

フェデレーション認証サービス

Contents

フェデレーション認証サービス 2411	10
以前のリリース	10
参照	11
フェデレーション認証サービス 2411	12
ユーザーへの影響なしにFAS承認証明書を更新する	12
FASでのキーストレージ管理プロセスの改善	12
楕円曲線キーのサポート	12
フェデレーション認証サービス KSPリモート処理 (一般提供)	12
修正された問題	13
既知の問題	13
第三者通知	13
システム要件	14
インストールと構成	16
インストールとセットアップの順序	16
フェデレーション認証サービスをインストールする	16
FASのアップグレード	17
StoreFrontストアでFASプラグインを有効にする	17
Delivery Controller™を構成する	17
グループポリシーを構成する	18
セッション内の動作	21
プロンプトの範囲	22
同意のタイムアウト	23
ロック時の切断	23
フェデレーション認証サービス管理コンソールの使用	23
証明書テンプレートを展開する	24
Active Directory証明書サービスをセットアップする	26

フェデレーション認証サービスを承認する	27
ルールの構成	29
Citrix Cloudへの接続	34
Citrix Cloudから切断する	39
高度な構成	40
関連情報	40
テナント顧客向けフェデレーション認証サービスを有効にする	40
前提条件	40
MSP顧客を構成する	40
既知の問題	43
Azure Active Directoryシングルサインオン	43
ドメイン参加済み VDA	44
ハイブリッド参加済みVDA	45
認証局の構成	46
FASで使用する複数のCAサーバーを設定する	47
予期される動作の変更	47
TCPアクセス用にMicrosoft認証局を構成する	47
ユーザー証明書を事前生成する	48
Active Directoryユーザーのリストを取得する	48
FASサーバー	49
FAS承認証明書を更新する	51
FAS管理コンソールを使用する	51
PowerShellを使用する	52
FASの認証解除とFAS証明書の削除	53
FAS管理コンソールの使用	53
PowerShellの使用	54
オフライン承認	55
関連情報	60

秘密鍵の保護	60
はじめに	60
FAS証明書とテンプレートに関する情報	61
FAS承認証明書	62
FASユーザー証明書	63
秘密鍵の保存オプション	63
キー構成PowerShellコマンド	64
構成シナリオの例	69
例1 - すべてのキーをMicrosoft Software Key Storage Providerに保存する	70
例 2 - 認証証明書キーを TPM に保存する	70
例 3 - すべてのキーを HSM に保存する	70
例 4 - 楕円曲線キーを使用する	71
秘密キー構成のテスト	72
FAS証明書の検査	72
承認証明書の検査	72
ユーザー証明書の検査	73
Citrix Virtual Apps and Desktops 2411より前のFASバージョンからのアップグレード	74
暗号化リモート処理	77
KSPリモート処理の無効化	78
メンテナンスモード	78
管理コンソールの使用	78
PowerShellの使用	79
関連情報	79
セキュリティとネットワーク構成	79
ネットワークアーキテクチャ	79
ファイアウォールとネットワークセキュリティ	80
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	81
セキュリティに関する考慮事項	82

委任された登録エージェント	82
アクセス制御リストの構成	82
ファイアウォール設定	82
イベントログの監視	83
ハードウェアセキュリティモジュール	83
管理者の責任	83
グループポリシー設定	83
証明書テンプレート	84
証明書テンプレートの名前を変更する	84
全般プロパティを変更する	84
要求処理プロパティを変更する	85
暗号化プロパティを変更する	85
キー構成証明プロパティの変更	85
廃止されたテンプレートプロパティの変更	85
拡張プロパティの変更	85
セキュリティプロパティの変更	85
サブジェクト名プロパティの変更	86
サーバープロパティの変更	86
発行要件プロパティの変更	86
互換性プロパティの変更	87
証明機関の管理	87
テンプレートの公開	87
ファイアウォール設定	88
登録の制限	88
ポリシーモジュールと監査	88
FAS管理	88
ACLを介したStoreFront、ユーザー、およびVDAの制限	89
ルールの構成	89

証明機関とテンプレートの構成	89
セッション内証明書と認証証明書	90
秘密鍵の保護と鍵長	90
イベントログ	90
管理アクセスと管理ツール	90
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	90
一般的なWindowsサーバーのセキュリティ	91
関連情報	91
パフォーマンスカウンター	91
Windows ログオンの問題のトラブルシューティング	93
証明書と公開鍵基盤	93
UPN名と証明書のマッピング	94
Active DirectoryにおけるUPN名	94
証明書マッピングサービス	95
ログオン ドメインコントローラーの選択を制御する	95
ドメインコントローラーの選択を制御する	95
使用中のドメインコントローラーを特定する	96
アカウント監査イベントを有効にする	96
証明書検証ログ	96
証明書の有効性を確認する	96
CAPIログを有効にする	96
CAPIログ	97
エラーメッセージ	97
Kerberosログ	98
ドメインコントローラーとワークステーションログ	98
ドメインコントローラー CAPI2 ログ	99
ドメインコントローラー セキュリティログ	99

VDA セキュリティログ	99
VDA CAPIログ	100
VDAシステムログ	100
Windowsイベントログを使用したFASの監視	100
FASサービスは実行中ですか？	100
FASヘルスイベント	100
クラウド接続FASイベント	102
セキュリティイベント	103
FASイベントログ	104
管理イベント	104
IDアサーションの作成	107
証明書利用者の役割を果たす	108
セッション内証明書サーバー	108
FASアサーションプラグイン	109
ワークスペース対応FAS	110
ログオン	111
セッション内証明書	112
証明書要求とキーペアの生成	112
エンドユーザーのエラーメッセージ	113
関連情報	114
PowerShell コマンドレット	114
展開アーキテクチャ	116
はじめに	116
アーキテクチャの概要	116
内部展開	117
シトリックス ゲートウェイ展開	118
ADFS SAML展開	119
B2Bアカウントマッピング	119

Windows 10 Azure AD ジョイン	120
ADFSの展開	122
はじめに	122
SAMLの概要	122
リダイレクトURL	122
識別子	123
返信アドレス	123
署名証明書	123
シングルサインアウト URL	123
構成	123
SAML ポリシーの入力	124
関連情報	124
Azure AD統合	124
はじめに	124
アーキテクチャ	126
DNSゾーンの作成	127
クラウドサービスを作成する	129
Windows仮想マシンを作成する	129
ドメインコントローラー	130
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	130
Citrix Virtual Desktops™ デリバリーコントローラー および VDA	131
内部DNSを構成する	131
外部DNSアドレスを構成する	132
セキュリティグループを構成する	132
ADFS証明書を作成する	132
Azure ADのセットアップ	133
新しいディレクトリの作成	133
グローバル管理者ユーザー (AzureAdmin) を作成する	135

ドメインを Azure AD に登録する	136
Azure AD Connect をインストールする	137
Azure AD Join を有効にする	147
Citrix Virtual AppsまたはCitrix Virtual Desktopsをインストールする	150
フェデレーション認証サービスをインストールする	151
StoreFrontを構成する	151
StoreFrontがCitrix Gatewayを使用するように構成する	152
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	153
アイコンの構成	153
SAML認証の構成	154
アプリケーションをユーザーに割り当てる	156
MyAppsページ	157
シングルサインオンURL	158
Citrix Gatewayのインストールと構成	158
Citrix Virtual Apps and Desktopsセットアップウィザードを実行する	158
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	160
StoreFrontアドレスを構成する	160
Citrix Gatewayの展開を検証する	161
Citrix Gateway SAML認証サポートを有効にする	162
エンドツーエンドシステムを検証する	162
付録	162
パブリックIPアドレスとDNSアドレスを提供する	162
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	163
関連情報	164
フェデレーション認証サービス2411ドキュメント履歴	165

フェデレーション認証サービス 2411

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。これはユーザーに証明書を動的に発行し、ユーザーが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。

フェデレーション認証サービス 2411 は、FASの最新のCurrent Releaseバージョンです。この記事では、この最新リリースにおける機能と構成について説明します。

以前のリリース

以前のFASリリースのドキュメントについては、以下を参照してください。

- [フェデレーション認証サービス 2407](#)
- [フェデレーション認証サービス 2402 LTSR](#)
- [フェデレーション認証サービス 2311](#)
- [フェデレーション認証サービス 2308](#)
- [フェデレーション認証サービス 2305](#)
- [フェデレーション認証サービス 2303](#)
- [フェデレーション認証サービス 2212](#)
- [フェデレーション認証サービス 2209](#)
- [フェデレーション認証サービス 2206](#)
- [フェデレーション認証サービス 2203 LTSR](#)
- [フェデレーション認証サービス 2112](#)
- [フェデレーション認証サービス 2109](#)
- [フェデレーション認証サービス 2106](#)
- [フェデレーション認証サービス 2103](#)
- [フェデレーション認証サービス 1912 LTSR](#)

- 「XenApp and XenDesktop 7.15 長期サービスリリース」(</ja-jp/xenapp-and-xendesktop/7-15-ltsr.html>)

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](#)に記載されています。

参照

- [Active Directory 証明書サービス概要](#)
- 「[Windows の証明書ログオンの構成](#)」

フェデレーション認証サービス 2411

ユーザーへの影響なしにFAS承認証明書を更新する

以前は、FAS承認証明書の更新はユーザーに中断を引き起こしていました。この変更により、プロセスが簡素化および改善され、ユーザーに中断を引き起こすことがなくなりました。詳細については、「[FAS承認証明書の更新](#)」を参照してください。

FASでのキーストレージ管理プロセスの改善

以前は、FAS秘密キーの保存場所の構成は、

`Citrix.Authentication.FederatedAuthenticationService.exe.config` XMLファイルを介して処理されていました。これは管理上の問題点であり、FASのアップグレード時に構成が保持されませんでした。この変更により、秘密キーの構成にはPowerShellコマンドレットが使用されます。ユーザーおよびRA証明書の秘密キーの構成は個別に保存され、さらに簡素化され、アップグレード後も保持されます。詳細については、「[秘密キーの保護](#)」を参照してください。

楕円曲線キーのサポート

これまで、FASは証明書での使用にRSAキーのみをサポートしていました。この変更により、FASはECC証明書のサポートを導入します。詳細については、「[例4 - 楕円曲線キーの使用](#)」を参照してください。

フェデレーション認証サービス KSPリモート処理 (一般提供)

この変更により、Windows VDAからFASサーバーへの暗号化操作のリモート処理は、[VDA上で実行されるキー記憶域プロバイダー \(KSP\) のペア](#)を使用して実現されます。これは、以前のバージョンのFASで使用されていた暗号化サービスプロバイダー (CSP) に代わるものです。KSPは、Windowsアプリケーションに暗号化操作を公開する最新の方法であり、より多くの機能をサポートしています。詳細については、「[KSPリモート処理](#)」を参照してください。

バグ修正については、「[修正された問題](#)」を参照してください。

修正された問題

Federated Authentication Service 2411には、修正された問題はありません。

既知の問題

FAS が EC (楕円曲線) キーでユーザー証明書を生成するように構成されている場合、以下の PowerShell コマンドは期待どおりに動作しません。

```
Test-FasCrypto
```

```
Test-FasUserCertificateCrypto
```

これらのコマンドは、暗号化証明書とユーザー証明書が正常であっても、常に失敗応答を返します。

第三者通知

このFederated Authentication Service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た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。

- シトリックス仮想アプリおよびデスクトップ サードパーティ通知 (PDFダウンロード)
- FlexNet Publisher 2017 (11.15.0.0) 用 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 2025、Standard および Datacenter エディション
 - Windows Server 2022、Standard および Datacenter エディション
 - 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
- Citrix では、他の Citrix コンポーネントがインストールされていないサーバーに FAS をインストールすることをお勧めします。
- Windows Server は、登録機関証明書と秘密キーにアクセスできるため、セキュリティで保護する必要があります。証明書と秘密キーにより、サーバーはドメインユーザーの証明書を発行できます。サーバーは、発行されたドメイン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 証明機関またはその他の検証済み証明機関 (CA) が必要です。以下の非 Microsoft PKI プロバイダーは、FAS で使用するためのソリューションを検証済みです。これらの検証に関するサポートについては、ベンダーにお問い合わせください。
 - キーファクター コマンド
 - セクティゴ サーティフィケート マネージャー
 - ベナフィ ゼロタッチ PKI
 - HDI PKIaaS (ベナフィ)
 - エントラスト WNES
 - AppViewX
 - エバートラスト ホライズン CLM

- オープントラスト PKI
- アイディーノミック PKI-3
- デジサート 自動登録サーバー
- Microsoft以外のCAでFASを使用する場合のサポートとガイダンスについては、関連するPKIプロバイダーにお問い合わせください。
- Microsoft以外の認証局の場合、以下を確認してください。
 - 認証局 (CA) は、登録サービスとしてActive Directoryに登録されている必要があります。
 - CA証明書は、ドメインコントローラーのNTAuthストアにあります。詳細については、[Enterprise NTAuthストアにサードパーティの認証局 \(CA\) 証明書をインポートする方法](#)を参照してください。
- 詳細については、[展開ガイド：Citrix Federated Authentication ServiceとSectigo MS Agent](#)を参照してください。

Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトでは：

- 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。

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 (FAS) をインストールする
2. StoreFrontストアでFASプラグインを有効にする
3. Delivery Controllerを構成する
4. グループポリシーを構成する
5. FAS管理コンソールを使用して、次の操作を行います。
 - a. 証明書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
 - c. FASが証明機関を使用することを承認する
 - d. ルールを構成する
 - e. FASをCitrix Cloudに接続する (オプション)

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ではフェデレーション認証サービス (FAS) を専用サーバーにインストールすることをお勧めします。このサーバーは、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する必要があります。FASは、次のいずれかの方法でインストールできます。

- Citrix Virtual Apps and Desktops™ インストーラー (ISO挿入時の自動実行スプラッシュ画面にある**Federated Authentication Service**ボタンから)、または
- スタンドアロンFASインストーラーファイル (Citrix DownloadsでMSIファイルとして入手可能)。

これらは以下のコンポーネントをインストールします。

- フェデレーション認証サービス
- 高度なFAS構成のための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)

- 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

FASのアップグレード

インプレースアップグレードを使用して、FASを新しいバージョンにアップグレードできます。アップグレードする前に、次の点を考慮してください。

- 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。
- FASをアップグレードする前に、FAS管理コンソールを閉じてください。
- 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。

アップグレードを開始するには、Citrix Virtual Apps and DesktopsインストーラーまたはスタンドアロンFASインストーラーファイルからFASをインストールします。

StoreFrontストアでFASプラグインを有効にする

注記:

Citrix CloudのみでFASを使用している場合は、この手順は不要です。

StoreFrontストアでFASプラグインを有効にする方法の詳細については、<https://docs.citrix.com/ja-jp/storefront/current-release/configure-authentication-and-delegation/fas>を参照してください。

Delivery Controller™を構成する

注記:

Citrix CloudのみでFASを使用している場合は、この手順は不要です。

FASを使用するには、Citrix Virtual AppsまたはCitrix Virtual Desktops™ Delivery Controllerが接続先のStoreFrontサーバーを信頼するように構成します。これには、**Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** PowerShellコマンドレットを実行します。このコマンドは、サイト内のDelivery Controllerの数に関係なく、サイトごとに1回実行します。

グループポリシーを構成する

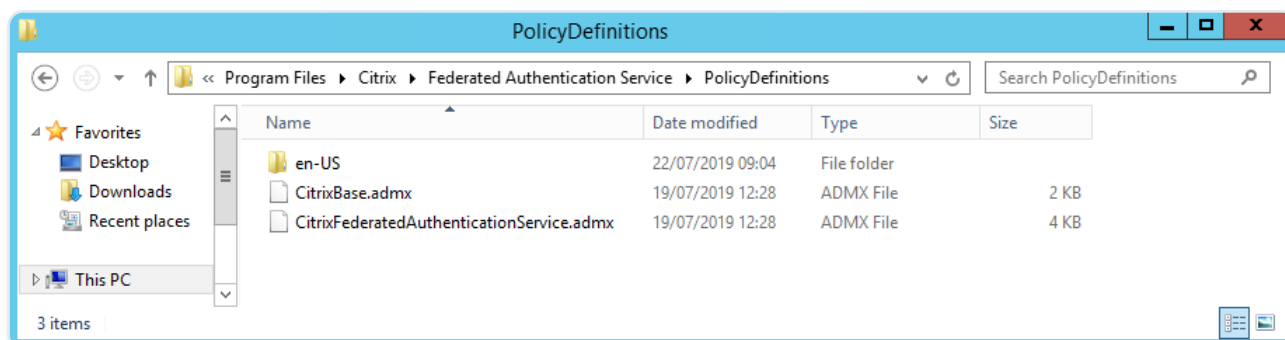
FASをインストールした後、インストールで提供されるグループポリシーテンプレートを使用して、グループポリシー内のサーバーの完全修飾ドメイン名（FQDN）を指定します。

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、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を含め、FQDNの同一の構成を持つことを確認してください。

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ドメインレベルで単一のポリシーを構成します。ただし、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FQDNのリストを参照している限り、FASは機能します。手順6を参照してください。

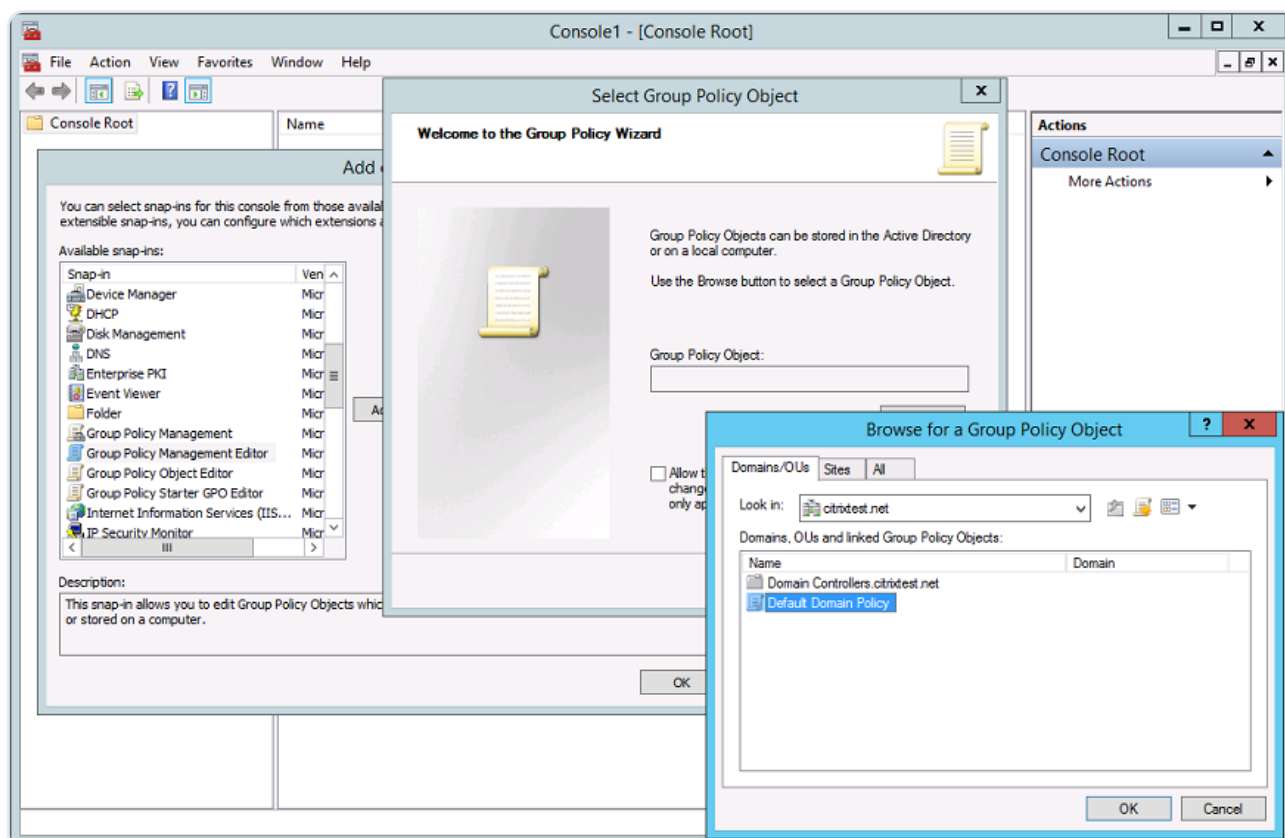
手順1. FASをインストールしたサーバーで、C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx および CitrixBase.admx ファイル、および en-US フォルダーを見つけます。



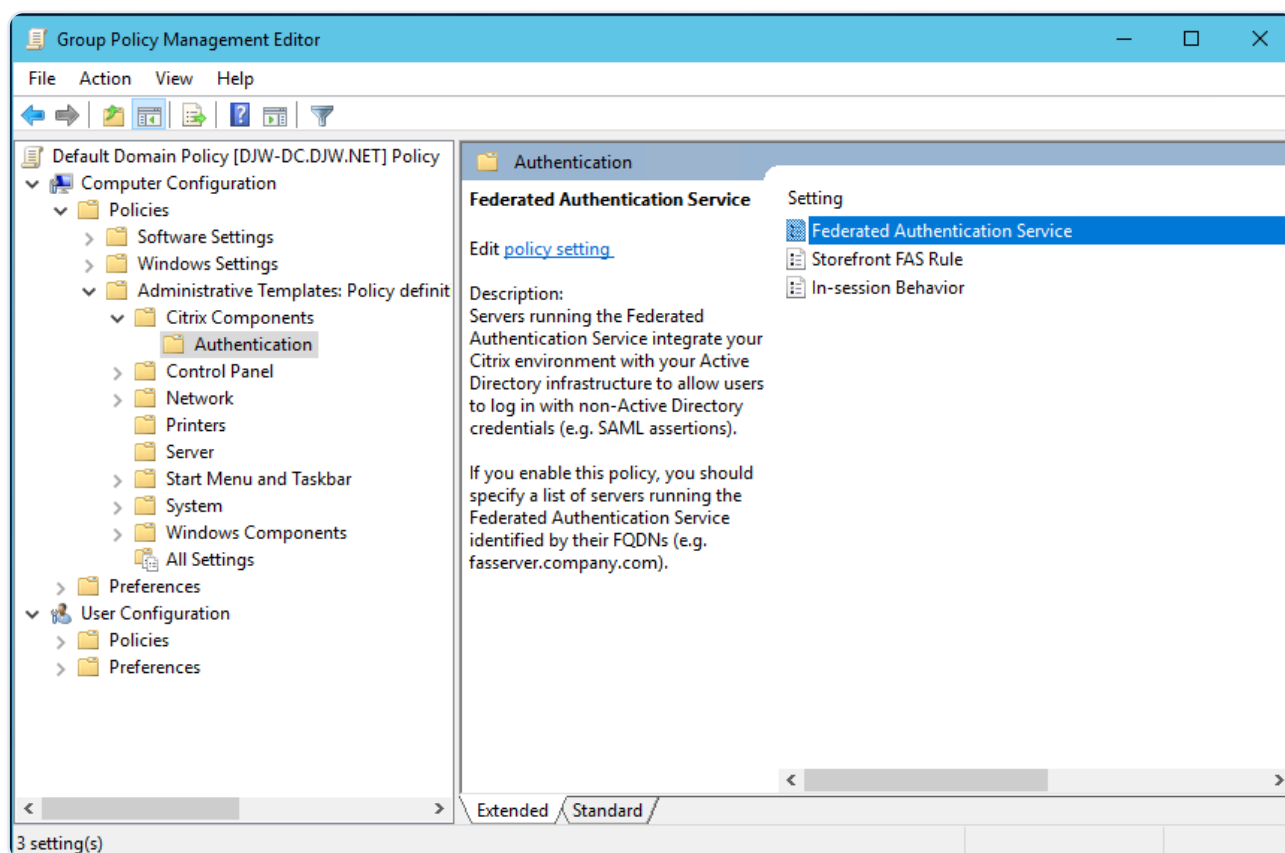
手順2. これらのファイルをドメインコントローラーにコピーし、C:\Windows\PolicyDefinitionsおよびen-USサブフォルダーに配置します。

ステップ 3. Microsoft Management Console (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、>を選択します。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、を選択し、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。



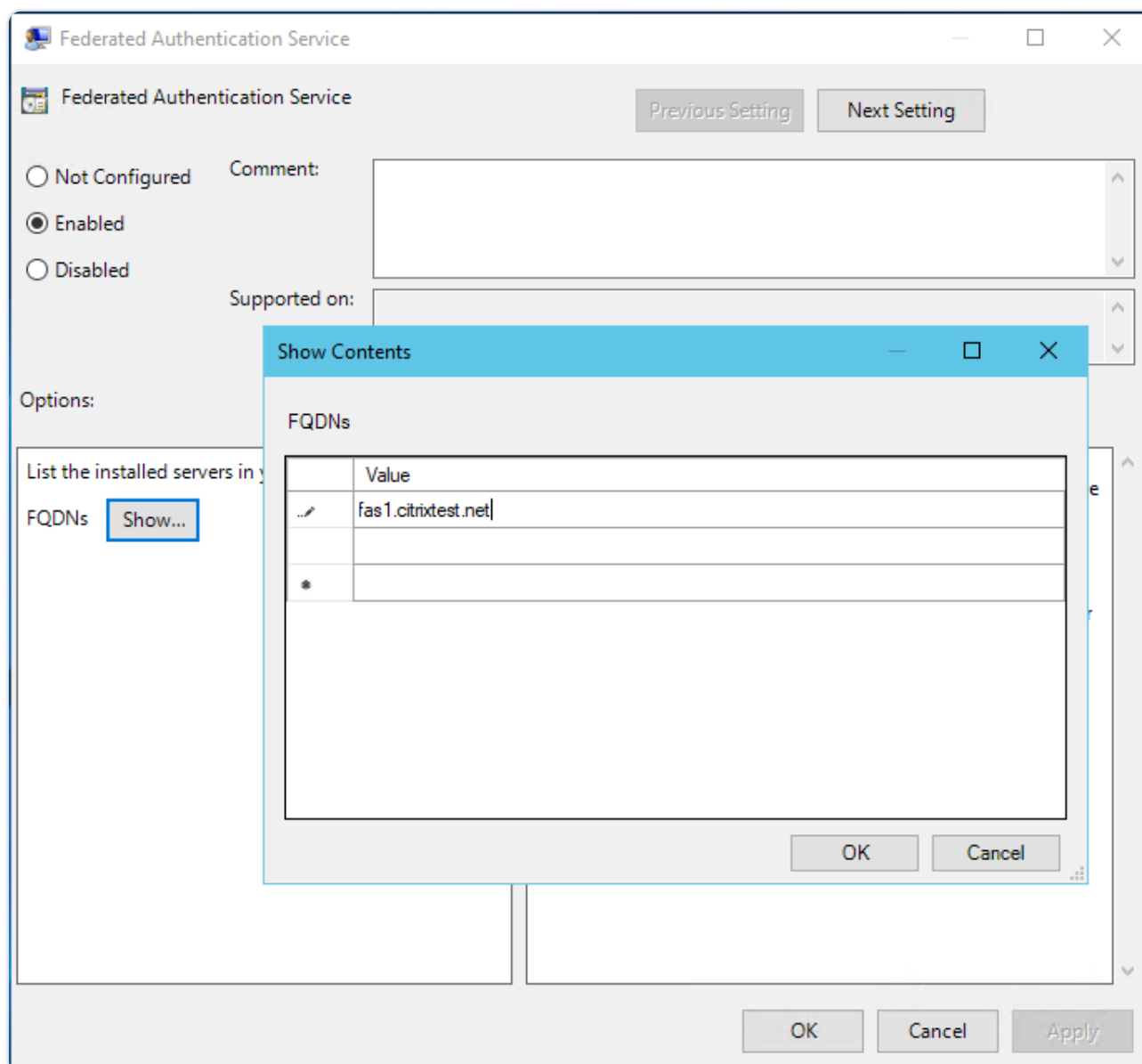
ステップ 4. コンピューターの構成/ポリシー/管理用テンプレート/Citrixコンポーネント/認証にある *Federated Authentication Service* ポリシーに移動します。



注記：

Federated Authentication Serviceポリシー設定は、CitrixBase.admx/CitrixBase.admlテンプレートファイルをPolicyDefinitionsフォルダーに追加した場合にのみ、ドメインGPOで利用できます。ステップ3の後、Federated Authentication Serviceポリシー設定は、>>フォルダーに表示されます。

ステップ 5. Federated Authentication Serviceポリシーを開き、 を選択します。これにより、 ボタンを選択できるようになり、FASサーバーのFQDNを構成できます。



ステップ 6. FASサーバーのFQDNを入力します。

重要：

複数のFQDNを入力する場合、VDA、StoreFrontサーバー（存在する場合）、およびFASサーバーから見て、リストの順序は一貫している必要があります。[グループポリシー設定](#)を参照してください。

ステップ 7. 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。

セッション内の動作

このポリシーは、ユーザーのVDAセッションでエージェントプロセスをアクティブ化し、セッション内証明書、同意、およびロック時の切断をサポートします。セッション内証明書は、このポリシーが有効になっており、かつ証明書の作成に使用されたFASルールでセッション内使用が許可されている場合にのみ利用できます。[ルールの構成](#)を参照してください。

In-session Behavior

Previous Setting Next Setting

☐ Not Configured Comment:
☒ Enabled
☐ Disabled

Supported on:

Options:

Prompt Scope: Per-process

Consent timeout (seconds): 30

☒ Disconnect on lock

Help:

Enabling this policy activates an agent process (Citrix.Authentication.VirtualSmartcard.exe) which runs inside the user's VDA session. This agent process provides support for the following functionality:

- In-session Certificates
- Disconnect-on-lock

In-session Certificates:

Certificates and private keys securely managed by the Federated Authentication Service can be made available to programs running in a user's VDA session.

Note that an in-session certificate is only available if this policy is enabled AND if the FAS rule used to create the certificate has in-session use allowed.

Most deployments do NOT need to use in-session certificates, because FAS performs a full Active Directory login to the VDA,

OK Cancel Apply

有効にすると、このポリシーが有効になり、FASエージェントプロセスがユーザーのVDAセッションで実行できるようになります。

無効にすると、このポリシーが無効になり、FASエージェントプロセスが実行されなくなります。

プロンプトの範囲

このポリシーが有効な場合、**プロンプトの範囲**は、アプリケーションがセッション内証明書を使用することを許可するための同意をユーザーに求める方法を制御します。次の3つのオプションがあります。

- **同意不要**—このオプションはセキュリティプロンプトを無効にし、秘密鍵はサイレントに使用されます。
- **プロセスごとの同意**—実行中の各プログラムが個別に同意を求めます。

- **セッションごとの同意**—ユーザーが**OK**をクリックすると、このオプションはセッション内のすべてのプログラムに適用されます。

同意のタイムアウト

このポリシーが有効な場合、**同意のタイムアウト**は、同意が持続する時間（秒単位）を制御します。たとえば、300秒の場合、ユーザーは5分ごとにプロンプトを表示されます。値がゼロの場合、すべての秘密鍵操作に対してユーザーにプロンプトが表示されます。

ロック時の切断

このポリシーが有効な場合、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。この動作は、「スマートカード取り外し時の切断」ポリシーに似ています。ユーザーがActive Directoryログオン資格情報を持っていない場合に、この機能を使用します。

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。

フェデレーション認証サービス管理コンソールの使用

注：

FAS管理コンソールはほとんどの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。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。

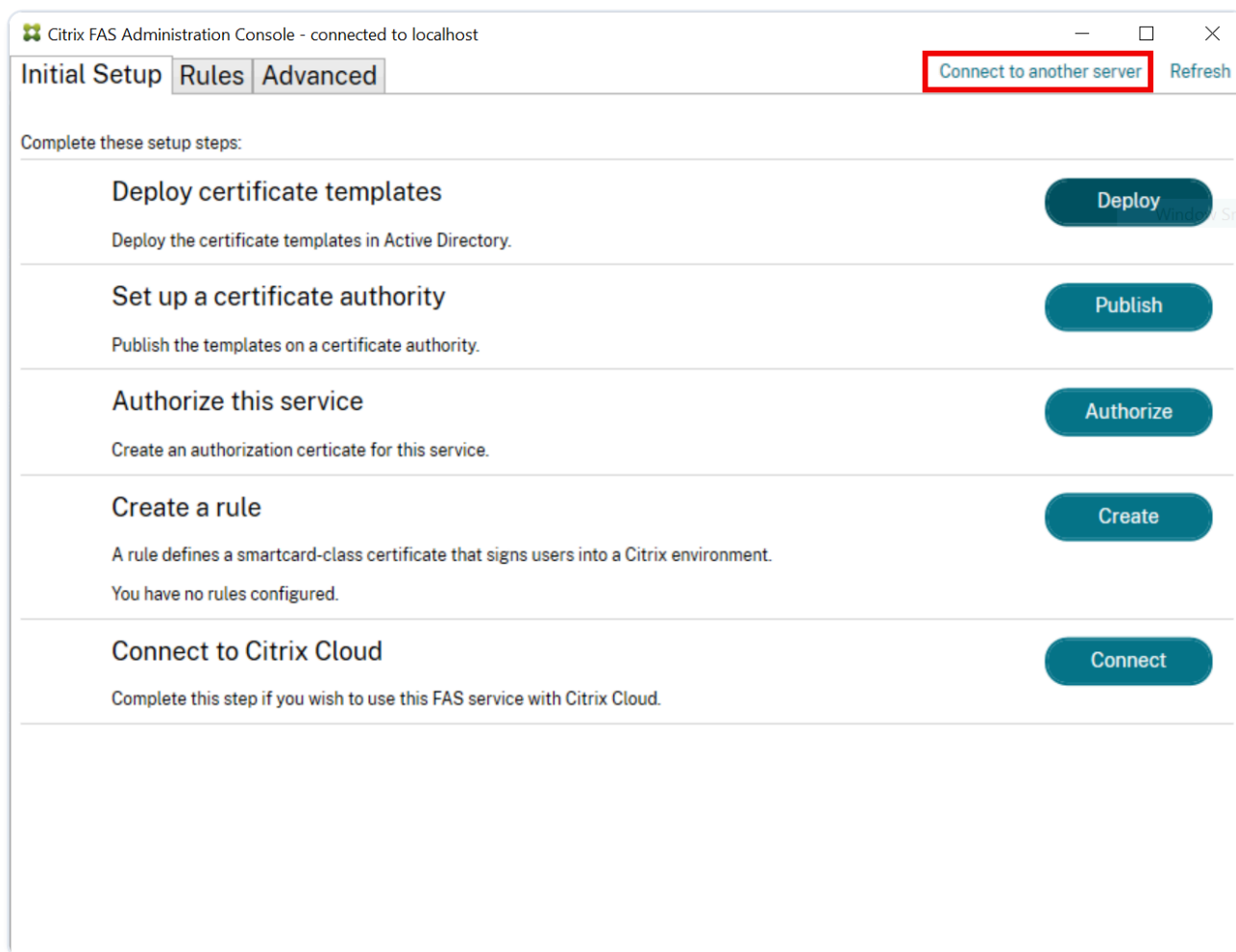
FAS管理コンソールはFASの一部としてインストールされます。アイコン（Citrix Federated Authentication Service）がスタートメニューに配置されます。

管理コンソールを初めて使用するときは、次のプロセスを実行するようにガイドされます。

- 証明書テンプレートを展開します。
- 証明機関をセットアップします。
- FASが証明機関を使用することを承認します。

OS構成ツールを使用して、一部の手順を手動で完了することもできます。

FAS管理コンソールは、デフォルトでローカルのFASサービスに接続します。必要に応じて、コンソールの右上にある**Connect to another server**を使用してリモートサービスに接続できます。

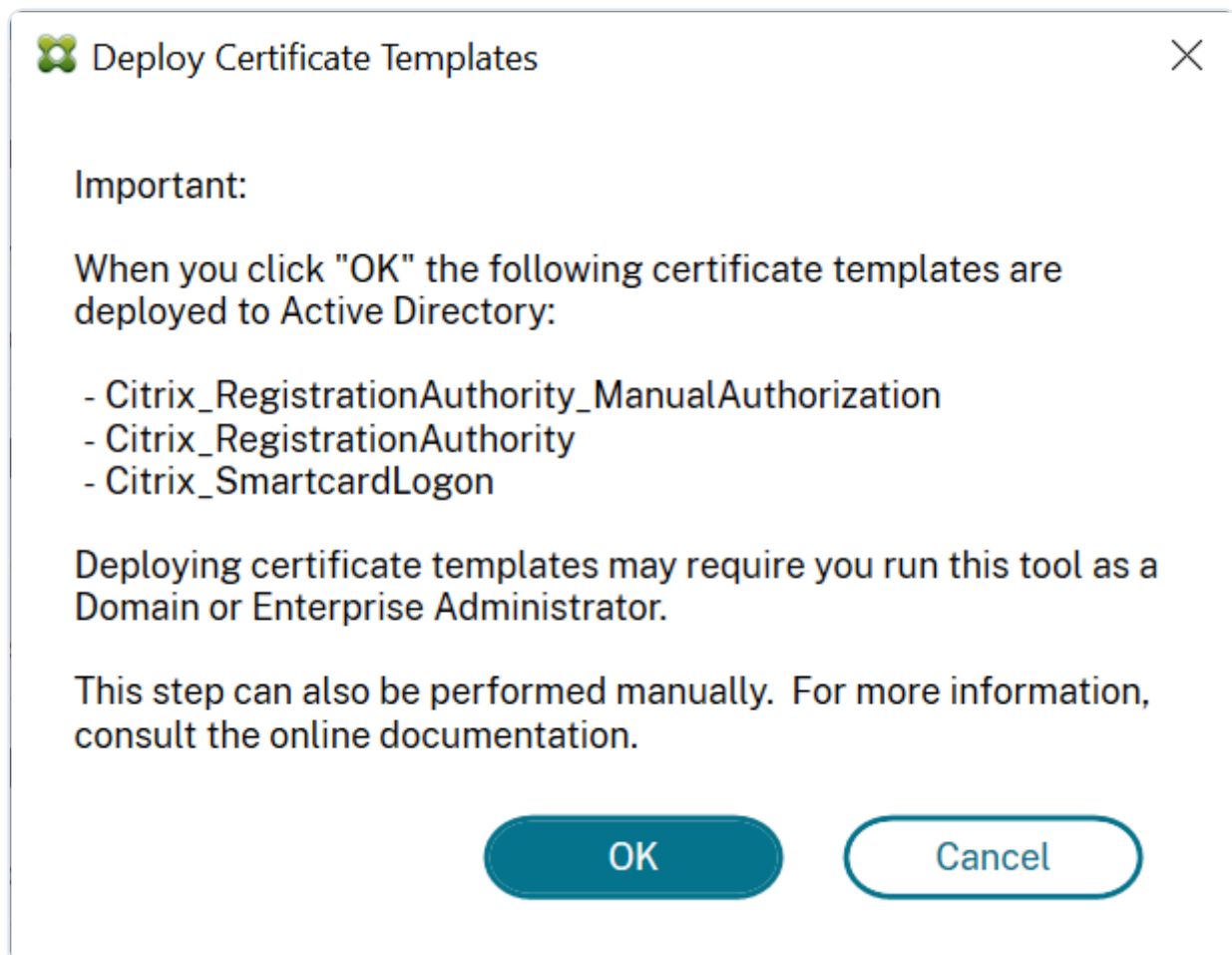


証明書テンプレートを展開する

他のソフトウェアとの相互運用性の問題を回避するため、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。「展開」ボタンをクリックし、「OK」をクリックします。



テンプレートの構成は、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。

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

This PC > OS (C:) > Program Files > Citrix > Federated Authentication Service > CertificateTemplates				
Name	Date modified	Type	Size	
Citrix_RegistrationAuthority.certificatetemplate	2/10/2020 5:25 AM	CERTIFICATETEM...	6 KB	
Citrix_RegistrationAuthority_ManualAuthorization.certificatetemplate	2/10/2020 5:25 AM	CERTIFICATETEM...	7 KB	
Citrix_SmartcardLogon.certificatetemplate	2/10/2020 5:25 AM	CERTIFICATETEM...	5 KB	

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、テンプレートを含むフォルダーから次のPowerShellコマンドを実行します。

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

$CertEnrol = New-Object -ComObject
```

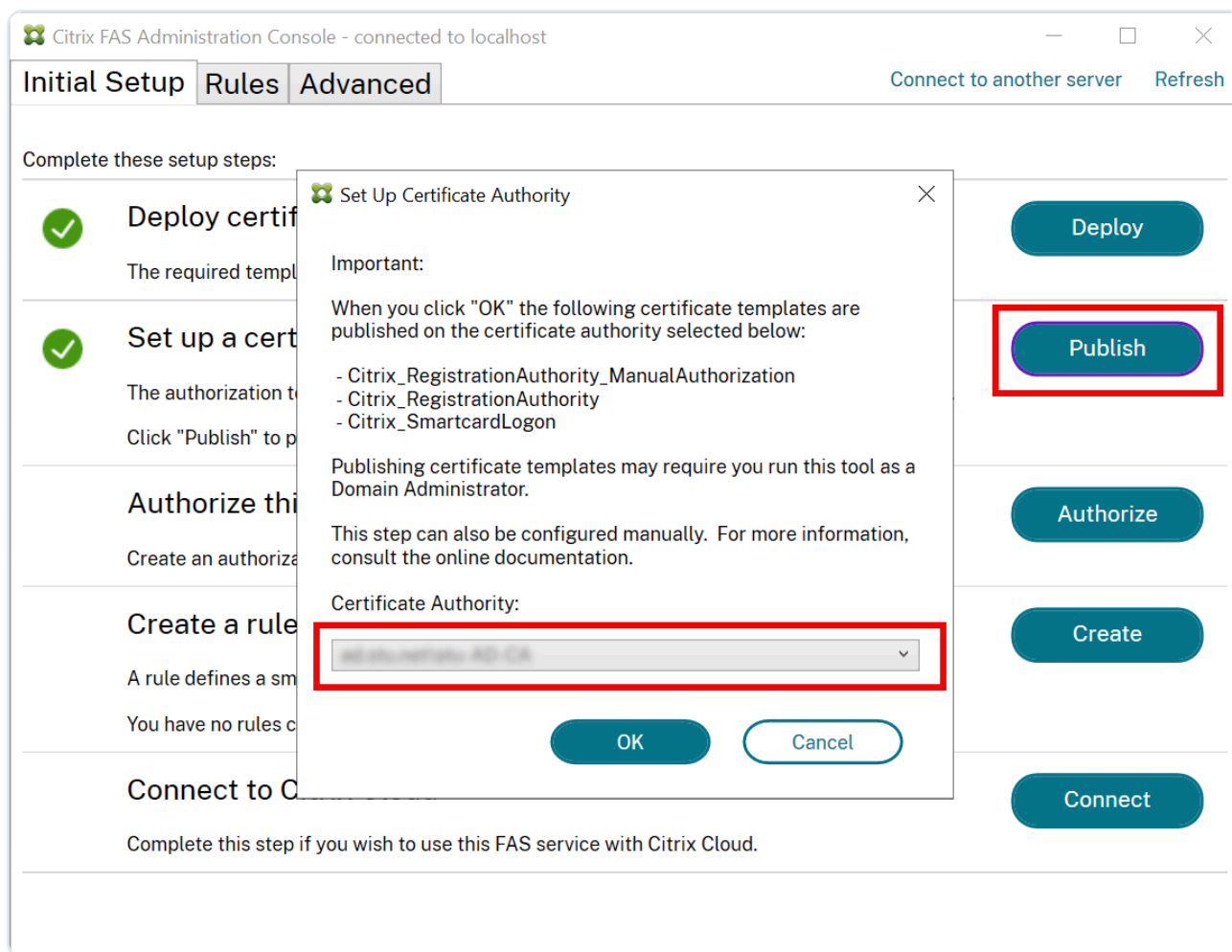
```
X509Enrollment.CX509EnrollmentPolicyWebService  
  
$CertEnrol.InitializeImport($template)  
  
$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)  
  
$writabletemplate = New-Object -ComObject  
X509Enrollment.CX509CertificateTemplateADWritable  
  
$writabletemplate.Initialize($comtemplate)  
  
$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、それらを1つ以上のMicrosoft Enterprise証明機関サーバーに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。

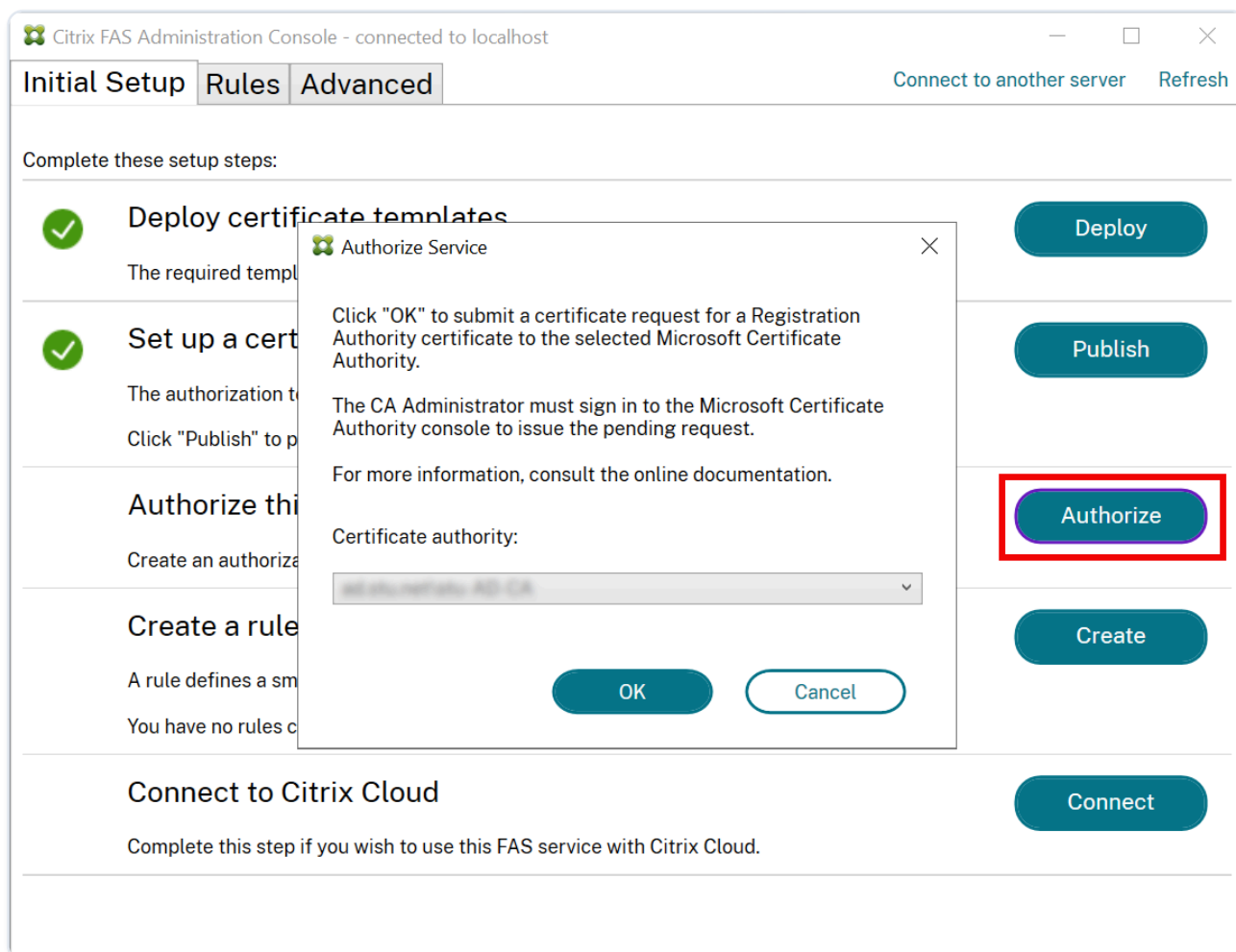
証明機関を管理する権限を持つユーザーは、少なくとも1つのサーバーにテンプレートを公開する必要があります。「**証明機関のセットアップ**」を使用して公開します。

(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

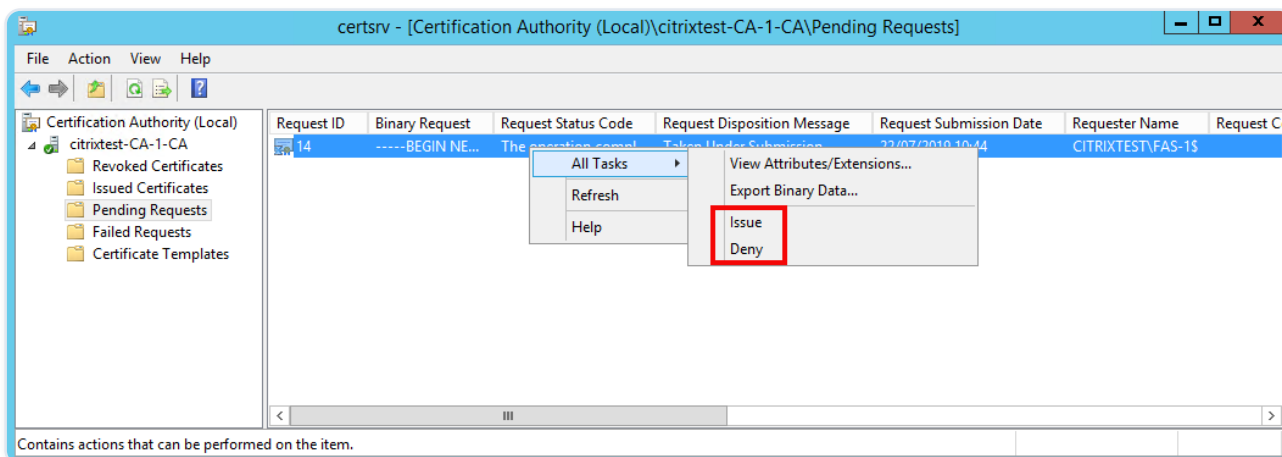
この手順により、FASの承認が開始されます。管理コンソールは、Citrix_RegistrationAuthority_ManualAuthorizationテンプレートを使用して証明書要求を生成し、そのテンプレートを公開している証明機関のいずれかに送信します。



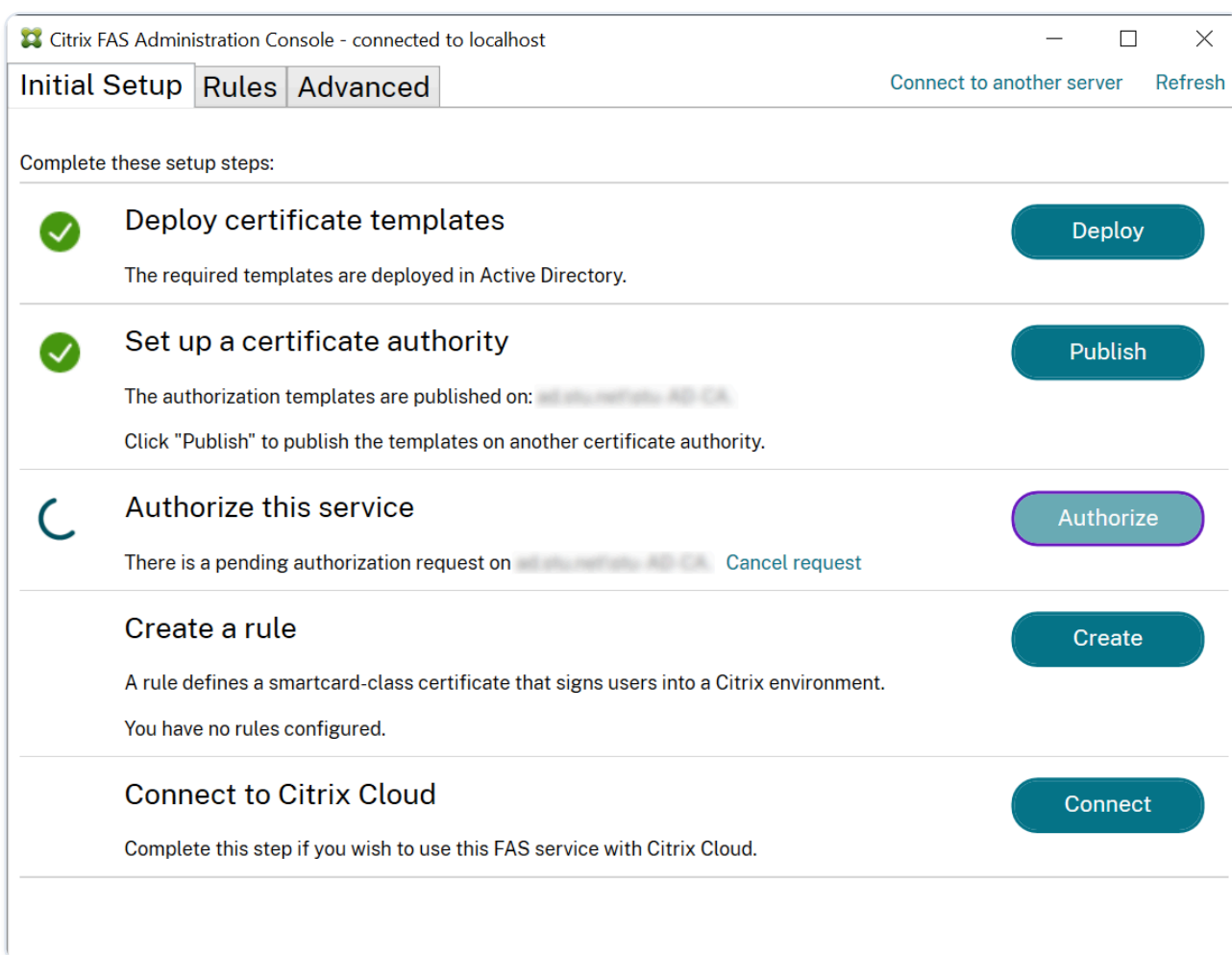
リクエストが送信されると、Microsoft Certification Authorityコンソールの保留中のリクエストリストに、FASマシンアカウントからの保留中のリクエストとして表示されます。FASの構成を続行する前に、証明機関管理者がそのリクエストを発行または拒否する必要があります。

管理者が**発行**または**拒否**を選択するまで、FAS管理コンソールはビジー状態の「スピナー」を表示します。

Microsoft Certification Authorityコンソールで、**すべてのタスク**を右クリックし、証明書リクエストに対して**発行**または**拒否**を選択します。**発行**を選択すると、FAS管理コンソールに承認証明書が表示されます。**拒否**を選択すると、コンソールにエラーメッセージが表示されます。



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。



ルールの構成

FASは、StoreFrontの指示に従い、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するためにルールを使用します。

各ルールは以下を指定します。

- 証明書を要求することが信頼されているStoreFrontサーバー。
- 証明書が要求されるユーザーのセット。
- 証明書の使用が許可されているVDAマシンのセット。

Citrixは、「default」という名前のルールを作成することを推奨します。これは、StoreFrontがFASに接続する際に、同じ名前のルールを要求するためです。

異なる証明書テンプレートや証明機関を参照し、異なるプロパティと権限を持つように構成するカスタムルールをさらに作成できます。これらのルールは、異なるStoreFrontサーバーまたはWorkspaceで使用するよう構成できます。グループポリシー構成オプションを使用して、StoreFrontサーバーがカスタムルールを名前で要求するように構成します。

作成（または「ルール」タブの**ルールの作成**）をクリックして、ルールを作成するための情報を収集するルール作成ウィザードを開始します。「ルール」タブには、各ルールの概要が表示されます。

Citrix FAS Administration Console - connected to localhost

Initial Setup Rules Advanced [Connect to another server](#) [Refresh](#)

A rule defines a smartcard-class certificate that signs users into a Citrix environment.

[+ Create rule](#)

Default	Summary
	Rule name: Default
	Status: OK
	Template: Citrix_SmartcardLogon
	Certificate authorities: ad-00000000-0000-0000-0000-000000000000 AD-CA
	Certificate available in-session: No
	Access control: Configured
	Restrictions: Not configured
	Cloud rule: No

ウィザードは次の情報を収集します。

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 ([証明書テンプレート](#)を参照)。

証明機関: ユーザー証明書を発行し、テンプレートを公開する証明機関。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。選択した証明機関のステータスが「Template available」と表示されていることを確認してください。[証明機関の管理](#)を参照してください。

セッション内での使用: セッション内での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。

- **セッション内での使用を許可**が選択されていない場合 (デフォルト、*推奨*) — 証明書はログオンまたは再接続にのみ使用され、ユーザーは認証後に証明書にアクセスできません。
- **セッション内での使用を許可**が選択されている場合 — ユーザーは認証後に証明書にアクセスできます。ほとんどのお客様は、このオプションを選択する必要はありません。イントラネットWebサイトやファイル共有など、VDAセッション内からアクセスされるリソースは、Kerberosシングルサインオンを使用してアクセスできるため、セッション内証明書は必要ありません。

セッション内での使用を許可を選択した場合、[セッション内動作グループポリシー](#)も有効にしてVDAに適用する必要があります。その後、証明書はログオン後にアプリケーションで使用するためにユーザーの個人証明書ストアに配置されます。たとえば、VDAセッション内のWebサーバーへのTLS認証が必要な場合、Internet Explorerはその証明書を使用できます。

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許可されている、信頼されたStoreFrontサーバーマシンのリスト。これらのすべての権限に対して、個々のADオブジェクトまたはグループを追加できます。

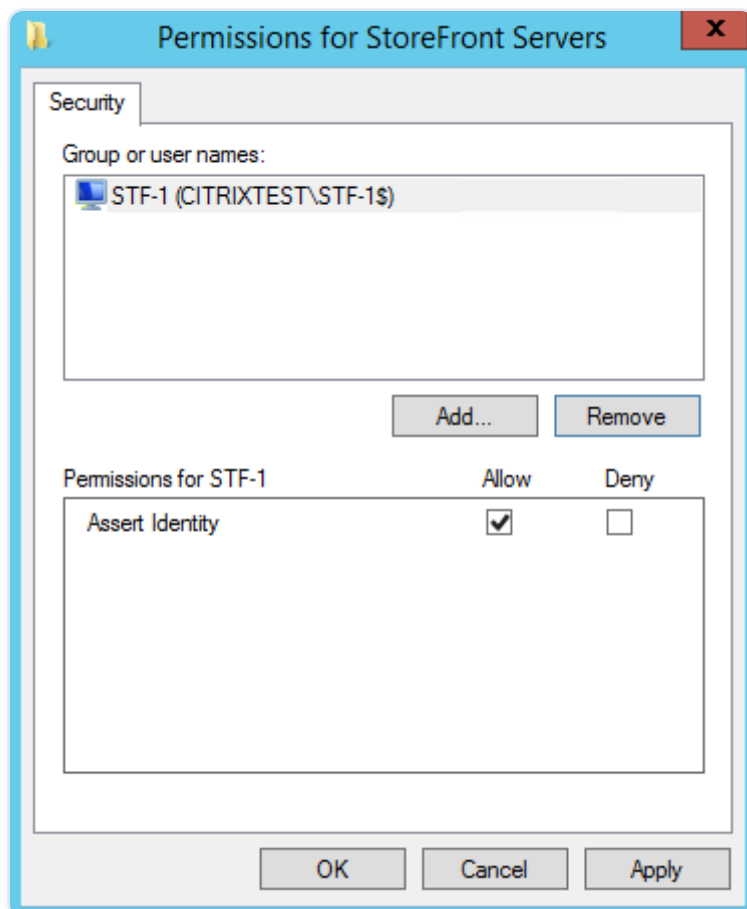
重要:

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。

注:

FASサーバーをCitrix Cloudでのみ使用している場合、アクセスコントロールを構成する必要はありません。ルールがCitrix Cloudによって使用される場合、StoreFrontのアクセス許可は無視されます。同じルールをCitrix CloudとオンプレミスのStoreFront展開の両方で使用できます。ルールがオンプレミスのStoreFrontによって使用される場合、StoreFrontのアクセス許可は引き続き適用されます。

デフォルトの権限（「Assert Identity」が許可されている）はすべてを拒否します。したがって、StoreFrontサーバーを明示的に許可する必要があります。

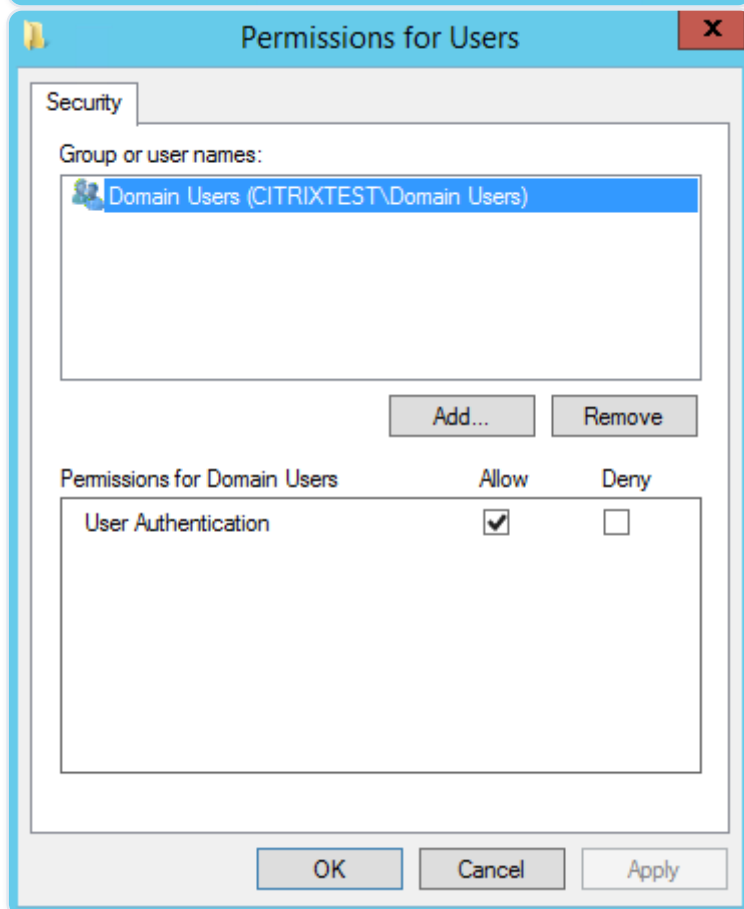
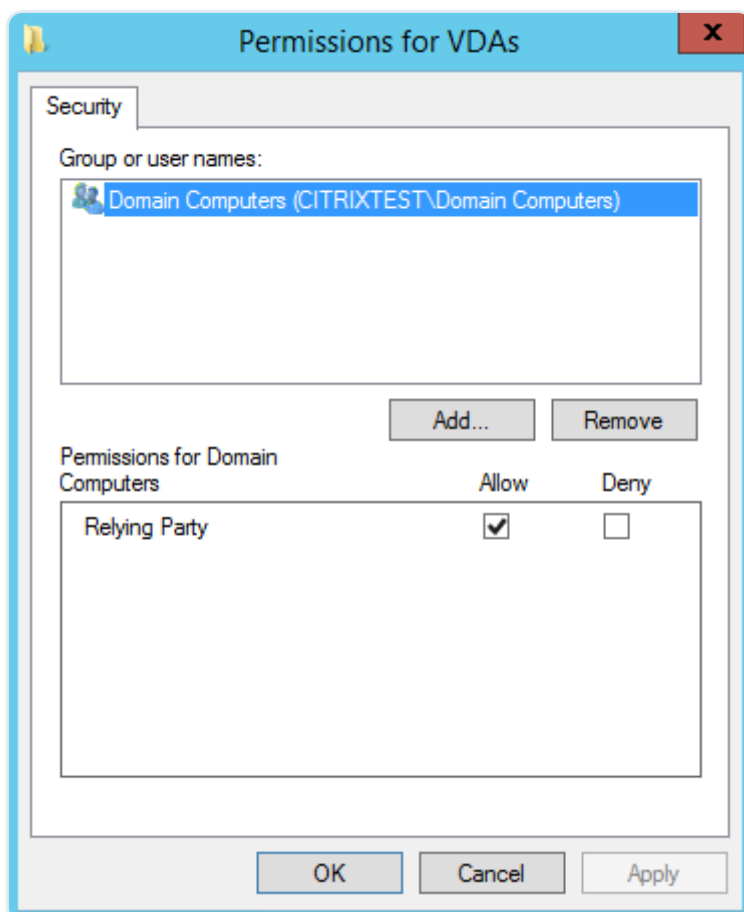


制限事項：FASを使用してユーザーをログオンできるVDAマシンのリスト、およびFASを介して証明書を発行できるユーザーのリスト。

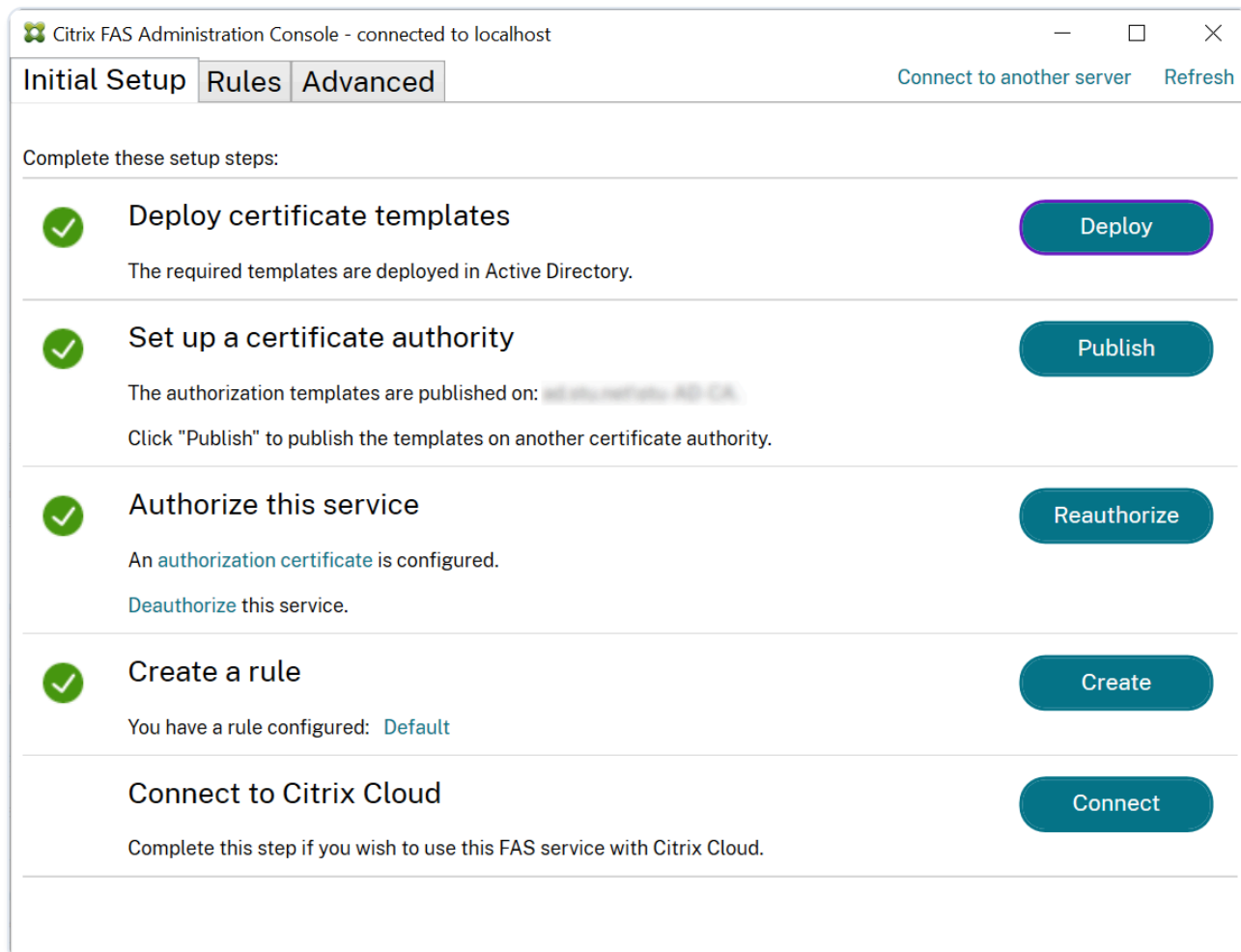
- **VDA権限の管理**では、FASを使用してユーザーをログオンできるVDAを指定できます。VDAのリストはデフォルトでDomain Computersになります。
- **ユーザー権限の管理**では、FASを使用してVDAにサインインできるユーザーを指定できます。ユーザーのリストはデフォルトでDomain Usersになります。

注：

FASサーバーのドメインがVDAおよびユーザーのドメインと異なる場合、デフォルトの制限を変更する必要があります。



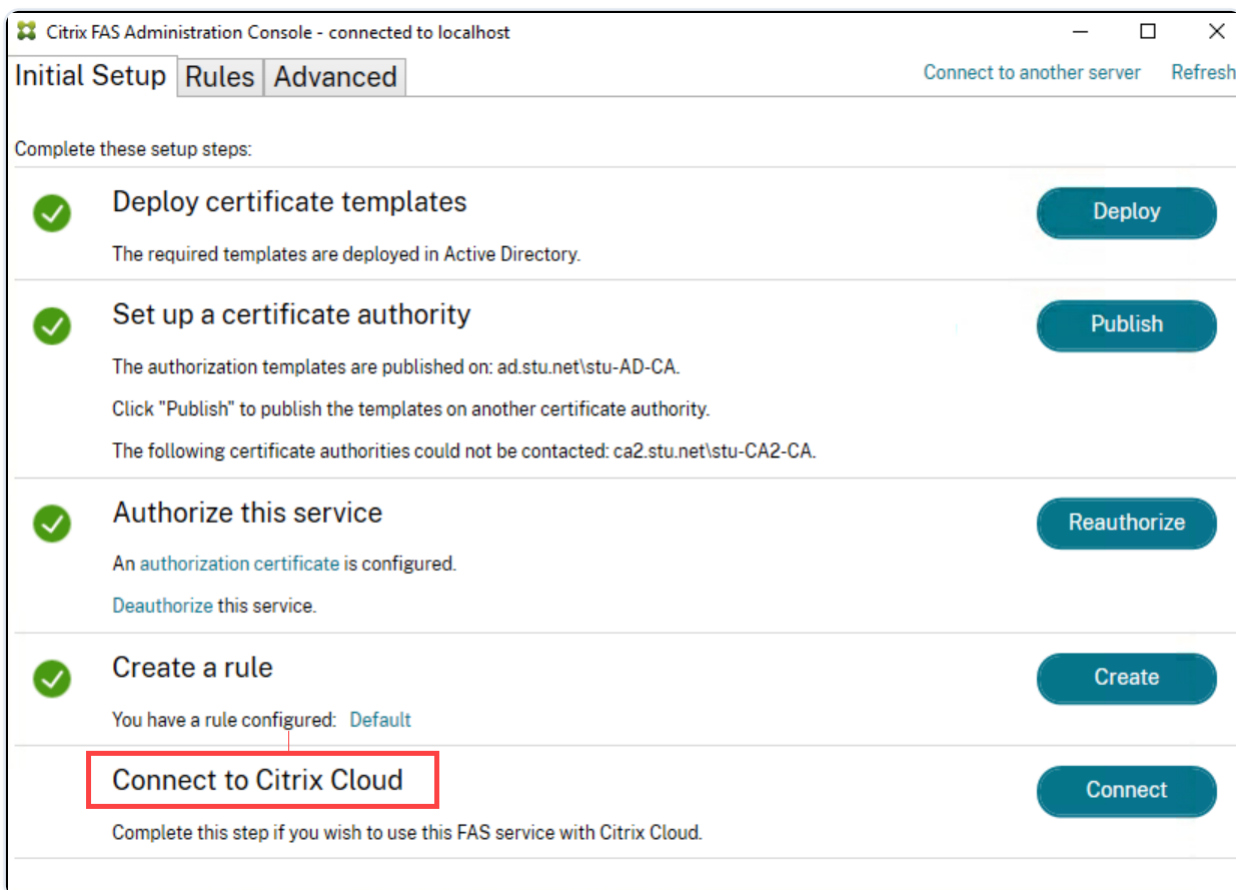
クラウド規則： Citrix WorkspaceからIDアサーションが受信されたときに規則が適用されるかどうかを示します。Citrix Cloudに接続するときに、Citrix Cloudに使用する規則を選択します。Citrix Cloudに接続した後、**Citrix Cloudへの接続**セクションのリンクから規則を変更することもできます。



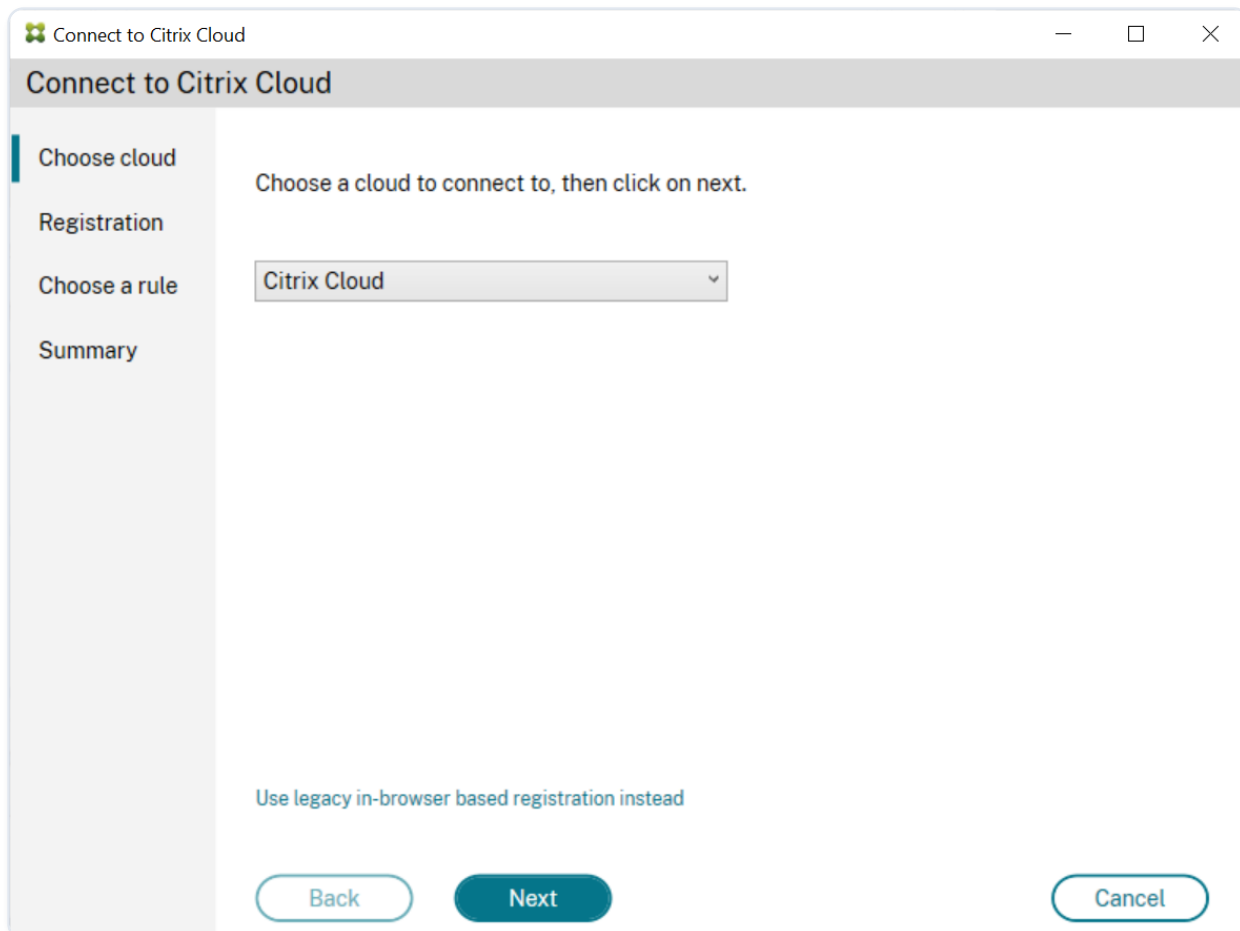
Citrix Cloudへの接続

FASサーバーをCitrix WorkspaceでCitrix Cloudに接続できます。この[Citrix Workspaceの記事](#)を参照してください。

1. 初期設定タブで、**Citrix Cloudへの接続**の下にある**接続**をクリックします。



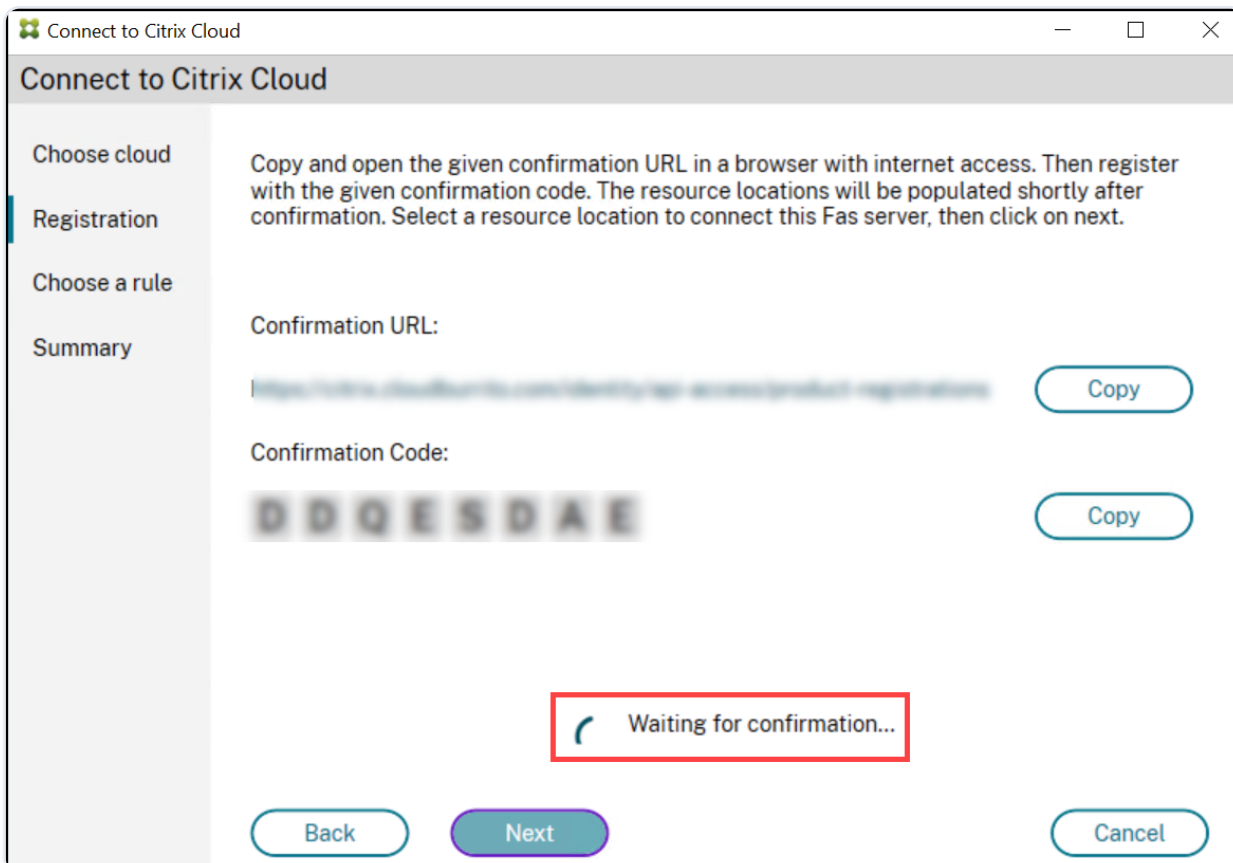
2. 接続するクラウドを選択し、次へをクリックします。



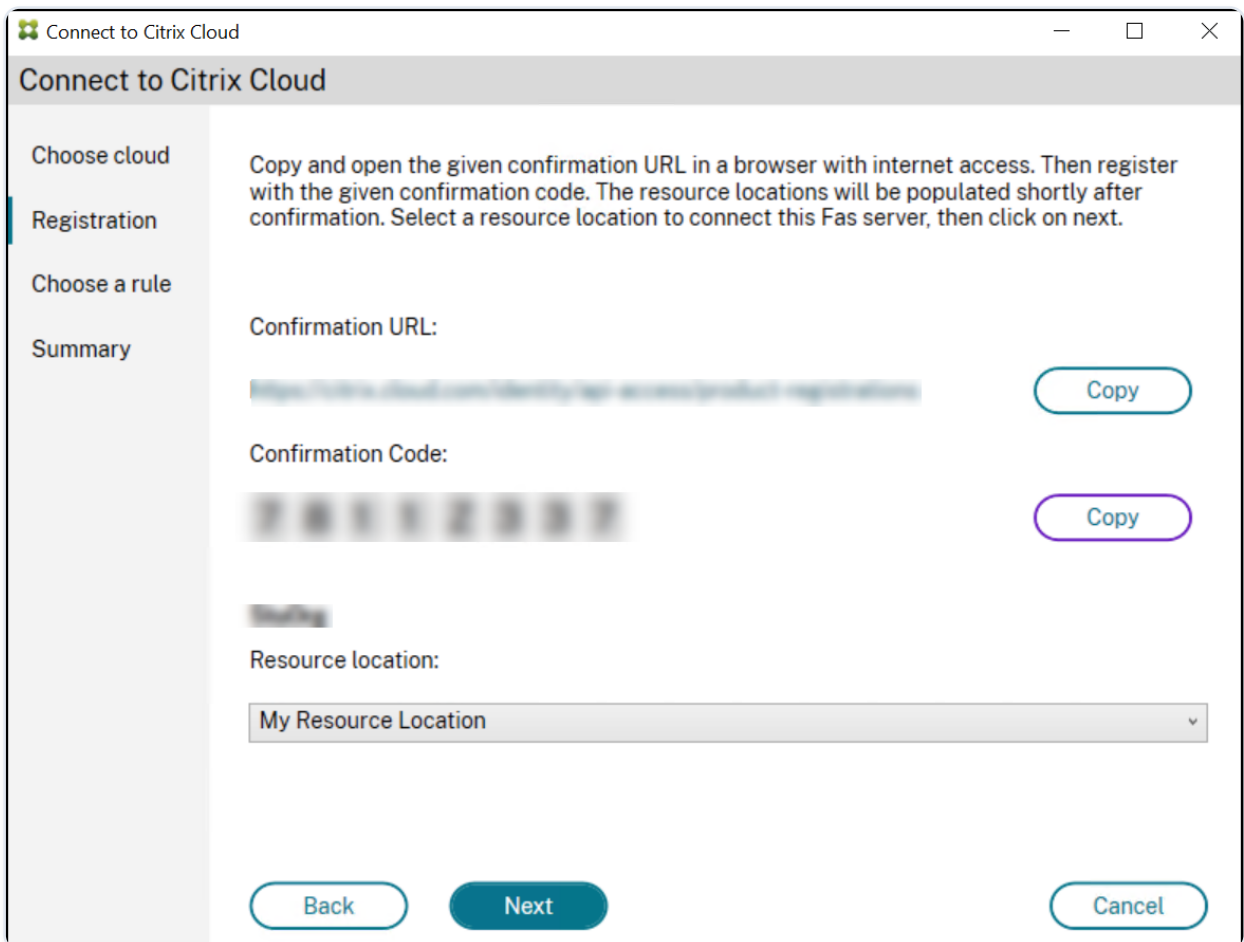
注

プレビューでは、**Citrix Cloud**のみが利用可能です。

3. ウィンドウに一意の登録コードが表示されます。これはCitrix Cloudで承認する必要があります。詳細については、「[オンプレミス製品をCitrix Cloudに登録する](#)」を参照してください。



4. 登録コードが検証されたら、ドロップダウンリストから必要なリソースの場所を選択します。



The screenshot shows a window titled "Connect to Citrix Cloud" with a sidebar on the left containing four options: "Choose cloud", "Registration" (which is selected and highlighted with a blue bar), "Choose a rule", and "Summary". The main area of the window contains the following text and controls:

Copy and open the given confirmation URL in a browser with internet access. Then register with the given confirmation code. The resource locations will be populated shortly after confirmation. Select a resource location to connect this Fas server, then click on next.

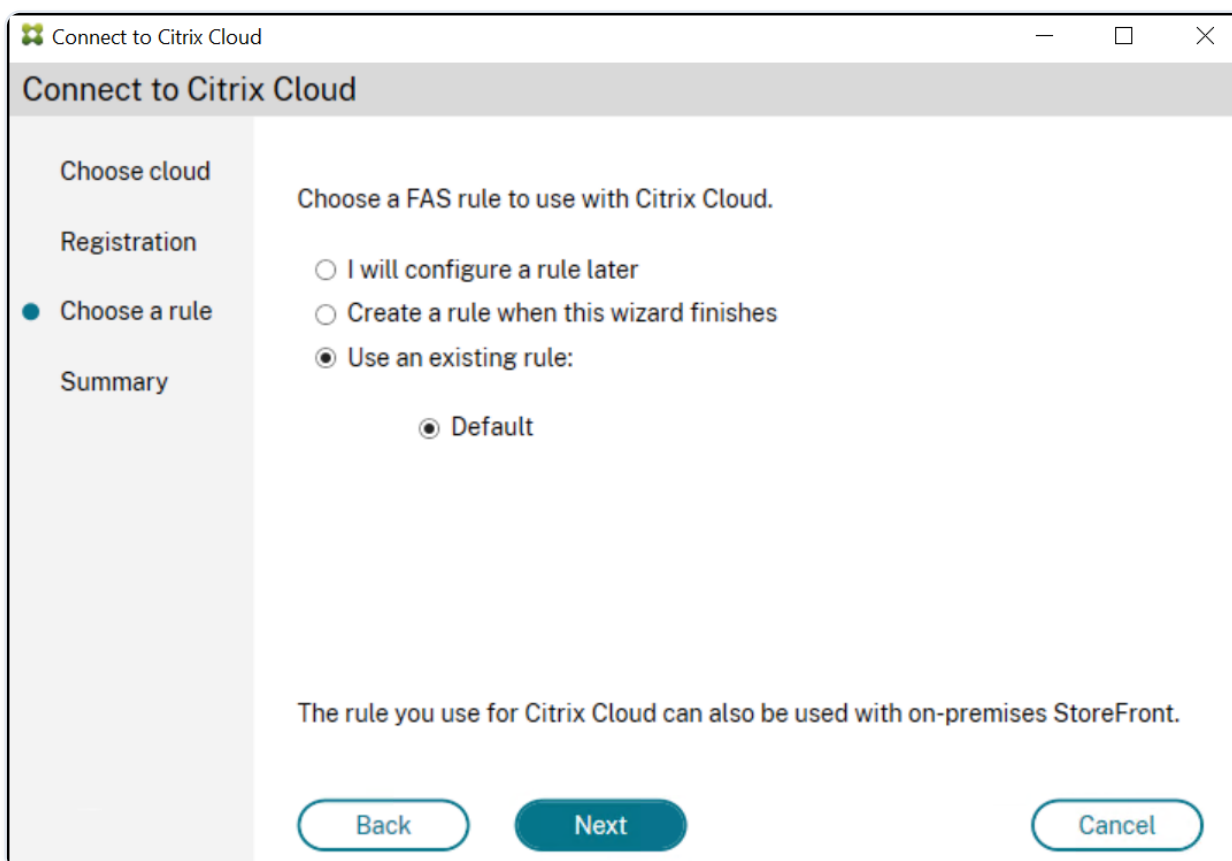
Confirmation URL:

Confirmation Code:

Resource location:

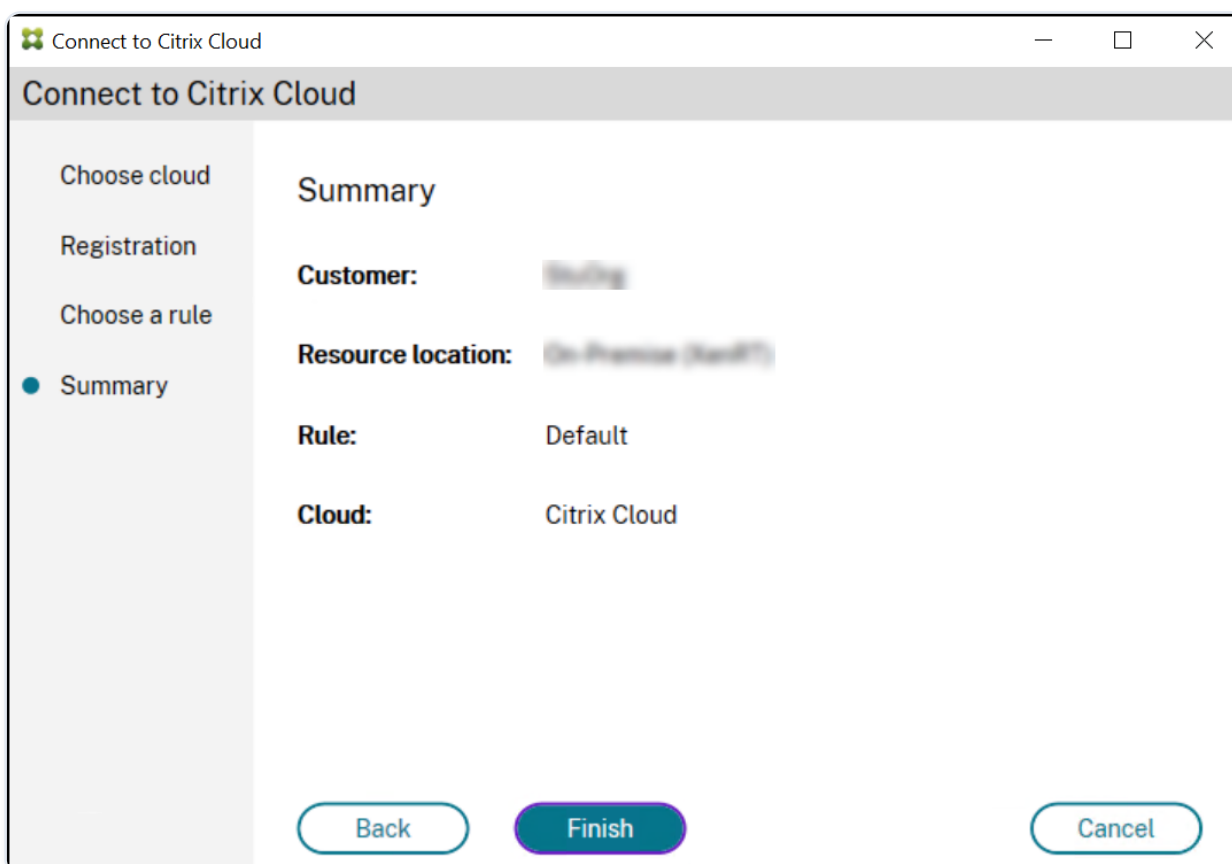
At the bottom of the window, there are three buttons: "Back", "Next" (which is highlighted in blue), and "Cancel".

5. 該当する場合は顧客アカウントを選択し、FASサーバーを接続するリソースの場所を選択します。続行をクリックし、確認ウィンドウを閉じます。
6. **ルールの選択**セクションで、既存のルールを使用するか、新しいルールを作成します。次へをクリックします。



The screenshot shows the 'Connect to Citrix Cloud' wizard window. The title bar says 'Connect to Citrix Cloud'. The left sidebar has four steps: 'Choose cloud', 'Registration', 'Choose a rule' (which is selected with a blue dot), and 'Summary'. The main area is titled 'Choose a FAS rule to use with Citrix Cloud.' and contains three radio button options: 'I will configure a rule later', 'Create a rule when this wizard finishes', and 'Use an existing rule:'. Under 'Use an existing rule:', there is a sub-option 'Default' which is selected. At the bottom, there is a note: 'The rule you use for Citrix Cloud can also be used with on-premises StoreFront.' and three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

7. 概要セクションで、完了をクリックしてCitrix Cloudへの接続を完了します。



The screenshot shows the 'Connect to Citrix Cloud' wizard window at the 'Summary' step. The left sidebar has four steps: 'Choose cloud', 'Registration', 'Choose a rule', and 'Summary' (which is selected with a blue dot). The main area is titled 'Summary' and displays four configuration items: 'Customer:' with a blurred value, 'Resource location:' with a blurred value, 'Rule:' with the value 'Default', and 'Cloud:' with the value 'Citrix Cloud'. At the bottom, there are three buttons: 'Back', 'Finish' (highlighted in blue), and 'Cancel'.

Citrix CloudはFASサーバーを登録し、Citrix Cloudアカウントの「リソースの場所」ページに表示します。

注:

オンプレミスのFASサーバーは、Citrix CloudとCitrix Virtual Apps and Desktopsへのアクセスを同時に許可するために、ユーザー証明書を発行できます。

Citrix Cloudから切断する

Citrix Cloudリソースの場所からFASサーバーを削除した後、この[Citrix Workspaceの記事](#)に記載されているように、「**Connect to Citrix Cloud**」で「**Disable**」を選択します。

高度な構成

このセクションの記事では、Federated Authentication Service (FAS) の高度な構成と管理に関する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に関する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。

テナント顧客向けフェデレーション認証サービスを有効にする

この記事では、マルチテナントのマネージドサービスプロバイダー (MSP) 環境でフェデレーション認証サービス (FAS) を有効にする手順について説明します。詳細については、「[リファレンスアーキテクチャ: Citrix Service Provider DaaS](#)」を参照してください。

前提条件

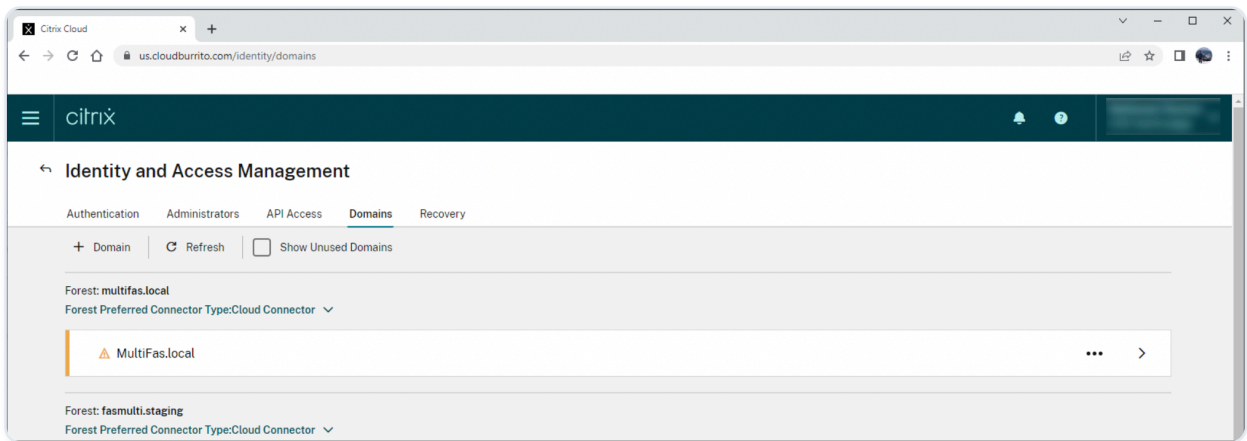
- Citrix Cloud のドメインとリソースの場所に管理者アクセス権があること。詳細については、「[管理者権限の変更](#)」を参照してください。
- テナントとMSPの関係を設定済みであること。詳細については、「[Citrix Service Provider 向け Citrix DaaS](#)」を参照してください。

MSP顧客を構成する

1. Cloud Connector を使用して、Active Directory ドメインを Citrix Cloud で利用できるようにします。

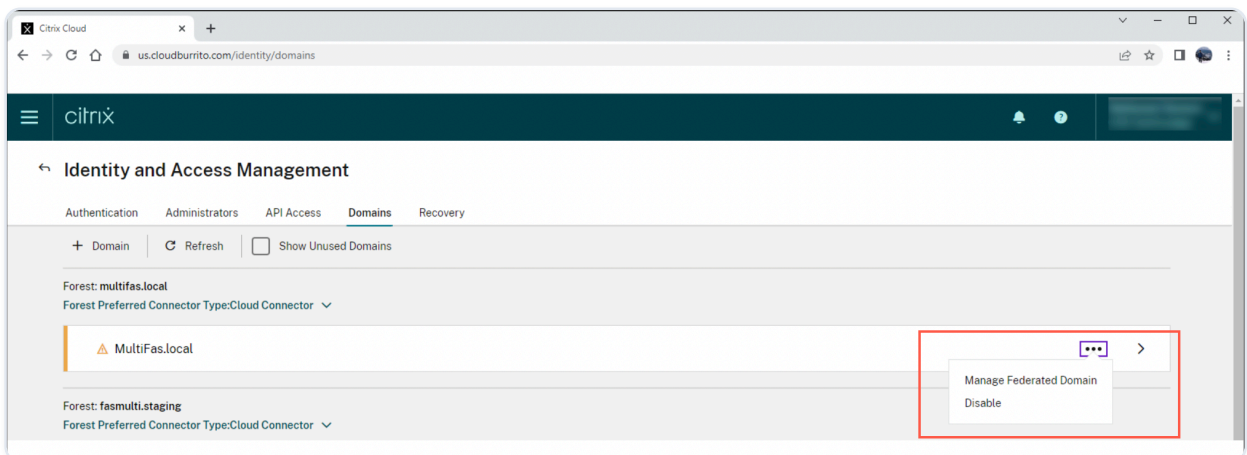
[Cloud Connector をインストールする](#) ことで、オンプレミスインフラストラクチャを Citrix Cloud に接続します。

オンプレミスドメインコントローラーに関連付けられているドメインが、> の下で利用可能であることを確認します。



2. ドメインをテナントにフェデレーションします。

ドメインを選択し、ドロップダウンメニュー (...) をクリックして、 をクリックします。



テナントを見つけて + をクリックします。その後、 をクリックします。

Add or remove customers to create a federated domain

1 available customers [Add all](#)

Search...

FAS Tenant1 with service profile. +

0 federated customers [Remove all](#)

Search...

Cancel Apply

3. 関連付けられているドメインがテナントに存在することを確認します。

この手順はオプションです。テナント顧客のコンソールにサインインし、>の下にドメインがリストされていることを確認します。

関連付けられているドメインがテナントに存在することを確認します(/en-us/federated-authentication-service/2411/media/fas-verify-domains.png)

MSP 顧客に戻ります。

4. FAS サーバーをインストールし、Citrix Cloud に登録します。

テナントの Citrix Virtual Apps and Desktops リソースが配置されている Active Directory (AD) フォレストに FAS をインストールします。FAS をその AD フォレストに関連付けられているクラウド リソースの場所に接続します。FAS サーバーをインストールするには、「[インストールと構成](#)」を参照してください。

5. テナント顧客を構成する

テナント顧客向けに FAS を有効にする

- ID プロバイダー (IdP) を構成する

テナント顧客に切り替えます。 > に移動します。 IdP に接続し、AD が IdP と同期されていることを確認します。

- テナント向けに FAS を有効にする

> に移動します。設定した認証を選択し、FAS を有効にします。

FAS テナントを有効にする(/en-us/federated-authentication-service//current-release/media/fas-enable-tenant.png)

既知の問題

テナントのフェデレーションドメインを削除する前に MSP ドメインを削除すると、既知の問題が発生します。テナント向けに FAS を有効にすることはできますが、MSP にドメインが存在しなくなるため、FAS は失敗します。

Azure Active Directory シングルサインオン

注：

2023年7月以降、MicrosoftはAzure Active Directory (Azure AD) の名称をMicrosoft Entra IDに変更しました。このドキュメントでは、Azure Active Directory、Azure AD、またはAADへの言及はすべてMicrosoft Entra IDを指します。

Citrix Federated Authentication Service (FAS) は、ドメイン参加済みVirtual Delivery Agent (VDA) へのシングルサインオン (SSO) を提供します。FASは、VDAにユーザー証明書を提供することでSSOを実現します。VDAはこの証明書を使用して、ユーザーをActive Directory (AD) に対して認証します。VDAセッションにサインオンすると、再認証なしでADリソースにアクセスできます。

Microsoft Entra ID (ME-ID) は、ADとMicrosoft Entra ID間の同期を使用して実装されるのが一般的で、これによりユーザーとコンピューターの両方にハイブリッドIDが作成されます。この記事では、FASを使用している場合に、VDAセッション内からMicrosoft Entra IDへのSSOを実現するために必要な追加の構成について説明します。これにより、ユーザーは再認証なしでMicrosoft Entra IDで保護されたアプリケーションにアクセスできます。

注：

- FASがMicrosoft Entra IDのSSOを使用するために特別な構成は必要ありません。
- FASのセッション内証明書は必要ありません。
- FASのどのバージョンでも使用できます。
- FASをサポートするVDAのどのバージョンでも使用できます。

Microsoft Entra ID SSOの技術は、次の表にまとめられています。

ME-ID認証タイプ	VDAはドメイン参加済み	VDAはハイブリッド参加済み
マネージド	ME-ID シームレス SSO を使用する	ME-ID 証明書ベース認証を使用する
Active Directory フェデレーション サービス (ADFS) とフェデレーションされている	ADFS で Windows 認証を有効にする	WS-Trust の <i>certificatemixed</i> エンドポイントが有効になっていることを確認する
サードパーティの ID プロバイダーとフェデレーションされている	サードパーティ ソリューションを使用する	サードパーティ ソリューションを使用する

- マネージド Microsoft Entra ID ドメインとは、ユーザー認証が Microsoft Entra ID で行われるドメインであり、ネイティブ Microsoft Entra ID 認証と呼ばれることもあります。
- フェデレーション Microsoft Entra ID ドメインとは、Microsoft Entra ID が認証を別の場所にリダイレクトするように構成されているドメインです。たとえば、ADFS やサードパーティの ID プロバイダーなどです。
- ハイブリッド参加済み VDA は、AD 参加済みであり、Microsoft Entra ID 参加済みです。

ドメイン参加済み VDA

ドメイン参加済み VDA の場合、Windows 認証 (従来は統合 Windows 認証、または Kerberos と呼ばれる) を使用して Microsoft Entra ID への SSO を実現します。Microsoft Entra ID への認証は、ユーザーが VDA セッション内から Microsoft Entra ID で保護されたアプリケーションにアクセスしたときに発生します。次の図は、認証プロセスを大まかに示しています。

ドメイン参加済み VDA(/en-us/federated-authentication-service/2411/media/domain-joined-vdas.png)

詳細な内容は、Microsoft Entra ID ドメインがマネージドであるかフェデレーションであるかによって異なります。

管理されたMicrosoft Entra IDドメインのセットアップについては、[シームレスシングルサインオン](#)を参照してください。

ADFSにフェデレーションされたMicrosoft Entra IDドメインの場合、ADFSサーバーでWindows認証を有効にします。

サードパーティのIDプロバイダーにフェデレーションされたMicrosoft Entra IDドメインの場合、同様のソリューションが存在します。詳細については、IDプロバイダーにお問い合わせください。

注：

ハイブリッド参加済みVDAには、ドメイン参加済みVDAに記載されているソリューションも使用できます。ただし、FASを使用する場合、Microsoft Entra IDプライマリ更新トークン（PRT）は生成されません。

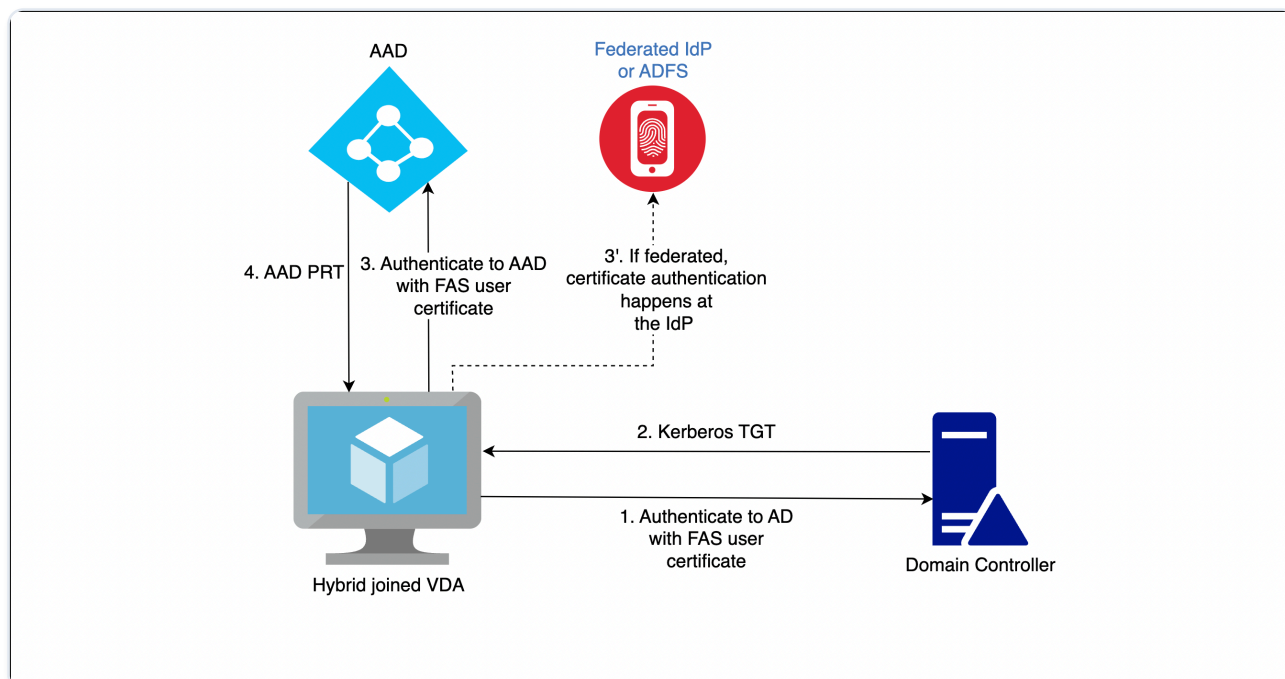
ハイブリッド参加済みVDA

ハイブリッド参加済みVDAは、ADとMicrosoft Entra IDに同時に参加しています。ユーザーがVDAにサインインすると、次のアーティファクトが作成されます。

- Kerberosチケット保証チケット（TGT）（ADリソースへの認証用）
- プライマリ更新トークン（PRT）（Microsoft Entra IDリソースへの認証用）

PRTには、ユーザーとコンピューターの両方に関する情報が含まれています。この情報は、必要に応じてMicrosoft Entra ID条件付きアクセス ポリシーで使用されます。

FASはVDAに証明書を提供することでユーザーを認証するため、Microsoft Entra IDの証明書ベースの認証が実装されている場合にのみ、PRTを作成できます。次の図は、認証プロセスを大まかに示しています。



正確な詳細は、Microsoft Entra ID ドメインが管理されているかフェデレーションされているかによって異なります。

管理された Microsoft Entra ID ドメインの場合、Microsoft Entra ID CBA を構成します。詳細については、[Azure AD 証明書ベース認証の概要](#)を参照してください。VDA は、Microsoft Entra ID CBA を使用して、ユーザーの FAS 証明書で Microsoft Entra ID に対してユーザーを認証します。

注：

Microsoft のドキュメントではスマートカード証明書によるサインインについて説明していますが、その基盤となる技術は FAS ユーザー証明書でサインインする場合にも適用されます。

ADFS にフェデレーションされた Microsoft Entra ID ドメインの場合、VDA は ADFS サーバーの *WS-Trust certificatemixed* エンドポイントを使用して、ユーザーの FAS 証明書で Microsoft Entra ID に対してユーザーを認証します。このエンドポイントはデフォルトで有効になっています。

サードパーティの ID プロバイダーにフェデレーションされた Microsoft Entra ID ドメインの場合、同様のソリューションが存在する可能性があります。ID プロバイダーは *WS-Trust certificatemixed* エンドポイントを実装する必要があります。詳細については、ID プロバイダーにお問い合わせください。

認証局の構成

この記事では、認証局 (CA) サーバーと統合するための Federated Authentication Service (FAS) の高度な構成について説明します。これらの構成のほとんどは、FAS 管理コンソールではサポートさ

れていません。手順では、FASが提供するPowerShell APIを使用します。この記事の指示を実行する前に、PowerShellの基本的な知識が必要です。

FASで使用する複数のCAサーバーを設定する

FAS管理コンソールを使用して、ルールを作成または編集する際に複数のCAでFASを構成できます。

2つのCAを使用するルールの編集。(/en-us/federated-authentication-service/2411/media/edit-rule-2cas.png)

選択したすべてのCAは、Citrix_SmartcardLogon証明書テンプレート (またはルールで選択したテンプレート) を公開している必要があります。

使用したいCAのいずれかが目的のテンプレートを公開していない場合は、そのCAに対して[認証局のセットアップ](#)手順を実行してください。

注:

すべてのCAに対して[このサービスを承認する](#)手順を実行する必要はありません。この手順で構成された承認証明書は、いずれかのCAで使用できるためです。

予期される動作の変更

FASサーバーを複数のCAサーバーで構成すると、ユーザー証明書の生成は、構成されているすべてのCAサーバーに分散されます。また、構成されているCAサーバーのいずれかが失敗した場合、FASサーバーは別の利用可能なCAサーバーに切り替わります。

TCPアクセス用にMicrosoft認証局を構成する

FASはDCOMを使用してMicrosoft CAにアクセスします。DCOMはポート135を使用して、サービスがリッスンしているポートを検出します。デフォルトでは、リッスンポートは動的に割り当てられます。これにより、ファイアウォールセキュリティを実装する際に複雑さが発生する可能性があります。そのため、Microsoftは静的ポートを構成する機能を提供しています。Microsoft CAで静的ポートを構成するには、**スタート > ファイル名を指定して実行 > dcomcnfg.exe** を選択して、**DCOM構成**パネルを開きます。コンピューター > マイコンピューター > **DCOM構成**を展開して、CertSrv Requestノードを表示します。次に、CertSrv Request DCOMアプリケーションのプロパティを編集します。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-caconfig-select-dcom-protocol.png)

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 (前の図では900) を指定します。

この例では、ファイアウォールはポート135とポート900を許可する必要があります。

変更を適用するには、Microsoft証明機関を再起動してください。

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。DCOMはRPCポート135を使用してネゴシエーション段階を持つためです。クライアントがDCOMを使用する必要がある場合、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（この例では）が開かれ、DCOMサーバーはクライアントにそのポートへの接続を指示します。

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短縮されます。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

以下の例に示すように、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 -NoTypeInformation -Encoding utf8
-delimiter "," $filename

} else {
```

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

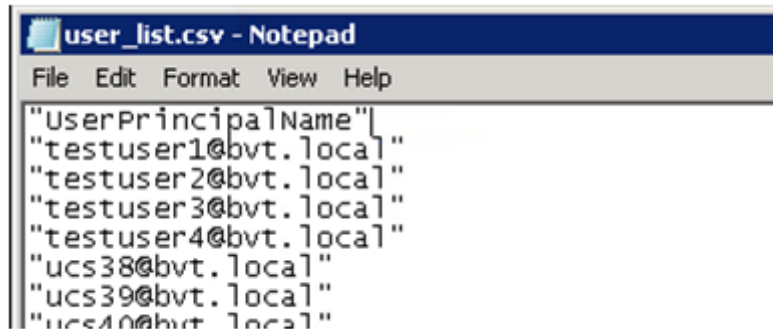
`Get-ADUser` は、ユーザーのリストをクエリするための標準的なコマンドレットです。上記の例には、`UserPrincipalName`を持ち、アカウントステータスが「有効」であるユーザーのみをリストするためのフィルター引数が含まれています。

`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。



```
user_list.csv - Notepad  
File Edit Format View Help  
"UserPrincipalName"  
"testuser1@bvt.local"  
"testuser2@bvt.local"  
"testuser3@bvt.local"  
"testuser4@bvt.local"  
"ucs38@bvt.local"  
"ucs39@bvt.local"  
"ucs40@bvt.local"
```

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受け取り、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  
  
    }  
  
}
```

FASサーバーが複数ある場合、特定のユーザーの証明書はメインサーバーとフェイルオーバーサーバーで2回生成されます。

この前のスクリプトは、「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」）を使用している場合は、スクリプト内の `$rule` 変数を変更してください。



Citrix FAS Administration Console - connected to localhost

Initial Setup Rules Advanced Connect to another server

A rule defines a smartcard-class certificate that signs users into a Citrix environment.

[+ Create rule](#)

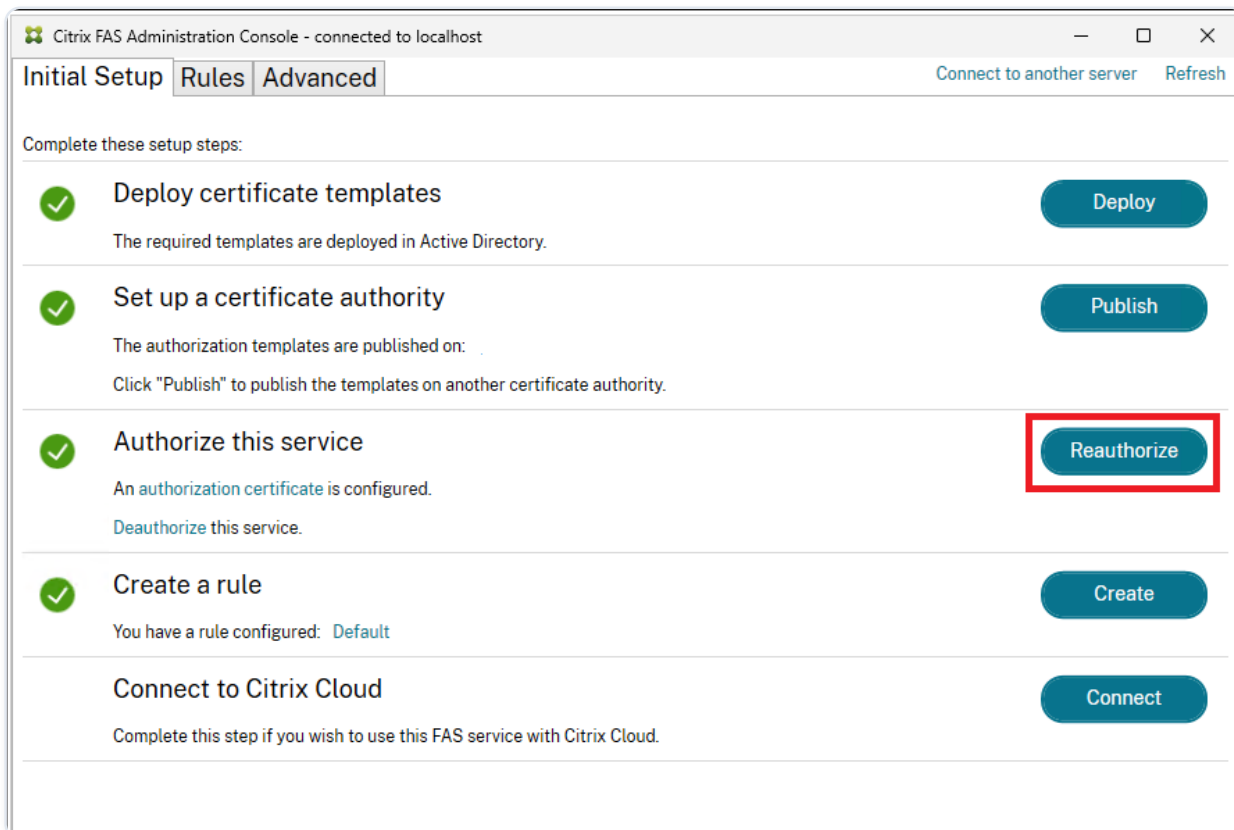
Default		Summary
hello	 	Rule name: hello Status: OK Template: Citrix_SmartcardLogon

FAS承認証明書を更新する

FAS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。

FAS管理コンソールを使用する

- 新しいFAS承認証明書要求を生成するには、**再承認**をクリックします。



Citrix FAS Administration Console - connected to localhost

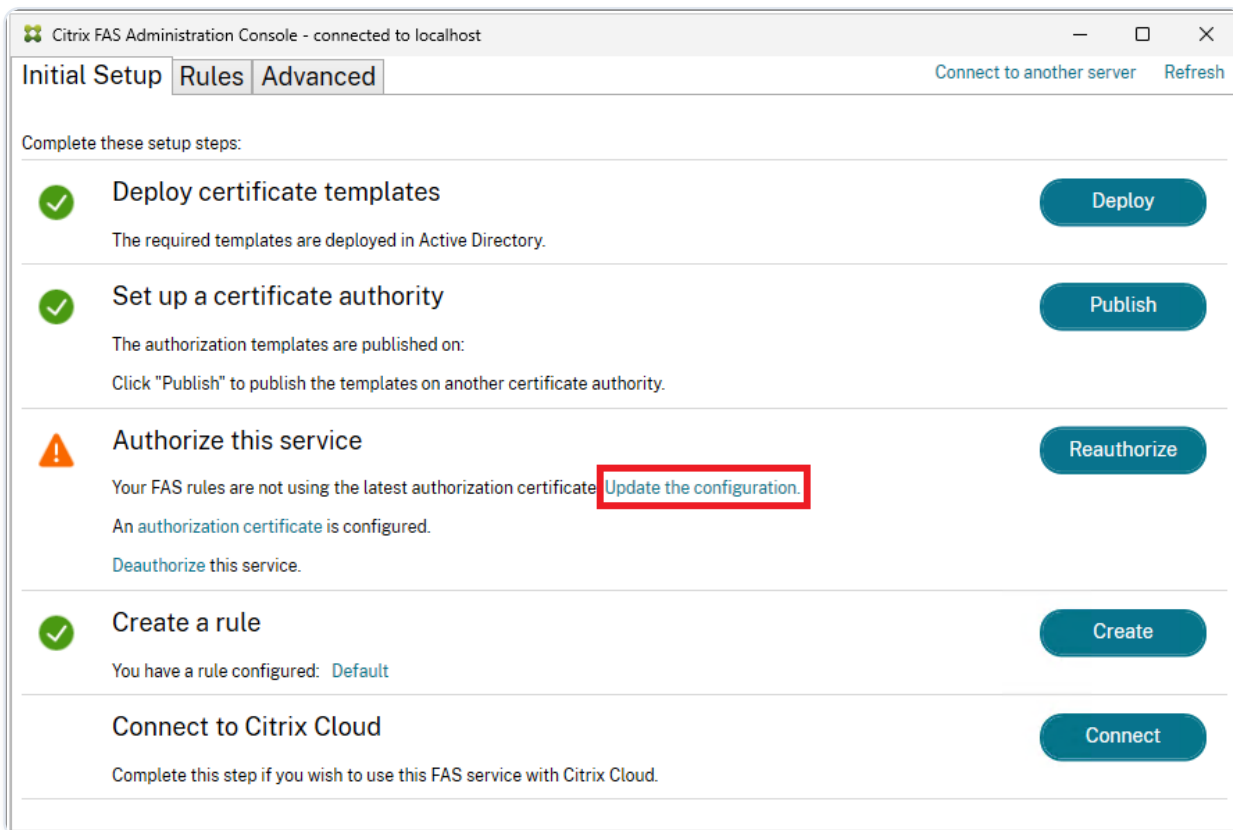
Initial Setup Rules Advanced Connect to another server Refresh

Complete these setup steps:

✓	Deploy certificate templates The required templates are deployed in Active Directory.	Deploy
✓	Set up a certificate authority The authorization templates are published on: . Click "Publish" to publish the templates on another certificate authority.	Publish
✓	Authorize this service An authorization certificate is configured. Deauthorize this service.	Reauthorize
✓	Create a rule You have a rule configured: Default	Create
	Connect to Citrix Cloud Complete this step if you wish to use this FAS service with Citrix Cloud.	Connect

CAで要求を手動で承認する必要があります。詳細については、「[フェデレーション認証サービスを承認する](#)」を参照してください。

- 新しい承認証明書が生成されると、FASはそれがまだルールに関連付けられていないことを示します。新しい承認証明書をルールに関連付けるには、**構成を更新**をクリックします。



PowerShellを使用する

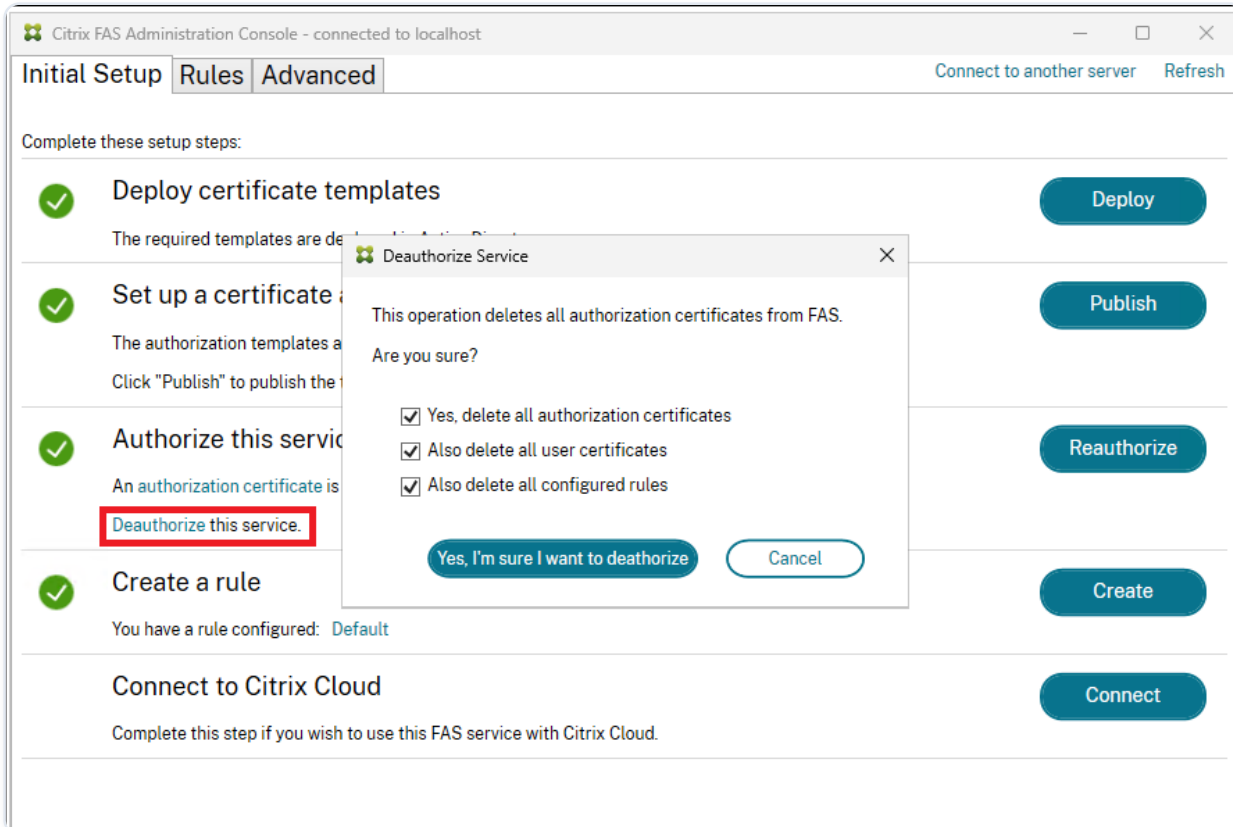
次のシーケンスを完了します。

- 承認証明書を作成します: `New-FasAuthorizationCertificate`
- `Get-FasAuthorizationCertificate` によって返される、新しい承認証明書のGUIDをメモします。
- 新しい承認証明書を交換します: `Set-FasCertificateDefinition - AuthorizationCertificate <GUID>`
- 古い承認証明書を削除します: `Remove-FasAuthorizationCertificate`。ユーザーアクティビティが中断されないように、`DeleteUserCerts $false option` を使用してください。

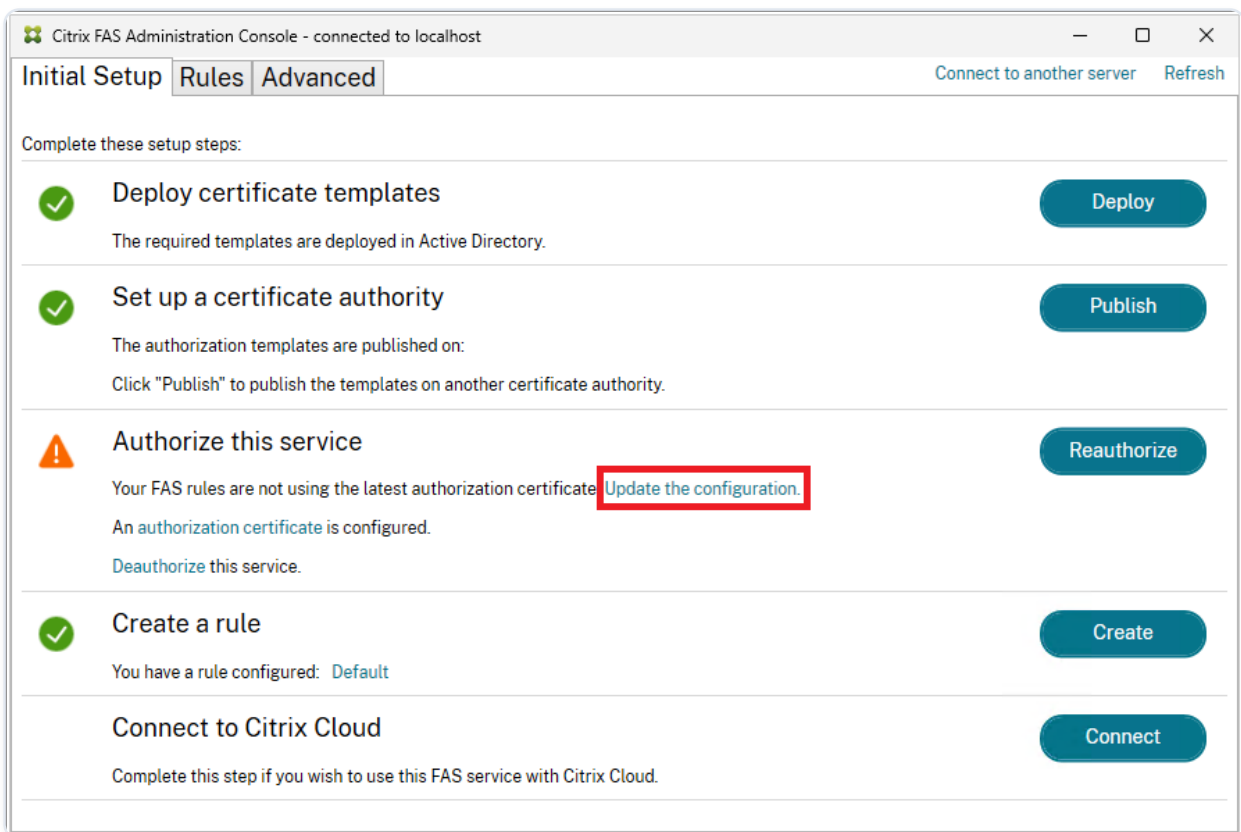
FASの認証解除とFAS証明書の削除

FAS管理コンソールの使用

- 「認証解除」リンクをクリックし、認証証明書を削除します。すべてのユーザー証明書とすべてのルールを削除できます（証明書をクリアするために必須ではありません）。



- ルールを削除しない場合、後でFASを認証すると、警告が表示されます。



この警告は、認証証明書がまだルールに関連付けられていないことを示しています。新しい認証証明書をルールに関連付けるには、「構成を更新」をクリックします。

PowerShellの使用

認証証明書とユーザー証明書を削除するには、次のPowerShellコマンドを使用します。

```
$AuthCert = Get-FasAuthorizationCertificate -Address localhost  
  
Remove-FasAuthorizationCertificate -Address localhost -Id $AuthCert.Id
```

注：

`Get-FasAuthorizationCertificate` は、認証証明書と保留中の認証証明書要求のリストを返します。これは、`Remove-FasAuthorizationCertificate` を続行する前に `$AuthCert` の値を確認するためのものです。

認証証明書を削除し、ユーザー証明書を保持するには、`DeleteUserCerts` パラメーターを `false` に設定します。

```
Remove-FasAuthorizationCertificate -Address localhost -Id $AuthCert.Id  
-DeleteUserCerts $false
```

残りのユーザー証明書は、VDAサインインおよびセッション内証明書のためにFASで引き続き使用できます。これは、FAS認証を更新する際に役立ちます。詳細については、「[FAS認証証明書の更新](#)」を参照してください。

- ユーザー証明書は次のように削除できます。

```
Remove-FasUserCertificate -Address localhost
```

このコマンドは、FASサーバーからすべてのユーザー証明書を削除します。このコマンドには、削除される証明書のセットをフィルターするオプションがあります。

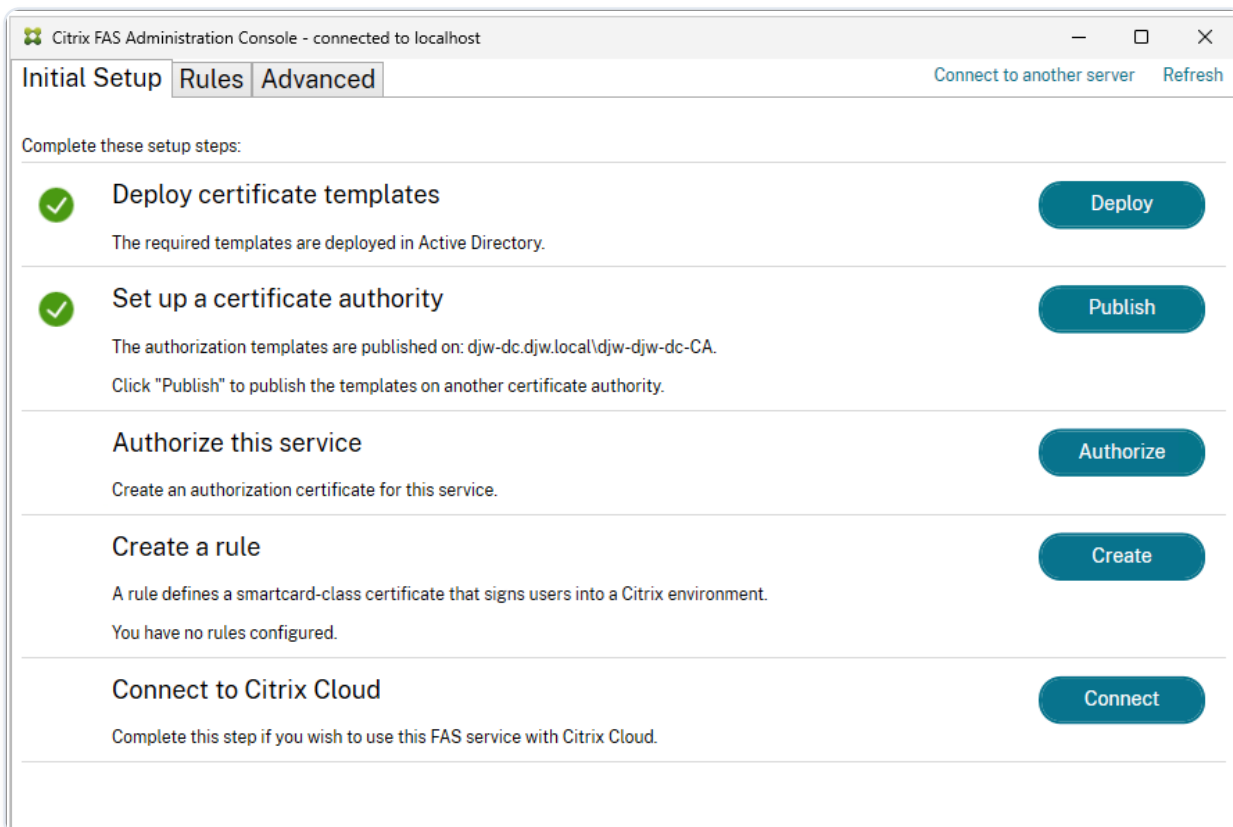
注：

FASが内部ストレージから承認またはユーザー証明書を削除すると、関連するキーペアも削除されます。

オフライン承認

FAS承認証明書は、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承認証明書を発行することを望まない組織に適しています。

1. 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つの手順のみを完了してください。証明書テンプレートを展開および証明機関をセットアップ。



2. 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`
```

3. FASサーバーで次のPowerShellコマンドレットを入力して、キーペアを生成し、証明書署名要求を作成します。

```
$AuthCertRequest = New-FasAuthorizationCertificateRequest -Address  
localhost $AuthCertRequest
```

これにより、次の結果が得られます。

```
PS C:\> $AuthCertRequest = New-FasAuthorizationCertificateRequest -Address localhost
PS C:\> $AuthCertRequest

Id                : a0da658f-a7e4-49b7-a0c3-6381c26a83a5
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE REQUEST-----
                  [Redacted Content]
                  -----END CERTIFICATE REQUEST-----
Status            : WaitingForApproval
```

注：

生成されるキーペアのプロパティは、FAS承認キー構成によって決定されます。詳細については、「[秘密キーの保護](#)」を参照してください。

4. 証明書要求をディスクにコピーします。

```
`$AuthCertRequest.CertificateRequest > c:\temp\authcert.csr
```

5. 証明書要求ファイル（この例ではauthcert.csr）を証明機関に提示し、要求を承認して、証明書応答を取得します。

以下の5つの手順は、Microsoft Enterprise証明機関を使用する場合に固有のものです。その他のCAについては、CAベンダーにお問い合わせください。

- 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。

The screenshot shows the 'Properties of New Template' dialog box with the following details:

- Subject Name**, **Server**, **Issuance Requirements**, **Superseded Templates**, **Extensions**, **Security**, **Compatibility**, **General** (selected), **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
- Buttons:** OK, Cancel, Apply, Help

- 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。作成したテンプレートを選択します。
- FASサーバーのPowerShellコマンドプロンプトに以下を入力して、証明書署名要求を証明機関に提出します。

```
certreq -submit -attrib "certificatetemplate:<certificate template
from step 5a>" <certificate request file from step 4>
```

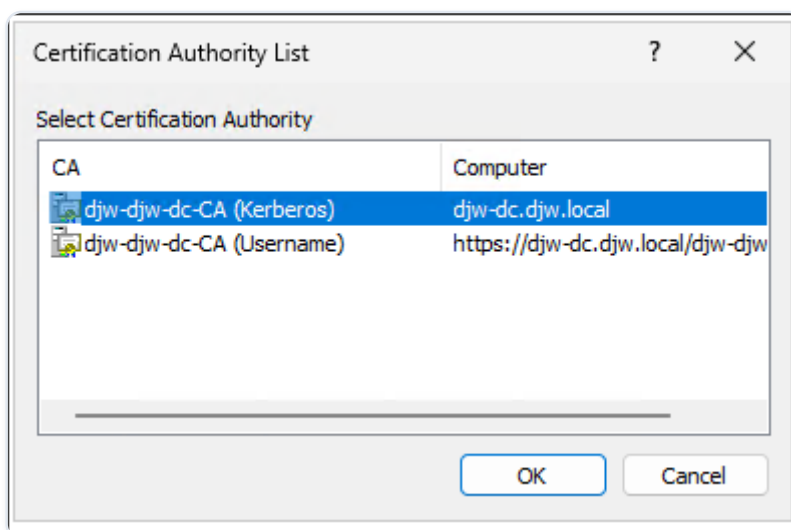
例:

```
certreq -submit -attrib "certificatetemplate:Offline_RA" C:
\temp\authcert.csr
```

前述のコマンドを実行すると、結果は次のようになります。

```
PS C:\> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\temp\authcert.csr
Active Directory Enrollment Policy
{3C06E1D3-4E2D-4B8B-94FA-C254192D09C6}
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。この例の証明機関は、DCOM（上）とHTTP（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** を選択し、**OK** をクリックします。

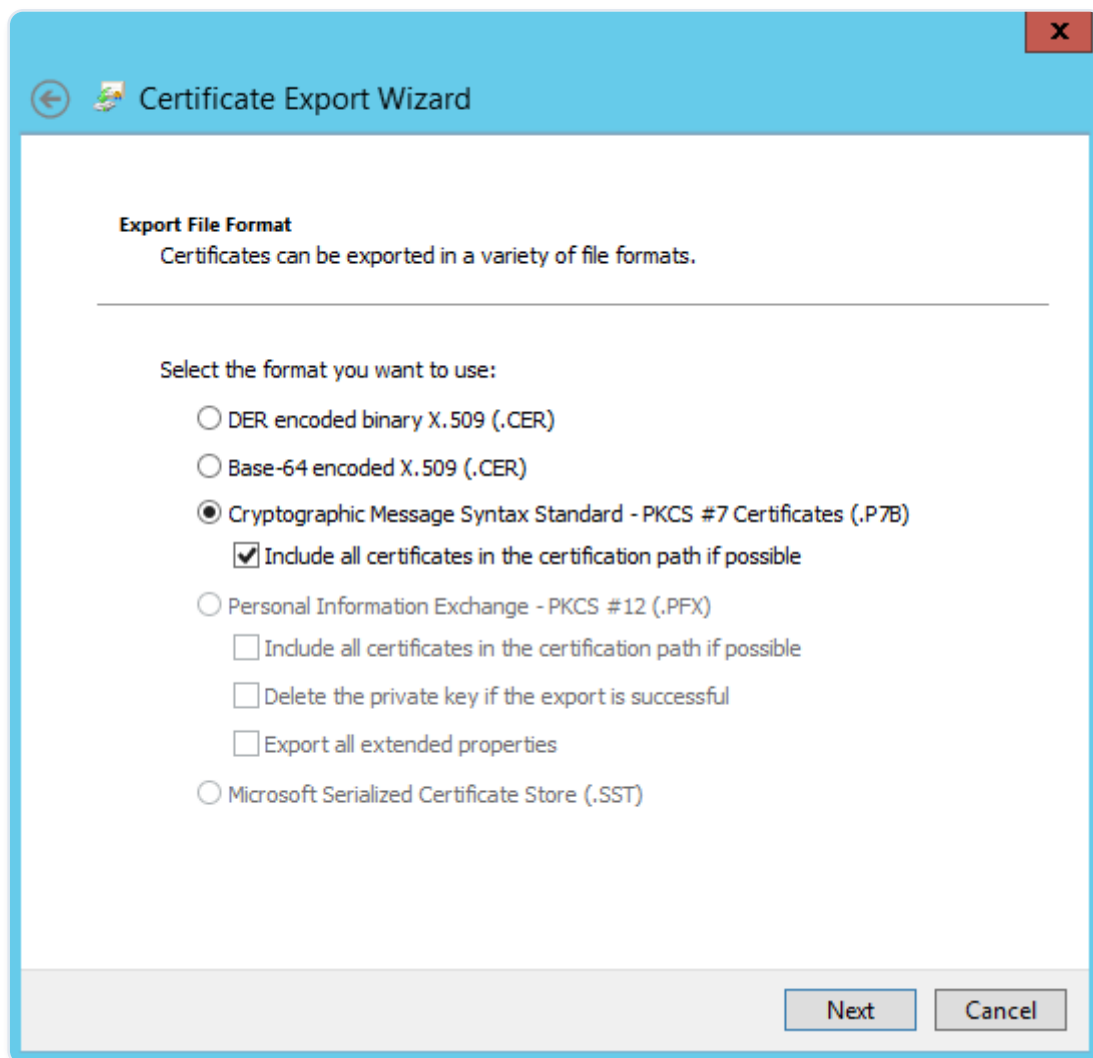


証明機関が指定されると、コマンドが完了し、RequestIDが表示されます。

```
PS C:\> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\temp\authcert.csr
Active Directory Enrollment Policy
{3C06E1D3-4E2D-4B8B-94FA-C254192D09C6}
ldap:
RequestId: 358
RequestId: "358"
Certificate request is pending: Taken Under Submission (0)
PS C:\> |
```

- 証明機関サーバーの証明機関MMCスナップインで、**保留中の要求**をクリックします。要求IDを見つけます。次に、要求を右クリックし、**発行**を選択します。

- **発行済み証明書**ノードを選択します。発行された証明書を見つけます（要求IDが一致する必要があります）。ダブルクリックして証明書を開きます。**詳細**タブを選択します。**ファイルへコピー**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。次へをクリックします。ファイル形式について以下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。

6. エクスポートされた証明書ファイルをFASサーバーにコピーします。
7. 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 localhost -Id  
$AuthCertRequest.Id -Pkcs7CertificateFile <Certificate file from step  
6>
```

例:

```
Import-FasAuthorizationCertificateResponse -Address localhost -Id  
$AuthCertRequest.Id -Pkcs7CertificateFile C:\temp\response.p7b
```

このコマンドを実行すると、次の結果が得られます。

FAS承認証明書のインポート応答(/en-us/federated-authentication-service/2411/media/import-fas-auth-cert-response.png)

8. FAS管理コンソールを確認します。FASが承認済みであることが表示されているはずです。

サービスの承認(/en-us/federated-authentication-service/2411/media/fas-admin-console-authorize-service.png)

注:

「このサービスを承認」のステップには、緑色のチェックマークが付いています。

9. ルールを作成して構成を続行します。詳細については、「[ルールを構成する](#)」を参照してください。

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の展開は、「[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。

秘密鍵の保護

はじめに

FAS証明書は、FASサーバー上の組み込みデータベースに保存されます。FAS証明書に関連付けられた秘密鍵は、FASサーバーのネットワークサービスアカウントの下に保存されます。デフォルトでは、鍵はエクスポート不可の2048ビットRSAで、Microsoft Software Key Storage Providerで作成および保存されます。

FAS PowerShellコマンド[PowerShellコマンドレット](#)を使用すると、秘密鍵のプロパティと保存場所を変更できます。

注：

FASの構成と証明書はFASサーバーにローカルに保存されます。データはFASサーバー間で共有されません。

Citrix Virtual Apps and Desktops 2411より前のFASリリースでは、秘密鍵のプロパティは `%programfiles%\Citrix\Federated Authentication Service\Citrix.Authentication.FederatedAuthenticationService.exe.config` にあるXMLファイルを編集して構成されていました。これはPowerShellコマンドに置き換えられ、より柔軟性があり、FASサーバーを再起動せずに適用できます。さらに、XMLファイルの設定とは異なり、PowerShellを使用して行われた構成は、FASサーバーがアップグレードされても保持されます。したがって、以下の設定に対するXMLファイルを使用した構成はサポートされなくなりました。

- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength`

「Citrix Virtual Apps and Desktops™ 2411より前のFASバージョンからのアップグレード」のセクションを参照してください。

FAS証明書とテンプレートに関する情報

FASが保持する証明書には2種類あります。通常1つのインスタンスである承認証明書と、ユーザー証明書です。

注記:

FAS承認証明書は、**登録機関**または**要求エージェント (RA)** 証明書と呼ばれることもあります。

FASは、次のセクションで説明するように、証明書を要求する際に証明書テンプレートを使用します。FASは証明書要求でテンプレート名を指定しますが、テンプレートの内容は読み取りません。したがって、テンプレートの設定を変更しても、FASが行う証明書要求には影響しません。テンプレートの特定のプロパティを変更すると、CAによって生成される証明書に影響します。たとえば、テンプレートを使用して有効期間を変更できます。

FAS承認証明書

この証明書は、FASを構成するときに作成されます。FAS管理コンソールの承認または再承認ボタンを使用して、新しい承認証明書を要求できます。

PowerShellコマンドを使用することも可能で、より柔軟性があります。

- `New-FasAuthorizationCertificate` : このコマンドはFAS管理コンソールと同様に動作しますが、承認プロセスで使用する証明書テンプレートを指定できる点が異なります。
- `New-FasAuthorizationCertificateRequest` : このコマンドは、承認証明書のオフライン要求を作成します。オフライン承認。

承認証明書は、FASが登録機関として機能し、ユーザーに代わって証明書を要求するため、RA証明書と呼ばれることもあります。この証明書には、拡張キー使用法証明書要求エージェントがあり、FASユーザー証明書を要求する際の承認資格情報として使用できます。

デフォルトでは、承認プロセスは次のテンプレートを使用します。

- `Citrix_RegistrationAuthority_ManualAuthorization` : このテンプレートを使用して作成された証明書は一時的で短命であり、承認プロセスをブートストラップするために使用されます。
- `Citrix_RegistrationAuthority` : このテンプレートを使用して作成された証明書は有効期間が長く、FASサーバーによって保存されます。

FASを承認すると、次の手順が実行されます。

1. FASはキーペアを作成し、キーペアの公開キーとテンプレート `Citrix_RegistrationAuthority_ManualAuthorization` を指定して、証明書署名要求 (CSR) をCAに送信します。
2. テンプレートの発行要件では、CSRはCA管理者によって手動で承認される必要があると指定されています。
3. CA管理者がCSRを承認すると、CAはFASが取得する証明書を作成します。この証明書は有効期間が1日と短く、次のステップでのみ使用されます。使用されると、FASはその証明書とキーペアを破棄します。
4. FASは別のキーペアを作成し、このキーペアの公開鍵とテンプレート `Citrix_RegistrationAuthority` を指定して、2番目のCSRをCAに送信します。この要求は、前のステップの証明書によって承認され、署名されます。
5. CAは自動的に証明書を発行し、FASは証明書を取得し、FASはこれで承認済みとなります。デフォルトでは、この承認証明書の有効期間は2年間です。

前述のキーペアを作成するために使用された設定は、このPowerShellコマンドを使用して表示できます。

```
Get-FasKeyConfig -Address localhost -CertificateType ra
```

FASユーザー証明書

FASは、ユーザーをVDAにサインインさせるためにユーザー証明書を作成します。

FASがユーザー証明書を作成すると、次のステップが実行されます。

- FASはキーペアを作成し、キーペアの公開鍵、ユーザーのID、およびデフォルトでテンプレート `Citrix_SmartcardLogon`（使用されるテンプレートは構成可能）を指定して、CSRをCAに送信します。
- CSRはFAS承認証明書を使用して署名されます。
- `Citrix_SmartcardLogon` テンプレートには発行要件 `Application Policy: Certificate Request Agent` があります。この属性はFAS承認証明書に存在するため、CAはユーザー証明書を自動的に発行します。
- FASは証明書を取得し、FASサーバー上の組み込みデータベースに保存します。
- デフォルトでは、証明書の有効期間は1週間です。

その後、ユーザー証明書はユーザーをサインインさせるためにVDAで利用可能になります。

前述のキーペアを作成するために使用された設定は、次のPowerShellコマンドを使用して表示できます。

```
Get-FasKeyConfig -Address localhost -CertificateType user
```

秘密鍵の保存オプション

FASは、キーペアを以下の3種類のストレージカテゴリに作成および保存するように構成できます。

- **ソフトウェア**: 通常、**Microsoft Software Key Storage Provider**を使用します。これはソフトウェアのみで保護されており、データはディスクに保存されます。
- **Trusted Platform Module (TPM)**: TPMは、コンピューター上の物理ハードウェアであるか、ハイパーバイザーによって提供される仮想TPMである場合があります。
- **Hardware Security Module (HSM)**: これは、暗号鍵を安全に保存するように設計されたハードウェア周辺機器またはネットワークデバイスです。

注:

考慮すべきトレードオフがあります。ハードウェアストレージはより安全である可能性がありますが、特に多数のユーザー証明書キーペアを作成および保存する場合、パフォーマンスが低下することがよくあります。

FAS承認証明書に関連付けられた秘密鍵は特に機密性が高く、その証明書のポリシーにより、秘密鍵を所有する者は誰でも、任意のユーザーの証明書要求を承認できるためです。結果として、この鍵を制御する者は誰でも、任意のユーザーとして環境に接続できます。

注:

Microsoft CAは、証明書を発行できるユーザーのセットを含め、FAS承認証明書の権限を制限するように構成できます。詳細については、「[委任された登録エージェント](#)」を参照してください。

このため、FASでは、承認証明書とユーザー証明書の秘密鍵プロパティを個別に構成できます。

一般的な構成をいくつか示します。

承認証明書キー	ユーザー証明書キー	コメント
ソフトウェア	ソフトウェア	デフォルト構成
TPM	ソフトウェア	承認証明書はハードウェア保護されています
HSM	HSM	すべての証明書はハードウェア保護されています

注:

ハードウェアTPMはユーザーキーには推奨されません。承認証明書キーにのみ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、ハイパーバイザーベンダーにTPM仮想化がサポートされているか確認してください。

キー構成PowerShellコマンド

秘密キーの構成に関連するコマンドは次のとおりです:

- `Get-FasKeyConfig`
- `Set-FasKeyConfig`
- `Reset-FasKeyConfig`
- `Test-FasKeyConfig`

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

認証およびユーザー証明書のキー構成は独立しており、`CertificateType` 引数によって指定されます。たとえば、認証証明書 (RA 証明書) を要求するときに使用される秘密キー構成を取得するには、次の手順を実行します。

```
Get-FasKeyConfig -Address localhost -CertificateType ra
```

ユーザー証明書を要求するときに使用される秘密キー構成を取得するには、次の手順を実行します。

```
Get-FasKeyConfig -Address localhost -CertificateType user
```

Set-FasKeyConfig と **Get-FasKeyConfig** を使用して、次の秘密キープロパティを設定および検査できます。

プロパティ	デフォルト	コメント
長さ	2048	ビット単位のキー長。Microsoft テンプレート GUI では、 暗号化 タブで *最小* キーサイズが指定されていることに注意してください。FAS で構成されたキー長がテンプレートで指定された最小キーサイズよりも短い場合、CSR は CA によって拒否されます。 RSAキーの場合、長さは1024ビット、2048ビット、または4096ビット

プロパティ	デフォルト	コメント
		にすることができます。 ECCキーの場合、長さは256ビット、384ビット、または521ビットにすることができます。
エクスポート可能	フォールス	秘密鍵をそのプロバイダーからエクスポートできるかどうか。
プレフィックス	なし	FASによって生成される秘密鍵の識別子に追加するプレフィックスを指定します。生成される識別子は、プレフィックスとGUIDで構成されます。例えば、 <code>MyPrefix70277985-6908-4C6F-BE59-B08691456804</code>。
楕円曲線	フォールス	trueの場合、ECCキーペアが生成され、それ以外の場合はRSAキーペアが生成されます。
キー記憶域プロバイダー (KSP)	真	trueの場合、FASは最新のWindows CNG APIを使用し、ProviderプロパティでKSPを指定する必要があります。 falseの場合、FASはレガシーCAPI API

プロパティ	デフォルト	コメント
		を使用し、Provider プロパティで暗号化 サービスプロバイ ダー (CSP) を指定 する必要があります。 CitrixはKSPの 使用を推奨します。
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	キーペアが作成およ び保存されるプロバ イダーの名前です。 このプロパティを変 更して、TPMまたは HSMを指定できま す。HSMのKSP (ま たはCSP) はHSMベ ンダーによって提供 されます。彼らはソ フトウェアのインス トール方法とプロバ イダーの名前に関す る指示を提供しま す。
CSPタイプ	24	KSP プロパティが false に設定されてい る場合にのみ関連し ます。 <code>Microsoft KeyContainerPerm issionAccessEntr y.ProviderType Property PROV_RSA_AES 24</code> を参照します。CSP を持つHSMを使用 しており、HSMベ ンダーが別途指定し

プロパティ	デフォルト	コメント
		ない限り、常に24である必要があります。

さらに、**Set-FasKeyConfig** は、便宜上、以下のスイッチとともに使用できます。

フラグ	説明
-UseDefaultSoftwareProvider	Provider プロパティを Microsoft Software Key Storage Provider に、 KSP フィールドを true に設定します。
-UseDefaultTpmProvider	Provider プロパティを Microsoft Platform Crypto Provider に、 KSP フィールドを true に設定します。

Microsoft Software Key Storage Provider は、通常、ディスク上にキーを作成および保存するために使用されるプロバイダーです。

Microsoft Platform Crypto Provider は、通常、TPM にキーを作成および保存するために使用されるプロバイダーです。

Get-FasKeyConfig は、どのプロバイダーとアルゴリズムが使用されているかを確認するのに役立つフィールドも提供します。

フィールド	意味
IsDefaultSoftwareProvider	true の場合、プロバイダーが Microsoft Software Key Storage Provider に設定され、 KSP フィールドが true に設定されていることを示します。
IsDefaultTpmProvider	「true」の場合、プロバイダーが「 Microsoft Platform Crypto Provider 」に設定され、「 KSP 」フィールドが「 true 」に設定されていることを示します。

フィールド	意味
アルゴリズム	「RSA」は、RSAキーが作成されることを示します（「EllipticCurve」プロパティは「false」です）。 「ECC」は、ECCキーが作成されることを示します（「EllipticCurve」プロパティは「true」です）。

`Reset-FasKeyConfig` を使用して、設定をデフォルトに戻すことができます。

```
Reset-FasKeyConfig -Address localhost -CertificateType ra
```

```
Reset-FasKeyConfig -Address localhost -CertificateType user
```

注：

秘密キー構成（`Set-FasKeyConfig` または `Reset-FasKeyConfig` を使用）への変更は、新しく作成された証明書にすぐに適用されます。ただし、異なる構成を持つ既存の承認証明書およびユーザー証明書には影響しません。

既存の証明書は、管理コンソールからFASサービスを非承認にするか、[FASの非承認とFAS証明書の削除](#)のPowerShellコマンドを使用して削除できます。

現在のユーザーキー構成に準拠しないキープール内の事前生成されたキーはすべて破棄されます。

構成シナリオの例

各例では、既存の証明書は構成変更の影響を受けないため、FASサービスを承認する前に、提供されているPowerShellを使用してキー構成を設定してください。

誤ったキー構成の承認証明書またはユーザー証明書が既にある場合は、[FAS証明書の検査とFASの非承認とFAS証明書の削除](#)でそれらを削除できます。

FASサーバーがライブ展開にある場合は、構成変更を行う際にメンテナンスモードにすることを検討してください[メンテナンスモード](#)。

例1 - すべてのキーをMicrosoft Software Key Storage Providerに保存する

これはデフォルトであるため、追加の構成は必要ありません。

以前にキー構成を変更した場合は、以下のコマンドを使用して **Microsoft Software Key Storage Provider** の使用に戻すことができます。

```
Set-FasKeyConfig -Address localhost -CertificateType ra  
-UseDefaultSoftwareProvider  
  
Set-FasKeyConfig -Address localhost -CertificateType user  
-UseDefaultSoftwareProvider
```

`Reset-FasKeyConfig` を使用して **Microsoft Software Key Storage Provider** に戻し、さらに他のすべてのキー構成設定をデフォルトに復元できます。

例2 - 認証証明書キーを TPM に保存する

この例では、FAS 認証証明書キーを TPM (物理または仮想) に保存し、ユーザー証明書キーは **Microsoft Software Key Storage Provider** に保存する方法を示します。

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たり、サイズが制限されたりする可能性があります。

次の PowerShell コマンドを使用します。

```
Set-FasKeyConfig -Address localhost -CertificateType ra  
-UseDefaultTpmProvider  
  
Set-FasKeyConfig -Address localhost -CertificateType user  
-UseDefaultSoftwareProvider
```

例3 - すべてのキーを HSM に保存する

この例では、HSM を使用して認証証明書とユーザー証明書の両方の秘密キーを保存する方法を示します。この例では、構成済みの HSM を前提としています。HSM にはプロバイダー名がありません。たとえば、**HSM Vendor Key Storage Provider** などです。

次の PowerShell コマンドを使用します (例のテキストを HSM のプロバイダーの実際の名前で置き換えてください)。

```
Set-FasKeyConfig -Address localhost -CertificateType ra -Provider "HSM  
Vendor Key Storage Provider"
```

```
Set-FasKeyConfig -Address localhost -CertificateType user -Provider "HSM  
Vendor Key Storage Provider"
```

例 4 - 楕円曲線キーを使用する

デフォルトでは、FAS は RSA キーを生成します。この例では、認証証明書とユーザー証明書の両方に楕円曲線 (ECC) キーが構成されています。

この例では、異なるキー長を使用しています。認証証明書は 384 ビットキーで構成され、ユーザー証明書は 256 ビットキーで構成されています。

```
Set-FasKeyConfig -Address localhost -CertificateType ra -EllipticCurve  
$true -Length 384
```

```
Set-FasKeyConfig -Address localhost -CertificateType user -EllipticCurve  
$true -Length 256
```

この時点では、FAS 証明書テンプレートの最小キーサイズがデフォルトで 1024 ビットに設定されているため、認証およびユーザー証明書要求が CA によって拒否される可能性があります。

したがって、この例では、テンプレートの最小キーサイズを次のように変更する必要があります。

- `Citrix_RegistrationAuthority_ManualAuthorization` and `Citrix_RegistrationAuthority` : 最小キーサイズを 384 (またはそれ以下) に変更します
- `Citrix_SmartcardLogon` : 最小キーサイズを 256 (またはそれ以下) に変更します

テンプレートを編集するには、`mmc.exe` を実行し、**証明書テンプレートスナップイン**を追加します。テンプレートを見つけて、そのプロパティを開きます。最小キーサイズの設定は、テンプレートのプロパティの**暗号化タブ**にあります。

注：

ECCキーを持つユーザー証明書は、Citrix Virtual Apps and Desktops 2411以降を実行しているWindows VDAでのみサポートされます。ECCキーはLinux VDAではサポートされていません。

秘密キー構成のテスト

`Set-FasKeyConfig` コマンドは一部の検証を行います、無効なキー構成を設定することは依然として可能です。たとえば、HSMのプロバイダー名に誤りがある場合や、指定したキー長がハードウェアでサポートされていない場合があります。

コマンド `Test-FasKeyConfig` が役立ちます。これは、現在のキー構成を使用してキーペアの作成を試み、**成功**または**失敗**を報告します。失敗が発生した場合は、失敗の理由が示されます。成功した場合、キーペアはすぐに破棄されます。

次のPowerShellコマンドは、それぞれ認証とユーザーキー構成をテストします。

```
Test-FasKeyConfig -Address localhost -CertificateType ra
```

```
Test-FasKeyConfig -Address localhost -CertificateType user
```

FASサーバーを承認し、ルールを作成したら、次のようにユーザー証明書のテストCSRをさらに作成できます。

```
Test-FasCertificateSigningRequest -Address localhost -UserPrincipalName  
user@example.com -Rule default
```

`<mailto:user@example.com/>` をActive Directory展開からの実際のUPNに置き換えます。FASルールは通常**default**という名前です。ただし、設定した別のルールをテストしたい場合は、その名前を指定してください。

CSRが成功した場合、FASは結果の証明書を破棄します。

FAS証明書の検査

PowerShellを使用して、証明書のプロパティを検査し、関連する秘密キーがどこに保存されているかを判断できます。

承認証明書の検査

FAS管理コンソールで**承認証明書**リンクをクリックすると、承認証明書を確認できます。

承認証明書(/en-us/federated-authentication-service/2411/media/auth-cert-config.png)

ただし、より詳細な情報を得るにはPowerShellを使用します。

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

いくつかのフィールドが返されますが、その中には**PrivateKeyProvider**も含まれており、証明書が作成および保存されたプロバイダーの表示が含まれています。

PRIVATEKEYPROVIDER	キーの保存場所
Microsoft ソフトウェア キー ストレージ プロバイダー	キーはディスクに保存され、Microsoftのソフトウェアプロバイダーによって保護されています。
Microsoft プラットフォーム クリプト プロバイダー	キーはTPM（物理または仮想）に保存されます。
HSM ベンダー キー ストレージ プロバイダー (例のみ)	キーはHSMに保存されます（この例では、ベンダーのプロバイダーは HSM Vendor Key Storage Provider という名前です）。

ユーザー証明書の検査

FASサーバーにキャッシュされているすべてのユーザー証明書のリストを次のように取得できます。

```
Get-FasUserCertificate -Address localhost -KeyInfo $true
```

KeyInfo パラメーターを使用すると、出力に証明書に関連付けられた秘密キーに関する詳細情報が含まれます。特に、**PrivateKeyProvider** フィールドは、証明書に関連付けられたキーペアがどこに保存されているかを示します（この値の解釈については、前のセクションを参照してください）。

`-UserPrincipalName` のようなさまざまなオプションパラメーターを使用して、返される証明書のセットをフィルターできます。

コマンド出力の証明書フィールドは、PEMエンコードされたユーザー証明書です。テキストを `.crt` ファイルにコピーして、Windows証明書GUIを使用して次のように証明書を表示します。

コマンド	説明
<code>\$CertInfos = Get-FasUserCertificate -Address localhost</code>	このリストには複数のユーザー証明書が含まれている場合があります。
<code>\$CertInfo = \$CertInfos[0]</code>	この例では、最初のユーザー証明書を選択します。

コマンド	説明
<code>\$CertInfo.Certificate > c:\temp\user.crt</code>	PEMデータを <code>.crt</code> ファイルにパイプします。
<code>c:\temp\user.crt</code>	Windows GUI で <code>.crt</code> ファイルを開きます。

Citrix Virtual Apps and Desktops 2411より前のFASバージョンからのアップグレード

Citrix Virtual Apps and Desktops 2411より前のFASリリースでは、秘密キーのプロパティは、XMLファイルを編集して構成されていました。

```
%programfiles%\Citrix\Federated Authentication
Service\Citrix.Authentication.FederatedAuthenticationService.exe.config
```

これは、このドキュメントで説明されているPowerShellコマンドに置き換えられました。これらのコマンドは、より柔軟性があり、FASサーバーを再起動せずに適用できます。

さらに、XMLファイルの設定とは異なり、PowerShellを使用して行われた構成は、FASサーバーがアップグレードされても保持されます。

秘密キーの構成に関連するXMLファイルの設定は、対応するPowerShellパラメーター（`Get-FasKeyConfig` および `Set-FasKeyConfig` で使用されているもの）とともに、次のようにリストされています。

XMLファイルの設定	XMLファイル内のデフォルト値	POWERSHELLの同等物	コメント
<code>Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength</code>	2048	-長さ	-
<code>Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameter</code>	GenerateNonExportableKey	<code>-Exportable</code> <code>-UseDefaultTpmProvider</code>	• NoProtectionは、

XMLファイルの 設定	XMLファイル内 のデフォルト値	POWERSHELL の同等物	コメント
s.KeyProtect ion			-Exportable を \$true に設定することで実現されます -GenerateNonExportableKey は、 -Exportable を \$false に設定することで実現されます -GenerateTPMProtectedKey は、 -UseDefaultTpmProvider スイッチを指定することで実現されます
Citrix.Trust Fabric.Client SDK.TrustArea JoinParameter s.ProviderLeg acyCsp	フォールス	-Ksp	- ProviderLegacyCsp false は、 -Ksp を \$true に設定

XMLファイルの 設定	XMLファイル内 のデフォルト値	POWERSHELL の同等物	コメント
			することで実現 されます <code>-ProviderLegacyCsp true</code> は、<code>-Ksp</code> を <code>\$false</code> に設 定することで 実現されま す。
<code>Citrix.Trust Fabric.Client SDK.TrustArea JoinParameter s.ProviderName</code>	-	-プロバイダー	-
<code>Citrix.Trust Fabric.Client SDK.TrustArea JoinParameter s.ProviderType</code>	-	-CspType	-

XML構成のデフォルトとPowerShellのデフォルトは機能的に同等です。つまり、デフォルトでは、このバージョンおよびCitrix Virtual Apps and Desktops 2411以前のバージョンでFASによって生成されたキーペアのプロパティは同じです。

したがって、XML構成ファイルで上記のいずれの設定も変更していない場合は、FASをアップグレードする際に何もアクションを実行する必要はありません。

ただし、上記のいずれかの設定を変更した場合は、次のようにFASをアップグレードしてください。

- FASをメンテナンスモードにします。[メンテナンスモード](#)。
- FAS インストーラーを実行するだけで、FAS を**その場で**アップグレードします。アップグレードが完了すると、以前の設定はすべて XML ファイルに存在なくなり、XML ファイルで構成することはできません。

- **キー構成 PowerShell コマンド** で説明されているように、PowerShell コマンド `Set-FasKeyConfig` を使用して、FAS プライベートキー構成を希望どおりに設定します。認証およびユーザー証明書に必要な設定を検討してください。
- **プライベートキー構成のテスト** で説明されているように、構成をテストします
- FAS サーバーをメンテナンスモードから解除します

次回アップグレードする際には、FAS プライベートキー構成設定は保持され、特別な操作を行う必要はありません。

暗号化リモート処理

FAS ユーザー証明書に関連付けられた秘密キーは、VDA に転送されることはありません。代わりに、VDA がユーザーの FAS 証明書を VDA へのサインインまたはセッション内での使用のために必要とする場合、暗号化要求は FAS サーバーにリモート処理されます。これにより、秘密キーが FAS キー ストレージ (ソフトウェア ストレージ、TPM、HSM のいずれであっても) から離れることがないため、セキュリティが向上します。

Windows VDA では、これは VDA 上のプロバイダーのペアを使用することで実現されます。暗号化要求を行うアプリケーションまたはオペレーティングシステムコードは、操作が FAS サーバーにリモート処理されていることを認識しません。

Citrix Virtual Apps and Desktops 2411 より前は、プロバイダーは **Cryptographic Service Providers (CSPs)** であり、アプリケーションおよびオペレーティングシステムコードのアクセスは、古い Windows CAPI API を介して行われていました。プロバイダーは次のとおりでした。

- `CitrixLogonCsp.dll` : VDA へのシングルサインオン用
- `CitrixVirtualSmartcardCsp.dll` : セッション内証明書用

Citrix Virtual Apps and Desktops 2411 以降、追加の Key Storage Providers (KSPs) が VDA に提供されます。アプリケーションおよびオペレーティングシステムコードは、新しい Windows CNG API を使用してこれらにアクセスします。新しいプロバイダーは次のとおりです。

- `CitrixLogonKsp.dll` : VDA へのシングルサインオン用
- `CitrixVirtualSmartcardKsp.dll` : セッション内証明書用

KSP は、Windows アプリケーションに暗号化操作を公開するための、より最新の方法であり、より多くの機能を提供します。例:

- ECCキーを持つ証明書がサポートされています
- 確率的署名方式 (PSS) パディングがサポートされています

FASとVDAの両方がCitrix Virtual Apps and Desktops 2411以降を実行している場合、KSPリモート処理（つまり、新しいKSPを介したリモート処理）が使用されます。そうでない場合、システムは古いCSPを使用してリモート処理を行うようにフォールバックします。

KSPリモート処理の無効化

互換性の問題が発生した場合、KSPリモート処理を無効にして、常に古いCSPリモート処理を使用できるようにすることが可能です。

次のPowerShellを使用します。

```
Set-FasServer -Address localhost -KspRemoting $false
```

メンテナンスモード

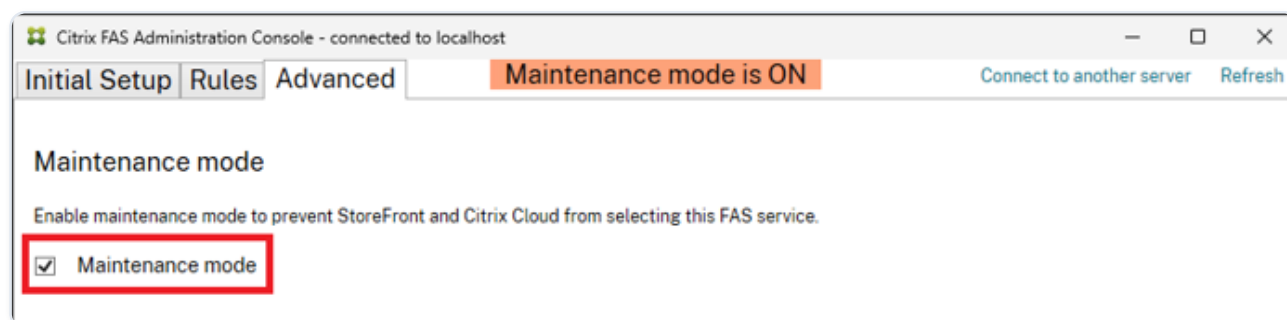
稼働中のFASサーバーの構成に変更を加える際は、メンテナンスモードにすることを検討してください。

FASがメンテナンスモードの場合、以下が適用されます。

- **Workspace** または **StoreFront™** が公開アプリケーションまたはデスクトップの起動シーケンスの一部としてFASを呼び出すと、FASはメンテナンスモードであることを示します。呼び出し元は、別のFASサーバーを選択することでこれに対応する必要があります。
- 追加の予防措置として、FASはメンテナンスモード中にユーザー証明書の自動作成を許可しません。これにより、意図しない設定でのユーザー証明書の誤った作成が回避されます。
- ただし、VDAサインインやセッション内での使用など、既存のユーザー証明書に関わるアクティビティは引き続き許可されます。

自動ユーザー証明書作成は許可されていませんが、管理者は `New-FasUserCertificate` や `Test-FasCertificateSigningRequest` などのPowerShellコマンドを使用してユーザー証明書を作成できます。

管理コンソールの使用



PowerShellの使用

FASサーバーをメンテナンスモードにするには、次のようにします。

```
Set-FasServer -Address localhost -MaintenanceMode $true
```

FASサーバーをメンテナンスモードから解除し（通常の操作に戻す）、次のようにします。

```
Set-FasServer -Address localhost -MaintenanceMode $false
```

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、[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

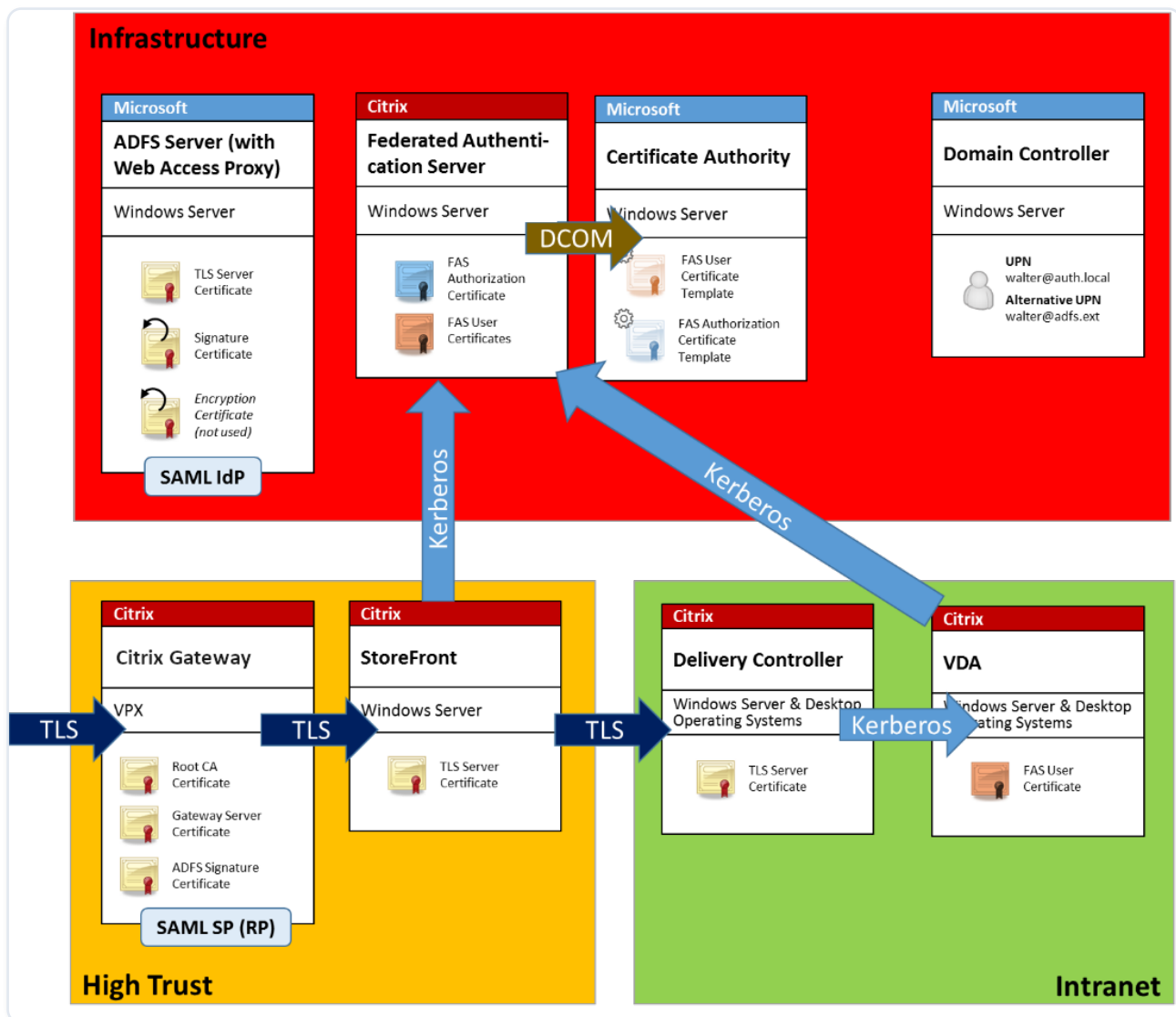
Federated Authentication Service (FAS) は、Microsoft Active Directory および Microsoft 証明機関と密接に統合されています。ドメインコントローラーやその他の重要なインフラストラクチャと同様に、システムが適切に管理および保護されるように、セキュリティポリシーを策定してください。

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セキュリティ保護に役立つ利用可能な機能の概要も説明します。

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です。フェデレーション環境では、Citrix Gateway と Citrix StoreFront がユーザー認証を実行す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

ポート 443 経由の TLS は、Citrix Gateway、StoreFront、および Delivery Controller™ コンポーネント間の通信を保護します。StoreFront サーバーは送信接続のみを実行し、Citrix Gateway は HTTPS ポート 443 を使用してインターネット経由の接続のみを受け入れます。

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。この認証方法により、Citrix Virtual Delivery Agent (VDA) がユーザーをログオンするために必要な、1 回限りの「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。また、VDA は証明書と秘密キー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、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 FAS サーバーが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Kerberos over HTTP、[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サーバーへの/からのHTTPS、[out] VDAへのHDX
StoreFront	[in] シトリックス ゲートウェイからの HTTPS、[out] デリバリーコントローラーへの HTTPS、[out] FASへのKerberos HTTP
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Kerberos over HTTP
VDA	[in/out] デリバリーコントローラーからの Kerberos over HTTP、[in] シトリックス ゲートウェイからのHDX、[out] FASへのKerberos HTTP
Microsoft証明機関	[in] FASからのDCOMおよび署名

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でのFAS管理コンソール
 - *.cloud.com
 - *.citrixworkspacesapi.net
 - お使いの環境でサードパーティのIDプロバイダーを使用している場合に必要となるアドレス
- ネットワークサービスアカウント下のFASサービス:

- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net

お使いの環境にプロキシサーバーが含まれている場合、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。

セキュリティに関する考慮事項

FASには、ドメインユーザーに自律的に証明書を発行できる登録機関証明書があります。これは、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開発および実装するのに役立ちます。

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証明機関では、登録エージェント、証明書テンプレート、および登録エージェントが証明書を発行できるユーザーを制限できます。

登録エージェントダイアログ(/en-us/federated-authentication-service/2411/media/delegated-enrollment-agents.png)

指定されたダイアログを使用して、以下を確認できます:

- 登録エージェントリストにはFASサーバーのみが含まれています。
- 証明書テンプレートリストにはFASテンプレートのみが含まれています。
- 権限リストには、FASの使用が許可されているユーザーが含まれています。たとえば、管理者または保護されたユーザーグループに証明書を発行しないことをお勧めします。

アクセス制御リストの構成

「[ルールを構成する](#)」セクションで説明されているように、StoreFrontサーバーのリストを構成する必要があります。これらのStoreFrontサーバーは、証明書が発行される際にFASにユーザーIDをアサートします。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。この機能は、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追加されるものです。

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を介した相互認証された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。このログは、監視および監査情報に使用できます。「[イベントログ](#)」セクションには、生成可能なイベントログエントリが一覧表示されています。

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キーを含むすべての秘密キーは、Network Serviceアカウントによってエクスポート不可能な秘密キー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。

PowerShellコマンドを使用して、低レベルの暗号化構成を利用できます。FAS承認証明書の秘密キーとユーザー証明書キーには、異なる設定を使用できます。詳細については、「[秘密キーの保護](#)」を参照してください。

管理者の責任

環境の管理は、次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	フォレスト内の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Controller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。

Citrixでは、誤った構成を避けるため、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は、特にエントリの削除や並べ替えを行う場合に注意してください。

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）に限定する必要があります。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る場合は、次の操作を行う必要があります。

- 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。)
 - Microsoft MMC 証明書テンプレートスナップインまたは Publish-FasMsTemplate コマンドを使用してテンプレートを公開し、
 - 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

デフォルトでは、ユーザー証明書の有効期間は 7 日間です。証明書テンプレートで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、[秘密鍵の保護](#) を参照してください。

キー構成証明プロパティの変更

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。

廃止されたテンプレートプロパティの変更

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

拡張プロパティの変更

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。

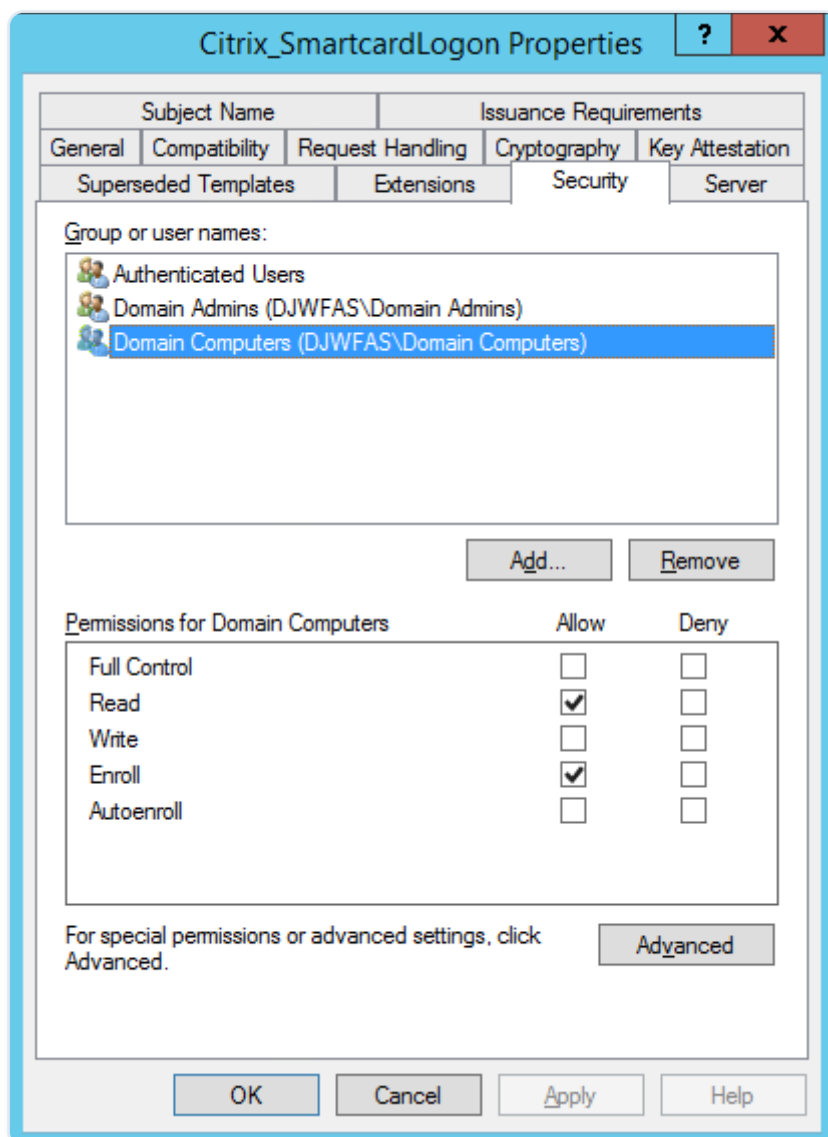
注:

不適切な拡張設定は、セキュリティ上の問題を引き起こしたり、使用できない証明書になったりする可能性があります。

セキュリティプロパティの変更

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お勧めします。FAS サービスは、その他のアクセス許可を必要としません。ただし、他の証明書テンプレートと同様に、次のことができます。

- 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
- 認証されたユーザーがテンプレートを読み取れるようにする



サブジェクト名プロパティの変更

Citrix は、これらのプロパティを変更しないことをお勧めします。

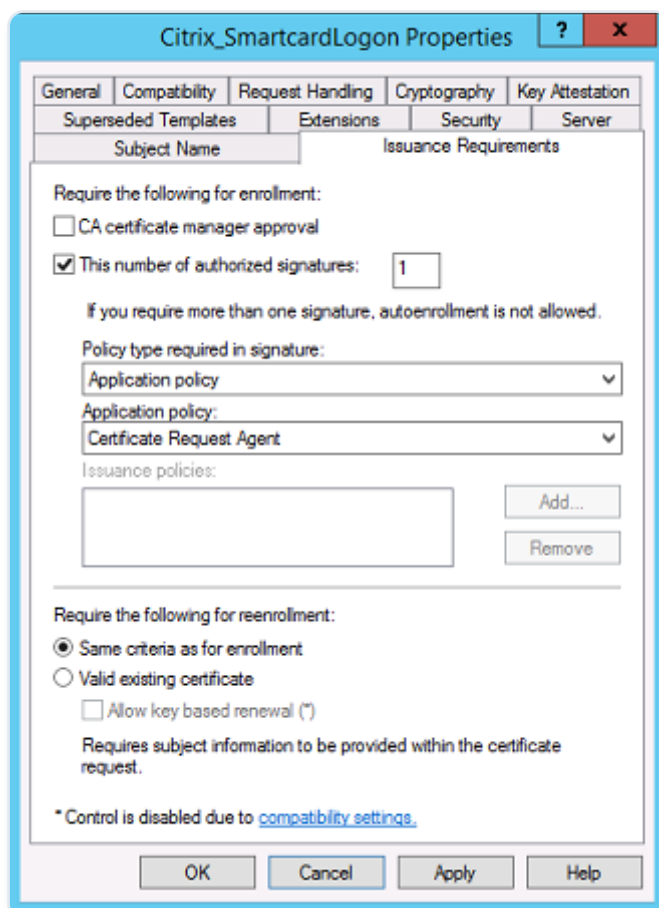
テンプレートで *Build from this Active Directory information* が選択されているため、証明機関はユーザーの SID を証明書拡張機能に含め、ユーザーの Active Directory アカウントへの強力なマッピングを提供します。

サーバープロパティの変更

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

発行要件プロパティの変更

これらの設定は変更しないでください。これらの設定は、次のようにする必要があります。



互換性プロパティの変更

これらの設定は変更できます。設定は少なくとも **Windows Server 2003 CAs** (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、上記で説明したように、FAS は **Windows Server 2008 CAs** (スキーマバージョン 3) または **Windows Server 2012 CAs** (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の秘密キーに責任を負います。

テンプレートの公開

証明機関がエンタープライズ管理者によって提供されたテンプレートに基づいて証明書を発行するには、証明機関管理者が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。

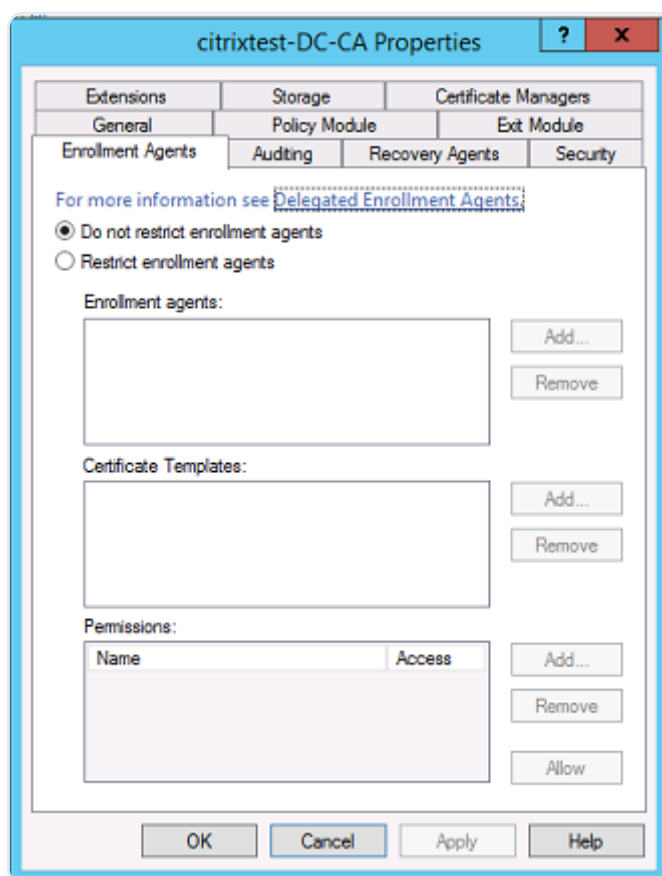
簡単なセキュリティ対策としては、FAS サーバーのインストール時に登録機関証明書テンプレートのみを公開するか、完全にオフラインの発行プロセスを要求することです。いずれの場合も、証明機関管理者は登録機関証明書要求の承認を完全に制御し、FAS サーバーを承認するためのポリシーを持つ必要があります。

ファイアウォール設定

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を制御し、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規則を構成できます。

登録の制限

デフォルトでは、登録機関証明書の所有者であれば誰でも、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。この証明書の発行は、「登録エージェントを制限する」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。



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し、拒否することができます。

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を介したStoreFront、ユーザー、およびVDAの制限

FASセキュリティモデルの中心にあるのは、どのKerberosアカウントが機能にアクセスできるかの制御です。

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に対して証明書が作成され、使用される可能性があります。
VDA [Relying party]	これらのマシンは、証明書と秘密鍵にアクセスすることを許可されています。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	このオプションは、どのユーザーがIdPによってアサートされるかを制御します。証明機関の「制限付き登録エージェント」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によって許可されてはなりません。

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Kerberosアクセス制御リスト（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

異なるアクセス権限に対して、異なる証明書テンプレートとCAを構成できます。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特権を持つ証明書を持つことができます。

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で使用可能であるかどうかを制御できます。例えば、ユーザーはセッション内で「署名」証明書のみを利用可能にでき、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ます。

秘密鍵の保護と鍵長

FAS管理者は、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FASを構成できます。Citrixは、少なくともFAS承認証明書の秘密鍵をTPMに保存して保護することを推奨しています。

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、RSAを使用する場合は少なくとも2048ビットの長さである必要があります。

注：

FASはユーザー証明書鍵をTPMまたはHSMで生成および保存できますが、大規模な展開ではハードウェアが遅すぎたり、サイズが制約されたりする可能性があります。

詳細については、「[秘密鍵の保護](#)」を参照してください。

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の[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。FAS構成は適切に維持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

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。

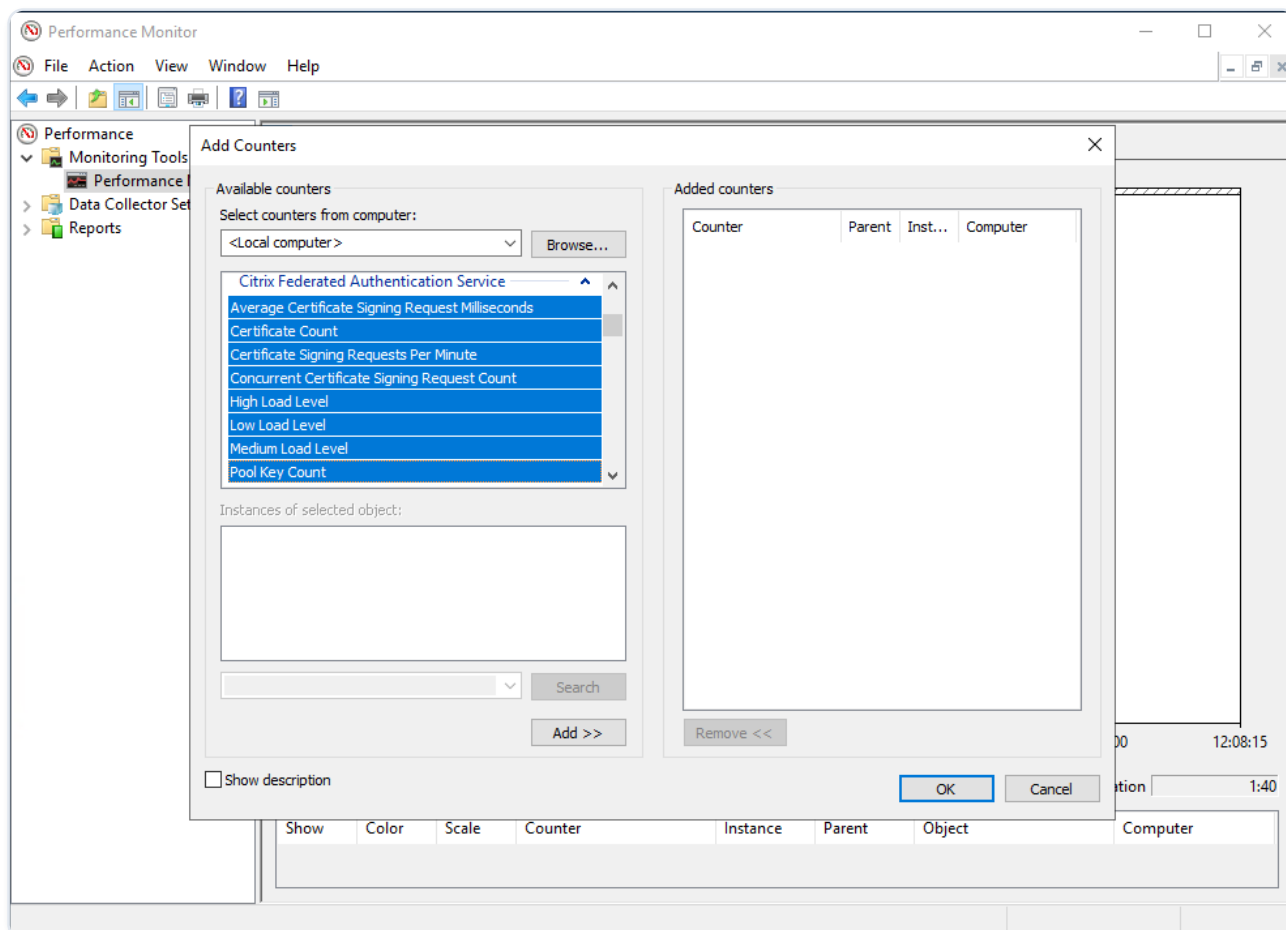
RDPアクセスは、承認された管理者に限定する必要があります。Citrixは、ユーザーアカウント、特に証明機関およびドメイン管理者アカウントに対して、スマートカードログオンを推奨しています。

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。
- FASアーキテクチャは、[展開アーキテクチャ](#)の記事で紹介されています。
- 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。

パフォーマンスカウンター

FASには、負荷追跡を目的とした一連のパフォーマンスカウンターが含まれています。



次の表に、利用可能なカウンターを示します。特に明記されていない限り、各カウンターは10秒ごとに更新されます。

名前	説明
平均証明書署名要求ミリ秒	証明書署名要求の平均期間（ミリ秒）。前の1分間のデータを使用して計算されます。
証明書数	フェデレーション認証サービスによって管理されている証明書の数。
1分あたりの証明書署名要求数	フェデレーション認証サービスによって1分あたりに発行された証明書署名要求の数。前の1分間のデータを使用して計算されます。
同時証明書署名要求数	フェデレーション認証サービスによって処理されている同時証明書署名要求の数。
プールキー数	証明書署名要求に使用できる、キープール内の事前生成されたキーペアの数。

名前	説明
1分あたりの秘密キー操作	Federated Authentication Serviceによって1分あたりに実行される証明書秘密キー操作の数。これは前分のデータを使用して計算されます。
セッション数	Federated Authentication Serviceによって追跡されているVDAセッションの数。
低/中/高負荷レベル	Federated Authentication Serviceが1分あたりに受け入れ可能な証明書署名要求の負荷の見積もり。見積もりは、前分のデータを使用して毎分更新されます。「高負荷」のしきい値を超えると、公開されたアプリまたはデスクトップの起動が失敗する可能性があります。

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、ユーザーが証明書またはスマートカード、あるいはその両方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。

証明書と公開鍵基盤

Windows Active Directoryは、ログオンするユーザーの証明書を管理するいくつかの証明書ストアを維持します。

- **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 プログラムから次のように入力します: `certutil -viewstore -enterprise NTAuth`
- **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、すべてのマシンの中間証明書ストアにはこれらの証明書が含まれている必要があります。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拡張キー使用法 (EKU) が含まれている必要があります。
AllowSignatureOnlyKeys	既定では、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	既定では、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。
EnumerateECCerts	楕円曲線認証を有効にします。
X509ヒントニーデッド	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、またはそれが曖昧な場合、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 (ドメインコントローラーで設定)。

- **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、Subject Alternate Name拡張機能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。

Active Directoryにおける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。単一のドメインは、RootDSEに複数のFQDNアドレスを登録できます。

また、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、各用途の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、コンピューターは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するため便利です。

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) を構成することで、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。この構成は、デバッグが完了したら元に戻す必要があります。

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できます。グループポリシーエディターを開くには、ドメインコントローラーで **gpedit.msc** を実行します。監査ポリシーが有効になると、ドメインコントローラーはセキュリティログに追加のイベントログ情報を生成します。

アカウント監査イベントを有効にする(/en-us/federated-authentication-service/2411/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。

ドメインコントローラーとVDAマシンで、イベントビューアーを開き、**アプリケーションとサービスログ > Microsoft > Windows > CAPI2 > Operational** に移動します。**Operational** を右クリックし、**ログの有効化** を選択します。

さらに、**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32** にあるレジストリ値を使用してCAPIログを微調整します。以下の値はデフォルトでは存在しません。これらを作成する必要があります。デフォルトのCAPI2ログ設定に戻したい場合は、これらの値を削除してください。

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CertGetCertificateChainを呼び出した (結果を含む)
失効の検証	LSAがCertVerifyRevocationを呼び出した (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 AppData\LocalLow\Microsoft\X509Objectsにダ ンプされます
チェーンポリシーの検証	LSAがCertVerifyChainPolicyを呼び出した (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 が成功しません。 (/ja-jp/federated- authentication-service/2411/config-manage/ troubleshoot-logon.html#certificates-and-

エラーコード	説明
	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	こ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ログインを有効にするには、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\LSa\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\LSa\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、診断が容易である必要があります。
- 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

ドメインコントローラーとワークステーションログ

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、次の形式でログエントリのシーケンスを生成します。

ドメインコントローラー CAPI2 ログ (/en-us/federated-authentication-service/2411/media/fas-troubleshoot-logon-capi2-log.png)

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。

ドメインコントローラー CAPI2 ログ 2 (/en-us/federated-authentication-service/2411/media/fas-troubleshoot-logon-capi2-chainpolicy.png)

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、主要なイベントは4768です。このイベントでは、証明書がKerberosチケット許可チケット (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への認証に使用されていることを示しています。

ドメインコントローラー セキュリティログ (/en-us/federated-authentication-service/2411/media/fas-troubleshoot-logon-dc-security-log.png)

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、winlogon.exeから発生するイベントID 4648のエントリです。

VDAセキュリティログ (/en-us/federated-authentication-service/2411/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および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。

VDA CAPIログ (/en-us/federated-authentication-service/2411/media/fas-troubleshoot-logon-capi-log.png)

VDA CAPIログ 2 (/en-us/federated-authentication-service/2411/media/fas-troubleshoot-logon-capi-chainpolicy.png)

VDAシステムログ

Kerberosログ記録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（無視して構いません）と、Kerberosログオンが成功したことを示すWindowsログオンからのエントリが表示されます。

VDAシステムログ (/en-us/federated-authentication-service/2411/media/fas-troubleshoot-logon-vda-system-log.png)

Windowsイベントログを使用したFASの監視

すべてのFASイベントは、Windowsのアプリケーションイベントログに書き込まれます。System Center Operations Manager (SCOM) などの製品を使用して、ここで説明されているプロセスとイベントを使用してFASサービスの正常性を監視できます。

FASサービスは実行中ですか？

FASサービスが実行中であるかどうかを判断するには、Citrix.Authentication.FederatedAuthenticationService.exeプロセスを監視します。

このセクションでは、FASサービスを監視するための最も重要なイベントのみを説明します。FAS イベントコードの完全なリストについては、[FASイベントログ](#)を参照してください。

FASヘルスイベント

以下のイベントは、FASサービスが正常であるかどうかを示します。

イベントソースは **Citrix.Authentication.FederatedAuthenticationService** です。

イベント	イベントテキスト	説明	注
[S003]	管理者 [{0}] がメンテナンスモードを [{1}] に設定	FASサービスがメンテナンスモードに移行したか、メンテナンスモードから解除されました。	メンテナンスモード中は、FASサーバーはシングルサインオンに使用できません。
[S022]	管理者 [{0}] がメンテナンスモードをオフに設定	FASサービスがメンテナンスモードから解除されました。	FAS 10.7 / Citrix Virtual Apps and Desktops 2109以降で利用可能です。
[S023]	管理者が[{0}]メンテナンスモードをオンに設定しました。	FASサービスがメンテナンスモードになりました。	FAS 10.7 / Citrix Virtual Apps and Desktops 2109以降で利用可能です。
[S123]	[upn: {0} role: {1}] [exception: {2}]の証明書をいずれのCAでも発行できませんでした。	このイベントは、FASが構成されているCAのいずれもユーザー証明書を正常に発行できなかった場合に、[S124]の後に発生します。そのユーザーのシングルサインオンは失敗します。	このイベントは、構成されているすべてのCAが機能していないことを示します。FASがHSMを使用するように構成されている場合、HSMが機能していないことも示している可能性があります。
[S124]	[certificate authority: {2}] [exception: {3}]で [upn: {0} role: {1}]の証明書を発行できませんでした。	FASが指定されたCAからユーザー証明書を要求しようとしたときに、失敗が発生しました。FASが複数のCAで構成されている場合、FASは別のCAで要求を試行します。	このイベントは、CAが機能していないか、連絡できないことを示している可能性があります。FASがHSMを使用するように構成されている場合、HSMが機能していないことも示している可能性があります。例外は、問題の原因を特定するのに役立ちます。

イベント	イベントテキスト	説明	注
[S413]	承認証明書の有効期限が間もなく切れま す（残り{0}日）。証 明書の詳細：{1}	このイベントは、 FAS承認証明書の有 効期限が近づくとき定 期的に生成されま す。デフォルトで は、承認証明書の有 効期限が30日以内で ある場合、このイベ ントは毎日生成され ます。	デフォルト設定は、 コマンドレット Set- FasRaCertificateMo nitor を使用して調整 できます。詳細につ いては、 PowerShell コマンドレット を参 照してください。
[S414]	承認証明書の有効期 限が切れました。証 明書の詳細: {0}	FAS承認証明書の有 効期限が切れると、 このイベントが定期 的に生成されます。 デフォルトでは、こ のイベントは毎日生 成されます。	有効期限が切れる と、FASは新しい ユーザー証明書を生 成できなくなり、シ ングルサインオンが 失敗し始めます。

クラウド接続FASイベント

Citrix Cloud™でFASを使用している場合、以下のイベントは、FASサービスが正常であるかどうかを示します。

イベントソースは **Citrix.Fas.Cloud** です。

イベント	イベントテキスト	説明	注
[S012]	FASサービスはCitrix Cloudからのシング ルサインオンに利用 可能です	このイベントは、 Workspace (つまり Citrix Cloud) からの シングルサインオン が機能しているはず であることを示しま す。	このイベントを発行 する前に、FASは (1) 構成されているこ と、(2) メンテナンス モードではないこ と、および (3) Citrix Cloudに接続されて いることを確認しま す。
[S013]	FASサービスはCitrix Cloudからのシング ルサインオンに利用	このイベントは、 FASがWorkspace (つまりCitrix	FASはCitrix Cloudへ の永続的な接続を維 持します。時折、こ

イベント	イベントテキスト	説明	注
	できません。[{0}] 詳細については、管理コンソールで確認できます。	Cloud) からのシングルサインオンを提供できないことを示しています。メッセージには、シングルサインオンが機能しない理由が含まれています。	の接続はさまざまな理由（ネットワークの不具合やプロキシサーバーの接続寿命ポリシーなど）で切断されることがあります。このような場合、イベントテキストには「Service is not connected to the cloud」と表示されます。これは通常の動作であり、FASはCitrix Cloudへの接続を直ちに再確立しようとします。

セキュリティイベント

次のイベントは、不正なエンティティがFASを使用しようとしたことを示しています。

イベントソースは **Citrix.Authentication.FederatedAuthenticationService** です。

イベント	イベントテキスト	説明
[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	FASの構成を表示または変更しようとしたましたが、呼び出し元はFAS管理者ではありませんでした。
[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	FASルールの構成を表示または変更しようとしたましたが、呼び出し元はFAS管理者ではありませんでした。
[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。	ユーザーIDをアサートしようとしたましたが、呼び出し元にはその権限がありません。FASルール構成で許可されているStoreFront™サーバー（および該当する場合は

イベント	イベントテキスト	説明
		Workspace) のみがユーザー IDをアサートできます。
[S104]	サーバー [{0}] はUPN [{1}] のアサートに失敗しました (UPNはロール [{2}] で許可されていません) 。	ユーザーIDをアサートしようとしたが、FASルール構成に従ってユーザーアカウントは許可されていません。
[S205]	依拠当事者アクセスが拒否されました - 呼び出し元アカウント [{0}] は、ルール [{1}] の許可された依拠当事者ではありません。	VDAがFASでシングルサインオンを実行しようとしたが、FASルール構成に従ってVDAは許可されていません。

FASイベントログ

次の表に、FASによって生成されるイベントログエントリを示します。

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}] はロール [{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}] からテンプレート [{2} and {3}] を使用して承認証明書を要求しています
[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}] がルール [{1}] を作成しています

ログコード
[S010] 管理者 [{0}] がルール [{1}] を更新しています
[S011] 管理者 [{0}] がルール [{1}] を削除しています
[S012] 管理者 [{0}] が証明書 [upn: {1} sid: {2} rule: {3}] を作成しています [Certificate Definition: {4} Security Context: {5}]
[S013] 管理者 [{0}] が証明書 [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}] を削除しています
[S015] 管理者 [{0}] が証明書要求 [TPM: {1}] を作成しています
[S016] 管理者 [{0}] が承認証明書をインポートしています [Reference: {1}]
[S022] 管理者 [{0}] がメンテナンスモードをオフに設定しています
[S023] 管理者 [{0}] がメンテナンスモードをオンに設定しています
[S024] 管理者 [{0}] がシステムヘルスマニターを設定しています
[S025] 管理者 [{0}] がシステムヘルスマニターを設定しています
[S026] 管理者 [{0}] がRA証明書モニターを設定しています
[S027] 管理者 [{0}] がRA証明書モニターをリセットしています
[S028] 管理者 [{0}] が [{1}] 証明書のキー構成を [{2}] に設定しています
[S029] 管理者 [{0}] が [{1}] 証明書のキー構成をデフォルト値にリセットしています [{2}]
[S030] 管理者 [{0}] がサービスプロパティを [{1}] に設定しています
[S050] 管理者 [{0}] がクラウド構成を作成しています: [{1}]
[S051] 管理者 [{0}] がクラウド構成を更新しています: [{1}]
[S052] 管理者 [{0}] がクラウド構成を削除しています
[S060] 管理者 [{0}] がクラウド登録を要求しています。インスタンス: {1}
[S060] 管理者 [{0}] がDirect Trustクラウド登録を要求しています。インスタンス: {1} CloudServiceUrlFormat: {2}

ログコード

[S061] 管理者 [{0}] クラウド登録を完了しています。リソースの場所: {1}、ルール名: {2}

[S062] 管理者 [{0}] クラウド登録が完了しました。リソースの場所: {1} ({2})、ルール名: {3}、顧客: {4} ({5})

[S063] クラウド登録中にKRSエラーが発生しました。例外は {0}

[S064] クラウド登録中に不明なエラーが発生しました。例外は {0}

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しています

[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構成に成功しました - MinThreadsが [workers: {0} completion: {1}] から [workers: {2} completion: {3}] に調整されました

[S410] ThreadPool構成に失敗しました - MinThreadsを [workers: {0} completion: {1}] から [workers: {2} completion: {3}] に調整できませんでした; これにより、FASサーバーのスケラビリティに影響が出る可能性があります

[S411] FASサービスを開始中にエラーが発生しました: [{0}]

[S412] 設定のアップグレードが完了しました -- [From version {0} to version {1}]

[S413] 承認証明書の有効期限が間もなく切れます ({0} 日残っています)。証明書の詳細: {1}

ログコード
[S414] 承認証明書の有効期限が切れました。証明書の詳細: {0}
[S415] 承認証明書のチェックが完了しました。{0} 件の問題がログに記録されました。次のチェックは {1} 後に予定されています

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}] のアサートに失敗しました (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}] のアサートに失敗しました (UPN はロール [{2}] で許可されていません)
[S105] サーバー [{0}] はIDアサーションを発行しました [upn: {1}, ロール {2}, セキュリティコンテキスト: [{3}]]
[S120] 証明書を発行しています [upn: {0} ロール: {1} セキュリティコンテキスト: [{2}]]
[S121] [upn: {0} role: {1}] に証明書が [certificate authority: {2}] によって発行されました
[S122] 警告: サーバーが過負荷状態です [upn: {0} role: {1}][1分あたりのリクエスト数 {2}]。
[S123] [upn: {0} role: {1}] の証明書をどのCAでも発行できませんでした [exception: {2}]
[S124] [upn: {0} role: {1}] の証明書を [certificate authority: {2}] で発行できませんでした [exception: {3}]
[S125] 保留中の証明書要求が完了するまで {0} 秒待機しましたが、呼び出しがタイムアウトしました [upn: {1} role: {2} Security Context: [{3}]]
[S126] サーバー [{0}] が未定義のルール [{1}] を使用してIDをアサートしようとした

ログコード

[S127] サーバーがメンテナンスモードのため、FASは [upn: {0} role: {1} definition: {2}] の証明書を要求できませんでした。メンテナンスモード中の動作を変更するには、PowerShellコマンドレット Set-FasServer を使用してください

証明書利用者の役割を果たす

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

ログコード

[S201] 証明書利用者 [{0}] はパスワードにアクセスできません。

[S202] 証明書利用者 [{0}] は証明書にアクセスできません。

[S203] 証明書利用者 [{0}] はログオンプロバイダーにアクセスできません

[S204] 証明書利用者 [{0}] が [upn: {1}] のログオンプロバイダーにアクセスしています (役割: [{2}])
[Operation: {3}] (承認者: [{4}])

[S205] 証明書利用者アクセスが拒否されました - 呼び出し元のアカウント [{0}] はルール [{1}] の許可された証明書利用者ではありません

[S206] 呼び出し元アカウント [{0}] は証明書利用者ではありません

[S208] 秘密鍵操作に失敗しました [操作: {0} upn: {1} ロール: {2} certificateDefinition {3} エラー {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サーバーでログに記録されます。

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

ログコード
[S304] ユーザー [{0}] がコンピューター [{2}] でプログラム [{1}] を実行しており、秘密鍵操作 [{6}] のため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] 秘密鍵操作に失敗しました [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}] はメソッド [{4}] の実行中に例外 [{3}] をスローしました)
[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}] は例外 [{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 (アクセス処分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)

ログコード
[S509] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (アクセス処分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 (アクセス処分はプラグイン [{2}] によって無効と見なされました)

ワークスペース対応FAS

これらのイベントは、FASがWorkspaceで使用されている場合にログに記録されます。

ログコード
[S001] Citrix Cloud 承認キーをローテーションしました [fas id: {0}] [old key id:{1}] [new key id:{2}]
[S002] クラウドサポートモジュールが起動しています。FasHub クラウドサービス URL: {0}
[S003] FAS がクラウドに登録されました [fas id: {0}] [transaction id: {1}]
[S004] FAS がクラウドへの登録に失敗しました [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S005] FAS が現在の構成をクラウドに送信しました [fas id: {0}] [transaction id: {1}]
[S006] FAS が現在の構成をクラウドに送信できませんでした [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S007] FAS がクラウドから登録解除されました [fas id: {0}] [transaction id: {1}]
[S009] FAS がクラウドからの登録解除に失敗しました [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S010] FAS サービスはクラウドメッセージング URL: {0} に接続されています
[S011] FAS サービスはクラウドに接続されていません
[S012] FAS サービスは Citrix Cloud からのシングルサインオンに利用可能です
[S013] FAS サービスは Citrix Cloud からのシングルサインオンに利用できません。[{0}] 詳細については、管理コンソールで確認できます
[S014] クラウドサービス <service name> への呼び出しが失敗しました [fas id: {0}] [transaction id: {1}] [exception: {2}]

ログコード
[S015] Citrix Cloud からのメッセージは、呼び出し元が許可されていないためブロックされました [message ID {0}] [transaction ID {1}] [caller {2}]
[S016] クラウドサービス <service name> への呼び出しが成功しました [fas id: {0}] [transaction id: {1}]
[S019] FASがクラウドから構成をダウンロードしました [fas id: {0}] [transaction id: {1}]
[S020] FASがクラウドから構成をダウンロードできませんでした [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S021] クラウドサポートモジュールの起動に失敗しました。例外: {0}
[S022] クラウドサポートモジュールを停止しています
[S023] Citrix Cloud認証キーのローテーションに失敗しました [fas id: {0}] [current key id:{1}] [new key id:{2}] [keys in cloud:{3}]
[S024] Citrix Cloud認証キーのローテーションを開始しています [fas id: {0}] [current key id:{1}] [new key id:{2}]
[S025] このサービスの認証キーはCitrix Cloudに存在します [current key: {0}] [keys in cloud: {1}]
[S026] このサービスの認証キーはCitrix Cloudに存在しません [current key: {0}] [keys in cloud: {1}]
[S027] Citrix Cloud認証キーのストレージ形式をアップグレードしました [fas id: {0}]
[S028] FASが現在のテレメトリをクラウドに送信しました [fas id: {0}] [transaction id: {1}]
[S029] FASが現在のテレメトリをクラウドに送信できませんでした [fas id: {0}] [transaction id: {1}] [exception: {2}]

ログオン

これらのイベントは、ログオン段階で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}]

ログコード
[S102] IDアサーションログオンに失敗しました。{0} のSIDルックアップに失敗しました [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。{0} への呼び出しが返しました [Error: {1} {2}]
[S105] IDアサーションログオン。ログオン中 [Username: {0} Domain: {1}]
[S106] IDアサーションログオン。 フェデレーション認証サービス: {0} ログオン中 [Certificate: {1}]
[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。アクセス拒否 [Caller: {0}]

セッション内証明書

ユーザーがセッション内証明書の使用を試みたときに、これらのイベントは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} のために承認されました
[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になっています

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に記録されます。

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}]

ログコード
[S014] Pkcs10Request::Create: PKCS10要求を作成しました [Distinguished Name: {0}] [Reason: {1}]
[S016] 秘密鍵の作成 [Identifier: {0}] [MachineWide: {1}] [Provider: {2}] [ProviderType: {3}] [EllipticCurve: {4}] [KeyLength: {5}] [isExportable: {6}] [CreateReason: {7}]
[S017] 秘密鍵の削除 [Provider: {0}] [Identifier {1}]
[S018] PrivateKey::Create に失敗しました [Identifier: {0}] [MachineWide: {1}] [Provider: {2}] [ProviderType: {3}] [EllipticCurve: {4}] [KeyLength: {5}] [isExportable: {6}] [CreateReason: {7}] [Exception: {8}]

ログコード
[S104] MicrosoftCertificateAuthority::GetCredentials: {0}を使用する権限があります
[S105] MicrosoftCertificateAuthority::SubmitCertificateRequest 応答の送信エラー [{0}]
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest 証明書を発行しました [{0}]
[S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - 承認待ち [CR_DISP_UNDER_SUBMISSION] [Reference: {0}]

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ログオンページに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鍵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「 Kerberos ログ 」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。資格情報を確認できませんでした。/ 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。「Kerberos認証」、「ドメインコント

表示されるエラーメッセージ	説明と参照
	ローラー認証」、または「ドメインコントローラー」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、これを試す価値はあります。
システムはログオンできない可能性があります。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。 証明書と公開鍵インフラストラクチャ 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のドメイン構成](#)
- [スマートカードログオンポリシー](#)
- [CAPIログの有効化](#)
- [Kerberosログの有効化](#)
- [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](#)

PowerShell コマンドレット

フェデレーション認証サービス (FAS) 管理コンソールは簡単な展開に使用できますが、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/>](https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/) を参照してください。

展開アーキテクチャ

はじめに

フェデレーション認証サービス (FAS) は、Active Directory 証明機関と統合されるCitrix® コンポーネントであり、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あらゆる認証テクノロジーを、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、複雑さが増す順に、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](#)
- [Citrix Gateway の展開](#)
- [ADFS SAML](#)
- [B2Bアカウントマッピング](#)
- [Windows 10 Azure 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](#)の記事は、FASをセットアップするための主要なリファレンスです。

アーキテクチャの概要

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 of 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。

信頼されたStoreFront™サーバーは、ユーザーがCitrix環境へのアクセスを要求すると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することを許可するチケットを発行します。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。FASのみがユーザー証明書の秘密キーにアクセスできます。VDAは、証明書で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。

次の図は、FASがMicrosoft証明機関と統合され、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様子を示しています。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-architecture.png)

内部展開

FASは、ユーザーが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るようにします。

これにより、ユーザー資格情報やスマートカードPINの入力を求めるプロンプトなしでWindows認証が可能になり、Single Sign-on Service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、エンドポイントデバイスにスマートカードで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、このサーバーはユーザーに代わってスマートカードクラス証明書を発行する権限を持っています。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環境で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。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-architectures-internal.png)

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済みます。（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）または組み込み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のインストール方法と構成方法について説明しています。

シトリックス ゲートウェイ展開

Citrix Gateway展開は内部展開と似ていますが、StoreFrontとペアになったCitrix Gatewayを追加し、認証の主要なポイントをCitrix Gateway自体に移動します。Citrix Gatewayには、会社の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、Citrix Gatewayに最初に認証してからユーザーセッションにログオンするときに発生する複数の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要求することなく、高度なCitrix Gateway認証テクノロジーの使用も可能にします。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-architectures-netscaler.png)

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）。

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るためです。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-architectures-netscaler-auth-settings.png)

関連情報:

- Citrix Gatewayを構成するには、「[How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and Citrix Virtual Desktops 7.6](#)」を参照してください。
- [Install and configure](#)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認証テクノロジーは、SAML IDプロバイダー (IdP) として機能できる Microsoft ADFSとの統合を可能にします。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。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-architectures-adfs-saml.png)

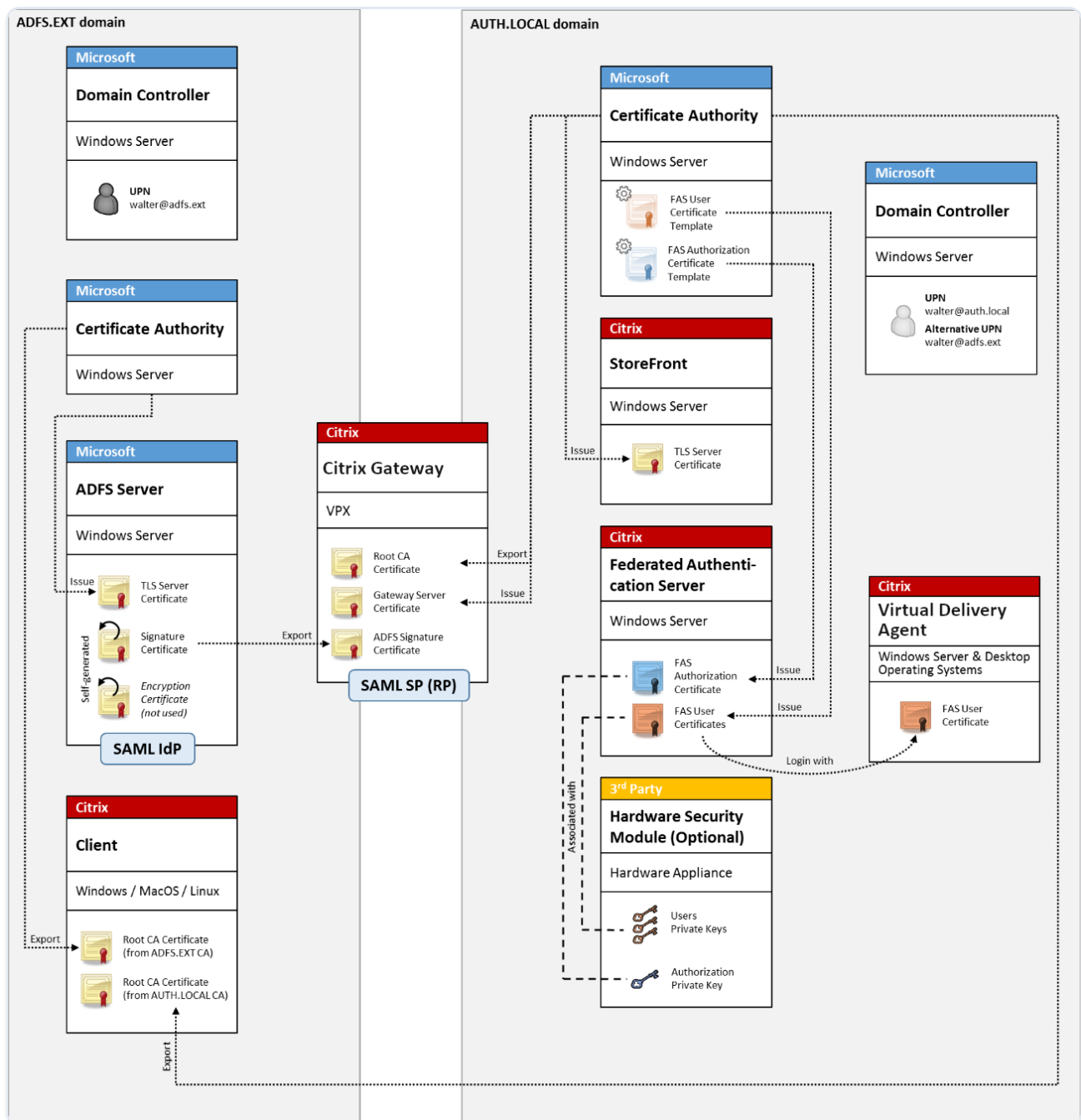
ADFSは、インターネット経由でリモートから企業リソースにユーザーを安全に認証するためによく使用されます。たとえば、Office 365の統合によく使用されます。

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(/ja-jp/federated-authentication-service/2411/deployment-architectures.html#citrix-gateway-deployment)セクションには、構成に関する考慮事項が含まれています。

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、ADFSはこれをピア会社のAD環境内の「シャドウアカウント」に自動的にマッピングします。



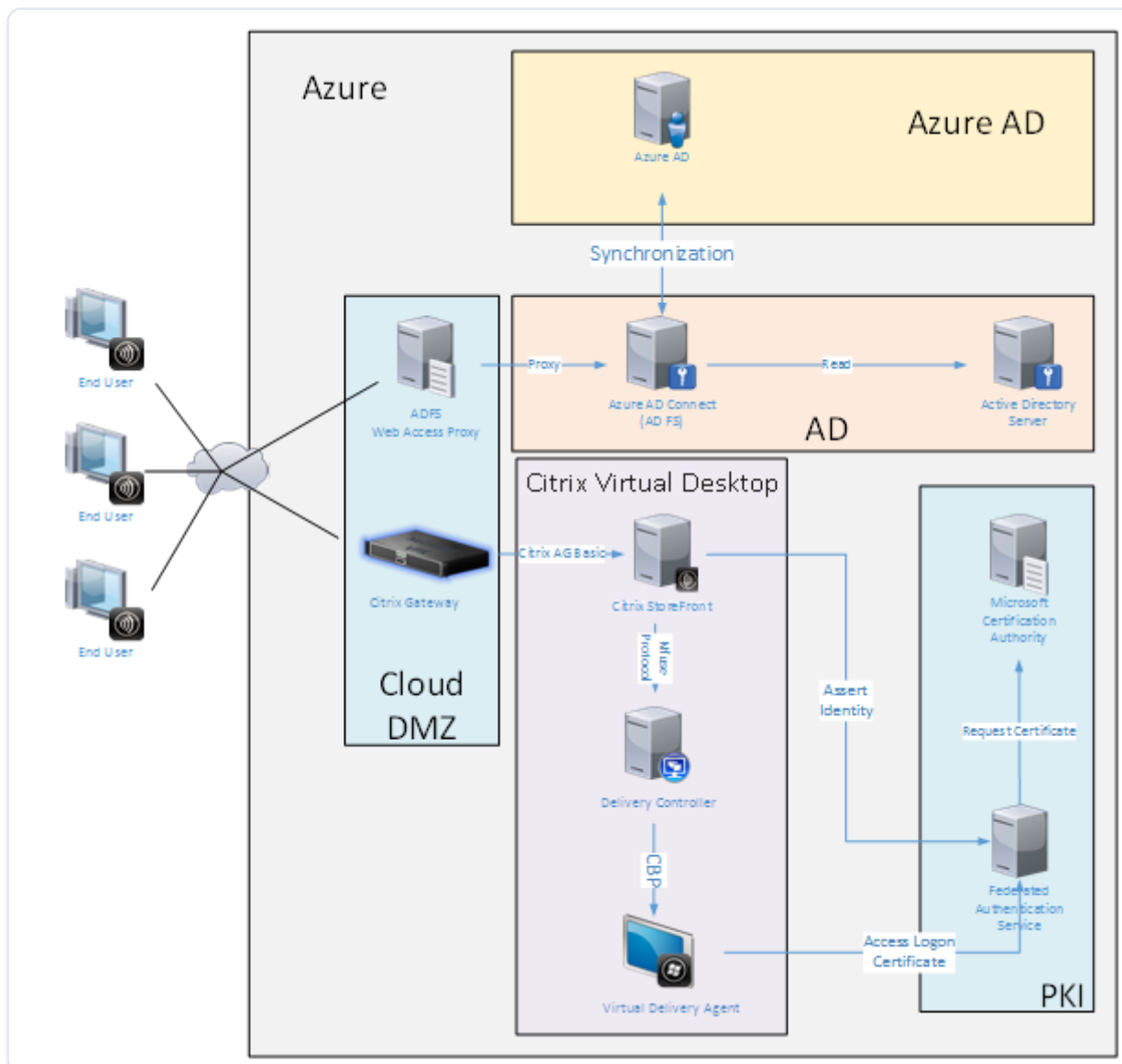
関連情報:

- ([/ja-jp/federated-authentication-service/2411/install-configure.html](http://ja-jp/federated-authentication-service/2411/install-configure.html))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。

Windows 10 Azure AD ジョイン

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、「オフィスにエンドユーザーがいる」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な場所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シンクロナイザーは、Azure ADに自動的に接続します。例のグラフィックでは、簡潔にするためにAzure VMを使用しています。

関連情報:

- ([/ja-jp/federated-authentication-service/2411/install-configure.html](https://aka.ms/ja-jp/federated-authentication-service/2411/install-configure.html))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。

- ([/ja-jp/federated-authentication-service/2411/deployment-architectures/azure-ad.html](https://ja-jp.federated-authentication-service/2411/deployment-architectures/azure-ad.html))の記事には詳細が記載されています。

ADFSの展開

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、シングルポイント認証を必要とする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。

フェデレーション認証サービス (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、従業員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/2411/media/fas-architectures-adfs-saml.png](https://en-us.federated-authentication-service/2411/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のどちらであっても、違いはありません。

SAMLの概要

Security Assertion Markup Language (SAML) は、「ログオンページへのリダイレクト」というシンプルな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がユーザーの認証が必要であ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ページへHTTP POSTを実行するよう指示します。これは通常、`https://` 形式のアドレスです：`https://adfs.mycompany.com/adfs/ls`。

このWebページPOSTには、ログオンが完了したときにADFSがユーザーを返す「戻りアドレス」を含む、他の情報が含まれています。

識別子

EntityId は、Citrix Gateway が ADFS に送信する POST データに含まれ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、必要に応じて異なる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 で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 の間で合意されていれば、一般的には何でも構いません。 `https://ns.mycompany.com/application/logonpage` .

返信アドレス

認証が成功すると、ADFS はユーザーの Web ブラウザに、SAML 認証 XML を EntityId 用に構成されている Reply URL のいずれかに 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、形式は次のとおりです。 `https://ns.mycompany.com/cgi/samlauth` .

複数の Reply 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 プロブに暗号署名します。この署名を検証するには、Citrix Gateway が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されている必要があります。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

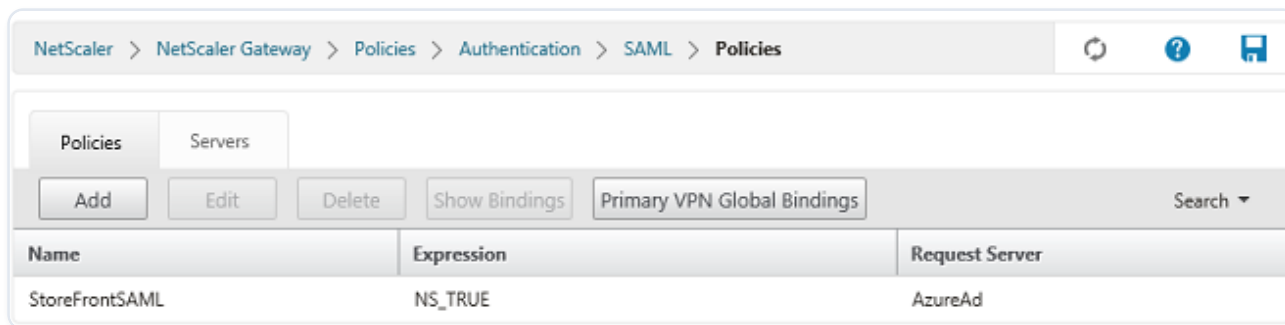
ADFS と Citrix Gateway は、「中央ログアウト」システムをサポートしています。これは、Citrix Gateway が時々ポーリングして、SAML 認証 XML プロブが現在ログオンしているセッションをまだ表しているかどうかを確認するための URL です。

これはオプション機能であり、構成する必要はありません。通常、 `https://` アドレスで、形式は `https://adfs.mycompany.com/adfs/logout` です。(Single Logon URL と同じにすることもできます。)

構成

セクション「Citrix Gateway の展開」([/ja-jp/federated-authentication-service/2411/deployment-architectures.html#citrix-gateway-deployment](#)) 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。こ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 上で作成できます。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。



SAML ポリシーの入力

ADFS 管理コンソールから以前に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 はログオンのためにユーザーを ADFS にリダイレクトし、ADFS 署名付き SAML 認証トークンを受け取ります。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-adfs-create-auth-saml-server.png)

関連情報

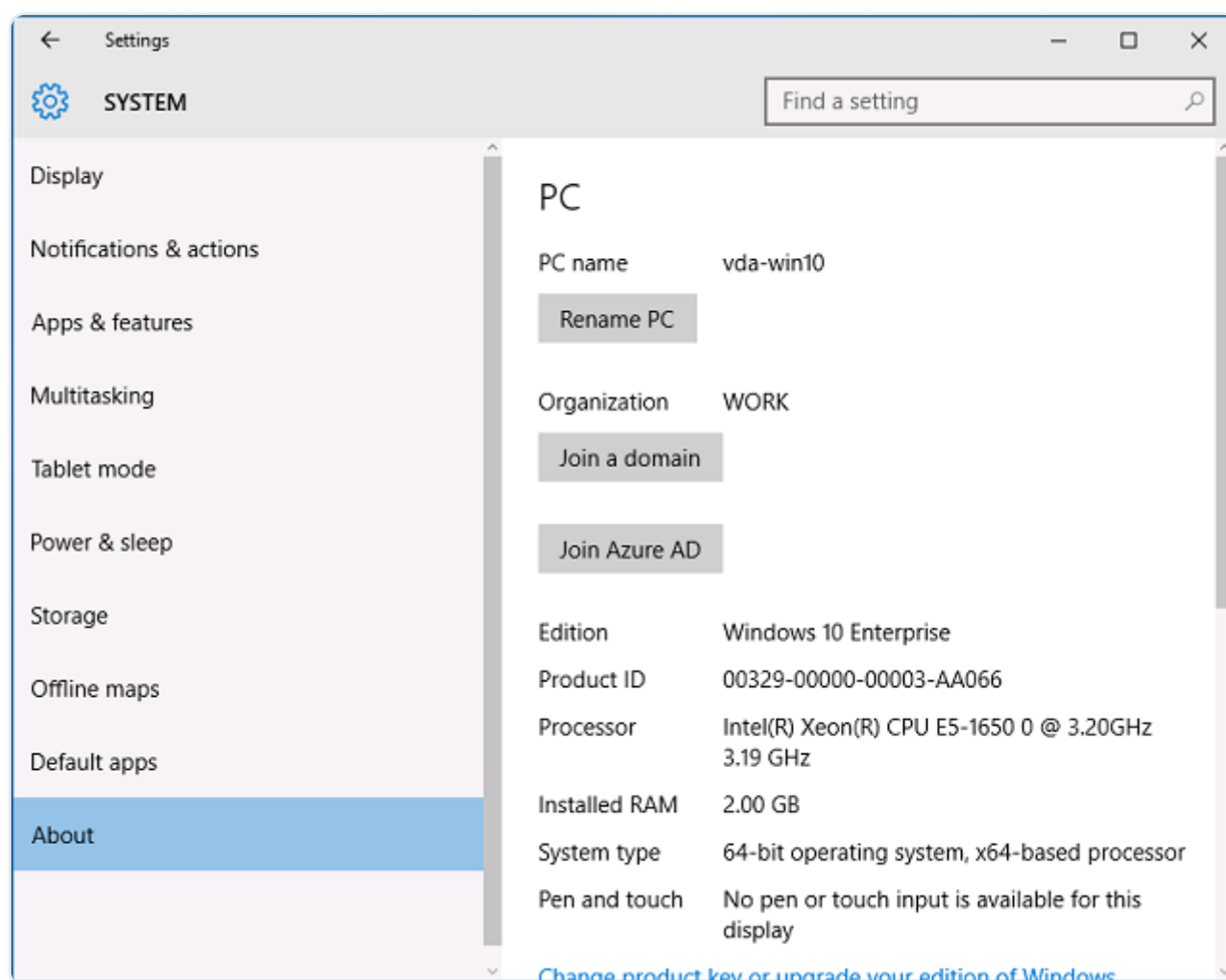
- [インストールと構成](#)は、FASのインストールと構成に関する主要なリファレンスです。
- 一般的なFAS展開は、[展開アーキテクチャ](#)の記事にまとめられています。
- 「ハウツー」記事は、[高度な構成](#)の記事で紹介されています。

Azure AD統合

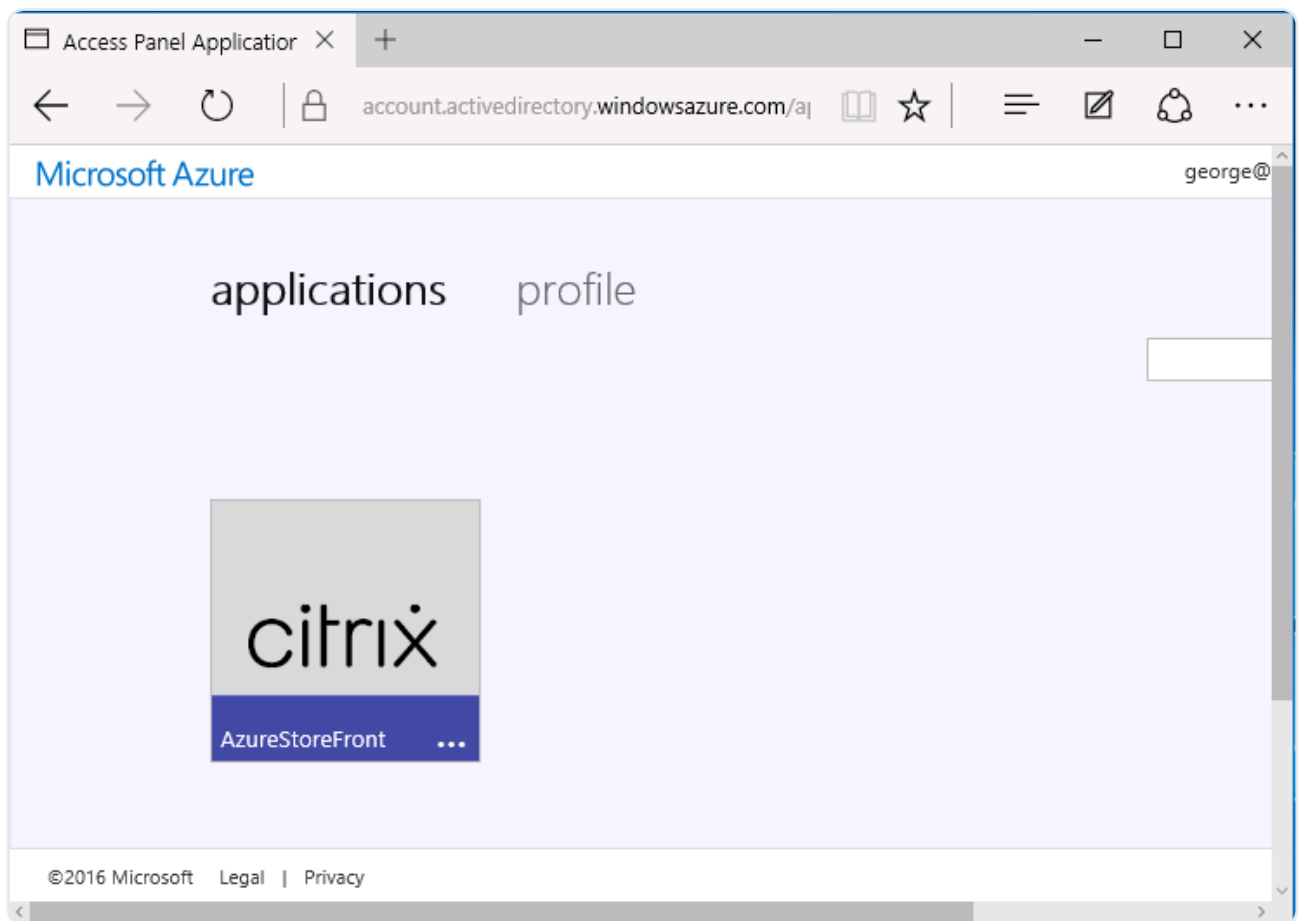
はじめに

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を目的として、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、**Settings** パネルの**System > About > Join Azure AD**オプションからこのコードにアクセスします。



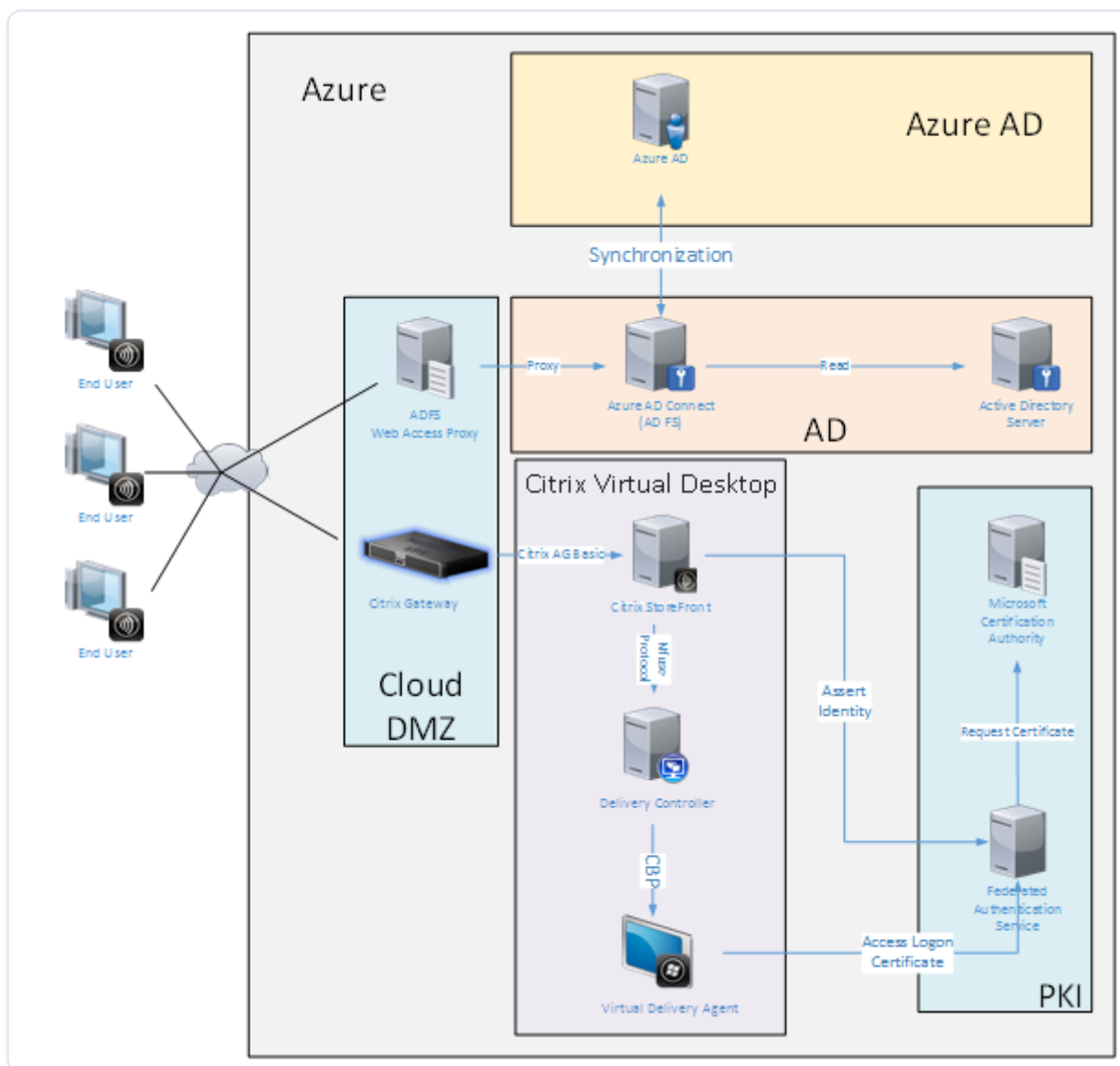
ラップトップが登録されると、Microsoft Edge Webブラウザは、Azure SaaSアプリケーションのWebページを介して、会社のWebサイトやCitrix公開アプリケーションに自動的にサインオンします。これには、Office 365などの他のAzureアプリケーションも含まれます。



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。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。



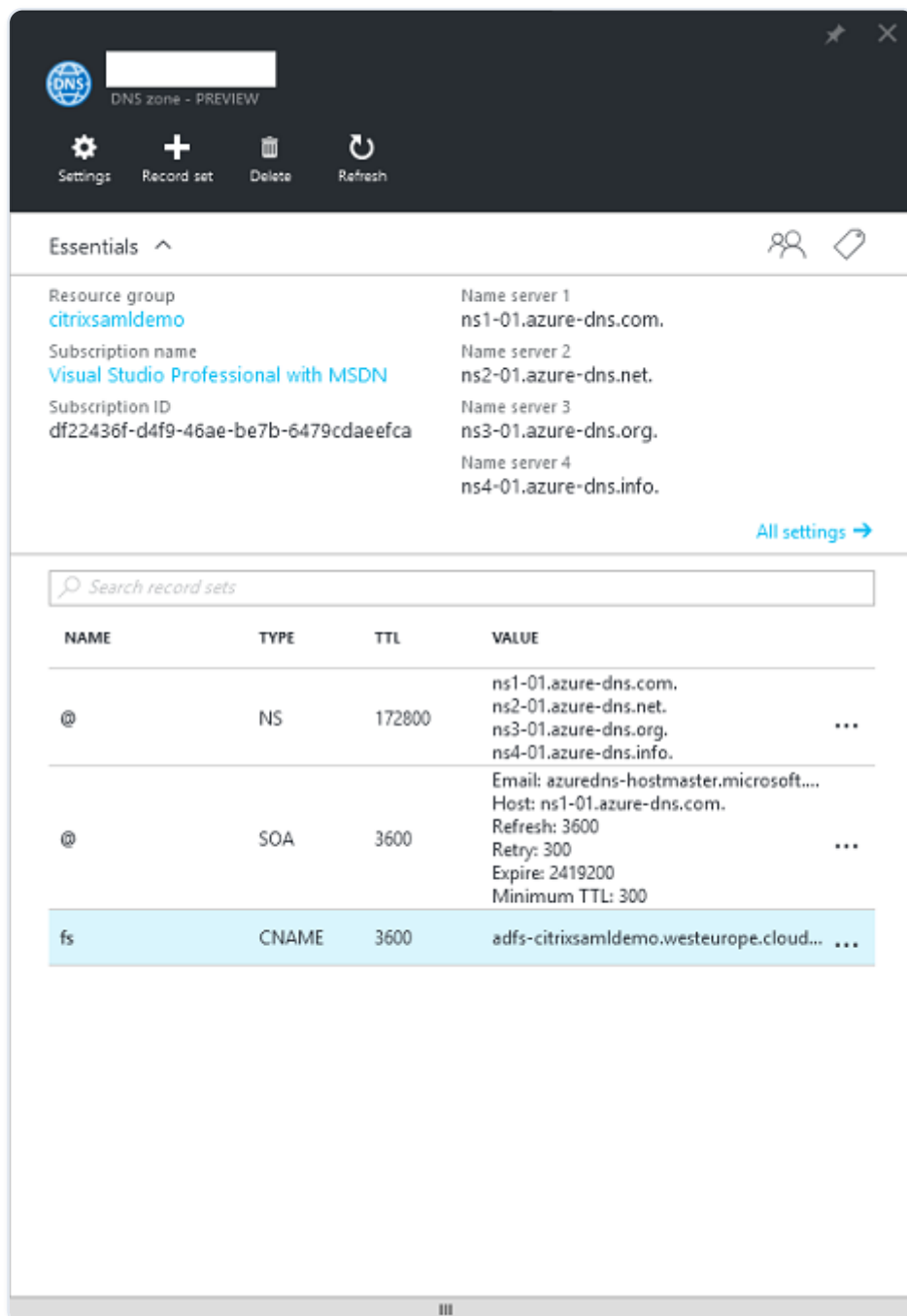
従来、ファイアウォールで保護されたLANとKerberos/NTLM認証であったセキュアな接続とシングルサインオンは、このアーキテクチャではAzureへのTLS接続とSAMLに置き換えられます。新しいサービスは、Azure ADに参加するAzureアプリケーションとして構築されます。Active Directoryを必要とする既存のアプリケーション（SQL Serverデータベースなど）は、Azure Cloud ServiceのIAAS部分にある標準のActive Directory Server VMを使用して実行できます。

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 Applications**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ゾーンの作成

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 n1-01.azure-dns.com`）。

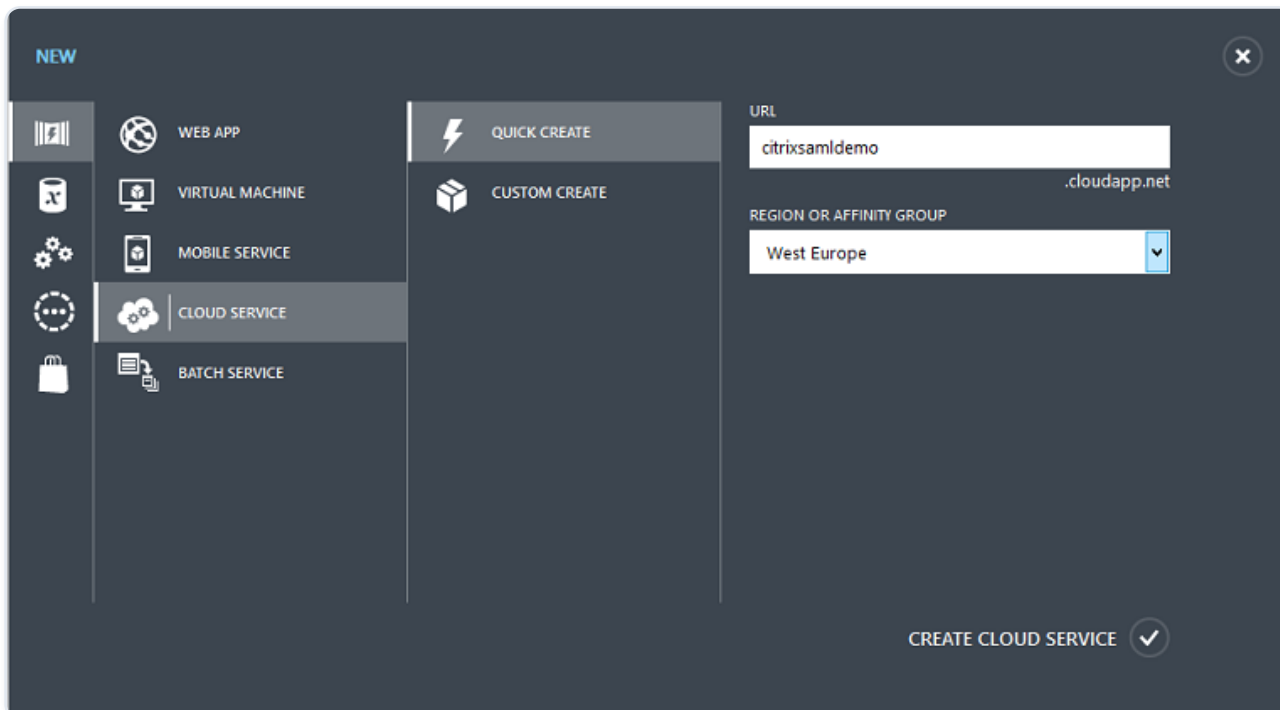
Azureで実行されているVMへの参照を追加する場合、VMのAzure管理DNSレコードへのCNAMEポインターを使用するのが最も簡単です。VMのIPアドレスが変更されても、DNSゾーンファイルを手動で更新する必要はありません。

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

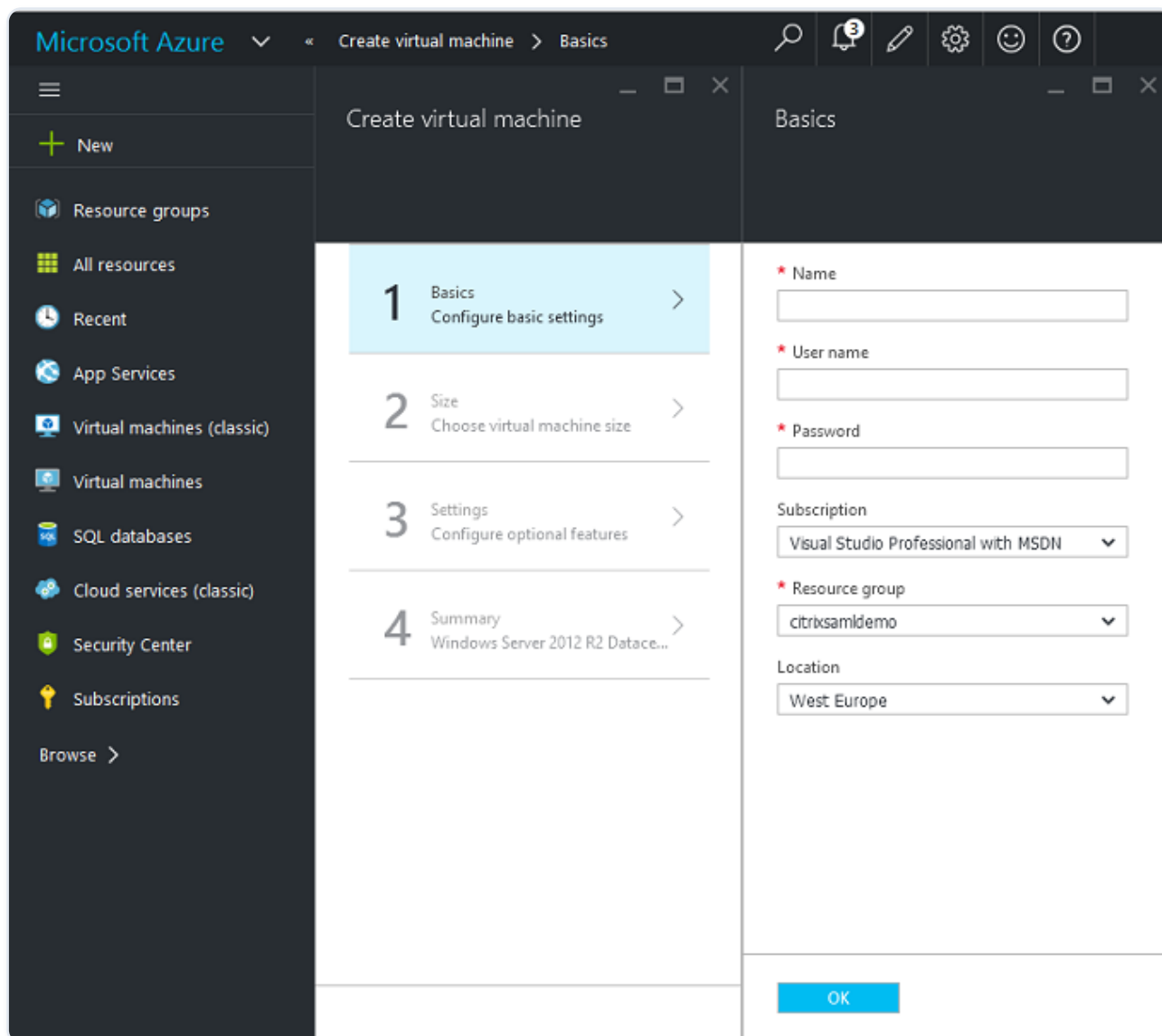
この例では、Azureで実行されているADFSサーバーを含むAD環境を含むCitrix環境を構成します。「citrixsamldemo」という名前のクラウドサービスが作成されます。



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)
- シトリックス バーチャル アプリケーションズ アンド デスクトップス デリバリー コントローラー
- Citrix Virtual Apps and Desktops 仮想配信エージェント (VDA)



ドメインコントローラー

- 標準的なActive Directory展開を作成するために、**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 (この例では、citrixsamldemo.net)。ドメイン昇格が完了した後、**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@citrixsamldemo.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**ページから行うことができます。(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citrixsamldemo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分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。

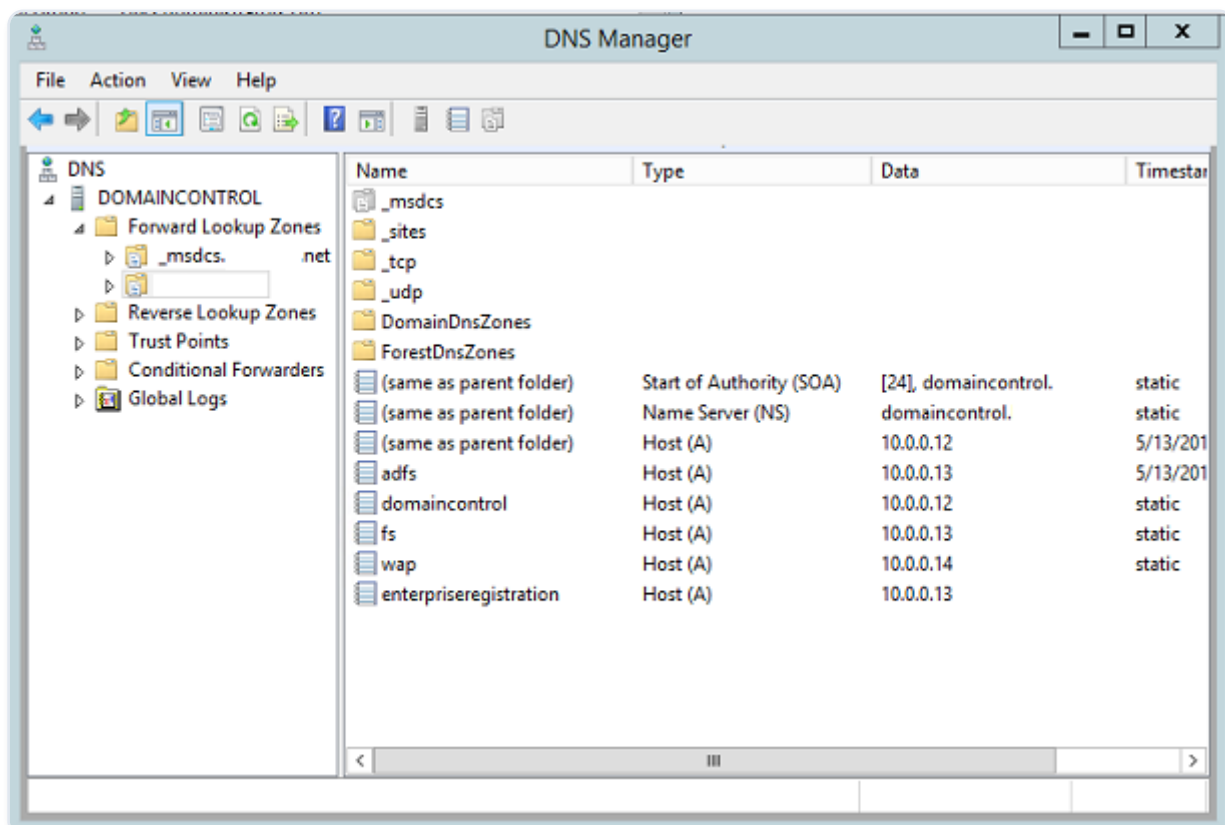
- AzureAD Connectツールからのファイアウォールを介したPSリモート処理を許可するために、これらのサーバーで**Enable-PSRemoting -Force**コマンドレットを実行します。

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

- citrixsamldemoに参加している残りの2台のWindowsサーバーに、Citrix Virtual AppsまたはCitrix Virtual Desktops Delivery Controller™およびVDAを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後、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。



以下の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ースGUIから実行できます。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-azure-config-internal-dns-dnsservers.png)

デフォルトでは、内部IPアドレス (10.0.0.9) 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が実行されている場合、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がデフォルトで各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。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-azure-config-external-dns-configuration.png)

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

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。(構成中は、パブリックIPアドレスが環境への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。デフォルトでは、すべてのVMがRDPアクセスを許可します。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。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-azure-config-security-groups.png)

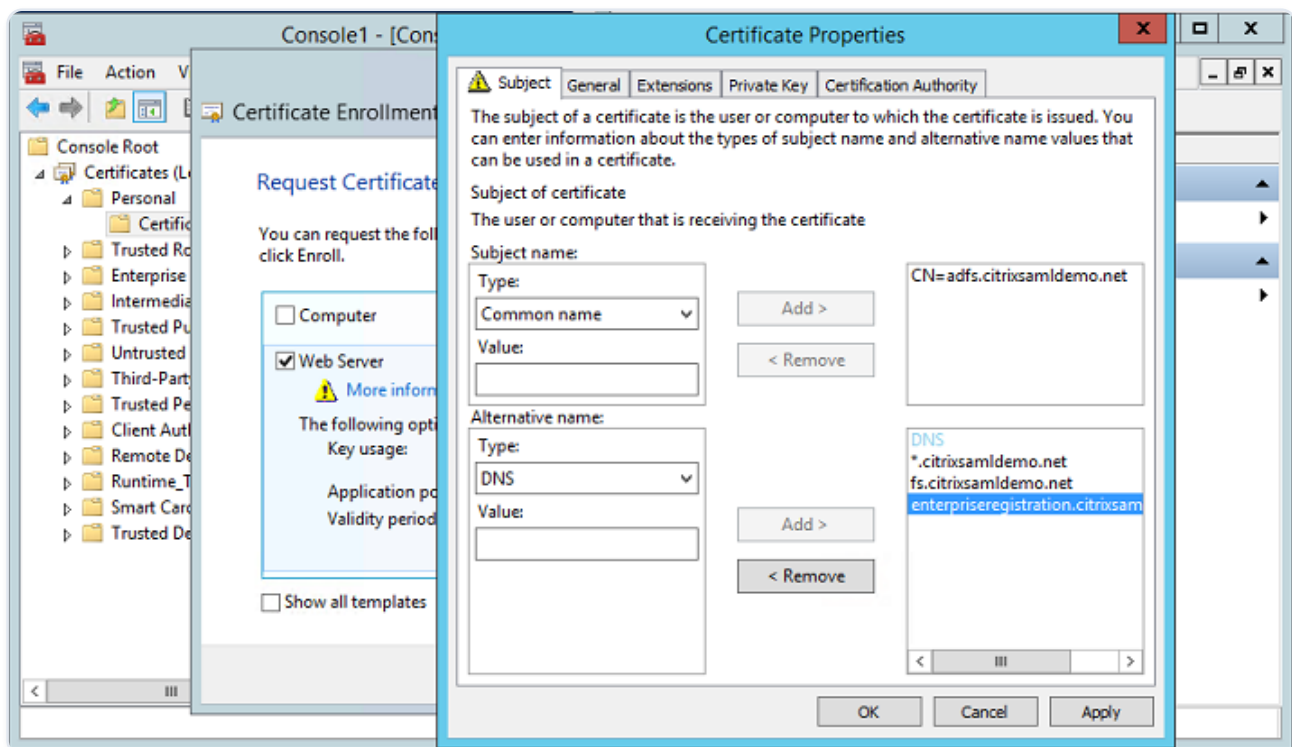
ADFS証明書を作成する

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、(秘密鍵を含めて) 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.citrixsaml demo.net
- サブジェクト代替名:
 - *.citrixsaml demo.net
 - fs.citrixsaml demo.net
 - enterpriseregistration.citrixsaml demo.net



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

Azure ADのセットアップ

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の作成

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 ?

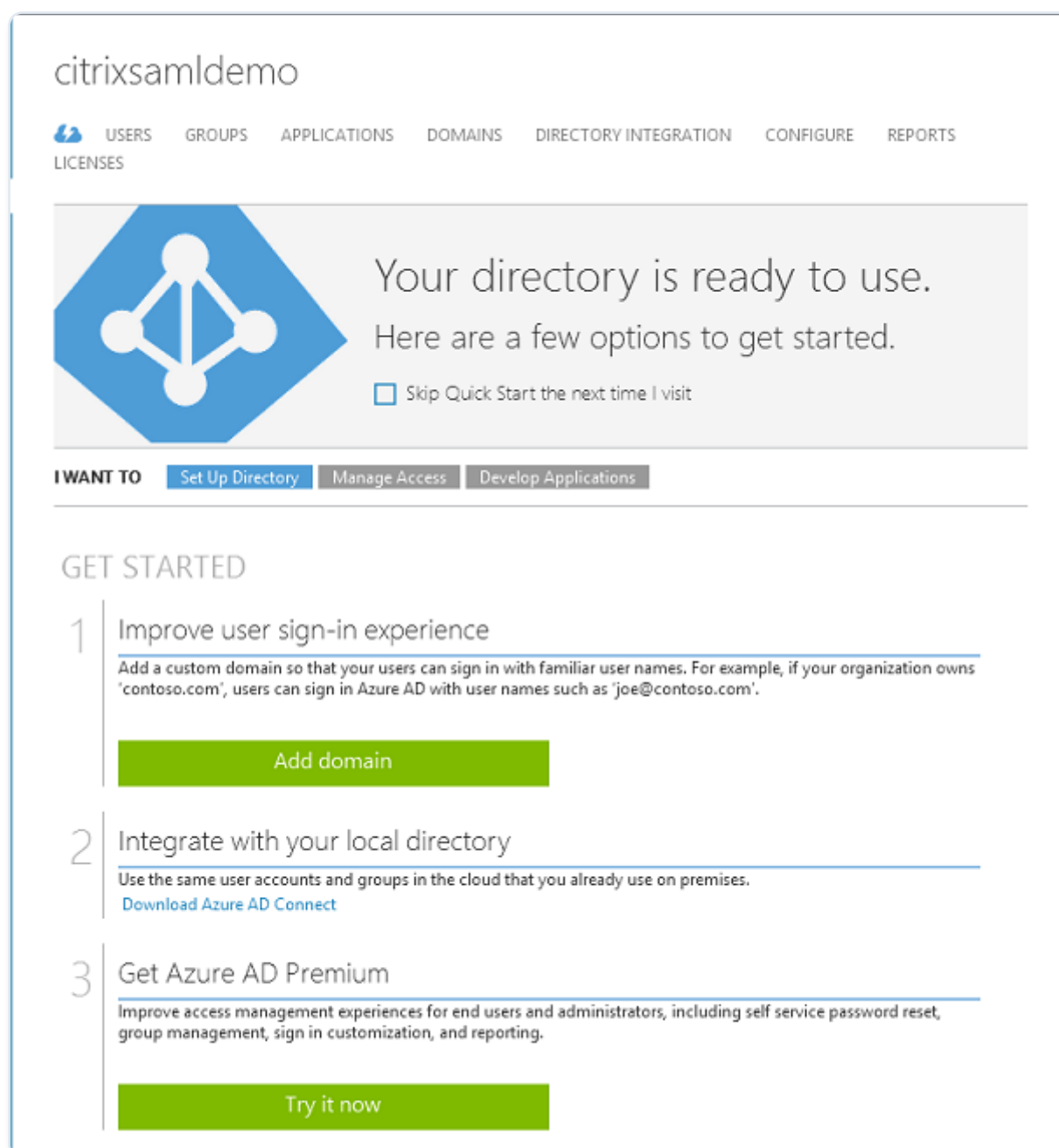
citrixsaml demo .onmicrosoft.com

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。



citrixsamldemo

[USERS](#) [GROUPS](#) [APPLICATIONS](#) [DOMAINS](#) [DIRECTORY INTEGRATION](#) [CONFIGURE](#) [REPORTS](#)
[LICENSES](#)



Your directory is ready to use.
Here are a few options to get started.

☐ Skip Quick Start the next time I visit

I WANT TO

[Set Up Directory](#) [Manage Access](#) [Develop Applications](#)

GET STARTED

- 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'.

[Add domain](#)
- 2 Integrate with your local directory

Use the same user accounts and groups in the cloud that you already use on premises.

[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.

[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 (この例では `AzureAdmin@citrixsamldemo.onmicrosoft.com`) を作成し、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

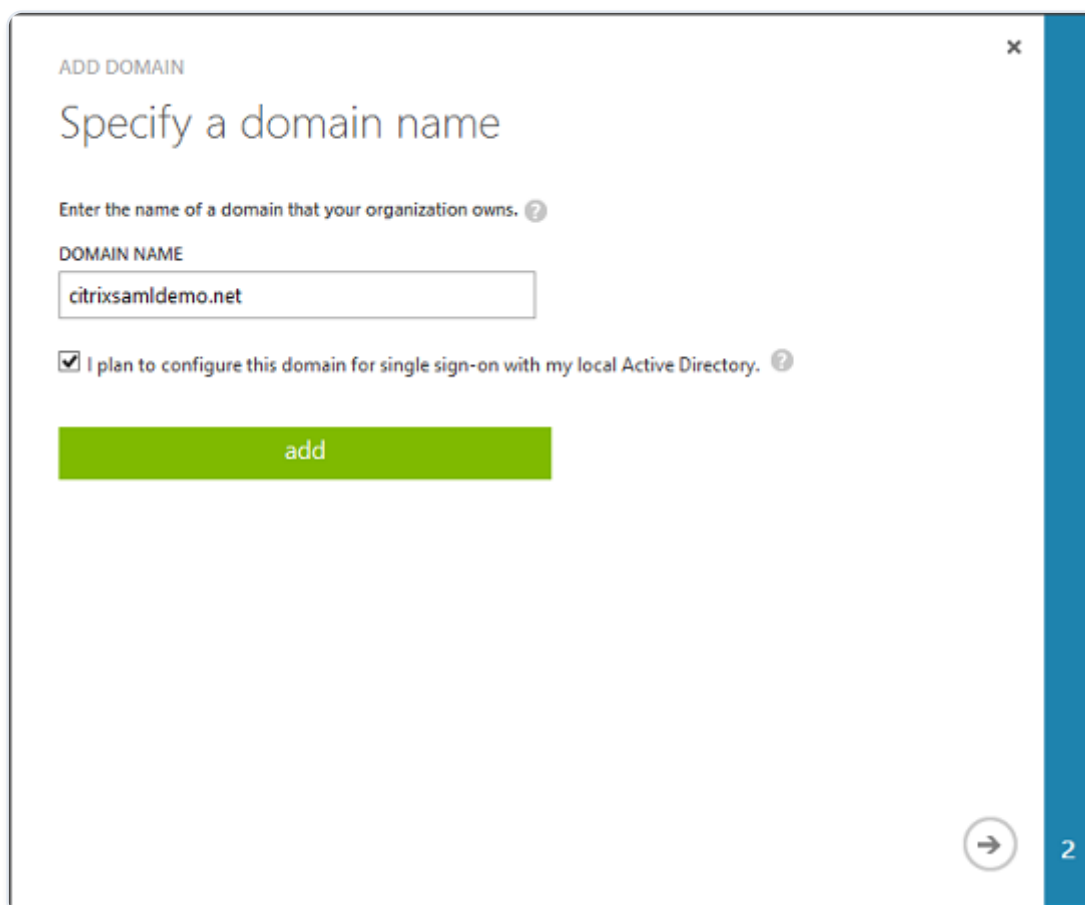
ドメインを Azure AD に登録する

デフォルトでは、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良いです: `<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 `citrixsam1demo.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

citrixsaml-demo.net

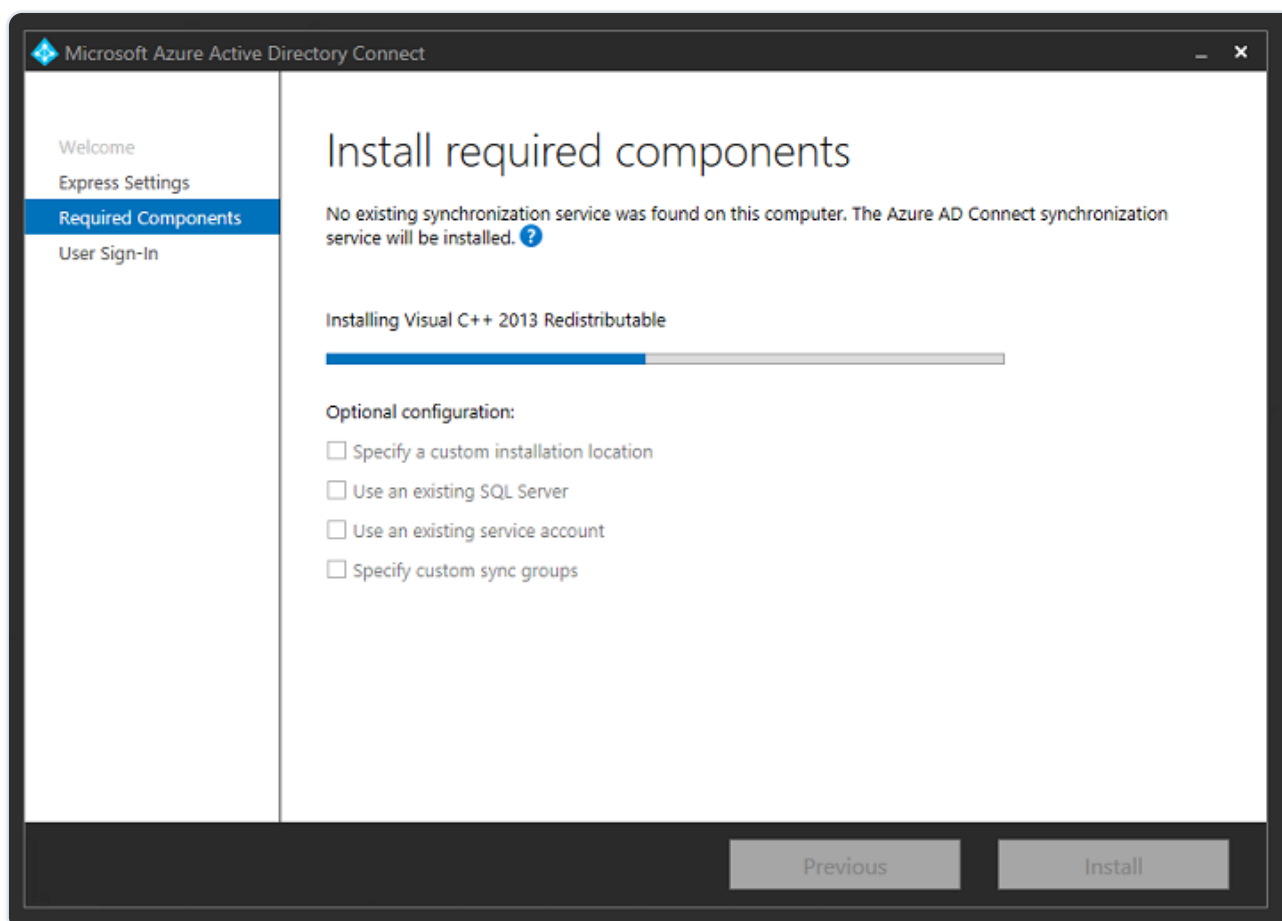
☒ I plan to configure this domain for single sign-on with my local Active Directory. ?

add

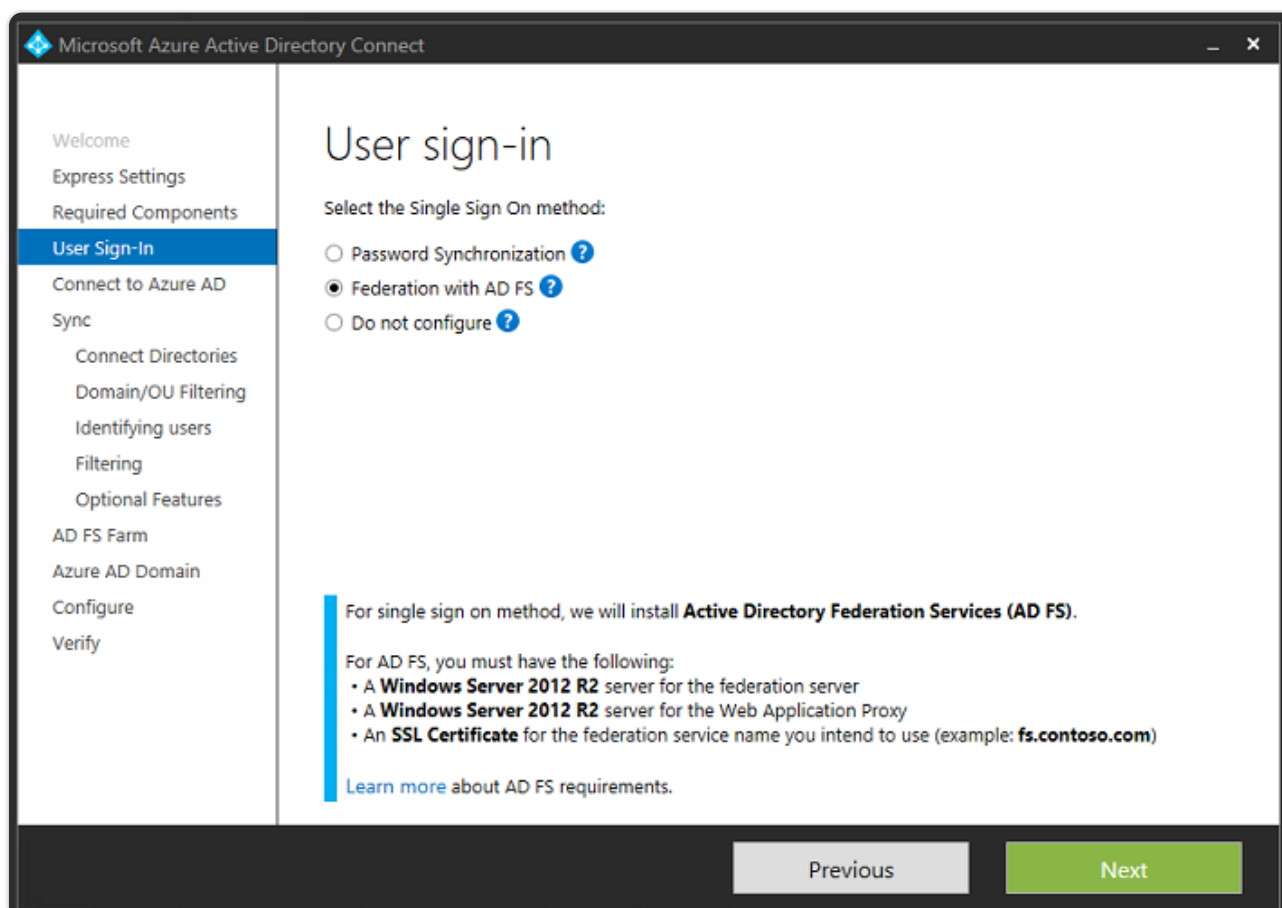
→ 2

Azure AD Connect をインストールする

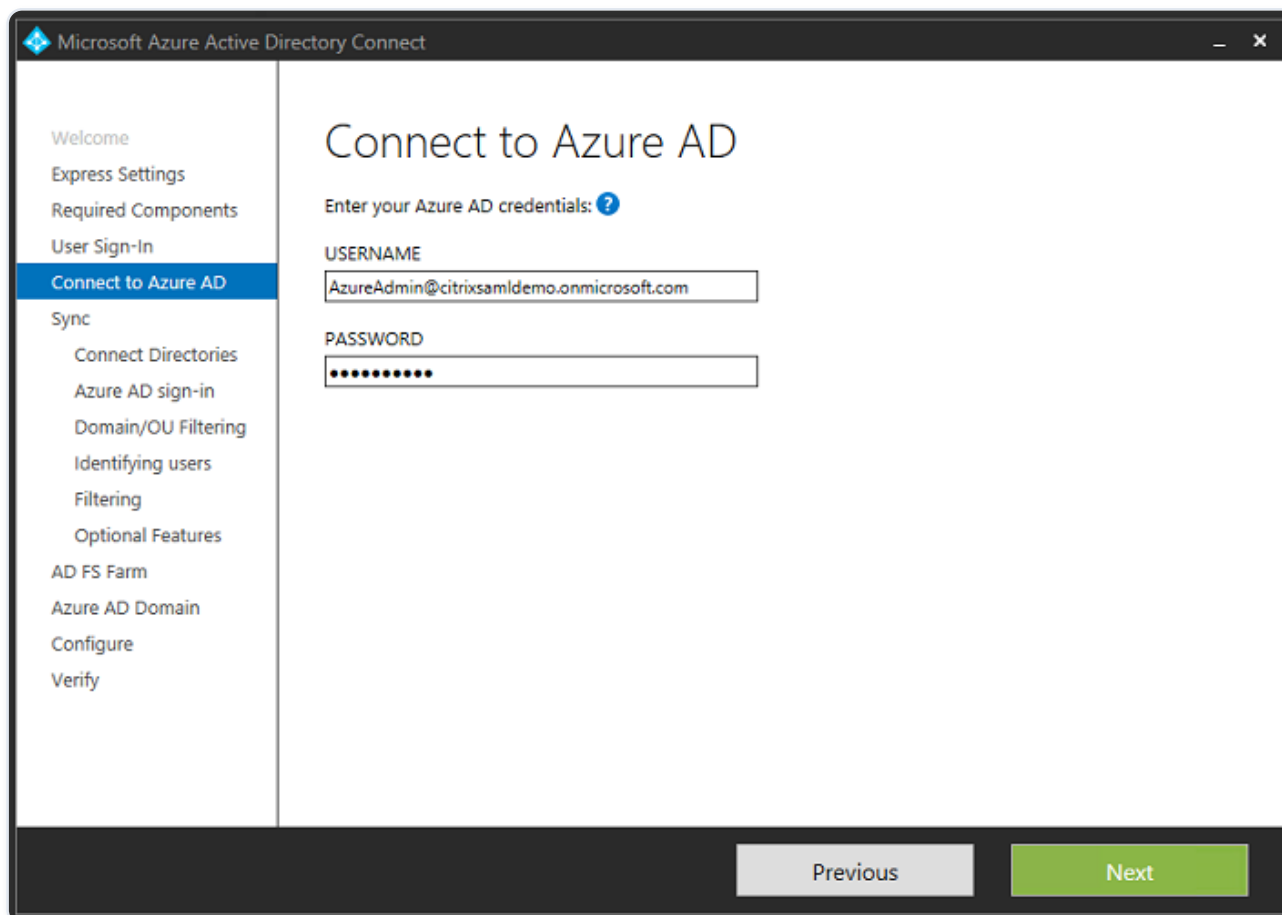
Azure AD 構成 GUI のステップ 2 は、Azure AD Connect の Microsoft ダウンロードページにリダイレクトされます。これを ADFS VM にインストールします。ADFS オプションが利用できるように、**簡易設定** ではなく **カスタムインストール** を使用してください。



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。



以前に作成した管理者アカウントでAzureに接続します。



The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. The title bar reads 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane with the following items: 'Welcome', 'Express Settings', 'Required Components', 'User Sign-In', 'Connect to Azure AD' (highlighted in blue), 'Sync', 'Connect Directories', 'Azure AD sign-in', 'Domain/OU Filtering', 'Identifying users', 'Filtering', 'Optional Features', 'AD FS Farm', 'Azure AD Domain', 'Configure', and 'Verify'. The main pane is titled 'Connect to Azure AD' and contains the text 'Enter your Azure AD credentials: ?'. Below this are two input fields: 'USERNAME' with the value 'AzureAdmin@citrixsaml demo.onmicrosoft.com' and 'PASSWORD' with masked characters. At the bottom right are 'Previous' and 'Next' buttons.

内部ADフォレストを選択します。

Microsoft Azure Active Directory Connect

Welcome

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

Connect Directories

Domain/OU Filtering

Identifying users

Filtering

Optional Features

AD FS Farm

Azure AD Domain

Configure

Verify

Connect your directories

Enter connection information for your on-premises directories or forests: ?

DIRECTORY TYPE

Active Directory

FOREST ?

citrixsaml demo.cloudapp.net

USERNAME

CITRIXSAMLdemo\Administrator

PASSWORD

.....

Add Directory

CONFIGURED DIRECTORIES

citrixsaml demo.cloudapp.net (Active Directory) ✓ Remove

Previous Next

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。

Microsoft Azure Active Directory Connect

Welcome

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

Connect Directories

Domain/OU Filtering

Identifying users

Filtering

Optional Features

AD FS Farm

Azure AD Domain

Configure

Verify

Domain and OU filtering

Directory: citrixsaml demo.cloudapp.net Refresh Ou/Domain ?

☐ Sync all domains and OUs

☒ Sync selected domains and OUs

- ☒ citrixsaml demo.cloudapp.net
 - ☒ Built-in
 - ☒ Computers
 - ☒ Domain Controllers
 - ☒ ForeignSecurityPrincipals
 - ☒ Infrastructure
 - ☐ LostAndFound
 - ☒ Managed Service Accounts
 - ☒ NTDS Quotas
 - ☒ Program Data
 - ☒ System
 - ☒ Users
 - ☒ Configuration

Previous Next

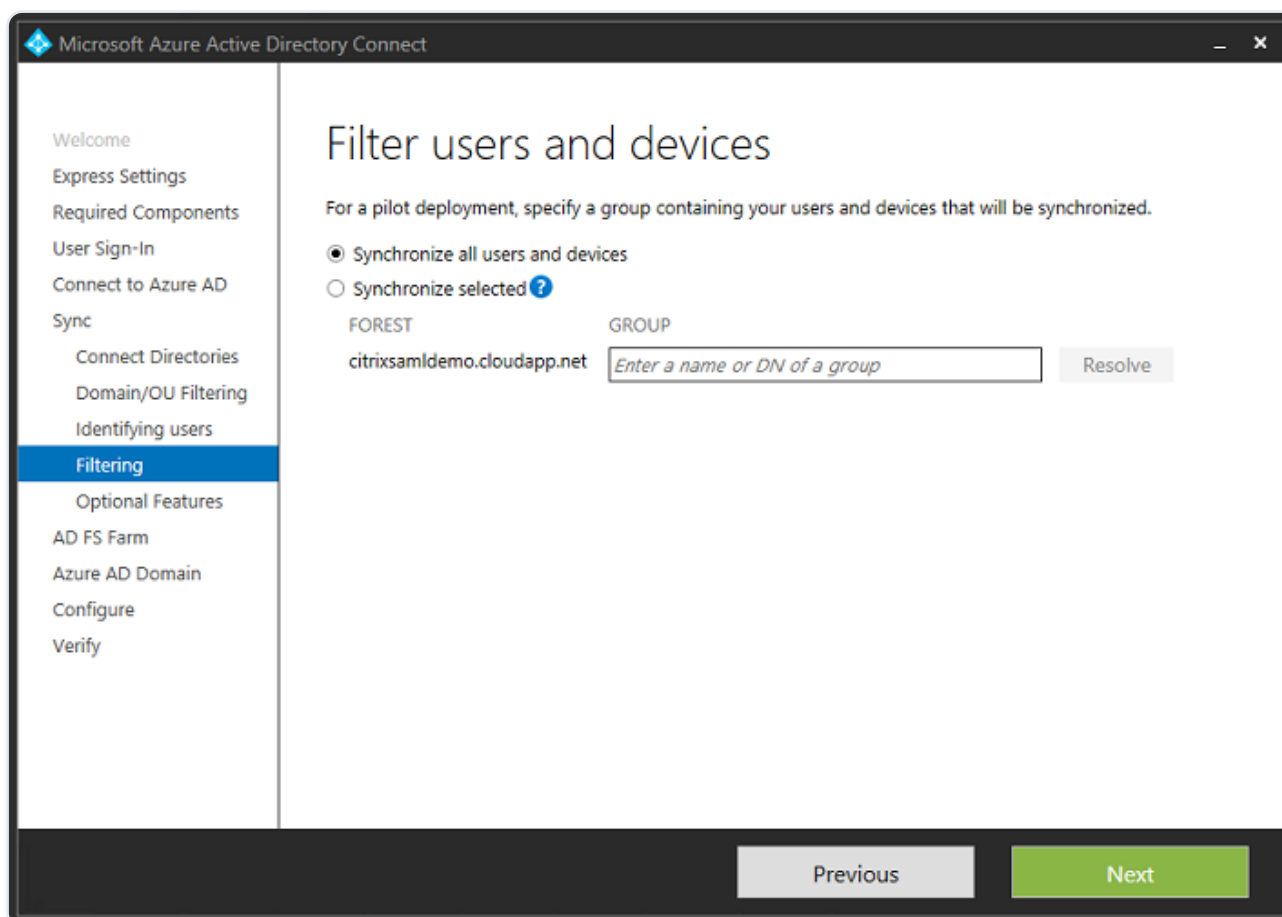
ディレクトリ構造が単純な場合は、ユーザー名が十分に一意であるため、ログオンするユーザーを識別できます。

The screenshot shows the 'Uniquely identifying your users' configuration window in Microsoft Azure Active Directory Connect. The left sidebar contains a navigation menu with the following items: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Domain/OU Filtering, Identifying users (highlighted), Filtering, Optional Features, AD FS Farm, Azure AD Domain, Configure, and Verify. The main content area is titled 'Uniquely identifying your users' and contains the following sections:

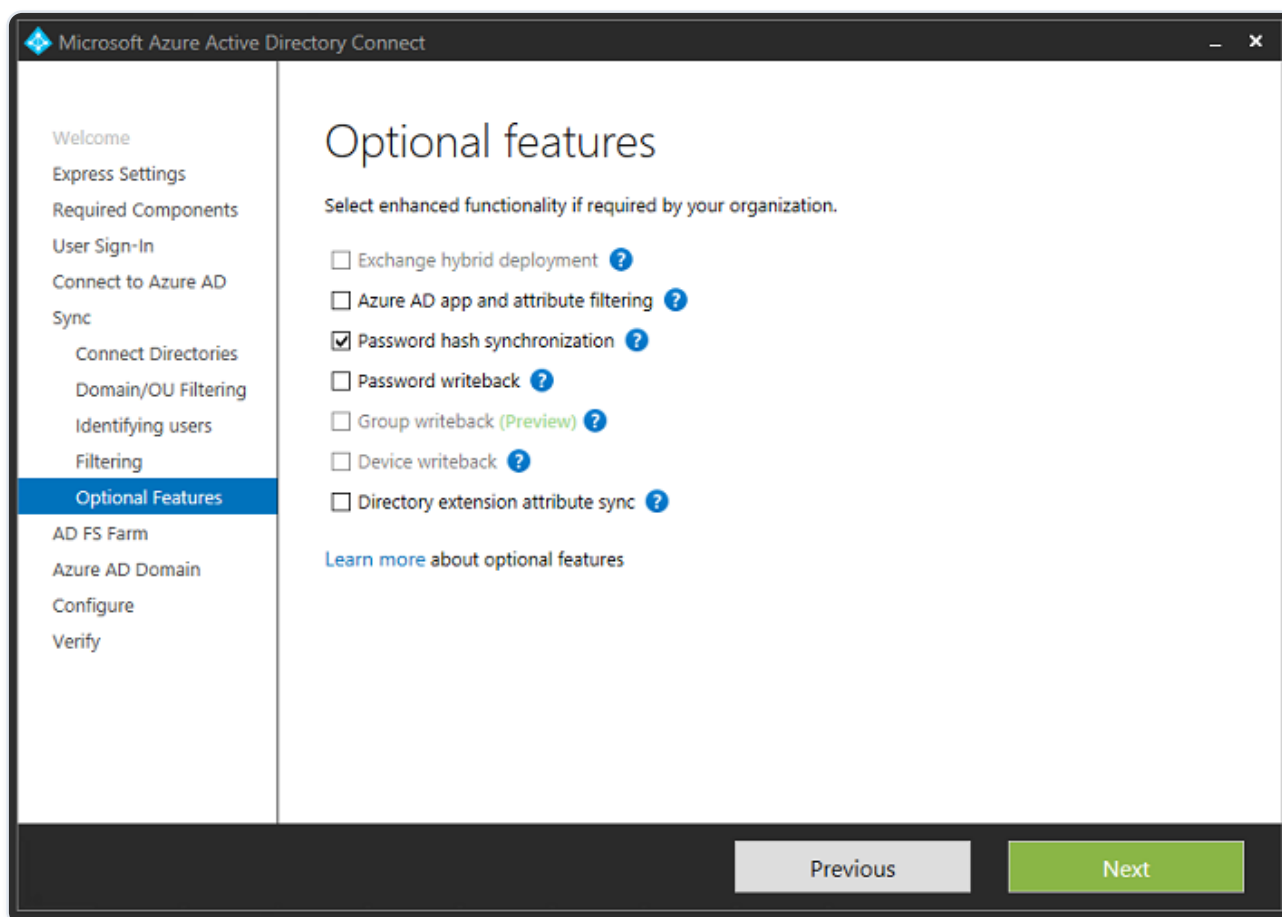
- Select how users should be identified in your on-premises directories. ?**
 - ☒ Users are represented only once across all directories.
 - ☐ User identities exist across multiple directories. Match using:
 - ☒ Mail attribute
 - ☐ ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
 - ☐ SAMAccountName and MailNickName attributes
 - ☐ A specific attribute
- CUSTOM ATTRIBUTE**
A dropdown menu is shown below this label.
- Select how users should be identified with Azure AD.**
- SOURCE ANCHOR ?**
A dropdown menu is shown with 'objectGUID' selected.
- USER PRINCIPAL NAME ?**
A dropdown menu is shown with 'userPrincipalName' selected.

At the bottom of the window, there are two buttons: 'Previous' (disabled) and 'Next' (active).

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。



必要に応じて、Azure ADのパスワードを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。



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。

Microsoft Azure Active Directory Connect

AD FS Farm

Configure a new Windows Server 2012 R2 AD FS farm

Use an existing Windows Server 2012 R2 AD FS farm

Specify the SSL certificate used to secure the communication between clients and AD FS.

☒ Provide a PFX Certificate File

☐ Use a Certificate installed on the Federation Machines

CERTIFICATE FILE ?

C:\Users\Fred.CITRIXSAMLDEMO\Desktop\adfs.pfx Browse

SUBJECT NAME

*.citrixsaml demo.net

SUBJECT NAME PREFIX

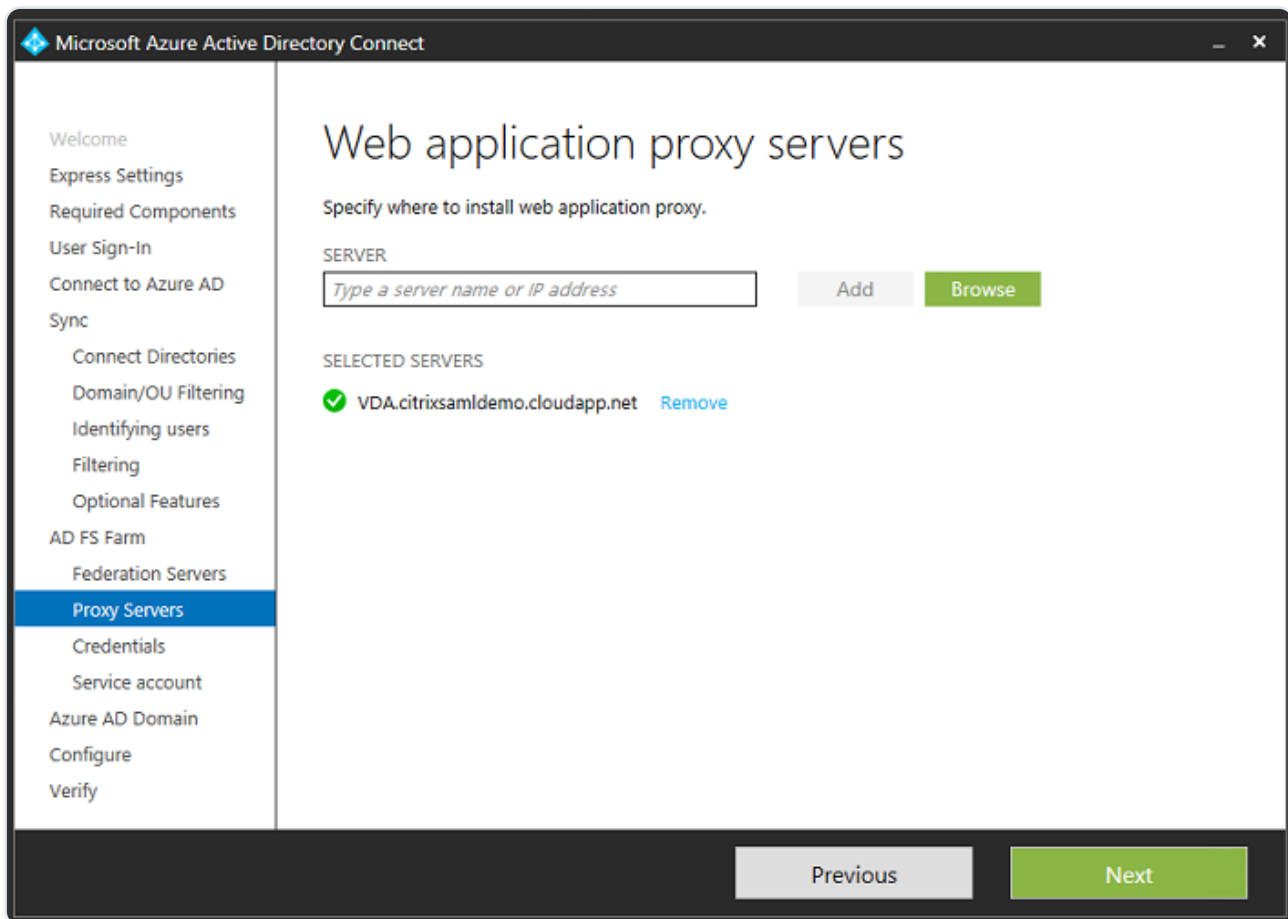
fs ✓

FEDERATION SERVICE NAME

https://fs.citrixsaml demo.net

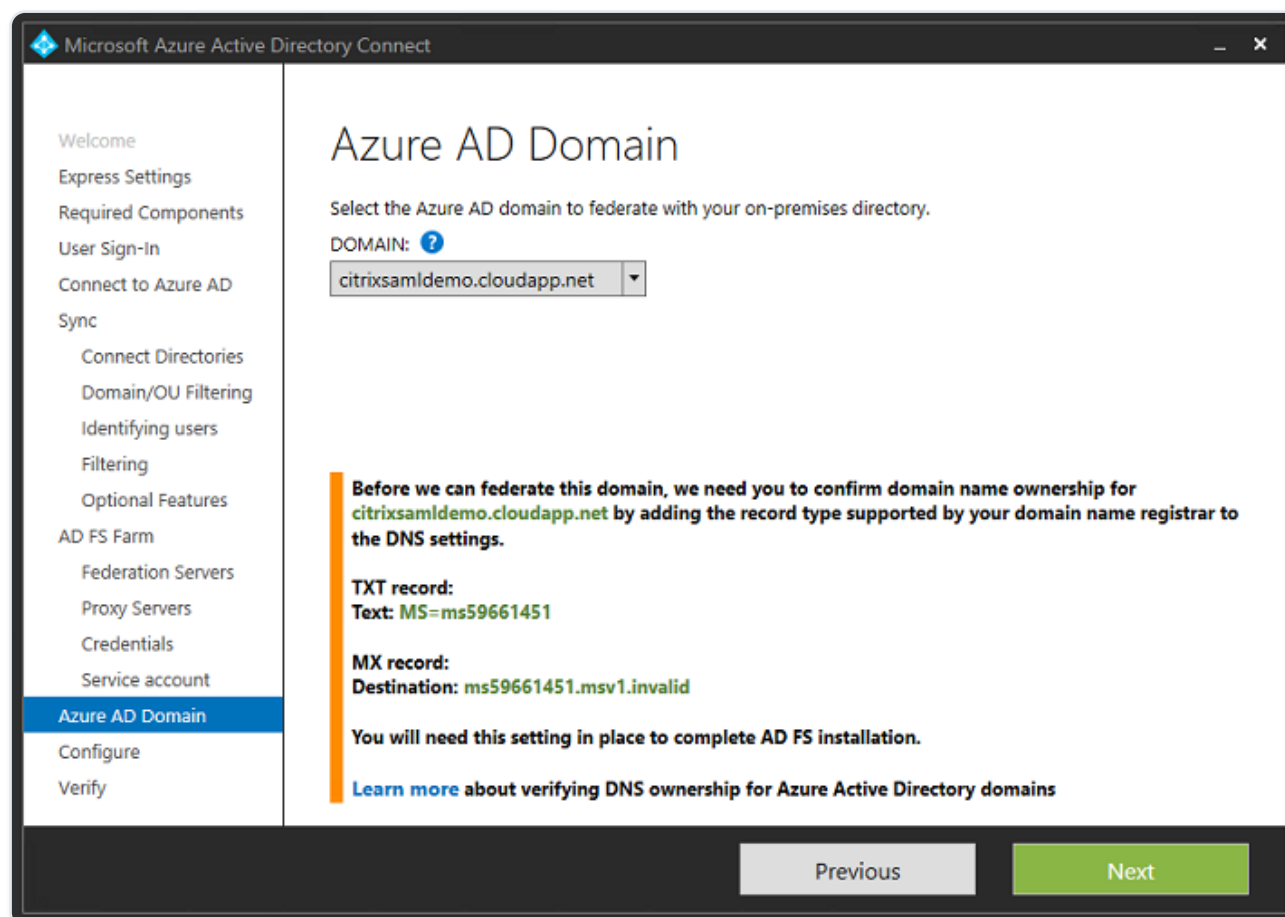
Previous Next

プロキシサーバーの選択を求められたら、wap.citrixsaml demo.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。



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

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

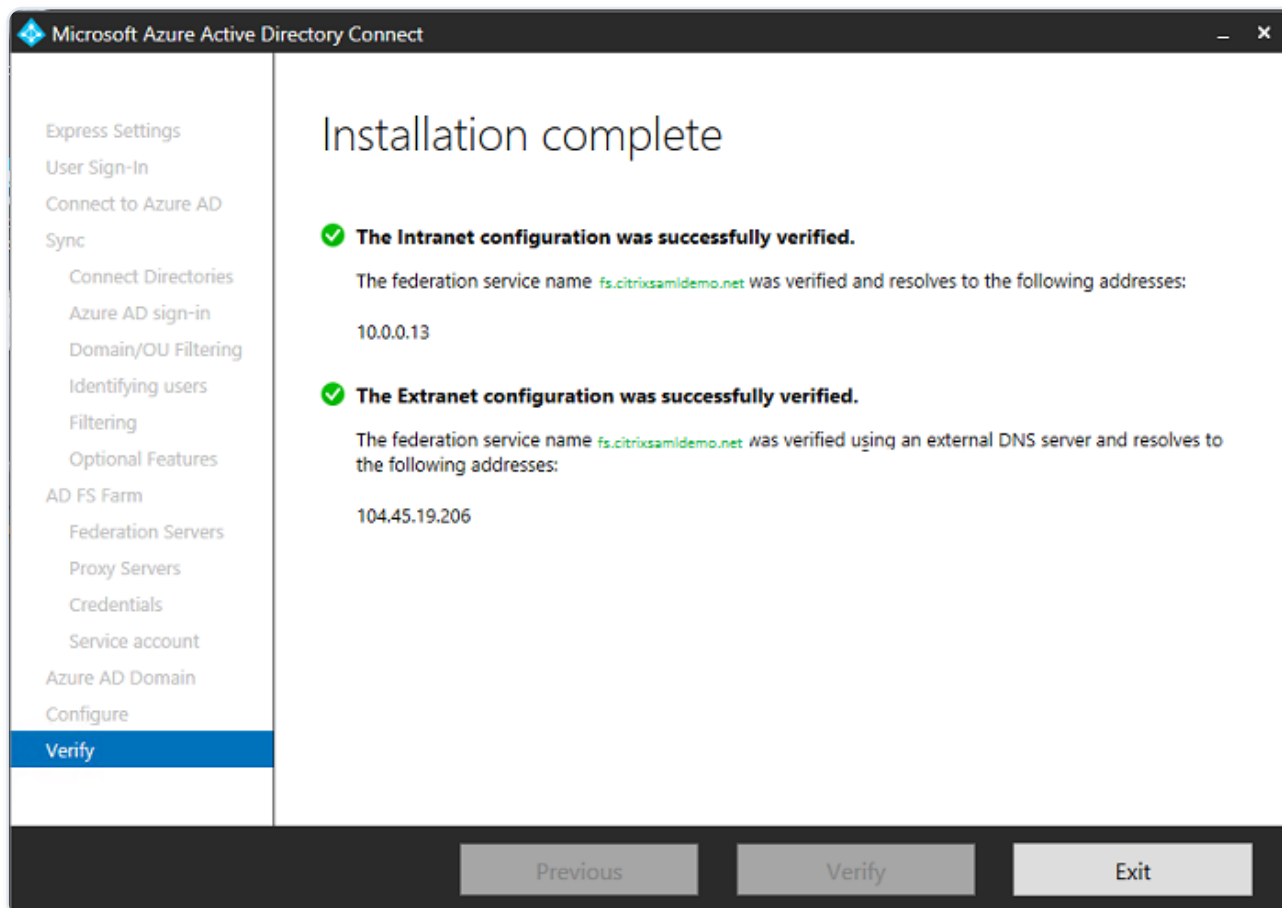
Azure 管理コンソールで をクリックします。

CitrixSamIDemo					
	USERS	GROUPS	APPLICATIONS	DOMAINS	DIRECTORY INTEGRATION CONFIGURE REPORTS LICENSES
DOMAIN NAME	TYPE	STATUS		SINGLE SIGN-ON	PRIMARY DOMAIN
citrixsamldemo.onmicrosoft.com	Basic	✓ Active		Not Available	Yes
citrixsamldemo.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サフィックスがADFSを指すCNAME DNSレコード（enterpriseregistration.<upnsuffix>）を構築するために使用されます。

この例では、これは fs.citrixsamldemo.net です。

enterpriseregistration.citrixsamdemo.net

Type
CNAME

* TTL
1 ✓

TTL unit
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。以前に生成し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](#)

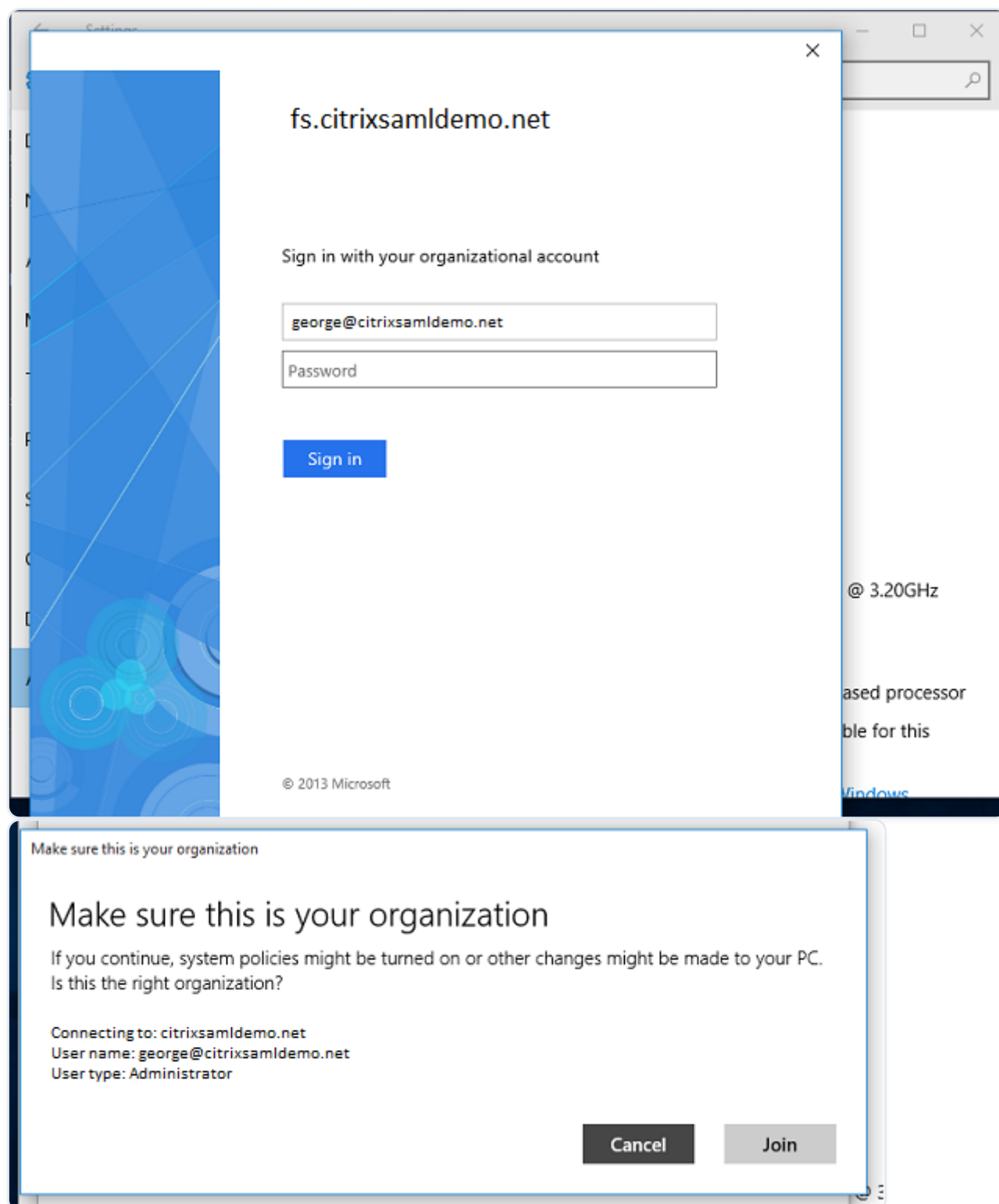
Which account should I use?

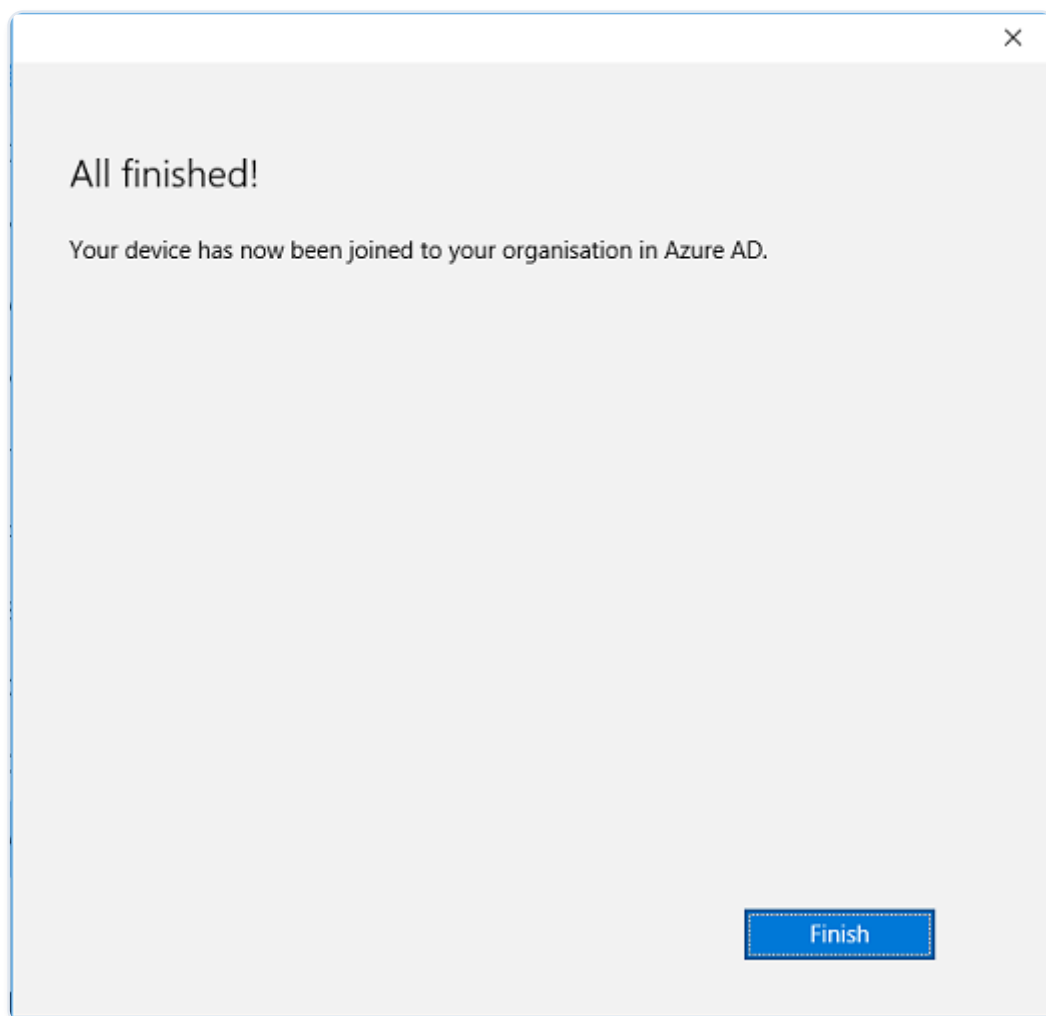
Sign in with the username and password you use with Office 365 (or other business services from Microsoft).

[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。



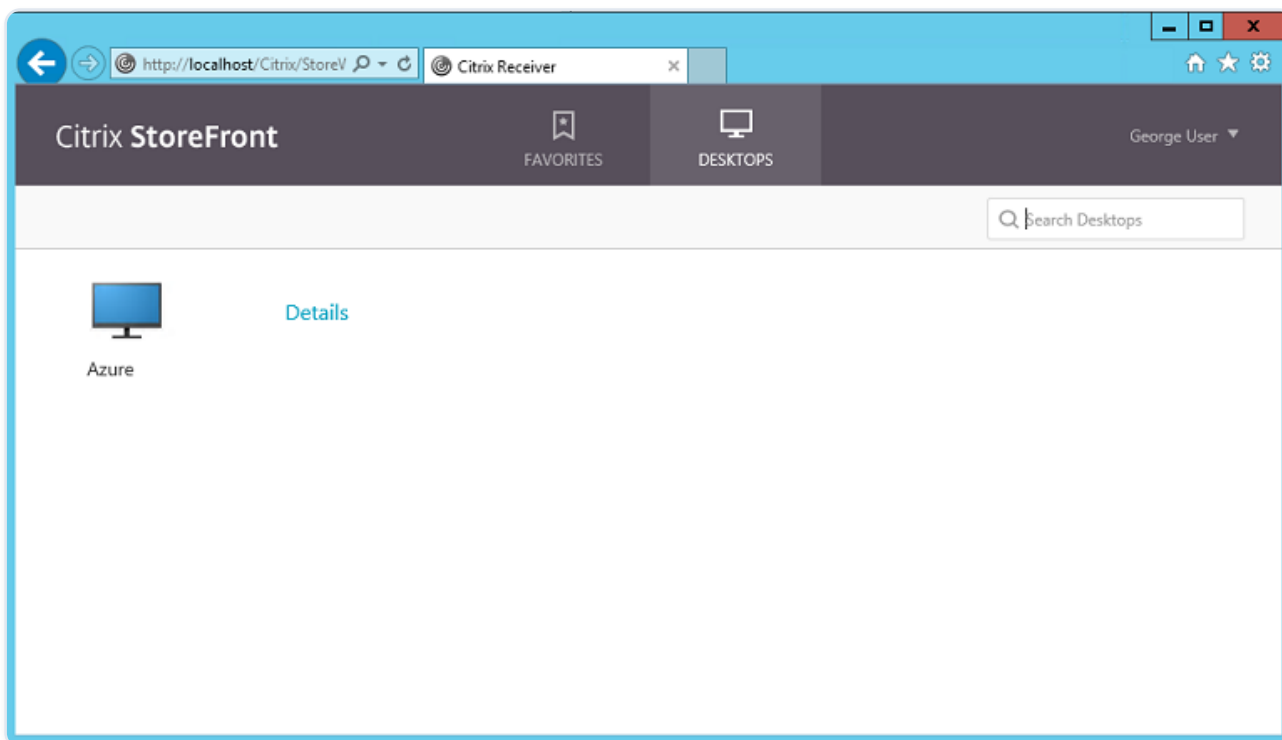


マシンを再起動し、ユーザーのメールアドレスを使用してログオンすることで、Azure AD参加が成功したことを確認します。ログオンしたら、Microsoft Edgeを起動して `<http://myapps.microsoft.com>` に接続します。ウェブサイトは自動的にシングルサインオンを使用するはずです。

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と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@citrixsamldemo.net がパスワードで認証できることを確認してください。



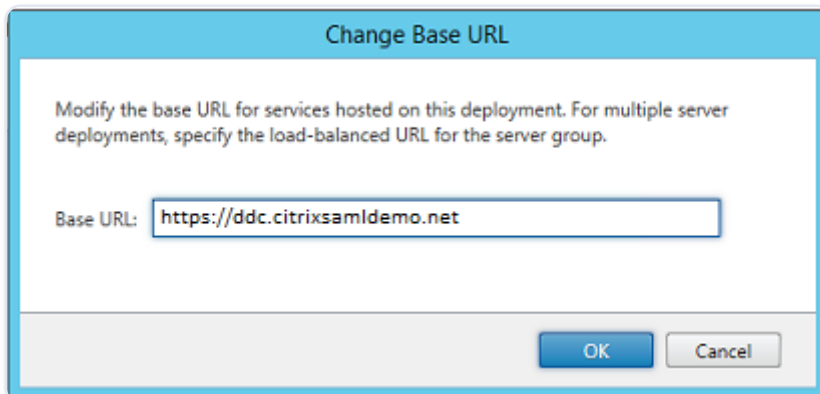
ユーザーの資格情報なしでStoreFront™が認証できるように、ControllerでPowerShellコマンドレット **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** を実行します。

フェデレーション認証サービスをインストールする

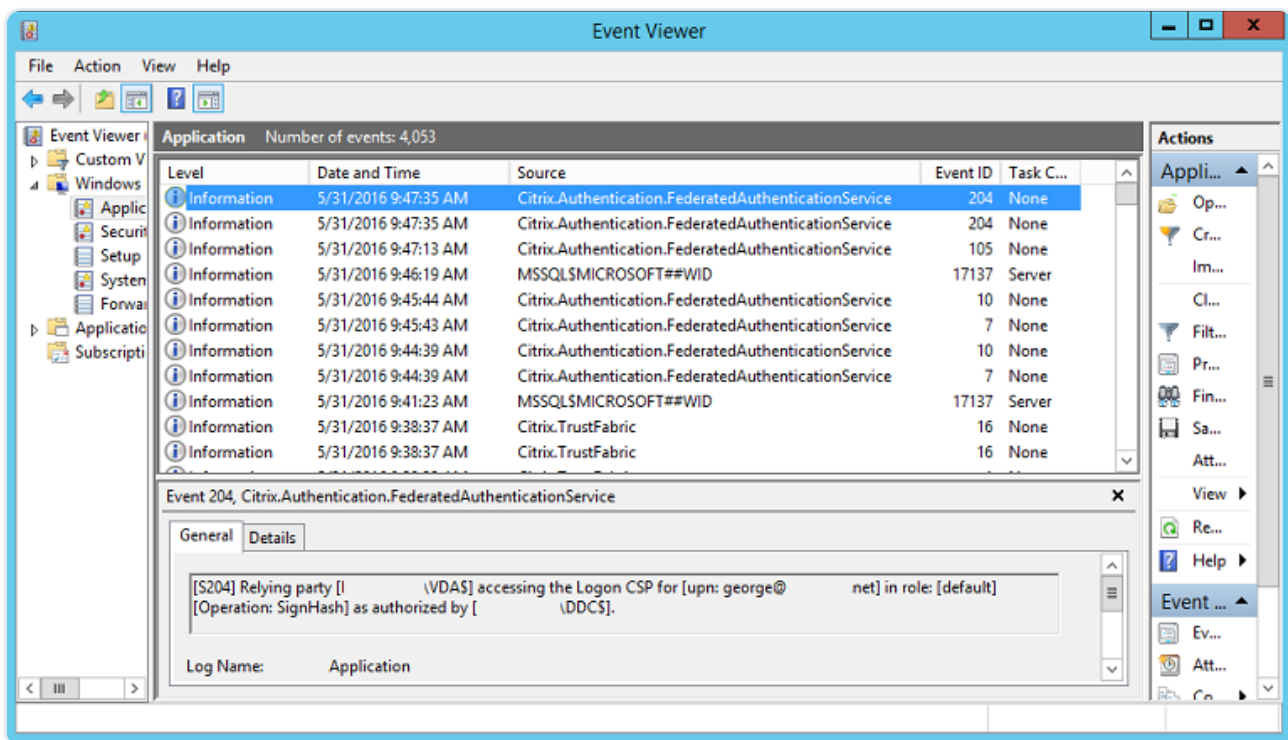
ADFSサーバーにFASをインストールし、Delivery Controllerが信頼されたStoreFrontとして機能するためのルールを設定します（この例では、StoreFrontはDelivery Controllerと同じVMにインストールされているため）。[インストールと構成](#)を参照してください。

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てIISとStoreFrontがHTTPSを使用するように構成し、StoreFrontのベースアドレスをhttps:に変更します。

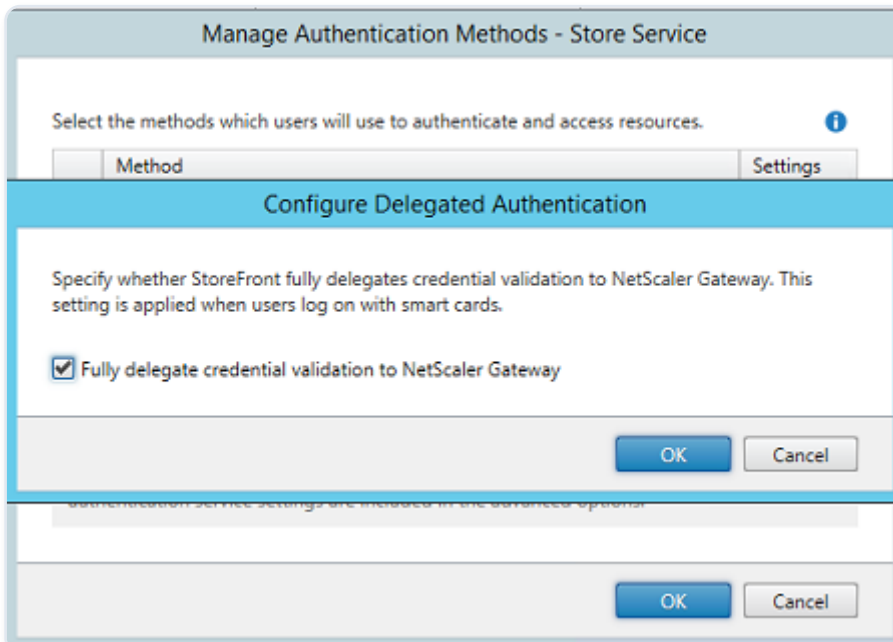


StoreFrontがFASサーバーを使用するように構成し（[インストールと構成](#)のPowerShellスクリプトを使用）、Azure内で内部的にテストして、FASサーバーのイベントビューアーを確認することでログオンがFASを使用していることを確認します。

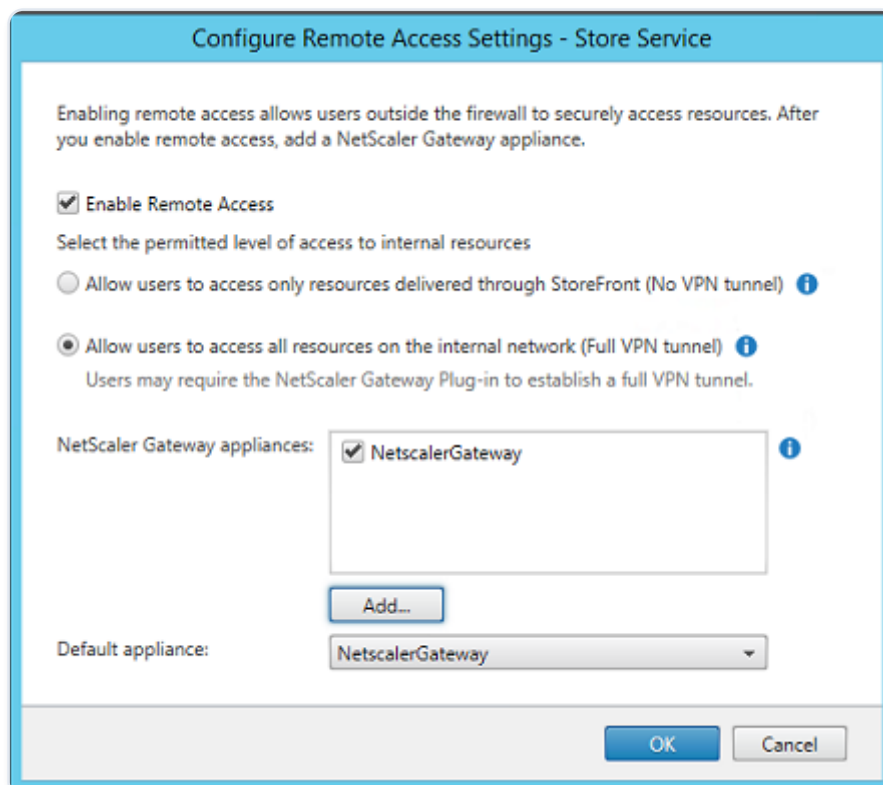


StoreFrontがCitrix Gatewayを使用するように構成する

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。

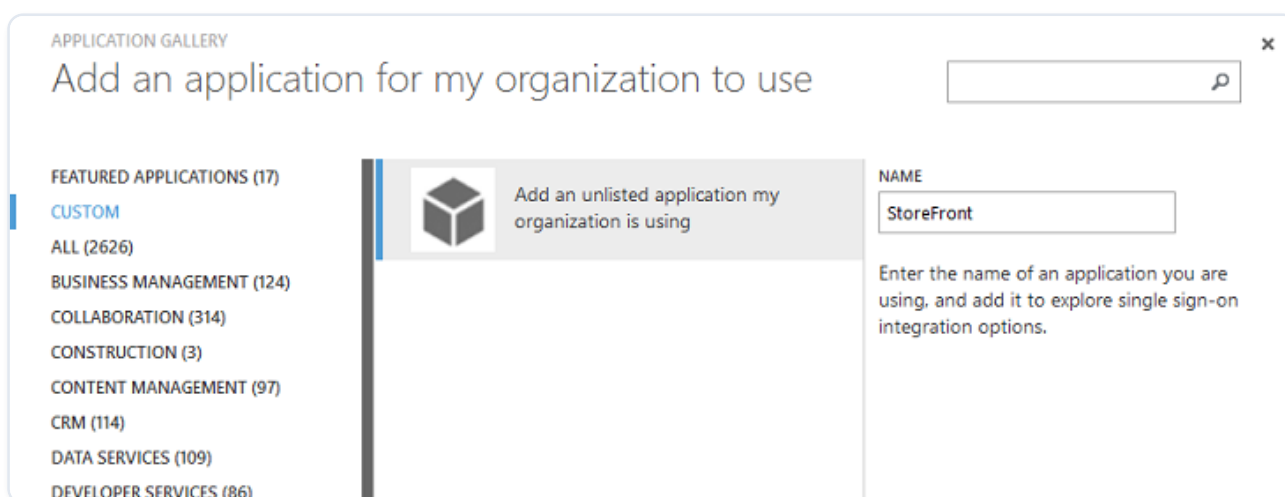


Citrix Gateway認証オプションを統合するには、Secure Ticket Authority (STA) を構成し、Citrix Gatewayアドレスを構成します。



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

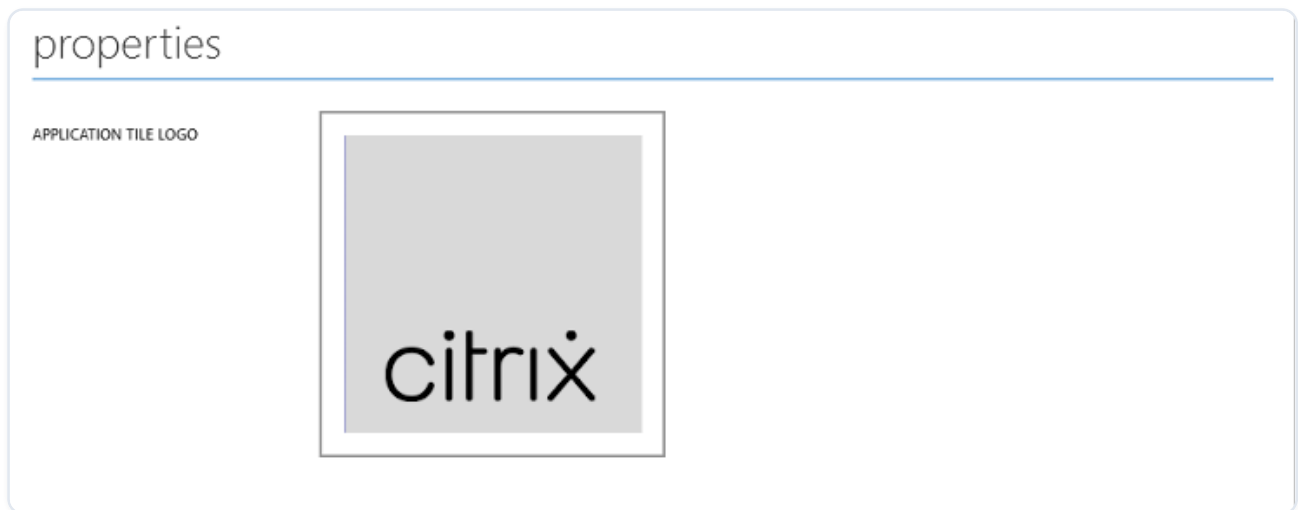
このセクションでは、現在Azure Active Directory Premiumサブスクリプションを必要とするAzure AD SAML 2.0シングルサインオン機能を使用します。Azure AD管理ツールで、**新しいアプリケーション**を選択し、**ギャラリーからアプリケーションを追加**を選択します。



「**CUSTOM > 組織が使用している未登録の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。

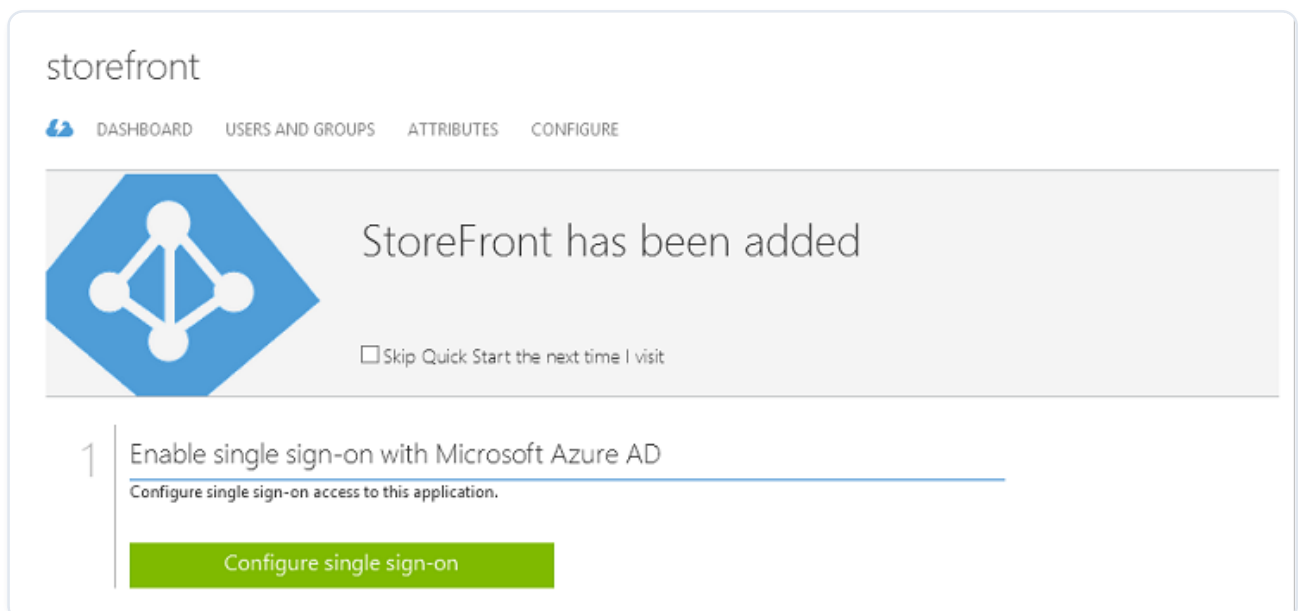
アイコンの構成

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



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。

CONFIGURE SINGLE SIGN-ON

How would you like users to sign on to StoreFront?

- ☒ **Microsoft Azure AD Single Sign-On**
Establish federation between Microsoft Azure AD and StoreFront
[Learn more](#)
- ☐ **Password Single Sign-On**
Microsoft Azure AD stores account credentials for users to sign on to StoreFront
[Learn more](#)
- ☐ **Existing Single Sign-On**
Configures Microsoft Azure AD to support single sign-on to StoreFront using Active Directory Federation Services or another third-party single sign-on provider.
[Learn more](#)

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 ?
 ✓

REPLY URL ?
 ✓

☐ 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.

1. 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 \(XML\)](#) 

2. Configure the certificate and values in AzureStoreFront

ISSUER URL

SINGLE SIGN-ON SERVICE URL

SINGLE SIGN-OUT SERVICE URL

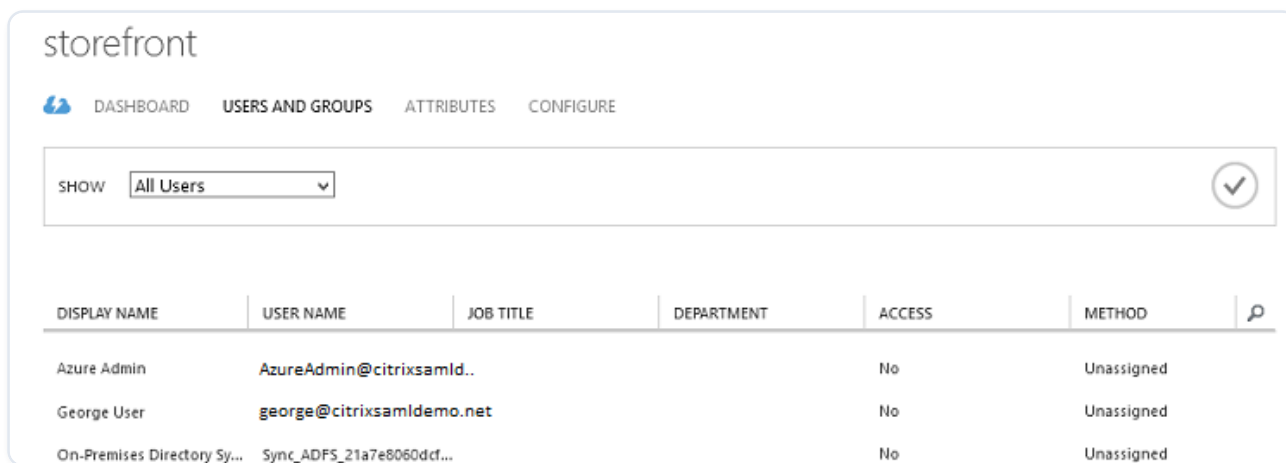
☐ Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate to start working for this application.



Base64信頼済み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

最後のステップは、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。

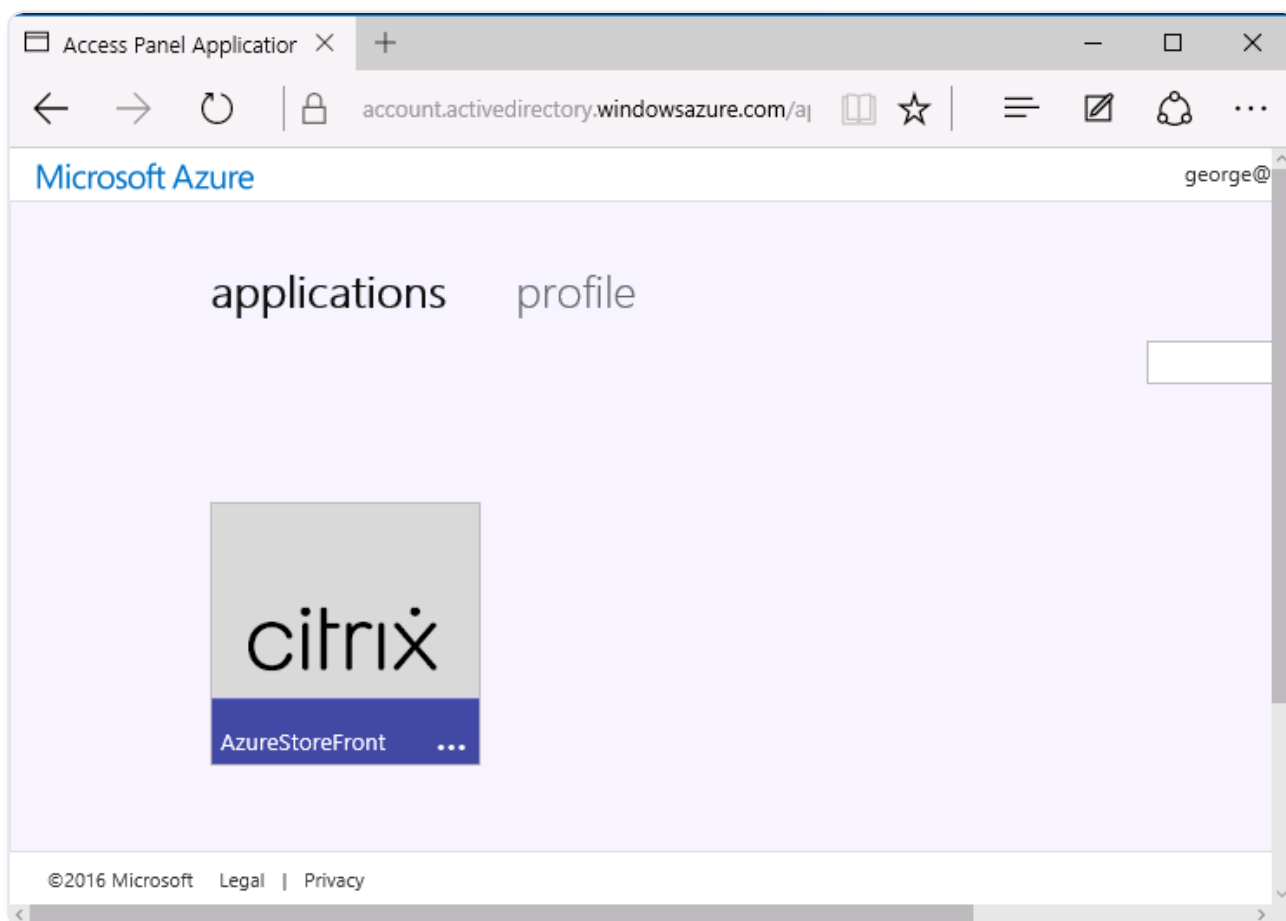


The screenshot shows the 'storefront' interface with tabs for DASHBOARD, USERS AND GROUPS, ATTRIBUTES, and CONFIGURE. Under 'USERS AND GROUPS', there is a 'SHOW' button and a dropdown menu set to 'All Users'. Below this is a table listing users.

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

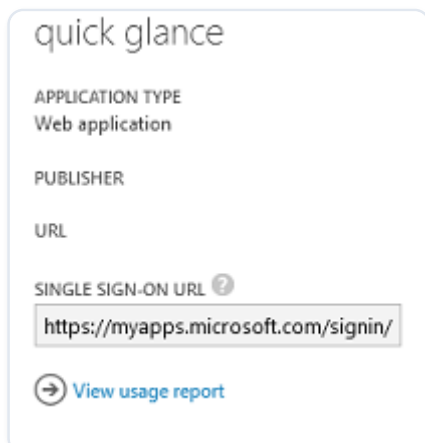
アプリケーションが構成されると、ユーザーが <https://myapps.microsoft.com> にアクセスしたときに、Azureアプリケーションのリストに表示されます。



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ダッシュボードで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ブラウザリンクを提供したり、ユーザーを直接StoreFrontに誘導するスタートメニュー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の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（現在のCitrix Gateway）を実行する別のVMを使用します。これはAzureストアから購入できます。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。

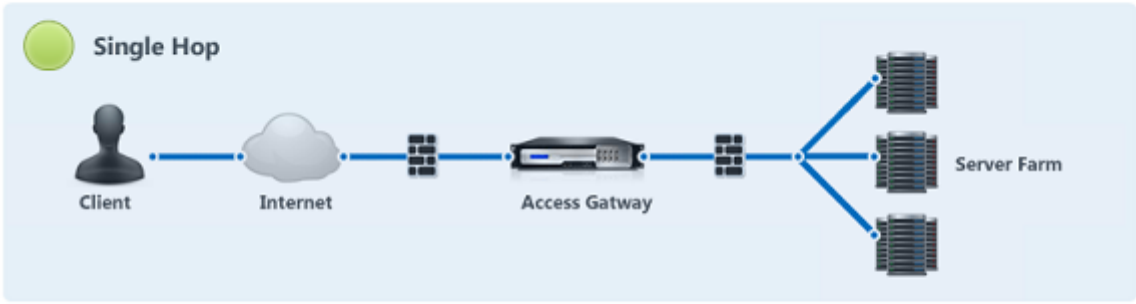
Citrix Virtual Apps and Desktopsセットアップウィザードを実行する

この例では、SAMLなしでシンプルな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。

XenApp/XenDesktop Setup Wizard

What is your deployment

Single Hop



The diagram illustrates a 'Single Hop' deployment architecture. It starts with a 'Client' (represented by a person icon) connected to the 'Internet' (cloud icon). The Internet connects to an 'Access Gateway' (server rack icon). The Access Gateway then connects to a 'Server Farm' (multiple server rack icons).

What is your Citrix Integration Point?

StoreFront

Continue Cancel

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。

NetScaler Gateway Settings

NetScaler Gateway IP Address*

10 . 0 . 0 . 18

Port*

4433

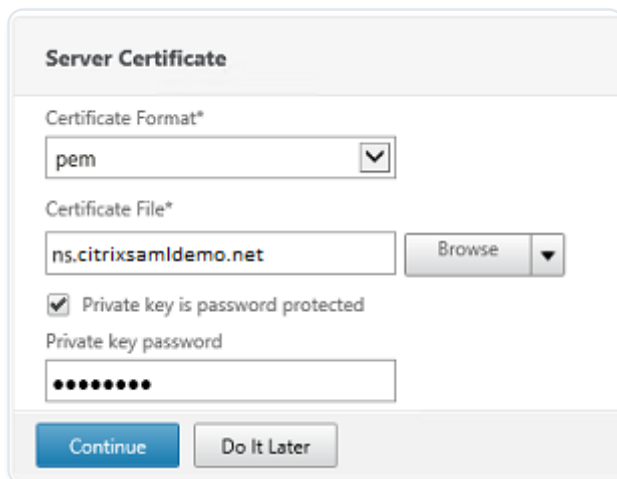
Virtual Server Name*

ns.citrixsaml demo.net

☐ Redirect requests from port 80 to secure port

Continue Cancel

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。



Server Certificate

Certificate Format*
pem

Certificate File*
ns.citrixsamldemo.net Browse

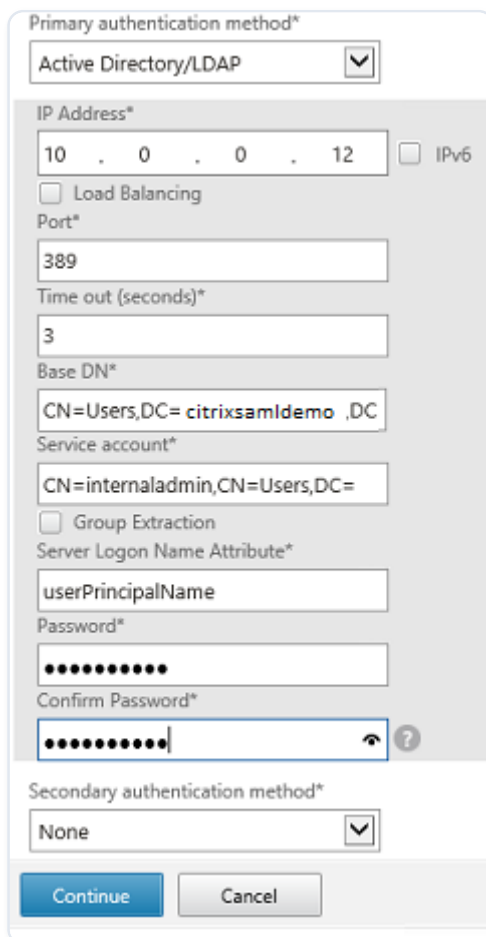
☒ Private key is password protected

Private key password
.....

Continue Do It Later

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。



Primary authentication method*
Active Directory/LDAP

IP Address*
10 . 0 . 0 . 12 ☐ IPv6

☐ Load Balancing

Port*
389

Time out (seconds)*
3

Base DN*
CN=Users,DC= citrixsamldemo ,DC=

Service account*
CN=internaladmin,CN=Users,DC=

☐ Group Extraction

Server Logon Name Attribute*
userPrincipalName

Password*
.....

Confirm Password*
..... ?

Secondary authentication method*
None

Continue Cancel

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。

StoreFront

StoreFront FQDN*

ddc.citrixsamldemo.net

Site Path*

/Citrix/StoreWeb

Single Sign-on Domain*

citrixsamldemo

Store Name*

/Citrix/StoreWeb

Secure Ticket Authority Server*

http://ddc.citrixsamldemo.net/sta

StoreFront Server*

10 . 0 . 0 . 15

Protocol*

SSL

Port*

443

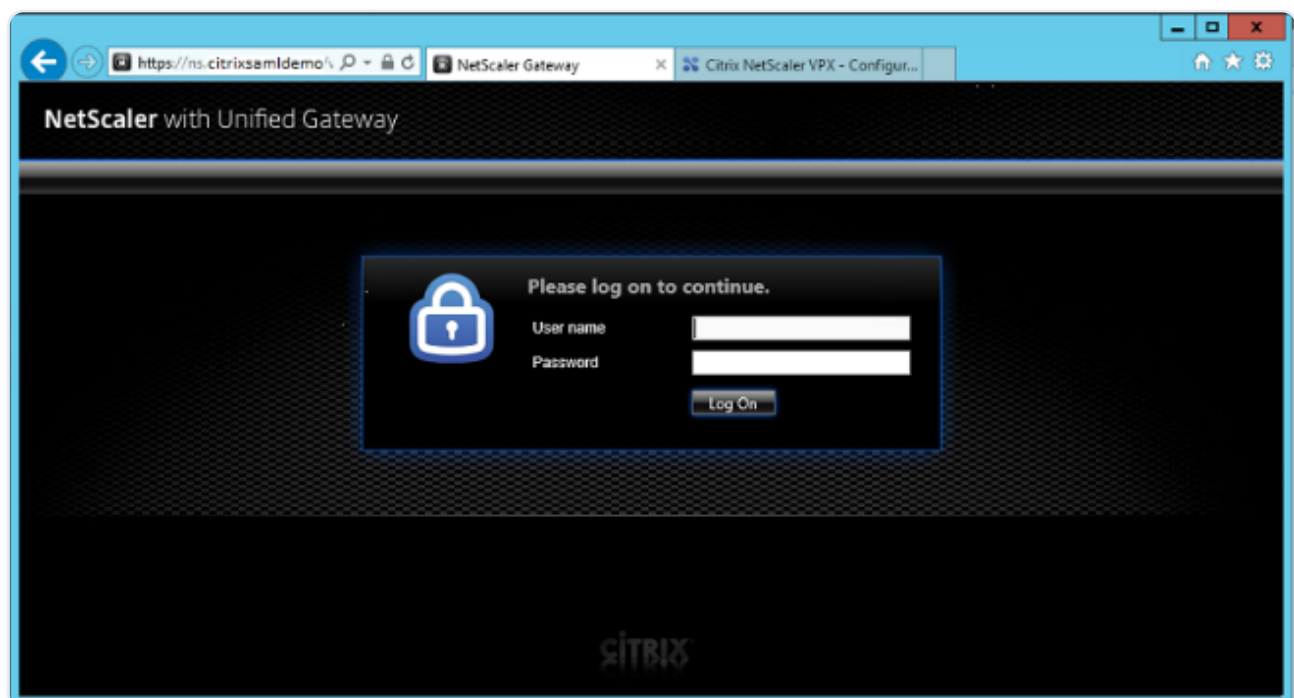
☐ Load Balancing

Continue

Cancel

Citrix Gatewayの展開を検証する

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を使用する方法は、他のWebサイトでSAMLを使用する方法と似ています。新しいSAMLポリシーを、**NS_TRUE**の式で追加します。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-azure-enable-ns-saml-policy.png)

以前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。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-azure-enable-ns-saml-idp-server.png)

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参加済み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。

ローカライズされた画像(/en-us/federated-authentication-service/2411/media/fas-azure-verify-end-to-end.png)

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、その後戻ってくることを確認します。

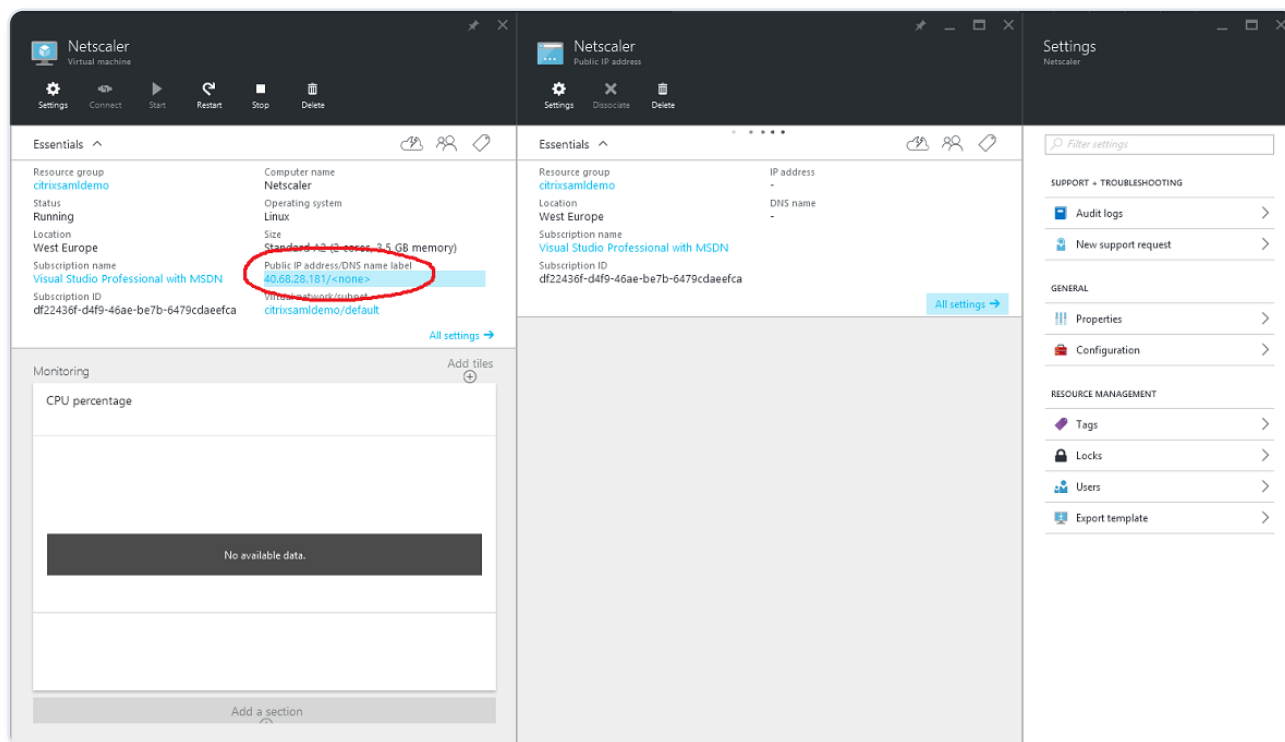
最後に、Azure ADに参加していないマシンも同じURLで機能することを確認します（ただし、最初の接続ではAzure ADへの明示的なシングルサインオンが発生します）。

付録

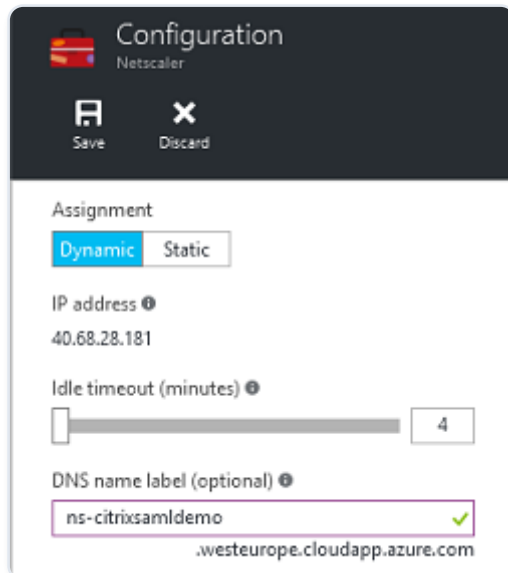
AzureでVMをセットアップする際には、以下の標準オプションを構成する必要があります。

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（この例では10.*.*) 上のIPアドレスを付与します。デフォルトでは、パブリックIPアドレスも提供され、これは動的に更新される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ゾーンファイルでのCNAME参照に使用でき、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。

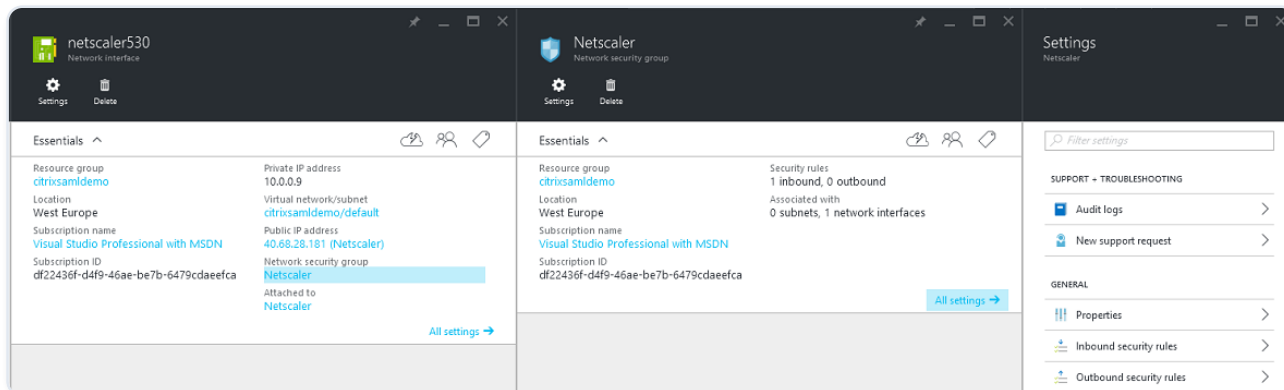


ファイアウォールルール（セキュリティグループ）を設定する

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ファイアウォールルールのセット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の展開は、[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。

フェデレーション認証サービス2411ドキュメント履歴

次の表に、フェデレーション認証サービス2411のドキュメントに対する重要な変更点を示します。これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

日付	変更	説明
18 Dec 2024	Windowsログオンの問題のトラブルシューティングの記事を更新	詳しくは、「 Windowsログオンの問題のトラブルシューティング 」を参照してください。
11 Dec 2024	StoreFrontストアでFASプラグインの有効化の記事を更新	詳しくは、「 StoreFrontストアでFASプラグインの有効化 」を参照してください。
03 Dec 2024	Citrixフェデレーション認証サービス2411の初期リリース	詳しくは、「 新機能 」を参照してください。