StoreFront 2402

Contents

StoreFront 2402 長期サービスリリースの概要 **5**

新機能 **6**

2402（初期リリース）の新機能 **6**

2402 の既知の問題 **11**

オンプレミスストアの新しい **UI (Technical Preview)** **12**

インストール、セットアップ、アップグレードおよびアンインストール **23**

StoreFront の展開計画 **23**

ユーザーアクセスのオプション **27**

システム要件 **33**

StoreFront のインストール **39**

Citrix カスタマーエクスペリエンス向上プログラム **43**

Citrix Analytics Service **45**

HTTPS による **StoreFront** のセキュリティ保護 **55**

StoreFront 展開環境のセキュリティ **60**

メールアドレスによるアカウント検出 **71**

新しい展開環境の作成 **72**

既存のサーバーグループへの参加 **73**

StoreFront のアップグレード **75**

サーバーを出荷時のデフォルト設定にリセット **80**

StoreFront のアンインストール **81**

認証と委任の構成 **82**

認証の構成 **83**

スマートカード認証 **85**

ドメインパススルー認証 **89**

Citrix Gateway からのパススルー **91**

SAML 認証 **95**

ユーザー名とパスワード認証 **101**

フェデレーション認証サービスの構成 **110**

ストアの構成と管理 **111**

ストアの作成 **113**

ストアの構成 **120**

ストアの削除 **121**

ユーザー用のストアプロビジョニングファイルのエクスポート **121**

ユーザーに対するストアの非表示および提供 **122**

Kerberos 委任 **123**

ストアに表示するリソースの管理 **124**

Citrix Gateway を介したストアへのリモートアクセスの管理 **145**

証明書失効一覧（**CRL**）のチェック **147**

共通のサブスクリプションデータストアを共有する **2** つの **StoreFront** ストアの構成 **155**

ストアのお気に入りを管理する **157**

Microsoft SQL Server を使用したサブスクリプションデータの保存 **163**

お気に入りの有効化または無効化 **182**

Citrix Virtual Apps and Desktops の構成 **183**

ストアの詳細設定 **185**

ストアの最適な **HDX** ルーティングの構成 **192**

サブスクリプションの同期 **196**

セッション設定の構成 **200**

ICA ファイルの署名 **201**

Citrix Workspace アプリの構成 **203**

Web サイトの管理 **204**

Web サイトの作成 **204**

Web サイトの構成 **207**

カテゴリ設定 **209**

外観のカスタマイズ **213**

おすすめアプリのグループ **215**

認証方法 **219**

Web サイトのショートカット **221**

Citrix Workspace アプリの展開 **223**

セッション設定の構成 **226**

ワークスペースコントロール **229**

クライアントインターフェイスの設定 **232**

App Protection **234**

Web サイトの削除 **235**

Workspace アプリの **Web** サイトを構成する **235**

サーバーグループの構成 **236**

Citrix Gateway および **NetScaler ADC** との統合 **238**

Citrix Gateway の構成 **239**

Citrix Gateway のインポート **247**

NetScaler ADC による負荷分散 **255**

DFA 用の **Citrix Gateway** および **StoreFront** の構成 **268**

異なるドメインを使用した認証 **271**

ビーコンポイントの構成 **281**

内部および外部で使用される単一の **FQDN** の作成 **283**

StoreFront 構成のエクスポートとインポート **284**

エンドユーザーガイド **294**

StoreFront SDK **302**

StoreFront のトラブルシューティング **312**

サードパーティ製品についての通知 **315**

StoreFront 2402 長期サービスリリースの概要

June 6, 2024

StoreFront は、Citrix Virtual Apps and DesktopsサイトおよびCitrix DaaSからアプリケーションとデスクトップを集約して、使いやすい単一のストアとして機能するエンタープライズアプリストアです。

StoreFront 内で 1 つ以上のストアを構成できます。各ストアには以下のような独自の構成があります:

- ユーザーが使用できるアプリとデスクトップを列挙するためのクエリを StoreFront が実行するリソースフィードのリスト。
- ストアへのアクセスで使用する Web サイトの外観。
- ユーザーがログオンするために使用する認証方法。
- NetScaler Gateway 経由の外部アクセス。

Citrix ユーザーは、ローカルにインストールされたCitrix Workspace アプリを通じて StoreFront ストアにアクセスすることも、ブラウザー内で HTML5 向け Citrix Workspace アプリを使用してアクセスすることもできます。詳しくは、「ユーザーアクセスオプション」を参照してください。

利用を開始するには、StoreFront の展開計画を立てて、システム要件を確認してから、StoreFront のインストールを行います。

新機能

次のリンクを使用して、このリリースの新機能、解決された問題、既知の問題の詳細を確認してください。

新機能

以前のリリース

以前のリリースについて詳しくは、ここを参照してください。

以前のリリースからアップグレードする手順については、「アップグレード」を参照してください。

サポートのライフサイクル

StoreFront の最新リリース（CR）および長期サービスリリース（LTSR）の製品ライフサイクル戦略は、Lifecycle Milestonesで説明しています。StoreFront のライフサイクルについてさらに詳しくは、CTX200356を参照してください。

新機能

June 6, 2024

2402 LTSR には次のリリースが含まれています。

- 2402 初期リリース

2402（初期リリース）の新機能

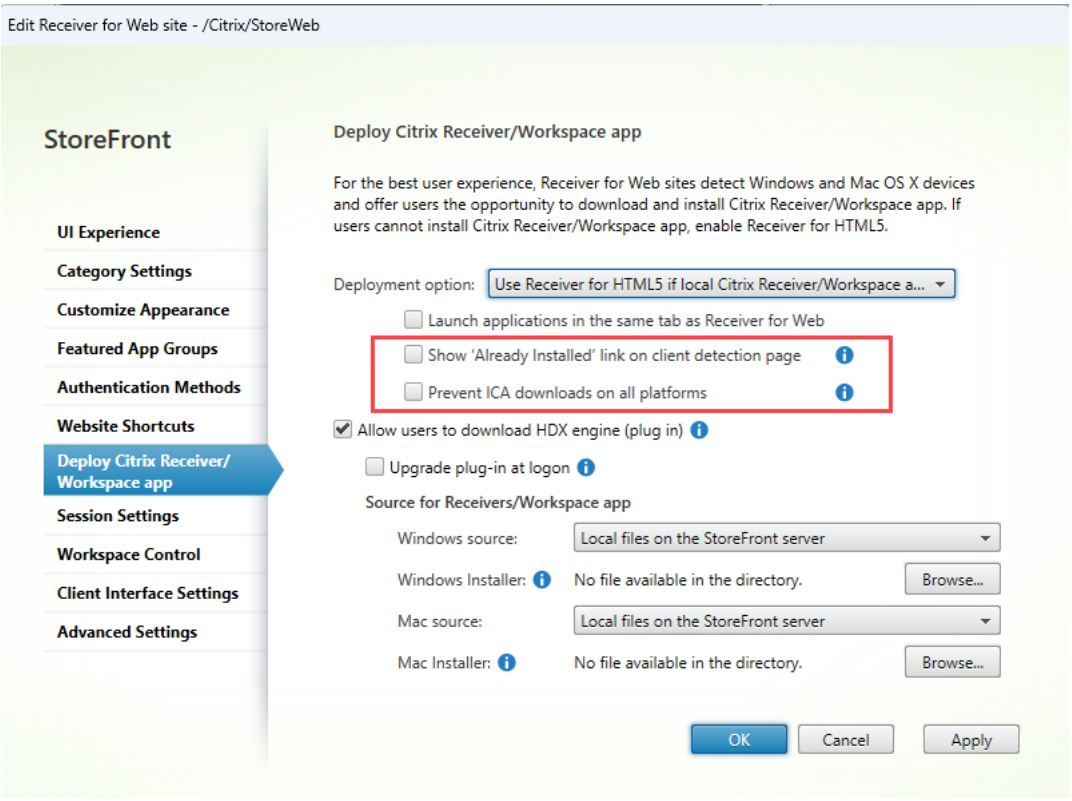
June 6, 2024

StoreFront 2402 LTSR には、StoreFront 2203 LTSR 以降の次の新機能と強化された機能が含まれています：

ハイブリッド起動中に**.ica** ファイルのダウンロードを禁止する

ローカルシステムでの `.ica`ファイルのダウンロードによって発生する可能性のあるセキュリティリスクを最小限に抑えるために、次の設定が導入されました。管理者は、ダウンロードした`.ica`ファイルの誤用を防ぐための予防策として、StoreFront 管理コンソールからこれらの設定を構成できます。
これらの設定には以下が含まれます：

- クライアント検出ページに「インストール済み」リンクを表示します
- すべてのプラットフォームで ICA のダウンロードを禁止します



詳しくは、「ICA ファイルのダウンロードを防止する」を参照してください。

すべてのストアの高度なヘルスチェックを有効にする

回復性を向上させるために、2402 へのアップグレード時にすべての既存ストアで高度なヘルスチェックが有効になります。高度なヘルスチェックにより、StoreFront は Delivery Controller の問題をより確実にチェックできます。Citrix Desktops as a Service で使用する場合、高度なヘルスチェックにより、リソースの場所にあるコネクタの追加情報が提供されます。これは停止の際に役立ちます。ユーザーがリソースを起動すると、ローカルホストキャッシュを使用してリソースを起動するための適切なコネクタが自動的に選択されます。

すべてのストアの高度なヘルスチェックを無効にする場合は、次の PowerShell スクリプトを使用できます:

```
foreach ($store in Get-STFStoreService)
{

    Set-STFStoreFarmConfiguration -StoreService $store -
       AdvancedHealthCheck $False
 }

<!--NeedCopy-->
```


Windows Server 2016 の廃止に関する情報

Windows Server 2016 への StoreFront のインストールのサポートは、将来のリリースで削除されます。サポートを継続するために、Windows Server の新しいバージョンにアップグレードすることをお勧めします。廃止されたアイテムについて詳しくは、「廃止のお知らせ」を参照してください。

StoreFront での **Citrix Secure Private Access**

新しい PowerShell コマンドまたは StoreFront 管理 UI コントロールを使用して、Citrix Secure Private Access オンプレミスサーバーに接続できるようになりました。これにより、ユーザーは StoreFront を通じて Web アプリや SaaS アプリに安全にアクセスできるようになります。詳しくは、「ストアに表示するリソースの管理」を参照してください。

FAS サーバーが利用できない場合でも **VDA** を中断なく起動

FAS サーバーが利用できない場合でも VDA の起動が成功するように StoreFront を構成できるようになりました。このような場合、エンド ユーザーは自分のユーザー名とパスワードを使用してサインインできます。以前は、FAS サーバーに到達できない場合、VDA の起動は失敗していました。
この機能はデフォルトでは無効になっており、次の Powershell コマンドを使用して有効にできます。

`Set-STFStoreLaunchOptions` 使用するパラメータ `FederatedAuthenticationServiceFailover`

必要に応じて、同じコマンドを使用してこの機能を無効にすることができます。
詳細については、「FAS」を参照してください。

ユーザーのプロセスに関するログの改善

以前はデフォルトでエラーのみがログに記録されていました。デフォルトのログレベルが変更され、警告とトレース情報が含まれるようになりました。さらに、ログメッセージも改善されました。ユーザーに関する主なプロセスの一部であるすべてのイベントがログに記録されるようになりました。デフォルトのログファイルのサイズが、サービスごとに 1GB（5*200MB）に増加しました。通常、これには 1GB（ローミングサービス用）+ ストアごとに 3GB（通常、各ストアサービスには対応する認証サービスと Receiver for Web サービスが存在するため）が必要です。十分なディスク容量があることを確認してください。詳細については、「診断ログ」を参照してください。

Citrix Workspace Web 拡張機能 **-** 一般提供

Citrix Workspace Web 拡張機能が StoreFront で使用できるようになりました。これらの Web 拡張機能は、Workspace Launcher を開いたり、`.ica`ファイルをダウンロードしたりするためのプロンプトを表示せずに、ロ

ーカル にインストールされた Citrix Workspace アプリでリソースを起動するのに役立ち、より安全で信頼性の高いエクスペリエンスが可能になります。詳細については、「Citrix Web 拡張機能」を参照してください。

StoreFront を新規インストールするたびに、Citrix Workspace Web 拡張機能の使用がデフォルトで有効になります。ただし、エンドユーザーがこの機能を使用するには、拡張機能をダウンロードする必要があります。

> 注:
>
> Citrix Workspace Web 拡張機能は、StoreFront バージョンのアップグレード中に自動的に有効になりません。アップグレード前にこの機能がオフになっていた場合、バージョンアップデート後も同じ状態のままになります。将来のリリースではすべての展開でこの機能が有効になる予定です。

既存の展開をアップグレードすると、次のコマンドを使用してこの機能を有効にできます:

```
Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension "
-IsEnabled $True
```

オンプレミスストアの新しい **UI (Technical Preview)**

新しい UI をオンプレミスストアで利用できるようになりました。この UI は、以前はクラウドストアでのみ利用可能でしたが、クラウドストアとオンプレミスストア全体で一貫した外観と操作性を実現します。

新しい UI では、次の重要な改善が行われています:

- ユーザーフレンドリーな **UI**: 視覚的な複雑さを軽減し、重要な機能に簡単にアクセスできるようにします。詳細については、「ワークスペースの視覚表示とレイアウトの改善」を参照してください。
- アクティビティマネージャー: アクティブな仮想アプリとデスクトップでの素早いアクションを簡単に実行でき、リソースを節約し、パフォーマンスを最適化します。詳細については、「アクティビティ マネージャー」を参照してください。
- アプリの分類の強化: エンドユーザーの画面サイズに応じた複数レベルのフォルダー構造。詳細については、「アプリの分類」を参照してください。
- 検索機能の向上: 新しい検索機能により、より適切かつ迅速な結果が得られます。詳細については、「検索オプション」を参照してください。

このプレビューの詳細については、「新しい UI (Tech Preview)」を参照してください。

> 注:
>
> このPodio フォームを使用して、この機能に対するフィードバックを送信できます。

HTML5 向け **Citrix Workspace** アプリ

このリリースには、HTML5 向け Citrix Workspace アプリ 2402が含まれています。

ハイブリッド起動の **App Protection**

App Protection は、キーロガーと画面キャプチャをブロックすることで、さらなるセキュリティを提供します。以前はこの機能は、Windows、Mac、Linux 向け Citrix Workspace アプリを通じてストアにアクセスするときのみ利用可能でした。Web ブラウザーでストアを表示すると、保護されたアプリが表示されませんでした。このリリースでは、ユーザーがアプリの起動に使用するために十分に新しいバージョンの Windows、Mac、または Linux 向け Citrix Workspace アプリがインストールされていることを StoreFront が検出した場合に限り、ブラウザーで表示したときに App Protection を必要とするアプリを表示するようにストア Web サイトを構成できるようになりました。

詳しくは、「App Protection」を参照してください。

デフォルトで有効になっている高度なヘルスチェック

このリリース以降、高度なヘルスチェック機能がデフォルトで新しいストアで有効になります。以前は手動で有効にする必要がありました。

Citrix DaaS と併用すると、高度なヘルスチェックにより、リソースの場所に存在するコネクタが StoreFront に認識されます。停止が発生した場合、ユーザーがリソースを起動すると、StoreFront はローカルホストキャッシュを使用してリソースを起動するための適切なコネクタを選択します。

XenApp サービスの廃止

このリリース以降、ストアに接続するための XenApp Services の URL（PNAgent とも呼ばれる）のサポートは廃止されています。将来のリリースでは削除される予定です。Citrix Workspace アプリを使用して、ストア URL からストアに接続します。

XenApp 6.5 Delivery Controller を追加する機能の削除

StoreFront 管理コンソールを使用して新しい XenApp 6.5 リソースフィードを追加することはできなくなりました。PowerShell Add-STFStoreFarmを使用して FarmType をXenAppとして指定することで、これらを追加することも可能です。たとえば、次のように設定します:

```
$store = Get-STFStoreService
Add-STFStoreFarm -StoreService $store -FarmName "XenApp" -FarmType
    XenApp -Port 80 -TransportType HTTP -Servers Xen1
<!--NeedCopy-->
```

既存の XenApp 6.5 リソースフィードは、管理コンソールを使用して変更できます。

> 注:
>
> XenApp 6.5 は Citrix ではサポートされていません。XenApp 6.5 Delivery Controller を使用する機能は、

> 将来のリリースでは削除される予定です。

Internet Explorer 11 内でリソースを開く機能の削除

Internet Explorer 11 Web ブラウザー内でリソースを開くことはできなくなりました。Internet Explorer 11 からストアにアクセスすることは引き続き可能ですが、リソースを起動できるようにするには Windows 向け Citrix Workspace アプリをインストールする必要があります。

解決された問題

以下は、バージョン 2203 CU4 以降で解決された問題の一覧です:

- StoreFront サーバーでのアプリの列挙が断続的に失敗する場合があります。[CVADHELP-23196]
- 特殊文字を含む名前は、［ホーム］タブと［設定］ドロップダウンメニューで正しく表示されない場合があります。[CVADHELP-24499]
- ユーザーが ChromeOS 上のブラウザーで初めてストアの Web サイトを開くと、ユーザーはクライアント検出を実行するように求められますが、ChromeOS 向け Citrix Workspace アプリはクライアント検出をサポートしていません。その結果、クライアントの検出が失敗し、ユーザーは続行するために［インストール済み］をクリックする必要があります。この修正により、Web サイトは ChromeOS 上のクライアント検出をスキップします。[WSP-22390]
- StoreFront ストアに接続すると、Mac 向け Citrix Workspace アプリがスリープモードから復帰した後にフリーズする場合があります。[CVADHELP-23217]
- 競合状態により、StoreFront サーバー上で Citrix Subscriptions Store Service が警告メッセージとともに予期せず終了する場合があります。[CVADHELP-23326]
- [CVADHELP-22435] ユーザーが Citrix Workspace アプリがインストールされていることを検出してから 1 年を経過すると、アプリは Citrix Workspace アプリではなくブラウザーで起動されます。
- [CVADHELP-21886] StoreFront ストアサービス API を使用してアプリを起動し、音質やプリンターの無効化などの設定を上書きすると、その設定は現在の要求だけでなく以降のすべての要求に影響を与える可能性があります。

2402 の既知の問題

June 6, 2024

2402 初期リリース

新しい既知の問題はありません。

オンプレミスストアの新しい **UI (Technical Preview)**

June 6, 2024

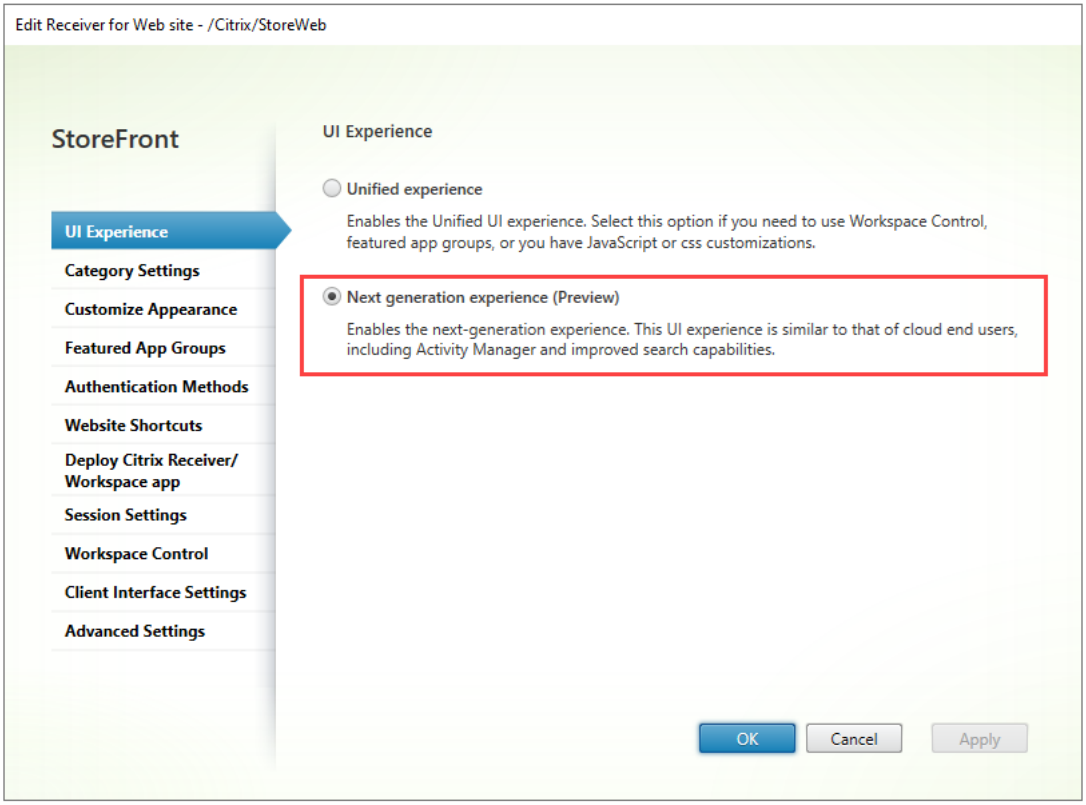
新しい UI がオンプレミスストアで利用できるようになりました。以前はクラウドストアでのみ利用可能だったこの UI により、クラウドストアとオンプレミスストア全体で一貫した外観と操作性が保証されます。

新しいユーザーインターフェイスは、Citrix アプリとデスクトップにアクセスするためのエンドユーザーエクスペリエンスを強化および簡素化するように設計されています。これにより、視覚的な複雑さが軽減され、重要な機能に簡単にアクセスできるようになり、StoreFront アプリのエクスペリエンスが向上します。仮想アプリとデスクトップのリソースの効果的な管理を容易にするアクティビティマネージャーなどの新機能をサポートします。

> 注:
>
> この記事では、現在の UI エクスペリエンスを統合 UI エクスペリエンスと呼びます。

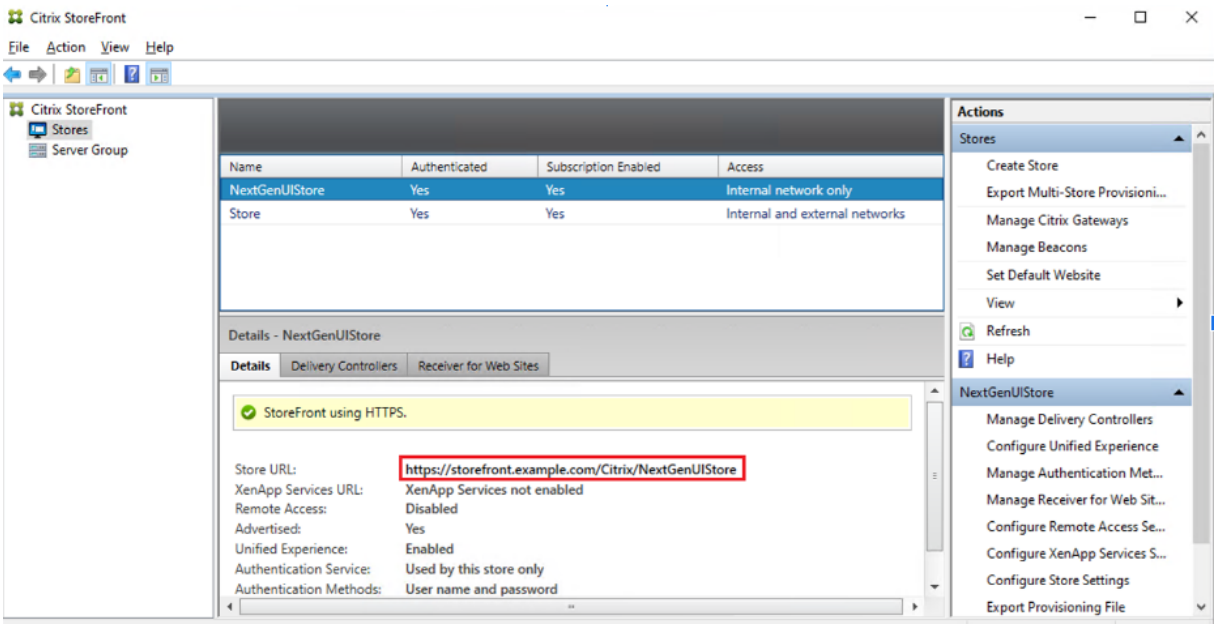
オンプレミスストアの新しい **UI** エクスペリエンスを有効にする

この機能は現在プレビュー段階にあるため、新しいストアを作成して、その特定のストアに対して新しい UI エクスペリエンスを有効にすることをお勧めします。
ストアを作成したら、[Web サイトの構成] ページで ［次世代エクスペリエンス］を選択して、新しい UI を有効にする必要があります。新しいストアで新しい UI を有効にすると、限られた数のユーザーで UI をテストするのに役立ちます。



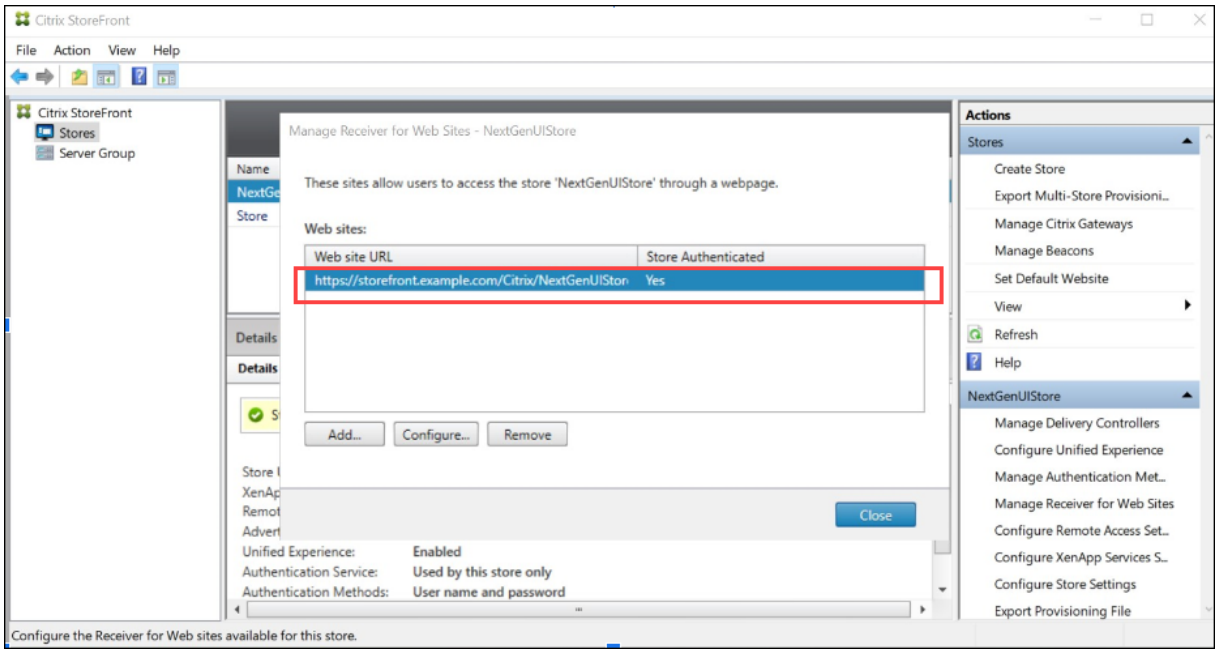
新しい UI を有効にして新しいストアを作成したら、Web サイトまたはストアのリンクをエンドユーザーと共有する必要があります。

- エンドユーザーがネイティブアプリケーションを使用している場合は、新しいストア リンクをエンドユーザーと共有する必要があります。



- エンドユーザーがブラウザーを介してサインインしている場合は、新しい Web サイトのリンクをエンドユー

ザーと共有する必要があります。



PowerShell コマンドを使用して新しい **UI** を有効にする

管理者は、次の PowerShell コマンド`Set-STFWebReceiverService`を使用して、エンド ユーザーに対して新しい UI を有効にできます。

例:

```
$rfw=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"
Set-STFWebReceiverService -WebReceiverService $rfw -WebUIExperence
    Workspace

<!--NeedCopy-->
```

テーマとロゴをカスタマイズする

新しい UI 対応ストアのテーマとロゴをカスタマイズできます。これらの設定は、[**Web** サイトの管理] の [外観のカスタマイズ] タブから管理できます。テーマとロゴの構成の詳細については、「外観のカスタマイズ」を参照してください。

主なメリット

新しい UI では、次の重要な改善が行われています:

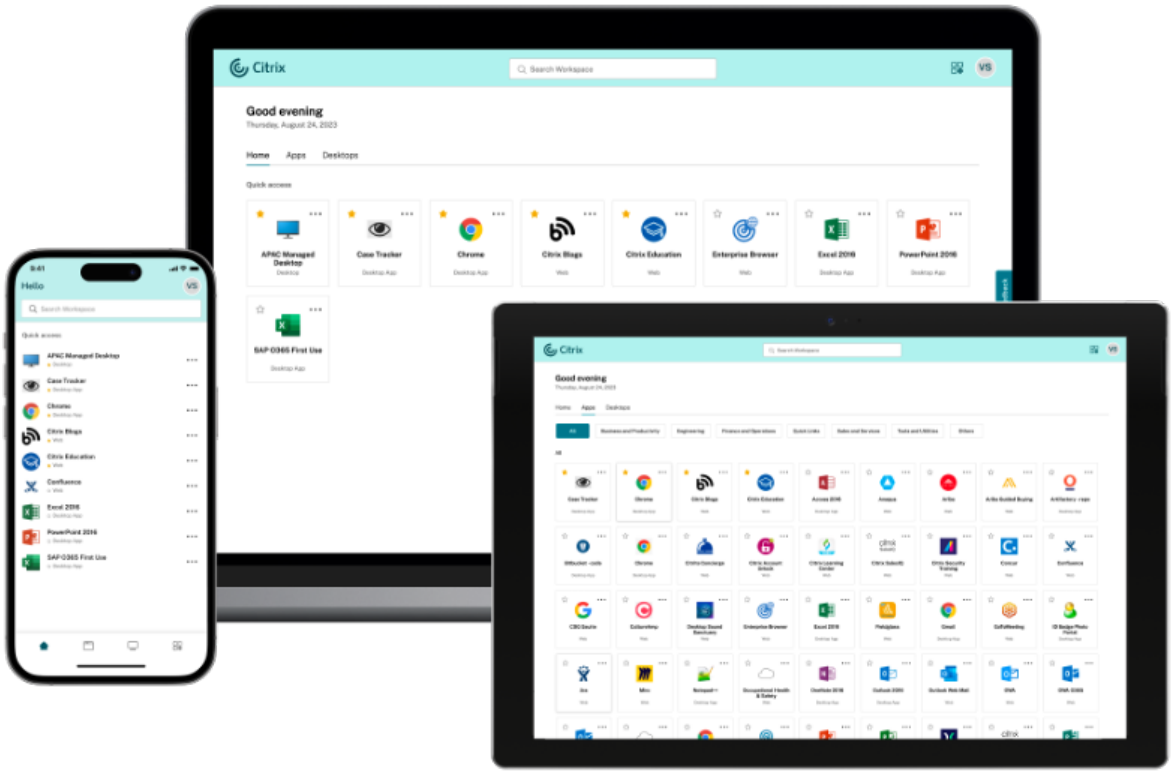
- ユーザーフレンドリーな **UI**：視覚的な複雑さを軽減し、重要な機能に簡単にアクセスできるようにします。詳細については、「ワークスペースの視覚表示とレイアウトの改善」を参照してください。
- アクティビティマネージャー：アクティブな仮想アプリとデスクトップでの素早いアクションを可能にし、リソースを節約し、パフォーマンスを最適化します。詳細については、「アクティビティ マネージャー」を参照してください。
- アプリの分類の強化：ユーザーの画面サイズに応じた複数レベルのフォルダー構造。詳細については、「アプリの分類」を参照してください。
- 検索機能の向上：新しい検索機能により、より適切かつ迅速な結果が得られます。詳細については、「検索オプション」を参照してください。

ワークスペースの視覚表示とレイアウトの改善

新しいユーザーエクスペリエンスは、直感的で簡素化されたエクスペリエンスを提供するように設計されています。アプリとデスクトップは、ナビゲーションが簡単になるように、[ホーム]、[アプリ]、[デスクトップ] ページに整理されています。お気に入りとしてマークされたアプリとデスクトップは、アクセスしやすいようにリストの先頭に配置されます。

ユーザーが所有するアプリの数が 20 未満の場合は、タブやカテゴリのないシンプルなビューに表示されます。すべてのアプリとデスクトップが同じページに表示されます。お気に入りとしてマークされたアプリはリストの先頭に配置され、その後に他のアプリがアルファベット順に配置されます。

エンドユーザーは、それぞれの星アイコンをクリックして、アプリまたはデスクトップをお気に入りとしてマークできます。同様に、それぞれの星アイコンをクリックすると、お気に入りのリストからアプリまたはデスクトップを削除できます。



ユーザーが 20 を超えるアプリを持っている場合、サインイン後に［ホーム］ページが表示されます。［ホーム］ページから、お気に入りおよび最近使用した最大 5 つのアプリとデスクトップにアクセスできます。管理者によって義務付けられたアプリとデスクトップは、星アイコンで示されます。エンドユーザーは、そのようなアプリやデスクトップをお気に入りのリストから削除できません。

管理者がホームページを有効にしていない場合は、［アプリ］ページが表示されます。このページでも、お気に入りのアプリが最初にリストされ、その後に他のすべてのアプリがアルファベット順に表示されます。管理者がアプリカテゴリを作成している場合、ユーザーはカテゴリをクリックしてアプリを見つけることができます。

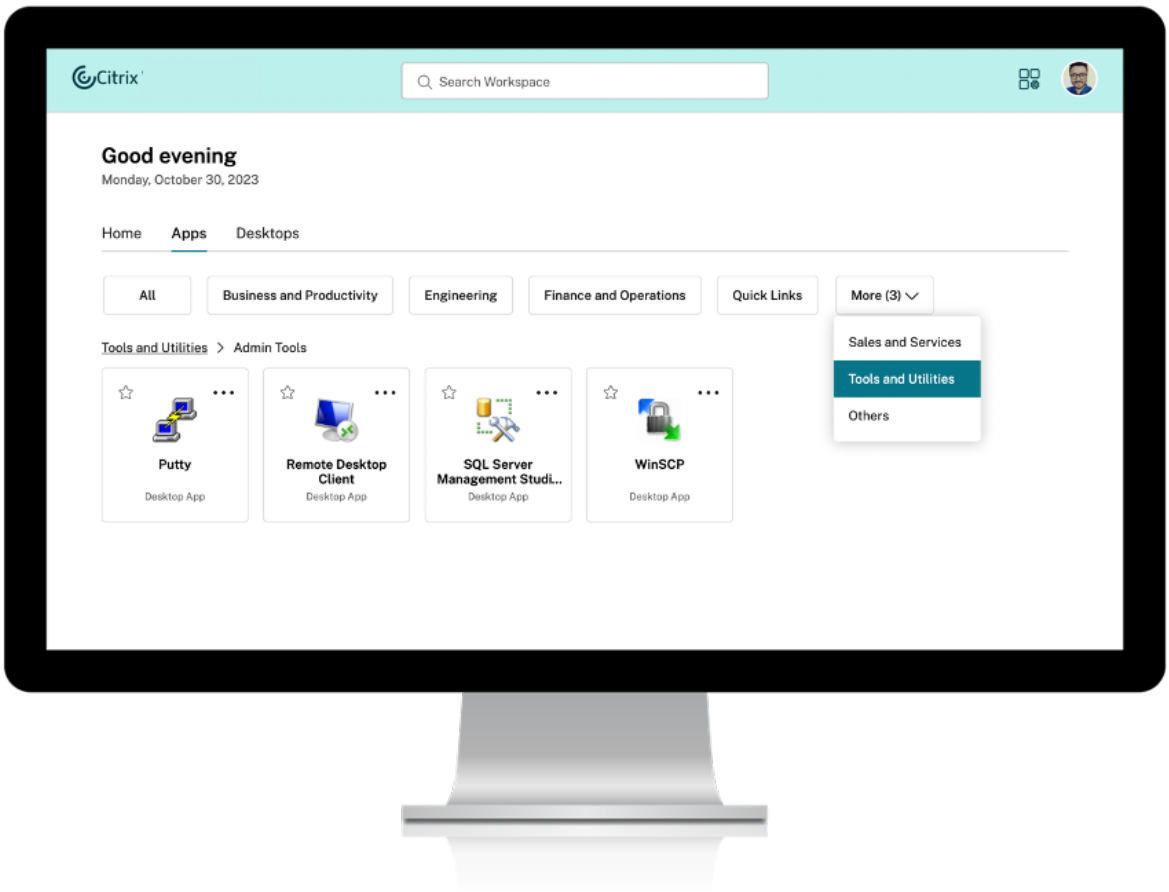
新しい **UI** でのアプリの分類

新しい UI では、エンドユーザーはアプリをカテゴリおよびサブカテゴリに分類して表示できます。サブカテゴリはフォルダー構造で表示されます。整理されたマルチレベル構造により、混乱のない、最適化されたエクスペリエンスが実現され、全体的なユーザー満足度の向上に役立ちます。フォルダーとサブフォルダーの作成の詳細については、「カテゴリ設定」を参照してください。

管理者が作成したプライマリカテゴリの数がユーザーの画面上で利用可能なスペースを超えると、ユーザーインターフェイスは画面サイズに基づいて調整され、カテゴリを ***** ［その他］ドロップダウンの下に動的に移動します。ナビゲーションのブレッドクラムがユーザーに表示されます。

モバイルプラットフォームでは、［アプリ］タブに移動し、［カテゴリ］ボックスをクリックして、使用可能なカテゴ

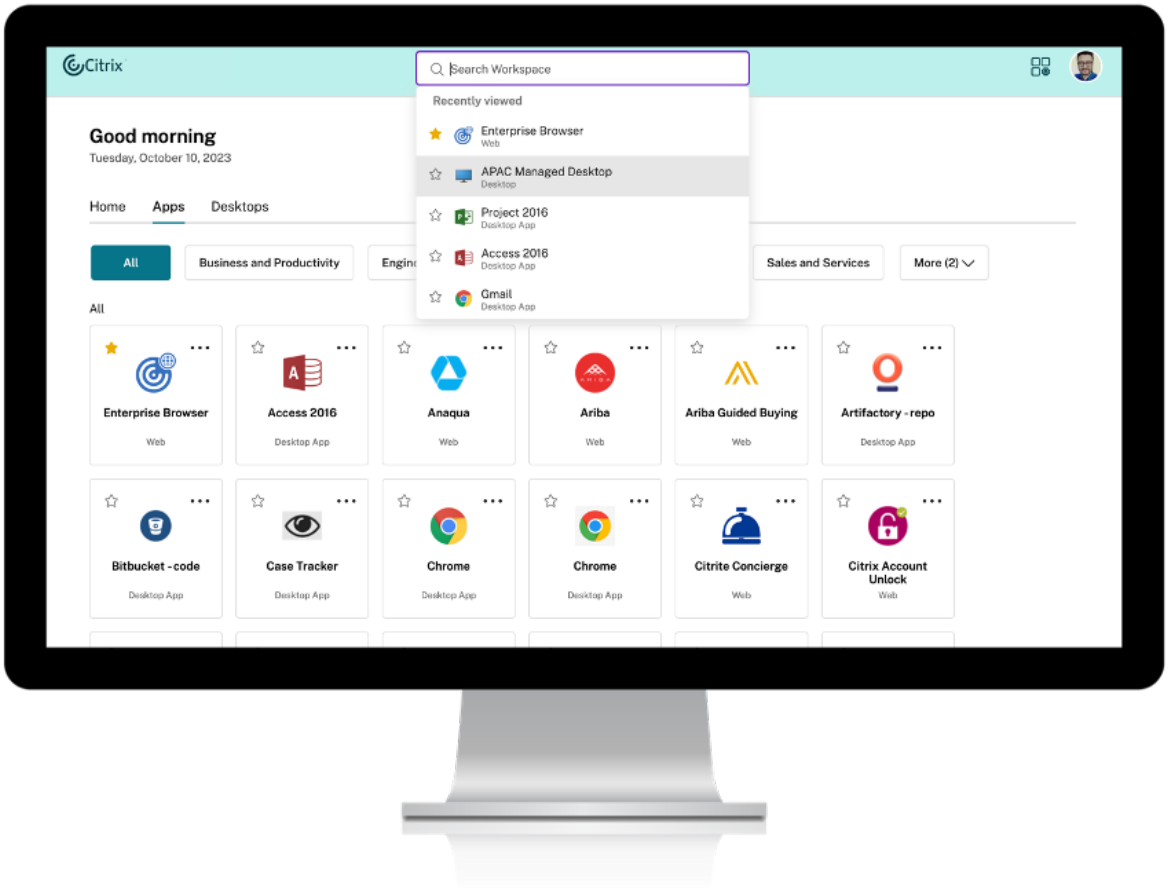
リのリストを表示します。サブカテゴリはフォルダーとして表示されます。サブフォルダーには、管理構成に応じてサブフォルダーまたはアプリが含まれる場合があります。



> 注:
>
> 統合 UI エクスペリエンスでは、アプリはフォルダーに分類されます。アプリまたはデスクトップを参照するときに、フォルダー階層がブレッドクラムとして表示されます。詳細については、「カテゴリ設定」を参照してください。

検索オプション

新しい UI の検索機能は、統合 UI よりも改善されています。新しい UI の強化された検索機能により、あいまい検索メカニズムを使用した検索エンジンからより正確な結果が得られます。検索オプションは使いやすさを考慮してツールバー内に表示され、迅速かつ直感的に検索を行うことができます。



これには次の改善が含まれます:

- デフォルトの検索では、最近使用した 5 つのアプリまたはデスクトップが表示されます
- 検索はスペルチェックで有効になり、オートコンプリート結果が表示されます
- 管理者が作成したカテゴリによる検索を実行する
- 検索結果の上部に［お気に入り］が表示されます

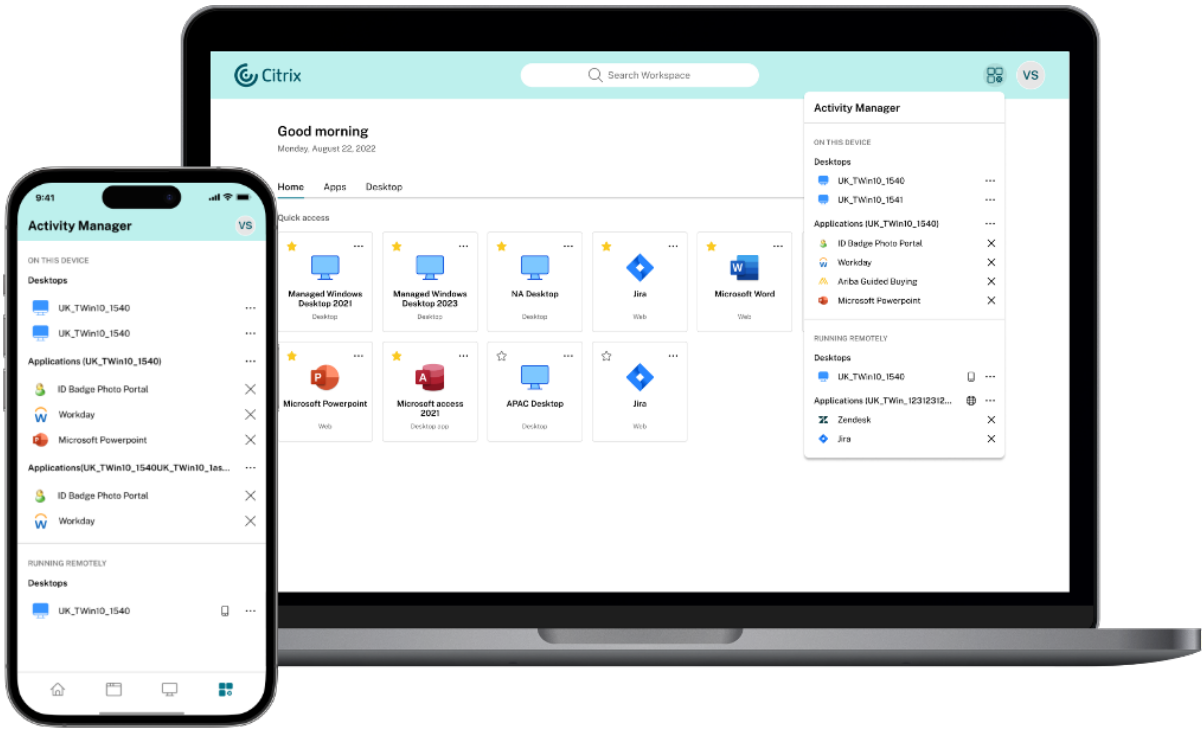
  統合 UI は基本的な検索メカニズムを展開しますが、新しい UI の検索機能ほど効果的ではない可能性があります。

アクティビティマネージャー

アクティビティマネージャーは、ユーザーが効果的にリソースを管理するための、Citrix Workspace のシンプルかつ強力な機能です。あらゆるデバイスからアクティブなアプリやデスクトップに対するすばやいアクションを容易にすることで、生産性を向上させます。ユーザーはセッションをシームレスに操作でき、不要になったセッションを終了または切断してリソースを解放し、パフォーマンスを最適化できます。

［アクティビティマネージャー］パネルには、現在のデバイスだけでなく、アクティブなセッションがあるリモートデ

バイス上の、アクティブなアプリとデスクトップの統合された一覧が表示されます。ユーザーは、デスクトップではプロファイルアイコンの横にあり、モバイルデバイスでは画面の下部にあるアクティビティマネージャーアイコンをクリックすると、この一覧を表示できます。

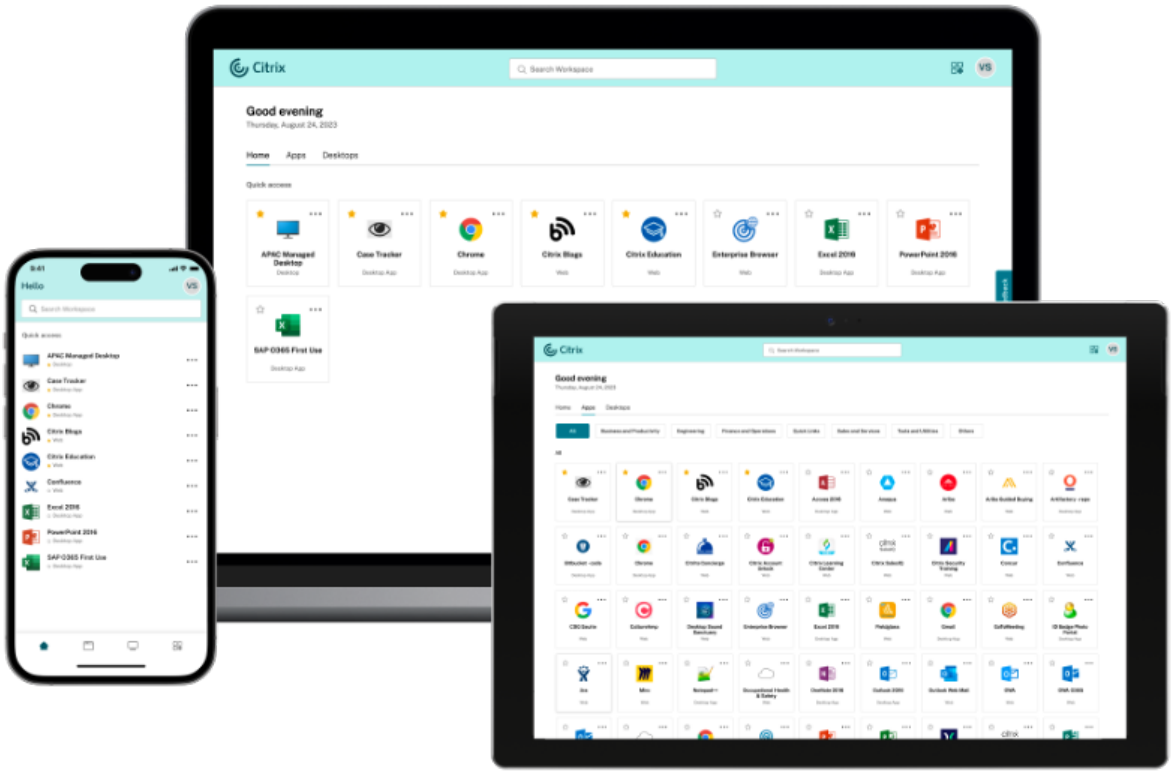


> 重要:
>
> アクティビティマネージャー機能は、新しい UI が有効になっているストアでのみ利用できます。統合 UI エクスペリエンスでは使用できません。

アクティビティマネージャーの使用

アクティブなアプリとデスクトップは、アクティビティマネージャーパネルで次のようにグループ化されます。

- このデバイスでアクティブなアプリとデスクトップは、［このデバイス上］にグループ化されます。
- 他のデバイスでアクティブなアプリとデスクトップは、［リモートで実行］にグループ化されます。

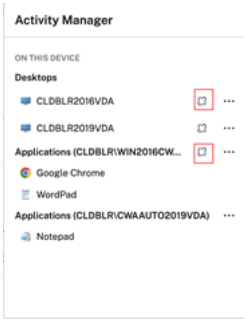


ユーザーは、それぞれの省略記号 (…) ボタンをクリックすることで、アプリまたはデスクトップ上で次のアクションを実行できます。

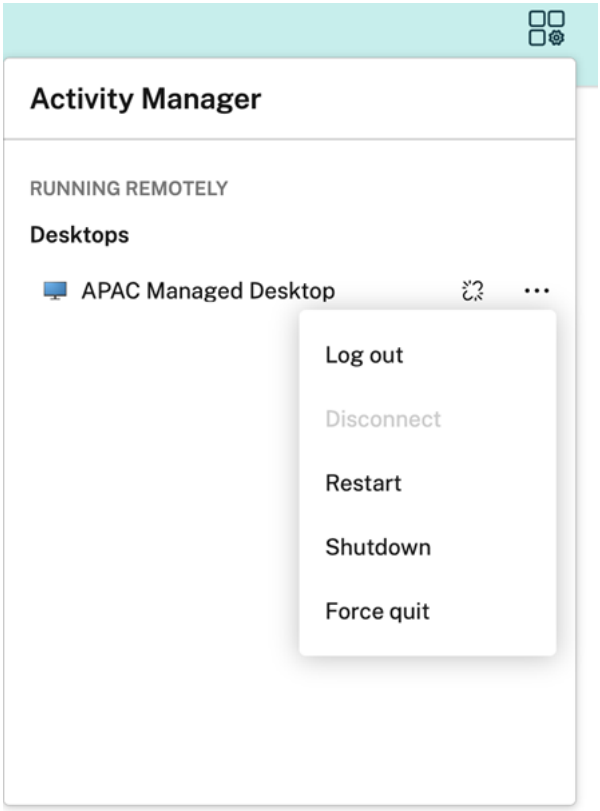
- 切断：リモートセッションは切断されますが、アプリとデスクトップはバックグラウンドでアクティブになっています。
- ログアウト：現在のセッションからログアウトされます。セッション内のすべてのアプリが閉じられ、保存されていないファイルはすべて失われます。
- シャットダウン：切断されたデスクトップを閉じます。
- 強制終了：技術的な問題が発生した場合、デスクトップの電源を切ります。
- 再起動：デスクトップをシャットダウンし、再度起動します。

切断されたアプリとデスクトップ

アクティビティマネージャーにより、エンドユーザーはローカルまたはリモートにおいて切断モードで実行されているアプリとデスクトップを表示し、それらに対するアクションを実行できるようになりました。モバイルまたはデスクトップデバイスからセッションを管理できるため、エンドユーザーは外出先でもアクションを実行できます。切断されたセッションに対してログアウトやシャットダウンなどのアクションを実行すると、リソースの使用が最適化されるので、消費電力が削減されます。



- 切断されたアプリとデスクトップは［アクティビティマネージャー］パネルに表示され、切断状態を示すアイコンで示されます。
- 切断されたアプリはそれぞれのセッションの下にグループ化され、それらのセッションには切断状態を示すアイコンが表示されます。



エンドユーザーは、切断されたデスクトップに対し、［省略記号］をクリックすることで次のアクションを実行できます：

- ログアウト：このオプションを使用すると、切断されたデスクトップからログアウトできます。セッション内のすべてのアプリが閉じられ、保存されていないファイルはすべて失われます。
- シャットダウン：このオプションを使用すると、切断されたデスクトップを閉じることができます。
- 電源オフ：技術的な問題が発生した場合に、このオプションを使用すると、切断されたデスクトップの電源を

強制的に切ることができます。
- 再起動：このオプションを使用すると、切断されたデスクトップをシャットダウンし、再度起動することができます。

切断されたセッションのアクティビティマネージャーにおける動作は、以下のようにさまざまです。

- ブラウザーを通じてサインインし、ローカル セッションから切断すると、切断されたセッションはまず ［このデバイス上］に表示されます。ただし、アクティビティマネージャーを閉じて再度開くと、切断されたセッションは ［リモートで実行］の下に移動しています。
- ネイティブデバイスにサインインしているときにローカルセッションから切断すると、切断されたセッションはリストに表示されなくなります。ただし、アクティビティマネージャーを閉じて再度開くと、切断されたセッションは ［リモートで実行］の下に移動します。

既知の制限事項

新しい UI には次の制限があります。これらの機能は、統合 UI エクスペリエンスのみで利用できます。

- 新しい UI は、JavaScript および CSS API を使用した詳細なカスタマイズをサポートしていません。
- 新しい UI は、アプリまたはデスクトップに直接アクセスする埋め込み URL ショートカットをサポートしていません。
- エンドユーザーがリモートデバイスからセッションに再度接続できるようにするワークスペースコントロール機能は、現在、新しい UI エクスペリエンスでは利用できません。
- 新しい UI ではパスワード変更機能は利用できません。
- Citrix Workspace Web 拡張機能はサポートされていません。[WSUI-8503]
- Web ブラウザーを使用して接続する場合、直接 SAML 認証を有効にすることはできません。SAML 認証は、Citrix Gateway で使用できます。

既知の問題

- 既存のストアの UI エクスペリエンスを変更すると、ローカルにインストールされた Citrix Workspace アプリを通じて接続しているユーザーは更新されません。ストアを削除し、アプリに再度追加する必要があります。[WSP-21493]
- ログアウト、切断などのアクティビティマネージャーの操作は、App Protection ポリシーが有効になっているアプリケーションではサポートされません。[WSP-21324]
- iOS 向け Citrix Workspace アプリでは、ユーザーのイニシャルがアバターに表示されません。[WSUI-8482]
- Mac Netscaler ストア向け Citrix Workspace アプリでは、［サインインに戻る］オプションが機能しない場合があります。[RFMAC-15496]
- iOS Netscaler ストア向け Citrix Workspace アプリでは、クライアントレス VPN（cVPN）ポリシーで Secure Private Access が有効になっている場合、ユーザーが新しい UI にサインインできない可能性があります。[RFIOS-13733]

インストール、セットアップ、アップグレードおよびアンインストール

June 6, 2024

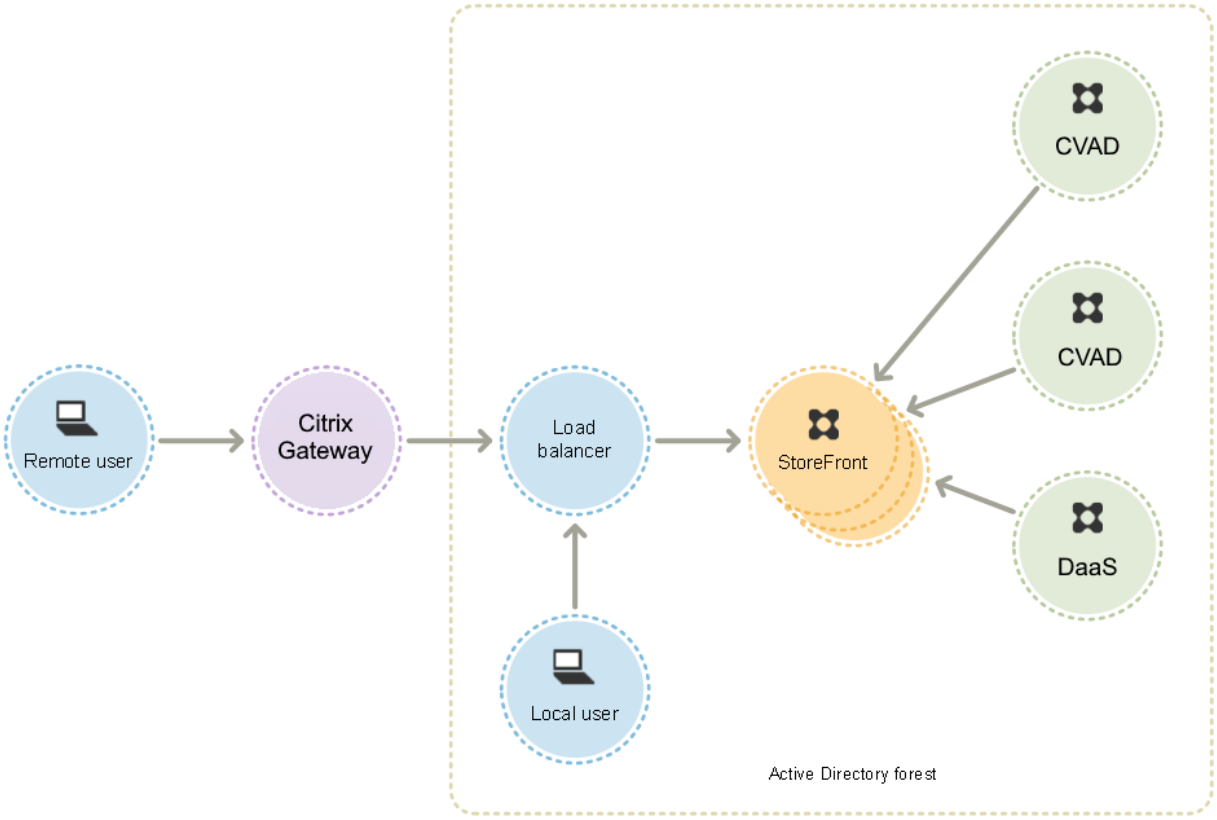
タスク	詳細
StoreFront の展開計画	StoreFront 環境に関係するコンポーネントの概要
ユーザーアクセスのオプション	ユーザーがストアにアクセスできる方法の概要
システム要件	StoreFront をインストールするための前提条件を満たしていることを確認する
StoreFront のインストール	新しいサーバーへの StoreFront のインストール
HTTPS を使用した StoreFront のセキュリティ	HTTPS の使用によるクライアントの StoreFront へのアクセスの暗号化
StoreFront 展開環境のセキュリティ	セキュリティ強化のために StoreFront を構成
新しい展開環境の作成	新しいストアを使用して新しい StoreFront サーバーを構成する。
既存のサーバーグループへの参加	新しい StoreFront サーバーを既存のサーバーグループに参加するように構成する。
StoreFront のアップグレード	古いバージョンを実行している StoreFront サーバーのアップグレード
CEIP	カスタマーエクスペリエンス向上プログラム（CEIP）へのオプトインまたはオプトアウト
Citrix Analytics Service	Citrix Analytics Service にデータを送信する StoreFront の構成
StoreFront のアンインストール	サーバーからの StoreFront の削除
サーバーを出荷時のデフォルト設定にリセット	StoreFront 設定をすべてクリアして再構成できるようにする。

StoreFront の展開計画

June 6, 2024

Citrix Virtual Apps and Desktops 展開環境に StoreFront を統合して、ユーザーにデスクトップおよびアプリケーションに対する単一のセルフサービスアクセスポイントを提供できます。

次の図は、一般的な StoreFront 展開の例を示しています。



Active Directory

StoreFront は、ユーザーの認証、グループメンバーシップおよびその他の詳細の検索、および StoreFront サーバー間のデータの同期に Active Directory を使用します。

単一サーバーの展開では、ドメインに参加していないサーバーに StoreFront をインストールできます（ただし利用できない機能があります）。それ以外の場合、各 StoreFront サーバーは、Citrix Virtual Apps and Desktops サイト/ファームに対する認証の委任を有効にしない限り、ユーザーアカウントが属している Active Directory ドメイン、またはそのドメインと信頼関係があるドメインに属している必要があります。同一デリバリーグループで使用するすべての StoreFront サーバーが同じドメインに属している必要があります。

StoreFront サーバーグループ

StoreFront では、単一サーバーの展開環境を構成することも、StoreFront サーバーグループと呼ばれる複数サーバーの展開環境を構成することもできます。サーバーグループでは、処理能力だけでなく可用性も向上します。StoreFront により、構成情報やユーザーのアプリケーションサブスクリプションの詳細がサーバーグループ内のすべてのサーバー上に格納され、複製されます。このため、何らかの理由でいずれかの StoreFront サーバーが停止しても、ユーザーはほかのサーバーを使用してストアにアクセスできます。停止したサーバーが動作を再開してサーバーグループに再接続すると、構成およびサブスクリプションのデータが自動的に更新されます。サブスクリプションデータは、サーバーがオンラインに復帰したときに更新されますが、オフライン中の更新が反映されていない場合は、

管理者が構成の変更を反映させる必要があります。ハードウェア障害などによりサーバーの交換が必要な場合でも、新しいサーバーに StoreFront をインストールして既存のサーバーグループに追加するだけです。これにより、新しいサーバーが自動的に構成され、最新のアプリケーションサブスクリプションデータが同期されます。

Citrix では、サーバーグループ内に配置するサーバーを最大 6 台にすることをお勧めします。サーバーが 6 台を超える場合、データ同期のオーバーヘッドがサーバーを追加するメリットを上回り、パフォーマンスが低下します。

StoreFront サーバーグループの展開は、サーバーグループ内のサーバー間のリンクの遅延が 40 ミリ秒未満（サブスクリプションが無効の場合）または 3 ミリ秒未満（サブスクリプションが有効の場合）のみの場合にサポートされます。理想的には、サーバーグループ内のすべてのサーバーは同じ場所（データセンター、アベイラビリティゾーン）に存在する必要がありますが、グループ内のサーバー間のリンクがこれらの遅延基準を満たしていれば、サーバーグループは同じリージョン内の場所に分散できます。たとえば、1 つのクラウドリージョン内または大都市圏データセンター間のアベイラビリティゾーンにまたがるサーバーグループなどがあります。ゾーン間の遅延はクラウドプロバイダーによって異なることに注意してください。複数の場所にまたがる障害回復構成は Citrix ではお勧めしませんが、高可用性に適している場合もあります。

負荷分散

StoreFront サーバーグループ内の複数のサーバーの場合は、外部の負荷分散を構成する必要があります。この場合、NetScaler ADC など、組み込みの監視機能やセッションパーシステンス機能を持つロードバランサーを使用してください。NetScaler ADC を使用した負荷分散について詳しくは、「負荷分散」を参照してください。

リモートアクセス用の **Citrix Gateway**

社内ネットワーク外からの StoreFront へのアクセスを有効にする場合、安全な接続をリモートユーザーに提供するには Citrix Gateway が必要です。社内ネットワークの外に Citrix Gateway を配置して、ファイアウォールで公共のネットワークと内部ネットワークの両方からその Citrix Gateway を分離します。Citrix Gateway が、StoreFront サーバーを含んでいる Active Directory フォレストにアクセスできることを確認してください。

グローバルサーバーのロードバランサー

大規模な Citrix 展開では、複数のデータセンターに StoreFront および NetScaler の展開がある可能性があります。グローバルサーバー負荷分散（GSLB）を使用すると、リージョンの 1 つにおけるゲートウェイの特定の URL に GSLB がリダイレクトする単一のグローバル URL を構成できます。通常、GSLB は、往復時間（RTT）または静的近接度などの負荷分散アルゴリズムに基づいて最も近いゲートウェイを選択します。

たとえば、次の 3 つのリージョンのゲートウェイがあるとします：

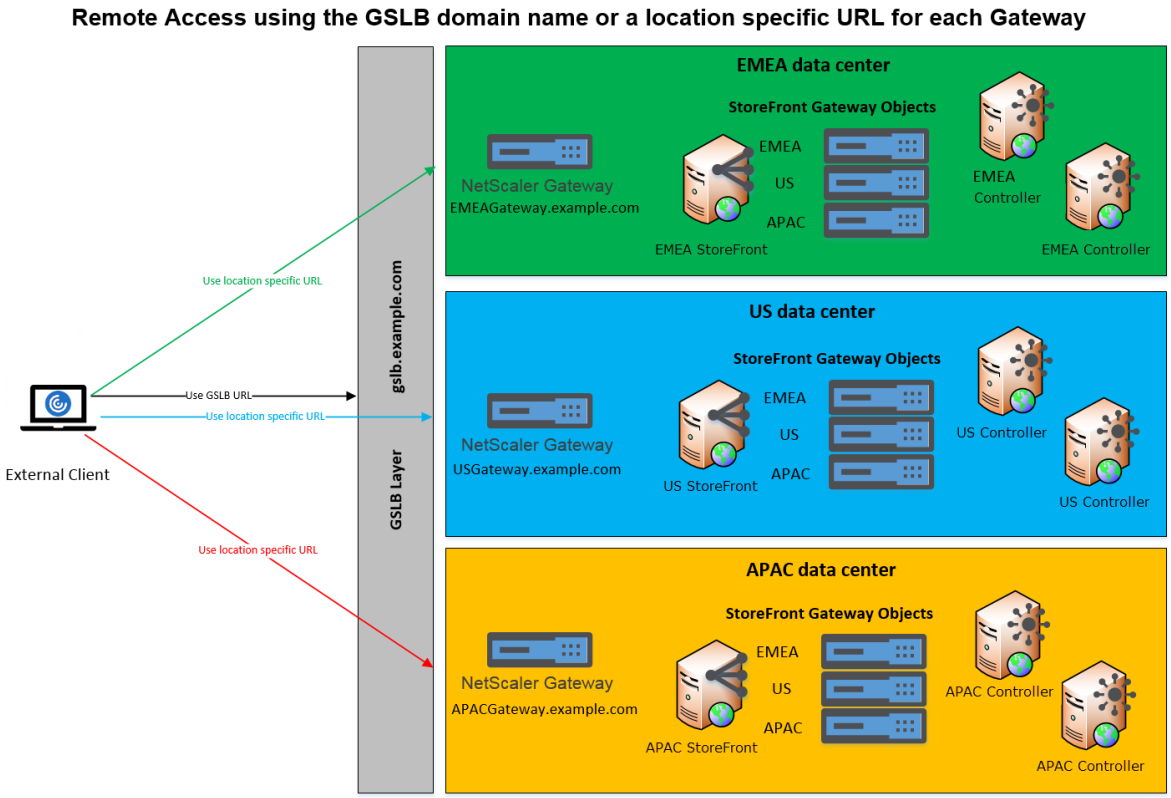
`emeagateway.example.com` - ヨーロッパのゲートウェイ

`usgateway.example.com` - 米国のゲートウェイ

`apacgateway.example.com` - アジア太平洋のゲートウェイ

使用する GSLB

`gslb.example.com`



GSLB を構成する前に、配置済みのサーバー証明書と組織での DNS 解決の実行方法について確認してください。Citrix Gateway および StoreFront の展開環境で使用する URL はすべて、サーバー証明書に記載されている必要があります。

StoreFront には、サーバーグループ間で構成を同期するためのメカニズムが組み込まれていません。代わりに、ユーザーがどのサーバーグループに接続しても一貫したエクスペリエンスが得られるように、各 StoreFront サーバーグループが同じ方法で構成されるように、管理者が設定することになります。

StoreFront は、サーバーグループ間で定期的にサブスクリプション（お気に入り）を同期できます。「サブスクリプションの同期」を参照してください。

ユーザーアクセス

「ユーザーアクセスのオプション」を参照してください。

ユーザーアクセスのオプション

June 6, 2024

ユーザーは、以下の 3 つの方法で StoreFront ストアにアクセスできます。

- ローカルにインストールされた Citrix Workspace アプリ - 適切なバージョンの Citrix Workspace アプリのユーザーは、Citrix Workspace アプリのユーザーインターフェイスから StoreFront ストアにアクセスできます。これにより、最良のユーザーエクスペリエンスと多くの機能が提供されます。
- HTML5 向け Citrix Workspace アプリ - 適切なバージョンの Web ブラウザーのユーザーは、ストアの Web サイトから StoreFront ストアにアクセスすることができます。デフォルトでは、デスクトップとアプリケーションにアクセスするために、ハイブリッド起動と呼ばれる適切なバージョンの Citrix Workspace アプリも必要です。ただし、Citrix Workspace アプリをインストールしなくてもブラウザーを通じてユーザーがリソースにアクセスできるように Web サイトを構成できます。
- XenApp Services の URL - アップグレードできない従来の Citrix クライアントを使用しているユーザーは、ストアの XenApp Services URL を使用してストアにアクセスできます。デフォルトでは、新しいストアを作成するときに、XenApp Services サイトの URL が有効になります。

ローカルにインストールされた **Citrix Workspace** アプリ

ローカルにインストールされたCitrix Workspace アプリからストアにアクセスすると、最良のユーザーエクスペリエンスが提供されます。この方法でストアにアクセスできる Citrix Workspace アプリのバージョンについては、「システム要件」を参照してください。

Citrix Workspace アプリでは、ビーコンポイントとして内部 URL および外部 URL を使用します。これらのビーコンポイントに Citrix Workspace アプリでアクセスできるかどうかにより、ユーザーがローカルに接続されているのかパブリックネットワークに接続されているのかが識別されます。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバーがそのユーザーの位置情報に基づいて適切な接続詳細を Citrix Workspace アプリに返します。これにより、Citrix Workspace アプリでは、ユーザーがデスクトップまたはアプリケーションにアクセスしたときに再ログオンする必要がなくなります。詳しくは、「ビーコンポイントの構成」を参照してください。

Workspace アプリへのストアの追加

Citrix Workspace アプリをインストールしたら、デスクトップやアプリケーションのストアに接続するための構成を行う必要があります。管理者は、次のいずれかの方法を使用してユーザーによる構成操作を簡略化できます。

> 重要:
>
> デフォルトでは、Citrix Workspace アプリはストアへの接続に HTTPS を必要とします。StoreFront が HTTPS 用に構成されていない場合、Citrix Receiver で HTTP 接続が使用されるようにユーザーが構成を変

> 更する必要があります。実稼働環境では、StoreFront へのすべてのユーザー接続が保護されるようにしてください。詳しくは、Windows 向け Citrix Workspace アプリのドキュメントの「ストア構成パラメーター」を参照してください。

手動構成　ユーザーは、Citrix Workspace アプリにストア URL を入力して Citrix Workspace アプリを自分のストアに接続できます。詳しくは、Citrix Workspace アプリのドキュメントを参照してください。

プロビジョニングファイル　管理者は、ストアへの接続情報が定義されたプロビジョニングファイルをユーザーに提供します。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、ストアのアカウントが自動的に構成されます。デフォルトでは、Web サイトがユーザーに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を提供します。管理者は、使用する各ストアの Web サイトからプロビジョニングファイルをダウンロードするようユーザーに指示します。また、ユーザーの設定をより詳細に管理するには、Citrix StoreFront 管理コンソールで特定のストアの接続情報を定義したプロビジョニングファイルを生成できます。その後で、それらのファイルを適切なユーザーに配布します。詳しくは、「ユーザーに対するストアプロビジョニングファイルのエクスポート」を参照してください。

セットアップ **URL** の自動生成　macOS を実行しているユーザーのために、Mac 向け Citrix Workspace アプリの Setup URL Generator を使ってストアの接続情報を含んでいるセットアップ URL を生成できます。ユーザーが Citrix Workspace アプリをインストールした後で、管理者から提供された URL をクリックするとストアのアカウントが自動的に構成されます。管理者は、Citrix Receiver for Mac Setup URL Generator で展開環境の詳細を入力して URL を生成し、その URL をユーザーに配布します。

メールアドレスによるアカウント検出　メールアドレスによるアカウント検出では、ストアへのアクセス情報を知っている必要はなく、代わりに Citrix Workspace アプリの初回構成時に自分のメールアドレスを入力します。この設定方法について詳しくは、「メールアドレスによるアカウント検出」を参照してください。

Global App Config Service

Global App Config Service を使用して、StoreFront のストア用に Citrix Workspace アプリを構成します。「オンプレミスストアの設定の構成」を参照してください。

HTML5 向け Citrix Workspace アプリ

ローカルにインストールされた Workspace アプリを使用する代わりに、HTML5 向け Workspace アプリを使用して、Web ブラウザーを通じてストアにアクセスできます。ユーザーがリソースを起動する場合、2 つの方法があります。

1. リソースがローカルにインストールされた Citrix Workspace アプリ内で起動します。これはハイブリッド起動と呼ばれます。オペレーティングシステムの完全な統合を活用できるため、ユーザーに最良のエクスペリエンスが提供されます。詳しくは、「ハイブリッド起動」を参照してください
2. リソースがブラウザー内で起動します。ユーザーはソフトウェアをローカルにインストールしなくてもリソースにアクセスできるようになります。

デフォルトの構成では、ハイブリッド起動のために Citrix Workspace アプリがローカルにインストールされていることが必要です。常にブラウザーでリソースを起動するか、ユーザーが起動方法を選択できるように構成を変更できます。「Workspace アプリの展開」を参照してください。

管理者が ［ローカル **Receiver** が使用できない場合 **Receiver for HTML5** を使用］を選択した場合、ユーザーが初めてブラウザーでストア Web サイトを開いたときに、［簡易バージョンを使用］をクリックして Web ブラウザー内でリソースを起動するオプションが表示されます。

ブラウザーでリソースを開くための要件

デフォルトでは、内部ネットワーク上のユーザーが Citrix Virtual Apps and Desktops で提供されるリソースに HTML5 向け Citrix Workspace アプリでアクセスすることはできません。HTML5 向け Citrix Workspace アプリでデスクトップやアプリケーションへのローカルアクセスを有効にするには、Citrix Virtual Apps and Desktops のサーバー側でポリシーの［ICA WebSockets 接続］を有効にします。Citrix Virtual Apps and Desktops は、HTML5 向け Citrix Workspace アプリへの接続にポート 8008 を使用します。ファイアウォールやほかのネットワークデバイスで、このポートへのアクセスが許可されることを確認してください。詳しくは、「WebSocket のポリシー設定」を参照してください。

Citrix Virtual Apps and Desktops リソースの起動を成功させるために、アプリとデスクトップをホストする VDA への TLS 接続を構成します。Citrix Gateway を介したリモート接続では、VDA への TLS 接続を設定せずに、HTML5 向け Citrix Workspace アプリを使用してリソースを起動できます。

ハイブリッド起動

ユーザーが最初にブラウザーを通じて HTML5 向け Citrix Workspace を開き、ローカルにインストールされた Citrix Workspace アプリ内でアプリを起動する場合、これはハイブリッド起動と呼ばれます。Web サイトがローカルにインストールされた Workspace アプリと通信してリソースを起動するには、さまざまな方法があります。

Citrix Workspace Launcher

サポートされているオペレーティングシステムとブラウザーを使用してユーザーが初めて StoreFront Web サイトにアクセスすると、HTML5 向け Citrix Workspace アプリは Citrix Workspace Launcher の起動を試みます。サポートされているバージョンの Citrix Workspace アプリがインストールされている場合、アプリは StoreFront に

通知します。HTML5 向け Citrix Workspace アプリはこれを記憶し、アプリを起動するときに Citrix Workspace Launcher を使用します。

ストアの Web サイトは、次のブラウザーを使用して Windows、Mac、および Linux で Citrix Workspace Launcher を呼び出します:

- Firefox 52 以降
- Chrome 42 以降
- Safari 12 以降
- Edge 25 以降

Citrix Workspace Launcher には、次の最小バージョンの Citrix Receiver または Citrix Workspace アプリが必要です。

- Receiver for Windows 4.3 以降
- Receiver for Mac 12.0 以降
- Linux 向け Workspace アプリ 2003 以降

Workspace アプリランチャーが使用できない場合、またはユーザーが Workspace アプリランチャーを開くことを許可していない場合、ローカルにインストールされた Citrix Workspace アプリを検出できません。ユーザーには、再試行するか、[インストール済み] をクリックするオプションがあり、その場合は.ica ファイルを使用してアプリを起動できます。ユーザーは、[設定] 画面に移動して [**Citrix Workspace** アプリを変更] をクリックすることで、後で再試行できます。

グローバルサーバー負荷分散の背後で複数のアクティブな StoreFront サーバーグループを使用している場合、Citrix Workspace Launcher が断続的に失敗する可能性があります。これを回避するには、クライアント検出プロセスの存続期間中、ユーザー Web セッションが 1 つの StoreFront サーバーグループに保持されるようにグローバルサーバー負荷分散を構成する必要があります。CTX460312を参照してください。または、Citrix Workspace Web 拡張機能を展開します。

Citrix Gateway 経由で Web サイトに接続する場合、Citrix Workspace Launcher は Gateway の HDX ルーティングを使用して、Citrix Workspace アプリからの要求を StoreFront サーバーにプロキシします。Gateway で (HDX ルーティングではなく) [認証のみ] が構成されている場合、Citrix Workspace Launcher は機能しません。HDX ルーティングを有効にするか、Citrix Workspace Web 拡張機能を展開します。

Citrix Workspace Web 拡張機能

Citrix Workspace Web 拡張機能は、ローカルにインストールされた Citrix Workspace アプリを検出し、仮想アプリとデスクトップを起動する際のユーザーエクスペリエンスを向上させるために一般的に使用される Web ブラウザーの拡張機能です。Citrix Workspace Launcher と比べると、これによって優れたユーザーエクスペリエンスが提供され、グローバルサーバー負荷分散の問題が回避されます。

ブラウザー拡張機能ベースのクライアント検出を有効にするには、次の手順を実行します:

- StoreFront サーバーでこの機能を有効にします。
- ブラウザー拡張機能をクライアントデバイスに展開します。
- Windows 2303、Mac 2304、または Linux 2302 以降用の Citrix Workspace アプリを展開します。

サポートされているプラットフォームでユーザーがストア Web サイトに初めてアクセスすると、ローカルにインストールされている Workspace アプリを検出するように求められます。まず Web 拡張機能の使用を試し、これが失敗した場合は、Citrix Workspace Launcher を試します。Workspace アプリの検出を既に完了している既存ユーザーは、［アカウント設定］に移動し、［**Citrix Workspace** アプリを変更］を クリックして Workspace アプリを再検出できます。

> 重要
>
> この機能は、新しいインストールでデフォルトで有効になっています。ただし、以前のバージョンからアップグレードする場合は、この機能を手動で有効にする必要があります。管理者は、StoreFront サーバーで次の PowerShell スクリプトを使用して、この機能を有効にできます: `Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension" -IsEnabled $True`。

Internet Explorer

ユーザーが Internet Explorer でストアの Web サイトを初めて開くと、Internet Explorer 用 Citrix ICA クライアントアドオンを含む Citrix Workspace アプリをインストールするよう求められます。プラグインがインストールされると、ローカルにインストールされた Citrix Workspace アプリを通じてアプリやデスクトップを起動するために使用されます。

ICA ファイルのダウンロード

HTML5 向け Citrix Workspace アプリがローカルにインストールされた Citrix Workspace アプリを他の方法で検出できない場合、ユーザーがアプリまたはデスクトップを起動すると、.ica ファイルがダウンロードされます。ユーザーは、ローカルにインストールされた Citrix Workspace アプリを使用してこのファイルを開くことができます。

リソースのショートカット

ストアで利用可能なデスクトップおよびアプリケーションへのアクセスを提供する URL を生成できます。生成した URL を内部ネットワーク上でホストされている Web サイトに埋め込んで、ユーザーがすばやくリソースにアクセスできるようにします。ユーザーがリンクをクリックすると、ストアの Web サイトにリダイレクトされます。ここで、ユーザーが Web サイトにログオンしていない場合はログオンします。ストアの Web サイトでは、リソースが自動的に起動します。リソースのショートカットの生成について詳しくは、「Web サイトのショートカット」を参照してください。

アプリケーションのショートカットを生成するときは、ストアで配信されているアプリケーションの名前が重複していないことを確認してください。ショートカットでは、同じ名前を持つアプリケーションの複数のインスタンスを区

別できません。同様に、単一のデスクトップグループの複数のデスクトップインスタンスをストアで配信する場合、インスタンスごとに異なるショートカットを作成することはできません。ショートカットでは、コマンドラインパラメーターをアプリケーションに渡すことはできません。

アプリケーションのショートカットを生成するには、そのショートカットをホストする内部 Web サイトの URL を StoreFront で一覧に追加します。ユーザーが Web サイト上のショートカットをクリックすると、StoreFront はこの一覧を照会し、要求が信頼できる Web サイトからのものであるかどうか確認します。

ユーザーインターフェイスのカスタマイズ

Citrix StoreFront では、ユーザーインターフェイスをカスタマイズできます。これらは、Citrix Workspace アプリからストアにアクセスする場合でも、Web ブラウザーからストアにアクセスする場合でも適用されます。表示される文字列、カスケーディングスタイルシート、および JavaScript ファイルを編集できます。また、ログオン前やログオフ後にカスタムの画面を表示したり、言語パックを追加したりすることもできます。詳しくは、「外観のカスタマイズ」を参照してください。

XenApp Services サイトの URL

> 注:
>
> XenApp Services（PNAgent とも呼ばれる）は、廃止されました。Citrix Workspace アプリを使用して、ストア URL を使用して StoreFront に接続することをお勧めします。

アップグレードできない古いバージョンの Citrix クライアントのユーザーは、クライアントを構成するときにストアの XenApp Services サイトの URL を指定することにより、ストアにアクセスできるようになります。また、管理者は、ドメインに参加しているデスクトップアプライアンスのユーザー、および Citrix Desktop Lock を実行している再目的化された PC のユーザーが XenApp Services サイト経由でストアにアクセスできるように構成することもできます。ドメインに参加しているデバイスとは、StoreFront サーバーを含んでいる Active Directory フォレスト内のドメインに属しているデバイスを意味します。

StoreFront では、Citrix Workspace アプリから XenApp Services サイトへの近接カードを使ったパススルー認証がサポートされます。Citrix Fast Connect API を使用する Citrix Ready パートナー製品では、Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリから XenApp Services サイトを介して効率的にストアにログオンできます。ユーザーは、近接カードを使ってワークステーションにログオンし、Citrix Virtual Apps and Desktops から提供されるデスクトップやアプリケーションに迅速に接続できます。詳しくは、最新のWindows 向け Citrix Workspace アプリのドキュメントを参照してください。

デフォルトでは、管理者が新しいストアを作成するときに、そのストアの XenApp Services URL が有効になります。XenApp Services サイトの URL は、http[s]://serveraddress/Citrix/storename/PNAgent/config.xml の形式です。ここで、<serveraddress> は StoreFront 展開環境のサーバーまたは負荷分散環境の完全修飾ドメイン名で、<storename> はストアの作成時に指定した名前です。これにより、PNAgent プロトコルのみを使用できる Citrix Workspace アプリが StoreFront に接続できます。XenApp Services URL を経由してストアにアクセスできるクライアントについては、「ユーザーデバイスの要件」を参照してください。

重要な注意事項

XenApp Services サイトの URL は、Citrix Workspace アプリにアップグレードできず、代替のアクセス方法を使用できないユーザーをサポートするために使用されます。以下の制限事項を考慮して、XenApp Services サイトでユーザーにストアへのアクセスを提供するかどうかを決定してください。

- ストアの XenApp Services URL は変更できません。
- 構成ファイル config.xml を編集して XenApp Services URL 設定を変更することはできません。
- XenApp Services サイトでは、指定ユーザー認証、ドメインパススルー認証、スマートカード認証、スマートカードパススルー認証がサポートされます。デフォルトでは、指定ユーザー認証が有効になります。各 XenApp Services サイトに構成できる認証方法と各ストアで使用できる XenApp Services サイトは、それぞれ 1 つだけです。複数の認証方法を有効にするには、個別のストアを作成して、それらの XenApp Services サイトで異なる認証方法を有効にします。この場合、どのストアにアクセスすべきかをユーザーに通知してください。詳しくは、「XML サービスベースの認証」を参照してください。
- XenApp Services サイトでは、ワークスペースコントロールがデフォルトで有効になっており、構成を変更したり無効にしたりすることはできません。
- ユーザーのパスワード変更要求は、StoreFront の認証サービスを介して、ストアにデスクトップとアプリケーションを提供する Citrix Virtual Apps and Desktops サーバーからドメインコントローラーに直接送信されます。

システム要件

June 6, 2024

StoreFront をインストールする前に、「StoreFront の展開計画」を参照してください。

StoreFront サーバーの要件

ソフトウェア

Citrix 社では、以下のプラットフォームへの StoreFront のインストールがテストされており、サポートが提供されます:

- Windows Server 2022 の Datacenter、および Standard エディション
- Windows Server 2019 の Datacenter、および Standard エディション
- Windows Server 2016 の Datacenter、および Standard エディション

> 注:
>
> StoreFront には Windows デスクトップ操作が必要であるため、Windows Server Core にはインストール

> できません。

サーバーグループ内のすべての StoreFront サーバーは、同じオペレーティングシステムのバージョン、言語、ロケールを使用する必要があります。

StoreFront が動作するサーバー上のオペレーティングシステムをアップグレードすることはサポートされていません。Citrix では新しくインストールしたオペレーティングシステムに StoreFront をインストールすることをお勧めします。

StoreFront をインストールする前に、Web サーバーで次の Windows 機能を有効にする必要があります。これらのコンポーネントは、新しい Windows インストールではデフォルトで有効になっているため、明示的にアンインストールしない限り、操作は必要ありません。

- NET-Framework-45-Features
  - NET-Framework-45-Core
- PowerShellRoot
  - PowerShell

インストールされている.NET Framework のバージョンが 4.7.2 より古い場合、インストーラーは自動的に.NET Framework 4.7.2 をインストールします。これには、NET-Framework-45-Core Windows 機能が既にインストールされている必要があることに注意してください。

StoreFront インストーラーが、次のいずれかの Windows 機能が満たされていないことを検出した場合、それらは自動的にインストールされます:

- Web-Server
  - Web-WebServer
    - Web-Common-Http
      - Web-Default-Doc
      - Web-Http-Errors
      - Web-Static-Content
      - Web-Http-Redirect
    - Web-Health
      - Web-Http-Logging
    - Web-Security
      - Web-Filtering
      - Web-Basic-Auth
      - Web-Windows-Auth
    - Web-App-Dev
      - Web-Net-Ext45

        - Web-AppInit
        - Web-Asp-Net45
        - Web-ISAPI-Ext
        - Web-ISAPI-Filter
    - Web-Mgmt-Tools
        - Web-Mgmt-Console
    - Web-Scripting-Tools
- NET-Framework-45-Features
    - NET-Framework-45-ASPNET
    - NET-WCF-Services45
        - NET-WCF-TCP-PortSharing45

StoreFront をインストールする前に、IIS Web サイトを別のディレクトリまたはドライブに移動することができます。StoreFront の IIS での相対パスが、サーバーグループ内のすべてのサーバーで同じである必要があります。

ハードウェア

StoreFront サーバーは、次の要件を満たしている必要があります:

- プロセッサ: 2 基以上の仮想 CPU、4 基の仮想 CPU を推奨
- RAM: 4GB。さらにユーザーごとに利用可能なリソースごとに 700 バイト。
- ストレージ:
    - StoreFront 自体には 250MB。
    - ストアごとに 1 つの Web サイトを想定した場合、ストアごとに 30MB。
    - お気に入りが有効になっているストアごとに 5MB。さらに、お気に入り 1000 件ごとに 8MB。
    - 要件に応じた IIS ログファイル用の十分な空き容量。IIS ログファイルストレージの管理に関する Microsoft ドキュメントを参照してください。
    - StoreFront 診断ログ用の十分な空き容量。デフォルトでは、StoreFront はサービスごとに 1GB のログを保持します。StoreFront 展開には通常、ストアごとに 1 つのローミングサービスに加えて 3 つのサービス（ストアサービス、認証サービス、および Receiver for Web サービス）が含まれます。「トラブルシューティング」を参照してください。

ネットワーク

StoreFront では、以下の通信ポートが使用されます。ファイアウォールやほかのネットワークデバイスで、これらのポートへのアクセスが許可されることを確認してください。

- TCP ポート 80 と 443 は、それぞれ HTTP および HTTPS 通信を使用してクライアントが StoreFront に接続するために使用されます。
- TCP ポート 808 は、サーバーグループ内の StoreFront サーバー間の通信で使用されます。
- サーバーグループ内の StoreFront サーバー間の通信では、すべての未割り当て TCP ポートからランダムに選択されるポートが使用されます。StoreFront のインストール時に構成される Windows ファイアウォール規則により、StoreFront の実行可能ファイルへのアクセスが有効になります。ただし、そのときに使用されるポートはランダムに選択されるため、内部ネットワーク上のファイアウォールやほかのネットワークデバイスで、すべての未割り当て TCP ポートへのトラフィックがブロックされないことを確認する必要があります。
- HTML5 向け Citrix Workspace アプリ、または有効な場合、Citrix Workspace アプリのサポート対象バージョンが、内部ネットワーク上のローカルユーザーからデスクトップやアプリケーションを提供するサーバーへの通信で TCP ポート 8008 を使用します。

StoreFront では、ピュア IPv6 ネットワークおよびデュアルスタック IPv4/IPv6 環境の両方がサポートされます。

Active Directory

StoreFront の多くの機能では、StoreFront がインストールされている Windows Server を Active Directory ドメインに参加させる必要があります。

ドメインに参加していないサーバーに StoreFront をインストールすると、次の機能は利用できなくなります:

- サーバーグループ
- お気に入り
- 明示的なユーザー名とパスワード以外の認証方法 (StoreFront に直接、または Gateway 経由)。StoreFront を構成して、認証を Delivery Controller に委任する必要があります。

Microsoft SQL Server を使用したサブスクリプションデータの保存

オプションで、Microsoft SQL Server を使用したサブスクリプションデータを保存できます。StoreFront でこのオプションがサポートされる Microsoft SQL Server バージョンは、Citrix Virtual Apps and Desktops でデータベースに関してサポートされる Microsoft SQL Server バージョンと同じです。Citrix Virtual Apps and Desktops の「システム要件」の「データベース」セクションを参照してください。

インフラストラクチャの要件

Citrix では、以下の Citrix インフラストラクチャ製品での StoreFront の使用がテストされており、サポートが提供されます。

Citrix Virtual Apps and Desktops

StoreFront は、次のバージョンの Citrix Virtual Apps and Desktops をサポートしています:

- Citrix Virtual Apps and Desktops 2402 LTSR
- Citrix Virtual Apps and Desktops 2311
- Citrix Virtual Apps and Desktops 2308
- Citrix Virtual Apps and Desktops 2305
- Citrix Virtual Apps and Desktops 2203 LTSR
- Citrix Virtual Apps and Desktops 1912 LTSR

Citrix Gateway

公共のネットワーク上のユーザーが StoreFront にアクセスできるようにする場合、以下のバージョンの Citrix Gateway を使用できます。

- Citrix Gateway 14.1
- Citrix Gateway 13.1
- Citrix Gateway 13.0

Citrix Gateway 経由の接続は、ICA プロキシ、Citrix Gateway Plug-in、またはクライアントレス VPN（cVPN）を使用して実行できます。

ユーザーデバイスの要件

StoreFront は、ユーザーがデスクトップやアプリケーションにアクセスするためのさまざまなオプションを提供します。Citrix ユーザーは、ローカルにインストールされた Citrix Workspace アプリを通じてストアにアクセスすることも、ブラウザー内で HTML5 向け Citrix Workspace アプリを使用することもできます。

ローカルにインストールされた **Citrix Workspace** アプリ

現在サポートされているすべてのバージョンの Citrix Workspace アプリで、内部ネットワーク接続と Citrix Gateway の両方から StoreFront ストアにアクセスできます。Citrix Workspace アプリのライフサイクル日程については、https://www.citrix.com/support/product-lifecycle/workspace-app.htmlを参照してください。

Web ブラウザーでの **HTML5** 向け **Citrix Workspace** アプリ

HTML5 向け Citrix Workspace アプリを使用して、Web ブラウザーでストアにアクセスできます。アプリとデスクトップは、ネイティブにインストールされた Citrix Workspace アプリ経由で（ハイブリッド起動と呼ばれます）、または Web ブラウザー内で起動できます。Web サイトの構成によっては、エンドユーザーが 2 つの起動方法を切り替えることができます。

以下のブラウザーの最新バージョンを使用してください。

Windows の場合:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Internet Explorer 11 - ストアの閲覧のみに使用され、リソースへの接続には使用されません。

Mac の場合:

- Safari
- Google Chrome
- Mozilla Firefox

Linux の場合:

- Google Chrome
- Mozilla Firefox

HTML5 向け Citrix Workspace アプリを使用して Web ブラウザー経由でリソースに接続するための要件について詳しくは、HTML5 向け Citrix Workspace アプリのドキュメントを参照してください。

レガシーデバイス

Citrix のレガシークライアントは、XenApp Services の URL を使用して、機能が限定された状態で StoreFront ストアにアクセスできます。XenApp Services の URL は、Citrix Receiver 3.4 Enterprise およびそれ以前のクライアントによる接続に対して、後方互換性のあるレガシーサポートを提供します。この機能は非推奨であり、将来のリリースから削除される予定です。

スマートカードの要件

スマートカードによる **Citrix Workspace** アプリの使用

Citrix は、U.S. Government Dept. Of Defense Common Access Card（CAC）、U.S. National Institute of Standards and Technology Personal Identity Verification（NIST PIV）カード、および一部の USB スマートカードトークンを対象として、互換性をテストします。USB Chip/Smart Card Interface Devices（CCID）仕様に準拠し、German Zentraler Kreditausschuss（ZKA）により Class 1 スマートカードリーダーとして分類される接触型カードリーダーを使用できます。ZKA Class 1 接触型カードリーダーを使用するには、ユーザーがリーダーにスマートカードを挿入する必要があります。Class 2 リーダー（PIN を入力するためのテンキー付属）を含むそのほかの種類のスマートカードリーダー、非接触型リーダー、および Trusted Platform Module（TPM）チップに基づく仮想スマートカードはサポートされません。

Receiver for Windows のスマートカードのサポートは、Microsoft の PC/SC（Personal Computer/Smart Card）標準仕様に基づいています。最小要件として、スマートカードおよびスマートカードリーダーがオペレーティングシステムでサポートされており、「Windows ハードウェア認定」を取得している必要があります。

Citrix 互換のスマートカードとミドルウェアについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「スマートカード」およびhttp://www.citrix.com/readyを参照してください。

Citrix Analytics Service の要件

Citrix StoreFront を構成して、Citrix Workspace アプリが Citrix Analytics Service にデータを送信できます。構成の詳細は、「Citrix Analytics Service」を参照してください。この機能は、次のシナリオでサポートされています:

- Web ブラウザーでアクセスするストア。
- Windows 向け Citrix Workspace アプリ 1903 以降からアクセスされるストア。
- Linux 向け Citrix Workspace アプリ 1901 以降からアクセスされるストア。

StoreFront のインストール

June 6, 2024

インストールおよび構成する前に

StoreFront をインストールして構成するには、次の手順に従います:

1. システム要件を確認してください。
2. StoreFront で Citrix Virtual Apps and Desktops のリソースをユーザーに配信する場合は、ユーザーアカウントが属している Microsoft Active Directory ドメイン、またはそのドメインと信頼関係があるドメインのいずれかに StoreFront サーバーが属していることを確認してください。

   > 重要:
   >
   > - 単一サーバー展開では、ドメインに参加していないサーバーに StoreFront をインストールできます。
   > - StoreFront をドメインコントローラー上にインストールすることはできません。

3. 複数サーバーの StoreFront 展開環境を構成する計画の場合は、必要に応じて StoreFront サーバーの負荷分散環境をセットアップします。

NetScaler ADC を使用して負荷分散を行うには、StoreFront サーバーのプロキシとなる仮想サーバーを定義します。NetScaler ADC を使用した負荷分散の構成について詳しくは、「NetScaler ADC による負荷分散」を参照してください。

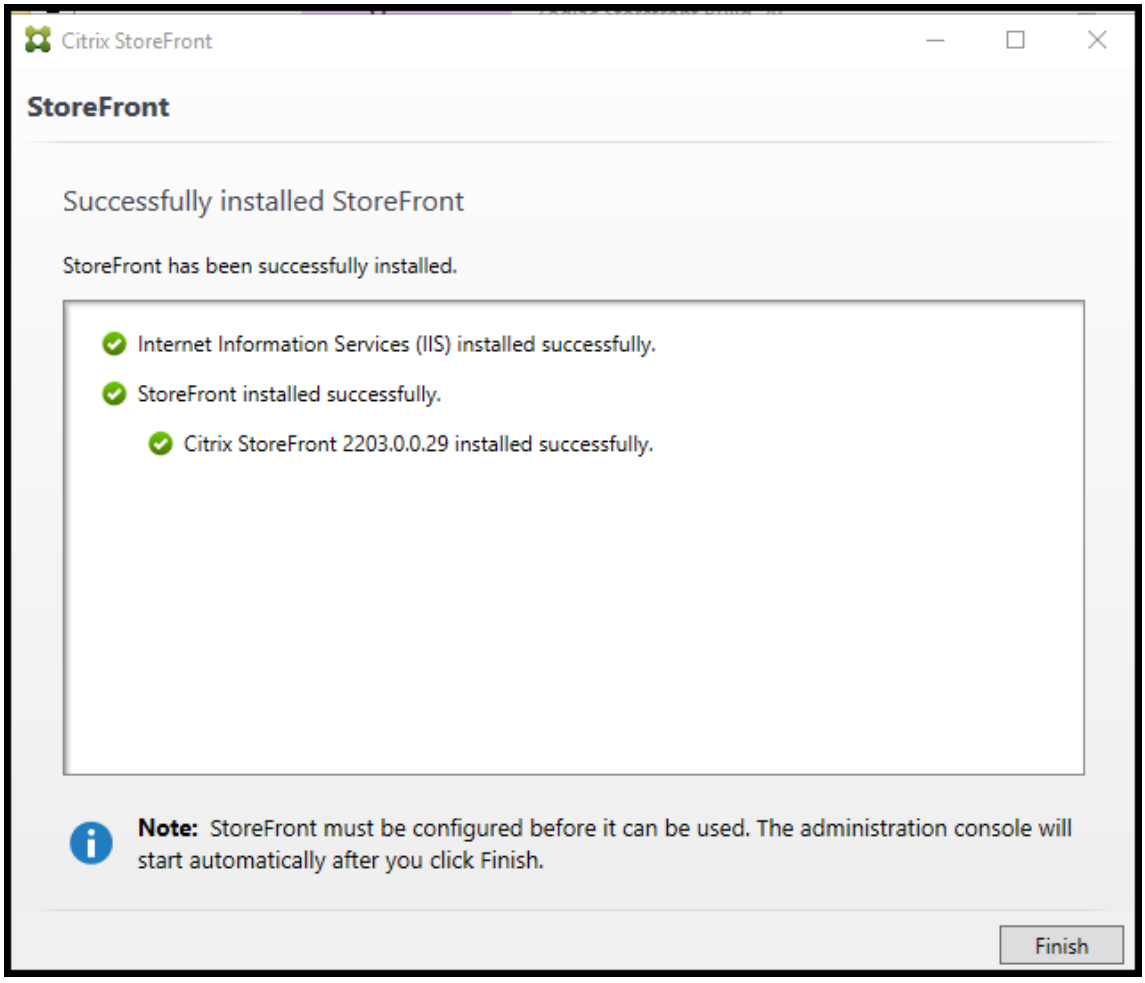
4. ファイアウォールやほかのネットワークデバイスで、社内ネットワーク内外からの TCP ポート 80 または 443 へのアクセスが許可されることを確認します。また、内部ネットワーク上のファイアウォールやほかのネットワークデバイスで、すべての未割り当て TCP ポートへのトラフィックがブロックされないことを確認します。

   StoreFront のインストール時に Windows ファイアウォールで構成される規則により、すべての未割り当て TCP ポートからランダムに選択されるポートを介した StoreFront の実行可能ファイルへのアクセスが有効になります。このポートは、サーバーグループ内の StoreFront サーバー間の通信で使用されます。

StoreFront のインストール

> 重要
>
> StoreFront インストール時にエラーやデータの損失が発生するのを回避するために、すべてのアプリケーションが閉じられていて、ターゲットシステム上で他のタスクや操作が実行されていないことを確認します。

1. ダウンロードページからインストーラーをダウンロードします。
2. ローカルの管理者権限を持つアカウントで StoreFront サーバーにログオンします。
3. CitrixStoreFront-x64.exe を検索し、管理者として実行します。
4. ライセンス契約書を読み、同意することを選択して、［次へ］をクリックします。
5. ［必須条件の確認］ページが開いた場合は、［次へ］をクリックします。
6. ［インストールの開始］ページで、インストール対象の必須条件および StoreFront コンポーネントを確認して、［インストール］をクリックします。
7. インストールが完了したら、［完了］をクリックします。



8. StoreFront は、インストールを完了するために再起動を要求することがあります。今すぐ再起動するには［はい］をクリックします。
9. Microsoft インターネットインフォメーションサービス（IIS）で HTTPS を構成します。手順については、「HTTPS による StoreFront のセキュリティ保護」を参照してください。

コマンドプロンプトから **StoreFront** をインストールするには

1. ローカルの管理者権限を持つアカウントで StoreFront サーバーにログオンします。
2. StoreFront をインストールする前に、StoreFront のインストール要件が満たされていることを確認します。「インストールおよび構成する前に」を参照してください。
3. インストールメディアの内容を参照するかパッケージをダウンロードして、CitrixStoreFront-x64.exe をサーバー上の任意のフォルダーに一時的にコピーします。
4. コマンドプロンプトでインストールファイルが含まれるフォルダーに移動して、次のコマンドを実行します:


```
CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR
    installationlocation] [-WINDOWS_CLIENT filelocation\filename.
    exe] [-MAC_CLIENT filelocation\filename.dmg]
<!--NeedCopy-->
```

StoreFront とその前提条件のサイレントインストールを実行するには、**-silent** 引数を使用します。StoreFront は、デフォルトで C:\Program Files\Citrix\Receiver StoreFront にインストールされます。ただし、**-INSTALLDIR** 引数を使用して別のインストール場所を指定することもできます。*installationlocation* には StoreFront のインストール先のフォルダーを指定します。サーバーをサーバーグループに含める場合は、StoreFront のインストール場所設定と IIS Web サイト設定の両方で、物理パスおよびサイト ID を一致させる必要があります。

デフォルトでは、ユーザーが Windows または macOS で Web ブラウザーを開き、Citrix Workspace アプリを検出できない場合、対象のプラットフォームに対応した Citrix Workspace アプリを Citrix の Web サイトからダウンロードしてインストールするようメッセージが表示されます。この動作を変更して、Citrix Workspace アプリのインストールファイルを StoreFront サーバーからダウンロードできるように構成することもできます。詳しくは、「ユーザーに対するリソースの表示方式の構成」を参照してください。

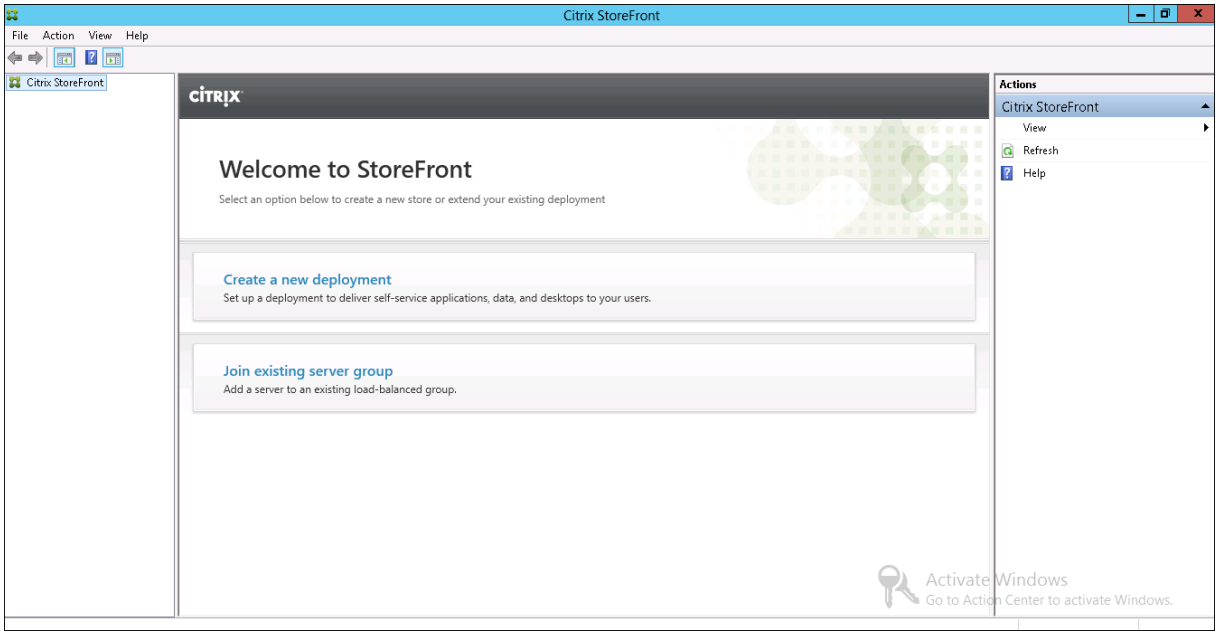
この構成を変更する場合は、**-WINDOWS_CLIENT** および **-MAC_CLIENT** 引数を指定して、Citrix Receiver for Windows または Windows 向け Citrix Workspace アプリ、および Citrix Receiver for Mac または Mac 向け Citrix Workspace アプリのインストールファイルをそれぞれ StoreFront 展開の適切な場所にコピーします。ここで *filelocation* はコピー対象のインストールファイルが格納されているフォルダーを示し、*filename* はインストールファイルの名前を示します。Citrix Receiver for Windows、および Citrix Receiver for Mac または Mac 向け Citrix Workspace アプリのインストールファイルは、Citrix Virtual Apps and Desktops のインストールメディアに含まれています。

インストールログ

ログファイルについて詳しくは、「インストールログ」を参照してください。

StoreFront の構成

インストールが完了すると、Citrix StoreFront 管理コンソールが自動的に起動します。また、［起動］メニューから StoreFront を開くこともできます。Citrix StoreFront 管理コンソールの初回起動時に、2 つのオプションが表示されます。



- 展開の作成。新しい StoreFront 展開環境の最初のサーバーを構成します。StoreFront を評価したり、小規模な展開環境を作成したりするには、単一サーバー環境が理想的です。最初の StoreFront サーバーを構成した後では、いつでもサーバーをグループに追加して展開環境の許容能力を拡張できます。
- 既存のサーバーグループへの参加。既存の StoreFront 展開環境に別のサーバーを追加します。StoreFront 展開環境の許容能力をすばやく拡張するには、このオプションを選択します。複数サーバーの展開環境には、外部の負荷分散機能が必要です。サーバーを追加する管理者には、展開環境内の既存のサーバーに対するアクセス権が必要です。

ユーザーはブラウザーまたは Citrix Workspace アプリを介してストアにアクセスできるようになりました。詳しくは ユーザーガイドを参照してください。

Citrix カスタマーエクスペリエンス向上プログラム

June 6, 2024

Citrix のカスタマーエクスペリエンス向上プログラム（CEIP）に参加すると、匿名の統計および使用状況情報が、Citrix 製品の品質およびパフォーマンスを向上させる目的で送信されます。

StoreFront をインストールすると CEIP に自動的に登録されるようになりました。StoreFront のインストールからおよそ 7 日後に、初回データアップロードが行われます。このデフォルトはレジストリ設定で変更できます。StoreFront のインストールの前にレジストリ設定を変更すると、その値が使用されます。StoreFront のアップグレードの前にレジストリ設定を変更すると、その値が使用されます。

> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

分析の自動アップロードを制御するレジストリ設定（デフォルト = 1）:

```
Location: HKLM:\Software\Citrix\Telemetry\CEIP
Name: Enabled
Type: REG_DWORD
Value: 0 = disabled, 1 = enabled
<!--NeedCopy-->
```

デフォルトで、**Enabled** プロパティはレジストリに表示されません。未指定のままの場合、自動アップロード機能は有効です。

PowerShell を使用する場合、次のコマンドレットは CEIP への登録を無効にします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0
```

> 注:
>
> このレジストリ設定では、同一サーバー上にあるすべてのコンポーネントの匿名の統計情報と使用状況情報の自動アップロードを制御します。たとえば、Delivery Controller と同じサーバー上に StoreFront をインストールし、レジストリ設定で CEIP への参加を無効にした場合、両方のコンポーネントで CEIP への参加が無効になります。

StoreFront で収集される **CEIP** データ

次の表に、収集される匿名情報の種類の例を示します。データでは、お客様を特定するすべての詳細は含まれません。

データ	説明
StoreFront のバージョン	インストールされている StoreFront のバージョンを示す文字列。例：3.8.0.0。
ストア数	展開環境に含まれるストア数を表すカウンター。
サーバーグループ内のサーバー数	サーバーグループに含まれるサーバー数を表すカウンター。
ストアごとの Delivery Controller 数	展開環境内の各ストアで利用可能な Delivery Controller の数を表す数値の一覧。

データ	説明
HTTPS 有効	展開で HTTPS が有効にされているかどうか（True または False）を示す文字列。
Citrix Receiver for Web の HTML 5 設定	各 Receiver for Web サイトの HTML5 Receiver 設定（Always、Fallback、または Off）を示す文字列の一覧。
Citrix Receiver/Citrix Workspace アプリのワークスペースコントロールの有効化	各 Web Receiver で「ワークスペースコントロール」が有効にされているかどうか（True または False）を示すブール値の一覧。
ストアのリモートアクセスの有効化	展開内の各ストアで「リモートアクセス」が有効にされているかどうか（ENABLED または DISABLED）を示す文字列の一覧。
ゲートウェイ数	展開環境で構成されている Citrix Gateway の数を表すカウンター。

Citrix Analytics Service

June 6, 2024

Citrix Cloud をご利用中でオンプレミスの StoreFront 展開環境をお持ちの場合、データが Citrix Cloud の Citrix Analytics Service に送信されるように StoreFront を構成できます。構成後は、Citrix Workspace アプリおよび Web ブラウザーがユーザーイベントを処理するために Citrix Analytics に送信します。Citrix Analytics は、ユーザー、アプリケーション、エンドポイント、ネットワーク、データに関する測定値を集約して、ユーザーの行動に関する包括的な分析情報を提供します。Citrix Analytics ドキュメントでこの機能について確認するには、「StoreFront を使用した Virtual Apps and Desktops サイトへのオンボード」を参照してください。

この機能を構成するには、以下を実行します:

- Citrix Analytics から構成ファイルをダウンロードします。
- Citrix Analytics データを PowerShell を使用してオンプレミスの StoreFront 展開にインポートします。

StoreFront の構成後は、Citrix Analytics Service が要求した時に Citrix Workspace アプリが StoreFront のストアからデータを送信できます。

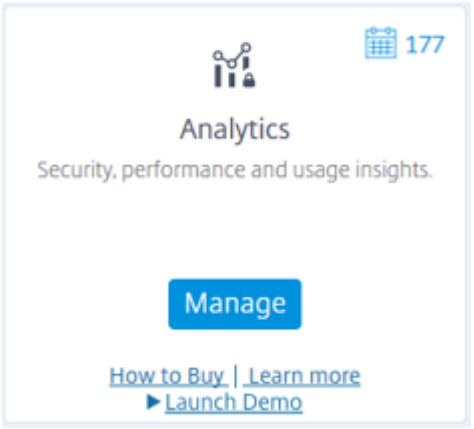
> 重要:
>
> この機能が正しく動作し、モニターサービスを消費するには、使用中の StoreFront 展開がポート 443 の次のアドレスと通信できるようにする必要があります:
>
> - `https://*.cloud.com`

- https://*.citrixdata.com

Citrix Analytics から構成ファイルをダウンロードする

> 重要:
>
> 初期構成には、機密情報を含む構成ファイルが必要です。ダウンロード後はファイルを安全に保管してください。このファイルを組織外の人と共有しないでください。構成後、このファイルは削除できます。別のマシンに構成を再適用する必要がある場合は、Citrix Analytics Service 管理コンソールからファイルを再度ダウンロードできます。

1. 管理者アカウントでモニター（https://citrix.cloud.com/）にログオンします。
2. モニター顧客を選択します。
3. ［管理］をクリックして、Citrix Analytics Service 管理コンソールを開きます。



4. Citrix Analytics Service 管理コンソールで、［**Settings**］**>**［**Data Sources**］を選択します。
5. Virtual App and Desktops カードで、（⊠）メニューアイコン、［**Connect StoreFront deployment**］の順に選択します。
6. ［Connect StoreFront Deployment］ページで ［**Download File**］を選択して *StoreFrontConfigurationFile.json* ファイルをダウンロードします。

構成ファイルの例

```
{

  "customerId": "<yourcloudcustomer>",
  "enablementService": " https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/<
     deviceid>/dsconfigdata",
  "cwsServiceKey": "PFJTPn …… .. T4=",
```



```
6    "enablementServiceStatus": " https://api.analytics.cloud.com /casvc/<
        yourcloudcustomer>/ctxana/v1/cas/storefront/config",
7    "instanceId": "d98f21d0-56e0-11e9-ba52-5136d90862fe",
8    "name": "CASSingleTenant"
9   }
10
11  <!--NeedCopy-->
```

:

customerId は、最新のモニターの顧客用の一意の ID です。

cwsServiceKey は、最新のモニターの顧客を特定する一意のキーです。

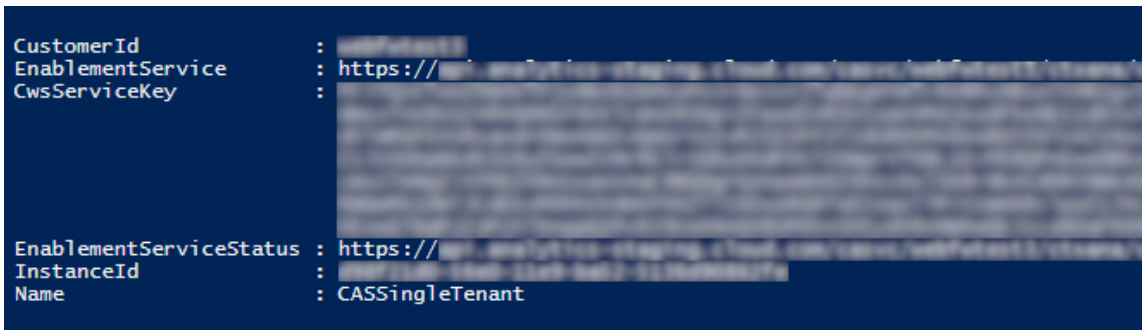
instanceID は、Citrix Workspace アプリから Citrix Analytics に対して送信された要求に署名（セキュリティ保護済み）するために生成された ID です。複数の StoreFront サーバーまたはサーバーグループをモニターに登録すると、それぞれに一意の instanceID が割り当てられます。

Citrix Analytics データを StoreFront 展開にインポートする

1. *StoreFrontConfigurationFile.json* ファイルをオンプレミスの StoreFront サーバー（または StoreFront サーバーグループのいずれかのサーバー）の適切なフォルダーにコピーします。以下のコマンドは、ファイルがデスクトップに保存されている場合です。
2. PowerShell ISE を開き、［管理者として実行］を選択します。
3. 次のコマンドを実行します:

```
1  Import-STFCasConfiguration -Path "$Env:UserProfile\Desktop\
      StoreFrontConfigurationFile.json"
2  Get-STFCasConfiguration
3  <!--NeedCopy-->
```

4. このコマンドはインポートされたデータのコピーを返し、それを PowerShell コンソールに表示します。



> 注:
>
> Windows Server 2012 R2 にインストールされているオンプレミス StoreFront サーバーでは、C++ ランタイムソフトウェアコンポーネントを手動でインストールして CAS に登録できるようにする必要があります。

> Citrix Virtual Apps and Desktops のインストール中に StoreFront がインストールされる場合、CVAD メタインストーラーが C++ ランタイムコンポーネントをインストールするため、この手順は不要です。C++ ランタイムのない CitrixStoreFront-x64.exe メタインストーラーで StoreFront がインストールされている場合、CAS 構成ファイルのインポート後、モニターへの登録に失敗する場合があります。

Citrix Analytics のデータを **StoreFront** サーバーグループに伝達する

StoreFront サーバーグループでこれらの操作を実行している場合は、インポートされた Citrix Analytics データをサーバーグループの全メンバーに伝達する必要があります。この手順は、単一の StoreFront サーバー展開では必要ありません。

データを伝達するには、以下のいずれかの方法を使用します:

- StoreFront 管理コンソールを使用します。
- PowerShell コマンドレット **Publish-STFServerGroupConfiguration** を使用します。

StoreFront サーバーグループ **ID** を確認する

Citrix Analytics Service に正常に登録されたかどうかを確認するには、PowerShell を使用して展開の ServerGroupID を検出します。

1. StoreFront サーバー、またはサーバーグループ内の 1 台の StoreFront サーバーにログオンします。
2. PowerShell ISE を開き、[管理者として実行] を選択します。
3. 次のコマンドを実行します:

```
$WebConfigPath = "C:\Program Files\Citrix\Receiver StoreFront\
    Framework\FrameworkData\Framework.xml"
$XMLObject = (Get-Content $WebConfigPath) -as [Xml]
$XMLObject.framework.properties.property
<!--NeedCopy-->
```

たとえば、これらのコマンドは次のような出力結果を生成します:

```
name value
---- -----
ClusterId 8b8ff5c8-44ba-46e4-87f0-2df8cff31432
HostBaseUrl https://storefront.example.com/
SelectedIISWebSiteId 1
AdminConsoleOperationMode Full
<!--NeedCopy-->
```

StoreFront から **Citrix Analytics** へのデータの送信を停止する

1. PowerShell ISE を開き、[管理者として実行] を選択します。

2. 次のコマンドを実行します:

   ```
   Remove-STFCasConfiguration
   ```

   ```
   Get-STFCasConfiguration
   ```

   以前にインポートされた Citrix Analytics データの削除に成功した場合、**Get-STFCasConfiguration** は値を返しません。

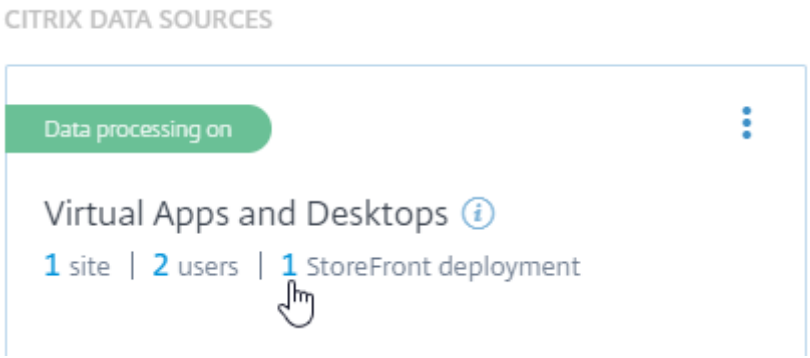
3. StoreFront サーバーグループでこれらの操作を実行している場合は、変更を伝達し、インポートされた Citrix Analytics データをサーバーグループの全メンバーから削除する必要があります。サーバーグループ内の 1 台のサーバーで、次のコマンドを実行します:

   ```
   Publish-STFServerGroupConfiguration
   ```

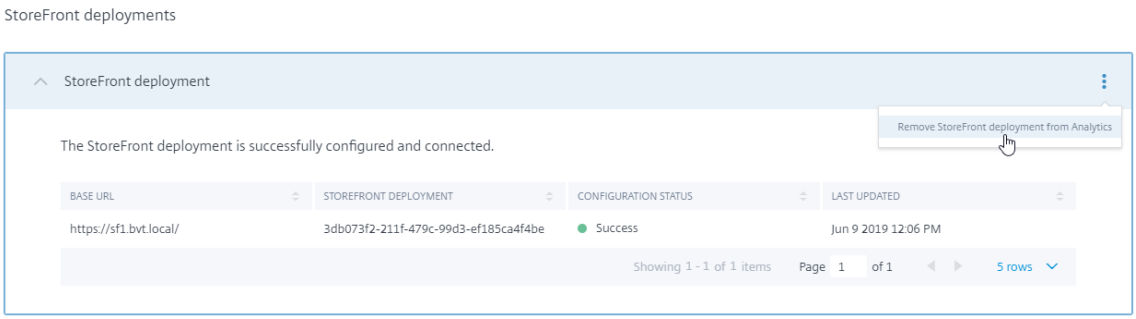
4. 他のサーバーグループメンバーで次のコマンドを実行して、Citrix Analytics 構成がグループ内のすべてのサーバーから正常に削除されたことを確認します:

   ```
   Get-STFCasConfiguration
   ```

5. 管理者アカウントでモニター（https://citrix.cloud.com/）にログオンします。
6. モニター顧客を選択します。
7. ［管理］をクリックして、Citrix Analytics Service 管理コンソールを開きます。
8. Citrix Analytics Service 管理コンソールで、［**Settings**］**>** ［**Data Sources**］を選択します。
9. Virtual App and Desktops カードで、StoreFront の展開数を選択します:



10. ホストベース URL および ServerGroupID を参照して削除対象の StoreFront 展開を特定します。
11. （⊠）メニューで、［**Remove StoreFront deployment from Analytics**］を選択します。



> 注:
>
> サーバー側で構成を削除する一方、Citrix Analytics からは削除しない場合、StoreFront 展開のエントリは Citrix Analytics に残るものの、StoreFront からはデータを受信しません。Citrix Analytics からのみ構成を削除する場合、StoreFront 展開のエントリは次回のアプリプールの再利用時（IIS のリセット時、または自動で 24 時間ごと）に再度追加されます。

Web プロキシを使用して **Citrix Cloud** に接続し、**Citrix Analytics** に登録するように **StoreFront** を構成する

StoreFront が Web プロキシの背後のホスト Web サーバーに配置されている場合、Citrix Analytics への登録は失敗します。StoreFront 管理者が Citrix 展開で HTTP プロキシを使用する場合、インターネットへの StoreFront トラフィックはクラウド内の Citrix Analytics に到達する前に Web プロキシを通過する必要があります。StoreFront は、ホスト OS のプロキシ設定を自動的に使用しません。Web プロキシを介してトラフィックを送信するようストアに指示するには、さらに構成が必要です。ストアの web.config ファイルに新しいセクションを追加して<system.net>プロキシ設定を構成できます。Citrix Analytics へのデータ送信に使用される StoreFront サーバー上のすべてのストアに対してこれを実行します。

方法 **1**：**Powershell** で **1** つまたは複数のストアでプロキシ構成を設定する（推奨）

Powershell スクリプト Config-StoreProxy.ps1 を実行すると、1 つまたは複数のストアでこのプロセスを自動化し、<system.net>を構成する有効な XML が自動的に挿入されます。また、このスクリプトは現在のユーザーのデスクトップにストアの web.config ファイルのバックアップを作成し、必要な場合変更されていない web.config ファイルを復元できるようにします。

> 注:
>
> スクリプトを複数回実行すると、複数の<system.net>XML のコピーが追加されます。ストアごとに<system.net>のエントリは 1 つのみにする必要があります。複数のコピーを追加すると、ストアのプロキシ構成が正しく機能しなくなります。

1. PowerShell ISE を開き、［管理者として実行］を選択します。
2. `$Stores = @("Store","Store2")` を設定して Web プロキシで構成するストアを含めます。

3. 次のいずれかを指定します:

   - IP アドレス、または
   - Web プロキシの FQDN

4. 次の PowerShell を実行します:

```
$Stores = @("Store","Store2")
$ProxyIP = "10.0.0.1"
$ProxyFQDN = "proxyserver.example.com"
$ProxyPort = 8888

# Set this for every Store using Stores array
function Set-StoreProxyServer() # Tested with both IP and FQDN
{

    [CmdletBinding()]
    param([Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
        Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
        array]$Stores,
         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
            string]$ProxyIP,
         [Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
            string]$ProxyFQDN,
         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
            Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")
            ][int]$ProxyPort)

    foreach($Store in $Stores)
    {

        Write-Host "Backing up the Store web.config file for store
             $Store before making changes..." -ForegroundColor "
            Yellow"
        Write-Host "`n"

        if(!(Test-Path "$env:UserProfile\desktop$Store"))
        {

            Write-Host "Creating $env:UserProfile\desktop$Store\
                directory for backup..." -ForegroundColor "Yellow"
            New-Item -Path "$env:UserProfile\desktop$Store" -
                ItemType "Directory" | Out-Null
            Write-Host "`n"
         }


        Write-Host "Copying c:\inetpub\wwwroot\Citrix$Store\web.
            config to $env:UserProfile\desktop$Store..." -
            ForegroundColor "Yellow"
        Copy-Item -Path "c:\inetpub\wwwroot\Citrix$Store\web.
            config" -Destination "$env:UserProfile\desktop$Store" -
            Force | Out-Null
```



```
33
34          if(Test-Path "$env:UserProfile\desktop$Store\web.config")
35          {
36
37              Write-Host "$env:UserProfile\desktop$Store\web.config
                    file backed up" -ForegroundColor "Green"
38           }
39
40          else
41          {
42
43              Write-Host "$env:UserProfile\desktop$Store\web.config
                    file NOT found!" -ForegroundColor "Red"
44           }
45
46          Write-Host "`n"
47
48          Write-Host "Setting the proxy server to $ProxyAddress for
                Store $Store..." -ForegroundColor "Yellow"
49          Write-Host "`n"
50
51          $StoreConfigPath = "c:\inetpub\wwwroot\Citrix$Store\web.
                config"
52          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
53
54          if([string]::IsNullOrEmpty($ProxyFQDN))
55          {
56
57              $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)
58           }
59
60          else
61          {
62
63              $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)
64           }
65
66
67          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
68
69          # Create 3 elements
70          $SystemNet = $XMLObject.CreateNode("element","system.net",
                "")
71          $DefaultProxy = $XMLObject.CreateNode("element","
                defaultProxy","")
72          $Proxy = $XMLObject.CreateNode("element","proxy","")
73          $Proxy.SetAttribute("proxyaddress","$ProxyServer")
74          $Proxy.SetAttribute("bypassonlocal","true")
75
76          # Move back up the XML tree appending new child items in
                reverse order
77          $DefaultProxy.AppendChild($Proxy)
78          $SystemNet.AppendChild($DefaultProxy)
```



```
79          $XMLObject.configuration.AppendChild($SystemNet)
80
81          # Save the modified XML document to disk
82          $XMLObject.Save($StoreConfigPath)
83
84          Write-Host "Getting the proxy configuration for c:\inetpub
                \wwwroot\Citrix$Store..." -ForegroundColor "Yellow"
85          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
86          $ConfiguredProxyServer = $XMLObject.configuration.'system.
                net'.defaultProxy.proxy.proxyaddress | Out-Null
87          Write-Host ("Configured proxy server for Store $Store"+":
                "+ $ConfiguredProxyServer) -ForegroundColor "Green"
88          Write-Host "`n"
89       }
90
91      Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
92      IISReset /RESTART
93   }
94
95
96  Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
        ProxyPort $ProxyPort
97  # OR
98  Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
        $ProxyPort
99  <!--NeedCopy-->
```

5. C:\inetpub\wwwroot\Citrix< Store>\web.config で web.config ファイルの最後に新しい<system.net>セクションが含まれていることを確認します。

```
1           </dependentAssembly>
2       </assemblyBinding>
3   </runtime>
4   <system.net>
5       <defaultProxy>
6       <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
            bypassonlocal="true" />
7       </defaultProxy>
8   </system.net>
9   </configuration>
10  <!--NeedCopy-->
```

6. 「Citrix Analytics データを StoreFront 展開にインポートする」の説明に従って、Citrix Analytics データをインポートします。

方法 **2**: 手動で **<system.net>** セクションをストアの **web.config** ファイルに追加する

これは、Citrix Analytics にデータを送信するために使用される StoreFront サーバー上のすべてのストアに対して実行する必要があります。

1. ストアの web.config ファイルのバックアップを作成し、C:\inetpub\wwwroot\Citrix<Store>\web.config 以外の別の場所にコピーします。
2. FQDN とポート番号の組み合わせか IP とポート番号の組み合わせを使用して、以下の XML でプロキシ設定を編集します。

   たとえば、FQDN とポート番号の組み合わせでは、以下のような<system.net>要素を使用します:

```
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
       bypassonlocal="true" />
    </defaultProxy>
</system.net>
<!--NeedCopy-->
```

   たとえば、IP とポート番号の組み合わせでは、以下のような<system.net>要素を使用します:

```
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true
       " />
    </defaultProxy>
</system.net>
<!--NeedCopy-->
```

3. ストアの web.config ファイルの最後に、以下のように適切な<system.net>要素を挿入します:

```
<runtime>
<gcServer enabled="true" />
<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
    <dependentAssembly>
    <assemblyIdentity name="System.Web.MVC" publicKeyToken="31
       BF3856AD364E35" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="
       5.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
    <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30
       ad4fe6b2a6aeed" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="
       9.0.0.0" />
    </dependentAssembly>
</assemblyBinding>
</runtime>

Insert the <system.net> element here

</configuration>
<!--NeedCopy-->
```

4.「Citrix Analytics データを StoreFront 展開にインポートする」の説明に従って、Citrix Analytics データをインポートします。

HTTPS による StoreFront のセキュリティ保護

June 6, 2024

StoreFront とユーザーデバイスの間の通信は、HTTPS で保護することをお勧めします。これにより、クライアントと StoreFront の間で送信されるパスワードおよびその他のデータが確実に暗号化されます。さらに、単純な HTTP 接続は、中間者攻撃などのさまざまな攻撃によって危険にさらされる可能性があります。特に、接続が公衆 Wi-Fi ホットスポットなどの安全はでない場所から行われる場合はその危険性があります。IIS で HTTPS が構成されていない場合、StoreFront の通信に HTTP が使用されます。

構成に応じて、ユーザーはゲートウェイまたはロードバランサー経由で StoreFront にアクセスできます。HTTPS 接続はゲートウェイまたはロードバランサーで終了できます。ただし、この場合でも、HTTPS を使用してゲートウェイと StoreFront 間のセキュリティで保護された接続を確保することをお勧めします。

StoreFront が HTTPS 用に構成されていない場合、次の警告が表示されます:

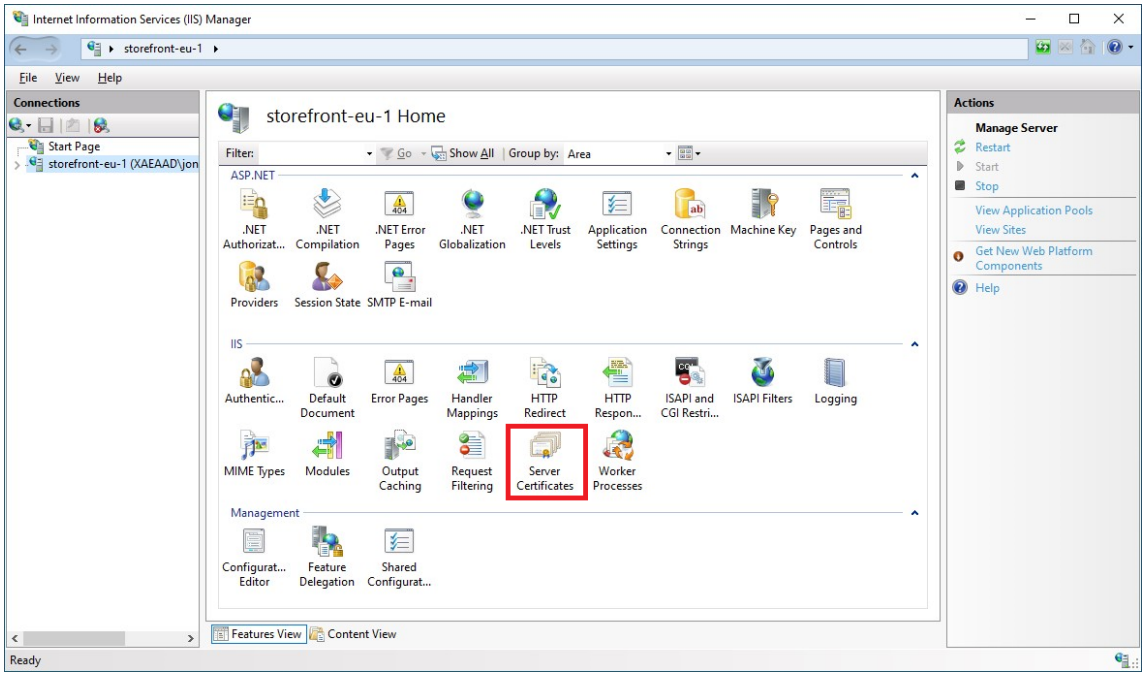
証明書の作成

- StoreFront へのアクセスに使用される FQDN が、サブジェクトの別名（SAN）として DNS フィールドに含まれていることを確認します。ロードバランサーを使用している場合は、個々のサーバーの FQDN とロードバランサーの FQDN を両方とも含めます。
- サードパーティ CA（Verisign など）または組織における会社のルート CA を使用して証明書に署名します。
- 秘密キーを含めて、この証明書を PFX 形式でエクスポートします。

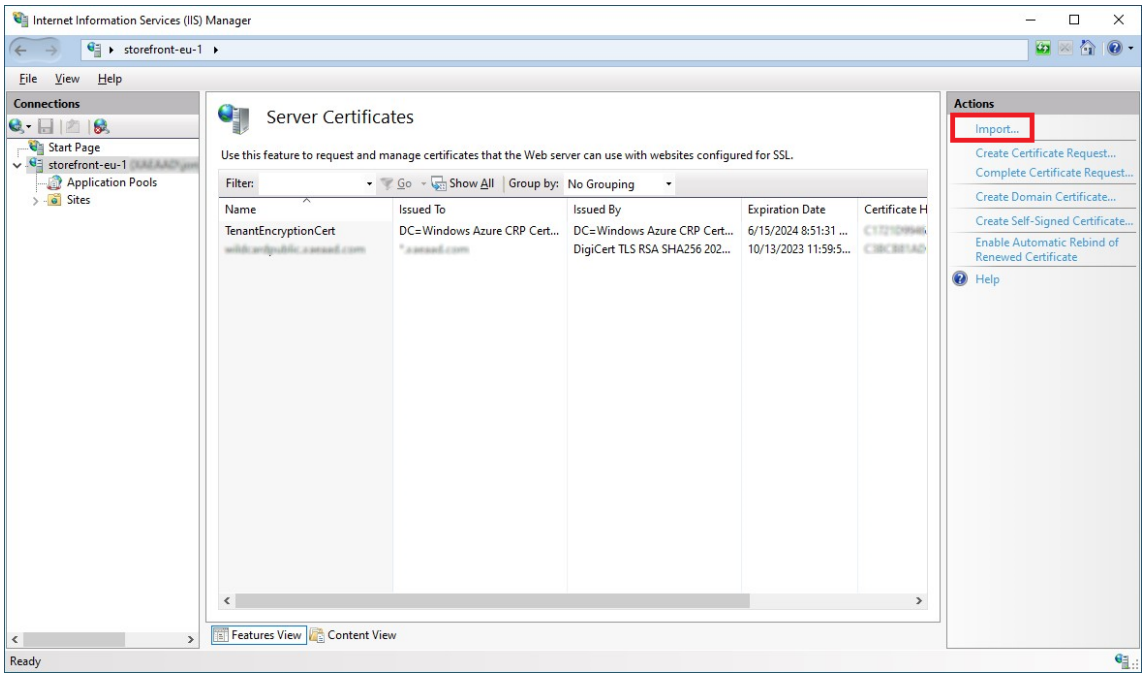
IIS を HTTPS 用に構成する

StoreFront サーバーの Microsoft インターネットインフォメーションサービス（IIS）で HTTPS を構成するには、以下の手順に従います:

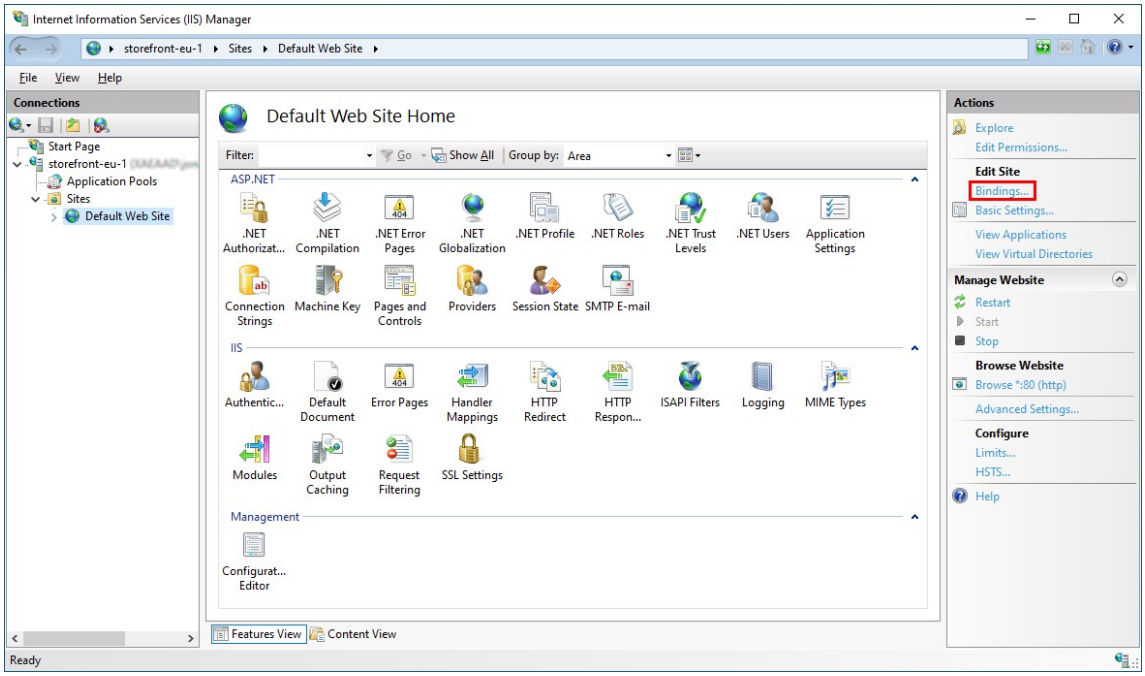
1. インターネットインフォメーションサービス（IIS）マネージャーコンソールの開始
2. 左側のツリー表示でサーバーを選択します。
3. 右側のペインで ［**Server Certifcates**］をダブルクリックします



4. [Server Certifcates] 画面から、既存の証明書をインポートするか、新しい証明書を作成することができます。

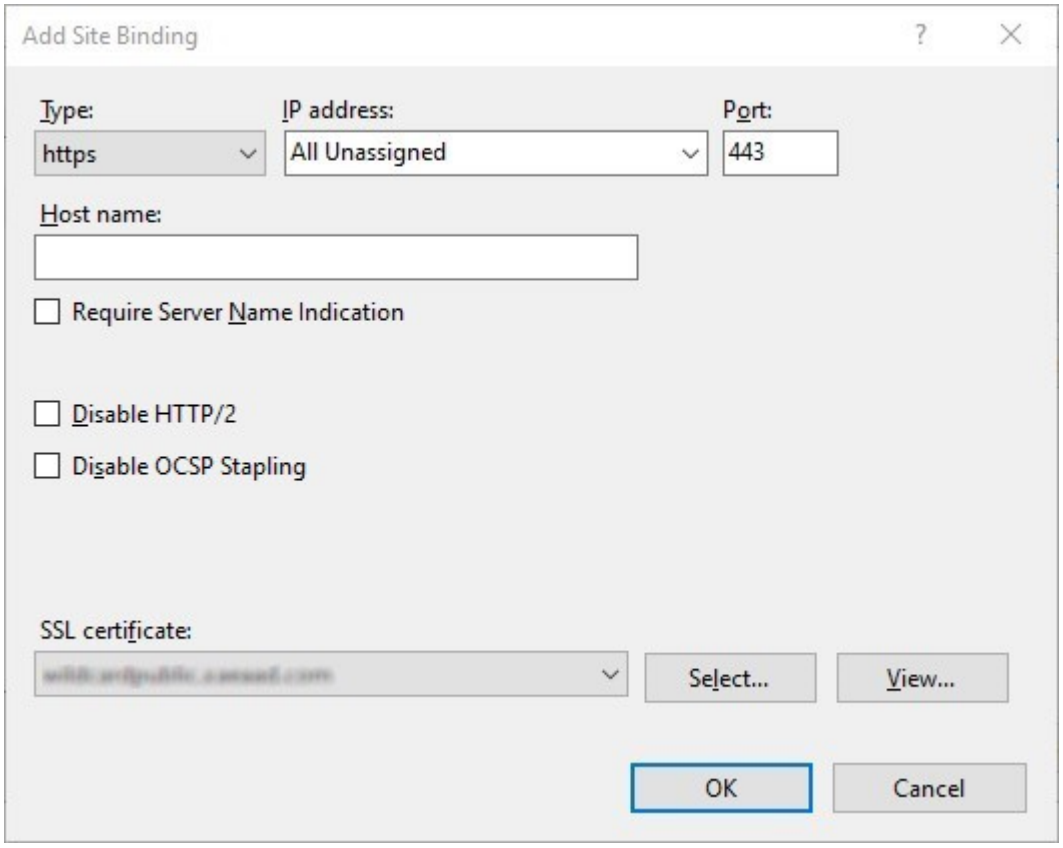


5. 左側のツリー表示で、[**Default Web Site**]（または適切な Web サイト）を選択します。
6. [Actions] ペインで [**Bindings**…] をクリックします。

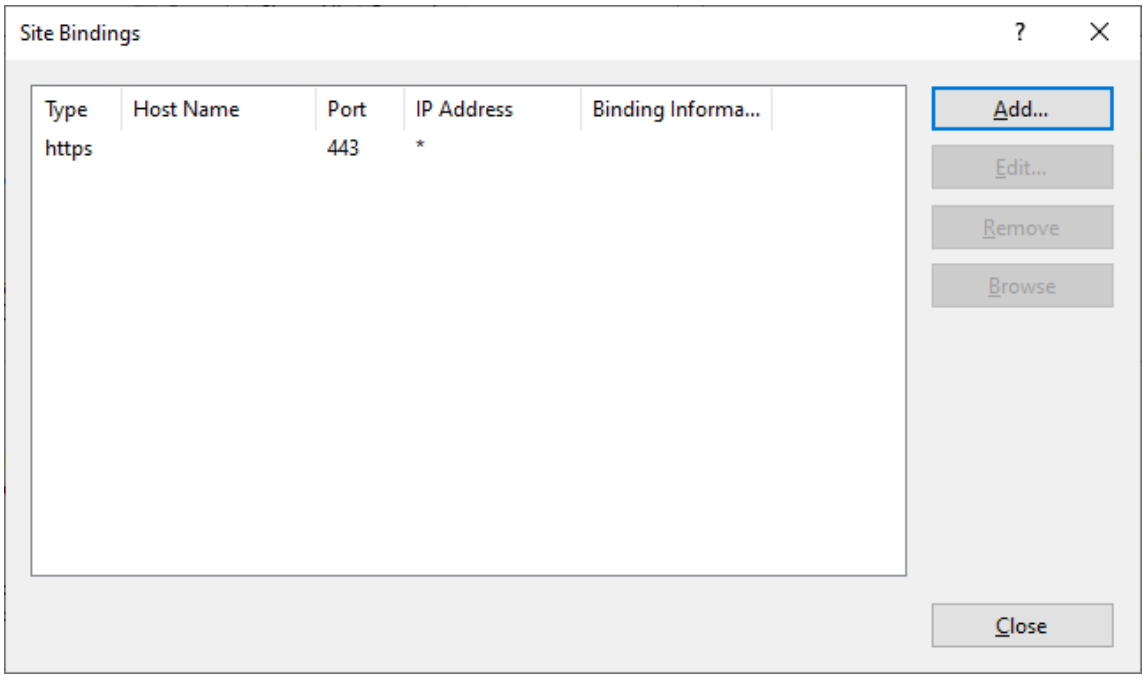


7. バインドウィンドウで ［**Add**…］をクリックします。
8. ［**Type**］ドロップダウンで ［**https**］を選択します。
9. Windows Server 2022 以降では、［**Disable Legacy TLS**］をクリックして 1.2 より古い TLS を無効にします。

   古い Windows Server バージョンでは、Windows レジストリ設定を使用してレガシー TLS バージョンを無効にすることができます。Windows Server のドキュメントを参照してください。
10. 以前にインポートした証明書を選択します。［OK］を押します



11. HTTP アクセスを削除するには、［HTTP］を選択して ［**Remove**］をクリックします。

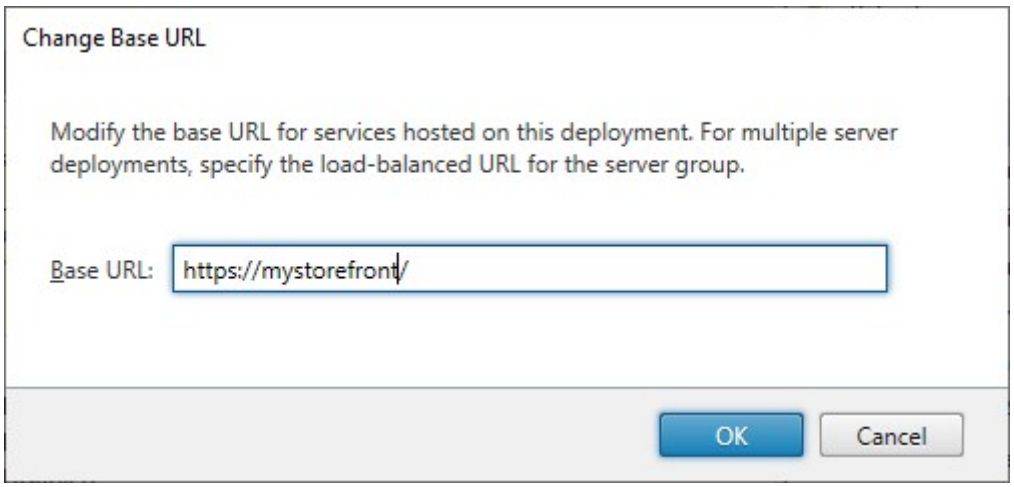


StoreFront サーバーのベース **URL** を **HTTP** から **HTTPS** に変更

最初に SSL 証明書をインストールおよび構成せずに Citrix StoreFront をインストールおよび構成した場合、StoreFront は通信に HTTP を使用します。

後から SSL 証明書をインストールして構成する場合は、次の手順を実行して StoreFront とそのサービスが HTTPS 接続を使用するようにしてください。

1. Citrix StoreFront 管理コンソールの左側のペインで ［サーバーグループ］を選択します。
2. ［操作］ペインの ［ベース **URL** の変更］を選択します。
3. `https:` で始まるベース URL を更新し、［**OK**］をクリックします。



HSTS

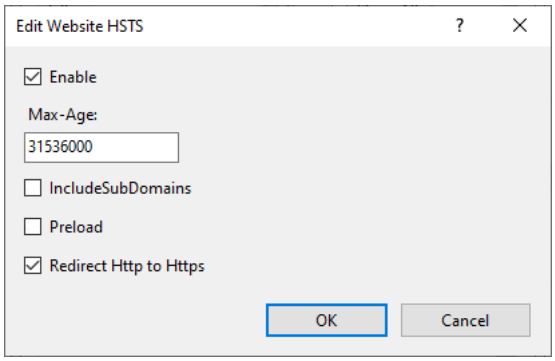
サーバー側で HTTPS を有効にした後でも、ユーザーのクライアントデバイスは脆弱です。たとえば、中間者攻撃者は、StoreFront サーバーになりすましユーザーをだまして、単純な HTTP 経由でなりすましサーバーに接続させる可能性があります。これによって、攻撃者はユーザーの資格情報などの機密情報にアクセスできるようになります。解決策は、ユーザーのブラウザーが HTTP 経由で RfWeb サーバーにアクセスしないようにすることです。これは、HTTP Strict Transport Security（HSTS）を使用することで実現できます。

HSTS が有効になっている場合、サーバーは、Web サイトへの要求は HTTPS 経由でのみ行う必要があることをブラウザーに示します。ユーザーが HTTP を使用して URL にアクセスしようとすると、ブラウザーは自動的に HTTPS の使用に切り替わります。これにより、IIS でのセキュアな接続に関してサーバー側の検証だけでなく、クライアント側の検証も確実に提供されます。ブラウザーは、構成された期間、この検証を提供し続けます。

Windows Server 2019 以降の場合：

1. インターネットインフォメーションサービス（**IIS**）マネージャーを開きます。
2. ［**Default Web Site**］（または適切な Web サイト）を選択します。
3. 右側の［Actions］ペインで、［**HSTS**…］をクリックします。

4. [**Enable**] にチェックを入れ、最大有効期間（例：1 年間の場合は 31536000）を入力し、[**Redirect HTTP to HTTPS**] にチェックを入れます。
5. [**OK**] を押します



> 注:
>
> HSTS を有効にすると、同じドメインのすべての Web サイトに影響します。たとえば、https://www.company.com/Citrix/StoreWebの Web サイトにアクセスできる場合、HSTS ポリシーはhttps://www.company.comの下のすべての Web サイトに適用されますが、これは望ましくない場合があります。

StoreFront 展開環境のセキュリティ

June 6, 2024

このトピックでは、StoreFront の展開および構成時に使用すべき、システムのセキュリティを保護するための機能について説明します。

エンドユーザーと StoreFront の通信

ユーザーデバイスと StoreFront の間の通信は、HTTPS で保護することをお勧めします。これにより、クライアントと StoreFront の間で送信されるパスワードおよびその他のデータが確実に暗号化されます。さらに、単純な HTTP 接続は、中間者攻撃などのさまざまな攻撃によって危険にさらされる可能性があります。特に、接続が公衆 Wi-Fi ホットスポットなどの安全はでない場所から行われる場合はその危険性があります。IIS で HTTPS が構成されていない場合、StoreFront の通信に HTTP が使用されます。

構成に応じて、ユーザーはゲートウェイまたはロードバランサー経由で StoreFront にアクセスできます。HTTPS 接続はゲートウェイまたはロードバランサーで終了できます。ただし、この場合でも、HTTPS を使用してゲートウェイまたはロードバランサーと StoreFront 間のセキュリティで保護された接続を確保することをお勧めします。

HTTPS を有効にし、HTTP を無効にし、HSTS を有効にするには、「HTTPS による StoreFront のセキュリティ保護」を参照してください。

StoreFront と **Citrix Virtual Apps and Desktops** サーバーとの通信

StoreFront と Citrix Virtual Apps and Desktops の Delivery Controller の間で通信されるデータを保護するために、HTTPS プロトコルを使用することをお勧めします。「TLS サーバー証明書の Controller へのインストール」を参照してください。StoreFront は、StoreFront と Delivery Controller 間で TLS 1.0 または TLS 1.1 プロトコルをサポートしません。代わりに、IPSec を使用してサーバー間の通信を保護するように Windows を構成することができます。

信頼できる StoreFront サーバーのみが Delivery Controller と通信できるように Delivery Controller と StoreFront を構成できます。「セキュリティキーの管理」を参照してください。

StoreFront と **Cloud Connector** の通信

StoreFront と Cloud Connector 間でデータの受け渡しを保護するには、HTTPS プロトコルを使用することをお勧めします。「Cloud Connector で SSL を有効にして XML トラフィックを保護する方法」を参照してください。StoreFront は、StoreFront と Cloud Connector 間で TLS 1.0 または TLS 1.1 プロトコルをサポートしません。代わりに、IPSec を使用してサーバー間の通信を保護するように Windows を構成することができます。

リモートアクセス

Citrix では、StoreFront サーバーをインターネットに直接公開することはお勧めしません。リモートユーザーに認証とアクセスを提供するには、Citrix Gateway を使用することをお勧めします。

Microsoft インターネットインフォメーションサービス（**IIS**）のセキュリティ強化

制限された IIS 構成で StoreFront を構成できます。これはデフォルトの IIS 構成ではありません。

ファイル拡張子

要求フィルターを使用して、許可されるファイル拡張子の一覧を構成し、一覧にないファイル名拡張子を禁止にできます。IIS のドキュメントを参照してください。

StoreFront では、次のファイル名拡張子が必要です：

- .（空白の拡張子）
- .appcache
- .aspx
- .cr
- .css
- .dtd

- .png
- .htm
- .html
- .ica
- .ico
- .jpg
- .js
- .png
- .svg
- .txt
- .xml

ストア Web サイトで Citrix Workspace アプリのダウンロード/アップグレードが有効になっている場合、StoreFront では次のファイル拡張子も必要です:

- .dmg
- .exe

HTML5 向け Citrix Workspace アプリが有効になっている場合、StoreFront では次のファイル拡張子も必要です:

- .eot
- .ttf
- .woff
- .wasm

動詞

要求フィルターを使用して、許可される動詞の一覧を構成し、一覧にない動詞を禁止にできます。IIS のドキュメントを参照してください。

- GET
- POST
- HEAD

URL 内の非 **ASCII** 文字

ストア名と Web サイト名に ASCII 文字のみを使用する場合、StoreFront URL には ASCII 文字が含まれません。要求フィルターを使用して、非 ASCII 文字を禁止にできます。IIS のドキュメントを参照してください。

MIME タイプ

以下のファイル拡張子に対応する OS シェルの MIME タイプを削除できます:

- .exe
- .dll
- .com
- .bat
- .csh

IIS のドキュメントを参照してください。

X-Powered-By ヘッダーを削除する

デフォルトでは、IIS は、値`ASP.NET`を含む`X-Powered-By`ヘッダーを追加することで、ASP.NET を使用していることをレポートします。このヘッダーを削除するように IIS を構成できます。IIS のカスタムヘッダーに関するドキュメントを参照してください。

IIS バージョンを使用する **Server** ヘッダーを削除する

デフォルトでは、IIS は`Server`ヘッダーを追加することで、IIS バージョンをレポートします。このヘッダーを削除するように IIS を構成できます。IIS の要求フィルターに関するドキュメントを参照してください。

StoreFront Web サイトを別のパーティションに移動する

StoreFront の Web サイトをシステムファイルとは別のパーティションでホストできます。IIS 内で、StoreFront 展開環境を作成する前に、適切なパーティションで **Default Web Site** を移動するか、別のサイトを作成する必要があります。

IIS の機能

StoreFront によってインストールおよび使用される IIS 機能の一覧については、「システム要件」を参照してください。他の IIS 機能を削除できます。

StoreFront は ISAPI フィルターを直接使用しませんが、この機能は ASP.NET に必要なため、アンインストールできません。

ハンドラーのマッピング

StoreFront には次のハンドラーのマッピングが必要です。他のハンドラーのマッピングは削除できます。

- ExtensionlessUrlHandler-Integrated-4.0
- PageHandlerFactory-Integrated-4.0
- StaticFile

IIS のハンドラーに関するドキュメントを参照してください。

ISAPI フィルター

StoreFront は ISAPI フィルターを必要としません。すべての ISAPI フィルターを削除できます。IIS の ISAPI フィルターに関するドキュメントを参照してください。

.NET 認証の規則

デフォルトでは、IIS サーバーの「.NET 認証の規則」は［すべてのユーザーを許可］に設定されています。デフォルトでは、StoreFront が使用する Web サイトはこの構成を継承します。

サーバーレベルで.NET 認証の規則を削除または変更する場合は、StoreFront が使用する Web サイトの規則を上書きして、「すべてのユーザー」の許可規則を追加し、その他の規則を削除する必要があります。

Retail モード

Retail モードを有効にすることができます。IIS ドキュメントを参照してください。

アプリケーションプール

StoreFront は次のアプリケーションプールを作成します:

- Citrix 構成 API
- Citrix Delivery Services 認証
- Citrix Delivery Services リソース
- および Citrix Receiver for Web

各 IIS アプリケーションが使用するアプリケーションプールや各プールの ID は変更しないでください。複数のサイトを使用している場合、各サイトが個別のアプリケーションプールを使用するように構成することはできません。

リサイクル設定では、アプリケーションプールのアイドルタイムアウトと仮想メモリの制限を設定できます。「Citrix Receiver for Web」アプリケーションプールがリサイクルされると、Web ブラウザー経由でログインしているユーザーがログアウトされるため、デフォルトでは、中断を最小限に抑えるために毎日午前 2 時にリサイクルされるように設定されています。リサイクル設定のいずれかを変更すると、ユーザーはその日の別の時間にログオフされる可能性があります。

必要な設定

- IIS 認証設定は変更しないでください。StoreFront は認証を管理し、StoreFront サイトのディレクトリを適切な認証設定で構成します。
- **SSL** 設定の StoreFront サイトで［**Client certificates: Require**］を選択しないでください。StoreFront のインストールでは、この設定で StoreFront サイトの適切なページを構成します。
- StoreFront では、セッション状態およびその他の機能に Cookie が必要です。特定のディレクトリでは、［**Session State**］、［**Cookie Settings**］、［**Mode**］を ［**Use Cookies**］に設定する必要があります。
- StoreFront では、［**.NET** 信頼レベル］を ［**Full Trust**］に設定する必要があります。.NET 信頼レベルを他の値に設定しないでください。

Services

StoreFront をインストールすると、次の Windows サービスが作成されます:

- Citrix Configuration Replication（NT SERVICE\CitrixConfigurationReplication）
- Citrix Cluster Join（NT SERVICE\CitrixClusterService）
- Citrix Peer Resolution（NT SERVICE\Citrix Peer Resolution Service）
- Citrix Credential Wallet（NT SERVICE\CitrixCredentialWallet）
- Citrix Subscriptions Store（NT SERVICE\CitrixSubscriptionsStore）
- Citrix Default Domain Services（NT SERVICE\CitrixDefaultDomainService）

これらのアカウントは `Network Service`としてログオンします。この構成は変更しないでください。

XenApp 6.5 に StoreFront Kerberos 制約付き委任を構成すると、さらに Citrix StoreFront Protocol Transition サービス（NT SERVICE\CitrixStoreFrontProtocolTransition）が作成されます。このサービスは`NT AUTHORITY\SYSTEM`として実行されます。この構成は変更しないでください。

ユーザー権限の割り当て

ユーザー権限の割り当てをデフォルトから変更すると、StoreFront で問題が発生する可能性があります。特に次の点を確認します:

- Microsoft IIS は、StoreFront がインストールされると有効化されます。Microsoft IIS により、組み込みグループ IIS_IUSRS にはバッチジョブとしてログオンするログオン権限、および認証後にクライアントを偽装する特権が付与されます。これは Microsoft IIS がインストールされるときの通常動作です。これらのユーザー権利は変更しないでください。詳しくは、Microsoft のドキュメントを参照してください。
- StoreFront がインストールされると、アプリケーションプールが作成され、IIS によってサービスとしてログオン、プロセスのメモリクォータの増加、セキュリティ監査の生成、およびプロセスレベルトークンの置き換えのユーザー権限が付与されます。

- 展開を作成または変更するには、管理者はファイルとディレクトリを復元する権限を持っている必要があります。
- サーバーをサーバーグループに参加させるには、Administrators グループにファイルとディレクトリの復元、ネットワーク経由でのコンピューターへのアクセス、および監査とセキュリティログの管理の権限が必要です。
- ユーザーがユーザー名とパスワード認証（直接または Gateway 経由）を使用してログオンするには、StoreFront が Delivery Controller 経由でパスワードを検証するように構成していない限り、「ローカルのログオンを許可する」権限を持っている必要があります。

これは包括的な一覧ではないため、これ以外のユーザーのアクセス権限が必要になる場合があります。

グループメンバーシップの構成

StoreFront サーバーグループを構成すると、次のサービスが管理者セキュリティグループに追加されます：

- Citrix Configuration Replication（NT SERVICE\CitrixConfigurationReplication）
- Citrix Cluster Join（NT SERVICE\CitrixClusterService）。このサービスはグループに属するサーバーでのみ表示され、参加処理中にのみ実行されます。

StoreFront が正しく動作して次の操作を行うには、これらのグループメンバーシップが必要です：

- 証明書の作成、エクスポート、インポート、削除、および証明書へのアクセス権限の設定
- Windows レジストリの読み取りおよび書き込み
- Global Assembly Cache（GAC）での Microsoft .NET Framework アセンブリの追加および削除
- フォルダー **Program Files\Citrix**<*StoreFrontLocation*> へのアクセス
- IIS アプリプール ID および IIS Web アプリケーションの追加、変更、削除
- ローカルセキュリティグループおよびファイアウォールルールの追加、変更、削除
- Windows サービスと PowerShell スナップインの追加および削除
- Microsoft Windows Communication Framework（WCF）エンドポイントの登録

上記操作の一覧は、StoreFront の更新プログラムで予告なく変更されることがあります。

StoreFront をインストールすると、以下のセキュリティグループも作成されます：

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSReplicators
- CitrixPNRSUsers
- CitrixStoreFrontAdministrators
- CitrixSubscriptionServerUsers

- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers

StoreFront は、これらのセキュリティグループのメンバーシップを保持します。メンバーシップは StoreFront 内でのアクセス制御のために使用され、ファイルやフォルダーなどの Windows リソースには適用されません。このグループメンバーシップは変更しないでください。

NTLM

StoreFront は、サーバーグループ内のサーバー間の認証に NTLM を使用します。NTLM を無効にすると、StoreFront はサーバーグループ内の StoreFront サーバー間でデータを同期できなくなります。

NTLMv2 のみを使用し、NTLMv1 を拒否するようにサーバーを構成できます。Microsoft のドキュメントを参照してください。

StoreFront での証明書

サーバー証明書

StoreFront では、コンピューターの識別と Transport Layer Security（TLS）通信の保護のためにサーバー証明書を使用します。ICA ファイルの署名機能を有効にする場合は、StoreFront で証明書を使用して ICA ファイルをデジタル署名することもできます。

詳しくは、「エンドユーザーと StoreFront の通信」および「ICA ファイルの署名」を参照してください。

トークン管理の証明書

認証サービスとストアのそれぞれに、トークン管理のための証明書が必要です。認証サービスまたはストアを作成すると、StoreFront により自己署名証明書が生成されます。StoreFront により生成される自己署名証明書をほかの用途で使用しないでください。

Citrix Delivery Services の証明書

StoreFront は、カスタムの Windows 証明書ストア（Citrix Delivery Services）に、いくつかの証明書を保持しています。Citrix Configuration Replication サービス、Citrix Credential Wallet サービス、および Citrix Subscriptions Store サービスは、これらの証明書を使用します。クラスター内の各 StoreFront サーバーは、これらの証明書のコピーを持っています。これらのサービスはセキュアな通信に TLS を使用せず、これらの証明書は TLS サーバー証明書として使用されません。これらの証明書は、StoreFront ストアの作成時または StoreFront のインストール時に作成されます。この Windows 証明書ストアのコンテンツは変更しないでください。

コード署名証明書

StoreFront は、*<InstallDirectory>*\Scripts のフォルダーに多数の PowerShell スクリプト（.ps1）を含みます。デフォルトの StoreFront インストールでは、これらのスクリプトは使用されません。これらのスクリプトにより、特殊で低頻度のタスクの構成手順が簡素化されます。スクリプトは署名されているため、StoreFront で PowerShell 実行ポリシーをサポートできるようになります。**AllSigned** ポリシーをお勧めします（PowerShell スクリプトの実行が妨げられるため、**Restricted** ポリシーはサポートされていません）。StoreFront は PowerShell 実行ポリシーを変更しません。

StoreFront では信頼できる発行元ストアにコード署名証明書はインストールされませんが、Windows でコード署名証明書を自動的に追加することができます。これは、PowerShell スクリプトが **Always run** オプションで実行されることで、可能になります。（**Never run** オプションを選択すると、信頼されていない証明書ストアに証明書が追加され、StoreFront PowerShell スクリプトは実行されません）。コード署名証明書が信頼された発行元ストアに追加されると、Windows は有効期限を確認しなくなります。StoreFront タスクが完了したら、信頼できる発行元ストアからこの証明書を削除できます。

従来の **TLS** バージョンの無効化

Windows サーバー上のクライアント通信とサーバー通信の両方で TLS 1.0 および 1.1 を無効にすることをお勧めします。これは、グループポリシーを使用するか、Windows レジストリ設定を使用して実行することができます。Microsoft のドキュメントを参照してください。

StoreFront のセキュリティ境界による分離

StoreFront と同じ Web ドメイン（ドメイン名とポート）に Web アプリケーションを展開すると、これらの Web アプリケーションの脆弱性により StoreFront 展開環境全体のセキュリティが低下する可能性があります。セキュリティ境界を分離してセキュリティを強化するため、Web アプリケーションと異なる Web ドメインに StoreFront を展開することをお勧めします。

ICA ファイルの署名

StoreFront には、サーバー上の特定の証明書を使用して ICA ファイルをデジタル署名するオプションがあり、この機能をサポートするバージョンの Citrix Workspace アプリでは、ファイルの発行元を信頼できるかどうかを検証できます。SHA-1 や SHA-256 など、StoreFront サーバーのオペレーティングシステムでサポートされるどのハッシュアルゴリズムでも、ICA ファイルを署名できます。詳しくは、「ICA ファイル署名の有効化」を参照してください。

ユーザーによるパスワードの変更

Active Directory ドメインの資格情報を使用して Web ブラウザー経由でログオンするユーザーが、必要に応じてパスワードを変更できるように設定することができます。ただし、その認証サービスを使用するストアにアクセスでき

るすべてのユーザーに、慎重に扱うべきセキュリティ機能が公開されることになります。組織のセキュリティポリシーにより、ユーザーパスワード変更機能が内部使用のみに制限される環境では、社内ネットワークの外側からそれらのストアにアクセスできないことを確認してください。認証サービスを作成したときのデフォルトの構成では、パスワードが失効しても、ユーザーはパスワードを変更できません。詳しくは、「ユーザーがパスワードを変更できるようにする」を参照してください。

カスタマイズ

セキュリティ強化のため、自分が管理していないサーバーからコンテンツまたはスクリプトをロードするカスタマイズは行わないでください。コンテンツまたはスクリプトは、カスタマイズを行う Web サイトのカスタムフォルダーにコピーしてください。StoreFront が HTTPS 接続用に構成されている場合、カスタムコンテンツやカスタムスクリプトへのリンクもすべて HTTPS を使用していることを確認してください。

セキュリティヘッダー

Web ブラウザーでストア Web サイトを表示すると、StoreFront は Web ブラウザーに制限を適用する次のセキュリティ関連ヘッダーを返します。

ヘッダー名	値	説明
`content-security-policy`	`frame-ancestors 'none'`	これにより、他のサイトが StoreFront Web サイトをフレーム内に埋め込むことができなくなり、クリックジャッキング攻撃が回避されます。StoreFront はインラインスクリプトとスタイルを使用するため、これらをブロックする content-security-policy を使用することはできません。StoreFront Web サイトには管理者が設定したコンテンツのみが表示され、ユーザーが入力したコンテンツは表示されないため、インラインスクリプトをブロックする必要はありません。
`X-Content-Type-Options`	`nosniff`	これにより、MIME タイプのスニッフィングが回避されます。

ヘッダー名	値	説明
X-Frame-Options	deny	これにより、他のサイトがStoreFront Web サイトをフレーム内に埋め込むことができなくなり、クリックジャッキング攻撃が回避されます。この機能は、content-security-policyによって廃止されframe-ancestors 'none'になりましたが、content-security-policyをサポートしていない一部の古いブラウザーでは認識されます
X-XSS-Protection	1; mode=block	XSS（クロスサイトスクリプティング）攻撃を軽減するために一部のブラウザーで使用されます

Cookies

StoreFront は複数の Cookie を使用します。Web サイトの運営に使用される Cookie の一部は次のとおりです:

Cookie	説明
ASP.NET_SessionId	認証状態を含むユーザーのセッションを追跡します。HttpOnlyが設定されています。
CtxsAuthId	セッション固定攻撃を防ぐために、StoreFront はさらに、この Cookie を使用してユーザーが認証されているかどうかを追跡します。HttpOnlyが設定されています。
CsrfToken	標準のCookie からヘッダーへのトークンパターンによるクロスサイトリクエストフォージェリを防ぐために使用されます。サーバーは Cookie にトークンを設定します。クライアントは Cookie からトークンを読み取り、そのトークンをクエリ文字列またはその後の要求のヘッダーに含めます。この Cookie は、クライアントの JavaScript が読み取ることができるように、HttpOnlyが設定されていないことが必要です。
CtxsDeviceId	デバイスを識別します。HttpOnlyが設定されています。

StoreFront は、ユーザーの状態を追跡するために他の多くの Cookie を設定します。Cookie のうちのいくつかは JavaScript によって読み取られる必要があるため、`HttpOnly`を設定しません。これらの Cookie には、認証に関する情報やその他の機密情報は含まれません。

セキュリティに関する詳細

> 注:
>
> この情報は予告なく変更されることがあります。

規制上の理由から、StoreFront のセキュリティスキャンを実行することをお勧めします。上記の設定オプションを使用することで、セキュリティスキャンの検出結果の一部をレポートから除外することができます。

セキュリティスキャナーと StoreFront の間にゲートウェイが介在している場合、検出結果のあるものは StoreFront 自体ではなくゲートウェイに関連する発見である可能性があります。セキュリティスキャンのレポートでは通常これらの発見は区別されません（たとえば、TLS 構成）。そのため、セキュリティスキャンレポートの技術的な説明により誤解が生じるおそれがあります。

メールアドレスによるアカウント検出

June 6, 2024

メールアドレスによるアカウント検出を有効にすると、デバイスに Citrix Workspace アプリを新規インストールしたユーザーが、ストア URL を知らなくても自分のメールアドレスを入力することでアカウントを自動的にセットアップできます。

Citrix Workspace アプリの初回構成時に、ユーザーのメールアドレスまたはストアの URL を入力するためのダイアログボックスが開きます。ユーザーがメールアドレスを入力すると、Citrix Workspace アプリは複数の場所でメールドメインを検索し、StoreFront サーバーを特定します。次に、表示されているすべてのストアをユーザーが選択できるように一覧にまとめます。

Global App Config Service を使用してメール検出を構成することをお勧めします。または、DNS SVR レコードまたは DNS エイリアスのいずれかを使用してメール検出を構成できます。

Global App Config Service

Glboal App Cofig Service を使用してメール検出を構成するには、「メールアドレスによる検出をセットアップする」を参照してください。

DNS SVR レコード

Global App Config Service の代わりに、DNS SVR レコードを使用して、Citrix Workspace アプリがメールドメインに対してどの StoreFront サーバーを使用するかを構成できます。

お使いのメールドメインの DNS サーバーに、次のプロパティを持つ **SRV** レコードを追加します。

プロパティ	値
サービス	_citrixreceiver
Proto	TCP
ターゲット	Citrix Gateway アプライアンス（ローカルおよびリモートのユーザーをサポートする場合）または StoreFront サーバー（ローカルユーザーのみをサポートする場合）の、*servername.domain:port* 形式での完全修飾ドメイン名とポート。

内部 DNS サーバーと外部 DNS サーバーの両方が環境に含まれている場合は、StoreFront サーバーの FQDN を指定する SRV レコードを内部 DNS サーバーに追加し、Citrix Gateway の FQDN を指定する別の SRV レコードを外部サーバーに追加することができます。この構成により、リモートユーザーには Citrix Gateway の接続情報が提供され、ローカルユーザーには StoreFront の接続情報が提供されます。

DNS DiscoverReceiver レコード

他の方法へのフォールバックとして、メールドメイン上の StoreFront サーバー`discoverReceiver`への DNS エイリアスを作成できます。たとえば、メールドメインが`example.com`の場合、`discoverReceiver.example.com`という DNS エイリアスを作成します。指定されたドメインに SRV レコードが見つからない場合、Citrix Workspace アプリは「discoverReceiver」という名前のマシンを検索して StoreFront サーバーを検出します。

このメカニズムを使用する場合は、StoreFront サーバーの HTTPS 証明書にサブジェクトの別名として`discoverReceiver`が含まれていることを確認してください。

新しい展開環境の作成

June 6, 2024

1. 新しいサーバー上で Citrix StoreFront 管理コンソールを開きます。これを行うには、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。

2. Citrix StoreFront 管理コンソールの結果ペインで、［新しい展開環境の作成］をクリックします。
3. 複数の IIS サイトがある場合は、**IIS** サイトのドロップダウンから使用するサイトを選択します。
4. 単一の StoreFront サーバーを使用する場合は、サーバー URL の ［ベース **URL**］を入力します。ロードバランサーの背後に複数の StoreFront サーバーを構成する場合は、負荷分散の URL を ［ベース **URL**］として入力します。

   負荷分散環境をセットアップしていない場合は、サーバーの URL を入力します。展開環境のベース URL はいつでも変更できます。
5. ［次へ］をクリックし、「ストアの作成」の説明に従って最初のストアを構成します。
6. すべての構成手順が完了したら、［作成］をクリックして展開環境とストアを作成します。
7. StoreFront は、作成したストアの概要を表示します。［完了］をクリックします。

PowerShell SDK を使用して新しい展開環境を作成する

PowerShell SDKを使用して展開環境を作成するには、コマンドレットAdd-STFDeploymentを呼び出します。

複数のインターネットインフォメーションサービス（**IIS**）**Web** サイト

StoreFront では、Windows サーバーごとに異なる IIS Web サイトで異なるストアを展開できます。これによって、ストアごとにそれぞれホスト名と証明書のバインドを持つことができます。

複数の Web サイトを作成するには、Microsoft IIS のドキュメントを参照してください。

管理コンソールを使用して複数の StoreFront 展開環境を作成することはできません。PowerShell SDK を使用する必要があります。たとえば、アプリケーション用とデスクトップ用の 2 つの IIS Web サイト展開を作成するには、次のコマンドを使用します:

```
Add-STFDeployment -SiteID 1 -HostBaseURL "https://apps.example.com"
Add-STFDeployment -SiteID 2 -HostBaseURL "https://desktops.example.com"
<!--NeedCopy-->
```

複数のサイトを有効にすると、StoreFront は管理コンソールを無効にし、StoreFront を単一サイトモードに戻すことはできなくなります。StoreFront SDK を使用してサイトを構成し、各コマンドに`SiteID`を含める必要があります。

既存のサーバーグループへの参加

June 6, 2024

グループに追加するサーバーに StoreFront をインストールする前に、次のことを確認してください:

- グループに追加するサーバーのオペレーティングシステムのバージョンおよびロケール設定が、グループ内のほかのサーバーと同じであることを確認してください。StoreFront サーバーグループ内でオペレーティングシステムのバージョンやロケール設定が異なるサーバーを混在させることはサポートされていません。
- 追加するサーバーの StoreFront の IIS での相対パスは、グループ内のほかのサーバーと同じです。

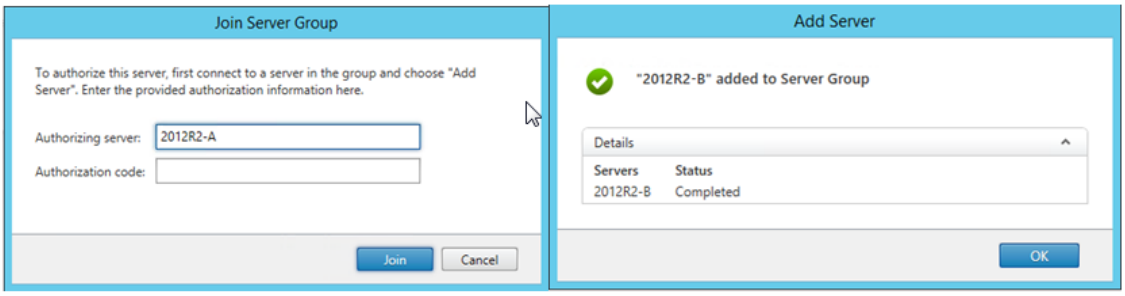
> 注:
>
> サーバーグループのサイズに関する推奨事項については、「StoreFront サーバーグループ」を参照してください。

追加する StoreFront サーバーがサーバーグループに属していて削除された場合、同じサーバーグループまたは異なるサーバーグループに再度追加される前に、出荷時のデフォルト設定にリセットする必要があります。「サーバーを出荷時のデフォルト設定にリセット」を参照してください。

> 重要:
>
> サーバーグループに新しいサーバーを追加すると、そのサーバーのローカル管理者グループにいくつかの StoreFront サービスアカウントが追加されます。これは、サーバーグループに参加したり情報を同期したりするために、これらのサービスでローカル管理者権限が必要になるためです。グループポリシーでローカル管理者グループへのアカウントの追加が禁止されている場合、またはサーバーのローカル管理者グループの権限が制限されている場合、StoreFront でサーバーをサーバーグループに追加できません。

1. 新しいサーバー上で Citrix StoreFront 管理コンソールを開きます。これを行うには、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。
2. Citrix StoreFront 管理コンソールの結果ペインで、［既存のサーバーグループへの参加］をクリックします。
3. 参加する StoreFront 展開環境のサーバーにログオンし、Citrix StoreFront 管理コンソールを開きます。コンソールの左ペインで［サーバーグループ］ノードを選択して、［操作］ペインで ［サーバーの追加］をクリックします。表示される承認コードをメモしておきます。
4. 新しいサーバーに戻り、［サーバーグループへの参加］ダイアログボックスの［承認サーバー］ボックスに、既存のサーバーの名前を指定します。そのサーバーから取得した承認コードを入力して ［参加］をクリックします。

   サーバーを既存のグループに追加すると、そのサーバーの構成がグループの既存のサーバーの構成と一致するように更新されます。また、グループ内のほかのすべてのサーバーは、新しいサーバーの詳細情報で更新されます。



複数サーバー展開環境を管理する場合、同時に複数のサーバー上で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。また、展開環境内で一貫した構成を保つため、構成の変更内容をグループ内のほかのサーバーに反映させる必要があります。

StoreFront のアップグレード

June 6, 2024

アップグレードすると、StoreFront 構成が保存され、ユーザーのお気に入りがそのまま残ります。一方、StoreFront のアンインストールは、StoreFront および関連サービス、サイト、お気に入り（スタンドアロンサーバーの場合）、関連構成を削除します。

アップグレードパスのサポート

以下から StoreFront 2402 にアップグレードできます:

- StoreFront 2311
- StoreFront 2308
- StoreFront 2203 LTSR（いずれかの CU）
- StoreFront 1912 LTSR（初期リリースまたはいずれかの CU）
- StoreFront 3.12 LTSR CU9

3.12 CU9 より前のバージョンからアップグレードするには、まず StoreFront 3.12 CU9 にアップグレードする必要があります。

> 警告:
>
> 1912 以前のバージョンからアップグレードすると、展開内のデスクトップアプライアンスサイトは自動的に削除されます。代わりに、Citrix ではドメイン不参加のユースケースでは「Citrix Workspace アプリ Desktop Lock」を使用することをお勧めします。

ヒント

- 製品終了（EOL）になった古い StoreFront から最新リリースへのアップグレードはサポートされていません。詳しくは、CTX200356を参照してください。
- StoreFront では、複数の製品バージョンが混在する複数サーバーの展開環境がサポートされないため、サーバーグループ内のすべてのサーバーを同じバージョンにアップグレードしてから、ユーザーが展開環境にアクセスできるようにしてください。

- 複数サーバー展開環境では、同時アップグレードはサポートされません。各サーバーを順番にアップグレードする必要があります。
- StoreFront のアップグレードを実行する前に、アップグレード前チェックを実行します。アップグレード前チェックが失敗した場合、アップグレードは開始されず、エラーに関する通知が表示されます。StoreFront のインストールは変更されません。エラーの原因を修復してから、アップグレードに戻ります。
- StoreFront のアップグレード自体が失敗すると、既存の StoreFront のインストールで初期構成が失われる可能性があります。StoreFront のインストールを機能する状態に復元してから、アップグレードを再度実行してください。StoreFront を機能する状態に復元するには、次の方法を検討してください:
  - アップグレード前に作成した仮想マシンスナップショットを復元する、
  - アップグレード前にエクスポートした StoreFront 構成をインポートする（「StoreFront 構成のエクスポートとインポート」を参照）、
  - 「StoreFront のアップグレードの問題に関するトラブルシューティング」のトラブルシューティング方法を実行する。
- Citrix Virtual Apps and Desktops Metainstaller で StoreFront のアップグレードが失敗した場合、ダイアログで報告され関連するエラーログへのリンクが記載されます。

アップグレードの準備

アップグレードを開始する前に、アップグレードの失敗を防ぐために次の手順の実行をお勧めします:

- アップグレード前にバックアップを計画します。
- StoreFront の製品終了となったバージョンからアップグレードしようとしていないことを確認してください。詳しくは、CTX200356を参照してください。
- サポートされているバージョンの StoreFront から最新バージョンにのみアップグレードしていることを確認してください。
- StoreFront インストーラーを Citrix Web サイトからダウンロードします。

単一の **StoreFront** サーバーのアップグレード

1. 仮想マシンスナップショットを作成してサーバーのバックアップを作成します。
2. 既存の StoreFront 構成をエクスポートします。サーバーグループに複数のサーバーがある場合は、1 つのサーバーからのみサーバーグループ構成をエクスポートします。サーバー間ですべての変更を伝達していることを前提としているため、サーバーグループ内のすべてのサーバーは同一コピーの構成を維持します。このバックアップにより、新しいサーバーグループを簡単に構築できるため、問題が発生した場合でも構成を簡単に復元できます。このバックアップは、エクスポート元と同じバージョンを実行しているサーバーにのみ復元できます。
3. default.ica や usernamepassword.tfrm など、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`のファイルを変更した場合は、ストアごとにバックアップを作成します。アップグレード後はそれらを復元して、変更内容を元に戻すことができます。

4. ロードバランサーからサーバーを削除するか、接続をブロックすることにより、ユーザーが接続できないようにします。
5. サーバーを再起動します:
6. StoreFront 管理コンソール、コマンドライン、PowerShell ウィンドウなど、StoreFront ファイルをロックする可能性のあるすべてのアプリケーションが実行されていないことを確認してください。これにより、アップグレード時にインストーラーがすべての StoreFront ファイルに確実にアクセスできるようになります。インストーラーがファイルにアクセスできない場合、それらのファイルを置き換えることができないため、アップグレードに失敗して既存の StoreFront 構成が削除されます。
7. StoreFront ファイルを含んでいるディレクトリで Windows エクスプローラーやコマンドプロンプトが開いていないことを確認してください
8. ウイルス対策アプリケーションをすべて無効にします。
9. 必要なバージョンの StoreFront 用のインストールファイルを実行します。

StoreFront サーバーグループをアップグレードするには

StoreFront サーバーグループのアップグレードでは、いずれかのサーバーを使用して他のサーバーをグループから削除します。削除されたサーバーは、グループに関連する構成を保持しているため、新しいサーバーグループに参加できなくなります。新しいサーバーグループを構築するために再利用する前に、またはスタンドアロンの StoreFront サーバーとして再利用する前に、削除されたサーバーを出荷時のデフォルト設定にリセットするか、または StoreFront に再インストールする必要があります。StoreFront サーバーグループのサーバーの同時アップグレードはサポートされていません。

例 **1**: スケジュールされたメンテナンスダウンタイム中に **3** ノードの **StoreFront** サーバーグループをアップグレードします

スケジュールされたダウンタイム中に、3 台のサーバー A、B、C による StoreFront サーバーグループをアップグレードします。

1. 負荷分散 URL を無効にして、サーバーグループへのユーザーアクセスを無効にします。これにより、ユーザーがアップグレードプロセス中に展開環境に接続できなくなります。
2. サーバー A を使用して、サーバー B と C をグループから削除します。

   サーバー B と C は、サーバーグループから「孤立」しています。
3. 「単一の StoreFront サーバーのアップグレード」の手順に従って、サーバー A をアップグレードします。
4. サーバー A が正常にアップグレードされたことを確認してください。
5. サーバー B と C で、現在インストールされている StoreFront をアンインストールし、新しいバージョンの StoreFront をインストールします。

6. アップグレードされたサーバーグループを作成するために、アップグレードされたサーバー A にサーバー B と C を参加させます。このサーバーグループは、アップグレードされた 1 台のサーバー（A）と 2 台の新しくインストールされたサーバー（B と C）で構成されています。

   既存のサーバーグループへの参加プロセスは自動的にすべての構成データとサブスクリプションデータを新しいサーバー B と C に伝達します。

7. すべてのサーバーが正しく機能していることを確認してください。
8. 負荷分散 URL を有効にして、アップグレードされたサーバーグループへのユーザーアクセスを有効にします。

例 **2**: スケジュールされたダウンタイムなしで **3** ノードの **StoreFront** サーバーグループをアップグレードします

スケジュールされたダウンタイムなしで、3 台のサーバー A、B、C による StoreFront サーバーグループをアップグレードします。

サーバーグループをアップグレードする前に、以下を実行します:

1. **Export-STFConfiguration** を使用して、StoreFront 構成をエクスポートします。このバックアップは、サーバーがプロセスの後半で工場出荷時設定にリセットされて構成データが削除されてしまうため、必要になります。
2. **Export-STFStoreSubscriptions** を使用してサーバー A からサブスクリプションデータをエクスポートします。このバックアップは、サーバーがプロセスの後半で工場出荷時設定にリセットされてサブスクリプションデータが削除されてしまうため、必要になります。「ストアのサブスクリプションデータの管理」を参照してください。
3. サーバー C をロードバランサーから削除して、サーバー C へのユーザーアクセスを無効にします。これにより、ユーザーはアップグレードプロセス中にサーバー C に接続できなくなります。ロードバランサーはサーバー A と B に要求を送信し続けます。
4. グループからサーバー C を削除するには、サーバー A を使用します。
   サーバー A と B は、引き続きユーザーのリソースへのアクセスを提供します。サーバー C はサーバーグループから孤立し、工場出荷時設定にリセットされました。
5. **Clear-STFDeployment** を使用して、孤立したサーバー C を出荷時のデフォルト設定にリセットします。
6. **Import-STFConfiguration** を使用して、以前にサーバー C にエクスポートしたことがあるStoreFront 構成をインポートします。これで、サーバー C は以前のサーバーグループと同じ構成になります。後からこの手順を繰り返す必要はありません。必要なのはサーバー 1 台分の構成データのコピーであり、グループに参加しているその他のサーバーにはデータが伝達されます。
7. 「単一の StoreFront サーバーのアップグレード」の手順に従って、サーバー C をアップグレードします。これで、サーバー C は以前のサーバーグループと同じ構成になり、新しいバージョンの StoreFront にアップグレードされます。
8. 以前にサーバー C にエクスポートしたサブスクリプションデータをインポートします。後からこの手順を繰り返す必要はありません。必要なのはサーバー 1 台分のサブスクリプションデータのコピーであり、グループに参加しているその他のサーバーにはデータが伝達されます。

9. サーバー B を使用して、手順 3、4、5、7 を繰り返します（手順 6 は繰り返さないでください）。この間、ユーザーはサーバー A のリソースにのみアクセスできます。そのためこの手順は、StoreFront サーバーグループの負荷が最小になると予想される、作業の少ない期間に実行することをお勧めします。
10. 既存のサーバーグループへの参加プロセスを使用して、サーバー B をサーバーグループ C に参加させます。これにより、StoreFront の現在のバージョンで単一サーバー（サーバー A）を、StoreFront の新しいバージョンで新しい 2 ノードサーバーグループ（サーバー B および C）を展開できます。
11. サーバー B と C を負荷分散サービスに追加にして、サーバー A から引き継ぐことができるようにします。
12. サーバー A をロードバランサーから削除して、ユーザーが新しくアップグレードされたサーバー B および C に接続されるようにします。
13. サーバー A を使用して、手順 3、4、5、7 を繰り返します（手順 6 は繰り返さないでください）。サーバーグループのアップグレードプロセスが完了すると、サーバー A、B、C には、元のグループと同じ構成およびサブスクリプションデータが配置されます。

> 注：
>
> サーバー A が唯一アクセス可能なサーバーである短い期間中に、サブスクリプションが失われる可能性があります（手順 9）。これによって、アップグレード後の新しいサーバーグループに存在するサブスクリプションデータベースが比較的古いものになり、新しいサブスクリプションレコードはすべて失われる可能性があります。
>
> サブスクリプションデータはユーザーがログオンしてリソースを起動できるようにするために不可欠な要素ではないため、これによる機能への影響はありません。ただし、サーバー A が工場出荷時の設定にリセットされ、新しくアップグレードされたグループに参加した後で、ユーザーはリソースを再度サブスクライブする必要があります。ダウンタイムなしで StoreFront 実稼働環境をライブでアップグレードすると、多数ではないものの、いくつかのサブスクリプションレコードが失われる可能性があります。

アップグレードが失敗した場合

1. *C:\Windows\Temp\StoreFront* で最新の *CitrixMsi*.log* を開き、例外エラーがないか確認します。

   Thumbs.db Access の例外：原因は *C:\inetpub\wwwroot\citrix* およびそのサブディレクトリ内の *thumbs.db* ファイルです。検出されたすべての *thumbs.db* ファイルを削除します。

   Cannot get exclusive file access \in use の例外：利用可能な場合スナップショット/バックアップを復元するか、サーバーを再起動し、すべての StoreFront サービスを手動で停止します。

   Service cannot be started の例外：利用可能な場合スナップショット/バックアップを復元するか、（クライアントプロファイルではなく）.NET framework 4.5 のフルバージョンをインストールします。

2. *CitrixMsi*.log* に例外エラーがない場合、サーバーの ［イベントビューアー］ **>** ［デリバリーサービス］で上記の例外エラーメッセージが含まれるエラーがないか確認します。対応するアドバイスを実行します。

3. イベントビューアーに例外エラーがない場合、Admin ログの *C:\ProgramFiles\Citrix\Receiver StoreFront\logs* で上記の例外エラーメッセージが含まれるエラーがないか確認します。対応するアドバイスを実行します。

ログファイルについて詳しくは、「インストールログ」を参照してください。

サーバーを出荷時のデフォルト設定にリセット

June 6, 2024

場合によっては、StoreFront インストールを初期インストール状態にリセットする必要があります。これは、StoreFront サーバーをサーバーグループに再度追加する前などに必要です。

手動でアンインストールおよび再インストールすることはできますが、時間がかかり、予期しない問題を引き起こす可能性があります。代わりに、**Clear-STFDeployment** PowerShell コマンドレットを実行して、StoreFront サーバーを出荷時のデフォルト設定にリセットできます。

1. StoreFront 管理コンソールが閉じられていることを確認してください。
2. PowerShell ISE を開き、［管理者として実行］を選択します。
3. PowerShell パスを設定します:

```
1 $env:PSModulePath = [Environment]::GetEnvironmentVariable('
     PSModulePath','Machine')
2 <!--NeedCopy-->
```

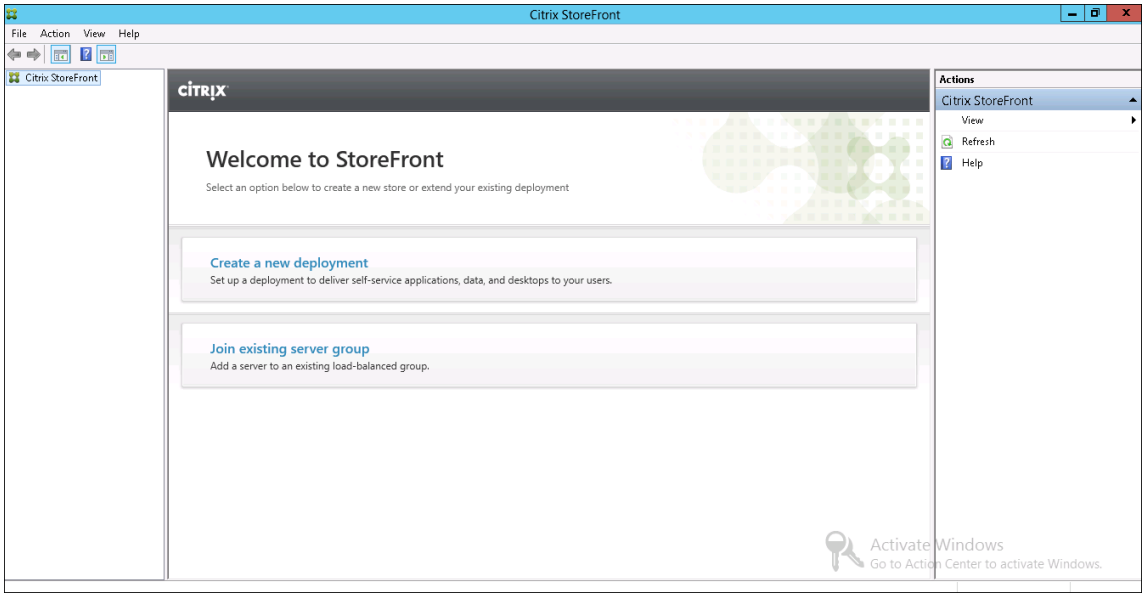
4. Citrix StoreFront モジュールをインポートします。

```
1 Import-Module citrix.storefront -verbose
2 <!--NeedCopy-->
```

5. モジュールのインポート後、**Clear-STFDeployment** コマンドを実行して StoreFront サーバーをデフォルトの設定にリセットします:

```
1 Clear-STFDeployment -Confirm $False
2 <!--NeedCopy-->
```

6. コマンドが正常に完了した後、StoreFront 管理コンソールを開き、すべての設定がリセットされたことを確認します。［新しい展開環境の作成］または ［既存のサーバー グループへの参加］を可能にするオプションが利用できるようになります。



StoreFront のアンインストール

June 6, 2024

StoreFront をアンインストールすると、StoreFront 自体のほか、認証サービス、ストア、Citrix Receiver for Web サイト、XenApp Services サイトの URL、および関連する構成が削除されます。ユーザーのアプリケーションサブスクリプションデータを含んでいるサブスクリプションストアサービスも削除されます。単一サーバー環境では、これによりユーザーのサブスクリプションデータが削除されてしまいます。複数サーバーの展開環境の場合は、これらのデータは展開環境内のほかのサーバー上で保持されます。.NET Framework の機能や Web サーバー（IIS）の役割サービスなど、StoreFront インストーラーにより有効になった必須機能は、StoreFront をアンインストールしても無効になりません。

1. ローカルの管理者権限を持つアカウントで StoreFront サーバーにログオンします。
2. StoreFront 管理コンソールが開いている場合は閉じます。
3. PowerShell SDK を使用して StoreFront の管理に使用されている可能性のある PowerShell セッションをすべて閉じます。
4. ［スタート］メニューを開き、［設定］（歯車アイコン）を押して、［アプリ］に移動します。
5. ［プログラムと機能］ウィンドウで、［**Citrix StoreFront**］を選択して ［アンインストール］をクリックします。これにより、サーバーからすべての StoreFront コンポーネントが削除されます。
6. ［**Citrix StoreFront** のアンインストール］ダイアログボックスで、［はい］をクリックします。アンインストールが完了したら、［**OK**］をクリックします。

手動で **StoreFront** を削除するには

StoreFront をアンインストールした後、StoreFront が完全に削除されたことを確認するには、次の手順を実行します:

1. Web サーバーの役割を削除します。
2. *C:\Program Files\Citrix\Receiver StoreFront* フォルダーを削除します。
3. *C:\Program Files\Citrix\StoreFront Install* のすべてのサブディレクトリを削除します。
4. *C:\Inetpub* フォルダーを削除します。

StoreFront を再インストールできるようになりました。

インストールログ

ログファイルについて詳しくは、「インストールログ」を参照してください。

認証と委任の構成

June 6, 2024

自分の要件によって、複数の認証と委任法方式があります。

方法	詳細
認証の構成	Citrix Workspace アプリを介してユーザーが StoreFront にログインするために使用できる方法を構成します。
スマートカード認証	スマートカード認証を設定します。
ユーザー名とパスワード認証	ユーザーが Active Directory のユーザー名とパスワードを使用して認証できるようにし、パスワードの変更やパスワード有効期限の通知に関するオプションを構成できるようにします。
ドメインパススルー認証	Windows デバイスが Windows 資格情報を使用してシングルサインオンできるようにします。
SAML 認証	SAML を使用してサードパーティ ID プロバイダーに認証を委任します。
フェデレーション認証サービスの構成	VDA へのシングルサインオンのためにフェデレーション認証サービスと統合するように StoreFront を構成する

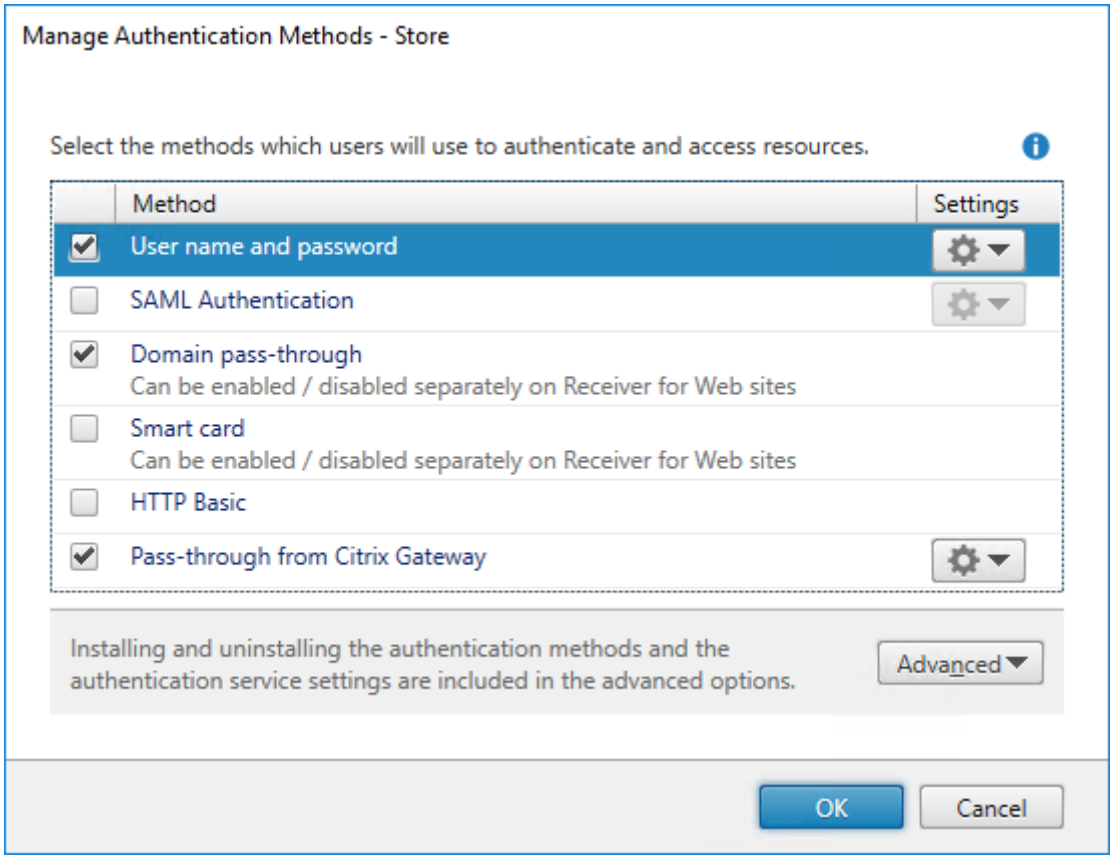
認証の構成

June 6, 2024

認証方法の管理

ストアごとに、Citrix Workspace アプリを通してストアにログインするときに使用できる認証方法を 1 つ以上選択できます。

1. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ノードを選択して、［操作］ペインの ［認証方法の管理］をクリックします。
2. ユーザーに許可するアクセス方法を指定します。



- Active Directory のユーザー名とパスワードの指定ユーザー認証を有効にするには ［ユーザー名とパスワード］チェックボックスをオンにします。詳しくは、「ユーザー名とパスワード認証」を参照してください。
- SAML ID プロバイダーとの統合を有効にするには、［**SAML** 認証］チェックボックスをオンにします。詳しくは、「SAML 認証」を参照してください。
- ユーザーデバイスから Active Directory ドメイン資格情報がパススルーされるようにするには、［ドメインパススルー］をオンにします。詳しくは、「ドメインパススルー認証」を参照してください。

- スマートカード認証を有効にするには、［スマートカード］をオンにします。詳しくは、「スマートカード認証」を参照してください。
- HTTP 基本認証を有効にするには、［**HTTP** 基本］をオンにします。ユーザー認証は、StoreFront サーバーの IIS Web サーバーで実行されます。
- Citrix Gateway からのパススルー認証を有効にするには、［**Citrix Gateway** からのパススルー］をオンにします。認証を有効化した Citrix Gateway 経由でユーザーが StoreFront に接続する場合は、これを有効にします。詳しくは、「Citrix Gateway からのパススルー」を参照してください。

ストアの認証方法を変更すると、Web ブラウザーを介してストアにアクセスするときに使用する認証方法も更新されます。Web ブラウザーを介してログオンするときの認証方法を変更するには、［認証方法］を参照してください。

PowerShell SDK を使用して認証方法を管理する

PowerShell SDKを使用して認証を構成するには:

1. Get-STFAuthenticationServiceを呼び出して、ストアまたは仮想ディレクトリの認証サービスを取得し、その現在の構成を表示します。
2. 認証サービスで、必要な認証プロトコルを有効または無効にします。使用可能なプロトコルの一覧を取得するには、Get-STFAuthenticationServiceProtocolを実行します。プロトコルを有効にするには、有効にするプロトコルの一覧を指定してEnable-STFAuthenticationServiceProtocolを実行します。プロトコルを無効にするには、無効にするプロトコルの一覧を指定してDisable-STFAuthenticationServiceProtocolを実行します。
3. 有効にした認証プロトコルを構成します。詳しくは、各プロトコルのドキュメントを参照してください。

共有認証サービス設定

共有認証サービス設定タスクを使ってストアを指定し、ストア間でシングルサインオンを有効にする認証サービスを共有します。

1. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインで、［認証方法の管理］をクリックします。
2. ［詳細］ドロップダウンメニューから、［共有認証サービス設定］を選択します。
3. ［共有認証サービスを使用する］チェックボックスをオンにして、［ストア］名ドロップダウンメニューからストアを選択します。

> 注:
>
> 共有認証サービスと専用認証サービスに機能的な違いはありません。2 つ以上のストアによって共有される認証サービスは、共有認証サービスとして扱われ、構成の変更はいずれも共有認証サービスを使用するすべてのストアに対して適用されます。

スマートカード認証

June 6, 2024

ユーザーは、ストアにアクセスするときに、スマートカードと PIN を使用して認証されます。StoreFront をインストールする際、スマートカード認証はデフォルトで無効になっています。スマートカード認証は、Citrix Workspace アプリ、Web ブラウザーおよび XenApp Services サイトからストアに接続するユーザーに対して有効にすることができます。

スマートカード認証を使用することで、ユーザーのログオンプロセスを合理化しつつ、ユーザーによるインフラストラクチャへのアクセスにおいてセキュリティを強化することができます。社内ネットワークへのアクセスは、公開キーのインフラストラクチャを使用した証明書ベースの 2 要素認証によって保護されます。秘密キーは、ハードウェアで保護されるため、スマートカードの外に漏れることはありません。ユーザーは、スマートカードと PIN を使用してさまざまなコーポレートデバイスからデスクトップとアプリケーションにアクセスできるようになります。

スマートカードは、Citrix Virtual Apps and Desktops で提供されるデスクトップとアプリケーションのユーザー認証を StoreFront 経由で行うために使用できます。StoreFront にスマートカードでログオンするユーザーは、Endpoint Management で提供されるアプリケーションにもアクセスできます。ただし、クライアント証明書認証を使用する Endpoint Management Web アプリケーションにアクセスするには、再度認証を受ける必要があります。

スマートカード認証を有効にする場合、StoreFront サーバーが属している Microsoft Active Directory ドメインか、そのドメインと直接の双方向の信頼関係が設定されているドメインのいずれかにユーザーのアカウントが属している必要があります。双方向の信頼関係を含んでいるマルチフォレスト展開環境がサポートされます。

StoreFront のスマートカード認証の構成は、ユーザーデバイス、インストールされているクライアント、およびデバイスがドメインに参加しているかどうかによって異なります。ドメインに参加しているデバイスとは、StoreFront サーバーを含んでいる Active Directory フォレスト内のドメインに属しているデバイスを意味します。

『Citrix 環境のためのスマートカードの構成』では、Citrix 環境でスマートカードを使用する場合に、特定の種類のスマートカードが使用されるように構成する方法について説明しています。同様の手順がほかのベンダーのスマートカードにも適用されます。

前提条件

- StoreFront サーバーを展開する Microsoft Active Directory ドメインか、そのドメインと直接の双方向の信頼関係が設定されているドメインのいずれかにすべてのユーザーアカウントが属していることを確認します。
- スマートカードパススルー認証を有効にする場合は、スマートカードリーダーの種類、ミドルウェアの種類と構成、およびミドルウェアの PIN のキャッシュポリシーでパススルー認証が許可されることを確認します。
- ユーザーのデスクトップやアプリケーションを提供する、Virtual Delivery Agent が動作する仮想マシンや物理マシンに、スマートカードのベンダーが提供するミドルウェアをインストールします。Citrix Virtual

Desktops 環境でスマートカードを使用する方法については、「スマートカード」を参照してください。

- お使いの公開キー基盤が適切に構成されていることを確認します。アカウントマッピングのための証明書が Active Directory 環境に対して正しく構成されており、ユーザー証明書の検証を正しく実行できることを確認します。

StoreFront の構成

- スマートカード認証を有効にするには、StoreFront とユーザーデバイス間の通信で HTTPS が使用されるように構成する必要があります。「HTTPS を使用した StoreFront のセキュリティ」を参照してください。
- Citrix Workspace アプリを介したストアへの接続時にスマートカード認証を有効にするには、［認証方法］で［スマートカード］にチェックを入れるか、チェックを外します。
- デフォルトでストアのスマートカード認証を有効にすると、そのストアのすべての Web サイトでもスマートカード認証が有効になります。［Receiver for Web サイトの管理］の［認証方法］タブで、特定の Web サイトのスマートカード認証を個別に有効または無効にできます。
- 管理者がスマートカード認証およびユーザー名とパスワード認証の両方を構成した場合、ユーザーは最初にスマートカードと PIN を使ったログオンを要求されますが、スマートカードでログオンできない場合は指定ユーザー認証を選択することができます。

StoreFront を信頼するように Delivery Controller を構成する

スマートカード認証を使用する場合、StoreFront はユーザーの資格情報にアクセスできないため、Citrix Virtual Apps and Desktops に認証できません。したがって、StoreFront からの要求を信頼するように Delivery Controller を構成する必要があります。Citrix Virtual Apps and Desktops の「セキュリティに関する考慮事項およびベストプラクティス」を参照してください。

Citrix Gateway を介したリモートアクセス

リモートアクセスの場合、Citrix Gateway でスマートカードを有効にしてから、StoreFront へのパススルー認証を委任認証で有効にすることができます。詳細については、「Gateway パススルー」を参照してください。

リソースへの接続が確立されたときにユーザーが仮想サーバーで資格情報を要求する追加のプロンプトを受信しないようにするには、仮想サーバーをもう 1 つ作成し、SSL（Secure Sockets Layer）パラメーターでクライアント認証を無効にします。詳しくは、「スマートカード認証の構成」を参照してください。スマートカード認証でゲートウェイを経由して StoreFront にアクセスする場合。ストアに対してデスクトップやアプリケーションを提供する展開への接続のために、この仮想サーバーを経由する最適な Citrix Gateway ルーティングを設定します。詳しくは、「ストアの最適な HDX ルーティングの構成」を参照してください。

VDA へのシングルサインオン

ユーザーのスマートカード資格情報のパススルーによって、VDA へのシングルサインオンを有効にすることができます。ストアには Web ブラウザーまたは Windows 向け Citrix Workspace アプリを通じてアクセスできますが、リソースは Windows 向け Citrix Workspace アプリで開く必要があります。他のオペレーティングシステムの場合、またはブラウザー経由でリソースにアクセスする場合、ユーザーは VDA に接続するときに資格情報を再入力する必要があります。

1. Windows 向け Citrix Workspace のインストール時にシングルサインオンコンポーネントを含めて、シングルサインオン用に構成します。「ドメインパススルー認証の構成」を参照してください。
2. テキストエディターを使用して、ストアの default.ica ファイルを開きます。「デフォルトの ica」を参照してください。
3. Citrix Gateway を経由しないでストアにアクセスするユーザーに対して、スマートカードの資格情報でのパススルーを有効にするには、［アプリケーション］セクションに次の設定を追加します。

   ```
   DisableCtrlAltDel=Off
   ```

   この設定はストアのすべてのユーザーに適用されます。デスクトップおよびアプリケーションに対するドメインパススルー認証とスマートカードパススルー認証の両方を有効にするには、これらの認証方法について個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
4. Citrix Gateway を経由してストアにアクセスするユーザーに対して、スマートカードの資格情報でのパススルーを有効にするには、［アプリケーション］セクションに次の設定を追加します。

   ```
   UseLocalUserAndPassword=On
   ```

   この設定はストアのすべてのユーザーに適用されます。一部のユーザーに対してのみパススルー認証を有効にする場合は、それらのユーザー用に個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。

FAS を使用した **VDA** へのシングルサインオン

また、HTML5 向け Citrix Workspace アプリではなく、ローカルにインストールされた Citrix Workspace アプリを使用する場合に、フェデレーション認証サービスを VDA へのシングルサインオンで構成することもできます。

重要な注意事項

StoreFront でのユーザー認証にスマートカードを使用する場合は、次の要件と制限があります。

- スマートカード認証で仮想プライベートネットワーク（VPN）トンネルを使用するには、ユーザーが Citrix Gateway Plug-in をインストールして Web ページ経由でログオンする必要があります。この場合、各手順で

スマートカードと PIN による認証が必要になります。スマートカードユーザーは、Citrix Gateway Plug-in を使用した StoreFront へのパススルー認証を使用できません。

- 同一ユーザーデバイス上で複数のスマートカードやスマートカードリーダーを使用することができますが、スマートカードでのパススルー認証を有効にする場合は、ユーザーがデスクトップやアプリケーションにアクセスするときにスマートカードが 1 枚のみ挿入されていることを確認する必要があります。
- アプリケーション内でスマートカードを使用する場合（デジタル署名または暗号化機能など）、スマートカードの挿入または PIN の入力を求めるメッセージが表示されることがあります。これは、同時に複数のスマートカードが挿入されている場合に発生します。また、構成設定（通常グループポリシーを使用して構成される PIN キャッシュなどのミドルウェア設定）が原因で発生することもあります。適切なスマートカードを挿入しているにもかかわらずスマートカードの挿入を求めるメッセージが表示された場合は、［キャンセル］をクリックする必要があります。ただし、PIN の入力が求められた場合は、PIN を再入力する必要があります。
- ドメイン参加デバイスを使用する Windows 向け Citrix Workspace アプリユーザーが Citrix Gateway を介してストアにアクセスしない場合に、Citrix Virtual Apps and Desktops へのスマートカードでのパススルー認証を有効にすると、この設定がストアのすべてのユーザーに適用されます。デスクトップおよびアプリケーションに対するドメインパススルー認証とスマートカードパススルー認証の両方を有効にするには、これらの認証方法について個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
- ドメイン参加デバイスを使用する Windows 向け Citrix Workspace アプリユーザーが Citrix Gateway を介してストアにアクセスする場合、Citrix Virtual Apps and Desktops へのスマートカードでのパススルー認証を有効にすると、この設定がストアのすべてのユーザーに適用されます。一部のユーザーに対してのみパススルー認証を有効にする場合は、それらのユーザー用に個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
- 各 XenApp Services サイトに構成できる認証方法と各ストアで使用できる XenApp Services サイトは、それぞれ 1 つだけです。スマートカード認証に加えてほかの認証方法を有効にする必要がある場合は、認証方法ごとに個別のストアを作成し、それぞれのストアに XenApp Services サイトを 1 つずつ割り当てる必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
- StoreFront インストール時の Microsoft インターネットインフォメーションサービス（IIS）のデフォルト構成では、StoreFront 認証サービスの証明書認証 URL への HTTPS 接続でのみクライアント証明書が要求されます。それ以外の StoreFront URL にはクライアント証明書は必要ありません。この構成により、管理者は、スマートカードでの認証に問題が生じた場合に指定ユーザー認証を使用できるように設定できます。適用される Windows ポリシー設定によっては、ユーザーが再認証なしにスマートカードを取り出すこともできます。

  すべての StoreFront URL への HTTPS 接続でクライアント証明書が必要になるように IIS を構成する場合は、認証サービスとストアを同じサーバー上に配置する必要があります。この場合、すべてのストアに有効なクライアント証明書を使用する必要があります。この IIS サイト構成では、スマートカードユーザーが Citrix Gateway 経由で接続できなくなり、指定ユーザー認証にもフォールバックされません。また、スマートカードをデバイスから取り出す場合は再度ログオンする必要があります。

ドメインパススルー認証

June 6, 2024

ユーザーはドメインに参加している Windows コンピューターに対して認証を行い、資格情報を使用して Citrix Workspace アプリに自動的にログインします。これは、Windows 向け Citrix Workspace アプリおよび Windows 上の次の Web ブラウザーでサポートされます:

- Internet Explorer
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

StoreFront 構成

Windows 向け Citrix Workspace アプリのドメインパススルーを有効にするには、［認証方法］ で ［ドメインパススルー］を選択します。

デフォルトでストアのドメインパススルー認証を有効にすると、そのストアのすべての Web サイトの HTML5 向け Citrix Workspace アプリでも、スマートカード認証が有効になります。［Receiver for Web サイトの管理］の［認証方法］タブで、特定の Web サイトのドメインパススルー認証を個別に有効または無効にできます。

StoreFront を信頼するように Delivery Controller を構成する

ドメインパススルー認証を使用する場合、StoreFront はユーザーの資格情報にアクセスできないため、Citrix Virtual Apps and Desktops に認証できません。したがって、StoreFront からの要求を信頼するように Delivery Controller を構成する必要があります。Citrix Virtual Apps and Desktops の「セキュリティに関する考慮事項およびベストプラクティス」を参照してください。

VDA へのシングルサインオン

VDA にシングルサインインするには、[シングルサインオンの有効化] コンポーネントを備えた Windows 向け Citrix Workspace アプリを使用する必要があります。「ドメインパススルー認証の構成」を参照してください。HTML5 向け Citrix Workspace アプリを使用する場合は、ブラウザーではなく Windows 向け Citrix Workspace アプリのリソースに接続するように構成する必要があります。

Windows 向け Citrix Workspace アプリの構成

Windows 向け Citrix Workspace アプリを使用してストアおよび VDA へのシングルサインオンでドメインパススルーを有効にするには、Windows 向け Citrix Workspace アプリのドキュメントを参照してください。

HTML5 向け **Citrix Workspace** アプリの構成

ドメインパススルー認証を許可するには、ユーザーの Web ブラウザー構成の更新が必要な場合があります。ドメインパススルーを使用して、Web ブラウザーからストアにサインインできます。VDA にシングルサインオンするには、ユーザーは Web ブラウザーではなく Windows 向け Citrix Workspace アプリでリソースを開く必要があります。

Internet Explorer、**Edge**、**Chrome**　ほとんどの Web ブラウザーは、Windows Internet Explorer のゾーン構成を使用して、シングルサインオンを有効にするかどうかを決定します。デフォルトでは、ローカルイントラネットゾーンのサイトに対してのみ、この設定は有効です。サイトをイントラネットゾーンに追加するには、次の手順を実行します:

1. ［コントロールパネル］を開きます
2. ［インターネットオプション］を開きます。
3. ［セキュリティ］タブに移動します。
4. ［ローカルイントラネット］を選択します
5. ［サイト］をクリックします。
6. ［詳細設定］をクリックします。
7. StoreFront の Web サイトを追加します。

これらの設定は、グループポリシーを使用して展開できます。

Firefox　シングルサインオン用に StoreFront Web サイトの URI を信頼するように、ブラウザーの詳細設定を変更します。

> 警告:
>
> 詳細設定を誤って編集すると、深刻な問題が発生することがあります。お客様の責任と判断の範囲で編集してください。

1. ドメインパススルーを使用して認証するコンピューターで Firefox を開きます。
2. アドレスバーに「about:config」と入力します。
3. 「危険性を承知の上で使用する」をクリックします。
4. 検索バーに「negotiate」と入力します。
5. 「network.negotiate-auth.delegation-uris」をダブルクリックします。
6. 企業の Windows ドメイン名を入力します（例：mydomain.com）。
7. ［OK］をクリックします。
8. 「network.negotiate-auth.trusted-uris」をダブルクリックします。
9. 企業の Windows ドメイン名を入力します（例：mydomain.com）。
10. ［OK］をクリックします。
11. Firefox を閉じて再起動します。

FAS を使用した **VDA** へのシングルサインオン

また、HTML5 向け Citrix Workspace アプリではなく、ローカルにインストールされた Citrix Workspace アプリを使用する場合に、フェデレーション認証サービスを VDA へのシングルサインオンで構成することもできます。

Citrix Gateway からのパススルー

June 6, 2024

ユーザーは Citrix Gateway にログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。Citrix Gateway からのパススルー認証は、ストアへのリモートアクセスを最初に構成するときにデフォルトで有効になります。ユーザーは、Citrix Workspace アプリまたは Web ブラウザーを使用して、Citrix Gateway 経由でストアに接続できます。Citrix Gateway を使用するための StoreFront の構成について詳しくは、「Citrix Gateway の構成」を参照してください。

StoreFront は、次の Citrix Gateway 認証方法でのパススルーをサポートします。

- ドメイン。ユーザーは、Active Directory のユーザー名とパスワードを使用してログオンします。
- **RSA**。ユーザーは、セキュリティトークンによって生成されるトークンコードから得られるパスコードを使用して Citrix Gateway にログオンします。トークンコードと暗証番号（PIN）を組み合わせてパスコードにする場合もあります。セキュリティトークンのみによるパススルー認証を有効にする場合は、ユーザーに提供するリソースでほかの認証方法（Microsoft Active Directory ドメインの資格情報など）が使用されないようにしてください。
- スマートカード。ユーザーはスマートカードを使用してログオンします
- **RSA+** ドメイン。Citrix Gateway にログオンするユーザーは、ドメイン資格情報とセキュリティトークンパスコードの両方を入力する必要があります。

Citrix Gateway で認証を無効にしている場合、またはシングルサインオンを無効にしている場合、パススルーは使用されないため、他の認証方法のいずれか 1 つを構成する必要があります。

Citrix Workspace アプリ内でストアにアクセスするリモートユーザーに対して Citrix Gateway での 2 要素認証を有効にする場合は、Citrix Gateway で 2 つの認証ポリシーを作成する必要があります。プライマリの認証方法として RADIUS（Remote Authentication Dial-In User Service）を構成し、セカンダリの認証方法として LDAP（Lightweight Directory Access Protocol）を構成します。セッションプロファイルでセカンダリの認証方法が使用されるように資格情報インデックスを変更して、LDAP 資格情報が StoreFront に渡されるようにします。Citrix Gateway アプライアンスを StoreFront 構成に追加する場合は、［ログオンの種類］を［ドメインおよびセキュリティトークン］に設定します。詳しくは、http://support.citrix.com/article/CTX125364を参照してください：

Citrix Gateway から StoreFront への複数ドメイン認証を有効にするには、各ドメインの Citrix Gateway LDAP 認証ポリシーで［SSO Name Attribute］を userPrincipalName に設定します。使用される LDAP ポリシーが特定されるように、Citrix Gateway のログオンページでユーザーにドメインを指定させることができます。StoreFront

に接続できるように Citrix Gateway セッションプロファイルを構成する場合は、シングルサインオンドメインを指定しないでください。管理者は、各ドメイン間の信頼関係を構成する必要があります。明示的に信頼されるドメインのみにアクセスを制限せず、ユーザーがどのドメインからも StoreFront へログオンできるようにします。

Citrix Gateway 展開環境でサポートされる場合は、SmartAccess 機能を使用して、Citrix Virtual Apps and Desktops リソースへのユーザーアクセスを Citrix Gateway セッションポリシーに基づいて制御できます。

Gateway パススルーの有効化

Workspace アプリを介した接続時のストアの Gateway パススルー認証を有効または無効にするには、［認証方法］ウィンドウで［**Citrix Gateway** からのパススルー］にチェックを入れるか、チェックを外します。

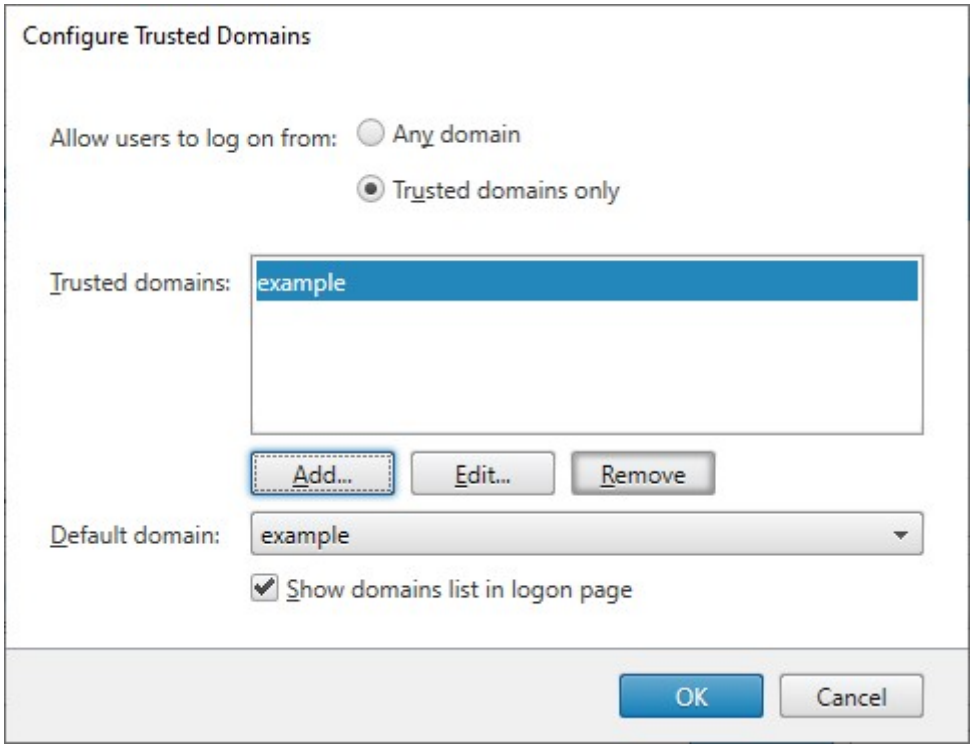
デフォルトで Citrix Gateway のパススルー認証を有効にすると、そのストアのすべての Web サイトでもスマートカード認証が有効になります。［認証方法］タブで、特定の Web サイトのユーザー名とパスワード認証を無効にできます。

信頼されるユーザードメインの構成

Citrix Gateway が LDAP 認証を使用するように構成されている場合は、特定のドメインへのアクセスを制限できます。

1. ［認証方法の管理］ウィンドウで、［**Citrix Gateway** からのパススルー］>［設定］ドロップダウンメニューから［信頼されるドメインの構成］を選択します。
2. ［信頼済みドメインのみ］をクリックして［追加］をクリックし、信頼されるドメインの名前を入力します。この認証サービスを使用するすべてのストアでは、ここで追加したドメインのアカウントでログオンできます。ドメイン名を変更するには、［信頼されるドメイン］の一覧でエントリを選択して［編集］をクリックします。特定ドメインのユーザーアカウントでのアクセスを禁止するには、一覧でそのドメインを選択して［削除］をクリックします。

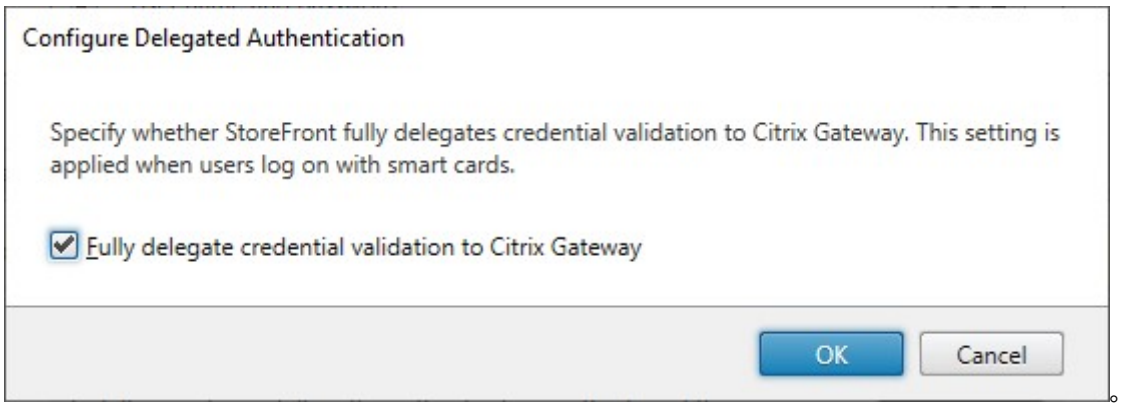
   管理者がドメイン名を指定する方法により、ユーザーが資格情報の入力時に使用すべき形式が決まります。ユーザーにドメインユーザー名形式で資格情報を入力させるには、一覧に NetBIOS 名を追加します。ユーザーにユーザープリンシパル名形式で資格情報を入力させるには、一覧に完全修飾ドメイン名を追加します。ユーザーがドメインユーザー名形式でもユーザープリンシパル名形式でも資格情報を入力できるようにするには、一覧に NetBIOS 名と完全修飾ドメイン名の両方を追加する必要があります。
3. 信頼されるドメインを複数構成する場合は、ユーザーがログオンするときにデフォルトで選択されるドメインを［デフォルトドメイン］ボックスの一覧から選択します。
4. ログオンページに信頼されるドメインを一覧表示するには、［ログオンページにドメイン一覧を表示する］チェックボックスをオンにします。



資格情報の検証を **Citrix Gateway** に委任する

デフォルトでは、StoreFront は Gateway から受信したユーザー名とパスワードを検証します。Citrix Gateway がスマートカードなどのパスワードレス認証方法を使用するように構成されている場合は、StoreFront が資格情報を検証せず、Gateway の認証に依存するように構成する必要があります。この場合、Gateway の構成時にコールバック URL を入力し、StoreFront が Gateway からのリクエストを確認できるようにすることをお勧めします。「Citrix Gateway の管理」を参照してください。

1. ［認証方法の管理］ウィンドウで、［**Citrix Gateway** からのパススルー］ > ［設定］ドロップダウンメニューから ［認証の委任構成］を選択します。
2. ［資格情報の検証を **Citrix Gateway** に委任する］を選択します。



PowerShell SDK

PowerShell SDK を使用して認証をゲートウェイに委任するようにストアを構成するには、コマンドレットSet-STFCitrixAGBasicOptionsを使用して`CredentialValidationMode`を`Auto`に設定します。資格情報を検証するように StoreFront を構成するには、`CredentialValidationMode`を`Password`に設定します。

ユーザーがログオン時にパスワードを変更できるようにする

Citrix Gateway が LDAP（ユーザー名とパスワード）認証を使用するように構成されている場合は、ログイン時に期限切れのパスワードを変更できるように NetScaler を構成できます。

1. NetScaler 管理 Web サイトへのログイン
2. サイドメニューで ［**Authentication**］ > ［**Dashboard**］に移動します。
3. 認証サーバーをクリックします。
4. ［**Other Settings**］で ［**Allow Password Change**］にチェックを入れます。

ユーザーがログオン後にパスワードを変更できるようにする

［**Citrix Gateway** からのパススルー］では、Citrix Gateway が認証の処理を担当します。ユーザーがログオン後にパスワードを変更できるように StoreFront を構成できます。この機能は、ローカルにインストールされた Workspace アプリではなく、HTML5 向け Citrix Workspace アプリを介して StoreFront のストアにアクセスする場合にのみ使用できます。

StoreFront のデフォルトの構成では、パスワードの有効期限が切れた場合でも、ユーザーはパスワードを変更できません。この機能を有効にする場合は、サーバーが属しているドメインのポリシーでユーザーによるパスワード変更が禁止されていないことを確認してください。ユーザーによるパスワードの変更を有効にすると、この認証サービスを使用するストアにアクセスできるすべてのユーザーに、慎重に扱うべきセキュリティ機能が公開されることになります。組織のセキュリティポリシーにより、ユーザーパスワード変更機能が内部使用のみに制限される環境では、社内ネットワークの外側からそれらのストアにアクセスできないことを確認してください。

1. ［認証方法の管理］ウィンドウで、［**Citrix Gateway** からのパススルー］ > ［設定］ドロップダウンメニューから ［パスワードオプションの管理］を選択します
2. ユーザーによるパスワードの変更を許可するには、［ユーザーにパスワードの変更を許可する］チェックボックスをオンにします。

> 注:
>
> ［ユーザーにパスワードの変更を許可する］を選択または選択解除すると、［ユーザー名とパスワード］認証の［パスワードオプションの管理］ の設定にも影響を与えます。

PowerShell SDK

PowerShell SDK を使用してパスワード変更オプションを変更するには、コマンドレットSet-STFExplicitCommonOptionsを使用します。

StoreFront を信頼するように Delivery Controller を構成する

Citrix Gateway が LDAP 認証を使用して構成されている場合、Gateway は資格情報を StoreFront に渡します。他の認証方法の場合、StoreFront はユーザーの資格情報にアクセスできないため、Citrix Virtual Apps and Desktops に認証できません。したがって、StoreFront からの要求を信頼するように Delivery Controller を構成する必要があります。Citrix Virtual Apps and Desktops の「セキュリティに関する考慮事項およびベストプラクティス」を参照してください。

フェデレーション認証サービスを使用した VDA へのシングルサインオン

ゲートウェイが LDAP 認証を使用して構成されている場合、ゲートウェイは資格情報を StoreFront に渡して、VDA にシングルサインオンできるようにします。他の認証方法の場合、StoreFront は資格情報にアクセスできないため、デフォルトではシングル サインオンは使用できません。フェデレーション認証サービスを使用してシングルサインオンを提供できます。

SAML 認証

June 6, 2024

SAML（Security Assertion Markup Language：セキュリティアサーションマークアップランゲージ）は、ID および認証製品で採用されているオープンスタンダードです。SAML を使用すると、認証のためにユーザーを外部 ID プロバイダーにリダイレクトするように StoreFront を構成できます。

> 注:
>
> 内部アクセス用に SAML 認証を使用して StoreFront を構成します。外部アクセスの場合は、SAML 認証を使用して Citrix Gateway を構成し、次にゲートウェイパススルー認証を使用して StoreFront を構成します。

StoreFront には、次のような SAML 2.0 準拠の ID プロバイダー（IdP）が必要です:

- SAML バインドを使用する Microsoft AD フェデレーションサービス（WS フェデレーションバインドは不可）。詳しくは、「AD FS Deployment」および「AD FS Operations」を参照してください。
- Citrix Gateway（IdP として構成）。
- Microsoft Entra ID。詳しくは、CTX237490を参照してください。

SAML アサーションには、ユーザーの UPN を含む`saml:Subject`属性が含まれている必要があります。

Workspace アプリを介した接続時のストアの SAML 認証を有効または無効にするには、［認証方法］ウィンドウで［**SAML** 認証］を選択するか、選択を解除します。デフォルトでストアの SAML 認証を有効にすると、そのストアのすべての Web サイトでも SAML 認証が有効になります。［認証方法］タブで、特定の Web サイトの SAML を個別に構成できます。

StoreFront SAML エンドポイント

SAML を構成するために、ID プロバイダーは次のエンドポイントを必要とする場合があります:

- エンティティ ID の URL。これはストアの認証サービスのパスです)通常は、https://[storefronthost]/Citrix/[StoreName]A
- Assertion Consumer Service の URL(通常は、https://[storefronthost]/Citrix/[StoreName]Auth/SamlForms/Asse
- メタデータサービス(通常は、https://[storefronthost]/Citrix/[StoreName]Auth/SamlForms/ServiceProvider/Meta

さらに、テストエンドポイントがあります(通常は、https://[storefronthost]/Citrix/[StoreName]Auth/SamlTest)

次の PowerShell スクリプトを使用して、指定したストアのエンドポイントを一覧表示できます。

```
# Change this value for your Store
$storeVirtualPath = "/Citrix/Store"

$auth = Get-STFAuthenticationService -Store (Get-STFStoreService -
    VirtualPath $storeVirtualPath)
$spId = $auth.AuthenticationSettings["samlForms"].SamlSettings.
    ServiceProvider.Uri.AbsoluteUri
$acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/AssertionConsumerService")
$md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/ServiceProvider/Metadata")
$samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlTest")
```



```
Write-Host "SAML Service Provider information:
Entity ID: $spId
Assertion Consumer Service: $acs
Metadata: $md
Test Page: $samlTest
<!--NeedCopy-->
```

出力例:

```
SAML Service Provider information:
Entity ID: https://storefront.example.com/Citrix/StoreAuth
Assertion Consumer Service: https://storefront.example.com/Citrix/
    StoreAuth/SamlForms/AssertionConsumerService
Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/
    ServiceProvider/Metadata
Test Page: https://storefront.example.com/Citrix/StoreAuth/SamlTest
<!--NeedCopy-->
```

メタデータの交換を使用して構成する

構成を簡単にするために、ID プロバイダーとサービスプロバイダー（この場合は StoreFront）の間でメタデータ）ID、証明書、エンドポイント、その他の構成）を交換できます。

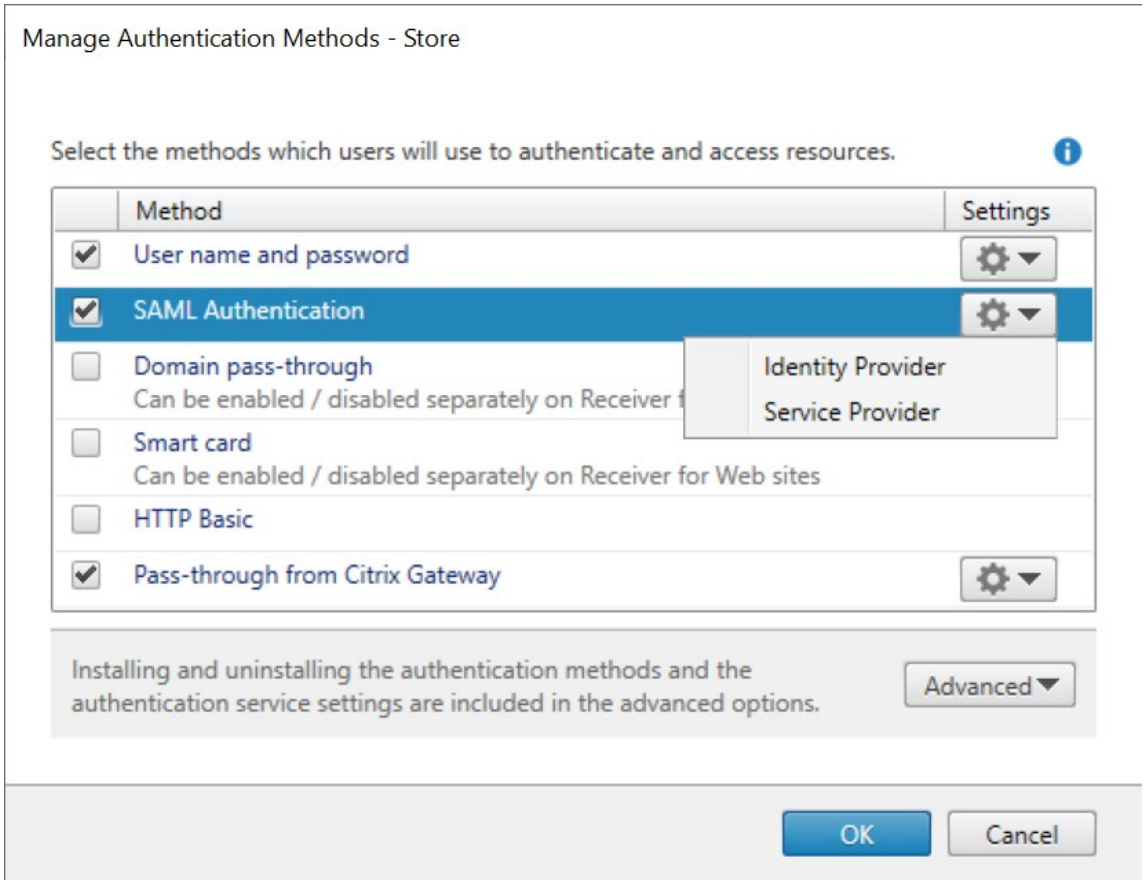
ID プロバイダーがメタデータのインポートをサポートしている場合は、StoreFront MetaData エンドポイントで指定できます。注：この操作は HTTPS を介して行う必要があります。

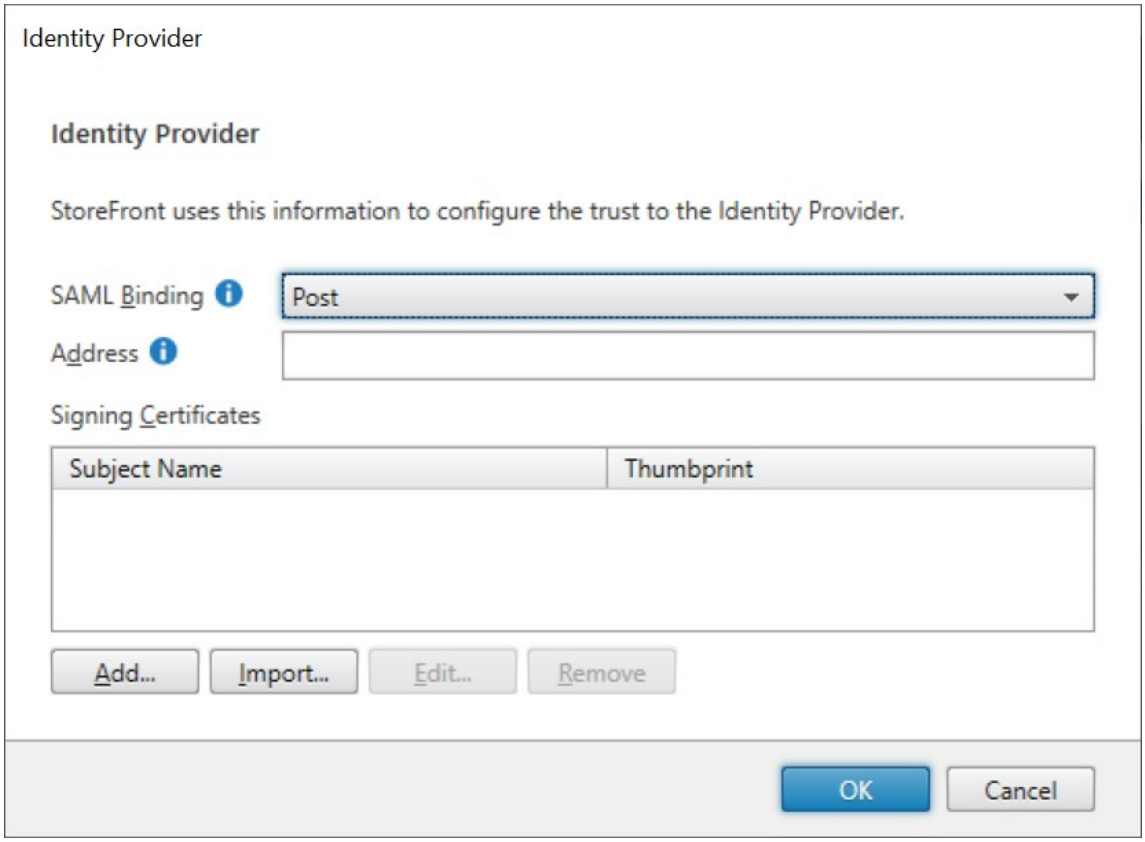
ID プロバイダーからのメタデータを使用して StoreFront を構成するには、次のようにUpdate-STFSamlIdPFromMetadataコマンドレットを使用します:

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module

# Remember to change this with the virtual path of your Store.
$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store

# To read the metadata directly from the Identity Provider, use the
    following:
# Note again this is only allowed for https endpoints
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https:
    //example.com/FederationMetadata/2007-06/FederationMetadata.xml

# If the metadata has already been download, use the following:
# Note: Ensure that the file is encoded as UTF-8
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C
    :\Users\exampleusername\Downloads\FederationMetadata.xml"
<!--NeedCopy-->
```


ID プロバイダーを構成する

1. ［**SAML** 認証］行の設定ドロップダウンをクリックし、［**ID** プロバイダー］をクリックします。

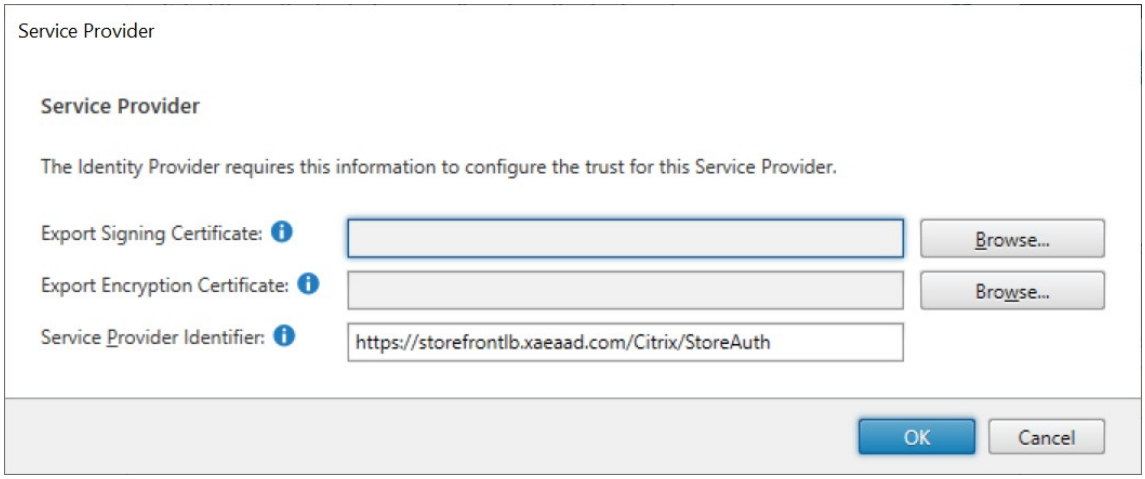




2. [**Post**] または [**Redirect**] の [**SAML** バインド] を選択します。
3. ID プロバイダーの [アドレス] を入力します。
4. SAML トークンの署名に使用される証明書をインポートします。
5. [**OK**] を押して変更を保存します。

サービスプロバイダーを構成する

1. [**SAML** 認証] 行の設定ドロップダウンをクリックし、[サービスプロバイダー] をクリックします。



2. 必要に応じて、ID プロバイダーへのメッセージに署名するために使用される［署名証明書のエクスポート］を選択します。
3. 必要に応じて、ID プロバイダーから受信したメッセージを暗号化解除するために使用される［暗号化証明書のエクスポート］を選択します。
4. ［サービス プロバイダー **ID**］には、ストアの認証サービスが事前に入力されます。
5. ［**OK**］を押して変更を保存します。

PowerShell SDK

PowerShell SDK の使用:

- 署名証明書をインポートするには、コマンドレットImport-STFSamlSigningCertificateを呼び出します。
- 暗号化証明書をインポートするには、コマンドレットImport-STFSamlEncryptionCertificateを呼び出します。

テスト

SAML 統合をテストするには:

1. SAML テストページに移動し、「StoreFront SAML エンドポイント」を参照してください。
2. これにより、ID プロバイダーにリダイレクトされます。資格情報を入力してください。
3. ID クレームとアサーションを表示するテストページにリダイレクトされます。

StoreFront を信頼するように Delivery Controller を構成する

SAML 認証を使用する場合、StoreFront はユーザーの資格情報にアクセスできないため、Citrix Virtual Apps and Desktops に認証できません。したがって、StoreFront からの要求を信頼するように Delivery Controller を構成

する必要があります。Citrix Virtual Apps and Desktops の「セキュリティに関する考慮事項およびベストプラクティス」を参照してください。

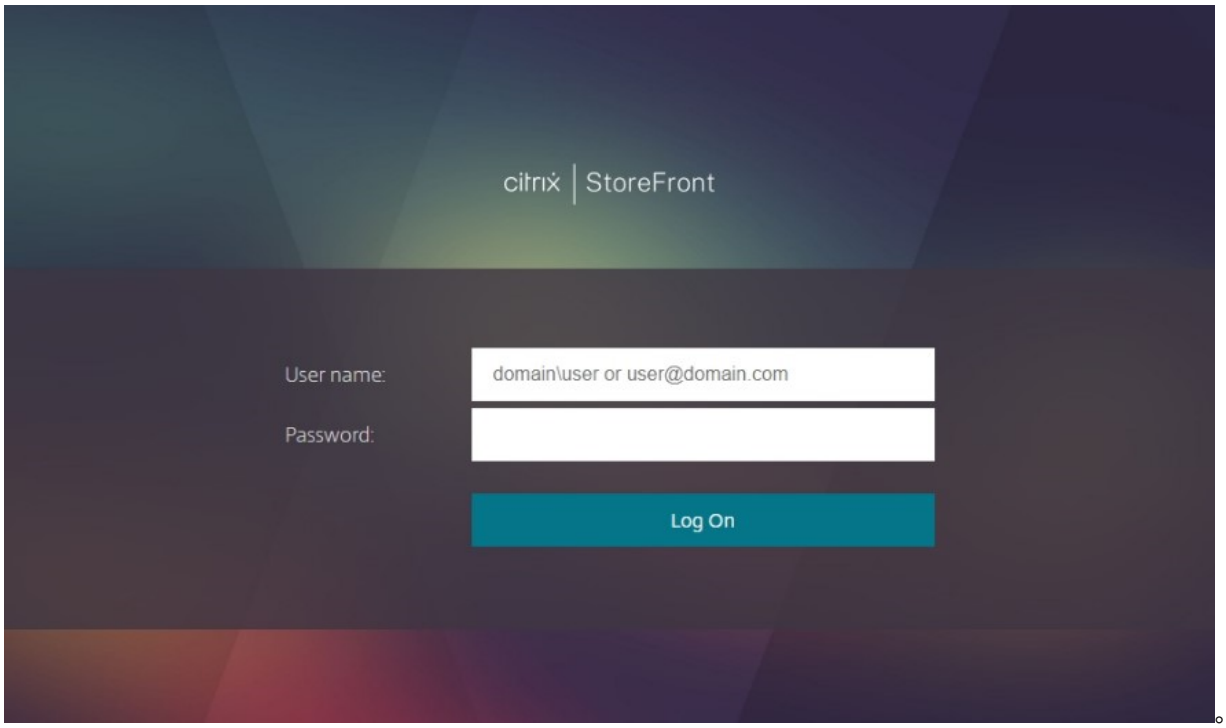
フェデレーション認証サービスを使用した **VDA** へのシングルサインオン

SAML 認証を使用する場合、StoreFront はユーザーの資格情報にアクセスできないため、デフォルトでは VDA へのシングルサインオンは使用できません。フェデレーション認証サービスを使用してシングルサインオンを提供できます。

ユーザー名とパスワード認証

June 6, 2024

ユーザー名とパスワード認証で、ユーザーは Active Directory の資格情報を入力します。



Workspace アプリを介した接続時のストアのユーザー名とパスワード認証を有効または無効にするには、［認証方法］ ウィンドウで ［ユーザー名とパスワード］にチェックを入れるか、チェックを外します。

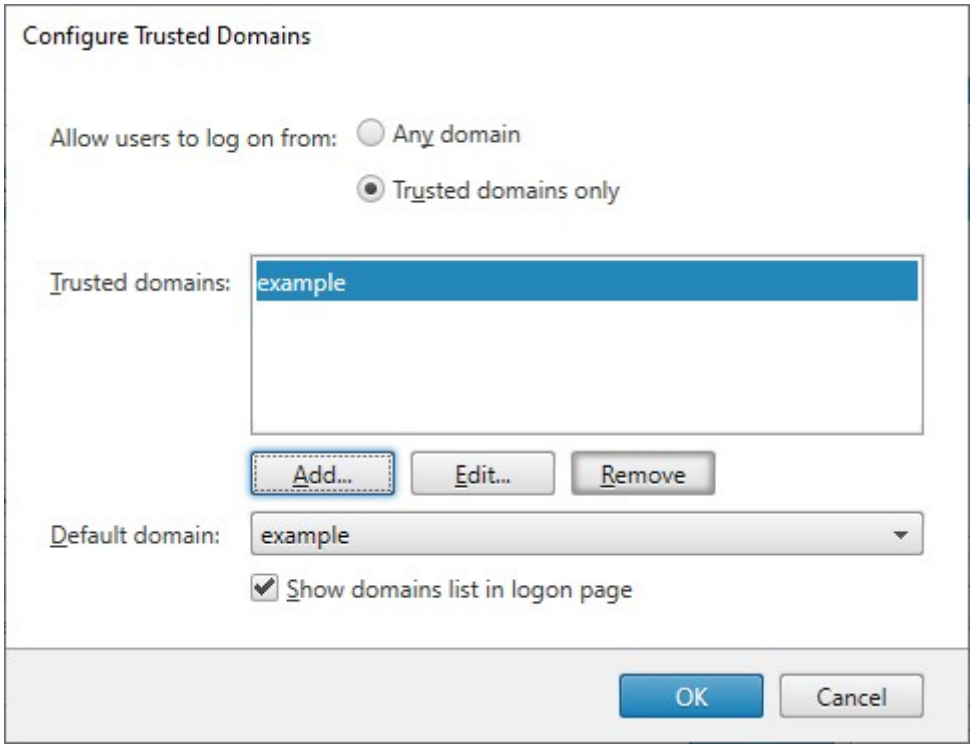
デフォルトでストアのユーザー名とパスワード認証を有効にすると、そのストアのすべての Web サイトでもユーザー名とパスワード認証が有効になります。［Receiver for Web サイトの管理］の［認証方法］ タブで、特定の Web サイトのユーザー名とパスワード認証を無効にできます。

信頼されるユーザードメインの構成

ドメインの資格情報を明示的に入力して直接または Citrix Gateway を介したパススルー認証でログオンするユーザーのストアへのアクセスを制限できます。

1. Citrix StoreFront 管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインで認証方法を選択します。［操作］ペインで、［認証方法の管理］をクリックします。
2. ［ユーザー名とパスワード］**>**［設定］の一覧から、［信頼されるドメインの構成］を選択します。
3. ［信頼済みドメインのみ］をクリックして ［追加］をクリックし、信頼されるドメインの名前を入力します。この認証サービスを使用するすべてのストアでは、ここで追加したドメインのアカウントでログオンできます。ドメイン名を変更するには、［信頼されるドメイン］の一覧でエントリを選択して ［編集］をクリックします。特定ドメインのユーザーアカウントでのアクセスを禁止するには、一覧でそのドメインを選択して ［削除］をクリックします。

   管理者がドメイン名を指定する方法により、ユーザーが資格情報の入力時に使用すべき形式が決まります。ユーザーにドメインユーザー名形式で資格情報を入力させるには、一覧に NetBIOS 名を追加します。ユーザーにユーザープリンシパル名形式で資格情報を入力させるには、一覧に完全修飾ドメイン名を追加します。ユーザーがドメインユーザー名形式でもユーザープリンシパル名形式でも資格情報を入力できるようにするには、一覧に NetBIOS 名と完全修飾ドメイン名の両方を追加する必要があります。
4. 信頼されるドメインを複数構成する場合は、ユーザーがログオンするときにデフォルトで選択されるドメインを［デフォルトドメイン］ボックスの一覧から選択します。
5. ログオンページに信頼されるドメインを一覧表示するには、［ログオンページにドメイン一覧を表示する］チェックボックスをオンにします。



ユーザーがパスワードを変更できるようにする

ユーザーがいつでもパスワードを変更できるようにすることができます。または、パスワードの有効期限が切れたユーザーにのみパスワードの変更を許可することもできます。これにより、ユーザーがパスワードの失効によりデスクトップやアプリケーションにアクセスできなくなることを防ぐことができます。

パスワード変更機能は、次のクライアントで利用できます:

Citrix Workspace アプリ	StoreFront で有効になっている場合、ユーザーが有効期限切れのパスワードを変更できる	パスワードの有効期限が切れたら、ユーザーに通知される	StoreFront で有効になっている場合は、パスワードの有効期限が切れる前に、ユーザーがそれを変更できる
Windows	はい		
Mac	はい		
Android			
iOS			
Linux	はい		
Web	はい	はい	はい

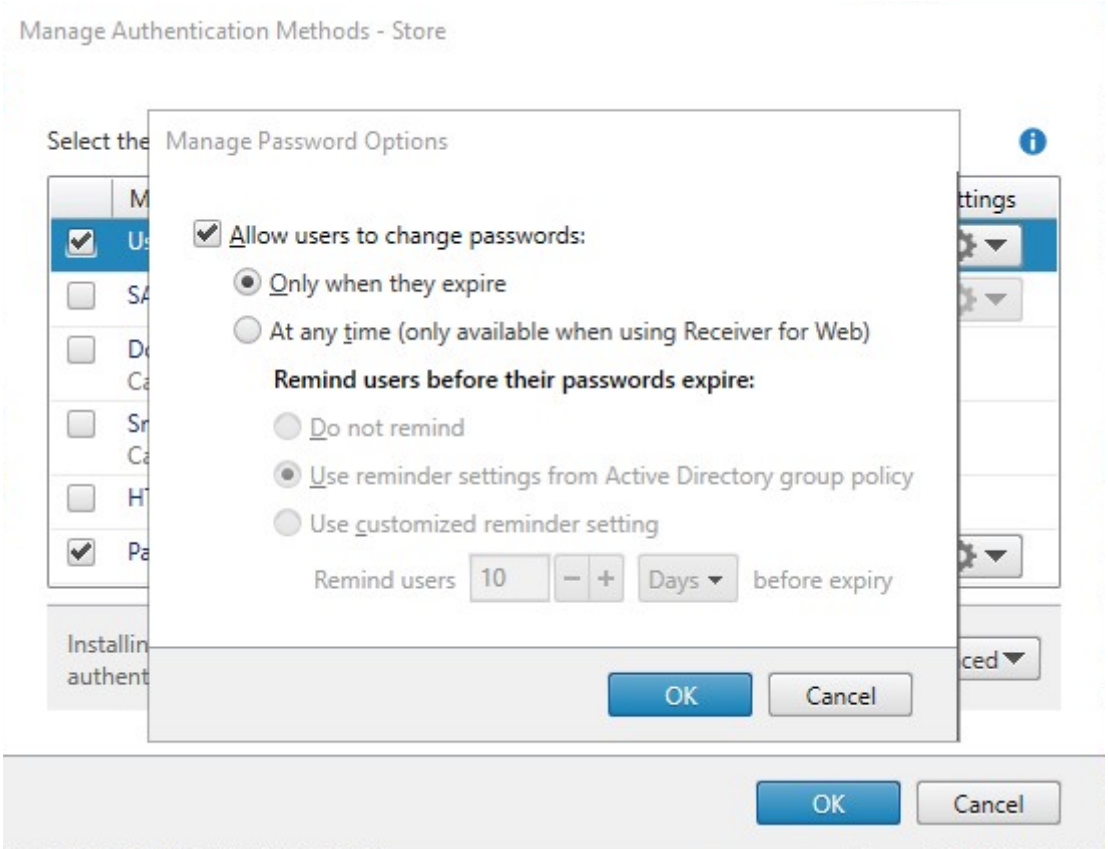
デフォルトの構成では、パスワードが失効しても、Citrix Workspace アプリおよび Web ブラウザーのユーザーはパスワードを変更できません。この機能を有効にする場合は、サーバーが属しているドメインのポリシーでユーザーによるパスワード変更が禁止されていないことを確認してください。ユーザーによるパスワードの変更を有効にすると、この認証サービスを使用するストアにアクセスできるすべてのユーザーに、慎重に扱うべきセキュリティ機能が公開されることになります。組織のセキュリティポリシーにより、ユーザーパスワード変更機能が内部使用のみに制限される環境では、社内ネットワークの外側からそれらのストアにアクセスできないことを確認してください。

ユーザーがいつでもパスワードを変更できるように設定してある場合は、パスワードの有効期限切れが近いローカルユーザーがログオンしたときに警告が表示されます。デフォルトでは、ユーザーに対する通知期間は、適用される Windows ポリシーの設定によって決まります。または、カスタムの通知期間を構成することができます。

1. ［認証方法の管理］ウィンドウで、［ユーザー名とパスワード］>［設定］ドロップダウンメニューから［パスワードオプションの管理］を選択します。
2. ユーザーによるパスワードの変更を許可するには、［ユーザーにパスワードの変更を許可する］チェックボックスをオンにします。

   > 注:
   > このオプションを選択しない場合は、パスワードが失効してデスクトップやアプリケーションにアクセスできないユーザーをどのようにサポートするかを検討しておく必要があります。

3. ユーザーがパスワードを変更できるのが有効期限が切れたときのみにするか、いつでもにするか選択します。
4. パスワードの有効期限が切れる前にユーザーに通知するかどうかを選択します。



注 **1**:

StoreFront では、Active Directory の細かい設定が可能なパスワードポリシーはサポートされません。

注 **2**:

StoreFront サーバー上にすべてのユーザーのプロファイルを保存するための空き領域があることを確認してください。StoreFront ではユーザーのパスワードの失効が近いかどうかを確認するため、サーバー上に各ユーザーのローカルプロファイルが作成されます。ユーザーのパスワードを変更するには、StoreFront はドメインコントローラーと通信する必要があります。

注 **3**:

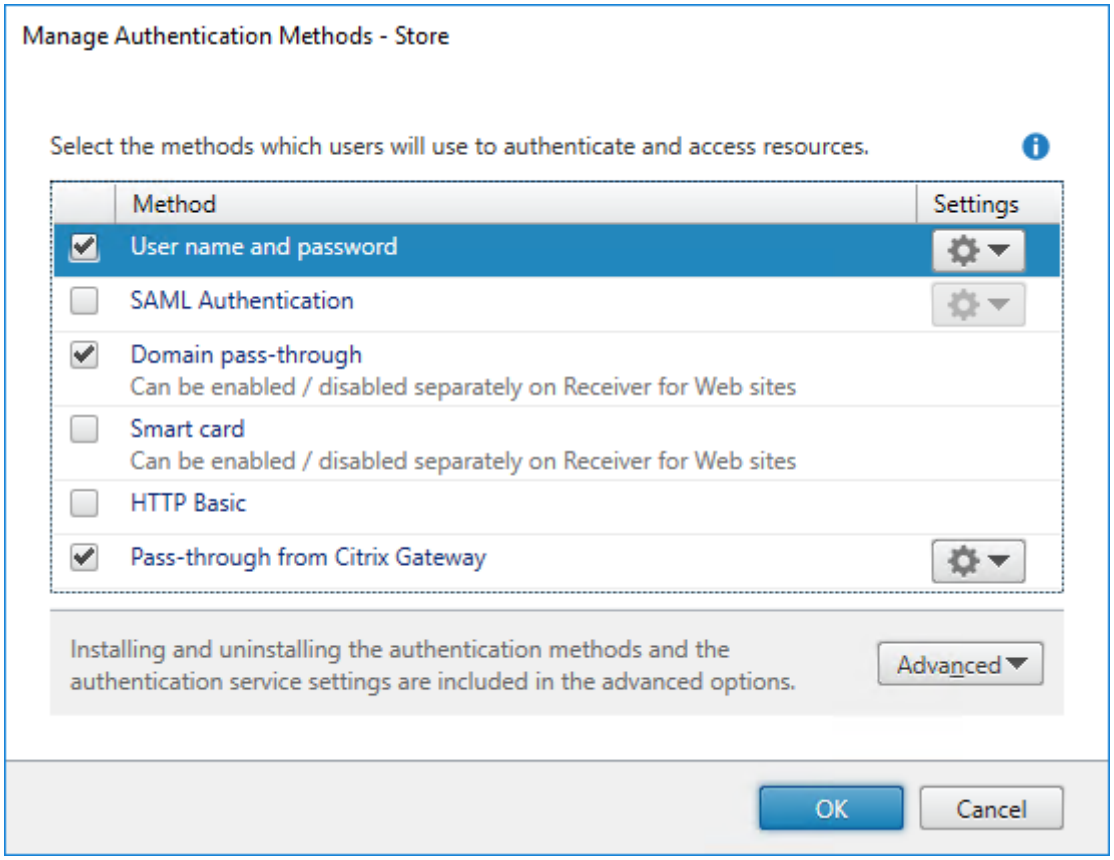
任意のときにパスワードを変更可能を有効または無効にすると、[**Citrix Gateway** からのパススルー] 認証の［パスワードオプションの管理］ の設定にも影響します。

資格情報パスワードの検証

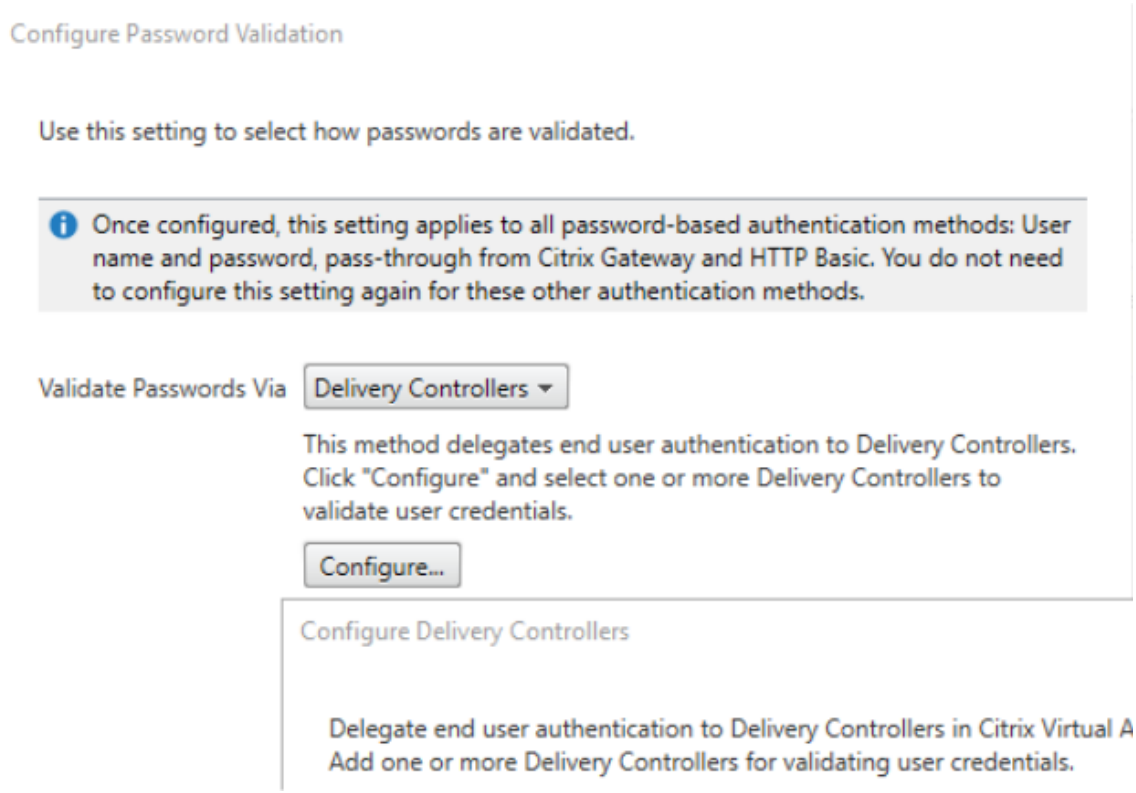
通常、StoreFront は Active Directory と直接通信して資格情報を検証します。

StoreFront が Citrix Virtual Apps and Desktops と同じドメイン内になく、Active Directory の信頼関係を利用できない場合には、Citrix Virtual Apps and Desktops Delivery Controller を使ってユーザー名とパスワード資格情報を認証するように StoreFront を構成できます:

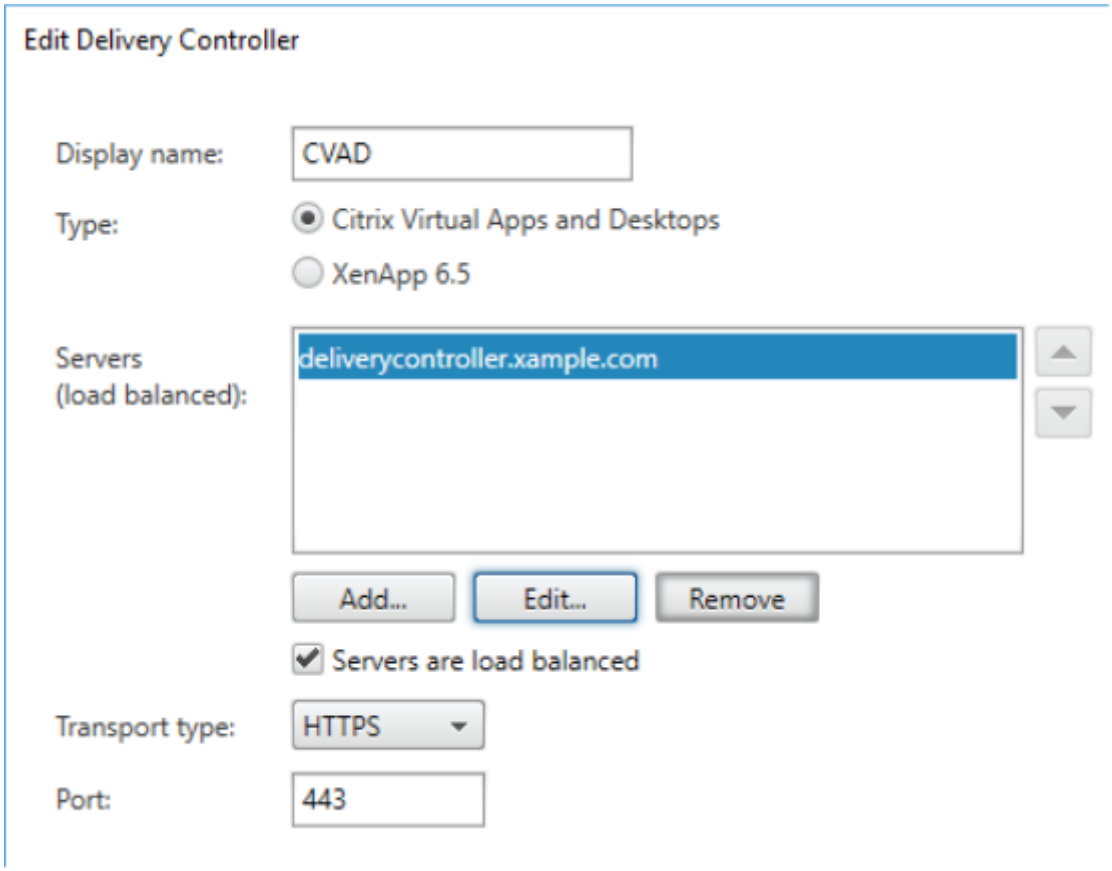
1. ［認証方法の管理］ウィンドウで、［ユーザー名とパスワード］**>**［設定］ドロップダウンメニューから、［パスワード確認の構成］を選択します。



2. ［パスワード検証方法］の一覧から ［**Delivery Controller**］を選択し、［構成］をクリックします。



3. ［**Delivery Controller** の構成］画面に従って、1 つまたは複数の **Delivery Controller** を追加して、ユーザー資格情報を確認し、［**OK**］をクリックします。



Active Directory の使用

1. ［認証方法の管理］ページで、［ユーザー名とパスワード］>［設定］の一覧から、［パスワード確認の構成］を選択します。
2. ［パスワード検証方法］ドロップダウンメニューから ［**Active Directory**］を選択し、［**OK**］をクリックします。

VDA へのシングルサインオン

ユーザーがリソースを起動すると、StoreFront はユーザーがストアへのサインオンに使用した資格情報を使用して VDA にシングルサインオンします。

ログオン画面のカスタマイズ

ログオン画面はテンプレートから生成され、通常は次の場所にあります。C:\inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\Templates\UsernamePassword.tfrm。画面をカスタマイズできます。

タイトルのテキスト

デフォルトでは、ユーザーがストアにログオンしても、ログオンダイアログボックスにタイトルテキストは表示されません。「ログオンしてください」というテキストを表示したり、カスタムメッセージを作成したりすることができます:

1. テキストエディターを使用して、認証サービスの UsernamePassword.tfrm ファイルを開きます。
2. ファイル内で次の行を見つけます。

```
@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
<!--NeedCopy-->
```

3. 先頭の **@*** と末尾の ***@** を削除して、このステートメントのコメントを解除します。

```
@Heading("ExplicitAuth:AuthenticateHeadingText")
<!--NeedCopy-->
```

これにより、Citrix Workspace アプリユーザーがこのストアにログオンしたときに、デフォルトのタイトル文字列である「Please log on」または「ログオンしてください」などが表示されます。

4. タイトル文字列を変更するには、テキストエディターを使って認証サービスの *ExplicitFormsCommon.xx.resx* ファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\resources\ディレクトリにあります。
5. ファイル内で次の要素を検索します。<value> 要素内の文字列を編集します。これにより、このストアのログオンダイアログボックスのタイトルが変更されます。

```
<data name="AuthenticateHeadingText" xml:space="preserve">
    <value>My Company Name</value>
</data>
<!--NeedCopy-->
```

ほかのロケールにいるユーザー用にログオンダイアログボックスのタイトルの文字列を変更するには、対象となる言語版の *ExplicitAuth.languagecode.resx* ファイルを編集します。ここで **languagecode** は、ロケール識別子です。

Windows 向け Citrix Workspace アプリでのパスワードおよびユーザー名のキャッシュ機能の無効化

Windows 向け Citrix Workspace アプリのデフォルトでは、ユーザーが StoreFront ストアにログオンしたときのパスワードがキャッシュされます。Windows 向け Citrix Workspace アプリでユーザーのパスワードをキャッシュしないようにするには、認証サービスのファイルを編集します。

1. テキストエディターを使って、inetpub\wwwroot\Citrix\[ストア名]Auth\App_Data\Templates\UsernamePassword
ファイルを開きます。
2. ファイル内で次の行を見つけます。


```
@SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
    "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
    ControlValue("SaveCredentials"))
<!--NeedCopy-->
```

3. 次のようにステートメントにコメントします。

```
<!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"),
    labelKey: "ExplicitFormsCommon:SaveCredentialsLabel",
    initiallyChecked: ControlValue("SaveCredentials")) -->
<!--NeedCopy-->
```

これにより、この認証サービスのストアにログオンするユーザーは、毎回パスワードの入力が必要になります。

デフォルトでは、Windows 向け Citrix Workspace では最後に入力されたユーザー名が自動的に抽出されて入力されます。[ユーザー名] フィールドの自動入力を無効にする場合、またはパスワードのキャッシュを無効にするための代替メカニズムについては、「Windows 向け Citrix Workspace アプリでのパスワードおよびユーザー名のキャッシュ機能の無効化」を参照してください。

Citrix Gateway を介したリモートアクセス

ユーザーがドメインのユーザー名とパスワードを使用してゲートウェイにサインオンするように Citrix Gateway を構成できます。これらの資格情報は StoreFront に渡され、ストアにサインオンできます。LDAP ユーザー名とパスワード認証用に Citrix Gateway を構成するには、NetScaler ドキュメントの「LDAP 認証」を参照してください。StoreFront を構成するには、「Citrix Gateway からのパススルー」を参照してください。

フェデレーション認証サービスの構成

June 6, 2024

SAML など、ユーザーが Citrix Workspace アプリに資格情報を直接入力しない認証方法を使用する場合、デフォルトでは VDA にシングルサインオンできません。このような場合、フェデレーション認証サービス（FAS）を使用して、証明書認証による VDA へのシングルサインオンを提供できます。

StoreFront で FAS を使用するには、PowerShell SDKを使用して StoreFront を構成する必要があります。Set-STFClaimsFactoryNamesを使用してクレームファクトリをFASClaimsFactoryに設定し、Set-STFStoreLaunchOptionsを使用して VDA ログオンデータのログオンプロバイダーをFASLogonDataProviderに設定します。

たとえば、ストアに対して FAS を有効にする場合:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]
$auth = Get-STFAuthenticationService -StoreService $store
```



```
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "FASClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "
    FASLogonDataProvider"
<!--NeedCopy-->
```

ストアの FAS を無効にするには:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "standardClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
<!--NeedCopy-->
```

[VirtualPath]を適切な仮想パス（例: /Citrix/Store）に置き換えます。

FAS サーバーの一覧およびその他の設定を構成するには、グループポリシーを使用する必要があります。詳しくは、FAS ドキュメントを参照してください。

ブラウザー経由でドメインパススルーまたはスマートカードを使用して認証する場合、FAS は使用されません。

FAS サーバーが利用できない

FAS サーバーが利用できない場合、デフォルトで起動に失敗します。ただし、FAS サーバーが利用できない場合、ユーザーが資格情報を入力して VDA にサインオンできるように StoreFront を構成できます。PowerShell を使用して設定を変更するには、パラメーターFederatedAuthenticationServiceFailoverを指定してコマンドレットSet-STFStoreLaunchOptionsを使用します。たとえば、ストアのフェールオーバーを有効にする場合:

```
$storeService = Get-STFStoreService -VirtualPath [VirtualPath]
Set-STFStoreLaunchOptions $storeService -
    FederatedAuthenticationServiceFailover $True
<!--NeedCopy-->
```

ストアの構成と管理

June 6, 2024

Citrix StoreFront では、Citrix Virtual Apps and Desktops からアプリケーションやデスクトップをまとめるストアを作成して管理し、ユーザーにリソースに対するセルフサービスアクセスをオンデマンドで提供できます。

タスク	詳細
ストアの作成	必要とするできるだけ多くの追加ストアを構成します。
ストアの構成	ストア設定の構成
ストアの削除	不必要なストアを削除します。
ユーザー用のストアプロビジョニングファイルのエクスポート	ストアに対して構成された Citrix Gateway 展開やビーコンなど、ストアに対する接続の詳細を含んでいるファイルを生成します。
ユーザーに対するストアの非表示および提供	ユーザーがメールアドレスによるアカウント検出機能または完全修飾ドメイン名（FQDN）を使って Citrix Workspace アプリを構成する場合、ユーザーに表示されているストアがユーザーのアカウントに追加されないようにします。
Kerberos 委任の構成	StoreFront が Delivery Controller への認証に Kerberos 委任を使用するかどうかを構成します。
ストアに表示するリソースの管理	ストアからのリソースの追加と削除
Citrix Gateway を介したストアへのリモートアクセスの管理	公共のネットワークから接続するユーザーに対して Citrix Gateway を介したストアへのアクセスを構成します。
証明書失効一覧（CRL）のチェック	StoreFront で、CVAD Delivery Controller が使用する TLS 証明書の状態を公開された証明書失効一覧（CRL）を使用して確認するよう構成します。
共通のサブスクリプションデータストアを共有する 2 つの StoreFront ストアの構成	共通のサブスクリプションデータストアを共有する 2 つの StoreFront ストアの構成
お気に入りの有効化または無効化	ストアのお気に入りを有効または無効にします。
ストアのサブスクリプションデータの管理	サブスクリプションデータ（お気に入り）を表示、インポート、エクスポート、および完全消去します。
共通のサブスクリプションデータストアを共有する 2 つの StoreFront ストアの構成	共通のサブスクリプションデータベースを共有する 2 つのストアの構成
Microsoft SQL Server を使用したお気に入りデータの保存	サブスクリプション（お気に入り）データを保存するために、外部 SQL Server データベースを使用します。
Citrix Virtual Apps and Desktops の構成	ストア Web サイトでのリソースの表示方法に関して Citrix Virtual Apps and Desktops 設定を構成します
ストアの詳細設定	上級ストア設定を構成します。
最適な HDX ルーティング	どのゲートウェイをどのリソースへの接続に使用するかを構成します。
デフォルトの ica 設定	HDX 設定を default.ica に追加して構成します

タスク	詳細
ICA ファイルの署名	ica ファイルの署名を構成します
Windows のショートカット	Windows 向け Citrix Workspace で、お気に入りおよび必須アプリのショートカットを［スタート］メニューおよびデスクトップに作成する方法を構成します。

ストアの作成

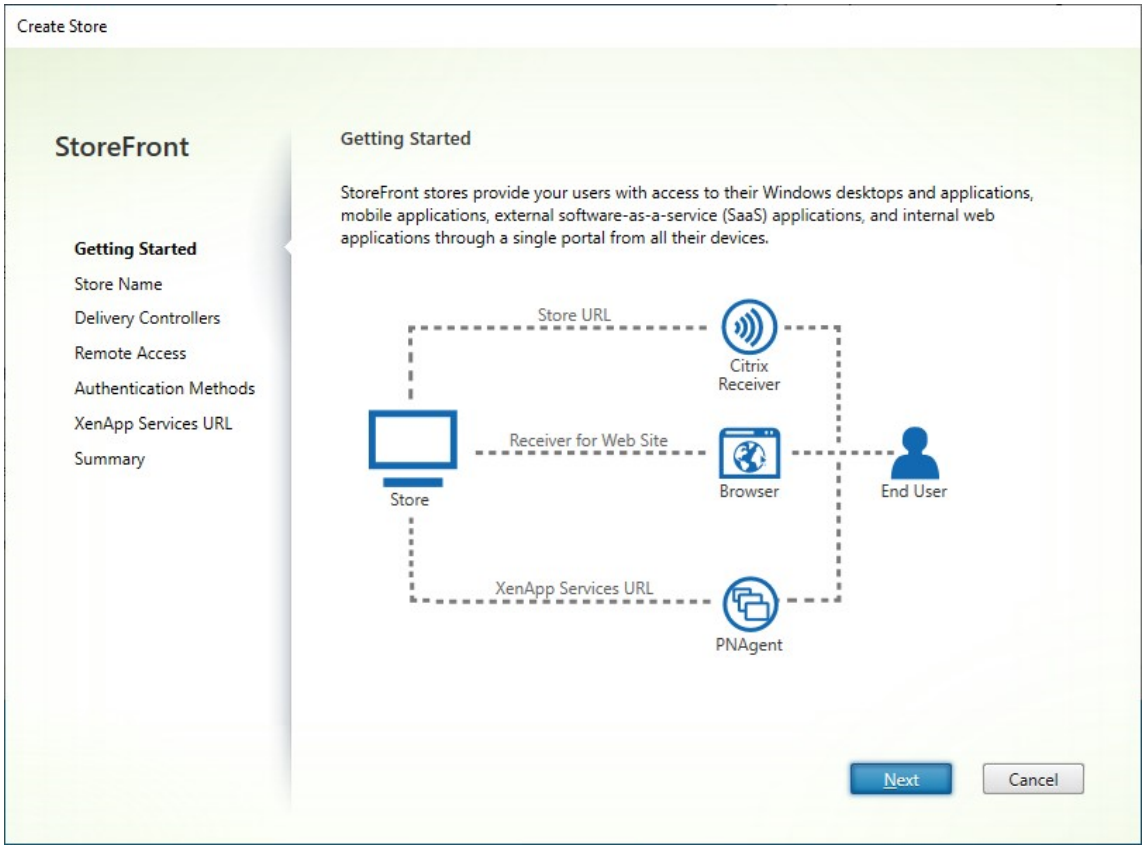
June 6, 2024

ストアは必要なだけ作成できます。たとえば、特定のユーザーグループ用にストアを作成したり、特定のリソースセットを集約するストアを作成したりできます。

> 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。

ストアを作成するには、そのストアのユーザーにリソースを提供するサーバーを指定して、その通信構成を行います。次に、Citrix Gateway 経由でのストアへのリモートアクセスを設定します（任意）。

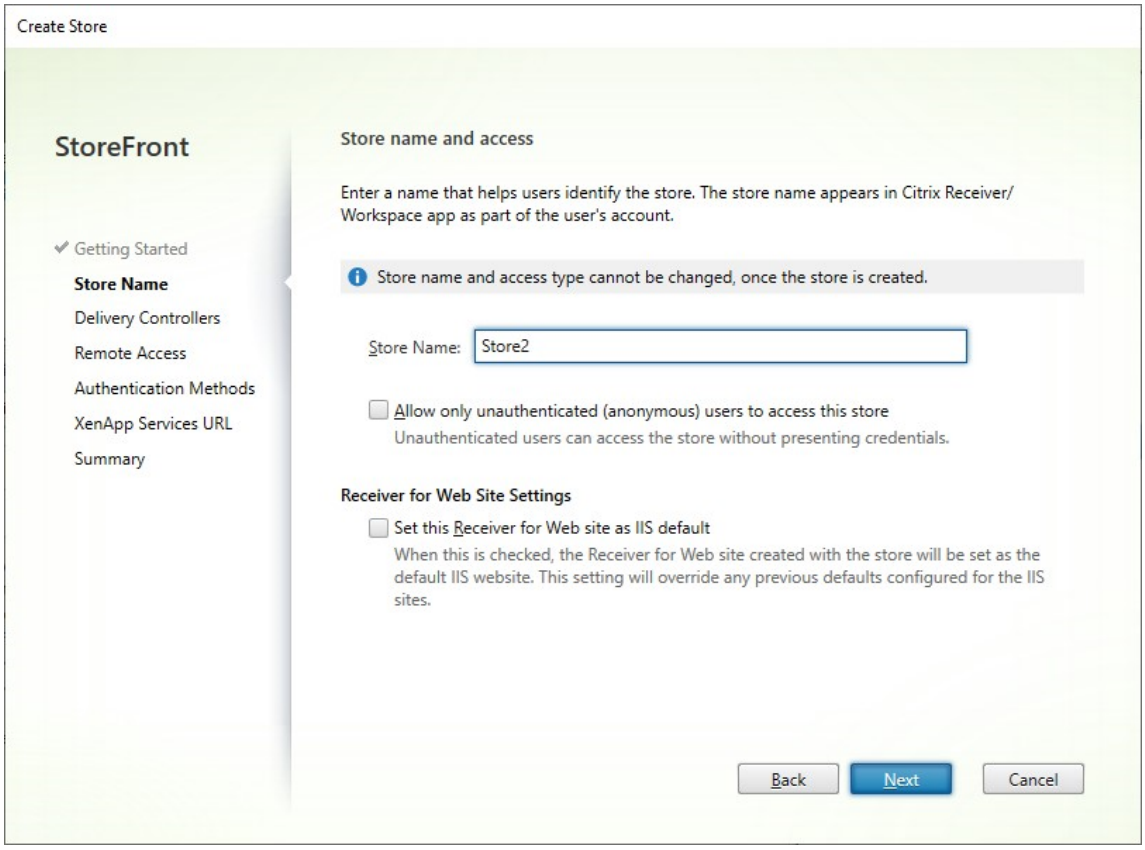
1. ［操作］ペインで、［ストアの作成］をクリックします。



［次へ］をクリックします。

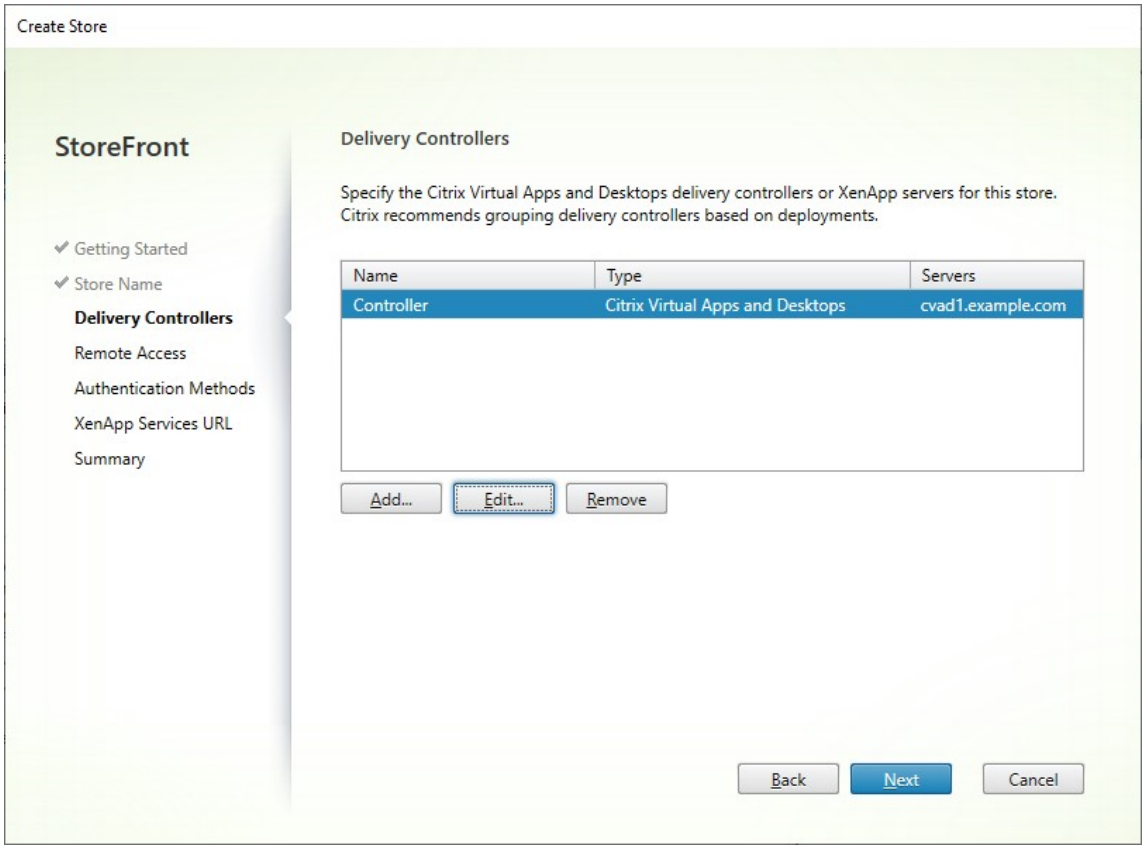
2. ［ストア名］タブで次のように入力します：

   - ストア名の入力
   - ユーザーが匿名または認証されていない状態でストアにアクセスできるようにする場合は、［このストアへのアクセスを非認証（匿名）ユーザーにのみ許可する］にチェックを入れます。認証が不要なストアを作成すると、［認証方法］ページおよび ［リモートアクセス］ページは利用できなくなり、左側の ［サーバーグループノード］ペインと［操作］ペインが、［ベース **URL** の変更］に置き換わります（ドメインに参加していないサーバーではサーバーグループを利用できないため、これが使用できる唯一のオプションです）。



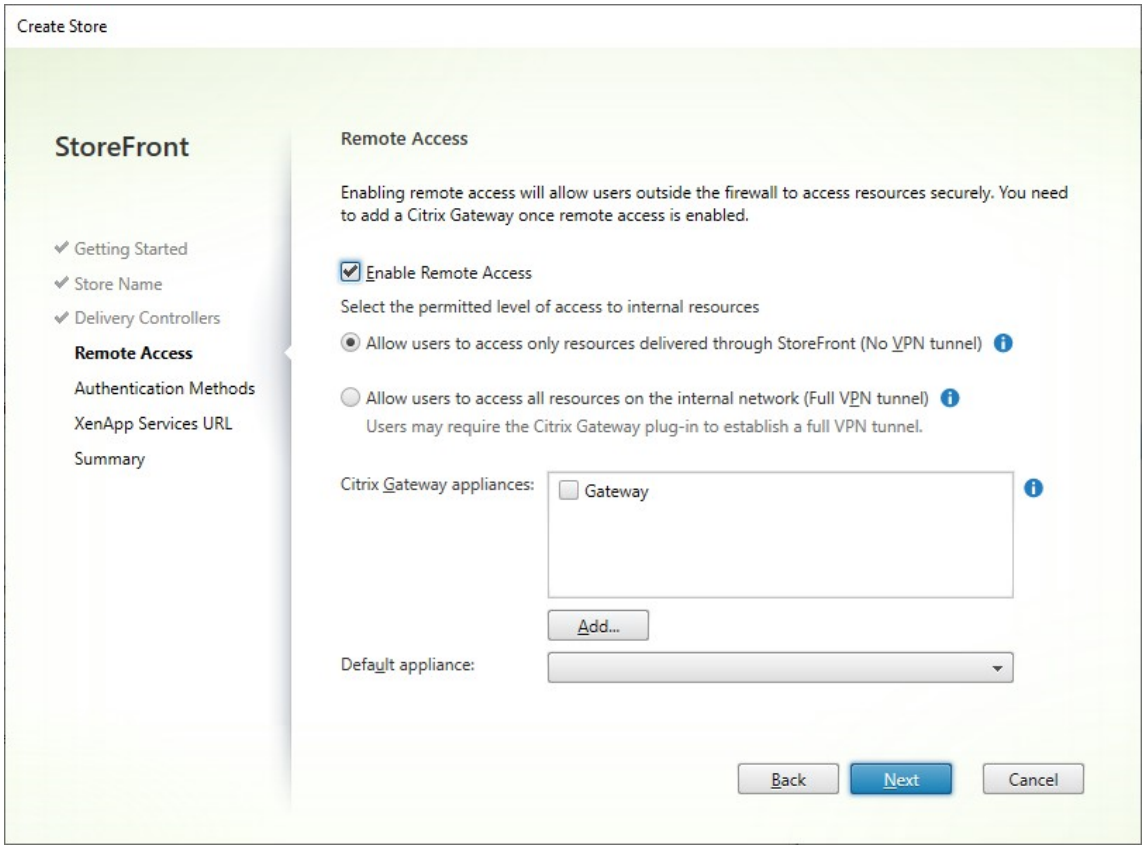
［次へ］をクリックします。

3. ［**Delivery Controller**］タブで、Virtual Desktops とアプリケーションのリソースフィードを追加します。詳しくは、「ストアに表示するリソースの管理」を参照してください。



［次へ］をクリックします。

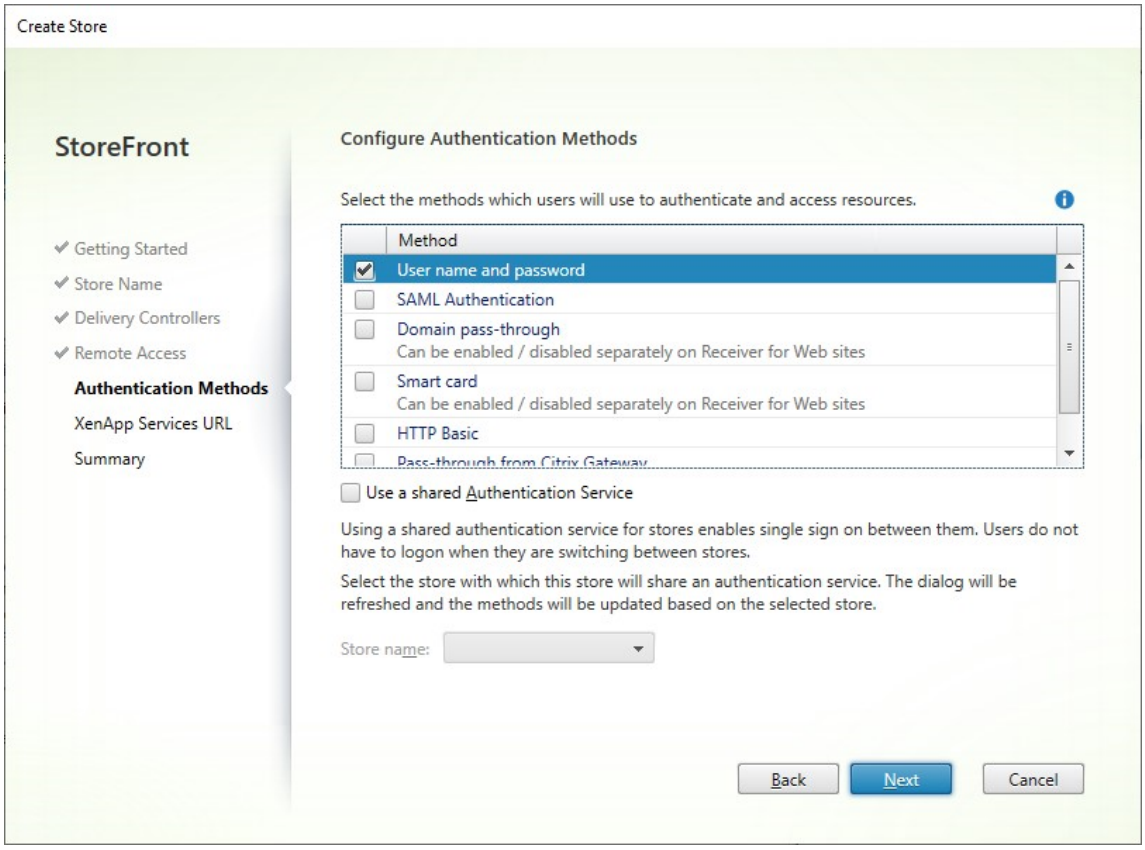
4. ［リモートアクセス］タブで、Citrix Gateway 経由でストアを利用可能にするかどうかを選択します。詳しくは、「Citrix Gateway を介したストアへのリモートアクセスの管理」を参照してください。



5. ［認証方法］タブで、ユーザーがストアにアクセスするための認証方法を選択し、［次へ］をクリックします。

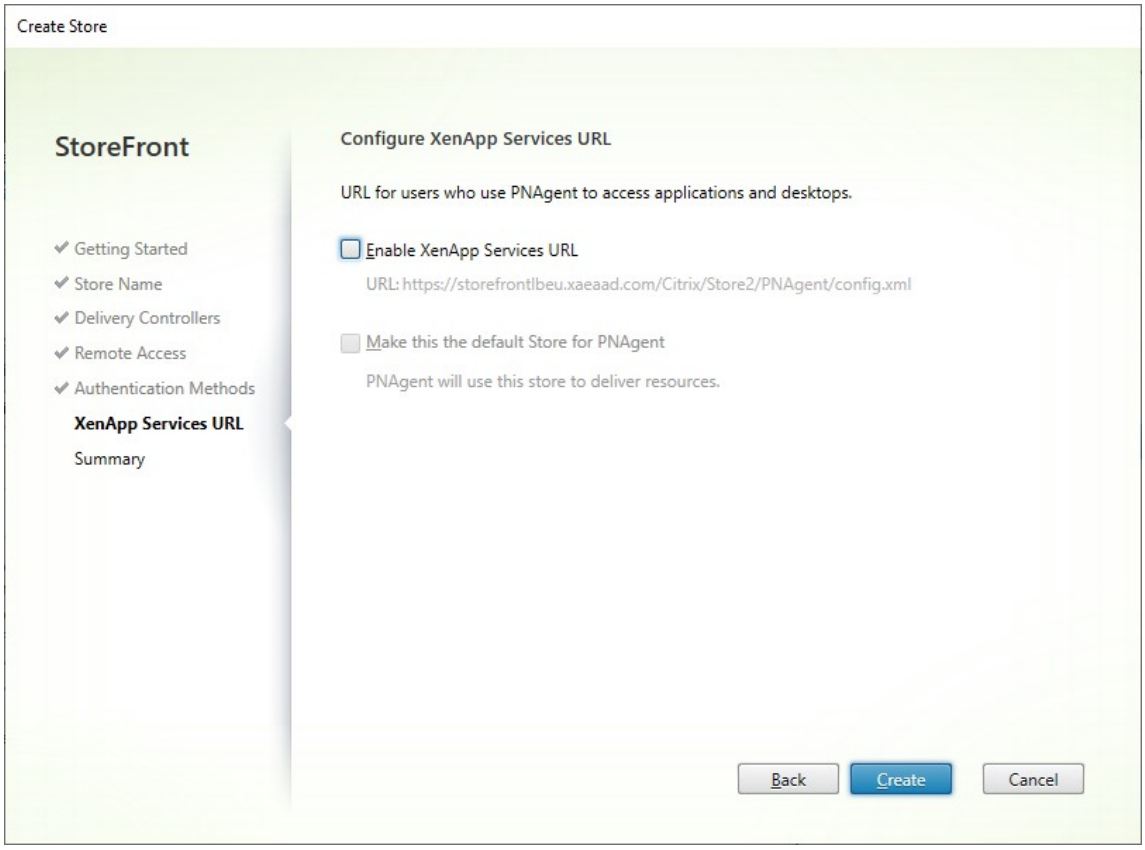
   使用可能な認証方法について詳しくは、「認証の構成」を参照してください。

   このストアの認証方法を個別に構成するのではなく、認証の構成を別のストアと共有することができます。これを行うには、［共有認証サービスを使用］にチェックを入れて、既存のストアを選択します。



［次へ］をクリックします。

6. ［**XenApp Services** の **URL**］タブで、PNAgent を必要とするレガシーデバイスがある場合は ［**XenApp Services** の **URL** を有効にする］にチェックを入れたままにし、そうでない場合はチェックを外します。



［作成］をクリックします。

7. ストアが作成されたら、［完了］をクリックします。

新しいストアが作成されると、ユーザーがストアにアクセスできるようにするための新しい Web サイトも作成されます。この Web サイトを構成したり、別の Web サイトを作成したりできます。

PowerShell SDK

PowerShell SDKを使用してストアを作成するには:

1. Add-STFAuthenticationServiceを使用して認証サービスを作成します。慣例により、仮想パスは通常/Citrix/[StoreName]Authです。または、Get-STFAuthenticationServiceを使用して既存の認証サービスを取得することもできます。匿名ストアの場合、この手順は必要ありません。
2. 必要に応じて認証サービスを構成します。「認証の構成」を参照してください。
3. Add-STFStoreServiceを呼び出します。
   - ストアの仮想パスを選択し、これを-VirtualPathパラメーターとして設定します。通常、これは/Citrix/[StoreName] です。
   - 手順 1 で作成した認証サービスに-AuthenticationServiceを設定します。または、匿名ストアの場合は-Anonymous $Trueを設定します

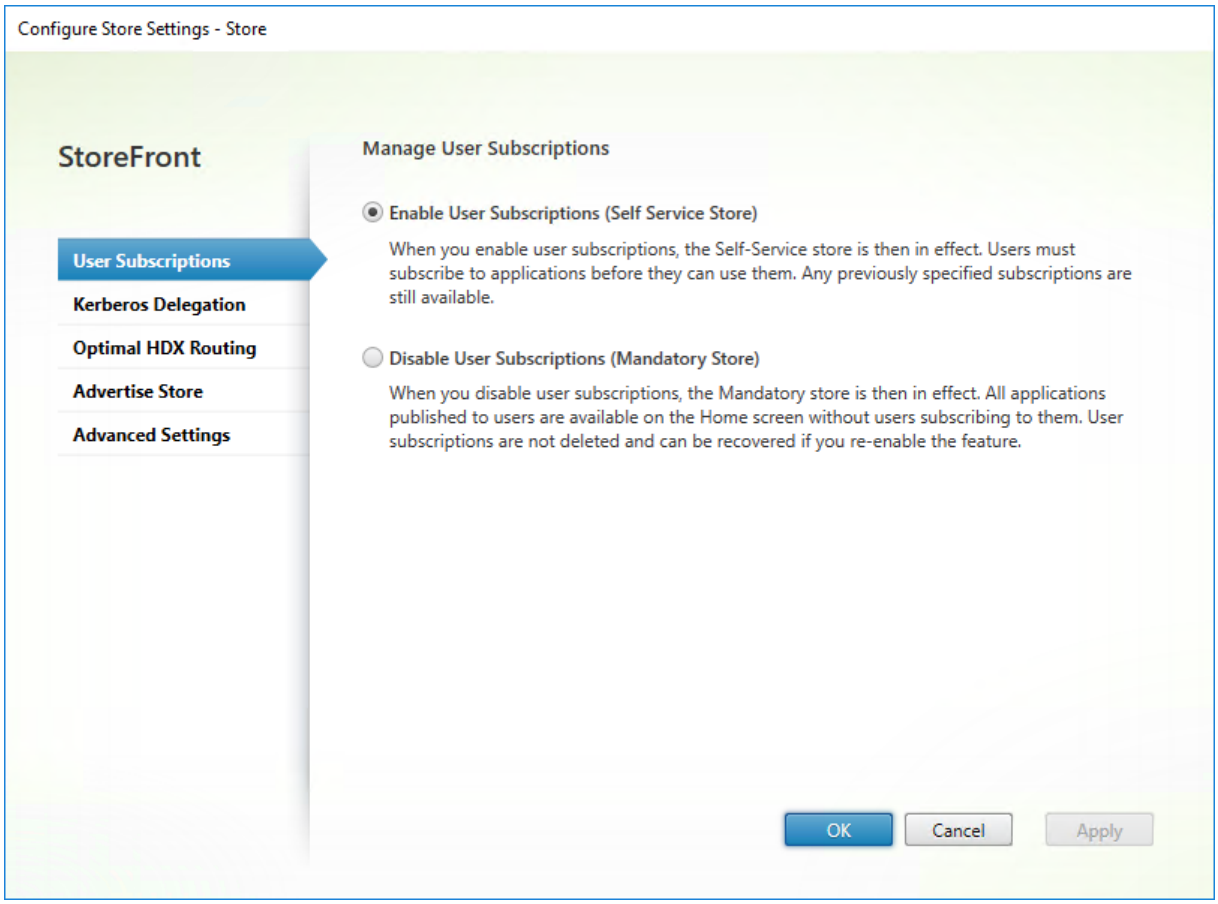
- 1 つのリソースフィードの詳細を含めることができます。それ以上のリソースフィードは個別に構成する必要があります。

ストアの構成

June 6, 2024

ストアを変更するには、以下を実行します:

1. Citrix StoreFront 管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインで［ストア設定の構成］をクリックします。
2. ［ユーザーのサブスクリプション］ タブに移動して、お気に入りを有効にするかどうかを構成します。
3. Delivery Controller の認証にストアがKerberos 委任を使用するかどうかを設定するには、［Kerberos 委任］タブに移動します。
4. ［最適な HDX ルーティング］ タブに移動し、場所に応じてアプリとデスクトップの起動にどのゲートウェイを使用するかを構成します。
5. ［ストアのアドバタイズ］ タブに移動し、ユーザーが FQDN またはメールアドレスを入力したときに Workspace アプリがユーザーに対してストアを表示するかどうかを構成します。

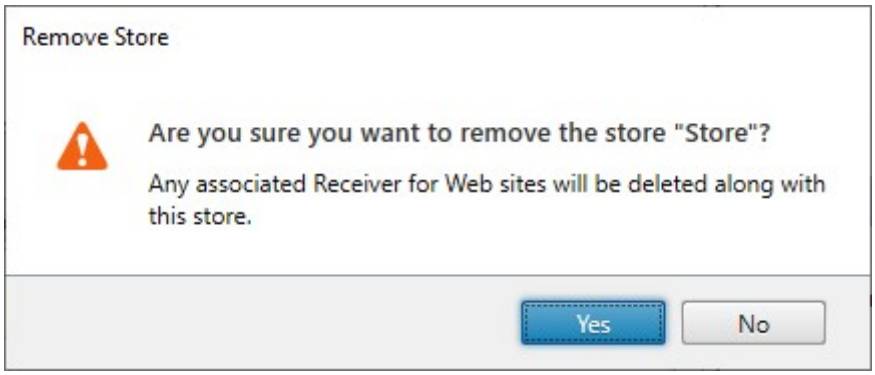


ストアの削除

June 6, 2024

ストアを削除するには:

1. 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. ［操作］ペインで、［ストアの削除］をクリックします。
3. 確認のウィンドウで ［はい］をクリックします。



ストアを削除すると、関連付けられている Web サイトもすべて削除されます。

ユーザー用のストアプロビジョニングファイルのエクスポート

June 6, 2024

ストアに対して構成された Citrix Gateway 展開やビーコンなど、ストアに対する接続の詳細を含んでいるファイルを生成できます。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 Citrix Workspace アプリを簡単に構成できるようになります。ユーザーは、Web ブラウザー経由でストアにアクセスするときに、Citrix Workspace アプリのプロビジョニングファイルをダウンロード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. 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。
2. ［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。

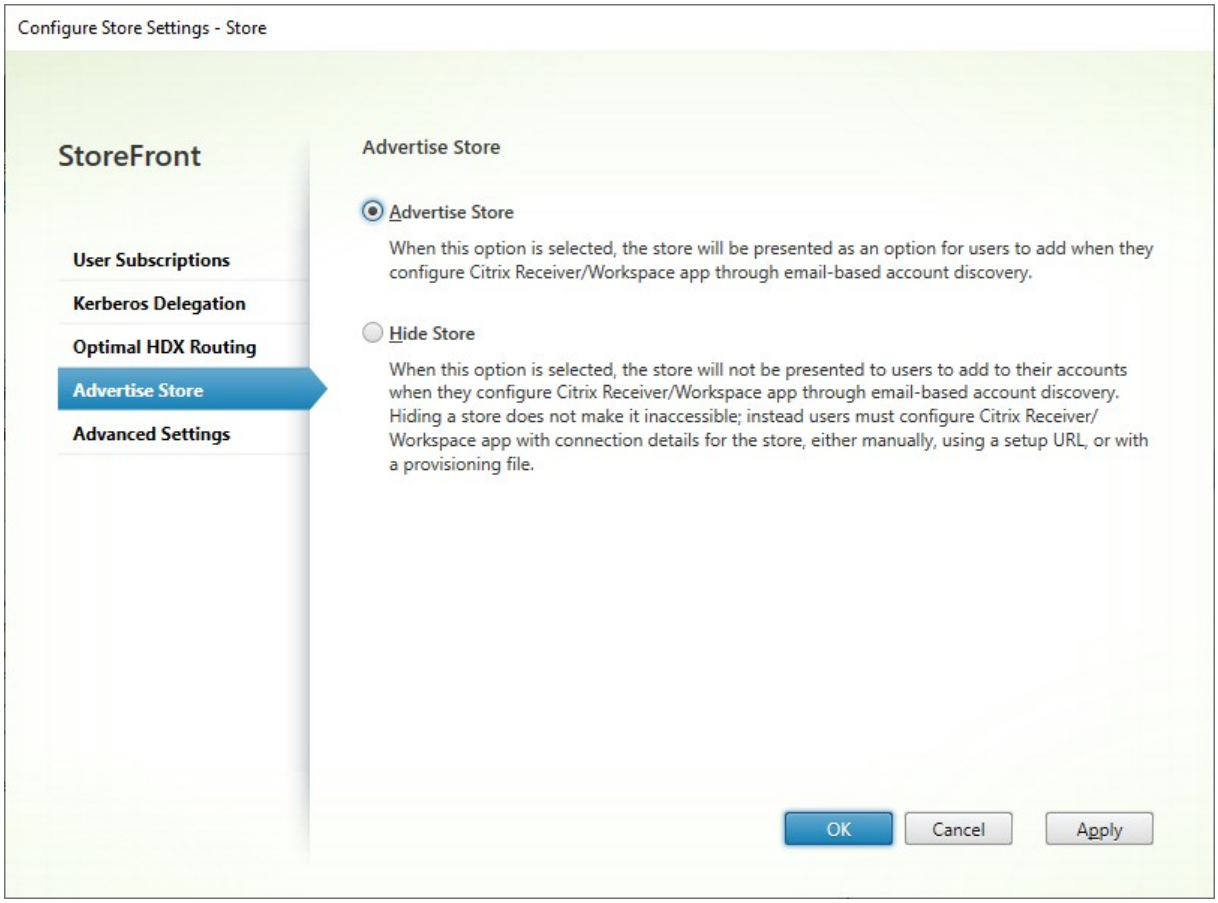
ユーザーに対するストアの非表示および提供

June 6, 2024

ユーザーがメールアドレスによるアカウント検出機能または完全修飾ドメイン名（FQDN）を使って Citrix Workspace アプリを構成する場合に、ユーザーに表示されているストアがユーザーのアカウントに追加されるかどうかを選べます。新規に作成するストアのデフォルトでは、ユーザーが Citrix Receiver で StoreFront ストアを追加するときに、オプションとしてそのストアが表示されます。ストアを非表示にしても、ユーザーがストアにアクセスできなくなるわけではありません。ユーザーは、メールアドレスによるアカウント検出機能の代わりに Citrix Workspace アプリでのストア接続を手作業で構成したり、セットアップ URL やプロビジョニングファイルを使用したりする必要があります。

> 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. Citrix StoreFront 管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインで ［ストア設定の構成］>［ストアのアドバタイズ］の順にクリックします。
2. ［ストアのアドバタイズ］ページで ［ストアのアドバタイズ］または ［ストアの非表示］を選択します。



Kerberos 委任

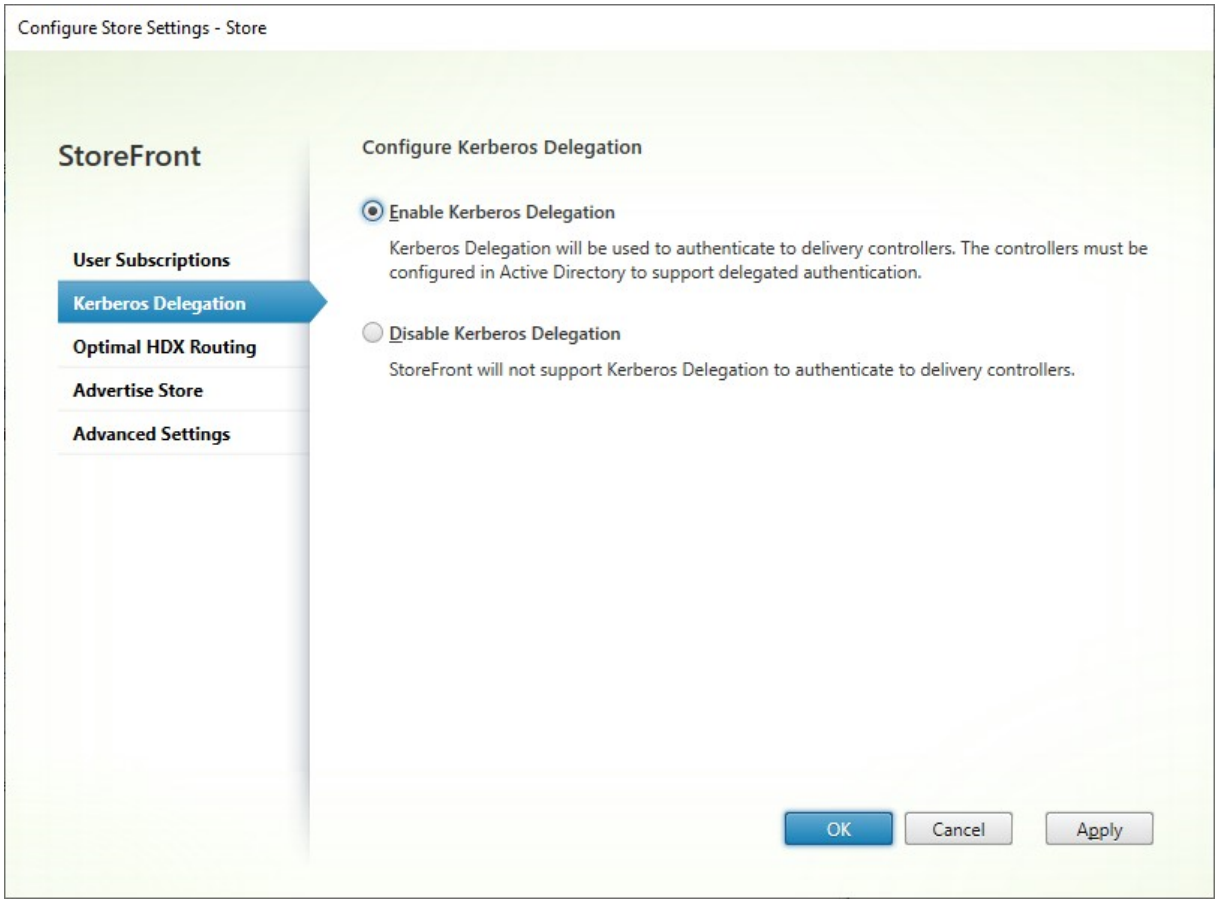
June 6, 2024

> 注:
>
> Kerberos 委任は廃止され、XenApp 6.5 以前でのみ使用できます。サポートされているバージョンの Citrix Virtual Apps and Desktops では使用できません。

ドメインパススルーまたはスマートカード認証を直接または Citrix Gateway 経由で使用する場合、StoreFront にはユーザーの資格情報がないため、ユーザーの資格情報を使用して Delivery Controller に認証できません。XenApp 6.5 以前を使用している場合は、Kerberos 委任を有効にして、StoreFront がユーザーに偽装して Delivery Controller に認証できるようにすることができます。このためには、Active Directory 内で委任を構成する必要があります。

1. [操作] ペインでストアを選択し、[ストア設定の構成] をクリックします。
2. [**Kerberos** 委任] タブを選択します。

3. [**Kerberos** 委任を有効にする] か、[**Kerberos** 委任を無効にする] かどうかを選択します。
4. [適用] または [**OK**] を押して変更を保存します。



PowerShell SDK

Kerberos 委任を構成するには、パラメーター`-KerberosDelegation`を指定したコマンドレットSet-STFStoreServiceを使用します

ストアに表示するリソースの管理

June 6, 2024

[**Delivery Controller** の管理] 画面を使用して、Citrix Virtual Apps and Desktops、Citrix Desktops as a Service、および Citrix Secure Private Access によって提供されるリソースフィードを追加、変更、削除します。

リソースフィードの表示

1. Citrix StoreFront 管理コンソール内の左ペインで ［ストア］ノードを選択します。
2. 結果ペインでストアを選択します
3. ［操作］ペインの ［**Delivery Controller** の管理］をクリックします。

PowerShell SDK を使用してリソースフィードを表示する

PowerShell SDKで、コマンドGet-STFStoreFarmを使用して、すべてのリソースフィードまたは特定のリソースフィードを一覧表示します。

リソースフィードの追加

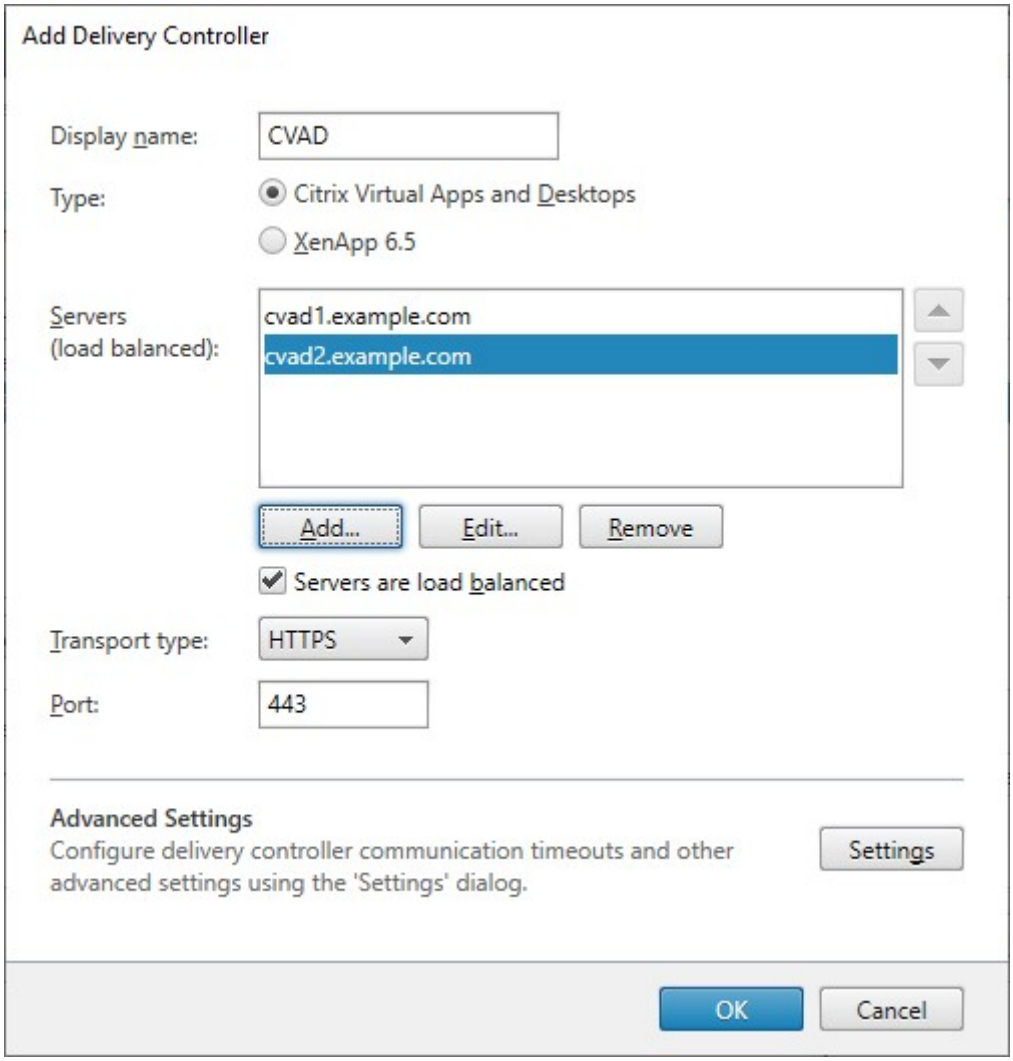
Citrix Virtual Apps and Desktops のリソースフィードの追加

1. ［**Delivery Controller** の管理］画面で ［追加］をクリックします。
2. フィードを識別するのに役立つ ［表示名］を入力します。
3. ［種類］として ［**Citrix Virtual Apps and Desktops**］を選択します。
4. ［サーバー］で ［追加］をクリックし、Delivery Controller の名前を入力します。各 Delivery Controller に対して繰り返します。負荷分散またはフェールオーバーのために、少なくとも 2 台のサーバーを用意することをお勧めします。
5. ［サーバーを負荷分散する］オプションを選択することをお勧めします。これにより、StoreFront は、起動時に毎回一覧からサーバーをランダムに選択して、すべての Delivery Controller またはコネクタ間で負荷を分散します。このオプションが選択されていない場合、サーバー一覧は優先度順のフェールオーバー一覧として機能します。この場合、一覧の最初のアクティブな Delivery Controller またはコネクタで 100% の起動が発生します。そのサーバーがオフラインになった場合は、一覧の 2 番目の Delivery Controller で 100% の起動が発生し、以降同様に順番に動作します。
6. ［トランスポートの種類］の一覧から、StoreFront でサーバーとの通信に使用する接続の種類を選択します。
   - 暗号化されていない接続でデータを送信するには ［**HTTP**］を選択します。このオプションを選択する場合は、StoreFront とサーバー間の接続を何らかの方法で保護することを検討してください。
   - 暗号化された接続でデータを送信するには（推奨）、［**HTTPS**］を選択します。Citrix Virtual Apps and Desktops サーバーに対してこのオプションを選択する場合は、Citrix XML Service がポートを IIS（Microsoft インターネットインフォメーションサービス）と共有する設定になっていることと、IIS が HTTPS をサポートするように構成されていることを確認してください。

> 注:
>
> StoreFront とサーバーの間の通信を HTTPS で保護する場合は、［サーバー］ボックスの一覧に指定し

> たサーバー名がそのサーバーの証明書のサーバー名と一致することを確認してください（大文字/小文字は区別されます）。

7. StoreFront がサーバーに接続するときに使用するポートを指定します。デフォルトでは、HTTP 接続では 80、HTTPS 接続では 443 が使用されます。指定したポートは、Citrix XML Service で使用されるものである必要があります。



Citrix Desktops as a Service のリソースフィードの追加

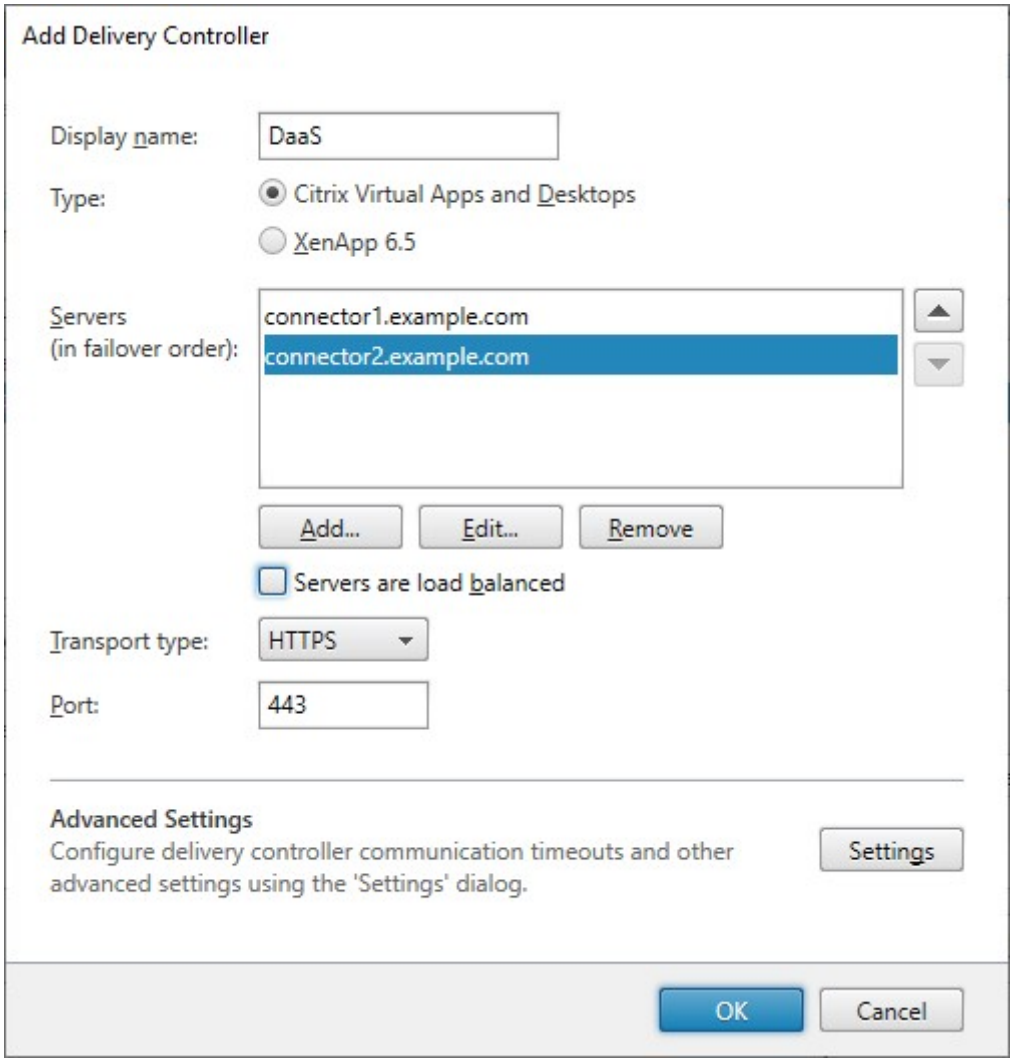
1. ［**Delivery Controller** の管理］画面で ［追加］をクリックします。
2. フィードを識別するのに役立つ ［表示名］を入力します。
3. ［種類］として ［**Citrix Virtual Apps and Desktops**］を選択します。
4. ［サーバー］で ［追加］をクリックし、Cloud Connector の名前を入力します。サーバーまたはコネクタごとに繰り返します。冗長性のために少なくとも 2 つのコネクタを用意することをお勧めします。複数のリソース

の場所がある場合は、すべてのリソースの場所から Cloud Connector を追加して、停止が発生した場合に StoreFront がローカルホストキャッシュを使用して適切な場所で VDA を起動できるようにすることをお勧めします。

5. 複数の場所からのコネクタがある場合は、StoreFront サーバーへの遅延が最も短いコネクタを一覧の一番上に置いて、［サーバーを負荷分散する］オプションをオフにすることをお勧めします。コネクタは情報を DaaS Delivery Controller にプロキシするだけであるため、負荷分散を使用するメリットは限定的です。
6. ［トランスポートの種類］の一覧から、StoreFront でサーバーとの通信に使用する接続の種類を選択します。
   - 暗号化されていない接続でデータを送信するには ［**HTTP**］を選択します。このオプションを選択する場合は、StoreFront と Cloud Connector 間の接続を何らかの方法で保護することを検討してください。
   - 暗号化された接続でデータを送信するには（推奨）、［**HTTPS**］を選択します。このオプションを選択した場合は、Cloud Connector が HTTPS 用に構成されていることを確認する必要があります。

   > 注:
   >
   > StoreFront とサーバーの間の通信を HTTPS で保護する場合は、［サーバー］ボックスの一覧に指定したサーバー名がそのサーバーの証明書のサーバー名と一致することを確認してください（大文字/小文字は区別されます）。

7. StoreFront がサーバーに接続するときに使用するポートを指定します。デフォルトでは、HTTP 接続では 80、HTTPS 接続では 443 が使用されます。



XenApp 6.5 のリソースフィードの追加

XenApp 6.5 は Citrix ではサポートされていません。管理コンソールを使用して新しい XenApp 6.5 リソースフィードを追加できません。ただし、PowerShell を使用して続行できます。

Citrix Secure Private Access のリソース フィードの追加

StoreFront サーバーが Citrix Secure Private Access 用に構成されている場合は、Citrix Secure Private Access リソースフィードを追加できます。

1. StoreFront の ［ストア］ > ［**Delivery Controllers**］に移動します。
2. ［追加］をクリックします。
3. ［**Delivery Controller** の追加］ウィンドウで、フィードを識別するための ［表示名］を指定します。

4. ［タイプ］として ［**Citrix Secure Private Access**］を選択します。
5. ［Citrix Secure Private Access］のサーバー名を入力します。
6. ［トランスポートの種類］ドロップダウンから、サーバーとの通信に使用できる接続の種類を選択します。

    - **HTTP**：暗号化されていない接続でデータを送信します：

    > 注：
    >
    > **HTTP** を選択する場合は、StoreFront とサーバー間の接続を何らかの方法で保護することを検討してください。

    - **HTTPS**：SSL（Secure Sockets Layer）または TLS（Transport Layer Security）を使用する保護された HTTP 接続でデータを送信します。

7. サーバーへの接続に使用するポートを指定します。**HTTP** のデフォルトポートは 80 で、**HTTPS** のデフォルトポートは 443 です。
8. ［**OK**］をクリックします。

PowerShell SDK を使用してリソースフィードを作成する

リソースフィードを追加するには、Add-STFStoreFarmコマンドを使用します

- Citrix Virtual Apps and Desktops または Citrix Desktops as a Service の場合は、`FarmType`を`XenDesktop`に設定します。
- XenApp 6.5 の場合は、`FarmType`を`XenApp`に設定します。
- Citrix Secure Private Access の場合は、`FarmType`を`SPA`に設定します。

リソースフィードの変更

［**Delivery Controller** の管理］画面でリソースフィードを選択し、［編集］をクリックします。

PowerShell SDK を使用してリソースフィードを変更する

PowerShell を使用してリソースフィードを変更するには、コマンドSet-STFStoreFarmを使用します

リソースフィードの削除

［**Delivery Controller** の管理］画面でリソースフィードを選択し、［削除］をクリックします。

PowerShell SDK を使用してリソースフィードを削除する

PowerShell を使用してリソースフィードを削除するには、コマンドRemove-STFStoreFarmを使用します

サーバーバイパス動作の構成

リソースを提供するサーバーの一部が使用できなくなったときのパフォーマンスを向上させるために、応答しないサーバーが StoreFront により一時的にバイパスされます。バイパスされたサーバーは StoreFront により無視され、リソースのアクセスに使用されません。このバイパスの期間は、次のパラメーターで指定します:

- ［すべての失敗のバイパス時間］では、特定の Delivery Controller のすべてのサーバーがバイパスされている場合に ［バイパス時間］の代わりに適用される短い期間を、分単位で指定します。デフォルトは 0 分です。
- ［バイパス時間］では、特定のサーバーへの接続に失敗した後で、StoreFront がそのサーバーをバイパスする期間を分単位で指定します。デフォルトのバイパス時間は 60 分間です。

［すべての失敗のバイパス時間］指定時の考慮事項

［すべての失敗のバイパス時間］を長く設定すると、特定の Delivery Controller を使用できないことによる影響を小さくすることができますが、一時的なネットワーク障害やサーバー障害の後で、ユーザーがこの Delivery Controller のリソースをその期間使用できなくなるという悪影響もあります。多くの Delivery Controller を単一のストア用に構成している場合、特に、業務に重要ではない Delivery Controller の場合は、［すべての失敗のバイパス時間］の値を大きめにすることを検討してください。

［すべての失敗のバイパス時間］を短くするとその Delivery Controller で提供されるリソースの可用性は高まりますが、単一のストアを構成する多くの Delivery Controller のうちの複数台が使用できない場合に、クライアント側でタイムアウトが発生しやすくなります。少数のファームを構成していて、業務に重要な Delivery Controller の場合は、デフォルト値の 0 分を使用することをお勧めします。

バイパスパラメーターを変更するには

1. Citrix StoreFront 管理コンソール内の左ペインで ［ストア］ノードを選択します。
2. 結果ペインでストアを選択します。
3. ［操作］ペインの ［**Delivery Controller** の管理］をクリックします。
4. コントローラーを選択して ［編集］をクリックし、［**Delivery Controller** の編集］画面で ［設定］をクリックします。
5. ［詳細設定］で ［設定］をクリックします。
6. ［詳細設定の構成］ダイアログボックスで、次の操作を行います:

    a) ［すべての失敗のバイパス期間］の行で 2 番目の列をクリックして、すべてのサーバーが応答しなくなった後に Delivery Controller がオフラインと見なされる時間を分単位で入力します。

b)［バイパス時間］の行で 2 番目の列をクリックして、1 つのサーバーが応答しなくなった後にオフラインと見なされる時間を分単位で入力します。

ユーザーをリソースフィードにマッピングする

デフォルトでは、ストアにアクセスしているユーザーには、そのストア用に構成されているすべてのリソースフィードから使用可能なすべてのリソースが集約されて表示されます。ユーザーごとに異なるリソースを提供するには、ストアや StoreFront 展開環境を個別に構成できます。または、Microsoft Active Directory グループのユーザーメンバーシップに基づいて、特定の展開環境へのアクセスを提供することができます。これにより、単一のストアで、ユーザーグループごとに異なるエクスペリエンスを構成できます。

たとえば、すべてのユーザーに共通するリソースを 1 つの展開環境でグループ化し、別の展開環境では経理（Accounts）部門用に財務アプリケーションをグループ化します。このような構成では、Accounts ユーザーグループに属していないユーザーは、このストアにアクセスしても共通リソースしか表示されません。Accounts ユーザーグループのメンバーには、共通リソースと財務アプリケーションの両方が表示されます。

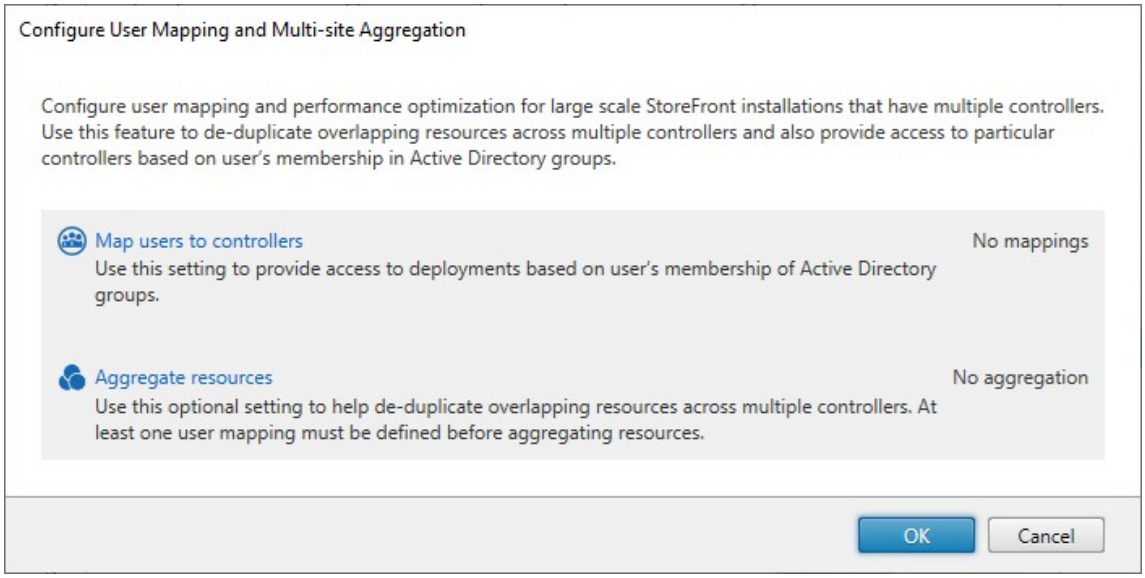
別の例として、より高速で強力なハードウェアを使用するパワーユーザー用の展開環境を作成して、ほかの展開環境と同じリソースを提供します。これにより、エグゼクティブチームなど、ビジネスクリティカルなユーザーのエクスペリエンスを向上させることができます。このストアにアクセスすると、すべてのユーザーに同じデスクトップやアプリケーションが表示されますが、Executives ユーザーグループのメンバーは、パワーユーザー用の展開環境のリソースに優先的に接続されます。

> 注:
>
> これにより、リソースフィード全体がフィルタリングされます。さらに、リソースフィード内では、Citrix Virtual Apps and Desktops Studio 構成内のユーザーグループでアプリケーションをフィルタリングできます。

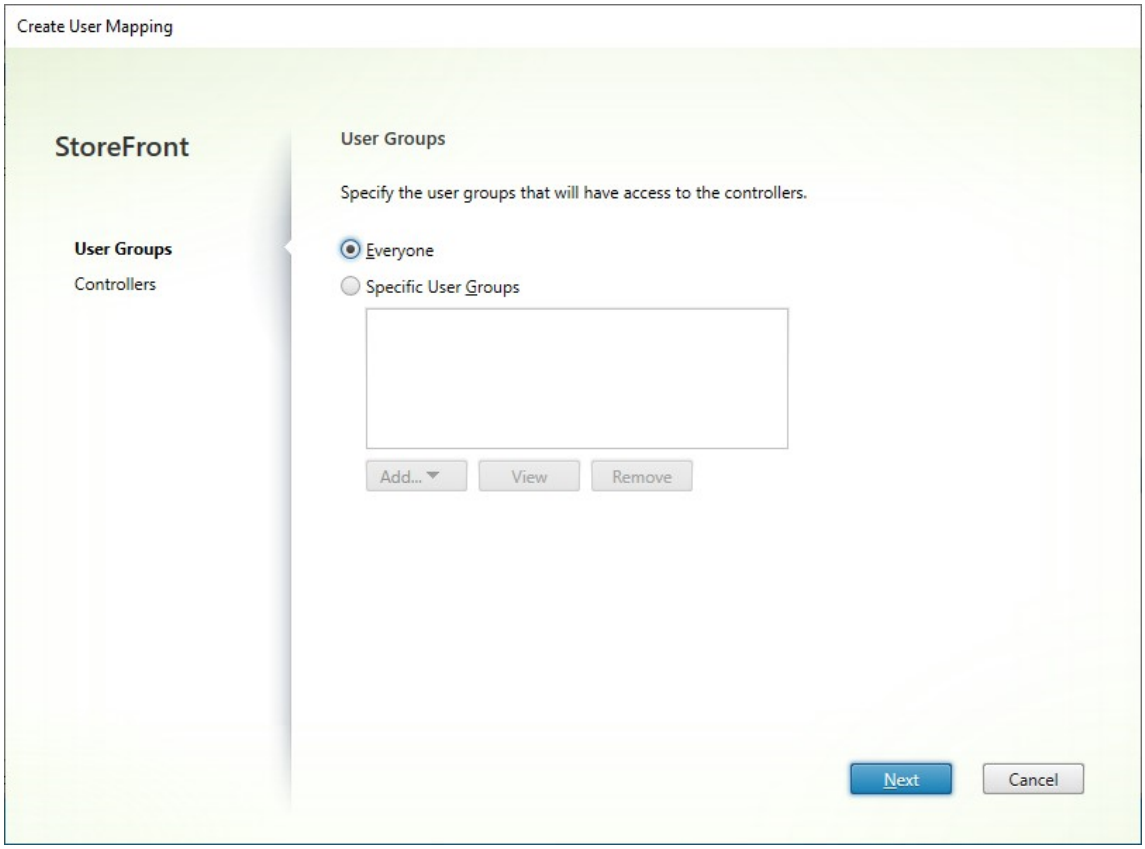
特定のユーザーグループに特定のリソースフィードを構成するには、次の手順を実行します:

1. ［**Delivery Controller** の管理］画面から、［ユーザー マッピングおよびマルチサイト集合体構成］の ［構成］をクリックします。このオプションは、2 つ以上のリソースフィードが構成されている場合にのみ使用できます。

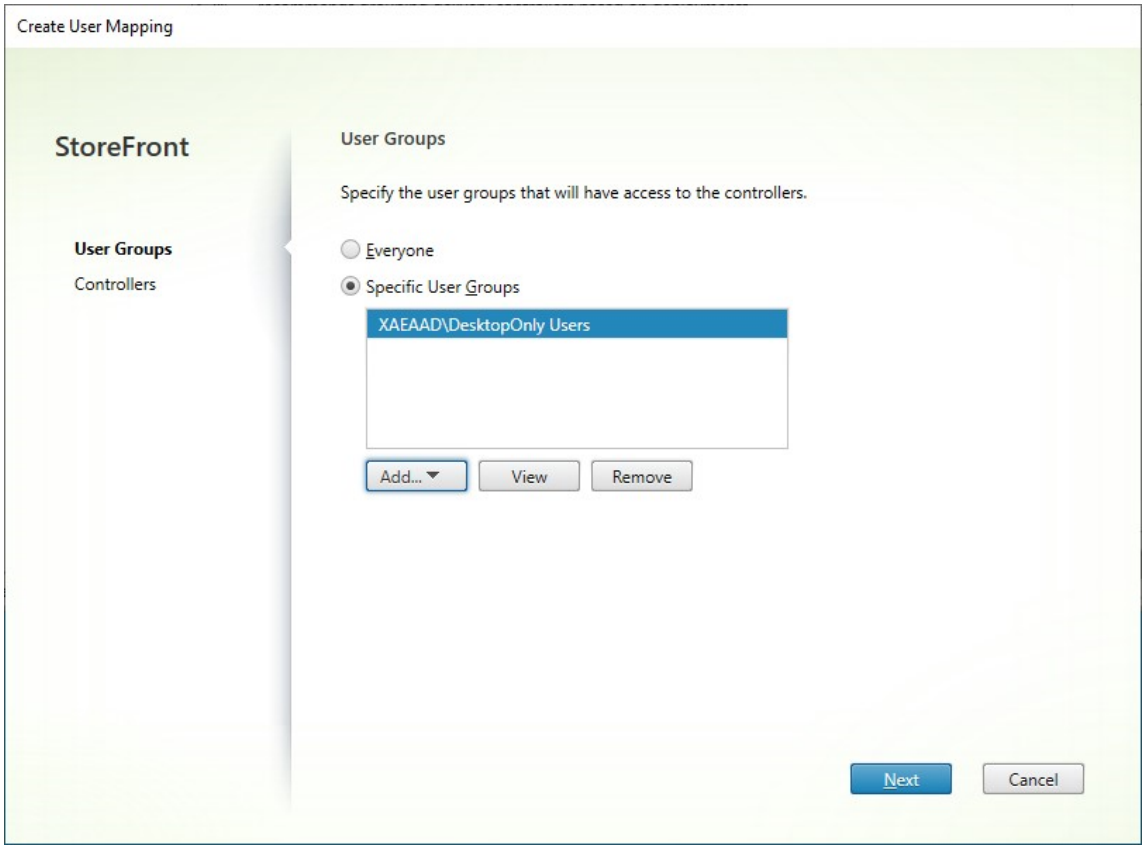
   これにより、［ユーザーマッピングおよびマルチサイト集合体の構成］画面が開きます。



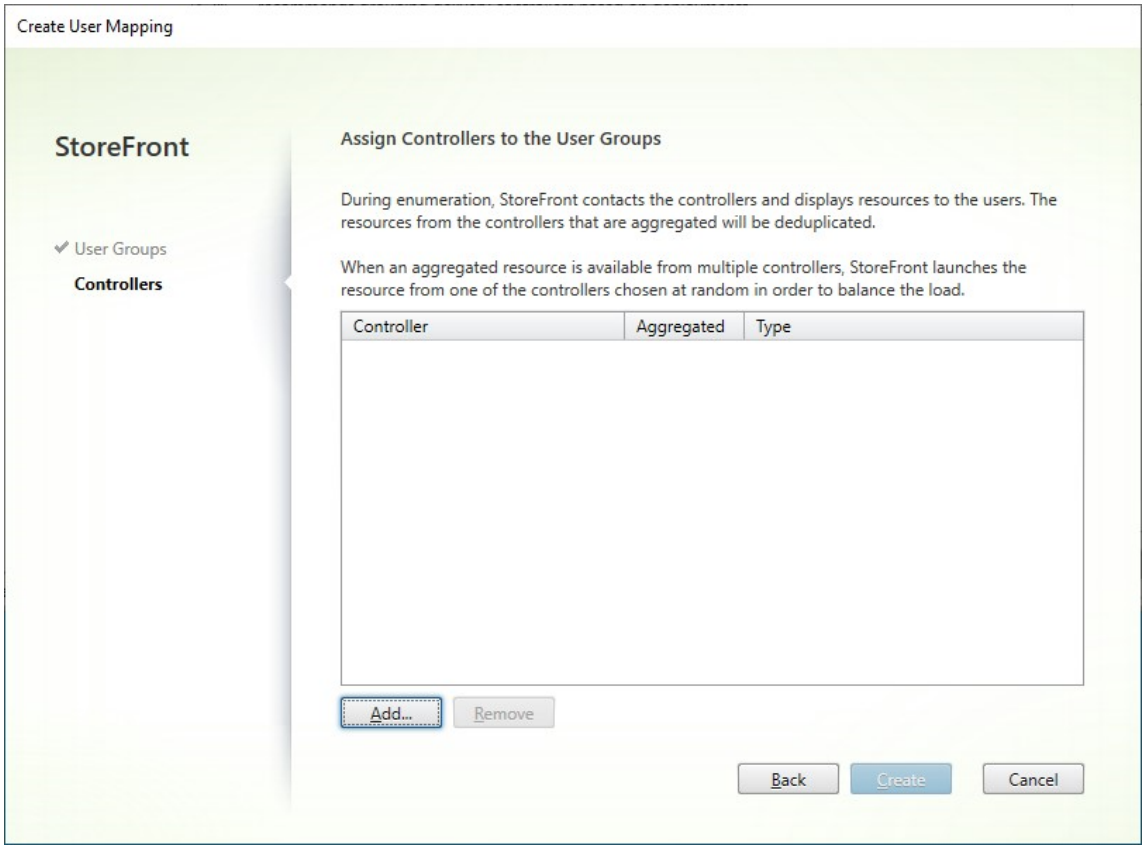
2. ［ユーザーをコントローラーにマップ］をクリックします。最初のマッピングを作成するための ［ユーザーマッピングの作成］画面が開きます。後でさらにマッピングを作成することができます。



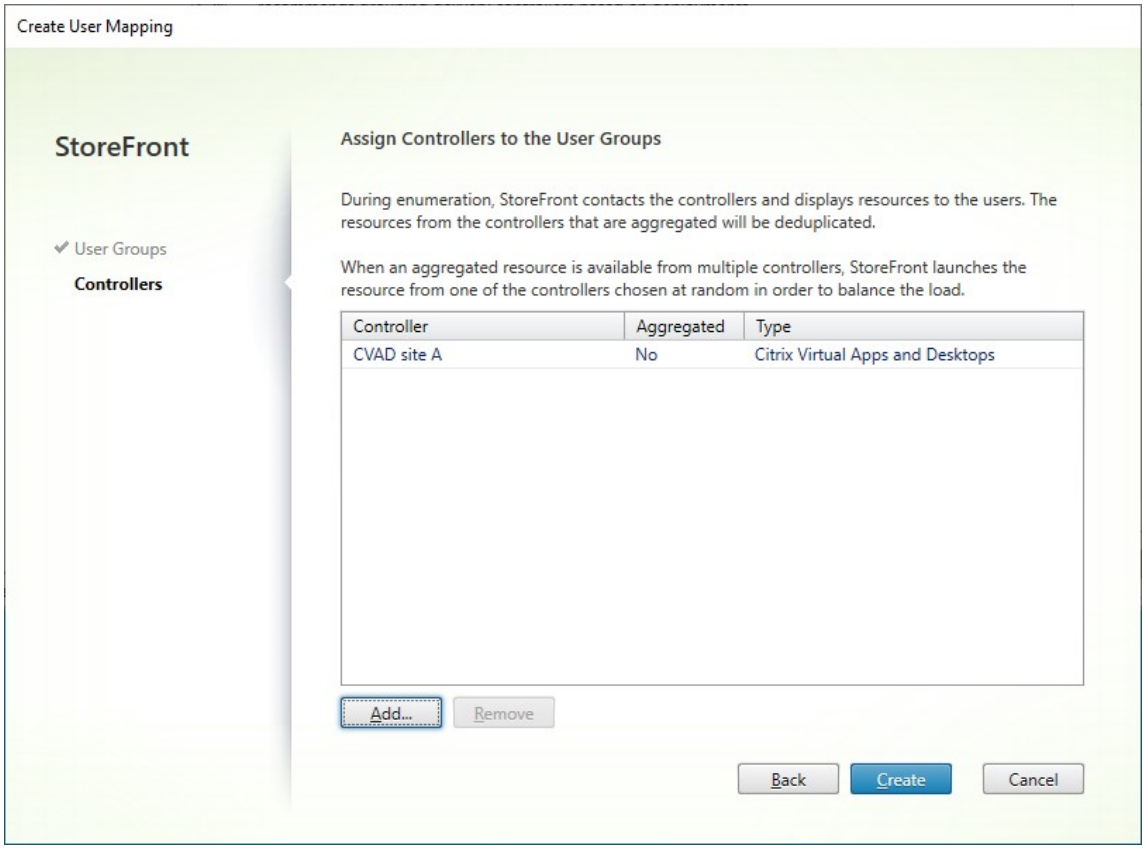
3. ［すべてのユーザー］を選択するか、［特定のユーザーグループ］を選択して 1 つ以上のグループを追加します。



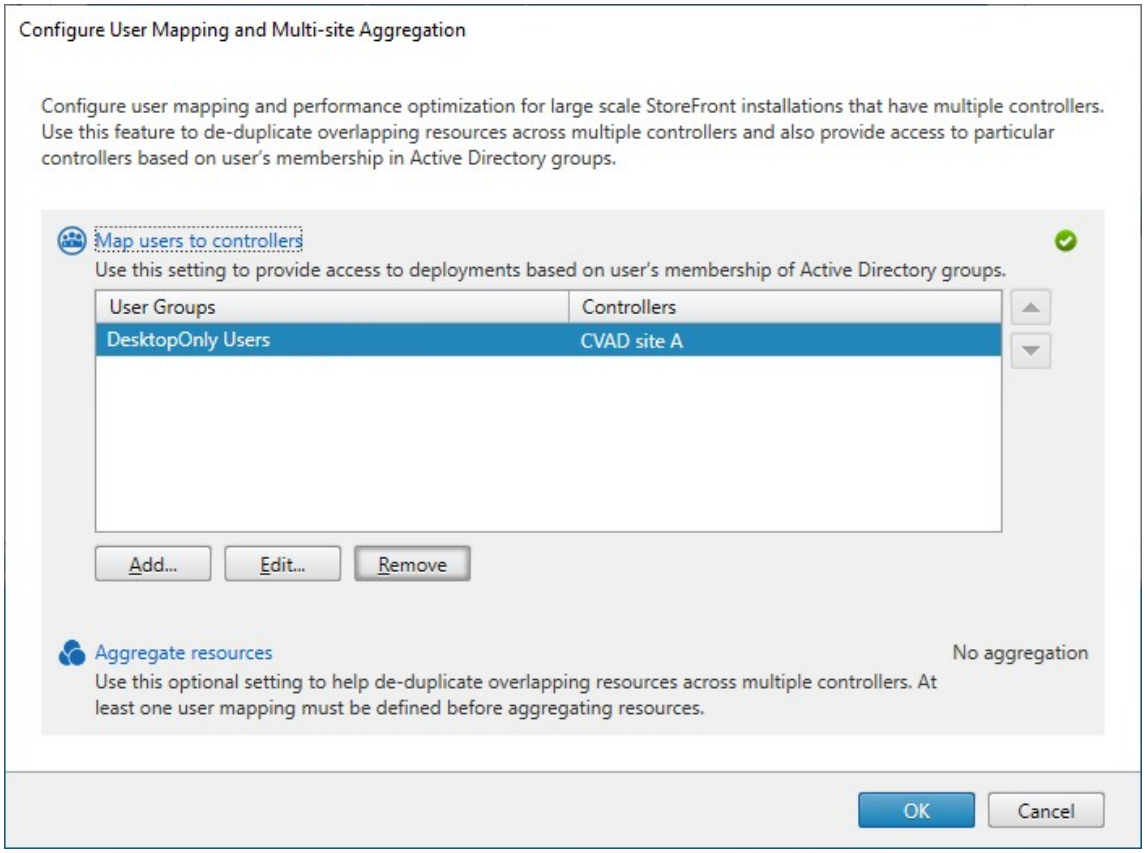
4. ［次へ］をクリックします。［コントローラー］タブが表示されます。



5. ［追加］をクリックして、1 つ以上のコントローラーを追加します。



6. [**Create**] をクリックします。



7. 必要に応じて、［追加…］をクリックしてさらにマッピングを作成します。

PowerShell SDK を使用してユーザーをリソースにマップする

PowerShell SDKを使用してユーザーをリソースにマップできます

1. リソースフィードごとに、EquivalentFarmset を作成します。すべてのリソースフィードはファームセットの一部である必要があります。そうでないと、どのユーザーもリソースフィードを利用できなくなります。次のパラメーターを使用してNew-STFEquivalentFarmsetを呼び出します：

   - `Name` - EquivalentFarmSet の一意の名前
   - `PrimaryFarms` - 非集約リソースフィード（ファーム）の名前。

2. 異なるリソースフィードのセットにアクセスする必要があるユーザーのセットごとに、それらのユーザーと各 EquivalentFarmSet の間のマッピングを作成します。UserFarmMapping を作成するには、次のパラメーターを指定してAdd-STFUserFarmMappingを呼び出します：

   - `StoreService` - UserFarmMapping を追加する Store サービス。
   - `Name` - マッピングの一意の名前。
   - `GroupMembers` - マッピングの一部であるユーザーグループの名前と SID を含むハッシュテーブル。名前は表示のみに使用されます。SID はグループを定義します。すべてのユーザーを追加するには、名前が`Everyone`、値が`Everyone`の単一のエントリをハッシュテーブルに作成します。

- `EquivalentFarmSet` - 前の手順で作成された EquivalentFarmSet。

すべてのリソースフィード（ファーム）が少なくとも 1 つの UserFarmMapping に含まれていることを確認する必要があります。そうしないと、ユーザーはそのリソースにアクセスできなくなります。

マルチサイト集計

StoreFront のデフォルトでは、ストアにデスクトップとアプリケーションを配信するすべての展開環境が列挙され、そのすべてのリソースが個別に扱われます。このため、複数の展開環境から同じリソースが同じ名前で配信されていても、リソースごとにアイコンが表示されます。ストアの高可用性やマルチサイト構成を有効にすると、同じデスクトップまたはアプリケーションを配信する Citrix Virtual Apps and Desktops の展開環境をグループ化して、それらのリソースを集約してユーザーに提供できます。グループ化された展開環境は同一である必要はありませんが、集約対象のリソースは、各サーバー上で名前とパスが同じである必要があります。

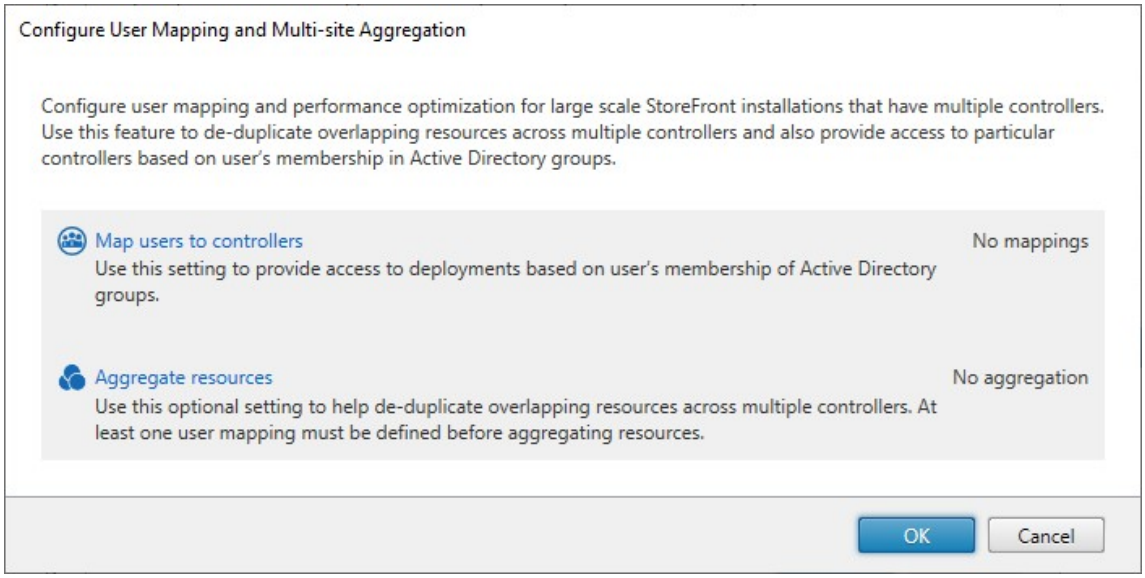
マルチサイト集計により、複数の Citrix Virtual Apps and Desktops の展開環境で配信されているデスクトップやアプリケーションがすべてストアで集約され、ユーザーには 1 つのアイコンだけが表示されます。ユーザーが集約リソースを起動すると、サーバーの可用性、そのユーザーがアクティブなセッションを確立済みかどうか、および管理者が指定した順番に基づいて、対象リソースから最適なインスタンスが選択されます。

StoreFront では、過負荷状態、または一時的に使用できない状態などで要求に応答できないサーバーが動的に監視されます。そのサーバーとの通信が再確立されるまで、別のサーバー上のリソースインスタンスがユーザーに提供されます。リソースの提供サーバーでサポートされている場合は、ユーザーが追加リソースを起動したときに、既存のユーザーセッションの再利用が試行されます。このため、ユーザーが選択した追加リソースが、そのユーザーの既存のセッションを実行している展開環境で提供されている場合、そのセッション内で追加リソースが起動します。これにより、各ユーザーのセッション数が最小限に抑えられるため、追加のデスクトップやアプリケーションの起動にかかる時間が短縮され、製品ライセンスをより効率的に使用できます。

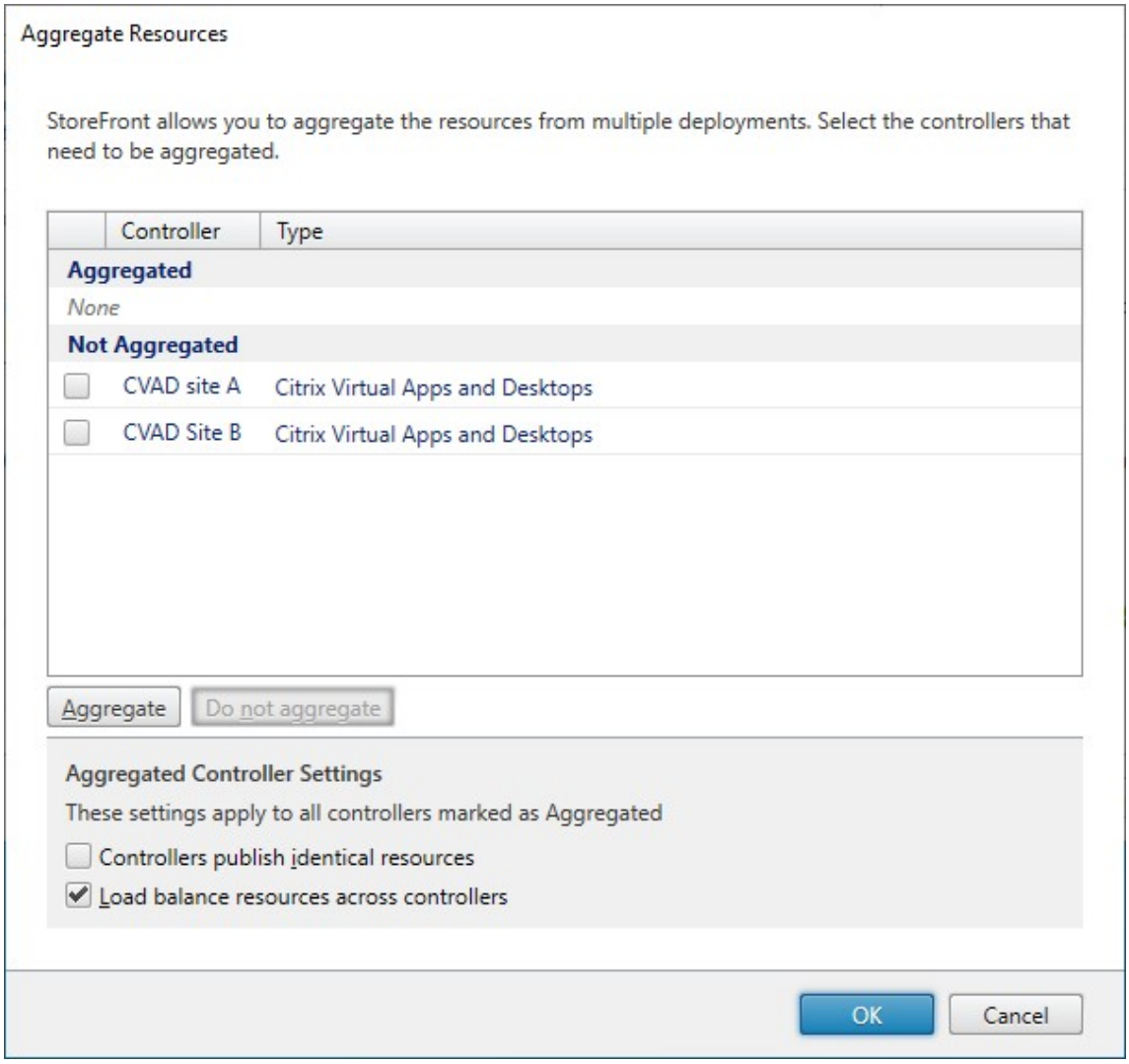
サーバーの可用性と既存のユーザーセッションを確認した後、StoreFront は指定された順番に基づいて、ユーザーが接続する展開環境を決定します。ユーザーが使用できる同等の展開環境が複数ある場合は、管理者の構成に基づいて、一覧の最初の展開環境または任意の展開環境が選択されます。一覧で最初に使用可能な展開環境が選択されるように構成すると、現在のユーザー数に対して使用中の展開環境の数を最小限に抑えることができます。一覧から展開環境がランダムに選択されるように構成すると、使用可能な展開環境間でユーザー接続を均一に分散させることができます。

Citrix Virtual Apps and Desktops で配信されるリソースでは、一覧での展開環境の順序を無視して、ユーザーが特定の展開環境のデスクトップやアプリケーションに接続されるように設定できます。これにより、特定のデスクトップやアプリケーションでは専用の展開環境に優先的にユーザーが接続されるようにして、ほかのリソースでは別の展開環境に接続されるように構成できます。このように構成するには、優先する展開環境のデスクトップやアプリケーションの説明に「`KEYWORDS:Primary`」という文字列を追加し、別の展開環境のリソースに「`KEYWORDS:Secondary`」という文字列を追加します。この場合、管理者が指定した展開環境の順序にかかわらず、ユーザーは優先される展開環境（プライマリ）に接続されます。優先される展開環境が使用できない場合、セカンダリリソースを提供する展開環境に接続されます。

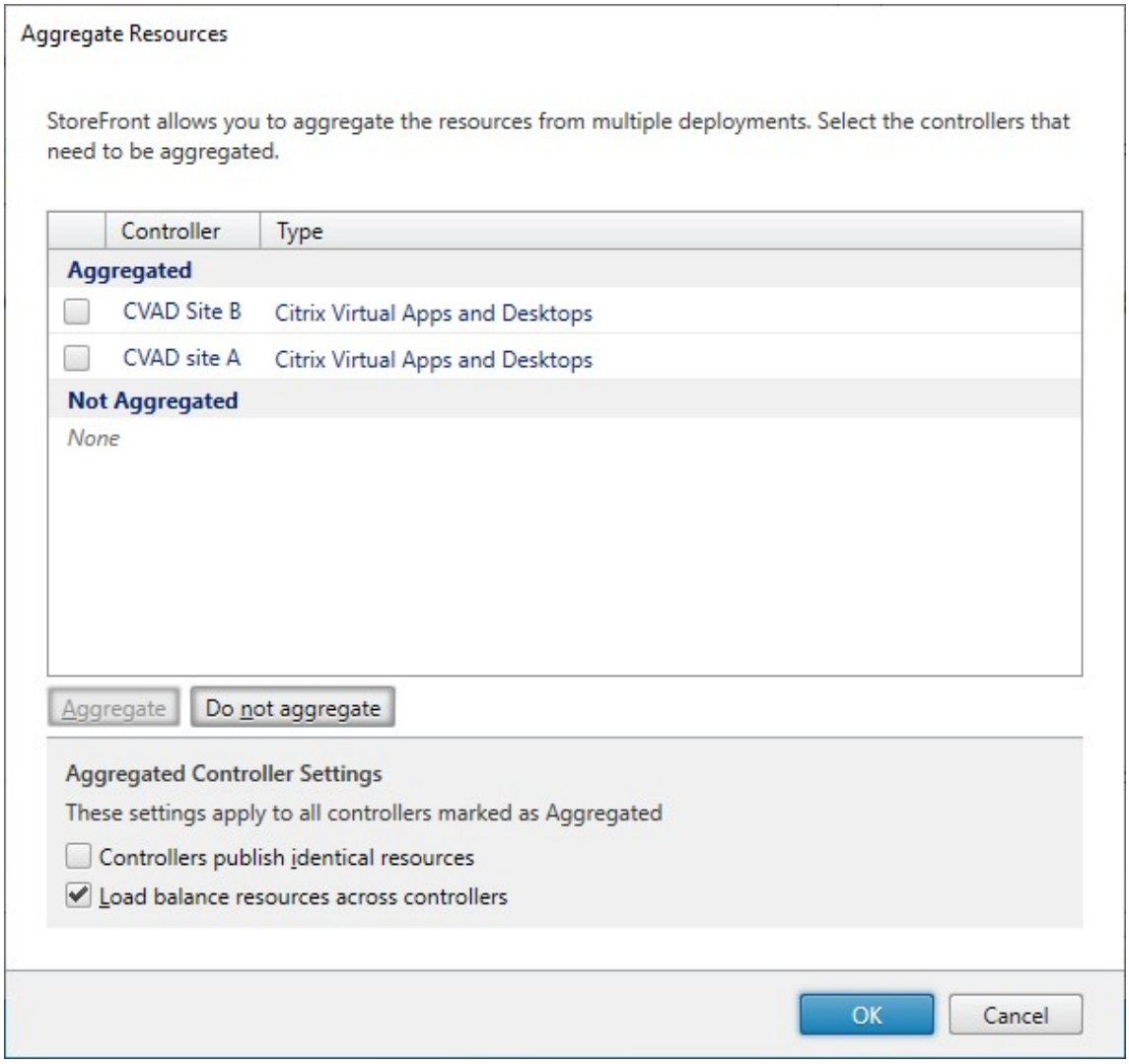
1. [**Delivery Controller** の管理] 画面で、[ユーザー マッピングおよびマルチサイト集合体構成] の [構成] をクリックします。このオプションは、2 つ以上のリソースフィードが構成されている場合にのみ使用できます。



2. [リソースを集約する] をクリックします。これによって、[リソースを集約する] 画面が表示されます。



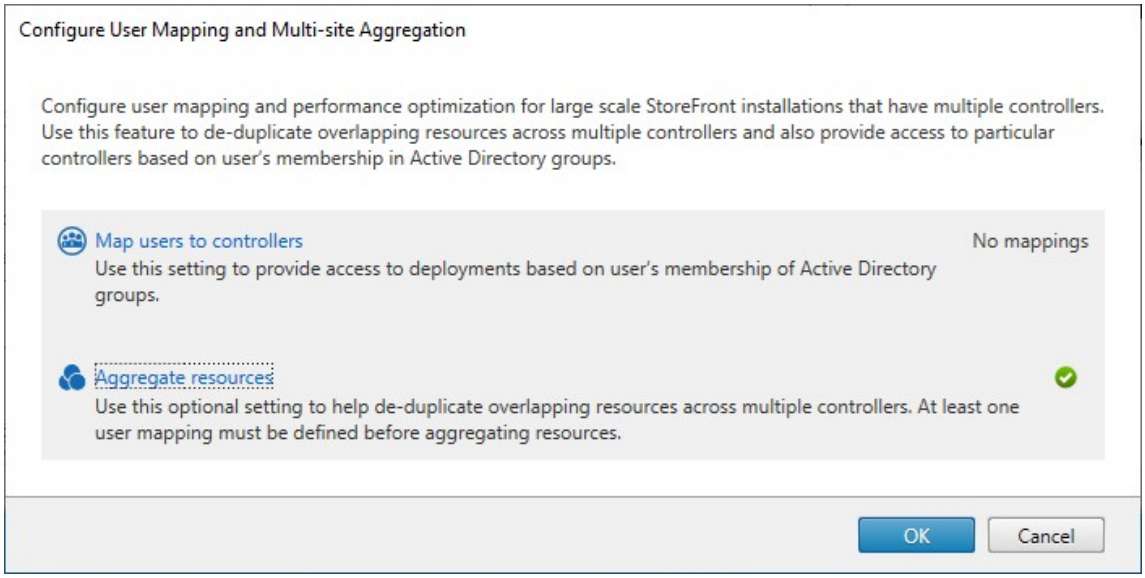
3. 同じリソースを持つリソースフィードを選択し、［集約］をクリックします。



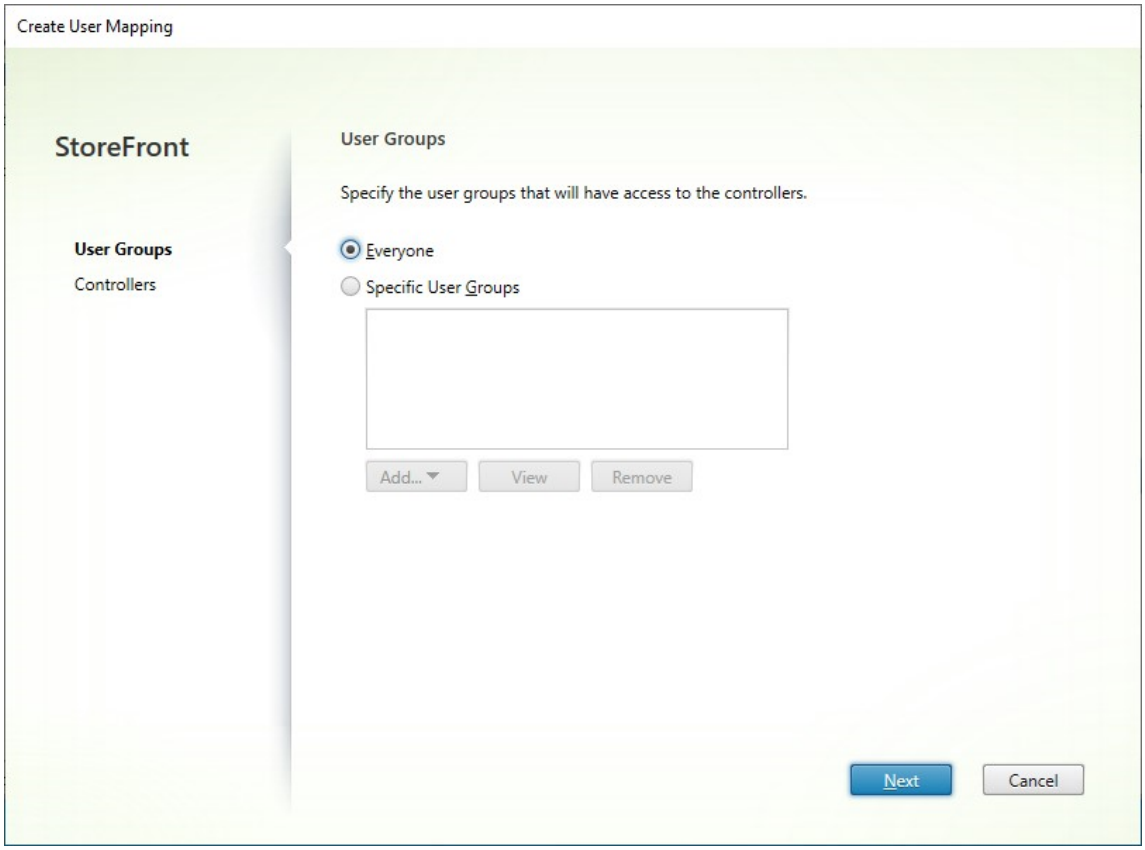
4. 必要に応じて ［集約済みコントローラーの設定］オプションを選択します:

   - コントローラーが同一のリソースを公開します - オンにすると、StoreFront により集約済みセットにあるいずれか 1 つのコントローラーのリソースのみが列挙されます。オフにすると、（利用できるリソースのユーザーのセット全体を集約するために）集約済みセットにあるすべてのコントローラーのリソースが StoreFront により列挙されます。このオプションをオンにするとリソース列挙時のパフォーマンスが向上します。ただし、リソースの一覧が集約済みのすべてのフィードで同一であることが確実でない限り、お勧めしません。
   - 複数のコントローラーでリソースを負荷分散します - オンにすると、利用可能なコントローラーに起動が均一に分散されます。オフにすると、起動はユーザーマッピングダイアログ画面で指定された最初のコントローラーに割り当てられ、その起動が失敗した場合は以降のコントローラーにフェールオーバーします。

5. ［**OK**］をクリックして、［ユーザー マッピングおよびマルチサイト集合体の構成］画面に戻ります。［リソースを集約する］にチェックマークが付きました。

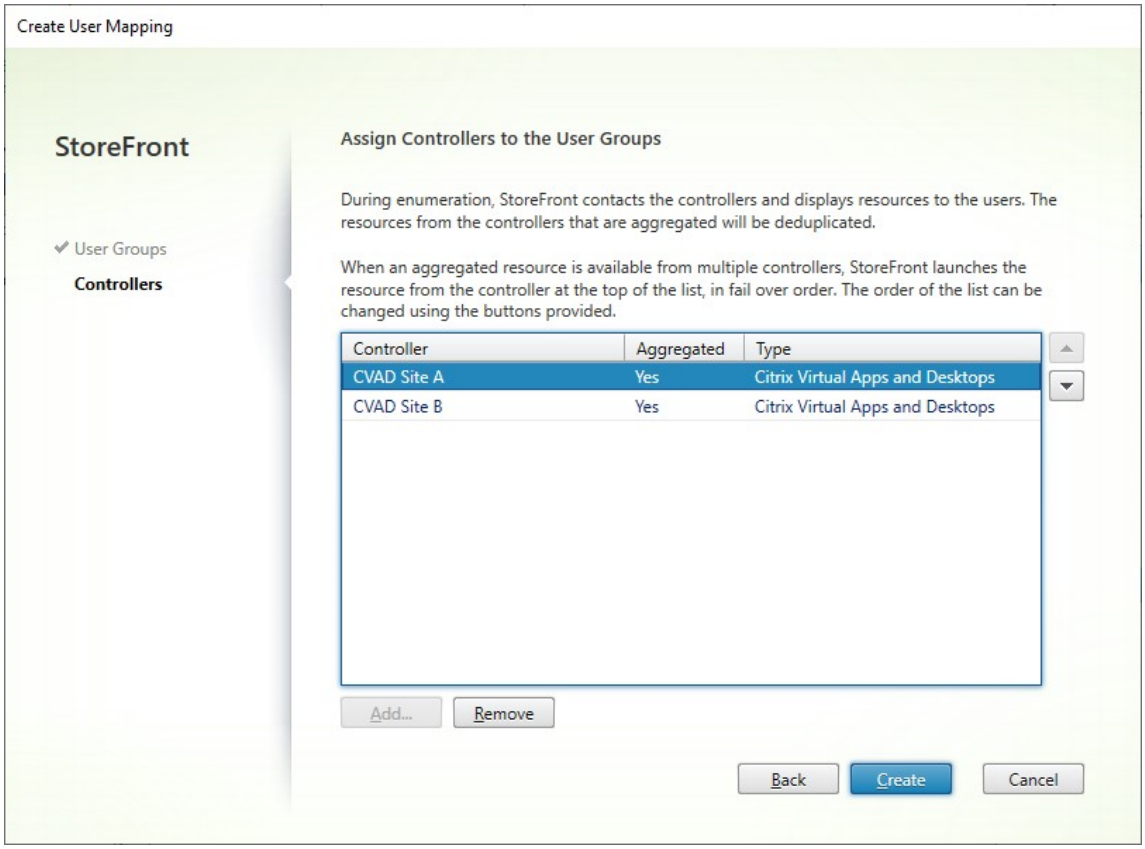


6. リソースが集約されると、デフォルトではリソースにアクセスできるユーザーがいないため、ユーザーマッピングを追加する必要があります。［ユーザーをコントローラーにマップ］をクリックします。［ユーザーマッピングの作成］画面が開きます。

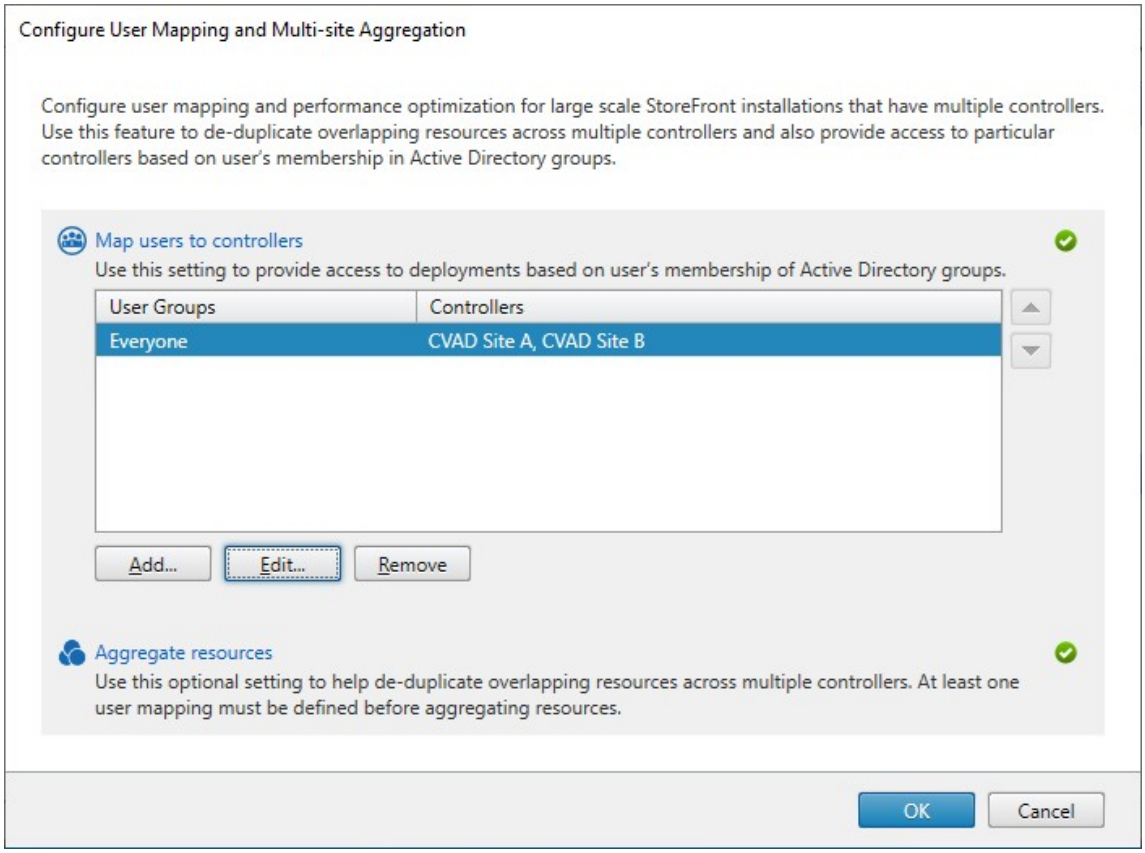


7. ［すべてのユーザー］を選択するか、［特定のユーザーグループ］を選択して 1 つ以上のグループを追加します。たとえば、特定の場所にいるユーザーを表すグループを選択したい場合があります。

8. 集約済みのリソースフィードを追加します。集約済みのリソースフィードをすべて追加する必要があります。含まれていないフィードは、［集約なし］になります。集約されていないリソースを含めることもできます。
9. ［複数のコントローラーでリソースを負荷分散します］にチェックを入れなかった場合は、StoreFront がリソースを優先して起動する順序を選択できます。



10. ［作成］を押して、［ユーザーマッピングおよびマルチサイト集合体の構成］に戻ります。



11. 必要に応じてさらにマッピングを追加します。すべてのリソースフィードがユーザーグループにマッピングされていることを確認してください。マッピングされていない場合、それらのリソースはどのユーザーも使用できなくなります。
12. [**OK**] をクリックします。

PowerShell SDK を使用した高度な構成

StoreFront 管理コンソールで、多くの一般的なマルチサイトおよび高可用性操作を構成できます。PowerShell SDKを使用して StoreFront を構成することもできます。これにより、次の追加機能が提供されます:

- 集約対象として複数の展開環境グループを指定する機能。
  - 管理コンソールでは展開環境を単一のグループにまとめることしかできませんが、大部分の場合はこれで十分です。
  - 参加していないリソースセットを持つ複数の展開環境があるストアでは、複数グループによりパフォーマンスが向上する場合があります。
- 集約済み展開環境に対して複雑な優先順位を指定する機能。管理コンソールでは、集約済みの展開環境を負荷分散したり、単一のフェールオーバーリストとして使用したりできます。PowerShell を使用すると、負荷分散されたフィードの複数のグループを作成し、異なるグループ間でフェールオーバーできます。

> 警告:
>
> PowerShell を使用して詳細なマルチサイトオプションを構成した後は、管理コンソールを使用してオプションを変更することはできません。

1. どのアグリゲーショングループを使用するかを決定します。アグリゲーショングループ内では、表示名が同じアプリケーションは 1 つのアイコンに集約されます。各アグリゲーショングループには名前が必要です。管理コンソールでは、作成できるアグリゲーショングループは 1 つだけです。PowerShell を使用して複数のアグリゲーショングループを定義できます。

2. アグリゲーショングループごとに、集約するリソースフィード（SDK ではファームと呼ばれます）を一覧表示する 1 つ以上の EquivalentFarmset を作成します。アグリゲーショングループ内の異なるリソースフィードが異なるユーザーに割り当てられる場合は、同じ`AggregationGroupName`を共有するユーザーのセットごとに個別の EquivalentFarmSet を作成する必要があります。EquivalentFarmSet を作成するには、次のパラメーターを指定して`New-STFEquivalentFarmset`を呼び出します:

   - `Name` - EquivalentFarmset の一意の名前。
   - `AggregationGroupName` - ファームセットが属しているアグリゲーショングループの名前。
   - `LoadBalanceMode` - `LoadBalanced`または`Failover`のいずれか。
   - `PrimaryFarms` - 集約したいファーム。`LoadBalanceMode`が`Failover`の場合は、ファームが必要な順序で表示されていることを確認してください。アグリゲーショングループに複数の EquivalentFarmSet がある場合、リソースの起動にどのリソースフィードを使用するかを評価するときに、この順序が UserFarmMapping で定義された IndexNumber と結合されます。
   - `BackupFarms` - プライマリファームが利用できない場合に使用するファームの一覧。この機能は廃止されました。代わりに、より大きい IndexNumber を持つ追加の EquivalentFarmSet を追加します。

3. アグリゲーショングループの一部ではないリソースフィードごとに、`AggregationGroupName`を指定せずに EquivalentFarmset を作成します。すべてのリソースフィードはファームセットの一部である必要があります。次のパラメーターを使用して`New-STFEquivalentFarmset`を呼び出します:

   - `Name` - EquivalentFarmSet の一意の名前
   - `PrimaryFarms` - 非集約ファームの名前。

4. 異なるリソースフィードのセットにアクセスする必要があるユーザーのセットごとに、それらのユーザーと各 EquivalentFarmSet の間のマッピングを作成します。UserFarmMapping を作成するには、次のパラメーターを指定して`Add-STFUserFarmMapping`を呼び出します:

   - `StoreService` - UserFarmMapping を追加する Store サービス。
   - `Name` - マッピングの一意の名前。
   - `GroupMembers` - マッピングの一部であるユーザーグループの名前と SID を含むハッシュテーブル。名前は表示のみに使用されます。SID はグループを定義します。すべてのユーザーを追加するには、名前が`Everyone`、値が`Everyone`の単一のエントリをハッシュテーブルに作成します。
   - `EquivalentFarmSet` - 前の手順で作成された EquivalentFarmSet。

- `IndexNumber` - リソースフィードが評価される順序を設定します。これにより、リソースの起動にどのリソースフィードを使用するかの優先順位が設定されます。

すべてのリソースフィード（ファーム）が少なくとも 1 つの UserFarmMapping に含まれていることを確認する必要があります。そうしないと、ユーザーはそのリソースにアクセスできなくなります。

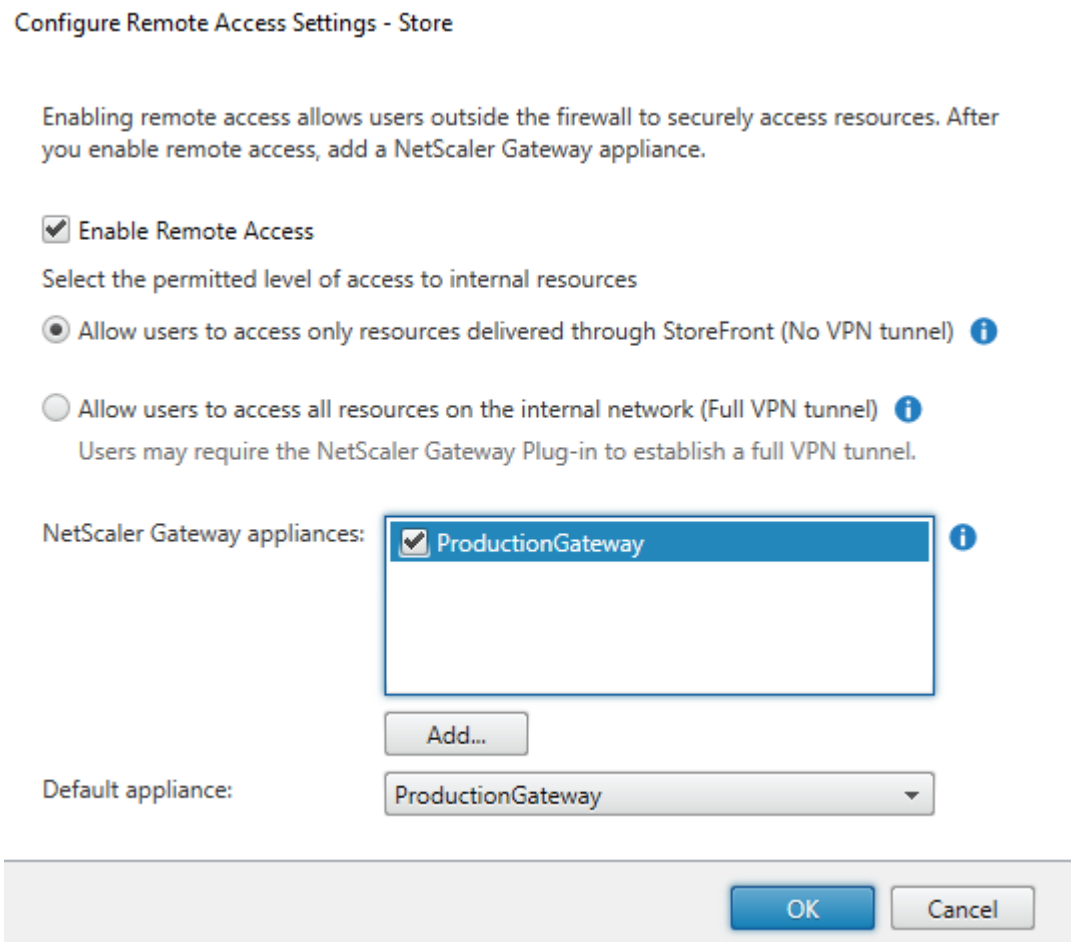
Citrix Gateway を介したストアへのリモートアクセスの管理

June 6, 2024

公共のネットワークから接続するユーザーに対して Citrix Gateway を介したストアへのアクセスを構成するには、［リモートアクセス設定］タスクを使用します。認証不要なストアでは、Citrix Gateway を介したリモートアクセスは許可されません。

> 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. Citrix StoreFront 管理コンソールの右ペインで［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインで ［リモートアクセス設定の構成］をクリックします。



2. [リモートアクセス設定の構成] ダイアログボックスでは、公共のネットワーク上のユーザーに Citrix Gateway を介したアクセスを提供するかどうか、およびその方法を指定します。

   - 公共のネットワーク上でユーザーがストアを使用できないようにするには、[リモートアクセスの有効化] チェックボックスをオフにします。これにより、内部ネットワークのローカルユーザーのみがストアにアクセスできるようになります。
   - リモートアクセスを有効化するには、[リモートアクセスの有効化] をオンにします。
     - Citrix Gateway 経由でアクセスするユーザーにストアのリソースのみを提供するには、[**VPN** トンネルなし] を選択します。ユーザーは ICAProxy またはクライアントレス VPN（cVPN）を使用して Citrix Gateway にログオンするため、Citrix Gateway Plug-in を使用して完全 VPN を確立する必要はありません。
     - Secure Sockets Layer（SSL）仮想プライベートネットワーク（VPN）トンネルを介して内部ネットワーク上のストアおよびそのほかのリソースへのアクセスを提供するには、[完全 **VPN** トンネル] を選択します。この場合、ユーザーは VPN トンネルを確立するために Citrix Gateway Plug-in を使用する必要があります。

   ストアへのリモートアクセスを有効にすると、認証方法として [**Citrix Gateway** からのパススルー] が自動的に有効になります。ユーザーは Citrix Gateway にログオンするときに認証されるため、スト

アにアクセスするときは自動的にログオンできます。

3. リモートアクセスを有効にした場合は、ユーザーがストアにアクセスするときに使用する展開環境を［**Citrix Gateway** アプライアンス］一覧から選択します。この一覧には、このストアやほかのストアの作成時に追加したゲートウェイ環境が表示されます。一覧にゲートウェイ環境を追加する場合は、［追加］をクリックし、「Citrix Gateway の構成」の手順に従います。
4. 一覧で複数のエントリを選択して複数のアプライアンスを介したアクセスを有効にする場合は、Citrix Workspace アプリからストアへのアクセスに使用される ［デフォルトアプライアンス］を指定します。
5. ［**OK**］をクリックして構成を保存し、［リモートアクセスの構成］ダイアログボックスを閉じます。

Citrix Workspace アプリは、ユーザーがローカルネットワークと公共のネットワークのどちらに接続しているのかをビーコンポイントを使用して識別し、適切なアクセス方法を選択します。ビーコンポイントの変更について詳しくは、「ビーコンポイントの構成」を参照してください。

デフォルトでは、StoreFront はユーザーがストアへの接続で経由している Gateway を使用してリソースを起動します。StoreFront がリソースを起動するために代替 Gateway を使用するか Gateway を使用しないように構成する場合は、「最適な HDX ルーティング」を参照してください。

証明書失効一覧（**CRL**）のチェック

June 6, 2024

はじめに

StoreFront で、CVAD Delivery Controller が使用する TLS 証明書の状態を公開された証明書失効一覧（CRL）を使用して確認するよう構成できます。次の場合、証明書へのアクセスの取り消しが必要なことがあります:

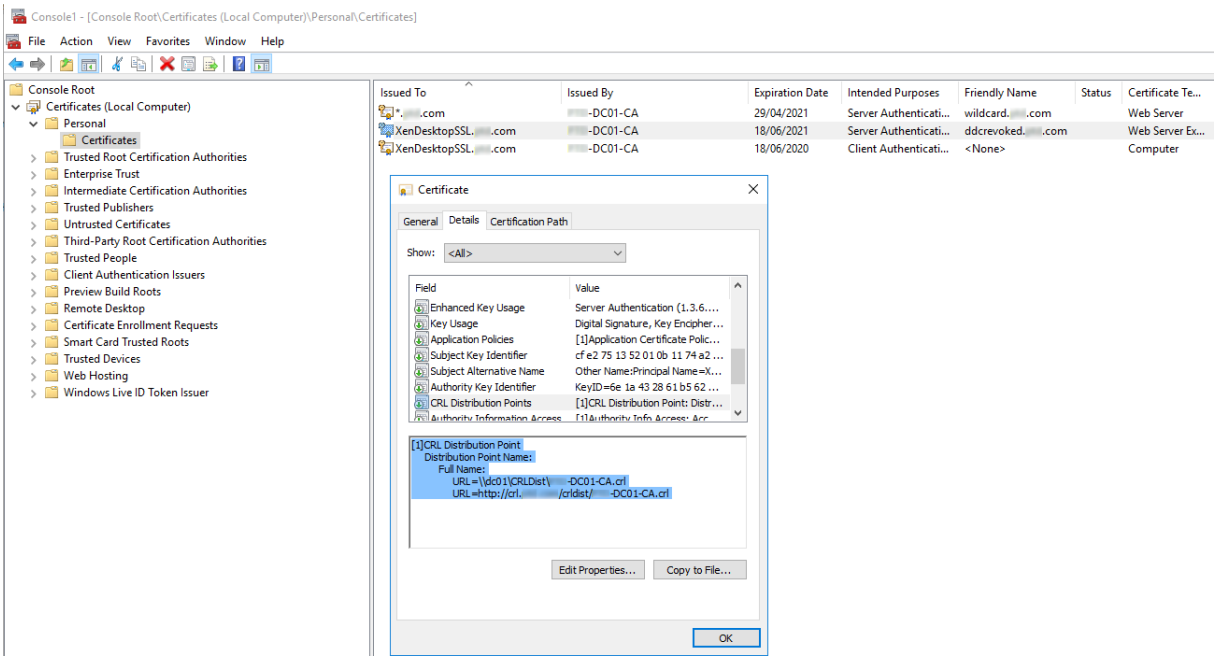
- 秘密キーが侵害された可能性がある
- CA が侵害された
- 所属が変更された
- 証明書が置き換えられた

> 注:
>
> このトピックは、StoreFront と Citrix Virtual Apps and Desktops Delivery Controller との間で HTTPS 接続が使用された場合のみ該当します。Delivery Controller への HTTP 接続に証明書は必要ありません。そのため、ここで説明されるストアの-CertRevocationPolicy 設定が影響することはありません。
>
> StoreFront は、CRL 配布ポイント
> （CDP）の拡張機能およびローカルにインストールされた証明書失効一覧

> （CRL）を使用した証明書失効チェックをサポートします。StoreFront は完全な CRL のみをサポートしています。デルタ CLR はサポートされていません。

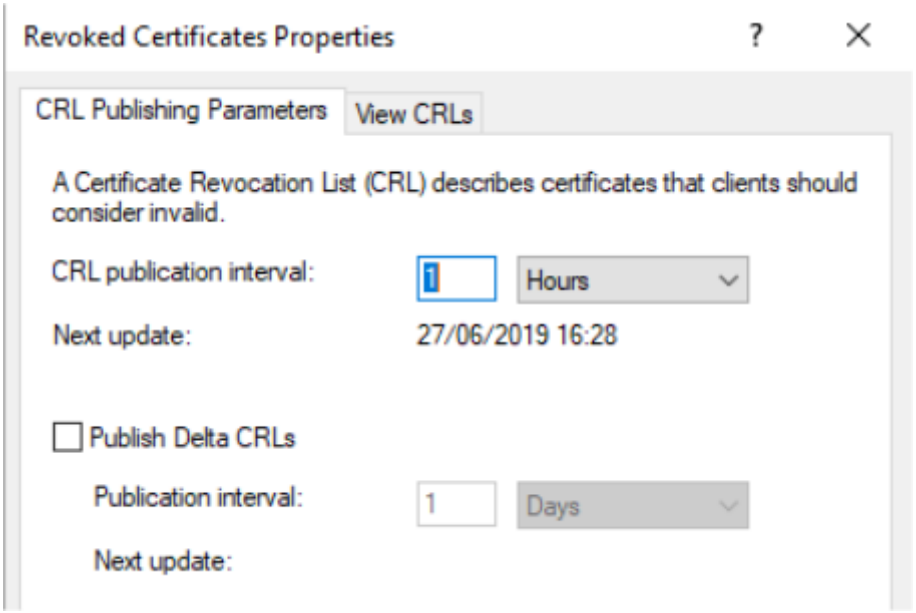
CRL 配布ポイント（**CDP**）拡張機能

Citrix Virtual Apps and Desktops Delivery Controller が使用している証明書が失効し、公開された CRL にシリアル番号が表示されている場合、StoreFront はこの Delivery Controller のリソースを列挙しません。StoreFront が失効した証明書を検出するには、CDP 証明書拡張機能で定義されているいずれかの URL を使用して、公開された CRL にアクセスする必要があります。



CRL の公開間隔

StoreFront がいち早く Delivery Controller 上の失効した証明書を検出できるようにするには、CA での CRL の公開期間を短縮する必要があります。CLR 配布ポイント拡張機能のプロパティを編集して、使用中の公開キー基盤により短い CRL 公開期間値を設定します。



クライアントの **CRL** キャッシュ

Windows 公開キー基盤のクライアントは、CRL をローカルにキャッシュします。最新の CRL は、ローカルにキャッシュされた CRL の有効期限が切れるまでダウンロードされません。

証明書失効リスト（**CRL**）への **StoreFront** のアクセス

証明書失効チェックのためには、StoreFront が CRL にアクセスできる必要があります。StoreFront が CRL を公開する Web サーバーや証明機関（CA）と通信する方法や、CRL の更新を受信する方法について慎重に確認してください。

Delivery Controller 上の内部エンタープライズ **CA** およびプライベート証明書　プライベート CA および証明書を使用する場合、StoreFront に必要なのは正しく構成されたエンタープライズ CA と、組織内の内部ネットワークからアクセスできる公開された CRL です。エンタープライズ CA が CDP 拡張機能を公開するように構成する情報については、Microsoft ドキュメントを参照してください。CA が
CDP 拡張機能を含むように構成される前に Delivery Controller 上に存在していた証明書は、再発行が必要な場合があります。

StoreFront サーバーおよび Citrix Virtual Apps and Desktops サーバーは通常、インターネット接続のない隔離されたプライベートネットワーク上に存在します。この場合、プライベート CA を使用する必要があります。

Delivery Controller 上の外部パブリック **CA** およびパブリック証明書　StoreFront サーバーおよび Citrix Virtual Apps and Desktops Delivery Controller は、パブリック CA によって発行された証明書を使用できます。StoreFront は、CDP 拡張機能で参照された URL を使用して、インターネット経由でパブリック CA の Web サーバ

ーと通信できる必要があります。パブリック証明書が失効した後、StoreFront が CDP URL を使用して CRL のコピーをダウンロードできない場合、StoreFront は CRL チェックを実行できなくなります。

証明書失効ポリシーの設定

Citrix StoreFront の PowerShell コマンドレット **Get-STFStoreFarmConfiguration** および **Set-STFStoreFarmConfiguration** を使用して、ストアの証明書失効ポリシーを設定します。**Get-Help Set-STFStoreFarmConfiguration -detailed** を実行すると、PowerShell のヘルプとオプション-CertRevocationPolicy の例を表示します。これらの StoreFront PowerShell コマンドレットについて詳しくは、Citrix StoreFront SDK PowerShell Modulesを参照してください。

-CertRevocationPolicy オプションは、以下の値に設定できます:

設定	説明
NoCheck	StoreFront は、Delivery Controller 上の証明書の失効状態をチェックしません。StoreFront は、失効した証明書を使用する Delivery Controller からのリソースを列挙し続けます。これがデフォルトの設定です。
MustCheck	これは最も安全なオプションです。StoreFront は、Delivery Controller 上の証明書の CDP 拡張機能で参照されている URL にアクセスして、CRL の取得を試みます。CRL が利用できない場合、または Delivery Controller で使用されている証明書が失効している場合、StoreFront は Delivery Controller からの列挙に失敗します。URL は、証明書がプライベートの場合は内部 Web サーバーを指し、証明書がパブリック CA によって発行された場合はパブリックインターネット Web サーバーを指します。
FullCheck	StoreFront は、Delivery Controller 証明書の CDP 拡張機能で公開されている URL への接続を試みます。StoreFront がこれらの URL から CRL のコピーの取得に失敗した場合でも、Delivery Controller からのリソースの列挙を許可します。StoreFront が CRL を正常に取得しても、Delivery Controller の証明書が失効している場合、StoreFront はリソースを列挙しません。URL は、証明書がプライベートの場合は内部 Web サーバーを指し、証明書がパブリック CA によって発行された場合はパブリックインターネット Web サーバーを指します。

設定	説明
NoNetworkAccess	StoreFront サーバー上の Citrix Delivery Server 証明書ストアにローカルにインポートされた CRL のみがチェックされます。StoreFront は、CDP 拡張機能で指定された URL への接続を試みません。StoreFront が CRL のローカルコピーの取得に失敗した場合でも、Delivery Controller からのリソースの列挙を許可します。StoreFront が Citrix Delivery Server 証明書ストアから CRL のローカルコピーを正常に取得しても、Delivery Controller の証明書が失効している場合、StoreFront はリソースを列挙しません。

ストアで証明書失効チェックを構成する

ストアの証明書失効ポリシーを設定するには、［管理者として実行］で PowerShell ISE を開いて、次の PowerShell コマンドレットを実行します。複数のストアがある場合、この手順をすべてのストアで繰り返します。-CertRevocationPolicy は、$StoreVirtualPath で指定されたストアに構成されたすべての Delivery Controller に影響を与えるストアレベルの設定です。

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
$StoreVirtualPath
Set-STFStoreFarmConfiguration -StoreService $StoreObject -
    CertRevocationPolicy "MustCheck"
<!--NeedCopy-->
```

設定が正しく適用されたことを確認する、または現在の -CertRevocationPolicy 構成を表示するには、次を実行します:

```
(Get-STFStoreFarmConfiguration -StoreService $StoreObject).
    CertRevocationPolicy
<!--NeedCopy-->
```

StoreFront サーバーでローカルにインポートされた CRL を使用する

ローカルにインポートされた CRL の使用はサポートされていますが、Citrix では推奨されていません。
以下はその理由です:

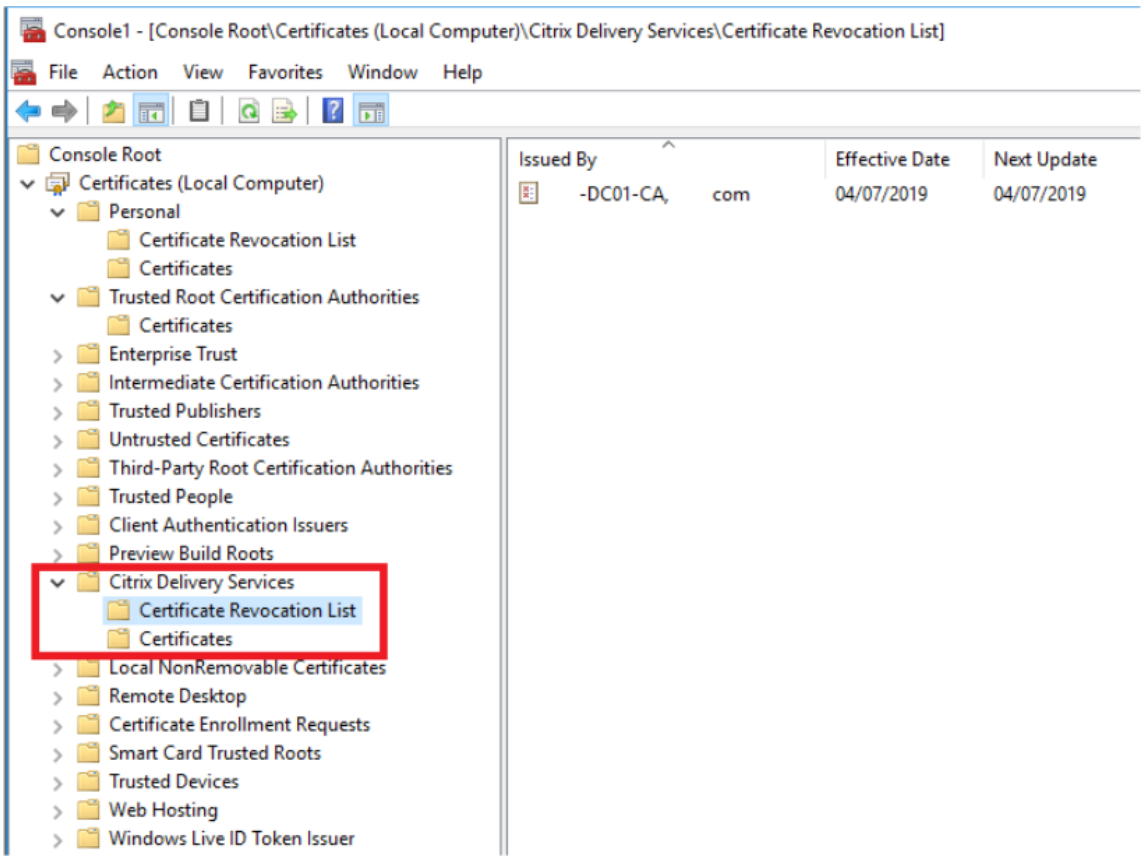
- 大規模な環境では複数の StoreFront サーバーグループが関係する可能性があるため、管理や更新が困難になります。

- 証明書が失効するたびにすべての StoreFront サーバーの CRL を手動で更新すると、Active Directory ドメイン全体で CDP 拡張機能および公開された CRL を使用する場合に比べて、大幅に効率が低下します。

-CertRevocationPolicy が「NoNetworkAccess」に設定されている場合、ローカルでインストールされているまたは更新された CRL を使用して、CRL をすべての StoreFront サーバーに効率的に配布できます。

ローカルにインポートされた **CLR** を使用するには

1. CRL を StoreFront サーバーのデスクトップにコピーします。StoreFront サーバーがサーバーグループの一部である場合は、グループ内のすべての StoreFront サーバーにコピーします。
2. MMC スナップインを開いて ［ファイル］**>**［スナップインの追加と削除］**>**［証明書］**>**［コンピューターアカウント］**>**［**Citrix Delivery Services** の証明書ストア］を選択します。
3. 右クリックして ［すべてのタスク］**>**［インポート］を選択し、.CRL ファイルを参照して［すべてのファイル］**>**［開く］**>**［証明書をすべて次のストアに配置する］**>**［**Citrix Delivery Services**］を選択します。



PowerShell またはコマンドラインで **CRL** を **Citrix Delivery Service** 証明書ストアに追加するには

1. StoreFront にログインし、
   .CRL ファイルを現在のユーザーのデスクトップにコピーします。

2. PowerShell ISE を開き、［管理者として実行］を選択します。
3. 以下を実行します:

```
certutil -addstore "Citrix Delivery Services" "$env:UserProfile\
    Desktop\Example-DC01-CA.crl"
```

正常に実行されると、次の値が返されます:

```
Citrix Delivery Services
CRL "CN=Example-DC01-CA, DC=example, DC=com" added to store.
CertUtil: -addstore command completed successfully.
```

このコマンドは、スクリプト経由で自動的に環境のすべての StoreFront
サーバーに CRL を配布する場合に使用できます。

Delivery Controller を使用した **XML** 認証

StoreFront を構成して、ユーザー認証を Citrix Virtual Apps and Desktops Delivery Controller に委任できます。Delivery Controller の証明書が失効した場合、ユーザーは StoreFront にサインインできなくなります。認証を担当する Citrix Virtual Apps and Desktops Delivery Controller 上の証明書が失効している場合、Active Directory ユーザーを StoreFront にサインインできなくする必要があるため、これは望ましい動作です。

ユーザー認証を **Delivery Controller** に委任するには

1. 前のセクション「ストアで証明書失効チェックを構成する」で説明したように、ストアで証明書の失効を構成します。
2. 「XML サービスベースの認証」の手順に従って、Delivery Controller で HTTPS の使用を構成します。

XML 認証サービスで証明書失効チェックを構成する

以下の手順は、展開で XML 認証を使用している場合にのみ必要です。

> 注:
>
> StoreFront では、ストアを認証サービスにマッピングするために 2 つの方法を利用できます。推奨される方法は、ストアと認証サービスの 1 対 1 のマッピングです。この場合、すべてのストアと関連する認証サービスに対して、このセクションの手順を実行する必要があります。
>
> ストアと認証サービスの両方で、証明書失効モードが同じ値に設定されていることを確認してください。また、すべてのストアが同一の認証構成を使用している場合、複数のストアが単一の認証サービスを共有するように構成できます。

認証サービスの PowerShell コマンドレットには **Set-STFStoreFarmConfiguration** に相当する値がないため、PowerShell の使用方法は多少異なります。前のセクションで説明したものと同じ証明書失効ポリシーの設定を使用します。

1. PowerShell ISE を開き、［管理者として実行］を選択します。

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$AuthVirtualPath = "/Citrix/StoreAuth"
<!--NeedCopy-->
```

2. XML 認証で使用されるストアサービス、認証サービス、Delivery Controller を選択します。Delivery Controller が既にストアで構成されていることを確認してください。

```
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
    $StoreVirtualPath
$FarmObject = Get-STFStoreFarm -StoreService $StoreObject -
    FarmName "CVAD"
$AuthObject = Get-STFAuthenticationService -SiteID $SiteID -
    VirtualPath $AuthVirtualPath
<!--NeedCopy-->
```

3. 認証サービスの CertRevocationPolicy
   プロパティを直接編集します。

```
$AuthObject.FarmsConfiguration.CertRevocationPolicy = "FullCheck"
$AuthObject.Save()
Enable-STFXmlServiceAuthentication -AuthenticationService
    $AuthObject -Farm $FarmObject
<!--NeedCopy-->
```

4. 正しい証明書失効モードを設定したことを確認してください。

```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
    $AuthVirtualPath
$AuthObject.FarmsConfiguration.CertRevocationPolicy
<!--NeedCopy-->
```

Windows イベントビューアーで予想されるエラー

CRL チェックが有効な場合、エラーは StoreFront サーバーの Windows イベントビューアーで報告されます。

イベントビューアーを開くには:

- StoreFront サーバーで **Run** と入力します。
- **eventvwr** と入力して、Enter キーを押します。
- ［アプリケーションとサービス］で、Citrix Delivery Service イベントを探します。

エラー例：ストアが失効した証明書を使用している **Delivery Controller** に接続できない

```
An SSL connection could not be established: An error occurred during
    SSL crytography: Access is denied.

This message was reported from the Citrix XML Service at address https:
    //deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.

The specified Citrix XML Service could not be contacted and has been
    temporarily removed from the list of active services.
<!--NeedCopy-->
```

エラー例：**Receiver for Web** で **XML** 認証の失敗によりユーザーがログインできない場合

```
An unexpected response was received during the authentication process.

Citrix.DeliveryServicesClients.Authentication.Exceptions.
    ExplicitAuthenticationFailure,
Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,
Culture=neutral, PublicKeyToken=null

General Authentication Failure

ExplicitResult.State: 5

AuthenticationControllerRequestUrl:
https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/
    LoginAttempt

ActionType: LoginAttempt

at
Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.
    GetExplicitAuthResult(ActionType
type, Dictionary`2 postParams)
<!--NeedCopy-->
```

共通のサブスクリプションデータストアを共有する 2 つの StoreFront ストアの構成

June 6, 2024

StoreFront のインストールプロセスでは、各 StoreFront サーバーに Windows データストアをローカルにインストールして、サブスクリプションデータを管理します。StoreFront サーバーグループ環境では、各サーバーで、そのデータストアが使用するサブスクリプションデータのコピーも管理されます。このデータは、ほかのサーバーに反映され、グループ全体でユーザーのサブスクリプションが管理されます。デフォルトでは、StoreFront は各ストア

に対して 1 つのデータストアを作成します。各サブスクリプションデータストアは、ストアごとに独立して更新されます。

異なる構成設定が必要な場合、一般的には、管理者が 2 つの異なるストアで StoreFront を構成します。ストアの 1 つは Citrix Gateway を使用してリソースに外部アクセスするため、もう 1 つは会社の LAN を使用して内部アクセスするために設定します。ストア用 web.config ファイルに簡単な変更を加えることで、共通のサブスクリプションデータストアを共有するように、「外部」ストアと「内部」ストアの両方を構成できます。

2 つのストアとそれに対応するサブスクリプションデータストアを含むデフォルトのシナリオでは、ユーザーは同じリソースに 2 回サブスクライブする必要があります。共通のサブスクリプションデータベースを共有するように 2 つのストアを構成すると、ユーザーが同じリソースに会社のネットワーク内外から簡単にアクセスできるようになり、ローミングエクスペリエンスが向上します。共有サブスクリプションデータストアを使用すると、新しいリソースを最初にサブスクライブするときに、ユーザーが「外部」ストアを使用しているのか「内部」ストアを使用しているのかは問題になりません。

- 各ストアの web.config ファイルは C:\inetpub\wwwroot\citrix<storename> にあります。
- 各ストアの web.config には、Subscription Store Service のクライアントエンドポイントが含まれています。

```
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
__Citrix_<StoreName>"authenticationMode="windows"transferMode="
Streamed">
```

各ストアのサブスクリプションデータは次の場所にあります。

```
C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\
SubscriptionsStore\1__Citrix_<StoreName>
```

2 つのストアでサブスクリプションデータストアを共有するには、一方のストアが、もう一方のストアのサブスクリプションサービスエンドポイントを参照するように設定します。サーバーグループ展開環境では、すべてのサーバーが、定義された同一の組み合わせのストアと、これらの両ストアが共有する共有データストアの同一のコピーを持ちます。

> 注:
>
> 各ストアの Citrix Virtual Apps and Desktops コントローラーの構成は一致している必要があります。構成が一致していない場合、各ストアでのリソースのサブスクリプションが一貫しなくなることがあります。データストアの共有は、2 つのストアが同じ StoreFront サーバーまたはサーバーグループ展開環境に存在する場合にのみサポートされます。

StoreFront サブスクリプションデータストアのエンドポイント

1. 単一 StoreFront 展開環境では、メモ帳を使用して外部ストアの web.config ファイルを開き、clientEndpoint を検索します。例:


```
<subscriptionsStoreClient enabled="true">
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
    __Citrix_External" authenticationMode="windows" transferMode="
    Streamed">
<clientCertificate thumbprint="0" />
</clientEndpoint>
</subscriptionsStoreClient>
<!--NeedCopy-->
```

2. 外部ストアエンドポイントを内部ストアエンドポイントと一致するように変更します:

```
<subscriptionsStoreClient enabled="true">
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
    __Citrix_Internal" authenticationMode="windows" transferMode="
    Streamed">
<clientCertificate thumbprint="0" />
</clientEndpoint>
</subscriptionsStoreClient>
<!--NeedCopy-->
```

3. StoreFront サーバーグループを使用している場合は、プライマリノードの web.config ファイルに対する変更をほかのすべてのノードに反映させます。

両ストアが内部ストアのサブスクリプションデータストアを共有するように設定されました。

ストアのお気に入りを管理する

June 6, 2024

PowerShell コマンドレットを使用してストアのサブスクリプションデータ（お気に入り）を管理します。

> 注:
>
> StoreFront 管理コンソールまたは PowerShell のどちらかを使用して、StoreFront を管理します。両方を同時に使用しないでください。StoreFront 構成を変更する場合、StoreFront 管理コンソールを閉じてから PowerShell を使用してください。既存のサブスクリプションデータを変更する時は、変更前の状態にロールバックできるようにバックアップを作成しておくことをお勧めします。

サブスクリプションデータの完全消去

サブスクリプションデータを格納するフォルダーおよびデータストアは、既存の環境の各ストアに存在します。

1. StoreFront サーバー上で、Citrix Subscriptions Store サービスを停止します。Citrix Subscriptions Store サービスの実行中は、ストアのサブスクリプションデータを削除できません。

2. StoreFront サーバー上で、サブスクリプションストアフォルダーを開きます: C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>
3. サブスクリプションストアフォルダー内のすべてのファイルを削除します。フォルダー自体は削除しないでください。
4. StoreFront サーバー上で、Citrix Subscriptions Store サービスを再起動します。

StoreFront 3.5 以降では、以下の PowerShell スクリプトを使用して、ストアのサブスクリプションデータを完全消去できます。サービスを停止または開始したり、ファイルを削除したりできる管理者権限でこの PowerShell を実行します。この PowerShell スクリプトは、上記で説明した手動の手順と同様に機能します。

コマンドレットを問題なく実行するには、サーバー上で Citrix Subscriptions Store サービスが実行されている必要があります。

```
function Remove-SubscriptionData
{

    [CmdletBinding()]

    [Parameter(Mandatory=$False)][String]$Store = "Store"

    $SubsService = "Citrix Subscriptions Store"

    # Path to Subscription Data in StoreFront version 2.6 or later

    $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\
       Roaming\Citrix\SubscriptionsStore\1__Citrix_$Store*"

    Stop-Service -displayname $SubsService

    Remove-Item $SubsPath -Force -Verbose

    Start-Service -displayname $SubsService

    Get-Service -displayname $SubsService
 }


Remove-SubscriptionData -Store "YourStore"
<!--NeedCopy-->
```

サブスクリプションデータのエクスポート

PowerShell コマンドレットを使用して、ストアサブスクリプションデータのバックアップをタブ区切りの TXT ファイル形式で取得できます。

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
   yourstore>"
```



```
2
3 Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
    :USERPROFILE\Desktop\Subscriptions.txt"
```

複数サーバー展開環境を管理している場合、この PowerShell コマンドレットを、StoreFront サーバーグループ内の任意のサーバー上で実行できます。サーバーグループの各サーバーは、ピアから同期されたサブスクリプションデータの同一コピーを保持します。StoreFront サーバー間でサブスクリプションの同期に問題がある場合、グループのすべてのサーバーからデータをエクスポートして、比較してください。

サブスクリプションデータの復元

既存のサブスクリプションデータを上書きするには、Restore-STFStoreSubscriptions を使用します。前述のように、Export-STFStoreSubscriptions を使用して作成したタブ区切りの TXT ファイル形式のバックアップから、ストアのサブスクリプションデータを復元できます。

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
    yourstore>"
2 Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath "
    $env:USERPROFILE\Desktop\Subscriptions.txt"
3 <!--NeedCopy-->
```

Restore-STFStoreSubscriptions について詳しくは、次を参照してください。https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2402/Restore-STFStoreSubscriptions/

1 つの StoreFront サーバー上でデータを復元する

単一のサーバー展開環境で、Subscriptions Store サービスをシャットダウンする必要はありません。また、サブスクリプションデータの復元前に既存のサブスクリプションデータを消去する必要もありません。

StoreFront サーバーグループ上でデータを復元する

サーバーグループにサブスクリプションデータを復元するには、次の手順に従う必要があります。

例：3 つの StoreFront サーバーを含むサーバーグループ環境。

- StoreFrontA
- StoreFrontB
- StoreFrontC

1. 3 つのサーバーのいずれかから、既存のサブスクリプションデータのバックアップを作成します。
2. サーバー StoreFrontB および StoreFrontC で Subscriptions Store サービスを停止します。この操作によって、StoreFrontA の更新中、サーバーはサブスクリプションデータを送受信することができなくなります。

3. サーバー StoreFrontB および StoreFrontC からサブスクリプションデータを完全消去します。これによって、復元されたサブスクリプションデータの不一致が発生しないようにします。
4. **Restore-STFStoreSubscriptions** コマンドレットで StoreFrontA 上にデータを復元します。Subscriptions Store サービスを停止したり、StoreFrontA でサブスクリプションデータを完全消去する必要はありません（復元操作中に上書きされます）。
5. サーバー StoreFrontB および StoreFrontC 上で、Subscriptions Store サービスを再起動します。これで、このサーバーは StoreFrontA からデータのコピーを受信できます。
6. すべてのサーバー間で同期が開始されるのを待ちます。このために必要な時間は、StoreFrontA に存在するレコード数によって異なります。すべてのサーバーがローカルネットワーク接続であれば、通常同期は迅速に行われます。WAN 接続でのサブスクリプションの同期には、多少時間がかかる場合があります。
7. StoreFrontB および StoreFrontC からデータをエクスポートして、同期が完了したことを確認します。またはストアサブスクリプションカウンターを表示します。

サブスクリプションデータのインポート

ストアにサブスクリプションデータがない場合、**Import-STFStoreSubscriptions** を使用します。このコマンドレットによって、サブスクリプションデータをストア間で転送したり、サブスクリプションデータを新しくプロビジョニングされた StoreFront サーバーにインポートしたりできます。

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
    yourstore>"
2 Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
    :USERPROFILE\Desktop\Subscriptions.txt"
3 <!--NeedCopy-->
```

Import-STFStoreSubscriptions について詳しくは、次を参照してください。https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2402/Import-STFStoreSubscriptions/

サブスクリプションデータファイルの詳細

サブスクリプションデータファイルは、各行に 1 つのユーザーサブスクリプションが記載されたテキストファイルです。各行には、以下の値がタブで区切られて記載されます：

```
<user-identifier> <resource-id> <subscription-id> <subscription-
status> <property-name> <property-value> <property-name> <property
-value> ...
```

各項目の意味は次のとおりです：

- <user-identifier>：必須キーで、ユーザーを識別する文字列です。この識別子には、ユーザーの Windows セキュリティ ID が使用されます。
- <resource-id>：必須キーで、サブスクライブされるリソースを識別する文字列です。

- <subscription-id>: 必須キーで、サブスクリプションを一意に識別する文字列です。この値は使用されません（ただし、データファイル内に値が存在する必要はあります）。
- <subscription-status>: 必須キーで、サブスクリプションの状態（subscribed または unsubscribed）です。
- <property-name>および<property-value> - オプション。0 個以上のプロパティ名/値の組み合わせです。StoreFront クライアント（通常は Citrix Workspace アプリ）によるサブスクリプションのプロパティを表します。複数の値を持つプロパティは、同じ名前の複数の「<property-name> <property-value>」ペアで示されます（MyProp が 2 つの値 A と B を持つ場合は「…MyProp A MyProp B …」など）。

例

S-0-0-00-0000000000-0000000000-0000000000-0000 XenApp.Excel 21EC2020-3AEA-4069-A2DD-08002B30309D Subscribed dazzle:position 1

StoreFront サーバーのディスク上にあるサブスクリプションデータのサイズ

レコードの数	サイズ（MB）
0	6.02
1,000	7.02
10,000	40.00
100,000	219.00
200,000	358.00
500,000	784.00
800,000	1213.02
1,000,000	1597.15
1,300,000	1919.15
1,500,000	2205.15
2,000,000	2915.15

インポートおよびエクスポートするテキストファイルのサイズ

レコードの数	サイズ（MB）
0	0.00
1,000	0.13
10,000	1.30
100,000	12.80
200,000	25.60
500,000	64.10
800,000	102.00
1,000,000	128.00
1,300,000	166.00
1,500,000	192.00
1,700,000	218.00
2,000,000	256.00

ストアのサブスクリプションカウンター

Microsoft Windows パフォーマンスモニターカウンター（[スタート] **>** [検索の開始] ボックスに「**perfmon**」と入力）を使用して、サーバー上のサブスクリプションレコードの合計数、StoreFront サーバーグループ間で同期されたレコード数などを表示できます。

PowerShell を使用したサブスクリプションカウンターの表示

```
Get-Counter -Counter "\Citrix Subscription Store(1__citrix_store)\
    Subscription Entries Count (including unpurged deleted records)"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\
    Subscriptions Store Synchronizing"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
     Subscriptions Synchronized"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
     Subscriptions Transferred"
<!--NeedCopy-->
```


Microsoft SQL Server を使用したサブスクリプションデータの保存

June 6, 2024

> 注:
>
> このドキュメントは、MS SQL Server と T-SQL クエリに関する基本的な知識を前提としています。管理者がこのドキュメントを参照するには、SQL Server を問題なく構成、使用、管理できるようにする必要があります。

はじめに

ESENT は、Windows で使用できる埋め込み可能なトランザクションデータベースエンジンです。StoreFront のすべてのバージョンは、デフォルトで組み込みの ESENT データベースの使用をサポートしています。また、ストアが SQL 接続文字列を使用するように構成されている場合、Microsoft SQL Server インスタンスに接続することもできます。

StoreFront を ESENT ではなく SQL を使用するように切り替えることの主な利点は、T-SQL の UPDATE ステートメントを使用して、サブスクリプションレコードを管理、変更、または削除できることです。SQL を使用すると、サブスクリプションデータでわずかな変更が実行されるたびに ESENT サブスクリプションデータ全体をエクスポート、変更、再インポートする必要はありません。

既存のサブスクリプションデータを ESENT から Microsoft SQL Server に移行するには、StoreFront からエクスポートされた ESENT のフラットデータを、一括インポート用の SQL フレンドリーな形式に変換する必要があります。新しいサブスクリプションデータのない新しい展開の場合、この手順は不要です。データ変換手順が必要なのは一度だけです。ここでは、参照している-STF PowerShell SDK が導入されたバージョン 3.5 以降のすべての StoreFront バージョンで使用できる、サポート対象の構成について説明します。

> 注:
>
> ネットワークの停止が原因で StoreFront がサブスクリプションデータを保存するために使用する SQL Server インスタンスへの接続に失敗した場合、StoreFront 展開は利用不能として表示されません。停止は、ユーザーエクスペリエンスを一時的に低下させるだけです。ユーザーは、SQL Server への接続が復元されるまで、お気に入りのリソースを追加、削除、または表示できません。リソースは、停止でも列挙および起動できます。予測される動作は、ESENT の使用中に Citrix Subscription Store サービスが停止する場合と同じです。
>
> ヒント:
>
> リソースが KEYWORDS:Auto または KEYWORDS:Mandatory で構成されていると、ESENT または SQL で両方を使用する場合と同じように動作します。いずれかの KEYWORD がユーザーのリソースに含まれている場合、ユーザーが最初にログオンすると、新しい SQL サブスクリプションレコードが自動的に作成されます。

ESENT および **SQL Server** の利点

ESENT	SQL
デフォルト。StoreFront を「そのまま」使用するため追加構成は不要です。	非常に管理しやすい。T-SQL クエリを使用してサブスクリプションデータを簡単に操作または更新できます。ユーザーごとのレコードを削除または更新可能。アプリケーション、Delivery Controller、またはユーザーごとに簡単にレコードをカウントできます。企業/組織から離職したユーザーの不要なユーザーデータを簡単に削除できます。管理者がアグリゲーションの使用に切り替えたときや、新しい Delivery Controller がプロビジョニングされたときなど、Delivery Controller の参照を簡単に更新できます。
サブスクリプションの同期と取得スケジュールを使用して、異なるサーバーグループ間でレプリケーションを簡単に構成できます。「サブスクリプション同期の構成」を参照してください。	StoreFront から切り離されているため、StoreFront をアップグレードする前にサブスクリプションデータをバックアップする必要はありません。データは別の SQL Server で維持されます。サブスクリプションのバックアップは StoreFront に依存せず、SQL のバックアップ戦略とメカニズムを使用します。
サブスクリプション管理が不要な場合、SQL は不要です。サブスクリプションデータを更新する必要がない場合、ESENT の方が顧客のニーズに適している可能性が高くなります。	サーバーグループのすべてのメンバーが共有するサブスクリプションデータの単一コピー。サーバー間のデータの違いやデータ同期の問題が発生する可能性が低くなります。

ESENT および **SQL Server** の欠点

ESENT	SQL
サブスクリプションデータを簡単かつきめ細かく管理する簡単な手段はありません。エクスポートされた.txt ファイルでサブスクリプションの操作を行う必要があります。サブスクリプションデータベース全体をエクスポートおよび再インポートする必要があります。場合によっては、何千ものレコードを検索と置換の手法を使用して変更する必要があります。この手法は手間がかかりエラーの可能性も高くなります。	基本的な SQL の専門知識とインフラストラクチャが必要です。SQL ライセンスの購入が必要になる場合があり、StoreFront 展開の総所有コストが増加します。ただし、Citrix Virtual Apps and Desktops データベースインスタンスを StoreFront と共有してコストを削減することもできます。

ESENT	SQL
サーバーグループ内の各 StoreFront サーバーで ESENT データベースのコピーを保持する必要があります。まれに、このデータベースがサーバーグループ内または異なるサーバーグループ間で同期しなくなることがあります。	サーバーグループ間でのサブスクリプションデータのレプリケーションは、重要な展開タスクです。複数の SQL インスタンスと、データセンターごとに各インスタンス間のトランザクションのレプリケーションが必要です。これには、MS SQL の専門知識が必要です。 ESENT からのデータ移行および SQL フレンドリーな形式への変換が必要です。このプロセスが必要なのは一度だけです。 追加の Windows サーバーとライセンスが必要になる場合があります。 StoreFront を展開するための追加手順。

展開シナリオ

> 注:
>
> ユーザーサブスクリプションをサポートするには、StoreFront 内で構成された各ストアに ESENT データベースまたは Microsoft SQL データベースが必要です。サブスクリプションデータの保存方法は、StoreFront 内のストアレベルで設定されます。

管理の複雑さを軽減し、構成ミスのスコープを減らすために、すべてのストアデータベースを同じ Microsoft SQL Server インスタンスに配置することを Citrix ではお勧めします。

すべて同じ接続文字列を使用するように構成されていれば、複数のストアで同じデータベースを共有できます。異なる Delivery Controller を使用していても問題ありません。複数のストアがデータベースを共有することの欠点は、各サブスクリプションレコードがどのストアに対応するかを知る方法がないことです。

複数のストアを持つ単一の StoreFront 展開では、技術的には 2 つのデータストレージ方法の組み合わせが可能です。ESENT を使用するように 1 つのストアを構成し、別のストアでは SQL を使用するように構成できます。これは、管理の複雑さと構成ミスのスコープがあるためお勧めしません。

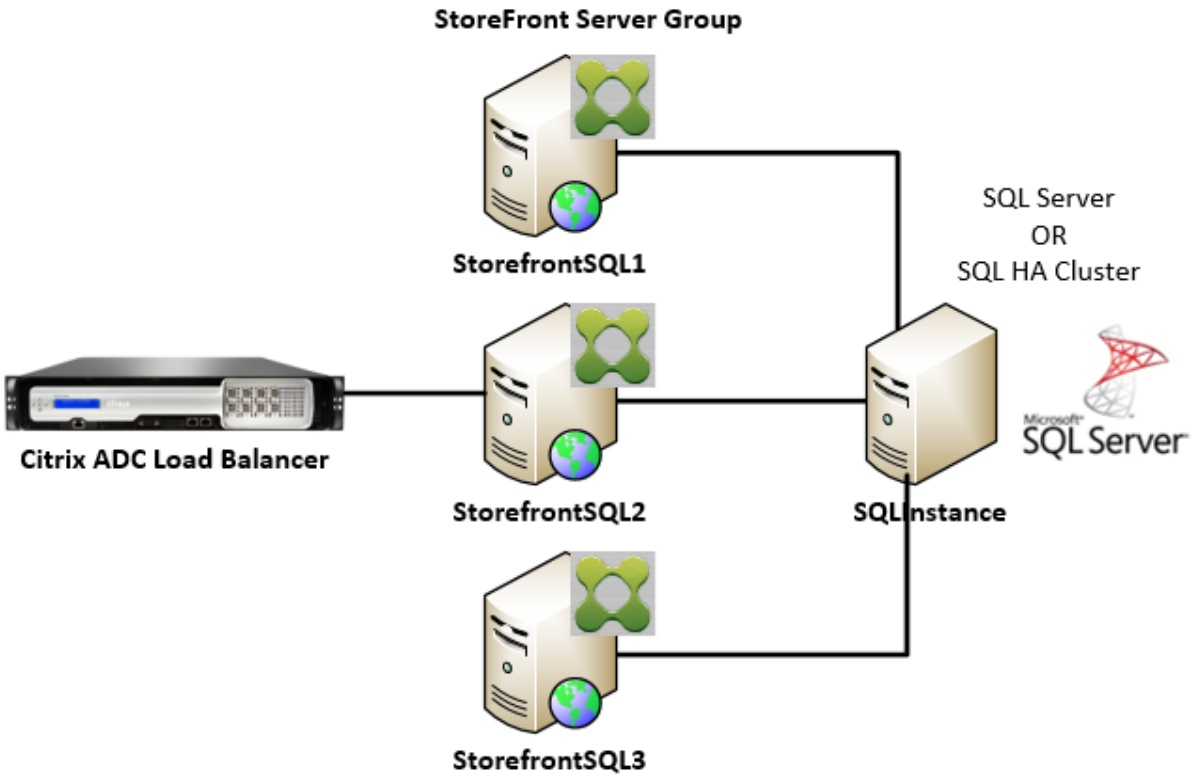
SQL
Server にサブスクリプションデータを保存する場合、4 つのシナリオがあります:

シナリオ **1**: **ESENT** を使用する単一の **StoreFront** サーバーまたはサーバーグループ（デフォルト）　デフォルトではバージョン 2.0 以降の StoreFront のすべてのバージョンは、フラット ESENT データベースを使用して、サーバーグループのメンバー間でサブスクリプションデータを保存および複製します。サーバーグループの各メンバーは、サブスクリプションデータベースの同一のコピーを保持し、これはサーバーグループの他のすべてのメンバーと同期されます。このシナリオでは、追加の構成手順は必要ありません。このシナリオは、Delivery Controller の名前を

頻繁に変更しないお客様や、古いユーザーサブスクリプションの削除や更新など、サブスクリプションデータの管理タスクを頻繁に実行する必要がない大半のお客様に適しています。

シナリオ **2**：単一の **StoreFront** サーバーとローカル **Microsoft SQL Server** インスタンスがインストールされている　StoreFront はローカルにインストールされた SQL Server インスタンスを使用します。両方のコンポーネントは同じサーバー上にあります。このシナリオは、Delivery Controller の名前を頻繁に変更する必要があるお客様や、古いユーザーサブスクリプションの削除や更新など、サブスクリプションデータの管理タスクを頻繁に実行する必要があるものの、高可用性 StoreFront 展開は必要ないお客様のシンプルな単一 StoreFront 展開に適しています。このシナリオは、Microsoft SQL データベースインスタンスをホストするサーバーグループメンバーに単一障害点を作成するため、サーバーグループにはお勧めしません。このシナリオは、大規模なエンタープライズ展開には適していません。

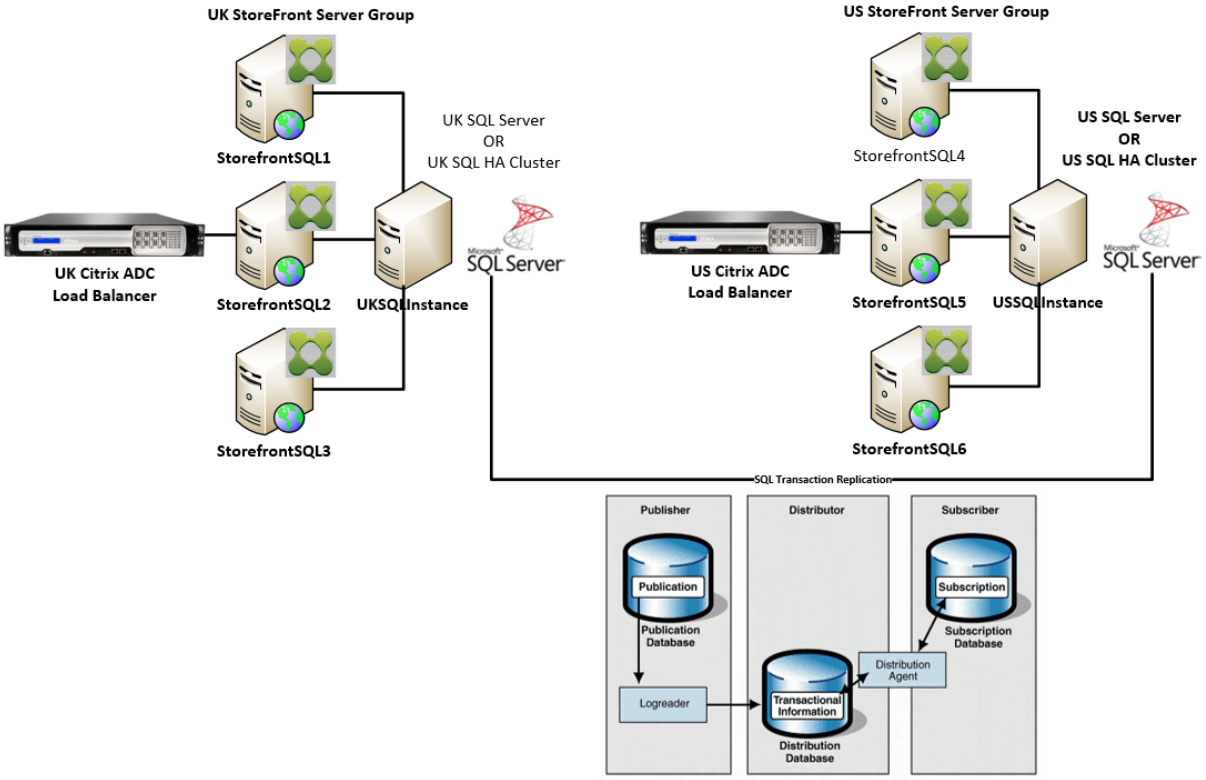
シナリオ **3**：高可用性用に構成された **StoreFront** サーバーグループおよび専用の **Microsoft SQL Server** インスタンス（推奨）　すべての StoreFront サーバーグループメンバーは、同じ専用の Microsoft SQL Server インスタンスまたは SQL フェールオーバークラスターに接続します。これは、Citrix 管理者が Delivery Controller の名前を頻繁に変更する必要性や、古いユーザーサブスクリプションの削除や更新など、サブスクリプションデータの管理タスクを頻繁に実行する必要性があり、高可用性が必要とされる大規模なエンタープライズ展開に適したモデルです。



シナリオ **4**：複数の **StoreFront** サーバーグループ、およびサーバーグループごとの各データセンター内の専用 **Microsoft SQL Server** インスタンス

> 注:
>
> これは高度な構成です。トランザクションレプリケーションに精通した経験豊富な SQL Server 管理者が存在し、正常に展開するために必要なスキルがある場合にのみ実行してください。

これはシナリオ 3 と同様のシナリオですが、異なるリモートデータセンターで複数の StoreFront サーバーグループが必要な状況に応じて拡張されています。Citrix 管理者は、サブスクリプションデータを同じデータセンター内の異なるサーバーグループ間で同期するか、異なるデータセンター内の異なるサーバーグループ間で同期するかを選択できます。データセンター内の各サーバーグループは、冗長性、フェールオーバー、パフォーマンスのために、専用の Microsoft SQL Server インスタンスに接続します。このシナリオでは、Microsoft SQL Server 構成とインフラストラクチャに大幅な追加が必要です。サブスクリプションデータとその SQL トランザクションのレプリケーションは、Microsoft SQL テクノロジに完全に依存しています。



リソース

https://github.com/citrix/sample-scripts/tree/master/storefrontから次のスクリプトをダウンロードできます:

構成スクリプト

- **Set-STFDatabase.ps1** –各ストアの MS SQL 接続文字列を設定します。StoreFront サーバーで実行します。

- **Add-LocalAppPoolAccounts.ps1** –ローカル StoreFront サーバーのアプリプールに、SQL データベースへの読み取りおよび書き込みアクセスを許可します。SQL Server でシナリオ 2 を実行します。
- **Add-RemoteSFAccounts.ps1** –サーバーグループ内のすべての StoreFront サーバーに、SQL データベースへの読み取りおよび書き込みアクセスを許可します。SQL Server でシナリオ 3 を実行します。
- **Create-StoreSubscriptionsDB-2016.sql** –SQL データベースとスキーマを作成します。SQL Server で実行します。

データの変換およびインポートスクリプト

- **Transform-SubscriptionDataForStore.ps1** –ESENT 内の既存のサブスクリプションデータをインポート用の SQL フレンドリーな形式にエクスポートして変換します。
- **Create-ImportSubscriptionDataSP.sql** – ストアドプロシージャを作成して Transform-SubscriptionDataForStore.ps1 で変換されたデータをインポートします。Create-StoreSubscriptionsDB-2016.sql を使用してデータスキーマを作成後、SQL Server でこのスクリプトを実行します。

SQL Server で StoreFront サーバーのローカルセキュリティグループを構成する

シナリオ **2**: 単一の **StoreFront** サーバーとローカル **Microsoft SQL Server** インスタンスがインストールされている

Microsoft SQL Server で<SQLServer>\StoreFrontServersというローカルセキュリティグループを作成し、IIS APPPOOL\DefaultAppPoolおよびIIS APPPOOL\Citrix Receiver for Webの仮想アカウントを追加してローカルにインストールされた StoreFront が SQL に読み取りおよび書き込みアクセスを許可します。このセキュリティグループは、ストアサブスクリプションデータベーススキーマを作成する.SQL スクリプトで参照されるため、グループ名が一致することを確認してください。

スクリプトAdd-LocalAppPoolAccounts.ps1をダウンロードできます:

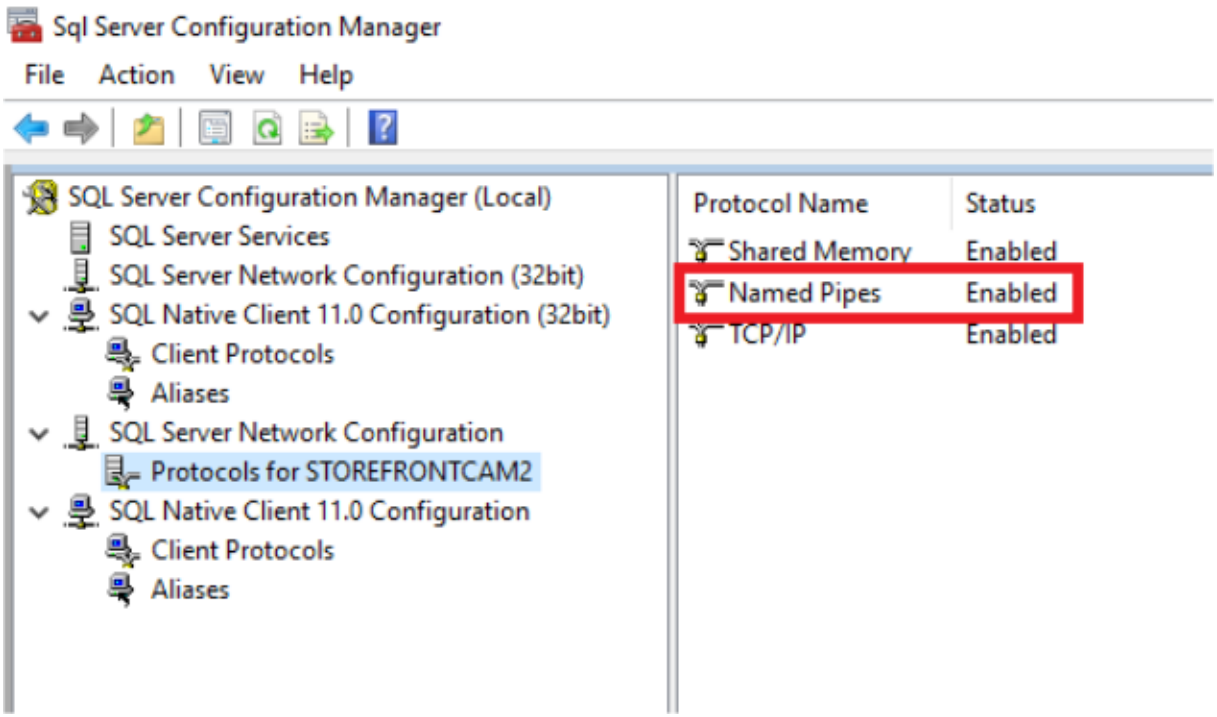
Add-LocalAppPoolAccounts.ps1 スクリプトを実行する前に StoreFront をインストールします。このスクリプトは、StoreFront がインストールされ構成されるまで存在しないIIS APPPOOL\Citrix Receiver for Web仮想 IIS アカウントを検出する機能に依存するためです。IIS APPPOOL\DefaultAppPoolは、IIS Web サーバーの役割をインストールすることで自動的に作成されます。

```
# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool Virtual Accounts"

# Check whether the Local Group Exists
if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
{

```



```
9       Write-Host "$LocalGroupName already exists!" -ForegroundColor "
            Yellow"
10   }
11
12  else
13  {
14
15  Write-Host "Creating $LocalGroupName local security group" -
        ForegroundColor "Yellow"
16
17  # Create Local User Group
18  $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
19  $LocalGroup = $Computer.Create("group",$LocalGroupName)
20  $LocalGroup.setinfo()
21  $LocalGroup.description = $Description
22  $Localgroup.SetInfo()
23  Write-Host "$LocalGroupName local security group created" -
        ForegroundColor "Green"
24   }
25
26  $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
27
28  # Add IIS APPPOOL\DefaultAppPool
29  $objAccount = New-Object System.Security.Principal.NTAccount("IIS
        APPPOOL\DefaultAppPool")
30  $StrSID = $objAccount.Translate([System.Security.Principal.
        SecurityIdentifier])
31  $DefaultSID = $StrSID.Value
32
33  $Account = [ADSI]"WinNT://$DefaultSID"
34  $Group.Add($Account.Path)
35
36  # Add IIS APPPOOL\Citrix Receiver for Web
37  $objAccount = New-Object System.Security.Principal.NTAccount("IIS
        APPPOOL\Citrix Receiver for Web")
38  $StrSID = $objAccount.Translate([System.Security.Principal.
        SecurityIdentifier])
39  $WebRSID = $StrSID.Value
40
41  $Account = [ADSI]"WinNT://$WebRSID"
42  $Group.Add($Account.Path)
43
44  Write-Host "AppPools added to $LocalGroupName local group" -
        ForegroundColor "Green"
45  <!--NeedCopy-->
```

SQL Server 構成マネージャーを使用して、ローカル SQL インスタンス内の名前付きパイプを有効にします。StoreFront と SQL Server のプロセス間通信には名前付きパイプが必要です。

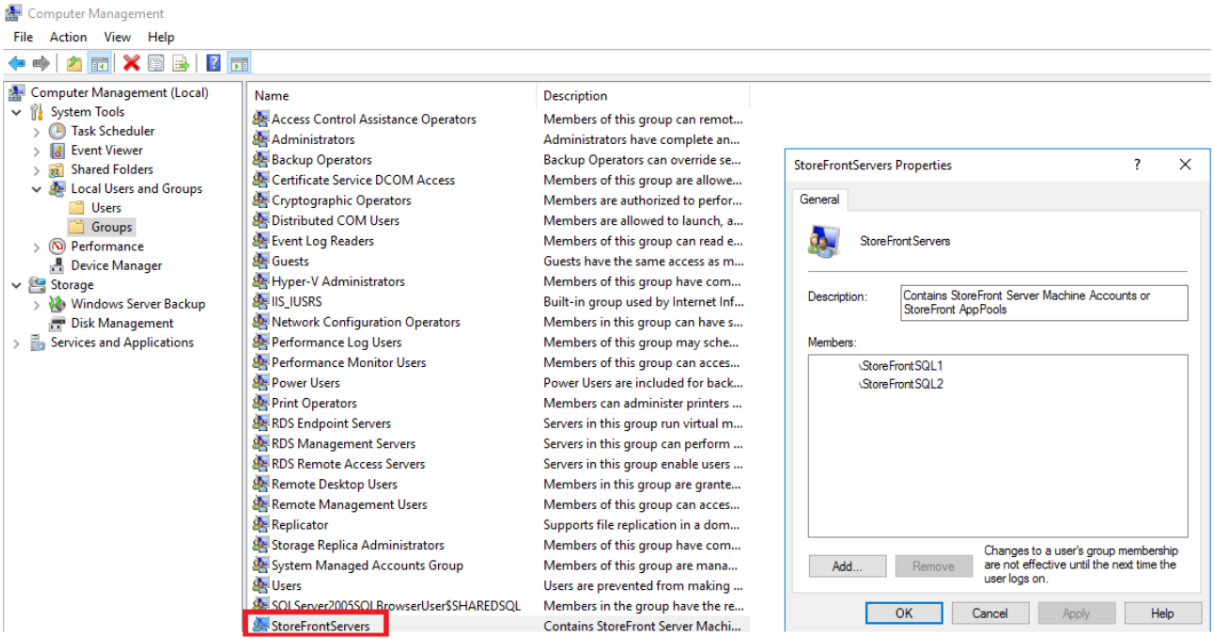


特定のポートまたは動的ポートを使用して SQL Server 接続を許可するように、Windows ファイアウォール規則が正しく構成されていることを確認します。使用中の環境でこれを実行する方法について詳しくは、Microsoft 社のドキュメントを参照してください。

> ヒント:
>
> ローカル SQL インスタンスへの接続に失敗する場合は、localhost または接続文字列で使用される<hostname>が正しい IPv4 アドレスに解決されていることを確認します。Windows は IPv4 の代わりに IPv6 の使用を試み、localhost の DNS 解決は StoreFront および SQL Server の正しい IPv4 アドレスではなく::1 を返すことがあります。この問題を解決するために、場合によってはホストサーバーで IPv6 ネットワークスタックを完全に無効にする必要があります。

シナリオ **3**: **StoreFront** サーバーグループおよび専用の **Microsoft SQL Server** インスタンス

Microsoft SQL Server で<SQLServer>\StoreFrontServersと呼ばれるローカルセキュリティグループを作成し、StoreFront サーバーグループのすべてのメンバーを追加します。このセキュリティグループは、後から SQL 内にサブスクリプションデータベーススキーマを作成する **Create-StoreSubscriptionsDB-2016.sql** スクリプトで参照されます。



すべての StoreFront サーバーグループのドメインコンピューターアカウントを<SQLServer>\StoreFrontServersグループに追加します。SQL Server が Windows 認証を使用している場合、このグループに登録されている StoreFront サーバーのドメインコンピューターアカウントのみが、SQL でサブスクリプションレコードを読み書きできます。スクリプトAdd-RemoteSFAccounts.ps1で提供される次の PowerShell 関数は、ローカルセキュリティグループを作成し、StoreFrontSQL1 および StoreFrontSQL2 という名前の 2 つの StoreFront サーバーに追加します。

```
function Add-RemoteSTFMachineAccounts
{

[CmdletBinding()]
param([Parameter(Mandatory=$True)][string]$Domain,
[Parameter(Mandatory=$True)][array]$StoreFrontServers)

# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool virtual accounts"

# Check whether the Local Security Group already exists
if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "
        Yellow"
 }

else
{

    Write-Host "Creating $LocalGroupName local group" -ForegroundColor
```

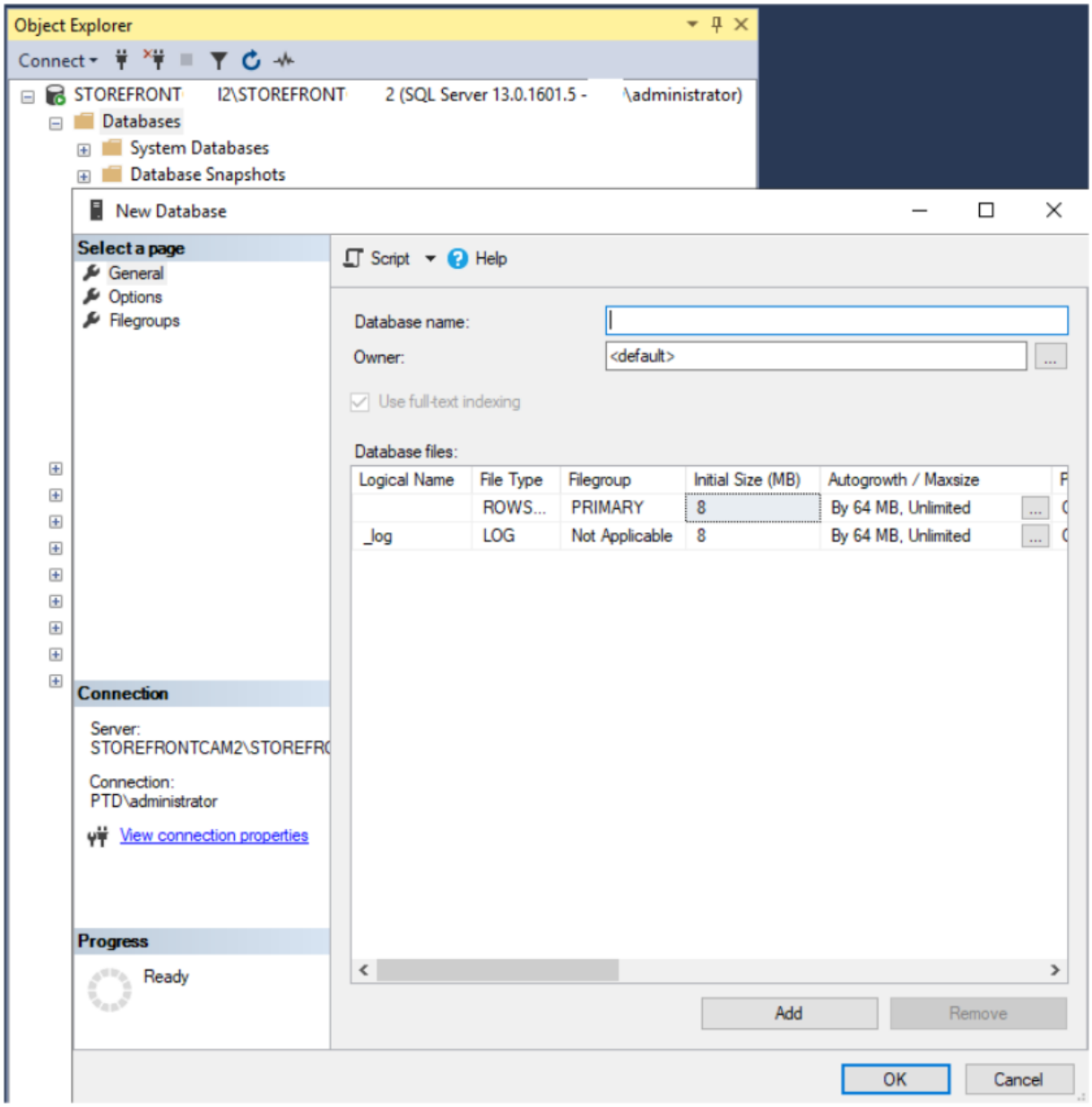


```
          "Yellow"
23
24      # Create Local Security Group
25      $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
26      $LocalGroup = $Computer.Create("group",$LocalGroupName)
27      $LocalGroup.setinfo()
28      $LocalGroup.description = $Description
29      $Localgroup.SetInfo()
30  Write-Host "$LocalGroupName local group created" -ForegroundColor "
        Green"
31   }
32
33  Write-Host "Adding $StoreFrontServers to $LocalGroupName local group" -
        ForegroundColor "Yellow"
34
35  foreach ($StoreFrontServer in $StoreFrontServers)
36  {
37
38      $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
39      $Computer = [ADSI]"WinNT://$Domain/$StoreFrontServer$"
40      $Group.Add($Computer.Path)
41   }
42
43  Write-Host "$StoreFrontServers added to $LocalGroupName" -
        ForegroundColor "Green"
44   }
45
46  Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers @("
        StoreFrontSQL1","StoreFrontSQL2")
47  <!--NeedCopy-->
```

Microsoft SQL Server 内でストアごとにサブスクリプションデータベーススキーマを構成する

StoreFront で使用する Microsoft SQL Server に名前付きインスタンスを作成します。使用する SQL のバージョンがインストールされている場所、またはそのデータベースファイルが保存されている場所に対応するように、.SQL スクリプト内のパスを設定します。サンプルスクリプトCreate-StoreSubscriptionsDB-2016.sqlは SQL Server 2016 Enterprise を使用しています。

［データベース］を右クリックしてから ［新しいデータベース］を選択し、SQL Server Management Studio（SSMS）を使用して空のデータベースを作成します。



ストアに一致する ［データベース名］を入力するか、*STFSubscriptions* のような異なる名前を選択します。

スクリプトを実行する前に、StoreFront 展開環境の各ストアでサンプルスクリプトの参照を変更して StoreFront 展開と SQL 展開を一致させます。たとえば、次の項目を変更します:

- 作成する各データベースに`USE [STFSubscriptions]`の StoreFront のストア名と一致する名前を付けます。
- データベースの.mdf ファイルと.ldf ファイルへのパスを、データベースを保存する場所に設定します。

  ```
  C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
  STFSubscriptions.mdf

  C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
  ```

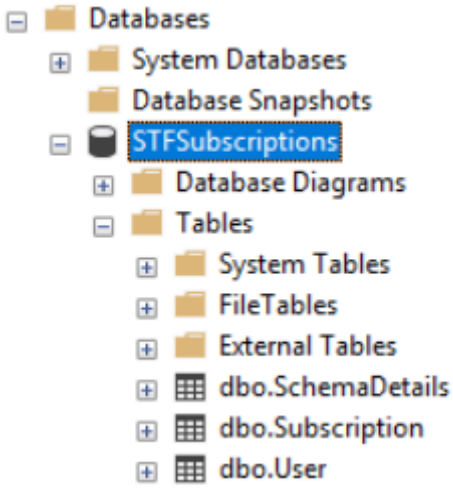


```
STFSubscriptions.ldf
```

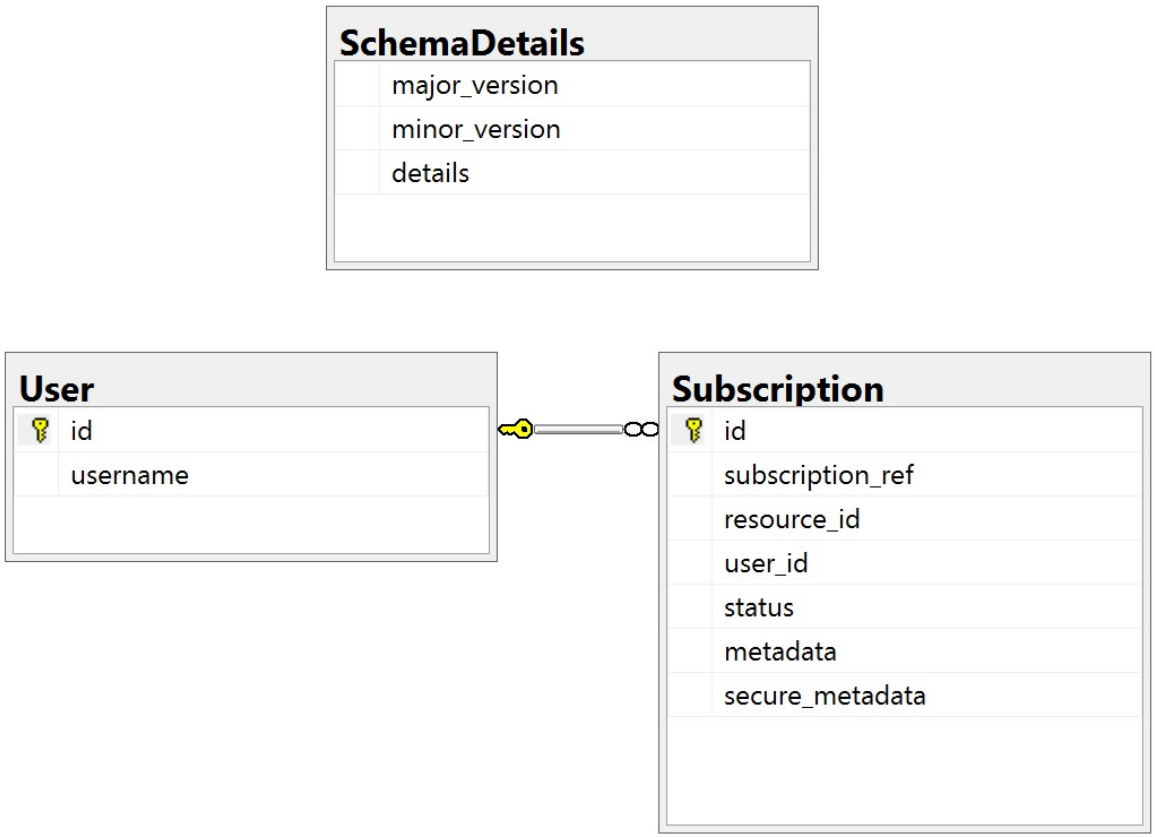
- スクリプト内で SQL Server の名前への参照を設定します:

```
CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;

ALTER LOGIN [SQL2016\StoreFrontServers]
```

スクリプトを実行します。スキーマが正常に構成されると、次の 3 つのデータベーステーブルが作成されます: *SchemaDetails*、*Subscription*、*User*。



次のデータベース図は、*Create-StoreSubscriptionsDB-2016.sql* スクリプトが作成したサブスクリプションデータベーススキーマです。



各 **StoreFront** ストアの **SQL Server** 接続文字列を構成する

シナリオ **1**

> ヒント：
>
> ESENT データベースのディスクに保存されている元のサブスクリプションデータは、破棄または削除されません。Microsoft SQL Server から ESENT の使用に戻す場合、ストア接続文字列を削除して、元のデータの使用に切り替えることができます。ストアで SQL が使用されている間に作成された追加のサブスクリプションは ESENT に存在せず、ユーザーにはこれらの新しいサブスクリプションレコードは表示されません。元のサブスクリプションレコードはすべて、引き続き存在します。

ストアでの **ESENT** サブスクリプションを再度有効にするには　PowerShell ISE を開き、［管理者として実行］を選択します。

-UseLocalStorage オプションを使用して、ESENT サブスクリプションを再度有効にするストアを指定します：

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store1"

# Sets SQL DB Connection String
```



```
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
    $StoreVirtualPath

# Removes the SQL DB Connection string and reverts back to using ESENT
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    UseLocalStorage
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
<!--NeedCopy-->
```

シナリオ **2**、**3**、**4**

PowerShell ISE を開き、［管理者として実行］を選択します。

$StoreVirtualPath を使用して接続文字列を設定するストアを指定します。

```
$SiteID = 1
$VirtualPath= "/Citrix/Store1"
$DBName = "Store1"
$DBServer = "SQL2016Ent"
$DBLocalServer = "localhost"
$SQLInstance = "StoreFrontInstance"

# For a remote database instance
$ConnectionString = "Server=$DBServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"
<!--NeedCopy-->
```

または

```
# For a locally installed database instance
$ConnectionString = "$DBLocalServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath "/
    Citrix/Store"
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    ConnectionString $ConnectionString
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
<!--NeedCopy-->
```

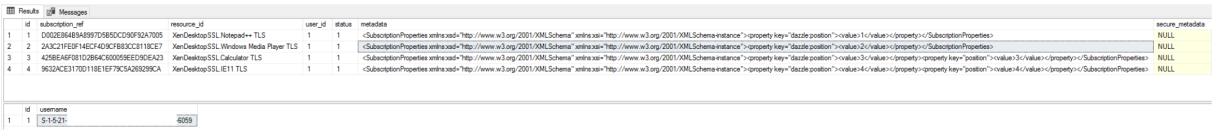
すべてのストアで SQL 接続文字列を使用するように構成する場合は、展開内のすべてのストアに対してこのプロセスを繰り返します。

ESENT から **Microsoft SQL Server** に既存のデータを移行する

既存の ESENT データを SQL に移行するには、2 段階のデータ変換プロセスが必要です。この一度のみの操作を実行するために役立つ 2 つのスクリプトが提供されています。StoreFront の接続文字列と SQL インスタンスが正しく構成されている場合、新しいサブスクリプションはすべて SQL 内で正しい形式で自動的に作成されます。移行後、過

去の ESENT サブスクリプションデータは SQL 形式に変換され、ユーザーは以前にサブスクライブしたリソースも表示できます。

例：同じドメインユーザーの **4** つの **SQL** サブスクリプション



手順 **1 Transform-SubscriptionDataForStore.ps1** スクリプトを使用して、**ESENT** データを一括インポート用の **SQL** フレンドリー形式に変換する　ESENT データを変換する StoreFront サーバーにログインします。

サーバーグループのすべてのメンバーに同じ数のサブスクリプションレコードが含まれている場合、どのメンバーでも使用できます。

PowerShell ISE を開き、［管理者として実行］を選択します。

スクリプトTransform-SubscriptionDataForStore.ps1を実行すると、<StoreName>.txtファイルが ESENT データベースから現在のユーザーのデスクトップにエクスポートされます。

PowerShell スクリプトは、デバッグを支援し、操作の成功を評価するために処理される各サブスクリプション行に関する詳細なフィードバックを提供します。この処理には時間がかかる場合があります。

変換されたデータはスクリプトが完了した後、現在のユーザーのデスクトップの<StoreName>SQL.txtに書き出されます。このスクリプトは、一意のユーザーレコード数と処理されたサブスクリプションの総数をまとめます。

SQL Server に移行するストアごとにこの処理を繰り返します。

手順 **2 T-SQL** ストアドプロシージャを使用して変換されたデータを一括 **SQL** インポートする　一度に 1 つのストアのデータのみをインポートする必要があります。

手順 1 で作成された<StoreName>SQL.txtファイルを StoreFront サーバーのデスクトップから Microsoft SQL Server のC:\にコピーして、SubscriptionsSQL.txt に名前を変更します。

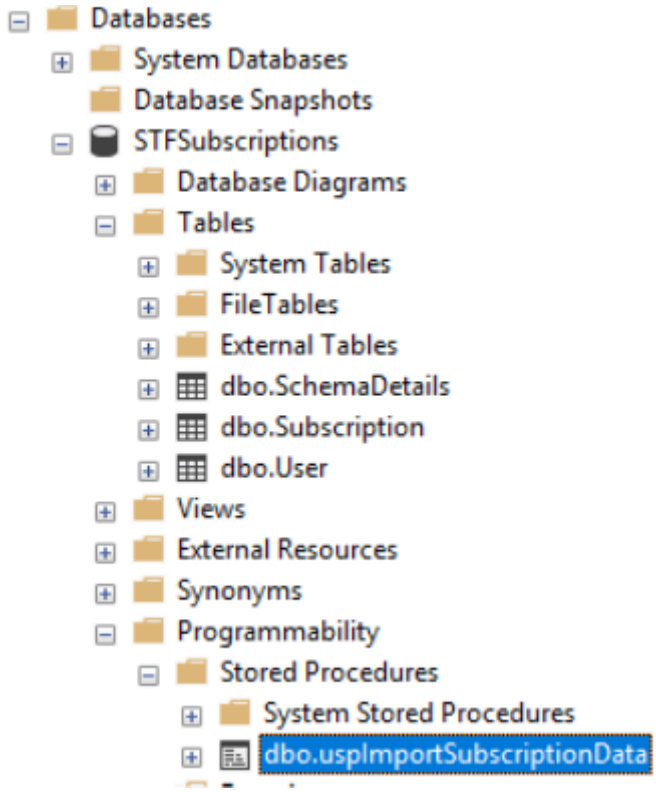
Create-ImportSubscriptionDataSP.sqlスクリプトは T-SQL ストアドプロシージャを作成して、サブスクリプションデータを一括インポートします。一意のユーザーごとに重複するエントリが削除されるため、結果の SQL データは正しく正規化され、正しいテーブルに分割されます。

Create-ImportSubscriptionDataSP.sql を実行する前に、USE [STFSubscriptions]を変更してストアドプロシージャを作成するデータベースに一致させます。

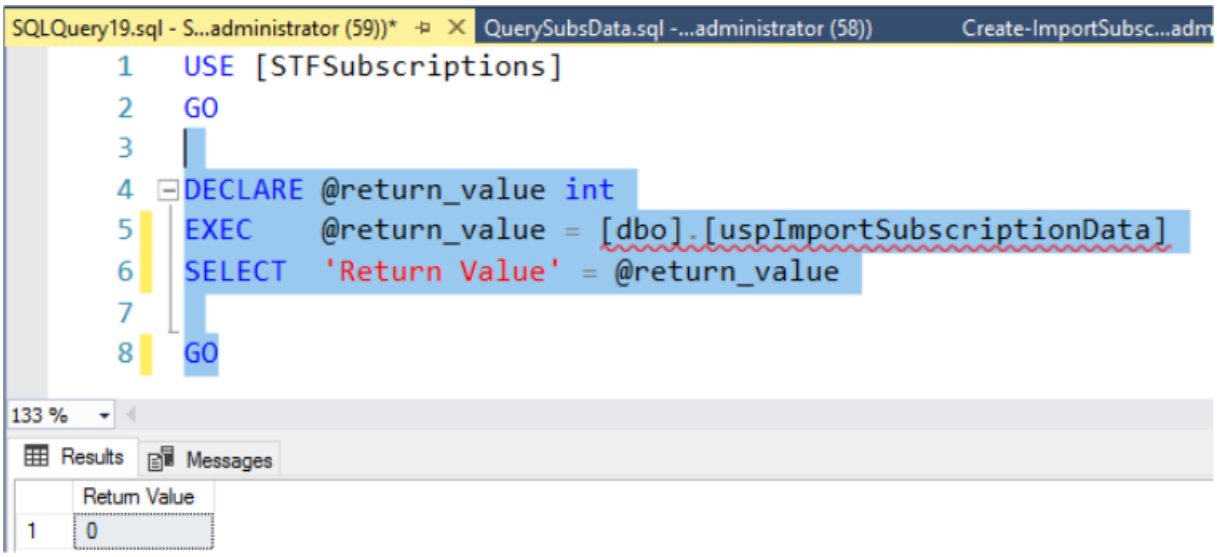
SQL Server Management Studio を使用して *Create-ImportSubscriptionDataSP.sql* ファイルを開き、その中のコードを実行します。このスクリプトは *ImportSubscriptionDataSP* ストアドプロシージャを以前に作成したデータベースに追加します。

ストアドプロシージャが正常に作成されると、SQL コンソールに次のメッセージが表示され、ImportSubscriptionDataSP ストアドプロシージャがデータベースに追加されます:

```
Commands completed successfully.
```



ストアドプロシージャを右クリックして実行し、［ストアドプロシージャの実行］を選択し ［**OK**］をクリックします。



戻り値 0 は、すべてのデータが正常にインポートされたことを示します。インポートに関する問題はすべて SQL コンソールに記録されます。ストアドプロシージャが正常に実行された後、サブスクリプションレコードの合計数と以

下の 2 つの SQL クエリの結果とともにTransform-SubscriptionDataForStore.ps1が提供する一意のユーザー数を比較します。2 つの合計数は一致する必要があります。

変換スクリプトからのサブスクリプションの総数は、SQL から報告される合計数と一致する必要があります。

```
SELECT COUNT(*) AS TotalSubscriptions
FROM [Subscription]
<!--NeedCopy-->
```

変換スクリプトからの一意のユーザー数は、SQL から報告される User テーブルのレコード数と一致する必要があります。

```
SELECT COUNT(*) AS TotalUsers
FROM [User]
<!--NeedCopy-->
```

変換スクリプトで 100 の一意のユーザーと 1000 の合計サブスクリプションレコードが表示された場合、移行が成功した後、SQL で同じ 2 つの数値が表示される必要があります。

StoreFront にログインして、既存のユーザーがサブスクリプションデータを表示できるかどうかを確認します。ユーザーがリソースをサブスクライブしたり、サブスクリプションを解除したりすると、既存のサブスクリプションレコードが SQL で更新されます。新しいユーザーとサブスクリプションレコードも SQL で作成されます。

手順 **3** インポートされたデータで **T-SQL** クエリを実行する

> 注:
>
> Delivery Controller の名前はすべて大文字と小文字が区別され、StoreFront 内で使用される名前および大文字と小文字に正確に一致する必要があります。

```
-- Get all SQL subscription records
Use [STFSubscriptions]
SELECT * FROM [Subscription]
SELECT * FROM [User]
<!--NeedCopy-->
```

```
-- Get all subscription records for a particular user SID
Use [STFSubscriptions]
SELECT * FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'

-- Get total number of Subscription records for a particular user SID
Use [STFSubscriptions]
SELECT COUNT(Subscription.id)
FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
```



```
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'
<!--NeedCopy-->
```

```
-- Get all subscription records for a particular delivery controller
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'

-- Get all subscription records for a particular application
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] = ' DeliveryController.Application'
<!--NeedCopy-->
```

T-SQL を使用して既存のサブスクリプションレコードを更新または削除する

> 免責:
>
> すべてのサンプル SQL UPDATE および DELETE ステートメントは、完全にお客様の責任において使用されます。Citrix は、提供された例を誤って使用したことによるサブスクリプションデータの損失または偶発的な変更について責任を負いません。以下の T-SQL ステートメントは、簡単な更新を実行できるようにするためのガイドとして提供されています。サブスクリプションの更新または古いレコードの削除を試みる前に、SQL データベースの完全バックアップですべてのサブスクリプションデータのバックアップを作成してください。必要なバックアップの実行に失敗すると、データの損失または破損が発生する可能性があります。独自の T-SQL UPDATE または DELETE ステートメントを実稼働データベースに実行する前に、実際の実稼働データベースから離れてダミーデータまたは実稼働データの冗長コピーでテストします。
>
> 注:
>
> Delivery Controller の名前はすべて大文字と小文字が区別され、StoreFront 内で使用される名前および大文字と小文字に正確に一致する必要があります。

```
-- Update the delivery controller used in all subscriptions.
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','NewDeliveryController.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
<!--NeedCopy-->
```

```
-- After enabling multi-site aggregation, update the resource_id
Use [STFSubscriptions]
```



```
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    DefaultAggregationGroup.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
<!--NeedCopy-->
```

```
-- Delete all subscription records for a particular Delivery Controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'
<!--NeedCopy-->
```

```
-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
<!--NeedCopy-->
```

```
-- Delete all subscription records for a particular application
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] LIKE '%.Application'
<!--NeedCopy-->
```

```
-- Delete all subscription records for an application published via a
    specific delivery controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] = 'DeliveryController.Application'
<!--NeedCopy-->
```

```
-- Delete all subscription records for a particular user SID
-- relies on cascade to delete records from [Subscription]
Use [STFSubscriptions]
DELETE FROM [User]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
<!--NeedCopy-->
```

```
-- Delete ALL subscription data from a particular database and reset
    the primary key clustered index to start numbering from 0.
-- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.
-- Can be useful whilst debugging data import issues to start with a
    clean database.

Use [STFSubscriptions]
DELETE FROM [Subscription]
DBCC CHECKIDENT ([Subscription], RESEED, 0)
DELETE FROM [User]
```



```
DBCC CHECKIDENT ([User], RESEED, 0)
<!--NeedCopy-->
```

お気に入りの有効化または無効化

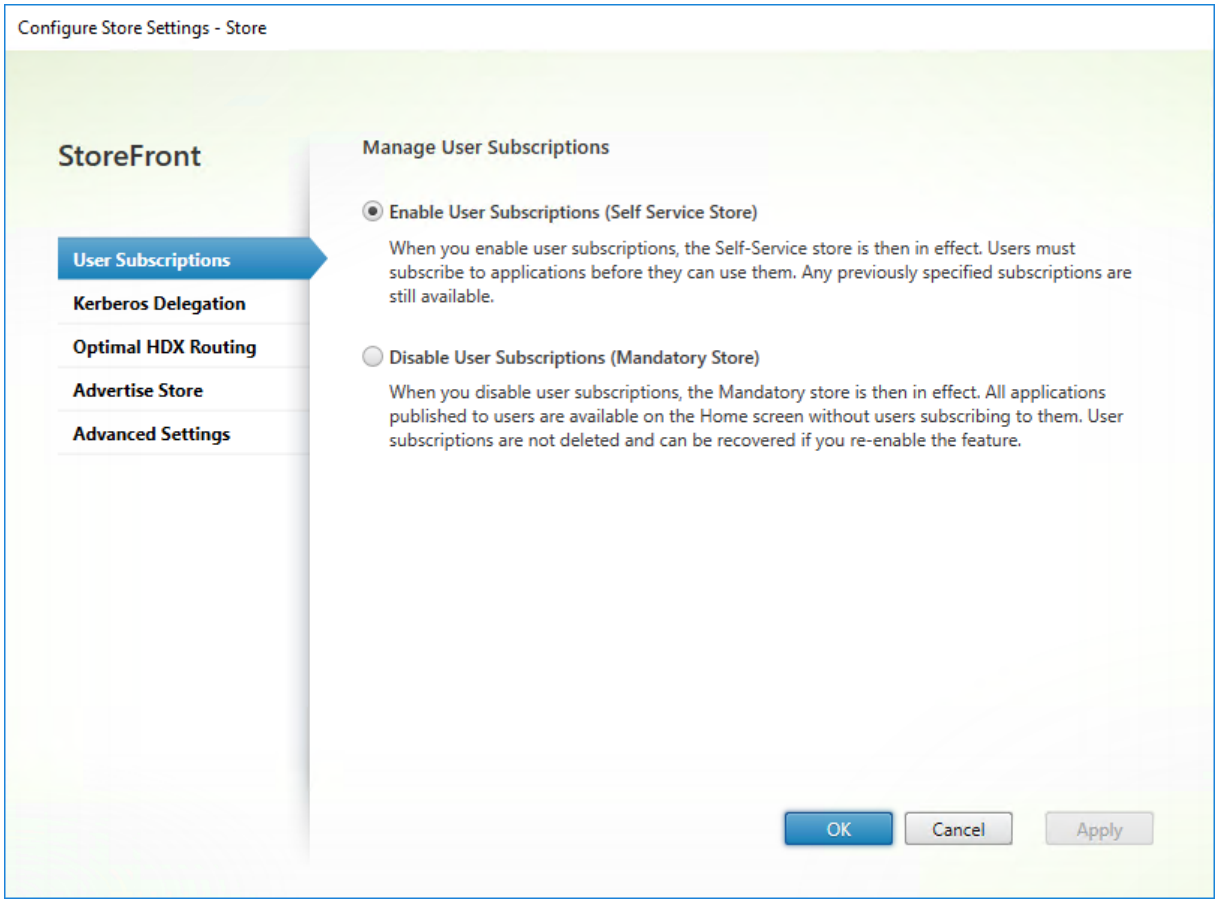
June 6, 2024

ユーザーサブスクリプション画面を使用して、以下のオプションのどちらかを選択します:

- ユーザーがお気に入りを作成および削除できるようにします（セルフサービスストア）。ユーザーは、アプリのタイルの星をクリックしてアプリをお気に入りに追加できます。もう一度星をクリックすると、アプリをお気に入りから外すことができます。お気に入りのアプリは ［ホーム］タブに表示されます。
- お気に入りを無効にします（必須ストア）。ユーザーはアプリをお気に入りに登録したり、お気に入りから外したりすることはできません。［ホーム］タブは表示されません。

サブスクリプションを無効にしても、ストアのサブスクリプションデータは削除されません。ストアのサブスクリプションを再度有効にすると、ユーザーが次回ログオンした時にお気に入りに登録されたアプリが［お気に入り］に表示されます。

1. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインで、［ストア設定の構成］を選択します
2. ［ユーザーのサブスクリプション］タブをクリックして、ユーザーのお気に入り機能のオフとオンを切り替えます。
3. ［ユーザーのサブスクリプションの有効化（セルフサービスストア）］を選択して、お気に入りを有効にします。
4. ［ユーザーのサブスクリプションの無効化（必須ストア）］を選択して、お気に入りを無効にします。



あるいは、PowerShell コマンドレットGet-STFStoreServiceを使用して、次の例のようにストアのユーザーサブスクリプションを構成することもできます:

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
    yourstore>"
Set-STFStoreService -StoreService $StoreObject -LockedDown $True -
    Confirm:$False
<!--NeedCopy-->
```

Citrix Virtual Apps and Desktops の構成

June 6, 2024

Citrix Virtual Apps and Desktops または Citrix Desktops as a Service でアプリケーションをユーザーに配信するときは、ストアの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。アプリケーションの配信について詳しくは、「アプリケーション」を参照してください。

- [**Application name**（**for user**）] フィールドに、ストアの Web サイト内に表示するアプリケーション名

を入力します。

- [**Description and keywords**] フィールドに、アプリの詳細を展開したときにストアの Web サイトの keywords の横に表示される説明を入力します。
- ユーザーが StoreFront Web サイト上のアプリケーションを視覚的に識別できるようにするには、**Application icon** を選択します。
- 必要に応じて、[**Application category**] フィールドにカテゴリを入力します。フォルダー階層を作成するには、カテゴリ名に\を含めます。たとえば、アプリケーションを種類ごとにグループ化したり、組織内のユーザーの役割ごとにフォルダーを作成したりすることができます。ストア Web サイトの [アプリ] タブの [カテゴリ] ビューには、カテゴリと各カテゴリのアプリの一覧が表示されます。

キーワード

アプリケーションの説明に文字列`KEYWORDS:[keywordname]`を追加することによってアプリやデスクトップにキーワードを追加できます。複数のキーワードを追加する場合は、`KEYWORDS:Accounts Featured`のようにスペースで区切ります。キーワードはさまざまな方法で使用できます:

- アプリケーションをフィルタリングする - 「ストアの詳細設定」を参照してください
- おすすめのアプリグループを作成する。
- 一部のキーワードには特別な意味があります。

キーワード名	説明
Mandatory（必須）	アプリケーションを [ホーム] タブに追加します。お気に入りとは異なり、必須のアプリケーションを [ホーム] タブから削除することはできません。ストアのお気に入りが無効になっている場合は効果がありません。
自動	ユーザーがストアにログオンすると、アプリケーションまたはデスクトップは自動的にお気に入りに登録され、[ホーム] タブに追加されます。そのようなアプリケーションをお気に入りから外すことができます。ストアのお気に入りが無効になっている場合は効果がありません。
TreatAsApp	デスクトップに適用すると、StoreFront がデスクトップをアプリとして扱うように強制されます。デスクトップは、[デスクトップ] タブではなく [アプリ] タブに表示されます。また、そのデスクトップはストアの Web サイトへのログオン時に自動起動せず、Desktop Viewer でアクセスできません。

キーワード名	説明
prefer=”*application*“	ここで、*application* はローカルにインストールされたアプリケーションを特定します。Windows 上の Citrix Workspace アプリにのみ適用されます。これは、ローカルにインストールされたアプリケーションのバージョンと、それに相当する配信されたインスタンスの両方が使用可能な場合に、ローカルにインストールされたアプリケーションが優先的に使用されることを意味します。詳しくは、「ローカルアプリアクセスのアプリケーションの構成」を参照してください。
Primary と **Secondary**	マルチサイト集計を使用する場合、キーワード **primary** が指定した要素が、キーワード **secondary** が指定されたものよりも常に優先されます。

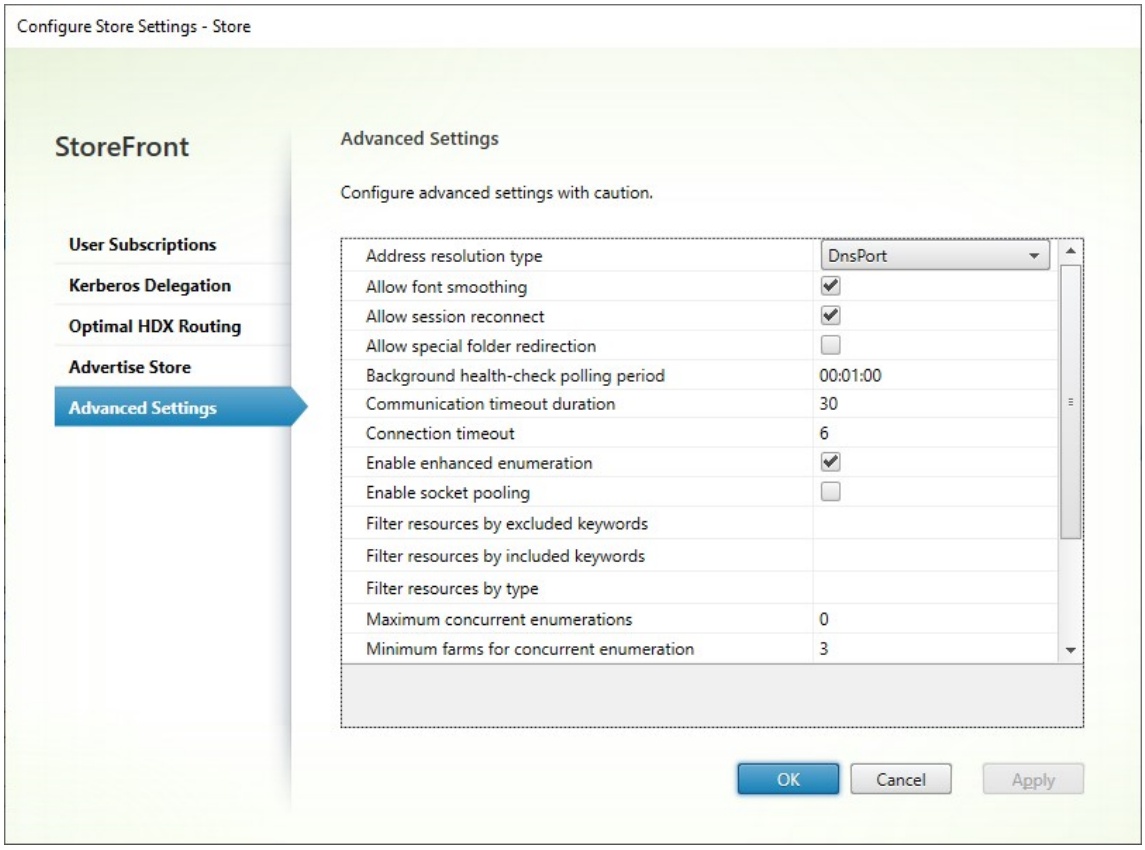
ストアの詳細設定

June 6, 2024

［ストア設定の構成］の［詳細設定］ページを使用して、ストアの詳細プロパティを構成できます。一部の設定は、PowerShell を使用してのみ変更できます。

> 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. 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、中央のペインでストアを選択して、［操作］ペインで ［ストア設定の構成］を選択します。
2. ［ストア設定の構成］ページで ［詳細設定］を選択して、必要な変更を加えます。



3. [**OK**] をクリックして変更を保存します。

アドレスの解決の種類

サーバーに要求するアドレスの種類を指定できます。デフォルトは［DnsPort］です。

［詳細設定］ウィンドウで、［アドレスの解決の種類］ドロップダウンリストから値を選択します。

- Dns
- DnsPort
- IPV4
- IPv4Port
- Dot
- DotPort
- Uri
- NoChange

フォントスムージングを許可する

HDX セッションでフォントスムージングを行うかどうかを指定できます。デフォルトは［オン］です。

［詳細設定］ウィンドウから、［フォントスムージングを許可する］オプションを選択し、［**OK**］をクリックします。

セッションの再接続を許可する

HDX セッションが再接続されるようにするかどうかを指定できます。デフォルトは［オン］です。

［詳細設定］ウィンドウから、［セッションの再接続を許可する］オプションを選択します。

特殊なフォルダーのリダイレクトを許可する

ユーザーフォルダーのリダイレクト機能により、サーバー上の Windows の特殊フォルダーがローカルコンピューター上のフォルダーにマップされます。ユーザーフォルダーという用語は、［ドキュメント］、［デスクトップ］など、ユーザー固有の Windows フォルダー（特殊フォルダー）を指すもので、Windows のバージョンが異なっていても同様のフォルダーが存在します。

［詳細設定］ウィンドウから、［特殊なフォルダーのリダイレクトを許可する］オプションを選択またはクリアして特殊なフォルダーのリダイレクトを有効または無効にし、［**OK**］をクリックします。

高度なヘルスチェック

StoreFront は、各 Citrix Virtual Apps and Desktops の Delivery Controller、Cloud Connector、および Secure Private Access で定期的にヘルスチェックを実行し、サーバーの可用性に対する断続的な影響を軽減させます。高度なヘルスチェックを使用すると、StoreFront はより詳細なチェックを実行するため、問題を検出する可能性が高くなります。

Cloud Connector 経由で Citrix Desktops as a Service（DaaS）に接続する場合、高度なヘルスチェックでは、Cloud Connector と同じ場所にある VDA に関する追加情報を取得できるというメリットもあります。Cloud Connector が Citrix DaaS に接続できない場合、Cloud Connector はローカルホストキャッシュを使用して、同じ場所に配置されている VDA に接続できるようにします。StoreFront は、高度なヘルスチェックによって得られた追加情報を使用して、アプリとデスクトップを起動するために最も適切なオンラインコネクタに接続します。

すべてのゾーン（リソースの場所）でリソースを公開することなく、停止中にリソースの可用性を確保するには、すべての StoreFront サーバーで、すべてのリソースの場所にすべての Cloud Connector が含まれるようにリソースフィードを構成し、高度なヘルスチェック機能を有効にしてください。

高度なヘルスチェックは、新しいストアでデフォルトで有効になっています。すべての StoreFront 展開で高度なヘルスチェックを有効にすることをお勧めします。高度なヘルスチェックを有効または無効にするには、パラメーター`AdvancedHealthCheck`を指定して PowerShell コマンドレットSet-STFStoreFarmConfigurationを使用します。

バックグラウンドヘルスチェックポーリング期間

StoreFront は、各 Citrix Virtual Apps and Desktops の Delivery Controller、Cloud Connector、および Secure Private Access で定期的にヘルスチェックを実行し、サーバーの可用性に対する断続的な影響を軽減させます。デフォルトは 1 分ごと（00:01:00）です。［詳細設定］ウィンドウから、［バックグラウンドヘルスチェックポーリング期間］の時間を指定し、［**OK**］をクリックしてヘルスチェックの頻度を制御します。高度なヘルスチェックが有効になっている場合、パフォーマンスに影響を与える可能性があるため、ポーリング期間を低い値に設定することはお勧めできません。

通信のタイムアウト期間

デフォルトでは、ストアにリソースを提供するサーバーへの StoreFront からの要求は、30 秒でタイムアウトします。通信の試行が 1 回失敗すると、サーバーが使用できないと見なされます。［詳細設定］ウィンドウから、デフォルトの時間に変更を行い、［**OK**］をクリックしてこれらの設定を変更します。

接続タイムアウト

Delivery Controller で最初の接続を確立するときに待機する秒数を指定できます。デフォルトは 6 です。

［詳細設定］ウィンドウから、最初の接続を確立するときに待機する秒数を指定し、［**OK**］をクリックします

拡張列挙を有効にする

このオプションでは、複数の Citrix Virtual Apps and Desktops サイトにわたってアプリやデスクトップを列挙する場合、StoreFront が Delivery Controller に対してクエリを同時に実行するか、連続して実行するかを制御できます。同時列挙は、複数サイト間のリソースを集約する場合に、ユーザーのクエリにより高速に応答できるいようにします。（デフォルトで）このオプションが選択されている場合、StoreFront はすべての Delivery Controller に同時に列挙要求を送信し、すべての応答を受信後に応答を集約します。［同時列挙の最大数］および ［同時列挙の最小ファーム数］オプションを使用して、この動作を調整できます。

［詳細設定］ウィンドウから、［拡張列挙を有効にする］オプションを選択（またはクリア）し、［**OK**］をクリックします。

ソケットプール機能を有効にする

ストアのソケットプール機能はデフォルトでは無効になっています。ソケットプール機能を有効にすると、StoreFront でソケットのプールが保持されます。これにより、必要になるたびにソケットを作成して接続が閉じたときにオペレーティングシステムに戻すという処理が不要になります。この機能を有効にすると、特に SSL（Secure Sockets Layer）接続でパフォーマンスが向上します。ソケットプール機能を有効にするには、ストアの構成ファイルを編集します。［詳細設定］ウィンドウから、［ソケットプール機能を有効にする］オプションを選択し、［**OK**］をクリックしてソケットプール機能を有効にします。

ファイルタイプの関連付け

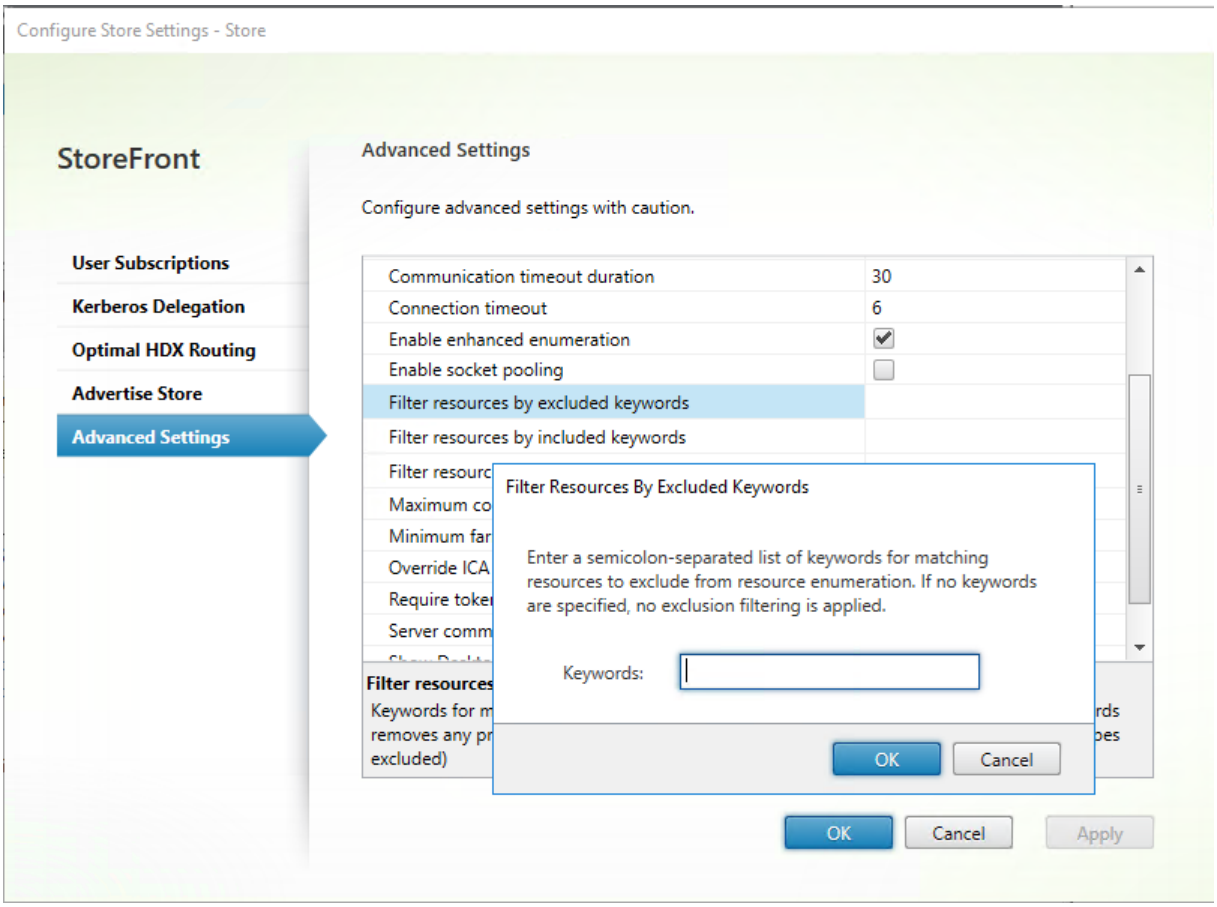
ストアのファイルタイプの関連付けは、デフォルトで有効になっています。このため、ユーザーがユーザーデバイス上で開いたローカルファイルは、サブスクライブ済みのアプリケーションで表示されます。ファイルタイプの関連付けの無効化を有効にするには、PowerShell コマンドSet-STFStoreFarmConfigurationを使用します。例:

```
$storeService = Get-STFStoreService  -VirtualPath '/Citrix/Store'
Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation
    $false
<!--NeedCopy-->
```

リソースを除外キーワードでフィルターする

一致するリソースを、除外キーワードでフィルターできます。除外キーワードを指定すると、それまで構成されていた包含キーワードは削除されます。既定値:［フィルターなし］(どのリソースの種類も除外されません)。

1. ［詳細設定］ウィンドウで、［リソースを除外キーワードでフィルターする］行を見つけます。
2. 右側の列をクリックして、［リソースを除外キーワードでフィルターする］ウィンドウを表示します。
3. キーワード入力ボックスにセミコロンで区切られたキーワードの一覧を入力します
4. ［**OK**］をクリックします。



PowerShell を使用して設定を変更するには、パラメーター `-FilterByKeywordsExclude`を指定してコマンドレットSet-STFStoreEnumerationOptionsを使用します。

以下のキーワードは予約されており、このフィルターで使用することはできません:

- 自動
- Mandatory（必須）

リソースを包含キーワードでフィルターする

一致するリソースを、包含キーワードでフィルターできます。包含キーワードを指定すると、それまで構成されていた除外キーワードは削除されます。既定値:［フィルターなし］（どのリソースの種類も除外されません）。

1. ［詳細設定］ウィンドウで、［リソースを包含キーワードでフィルターする］行を見つけます。
2. 右側の列をクリックして、［リソースを包含キーワードでフィルターする］ウィンドウを表示します。
3. キーワード入力ボックスにセミコロンで区切られたキーワードの一覧を入力します
4. ［**OK**］をクリックします。

PowerShell を使用して設定を変更するには、パラメーター `-FilterByKeywordsInclude`を指定してコマンドレットSet-STFStoreEnumerationOptionsを使用します。

以下のキーワードは予約されており、このフィルターで使用することはできません:

- 自動
- Mandatory（必須）

リソースを種類でフィルターする

リソースの列挙に含めるリソースの種類を選択します。既定値:［フィルターなし］（すべてのリソースの種類が含まれます）。

［詳細設定］ウィンドウから、［リソースを種類でフィルターする］を選択し、その右側をクリックして、列挙に含めるリソースの種類を選択し、［**OK**］をクリックします。

PowerShell を使用して設定を変更するには、パラメーター`-FilterByTypesInclude`を指定してコマンドレットSet-STFStoreEnumerationOptionsを使用し、リソースの種類（アプリケーション、デスクトップ、またはドキュメント）の配列を指定します。

同時列挙の最大数

すべての Delivery Controller に送信する同時要求の最大数を指定します。このオプションは、［拡張列挙を有効にする］オプションが有効になっている場合に機能します。デフォルト値は 0（制限なし）です。

［詳細設定］ウィンドウから、［同時列挙の最大数］を選択し、［**OK**］をクリックします。

同時列挙の最小ファーム数

同時列挙をトリガーするために必要な Delivery Controller の最小数を指定します。このオプションは、［拡張列挙を有効にする］オプションが有効になっている場合に機能します。デフォルトは 3 です。

［詳細設定］ウィンドウから、［同時列挙の最小ファーム数］を選択し、数値を入力してから ［**OK**］をクリックします。

ICA クライアント名を上書きする

.ica 起動ファイルのクライアント名設定を、Web ブラウザーで生成された一意の ID で上書きします。無効にすると、Citrix Workspace アプリによってクライアント名が指定されます。デフォルトは［オフ］です。

［詳細設定］ウィンドウから、［**ICA** クライアント名を上書きする］オプションを選択し、［**OK**］をクリックします。

トークンの一貫性を要求する

有効にすると、StoreFront によって、認証に使用されるゲートウェイとストア全体のゲートウェイとの整合性が強制されます。これらの値に不整合がある場合、ユーザーは再認証を行う必要があります。Smart Access ではこのオプションを有効にする必要があります。ユーザーが認証を無効にしてゲートウェイを介してストアにアクセスする場合は、このオプションを無効にする必要があります。デフォルトは［オン］です。

［詳細設定］ウィンドウから、［トークンの一貫性を要求する］オプションを選択し、［**OK**］をクリックします。

サーバー通信試行回数

Delivery Controller が利用不可とマークされるまでの、Delivery Controller との通信を試行する回数を指定します。デフォルトは 1 です。

［詳細設定］ウィンドウから、［サーバー通信試行回数］を選択し、数値を入力してから ［**OK**］をクリックします。

Desktop Viewer を有効にする

ユーザーが古いクライアントからデスクトップにアクセスする際に、Citrix Desktop Viewer ウィンドウおよびツールバーを表示するかどうかを指定します。デフォルトは［オフ］です。

［詳細設定］ウィンドウから、［古いクライアントで **Desktop Viewer** を表示する］オプションを選択し、［**OK**］をクリックします。

デスクトップをアプリとして扱う

ストアにアクセスしたときに、デスクトップをデスクトップ表示ではなくアプリ表示で表示するかどうかを指定します。デフォルトは［オフ］です。

［詳細設定］ウィンドウから、［デスクトップをアプリとして扱う］オプションを選択し、［**OK**］をクリックします。

ストアの最適な **HDX** ルーティングの構成

June 6, 2024

最適な Citrix Gateway ルーティングを構成して、HDX エンジンから StoreFront を使用して Citrix Virtual Apps and Desktops の公開アプリケーションにアクセスする ICA 接続の処理を最適化します。通常、サイトの最適なゲートウェイは、同じ地理的な場所に配置されます。

「最適な Citrix Gateway アプライアンス」は、ユーザーが StoreFront にアクセスするときに最適なゲートウェイが使用されない展開環境でのみ定義します。起動要求をその要求元のゲートウェイ経由で返送する必要がある場合、StoreFront がこれを自動的に行います。

ゲートウェイを特定の Delivery Controller またはゾーンにマッピングできます。ゾーンは Delivery Controller をグループ化したもので、通常は地理的な場所にある 1 つのデータセンターを表します。ゾーンは Citrix Virtual Apps and Desktops で定義され、StoreFront で定義されたゾーンは、Citrix Virtual Apps and Desktops で定義されたゾーン名と正確に一致する必要があります。1 つの最適なゲートウェイを複数のゾーンにマッピングすることができますが、通常は単一のゾーンを使用してください。一般に、ゾーンはある地理的な場所にある 1 つのデータセンターを表します。各ゾーンには少なくとも 1 つの最適な Citrix Gateway があり、その Citrix Gateway がそのゾーン内のリソースへの HDX 接続に使用されることが想定されます。

ゾーンについて詳しくは、「ゾーン」を参照してください。

ファーム使用のシナリオ例

1×UK ゲートウェイ -> 1×UK StoreFront

- UK アプリおよびデスクトップ（ローカル）
- US アプリおよびデスクトップ（UK ユーザーのフェールオーバーとして）

1×US ゲートウェイ -> 1×US StoreFront

- US アプリおよびデスクトップ（ローカル）
- UK アプリおよびデスクトップ（US ユーザーのフェールオーバーとして）

UK ゲートウェイは、UK の StoreFront を使用して、アプリやデスクトップなどの UK がホストするリソースへのリモートアクセスを提供します。

UK の StoreFront には、UK および US ベース両方の定義された Citrix Gateway と、Delivery Controller 一覧に UK および US Controller があります。UK のユーザーは、地理的に同じ場所に配置されたゲートウェイ、StoreFront、およびファームを使用してリモートリソースにアクセスします。UK のリソースが使用不能になった場合は、フェールオーバーとして一時的に US のリソースにアクセスできるようになります。

最適なゲートウェイルーティングがない場合、すべての ICA 起動は、リソースが地理的にどこに位置しているかにかかわらず、起動要求を行った UK ゲートウェイを経由します。デフォルトでは、起動要求時にその要求元のゲートウェイが StoreFront により動的に識別されます。最適なゲートウェイルーティング構成によりこの動作が無視され、US リソースへの接続が US ファームに地理的に近いゲートウェイを経由するようになります。

> 注:
>
> 最適なゲートウェイとしてマップできるのは、各サイトの StoreFront ストアについて 1 つのみです。

ゾーン使用のシナリオ例

1×CAMZone -> 2×UK StoreFront

- ケンブリッジ（UK）: アプリおよびデスクトップ
- フォートローダーデール（US 東部）: アプリおよびデスクトップ
- バンガロール（インド）: アプリおよびデスクトップ

1×FTLZone -> 2×US StoreFront

- フォートローダーデール（US 東部）: アプリおよびデスクトップ
- ケンブリッジ（UK）: アプリおよびデスクトップ
- バンガロール（インド）: アプリおよびデスクトップ

1×BGLZone -> 2×IN StoreFront

- バンガロール（インド）: アプリおよびデスクトップ
- ケンブリッジ（UK）: アプリおよびデスクトップ
- フォートローダーデール（US 東部）: アプリおよびデスクトップ

図 1: 最適ではないゲートウェイルーティング

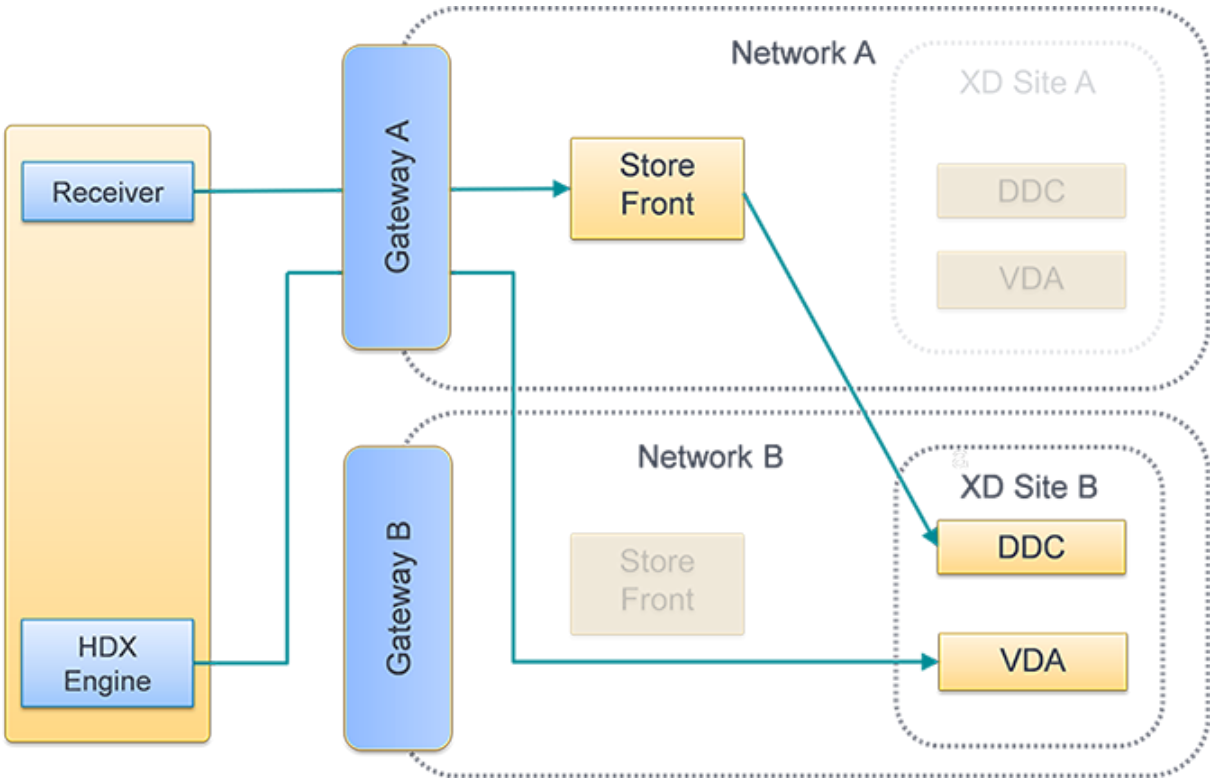
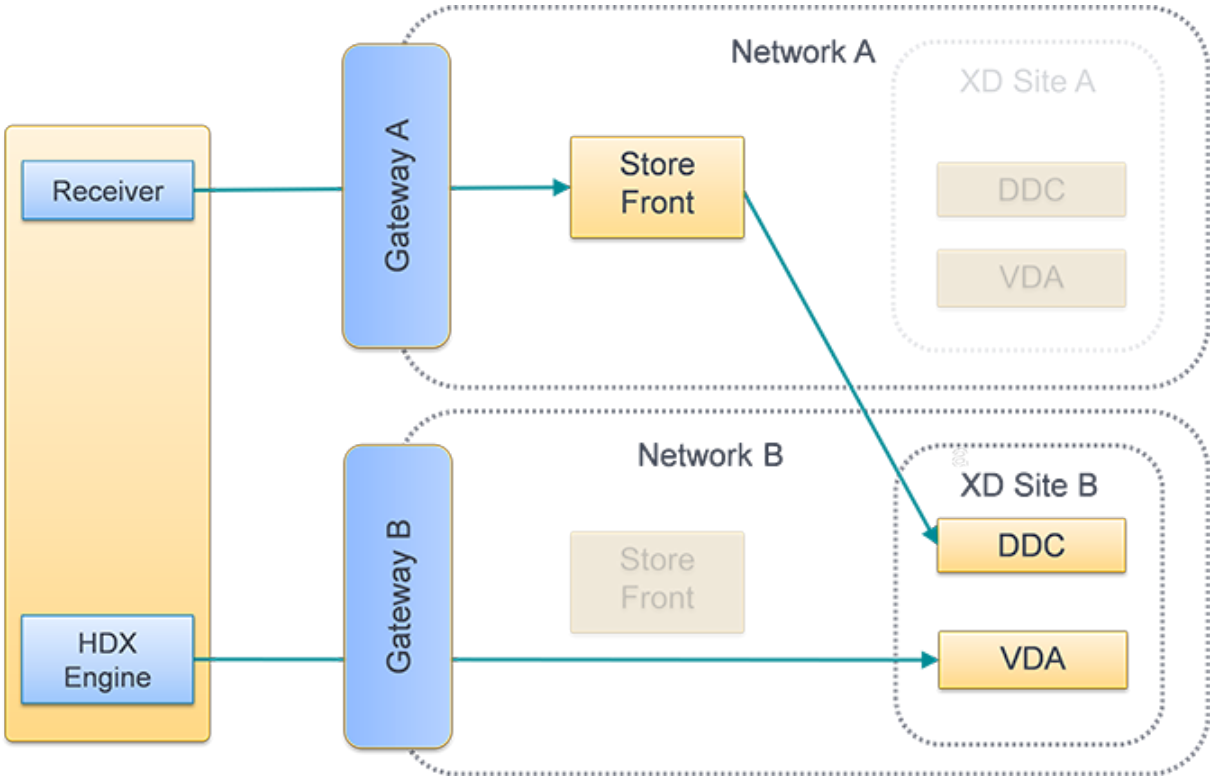


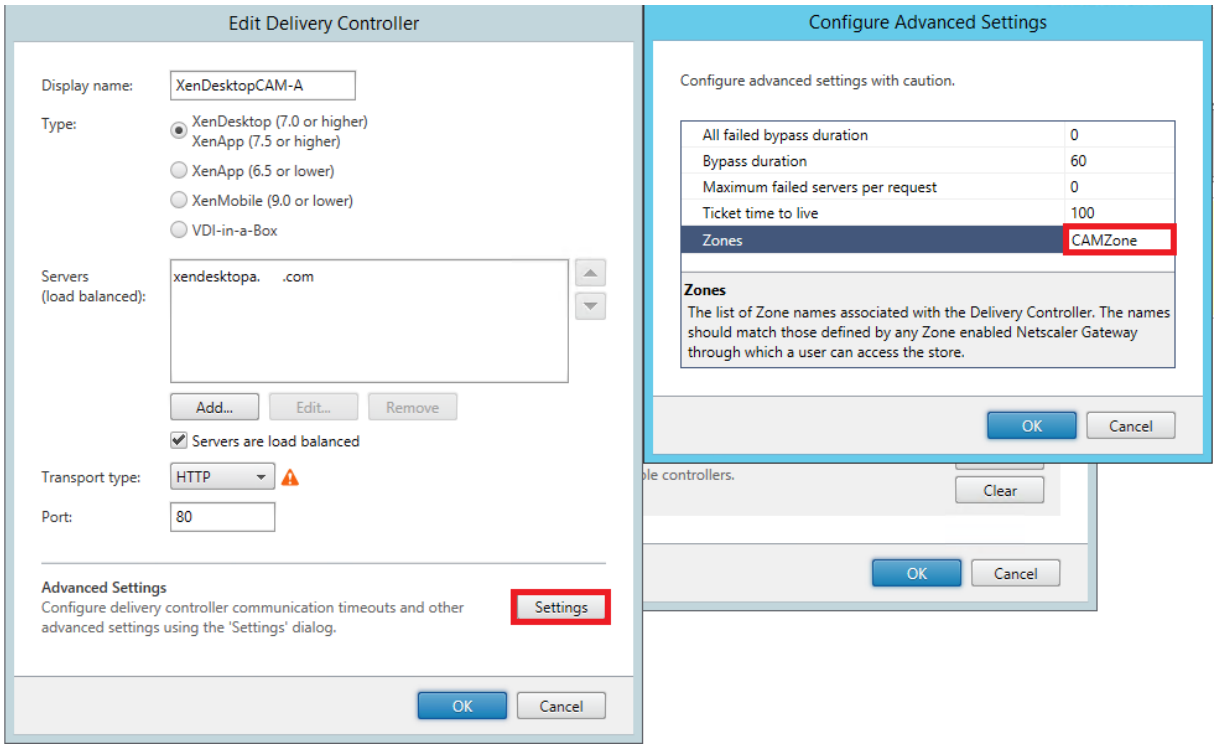
図 2：最適なゲートウェイルーティング



Delivery Controller のゾーンへの配置

ゾーン内に配置するすべての Delivery Controller に対して、ゾーン属性を設定します。

1. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ノードを選択して、［操作］ペインの ［**Delivery Controller** の管理］をクリックします。
2. コントローラーを選択して ［編集］をクリックし、［**Delivery Controller** の編集］画面で ［設定］をクリックします。
3. **Zones** 行で、2 番目の列をクリックします。
4. ［**Delivery Controller** ゾーン名］画面の ［追加］をクリックして、ゾーン名を追加します。



最適な **HDX** ルーティングの構成

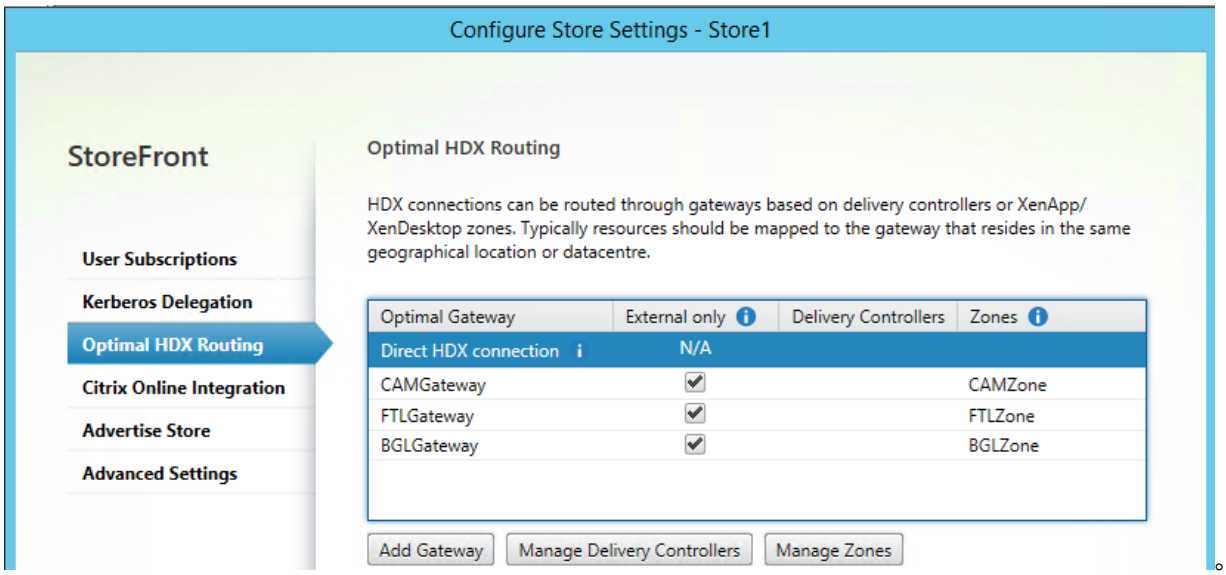
1. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインで、［ストア設定の構成］を選択します。
2. ［最適な **HDX** ルーティング］タブを選択します。
3. ゲートウェイを選択します。

    a) 特定の Delivery Controller からリソースにアクセスするときにゲートウェイを使用するには、［**Delivery Controller** の管理］をクリックして 1 つ以上の Delivery Controller にチェックを入れます。

    b) ゾーン内の Delivery Controller のグループからリソースにアクセスするときにゲートウェイを使用するには、［ゾーンの管理］をクリックして 1 つ以上のゾーンを入力します。

c) デフォルトでは、Delivery Controller またはゾーンを追加すると、[直接アクセス] にチェックが入ります。これは、ゲートウェイを経由して StoreFront に接続しているユーザーに対してのみ、StoreFront がゲートウェイを使用して StoreFront を起動することを意味します。ゲートウェイを経由することなく StoreFront に直接接続したユーザーのリソースを起動するためにもゲートウェイを使用したい場合は、［直接アクセス］のチェックを外します。

4. ユーザーがゲートウェイ経由で StoreFront にリモートアクセスする場合でも、ゲートウェイを使用せずに特定のリソースに常に直接接続したい場合は、［ゲートウェイを使用しない］を選択し、いくつかの Delivery Controller またはゾーンを選択します。



PowerShell を使用して最適な Citrix Gateway ルーティングを構成するには

- ストアに最適なゲートウェイルーティングを構成するには、Register-STFStoreOptimalLaunchGatewayを使用します。
- ストアに最適なゲートウェイルーティングを削除するには、Unregister-STFStoreOptimalLaunchGatewayを使用します。
- ストアに最適なルーティングを表示するには、Get-STFStoreRegisteredOptimalLaunchGatewayを使用します。

サブスクリプションの同期

June 6, 2024

StoreFront は、StoreFront サーバーグループ内のサーバー間でサブスクリプションを自動的に同期します。複数のサーバーグループがある（通常は地理的に異なる場所にある）場合、異なる StoreFront 環境内のストアからユーザーのサブスクリプションが定期的に同期されるように構成できます。これは PowerShell を使用して行う必要があります。

> 注:
>
> StoreFront 管理コンソールと PowerShell コンソールを同時に開くことはできません。StoreFront 管理コンソールを閉じてから PowerShell コンソールを開いてください。同様に、PowerShell のすべてのインスタンスを閉じてから StoreFront 管理コンソールを開いてください。

サブスクリプションの同期を確立するときは、同期するストア間で構成された Delivery Controller を同一の名前（大文字と小文字を区別）にする必要があります。Delivery Controller 名が異なると、同期サイト間で異なるサブスクリプションが使用される場合があります。集約されたリソースからサブスクリプションを同期する場合、両方のストアで使用されるアグリゲーショングループの名前も一致している必要があります。Delivery Controller 名とアグリゲーショングループ名では大文字と小文字が区別されます。たとえば、*CVAD_US* と *Cvad_Us* は異なります。

1. ローカル管理者権限を持つアカウントを使用して、Windows PowerShell ISE を起動します。
2. 同期を構成するには、Publish-STFServerGroupConfigurationコマンドを使用します。開始時刻と繰り返し間隔、または時刻の一覧を指定できます。たとえば、08:00 に同期を開始し、その後は 30 分ごとに同期する場合:

   ```
   1 Add-STFSubscriptionSynchronizationSchedule -RecurringStartTime
       08:00:00 -RecurringInterval 30
   2 <!--NeedCopy-->
   ```

   2 つのサーバーグループが互いにサブスクリプションデータを同時に取得しないように、プルスケジュールをずらすことをお勧めします。たとえば、各サーバーグループから 60 分ごとにデータを取得するスケジュールは、次のように構成されます。サーバーグループ 1 が、サーバーグループ 2 から 01:00、02:00、03:00 のようなスケジュールでデータを取得します。サーバーグループ 2 は、サーバーグループ 1 から 01:30、02:30、03:30 のようなスケジュールでデータを取得します。
3. 同期させるストアを含むリモート StoreFront 展開を指定するには、次のコマンドを入力します。StoreFront サーバーグループが存在するデータセンターごとにこれを構成して、他のリモートデータセンターからサブスクリプションデータを取得できるようにする必要があります。次の米国および英国のデータセンターの例を参照してください:

   - 米国データセンターの StoreFront サーバーで実行して、英国データセンターのサーバーからデータを取得します:

     ```
     1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
         Citrix/Store"
     2 Add-STFSubscriptionSynchronizationSource -FriendlyName "
         SyncFromUKStore" -StoreService $StoreObject -
         RemoteStoreFrontAddress "UKloadbalancedStoreFront.example.
         com"
     ```



```
3   <!--NeedCopy-->
```

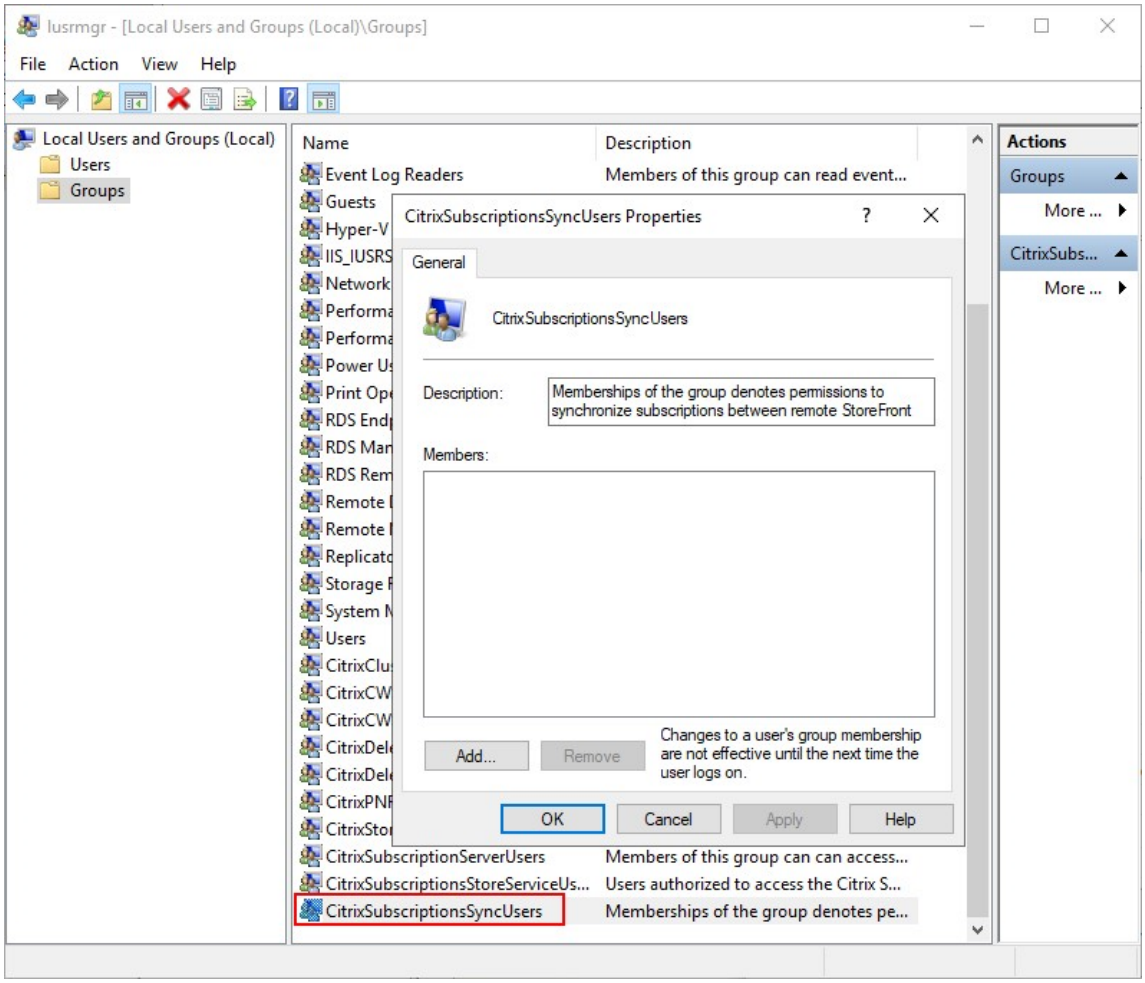
- 英国データセンターの StoreFront サーバーで実行して、米国データセンターのサーバーからデータを取得します:

```
1   $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
        Citrix/Store"
2   Add-STFSubscriptionSynchronizationSource -FriendlyName "
        SyncFromUSStore" -StoreService $StoreObject -
        RemoteStoreFrontAddress "USloadbalancedStoreFront.example.
        com"
3   <!--NeedCopy-->
```

ここで、*FriendlyName* はリモートの展開環境を識別するために定義する名前で、*RemoteStoreFrontAddress* は StoreFront サーバーまたは負荷分散サーバーグループの FQDN です。アプリケーションサブスクリプションを複数のストア間で同期するには、同期されるすべてのストアがそれぞれの StoreFront 展開環境で同じ名前を持つ必要があります。

4. 現在のサーバー上のローカル Windows ユーザーグループ CitrixSubscriptionSyncUsers に、リモート展開の各 StoreFront サーバーの Microsoft Active Directory ドメインマシンアカウントを追加します。

   これにより、同期スケジュールを構成すると、現在のサーバーは、CitrixSubscriptionSyncUsers に表示されているリモートサーバーから新規または更新されたサブスクリプションデータを取得できます。ローカルユーザーグループの変更については、https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524(v=ws.11)を参照してください。



5. 正常にスケジュールを構成した後、Citrix StoreFront 管理コンソールまたは以下の Powershell を使用して、サブスクリプション同期スケジュールとソースをグループ内の他のすべてのサーバーに反映します。

```
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

複数サーバーで構成される StoreFront 展開環境への変更の適用について詳しくは、「サーバーグループの構成」を参照してください。

6. 既存のサブスクリプション同期スケジュールを削除するには、次のコマンドを入力し、展開環境のほかの StoreFront サーバーに構成の変更を反映させます。

```
Clear-STFSubscriptionSynchronizationSchedule
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

7. 特定のサブスクリプション同期ソースを削除するには、次のコマンドを実行し、展開環境のほかの StoreFront サーバーに構成の変更を反映させます。

```
Remove-STFSubscriptionSynchronizationSource -FriendlyName "
    SyncFromUKStore"
```



```
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

8. すべての既存のサブスクリプション同期ソースを削除するには、次のコマンドを入力し、展開環境のほかの StoreFront サーバーに構成の変更を反映させます。

```
Clear-STFSubscriptionSynchronizationSource
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

9. StoreFront 展開用に現在構成されているサブスクリプション同期スケジュールを一覧表示するには、次のコマンドを実行します。

```
Get-STFSubscriptionSynchronizationSchedule
<!--NeedCopy-->
```

10. StoreFront 展開用に現在構成されているサブスクリプション同期ソースを一覧表示するには、次のコマンドを実行します。

```
Get-STFSubscriptionSynchronizationSource
<!--NeedCopy-->
```

セッション設定の構成

June 6, 2024

ユーザーがアプリケーションを起動すると、StoreFront は、Citrix Workspace アプリがそのセッションを起動して構成するために必要なすべての設定を含むドキュメント（ica ファイルと呼ばれます）を生成します。

通常は、Citrix Virtual Apps and Desktops ポリシーまたはCitrix DaaS ポリシーを使用してセッション設定を変更することをお勧めします。ただし、場合によっては、特定のストアのこれらの設定を上書きすることも可能です。これは、ストアが複数のサイトからリソースを集約しており、そのストアのすべてのリソースに同じ設定を適用したい場合に便利です。

ストアのセッション設定を定義するには、次のいずれかを実行します:

- Global App Config Service を使用します。これは Citrix Cloud 上のサービスです。詳しくは、「Global App Configuration Service を使用した Citrix Workspace アプリの構成」を参照してください。
- StoreFront サーバーで、ストアの default.ica ファイルに設定を追加します。

StoreFront サーバーの default.ica ファイルは`\inetpub\wwwroot\Citrix\[StoreName]\App_Data`ディレクトリにあります。

利用可能な設定の一覧については、「ICA 設定リファレンス」を参照してください。一部の設定はグローバルに適用されます。Studio で構成したアプリケーション名と完全に一致する名前のセクションを追加することで、特定のアプリに適用するセクションを追加することもできます。

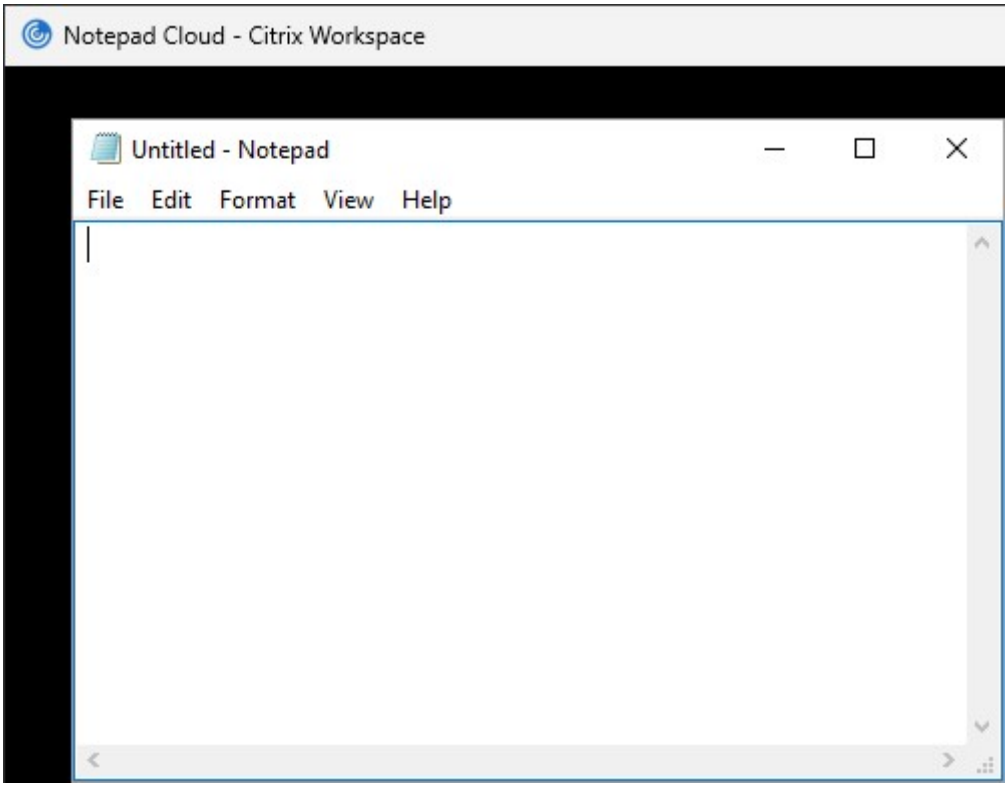
例：メモ帳をウィンドウモードで起動する

ウィンドウモードで起動するようにアプリケーションを構成するには、default.ica に次の設定を含むアプリケーションのセクションを追加します：

- TWIMode - ウィンドウモードを有効にするには、Off に設定します。
- DesiredHRES - 水平方向のピクセル数（オプション）。
- DesiredVRES - 垂直方向のピクセル数（オプション）。

例：

```
[Notepad]
TWIMode=Off
DesiredHRES=1024
DesiredVRES=768
<!--NeedCopy-->
```



ICA ファイルの署名

June 6, 2024

StoreFront には、ICA ファイルにデジタル署名を追加するオプションが用意されています。これにより、この機能をサポートするバージョンの Citrix Workspace アプリで、ICA ファイルが信頼されるサーバーからのものであるこ

とを検証できるようになります。StoreFront でファイルの署名を有効にすると、ユーザーがアプリケーションを起動するときに生成される ICA ファイルが、StoreFront サーバーの個人証明書ストアにある証明書を使用して署名されます。StoreFront サーバーのオペレーティングシステムでサポートされる任意のハッシュアルゴリズムを使って ICA ファイルを署名できます。クライアントソフトウェアがこの機能をサポートしない場合や ICA ファイルの署名用に構成されていない場合、デジタル署名は無視されます。署名処理に失敗した場合は、デジタル署名なしで ICA ファイルが生成され、Citrix Workspace アプリに送信されます。未署名のファイルを受け入れるかどうかは、Receiver 側での構成により決定されます。

StoreFront の ICA ファイルの署名機能で使用する証明書には秘密キーが含まれ、許可された有効期間内である必要があります。証明書にキー使用法の拡張が含まれる場合、キーをデジタル署名に使用できるようにする必要があります。拡張キー使用法エクステンションが含まれる場合は、コード署名またはサーバー認証用に設定されている必要があります。

ICA ファイルを署名する場合、商用の証明機関または組織内の独自の証明機関から取得したコード署名または SSL 署名証明書を使用することをお勧めします。証明機関から適切な証明書を取得できない場合は、サーバー証明書のような既存の SSL 証明書を使用するか、新しいルート証明機関証明書を作成してユーザーデバイスに配布することができます。

ストアの ICA ファイルの署名機能はデフォルトでは無効になっています。ICA ファイルの署名機能を有効にするには、ストアの構成ファイルを編集してから Windows PowerShell コマンドを実行します。Windows 向け Citrix Workspace アプリで ICA ファイル署名を有効にする方法の詳細については、「ICA ファイル署名」を参照してください。

> 注:
>
> StoreFront 管理コンソールと PowerShell コンソールを同時に開くことはできません。StoreFront 管理コンソールを閉じてから PowerShell コンソールを開いてください。同様に、PowerShell のすべてのインスタンスを閉じてから StoreFront 管理コンソールを開いてください。

1. ICA ファイルの署名に使用する証明書が、現在のユーザーの証明書ストアではなく、StoreFront サーバーの Citrix Delivery Services 証明書ストアで使用できることを確認します。
2. `Set-STFStoreService`PowerShell コマンドレットを使用して署名を有効にします。

```
$storeService = Get-STFStoreService
Set-STFStoreService $storeService -IcaFileSigning $true -
    IcaFileSigningCertificateThumbprint [certificatethumbprint]
<!--NeedCopy-->
```

   ここで **[certificatethumbprint]** は、ハッシュアルゴリズムにより生成される証明書データのダイジェスト（または拇印）です。

   SHA-1 以外のハッシュアルゴリズムを使用する場合は、必要に応じて sha256、sha384、または sha512 に設定された**-IcaFileSigningHashAlgorithm** パラメーターを追加します。

Citrix Workspace アプリの構成

June 6, 2024

Global App Config Service

Global App Config Service は、Citrix Workspace アプリ構成を管理するためのクラウドサービスです。Citrix Cloud アカウント内で、ストア URL を要求し、各ストアの構成を定義できます。詳しくは、「オンプレミスストアの設定の構成」を参照してください。

ストアアカウント設定

Global App Config Service の代わりに、ストアアカウント設定を通じて Citrix Workspace アプリを構成できます。ユーザーがローカルにインストールされた Citrix Workspace アプリにストアを追加すると、ストアアカウント設定 StoreFront が取得されます。これには、Windows 向け Citrix Workspace アプリにアプリのスタートメニューショートカットを作成するかどうかを指示するなどの構成プロパティを含めることができます。プロパティの詳細については、Workspace アプリのドキュメントの「アプリショートカットをカスタマイズするための StoreFront アカウント設定の使用」などを参照してください。

これらの設定を変更するには、以下の手順を実行します:

1. C:\inetpub\wwwroot\Citrix\Roamingで web.config ファイルを開きます。
2. <Accounts>セクションで、変更するストアの要素<account ... name="Store"... >を見つけます。
3. Accountセクションで、<annotatedServices>/<annotatedServiceRecord>/<metadata>/<properties>セクションを見つけます。
4. <clear/>要素の後に、<property name="[name]"value="[value]"/>の形式でプロパティを追加します。例:

```
<properties>
    <clear/>
    <property name="PutShortcutsOnDesktop" value="true"/>
    <property name="DesktopDir" value="Citrix Applications"/>
</properties>
<!--NeedCopy-->
```

> 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。

Workspace アプリの Web サイト

ローカルにインストールされた Citrix Workspace アプリでどの Web サイト構成が使用されるかを構成するには、「Workspace アプリの Web サイトを構成する」を参照してください。

Web サイトの管理

June 6, 2024

ストアごとに、ユーザーが Web ブラウザーまたは Citrix Workspace アプリを介してアクセスできる、1 つ以上の Web サイトを構成できます。

StoreFront 管理コンソールを使って、次のタスクを実行します:

タスク	詳細
Web サイトの作成	ユーザーが Web ページまたは Workspace アプリを介してストアにアクセスできるようになる、Web サイトを作成します。
Web サイトの構成	Web サイトの設定を変更します。
Web サイトの削除	Citrix Receiver for Web サイトの削除
Workspace アプリの Web サイトを構成する	Citrix Workspace アプリ内から使用する Web サイトを選択します。

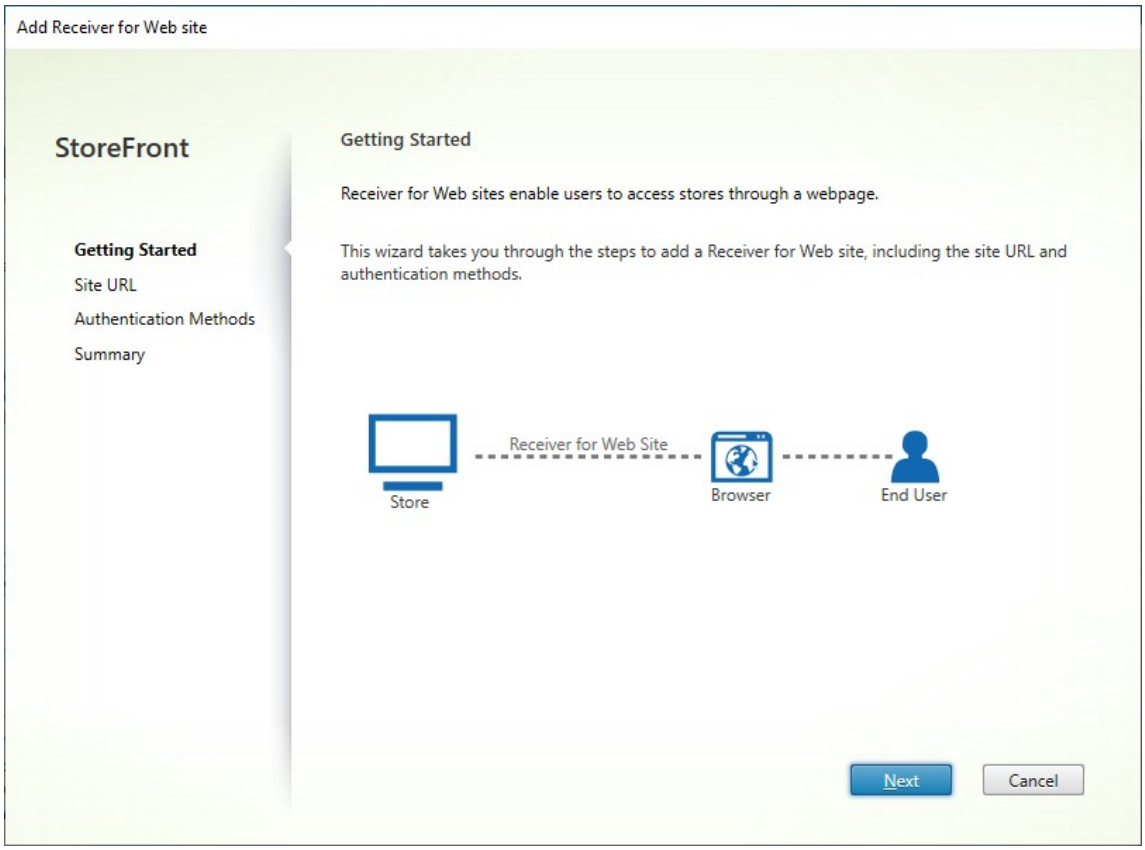
Web サイトの作成

June 6, 2024

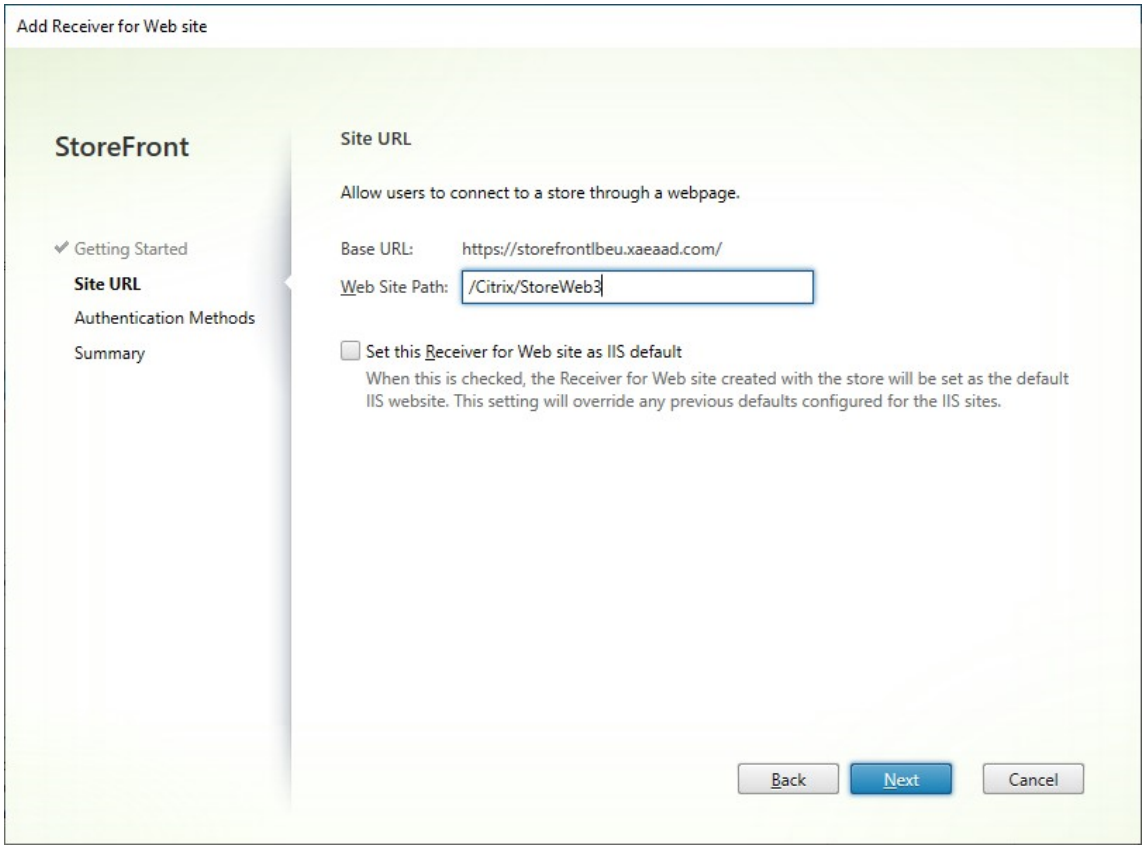
ストアを作成すると、そのストアの Web サイトが自動的に作成されます。既存のストアに Web サイトを追加できます。これにより、構成が異なる別の URL をユーザーに提供することができます。ただし、Citrix Workspace アプリはストアについて 1 つの特定の Web サイトを使用するように構成されています。このため、複数の Web サイトへのアクセスは Web ブラウザーを介してのみ行うことができます。詳しくは、「Workspace アプリの Web サイトの構成」を参照してください。

> 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。

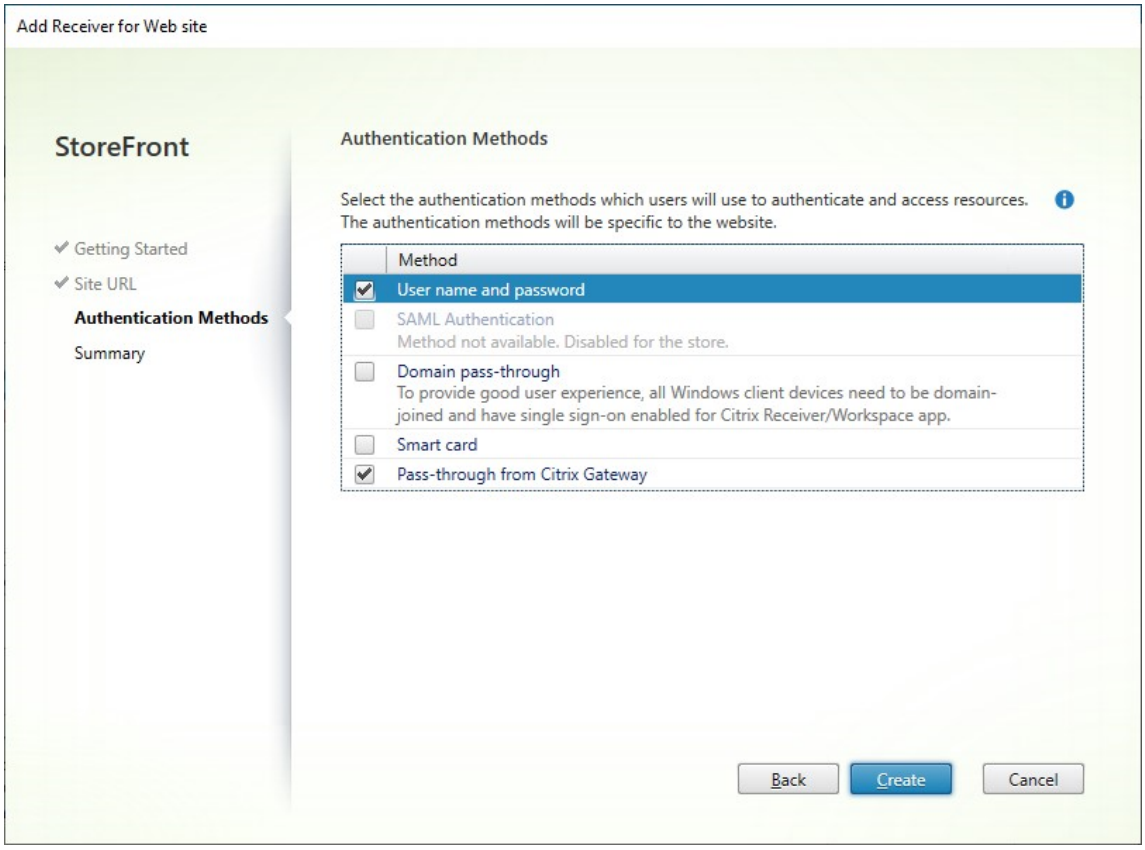
1. 管理コンソールから、Web サイトを作成するストアを選択し、［操作］ペインの ［**Receiver for Web** サイトの管理］をクリックします。
2. ［追加］をクリックし、［次へ］をクリックします。



3. 目的の **Web** サイトのパスを入力し、これをベース URL のデフォルトの Web サイトにするかどうかを選択して、［次へ］をクリックします。



4. 希望する認証方法にチェックを入れるか、チェックを外します。一部の方法は、ストア用に構成されている場合にのみ使用できます。［次へ］を押します。



5. サイトが作成されたら、［完了］をクリックします。
6. 新しく作成したサイトを選択し、［編集］を押して必要に応じて Web サイトを構成します。「Web サイトの構成」を参照してください。

PowerShell SDK を使用して Web サイトを作成する

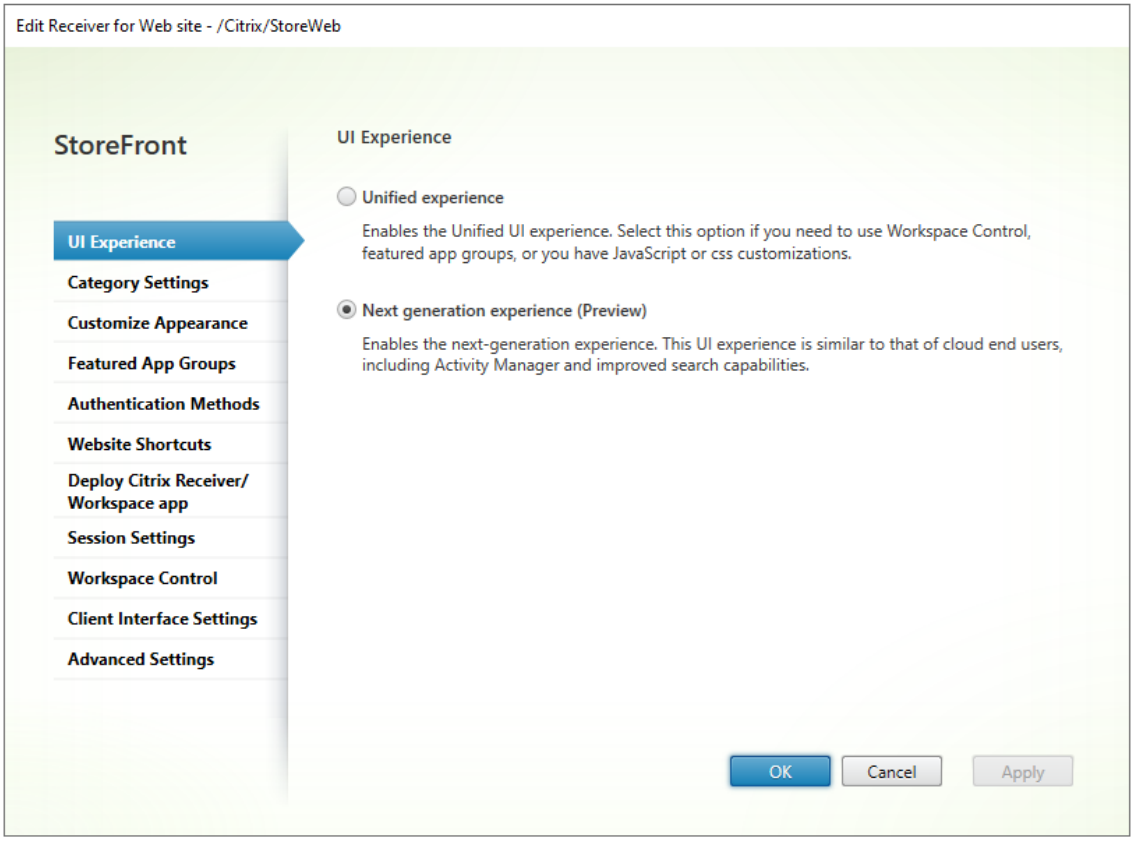
PowerShell SDKを使用して Web サイトを作成するには、Add-STFWebReceiverServiceコマンドレットを呼び出します。

Web サイトの構成

June 6, 2024

Web サイトを構成するには、以下の手順を実行します:

1. 左ペインで ［ストア］ノードを選択して、［操作］ペインで ［**Receiver for Web** の管理］をクリックします。
2. Web サイトを選択し、**[**設定…**]** を押します。



3. 適切なタブで設定を変更します。

   - UI エクスペリエンス
   - カテゴリ設定
   - 外観のカスタマイズ
   - おすすめアプリのグループ
   - 認証方法
   - Web サイトのショートカット
   - Citrix Receiver/Workspace アプリの展開
   - セッションの設定
   - ワークスペースコントロール
   - クライアントインターフェイスの設定
   - 詳細設定

4. 変更が完了したら、[**OK**] をクリックします。

5. App Protectionを構成するには、PowerShell を使用する必要があります。PowerShell コマンドを実行する前に、StoreFront 管理コンソールを閉じる必要があります。

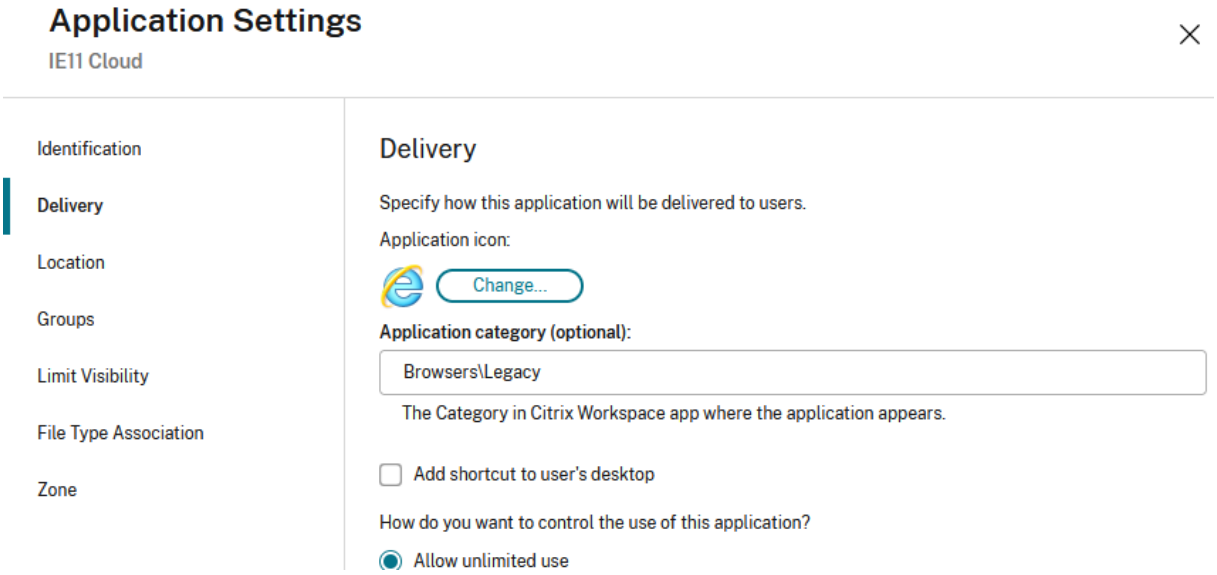
> 重要:
>
> 複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでくださ

> 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。

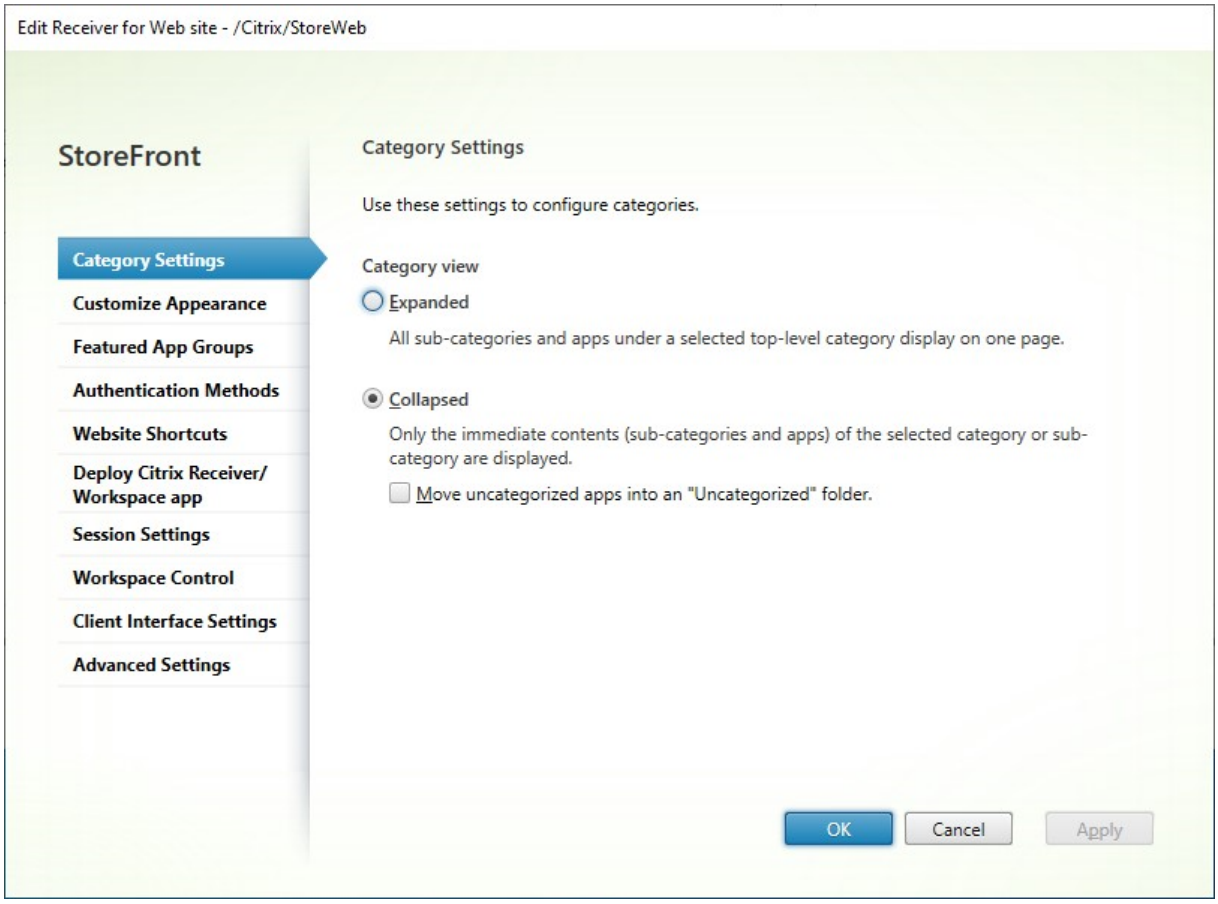
カテゴリ設定

June 6, 2024

「アプリケーション」の記事で説明されているように、Citrix Virtual Apps and Desktops 内で各アプリケーションをカテゴリに割り当てることができます。カテゴリのフォルダー階層を作成するには、\記号を使用します。StoreFront 内で、このフォルダー階層の表示方法を構成できます。



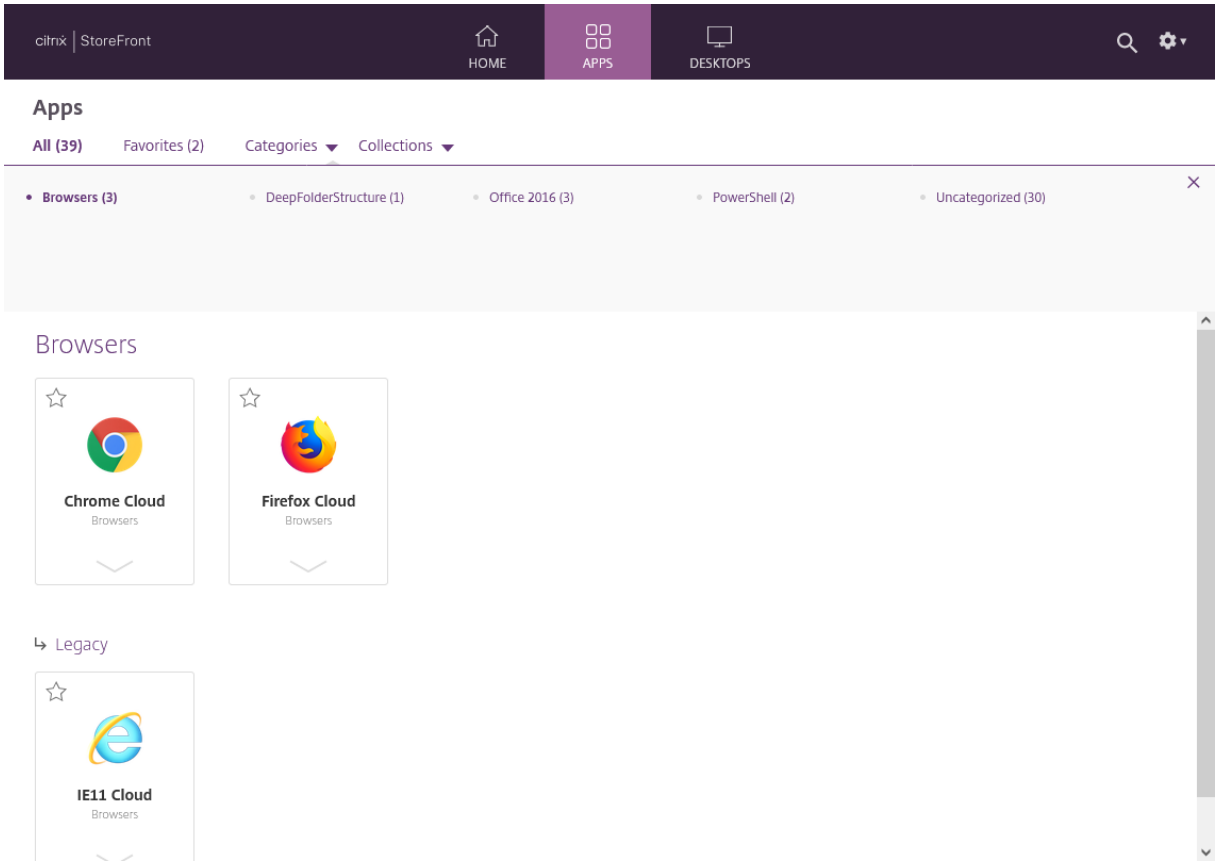
カテゴリ設定を変更するには、［Receiver for Web サイトの編集］に移動し、［カテゴリ設定］タブを選択します。



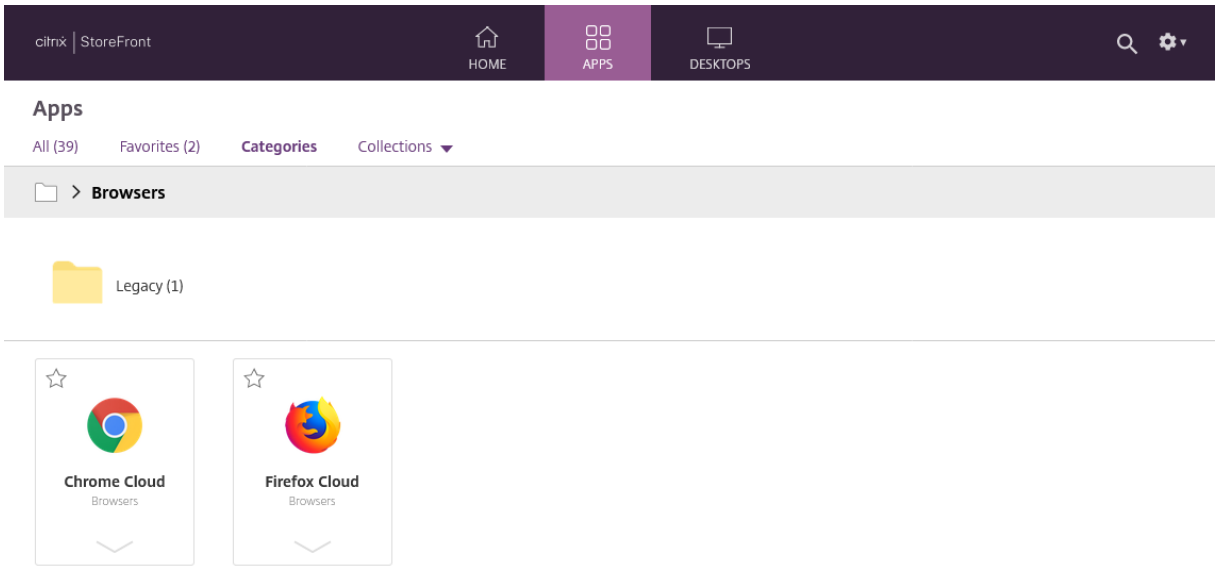
カテゴリの表示

展開されたビューでは、StoreFront にトップレベルのカテゴリの一覧が表示されます。ユーザーがトップレベルのカテゴリをクリックすると、StoreFront はすべてのサブカテゴリのすべてのアプリを 1 ページに表示します。

たとえば、サブカテゴリ「Legacy」を持つカテゴリ「Browser」がある場合、「Legacy」の下にあるブラウザーを含むすべてのブラウザーが 1 ページに表示されます:

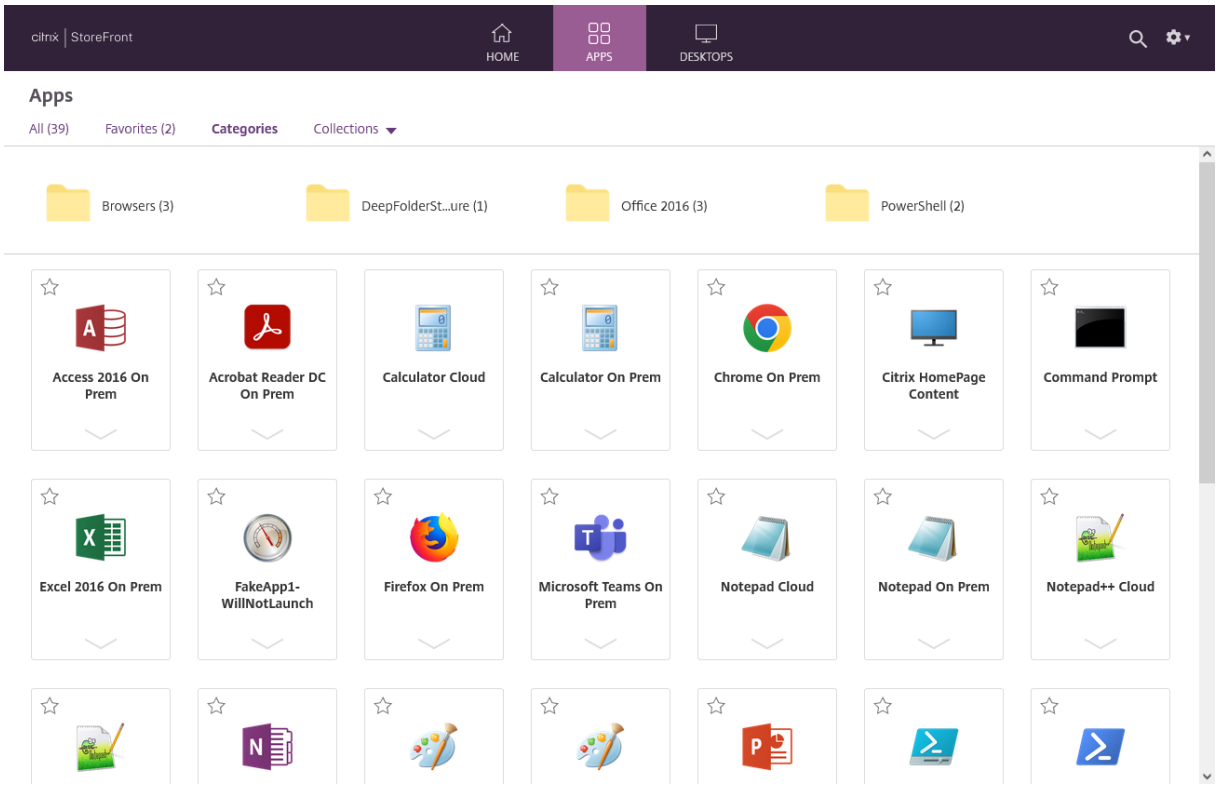


折りたたまれたビューでは、StoreFront は最初にトップレベルのカテゴリの一覧を表示し、オプションですべての未分類のアプリを表示します。ユーザーがカテゴリをクリックすると、StoreFront は選択したカテゴリの直近のコンテンツ（サブカテゴリとアプリ）のみを表示します。ユーザーは各サブカテゴリをクリックしてコンテンツを展開できます。

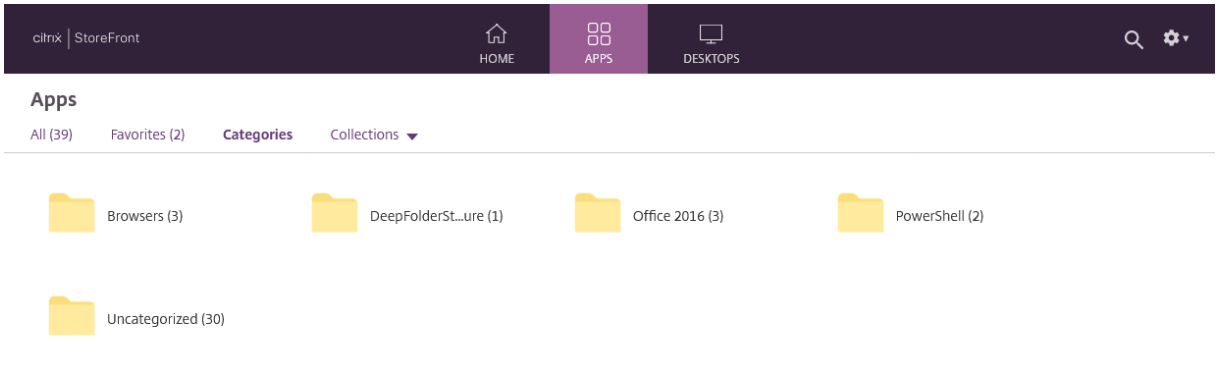


未分類のアプリ

折りたたまれたビューで、[未分類のアプリを「未分類」フォルダーに移動する] オプションをオフにすると、最初のビューにカテゴリのないすべてのアプリとデスクトップが表示されます。この動作は、StoreFront の以前のバージョンと似ています。



折りたたまれたビューで、[未分類のアプリを「未分類」フォルダーに移動する] をオンにすると、カテゴリのないすべてのアプリとデスクトップが別の「未分類」フォルダーに移動します。



PowerShell SDK を使用してカテゴリ設定を構成する

PowerShell SDK を使用してカテゴリビューを有効または無効にするには、パラメーター`EnableAppsFolderView`を指定してコマンドレットSet-STFWebReceiverUserInterfaceを呼び出します。

PowerShell SDK を使用してカテゴリビューを変更するには、パラメーター`CategoryViewCollapsed`を指定してコマンドレットSet-STFWebReceiverUserInterfaceを呼び出します。

外観のカスタマイズ

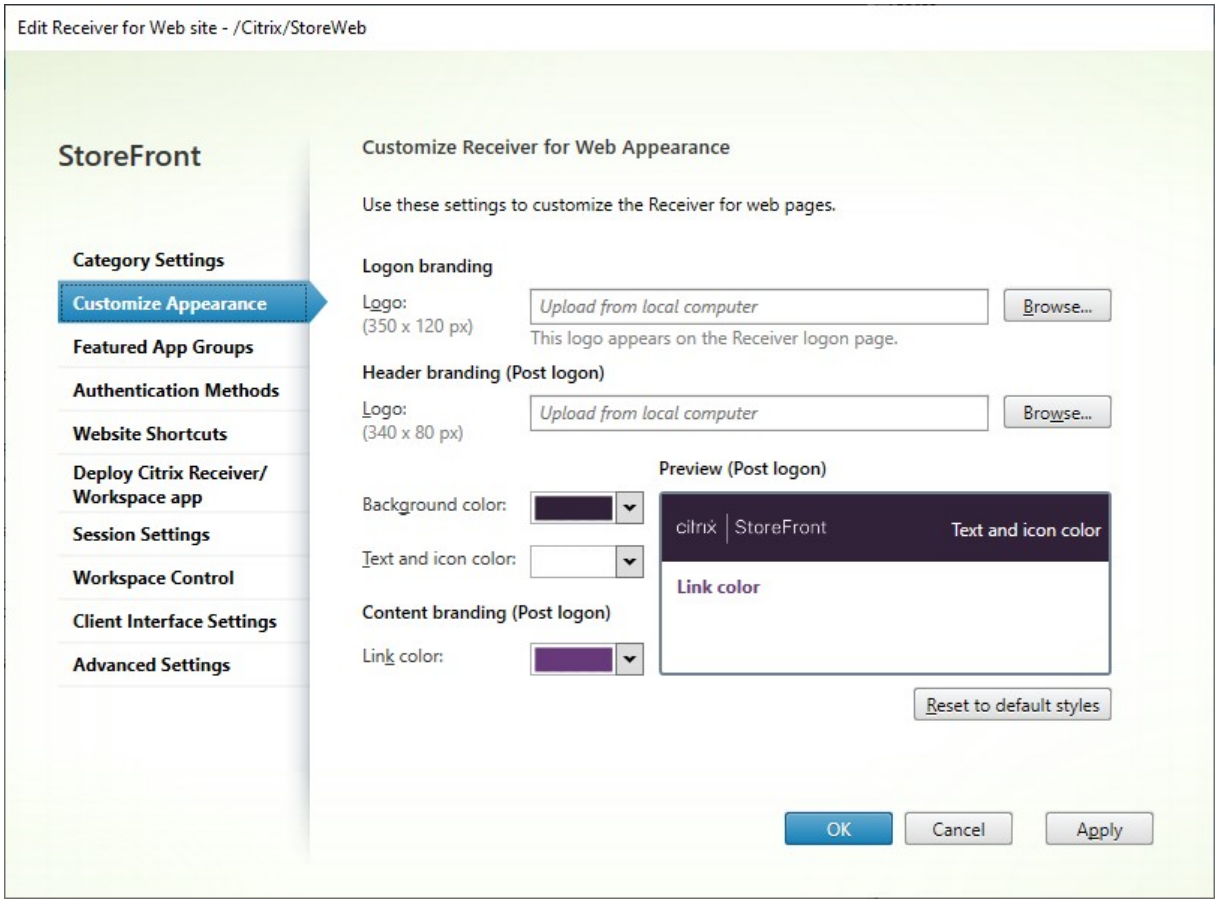
June 6, 2024

ストアの Web サイト内で使用されるロゴと色を変更できます。

ロゴと色の編集

外観をカスタマイズするには、［Receiver for Web サイトの編集］に移動し、［外観のカスタマイズ］タブを選択します。以下を変更できます:

- ログオンブランドロゴ - ログオン画面に表示されるロゴ。Citrix Gateway 経由でログオンする場合は表示されません。［参照…］を押して、.jpg、.jpeg、.png、.png、または.bmp タイプのファイルを選択します。350px x 120px のサイズの画像を使用することをお勧めします。
- ヘッダーブランドロゴ。ログオン後の左上隅に表示されるロゴ。［参照…］を押して、.jpg、.jpeg、.png、.png、または.bmp タイプのファイルを選択します。340px x 80px のサイズの画像を使用することをお勧めします。
- 背景色 - ページ上部のナビゲーションセクションの背景色。
- テキストとアイコンの色 - ページ上部のナビゲーションセクションのテキストとアイコンの色。
- リンクの色 - 現在選択されているアイテムを強調表示するために使用される色。



PowerShell SDK を使用してロゴと色を編集する

PowerShell SDKを使用して、コマンドレットSet-STFWebReceiverSiteStyleを呼び出します。

外観をデフォルトにリセットする

ロゴと色をデフォルトに戻すには、［デフォルトスタイルにリセット］を押します。

PowerShell SDK を使用して外観をデフォルトにリセットする

PowerShell SDKを使用して、コマンドレットClear-STFWebReceiverSiteStyleを呼び出します。

JavaScript と **CSS** による追加のカスタマイズ

StoreFront クライアント UI カスタマイズ APIを使用して、Web サイトをさらにカスタマイズできます。

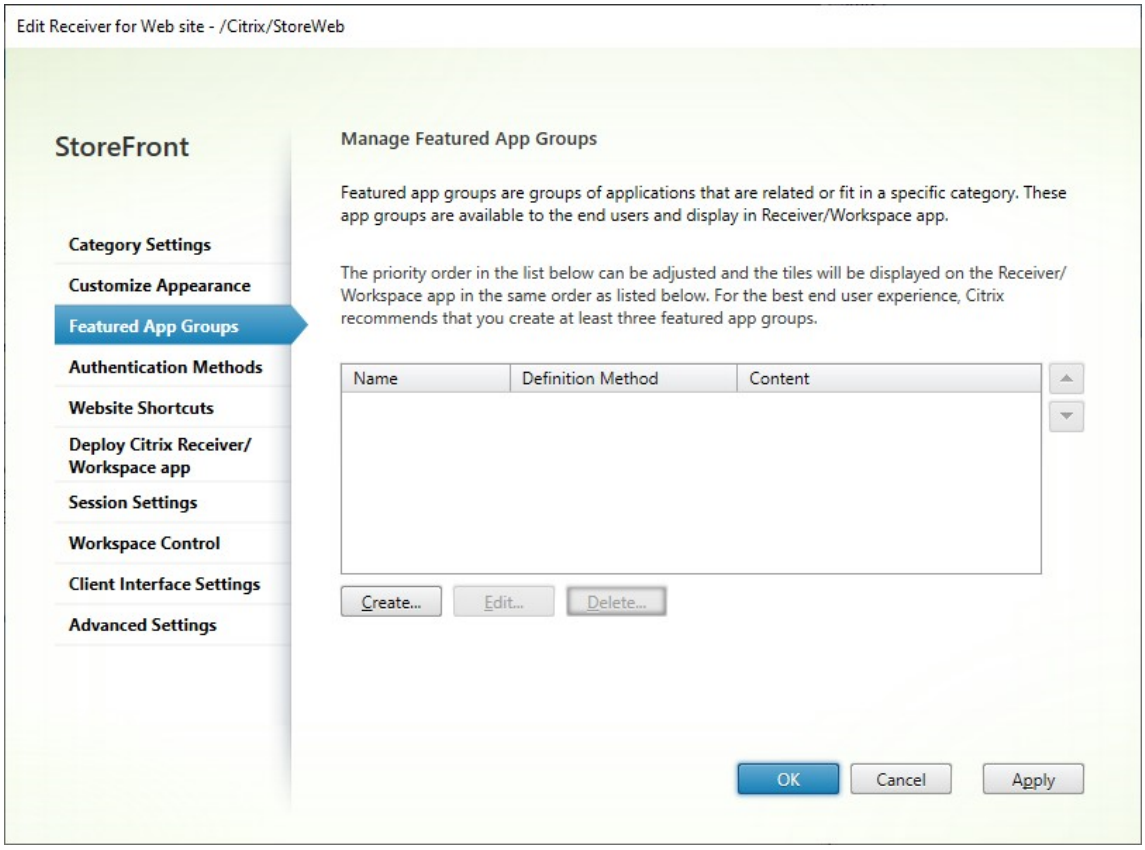
おすすめアプリのグループ

June 6, 2024

特定のカテゴリに関連するまたはそれと適合するエンドユーザーに対するお勧めのアプリケーショングループを作成できます。たとえば、営業部により使用されるアプリケーションを含む、営業部にお勧めのアプリケーショングループを作成できます。アプリケーション名を使ったり、Studio コンソールで定義されたキーワードまたはアプリケーションカテゴリを使ったりして、StoreFront 管理コンソールでお勧めのアプリケーションを定義できます。

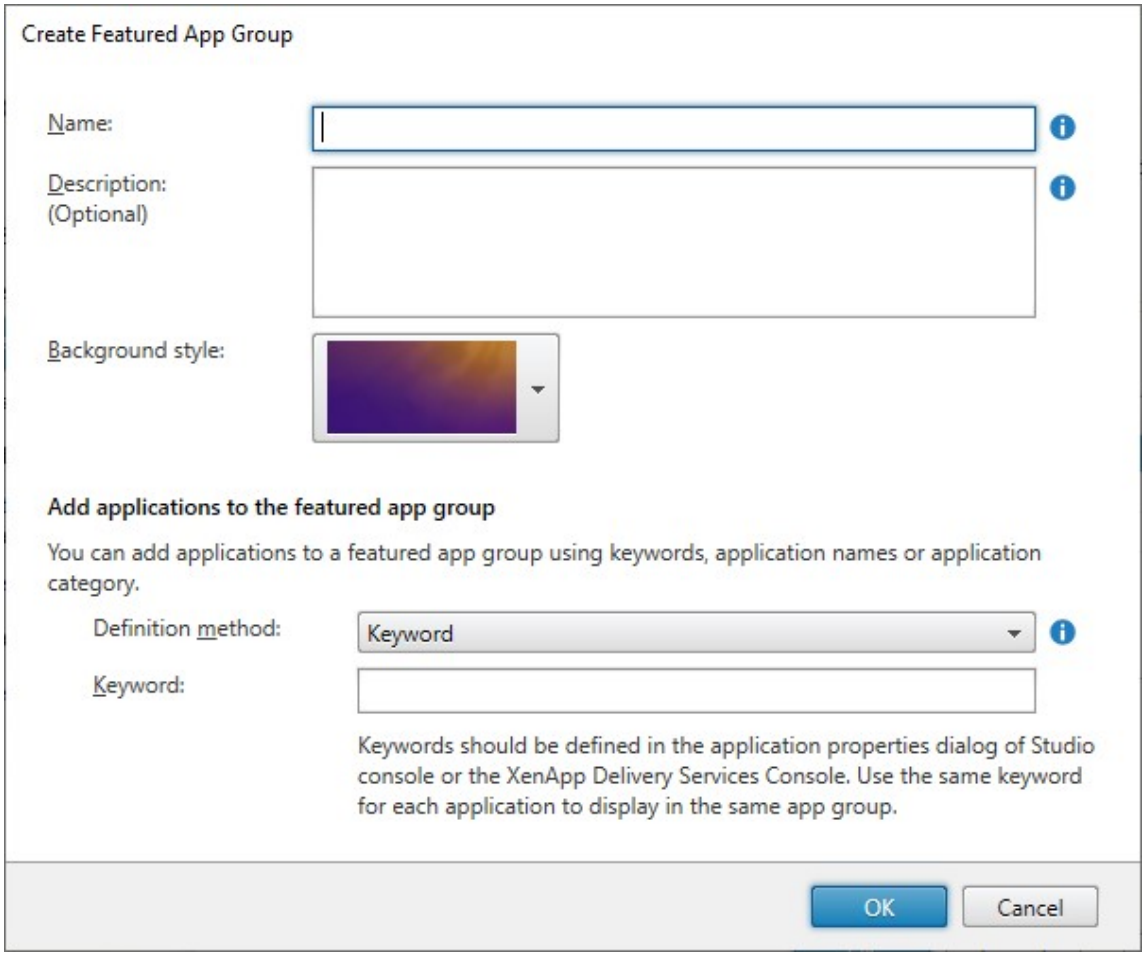
お勧めのアプリケーショングループの作成

1. ［Receiver for Web サイトの編集］ 画面で、［お勧めのアプリケーショングループ］タブを選択します。



2. ［作成］をクリックして、お勧めのアプリケーショングループを定義します。
3. お勧めのアプリケーショングループ名、説明（任意）、背景、およびお勧めのアプリケーショングループを定義する方法を指定します。キーワード、アプリケーション名、またはアプリケーションカテゴリを選択します。

オプション	説明
キーワード	アプリの説明にキーワードを含めることによって、Studio で定義されたキーワードに基づいてアプリを照合します。例:「電子メールの送受信に使用 KEYWORDS:collaboration」
アプリケーションカテゴリ	Studio に入力された特定のアプリケーションカテゴリのアプリを照合します。
アプリケーション名	アプリケーション名を使ってお勧めのアプリケーショングループを定義します。[お勧めのアプリケーショングループの作成] ダイアログボックスのここに含まれている名前と一致するすべてのアプリケーション名は、お勧めのアプリケーショングループに含まれます。StoreFront はアプリケーション名でワイルドカードをサポートしません。一致する内容では大文字と小文字は区別されませんが、全体が一致する必要があります。たとえば、「Excel」と入力すると、StoreFront では公開アプリケーション名の Microsoft Excel 2013 が一致となりますが、「Exc」と入力しても一致するものはありません。

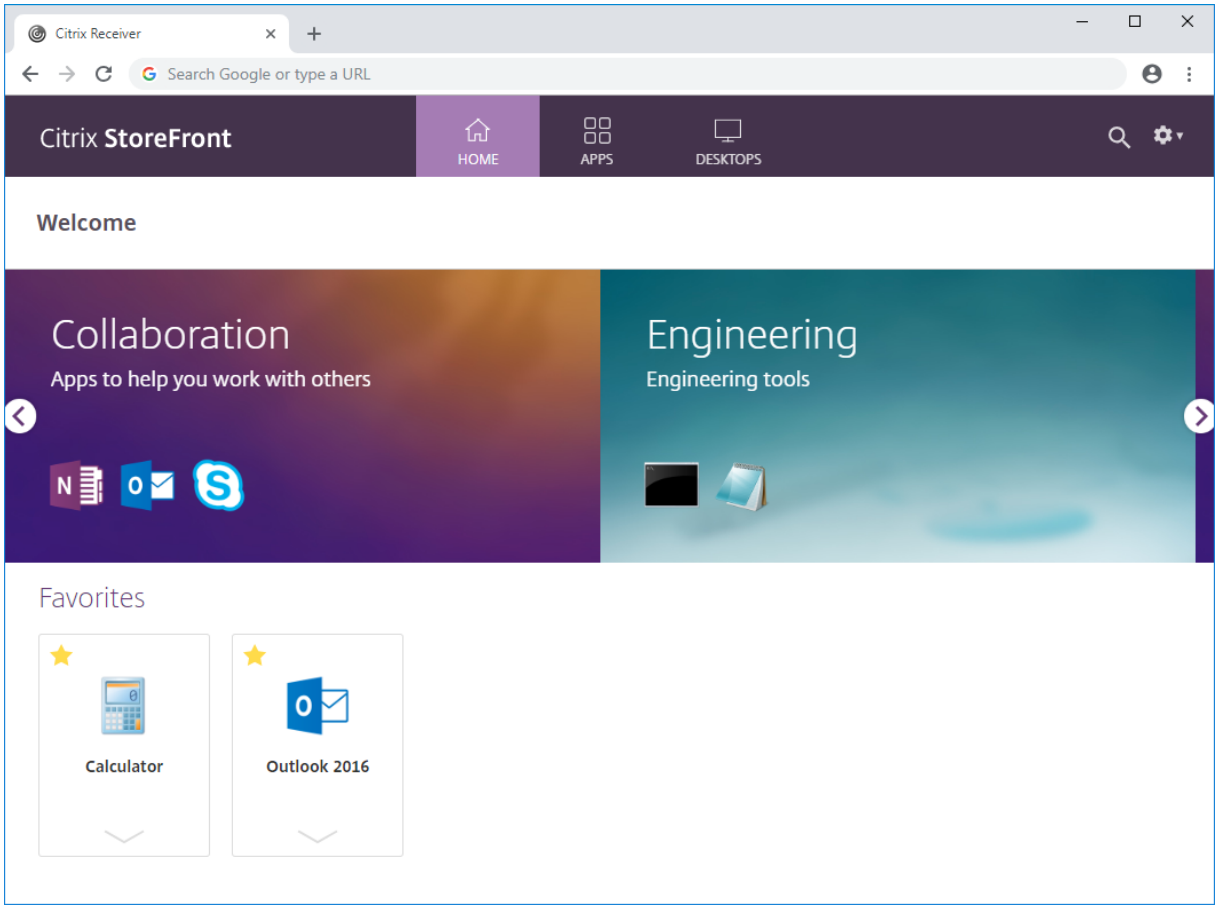


4. [**OK**] をクリックします。

例:

2 つのお勧めのアプリケーショングループを作成しました:

- コラボレーション - Studio の **Collaboration** カテゴリに含まれるアプリケーションとの一致を指定することによって作成しました。
- 開発 - アプリケーショングループに名前を付けて、アプリケーション名のコレクションを指定することによって作成しました。



PowerShell SDK を使用してお勧めのアプリケーショングループを作成する

PowerShell SDKを使用してお勧めのアプリケーショングループを追加するには、コマンドレットNew-STFWebReceiverFeaturedAppGroupを使用します。

お勧めのアプリケーショングループの編集

［Receiver for Web サイトの編集］ 画面で、［お勧めのアプリケーショングループ］タブを選択します。編集するグループを選択して、［編集…］をクリックします

PowerShell SDK を使用してお勧めのアプリケーショングループを編集する

PowerShell SDKを使用してお勧めのアプリケーショングループを変更するには、コマンドレットSet-STFWebReceiverFeaturedAppGroupを使用します。

お勧めのアプリケーショングループの削除

［Receiver for Web サイトの編集］ 画面で、［お勧めのアプリケーショングループ］タブを選択します。削除するグループを選択して、［削除…］をクリックします

PowerShell SDK を使用してお勧めのアプリケーショングループを削除する

PowerShell SDKを使用してお勧めのアプリケーショングループを削除するには、コマンドレットRemove-STFWebReceiverFeaturedAppGroupを使用します。すべてのお勧めのアプリケーショングループを削除するには、コマンドレットClear-STFWebReceiverFeaturedAppGroupを使用します。

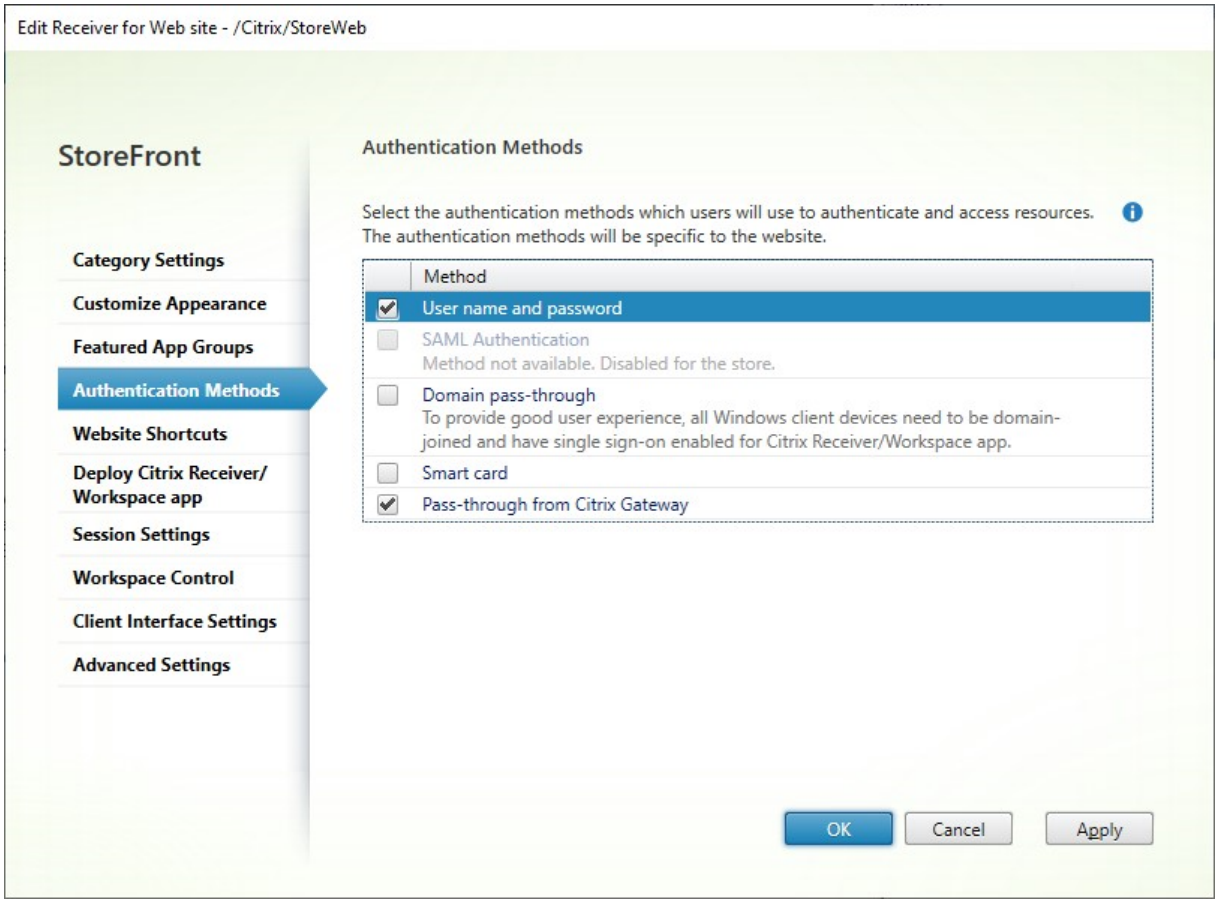
認証方法

June 6, 2024

ストアで使用可能な認証方法を構成するには、「認証の構成」を参照してください。特定の Web サイトのこれらの設定の一部を上書きできます。これらの上書きは、Web ブラウザー経由で HTML5 向け Citrix Workspace アプリを使用する場合にのみ適用されます。ローカルにインストールされた Citrix Workspace アプリは、Web サイトではなくストアの設定を使用します。

> 警告:
> ストアの認証方法を変更すると、そのストアのすべての Web サイトの設定が常に上書きされるため、変更を再適用する必要があります。

認証方法を変更するには、 ［Receiver for Web サイトの編集］ に移動し、［認証方法］タブを選択します。



- 指定ユーザー認証を有効にするには ［ユーザー名とパスワード］チェックボックスをオンにします。「ユーザー名とパスワード認証」を参照してください。このオプションは、ストアで有効になっている場合にのみ使用できます。
- SAML ID プロバイダーとの統合を有効にするには、［**SAML** 認証］チェックボックスをオンにします。「SAML 認証」を参照してください。このオプションは、ストアで有効になっている場合にのみ使用できます。
- ユーザーデバイスから Active Directory ドメイン資格情報がパススルーされるようにするには、［ドメインパススルー］をオンにします。「ドメインパススルー認証」を参照してください。このオプションは、ストアで有効になっている場合にのみ使用できます。
- スマートカード認証を有効にするには、［スマートカード］をオンにします。「スマートカード認証」を参照してください。
- Citrix Gateway からのパススルー認証を有効にするには、［**Citrix Gateway** からのパススルー］をオンにします。認証を有効化した Citrix Gateway 経由でユーザーが StoreFront に接続する場合は、これを有効にします。「Citrix Gateway からのパススルー」を参照してください。

PowerShell SDK を使用して構成する

PowerShell SDKを使用して利用可能な認証方法を構成するには、コマンドレットSet-STFWebReceiverAuthenticationMethod
使用します。

Web サイトのショートカット

June 6, 2024

内部ネットワーク上でホストされている信頼できる Web サイトからデスクトップやアプリケーションにすばやくアクセスできるようにするには、Web サイトのショートカットを使用します。Citrix Receiver for Web サイトで配信するリソースの URL を生成して、これらのリンクを Web サイトに埋め込みます。ユーザーがリンクをクリックすると、Receiver for Web サイトにリダイレクトされます。ここで、ユーザーが Receiver for Web サイトにログオンしていない場合はログオンします。Receiver for Web サイトでは、リソースが自動的に起動します。ユーザーがサブスクライブしていないアプリケーションの場合は、自動的にサブスクライブされます。

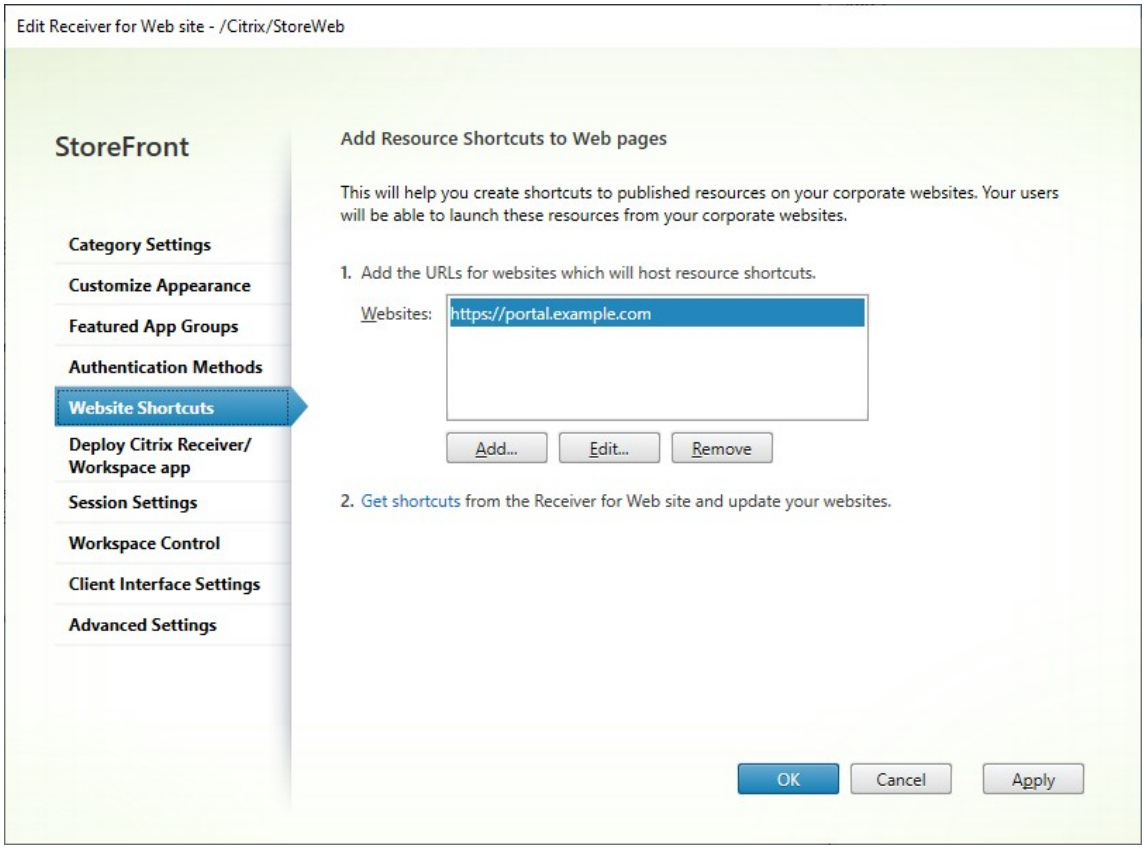
リソースのショートカットを生成する前に、Citrix StoreFront 管理コンソールまたは PowerShell を使用して、ホスト Web サイトの URL を「信頼できる *URL*」一覧に追加する必要があります。

デフォルトでは、信頼できない Web サイトからのリソースショートカットを起動しようとするユーザーに警告が StoreFront により表示されますが、ユーザーは引き続きリソースの起動を選択できます。これらの警告が表示されないようにするには、［ストア］ペインで ［**Receiver for Web** サイトの管理］をクリックし、**** ［構成］**** で［詳細設定］を選択して、**** ［信頼できないショートカットについてメッセージを表示する］** オプションをオフにします。

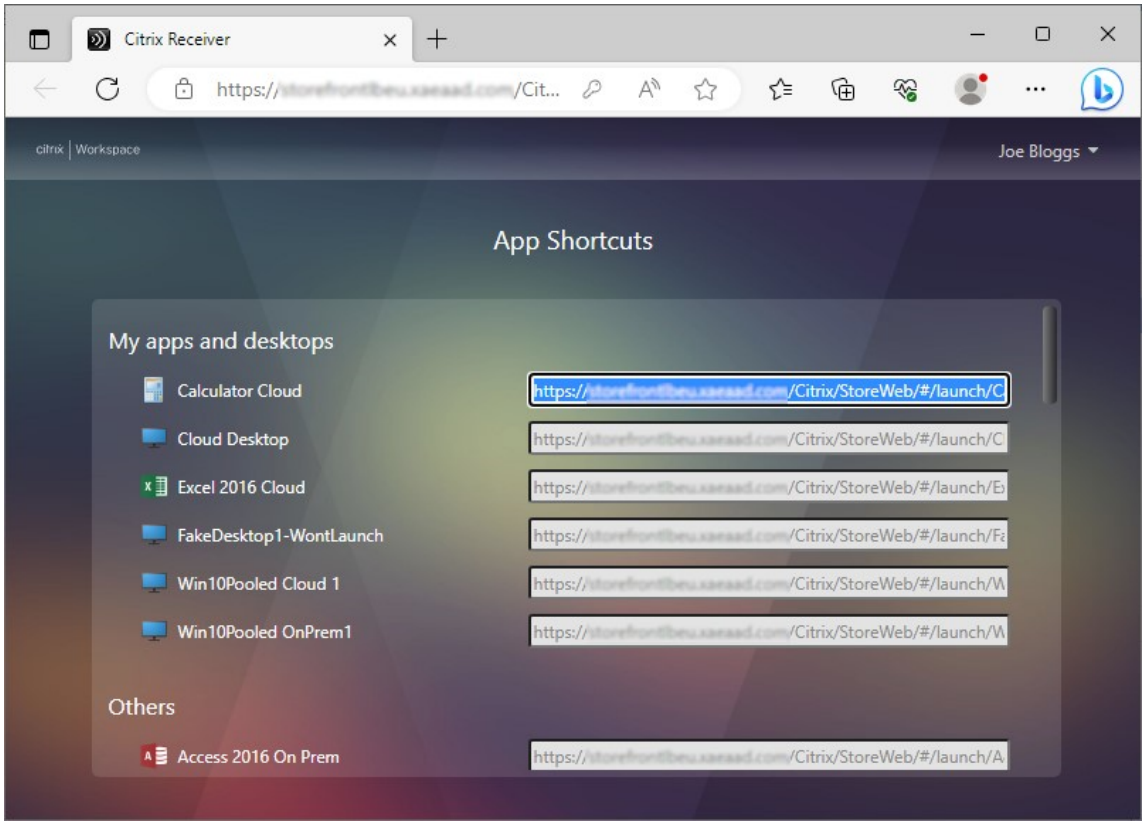
セキュリティ上の理由により、Internet Explorer ユーザーには、ショートカット経由でアクセスしたリソースの起動を確認するメッセージが表示される場合があります。このメッセージが表示されなくなるようにするには、Internet Explorer の［ローカルイントラネット］または［信頼済みサイト］のゾーンに StoreFront サーバーの FQDN を追加するようユーザーに指示します。

管理コンソールを使用して信頼できる **Web** サイトを追加する

1. ［Receiver for Web サイトの編集］ 画面で、［**Web** サイトのショートカット］タブを選択します。



2. ［追加］をクリックして、ショートカットをホストしようとする Web サイトの URL を入力します。URL は、*http[s]://hostname[:port]* の形式で指定する必要があります。ここで、<hostname> は Web サイトホストの完全修飾ドメイン名です。<port> は使用できないプロトコルのデフォルトポートのホストとの通信に使用するポートです。Web サイトの特定のページへのパスを指定する必要はありません。URL を変更するには、［Web サイト］の一覧でエントリを選択して ［編集］をクリックします。Citrix Receiver for Web サイトのリソースへのショートカットを削除するには、一覧で Web サイトを選択して、［削除］をクリックします。
3. ［ショートカットを取得］をクリックし、Web サイトに必要な URL をコピーします。



PowerShell SDK を使用して信頼できる **Web** サイトを追加する

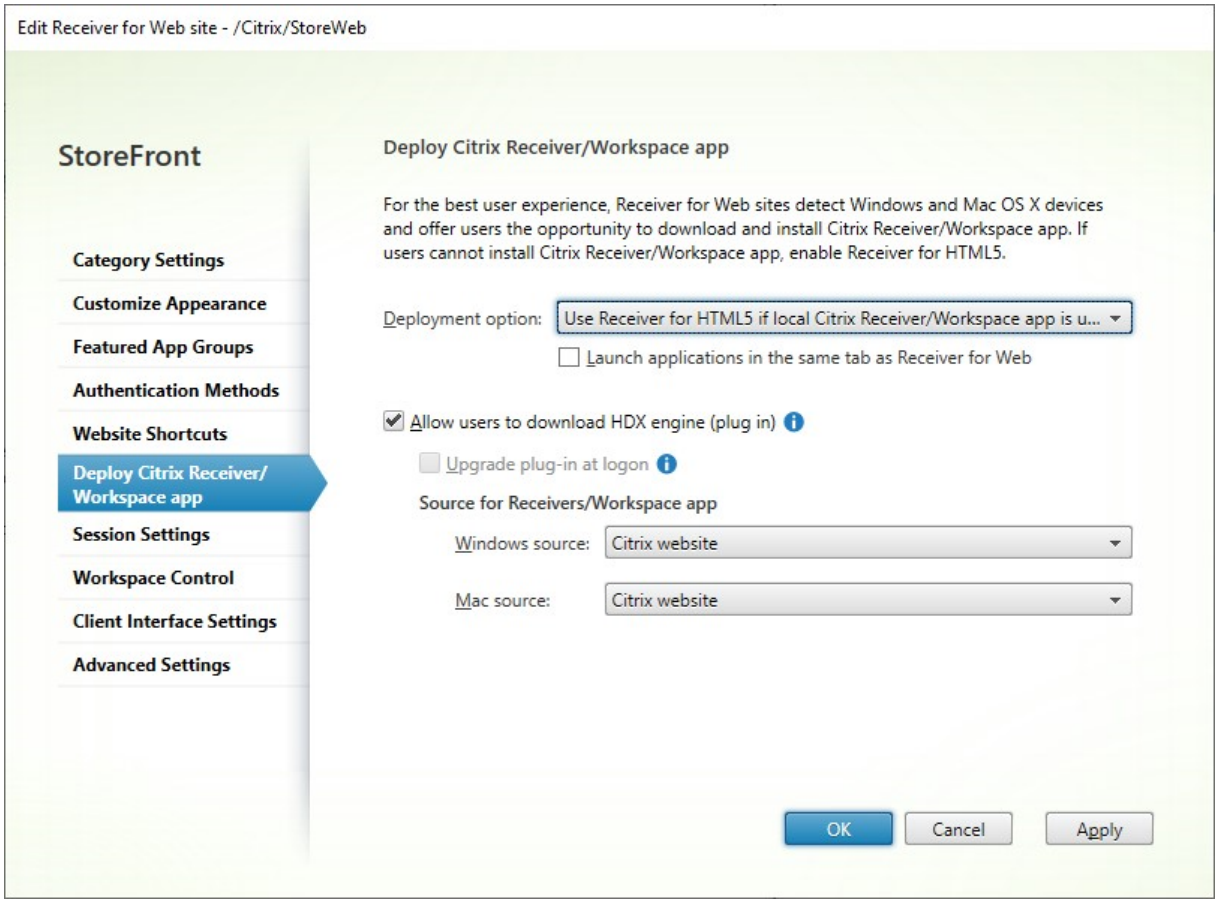
Set-STFWebReceiverApplicationShortcuts PowerShell コマンドレットを使用して信頼できる URL を追加できます。

Citrix Workspace アプリの展開

June 6, 2024

デフォルトでは、ユーザーが最初に Windows、macOS または Linux 上の Web ブラウザーを使用してストアを参照すると、StoreFront は Citrix Workspace アプリがローカルにインストールされているかどうかを自動的に判別します。

ローカルに展開された Citrix Workspace アプリが検出されない場合は、Citrix Workspace アプリをダウンロードしてインストールするよう求められます。デフォルトのダウンロード場所は Citrix Web サイトですが、StoreFront サーバーまたはその他の場所でインストーラーをホストすることもできます。Citrix Workspace アプリをローカルにインストールできないユーザーは、Web ブラウザーを通じて HTML5 向け Citrix Workspace アプリを使用できます。



展開オプションを変更するには、［Receiver for Web サイトの編集］に移動し、［**Citrix Receiver/Workspace** アプリの展開］タブを選択します。

展開オプション

- Citrix Workspace アプリをローカルにダウンロードしてインストールすることを求めるプロンプトを表示せずに、常に Web ブラウザーを使用してリソースにアクセスできるようにするには、［常に **Receiver for HTML5** を使用］を選択します。このオプションを選択すると、Workspace for HTML5 ユーザーは常にブラウザーを通じてリソースに直接アクセスします。
- ［ローカル **Receiver** が使用できない場合 **Receiver for HTML5** を使用］を選択して、Citrix Workspace アプリをローカルにダウンロードしてインストールするためのメッセージがストアの Web サイトに表示されるようにし、インストールできない場合はブラウザーを介してリソースにアクセスできるようにします。この場合、Citrix Workspace アプリをインストールしていないユーザーが Receiver for Web サイトにログオンするたびに、Citrix Workspace アプリをダウンロードしてインストールすることを求めるメッセージが表示されます。
- ［ローカルにインストール］を選択して、常にローカルにインストールされた Citrix Workspace アプリからアクセスするようにします。ユーザーは使用しているプラットフォームに対応した Citrix Workspace アプリをダウンロードしてインストールするよう求められます。ユーザーは引き続き Web ブラウザーを介してスト

アにアクセスできますが、リソースを起動すると、ローカルにインストールされた Workspace アプリで開きます。

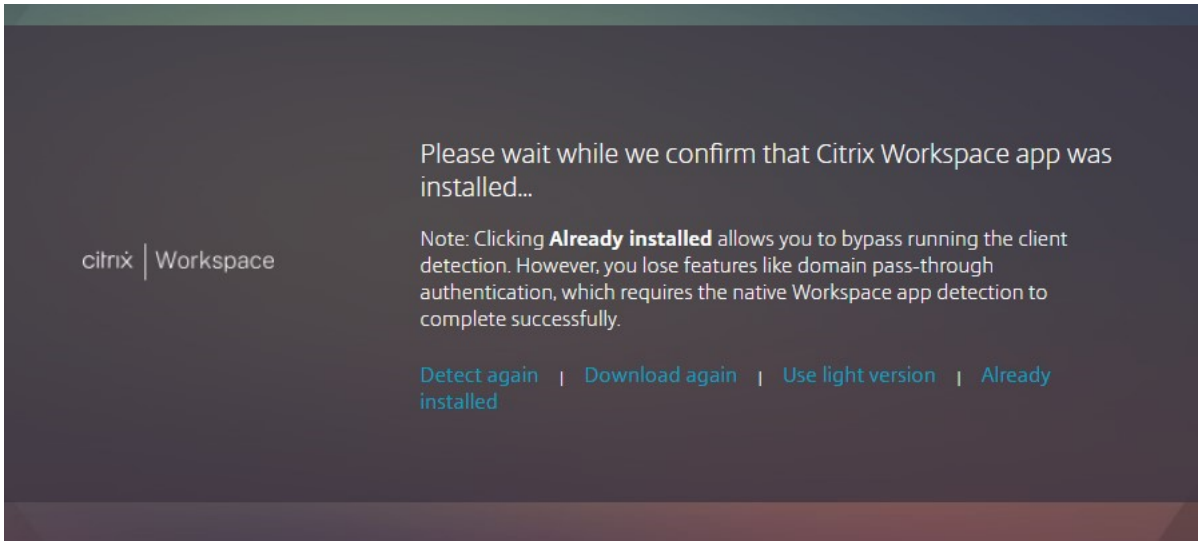
同じタブでアプリケーションを起動する

［常に **Receiver for HTML5** を使用］または ［ローカル **Receiver** が使用できない場合 **Receiver for HTML5** を使用］を選択した場合、デフォルトでは、ブラウザーで起動されたリソースにより新しいブラウザータブが開きます。リソースを同じタブで開き、HTML5 向け Workspace アプリを置き換えるには、［**Receiver for Web** と同じタブでアプリケーションを起動する］を選択します。

クライアント検出ページに ［インストール済み］オプションを表示します

> 注:
>
> この設定は、Windows、MacOS、Linux デバイスにのみ適用されます。ユーザーが Workspace Web 拡張機能をインストールしている場合、クライアントの検出と起動 は Web 拡張機能によって処理されます。このような場合、この 設定は適用されません。

エンドユーザーが Windows、macOS、または Linux 上のブラウザーで初めてストアを開くと、Web サイトは Citrix Workspace Launcher を使用してローカルにインストールされたアプリを検出しようとします。その後、ユーザーがリソースを起動すると、Citrix Workspace Launcher はローカルにインストールされた Citrix Workspace アプリと通信します。ユーザーが ［インストール済み］オプションをクリックすると、クライアント検出プロセスはスキップされます。その結果、ユーザーがリソースを起動すると、`.ica`ファイルがダウンロードされ、ユーザーはローカルにインストールされた Citrix Workspace アプリで開くことができます。ドメインパススルーや App Protection などの機能はサポートされません。



ダウンロードされたこの`.ica`ファイルはセキュリティ上のリスクをもたらす可能性があります。Citrix では、［インストール済み］オプションを非表示にするために、［クライアント検出ページに「インストール済み」リンクを表示します］チェックボックスをオフにすることをお勧めします。

すべてのプラットフォームで **ICA** のダウンロードを禁止します

これにより、すべてのプラットフォームで`.ica`のダウンロードが完全にブロックされ、さらに高いレベルの保護が提供されます。Citrix Workspace Launcher は iOS、Android、Chrome では利用できないため、ユーザーは利用可能な場合は簡易バージョンを使用するか、ローカルにインストールされた Citrix Workspace アプリにストアを追加する必要があります。

> 重要:
>
> このオプションは、［クライアント検出ページに「インストール済み」を表示します］オプションと組み合わせて使用しないでください。

ユーザーが **Windows** または **Mac** 向け **Citrix Workspace** アプリをダウンロードできるようにする

［ローカルにインストール］または ［ローカル **Receiver** が使用できない場合 **Receiver for HTML5** を使用］を選択し、［ユーザーによる **HDX** エンジン（プラグイン）のダウンロードを許可する］を有効にして、HTML5 向け Citrix Workspace アプリがローカルにインストールされた Workspace アプリを検出しない場合は、Windows 向けまたは Mac 向けの Citrix Workspace アプリをダウンロードするオプションが表示されます。

ログオン時に **Workspace** アプリをアップグレードする

［ログオン時にプラグインをアップグレードする］を選択すると、HTML5 向け Workspace アプリでログオン時にローカルにインストールされた Citrix Workspace アプリクライアントをアップグレードするかどうかをユーザーが選択できます。ユーザーはアップグレードをスキップすることもでき、ブラウザーの Cookie が消去されない限り、アップグレードを求めるメッセージが再度表示されることはありません。この機能を有効にするには、StoreFront サーバー上で Citrix Workspace アプリファイルを使用できるようにしてください。

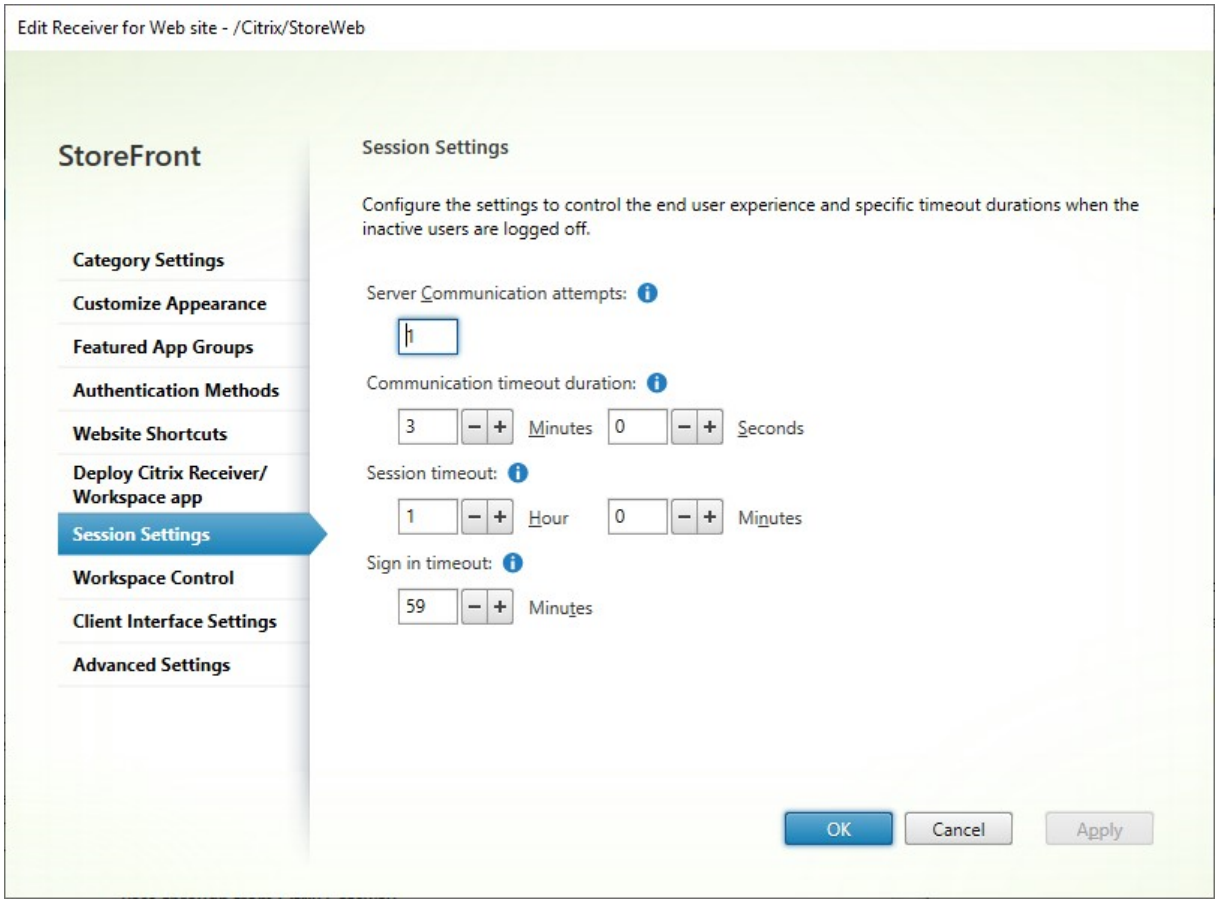
ソースのダウンロード

エンドユーザーがダウンロードボタンをクリックすると、Citrix Web サイトにリダイレクトされるか、サーバーからファイルを直接ダウンロードするかを選択できます。［**Citrix Web** サイト］、［**StoreFront** サーバーのローカルファイル］、または ［リモートサーバーのファイル（**URL** を使用）］を選択できます。

セッション設定の構成

June 6, 2024

セッション設定を変更するには、［Receiver for Web サイトの編集］ 画面に移動し、［セッション設定］タブを選択します。



サーバー通信試行回数

StoreFront 内部の、Web プロキシとストアサービス間の呼び出しの試行回数。通常、この設定を変更する必要はありません。

通信のタイムアウト期間

StoreFront 内部の、Web プロキシとストアサービス間の呼び出しに許可される時間。通常、この設定を変更する必要はありません。

セッション非アクティブタイムアウト

Web ブラウザーを通じて StoreFront ストアにアクセスしているときに、一定期間非アクティブ状態が続くと、「アクティブでないため、セッションはタイムアウトしました。」というメッセージがユーザーに表示されます。ユーザーの使用パターンに応じてセッションタイムアウトを変更できます。これは、Citrix Workspace アプリには影響しません。

または、PowerShell を使用することもできます。たとえば、Web サイト「/Citrix/StoreWeb」のタイムアウトを 30 分に設定するには、次の手順を実行します。

```
$rfw = Get-STFWebReceiverService '/Citrix/StoreWeb'
Set-STFWebReceiverService $rfw -SessionStateTimeout 30
<!--NeedCopy-->
```

セッションタイムアウトを ［認証トークンの有効期間］または ［最大有効期間］よりも大きくなるように変更すると、それに合わせて認証トークンの有効期間や最大有効期間も更新されます。

認証トークンの有効期間

ユーザーがブラウザー経由で StoreFront ストアにアクセスすると、デフォルトでは、アクティビティに関係なく、ユーザーは 8 時間後にログアウトされます。これは、Citrix Workspace アプリには影響しません。このタイムアウトを増やすには、次の手順を実行します。

1. StoreFront で **c:\inetpub\wwwroot\Citrix<StoreWeb>** に移動します。
2. `web.config`ファイルを開きます。
3. 次のエントリを特定します：**<authentication tokenLifeTime="08:00:00"method="Auto"/>**
4. 必要な値に**tokenLifeTime**を変更します。1 日以上の値を入力するには、`d.h:m:s`の形式を使用します。

セッションタイムアウトを 20 時間以上に増やす場合は、認証サービスのトークンの最大有効期間も増やす必要があります。

認証サービスのトークンの最大有効期間

認証サービスは、Web ブラウザーまたは Citrix Workspace アプリを介してストアに接続するときに使用されるトークンを発行します。Citrix Workspace アプリの場合、これは更新する必要がある唯一のログインタイムアウトです。ブラウザーを通じて StoreFront にアクセスする場合、このタイムアウトは他のタイムアウトとともに使用されます。このページで説明されている他の設定とは異なり、これはストアのすべての Web サイトに適用されます。

StoreFront に Citrix Gateway を接続する場合、Citrix Gateway はユーザー資格情報を持ち、StoreFront に対して SSO を実行します。StoreFront トークンの有効期限が切れると、StoreFront は CitrixAG Basic チャレンジを発行し、Citrix Gateway は StoreFront にログインするための資格情報を提供します。したがって、Citrix Gateway も使用している場合は、独自のセッションタイムアウトも構成する必要があります。

1. StoreFront サーバーにインストールされている Citrix Workspace アプリの場合、ストアの認証サービス**c:\inetpub\wwwroot\Citrix\<Store>Auth**のパスに移動します（ストアの数に応じて、複数の認証サービスの 1 つとなる可能性があります）。

2. web.configファイル内で、**Authentication Token Producer** サービスを見つけて、その中でidが **Authentication Token Producer** のものと一致するaddエレメントを探します。次の例では、id="f7cac185-57c1-4629-a33c-88a89dd4295d"encipherId="2948f7ad-735e-4e03-8e01-8d4f5d3ca75b"を持つadd要素が必要です:

```
<service id="f7cac185-57c1-4629-a33c-88a89dd4295d" displayName="
    Authentication Token Producer">
     <relyingParties signingId="2948f7ad-735e-4e03-8e01-8
        d4f5d3ca75b" defaultLifetime="01:00:00" maxLifetime="
        01:00:00">
     <clear />
     <add id="f7cac185-57c1-4629-a33c-88a89dd4295d" encipherId="
        2948f7ad-735e-4e03-8e01-8d4f5d3ca75b" defaultLifetime="
        01:00:00" maxLifetime="20:00:00" />
<!--NeedCopy-->
```

3. 必要な値に**maxLifetime**を変更します。デフォルトは20:00:00です。1 日以上の値を入力するには、dd.hh:mm:ssの形式を使用します。
4. **iisreset** コマンドを実行して変更を適用します。このコマンドを実行すると、ユーザーは Citrix StoreFront Web からログオフされますが、現在の ICA セッションには影響しません。

ワークスペースコントロール

June 6, 2024

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのアプリケーションでの作業を継続できます。ユーザーは、新しいデバイスにログオンするたびにすべてのアプリケーションを再起動する必要がなく、複数のデバイスを切り替えながら同じアプリケーションインスタンスを使用できます。これにより、たとえば病院で臨床医がワークステーションを切り替えて患者データにアクセスするときの時間を節約できます。

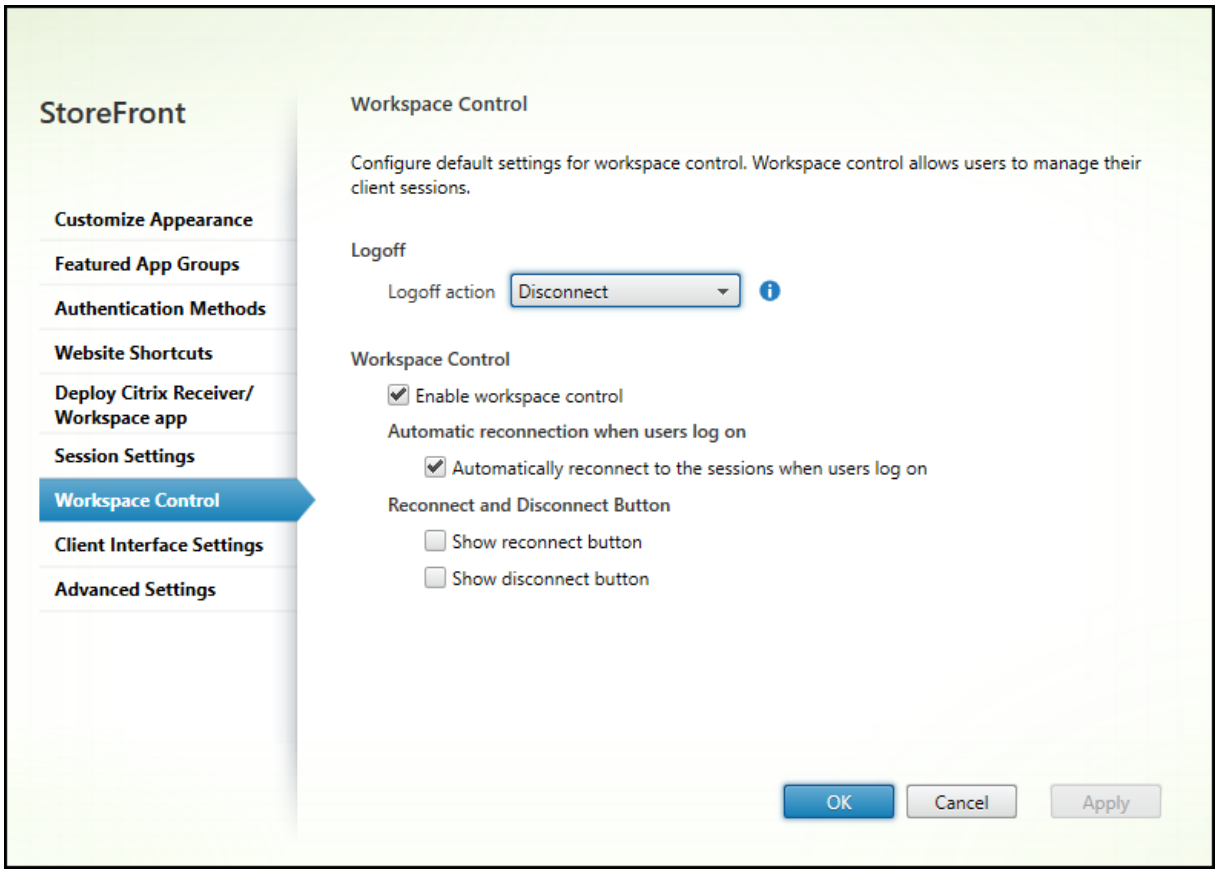
ユーザーがログオンすると、実行したままのアプリケーションに自動的に再接続されます。たとえば、ユーザーがストアにログオンし、いくつかのアプリケーションを起動したとします。その後、ユーザーが別のデバイスで同じアクセス方法を使用して同じストアにログオンすると、実行中のアプリケーションが自動的に新しいデバイスで使用可能になります。ユーザーがストアで起動したすべてのアプリケーションは、そのストアからログオフすると自動的に切断されます。ただし、シャットダウンはされません。Web ブラウザーを介してストアにアクセスする場合は、同じブラウザーを使用してログオン、アプリケーションの起動、およびログオフを行う必要があります。

HTML5 向け **Citrix Workspace** アプリでワークスペースコントロールを構成する

StoreFront 管理コンソール内のワークスペースコントロール設定は、Web ブラウザーを介してストアにアクセスする場合にのみ適用されます。これには、次の要件と制限が適用されます:

- HTML 向け Workspace アプリがホストされたデスクトップまたはアプリケーション内で実行されている場合、ワークスペースコントロールは使用できません。
- Windows デバイスから Web サイトにアクセスするユーザーについては、ユーザーデバイスに Windows 向け Citrix Workspace アプリがインストールされていることをサイトで検出できる場合、および HTML5 向け Citrix Workspace アプリが使用される場合にのみ、ワークスペースコントロールが有効になります。
- 切断したアプリケーションに再接続するには、Internet Explorer で Web サイトにアクセスするユーザーは［ローカルイントラネット］または［信頼済みサイト］のゾーンにサイトを追加する必要があります。
- ただし、ワークスペースコントロールが有効になっていても、Web サイトで使用可能なデスクトップが 1 つのみの場合にそのデスクトップが自動的に起動するように構成すると、アプリケーションは再接続されません。
- アプリケーションを切断するときに、起動に使用した Web ブラウザーを使用する必要があります。別の Web ブラウザーで起動したリソースや、デスクトップや［スタート］メニューから Citrix Workspace アプリで起動したリソースは、HTML5 向け Citrix Workspace アプリで切断したりシャットダウンしたりできません。
- リソースが同じブラウザータブ内で開いている場合、ワークスペースコントロールは使用できません。これを構成するには、「Citrix Workspace アプリの展開」を参照してください。

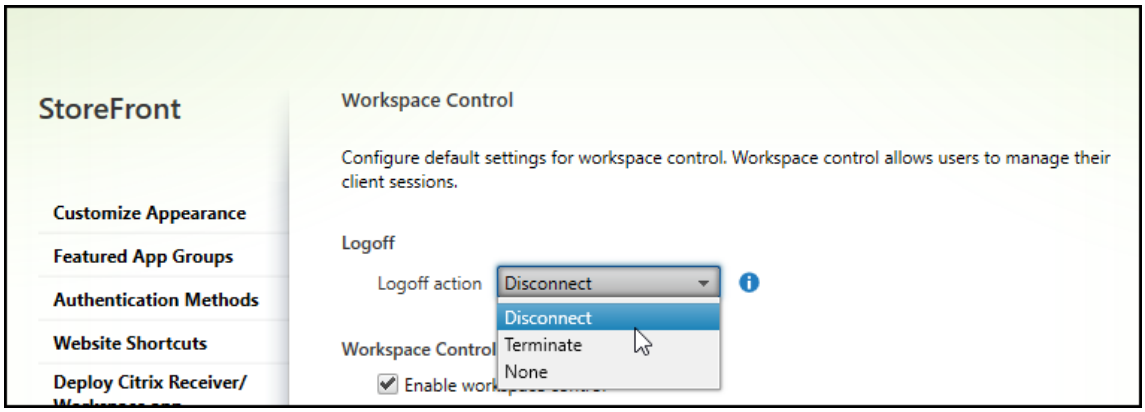
ストアへのアクセスがする Web ブラウザーを介して行われる場合のワークスペースコントロールの設定を変更するには、［Receiver for Web サイトの編集］画面で ［ワークスペースコントロール］を選択します。



ワークスペースコントロールの設定を次のように構成します：

- ［ログオフアクション］を指定します。ログオフアクションは次のとおりです：

- ［切断］：サイトからログオフすると、アプリとデスクトップのセッションはクライアントデバイスから自動的に切断されます。
- ［終了］：サイトからログオフすると、アプリとデスクトップのセッションはサーバー上で自動的に終了します。
- ［なし］：サイトからログオフしても、アプリとデスクトップのセッションは引き続き実行されます。



- ［ワークスペースコントロールを有効にする］チェックボックスをオンにします。
- ［ユーザーログオン時の自動再接続］の ［ユーザーがログオンしたときに自動的にセッションに再接続する］チェックボックスをオンにします。

PowerShell SDK を使用してワークスペースコントロールを構成する

PowerShell コマンドレットSet-STFWebReceiverUserInterfaceを使用してワークスペースコントロールを構成できます。

Windows 向け **Workspace** アプリでワークスペースコントロールを構成する

Windows 向け Workspace でワークスペースコントロールを構成するには、「ワークスペースコントロール再接続の管理」を参照してください。

Mac 向け **Workspace** アプリでワークスペースコントロールを構成する

Mac 向け Workspace アプリのワークスペースコントロールを構成するには、「ワークスペースコントロール設定の構成」を参照してください。

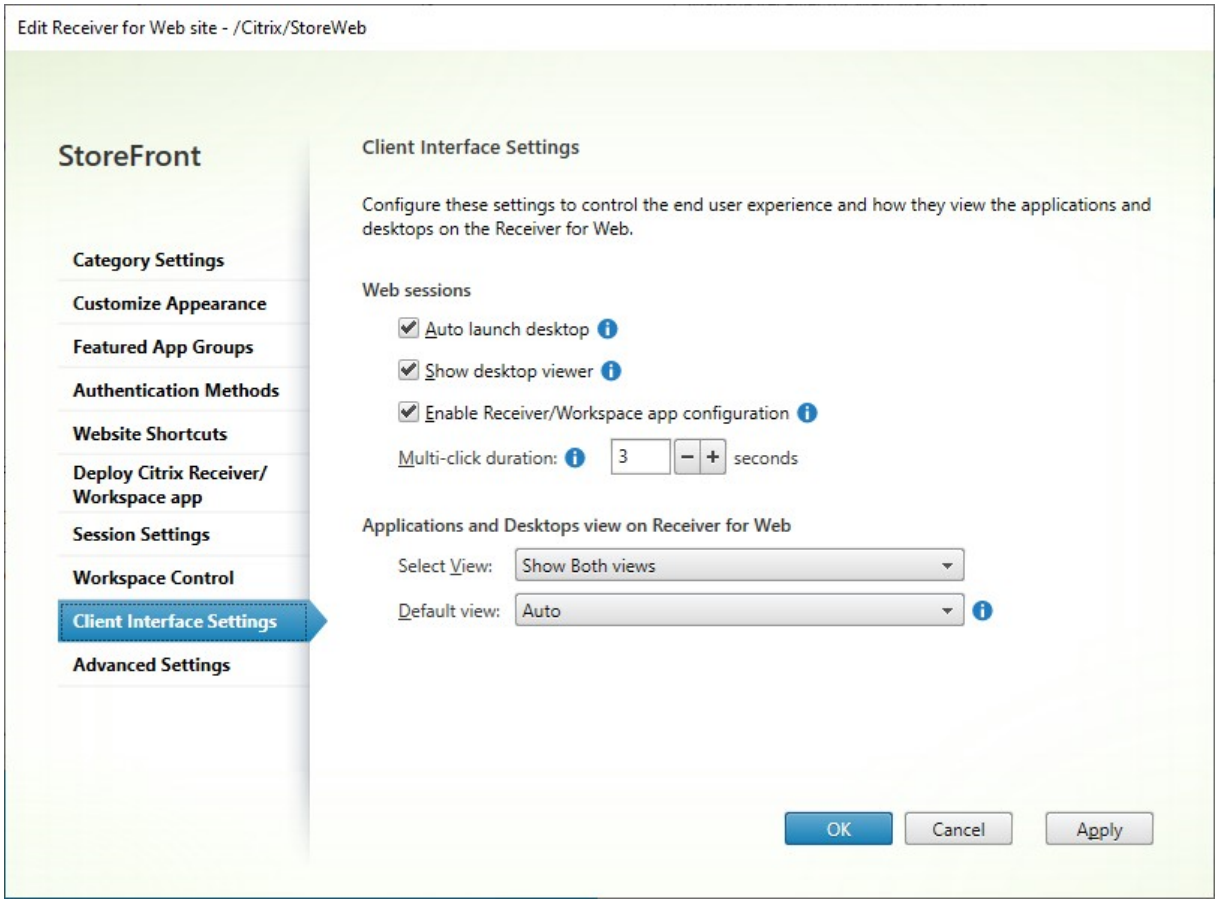
すべてのアプリでワークスペースコントロールを無効にする

Workspace アプリ全体で StoreFront でのセッション再接続を無効にするには、どのような構成であっても、［詳細設定］タブに移動し、［セッションの再接続を許可する］チェックボックスをオフにします。

クライアントインターフェイスの設定

June 6, 2024

［Receiver for Web サイトの編集］画面からクライアントインターフェイス設定を変更するには、［クライアントインターフェイスの設定］タブを選択します。



デスクトップを自動的に起動する

この設定が有効で、ユーザーのデスクトップが 1 つだけの場合、ユーザーがサインインするとデスクトップが起動します。

PowerShell SDK を使用してデスクトップの自動起動設定を変更するには、パラメーター`AutoLaunchDesktop`を指定してコマンドレットSet-STFWebReceiverUserInterfaceを呼び出します。

この設定は、HTML5 向け Citrix Workspace アプリにのみ適用されます。これは、ローカルにインストールされた Citrix Workspace アプリには適用されません。

Desktop Viewer を表示する

Desktop Viewer は、HDX 設定に簡単にアクセスできるツールバーです。この設定を使用して、これを表示するかどうかを選択します。

この設定は、HTML5 向け Citrix Workspace アプリにのみ適用されます。これは、ローカルにインストールされた Citrix Workspace アプリには適用されません。

複数クリックの間隔

構成された期間内にユーザーが同じアプリケーションを複数回起動できないようにします。これは HTML5 向け Citrix Workspace アプリにのみ適用され、ネイティブ Citrix Workspace アプリには適用されません。

PowerShell SDK を使用して複数クリック間隔を変更するには、パラメーター`MultiClickTimeout`を指定してコマンドレットSet-STFWebReceiverUserInterfaceを呼び出します。

この設定は、HTML5 向け Citrix Workspace アプリにのみ適用されます。これは、ローカルにインストールされた Citrix Workspace アプリには適用されません。

Receiver/Workspace アプリ構成を有効にする

オンにすると、HTML5 向け Citrix Workspace アプリによりプロビジョニングファイルが提供されます。ユーザーは、このファイルを使用してネイティブの Citrix Workspace アプリでストアを自動で構成できます。このプロビジョニングファイルには、その Receiver for Web サイトのリソースを提供するストアに接続するための詳細（Citrix Gateway 展開環境やビーコンの詳細など）が定義されています。

PowerShell SDK を使用してこのオプションを変更するには、パラメーター`ReceiverConfigurationEnabled`を指定してコマンドレットSet-STFWebReceiverUserInterfaceを呼び出します。

アプリケーションおよびデスクトップ表示

デスクトップとアプリケーションの両方にアクセスできる場合、Citrix Workspace アプリにはデフォルトでデスクトップとアプリケーションが別々のビューで表示されます。お気に入りは ［ホーム］ビューに表示されます。サイトにログオンすると、最初に［ホーム］ビューが表示されます。

［ビューの選択］ドロップダウンリストから、アプリとデスクトップのどちらを表示するか、または両方を表示するかを選択します。

［デフォルト］ビュードロップダウンリストから、ユーザーがログインしたときに表示されるビューを選択します。

オプション	説明
自動	［ホーム］ビューを表示する
アプリ	アプリビューを表示する
デスクトップ	デスクトップビューを表示する

PowerShell SDK を使用してこれらのオプションを変更するには、パラメーターShowAppsView、ShowDesktopsViewおよびDefaultViewを指定してコマンドレットSet-STFWebReceiverUserInterfaceを呼び出します。

App Protection

June 6, 2024

App Protection は、キーロギングと画面キャプチャをブロックすることで、さらなるセキュリティを提供します。詳しくは、「App Protection」のドキュメントを参照してください。

Workspace アプリ

App Protection は、Windows、Mac、Linux 向け Citrix Workspace アプリを通じてストアにアクセスするときにデフォルトで利用可能です。

ハイブリッド起動の App Protection

Web ブラウザー経由でストアにアクセスすると、App Protection を必要とするアプリはデフォルトで非表示になります。StoreFront は、Citrix Workspace アプリの次の最小バージョンを検出したときに、保護されたアプリを表示するように構成できます:

アプリ	バージョン
Windows 向け Citrix Workspace アプリ	1912
Mac 向け Citrix Workspace アプリ	2001
Linux 向け Citrix Workspace アプリ	2108

以前のバージョンの Workspace アプリを使用している場合、または iOS、Android、ChromeOS 上で使用している場合、または HTML5 向け Citrix Workspace アプリを使用してブラウザーでアプリを起動している場合、StoreFront は保護されたアプリを表示しません。

サポートされている Workspace バージョンで保護されたアプリを StoreFront が表示できるようにするには、PowerShell SDKコマンドレットSet-STFWebReceiverAppProtectionを使用します。

ユーザーがブラウザー経由で Workspace アプリを起動することを選択した場合（管理者構成によって、またはユーザーが **Workspace lite** の使用を選択することによって）、App Protection は利用できません。ローカルにインストールされた Citrix Workspace アプリを使用して常に起動するようにストアを構成できます。「Citrix Workspace アプリの展開」を参照してください。

StoreFront は、Citrix Workspace Web 拡張機能が利用可能および構成されている場合、これを使用して、Citrix Workspace アプリのバージョンを判断します（「ブラウザー拡張機能ベースのクライアント検出」を参照してください）。それ以外の場合、StoreFront は、ユーザーがストアの Web サイトに初めてアクセスしたときのクライアント検出の一環として、Citrix Workspace アプリのバージョンを判断します。ユーザーが ［インストール済み］を選択して検出をスキップした場合、StoreFront はアプリのバージョンを判断できないため、保護されたアプリケーションは表示されません。したがって、［インストール済み］オプションを無効にすることをお勧めします。「Citrix Workspace アプリの展開」を参照してください。

> 警告
>
> Citrix Workspace Web 拡張機能が利用できない場合、StoreFront は、ユーザーが Web サイトに初めてアクセスしたときに、Citrix Workspace アプリのバージョンを判断します。その後、ユーザーが別のバージョンの Workspace アプリをインストールすると、StoreFront はその変更を認識しないため、保護されたアプリの起動が誤って許可または禁止される可能性があります。App Protection のセキュリティ態勢チェックを構成して、App Protection をサポートしていない以前のバージョンの Citrix Workspace アプリからの仮想アプリやデスクトップの起動をブロックすることをお勧めします。

Web サイトの削除

June 6, 2024

1. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ノードを選択して、Citrix Receiver for Web サイトを作成するストアを選択し、［操作］ペインの ［**Receiver for Web** サイトの管理］をクリックします。
2. サイトを選択し、［削除］をクリックします。サイトを削除すると、ユーザーはその Web ページを使用してストアにアクセスできなくなります。

Workspace アプリの Web サイトを構成する

June 6, 2024

StoreFront を使って新しいストアを作成すると、Web サイトが自動的に作成され、ストアに割り当てられます。ストアに複数の Web サイトがある場合、ユーザーが Citrix Workspace アプリを使用してストアにアクセスしたときにどの Web サイトを表示するかを選択します。

1. 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. 中央ペインでストアを選択し、アクションペインで ［ユニファイド エクスペリエンスの構成］をクリックします作成された Citrix Receiver for Web の Web サイトがない場合は、Receiver for Web サイトの追加ウィザードへのリンクを含むメッセージが表示されます。
3. ユーザーがこのストアにアクセスしたときに Citrix Workspace アプリクライアントが表示するようにする Web サイトを選択します。
4. ［**OK**］をクリックします。

サーバーグループの構成

June 6, 2024

以下のタスクでは、複数サーバーの StoreFront 展開環境の設定を変更します。複数サーバー展開環境を管理する場合、同時に複数のサーバー上で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。また、展開環境内で一貫した構成を保つため、構成の変更内容をグループ内のほかのサーバーに反映させる必要があります。

StoreFront サーバーグループに含まれるサーバーは、StoreFront のインストール場所の設定と IIS Web サイトの設定（物理パスやサイト ID など）の両方が同じになるように構成する必要があります。

サーバーグループへのサーバーの追加

［サーバーの追加］タスクを使用して、新しくインストールした StoreFront サーバーを既存の展開環境に追加するための承認コードを取得します。新しいサーバーを既存の StoreFront 展開環境に追加する方法について詳しくは、「既存のサーバーグループへの参加」を参照してください。グループ内のいくつのサーバーにアクセスする必要があるかについては、「StoreFront の展開計画」の「スケーラビリティ」の説明を参照してください。

サーバーグループからのサーバーの削除

複数サーバーの StoreFront 展開環境からサーバーを削除するには、［サーバーの削除］タスクを使用します。このタスクでは、StoreFront 管理コンソールを実行しているサーバー以外の任意のサーバーをグループから削除できます。ただし、複数サーバーの展開環境からサーバーを削除する前に、そのサーバーを負荷分散環境から削除しておく必要があります。

削除された StoreFront サーバーが、同じサーバーグループまたは異なるサーバーグループに再度追加される前に、出荷時のデフォルト設定にリセットする必要があります。「サーバーを出荷時のデフォルト設定にリセット」を参照してください。

サーバーグループへのローカルの変更の反映

現在のサーバー上で行った変更内容を、複数サーバーの StoreFront 展開環境内のほかのすべてのサーバーに反映させるには、［変更の伝達］タスクを使用します。構成情報の伝達は手動で開始されるため、グループ内のサーバーが構成変更で更新されるタイミングと状況を制御できます。このタスクの実行中は、グループ内のすべてのサーバーが更新されるまで、追加の変更を加えることはできません。

> 重要:
>
> これにより、伝達中にグループ内のほかのサーバー上で行ったすべての変更が破棄されます。サーバーの構成を更新する場合、変更をグループ内の他のサーバーに反映することで、後で展開の別のサーバーからの変更を反映する場合でもこれらの変更が失われないようにします。

グループ内のサーバー間で反映される情報には、次の項目が含まれます:

- StoreFront 構成を含むすべての web.config ファイルの内容。
- `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe`や`C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`のような`C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients`の内容。
- `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib`の内容。
- コピーされたイメージや customisation.js ファイルのような`C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom folder`の内容。
- 手動でインポートされた証明書失効一覧（CRL）を除く、Citrix Delivery Services 証明書ストアの内容。ローカル CRL の配布について詳しくは、「証明書失効一覧（CRL）のチェック」を参照してください。

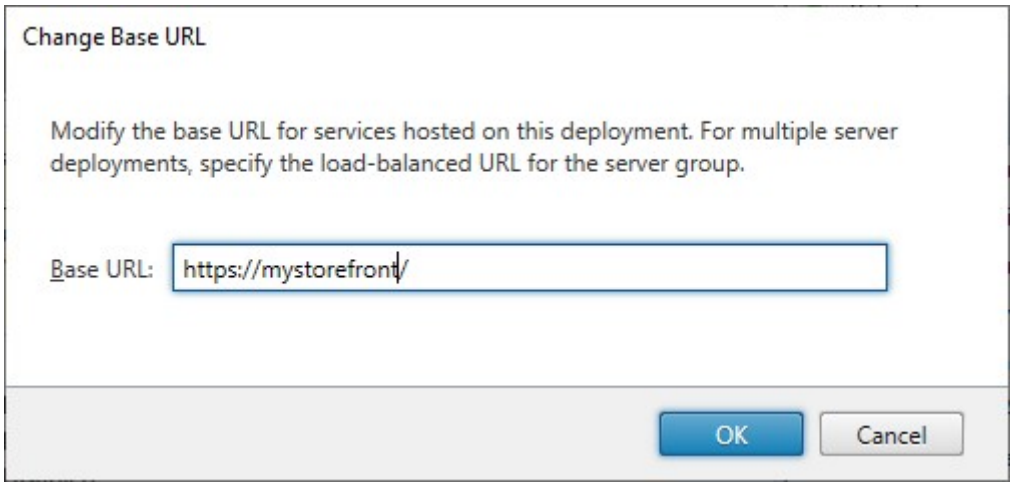
> 注:
>
> サブスクリプションデータは、変更の反映メカニズムとは無関係に他のサーバーと同期されます。これは自動的に行われ、変更の反映タスクが開始されることはありません。

展開環境のベース **URL** の変更

StoreFront 展開環境でホストされるストアやほかの StoreFront サービスのルート URL としてベース URL が使用されます。複数サーバーの展開環境の場合は、負荷分散 URL を指定します。

ベース URL を変更するには、以下の手順を実行します:

1. Citrix StoreFront 管理コンソールの左側のペインで ［サーバーグループ］ ノードを選択します。
2. ［操作］ ペインの ［ベース **URL** の変更…］ をクリックします。
3. 新しい URL を入力します
4. ［**OK**］ を押します。



Citrix Gateway および **NetScaler ADC** との統合

June 6, 2024

Citrix Gateway を StoreFront と一緒に使って、社内ネットワークと NetScaler ADC の外側にいるユーザーにセキュアなリモートアクセスを提供し、負荷分散を実行します。

タスク	詳細
Citrix Gateway のインポート	Citrix Gateway から構成をエクスポートし、StoreFront にインポートします
Citrix Gateway の管理	Citrix Gateway の接続設定を追加、削除、編集します
NetScaler ADC による負荷分散 DFA 用の NetScaler ADC および StoreFront の構成	StoreFront サーバーグループの前でロードバランサーとして NetScaler ADC を構成します
異なるドメインを使用した認証	StoreFront と Citrix Gateway を構成して、ユーザーがまず 1 つのドメインの Gateway で認証してから、次に別のドメインの StoreFront で認証するようにします。
ビーコンポイントの構成	社内ネットワークの内部か外部かを判断するために Citrix Workspace アプリが使用できるビーコン URL を構成します。

タスク	詳細
内部および外部で使用される単一の FQDN の作成	社内ネットワーク内から直接、または Citrix Gateway 経由でリモートからストアにアクセスできる、単一の完全修飾ドメイン名（FQDN）を作成します。

Citrix Gateway の構成

June 6, 2024

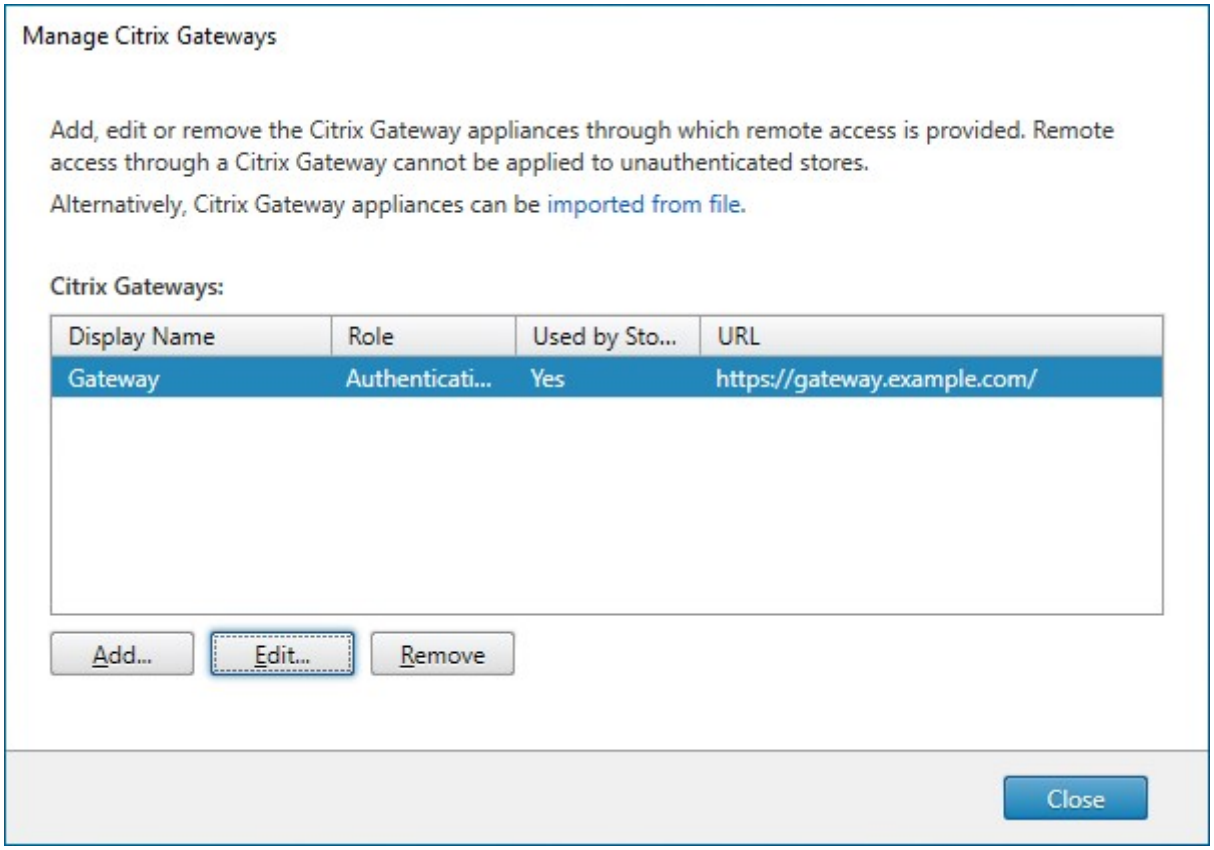
Citrix Gateway を使用して、StoreFront に対するリモートアクセスを提供します。Citrix Gateway は、ハードウェアまたはソフトウェアの NetScaler ADC または NetScaler Gateway アプライアンス上で実行されます。

Gateway の構成について詳しくは、「NetScaler Gateway と StoreFront の統合」を参照してください。

StoreFront がゲートウェイ経由のアクセスを許可する前に、StoreFront 内でゲートウェイを構成する必要があります。

Gateway の表示

StoreFront 内で構成されたゲートウェイを表示するには、Citrix StoreFront 管理コンソールの左ペインで［ストア］ノードを選択して、［**Citrix Gateway** の管理］をクリックします。これによって、［**Citrix Gateway** の管理］ウィンドウが開きます。



PowerShell

ゲートウェイとその構成の一覧を取得するには、Get-STFRoamingGatewayを呼び出します。

Citrix Gateway の追加

> 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. [**Citrix Gateway** の管理] ウィンドウで、[追加] をクリックします。
2. [全般設定] タブで設定を入力し、[次へ] を押します。
   - Citrix Gateway 展開環境にユーザーにとってわかりやすい表示名を指定します。

     ここで指定する表示名がユーザーの Citrix Workspace アプリに表示されます。そのため、ユーザーが使用する展開環境を判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザ

ーが自分のいる場所に最も便利な Citrix Gateway を簡単に特定できるように、表示名に地理情報を含めることができます。

- ゲートウェイの URL を入力します。

  StoreFront 展開環境の FQDN（Fully Qualified Domain Name：完全修飾ドメイン名）は一意で、Citrix Gateway 仮想サーバーの FQDN と異なるものである必要があります。StoreFront と Citrix Gateway 仮想サーバーに同じ FQDN を使用することはサポートされていません。ゲートウェイは URL を`X-Citrix-Via` HTTP ヘッダーに追加します。StoreFront はこのヘッダーを使用して、どのゲートウェイが使用されているか特定します。

  GUI では、ゲートウェイ URL を 1 つだけ追加できます。ゲートウェイに複数の URL からアクセスできる場合は、URL 以外が同一の構成である同じゲートウェイを 2 回追加する必要があります。簡単な構成のために、ゲートウェイへのアクセスに使用されるセカンダリ URL を構成できます。このオプションは GUI では使用できないため、PowerShell を使用して構成する必要があります。PowerShell コマンドを実行する前に、管理コンソールを閉じる必要があります。たとえば、グローバルサーバー負荷分散の背後に複数のゲートウェイがある場合、通常は、テストやトラブルシューティングの目的で、GSLB URL と、特定のリージョナルゲートウェイそれぞれにアクセスするために使用できる URL の両方を追加すると便利です。ゲートウェイを作成したら、`Set-STFRoamingGateway`を使用し、セカンダリ URL に`-GSLBurl`パラメーターを使用して、URL を追加できます。このパラメーターは`GSLBurl`と呼ばれますが、これは 2 番目の URL を追加するあらゆる状況に使用できます。例:

```
1  Set-STFRoamingGateway -Name "Europe Gateway" -GSLBurl "
       eugateway.example.com" -GatewayUrl "gslb.example.com"
2  <!--NeedCopy-->
```

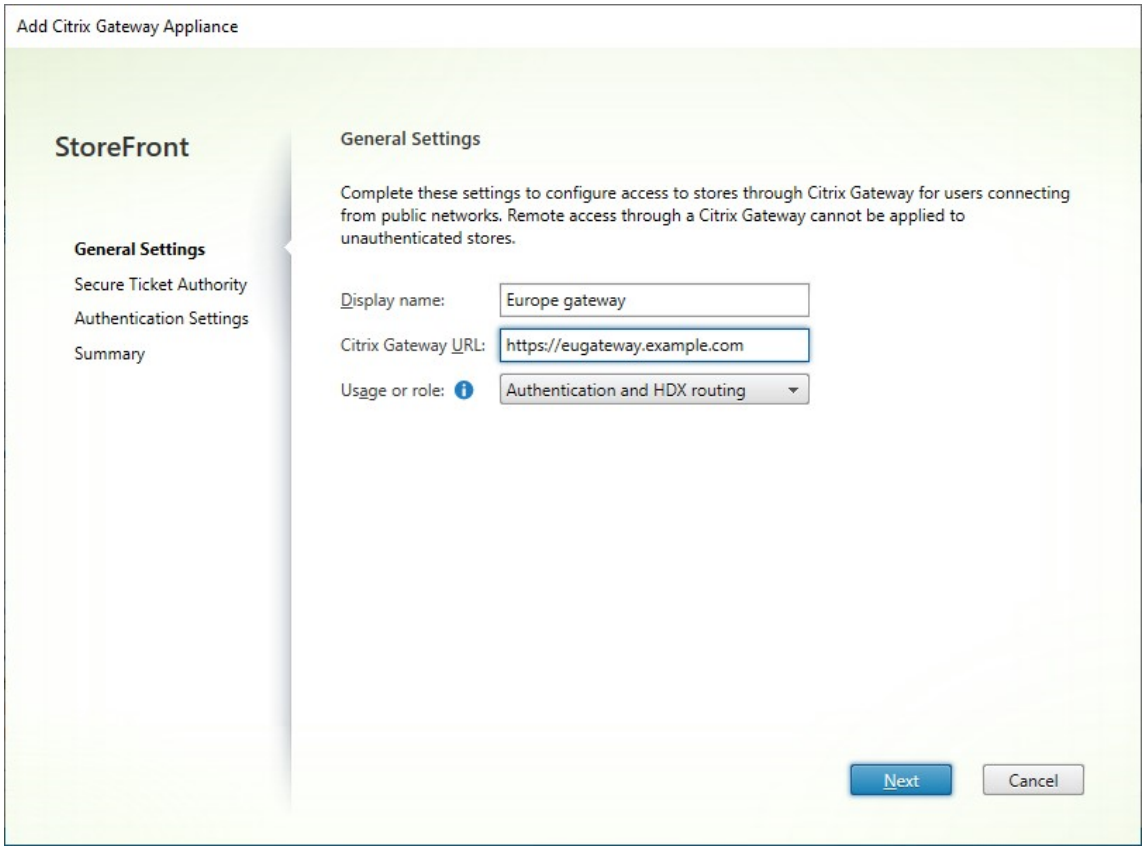
> 注:
>
> この例では直観に反して、`GSLBurl`パラメーターにはリージョナル URL が含まれていますが、`GatewayUrl`パラメーターに含まれているのは GSLB の URL です。ほとんどの目的において、これらの URL は同じように扱われ、ストアに Web ブラウザーのみを介してアクセスする場合は、どちらの方法でも構成できます。ただし、Citrix Workspace アプリを介して StoreFront にアクセスする場合は、StoreFront から`GatewayUrl`を読み取って、それを以降のリモートアクセスで使用します。このため、常に GSLB の URL に接続するように構成することが望ましいです。

  3 つ以上の URL が必要な場合は、これを別個のゲートウェイとして構成する必要があります。

- 使用状況または役割を選択します:

使用状況または役割	説明
認証および HDX ルーティング	StoreFront へのリモートアクセスの提供と VDA へのアクセスの両方のために、ゲートウェイを使用します。
認証のみ	ゲートウェイが StoreFront へのリモートアクセスのためにのみ使用される場合は、これを選択します。

使用状況または役割	説明
HDX ルーティングのみ	StoreFront インスタンスがないサイトなど、VDA への HDX のアクセスを提供するためにのみゲートウェイが使用される場合は、これを選択します。



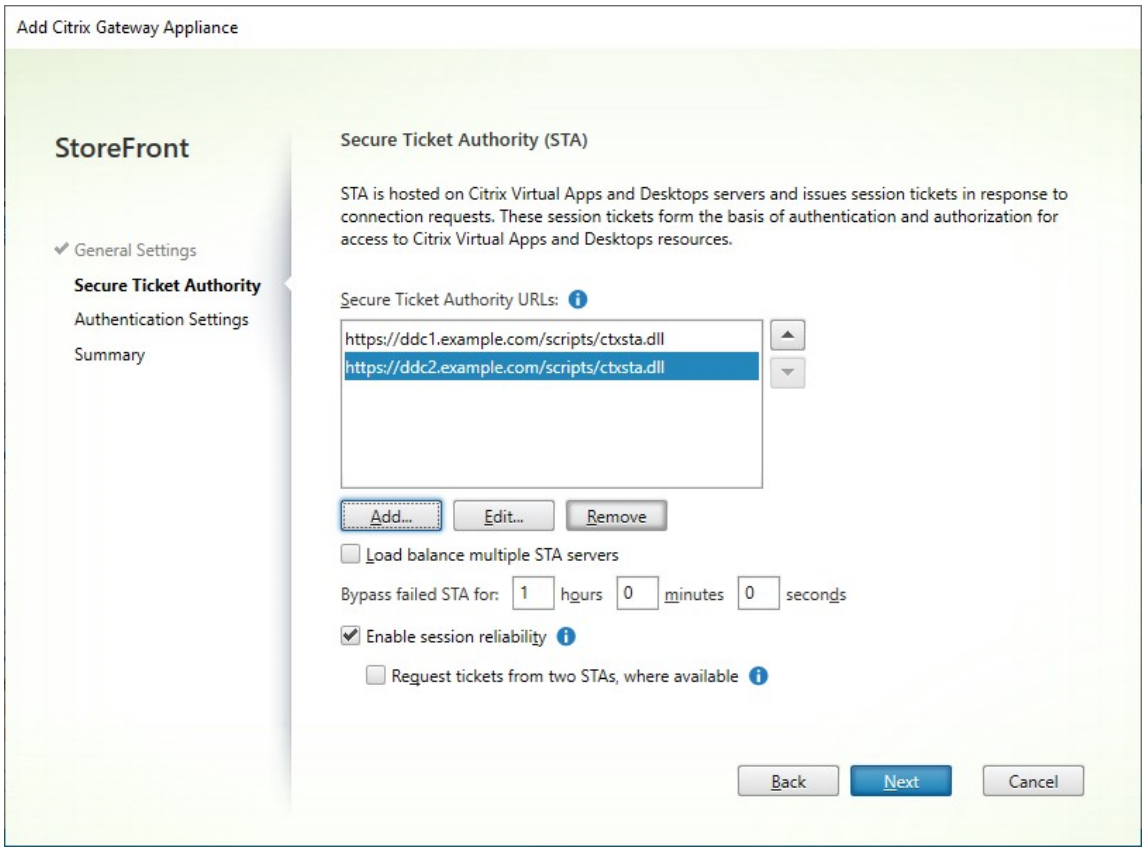
3. [**Secure Ticketing Authority**] タブで設定を入力します。

   Secure Ticket Authority は、接続の要求に応じてセッションチケットを発行します。セッションチケットは、Citrix Virtual Apps and Desktops リソースへのアクセスを認証および承認するための基本機能です。

   - Secure Ticket Authority のサーバー URL を 1 つ以上入力します。Citrix Virtual Apps and Desktops を使用している場合は、Delivery Controller を STA として使用できます。Citrix Desktop as a Service を使用している場合は、Citrix Cloud のチケット発行機関への要求をプロキシする Cloud Connector を入力できます。この一覧のエントリは、Citrix Gateway で構成されたリストと正確に一致する必要があります。
   - [複数の **STA** サーバーを負荷分散する] にチェックを入れると、STA サーバー間で要求を分散します。チェックを外すと、StoreFront は一覧の順番どおりにサーバーを試行します。
   - StoreFront が STA サーバーにアクセスできない場合、一定期間そのサーバーの使用を回避します。デフォルトではこの期間は 1 時間ですが、この値をカスタマイズすることができます。

- Citrix Virtual Apps and Desktops が自動的に再接続を実行する間に、切断したセッションを Citrix Workspace アプリで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数の STA を構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は **2** つの **STA** にチケットを要求する］チェックボックスをオンにします。

  ［可能な場合は 2 つの STA にチケットを要求する］チェックボックスをオンにすると、セッションの途中で 1 つの STA が使用できなくなってもユーザーセッションが中断されないように、StoreFront により 2 つの異なる STA からセッションチケットが取得されます。StoreFront がどちらの STA にもアクセスできない場合は、単一の STA を使用するようにフォールバックされます。



設定の入力が完了したら、［次へ］を押します

4. ［認証設定］タブで設定を入力します。

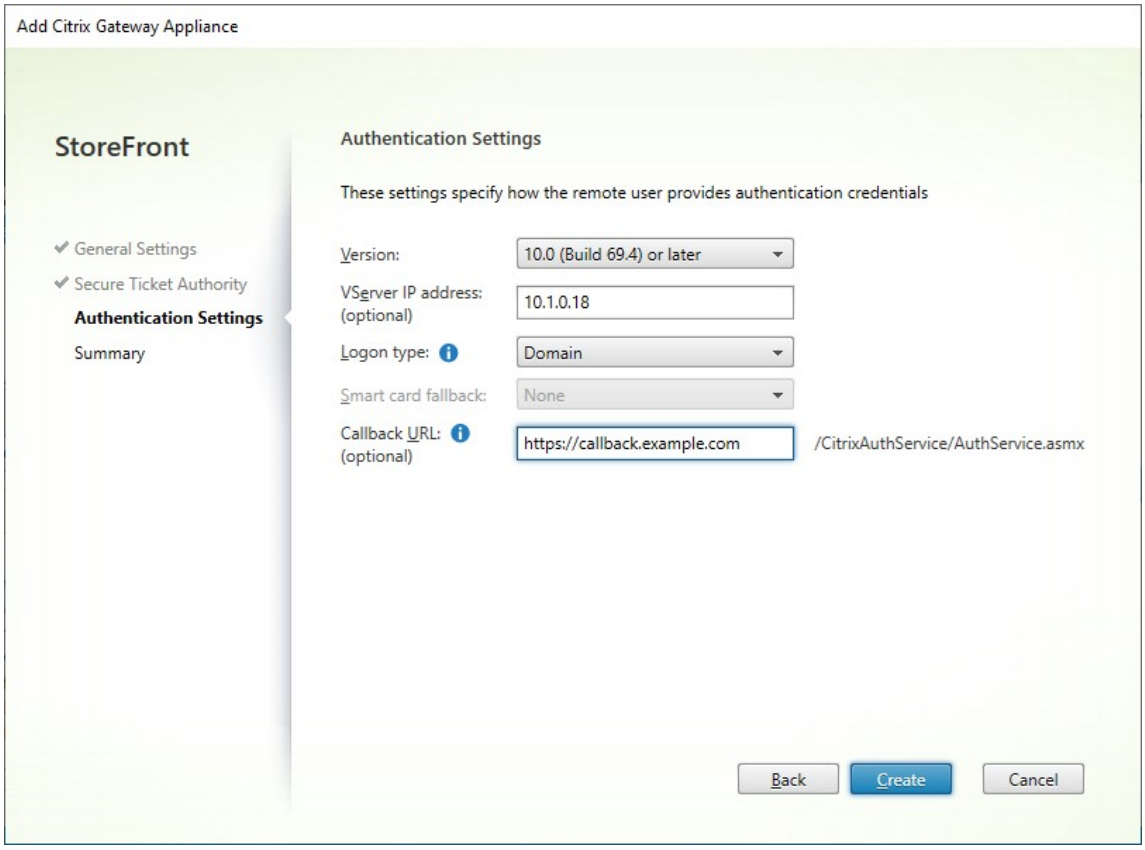
   - NetScaler のバージョンを選択します。
   - 同じ URL を持つ複数のゲートウェイがあるとき（一般的にはグローバルサーバーのロードバランサーを使用している場合）に、コールバック URL を入力した場合は、ゲートウェイの仮想 IP アドレスを入力する必要があります。これにより、StoreFront は要求がどのゲートウェイからのものであるかを識別できるようになり、その結果、コールバック URL を使用してどのサーバーと通信するかを判断できます。それ以外の場合は、空白のままで構いません。
   - ［ログオンの種類］の一覧から、Citrix Workspace アプリユーザー向けにアプライアンス上で構成した認証方法を選択します。

Citrix Gateway アプライアンスに関する構成情報は、ストアのプロビジョニングファイルに追加されます。これにより、Citrix Workspace アプリは、アプライアンスへの初回接続時に適切な接続要求を送信できるようになります。

- ユーザーの Microsoft Active Directory ドメインの資格情報を入力させる場合は、［ドメイン］を選択します。
- セキュリティトークンから取得するトークンコードを入力させる場合は、［セキュリティトークン］を選択します。
- ユーザーのドメイン資格情報とセキュリティトークンから取得するトークンコードの両方を入力させる場合は、［ドメインおよびセキュリティトークン］を選択します。
- テキストメッセージで送信されるワンタイムパスワードを入力させる場合は、［SMS 認証］を選択します。
- スマートカードを挿入して PIN を入力させる場合は、［スマートカード］を選択します。

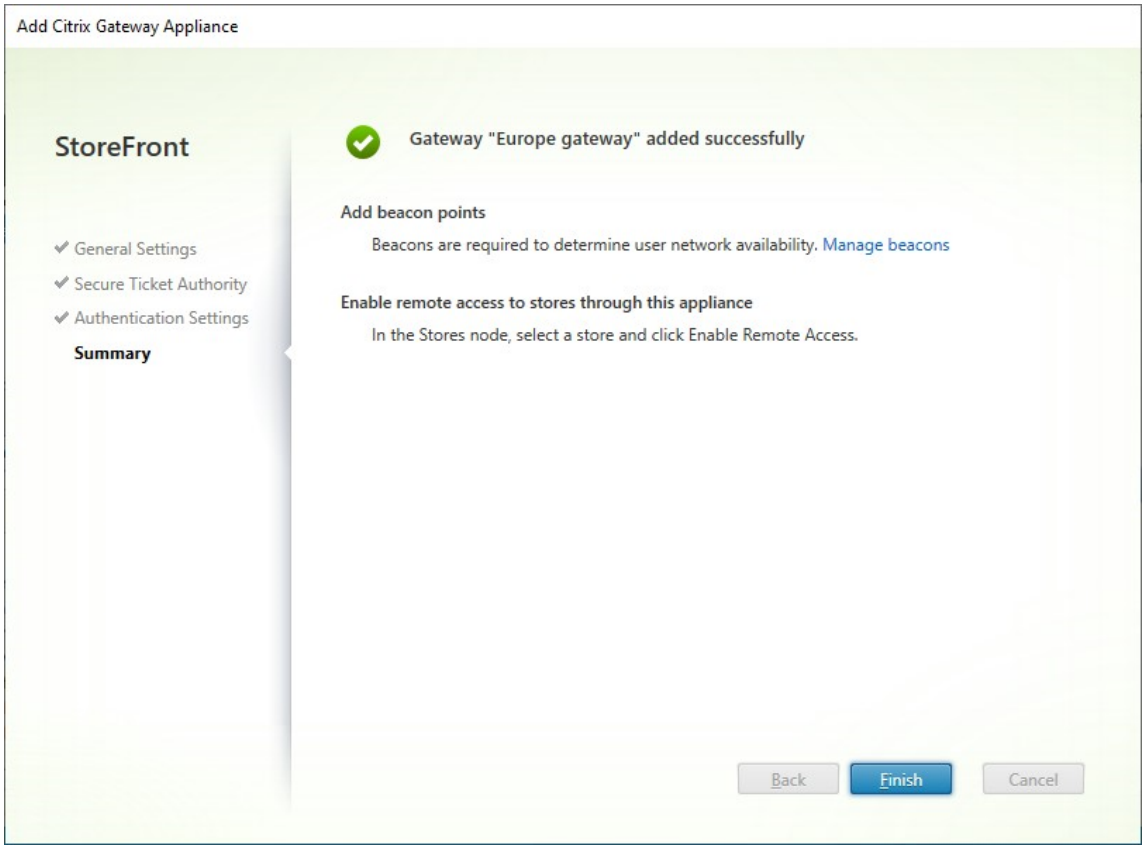
スマートカードでの認証に問題が生じた場合に代替の認証方法を使用できるようにするには、［スマートカードフォールバック］の一覧から代替の認証方法を選択します。

- 必要に応じて、内部的にアクセス可能なゲートウェイの URL を［コールバック URL］ボックスに入力します。これにより StoreFront は Citrix Gateway 認証サービスに接続して、Citrix Gateway からの要求の送信元がそのアプライアンスであることを確認できます。これは、スマートアクセスまたは、スマートカードや SAML などのパスワードレス認証のシナリオに必要です。それ以外の場合は、空白のままで構いません。同じ URL を持つ複数の Citrix Gateway がある場合、この URL は特定のゲートウェイサーバー用のものとなります。



設定の入力が完了したら、［次へ］を押します

5. ［作成］をクリックしてこの構成を適用します。



6. 展開環境が適用されたら、［完了］をクリックします。
7. ユーザーが Gateway を介してストアにアクセスできるようにするには、リモートユーザーアクセスを構成します。

PowerShell SDK

PowerShell SDK を使用してゲートウェイを追加するには、コマンドレットNew-STFRoamingGatewayを呼び出します。

Citrix Gateway の編集

1. ［**Citrix Gateway** の管理］ウィンドウで、変更するゲートウェイをクリックし、［編集］を押します。

   パラメーターの説明については、「Citrix Gateway の追加」を参照してください

2. ［保存］を押して変更を保存します。

PowerShell SDK

PowerShell SDK を使用してゲートウェイ構成を変更するには、コマンドレットSet-STFRoamingGatewayを呼び出します。

Citrix Gateway の削除

1. [**Citrix Gateway** の管理] ウィンドウで、変更するゲートウェイをクリックし、[削除] を押します。
2. 確認のウィンドウで [はい] を押します。

PowerShell SDK

PowerShell SDK を使用してゲートウェイを削除するには、Remove-STFRoamingGatewayを呼び出します。

Citrix Gateway のインポート

June 6, 2024

Citrix Gateway 管理コンソールのリモートアクセス設定は、StoreFront で構成されているものと同じように構成する必要があります。この記事では、Citrix Gateway と StoreFront を適切に構成して連携させるために Citrix Gateway 仮想サーバーをインポートする方法について説明します。

要件

- 複数のゲートウェイ仮想サーバーを ZIP ファイルにエクスポートするには、NetScaler 11.1.51.21 以降が必要です。

  > 注:
  >
  > Citrix Gateway は、Citrix Virtual Apps and Desktops ウィザードを使用して作成されたゲートウェイ仮想サーバーのみをエクスポートできます。

- Citrix Gateway により生成される ZIP ファイル内の GatewayConfig.json ファイルに記載されているすべての STA（Secure Ticket Authority）サーバーの URL を DNS が解決でき、StoreFront がアクセスできる必要があります。
- Citrix Gateway で生成される ZIP ファイル内の GatewayConfig.json ファイルには、StoreFront サーバー上にある既存の Citrix Receiver for Web サイトの URL が含まれている必要があります。Citrix Gateway バージョン 11.1 以降は、エクスポート用の ZIP ファイルの生成前に StoreFront サーバーにアクセスして既存のストアと Citrix Receiver for Web サイトをすべて列挙し、この処理を自動で行います。

- StoreFront で、インポートしたゲートウェイを使用して認証できるように、ゲートウェイ VPN 仮想サーバーの IP アドレスへの DNS のコールバック URL を解決できる必要があります。

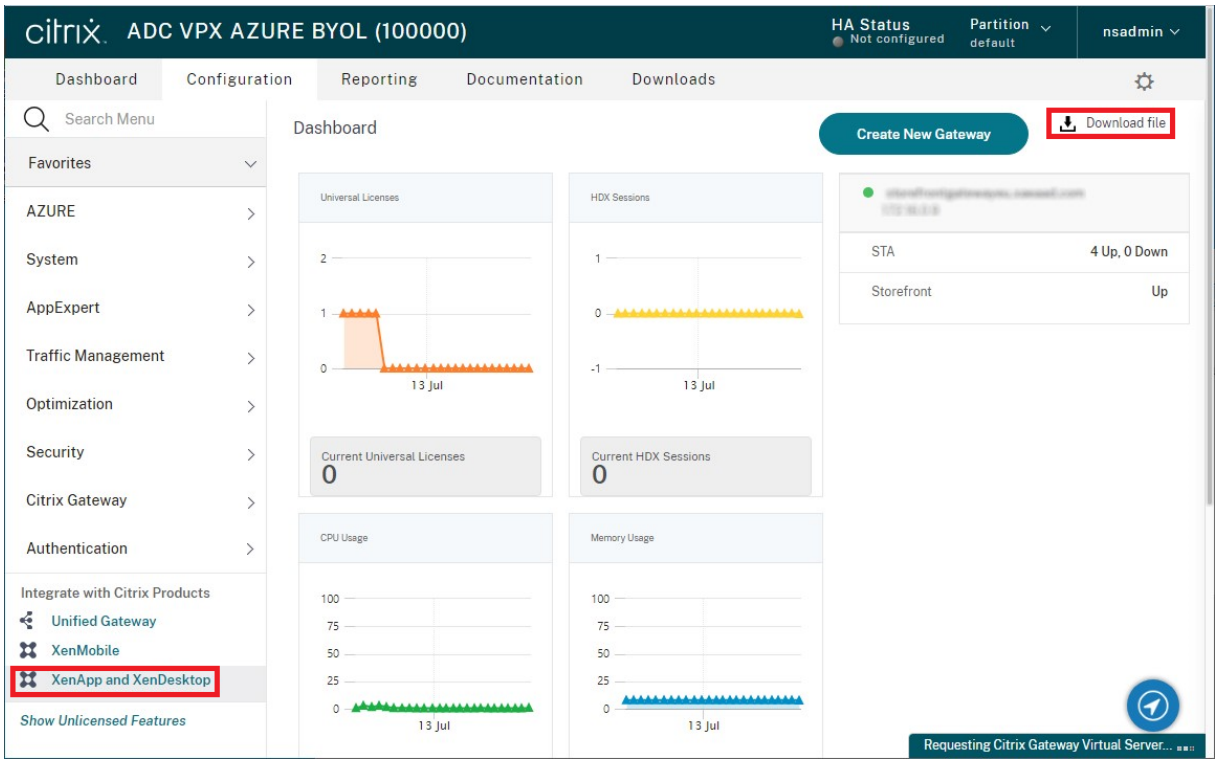
  StoreFront でゲートウェイ URL を解決できる場合、使用するコールバック URL とポートの組み合わせは、通常、ゲートウェイ URL とポートの組み合わせと同じものにします。

  または

  環境内で外部と内部に違う DNS 名前空間を使用する場合は、コールバック URL とポートの組み合わせをゲートウェイ URL とポートの組み合わせとは異なるものにしても構いません。ゲートウェイを DMZ 内に配置して<example.com>の URL を使用しており、StoreFront はプライベートの社内ネットワークに配置して<example.local>の URL を使用している場合、<example.local>コールバック URL を使用して DMZ 内のゲートウェイ仮想サーバーへポイントバックすることができます。

Citrix Gateway から構成をエクスポート

1. Citrix Gateway にログオンします。
2. ［構成］タブに移動します
3. ［Integrate with Citrix Products］の下の［XenApp and XenDesktop］を選択します。
4. 右上の［Download file］をクリックします。



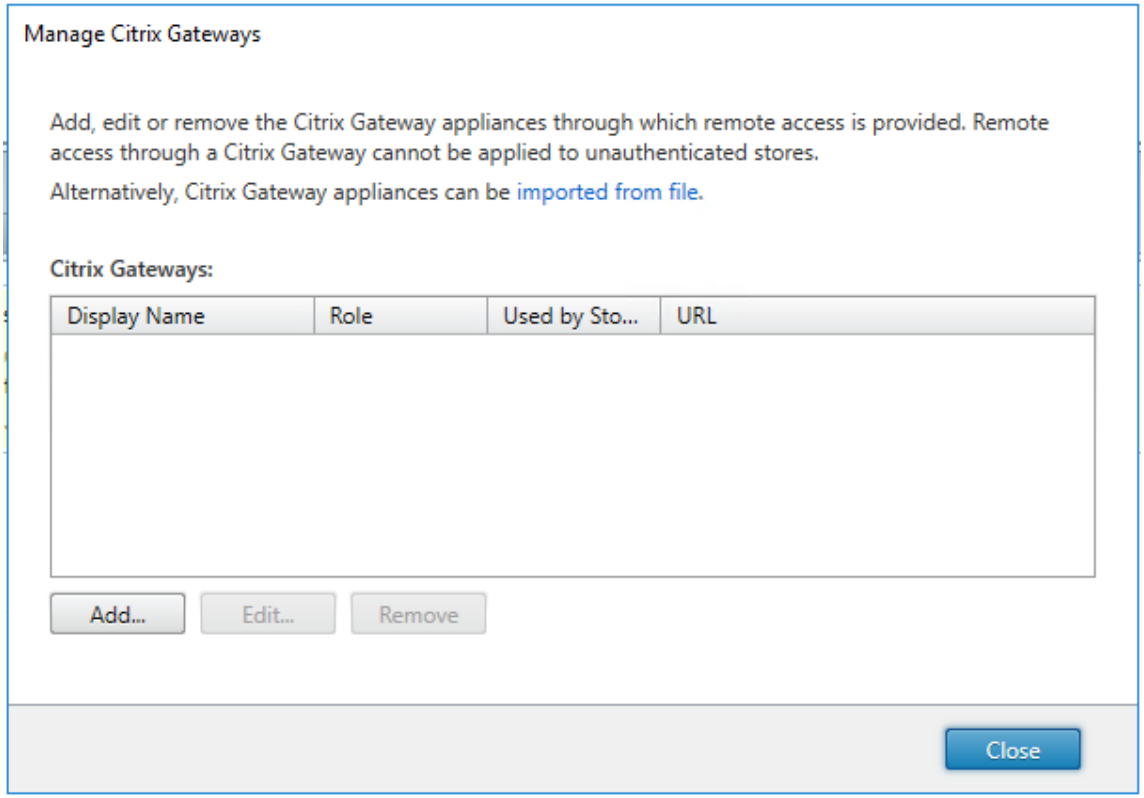
1. すべてのゲートウェイの構成をダウンロードするか、特定のゲートウェイの構成をダウンロードするかを選択します。

コンソールを使用して **Citrix Gateway** をインポートする

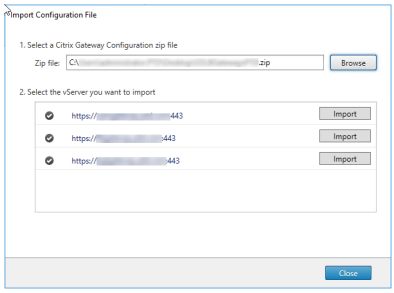
同じインポートファイルを使用して、1 つ以上の Citrix Gateway 仮想サーバー構成をインポートできます。異なる Citrix Gateway からの複数のゲートウェイ仮想サーバーがある場合は、複数のインポートファイルを使用する必要があります。

> 重要:
>
> Citrix Gateway からエクスポートされた構成ファイルを手動で編集することはできません。

1. Citrix StoreFront 管理コンソールの左ペインで［ストア］を選択して、［操作］ペインの［**Citrix Gateway** の管理］をクリックします。
2. ［Citrix Gateway の管理］画面で、［ファイルからインポート］リンクをクリックします。

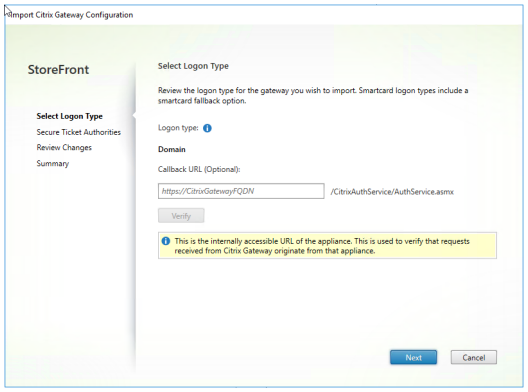


3. Citrix Gateway 仮想サーバー構成ファイルを参照します。
4. 選択した ZIP ファイルに含まれるゲートウェイ仮想サーバーの一覧が表示されます。インポートするゲートウェイ仮想サーバーを選択し、［インポート］をクリックします。仮想サーバーを繰り返してインポートする場合、［インポート］ボタンは［更新］ボタンになります。［更新］をクリックした場合、後でゲートウェイを上書きするか新規に作成することができます。



5. 選択したゲートウェイのログオンの種類を確認し、必要に応じてコールバック **URL** を指定します。［ログオンの種類］の一覧から、Citrix Workspace アプリユーザー向けに Citrix Gateway 上で構成した認証方法を選択します。ログオンの種類によってはコールバック URL が必要になります（表を参照）。

   - ［確認］をクリックして、コールバック URL が有効であり StoreFront サーバーから到達可能であることをチェックします。

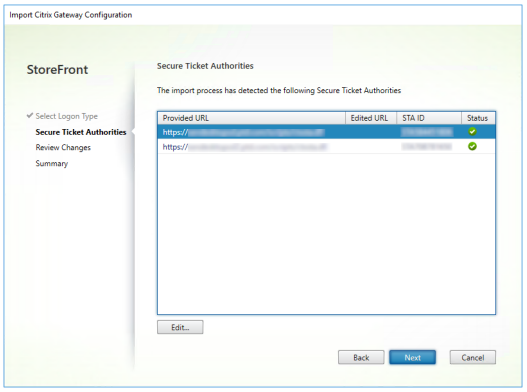


コンソールでのログオンタイプ	**JSON** ファイルでの **LogonType**	コールバック **URL** が必須
ドメイン	ドメイン	いいえ
ドメインおよびセキュリティトークン	DomainAndRSA	いいえ
セキュリティトークン	RSA	はい
スマートカード - フォールバックがありません	SmartCard	はい
スマートカード - ドメイン	SmartCardDomain	はい
スマートカード - ドメインおよびセキュリティトークン	SmartCardDomainAndRSA	はい
スマートカード - セキュリティトークン	SmartCardRSA	はい
スマートカード - SMS 認証	SmartCardSMS	はい
SMS 認証	SMS	はい

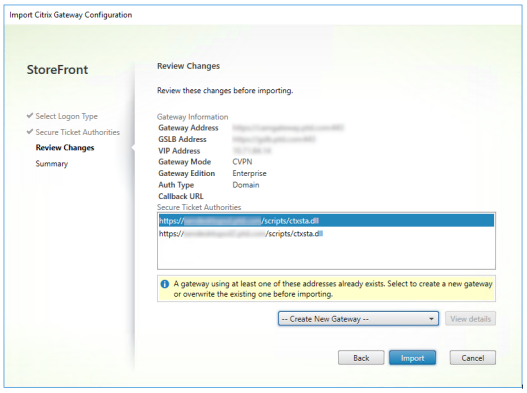
コールバック URL が必須な場合、ZIP ファイルに記載されているゲートウェイ URL に基づいて StoreFront によりコールバック URL が自動で入力されます。この URL は、適切な Citrix Gateway VIP にポイントバックする有効な URL に変更できます。GSLB ゲートウェイの場合、インポートするゲートウェイごとに固有のコールバック URL が必要です。

スマートアクセスまたはパスワードレス認証を使用する場合、コールバック URL は必須です。

6. ［次へ］をクリックします。
7. StoreFront が、ZIP ファイルに記載されているすべての STA（Secure Ticket Authority）サーバーの URL へ DNS を使用してアクセスし、これらのサーバーが動作中の STA チケット発行サーバーであることを確認します。いずれかの STA URL が無効である場合、インポートは中断されます。



8. ［次へ］をクリックします。
9. インポートの詳細を確認します。ゲートウェイ URL とポートの組み合わせ（ゲートウェイ URL: ポート）の同じゲートウェイが既に存在する場合は、ボックスの一覧からゲートウェイを選択して上書きするか、新規ゲートウェイを作成します。



StoreFront では「ゲートウェイ URL: ポート」の組み合わせを使用して、インポートするゲートウェイが（更新が必要になる）既存のゲートウェイと一致するかどうかを判定します。ゲートウェイの「ゲートウェイ URL: ポート」の組み合わせが異なる場合、StoreFront ではこのゲートウェイを新規ゲートウェイとして扱います。次のゲートウェイ設定の表に、更新可能な設定を示します。

ゲートウェイの設定	更新の可否
「ゲートウェイ URL: ポート」の組み合わせ	いいえ
GSLB の URL	はい
Netscaler の信頼証明書と捺印	はい
コールバック URL	はい
Receiver for Web サイトの URL	はい
ゲートウェイのアドレス/VIP	はい
STA の URL および STA の ID	はい
すべてのログオンの種類	はい

10. ［インポート］をクリックします。StoreFront サーバーがサーバーグループに含まれている場合、インポートしたゲートウェイ設定をグループ内の他のサーバーに反映させるように求めるメッセージが表示されます。
11. ［完了］をクリックします。

別の仮想サーバー構成をインポートする場合は、上記の手順を繰り返します。

> 注:
>
> 別のゲートウェイを使用するように Citrix Workspace アプリを構成していない場合、ストアのデフォルトゲートウェイが、Citrix Workspace アプリが接続に使用するゲートウェイとなります。ストアのゲートウェイが構成されていない場合、ZIP ファイルからインポートされた 1 番目のゲートウェイが、Citrix Workspace アプリが使用するデフォルトゲートウェイになります。後でゲートウェイをインポートしても、ストアに設定済みのデフォルトゲートウェイは変更されません。

PowerShell を使用して複数の **Citrix Gateway** をインポートする

Read-STFNetScalerConfiguration

- 現在ログオンしている StoreFront 管理者のデスクトップに ZIP ファイルをコピーします。
- Citrix Gateway 仮想サーバー構成ファイルの ZIP ファイルの内容をメモリに読み込み、インデックス値を使用してファイルに含まれる 3 つのゲートウェイを確認します。

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
     USERPROFILE\desktop\GatewayConfig.zip"
2 <!--NeedCopy-->
```

Read-STFNetScalerConfiguration コマンドレットを使用して、Netscaler の ZIP インポートパッケージからメモリ内に読み込んだ 3 つのゲートウェイオブジェクトを表示します。


```
$ImportedGateways.Document.Gateways[0]
$ImportedGateways.Document.Gateways[1]
$ImportedGateways.Document.Gateways[2]

GatewayMode            : CVPN
CallbackUrl            :
GslbAddressUri         : https://gslb.example.com/
AddressUri             : https://emeagateway.example.com/
Address                : https://emeagateway.example.com:443
GslbAddress            : https://gslb.example.com:443
VipAddress             : 10.0.0.1
Stas                   : {
 STA298854503, STA909374257 }

StaLoadBalance         : True
CertificateThumbprints : {
 F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType        : Domain
GatewayEdition         : Enterprise
ReceiverForWebSites    : {
 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }


GatewayMode            : CVPN
CallbackUrl            :
GslbAddressUri         : https://gslb.example.com/
AddressUri             : https://emeagateway.example.com/
Address                : https://emeagateway.example.com:444
GslbAddress            : https://gslb.example.com:443
VipAddress             : 10.0.0.2
Stas                   : {
 STA298854503, STA909374257 }

StaLoadBalance         : True
CertificateThumbprints : {
 F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType        : DomainAndRSA
GatewayEdition         : Enterprise
ReceiverForWebSites    : {
 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }


GatewayMode            : CVPN
CallbackUrl            : https://emeagateway.example.com:445
GslbAddressUri         : https://gslb.example.com/
AddressUri             : https://emeagateway.example.com/
Address                : https://emeagateway.example.com:445
GslbAddress            : https://gslb.example.com:443
VipAddress             : 10.0.0.2
```



```
Stas                    : {
 STA298854503, STA909374257 }

StaLoadBalance          : True
CertificateThumbprints : {
 F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType         :SmartCard
GatewayEdition          : Enterprise
ReceiverForWebSites     : {
 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }

<!--NeedCopy-->
```

CallbackURL を指定しない **Import-STFNetScalerConfiguration**

現在ログインしている StoreFront 管理者のデスクトップに ZIP ファイルをコピーします。Citrix Gateway 構成の ZIP インポートパッケージをメモリに読み込み、インデックス値を使用してファイルに含まれる 3 つのゲートウェイを確認します。

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
<!--NeedCopy-->
```

Import-STFNetScalerConfiguration コマンドレットを使用し、必要なゲートウェイインデックスを指定して StoreFront に新しい 3 つのゲートウェイをインポートします。**-Confirm:$False** パラメーターを使用することで、Powershell GUI からゲートウェイのインポートを 1 つ 1 つ許可するように求められなくなります。1 度に 1 つのゲートウェイをインポートする場合、このパラメーターは削除してください。

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -Confirm:$False
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -Confirm:$False
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -Confirm:$False
<!--NeedCopy-->
```

任意の **CallbackURL** を指定する **Import-STFNetScalerConfiguration**

Import-STFNetScalerConfiguration コマンドレットと-callbackUrl パラメーターを使用し、任意のコールバック URL を指定して 3 つの新しいゲートウェイを StoreFront へインポートします。

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"

```



```
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443 -
    Confirm:$False
4
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -
    Confirm:$False
6
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -
    Confirm:$False
8 <!--NeedCopy-->
```

Import-STFNetScalerConfiguration を使用してインポートファイルに格納されている認証方法を上書きし、任意の **CallbackURL** を指定

Import-STFNetScalerConfiguration コマンドレットと-callbackUrl パラメーターを使用し、任意のコールバック URL を指定して 3 つの新しいゲートウェイを StoreFront へインポートします。

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
2
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:443" -Confirm:$False
4
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:444" -Confirm:$False
6
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:445" -Confirm:$False
8 <!--NeedCopy-->
```

NetScaler ADC による負荷分散

June 6, 2024

ここでは、すべてのアクティブな負荷分散構成に 2 つ以上の StoreFront サーバーを含む StoreFront サーバーグループを展開する方法について説明します。サーバーグループの StoreFront サーバー間で Citrix Workspace アプリとブラウザーからの受信要求を負荷分散するため、NetScaler ADC アプライアンスを構成する方法について詳しく説明します。

負荷分散化される展開のサーバー証明書の要件

商用証明機関から証明書を購入する、またはエンタープライズ証明機関から発行しようとする前に、次のオプションについて検討します。

- オプション **1**： **.example.com* ワイルドカード証明書を NetScaler ADC アプライアンス負荷分散仮想サーバーと StoreFront サーバーグループノードの両方で使用する。これにより構成が簡素化され、将来的には証明書を置き換える必要なく追加の StoreFront サーバーを増やすことができます。
- オプション **2**：サブジェクトの別名（SAN）を含む証明書を NetScaler ADC アプライアンス負荷分散仮想サーバーと StoreFront サーバーグループノードの両方で使用する。すべての StoreFront サーバーの完全修飾ドメイン名（FQDN）と一致する証明書内の追加の SAN はオプションですが、これにより StoreFront 展開環境に柔軟性がもたらされるため、推奨されます。

StoreFront サーバーグループ負荷分散用の **DNS** レコードの作成

選択した共用 FQDN 用に DNS A および PTR レコードを作成します。ネットワーク内のクライアントはこの FQDN を使用して、NetScaler ADC アプライアンスロードバランサーを使用する StoreFront サーバーにアクセスします。

例：`storefront.example.com`が負荷分散仮想サーバーの仮想 IP（VIP）に解決されます。

StoreFront サーバーの構成

負荷分散を行うすべての StoreFront サーバーは、サーバー間の構成を同期して同一に構成されるようにしている、StoreFront サーバーグループの一部として構成する必要があります。サーバーグループへのサーバーの追加について詳しくは、「既存のサーバーグループへの参加」を参照してください。

ロードバランサーと StoreFront サーバー間の通信が暗号化されるように、各サーバーを HTTPS 用に構成する必要があります。「HTTPS による StoreFront のセキュリティ保護」を参照してください。証明書は、共通名（CN）またはサブジェクトの別名（SAN）として負荷分散された FQDN を含む必要があります。

サーバーグループのベース URL をロードバランサーの URL に設定します。ベース URL を変更するには、Citrix StoreFront 管理コンソール内の左側のペインで ［サーバーグループ］を右クリックし、［ベース **URL** の変更］をクリックします。ロードバランサーの仮想サーバーの URL を入力します。

必要に応じて **HTTPS** 用に **Citrix Service Monitor** を構成する

StoreFront のインストールには、**Citrix Service Monitor** Windows サービスが含まれています。このサービスは他のサービスには依存せず、他の重要な StoreFront サービスのヘルスを監視します。これにより、NetScaler ADC および他のサードパーティアプリケーションが StoreFront サーバー展開の相対的なヘルスを監視できるようになります。

デフォルトでは、モニターはポート 8000 で HTTP を使用します。必要に応じて、この設定をポート 443 で HTTPS を使用するように変更できます。

1. プライマリ StoreFront サーバーで PowerShell Integrated Scripting Environment（ISE）を開き、以下のコマンドを実行してデフォルトモニターを HTTPS 443 に変更します:

```
$ServiceUrl = "https://localhost:443/StorefrontMonitor"
Set-STFServiceMonitor -ServiceUrl $ServiceUrl
Get-STFServiceMonitor
<!--NeedCopy-->
```

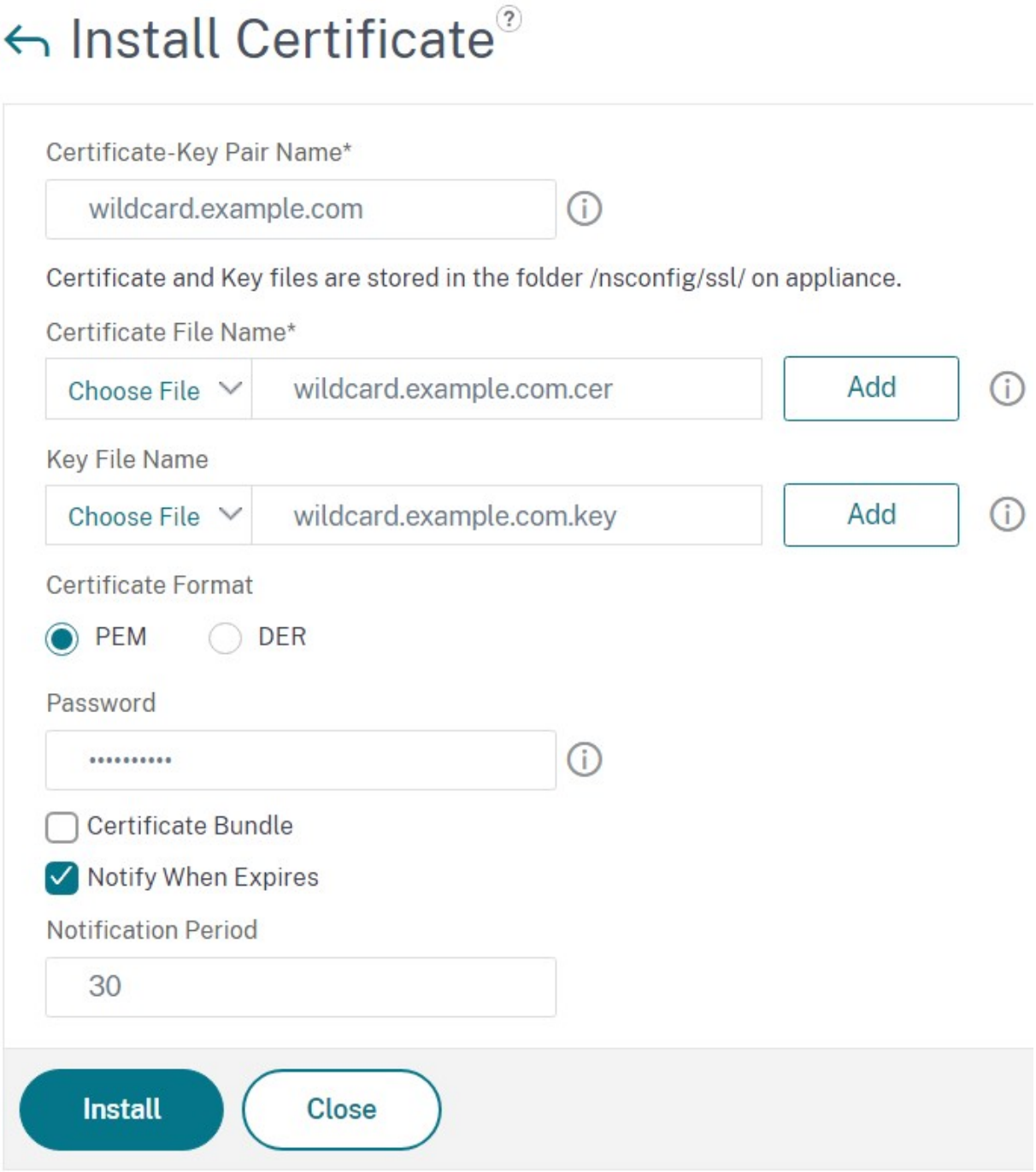
2. 変更が完了したら、StoreFront サーバーグループ内の外のすべてのサーバーに変更を反映させます。
3. モニターでクイックテストを実行するには、StoreFront サーバー、または StoreFront サーバーへネットワークアクセスするほかの任意のマシンでブラウザーに次の URL を入力します。ブラウザーは、すべての StoreFront サービスの状態について XML サマリーを返します。

   ```
   https://<loadbalancingFQDN>/StoreFrontMonitor/GetSFServicesStatus
   ```

NetScaler ロードバランサーの構成

NetScaler ADC での **SSL** 証明書の構成

1. NetScaler ADC アプライアンス管理 GUI にログオンします。
2. [**Traffic Management**] > [**SSL**] > [**Certificates**] > [**Server Certificates**] を選択します。
3. [**Install**] をクリックします。
4. [**Install Server Certificate**] ページで、証明書とキーのペアの名前を入力し、[**Choose File**] をクリックして証明書ファイルを参照します。証明書ファイルに秘密キーが含まれていない場合は、追加でキーファイルを選択する必要があります。

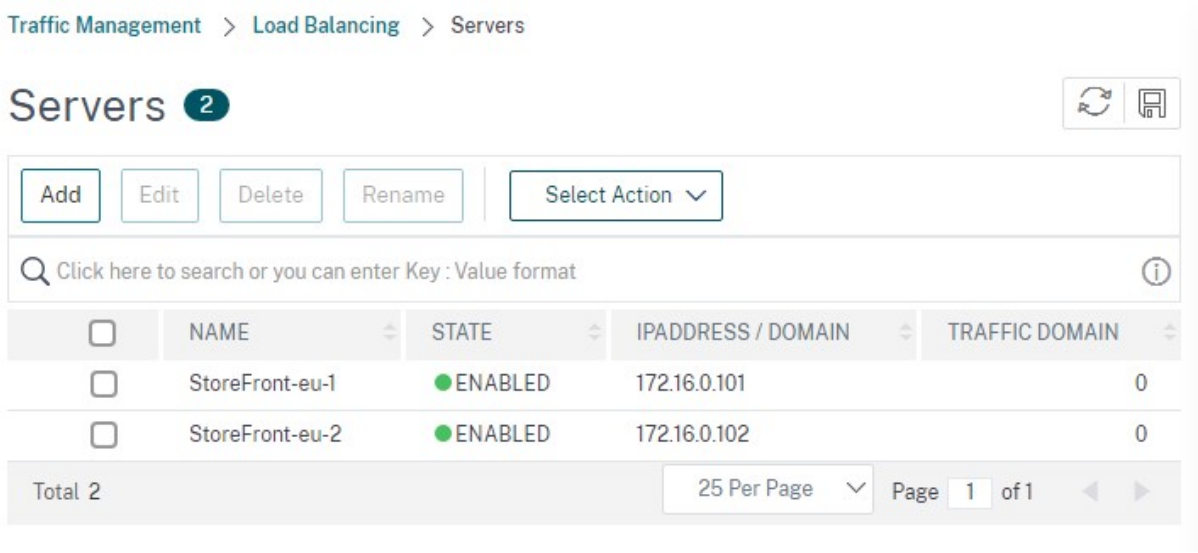


個々の **StoreFront** サーバーノードの **NetScaler ADC** アプライアンスロードバランサーへの追加

1. [**Traffic Management**] > [**Load Balancing**] > [**Servers**] の順に移動します。[**Add**] をクリックし、負荷分散する StoreFront サーバーをそれぞれ追加します。

   例 = StoreFront-eu-1 および StoreFront-eu-2 という名前の 2 台の StoreFront サーバー

2. IP ベースのサーバー構成を使用し、各 StoreFront ノードのサーバー IP アドレスを入力します。



StoreFront モニターを定義して、サーバーグループ内のすべての **StoreFront** ノードをチェックします

1. NetScaler ADC 管理 GUI にログオンします。
2. [**Traffic Management**] > [**Load Balancing**] > [**Monitors**] > [**Add**] の順に選択し、*StoreFront* を呼び出す新しいモニターを追加し、すべてのデフォルトの設定を受け入れます。
3. [**Type**] ドロップダウンの一覧から [**StoreFront**] を選択します。
4. StoreFront モニターを HTTPS 用に構成した場合は、[セキュア] オプションが選択されていることを確認してください。それ以外の場合は、このオプションを選択解除したままにし、ポート 8000 を入力します。
5. [バックエンドサービスの確認] オプションを選択します。このオプションにより、StoreFront サーバーで監視サービスの実行が有効になります。StoreFront サーバーで実行する Windows サービスをプローブして StoreFront サービスが監視され、次のサービスの状態が返されます:

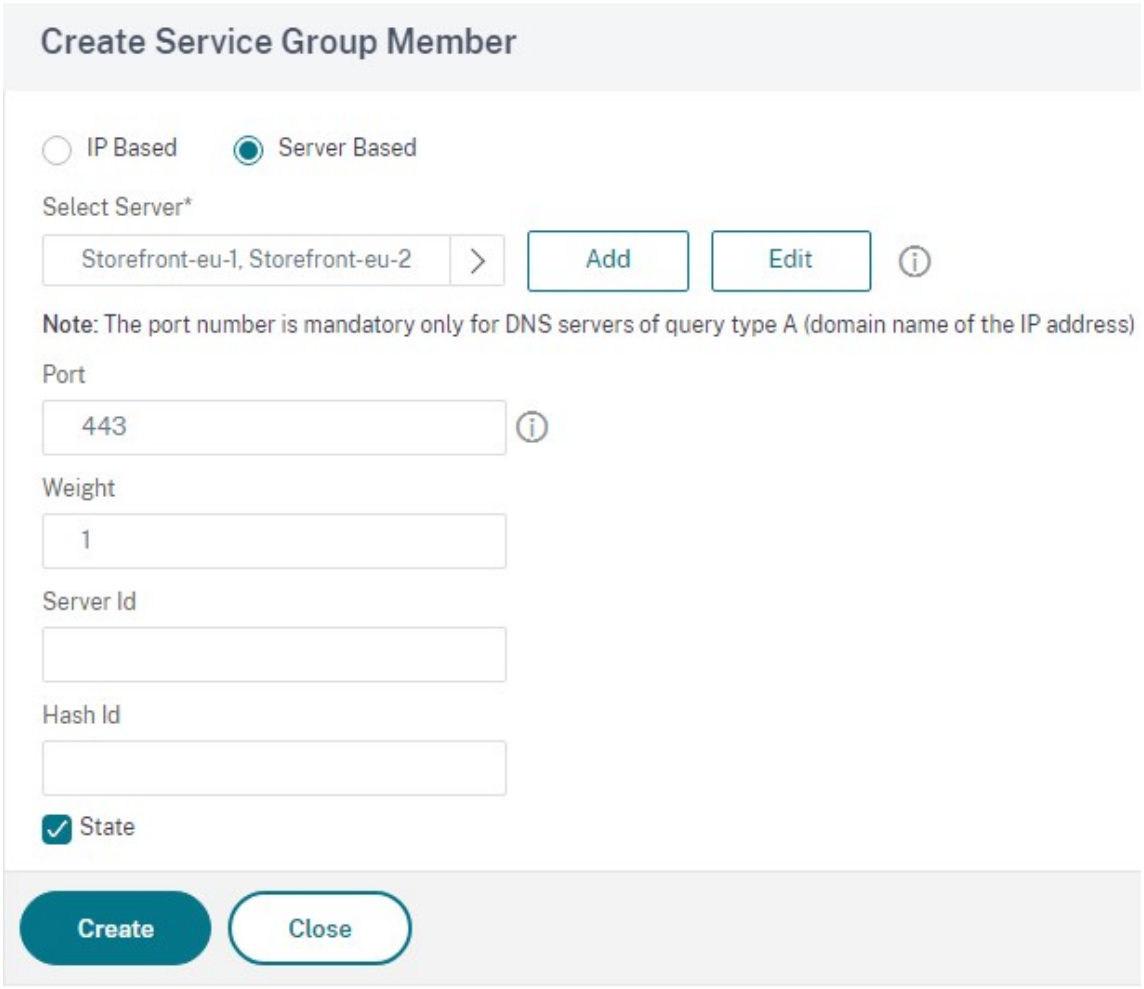
   - W3SVC (IIS)
   - WAS（Windows プロセスアクティブ化サービス）
   - CitrixCredentialWallet
   - CitrixDefaultDomainService

すべての **StoreFront** サーバーを含むサービスグループの作成

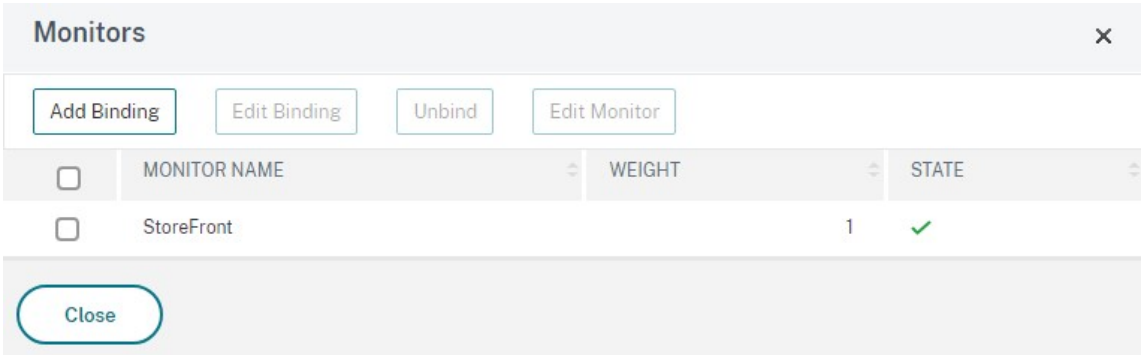
1. [**Traffic Management**] > [**Load Balancing**] > [**Service Groups**] の順に移動します。[**Add**] を押します。HTTPS 経由で StoreFront サーバーに接続するには、SSL のプロトコルを選択します。他の設定はデフォルトのままにします。[**OK**] を押します。

2. サービスグループ内の［サービスグループメンバー］で、［サービスグループメンバーなし］をクリックします。

   a) ［サービスベース］をクリックします。
   b) 以前に定義したサーバーをすべて選択します。
   c) ロードバランサーと StoreFront サーバーの間で SSL を使用するには、ポート 443 を入力します。それ以外の場合は、ポート 80 を入力します。

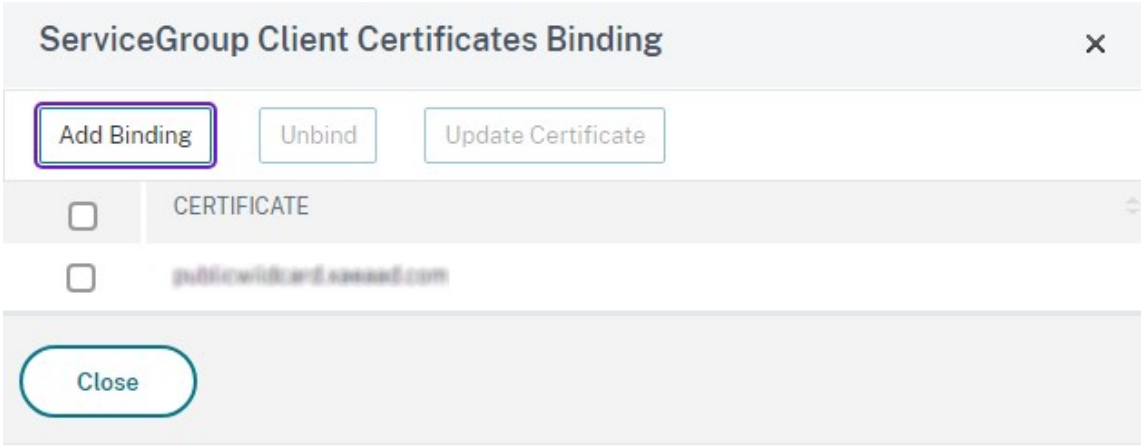


3. ［モニター］セクションを追加し、前に作成した StoreFront モニターを選択します。



4. [証明書] セクションを追加します。

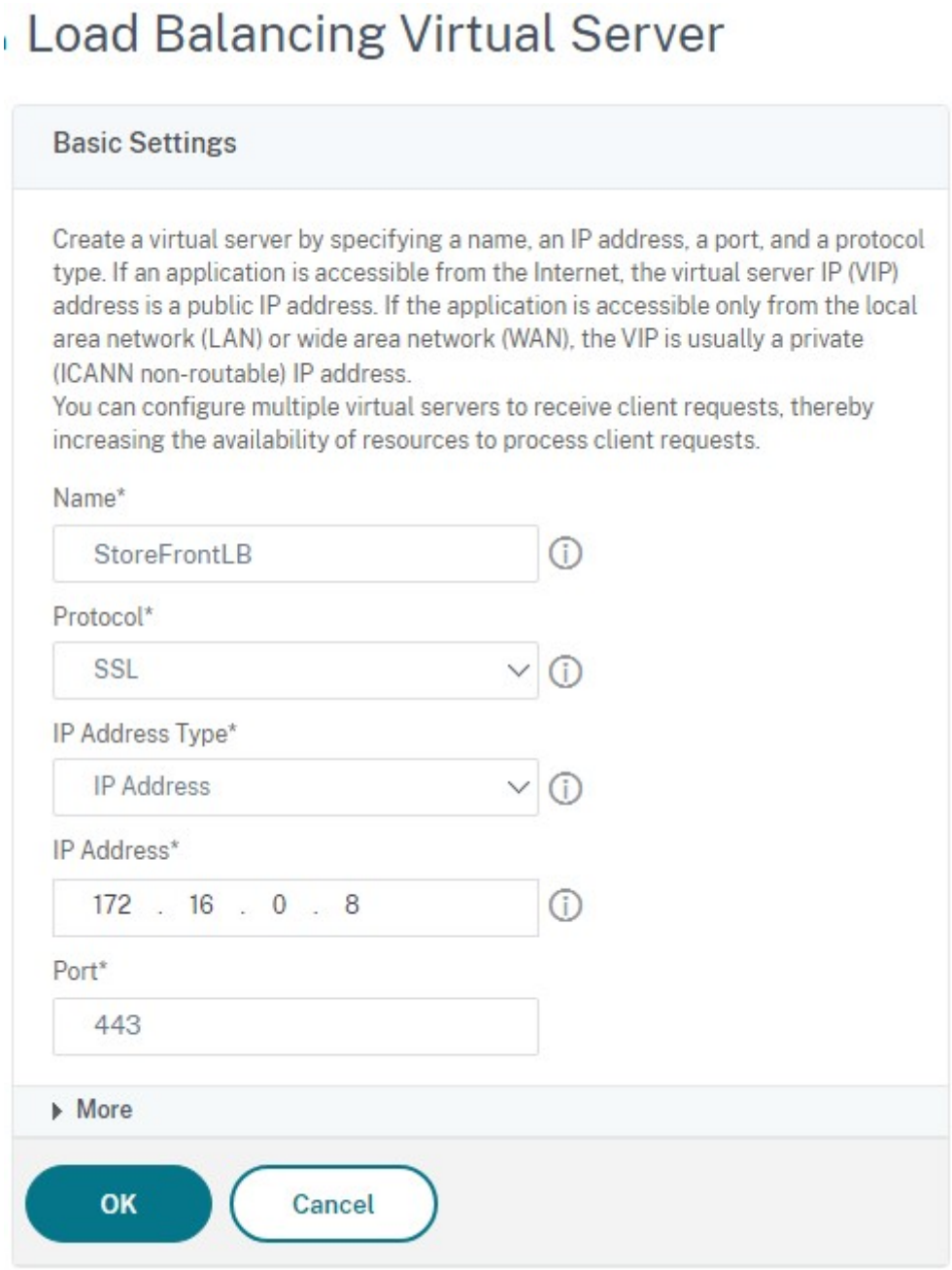
   a) クライアント証明書をバインドします。
   b) 以前にインポートしたサーバー証明書の署名に使用された CA 証明書と、PKI チェーン信頼の一部の可能性があるそのほかの CA をバインドします。



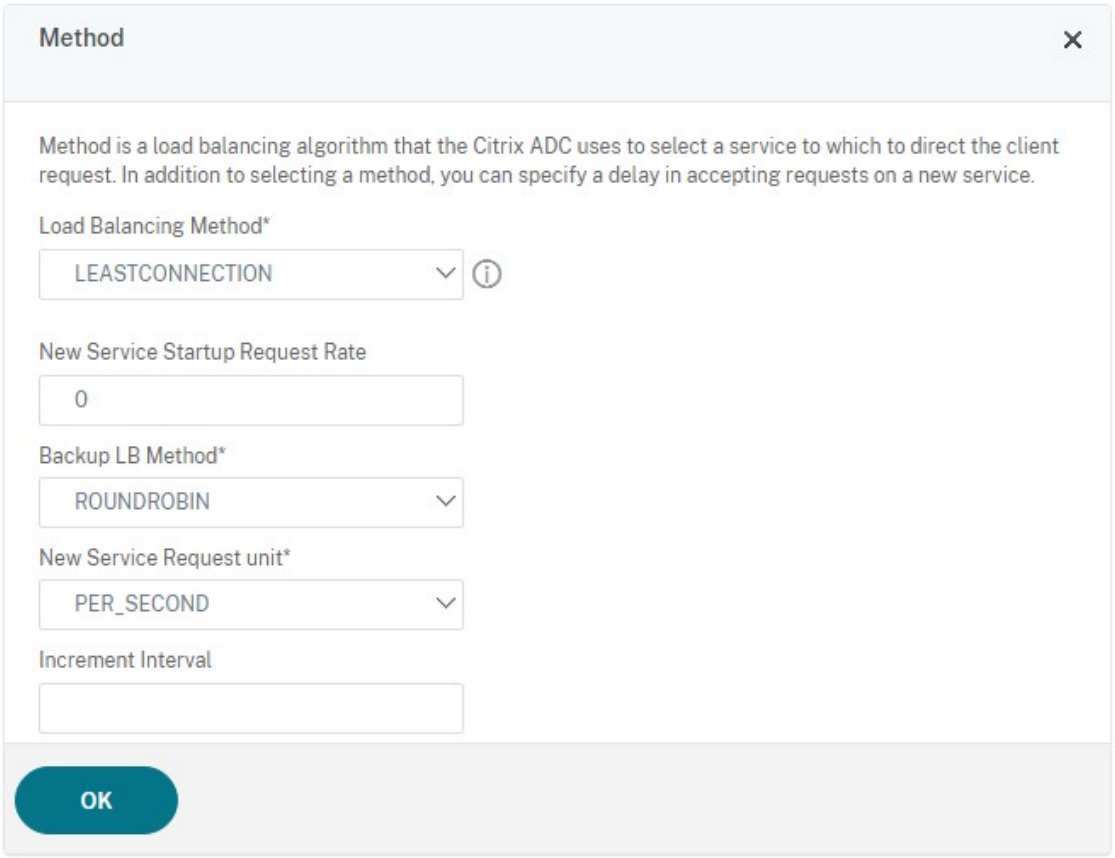
5. [設定]セクションを追加します[クライアント **IP** ヘッダーの挿入]を選択し、ヘッダー名として **X-Forwarded-For** を入力します。これにより、クライアント IP アドレスをCitrix Virtual Apps and Desktops ポリシーで使用できるようになります。

ユーザートラフィック用負荷分散仮想サーバーの作成

1. NetScaler ADC アプライアンス管理 GUI にログオンします。
2. [**Traffic Management**] > [**Load Balancing**] > [**Virtual Servers**] > [**Add**] の順に選択し、新しい仮想サーバーを作成します。
3. 名前を入力し、SSL のプロトコルを選択してポートを入力します。[OK] をクリックして仮想サーバーを作成します。



4. 前に作成したサービスグループを負荷分散仮想サーバーにバインドします。
5. 以前にサービスグループにバインドしたのと同じ SSL および CA 証明書をバインドします。
6. ［方法］セクションを追加し、負荷分散方法を選択します。StoreFront 負荷分散で共通の選択は、［**round robin**］または ［**least connection**］です。



7. ［パーシステンス］セクションを追加します。

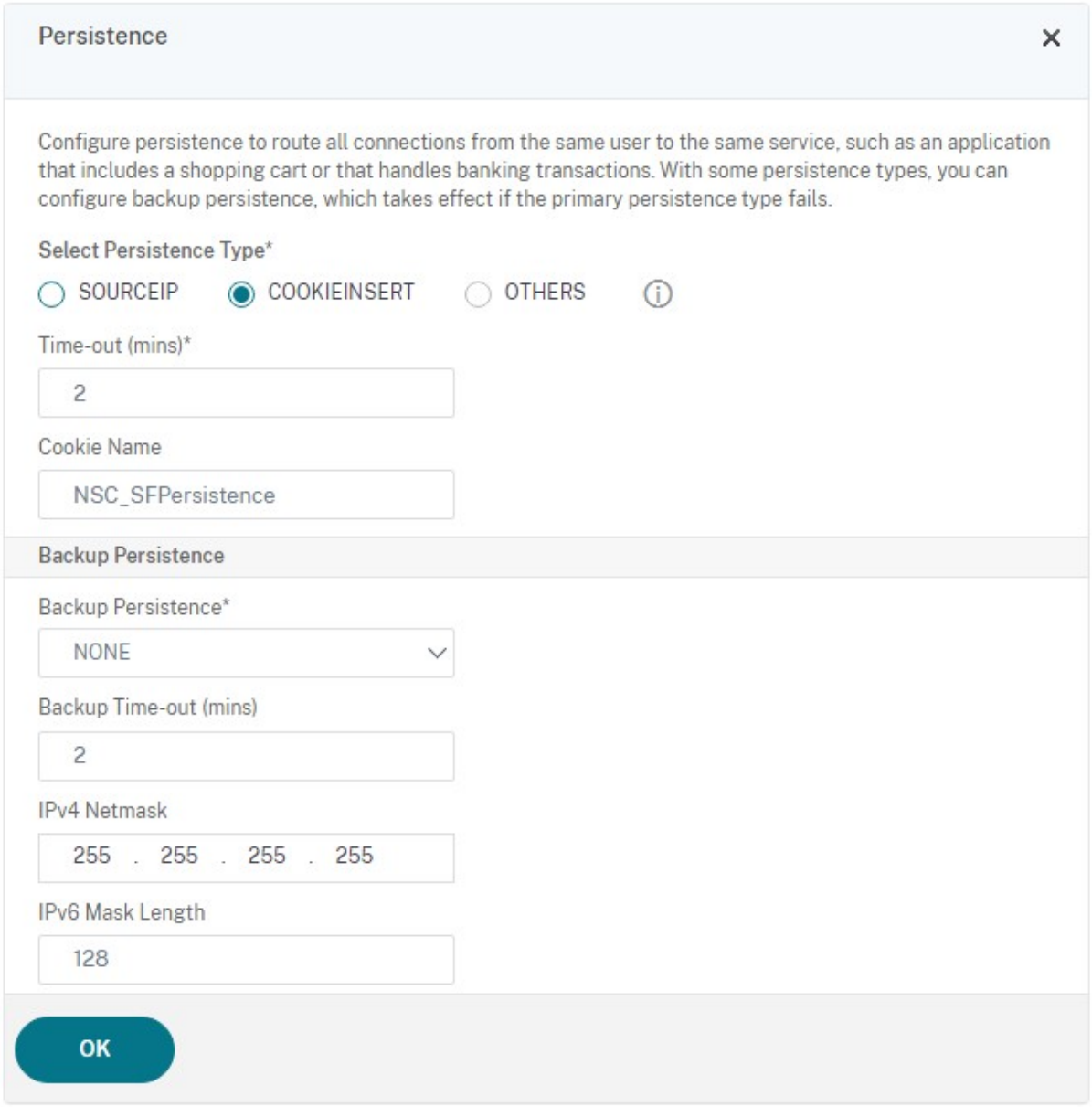
   a) パーシステンス方式を **COOKIEINSERT** に設定します。

   b) タイムアウトを、StoreFront 内のセッションタイムアウト（デフォルトでは 20 分）と同じ設定にします。

   c) cookie に名前を付けます。たとえば、デバッグ時に見つけやすいように **NSC_SFPersistence** という名前を付けます。

   d) バックアップパーシステンスを ［**NONE**］に設定します。

> 注:
>
> クライアントが HTTP Cookie を保存できない場合は、以降の要求に HTTP Cookie が含まれなくなり、パーシステンスは適用されません。



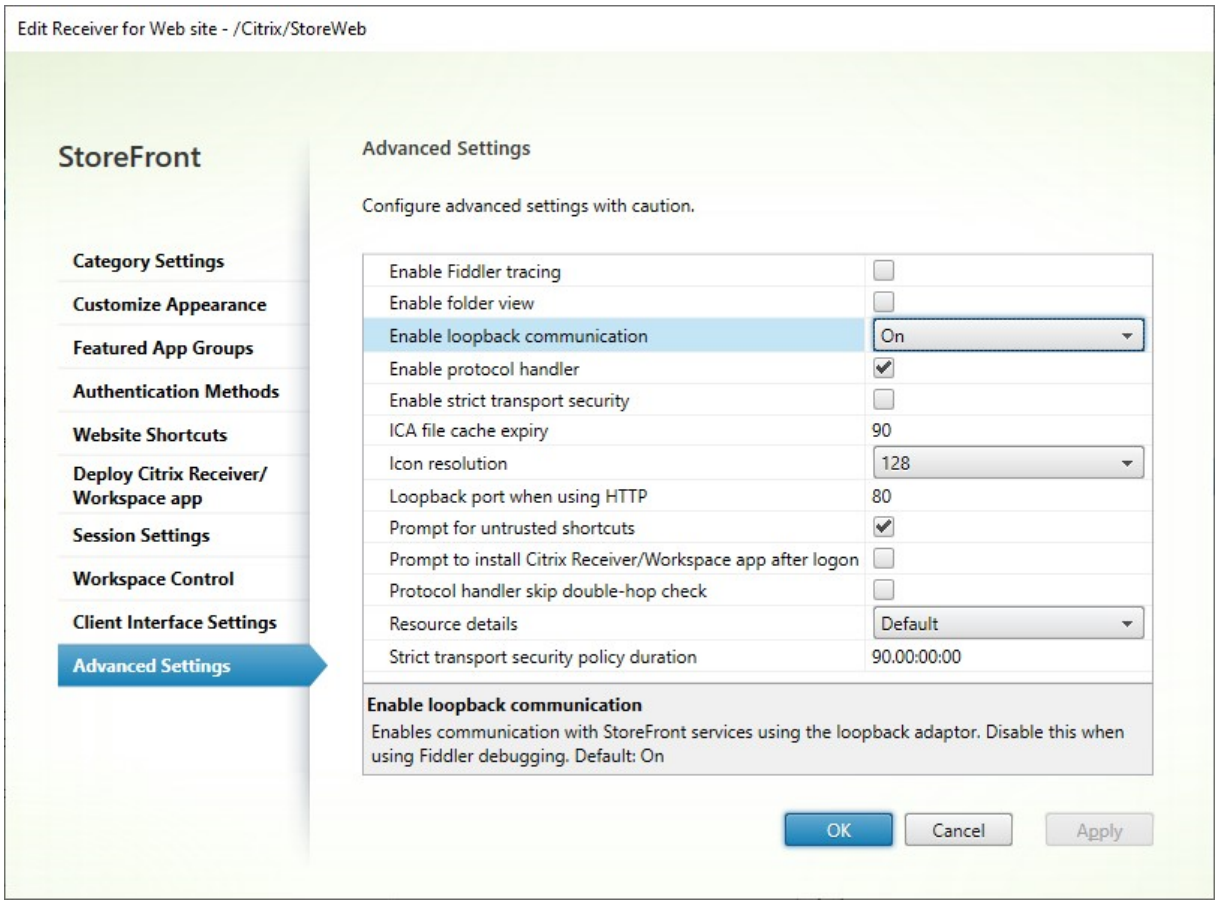
StoreFront ループバックの構成

ベースアドレスがロードバランサーである場合、StoreFront サービス間の内部通信では、トラフィックがロードバランサーにルーティングされ、場合によっては別のサーバーにルーティングされる可能性があります。これにより、パフォーマンスが低下し、予期しない動作が発生します。これを回避するには、StoreFront 設定の ［ループバック通信を有効にする］を使用します。デフォルトでは、これは ［オン］に設定されています。これは、スキーマ（HTTP または HTTPS）をそのまま維持しながら、サービスアドレスのホスト部分をループバック IP アドレス 127.0.0.1 に置き換えることを意味します。これは単一サーバー展開および非 SSL 終了ロードバランサーがある展開で機能します。

ロードバランサーが SSL で終了し、HTTP 経由で StoreFront と通信する場合（非推奨）、StoreFront ループバッ

ク通信を **OnUsingHttp** に構成する必要があります。これは、StoreFront がスキーマを HTTPS から HTTP に変更することを意味します。

1. Citrix StoreFront を開きます。
2. ストアごとに、[**Receiver for Web** サイトの管理] に移動します。Web サイトごとに、[構成] に移動します。
3. [詳細設定] に移動
4. [ループバック通信を有効にする] 設定を **OnUsingHttp** に変更します。



ロードバランサーが SSL で終了し、HTTP 経由で StoreFront と通信する場合（非推奨）、StoreFront ループバック通信を **OnUsingHttp** に構成する必要があります。これは、StoreFront がスキーマを HTTPS から HTTP に変更することを意味します。

サーバーグループ間のサブスクリプション同期用 **NetScaler ADC** ロードバランサーの構成

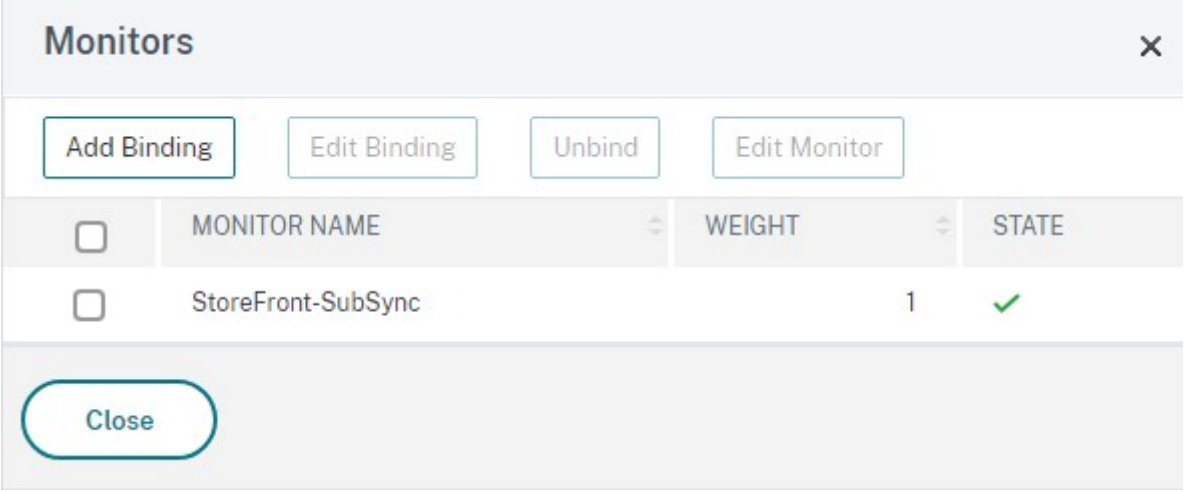
2 つ以上の StoreFront サーバーグループで構成されるマルチサイト展開がある場合は、繰り返しスケジュールでプル戦略を使用して、それらの間でサブスクリプションデータをレプリケートできます。StoreFront サブスクリプションレプリケーションは TCP ポート 808 を使用するため、既存の負荷分散仮想サーバーを HTTP ポート 80 または HTTPS 443 で使用することはできません。このサービスに対して高い可用性を提供するには、展開内の各 NetScaler ADC アプライアンスで 2 つ目の仮想サーバーを作成して、各 StoreFront サーバーグループの TCP ポ

ート 808 へ負荷分散します。

サブスクリプション同期用のサービスグループの構成

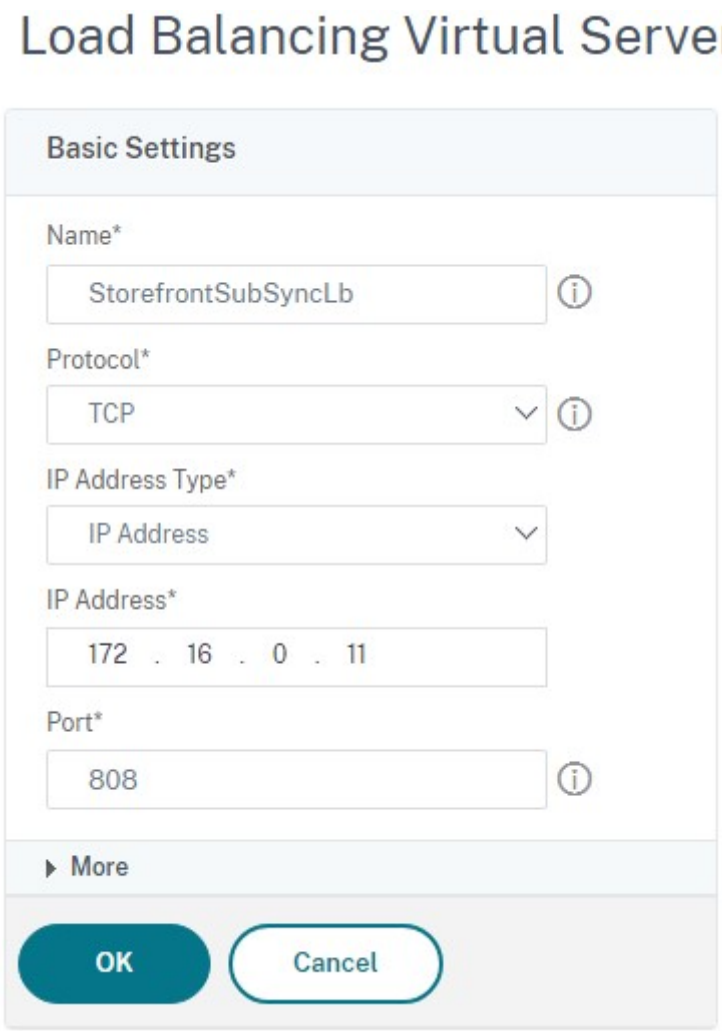
1. NetScaler ADC アプライアンス管理 GUI にログオンします。
2. ［トラフィック管理］**>**［負荷分散］**>**［サービスグループ］**>**［追加］の順に選択します。
3. サービスグループ名を入力し、プロトコルを ［**TCP**］に変更し、［**OK**］をクリックして保存します。
4. ［サービスグループメンバー］セクション内で、［サーバー］セクションで以前定義したすべての StoreFront サーバーノードを追加して ［ポート］を **808** に指定します。
5. ［モニター］セクションを追加します。

   a)「バインドを監視するサービスグループがありません」と表示されている場所をクリックします。
   b)［追加］をクリックします。モニターの［名前］を入力し、その［種類］を［**TCP**］に設定します。［**Create**］をクリックします。
   c)［**Bind**］をクリックします。



サブスクリプション同期用負荷分散仮想サーバーの作成

1. NetScaler ADC アプライアンス管理 GUI にログオンします。
2. ［トラフィック管理］**>**［負荷分散］**>**［仮想サーバー］**>**［追加］の順に選択し、新しいサービスグループを作成します。
3. ［名前］の入力
4. プロトコルを ［**TCP**］に変更します。
5. IP アドレスを入力します。
6. ［ポート］として **808** を入力します。



7. [**OK**] をクリックします。
8. [負荷分散仮想サーバーのサービスグループバインドなし] をクリックし、前に作成したサービスグループを選択して、[バインド] をクリックします。
9. [方法] セクションを追加し、[負荷分散方式] を [**ROUNDROBIN**] に設定します
10. [**Done**] をクリックして変更を完了します。

ロードバランサー経由でサブスクリプションデータを取得するように **StoreFront** を構成する

「サブスクリプション同期の構成」を参照してください。

レプリケーションスケジュールを構成する場合、サブスクリプション同期仮想サーバーの仮想ロードバランサー IP アドレスと一致するサーバーグループアドレスを指定します。

DFA 用の Citrix Gateway および StoreFront の構成

June 6, 2024

拡張認証機能により、Citrix Gateway および StoreFront のフォームベース認証を拡張するための単一のカスタマイズポイントが提供されます。拡張認証 SDK を使用した認証ソリューションを実現するには、Citrix Gateway と StoreFront の間に Delegated Forms Authentication（DFA）を構成する必要があります。DFA プロトコルを使用すると、資格情報検証などの認証フォームの生成と処理をほかのコンポーネントに委任することができます。たとえば、Citrix Gateway は認証を StoreFront に委任し、StoreFront はサードパーティの認証サーバーまたは認証サービスとやりとりします。

Citrix Gateway での DFA の構成については、CTX200383を参照してください。

インストールに関する推奨事項

- Citrix Gateway と StoreFront の間の通信を確実に保護するには、HTTP プロトコルの代わりに HTTPS プロトコルを使用します。
- クラスター展開環境では、すべてのノードに同じサーバー証明書をインストールし、IIS HTTPS バインドを構成してから、構成手順を実行する必要があります。
- StoreFront で HTTPS を構成するときは、Citrix Gateway に StoreFront のサーバー証明書の発行者を信頼された証明書機関として設定する必要があります。

StoreFront クラスターインストールに関する注意事項

- すべてのノードにサードパーティの認証プラグインをインストールしてから、これらのノードをクラスターに追加します。
- 1 つのノードですべての DFA 関連設定を構成し、その内容をほかのノードに反映させます。「DFA の有効化」を参照してください。

DFA の有効化

StoreFront には Citrix の事前共有キー設定を設定する GUI がないので、PowerShell コンソールを使用して DFA をインストールします。

1. DFA をインストールします。DFA はデフォルトではインストールされないので、PowerShell コンソールを使用してインストールする必要があります。

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\
    Receiver StoreFront\Scripts'
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\
    ImportModules.ps1
```



```
Adding snapins
Importing modules
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-DSDFAServer
Id                              : bf694fbc-ae0a-4d56-8749-c945559e897a
ClassType                       : e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc
FrameworkController             : Citrix.DeliveryServices.Framework.FileBased.FrameworkController
ParentInstance                  : 8dd182c7-f970-466c-ad4c-27a5980f716c
RootInstance                    : 5d0cdc75-1dee-4df7-8069-7375d79634b3
TenantId                        : 860e9401-39c8-4f2c-928d-34251102b840
Data                            : {
  }

ReadOnlyData                    : {
 [Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer
                                   vices.Web.Commands], [Tenant, 860e9401-39c8-4f2c-928d-34251102b840] }

ParameterData                   : {
 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f
                                   970-466c-ad4c-27a5980f716c], [TenantId, 860e9401-39c8-4f2c-928d-34251102b840] }

AdditionalInstanceDependencies : {
 b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }

IsDeployed                      : True
FeatureClass                    : Citrix.DeliveryServices.Framework.Feature.FeatureClass
<!--NeedCopy-->
```

2. Citrix Trusted Client を追加します。StoreFront と Citrix Gateway の間で共有シークレットキー（パスフレーズ）を構成します。パスフレーズとクライアント ID は、Citrix Gateway で構成したものと同一である必要があります。

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -passphrase secret
```



```
<!--NeedCopy-->
```

3. DFA Conversation Factory を設定して、すべてのトラフィックをカスタムフォームにルーティングします。Conversation Factory を見つけるには、C:\inetpub\wwwroot\Citrix\Authentication\web.config で ConversationFactory を探します。次に表示例を示します。

```
<example connectorURL="http://Example.connector.url:8080/adapters-sf-aaconnector-webapp">
   <routeTable order="1000">
     <routes>
       <route name="StartExampleAuthentication" url="Example-Bridge-Forms/Start">
         <defaults>
           <add param="controller" value="ExplicitFormsAuthentication" />
           <add param="action" value="AuthenticateStart" />
           <add param="postbackAction" value="Authenticate" />
           <add param="cancelAction" value="CancelAuthenticate" />
           <add param="conversationFactory" value="ExampleBridgeAuthentication" />
           <add param="changePasswordAction" value="StartChangePassword" />
           <add param="changePasswordController" value="ChangePassword" />
           <add param="protocol" value="CustomForms" />
         </defaults>
       </route>
<!--NeedCopy-->
```

4. PowerShell で、DFA Conversation Factory を設定します。この例では、ExampleBridgeAuthentication に設定しています。

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
<!--NeedCopy-->
```

PowerShell の引数では大文字と小文字が区別されません。**-ConversationFactory** は **-conversationfactory** と同意です。

StoreFront のアンインストール

サードパーティの認証プラグインは StoreFront の機能に影響を与えるので、すべてのサードパーティの認証プラグインをアンインストールしてから、StoreFront をアンインストールします。

異なるドメインを使用した認証

June 6, 2024

組織によっては、サードパーティの開発者や契約社員に実稼働環境で公開リソースへのアクセスをポリシーで禁止している場合があります。ここでは、Citrix Gateway 経由で 1 つのドメインに認証することでテスト環境での公開リソースへのアクセスを許可する方法を説明します。これによって、異なるドメインを使用して StoreFront および Receiver for Web サイトへの認証を実行できます。ここで説明された Citrix Gateway 経由の認証は、Receiver for Web サイト経由でログオンするユーザーが対象です。この認証方法は、ネイティブのデスクトップまたはモバイル Citrix Receiver または Citrix Workspace アプリのユーザーは使用できません。

テスト環境のセットアップ

ここでは、production.com という実稼働ドメインと development.com というテストドメインを使用します。

production.com ドメイン

この例では、`production.com`ドメインを以下のようにセットアップします:

- `production.com`の LDAP 認証ポリシーが構成された Citrix Gateway。
- production\testuser1 アカウントおよびパスワードを使用してゲートウェイ経由で認証。

development.com ドメイン

この例では、`development.com`ドメインを以下のようにセットアップします:

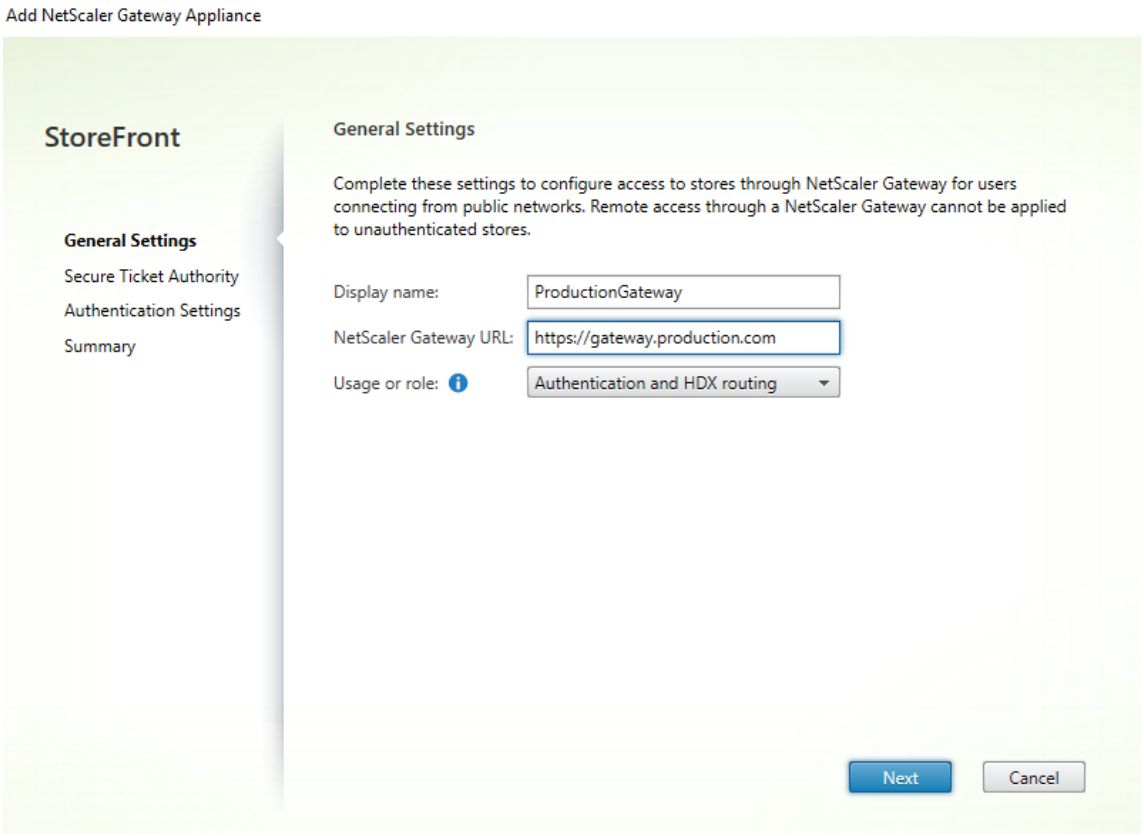
- StoreFront、Citrix Virtual App and Desktops、および VDA はすべて`development.com`ドメイン上にあります。
- production\testuser1 アカウントおよびパスワードを使用して Citrix Receiver for Web サイトに認証。
- 2 つのドメインの間には、信頼関係はありません。

ストアの **Citrix Gateway** の構成

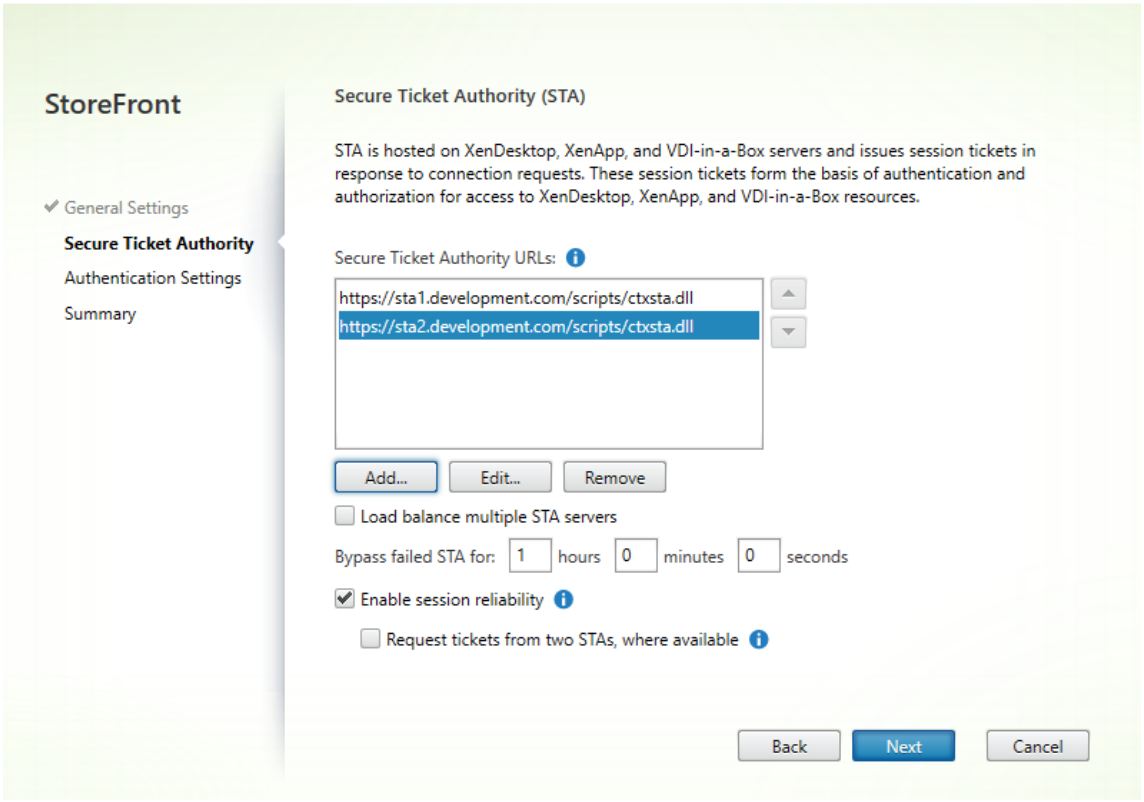
ストアの Citrix Gateway を構成するには:

1. Citrix StoreFront 管理コンソールの左ペインで［ストア］を選択して、［操作］ペインの［**Citrix Gateway** の管理］をクリックします。
2. ［Citrix Gateway の管理］画面で、［追加］をクリックします。

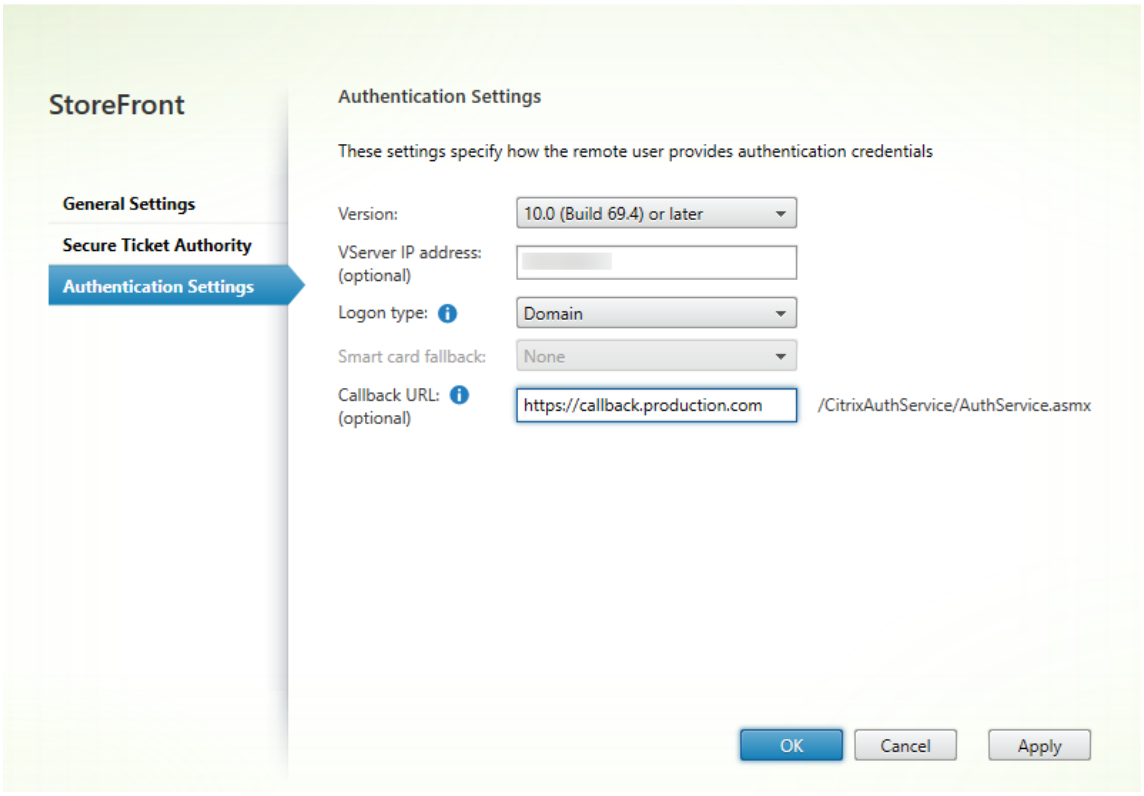
3. 全般設定、Secure Ticket Authority、認証手順を完了します。



Add NetScaler Gateway Appliance



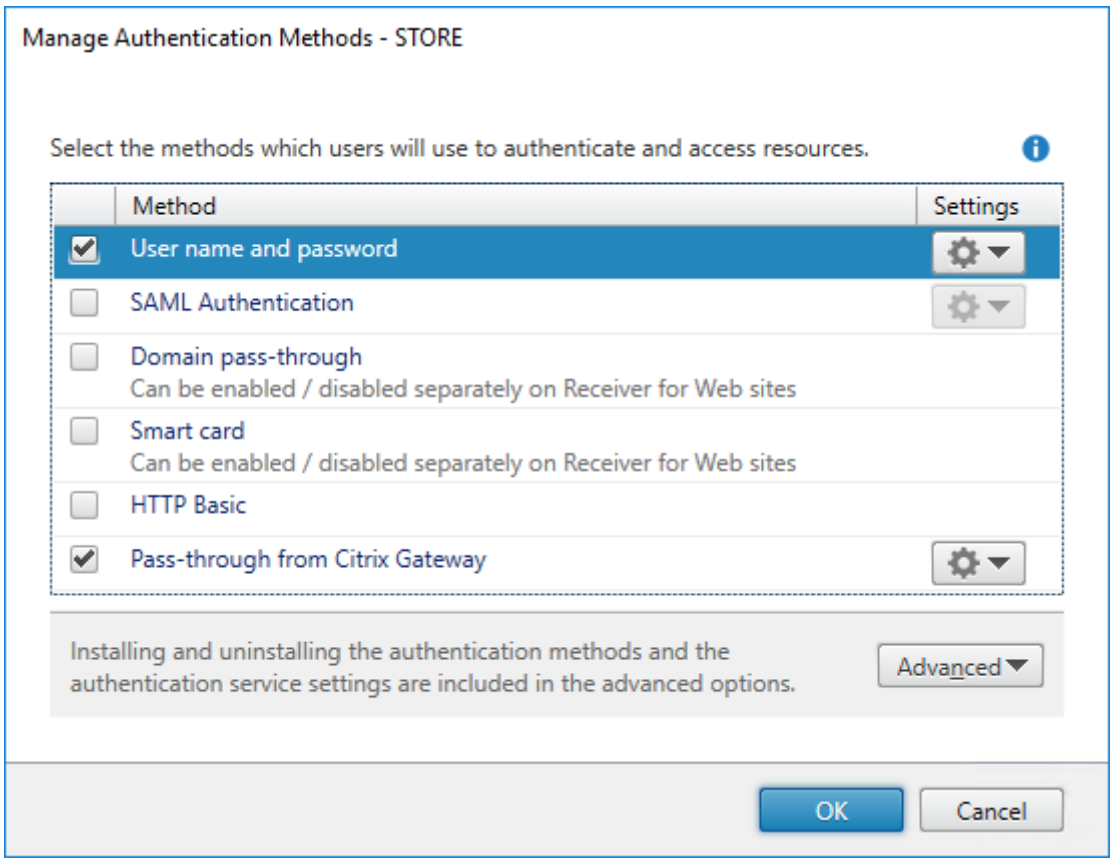
Edit NetScaler Gateway appliance - ProductionGateway



> 注:
>
> 両方のドメインで使用中の DNS サーバーが他方のドメインの FQDN を解決できるよう、DNS 条件付きフォワーダーの追加が必要な場合があります。Citrix Gateway は、`production.com`の DNS サーバーを使用して、`development.com`ドメインで STA サーバーの FQDN を解決できるようにする必要があります。StoreFront は、`development.com`の DNS サーバーを使用して、`production.com`ドメインでコールバック URL を解決できるようにする必要があります。または、`development.com`の FQDN を使用して、Citrix Gateway 仮想サーバー virtual IP（VIP）として解決することもできます。

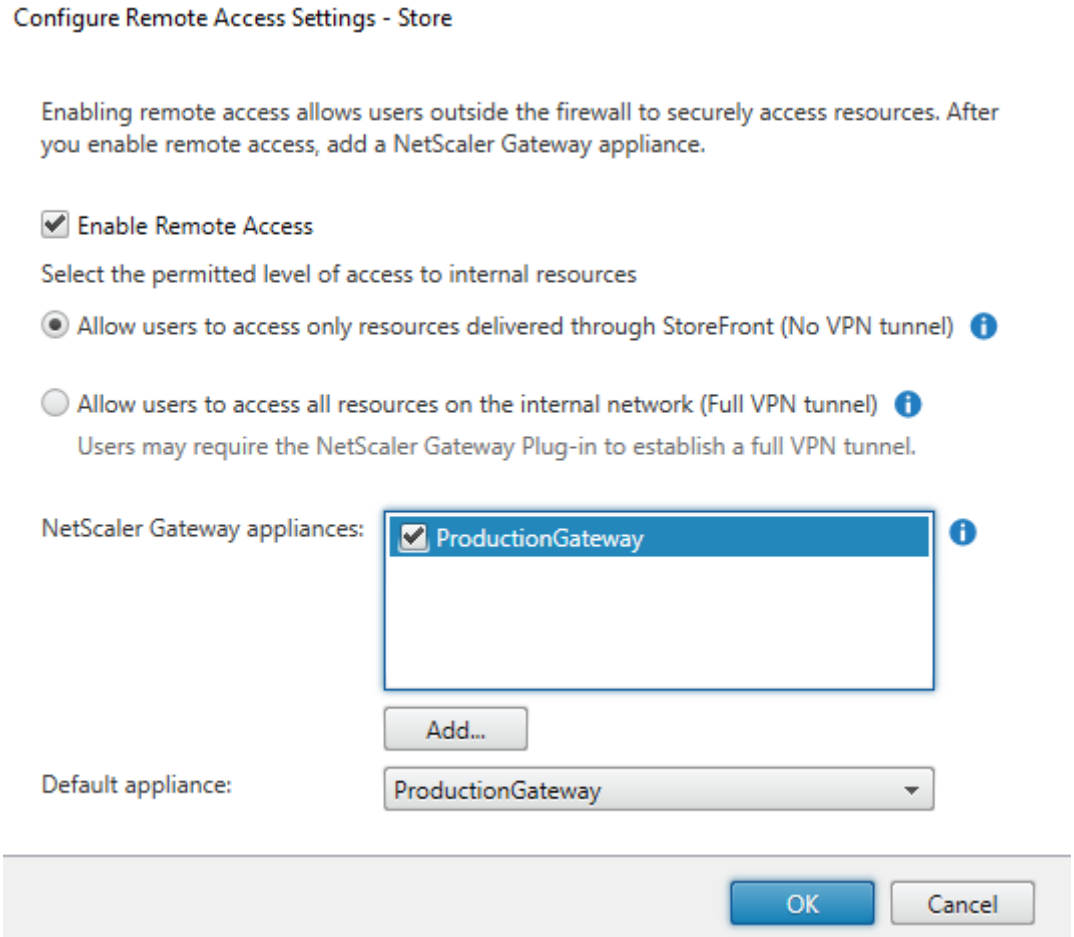
Citrix Gateway からのパススルーを有効にする

1. Citrix StoreFront 管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインの［認証方法の管理］をクリックします。
2. ［認証方法の管理］画面で、［**Citrix Gateway** からのパススルー］を選択します。
3. ［**OK**］をクリックします。



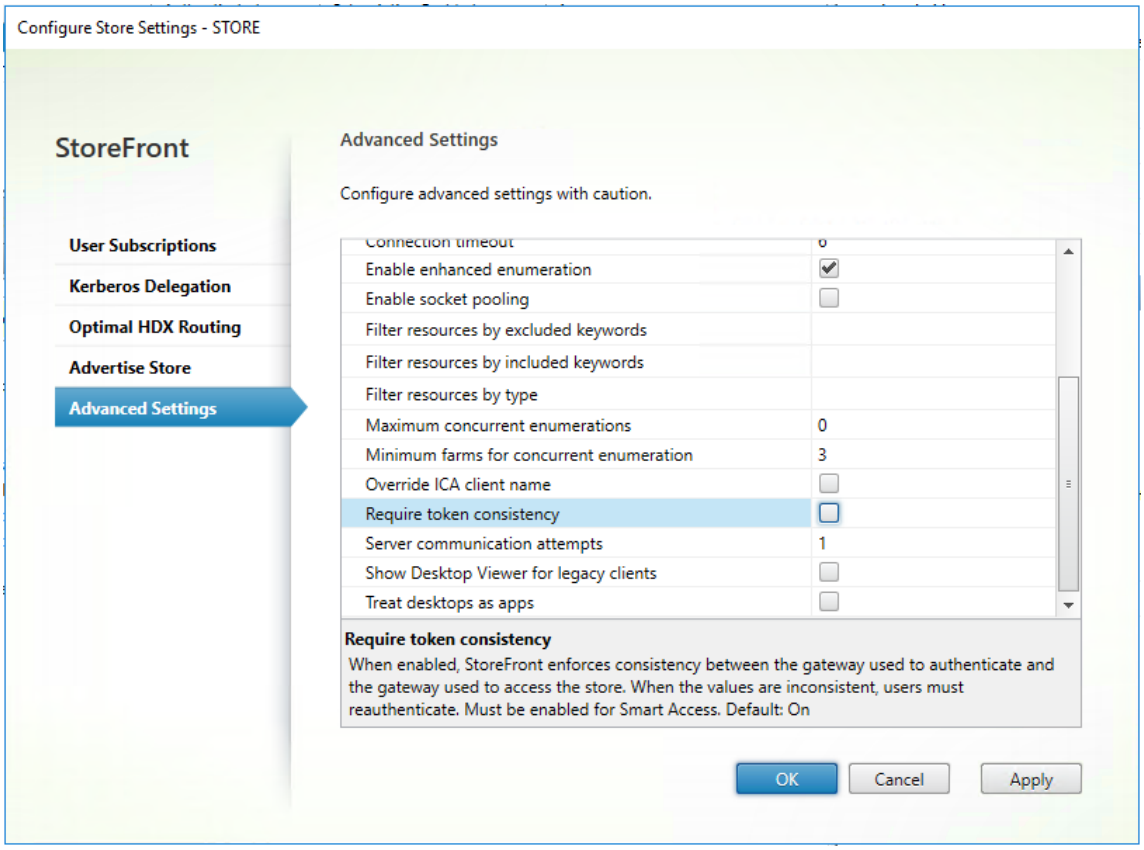
NetScaler Gateway を使用したリモートアクセスをストアで構成する

1. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインで ［リモートアクセス設定の構成］をクリックします。
2. ［リモートアクセスの有効化］を選択します。
3. Citrix Gateway がストアに登録されたことを確認します。Citrix Gateway が登録されていないと、STA チケット発行機能は機能しません。



トークンの一貫性を無効にする

1. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインで、［ストア設定の構成］を選択します。
2. ［ストア設定の構成］ページで、［詳細設定］を選択します。
3. ［トークンの一貫性を要求する］チェックボックスをオフにします。詳しくは、「上級ストア設定」を参照してください。



4. [**OK**] をクリックします。

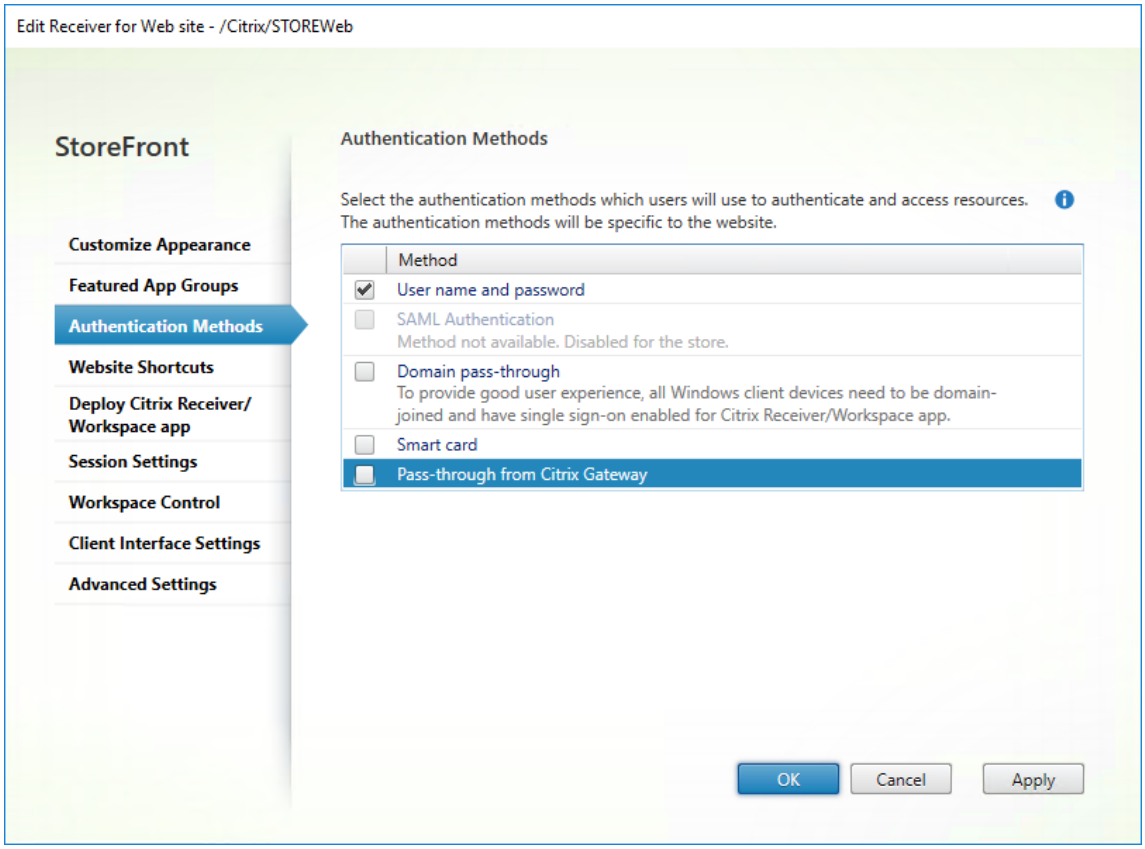
> 注:
>
> [トークンの一貫性を要求する] 設定はデフォルトでオンになっています。この設定を無効にすると、Citrix Gateway End Point Analysis（EPA）SmartAccess 機能が停止します。SmartAccess について詳しくは、CTX138110を参照してください。

Web サイトで Citrix Gateway からのパススルーを無効にする

> 重要:
>
> Citrix Gateway からのパススルーを無効にすると、Web サイトが Citrix Gateway から渡されたproduction.comドメインの誤った資格情報を使用しないようにできます。Citrix Gateway からのパススルーを無効にすると、Web サイトがユーザーに資格情報の入力を求めます。これらの資格情報は、Citrix Gateway でログオンする場合に使用する資格情報とは異なります。

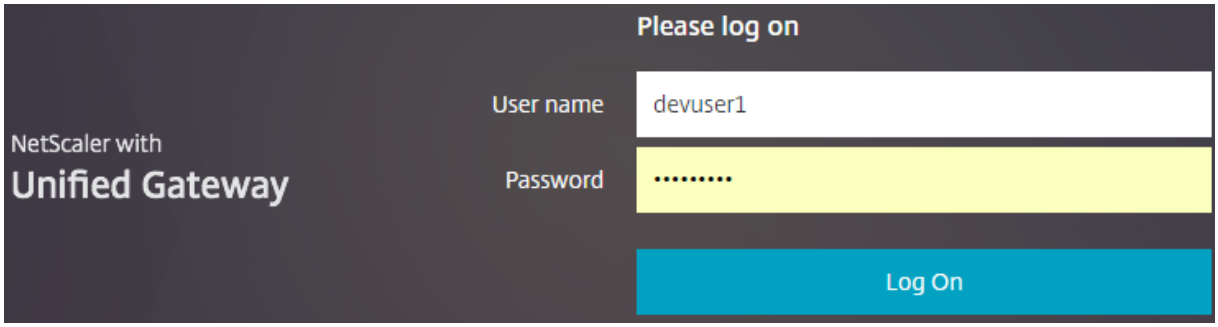
1. Citrix StoreFront 管理コンソールの左ペインで [ストア] ノードを選択します。
2. 変更するストアを選択します。
3. [操作] ペインで [**Receiver for Web** サイトの管理] をクリックします。
4. 認証方法で、[**Citrix Gateway** からのパススルー] をオフにします。

5. [**OK**] をクリックします。

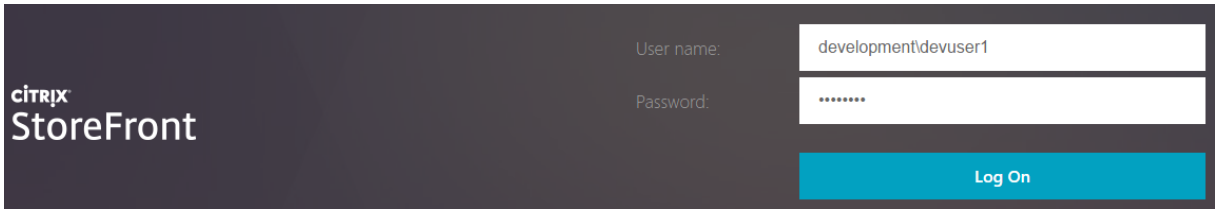


`production.com` ユーザー名およびパスワードを使用して **NetScaler Gateway** にログオンする

テストのために、`production.com`ユーザー名およびパスワードを使用して、NetScaler Gateway にログオンします。



ログオン後、ユーザーは`development.com`の資格情報を入力するよう求められます。

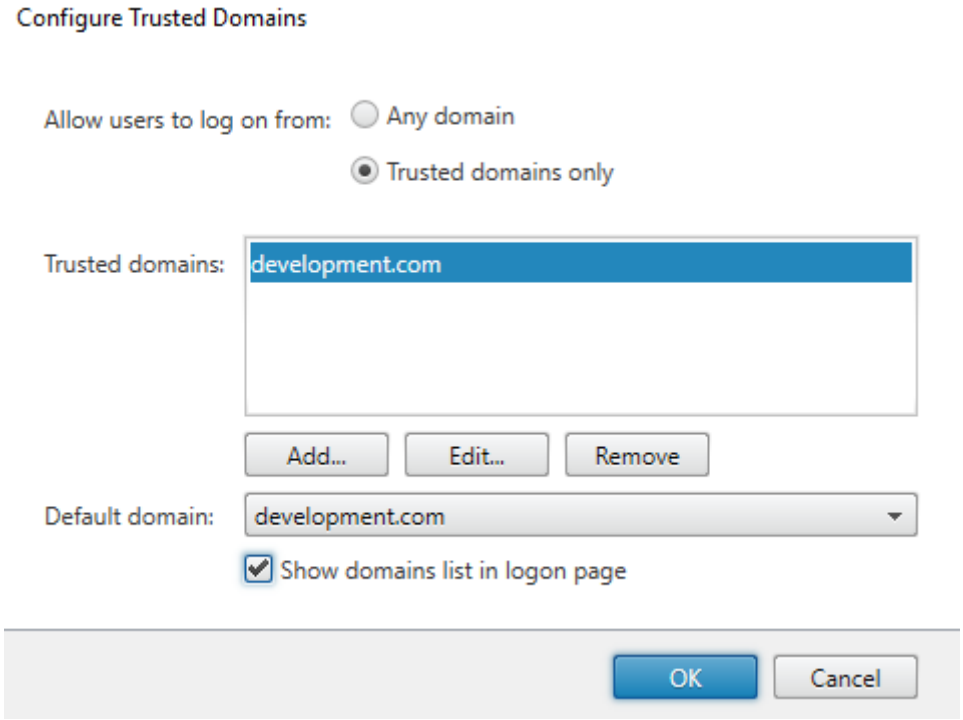


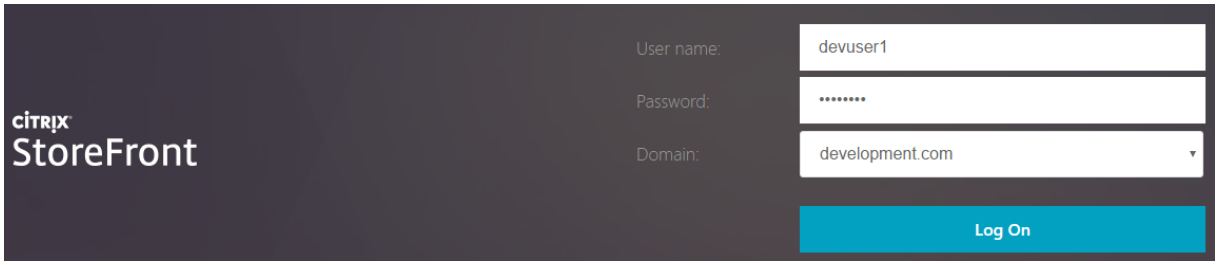
StoreFront で信頼済みドメインドロップダウンリストを追加する（オプション）

この設定はオプションですが、これによって Citrix Gateway 経由の認証で誤ったドメインの入力を回避できる場合があります。

両方のドメインで同じユーザー名を使用する場合、誤ったドメインを入力する可能性が高くなります。慣れていないユーザーが、Citrix Gateway 経由でログオンする時、ドメインの入力を省略することもあります。その後、Receiver for Web サイトにログオンするよう求められると、ドメインでドメイン\ユーザー名の入力を忘れる可能性があります。

1. Citrix StoreFront 管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインの［認証方法の管理］をクリックします。
2. ［ユーザー名とパスワード］の横の下向き矢印を選択します。
3. ［追加］を選択して、`development.com`を信頼済みドメインとして追加し、［ログオンページにドメイン一覧を表示する］チェックボックスをオンにします。
4. ［**OK**］をクリックします。

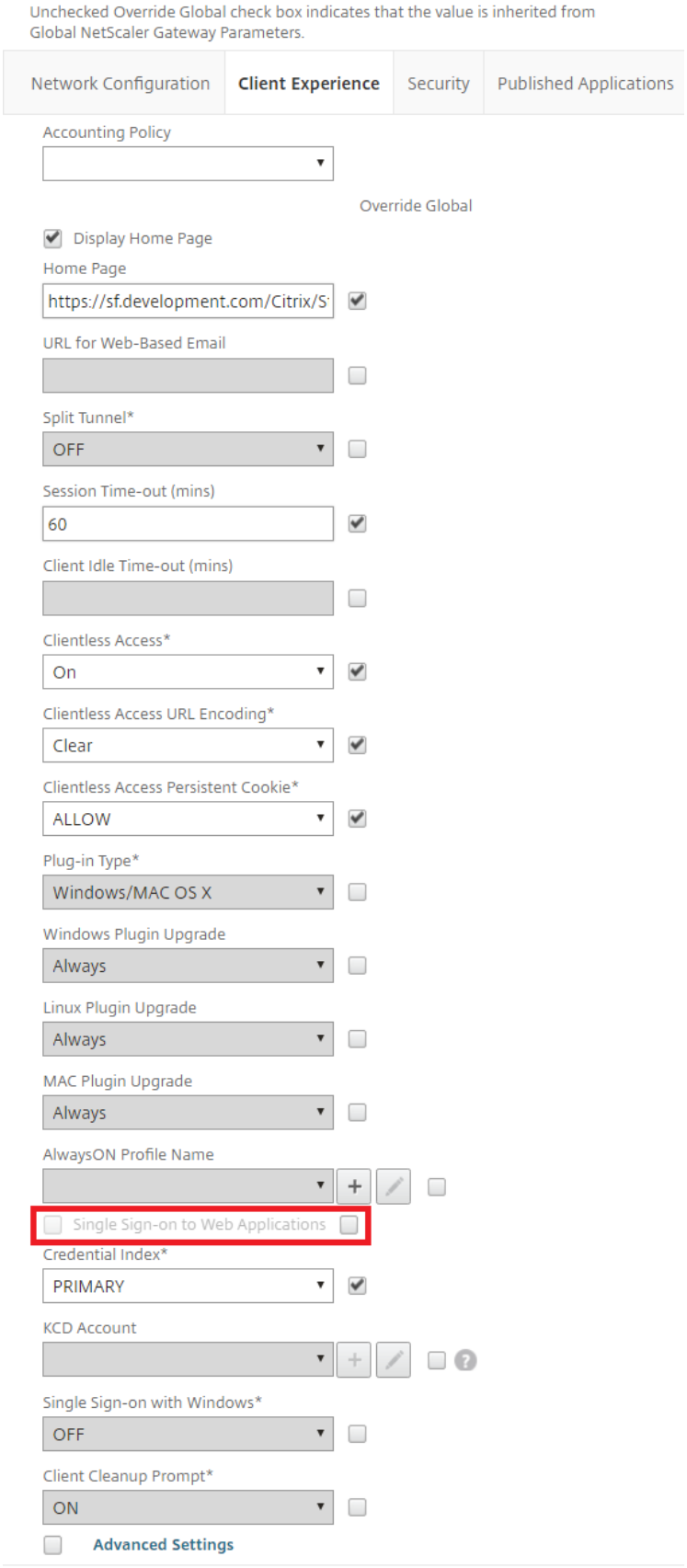


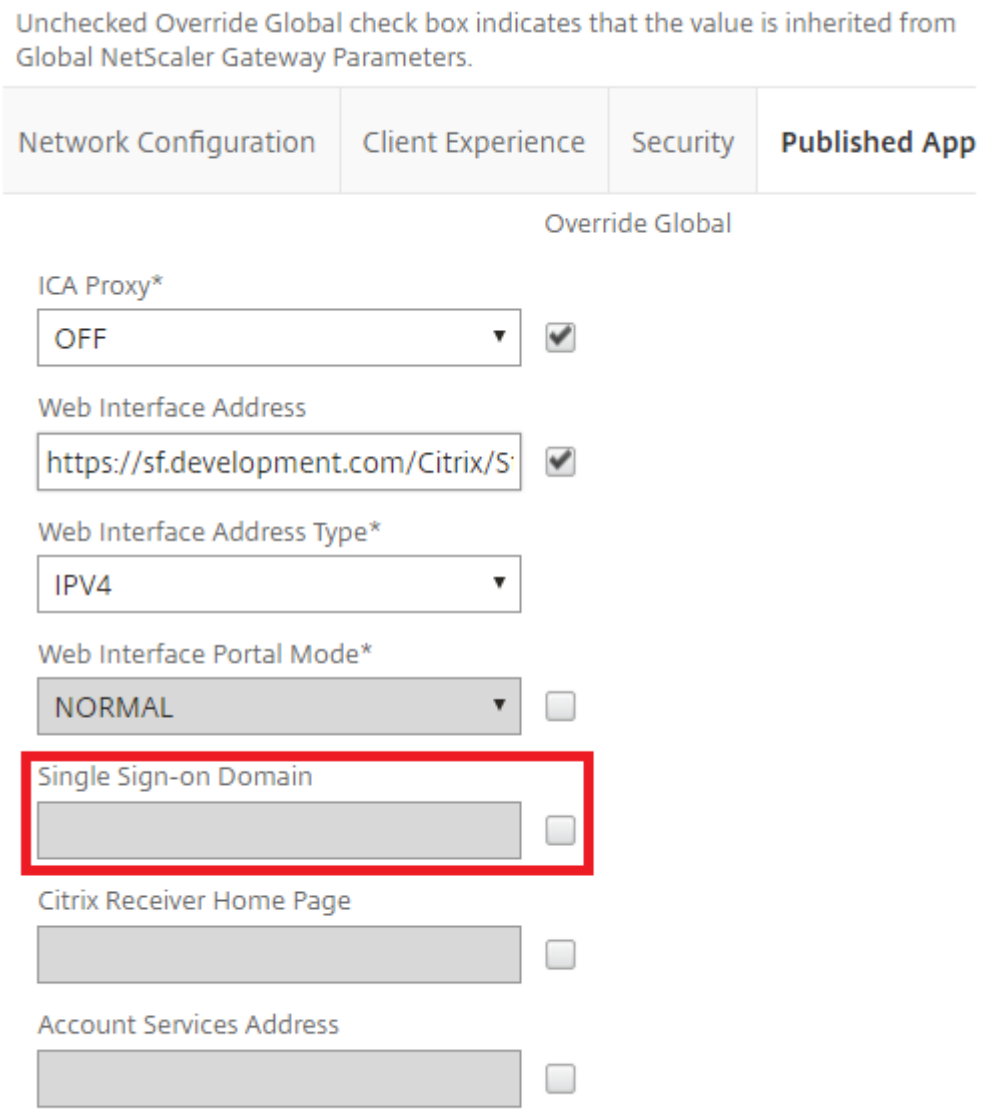


> 注:
>
> この認証方法では、ブラウザーのパスワードキャッシュ機能は使用しないでください。2 つの異なるドメインアカウントに異なるパスワードがある場合、パスワードキャッシュによって操作が複雑になる可能性があります。

NetScaler セッションの操作ポリシー

- Citrix Gateway セッションポリシーで Web アプリケーションへのシングルサインオン機能が有効になっていると、Citrix Gateway から Web サイトに送信された正しくない資格情報は無視されます。これは、Web サイトで ［**Citrix Gateway** からのパススルー］認証方法が無効になっているためです。このオプションがどのように設定されていても、Web サイトは資格情報を求めます。
- Citrix Gateway の［Client Experience］および［Published Applications］タブでシングルサインオンを指定しても、ここで説明された動作は影響を受けません。



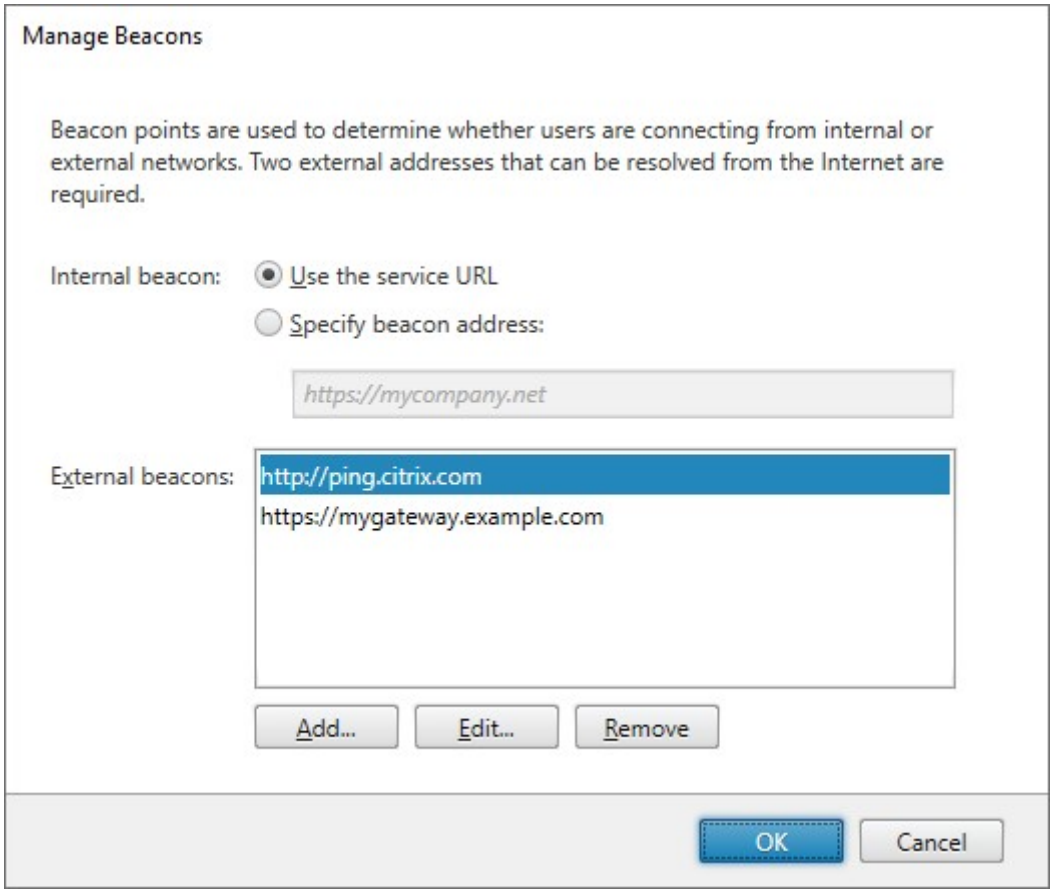


ビーコンポイントの構成

June 6, 2024

> 重要:
>
> `http://ping.citrix.com` は現在利用できないため、代わりのビーコンを設定する必要があります。
>
> 所有していないサードパーティの Web サイトを外部ビーコンとして使用しないでください。代わりに、所属する組織が管理する Web サイトを使用してください。

［ビーコンの管理］画面で、ビーコンポイントとして使用する、内部ネットワークの内側と外側の URL を指定します。ローカルにインストールされた Citrix Workspace アプリは、ユーザーがローカルネットワークとパブリックネットワークのどちらに接続しているのかをビーコンポイントを使用して識別します。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバーがそのユーザーの位置情報に基づいて適切な接続詳細を Citrix Workspace アプリに返します。これにより、ユーザーがデスクトップまたはアプリケーションにアクセスしたときに再ログオンする必要がなくなります。HTML5 向け Citrix Workspace アプリではビーコンは使用されません。



たとえば、内部ビーコンポイントにアクセス可能な場合、そのユーザーはローカルネットワークに接続していると認識されます。これに対し、Citrix Workspace アプリで内部ビーコンポイントにアクセスできず、2 つの外部ビーコンポイントからの応答を受信した場合、そのユーザーは社内ネットワークの外からインターネット経由で接続していると認識されます。このため、ユーザーは Citrix Gateway 経由でデスクトップやアプリケーションに接続する必要があります。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバーが、使用されるべき Citrix Gateway アプライアンスの詳細を提供します。このため、ユーザーがその NetScaler Gateway アプライアンスにログオンする必要はありません。

デフォルトでは、StoreFront は以下を設定します:

- 展開のベース URL への内部ビーコン。
- `http://ping.citrix.com`への外部ビーコンと、最初に追加する Citrix Gateway 展開の URL。

ビーコンポイントを構成するには、以下の手順を実行します:

1. Citrix StoreFront 管理コンソールの左ペインで ［ストア］ノードを選択して、［操作］ペインの ［ビーコンの管理］をクリックします。
2. 内部ビーコンポイントとして使用する URL を指定します。
   - StoreFront 展開環境でサーバーの URL または負荷分散 URL を使用するには、［サービス **URL** を使用する］を選択します。
   - 別の URL を使用するには、［ビーコンアドレスを指定する］を選択して、内部ネットワーク内の可用性の高い URL を入力します。
3. 外部ビーコンポイントの URL を入力するには、［追加］をクリックします。ビーコンポイントを変更するには、［外部ビーコン］ボックスの一覧で URL を選択して ［編集］をクリックします。ビーコンポイントとしてそのアドレスが使われないようにするには、一覧で URL を選択して［削除］をクリックします。

   公共のネットワーク上で解決でき、可用性の高い外部ビーコンポイントを少なくとも 2 つ指定する必要があります。ビーコン URL は、`http://example`などの簡略化された NetBIOS 名ではなく、`http://example.com`などの完全修飾ドメイン名にする必要があります。これにより、内部ネットワークとユーザーの間に、ホテルやインターネットカフェなど、インターネットペイウォール（有料の壁）があるかどうかを Citrix Workspace アプリで判別できるようになります。インターネットペイウォールがある場合、すべての外部ビーコンポイントが同じプロキシに接続されます。サードパーティの Web サイトではなく、組織によって管理されている URL を使用する必要があります。

ビーコンポイントの設定を変更する場合は、そのビーコンポイントをユーザーに通知して Citrix Workspace アプリの設定を変更させる必要があります。ユーザーは、HTML5 向け Citrix Workspace アプリから更新された Citrix Workspace アプリのプロビジョニングファイルを入手できます。Receiver for Web サイトが構成済みでない場合は、管理者がストアのプロビジョニングファイルをエクスポートしてユーザーに提供します。

PowerShell SDK

現在のビーコンを取得するには、Get-STFRoamingBeaconを使用します。

ビーコンを追加するには、Set-STFRoamingBeaconを使用します。

ビーコンをデフォルトに設定するには、Clear-STFRoamingBeaconを使用します。

内部および外部で使用される単一の **FQDN** の作成

June 6, 2024

社内ネットワーク内から直接、または Citrix Gateway 経由でリモートからストアにアクセスできる、単一の完全修飾ドメイン名（FQDN）を作成できます。

以下のドキュメントでは、例として次のように使用します:

- `https://storefront.example.com`をユーザーが StoreFront にアクセスするために使用される単一の URL として使用します。ネットワーク内では、これは StoreFront サーバーまたはロードバランサーに解決されます。ネットワークの外側では、ゲートウェイに解決されます。
- コールバック URL としての`https://storefrontcb.example.com`。これは内部でゲートウェイに解決されます。これは、スマートアクセスまたはパスワードレス認証の場合にのみ必要です。ゲートウェイ上の証明書にこのアドレスが SAN として含まれていることを確認し、ワイルドカード証明書を使用する必要があります。

サーバーグループのベース **URL**

ベース URL を単一の URL に変更します。「展開環境のベース URL の変更」を参照してください。

ローカルにインストールされた **Citrix Workspace** アプリ用の **StoreFront** ビーコン

ローカルにインストールされた Citrix Workspace アプリは、ユーザーがローカルネットワークとパブリックネットワークのどちらに接続しているのかをビーコンポイントを使用して識別します。

デフォルトでは、StoreFront はサーバーグループのベース URL を内部ビーコン URL として使用します。この構成では、同じ URL が内部と外部の両方で有効であるため、ビーコンとして使用できません。したがって、内部ビーコンを、内部でのみアクセス可能であるとわかっている URL に設定する必要があります。

「ビーコンの構成」を参照してください。

外部 **DNS**

- storefront.example.com は、Citrix Gateway 仮想サーバーの外部に対する IP に解決されます。

内部 **DNS**

- storefront.example.com は StoreFront のロードバランサーまたは単一の StoreFront サーバー IP に解決されます。
- storefrontcb.example.com は、Gateway 仮想サーバーの仮想 IP アドレスに解決されます。DMZ と会社のローカルネットワークの間にファイアウォールが存在する場合は、これを許可します。

StoreFront 構成のエクスポートとインポート

June 6, 2024

> 注:
>
> インポートできるのは、対象の StoreFront インストールと同じバージョンの StoreFront 構成のみです。

StoreFront 展開環境の構成全体をエクスポートできます。これには、単一サーバー環境とサーバーグループ構成の両方が含まれます。既存の展開環境がインポートサーバーに既に存在している場合、現在の構成が消去されてから、バックアップアーカイブ内に含まれている構成で置き換えられます。ターゲットサーバーがクリーンな工場出荷時のデフォルトインストールの場合、バックアップ内に保存されているインポートされた構成を使用して新しい環境が作成されます。エクスポートされた構成のバックアップは、単一の.zip アーカイブ形式（暗号化されていない場合）または.ctxzip 形式（作成時にバックアップファイルの暗号化を選択した場合）です。

構成のエクスポートとインポートを使用できるシナリオ

- StoreFront 展開環境は動作し、信頼できる状態の場合のみバックアップが作成されます。構成を変更した場合は、古いバックアップを置き換えるために新しいバックアップを作成する必要があります。backup.zip ファイルのファイルハッシュが変更を妨げるため、既存のバックアップを変更することはできません。
- StoreFront をアップグレードする前に障害回復用のバックアップを作成します。
- 既存のテスト用 StoreFront 展開を複製して実稼働環境に配置します。
- 実稼働環境をテスト環境に複製することにより、ユーザー承認環境を作成します。
- OS の移行中（Window Server 2019 から Windows 2022 へのホスティングのアップグレードなど）に、StoreFront を移動します。OS のインプレースアップグレードはサポートされていません。
- 複数のデータセンターを持つ大企業など、複数地域での展開で追加のサーバーグループを構築します。

StoreFront 構成のエクスポートおよびインポート時の検討事項

- 現在 Citrix が公開している認証 SDK の例（Magic Word Authentication など）またはサードパーティの認証カスタマイズを使用していますか。使用している場合は、これらのパッケージをすべてのインポートサーバーにインストールしてから、追加の認証方式を含む構成をインポートする必要があります。必要な認証 SDK パッケージがどのインポートサーバーにもインストールされていない場合、構成のインポートは失敗します。構成をサーバーグループにインポートする場合は、グループのすべてのメンバーに認証パッケージをインストールします。
- 構成のバックアップを暗号化または暗号化解除できます。エクスポートおよびインポート PowerShell コマンドレットはどちらのユースケースもサポートします。
- 暗号化されたバックアップ（.ctxzip）は後から暗号化解除できますが、StoreFront は暗号化されていないバックアップファイル（.zip）を再暗号化できません。暗号化されたバックアップが必要な場合は、選択したパスワードを含む PowerShell 資格情報オブジェクトを使用してもう一度エクスポートを実行します。
- StoreFront が現在インストールされている IIS（エクスポート元サーバー）における Web サイトの SiteID は、バックアップされた StoreFront 構成をリストアする IIS（インポート先サーバー）におけるターゲット Web サイトの SiteID に一致する必要があります。

PowerShell コマンドレット

Export-STFConfiguration

パラメーター	説明
-TargetFolder（文字列）	バックアップアーカイブへのエクスポートパス。例:”$env:userprofile\desktop\”
-Credential（PSCredential オブジェクト）	エクスポート中に暗号化された.ctxzip バックアップアーカイブを作成する資格情報オブジェクトを指定します。PowerShell 資格情報オブジェクトには、暗号化と暗号化解除に使用されるパスワードが含まれます。**-Credential** を **-NoEncryption** パラメーターと一緒に使用しないでください。例：$CredObject
-NoEncryption（スイッチ）	バックアップアーカイブを暗号化されていない.zip にすることを指定します。**-Credential** パラメーターを**-NoEncryption** パラメーターと一緒に使用しないでください。
-ZipFileName（文字列）	StoreFront 構成のバックアップアーカイブの名前。.zip や.ctxzip などのファイル拡張子を追加しないでください。ファイル拡張子は、エクスポート中に**-Credential** または**-NoEncryption** のどちらのパラメーターを指定したかによって自動的に追加されます。例:”backup”
-Force（ブール型）	このパラメーターは、バックアップアーカイブを、指定されたエクスポート先にある既存のバックアップファイルと同じファイル名で自動的に上書きします。

> 重要:
>
> StoreFront 3.5 にあった **SiteID** パラメーターは、バージョン 3.6 で廃止されました。バックアップアーカイブに含まれる **SiteID** が常に使用されるようになったため、インポートを実行するときに SiteID を指定する必要はなくなりました。SiteID が、インポート先サーバーの IIS 内で既に構成されている既存の StoreFront Web サイトに一致することを確認します。**SiteID 1** から **SiteID 2** への構成のインポートはサポートされません。

Import-STFConfiguration

パラメーター	説明
-ConfigurationZip（文字列）	インポートするバックアップアーカイブへのフルパス。ファイル拡張子も含めます。暗号化されていない場合は.zip、暗号化されたバックアップアーカイブの場合は.ctxzip を使用します。例：`$env:userprofile\desktop\backup.ctxzip`
-Credential（PSCredential オブジェクト）	インポート中に暗号化されたバックアップを暗号化解除する資格情報オブジェクトを指定します。例：`$CredObject`
-HostBaseURL（文字列）	このパラメーターが含まれると、指定したホストベース URL がエクスポートサーバーのホストベース URL の代わりに使用されます。例：`https://<importingserver>.example.com`

Unprotect-STFConfigurationBackup

パラメーター	説明
-TargetFolder（文字列）	バックアップアーカイブへのエクスポートパス。例：$env:userprofile\desktop
-Credential（PSCredential オブジェクト）	このパラメーターを使用して暗号化されたバックアップアーカイブの暗号化されていないコピーを作成します。暗号化解除に使用するパスワードを含む PowerShell 資格情報オブジェクトを指定します。例：`$CredObject`
-EncryptedConfigurationZip（文字列）	暗号化解除する暗号化されたバックアップアーカイブのフルパス。ファイル拡張子.ctxzip を指定する必要があります。例：`$env:userprofile\\desktop\\backup.ctxzip`

パラメーター	説明
-OutputFolder（文字列） -Force（ブール型）	暗号化された（.ctxzip）バックアップアーカイブから暗号化されていないコピー（.zip）を作成するパス。元の暗号化されたバックアップのコピーは保持され、再使用できます。暗号化されていないコピーのファイル名とファイル拡張子は指定しないでください。例: $env:userprofile\desktop このパラメーターは、バックアップアーカイブを、指定されたエクスポート先にある既存のバックアップファイルと同じファイル名で自動的に上書きします。

構成のエクスポートおよびインポート例

現在の **PowerShell** セッションへの **StoreFront** コマンドレットのインポート

StoreFront サーバーで PowerShell Integrated Scripting Environment（ISE）を開き、以下を実行します。

```
$env:PSModulePath = [Environment]::GetEnvironmentVariable('PSModulePath','Machine')
$SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'
Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
Import-Module "$SDKModules.Authentication\Citrix.StoreFront.Authentication.psd1" -verbose
Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -verbose
Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -verbose
Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.psd1" -verbose
<!--NeedCopy-->
```

単一サーバーのシナリオ

サーバー **A** で既存の構成の暗号化されていないバックアップを作成し、それを同じ環境に復元する　バックアップするサーバーの構成をエクスポートします。

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -zipFileName "backup" -NoEncryption
<!--NeedCopy-->
```

backup.zip ファイルを安全な場所にコピーします。このバックアップを障害回復で使用して、サーバーを以前の状態に復元できます。


```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://storefront.example.com"
<!--NeedCopy-->
```

サーバー **A** の既存の構成をバックアップし、サーバー **B** に復元して既存のサーバーのクローンを作成する　バックアップするサーバーの構成をエクスポートします。

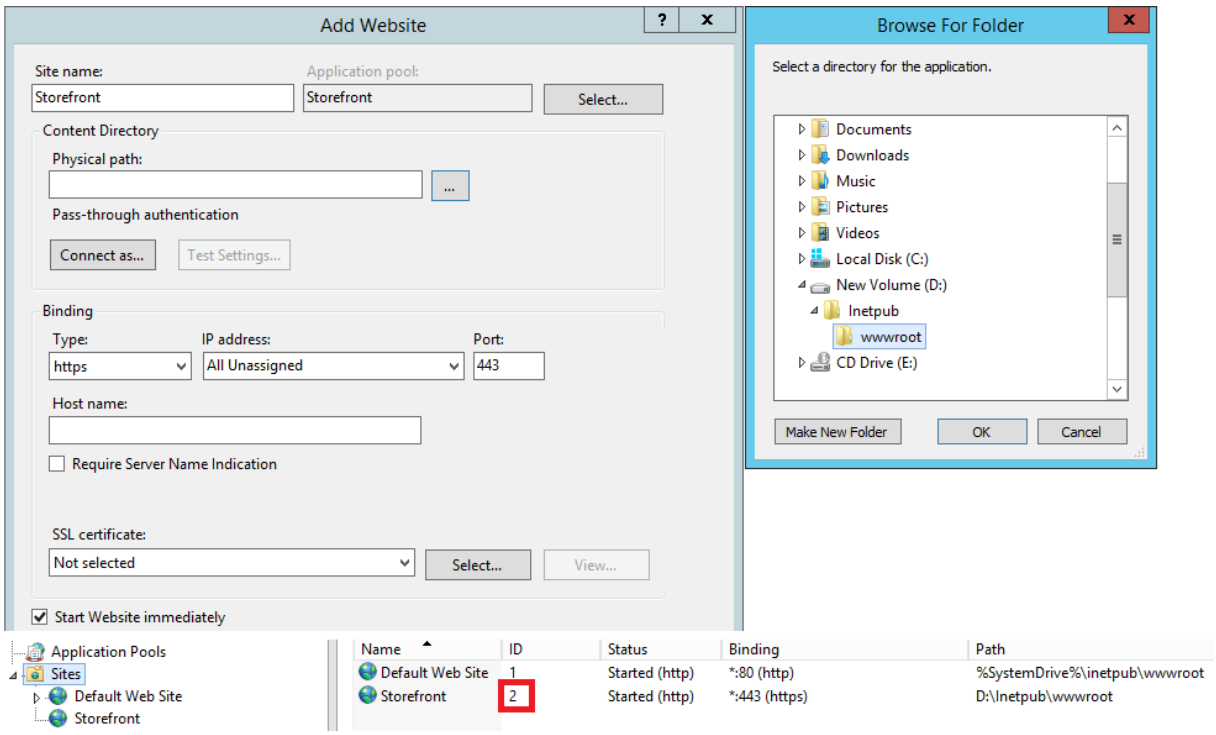
```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -NoEncryption
<!--NeedCopy-->
```

backup.zip ファイルをサーバー B のデスクトップにコピーします。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://serverB.example.com"
<!--NeedCopy-->
```

StoreFront は **IIS** のカスタムの **Web** サイトに既に展開されている。この構成を別のカスタム **Web** サイト環境に復元する　サーバー A では StoreFront を IIS 内の通常のデフォルトの Web サイトではなくカスタムの Web サイトの場所に展開しています。IIS 内に作成された 2 つ目の Web サイトの IIS SiteID は 2 です。StoreFront Web サイトの物理パスは、d:\など別のシステム以外のドライブまたはデフォルトの c:\システムドライブに置くことができますが、1 を超える IIS SiteID を使用する必要があります。

StoreFront という新しい Web サイトが、**SiteID = 2** を使用する IIS 内で構成されています。StoreFront は、ドライブ`d:\inetpub\wwwrooot`の物理パスで IIS 内のカスタム Web サイトに既に展開されています。



1. サーバー A の構成のコピーをエクスポートします。
2. サーバー B で、**SiteID 2** を使用する **StoreFront** という新しい Web サイトを IIS で構成します。
3. サーバー A の構成をサーバー B にインポートします。バックアップに含まれるサイト ID を使用し、この ID が StoreFront 構成のインポート先 Web サイトに一致する必要があります。

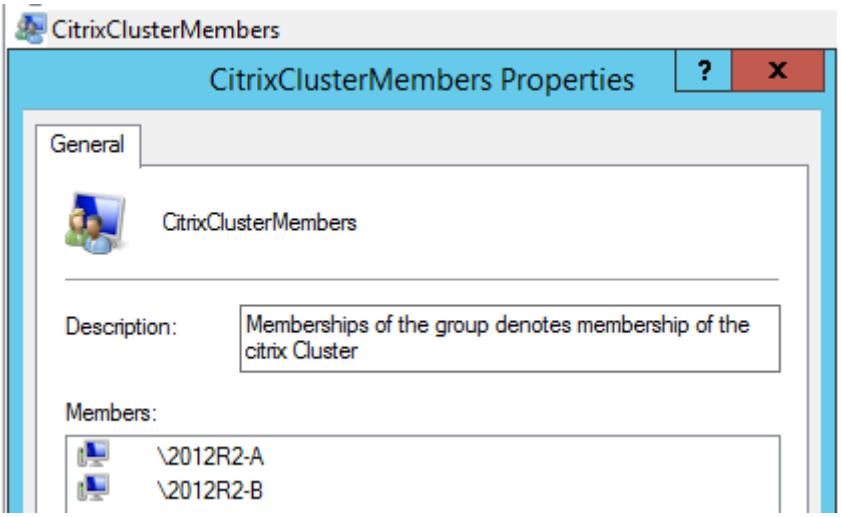
```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://serverB.example.
    com"
<!--NeedCopy-->
```

サーバー グループ シナリオ

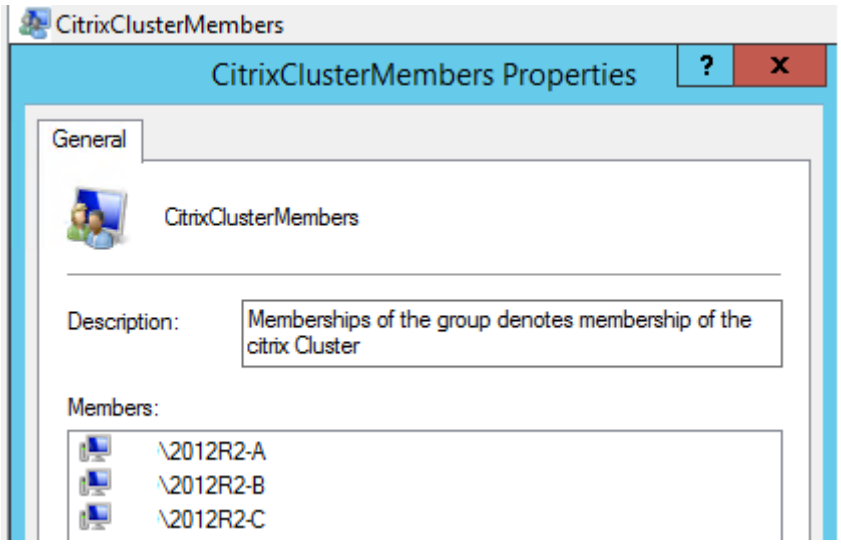
シナリオ **1**: 既存のサーバーグループ構成をバックアップし、後でそのバックアップを同じサーバーグループ環境で復元する　前の構成バックアップは、2 つの StoreFront サーバー（2012R2-A と 2012R2-B）のみがサーバーグループのメンバーであるときに取得されました。バックアップアーカイブ内には、元のサーバー 2012R2-A と 2012R2-B のみを含む、バックアップが取得された時点の **CitrixClusterMembership** のレコードが含まれます。StoreFront サーバーグループ環境では、ビジネス上の需要に伴い、元のバックアップが取得された時点よりサイズが増え続けています。したがって、追加のノード 2012R2-C がサーバーグループに追加されています。バックアップに保持されているサーバーグループの基になる StoreFront 構成は変更されていません。2 つの元のサーバーグループノードのみを含む古いバックアップがインポートされている場合でも、3 つのサーバーの現在の CitrixClusterMembership を維持する必要があります。インポート中に、現在のクラスターメンバーシップが保持されて、構成がプライマリサーバーに正常にインポートされた後にライトバックされます。元のバックア

ップが取得された後にサーバーグループノードがサーバーグループから削除された場合、インポートでは現在の CitrixClusterMembership も保持されます。

1. サーバーグループ 1 の構成を 2012R2-A からエクスポートします。2012R2-A はサーバーグループ全体を管理するために使用されるプライマリサーバーです。



2. 後で、追加のサーバー 2012R2-C を既存のサーバーグループに追加します。



3. サーバーグループの構成を既知の前の作業状態に復元する必要があります。StoreFront では、インポートプロセスの実行中に 3 つのサーバーの現在の CitrixClusterMembership がバックアップされ、インポートの成功後に復元されます。

4. サーバーグループ 1 の構成をノード 2012R2-A にインポートして戻します。

```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://servergroup1.
    example.com"
<!--NeedCopy-->
```


5. 新しくインポートした構成をサーバーグループ全体に反映して、インポート後にすべてのサーバーの構成が一致するようにします。

シナリオ **2**: 既存の構成をサーバーグループ **1** からバックアップし、そのバックアップを使用して別の工場出荷時のデフォルト環境に新しいサーバーグループを作成する。ほかの新しいサーバーグループメンバーを新しいプライマリサーバーに追加できる　新しい 2 つのサーバー 2012R2-C と 2012R2-D を含むサーバーグループ 2 が作成されます。サーバーグループ 2 の構成は既存環境のサーバーグループ 1 の構成に基づきます。サーバーグループ 1 にも 2 つのサーバー 2012R2-A と 2012R2-B が含まれています。バックアップアーカイブに含まれる CitrixClusterMembership は、新しいサーバーグループの作成時には使用されません。現在の CitrixClusterMembership が常にバックアップされ、インポートの成功後に復元されます。インポートされた構成を使用して新しい展開環境を作成すると、追加サーバーが新しいグループに加わるまでは、CitrixClusterMembership セキュリティグループには 1 つのインポートサーバーのみが含まれます。サーバーグループ 2 は新しい環境で、サーバーグループ 1 と共存することを目的としています。-HostBaseURL パラメーターを指定します。サーバーグループ 2 は、新しい工場出荷時のデフォルト StoreFront 環境を使用して作成されます。

1. サーバーグループ 1 の構成を 2012R2-A からエクスポートします。2012R2-A はサーバーグループ全体を管理するために使用されるプライマリサーバーです。
2. サーバーグループ 1 の構成をノード 2012R2-C にインポートします。2012R2-C は新しいサーバーグループ 2 のプライマリサーバーです。

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\
     desktop\backup.ctxzip" -HostBaseURL "https://servergroup2.
     example.com"
2 <!--NeedCopy-->
```

3. 新しいサーバーグループ 2 環境の一部となる追加のサーバーを追加します。サーバーグループ 1 からサーバーグループ 2 の新しいすべてのメンバーに新しくインポートされた構成が自動的に反映されます。これは新しいサーバーが追加されたときの標準の追加プロセスの一部になります。

シナリオ **3**: 既存の構成をサーバーグループ **A** からバックアップし、そのバックアップを使用して既存のサーバーグループ **B** の構成を上書きする　サーバーグループ 1 とサーバーグループ 2 は既に 2 つの個別のデータセンターに存在します。多くの StoreFront 構成の変更はサーバーグループ 1 で行われ、もう一方のデータセンターのサーバーグループ 2 に適用する必要があります。サーバーグループ 1 の変更をサーバーグループ 2 に移植できます。サーバーグループ 2 のバックアップアーカイブ内で **CitrixClusterMembership** を使用しないでください。インポート中に**-HostBaseURL** パラメーターを指定します。サーバーグループ 2 のホストベース URL は、サーバーグループ 1 で現在使用されている同じ FQDN に変更できません。サーバーグループ 2 は既存の環境です。

1. サーバーグループ 1 の構成を 2012R2-A からエクスポートします。2012R2-A はサーバーグループ全体を管理するために使用されるプライマリサーバーです。
2. サーバーグループ 1 の構成をノード 2012R2-C の工場出荷時のデフォルト環境にインポートします。2012R2-C は新しいサーバーグループ 2 のプライマリサーバーです。


```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.zip" -NoEncryption -HostBaseURL "https://
    servergroup2.example.com"
<!--NeedCopy-->
```

サーバー構成の暗号化されたバックアップを作成

PowerShell 資格情報オブジェクトには、Windows アカウントのユーザー名とパスワードの両方が結合されています。PowerShell 資格情報オブジェクトにより、パスワードがメモリ内で保護されます。

> 注:
>
> 構成バックアップのアーカイブを暗号化するには、暗号化と暗号化解除を実行するためのパスワードのみ必要です。資格情報オブジェクト内に保存されているユーザー名は使用されません。PowerShell セッション内に同じパスワードを含む資格情報オブジェクトを作成する必要があります。これは、エクスポートサーバーおよびインポートサーバーの両方で使用されます。資格情報オブジェクト内では、どのユーザーでも指定できます。

PowerShell では、新しい資格情報オブジェクトを作成するときにユーザーを指定する必要があります。便宜上、このコード例では現在ログオンしている Windows ユーザーを取得します。

エクスポートサーバーの Powershell セッション内で PowerShell 資格情報オブジェクトを作成します。

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)
<!--NeedCopy-->
```

暗号化された zip ファイルである backup.ctxzip に構成をエクスポートします。

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -Credential $CredObject
<!--NeedCopy-->
```

インポートサーバーの Powershell セッション内で同一の PowerShell 資格情報オブジェクトを作成します。

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.ctxzip" -Credential $CredObject -HostBaseURL "https://
    storefront.example.com"
<!--NeedCopy-->
```

既存の暗号化されたバックアップアーカイブの保護を解除する

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)
```



```
5
6 Unprotect-STFConfigurationExport -encryptedConfigurationZip "$env:
    userprofile\desktop\backup.ctxzip" -credential $CredObject -
    outputFolder "c:\StoreFrontBackups" -Force
7 <!--NeedCopy-->
```

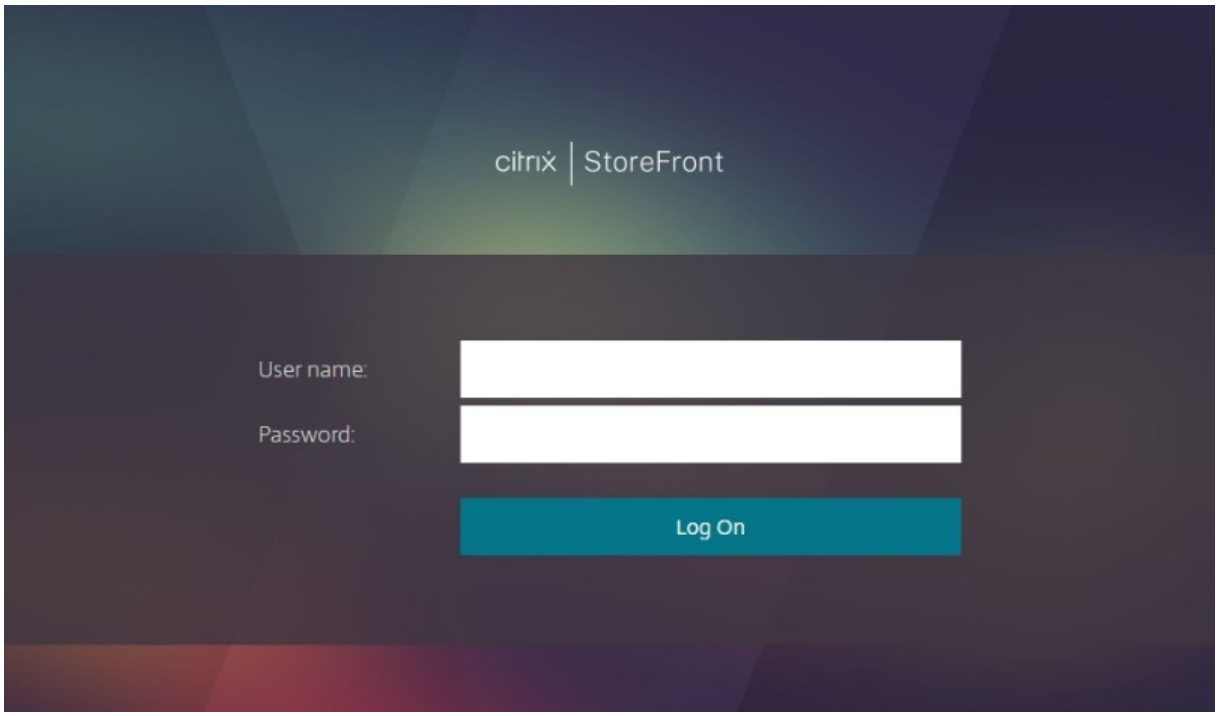
エンドユーザーガイド

June 6, 2024

このセクションでは、Web ブラウザーまたは Citrix Workspace アプリを通じて表示したときのストアの機能と外観について説明します。

ログオン

認証方法によって、またはシングルサインオンが有効かどうかによって、ログオンが必要になることがあります。



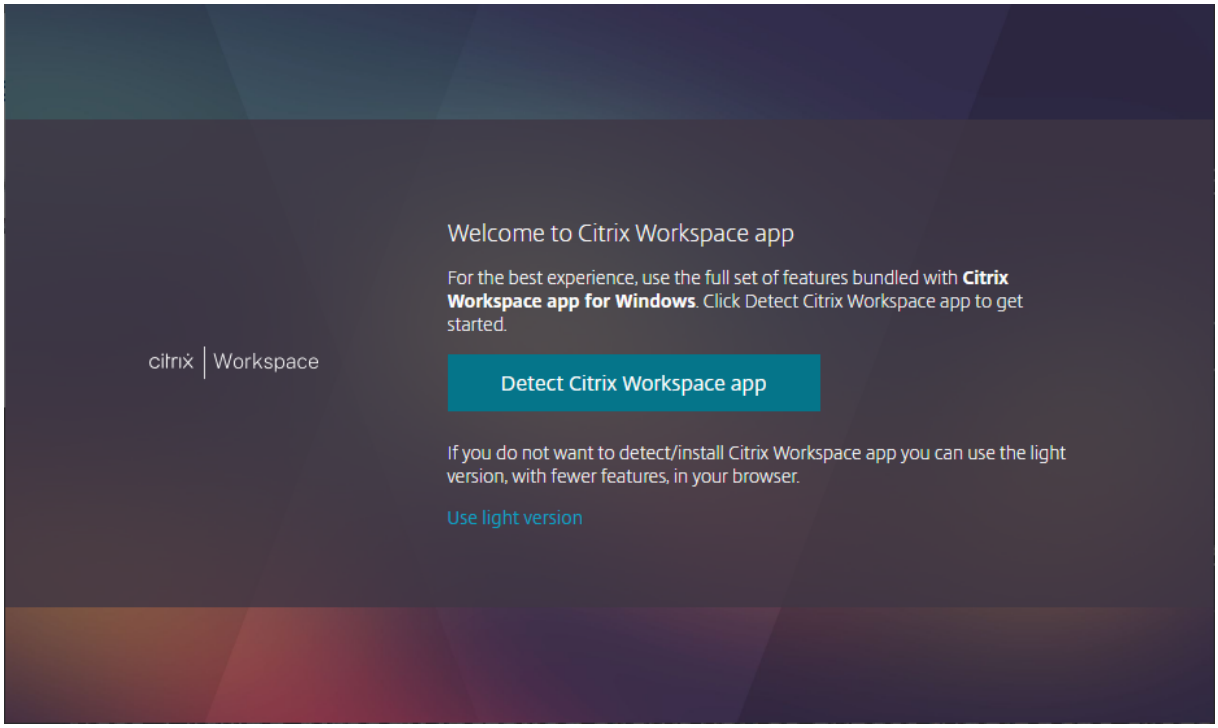
Citrix Workspace アプリの検出

> 注:
>
> この手順は、ローカルにインストールされた Citrix Workspace アプリではなく、Web ブラウザーを通じてス

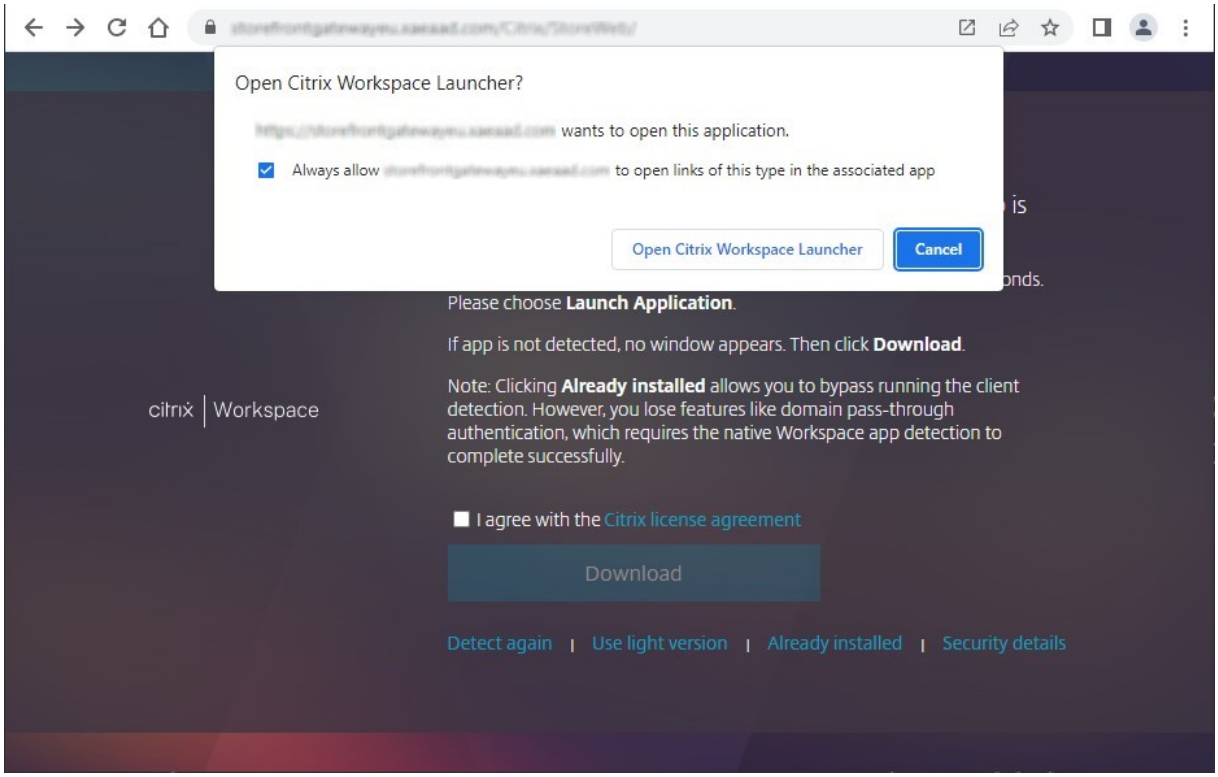
> トアにアクセスする場合にのみ適用されます。この手順は、構成に応じてログオンの前または後に実行できます。

構成に応じて、Web ブラウザーを通じてストアに初めてアクセスするとき、または Cookie をクリアした後に「**Citrix Workspace** アプリへようこそ」画面が表示される場合があります。次のどちらかを選択します:

- ローカルにインストールされた Citrix Workspace アプリでリソースを起動する場合は、[**Citrix Workspace** アプリを検出] をクリックします。これは最良のエクスペリエンスを得るために推奨されます。
- 常にブラウザー内でリソースを起動するには、[簡易バージョンを使用] (利用可能な場合) をクリックします。



[**Citrix Workspace** アプリを検出] をクリックすると、ローカルにインストールされた Citrix Workspace アプリの検出が試行されます。まず、Citrix Workspace Web 拡張機能の使用を試みます。これがインストールされていない場合、またはローカルにインストールされた Citrix Workspace アプリの検出に失敗した場合、Citrix Workspace アプリのコンポーネントである **Citrix Workspace Launcher** を開こうとします。Citrix Workspace アプリがインストールされている場合は、ブラウザーに **Citrix Workspace Launcher** の実行を求めるウィンドウがポップアップ表示されます。[**Citrix Workspace Launcher** を開く] または [リンクを開く] を (ブラウザーに応じて) クリックします。リソースを起動するたびにこのウィンドウが表示されないようにするために、[**Always allow *domain* to open links of this type in the associated app**] にもチェックを入れることをお勧めします。



ローカルにインストールされた Citrix Workspace アプリが検出された場合は、数秒後に次の画面に進みます。その後リソースを起動すると、検出された結果に応じて、Citrix Workspace Web 拡張機能または Citrix Workspace Launcher のいずれかを使用して、ローカルにインストールされた Citrix Workspace アプリ内のリソースを開きます。

Citrix Workspace アプリがインストールされていない場合、またはランチャーをキャンセルした場合は、構成に応じて次のオプションがあります:

- ダウンロード - Citrix Web サイトまたは StoreFront サーバーから Citrix Workspace アプリをダウンロードします。Citrix Workspace アプリをインストールした後、［再検出］をクリックします。
- 再検出 - ローカルにインストールされた Citrix Workspace アプリの再検出を試みます。
- 軽量バージョンを使用する - Workspace アプリの検出をスキップし、常に Web ブラウザーでリソースを開きます。
- インストール済み - Citrix Workspace Launcher または Citrix Workspace Web 拡張機能をサポートしていない古いバージョンの Citrix Receiver がインストールされている場合は、このオプションを使用します。このオプションを選択する場合、仮想アプリまたはデスクトップを起動するときに、Citrix Receiver で開くことができるファイル **launch.ica** がブラウザーによってダウンロードされます。このオプションを選択すると機能が限定されるため、お勧めできません。

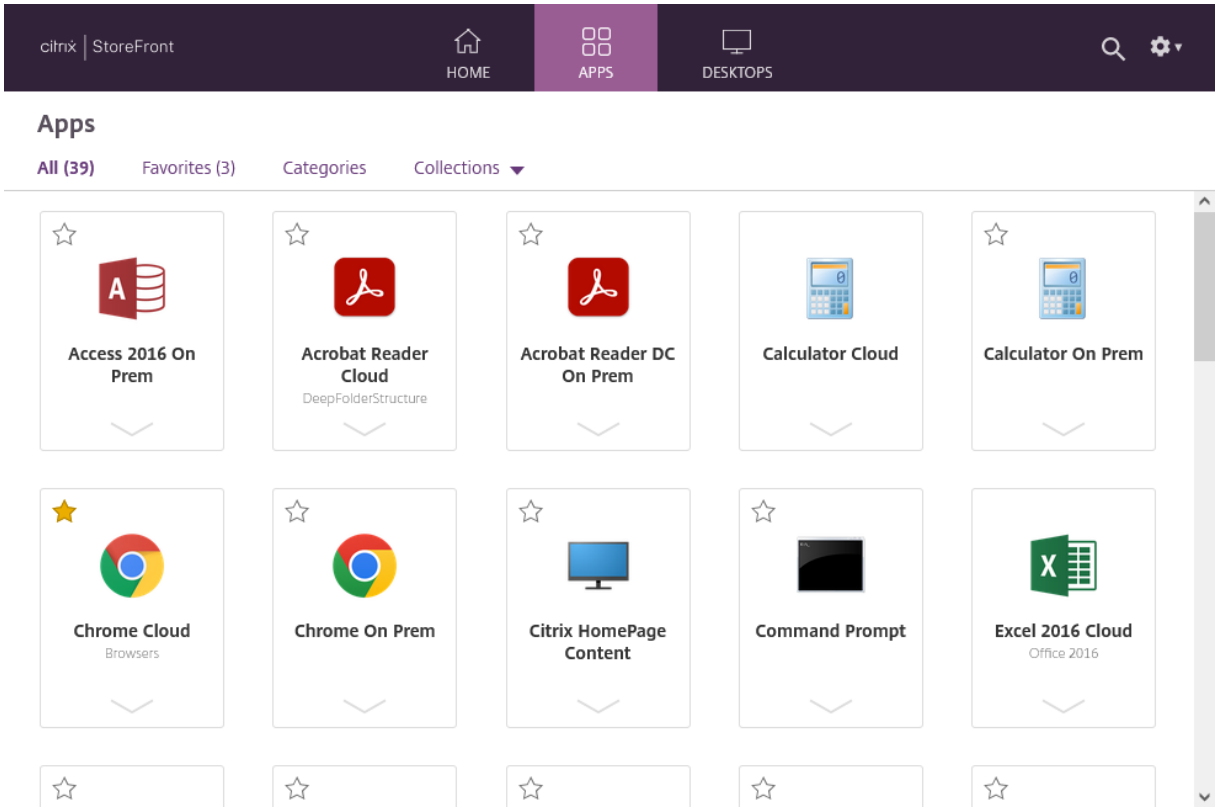
［ホーム］タブ

［ホーム］タブには、お勧めのアプリケーショングループと、お気に入りのアプリまたは必須アプリおよびデスクトップが表示されます。［ホーム］タブは、ストアでお気に入りが有効になっている場合にのみ表示されます。

［アプリ］タブ

［アプリ］タブには以下の複数のサブビューがあります:

- ［すべて］ - すべてのアプリを表示します。
- ［お気に入り］ - すべてのお気に入りのアプリを表示します。
- ［カテゴリ］ - カテゴリを表示し、そのカテゴリ内のアプリも表示します。カテゴリの表示方法は、［カテゴリの設定］によって異なります。
- ［コレクション］ お勧めのアプリケーショングループを表示します。



[デスクトップ] タブ

[デスクトップ] タブには以下の 2 つのサブビューがあります:

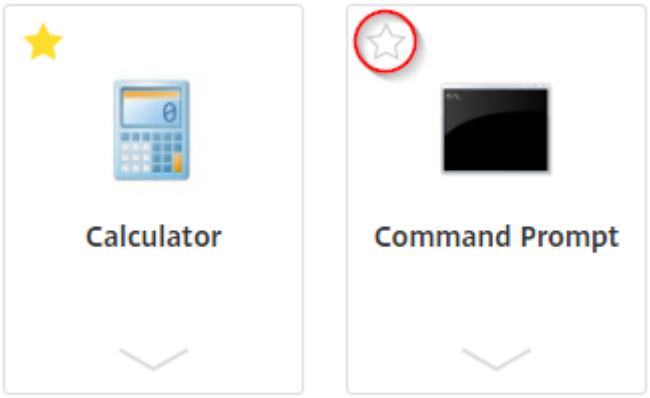
- [すべて] - すべてのデスクトップを表示します。
- [お気に入り] - お気に入りのデスクトップを表示します。

アプリとデスクトップのタイル

アイコンをクリックしてアプリまたはデスクトップを起動します。

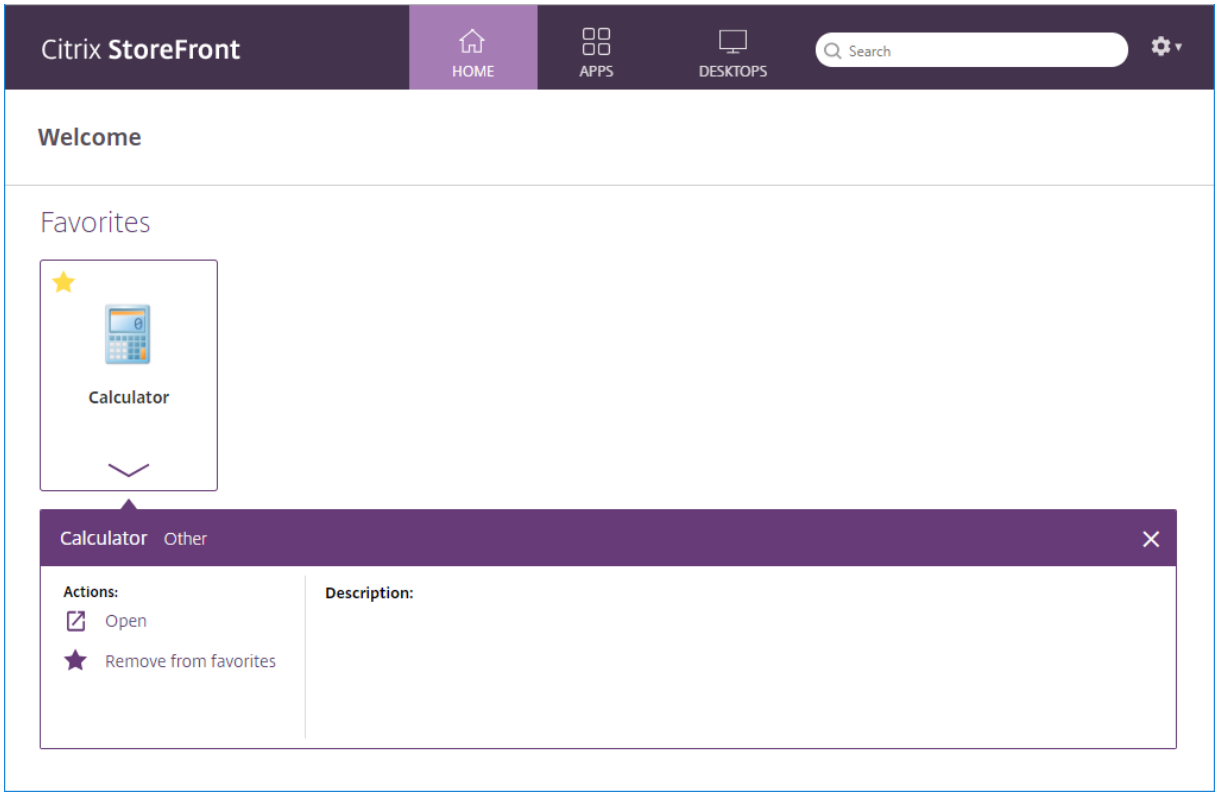
お気に入り

アイテムをお気に入りに登録するには、星をクリックまたはタップします:



詳細と操作の表示

各アイコンの下のパネルを展開して、アプリの説明と操作を表示できます。



以下のアクションが利用できる場合があります:

- [開く] - アプリやデスクトップを起動するか、再接続します。
- [お気に入りに追加] - アイテムがお気に入りでなく、必須ではなく、ストアでお気に入りが有効になっている場合は、アプリまたはデスクトップをお気に入りに追加します。
- [お気に入りから削除] - アイテムがお気に入りで、必須ではなく、ストアでお気に入りが有効になっている場合は、アプリまたはデスクトップをお気に入りから削除します。

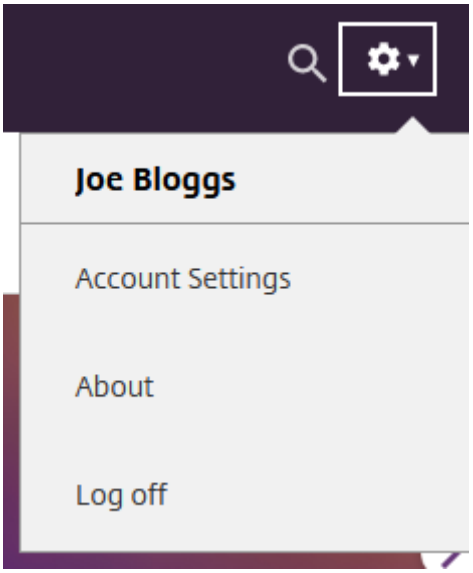
- ［再起動］ - 再起動が可能な割り当てられたデスクトップの場合、デスクトップを再起動します。

検索

虫眼鏡アイコンをクリックして検索ボックスを表示します。すべてのアプリ、デスクトップ、カテゴリを横断して検索します:

設定

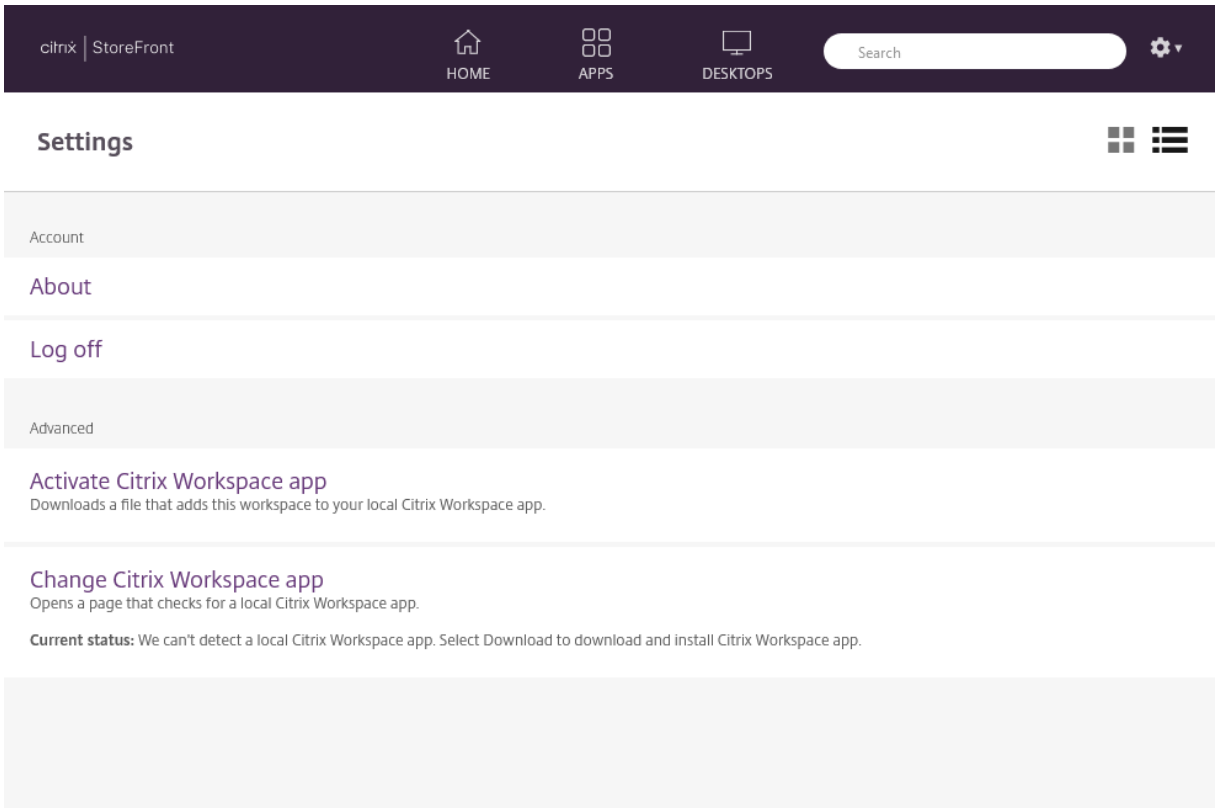
設定メニューは、Web ブラウザーを通じてストアにアクセスする場合にのみ使用できます。



設定メニューには次のオプションがあります:

- ［アカウント設定］ - 設定ページを開きます。
- ［バージョン情報］ - アプリケーションに関する情報を表示します。
- ［ログオフ］ - Web サイトからログオフします。

アカウント設定



以下のオプションを使用できる場合があります：

接続。切断されたセッションを再開します。

切断。現在のすべてのセッションを切断し、ログオフします。

Citrix Workspace アプリのアクティブ化。このストアをローカルの Citrix Workspace アプリに追加するファイルをダウンロードします。

Citrix Workspace アプリを変更。ローカルにインストールされた Citrix Workspace アプリを確認するページを開きます。これによってユーザーがローカルにインストールされた Citrix Workspace アプリを使用したリソースの起動と Web ブラウザーでのリソースの起動とを切り替えることもできます。

ログオフ

ログオフするには、設定メニューを開き、［ログオフ］をクリックします。これによりストアからログオフされます。リソースに接続している場合は、構成に応じて次のいずれかが行われます：

- リソースを終了する。
- リソースから切断する
- リソースを接続したままにする。

StoreFront SDK

June 6, 2024

Citrix StoreFront は、多くの Microsoft Windows PowerShell のバージョン 2.0 モジュールをベースとした SDK を提供しています。この SDK により、StoreFront MMC コンソールと同じタスクだけでなく、コンソールだけでは実行できないタスクも実行できます。

> 注:
>
> PowerShell SDK は PowerShell 6 以降と互換性がありません。

SDK については、StoreFront SDKを参照してください。

SDK の使用

この SDK は、さまざまな StoreFront コンポーネントをインストールおよび構成する場合に、インストールウィザードにより自動的にインストールされた多くの PowerShell スナップインで構成されています。

コマンドレットにアクセスして実行するには:

1. 管理者として PowerShell コマンドラインプロンプトまたは **Windows PowerShell ISE** を起動します。

   StoreFront サーバーのローカルの管理者グループのメンバーを使って、シェルまたはスクリプトを実行する必要があります。

2. スクリプト内で SDK コマンドレットを使用するには、PowerShell 実行ポリシーを設定する必要があります。

   PowerShell 実行ポリシーについて詳しくは、Microsoft 社のドキュメントを参照してください。

3. Windows PowerShell コンソールで **Add-Module** コマンドを使って、必要なモジュールを PowerShell 環境に追加します。たとえば、次のように入力します:

   ```
   Import-Module Citrix.StoreFront
   ```

   すべてのコマンドレットをインポートするには、次のように入力します:

   ```
   Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("
   Citrix.StoreFront")} | Import-Module
   ```

インポートが完了すると、各コマンドレットとそのヘルプにアクセスできます。

SDK の導入

スクリプトを作成するには、次の手順を実行します:

1. StoreFront によって **%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples** フォルダー内にインストールされた、指定の SDK サンプルの一つを実行します。
2. 独自のスクリプトのカスタマイズを容易にするため、サンプル スクリプトをレビューして、各部の実行内容について把握します。詳しくは、スクリプトの実行内容についての詳細を説明している使用例を参照してください。
3. 例のスクリプトをより実際の環境に応じて編集します。これを行うには、以下の手順に従います:
    - PowerShell ISE または同様のツールを使ってスクリプトを編集します。
    - 変数を使って、再使用または変更するための値を割り当てます。
    - 不要なコマンドを削除します。
    - StoreFront コマンドレットはプレフィックス STF により識別することができます。
    - **Get-Help** コマンドレットを使って、特定のコマンド上により詳細な情報のためのコマンドレット名および **-Full** パラメーターを指定します。

例

> 注:
>
> SDK に拡張や修正が追加されていることがあるため、例のスクリプトをコピーして貼り付けるのではなく、説明されている手順を実際に実行することをお勧めします。

例	説明
簡素な展開の作成	スクリプト：単一の XenDesktop サーバーで構成された StoreFront Controller のある簡素な展開を作成します。
リモートアクセス展開の作成	スクリプト：以前のスクリプト上に構築して、展開にリモートアクセスを追加します。
最適な起動ゲートウェイがあるリモートアクセス展開の作成	スクリプト：以前のスクリプト上に構築して、ユーザーエクスペリエンスをより良いものに吸うため、優先する最適な起動ゲートウェイを追加します。

例：簡素な展開の作成

次の例では、1 つの XenDesktop Controller で構成された簡素な展開の作成方法を示します。

まず、「SDK の導入」で説明されている手順を実行しておく必要があります。StoreFront 展開を自動化するスクリプトの作成について説明した手法を使って、この例をカスタマイズできます。

> 注:
>
> SDK に拡張や修正が追加されていることがあるため、このドキュメントのスクリプト例をコピーして貼り付けるのではなく、このドキュメントで説明されている手順を実際に実行することをお勧めします。

スクリプトの理解　ここでは、StoreFront により生成されるスクリプトの各部で何を実行しているかについて説明します。これを理解することで、スクリプトを目的に応じてカスタマイズできるようになります。

- エラー処理要件を設定し、必要な StoreFront モジュールをインポートします。より新しいバージョンの PowerShell ではインポートの必要はありません。

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox")]
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP"
    )
    # Import StoreFront modules. Required for versions of PowerShell earlier than 3.0 that do not support autoloading
    Import-Module Citrix.StoreFront
    Import-Module Citrix.StoreFront.Stores
    Import-Module Citrix.StoreFront.Authentication
    Import-Module Citrix.StoreFront.WebReceiver
<!--NeedCopy-->
```

- 指定の **$StoreVirtualPath** をベースとして認証および Citrix Receiver for Web サービスの仮想パスを自動化します。仮想パスは常に IIS のパスであるため、**$StoreVirtualPath** は **$StoreIISpath** と同じです。したがって Powershell では、「/Citrix/Store」、「/Citrix/StoreWeb」または「/Citrix/StoreAuth」のような値が使用されます。

```
# Determine the Authentication and Receiver virtual path to use based of the Store
$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
$receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
<!--NeedCopy-->
```

- 必要な StoreFront サービスの追加準備に備えて新しい展開を作成します（まだ存在していない場合）。**-Confirm:$false** は、展開を進めることができることを確認する要件を無効にします。


```
# Determine if the deployment already exists
$existingDeployment = Get-STFDeployment
if(-not $existingDeployment)
{

    # Install the required StoreFront components
    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
        Confirm:$false
 }

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
{

    # The deployment exists but it is configured to the desired
        hostbase url
    Write-Output "A deployment has already been created with the
        specified hostbase url on this server and will be used."
 }

else
{

    Write-Error "A deployment has already been created on this
        server with a different host base url."
 }

<!--NeedCopy-->
```

- 新しい認証サービスを指定された仮想パスで作成します（パスに認証サービスが存在しない場合）。ユーザー名とパスワードを使ったデフォルトの認証方法が有効です。

```
# Determine if the authentication service at the specified
    virtual path exists
$authentication = Get-STFAuthenticationService -VirtualPath
    $authenticationVirtualPath
if(-not $authentication)
{

    # Add an Authentication service using the IIS path of the
        Store appended with Auth
    $authentication = Add-STFAuthenticationService
        $authenticationVirtualPath
 }

else
{

    Write-Output "An Authentication service already exists at the
         specified virtual path and will be used."
 }

<!--NeedCopy-->
```


- 指定された仮想パスで、配列 **$XenDesktopServers** で定義されたサーバーがある 1 つの XenDesktop Controller で構成された新しいストアサービスを作成します（まだ存在していない場合）。

```
# Determine if the store service at the specified virtual path exists
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
if(-not $store)
{

# Add a Store that uses the new Authentication service configured to publish resources from the supplied servers
$store = Add-STFStoreService -VirtualPath $StoreVirtualPath -AuthenticationService $authentication -FarmName $Farmtype -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers `
     -Port $Port -SSLRelayPort $SSLRelayPort -TransportType $TransportType
 }

else
{

    Write-Output "A Store service already exists at the specified virtual path and will be used. Farm and servers will be appended to this store."
    # Get the number of farms configured in the store
    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count
    # Append the farm to the store with a unique name
    Add-STFStoreFarm -StoreService $store -FarmName "Controller$($farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers -Port $Port `
     -SSLRelayPort $SSLRelayPort -TransportType $TransportType
 }

<!--NeedCopy-->
```

- 指定の IIS 仮想パスで Citrix Receiver for Web サービスを追加して、上記で作成されたストアで公開されたアプリケーションにアクセスします。

```
# Determine if the receiver service at the specified virtual path exists
$receiver = Get-STFWebReceiverService -VirtualPath $receiverVirtualPath
if(-not $receiver)
{

    # Add a Receiver for Web site so users can access the applications and desktops in the published in the Store
    $receiver = Add-STFWebReceiverService -VirtualPath $receiverVirtualPath -StoreService $store
 }

```



```
else
{

    Write-Output "A Web Receiver service already exists at the
        specified virtual path and will be used."
 }

<!--NeedCopy-->
```

- ストアに対して XenApp サービスを有効にして、古い Citrix Receiver または Citrix Workspace アプリクライアントは公開アプリケーションに接続できます。

```
# Determine if PNA is configured for the Store service
$storePnaSettings = Get-STFStorePna -StoreService $store
if(-not $storePnaSettings.PnaEnabled)
{

# Enable XenApp services on the store and make it the default for
    this server
Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
   -DefaultPnaService
 }

<!--NeedCopy-->
```

例：リモートアクセス展開の作成

次の例は以前のスクリプト上に構築して、リモートアクセスのある展開を追加します。

まず、「SDK の導入」で説明されている手順を実行しておく必要があります。StoreFront 展開を自動化するスクリプトの作成について説明した手法を使って、この例をカスタマイズできます。

> 注：
>
> SDK に拡張や修正が追加されていることがあるため、このドキュメントのスクリプト例をコピーして貼り付けるのではなく、このドキュメントで説明されている手順を実際に実行することをお勧めします。

スクリプトの理解　ここでは、StoreFront により生成されるスクリプトの各部で何を実行しているかについて説明します。これを理解することで、スクリプトを目的に応じてカスタマイズできるようになります。

- エラー処理要件を設定し、必要な StoreFront モジュールをインポートします。より新しいバージョンの PowerShell ではインポートの必要はありません。

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [Parameter(Mandatory=$true)]
    [long]$SiteId = 1,
    [string]$Farmtype = "XenDesktop",
```



```
7       [Parameter(Mandatory=$true)]
8       [string[]]$FarmServers,
9       [string]$StoreVirtualPath = "/Citrix/Store",
10      [bool]$LoadbalanceServers = $false,
11      [int]$Port = 80,
12      [int]$SSLRelayPort = 443,
13      [ValidateSet("HTTP","HTTPS","SSL")]
14      [string]$TransportType = "HTTP",
15      [Parameter(Mandatory=$true)]
16      [Uri]$GatewayUrl,
17      [Parameter(Mandatory=$true)]
18      [Uri]$GatewayCallbackUrl,
19      [Parameter(Mandatory=$true)]
20      [string[]]$GatewaySTAUrls,
21      [string]$GatewaySubnetIP,
22      [Parameter(Mandatory=$true)]
23      [string]$GatewayName
24  )
25  Set-StrictMode -Version 2.0
26
27  # Any failure is a terminating failure.
28  $ErrorActionPreference = 'Stop'
29  $ReportErrorShowStackTrace = $true
30  $ReportErrorShowInnerException = $true
31  # Import StoreFront modules. Required for versions of PowerShell
       earlier than 3.0 that do not support autoloading
32  Import-Module Citrix.StoreFront
33  Import-Module Citrix.StoreFront.Stores
34  Import-Module Citrix.StoreFront.Roaming
35  <!--NeedCopy-->
```

- 以前のサンプルスクリプトを呼び出して、内部アクセスの StoreFront 展開を作成します。ベース展開が拡張され、リモートアクセスがサポートされます。

```
1  # Create a simple deployment by invoking the SimpleDeployment
       example
2  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
       Definition -Parent
3  $scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"
4  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
       FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
       Farmtype $Farmtype `
5       -LoadbalanceServers $LoadbalanceServers -Port $Port  -
           SSLRelayPort $SSLRelayPort -TransportType $TransportType
6  <!--NeedCopy-->
```

- リモートアクセスがサポートされるように更新する必要があるため、簡素な展開で作成されたサービスを取得します。

```
1  # Determine the Authentication and Receiver sites based on the
       Store
2  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3  $authentication = Get-STFAuthenticationService -StoreService
```



```
    $store
$receiverForWeb = Get-STFWebReceiverService -StoreService $store
<!--NeedCopy-->
```

- Citrix Gateway を使用したリモートアクセスで必要な Citrix Receiver for Web サービス上で、CitrixAGBasic を有効にします。サポートされているプロトコルから Citrix Receiver for Web の CitrixAGBasic および ExplicitForms 認証方法を取得します。

```
# Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms
    authentication method from the supported protocols
# Included for demonstration purposes as the protocol name can be
    used directly if known
$receiverMethods = Get-
    STFWebReceiverAuthenticationMethodsAvailable | Where-Object {
 $_ -match "Explicit" -or $_ -match "CitrixAG"  }

# Enable CitrixAGBasic in Receiver for Web (required for remote
    access)
Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods
    $receiverMethods
<!--NeedCopy-->
```

- 認証サービスで CitrixAGBasic を有効にします。これはリモートアクセスで必要です。

```
# Get the CitrixAGBasic authentication method from the protocols
    installed.
# Included for demonstration purposes as the protocol name can be
    used directly if known
$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-
    Object {
 $_ -match "CitrixAGBasic"  }

# Enable CitrixAGBasic in the Authentication service (required
    for remote access)
Enable-STFAuthenticationServiceProtocol -AuthenticationService
    $authentication -Name $citrixAGBasic
<!--NeedCopy-->
```

- 新しいリモートアクセスゲートウェイを、オプションのサブネット IP アドレスを指定して追加し、リモートでアクセスするストアに登録します。

```
# Add a new Gateway used to access the new store remotely
Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -
    Version Version10_0_69_4 -GatewayUrl $GatewayUrl '
-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
    $GatewaySTAUrls
# Get the new Gateway from the configuration (Add-
    STFRoamingGateway will return the new Gateway if -PassThru is
    supplied as a parameter)
$gateway = Get-STFRoamingGateway -Name $GatewayName
# If the gateway subnet was provided then set it on the gateway
    object
```



```
if($GatewaySubnetIP)
{

    Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
       $GatewaySubnetIP
 }

# Register the Gateway with the new Store
Register-STFStoreGateway -Gateway $gateway -StoreService $store -
   DefaultGateway
<!--NeedCopy-->
```

例：最適な起動ゲートウェイがあるリモートアクセス展開の作成

次の例は以前のスクリプト上に構築して、オプションの起動ゲートウェイリモートアクセスのある展開を追加します。

まず、「SDK の導入」で説明されている手順を実行しておく必要があります。StoreFront 展開を自動化するスクリプトの作成について説明した手法を使って、この例をカスタマイズできます。

> 注:
>
> SDK に拡張や修正が追加されていることがあるため、このドキュメントのスクリプト例をコピーして貼り付けるのではなく、このドキュメントで説明されている手順を実際に実行することをお勧めします。

スクリプトの理解　ここでは、StoreFront により生成されるスクリプトの各部で何を実行しているかについて説明します。これを理解することで、スクリプトを目的に応じてカスタマイズできるようになります。

- エラー処理要件を設定し、必要な StoreFront モジュールをインポートします。より新しいバージョンの PowerShell ではインポートの必要はありません。

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
```



```
19      [string[]]$GatewaySTAUrls,
20      [string]$GatewaySubnetIP,
21      [Parameter(Mandatory=$true)]
22      [string]$GatewayName,
23      [Parameter(Mandatory=$true)]
24      [Uri]$OptimalGatewayUrl,
25      [Parameter(Mandatory=$true)]
26      [string[]]$OptimalGatewaySTAUrls,
27      [Parameter(Mandatory=$true)]
28      [string]$OptimalGatewayName
29  )
30  Set-StrictMode -Version 2.0
31  # Any failure is a terminating failure.
32  $ErrorActionPreference = 'Stop'
33  $ReportErrorShowStackTrace = $true
34  $ReportErrorShowInnerException = $true
35  # Import StoreFront modules. Required for versions of PowerShell
        earlier than 3.0 that do not support autoloading
36  Import-Module Citrix.StoreFront
37  Import-Module Citrix.StoreFront.Stores
38  Import-Module Citrix.StoreFront.Roaming
39  <!--NeedCopy-->
```

- リモートアクセス展開スクリプト内に呼び出し、基本展開を構成し、リモートアクセスを追加します。

```
1  # Create a remote access deployment
2  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
       Definition -Parent
3  $scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
       ps1"
4  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
       FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
       Farmtype $Farmtype `
5       -LoadbalanceServers $LoadbalanceServers -Port $Port  -
           SSLRelayPort $SSLRelayPort -TransportType $TransportType `
6       -GatewayUrl $GatewayUrl -GatewayCallbackUrl
           $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
           GatewayName $GatewayName
7  <!--NeedCopy-->
```

- 優先的で最適な起動ゲートウェイを追加し、構成済みゲートウェイの一覧からそれを取得します。

```
1  # Add a new Gateway used for remote HDX access to desktops and
       apps
2  $gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -
       LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -
       SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
3  <!--NeedCopy-->
```

- 最適なゲートウェイを使用するためにストアサービスを取得し、ゲートウェイをファームからの起動に割り当てて登録します。

```
1  # Get the Store configured by SimpleDeployment.ps1
```



```
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
# Register the Gateway with the new Store for launch against all
    of the farms (currently just one)
$farmNames = @($store.FarmsConfiguration.Farms | foreach {
 $_.FarmName  }
)
Register-STFStoreOptimalLaunchGateway -Gateway $gateway -
    StoreService $store -FarmName $farmNames
<!--NeedCopy-->
```

StoreFront のトラブルシューティング

June 6, 2024

インストールログ

StoreFront のインストール時やアンインストール時に、インストーラーにより *C:\Windows\Temp\StoreFront* に以下のログファイルが作成されます。これらのログファイルには、作成元のコンポーネントと日時を示すファイル名が付けられます。

- Citrix-DeliveryServicesRoleManager-*.log: StoreFront のインタラクティブインストール時に作成されます。
- Citrix-DeliveryServicesSetupConsole-*.log: StoreFront のサイレントインストール時、インタラクティブアンインストール時、およびサイレントアンインストール時に作成されます。
- CitrixMsi-CitrixStoreFront-x64-*.log: StoreFront のインタラクティブインストール時、サイレントインストール時、インタラクティブアンインストール時、およびサイレントアンインストール時に作成されます。

イベントログ

StoreFront の認証サービス、ストア、および Receiver for Web サイトのイベントは、Windows イベントログに書き込まれます。生成されたイベントは StoreFront のアプリケーションログに書き込まれます。このログを表示するには、イベントビューアで ［アプリケーションとサービスログ］**>** ［**Citrix Delivery Services**］または［**Windows** ログ］**>** ［アプリケーション］の順に選択します。単一イベントに対して同じログエントリが何度も書き込まれないようにするには、認証サービス、ストア、および Receiver for Web サイトの構成ファイルを編集してログ調整を構成します。

ログ調整

1. 認証サービス、ストア、または Receiver for Web サイトの *web.config* ファイルをテキストエディターで開きます。これらのファイルは通常、それぞれ C:\inetpub\wwwroot\Citrix\Authentication、

C:\inetpub\wwwroot\Citrix\storename、C:\inetpub\wwwroot\Citrix\storenameWeb\フォルダーにあります。ここで、storename はストアの作成時に指定した名前です。

2. ファイル内で次の要素を検索します。

   <logger duplicateInterval="00:01:00"duplicateLimit="10">

   StoreFront のデフォルトでは、重複するログエントリの数が 1 分あたり 10 件までに制限されます。

3. duplicateInterval 属性の値を変更して、重複エントリの監視期間を時間、分、秒で設定します。duplicate-Limit 属性の値を変更して、指定した監視期間内に記録される重複エントリの数を設定します。この数を超えるとログ調整が実行されます。

ログ調整が実行されると、指定した数を超える重複ログエントリが抑制され、それを示す警告メッセージが記録されます。監視期間が経過すると、ログ調整が解除され、それを示す情報メッセージが記録されます。

Powershell と管理コンソールのログ

PowerShell または管理コンソールを介して行われた構成の変更のログが`C:\Program Files\Citrix\Receiver StoreFront\Admin\logs`に記録されます。このログファイルの名前は、実行されたコマンド処理、対象、および実行順序を識別するための日時で構成されます。

診断ログ

StoreFront は診断ログを`c:\Program Files\Citrix\Receiver StoreFront\admin\trace`に書き込みます

デフォルトでは、エラー、警告、情報レベルのメッセージがログに記録されます。ほとんどの場合、これには問題を診断するのに十分な情報が含まれています。

トラブルシューティングの目的で、追加の詳細ログを有効にすることができます。これは、Citrix サポートから要求された場合にのみ必要です。これはパフォーマンスに影響を与える可能性があるため、トラブルシューティングが完了したら`TraceLevel`を`Info`に戻す必要があります。

詳細ログを有効にするには、以下の手順を実行します:

1. ローカル管理者権限を持つアカウントを使用して、Windows PowerShell を起動します
2. コマンドを入力します:

   ```
   1 Set-STFDiagnostics -All -TraceLevel "Verbose" -confirm:$False
   2 <!--NeedCopy-->
   ```

   これにより、確認を求めるプロンプトを表示せずに、すべてのサービスの「詳細」ログが有効になります。このコマンドを入力すると、Storefront サービスが再起動されます。PowerShell プロンプトが戻り、サービスの再起動が完了したことを確認するまで待ちます。これらのサービスが再起動している間、ユーザーは StoreFront サーバーにアクセスできません。

3. 問題を再現してログを作成します。
4. すべてのサービスのログ記録をデフォルトレベルに戻します

```
 Set-STFDiagnostics -All -TraceLevel "Info" -confirm:$False
<!--NeedCopy-->
```

診断ログをさらにカスタマイズできます:

- StoreFront はサービスごとに個別のログファイルに書き込みます。デフォルトでは、各ログファイルは最大 200Mb であり、StoreFront は古いログファイルを削除する前にサービスごとに最大 5 つのログファイルに書き込みます。書き込まれるログのサイズまたは数をカスタマイズする必要がある場合は、`-FileSizeKb`および`-FileCount`パラメーターを使用してこれを行うことができます。
- `-TraceLevel`を使用してログに記録される詳細レベルを変更します。使用できる値は、`Off`、`Error`、`Warning`、`Info`、または`Verbose`です。
- パラメーター`-All`を使用すると、すべてのサービスのログパラメーターが設定されます。`-Service [Service name]`を使用して、個々のサービスのログをカスタマイズできます

`Set-STFDiagnostics`コマンドレットについて詳しくは、StoreFront PowerShell SDK のドキュメントを参照してください。

Launch.ica ファイルのログ

ユーザーがアプリまたはデスクトップを起動すると、StoreFront が launch.ica というファイルを生成します。このファイルは、Workspace アプリが読み取って、アプリやデスクトップへの接続方法を決めるのに使用されます。構成によっては、このファイルはメモリに保存され、直接アクセスできない可能性があります。起動エラーを診断するには、launch.ica の内容を表示するのが役に立ちます。

クライアント PC で launch.ica ファイルのログ作成を有効にするには、次の手順を完了します:

1. レジストリエディターを使用して次のレジストリキーを参照します:

   32 ビットシステム: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

   64 ビットシステム: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

2. 次の 2 つの文字列キー値を設定します:

   - LogFile=「ログファイルへのパス」
   - LogICAFile=true

   例:


```
LogFile=C:\ica\ica.log
LogICAFile=true
<!--NeedCopy-->
```

> 注:
>
> トラブルシューティング目的以外で環境で ICA ファイルを使用する場合について詳しくは、CTX200126を参照してください。

サードパーティ製品についての通知

June 6, 2024

StoreFront には、以下の条件でライセンスが有効になったサードパーティソフトウェアが含まれている可能性があります。この一覧は、一覧の作成日時点のサードパーティソフトウェアを使用して生成されています。この一覧は製品のバージョンに応じて変更されることがあります。この一覧は「現状のまま」提供されるものであり、適用法令により許容される限度において、CITRIX およびその製品供給者は、一覧または一覧の正確性もしくは完全性について、あるいは一覧の使用または配布によって生じる結果について、明示または黙示を問わず、法令上その他いかなる保証または条件もお客様に付与するものではありません。この一覧を使用または配布することにより、お客様は、いかなる場合においても、一覧の使用または配布によって生じる特別、直接的、間接的、または付随的損害、あるいはその他の損害について、CITRIX が責任を負わないことに同意するものとします。

Castle Windsor 3.3.0

Copyright 2004-2013 Castle Project - http://www.castleproject.org/

Apache License、Version 2.0 によるライセンス

Microsoft Unity Application Block (Unity) 2.1

Copyright © 2011 Microsoft Corporation.

Microsoft Public License（MS-PL）によるライセンスhttps://msdn.microsoft.com/en-us/library/hh237493.aspx

Microsoft Patterns & Practices：Prism 2.2

Copyright © 2010 Microsoft Corporation.

Microsoft Public License（MS-PL）によるライセンスhttp://compositewpf.codeplex.com/releases/view/46046

Microsoft & Practices：Common Service Locator 1.0

Copyright © Microsoft Corporation.

Microsoft Public License（MS-PL）によるライセンス

Microsoft .Net Reference Source

Copyright © Microsoft Corporation. MIT ライセンスによるライセンス。

マネージド済み リリース **1.9.4**

Copyright © Microsoft Corporation.

Microsoft Public License（MS-PL）によるライセンスhttp://managedesent.codeplex.com/license

jQuery UI - v1.10.4 - 2014-03-12

http://jqueryui.com/

Copyright 2014 jQuery Foundation and other contributors; Licensed MIT

jQuery JavaScript Library v1.12.4

http://jquery.com/

Sizzle.js を含む

http://sizzlejs.com/

Copyright jQuery Foundation and other contributors

MIT ライセンスによるライセンス

http://jquery.org/license

日付：2016-05-20T17:17Z

jQuery jScrollPane v2.0.0beta11

jScrollPane - v2.0.0beta11 - 2011-07-04 http://jscrollpane.kelvinluck.com/

Copyright (c) 2010 Kelvin Luck

MIT および GPL ライセンスのデュアルライセンス。

jquery.contextmenu.js

jQuery Plugin for Context Menus

http://www.JavascriptToolbox.com/lib/contextmenu

Copyright (c) 2008 Matt Kruse (javascripttoolbox.com)

MIT および GPL ライセンスのデュアルライセンス。

jQuery plugin for Hammer.JS - v1.0.0 - 2014-01-02

http://eightmedia.github.com/hammer.js

Copyright (c) 2014 Jorik Tangelder j.tangelder@gmail.com;

MIT ライセンスによるライセンス

jQuery MouseWheel

Copyright (c) 2011 Brandon Aaron (http://brandonaaron.net)

MIT ライセンス（LICENSE.txt）によるライセンス。

WPF Toolkit 3.5

WPF Toolkit (http://wpf.codeplex.com/) Copyright (c) 2006-2014 Microsoft

MS-PL ライセンスhttp://wpf.codeplex.com/license
9

Extended WPF Toolkit 3.0

Copyright (C) 2007-2013 Xceed Software Inc.

このプログラムは、http://wpftoolkit.codeplex.com/licenseで公開されている Microsoft Public License（Ms-PL）の条件に基づいて提供されます。

追加の機能、コントロール、迅速なプロフェッショナルサポートについては、Plus Edition（http://xceed.com/wpf_toolkit）を使用してください

最新情報：Twitter で @datagrid をフォローするかhttp://facebook.com/datagridsでいいね! してください

WiX Toolset

Copyright (c) Outercurve Foundation. Common Public License Version 1.0.

CLR Security

Copyright (c) Microsoft Corporation. Microsoft Limited Permissive License（MS-LPL）

Stack Exchange Redis 1.1

StackExchange.Redis.StrongName 1.1 https://stackexchange.github.io/StackExchange.Redis Copyright (c) 2014 Stack Exchange

MIT ライセンスによるライセンス

Newtonsoft JSON

Copyright (c) 2007 James Newton-King

MIT ライセンスによるライセンス。

jQuery JavaScript Library v3.7.0

https://jquery.com/

Sizzle.js を含む

https://sizzlejs.com/

Copyright JS Foundation and other contributors

MIT ライセンスによるライセンス

https://jquery.org/license

日付：2020-05-04T22:49Z

jQuery UI - v1.13.2 -2022 -07-14

http://jqueryui.com

Copyright jQuery Foundation and other contributors; Licensed MIT

Hammer.JS - v2.0.4 - 2014-09-28

Hammer.JS - v2.0.8 - 2016-04-23

http://hammerjs.github.io/

Copyright (c) 2016 Jorik Tangelder;

MIT ライセンスによるライセンス

VelocityJS.org (1.5.0)

velocity-animate (C) 2014-2017 Julian Shapiro.

MIT ライセンスによるライセンス。詳しくは、プロジェクトルートのライセンスファイルを参照してください。

slick.js - 1.8.0

MIT ライセンス（MIT）

Copyright (c) 2013-2016

jQuery UI Touch Punch 0.2.3

Copyright 2011–2014, Dave Furfero

MIT および GPL バージョン 2 ライセンスのデュアルライセンス。

付録：参照ライセンス

MIT ライセンス

```
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
```



```
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
<!--NeedCopy-->
```

Apache License、Version 2.0

```
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/


TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction,
   and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by
   the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all
   other entities that control, are controlled by, or are under common
   control with that entity. For the purposes of this definition,
   "control" means (i) the power, direct or indirect, to cause the
   direction or management of such entity, whether by contract or
   otherwise, or (ii) ownership of fifty percent (50%) or more of the
   outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity
   exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications,
   including but not limited to software source code, documentation
   source, and configuration files.

   "Object" form shall mean any form resulting from mechanical
   transformation or translation of a Source form, including but
   not limited to compiled object code, generated documentation,
   and conversions to other media types.

   "Work" shall mean the work of authorship, whether in Source or
   Object form, made available under the License, as indicated by a
```



```
    copyright notice that is included in or attached to the work
    (an example is provided in the Appendix below).

    "Derivative Works" shall mean any work, whether in Source or Object
    form, that is based on (or derived from) the Work and for which the
    editorial revisions, annotations, elaborations, or other modifications
    represent, as a whole, an original work of authorship. For the purposes
    of this License, Derivative Works shall not include works that remain
    separable from, or merely link (or bind by name) to the interfaces of,
    the Work and Derivative Works thereof.

    "Contribution" shall mean any work of authorship, including
    the original version of the Work and any modifications or additions
    to that Work or Derivative Works thereof, that is intentionally
    submitted to Licensor for inclusion in the Work by the copyright owner
    or by an individual or Legal Entity authorized to submit on behalf of
    the copyright owner. For the purposes of this definition, "submitted"
    means any form of electronic, verbal, or written communication sent
    to the Licensor or its representatives, including but not limited to
    communication on electronic mailing lists, source code control systems,
    and issue tracking systems that are managed by, or on behalf of, the
    Licensor for the purpose of discussing and improving the Work, but
    excluding communication that is conspicuously marked or otherwise
    designated in writing by the copyright owner as "Not a Contribution."

    "Contributor" shall mean Licensor and any individual or Legal Entity
    on behalf of whom a Contribution has been received by Licensor and
    subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of
    this License, each Contributor hereby grants to You a perpetual,
    worldwide, non-exclusive, no-charge, royalty-free, irrevocable
    copyright license to reproduce, prepare Derivative Works of,
    publicly display, publicly perform, sublicense, and distribute the
    Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
    this License, each Contributor hereby grants to You a perpetual,
    worldwide, non-exclusive, no-charge, royalty-free, irrevocable
    (except as stated in this section) patent license to make, have made,
    use, offer to sell, sell, import, and otherwise transfer the Work,
    where such license applies only to those patent claims licensable
    by such Contributor that are necessarily infringed by their
```



```
   Contribution(s) alone or by combination of their Contribution(s)
   with the Work to which such Contribution(s) was submitted. If You
   institute patent litigation against any entity (including a
   cross-claim or counterclaim in a lawsuit) alleging that the Work
   or a Contribution incorporated within the Work constitutes direct
   or contributory patent infringement, then any patent licenses
   granted to You under this License for that Work shall terminate
   as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and
       do not modify the License. You may add Your own attribution
       notices within Derivative Works that You distribute, alongside
       or as an addendum to the NOTICE text from the Work, provided
       that such additional attribution notices cannot be construed
       as modifying the License.

   You may add Your own copyright statement to Your modifications and
   may provide additional or different license terms and conditions
   for use, reproduction, or distribution of Your modifications, or
   for any such Derivative Works as a whole, provided Your use,
   reproduction, and distribution of the Work otherwise complies with
   the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
   any Contribution intentionally submitted for inclusion in the Work
   by You to the Licensor shall be under the terms and conditions of
```



```
   this License, without any additional terms or conditions.
   Notwithstanding the above, nothing herein shall supersede or modify
   the terms of any separate license agreement you may have executed
   with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
   names, trademarks, service marks, or product names of the Licensor,
   except as required for reasonable and customary use in describing
      the
   origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this
      License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,
   incidental, or consequential damages of any character arising as a
   result of this License or out of the use or inability to use the
   Work (including but not limited to damages for loss of goodwill,
   work stoppage, computer failure or malfunction, or any and all
   other commercial damages or losses), even if such Contributor
   has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
   the Work or Derivative Works thereof, You may choose to offer,
   and charge a fee for, acceptance of support, warranty, indemnity,
   or other liability obligations and/or rights consistent with this
   License. However, in accepting such obligations, You may act only
   on Your own behalf and on Your sole responsibility, not on behalf
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS
<!--NeedCopy-->
```

Microsoft Public License（MS-PL）

```
This license governs use of the accompanying software. If you use the
```



```
    software, you accept this license. If you do not accept the license,
     do not use the software.
2
3   1. Definitions
4   The terms “reproduce,” “reproduction,” “derivative works,” and “
    distribution” have the
5   same meaning here as under U.S. copyright law.
6
7   A “contribution” is the original software, or any additions or
    changes to the software.
8
9   A “contributor” is any person that distributes its contribution under
     this license.
10
11   “Licensed patents” are a contributor’ s patent claims that read
    directly on its contribution.
12
13  2. Grant of Rights
14
15  (A) Copyright Grant- Subject to the terms of this license, including
    the license conditions and limitations in section 3, each
    contributor grants you a non-exclusive, worldwide, royalty-free
    copyright license to reproduce its contribution, prepare derivative
    works of its contribution, and distribute its contribution or any
    derivative works that you create.
16
17  (B) Patent Grant- Subject to the terms of this license, including the
    license conditions and limitations in section 3, each contributor
    grants you a non-exclusive, worldwide, royalty-free license under
    its licensed patents to make, have made, use, sell, offer for sale,
    import, and/or otherwise dispose of its contribution in the software
     or derivative works of the contribution in the software.
18
19  3. Conditions and Limitations
20
21  (A) No Trademark License- This license does not grant you rights to use
     any contributors’ name, logo, or trademarks.
22
23  (B) If you bring a patent claim against any contributor over patents
    that you claim are infringed by the software, your patent license
    from such contributor to the software ends automatically.
24
25  (C) If you distribute any portion of the software, you must retain all
    copyright, patent, trademark, and attribution notices that are
    present in the software.
26
27  (D) If you distribute any portion of the software in source code form,
    you may do so only under this license by including a complete copy
    of this license with your distribution. If you distribute any
    portion of the software in compiled or object code form, you may
    only do so under a license that complies with this license.
28
29  (E) The software is licensed “as-is.” You bear the risk of using it.
```



```
      The contributors give no express warranties, guarantees or
      conditions. You may have additional consumer rights under your local
       laws which this license cannot change. To the extent permitted
      under your local laws, the contributors exclude the implied
      warranties of merchantability, fitness for a particular purpose and
      non-infringement.
<!--NeedCopy-->
```