



# フェデレーション認証サービス 1912 LTSR

# Contents

|                                            |    |
|--------------------------------------------|----|
| フェデレーション認証サービス 1912 LTSR                   | 9  |
| 参照                                         | 10 |
| フェデレーション認証サービス 1912 LTSR                   | 11 |
| 修正された問題                                    | 11 |
| 1912で修正された問題                               | 11 |
| 既知の問題                                      | 11 |
| サードパーティに関する通知                              | 12 |
| システム要件                                     | 13 |
| インストールと構成                                  | 15 |
| インストールとセットアップの順序                           | 15 |
| フェデレーション認証サービスをインストールする                    | 15 |
| StoreFront™ストアでFASプラグインを有効にする              | 15 |
| Delivery Controller™を構成する                  | 16 |
| グループポリシーを構成する                              | 16 |
| セッション内証明書のサポートとロック時の切断                     | 20 |
| セッション内証明書のサポート                             | 20 |
| ロック時の切断                                    | 21 |
| Federated Authentication Service管理コンソールの使用 | 21 |
| 証明書テンプレートを展開する                             | 21 |
| Active Directory証明書サービスをセットアップする           | 23 |
| フェデレーション認証サービスを承認する                        | 24 |
| ユーザー規則の構成                                  | 25 |
| 高度な使用法                                     | 28 |
| アップグレードに関する考慮事項                            | 28 |
| セキュリティに関する考慮事項                             | 29 |
| 委任された登録エージェント                              | 29 |

|                       |    |
|-----------------------|----|
| アクセス制御リストの構成          | 29 |
| ファイアウォール設定            | 29 |
| イベントログの監視             | 30 |
| ハードウェアセキュリティモジュール     | 30 |
| PowerShell SDK        | 31 |
| パフォーマンスカウンター          | 31 |
| イベントログ                | 33 |
| 管理イベント                | 33 |
| IDアサーションの作成           | 34 |
| 証明書利用側としての動作          | 35 |
| セッション内証明書サーバー         | 35 |
| FASアサーションプラグイン        | 36 |
| ログオン                  | 37 |
| セッション内証明書             | 38 |
| 証明書要求とキーペアの生成         | 38 |
| 関連情報                  | 39 |
| 展開アーキテクチャ             | 40 |
| はじめに                  | 40 |
| 仕組み                   | 40 |
| 内部展開                  | 41 |
| Citrix Gatewayの展開     | 43 |
| ADFS SAML展開           | 46 |
| B2Bアカウントマッピング         | 47 |
| ウィンドウズ 10 アジュール AD 参加 | 48 |
| ADFS展開                | 50 |
| はじめに                  | 50 |
| SAMLの概要               | 50 |
| リダイレクトURL             | 50 |

|                                                        |    |
|--------------------------------------------------------|----|
| 識別子                                                    | 50 |
| 戻りアドレス                                                 | 51 |
| 署名証明書                                                  | 51 |
| シングルサインアウトURL                                          | 51 |
| 構成                                                     | 51 |
| SAMLポリシーを記入する                                          | 52 |
| 関連情報                                                   | 52 |
| Azure AD の統合                                           | 53 |
| はじめに                                                   | 53 |
| アーキテクチャ                                                | 54 |
| DNS ゾーンの作成                                             | 56 |
| クラウドサービスを作成する                                          | 57 |
| Windows仮想マシンを作成する                                      | 57 |
| ドメインコントローラー                                            | 58 |
| ADFSコントローラーとWebアプリケーションプロキシサーバー                        | 58 |
| Citrix Virtual Desktops™ デリバリーコントローラーおよびVDA            | 59 |
| 内部DNSを構成する                                             | 59 |
| 外部 DNS アドレスを構成する                                       | 60 |
| セキュリティグループを構成する                                        | 61 |
| ADFS 証明書を作成する                                          | 61 |
| Azure ADをセットアップする                                      | 62 |
| 新しいディレクトリを作成する                                         | 62 |
| グローバル管理者ユーザー (AzureAdmin) を作成する                        | 64 |
| ドメインを Azure AD に登録する                                   | 65 |
| Azure AD Connect をインストールする                             | 66 |
| Azure AD Join を有効にする                                   | 71 |
| Citrix Virtual AppsまたはCitrix Virtual Desktopsをインストールする | 74 |
| フェデレーション認証サービスをインストールする                                | 75 |

|                                                   |    |
|---------------------------------------------------|----|
| StoreFrontを構成する                                   | 75 |
| StoreFrontがCitrix Gatewayを使用するように構成する             | 76 |
| StoreFrontへのシングルサインオン用に新しいAzure ADアプリケーションを構成する   | 77 |
| アイコンの構成                                           | 78 |
| SAML認証の構成                                         | 78 |
| アプリケーションをユーザーに割り当てる                               | 81 |
| MyAppsページ                                         | 81 |
| シングルサインオンURL                                      | 82 |
| Citrix Gatewayのインストールと構成                          | 83 |
| Citrix Virtual Apps and Desktops セットアップウィザードを実行する | 84 |
| AD アカウント管理のためにドメインコントローラーを構成する                    | 84 |
| StoreFront アドレスを構成する                              | 84 |
| Citrix Gateway の展開を確認する                           | 84 |
| Citrix Gateway SAML認証サポートを有効にする                   | 85 |
| エンドツーエンドシステムを検証する                                 | 86 |
| 付録                                                | 87 |
| パブリックIPアドレスとDNSアドレスを提供する                          | 87 |
| ファイアウォールルール（セキュリティグループ）を設定する                      | 88 |
| 関連情報                                              | 89 |
| 高度な構成                                             | 90 |
| 関連情報                                              | 90 |
| 証明機関の構成                                           | 90 |
| TCPアクセス用にMicrosoft証明機関を構成する                       | 90 |
| ユーザー証明書を事前生成する                                    | 92 |
| Active Directoryユーザーのリストを取得する                     | 92 |
| FASサーバー                                           | 93 |
| 登録機関証明書の更新                                        | 94 |
| 関連情報                                              | 95 |

|                                        |     |
|----------------------------------------|-----|
| 秘密キーの保護                                | 96  |
| はじめに                                   | 96  |
| 秘密キーの構成設定                              | 97  |
| 構成シナリオの例                               | 100 |
| 例 1                                    | 100 |
| 例2                                     | 100 |
| 例 3                                    | 109 |
| FAS証明書ストレージ                            | 112 |
| 関連情報                                   | 113 |
| セキュリティとネットワーク構成                        | 113 |
| ネットワークアーキテクチャ                          | 113 |
| ファイアウォールとネットワークセキュリティ                  | 114 |
| シトリックス フェデレーテッド認証サービスとシトリックス クラウド™間の接続 | 115 |
| 管理者の役割                                 | 116 |
| グループポリシー設定                             | 116 |
| 証明書テンプレート                              | 117 |
| 証明書テンプレートの名前を変更する                      | 117 |
| 全般プロパティを変更する                           | 117 |
| 要求処理プロパティを変更する                         | 117 |
| 暗号化プロパティを変更する                          | 117 |
| キー構成証明プロパティを変更する                       | 117 |
| 置き換えられたテンプレートプロパティを変更する                | 118 |
| 拡張機能のプロパティを変更する                        | 118 |
| セキュリティプロパティを変更する                       | 118 |
| サブジェクト名のプロパティを変更する                     | 119 |
| サーバープロパティを変更する                         | 119 |
| 発行要件のプロパティを変更する                        | 119 |
| 互換性プロパティの変更                            | 120 |

|                                               |     |
|-----------------------------------------------|-----|
| 証明機関の管理                                       | 120 |
| テンプレートの公開                                     | 120 |
| ファイアウォール設定                                    | 120 |
| 登録の制限                                         | 120 |
| ポリシーモジュールと監査                                  | 121 |
| FAS管理                                         | 121 |
| ACLによるStoreFront、ユーザー、VDAの制限                  | 121 |
| ルールの構成                                        | 122 |
| 証明機関とテンプレートの構成                                | 122 |
| セッション内証明書と認証証明書                               | 122 |
| 秘密鍵の保護と鍵長                                     | 122 |
| イベントログ                                        | 122 |
| 管理アクセスと管理ツール                                  | 122 |
| シトリックス バーチャル アプリ、シトリックス バーチャル デスクトップ、およびVDA管理 | 123 |
| 者                                             |     |
| 一般的なWindowsサーバーのセキュリティ                        | 123 |
| 関連情報                                          | 123 |
| Windowsログオンの問題のトラブルシューティング                    | 123 |
| 証明書と公開キー基盤                                    | 123 |
| UPN名と証明書のマッピング                                | 125 |
| アクティブ ディレクトリのUPN名                             | 125 |
| 証明書マッピングサービス                                  | 125 |
| ログオンドメインコントローラーの選択を制御する                       | 126 |
| ドメインコントローラーの選択を制御する                           | 126 |
| 使用中のドメインコントローラーを特定する                          | 126 |
| アカウント監査イベントを有効にする                             | 126 |
| 証明書検証ログ                                       | 127 |
| 証明書の有効性を確認する                                  | 127 |

|                              |     |
|------------------------------|-----|
| CAPIログを有効にする                 | 127 |
| CAPI ログ                      | 127 |
| エラーメッセージ                     | 128 |
| Kerberosログ                   | 128 |
| イベントログメッセージ                  | 129 |
| ドメインコントローラー CAPI2 ログ         | 129 |
| ドメインコントローラーセキュリティログ          | 130 |
| VDA セキュリティログ                 | 131 |
| VDA CAPI ログ                  | 131 |
| VDA システムログ                   | 132 |
| エンドユーザーのエラーメッセージ             | 132 |
| 関連情報                         | 133 |
| PowerShellコマンドレット            | 133 |
| フェデレーション認証サービス 1912 ドキュメント履歴 | 134 |

# フェデレーション認証サービス 1912 LTSR

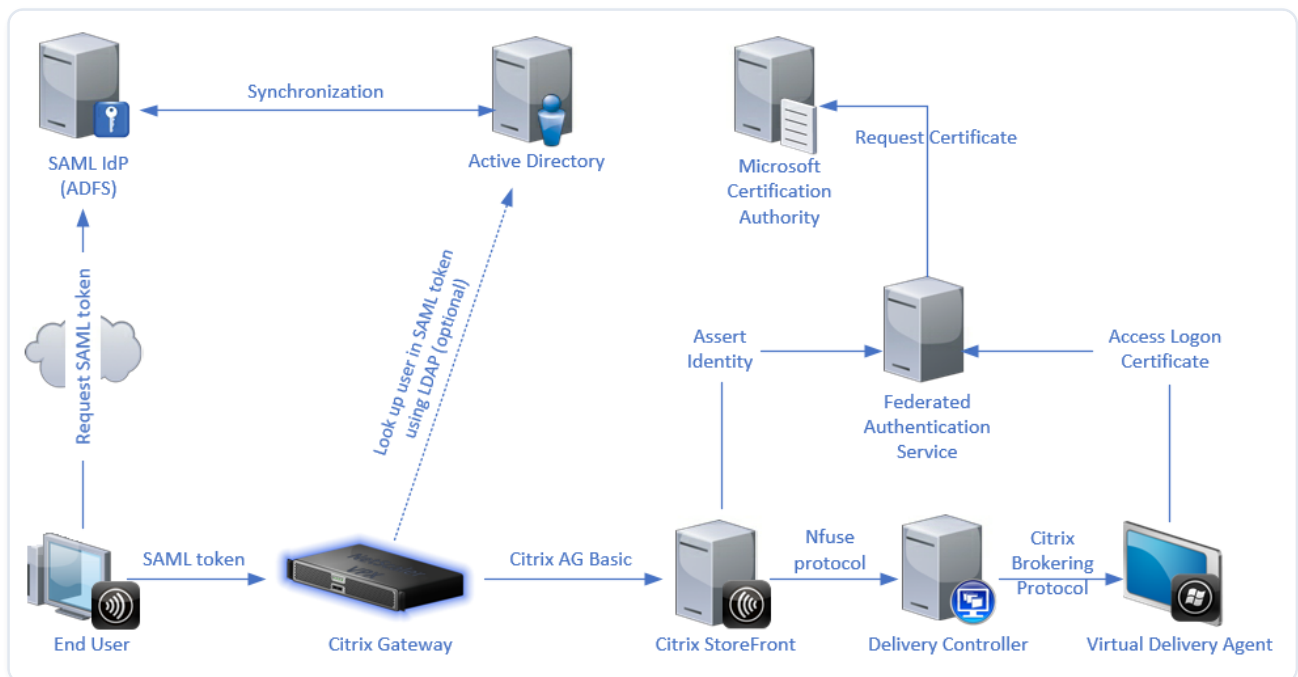
---

注記：

このドキュメントは、**フェデレーション認証サービス 1912** をサポートしています。これは、Citrix Virtual Apps and Desktops 7 1912 LTSR のベースラインコンポーネントです。最新のコンテンツについては、フェデレーション認証サービス [現在のリリースドキュメント](#) を参照してください。現在のリリース（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については、[ライフサイクルマイルストーン](#) で説明されています。

フェデレーション認証サービス（FAS）は、Active Directory 証明書サービスと統合するように設計された特権コンポーネントです。FASはユーザーに証明書を動的に発行し、スマートカードを持っているかのようにActive Directory環境にログオンできるようにします。これにより、StoreFront™はSAML（Security Assertion Markup Language）アサーションなど、より広範な認証オプションを使用できるようになります。SAMLは、インターネット上で従来のWindowsユーザーアカウントの代替として一般的に使用されています。

次の図は、FASがMicrosoft証明機関と統合し、StoreFrontおよびCitrix Virtual Apps and Desktops™ Virtual Delivery Agent（VDA）にサポートサービスを提供していることを示しています。



ユーザーがCitrix環境へのアクセスを要求すると、信頼されたStoreFrontサーバーはFASに接続します。FASは、単一のCitrix Virtual AppsまたはCitrix Virtual Desktops™セッションがそのセッションの証明書で認証できるようにするチケットを付与します。VDAがユーザーを認証する必要がある場合、FASに接続してチケットを引き換えます。ユーザー証明書の秘密キーにアクセスできるのはFASのみです。VDAは、証明書を使用して実行する必要がある署名および復号化操作をすべてFASに送信する必要があります。

## 参照

- Active Directory証明書サービス <[https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740\(v=ws.11\)](https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11))>
- 証明書ログオン用にWindowsを構成する <<http://support.citrix.com/article/CTX206156>>

# フェデレーション認証サービス 1912 LTSR

---

このフェデレーション認証サービスのリリースでは、全体的なパフォーマンスと安定性の向上に貢献するいくつかの問題に対処しています。新機能は追加されていません。

バグ修正に関する情報については、「修正された問題」(</ja-jp/federated-authentication-service/1912-ltsr/whats-new/fixed-issues.html>)を参照してください。

## 修正された問題

### 1912で修正された問題

比較対象: フェデレーション認証サービス 1909

Federated Authentication Service 1912には、以下の修正が含まれています。

- Citrix\_SmartcardLogon証明書テンプレートのプロパティで、Key Usage拡張機能の説明には「Digital signature」と「Key encipherment」のみが含まれるべきですが、追加の項目がリストされています。ただし、このテンプレートを使用して発行された証明書は正しいです。
- FAS管理コンソールを使用して証明書テンプレートをActive Directoryに展開する場合、テンプレートのセキュリティ権限に「自動登録」権限が含まれなくなりました。この権限はFASの正しい動作には不要であり、一部の顧客環境でドメインコンピューターによる不要な登録試行を引き起こしていました。

## 既知の問題

Federated Authentication Service 1912 には既知の問題はありません。

この警告は、レジストリエントリの変更を推奨するすべての回避策に適用されます。

**警告：**

レジストリを誤って編集すると、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ような深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

## サードパーティに関する通知

Federated Authentication Serviceのこのリリースには、以下のドキュメントに定義されている条件に基づいてライセンスされているサードパーティ製ソフトウェアが含まれる場合があります。

- [Citrix Virtual Apps and Desktops サードパーティに関する通知 \(PDFダウンロード\)](#)
- [FlexNet Publisher 2017 \(11.15.0.0\) の非商用ソフトウェア開示 \(PDFダウンロード\)](#)
- [FlexNet Publisher ドキュメント補足 FlexNet Publisher 11.15.0 で使用されているサードパーティおよびオープンソースソフトウェア \(PDFダウンロード\)](#)

# システム要件

- Federated Authentication Service (FAS) は、以下のWindows Serverバージョンでサポートされています。
  - Windows Server 2019、StandardおよびDatacenterエディション、およびServer Coreオプション
  - Windows Server 2016、StandardおよびDatacenterエディション、およびServer Coreオプション
  - Windows Server 2012 R2、StandardおよびDatacenterエディション、およびWindows Server 2012 R2のServer Core
- Citrix®は、他のCitrixコンポーネントを含まないサーバーにFASをインストールすることを推奨します。
- Windows Serverは保護されている必要があります。ドメインユーザーに証明書を自動的に発行できる登録機関証明書と秘密キーにアクセスでき、それらのユーザー証明書と秘密キーにもアクセスできます。
- FASのPowerShellコマンドレットには、FASサーバーにWindows PowerShell 64ビットがインストールされている必要があります。
- ユーザー証明書を発行するには、Microsoft Enterprise証明機関が必要です。

Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトでは、次のようになります。

- Delivery Controller、Virtual Delivery Agent (VDA)、およびStoreFront™サーバーはすべてサポートされているバージョンである必要があります。

**注：**

FASは、XenAppおよびXenDesktop 7.6 Long Term Service Release (LTSR)ではサポートされていません。

- マシンカタログを作成する前に、Federated Authentication Serviceのグループポリシー構成がVDAに正しく適用されている必要があります。詳細については、[グループポリシーの構成セクション](#)を参照してください。

このサービスの展開を計画する際は、[セキュリティに関する考慮事項](#)セクションを確認してください。

# インストールと構成

## インストールとセットアップの順序

1. フェデレーション認証サービスをインストールする (FAS)
2. StoreFrontストアでFASプラグインを有効にする
3. グループポリシーを構成する
4. FAS管理コンソールを使用して、(a) 提供されたテンプレートを展開する、(b) 証明機関をセットアップする、および (c) FASが証明機関を使用することを承認する
5. ユーザー規則を構成する

## フェデレーション認証サービスをインストールする

セキュリティのため、Citrix®は、フェデレーション認証サービス (FAS) を、ドメインコントローラーまたは証明機関と同様の方法で保護された専用サーバーにインストールすることを推奨します。ISOが挿入されたときに、自動実行スプラッシュ画面の**Federated Authentication Service**ボタンからFASをインストールできます。

これにより、次のコンポーネントがインストールされます。

- フェデレーション認証サービス
- FASをリモートで構成するためのPowerShellスナップインコマンドレット
- FAS管理コンソール
- FASグループポリシーテンプレート (CitrixFederatedAuthenticationService.admx/adml)
- シンプルな証明機関構成用の証明書テンプレートファイル
- パフォーマンスカウンターおよびイベントログ

## StoreFront™ストアでFASプラグインを有効にする

StoreFrontストアでFAS統合を有効にするには、管理者アカウントとして以下の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、またはストアの名前が異なる場合、以下のパステキストは異なることがあります。

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

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName
"FASClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider
"FASLogonDataProvider"
```

FASの使用を停止するには、以下のPowerShellスクリプトを使用します。

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

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName
"standardClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

## Delivery Controller™を構成する

FASを使用するには、Citrix Virtual AppsまたはCitrix Virtual Desktops™ Delivery Controllerが、それに接続できるStoreFrontサーバーを信頼するように構成します。**Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** PowerShellコマンドレットを実行します。

## グループポリシーを構成する

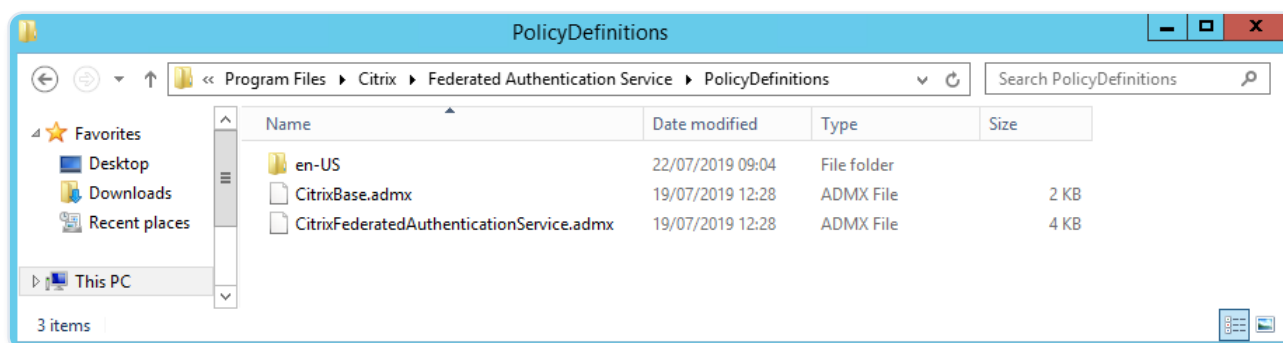
FASをインストールした後、インストールで提供されるグループポリシーテンプレートを使用して、グループポリシーでFASサーバーの完全なDNSアドレスを指定する必要があります。

**重要：**

チケットを要求するStoreFrontサーバーと、チケットを引き換えるVirtual Delivery Agent (VDA) が、DNSアドレスの構成を同一にしていることを確認してください。これには、グループポリシーオブジェクトによって適用される自動サーバー番号付けも含まれます。

簡素化のため、以下の例では、すべてのマシンに適用される単一のポリシーをドメインレベルで構成していますが、これは必須ではありません。StoreFrontサーバー、VDA、およびFAS管理コンソールを実行しているマシンが同じDNSアドレスのリストを参照している限り、FASは機能します。グループポリシーオブジェクトは各エントリにインデックス番号を追加することに注意してください。複数のオブジェクトを使用する場合、これも一致する必要があります。

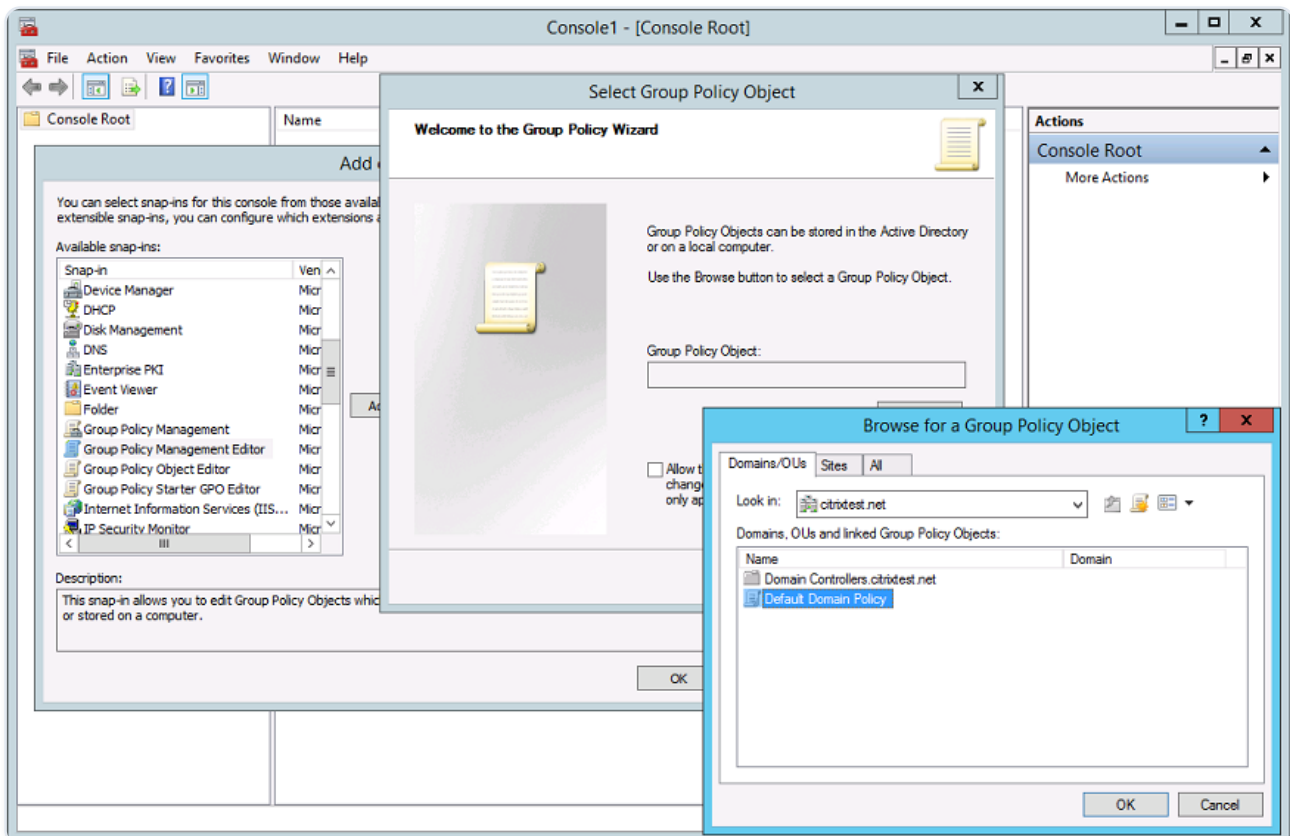
**手順 1.** FASをインストールしたサーバーで、C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx および CitrixBase.admx ファイル、および en-US フォルダーを見つけます。



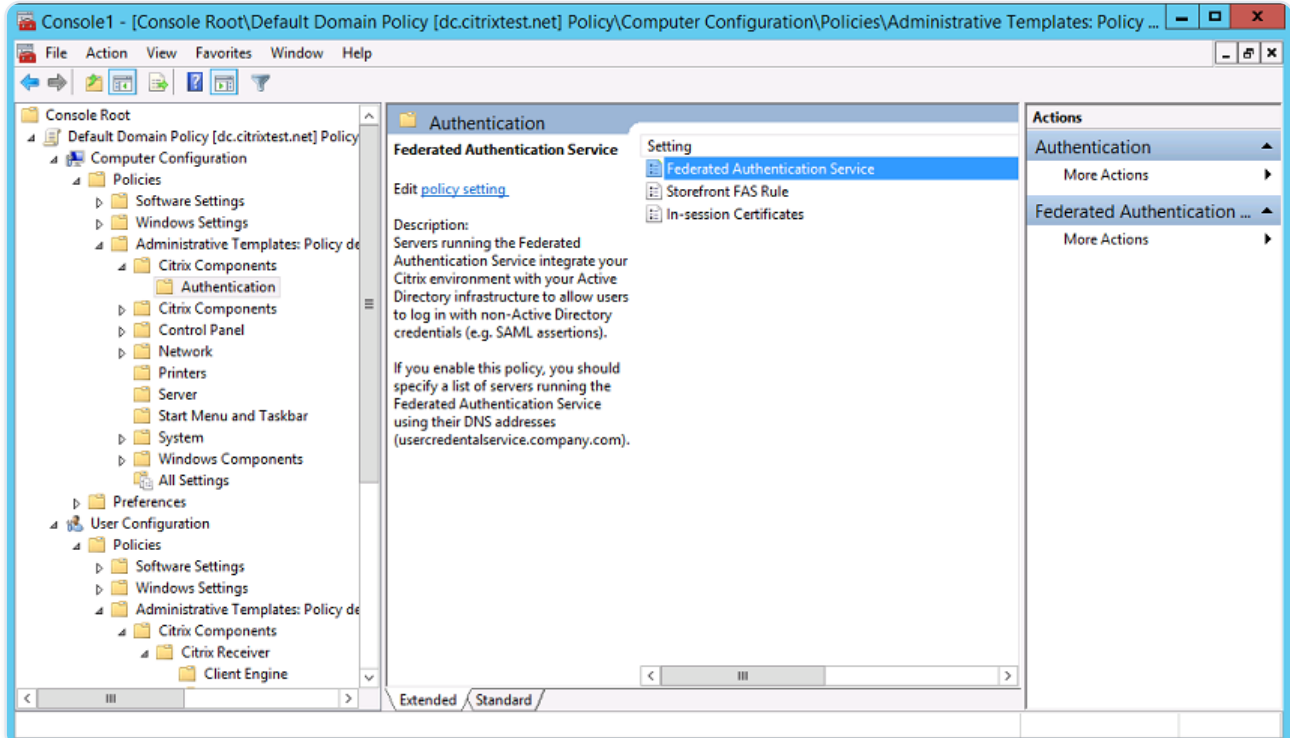
**手順 2.** これらをドメインコントローラーにコピーし、C:\Windows\PolicyDefinitionsおよびen-US サブフォルダーに配置します。

**手順 3.** Microsoft管理コンソール (コマンドラインからmmc.exe) を実行します。メニューバーから、**ファイル > スナップインの追加と削除**を選択します。**グループポリシー管理エディター**を追加します。

グループポリシーオブジェクトの入力を求められたら、**参照**を選択し、次に**既定のドメインポリシー**を選択します。または、任意のツールを使用して、環境に適したポリシーオブジェクトを作成および選択できます。このポリシーは、影響を受けるCitrixソフトウェア（VDA、StoreFrontサーバー、管理ツール）を実行しているすべてのマシンに適用する必要があります。



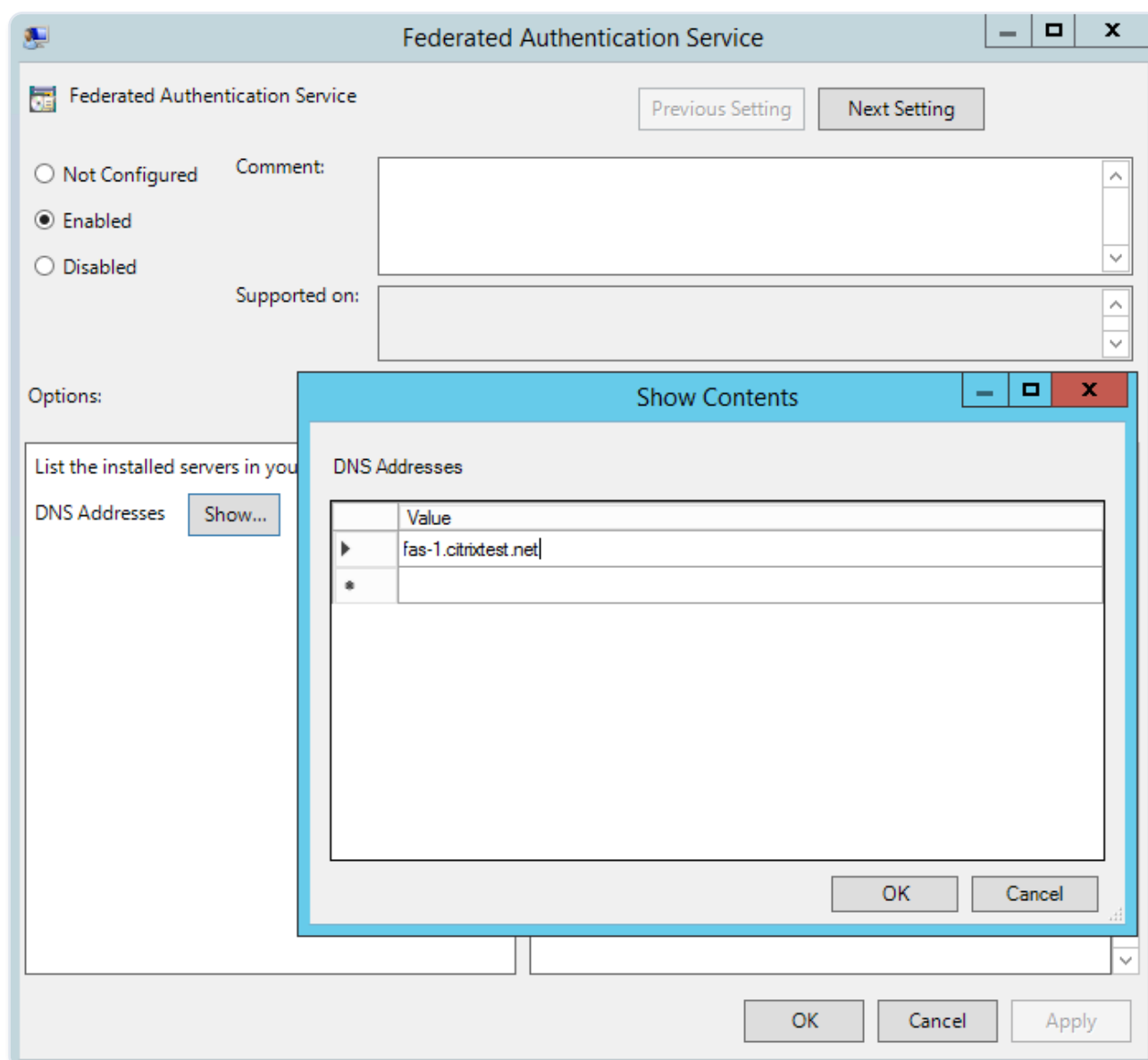
手順4. Computer Configuration/Policies/Administrative Templates/Citrix Components/Authenticationにある フェデレーション認証サービスポリシーに移動します。



**注：**

CitrixBase.admx/CitrixBase.admlテンプレートファイルをPolicyDefinitionsフォルダーに追加すると、フェデレーション認証サービスポリシー設定はドメインGPOでのみ使用可能になります。その後、フェデレーション認証サービスポリシー設定は、管理用テンプレート > Citrix コンポーネント > 認証フォルダーに表示されます。

**手順5.** フェデレーション認証サービスポリシーを開き、**有効**を選択します。これにより、**表示**ボタンを選択して、FASサーバーのDNSアドレスを構成できます。



**手順6.** FASをホストするサーバーの完全修飾ドメイン名（FQDN）を入力します。

**注意：** 複数のFQDNを入力する場合、リストの順序はStoreFrontサーバーとVDAの間で一貫している必要があります。これには、空白または未使用のリストエントリが含まれます。

**手順7. OK**をクリックしてグループポリシーウィザードを終了し、グループポリシーの変更を適用します。変更を有効にするには、マシンを再起動するか（またはコマンドラインから**gpupdate /force**を実行する）、必要がある場合があります。

## セッション内証明書のサポートとロック時の切断

**In-session Certificates**

Previous Setting   Next Setting

☐ Not Configured   Comment:   
☒ Enabled   
☐ Disabled

Supported on:

Options:

Prompt Scope: **Per-process**

Consent timeout (seconds): **30**

☒ Disconnect on lock

Help:

Certificates and private keys securely managed by the Federated Authentication Service can be made available to programs running in users' sessions. If this policy is disabled, this feature will be unavailable.

If this policy is enabled, the Prompt Scope setting will control how users are prompted for consent. There are three options:

- No consent required -- This option disables the security prompt and private keys are used silently.
- Per-process consent -- Each running program will individually prompt for consent.
- Per-session consent -- Once the user has clicked ok, this will apply to all programs in the session

If this policy is enabled, the Consent Timeout will control how long (in seconds) the consent lasts. So for example, if set to 300 seconds the user will see a prompt every five minutes. A value of zero will prompt the user for every private key operation.

If this policy is enabled, it is also possible to automatically disconnect a user's session rather than display the logon prompt. This functionality provides similar behaviour to the "disconnect on smart card removal" policy, and is useful for situations where users do not have Active Directory logon credentials.

OK   Cancel   Apply

## セッション内証明書のサポート

デフォルトでは、VDAはログオン後に証明書へのアクセスを許可しません。必要に応じて、グループポリシーテンプレートを使用して、セッション内証明書用にシステムを構成できます。これにより、ログオン後にユーザーの個人証明書ストアに証明書が配置され、アプリケーションで使用できるようになります。たとえば、VDAセッション内でWebサーバーへのTLS認証が必要な場合、その証明書はInternet Explorerで使用できます。

## ロック時の切断

このポリシーが有効になっている場合、ユーザーが画面をロックすると、ユーザーのセッションは自動的に切断されます。この機能は、「スマートカード取り外し時の切断」ポリシーと同様の動作を提供し、ユーザーがActive Directoryログオン資格情報を持っていない状態で役立ちます。

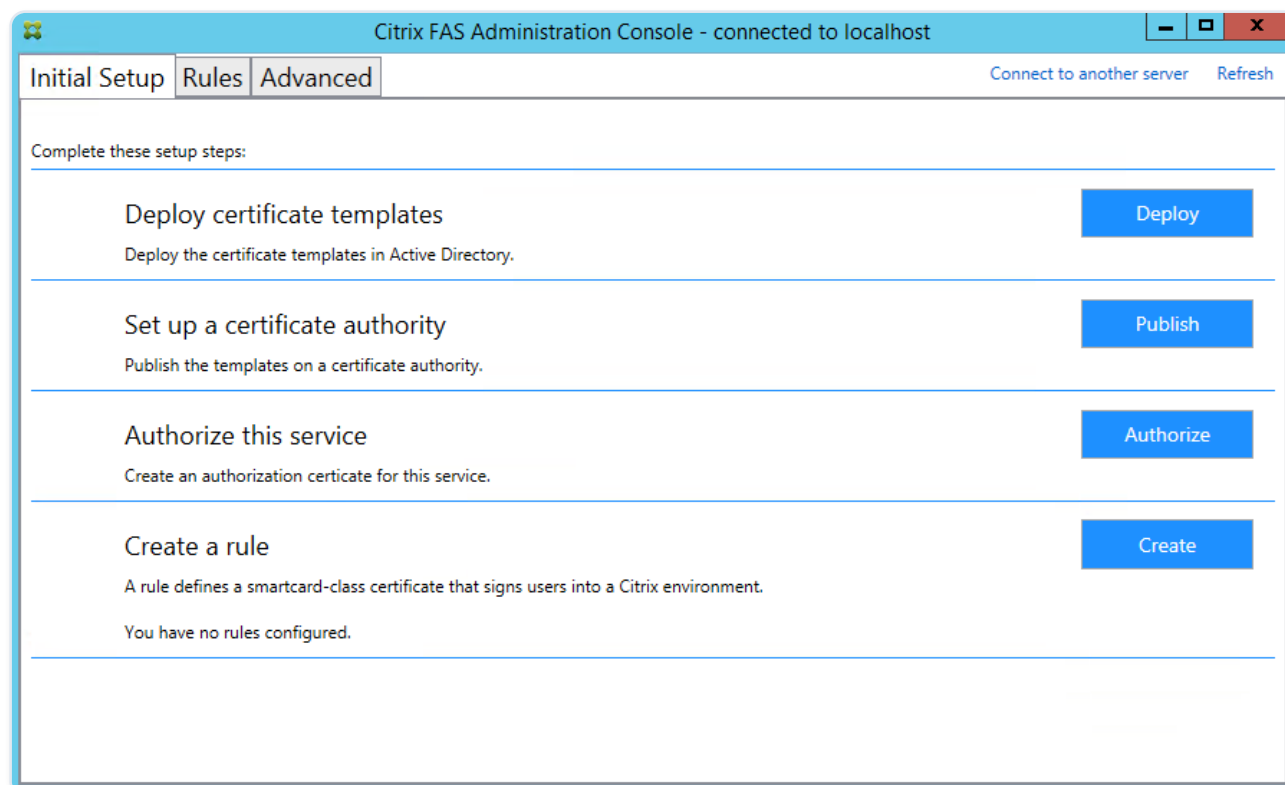
### 注：

ロック時の切断ポリシーは、VDA上のすべてのセッションに適用されます。

## Federated Authentication Service管理コンソールの使用

FAS管理コンソールはFASの一部としてインストールされます。アイコン（Citrix Federated Authentication Service）はスタートメニューに配置されます。

管理コンソールを初めて使用する際は、証明書テンプレートの展開、証明機関の設定、およびFASが証明機関を使用するための承認を行うプロセスをガイドします。一部の手順は、OS構成ツールを使用して手動で完了することもできます。

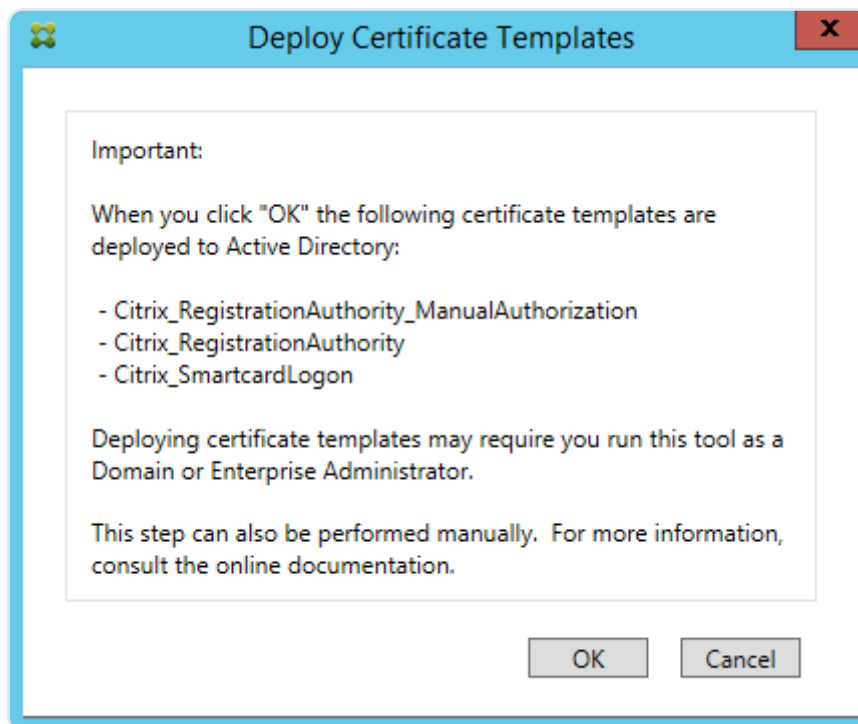


## 証明書テンプレートを展開する

他のソフトウェアとの相互運用性の問題を避けるため、FASは独自の用途のために3つのCitrix証明書テンプレートを提供します。

- Citrix\_RegistrationAuthority\_ManualAuthorization
- Citrix\_RegistrationAuthority
- Citrix\_SmartcardLogon

これらのテンプレートはActive Directoryに登録する必要があります。コンソールがそれらを見つけられない場合、**証明書テンプレートの展開ツール**でインストールできます。このツールは、Enterpriseフォレストを管理する権限を持つアカウントとして実行する必要があります。



テンプレートの設定は、FASとともにインストールされる拡張子.certificatetemplateのXMLファイルにあります。場所は次のとおりです。

C:\Program Files\Citrix\Federated Authentication Service\CertificateTemplates

これらのテンプレートファイルをインストールする権限がない場合は、Active Directory管理者に渡してください。

テンプレートを手動でインストールするには、次のPowerShellコマンドを使用します。

```
$template =
[System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemplate")

$CertEnrol = New-Object -ComObject
X509Enrollment.CX509EnrollmentPolicyWebService

$CertEnrol.InitializeImport($template)
```

```
$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)

$writabletemplate = New-Object -ComObject
X509Enrollment.CX509CertificateTemplateADWritable

$writabletemplate.Initialize($comtemplate)

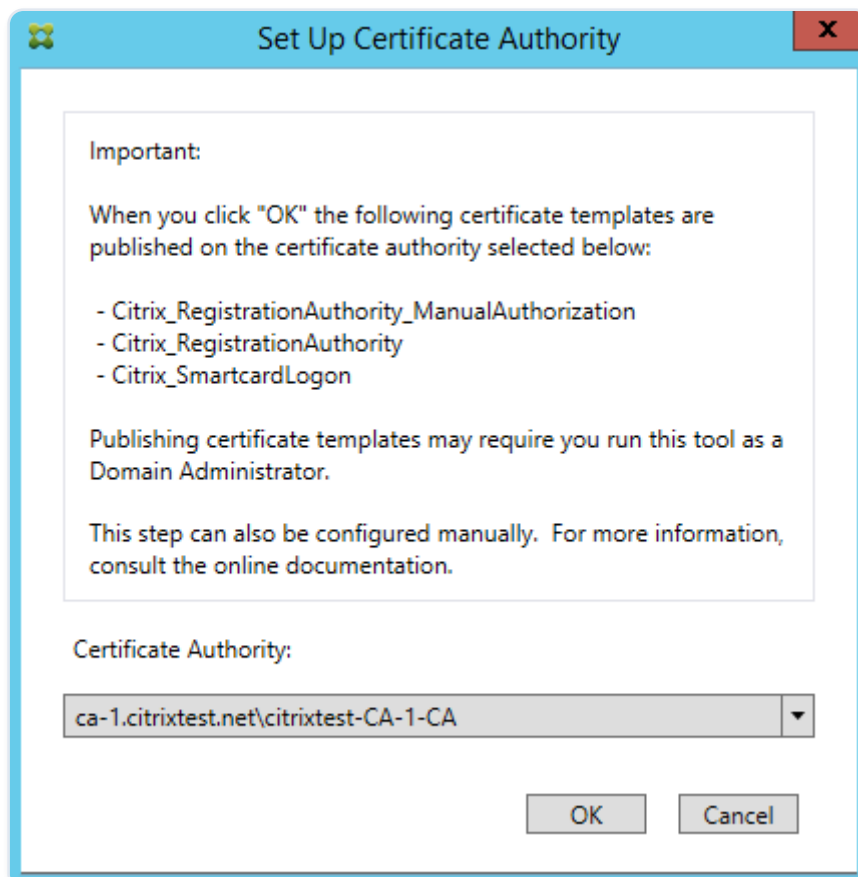
$writabletemplate.Commit(1, $NULL)
```

## Active Directory証明書サービスをセットアップする

Citrix証明書テンプレートをインストールした後、1つ以上のMicrosoft証明機関サーバーで公開する必要があります。Active Directory証明書サービスの展開方法については、Microsoftのドキュメントを参照してください。

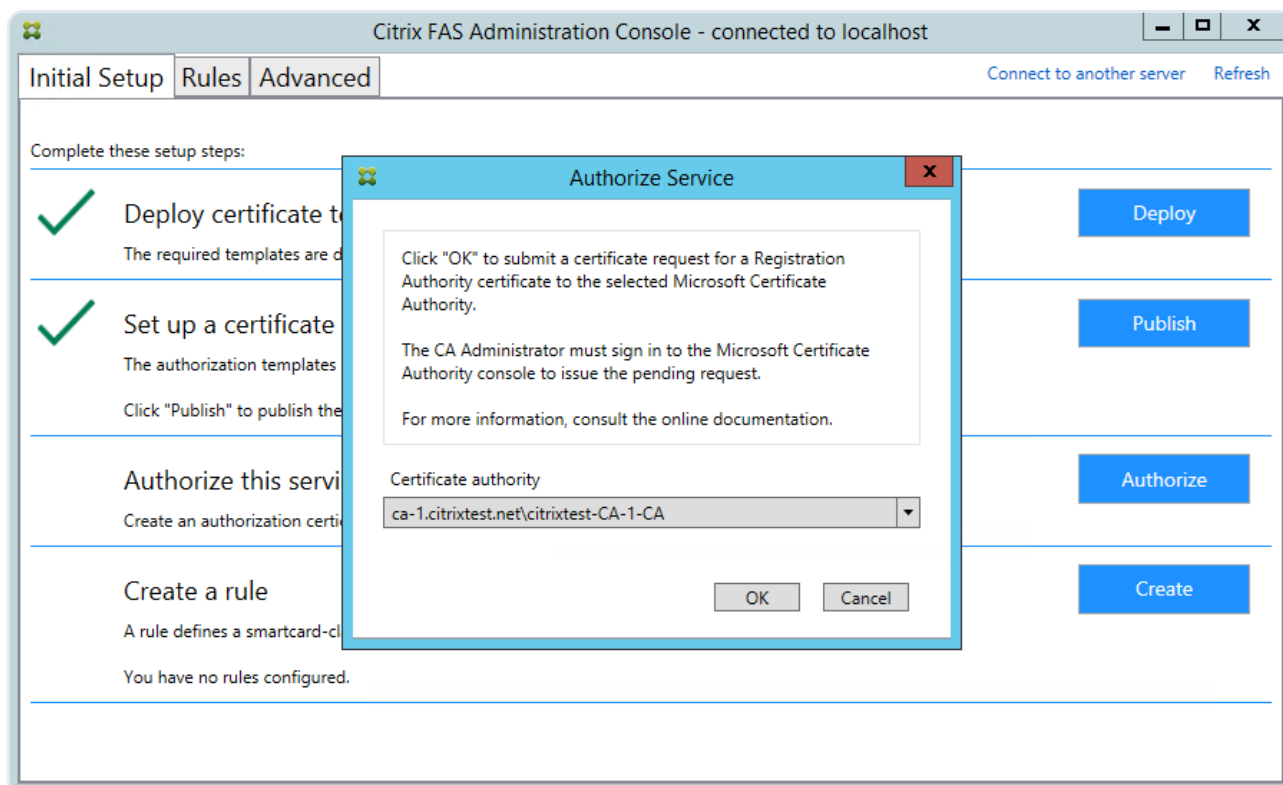
テンプレートが少なくとも1つのサーバーで公開されていない場合、**証明機関のセットアップツール**はそれらを公開することを提案します。このツールは、証明機関を管理する権限を持つユーザーとして実行する必要があります。

(証明書テンプレートは、Microsoft証明機関コンソールを使用して公開することもできます。)

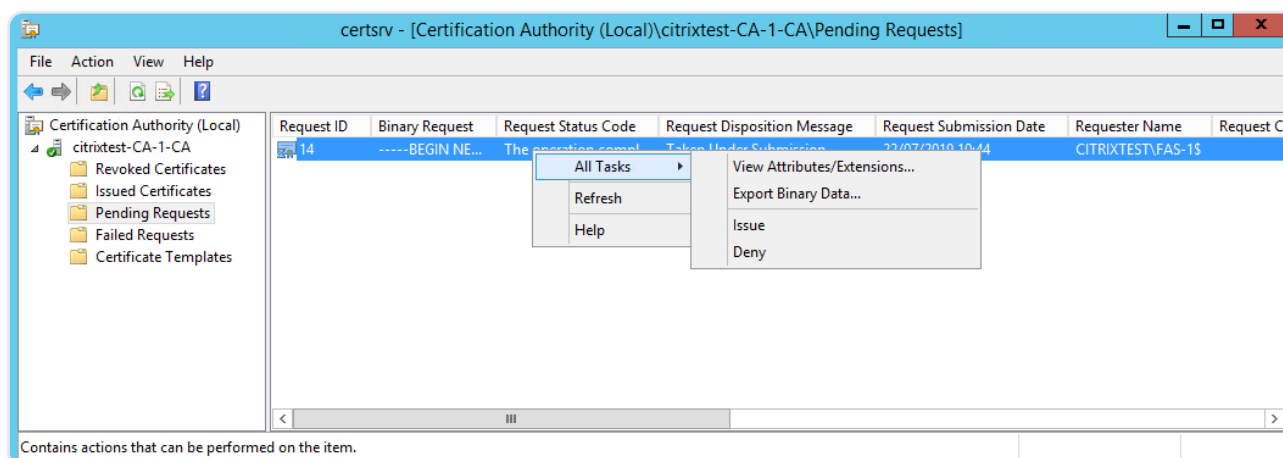


## フェデレーション認証サービスを承認する

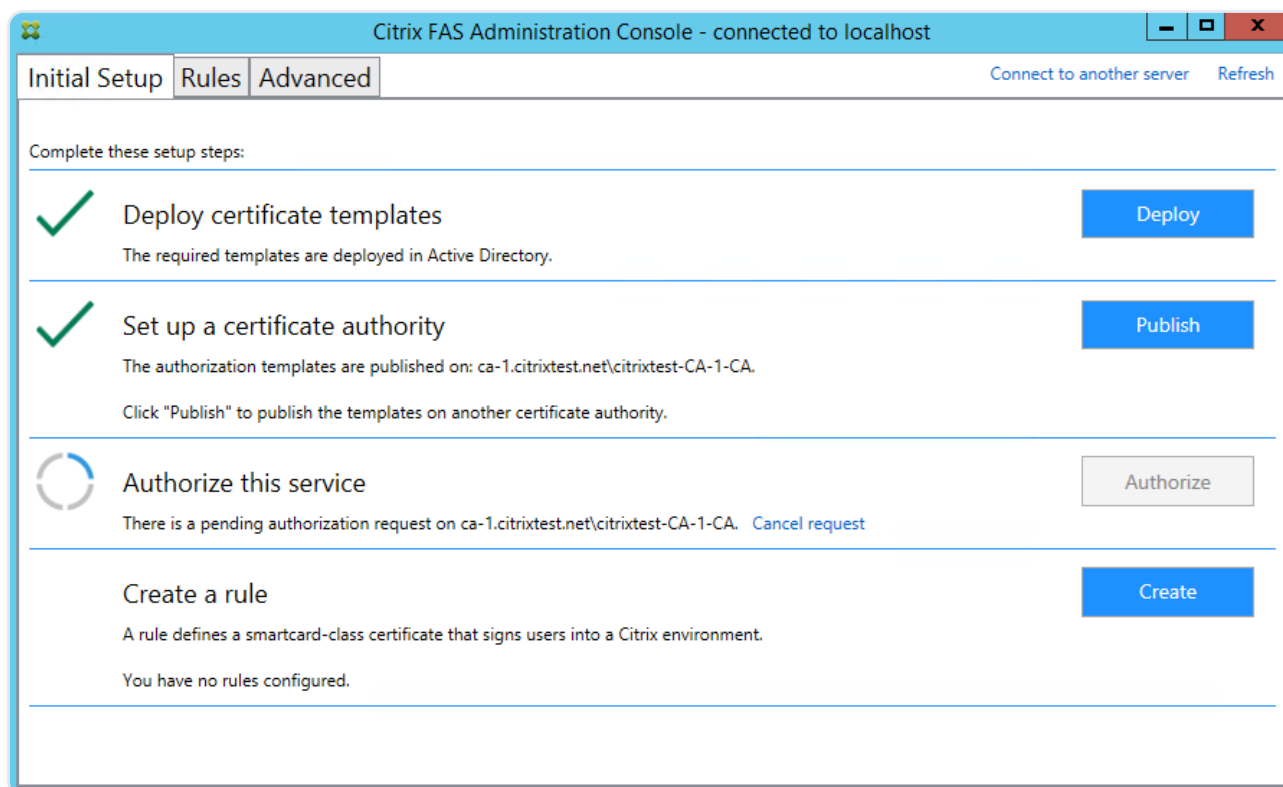
この手順により、FASの承認が開始されます。管理コンソールは、Citrix\_RegistrationAuthority\_ManualAuthorizationテンプレートを使用して証明書要求を生成し、そのテンプレートを公開している証明機関のいずれかに送信します。



要求が送信されると、Microsoft証明機関コンソールの**保留中の要求**リストに表示されます。FASの構成を続行する前に、証明機関管理者は要求を**発行**するか**拒否**するかを選択する必要があります。承認要求は、FASマシンアカウントからの**保留中の要求**として表示されることに注意してください。



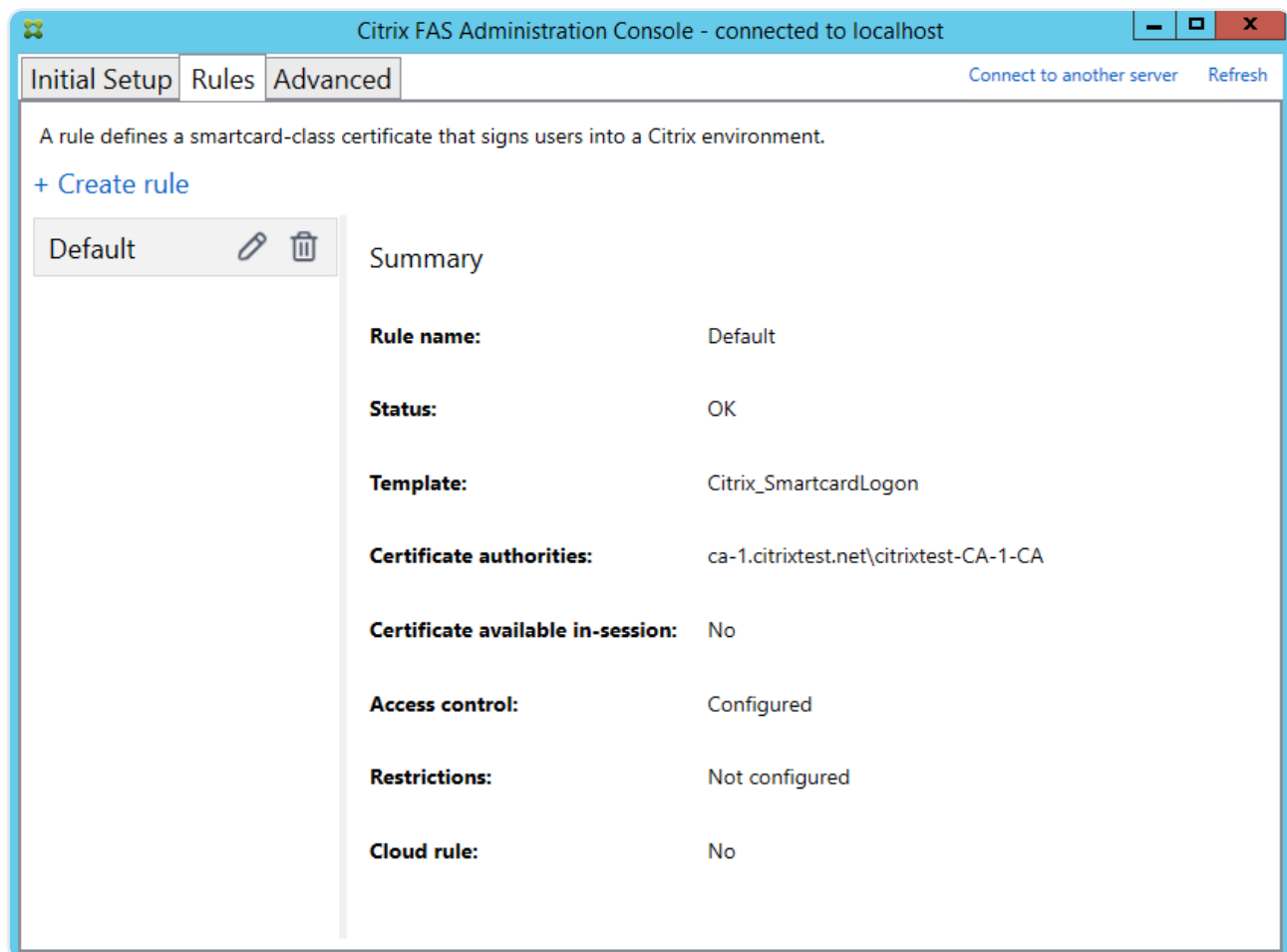
**すべてのタスク**を右クリックし、証明書要求に対して**発行**または**拒否**を選択します。FAS管理コンソールは、このプロセスが完了したことを自動的に検出します。これには数分かかる場合があります。



## ユーザー規則の構成

ユーザー規則は、StoreFrontの指示に従って、VDAログオンおよびセッション内使用のための証明書の発行を承認します。各規則は、証明書を要求することが信頼されているStoreFrontサーバー、証明書を要求できるユーザーのセット、および証明書を使用することが許可されているVDAマシンのセットを指定します。

FASのセットアップを完了するには、デフォルトの規則を定義する必要があります。規則を作成するには**作成**をクリックするか、「規則」タブに切り替えて**規則の作成**をクリックします。ウィザードは、規則を定義するために必要な情報を収集します。



ウィザードによって以下の情報が収集されます:

**テンプレート:** ユーザー証明書の発行に使用される証明書テンプレート。これは Citrix\_SmartcardLogonテンプレート、またはその変更されたコピーである必要があります。

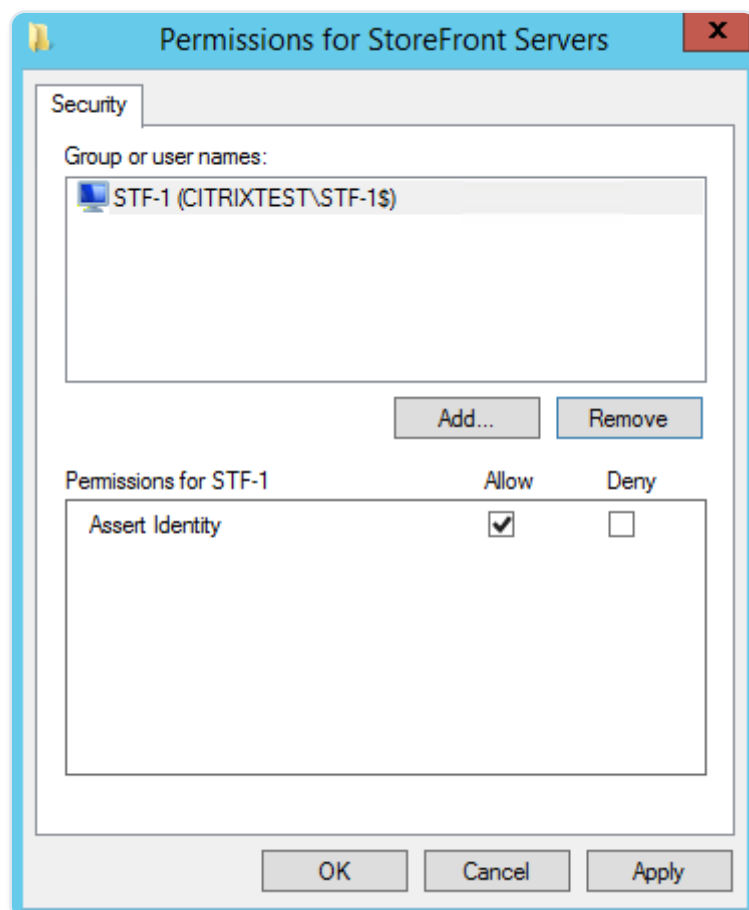
**証明機関:** ユーザー証明書を発行する証明機関。テンプレートは証明機関によって公開されている必要があります。FASは、フェールオーバーと負荷分散のために複数の証明機関の追加をサポートしています。

**セッション内使用:** セッション内使用を許可オプションは、VDAへのログオン後に証明書を使用できるかどうかを制御します。認証後にユーザーが証明書にアクセスできるようにしたい場合にのみ、このオプションを選択してください。このオプションが選択されていない場合、証明書はログオンまたは再接続にのみ使用され、認証後にユーザーは証明書にアクセスできません。

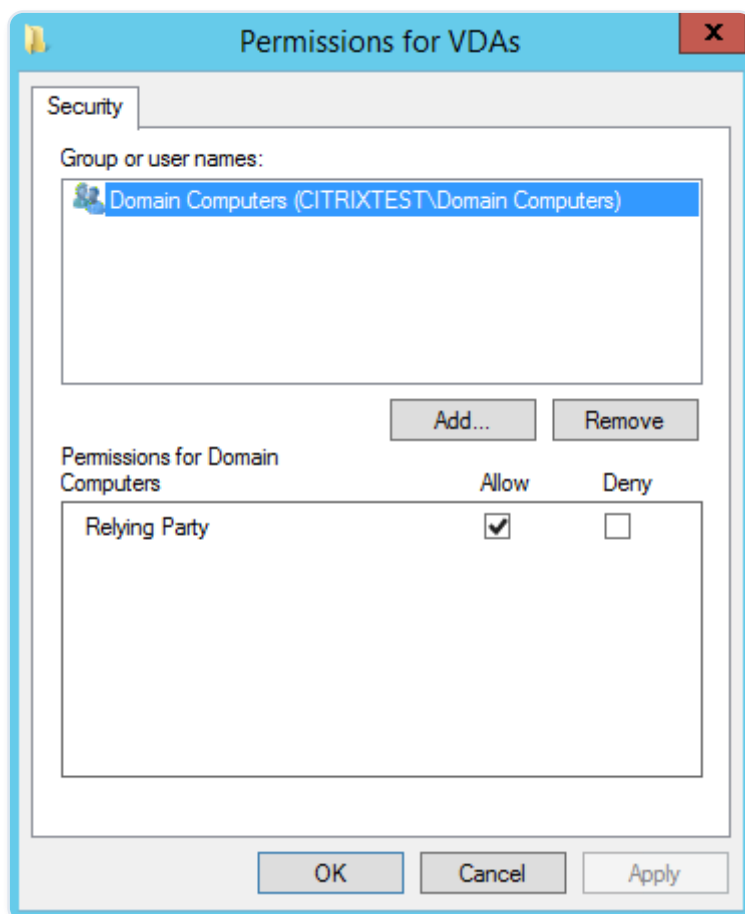
**アクセスコントロール:** ユーザーのログオンまたは再接続のために証明書を要求することを承認された、信頼できるStoreFrontサーバーマシンのリスト。

#### 重要:

アクセスコントロール設定はセキュリティ上重要であり、慎重に管理する必要があります。



**制限:** FASを使用してユーザーをログオンできるVDAマシンのリストと、FASを通じて証明書を発行できるユーザーのリスト。VDAのリストはデフォルトでDomain Computers、ユーザーのリストはデフォルトでDomain Usersですが、デフォルトが不適切な場合は変更できます。



ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/allowed-users.png)

クラウド規則: 現在サポートされていません。

## 高度な使用法

異なるプロパティと権限を持つように構成できる、異なる証明書テンプレートと認証局を参照するための追加の規則を作成できます。これらの規則は、異なるStoreFrontサーバーで使用するよう構成でき、それらのサーバーは新しい規則を名前で要求するように構成する必要があります。デフォルトでは、StoreFrontはFASに接続する際に**default**を要求します。これは、グループポリシー構成オプションを使用して変更できます。

新しい証明書テンプレートを作成するには、Microsoft証明機関コンソールでCitrix\_SmartcardLogonテンプレートを複製し、名前を変更（例：Citrix\_SmartcardLogon2）して、必要に応じて変更します。**追加**をクリックして、新しい証明書テンプレートを参照する新しいユーザー規則を作成します。

## アップグレードに関する考慮事項

- インプレースアップグレードを実行すると、すべてのFASサーバー設定が保持されます。

- フル製品のVirtual Apps and Desktopsインストーラーを実行してFASをアップグレードします。
- FASをアップグレードする前に、ControllerとVDA（およびその他のコアコンポーネント）を必要なバージョンにアップグレードしてください。
- FASをアップグレードする前に、FAS管理コンソールが閉じていることを確認してください。
- 常に少なくとも1つのFASサーバーが利用可能であることを確認してください。Federation Authentication Serviceが有効なStoreFrontサーバーからサーバーに到達できない場合、ユーザーはログオンしたりアプリケーションを起動したりできません。

## セキュリティに関する考慮事項

FASは、ドメインユーザーに代わって自律的に証明書を発行できる登録機関証明書を持っています。そのため、FASサーバーを保護し、その権限を制限するためのセキュリティポリシーを策定および実装することが重要です。

### 委任された登録エージェント

FASは、登録エージェントとして機能することでユーザー証明書を発行します。Microsoft証明機関は、FASサーバーが使用できるテンプレートを制御し、FASサーバーが証明書を発行できるユーザーを制限できます。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/delegated-enrollment-agents.png)

Citrixは、FASが意図したユーザーにのみ証明書を発行できるように、これらのオプションを設定することを強く推奨します。たとえば、FASが管理者グループまたは保護されたユーザーグループのユーザーに証明書を発行するのを防ぐことは、良い習慣です。

### アクセス制御リストの構成

**ユーザー規則の構成**セクションで説明されているように、証明書が発行される際に、FASにユーザーIDをアサートすることを信頼されているStoreFrontサーバーのリストを構成する必要があります。同様に、どのユーザーに証明書が発行されるか、およびどのVDAマシンに認証できるかを制限できます。これは、構成する標準のActive Directoryまたは証明機関のセキュリティ機能に加えて行われます。

### ファイアウォール設定

FASサーバーへのすべての通信は、ポート80経由で相互認証されたWindows Communication Foundation (WCF) Kerberosネットワーク接続を使用します。

## イベントログの監視

FASとVDAは、Windowsイベントログに情報を書き込みます。これは、監視および監査情報として使用できます。[イベントログ](#)セクションには、生成される可能性のあるイベントログエントリがリストされています。

## ハードウェアセキュリティモジュール

FASによって発行されたユーザー証明書の秘密鍵を含むすべての秘密鍵は、ネットワークサービスアカウントによってエクスポート不可能な秘密鍵として保存されます。セキュリティポリシーで必要とされる場合、FASは暗号化ハードウェアセキュリティモジュールの使用をサポートします。

低レベルの暗号化構成は、FederatedAuthenticationService.exe.configファイルで利用できます。これらの設定は、秘密鍵が最初に作成されるときに適用されます。したがって、登録機関の秘密鍵（たとえば、4096ビット、TPM保護）とランタイムユーザー証明書には、異なる設定を使用できます。

| パラメーター            | 説明                                                                                                                                      |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| ProviderLegacyCsp | trueに設定すると、FASはMicrosoft CryptoAPI (CAPI)を使用します。それ以外の場合、FASはMicrosoft Cryptography Next Generation API (CNG)を使用します。                     |
| ProviderName      | 使用するCAPIまたはCNGプロバイダーの名前。                                                                                                                |
| ProviderType      | Microsoft KeyContainerPermissionAccessEntry.ProviderType プロパティ PROV_RSA_AES 24 を参照します。CAPIでHSMを使用しており、HSMベンダーが別途指定しない限り、常に24である必要があります。 |
| KeyProtection     | 秘密キーの「エクスポート可能」フラグを制御します。また、ハードウェアでサポートされている場合、Trusted Platform Module (TPM) キー ストレージの使用も許可します。                                         |
| KeyLength         | RSA秘密キーのキー長。サポートされている値は1024、2048、4096です (デフォルト: 2048)。                                                                                  |

## PowerShell SDK

FAS管理コンソールはシンプルな展開に適していますが、PowerShellインターフェイスはより高度なオプションを提供します。コンソールで利用できないオプションを使用する場合、Citrixは構成にPowerShellのみを使用することを推奨します。

次のコマンドはPowerShellコマンドレットを追加します。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

コマンドレットのヘルプを表示するには、**Get-Help** <cmdlet name> を使用します。次の表に、\*が標準のPowerShell動詞 (New、Get、Set、Removeなど) を表すいくつかのコマンドを示します。

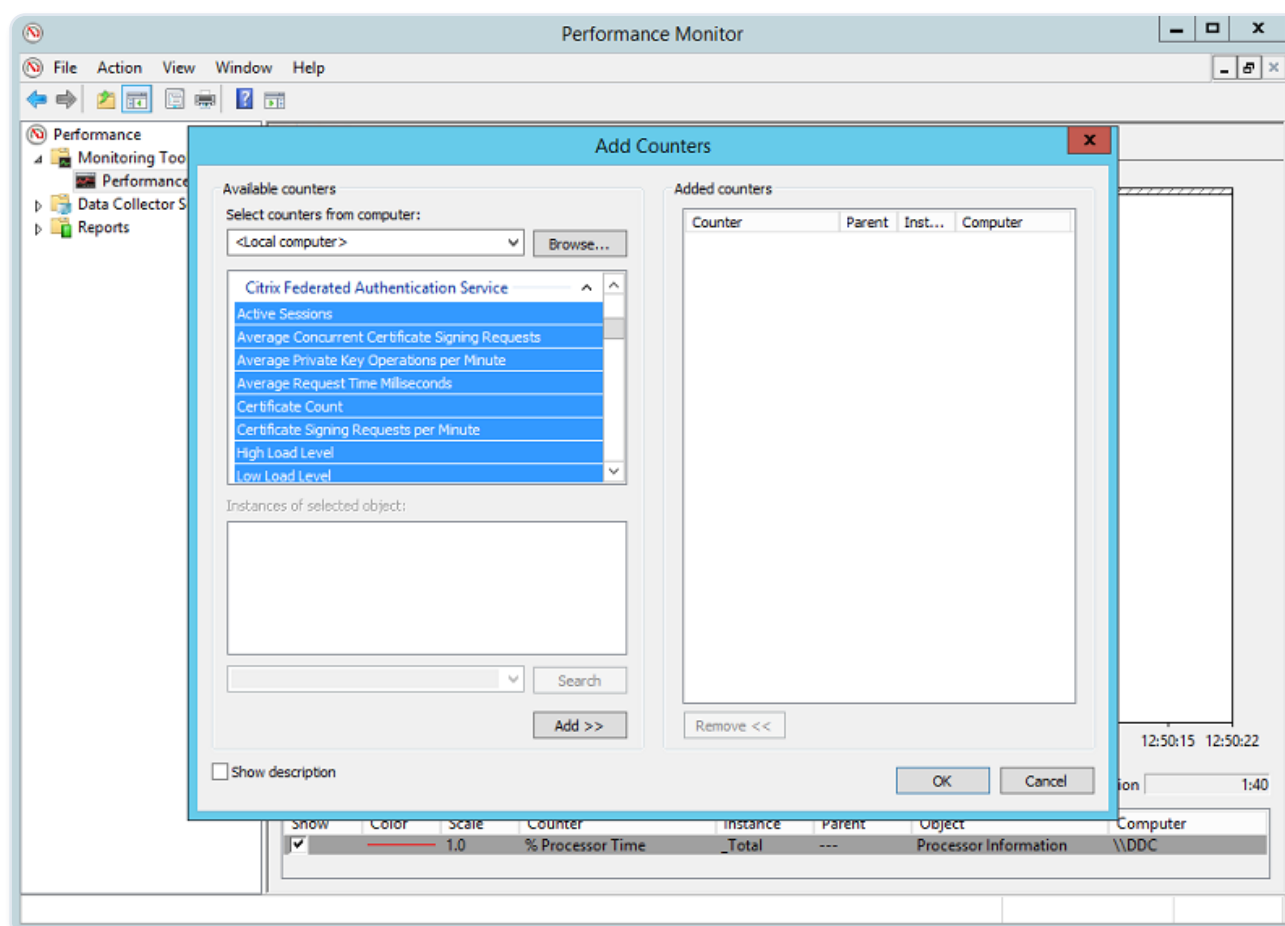
| コマンド                          | 概要                              |
|-------------------------------|---------------------------------|
| *-FasServer                   | 現在の環境にあるFASサーバーを一覧表示し、再構成します。   |
| *-FasAuthorizationCertificate | 登録機関証明書を管理します。                  |
| *-FasCertificateDefinition    | FASが証明書の生成に使用するパラメーターを制御します。    |
| *-FasRule                     | FASで構成されたユーザー規則を管理します。          |
| *-FasUserCertificate          | FASによってキャッシュされた証明書を一覧表示し、管理します。 |

FASサーバーのアドレスを指定することで、PowerShellコマンドレットをリモートで使用できます。

FAS PowerShellコマンドレットの詳細については、[PowerShellコマンドレット](#)を参照してください。

## パフォーマンスカウンター

FASには、負荷追跡目的のパフォーマンスカウンターのセットが含まれています。



次の表に、利用可能なカウンターを示します。ほとんどのカウンターは、5分間の移動平均です。

| 名前         | 説明                                                                    |
|------------|-----------------------------------------------------------------------|
| アクティブセッション | FASによって追跡される接続の数。                                                     |
| 同時CSR      | 同時に処理される証明書要求の数。                                                      |
| 秘密鍵操作      | 1分あたりに実行される秘密鍵操作の数。                                                   |
| 要求時間       | 証明書を生成および署名するのにかかる時間。                                                 |
| 証明書数       | FASにキャッシュされている証明書の数。                                                  |
| 1分あたりのCSR  | 1分あたりに処理される証明書署名要求の数。                                                 |
| 低/中/高      | FASが「1分あたりのCSR数」で受け入れ可能な負荷の推定値。「高負荷」のしきい値を超えると、セッションの起動が失敗する可能性があります。 |

# イベントログ

次の表は、FASによって生成されるイベントログエントリを示しています。

## 管理イベント

これらのイベントは、FASサーバーでの構成変更に応じてログに記録されます。

| ログコード                                                                                                     |
|-----------------------------------------------------------------------------------------------------------|
| [S001] アクセス拒否: ユーザー [{0}] はAdministratorsグループのメンバーではありません                                                 |
| [S002] アクセス拒否: ユーザー [{0}] は役割 [{1}] の管理者ではありません                                                           |
| [S003] 管理者 [{0}] がメンテナンスモードを [{1}] に設定しています                                                               |
| [S004] 管理者 [{0}] がCA [{1}] テンプレート [{2}] and [{3}] に登録しています                                                |
| [S005] 管理者 [{0}] がCA [{1}] の承認を取り消しています                                                                   |
| [S006] 管理者 [{0}] が新しい証明書定義 [{1}] を作成しています                                                                 |
| [S007] 管理者 [{0}] が証明書定義 [{1}] を更新しています                                                                    |
| [S008] 管理者 [{0}] が証明書定義 [{1}] を削除しています                                                                    |
| [S009] 管理者 [{0}] が新しい役割を作成中 [{1}]                                                                         |
| [S010] 管理者 [{0}] が役割を更新中 [{1}]                                                                            |
| [S011] 管理者 [{0}] が役割を削除中 [{1}]                                                                            |
| [S012] 管理者 [{0}] が証明書を作成中 [upn: {1} sid: {2} role: {3} Certificate Definition: {4} Security Context: {5}] |
| [S013] 管理者 [{0}] が証明書を削除中 [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}]          |
| [S015] 管理者 [{0}] が証明書要求を作成中 [TPM: {1}]                                                                    |
| [S016] 管理者 [{0}] が承認証明書をインポート中 [Reference: {1}]                                                           |

| ログコード                                                                                                            |
|------------------------------------------------------------------------------------------------------------------|
| [S401] 構成のアップグレードを実行中 -- [From version {0} to version {1}]                                                       |
| [S402] エラー: Citrix Federated Authentication Service は Network Service として実行する必要があります [currently running as: {0}] |
| [S404] Citrix Federated Authentication Service データベースを強制的に消去中                                                    |
| [S405] レジストリからデータベースへのデータ移行中にエラーが発生しました: [{0}]                                                                   |
| [S406] レジストリからデータベースへのデータ移行が完了しました (注: ユーザー証明書は移行されません)                                                          |
| [S407] データベースが既に存在するため、レジストリベースのデータはデータベースに移行されませんでした                                                            |
| [S408] 構成をダウングレードできません -- [From version {0} to version {1}]                                                      |
| [S409] ThreadPool MinThreads は [workers: {0} completion: {1}] から [workers: {2} completion: {3}] に調整されました         |
| [S410] ThreadPool MinThreads を [workers: {0} completion: {1}] から [workers: {2} completion: {3}] に調整できませんでした      |

## IDアサーションの作成

これらのイベントは、信頼されたサーバーがユーザーログオンをアサートしたときに、FASサーバーで実行時にログに記録されます。

| ログコード                                                                      |
|----------------------------------------------------------------------------|
| [S101] サーバー [{0}] は、ロール [{1}] でIDをアサートする権限がありません                           |
| [S102] サーバー [{0}] は UPN [{1}] をアサートできませんでした (例外: {2}{3})                   |
| [S103] サーバー [{0}] は UPN [{1}] SID {2} を要求しましたが、ルックアップは SID {3} を返しました      |
| [S104] サーバー [{0}] は UPN [{1}] をアサートできませんでした (UPN はロール [{2}] によって許可されていません) |

| ログコード                                                                                       |
|---------------------------------------------------------------------------------------------|
| [S105] サーバー [{0}] はIDアサーションを発行しました [upn: {1}, role {2}, セキュリティコンテキスト: [{3}]]                |
| [S120] [upn: {0} role: {1} セキュリティコンテキスト: [{2}]] に証明書を発行しています                                |
| [S121] [certificate authority: {2}] によって [upn: {0} role: {1}] に証明書が発行されました                  |
| [S122] 警告: サーバーが過負荷です [upn: {0} role: {1}][1分あたりのリクエスト数 {2}]。                               |
| [S123] [upn: {0} role: {1}] [exception: {2}] の証明書を発行できませんでした                                |
| [S124] [upn: {0} role: {1}] の証明書を [certificate authority: {2}] [exception: {3}] で発行できませんでした |

## 証明書利用側としての動作

これらのイベントは、VDAがユーザーをログオンさせるときに、FASサーバーで実行時にログに記録されます。

| ログコード                                                                                              |
|----------------------------------------------------------------------------------------------------|
| [S201] 証明書利用側 [{0}] はパスワードにアクセスできません。                                                              |
| [S202] 証明書利用側 [{0}] は証明書にアクセスできません。                                                                |
| [S203] 証明書利用側 [{0}] はログオンCSPにアクセスできません                                                             |
| [S204] 証明書利用側 [{0}] が、[upn: {1}] のログオンCSPに、役割: [{2}] [Operation: {3}] として、[{4}] によって承認されてアクセスしています |
| [S205] 呼び出し元アカウント [{0}] は、役割 [{1}] の証明書利用側ではありません                                                  |
| [S206] 呼び出し元アカウント [{0}] は証明書利用側ではありません                                                             |
| [S208] 秘密キー操作が失敗しました [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}]。  |

## セッション内証明書サーバー

これらのイベントは、ユーザーがセッション内証明書を使用するときにFASサーバーにログ記録されます。

| ログコード                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------|
| [S301] アクセス拒否: ユーザー [{0}] は仮想スマートカードへのアクセス権がありません。                                                                       |
| [S302] ユーザー [{0}] が不明な仮想スマートカード [thumbprint: {1}] を要求しました。                                                               |
| [S303] アクセス拒否: ユーザー [{0}] は仮想スマートカード [upn: {1}] と一致しません。                                                                 |
| [S304] ユーザー [{0}] がコンピューター [{2}] でプログラム [{1}] を実行し、秘密鍵操作 [{6}] に仮想スマートカード [upn: {3} role: {4} thumbprint: {5}] を使用しています。 |
| [S305] 秘密鍵操作が失敗しました [Operation: {0} upn: {1} role: {2} containerName {3} Error {4} {5}]。                                 |

## FASアサーションプラグイン

これらのイベントはFASアサーションプラグインによってログに記録されます。

| ログコード                                                                                             |
|---------------------------------------------------------------------------------------------------|
| [S500] FASアサーションプラグインが構成されていません。                                                                  |
| [S501] 構成されたFASアサーションプラグインをロードできませんでした [exception:{0}]。                                           |
| [S502] FASアサーションプラグインがロードされました [pluginId={0}] [assembly={1}] [location={2}]。                      |
| [S503] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (ログオン証拠が提供されましたが、プラグイン [{2}] はそれをサポートしていません)。           |
| [S504] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (ログオン証拠が提供されましたが、構成されたFASプラグインがありません)。                  |
| [S505] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (プラグイン [{2}] はログオン証拠をステータス [{3}] とメッセージ [{4}] で拒否しました) |
| [S506] プラグイン [{0}] は、サーバー [{1}] からの UPN [{2}] のログオン証拠をメッセージ [{3}] で受け入れました                        |
| [S507] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (プラグイン [{2}] が例外 [{3}] をスローしました)                       |

| ログコード                                                                                   |
|-----------------------------------------------------------------------------------------|
| [S507] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (プラグイン [{2}] が例外 [{3}] をスローしました)             |
| [S508] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (アクセス処理が提供されましたが、プラグイン [{2}] はそれをサポートしていません) |
| [S509] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (アクセス処理が提供されましたが、構成された FAS プラグインがありません)      |
| [S510] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (アクセス処理はプラグイン [{2}] によって無効と見なされました)          |

## ログオン

これらのイベントは、ログオン段階中に VDA に記録されます。

| ログコード                                                                      |
|----------------------------------------------------------------------------|
| [S101] IDアサーションログオンに失敗しました。認識されないフェデレーション認証サービス [id: {0}]                  |
| [S102] IDアサーションログオンに失敗しました。{0} の SID を検索できませんでした [Exception: {1}{2}]       |
| [S103] IDアサーションログオンに失敗しました。ユーザー {0} の SID は {1} ですが、期待される SID は {2} です     |
| [S104] IDアサーションログオンに失敗しました。フェデレーション認証サービスへの接続に失敗しました: {0} [Error: {1} {2}] |
| [S105] IDアサーションログオン。ログイン中 [Username: {0} Domain: {1}]                      |
| [S106] IDアサーションログオン。ログイン中 [Certificate: {0}]                               |
| [S107] IDアサーションログオンに失敗しました。 [Exception: {0}{1}]                            |
| [S108] IDアサーションサブシステム。ACCESS_DENIED [Caller: {0}]                          |

## セッション内証明書

これらのイベントは、ユーザーがセッション内証明書を使用しようとしたときにVDAにログ記録されます。

| ログコード                                                                                                 |
|-------------------------------------------------------------------------------------------------------|
| [S201] 仮想スマートカードアクセスは [{0}] によって [PID: {1} Program Name: {2} Certificate thumbprint: {3}] に対して承認されました |
| [S203] 仮想スマートカードサブシステム。アクセス拒否 [caller: {0}, session {1}]                                              |
| [S204] 仮想スマートカードサブシステム。スマートカードのサポートが無効です                                                              |

## 証明書要求とキーペアの生成

これらのイベントは、FASサーバーが低レベルの暗号化操作を実行したときにログ記録されます。

| ログコード                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------|
| [S001] TrustArea::TrustArea: インストールされた証明書 [TrustArea: {0}] [Certificate {1} TrustAreaJoinParameters{2}]                                         |
| [S014] Pkcs10Request::Create: PKCS10リクエストを作成しました [Distinguished Name {0}]                                                                       |
| [S016] PrivateKey::Create [Identifier {0} MachineWide: {1} Provider: {2} ProviderType: {3} EllipticCurve: {4} KeyLength: {5} isExportable: {6}] |
| [S017] PrivateKey::Delete イベント [CspName: {0}, Identifier {1}]                                                                                   |

| ログコード                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------|
| [S104] MicrosoftCertificateAuthority::GetCredentials: {0}を使用する権限が付与されました                                          |
| [S105] MicrosoftCertificateAuthority::SubmitCertificateRequest 応答の送信エラー [{0}]                                     |
| [S106] MicrosoftCertificateAuthority::SubmitCertificateRequest 発行された証明書 [{0}]                                     |
| [S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - 承認待ち [CR_DISP_UNDER_SUBMISSION] [Reference: {0}] |

## 関連情報

- 一般的なFAS展開は、[Deployment architectures](#)にまとめられています。
- 「How-to」記事は、[Advanced configuration](#)で紹介されています。

# 展開アーキテクチャ

---

## はじめに

Federated Authentication Service (FAS) は、Citrix® コンポーネントであり、Active Directory 証明書サービスと統合することで、ユーザーがCitrix環境内でシームレスに認証されることを可能にします。このドキュメントでは、展開に適したさまざまな認証アーキテクチャについて説明します。

有効にすると、FAS はユーザー認証の決定を信頼された StoreFront サーバーに委任します。StoreFront には、最新の Web テクノロジーに基づいて構築された包括的な組み込み認証オプションがあり、StoreFront SDK またはサードパーティの IIS プラグインを使用して簡単に拡張できます。基本的な設計目標は、Web サイトにユーザーを認証できる認証テクノロジーであれば、Citrix Virtual Apps または Citrix Virtual Desktops™ 展開へのログインに使用できるようになったことです。

このドキュメントでは、複雑さが増すにつれて、トップレベルの展開アーキテクチャの例について説明します。

- [内部展開](#)
- [シトリックス ゲートウェイのデプロイ](#)
- [ADFS SAML](#)
- [B2B アカウントマッピング](#)
- [ウィンドウズ 10 アジュール AD への参加](#)

関連する FAS 記事へのリンクが提供されています。すべてのアーキテクチャについて、[インストールと構成](#) の記事が FAS の設定に関する主要なリファレンスです。

## 仕組み

FAS は、StoreFront によって認証された Active Directory ユーザーに代わって、スマートカードクラスの証明書を自動的に発行することを許可されています。これは、管理者が物理スマートカードをプロビジョニングできるツールと同様の API を使用します。

ユーザーが Citrix Virtual Apps™ または Citrix Virtual Desktops Virtual Delivery Agent (VDA) に仲介されると、証明書がマシンにアタッチされ、Windows ドメインはログオンを標準のスマートカード認証として認識します。

## 内部展開

FASを使用すると、ユーザーはさまざまな認証オプション（Kerberosシングルサインオンを含む）を使用してStoreFrontに安全に認証し、完全に認証されたCitrix HDX™セッションに接続できます。

これにより、ユーザー資格情報やスマートカードのPINを入力するプロンプトなしでWindows認証が可能になり、シングルサインオンサービスなどの「保存されたパスワード管理」機能を使用する必要がなくなります。これは、以前のバージョンのCitrix Virtual Appsで利用可能だったKerberos Constrained Delegationログオン機能を置き換えるために使用できます。

すべてのユーザーは、スマートカードを使用してエンドポイントデバイスにログオンしているかどうかにかかわらず、セッション内で公開鍵インフラストラクチャ（PKI）証明書にアクセスできます。これにより、スマートカードリーダーを持たないスマートフォンやタブレットなどのデバイスからでも、二要素認証モデルへのスムーズな移行が可能になります。

この展開では、FASを実行する新しいサーバーが追加され、ユーザーに代わってスマートカードクラスの証明書を発行する権限が与えられます。これらの証明書は、スマートカードログオンが使用されたかのように、Citrix HDX環境のユーザーセッションにログオンするために使用されます。



Citrix Virtual AppsまたはCitrix Virtual Desktops環境は、スマートカードログオンと同様の方法で構成する必要があります。これは[CTX206156](#)に記載されています。

既存の展開では、通常、ドメインに参加しているMicrosoft証明機関が利用可能であり、ドメインコントローラーにドメインコントローラー証明書が割り当てられていることを確認するだけです。（[CTX206156](#)の「ドメインコントローラー証明書の発行」セクションを参照してください。）

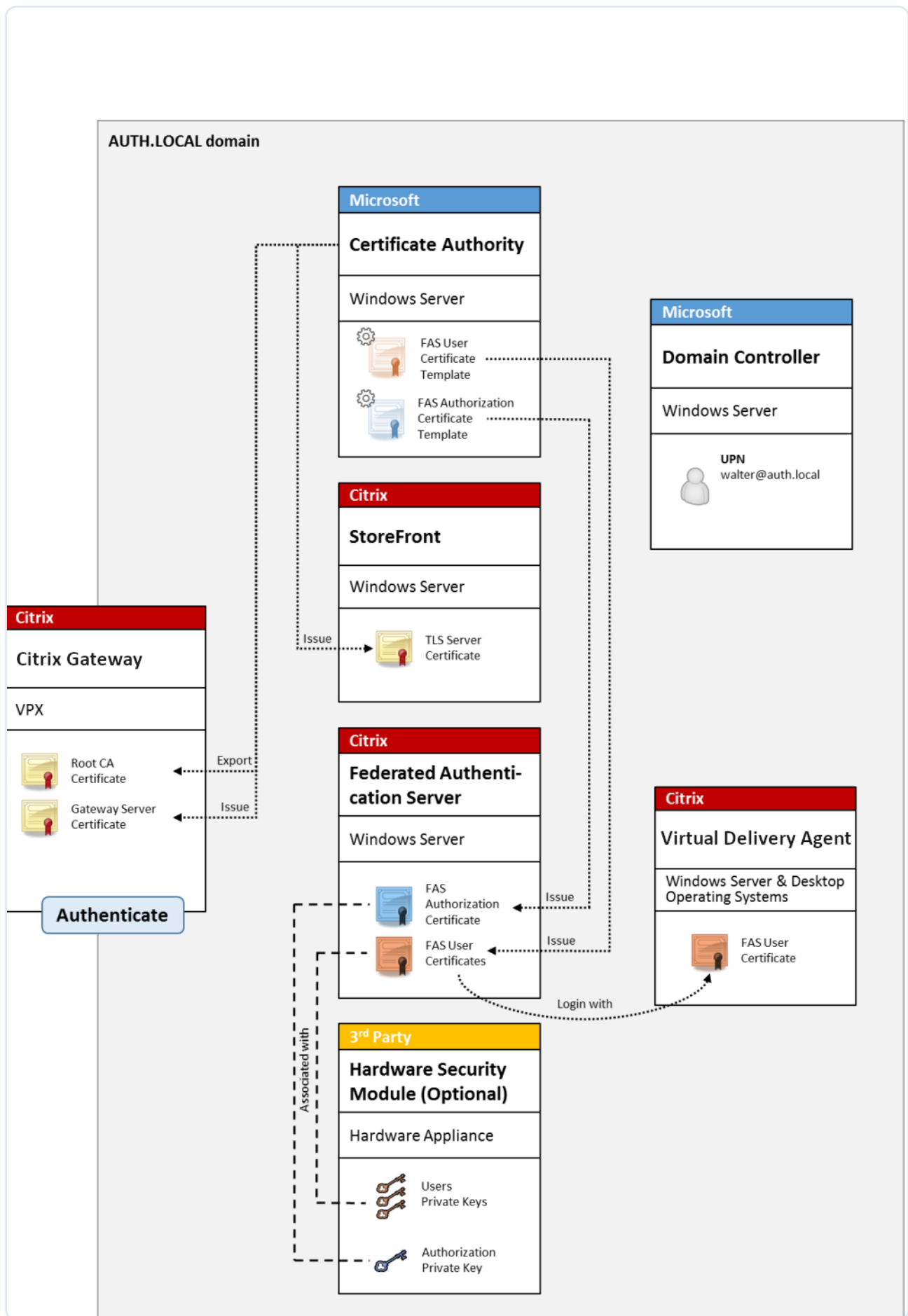
関連情報:

- キーは、ハードウェアセキュリティモジュール（HSM）または内蔵のトラステッドプラットフォームモジュール（TPM）に保存できます。詳細については、[秘密鍵の保護](#)の記事を参照してください。
- [インストールと構成](#)の記事では、FASのインストールと構成方法について説明しています。

## Citrix Gatewayの展開

Citrix Gatewayの展開は内部展開と似ていますが、StoreFrontとペアになったCitrix Gatewayが追加され、認証の主要なポイントがCitrix Gateway自体に移されます。Citrix Gatewayには、企業のWebサイトへのリモートアクセスを保護するために使用できる高度な認証および承認オプションが含まれています。

この展開は、最初にCitrix Gatewayに認証してからユーザーセッションにログインする際に発生する複数のPINプロンプトを回避するために使用できます。また、ADパスワードやスマートカードを別途必要とせずに、高度なCitrix Gateway認証テクノロジーを使用することもできます。



Citrix Virtual AppsまたはCitrix Virtual Desktops環境は、スマートカードログオンと同様の方法で構成する必要があります。これはCTX206156に記載されています。

既存の展開では、通常、ドメイン参加済みのMicrosoft証明機関が利用可能であること、およびドメインコントローラーにドメインコントローラー証明書が割り当てられていることを確認するだけです。(CTX206156の「ドメインコントローラー証明書の発行」セクションを参照してください)。

Citrix Gatewayをプライマリ認証システムとして構成する場合、Citrix GatewayとStoreFront間のすべての接続がTLSで保護されていることを確認してください。特に、コールバックURLがCitrix Gatewayサーバーを指すように正しく構成されていることを確認してください。これは、この展開でCitrix Gatewayサーバーを認証するために使用できます。

**Add NetScaler Gateway Appliance**

**StoreFront**

- ✓ General Settings
- ✓ Secure Ticket Authority
- Authentication Settings**
- Summary

**Authentication Settings**

These settings specify how the remote user provides authentication credentials

Version: 10.0 (Build 69.4) or later

VServer IP address: v10.0: SNIP or MIP, v10.1+: VIP

Logon type: Domain

Smart card fallback: None

Callback URL: https://NetScalerGatewayFQDN /CitrixAuthService/AuthService.asmx

⚠ When no Callback URL is specified, Smart Access is not available.

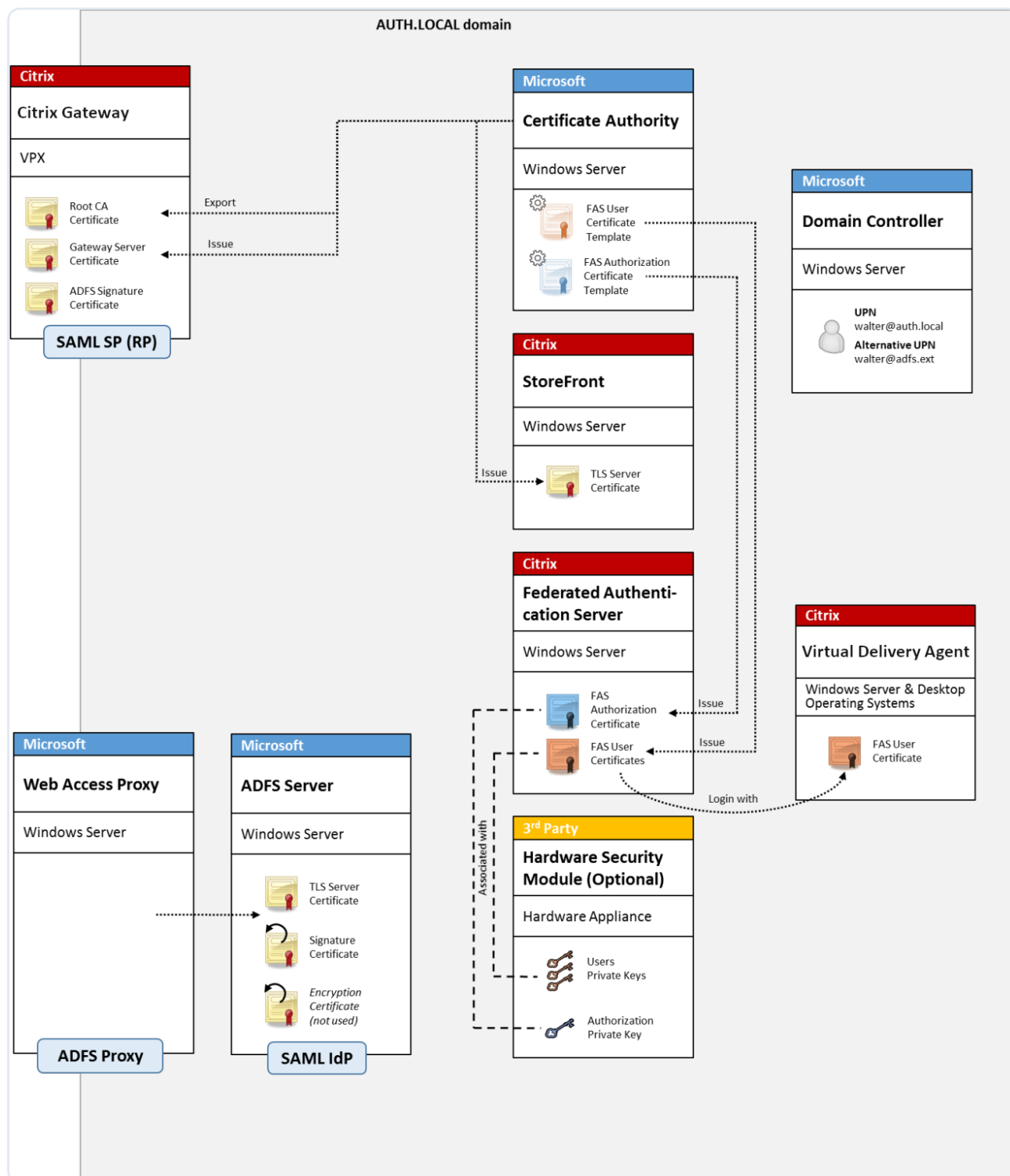
Back Create Cancel

関連情報:

- Citrix Gatewayを構成するには、「[NetScaler Gateway 10.5をStoreFront 3.6およびCitrix Virtual Desktops 7.6で使用するよう構成する方法](#)」を参照してください。
- [インストールと構成](#)では、FASのインストールと構成方法について説明しています。

# ADFS SAML展開

主要なCitrix Gateway認証テクノロジーにより、SAML IDプロバイダー (IdP) として機能できる Microsoft ADFSとの統合が可能になります。SAMLアサーションは、信頼されたIdPによって発行される暗号署名されたXMLブロックであり、ユーザーがコンピューターシステムにログオンすることを承認します。これは、FASサーバーがユーザーの認証をMicrosoft ADFSサーバー (またはその他のSAML対応IdP) に委任できることを意味します。



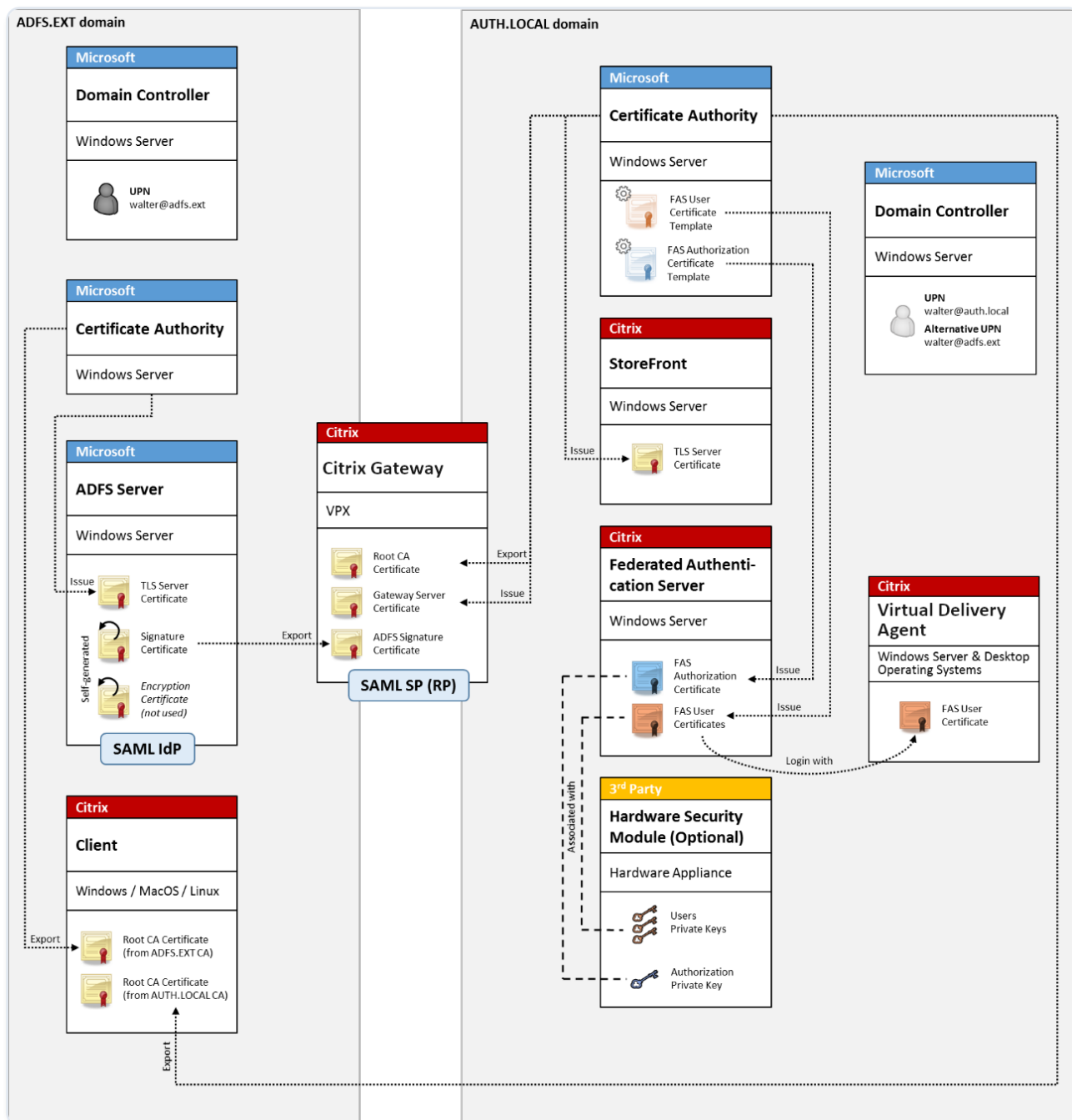
ADFSは、インターネット経由でリモートで企業リソースにユーザーを安全に認証するためによく使用されます。たとえば、Office 365との統合によく使用されます。

関連情報:

- [ADFS展開](#)の記事に詳細が記載されています。
- [インストールと構成](#)の記事では、FASのインストールと構成方法について説明しています。
- この記事の[Citrix Gateway展開](#)セクションに構成に関する考慮事項が記載されています。

## B2Bアカウントマッピング

2つの会社が互いのコンピューターシステムを使用したい場合、一般的な選択肢は、信頼関係を持つActive Directory Federation Service (ADFS) サーバーをセットアップすることです。これにより、一方の会社のユーザーは、もう一方の会社のActive Directory (AD) 環境にシームレスに認証できます。ログオン時、各ユーザーは自社のログオン資格情報を使用します。ADFSはこれをピア会社のAD環境の「シャドウアカウント」に自動的にマッピングします。



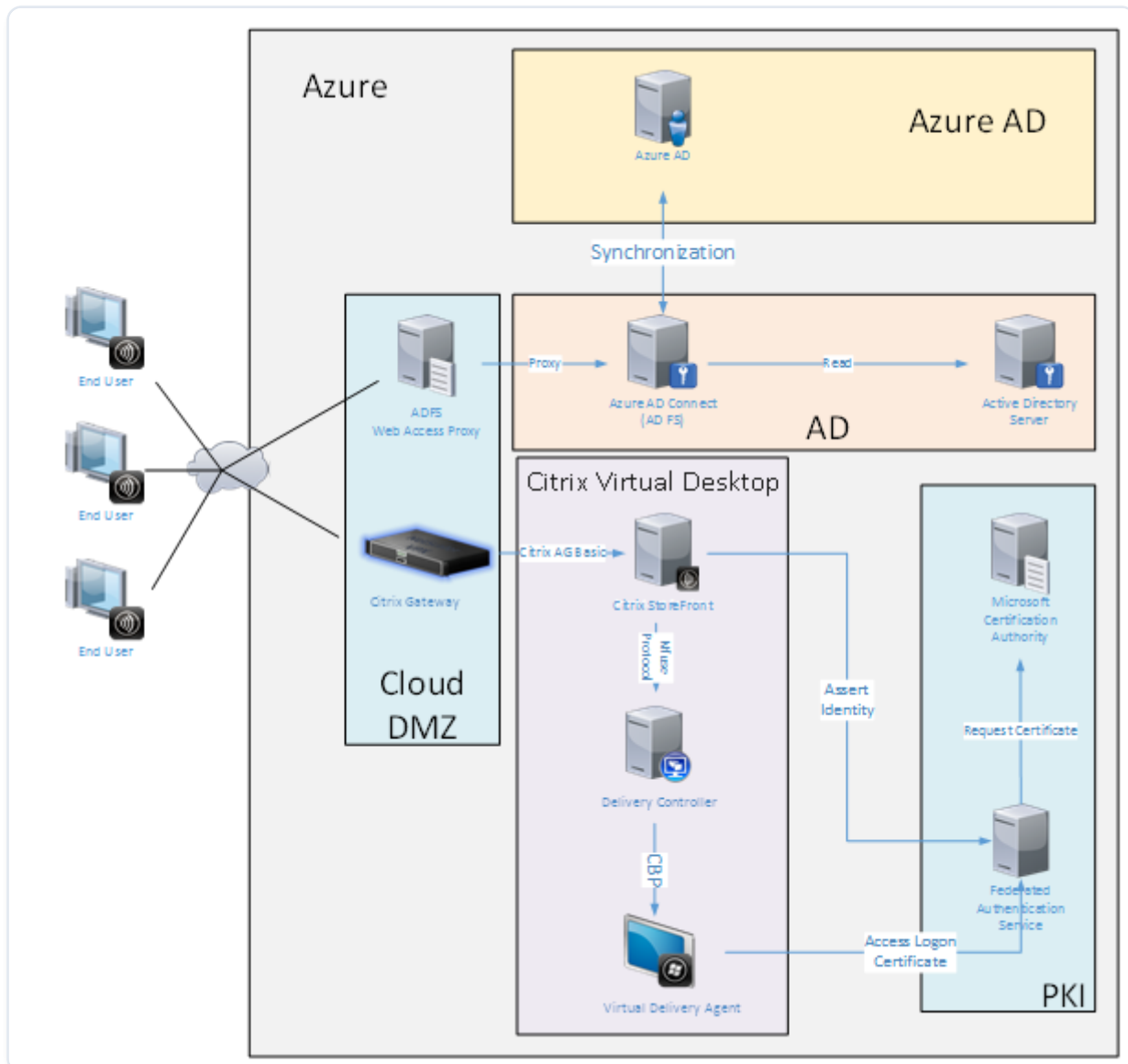
関連情報:

- [インストールと構成](#)の記事では、FASのインストールと構成方法について説明しています。

## ウィンドウズ 10 アジュール AD 参加

Windows 10では、「Azure AD Join」という概念が導入されました。これは、従来のWindowsドメイン参加と概念的には似ていますが、「インターネット経由」のシナリオを対象としています。これはラップトップやタブレットでうまく機能します。従来のWindowsドメイン参加と同様に、Azure ADには会社のWebサイトやリソースに対するシングルサインオンモデルを可能にする

機能があります。これらはすべて「インターネット対応」であるため、オフィスLANだけでなく、インターネットに接続されたあらゆる場所から機能します。



この展開は、「オフィスにいるエンドユーザー」という概念が実質的に存在しない例です。ラップトップは、最新のAzure AD機能を使用して、完全にインターネット経由で登録および認証されます。

この展開のインフラストラクチャは、IPアドレスが利用可能であればどこでも実行できることに注意してください。オンプレミス、ホスト型プロバイダー、Azure、またはその他のクラウドプロバイダーです。Azure AD Connect同期ツールは、Azure ADに自動的に接続します。この例の図では、簡素化のためにAzure VMを使用しています。

関連情報:

- [インストールと構成](#)の記事では、FASのインストールと構成方法について説明しています。
- [Azure AD統合](#)の記事に詳細が記載されています。

# ADFS展開

## はじめに

このドキュメントでは、Citrix®環境をMicrosoft ADFSと統合する方法について説明します。

多くの組織では、単一の認証ポイントを必要とするWebサイトへの安全なユーザーアクセスを管理するためにADFSを使用しています。たとえば、企業は従業員が利用できる追加のコンテンツやダウンロードを持っている場合があります。これらの場所は、標準のWindowsログオン資格情報で保護する必要があります。

Federated Authentication Service (FAS) は、Citrix Gateway および Citrix StoreFront™ を ADFS ログオンシステムと統合することも可能にし、会社のスタッフの潜在的な混乱を軽減します。

この展開では、Citrix Gateway を Microsoft ADFS の証明書利用者として統合します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-architectures-adfs-saml.png)

### 注：

バックエンドリソースがWindows VDAまたはLinux VDAのいずれであっても、違いはありません。

## SAMLの概要

Security Assertion Markup Language (SAML) は、シンプルな「ログオンページへのリダイレクト」Webブラウザログオンシステムです。構成には次の項目が含まれます。

### リダイレクトURL

Citrix Gateway は、ユーザーが認証を必要とすることを検出すると、ユーザーのWebブラウザに、ADFSサーバー上のSAMLログオンWebページにHTTP POSTを実行するように指示します。これは通常、`https://` の形式のアドレスです: `https://adfs.mycompany.com/adfs/ls`。

このWebページPOSTには、ログオン完了時にADFSがユーザーを返す「戻りアドレス」を含むその他の情報が含まれています。

### 識別子

EntityIdは、Citrix GatewayがADFSへのPOSTデータに含める一意の識別子です。これにより、ユーザーがどのサービスにログオンしようとしているかをADFSに通知し、適切な認証ポリシーを

適用します。発行された場合、SAML認証XMLはEntityIdによって識別されるサービスへのログオンにのみ適しています。

通常、EntityIDはCitrix GatewayサーバーのログオンページのURLですが、Citrix GatewayとADFSがそれに同意する限り、一般的には何でも構いません。 `https://ns.mycompany.com/application/logonpage` .

## 戻りアドレス

認証が成功した場合、ADFSはユーザーのWebブラウザに、EntityId用に構成されている応答URLのいずれかにSAML認証XMLをPOSTするよう指示します。これは通常、元のCitrix Gatewayサーバー上の `https://` アドレスで、形式は `https://ns.mycompany.com/cgi/samlauth` です。

複数の応答URLアドレスが構成されている場合、Citrix Gatewayは、ADFSへの最初のPOSTでいずれかを選択できます。

## 署名証明書

ADFSは、秘密鍵を使用してSAML認証XMLプロブを暗号的に署名します。この署名を検証するには、Citrix Gatewayは、証明書ファイルに含まれる公開鍵を使用してこれらの署名をチェックするように構成する必要があります。証明書ファイルは通常、ADFSサーバーから取得したテキストファイルです。

## シングルサインアウトURL

ADFSとCitrix Gatewayは「中央ログアウト」システムをサポートしています。これは、Citrix GatewayがSAML認証XMLプロブが現在ログオンしているセッションをまだ表しているかどうかを確認するために、時々ポーリングするURLです。

これは、構成する必要のないオプション機能です。これは通常、 `https://` 形式の `https://adfs.mycompany.com/adfs/logout` アドレスです。(シングルログオンURLと同じである場合もあります。)

## 構成

セクション [Citrix Gatewayの展開](#) では、標準のLDAP認証オプションを処理するようにCitrix Gatewayを設定する方法について説明しています。それが正常に完了した後、SAML認証を許可する新しい認証ポリシーをCitrix Gateway上に作成できます。これにより、Citrix Gatewayウィザードで使用されるデフォルトのLDAPポリシーを置き換えることができます。

NetScaler > NetScaler Gateway > Policies > Authentication > SAML > Policies

| Name           | Expression | Request Server |
|----------------|------------|----------------|
| StoreFrontSAML | NS_TRUE    | AzureAd        |

## SAMLポリシーを記入する

以前にADFS管理コンソールから取得した情報を使用して、新しいSAML IdPサーバーを構成します。このポリシーが適用されると、Citrix GatewayはユーザーをログオンのためにADFSにリダイレクトし、その見返りとしてADFS署名付きSAML認証トークンを受け入れます。

**Create Authentication SAML Server**

**Create Authentication SAML Server**

Name\*  
AzureAd

Authentication Type  
SAML

IDP Certificate Name\*  
AzureADSAML

Redirect URL\*  
29f-4c20-9826-14d5e484c62e/saml2

Single Logout URL  
29f-4c20-9826-14d5e484c62e/saml2

User Field  
userprincipalname

Signing Certificate Name  
[Dropdown]

Issuer Name  
https://ns.citrixsaml demo.net/Citrix/

Reject Unsigned Assertion\*  
ON

SAML Binding\*  
POST

Default Authentication Group  
[Text Box]

Skew Time(mins)  
5

Two Factor  
☐ ON ☒ OFF

Assertion Consumer Service Index  
255

Attribute Consuming Service Index  
255

Requested Authentication Context\*  
Exact

Authentication Class Types  
InternetProtocol  
InternetProtocolPassword

Signature Algorithm\*  
☐ RSA-SHA1 ☒ RSA-SHA256

Digest Method\*  
☐ SHA1 ☒ SHA256

☐ Send Thumbprint  
☒ Enforce Username

Attribute 1  
[Text Box] [Dropdown]

Attribute 3  
[Text Box] [Dropdown]

Attribute 5  
[Text Box] [Dropdown]

Attribute 7  
[Text Box] [Dropdown]

## 関連情報

- インストールと構成 は、FAS のインストールと構成に関する主要なリファレンスです。

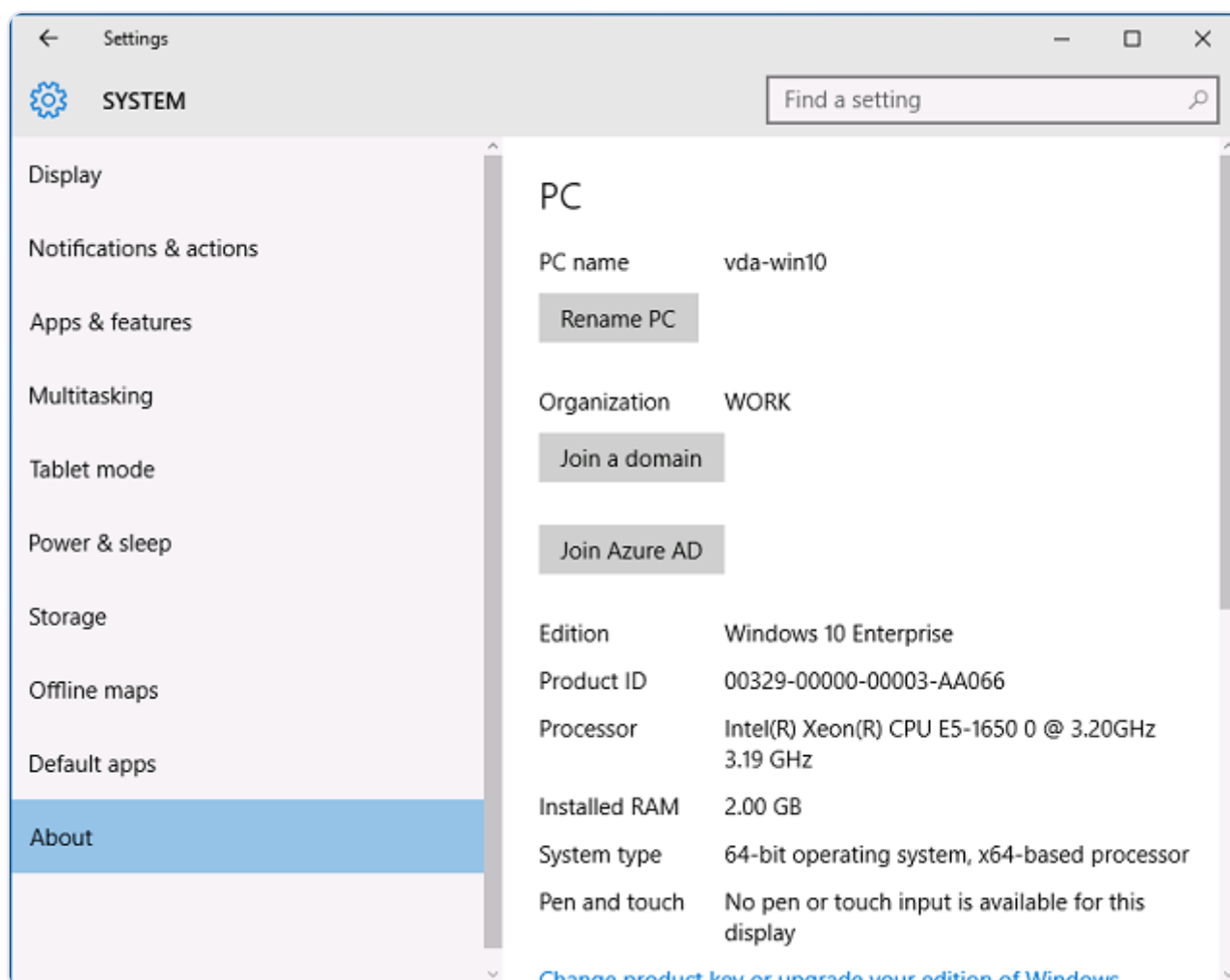
- 一般的な FAS 展開は、[展開アーキテクチャ](#) の記事にまとめられています。
- 「ハウツー」記事は、[高度な構成](#) の記事で紹介されています。

## Azure AD の統合

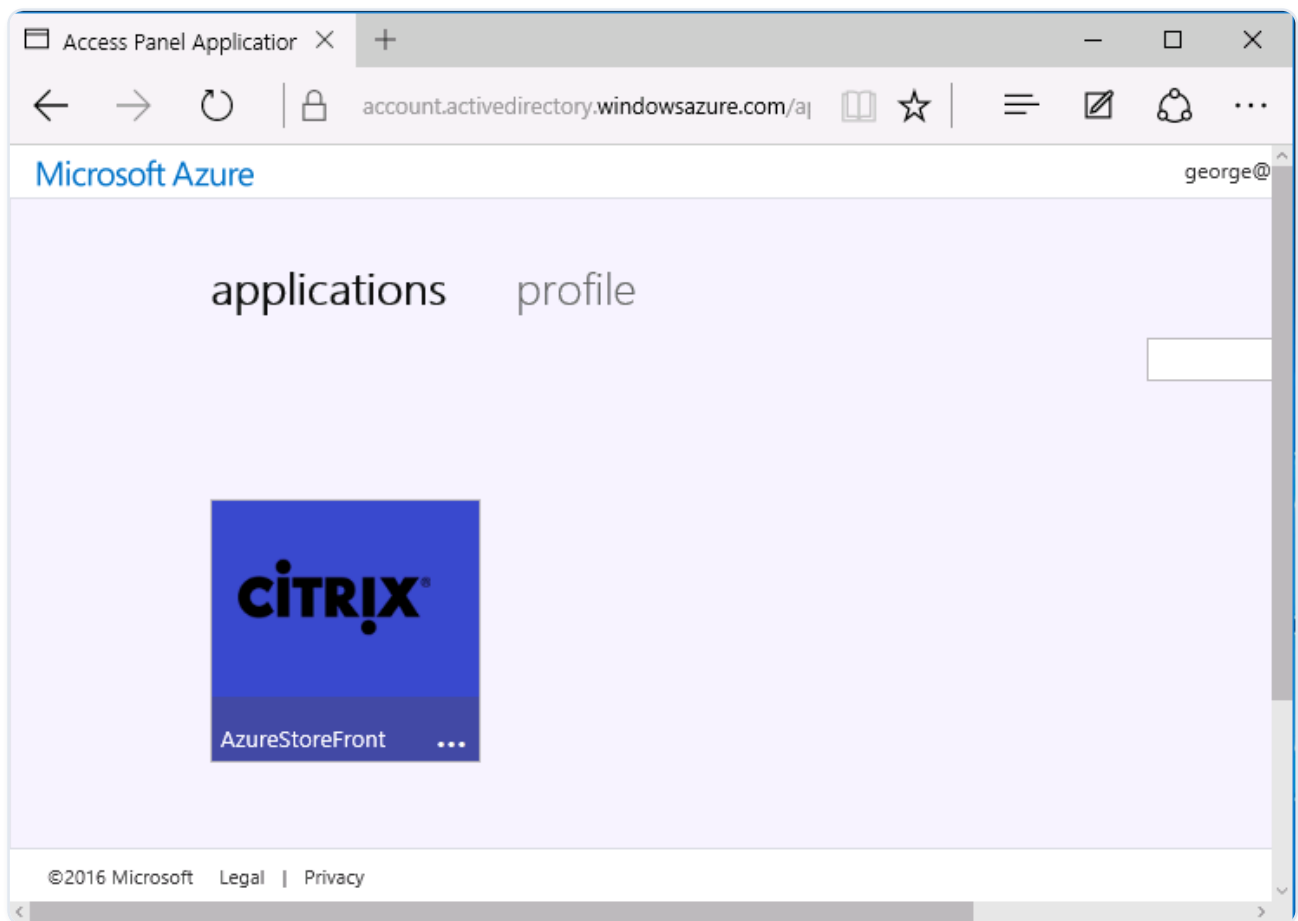
### はじめに

このドキュメントでは、Citrix® 環境を Windows 10 の Azure AD 機能と統合する方法について説明します。Windows 10 で導入された Azure AD は、管理とシングルサインオンのために、ローミング中のラップトップをインターネット経由で企業ドメインに参加させることができる新しいドメイン参加モデルです。

このドキュメントの展開例では、IT 部門が新規ユーザーに企業メールアドレスと個人用 Windows 10 ラップトップ用の登録コードを提供するシステムについて説明します。ユーザーは、**設定** パネルの **システム > バージョン情報 > Azure AD** に参加オプションからこのコードにアクセスします。



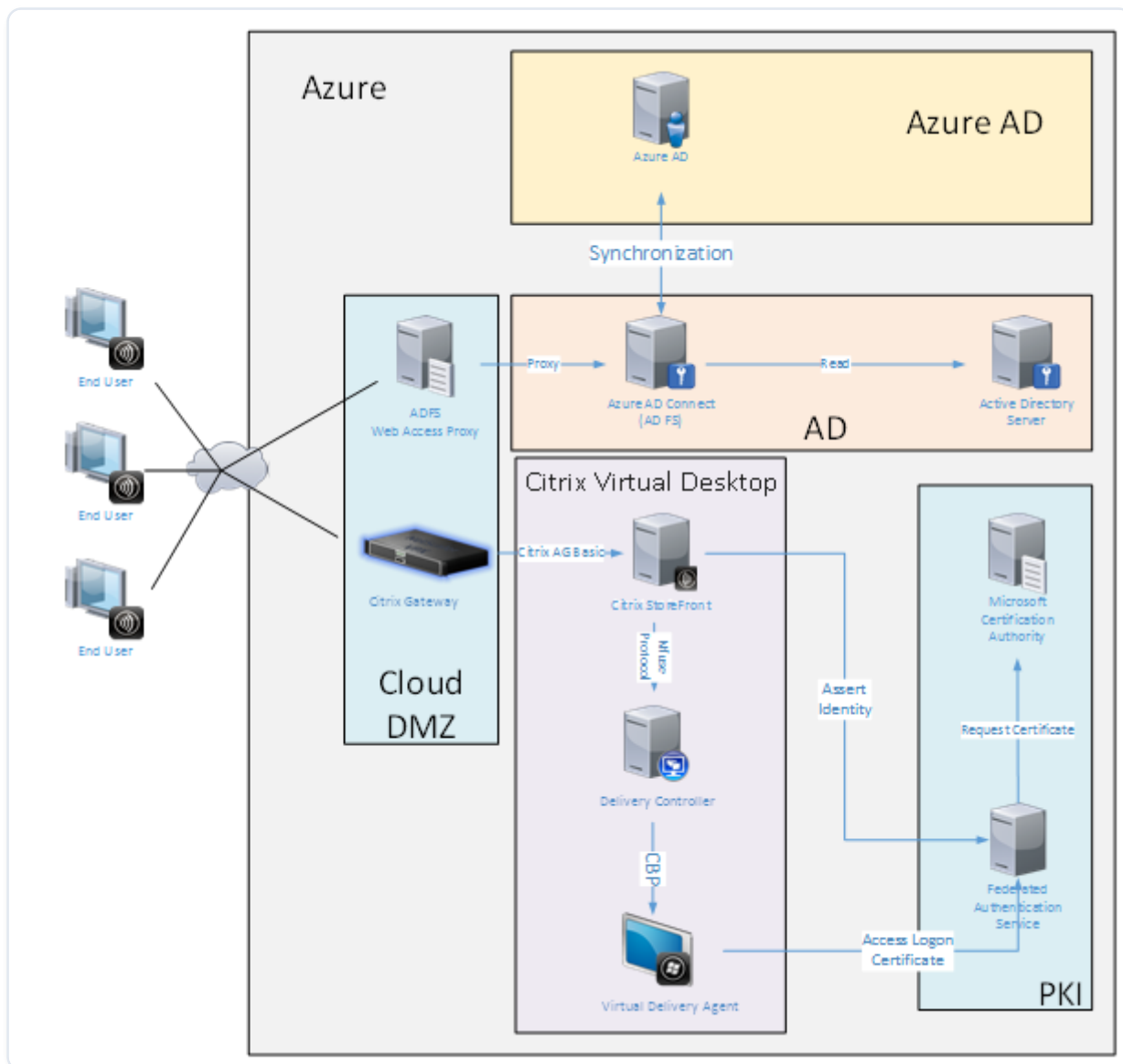
ラップトップが登録されると、Microsoft Edge Web ブラウザーは、Azure SaaS アプリケーションの Web ページを介して、会社の Web サイトや Citrix 公開アプリケーションに自動的にサインオンします。これには、Office 365 などの他の Azure アプリケーションも含まれます。



## アーキテクチャ

このアーキテクチャは、従来の企業ネットワークを Azure 内で完全に複製し、Azure AD や Office 365 などの最新のクラウドテクノロジーと統合します。エンドユーザーはすべてリモートワーカーと見なされ、オフィスイントラネット上にいるという概念はありません。

このモデルは、既存のオンプレミスシステムを持つ企業にも適用できます。これは、Azure AD Connect 同期がインターネット経由で Azure にブリッジできるためです。



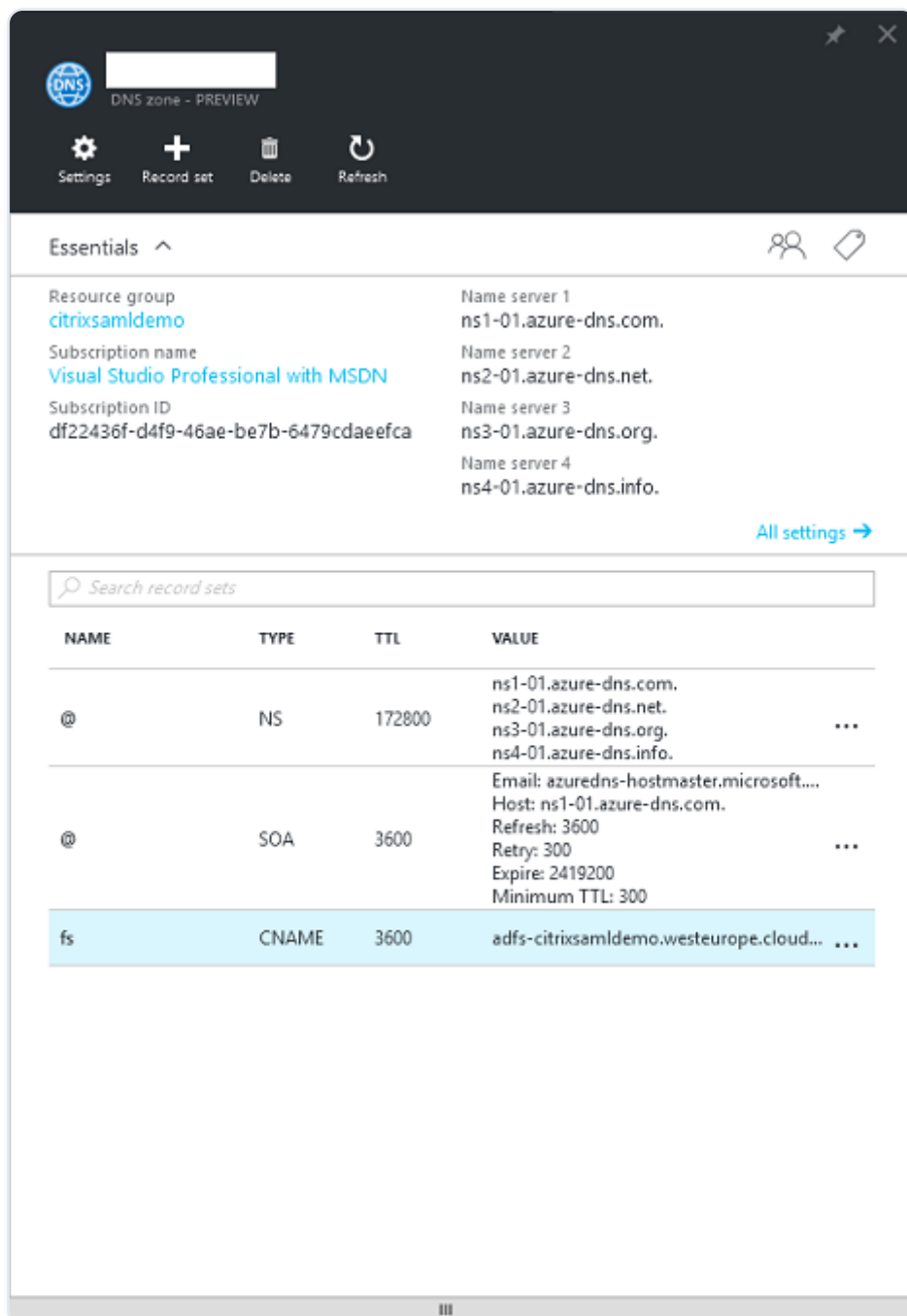
従来、ファイアウォールで保護された LAN と Kerberos/NTLM 認証であったセキュアな接続とシングルサインオンは、このアーキテクチャでは Azure への TLS 接続と SAML に置き換えられます。新しいサービスは、Azure AD に参加する Azure アプリケーションとして構築されます。Active Directory を必要とする既存のアプリケーション (SQL Server データベースなど) は、Azure Cloud Service の IAAS 部分で標準の Active Directory Server VM を使用して実行できます。

ユーザーが従来のアプリケーションを起動すると、Citrix Virtual Apps and Desktops™ 公開アプリケーションを使用してアクセスされます。さまざまな種類のアプリケーションは、Microsoft Edge のシングルサインオン機能を使用して、ユーザーの **Azure アプリケーション** ページを通じて照合されます。Microsoft は、Azure アプリケーションを列挙して起動できる Android および iOS アプリも提供しています。

## DNS ゾーン作成

Azure AD では、管理者がパブリック DNS アドレスを登録し、ドメイン名サフィックスの委任ゾーンを制御する必要があります。これを行うには、管理者は Azure DNS ゾーン機能を使用できます。

この例では、DNSゾーン名 *citrixsamldemo.net* を使用します。



コンソールには Azure DNS ネームサーバーの名前が表示されます。これらは、ゾーンの DNS レジストラの NS エントリで参照される必要があります（例: [citrixsamldemo.net. NS ns1-01.azure-dns.com](#)）。

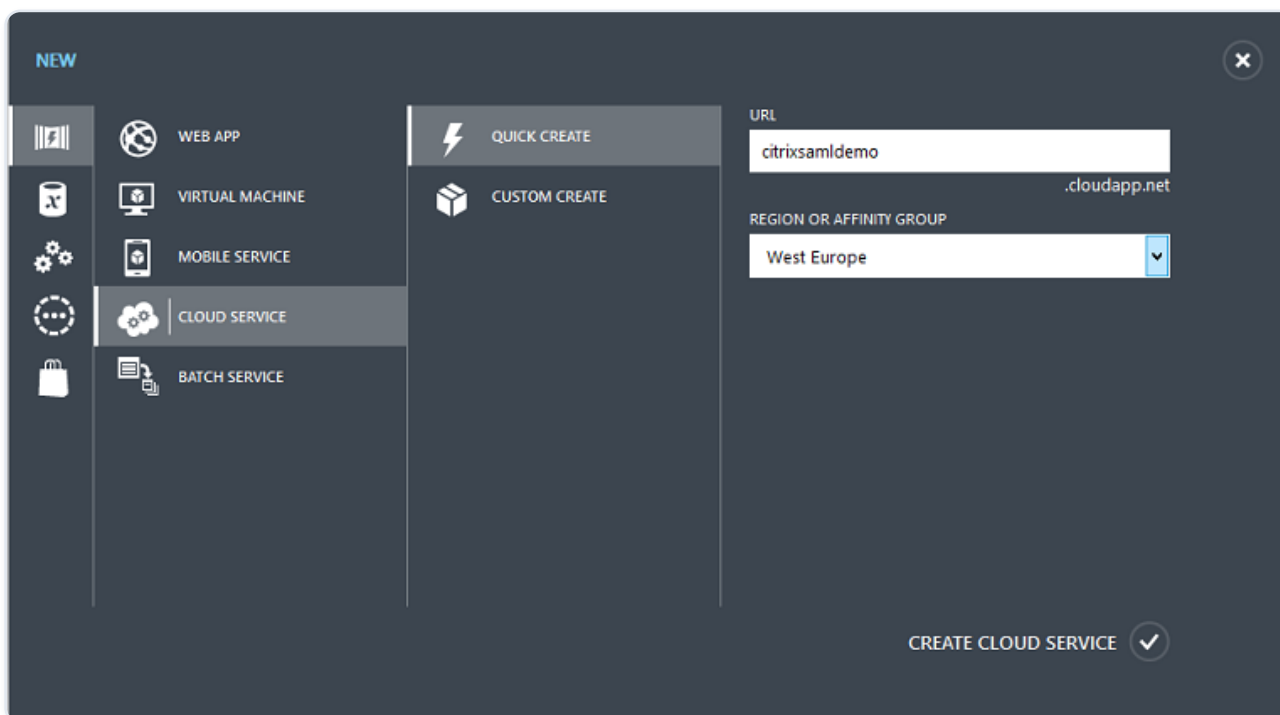
Azureで実行されているVMへの参照を追加する場合、VMのAzure管理DNSレコードへのCNAMEポインターを使用するのが最も簡単です。VMのIPアドレスが変更されても、DNSゾーンファイルを手動で更新する必要はありません。

この展開では、内部および外部のDNSアドレスサフィックスが一致します。ドメインはcitrixsamldemo.netで、スプリットDNS（内部的には10.0.0.\*）を使用します。

Web Application Proxyサーバーを参照する「fs.citrixsamldemo.net」エントリを追加します。これはこのゾーンのフェデレーションサービスです。

## クラウドサービスを作成する

この例では、Azureで実行されているADFSサーバーを含むAD環境を含むCitrix環境を構成します。「citrixsamldemo」という名前のクラウドサービスが作成されます。



## Windows仮想マシンを作成する

クラウドサービスで実行される5つのWindows VMを作成します。

- ドメインコントローラー (domaincontrol)
- アジュール コネクト ADFSサーバー (adfs)
- ADFS Webアクセスプロキシ (Web Application Proxy、ドメイン参加なし)
- Citrix Virtual Apps and Desktops デリバリーコントローラー
- Citrix Virtual Apps and Desktops 仮想デリバリーエージェント (VDA)

Microsoft Azure

Create virtual machine > Basics

Create virtual machine

Basics

1 Basics  
Configure basic settings

2 Size  
Choose virtual machine size

3 Settings  
Configure optional features

4 Summary  
Windows Server 2012 R2 Datacenter

\* Name

\* User name

\* Password

Subscription  
Visual Studio Professional with MSDN

\* Resource group  
citrixsaml-demo

Location  
West Europe

OK

## ドメインコントローラー

- 標準のActive Directory展開（この例ではcitrixsaml-demo.net）を作成するために、**DNSサーバー**と**Active Directory ドメインサービス**の役割を追加します。ドメイン昇格が完了したら、**Active Directory 証明書サービス**の役割を追加します。
- テスト用の通常のユーザーアカウントを作成します（例: [George@citrixsaml-demo.net](mailto:George@citrixsaml-demo.net)）。
- このサーバーは内部DNSを実行するため、すべてのサーバーはDNS解決のためにこのサーバーを参照する必要があります。これは、**Azure DNS設定**ページから実行できます。（詳細については、このドキュメントの付録を参照してください。）

## ADFSコントローラーとWebアプリケーションプロキシサーバー

- ADFSサーバーをcitrixsaml-demoドメインに参加させます。Webアプリケーションプロキシサーバーは隔離されたワークグループに残しておく必要があるため、AD DNSにDNSアドレスを手動で登録します。

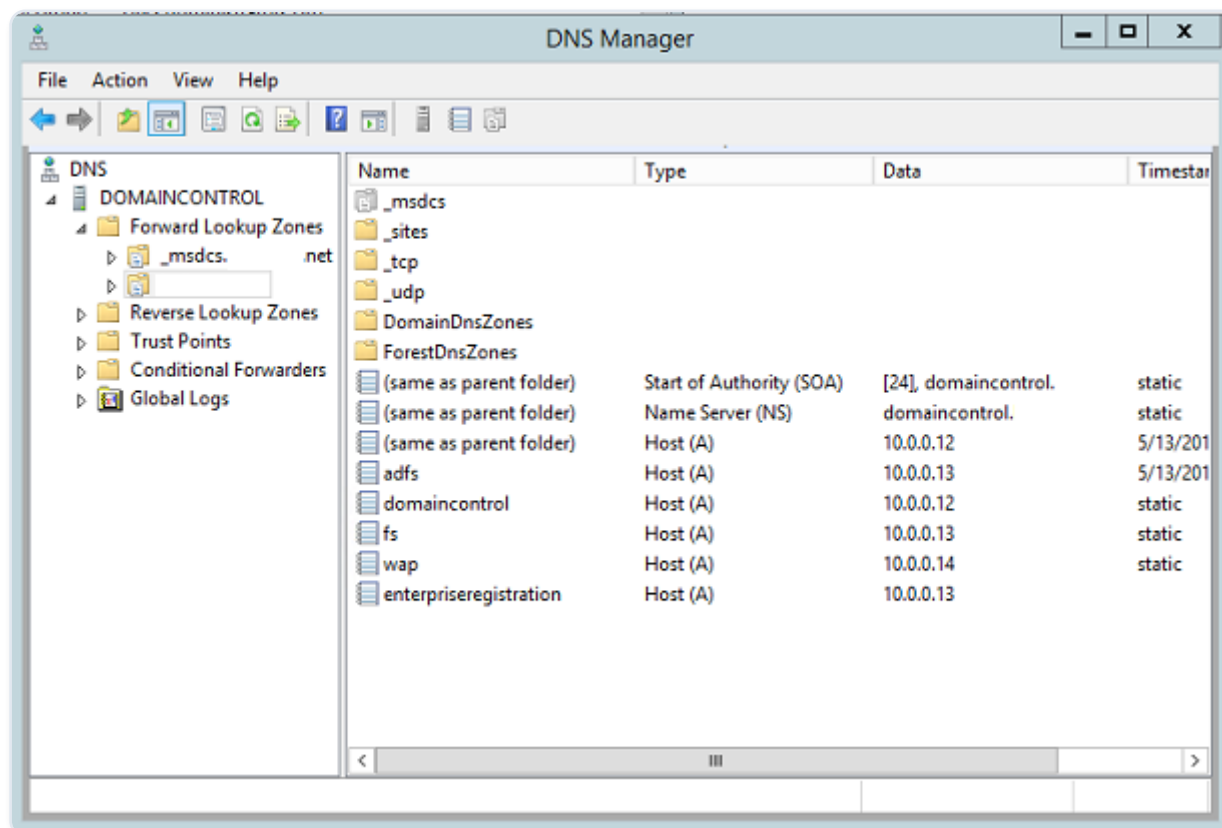
- AzureAD Connectツールからのファイアウォール経由でのPSリモート処理を許可するために、これらのサーバーで**Enable-PSRemoting -Force**コマンドレットを実行します。

## Citrix Virtual Desktops™ デリバリーコントローラーおよびVDA

- Citrix Virtual AppsまたはCitrix Virtual Desktops Delivery Controller™とVDAを、citrixsamldemo.netに参加している残りの2台のWindowsサーバーにインストールします。

## 内部DNSを構成する

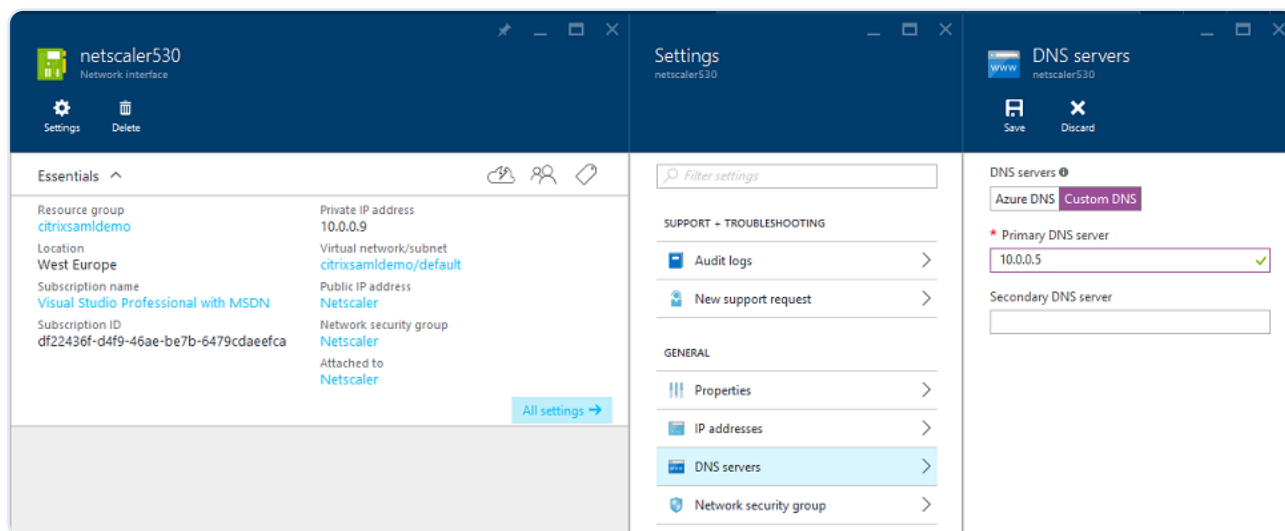
ドメインコントローラーがインストールされたら、DNSサーバーを構成してcitrixsamldemo.netの内部ビューを処理し、外部DNSサーバー（例: 8.8.8.8）へのフォワーダーとして機能するようにします。



静的レコードを追加します:

- wap.citrixsamldemo.net
- fs.citrixsamldemo.net
- enterpriseregistration.citrixsaml.net

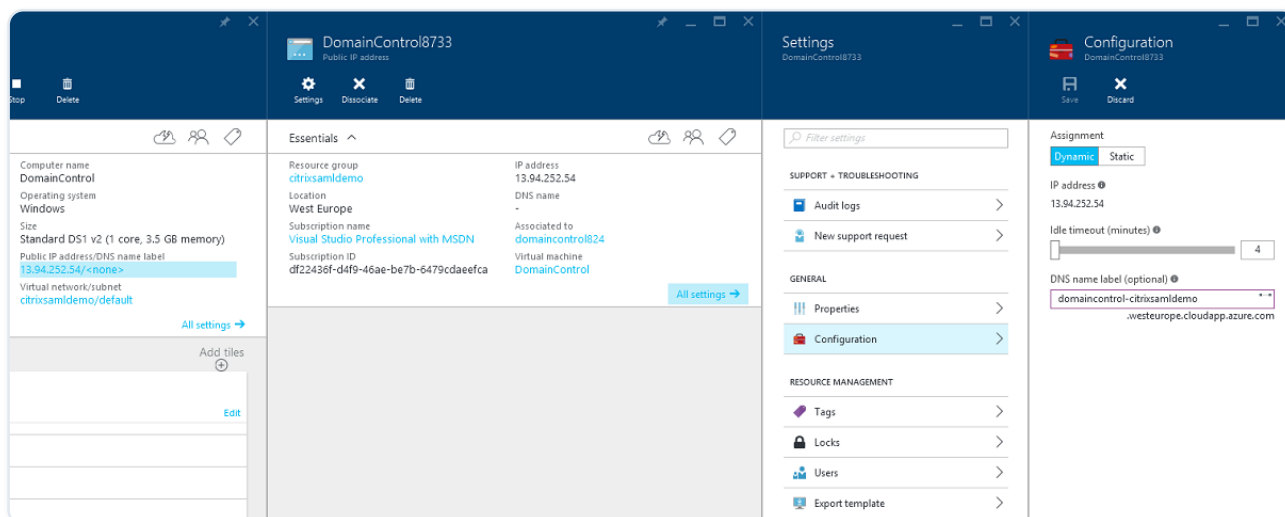
Azure で実行されているすべての VM は、この DNS サーバーのみを使用するように構成する必要があります。これは、ネットワークインターフェイスの GUI を介して行うことができます。



既定では、内部 IP (10.0.0.9) アドレスは動的に割り当てられます。IP アドレス設定を使用して、IP アドレスを永続的に割り当てることができます。これは、Web アプリケーションプロキシサーバーとドメインコントローラーに対して行う必要があります。

## 外部 DNS アドレスを構成する

VM の実行中、Azure は VM に割り当てられている現在のパブリック IP アドレスを指す独自の DNS ゾーンサーバーを維持します。これは、Azure が既定で各 VM の起動時に IP アドレスを割り当てるため、有効にすると便利な機能です。

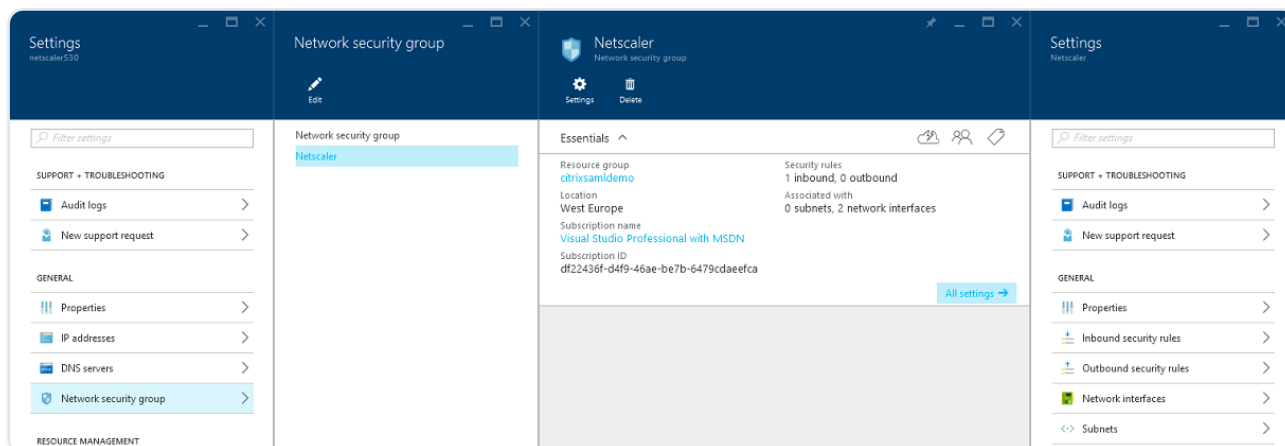


この例では、domaincontrol-citrixsamdemo.westeurope.cloudapp.azure.com の DNS アドレスをドメインコントローラーに割り当てます。

リモート構成が完了すると、Web アプリケーションプロキシと Citrix Gateway VM のみがパブリック IP アドレスを有効にする必要があることに注意してください。(構成中、パブリック IP アドレスは環境への RDP アクセスに使用されます)。

## セキュリティグループを構成する

Azure クラウドは、セキュリティグループを使用して、インターネットから VM への TCP/UDP アクセスに対するファイアウォールルールを管理します。既定では、すべての VM で RDP アクセスが許可されています。Citrix Gateway および Web アプリケーションプロキシサーバーも、ポート 443 で TLS を許可する必要があります。

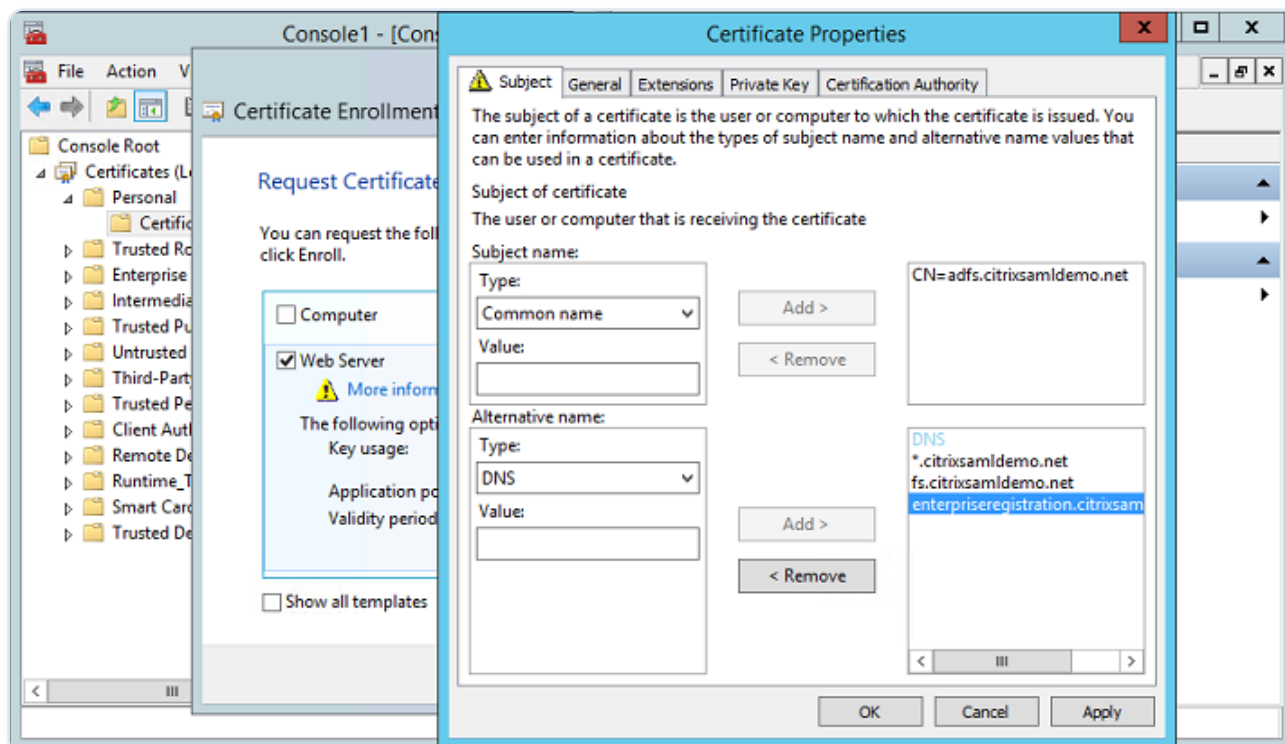


## ADFS 証明書を作成する

Microsoft 証明機関で **Webサーバー** 証明書テンプレートを有効にします。これにより、カスタム DNS アドレスを持つ証明書を作成し、(秘密キーを含めて) pfx ファイルにエクスポートできます。この証明書は ADFS サーバーと Web アプリケーションプロキシサーバーの両方にインストールする必要がありますため、PFX ファイルが推奨されるオプションです。

以下のサブジェクト名で Web サーバー証明書を発行します。

- コモンネーム:
  - adfs.citrixsamldemo.net
- サブジェクト代替名:
  - \*.citrixsamldemo.net
  - fs.citrixsamldemo. ネットワーク
  - enterpriseregistration.citrixsamldemo.net



パスワードで保護された秘密キーを含め、証明書をpfxファイルにエクスポートします。

## Azure ADをセットアップする

このセクションでは、新しいAzure ADインスタンスをセットアップし、Windows 10をAzure ADに参加させるために使用できるユーザーIDを作成するプロセスについて詳しく説明します。

### 新しいディレクトリを作成する

クラシックAzureポータルにログインし、新しいディレクトリを作成します。

**ADD DIRECTORY**

**DIRECTORY** ⓘ

Create new directory ▼

**NAME** ⓘ

CitrixSAMLdemo

**DOMAIN NAME** ⓘ

citrixsaml demo ✓ .onmicrosoft.com

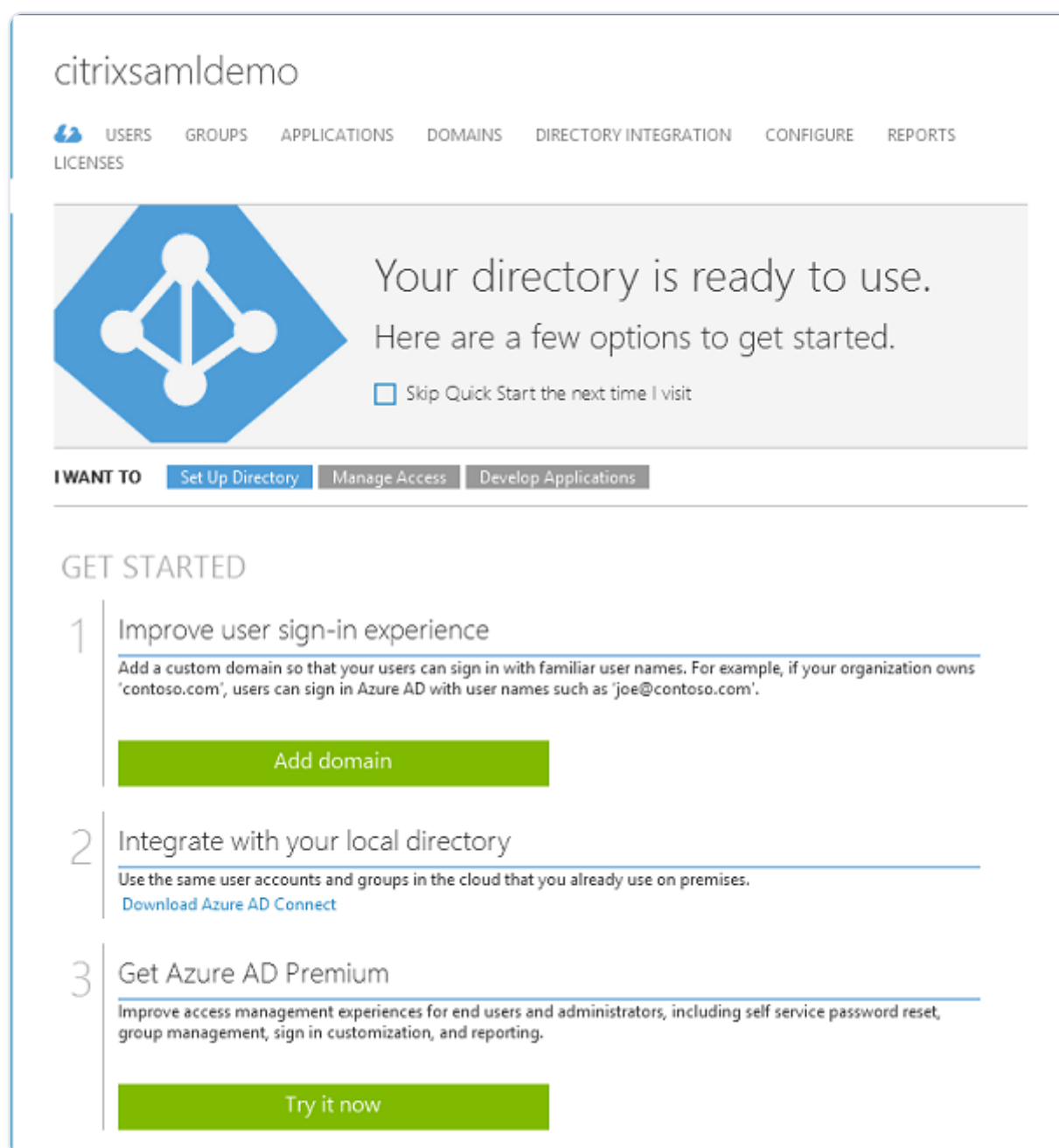
**COUNTRY OR REGION** ⓘ

United Kingdom ▼

☐ This is a B2C directory. ⓘ **PREVIEW**

✓

完了すると、概要ページが表示されます。



The screenshot shows the Citrix SAML Demo web application. At the top, the title "citrixsamldemo" is displayed. Below it is a navigation bar with links: USERS, GROUPS, APPLICATIONS, DOMAINS, DIRECTORY INTEGRATION, CONFIGURE, REPORTS, and LICENSES. The main content area features a large blue hexagonal icon with a white network diagram. To the right of the icon, the text reads: "Your directory is ready to use. Here are a few options to get started." Below this text is a checkbox labeled "Skip Quick Start the next time I visit". Underneath, there is a section titled "I WANT TO" with three buttons: "Set Up Directory" (highlighted in blue), "Manage Access", and "Develop Applications". Below this is a section titled "GET STARTED" with three numbered steps:
 

- 1 Improve user sign-in experience**: Add a custom domain so that your users can sign in with familiar user names. For example, if your organization owns 'contoso.com', users can sign in Azure AD with user names such as 'joe@contoso.com'. Below this is a green button labeled "Add domain".
- 2 Integrate with your local directory**: Use the same user accounts and groups in the cloud that you already use on premises. Below this is a blue link labeled "Download Azure AD Connect".
- 3 Get Azure AD Premium**: Improve access management experiences for end users and administrators, including self service password reset, group management, sign in customization, and reporting. Below this is a green button labeled "Try it now".

## グローバル管理者ユーザー (AzureAdmin) を作成する

Azure でグローバル管理者を作成し (この例では

[AzureAdmin@citrixsamldemo.onmicrosoft.com](mailto:AzureAdmin@citrixsamldemo.onmicrosoft.com))、新しいアカウントでログオンしてパスワードを設定します。

ADD USER

user profile

FIRST NAME: Azure

LAST NAME: Admin

DISPLAY NAME: Azure Admin

ROLE: Global Admin

ALTERNATE EMAIL ADDRESS: [Red error icon]

MULTI-FACTOR AUTHENTICATION: ☐ Enable Multi-Factor Authentication

1 3

## ドメインを Azure AD に登録する

既定では、ユーザーは `<user.name>@<company>.onmicrosoft.com` の形式のメールアドレスで識別されます。

これでも追加設定なしで機能しますが、標準形式のメールアドレス、できればエンドユーザーのメールアカウントと一致するものがより適切です: `<user.name>@<company>.com`。

ドメインの追加アクションは、実際の会社のドメインからのリダイレクトを設定します。この例では `citrixsamldemo.net` を使用します。

シングルサインオンのために ADFS を設定する場合は、チェックボックスを有効にします。

ADD DOMAIN

Specify a domain name

Enter the name of a domain that your organization owns. ?

DOMAIN NAME

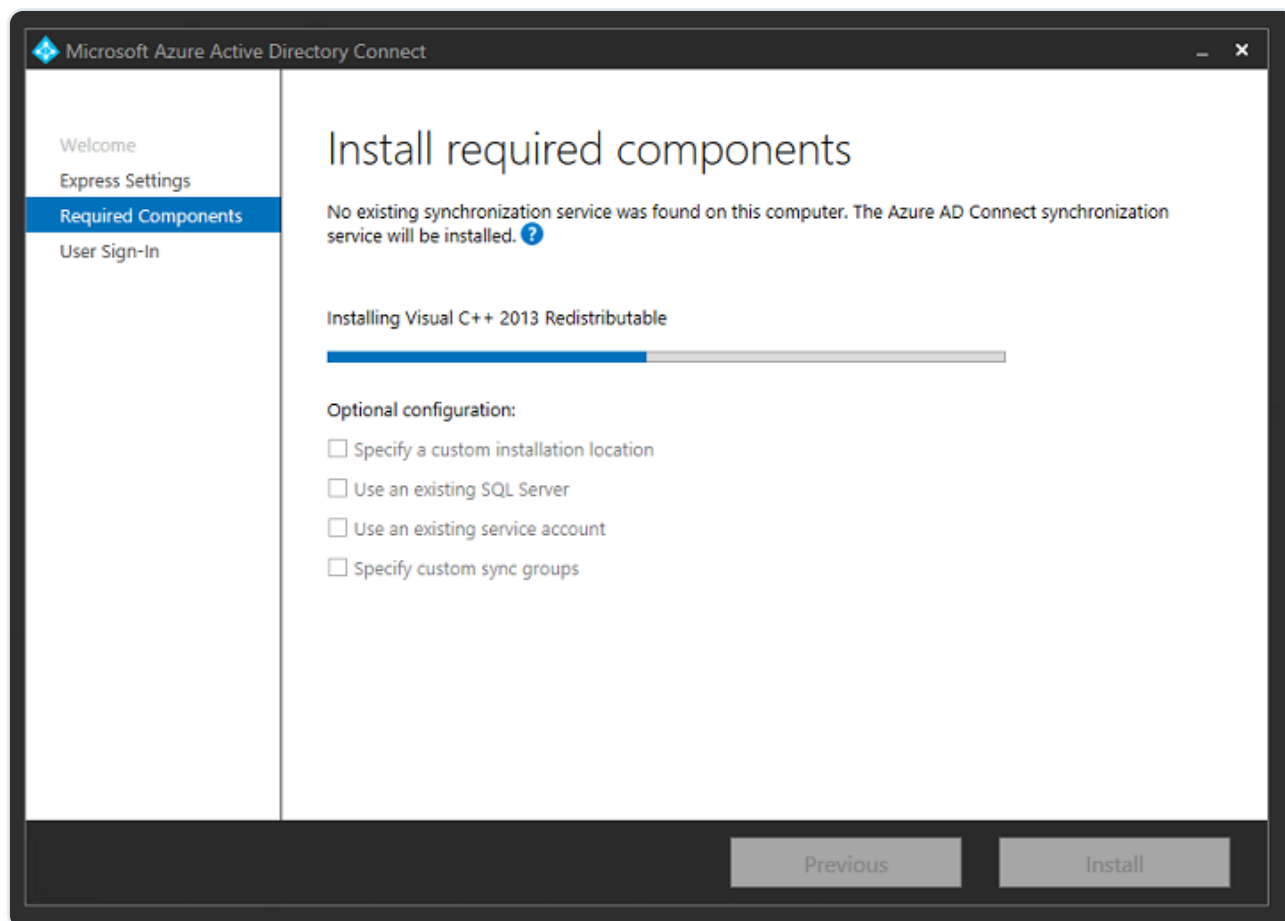
☒ I plan to configure this domain for single sign-on with my local Active Directory. ?

add

2

## Azure AD Connect をインストールする

Azure AD 構成 GUI の手順 2 は、Azure AD Connect の Microsoft ダウンロードページにリダイレクトされます。これを ADFS VM にインストールします。ADFS オプションを利用できるように、カスタムインストールを使用し、簡易設定は使用しないでください。



AD FS とのフェデレーションシングルサインオンオプションを選択します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-setup-azure-usersignin.png)

以前作成した管理者アカウントでAzureに接続します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-setup-azure-connect.png)

内部ADフォレストを選択します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-setup-azure-connect-dirs.png)

すべてのレガシーActive DirectoryオブジェクトをAzure ADと同期します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-setup-azure-domain-ou-filter.png)

ディレクトリ構造が単純な場合は、ユーザー名が十分に一意であるため、ログオンするユーザーを識別できます。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-setup-azure-unique-id-users.png)

デフォルトのフィルタリングオプションを受け入れるか、ユーザーとデバイスを特定のグループセットに制限します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-setup-azure-filter-users-devices.png)

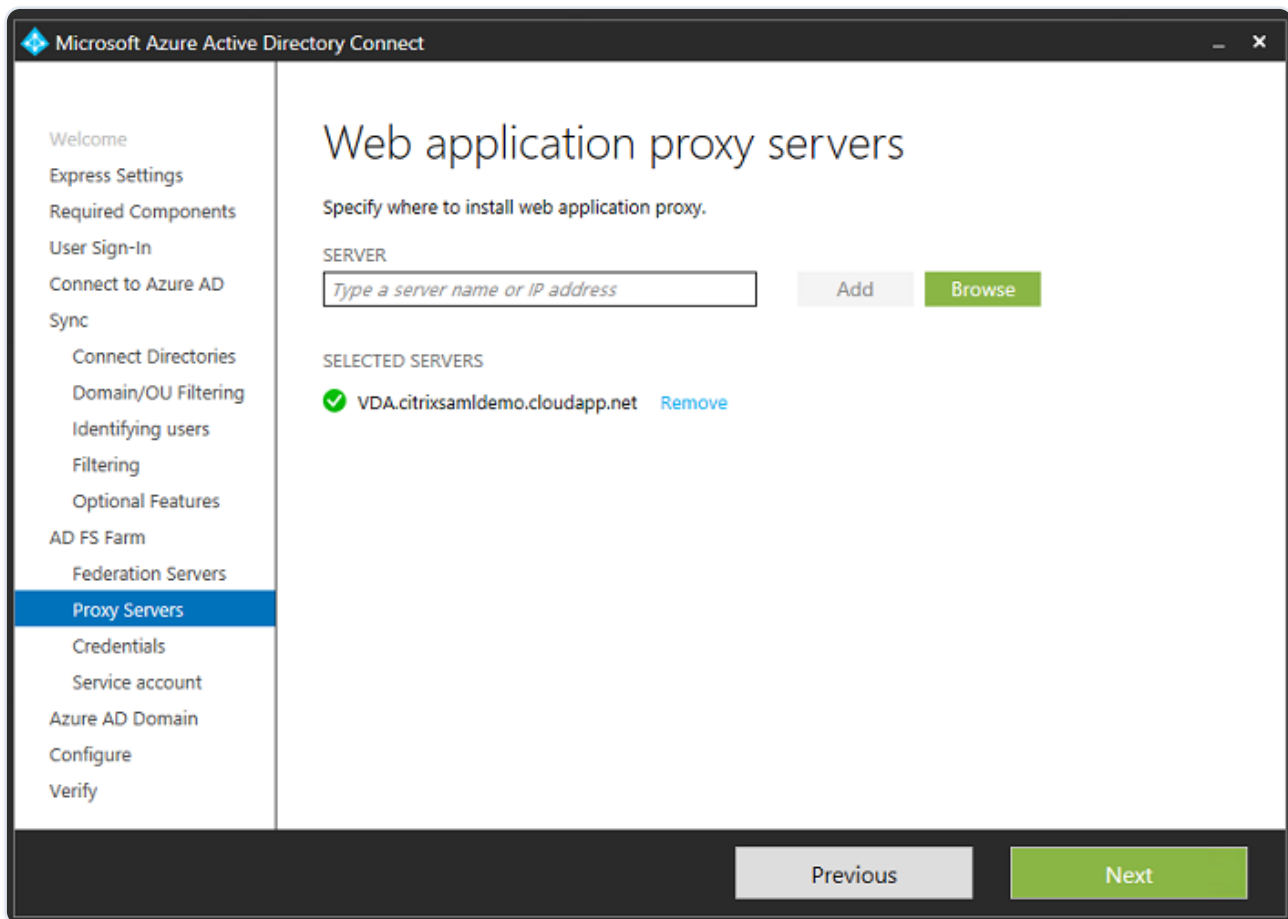
必要に応じて、Azure ADパスワードをActive Directoryと同期できます。これは通常、ADFSベースの認証には必要ありません。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-setup-azure-optional-features.png)

AD FSで使用する証明書PFXファイルを選択し、DNS名としてfs.citrixsamldemo.netを指定します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-setup-azure-adfs-farm.png)

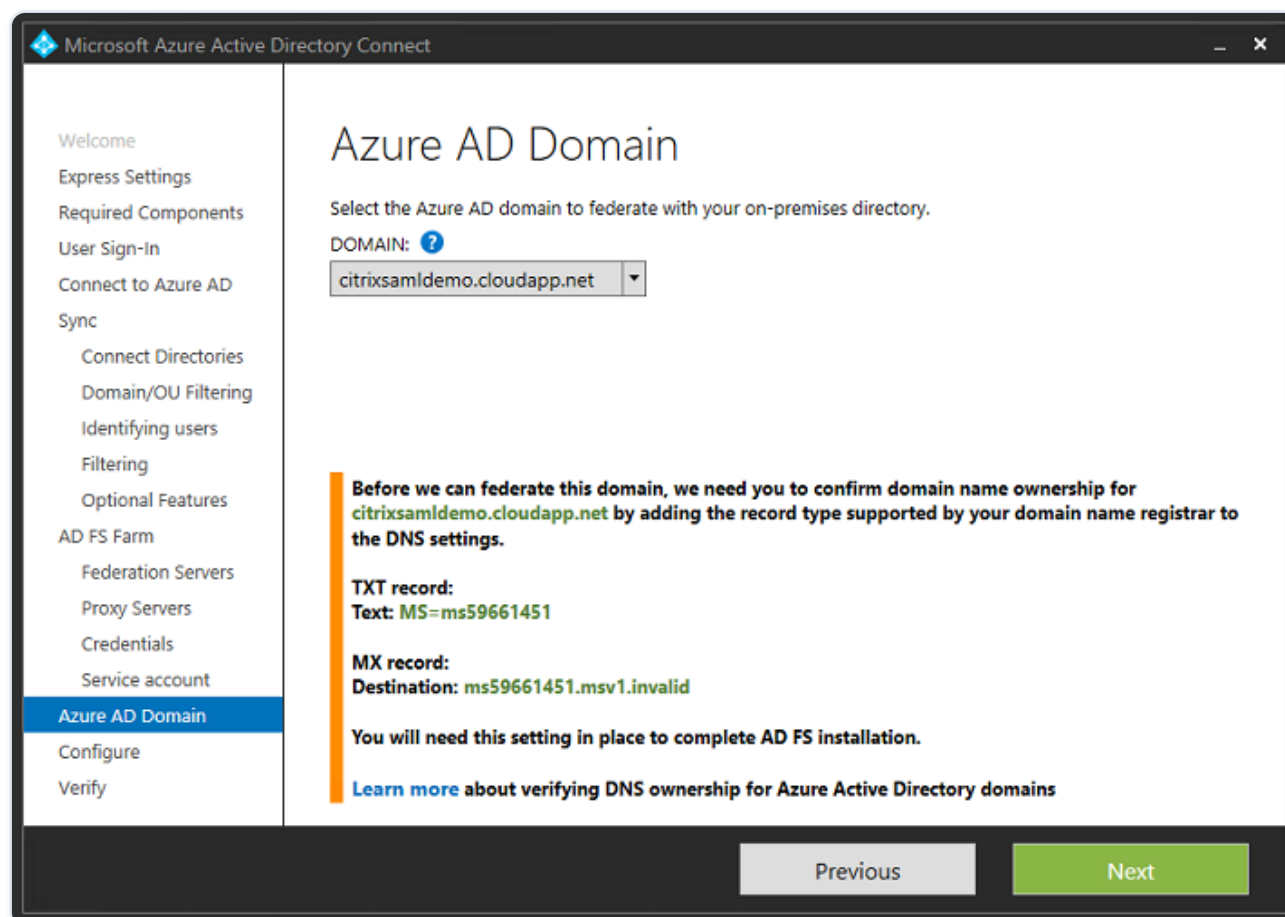
プロキシサーバーの選択を求められたら、wap.citrixsamldemo.net サーバーのアドレスを入力します。Azure AD Connect が構成できるように、Web アプリケーションプロキシサーバーで管理者として **Enable-PSRemoting -Force** コマンドレットを実行する必要がある場合があります。



**注:**

リモート PowerShell の信頼性の問題によりこの手順が失敗した場合は、Web アプリケーションプロキシサーバーをドメインに参加させてみてください。

ウィザードの残りの手順では、標準の管理者パスワードを使用し、ADFS のサービスアカウントを作成します。その後、Azure AD Connect は DNS ゾーンの所有権を検証するよう求めます。



TXT および MX レコードを Azure の DNS アドレスレコードに追加します。

| Search record sets |       |        |                                                                                                                                                   |
|--------------------|-------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| NAME               | TYPE  | TTL    | VALUE                                                                                                                                             |
| @                  | NS    | 172800 | ns1-01.azure-dns.com,<br>ns2-01.azure-dns.net,<br>ns3-01.azure-dns.org,<br>ns4-01.azure-dns.info. ...                                             |
| @                  | SOA   | 3600   | Email: azuredns-hostmaster.microsoft...,<br>Host: ns1-01.azure-dns.com,<br>Refresh: 3600<br>Retry: 300<br>Expire: 2419200<br>Minimum TTL: 300 ... |
| @                  | TXT   | 3600   | ms70102213 ...                                                                                                                                    |
| fs                 | CNAME | 3600   | adfs-citrixsaml demo.westeurope.cloud... ...                                                                                                      |

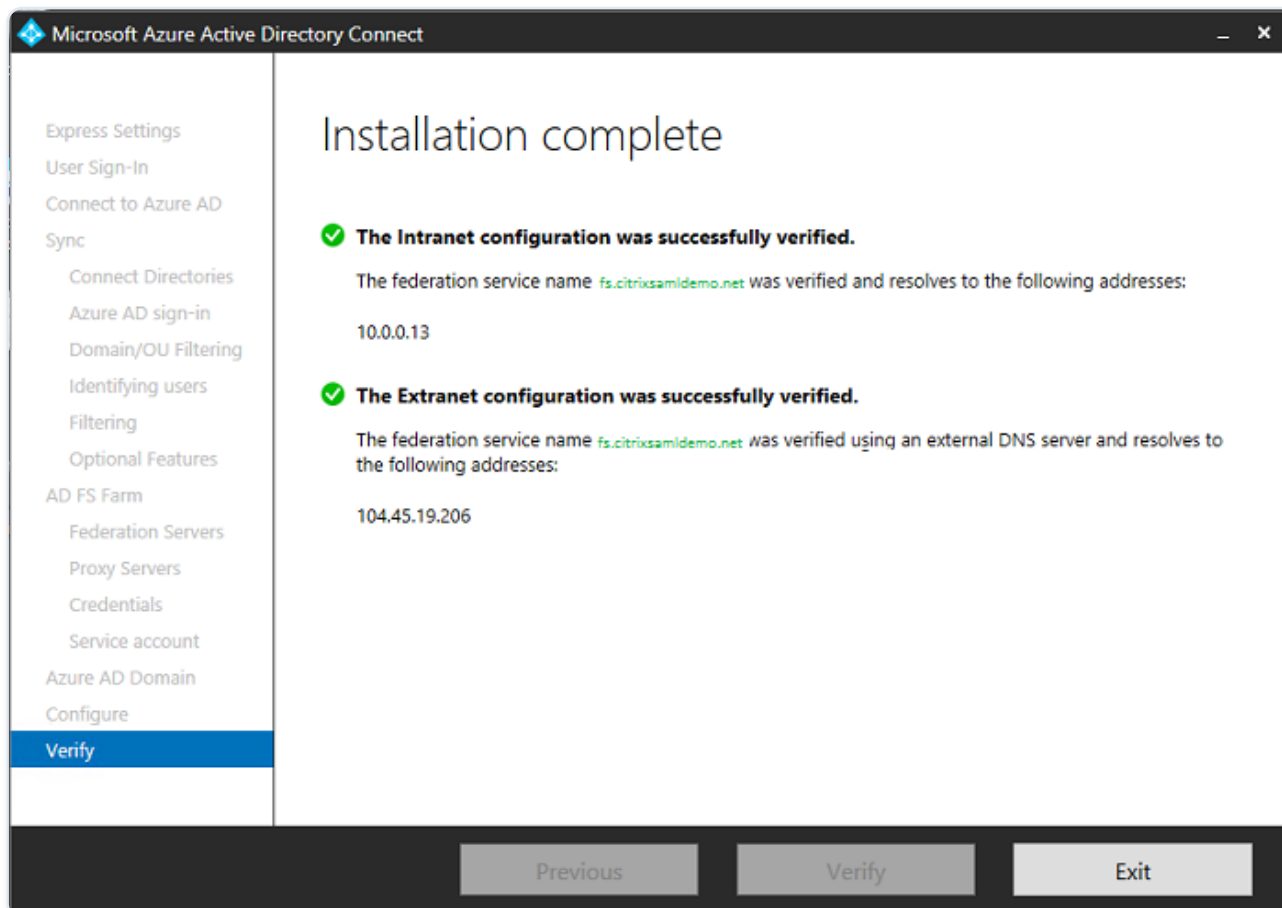
Azure 管理コンソールで 検証 をクリックします。

| CitrixSamlDemo                  |        |            |                |                |  |
|---------------------------------|--------|------------|----------------|----------------|--|
| DOMAIN NAME                     | TYPE   | STATUS     | SINGLE SIGN-ON | PRIMARY DOMAIN |  |
| citrixsaml demo.onmicrosoft.com | Basic  | Active     | Not Available  | Yes            |  |
| citrixsaml demo.net             | Custom | Unverified | Not Configured | No             |  |

**注:**

この手順が失敗した場合は、Azure AD Connect を実行する前にドメインを検証できます。

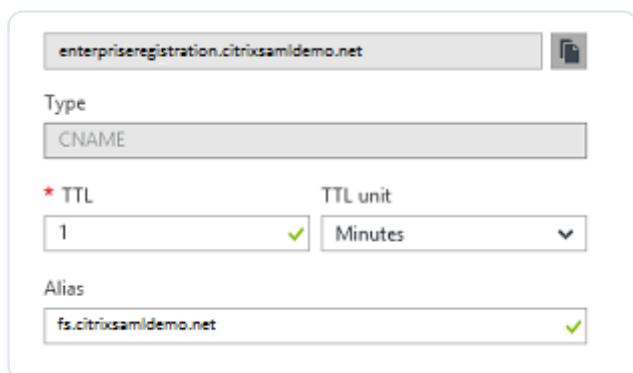
完了すると、外部アドレス fs.citrixsamldemo.net がポート 443 経由で接続されます。



## Azure AD Join を有効にする

ユーザーがメールアドレスを入力してWindows 10がAzure AD参加を実行できるようにすると、DNSサフィックスを使用して、ADFSを指すCNAME DNSレコードが構築されます: enterpriseregistration.\<upnsuffix>。

この例では、これは fs.citrixsamldemo.net です。



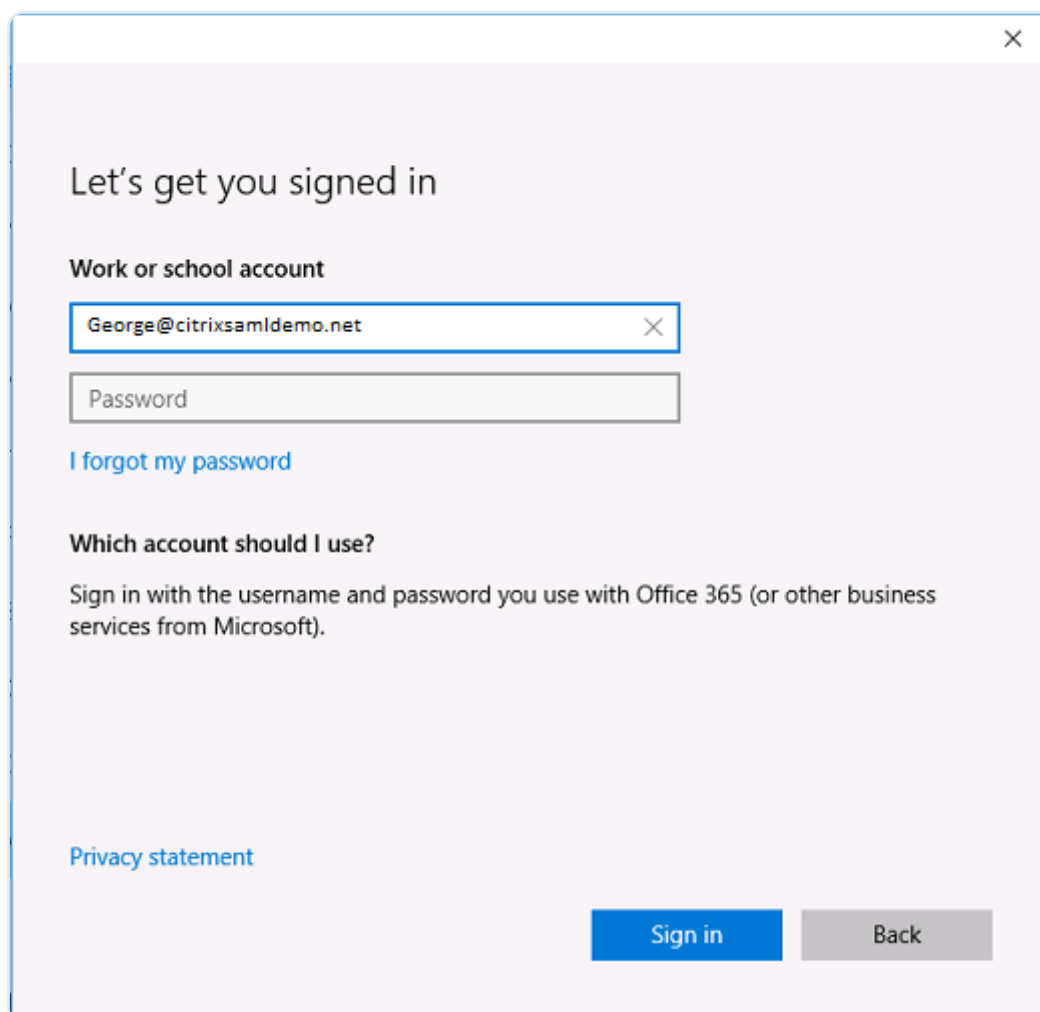
enterpriseregistration.citrixsamdemo.net

Type  
CNAME

\* TTL      TTL unit  
1      Minutes

Alias  
fs.citrixsamdemo.net

公開証明機関を使用していない場合は、WindowsがADFSサーバーを信頼するように、ADFSルート証明書がWindows 10コンピューターにインストールされていることを確認してください。以前に生成された標準ユーザーアカウントを使用して、Azure ADドメイン参加を実行します。



Let's get you signed in

Work or school account

George@citrixsamdemo.net

Password

[I forgot my password](#)

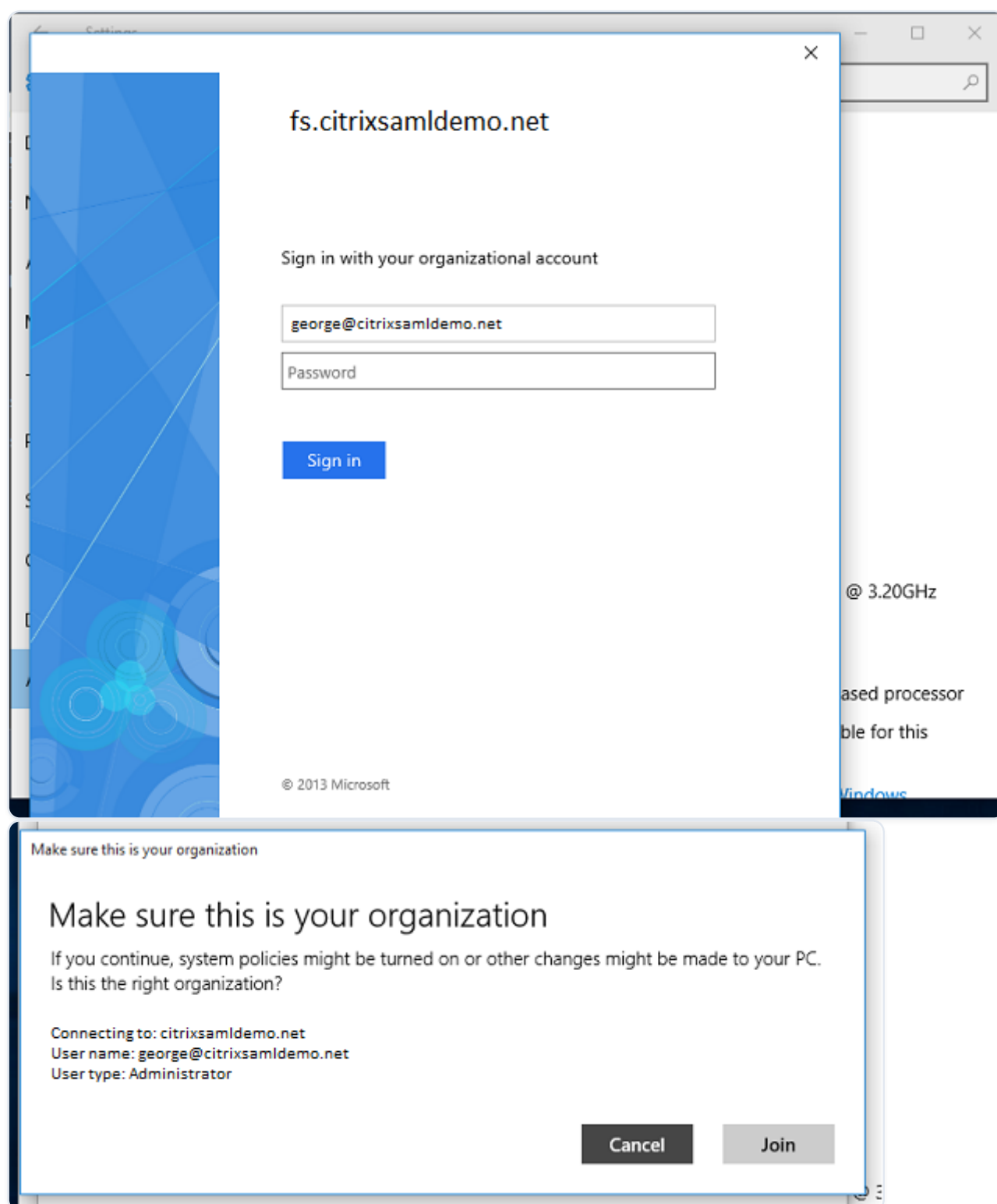
Which account should I use?

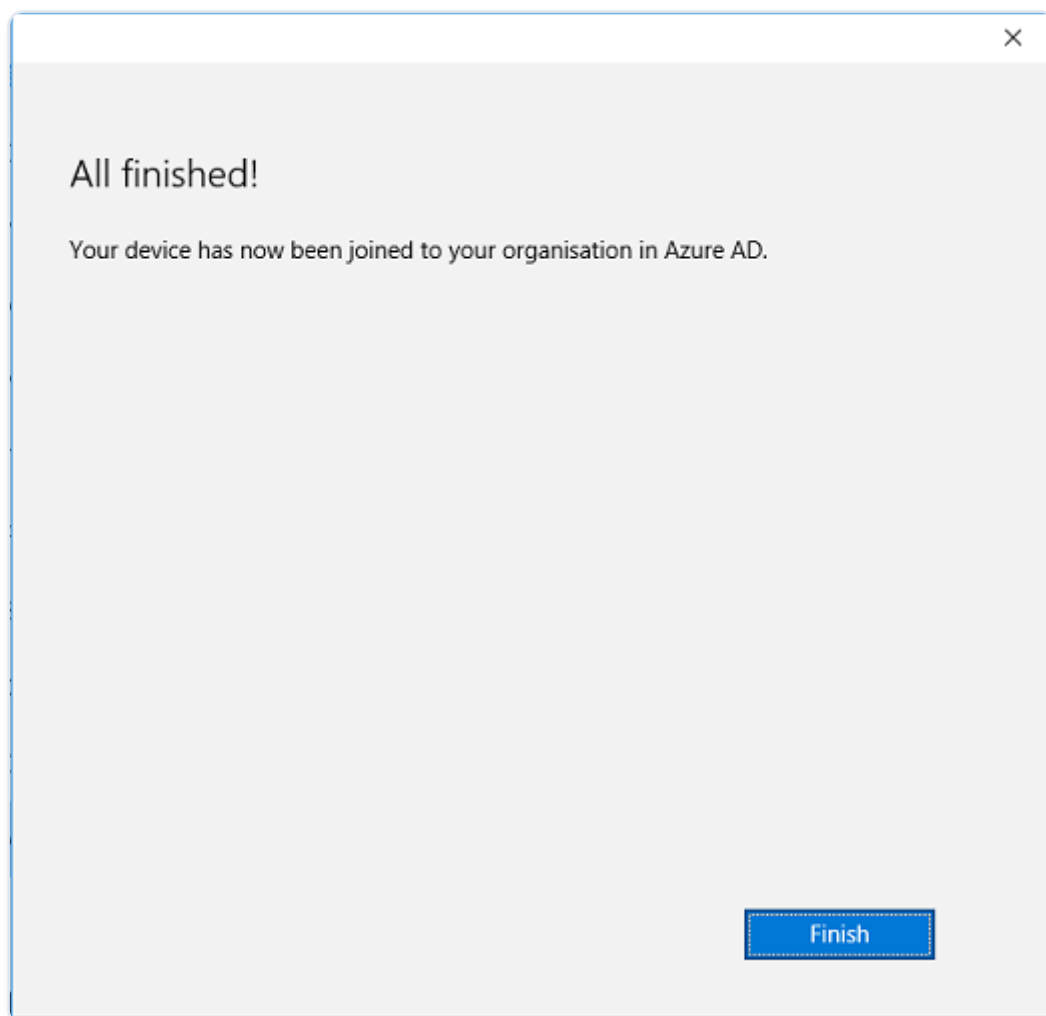
Sign in with the username and password you use with Office 365 (or other business services from Microsoft).

[Privacy statement](#)

Sign in      Back

UPNは、ADFSドメインコントローラーによって認識されるUPNと一致する必要があることに注意してください。



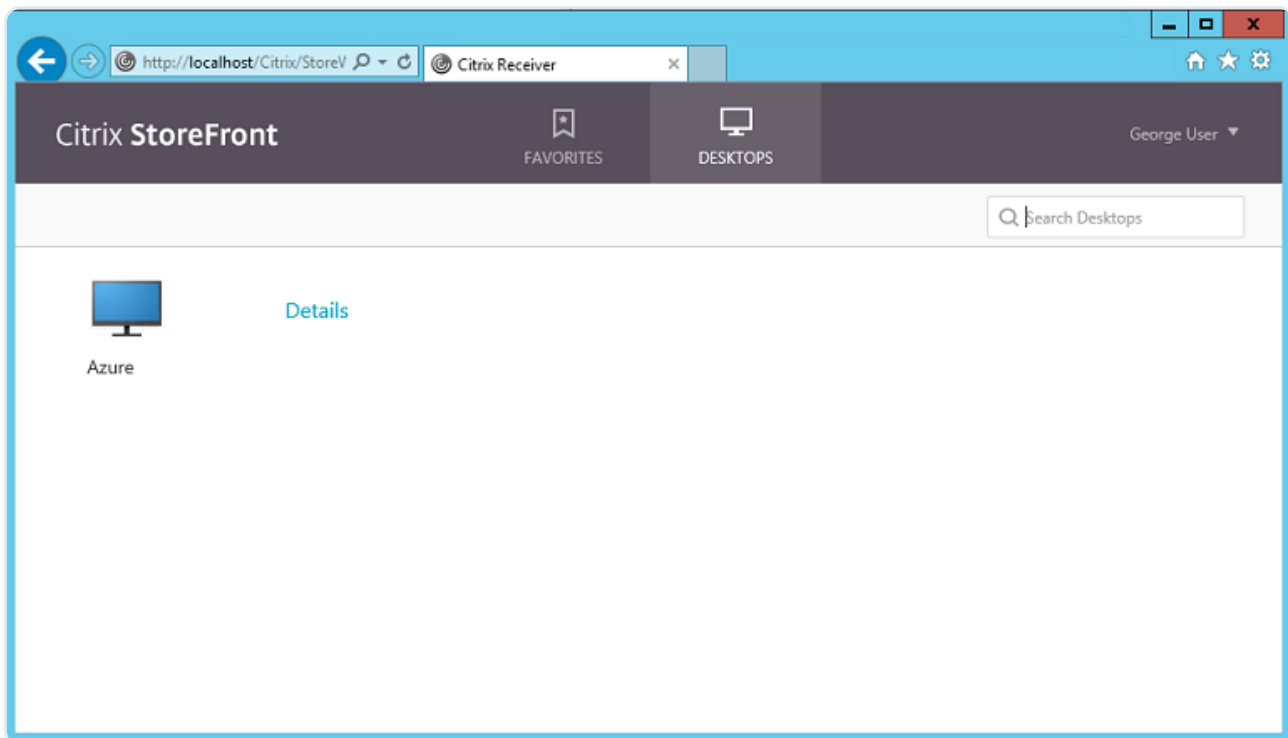


マシンを再起動し、ユーザーのメールアドレスを使用してログオンすることで、Azure AD参加が成功したことを確認します。ログオンしたら、Microsoft Edgeを起動して `<http://myapps.microsoft.com>` に接続します。ウェブサイトは自動的にシングルサインオンを使用するはずです。

## Citrix Virtual AppsまたはCitrix Virtual Desktopsをインストールする

通常の方法で、Citrix Virtual AppsまたはCitrix Virtual DesktopsのISOから直接、AzureにDelivery ControllerおよびVDA仮想マシンをインストールできます。

この例では、StoreFrontはDelivery Controllerと同じサーバーにインストールされています。VDAは、Machine Creation Servicesと統合せずに（オプションで構成可能ですが）、スタンドアロンのWindows 2012 R2 RDSワーカーとしてインストールされます。続行する前に、ユーザー `George@citrixsamdemo.net` がパスワードで認証できることを確認してください。



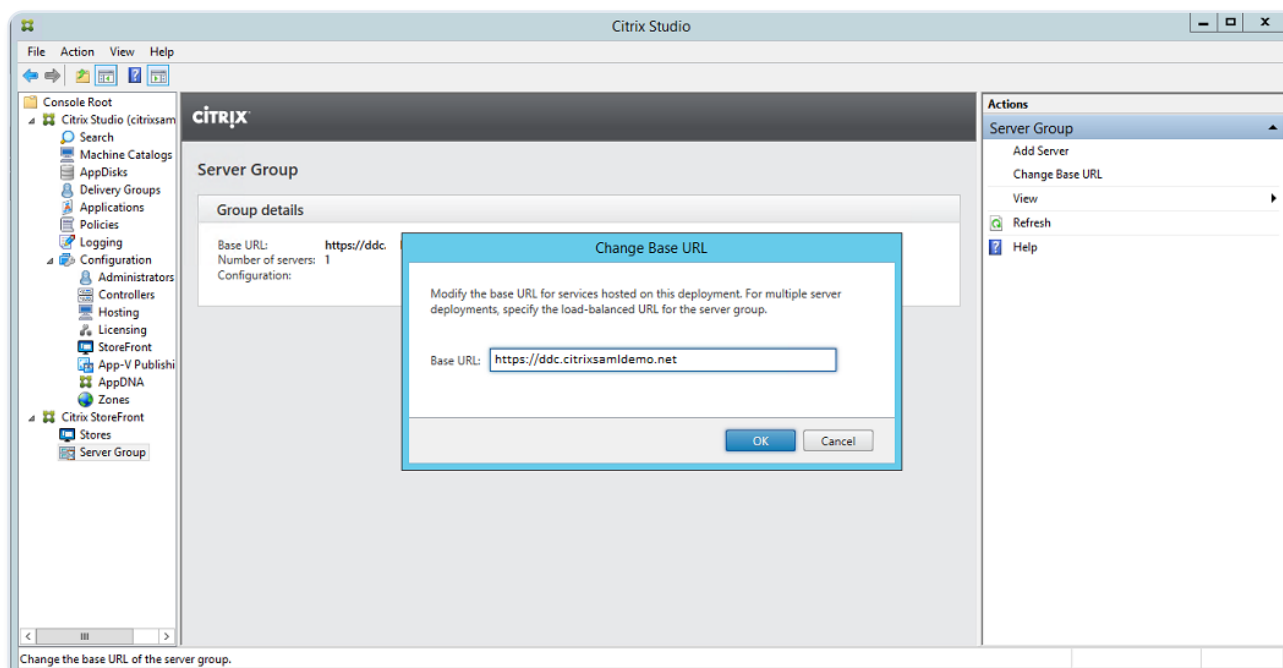
Controllerで**Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** PowerShellコマンドレットを実行して、StoreFront™がユーザーの資格情報なしで認証できるようにします。

## フェデレーション認証サービスをインストールする

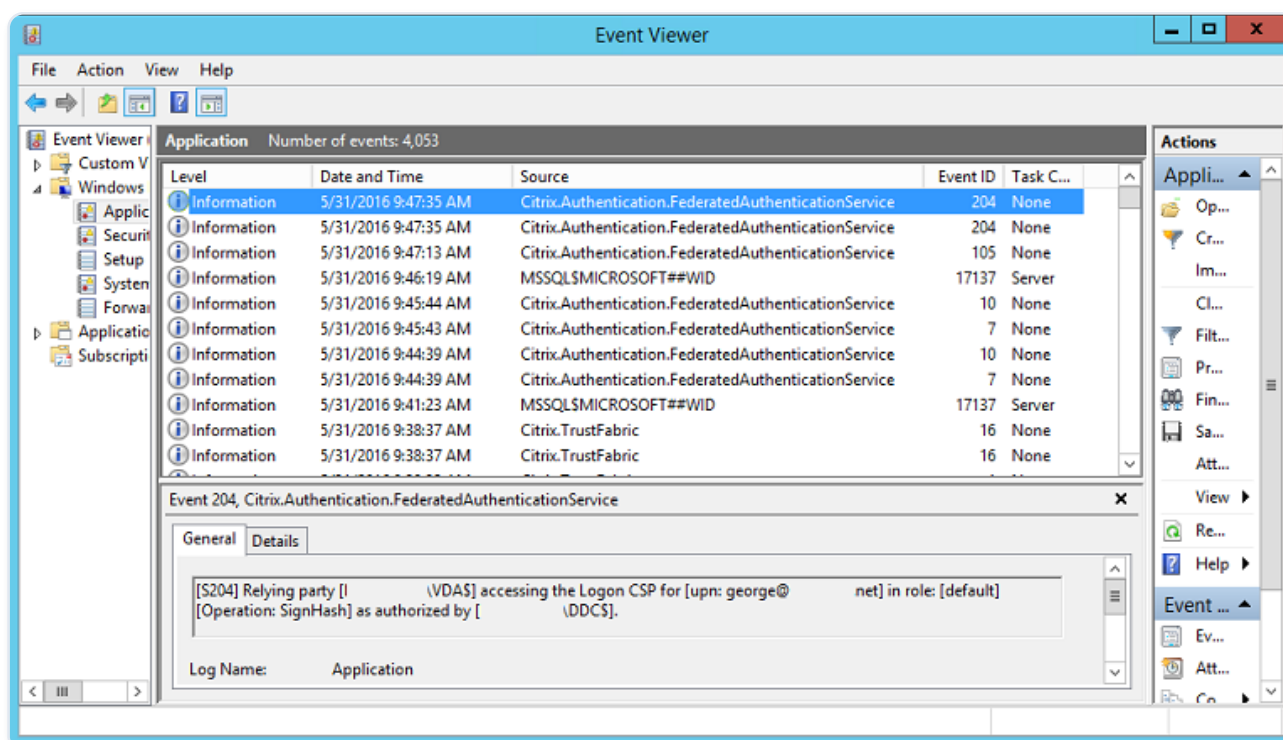
ADFSサーバーにFASをインストールし、Delivery Controllerが信頼されたStoreFrontとして機能するためのルールを構成します（この例では、StoreFrontはDelivery Controllerと同じVMにインストールされています）。[インストールと構成](#)を参照してください。

## StoreFrontを構成する

Delivery Controllerのコンピューター証明書を要求し、ポート443のIISバインディングを設定し、StoreFrontのベースアドレスをhttps:に変更して、IISとStoreFrontがHTTPSを使用するように構成します。

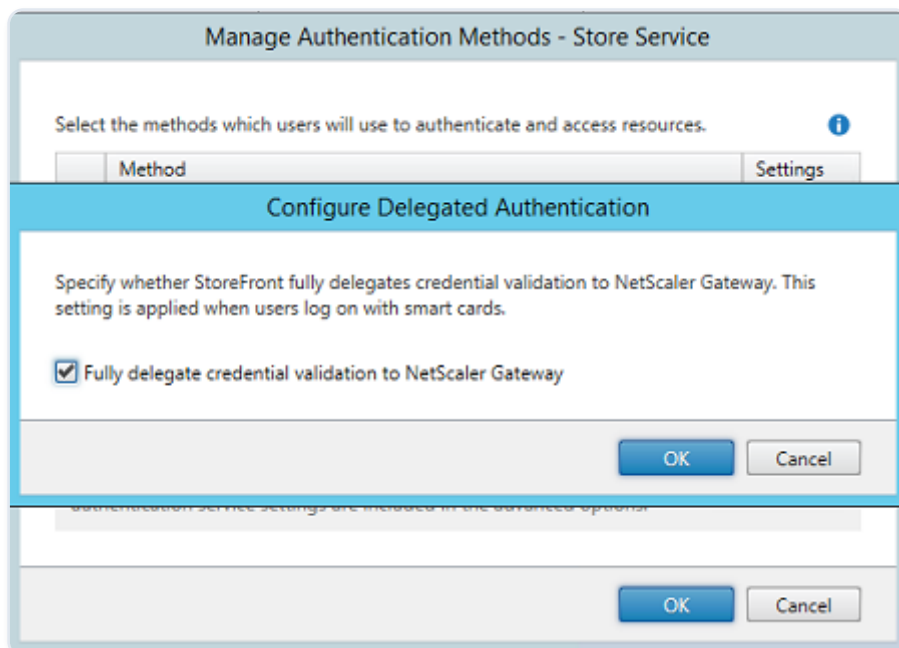


StoreFrontがFASサーバーを使用するように構成し（インストールと構成のPowerShellスクリプトを使用）、Azure内で内部的にテストし、FASサーバーのイベントビューアーを確認してログオンがFASを使用していることを確認します。

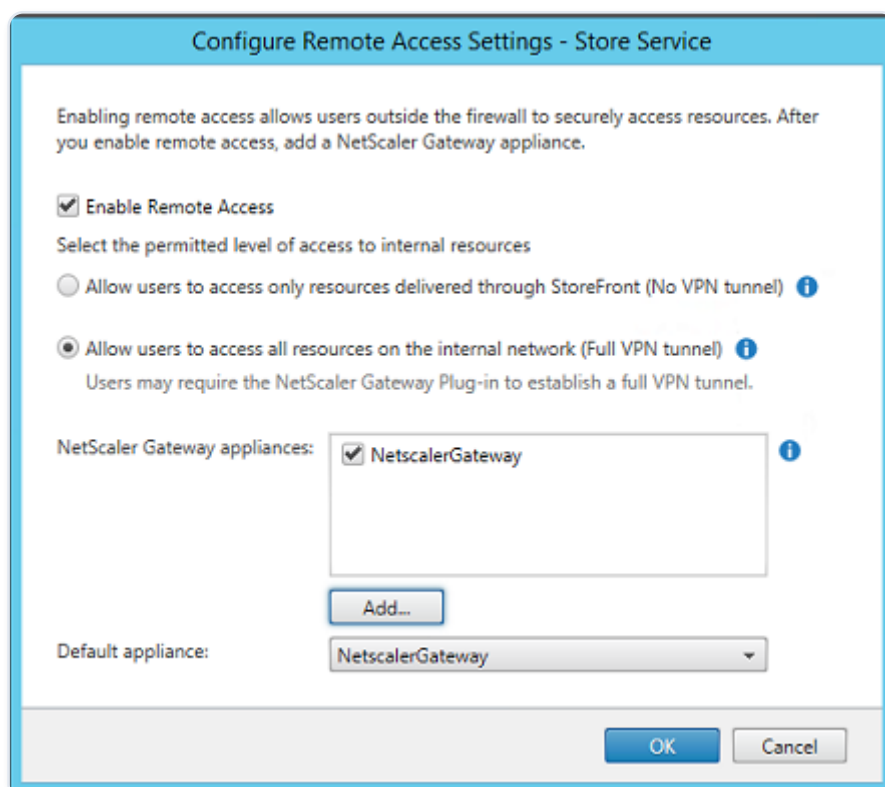


## StoreFrontがCitrix Gatewayを使用するように構成する

StoreFront管理コンソールの認証方法の管理GUIを使用して、StoreFrontがCitrix Gatewayを使用して認証を実行するように構成します。

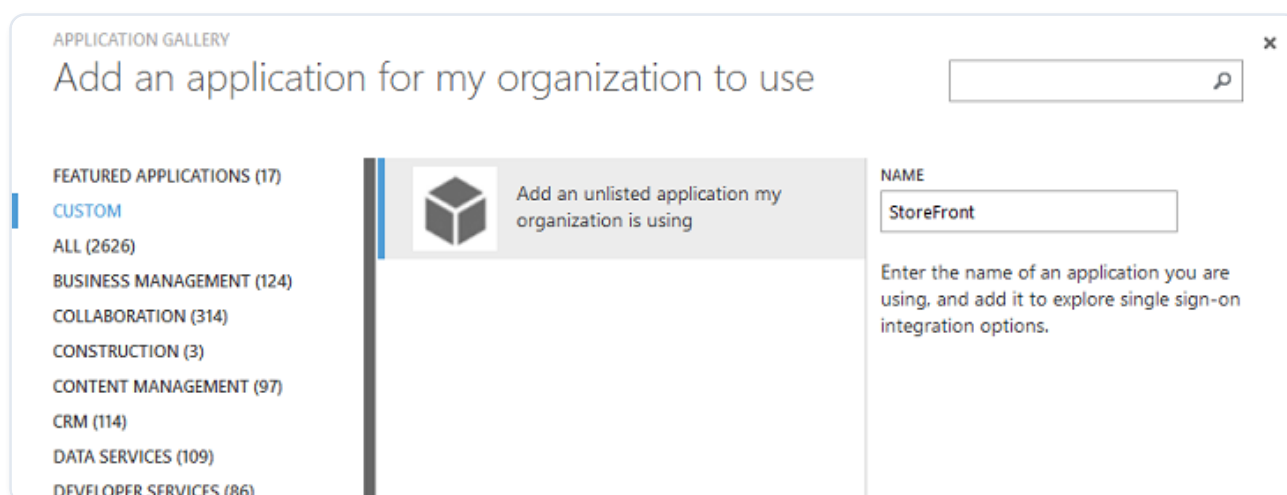


Citrix Gateway認証オプションを統合するには、Secure Ticket Authority (STA) を構成し、Citrix Gatewayアドレスを構成します。



## StoreFrontへのシングルサインオン用に新しいAzure ADアプリケーションを構成する

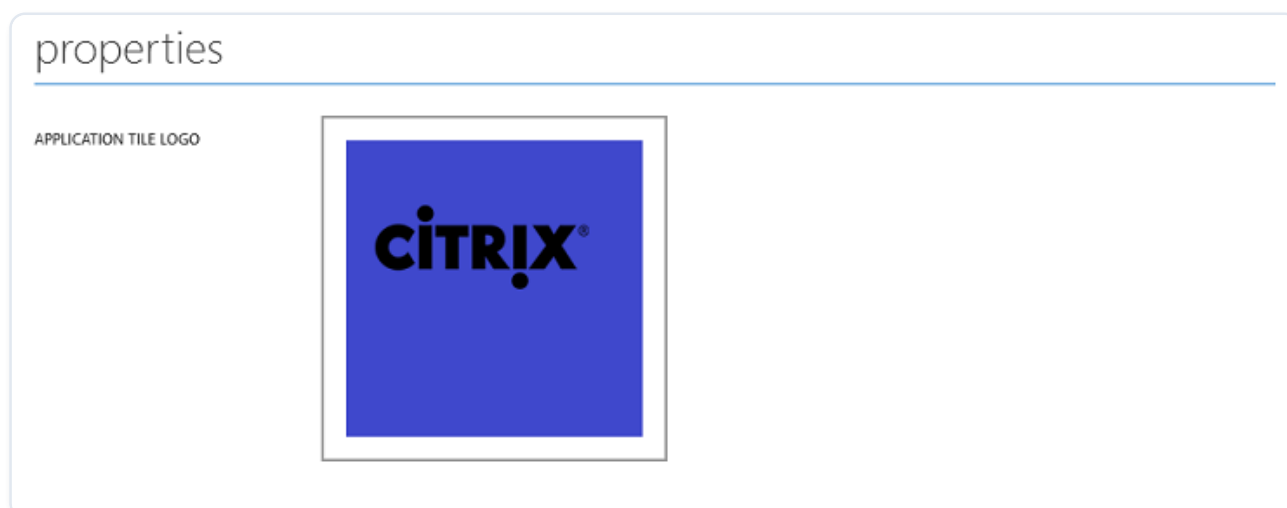
このセクションでは、現在Azure Active Directory Premiumサブスクリプションを必要とするAzure AD SAML 2.0シングルサインオン機能を使用します。Azure AD管理ツールで、**新しいアプリケーション**を選択し、**ギャラリーからアプリケーションを追加**を選択します。



「カスタム > 組織が使用している一覧にないアプリケーションを追加」を選択して、ユーザー用の新しいカスタムアプリケーションを作成します。

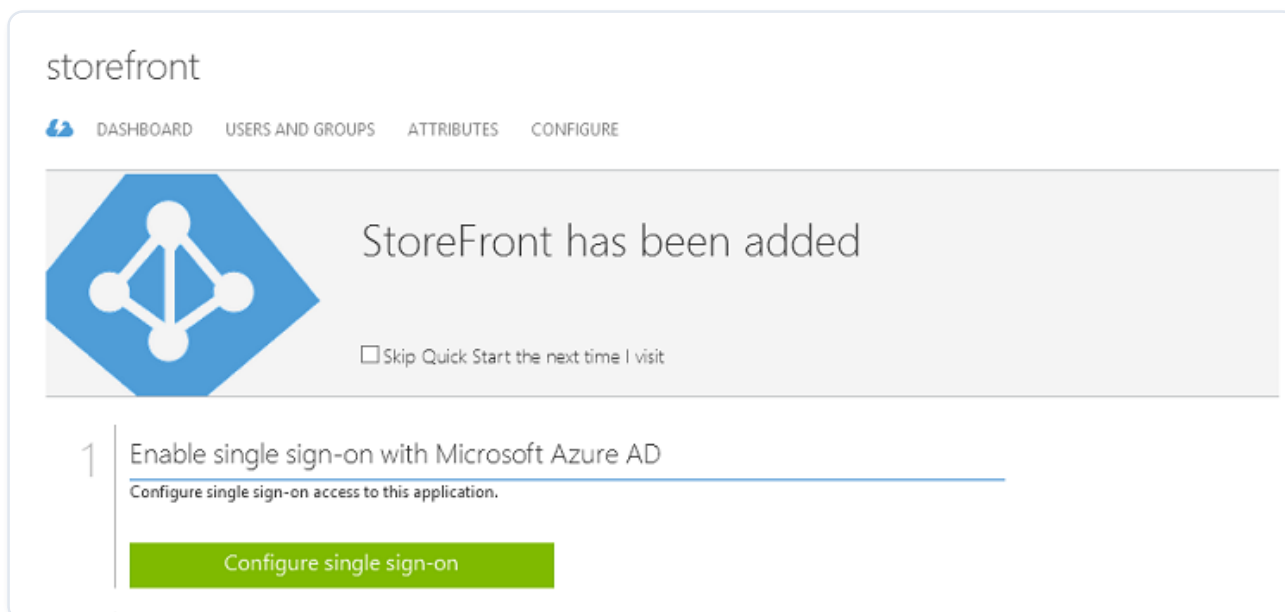
## アイコンの構成

215 x 215ピクセルの画像を作成し、CONFIGUREページにアップロードして、アプリケーションのアイコンとして使用します。

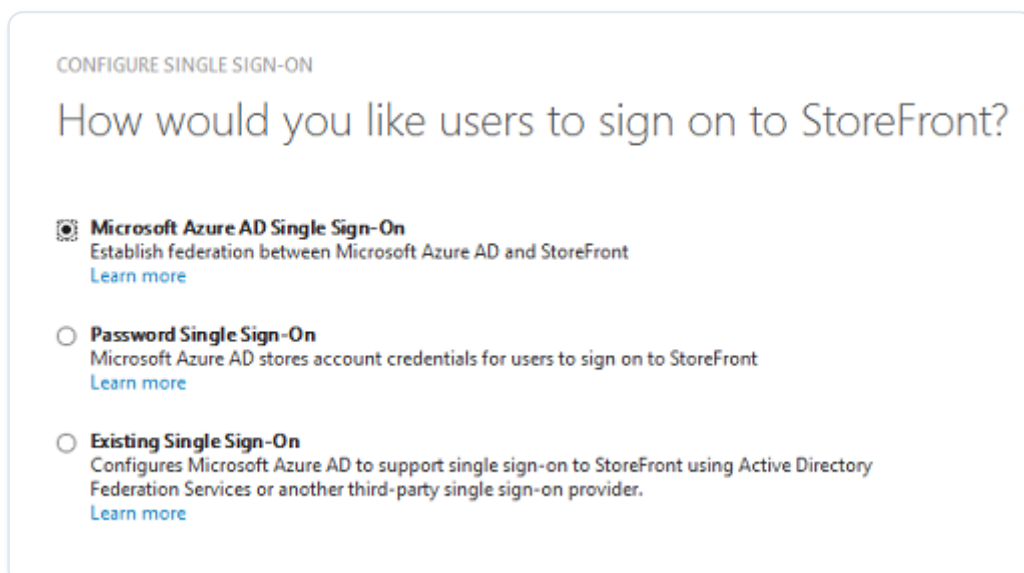


## SAML認証の構成

アプリケーションダッシュボードの概要ページに戻り、「シングルサインオンの構成」を選択します。



この展開では、**Microsoft Azure AD シングルサインオン**に対応するSAML 2.0認証を使用します。



識別子は任意の文字列にできます（Citrix Gatewayに提供される構成と一致する必要があります）。この例では、**応答URL**はCitrix Gatewayサーバー上の `/cgi/samlauth` です。

CONFIGURE SINGLE SIGN-ON

## Configure App Settings

Enter the settings of AzureStoreFront application below. [Learn more](#)

IDENTIFIER ?

`https://ns.citrixsamldemo.net/Citrix/StoreFront` ✓

REPLY URL ?

`https://ns.citrixsamldemo.net/cgi/samlauth` ✓

☐ Show advanced settings (optional).

☐ Configure the certificate used for federated single sign-on (optional).

次のページには、Citrix GatewayをAzure ADへの証明書利用者として構成するために使用される情報が含まれています。

CONFIGURE SINGLE SIGN-ON

## Configure single sign-on at AzureStoreFront

To accept the SAML token issued by Azure Active Directory, your application will need the information below. Refer to your application's SAML documentation or source code for details.

- The following certificate will be used for federated single sign-on:  
Thumbprint: 8D1E02EBF7C111EDDBBD325F526053BA9626A73B  
Expiry: 05/31/2018 11:06:20 UTC  
  
[Download Certificate \(Base 64 - most common\)](#) 
  
[Download Certificate \(Raw\)](#) 
  
[Download Metadata \(XML\)](#) 
- Configure the certificate and values in AzureStoreFront

ISSUER URL

`https://sts.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e/`

SINGLE SIGN-ON SERVICE URL

`https://login.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e`

SINGLE SIGN-OUT SERVICE URL

`https://login.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e`

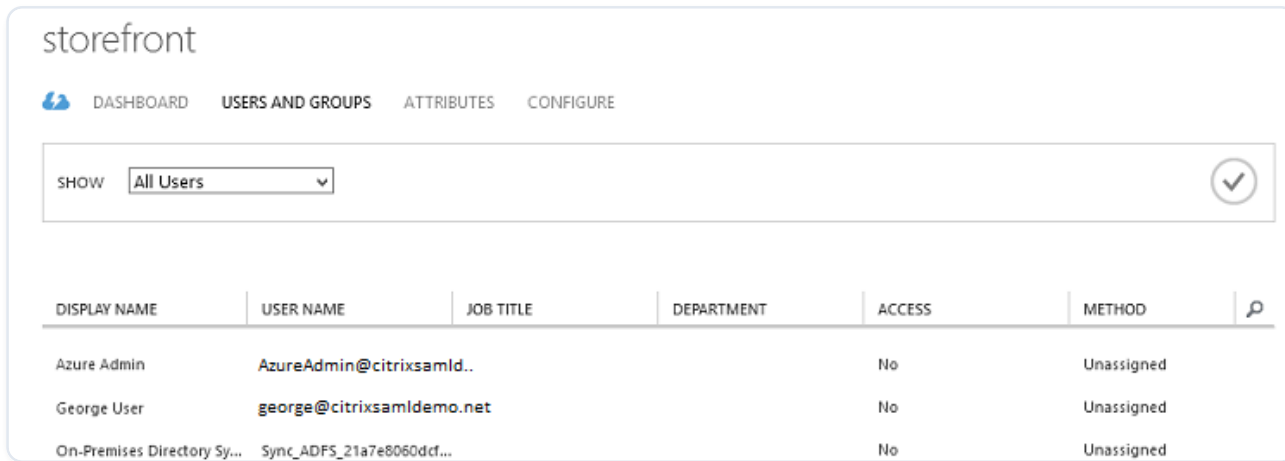
☐ Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate to start working for this application.




Base 64の信頼された署名証明書をダウンロードし、サインオンURLとサインアウトURLをコピーします。これらは後でCitrix Gatewayの構成画面に貼り付けます。

## アプリケーションをユーザーに割り当てる

最終ステップは、アプリケーションを有効にして、ユーザーの「myapps.microsoft.com」コントロールページに表示されるようにすることです。これは「USERS AND GROUPS」ページで行います。Azure AD Connectによって同期されたドメインユーザーアカウントにアクセスを割り当てます。他のアカウントも使用できますが、それらは<user>@<domain>パターンに準拠していないため、明示的にマッピングする必要があります。



storefront

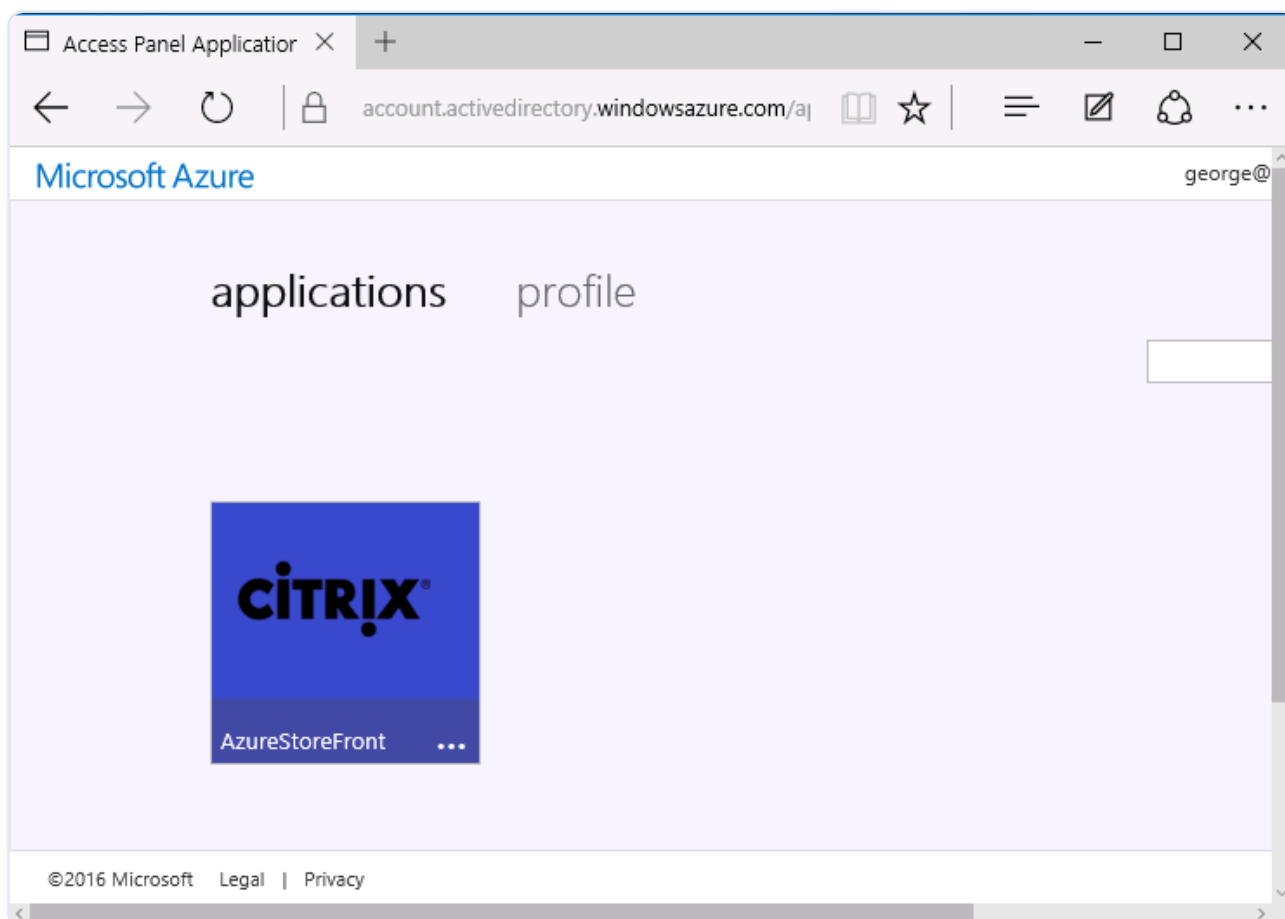
DASHBOARD USERS AND GROUPS ATTRIBUTES CONFIGURE

SHOW All Users

| DISPLAY NAME                | USER NAME                 | JOB TITLE | DEPARTMENT | ACCESS | METHOD     |  |
|-----------------------------|---------------------------|-----------|------------|--------|------------|--|
| Azure Admin                 | AzureAdmin@citrixsamld..  |           |            | No     | Unassigned |  |
| George User                 | george@citrixsamldemo.net |           |            | No     | Unassigned |  |
| On-Premises Directory Sy... | Sync_ADFS_21a7e8060dcf... |           |            | No     | Unassigned |  |

## MyAppsページ

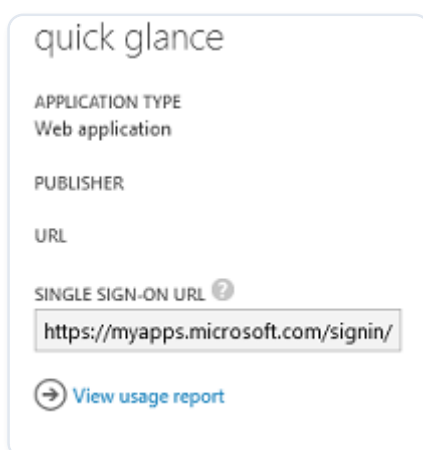
アプリケーションが構成されると、ユーザーが <https://myapps.microsoft.com> にアクセスしたときに、Azureアプリケーションのユーザーリストに表示されます。



Azure ADに参加している場合、Windows 10はログオンしたユーザーに対してAzureアプリケーションへのシングルサインオンをサポートします。アイコンをクリックすると、ブラウザは以前に構成されたSAML cgi/samlauth Webページに移動します。

## シングルサインオンURL

Azure ADダッシュボードのアプリケーションに戻ります。アプリケーションで利用可能なシングルサインオンURLが作成されています。このURLは、Webブラウザのリンクを提供したり、ユーザーをStoreFrontに直接誘導するスタートメニューのショートカットを作成したりするために使用されます。



このURLをWebブラウザに貼り付けて、Azure ADによって以前に構成されたCitrix Gateway cgi/samlauth Webページにリダイレクトされることを確認します。これは、割り当てられたユーザーに対してのみ機能し、Windows 10 Azure AD参加ログオンセッションに対してのみシングルサインオンを提供します。（他のユーザーはAzure AD資格情報の入力を求められます。）

## Citrix Gatewayのインストールと構成

展開にリモートアクセスするために、この例ではNetScaler（現在はCitrix Gateway）を実行する別のVMを使用します。これはAzure Storeから購入できます。この例では、NetScaler 11.0の「Bring your own License」バージョンを使用します。



NetScaler® VMにログオンし、Webブラウザを内部IPアドレスに向け、ユーザーが認証したときに指定された資格情報を使用します。Azure AD VMでは、nsrootユーザーのパスワードを変更する必要があることに注意してください。

ライセンスを追加し、各ライセンスファイルの追加後に再起動を選択し、DNSリゾルバーをMicrosoftドメインコントローラーに向けます。

## Citrix Virtual Apps and Desktops セットアップウィザードを実行する

この例では、SAML を使用しないシンプルな StoreFront 統合を構成することから始めます。その展開が機能した後、SAML ログオンポリシーを追加します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-install-ns-xaxd-setup.png)

標準の Citrix Gateway StoreFront 設定を選択します。Microsoft Azure で使用する場合、この例ではポート 443 ではなくポート 4433 を構成します。または、Citrix Gateway 管理 Web サイトをポート転送または再マッピングすることもできます。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-install-ns-xaxd-port.png)

簡素化のため、この例ではファイルに保存されている既存のサーバー証明書と秘密鍵をアップロードします。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-install-ns-xaxd-server-cert.png)

## AD アカウント管理のためにドメインコントローラーを構成する

ドメインコントローラーはアカウント解決に使用されるため、その IP アドレスをプライマリ認証方法に追加します。ダイアログボックスの各フィールドで期待される形式に注意してください。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-install-ns-dc.png)

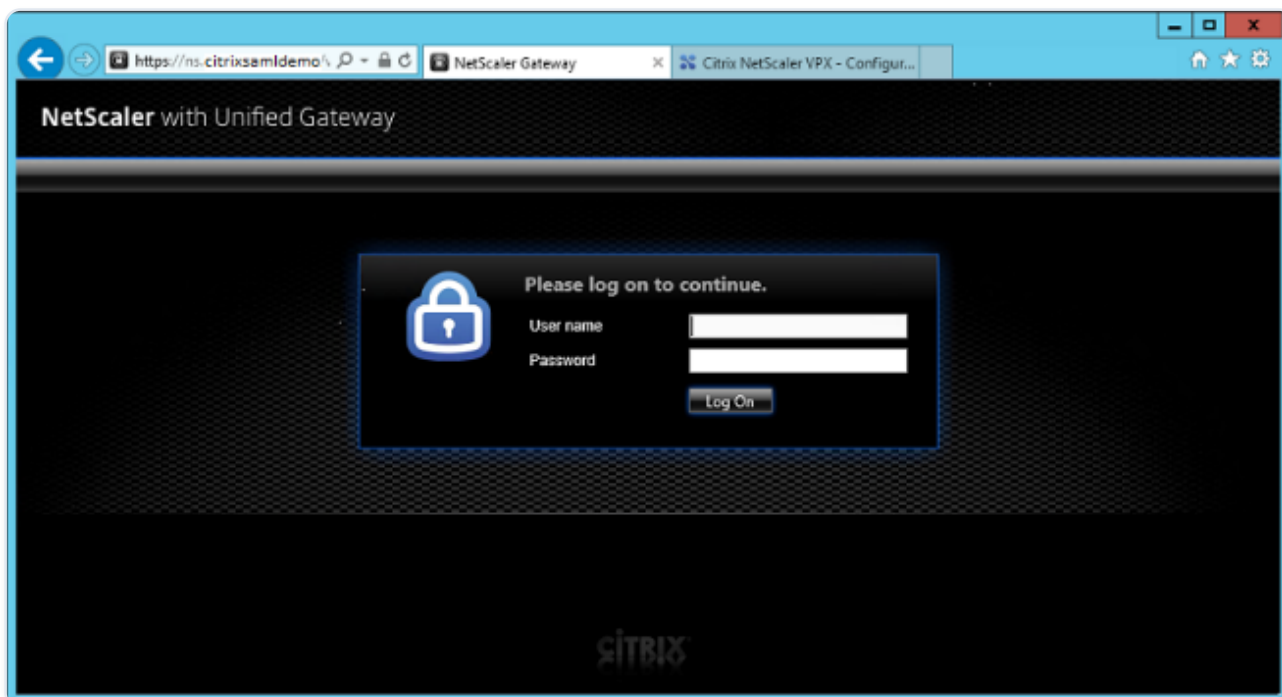
## StoreFront アドレスを構成する

この例では、StoreFront は HTTPS を使用して構成されているため、SSL プロトコルオプションを選択します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-azure-config-sf-address-ssl.png)

## Citrix Gateway の展開を確認する

Citrix Gateway に接続し、ユーザー名とパスワードで認証と起動が成功することを確認します。



## Citrix Gateway SAML認証サポートを有効にする

StoreFrontでSAMLを使用することは、他のWebサイトでSAMLを使用することと似ています。新しいSAMLポリシーを、**NS\_TRUE**の式で追加します。

以前にAzure ADから取得した情報を使用して、新しいSAML IdPサーバーを構成します。

### Create Authentication SAML Server

### Create Authentication SAML Server

Name\*

Authentication Type

SAML

IDP Certificate Name\*

Redirect URL\*

Single Logout URL

User Field

Signing Certificate Name

Issuer Name

Reject Unsigned Assertion\*

SAML Binding\*

Default Authentication Group

Skew Time(mins)

5

Two Factor

☐ ON ☒ OFF

Assertion Consumer Service Index

Attribute Consuming Service Index

Requested Authentication Context\*

Authentication Class Types



Signature Algorithm\*

☐ RSA-SHA1 ☒ RSA-SHA256

Digest Method\*

☐ SHA1 ☒ SHA256

☐ Send Thumbprint

☒ Enforce Username

Attribute 1

Attribute 3

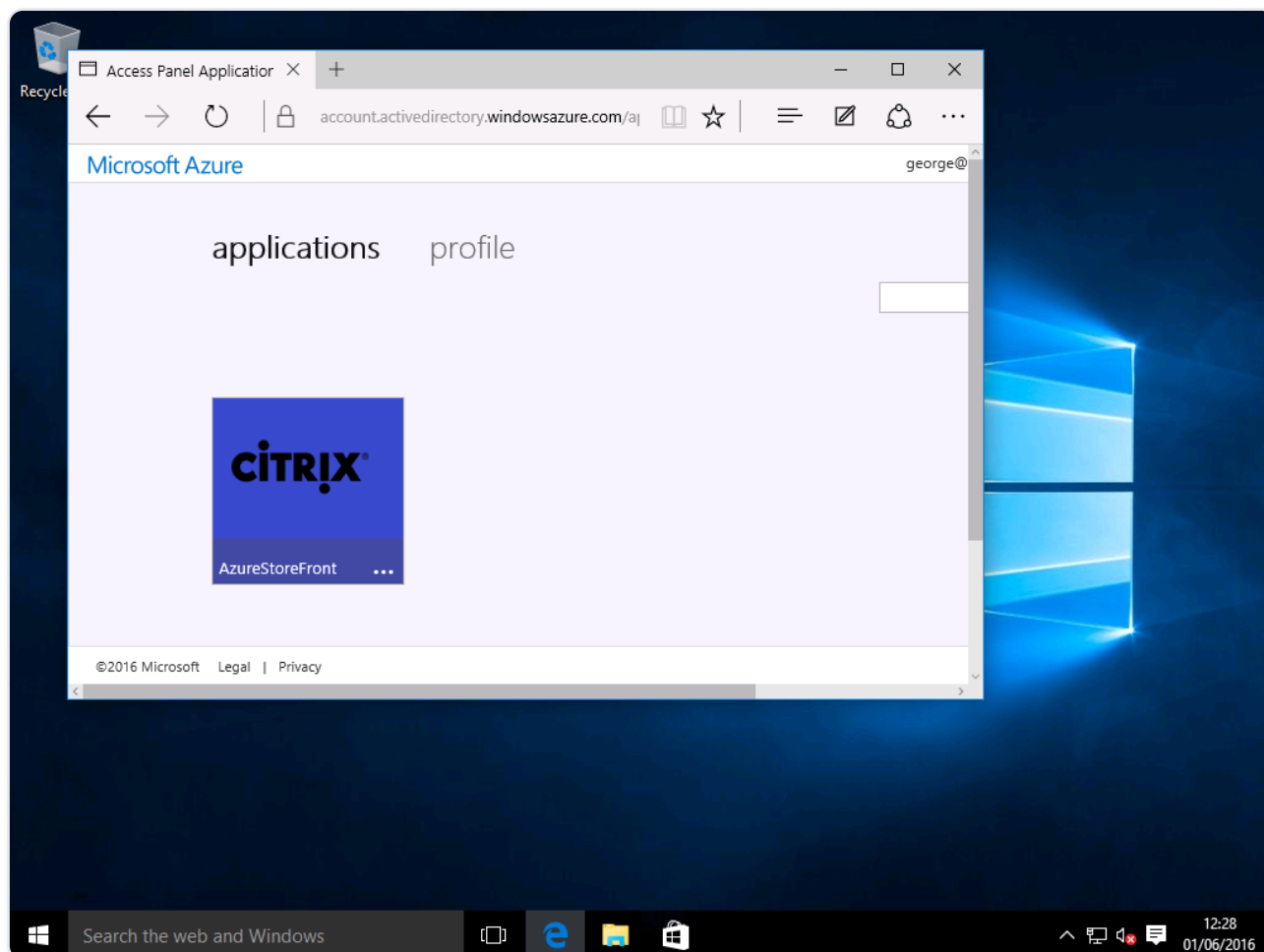
Attribute 5

Attribute 7

## エンドツーエンドシステムを検証する

Azure ADに登録されているアカウントを使用して、Azure ADに参加しているWindows 10デスクトップにログオンします。Microsoft Edgeを起動し、`<https://myapps.microsoft.com>` に接続します。

Webブラウザには、ユーザーのAzure ADアプリケーションが表示されるはずですが、



アイコンをクリックすると、認証されたStoreFrontサーバーにリダイレクトされることを確認します。

同様に、シングルサインオンURLを使用した直接接続とCitrix Gatewayサイトへの直接接続が、Microsoft Azureにリダイレクトされ、元に戻ることを確認します。

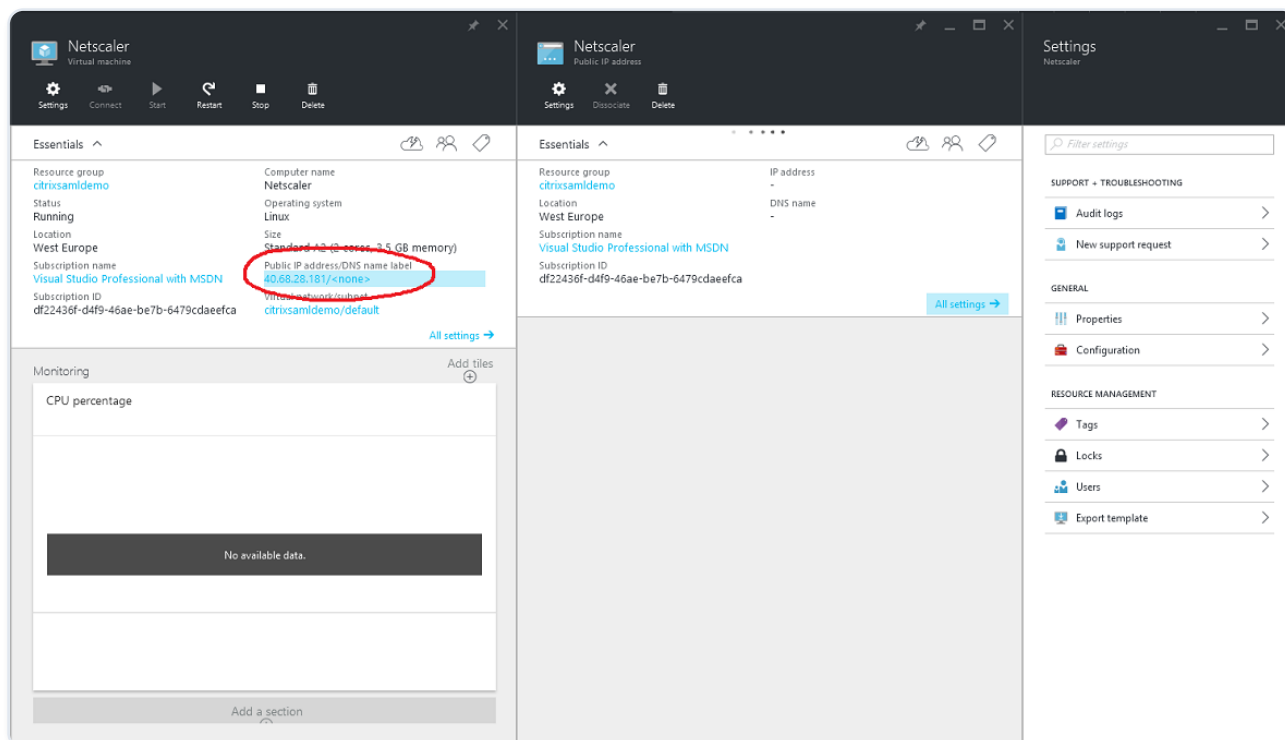
最後に、Azure ADに参加していないマシンも同じURLで機能することを確認します（ただし、最初の接続ではAzure ADへの単一の明示的なサインオンが発生します）。

## 付録

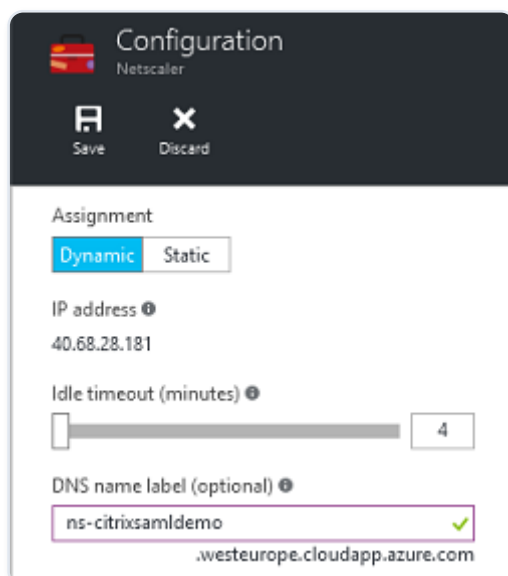
AzureでVMをセットアップする際には、以下の標準オプションを構成する必要があります。

### パブリックIPアドレスとDNSアドレスを提供する

Azureは、すべてのVMに内部サブネット上のIPアドレス（この例では10.\*.\*)を割り当てます。デフォルトでは、パブリックIPアドレスも提供され、動的に更新されるDNSラベルによって参照できます。



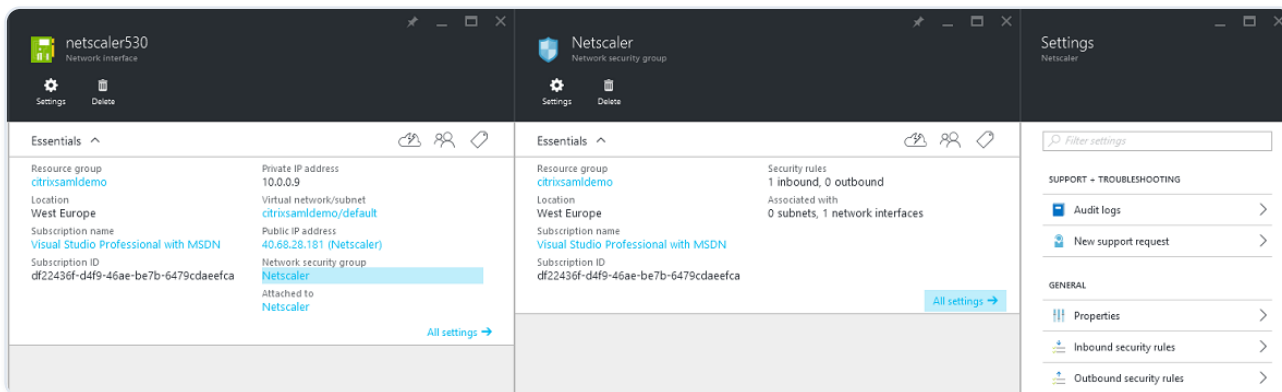
**Public IP address/DNS name labelのConfiguration**を選択します。VMのパブリックDNSアドレスを選択します。これは、他のDNSゾーンファイルでCNAME参照として使用でき、IPアドレスが再割り当てされた場合でも、すべてのDNSレコードがVMを正しく指し続けることを保証します。



## ファイアウォールルール（セキュリティグループ）を設定する

クラウド内の各VMには、セキュリティグループとして知られる一連のファイアウォールルールが自動的に適用されます。セキュリティグループは、パブリックIPアドレスからプライベートIPアドレスに転送されるトラフィックを制御します。デフォルトでは、AzureはRDPをすべてのVMに転送することを許可します。Citrix GatewayおよびADFSサーバーもTLSトラフィック（443）を転送する必要があります。

VMの**Network Interfaces**を開き、**Network Security Group**ラベルをクリックします。適切なネットワークトラフィックを許可するように**Inbound security rules**を設定します。



## 関連情報

- [インストールと構成](#)は、FASのインストールと構成に関する主要なリファレンスです。
- 一般的なFAS展開は、[展開アーキテクチャ](#)の記事にまとめられています。
- 「ハウツー」記事は、[高度な構成](#)の記事で紹介されています。

# 高度な構成

このセクションのハウツー記事では、Federated Authentication Service (FAS) の高度な構成と管理のガイダンスを提供します。

## 関連情報

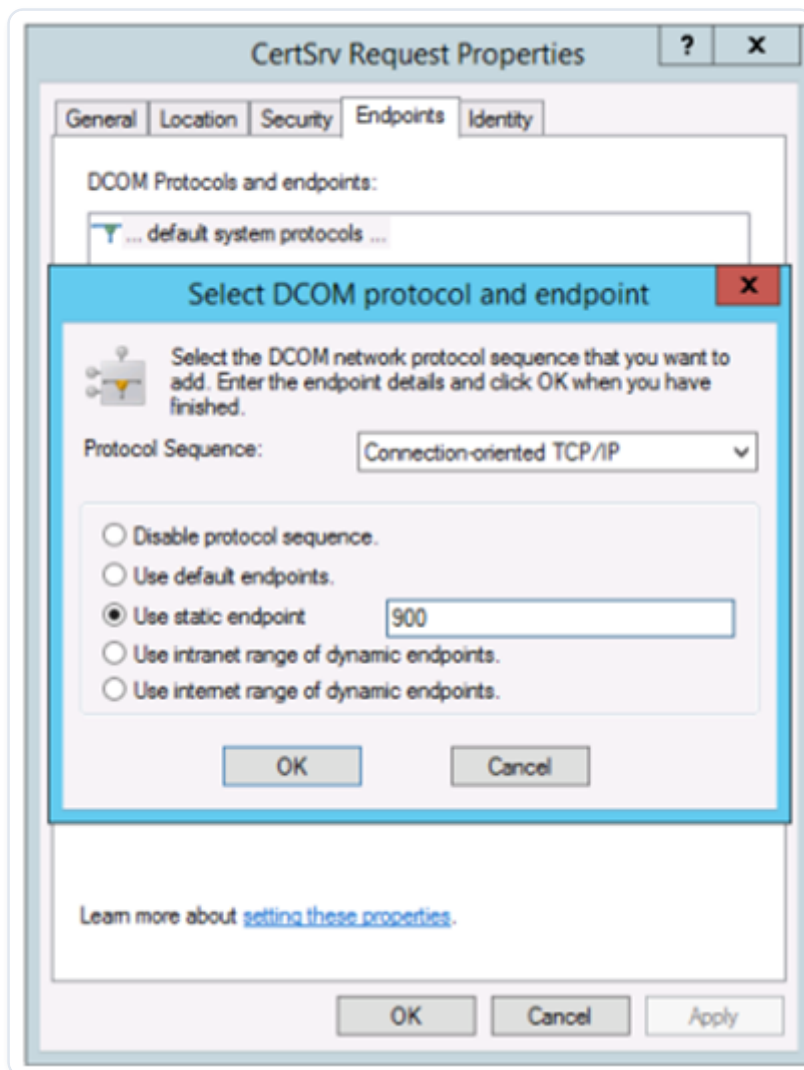
- FAS のインストールと初期設定の主要なリファレンスは、[インストールと構成](#) の記事です。
- [展開アーキテクチャ](#) の記事では、主要な FAS アーキテクチャの概要と、より複雑なアーキテクチャに関する他の記事へのリンクを提供します。

## 証明機関の構成

この記事では、FAS管理コンソールでサポートされていない証明機関サーバーと統合するための、フェデレーション認証サービス (FAS) の高度な構成について説明します。手順では、FASが提供するPowerShell APIを使用します。この記事の手順を実行する前に、PowerShellの基本的な知識が必要です。

### TCPアクセス用にMicrosoft証明機関を構成する

デフォルトでは、Microsoft証明機関はアクセスにDCOMを使用します。これはファイアウォールセキュリティを実装する際に複雑さをもたらす可能性があるため、Microsoftは静的TCPポートに切り替えるための規定を設けています。Microsoft証明機関で、DCOM構成パネルを開き、「CertSrv Request」 DCOMアプリケーションのプロパティを編集します。



「エンドポイント」を変更して静的エンドポイントを選択し、TCPポート番号を指定します (上記の図では900)。

Microsoft証明機関を再起動し、証明書要求を送信します。 `netstat -a -n -b` を実行すると、certsrvがポート900でリッスンしていることが確認できます。

|               |              |      |           |
|---------------|--------------|------|-----------|
| TCP           | 0.0.0.0:636  | dc:0 | LISTENING |
| [lsass.exe]   |              |      |           |
| TCP           | 0.0.0.0:900  | dc:0 | LISTENING |
| [certsrv.exe] |              |      |           |
| TCP           | 0.0.0.0:3268 | dc:0 | LISTENING |
| [lsass.exe]   |              |      |           |
| TCP           | 0.0.0.0:3269 | dc:0 | LISTENING |

DCOMにはRPCポートを使用したネゴシエーション段階があるため、FASサーバー（または証明機関を使用する他のマシン）を構成する必要はありません。クライアントがDCOMを使用する必要がある場合、証明書サーバー上のDCOM RPCサービスに接続し、特定のDCOMサーバーへのアクセスを要求します。これによりポート900が開かれ、DCOMサーバーはFASサーバーに接続方法を指示します。

## ユーザー証明書を事前生成する

FASサーバー内でユーザー証明書が事前生成されると、ユーザーのログオン時間が大幅に改善されます。以下のセクションでは、単一または複数のFASサーバーでこれを実行する方法について説明します。

### Active Directoryユーザーのリストを取得する

次の例に示すように、ADをクエリし、ユーザーのリストをファイル（たとえば、.csvファイル）に保存することで、証明書の生成を改善できます。

```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users,
leave it blank to search all

$filename = "user_list.csv" # Filename to save

if ($searchbase -ne ""){

    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq
"true") } -SearchBase $searchbase -Properties UserPrincipalName | Select
UserPrincipalName | Export-Csv -NoTypeInfoation -Encoding utf8
-delimiter "," $filename

} else {

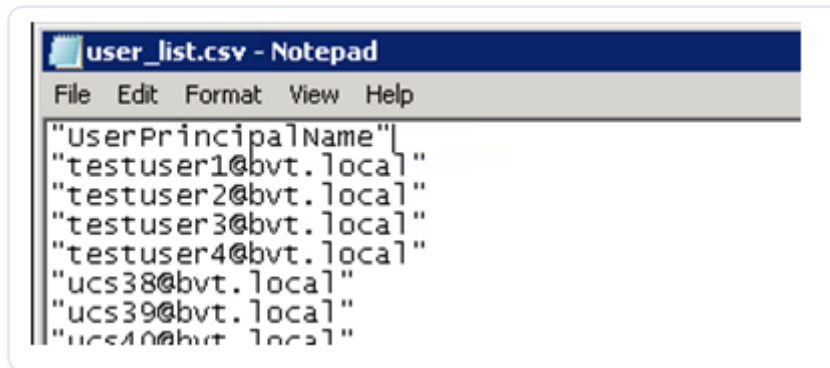
    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq
"true") } -Properties UserPrincipalName | Select UserPrincipalName |
Export-Csv -NoTypeInfoation -Encoding utf8 -delimiter "," $filename

}
```

Get-ADUserは、ユーザーのリストをクエリするための標準的なコマンドレットです。上記の例には、UserPrincipalNameを持ち、アカウントステータスが「有効」であるユーザーのみをリストするためのフィルター引数が含まれています。

SearchBase引数は、ADのどの部分でユーザーを検索するかを絞り込みます。AD内のすべてのユーザーを含めたい場合は、これを省略できます。注：このクエリは多数のユーザーを返す可能性があります。

CSVは次のようになります。



## FASサーバー

次のPowerShellスクリプトは、以前に生成されたユーザーリストを取得し、ユーザー証明書のリストを作成します。

```
Add-PSSnapin Citrix.A*

$csv = "user_list.csv"

$rule = "default" # rule/role in your admin console

$users = Import-Csv -encoding utf8 $csv

foreach ( $user in $users )
{
    $server = Get-FasServerForUser -UserPrincipalNames
    $user.UserPrincipalName

    if( $server.Server -ne $NULL) {

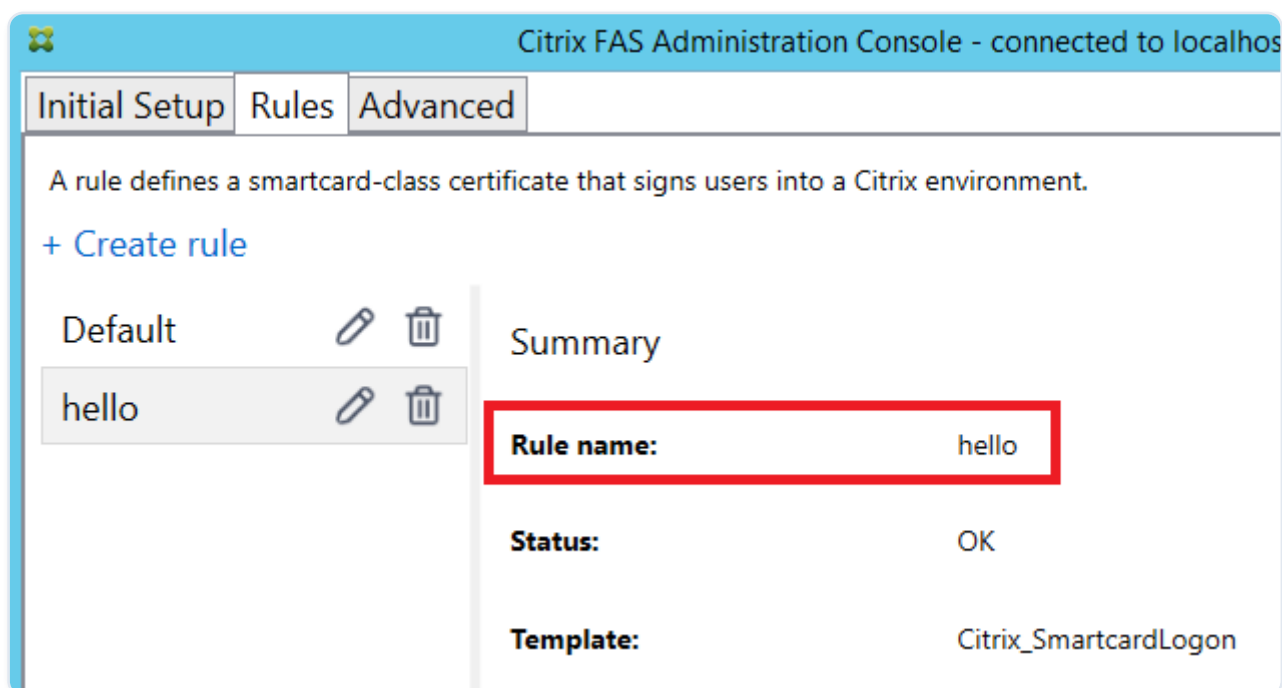
        New-FasUserCertificate -Address $server.Server -UserPrincipalName
        $user.UserPrincipalName -CertificateDefinition $rule"_Definition" -Rule
        $rule

    }
}
```

```
if( $server.Failover -ne $NULL) {  
  
    New-FasUserCertificate -Address $server.Failover  
-UserPrincipalName $user.UserPrincipalName -CertificateDefinition  
$rule"_Definition" -Rule $rule  
  
}  
  
}
```

複数のFASサーバーがある場合、特定のユーザーの証明書は2回生成されます。1つはメインサーバーで、もう1つはフェールオーバーサーバーで生成されます。

上記のスクリプトは、「default」という名前のルールに対応しています。異なるルール名（例：「hello」）を使用する場合は、スクリプト内の\$rule変数を変更してください。

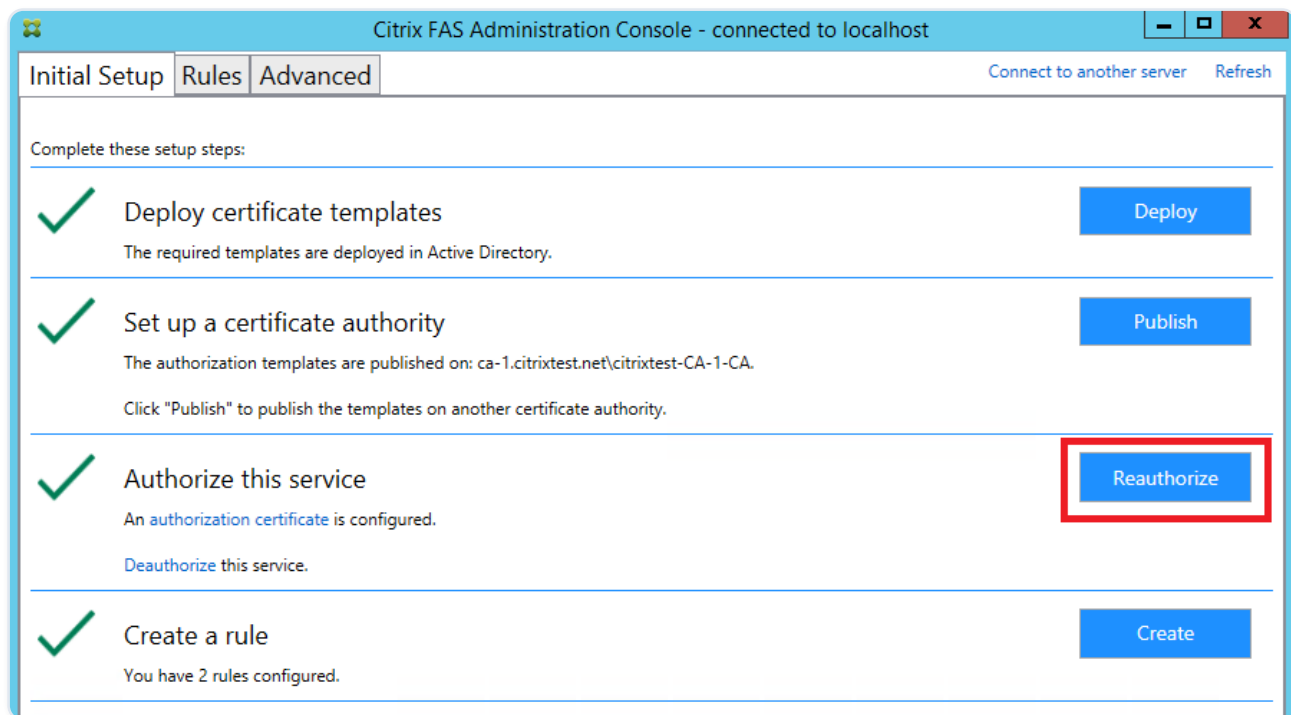


## 登録機関証明書の更新

複数のFASサーバーが使用されている場合、ログオンしているユーザーに影響を与えることなく、FAS承認証明書を更新できます。

### 注：

GUIを使用してFASを再承認することもできます。



次のシーケンスを完了します。

1. 新しい承認証明書を作成します: `New-FasAuthorizationCertificate`
2. 新しい承認証明書のGUIDをメモします。これは、`Get-FasAuthorizationCertificate` によって返されます。
3. FASサーバーをメンテナンスモードにします: `Set-FasServer -Address <FAS server> -MaintenanceMode $true`
4. 新しい承認証明書を交換します: `Set-FasCertificateDefinition - AuthorizationCertificate <GUID>`
5. FASサーバーをメンテナンスモードから解除します: `Set-FasServer -Address <FAS server> -MaintenanceMode $false`
6. 古い承認証明書を削除します: `Remove-FasAuthorizationCertificate`

## 関連情報

- [インストールと構成](#)の記事は、FASのインストールと構成に関する主要なリファレンスです。
- 一般的なフェデレーション認証サービス展開は、[展開アーキテクチャ](#)の記事にまとめられています。
- その他の「ハウツー」記事は、[高度な構成](#)の記事で紹介されています。

# 秘密キーの保護

## はじめに

秘密キーは、ネットワークサービスアカウントによって保存され、デフォルトでエクスポート不可としてマークされます。

秘密キーには、次の2種類があります。

- Citrix\_RegistrationAuthority証明書テンプレートからの、登録機関証明書に関連付けられた秘密キー。
- Citrix\_SmartcardLogon証明書テンプレートからの、ユーザー証明書に関連付けられた秘密キー。

実際には、2つの登録機関証明書があります。Citrix\_RegistrationAuthority\_ManualAuthorization（デフォルトで24時間有効）とCitrix\_RegistrationAuthority（デフォルトで2年間有効）です。

Federated Authentication Service (FAS) 管理コンソールの\*\* [Initial Setup] タブのステップ3で、[Authorize] \*\*をクリックすると、FASサーバーはキーペアを生成し、Citrix\_RegistrationAuthority\_ManualAuthorization証明書用の証明書署名要求を証明機関に送信します。これは一時的な証明書で、デフォルトで24時間有効です。証明機関はこの証明書を自動的に発行しません。発行は、証明機関で管理者が手動で承認する必要があります。証明書がFASサーバーに発行されると、FASはCitrix\_RegistrationAuthority\_ManualAuthorization証明書を使用して、Citrix\_RegistrationAuthority証明書（デフォルトで2年間有効）を自動的に取得します。FASサーバーは、Citrix\_RegistrationAuthority証明書を取得するとすぐに、Citrix\_RegistrationAuthority\_ManualAuthorizationの証明書とキーを削除します。

登録機関証明書に関連付けられた秘密キーは特に機密性が高く、登録機関証明書ポリシーにより、秘密キーを所有する者は、テンプレートで構成されたユーザーセットに対して証明書要求を発行できるためです。結果として、このキーを制御する者は、そのセット内の任意のユーザーとして環境に接続できます。

FASサーバーは、組織のセキュリティ要件に合った方法で秘密キーを保護するように構成できます。次のいずれかを使用します。

- 登録機関証明書とユーザー証明書の秘密キーの両方に、Microsoft Enhanced RSA and AES Cryptographic ProviderまたはMicrosoft Software Key Storage Providerを使用します。
- 登録機関証明書の秘密キーにはTrusted Platform Module (TPM) チップを備えたMicrosoft Platform Key Storage Providerを、ユーザー証明書の秘密キーにはMicrosoft Enhanced RSA

and AES Cryptographic ProviderまたはMicrosoft Software Key Storage Providerを使用します。

- 登録機関証明書とユーザー証明書の秘密キーの両方に、HSMデバイスを備えたHardware Security Module (HSM) ベンダーのCryptographic ServiceまたはKey Storage Providerを使用します。

## 秘密キーの構成設定

FASを3つのオプションのいずれかを使用するように構成します。テキストエディターを使用してCitrix.Authentication.FederatedAuthenticationService.exe.configファイルを編集します。ファイルのデフォルトの場所は、FASサーバーのProgram Files\Citrix\Federated Authentication Service フォルダー内です。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-privatekeys-config-file.png)

FAS は、サービス開始時にのみ構成ファイルを読み取ります。値が変更された場合、新しい設定を反映させるには FAS を再起動する必要があります。

Citrix.Authentication.FederatedAuthenticationService.exe.config ファイルで関連する値を次のように設定します。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (CAPI と CNG API を切り替えます)

| 値             | コメント            |
|---------------|-----------------|
| はい            | CAPI API を使用します |
| false (デフォルト) | CNG API を使用します  |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (使用するプロバイダーの名前)

| 値                                | コメント               |
|----------------------------------|--------------------|
| マイクロソフト強化RSAおよびAES暗号化プロバイダー      | デフォルトの CAPI プロバイダー |
| Microsoft ソフトウェア キー ストレージ プロバイダー | デフォルトのCNGプロバイダー    |

| 値                                  | コメント                                                                                                                                |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft プラットフォーム キー ストレージ プロバイダー | デフォルトのTPMプロバイダー。TPMはユーザーキーには推奨されません。登録機関キーにのみTPMを使用してください。FASサーバーを仮想化環境で実行する予定がある場合は、仮想化がサポートされているかどうかをTPMおよびハイパーバイザーベンダーに確認してください。 |
| HSM_Vendor CSP/キーストレージプロバイダー       | HSMベンダーによって提供されます。値はベンダーによって異なります。FASサーバーを仮想化環境で実行する予定がある場合は、仮想化がサポートされているかどうかをHSMベンダーに確認してください。                                    |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (CAPI APIの場合にのみ必須)

| 値  | コメント                                                                                                                                          |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 24 | デフォルト。Microsoft KeyContainerPermissionAccessEntry.ProviderType プロパティ PROV_RSA_AES 24 を参照します。CAPIでHSMを使用しており、HSMベンダーが別途指定しない限り、常に24である必要があります。 |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (FASが秘密鍵操作を実行する必要がある場合、ここで指定された値を使用します) 秘密鍵の「エクスポート可能」フラグを制御します。ハードウェアでサポートされている場合、TPMキーストレージの使用を許可します。

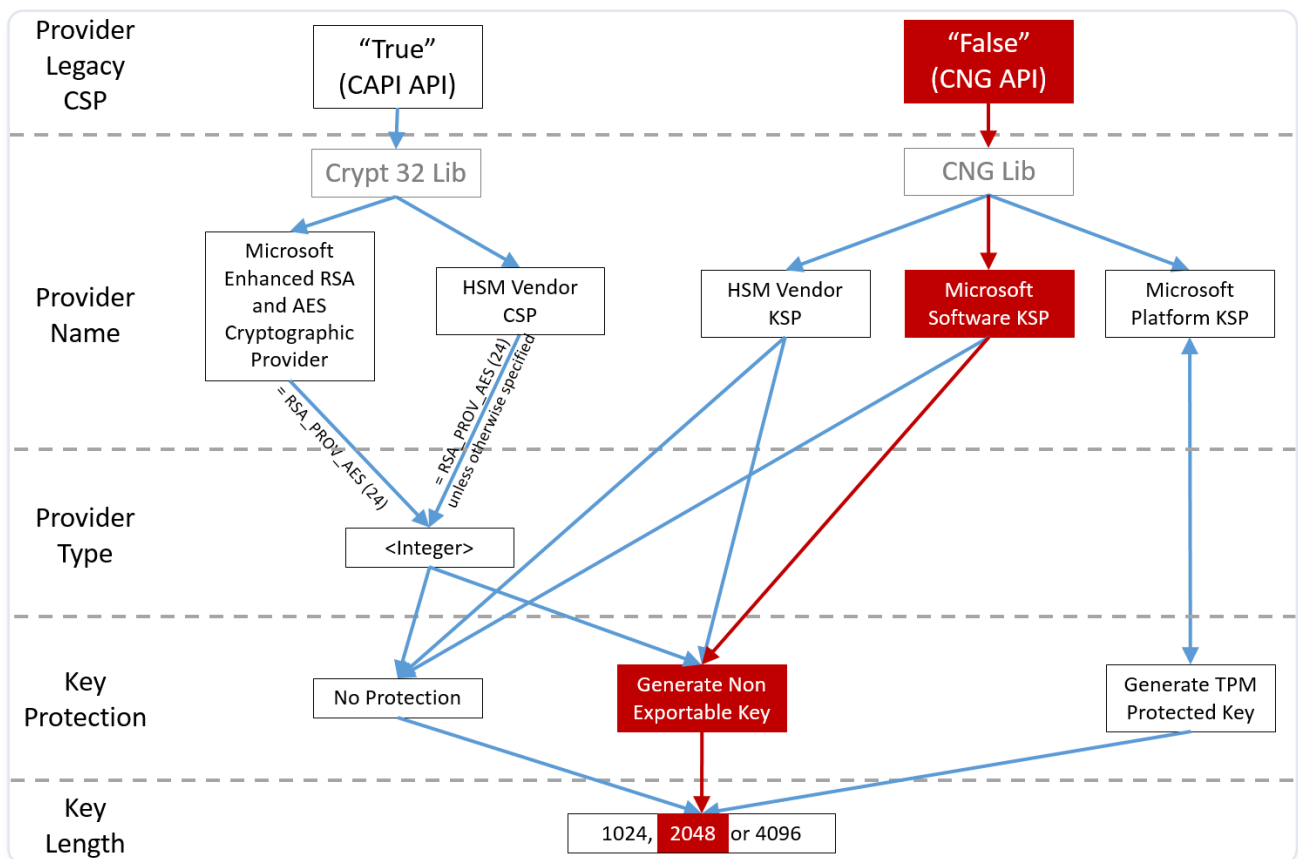
| 値                        | コメント                    |
|--------------------------|-------------------------|
| NoProtection             | 秘密キーはエクスポートできます。        |
| GenerateNonExportableKey | デフォルト。秘密キーはエクスポートできません。 |

| 値                       | コメント                                                                                                          |
|-------------------------|---------------------------------------------------------------------------------------------------------------|
| GenerateTPMProtectedKey | 秘密キーはTPMを使用して管理されます。秘密キーは、ProviderNameで指定したProviderName（例：Microsoft Platform Key Storage Provider）を介して保存されます。 |

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (秘密キーのサイズをビット単位で指定します)

| 値    | コメント                      |
|------|---------------------------|
| 2048 | デフォルト。1024または4096も使用できます。 |

設定ファイルの構成は、次のようにグラフィカルに表示されます（インストール時のデフォルトは赤で表示されています）。



## 構成シナリオの例

### 例 1

この例では、Microsoft Software Key Storage Providerを使用して保存される登録機関証明書の秘密キーとユーザー証明書の秘密キーについて説明します。

これはデフォルトのインストール後構成です。追加の秘密鍵構成は必要ありません。

### 例2

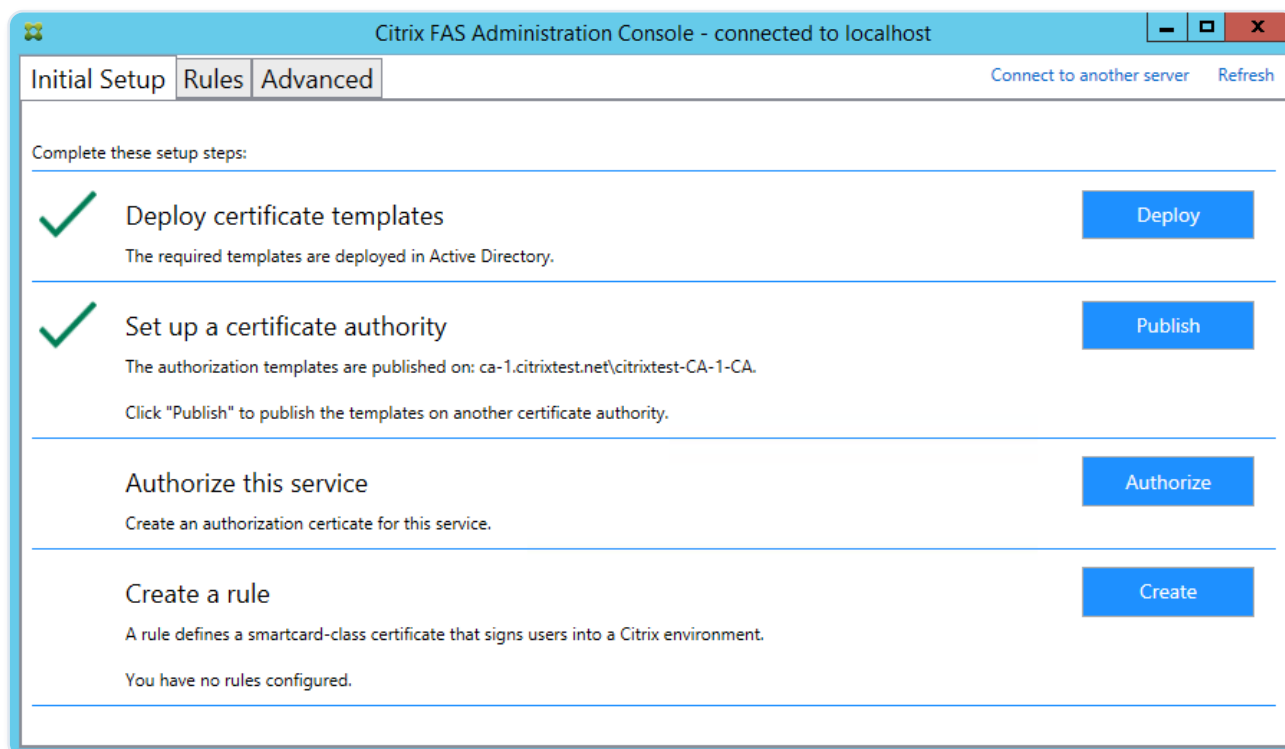
この例では、登録機関証明書の秘密鍵がMicrosoft Platform Key Storage Providerを介してFASサーバーのマザーボードのハードウェアTPMに保存され、ユーザー証明書の秘密鍵がMicrosoft Software Key Storage Providerを使用して保存されることを示します。

このシナリオでは、FASサーバーのマザーボード上のTPMが、TPM製造元のドキュメントに従ってBIOSで有効にされ、Windowsで初期化されていることを前提としています。 [<https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-vista/cc749022\(v=ws.10\)>](https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)>) を参照してください。

### FAS管理コンソールの使用

FAS管理コンソールはオフラインの証明書署名要求を実行できないため、組織が登録機関証明書のオンライン証明書署名要求を許可しない限り、その使用は推奨されません。

管理コンソールを使用してFASの初期構成を行う際は、最初の2つの手順である**証明書テンプレートの展開**と**証明機関のセットアップ**のみを完了し、その後、次のように進めます。



**手順1:** 次のように、構成ファイルの次の行を変更して編集します。

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>
```

ファイルは次のようになります。

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API (true) and CNG API (false) Cryptographic Providers -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name. -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP). For example: PROV_RSA_AES is 24 -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Suppress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value="" / -->
  </appSettings>
</configuration>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

一部のTPMは鍵長を制限します。デフォルトの鍵長は2048ビットです。ハードウェアでサポートされている鍵長を指定してください。

**手順2:** Citrix Federated Authentication Serviceを再起動して、構成ファイルから値を読み取りま

**手順3:** サービスを承認します。

**ステップ4:** 証明機関サーバーから保留中の証明書要求を手動で発行します。登録機関証明書が取得されると、管理コンソールのセットアップシーケンスのステップ3が緑色になります。この時点で、登録機関証明書の秘密キーはTPMで生成されています。証明書はデフォルトで2年間有効です。

登録機関証明書の秘密キーがTPMに正しく保存されていることを確認するには、以下のPowerShellコマンドを使用します。登録機関証明書の秘密キーがTPMに保存されている場合、PrivateKeyProviderフィールドは *Microsoft Platform Crypto Provider* に設定されます。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

**ステップ5:** 設定ファイルを以下のように編集し直します。

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

**注：**

FASはTPMで保護されたキーを持つユーザー証明書を生成できますが、大規模な展開ではTPMハードウェアが遅すぎる場合があります。

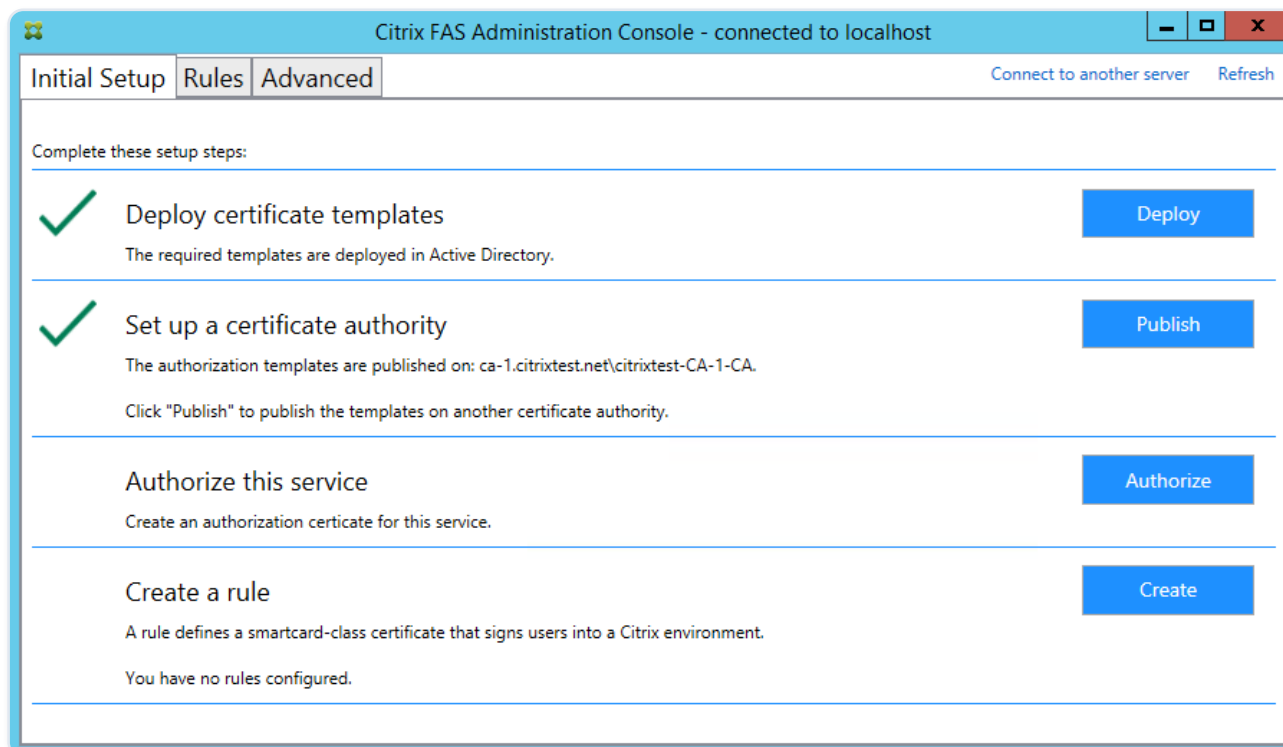
**ステップ6：** FASを再起動します。これにより、サービスは設定ファイルを再読み込みし、変更された値を反映します。その後の自動秘密キー操作はユーザー証明書キーに影響を与えます。これらの操作は秘密キーをTPMに保存せず、Microsoft Software Key Storage Providerを使用します。

**ステップ7：** FAS管理コンソールでルールタブを選択し、[インストール](#)と[構成](#)で説明されているように設定を編集します。

**PowerShellの使用**

登録機関証明書は、PowerShellを使用してオフラインで要求できます。これは、証明機関がオンライン証明書署名要求を介して登録機関証明書を発行することを望まない組織に適しています。FAS管理コンソールを使用してオフラインの登録機関証明書署名要求を行うことはできません。

**ステップ1：** 管理コンソールを使用してFASの初期構成を行う際、「証明書テンプレートの展開」と「証明機関のセットアップ」の最初の2つのステップのみを完了します。



**ステップ2:** 証明機関サーバーで、証明書テンプレートMMCスナップインを追加します。

**Citrix\_RegistrationAuthority\_ManualAuthorization**テンプレートを右クリックし、テンプレートの複製を選択します。

**全般**タブを選択します。名前と有効期間を変更します。この例では、名前は *Offline\_RA* で、有効期間は2年です。

| Subject Name         | Server  | Issuance Requirements |
|----------------------|---------|-----------------------|
| Superseded Templates |         | Extensions            |
| Security             |         |                       |
| Compatibility        | General | Request Handling      |
|                      |         | Cryptography          |
|                      |         | Key Attestation       |

Template display name:  
Offline\_RA

Template name:  
Offline\_RA

Validity period: 2 years      Renewal period: 0 days

☐ Publish certificate in Active Directory

☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

**ステップ3:** 証明機関サーバーで、証明機関MMCスナップインを追加します。証明書テンプレートを右クリックします。新規を選択し、発行する証明書テンプレートをクリックします。作成したばかりのテンプレートを選択します。

**ステップ4:** FASサーバーで次のPowerShellコマンドレットをロードします。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

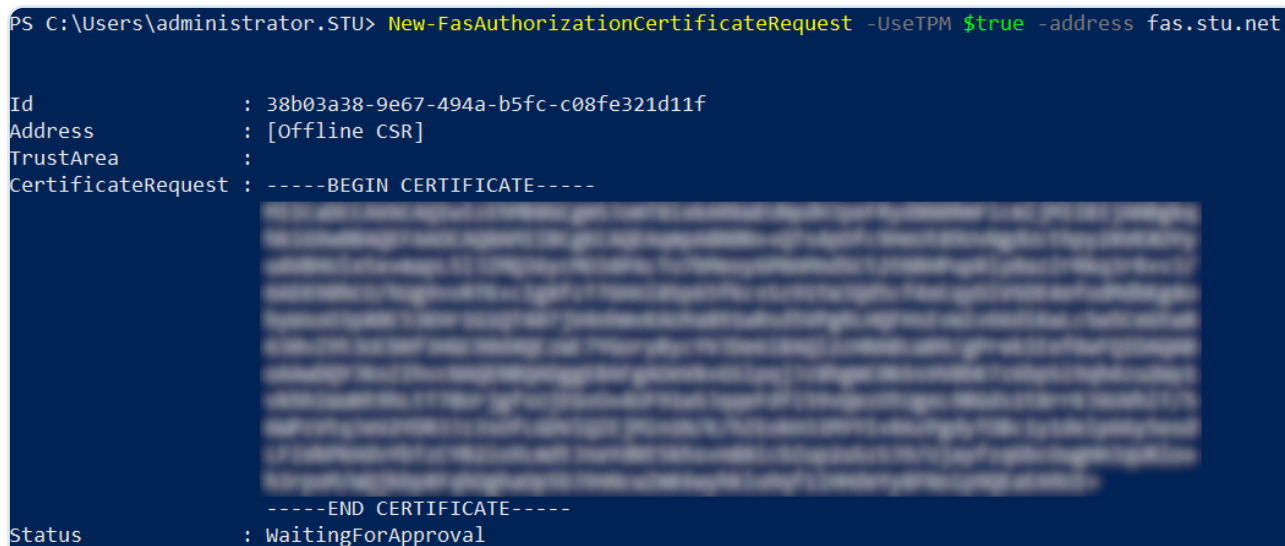
**ステップ 5:** FASサーバーのTPM内でRSAキーペアを生成し、FASサーバーで次のPowerShellコマンドレットを入力して証明書署名要求を作成します。**注:** 一部のTPMはキー長を制限します。デフォルトのキー長は2048ビットです。ハードウェアでサポートされているキー長を指定してください。

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address \&lt;FQDN of FAS Server>
```

例：

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net
```

次のように表示されます。



```
PS C:\Users\administrator.STU> New-FasAuthorizationCertificateRequest -UseTPM $true -address fas.stu.net

Id                : 38b03a38-9e67-494a-b5fc-c08fe321d11f
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE-----
                  [Blurred Certificate Content]
                  -----END CERTIFICATE-----
Status            : WaitingForApproval
```

# 注：

- Id GUID（この例では「5ac3d8bd-b484-4ebe-abf8-4b2cf62ca39」）は、後続のステップで必要になります。
- このPowerShellコマンドレットは、登録機関証明書の秘密キーを生成するために使用される1回限りの「オーバーライド」と考えてください。
- このコマンドレットを実行すると、FASの起動時に構成ファイルから読み取られた値がチェックされ、使用するキー長が決定されます（デフォルトは2048）。
- この手動のPowerShellで開始された登録機関証明書秘密キー操作では、-UseTPMが\$trueに設定されているため、システムはTPMの使用に必要な設定と一致しないファイルからの値を無視します。
- このコマンドレットを実行しても、構成ファイルの設定は変更されません。
- その後の自動FAS開始ユーザー証明書秘密キー操作では、FASの起動時にファイルから読み取られた値が使用されます。
- FASサーバーがユーザー証明書を発行してTPMで保護されたユーザー証明書秘密キーを生成する場合、構成ファイルのKeyProtection値をGenerateTPMProtectedKeyに設定することも可能です。

TPMがキーペアの生成に使用されたことを確認するには、キーペアが生成されたときにFASサーバーのWindowsイベントビューアーのアプリケーションログを確認します。

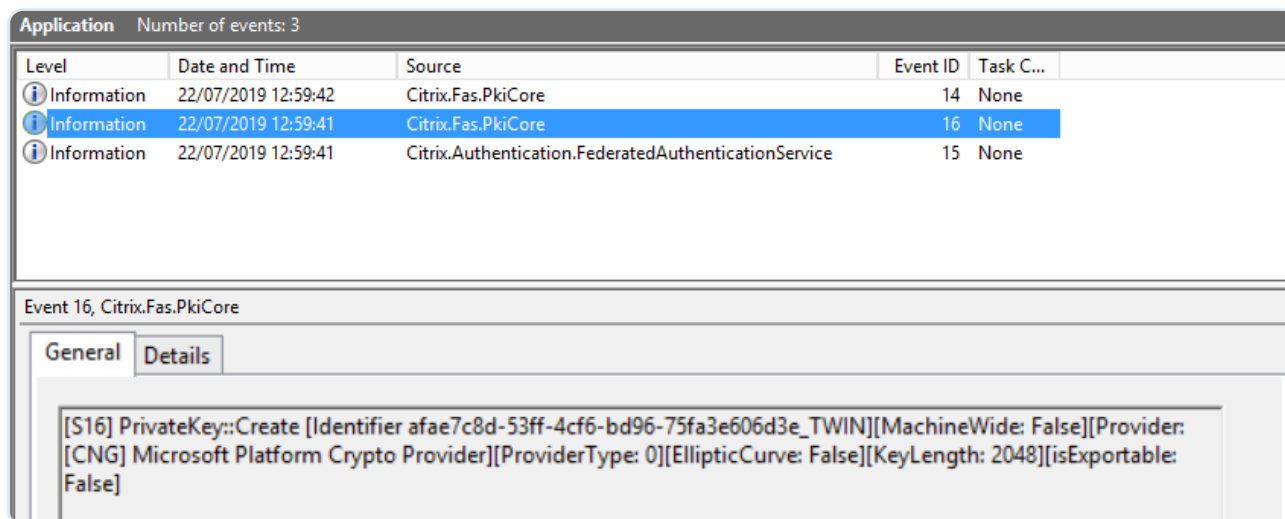
|             |                     |                                                      |    |      |
|-------------|---------------------|------------------------------------------------------|----|------|
| Information | 22/07/2019 12:59:42 | Citrix.Fas.PkiCore                                   | 14 | None |
| Information | 22/07/2019 12:59:41 | Citrix.Fas.PkiCore                                   | 16 | None |
| Information | 22/07/2019 12:59:41 | Citrix.Authentication.FederatedAuthenticationService | 15 | None |

| Event 15, Citrix.Authentication.FederatedAuthenticationService                                                                              |         |
|---------------------------------------------------------------------------------------------------------------------------------------------|---------|
| General                                                                                                                                     | Details |
| [S15] Administrator [CITRIXTEST\Administrator] creating certificate request [TPM: True] [correlation: e61a73d7-bb61-44af-8d21-1159d864d82e] |         |

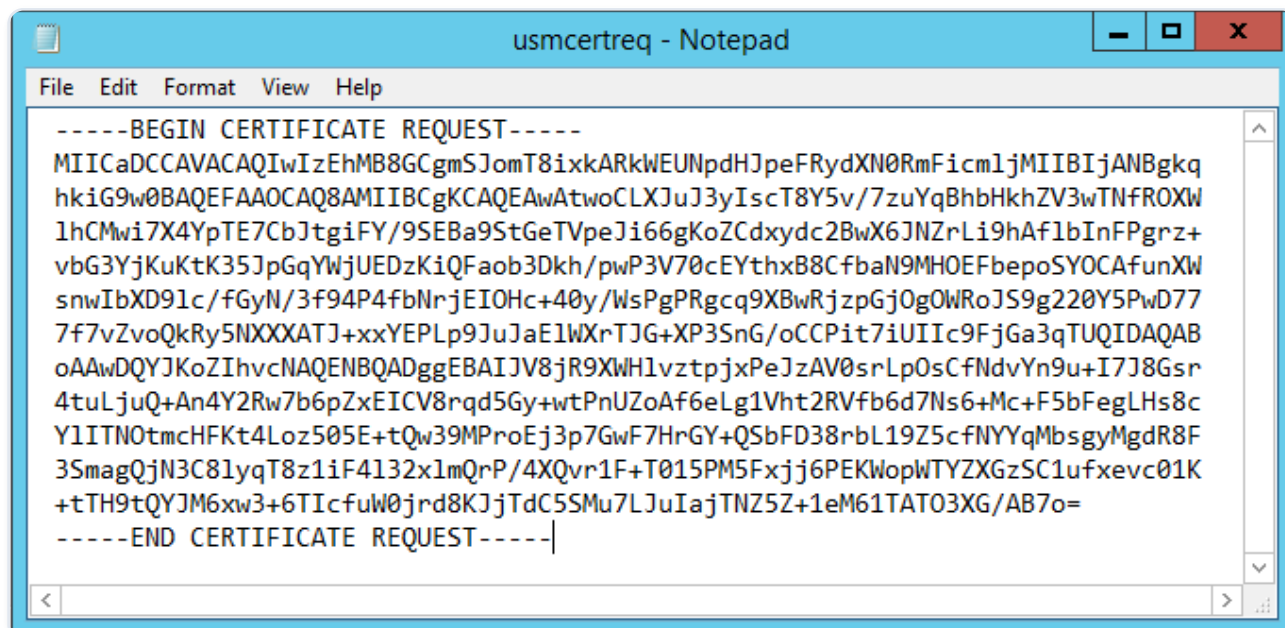
注: ""

続いて：



注: "プロバイダー: Microsoft Platform Crypto Provider"

**手順 6:** 証明書要求セクションをテキストエディターにコピーし、テキストファイルとしてディスクに保存します。



**手順 7:** FASサーバーでPowerShellに次のように入力して、証明書署名要求を証明機関に送信します。

```
certreq -submit -attrib "certificatetemplate:\&lt;certificate template
from step 2>" \&lt;certificate request file from step 6>
```

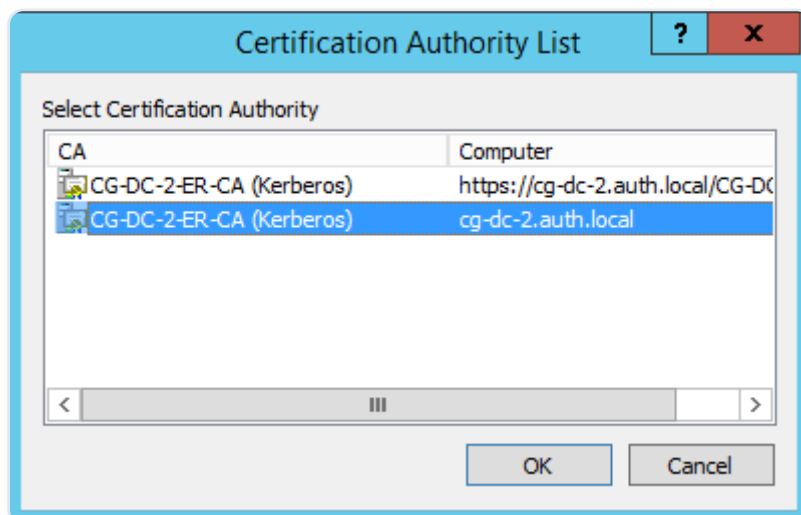
例:

```
certreq -submit -attrib "certificatetemplate:Offline_RA" C:
\Users\Administrator.AUTH\Desktop\usmcertreq.txt
```

次のように表示されます。

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-DB0C-4D21-A4FD-2E29502177C2}
ldap:
```

この時点で、証明機関リストウィンドウが表示される場合があります。この例の証明機関では、http (上) とDCOM (下) の両方の登録が有効になっています。利用可能な場合は、DCOMオプションを選択します。

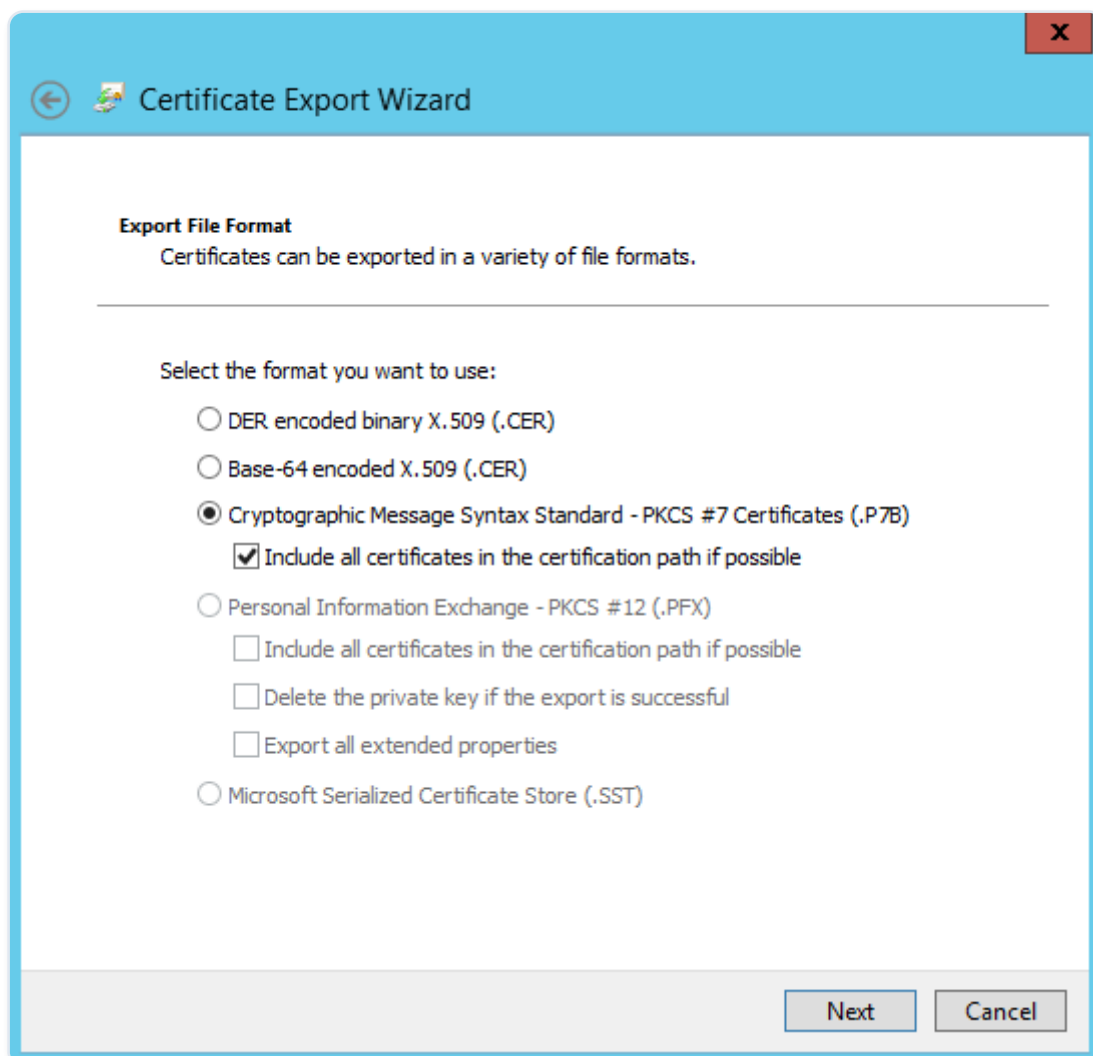


証明機関が指定されると、PowerShellにRequestIDが表示されます。

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-DB0C-4D21-A4FD-2E29502177C2}
ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

**手順 8:** 証明機関サーバーで、証明機関 MMC スナップインのをクリックします。要求 ID をメモします。次に、要求を右クリックし、を選択します。

**手順 9:** ノードを選択します。発行されたばかりの証明書を見つけます（要求 ID が一致するはず）。ダブルクリックして証明書を開きます。タブを選択します。をクリックします。証明書のエクスポートウィザードが起動します。をクリックします。ファイル形式について、次のオプションを選択します。



形式は「**暗号メッセージ構文標準 - PKCS #7 証明書 (.P7B)**」であり、「**可能であれば証明のパスにあるすべての証明書を含める**」が選択されている必要があります。

**手順 10:** エクスポートした証明書ファイルを FAS サーバーにコピーします。

**手順 11:** FAS サーバーで次の PowerShell コマンドレットを入力して、登録機関証明書を FAS サーバーにインポートします。

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

例：

```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

次のように表示されます。

```
PS C:\Users\administrator.STU> Import-FasAuthorizationCertificateResponse -Address fas.stu.net -Id 74d427ff-c55b-4d6d-87ae-1ff98b0c2705 -Pkcs7CertificateFile C:\Users\administrator.STU\Desktop\TPM_FAS_Cert.p7b
```

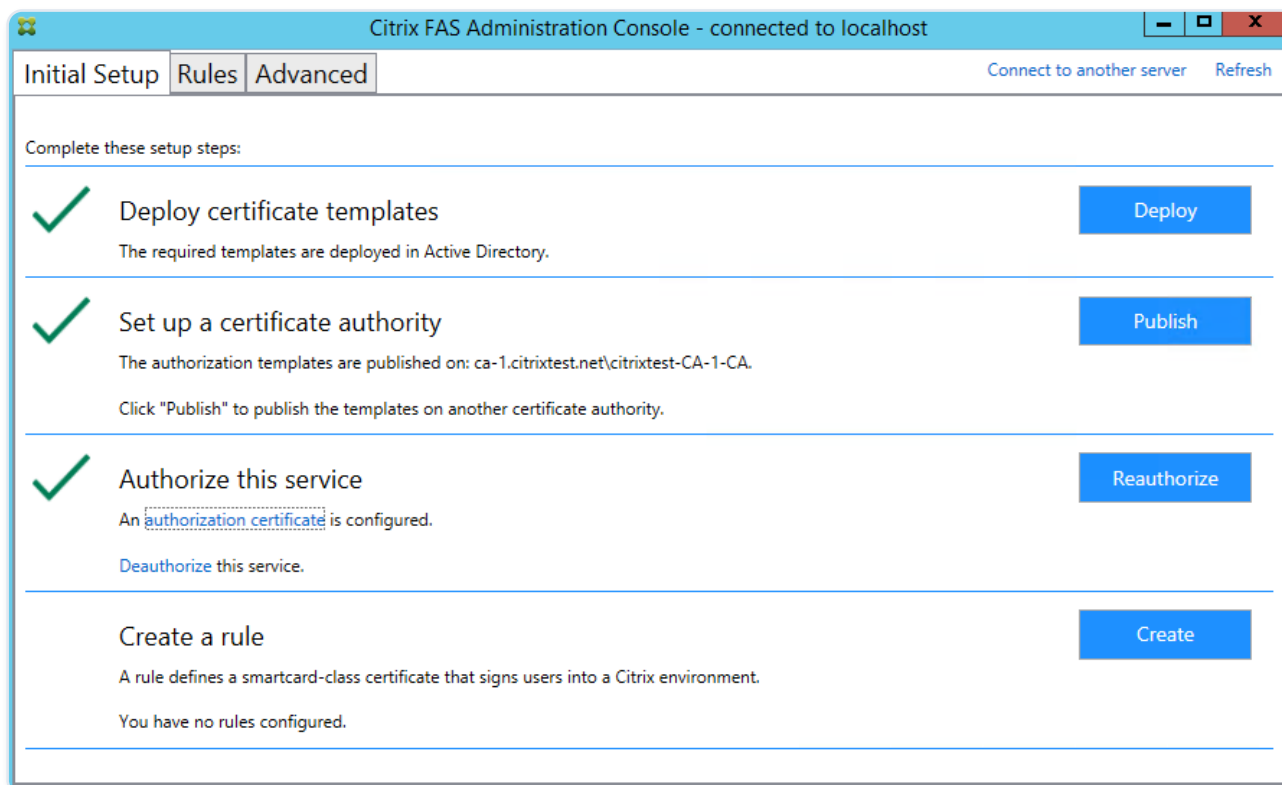
```
Id           : 74d427ff-c55b-4d6d-87ae-1ff98b0c2705
Address      : [Offline CSR]
TrustArea    : 978816cd-8b2f-4695-8c5d-08bb7df1816b
CertificateRequest :
Status       : Ok
```

登録機関証明書の秘密キーが TPM に正しく保存されていることを確認するには、次の PowerShell コマンドを使用します。登録機関証明書の秘密キーが TPM に保存されている場合、PrivateKeyProvider フィールドは *Microsoft Platform Crypto Provider* に設定されます。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

```
Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

**手順 12:** FAS 管理コンソールを閉じてから、再起動します。



注：「このサービスを承認」の手順に緑色のチェックマークが付いています。

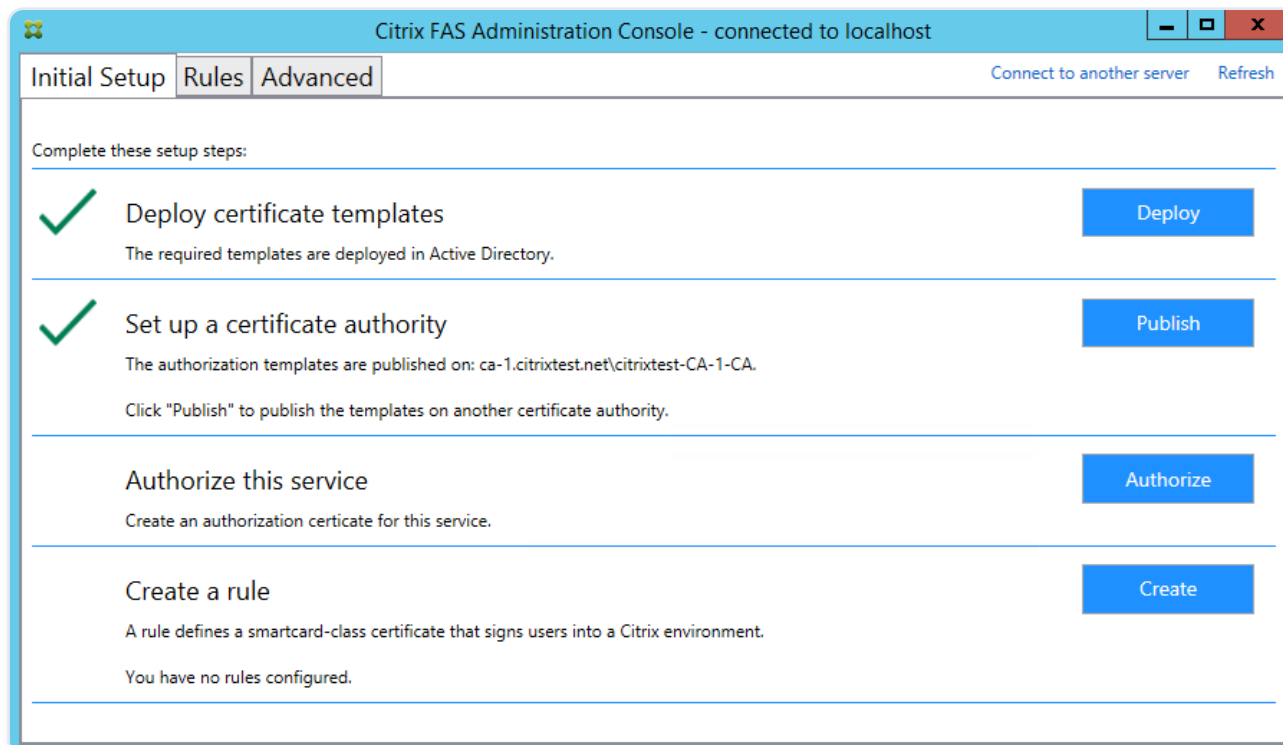
**ステップ 13:** FAS管理コンソールでルールタブを選択し、インストールと構成に記載されている設定を編集します。

### 例 3

この例では、HSMに保存されている登録機関証明書の秘密キーとユーザー証明書の秘密キーについて説明します。この例では、HSMが構成されていることを前提としています。HSMには、たとえば「HSM\_Vendor's Key Storage Provider」のようなプロバイダー名があります。

仮想化環境でFASサーバーを実行する予定がある場合は、ハイパーバイザーのサポートについてHSMベンダーに確認してください。

**ステップ 1.** 管理コンソールを使用してFASを最初にセットアップする際に、「証明書テンプレートの展開」と「証明機関のセットアップ」の最初の2つのステップのみを完了します。



**ステップ 2:** HSMのProviderName値が何であるべきかを判断するには、HSMベンダーのドキュメントを参照してください。HSMがCAPIを使用している場合、プロバイダーはドキュメントでCryptographic Service Provider (CSP) として参照されることがあります。HSMがCNGを使用している場合、プロバイダーはKey Storage Provider (KSP) として参照されることがあります。

**ステップ 3:** 設定ファイルを次のように編集します。

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
value="HSM_Vendor's Key Storage Provider"/>
```

ファイルは次のようになります。

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API (true) and CNG API (false) Cryptographic Providers -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name. -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP). For example: PROV_RSA_AES is 24 -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Suppress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value="" / -->
  </appSettings>
</startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

このシナリオでは、HSMがCNGを使用しているため、ProviderLegacyCsp値はfalseに設定されています。HSMがCAPIを使用している場合、ProviderLegacyCsp値はtrueに設定する必要があります。HSMがCAPIとCNGのどちらを使用しているかを判断するには、HSMベンダーのドキュメントを参照してください。また、非対称RSAキー生成でサポートされているキー長についても、HSMベンダーのドキュメントを参照してください。この例では、キー長はデフォルトの2048ビットに設定されています。指定するキー長がハードウェアでサポートされていることを確認してください。

**ステップ 4:** Citrix Federated Authentication Serviceを再起動して、設定ファイルから値を読み込みます。

**ステップ 5:** FAS管理コンソールの**初期設定**タブで**承認**をクリックして、HSM内でRSAキーペアを生成し、証明書署名要求を作成します。

**ステップ 6:** キーペアがHSMで生成されたことを確認するには、Windowsイベントログのアプリケーションエントリを確認します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-privatekeys-eventlog-hsm.png)

注: [プロバイダー: HSMベンダーのキーストレージプロバイダー]

**手順 7:** 証明機関サーバーで、証明機関MMCの**保留中の要求**ノードを選択します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-privatekeys-cammc-pendingrequests.png)

要求を右クリックし、**発行**を選択します。

注: 「このサービスを承認する」の手順には緑色のチェックマークが付いています。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-privatekeys-startup-threestep2.png)

手順 8: FAS管理コンソールでルールタブを選択し、インストールと構成に記載されているように設定を編集します。

## FAS証明書ストレージ

FASは、証明書を保存するためにFASサーバー上のMicrosoft証明書ストアを使用しません。埋め込みデータベースを使用します。

登録機関証明書のGUIDを特定するには、FASサーバーで次のPowerShellコマンドレットを入力します。

```
Add-pssnapin Citrix.a&ast;  
  
Get-FasAuthorizationCertificate -address \&lt;FAS server FQDN>
```

例えば、**Get-FasAuthorizationCertificate -address cg-fas-2.auth.net** :

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-privatekeys-get-fasauthorizationcertificate-example.png)

ユーザー証明書のリストを取得するには、次を入力します。

```
Get-FasUserCertificate -address \&lt;FAS server FQDN>
```

例えば、**Get-FasUserCertificate -address cg-fas-2.auth.net**

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-privatekeys-get-fasusercertificate-example.png)

### 注:

秘密鍵を保存するためにHSMを使用する場合、HSMコンテナはGUIDで識別されます。HSM内の秘密鍵のGUIDは、以下を使用して取得できます。

```
Get-FasUserCertificate -address \&lt;FAS server FQDN> -KeyInfo $true
```

例:

```
Get-FasUserCertificate -address fas3.djwfas.net -KeyInfo $true
```

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/get-fasusercertificate.png)

## 関連情報

- [インストールと構成](#)は、FASのインストールと構成に関する主要なリファレンスです。
- 一般的なFASの展開は、[フェデレーション認証サービスアーキテクチャの概要](#)の記事にまとめられています。
- その他の「ハウツー」記事は、[高度な構成](#)の記事で紹介されています。

## セキュリティとネットワーク構成

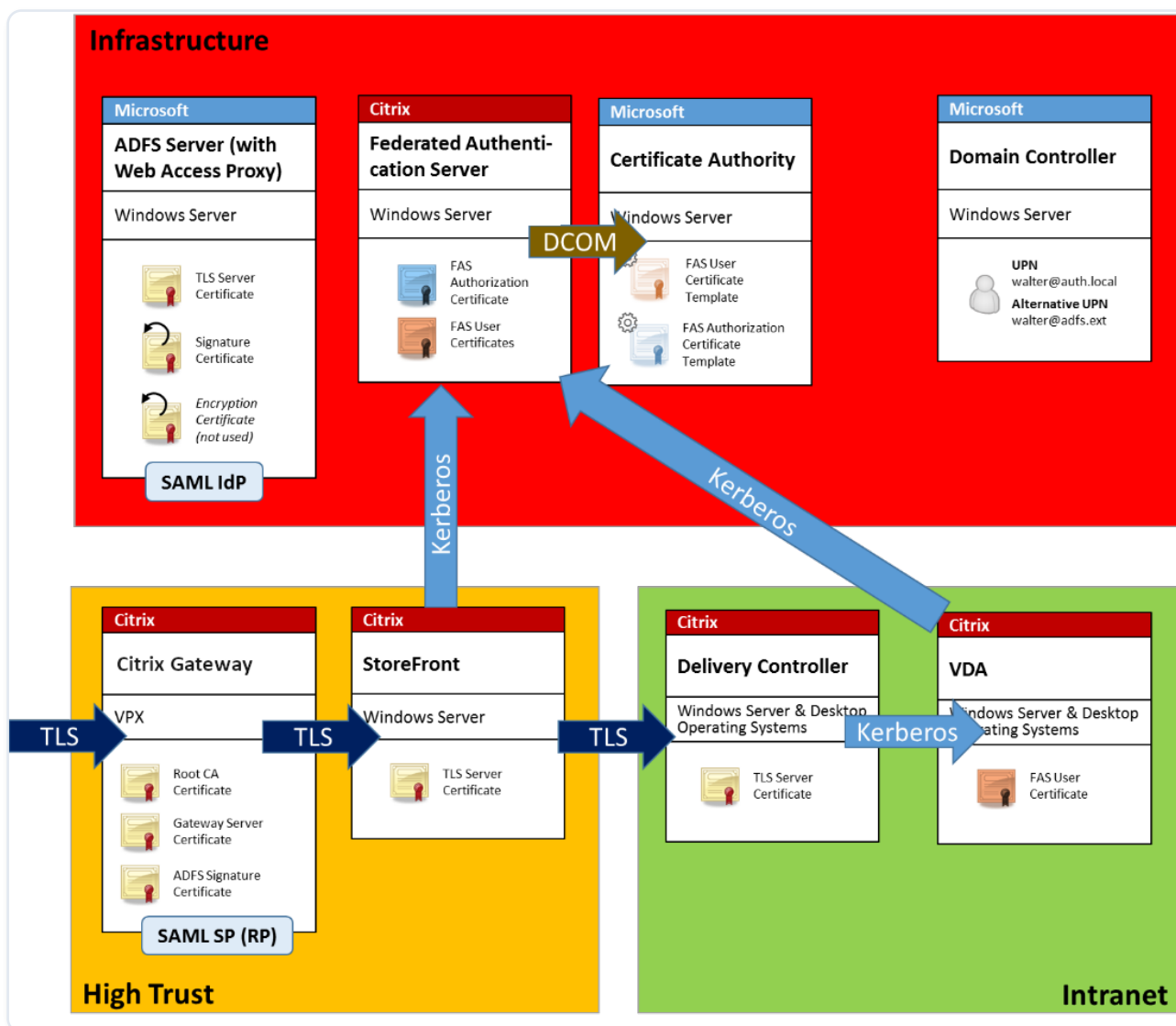
Federated Authentication Service (FAS) は、Microsoft Active Directory および Microsoft 証明機関と密接に統合されています。ドメインコントローラーやその他の重要なインフラストラクチャと同様に、セキュリティポリシーを策定し、システムが適切に管理および保護されていることを確認することが不可欠です。

このドキュメントでは、FAS を展開する際に考慮すべきセキュリティ問題の概要を説明します。また、インフラストラクチャの保護に役立つ利用可能な機能の概要も提供します。

## ネットワークアーキテクチャ

次の図は、FAS 展開で使用される主要なコンポーネントとセキュリティ境界を示しています。

FAS サーバーは、証明機関およびドメインコントローラーとともに、セキュリティ上重要なインフラストラクチャの一部として扱われるべきです。フェデレーション環境では、Citrix Gateway と Citrix Storefront はユーザー認証を実行するために信頼されるコンポーネントです。その他の Citrix Virtual Apps and Desktops™ コンポーネントは、FAS の導入による影響を受けません。



## ファイアウォールとネットワークセキュリティ

Citrix Gateway、StoreFront、および Delivery Controller™ コンポーネント間の通信は、ポート 443 経由の TLS によって保護される必要があります。StoreFront サーバーは発信接続のみを実行し、Citrix Gateway はインターネット経由の HTTPS ポート 443 を使用した接続のみを受け入れる必要があります。

StoreFront サーバーは、相互認証された Kerberos を使用してポート 80 経由で FAS サーバーに接続します。認証には、FAS サーバーの Kerberos HOST/fqdn ID と、StoreFront サーバーの Kerberos マシンアカウント ID が使用されます。これにより、Citrix Virtual Delivery Agent (VDA) がユーザーをログオンするために必要な、単一使用の「資格情報ハンドル」が生成されます。

HDX セッションが VDA に接続されると、VDA もポート 80 経由で FAS サーバーに接続します。認証には、FAS サーバーの Kerberos HOST/fqdn ID と、VDA の Kerberos マシン ID が使用されます。さらに、VDA は証明書と秘密鍵にアクセスするために「資格情報ハンドル」を提供する必要があります。

Microsoft 証明機関は、Kerberos 認証された DCOM を使用した通信を受け入れます。これは固定 TCP ポートを使用するように構成できます。証明機関はさらに、FAS サーバーが信頼された登録エージェント証明書によって署名された CMC パケットを提供することを要求します。

| サーバー           | ファイアウォールポート                                                                                |
|----------------|--------------------------------------------------------------------------------------------|
| フェデレーション認証サービス | [in] StoreFront™およびVDAからのHTTP経由 Kerberos、[out] Microsoft証明機関へのDCOM                         |
| シトリックス ゲートウェイ  | [in] クライアントマシンからのHTTPS、[in/out] StoreFrontサーバーとのHTTPS、[out] VDAへのHDX                       |
| StoreFront     | シトリックス ゲートウェイからのHTTPS [in]、デリバリー コントローラーへのHTTPS [out]、FASへのKerberos HTTP [out]             |
| デリバリー コントローラー  | [in] StoreFrontサーバーからのHTTPS、[in/out] VDAからのHTTP経由Kerberos                                  |
| VDA            | デリバリー コントローラーからのHTTP経由 Kerberos [in/out]、シトリックス ゲートウェイからのHDX [in]、FASへのKerberos HTTP [out] |
| Microsoft証明機関  | [in] FASからのDCOMおよび署名済み                                                                     |

## シトリックス フェデレーテッド認証サービスとシトリックス クラウド™間の接続

コンソールとFASは、それぞれユーザーアカウントとネットワークサービスアカウントを使用して、次のアドレスにアクセスします。

- ユーザーアカウント下のFAS管理コンソール
  - \*.cloud.com
  - \*.citrixworkspacesapi.net
  - 環境でサードパーティのIDプロバイダーが使用されている場合、そのプロバイダーが必要とするアドレス
- ネットワークサービスアカウント下のFASサービス: \*.citrixworkspacesapi.net

環境にプロキシサーバーが含まれている場合は、FAS管理コンソールのアドレスでユーザープロキシを構成します。また、ネットワークサービスアカウントのアドレスがnetshまたは同様のツールを使用して構成されていることを確認してください。

## 管理者の役割

環境の管理は、以下のグループに分けられます。

| 名前                           | 責任                           |
|------------------------------|------------------------------|
| エンタープライズ管理者                  | フォレストに証明書テンプレートをインストールして保護する |
| ドメイン管理者                      | グループポリシー設定を構成する              |
| 証明機関管理者                      | 証明機関を構成する                    |
| FAS管理者                       | FASサーバーをインストールして構成する         |
| StoreFront/Citrix Gateway管理者 | ユーザー認証を構成する                  |
| シトリックス バーチャル デスクトップ™ 管理者     | VDAとコントローラーを構成する             |

各管理者は、全体的なセキュリティモデルの異なる側面を制御し、システムを保護するための多層防御アプローチを可能にします。

## グループポリシー設定

信頼されたFASマシンは、グループポリシーを通じて構成された「インデックス番号 -> FQDN」のルックアップテーブルによって識別されます。FASサーバーに接続する際、クライアントはFASサーバーの `HOST\<fqdn>` Kerberos IDを検証します。FASサーバーにアクセスするすべてのサーバーは、同じインデックスに対して同一のFQDN構成を持つ必要があります。そうでない場合、StoreFrontとVDAは異なるFASサーバーに接続する可能性があります。

誤った構成を避けるため、Citrixは環境内のすべてのマシンに単一のポリシーを適用することを推奨しています。FASサーバーのリストを変更する際、特にエントリを削除したり並べ替えたりする際には注意してください。

このGPOの制御は、FASサーバーをインストールおよび廃止するFAS管理者（および/またはドメイン管理者）に限定されるべきです。FASサーバーを廃止した直後にマシンのFQDN名を再利用しないように注意してください。

## 証明書テンプレート

FASに付属のCitrix\_SmartcardLogon証明書テンプレートを使用しない場合は、そのコピーを変更できます。以下の変更がサポートされています。

### 証明書テンプレートの名前を変更する

Citrix\_SmartcardLogonの名前を組織のテンプレート命名標準に合わせて変更したい場合は、次の手順を実行する必要があります。

- 証明書テンプレートのコピーを作成し、組織のテンプレート命名標準に合わせて名前を変更します。
- 管理ユーザーインターフェイスではなく、FAS PowerShellコマンドを使用してFASを管理します。(管理ユーザーインターフェイスは、Citrixのデフォルトテンプレート名でのみ使用することを目的としています。)
  - テンプレートを公開するには、Microsoft MMC証明書テンプレートスナップインまたはPublish-FasMsTemplateコマンドのいずれかを使用し、
  - New-FasCertificateDefinitionコマンドを使用して、テンプレート名でFASを構成します。

### 全般プロパティを変更する

証明書テンプレートの有効期間を変更できます。

更新期間は変更しないでください。FASは、証明書テンプレートのこの設定を無視します。FASは、有効期間の途中で証明書を自動的に更新します。

### 要求処理プロパティを変更する

これらのプロパティは変更しないでください。FASは、証明書テンプレートのこれらの設定を無視します。FASは常に**秘密キーのエクスポートを許可する**の選択を解除し、**同じキーで更新する**の選択を解除します。

### 暗号化プロパティを変更する

これらのプロパティは変更しないでください。FASは、証明書テンプレートのこれらの設定を無視します。

FASが提供する同等の設定については、[秘密キーの保護](#)を参照してください。

### キー構成証明プロパティを変更する

これらのプロパティは変更しないでください。FASはキー構成証明をサポートしていません。

## 置き換えられたテンプレートプロパティを変更する

これらのプロパティは変更しないでください。FASはテンプレートの置き換えをサポートしていません。

## 拡張機能のプロパティを変更する

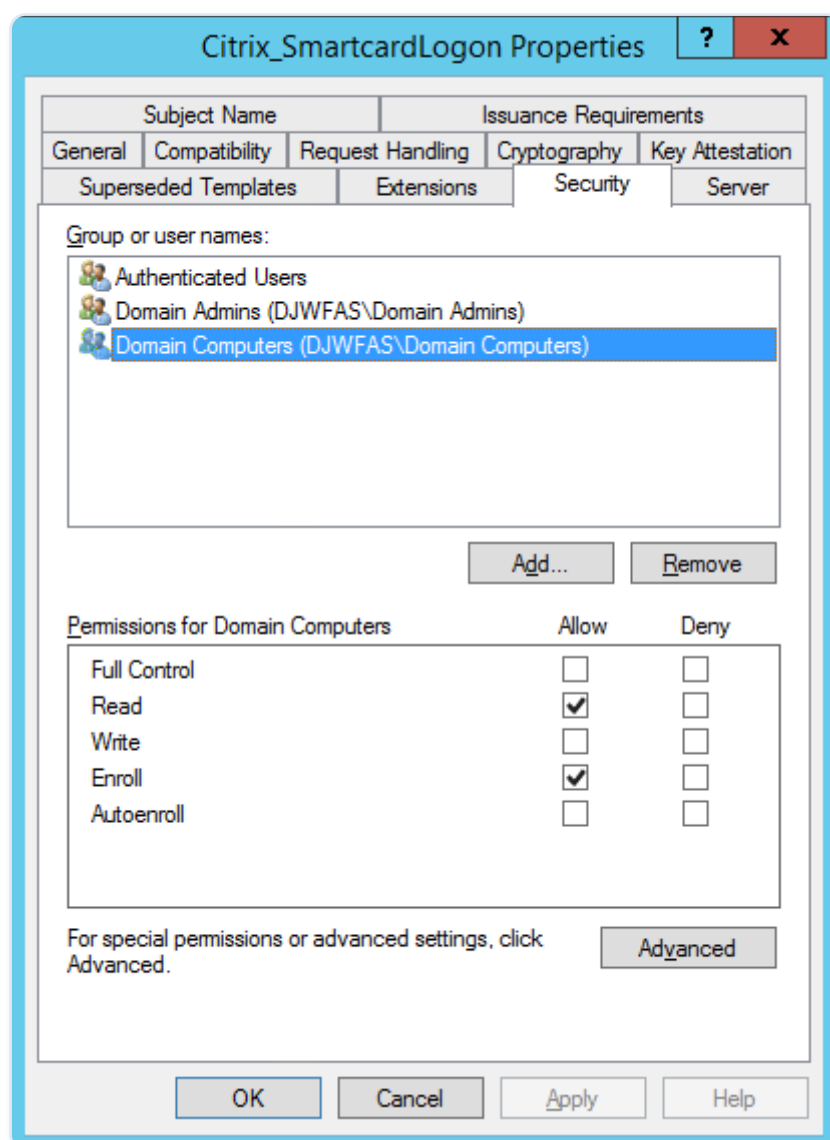
これらの設定は、組織のポリシーに合わせて変更できます。

注：不適切な拡張機能の設定は、セキュリティ上の問題を引き起こしたり、証明書が使用できなくなる原因となる可能性があります。

## セキュリティプロパティを変更する

Citrixでは、これらの設定を変更して、FASサーバーのマシンアカウントのみに**読み取り**および**登録**のアクセス許可を付与することを推奨しています。FASサービスでは、その他のアクセス許可は必要ありません。ただし、他の証明書テンプレートと同様に、次のことを検討する場合があります。

- 管理者がテンプレートを読み取りまたは書き込みできるようにする
- 認証済みユーザーがテンプレートを読み取れるようにする



## サブジェクト名のプロパティを変更する

Citrixでは、これらのプロパティを変更しないことを推奨しています。

テンプレートには「このActive Directory情報から構築」が選択されており、これにより証明機関はユーザーのSIDを証明書拡張機能に含めます。これは、ユーザーのActive Directoryアカウントへの強力なマッピングを提供します。

## サーバープロパティを変更する

Citrixは推奨していませんが、必要に応じて、これらの設定を組織のポリシーに合わせて変更できます。

## 発行要件のプロパティを変更する

これらの設定は変更しないでください。これらの設定は次のように表示されるはずです。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-security-props-issuance.png)

## 互換性プロパティの変更

これらの設定を変更できます。設定は少なくとも**Windows Server 2003 CA**（スキーマバージョン2）である必要があります。ただし、FASはWindows Server 2008以降のCAのみをサポートします。また、前述のとおり、FASは**Windows Server 2008 CA**（スキーマバージョン3）または**Windows Server 2012 CA**（スキーマバージョン4）を選択することで利用できる追加設定を無視します。

## 証明機関の管理

証明機関管理者は、証明機関サーバーの構成と、それが使用する発行証明書秘密キーの責任を負います。

## テンプレートの公開

エンタープライズ管理者が提供するテンプレートに基づいて証明機関が証明書を発行するには、証明機関管理者はそのテンプレートを公開することを選択する必要があります。

単純なセキュリティ対策としては、FASサーバーのインストール時に登録機関証明書テンプレートのみを公開するか、完全にオフラインの発行プロセスを徹底することです。いずれの場合も、証明機関管理者は登録機関証明書要求の承認を完全に制御し、FASサーバーを承認するためのポリシーを持つ必要があります。

## ファイアウォール設定

一般的に、証明機関管理者は証明機関のネットワークファイアウォール設定も制御し、受信接続を制御できます。証明機関管理者は、FASサーバーのみが証明書を要求できるようにDCOM TCP およびファイアウォールルールを構成できます。

## 登録の制限

デフォルトでは、登録機関証明書の所有者は、アクセスを許可する任意の証明書テンプレートを使用して、任意のユーザーに証明書を発行できます。これは、「登録エージェントの制限」証明機関プロパティを使用して、非特権ユーザーのグループに制限する必要があります。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-security-props-enrollmentagents.png)

## ポリシーモジュールと監査

高度な展開の場合、カスタムセキュリティモジュールを使用して証明書の発行を追跡および拒否できます。

## FAS管理

FASにはいくつかのセキュリティ機能があります。

### ACLによるStoreFront、ユーザー、VDAの制限

FASセキュリティモデルの中心は、どのKerberosアカウントが機能にアクセスできるかを制御することです。

| アクセスベクター            | 説明                                                                                                                                                                                                                           |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StoreFront [IdP]    | これらのKerberosアカウントは、ユーザーが正しく認証されたことを宣言するために信頼されています。これらのアカウントのいずれかが侵害された場合、FASの構成によって許可されたユーザーのために証明書が作成され、使用される可能性があります。                                                                                                     |
| VDA [Relying party] | これらは、証明書と秘密キーへのアクセスが許可されているマシンです。IdPによって取得された資格情報ハンドルも必要であるため、このグループ内の侵害されたVDAアカウントがシステムを攻撃できる範囲は限られています。                                                                                                                    |
| ユーザー                | これは、IdPによってアサートできるユーザーを制御します。証明機関の「Restricted Enrollment Agent」構成オプションと重複する点があることに注意してください。一般的に、このリストには非特権アカウントのみを含めることをお勧めします。これにより、侵害されたStoreFrontアカウントがより高い管理レベルに特権を昇格させることを防ぎます。特に、ドメイン管理者アカウントはこのACLによって許可されるべきではありません。 |

## ルールの構成

複数の独立したCitrix Virtual Apps™またはCitrix Virtual Desktops展開が同じFASサーバーインフラストラクチャを使用する場合、ルールは役立ちます。各ルールには個別の構成オプションセットがあり、特にACLは個別に構成できます。

## 証明機関とテンプレートの構成

異なる証明書テンプレートとCAは、異なるアクセス権限に対して構成できます。高度な構成では、環境に応じて、より強力な証明書またはより強力でない証明書を使用することを選択できます。たとえば、「外部」として識別されたユーザーは、「内部」ユーザーよりも少ない権限を持つ証明書を持つ場合があります。

## セッション内証明書と認証証明書

FAS管理者は、認証に使用される証明書がユーザーのセッション内で使用可能であるかどうかを制御できます。たとえば、これにより、「署名」証明書のみをセッション内で利用可能にし、より強力な「ログオン」証明書はログオン時にのみ使用されるようにすることができます。

## 秘密鍵の保護と鍵長

FAS管理者は、FASが秘密鍵をハードウェアセキュリティモジュール (HSM) またはトラステッドプラットフォームモジュール (TPM) に保存するように構成できます。Citrixは、少なくとも登録機関の証明書秘密鍵をTPMに保存することで保護することを推奨しています。このオプションは、「オフライン」証明書要求プロセスの一部として提供されます。

同様に、ユーザー証明書の秘密鍵はTPMまたはHSMに保存できます。すべての鍵は「エクスポート不可」として生成され、長さは2048ビット以上である必要があります。

## イベントログ

FASサーバーは、監査および侵入検知に使用できる詳細な構成およびランタイムイベントログを提供します。

## 管理アクセスと管理ツール

FASには、リモート管理機能（相互認証Kerberos）とツールが含まれています。「ローカル管理者グループ」のメンバーは、FAS構成を完全に制御できます。このリストは慎重に管理する必要があります。

## シトリックス バーチャル アプリ、シトリックス バーチャル デスクトップ、およびVDA管理者

一般に、FASの使用は、FASの「資格情報ハンドル」が「Active Directoryパスワード」を単に置き換えるため、Delivery ControllerおよびVDA管理者のセキュリティモデルを変更しません。

ControllerおよびVDA管理グループには、信頼できるユーザーのみを含める必要があります。監査およびイベントログは維持する必要があります。

### 一般的なWindowsサーバーのセキュリティ

すべてのサーバーは完全にパッチが適用され、標準のファイアウォールおよびウイルス対策ソフトウェアが利用可能である必要があります。セキュリティ上重要なインフラストラクチャサーバーは、物理的に安全な場所に保管し、ディスク暗号化と仮想マシンのメンテナンスオプションに注意を払う必要があります。

監査およびイベントログは、リモートマシンに安全に保存する必要があります。

RDPアクセスは、許可された管理者に限定されるべきです。可能な限り、ユーザーアカウントはスマートカードログオンを必要とすべきであり、特に証明機関およびドメイン管理者アカウントの場合に必要です。

### 関連情報

- (</ja-jp/federated-authentication-service/1912-ltsr/install-configure.html>)は、FASのインストールと構成に関する主要なリファレンスです。
- FASアーキテクチャについては、(</ja-jp/federated-authentication-service/1912-ltsr/deployment-architectures.html>)記事で紹介されています。
- その他の「ハウツー」記事については、(</ja-jp/federated-authentication-service/1912-ltsr/config-manage.html>)記事で紹介されています。

## Windowsログオンの問題のトラブルシューティング

この記事では、ユーザーが証明書やスマートカードを使用してログオンする際にWindowsが提供するログとエラーメッセージについて説明します。これらのログは、認証の失敗をトラブルシューティングするために使用できる情報を提供します。

### 証明書と公開キー基盤

Windows Active Directoryは、ログオンするユーザーの証明書を管理する複数の証明書ストアを保持しています。

- **NTAuth 証明書ストア:** Windowsに認証するには、ユーザー証明書を直接発行する証明機関（つまり、チェーンはサポートされていません）をNTAuthストアに配置する必要があります。これらの証明書を表示するには、certutilプログラムから「certutil -viewstore -enterprise NTAuth」と入力します。
- **ルートおよび中間証明書ストア:** 通常、証明書ログオンシステムは単一の証明書しか提供できないため、チェーンが使用されている場合は、すべての中間証明書ストアにこれらの証明書を含める必要があります。ルート証明書は信頼されたルートストアに、最後から2番目の証明書はNTAuthストアにある必要があります。
- **ログオン証明書拡張機能とグループポリシー:** Windowsは、EKUおよびその他の証明書ポリシーの検証を強制するように構成できます。Microsoftのドキュメントを参照してください:  
[https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287\(v=ws.10\)>](https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)>)。

| レジストリポリシー                                          | 説明                                                                                                  |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| AllowCertificatesWithNoEKU                         | 無効にすると、証明書にはスマートカードログオンの拡張キー使用法 (EKU) が含まれている必要があります。                                               |
| AllowSignatureOnlyKeys                             | デフォルトでは、WindowsはRSA復号化を許可しない証明書の秘密キーを除外します。このオプションはそのフィルターを上書きします。                                  |
| AllowTimeInvalidCertificates                       | デフォルトでは、Windowsは期限切れの証明書を除外します。このオプションはそのフィルターを上書きします。                                              |
| EnumerateECCCert                                   | 楕円曲線認証を有効にします。                                                                                      |
| X509ヒントが必要                                         | 証明書に一意のユーザープリンシパル名 (UPN) が含まれていない場合、または曖昧である可能性がある場合、このオプションを使用すると、ユーザーはWindowsログオンアカウントを手動で指定できます。 |
| UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors | 失効チェックを無効にします（通常、ドメインコントローラーで設定されます）。                                                               |

- **ドメインコントローラー証明書:** Kerberos接続を認証するには、すべてのサーバーに適切な「ドメインコントローラー」証明書が必要です。これらは、「ローカルコンピューター証明書個人ストア」MMCスナップインメニューを使用して要求できます。

## UPN名と証明書のマッピング

ユーザー証明書には、サブジェクト代替名拡張に一意のユーザープリンシパル名 (UPN) を含めることをお勧めします。

### アクティブ ディレクトリのUPN名

デフォルトでは、Active Directoryのすべてのユーザーは、`\<samUsername>@\<domainNetBios>` および `\<samUsername>@\<domainFQDN>` のパターンに基づいた暗黙的なUPNを持っています。利用可能なドメインとFQDNは、フォレストのRootDSEエントリに含まれています。単一のドメインがRootDSEに複数のFQDNアドレスを登録できることに注意してください。

さらに、Active Directoryのすべてのユーザーは、明示的なUPNとaltUserPrincipalNamesを持っています。これらは、ユーザーのUPNを指定するLDAPエントリです。

UPNでユーザーを検索する場合、Windowsはまず現在のドメイン（UPNを検索するプロセスのIDに基づく）で明示的なUPNを検索し、次に代替UPNを検索します。一致するものがない場合、暗黙的なUPNを検索します。これはフォレスト内の異なるドメインに解決される可能性があります。

### 証明書マッピングサービス

証明書に明示的なUPNが含まれていない場合、Active Directoryには、各使用のために正確な公開証明書を「x509certificate」属性に保存するオプションがあります。このような証明書をユーザーに解決するには、コンピューターがこの属性を直接クエリできます（デフォルトでは、単一ドメイン内）。

ユーザーがこの検索を高速化するユーザーアカウントを指定できるオプションが提供されており、この機能はクロスドメイン環境でも使用できます。

フォレスト内に複数のドメインがあり、ユーザーが明示的にドメインを指定しない場合、Active Directory の rootDSE が証明書マッピングサービスの場所を指定します。これは通常、グローバルカタログマシンにあり、フォレスト内のすべての x509 証明書属性のキャッシュされたビューを持っています。このコンピューターは、証明書のみに基づいて、任意のドメイン内のユーザーアカウントを効率的に見つけるために使用できます。

## ログオンドメインコントローラーの選択を制御する

環境に複数のドメインコントローラーが含まれている場合、認証に使用されるドメインコントローラーを確認および制限できると、ログを有効にして取得できるため便利です。

### ドメインコントローラーの選択を制御する

Windows がログオンに特定の Windows ドメインコントローラーを使用するように強制するには、lmhosts ファイル (\Windows\System32\drivers\etc\lmhosts) を構成して、Windows マシンが使用するドメインコントローラーのリストを明示的に設定できます。

通常、その場所に「lmhosts.sam」という名前のサンプルファイルがあります。次の行を含めるだけです。

```
1.2.3.4 dcnetbiosname #PRE #DOM:mydomain
```

ここで、「1.2.3.4」は「mydomain」ドメイン内の「dcnetbiosname」という名前のドメインコントローラーの IP アドレスです。

再起動後、Windows マシンはその情報を使用して mydomain にログオンします。デバッグが完了したら、この構成を元に戻す必要があることに注意してください。

### 使用中のドメインコントローラーを特定する

ログオン時に、Windows はユーザーをログオンさせたドメインコントローラーを含む MSDOS 環境変数を設定します。これを確認するには、コマンドプロンプトを起動し、**echo %LOGONSERVER%** コマンドを実行します。

認証に関連するログは、このコマンドによって返されるコンピューターに保存されます。

## アカウント監査イベントを有効にする

デフォルトでは、Windows ドメインコントローラーは完全なアカウント監査ログを有効にしません。これは、グループポリシーエディターのセキュリティ設定にある監査ポリシーを通じて制御されます。有効にすると、ドメインコントローラーはセキュリティログファイルに追加のイベントログ情報を生成します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-troubleshoot-logon-auditpolicy.png)

## 証明書検証ログ

### 証明書の有効性を確認する

スマートカード証明書がDER証明書としてエクスポートされた場合（秘密鍵は不要）、次のコマンドで検証できます: `certutil -verify user.cer`

### CAPIログを有効にする

ドメインコントローラーとユーザーのマシンで、イベントビューアーを開き、Microsoft/Windows/CAPI2/Operational Logs のログを有効にします。

CAPIログは、次のレジストリキーで制御できます: `CurrentControlSet\Services\crypt32`。

| 値                           | 説明                              |
|-----------------------------|---------------------------------|
| DiagLevel (DWORD)           | 詳細レベル (0～5)                     |
| DiagMatchAnyMask (QUADWORD) | イベントフィルター (すべてに 0xffffffff を使用) |
| DiagProcessName (MULTI_SZ)  | プロセス名でフィルター (例: LSASS.exe)      |

### CAPI ログ

| メッセージ       | 説明                                                                                                |
|-------------|---------------------------------------------------------------------------------------------------|
| チェーンの構築     | LSA が <code>CertGetCertificateChain</code> を呼び出しました (結果を含む)                                       |
| 失効の検証       | LSA が <code>CertVerifyRevocation</code> を呼び出しました (結果を含む)                                          |
| X509 オブジェクト | 詳細モードでは、証明書と証明書失効リスト (CRL) が<br><code>AppData\LocalLow\Microsoft\X509Objects</code> に<br>ダンプされます。 |
| チェーンポリシーの検証 | LSA が <code>CertVerifyChainPolicy</code> を呼び出しました (パラメーターを含む)                                     |

## エラーメッセージ

| エラーコード        | 説明                                                                                                                                                                                                                                                                  |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 証明書が信頼されていません | スマートカード証明書は、コンピューターの中間証明書ストアおよび信頼されたルート証明書ストアにある証明書を使用して構築できませんでした。                                                                                                                                                                                                 |
| 証明書失効チェックエラー  | スマートカードのCRLは、証明書のCRL配布ポイントで指定されたアドレスからダウンロードできませんでした。失効チェックが義務付けられている場合、これによりログオンが成功しくなくなります。「証明書と公開鍵インフラストラクチャ」(/ja-jp/federated-authentication-service/1912-ltsr/config-manage/troubleshoot-logon.html#certificates-and-public-key-infrastructure)セクションを参照してください。 |
| 証明書使用エラー      | その証明書はログオンに適していません。たとえば、サーバー証明書または署名証明書である可能性があります。                                                                                                                                                                                                                 |

## Kerberosログ

Kerberosログを有効にするには、ドメインコントローラーとエンドユーザーマシンで、次のレジストリ値を作成します。

| ハイブ                                                         | 値の名前             | 値 [DWORD]  |
|-------------------------------------------------------------|------------------|------------|
| CurrentControlSet\Control\LocalSecurity\Kerberos\Parameters | LogLevel         | 0x1        |
| CurrentControlSet\Control\LocalSecurity\Kerberos\Parameters | KerbDebuglevel   | 0xffffffff |
| CurrentControlSet\Services\Kdc                              | KdcDebugLevel    | 0x1        |
| CurrentControlSet\Services\Kdc                              | KdcExtraLogLevel | 0x1f       |

Kerberosログはシステムイベントログに出力されます。

- 「信頼されていない証明書」のようなメッセージは診断が容易であるはずです。
- 2つのエラーコードは情報提供であり、安全に無視できます。
  - KDC\_ERR\_PREAUTH\_REQUIRED (古いドメインコントローラーとの下位互換性のために使用されます)
  - 不明なエラー 0x4b

## イベントログメッセージ

このセクションでは、ユーザーが証明書でログオンしたときのドメインコントローラーとワークステーション上の予期されるログエントリについて説明します。

- ドメインコントローラーCAPI2ログ
- ドメインコントローラーセキュリティログ
- Virtual Delivery Agent (VDA) セキュリティログ
- VDA CAPI ログ
- VDA システムログ

## ドメインコントローラー CAPI2 ログ

ログオン中、ドメインコントローラーは呼び出し元の証明書を検証し、次の形式で一連のログエントリを生成します。

| Operational Number of events: 6 |                     |        |          |                     |
|---------------------------------|---------------------|--------|----------|---------------------|
| Level                           | Date and Time       | Source | Event ID | Task Category       |
| Information                     | 21/06/2016 15:14:54 | CAPI2  | 30       | Verify Chain Policy |
| Information                     | 21/06/2016 15:14:54 | CAPI2  | 11       | Build Chain         |
| Information                     | 21/06/2016 15:14:54 | CAPI2  | 90       | X509 Objects        |
| Information                     | 21/06/2016 15:14:54 | CAPI2  | 41       | Verify Revocation   |
| Information                     | 21/06/2016 15:14:54 | CAPI2  | 40       | Verify Revocation   |
| Information                     | 21/06/2016 15:14:54 | CAPI2  | 10       | Build Chain         |

最終的なイベントログメッセージは、ドメインコントローラー上の lsass.exe が VDA から提供された証明書に基づいてチェーンを構築し、その有効性（失効を含む）を検証していることを示しています。結果は「ERROR\_SUCCESS」として返されます。

```
- CertVerifyCertificateChainPolicy
  - Policy
    [ type]      CERT_CHAIN_POLICY_NT_AUTH
    [ constant]  6
  - Certificate
    [ fileRef]    23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    [ subjectName] fred
  - CertificateChain
    [ chainRef]   {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - Flags
    [ value]      0
  - Status
    [ chainIndex] -1
    [ elementIndex] -1
  - EventAuxInfo
    [ ProcessName] lsass.exe
  - CorrelationAuxInfo
    [ TaskId]      {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    [ SeqNumber] 1
  - Result
    [ value]      0
```

## ドメインコントローラーセキュリティログ

ドメインコントローラーは一連のログオンイベントを表示します。主要なイベントは4768で、ここでは証明書がKerberos Ticket Granting Ticket (krbtgt) の発行に使用されます。

これより前のメッセージは、サーバーのマシンアカウントがドメインコントローラーに対して認証を行っていることを示しています。これに続くメッセージは、新しい krbtgt に属するユーザーアカウントがドメインコントローラーに対して認証に使用されていることを示しています。

| Keywords      | Date and Time       | Source            | Event ID | Task Category                      |
|---------------|---------------------|-------------------|----------|------------------------------------|
| Audit Success | 21/06/2016 15:14:56 | Security-Auditing | 4624     | Logon                              |
| Audit Success | 21/06/2016 15:14:56 | Security-Auditing | 4624     | Logon                              |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4769     | Kerberos Service Ticket Operations |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4768     | Kerberos Authentication Service    |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4769     | Kerberos Service Ticket Operations |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4634     | Logoff                             |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4624     | Logon                              |
| Audit Success | 21/06/2016 15:14:54 | Security-Auditing | 4624     | Logon                              |

**Event 4768, Security-Auditing**

**General** | Details

☒ Friendly View    ☐ XML View

**+ System**

**- EventData**

**TargetUserName** fred

**TargetDomainName** CITRIXTEST.NET

**TargetSid** S-1-5-21-390731715-1143989709-1377117006-1106

**ServiceName** krbtgt

**ServiceSid** S-1-5-21-390731715-1143989709-1377117006-502

**TicketOptions** 0x40810010

**Status** 0x0

**TicketEncryptionType** 0x12

**PreAuthType** 16

**IpAddress** ::ffff:192.168.0.10

**IpPort** 49348

**CertIssuerName** citrixtest-DC-CA

**CertSerialNumber** 5F0001D1FCA2AC30F36879CEEC00000001D1FC

**CertThumbprint** 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F

## VDA セキュリティログ

ログオンイベントに対応する VDA セキュリティ監査ログは、イベント ID 4648 を持つエントリで、winlogon.exe から発生します。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-troubleshoot-logon-vda-security-log.png)

## VDA CAPI ログ

このVDA CAPIログの例は、lsass.exeからの単一のチェーン構築と検証シーケンスを示しており、ドメインコントローラー証明書 (dc.citrixtest.net) を検証しています。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-troubleshoot-logon-capi-log.png)

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-troubleshoot-logon-capi-chainpolicy.png)

## VDA システムログ

Kerberosログが有効になっている場合、システムログにはエラー

KDC\_ERR\_PREAUTH\_REQUIRED (これは無視できます) と、Kerberosログオンが成功したことを示すWinlogonからのエントリが表示されます。

ローカライズされた画像(/en-us/federated-authentication-service/1912-ltsr/media/fas-troubleshoot-logon-vda-system-log.png)

## エンドユーザーのエラーメッセージ

このセクションでは、Windowsログオンページでユーザーに表示される一般的なエラーメッセージを一覧表示します。

| 表示されるエラーメッセージ                                      | 説明と参照                                                                                                                                                                                                                        |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 無効なユーザー名またはパスワード                                   | コンピューターは、有効な証明書と秘密キーを持っていると認識していますが、Kerberosドメインコントローラーが接続を拒否しました。この記事の「 <a href="#">Kerberos ログ</a> 」セクションを参照してください。                                                                                                        |
| システムはログオンできませんでした。資格情報を検証できませんでした。/ 要求はサポートされていません | ドメインコントローラーに接続できないか、ドメインコントローラーがスマートカード認証をサポートする証明書で構成されていません。「 <a href="#">Kerberos 認証</a> 」、「 <a href="#">ドメインコントローラー認証</a> 」、または「 <a href="#">ドメインコントローラー</a> 」証明書をドメインコントローラーに登録してください。既存の証明書が有効に見える場合でも、これは通常試す価値があります。 |
| システムがログオンできませんでした。認証に使用されたスマートカード証明書は信頼されていませんでした。 | 中間証明書とルート証明書がローカルコンピューターにインストールされていません。 <a href="#">証明書と公開キーインフラストラクチャ</a> を参照してください。                                                                                                                                        |
| 不正な要求                                              | これは通常、証明書の拡張機能が正しく設定されていないか、RSAキーが短すぎる (<2048 ビット) ことを示します。                                                                                                                                                                  |

## 関連情報

- スマートカードログオン用にドメインを構成する: <http://support.citrix.com/article/CTX206156>
- スマートカードログオンポリシー: [https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287\(v=ws.10\)](https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10))
- CAPIログ記録を有効にする: <http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx>
- Kerberosログ記録を有効にする: <https://support.microsoft.com/ja-jp/kb/262177>
- サードパーティの認証局でスマートカードログオンを有効にするためのガイドライン: <https://support.microsoft.com/ja-jp/kb/281245>

## PowerShellコマンドレット

シンプルな展開にはFederated Authentication Service (FAS) 管理コンソールを使用できますが、PowerShellインターフェイスではより高度なオプションが提供されます。コンソールで利用できないオプションを使用する予定がある場合は、Citrix®は構成にPowerShellのみを使用することを推奨します。

次のコマンドは、FAS PowerShellコマンドレットを追加します。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

PowerShellウィンドウで、Get-Help \<cmdlet name>を使用してコマンドレットのヘルプを表示できます。

FAS PowerShell SDKコマンドレットの詳細については、<https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/>を参照してください。

# フェデレーション認証サービス 1912 ドキュメント履歴

以下の表は、フェデレーション認証サービス 1912 ドキュメントの重要な変更点について説明しています。これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

| 日付          | 変更点                         | 説明                                                                    |
|-------------|-----------------------------|-----------------------------------------------------------------------|
| 18 Dec 2019 | フェデレーション認証サービス 1912 の初回リリース | フェデレーション認証サービス 1912 の初回リリース。詳細については、「 <a href="#">新機能</a> 」を参照してください。 |