、このポリシーが有効になります。このポリシーは、Exchange Serverが内部ネットワーク内にあり、Citrix Gatewayを使用して内部Exchange Serverへの接続をプロキシする場合に使用します。

バックグラウンドサービスチケットの有効期限

- iOS: はい
- Android: はい
- デフォルト設定: 168時間 (7日間)

バックグラウンドネットワークサービスゲートウェイ

- iOS: はい
- Android: はい
- デフォルト設定: 空

注:

このポリシーを構成する場合は、ネットワークアクセスポリシーを「内部ネットワークへのトンネル」に設定してください。その後、このポリシーが有効になります。このポリシーは、Exchange Serverが内部ネットワーク内にある場合、またはCitrix Gatewayを使用して内部Exchange Serverへの接続をプロキシする場合に使用します。このポリシーは、ネットワークアクセスポリシーを構成すると有効になります。

連絡先のエクスポート

- iOS: はい
- Android: はい
- デフォルト設定: オフ

エクスポートする連絡先フィールド

- iOS: はい
- Android: はい
- デフォルト設定: すべて

すべてのSSL証明書を承認する

- iOS: はい
- Android: はい
- デフォルト設定: オフ

ロック画面の通知を制御する

- iOS: はい
- Android: はい
- 既定の設定: 許可

セキュア接続の使用

- iOS: いいえ
- Android: はい
- 既定の設定: オン

既定のメール通知

- iOS: はい
- Android: いいえ
- 既定の設定: オン

既定の同期間隔

- iOS: はい
- Android: はい

- 既定の設定: 3日

注:

Exchange ActiveSyncメールボックスポリシー設定の「最大メール保持期間フィルター」は、このポリシーよりも優先されます。Secure Mailには、「最大メール保持期間フィルター」よりも短い同期間隔の値のみが表示されます。

メールの検索制限

- iOS: はい
- Android: はい
- デフォルト設定: 無制限

最大同期間隔

- iOS: はい
- Android: はい
- デフォルト設定: すべて

週番号を有効にする

- iOS: はい
- Android: はい
- デフォルト設定: オフ

Wi-Fi経由での添付ファイルのダウンロードを有効にする

- iOS: はい
- Android: はい
- デフォルト設定: オフ

オフラインドキュメントを許可

- iOS: はい
- Android: はい
- デフォルト設定: 無制限

情報権限管理

- iOS: はい
- Android: はい
- デフォルト設定: オフ

メール分類

- iOS: はい
- Android: いいえ
- デフォルト設定: オフ

メール分類マーク

- iOS: はい
- Android: いいえ
- デフォルト設定: 空

メール分類名前空間

- iOS: はい
- Android: いいえ
- デフォルト設定: 空

メール分類バージョン

- iOS: はい
- Android: いいえ
- デフォルト設定: 空

デフォルトのメール分類

- iOS: はい
- Android: いいえ
- デフォルト設定: UNOFFICIAL

下書きメールの自動保存を有効にする

- iOS: はい
- Android: はい

- デフォルト設定: オン

iOSデータ保護を有効にする

- iOS: はい
- Android: いいえ
- デフォルト設定: オフ

プッシュ通知EWSホスト名

- iOS: はい
- Android: いいえ
- デフォルト設定: 空

プッシュ通知

- iOS: はい
- Android: いいえ
- デフォルト設定: オフ

プッシュ通知の地域

- iOS: はい
- Android: いいえ
- デフォルト設定: 米州

セキュアメールの初回起動時にS/MIMEを有効にする

- iOS: はい
- Android: いいえ
- デフォルト設定: オフ

初回認証メカニズム

- iOS: はい
- Android: はい
- デフォルト設定: MDXが提供するメールサーバーアドレスを使用

初回認証資格情報

- iOS: はい
- Android: はい
- デフォルト設定: 登録ユーザー名

週番号を有効にする

- iOS: はい
- Android: はい
- デフォルト設定: オフ

カレンダーのWebおよびオーディオオプション

- iOS: はい
- Android: はい
- デフォルト設定: GoToMeetingおよびユーザー入力

S/MIME公開証明書ソース

- iOS: はい
- Android: はい
- デフォルト設定: Exchange

LDAPサーバーアドレス

- iOS: はい
- Android: はい
- デフォルト設定: 空

LDAPベースDN

- iOS: はい
- Android: はい
- デフォルト設定: 空

LDAPに匿名でアクセス

- iOS: はい
- Android: はい

- デフォルト設定: オフ

許可されたメール ドメイン

- iOS: はい
- Android: いいえ
- デフォルト設定: 空

注

空の場合、ドメインを制限しません。

認証失敗時にユーザー名の移行を試行する

- iOS: はい
- Android: はい
- デフォルト設定: オフ

フィッシングメールアドレスを報告する

- iOS: はい
- Android: はい
- デフォルト設定: 空

フィッシング報告メカニズム

- iOS: いいえ
- Android: はい
- デフォルト設定: 添付ファイル (.eml) 経由で報告

Skype for Business会議ドメイン

- iOS: はい
- Android: はい
- デフォルト設定: 空

カレンダーのエクスポート

- iOS: はい

- Android: はい
- デフォルト設定: 会議時間

Slack を有効にする

- iOS: はい
- Android: はい
- デフォルト設定: オフ

Slack ワークスペース名

- iOS: はい
- Android: はい
- デフォルト設定: 空

発信者ID

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

注:

オンの場合、Secure Mail は発信者識別のため、保存されている連絡先の名前と電話番号を iOS に提供します。

分析

Google Analytics を有効にする

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

Google Analytics の詳細レベル

- iOS: はい
- Android: はい
- デフォルト設定: 完了

レポート

Citrix レポート

- iOS: はい
- Android: いいえ
- デフォルト設定: オフ

注:

Citrix は、この機能を機能フラグで制御する場合があります。この機能が機能するには、機能フラグとこのポリシーの両方を有効にする必要があります。

アップロードトークン

- iOS: はい
- Android: いいえ
- デフォルト設定: 空

Wi-Fi 経由でのみレポートを送信

- iOS: はい
- Android: いいえ
- デフォルト設定: オン

レポートファイルキャッシュの最大値

- iOS: はい
- Android: いいえ
- デフォルト設定: 2 MB

Office 365 の OAuth サポート

Office 365 にモダン認証を使用する

- iOS: いいえ
- Android: はい
- デフォルト設定: オフ

Office 365 認証メカニズム

- iOS: はい
- Android: いいえ
- デフォルト設定: OAuth を使用しない

信頼できる Exchange Online ホスト名

- iOS: はい
- Android: はい
- 既定の設定: `outlook.office365.com`

信頼されたAD FSホスト名

- iOS: はい
- Android: はい
- 既定の設定: `login.microsoftonline.com`

最新の認証用のカスタムユーザーエージェント

- iOS: いいえ
- Android: はい
- 既定の設定: 空

注:

このポリシーを構成しない場合、最新の認証中に既定のSecure Mailユーザーエージェントが使用されます。

メールリダイレクト

メールリダイレクト

- iOS: はい
- Android: いいえ
- デフォルト設定: Secure Mail

Slack連携

Slackを有効にする

- iOS: はい
- Android: はい
- デフォルト設定: オフ

Slackワークスペース名

- iOS: はい
- Android: はい
- デフォルト設定: 空

Android向けモバイル生産性アプリのMDXポリシー

この記事では、AndroidアプリのMDXポリシーについて説明します。ポリシー設定は、Citrix Endpoint Managementコンソールで変更します。詳細については、「アプリの追加」(</ja-jp/citrix-endpoint-management/apps.html>)を参照してください。

以下のリストには、Secure Webに固有のMDXポリシーは含まれていません。Secure Webに表示されるポリシーの詳細については、「Secure Webポリシー」(</ja-jp/citrix-secure-web/citrix-secure-web.html#secure-web-policies>)を参照してください。

認証

アプリのパスコード

オンの場合、アプリの起動時、または一定期間の非アクティブ状態からの再開時に、アプリのロックを解除するためにPINまたはパスコードが必要です。デフォルト値はオンです。

すべてのアプリの非アクティブタイマーを構成するには、**設定タブのクライアントプロパティ**で INACTIVITY_TIMERの値を分単位で設定します。デフォルトの非アクティブタイマー値は60分です。非アクティブタイマーを無効にして、アプリの起動時にのみPINまたはパスコードのプロンプトが表示されるようにするには、値をゼロに設定します。

注：

暗号化キーポリシーで「セキュアオフライン」を選択した場合、このポリシーは自動的に有効になります。

最大オフライン期間（時間）

アプリが、資格の再確認とポリシーの更新のためにネットワークログオンなしでオフラインで実行できる最大期間を定義します。デフォルト値は**168時間**（7日間）です。最小期間は1時間です。

期間が終了する30分前、15分前、5分前に、ユーザーにログオンを促す通知が表示されます。期間の終了後、ユーザーが正常にネットワークログオンを完了するまで、アプリはロックされたままになります。

代替 シトリックス ゲートウェイ

注：

Endpoint Managementコンソールでのこのポリシー名は**代替NetScaler® Gateway**です。

認証およびこのアプリとのマイクロVPNセッションに使用される特定の代替Citrix Gateway（旧称NetScaler Gateway）のアドレス。**代替NetScaler Gateway**は、オンラインセッション必須ポリシーと併用すると、アプリが特定のゲートウェイに再認証することを強制するオプションのポリシーです。このようなゲートウェイは通常、異なる（より高い保証の）認証要件とトラフィック管理ポリシーを持っています。空 の場合、常にサーバーのデフォルトが使用されます。デフォルト値は空です。

デバイスのセキュリティ

ジェイルブレイクまたはルート化されたデバイスをブロック

Onの場合、デバイスがジェイルブレイクまたはルート化されているとアプリはロックされます。**Off**の場合、デバイスがジェイルブレイクまたはルート化されていてもアプリは実行できます。デフォルト値は**On**です。

デバイスの暗号化を必須にする

Onの場合、デバイスに暗号化が構成されていないとアプリはロックされます。**Off**の場合、デバイスに暗号化が構成されていなくてもアプリは実行を許可されます。デフォルト値は**Off**です。

注：

このポリシーはAndroid 3.0（Honeycomb）でのみサポートされています。ポリシーを**On**に設定すると、古いバージョンではアプリが実行されなくなります。

デバイスロックを必須にする

Device PIN or passcodeが選択されている場合、デバイスにPINまたはパスコードがないとアプリはロックされます。**Device pattern screen lock**が選択されている場合、デバイスにパターン画面ロックが設定されていないとアプリはロックされます。**Off**の場合、デバイスにPIN、パスコード、またはパターン画面ロックが設定されていなくてもアプリは実行を許可されます。デフォルト値は**Off**です。

Device PIN or passcodeには、Android 4.1（Jelly Bean）以降のバージョンが必要です。ポリシーを**Device PIN or passcode**に設定すると、古いバージョンではアプリが実行されなくなります。

Android Mデバイスでは、**Device PIN or passcode**と**Device pattern screen lock**オプションは同じ効果を持ちます。どちらのオプションでも、デバイスにPIN、パスコード、またはパターン画面ロックが設定されていない場合、アプリはロックされます。

ネットワーク要件

Wi-Fiを必須にする

Onの場合、デバイスがWi-Fiネットワークに接続されていないとアプリはロックされます。**Off**の場合、デバイスが4G/3G、LAN、Wi-Fi接続などのアクティブな接続を持っている場合、アプリは実行できます。デフォルト値は**Off**です。

許可されたWi-Fiネットワーク

許可されたWi-Fiネットワークのコンマ区切りリスト。ネットワーク名に英数字以外の文字（コンマを含む）が含まれる場合、名前は二重引用符で囲む必要があります。アプリは、リストされているネットワークのいずれかに接続されている場合にのみ実行されます。空白のままにした場合、すべてのネットワークが許可されます。この値は、セルラーネットワークへの接続には影響しません。デフォルト値は空白です。

その他のアクセス

アプリ更新猶予期間（時間）

システムがアプリの更新が利用可能であることを検出した後、アプリを使用できる猶予期間を定義します。デフォルト値は**168時間**（7日間）です。

注：

ゼロを使用することはお勧めしません。更新がダウンロードされてインストールされるまで（ユーザーへの警告なしに）、実行中のアプリがすぐに使用できなくなるためです。この値は、アプリを実行しているユーザーが、必要な更新に準拠するためにアプリを終了せざるを得なくなる（作業が失われる可能性のある）状況につながる可能性があります。

必須アップグレードを無効にする

ユーザーがApp Storeでアプリの最新バージョンにアップグレードする必要性を無効にします。デフォルト値は**ON**です。

ロック時にアプリデータを消去

アプリがロックされたときにデータを消去し、アプリをリセットします。**オフ**の場合、アプリがロックされてもアプリデータは消去されません。デフォルト値は**オフ**です。

アプリは、次のいずれかの理由でロックされることがあります。

- ユーザーのアプリエンタイトルメントの喪失
- アプリのサブスクリプションが削除された
- アカウントが削除された
- Secure Hub がアンインストールされました
- アプリの認証失敗が多すぎます
- ジェイルブレイクされたデバイスが検出されました (ポリシー設定による)
- 他の管理操作によってデバイスがロック状態にされました

アクティブポーリング期間 (分)

アプリが起動すると、MDXフレームワークはCitrix Endpoint Managementをポーリングして、現在のアプリとデバイスのステータスを判断します。Endpoint Managementを実行しているサーバーに到達可能であると仮定すると、フレームワークはデバイスのロック/消去ステータスとアプリの有効/無効ステータスに関する情報を返します。サーバーに到達可能であるかどうかにかかわらず、アクティブポーリング期間の間隔に基づいて後続のポーリングがスケジュールされます。期間が経過すると、新しいポーリングが再度試行されます。デフォルト値は**60分** (1時間) です。

重要:

この値は、リスクの高いアプリの場合にのみ低く設定してください。そうしないと、パフォーマンスに影響が出る可能性があります。

暗号化

暗号化の種類

MDXとデバイスプラットフォームのどちらがデータの暗号化を処理するかを選択できます。**MDX暗号化**を選択すると、MDXがデータを暗号化します。**コンプライアンス強制によるプラットフォーム暗号化**を選択すると、デバイスプラットフォームがデータを暗号化します。デフォルト値は**MDX暗号化**です。

非準拠デバイスの動作

デバイスが暗号化の最小コンプライアンス要件に準拠していない場合に実行するアクションを選択できます。アプリを通常どおり実行するには、**アプリを許可**を選択します。警告が表示された後にアプリを実行するには、**警告後にアプリを許可**を選択します。アプリの実行をブロックするには、**ブロック**を選択します。デフォルト値は**警告後にアプリを許可**です。

暗号化キー

暗号化キーの派生に使用されるシークレットをデバイスに永続化できるようにします。利用可能なオプションは「オフラインアクセスを許可」のみです。

Citrixでは、暗号化されたコンテンツへのアクセスを保護するために、認証ポリシーをネットワークログオンまたはオフラインパスワードチャレンジを有効にするように設定することをお勧めします。

プライベートファイルの暗号化

次の場所にあるプライベートデータファイルの暗号化を制御します: /data/data/<appname> および /mnt/sdcard/Android/data/<appname>。

Disabled オプションは、プライベートファイルが暗号化されないことを意味します。

SecurityGroup オプションは、同じセキュリティグループ内のすべてのMDXアプリで共有されるキーを使用してプライベートファイルを暗号化します。**Application** オプションは、このアプリに固有のキーを使用してプライベートファイルを暗号化します。デフォルト値は**SecurityGroup**です。

プライベートファイルの暗号化の除外

コンマ区切りのファイルパスのリストが含まれます。各パスは、暗号化される1つ以上のファイルを表す正規表現です。ファイルパスは、内部および外部サンドボックスに対する相対パスです。デフォルト値は空です。

除外は、以下のフォルダーにのみ適用されます。

- 内部ストレージ:

```
/data/data/<your_package_name>
```

- SDカード:

```
/storage/emulated/\<SD Card Slot>/Android/data/<your_package_name>
```

```
/storage/emulated/legacy/Android/data/<your_package_name>
```

例

除外するファイル	プライベートファイルの暗号化の除外における値
/data/data/com.citrix.mail/files/a.txt	^files/a.txt
/storage/emulated/0/Android/data/com.citrix.mail/files 内のすべてのテキストファイル	^files/(.)+.txt\$
/data/data/com.citrix.mail/files 内のすべてのファイル	^ファイル/

公開ファイルのアクセス制限

コンマ区切りのリストが含まれています。各エントリは、正規表現パスの後に(NA)、(RO)、または(RW)が続きます。パスに一致するファイルは、**アクセスなし**、**読み取り専用**、または**読み取り/書き込み**アクセスに制限されます。リストは順番に処理され、最初に一致したパスがアクセス制限の設定に使用されます。デフォルト値は空です。

このポリシーは、**公開ファイルの暗号化が有効になっている場合**（無効オプションから**SecurityGroup**または**Application**オプションに変更された場合）にのみ適用されます。このポリシーは、既存の暗号化されていない公開ファイルにのみ適用され、これらのファイルがいつ暗号化されるかを指定します。

除外するファイル	プライベートファイル暗号化の値
外部ストレージのダウンロードフォルダは読み取り専用	EXT:\^Download/(RO)
仮想ストレージの Music フォルダ内のすべてのMP3ファイルにアクセスなし	VS:\^Music/(.)+.mp3\$(NA)

公開ファイルの暗号化

公開ファイルの暗号化を制御します。**Disabled**の場合、公開ファイルは暗号化されません。**SecurityGroup**の場合、同じセキュリティグループ内のすべてのMDXアプリで共有されるキーを使用して公開ファイルを暗号化します。**Application**の場合、このアプリに固有のキーを使用して公開ファイルを暗号化します。

デフォルト値は**SecurityGroup**です。

公開ファイルの暗号化除外

ファイルパスのコンマ区切りリストが含まれます。各パスは、暗号化されない1つ以上のファイルを表す正規表現です。ファイルパスは、デフォルトの外部ストレージおよびデバイス固有の外部ストレージに対して相対的です。

公開ファイルの暗号化除外には、外部フォルダーの場所のみが含まれます。

例

除外するファイル	公開ファイルの暗号化除外の値
SDカードのダウンロードフォルダー	ダウンロード
Music フォルダー内のすべてのMP3ファイル	\^Music/(.)+.mp3\$

公開ファイルの移行

このポリシーは、公開ファイル暗号化ポリシーを有効にした場合（**Disabled**から**SecurityGroup**または**Application**に変更した場合）にのみ適用されます。このポリシーは、既存の暗号化されていない公開ファイルにのみ適用され、これらのファイルがいつ暗号化されるかを指定します。デフォルト値は****Write (RO/RW)****です。

「無効」オプションは、既存のファイルが暗号化されないことを意味します。「書き込み (**RO/RW**)」オプションは、書き込み専用または読み取り/書き込みアクセスで開かれた場合にのみ、既

存のファイルを暗号化します。「任意」オプションは、任意のモードで開かれた場合に既存のファイルを暗号化します。オプション:

- **無効**。既存のファイルを暗号化しません。
- **書き込み (RO/RW)**。書き込み専用または読み取り/書き込みアクセスで開かれた場合にのみ、既存のファイルを暗号化します。
- **任意**。任意のモードで開かれた場合に既存のファイルを暗号化します。

注:

-新しいファイル、または上書きされた既存の暗号化されていないファイルは、すべての場合において置換ファイルを暗号化します。-既存の公開ファイルを暗号化すると、同じ暗号化キーを持たない他のアプリからそのファイルにアクセスできなくなります。

アプリの相互作用

セキュリティグループ

Citrix Endpoint Management™ で管理されているすべてのモバイルアプリが相互に情報を交換できるようにする場合は、このフィールドを空白のままにします。特定のアプリセット (例: 財務または人事) のセキュリティ設定を管理するために、セキュリティグループ名を定義します。

注意:

既存のアプリに対してこのポリシーを変更した場合、ユーザーはポリシーの変更を適用するためにアプリを削除して再インストールする必要があります。

切り取りとコピー

このアプリのクリップボードの切り取りおよびコピー操作をブロック、許可、または制限します。「制限」の場合、コピーされたクリップボードデータは、MDXアプリのみが利用できるプライベートクリップボードに配置されます。デフォルト値は「制限」です。

貼り付け

このアプリのクリップボードの貼り付け操作をブロック、許可、または制限します。「制限」の場合、貼り付けられたクリップボードデータは、MDXアプリのみが利用できるプライベートクリップボードから取得されます。デフォルト値は「無制限」です。

ドキュメント交換 (Open In)

アプリのドキュメント交換操作をブロック、許可、または制限します。**制限付き**の場合、ドキュメントは他のMDXアプリおよび「制限付きOpen-In例外リスト」ポリシーで指定されたアプリ例外とのみ交換できます。**無制限**の場合、ユーザーがラップされていないアプリでドキュメントを開けるように、「プライベートファイル暗号化」および「パブリックファイル暗号化」ポリシーを**無効**に設定します。デフォルト値は**制限付き**です。

フィルタリングから除外されるURLドメイン

このポリシーは、特定の送信URLをMDXフィルタリングから除外するために使用されます。以下の完全修飾ドメイン名 (FQDN) またはDNSサフィックスのコンマ区切りリストは、MDXフィルタリングから除外されます。このポリシーにエントリが含まれている場合、リスト内の少なくとも1つの項目に一致するホストフィールドを持つURL (DNSサフィックスの一致による) は、変更されずにデフォルトのブラウザに送信されます。デフォルト値は空です。

許可されたSecure Webドメイン

このポリシーは、URLフィルタリングポリシーによって除外されていないドメインにのみ適用されます。ドキュメント交換が制限されている場合にSecure Webアプリにリダイレクトされる、完全修飾ドメイン名 (FQDN) またはDNSサフィックスのコンマ区切りリストを追加します。

このポリシーにエントリが含まれている場合、リスト内の少なくとも1つの項目に一致するホストフィールドを持つURL (DNSサフィックスの一致による) のみが、ドキュメント交換が制限されている場合にSecure Webアプリにリダイレクトされます。

その他のすべてのURLは、デフォルトのAndroid Webブラウザに送信されます (ドキュメント交換制限ポリシーをバイパスします)。デフォルト値は空です。

制限付きOpen-In例外リスト

ドキュメント交換 (Open In) ポリシーが**制限付き**の場合、このAndroidインテントのリストは管理対象外アプリに渡すことが許可されます。リストにフィルタを追加するには、Androidインテントに関する知識が必要です。フィルタは、アクション、パッケージ、スキーム、またはそれらの任意の組み合わせを指定できます。

例

```
{action=android.intent.action.MAIN}

{package=com.sharefile.mobile}

{action=android.intent.action.DIAL scheme=tel}
```

```
{action=android.intent.action.VIEW scheme=msteams  
package=com.microsoft.teams}
```

注意

このポリシーのセキュリティ上の影響を考慮してください。例外リストにより、管理対象外アプリとMDX環境の間でコンテンツが移動できるようになります。

受信ドキュメント交換 (Open In)

このアプリの受信ドキュメント交換操作をブロック、制限、または許可します。**制限付き**の場合、ドキュメントは他のMDXアプリとのみ交換できます。デフォルト値は**無制限**です。

「**ブロック済み**」または「**制限済み**」の場合、受信ドキュメント交換ホワイトリストポリシーを使用して、このアプリにドキュメントを送信できるアプリを指定できます。他のポリシーの相互作用については、Block Galleryポリシーを参照してください。

オプション：「**無制限**」、「**ブロック済み**」、または「**制限済み**」

受信ドキュメント交換ホワイトリスト

受信ドキュメント交換ポリシーが制限されているかブロックされている場合、MDX以外のアプリを含むこのコンマ区切りのアプリIDリストは、アプリにドキュメントを送信できます。このポリシーは非表示であり、編集できません。

接続セキュリティレベル

接続に使用されるTLS/SSLの最小バージョンを決定します。「**TLS**」の場合、接続はすべてのTLSプロトコルをサポートします。「**SSLv3 and TLS**」の場合、接続はSSL 3.0とTLSをサポートします。デフォルト値は「**TLS**」です。

アプリの制限

重要：

アプリが電話機能にアクセスしたり使用したりするのをブロックするポリシーのセキュリティ上の影響を考慮してください。これらのポリシーが「**オフ**」の場合、管理されていないアプリとセキュア環境の間でコンテンツが移動する可能性があります。

カメラをブロック

「オン」の場合、アプリがカメラハードウェアを直接使用するのを防ぎます。デフォルト値は「オン」です。

ギャラリーをブロック

「オン」の場合、アプリがデバイス上のギャラリーにアクセスするのを防ぎます。デフォルト値は「オフ」です。このポリシーは、受信ドキュメント交換（Open In）ポリシーと連携して機能します。

- 受信ドキュメント交換（Open In）が「**制限済み**」に設定されている場合、管理対象アプリで作業しているユーザーは、Block Galleryの設定に関係なく、ギャラリーから画像を添付できません。
- 受信ドキュメント交換（Open In）が「**無制限**」に設定されている場合、管理対象アプリで作業しているユーザーは、次のようになります。
 - ギャラリーブロックが**オフ**に設定されている場合、ユーザーは画像を添付できます。
 - ギャラリーブロックが**オン**の場合、ユーザーは画像を添付できません。

マイク録音をブロック

オンの場合、アプリがマイクハードウェアを直接使用するのを防ぎます。デフォルト値は**オン**です。

位置情報サービスをブロック

オンの場合、アプリが位置情報サービスコンポーネント（GPSまたはネットワーク）を使用するのを防ぎます。Secure Mailのデフォルト値は**オフ**です。

SMS作成をブロック

オンの場合、アプリからSMS/テキストメッセージを送信するために使用されるSMS作成機能がアプリで使用されるのを防ぎます。デフォルト値は**オン**です。

画面キャプチャをブロック

オンの場合、アプリの実行中にユーザーが画面キャプチャを撮るのを防ぎます。また、ユーザーがアプリを切り替えるときに、アプリ画面を隠します。デフォルト値は**オン**です。

Androidの近距離無線通信（NFC）機能を使用する場合、一部のアプリはコンテンツを送信する前に自身のスクリーンショットを撮ります。ラップされたアプリでその機能を有効にするには、**画面キャプチャをブロックポリシーをオフに変更**します。

デバイスセンサーをブロック

オンの場合、アプリがデバイスセンサー（加速度計、モーションセンサー、ジャイロ스코ープなど）を使用するのを防ぎます。デフォルト値は**オン**です。

NFCをブロック

オンの場合、アプリが近距離無線通信（NFC）を使用するのを防ぎます。デフォルト値は**オン**です。

アプリログをブロック

オンの場合、アプリがモバイル生産性アプリの診断ログ機能を使用することを禁止します。**オフ**の場合、アプリログが記録され、Secure Hubのメールサポート機能を使用して収集される可能性があります。デフォルト値は**オフ**です。

印刷をブロック

オンの場合、アプリがデータを印刷するのを防ぎます。アプリに共有コマンドがある場合、印刷を完全にブロックするには、ドキュメント交換（で開く）を**制限**または**ブロック**に設定する必要があります。デフォルト値は**オン**です。

ShareFileを有効にする

ユーザーがShareFileを使用してファイルを転送できるようにします。デフォルト値は**オン**です。

アプリのネットワークアクセス

ネットワークアクセス

注：

トンネル化 - Web SSO は、設定における **Secure Browse** の名称です。動作は同じです。

設定オプションは次のとおりです。

- **以前の設定を使用:** 以前のポリシーで設定した値がデフォルトになります。このオプションを変更した場合、このオプションに戻すことはできません。また、新しいポリシーへの変更は、ユーザーがアプリをバージョン18.12.0以降にアップグレードするまで有効になりません。
- **ブロック済み:** アプリが使用するネットワークAPIは失敗します。以前のガイドラインに従い、このような失敗は適切に処理する必要があります。
- **無制限:** すべてのネットワーク呼び出しは直接行われ、トンネル化されません。

- **トンネル化 - フルVPN:** 管理対象アプリからのすべてのトラフィックはCitrix Gatewayを介してトンネル化されます。
- **トンネル化 - Web SSO:** HTTP/HTTPS URLが書き換えられます。このオプションでは、HTTPおよびHTTPSトラフィックのトンネル化のみが可能です。**トンネル化 - Web SSO**の大きな利点は、HTTPおよびHTTPSトラフィックのシングルサインオン (SSO) と、PKINIT認証です。Androidでは、このオプションはセットアップのオーバーヘッドが低いため、Webブラウジングタイプの操作に推奨されるオプションです。

トンネル化モードのいずれかが選択されている場合、この初期モードでは、エンタープライズネットワークへのアプリごとのVPNトンネルが作成されます。ここでは、Citrix Gatewayの分割トンネル設定が使用されます。Citrixは、クライアント証明書またはエンドツーエンドSSLをエンタープライズネットワーク内のリソースに利用する接続には、**トンネル化フルVPN**を推奨しています。Citrixは、シングルサインオン (SSO) を必要とする接続には、**トンネル化 - Web SSO**を推奨しています。

Micro VPNセッションが必要

はいの場合、ユーザーはエンタープライズネットワークへの接続とアクティブなセッションを持っている必要があります。いいえの場合、アクティブなセッションは必要ありません。デフォルト値は**以前の設定**を使用です。新しくアップロードされたアプリの場合、デフォルト値はいいえです。このポリシーへのアップグレード前に選択されていた設定は、**以前の設定**を使用以外のオプションが選択されるまで有効です。

除外リスト

VPN接続を介さずに直接アクセスされるFQDNまたはDNSサフィックスのコンマ区切りリスト。このポリシーは、Citrix Gatewayが分割トンネルリバースモードで構成されている場合の**トンネル化 - Web SSO**モードにのみ適用されます。

localhost接続をブロック

オンの場合、アプリはlocalhost接続を行うことが許可されません。localhostは、デバイス上でローカルに発生する通信用のアドレス（127.0.0.1など）です。localhostは、ローカルネットワークインターフェイスハードウェアをバイパスし、ホスト上で実行されているネットワークサービスにアクセスします。オフの場合、このポリシーはネットワークアクセスポリシーを上書きします。つまり、デバイスがローカルでプロキシサーバーを実行している場合、アプリはセキュアコンテナの外部に接続できます。デフォルトは**オフ**です。

証明書ラベル

When used with the StoreFront™ certificate integration service, this label identifies the specific certificate required for this app. If no label is provided, a certificate is not made available for use with a public key infrastructure (PKI). Default value is empty (no certificate used).

アプリログ

デフォルトのログ出力

Citrix Endpoint Managementアプリ診断ログ機能がデフォルトで使用する出力媒体を決定します。ファイル、コンソール、またはその両方が可能です。デフォルト値はファイルです。

デフォルトのログレベル

モバイル生産性アプリ診断ログ機能のデフォルトの詳細度を制御します。レベル番号が高いほど、より詳細なログが含まれます。

- 0 - ログなし
- 1 - 重大なエラー
- 2 - エラー
- 3 - 警告
- 4 - 情報メッセージ
- 5 - 詳細情報メッセージ
- 6～15 - デバッグレベル1～10

デフォルト値はレベル4 (情報メッセージ) です。

最大ログファイル数

モバイル生産性アプリの診断ログ機能によって保持されるログファイルの数を、ロールオーバーする前に制限します。最小値は2です。最大値は8です。デフォルト値は2です。

最大ログファイルサイズ

モバイル生産性アプリの診断ログ機能によって保持されるログファイルのサイズ (MB) を、ロールオーバーする前に制限します。最小値は1 MBです。最大値は5 MBです。デフォルト値は2 MBです。

アプリログのリダイレクト

Onの場合、アプリからのシステムログまたはコンソールログを傍受し、モバイル生産性アプリの診断機能にリダイレクトします。この設定が**Off**の場合、アプリによるシステムログまたはコンソールログの使用は傍受されません。デフォルト値は**On**です。

ログの暗号化

オンの場合、Citrix Endpoint Managementは診断ログを記録する際に暗号化します。**オフ**の場合、診断ログはアプリのサンドボックス内で暗号化されずに残ります。

注意:

構成されたログレベルによっては、ログの暗号化はアプリのパフォーマンスとバッテリー寿命に著しい影響を与える可能性があります。

デフォルト値は**オフ**です。

アプリのジオフェンス

中心点の経度

アプリが動作するように制限されているポイント/半径ジオフェンスの中心点の経度（X座標）。構成されたジオフェンスの外で操作された場合、アプリはロックされたままになります。値は符号付き度数形式（DDD.dddd）で表現する必要があります。例: 「-31.9635」。西経にはマイナス記号を付ける必要があります。デフォルト値は**0**です。

中心点の緯度

アプリが動作するように制限されているポイント/半径ジオフェンスの中心点の緯度（Y座標）。構成されたジオフェンスの外で操作された場合、アプリはロックされたままになります。

値は符号付き度数形式（DDD.dddd）で表現する必要があります。例: 「43.06581」。南緯にはマイナス記号を付ける必要があります。デフォルト値は**0**です。

半径

アプリが動作するように制限されているジオフェンスの半径。構成されたジオフェンスの外で操作された場合、アプリはロックされたままになります。値はメートルで表現する必要があります。ゼロに設定すると、ジオフェンスは無効になります。デフォルトは**0**（無効）です。

分析

Google Analyticsの詳細

Citrixは製品品質向上のため、分析データを収集します。匿名を選択すると、企業を特定できる情報の収集から除外されます。

アプリ設定

セキュアメール Exchangeサーバー

Exchange Serverの完全修飾ドメイン名 (FQDN) または、iOSのみの場合、IBM Notes Traveler サーバーのFQDNです。デフォルト値は空です。このフィールドにドメイン名を入力すると、ユーザーは編集できません。フィールドを空のままにすると、ユーザーは独自のサーバー情報を提供します。

注意:

既存のアプリに対してこのポリシーを変更した場合、ユーザーはポリシーの変更を適用するためにアプリを削除して再インストールする必要があります。

Secure Mailユーザー ドメイン

Exchangeユーザー、またはiOSのみの場合、NotesユーザーのデフォルトのActive Directoryドメイン名です。デフォルト値は空です。

バックグラウンドネットワークサービス

バックグラウンドネットワークアクセスが許可されているサービスアドレスのFQDNとポート。この値は、社内ネットワーク内、またはSecure Mailが接続する別のネットワーク内にあるExchange ServerまたはActiveSyncサーバーである可能性があります（例：mail.example.com:443）。

このポリシーを構成する場合は、ネットワークアクセスポリシーを**内部ネットワークにトンネル接続**に設定します。このポリシーは、ネットワークアクセスポリシーを構成したときに有効になります。Exchange Serverが社内ネットワーク内にあり、NetScaler Gatewayを使用して社内Exchange Serverへの接続をプロキシしたい場合に、このポリシーを使用します。

デフォルト値は空であり、バックグラウンドネットワークサービスが利用できないことを意味します。

バックグラウンドサービスチケットの有効期限

バックグラウンドネットワークサービスチケットが有効な期間。有効期限が切れると、チケットを更新するためにエンタープライズログオンが必要になります。デフォルト値は**168時間**（7日間）です。

バックグラウンドネットワークサービスゲートウェイ

バックグラウンドネットワークサービスに使用する代替ゲートウェイアドレス（FQDN:ポート形式）。このアドレスは、Secure Mailが社内Exchange Serverに接続するために使用するCitrix GatewayのFQDNとポート番号です。Citrix Gateway構成ユーティリティで、Secure Ticket Authority (STA) を構成し、ポリシーを仮想サーバーにバインドする必要があります。

デフォルト値は空であり、代替ゲートウェイが存在しないことを意味します。

このポリシーを構成する場合は、ネットワークアクセスポリシーを**内部ネットワークにトンネル接続**に設定します。このポリシーは、ネットワークアクセスポリシーを構成したときに有効になります。このポリシーは、Exchange Serverが内部ネットワークに存在し、Citrix Gatewayを使用して内部Exchange Serverへの接続をプロキシする場合に使用します。

連絡先のエクスポート

重要：

ユーザーがExchange Serverに直接アクセスできる場合（つまり、Citrix Gatewayの外部から）、この機能を有効にしないでください。そうしないと、連絡先がデバイスとExchangeで重複します。

オフの場合、Secure Mailの連絡先がデバイスに一方方向で同期されるのを防ぎ、Secure Mailの連絡先（vCardとして）が共有されるのを防ぎます。デフォルト値は**オフ**です。

エクスポートする連絡先フィールド

アドレス帳にエクスポートする連絡先フィールドを制御します。**すべての場合**、すべての連絡先フィールドがエクスポートされます。**名前と電話番号**の場合、名前と電話番号に関連するすべての連絡先フィールドがエクスポートされます。**名前、電話番号、メールアドレス**の場合、名前、電話番号、メールアドレスに関連するすべての連絡先フィールドがエクスポートされます。デフォルト値は**すべて**です。

すべてのSSL証明書を承認する

オンの場合、Secure MailはすべてのSSL証明書（有効かどうかにかかわらず）を承認し、アクセスを許可します。オフの場合、Secure Mailは証明書エラーが発生したときにアクセスをブロックし、警告を表示します。デフォルト値は**オフ**です。

セキュア接続を使用する

オンの場合、Secure Mailはセキュア接続を使用します。オフの場合、Secure Mailはセキュア接続を使用しません。デフォルトは**オン**です。

情報権限管理

オンの場合、Secure MailはExchange Information Rights Management (IRM) 機能に対応します。デフォルト値は**オフ**です。

ロック画面通知を制御する

ロックされたデバイス画面にメールとカレンダーの通知を表示するかどうかを制御します。**許可**が選択されている場合、通知に含まれるすべての情報が表示されます。**ブロック**が選択されている場合、通知は表示されません。**メール送信者またはイベントのタイトル**が選択されている場合、メール送信者の名前またはカレンダーイベントのタイトルのみが表示されます。**件数のみ**が選択されている場合、メールと会議の招待の件数、およびカレンダーリマインダーの時刻のみが表示されます。デフォルト値は**許可**です。

デフォルトの同期間隔

Secure Mailのデフォルトの同期間隔を指定します。Secure Mailユーザーはデフォルトを変更できます。

Exchange ActiveSyncメールボックスポリシー設定の**最大メール保持期間フィルター**は、このポリシーよりも優先されます。最大メール保持期間フィルターよりも長いデフォルトの同期間隔を指定した場合、代わりに**最大メール保持期間フィルター**設定が使用されます。Secure Mailは、**Active Sync****最大メール保持期間フィルター**設定よりも短い同期間隔の値のみを表示します。

デフォルト値は**3日間**です。

Wi-Fi経由での添付ファイルのダウンロードを有効にする

オンの場合、Secure Mailの添付ファイルのダウンロードオプションが有効になり、ユーザーはデフォルトで社内Wi-Fiネットワーク経由で添付ファイルをダウンロードできます。オフの場合、Secure Mailの添付ファイルのダウンロードオプションが無効になり、ユーザーはデフォルトでWi-Fi経由で添付ファイルをダウンロードできません。デフォルト値は**オフ**です。

オフラインドキュメントを許可する

ユーザーがデバイスにオフラインドキュメントを保存できるかどうか、および保存期間を指定します。デフォルト値は**無制限**です。

メール下書きの自動保存を有効にする

オンの場合、Secure Mailはメッセージを下書きフォルダーに自動保存することをサポートします。デフォルト値は**オン**です。

初回認証メカニズム

このポリシーは、初回使用時のプロビジョニング画面で**アドレスフィールド**に入力されるのが、MDXによって提供されるメールサーバーアドレスか、ユーザーのメールアドレスかを示します。デフォルト値は**メールサーバーアドレス**です。

初回認証資格情報

このポリシーは、初回使用時のプロビジョニング画面に入力するユーザー名として選択する必要がある値を定義します。デフォルト値は**登録ユーザー名**です。

週番号を有効にする

オンの場合、カレンダービューに週番号が含まれます。デフォルト値は**オフ**です。

メール分類

オンの場合、Secure MailはSEC（セキュリティ）およびDLM（配布制限マーカー）のメール分類マーキングをサポートします。分類マーキングは、メールヘッダーに**X-Protective-Marking values**として表示されます。関連するメール分類ポリシーを必ず構成してください。デフォルト値は**オフ**です。

メール分類マーキング

エンドユーザーが利用できる分類マーキングを指定します。リストが空の場合、Secure Mailには保護マーキングのリストは含まれません。マーキングリストには、セミコロンで区切られた値のペアが含まれます。各ペアには、Secure Mailに表示される値と、Secure Mailのメール件名およびヘッダーに追加されるテキストであるマーキング値が含まれます。たとえば、マーキングペア `"UNOFFICIAL, SEC=UNOFFICIAL;"` では、リスト値は**「UNOFFICIAL」で、マーキング値は「SEC=UNOFFICIAL」**です。

メール分類ネームスペース

使用される分類標準によってメールヘッダーで必要とされる分類ネームスペースを指定します。たとえば、ネームスペース「gov.au」はヘッダーに「NS=gov.au」と表示されます。デフォルト値は空です。

メール分類バージョン

使用される分類標準によってメールヘッダーで必要とされる分類バージョンを指定します。たとえば、バージョン「2012.3」はヘッダーに「VER=2012.3」と表示されます。デフォルト値は空です。

デフォルトのメール分類

ユーザーがマーキングを選択しなかった場合にSecure Mailがメールに適用する保護マーキングを指定します。この値は、メール分類マーキングポリシーのリストに含まれている必要があります。デフォルト値は**UNOFFICIAL**です。

メール検索制限

メールサーバー検索に含まれる日数を制限することで、モバイルデバイスからアクセスできるメール履歴の量を制限します。モバイルデバイスに同期されるメールの量を制限するには、最大同期間隔ポリシーを構成します。デフォルト値は**無制限**です。

最大同期間隔

モバイルデバイスにローカルに保存されるメールの量を、同期期間を制限することで制御します。

デバイスがメールサーバーを検索できる期間を制限するには、メールサーバー検索制限ポリシーを構成します。

値は次のとおりです。

- 3日間
- 1週間
- 2週間
- 1か月
- すべて

デフォルト値は**すべて**です。

カレンダーのWebおよびオーディオオプション

- **GoToMeetingとユーザー入力** - このオプションを選択すると、ユーザーは設定したい会議の種類を選択できます。オプションには、GoToMeetingページを開くGoToMeetingと、ユーザーが会議情報を手動で入力できるその他の会議が含まれます。
- **ユーザー入力のみ** - このオプションを選択すると、ユーザーは直接「その他の会議」ページに移動し、会議情報を手動で入力できます。

S/MIME公開証明書のソース

S/MIME公開証明書のソースを指定します。**Exchange**の場合、Secure MailはExchange Serverから証明書を取得します。**LDAP**の場合、Secure MailはLDAPサーバーから証明書を取得します。デフォルト値は**Exchange**です。

LDAPサーバーアドレス

ポート番号を含むLDAPサーバーアドレス。デフォルト値は空です。

LDAPベースDN

LDAPベース識別名。デフォルト値は空です。

LDAPに匿名でアクセス

このポリシーがオンの場合、Secure Mailは事前の認証なしにLDAPを検索できます。デフォルトはオフです。

許可されたメールアドレスドメイン

server.company.com,server.company.co.uk のように、許可されたメールアドレスドメインのリストをコンマ区切り形式で定義します。デフォルト値は空であり、Secure Mailがメールアドレスドメインをフィルタリングせず、すべてのメールアドレスドメインをサポートすることを意味します。Secure Mailは、リストされたドメインをメールアドレスのドメイン名と照合します。

たとえば、server.company.com がリストされたドメイン名で、メールアドレスが user@internal.server.company.com の場合、Secure Mailはそのメールアドレスをサポートします。

プッシュ通知

メールボックスのアクティビティに関するFCMベースの通知を有効にします。**オン**の場合、Secure Mailはプッシュ通知をサポートします。デフォルト値は**オフ**です。

プッシュ通知EWSホスト名

メール用のExchange Web Services (EWS) をホストするサーバー。値は、ポート番号を含むEWSのURLである必要があります。デフォルト値は空です。

プッシュ通知リージョン

Secure MailユーザーのFCMホストが配置されているリージョン。オプションは、南北アメリカ、EMEA、PACです。デフォルト値は南北アメリカです。

認証失敗時にユーザー名移行を試行

このポリシーは、認証のためにExchangeユーザー名をUPNに移行しようとしています。デフォルト値はオフです。

フィッシングメールアドレスの報告

設定されている場合、疑わしいフィッシングメールを指定されたメールアドレス、またはコンマ区切りのメールアドレスのリストに報告できます。デフォルト値は空です。このポリシーを設定しない場合、フィッシングメッセージを報告できません。

フィッシング報告メカニズム

このポリシーは、疑わしいフィッシングメールを報告するために使用されるメカニズムを示します。

- 添付ファイル (.eml) で報告 – フィッシングメールを添付ファイルとして報告します。添付ファイルは、「フィッシングメールアドレスの報告」ポリシーで構成されたメールアドレス、またはコンマ区切りのメールアドレスのリストに送信されます。
- 転送で報告 – フィッシングメールを転送として報告します。メールは、「フィッシングメールアドレスの報告」ポリシーで構成されたメールアドレス、またはコンマ区切りのメールアドレスのリストに転送されます。

注:

このポリシーは、Microsoft Exchangeサーバーでのみ利用可能です。

デフォルトは添付ファイル (.eml) で報告です。

Skype for Business会議ドメイン

このポリシーには、Skype for Business会議に使用されるドメインのコンマ区切りリストが含まれています。Secure Mailは、以下のURLプレフィックスを持つ会議をすでに処理します。

- `https://join`
- `https://meet`
- `https://lync`

このポリシーを使用すると、`https://*domain*` の形式で他のSkype for Businessドメインを追加できます。ドメインは英数字の文字列であり、特殊文字を含めることはできません。先頭の`https://` や末尾のドットは入力しないでください。

例

ポリシー値が `customDomain1,customDomain2` の場合、Skype for BusinessでサポートされるURLプレフィックスは次のとおりです。 `https://customDomain1` `http://customDomain1`
`https://customDomain2` `http://customDomain2`

デフォルト値は空です。

カレンダーのエクスポート

このポリシーにより、Secure Mailの予定をデバイスまたは個人のカレンダーにエクスポートできます。個人のカレンダーで予定を表示できます。Secure Mailを使用して予定を編集できます。デフォルト値は**会議時間**です。

個人のカレンダーに表示される予定のフィールドには、次のMDXポリシー値を使用できます。

- なし (エクスポートしない)
- 会議時間
- 会議時間、場所
- 会議時間、件名、場所
- 会議時間、空き時間、出席者、件名、場所、メモ

Office 365のOAuthサポート

O365に最新の認証を使用

このポリシーがオンの場合、Secure MailはOffice 365でアカウントを設定する際に認証にOAuthプロトコルを使用します。オフの場合、Secure Mailは基本認証を使用します。デフォルトはオフです。

信頼されたExchange Onlineホスト名

アカウント設定時に認証にOAuthメカニズムを使用する、信頼されたExchange Onlineホスト名のリストを定義します。この値は、`server.company.com`, `server.company.co.uk` のようなコンマ区切

りの形式です。リストが空の場合、Secure Mailはアカウント設定に基本認証を使用します。デフォルト値はoutlook.office365.comです。

信頼されたAD FSホスト名

Office 365 OAuth認証中にパスワードが自動入力されるWebページ用の、信頼されたAD FSホスト名のリストを定義します。この値は、`sts.companyname.com`、`sts.company.co.uk` のようなコンマ区切りの形式です。リストが空の場合、Secure Mailはパスワードを自動入力しません。Secure Mailは、Office 365認証中に検出されたWebページのホスト名とリストされたホスト名を照合し、そのページがHTTPSプロトコルを使用しているかどうかを確認します。

例えば、sts.company.comがリストされたホスト名であり、ユーザーが `https://sts.company.com` に移動した場合、そのページにパスワードフィールドがあれば、Secure Mailはパスワードを自動入力します。デフォルト値は `login.microsoftonline.com` です。

最新の認証用のカスタムユーザーエージェント

このポリシーを使用すると、最新の認証のデフォルトのユーザーエージェント文字列を変更できます。設定されている場合、このユーザーエージェント文字列はMicrosoft AD FSでの認証に使用されます。このポリシーを設定しない場合、最新の認証中にデフォルトのSecure Mailユーザーエージェントが使用されます。

Slack連携

Slackを有効にする

Slack連携をブロックまたは許可します。「オン」の場合、Secure MailインターフェイスにはSlack機能が含まれます。「オフ」の場合、Secure MailインターフェイスにはSlack機能は含まれません。

Slackワークスペース名

会社のSlackワークスペース名。名前を指定すると、Secure Mailはサインオン時にワークスペース名を事前入力します。名前を指定しない場合、ユーザーはワークスペース名 (name.slack.com) を入力する必要があります。

iOS向けモバイル生産性アプリのMDXポリシー

この記事では、iOSアプリのMDXポリシーについて説明します。ポリシー設定はCitrix Endpoint Managementコンソールで変更します。詳細については、「[アプリの追加](#)」を参照してください。

次のリストには、Secure Webに固有のMDXポリシーは含まれていません。Secure Webに表示されるポリシーの詳細については、「[Secure Webポリシー](#)」を参照してください。

認証

デバイスパスコード

オンの場合、デバイスの起動時、または一定期間の非アクティブ状態からの再開時に、デバイスのロックを解除するためにPINまたはパスコードが必要です。Appleファイル暗号化を使用してアプリデータを暗号化するには、デバイスパスコードが必要です。デバイス上のすべてのアプリのデータが暗号化されます。デフォルト値は**オフ**です。

アプリパスコード

オンの場合、アプリの起動時、または一定期間の非アクティブ状態からの再開時に、アプリのロックを解除するためにPINまたはパスコードが必要です。デフォルト値は**オン**です。

すべてのアプリの非アクティブタイマーを構成するには、**設定タブのクライアントプロパティで INACTIVITY_TIMER**の値を分単位で設定します。デフォルトの非アクティブタイマー値は**60分**です。非アクティブタイマーを無効にして、アプリの起動時にのみPINまたはパスコードのプロンプトが表示されるようにするには、値をゼロに設定します。

注：

暗号化キーポリシーで**オフラインを保護**を選択した場合、このポリシーは自動的に有効になります。

最大オフライン期間（時間）

アプリがCitrix Endpoint Managementからアプリの資格を再確認し、ポリシーを更新することなく実行できる最大期間を定義します。有効期限が切れると、必要に応じてサーバーへのログオンがトリガーされる場合があります。デフォルト値は**168時間（7日間）**です。最小期間は**1時間**です。

代替シトリックス ゲートウェイ

注：

Endpoint Management コンソールでのこのポリシー名は、**代替NetScaler® Gateway**です。

このアプリでの認証およびマイクロVPNセッションに使用する必要がある、特定の代替Citrix Gatewayのアドレス。このポリシーはオプションです。オンラインセッション必須ポリシーと併

用すると、アプリは特定のゲートウェイに再認証するよう強制されます。このようなゲートウェイは通常、異なる（より高い保証の）認証要件とトラフィック管理ポリシーを持っています。空のままにすると、サーバーのデフォルトゲートウェイが常に使用されます。デフォルト値は空です。

デバイスセキュリティ

ジェイルブレイクまたはルート化されたデバイスをブロック

オンの場合、デバイスがジェイルブレイクまたはルート化されているとアプリはロックされます。オフの場合、デバイスがジェイルブレイクまたはルート化されていてもアプリは実行できます。デフォルト値はオンです。

ネットワーク要件

Wi-Fiを必須にする

オンの場合、デバイスがWi-Fiネットワークに接続されていないとアプリはロックされます。オフの場合、デバイスが4G/3G、LAN、Wi-Fi接続などのアクティブな接続を持っている場合、アプリは実行できます。デフォルト値はオフです。

許可されたWi-Fiネットワーク

Wi-Fiネットワークのコンマ区切りリスト。ネットワーク名に英数字以外の文字（コンマを含む）が含まれる場合、名前は二重引用符で囲む必要があります。アプリは、リストされているネットワークのいずれかに接続されている場合にのみ実行されます。空白の場合、すべてのネットワークが許可されます。この値は、セルラーネットワークへの接続には影響しません。デフォルト値は空白です。

その他のアクセス

必須アップグレードを無効にする

ユーザーがApp Storeでアプリの最新バージョンにアップグレードする必要性を無効にします。デフォルト値はオンです。

アプリ更新猶予期間（時間）

システムがアプリの更新が利用可能であることを検出した後も、アプリが引き続き使用できる猶予期間を定義します。デフォルト値は**168時間（7日間）**です。

注記:

ゼロの値を使用しないことをお勧めします。ゼロの値は、更新がダウンロードおよびインストールされるまで（ユーザーへの警告なしに）実行中のアプリが使用されるのを直ちに防ぎます。この値を使用すると、ユーザーが必須の更新に準拠するためにアプリを終了せざるを得なくなる（作業が失われる可能性がある）状況につながる可能性があります。

ロック時にアプリデータを消去

アプリがロックされたときにデータを消去し、アプリをリセットします。**オフ**の場合、アプリがロックされてもアプリデータは消去されません。デフォルト値は**オフ**です。

アプリは、次のいずれかの理由でロックされることがあります。

- ユーザーのアプリエンタイトルメントの喪失
- アプリのサブスクリプションが削除された
- アカウントが削除された
- Secure Hubがアンインストールされた
- アプリ認証の失敗が多すぎる
- ジェイルブレイクされたデバイスが検出された（ポリシー設定による）
- 他の管理操作によってデバイスがロック状態にされた

アクティブポーリング期間（分）

アプリが起動すると、MDX FrameworkはCitrix Endpoint Managementをポーリングして、現在のアプリとデバイスのステータスを判断します。Endpoint Managementを実行しているサーバーに到達可能であると仮定すると、フレームワークはデバイスのロック/消去ステータスとアプリの有効/無効ステータスに関する情報を返します。サーバーに到達可能であるかどうかにかかわらず、アクティブポーリング期間の間隔に基づいて後続のポーリングがスケジュールされます。期間が終了すると、新しいポーリングが再度試行されます。デフォルト値は**60分**（1時間）です。

重要:

高リスクのアプリの場合にのみこの値を低く設定してください。そうしないと、パフォーマンスに影響が出る可能性があります。

暗号化

暗号化の種類

MDXとデバイスプラットフォームのどちらがデータの暗号化を処理するかを選択できます。**MDX暗号化**を選択した場合、MDXがデータを暗号化します。**コンプライアンス強制によるプラットフォーム暗号化**を選択した場合、デバイスプラットフォームがデータを暗号化します。デフォルト値は**MDX暗号化**です。

非準拠デバイスの動作

デバイスが暗号化の最小コンプライアンス要件に準拠していない場合に実行するアクションを選択できます。アプリを通常どおり実行するには、**アプリを許可**を選択します。警告が表示された後にアプリを実行するには、**警告後にアプリを許可**を選択します。アプリの実行をブロックするには、**ブロック**を選択します。デフォルト値は**警告後にアプリを許可**です。

MDX暗号化を有効にする

オフの場合、デバイスに保存されているデータは暗号化されません。オンの場合、デバイスに保存されているデータは暗号化されます。デフォルト値は**オン**です。

注意：

アプリを展開した後にこのポリシーを変更すると、ユーザーはアプリを再インストールする必要があります。

データベース暗号化の除外

自動的に暗号化されないデータベースの除外リスト。特定のデータベースの暗号化を防止するには、正規表現のコンマ区切りリストにエントリを追加します。データベースのパス名が正規表現のいずれかに一致する場合、そのデータベースは暗号化から除外されます。除外パターンはPosix 1003.2拡張正規表現構文をサポートしています。パターンマッチングでは大文字と小文字は区別されません。

例

`\\.db$,\\.sqlite$` は、`.db` または `.sqlite` のいずれかで終わるデータベースパス名をすべて除外します。

`\\Database\\unencrypteddb\\.db` は、Databaseサブフォルダー内のデータベース `unencrypteddb.db` に一致します。

`\\Database\\` は、パスに `/Database/` を含むすべてのデータベースに一致します。

デフォルト値は空です。

ファイル暗号化の除外

自動的に暗号化されないファイルの除外リストです。特定のファイルの暗号化を防止するには、このコンマ区切りの正規表現リストにエントリを追加します。ファイルパス名が正規表現のいずれかに一致する場合、そのファイルは暗号化から除外されます。除外パターンは Posix 1003.2 拡張正規表現構文をサポートしています。パターンマッチングでは大文字と小文字は区別されません。

例

`\\.log$,\\.dat$` は、`.log` または `.dat` で終わるすべてのファイルパス名を除外します。

`\\Documents\\Unencrypteddoc\\.txt` は、Documents サブフォルダー内のファイル `unencrypteddoc.txt` のコンテンツに一致します。

`\\Documents\\UnencryptedDocs\\.*\\.txt` は、サブパス `/Documents/UnencryptedDocs/` の下の「.txt」ファイルに一致します。

デフォルト値は空です。

アプリの操作

切り取りとコピー

このアプリのクリップボードの切り取りおよびコピー操作をブロック、許可、または制限します。制限されている場合、コピーされたクリップボードデータは、MDX アプリのみが利用できるプライベートクリップボードに配置されます。デフォルト値は**制限**です。

貼り付け

このアプリのクリップボードの貼り付け操作をブロック、許可、または制限します。**制限**されている場合、貼り付けられたクリップボードデータは、MDX アプリのみが利用できるプライベートクリップボードから取得されます。デフォルト値は**無制限**です。

ドキュメント交換 (Open In)

このアプリのドキュメント交換操作をブロック、許可、または制限します。**制限**されている場合、ドキュメントは他のMDXアプリとのみ交換できます。

無制限の場合、ユーザーがラップされていないアプリでドキュメントを開けるように、Enable encryptionポリシーを**オン**に設定します。受信アプリがラップされていないか、暗号化が無効に

なっている場合、Citrix Endpoint Managementはドキュメントを復号化します。デフォルト値は**制限**です。

制限付きOpen-In例外リスト

Document exchange (Open In)ポリシーが**制限**されている場合、MDXアプリは、管理対象外のアプリIDのこのコンマ区切りリストとドキュメントを共有できます。これは、Document exchange (Open In)ポリシーが**制限**されており、Enable encryptionが**オン**の場合でも同様です。デフォルトの例外リストでは、Office 365アプリが許可されます。

com.microsoft.Office.Word,com.microsoft.Office.Excel,com.microsoft.Office.Powerpoint,
com.microsoft.onenote,com.microsoft.onenoteiPad,com.microsoft.Office.Outlook

このポリシーでサポートされているのはOffice 365アプリのみです。

注意：

このポリシーのセキュリティ上の影響を考慮してください。例外リストにより、管理対象外のアプリとMDX環境の間でコンテンツが移動できるようになります。

接続セキュリティレベル

接続に使用されるTLS/SSLの最小バージョンを決定します。**TLS**の場合、接続はすべてのTLSプロトコルをサポートします。**SSLv3およびTLS**の場合、接続はSSL 3.0およびTLSをサポートします。デフォルト値は**TLS**です。

受信ドキュメント交換（Open In）

このアプリの受信ドキュメント交換操作をブロック、制限、または許可します。**制限**されている場合、ドキュメントは他のMDXアプリとのみ交換できます。デフォルト値は**無制限**です。

ブロックまたは**制限**されている場合、Inbound document exchange whitelistポリシーを使用して、このアプリにドキュメントを送信できるアプリを指定できます。

オプション：**無制限**、**ブロック**、または**制限**

アプリのURLスキーム

iOSアプリは、特定のスキーム（「`http://`」など）を処理するように登録されている他のアプリにURLリクエストをディスパッチできます。この機能により、アプリは別のアプリにヘルプリクエストを渡すメカニズムを提供します。このポリシーは、このアプリで処理するために渡される

スキーム（つまり、インバウンドURL）をフィルタリングする役割を果たします。デフォルト値は空であり、登録されているすべてのアプリURLスキームがブロックされることを意味します。

ポリシーは、各パターンにプラス「+」またはマイナス「-」が先行する、コンマ区切りのパターンリストとしてフォーマットする必要があります。インバウンドURLは、一致が見つかるまで、リストされた順序でパターンと比較されます。一致すると、プレフィックスによって実行されるアクションが決定されます。

- マイナス「-」プレフィックスは、URLがこのアプリに渡されるのをブロックします。
- プラス「+」プレフィックスは、URLが処理のためにアプリに渡されることを許可します。
- パターンに「+」も「-」も指定されていない場合、「+」（許可）が想定されます。
- インバウンドURLがリスト内のどのパターンにも一致しない場合、そのURLはブロックされません。

次の表に、アプリURLスキームの例を示します。

スキーム	URLスキームを必要とするアプリ	目的
<code>ctxmobilebrowser</code>	セキュアウェブ-	Secure Webが他のアプリからのHTTP: URLを処理することを許可します。 -
<code>ctxmobilebrowsers</code>	セキュアウェブ-	Secure Webが他のアプリからのHTTPS: URLを処理することを許可します。
<code>ctxmail</code>	セキュアメール-	Secure Mailが他のアプリからの <code>mailto:</code> URLを処理することを許可します。
COL-G2M	GoToMeeting-	ラップされたGoToMeetingアプリが会議リクエストを処理することを許可します。
<code>ctxsalesforce</code>	シトリックス for セールスフォース-	Citrix for SalesforceがSalesforceリクエストを処理することを許可します。
<code>wbx</code>	WebEx	ラップされたWebExアプリが会議リクエストを処理することを許可します。

アプリ連携 (送信URL)

URLフィルタリングから除外されるドメイン

このポリシーは、「許可されたURL」フィルタリングから送信URLを除外します。「許可されたURL」フィルタリングから除外する完全修飾ドメイン名 (FQDN) またはDNSサフィックスのコンマ区切りリストを追加します。このポリシーが空の場合 (デフォルト)、定義された「許可されたURL」フィルタリングプロセスはURLです。このポリシーにエントリが含まれている場合、リスト内の少なくとも1つの項目に一致するホストフィールドを持つURL (DNSサフィックスの一致を介して) は、変更されずにiOSに送信されます。この通信は、「許可されたURL」フィルタリングロジックをバイパスします。デフォルト値は空です。

許可されたURL

iOSアプリは、特定のスキーム ("http://" など) を処理するように登録されている他のアプリケーションにURLリクエストをディスパッチできます。この機能により、アプリはヘルプのリクエストを別のアプリに渡すメカニズムが提供されます。このポリシーは、このアプリから他のアプリに処理のために渡されるURL (つまり、送信URL) をフィルタリングする役割を果たします。

ポリシーは、各パターンの前にプラス「+」またはマイナス「-」が付く可能性がある、コンマ区切りのパターンリストとしてフォーマットする必要があります。送信URLは、一致が見つかるまで、リストに記載されている順序でパターンと比較されます。一致すると、プレフィックスによって実行されるアクションが決定されます。マイナス「-」プレフィックスは、URLが別のアプリに渡されるのをブロックします。プラス「+」プレフィックスは、URLが処理のために別のアプリに渡されることを許可します。パターンに「+」も「-」も指定されていない場合、「+」(許可)が想定されます。「=」で区切られた値のペアは、最初の文字列の出現箇所が2番目の文字列に置き換えられる置換を示します。正規表現の「\」プレフィックスを使用して文字列を検索し、URLの先頭に固定することができます。送信URLがリスト内のどのパターンとも一致しない場合、ブロックされます。

デフォルト

+maps.apple.com

+itunes.apple.com

\^http:=ctxmobilebrowser: :

\^https:=ctxmobilebrowsers: :

\^mailto:=ctxmail: :

+\\^citrixreceiver: :

+\\^telprompt::

+\\^tel::

+\\^lmi-g2m::

+\\^maps:ios_addr

+\\^mapitem::

+\\^sms::

+\\^facetime::

+\\^ctxnotes::

+\\^ctxnotesex::

+\\^ctxtasks::

+\\^facetime-audio::

+\\^itms-apps::

+\\^ctx-sf::

+\\^sharefile::

+\\^lync::

+\\^slack::

+\\^msteams::

設定が空白の場合、すべてのURLがブロックされます。ただし、以下を除きます。

- http::
- https::
- +citrixreceiver: +tel::

次の表に、許可されたURLの例を示します。

URL形式	説明
<code>\^mailto:=ctxmail:</code>	すべての <code>mailto:</code> URLはSecure Mailで開きます。
<code>\^http:</code>	すべてのHTTP URLはSecure Webで開きます。
<code>\^https:</code>	すべてのHTTPS URLはSecure Webで開きます。
<code>\^tel:</code>	ユーザーが通話できるようにします。
<code>-//www.dropbox.com</code>	管理対象アプリからディスパッチされたDropbox URLをブロックします。
<code>+\\^COL-G2M:</code>	管理対象アプリがGoToMeetingクライアントアプリを開くことを許可します。
<code>-\\^SMS:</code>	メッセージングチャットクライアントの使用をブロックします。
<code>-\\^wbx:</code>	管理対象アプリがWebExクライアントアプリを開くことをブロックします。
<code>+\\^ctxsalesforce:</code>	Citrix for SalesforceがSalesforceサーバーと通信することを許可します。

許可されたSecure Webドメイン

このポリシーは、URLをSecure Webアプリにリダイレクトする「許可されたURL」ポリシーエントリ（`\^ http:=ctxmobilebrowser:` および `\^https:=ctxmobilebrowsers:`）にのみ影響します。Secure Webアプリにリダイレクトすることを許可する、完全修飾ドメイン名（FQDN）またはDNSサフィックスのコンマ区切りリストを追加します。このポリシーが空の場合（デフォルト）、すべてのドメインがSecure Webアプリにリダイレクトできます。このポリシーにエントリが含まれている場合、リスト内の少なくとも1つの項目に一致するホストフィールドを持つURL（DNSサフィックスの一致による）のみがSecure Webアプリにリダイレクトされます。その他のすべてのURLは、Secure Webアプリをバイパスして、変更されずにiOSに送信されます。デフォルト値は空です。

アプリの制限

重要:

アプリが電話機能にアクセスしたり使用したりするのをブロックするポリシーのセキュリティ上の影響を考慮してください。これらのポリシーが**オフ**の場合、コンテンツは管理対象外のアプリとセキュアな環境の間を移動できます。

カメラをブロック

オンの場合、アプリがカメラハードウェアを直接使用するのを防ぎます。デフォルト値は**オフ**です。

写真ライブラリをブロック

オンの場合、アプリがデバイス上の写真ライブラリにアクセスするのを防ぎます。デフォルト値は**オン**です。

マイク録音をブロック

オンの場合、アプリがマイクハードウェアを直接使用するのを防ぎます。デフォルト値は**オン**です。

音声入力をブロック

オンの場合、アプリが音声入力サービスを直接使用するのを防ぎます。デフォルト値は**オン**です。

位置情報サービスをブロック

オンの場合、アプリが位置情報サービスコンポーネント（GPSまたはネットワーク）を使用するのを防ぎます。Secure Mail のデフォルト値は**オフ**です。

SMS作成をブロック

オンの場合、アプリがSMS/テキストメッセージを送信するために使用するSMS作成機能を使用するのを防ぎます。デフォルト値は**オン**です。

メール作成をブロック

オンの場合、アプリがメールメッセージを送信するために使用するメール作成機能を使用するのを防ぎます。デフォルト値は**オン**です。

iCloudをブロック

オンの場合、アプリが設定やデータの保存および共有にiCloudを使用するのを防ぎます。

注

iCloud データファイルは、ファイルバックアップのブロックポリシーによって制御されます。

既定値は**オン**です。

ルックアップをブロック

オンの場合、アプリがルックアップ機能を使用することを禁止します。この機能は、辞書、iTunes、App Store、映画の上映時間、近くの場所などでハイライトされたテキストを検索します。既定値は**オン**です。

ファイルバックアップをブロック

オンの場合、iCloudまたはiTunesがデータファイルをバックアップすることを禁止します。既定値は**オン**です。

AirPrintをブロック

オンの場合、アプリがAirPrint機能を使用してデータをAirPrint対応プリンターに印刷することを禁止します。既定値は**オン**です。

AirDropをブロック

オンの場合、アプリがAirDropを使用することを禁止します。既定値は**オン**です。

ファイル添付をブロック**注**

このポリシーはiOS 11以降で適用されます。

オンの場合、添付ファイルの処理が無効になります。既定値は**オフ**です。

FacebookおよびTwitter APIをブロック

「**On**」の場合、アプリがiOSのFacebookおよびTwitter APIを使用するのを防ぎます。デフォルト値は「**On**」です。

画面コンテンツを隠す

「On」の場合、ユーザーがアプリを切り替えると、画面が隠されます。このポリシーは、iOSが画面コンテンツを記録したりサムネイルを表示したりするのを防ぎます。デフォルト値は「On」です。

サードパーティ製キーボードをブロックする (iOS 11以降のみ)

「On」の場合、アプリがiOS 8以降でサードパーティ製キーボード拡張機能を使用するのを防ぎます。デフォルト値は「On」です。

アプリログをブロックする

「On」の場合、アプリがモバイル生産性アプリの診断ログ機能を使用することを禁止します。
「Off」の場合、アプリログは記録され、Secure Hubのメールサポート機能を使用して収集される可能性があります。デフォルト値は「Off」です。

ShareFileを有効にする

ユーザーがShareFileを使用してファイルを転送できるようにします。デフォルト値は「On」です。

ファイルから添付を有効にする

ユーザーがiOSファイルアプリから添付ファイルを追加できるようにします。デフォルト値は「On」です。

アプリのネットワークアクセス

ネットワークアクセス

注:

Tunneled - Web SSO は、設定における **Secure Browse** の名称です。動作は同じです。

設定オプションは次のとおりです。

- **ブロック済み:** すべてのネットワークアクセスがブロックされます。アプリで使用されるネットワークAPIは失敗します。以前のガイドラインに従って、このような障害を適切に処理する必要があります。
- **無制限:** すべてのネットワーク呼び出しは直接行われ、トンネル化されません。

- **トンネル化 - Web SSO**: HTTP/HTTPS URLが書き換えられます。このオプションでは、HTTPおよびHTTPSトラフィックのトンネル化のみが可能です。**トンネル化 - Web SSO**の大きな利点は、HTTPおよびHTTPSトラフィックのシングルサインオン (SSO) とPKINIT認証です。Androidでは、このオプションはセットアップのオーバーヘッドが低いため、Webブラウジングタイプの操作に推奨されるオプションです。

トンネル化 - フルVPNまたはトンネル化 - フルVPNおよびWeb SSOポリシーを使用している場合は、トンネル化 - Web SSOポリシーに切り替える必要があります。非推奨のポリシーを使い続けると、メールの同期に失敗します。

注:

トンネル化 - フルVPNを使用しており、Secure Ticket Authority (STA) が構成されている場合、最新の認証画面はロードに失敗します。

Micro VPNセッションが必要

はいの場合、ユーザーはエンタープライズネットワークへの接続とアクティブなセッションを持っている必要があります。いいえの場合、アクティブなセッションは必要ありません。デフォルト値は**以前の設定**を使用です。新しくアップロードされたアプリの場合、デフォルト値はいいえです。この新しいポリシーへのアップグレード前に選択されていた設定は、**以前の設定**を使用以外のオプションが選択されるまで有効です。

Micro VPNセッションの猶予期間 (分)

この値は、オンラインセッション必須ポリシーによってそれ以上アプリを使用できなくなるまでの時間 (オンラインセッションが検証されるまで) を分単位で決定します。デフォルト値は**0** (猶予期間なし) です。このポリシーは、Microsoft Intune/EMSとの統合には適用されません。

証明書ラベル

StoreFront™証明書統合サービスと併用する場合、このラベルは、このアプリに必要な特定の証明書を識別します。ラベルが指定されていない場合、公開鍵インフラストラクチャ (PKI) で使用できる証明書は提供されません。デフォルト値は空 (証明書は使用されません) です。

除外リスト

VPN接続を介さずに直接アクセスされるFQDNまたはDNSサフィックスのコンマ区切りリスト。この値は、Citrix Gatewayがスプリットトンネルリバースモードで構成されている場合の**トンネル化 - Web SSO**モードにのみ適用されます。

アプリログ

デフォルトのログ出力

モバイル生産性アプリの診断ログ機能でデフォルトで使用される出力メディアを決定します。選択肢はファイル、コンソール、またはその両方です。デフォルト値は**ファイル**です。

デフォルトのログレベル

モバイル生産性アプリの診断ログ機能のデフォルトの詳細度を制御します。各レベルには、それより低い値のレベルが含まれます。設定可能なレベルの範囲は次のとおりです。

- 0 - 何もログに記録しない
- 1 - 致命的なエラー
- 2 - エラー
- 3 - 警告
- 4 - 情報メッセージ
- 5 - 詳細な情報メッセージ
- 6～15 - デバッグレベル1～10

デフォルト値はレベル4 (情報メッセージ) です。

最大ログファイル数

モバイル生産性アプリの診断ログ機能がロールオーバーする前に保持するログファイルの数を制限します。最小値は2です。最大値は8です。デフォルト値は2です。

ログファイルの最大サイズ

モバイル生産性アプリの診断ログ機能によって保持されるログファイルのサイズ (MB) を、ロールオーバーする前に制限します。最小値は1 MBです。最大値は5 MBです。デフォルト値は2 MBです。

アプリのジオフェンス

中心点の経度

アプリの動作が制限されるポイント/半径ジオフェンスの中心点の経度 (X座標)。設定されたジオフェンスの外で操作された場合、アプリはロックされたままになります。

値は符号付き度数形式 (DDD.dddd) で表現する必要があります。例: 「-31.9635」。西経にはマイナス記号を付ける必要があります。デフォルト値は**0**です。

中心点の緯度

アプリの動作が制限されるポイント/半径ジオフェンスの中心点の緯度（Y座標）。設定されたジオフェンスの外で操作された場合、アプリはロックされたままになります。

値は符号付き度数形式（DDD.dddd）で表現する必要があります。例：「43.06581」。南緯にはマイナス記号を付ける必要があります。デフォルト値は**0**です。

半径

アプリの動作が制限されるジオフェンスの半径。設定されたジオフェンスの外で操作された場合、アプリはロックされたままになります。

値はメートルで表現する必要があります。ゼロに設定すると、ジオフェンスは無効になります。

「位置情報サービスをブロック」ポリシーが有効になっている場合、ジオフェンスは正常に機能しません。デフォルトは**0**（無効）です。

Google Analyticsを有効にする

Onの場合、Citrixは製品品質向上のために匿名データを収集します。**Off**の場合、データは収集されません。デフォルト値は**On**です。

分析

Google Analytics の詳細レベル

Citrix は製品品質向上のために分析データを収集します。**匿名**を選択すると、企業を特定できる情報を含めることからユーザーが除外されます。デフォルトは「完全」です。

レポート

Citrix レポート

オンの場合、Citrix は問題のトラブルシューティングに役立つクラッシュレポートと診断を収集します。**オフ**の場合、Citrix はデータを収集しません。

注

Citrix は、この機能を機能フラグで制御する場合もあります。この機能が機能するには、機能フラグとこのポリシーの両方が有効になっている必要があります。

デフォルト値は**オフ**です。

アップロードトークン

Citrix Insight Services (CIS) アカウントからアップロードトークンを取得できます。このオプションのトークンを指定すると、CIS はデバイスからアップロードされたクラッシュレポートと診断へのアクセスを許可します。Citrix は同じ情報にアクセスできます。デフォルト値は空です。

Wi-Fi 経由でのみレポートを送信

オンの場合、Citrix は Wi-Fi ネットワークに接続されている場合にのみクラッシュレポートと診断を送信します。デフォルト値はオンです。

レポートファイルキャッシュの最大値

キャッシュをクリアする前に保持されるクラッシュレポートと診断バンドルのサイズを制限します。最小は 1 MB です。最大は 5 MB です。デフォルト値は 2 MB です。

アプリの操作

明示的なログオフ通知

「無効」の場合、ユーザーのログオフ中にアプリはアクティブ化されません。「共有デバイスのみ」の場合、デバイスが共有デバイスとして構成されている場合にのみ、ユーザーのログオフ中にアプリがアクティブ化されます。Secure Mail のデフォルトは「共有デバイスのみ」です。

アプリ設定

セキュアメール Exchange サーバー

Exchange Server の完全修飾ドメイン名 (FQDN)、または iOS のみの場合、IBM Notes Traveler サーバーの完全修飾ドメイン名 (FQDN)。デフォルト値は空です。このフィールドにドメイン名を入力すると、ユーザーは編集できません。フィールドを空のままにすると、ユーザーは独自のサーバー情報を提供します。

注意

既存のアプリに対してこのポリシーを変更した場合、ユーザーはポリシーの変更を適用するためにアプリを削除して再インストールする必要があります。

Secure Mail ユーザー ドメイン

Exchange ユーザー、または iOS のみの場合、Notes ユーザーのデフォルトの Active Directory ドメイン名。デフォルト値は空です。

バックグラウンドネットワークサービス

バックグラウンドネットワークアクセスが許可されているサービスアドレスの FQDN とポート。この値は、社内ネットワーク内または Secure Mail が接続する別のネットワーク内にある Exchange Server または ActiveSync サーバーである可能性があります（例: mail.example.com:443）。

このポリシーを構成する場合は、ネットワークアクセスポリシーを「**内部ネットワークにトンネル接続**」に設定します。このポリシーは、ネットワークアクセスポリシーを構成したときに有効になります。このポリシーは、Exchange Server が社内ネットワーク内にあり、Citrix Gateway (旧 NetScaler Gateway) を使用して内部 Exchange Server への接続をプロキシしたい場合に使用します。

デフォルト値は空で、バックグラウンドネットワークサービスが利用できないことを意味します。

バックグラウンドサービスチケットの有効期限

バックグラウンドネットワークサービスチケットが有効である期間。有効期限が切れると、チケットを更新するためにエンタープライズログオンが必要になります。デフォルト値は「**168時間**」（7日間）です。

バックグラウンドネットワークサービスゲートウェイ

バックグラウンドネットワークサービスに使用する代替ゲートウェイアドレス。形式は `fqdn:port` です。この値は、Secure Mail が内部 Exchange Server に接続するために使用する Citrix Gateway の FQDN とポート番号です。Citrix Gateway の構成ユーティリティで、Secure Ticket Authority (STA) を構成し、ポリシーを仮想サーバーにバインドする必要があります。デフォルト値は空で、代替ゲートウェイが存在しないことを意味します。

このポリシーを構成する場合は、ネットワークアクセスポリシーを **内部ネットワークへのトンネル接続** に設定します。このポリシーは、ネットワークアクセスポリシーを構成したときに有効になります。このポリシーは、Exchange Server が内部ネットワーク内にあり、Citrix Gateway を使用して内部 Exchange Server への接続をプロキシしたい場合に使用します。

連絡先のエクスポート

重要:

ユーザーが Exchange Server に直接アクセスできる場合（つまり、Citrix Gateway 経由ではない場合）は、この機能を有効にしないでください。そうしないと、デバイスと Exchange の両方に重複する連絡先が作成されます。

オフ の場合、Secure Mail の連絡先がデバイスに一方向で同期されること、および Secure Mail の連絡先が（vCard として）共有されることを防ぎます。デフォルト値は **オフ** です。

エクスポートする連絡先フィールド

アドレス帳にエクスポートする連絡先フィールドを制御します。**すべて** の場合、すべての連絡先フィールドがエクスポートされます。**名前と電話番号** の場合、名前と電話番号に関連するすべての連絡先フィールドがエクスポートされます。**名前、電話番号、メールアドレス** の場合、名前、電話番号、メールアドレスに関連するすべての連絡先フィールドがエクスポートされます。

デフォルト値は **すべて** です。

すべてのSSL証明書を承認する

オン の場合、Secure Mail はすべての SSL 証明書（有効かどうかにかかわらず）を受け入れ、アクセスを許可します。**オフ** の場合、Secure Mail は証明書エラーが発生したときにアクセスをブロックし、警告を表示します。

デフォルト値は **オフ** です。

ロック画面通知の制御

ロックされたデバイス画面にメールとカレンダーの通知が表示されるかどうかを制御します。**許可** の場合、通知に含まれるすべての情報が表示されます。**ブロック** の場合、通知は表示されません。**メール送信者またはイベントのタイトル** の場合、メール送信者の名前またはカレンダーイベントのタイトルのみが表示されます。**件数のみ** の場合、メールと会議の招待の件数とカレンダーリマインダーの時刻が表示されます。デフォルト値は **許可** です。

デフォルトのメール通知

オン の場合、Secure Mail はメールのロック画面通知を表示します。デフォルト値は**オン**です。

デフォルトの同期間隔

Secure Mail のデフォルトの同期間隔を指定します。Secure Mail ユーザーはデフォルトを変更できます。**Exchange ActiveSync メールボックスポリシー設定の最大メール保持期間フィルター** は、このポリシーよりも優先されます。デフォルトの同期間隔が最大メール保持期間フィルターよりも大きい場合、代わりに**最大メール保持期間フィルター**設定が使用されます。

Secure Mail は、**Active Sync 最大メール保持期間フィルター**設定よりも小さい同期間隔の値のみを表示します。

デフォルト値は**3 日**です。

メール検索制限

メールサーバー検索に含まれる日数を制限することで、モバイルデバイスからアクセスできるメール履歴の量を制限します。デフォルト値は**無制限**です。

モバイルデバイスに同期されるメールの量を制限するには、最大クライアント同期期間ポリシーを構成します。

最大同期間隔

同期間隔を制限することで、モバイルデバイスにローカルに保存されるメールの量を制御します。デフォルト値は**すべて**です。デバイスがメールサーバーで検索できる期間を制限するには、メールサーバー検索制限ポリシーを構成します。

週番号を有効にする

オンの場合、カレンダービューに週番号が含まれます。デフォルト値は**オフ**です。

Wi-Fi 経由での添付ファイルのダウンロードを有効にする

オンの場合、Secure Mail の添付ファイルのダウンロードオプションが有効になり、ユーザーはデフォルトで許可された内部 Wi-Fi ネットワーク経由で添付ファイルをダウンロードできます。**オフ**の場合、Secure Mail の添付ファイルのダウンロードオプションが無効になり、ユーザーはデフォルトで Wi-Fi 経由で添付ファイルをダウンロードできません。

既定値は**オフ**です。

オフラインドキュメントを許可する

ユーザーがデバイスにオフラインドキュメントを保存できるかどうか、および保存期間を指定します。既定値は**無制限**です。

情報権限管理

オンの場合、Secure MailはExchange情報権限管理 (IRM) 機能をサポートします。既定値は**オフ**です。

メール分類

オンの場合、Secure MailはSEC (セキュリティ) およびDLM (配布制限マーカー) のメール分類マーキングをサポートします。分類マーキングは、メールヘッダーに「X-Protective-Marking」値として表示されます。関連するメール分類ポリシーを必ず構成してください。

既定値は**オフ**です。

メール分類マーキング

ユーザーが利用できる分類マーキングを指定します。リストが空の場合、Secure Mailには保護マーキングのリストは含まれません。マーキングリストには、セミコロンで区切られた値のペアが含まれます。各ペアには、Secure Mailに表示される値と、Secure Mailのメール件名およびヘッダーに追加されるテキストであるマーキング値が含まれます。たとえば、マーキングペア「UNOFFICIAL,SEC=UNOFFICIAL;」では、リスト値は「UNOFFICIAL」で、マーキング値は「SEC=UNOFFICIAL」です。

メール分類名前空間

使用される分類標準によってメールヘッダーで必要とされる分類名前空間を指定します。たとえば、名前空間「gov.au」はヘッダーに「NS=gov.au」と表示されます。

既定値は空です。

メール分類バージョン

使用される分類標準によってメールヘッダーで必要とされる分類バージョンを指定します。たとえば、バージョン「2012.3」はヘッダーに「VER=2012.3」と表示されます。

デフォルト値は空です。

デフォルトのメール分類

ユーザーがマーキングを選択しなかった場合に、Secure Mailがメールに適用する保護マーキングを指定します。この値は、メール分類マーキングポリシーのリストに含まれている必要があります。

デフォルト値は**UNOFFICIAL**です。

メール下書きの自動保存を有効にする

Onの場合、Secure Mailはメッセージを下書きフォルダーに自動保存することをサポートします。

デフォルト値は**On**です。

初回認証メカニズム

このポリシーは、初回使用時のプロビジョニング画面で「アドレス」フィールドに入力するために、MDXによって提供されるメールサーバーアドレスとユーザーのメールアドレスのどちらを使用する必要があるかを示します。

デフォルト値は**「メールサーバーアドレス」**です。

初回認証資格情報

このポリシーは、初回使用時のプロビジョニング画面に入力するユーザー名として選択する必要がある値を定義します。

デフォルト値は**「登録ユーザー名」**です。

ユーザー名の自動入力の有効化

有効にすると、アカウントプロビジョニングユーザーインターフェイスにユーザー名が自動的に入力されます。デフォルト値は**ON**です。

iOSデータ保護を有効にする

注：

このポリシーは、オーストラリア信号局（ASD）のコンピューターセキュリティ要件を満たす必要がある企業向けです。

ファイル操作時にiOSデータ保護を有効にします。**オン**の場合、アプリサンドボックスでファイルを作成および開く際のファイル保護レベルを指定します。デフォルト値は**オフ**です。

プッシュ通知EWSホスト名

メール用のExchange Web Services（EWS）をホストするサーバー。値はEWSのURLとポート番号である必要があります。デフォルト値は空です。

プッシュ通知

メールボックスのアクティビティに関するAPNsベースの通知を有効にします。**オン**の場合、Secure Mailはプッシュ通知をサポートします。

デフォルト値は**オフ**です。

プッシュ通知リージョン

Secure MailユーザーのAPNsホストが配置されているリージョン。オプションは**南北アメリカ**、**EMEA**、**APAC**です。デフォルト値は**南北アメリカ**です。

S/MIME公開証明書ソース

S/MIME証明書のソースを指定します。**メール**の場合、ユーザー証明書をユーザーにメールで送信する必要があります。ユーザーはSecure Mailでメールを開き、添付された証明書をインポートします。

共有ボールドの場合、サポートされているデジタルIDプロバイダーがSecure App共有ボールドに証明書を提供します。サードパーティプロバイダーとの統合には、関連するアプリをユーザーに公開する必要があります。ユーザーエクスペリエンスの詳細については、「Secure Mailの初回起動時にS/MIMEを有効にする」ポリシーの説明を参照してください。

デフォルト値はメールです。

最初のSecure Mail起動時にS/MIMEを有効にする

S/MIME証明書ソースポリシーが共有ボールドの場合、Secure Mailが最初のSecure Mail起動時にS/MIMEを有効にするかどうかを決定します。オンの場合、共有ボールドにユーザーの証明書があれば、Secure MailはS/MIMEを有効にします。共有ボールドに証明書がない場合、ユーザーは証明書のインポートを求められます。どちらのシナリオでも、ユーザーはSecure Mailでアカウントを作成する前に、サポートされているデジタルIDプロバイダーアプリから証明書を設定する必要があります。

オフの場合、Secure MailはS/MIMEを有効にせず、ユーザーはSecure Mailの設定で有効にできません。デフォルト値はオフです。

カレンダーのWebおよびオーディオオプション

- **GoToMeetingとユーザー入力:** ユーザーは設定したい会議の種類を選択できます。オプションには、GoToMeetingページを開く**GoToMeeting**と、ユーザーが会議情報を手動で入力できる**その他の会議**が含まれます。
- **ユーザー入力のみ:** ユーザーは直接「その他の会議」ページに移動し、会議情報を手動で入力できます。

S/MIME公開証明書ソース

S/MIME公開証明書のソースを指定します。**Exchange**の場合、Secure MailはExchange Serverから証明書を取得します。**LDAP**の場合、Secure MailはLDAPサーバーから証明書を取得します。デフォルト値は**Exchange**です。

LDAPサーバーアドレス

ポート番号を含むLDAPサーバーアドレス。デフォルト値は空です。

LDAPベースDN

LDAPベース識別名。デフォルト値は空です。

LDAPに匿名でアクセス

このポリシーがオンの場合、Secure Mailは事前の認証なしにLDAPを検索できます。デフォルトはオフです。

許可されたメール ドメイン

カンマ区切りの形式（例：server.company.com,server.company.co.uk）で許可されるメール ドメインのリストを定義します。デフォルト値は空で、Secure Mail がメール ドメインをフィルタリングせず、すべてのメール ドメインをサポートすることを意味します。Secure Mail は、リストされたドメインをメールアドレスのドメイン名と照合します。たとえば、server.company.com がリストされたドメイン名で、メールアドレスが user@internal.server.company.com の場合、Secure Mail はそのメールアドレスをサポートします。

認証失敗時のユーザー名移行を試行

認証のためにExchangeユーザー名をUPNに移行しようとします。デフォルト値はオフです。

フィッシングメールアドレスを報告

設定されている場合、疑わしいフィッシングメールを指定されたメールアドレス、またはカンマ区切りのメールアドレスのリストに報告できます。デフォルト値は空です。このポリシーを設定しない場合、フィッシングメッセージを報告することはできません。

フィッシング報告メカニズム

このポリシーは、疑わしいフィッシングメールを報告するために使用されるメカニズムを示します。

- **添付ファイルとして報告:** フィッシングメールを添付ファイルとして報告します。添付ファイルは、「フィッシングメールアドレスを報告」ポリシーで設定されたメールアドレス、またはカンマ区切りのメールアドレスのリストに送信されます。
- **転送として報告:** フィッシングメールを転送として報告します。メールは、「フィッシングメールアドレスを報告」ポリシーで設定されたメールアドレス、またはカンマ区切りのメールアドレスのリストに転送されます。

注:

このポリシーは、Microsoft Exchange Serverでのみ利用可能です。

デフォルトは添付ファイルとして報告です。

Skype for Business会議ドメイン

このポリシーには、Skype for Business会議に使用されるドメインのカンマ区切りリストが含まれています。

Secure Mailは、以下のURLプレフィックスを持つ会議をすでに処理します。

- `https://join`
- `https://meet`
- `https://lync`

このポリシーを使用すると、他のSkype for Businessドメインを `https://*domain*` の形式で追加できます。ドメインは英数字の文字列であり、特殊文字を含めることはできません。先頭の `https://` や後続のドットは入力しないでください。

例:

ポリシー値が`customDomain1,customDomain2`の場合、Skype for BusinessでサポートされるURLプレフィックスは次のとおりです。

- `https://customDomain1`
- `http://customDomain1`
- `https://customDomain2`
- `http://customDomain2`

デフォルト値は空です。

カレンダーのエクスポート

このポリシーにより、Secure Mailのカレンダーイベントをデバイスまたは個人のカレンダーにエクスポートできます。個人のカレンダーでイベントを表示できます。Secure Mailを使用してイベントを編集できます。デフォルト値は**会議時間**です。

個人のカレンダーに表示されるカレンダーイベントフィールドには、次のMDXポリシー値が利用可能です。

- なし (エクスポートしない)
- 会議時間
- 会議時間、場所
- 会議時間、件名、場所

- 会議時間、件名、場所、メモ

発信者識別

「オン」の場合、Secure Mailは、発信者識別のために、保存されている連絡先の名前と電話番号をiOSに提供します。このデータは、保存されているSecure Mailの連絡先リストからの着信を識別し、詳細を表示するためにのみ使用されます。デフォルト値は「オン」です。

Office 365のOAuthサポート

Office 365認証メカニズム

このポリシーは、Office 365でアカウントを設定する際に認証に使用されるOAuthメカニズムを示します。

- 「**OAuthを使用しない**」: OAuthは使用されず、Secure Mailはアカウント設定に基本認証を使用します。
- 「**ユーザー名とパスワードでOAuthを使用する**」: ユーザーは、OAuthフローのためにユーザー名とパスワード、およびオプションでMFAコードを提供する必要があります。
- 「**クライアント証明書でOAuthを使用する**」: ユーザーはクライアント証明書を使用してOAuthフローを認証します。

デフォルトは「**OAuthを使用しない**」です。

信頼できるExchange Onlineホスト名

アカウント設定時に認証にOAuthメカニズムを使用する、信頼できるExchange Onlineホスト名のリストを定義します。この値は、server.company.com, server.company.co.uk のようなコンマ区切りの形式です。リストが空の場合、Secure Mailはアカウント設定に基本認証を使用します。デフォルト値は「**outlook.office365.com**」です。

信頼されたAD FSホスト名

Office 365 OAuth認証中にパスワードが自動入力されるウェブページについて、信頼されたAD FSホスト名のリストを定義します。この値は、sts.compname.com, sts.company.co.uk のように、コンマ区切りの形式です。リストが空の場合、Secure Mailはパスワードを自動入力しません。Secure Mailは、Office 365認証中にアクセスしたウェブページのホスト名とリストされたホスト名を照合し、そのページがHTTPSプロトコルを使用しているかを確認します。例えば、sts.company.comがリストされたホスト名であり、ユーザーが `https://sts.company.com` に移動した場合、そのページにパスワードフィールドがあれば、Secure Mailはパスワードを自動入力します。デフォルト値は **login.microsoftonline.com** です。

メールリダイレクト

メールリダイレクト

メールの作成をブロックまたは制限します。Secure Mailはメール作成をSecure Mailにリダイレクトします。アカウントが設定されている場合、ネイティブメールはメール作成をネイティブメールにリダイレクトします。デフォルト値は **Secure Mail** です。

Slack連携

Slackを有効にする

Slack連携をブロックまたは許可します。**ON** の場合、Secure MailインターフェースにSlack機能が含まれます。**OFF** の場合、Secure MailインターフェースにSlack機能は含まれません。デフォルト値は **OFF** です。

Slackワークスペース名

会社のSlackワークスペース名。名前を指定すると、Secure Mailはサインオン時にワークスペース名を事前入力します。名前を指定しない場合、ユーザーはワークスペース名 (name.slack.com) を入力する必要があります。デフォルト値は空です。

プラットフォーム別の機能

以下の表は、Citrix モバイル生産性向上アプリの機能をまとめたものです。X は、そのプラットフォームで機能が利用可能であることを示します。QuickEdit の機能については、[Citrix QuickEdit](#) を参照してください。

シトリックス セキュアハブ™

機能	IOS	アンドロイド
サインオンして認証する	X	X
ポリシーの順守を監視する	X	X
アプリとデスクトップにアクセスする	X	X
HDX™アプリとデスクトップ	X	X
問題ログを作成して送信する	X	X
ログにスクリーンショットを添付する	X	X
アプリ内からヘルプデスクに連絡する	X	X
アプリ内からCitrix®サポートに連絡する	X	X
クラッシュの収集と分析	X	X
オフライン認証	X	X
Citrix Secure Mail™ でログを送信	X	X
Google アナリティクス	X	X

機能	IOS	アンドロイド
縦向きモードと横向きモード	X	X
アプリを信頼するためのアプリ内ガイド	X	X
メールで登録した場合、Secure Mailへの自動登録(MAMのみ)	X	X
Touch IDオフライン認証	X	X
派生資格情報で登録	X	
生体認証		X
Workspaceアプリストアの使用	X	X

シトリックス セキュアメール

機能	IOS	アンドロイド
メールの生産性		
下書きを最小化	X	X
送信済みメールの取り消し		X
暗号化管理	X	X
カレンダーの予定ウィジェット		X
Secure Mail の連絡先画像	X	X
レスポンスメールのサポート	X	X
下書きフォルダーの自動同期	X	X

機能	IOS	アンドロイド
下書きフォルダーでの添付ファイルの同期		X
メールの送信、受信、返信、全員に返信、転送	X	X
下書きの作成、編集、削除	X	X
メールのフラグ付け	X	X
未読にする	X	X
すべてのフォルダーとサブフォルダーの表示	X	X
アプリがバックグラウンドになったときの下書きの自動保存	X	X
Citrix Secure Notes を使用したメールからメモへの変換。 重要: Secure Notes は、December 31, 2018 にサポート終了 (EOL) ステータスに達しました。詳細については、「 EOL および非推奨のアプリ 」を参照してください。	X	X
メール検索 (ローカルおよびサーバー)	X	X
メール同期期間の選択 (最大 1 か月またはすべてのメール)	X	X
未読メールの表示	X	X
画像、ビデオ、オーディオの添付ファイルを安全に表示/再生	X	X
複数の添付ファイル	X	X

機能	IOS	アンドロイド
添付ファイルの返信と転送	X	X
Citrix Filesからファイルを添付	X	X
Citrix Filesの制限付きゾーンとコネクタからファイルを添付	X	X
添付ファイルリポジトリ	X	X
リッチテキスト編集	X	X
件名付きメール通知、ロック画面でのプレビュー	X	X
通知画面からメールや招待に返信、削除	X	
写真を添付または撮影	X	X
複数のメッセージを選択	X	X
添付ファイルをダウンロード	X	X
画像をインラインで読み込む	X	X
高速ソート	X	X
.zipファイル添付ファイルの送受信、開く、保存	X	X
縦向きモードと横向きモード	X; メールリスト、メール閲覧、作成、カレンダー、連絡先ビュー全体で	X: メール閲覧および作成ビューのみ
貼り付けたテキストは書式を維持する	X	X
連絡先からのSMS	X	X
連絡先からのFaceTime	X	

機能	IOS	アンドロイド
接続の問題またはメールボックスの容量不足により送信されなかったメッセージは送信トレイに保存されます	X	X
最近使用したフォルダーが上位に表示される		X
プルダウンによるメール更新	X	X
最終更新タイムスタンプ	X	X
メッセージ操作のための左スワイプ	X	X
Microsoft Exchange および IBM Notes Traveler のサポート	X	X
メール、カレンダー、連絡先を更新するにはタップ	X	X
メール表示でデバイスのアクセシビリティ/フォントサイズ設定を尊重する	X	X
S/MIME署名と暗号化	X	X
S/MIME証明書のメールによるインポート	X	X
S/MIME、Intercede連携	X	
S/MIME、Entrust連携	X	
メッセージ本文のMicrosoft IRM保護	X	X
プッシュ通知	X	X
受信トレイへのプッシュ通知により、カレンダーを含む	X	

機能	IOS	アンドロイド
すべてのフォルダーが自動的に更新されます		
Office 365 ドキュメントを開く	X	X
3D Touch アクション	X	
ロック画面のコンテキストアイコン	X	X
フォルダーを検索	X	X
VIP メールフォルダー	X	X
Dynamic Type のサポート	X	X
展開されたフォルダーを維持	X	X
メッセージ分類マーカー	X	X
スペルチェック	X	
最後に撮影した写真を添付	X	X
URLプレビュー	X	X
Citrix FilesでCitrix Filesリンクを開く	X	X
<code>.pass</code> ファイルへの対応	X	
検索モードで複数のメールを選択	X	X
画像をインラインで挿入	X	X
Exchange ActiveSync (EAS) バージョン 16 へのアップグレード	X	X

機能	IOS	アンドロイド
ユーザーが不明なドメインまたは個人ドメインを使用することを制限する	X	
超ワイドデバイス画面をサポート		X
複数のExchangeアカウントを構成する	X	X
その他の操作のために左右にスワイプする	X	X
暗号化されたメールへの返信または転送を暗号化する	X	
メールとインライン画像を印刷	X	
設定の「プレビュー行数」を使用して、メールボックスビューでメール本文のプレビューとして表示される行数を構成します	X	
レスポンスメールのサポート	X	X
添付ファイル（MS Officeまたは画像）のアプリ内プレビュー	X	X
個人連絡先グループ	X	X
ユーザー名をメールアドレス（UPN）に移行	X	X
フィッシングメールを報告	X	X
モダン認証 (OAuth)	X	X
添付ファイルを印刷	X	

機能	IOS	アンドロイド
アンドロイド エンタープライズ (アンドロイド フォー ワーク)	X	
リッチテキスト署名	X	
リッチプッシュ通知	X	
フィード	X	X
写真添付機能の改善	X	X
グループ通知	X	
Slack連携 (プレビュー)	X	X
フィードの管理	X	
内部ドメイン	X	X
フィードを管理	X	X
MS Teams連携	X	X
自己診断 (Troubleshoooot) オプション		X
デュアルモード (MAM SDK)	X	X
自己診断ツール		X
カレンダー		
ICSファイルをカレンダーイベントとしてプレビューおよびインポート		X
カレンダーイベントのドラッグアンドドロップ	X	X
日、週、月、および議題ビュー	X	X

機能	IOS	アンドロイド
ロック画面での詳細なリマインダー	X	X
6か月間の同期	X	X
イベントをプライベートに設定	X	X
最初のイベントの1時間前にスクロール	X	
手動更新オプション	X	X
リマインダーを設定	X	X
タップして住所を地図表示	X	X
週番号	X	X
Dynamic Type のサポート	X	X
セキュリティ分類マーカー	X	X
アドレスの長押し	X	
週の開始日を設定	X	X
選択した日付の週にビューをフォーカス	X	
常に現在の日付をハイライト表示	X	X
添付リポジトリからのカレンダー添付ファイル	X	X
個人カレンダーのサポート	X	X
個人カレンダーイベントとの競合を表示		X
カレンダーイベントを印刷	X	

機能	IOS	アンドロイド
カレンダーの件名行にある電話番号とWebアドレスをタップ	X	
カレンダーを検索	X	
会議		
会議の返信、全員に返信、転送	X	X
招待への応答の主催者ビュー	X	X
招待者の空き状況と提案された空き状況の主催者ビュー	X	X
タップしてオンライン会議に参加します。注: WebEx および Lync の場合、これらのアプリを有効にするには、Citrix Endpoint Management™ でポリシーを構成する必要があります。	X	X
タップして音声会議に参加	X	X
新しい招待でオンライン会議、音声、会議をスケジュールする	X	X
新しい招待にShareFileリンクを追加する	X	X
添付ファイル付きの招待を転送する	X	X
「遅れます」メールを送信するためにタップする	X	X
会議の主催者に返信するためにタップする	X	X

機能	IOS	アンドロイド
すべての会議招待に返信するをタップ	X	X
すべての会議出席者に返信するをタップ	X	X
添付ファイル付きですべての会議出席者に返信するをタップ	X	X
GoToMeeting にダイヤルイン	X	X
ロック画面または通知画面から招待に応答	X	X
WebExまたはLync会議にダイヤルインする	X	X
辞退されたイベントを非表示にする	X	X
3つ以上の同時イベントを表示する	X	X
招待者のステータスをすばやく表示	X	X
キャンセルされたイベントの削除、返信、全員に返信、コメントの追加	X	X
転送された招待状に主催者名を表示	X	X
共有デバイス	X	X
Skype for Business会議に参加	X	X
承諾、辞退、仮承諾などの会議通知に応答する。	X	X

機能	IOS	アンドロイド
返信および削除でメッセージ通知に応答する	X	
連絡先		
連絡先にフォルダーを作成		X
双方向の連絡先同期	X	X
詳細な連絡先情報 GAL検索	X	X
Secure Mailの連絡先をローカルの連絡先にエクスポートして同期	X	X
連絡先: お気に入りおよびカテゴリ		X
どの連絡先フィールドをエクスポートするかを制御する	X	X
Secure Mail以外の連絡先の詳細	X	X
ダイナミックタイプサポート	X	X
連絡先をVIPとしてマークする	X	X
<code>.vcards</code> と連絡先を共有する	X	X
長押しで連絡先を表示		X
ネイティブメールアカウントが存在する場合でも連絡先をエクスポート	X	X
フォルダーとサブフォルダーを表示	X	
デバイスで構成された設定		

機能	IOS	アンドロイド
iMessageのサポート	X	
通知を制御するための高度なオプション	X	X
ロック画面の通知制御	X	X
メールとカレンダーの通知音	X	X
フォルダの自動更新	X	X
社内および社外の不在通知を設定	X	X
削除前に確認	X	X
スレッド形式の会話または時系列表示	X	X
Wi-Fiで添付ファイルを読み込む	X	X
Wi-Fiでの添付ファイルの読み込みをデフォルトにする	X	X
メールの同期期間を設定する	X	X
無制限の同期/すべてのメールを同期		X
メールの署名を設定する	X	X
連絡先を名または姓で一覧表示	X	X
自動進行	X	X
自宅のタイムゾーンを使用		X
クイック応答テンプレート		X
プッシュメール構成の頻度		X

機能	IOS	アンドロイド
設定のエクスポート/インポート	X	X
デバイスの戻るボタンをタップして、フローティングアクションボタンのオプションを閉じます		X
マイクロソフト チームズ	X	X

シトリックス セキュアウェブ™

機能	IOS	アンドロイド
マルチタスクで2つのアプリを同時に使用する	X	
ファイルをダウンロードする	X	X
お気に入りに追加する	X	X
保存されたユーザー名とパスワードをクリア	X	X
キャッシュ/履歴/Cookieを削除	X	X
ポップアップをブロック	X	X
オフラインページを保存	X	X
アドレスバーで検索	X	X
通知からダウンロードした項目を開く	X	X
パスワードの自動保存	X	X
プロキシのサポート		
エンタープライズプロキシ	X	X

機能	IOS	アンドロイド
URLブロックリストと許可リスト	X	X
履歴	X	X
デフォルトのホームページ	X	X
タブ	X	X
ブックマークのプッシュ	X	X
スクリーンキャプチャのブロック		X
現在のページを検索	X	X
3D Touchアクション	X	
共有デバイス	X	X
共有デバイスでのファイル改ざん防止	X	
設定のエクスポート/インポート	X	X
縦向きモードと横向きモード	X	X
アンドロイド エンタープライズ (アンドロイド フォーワーク)		X
画面のコンテンツをプルして更新	X	X
Secure Web を既定のブラウザとして		X

機能フラグ管理

機能フラグの下にある機能が最適に動作するようにするには、

`features.netscalergateway.net` へのトラフィックを有効にする必要があります。

機能フラグは、機能を動的に有効または無効にするために使用されます。本番環境でモバイル生産性アプリに問題が発生した場合、機能が出荷された後でも、影響を受ける機能を動的に無効にすることができます。そのためには、Citrix が管理する機能フラグを使用します。

機能管理のためのトラフィックを有効にするために手動での設定は必要ありませんが、アウトバウンドトラフィックをブロックするファイアウォールまたはプロキシがある場合は例外です。その場合、ポリシー要件に応じて、特定のURLまたはIPアドレスを使用してトラフィックを有効にする必要があります。

IPアドレス

許可リストにIPアドレスを記載する必要がある場合は、`features.netscalergateway.net` へのトラフィックを許可するために、次のIPアドレスを含めてください。

- 57.153.121.183 (ヨーロッパ西部地域の場合)
- 172.202.161.151 (米国中南部地域の場合)
- 48.218.128.128 (日本東部地域の場合)

これらのIPアドレスを追加することで、インフラストラクチャの更新に合わせてファイアウォールの設定が自動的に更新されるようにすることができます。

システム要件

NetScaler Gateway を使用していて、スプリットトンネリングが **OFF** に設定されている場合は、NetScaler がポート 443 経由で `features.netscalergateway.net` を解決し、接続できることを確認してください。

次の表に、機能フラグ管理をサポートするモバイル生産性アプリの最小バージョンを示します。

モバイル生産性アプリ	オペレーティングシステム	サポートされる最小バージョン
セキュアハブ	アンドロイド	24.8.0以降
セキュアハブ	iOS	24.9.0以降
MAM SDK	アンドロイド	24.9.0以降
MAM SDK	iOS	24.7.1以降
セキュアメール	アンドロイド、iOS	24.9.0 以降
セキュアウェブ	アンドロイド	24.8.0 以降
セキュアウェブ	iOS	24.9.0 以降

シトリックス セキュアハブ™

Citrix Secure Hubは、Citrix Endpoint Management™（旧称: XenMobile）エクスペリエンスのランチパッドです。ユーザーはSecure Hubにデバイスを登録してStoreにアクセスします。Storeから、Citrixが開発したモバイル生産性向上アプリやサードパーティ製アプリを追加できます。

Secure Hubおよびその他のモバイル生産性向上アプリのシステム要件については、「[システム要件](#)」を参照してください。

Secure Hubの管理

Secure Hubに関連する管理タスクのほとんどは、Endpoint Managementの初期構成時に実行します。Secure HubをiOSおよびAndroidユーザーが利用できるようにするには、Secure HubをiOS App StoreおよびGoogle Play Storeにアップロードします。

Citrixアプリのポータルを提供するだけでなく、ユーザーのCitrix GatewayセッションがCitrix Gatewayを使用した認証後に更新されると、Secure HubはインストールされているアプリのEndpoint Managementに保存されているほとんどのMDXポリシーを更新します。

重要:

以下のいずれかのポリシーを変更した場合、更新されたポリシーを適用するには、ユーザーがアプリを削除して再インストールする必要があります。セキュリティグループ、暗号化の有効化、およびSecure Mail Exchange Server。

シトリックス PIN

Secure HubでCitrix PINを使用するように構成できます。これは、Endpoint Managementコンソールの**設定 > クライアントプロパティ**で有効にするセキュリティ機能です。この設定では、登録済みのモバイルデバイスユーザーがSecure Hubにサインオンし、個人識別番号（PIN）を使用してMDXでラップされたアプリをアクティブ化する必要があります。

Citrix PIN機能は、保護されたラップされたアプリにログオンする際のユーザー認証エクスペリエンスを簡素化します。ユーザーは、Active Directoryのユーザー名やパスワードなどの別の資格情報を繰り返し入力する必要がありません。

Secure Hubに初めてサインオンするユーザーは、Active Directoryのユーザー名とパスワードを入力する必要があります。サインオン中に、Secure HubはActive Directoryの資格情報またはクライアント証明書をユーザーデバイスに保存し、ユーザーにPINの入力を求めます。ユーザーが再度サインオンするときは、アクティブなユーザーセッションの次のアイドルタイムアウト期間が終了するまで、PINを入力してCitrixアプリとStoreに安全にアクセスします。関連するクライアントプロパティを使用すると、PINを使用してシークレットを暗号化したり、PINのパスコードタイプを指定したり、PINの強度と長さの要件を指定したりできます。詳細については、「[クライアントプロパティ](#)」を参照してください。

指紋認証が有効になっている場合、アプリの非アクティブ化によりオフライン認証が必要な場合、ユーザーは指紋を使用してサインオンできます。ユーザーは、Secure Hubに初めてサインオンするとき、デバイスを再起動するとき、および非アクティブタイマーの期限が切れた後には、引き続きPINを入力する必要があります。指紋認証を有効にする方法については、「[指紋またはTouch ID認証](#)」を参照してください。

証明書ピンニング

iOSおよびAndroid版Secure Hubは、SSL証明書ピンニングをサポートしています。この機能により、CitrixクライアントがEndpoint Managementと通信する際に、企業によって署名された証明書が使用されることが保証されます。証明書ピンニングは、デバイスへのルート証明書のインストールによってSSLセッションが侵害された場合に、クライアントからEndpoint Managementへの接続を防止します。Secure Hubがサーバーの公開鍵に対する変更を検出すると、Secure Hubは接続を拒否します。

Android N以降、オペレーティングシステムはユーザーが追加した認証局 (CA) を許可なくなりました。Citrixでは、ユーザーが追加したCAの代わりにパブリックルートCAを使用することをお勧めします。

Android Nにアップグレードするユーザーは、プライベートCAまたは自己署名CAを使用している場合、問題が発生する可能性があります。Android Nデバイスでの接続は、以下のシナリオで切断されます。

- プライベート/自己署名CAを使用しており、AutoDiscovery ServiceのEndpoint Managementの必須の信頼済みCAオプションが**ON**に設定されている場合。詳細については、「[Endpoint Management AutoDiscovery Service](#)」を参照してください。
- プライベート/自己署名CAを使用しており、AutoDiscovery Service (ADS) に到達できない場合。セキュリティ上の懸念から、ADSに到達できない場合、必須の信頼済みCAは、最初に**OFF**に設定されていても**ON**になります。

デバイスを登録したりSecure Hubをアップグレードしたりする前に、証明書ピン留めを有効にすることを検討してください。このオプションはデフォルトでオフになっており、Endpoint Management Auto Discovery Service (ADS) によって管理されます。証明書ピン留めを有効にすると、ユーザーは自己署名証明書を使用してEndpoint Managementに登録できなくなります。ユーザーが自己署名証明書で登録しようとする、証明書が信頼されていないという警告が表示されます。ユーザーが証明書を受け入れない場合、登録は失敗します。

証明書ピン留めを使用するには、CitrixにCitrix ADSサーバーへの証明書のアップロードを依頼してください。 [Citrixサポートポータル](#)を使用してテクニカルサポートケースをオープンし、以下の情報を提供してください。

- ユーザーが登録するアカウントを含むドメイン。
- Endpoint Managementの完全修飾ドメイン名 (FQDN)。
- Endpoint Managementインスタンス名。デフォルトでは、インスタンス名はzdmであり、大文字と小文字が区別されます。
- ユーザーIDの種類。UPNまたはメールアドレスのいずれかです。デフォルトでは、種類はUPNです。
- デフォルトのポート8443からポート番号を変更した場合の、iOS登録に使用されるポート。
- デフォルトのポート443からポート番号を変更した場合の、Endpoint Managementが接続を受け入れるポート。
- Citrix Gatewayの完全なURL。
- オプションで、Endpoint Management管理者のメールアドレス。
- ドメインに追加するPEM形式の証明書。

Secure Hub の証明書 + ワンタイムパスワード認証の構成

Citrix ADC を構成して、Secure Hub が証明書とワンタイムパスワードとして機能するセキュリティトークンを使用して認証できるようにすることができます。この構成により、デバイスにActive Directory のフットプリントを残さない強力なセキュリティオプションが提供されます。

Secure Hub でこの種類の認証を使用できるようにするには、Citrix ADC でリライトアクションとリライトポリシーを追加し、Citrix Gateway のログオンの種類を示す **X-Citrix-AM-GatewayAuthType: CertAndRSA** 形式のカスタム応答ヘッダーを挿入します。

通常、Secure Hub は Endpoint Management コンソールで構成された Citrix Gateway のログオンの種類を使用します。ただし、この情報は Secure Hub が初めてログオンを完了するまで Secure Hub で利用できません。そのため、Secure Hub がこれを行うにはカスタムヘッダーが必要です。

注：

Endpoint Management と Citrix ADC で異なるログオンの種類が設定されている場合、Citrix ADC の構成が優先されます。詳細については、「[Citrix Gateway と Endpoint Management](#)」を参照してください。

1. Citrix ADC で、**[Configuration] > [AppExpert] > [Rewrite] > [Actions]** の順に移動します。

2. **[Add]** をクリックします。

[Create Rewrite Action] 画面が表示されます。

3. 次の図に示すように各フィールドに入力し、**[Create]** をクリックします。

Create Rewrite Action

Name*
InsertGatewayAuthTypeHeader ?

Type*
INSERT_HTTP_HEADER

Use this action type to insert a header.

Header Name*
X-Citrix-AM-GatewayAuthType

Expression Expression Editor
 Operators Saved Policy Expressions Frequently Used Expressions Clear
 "CertAndRSA" Evaluate

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.

Comments

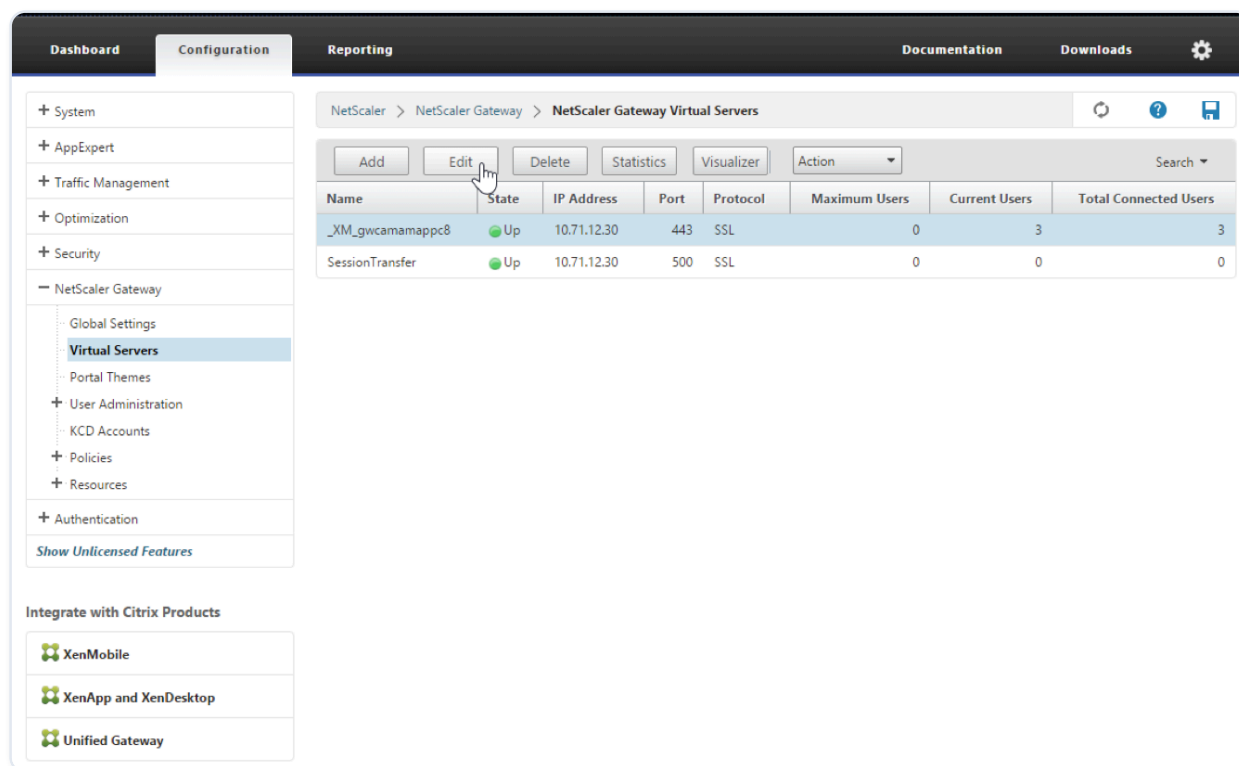
Create Close

メインの **[Rewrite Actions]** 画面に次の結果が表示されます。

Name	Type	Target Expression	Expression	Pattern
ns_cvprn_sp_js_checkout_rw_act	insert_after_all	TEXT	"\^'+window.location.pathname.split('\^')[1]+\^'+wi...	re~a.substr(0,3\).toLowerCase\(\)=~\ "%2f\)\a=
InsertGatewayAuthTypeHeader	insert_http_header	X-Citrix-AM-GatewayAuthType	"CertAndRSA"	

4. リライトアクションをリライトポリシーとして仮想サーバーにバインドします。

[Configuration] > [NetScaler® Gateway] > [Virtual Servers] に移動し、仮想サーバーを選択します。



5. 「編集」をクリックします。
6. 「仮想サーバー構成」画面で、「ポリシー」までスクロールします。
7. ポリシーを追加するには「+」をクリックします。

ポリシー追加オプションの画像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-virtual-server-configuration-screen.png)

8. 「ポリシーの選択」フィールドで、「書き換え」を選択します。
9. 「種類の選択」フィールドで、「応答」を選択します。

応答オプションの画像(/en-us/mobile-productivity-apps/media/netscaler-policy-settngs-response.png)

10. 「続行」をクリックします。

「ポリシーバインディング」セクションが展開されます。

ポリシーバインディングセクションの画像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-policy-click-to-select.png)

11. 「ポリシーの選択」をクリックします。

利用可能なポリシーの画面が表示されます。

利用可能なポリシーの画像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-rewrite-policies.png)

- 作成したポリシーの行をクリックし、次に「**選択**」をクリックします。「**ポリシーバインディング**」画面が再度表示され、選択したポリシーが入力されています。

選択したポリシーの画像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-policy-binding-policy-showing.png)

- 「**バインド**」をクリックします。

バインドが成功すると、完了した書き換えポリシーが表示されたメイン構成画面が表示されます。

成功したバインドの画像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-bind-successful.png)

- ポリシーの詳細を表示するには、「**書き換えポリシー**」をクリックします。

書き換えポリシーの詳細の画像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-rewrite-policy.png)

AndroidデバイスのADS接続のポート要件

ポート構成により、Secure Hubから接続するAndroidデバイスが社内ネットワーク内からCitrix ADSにアクセスできるようになります。ADSへのアクセス機能は、ADSを通じて利用可能になるセキュリティ更新プログラムをダウンロードする際に重要です。ADS接続はプロキシサーバーと互換性がない場合があります。このシナリオでは、ADS接続がプロキシサーバーをバイパスできるようにします。

重要:

AndroidおよびiOS版Secure Hubでは、AndroidデバイスがADSにアクセスできるようにする必要があります。詳細については、Endpoint Managementのドキュメントの[ポート要件](#)を参照してください。この通信は送信ポート443で行われることに注意してください。既存の環境では、このアクセスが許可されるように設計されている可能性が非常に高いです。この通信を保証できないお客様は、Secure Hub 10.2へのアップグレードを強くお勧めしません。ご不明な点がございましたら、Citrixサポートにお問い合わせください。

証明書ピンニングを有効にするには、次の前提条件を満たす必要があります。

- Endpoint ManagementおよびCitrix ADC証明書を収集します。証明書はPEM形式であり、公開証明書である必要があります、秘密鍵であってはなりません。

- Citrixサポートに連絡し、証明書ピンニングを有効にするようリクエストしてください。このプロセス中に、証明書の提出を求められます。

新しい証明書ピンニングの改善により、デバイスは登録前にADSに接続する必要があります。これにより、デバイスが登録される環境に対して、Secure Hubで最新のセキュリティ情報が利用可能になります。デバイスがADSに到達できない場合、Secure Hubはデバイスの登録を許可しません。したがって、デバイスが登録できるようにするには、内部ネットワーク内でADSアクセスを開放することが重要です。

Android版Secure HubのADSへのアクセスを許可するには、次のIPアドレスとFQDNに対してポート443を開放します。

FQDN	IPアドレス	ポート	IPおよびポートの使用状況
<code>discovery.mdm.ze nprise.com</code>	52.5.138.94	443	セキュアハブ - エー ディーエス通信
<code>discovery.mdm.ze nprise.com</code>	52.1.30.122	443	セキュアハブ - エー ディーエス通信
<code>ads.xm.cloud.com</code> : SecureHubバー ジョン10.6.15以降で は <code>ads.xm.cloud.com</code> を使用することに注 意してください。	34.194.83.188	443	セキュアハブ - エー ディーエス通信
<code>ads.xm.cloud.com</code> : SecureHub バー ジョン 10.6.15 以降 では <code>ads.xm.cloud.com</code> が使用されることに 注意してください。	34.193.202.23	443	Secure Hub - ADS 通 信

証明書ピン留めが有効な場合:

- Secure Hub は、デバイス登録中にエンタープライズ証明書をピン留めします。
- アップグレード中に、Secure Hub は現在ピン留めされている証明書を破棄し、登録済みユーザーの最初の接続時にサーバー証明書をピン留めします。

注:

アップグレード後に証明書ピン留めを有効にした場合、ユーザーは再度登録する必要があります。

- 証明書の公開鍵が変更されていない限り、証明書の更新に再登録は必要ありません。

証明書ピン留めは、中間証明書や発行者証明書ではなく、リーフ証明書をサポートします。証明書ピン留めは、Endpoint Management や Citrix Gateway などの Citrix サーバーに適用され、サードパーティサーバーには適用されません。

Secure Hub の機能

Secure Hub を使用すると、ストアとライブサポートへのアクセスを提供しながら、モバイルポリシーを監視および適用できます。ユーザーは、Apple、Android、または Windows のアプリストアから Secure Hub をデバイスにダウンロードすることから始めます。

Secure Hub が開くと、ユーザーは会社から提供された資格情報を入力して、デバイスを Secure Hub に登録します。デバイス登録の詳細については、「[ユーザー、アカウント、役割、および登録](#)」を参照してください。

Android 版 Secure Hub では、初回インストール時および登録時に、次のメッセージが表示されます: Secure Hub にデバイス上の写真、メディア、ファイルへのアクセスを許可しますか？

このメッセージはAndroidオペレーティングシステムからのものであり、Citrixからのものではありません。許可をタップしても、CitrixおよびSecure Hubを管理する管理者がお客様の個人データを閲覧することはありません。ただし、管理者とのリモートサポートセッションを実施する場合、管理者はセッション内でお客様の個人ファイルを閲覧できます。

登録が完了すると、ユーザーはプッシュされたすべてのアプリとデスクトップをマイアプリタブで確認できます。ユーザーはストアからさらにアプリを追加できます。電話では、ストアのリンクは左上隅のハンバーガーアイコンの下にあります。

ストアリンクの画像(/en-us/mobile-productivity-apps/media/secure-hub-settings.png)

タブレットでは、ストアは別のタブになっています。

タブレット上のストアの画像(/en-us/mobile-productivity-apps/media/secure-hub-ipad-myapps.png)

iOS 9以降を実行しているiPhoneユーザーがEndpoint Managementアプリストアからモバイル生産性アプリをインストールすると、エンタープライズ開発者であるCitrixがそのiPhoneで信頼されていないため、開発者が信頼されるまでアプリは使用できないというメッセージが表示されます。このメッセージが表示された場合、Secure Hubは、iPhone用のCitrixエンタープライズアプリを信頼するプロセスを案内するガイドを表示するようにユーザーに促します。

MAMのみの展開の場合、Endpoint Managementを構成して、メール資格情報を使用してSecure Hubに登録するAndroidまたはiOSデバイスのユーザーがSecure Mailに自動的に登録されるようにすることができます。ユーザーは、Secure Mailに登録するために追加情報を入力したり、追加の手順を実行したりする必要はありません。

Secure Mailを初めて使用する際、Secure MailはSecure Hubからユーザーのメールアドレス、ドメイン、およびユーザーIDを取得します。Secure Mailはメールアドレスを自動検出に使用します。ExchangeサーバーはドメインとユーザーIDを使用して識別され、これによりSecure Mailはユーザーを自動的に認証できます。ポリシーがパスワードを渡さないように設定されている場合、ユーザーはパスワードの入力を求められますが、それ以上の情報を入力する必要はありません。

この機能を有効にするには、次の3つのプロパティを作成します。

- サーバープロパティMAM_MACRO_SUPPORT。手順については、「」([/ja-jp/xenmobile/server/install-configure/server-properties.html](#))を参照してください。
- クライアントプロパティENABLE_CREDENTIAL_STOREおよびSEND_LDAP_ATTRIBUTES。手順については、「」([/ja-jp/citrix-endpoint-management/advanced-concepts/deployment/client-properties.html](#))を参照してください。

ストアをカスタマイズする場合は、**設定 > クライアントブランディング**に移動して、名前を変更し、ロゴを追加し、アプリの表示方法を指定します。

クライアントブランディング画像の画像([/en-us/mobile-productivity-apps/media/worxhome-client-branding.png](#))

Endpoint Managementコンソールでアプリの説明を編集できます。**構成**をクリックし、次に**アプリ**をクリックします。テーブルからアプリを選択し、**編集**をクリックします。編集する説明を持つアプリのプラットフォームを選択し、**説明**ボックスにテキストを入力します。

説明ボックスの画像([/en-us/mobile-productivity-apps/media/worxhome-edit-app-descriptions-xm.png](#))

ストアでは、ユーザーはEndpoint Managementで構成および保護したアプリとデスクトップのみを閲覧できます。アプリを追加するには、ユーザーは**詳細**をタップし、次に**追加**をタップします。

Secure Hubは、ユーザーがヘルプを得るためのさまざまな方法も提供します。タブレットでは、右上隅の疑問符をタップするとヘルプオプションが開きます。電話では、ユーザーは左上隅のハンバーガーメニューアイコンをタップし、次にヘルプをタップします。

ヘルプ画面の画像(/en-us/mobile-productivity-apps/media/secure-hub-helpdesk.png)

IT部門には、会社のヘルプデスクの電話番号とメールアドレスが表示され、ユーザーはアプリから直接アクセスできます。電話番号とメールアドレスはEndpoint Managementコンソールに入力します。右上隅の歯車アイコンをクリックします。**設定**ページが表示されます。**その他**をクリックし、次に**クライアントサポート**をクリックします。情報を入力する画面が表示されます。

クライアントサポート画面の画像(/en-us/mobile-productivity-apps/media/worxhome-edit-client-support-xm.png)

問題の報告にはアプリのリストが表示されます。ユーザーは問題のあるアプリを選択します。Secure Hubは自動的にログを生成し、ログをzipファイルとして添付したメッセージをSecure Mailで開きます。ユーザーは件名と問題の説明を追加します。スクリーンショットを添付することもできます。

Citrixにフィードバックを送信すると、Citrixサポートのアドレスが入力されたメッセージがSecure Mailで開きます。メッセージ本文には、Secure Mailを改善するための提案を入力できます。Secure Mailがデバイスにインストールされていない場合は、ネイティブのメールプログラムが開きます。

ユーザーは**Citrixサポート**をタップすることもでき、これにより**Citrix Knowledge Center**が開きます。そこから、すべてのCitrix製品のサポート記事を検索できます。

設定では、ユーザーは自分のアカウントとデバイスに関する情報を見つけることができます。

Secure Hubは、たとえば、企業所有のデバイスが特定の地理的境界を越えないようにしたい場合に、地理的位置情報および地理的追跡ポリシーも提供します。詳細については、**位置情報デバイスポリシー**を参照してください。さらに、Secure Hubは障害情報を自動的に収集および分析するため、特定の障害の原因を把握できます。この機能は、Crashlyticsソフトウェアによってサポートされています。

Secure Mail の概要

Citrix Secure Mail™ を使用すると、ユーザーはモバイルフォンやタブレットでメール、カレンダー、連絡先を管理できます。Microsoft Outlook または IBM Notes アカウントとの継続性を維持するために、Secure Mail は Microsoft Exchange Server および IBM Notes Traveler Server と同期します。

Citrix アプリスイートの一部として、Secure Mail は Citrix Secure Hub とのシングルサインオン (SSO) 互換性によるメリットがあります。ユーザーが Secure Hub にサインオンすると、ユーザー名とパスワードを再入力することなく、Secure Mail にシームレスに移行できます。Secure Mail は、デバイスが Secure Hub に登録されたときに自動的にユーザーのデバイスにプッシュされるように構成することも、ユーザーがストアからアプリを追加することもできます。

注:

- Exchange Server 2010 のサポートは October 13, 2020 に終了しました。
- Exchange Server 2013 のサポートは April 11, 2023 に終了しました。

Secure Mail は以下と互換性があります。

- エクスチェンジ サーバー SE RTM
- Exchange Server 2019 累積更新プログラム 15
- Exchange Server 2019 累積更新プログラム 14
- Exchange Server 2019 累積更新プログラム 13
- Exchange Server 2019 累積更新プログラム 12
- Exchange Server 2019 累積更新プログラム 11
- Exchange Server 2019 累積更新プログラム 10
- Exchange Server 2019 累積更新プログラム 9
- Exchange Server 2019 累積更新プログラム 8
- Exchange Server 2019 累積更新プログラム 7
- Exchange Server 2019 累積更新プログラム 6

- Exchange Server 2016 累積更新プログラム 23
- Exchange Server 2016 累積更新プログラム 22
- Exchange Server 2016 累積更新プログラム 21
- Exchange Server 2016 累積更新プログラム 20
- Exchange Server 2016 累積更新プログラム 19
- Exchange Server 2016 累積更新プログラム 18
- Exchange Server 2016 累積更新プログラム 17
- HCL Domino バージョン 14.0 FP1
- HCL Domino バージョン 12.0.2 FP2
- HCL Traveler バージョン 12.0.2.1 ビルド 202302010413_30
- HCL Domino 11 (以前の名称: Lotus Notes)
- HCL Domino 10.0.1 (以前の名称: Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197 (旧 ロータス ノーツ)
- HCL Domino 10.0.1.0 build 201811191126_20 (旧 ロータス ノーツ)
- HCL Domino 9.0.1.21 (旧 ロータス ノーツ)
- Microsoft Office 365 (エクスチェンジ オンライン)

まず、[Citrix Endpoint Management Downloads](#)からSecure Mail およびその他の Endpoint Management コンポーネントをダウンロードしてください。

Secure Mail およびその他のモビリティアプリのシステム要件については、[システム要件](#)を参照してください。

iOS および Android 版 Secure Mail での通知（アプリがバックグラウンドで実行されている場合、または閉じられている場合）に関する情報については、[Secure Mail のプッシュ通知](#)を参照してください。

Secure Mail でサポートされている iOS の機能については、[Secure Mail の iOS 機能](#)を参照してください。

Secure Mail でサポートされている Android の機能については、[Secure Mail の Android 機能](#)を参照してください。

Secure Mail でサポートされている iOS および Android の機能については、[Secure Mail の iOS および Android 機能](#)を参照してください。

ユーザーヘルプドキュメントについては、Citrix ユーザーヘルプセンターの[Citrix Secure Mail](#)ページを参照してください。

シトリックス セキュアウェブ™

Citrix Secure Webは、内部および外部サイトへのセキュアなアクセスを提供するHTML5互換のモバイルWebブラウザです。デバイスがSecure Hubに登録されている場合、Secure Webをユーザーデバイスに自動的にプッシュするように構成できます。または、Endpoint Managementアプリストアからアプリを追加することもできます。

Secure Webおよびその他のモバイル生産性アプリのシステム要件については、「[システム要件](#)」を参照してください。

Secure Webの統合と配信

注：

MDX Toolkit 10.7.10は、モバイル生産性アプリのラッピングをサポートする最終リリースです。ユーザーは、バージョン10.7.5以降のモバイル生産性アプリをパブリックアプリストアからアクセスします。

Secure Webを統合して配信するには、次の一般的な手順に従います。

1. 内部ネットワークへのシングルサインオン (SSO) を有効にするには、Citrix Gatewayを構成します。

HTTPトラフィックの場合、Citrix ADCはCitrix ADCでサポートされているすべてのプロキシ認証タイプに対してSSOを提供できます。HTTPSトラフィックの場合、Webパスワードキャッシュポリシーにより、Secure WebはMDXを介してプロキシサーバーに認証し、SSOを提供できます。MDXは、基本、ダイジェスト、およびNTLMプロキシ認証のみをサポートします。パスワードはMDXを使用してキャッシュされ、機密性の高いアプリデータのセキュアな保存領域であるEndpoint Management共有ボールドに保存されます。Citrix Gatewayの構成の詳細については、「[Citrix Gateway](#)」を参照してください。

2. Secure Webをダウンロードします。
3. 内部ネットワークへのユーザー接続をどのように構成するかを決定します。

4. 他のMDXアプリと同じ手順を使用してSecure WebをEndpoint Managementに追加し、MDXポリシーを構成します。Secure Webに固有のポリシーの詳細については、この記事の後半にある「Secure Webポリシーについて」を参照してください。

ユーザー接続の構成

Secure Webは、ユーザー接続に対して次の構成をサポートしています。

- **トンネル化 - Web SSO**： 内部ネットワークにトンネル接続する接続は、トンネル化 - Web SSOと呼ばれるクライアントレスVPNのバリエーションを使用できます。これは、**優先VPN**モードポリシーに指定されているデフォルト構成です。トンネル化 - Web SSOは、シングルサインオン (SSO) を必要とする接続に推奨されます。
- **フルVPNトンネル**： 内部ネットワークにトンネル接続する接続は、**優先VPN**モードポリシーによって構成されるフルVPNトンネルを使用できます。フルVPNトンネルは、クライアント証明書または内部ネットワーク内のリソースへのエンドツーエンドSSLを使用する接続に推奨されます。ただし、Secure Webは、モバイルデバイスに保存されているクライアント証明書を読み取ることができるアプリではありません。この機能を提供するサードパーティ製のラップされたエンタープライズアプリがインストールされている場合があります。フルVPNトンネルは、TCP上のあらゆるプロトコルを処理し、iOSおよびAndroidデバイスに加えて、WindowsおよびMacコンピューターで使用できます。
- **VPNモード切り替えの許可**ポリシーは、必要に応じてフルVPNトンネルモードとトンネル化されたWeb SSOモード間の自動切り替えを許可します。デフォルトでは、このポリシーはオフです。このポリシーがオンの場合、優先VPNモードで処理できない認証要求が原因で失敗したネットワーク要求は、代替モードで再試行されます。たとえば、フルVPNトンネルモードはクライアント証明書のサーバーチャレンジに対応しますが、トンネル化されたWeb SSOモードは対応しません。同様に、トンネル化されたWeb SSOモードを使用する場合、HTTP認証チャレンジはSSOで処理される可能性が高くなります。

以下の表は、構成とサイトの種類に基づいて、Secure Webがユーザーに資格情報の入力を求めるかどうかを示しています。

接続モード	サイトの種類	パスワード キャッシュ	CITRIX GATEWAY用に構成 された SSO	SECURE WEBは、 WEBサイ トへの初回 アクセス時 に資格情報 の入力を求 めます	SECURE WEBは、 WEBサイ トへのその 後のアクセ ス時に資格 情報の入力 を求めます	SECURE WEBは、 パスワード 変更後に資 格情報の入 力を求めま す
トンネル 化された Web SSO	HTTP	いいえ	はい	いいえ	いいえ	いいえ
トンネル 化 – Web SSO	HTTPS	いいえ	はい	いいえ	いいえ	いいえ
フルVPN	HTTP	いいえ	はい	いいえ	いいえ	いいえ
フルVPN	HTTPS	はい。 Secure Web MDX ポリシー の「Web パスワー ドキャッ シュを有 効にする 」がオ ンの場 合。	いいえ	はい。 Secure Webで資 格情報を キャッ シュする ために必 要です。	いいえ	はい

Secure Webポリシー

Secure Webを追加する際は、Secure Webに固有の以下のMDXポリシーに注意してください。サポートされているすべてのモバイルデバイスの場合：

許可またはブロックされたWebサイト

Secure Webは通常、Webリンクをフィルタリングしません。このポリシーを使用して、許可またはブロックするサイトの特定のリストを構成できます。ブラウザが開くことができるWebサイトを制限するために、URLパターンをコンマ区切りのリストとして構成します。リスト内の各パターンの前にはプラス記号 (+) またはマイナス記号 (-) が付きます。ブラウザは、一致が見つかるま

で、リストに記載されている順序でURLをパターンと比較します。一致が見つかった場合、プレフィックスは次のように実行するアクションを決定します。

- マイナス (-) プレフィックスは、ブラウザにURLをブロックするよう指示します。この場合、URLはWebサーバーアドレスが解決できないかのように扱われます。
- プラス (+) プレフィックスは、URLが通常どおり処理されることを許可します。
- パターンに + も - も指定されていない場合、+ (許可) が想定されます。
- リスト内のどのパターンにもURLが一致しない場合、そのURLは許可されます。

他のすべてのURLをブロックするには、リストをマイナス記号の後にアスタリスク (-*) を付けて終了します。例:

- ポリシー値 `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` は、`mycorp.com` ドメイン内のHTTP URLを許可しますが、それ以外の場所ではブロックし、HTTPSおよびFTP URLはどこでも許可し、他のすべてのURLをブロックします。
- ポリシー値 `+http://*.training.lab/*,+https://*.training.lab/*,-*` は、ユーザーがHTTPまたはHTTPS経由でTraining.labドメイン（イントラネット）内の任意のサイトを開くことを許可します。ただし、プロトコルに関係なく、Facebook、Google、Hotmailなどの公開URLを開くことはできません。

デフォルト値は空です（すべてのURLが許可されます）。

ポップアップをブロック

ポップアップとは、Webサイトがユーザーの許可なく開く新しいタブのことです。このポリシーは、Secure Webがポップアップを許可するかどうかを決定します。「オン」の場合、Secure WebはWebサイトがポップアップを開くのを防ぎます。デフォルト値は「オフ」です。

事前読み込みされたブックマーク

Secure Webブラウザ用の事前読み込みされたブックマークのセットを定義します。このポリシーは、フォルダ名、フレンドリ名、Webアドレスを含むタプルのコンマ区切りリストです。各トリプレットは、`folder, name, url` の形式である必要があり、`folder`と`name`はオプションで二重引用符 (") で囲むことができます。

たとえば、ポリシー値 `,"Mycorp, Inc. home page",https://www.mycorp.com,"MyCorp Links",Account logon,https://www.mycorp.com/Accounts "MyCorp Links/Investor Relations","Contact us",https://www.mycorp.com/IR/Contactus.aspx` は3つのブックマークを定義します。1つ目は「Mycorp, Inc. home page」というタイトルのプライマリリンク（フォルダ名なし）です。2つ目のリンクは「MyCorp Links」というタイトルのフォルダに配置さ

れ、「Account logon」とラベル付けされています。3つ目は「MyCorp Links」フォルダの「Investor Relations」サブフォルダに配置され、「Contact us」と表示されます。

デフォルト値は空です。

ホームページURL

Secure Webの起動時に読み込まれるWebサイトを定義します。デフォルト値は空です（デフォルトのスタートページ）。

サポートされているAndroidおよびiOSデバイスのみ:

ブラウザのユーザーインターフェイス

Secure Web のブラウザユーザーインターフェイスコントロールの動作と表示を決定します。通常、すべてのブラウジングコントロールが利用可能です。これには、進む、戻る、アドレスバー、更新/停止コントロールが含まれます。このポリシーを構成して、これらのコントロールの一部の使用と表示を制限できます。デフォルト値は「すべてのコントロールを表示」です。

オプション

- すべてのコントロールを表示。すべてのコントロールが表示され、ユーザーはそれらを使用することを制限されません。
- 読み取り専用アドレスバー。すべてのコントロールが表示されますが、ユーザーはブラウザのアドレスフィールドを編集できません。
- アドレスバーを非表示。アドレスバーは非表示になりますが、他のコントロールは非表示になりません。
- すべてのコントロールを非表示。ツールバー全体を非表示にし、フレームレスなブラウジングエクスペリエンスを提供します。

Web パスワードキャッシュを有効にする

Secure Web ユーザーが Web リソースへのアクセスまたは要求時に資格情報を入力した場合、このポリシーは Secure Web がデバイスにパスワードをサイレントにキャッシュするかどうかを決定します。このポリシーは、認証ダイアログで入力されたパスワードに適用され、Web フォームで入力されたパスワードには適用されません。

オンの場合、Secure Web はユーザーが Web リソースを要求する際に入力したすべてのパスワードをキャッシュします。オフの場合、Secure Web はパスワードをキャッシュせず、既存のキャッシュされたパスワードを削除します。デフォルト値はオフです。

このポリシーは、Preferred VPN ポリシーをこのアプリの Full VPN tunnel に設定した場合にのみ有効になります。

プロキシサーバー

Tunneled – Web SSO モードで使用する場合、Secure Web のプロキシサーバーを構成することもできます。詳細については、この[ブログ投稿](#)を参照してください。

DNS サフィックス

Android では、DNS サフィックスが構成されていない場合、VPN が失敗する可能性があります。DNS サフィックスの構成の詳細については、「[Android デバイスの DNS サフィックスを使用した DNS クエリのサポート](#)」を参照してください。

Secure Web 用のイントラネットサイトの準備

このセクションは、AndroidおよびiOS版Secure Webで使用するイントラネットサイトを準備する必要があるWebサイト開発者向けです。デスクトップブラウザ向けに設計されたイントラネットサイトは、AndroidおよびiOSデバイスで適切に動作するように変更が必要です。

Secure Webは、Webテクノロジーのサポートを提供するためにAndroid WebViewおよびiOS WkWebViewに依存しています。Secure WebでサポートされているWebテクノロジーの一部は次のとおりです。

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL
- WebSockets

Secure WebでサポートされていないWebテクノロジーの一部は次のとおりです。

- フラッシュ
- ジャバ

次の表は、Secure WebでサポートされているHTMLレンダリング機能とテクノロジーを示しています。「X」は、その機能がプラットフォーム、ブラウザ、コンポーネントの組み合わせで利用可能であることを示します。

テクノロジー	IOS セキュアウェブ	ANDROID 6.X/7.X セキュアウェブ
JavaScriptエンジン	JavaScriptCore	V8
ローカルストレージ	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
シークレット	X	X
WebGL		X
requestAnimationFrame API		X
ナビゲーションタイミングAPI		X
リソースタイミングAPI		X

テクノロジーはデバイス間で同じように動作します。ただし、Secure Webはデバイスごとに異なるユーザーエージェント文字列を返します。Secure Webで使用されているブラウザのバージョンを特定するには、そのユーザーエージェント文字列を表示できます。Secure Webから、`<https://whatsmyuseragent.com/>` に移動します。

イントラネットサイトのトラブルシューティング

Secure Webでイントラネットサイトを表示したときにレンダリングの問題をトラブルシューティングするには、Secure Webと互換性のあるサードパーティ製ブラウザでウェブサイトがどのようにレンダリングされるかを比較してください。

iOSの場合、テスト用の互換性のあるサードパーティ製ブラウザはChromeとDolphinです。

Androidの場合、テスト用の互換性のあるサードパーティ製ブラウザはDolphinです。

注:

ChromeはAndroidのネイティブブラウザです。比較には使用しないでください。

iOSでは、ブラウザがデバイスレベルのVPNをサポートしていることを確認してください。デバイスでVPNを構成するには、**設定 > VPN > VPN構成を追加**に移動します。

App Storeで入手可能なVPNクライアントアプリ（Citrix VPN、Cisco AnyConnect、Pulse Secure など）も使用できます。

- 2つのブラウザでウェブページが同じようにレンダリングされる場合、問題はウェブサイトにあります。サイトを更新し、OSで適切に動作することを確認してください。
- ウェブページの問題がSecure Webでのみ発生する場合は、Citrixサポートに連絡してサポートチケットを開いてください。テストしたブラウザとOSの種類を含むトラブルシューティング手順を提供してください。iOS版Secure Webでレンダリングの問題がある場合は、以下の手順で説明されているページのウェブアーカイブを含めてください。これにより、Citrixは問題をより迅速に解決できます。

ウェブアーカイブファイルを作成するには

macOS 10.9以降のSafariを使用すると、ウェブページをウェブアーカイブファイル（リーディングリストとも呼ばれます）として保存できます。ウェブアーカイブファイルには、画像、CSS、JavaScriptなどのすべてのリンクされたファイルが含まれます。

1. Safariからリーディングリストフォルダを空にします。**Finder**で、**メニューバーの移動メニュー**をクリックし、**フォルダへ移動**を選択し、パス名 `~/Library/Safari/ReadingListArchives/` を入力して、その場所にあるすべてのフォルダを削除します。
2. **メニューバー**で、**Safari > 環境設定 > 詳細**に移動し、**メニューバーの開発メニューを表示**を有効にします。
3. **メニューバー**で、**開発 > ユーザーエージェント**に移動し、Secure Webのユーザーエージェント (Mozilla/5.0 (iPad; CPU OS 8_3 like macOS) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F69 Secure Web/ 10.1.0(build 1.4.0) Safari/8536.25) を入力します。
4. Safariで、リーディングリスト（ウェブアーカイブファイル）として保存したいウェブサイトを開きます。
5. **メニューバー**で、**ブックマーク > リーディングリスト**に追加に移動します。アーカイブはバックグラウンドで行われ、数分かかる場合があります。
6. アーカイブされたリーディングリストを見つけます。**メニューバー**で、**表示 > リーディングリストサイドバーを表示**に移動します。

7. アーカイブファイルを検証します:

- Macへのネットワーク接続をオフにします。
- リーディングリストからWebサイトを開きます。

Webサイトが完全にレンダリングされます。

8. アーカイブファイルを圧縮します: **Finder**で、**メニューバーの移動メニュー**をクリックし、**フォルダへ移動**を選択して、パス名 `~/Library/Safari/ReadingListArchives/` を入力します。次に、ファイル名がランダムな16進数文字列になっているフォルダを圧縮します。サポートチケットを開く際に、このファイルをCitrixサポートに送信できます。

Secure Webの機能

Secure Webは、モバイルデータ交換テクノロジーを使用して、ユーザーが内部および外部のWebサイト、およびその他すべてのWebサイトにアクセスするための専用VPNトンネルを作成します。これには、組織のポリシーによって保護された環境で、機密情報を含むサイトも含まれます。

Secure WebとSecure MailおよびCitrix Filesの統合により、セキュアなEndpoint Managementコンテナ内でシームレスなユーザーエクスペリエンスが提供されます。統合機能の例をいくつか示します。

- ユーザーが**Mailto**リンクをタップすると、Citrix Secure Mail™で新しいメールメッセージが開き、追加の認証は不要です。
- iOSでは、ユーザーはURLの前に**ctxmobilebrowser://**を挿入することで、ネイティブメールアプリからSecure Webでリンクを開くことができます。たとえば、ネイティブメールアプリから `example.com` を開くには、URL `ctxmobilebrowser://example.com` を使用します。
- ユーザーがメールメッセージ内のイントラネットリンクをクリックすると、Secure Webはそのサイトに移動し、追加の認証は不要です。
- ユーザーは、Secure WebでWebからダウンロードしたファイルをCitrix Filesにアップロードできます。

Secure Webユーザーは、次のアクションも実行できます。

- ポップアップをブロックする。

注:

Secure Webのメモリの多くはポップアップのレンダリングに使われるため、設定でポップアップをブロックするとパフォーマンスが向上することがよくあります。

- お気に入りのサイトをブックマークする。
- ファイルをダウンロードする。
- ページをオフラインで保存する。
- パスワードを自動保存する。
- キャッシュ/履歴/Cookieをクリアする。
- CookieとHTML5ローカルストレージを無効にする。
- デバイスを他のユーザーと安全に共有する。
- アドレスバー内で検索する。
- Secure Webで実行するWebアプリが自分の位置情報にアクセスすることを許可する。
- 設定をエクスポートおよびインポートする。
- ファイルをダウンロードせずに、Citrix Filesで直接ファイルを開く。この機能を有効にするには、Endpoint Managementの許可されたURLポリシーに**ctx-sf**を追加します。
- iOSでは、3D Touchアクションを使用して新しいタブを開き、オフラインページ、お気に入りのサイト、ダウンロードにホーム画面から直接アクセスする。
- iOSでは、任意のサイズのファイルをダウンロードし、Citrix Filesまたは他のアプリで開く。

注:

Secure Web をバックグラウンドに置くと、ダウンロードが停止します。

- **ページ内検索**を使用して、現在のページビュー内で用語を検索します。

ページ内検索オプションの画像(/en-us/mobile-productivity-apps/media/worxweb-findinpage.png)

Secure Web は動的テキストもサポートしています。アプリは、ユーザーがデバイスで設定したフォントを表示します。

注：

- Citrix Files for XenMobile は July 1, 2023 に EOL に達しました。詳細については、[EOL および非推奨アプリ](#)を参照してください。

エンドポイント管理向け Citrix Content Collaboration™

Endpoint Management 向け Citrix Content Collaboration クライアントは、Citrix Files モバイルクライアントの MDX 対応バージョンです。これらのクライアントは、他の MDX ラップされたアプリのデータへの安全で統合されたアクセスを提供します。Endpoint Management 向け Citrix Content Collaboration クライアントは、マイクロ VPN、Secure Hub を使用したシングルサインオン (SSO)、2 要素認証などの MDX 機能の恩恵も受けます。

Citrix Files は、ユーザーがドキュメントを簡単かつ安全に交換できるエンタープライズファイル同期および共有サービスです。Citrix Files は、Citrix Files for Android Phone や Citrix Files for iPad などの Citrix Files モバイルクライアントを含む、さまざまなアクセスオプションをユーザーに提供します。

Citrix Files を Endpoint Management と統合して、Citrix Files の全機能セットを提供したり、ストレージゾーンコネクタへのアクセスのみを提供したりできます。デフォルトでは、Citrix Endpoint Management コンソールは Citrix Files の構成のみを有効にします。代わりにストレージゾーンコネクタで使用するよう Endpoint Management を構成するには、Citrix Endpoint Management ドキュメントの「[Endpoint Management で Citrix Content Collaboration を使用する](#)」を参照してください。

Endpoint Management 向け Citrix Content Collaboration クライアントを展開および管理するには、Endpoint Management、Citrix Files、ストレージゾーンコントローラ、および Citrix ADC を次のように使用します。

- Endpoint Management が Citrix Files で構成されている場合、Endpoint Management は SAML ID プロバイダー (IdP) として機能し、Endpoint Management 向け Citrix Content Collaboration クライアントを展開します。Citrix Files は Citrix Files データを管理します。Citrix Files データは Endpoint Management を経由しません。
- Endpoint Management が Citrix Files またはストレージゾーンコネクタで構成されている場合、ストレージゾーンコントローラはネットワーク共有および SharePoint のデータへの接続を提供します。ユーザーは Citrix Files モバイル生産性向上アプリを介して保存されたデータにアクセスします。ユーザーはモバイルデバイスから Microsoft Office ドキュメントを編集したり、Adobe PDF ファイルをプレビューしたり、注釈を付けたりできます。

- Citrix ADC は、外部ユーザーからの要求を管理し、接続を保護し、要求の負荷分散を行い、ストレージゾーンコネクタのコンテンツスイッチングを処理します。

Endpoint Management 向け Citrix Content Collaboration およびその他のモバイル生産性向上アプリのシステム要件については、「[モバイル生産性向上アプリのサポート](#)」を参照してください。

Endpoint Management 向け Citrix Content Collaboration クライアントが Citrix Files モバイルクライアントと異なる点

以下に、Endpoint Management 向け Citrix Content Collaboration クライアントと Citrix Files モバイルクライアントの違いについて説明します。

ユーザーアクセス

Endpoint Management 向け Citrix Content Collaboration クライアント:

ユーザーは Secure Hub から Endpoint Management 向け Citrix Content Collaboration クライアントを入手して開きます。

Citrix Files モバイルクライアント:

ユーザーはアプリストアからCitrix Filesモバイルクライアントを入手します。

SSO

シトリックス コンテンツ コラボレーション フォー エンドポイント マネジメント クライアント:

Endpoint ManagementとCitrix Filesの統合の場合：Citrix FilesのSAML IdPとしてEndpoint Managementを構成できます。この構成では、Secure HubはEndpoint ManagementをSAML IdPとして使用し、Citrix Content Collaboration for Endpoint Managementクライアント用のSAMLトークンを取得します。Citrix Content Collaboration for Endpoint Managementクライアントを起動したがSecure Hubにサインオンしていないユーザーは、Secure Hubへのサインオンを求められます。ユーザーはCitrix Filesのドメイン情報やアカウント情報を知る必要はありません。

Citrix Files モバイルクライアント:

Citrix FilesのSAML IdPとしてEndpoint ManagementとCitrix Gatewayを構成できます。この構成では、Webブラウザーまたは他のCitrix Filesクライアントを使用してCitrix Filesにログオンするユーザーは、ユーザー認証のためにEndpoint Management環境にリダイレクトされます。Endpoint Managementによる認証が成功すると、ユーザーはCitrix Filesアカウントへのログオンに有効なSAMLトークンを受け取ります。

マイクロVPN

シトリックス コンテンツ コラボレーション フォー エンドポイント マネジメント クライアント:

リモートユーザーは、Citrix Gatewayを介したVPNまたはマイクロVPN接続を使用して、社内ネットワーク内のアプリやデスクトップにアクセスできます。Endpoint ManagementとCitrix ADCの統合によって利用できるこの機能は、ユーザーには透過的です。

Citrix Files モバイルクライアント:

該当なし。

2要素認証

シトリックス コンテンツ コラボレーション エンドポイント マネジメント向けクライアント:

Endpoint ManagementとCitrix ADCの統合は、クライアント証明書認証と、LDAPやRADIUSなどの別の認証タイプを組み合わせた認証もサポートしています。

Citrix Files モバイルクライアント:

該当なし。

フォルダーのアクセス許可

Endpoint Management クライアント用Citrix Content CollaborationおよびCitrix Files モバイルクライアント:

Endpoint ManagementとCitrix Filesの統合の場合: Citrix Filesによって決定されます。

ドキュメントアクセス保護

エンドポイント マネジメント クライアント向けのシトリックス コンテンツ コラボレーション:

ユーザーは、Secure Mailで受信した添付ファイル、またはMDXでラップされたアプリによってダウンロードされた添付ファイルを開くことができます。ユーザーが「Open In」アクションを実行すると、MDXでラップされたアプリのみが表示されます。ラップされていないアプリからのデータは、Endpoint Managementクライアント用Citrix Content Collaborationでは利用できません。Secure Mailユーザーは、ファイルをデバイスにダウンロードすることなく、Citrix Filesリポジトリからファイルを添付できます。ユーザーがデバイス上でラップされたCitrix FilesとラップされていないCitrix Filesを使用している場合、ラップされたCitrix Filesクライアントは、ユーザーの個人用Citrix Filesアカウント内のファイルにアクセスできません。ラップされたCitrix Filesクライアントは、Endpoint Managementで構成されたCitrix Filesサブドメインにのみアクセスできます。

Citrix Files モバイルクライアント:

ユーザーは、任意のアプリから添付ファイルを開くことができます。

Citrix Files アカウントへのアクセス

エンドポイント マネジメント クライアント向けの シトリックス コンテンツ コラボレーション:

Endpoint Management と Citrix Files の統合の場合: 個人用 Citrix Files アカウントまたはサードパーティの Citrix Files アカウントにアクセスするには、ユーザーはデバイス上で MDX 以外のバージョンの Citrix Files を使用する必要があります。

Citrix Files モバイルクライアント:

Endpoint Management と Citrix Files の統合の場合: Citrix Files クライアントから利用できます。

デバイスポリシー

Citrix Content Collaboration for Endpoint Management クライアントおよび *Citrix Files* モバイルクライアント:

Endpoint Management と Citrix Files の両方のデバイスポリシーが、*Citrix Content Collaboration for Endpoint Management* クライアントに適用されます。たとえば、Endpoint Management コンソールからデバイスワイプを実行できます。Citrix Files コンソールから、Citrix Files アプリをリモートでワイプできます。

MDX ポリシー

エンドポイント管理向けシトリックス コンテンツコラボレーション クライアント:

MDX ポリシーを使用すると、Endpoint Management アプリストアが適用する Citrix Endpoint Management™ の設定を構成できます。MDX でのみ利用可能なポリシーには、カメラ、マイク、メール作成、スクリーンキャプチャ、クリップボードの切り取り、コピー、貼り付け操作をブロックする機能が含まれます。

Citrix Files モバイルクライアント:

該当なし。

データ暗号化

Citrix Content Collaboration for Endpoint Management クライアントおよび *Citrix Files* モバイルクライアント:

すべての保存データをAES-256で暗号化し、SSL 3.0と最低128ビット暗号化で転送中のデータを保護します。

可用性

エンドポイント管理向けシトリックス コンテンツコラボレーション クライアント:

Citrix Content Collaboration for Endpoint Managementクライアントは、Endpoint Management AdvancedおよびEnterpriseエディションに含まれています。

Citrix Files モバイルクライアント:

すべてのEndpoint Managementエディションには、すべてのCitrix Files機能が含まれています。Endpoint ManagementをCitrix Filesの全機能セットと統合することも、ストレージゾーンコネクタのみと統合することもできます。

Endpoint Managementクライアント向けCitrix Content Collaborationの統合と提供

Endpoint Managementクライアント向けCitrix Content Collaborationを統合して提供するには、以下の一般的な手順に従ってください。

1. Citrix FilesクライアントからCitrix FilesへのSSOを提供するために、Endpoint ManagementをCitrix FilesのSAML IdPとして有効にします。これを行うには、Endpoint ManagementでCitrix Filesアカウント情報を構成する必要があります。詳細については、「Endpoint ManagementでSSO用のCitrix Filesアカウント情報を構成するには」セクションを参照してください。

重要:

Citrix Files WebアプリやCitrix Files Syncクライアントなど、非MDX Citrix Filesクライアント向けにEndpoint ManagementをSAML IdPとして使用するには、追加の構成が必要です。

2. Citrix Filesクライアントをダウンロードします。
3. Citrix FilesクライアントをEndpoint Managementに追加します。詳細については、この記事の後半にある「Citrix FilesをEndpoint Managementに追加するには」を参照してください。
4. 構成を検証します。詳細については、この記事の後半にある「Citrix Filesクライアントを検証するには」を参照してください。

Endpoint ManagementでCitrix Filesを構成するための画像(/en-us/mobile-productivity-apps/media/configure-sharefile-endpointmanagement.png)

設定について:

- ドメインは、クライアントに使用されるCitrix Filesのサブドメインです。
- 選択されたDGのユーザーのみが、クライアントからCitrix FilesへのSSOアクセス権を持ちます。

DG内のユーザーがCitrix Filesアカウントを持っていない場合、Citrix FilesクライアントをEndpoint Managementに追加すると、Endpoint ManagementはそのユーザーをCitrix Filesにプロビジョニングします。

- Citrix Files管理者アカウントのログオン情報は、Endpoint ManagementがCitrix FilesコントロールプレーンにSAML設定を保存するために使用されます。

重要:

Citrix FilesクライアントからCitrix FilesへのSSOを有効にする構成では、ユーザーはネットワーク共有またはSharePointドキュメントライブラリに対して認証されません。これらのコネクタデータソースへのアクセスには、ネットワーク共有またはSharePointサーバーが存在するActive Directoryドメインへの認証が必要です。

SSOのためにEndpoint ManagementでCitrix Filesアカウント情報を構成するには

Secure Hubからモバイル生産性アプリへのSSOを有効にするには、Endpoint ManagementコンソールでCitrix FilesアカウントとCitrix Files管理者サービスアカウントの情報を指定します。この構成により、Endpoint Managementは、モバイル生産性アプリクライアント、Citrix Filesクライアント、および非MDX Citrix Filesクライアントに対して、Citrix FilesのSAML IdPとして機能します。ユーザーがモバイル生産性アプリクライアントを起動すると、Secure HubはEndpoint ManagementからユーザーのSAMLトークンを取得し、それをCitrix Filesクライアントに送信します。

Endpoint Managementコンソールで、**Configure > Content Collaboration** をクリックします。これはCitrix Filesの旧称です。

Endpoint ManagementにEndpoint Managementクライアント用のCitrix Content Collaborationを追加するには

Endpoint ManagementにEndpoint Managementクライアント用のCitrix Content Collaborationを追加すると、Endpoint Managementクライアント用のCitrix Content CollaborationからコネクタデータソースへのSSOアクセスを有効にできます。これを行うには、このセクションで説明されているように、ネットワークアクセスポリシーと優先VPNモードポリシーを構成します。

前提条件

- Endpoint ManagementはCitrix Filesサブドメインに到達できる必要があります。接続をテストするには、Endpoint ManagementサーバーからCitrix Filesサブドメインにpingを実行します。
- Citrix FilesアカウントとEndpoint Managementを実行しているハイパーバイザーに構成されているタイムゾーンは同じである必要があります。タイムゾーンが異なる場合、SAMLトークンが予期された時間内にCitrix Filesに到達しない可能性があるため、SSO要求が失敗することがあります。Endpoint ManagementのNTPサーバーを構成するには、Endpoint Managementコマンドラインインターフェイスを使用します。

注：

Hyper-Vホストは、Linux VMの時刻をUTCではなくローカルタイムゾーンに設定します。

- 管理者としてShareFileアカウントにログインし、**Settings > Admin Settings > Security > Login & Security Policy > Single sign-on / SAML 2.0 Configuration** でSAML SSO設定を確認します。
- Endpoint Managementクライアント用のCitrix Content Collaborationをダウンロードします。

手順：

- Endpoint Managementコンソールで、**Configure > Apps** をクリックし、次に **Add** をクリックします。
- 「**MDX**」をクリックします。
- アプリの**名前**、必要に応じて**説明**、**アプリカテゴリ**を入力します。
- 「**次へ**」をクリックし、Citrix Content Collaboration for Endpoint Managementクライアントの.mdxファイルをアップロードします。
- 「**次へ**」をクリックして、アプリ情報とポリシーを構成します。

Citrix Content Collaboration for Endpoint ManagementクライアントからCitrix FilesへのSSOを有効にする構成では、ユーザーはネットワーク共有またはSharePointドキュメントライブラリに対して認証されません。

6. Secure HubマイクロVPNとストレージゾーンコントローラーの間でSSOを有効にするには、以下のポリシー構成を完了します。

- ネットワークアクセス ポリシーを**内部ネットワークにトンネル化**に設定します。

このモードでは、MDXフレームワークはCitrix Content Collaboration for Endpoint Managementクライアントからのすべてのネットワークトラフィックを傍受します。その後、ネットワークトラフィックはアプリ固有のマイクロVPNを使用してCitrix Gateway経由でリダイレクトされます。

- **優先VPNモード** ポリシーを**トンネル化 - Web SSO**に設定します。

このトンネルモードでは、MDXフレームワークはMDXアプリからのSSL/HTTPトラフィックを終端し、その後、ユーザーに代わって内部接続への新しい接続を開始します。このポリシー設定により、MDXフレームワークはWebサーバーによって発行された認証チャレンジを検出して応答できます。

7. 必要に応じて、承認とデリバリーグループ（DG）の割り当てを完了します。

選択したDGのユーザーのみが、Citrix Content Collaboration for Endpoint ManagementクライアントからCitrix FilesへのSSOアクセス権を持ちます。DG内のユーザーがCitrix Filesアカウントを持っていない場合、Citrix Content Collaboration for Endpoint ManagementクライアントをEndpoint Managementに追加すると、Endpoint ManagementはユーザーをCitrix Filesにプロビジョニングします。

Citrix Content Collaboration for Endpoint Managementクライアントを検証するには

1. この記事で説明されている構成を完了した後、Citrix Content Collaboration for Endpoint Managementクライアントを起動します。Citrix Filesはサインオンを要求しません。
2. Secure Mailで、メールを作成し、Citrix Filesから添付ファイルを追加します。サインオンを要求されることなく、Citrix Filesのホームページが開きます。

注記:

- Citrix Files for XenMobile は July 1, 2023 をもって EOL となりました。詳細については、[EOLおよび非推奨アプリ](#)を参照してください。

EOLおよび非推奨のアプリ

以下のアプリは、End of Life (EOL) に達しているか、まもなくEOLステータスに達します。製品リリースがEOLに達した場合でも、製品ライセンス契約の条件内で製品を使用できますが、利用可能なサポートオプションは限られます。過去の情報は、ナレッジセンターまたはその他のオンラインリソースに掲載されています。ドキュメントは更新されなくなり、現状有姿で提供されます。製品ライフサイクルのマイルストーンの詳細については、[製品マトリックス](#)を参照してください。

注：

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

Citrix Files for XenMobile® (MDX): Citrix Files for XenMobileは、July 1, 2023にEOLに達しました。

お客様には、Apple App StoreおよびGoogle Playで入手可能なCitrix Filesを使用することをお勧めします。これはMAM SDKに対応しています。

Secure Mail for Intune SDK (iOS & Android): Secure Mailは、April 30, 2023にEOLに達しました。

Citrix Files for Intune: December 31, 2020に非推奨となりました。

Android Enterprise (Work Profileを使用) およびiOSユーザー登録を介して、通常のCitrix Filesアプリ (アプリストアで入手可能) をコンテナ化するためのプラットフォーム機能を活用するオプションを検討することをお勧めします。

ShareConnect: ShareConnectは、June 30, 2020にEOLに達しました。

Secure Notes: EOLライフサイクル終了日はDecember 31, 2018でした。

Secure NotesおよびSecure Tasksの機能が必要な場合は、MDXポリシーで保護できるサードパーティ製アプリであるNotate for Citrixをお勧めします。

Secure NotesおよびSecure TasksのユーザーがOutlookにデータを保存していた場合、Notateでそのデータにアクセスできます。ユーザーがShareFile (現在のCitrix Files) にデータを保存していた場合、データは移行されません。

ユーザーは、プラットフォームのオペレーティングシステムがユーザーインターフェイスのサポートを停止するまで、EOL日以降もSecure Notesを実行し続けることができます。ただし、サポートされていない製品を使用することはお勧めしません。

Secure Tasks: EOLライフサイクル終了日はDecember 31, 2018でした。

Secure Forms: EOLライフサイクル日付はMarch 31, 2018でした。お客様は、Citrix Files PlatinumおよびPremiumアカウントに含まれるCitrix ShareFile Workflowsへの移行をお勧めします。詳細については、[Citrix ShareFile Workflows](#)を参照してください。

ScanDirect: ScanDirectはSeptember 1, 2018にEOLに達しました。

Full VPN tunnel: EOL日は2021年9月でした。詳細については、Citrix Endpoint Management製品ドキュメントの[Deprecation](#)を参照してください。

Full VPN tunnel- Android: 2020年3月に非推奨になりました。EOL日は2021年9月でした。代替として、お客様にはMAM SDK Web SSOモードの使用をお勧めします。

Permit VPN mode switching - Android: 2020年3月に非推奨になりました。EOL日は2021年9月でした。

Inbound Document Exchange - Android: 2020年3月に非推奨になりました。EOL日は2021年9月でした。

Office 365アプリとの安全な対話を許可する

Citrix Secure Mail™、Citrix Secure Web、およびCitrix Filesは、MDXコンテナを開いて、ユーザーがドキュメントやデータをMicrosoft Office 365アプリに転送できるようにするオプションを提供します。この機能は、Endpoint Managementコンソールの「開く」ポリシーを通じて、iOSおよびAndroidプラットフォーム向けに管理します。

Microsoftアプリで開かれたデータは、MDXコンテナ内では保護または暗号化されなくなります。この機能を有効にする前に、セキュリティ上の影響を考慮してください。特に、データ損失防止に関心のあるお客様や、HIPAAまたはその他の厳格なコンプライアンス要件の対象となるお客様は、コンテナを開くことのトレードオフを検討する必要があります。

iOSでのOffice 365の有効化

- Secure Mail、Secure Web、またはCitrix Filesアプリの最新バージョンを[Endpoint Managementダウンロードページ](#)からダウンロードします。
- ファイルをEndpoint Managementコンソールにアップロードします。
- ドキュメント交換 (Open In) ポリシーを見つけて、制限付きに設定します。制限付きOpen-in例外 リストには、Microsoft Word、Excel、PowerPoint、OneNote、およびOutlookが自動的にリストされます。例: com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, a sub-navigation bar lists 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Apps' section is active, displaying a list of applications on the left, including 'MDX'. The 'MDX' application is selected, showing its configuration details on the right. The configuration includes a 'Document exchange (Open In)' dropdown set to 'Restricted', a 'Restricted Open-In exception list' with a text input field containing 'com.microsoft.Office.Word,c', and a 'Connection security level' dropdown set to 'TLS'. Each configuration item has a help icon (question mark) to its right.

MDM登録では、iOSデバイス向けにさらに多くの制御が利用可能です。

iTunesアプリをEndpoint Managementコンソールにアップロードし、デバイスにプッシュできます。このオプションを選択する場合は、以下のポリシーを**ON**に設定します。

- MDMプロファイルが削除された場合にアプリを削除する
- アプリデータのバックアップを防止する
- アプリを管理対象にするように強制する（選択的ワイプではアプリとすべてのデータが削除されることに注意してください）

ドキュメントやデータがMicrosoftアプリからデバイス上の管理対象外アプリに流れるのを防ぐには、Endpoint Managementコンソールで**構成 > デバイス > 制限 > iOS**に移動し、**管理対象アプリ**から**管理対象外アプリ**へのドキュメントと**管理対象外アプリ**から**管理対象アプリ**へのドキュメントを**OFF**に設定します。

AndroidでのOffice 365の有効化

1. Secure Mail、Secure Web、またはCitrix Filesアプリの最新バージョンを[Endpoint Managementダウンロードページ](#)からダウンロードします。
2. ファイルをEndpoint Managementコンソールにアップロードします。
3. **ドキュメント交換 (Open In)** ポリシーまでスクロールし、**制限**を選択します。
4. **制限付きOpen-in例外リスト**に、次のパッケージIDを追加します。

```
{package=com.microsoft.office.word} {package=com.microsoft.office.powerpoint}  
{package=com.microsoft.office.excel}
```

5. 他のアプリポリシーを通常どおり構成し、アプリを保存します。

ユーザーは、Secure Mail、Secure Web、またはCitrix Filesからファイルをデバイスに保存し、Office 365アプリでファイルを開く必要があります。

iOSとAndroidの両方で、ユーザーはデバイス上で次の種類のファイルを開いて編集できます。

サポートされているファイル形式

サポートされているファイル形式については、Microsoft Officeのドキュメントを参照してください。

業務用モバイルアプリのドキュメント履歴

次の表に、業務用モバイルアプリ製品のドキュメントに対する重要な変更点を示します。これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

日付	変更	説明
30 May 2025	Secure Mail for iOS 25.5.0のEAR	次のリリースのプレビュー
30 May 2025	Secure Web for iOS 25.5.0のEAR	次のリリースのプレビュー
21 May 2025	Secure Hub for Androidバージョン25.4.0のリリース	最新バージョンの新機能
02 Apr 2025	Secure Mail for Androidバージョン25.3.0のリリース	最新バージョンの新機能
02 Apr 2025	Secure Web for Androidバージョン25.3.0のリリース	最新バージョンの新機能
17 Feb 2025	Secure Mail for Androidバージョン25.1.0のリリース	最新バージョンの新機能
17 Feb 2025	Secure Hub for iOSバージョン25.1.0のリリース	最新バージョンの新機能
12 Feb 2025	Secure Mail for iOSバージョン25.1.0のリリース	最新バージョンの新機能
10 Feb 2025	Secure Hub for Androidバージョン25.1.0のリリース	最新バージョンの新機能
10 Feb 2025	Secure Web for iOSバージョン25.1.0のリリース	最新バージョンの新機能

日付	変更	説明
10 Feb 2025	Secure Web for Androidバージョン25.1.0のリリース	最新バージョンの新機能
09 Dec 2024	Secure Mail for iOSバージョン24.11.0のリリース	最新バージョンの新機能
09 Dec 2024	Secure Hub for iOSバージョン24.11.0のリリース	最新バージョンの新機能
06 Dec 2024	Secure Web for iOSバージョン24.11.0のリリース	最新バージョンの新機能
05 Dec 2024	Secure Mail for Androidバージョン24.11.0のリリース	最新バージョンの新機能
04 Dec 2024	Secure Mail for Android 24.11.0のEAR	次のリリースのプレビュー
04 Dec 2024	Secure Mail for iOS 24.11.0のEAR	次のリリースのプレビュー
26 Nov 2024	Secure Web for iOS 24.11.0のEAR	次のリリースのプレビュー
26 Nov 2024	Secure Hub for iOS 24.11.0のEAR	次のリリースのプレビュー
25 Nov 2024	新章：フィーチャーフラグ管理	フィーチャーフラグ管理
05 Nov 2024	Secure Hub for Androidバージョン24.10.0のリリース	最新バージョンの新機能
24 Oct 2024	Secure Hub for Android 24.10.0のEAR	次のリリースのプレビュー
22 Oct 2024	Secure Mail for Androidバージョン24.9.1のリリース	最新バージョンの新機能
15 Oct 2024	Secure Hub for iOSバージョン24.9.0のリリース	最新バージョンの新機能

日付	変更	説明
09 Oct 2024	Secure Web for Androidバージョン24.9.0のリリース	最新バージョンの新機能
09 Oct 2024	Secure Mail for Androidバージョン24.9.0のリリース	最新バージョンの新機能
09 Oct 2024	Secure Hub for iOS 24.9.0のEAR	次のリリースのプレビュー
27 Sep 2024	Secure Web for Android 24.9.0のEAR	次のリリースのプレビュー
27 Sep 2024	Secure Mail for Android 24.9.0のEAR	次のリリースのプレビュー
20 Sep 2024	Secure Mail for iOSバージョン24.9.0のリリース	最新バージョンの新機能
16 Sep 2024	Secure Web for iOSバージョン24.9.0のリリース	最新バージョンの新機能
06 Sep 2024	新しい機能でSecure Hub for Androidバージョン24.8.0のリリースを改訂	最新バージョンの新機能
04 Sep 2024	Secure Mail for iOS 24.9.0のEAR	次のリリースのプレビュー
03 Sep 2024	Secure Web for iOS 24.9.0のEAR	次のリリースのプレビュー
02 Sep 2024	Secure Hub for Androidバージョン24.8.0のリリース	最新バージョンの新機能
28 Aug 2024	Secure Web for Androidバージョン24.8.0のリリース	最新バージョンの新機能
23 Aug 2024	Secure Web for Androidバージョン24.8.0のEAR	次のリリースのプレビュー
21 Aug 2024	Secure Hub for Android version 24.8.0のEAR	次のリリースのプレビュー

日付	変更	説明
29 Jul 2024	Secure Mail for Androidバージョン24.7.0のリリース	Secure Mail 24.7.0：最新バージョンの新機能
16 Jul 2024	Secure Mail for Android 24.7.0のEAR	次のリリースのプレビュー
01 Jul 2024	Secure Hub for Androidバージョン24.6.0のリリース	Secure Hub 24.6.0：最新バージョンの新機能
06 May 2024	Secure Hub for iOSバージョン24.5.0のリリース	Secure Hub 24.5.0：最新バージョンの新機能
22 Apr 2024	新しい機能でSecure Hub for Androidバージョン24.3.0のリリースを改訂。	Secure Hub 24.3.0：最新バージョンの新機能
22 Apr 2024	新しい機能を追加して、Secure Hub for Androidバージョン23.12.0のリリースを改訂しました。	Secure Hub 23.12.0：最新バージョンの新機能
11 Apr 2024	Secure Hub for Androidバージョン24.3.0のリリース	Secure Hub 24.3.0：バグ修正
25 Mar 2024	Secure Web for iOSバージョン24.3.0のリリース	Secure Web 24.3.0：バグ修正
25 Mar 2024	Secure Mail for iOSバージョン24.3.0のリリース	Secure Mail 24.3.0：バグ修正
18 Mar 2024	Secure Web for Androidバージョン24.3.0のリリース	Secure Web 24.3.0：バグ修正
21 Feb 2024	Secure Web for iOSバージョン24.2.0のリリース	Secure Web 24.2.0：バグ修正
21 Feb 2024	Secure Web for iOSバージョン24.2.0のリリース	Secure Web 24.2.0：最新バージョンの新機能
21 Feb 2024	Secure Mail for iOSバージョン24.2.0のリリース	Secure Mail 24.2.0：バグ修正

日付	変更	説明
21 Feb 2024	Secure Mail for iOSバージョン24.2.0のリリース	Secure Mail 24.2.0：最新バージョンの新機能
19 Feb 2024	Secure Web for Androidバージョン24.1.0のリリース	Secure Web 24.1.0：バグ修正
19 Feb 2024	Secure Mail for Androidバージョン24.1.0のリリース	Secure Mail 24.1.0：バグ修正
19 Feb 2024	Secure Mail for Androidバージョン24.1.0のリリース	Secure Mail 24.1.0：最新バージョンの新機能
16 Jan 2024	Secure Hub for iOSバージョン24.1.0のリリース	Secure Hub 24.1.0：最新バージョンの新機能
16 Jan 2024	Secure Hub for iOSバージョン24.1.0のリリース	Secure Hub 24.1.0：バグ修正
16 Jan 2024	Secure Hub for Androidバージョン23.12.0のリリース	Secure Hub 23.12.0：最新バージョンの新機能とバグ修正
04 Dec 2023	画面を不鮮明にするドキュメントを追加	Secure Mail：画面の内容を不鮮明にする
28 Nov 2023	Secure Hub for iOSバージョン23.11.0のリリース	Secure Hub 23.11.0：最新バージョンの新機能
28 Nov 2023	Secure Hub for iOSバージョン23.11.0のリリース	Secure Hub 23.11.0：バグ修正
17 Nov 2023	Secure Web for Androidバージョン23.10.0のリリース	Secure Web 23.10.0：最新バージョンの新機能
17 Nov 2023	Secure Mail for Androidバージョン23.10.0のリリース	Secure Mail 23.10.0：バグ修正
27 Oct 2023	Secure Mail for Androidバージョン23.8.2のリリース	Secure Mail 23.8.2：最新バージョンの新機能
19 Oct 2023	Secure Hub for Androidバージョン23.10.0のリリース	Secure Hub 23.10.0：最新バージョンの新機能

日付	変更	説明
04 Oct 2023	Secure Mail for Androidバージョン23.7.0のリリース	Secure Mail 23.7.0：最新バージョンの新機能
04 Oct 2023	Secure Mail for iOSバージョン23.7.0のリリース	Secure Mail 23.7.0：最新バージョンの新機能
29 Sep 2023	Secure Mail for Androidバージョン23.8.1のリリース	Secure Mail 23.8.1：最新バージョンの新機能
20 Sep 2023	Secure Web for iOSバージョン23.9.0のリリース	Secure Web 23.9.0：最新バージョンの新機能
20 Sep 2023	Secure Mail for iOSバージョン23.9.0のリリース	Secure Mail 23.9.0：最新バージョンの新機能
20 Sep 2023	Secure Web for Androidバージョン23.8.0のリリース	Secure Web 23.8.0：最新バージョンの新機能
20 Sep 2023	Secure Mail for Androidバージョン23.8.0のリリース	Secure Mail 23.8.0：最新バージョンの新機能
01 Sep 2023	Secure Hub for Androidバージョン23.9.0のリリース	Secure Hub 23.9.0：最新バージョンの新機能
25 Aug 2023	Secure Hub for iOSバージョン23.8.1のリリース	Secure Hub 23.8.1：最新バージョンの新機能
08 Aug 2023	Secure Hub for iOSバージョン23.8.0のリリース	Secure Hub 23.8.0：最新バージョンの新機能
31 Jul 2023	Secure Web for Androidバージョン23.7.0のリリース	Secure Web 23.7.0：最新バージョンの新機能
31 Jul 2023	Secure Mail for Androidバージョン23.7.0のリリース	Secure Mail 23.7.0：最新バージョンの新機能
26 Jul 2023	Secure Hub for Androidバージョン23.7.0のリリース	Secure Hub 23.7.0：最新バージョンの新機能
07 Jul 2023	Secure Hub for iOSバージョン23.4.0のリリース	Secure Hub 23.4.0：最新バージョンの新機能

日付	変更	説明
22 Jun 2023	既知の問題CXM-110137を追加	Secure Mail for Androidの既知の問題
07 Jun 2023	Secure Mail for Androidバージョン23.6.0のリリース	Secure Mail 23.6.0：最新バージョンの新機能
31 May 2023	Secure Web for iOSバージョン23.5.0のリリース	Secure Web 23.5.0：最新バージョンの新機能
31 May 2023	Secure Mail for iOSバージョン23.5.0のリリース	Secure Mail 23.5.0：最新バージョンの新機能
26 May 2023	Secure Hub for Androidバージョン23.4.0のリリース	Secure Hub 23.4.0：最新バージョンの新機能
23 May 2023	Secure Hub for Androidバージョン23.2.0のリリース	Secure Hub 23.2.0：最新バージョンの新機能
12 Apr 2023	Secure Web for Androidバージョン23.3.5のリリース	既知の問題を追加
28 Mar 2023	Secure Web for Androidバージョン23.3.5のリリース	Secure Web 23.3.5：最新バージョンの新機能
28 Mar 2023	Secure Mail for Androidバージョン23.3.5のリリース	Secure Mail 23.3.5：最新バージョンの新機能
09 Jan 2023	Secure Hub for Androidバージョン22.11.0のリリース	Secure Hub 22.11.0：最新バージョンの新機能
01 Feb 2023	Secure Web for iOSおよびWecure Web for Androidバージョン23.2.0のリリース	Secure Web 23.2.0：最新バージョンの新機能
01 Feb 2023	Secure Mail for Androidバージョン23.2.0のリリース	Secure Mail 23.2.0：最新バージョンの新機能
28 Oct 2022	Secure Mail for Androidバージョン22.11.0のリリース	Secure Mail 22.11.0：最新バージョンの新機能
12 Oct 2022	Secure Hub for Androidバージョン22.9.0のリリース	Secure Hub 22.9.0：最新バージョンの新機能

日付	変更	説明
28 Sep 2022	Secure Mail for Androidバージョン22.9.0のリリース	Secure Mail 22.9.0：最新バージョンの新機能
28 Sep 2022	Secure Web for Androidバージョン22.9.0のリリース	Secure Web 22.9.0：最新バージョンの新機能
08 Sep 2022	Secure Web for iOSバージョン22.9.1のリリース	Secure Web 22.9.1：最新バージョンの新機能
07 Sep 2022	Secure Web for iOSバージョン22.9.0のリリース	Secure Web 22.9.0：最新バージョンの新機能
07 Sep 2022	Secure Mailバージョン22.9.0のリリース	Secure Mail 22.9.0：最新バージョンの新機能
01 Sep 2022	Secure Web for iOSバージョン22.9.0のリリース	Secure Web 22.9.0は、2022年9月2日にロールバックされました。現在、プログラムの修正に取り組んでおり、近日中に修正リリースを発表する予定です
01 Sep 2022	Secure Mailバージョン22.9.0のリリース	Secure Mail 22.9.0は、2022年9月2日にロールバックされました。現在、プログラムの修正に取り組んでおり、近日中に修正リリースを発表する予定です。
26 Jul 2022	Secure Hub for Androidバージョン22.7.0のリリース	Secure Hub 22.7.0：最新バージョンの新機能
13 Jul 2022	Secure Web for iOSバージョン22.6.0のリリース	Secure Web 22.6.0：最新バージョンの新機能
14 Jun 2022	Secure Mailバージョン22.6.0のリリース	Secure Mail 22.6.0：最新バージョンの新機能
14 Jun 2022	Secure Web for Androidバージョン22.6.0のリリース	Secure Web 22.6.0：最新バージョンの新機能

日付	変更	説明
14 Jun 2021	Secure Hub for Androidバージョン22.6.0のリリース	Secure Hub 22.6.0：最新バージョンの新機能
09 Feb 2022	Secure Mailバージョン22.2.0のリリース	Secure Mail 22.2.0：最新バージョンの新機能
09 Feb 2022	Secure Webバージョン22.2.0のリリース	Secure Web 22.2.0：最新バージョンの新機能
08 Dec 2021	Secure Mailバージョン21.12.0のリリース	Secure Mail 21.12.0：最新バージョンの新機能
08 Dec 2021	Secure Webバージョン21.12.0のリリース	Secure Web 21.12.0：最新バージョンの新機能
27 Oct 2021	Secure Mailバージョン21.10.5のリリース	Secure Mail 21.10.5：最新バージョンの新機能
27 Oct 2021	Secure Webバージョン21.10.5のリリース	Secure Web 21.10.5：最新バージョンの新機能
13 Oct 2021	Secure Hubバージョン21.10.0のリリース	Secure Hub 21.10.0：最新バージョンの新機能
13 Oct 2021	Secure Mailバージョン21.10.0のリリース	Secure Mail 21.10.0：最新バージョンの新機能
13 Oct 2021	Secure Webバージョン21.10.0のリリース	Secure Web 21.10.0：最新バージョンの新機能
20 Sep 2021	Secure Mailバージョン21.9.1のリリース	Secure Mail 21.9.1：最新バージョンの新機能
20 Sep 2021	Secure Webバージョン21.9.1のリリース	Secure Web 21.9.1：最新バージョンの新機能
08 Sep 2021	Secure Mailバージョン21.9.0のリリース	Secure Mail 21.9.0：最新バージョンの新機能
08 Sep 2021	Secure Webバージョン21.9.0のリリース	Secure Web 21.9.0：最新バージョンの新機能

日付	変更	説明
24 Aug 2021	Secure Mail for Androidバージョン21.8.5のリリース	Secure Mail 21.8.5：最新バージョンの新機能
24 Aug 2021	Secure Web for Androidバージョン21.8.5のリリース	Secure Web 21.8.5：最新バージョンの新機能
13 Aug 2021	Secure Hub for iOSバージョン21.8.0のリリース	Secure Hub 21.8.0：最新バージョンの新機能
13 Aug 2021	Secure Mailバージョン21.8.0のリリース	Secure Mail 21.8.0：最新バージョンの新機能
13 Aug 2021	Secure Webバージョン21.8.0のリリース	Secure Web 21.8.0：最新バージョンの新機能
10 Aug 2021	Secure Hub for Androidバージョン21.7.1のリリース	Secure Hub 21.7.1：最新バージョンの新機能
15 Jul 2021	Secure Mailバージョン21.7.0のリリース	Secure Mail 21.7.0：最新バージョンの新機能
15 Jul 2021	Secure Webバージョン21.7.0のリリース	Secure Web 21.7.0：最新バージョンの新機能
07 Jul 2021	Secure Hub for iOSバージョン21.7.0のリリース	Secure Hub 21.7.0：最新バージョンの新機能
06 Jul 2021	Secure Hub for Androidバージョン21.7.0のリリース	Secure Hub 21.7.0：最新バージョンの新機能
24 Jun 2021	Secure Mail for iOSバージョン21.6.0のリリース	Secure Mail 21.6.0：最新バージョンの新機能
16 Jun 2021	Secure Hubバージョン21.6.0のリリース	Secure Hub 21.6.0：最新バージョンの新機能
16 Jun 2021	Secure Mail for Androidバージョン21.6.0のリリース	Secure Mail 21.6.0：最新バージョンの新機能
16 Jun 2021	Secure Webバージョン21.6.0のリリース	Secure Web 21.6.0：最新バージョンの新機能

日付	変更	説明
20 May 2021	Secure Hubバージョン21.5.1のリリース	Secure Hub 21.5.1：最新バージョンの新機能
12 May 2021	Secure Hubバージョン21.5.0のリリース	Secure Hub 21.5.0：最新バージョンの新機能
12 May 2021	Secure Mailバージョン21.5.0のリリース	Secure Mail 21.5.0：最新バージョンの新機能
12 May 2021	Secure Web for iOSバージョン21.5.0のリリース	Secure Web 21.5.0：バグ修正
04 May 2021	Secure Mail for Androidバージョン21.4.5のリリース	Secure Mail 21.4.5：最新バージョンの新機能
04 May 2021	Secure Web for Androidバージョン21.4.5のリリース	Secure Web 21.4.5：バグ修正
15 Apr 2021	Secure Hubバージョン21.4.0のリリース	Secure Hub 21.4.0：最新バージョンの新機能
15 Apr 2021	Secure Mail for iOSバージョン21.4.0のリリース	Secure Mail 21.4.0：バグ修正
31 Mar 2021	Secure Hub for iOSバージョン21.3.2のリリース	Secure Hub 21.3.2：バグ修正
30 Mar 2021	Secure Mail for Androidバージョン21.3.5のリリース	Secure Mail 21.3.5：最新バージョンの新機能
30 Mar 2021	Secure Web for Androidバージョン21.3.5のリリース	Secure Web 21.3.0：バグ修正
22 Mar 2021	Secure Mail for iOSバージョン21.3.0のリリース	Secure Mail 21.3.0：最新バージョンの新機能
17 Mar 2021	Secure Hubバージョン21.3.0のリリース	Secure Hub 21.3.0：バグ修正
17 Mar 2021	Secure Mail for Androidバージョン21.3.0のリリース	Secure Mail 21.3.0：最新バージョンの新機能

日付	変更	説明
17 Mar 2021	Secure Web for Androidバージョン21.3.0のリリース	Secure Web 21.3.0：バグ修正
24 Feb 2021	Secure Mailバージョン21.2.0のリリース	Secure Mail 21.2.0：最新バージョンの新機能
24 Feb 2021	Secure Webバージョン21.2.0のリリース	Secure Web 21.2.0：最新バージョンの新機能
18 Feb 2021	Secure Hub for Androidバージョン21.2.0のリリース	Secure Hub 21.2.0：バグ修正
01 Feb 2021	Secure Mail for iOSバージョン21.1.5のリリース	Secure Mail 21.1.5：バグ修正
01 Feb 2021	Secure Web for iOSバージョン21.1.5のリリース	Secure Web 21.1.5：バグ修正
14 Jan 2021	Secure Mailバージョン21.1.0のリリース	Secure Mail 21.1.0：バグ修正
14 Jan 2021	Secure Webバージョン21.1.0のリリース	Secure Web 21.1.0：バグ修正
12 Jan 2021	Secure Hubバージョン21.1.0のリリース	Secure Web 21.1.0：バグ修正
15 Dec 2020	Secure Hubバージョン20.12.0のリリース	Secure Hub 20.12.0：最新バージョンの新機能
15 Dec 2020	Secure Mail for iOSバージョン20.12.0のリリース	Secure Mail 20.12.0：バグ修正
15 Dec 2020	Secure Web for iOSバージョン20.12.0のリリース	Secure Web 20.12.0：バグ修正
19 Nov 2020	Secure Hub for Androidバージョン20.11.0のリリース	Secure Hub 20.11.0：最新バージョンの新機能
19 Nov 2020	Secure Mail for Androidバージョン20.11.0のリリース	Secure Mail 20.11.0：最新バージョンの新機能

日付	変更	説明
19 Nov 2020	Secure Web for Androidバージョン20.11.0のリリース	Secure Web 20.11.0：バグ修正
17 Nov 2020	Secure Mail for iOSバージョン20.11.0のリリース	Secure Mail 20.11.0：最新バージョンの新機能
17 Nov 2020	Secure Web for iOSバージョン20.11.0のリリース	Secure Web 20.11.0：バグ修正
27 Oct 2020	Secure Mailバージョン20.10.5のリリース	Secure Mail 20.10.5：最新バージョンの新機能
27 Oct 2020	Secure Web for Androidバージョン20.10.5のリリース	Secure Web 20.10.5：最新バージョンの新機能
27 Oct 2020	Secure Hub for iOSバージョン20.10.5のリリース	Secure Hub 20.10.5：バグ修正
21 Oct 2020	Secure Hub for Androidバージョン20.10.5のリリース	Secure Hub 20.10.5：バグ修正
15 Oct 2020	Secure Mailバージョン20.10.0のリリース	Secure Mail 20.10.0：最新バージョンの新機能
15 Oct 2020	Secure Web for Androidバージョン20.10.0のリリース	Secure Mail 20.10.0：最新バージョンの新機能
29 Sep 2020	Secure Mail for Androidバージョン20.9.5のリリース	Secure Mail 20.9.5：バグ修正
29 Sep 2020	Secure Web for iOSバージョン20.9.5のリリース	Secure Web 20.9.5：バグ修正
17 Sep 2020	Secure Mailバージョン20.9.0のリリース	Secure Mail 20.9.0：バグ修正
17 Sep 2020	Secure Web for Androidバージョン20.9.0のリリース	Secure Web 20.9.0：最新バージョンの新機能
04 Sep 2020	Secure Hubバージョン20.9.0のリリース	Secure Hub 20.9.0：最新バージョンの新機能

日付	変更	説明
27 Aug 2020	Secure Mailバージョン20.8.5のリリース	Secure Mail 20.8.5：最新バージョンの新機能
27 Aug 2020	Secure Webバージョン20.8.5のリリース	Secure Web 20.8.5：最新バージョンの新機能
20 Aug 2020	Secure Hubバージョン20.7.5のリリース	Secure Hub 20.7.5：最新バージョンの新機能
19 Aug 2020	Secure Mailバージョン20.8.0のリリース	Secure Mail 20.8.0：最新バージョンの新機能
19 Aug 2020	Secure Webバージョン20.8.0のリリース	Secure Web 20.8.0：最新バージョンの新機能
12 Aug 2020	Citrix ShareConnectは製品終了（EOL）となりました。	詳しくは、「製品マトリクス」の製品ライフサイクルのマイルストーンを参照してください。
29 Jul 2020	Secure Mailバージョン20.7.5のリリース	Secure Mail 20.7.5：最新バージョンの新機能
29 Jul 2020	Secure Webバージョン20.7.5のリリース	Secure Web 20.7.5：バグ修正
14 Jul 2020	Secure Mailバージョン20.7.0のリリース	Secure Mail 20.7.0：バグ修正
14 Jul 2020	Secure Webバージョン20.7.0のリリース	Secure Web 20.7.0：最新バージョンの新機能
10 Jul 2020	iOSデバイスで構成されたプロキシが、Wi-Fi設定で構成されたプロキシサーバーを使用できるようになりました。	「Secure Hubの新機能」を参照してください
06 Jul 2020	アプリが32ビット版から64ビット版へ移行。AndroidデバイスをSecure Hubバージョン20.6.5にアップグレードすると、以降のバージョンに	「Secure Hubの新機能」を参照してください

日付	変更	説明
	アップグレードするときの再認証を回避できます。	
01 Jul 2020	Secure Hubバージョン20.6.5のリリース	Secure Hub 20.6.5： バグ修正
01 Jun 2020	Secure Mailバージョン20.6.5のリリース	Secure Mail 20.6.5： バグ修正
19 Jun 2020	QuickEditのプラットフォーム暗号化	詳しくは、「 QuickEditの暗号化 」を参照してください。
16 Jun 2020	Secure Mailバージョン20.6.0のリリース	Secure Mail 20.6.0： バグ修正
16 Jun 2020	Secure Webバージョン20.6.0のリリース	Secure Web 20.6.0： バグ修正
02 Jun 2020	MDX暗号化の製品終了が近づいています。2020年9月1日までに、すべてのデバイスをプラットフォーム暗号化に移行する必要があります。	詳しくは、「 最新の情報 」を参照してください。
19 May 2020	Secure Mail for iOSバージョン20.5.0のリリース	Secure Mail 20.5.0： バグ修正
19 May 2020	Secure Web for iOSバージョン20.5.0のリリース	Secure Web 20.5.0： バグ修正
11 May 2020	Secure Mail for iOSバージョン20.4.5のリリース	Secure Mail 20.4.5： 最新バージョンの新機能
11 May 2020	Secure Web for iOSバージョン20.4.5のリリース	Secure Web 20.4.5： 最新バージョンの新機能
28 Apr 2020	Secure Mail for Androidバージョン20.4.5のリリース	Secure Mail 20.4.5： 最新バージョンの新機能
28 Apr 2020	Secure Web for Androidバージョン20.4.5のリリース	Secure Web 20.4.5： バグ修正

日付	変更	説明
21 Apr 2020	Secure Mail for iOSバージョン20.4.0のリリース	Secure Mail 20.4.0：最新バージョンの新機能
21 Apr 2020	Secure Web for iOSバージョン20.4.0のリリース	Secure Web 20.4.0：バグ修正
14 Apr 2020	Secure Mail for Androidバージョン20.4.0のリリース	Secure Mail 20.4.0：最新バージョンの新機能
14 Apr 2020	Secure Web for Androidバージョン20.4.0のリリース	Secure Web 20.4.0：バグ修正
31 Mar 2020	Secure Hub for iOSバージョン20.3.0のリリース	Secure Hub 20.3.0：最新バージョンの新機能
24 Mar 2020	Secure Mailバージョン20.3.0のリリース	Secure Mail 20.3.0：最新バージョンの新機能
24 Mar 2020	Secure Webバージョン20.3.0のリリース	Secure Web 20.3.0：バグ修正
11 Feb 2020	Secure Hub for iOSバージョン20.2.0のリリース	Secure Hub 20.2.0：バグ修正
11 Feb 2020	Secure Mailバージョン20.2.0のリリース	Secure Mail 20.2.0：最新バージョンの新機能
29 Jan 2020	Secure Hubバージョン20.1.5のリリース	Secure Hub 20.1.5：バグ修正
29 Jan 2020	Secure Mailバージョン20.1.5のリリース	Secure Mail 20.1.5：最新バージョンの新機能
07 Jan 2020	Secure Mailバージョン20.1.0のリリース	Secure Mail 20.1.0：最新バージョンの新機能
12 Dec 2019	Secure Hubバージョン19.12.5のリリース	Secure Hub 19.12.5：バグ修正
12 Dec 2019	Secure Mailバージョン19.12.5のリリース	Secure Mail 19.12.5：最新バージョンの新機能

日付	変更	説明
12 Dec 2019	Secure Webバージョン 19.10.5のリリース	Secure Web 19.12.5：バグ修正
13 Nov 2019	Secure Mailバージョン 19.11.5のリリース	Secure Mail 19.11.5：最新バージョンの新機能
13 Nov 2019	Secure Webバージョン 19.11.5のリリース	Secure Web 19.11.5：バグ修正
06 Nov 2019	Secure Hubバージョン 19.11.5のリリース	Secure Hub 19.11.5：バグ修正
22 Oct 2019	Secure Mail for iOSバージョン 19.10.6のリリース	Secure Mail for iOS 19.10.6：バグ修正
15 Oct 2019	Secure Mailバージョン 19.10.5のリリース	Secure Mail 19.10.5：最新バージョンの新機能
15 Oct 2019	Secure Webバージョン 19.10.5のリリース	Secure Web 19.10.5：バグ修正
14 Oct 2019	Secure Hub for Androidバージョン 19.10.5のリリース	Secure Hub 19.10.5：最新バージョンの新機能
03 Oct 2019	Secure Hub for iOSバージョン 19.10.0のリリース	Secure Hub 19.10.0：バグ修正
03 Oct 2019	Secure Mail for iOSバージョン 19.10.0のリリース	Secure Mail 19.10.0：最新バージョンの新機能
03 Oct 2019	Secure Web for iOSバージョン 19.10.0のリリース	Secure Web 19.10.0：最新バージョンの新機能
01 Oct 2019	Secure Mail for Androidバージョン 19.10.0のリリース	Secure Mail 19.10.0：最新バージョンの新機能
01 Oct 2019	Secure Web for Androidバージョン 19.10.0のリリース	Secure Web 19.10.0：最新バージョンの新機能
24 Sep 2019	Secure Hub for Androidバージョン 19.10.0のリリース	Secure Hub 19.10.0：バグ修正

日付	変更	説明
19 Sep 2019	Secure Mail for iOSバージョン19.9.5のリリース	Secure Mail 19.9.5：最新バージョンの新機能
19 Sep 2019	Secure Web for iOSバージョン19.9.5のリリース	Secure Web 19.9.5：バグ修正
17 Sep 2019	Secure Mail for Androidバージョン19.9.5のリリース	Secure Mail 19.9.5：最新バージョンの新機能
17 Sep 2019	Secure Web for Androidバージョン19.9.5のリリース	Secure Web 19.9.5：最新バージョンの新機能
11 Sep 2019	Secure Hub for Androidバージョン19.9.5のリリース	Secure Hub 19.9.5：最新バージョンの新機能
04 Sep 2019	Secure Mailバージョン19.9.0のリリース	Secure Mail 19.9.0：最新バージョンの新機能
04 Sep 2019	Secure Webバージョン19.9.0のリリース	Secure Web 19.9.0：最新バージョンの新機能
03 Sep 2019	Secure Hubバージョン19.9.0のリリース	Secure Hub 19.9.0：最新バージョンの新機能
23 Aug 2019	Secure Hubバージョン19.8.5のリリース	Secure Hub 19.8.5：最新バージョンの新機能
23 Aug 2019	Secure Mail for Androidバージョン19.8.5のリリース	Secure Mail 19.8.5：パフォーマンスの向上とバグの修正
23 Aug 2019	Secure Web for Androidバージョン19.8.5のリリース	Secure Web 19.8.5：パフォーマンスの向上とバグの修正
09 Aug 2019	Secure Mail for Androidバージョン19.8.0のリリース	Secure Mail 19.8.0：最新バージョンの新機能
09 Aug 2019	Secure Web for Androidバージョン19.8.0のリリース	Secure Web 19.8.0：パフォーマンスの向上とバグの修正

日付	変更	説明
31 Jul 2019	Secure Hubバージョン19.8.0のリリース	Secure Hub 19.8.0：最新バージョンの新機能
02 Aug 2019	Secure Mail for iOSバージョン19.8.0のリリース	Secure Mail 19.8.0：最新バージョンの新機能
02 Aug 2019	Secure Web for iOSバージョン19.8.0のリリース	Secure Web 19.8.0：パフォーマンスの向上とバグの修正
18 Jul 2019	Secure Hubバージョン19.7.5のリリース	Secure Hub 19.7.5：最新バージョンの新機能
18 Jul 2019	Secure Mailバージョン19.7.5のリリース	Secure Mail 19.7.5：最新バージョンの新機能
18 Jul 2019	Secure Webバージョン19.7.5のリリース	Secure Web 19.7.5：パフォーマンスの向上とバグの修正
30 Jun 2019	Secure Hub for iOSバージョン19.6.6のリリース	Secure Hub for iOS 19.6.6：パフォーマンスの向上とバグの修正
27 Jun 2019	Secure Mail 19.6.5 for Androidの新機能一覧	Secure Mail 19.6.5：最新バージョンの新機能
27 Jun 2019	Secure Webバージョン19.6.5のリリース	Secure Web 19.6.5：パフォーマンスの向上とバグの修正
26 Jun 2019	Secure Hubバージョン19.6.5のリリース	Secure Hub 19.6.5：既知の問題
17 Jun 2019	Secure Mail 19.5.5 for iOSの新機能一覧	Secure Mail 19.5.5：最新バージョンの新機能
05 Jun 2019	Secure Hub for Android、Secure Mail for Android、Secure Web for Androidバージョン19.5.5のリリース	Secure MailとSecure Webの段階的リリースプロセスについては、「業務用モバイルア

日付	変更	説明
		プリのリリーススケジュール 」を参照してください。
23 May 2019	Secure Mail for Androidでの下書きの同期機能に関するビデオ（1分）	バージョン19.5.0でリリースされたSecure Mail for Androidの下書きフォルダー同期機能に関するビデオを追加しました： 下書きフォルダーの自動同期
08 May 2019	Secure Hubバージョン19.5.0のリリース	Secure Hub 19.5.0での 既知の問題と解決された問題
08 May 2019	Secure Mailバージョン19.5.0のリリース	Secure Mail 19.5.0： 解決された問題
08 May 2019	Secure Web 19.5.0のリリース	Secure Web 19.5.0で 解決された問題
05 Apr 2019	Secure Hubバージョン19.3.5のリリース	Secure Hub 19.3.5での 既知の問題と解決された問題
05 Apr 2019	Secure Mailバージョン19.3.5のリリース	Secure Mail 19.3.5： 解決された問題
05 Apr 2019	Secure Webバージョン19.3.5のリリース	Secure Web 19.3.5で 解決された問題