



Secure Hub

Contents

シトリックス セキュアハブ™	19
Secure Hubの管理	19
シトリックス PIN	19
証明書ピンニング	20
Secure Hub の証明書 + ワンタイムパスワード認証の構成	21
AndroidデバイスのADS接続のポート要件	24
Secure Hub の機能	26
シトリックス セキュアハブ™	29
現在のバージョンでの新機能	29
iOS版セキュアハブ 26.8.1	29
Android版セキュアハブ 26.8.0	29
COSUモードのランチャー構成ポリシーで自動起動アプリを設定する	29
MDMデバイス証明書の自動検出と更新	30
以前のバージョンの新機能	30
iOS版セキュアハブ 26.8.0	30
iOS/iPadOS 27のサポート	30
Android版セキュアハブ 26.5.0	30
Android 17のサポート	30
Android版セキュアハブ 26.2.0	30
デバイス証明書のトラブルシューティングの強化	30
iOS版 セキュアハブ 25.8.0	31
iOS 26のサポート	31
Android版 セキュアハブ 25.10.0	31
16KBメモリページサイズのサポート	31
Android版 セキュアハブ 25.7.0	31
iOS版 セキュアハブ 25.6.0	31

Android 用 セキュアハブ 25.4.0	32
Android 16のサポート	32
TLS 1.3プロトコルのサポート	32
Android 用 セキュアハブ 25.1.0	32
iOS 用 セキュアハブ 25.1.0	32
iOS向け セキュアハブ 24.11.0	32
Android向け セキュアハブ 24.10.0	33
Android 15 のサポート	33
iOS向け セキュアハブ 24.9.0	33
デバイス登録プログラムで利用規約を表示	33
Android向け セキュアハブ 24.8.0	33
Android デバイスでのコンプライアンスチェック (テクニカルプレビュー)	33
アンドロイド用 セキュアハブ 24.6.0	34
ログ収集とレポート機能の改善	34
iOS 用 セキュアハブ 24.5.0	35
iOS 17 の Return to Service に対応	35
アンドロイド用 セキュアハブ 24.3.0	35
サムスンノックス エンハンスド アテステーション バージョン3 に対応	35
アンドロイド用 セキュアハブ 23.12.0	36
Samsung Knoxによるセキュリティ強化	36
ユーザーの個人プロファイルからSecure Mailにアクセスする	36
iOS版 セキュアハブ 24.1.0	37
Android版 セキュアハブ 23.12.0	37
サインインページに認証PINに関するヒントを追加する	37
nFactor認証はシングルサインオン機能をサポート	38
ダイレクトブートモードでの完全ワイプをサポート	38
Secure HubのApp Storeの読み込み速度を最適化	38
iOS用 セキュアハブ 23.11.0	38

サインインページに認証PINに関するヒントを追加	38
nFactor認証がシングルサインオン機能をサポート	38
セキュアハブ 23.10.0	39
Android向けセキュアハブ	39
セキュアハブ 23.9.0	39
Android版 セキュアハブ	39
セキュアハブ 23.8.1	39
iOS用セキュアハブ	39
セキュアハブ 23.8.0	39
iOS用セキュアハブ	39
セキュアハブ 23.7.0	39
Android用セキュアハブ	39
セキュアハブ 23.4.0	40
iOS用セキュアハブ	40
セキュアハブ 23.4.1	41
Android 用セキュアハブ	41
セキュアハブ 23.4.0	41
Android 用セキュアハブ	41
セキュアハブ 23.2.0	41
Android 用セキュアハブ	41
セキュアハブ 22.11.0	42
Android 用 セキュアハブ	42
セキュアハブ 22.9.0	42
Android 用 セキュアハブ	42
セキュアハブ 22.7.0	43
Android版 セキュアハブ	43
セキュアハブ 22.6.0	44
Android版 セキュアハブ	44

セキュアハブ 22.5.0	44
iOS版 セキュアハブ	44
セキュアハブ 22.4.0	44
Android版 セキュアハブ	44
セキュアハブ 22.2.0	44
iOS用セキュアハブ	44
Android用セキュアハブ	44
セキュアハブ 21.11.0	44
Android用セキュアハブ	44
セキュアハブ 21.10.0	44
iOS用セキュアハブ	44
Android用セキュアハブ	45
セキュアハブ 21.8.0	45
iOS 用セキュアハブ	45
セキュアハブ 21.7.1	45
Android 用セキュアハブ	45
セキュアハブ 21.7.0	45
iOS 用セキュアハブ	45
Android 用セキュアハブ	45
セキュアハブ 21.6.0	46
iOS版セキュアハブ	46
Android版セキュアハブ	46
セキュアハブ 21.5.1	46
iOS版セキュアハブ	46
Android版セキュアハブ	46
セキュアハブ 21.5.0	46
iOS版セキュアハブ	46
セキュアハブ 21.4.0	46

セキュアハブ 21.3.2	46
iOS用セキュアハブ	46
セキュアハブ 21.3.0	46
セキュアハブ 21.2.0	47
Android用セキュアハブ	47
セキュアハブ 21.1.0	47
iOS用セキュアハブ	47
Android用セキュアハブ	47
セキュアハブ 20.12.0	47
iOS用セキュアハブ	47
Android向けセキュアハブ	47
セキュアハブ 20.11.0	47
Android向けセキュアハブ	47
セキュアハブ 20.10.5	47
セキュアハブ 20.9.0	47
iOS向けセキュアハブ	47
Android向けセキュアハブ	48
セキュアハブ 20.7.5	48
Android向けセキュアハブ	48
セキュアハブ 20.6.5	48
Android版セキュアハブ	48
iOS向けセキュアハブ	49
セキュアハブ 20.3.0	49
iOS向けセキュアハブ	49
セキュアハブ 20.2.0	50
iOS版 セキュアハブ	50
セキュアハブ 20.1.5	50
セキュアハブ 19.12.5	50

セキュアハブ 19.11.5	50
Secure Hub バージョン 19.10.5	50
Android版 Secure Hub	50
セキュアハブ 19.10.0	50
セキュアハブ 19.9.5	50
iOSデバイス用のSecure Hub	50
Androidデバイス用のSecure Hub	50
セキュアハブ 19.9.0	51
iOS版セキュアハブ	51
セキュアハブ Android版	51
セキュアハブ Android版 19.8.5	51
セキュアハブ 19.8.0	51
iOS用セキュアハブ	51
Android版セキュアハブ	51
Secure Hub バージョン 19.7.5	51
iOS向けセキュアハブ	51
Android向けセキュアハブ	52
Secure Hub 19.3.5から19.6.6	52
セキュアハブ 19.3.0	52
セキュアハブ 19.2.0	52
セキュアハブ 19.1.5	52
セキュアハブ 19.1.0	53
セキュアハブ 18.12.0	53
セキュアハブ 18.11.5	53
セキュアハブ 18.10.0	53
Secure Hub 10.8.60から18.9.0	53
セキュアハブ 10.8.60	54
セキュアハブ 10.8.55	55

Secure Hubの管理	55
シトリックス ピン	56
証明書のピン留め	57
証明書 + ワンタイムパスワード認証	58
AndroidデバイスのADS接続に必要なポート	61
アカウント削除オプションの無効化	63
Secure Hubの使用	63
Secure Mailへの自動登録	65
カスタマイズされたストア	66
構成済みのヘルプオプション	67
位置情報ポリシー	68
クラッシュの収集と分析	68
Secure Hubのデバイス側ログを生成する	69
既知の解決済み問題	70
iOS用セキュアハブ 26.8.1	70
解決済みの問題	70
既知の問題	70
Android用セキュアハブ 26.8.0	70
解決済みの問題	70
既知の問題	70
iOS用セキュアハブ 26.8.0	71
修正された問題	71
既知の問題	71
Android用 セキュアハブ 26.5.0	71
修正された問題	71
既知の問題	71
Android 用 セキュアハブ 26.2.0	72
修正された問題	72

既知の問題	72
Android 用 セキュアハブ 25.10.0	72
修正された問題	72
既知の問題	72
iOS 用 セキュアハブ 25.8.0	72
修正された問題	72
既知の問題	72
Android 用 セキュアハブ 25.7.0	73
修正された問題	73
既知の問題	73
iOS 用 セキュアハブ 25.6.0	73
修正された問題	73
既知の問題	73
アンドロイド向けセキュアハブ 25.4.0	73
修正された問題	73
既知の問題	73
iOS 向け Secure Hub 25.1.0	74
修正された問題	74
既知の問題	74
アンドロイド向けセキュアハブ 25.1.0	74
修正された問題	74
既知の問題	74
iOS版セキュアハブ 24.11.0	74
修正された問題	74
既知の問題	74
Android版セキュアハブ 24.10.0	74
修正された問題	74
既知の問題	74

iOS版セキュアハブ 24.9.0	75
修正された問題	75
既知の問題	75
Android用 セキュアハブ 24.8.0	75
修正された問題	75
既知の問題	75
Android 用 セキュアハブ 24.6.0	75
修正された問題	75
既知の問題	75
iOS 用 セキュアハブ 24.5.0	75
修正された問題	75
既知の問題	75
Android用セキュアハブ 24.3.0	76
修正された問題	76
既知の問題	76
iOS用セキュアハブ 24.1.0	76
修正された問題	76
Android 版 セキュアハブ 23.12.0	77
修正された問題	77
iOS 版 セキュアハブ 23.11.0	77
修正された問題	77
Android 用 セキュアハブ 23.10.0	77
修正された問題	77
既知の問題	77
Android 用 セキュアハブ 23.9.0	78
修正された問題	78
既知の問題	78
iOS 用 セキュアハブ 23.8.1	78

修正された問題	78
既知の問題	78
iOS 用 セキュアハブ 23.8.0	78
修正された問題	78
既知の問題	78
以前のバージョンにおける既知の問題と修正された問題	78
Secure Hub の既知の修正済み問題の履歴	79
アンドロイド用 セキュアハブ 23.7.0	79
修正された問題	79
既知の問題	79
アイオーエス用 セキュアハブ 23.4.0	80
修正された問題	80
既知の問題	80
アンドロイド用セキュアハブ 23.4.1	80
修正された問題	80
既知の問題	80
アンドロイド用セキュアハブ 23.4.0	80
修正された問題	80
既知の問題	80
Android向けセキュアハブ 23.2.0	81
修正された問題	81
セキュアハブ 22.11.0	81
セキュアハブ 22.9.0	81
セキュアハブ 22.7.0	82
修正された問題	82
セキュアハブ 22.6.0	82
セキュアハブ 22.5.0	82
セキュアハブ 22.4.0	82

セキュアハブ 22.2.0	82
Secure Hub 22.2.0の既知の問題	82
Secure Hub 22.2.0の修正された問題	82
iOS版セキュアハブ	82
Android版セキュアハブ	83
セキュアハブ 21.11.0	83
Secure Hub 21.11.0 の既知の問題	83
Secure Hub 21.11.0 で修正された問題	83
Android 用 セキュアハブ	83
セキュアハブ 21.10.0	84
Secure Hub 21.10.0 の既知の問題	84
Secure Hub 21.10.0 で修正された問題	84
iOS 用 セキュアハブ	84
Android 用 セキュアハブ	84
セキュアハブ 21.8.0	84
iOS版セキュアハブ	84
Secure Hub 21.8.0の既知の問題	84
Secure Hub 21.8.0で修正された問題	84
セキュアハブ 21.7.1	84
Android版セキュアハブ	84
以前のバージョンにおける既知の問題と修正された問題	85
セキュアハブ 21.7.1	85
アンドロイド版Secure Hub	85
セキュアハブ 21.7.0	85
iOS版 セキュアハブ	85
Android版 セキュアハブ	85
Secure Hub 21.7.0の既知の問題	85
Secure Hub 21.7.0で修正された問題	85

セキュアハブ 21.6.0	85
iOS版 セキュアハブ	85
Secure Hub 21.6.0の既知の問題	85
Secure Hub 21.6.0で修正された問題	85
Android版 セキュアハブ	86
Secure Hub 21.6.0の既知の問題	86
Secure Hub 21.6.0で修正された問題	86
セキュアハブ 21.5.1	86
iOS用セキュアハブ	86
アンドロイド用セキュアハブ	86
セキュアハブ 21.5.0	86
Secure Hub 21.5.0の既知の問題	86
Secure Hub 21.5.0で修正された問題	86
セキュアハブ 21.4.0	86
セキュアハブ 21.3.2	87
iOS向けセキュアハブ	87
Secure Hub 21.3.2の既知の問題	87
Secure Hub 21.3.2で修正された問題	87
セキュアハブ 21.3.0	87
Secure Hub 21.3.0の既知の問題	87
Secure Hub 21.3.0で修正された問題	87
セキュアハブ 21.2.0	87
Android版セキュアハブ	87
Secure Hub 21.2.0 の既知の問題	87
Secure Hub 21.2.0 で修正された問題	88
セキュアハブ 21.1.0	88
Secure Hub 21.1.0 の既知の問題	88
Secure Hub 21.1.0 で修正された問題	88

セキュアハブ 20.12.0	88
Secure Hub 20.12.0 の既知の問題	88
Secure Hub 20.12.0 で修正された問題	88
セキュアハブ 20.11.0	89
Android版セキュアハブ	89
Secure Hub 20.11.0の既知の問題	89
Secure Hub 20.11.0で修正された問題	89
セキュアハブ 20.10.5	89
Secure Hub 20.10.5の既知の問題	89
Secure Hub 20.10.5で修正された問題	89
セキュアハブ 20.9.0	89
Secure Hub 20.9.0における既知の問題	89
Secure Hub 20.9.0における修正された問題	90
セキュアハブ 20.7.5	90
Secure Hub 20.7.5における既知の問題	90
Secure Hub 20.7.5における修正された問題	90
セキュアハブ 20.6.5	90
セキュアハブ 20.3.0	90
iOS用セキュアハブ	90
セキュアハブ 20.2.0	90
iOS用セキュアハブ	90
Secure Hub 20.2.0の既知の問題	91
Secure Hub 20.2.0で修正された問題	91
セキュアハブ 20.1.5	91
セキュアハブ 19.12.5	91
Secure Hub 19.12.5における既知の問題	91
Secure Hub 19.12.5における修正済みの問題	91
セキュアハブ 19.11.5	91

Secure Hub 19.11.5における既知の問題	91
Secure Hub 19.11.5における修正済みの問題	91
セキュアハブ 19.10.5	92
Android版 セキュアハブ	92
Secure Hub 19.10.5における既知の問題	92
Secure Hub 19.10.5 で修正された問題	92
セキュアハブ 19.10.0	92
Secure Hub 19.10.0 の既知の問題	92
Secure Hub 19.10.0 で修正された問題	92
セキュアハブ 19.9.5	92
Secure Hub 19.9.0 バージョン	92
Secure Hub 19.9.0 の既知の問題	92
Secure Hub 19.9.0 で修正された問題	93
Secure Hub 19.8.5 バージョン	93
Secure Hub バージョン 19.8.0	93
Secure Hub 19.8.0 の既知の問題	93
Secure Hub 19.8.0 で修正された問題	93
Secure Hub バージョン 19.7.5	93
Secure Hub 19.7.5 の既知の問題	93
Secure Hub 19.7.5 で修正された問題	93
セキュアハブ 19.6.5	94
Secure Hub 19.6.5の既知の問題	94
Secure Hub 19.6.5で修正された問題	94
セキュアハブ 19.5.5	94
Secure Hub 19.5.5の既知の問題	94
Secure Hub 19.5.5 で修正された問題	94
セキュアハブ 19.5.0	95
Secure Hub 19.5.0 の既知の問題	95

Secure Hub 19.5.0 で修正された問題	95
セキュアハブ 19.4.5	95
Secure Hub 19.4.5 の既知の問題	95
Secure Hub 19.4.5で修正された問題	95
セキュアハブ 19.3.5	96
Secure Hub 19.3.5の既知の問題	96
Secure Hub 19.3.5で修正された問題	96
セキュアハブ 19.3.0	96
Secure Hub 19.3.0の既知の問題	96
Secure Hub 19.3.0で修正された問題	97
セキュアハブ 19.2.0	97
Secure Hub 19.2.0の既知の問題	97
Secure Hub 19.2.0で修正された問題	97
セキュアハブ 19.1.5	97
Secure Hub 19.1.5 の既知の問題	97
Secure Hub 19.1.5 で修正された問題	98
セキュアハブ 19.1.0	98
Secure Hub 19.1.0 の既知の問題	98
Secure Hub 18.12.0 で修正された問題	98
セキュアハブ 18.11.0	98
Secure Hub 18.11.0 で修正された問題	98
セキュアハブ 18.10.5	99
Secure Hub 18.10.5で修正された問題	99
Secure Hubバージョン10.8.25～18.10.6	99
Secure Hubバージョン10.8.25～18.10.6で修正された問題	99
セキュアハブ 18.10.0	99
Secure Hub 18.10.0で修正された問題	99
セキュアハブ 10.8.60	99

Secure Hub 10.8.60で修正された問題	99
セキュアハブ 10.8.55	100
Secure Hub 10.8.55で修正された問題	100
バージョン10.8.55で修正されたMDX関連の問題	100
セキュアハブ 10.8.55	100
Secure Hub 10.8.55の既知の問題	100
セキュアハブ 10.8.50	100
Secure Hub 10.8.50 の既知の問題	100
セキュアハブ 10.8.35	101
Secure Hub 10.8.35 で修正された問題	101
セキュアハブ 10.8.25	101
Secure Hub 10.8.25 で修正された問題	101
セキュアハブ 10.8.20	101
Secure Hub 10.8.20 で修正された問題	101
セキュアハブ 10.8.15	101
Secure Hub 10.8.15で修正された問題	101
セキュアハブ 10.8.10	102
Secure Hub 10.8.10で修正された問題	102
Secure Hub for Android and iOS - プレビュー	103
機能フラグ管理	104
認証プロンプトのシナリオ	105
資格情報の種類	107
Secure Hubの画面切り替えについて	109
デバイスパスコードのパスコードの複雑さ（Android 12以降）	110
派生資格情報を使用してデバイスを登録する	112
派生資格情報を使用する場合のデバイス登録手順	112
Citrix Endpoint Management™ コンソールを介してヒントを構成する	114
ヒントをテキストとして構成する	114

Webページリンクでヒントテキストを構成する	115
Androidデバイスでのコンプライアンスチェック (テクニカルレビュー)	117

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.

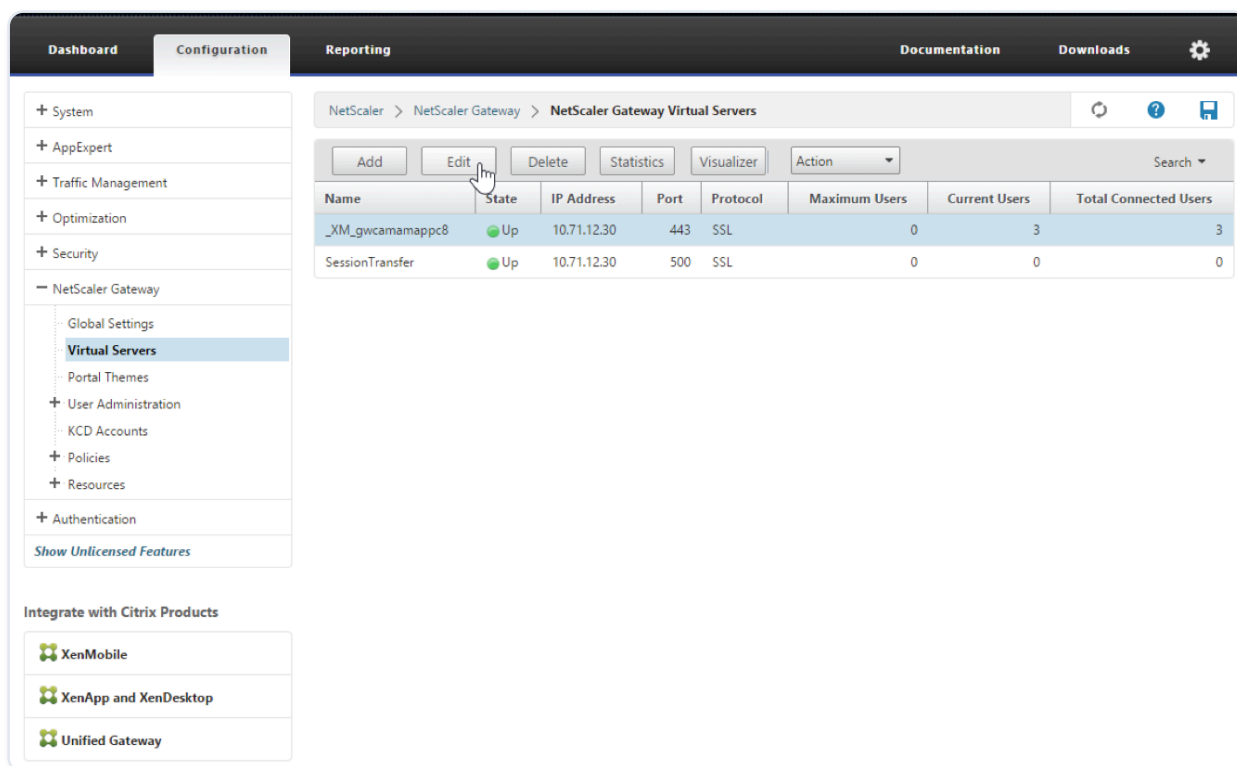
Comments

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。

シトリックス セキュアハブ™

Citrix Secure Hubは、モバイル生産性向上アプリの起動パッドです。ユーザーはSecure Hubにデバイスを登録し、アプリストアにアクセスできます。アプリストアから、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およびその他のコンポーネントは、[Citrix Endpoint Managementダウンロードページ](#)からダウンロードできます。

Secure Hubおよびモバイル生産性向上アプリのその他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。

モバイル生産性向上アプリの最新情報については、[最新のお知らせ](#)を参照してください。

以下のセクションでは、Secure Hubの現在および以前のリリースにおける新機能について説明します。

注：

Secure HubのAndroid 9.xおよびiOS 11.xバージョンに対するサポートは、2025年4月に終了しました。

現在のバージョンでの新機能

iOS版セキュアハブ 26.8.1

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

バグ修正の詳細については、[既知の問題と修正された問題](#)を参照してください。

Android版セキュアハブ 26.8.0

COSUモードのランチャー構成ポリシーで自動起動アプリを設定する

Citrix Launcherを実行しているAndroid Enterpriseキオスク（COSU）デバイスでは、管理者は、ランチャー構成ポリシーで自動起動アプリを設定し、デバイスの起動時に1つの管理対象アプリを自

動的に起動できるようになりました。Secure Hubは設定をCitrix Launcherに転送し、Citrix Launcherが起動を実行します。

MDMデバイス証明書の自動検出と更新

Android版Secure Hubは、無効、欠落、または期限切れのMDMデバイス証明書を自動的に検出し、バックグラウンドで更新するようになりました。これにより、ユーザーが手動で証明書のトラブルシューティングを実行したり、デバイスを再登録したりすることなく、デバイスの接続が復元されます。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

以前のバージョンの新機能

iOS版セキュアハブ 26.8.0

iOS/iPadOS 27のサポート

iOS版Secure Hub 26.8.0のリリース以降、このアプリはiOS/iPadOS 27と互換性があります。デバイスをiOS/iPadOS 27にアップグレードして、最新バージョンのSecure Hubを引き続き使用できます。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

Android版セキュアハブ 26.5.0

Android 17のサポート

Android版Secure Hub 26.5.0のリリース以降、このアプリはAndroid 17と互換性があります。デバイスをAndroid 17にアップグレードして、最新バージョンのSecure Hubを引き続き使用できます。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

Android版セキュアハブ 26.2.0

デバイス証明書のトラブルシューティングの強化

Android版Secure Hub 26.2.0のリリース以降、Secure Hubには、失効したクライアント証明書または無効なクライアント証明書によって引き起こされるデバイス接続の問題を診断および解決するのに役立つセルフサービスデバイス証明書トラブルシューティングツールが含まれています。

証明書の問題が検出されると、ツールは自動的に証明書の更新を試行し、接続を復元します。このツールにアクセスするには、>> に移動し、 をタップします。

デバイス証明書のトラブルシューティングの画像(/en-us/mobile-productivity-apps/media/device-certificate-troubleshooting.png)

バグ修正の詳細については、[既知の問題と修正された問題](#)を参照してください。

iOS版 セキュアハブ 25.8.0

iOS 26のサポート

iOS版Secure Hub 25.8.0のリリース以降、このアプリはiOS 26を実行しているデバイスをサポートします。Secure Hubバージョン25.8.0にアップグレードすると、iOS 26に更新されたデバイスに対する継続的なサポートと互換性が保証されます。

バグ修正の詳細については、[既知の問題と修正された問題](#)を参照してください。

Android版 セキュアハブ 25.10.0

16KBメモリページサイズのサポート

Android版Secure Hub 25.10.0のリリース以降、このアプリは16KBメモリページサイズをサポートし、パフォーマンスを最適化し、Google Playの要件に準拠します。

バグ修正の詳細については、[既知の問題と修正された問題](#)を参照してください。

Android版 セキュアハブ 25.7.0

このリリースでは、いくつかの問題に対処し、全体的なパフォーマンスと安定性の向上に役立っています。

バグ修正の詳細については、[既知の問題と修正された問題](#)を参照してください。

iOS版 セキュアハブ 25.6.0

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題に対処しています。

バグ修正の詳細については、「[既知の問題と修正済みの問題](#)」 (/ja-jp/citrix-secure-hub/known-fixed-issues.html)を参照してください。

Android 用 セキュアハブ 25.4.0

Android 16のサポート

Secure Hub 25.4.0 for Androidのリリース以降、このアプリはAndroid 16と互換性があります。デバイスをAndroid 16にアップグレードして、Secure Hubの最新バージョンを引き続き使用できます。

TLS 1.3プロトコルのサポート

Secure Hub 25.4.0 for Androidのリリース以降、このアプリはAndroidデバイスでTLS 1.3プロトコルをサポートします。TLS 1.3はTLSプロトコルの最新バージョンであり、TLS 1.2と比較して、より高速なパフォーマンス、強化されたセキュリティ、およびサイバー攻撃に対する優れた回復力を提供します。TLS 1.3はネットワーク遅延も削減し、HTTPS接続の高速化とユーザーエクスペリエンスの向上をもたらします。

TLS 1.3の詳細については、[The Transport Layer Security \(TLS\) Protocol Version 1.3](#)を参照してください。

バグ修正の詳細については、「既知の問題と修正済みの問題」([/ja-jp/citrix-secure-hub/known-fixed-issues.html](#))を参照してください。

Android 用 セキュアハブ 25.1.0

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題に対処しています。

バグ修正の詳細については、「既知の問題と修正済みの問題」([/ja-jp/citrix-secure-hub/known-fixed-issues.html](#))を参照してください。

iOS 用 セキュアハブ 25.1.0

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題に対処しています。

バグ修正の詳細については、「既知の問題と修正済みの問題」([/ja-jp/citrix-secure-hub/known-fixed-issues.html](#))を参照してください。

iOS向け セキュアハブ 24.11.0

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

バグ修正の詳細については、[既知の問題と修正された問題](#)を参照してください。

Android向け セキュアハブ 24.10.0

Android 15 のサポート

Secure Hub のバージョンを 24.10.0 にアップグレードすると、Android 15 に更新されたデバイスに対する継続的なサポートが保証されます。

バグ修正の詳細については、[既知の問題](#)と[修正された問題](#)を参照してください。

iOS向け セキュアハブ 24.9.0

デバイス登録プログラムで利用規約を表示

iOS 用 Secure Hub 24.9.0 以降、管理者は Citrix Endpoint Management (CEM) を介して利用規約デバイスポリシーを構成できます。構成されると、Apple のデバイス登録プログラム (DEP) を介して登録されたデバイスの登録プロセス中に、**利用規約**ページが表示されます。これにより、ユーザーは登録を完了する前に利用規約を確認して同意し、デバイスのオンボーディング中のコンプライアンスとセキュリティ対策を強化できます。

Android向け セキュアハブ 24.8.0

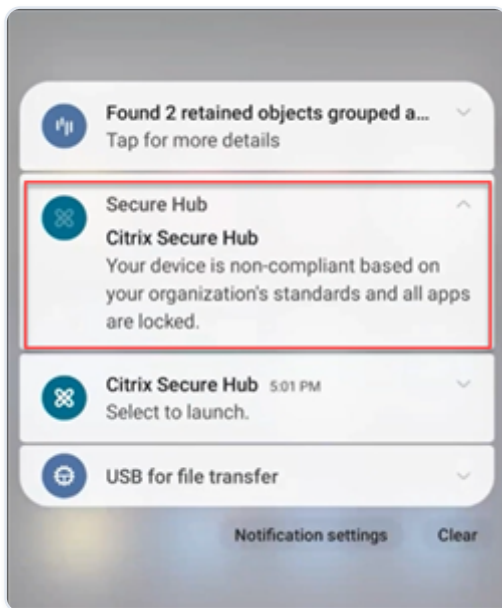
Android デバイスでのコンプライアンスチェック (テクニカルプレビュー)

注:

デバイス所有者モードで登録された Android デバイスにこの機能が適用されます。

このリリース以降、Secure Hub は、管理者が Citrix Endpoint Management を介して構成したポリシーに対して Android デバイスのコンプライアンスを検証します。これらのコンプライアンスチェックには、デバイスのパスワード強度の確保、必須アプリのインストールの検証、禁止アプリの削除の確認が含まれます。

デバイスが管理者によって設定されたポリシーに準拠していないと判断された場合、Secure Hub はそのすべてのアプリをロックし、ユーザーにコンプライアンスの問題を解決してロックを解除するよう促します。デバイスが非準拠の場合、ユーザーデバイスに次の通知が表示されます。

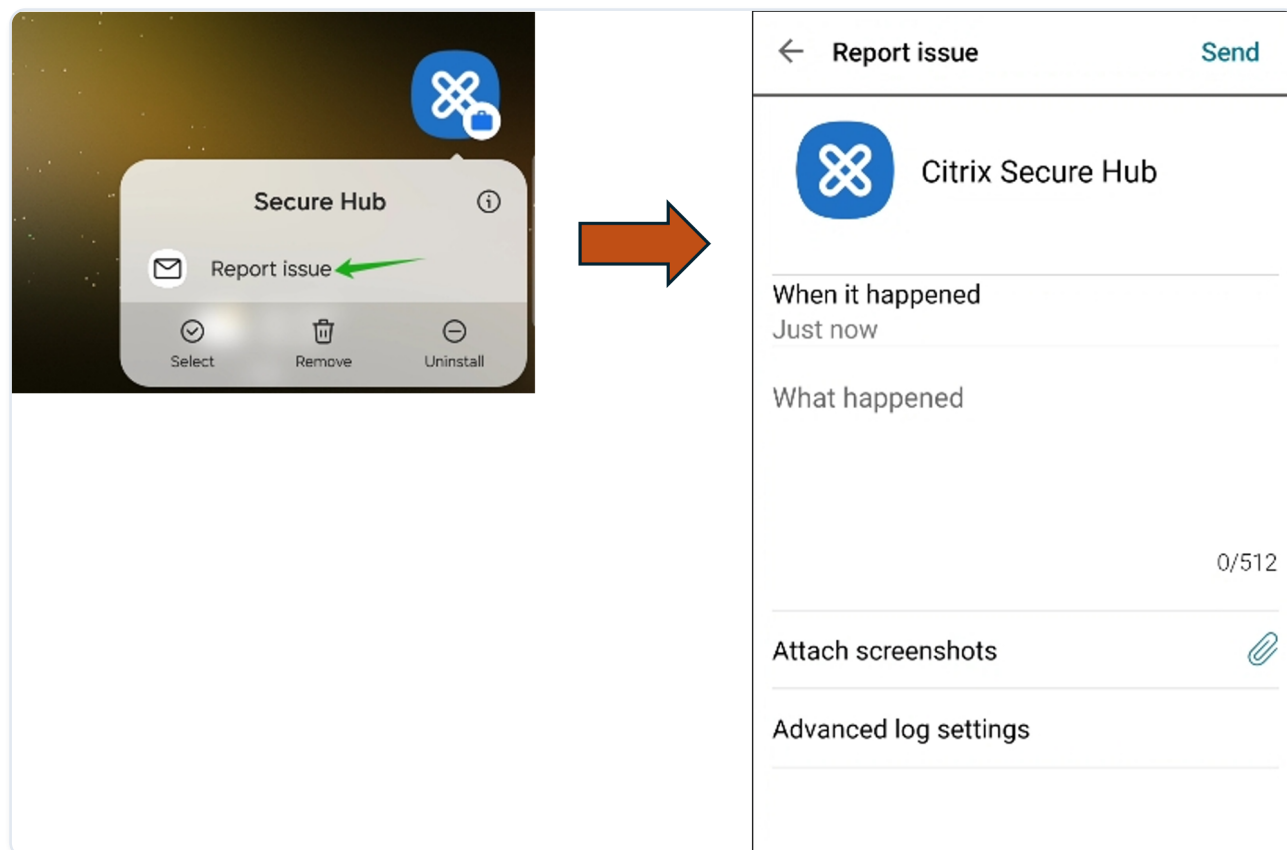


詳しくは、「[Android デバイスでのコンプライアンスチェック](#)」を参照してください。

Android用 セキュアハブ 24.6.0

ログ収集とレポート機能の改善

Secure Hub は、Secure Hub を開かずに問題を報告し、ログをシームレスに送信する機能を強化しました。このリリースでは、ユーザーは Secure Hub アプリアイコンを長押しすることで、オプションにアクセスできます。オプションをクリックすると、Secure Hub は直接 ページを開きます。



iOS 用 セキュアハブ 24.5.0

iOS 17 の Return to Service に対応

Secure Hub は、iOS 17 の Return to Service 機能をサポートしており、より効率的で安全なモバイルデバイス管理 (MDM) エクスペリエンスを提供します。以前は、デバイスをワイプした後、新しいユーザーのために手動で設定する必要がありました。現在、Return to Service 機能は、会社のデバイスを再利用する場合でも、個人デバイス (BYOD) を適切なセキュリティポリシーと統合する場合でも、このプロセスを自動化します。

Return to Service 機能を使用すると、MDM サーバーは、Wi-Fi の詳細とデフォルトの MDM 登録プロファイルを含む消去コマンドをユーザーデバイスに送信できます。その後、デバイスはすべてのユーザーデータを自動的にワイプし、指定された Wi-Fi ネットワークに接続し、提供された登録プロファイルを使用して MDM サーバーに再登録します。

アンドロイド用 セキュアハブ 24.3.0

サムスンノックス エンハンスド アテステーションバージョン3 に対応

Secure Hub は、Samsung Enhanced Attestation v3 をサポートするようになり、Knox アテステーションを活用して、Citrix Endpoint Management を介して管理される Samsung デバイスのセキュリティ対策を強化します。この高度なアテステーションプロトコルは、デバイスの整合性とセキュ

リティ状態を検証し、ルート化されておらず、承認されたファームウェアが実行されていることを保証します。この機能は、セキュリティの脅威に対する不可欠な保護層を提供し、企業セキュリティポリシーへの準拠を保証します。

Android用 セキュアハブ 23.12.0

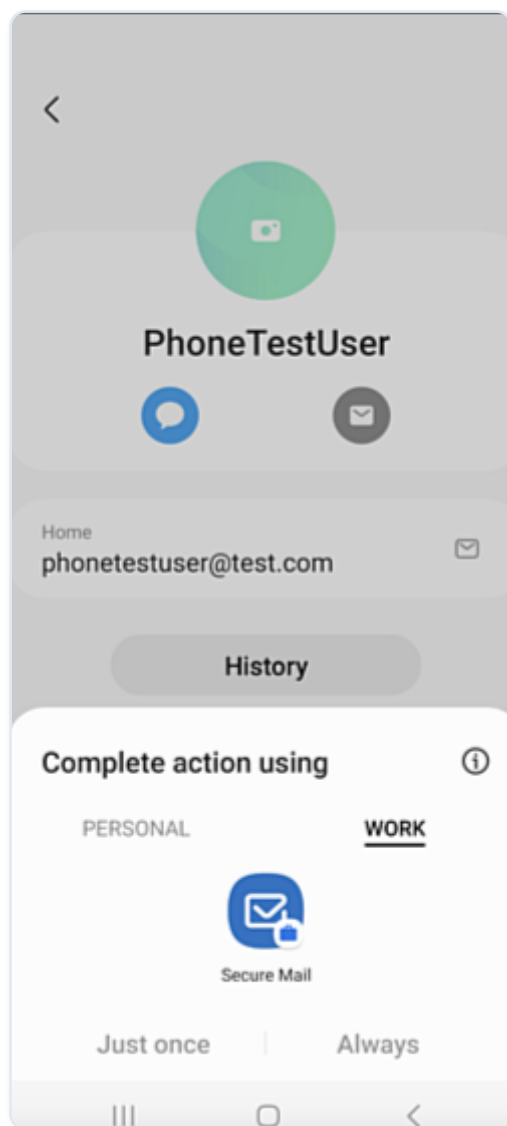
Samsung Knoxによるセキュリティ強化

Citrix Endpoint ManagementにKnox Platform for Enterpriseキーデバイスポリシーが追加されたことで、Samsungデバイス上のSecure Hubのセキュリティ機能が大幅に強化されました。このポリシーにより、必要なSamsung Knox Platform for Enterprise (KPE) ライセンス情報を提供し、KPE ライセンスを使用してSamsungデバイスのセキュリティを強化できます。Samsung Knoxは、エンタープライズデータを保護しつつ、管理の容易さとスムーズなユーザーエクスペリエンスを維持します。

詳細については、「[Knox Platform for Enterpriseキーデバイスポリシー](#)」を参照してください。

ユーザーの個人プロフィールからSecure Mailにアクセスする

ユーザーは、個人プロフィールから仕事用プロフィール内のSecure Mailにアクセスして使用できるようになりました。ユーザーが個人プロフィールのアドレス帳にあるメールアドレスをクリックすると、仕事用プロフィールでSecure Mailを使用するオプションが表示されます。この機能は、ユーザーが個人プロフィールからメールを送信できるという利便性を提供します。この機能は、BYODまたはWPCODデバイスに適用されます。



iOS版 セキュアハブ 24.1.0

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

Android版 セキュアハブ 23.12.0

サインインページに認証PINに関するヒントを追加する

23.12.0リリース以降、サインインページに認証PINに関するヒントを追加できるようになりました。この機能はオプションであり、2要素認証に登録されているデバイスに適用されます。ヒントは、PINへのアクセス方法を示します。

ヒントはテキストまたはリンクとして構成できます。ヒントテキストはPINに関する簡潔な情報を提供し、リンクはPINへのアクセス方法に関する詳細情報を提供します。ヒントの構成方法の詳細については、「[Citrix Endpoint Managementコンソールを介してヒントを構成する](#)」を参照してください。

nFactor認証はシングルサインオン機能をサポート

Secure Hub for Androidバージョン23.12.0以降、Mobile Application Management (MAM) の登録またはログインにおけるnFactorは、シングルサインオン (SSO) 機能をサポートします。この機能により、以前に入力されたサインイン資格情報がMAMの登録またはログインプロセスを通過できるようになり、ユーザーが手動で再入力する必要がなくなります。nFactor SSOプロパティの詳細については、Citrix Endpoint Managementドキュメントの「[クライアントプロパティリファレンス](#)」を参照してください。

ダイレクトブートモードでの完全ワイプをサポート

以前は、再起動したデバイスで完全ワイプコマンドを実行するには、デバイスのロックを解除する必要がありました。現在では、デバイスがロックされていても、ダイレクトブートモードで完全ワイプコマンドを実行できます。この機能は、特にデバイスが不正な個人の手に渡った場合に、セキュリティの観点から役立ちます。完全ワイプコマンドの詳細については、Citrix Endpoint Managementドキュメントの[セキュリティアクション](#)を参照してください。

Secure HubのApp Storeの読み込み速度を最適化

Secure HubのApp Storeの読み込みが以前よりも速くなり、ユーザーはより迅速にアクセスできるようになりました。

iOS用 セキュアハブ 23.11.0

サインインページに認証PINに関するヒントを追加

23.11.0リリース以降、サインインページに認証PINに関するヒントを追加できるようになりました。この機能はオプションであり、2要素認証に登録されたデバイスに適用されます。このヒントにより、PINへのアクセス方法がわかります。

ヒントはテキストまたはリンクとして構成できます。ヒントテキストはPINに関する簡潔な情報を提供し、リンクはPINへのアクセス方法に関する詳細情報を提供します。ヒントの構成方法の詳細については、[Citrix Endpoint Managementコンソールを介したヒントの構成](#)の記事を参照してください。

nFactor認証がシングルサインオン機能をサポート

Secure Hub for iOSバージョン23.11.0以降、モバイルアプリケーション管理 (MAM) 登録またはサインイン用のnFactorがシングルサインオン (SSO) 機能をサポートします。この機能により、以前に入力されたサインイン資格情報がMAM登録またはサインインプロセスを通過できるようになり、ユーザーが手動で再入力する必要がなくなります。

nFactor SSOプロパティの詳細については、Citrix Endpoint Managementドキュメントの[クライアントプロパティリファレンス](#)を参照してください。

セキュアハブ 23.10.0

Android向けセキュアハブ

Secure Hub for Android 23.10.0はAndroid 14をサポートしています。Secure Hubのバージョンを23.10.0にアップグレードすることで、Android 14に更新されたデバイスの継続的なサポートが保証されます。

セキュアハブ 23.9.0

Android版 セキュアハブ

このリリースでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

セキュアハブ 23.8.1

iOS用セキュアハブ

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題に対処しています。

セキュアハブ 23.8.0

iOS用セキュアハブ

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題に対処しています。

セキュアハブ 23.7.0

Android用セキュアハブ

プレイ インテグリティ API

SafetyNet Attestation API は、Google の廃止スケジュールに従ってまもなく廃止され、推奨される Play Integrity API に移行されます。

詳しくは、Citrix Endpoint Management ドキュメントの「[Play Integrity API](#)」を参照してください。

廃止の詳細については、Citrix Endpoint Management ドキュメントの「[廃止と削除](#)」を参照してください。

Android SafetyNet 機能については、「[SafetyNet](#)」を参照してください。

セキュアハブ 23.4.0

iOS用セキュアハブ

ユーザーエクスペリエンスの向上

バージョン23.4.0以降、iOS版Secure Hubでは以下のユーザーエクスペリエンスが向上しています。

- ストアエクスペリエンス：

- ◆ 以前は、[マイアプリ] ページが最初に表示されていました。バージョン23.4.0では、[ストア] ページが最初に表示されます。

- ◆ 以前は、ユーザーが [ストア] オプションをクリックするたびに、Secure Hubストアで再読み込みアクションが実行されていました。

バージョン23.4.0では、ユーザーエクスペリエンスが向上しました。アプリは、ユーザーが初めてアプリを起動したとき、アプリを再起動したとき、または画面を下にスワイプしたときに再読み込みされるようになりました。

- ユーザーインターフェイス：以前は、[サインオフ] オプションは画面の左下に配置されていました。バージョン23.4.0では、[サインオフ] オプションはメインメニューの一部となり、[バージョン情報] オプションの上に配置されています。

- ハイパーリンク：以前は、アプリの詳細ページのハイパーリンクはプレーンテキストとして表示されていました。バージョン23.4.0では、ハイパーリンクはクリック可能になり、リンクを示す下線付きの書式設定が適用されます。

MDXからMAM SDKへの移行エクスペリエンス

バージョン23.4.0以降、レガシーMDXからMAM SDKへの移行エクスペリエンスがiOSデュアルモードアプリ向けに強化されました。この機能により、アラートメッセージを減らし、Secure Hubに切り替えることで、モバイル生産性アプリ使用時のユーザーエクスペリエンスが向上します。

Citrix PINを使用してアプリのロックを解除する

以前は、エンドユーザーはデバイスのパスコードを入力して、モバイルアプリ管理（MAM）に基づくアプリのロックを解除していました。

バージョン23.4.0以降、エンドユーザーはCitrix PINをパスコードとして入力し、MAMベースのアプリのロックを解除できます。管理者は、CEMサーバーのクライアントプロパティを使用して、パスコードの複雑さを構成できます。

アプリが許可された時間以上非アクティブになった場合、エンドユーザーは管理者が設定した構成に応じてCitrix PINを入力してアプリのロックを解除できます。

Secure Hub for Android の場合、MAM アプリケーションでの非アクティブタイマーの処理方法を構成するための個別のクライアントプロパティがあります。詳細については、「[Android 用の個別の非アクティブタイマー](#)」を参照してください。

セキュアハブ 23.4.1

Android 用セキュアハブ

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

セキュアハブ 23.4.0

Android 用セキュアハブ

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

セキュアハブ 23.2.0

Android 用セキュアハブ

注：

- 欧州連合 (EU)、欧州経済領域 (EEA)、スイス、および英国 (UK) のユーザーについては、分析データは収集されません。

MDX フル トンネル モード VPN

MDX Micro VPN (フル トンネル モード) は非推奨になりました。

詳細については、Citrix Endpoint Management ドキュメントの「[非推奨](#)」を参照してください。

Android 用の個別の非アクティブタイマー

以前は、**Inactivity Timer** クライアントプロパティは、Android および iOS 用 Secure Hub で共通でした。

バージョン 23.2.0 以降、IT 管理者は新しいクライアントプロパティ

Inactivity_Timer_For_Android を使用して、非アクティビティタイマーを iOS から分離できます。IT 管理者は、**Inactivity_Timer_For_Android** の **Value** を 0 に設定することで、Android の非アクティビティタイマーを個別に無効にできます。これにより、Secure Hub を含むワークプロファイル内のすべてのアプリは、ワークPINのみを要求します。

Android 用の非アクティビティタイマーを分離する(/en-us/mobile-productivity-apps/media/separate-inactivity-timer-for-android.png)

クライアントプロパティの追加および変更方法の詳細については、XenMobile ドキュメントの「[クライアントプロパティ](#)」を参照してください。

セキュアハブ 22.11.0

Android 用 セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 22.9.0

Android 用 セキュアハブ

このリリースには以下が含まれます。

- デバイスパスコードのパスコードの複雑さ (Android 12 以降)
- SDK 31 のサポート
- バグ修正

デバイスパスコードのパスコードの複雑さ (Android 12 以降)

パスコードの複雑さは、カスタムパスワード要件よりも優先されます。パスコードの複雑さのレベルは、事前定義されたレベルのいずれかです。そのため、エンドユーザーはより低い複雑さのレベルのパスワードを設定できません。

Android 12以降のデバイスのパスコードの複雑さは次のとおりです。

- **パスコードの複雑さを適用:** カスタムパスワード要件ではなく、プラットフォームで定義された複雑さレベルのパスワードを要求します。Android 12以降のデバイスでSecure Hub 22.9以降を使用している場合にのみ適用されます。

- **複雑さレベル:** パスワードの複雑さの事前定義されたレベル。
 - **なし:** パスワードは不要です。
 - **低:** パスワードは次のいずれかです。
 - パターン
 - 4桁以上のPIN
 - **中:** パスワードは次のいずれかです。
 - 繰り返しシーケンス (4444) や順序付きシーケンス (1234) を含まない、4桁以上のPIN
 - 4文字以上の英字
 - 4文字以上の英数字
 - **高:** パスワードは次のいずれかです。
 - 繰り返しシーケンス (4444) や順序付きシーケンス (1234) を含まない、8桁以上のPIN
 - 6文字以上の英字
 - 6文字以上の英数字

注記:

- BYODデバイスの場合、最小の長さ、必須文字、生体認証、高度なルールなどのパスコード設定は、Android 12以降では適用されません。代わりにパスコードの複雑さを使用してください。
- ワークプロファイルのパスコードの複雑さが有効になっている場合、デバイス側のパスコードの複雑さも有効にする必要があります。

詳細については、Citrix Endpoint Managementのドキュメントの[Android Enterprise設定](#)を参照してください。

セキュアハブ 22.7.0

Android版 セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 22.6.0

Android版 セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 22.5.0

iOS版 セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 22.4.0

Android版 セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 22.2.0

iOS用セキュアハブ

このリリースにはバグ修正が含まれています。

Android用セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 21.11.0

Android用セキュアハブ

会社所有デバイスのワークプロファイルのサポート

Android Enterpriseデバイスでは、会社所有デバイスモードのワークプロファイルにSecure Hubを登録できるようになりました。この機能は、Android 11以降を実行しているデバイスで利用できます。以前にCorporate Owned Personally Enabled (COPE) モードに登録されていたデバイスは、デバイスがAndroid 10からAndroid 11以降にアップグレードされると、会社所有デバイスモードのワークプロファイルに自動的に移行します。

セキュアハブ 21.10.0

iOS用セキュアハブ

このリリースにはバグ修正が含まれています。

Android用セキュアハブ

Android 12のサポート。このリリース以降、Secure HubはAndroid 12を実行しているデバイスでサポートされます。

セキュアハブ 21.8.0

iOS 用セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 21.7.1

Android 用セキュアハブ

すでに登録されているデバイスでの **Android 12** のサポート。Android 12 へのアップグレードを検討している場合は、まず Secure Hub をバージョン 21.7.1 にアップデートしてください。Secure Hub 21.7.1 は、Android 12 にアップグレードするために必要な最小バージョンです。このリリースにより、すでに登録されているユーザーは Android 11 から Android 12 ヘシームレスにアップグレードできます。

注：

Android 12 にアップグレードする前に Secure Hub がバージョン 21.7.1 にアップデートされていない場合、以前の機能を回復するために、デバイスの再登録または工場出荷時設定へのリセットが必要になる場合があります。

Citrix は Android 12 の Day 1 サポートを提供することにコミットしており、Android 12 を完全にサポートするために、Secure Hub の後続バージョンにさらなるアップデートを追加する予定です。

セキュアハブ 21.7.0

iOS 用セキュアハブ

このリリースにはバグ修正が含まれています。

Android 用セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 21.6.0

iOS版セキュアハブ

このリリースにはバグ修正が含まれています。

Android版セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 21.5.1

iOS版セキュアハブ

このリリースにはバグ修正が含まれています。

Android版セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 21.5.0

iOS版セキュアハブ

このリリースでは、MDX Toolkitバージョン19.8.0以前でラップされたアプリは動作しなくなります。適切な機能を再開するには、最新のMDX Toolkitでアプリをラップしてください。

セキュアハブ 21.4.0

Secure Hubのカラーデザインを刷新しました。Secure HubはCitrixブランドのカラーアップデートに準拠しています。

セキュアハブ 21.3.2

iOS用セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 21.3.0

このリリースにはバグ修正が含まれています。

セキュアハブ 21.2.0

Android用セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 21.1.0

iOS用セキュアハブ

このリリースにはバグ修正が含まれています。

Android用セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 20.12.0

iOS用セキュアハブ

このリリースにはバグ修正が含まれています。

Android向けセキュアハブ

Android版Secure HubはDirect Bootモードをサポートしています。Direct Bootモードの詳細については、*Developer.android.com.*のAndroidドキュメントを参照してください。

セキュアハブ 20.11.0

Android向けセキュアハブ

Secure Hubは、Android 10向けのGoogle Playの現在のターゲットAPI要件をサポートしています。

セキュアハブ 20.10.5

このリリースにはバグ修正が含まれています。

セキュアハブ 20.9.0

iOS向けセキュアハブ

iOS版Secure HubはiOS 14をサポートしています。

Android向けセキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 20.7.5

Android向けセキュアハブ

- Android版Secure HubはAndroid 11をサポートしています。
- **アプリケーションのSecure Hub 32ビットから64ビットへの移行。** Secure Hubバージョン20.7.5では、アプリケーションの32ビットアーキテクチャのサポートが終了し、Secure Hubは64ビットに更新されました。Citrixは、お客様がバージョン20.6.5からバージョン20.7.5にアップグレードすることを推奨しています。ユーザーがSecure Hubバージョン20.6.5へのアップグレードをスキップし、代わりに20.1.5から20.7.5に直接更新した場合、再認証が必要です。再認証には、資格情報の入力とSecure Hub PINのリセットが含まれます。Secure Hubバージョン20.6.5はGoogle Playストアで入手できます。
- **App Storeからアップデートをインストールします。** Android版Secure Hubでは、アプリケーションに利用可能なアップデートがある場合、そのアプリケーションが強調表示され、App Store画面に**利用可能なアップデート**機能が表示されます。

利用可能なアップデートをタップすると、保留中のアップデートがあるアプリケーションのリストが表示されるストアに移動します。アプリケーションの横にある**詳細**をタップしてアップデートをインストールします。アプリケーションがアップデートされると、**詳細**の下向き矢印がチェックマークに変わります。

セキュアハブ 20.6.5

Android版セキュアハブ

アプリケーションの32ビットから64ビットへの移行。 Secure Hub 20.6.5リリースは、Androidモバイルアプリケーションの32ビットアーキテクチャをサポートする最終リリースです。以降のリリースでは、Secure Hubは64ビットアーキテクチャをサポートします。Citrixは、ユーザーがSecure Hubバージョン20.6.5にアップグレードすることを推奨しており、これによりユーザーは再認証なしで以降のバージョンにアップグレードできます。ユーザーがSecure Hubバージョン20.6.5へのアップグレードをスキップし、代わりに20.7.5に直接更新した場合、再認証が必要です。再認証には、資格情報の入力とSecure Hub PINのリセットが含まれます。

注:

20.6.5リリースでは、Android 10を実行しているデバイスのデバイス管理者モードでの登録はブロックされません。

iOS向けセキュアハブ

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

セキュアハブ 20.3.0

注:

Secure Hub、Secure Mail、Secure Web、およびCitrix WorkspaceアプリのAndroid 6.xおよびiOS 11.xバージョンのサポートは、2020年6月に終了します。

iOS向けセキュアハブ

- **ネットワーク拡張機能が無効になりました。** App Storeの審査ガイドラインの最近の変更により、リリース20.3.0以降、Secure HubはiOSを実行しているデバイスでのネットワーク拡張機能（NE）をサポートしません。NEはCitrixが開発したモバイル生産性向上アプリには影響しません。ただし、NEの削除は、展開されているエンタープライズMDXラップアプリにいくつかの影響を与えます。エンドユーザーは、認証トークン、タイマー、PINの再試行などのコンポーネントを同期する際に、Secure Hubへの余分な切り替えを経験する可能性があります。

注記:

新規ユーザーには、VPNをインストールするようプロンプト表示されません。

- **拡張登録プロファイルのサポート。** Secure Hubは、[登録プロファイルのサポート](#)でCitrix Endpoint Management向けに発表された拡張登録プロファイル機能をサポートします。

セキュアハブ 20.2.0

iOS版 セキュアハブ

このリリースにはバグ修正が含まれています。

セキュアハブ 20.1.5

このリリースには以下が含まれます。

- ユーザープライバシーポリシーの書式設定と表示の更新。この機能更新により、Secure Hubの登録フローが変更されます。
- バグ修正。

セキュアハブ 19.12.5

このリリースにはバグ修正が含まれています。

セキュアハブ 19.11.5

このリリースにはバグ修正が含まれています。

Secure Hub バージョン 19.10.5

Android版 Secure Hub

Secure HubをCOPEモードで登録します。 Android Enterpriseデバイスでは、Citrix Endpoint ManagementがCOPE登録プロファイルで構成されている場合、Secure HubをCorporate Owned Personally Enabled (COPE) モードで登録します。

セキュアハブ 19.10.0

このリリースにはバグ修正が含まれています。

セキュアハブ 19.9.5

iOSデバイス用のSecure Hub

このリリースにはバグ修正が含まれています。

Androidデバイス用のSecure Hub

Android Enterpriseのワークプロファイルおよび完全に管理されたデバイスのキーガード機能の管理をサポート。 Androidキーガードは、デバイスおよびワークチャレンジのロック画面を管理し

まず、Citrix Endpoint Managementのキーガード管理デバイスポリシーを使用して、ワークプロファイルデバイスでのキーガード管理、および完全に管理された専用デバイスでのキーガード管理を制御します。キーガード管理を使用すると、キーガード画面のロックを解除する前に、信頼エージェントやセキュアカメラなど、ユーザーが利用できる機能を指定できます。または、すべてのキーガード機能を無効にすることもできます。

機能設定とデバイスポリシーの構成方法について詳しくは、「[キーガード管理デバイスポリシー](#)」を参照してください。

セキュアハブ 19.9.0

iOS版セキュアハブ

iOS版Secure HubはiOS 13をサポートしています。

セキュアハブ Android版

このリリースにはバグ修正が含まれています。

セキュアハブ Android版 19.8.5

このリリースにはバグ修正が含まれています。

セキュアハブ 19.8.0

iOS用セキュアハブ

このリリースには、パフォーマンスの強化とバグ修正が含まれています。

Android版セキュアハブ

Android Qのサポート。 このリリースにはAndroid Qのサポートが含まれています。Android Qプラットフォームにアップグレードする前に、Googleデバイス管理APIの非推奨がAndroid Qを実行しているデバイスにどのように影響するかについては、[デバイス管理からAndroid Enterpriseへの移行](#)を参照してください。また、ブログ[Citrix Endpoint Management and Android Enterprise - a Season of Change](#)も参照してください。

Secure Hub バージョン 19.7.5

iOS向けセキュアハブ

このリリースには、パフォーマンスの強化とバグ修正が含まれています。

Android向けセキュアハブ

Samsung Knox SDK 3.xのサポート。 Android用Secure HubはSamsung Knox SDK 3.xをサポートしています。Samsung Knox 3.xへの移行の詳細については、[Samsung Knox開発者向けドキュメント](#)を参照してください。このリリースには、新しいSamsung Knox名前空間のサポートも含まれています。古いSamsung Knox名前空間の変更の詳細については、[古いSamsung Knox名前空間の変更](#)を参照してください。

注：

Android用Secure Hubは、Android 5を実行しているデバイスではSamsung Knox 3.xをサポートしていません。

Secure Hub 19.3.5から19.6.6

これらのリリースには、パフォーマンスの強化とバグ修正が含まれています。

セキュアハブ 19.3.0

Samsung Knox Platform for Enterpriseのサポート。 Android版Secure Hubは、Android EnterpriseデバイスでKnox Platform for Enterprise (KPE)をサポートします。

セキュアハブ 19.2.0

このリリースには、パフォーマンスの強化とバグ修正が含まれています。

セキュアハブ 19.1.5

Android Enterprise版Secure Hubは、以下のポリシーをサポートするようになりました。

- **Wi-Fiデバイスポリシー。** Wi-Fiデバイスポリシーは、Android Enterpriseをサポートするようになりました。このポリシーの詳細については、「[Wi-Fiデバイスポリシー](#)」を参照してください。
- **カスタムXMLデバイスポリシー。** カスタムXMLデバイスポリシーは、Android Enterpriseをサポートするようになりました。このポリシーの詳細については、「[カスタムXMLデバイスポリシー](#)」を参照してください。
- **ファイルデバイスポリシー。** Citrix Endpoint Managementでスクリプトファイルを追加して、Android Enterpriseデバイスで機能を実行できます。このポリシーの詳細については、「[ファイルデバイスポリシー](#)」を参照してください。

セキュアハブ 19.1.0

Secure Hubは、フォント、色、その他のUI改善を刷新しました。この刷新により、Citrixのモバイル生産性アプリの全スイートにおけるブランドの美学と密接に連携しながら、豊かなユーザーエクスペリエンスが提供されます。

セキュアハブ 18.12.0

このリリースには、パフォーマンスの強化とバグ修正が含まれています。

セキュアハブ 18.11.5

- **Android Enterprise向け制限デバイスポリシー設定。** 制限デバイスポリシーの新しい設定により、ユーザーはAndroid Enterpriseデバイスで以下の機能にアクセスできるようになります: ステータスバー、ロック画面キーガード、アカウント管理、位置情報共有、Android Enterpriseデバイスの画面常時オン。詳しくは、[制限デバイスポリシー](#)を参照してください。

Secure Hub 18.10.5から18.11.0には、パフォーマンスの強化とバグ修正が含まれています。

セキュアハブ 18.10.0

- **Samsung DeXモードのサポート:** Samsung DeXを使用すると、ユーザーはKNOX対応デバイスを外部ディスプレイに接続して、PCのようなインターフェイスでアプリを使用したり、ドキュメントを確認したり、ビデオを視聴したりできます。Samsung DeXのデバイス要件とセットアップについては、[Samsung DeXの仕組み](#)を参照してください。

Citrix Endpoint ManagementでSamsung DeXモードの機能を構成するには、Samsung Knoxの制限デバイスポリシーを更新します。詳しくは、[制限デバイスポリシーのSamsung KNOX設定](#)を参照してください。

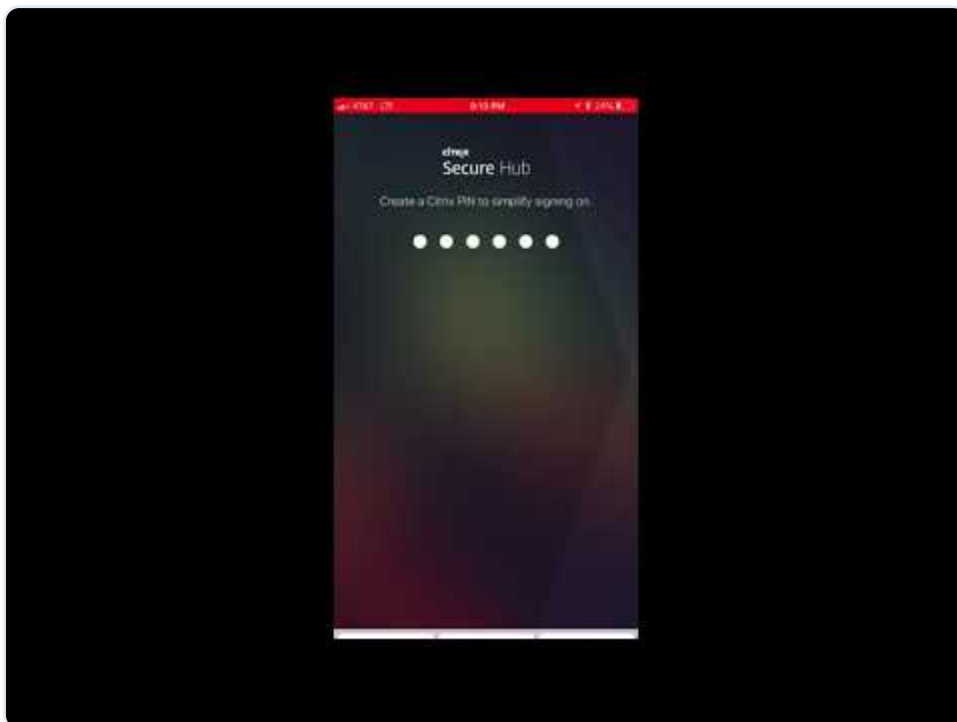
- **Android SafetyNetのサポート:** Endpoint Managementを構成して、**Android SafetyNet**機能を使用し、Secure HubがインストールされているAndroidデバイスの互換性とセキュリティを評価できます。その結果は、デバイスで自動アクションをトリガーするために使用できます。詳しくは、[Android SafetyNet](#)を参照してください。
- **Android Enterpriseデバイスでのカメラ使用の禁止:** 制限デバイスポリシーの新しいカメラの使用を許可設定により、ユーザーがAndroid Enterpriseデバイスでカメラを使用することを禁止できます。詳しくは、[制限デバイスポリシー](#)を参照してください。

Secure Hub 10.8.60から18.9.0

これらのリリースには、パフォーマンスの強化とバグ修正が含まれています。

セキュアハブ 10.8.60

- ポーランド語のサポート。
- Android Pのサポート。
- Workspaceアプリストアの使用のサポート。 Secure Hubを開くと、ユーザーはSecure Hubストアを表示しなくなります。 **アプリの追加**ボタンをクリックすると、ユーザーはWorkspaceアプリストアに移動します。以下のビデオは、Citrix Workspace™ アプリを使用してCitrix Endpoint Managementに登録を実行するiOSデバイスを示しています。



重要:

この機能は新規のお客様のみが利用できます。既存のお客様の移行は現在サポートしていません。

この機能を使用するには、以下を構成します。

- パスワードキャッシュポリシーとパスワード認証ポリシーを有効にします。ポリシーの構成について詳しくは、「[モバイル生産性向上アプリのMDXポリシーの概要](#)」を参照してください。
- Active Directory認証をADまたはAD+Certとして構成します。これら2つのモードをサポートしています。認証の構成について詳しくは、「[ドメインまたはドメインとセキュリティトークン認証](#)」を参照してください。

- Endpoint ManagementのWorkspace統合を有効にします。Workspace統合について詳しくは、「[ワークスペースの構成](#)」を参照してください。

重要：

この機能が有効になると、Citrix Files SSOはEndpoint Management（旧XenMobile®）ではなくWorkspaceを介して行われます。Workspace統合を有効にする前に、Endpoint ManagementコンソールでCitrix Files統合を無効にすることをお勧めします。

セキュアハブ 10.8.55

- 構成JSONを使用して、Google zero-touchおよびSamsung Knox Mobile Environment（KME）ポータルにユーザー名とパスワードを渡す機能。詳しくは、「[Samsung Knoxの一括登録](#)」を参照してください。
- 証明書のピン留めを有効にすると、ユーザーは自己署名証明書でEndpoint Managementに登録できません。ユーザーが自己署名証明書でEndpoint Managementに登録しようとすると、証明書が信頼されていないという警告が表示されます。

Secure Hub 10.8.25： Android版Secure Hubは、Android Pデバイスをサポートしています。

注：

Android Pプラットフォームにアップグレードする前に：サーバーインフラストラクチャが、subjectAltName（SAN）拡張機能に一致するホスト名を持つセキュリティ証明書に準拠していることを確認してください。ホスト名を確認するには、サーバーは一致するSANを持つ証明書を提示する必要があります。ホスト名に一致するSANを含まない証明書は信頼されなくなります。詳しくは、Android開発者向けドキュメントを参照してください。

Secure Hub for iOS update on March 19, 2018: iOS版Secure Hubバージョン10.8.6は、VPPアプリポリシーの問題を修正するために利用可能です。

Secure Hub 10.8.5： Android版Secure Hubで、Android Work（Android for Work）のCOSUモードをサポート。詳しくは、「[Citrix Endpoint Managementのドキュメント](#)」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とGoogle Play Storeにアップロードします。

Secure Hubは、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たときに、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ポリシーも更新します。

重要：

これらのポリシー（セキュリティグループ、暗号化の有効化、Secure Mail Exchange Server）のいずれかを変更した場合、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。

シトリックスピン

Secure HubをCitrix PINを使用するように構成できます。Citrix PINは、Endpoint Managementコンソールの**設定 > クライアントプロパティ**で有効にな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、保護されたラップ済み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、PINを入力してCitrixアプリとStoreに安全にアクセスできます。これは、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続きます。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。詳しくは、「クライアントプロパティ」(</ja-jp/citrix-endpoint-management/advanced-concepts/deployment/client-properties.html>)を参照してください。

指紋（Touch ID）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ときに、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」(</ja-jp/mobile-productivity-apps/administrator-tasks.html#fingerprint-or-touch-id-authentication>)を参照してください。

証明書のピン留め

iOSおよびAndroid版Secure Hubは、SSL証明書のピン留め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。これにより、デバイスにルート証明書がインストールされて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への接続が防止されます。Secure Hubがサーバー公開鍵の変更を検出すると、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証明機関（CA）を許可しなくなりました。Citrix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、次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、Endpoint Managementの「信頼されたCAを必須にする」オプションが**ON**に設定されている場合。詳しくは、「デバイス管理」([/ja-jp/citrix-endpoint-management/device-management.html](https://ja-jp/citrix-endpoint-management/device-management.html))を参照してください。
- プライベート/自己署名CAおよびEndpoint Management AutoDiscovery Service (ADS) に到達できません。セキュリティ上の懸念から、ADSに到達できない場合、Required Trusted 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、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に登録できません。ユーザーが自己署名証明書で登録しようとすると、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承認しない場合、登録は失敗します。

証明書ピン留めを使用するには、Citrixに証明書をCitrix ADSサーバーにアップロードするよう要求してください。[Citrix Support portal](#)を使用してテクニカルサポートケースをオープンします。秘密鍵をCitrixに送信しないようにしてください。次に、以下の情報を提供します。

- 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、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Email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、管理者用のメールアドレス。
- ドメインに追加したいPEM形式の証明書。これらは公開証明書であり、秘密鍵ではありません。
- 既存のサーバー証明書の処理方法：古いサーバー証明書を直ちに削除するか（侵害されているため）、または有効期限が切れるまで古いサーバー証明書をサポートし続けるか。

詳細と証明書がCitrixサーバーに追加されると、テクニカルサポートケースが更新されます。

証明書 + ワンタイムパスワード認証

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するように設定できます。この構成は、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を提供します。

Secure Hub で証明書とワンタイムパスワードタイプの認証を使用できるようにするには、次の手順を実行します。Citrix Gateway のログオンタイプを示すために、**X-Citrix-AM-GatewayAuthType: CertAndRSA** 形式のカスタム応答ヘッダーを挿入するリライトアクションとリライトポリシーを Citrix ADC に追加します。

通常、Secure Hub は Endpoint Management コンソールで構成された Citrix Gateway ログオンタイプを使用します。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、カスタムヘッダーが必要です。

注：

Endpoint Management と Citrix ADC で異なるログオンタイプ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** 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*

Type*

Use this action type to insert a header.

Header Name*

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。

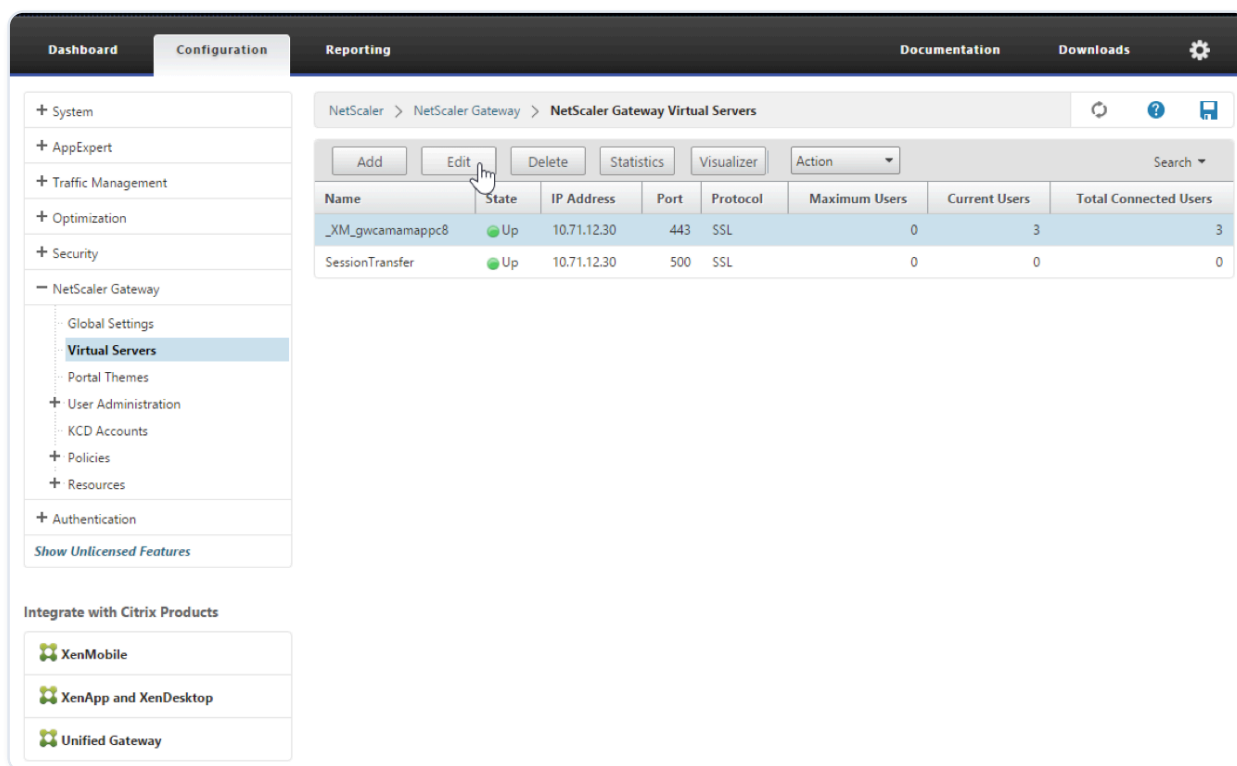
NetScaler > AppExpert > Rewrite > Rewrite Actions

Add Edit Delete Action Show built-in Rewrite Actions Search

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"	

- 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. **Edit** 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. 「+」をクリックしてポリシーを追加します。

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、「リライト」を選択します。
9. 「**種類の選択**」フィールドで、「レスポンス」を選択します。

レスポンスオプションの画像(/en-us/mobile-productivity-apps/media/netScaler-policy-settings-response.png)

10. 「**続行**」をクリックします。

「ポリシーバインド」セクションが展開されます。

ポリシーバインドセクションの画像(/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、その後「選択」をクリックします。「ポリシーバインド」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設定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、 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接続に必要なポート

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を介して利用可能になるセキュリティ更新プログラムをダウンロードする際には、ADSへのアクセス機能が重要です。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、Citrix Endpoint Managementドキュメントの[ポート要件](#)を参照してください。この通信はアウトバウンドポート443で行われます。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推奨しません。ご不明な点がある場合は、Citrixサポートにお問い合わせください。

前提条件:

- Endpoint ManagementおよびCitrix ADC証明書を収集します。証明書はPEM形式で、公開証明書である必要があり、秘密キー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。この前提条件により、デバイスが登録される環境の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、デバイスの登録を可能にするには、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、以下の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とポートの使用状況
<code>discovery.mdm.ze nprise.com</code>	52.5.138.94	443	セキュアハブ - ADS 通信
<code>discovery.mdm.ze nprise.com</code>	52.1.30.122	443	セキュアハブ - ADS 通信
<code>ads.xm.cloud.com</code> : Secure Hubバー ジョン10.6.15以降は <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 - ADS 通信
<code>ads.xm.cloud.com</code> : Secure Hubバー ジョン10.6.15以降は <code>ads.xm.cloud.com</code> を使用することに注 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場合、証明書の更新に再登録は不要です。

証明書ピン留めはリーフ証明書をサポートし、中間証明書や発行者証明書はサポートしません。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。

アカウント削除オプションの無効化

Auto Discovery Services (ADS) が有効な環境では、Secure Hub のアカウント削除オプションを無効にできます。

アカウント削除オプションを無効にするには、次の手順を実行します:

1. ドメイン用にADSを構成します。
2. Citrix Endpoint Managementで**AutoDiscovery Service Information**を開き、`displayReenrollLink` の値を**False**に設定します。デフォルトでは、この値は**True**です。
3. デバイスがMDM+MAM (ENT) モードで登録されている場合、変更を有効にするには一度ログオフして再度ログインしてください。デバイスが他のモードで登録されている場合は、デバイスを再登録する必要があります。

Secure Hubの使用

ユーザーはまず、AppleまたはAndroidストアからSecure Hubをデバイスにダウンロードします。

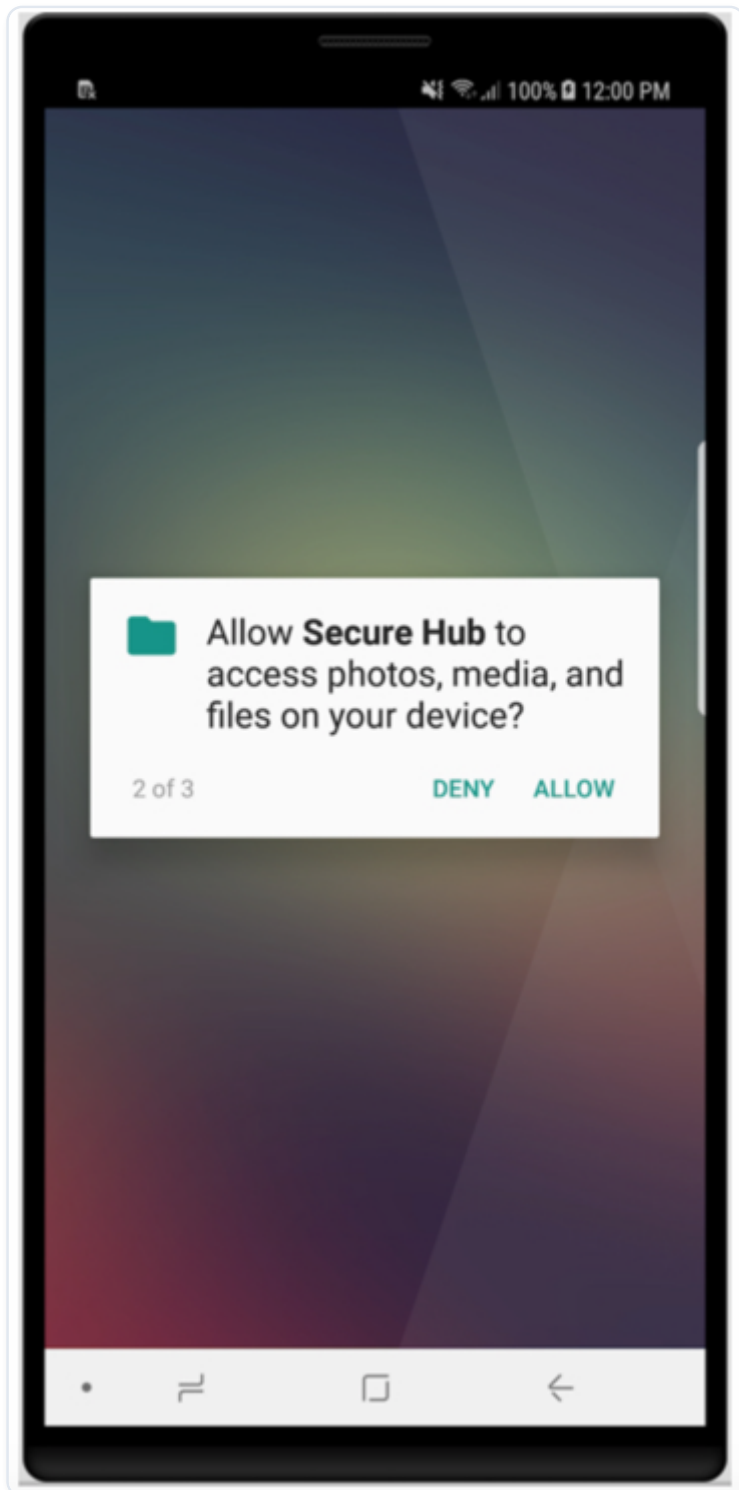
Secure Hubが起動したら、ユーザーは会社から提供された資格情報を入力して、デバイスをSecure Hubに登録します。デバイス登録の詳細については、「ユーザーアカウント、役割、および登録」(</ja-jp/citrix-endpoint-management/users.html>)を参照してください。

Android版Secure Hubでは、初回インストールおよび登録時に次のメッセージが表示されます。

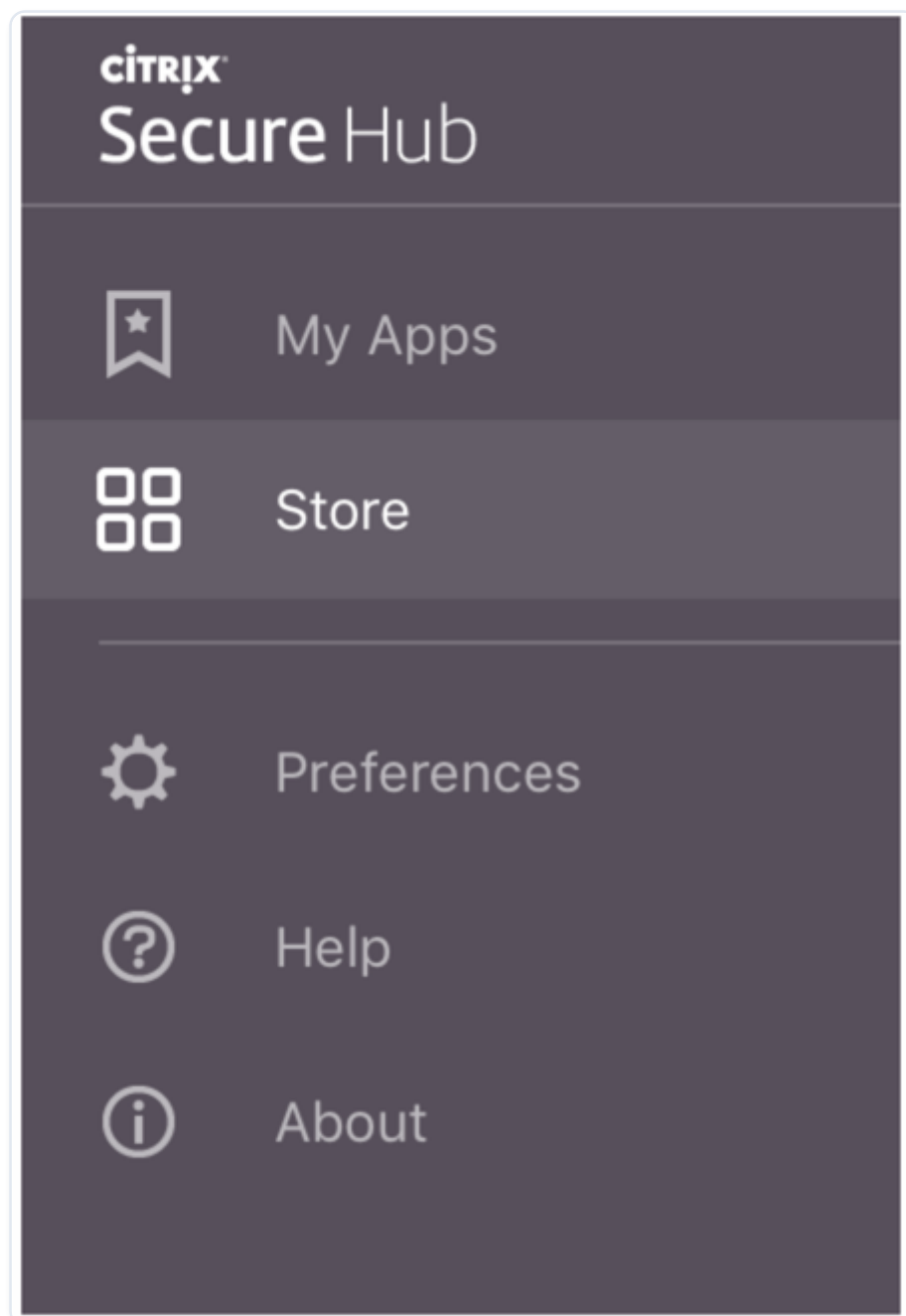
「Secure Hubにデバイス上の写真、メディア、ファイルへのアクセスを許可しますか？」

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した場合、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にある**設定**ハンバーガーアイコンの下にあります。



タブレットでは、ストアは別のタブになっています。



iOS 9以降を実行しているiPhoneユーザーが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、メッセージが表示されます。このメッセージは、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ことを示しています。また、開発者が信頼されるまでアプリは使用できないことも示しています。このメッセージが表示されると、Secure Hubはユーザーに、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促します。

Secure Mailへの自動登録

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、ユーザーIDを取得します。Secure MailはAutoDiscoveryにメールアドレスを使用します。Exchange Server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。ただし、ユーザーは追加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、「[サーバープロパティ](#)」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、「[クライアントプロパティ](#)」を参照してください。

カスタマイズされたストア

ストアをカスタマイズする場合は、**[設定] > [クライアントのブランド設定]** に移動して、名前の変更、ロゴの追加、アプリの表示方法の指定を行います。

The screenshot shows the 'Client Branding' configuration page in the XenMobile interface. The page has a green header with 'XenMobile' and navigation tabs: 'Analyze', 'Manage', and 'Configure'. The user is logged in as 'administrator'. The breadcrumb trail is 'Settings > Client Branding'. The main heading is 'Client Branding' with a subtext: 'You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.'

The configuration fields are:

- Store name***: A text input field containing 'Store'.
- Default store view**: Radio buttons for 'Category' and 'A-Z' (selected).
- Device**: Radio buttons for 'Phone' (selected) and 'Tablet'.
- Branding file**: A text input field with a 'Browse' button next to it.

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.
- A .zip file should be created from the files, not a folder with the files inside of it.

At the bottom right, there are 'Cancel' and 'Save' buttons.

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、**【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。

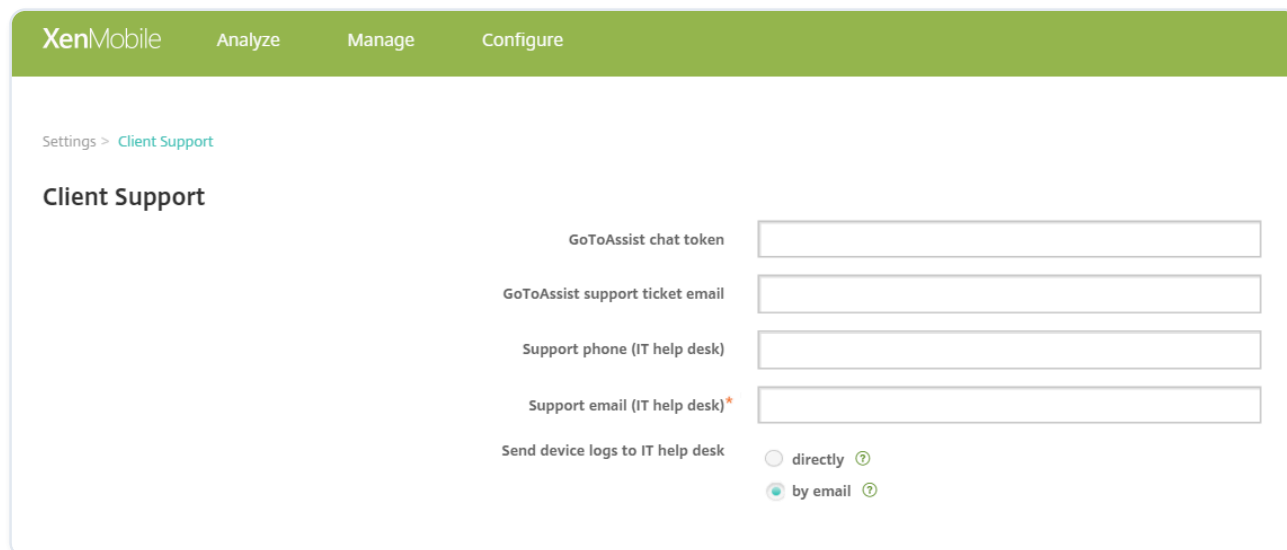
ストアでは、ユーザーはEndpoint Managementで構成および保護したアプリとデスクトップのみを参照できます。アプリを追加するには、ユーザーは**【詳細】** をタップし、**【追加】** をタップします。

構成済みのヘルプオプション

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、**【ヘルプ】** をタップします。

【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コンソールで入力します。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、[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。



[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] をクリックすると、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 Support**をタップして、**Citrix Knowledge Center**を開くこともできます。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。

Preferencesで、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。

位置情報ポリシー

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。

クラッシュの収集と分析

Secure Hubは、特定の障害の原因を把握できるように、障害情報を自動的に収集および分析します。ソフトウェアのCrashlyticsがこの機能をサポートしています。

iOSおよびAndroidで利用可能なその他の機能については、[Citrix Secure Hub](#)のプラットフォーム別機能マトリックスを参照してください。

Secure Hubのデバイス側ログを生成する

このセクションでは、Secure Hubのデバイス側ログを生成し、それらの正しいデバッグレベルを設定する方法について説明します。

Secure Mailのログを取得するには、次の手順を実行します。

1. **Secure Hub > ヘルプ > 問題を報告**に移動します。アプリのリストからSecure Mailを選択します。組織のヘルプデスク宛てのメールが開きます。
2. サポートチームから指示があった場合にのみ、ログ設定を変更してください。設定が正しく行われていることを常に確認してください。
3. Secure Mailに戻り、問題を再現します。問題の再現を開始した時刻と、問題が発生した、またはエラーメッセージが表示された時刻をメモします。
4. **Secure Hub > ヘルプ > 問題を報告**に戻ります。アプリのリストからSecure Mailを選択します。組織のヘルプデスク宛てのメールが開きます。
5. 件名と本文に問題の簡単な説明を入力します。手順3で収集したタイムスタンプを含め、**送信**をクリックします。完了したメッセージが、圧縮されたログファイルを添付して開きます。
6. **送信**を再度クリックします。

送信されたzipファイルには、以下のログが含まれます。

- CtxLog_AppInfo.txt（アイオーエス）、Device_And_AppInfo.txt（アンドロイド）、logx.txt、およびWH_logx.txt（ウィンドウズフォン）

アプリ情報ログには、デバイスとアプリに関する情報が含まれます。

既知の解決済み問題

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。

iOS用セキュアハブ 26.8.1

解決済みの問題

- Citrix Workspaceアプリを介してiOS用Secure HubからHDXアプリを起動すると、アプリが起動に失敗する場合があります。

既知の問題

このリリースには既知の問題はありません。

Android用セキュアハブ 26.8.0

解決済みの問題

- Android Enterprise制限ポリシーで、特定のシステムアプリのホワイトリストを設定すると、****All****設定が上書きされ、すでにホワイトリストに登録されているシステムアプリが再度非表示になる場合があります。
- Android Enterpriseキオスク（COSU）デバイスでは、デバイスがジオフェンスの境界を離れたときにSecure Hubが適用したデバイスロックPINが、デバイスが許可されたエリアに戻った後も削除されない場合があります。その結果、デバイスはPINの入力を求め続け、管理者はコンソールからPINを取得してデバイスを手動でロック解除する必要があります。
- Android 16およびAndroid 17を実行しているデバイス（One UI 8.5を実行しているSamsungデバイスを含む）では、完全に管理されたデバイスまたは専用デバイスの登録が完了した後も、デバイスがロックタスク（キオスク）モードのままになる場合があります。その結果、ユーザーはSecure Hub画面を離れることができず、登録が不完全に表示され、デバイスを再起動する必要があります。

既知の問題

このリリースには既知の問題はありません。

iOS用セキュアハブ 26.8.0

修正された問題

- Microsoft Authentication Library (MSAL) のサインアウトを呼び出すと、競合状態またはデッドロックが原因でSecure Hubがクラッシュする可能性があります。
- `mam-app-data-sharing` 機能フラグが有効になっている場合、Secure MailとSecure Webが初回使用時に失敗する可能性があります。
- DEPデバイスでは、セキュアアプリによってトリガーされた選択的ワイプ中にMDMプロファイルが削除されない場合があります。
- ユーザーがSecure Hubからフィードバックを送信すると、フィードバックが古いサポートメールアドレスに送信される可能性があります。
- アカウントが削除された後もPINポップアップが残る場合があります。
- ログの送信ボタンをタップしても反応しない場合があります。
- Secure Hubには不要な `NSAppleMusicUsageDescription` 権限が含まれている可能性があります。
- 2100を超えるライセンスを持つテナントの場合、Volume Purchase Program (VPP) アプリをインストールすると、アプリがインストールされずにユーザーがApp Storeにリダイレクトされる可能性があります。
- 共有キーチェーンボルトの読み込み中に、Secure HubがSIGABRTエラーでクラッシュする可能性があります。

既知の問題

このリリースには既知の問題はありません。

Android用 セキュアハブ 26.5.0

修正された問題

ADSサーバーのURLに無効なポート値が含まれている場合、Secure Hubの自動検出が失敗する可能性があります。

既知の問題

このリリースには既知の問題はありません。

Android 用 セキュアハブ 26.2.0

修正された問題

このバージョンでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

既知の問題

このリリースには既知の問題はありません。

Android 用 セキュアハブ 25.10.0

修正された問題

必要なアプリがインストールされていないためにポリシー展開がブロック解除されない場合、Secure HubはCEMサーバーに展開の失敗を報告します。

既知の問題

このリリースには既知の問題はありません。

iOS 用 セキュアハブ 25.8.0

修正された問題

- モバイルアプリケーション管理 (MAM) アプリのデータ共有機能フラグをオン/オフに切り替えると、一部のMAMアプリで「アプリが削除されました」というポップアップアラートが表示されることがあります。
- Secure Hub の登録を解除すると、一部の MAM アプリが引き続き使用可能になる場合があります。
- Secure Hub から MAM アプリのログ設定を変更しても、変更が有効にならない場合があります。

既知の問題

このリリースには既知の問題はありません。

Android 用 セキュアハブ 25.7.0

修正された問題

このバージョンでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

既知の問題

このリリースには既知の問題はありません。

iOS 用 セキュアハブ 25.6.0

修正された問題

- Secure Hub アプリを使用しているときに、ストアへのアクセス時に、何度か再試行しても「ストアを読み込めませんでした。もう一度お試しください。」というエラーメッセージが表示されたり、アプリがクラッシュしたりする場合があります。
- Mobile Device Management (MDM) のみのモードで Device Enrollment Program (DEP) または Return To Service (RTS) を使用する場合、そのプロセスはサポートされない可能性があります。
- オンプレミス Active Directory によって登録されたデバイスの Azure Active Directory (AAD) 登録中に、エラーが発生する場合があります。

既知の問題

このリリースには既知の問題はありません。

アンドロイド向けセキュアハブ 25.4.0

修正された問題

ユーザーがデバイスをワイプしてCEMコンソールから削除せずに同じデバイスを再登録した場合、サービスが無効になっているとポリシーを手動で更新できません。

既知の問題

このリリースには既知の問題はありません。

iOS 向け Secure Hub 25.1.0

修正された問題

このバージョンでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

既知の問題

このリリースには既知の問題はありません。

Android向けセキュアハブ 25.1.0

修正された問題

このバージョンでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

既知の問題

このリリースには既知の問題はありません。

iOS版セキュアハブ 24.11.0

修正された問題

iOSデバイスがDevice Enrollment Program (DEP) にすでに登録されているにもかかわらず、Secure Hubを開く際にユーザーにユーザープリンシパル名 (UPN) の入力を求めるプロンプトが表示されます。

既知の問題

このリリースには既知の問題はありません。

Android版セキュアハブ 24.10.0

修正された問題

このリリースには修正された問題はありません。

既知の問題

このリリースには既知の問題はありません。

iOS版セキュアハブ 24.9.0

修正された問題

このリリースには修正された問題はありません。

既知の問題

このリリースには既知の問題はありません。

Android用 セキュアハブ 24.8.0

修正された問題

このリリースには修正された問題はありません。

既知の問題

このリリースには既知の問題はありません。

Android 用 セキュアハブ 24.6.0

修正された問題

このリリースには修正された問題はありません。

既知の問題

このリリースには既知の問題はありません。

iOS 用 セキュアハブ 24.5.0

修正された問題

このリリースには修正された問題はありません。

既知の問題

このリリースには既知の問題はありません。

Android用セキュアハブ 24.3.0

修正された問題

ファクトリーリセットの制限ポリシーが「NO」に設定されている場合でも、ユーザーは会社所有のAndroid Enterpriseデバイスでファクトリーリセットを実行できます。この問題は、ユーザーがSecure Hubを再起動したときに発生します。

既知の問題

このリリースには既知の問題はありません。

iOS用セキュアハブ 24.1.0

修正された問題

- Palera1nアプリでiOSデバイスをジェイルブレイクしても、Citrix Endpoint Management™サーバーはデバイスをジェイルブレイク済みとして検出しません。その結果、Endpoint Managementサーバーはジェイルブレイクされたデバイスを工場出荷時の状態にリセットできません。さらに、Endpoint Managementサーバーはサーバーコンソールからジェイルブレイクされたデバイスのエントリをクリアできません。
- MAM SDKを使用してiOSアプリを管理すると、Secure Hubストアで次のいずれかの問題が発生します。
 - アプリのアップデートが利用可能になっても通知されません。
 - アプリが更新された後も、継続的にアップデートが通知されます。
- MAM SDKを使用してiOSアプリを管理すると、次のコンプライアンスアラートが表示されることがあります。

「このアプリはアカウントから削除されました。デバイスから削除できます。」

この問題は、MAM SDK と MDX ツールキットの両方を同じ iOS デバイスにインストールした場合に発生します。

Android 版 セキュアハブ 23.12.0

修正された問題

Citrix Gateway の資格情報が期限切れになると、Secure Hub は Citrix Gateway サーバーに接続するための新しい証明書を生成しない場合があります。その結果、Secure Hub は次のエラーメッセージを表示して起動に失敗します。

"接続中にエラーが発生しました。もう一度接続を試してください"

iOS 版 セキュアハブ 23.11.0

修正された問題

- Citrix Gateway クライアント証明書が期限切れになっても自動更新されないため、iOS デバイスで Secure Hub の認証が失敗します。この問題は、Citrix Gateway が TLSv1.3 プロトコルを使用している場合に発生します。
- Citrix Gateway を介して Secure Hub にサインインすると、次のエラーメッセージが表示されることがあります。

"サインオンできませんでした。資格情報が正しくありません。セッションを終了します"

この問題は、nFactor を使用して iOS デバイスを Citrix Endpoint Management (CEM) に登録した場合に発生します。

Android 用 セキュアハブ 23.10.0

修正された問題

Android バージョン 11 以降では、Android Enterprise デバイスの Wi-Fi ポリシーが展開されない場合があります。この問題は、Wi-Fi ポリシーの匿名フィールドにドメイン値が指定されていない場合に発生します。

既知の問題

このリリースには既知の問題はありません。

Android 用 セキュアハブ 23.9.0

修正された問題

このリリースでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

既知の問題

このリリースには既知の問題はありません。

iOS 用 セキュアハブ 23.8.1

修正された問題

- ユーザーが Secure Hub 23.8.0 を使用してデバイスを登録しようとし、ユーザー名が `sAMAccount` の形式である場合、プロセスは次のエラーメッセージで失敗する可能性があります。

「登録に失敗しました。MAM にログインしたユーザーが登録済みユーザーと一致しません。
もう一度登録を試してください。」

既知の問題

このリリースには既知の問題はありません。

iOS 用 セキュアハブ 23.8.0

修正された問題

- nFactor を使用して iOS デバイスを Citrix Endpoint Management (CEM) に登録すると、マイクロ VPN トンネルの確立に問題が発生する可能性があります。

既知の問題

このリリースには既知の問題はありません。

以前のバージョンにおける既知の問題と修正された問題

Secure Hub の以前のバージョンにおける既知の問題と修正された問題については、[Secure Hub の既知の問題と修正された問題の履歴](#) を参照してください。

Secure Hub の既知の修正済み問題の履歴

この記事では、最近サポートされているバージョンよりも前のバージョンの Secure Hub の修正済みおよび既知の問題を一覧表示します。最新のドキュメントについては、[Citrix Secure Hub](#)を参照してください。

アンドロイド用 セキュアハブ 23.7.0

修正された問題

- Android Enterprise プラットフォームでは、登録後に管理対象構成ポリシーがデバイスに適用されない場合があります。
- Android Enterprise プラットフォームでは、登録後に必要なパブリックアプリストアアプリがデバイスに自動的にインストールされない場合があります。
- デバイスを再起動してロック解除しない場合、IT 管理者によって発行されたロックコマンドを通じてデバイスのパスコードをリセットできない場合があります。

この方法は、エンドユーザーがデバイスのパスコードを忘れたり、デバイスを紛失したりした場合に役立ちます。管理者にデバイスのパスコードをリセットするか、ロックコマンドを通じてデバイスをロックするように依頼できます。

- エンドユーザーが特定の Android デバイスで登録のために Secure Hub を開くと、Secure Hub アプリが応答しなくなる

この問題は、ライセンスの有効期限が切れているために MDM 登録が失敗した場合に発生します。その結果、Secure Mail アプリは利用できません。

- 認証目的で Citrix Gateway を ID プロバイダー (IdP) として構成し、ゲートウェイへのネットワーク接続が不安定な場合、認証が失敗し、エンドユーザーは Secure Hub にサインインできません。

既知の問題

このリリースには既知の問題はありません。

アイオーエス用 セキュアハブ 23.4.0

修正された問題

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題に対処しています。

既知の問題

このリリースには既知の問題はありません。

アンドロイド用セキュアハブ 23.4.1

修正された問題

- Secure Hub アプリを起動すると、読み込みスピナー UI が表示されます。この問題は、デッドロック状態が原因で発生します。

既知の問題

このリリースには既知の問題はありません。

アンドロイド用セキュアハブ 23.4.0

修正された問題

- デバイスを Android 11 から Android 12、そして Android 13 にアップグレードすると、Secure Hub アプリが起動に失敗します。
- 企業所有の単一用途 (COSU) デバイスに登録した後、Secure Hub アプリは Citrix PIN の代わりに Active Directory (AD) パスワードを要求します。この問題は、Secure Hub バージョン 23.2.0 以前でキャッシュされた資格情報が失われたために発生する可能性があります。
- コード内の例外により PIN が受け入れられないため、Secure Hub アプリが応答しなくなります。

既知の問題

このリリースには既知の問題はありません。

Android向けセキュアハブ 23.2.0

修正された問題

- 企業所有の単一用途 (COSU) デバイスに登録し、制限ポリシーでSDカードの使用が許可されている場合でも、これらのデバイスで外部SDカードにアクセスできない場合があります。この問題は、専用デバイスであるために発生します。
- Android Enterpriseデバイスのパスワード有効期限に関するパスコードポリシー設定が期待どおりに機能しません。パスコード変更のプロンプトが表示されず、手動でパスコードを変更する必要があります。
- 時折、デバイスをAndroid 11からAndroid 13にアップグレードした後、Secure Hubアプリが応答しなくなります。
- Secure Hubにサインインするたびに、アプリがCitrix PINではなくActive Directory (AD) パスワードを要求します。この問題は、ADパスワードを変更した後に発生します。
- Active Directory (AD) パスワードを変更した後、Secure Hubへのサインイン試行が以下のエラーメッセージとともに失敗します。

資格情報が正しくありません。

セキュアハブ 22.11.0

- CEMコンソールから**Enrollment App**チャンネルにプッシュメッセージが送信された場合、メッセージはデバイスに届きますが、サウンドアラートがトリガーされません。
- **資格情報ポリシー**を構成し、証明書エイリアスを定義すると、カスタム証明書エイリアスを使用している場合にCitrix SSOアプリが認証エラーでVPNに接続できません。以下のエラーメッセージが表示されます。

接続エラー: *certificate ID*に接続できません。インターネット接続を確認し、*certificate ID*の設定を検証してください。

この問題は、Citrix SSOアプリの証明書をアプリが使用することを許可した場合に発生します。

セキュアハブ 22.9.0

このリリースには、既知の問題や修正された問題はありません。

セキュアハブ 22.7.0

修正された問題

- Mobile Device Experience (MDX)からCitrix Mobile Application Management (MAM) SDKに切り替え、XenMobile Serverを10.13 RP4にアップグレードした後、Secure Hub/Secure Webを介してイントラネットサイトにアクセスできない場合があります。

次のエラーメッセージが表示されます: "Err_Name_not_resolved"。

- 登録構成がWork Profile for Company Owned Devices (WPCOD)であるワークプロファイルには、管理対象構成ポリシー設定が適用されません。この問題は、認証がIdentity Provider (IdP)を介して行われ、ワークプロファイルがプロビジョニング済みとしてマークされていない場合に発生します。

セキュアハブ 22.6.0

このリリースには、既知の問題も修正された問題もありません。

セキュアハブ 22.5.0

このリリースには、既知の問題も修正された問題もありません。

セキュアハブ 22.4.0

このリリースには、既知の問題も修正された問題もありません。

セキュアハブ 22.2.0

Secure Hub 22.2.0の既知の問題

このリリースには、既知の問題はありません。

Secure Hub 22.2.0の修正された問題

iOS版セキュアハブ

- iOS版Secure Hubでは、Apple Deployment Programを通じて登録されたデバイスで、PINを使用して登録するよう求められます。
- デバイスがアイドル状態になった後、Secure Mailにサインインすると、iOS版Secure Hubが次のエラーメッセージとともに開きます。

「Secure Hubは、このアプリを承認する必要があります。」

承認をクリックして資格情報を入力すると、認証がループに入ります。再起動後も再認証またはサインインできません。

- iOS 15.1を実行しているデバイスでエラーを報告すると、iOS版Secure Hubが応答しなくなります。
- iOS版Secure Hubでは、新しい通知がないにもかかわらず、バッジカウントが1または2と表示されます。
- iOS版Secure Hubでは、一部のデバイスで登録が失敗する場合があります。
- Citrix Gatewayセッションタイムアウトポリシーの値を30日に設定すると、iOS版Secure Hubは24～72時間ごとにユーザーに再認証を求めます。

Android版セキュアハブ

- Samsung DeXモードでPINを入力すると、Secure Hubが応答しなくなります。
- Samsung S20デバイスをフルマネージドモードでAndroid Enterpriseに登録すると、次のエラーが表示されます。「無効なサーバー証明書」
- Android 10または11を実行しているデバイスの登録が失敗し、次のエラーメッセージが表示されます。「セキュリティポリシーにより接続できません」
- Android版Secure Hubに登録する際、ポートレートモードからランドスケープモードに切り替えると、資格情報がランダムな数字に置き換えられます。

セキュアハブ 21.11.0

Secure Hub 21.11.0 の既知の問題

このリリースには既知の問題はありません。

Secure Hub 21.11.0 で修正された問題

Android 用 セキュアハブ

- Android 用 Secure Hub への登録中に、「証明書が見つかりません」というエラーメッセージが表示されます。「証明書をインストール」をクリックすると、証明書のない空のリンクが表示されます。「キャンセル」をクリックすると、認証画面が表示されます。この問題は、Secure Hub からサインアウトして再度サインインした際にも発生します。

セキュアハブ 21.10.0

Secure Hub 21.10.0 の既知の問題

このリリースには既知の問題はありません。

Secure Hub 21.10.0 で修正された問題

iOS 用 セキュアハブ

- iOS 用 Secure Hub では、Apple Deployment Program を介して登録されたデバイスで、PIN を使用して登録するよう求められます。

Android 用 セキュアハブ

- 企業所有デバイスモードでワークプロファイルに登録するための Android デバイスの登録プロファイルを作成する際、「BYOD ワークプロファイル」設定を有効にする必要があります。この設定を有効にしないと、デバイスの登録に失敗します。
- Android 用 Secure Hub にサインインする際、メール ID が自動入力されます。

セキュアハブ 21.8.0

iOS版セキュアハブ

Secure Hub 21.8.0の既知の問題

このリリースには既知の問題はありません。

Secure Hub 21.8.0で修正された問題

- デバイスがアイドル状態になった後、Secure Mailにログインすると、iOS版Secure Hubが開き、ログオンを試行しますが、ログオン要求は失敗します。Secure Mailはログオンを繰り返し要求し、サインオンループが発生します。
- ユーザー名またはパスワードに特定の特殊文字が含まれるユーザーは、登録できません。

セキュアハブ 21.7.1

Android版セキュアハブ

このリリースには既知の問題も修正された問題もありません。

以前のバージョンにおける既知の問題と修正された問題

Secure Hubの以前のバージョンにおける既知の問題と修正された問題については、[Secure Hubの既知の問題と修正された問題の履歴](#)を参照してください。

セキュアハブ 21.7.1

Android版Secure Hub

このリリースには既知の問題も修正された問題也没有ありません。

セキュアハブ 21.7.0

iOS版 セキュアハブ

このリリースには、既知の問題も修正された問題也没有ありません。

Android版 セキュアハブ

Secure Hub 21.7.0の既知の問題

このリリースには既知の問題はありません。

Secure Hub 21.7.0で修正された問題

- Android版Secure Hubで、デバイスを再起動した後、> に移動すると、Secure MailおよびSecure Webのログがありません。

セキュアハブ 21.6.0

iOS版 セキュアハブ

Secure Hub 21.6.0の既知の問題

このリリースには既知の問題はありません。

Secure Hub 21.6.0で修正された問題

iOS版Secure Hubで、ユーザープリンシパル名（UPN）を使用してデバイスを登録すると、ユーザー名が自動入力されません。この問題は、自動検出サービスが有効になっている場合に発生します。

Android版 セキュアハブ

Secure Hub 21.6.0の既知の問題

Secure Hub for Androidでは、提供されたFQDNに大文字が含まれている場合、デバイスをMDM+MAMモードで登録できません。代わりに、デバイスはMAMモードで登録されます。

Secure Hub 21.6.0で修正された問題

Secure Hub for Androidでは、Samsung Knoxを実行している工場出荷時設定にリセットされたデバイスをデバイス管理者モードで登録できません。

セキュアハブ 21.5.1

iOS用セキュアハブ

このリリースには、既知の問題も修正された問題もありません。

アンドロイド用セキュアハブ

このリリースには、既知の問題も修正された問題もありません。

セキュアハブ 21.5.0

Secure Hub 21.5.0の既知の問題

このリリースには既知の問題はありません。

Secure Hub 21.5.0で修正された問題

Secure Hub for Androidでは、Android EnterpriseデバイスにWi-Fiデバイスポリシーを展開できません。ポリシーは保留状態のままになります。

セキュアハブ 21.4.0

このリリースには、既知の問題も修正された問題もありません。

セキュアハブ 21.3.2

iOS向けセキュアハブ

Secure Hub 21.3.2の既知の問題

このリリースには既知の問題はありません。

Secure Hub 21.3.2で修正された問題

Citrix PINを入力した後、Citrix Endpoint Management™にデバイスを登録できません。Secure HubはPIN要件の正しいメッセージを表示しません。

セキュアハブ 21.3.0

Secure Hub 21.3.0の既知の問題

Android版Secure Hubバージョン20.9.0以降では、Google Pixel 2デバイスでVPNモードで接続できません。

Secure Hub 21.3.0で修正された問題

- Android版Secure Hubでは、SIMカードが挿入されていないデバイスに対して、集積回路カードID (ICCID) が表示されます。
- Android版Secure Hubでは、デバイスを再起動すると、インストールされているモバイル生産性アプリがマイアプリ画面に表示されません。
- Android版Secure Hubでは、誤ったパスワードを複数回入力し、デバイスを再起動しようとすると、Android Enterpriseデバイスのロックを解除できません。次のエラーメッセージが表示されます: 電話の電源がオフになりました。IT管理者に連絡してください。

セキュアハブ 21.2.0

Android版セキュアハブ

Secure Hub 21.2.0 の既知の問題

Android 版 Secure Hub では、デバイスを再起動すると、インストールされているモバイル生産性アプリがマイアプリ画面に表示されません。

Secure Hub 21.2.0 で修正された問題

- Android 版 Secure Hub がデバイスの登録中にハングします。
- Android 版 Secure Hub の特定のバージョンでは、Samsung Knox デバイスで登録が完了すると、ホームボタンと戻るボタンが表示されません。

セキュアハブ 21.1.0

Secure Hub 21.1.0 の既知の問題

このリリースには既知の問題はありません。

Secure Hub 21.1.0 で修正された問題

- Android を実行しているデバイスでは、接続スケジューリングデバイスポリシーが有効になっている場合、Secure Hub が Citrix Endpoint Management への接続に失敗します。
- 特定の登録済み Samsung デバイスでは、Citrix Endpoint Management コンソールに誤ったシリアル番号が報告されます。

セキュアハブ 20.12.0

Secure Hub 20.12.0 の既知の問題

このリリースには既知の問題はありません。

Secure Hub 20.12.0 で修正された問題

- iOS版Secure Hubでは、デバイスを登録できません。次のエラーが表示されます: **デバイスが登録されていません**。
- iOS版Secure Hubでは、MAM+MDMに登録されているデバイスのユーザーエージェント文字列にOSバージョンが含まれていません。
- Android Enterpriseデバイスでは、登録中にSecure Hubがクラッシュします。
- Android版Secure Hubバージョン20.11.0は、特定のSamsungデバイスでクラッシュします。

セキュアハブ 20.11.0

Android版セキュアハブ

Secure Hub 20.11.0の既知の問題

このリリースには既知の問題はありません。

Secure Hub 20.11.0で修正された問題

一部のSamsungデバイスでAndroid版Secure Hubがクラッシュし、次のエラーが表示されます:
Secure Hubは動作を停止し続けています。

セキュアハブ 20.10.5

Secure Hub 20.10.5の既知の問題

このリリースには既知の問題はありません。

Secure Hub 20.10.5で修正された問題

- Android 11を実行している企業所有シングルユース (COSU) デバイスでは、Secure Hubをデフォルトのランチャーとして設定できません。
- Androidデバイスで、特定のSamsungデバイスにおいてワークプロファイルの作成に失敗します。次のエラーが表示されます: **ワークプロファイルを構成できません**。
- Citrix Endpoint Management AutoDiscovery Serviceを介したAndroidデバイスのモバイルアプリ管理 (MAM) 登録が失敗します。
- iOSデバイスで、特定のアプリを起動できません。Secure Hubのアップデートが利用できない場合でも、このアプリを使用するには**Secure Hubを更新してください**というエラーが表示されます。
- iOSデバイスで、最大オフライン期間が経過するとSecure Mailは認証を要求します。その後、Secure MailはSecure Hubに切り替わり、使用できなくなります。

セキュアハブ 20.9.0

Secure Hub 20.9.0における既知の問題

このリリースには既知の問題はありません。

Secure Hub 20.9.0における修正された問題

- iOS版Secure Hubで、証明書ピン留めが有効になっている場合、いずれかのサーバーからピン留めされた証明書が正しくない場合でも、サーバー間で接続が確立されます。
- iOS版Secure Hubで、通知を受信できません。次のエラーが表示されます: **有効なSecure Hub トークンを持つデバイスがありません。**

セキュアハブ 20.7.5

Secure Hub 20.7.5における既知の問題

Android 11を実行している企業所有の単一用途 (COSU) デバイスで、Secure Hubをデフォルトのランチャーとして設定できません。

Secure Hub 20.7.5における修正された問題

- Android版Secure Hubで、証明書ピン留めが有効になっている場合、Androidデバイスの登録が失敗します。
- Secure Hub for Androidでは、制限ポリシーの日付と時刻の**変更機能**がSamsungデバイスで動作しません。
- Secure Hub for Androidでは、ファイアウォールポリシーがバージョン19.12.5以降を実行しているSamsungデバイスで動作しません。
- Secure Hub for Androidでは、**マイアプリ**からアプリをアンインストールできません。

セキュアハブ 20.6.5

このリリースには既知の問題も修正された問題もありません

セキュアハブ 20.3.0

iOS用セキュアハブ

このリリースには既知の問題も修正された問題もありません。

セキュアハブ 20.2.0

iOS用セキュアハブ

Secure Hub 20.2.0の既知の問題

このリリースには既知の問題はありません。

Secure Hub 20.2.0で修正された問題

- Secure Hub for iOSでは、モバイルアプリケーション管理 (MAM) の登録が一部のiOSデバイスで失敗します。
- Secure Hub for iOSでは、デバイスからアプリがランダムに削除されます。

セキュアハブ 20.1.5

このリリースには、既知の、または修正済みの問題はありません。

セキュアハブ 19.12.5

Secure Hub 19.12.5における既知の問題

このリリースには、既知の問題はありません。

Secure Hub 19.12.5における修正済みの問題

iOS 13を実行しているデバイスでは、ユーザー証明書の有効期限を確認するためにSSLエラーコードに依存するのではなく、XenMobile® Serverのユーザー証明書は実際の有効期限日に確認および更新されます。

セキュアハブ 19.11.5

Secure Hub 19.11.5における既知の問題

このリリースには、既知の問題はありません。

Secure Hub 19.11.5における修正済みの問題

iOS版Secure Hubでは、ユーザーエントロピーを無効にした後、MDXでラップされたアプリの登録が失敗します。

セキュアハブ 19.10.5

Android版 セキュアハブ

Secure Hub 19.10.5における既知の問題

このリリースには既知の問題はありません。

Secure Hub 19.10.5 で修正された問題

Android版Secure Hubでは、資格情報ポリシーが構成されている場合、Secure Hubバージョン19.10.5を実行しているデバイスにビジネスアプリをインストールできません。

セキュアハブ 19.10.0

Secure Hub 19.10.0 の既知の問題

- Android版Secure Hubでは、Androidバージョン10を実行しているGoogle Pixel 2デバイスのデバイス所有者モードでの登録が、権限の失敗により失敗します。
- Android版Secure Hubでは、Androidバージョン10を実行しているGoogle Pixelデバイスで、デバイス所有者モードでのデバイス登録が、位置情報権限の検証の失敗により失敗します。

Secure Hub 19.10.0 で修正された問題

このリリースには修正された問題はありません。

セキュアハブ 19.9.5

このリリースには既知の問題も修正された問題もありません。

Secure Hub 19.9.0 バージョン

Secure Hub 19.9.0 の既知の問題

Android Enterpriseが有効なAndroid版Secure Hub 19.9.0では、Pixel 2デバイスで次の問題が発生します。資格情報ポリシーが正常に展開されません。その結果、ユーザーはパスワードとともに証明書を要求されず、証明書もインストールされません。回避策として、ユーザーはアプリの **Preferences > Device Information** からポリシーを手動で更新できます。そこから、**Refresh policy** を押し、資格情報を入力し、成功メッセージを確認します。

Secure Hub 19.9.0 で修正された問題

このリリースには修正された問題はありません。

Secure Hub 19.8.5 バージョン

このリリースには既知の問題も修正された問題もありません。

Secure Hub バージョン 19.8.0

Secure Hub 19.8.0 の既知の問題

iOS版Secure Hubで、共有デバイスで誤ったパスワードを入力し、**Switch user**をタップして再度ログインしようとする、**Please wait**メッセージが無限に表示されます。

Secure Hub 19.8.0 で修正された問題

フルVPN経由で接続されている場合、モバイルデバイス管理ネットワークが不適切にルーティングされます。

Secure Hub バージョン 19.7.5

Secure Hub 19.7.5 の既知の問題

このリリースには既知の問題はありません。

Secure Hub 19.7.5 で修正された問題

- Android版Secure Hubで、Webクリップをインストールするためのプロンプトが急速に表示され、Secure Hub PINの設定を妨げます。
- Samsung Knoxデバイスバージョン3以降で、Secure Hubをプロファイル所有者モードで登録し、Android Enterpriseプラットフォーム向けに**Samsung MDM license key**ポリシーをプッシュすると、**Device Container Password Reset**コマンドが失敗します。
- Apple Storeからの新しいアプリURLを使用してMAMモードでパブリックアプリを設定しようとする、iOS版Secure Hubで以下のエラーが表示されます: **ストアを読み込めませんでした。もう一度お試しください。** 回避策については<https://support.citrix.com/article/CTX256704>を参照してください。
- Secure Hub for Androidでは、フルVPNトンネルが確立されている場合、MDXアプリをインストールできません。

- 共有デバイスモードでSecure Hub for Androidを実行しているPoint Mobile PM80デバイスでセッションタイムアウトが発生すると、再度ログインできません。
- Secure Hub for Androidで、内部でラップされたアプリケーションをインストールして起動した後、次のエラーが表示されます: このアプリでのデータの暗号化方法が変更されました。このアプリを削除して再インストールしてください。

セキュアハブ 19.6.5

Secure Hub 19.6.5の既知の問題

このリリースには既知の問題はありません

Secure Hub 19.6.5で修正された問題

- iOSを実行しているデバイスでは、グローバルサーバー負荷分散のフェールオーバーが発生した場合、Secure Hubはストアをロードしません。
- Secure Hub for Androidでは、更新ポリシーが失敗します。その結果、新しいデバイスポリシーを展開できません。
- Secure Hub for Androidでは、Samsung S10デバイスでの登録または更新ポリシーアクションに時間がかかります。
- Androidを実行しているデバイスでは、Secure HubがフルVPN接続を確立すると、非管理対象アプリの接続が失われます。

セキュアハブ 19.5.5

Secure Hub 19.5.5の既知の問題

- Secure Hub for Androidでは、Corporate Owned Single Use (COSU) モードのデバイスは、登録後数分で接続が失われ、GCMが有効になっていても通知を受信しません。
- デバイスにロケーションポリシーをデプロイする際、Profile OwnerモードとDevice Ownerモードの両方で同時にデプロイすると、Device Ownerモードのユーザーアカウントが削除されます。この問題は、NFCバンブ登録時、およびEndpoint ManagementがMDMモードで構成されている場合に発生します。

Secure Hub 19.5.5 で修正された問題

- このリリース以降、Secure Hub は Android 5.0 以降を実行しているデバイスのみをサポートします。

- Android 版 Secure Hub で、デバイスをデバイス所有者モードで登録し、新しいパスワードを設定します。最初の試行ではデバイスはロックされません。

セキュアハブ 19.5.0

Secure Hub 19.5.0 の既知の問題

- 登録後、OnePlus Android バージョン 7.1.1 および OnePlus 5T Android バージョン 9.0.3 のデバイスでは、Citrix PIN の入力を求められるようにするには、Secure Hub の手動再起動が必要です。
- Android 版 Secure Hub では、ポリシーを更新するかストアを更新しない限り、必要なアプリは Android デバイスに展開されません。

Secure Hub 19.5.0 で修正された問題

- このリリース以降、Secure Hub は Android 5.0 以降を実行しているデバイスのみをサポートします。
- Android 版 Secure Hub では、サーバー証明書に複数のサブジェクト代替名が存在する場合、Android 6.0 デバイスの登録に失敗します。
- Android 版 Secure Hub では、デバイスの登録解除後に管理対象アプリがアンインストールされません。
- Samsung S9 デバイスで、ユーザーが Android P に更新した後、次の問題が発生します。Endpoint Management 経由でデバイスのパスワードを変更しても、デバイスのパスワードは変更されません。代わりに画面が真っ暗になり、Endpoint Management コンソールにはロックされたデバイスのステータスが表示されます。

セキュアハブ 19.4.5

Secure Hub 19.4.5 の既知の問題

このリリースには既知の問題はありません。

Secure Hub 19.4.5で修正された問題

iOSデバイスでは、デバイス登録リンクをクリックしても、Secure HubにEndpoint Management FQDNインスタンス名が自動入力されません。デバイス登録要求が失敗します。

セキュアハブ 19.3.5

Secure Hub 19.3.5の既知の問題

iOS版Secure Hubから通知が送信されても、Secure Hubの通知バッジカウントが更新されません。

Secure Hub 19.3.5で修正された問題

- Android版Secure Hubで、共有デバイスを登録し、**Webclip**ポリシーを展開してWebアプリとSaaSアプリを追加すると、展開は成功します。しかし、この展開はCitrix Endpoint Managementコンソールの**アプリインベントリ**画面で失敗として表示されます。
- Android版Secure Hubで、ユーザーがセキュアPINでログインするとVPNトンネルが確立されますが、Secure WebはどのWebサイトも読み込みません。ただし、Secure Webを閉じて再度開くと、Webサイトは期待どおりに読み込まれます。
- Microsoft Intuneポリシーで構成されたAndroid版Secure Mailは、認証後に空白の画面を返します。
- Android版Secure Hubで、暗号化を無効にしたアプリがSecure Hubから暗号化キーを取得しようとしています。
- Intune Company Portalバージョン5.0.4324.0がインストールされている場合、Android版Secure Mailは起動時にクラッシュします。
- Android版Secure Hubで、Android 7.1.1で動作する企業所有の単一用途 (COSU) Android Enterpriseデバイスでは、システムアプリを使用できません。
- Android版Secure Hubで、Google Playから複数のアプリを必須アプリとして構成し、登録しようすると、最初のアプリのインストールを促されます。最初のプロンプトの直後に、2番目のアプリのインストールを促す別のプロンプトが表示され、その後も同様に続きます。

セキュアハブ 19.3.0

Secure Hub 19.3.0の既知の問題

- Android版Secure Hubで、共有デバイスを登録し、Webクリップポリシーを展開してWebアプリとSaaSアプリを追加すると、展開は成功します。ただし、この展開はCitrix Endpoint Managementコンソールの**アプリインベントリ**画面で失敗として表示されます。
- Android Enterpriseデバイスで、ロケーションポリシーのジオフェンス違反に対してロックアクションが設定されている場合、デバイスはシステム生成のパスコードを使用する代わりに、新しいパスコードを設定するように求めます。

Secure Hub 19.3.0で修正された問題

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

セキュアハブ 19.2.0

Secure Hub 19.2.0の既知の問題

このリリースには既知の問題はありません。

Secure Hub 19.2.0で修正された問題

- iOS版Secure Hubで、ユーザーがSecure Hubストアからログオフすると、「Network request to fetch apps is timed out from Server.」というSSLハンドシェイク失敗メッセージが繰り返し表示されます。
- Android Enterpriseのファイルデバイスポリシーは、ワークプロファイルモードのAndroidデバイスに展開されません。
- Android版Secure Hubで、共有デバイスでの新規ユーザーのログイン認証に時間がかかります。登録済みユーザーとしてログオフし、新規ユーザーとしてログインしようとすると、デバイスを再起動するまでSecure Hubはロードし続けます。
- Android版Secure Hubで、クラウドのお客様は外部IDプロバイダーを使用してAndroid Enterpriseデバイスを登録できません。
- Android版Secure Hubで、COSU（Corporate Owned Single Use）モードの場合、Secure Hubでアプリアイコンが重なって表示されます。
- Android版Secure Hubで、既存のセットアップで証明書ピン留めが有効になっている場合、証明書に複数のサブジェクト代替名があるときに認証が失敗し、初回ユーザー画面に戻ります。

セキュアハブ 19.1.5

Secure Hub 19.1.5 の既知の問題

- Android 版 Secure Hub で、パスワードポリシーの変更によりパスワードを更新すると、バッジ付きアプリが Samsung Galaxy S8 デバイスに表示されません。
- Android 版 Secure Hub で、Files デバイスポリシー Android Enterprise が、ワークプロファイルモードのデバイスに展開されません。

Secure Hub 19.1.5 で修正された問題

- Android 版 Secure Hub で、ユーザーが Secure PIN でログインすると VPN トンネルが確立されますが、Secure Web はどの Web サイトも読み込みません。ただし、Secure Web を閉じて再度開くと、Web サイトは期待どおりに読み込まれます。
- Android 版 Secure Hub で、Secure PIN でログオンすると VPN トンネルが確立されますが、Secure Web はどの Web サイトも読み込みません。ただし、Secure Web を閉じて再度開くと、Web サイトは期待どおりに読み込まれます。
- Android 版 Secure Hub で、TechXpert という社内アプリのログをキャプチャしようとする、Secure Hub が再起動し、再認証を求められます。

セキュアハブ 19.1.0

Secure Hub 19.1.0 の既知の問題

iOS 版 Secure Hub で、MDX および Web または SaaS アプリを展開すると、それらは **My Apps** 画面に表示されます。**More** をタップすると、古い UI ブランドの形式を持つ **Delete** および **Cancel** オプションを含むポップアップが表示されます。

Secure Hub 18.12.0 で修正された問題

- Android For Work に登録されている Samsung Knox デバイスで、パスワードポリシーが 1 日または 2 日で期限切れになるように構成されている場合、**Password Expired** メッセージが繰り返し表示されます。
- QR コード登録方法を使用して、OnePlus 5T デバイスを Android Enterprise に登録できません。

セキュアハブ 18.11.0

Secure Hub 18.11.0 で修正された問題

- Shared Deviceモードに登録されているAndroidデバイスでシングルサインオンを実行できません。次のエラーが表示されます: 現時点では会社の資格情報を取得できません。管理者ポリシーにより、ShareFileへの手動ログインはブロックされています。
- 企業所有の単一用途（COSU）デバイスでAndroidの音量レベルを編集できません。

セキュアハブ 18.10.5

Secure Hub 18.10.5で修正された問題

- XenMobile ServerでFIPSモードが有効になっている場合、ユーザーがSecure Hub for iOSをバージョン18.10.5に更新した後、アプリを開くと暗号化関連のエラーメッセージが表示されます。

Secure Hubバージョン10.8.25～18.10.6

Secure Hubバージョン10.8.25～18.10.6で修正された問題

- Secure Hubバージョン10.8.25～18.10.6（Android）には既知の問題はありません。以下の問題はSecure Hubで修正されています。このリストには、Secure Hubに影響するMDXの問題が含まれています。

セキュアハブ 18.10.0

Secure Hub 18.10.0で修正された問題

- EMSコンソールでMVPNポリシーがオフになっている場合、Intune管理アプリを開こうとするとSecure Hubに空白の画面が表示されます。

セキュアハブ 10.8.60

Secure Hub 10.8.60で修正された問題

- Samsung Galaxy Tab Active 2 SM-T395デバイスでは、管理者がXenMobileで工場出荷時設定へのリセット無効化の制限を設定している場合、Secure Hub for Androidの完全ワイプセキュリティアクションが失敗します。
- VPNポリシーが構成されており、Citrix SSOアプリケーションがデバイスにインストールされていない場合、デバイスの登録中にSecure Hub for Androidが応答しなくなります。戻るボタンをタップするか、アプリを再起動すると応答するようになります。
- Android Enterprise環境でデバイス所有者モードで登録中に、Android版Secure Hubがクラッシュします。
- ユーザーがiOS版Secure Hubに有効なPINを入力した後、Secure HubがPINを繰り返し要求します。

- Android Enterprise環境でプロファイル所有者モードで登録中に、Android版Secure Hubがクラッシュします。
- Android版Secure HubでAndroid Enterpriseを使用すると、デフォルトでGoogle Chromeがインストールされます。
- iOS版Secure Hubをバージョン10.8.55にアップグレードすると、既存または新規のiOSデバイスの登録が許可されません。

セキュアハブ 10.8.55

Secure Hub 10.8.55で修正された問題

- G Suiteの資格情報がEndpoint Managementの資格情報と異なる場合、ユーザーはAndroid for Workアカウントに登録するためにSecure Hubにサインオンできません。

バージョン10.8.55で修正されたMDX関連の問題

- 優先VPNモードがSecureBrowseに設定されている場合、エンタープライズアプリで内部リソースへの接続の問題が発生する可能性があります。
- アプリケーションクラスとしてandroid.support.multidex.MultiDexApplicationまたはandroid.app.Applicationを指定するアプリは、トンネル化 - Web SSOモードで内部ネットワークに接続できません。
- Androidデバイスでは、複数の証明書が生成され、有効期限前に失効しています。

セキュアハブ 10.8.55

Secure Hub 10.8.55の既知の問題

- デバイスからSecure Hubアカウントを削除した後、MDMの再登録が失敗します。

セキュアハブ 10.8.50

Secure Hub 10.8.50 の既知の問題

- Android 版 Secure Hub では、ユーザーは Web リンクのショートカットを追加できません。

セキュアハブ 10.8.35

Secure Hub 10.8.35 で修正された問題

- Android O では、ポリシーによって作成されたショートカットがデバイスのホーム画面に表示されません。この動作は Android O の設計によるものです。
- Android では、一定期間操作がないと Secure Hub が Samsung タブレットで開かなくなります。
- Android 版 Secure Hub では、Samsung Knox デバイスにプッシュポリシーを展開できません。
- iOS 版 Secure Hub では、次のような問題が時折発生します: ユーザーが Active Directory パスワードを変更した後、PIN を繰り返し入力し続ける必要があります。

セキュアハブ 10.8.25

Secure Hub 10.8.25 で修正された問題

- MDX Toolkit バージョン 10.7.20 でラップされたサードパーティの iOS Cordova アプリの場合、画面コンテンツを隠すポリシーを有効にすると、PIN 画面の代わりに黒い画面が表示されます。
- Android 7 を実行している Zebra T51 デバイスでは、ユーザーは Citrix Launcher アプリをインストールできません。

セキュアハブ 10.8.20

Secure Hub 10.8.20 で修正された問題

- ユーザーが Android デバイスをバージョン 8 (Oreo) にアップデートした後: Endpoint Management から展開するエンタープライズアプリまたは .apk アプリをアプリストアからインストールできません。サードパーティ製アプリのインストールを有効にしても、この問題は解決しません。この問題は Samsung デバイスに限定されません。

セキュアハブ 10.8.15

Secure Hub 10.8.15 で修正された問題

- Android O を実行しているデバイスで、Android 版 Secure Hub が位置情報の取得中にクラッシュします。

セキュアハブ 10.8.10

Secure Hub 10.8.10で修正された問題

- Androidデバイスで、複数のアプリが自動的にインストールされない場合、またはユーザーが自分でインストールをクリックしない場合、アプリはダウンロードを続けます。その結果、データ使用量が多くなります。
- Android 7以降を実行しているデバイスで: XenMobile Serverからパスワード付きのロックセキュリティアクションをデバイスに送信すると、デバイスはロックされます。ただし、ユーザーが既存のロック画面パスワードを持っている場合、デバイスのパスワードは変更されません。ユーザーは元のパスコードを使用してデバイスのロックを解除できます。

March 19, 2018のiOS版Secure Hubのアップデート: iOS版Secure Hubバージョン10.8.6が、VPPアプリポリシーに関する問題を修正するために利用可能です。

Secure Hub for Android and iOS - プレビュー

今後のリリースで追加される新機能と解決済みの問題にご期待ください。

現在のリリースの詳細については、[Secure Hubの新機能](#)を参照してください。

機能フラグ管理

管理者は、プレビュー機能にアクセスし、本番環境で機能を動的に制御するために、機能フラグを管理できます。機能フラグの下にある機能が最適に機能するようにするには、URL `features.netscalergateway.net` へのトラフィックを有効にする必要があります。詳細については、「機能フラグ管理」を参照してください(/ja-jp/mobile-productivity-apps/feature-flag-management.html)。

認証プロンプトのシナリオ

さまざまなシナリオで、ユーザーはデバイスに資格情報を入力してSecure Hubで認証するように求められます。

シナリオは、以下の要因によって異なります。

- Endpoint Managementコンソール設定でのMDXアプリポリシーとクライアントプロパティの構成。
- 認証がオフラインで行われるかオンラインで行われるか（デバイスがEndpoint Managementへのネットワーク接続を必要とするか）。

さらに、ユーザーが入力する資格情報の種類（Active Directoryパスワード、Citrix PINまたはパスコード、ワンタイムパスワード、指紋認証（iOSではTouch IDとして知られる）など）も、認証の種類と認証の頻度に基づいて変化します。

まず、認証プロンプトが表示されるシナリオから始めましょう。

- **デバイスの再起動:** ユーザーがデバイスを再起動すると、Secure Hubで再認証する必要があります。
- **オフラインでの非アクティブ（タイムアウト）:** App Passcode MDXポリシーが有効になっている（デフォルト）場合、Endpoint ManagementクライアントプロパティであるInactivity Timerが適用されます。Inactivity Timerは、セキュアコンテナを使用するいずれかのアプリでユーザーアクティビティがないまま経過できる時間の長さを制限します。

Inactivity Timerが期限切れになると、ユーザーはデバイス上のセキュアコンテナに再認証する必要があります。たとえば、ユーザーがデバイスを置いて離れ、Inactivity Timerが期限切れになった場合、他の人がデバイスを拾ってコンテナ内の機密データにアクセスすることはできません。

Inactivity Timer clientプロパティはEndpoint Managementコンソールで設定します。デフォルトは15分です。App Passcodeが**ON**に設定されていることと、Inactivity Timer clientプロパティの組み合わせは、おそらく最も一般的な認証プロンプトシナリオの原因となります。

- **Secure Hubからのサインオフ:** ユーザーがSecure Hubからサインオフすると、次回Secure HubまたはMDXアプリにアクセスする際に、アプリがApp Passcode MDXポリシーとInactivity Timerのステータスによってパスコードを要求する場合、再認証する必要があります。

- **最大オフライン期間：** このシナリオは、アプリごとのMDXポリシーによって駆動されるため、個々のアプリに固有です。Maximum offline period MDXポリシーのデフォルト設定は3日です。Secure Hubでのオンライン認証なしでアプリが実行できる期間が経過した場合、アプリの資格を確認し、ポリシーを更新するためにEndpoint Managementとのチェックインが必要です。このチェックインが発生すると、アプリはSecure Hubにオンライン認証をトリガーします。ユーザーはMDXアプリにアクセスする前に再認証する必要があります。

Note the relationship between the Maximum offline period and the Active poll period MDX policy:

- The Active poll period is the interval during which apps check in with Endpoint Management for performing security actions, such as app lock and app wipe. In addition, the app also checks for updated app policies.
- After a successful check for policies via the Active poll period policy, the Maximum offline period timer is reset and begins counting down again.

Endpoint Managementとの両方のチェックイン（アクティブポーリング期間および最大オフライン期間の期限切れ）には、デバイス上に有効なCitrix Gatewayトークンが必要です。デバイスに有効なCitrix Gatewayトークンがある場合、アプリはユーザーに中断を与えることなくEndpoint Managementから新しいポリシーを取得します。アプリがCitrix Gatewayトークンを必要とする場合、Secure Hubに切り替わり、ユーザーはSecure Hubで認証プロンプトを目にします。

Androidデバイスでは、Secure Hubのアクティビティ画面は現在のアプリ画面の真上に直接開きます。しかし、iOSデバイスでは、Secure Hubがフォアグラウンドに表示される必要があり、一時的に現在のアプリが置き換えられます。

ユーザーが資格情報を入力すると、Secure Hubは元のアプリに戻ります。この場合、キャッシュされたActive Directory資格情報を許可しているか、クライアント証明書が構成されている場合、ユーザーはPIN、パスワード、または指紋認証を入力できます。そうでない場合、ユーザーは完全なActive Directory資格情報を入力する必要があります。

Citrix ADCトークンは、Citrix Gatewayセッションの非アクティブ状態、または以下のCitrix Gatewayポリシーのリストで説明されているように、強制セッションタイムアウトポリシーにより無効になる場合があります。ユーザーがSecure Hubに再度サインオンすると、アプリの実行を継続できます。

- **Citrix Gatewayセッションポリシー：** 2つのCitrix Gatewayポリシーも、ユーザーが認証を求められるタイミングに影響します。これらの場合、ユーザーはEndpoint Managementに接続するためにCitrix ADCとのオンラインセッションを作成するために認証します。
 - **セッションタイムアウト：** 設定された期間ネットワークアクティビティがない場合、Endpoint Management用のCitrix ADCセッションは切断されます。デフォルトは30分で

す。ただし、Citrix Gatewayウィザードを使用してポリシーを構成する場合、デフォルトは1440分です。ユーザーは企業ネットワークに再接続するための認証プロンプトを目にします。

- **強制タイムアウト：** オンの場合、強制タイムアウト期間が経過すると、Endpoint Management用のCitrix ADCセッションは切断されます。強制タイムアウトにより、設定された期間後に再認証が必須になります。ユーザーは次回使用時に企業ネットワークに再接続するための認証プロンプトを目にします。デフォルトは**オフ**です。ただし、Citrix Gatewayウィザードを使用してポリシーを構成する場合、デフォルトは1440分です。

資格情報の種類

前のセクションでは、ユーザーが認証を求められるタイミングについて説明しました。このセクションでは、ユーザーが入力する必要がある資格情報の種類について説明します。デバイス上の暗号化されたデータにアクセスするには、さまざまな認証方法による認証が必要です。最初にデバイスのロックを解除するには、プライマリコンテナのロックを解除します。これが完了し、コンテナが再度保護された後、再度アクセスするには、セカンダリコンテナのロックを解除します。

注：

用語 **管理対象アプリ**とは、MDX Toolkitによってラップされたアプリを指し、App Passcode MDXポリシーがデフォルトで有効になっており、Inactivity Timerクライアントプロパティを使用しているアプリです。

資格情報の種類を決定する状況は次のとおりです。

- **プライマリコンテナのロック解除：** プライマリコンテナのロックを解除するには、Active Directoryパスワード、Citrix PINまたはパスコード、ワンタイムパスワード、Touch IDまたは指紋IDが必要です。
 - iOSでは、アプリがデバイスにインストールされた後、ユーザーがSecure Hubまたは管理対象アプリを初めて開くとき。
 - iOSでは、ユーザーがデバイスを再起動してからSecure Hubを開くとき。
 - Androidで、Secure Hubが実行されていないときにユーザーが管理対象アプリを開く場合。
 - Androidで、デバイスの再起動を含む何らかの理由でユーザーがSecure Hubを再起動する場合。

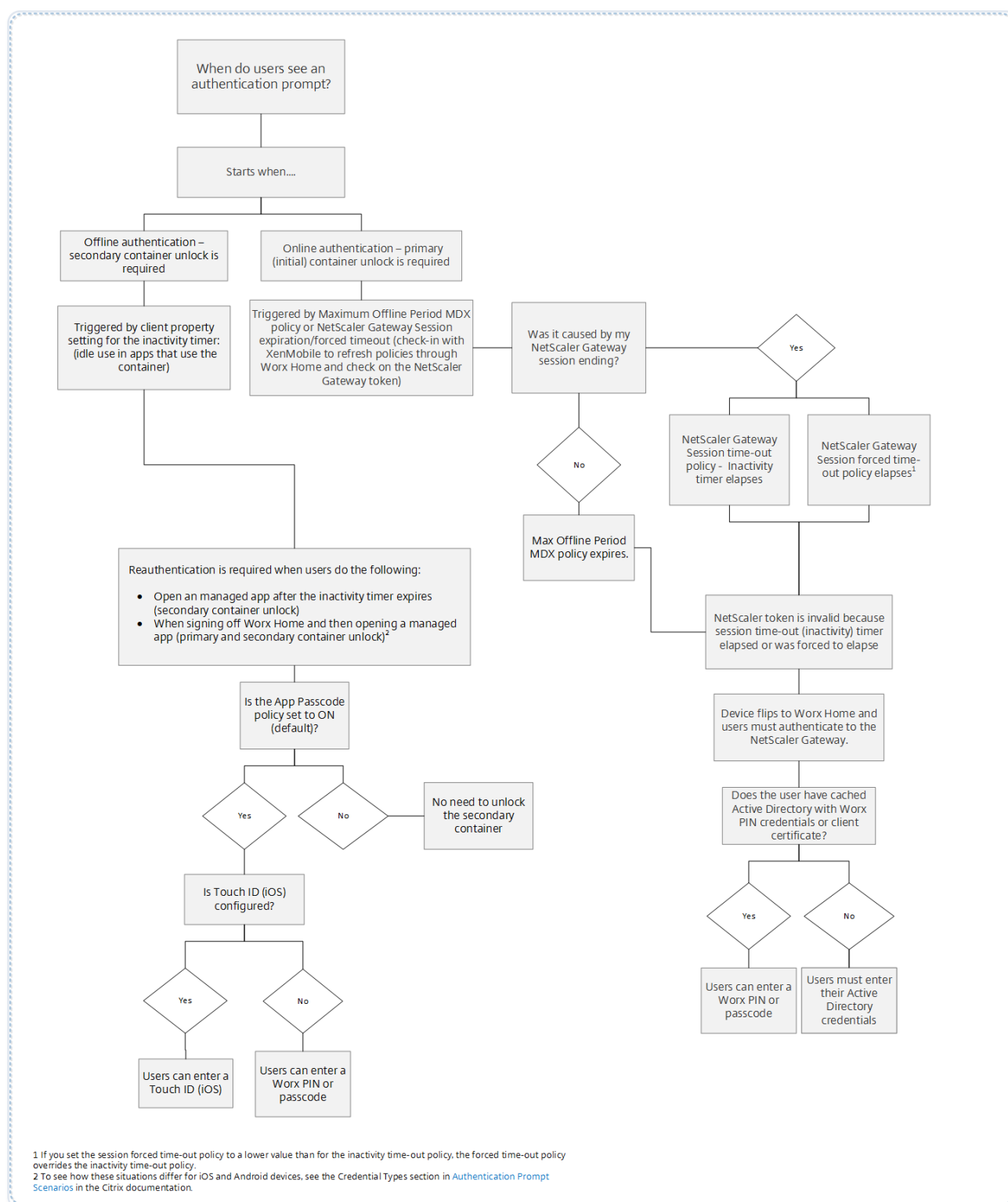
- **セカンダリコンテナのロック解除:** セカンダリコンテナのロックを解除するために、指紋認証（構成されている場合）、Citrix PINまたはパスコード、またはActive Directory資格情報を使用します。
 - 非アクティビティタイマーの期限が切れた後、ユーザーが管理対象アプリを開く場合。
 - ユーザーがSecure Hubからサインオフしてから管理対象アプリを開く場合。

以下の条件が満たされる場合、いずれかのコンテナロック解除状況でActive Directory資格情報が必要です。

- ユーザーが企業アカウントに関連付けられているパスコードを変更する場合。
- Endpoint ManagementコンソールでCitrix PINを有効にするクライアントプロパティ（ENABLE_PASSCODE_AUTHおよびENABLE_PASSWORD_CACHING）を設定していない場合。
- NetScaler® Gatewayセッションが終了する場合。これは、セッションタイムアウトまたは強制タイムアウトポリシータイマーの期限が切れた場合、デバイスが資格情報をキャッシュしない場合、またはクライアント証明書がない場合に発生します。

指紋認証が有効になっている場合、アプリの非アクティビティによりオフライン認証が必要なときに、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、およびデバイスを再起動するときには、引き続きPINを入力する必要があります。指紋認証の有効化については、「[指紋認証またはTouch ID認証](#)」を参照してください。

次のフローチャートは、認証を求められたときにユーザーが入力する必要がある資格情報を決定する意思決定フローをまとめたものです。



Secure Hubの画面切り替えについて

もう1つ注意すべき状況は、アプリからSecure Hubへ、そして再びアプリへと切り替えが必要な場合です。この切り替えでは、ユーザーが確認する必要がある通知が表示されます。この場合、認証は不要です。この状況は、Maximum offline periodおよびActive poll period MDXポリシーで指定されているように、Endpoint Managementとのチェックインが行われた後、Endpoint Management

がSecure Hubを介してデバイスにプッシュする必要がある更新されたポリシーを検出したときに発生します。

デバイスパスコードのパスコードの複雑さ（Android 12以降）

パスコードの複雑さは、カスタムパスワード要件よりも推奨されます。パスコードの複雑さレベルは、事前定義されたレベルの1つです。したがって、エンドユーザーはより低い複雑さレベルのパスワードを設定できません。

Android 12以降のデバイスのパスコードの複雑さは次のとおりです。

- **パスコードの複雑さを適用:** カスタムパスワード要件ではなく、プラットフォームによって定義された複雑さレベルのパスワードが必要です。Android 12以降のデバイスでSecure Hub 22.9以降を使用している場合にのみ適用されます。
- **複雑さレベル:** 事前定義されたパスワードの複雑さレベル。
 - **なし:** パスワードは不要です。
 - **低:** パスワードは次のいずれかです。
 - パターン
 - 4桁以上のPIN
 - **中:** パスワードは次のいずれかです。
 - 繰り返しシーケンス (4444) または順序付きシーケンス (1234) を含まないPINで、かつ4桁以上
 - 4文字以上の英字
 - 4文字以上の英数字
 - **高:** パスワードは次のいずれかです。
 - 繰り返しシーケンス (4444) または順序付きシーケンス (1234) を含まないPINで、かつ8桁以上
 - 6文字以上の英字
 - 最低6文字の英数字

注記:

- BYODデバイスの場合、最小の長さ、必須文字、生体認証、詳細ルールなどのパスコード設定はAndroid 12以降では適用されません。代わりにパスコードの複雑さを使用してください。
- ワークプロファイルのパスコードの複雑さが有効になっている場合、デバイス側のパスコードの複雑さも有効にする必要があります。

詳細については、Citrix Endpoint Managementのドキュメントにある[Android Enterprise設定](#)を参照してください。

派生資格情報を使用してデバイスを登録する

派生資格情報は、モバイルデバイスに強力な認証を提供します。スマートカードから派生した資格情報は、カードではなくモバイルデバイスに存在します。スマートカードは、個人識別検証 (PIV) カードまたは共通アクセスカード (CAC) のいずれかです。

派生資格情報は、UPNなどのユーザー識別子を含む登録証明書です。Endpoint Managementは、資格情報プロバイダーから取得した資格情報をデバイス上の安全なボールドに保存します。

Endpoint Managementは、iOSデバイスの登録に派生資格情報を使用できます。派生資格情報用に構成されている場合、Endpoint ManagementはiOSデバイスの登録招待またはその他の登録モードをサポートしません。ただし、同じEndpoint Managementサーバーを使用して、登録招待やその他の登録モードを通じてAndroidデバイスを登録できます。

派生資格情報を使用する場合のデバイス登録手順

登録には、ユーザーがスマートカードをデスクトップに接続されたリーダーに挿入する必要があります。

1. ユーザーはSecure Hubと、派生資格情報プロバイダーからのアプリをインストールします。この例では、IDプロバイダーアプリはIntercede MyID Identity Agentです。

IDプロバイダーアプリの画像(/en-us/mobile-productivity-apps/media/derived-credentials-secure-hub-myid.png)

2. ユーザーはSecure Hubを起動します。プロンプトが表示されたら、ユーザーはEndpoint Managementの完全修飾ドメイン名 (FQDN) を入力し、次へをクリックします。Secure Hubでの登録が開始されます。Endpoint Managementが派生資格情報をサポートしている場合、Secure HubはユーザーにCitrix PINの作成を促します。

資格情報プロンプトの画像(/en-us/mobile-productivity-apps/media/derived-credentials-secure-hub-enroll.png)

登録プロンプトの画像(/en-us/mobile-productivity-apps/media/derived-credentials-secure-hub-enroll-yes.png)

PINプロンプトの画像(/en-us/mobile-productivity-apps/media/derived-credentials-secure-hub-pin.png)

3. ユーザーは指示に従ってスマート資格情報をアクティブ化します。スプラッシュ画面が表示され、続いてQRコードをスキャンするよう促されます。

QRコードプロンプトの画像(/en-us/mobile-productivity-apps/media/derived-credentials-kiosk.png)

4. ユーザーはカードをデスクトップに接続されたスマートカードリーダーに挿入します。デスクトップアプリはQRコードを表示し、ユーザーにモバイルデバイスを使用してコードをスキャンするよう促します。

スキャンプロンプトの画像(/en-us/mobile-productivity-apps/media/derived-credentials-kiosk2.png)

ユーザーは、プロンプトが表示されたらSecure HubのPINを入力します。

PINプロンプトの画像(/en-us/mobile-productivity-apps/media/derived-credentials-secure-hub-pin.png)

PINの認証後、Secure Hubは証明書をダウンロードします。その後、ユーザーはプロンプトに従って登録を完了します。

Endpoint Managementコンソールでデバイス情報を表示するには、次のいずれかを実行します。

- **管理 > デバイス** に移動し、デバイスを選択してコマンドボックスを表示します。**詳細を表示** をクリックします。
- **分析 > ダッシュボード** に移動します。

Citrix Endpoint Management™ コンソールを介してヒントを構成する

管理者は、登録モードが**Two Factor**に設定されているデバイス向けに、Secure Hubサインインページでヒントを構成できます。ヒントは次のいずれかの方法で構成できます。

- ヒントをテキストとして構成する
- Webページリンク付きでヒントテキストを構成する

ヒントをテキストとして構成する

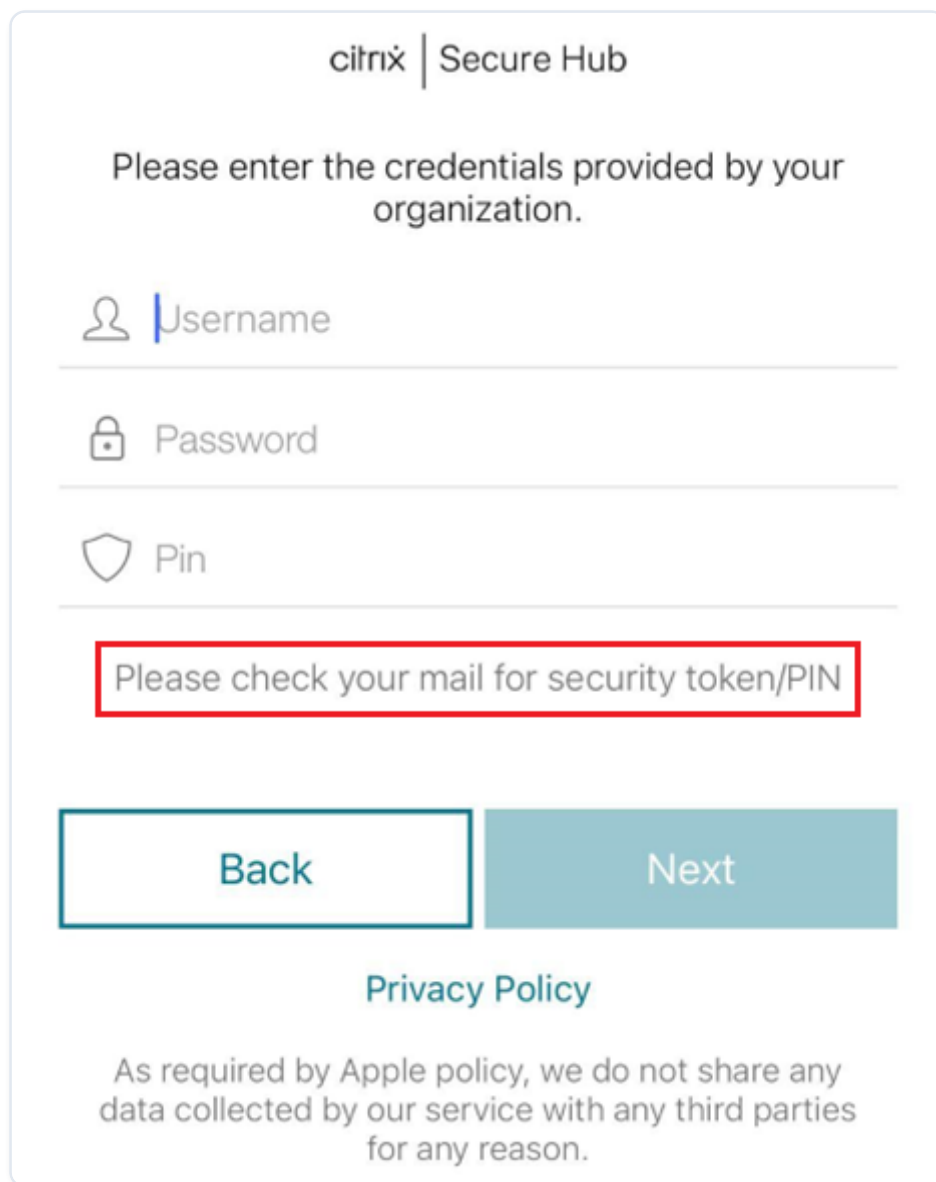
ヒントテキストを構成するには、次の手順を実行します。

1. 管理者資格情報を使用してCitrix Endpoint Managementコンソールにサインインします。
2. **Settings > Client Properties**に移動し、**Add New Client Property**をクリックします。
3. **Key**ドロップダウンリストから、**Custom Key**を選択します。
4. **Key**フィールドに、**enrollment.twofactor.token.hint**と入力します。
5. **Value**フィールドに、サインインページにヒントとして表示されるテキストを入力できます。このヒントは、ユーザーが2要素認証用のPINを見つけるのに役立ちます。
6. **Name**フィールドに、**enrollment.twofactor.token.hint**と入力します。
7. **Description**フィールドに、構成したヒントに関する備考を入力できます。これは今後の参照に役立ちます。

ヒントをテキストとして構成するイメージ(/en-us/mobile-productivity-apps/media/sh-config-hint-text-1.png)

8. **Save**をクリックします。

構成が完了すると、サインインページにヒントテキストが表示されます。



The image shows the Citrix Secure Hub login interface. At the top, the Citrix logo and 'Secure Hub' text are displayed. Below this, a message asks the user to enter credentials provided by their organization. There are three input fields: 'Username' (with a person icon), 'Password' (with a lock icon), and 'Pin' (with a shield icon). A red rectangular box highlights the text 'Please check your mail for security token/PIN'. Below the input fields are two buttons: 'Back' (white with a blue border) and 'Next' (solid blue). At the bottom, there is a link for 'Privacy Policy' and a disclaimer stating that data collected by the service is not shared with third parties as required by Apple policy.

citrix | Secure Hub

Please enter the credentials provided by your organization.

Username

Password

Pin

Please check your mail for security token/PIN

Back Next

[Privacy Policy](#)

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

Webページリンクでヒントテキストを構成する

PINへのアクセスに関する詳細情報を含むWebページを構成できます。その後、ヒントテキストにハイパーリンクとしてWebページリンクを提供します。ユーザーがサインインページのヒントをクリックすると、Secure Hubは埋め込みブラウザを開き、すでに構成したWebページに移動します。

Webページリンクでヒントテキストを構成するには、まず、([/ja-jp/citrix-secure-hub/configure-hint-cem.html#configure-hint-as-text](#))の記事で説明されているようにヒントテキストを構成する必要があります。完了したら、次の手順に進みます。

1. 管理者資格情報を使用してCitrix Endpoint Managementコンソールにサインインします。
2. **設定 > クライアントプロパティ** の順に移動し、**新しいクライアントプロパティの追加** をクリックします。

3. **【キー】** ドロップダウンリストから、**【カスタムキー】** を選択します。
4. **【キー】** フィールドに、「**enrollment.twofactor.token.hint.url**」と入力します。
5. **【値】** フィールドに、構成したWebページのURLを入力します。
6. **【名前】** フィールドに、「**enrollment.twofactor.token.hint.url**」と入力します。
7. **【説明】** フィールドには、構成したヒントに関する備考を入力できます。これは、今後の参照に役立ちます。

注：

ユーザーがヒントリンクをクリックすると、埋め込みブラウザにWebページが表示されます。

Settings > Client Properties > Add New Client Property

Add New Client Property

Key	Custom Key	?
Key *	enrollment.twofactor.token.hint.url	
Value *	https://www.citrix.com/contact/	
Name *	enrollment.twofactor.token.hint.url	
Description *	https://www.citrix.com/contact/	

8. **「保存」** をクリックします。

設定が完了すると、ウェブページリンク付きのヒントテキストがサインインページに表示されます。

ヒントリンクのサインインページの画像(/en-us/mobile-productivity-apps/media/sh-config-hint-link-2.png)

Androidデバイスでのコンプライアンスチェック (テクニカルプレビュー)

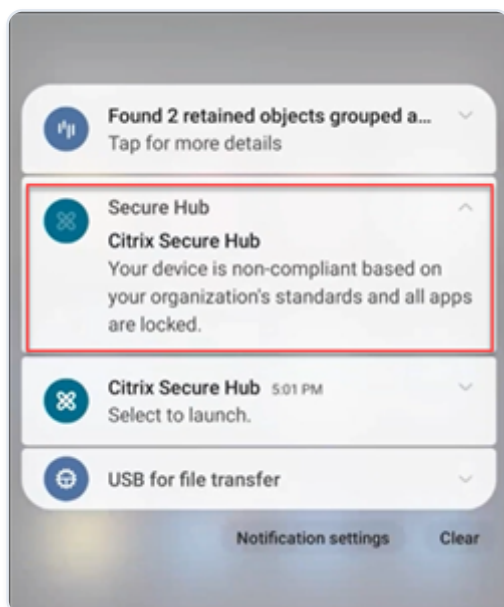
注:

この機能は、デバイス所有者モードで登録されたAndroidデバイスに適用されます。

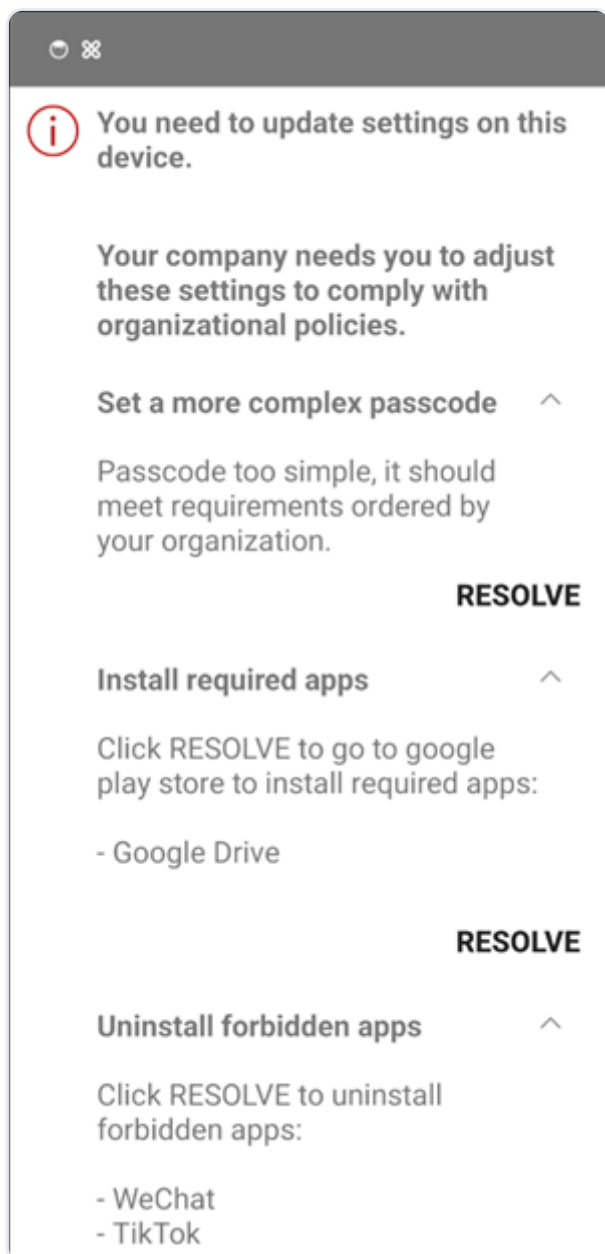
Secure Hub for Android 24.8.0のリリース以降、Secure Hubは、Citrix Endpoint Managementを通じて管理者が構成したポリシーに対してAndroidデバイスのコンプライアンスを検証します。これらのコンプライアンスチェックには以下が含まれます。

- デバイスのパスワード強度を確保する
- 必須アプリのインストールを確認する
- 禁止されているアプリの削除を確認する

デバイスが非準拠の場合、ユーザーデバイスに次の通知が表示されます。



デバイスが非準拠の場合、ユーザーがSecure Hubを開くと次のメッセージが表示されます。



ユーザーは解決ボタンをクリックして、それぞれの問題に対処できます。

注:

- コンプライアンスが満たされるまで、アプリはロックされたままになります。
- 特定のアプリを「アプリのロック解除」リストに追加することで、ロックを解除するオプションがあります。詳細については、「[Androidデバイスのコンプライアンス適用 \(テクニカルレビュー\)](#)」を参照してください。

ポリシーとコンプライアンスチェックの設定の詳細については、Citrix Endpoint Management製品ドキュメントの[Compliance Enforcement for Android Devices \(Technical Preview\)](#)を参照してください。