iOS 向け Citrix Workspace アプリ

Contents

iOS 向け Citrix Workspace アプリの新機能

May 20, 2019

1905 の新機能

ワークスペースハブの機能強化

Citrix Workspace アプリに、iOS デバイス上の信頼できるデバイス一覧に対してワークスペースハブを追加または削除する新しい手順が統合されました。詳しくは、「Security Connection」を参照してください。

ホストからクライアントへのリダイレクト

コンテンツのリダイレクト機能では、ユーザーが特定の種類のコンテンツにアクセスするときに、公開アプリケーションを使うのか、ユーザーデバイス上のアプリケーションを使うのかを制御できます。

ホストからクライアントへのリダイレクトは、コンテンツリダイレクト機能の一種です。この機能は、サーバー OS の VDA でのみサポートされ、デスクトップ OS の VDA ではサポートされません。

ホストからクライアントへのリダイレクト機能を有効にすると、URL はサーバー VDA でインターセプトされてからユーザーデバイスに送信されます。これらの URL は、ユーザーデバイス上の Web ブラウザーまたはマルチメディアプレーヤーで開かれます。
ホストからクライアントへのリダイレクト機能を有効にしても、ユーザーデバイスから URL に接続できない場合は、その URL がサーバー VDA に戻されます。
ホストからクライアントへのリダイレクト機能が無効な場合、URL はサーバー VDA 上の Web ブラウザーまたはマルチメディアプレーヤーで開きます。
ホストからクライアントへのリダイレクト機能が有効な場合、ユーザーがこの機能を無効にすることはできません。

ホストからクライアントへのリダイレクト機能は、サーバーからクライアントへのリダイレクト機能の新名称です。

詳しくは、「一般コンテンツリダイレクト」を参照してください。

1904.5 の新機能

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

1904.2 の新機能

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

1904 の新機能

- 最近使用した SaaS および Web アプリの一覧を［最近使用］に表示できるようになりました。
- セキュリティ上の理由から、Citrix Ready ワークスペースハブでは、モバイルデバイスとハブ間の SSL（Secure Sockets Layer）接続がサポートされます。各デバイスを一意に特定するため、完全修飾ドメイン名（FQDN）を設定する必要があります。詳しくは、Citrix Ready ワークスペースハブのドキュメントの「セキュリティ接続」を参照してください。

1903 の新機能

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

1902 の新機能

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

1901 の新機能

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

1812 の新機能

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

1811 の新機能

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

1810.2 の新機能

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

> 注:
>
> Citrix Ready ワークスペースハブの内部ビーコンの構成について詳しくは、Knowledge Center のCTX218708を参照してください。

1810.1 の新機能

Citrix Ready ワークスペースハブのサポート

Citrix Ready ワークスペースハブは、デジタル環境と物理環境を組み合わせて、セキュアなスマートスペース内にアプリやデータを配信します。このシステム全体が、モバイルアプリやセンサーなどのデバイス（またはモノ）を接続して、インテリジェントで応答性の高い環境を作ります。

Citrix Ready ワークスペースハブは Raspberry Pi 3 プラットフォーム上に構築されます。Citrix Workspace アプリを実行しているデバイスは Citrix Ready ワークスペースハブに接続し、デスクトップまたはアプリをより大きなディスプレイにキャストします。

iOS 向け Citrix Workspace アプリの Citrix Ready ワークスペースハブについて詳しくは、「Citrix Ready ワークスペースハブの構成」を参照してください。

Citrix Ready ワークスペースハブについて詳しくは、Citrix Ready ワークスペースハブのドキュメントを参照してください。

1810 の新機能

Purebred による派生資格情報のサポート

このリリースでは、iOS 向け Citrix Workspace アプリで Purebred による派生資格情報がサポートされるようになりました。派生資格情報を使用できるストアに接続するときに、ユーザーは仮想スマートカードを使用して iOS 向け Citrix Workspace アプリにログオンできます。この機能は、オンプレミス展開のみでサポートされます。

> 注:
>
> この機能を使用するには、Citrix Virtual Apps and Desktops 7 1808 以降が必要です。

派生資格情報の構成について詳しくは、「派生資格情報の構成」を参照してください。

1809 の新機能

iOS 12 のサポート

iOS 用 Citrix Workspace アプリは、iOS 12 を完全にサポートします。

1808 の新機能

エンドユーザーヘルプの更新

iOS 向けの Citrix Workspace アプリでの変更事項をすべて反映するように、アプリに組み込まれたエンドユーザー向けヘルプが新しく書き直されています。

解決された問題

May 20, 2019

1905 で解決された問題

このリリースは、さまざまな問題にも対応しているため、パフォーマンスや安定性が総合的に向上しています。

1904.5 で解決された問題

- Citrix Workspace アプリに初めてログオンすると、ログインに失敗して次のエラーメッセージが表示されることがあります:

  「サーバーに接続できません。再試行してください。」

  [RFIOS-3588]

- 現在の緯度および経度レポートの詳細を取得できません。[RFIOS-3668]
- ［アカウント設定］ からクライアント証明書を削除すると、Workspace アプリが予期せず終了することがあります。[RFIOS-4212]

1904.2 で解決された問題

- カスタムツールバーの「矢印」アイコンをタップすると、カスタム方向キーが見えなくなります。[RFIOS-4233]

1904 で解決された問題

- PNAgent アカウントをシームレスに追加できるようになりました。[RFIOS-3342]
- 特定の接続関連のエラーメッセージに WiFi SSID が表示されるようになりました。WiFi SSID により、接続しようとしている Citrix Ready ワークスペースハブと同じネットワークを使用していることが確認できます。[WH-1903]
- Active Directory（AD）パスワードの有効期限が切れている場合、Citrix Workspace アプリから AD パスワードをリセットできません。[RFIOS-3241]
- 日本語の VDA 上で実行されているセッションで、option（または alt）+ Return キーを押すと、IME モードを保持したまま Microsoft Excel でセルに新しい行を入力できます。[RFIOS-4046]
- デバイスと VDA を再接続すると、デバイスがスリープモードから回復した後、10 ～ 20 秒間ディスプレイが応答しなくなります。[RFIOS-4146]

- Google の 2 要素認証を使用する場合、iOS デバイスから Citrix Workspace アプリへのログオンが失敗し、次のエラーメッセージが表示されます:

  ユーザ名、パスワード、またはパスコードが正しくありません

  [RFIOS-4064]

1903 で解決された問題

- iPhone X で Citrix Workspace アプリバージョン 1810 を使用しているときに、クライアントデバイスの画面が横向きになるとキーボードシンボルが表示されなくなります。[LD0619]
- 英語以外のシステムで Citrix Workspace アプリバージョン 1812 を使用すると、［新しいアカウントの追加］フィールドのラベルが英語で表示されます。[LD1066]
- クライアントデバイスが長時間アイドル状態になると、Citrix X1 マウスが反応しなくなります。[LD0842]
- バージョン 1903 以降で、Citrix Workspace アプリのスプラッシュスクリーンダイアログが表示されません。[RFIOS-3509]

1902 で解決された問題

- Enlightened Data Transport（EDT）プロトコルを使用すると、デバイスがスリープモードから回復した後、10 ～ 20 秒間ディスプレイが応答しなくなります。[LD0854]
- 認証のためにユーザー名とパスワードを入力するときに、パスワードフィールドを使用中キーボードレイアウトが別の言語に切り替わります。[LD0588]

1901 で解決された問題

- 外付けの Apple Bluetooth キーボードが接続されているときに、Shift+0 を押して右かっこ記号（)）を入力すると、セッションが切断されます。[RFIOS-3658]

1812 で解決された問題

- 画面の解像度が［自動調整 - 低］に設定され、理論値が 1024 x 1366 の場合、画面上の文字間隔が正しく表示されません。[LC9808]
- Citrix Gateway が Web Interface に接続するときにストアが正しく列挙されず、ストアアカウントの追加時に問題が発生することがあります。[RFIOS-3342]
- ［よく使うアプリケーション］ 一覧から必須アプリを削除しようとすると、Citrix Workspace アプリでアラートメッセージが表示されません。[RFIOS-1556]

- 仮想キーボードが表示されるときに、マウス座標（X1）のオフセットにより誤った選択範囲が表示される場合があります。[RFIOS-3418]
- PNAgent アカウントにサインインするときに、ドメイン資格情報の入力を求める画面が表示されません。この問題は、最初にドメイン資格情報を入力しなかった場合に発生します。[RFIOS-2944]
- iOS 向け Citrix Workspace アプリ 1809 にアップグレードした後に公開アプリを起動すると、「信頼されていない証明書」エラーメッセージが表示されます。[RFIOS-3368]

1811 で解決された問題

- デジタル署名が正しくキャプチャされない場合があります。この問題を解決するには、*HandleDoubleTapLocally=no* パラメーターを default.ica ファイルに追加して、この動作を無効にします。

  StoreFront または Web Interface サーバーの default.ica ファイルの変更については、Knowledge Center のCTX116357を参照してください。[LD0629]

1810.2 で解決された問題

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

1810.1 で解決された問題

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

1810 で解決された問題

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

1809 で解決された問題

- Citrix Receiver から Citrix Workspace アプリにアップグレードすると、ユーザーがストアへログオンできない場合があります。[RFIOS-3233]

1808 で解決された問題

このリリースは、さまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

既知の問題

May 20, 2019

1905 での既知の問題

このリリースで確認されている新しい問題はありません。

1904.5 での既知の問題

このリリースで確認されている新しい問題はありません。

1904.2 での既知の問題

このリリースで確認されている新しい問題はありません。

1904 での既知の問題

このリリースで確認されている新しい問題はありません。

1903 での既知の問題

- Safari Web ブラウザーを使用して StoreFront にサインオンすると、仮想デスクトップやアプリケーションが開かないことがあります。[RFIOS-4178]

1902 での既知の問題

このリリースで確認されている新しい問題はありません。

1901 での既知の問題

このリリースで確認されている新しい問題はありません。

1812 での既知の問題

このリリースで確認されている新しい問題はありません。

1811 での既知の問題

- 12.9 インチ iPad Pro で ［自動調整 **-** 高］ 設定を使用すると、指タップが正しく認識されないことがあります。回避策としては、Citrix Workspace アプリの［表示オプション］で別の設定に変更してください。[RFIOS-1766]

1810.2 での既知の問題

- 12.9 インチ iPad Pro で ［自動調整 **-** 高］ 設定を使用すると、指タップが正しく認識されないことがあります。回避策としては、Citrix Workspace アプリの［表示オプション］で別の設定に変更してください。[RFIOS-1766]
- ネットワークを切り替えると、セッションが再接続または再起動しないことがあります。回避策としては、Citrix Workspace アプリを終了して再起動してください。[RFIOS-3246]
- エラー「HdxSdkErrorDomain_Session error 8」が表示され、セッションが起動しないことがあります。回避策としては、Citrix Workspace アプリを終了して再起動してください。[RFIOS-3374]

1810.1 での既知の問題

このリリースで確認されている新しい問題はありません。

1810 での既知の問題

このリリースで確認されている新しい問題はありません。

1809 での既知の問題

このリリースで確認されている新しい問題はありません。

1808 での既知の問題

- iPhone でスマートカードを使用している場合、ログオフ後にアプリを起動すると、読み込み中の状態のまま進まなくなります。回避策としては、アプリを再起動してください。[RFIOS-2550]
- スマートカードを使用している場合、iOS 向け Citrix Workspace アプリへのアップグレード後にセッションから正しくサインアウトできないことがあります。回避策としては、アプリを再起動してください。[RFIOS-3076]

システム要件

May 20, 2019

デバイスの要件

- iOS 向け Citrix Workspace アプリバージョン 1808 は、iOS 10、11 および 12 をサポートします。
- このソフトウェアアップデートは、以下のデバイスで検証済みです:
  - iPhone 5x モデル、iPhone 6x モデル、iPhone 7x モデル、iPhone 8x モデル、iPhone X のみ。
  - iPad Pro を含めたすべての iPad モデル（iPad 1 と iPad 2 はサポートされていません）
- 外部ディスプレイのサポートは次のとおりです。
  - iPhone - iOS でサポートされるデバイス。
  - iPad - iOS でサポートされるデバイス（ディスプレイ全体には表示されません）。

サーバーの要件

各サーバーに最新の Hotfix がインストールされていることを確認してください。

- iOS 向け Citrix Workspace アプリで仮想デスクトップやアプリに接続する場合、Citrix StoreFront、および Web Interface がサポートされます。

  StoreFront:

  - StoreFront 3.6 以降（推奨）。iOS 向け Citrix Workspace アプリは StoreFront の最新バージョンで検証済みです。サポートされる前バージョンは、StoreFront 2.6 以降です。

    StoreFront ストアへの直接アクセスを提供します。iOS 向け Citrix Workspace アプリでは、前バージョンの StoreFront もサポートされます。

    > 注:
    >
    > XenApp および XenDesktop 7.8 で、Framehawk 仮想チャネルおよび 3D Pro がサポートされるようになりました。この機能は、iOS 向け Citrix Workspace アプリに拡張されました。

  - Workspace for Web サイトが構成された StoreFront

    StoreFront ストアへの Safari Web ブラウザーからのアクセスを提供します。ユーザーはブラウザーを使って手動で ICA ファイルを開く必要があります。この展開方法での制限事項については、StoreFrontのドキュメントを参照してください。

  Web Interface:

  - Web Interface 5.4 と Web Interface サイト。
  - Web Interface 5.4 と XenApp Services サイト。

  - Citrix Gateway 上の Web Interface（Safari のみを使うブラウザーベースのアクセス）

    Citrix Gateway で提供されるリライトポリシーを有効にする必要があります。

- **Citrix Virtual Apps and Desktops**、**XenApp** および **XenDesktop** の以下のバージョン：
  - Citrix Virtual Apps and Desktops 7 1808 以降
  - Citrix XenDesktop 7.x 以降
  - Citrix XenApp 7.5 以降
  - Citrix XenApp 6.5 for Windows Server 2008 R2

接続性と認証

StoreFront への接続では、iOS 向け Citrix Workspace アプリで以下の認証方法がサポートされます：

	Web 向け Workspace（ブラウザー環境）	StoreFront サービスサイト（ネイティブ）	StoreFront XenApp Services サイト（ネイティブ）	Citrix Gateway から Workspace for Web（ブラウザー）	Citrix Gateway から StoreFront サービスサイト（ネイティブ）
匿名	はい	はい			
ドメイン	はい	はい	はい	はい *	はい *
ドメインパススルー	はい	はい	はい		
セキュリティトークン				はい *	はい *
2 要素認証（ドメイン + セキュリティトークン）				はい *	はい *
SMS				はい *	いいえ
スマートカード		はい		はい *	はい *
ユーザー証明書				はい（Citrix Gateway Plug-in）	はい（Citrix Gateway Plug-in）

*Workspace for Web サイトおよび Citrix Gateway を含む展開に対してのみ使用できます（デバイスへの関連プラグインのインストールは不問）。

Web Interface 5.4 への接続では、iOS 向け Citrix Workspace アプリで以下の認証方法がサポートされます:

> 注:
>
> Web Interface では、「指定ユーザー」による認証がドメインおよびセキュリティトークン認証に相当します。

	Web Interface（ブラウザー）	Web Interface XenApp Services サイト	Citrix Gateway から Web Interface（ブラウザー）	Citrix Gateway から Web Interface XenApp Services サイト
匿名	はい			
ドメイン	はい	はい	はい *	
ドメインパススルー	はい			
セキュリティトークン			はい *	
2 要素認証（ドメイン + セキュリティトークン）			はい *	
SMS			はい *	
スマートカード				
ユーザー証明書			はい（Citrix Gateway Plug-in が必要）	

セキュリティで保護された接続と証明書について

プライベート（自己署名）証明書

リモートゲートウェイにプライベート証明書がインストールされている場合は、組織の証明機関のルート証明書をデバイスにインストールしないと、iOS 向け Citrix Workspace アプリを使用してシトリックスのリソースにアクセスできません。

> 注:
>
> 接続時にリモートゲートウェイの証明書を検証できない場合（ローカルのキーストアにルート証明書が含まれていないため）、信頼されていない証明書の警告が表示されます。ユーザーが警告に対してそのまま続行することを選択した場合、アプリケーションの一覧が表示されますが、アプリケーションの起動に失敗します。

手動でインストールした証明書を信頼する

iOS 10.3 以降では、手動でインストールしたプロファイルに含まれる証明書は、SSL 通信に対して自動的には信頼されません。iOS で手動でインストールした証明書プロファイルを信頼するには:

1. 証明書プロファイルがデバイス上にインストールされていることを確認します。
2. ［設定］>［一般］>［情報］>［証明書信頼設定］ の順に選択します。

   プロファイルを介してインストールされた各ルート証明書は、［ルート証明書を全面的に信頼する］ の下に表示されます。
3. 各ルート証明書に対して、信頼設定を切り替えることができます。

iPad および **iPhone** へのルート証明書のインポート

証明書の発行者のルート証明書を取得して、デバイスに構成されているメールアカウントにメールで送信します。添付ファイルをクリックすると、ルート証明書をインポートするかどうかを確認するメッセージが表示されます。

ワイルドカード証明書

ワイルドカード証明書は、同一ドメイン内の任意のサーバーで個別のサーバー証明書の代わりに使用します。iOS 向け Citrix Workspace アプリでは、ワイルドカード証明書がサポートされています。

中間証明書と **Citrix Gateway**

証明書チェーンに中間証明書が含まれる場合は、中間証明書を Citrix Gateway（または Access Gateway）のサーバー証明書に追加する必要があります。Access Gateway でのインストールについては、使用する Access Gateway のエディションに関する Knowledge Base アーティクルを参照してください:

CTX114146: How to Install an Intermediate Certificate on Access Gateway Enterprise Edition

RSA SecurID 認証は、Secure Gateway 構成 (Web Interface を使用する環境のみ) と、すべての Access Gateway 構成でサポートされています。

iOS 向け Citrix Workspace アプリでは、Access Gateway でサポートされるすべての認証方法がサポートされています。

スマートカード

iOS 向け Citrix Workspace アプリは、SITHS スマートカードのセッション中の接続のみをサポートしています。

FIPS Citrix Gateway デバイスを使用している場合は、SSL の再ネゴシエーションを拒否するようにシステムを構成します。詳しくは、「How to configure the -denySSLReneg parameter」を参照してください。

サポートされる製品および構成は以下のとおりです:

- サポートされるスマートカードリーダー:
  - Precise Biometrics Tactivo for iPad Mini ファームウェアバージョン 3.8.0
  - Precise Biometrics Tactivo for iPad（第 4 世代）、Tactivo for iPad（第 3 世代）および iPad 2 ファームウェアバージョン 3.8.0
  - BaiMobile®301MP および 301MP-L スマートカードリーダー
    （VDA スマートカードミドルウェア対応）
  - ActivIdentity
- サポートされるスマートカード:
  - PIV カード
  - Common Access Card（CAC）
- サポートされる構成:
  - StoreFront 2.x および XenDesktop 7.x 以降、または XenApp 6.5 以降と統合された Citrix Gateway でのスマートカード認証

展開

May 20, 2019

iOS デバイスユーザーへのアクセス情報の提供

管理者は、ユーザーに iOS 向け Citrix Workspace アプリアカウントの情報を提供します。ユーザーは、この情報を使用してアプリケーション、デスクトップ、およびデータにアクセスします。次の方法でユーザーに情報を提供できます:

- メールアドレスによるアカウント検出を構成する
- ユーザーにプロビジョニングファイルを提供する
- アカウント情報をユーザーに手入力させる

メールアドレスによるアカウント検出を構成する

管理者は、メールアドレスによる iOS 向け Citrix Workspace アプリアカウントの検出機能を構成できます。この機能を有効にした場合、ユーザーは iOS 向け Citrix Workspace アプリの初期設定時にサーバーの URL の代わりに自分のメールアドレスを入力できます。DNS（Domain Name System）サービス（SRV）レコードにより、そのメールアドレスに関連付けられている Access Gateway、StoreFront サーバー、または AppController 仮想アプライアンスが自動的に検出され、ホストされているアプリケーション、デスクトップ、およびデータにアクセスするためのログオンを求めるメッセージが表示されます。

> 注:
>
> iOS 向け Citrix Workspace アプリで Web Interface に接続する環境では、メールアドレスによるアカウント検出がサポートされません。

ユーザーにプロビジョニングファイルを提供する

管理者は、StoreFront を使用して、接続の詳細情報を定義したプロビジョニングファイルを作成できます。作成したプロビジョニングファイルをユーザーに提供して、iOS 向け Citrix Workspace アプリを自動的に構成できるようにします。デバイスに iOS 向け Citrix Workspace アプリをインストールした後で、提供された CR ファイルをユーザーが開くと iOS 向け Citrix Workspace アプリが自動的に構成されます。Workspace for Web サイトを構成する場合は、そのサイトからユーザーに iOS 向け Citrix Workspace アプリのプロビジョニングファイルを提供することもできます。

詳しくは、StoreFrontのドキュメントを参照してください。

アカウント情報をユーザーに手入力させる

ユーザーにアカウント情報を入力させる場合は、以下の情報を提供する必要があります:

- StoreFront URL または XenApp Services サイトがホストするリソース。例: `servername.company.com`
- Citrix Gateway を使用する場合は、そのアドレスと認証方法。

ユーザーが新しいアカウントの詳細を入力すると、iOS 向け Citrix Workspace アプリにより接続が検証されます。検証に成功すると、そのアカウントにログオンするための画面が開きます。

セッション共有

iOS 向け Citrix Workspace アプリアカウントをログオフするときに、実行中のアプリケーションやデスクトップが検出されると、セッションを切断するかログオフするかを選択する画面が開きます:

- 切断: アカウントからログオフされますが、Windows アプリケーションやデスクトップはサーバー上で実行されたままになります。ほかのデバイス上の iOS 向け Citrix Workspace アプリからこのセッションに再接続すると、切断時の状態から作業を続行できます。このオプションにより、ユーザーがほかのデバイスに移動して、作業を続行できるようになります。
- ログオフ: 実行中の Windows アプリケーションが終了し、Citrix Virtual Apps and Desktops サーバーからログオフされます。このオプションにより Citrix Workspace セッションが終了します。次に iOS 向け Citrix Workspace アプリを起動すると、デフォルトの画面が開きます。

RSA SecurID 認証の **iOS** デバイス用の設定

iOS 向け Citrix Workspace アプリに対する RSA SecurID 認証は、Secure Web Gateway 構成（Web Interface を使用する環境のみ）と、すべての Citrix Gateway 構成でサポートされています。

ソフトウェアトークン用の **URL** スキーム：iOS 向け Citrix Workspace アプリで使用される RSA SecurID ソフトウェアトークンにより、URL スキーム「com.citrix.securid」のみが登録されます。

iOS デバイスに iOS 向け Citrix Workspace アプリと RSA SecurID アプリの両方をインストールしたユーザーは、URL スキーム「com.citrix.securid」を選択して iOS 向け Citrix Workspace アプリに RSA SecurID Software Authenticator（ソフトウェアトークン）をインポートする必要があります。

RSA ソフトトークンを **iOS** 向け **Citrix Workspace** アプリにインポートするには

RSA ソフトトークンを iOS 向け Citrix Workspace アプリで使用するため、ユーザーはこの手順に従う必要があります。

PIN 長のポリシー、PIN の種類（数字のみ、英数字）、および PIN 再使用の制限は、RSA 認証サーバーで指定されます。

RSA サーバーへの認証に成功した後は、これを一度指定するだけで済みます。ユーザーが PIN を確認した後に StoreFront サーバーでも認証が実行されて、使用可能な公開アプリケーションやデスクトップが表示されます。

iOS 向け **Citrix Workspace** アプリで **RSA** ソフトトークンを使用するには

1. 組織から提供された RSA ソフトトークンをインポートします。
2. SecurID ファイルが添付されたメールで、インポート先として［**Open in Workspace**］を選択します。ソフトトークンがインポートされたら、iOS 向け Citrix Workspace アプリが自動的に開きます。
3. インポートを完了させるために組織によりパスワードが提供されている場合は、そのパスワードを入力して［**OK**］をクリックします。［**OK**］をクリックした後、トークンが正常にインポートされたことを示すメッセージが表示されます。
4. インポートメッセージを閉じ、iOS 向け Citrix Workspace アプリで ［アカウントの追加］ をクリックします。
5. 組織から提供されたストアの URL を入力し、［次へ］ をクリックします。
6. ［ログオン］画面で、資格情報を入力します：ユーザー名、パスワード、ドメイン。組織によって別のデフォルト PIN が指定されていない場合は、［PIN］に「**0000**」と入力します（PIN 0000 は RSA のデフォルトですが、セキュリティポリシーに準拠させるため組織によって変更されていることがあります）。
7. 左上の［ログオン］をクリックします。［ログオン］をクリックした後に、新しい PIN の作成を求められます。
8. 新しい PIN を 4 ～ 8 文字で入力し ［**OK**］ をクリックします。

9. 新しい PIN の確認入力を求められます。PIN をもう一度入力して［**OK**］をクリックします。［OK］をクリックした後、アプリやデスクトップにアクセスできるようになります。

Next Token Mode のサポート

Citrix Gateway の RSA SecurID 認証を設定すると、iOS 向け Citrix Workspace アプリで次のトークンモードがサポートされます。このモードを有効にすると、ユーザーが不正なパスワードを 3 回（デフォルト設定）入力したときに、Citrix Gateway Plug-in によりメッセージが表示され、次のトークンが表示されるまで待機すればログオンできるようになります。ユーザーが不正なパスワードで何度もログオンしようとした場合に、そのユーザーのアカウントが無効になるように RSA サーバーを設定できます。

パスワードの保存

Citrix Web Interface 管理コンソールでは、認証時にユーザーがパスワードを保存することを許可できます。管理者がユーザーのアカウントを設定すると、パスワードが暗号化され、そのユーザーの初回接続時まで保存されます。以下に注意してください。

- ユーザーによるパスワードの保存を許可すると、パスワードがデバイス上に格納され、アプリケーションへの接続時にパスワードの再入力が不要になります。

> 注:
>
> パスワードが保存されるのは、ユーザーがアカウントを作成する時にパスワードを入力した場合のみです。アカウントのパスワードが入力されていない場合は、サーバー側の設定にかかわらずパスワードは保存されません。

- 管理者がパスワードの保存を無効（デフォルト設定）にすると、接続時に常にパスワードの入力が必要になります。

> 注:
>
> StoreFront 直接接続では、パスワードを保存することはできません。

パスワード保存設定を上書きするには

サーバー側でパスワードの保存を有効にしても、ユーザーは以下の方法でパスワードの入力が毎回要求されるように設定できます:

- アカウント作成時に、パスワードフィールドを空白のままにする。
- アカウント編集時に、パスワードを削除して設定を保存する。

パスワードの保存機能の使用

iOS 向け Citrix Workspace アプリでパスワードを保存することができるため、接続プロセスが効率的に処理されます。これにより、iOS 向け Citrix Workspace アプリを開くたびにセッションを認証する追加手順が省かれます。

> 注:
>
> パスワードの保存機能は現在、PNA プロトコルと連携して機能します。StoreFront ネイティブモードでは機能しません。ただし、StoreFront で PNA レガシモードを有効にするとこの機能が有効になります。

StoreFront PNA レガシモードの構成

StoreFront PNA レガシモードを構成してパスワードの保存機能を有効にするには:

1. 既存のストアを構成している場合は、手順 3 に移動します。
2. 新しい StoreFront 展開を構成するには、Citrix StoreFront の「インストール、セットアップ、およびアンインストール」で説明されているベストプラクティスの説明に従ってください。
3. Citrix StoreFront 管理コンソールを開きます。ベース URL が HTTPS を使用し、SSL 証明書の生成時に指定したのと同じ共通名にする必要があります。
4. 構成するストアを選択します。
5. [**XenApp Services** サポートの構成] をクリックします。
6. [レガシサポート] を有効にして [**OK**] をクリックします。
7. c:\\inetpub\wwwroot\Citrix\<store name>\Views\PnaConfig\にあるテンプレート構成ファイルにアクセスします。ここで、store name はストア名です。
8. Config.aspx のバックアップを作成します。
9. 元の Config.aspx ファイルを開きます。
10. 行「<EnableSavePassword>**false**</EnableSavePassword>」の「**false**」値を「**true**」に変更します。
11. 編集した Config.aspx ファイルを保存します。
12. StoreFront サーバーで、管理者権限を使って PowerShell を実行します。
13. PowerShell コンソールで、次のように実行します:

    a. 次のディレクトリに変更します。c:\\Program Files\Citrix\Workspace StoreFront\Scripts

    b. 次のように入力します。「Set-ExecutionPolicy RemoteSigned」

    c. 次のように入力します。「.\\ImportModules.ps1」

    d. 次のように入力します。「Set-DSDerviceMonitorFeature –ServiceUrl `https://localhost:443/StorefrontMonitor`

14. StoreFront グループがある場合は、グループのすべてのメンバーで同じコマンドを実行します。

パスワードを保存する **Citrix Gateway** の構成

> 注:
>
> この構成は、Citrix Gateway 負荷分散サーバーを使用します。

Citrix Gateway を構成してパスワードの保存機能をサポートするには:

1. Citrix Gateway 管理コンソールにログオンします。
2. Citrix ベストプラクティスに従って負荷分散仮想サーバー用の証明書を作成します。
3. [Configuration] タブで、[Traffic Management] > [Load Balancing] > [Servers] の順に移動し、[**Add**] をクリックします。
4. StoreFront サーバーのサーバー名と IP アドレスを入力します。
5. [**Create**] をクリックします。StoreFront グループがある場合は、グループ内のすべてのサーバーで手順 5. を繰り返します。
6. [Configuration] タブで、[**Traffic Management**] > [**Load Balancing**] > [**Monitor**] の順に移動し、[**Add**] をクリックします。
7. モニター名を入力します。[Type] として [**STOREFRONT**] を選択します。ページ下部で、[**Secure**] を選択します（StoreFront サーバーでは HTTPS を使用するためこれを選択する必要があります）。
8. [**Special Parameters**] タブをクリックします。前の手順で構成した StoreFront 名を入力し、[**Check Backed Services**] を選択してから [**Create**] をクリックします。
9. [**Configuration**] タブで、[Traffic Management] > [Load Balancing] > [Service Groups] に移動し、[**Add**] をクリックします。
10. サービスグループ名を入力し、プロトコルを [**SSL**] に設定します。[**OK**] をクリックします。
11. 画面の右側の [Advanced Settings] で [**Settings**] を選択します。
12. クライアント IP を有効にして、Header 値を **X-Forwarded-For** にして [**OK**] をクリックします。
13. 画面右側で（[Advanced Settings] の下）[**Monitors**] を選択します。矢印をクリックして新しいモニターを追加します。
14. [**Add**] ボタンをクリックし、[**Select Monitor**] ドロップダウンを選択します。モニターの一覧（Citrix Gateway で構成）が表示されます。
15. 作成したモニターの横にあるラジオボタンをクリックして、[**Select**]、[**Bind**] の順にクリックします。
16. 画面右側で（[Advanced Settings] の下）[**Members**] を選択します。矢印をクリックして新しいサービスグループメンバーを追加します。
17. [**Add**] ボタンをクリックして、[**Select Member**] ドロップダウンを選択します。
18. [**Server Based**] を選択します。サーバーメンバーの一覧（Citrix Gateway で構成）が表示されます。作成した StoreFront サーバーの横にあるラジオボタンをクリックします。

19. ポート番号として「443」と入力し、Hash ID に一意の番号を指定してから［**Create**］、［**Done**］ の順にクリックします。すべてが適切に構成されたら、［**Effective State**］ が緑となってモニターが適正に機能していることが示されます。
20. ［Traffic Management］>［Load Balancing］>［Virtual Server］の順にクリックし、［**Add**］ をクリックします。サーバー名を入力してプロトコルに ［**SSL**］ を選択します。
21. StoreFront 負荷分散サーバーの IP アドレスを入力し、［**OK**］ をクリックします。
22. ［**Load Balancing Virtual Server Service Group**］ を選択し、矢印をクリックして以前に作成したサービスグループを追加します。［**OK**］ を 2 回クリックします。
23. 負荷分散仮想サーバーに対して作成された SSL 証明書を割り当てます。［**No Server Certificate**］ を選択します。
24. 一覧から負荷分散サーバー証明書を選択し ［**Bind**］ をクリックします。
25. ドメイン証明書を負荷分散サーバーに追加します。［**No CA certificate**］ をクリックします。
26. ドメイン証明書をクリックし、［**Bind**］ をクリックします。
27. 画面右側で ［**Persistence**］ を選択します。
28. ［Persistence］を［**SOURCEIP**］に変更して、タイムアウト値を［**20**］に設定します。［**Save**］、［**Done**］の順にクリックします。
29. ドメイン DNS サーバーで負荷分散サーバー（未作成の場合）を追加します。
30. iOS デバイスで iOS 向け Citrix Workspace アプリを起動して、完全な XenApp URL を入力します。

構成

May 20, 2019

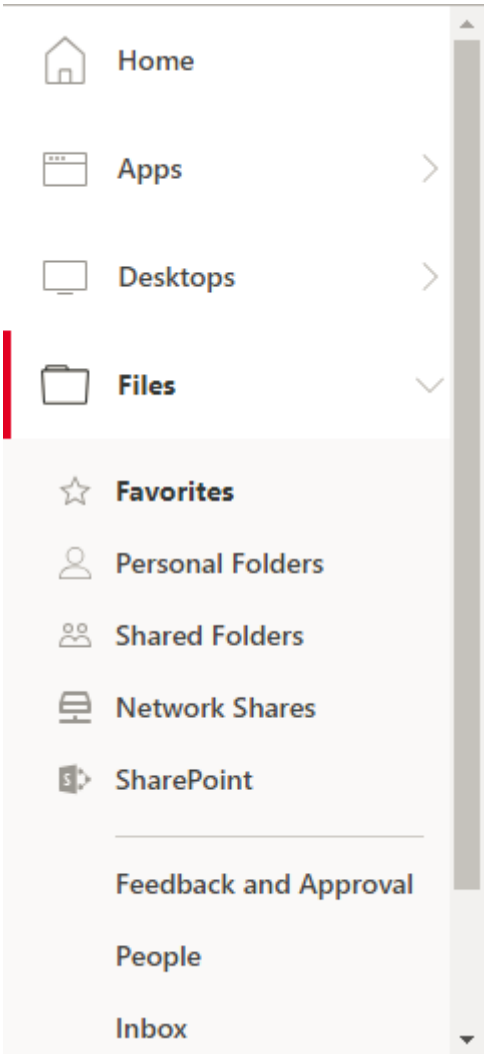
Citrix Workspace アプリでの **Content Collaboration** サービスの統合

Citrix Content Collaboration を使用すると、ドキュメントを簡単かつセキュアに交換したり、メールで大容量のドキュメントを送信したり、サードパーティへのドキュメント転送をセキュアに処理したり、コラボレーションスペースにアクセスすることができます。また、Web ベースのインターフェイス、モバイルクライアント、デスクトップアプリ、Microsoft Outlook や Gmail との統合など、さまざまな方法で作業できます。

Citrix Content Collaboration 機能には、Citrix Workspace アプリの［ファイル］タブからアクセスできます。［ファイル］タブは、Citrix Cloud コンソールのワークスペース構成で Content Collaboration サービスが有効になっている場合にのみ表示されます。

> 注:
>
> オペレーティングシステムでセキュリティオプションが設定されているため、Citrix Workspace アプリでの Citrix Content Collaboration の統合は、Windows Server 2012 および Windows Server 2016 ではサポートされていません。

次の図は、新しい Citrix Workspace アプリの［ファイル］タブの例です:



制限事項:

- Citrix Workspace アプリをリセットしても、Citrix Content Collaboration はログオフされません。
- Citrix Workspace アプリでストアを切り替えても、Citrix Content Collaboration はログオフされません。

環境の構成

iOS 向け Citrix Workspace アプリは Citrix Virtual Apps 環境向けの Web Interface の構成をサポートします。Web Interface では、XenApp Services サイトと Citrix Virtual Apps and Desktops サイトの 2 種類のサイト

を作成できます。これらの Web Interface サイトにより、クライアントデバイスがサーバーファームに接続できるようになります。iOS 向け Citrix Workspace アプリと Web Interface サイト間での認証は、Citrix Secure Web Gateway など、さまざまな方法で実装できます。

また、StoreFront が iOS 向け Citrix Workspace アプリへの認証およびリソース配信を提供するように構成して、デスクトップ、アプリケーション、およびそのほかのリソースをユーザーに配信する一拠点のエンタープライズリソースストアを作成することもできます。

接続の構成については、http://community.citrix.comを参照してください。ビデオ、ブログ、サポートフォーラムなどを利用できます。

Citrix Virtual Apps and Desktops の展開環境で公開されているアプリケーションにユーザーがアクセスできるようにするには、以下のコンポーネントを構成する必要があります。

- アプリケーションを公開するときは、StoreFront のストアを経由してアプリケーションにアクセスするユーザーのエクスペリエンスを向上させるために、次のオプションについて検討します。
  - 公開アプリケーションを簡単に識別できるように、わかりやすい説明を入力します。この説明は、ユーザーの iOS 向け Citrix Workspace アプリに表示されます。
  - 管理者は、iOS 向け Citrix Workspace アプリの［おすすめ］の一覧にアプリケーションを表示して、モバイルデバイスユーザー用の公開アプリケーションを強調できます。iOS 向け Citrix Workspace アプリの［おすすめ］の一覧にアプリケーションを追加するには、サーバー上でその公開アプリケーションのプロパティを編集し、［説明］ボックスに文字列「KEYWORDS:Featured」を追加します。
  - アプリケーションの表示サイズをモバイルデバイスの画面サイズに合わせる機能を有効にするには、サーバー上でその公開アプリケーションのプロパティを編集し、［説明］ボックスに文字列「KEYWORDS:mobile」を追加します。このキーワードの追加により、そのアプリケーションでの自動スクロール機能も有効になります。
  - アプリケーションがストアのユーザー全員に自動的にサブスクライブされるようにするには、Citrix Virtual Apps でそのアプリケーションを公開する時に、説明に KEYWORDS:Auto という文字列を追加します。ユーザーがストアにログオンすると、そのアプリケーションを手動でサブスクライブしなくても自動的にプロビジョニングされます。
- Citrix Virtual Apps and Desktops 展開環境の Web Interface で、Web サイトまたは Citrix Virtual Apps and Desktops サイトを作成します。サイト名およびその作成方法は、インストールしている Web Interface のバージョンにより異なります。サイトの作成方法について詳しくは、使用するバージョンのWeb Interfaceのドキュメントで「サイトの作成」に関するトピックを参照してください。

StoreFront の構成

重要:

- StoreFront を使用すると、iOS 向け Citrix Workspace アプリは Citrix Access Gateway Enterprise Edition 9.3 以降および Citrix Gateway 12 以前をサポートします。
- iOS 向け Citrix Workspace アプリでは、Web Interface の XenApp Services サイトがサポートされます。

- iOS 向け Citrix Workspace アプリは、Web ブラウザーが Workspace for Web と連携している限り、セッションの開始をサポートします。セッションが開始しない場合、iOS 向け Citrix Workspace アプリを介して直接アカウントを構成します。ユーザーは Citrix Workspace のブラウザーを開く機能を使って手動で ICA ファイルを開く必要があります。この展開方法での制限事項については、StoreFrontのドキュメントを参照してください。

StoreFront で作成するストアは、iOS 向け Citrix Workspace アプリのリソース配信インフラストラクチャと認証を提供するサービスにより構成されます。このストアにより、Citrix Virtual Apps and Desktops サイトおよび Citrix Virtual Apps ファームからデスクトップとアプリケーションが列挙および集約され、これらのリソースをユーザーが使用できるようになります。

1. StoreFront をインストールして構成します。詳しくは、StoreFrontの製品ドキュメントを参照してください。iOS 向け Citrix Workspace アプリダウンロードサイトを独自に作成する管理者用に、テンプレートが提供されています。
2. Citrix Virtual Apps and Desktops のアプリケーションと同様の手順で、StoreFront 用にストアを構成します。ユーザーのモバイルデバイス側で特別な構成を行う必要はありません。詳しくは、製品ドキュメントの「StoreFront」のセクションで、「ユーザーアクセスオプション」を参照してください。以下のいずれかの方法を使用します:
    - プロビジョニングファイル。管理者は、ストアに接続するための詳細が定義されたプロビジョニングファイル（CR ファイル）をユーザーに提供します。デバイスにインストールした後で、提供された CR ファイルをユーザーが開くと iOS 向け Citrix Workspace アプリが自動的に構成されます。Web 向け Workspace のサイトは、デフォルトではそのサイトの単一ストア用のプロビジョニングファイルがユーザーに提供されます。または、管理者が Citrix StoreFront 管理コンソールで単一または複数のストア用のプロビジョニングファイルを生成して、それらをユーザーにメールなどで配布することもできます。
    - 手動構成。デスクトップやアプリケーションにアクセスするには、Citrix Gateway またはストア URL が必要であることをユーザーに直接知らせることができます。Citrix Gateway を経由する接続の場合、ユーザーは製品のエディションと必要な認証方法についても把握する必要があります。インストール後、iOS 向け Citrix Workspace アプリにこれらの詳細を入力し、接続が検証され成功すると、ログオンを求められます。
    - 自動構成。ようこそ画面で ［アカウントの追加］ をタップして、アドレスフィールドに StoreFront サーバーの URL を入力します。追加中、アカウントは自動的に構成されます。

Citrix Gateway を構成するには

外部から接続するユーザー（遠隔地からインターネット経由で接続するユーザーなど）にアクセスを提供するには、Citrix Gateway を使用した認証を構成します。

- StoreFront を使用すると、iOS 向け Citrix Workspace アプリは Citrix Access Gateway Enterprise Edition 9.3 以降および Citrix Gateway 12 以前をサポートします。

iOS 向け **Citrix Workspace** アプリでのアプリへのアクセスを構成するには

1. アプリへ自動的にアクセスするよう iOS 向け Citrix Workspace アプリを構成する場合、新しいアカウントを作成する時に［アドレス］フィールドにストアの一致 URL を入力します（例: storefront.organization.com）。
2. スマートカードを使って認証している場合は、［スマートカードの使用］ オプションを選択します。
3. 手動で構成する場合（［オプション］>［手動セットアップ］の順にタップ）、そのほかの必要な情報を入力し、セキュリティトークンを有効にしたり認証の種類を選択したりするなど、Citrix Gateway の認証方法を選択して設定を保存します。

> 注:
>
> ストアへのログオンは約 1 時間有効です。これを超過した場合、再ログオンするまでアプリケーション一覧を更新したりほかのアプリケーションを起動したりできなくなります。

クライアント証明書認証の構成

重要:

- StoreFront を使用すると、iOS 向け Citrix Workspace アプリは Citrix Access Gateway Enterprise Edition 9.3 以降および NetScaler Gateway 11 以前をサポートします。
- クライアント証明書による認証は、iOS 向け Citrix Workspace アプリでサポートされます。
- クライアント証明書による認証は、Access Gateway Enterprise Edition 9.x および 10.x 以降でのみサポートされます。
- 2 要素認証の種類は、Cert と LDAP である必要があります。
- iOS 向け Citrix Workspace アプリでは、クライアント証明書による認証をオプション（選択自由）として設定することもできます。
- この認証では、P12 形式の証明書のみがサポートされます。

Citrix Gateway 仮想サーバーにログオンするユーザーを、クライアント証明書の属性に基づいて認証することもできます。クライアント証明書による認証は、LDAP を使用した 2 要素認証でも使用できます。

クライアント側の証明書の属性でユーザーを認証するには、仮想サーバー上のクライアント認証が有効になっており、クライアント証明書を要求するように構成されている必要があります。さらに、Citrix Gateway 上でルート証明書をその仮想サーバーにバインドする必要があります。

Citrix Gateway 仮想サーバーにログオンしたユーザーの認証後、そのユーザー名およびドメインの情報が証明書の特定フィールドから抽出されます。この情報は、証明書の **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** フィールドにあります。その形式は、「username@domain」です。ユーザー名とドメインが問題なく抽出されたら、ユーザーはそのほかの必須情報（パスワードなど）を提供して、その後ユーザーが認証されます。有効な証明書や資格情報が提供されなかったり、ユーザー名とドメインの抽出に失敗したりすると、認証に失敗します。

クライアント証明書に基づいて認証するには、既定の認証の種類としてクライアント証明書を指定します。また、「証明書アクション」を作成して、クライアントの SSL 証明書に基づいた認証時の動作を定義することもできます。

XenApp Services サイトを構成するには

XenApp Services サイトを作成していない場合は、インストールした Citrix Virtual Apps のバージョンにより、Citrix Virtual Apps の管理コンソールまたは Web Interface 管理コンソールを使ってモバイルデバイス用の XenApp Services サイトを作成します。

iOS 向け Citrix Workspace アプリでは、そのユーザーがアクセスできるアプリケーションの情報を XenApp Services サイトから取得して、モバイルデバイス上で実行中のアプリに表示します。これは、Web Interface を使用して、従来の SSL ベースの Citrix Virtual Apps 接続のために Citrix Gateway を設定する方法に似ています。

iOS 向け Citrix Workspace アプリのために、モバイルデバイス用の XenApp Services サイトを Citrix Gateway 経由の接続をサポートするように構成します。

1. XenApp Services サイトで［**Manage secure client access**］**>**［**Edit secure client access]** の順に選択します。
2. ［Access Method］を［Gateway Direct］に変更します。
3. Citrix Gateway アプライアンスの完全修飾ドメイン名（FQDN）を入力します。
4. Secure Ticket Authority（STA）の情報を入力します。

Citrix Gateway アプライアンスを構成するには

クライアント証明書による認証を使用するには、Citrix Gateway で Cert と LDAP による 2 要素認証を構成する必要があります。

1. Citrix Gateway でセッションポリシーを作成し、iOS 向け Citrix Workspace アプリからの Citrix Virtual Apps 接続を受け付けるように設定し、新しく作成した XenApp Services サイトの場所を指定します。
   - iOS 向け Citrix Workspace アプリからの接続を識別するセッションポリシーを作成します。セッションポリシーを作成したら、次の式を設定し、式の演算子として［Match All Expressions］を選択します:
     REQ.HTTP.HEADER User-Agent CONTAINS CitrixWorkspace
   - セッションポリシーのプロファイル設定で、［Security］タブの［Default Authorization］を［Allow］に設定します。
     ［Published Applications］タブで、これがグローバル設定でない（［Override Global］チェックボックスをオンにする）場合は［ICA Proxy］が［ON］であることを確認します。
     Web Interface のアドレスとして、モバイルデバイスユーザー用に作成した XenApp Services サイトの URL を、「config.xml」を含めて入力します（//XenAppServerName/Citrix/PNAgent/config.xml または/XenAppServerName/CustomPath/config.xml など）。
   - このセッションポリシーを、仮想サーバーにバインドします。
   - Cert と LDAP 用の認証ポリシーを作成します。
   - これらの認証ポリシーを、仮想サーバーにバインドします。
   - TLS ハンドシェイク時にクライアント証明書を要求するように仮想サーバーを構成します。これを行うには、［Certificate］タブの［SSL Parameters］を開き、［Client Authentication］の［Client

Certificate］で［Mandatory］を設定します。
重要：Citrix Gateway で使用するサーバー証明書が（中間証明書を伴う）証明書チェーンの一部である場合は、中間証明書も正しく Citrix Gateway にインストールしてください。証明書のインストールについては、Citrix Gateway のドキュメントを参照してください。

iOS 向け **Citrix Workspace** アプリのモバイルデバイスを構成するには

Citrix Gateway でクライアント証明書による認証を有効にすると、クライアント証明書の属性に基づいてユーザーが認証されます。認証が問題なく完了すると、ユーザー名とドメインが証明書から抽出され、そのユーザーに対して指定されたポリシーが適用されます。

1. iOS 向け Citrix Workspace アプリで、[アカウント] の［サーバー］ボックスに、Citrix Gateway サーバーの FQDN を「GatewayClientCertificateServer.organization.com」のように入力します。iOS 向け Citrix Workspace アプリにより、クライアント証明書が必要であることが自動的に検出されます。
2. ユーザーは、新しい証明書をインストールするか、インストール済みのものを一覧から選択できます。iOS のクライアント証明書認証では、証明書のダウンロードおよびインストールを iOS 向け Citrix Workspace アプリのみを使用して行う必要があります。
3. 有効な証明書を選択した後、ログオン画面にその証明書の情報に基づいてユーザー名とドメインが自動的に入力され、ユーザーはパスワードを含むそのほかの情報を自分で入力します。
4. クライアント証明書による認証をオプションとして設定した場合、ユーザーは証明書ページの［戻る］をクリックすることで証明書の選択をスキップすることができます。この場合、iOS 向け Citrix Workspace アプリはそのまま接続を続行し、ユーザーにログオン画面を表示します。
5. ユーザーが初回ログオンを完了すると、証明書を提示しなくてもアプリケーションを起動できるようになります。ユーザーのアカウントで使用された証明書は iOS 向け Citrix Workspace アプリに格納され、次回以降のログオン時に自動的に使用されるようになります。

Citrix Secure Gateway の構成

XenApp Services サイトを構成するには

重要:

- iOS 向け Citrix Workspace アプリで XenApp Services サイトを使用する場合、Citrix Secure Gateway 3.x がサポートされます。
- iOS 向け Citrix Workspace アプリで Citrix Virtual Apps Web サイトを使用する場合、Citrix Secure Gateway 3.x がサポートされます。
- XenApp Services サイトでは 1 要素認証のみがサポートされ、Citrix Virtual Apps Web サイトでは 1 要素認証および 2 要素認証がサポートされます。
- デバイスに組み込まれているすべての Web ブラウザーでサポートされている、Web Interface 5.4 を使用する必要があります。

この設定を実行する前に、Citrix Gateway をインストールして Web Interface と連動するように設定します。これらの手順は運用環境に合わせて適宜変更できます。

Citrix Secure Gateway 接続を使用する環境では、iOS 向け Citrix Workspace アプリ上の Citrix Gateway オプションを設定しないでください。

iOS 向け Citrix Workspace アプリでは、そのユーザーがアクセスできるアプリケーションの情報を XenApp Services サイトから取得して、デバイス上で実行中の iOS 向け Citrix Workspace アプリに表示します。これは、Web Interface を使用して、従来の SSL ベースの Citrix Virtual Apps 接続のために Citrix Gateway を設定する方法に似ています。Web Interface 5.x 上で動作する XenApp Services サイトには、この構成機能が組み込まれています。

Citrix Secure Gateway からの接続をサポートするように XenApp Services サイトを設定します:

1. XenApp Services サイトで［Manage secure client access］>［Edit secure client access］の順に選択します。
2. ［Access Method］を［Gateway Direct］に変更します。
3. Secure Web Gateway の完全修飾ドメイン名（FQDN）を入力します。
4. Secure Ticket Authority（STA）の情報を入力します。

> 注:
>
> Citrix Secure Gateway の場合、このサイトに対して Citrix 定義のデフォルトのパス（//XenAppServerName/Citrix/PNAgent）を使用することをお勧めします。既定のパスを使用すると、ユーザーは XenApp Services サイト内の config.xml ファイルのフルパス（//XenAppServerName/CustomPath/config.xml など）の代わりに、接続する Secure Web Gateway の FQDN を指定できるようになります。

Citrix Secure Gateway を構成するには

1. Citrix Secure Gateway で、Citrix Secure Gateway 構成ウィザードを使って XenApp Service サイトをホストするセキュアなネットワーク内のサーバーと連動するように Citrix Secure Gateway を設定します。間接オプションを選択した後、Secure Web Gateway サーバーの FQDN パスを入力し、ウィザードを進めます。
2. ユーザーデバイスからの接続をテストして、Secure Web Gateway のネットワークと証明書の割り当てが正しく設定されていることを確認します。

iOS 向け **Citrix Workspace** アプリのモバイルデバイスを構成するには

1. Citrix Secure Gateway アカウントを追加する場合、［アドレス］ フィールドに一致する Citrix Secure Gateway サーバーの FQDN を入力します:
   - 既定のパス（/Citrix/PNAgent）を使って XenApp Services サイトを作成した場合は、Secure Web Gateway の FQDN を「FQDNofSecureGateway.companyName.com」のように入力します。

- 既定のパスを使わず XenApp Services サイトのパスをカスタマイズした場合は、config.xml ファイルへのパスを「FQDNofSecureGateway.companyName.com/CustomPath/config.xml」のように入力します。

2. アカウントを手動で構成する場合は、Citrix Gateway オプションの ［新規アカウント］ ダイアログをオフにします。

Web Interface の構成

Web Interface サイトを構成するには

iPhone および iPad のユーザーは、デバイスの Safari ブラウザーで Web Interface サイトに接続してアプリケーションを起動します。管理者は、ほかの Citrix Virtual Apps アプリケーションと同じ方法で Web Interface サイトを設定できます。モバイルデバイス用に XenApp Services サイトが設定されていない場合、iOS 向け Citrix Workspace アプリは自動的に Web Interface サイトに接続されます。ユーザーのモバイルデバイス側で特別な構成を行う必要はありません。

iPhone および iPad の Safari では、Web Interface 5.x がサポートされています。

iOS デバイス上でアプリケーションを起動するには

ユーザーデバイスで、通常の資格情報を入力して Web Interface サイトにログオンします。

モバイルデバイスの自動構成

StoreFront で、ストアで使用される Citrix Gateway 環境やビーコンポイントなどの詳細情報が定義されたプロビジョニングファイルを生成するには、［複数ストアのプロビジョニングファイルのエクスポート］および［プロビジョニングファイルのエクスポート］タスクを使用します。ユーザーにプロビジョニングファイルを提供すると、ユーザーが iOS 向け Citrix Workspace アプリを簡単に構成できるようになります。iOS 向け Citrix Workspace アプリのプロビジョニングファイルは、Workspace for Web サイトから入手できるようにすることもできます。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上で Citrix StoreFront 管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windows の［スタート］画面または［アプリ］画面で、[Citrix StoreFront］タイルをクリックします。Citrix StoreFront 管理コンソールの左ペインで［ストア］ノードを選択します。
2. 複数のストアの詳細情報が定義されたプロビジョニングファイルを生成するには、［操作］ペインの［複数ストアのプロビジョニングファイルのエクスポート］をクリックして、対象のサイトを選択します。
3. ［エクスポート］をクリックして、拡張子が.cr のプロビジョニングファイルをネットワーク上の適切な場所に保存します。

アカウントの手作業での構成

通常、iOS 向け Citrix Workspace アプリで Citrix Gateway に接続すると、認証の後で XenApp Services サイトまたは Citrix Virtual Apps Web サイトが検出されます。サイトが検出されない場合、iOS 向け Citrix Workspace アプリはエラーを表示します。この問題を避けるには、iOS 向け Citrix Workspace アプリが正しく Citrix Gateway に接続されるように、手作業でアカウントを構成します。

1. 画面右上の［アカウント］アイコンをタップして、［アカウント］画面のプラス記号（+）をタップします。［新規アカウント］画面が開きます。
2. 画面左下の［オプション］の左側のアイコンをタップして、［手動セットアップ］をタップします。画面に追加のフィールドが表示されます。
3. ［アドレス］フィールドに、接続先のサイトまたは Citrix Gateway の URL（agee.mycompany.com など）を入力します。
4. 次のいずれかの接続オプションを選択します。選択するオプションにより、異なるフィールドが表示されます。
   - Web Interface - iOS 向け Citrix Workspace アプリで Citrix Virtual Apps Web サイトを表示する場合は、このオプションを選択します。Web ブラウザーでの表示に似ており、「Web ビュー」とも呼ばれます。
   - XenApp Services - Citrix Gateway 経由の認証が構成されていない特定の XenApp Services サイトを指定する場合は、このオプションを選択します。追加されるフィールドに、ログオン用の資格情報を入力します。
     - <StoreFront FQDN>：複数のストアがある場合は一覧が表示され、追加するストアをユーザーが選択できます。
     - <StoreFront FQDN>/citrix/<Store Name>：<Store Name> に指定する StoreFront のストアが追加されます。ここで、Store Name はストア名です。
     - <StoreFront FQDN>/citrix/PnAgent/config.xml：従来の既定の PNAgent ストアが追加されます。
     - <StoreFront FQDN>/citrix/<Store Name>/PnAgent/config.xml：<Store Name> に関連付けられている従来の PNAgent ストアが追加されます。ここで、Store Name はストア名です。
   - Citrix Gateway - 特定の Citrix Gateway 経由で XenApp Services サイトに接続する場合は、このオプションを選択します。追加されるオプションでサーバーのエディションを選択し、ログオン用の資格情報、セキュリティトークンを使用するかどうかなどを指定します。
5. ［証明書の警告を無視］で、無効、自己署名、または期限切れの証明書を無視してサーバーに接続するかどうかを指定します。デフォルトでは、［オフ］になっています。

   重要：このオプションをオンにする場合は、常に接続先のサーバーが正しいかどうかを確認してください。ユーザーのデバイスを不正な攻撃から守るため、すべてのサーバー上に有効な証明書をインストールしておくことを強くお勧めします。証明機関から入手した SSL 証明書を使用すると、サーバーのセキュリティが向上します。自己署名入りの証明書を使用したり、証明書を使用しなかったりすることは推奨されません。
6. ［保存］をタップします。
7. ユーザー名およびパスワード（2 要素認証を選択した場合はトークン）を入力し、［ログオン］をタップします。iOS 向け Citrix Workspace アプリの画面が開き、デスクトップにアクセスしたり、アプリを追加および

実行したりできます。

派生資格情報の構成

iOS 向け Citrix Workspace アプリでは、Purebred による派生資格情報がサポートされています。派生資格情報を使用できるストアに接続するときに、ユーザーは仮想スマートカードを使用して iOS 向け Citrix Workspace アプリにログオンできます。この機能は、オンプレミス展開のみでサポートされます。

> 注:
>
> この機能を使用するには、Citrix Virtual Apps and Desktops 7 1808 以降が必要です。

iOS 向け Citrix Workspace アプリで派生資格情報を有効にするには:

1. ［設定］**>**［詳細］**>**［派生資格情報］ に移動します。
2. ［派生資格情報を使用］ をタップします。

派生資格情報で使用する仮想スマートカードを作成するには:

1. ［設定］**>**［詳細］**>**［派生資格情報］ で、［新しい仮想スマートカードを追加］ をタップします。
2. 表示された仮想スマートカードの名前を編集します。
3. 数字のみ 8 桁の PIN を入力し、確定します。
4. ［次へ］ をタップします。
5. ［認証証明書］で、［証明書のインポート］ をタップします。
6. ドキュメントピッカーが表示されます。［参照］ をタップします。
7. ［場所］で、［**Purebred Key Chain**］ を選択します。
8. 一覧から、インポートする認証証明書を選択します。
9. ［キーのインポート］ をタップします。
10. 手順 5 ～ 9 を繰り返して、デジタル署名証明書と暗号化証明書をインポートします（必要な場合）。
11. ［保存］ をタップします。

証明書は、仮想スマートカードに最大 3 つまでインポートできます。仮想スマートカードが正しく動作するには、認証証明書が必要です。暗号化証明書とデジタル署名証明書は、VDA セッション内で使用するために追加することができます。

> 注:
>
> HDX セッションに接続する場合は、作成された仮想スマートカードがセッションにリダイレクトされます。

既知の制限事項

- ユーザーは、有効なカードを一度に 1 つだけ保持することができます。
- 仮想スマートカードは、いったん作成すると編集することができません。仮想スマートカードに変更を加えるには、ユーザーはカードを削除し、新しいカードを作成する必要があります。
- 無効な PIN は、10 回まで入力できます。10 回目の試行後、仮想スマートカードは削除されます。

- 派生資格情報を選択すると、セッションでスマートカードが必要な場合に、作成した仮想スマートカードが物理スマートカードよりも優先されます。

Citrix Ready ワークスペースハブの構成

次のシステム要件がすべて満たされている場合、Citrix Workspace アプリで Citrix Ready ワークスペースハブが有効になります:

- iOS 向け Citrix Workspace アプリ 1810.1 以降
- Bluetooth に対応している
- モバイルデバイスとワークスペースハブが同じ Wi-Fi ネットワークを使用している

構成

Citrix Ready ワークスペースハブの各機能を有効にするには、デバイス上で［設定］に移動し、［**Citrix Casting**］をタップして機能を有効化します。詳しくは、iOSデバイスのヘルプドキュメントを参照してください。

既知の制限事項

- セッションのローミングは、オンプレミスのストアに接続されている iPhone デバイスに限られます。
- VDA 7.18 およびそれ以前の場合、ワークスペースハブにキャストするには、使用するデスクトップまたはその他のリソースで H.264 の全画面ポリシーが有効、および従来のグラフィックモードポリシーが無効になっている必要があります。

トラブルシューティング

May 20, 2019

セッションの切断

ユーザーが以下の操作を行うと、iOS 向け Citrix Workspace アプリセッションを終了せずに切断できます:

- セッションで公開アプリまたはデスクトップを表示している間に次のことを実行する:
  - 画面を上部で矢印をタップして、セッションのドロップダウンメニューを表示させる。
  - ［ホーム］ ボタンをタップして、起動パッドに戻る。
  - アクティブなセッションに残っている公開アプリのいずれかのアイコンの下にある白い影をタップする。
  - 切断をタップする。
- iOS 向け Citrix Workspace アプリを終了する:

  - デバイスの ［ホーム］ ボタンをダブルタップする。
  - iOS App Switcher ビューで、iOS 向け Citrix Workspace アプリを探す。
  - 表示されるダイアログで切断をタップする。
- モバイルデバイスのホームボタンを押す。
- アプリのドロップダウンメニュー内の［ホーム］または［切り替え］をタップする。

これらの操作を行うと、セッションは切断状態のままサーバーに保持されます。ユーザーはこの切断セッションに再接続できますが、管理者は特定の時間が経過した後に切断セッションが自動的に終了するように設定できます。これを行うには、リモートデスクトップセッションホストサーバーの構成（「ターミナルサービス構成」の新名称）で［ICA-tcp］接続の設定を変更します。リモートデスクトップサービス（「ターミナルサービス」の新名称）の設定について詳しくは、Microsoft Windows Server の製品ドキュメントを参照してください。

アプリケーションでのテンキーの問題

公開アプリケーションでテンキーの使用に問題が生じる場合は、iOS 向け Citrix Workspace アプリで Unicode キーボードを無効にします。これを行うには、［設定］タブで ［キーボードオプション］ をタップし、［Unicode キーボードを使用］を ［オフ］ にします。

Citrix Virtual Apps and Desktops での **HDX** の音質

iOS 向け Citrix Workspace アプリを使用した Citrix Virtual Apps and Desktops のセッションで、音声と動画を使用するときに HDX 機能の音質が低下することがあります。この問題は、Citrix Virtual Apps and Desktops の HDX に関連するポリシーが音声と動画のデータ量に対応できない場合に発生します。音質を改善するためのポリシー作成については、Knowledge Center のCTX123543を参照してください。

Citrix Cloud で使用できるデモ用アカウント

現在アカウントを持っていないユーザーは、Citrix Cloud（http://cloud.citrix.com/）デモサイトでデモ用ユーザーアカウントを作成できます。

Citrix Cloud では、独自に環境を設定しなくても、Citrix ソリューションの有効性を体験することができます。Citrix Cloud デモ環境では、Citrix Virtual Apps and Desktops、Citrix Gateway などの、数多くの主要な Citrix ソリューションが使用されています。

ただし、このデモ環境ではデータが保存されません。また、セッションを切断した後に再接続できない可能性があります。

有効期限が切れたパスワード

iOS 向け Citrix Workspace アプリでは、有効期限が切れたパスワードをユーザーが変更することができます。パスワードの有効期限が切れると、必要な情報を入力するためのメッセージが表示されます。

接続パフォーマンスの低下

XenApp Services サイトへの接続パフォーマンスが低下したり、アプリケーションアイコンが表示されなくなったり、「プロトコルドライバーエラー」が表示されたりする場合は、Citrix Virtual Apps サーバーおよび Citrix Secure Web Gateway または Web Interface サーバーのネットワークインターフェイスで、以下の Citrix PV Ethernet Adapter プロパティを無効にしてください:

- 大量送信オフロード
- オフロード IP チェックサム
- オフロード TCP チェックサム
- オフロード UDP チェックサム

サーバーを再起動する必要はありません。この回避策は、Windows Server 2003 および Windows Server 2008（32 ビット）で使用できます。Windows Server 2008 R2 では、この問題は発生しません。

アプリケーションが個別のセッションで実行されることがある

アプリケーションの共有機能が有効になっている場合でも、サーバー側でこの問題が発生することがあります。これは間欠的な問題であり、現在回避策はありません。

App Switcher が動作していない

IT 管理者によりアプリが同じサーバー上で公開されている必要があります。そうでない場合は、App Switcher は動作しません。

ジェイルブレイクされたデバイスでの **StoreFront** からのアプリケーションの実行の禁止

ユーザーがジェイルブレイクされた iOS デバイスで接続することにより、展開環境のセキュリティを侵害する可能性があります。ジェイルブレイクしたデバイスは、その所有者によりセキュリティ権限が変更され、特定のセキュリティ保護機能を効果的にバイパスします。

iOS 向け Citrix Workspace アプリでジェイルブレイクされた iOS が検出されると、ユーザーに通知が表示されます。環境のセキュリティをさらに保護する野に役立てるため、StoreFront または Web Interface を構成して、検出したジェイルブレイクされたデバイスでアプリを実行できないようにすることができます。

要件

- Citrix Receiver for iOS 6.1 以降
- StoreFront 3.0 または Web Interface 5.4 以降
- StoreFront または Web Interface への管理者アカウントによるアクセス

検出したジェイルブレイクされたデバイスでアプリを実行できないようにするには

1. StoreFront または Web Interface サーバーに管理者特権を持つユーザーとしてログオンします。
2. default.ica ファイルを見つけます。このファイルは以下のいずれかの場所にあります:
    - **C:\inetpub\wwwroot\Citrix***storename***conf**（Microsoft インターネットインフォメーションサービス）
    - **C:\inetpub\wwwroot\Citrix***storename***App_Data**（Microsoft インターネットインフォメーションサービス）
    - **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF**（Apache Tomcat）
3. **[Application]** セクションに以下の行を追加します。**AllowJailBrokenDevices=OFF**
4. ファイルを保存して StoreFront または Web Interface サーバーを再起動します。

StoreFront サーバーを再起動した後は、ジェイルブレイクされたデバイスについての通知を受け取ったユーザーは StoreFront または Web Interface サーバーからアプリを起動できません。

検出したジェイルブレイクされたデバイスでアプリを実行できるようにするには

AllowJailBrokenDevices を設定しなければ、デフォルトの動作ではジェイルブレイクされたデバイスについてユーザーに通知が表示されますが、依然としてアプリケーションを起動が許可されます。

ジェイルブレイクされたデバイスでのアプリの実行をユーザーに明確に許可するには、次の手順に従います:

1. StoreFront または Web Interface サーバーに管理者特権を持つユーザーとしてログオンします。
2. default.ica ファイルを見つけます。このファイルは以下のいずれかの場所にあります:
    - **C:\inetpub\wwwroot\Citrix***storename***conf**（Microsoft インターネットインフォメーションサービス）
    - **C:\inetpub\wwwroot\Citrix***storename***App_Data**（Microsoft インターネットインフォメーションサービス）
    - **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF**（Apache Tomcat）
3. **[Application]** セクションに以下の行を追加します。**AllowJailBrokenDevices=ON**
4. ファイルを保存して StoreFront または Web Interface サーバーを再起動します。

AllowJailBrokenDevices を ON に設定すると、ユーザーはジェイルブレイクされたデバイスについて通知を受け取りますが、StoreFront または Web Interface サーバー経由でアプリケーションを実行できます。

iOS 向け Citrix Workspace アプリ通信のセキュリティ保護

サーバーファームと iOS 向け Citrix Workspace アプリ間の通信を保護するには、Citrix Gateway など、以下の一連のセキュリティ技術を使用します。

> 注:
>
> StoreFront サーバーとユーザーデバイス間の通信を保護するには、Citrix Gateway を使用することをお勧めします。

- SOCKS プロキシサーバーまたは Secure プロキシサーバー（セキュリティプロキシサーバー、HTTPS プロキシサーバーとも呼ばれます）。プロキシサーバーでネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、iOS 向け Citrix Workspace アプリとサーバー間の接続を制御できます。iOS 向け Citrix Workspace アプリは、SOCKS プロトコルと Secure プロキシプロトコルをサポートしています。
- Secure Web Gateway。Secure Web Gateway を Web Interface と一緒に使うと、社内ネットワーク上のサーバーにインターネットを介して接続できる、暗号化された安全な単一のアクセスポイントをユーザーに提供できます。
- Transport Layer Security（TLS）プロトコルによる SSL Relay ソリューション。
- ファイアウォール。ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。サーバーの内部 IP アドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまり NAT（Network Address Translation：ネットワークアドレス変換））を介して iOS 向け Citrix Workspace アプリを使用する場合は、外部アドレスを構成します。

証明書について

プライベート（自己署名）証明書

リモートゲートウェイにプライベート証明書がインストールされている場合は、組織の証明機関のルート証明書をユーザーデバイスにインストールしないと、iOS 向け Citrix Workspace アプリを使用して Citrix リソースにアクセスできません。

> 注:
>
> 接続時にリモートゲートウェイの証明書を検証できない場合（iOS のキーストアにルート証明書が含まれていないため）、信頼されていない証明書の警告が表示されます。ユーザーが警告に対してそのまま続行することを選択した場合、アプリケーションの一覧が表示されますが、アプリケーションの起動に失敗します。

iOS 向け **Citrix Workspace** アプリデバイスへのルート証明書のインポート

証明書の発行者のルート証明書を取得して、デバイスに設定されているアカウントに電子メールで送信します。添付ファイルをクリックすると、ルート証明書をインポートするかどうかを確認するメッセージが表示されます。

ワイルドカード証明書

ワイルドカード証明書は、同一ドメイン内の任意のサーバーで個別のサーバー証明書の代わりに使用します。iOS 向け Citrix Workspace アプリでは、ワイルドカード証明書がサポートされています。

中間証明書と **Citrix Gateway**

証明書チェーンに中間証明書が含まれる場合は、中間証明書を Citrix Gateway のサーバー証明書に関連付ける必要があります。中間証明書を Citrix Gateway アプライアンスにインストールして、プライマリ CA とリンクする方法については、Knowledge Center のCTX114146を参照してください。

サーバー証明書検証ポリシー

iOS 向け Citrix Workspace アプリのリリースでは、サーバー証明書に関する厳格な検証ポリシーがあります。

> 重要
>
> このバージョンの iOS 向け Citrix Workspace アプリをインストールする前に、サーバーまたはゲートウェイの証明書が、ここで説明されているように正しく構成されていることを確認してください。以下の場合、接続できないことがあります:
>
> - サーバーまたはゲートウェイの構成に間違ったルート証明書が含まれている
> - サーバーまたはゲートウェイ構成にすべての中間証明書が含まれていない
> - サーバーまたはゲートウェイ構成に期限切れまたは無効な中間証明書が含まれている
> - サーバーまたはゲートウェイ構成にクロスルート用中間証明書が含まれていない

iOS 向け Citrix Workspace アプリは、サーバー証明書を検証するときにサーバー（またはゲートウェイ）が提供するすべての証明書を使用するようになりました。以前のリリース同様、iOS 向け Citrix Workspace アプリは、証明書が信頼済みかについても確認します。すべての証明書が信頼済みでない場合、接続に失敗します。

このポリシーは、Web ブラウザーの証明書ポリシーより厳格です。多くの Web ブラウザーには、多数の信頼済みのルート証明書セットが含まれます。

サーバー（またはゲートウェイ）は、正しい証明書セットで構成する必要があります。不正な証明書のセットを使用すると、iOS 向け Citrix Workspace アプリの接続に失敗することがあります。

以下は、ゲートウェイがこのような有効な証明書で構成されていることを前提としています。この構成は、iOS 向け Citrix Workspace アプリで使用されるルート証明書を正確に確認するために、より厳格な検証が必要なユーザーにお勧めします:

- 「サーバー証明書サンプル」
- 「中間証明書サンプル」
- 「ルート証明書サンプル」

次に、iOS 向け Citrix Workspace アプリはこれらすべての証明書が有効であることを確認します。iOS 向け Citrix Workspace アプリが「ルート証明書サンプル」を信頼済みであることも確認します。iOS 向け Citrix Workspace アプリが「ルート証明書サンプル」を信頼していない場合、接続に失敗します。

> 重要
>
> 証明機関によっては、複数のルート証明書があります。このような、より厳格な検証が必要であれば、構成で

> 適切なルート証明書が使用されていることを確認してください。たとえば、現在同じサーバー証明書を検証できる 2 つの証明書（「DigiCert」/「GTE CyberTrust Global Root」および「DigiCert Baltimore Root」/「Baltimore CyberTrust Root」）があるとします。ユーザーデバイスによっては、両方のルート証明書が使用できます。その他のデバイスでは、1 つの証明書のみを使用できます（「DigiCert Baltimore Root」/「Baltimore CyberTrust Root」）。ゲートウェイで「GTE CyberTrust Global Root」を構成すると、これらのユーザーデバイスで iOS 向け Citrix Workspace アプリの接続に失敗します。どのルート証明書を使用すべきかについては、証明機関のドキュメントを参照してください。また、ルート証明書の有効期限についても注意してください。

iOS 向け Citrix Workspace アプリはこれらすべての証明書が有効であることを確認します。次に、ユーザーデバイスでルート証明書を検索します。正しく検証される証明書が見つかり、信頼済みである場合（「ルート証明書サンプル」など）、接続は成功します。信頼済みの証明書が見つからない場合は、失敗します。この構成では、iOS 向け Citrix Workspace アプリが必要とする中間証明書が提供されますが、iOS 向け Citrix Workspace アプリは任意の有効な、信頼済みのルート証明書を選択できます。

以下は、ゲートウェイがこのような証明書で構成されていることを前提としています。

- 「サーバー証明書サンプル」
- 「中間証明書サンプル」
- 「間違ったルート証明書」

Web ブラウザーは、不正なルート証明書を無視することがありますが、iOS 向け Citrix Workspace アプリは不正なルート証明書を無視しないため、接続は失敗します。

証明機関によっては、複数の中間証明書を使用します。この場合、ゲートウェイは通常、以下のようにすべて中間証明書（ルート証明書ではない）で構成されます：

- 「サーバー証明書サンプル」
- 「中間証明書サンプル 1」
- 「中間証明書サンプル 2」

> 重要
>
> 証明機関によっては、クロスルート用中間証明書を使用します。これは、複数のルート証明書があり、以前のルート証明書が最新のルート証明書と同時に使用中の状況を想定しています。この場合、少なくとも 2 つの中間証明書が存在します。たとえば、以前のルート証明書「Class 3 Public Primary Certification Authority」には、関連するクロスルート用中間証明書「VeriSign Class 3 Public Primary Certification Authority - G5」があります。ただし、最新のルート証明書「VeriSign Class 3 Public Primary Certification Authority - G5」も利用可能であり、「Class 3 Public Primary Certification Authority」に置き換わります。最新のルート証明書はクロスルート用中間証明書を使用しません。
>
> 注
>
> クロスルート用中間証明書およびルート証明書は、同じサブジェクト名（発行先）ですが、クロスルート中間証明書には異なる発行者名（発行元）があります。これによって、クロスルート用中間証明書と通常の中間証明書（「中間証明書サンプル 2」など）を区別できます。

通常は、このルート証明書およびクロスルート用中間証明書を省略した構成が推奨されます:

- 「サーバー証明書サンプル」
- 「中間証明書サンプル」

クロスルート用中間証明書をゲートウェイで構成しないでください。これは、ゲートウェイで以前のルート証明書が選択されるようになるのを避けるためです:

- 「サーバー証明書サンプル」
- 「中間証明書サンプル」
- 「クロスルート用中間証明書サンプル」(非推奨)

ゲートウェイでサーバー証明書のみを構成しないでください:

- 「サーバー証明書サンプル」

この場合、iOS 向け Citrix Workspace アプリはすべての中間証明書を検出できないため、接続に失敗します。

Citrix Gateway による接続

リモートのユーザーが Citrix Gateway を介して Citrix Endpoint Management 環境に接続できるようにするには、StoreFront と通信するように証明書を構成します。このアクセスを有効にする方法は、Citrix Endpoint Management のエディションによって異なります。

ネットワークで Citrix Endpoint Management を展開する場合、Citrix Gateway と StoreFront を統合することで Citrix Gateway を経由して内部ユーザーやリモートユーザーが StoreFront に接続できます。ユーザーは、StoreFront に接続して XenApp の公開アプリケーションや XenDesktop の仮想デスクトップにアクセスします。ユーザーは、iOS 向け Citrix Workspace アプリを使用して接続を行います。

Secure Web Gateway による接続

このトピックの内容は、Web Interface 環境にのみ適用されます。

Secure Web Gateway を通常モードまたはリレーモードのどちらかで使用して、iOS 向け Citrix Workspace アプリとサーバーの間にセキュアな通信チャネルを提供できます。Secure Web Gateway を通常モードで使用し、ユーザーが Web Interface 経由で接続する場合は、iOS 向け Citrix Workspace アプリ側での構成は不要です。

iOS 向け Citrix Workspace アプリが Secure Web Gateway サーバーに接続するときは、リモートの Web Interface サーバーで構成されている設定が使用されます。

Secure Web Gateway Proxy がセキュリティで保護されたネットワーク内のサーバーにインストールされている場合は、Secure Web Gateway Proxy をリレーモードで使用できます。ただし、リレーモードで使用する場合、Secure Web Gateway サーバーはプロキシサーバーとして機能するため、iOS 向け Citrix Workspace アプリで次の項目を構成する必要があります:

- Secure Web Gateway サーバーの完全修飾ドメイン名(FQDN)。

- Secure Web Gateway サーバーのポート番号。Secure Web Gateway Version 2.0 では、リレーモードはサポートされていません。

完全修飾ドメイン名には、以下の 3 つの要素を順に指定する必要があります:

- ホスト名
- サブドメイン名
- 最上位ドメイン名

例えば、my_computer.example.com は完全修飾ドメイン名です。ホスト名（my_computer）、サブドメイン名（example）、最上位ドメイン名（com）が順に指定されています。一般的には、サブドメイン名と最上位ドメイン名の組み合わせ（example.com）をドメイン名といいます。

プロキシサーバー経由の接続

プロキシサーバーは、ネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、iOS 向け Citrix Workspace アプリとサーバー間の接続を制御するために使います。iOS 向け Citrix Workspace アプリは、SOCKS プロトコルと Secure プロキシプロトコルをサポートしています。

iOS 向け Citrix Workspace アプリで Citrix Virtual Apps and Desktops サーバーと通信する場合、Web Interface サーバー上でリモートで構成されているプロキシサーバー設定が使用されます。

iOS 向け Citrix Workspace アプリで Web サーバーと通信する場合は、ユーザーデバイス上の既定の Web ブラウザーで構成されているプロキシサーバー設定が使用されます。各ユーザーデバイス上の既定の Web ブラウザーで、プロキシサーバー設定を構成する必要があります。

ファイアウォールを介した接続

ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。ファイアウォールが使用されている環境では、iOS 向け Citrix Workspace アプリと Web サーバーおよびシトリックス製品のサーバーとの通信がファイアウォールでブロックされないように設定する必要があります。このためには、ユーザーデバイスと Web サーバー間の HTTP トラフィック（一般に標準 HTTP ポート 80、またはセキュアな Web サーバーを使用している場合はポート 443 での通信）がファイアウォールを通過できるように設定します。また、シトリックス製品サーバー通信では、ポート 1494 とポート 2598 の受信 ICA トラフィックがファイアウォールを通過できるように設定します。

ファイアウォールによるネットワークアドレス変換（NAT：Network Address Translation）を使用している場合は、Web Interface を使って内部アドレスから外部アドレスおよびポートへのマッピングを定義できます。たとえば、Citrix Virtual Apps and Desktops サーバーに代替アドレスが設定されていない場合は、Web Interface から iOS 向け Citrix Workspace アプリに代替アドレスが提供されるように設定できます。これにより、iOS 向け Citrix Workspace アプリでのサーバー接続で、外部アドレスおよびポート番号が使用されるようになります。

TLS を使用したインストール

iOS 向け Citrix Workspace アプリは XenApp/XenDesktop との TLS 接続に、以下の暗号の組み合わせを使用した TLS 1.0、1.1、1.2 をサポートします:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> 注:
>
> iOS 9 上で実行されている iOS 向け Citrix Workspace アプリは、以下の暗号化の組み合わせをサポートしません:
>
> - TLS_RSA_WITH_RC4_128_SHA
> - TLS_RSA_WITH_RC4_128_MD5

Transport Layer Security(TLS)は、SSL プロトコルの最新の標準化バージョンです。IETF(Internet Engineering TaskForce)が、TLS の公開標準規格の開発を Netscape Communications 社から引き継いだ時に、SSL という名前を TLS に変更しました。

TLS は、サーバーの認証、データの暗号化、メッセージの整合性の確認を行って、データ通信をセキュアに保護します。米国政府機関をはじめとする組織の中には、データ通信を保護するために TLS の使用を義務付けているところもあります。このような組織では、さらに FIPS 140(Federal Information Processing Standard)などのテスト済み暗号化基準の使用を義務付けられる場合があります。FIPS 140 は、暗号化の情報処理規格です。

iOS 向け Citrix Workspace アプリは、ビット長 1024、2048 および、3072 の RSA キーをサポートします。さらに、ビット長 4096 の RSA キーを持つルート証明書がサポートされます。

> 注:
>
> iOS 向け Citrix Workspace アプリは、プラットフォーム(iOS)の暗号化機能を iOS 向け Citrix Workspace アプリと StoreFront の接続に使用します。

iOS 向け **Citrix Workspace** アプリの **TLS** の構成と有効化

TLS のセットアップは、以下の 2 つの手順で行います:

1. Citrix Virtual Apps and Desktops サーバーおよび Web Interface サーバー上で SSL Relay をセットアップし、必要なサーバー証明書を入手してインストールします。
2. ユーザーデバイス上で、ルート証明書をインストールします。

ユーザーデバイスへのルート証明書のインストール

TLS 機能が有効になっている iOS 向け Citrix Workspace アプリと Citrix Virtual Apps and Desktops 間の通信を TLS で保護するには、サーバー証明書の証明機関の署名を認証するためのルート証明書がユーザーデバイスにインストールされている必要があります。

iOS には約 100 の商用ルート証明書が付属していますが、ほかの証明書を使用する場合は、証明機関から証明書を入手して、それを各ユーザーデバイスにインストールします。

企業の方針によっては、ルート証明書のインストールはエンドユーザーではなく管理者が行う場合があります。ルート証明書を簡単および確実にインストールするには、iOS のキーチェーンにその証明書を追加します。

ルート証明書をキーチェーンに追加するには

1. 証明書ファイルをメール添付で自分に送信します。
2. 証明書ファイルをデバイスで開きます。これにより、キーチェーンアクセスが起動します。
3. プロンプトに従って証明書を追加します。
4. iOS 10 を起動して［iOS 設定］>［情報］>［証明書信頼設定］から証明書が信頼されていることを確認します。［証明書信頼設定］で、［ルート証明書の完全な信頼を有効にする］のセクションを参照します。証明書が完全に信頼されていることを確認して下さい。

ルート証明書がインストールされ、TLS が有効なクライアントおよび TLS を使用するすべてのアプリケーションで使用可能になります。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States