



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 2206	9
フェデレーション認証サービス 2206	10
修正された問題	10
既知の問題	10
サードパーティ通知	11
システム要件	12
インストールと構成	13
インストールとセットアップの順序	13
フェデレーション認証サービスをインストールする	13
FASのアップグレード	14
StoreFrontストアでFASプラグインを有効にする	14
Delivery Controller™を構成する	15
グループポリシーを構成する	15
セッション中の動作	19
プロンプトスコープ	20
同意のタイムアウト	21
ロック時の切断	21
Federated Authentication Service管理コンソールの使用	21
証明書テンプレートを展開する	22
Active Directory証明書サービスをセットアップする	24
フェデレーション認証サービスを承認する	24
ルールの構成	26
Citrix Cloudへの接続	30
Citrix Cloudから切断する	35
高度な構成	36
関連情報	36

証明機関の構成	36
FAS で使用する複数の CA サーバーをセットアップする	36
予期される動作の変更	37
TCP アクセス用に Microsoft 証明機関を構成する	38
ユーザー証明書を事前生成する	39
Active Directoryユーザーのリストを取得する	39
FASサーバー	40
登録機関証明書を更新する	42
関連情報	43
秘密鍵の保護	43
はじめに	43
秘密鍵の構成設定	44
構成シナリオの例	47
例1	47
例 2	47
例3	56
FAS証明書ストレージ	59
関連情報	61
セキュリティとネットワーク構成	61
ネットワークアーキテクチャ	61
ファイアウォールとネットワークセキュリティ	62
Citrix フェデレーテッド認証サービスとCitrix Cloud™間の接続	63
セキュリティに関する考慮事項	63
委任された登録エージェント	63
アクセス制御リストの構成	64
ファイアウォール設定	64
イベントログの監視	64
ハードウェアセキュリティモジュール	64

管理者の責任	65
グループポリシー設定	65
証明書テンプレート	66
証明書テンプレートの名前を変更する	66
全般プロパティの変更	66
要求処理プロパティの変更	67
暗号化プロパティの変更	67
キー構成証明プロパティの変更	67
置き換えられたテンプレートのプロパティを変更する	67
拡張機能のプロパティを変更する	67
セキュリティのプロパティを変更する	67
サブジェクト名のプロパティを変更する	68
サーバーのプロパティを変更する	68
発行要件プロパティの変更	68
互換性プロパティの変更	69
証明機関の管理	69
テンプレートの公開	69
ファイアウォール設定	70
登録の制限	70
ポリシーモジュールと監査	70
FAS管理	70
ACLによるStoreFront、ユーザー、およびVDAの制限	71
ルールの構成	71
証明機関とテンプレートを構成する	71
セッション内証明書と認証証明書	72
秘密鍵の保護と鍵長	72
イベントログ	72
管理アクセスと管理ツール	72

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	72
一般的なWindowsサーバーのセキュリティ	72
関連情報	73
パフォーマンスカウンター	73
Windows ログオンの問題のトラブルシューティング	75
証明書と公開鍵基盤	75
UPN名と証明書のマッピング	76
アクティブディレクトリにおけるUPN名	76
証明書マッピングサービス	77
ログオンドメインコントローラーの選択を制御する	77
ドメインコントローラーの選択を制御する	77
使用中のドメインコントローラーを特定する	78
アカウント監査イベントを有効にする	78
証明書の検証ログ	78
証明書の有効性を確認する	78
CAPIログを有効にする	79
CAPI ログ	79
エラーメッセージ	79
Kerberosログ	80
ドメインコントローラーおよびワークステーションログ	81
ドメインコントローラー CAPI2 ログ	81
ドメインコントローラーのセキュリティログ	82
VDA セキュリティログ	83
VDA CAPI ログ	84
VDAシステムログ	85
Windowsイベントログを使用したFASの監視	85
FASサービスは実行中ですか?	86

FAS健全性イベント	86
クラウド接続FASイベント	87
セキュリティイベント	88
FASイベントログ	89
管理イベント	89
IDアサーションの作成	92
証明書利用者として機能する	93
セッション内証明書サーバー	93
FASアサーションプラグイン	94
Workspace 対応 FAS	95
ログオン	96
セッション内証明書	97
証明書要求とキーペア生成	97
エンドユーザーのエラーメッセージ	98
関連情報	99
PowerShell コマンドレット	99
展開アーキテクチャ	100
はじめに	100
アーキテクチャの概要	100
内部展開	101
シトリックス ゲートウェイ展開	104
ADFS SAML 展開	105
B2Bアカウントマッピング	105
ウィンドウズ 10 アジュール AD 参加	106
ADFSの展開	108
はじめに	108
SAMLの概要	110
リダイレクトURL	110

識別子	110
戻りアドレス	110
署名証明書	110
シングルサインアウトURL	111
構成	111
SAMLポリシーの入力	111
関連情報	112
Azure AD 統合	112
はじめに	112
アーキテクチャ	114
DNSゾーンの作成	115
クラウドサービスの作成	116
Windows仮想マシンの作成	116
ドメインコントローラー	117
ADFSコントローラーとWeb Application Proxyサーバー	117
Citrix Virtual Desktops™ デリバリーコントローラーおよびVDA	118
内部DNSの構成	118
外部DNSアドレスを構成する	119
セキュリティグループを構成する	120
ADFS証明書を作成する	120
Azure AD のセットアップ	121
新しいディレクトリを作成する	121
グローバル管理者ユーザー (AzureAdmin) を作成する	123
ドメインを Azure AD に登録する	124
Azure AD Connect をインストールする	125
Azure AD Join を有効にする	133
Citrix Virtual AppsまたはCitrix Virtual Desktopsをインストールする	134
フェデレーション認証サービスをインストールする	134

StoreFrontを構成する	134
StoreFrontでCitrix Gatewayを使用するように構成する	135
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	136
アイコンの構成	137
SAML認証の構成	137
アプリケーションをユーザーに割り当てる	138
MyAppsページ	138
シングルサインオンURL	139
Citrix Gatewayのインストールと構成	140
Citrix Virtual Apps and Desktopsセットアップウィザードの実行	140
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	141
StoreFrontアドレスを構成する	142
Citrix Gatewayの展開を確認する	143
Citrix Gateway SAML 認証サポートを有効にする	144
エンドツーエンドシステムを確認する	145
付録	146
パブリック IP アドレスと DNS アドレスを提供する	146
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	147
関連情報	147
Federated Authentication Service 2206 ドキュメント履歴	148

フェデレーション認証サービス 2206

このFederated Authentication Service (FAS) リリースには、次の新機能が含まれています。

- **FASサーバーの登録。** Federated Authentication Service (FAS) サーバーのCitrix Cloud™登録フローを更新し、一貫したユーザーエクスペリエンスを提供し、FASサーバーのセキュリティ体制を向上させました。

FASの新しい登録サービスにより、サーバーで新しいブラウザを開く必要がなくなります。この登録サービスは、他のCitrixオンプレミス製品との一貫したオンプレミスユーザーエクスペリエンスを提供し、FASサーバーのセキュリティ体制を向上させ、FASサーバーでの管理者構成を削減します。詳細については、「[Citrix Cloudへの接続](#)」を参照してください。

- **イベントログの改善。** 新しいFASイベントログを追加しました。これらのイベントログの詳細については、「[FASイベントログ](#)」を参照してください。

バグ修正に関する情報については、「[修正された問題](#)」を参照してください。

フェデレーション認証サービス 2206

このFederated Authentication Service (FAS)リリースには、次の新機能が含まれています。

- **FASサーバーの登録。** Federated Authentication Service (FAS)サーバーのCitrix Cloud™登録フローを更新し、一貫したユーザーエクスペリエンスを提供し、FASサーバーのセキュリティ体制を向上させました。

FASの新しい登録サービスにより、サーバーで新しいブラウザを開く必要がなくなります。この登録サービスは、他のCitrixオンプレミス製品との一貫したオンプレミスユーザーエクスペリエンスを提供し、FASサーバーのセキュリティ体制を向上させ、FASサーバーでの管理者構成を削減します。詳しくは、「Citrix Cloudへの接続」(</ja-jp/federated-authentication-service/2206/install-configure.html#connect-to-citrix-cloud>)を参照してください。

- **イベントログの改善。** 新しいFASイベントログを追加しました。これらのイベントログの詳細については、「FASイベントログ」(</ja-jp/federated-authentication-service/2206/config-manage/troubleshoot-logon.html#fas-event-logs>)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」(</ja-jp/federated-authentication-service/2206/whats-new/fixed-issues.html>)を参照してください。

修正された問題

Federated Authentication Service 2206 には、修正された問題はありません。

既知の問題

Federated Authentication Service 2206には既知の問題はありません。

レジストリエントリの変更を推奨する回避策には、以下の警告が適用されます。

警告：

レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターはご自身の責任において使用してください。編集する前に必ずレジストリをバックアップしてください。

サードパーティ通知

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ソフトウェアが含まれている場合があります。

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

システム要件

- Federated Authentication Service (FAS) は、以下の Windows Server バージョンでサポートされています。
 - Windows Server 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 コンポーネントを含まないサーバーに FAS をインストールすることをお勧めします。
- Windows Server はセキュリティで保護されている必要があります。ドメインユーザーに証明書を自動的に発行できる登録機関証明書と秘密キーにアクセスでき、それらのユーザー証明書と秘密キーにもアクセスできます。
- FAS の ([/ja-jp/federated-authentication-service/2206/config-manage/ps-sdk.html](#)) 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（ルートまたは下位）が必要です。

Citrix Virtual Apps または Citrix Virtual Desktops™ サイトの場合:

- 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。
- マシンカタログを作成する前に、Federated Authentication Service のグループポリシー構成が VDA に正しく適用されている必要があります。詳細については、「([/ja-jp/federated-authentication-service/2206/install-configure.html#configure-group-policy](#))」セクションを参照してください。

このサービスの展開を計画する際は、「([/ja-jp/federated-authentication-service/2206/config-manage/security.html#security-considerations](#))」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

セキュリティ上の理由から、Citrixでは、フェデレーション認証サービス (FAS) を、ドメインコントローラーまたは証明機関と同様の方法で保護された専用サーバーにインストールすることを推奨しています。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ダウンロード](#) から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構成用の ([/ja-jp/federated-authentication-service/2206/config-manage/ps-sdk.html](#))
- ([/ja-jp/federated-authentication-service/2206/install-configure.html#using-the-federated-authentication-service-administration-console](#))

- 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
- (/ja-jp/federated-authentication-service/2206/config-manage/performance-counters.html)および (/ja-jp/federated-authentication-service/2206/config-manage/troubleshoot-logon.html#fas-event-logs)

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、以下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サーバー設定は保持されます。
- FASをアップグレードする前に、FAS管理コンソールが閉じていることを確認してください。
- 常に少なくとも1つのFASサーバーが利用可能であることを確認してください。フェデレーション認証サービスが有効な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インストーラーからFASをインストールするか、スタンドアロンFASインストーラーファイルから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:

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

StoreFrontストアでFAS統合を有効にするには、管理者アカウントとして次のPowerShellコマンドレットを実行します。ストア名が異なる場合は、`$StoreVirtualPath` を修正してください。

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

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

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

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

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

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module  
  
$StoreVirtualPath = "/Citrix/Store"  
  
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath  
  
$auth = Get-STFAuthenticationService -StoreService $store  
  
Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName  
"standardClaimsFactory"  
  
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

Delivery Controller™を構成する

注:

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

FASを使用するには、Citrix Virtual AppsまたはCitrix Virtual Desktops™ Delivery Controllerが、それに接続できるStoreFrontサーバーを信頼するように構成します。これには、**Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** PowerShellコマンドレットを実行します。これは、サイト内のDelivery Controllerの数に関係なく、サイトごとに1回だけ実行すれば十分です。

グループポリシーを構成する

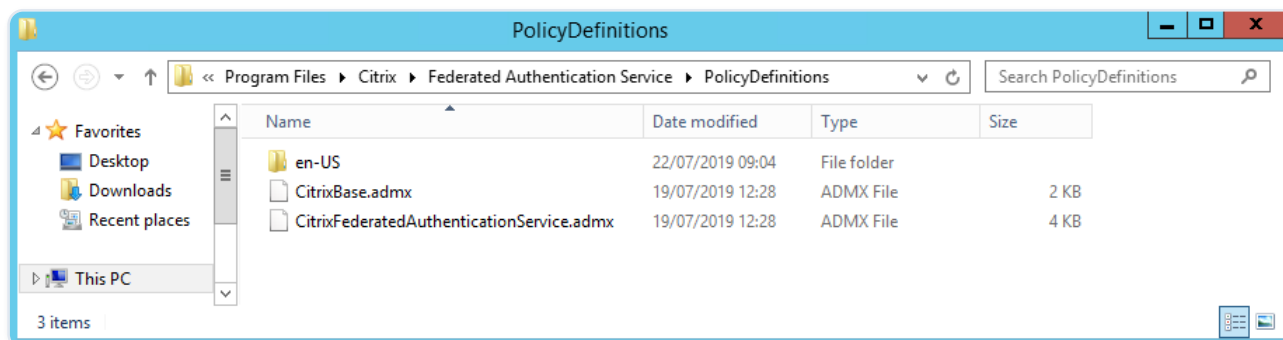
FASをインストールした後、インストールで提供されるグループポリシーテンプレートを使用して、グループポリシーでFASサーバーの完全修飾ドメイン名（FQDN）を指定する必要があります。

重要:

チケットを要求するStoreFrontサーバーと、チケットを引き換えるVirtual Delivery Agent (VDA) が、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ています。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。

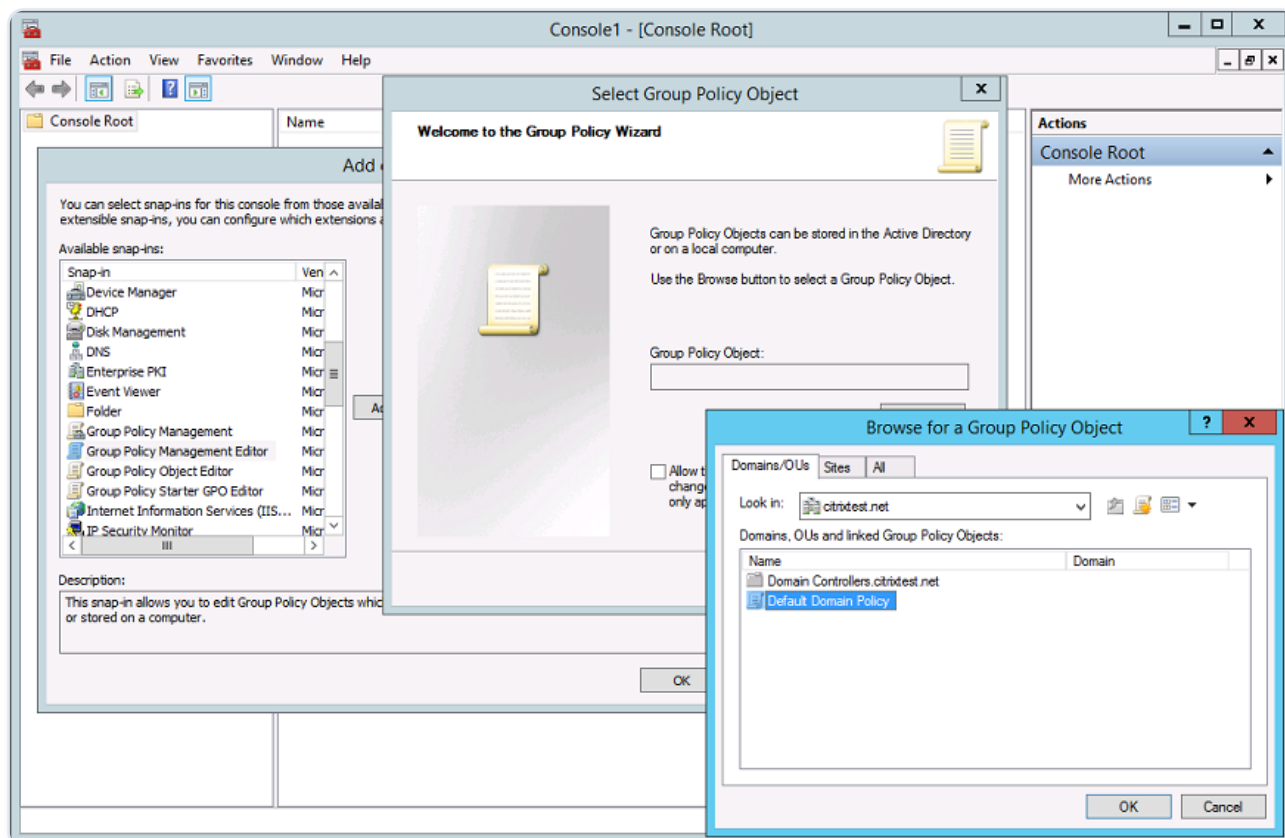
手順1. FASをインストールしたサーバーで、C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx および CitrixBase.admx ファイル、および en-US フォルダーを見つけます。



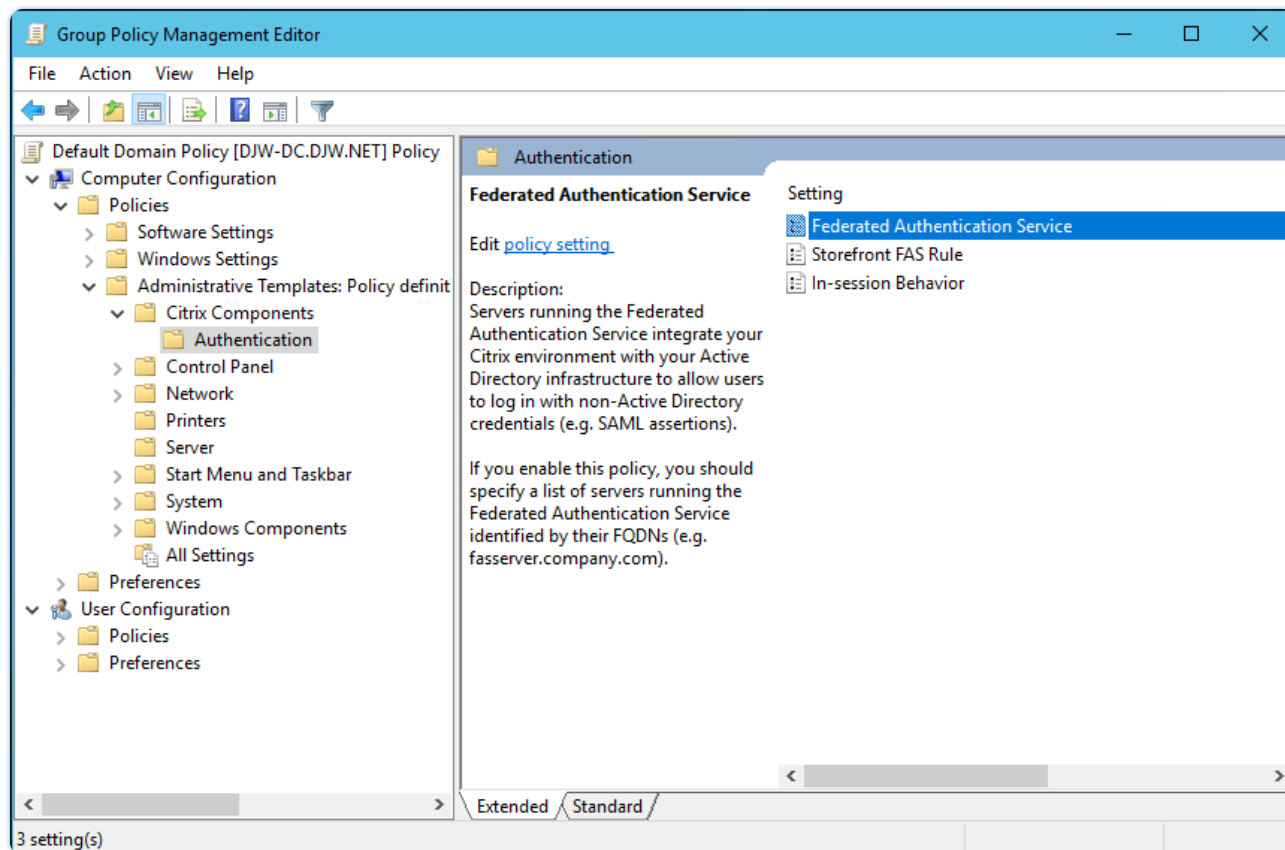
ステップ2. これらをドメインコントローラーにコピーし、C:\Windows\PolicyDefinitionsおよびen-USサブフォルダーに配置します。

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することもできます。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。



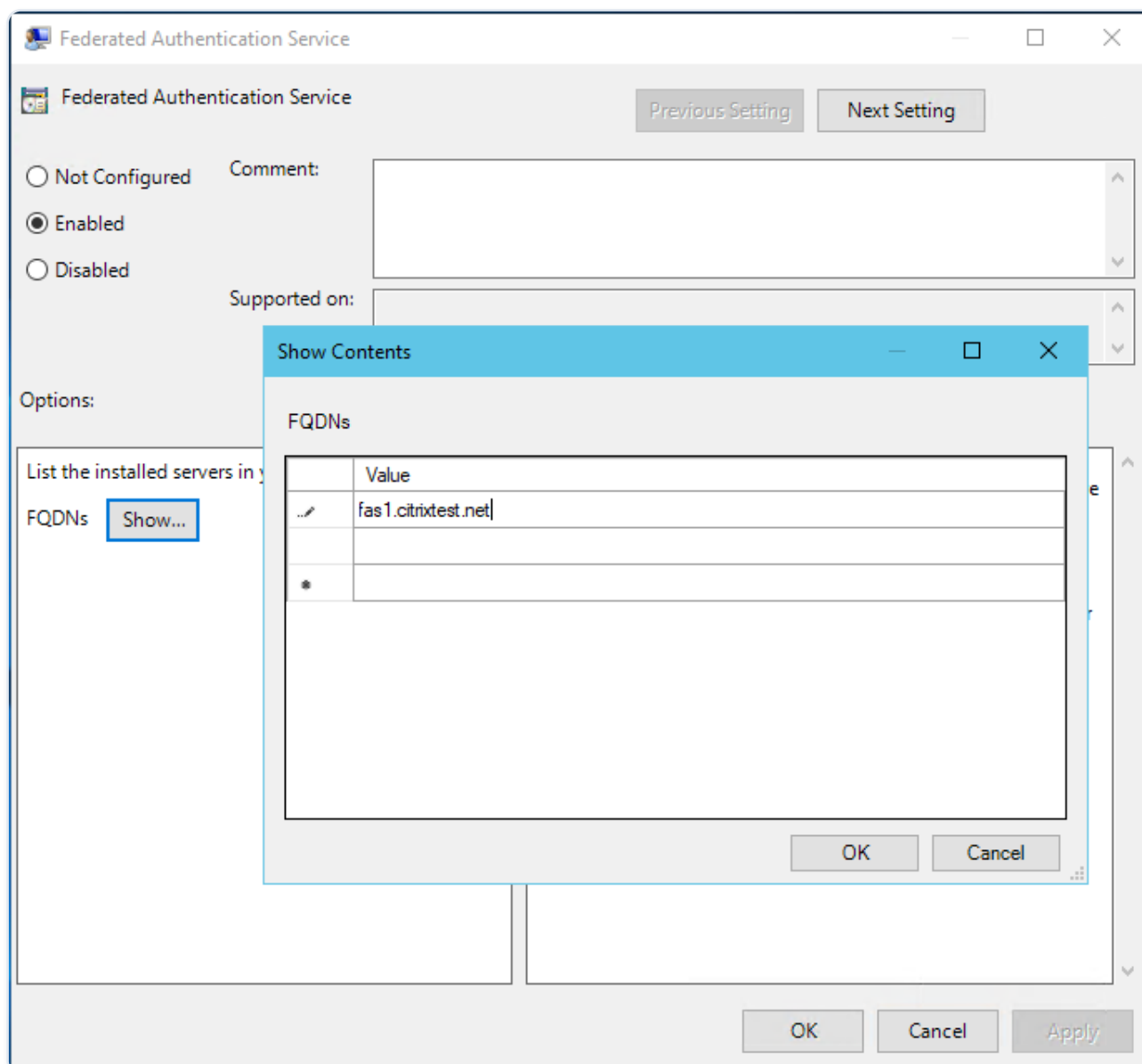
ステップ4. / にある *Federated Authentication Service* ポリシーに移動します。



注：

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、リストの順序は、VDA、StoreFrontサーバー（存在する場合）、およびFASサーバーから見て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）、再起動が必要になる場合があります。

セッション中の動作

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いる かつ 証明書の作成に使用される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可能です。[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、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。

プロンプトスコープ

このポリシーが有効な場合、**プロンプトスコープ**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、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、同意が持続する期間（秒単位）を制御します。たとえば、300秒に設定すると、ユーザーは5分ごとにプロンプトが表示されます。値がゼロの場合、秘密鍵の操作ごとに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。この機能は、「スマートカード取り外し時の切断」ポリシーと同様の動作を提供し、ユーザーがActive Directoryログオン資格情報を持っていない状況で役立ちます。

注：

ロック時の切断ポリシーは、VDA上のすべてのセッションに適用されます。

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

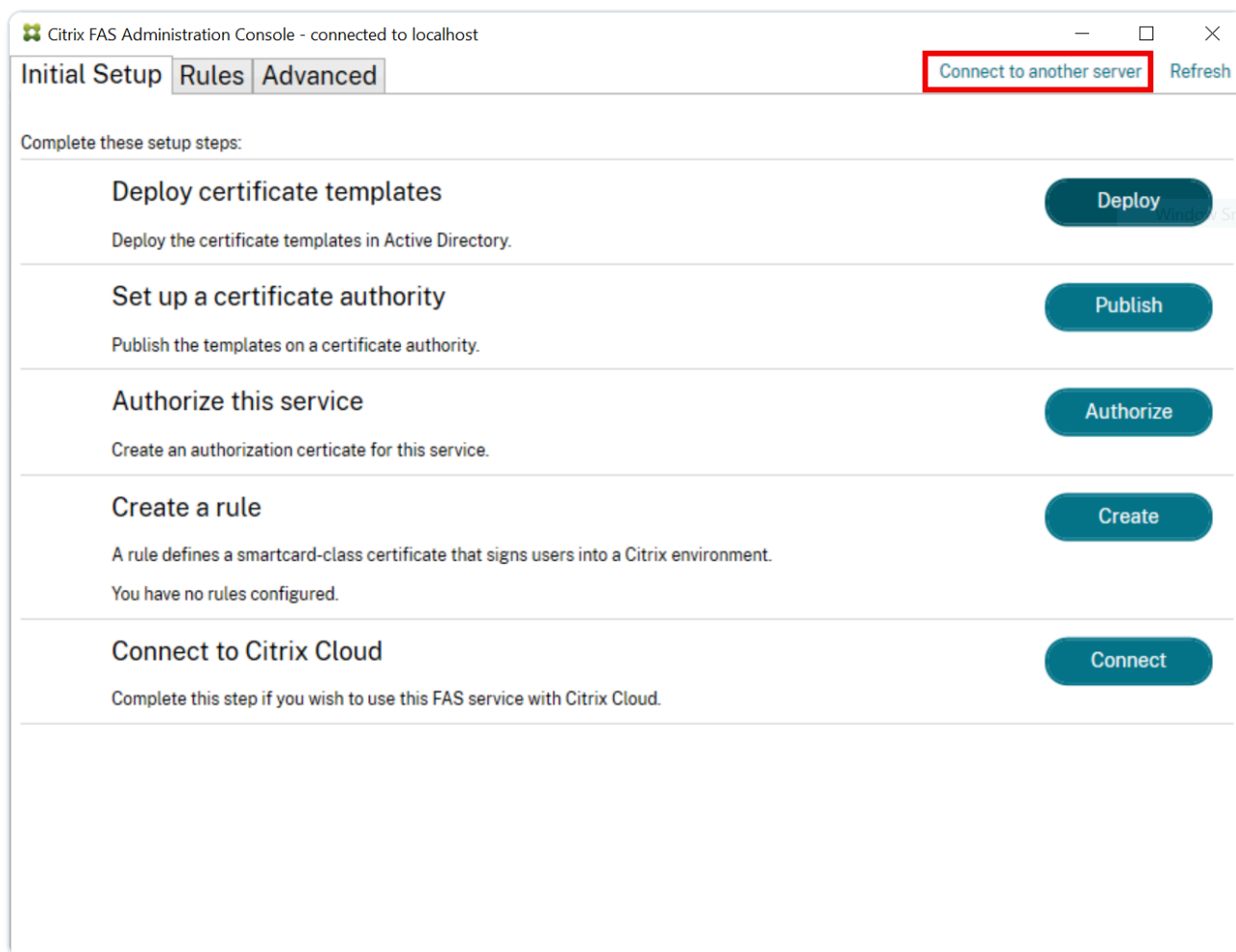
注：

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インターフェイスではより高度なオプションが提供されます。FAS PowerShellコマンドレットについては、「[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、証明書テンプレートの展開、証明機関のセットアップ、およびFASが証明機関を使用するための承認を行うプロセスが案内されます。一部の手順は、OS構成ツールを使用して手動で完了することもできます。

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

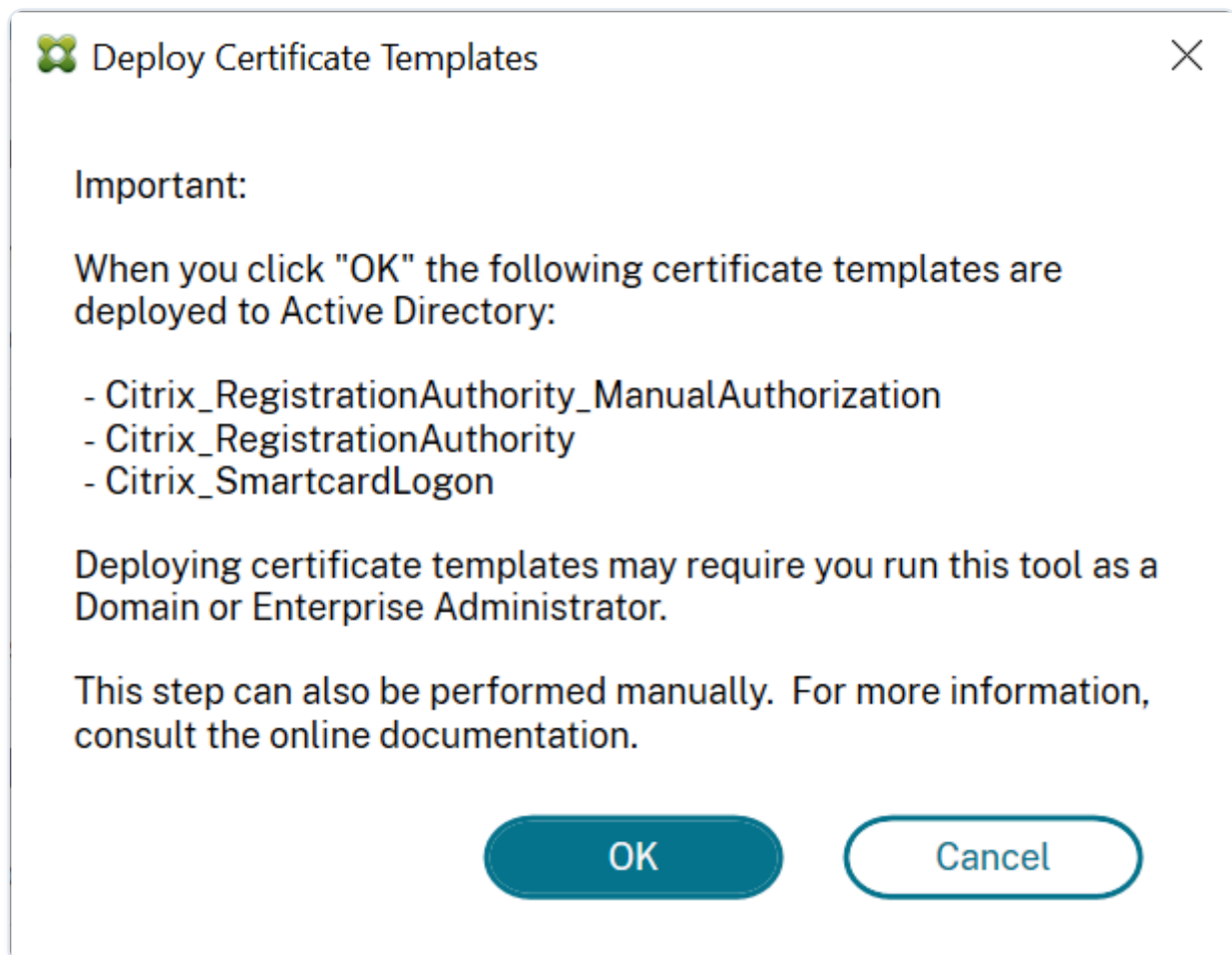


証明書テンプレートを展開する

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。**「Deploy」ボタンをクリックし、次に「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:\プログラムファイル\Citrix\フェデレーテッド認証サービス\証明書テンプレート

証明書テンプレートフォルダー。(/en-us/federated-authentication-service/2206/media/certificate-templates.png)

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以下の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、それらは1つ以上のMicrosoft Enterprise証明機関サーバーに公開される必要があります。Active Directory証明書サービスの展開方法については、Microsoftのドキュメントを参照してください。

テンプレートが少なくとも1つのサーバーに公開されていない場合は、**証明機関のセットアップ**を使用して公開します。証明機関を管理する権限を持つユーザーとしてこれを行う必要があります。

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

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/setup-cert-authority.png)

フェデレーション認証サービスを承認する

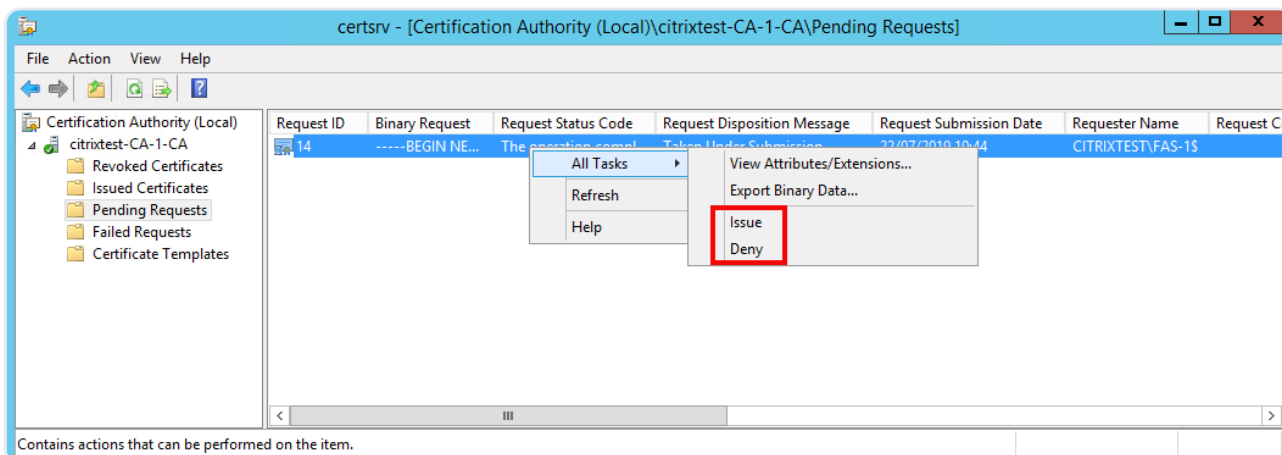
この手順により、FASの承認が開始されます。管理コンソールはCitrix_RegistrationAuthority_ManualAuthorizationテンプレートを使用して証明書要求を生成し、そのテンプレートを公開している証明機関のいずれかに送信します。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/authorize-service.png)

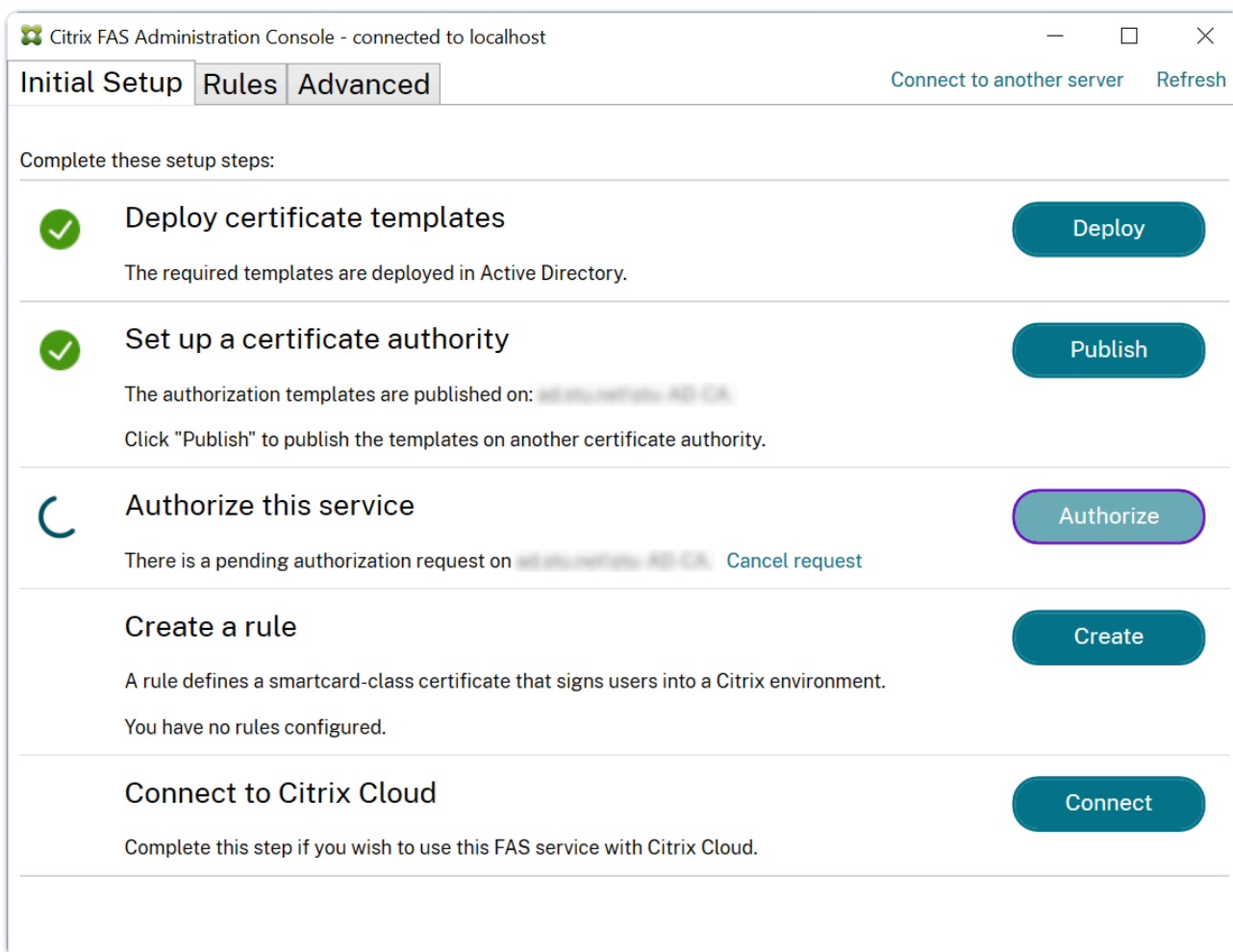
要求が送信されると、Microsoft証明機関コンソールの**保留中の要求**リストに、FASマシンアカウントからの保留中の要求として表示されます。FASの構成を続行する前に、証明機関管理者は要求を発行または拒否する必要があります。

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証明機関コンソールで、**すべてのタスク**を右クリックし、証明書要求に対して**発行**または**拒否**を選択します。**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すると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。



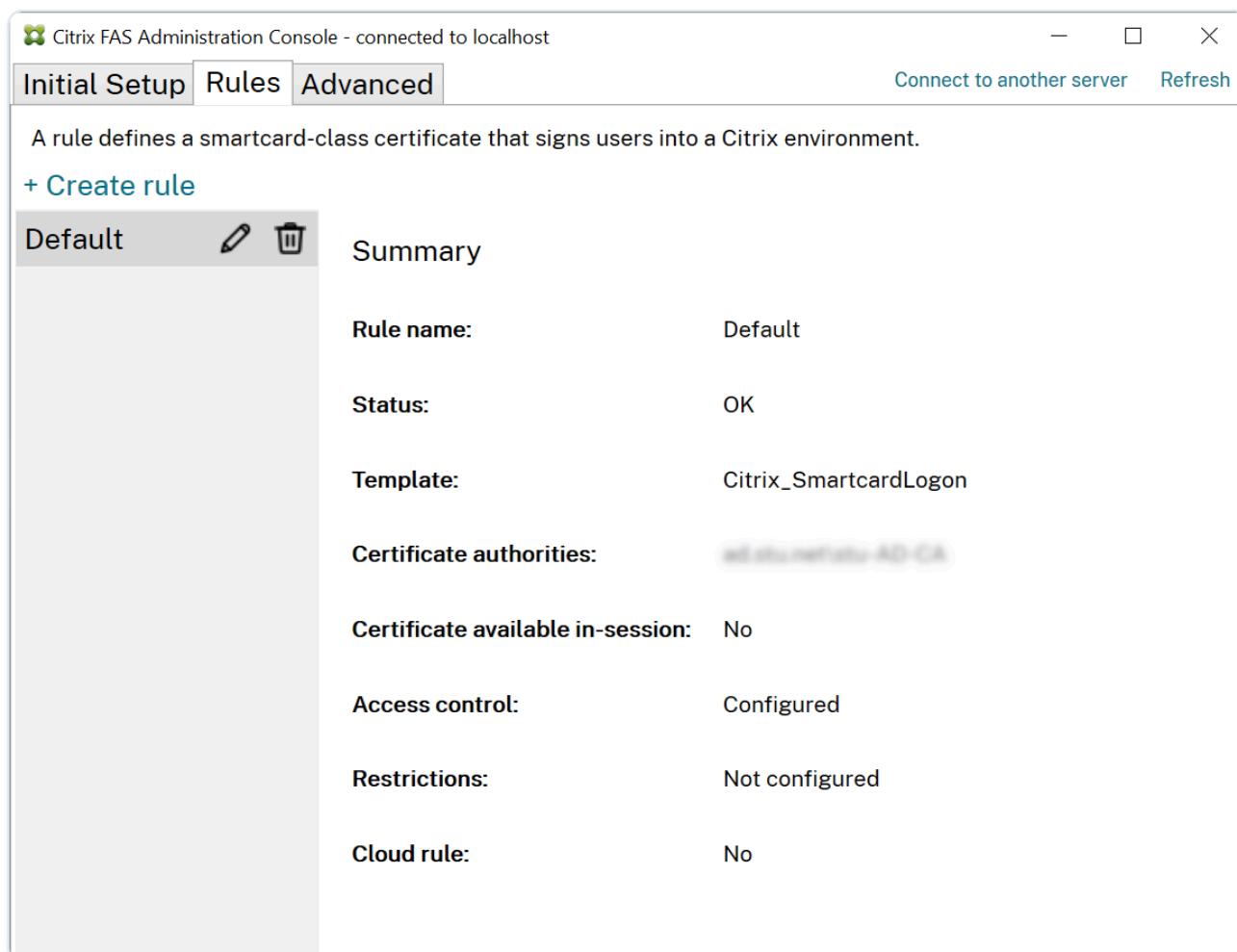
ルールの構成

FASは、StoreFrontの指示に従って、VDAログオンおよびセッション内使用のための証明書の発行を承認するためにルールを使用します。各ルールは、証明書を要求するために信頼されているStoreFrontサーバー、それらを要求できるユーザーのセット、およびそれらを使用することを許可されているVDAマシンのセットを指定します。

FASには、少なくとも1つのルールを作成および構成する必要があります。「default」という名前のルールを作成することをお勧めします。なぜなら、デフォルトでは、StoreFrontがFASに接続する際に「default」という名前のルールを要求するからです。

異なる証明書テンプレートと証明機関を参照し、異なるプロパティと権限を持つように構成するために、追加のカスタムルールを作成できます。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**ルールを作成**）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: 
	Certificate available in-session: No
	Access control: Configured
	Restrictions: Not configured
	Cloud rule: No

ウィザードによって収集される情報は次のとおりです。

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

セッション内使用: セッション内使用を許可オプションは、VDAへのログオン後に証明書を使用できるかどうかを制御します。

- **セッション内使用を許可**が選択されていない (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。
- **セッション内使用を許可**が選択されている — 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べきではありません。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。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セッション内でWebサーバーへのTLS認証が必要な場合、証明書はInternet Explorerで使用できます。

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。

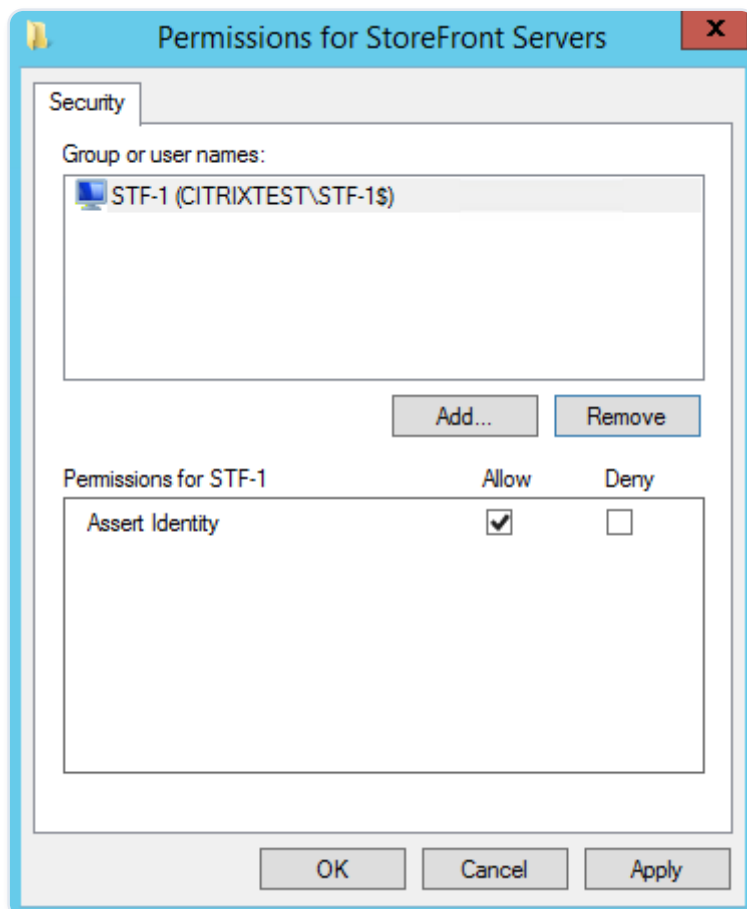
重要:

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。Citrix Cloudでルールが使用される場合、StoreFrontのアクセス許可は無視されます。Citrix CloudとオンプレミスのStoreFront展開の両方で同じルールを使用できます。オンプレミスのStoreFrontでルールが使用される場合、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（「IDアサート」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。

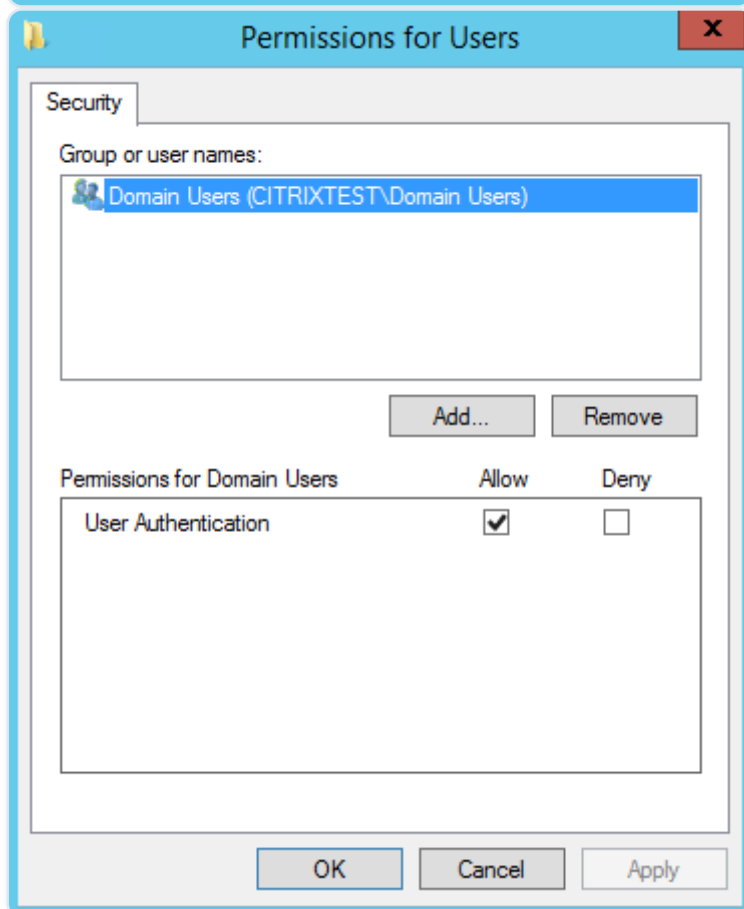
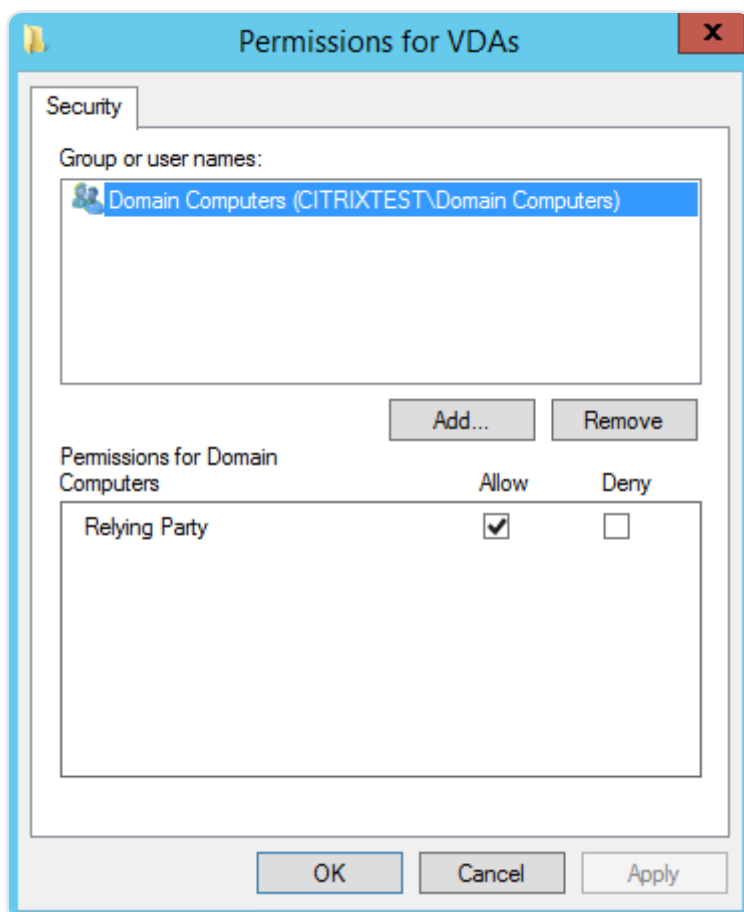


制限: FASを使用してユーザーをログオンできるVDAマシンのリストと、FASを通じて証明書を発行できるユーザーのリスト。

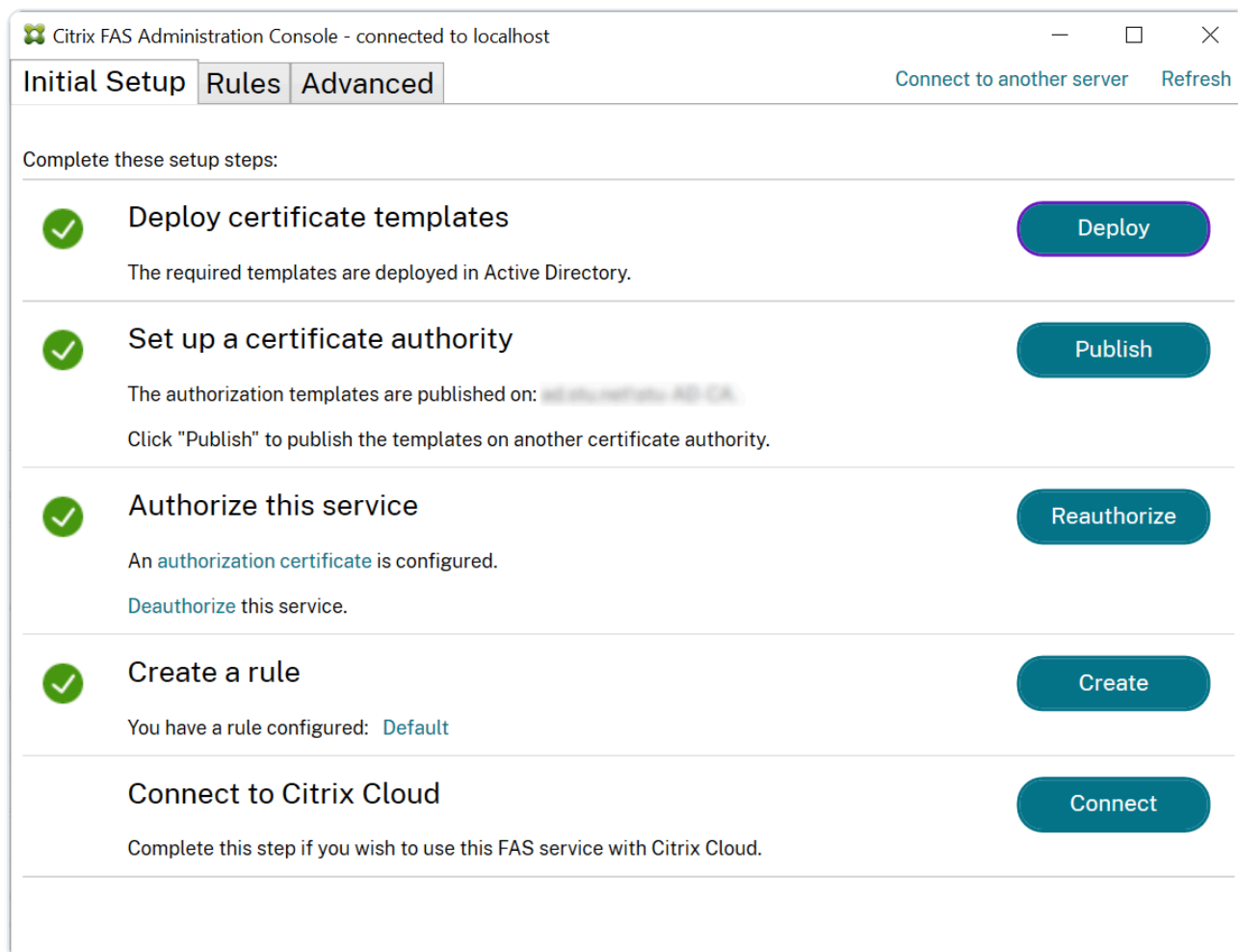
- **VDA権限の管理**では、どのVDAがFASを使用してユーザーをログオンできるかを指定できます。VDAのリストはデフォルトで「ドメインコンピューター」です。
- **ユーザー権限の管理**では、どのユーザーがFASを使用してVDAにサインインできるかを指定できます。ユーザーのリストはデフォルトで「ドメインユーザー」です。

注:

FASサーバーがVDAおよびユーザーとは異なるドメインにある場合、デフォルトの制限を変更する必要があります。



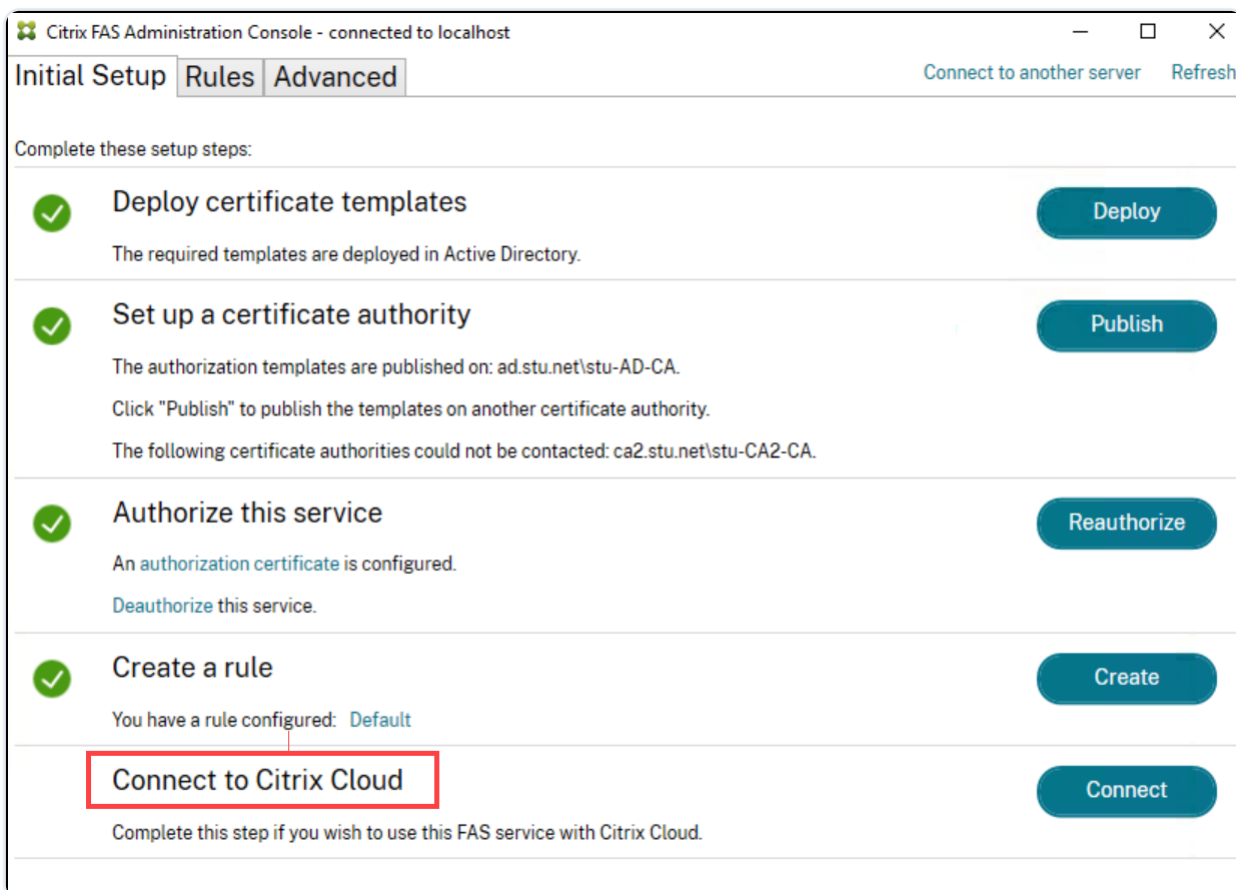
クラウドルール: Citrix WorkspaceからIDアサーションが受信されたときにルールが適用されるかどうかを示します。Citrix Cloudに接続するときに、Citrix Cloudで使用するルールを選択します。また、「**Connect to Citrix Cloud**」セクションのリンクからCitrix Cloudに接続した後でルールを変更することもできます。



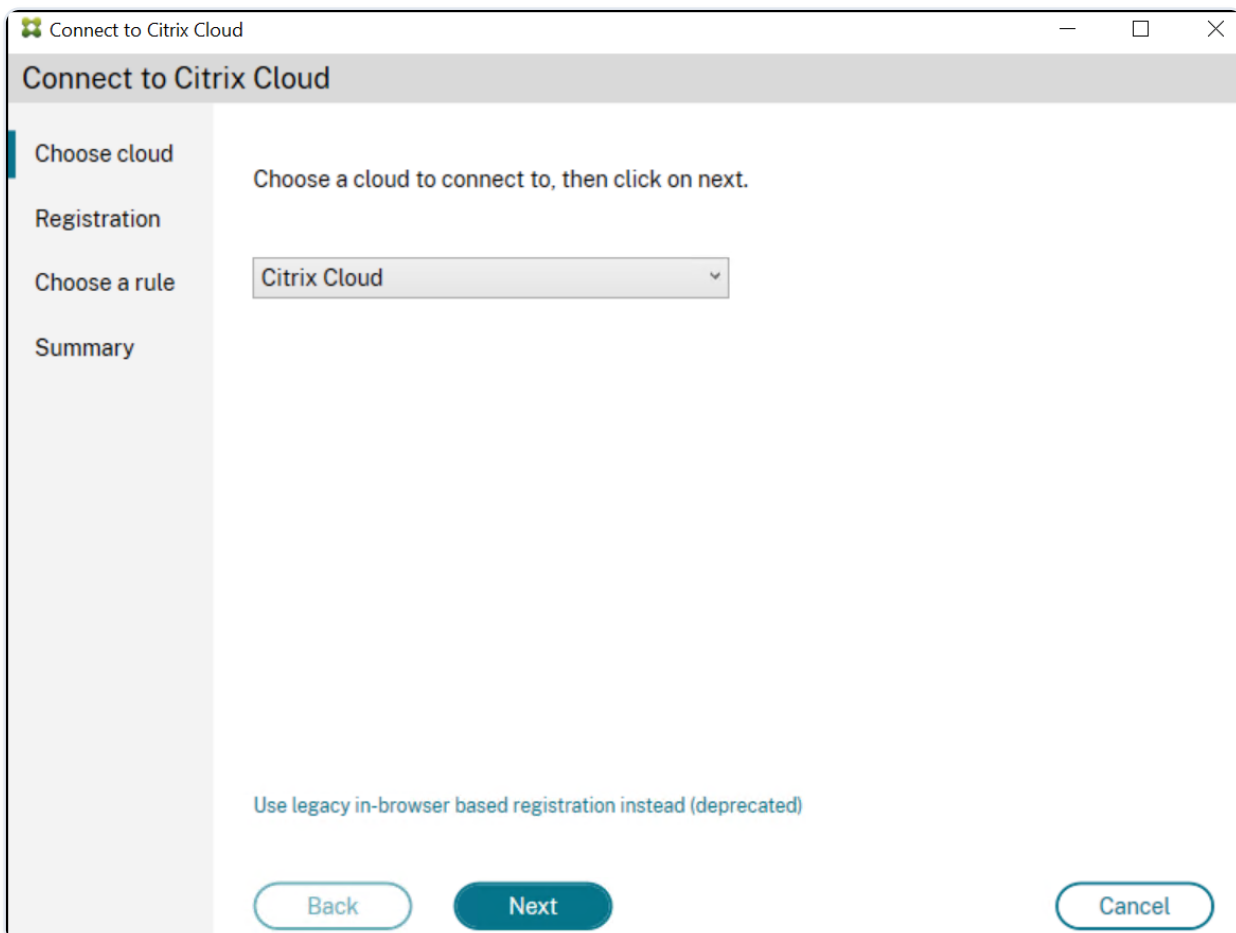
Citrix Cloudへの接続

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

1. タブの「**Connect to Citrix Cloud**」で、をクリックします。



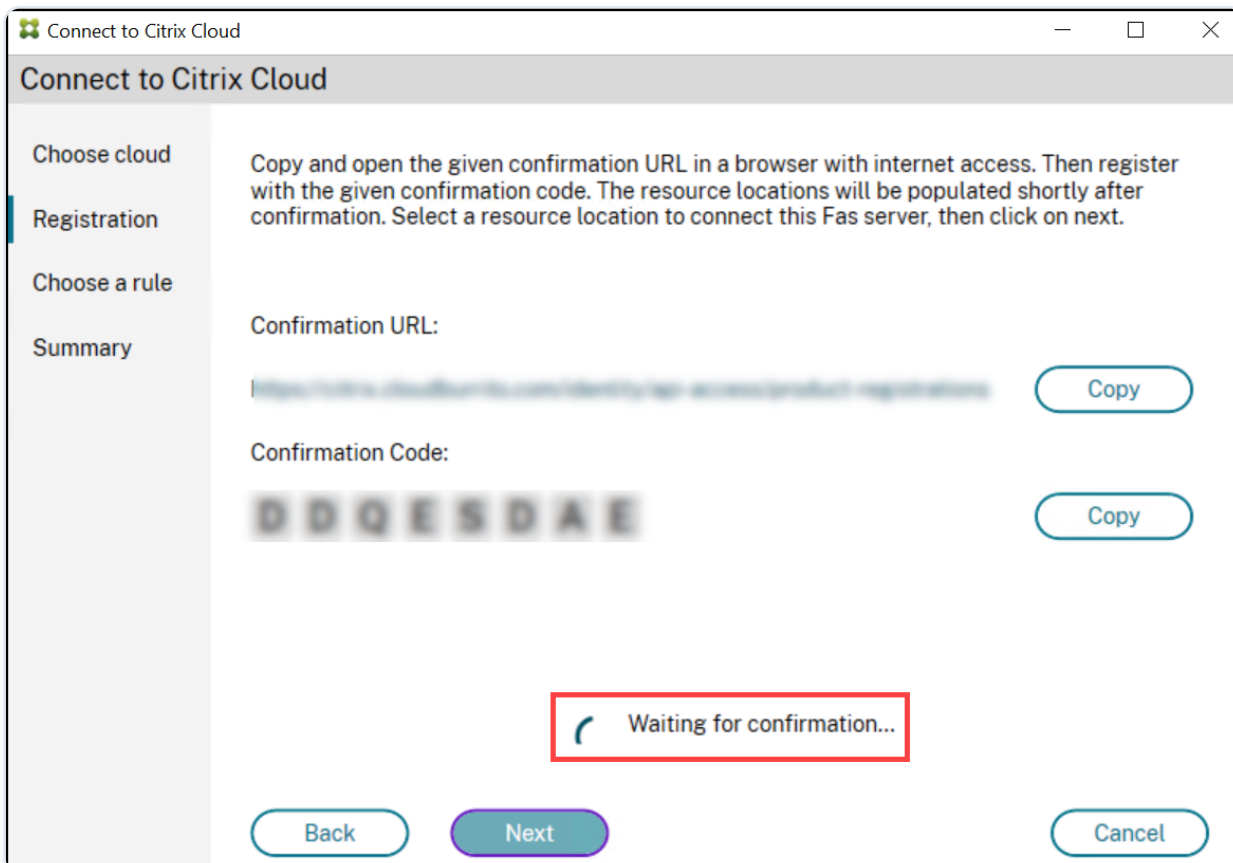
2. 接続するクラウドを選択し、をクリックします。



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。このコードはCitrix Cloudで承認する必要があります。詳しくは、「[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目的の「リソースの場所」を選択します。

Connect to Citrix Cloud

Choose cloud

Registration

Choose a rule

Summary

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:

[https://www.citrix.com/identity/api/.../product/registration](#) Copy

Confirmation Code:

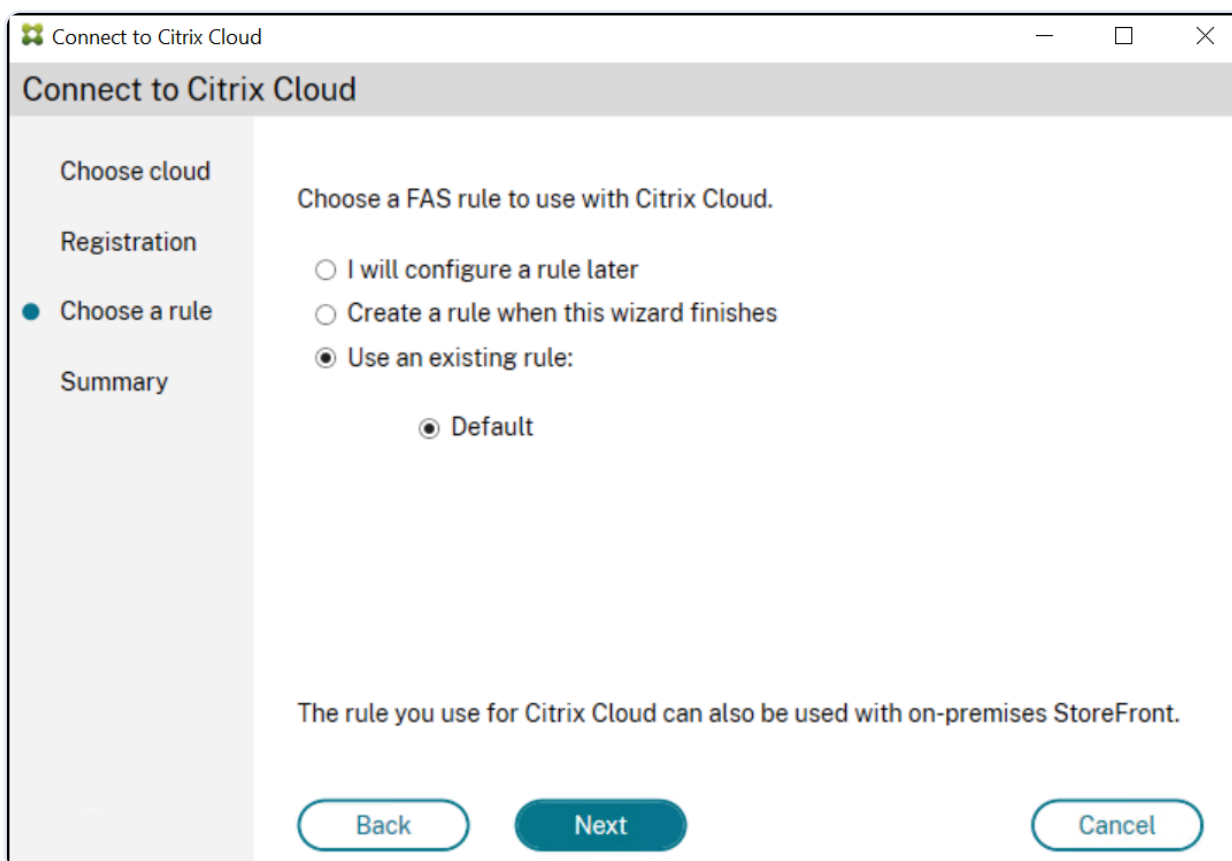
7 8 5 5 2 8 8 8 Copy

Resource location:

My Resource Location

Back Next 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。をクリックし、確認ウィンドウを閉じます。
6. 「**ルールを選択**」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。



Connect to Citrix Cloud

Choose cloud

Registration

● Choose a rule

Summary

Choose a FAS rule to use with Citrix Cloud.

☐ I will configure a rule later

☐ Create a rule when this wizard finishes

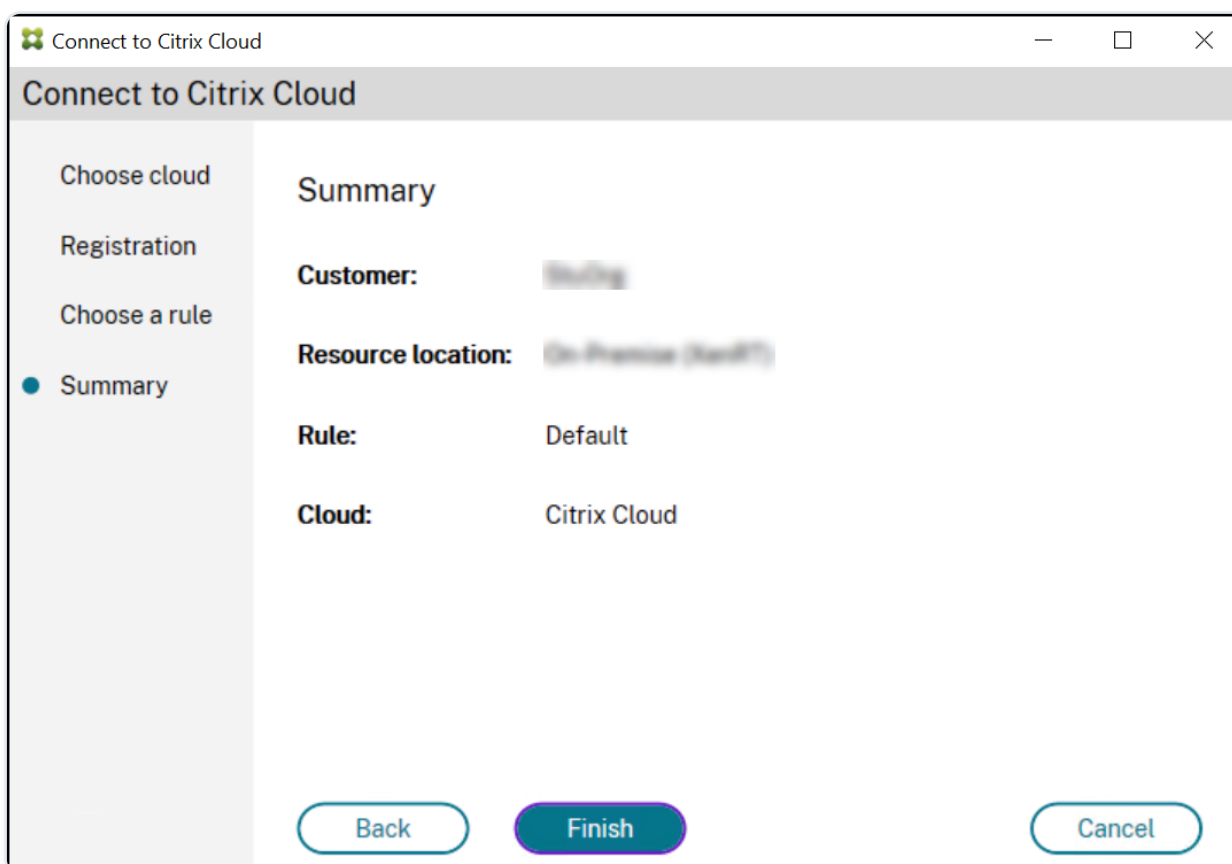
☒ Use an existing rule:

☒ Default

The rule you use for Citrix Cloud can also be used with on-premises StoreFront.

Back Next 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。



Connect to Citrix Cloud

Choose cloud

Registration

Choose a rule

● Summary

Summary

Customer: **Routing**

Resource location: **On-Premise (Self?)**

Rule: **Default**

Cloud: **Citrix Cloud**

Back Finish 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。

Citrix Cloudから切断する

この[Citrix Workspaceの記事](#)に記載されているように、Citrix Cloudリソースの場所からFASサーバーを削除した後、「**Citrix Cloudに接続**」で「**無効にする**」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。

証明機関の構成

この記事では、Federated Authentication Service (FAS) を証明機関 (CA) サーバーと統合するため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。この記事の手順を実行する前に、PowerShell の基本的な知識があることを確認してください。

FAS で使用する複数の CA サーバーをセットアップする

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。

Edit Rule

Edit rule "hello"

Choose the certificate authority (CA) where user certificates will be generated. You can choose multiple certificate authorities for load balancing and failover. [Refresh](#)

Name	Status
☒ ad-itu.net-itu-AD-CA	Template available
☒ ad-itu.net-itu-CA2-CA	Template available

☒ Only show CAs publishing Citrix_SmartcardLogon (recommended).

[Apply](#) [Cancel](#)

選択するすべての 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）を発行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発行していない場合は、その CA に対して [証明機関をセットアップする](#) の手順を実行します。

注：

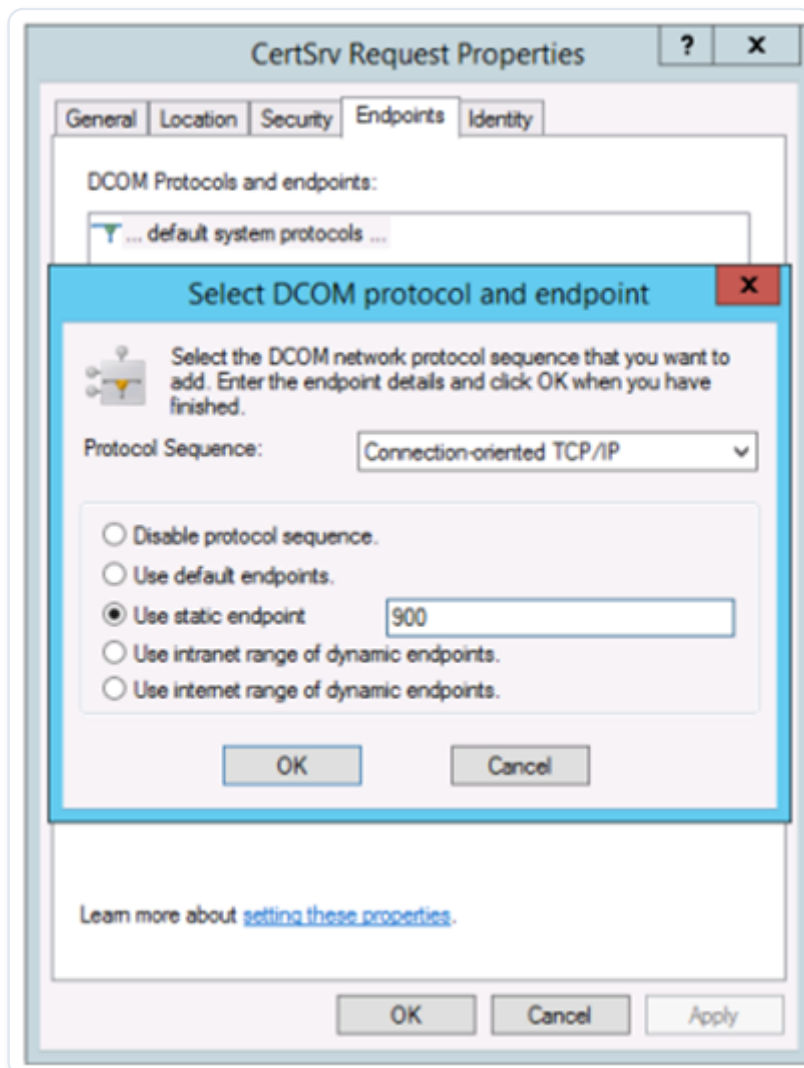
すべての CA に対して [このサービスを承認する](#) の手順を実行する必要はありません。この手順で構成された承認証明書は、どの CA でも使用できるためです。

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 サーバーは利用可能な別の CA サーバーに切り替わります。

TCP アクセス用に Microsoft 証明機関を構成する

デフォルトでは、Microsoft CA はアクセスに DCOM を使用します。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増す可能性があるため、Microsoft は静的 TCP ポートに切り替えるための規定を設けています。Microsoft CA で、**[スタート] > [ファイル名を指定して実行] > 「dcomcnfg.exe」** を使用して DCOM 構成パネルを開き、**[コンピューター] > [マイコンピューター] > [DCOM の構成]** を展開して **CertSrv Request** ノードを表示し、CertSrv Request DCOM アプリケーションのプロパティを編集します。



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

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

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

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

ユーザー証明書を事前生成する

FASサーバー内でユーザー証明書を事前生成すると、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

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。以下の例を参照してください。

```
Import-Module ActiveDirectory

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

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

if ($searchbase -ne ""){

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

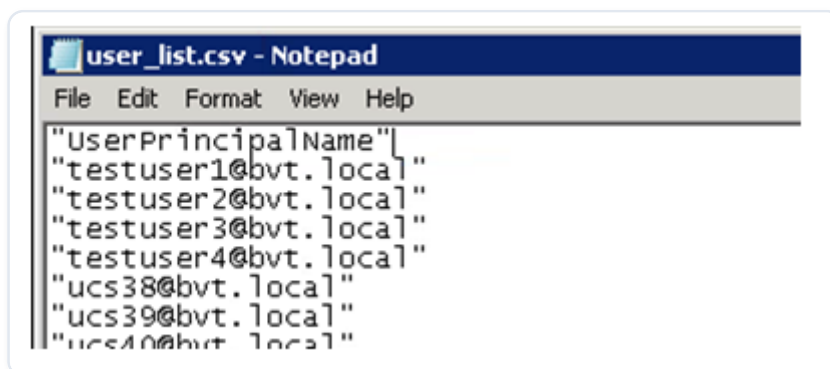
} else {
```

```
Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true") } -Properties UserPrincipalName | Select UserPrincipalName |  
Export-Csv -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「enabled」のユーザーのみをリストするためのフィルター引数が含まれています。

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

CSVは次のようになります。



FASサーバー

次のPowerShellスクリプトは、以前に生成されたユーザーリストを受け取り、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

}

}
```

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

上記のスクリプトは、「default」という名前のルールに対応しています。異なるルール名（たとえば、「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...

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

[+ Create rule](#)

Default	 	Summary
hello	 	

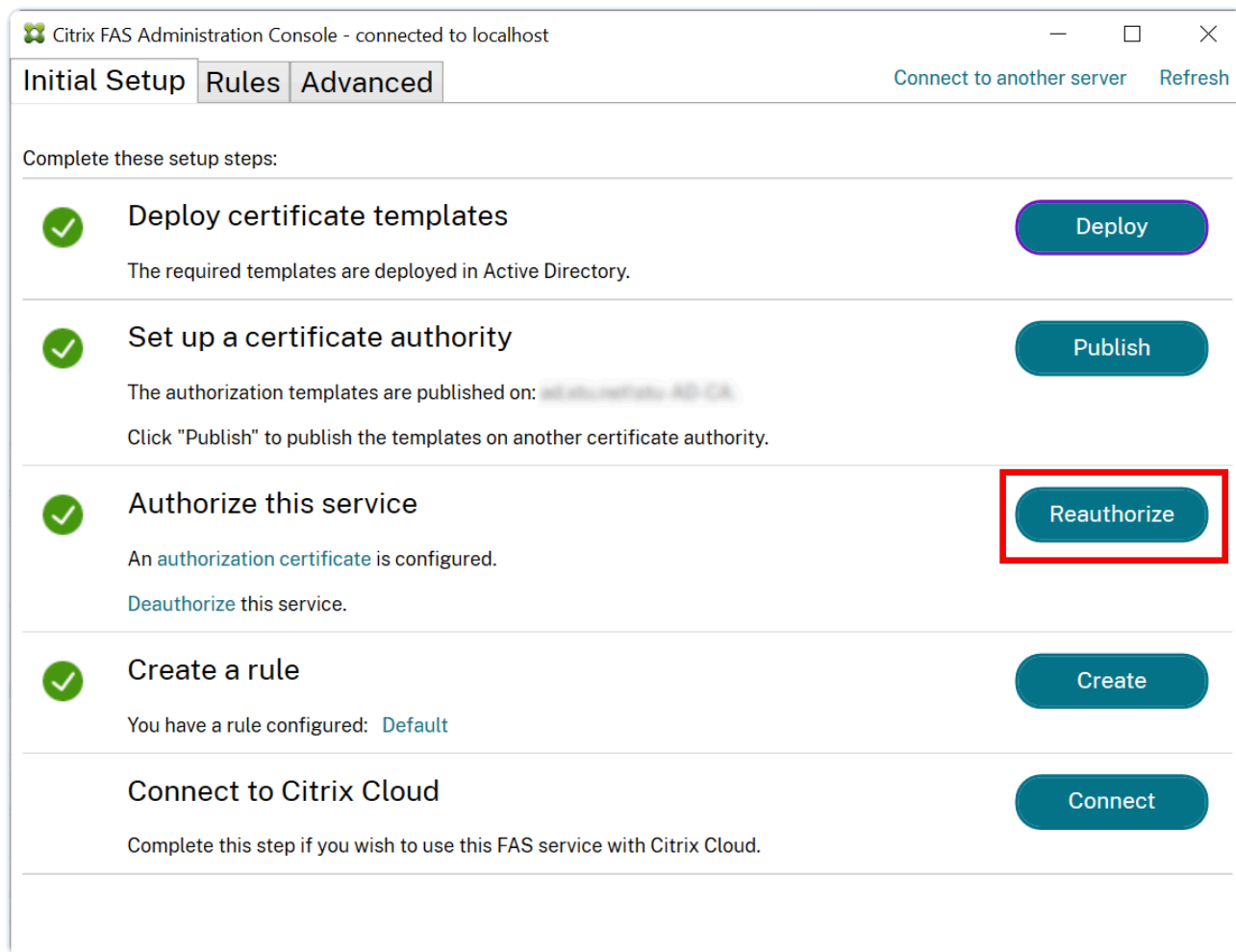
Rule name:	hello
Status:	OK
Template:	Citrix_SmartcardLogon

登録機関証明書を更新する

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

注：

GUIを使用してFASを再承認することもできます。



次のシーケンスを完了します。

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

5. FASサーバーをメンテナンスモードから解除します: `Set-FasServer -Address <FAS server> -MaintenanceMode $false`
6. 古い承認証明書を削除します: `Remove-FasAuthorizationCertificate`

関連情報

- [インストールと構成](#)の記事は、FASのインストールと構成に関する主要なリファレンスです。
- 一般的なフェデレーション認証サービスの展開については、[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

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。関連する秘密鍵は、FASサーバーのネットワークサービスアカウントによって保存され、デフォルトでエクスポート不可としてマークされます。

秘密鍵には2種類あります。

- Citrix_RegistrationAuthority証明書テンプレートからの、登録機関証明書に関連付けられた秘密鍵。
- Citrix_SmartcardLogon証明書テンプレートからの、ユーザー証明書に関連付けられた秘密鍵。

登録機関証明書は実際には2種類あります。Citrix_RegistrationAuthority_ManualAuthorization（デフォルトで24時間有効）とCitrix_RegistrationAuthority（デフォルトで2年間有効）です。

フェデレーション認証サービス（FAS）管理コンソールの**初期設定**タブのステップ3で、**承認**をクリックすると、FASサーバーはキーペアを生成し、

Citrix_RegistrationAuthority_ManualAuthorization証明書用の証明書署名要求を証明機関に送信します。これは一時的な証明書で、デフォルトで24時間有効です。証明機関はこの証明書を自動的に発行しません。その発行は、証明機関で管理者によって手動で承認される必要があります。証明書がFASサーバーに発行されると、FASはCitrix_RegistrationAuthority_ManualAuthorization証明書を使用して、Citrix_RegistrationAuthority証明書（デフォルトで2年間有効）を自動的に取得します。FASサーバーは、Citrix_RegistrationAuthority証明書を取得するとすぐに、Citrix_RegistrationAuthority_ManualAuthorizationの証明書とキーを削除します。

登録機関証明書に関連付けられた秘密鍵は特に機密性が高いです。なぜなら、登録機関証明書ポ
リシーにより、秘密鍵を所有する者は誰でも、テンプレートで構成されたユーザーセットに対して
証明書要求を発行できるからです。その結果、この鍵を制御する者は誰でも、そのセット内の任意
のユーザーとして環境に接続できます。

FASサーバーは、組織のセキュリティ要件に合った方法で秘密鍵を保護するように、以下のいずれ
かを使用して構成できます。

- 登録機関証明書とユーザー証明書の秘密鍵の両方に対して、Microsoft Enhanced RSA and AES Cryptographic ProviderまたはMicrosoft Software Key Storage Providerを使用します。
- 登録機関証明書の秘密鍵には、Trusted Platform Module (TPM) チップを備えたMicrosoft Platform Key Storage Providerを使用し、ユーザー証明書の秘密鍵には、Microsoft Enhanced RSA and AES Cryptographic ProviderまたはMicrosoft Software Key Storage Providerを使用します。
- 登録機関証明書とユーザー証明書の秘密鍵の両方に対して、ハードウェアセキュリティモジュール (HSM) デバイスを備えたHSMベンダーの暗号化サービスまたはキーストレージプロバイダーを使用します。

秘密鍵の構成設定

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

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-privatekeys-
config-file.png)

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

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

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

値	コメント
有効	CAPI API を使用する

値	コメント
false (デフォルト)	CNG API を使用する

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

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

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

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

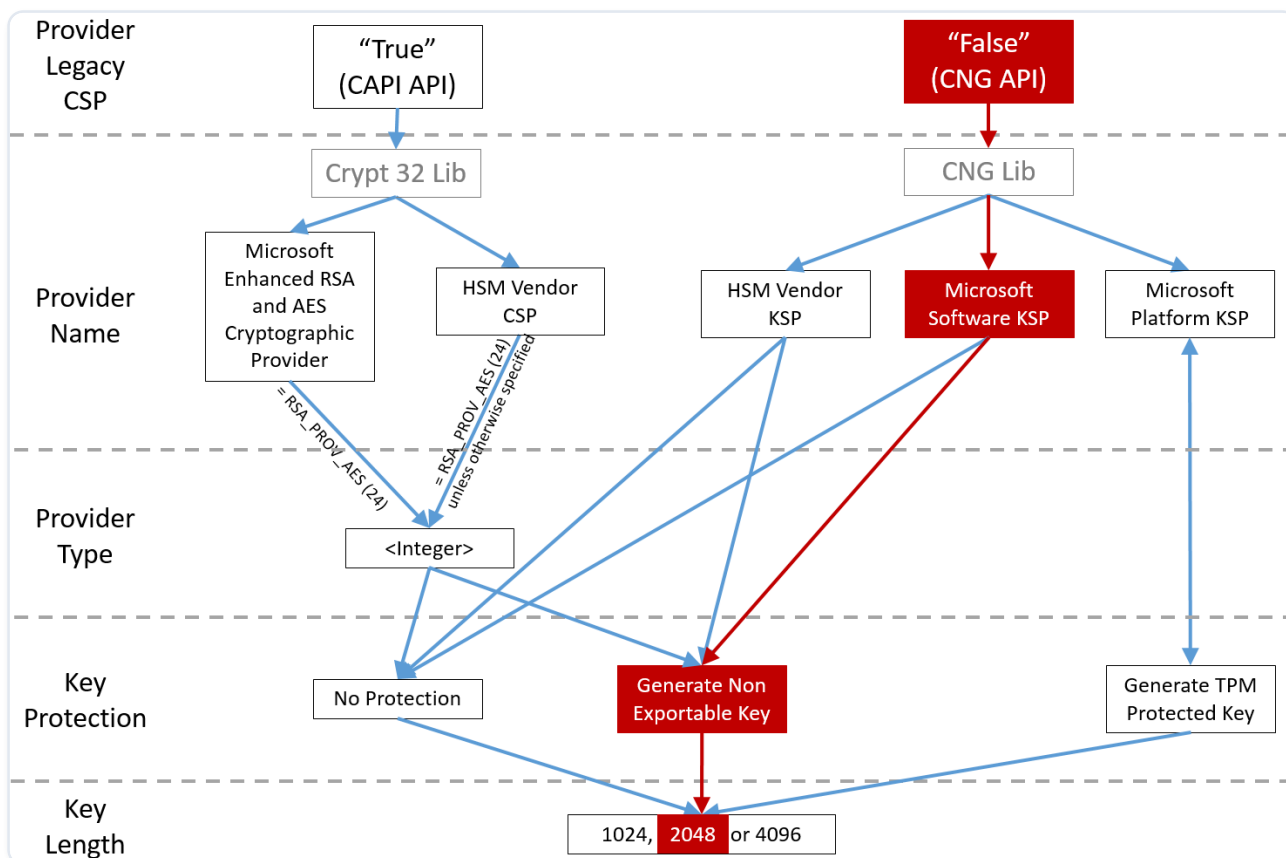
Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (FASが秘密鍵操作を実行する必要がある場合、ここで指定された値を使用します) 秘密鍵の「エクスポート可能」フラグを制御します。ハードウェアでサポートされている場合、TPMキーストレージの使用を許可します。

値	コメント
NoProtection	秘密キーはエクスポートできます。
GenerateNonExportableKey	デフォルト。秘密キーはエクスポートできません。
GenerateTPMProtectedKey	秘密キーはTPMを使用して管理されます。秘密キーは、ProviderNameで指定したProviderName（例：Microsoft Platform Key Storage Provider）を介して保存されます。

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

値	コメント
2048	デフォルト。1024または4096も使用できます。

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



構成シナリオの例

例1

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

これはデフォルトのインストール後構成です。追加の秘密鍵構成は不要です。

例 2

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

このシナリオでは、FASサーバーのマザーボード上のTPMが、TPMメーカーのドキュメントに従ってBIOSで有効にされ、その後Windowsで初期化されていることを前提としています。

<[https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-vista/cc749022\(v=ws.10\)>](https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)>) を参照してください。

FAS管理コンソールの使用

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

初期のFASセットアップを実行する際、証明書テンプレートを展開し、証明機関をセットアップした後、サービスを承認する前（構成シーケンスのステップ3）に、次の手順を実行します。

ステップ 1: 次のように、構成ファイルを編集して以下の行を変更します。

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

ファイルは次のようになります。

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

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

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

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

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

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

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

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

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

ステップ 2: Citrix Federated Authentication Serviceを再起動して、構成ファイルから値を読み取ります。

ステップ 3: サービスを承認します。

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

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

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

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

ステップ5: 設定ファイルを以下のように編集し直します:

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

注:

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

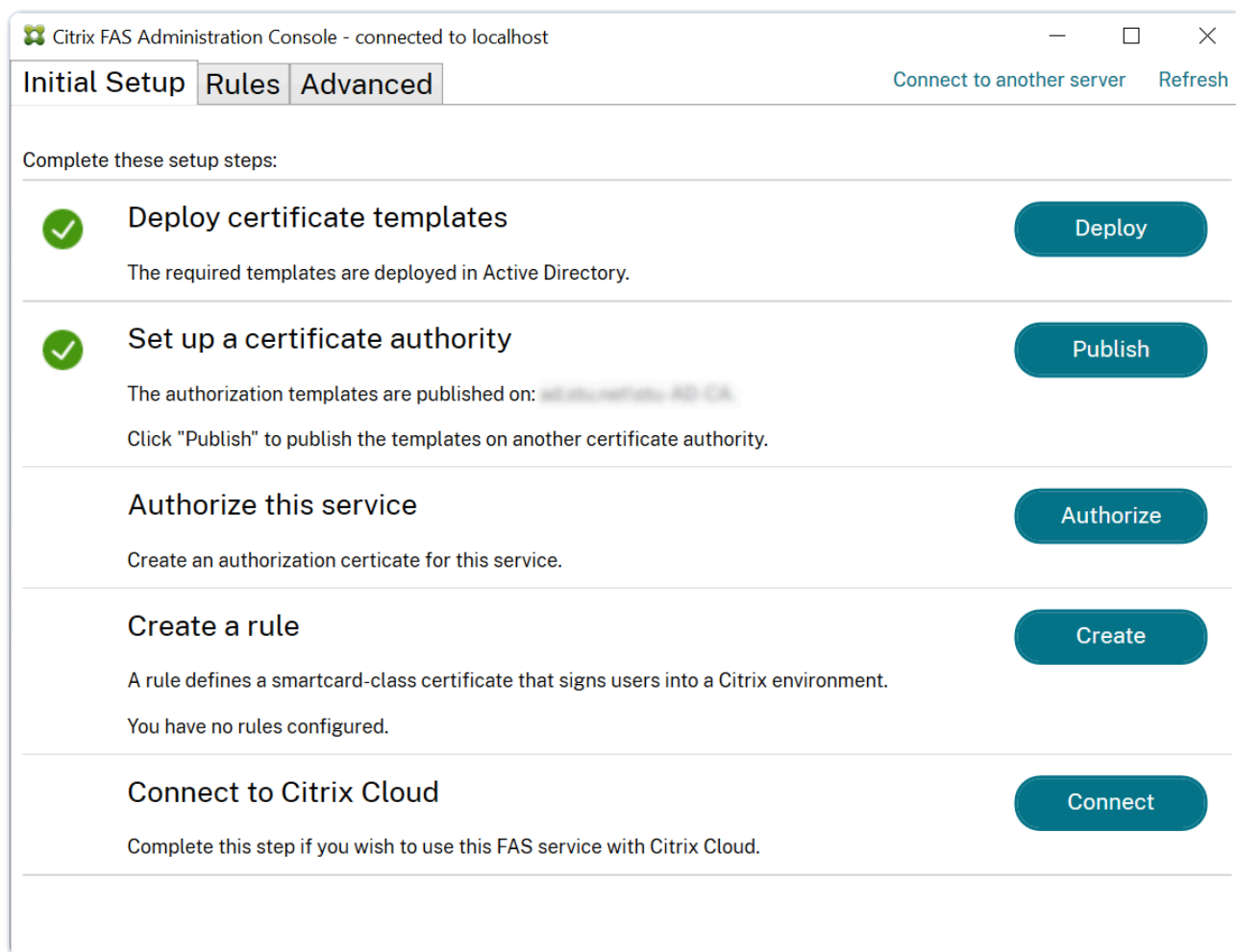
ステップ6: FASを再起動します。これにより、サービスは設定ファイルを再読み込みし、変更された値を反映します。その後の自動秘密キー操作はユーザー証明書キーに影響します。これらの操作は秘密キーをTPMに保存せず、Microsoft Software Key Storage Providerを使用します。

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

PowerShellの使用

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

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



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

Citrix_RegistrationAuthority_ManualAuthorizationテンプレートを右クリックし、テンプレートの複製を選択します。

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

Properties of New Template

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

Template display name:
Offline_RA

Template name:
Offline_RA

Validity period: 2 years Renewal period: 0 days

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

OK Cancel Apply Help

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

ステップ4: FASサーバーで以下のPowerShellコマンドレットをロードします:

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

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

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address \<FQDN of FAS Server>
```

例:

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

以下が表示されます:

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

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

注:

- Id GUID（この例では「5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39」）は、次のステップで必要になります。
- このPowerShellコマンドレットは、登録機関証明書の秘密キーを生成するために使用される1回限りの「オーバーライド」と考えてください。
- このコマンドレットを実行すると、FASの起動時に構成ファイルから読み取られた値がチェックされ、使用するキー長が決定されます（デフォルトは2048）。
- この手動のPowerShellで開始された登録機関証明書の秘密キー操作で-UseTPMが\$trueに設定されているため、システムはTPMの使用に必要な設定と一致しないファイルからの値を無視します。
- このコマンドレットを実行しても、構成ファイルの設定は変更されません。
- その後の自動FAS開始ユーザー証明書秘密キー操作では、FASの起動時にファイルから読み取られた値が使用されます。
- FASサーバーがユーザー証明書を発行する際に、TPMによって保護されたユーザー証明書の秘密鍵を生成するために、configファイルでKeyProtectionの値をGenerateTPMProtectedKeyに設定することも可能です。

TPMがキーペアの生成に使用されたことを確認するには、キーペアが生成された時点で、FASサーバーのWindowsイベントビューアーにあるアプリケーションログを確認してください。

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

Event 15, Citrix.Authentication.FederatedAuthenticationService

General Details

[S15] Administrator [CITRIXTEST\Administrator] creating certificate request [TPM: True] [correlation: e61a73d7-bb61-44af-8d21-1159d864d82e]

注: 「」

続いて表示されるのは次のとおりです。

Application Number of events: 3

Level	Date and Time	Source	Event ID	Task C...
Information	22/07/2019 12:59:42	Citrix.Fas.PkiCore	14	None
Information	22/07/2019 12:59:41	Citrix.Fas.PkiCore	16	None
Information	22/07/2019 12:59:41	Citrix.Authentication.FederatedAuthenticationService	15	None

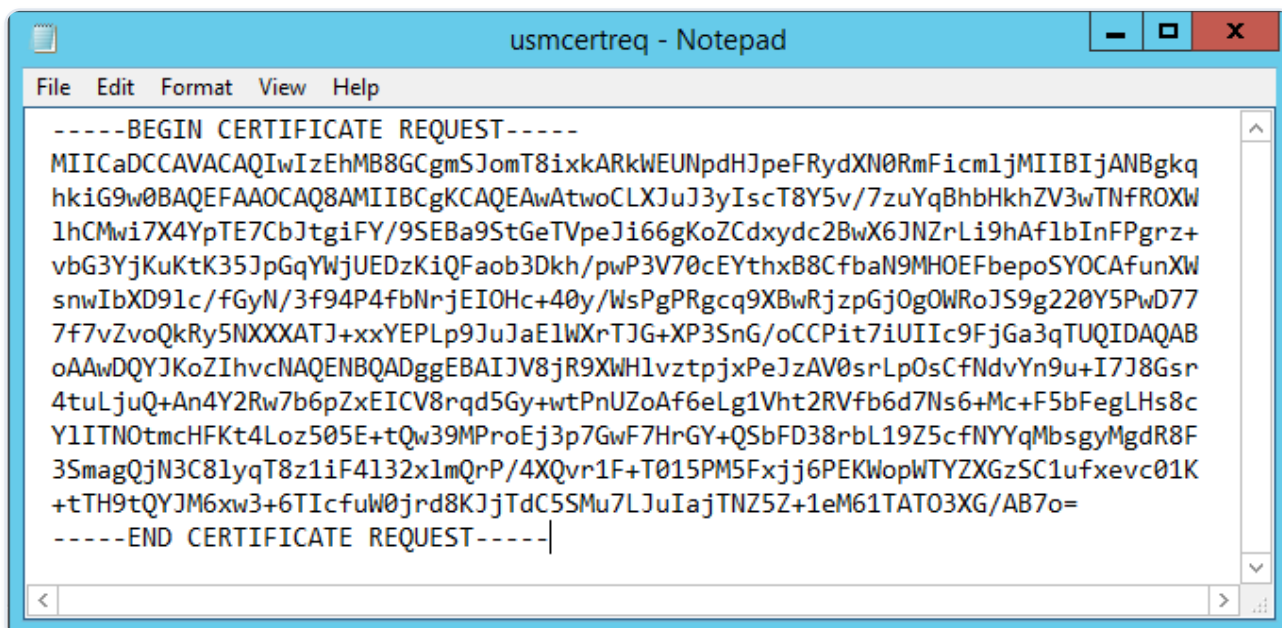
Event 16, Citrix.Fas.PkiCore

General Details

[S16] PrivateKey::Create [Identifier afae7c8d-53ff-4cf6-bd96-75fa3e606d3e_TWIN][MachineWide: False][Provider: [CNG] Microsoft Platform Crypto Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]

注: 「プロバイダー: Microsoft Platform Crypto Provider」

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



手順7: 証明書署名要求を証明機関に提出するには、FASサーバーでPowerShellに次のように入力します。

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

例：

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

次のように表示されます。

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-0BDC-4021-A4FD-2E29502177C2}
Idap:
```

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

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-privatekeys-certificate-authority-list.png)

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

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-privatekeys-certificate-authority-list-display.png)

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

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

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-privatekeys-certificate-export-wizard.png)

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。

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

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

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-privatekeys-import-fasauthorizationcertificiate-response.png)

例:

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-privatekeys-import-fasauthorizationcertificiate-response-example.png)

次のように表示されます。

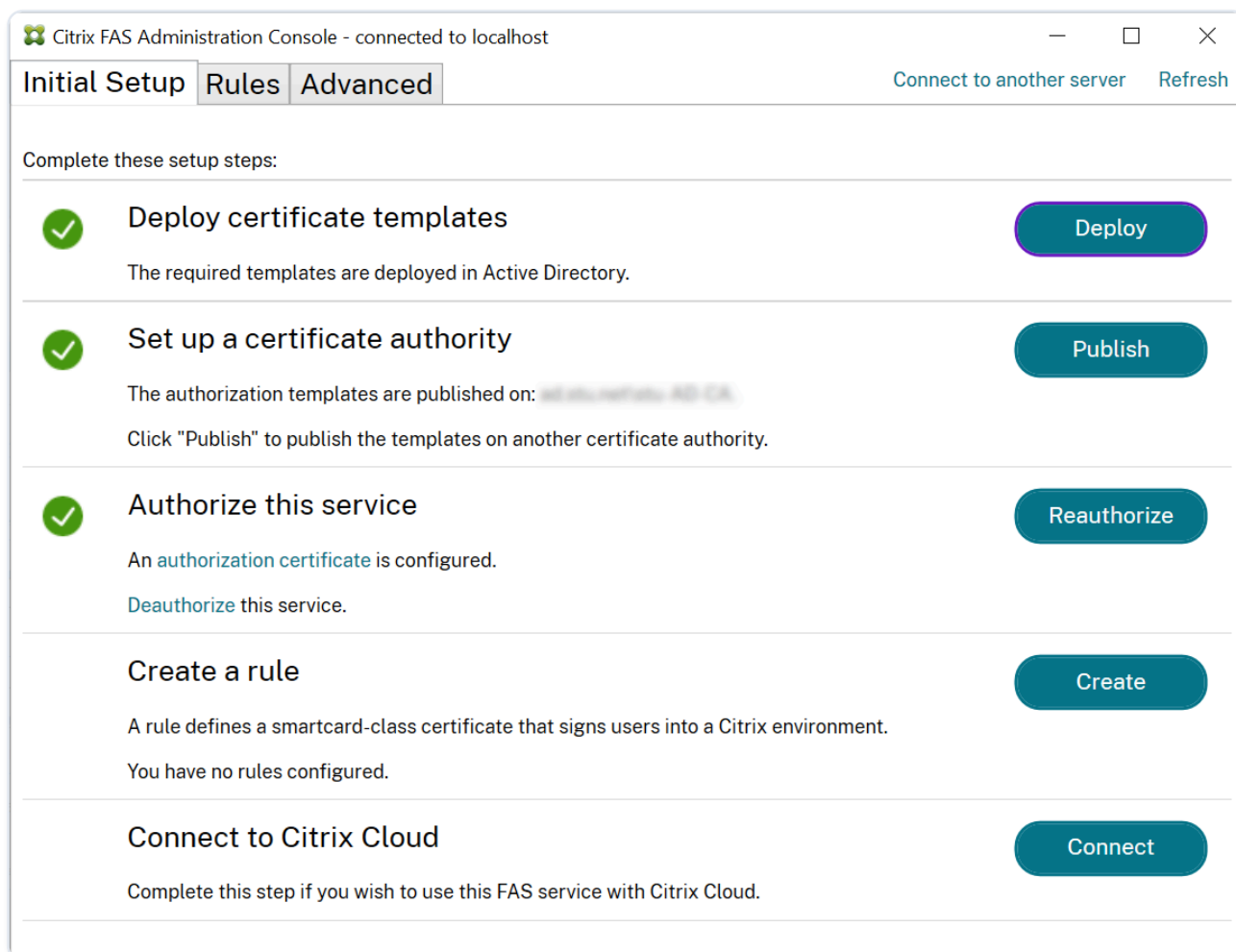
ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-privatekeys-import-fasauthorizationcertificiate-response-display.png)

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

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

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

ステップ12: FAS管理コンソールを閉じてから、再起動します。



注: 「Authorize this service」のステップには緑色のチェックマークが付いています。

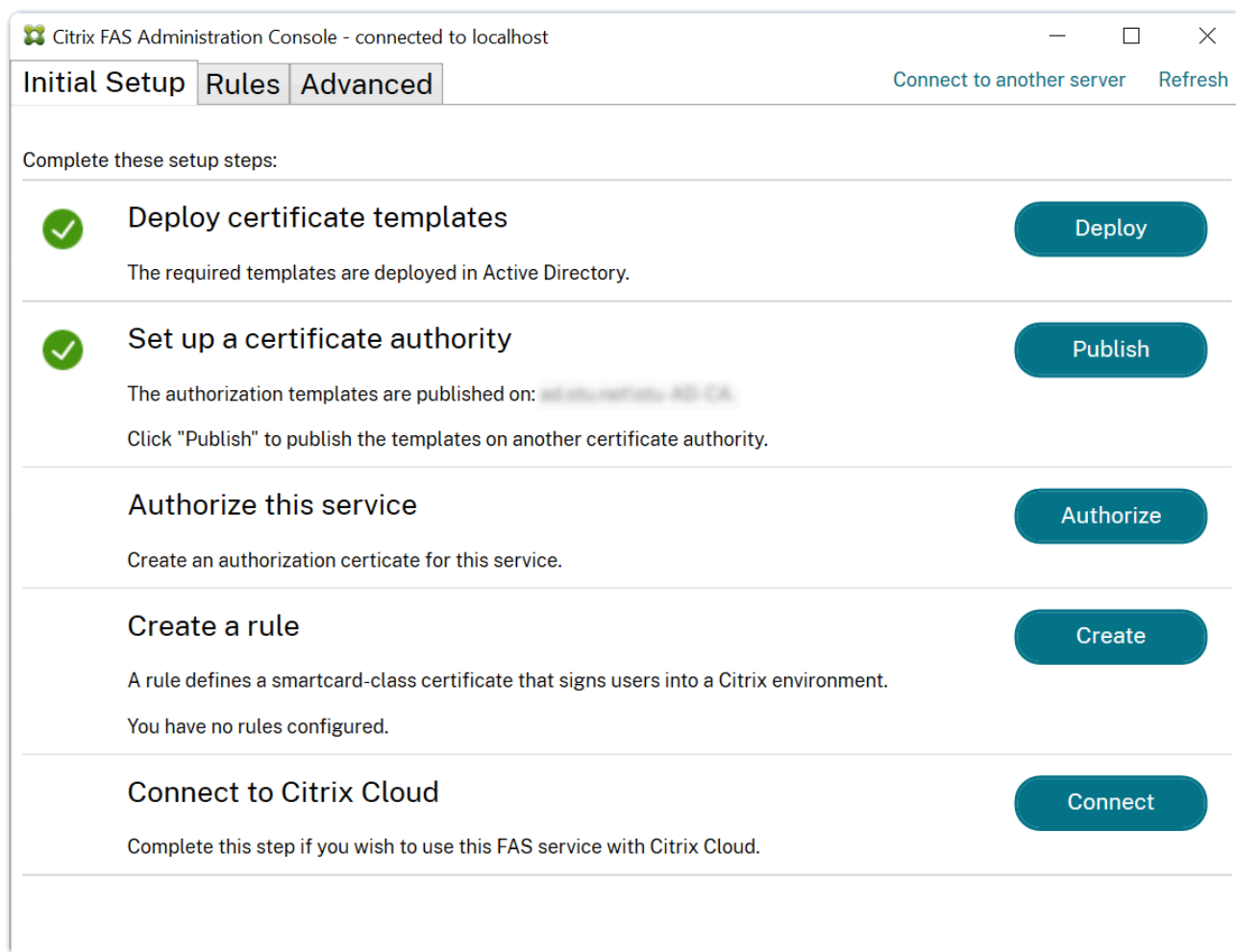
ステップ13: FAS管理コンソールで**Rules**タブを選択し、インストールと構成で説明されている設定を編集します。

例3

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

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

ステップ1. 管理コンソールを使用してFASの初期設定を行う際、「Deploy certificate templates」と「Set up a certificate authority」の最初の2つのステップのみを完了します。



Citrix FAS Administration Console - connected to localhost

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

Complete these setup steps:

-  **Deploy certificate templates** [Deploy](#)
The required templates are deployed in Active Directory.
-  **Set up a certificate authority** [Publish](#)
The authorization templates are published on: `adcs/infopkcs-AD-CA`.
Click "Publish" to publish the templates on another certificate authority.
- Authorize this service** [Authorize](#)
Create an authorization certificate for this service.
- Create a rule** [Create](#)
A rule defines a smartcard-class certificate that signs users into a Citrix environment.
You have no rules configured.
- Connect to Citrix Cloud** [Connect](#)
Complete this step if you wish to use this FAS service with Citrix Cloud.

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

ステップ3: 設定ファイルを次のように編集します。

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

ファイルは次のようになります。

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

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

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

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

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

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

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

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

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

手順4： Citrix Federated Authentication Serviceを再起動して、構成ファイルから値を読み取ります。

手順5： FAS管理コンソールの** [Initial Setup] タブで [Authorize] **をクリックして、HSM内にRSAキーペアを生成し、証明書署名要求を作成します。

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

```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG]
HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

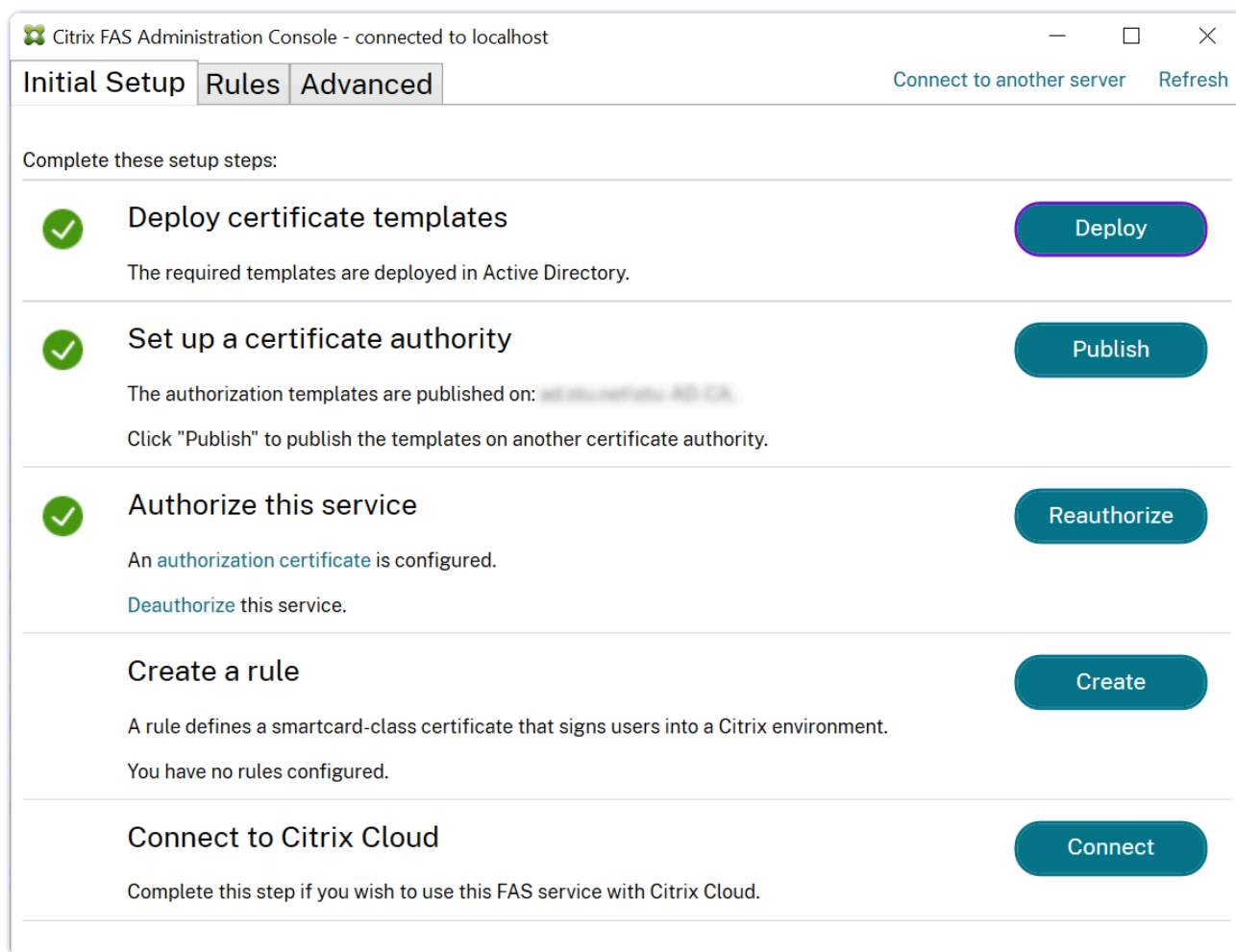
注：[プロバイダー: HSMベンダーのキーストレージプロバイダー]

手順7： 証明機関サーバーで、証明機関MMCの** [Pending Requests] **ノードを選択します。

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
107	-----BEGIN NE...	The operation compl...	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSMS	

要求を右クリックし、** [Issue] **を選択します。

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



手順8：FAS管理コンソールで** [Rules] **タブを選択し、(/ja-jp/federated-authentication-service/2206/install-configure.html)に記載されているように設定を編集します。

FAS証明書ストレージ

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

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

```
Add-pssnapin Citrix.a&ast;
```

```
Get-FasAuthorizationCertificate -address \<FAS server FQDN>
```

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

ユーザー証明書のリストを取得するには、次のように入力します。

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

注:

秘密キーの保存にHSMを使用する場合、HSMコンテナはGUIDで識別されます。HSM内の秘密キーのGUIDは、次を使用して取得できます。

例:

© 1997–2026 Citrix Systems, Inc. All rights reserved. 60

```
PS C:\Users\administrator> Get-FasUserCertificate -Address fas3.djwfas.net -KeyInfo $true

PrivateKeyIdentifier : 38405c4d-63af-43e4-9135-2412246b1112
PrivateKeyProvider   : Microsoft Software Key Storage Provider
PrivateKeyIsCng       : True
ThumbPrint           : AD2441F050A02966AA4DB190BA084976528DB667
UserPrincipalName    : joe@djwfas.net
Role                 : default
CertificateDefinition : default_Definition
SecurityContext       :
ExpiryDate            : 19/01/2018 09:18:48
```

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参照資料です。
- 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

フェデレーション認証サービス (FAS) は、Microsoft Active Directory および Microsoft 証明機関と密接に統合されています。ドメインコントローラーやその他の重要なインフラストラクチャと同様にセキュリティポリシーを策定し、システムが適切に管理され、セキュリティが確保されていることを確認することが不可欠です。

このドキュメントでは、FAS を展開する際に考慮すべきセキュリティ問題の概要を説明します。また、インフラストラクチャの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 の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同様に、セキュリティ上重要なインフラストラクチャの一部として扱われる必要があります。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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-security-network.png)

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。これにより、Citrix Virtual Delivery Agent (VDA) がユーザーをログオンするために必要な、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。証明機関はまた、FAS サーバーが信頼された登録エージェント証明書によって署名された CMC パケットを提供することを要求します。

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

Citrix フェデレーテッド認証サービスとCitrix Cloud™間の接続

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

- ユーザーアカウント下のFAS管理コンソール
 - *.cloud.com
 - *.citrixworkspacesapi.net
 - 環境でサードパーティのIDプロバイダー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

環境にプロキシサーバーが含まれている場合は、FAS管理コンソールのアドレスでユーザープロキシを構成します。また、netshまたは同様のツールを使用して、ネットワークサービスアカウントのアドレスが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は、ドメインユーザーに代わって自律的に証明書を発行できる登録機関証明書を持っています。そのため、FASサーバーを保護し、その権限を制限するためのセキュリティポリシーを策定し、実装することが重要です。

委任された登録エージェント

FASは、登録エージェントとして機能することでユーザー証明書を発行します。Microsoft証明機関では、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/2206/media/delegated-enrollment-agents.png)

この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ること。
- 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ること。
- 権限リストにはFASの使用が許可されているユーザーのみが含まれていること。たとえば、FASが管理者グループまたは保護されたユーザーグループのユーザーに証明書を発行しないようにすることは良い習慣です。

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、証明書が発行される際に、FASにユーザーIDをアサートすることを信頼されているStoreFrontサーバーのリストを構成する必要があります。同様に、どのユーザーに証明書が発行されるか、およびどのVDAマシンに認証できるかを制限できます。この機能は、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経由で相互認証されたWindows Communication Foundation (WCF) Kerberosネットワーク接続を使用します。

イベントログの監視

FASとVDAは、Windowsイベントログに情報を書き込みます。このログは、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。

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

パラメーター	説明
ProviderLegacyCsp	trueに設定すると、FASはMicrosoft CryptoAPI (CAPI)を使用します。それ以外の場合、FASはMicrosoft Cryptography Next Generation API (CNG)を使用します。
ProviderName	使用するCAPIまたはCNGプロバイダーの名前。
ProviderType	Microsoft KeyContainerPermissionAccessEntry.Provider Type プロパティ PROV_RSA_AES 24 を指します。CAPIでHSMを使用しており、HSMベン

パラメーター	説明
	ダーが別途指定している場合を除き、常に24である必要があります。
KeyProtection	秘密鍵の「エクスポート可能」フラグを制御します。また、ハードウェアでサポートされている場合、トラステッドプラットフォームモジュール (TPM) キー ストレージの使用も許可します。
KeyLength	RSA秘密鍵の鍵長。サポートされている値は1024、2048、4096です (デフォルト: 2048)。

管理者の責任

環境の管理は、以下のグループに分けられます。

名前	責任
エンタープライズ管理者	フォレスト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 デスクトップス™ 管理者	VDAとコントローラーを構成する

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

グループポリシー設定

信頼できる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できます。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は、誤った構成を避けるために、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ます。FASサーバーのリストを変更する際は、特にエントリを削除したり並べ替えたりする際には注意してください。

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

証明書テンプレート

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

証明書テンプレートの名前を変更する

Citrix_SmartcardLogon を組織のテンプレート命名標準に合わせて名前を変更したい場合は、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ます。
 - New-FasCertificateDefinitionコマンドを使用して、テンプレートの名前でFASを構成します。

全般プロパティの変更

証明書テンプレートの有効期間を変更できます。

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

要求処理プロパティの変更

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は証明書テンプレートのこれらの設定を無視します。

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

キー構成証明プロパティの変更

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。

置き換えられたテンプレートのプロパティを変更する

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

拡張機能のプロパティを変更する

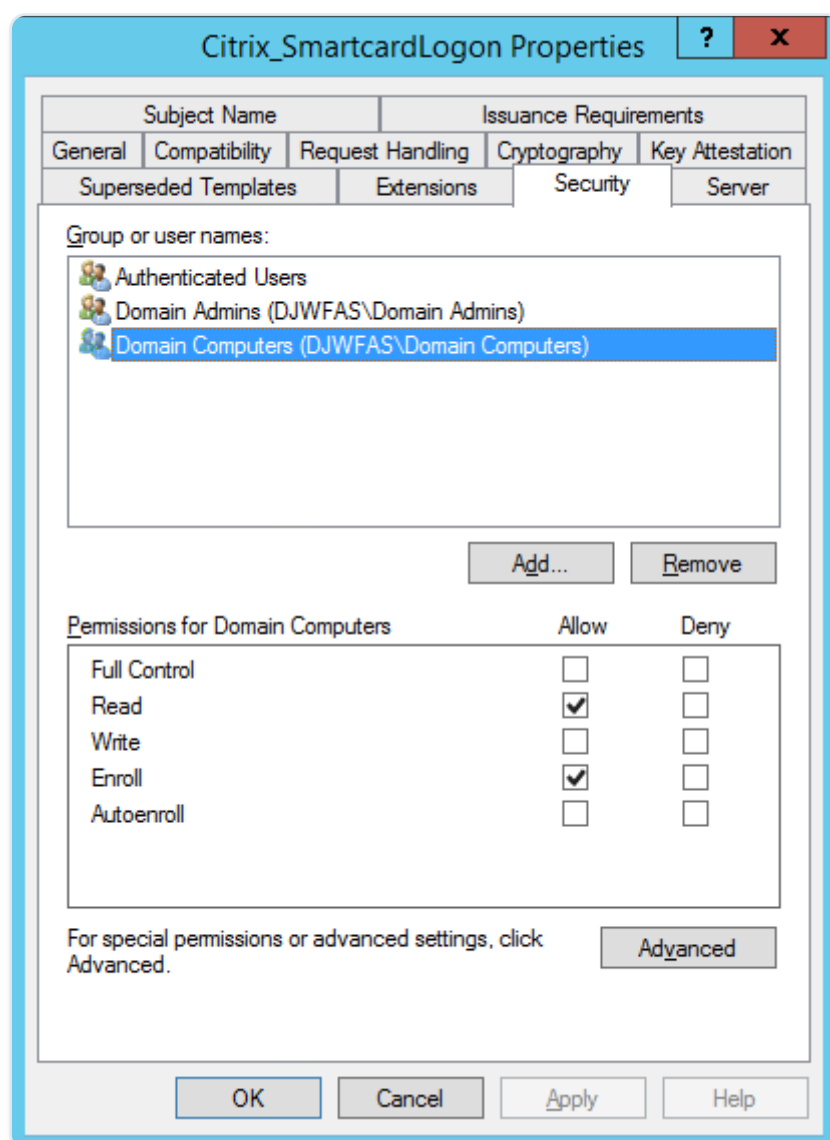
これらの設定は、組織のポリシーに合わせて変更できます。

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

セキュリティのプロパティを変更する

Citrixは、これらの設定を、FASサーバーのマシンアカウントのみに対して読み取りおよび登録のアクセス許可を許可するように変更することを推奨します。FASサービスは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



サブジェクト名のプロパティを変更する

Citrixは、これらのプロパティを変更しないことを推奨します。

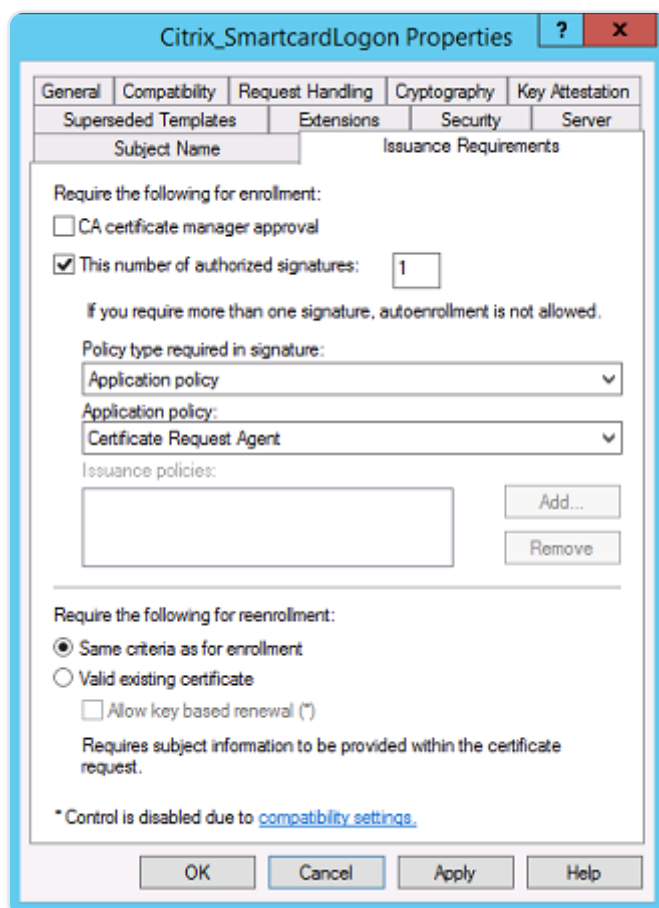
テンプレートには、このActive Directory情報から構築が選択されており、証明機関がユーザーのSIDを証明書拡張機能に含めるようになります。これにより、ユーザーのActive Directoryアカウントへの強力なマッピングが提供されます。

サーバーのプロパティを変更する

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

発行要件プロパティの変更

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表示されるはずです。



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 CA**（スキーマバージョン2）である必要があります。ただし、FASはWindows Server 2008以降のCAのみをサポートします。また、上記で説明したように、FASは**Windows Server 2008 CA**（スキーマバージョン3）または**Windows Server 2012 CA**（スキーマバージョン4）を選択することで利用できる追加設定を無視します。

証明機関の管理

証明機関管理者は、証明機関サーバーの構成と、それが使用する証明書秘密鍵の発行に責任を負います。

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。

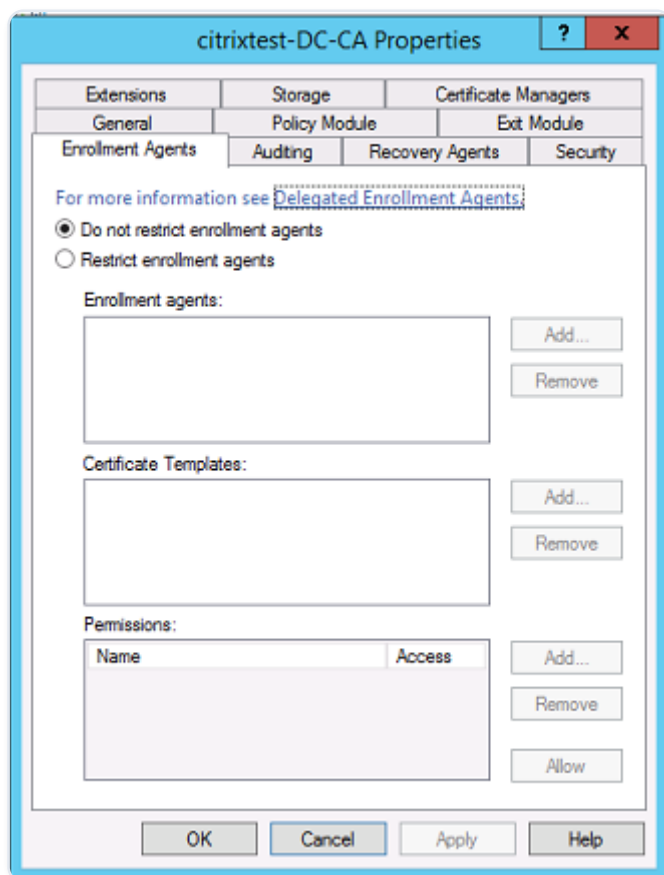
簡単なセキュリティ対策としては、FASサーバーのインストール時に登録機関証明書テンプレートのみを公開するか、完全にオフラインの発行プロセスを徹底することです。いずれの場合も、証明機関管理者は登録機関証明書要求の承認を完全に制御し、FASサーバーを承認するためのポリシーを持つべきです。

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、DCOM TCPおよびファイアウォールルールを構成して、FASサーバーのみが証明書を要求できるようにすることができます。

登録の制限

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



ポリシーモジュールと監査

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

FAS管理

FASにはいくつかのセキュリティ機能があります。

ACLによるStoreFront、ユーザー、およびVDAの制限

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

アクセスベクター	説明
StoreFront [IdP]	これらのKerberosアカウントは、ユーザーが正しく認証されたことを宣言するために信頼されています。これらのアカウントのいずれかが侵害された場合、FASの構成で許可されている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]	これらは、証明書と秘密キーへのアクセスが許可されているマシンです。IdPによって取得された資格情報ハンドルも必要となるため、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によってアサートできるかを制御します。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。この機能により、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のを防ぎます。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を構成する

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権限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セッション内で使用可能であるかどうかを制御できます。たとえば、この機能を使用して、セッション内では「署名」証明書のみを使用可能にし、より強力な「ログオン」証明書はログオン時のみに使用するようになります。

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、セキュリティのために登録機関証明書の秘密鍵をTPMに保存することを推奨します。このオプションは、「オフライン」証明書要求プロセスの一部として提供されます。

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

イベントログ

FASサーバーは、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。これらは監査および侵入検知に使用できます。

管理アクセスと管理ツール

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

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

FASの使用は、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。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です。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。

監査ログとイベントログは、リモートマシンに安全に保存する必要があります。

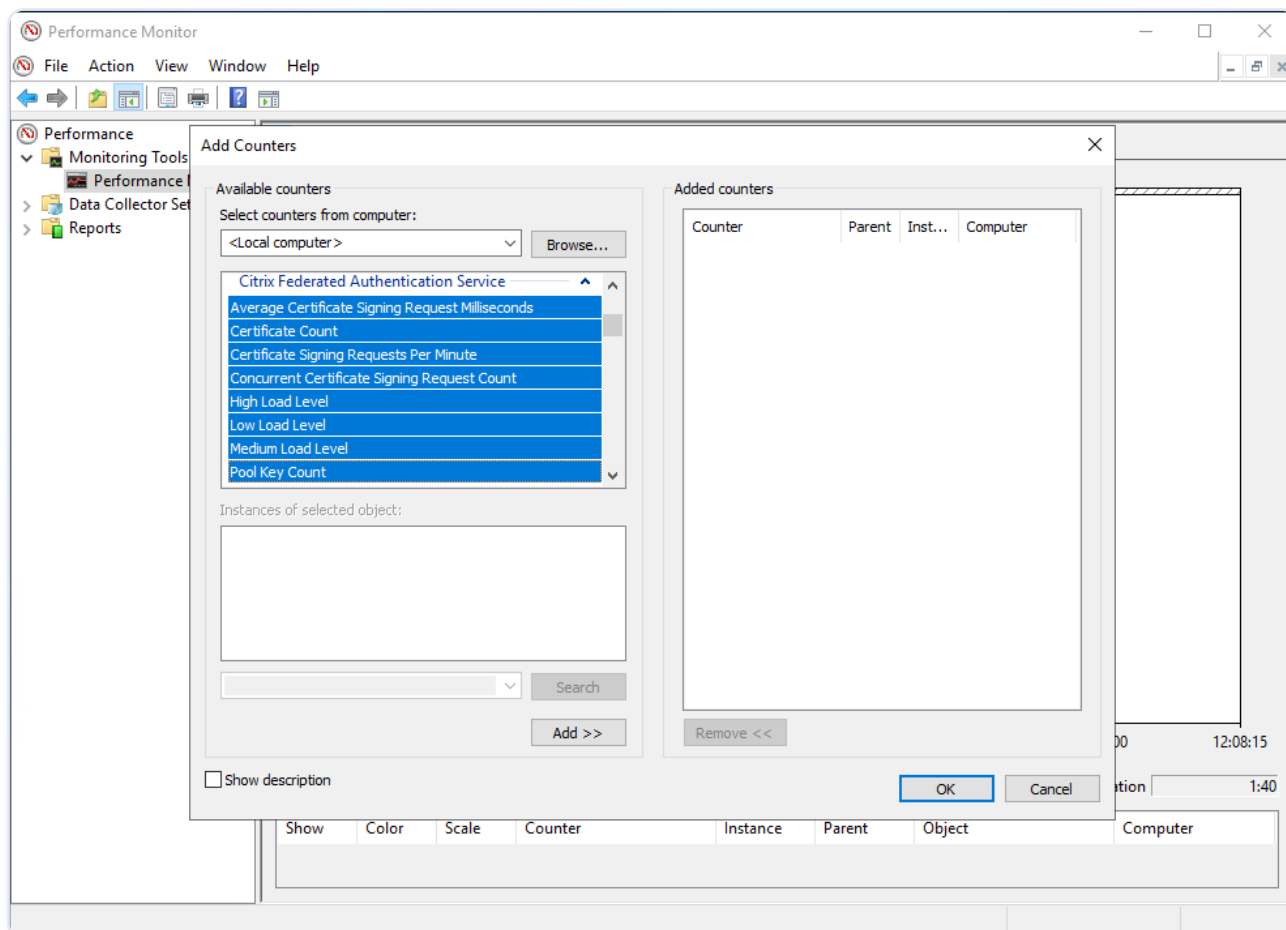
RDPアクセスは、許可された管理者に限定する必要があります。可能な場合は、特に証明機関およびドメイン管理者アカウントの場合、ユーザーアカウントにスマートカードログオンを要求する必要があります。

関連情報

- (</ja-jp/federated-authentication-service/2206/install-configure.html>)は、FASのインストールと構成に関する主要なリファレンスです。
- FASアーキテクチャについては、(</ja-jp/federated-authentication-service/2206/deployment-architectures.html>)の記事で紹介しています。
- その他の「ハウツー」記事については、(</ja-jp/federated-authentication-service/2206/config-manage.html>)の記事で紹介しています。

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）。直前の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。直前の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。この見積もりは、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、ユーザーが証明書やスマートカードを使用してログオンする際に Windows が提供するログとエラーメッセージについて説明します。これらのログは、認証失敗のトラブルシューティング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複数の証明書ストアを保持しています。

- **NTAuth 証明書ストア:** Windows に認証するには、ユーザー証明書を直接発行する証明機関（つまり、チェーンはサポートされていません）は、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ません。そのため、チェーンが使用されている場合、すべて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、そして最後から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	デフォルトでは、Windows は RSA 復号化を許可しない証明書の秘密鍵を除外します。このオプションは、そのフィルターを上書きします。
AllowTimeInvalidCertificates	デフォルトでは、Windows は期限切れの証明書を除外します。このオプションは、そのフィルターを上書きします。
EnumerateECCerts	楕円曲線認証を有効にします。
エクスゴーマルキューヒントズニーデッド	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、または曖昧な可能性がある場合、このオプションを使用すると、ユーザーは手動で Windows ログオンアカウントを指定できます。
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	失効チェックを無効にします（通常、ドメインコントローラーで設定されます）。

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

UPN名と証明書のマッピング

ユーザー証明書には、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。

アクティブディレクトリにおける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。単一のドメインがRootDSEに複数のFQDNアドレスを登録できることに注意してください。

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

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

証明書マッピングサービス

証明書に明示的なUPNが含まれていない場合、Active Directoryには、各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、これによりこの検索が高速化され、この機能をクロスドメイン環境で使用することも可能になります。

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

ログオンドメインコントローラーの選択を制御する

環境に複数のドメインコントローラーが含まれている場合、認証に使用されるドメインコントローラーを確認し、制限することは、ログを有効にして取得できるようにするために役立ちます。

ドメインコントローラーの選択を制御する

Windowsが特定のWindowsドメインコントローラーをログオンに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:mydomaini

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

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

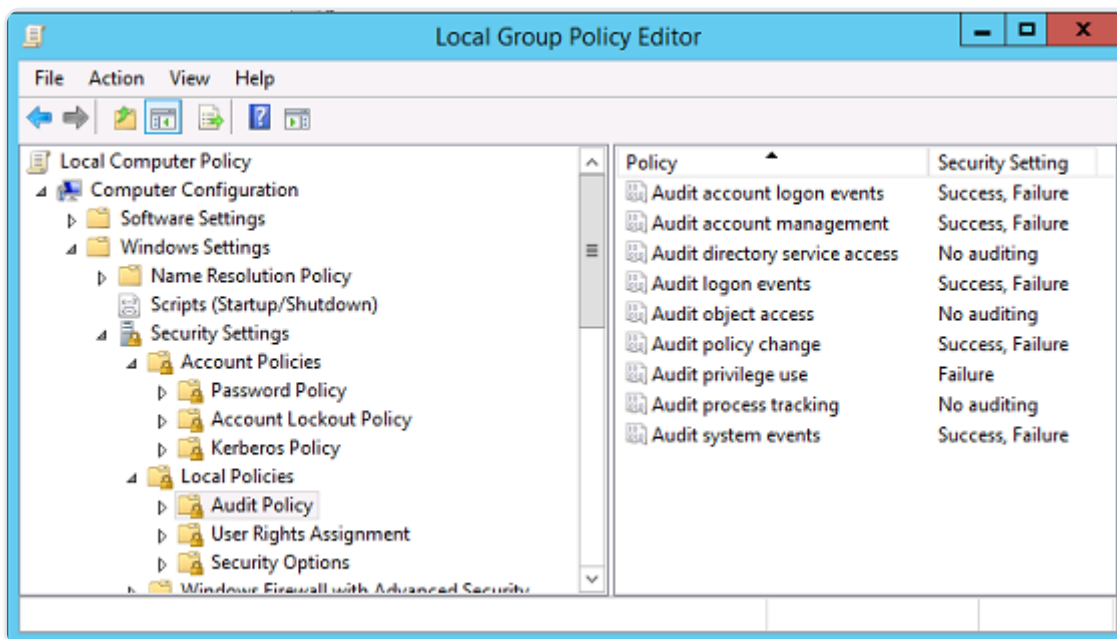
使用中のドメインコントローラーを特定する

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

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

アカウント監査イベントを有効にする

デフォルトでは、Windowsドメインコントローラーは完全なアカウント監査ログを有効にいません。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。これらが有効になると、ドメインコントローラーはセキュリティログファイルに追加のイベントログ情報を生成します。



証明書の検証ログ

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（秘密キーは不要）、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 のログ記録を有効にします。

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

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

CAPI ログ

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

エラーメッセージ

エラーコード	説明
証明書が信頼されていません	スマートカード証明書は、コンピューターの 中間証明書ストアおよび信頼されたルート証 明書ストアにある証明書を使用して構築でき ませんでした。

エラーコード	説明
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。失効チェックが必須の場合、これによりログオンが成功しくなくなります。(//ja-jp/federated-authentication-service/2206/config-manage/troubleshoot-logon.html#certificates-and-public-key-infrastructure)セクションの「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。
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、診断が容易であるはずです。
- 2つのエラーコードは情報提供であり、安全に無視できます。
 - KDC_ERR_PREAUTH_REQUIRED (古いドメインコントローラーとの下位互換性のために使用されます)

- 。 不明なエラー 0x4b

ドメインコントローラーおよび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のセキュリティログ
- 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

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

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

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

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

ドメインコントローラーのセキュリティログ

ドメインコントローラーは一連のログオンイベントを表示します。主要なイベントは 4768 で、証明書が Kerberos チケット保証チケット (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に対して認証を行うために使用されていることを示しています。

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

Event 4768, Security-Auditing

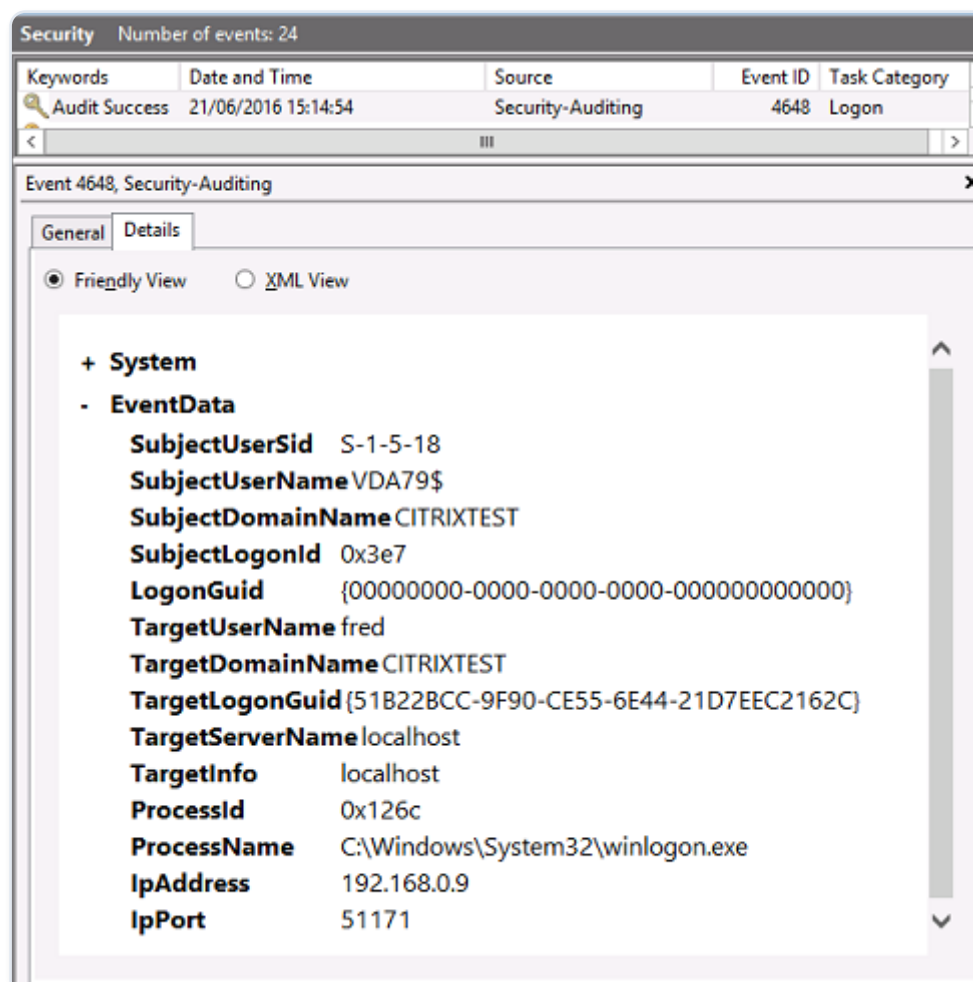
General Details

☒ Friendly View
☐ XML View

+ System
- EventData
 TargetUserName fred
 TargetDomainName CITRIXTEST.NET
 TargetSid S-1-5-21-390731715-1143989709-1377117006-1106
 ServiceName krbtgt
 ServiceSid S-1-5-21-390731715-1143989709-1377117006-502
 TicketOptions 0x40810010
 Status 0x0
 TicketEncryptionType 0x12
 PreAuthType 16
 IpAddress ::ffff:192.168.0.10
 IpPort 49348
 CertIssuerName citrixtest-DC-CA
 CertSerialNumber 5F0001D1FCA2AC30F36879CEEC00000001D1FC
 CertThumbprint 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F

VDA セキュリティログ

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



VDA CAPI ログ

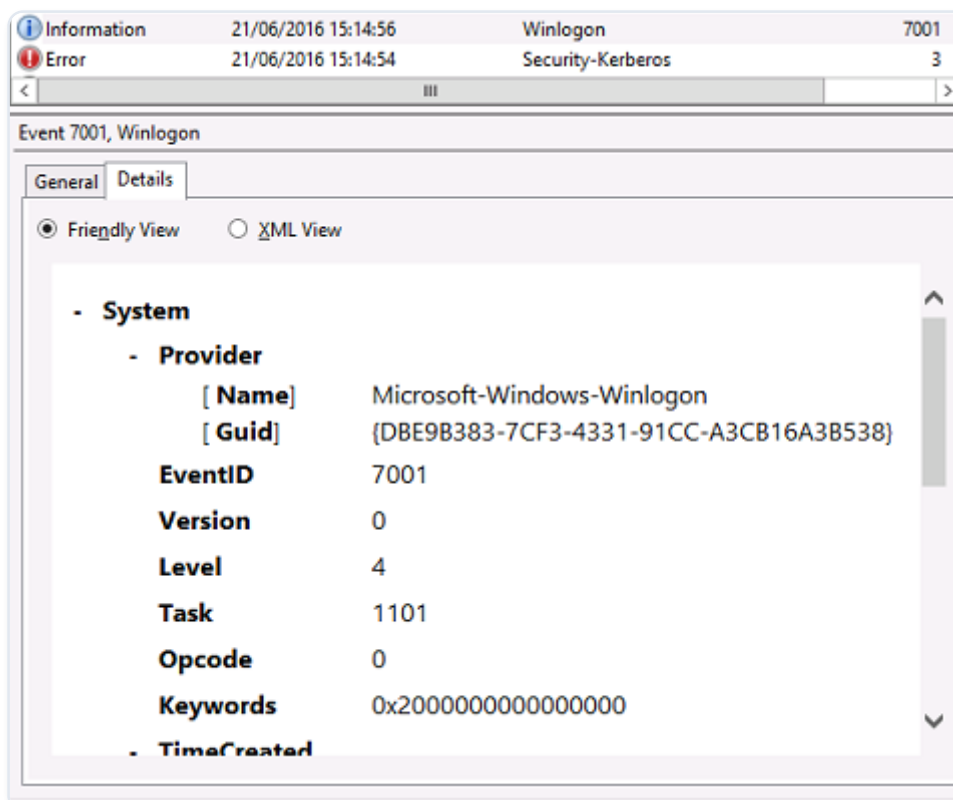
このVDA CAPIログの例は、lsass.exeからの単一のチェーン構築と検証シーケンスを示しており、ドメインコントローラー証明書 (dc.citrixtest.net) を検証しています。

Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain P...
Information	21/06/2016 15:14:54	CAPI2	11	Build Chain
Information	21/06/2016 15:14:54	CAPI2	90	X509 Objects
Information	21/06/2016 15:14:54	CAPI2	41	Verify Revocat...
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocat...
Information	21/06/2016 15:14:54	CAPI2	10	Build Chain

- UserData	
- CertVerifyCertificateChainPolicy	
- Policy	
[type]	CERT_CHAIN_POLICY_NT_AUTH
[constant]	6
- Certificate	
[fileRef]	813C6D12E1E1800E61B8DB071E186EB912B7
[subjectName]	dc.citrixtest.net
- CertificateChain	
[chainRef]	{84E0B3D1-A4D4-4AC7-BA99-5291415B343}
- Flags	
[value]	0
- Status	
[chainIndex]	-1

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



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アプリケーションイベントログに書き込まれます。System Centre 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サービスの健全性を監視できます。

FASサービスは実行中ですか？

FASサービスが実行中かどうかを判断するには、プロセス

Citrix.Authentication.FederatedAuthenticationService.exeを監視します。

FASサービスを監視するための最も重要なイベントのみがこのセクションで説明されています。

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健全性イベント

次のイベントは、FASサービスが健全であるかどうかを示しています。

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	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設定されたか、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 / CVAD 2109 以降で利用可能です。
[S023]	管理者 [{0}] がメンテナンスモードをオンに設定	FASサービスはメンテナンスモードになりました。	FAS 10.7 / CVAD 2109以降で利用可能です。
[S123]	[upn: {0} role: {1}] [exception: {2}]の証明書の発行に失敗しました。	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の発行に成功しなかった場合に、[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。
[S124]	[certificate authority: {2}] [exception: {3}]で	FASが指定されたCAからユーザー証明書	このイベントは、CAが機能していない

イベント	イベントテキスト	説明	注
	[upn: {0} role: {1}]の証明書の発行に失敗しました。	を要求しようとしたときに、エラーが発生しました。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。	か、連絡できない状態である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。
[S413]	認証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認証証明書の有効期限が近づくと定期的に生成されます。デフォルトでは、認証証明書の有効期限が30日以内である場合、イベントは毎日生成されます。	デフォルト設定は、cmdlet Set-FasRaCertificateMonitor 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]	認証証明書の有効期限が切れました。証明書の詳細: {0}	FAS認証証明書の有効期限が切れると、このイベントは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™と連携して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	注記
[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。	このイベントは、FASがWorkspace（つまりCitrix 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。	FASはCitrix Cloudへの永続的な接続を維持します。この接続は、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、さまざまな理由で時々切断されることがあります。この場合、イベントテキストには「Service is not connected to the cloud」と表示されます。これは正常な動作であり、FASは直ちにCitrix Cloudへの接続を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の設定を表示または変更しようとしたましたが、呼び出

イベント	イベントテキスト	説明
		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}] はロール [{1}] の管理者ではありません	FASルールの設定を表示または変更しようとしたが、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ルール構成によりユーザーアカウントは許可されていません。
[S205]	証明書利用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}] の許可された証明書利用者ではありません	VDAがFASでシングルサインオンを実行しようとしたが、FASルール構成によりVDAは許可されていません。

FASイベントログ

次の表に、FASによって生成された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}] は管理者グループのメンバーではありません
[S002] アクセス拒否: ユーザー [{0}] は役割 [{1}] の管理者ではありません

ログコード
[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}] が新しい証明書定義 [{1}] を作成しています
[S007] 管理者 [{0}] が証明書定義 [{1}] を更新しています
[S008] 管理者 [{0}] が証明書定義 [{1}] を削除しています
[S009] 管理者 [{0}] が新しいルール [{1}] を作成しています
[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}][Certificate Definition: {4}] を作成しています [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 [Reference: {1}] をインポートしています
[S022] 管理者 [{0}] がメンテナンスモードをオフに設定
[S023] 管理者 [{0}] がメンテナンスモードをオンに設定
[S024] 管理者 [{0}] がシステムヘルスマニターを設定
[S025] 管理者 [{0}] がシステムヘルスマニターを設定
[S026] 管理者 [{0}] がRA証明書モニターを設定
[S027] 管理者 [{0}] がRA証明書モニターをリセット
[S050] 管理者 [{0}] が新しいクラウド構成を作成: [{1}]

ログコード
[S051] 管理者 [{0}] がクラウド構成を更新: [{1}]
[S052] 管理者 [{0}] がクラウド構成を削除
[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}] がダイレクトトラストクラウド登録を要求しています。インスタンス: {1} CloudServiceUrlFormat: {2}
[S061] 管理者 [{0}] が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}] がクラウド登録を完了しました。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} でした。
[S063] [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} でした。

ログコード
[S401] 構成アップグレードを実行中 -- [バージョン {0} から][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 -- [バージョン {0} から][to version {1}]
[S409] ThreadPool の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

ログコード
[S410] ThreadPool の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 サービスの開始中にエラーが発生しました: [{0}]
[S412] 構成アップグレードが完了しました -- [バージョン {0} から][to version {1}]
[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}
[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] 承認証明書の確認が完了しました。{0} 件の問題がログに記録されました。次回の確認は {1} 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}] をアサートできませんでした (例外: {2}{3})
[S103] サーバー [{0}] はUPN [{1}] SID {2} を要求しましたが、ルックアップはSID {3} を返しました
[S104] サーバー [{0}] はUPN [{1}] をアサートできませんでした (UPNはロール [{2}] 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}, role {2}, Security Context: [{3}]]
[S120] 証明書を発行中 [upn: {0} role: {1} Security Context: [{2}]]
[S121] 証明書は [certifcate authority: {2}] によって [upn: {0} role: {1}] に発行されました
[S122] 警告: サーバーが過負荷です [upn: {0} role: {1}][1分あたりのリクエスト数 {2}]。
[S123] [upn: {0} role: {1}] [exception: {2}] の証明書の発行に失敗しました

ログコード

[S124] [upn: {0} role: {1}] の証明書を [certificate authority: {2}] [exception: {3}] で発行できませんでした

証明書利用者として機能する

VDAがユーザーをログオンさせるときに、これらのイベントが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CSPにアクセスできません。

[S204] 証明書利用者 [{0}] が、[{4}] によって承認されたロール: [{2}] [Operation: {3}] で [upn: {1}] のログオンCSPにアクセスしています。

[S205] 証明書利用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] 秘密キー操作が失敗しました [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}][Error {4} {5}]。

セッション内証明書サーバー

ユーザーがセッション内証明書を使用するとき、これらのイベントが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にアクセスできません。

[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}] が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}] 上でプログラム [{1}] を実行しており、秘密鍵操作 [{6}] に仮想スマートカード [upn: {3} role: {4} thumbprint: {5}] を使用しています
[S305] 秘密鍵操作が失敗しました [Operation: {0}][upn: {1} role: {2} containerName {3}][Error {4} {5}]。

FASアサーションプラグイン

これらのイベントはFASアサーションプラグインによってログに記録されます。

ログコード
[S500] FASアサーションプラグインが構成されていません
[S501] 構成されたFASアサーションプラグインをロードできませんでした [exception:{0}]
[S502] FASアサーションプラグインがロードされました [pluginId={0}] [assembly={1}] [location={2}]
[S503] サーバー [{0}] が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}] が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}] がUPN [{1}] のアサートに失敗しました（プラグイン [{2}] が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}] がサーバー [{1}] からUPN [{2}] のログオン証拠をメッセージ [{3}] で受け入れました
[S507] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (プラグイン [{2}] がメソッド [{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}] が例外 [{3}] をスローしました)
[S508] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (アクセス処理が提供されましたが、プラグイン [{2}] はそれをサポートしていません)

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 (アクセス処理が提供されましたが、構成された FAS プラグインがありません)
[S510] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (アクセス処理はプラグイン [{2}] によって無効と見なされました)

Workspace 対応 FAS

これらのイベントは、FAS が Workspace と連携して使用されるとき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に接続されています: {0}
[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}] 詳細は管理コンソールで確認できます
[S014] クラウドサービスへの呼び出しが失敗しました <service name> [fas id: {0}] [transaction id: {1}] [exception: {2}]

ログコード
[S015] 発信者が許可されていないため、Citrix Cloudからのメッセージがブロックされました [message ID {0}] [transaction ID {1}] [caller {2}]
[S016] クラウドサービスへの呼び出しが成功しました <service name> [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がクラウドからの構成のダウンロードに失敗しました [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}]

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}]
[S102] IDアサーションログオンに失敗しました。{0}のSIDを検索できませんでした [Exception: {1}] {2}]
[S103] IDアサーションログオンに失敗しました。ユーザー{0}のSIDは{1}ですが、期待されるSIDは{2}です

ログコード
[S104] IDアサーションログオンに失敗しました。フェデレーション認証サービスへの接続に失敗しました: {0} [Error: {1} {2}]
[S105] IDアサーションログオン。[ユーザー名: {0}]でログオンしています[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。ACCESS_DENIED [Caller: {0}]

セッション内証明書

これらのイベントは、ユーザーがセッション内証明書の使用を試みたときにVDAにログ記録されます。

ログコード
[S201] 仮想スマートカードアクセスが [{0}] によって [PID: {1}] プログラム名: {2}] のために承認されました [Certificate thumbprint: {3}]
[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。スマートカードサポートが無効になっています

証明書要求とキーペア生成

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

ログコード
[S001] TrustArea::TrustArea: インストールされた証明書 [TrustArea: {0}] [Certificate {1}] [TrustAreaJoinParameters{2}]
[S014] Pkcs10Request::Create: PKCS10要求が作成されました [Distinguished Name {0}]
[S016] PrivateKey::Create [識別子 {0}][マシン全体: {1}][プロバイダー: {2}][プロバイダータイプ: {3}] [楕円曲線: {4}][キー長: {5}][isExportable: {6}]
[S017] プライベートキー::デリート [CspName: {0}, Identifier {1}]

ログコード
[S104] MicrosoftCertificateAuthority::GetCredentials: {0} を使用する権限があります
[S105] MicrosoftCertificateAuthority::SubmitCertificateRequest エラー応答の送信 [{0}]
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest 証明書の発行 [{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。資格情報を検証できませんでした。 / 要求はサポートされていません	ドメインコントローラーに接続できないか、ドメインコントローラーがスマートカード認証をサポートする証明書で構成されていません。「 Kerberos 認証 」、「 ドメインコントローラー 認証 」、または「 ドメインコントローラー 」証明書のためにドメインコントローラーを登録してください。既存の証明書が有効に見える場合でも、これは通常試す価値があります。
システムはログオンできませんでした。認証に使用されたスマートカード証明書は信頼されていませんでした。	中間証明書とルート証明書がローカルコンピューターにインストールされていません。 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、またはRSAキーが短すぎる（<2048ビット）ことを示します。

関連情報

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

PowerShell コマンドレット

シンプルな展開には、フェデレーション認証サービス (FAS) 管理コンソールを使用できます。ただし、PowerShellインターフェイスにはより高度なオプションが用意されています。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では構成にPowerShellのみを使用することをお勧めします。

次のコマンドは、FAS PowerShellコマンドレットを追加します。

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

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

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

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、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する Citrix® コンポーネントです。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用意されており、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™ 展開へのログオ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、トップレベルの展開アーキテクチャの例を、複雑さが増す順に説明します。

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

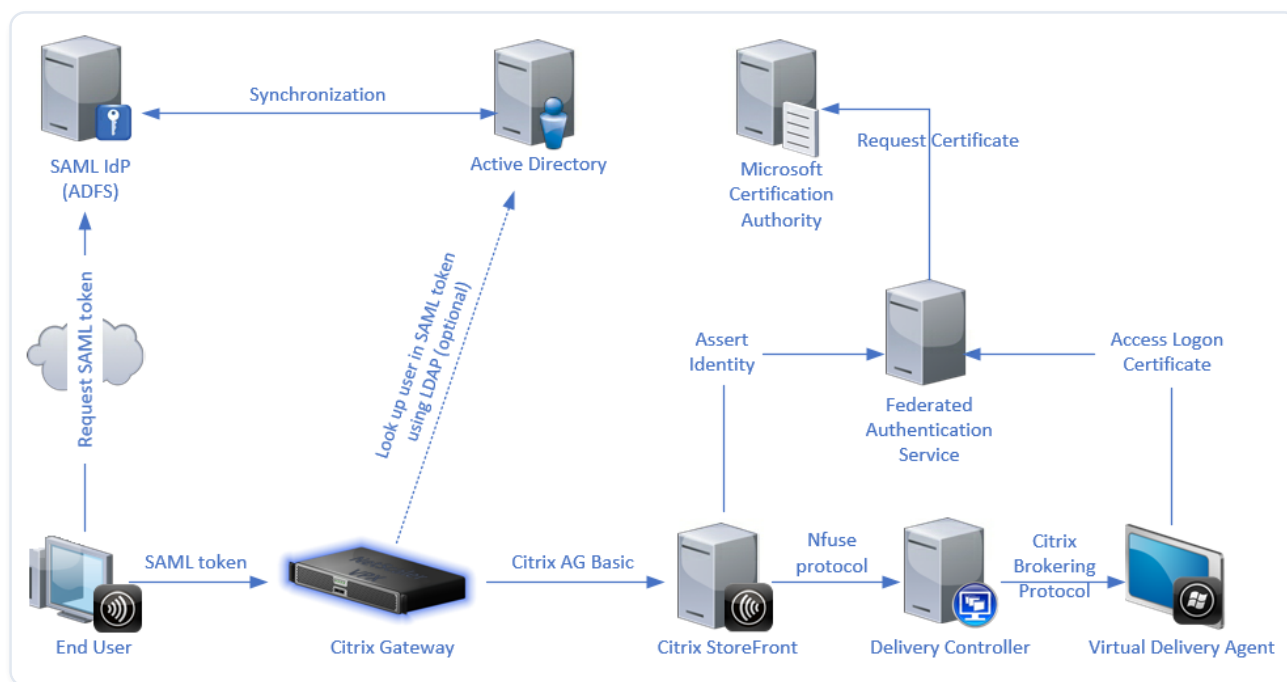
関連する FAS 記事へのリンクが提供されています。すべてのアーキテクチャについて、[インストールと構成](#) 記事は FAS のセットアップに関する主要なリファレンスです。

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の証明書を自動的に発行することを承認されています。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。

ユーザーが Citrix 環境へのアクセスを要求すると、信頼された StoreFront™ サーバーは FAS に接続します。FAS は、そのセッションの証明書を使用して単一の Citrix Virtual Apps または Citrix Virtual Desktops セッションが認証できるようにするチケットを付与します。VDA がユーザーを認証する必要がある場合、FAS に接続してチケットを引き換えます。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ことを示しています。



内部展開

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

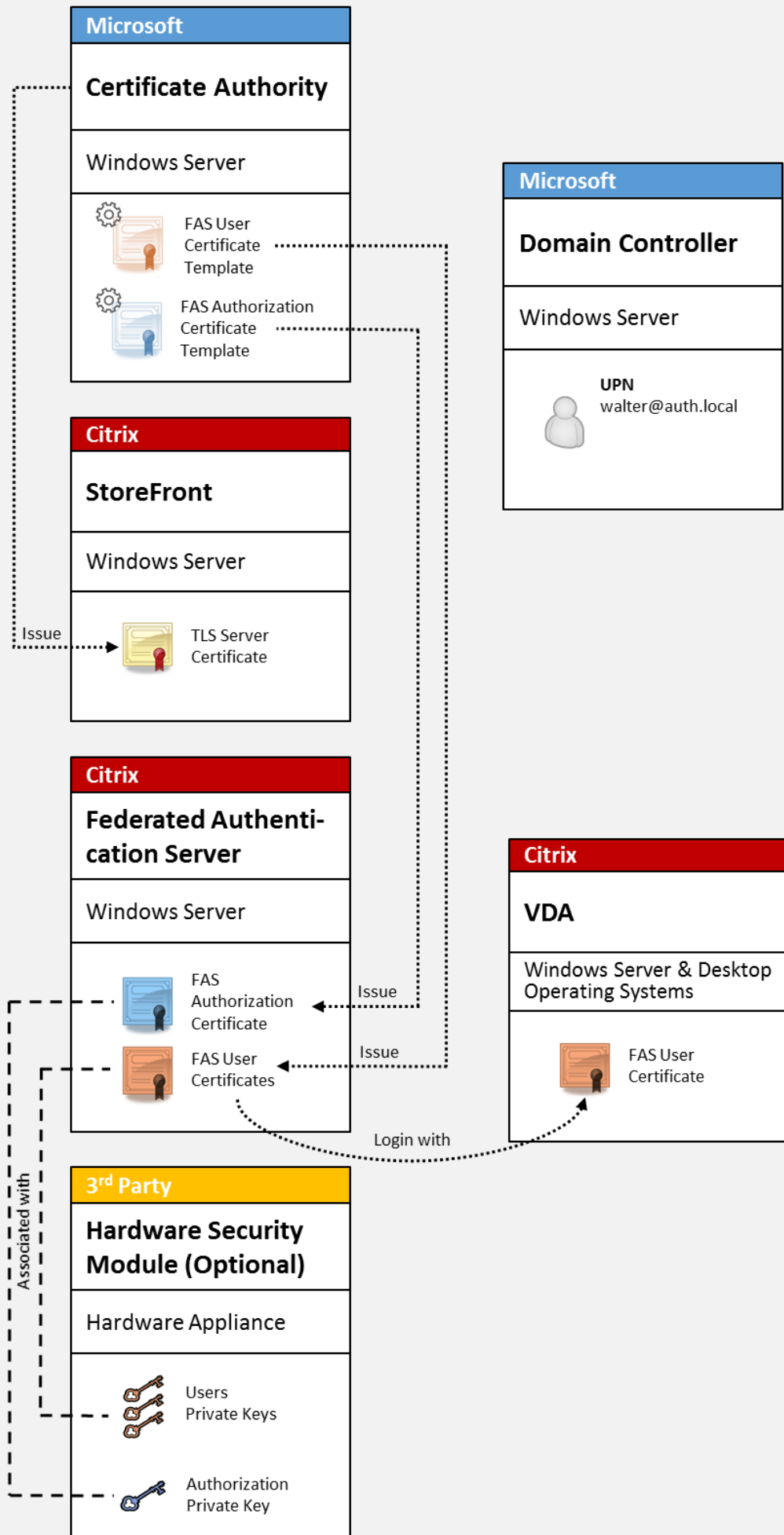
これにより、ユーザー資格情報やスマートカードPINの入力を求めるプロンプトなしでWindows認証が可能になり、シングルサインオンサービスなどの「保存されたパスワード管理」機能を使用する必要もありません。これは、以前のバージョンのCitrix Virtual Appsで利用可能だった Kerberos Constrained Delegationログオン機能を置き換えるために使用できます。

すべてのユーザーは、スマートカードを使用してエンドポイントデバイスにログオンしているかどうかにかかわらず、セッション内で公開鍵インフラストラクチャ（PKI）証明書にアクセスできま

す。これにより、スマートカードリーダーを持たないスマートフォンやタブレットなどのデバイスからでも、二要素認証モデルへのスムーズな移行が可能になります。

この展開では、FASを実行する新しいサーバーが追加され、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の証明書を発行することを承認されています。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。

AUTH.LOCAL domain



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

既存の展開では、通常、ドメイン参加済みのMicrosoft証明機関が利用可能であり、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が追加され、認証の主要なポイントがCitrix Gateway自体に移動します。Citrix Gatewayには、企業のWebサイトへのリモートアクセスを保護するために使用できる高度な認証および承認オプションが含まれています。

この展開は、最初にCitrix Gatewayに認証し、次にユーザーセッションにログオンする際に発生する複数のPINプロンプトを回避するために使用できます。また、ADパスワードやスマートカードを別途要求することなく、高度なCitrix Gateway認証テクノロジーを使用することも可能です。

ローカライズされた画像(/en-us/federated-authentication-service/2206/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、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、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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-architectures-netscaler-auth-settings.png)

関連情報:

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

ADFS SAML 展開

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

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-architectures-adfs-saml.png)

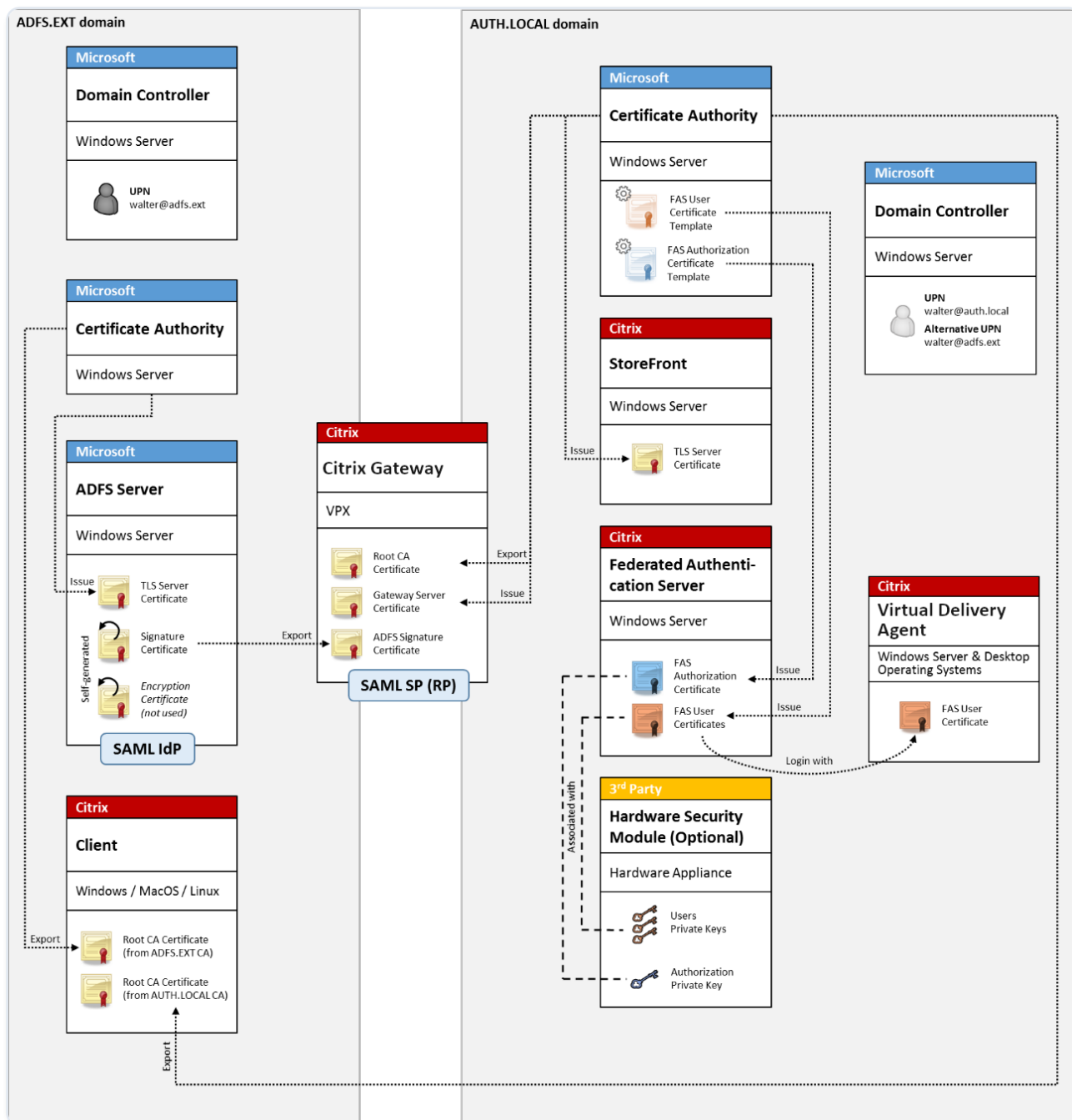
ADFS は、インターネット経由でリモートから企業リソースにユーザーを安全に認証するためによく使用されます。たとえば、Office 365 との統合によく使用されます。

関連情報:

- [ADFS 展開](#)の記事に詳細が記載されています。
- [インストールと構成](#)の記事では、FAS のインストールと構成方法について説明しています。
- このアートの [Citrix Gateway 展開](#) 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、各ユーザーは自身の会社のログオン資格情報を使用します。ADFSはこれをピア会社のAD環境の「シャドウアカウント」に自動的にマッピングします。



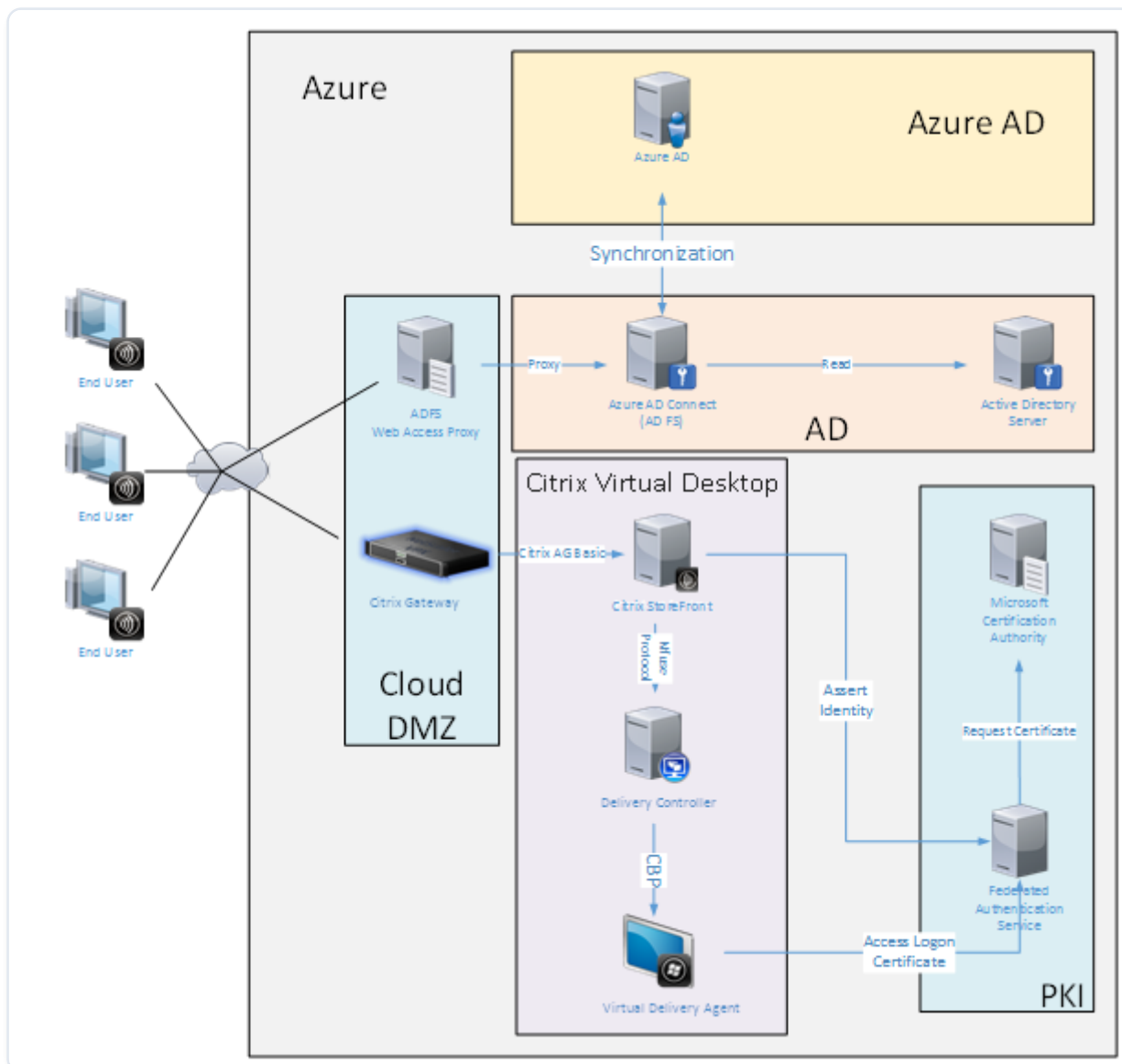
関連情報:

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

ウィンドウズ 10 アジュール AD 参加

Windows 10では、「Azure AD参加」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ます。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、簡素化のためにAzure VMを使用しています。

関連情報:

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

- [Azure AD統合](#)の記事には詳細が記載されています。

ADFSの展開

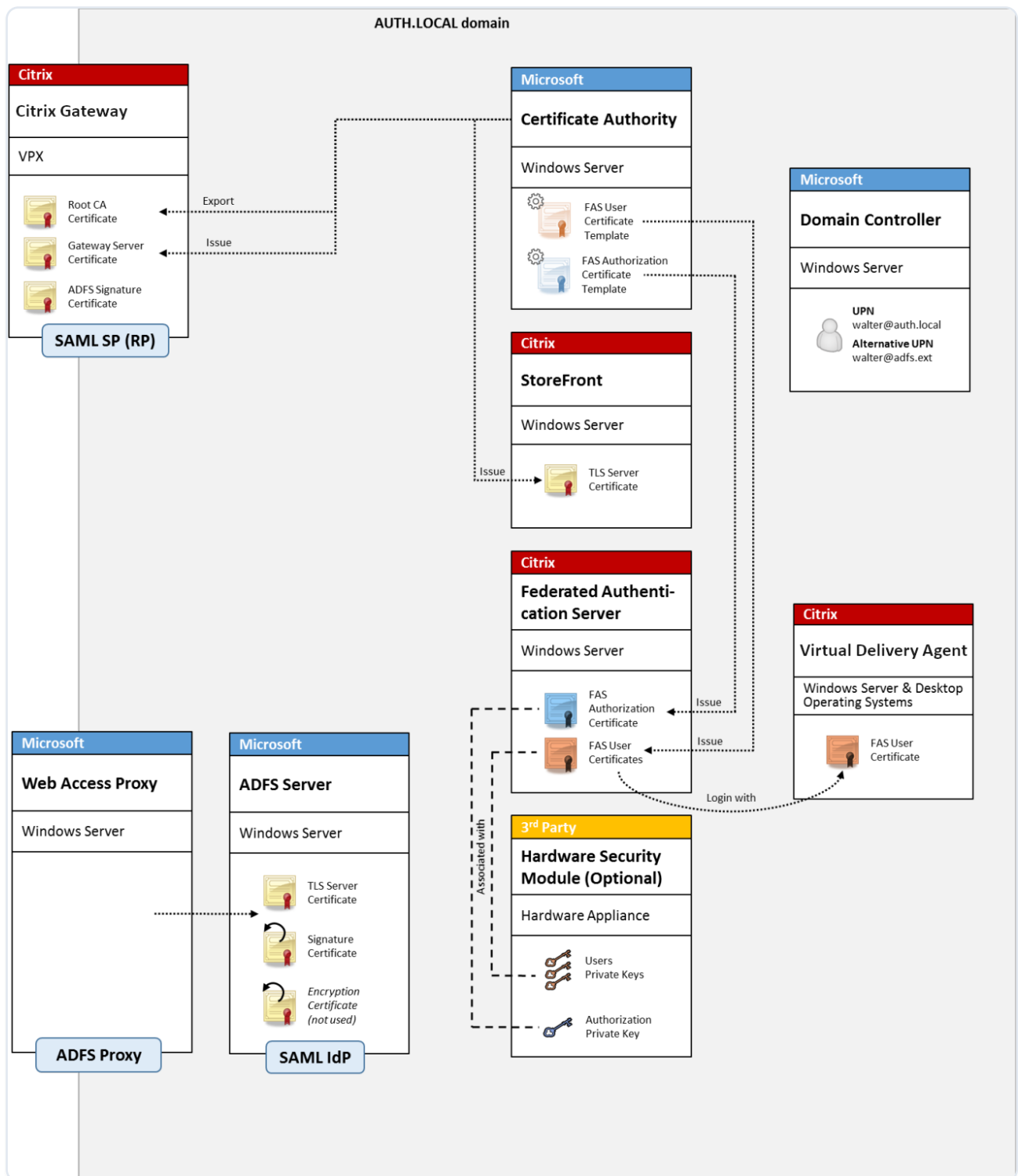
はじめに

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、単一の認証ポイントを必要とするWebサイトへの安全なユーザーアクセスを管理するためにADFSを使用しています。たとえば、企業が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、それらの場所は標準のWindowsログオン資格情報で保護する必要があります。

Federated Authentication Service (FAS) を使用すると、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でき、会社のスタッフの混乱を軽減できます。

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



注：

バックエンドリソースがWindows VDAであろうとLinux VDAであろうと、違いはありません。

SAMLの概要

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

リダイレクトURL

Citrix Gateway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ページにHTTP POSTを実行するように指示します。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、ログオン完了時にADFSがユーザーを返す「戻りアドレス」を含むその他の情報が含まれます。

識別子

EntityIdは、Citrix GatewayがADFSへのPOSTデータに含める一意の識別子です。これにより、ADFSはユーザーがどのサービスにログオンしようとしているのかを認識し、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によって識別されるサービスへのログオンにのみ適しています。

通常、EntityIdはCitrix GatewayサーバーのログオンページのURLですが、Citrix GatewayとADFSが合意していれば、一般的には何でも構いません。 `https://ns.mycompany.com/application/logonpage`。

戻りアドレス

認証が成功すると、ADFSはユーザーのWebブラウザに対し、EntityId用に構成されているリプライURLのいずれかにSAML認証XMLをPOSTするよう指示します。これは通常、元のCitrix Gatewayサーバー上の `https://` アドレスで、形式は次のとおりです。 `https://ns.mycompany.com/cgi/samlauth`。

複数のリプライ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。

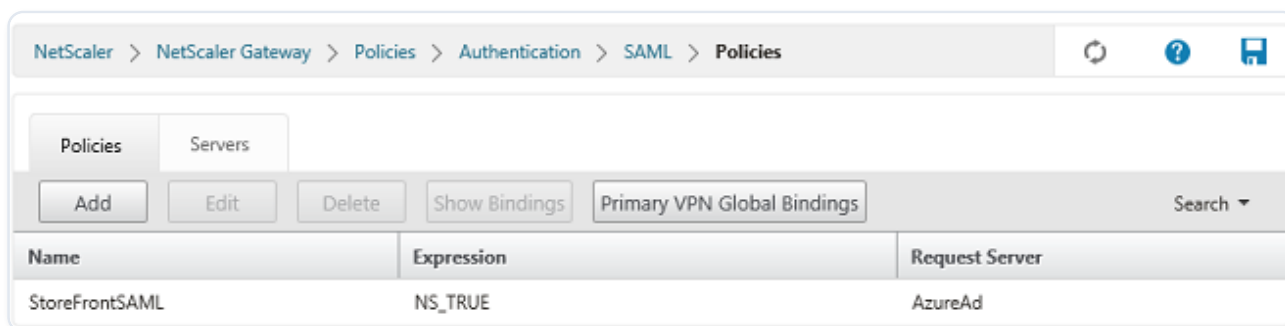
シングルサインアウトURL

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SAML認証XMLプロブが現在ログオン中のセッションをまだ表しているかどうかを確認するために、時々ポーリングするURLです。

これは構成する必要のないオプション機能です。通常、`https://` アドレスで、形式は `https://adfs.mycompany.com/adfs/logout` です。（シングルログオンURLと同じにすることも可能です。）

構成

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



SAMLポリシーの入力

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

Create Authentication SAML Server

Create Authentication SAML Server

Name*
AzureAd

Authentication Type
SAML

IDP Certificate Name*
AzureADSAML

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

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

User Field
userprincipalname

Signing Certificate Name

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

Reject Unsigned Assertion*
ON

SAML Binding*
POST

Default Authentication Group

Skew Time(mins)
5

5

Two Factor
☐ ON ☒ OFF

Assertion Consumer Service Index
255

Attribute Consuming Service Index
255

Requested Authentication Context*
Exact

Authentication Class Types
InternetProtocol
InternetProtocolPassword

Signature Algorithm*
☐ RSA-SHA1 ☒ RSA-SHA256

Digest Method*
☐ SHA1 ☒ SHA256

☐ Send Thumbprint
☒ Enforce Username

Attribute 1
Attri

Attribute 3
Attri

Attribute 5
Attri

Attribute 7
Attri

関連情報

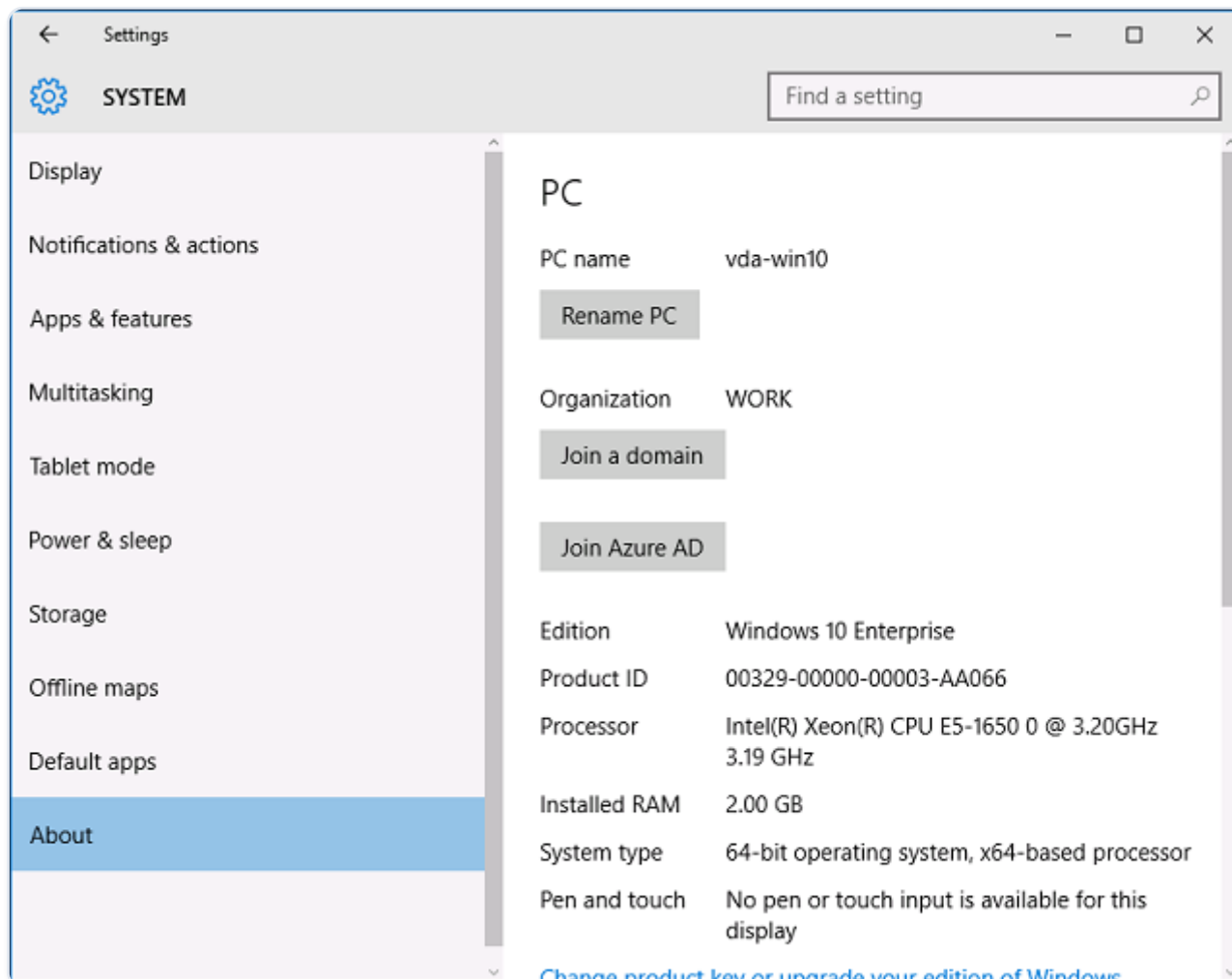
- [インストールと構成](#) は、FASのインストールと構成に関する主要な参照情報です。
- 一般的なFASの展開は、[展開アーキテクチャ](#) の記事にまとめられています。
- 「ハウツー」記事は、[高度な構成](#) の記事で紹介されています。

Azure AD 統合

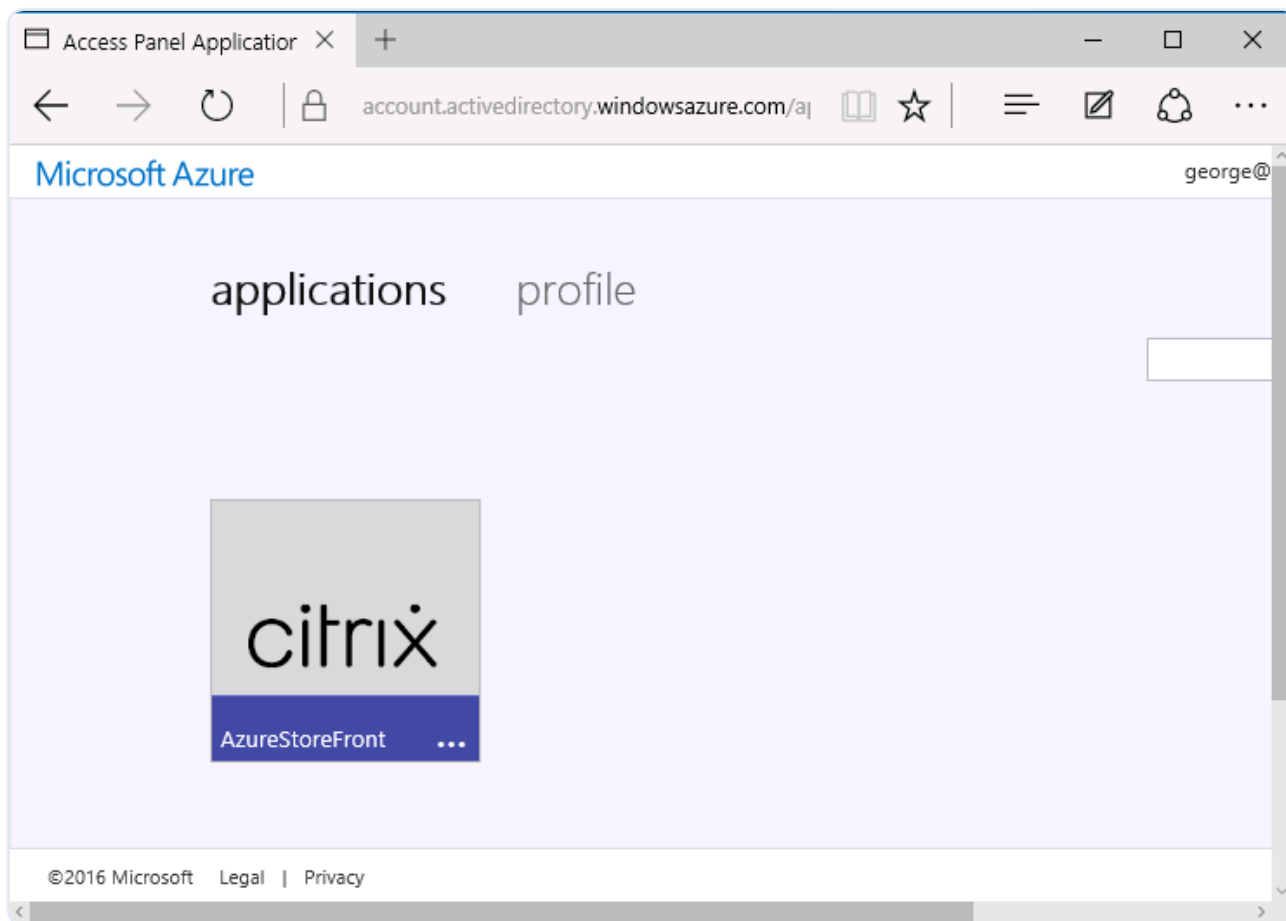
はじめに

このドキュメントでは、Citrix環境をWindows 10 Azure AD機能と統合する方法について説明します。Windows 10ではAzure ADが導入されました。これは、ローミング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、管理とシングルサインオンを目的とす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、個人のWindows 10ラップトップ用の登録コードを提供するシステムについて説明します。ユーザーは、設定パネルのシステム > バージョン情報 > Azure ADに参加オプションからこのコードにアクセスします。



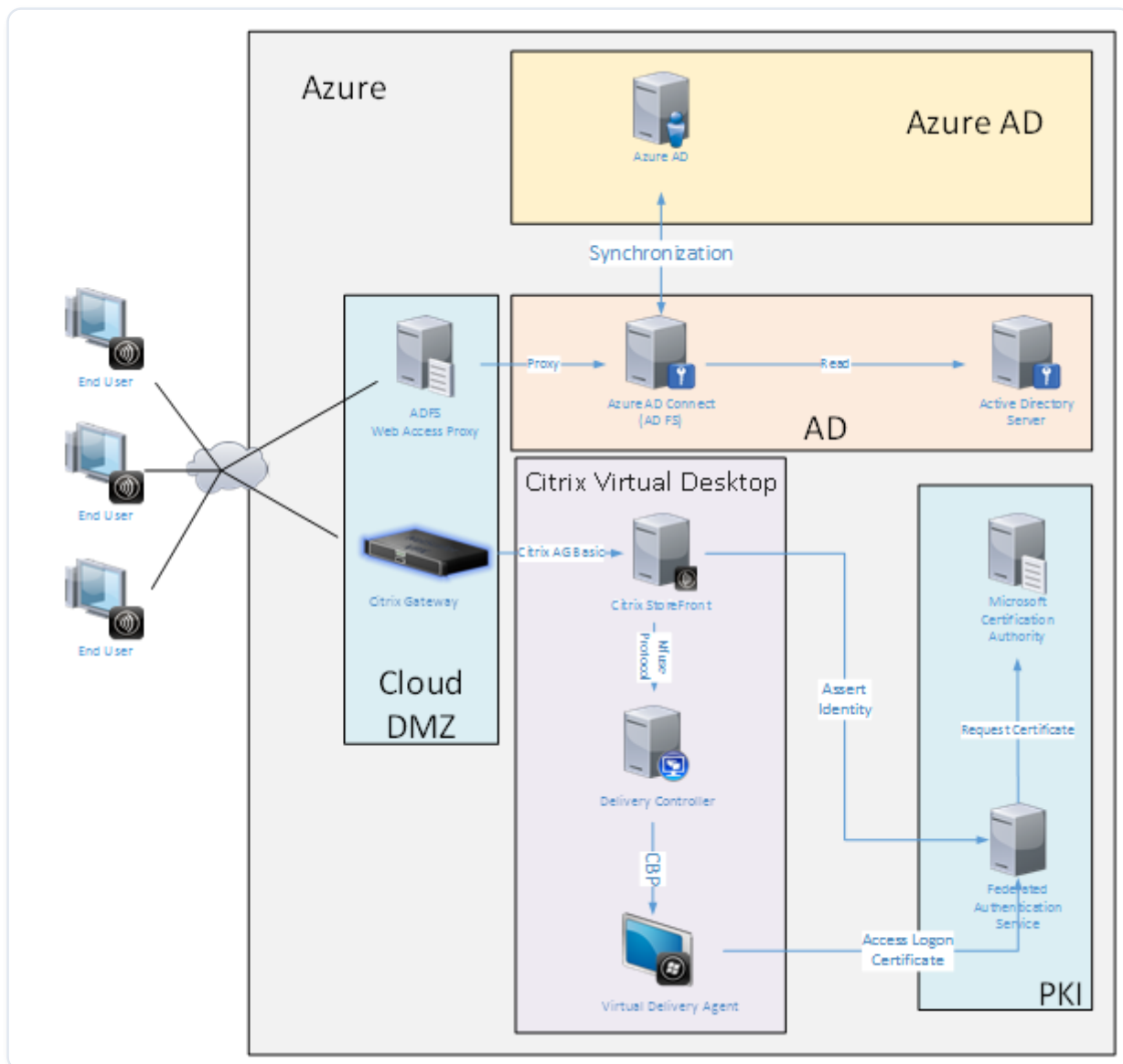
ラップトップが登録されると、Microsoft Edge Webブラウザは、Azure SaaSアプリケーションWebページを介して、会社のWebサイトやCitrix公開アプリケーションに自動的にサインオンします。これには、Office 365などの他のAzureアプリケーションも含まれます。



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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-create-dns-zone.png)

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。

クラウドサービスの作成

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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-create-cloud-svc.png)

Windows仮想マシンの作成

クラウドサービスで実行される5つのWindows VMを作成します。

- ドメインコントローラー (domaincontrol)
- アジュール コネクト ADFS サーバー (adfs)
- ADFS Webアクセスプロキシ (Web Application Proxy、ドメイン参加なし)
- Citrix Virtual Apps and Desktops デリバリーコントローラー
- シトリックス仮想アプリおよびデスクトップ 仮想デリバリーエージェント (VDA)

Microsoft Azure

Create virtual machine > Basics

Create virtual machine

Basics

1 Basics
Configure basic settings

2 Size
Choose virtual machine size

3 Settings
Configure optional features

4 Summary
Windows Server 2012 R2 Datacenter

* Name

* User name

* Password

Subscription
Visual Studio Professional with MSDN

* Resource group
citrixsamldemo

Location
West Europe

OK

ドメインコントローラー

- 標準のActive Directory展開（この例ではcitrixsamldemo.net）を作成するには、**DNSサーバー**と**Active Directory Domain Services**の役割を追加します。ドメイン昇格が完了したら、**Active Directory Certification Services**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 Application Proxyサーバー

- ADFSサーバーをcitrixsamldemoドメインに参加させます。Web Application Proxy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。

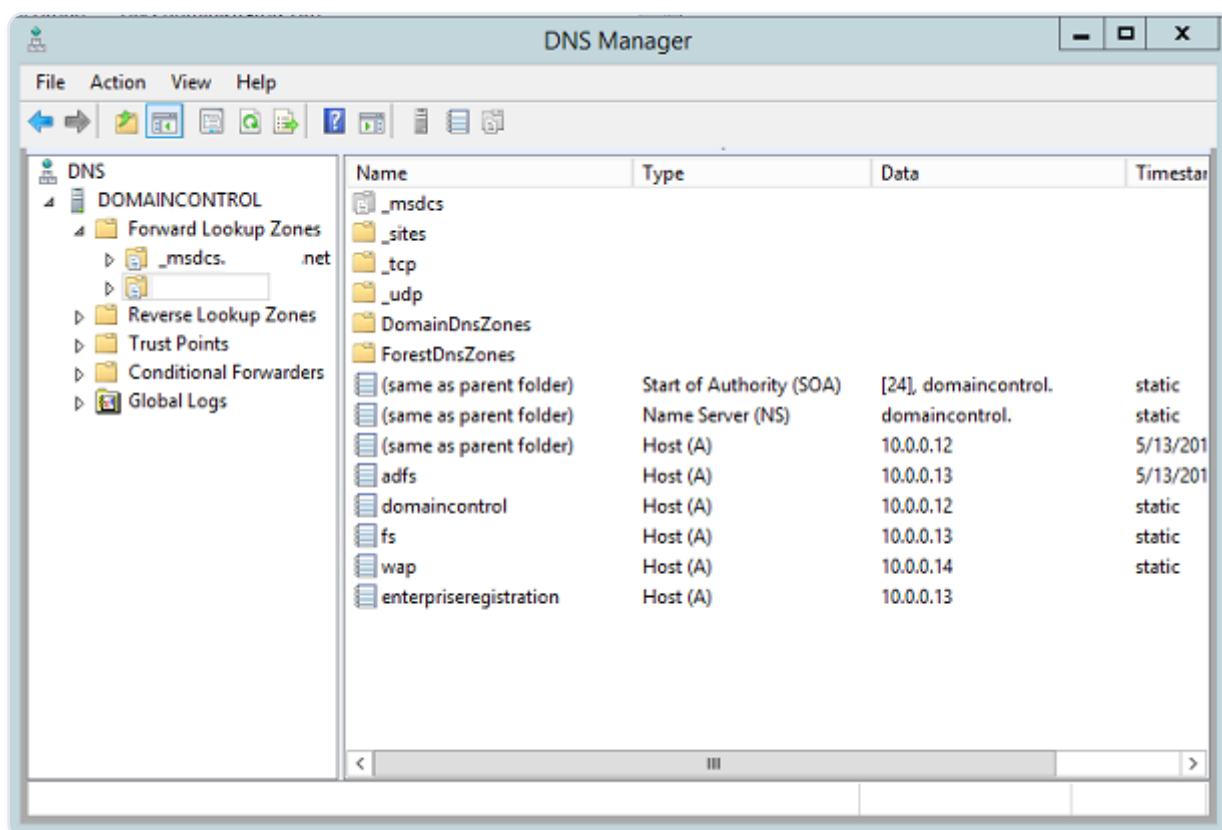
- AzureAD ConnectツールからのPSリモート処理をファイアウォール経由で許可するために、これらのサーバーで**Enable-PSRemoting -Force**コマンドレットを実行します。

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

- 残りの2台のWindowsサーバー（citrixsamldemoに参加済み）にCitrix Virtual AppsまたはCitrix Virtual Desktops Delivery Controller™とVDAをインストールします。

内部DNSの構成

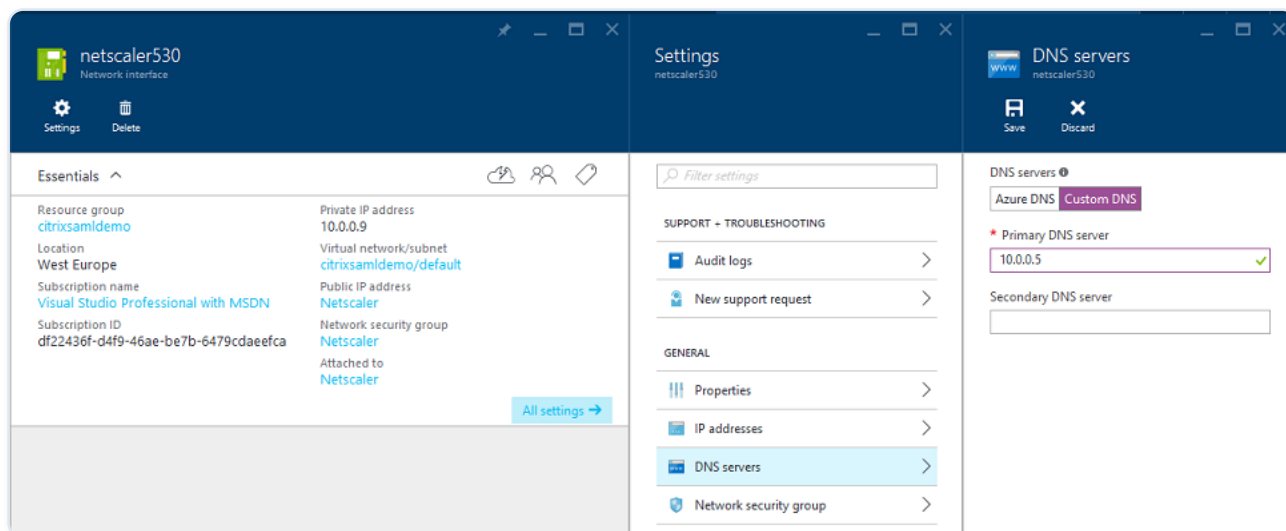
ドメインコントローラーのインストール後、DNSサーバーを構成して、citrixsamldemo.netの内部ビューを処理し、外部DNSサーバー（例：8.8.8.8）へのフォワーダーとして機能させます。



次の静的レコードを追加します。

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

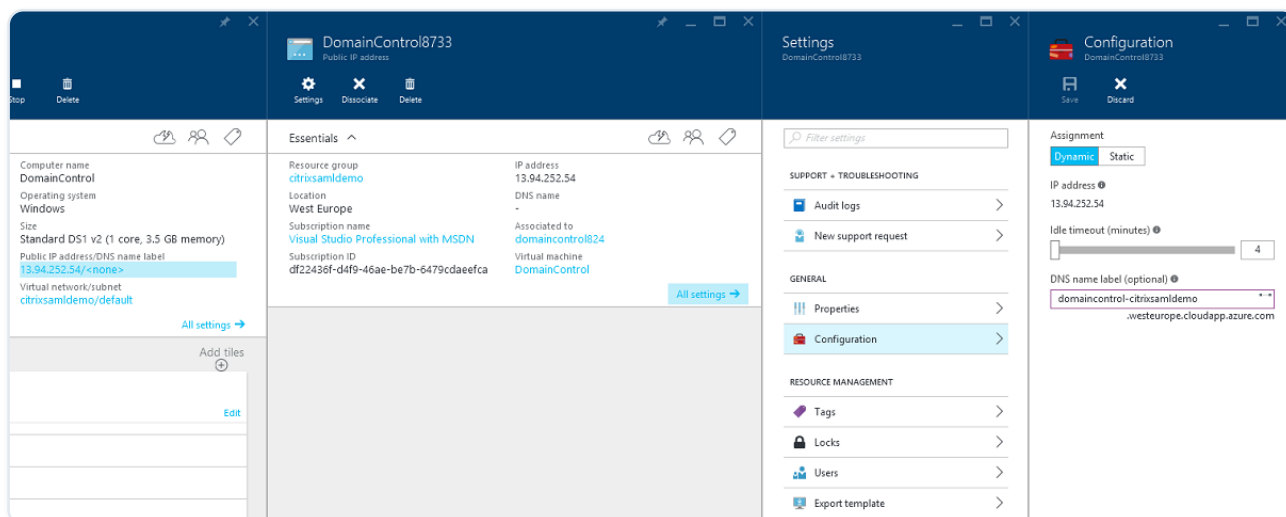
Azureで実行されているすべてのVMは、このDNSサーバーのみを使用するように構成する必要があります。これは、ネットワークインターフェースのGUIから実行できます。



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に割り当てられた現在のパブリック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。

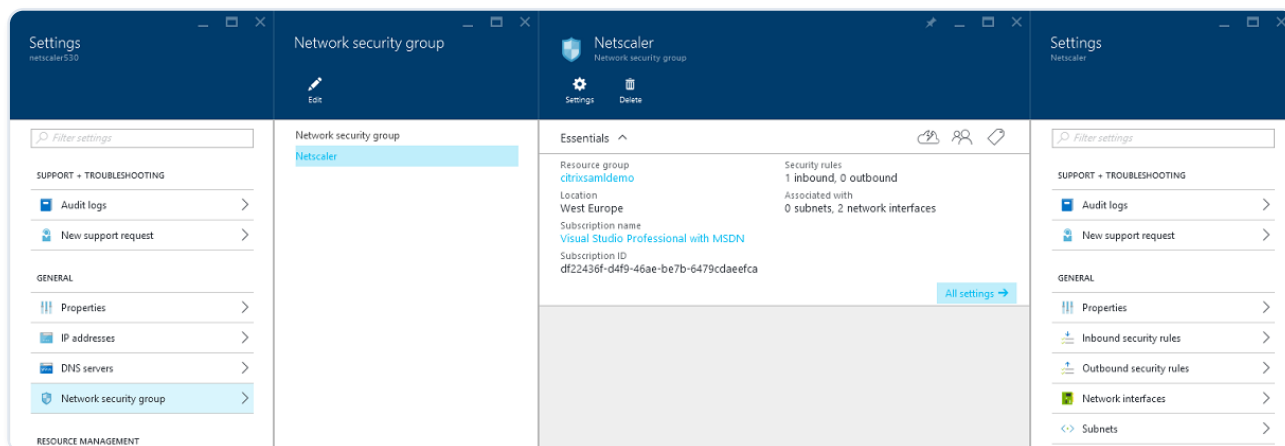


この例では、ドメインコントローラーにdomaincontrol-citrixsamldemo.westeurope.cloudapp.azure.comというDNSアドレスを割り当てます。

リモート構成が完了したら、WebアプリケーションプロキシとCitrix GatewayのVMのみがパブリックIPアドレスを有効にする必要があります。(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。

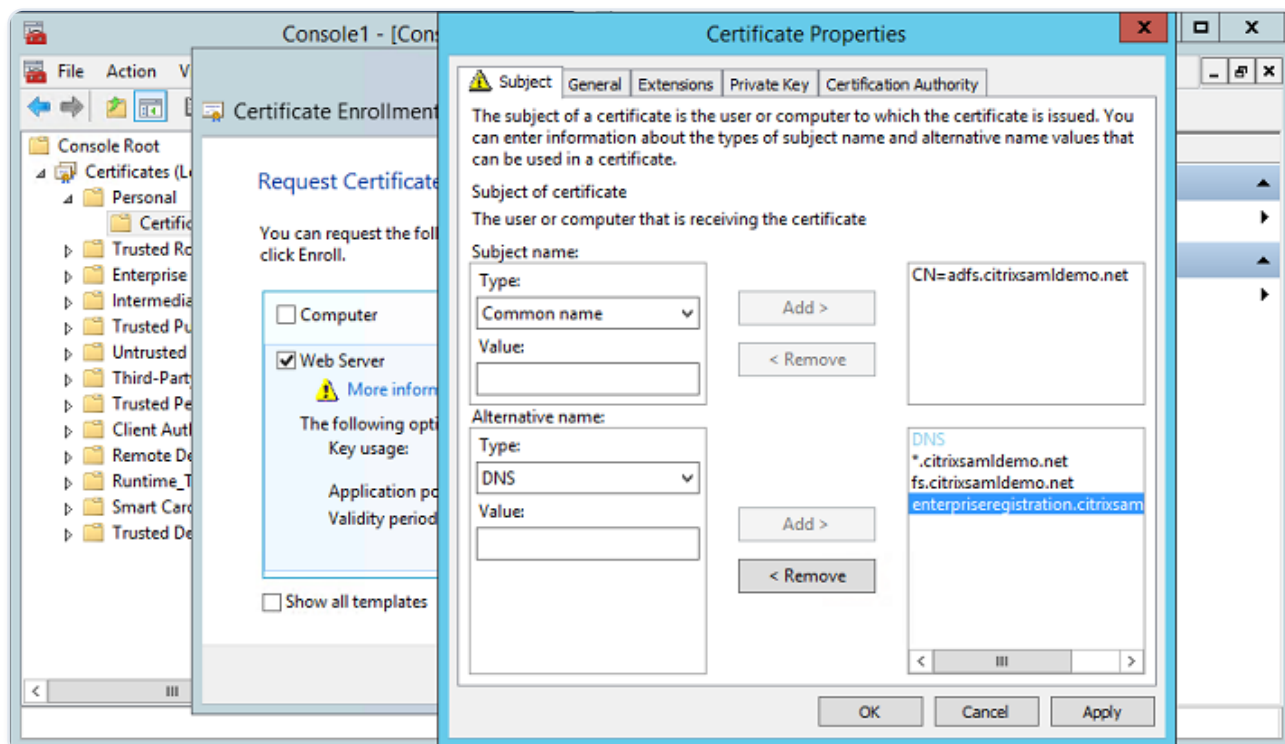


ADFS証明書を作成する

Microsoft 証明機関で **Web Server** 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 Application Proxy サーバーの両方にインストールするため、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. ネットワーク
 - enterpriseregistration.citrixsaml demo.net



パスワードで保護された秘密鍵を含め、証明書を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を作成する

従来のAzureポータルにログインし、新しいディレクトリを作成します。

ADD DIRECTORY

DIRECTORY ⓘ

Create new directory ▼

NAME ⓘ

CitrixSAMLdemo

DOMAIN NAME ⓘ

citrixsaml demo ✓ .onmicrosoft.com

COUNTRY OR REGION ⓘ

United Kingdom ▼

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

✓

完了すると、概要ページが表示されます。

The screenshot shows the Citrix SAML Demo web application. At the top, the title 'citrixsamldemo' is displayed. Below it is a navigation bar with links: USERS, GROUPS, APPLICATIONS, DOMAINS, DIRECTORY INTEGRATION, CONFIGURE, REPORTS, and LICENSES. The main content area features a large blue hexagonal icon with a white network diagram. To the right of the icon, the text reads: 'Your directory is ready to use. Here are a few options to get started.' Below this text is a checkbox labeled 'Skip Quick Start the next time I visit'. Underneath, there is a section titled 'I WANT TO' with three buttons: 'Set Up Directory' (highlighted in blue), 'Manage Access', and 'Develop Applications'. Below this is a section titled 'GET STARTED' with three numbered steps: 1. 'Improve user sign-in experience' with a description and an 'Add domain' button; 2. 'Integrate with your local directory' with a description and a 'Download Azure AD Connect' link; 3. 'Get Azure AD Premium' with a description and a 'Try it now' button.

グローバル管理者ユーザー (AzureAdmin) を作成する

Azure でグローバル管理者を作成し（この例では

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

ADD USER

user profile

FIRST NAME: Azure

LAST NAME: Admin

DISPLAY NAME: Azure Admin

ROLE: Global Admin

ALTERNATE EMAIL ADDRESS: [Red error icon]

MULTI-FACTOR AUTHENTICATION: ☐ Enable Multi-Factor Authentication

1 3

ドメインを Azure AD に登録する

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動作しますが、標準形式のメールアドレス、できればエンドユーザーのメールアカウントと一致するものがより適切です: `<user.name>@<company>.com`。

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

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

ADD DOMAIN

Specify a domain name

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

DOMAIN NAME

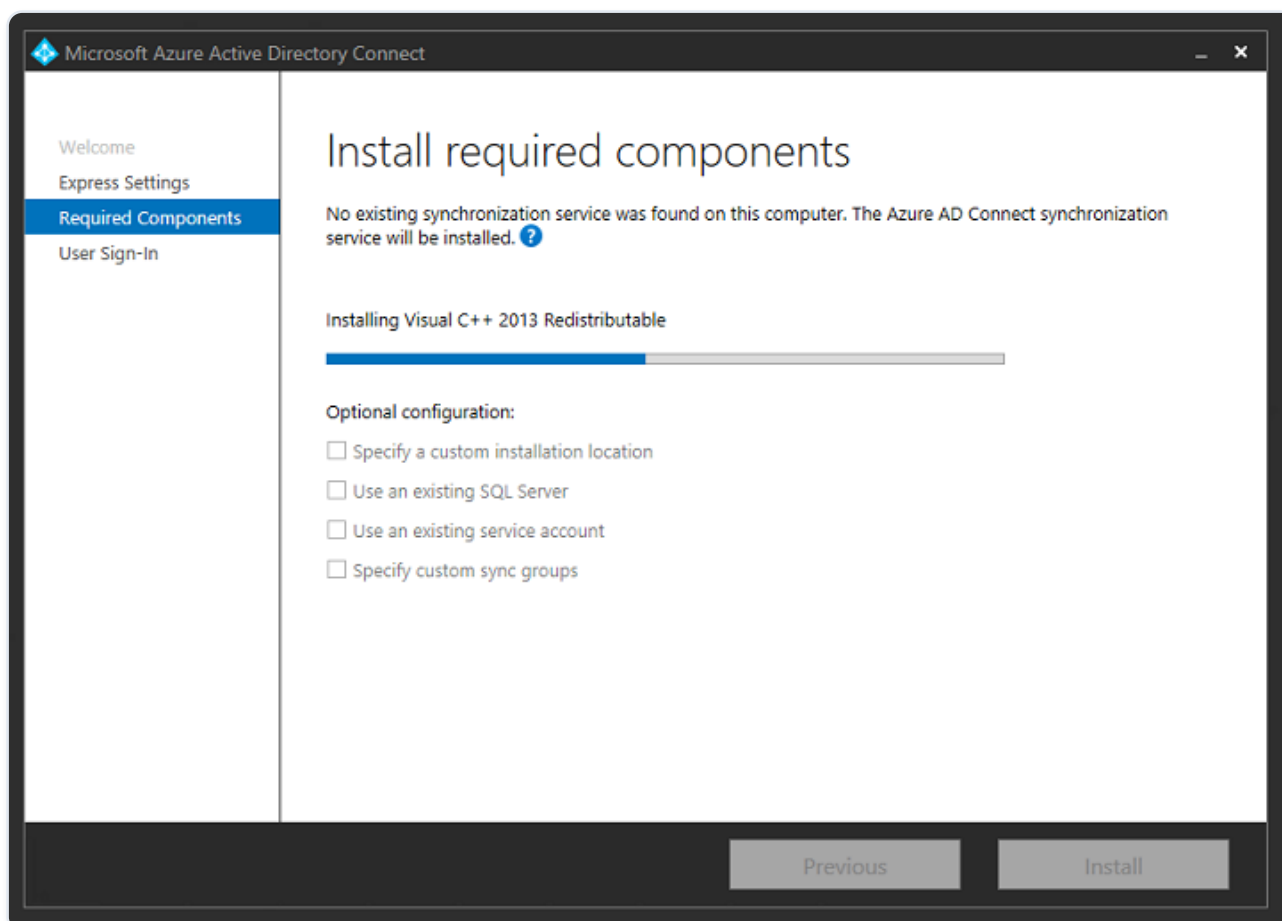
☒ I plan to configure this domain for single sign-on with my local Active Directory. ?

add

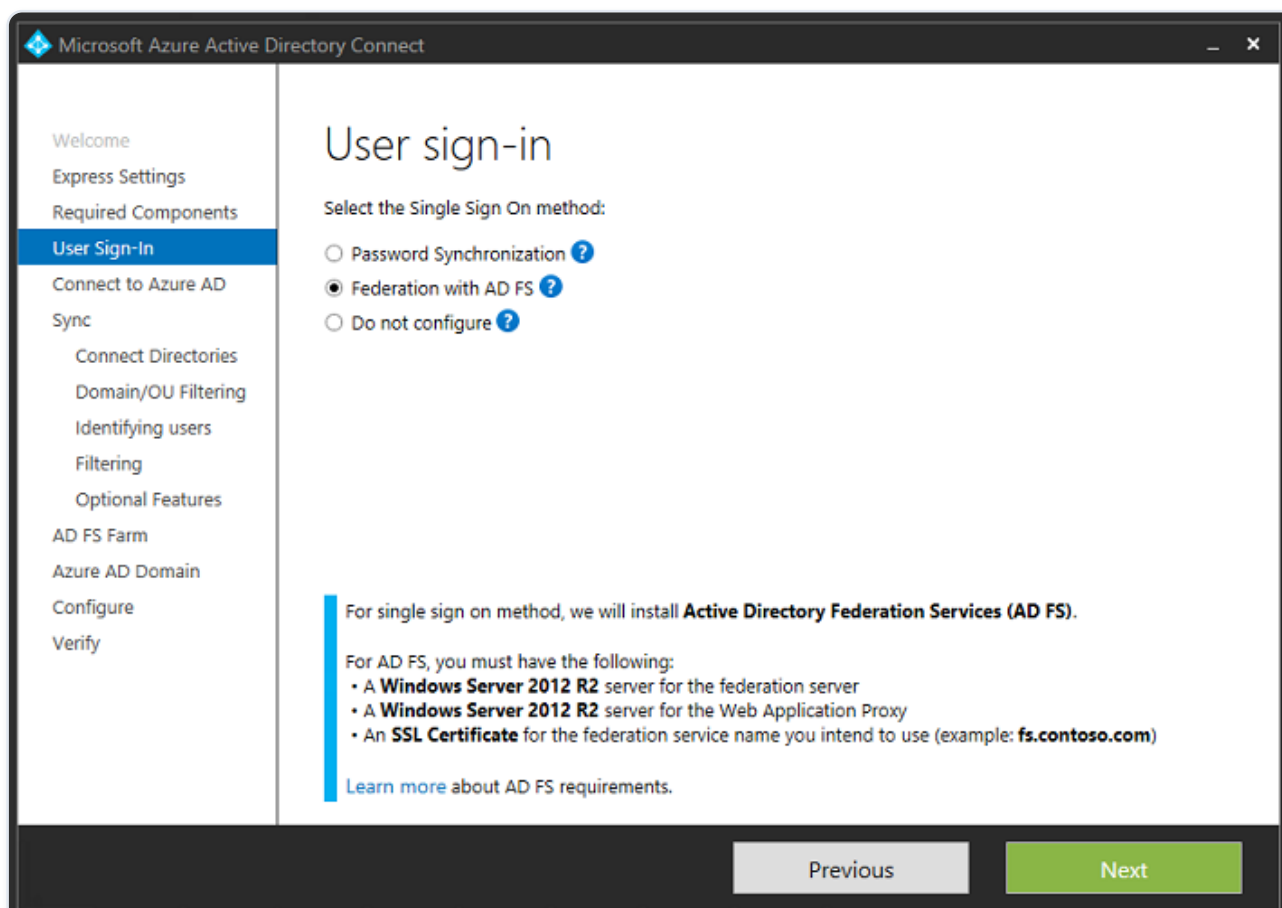
2

Azure AD Connect をインストールする

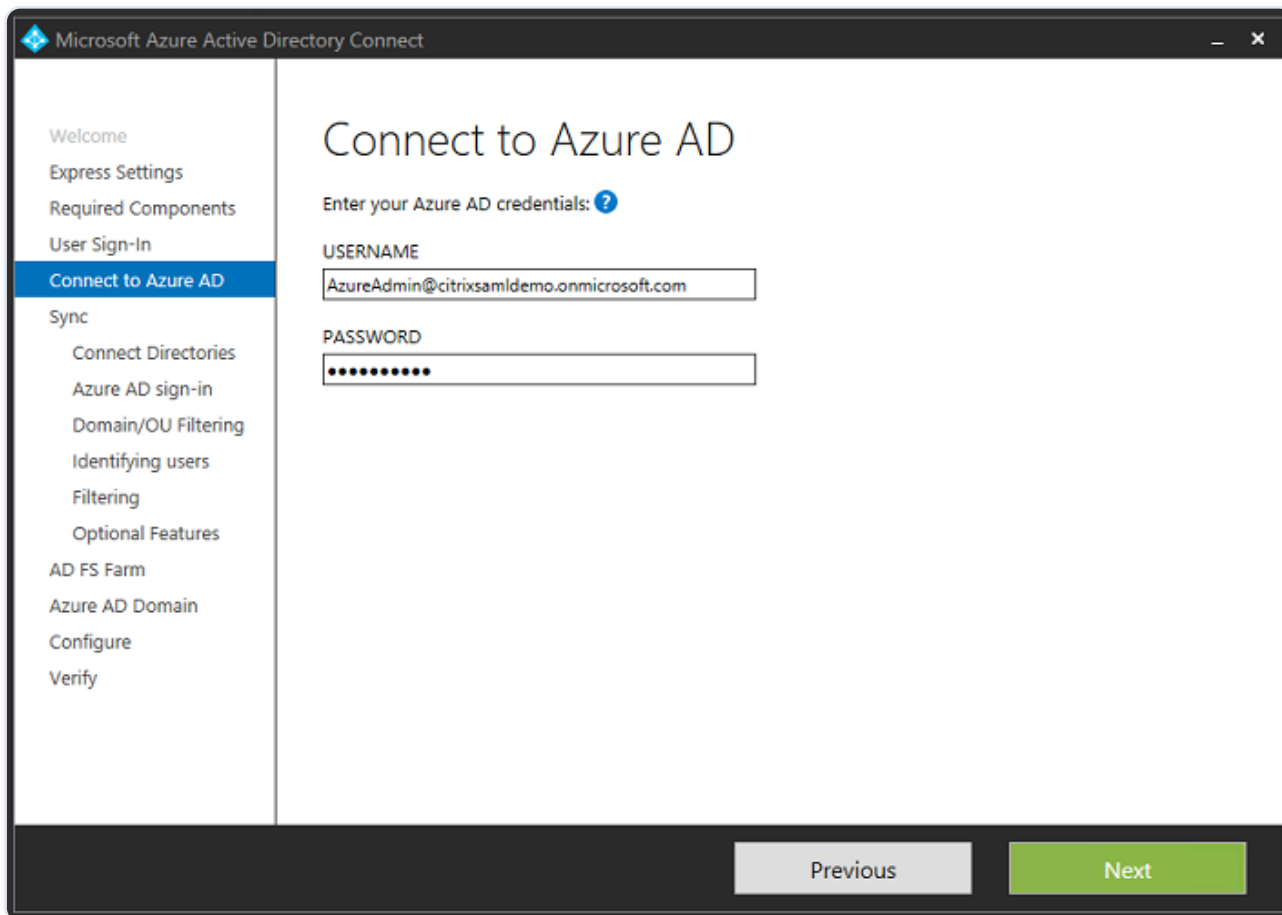
Azure AD 構成 GUI のステップ 2 は、Azure AD Connect の Microsoft ダウンロードページにリダイレクトされます。これを ADFS VM にインストールします。ADFS オプションが利用できるように、**Express Settings** ではなく、**Custom install** を使用してください。



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 area 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.

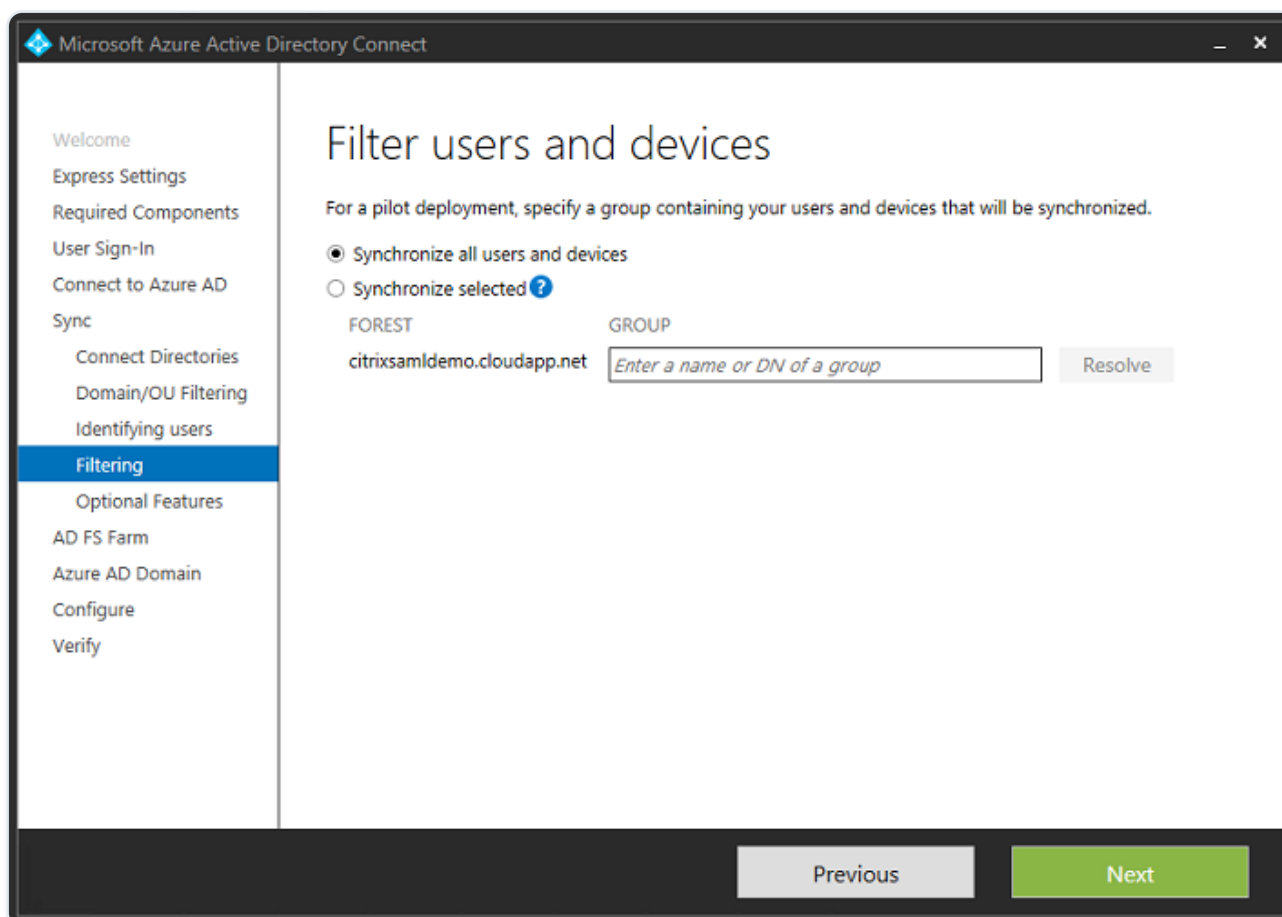
内部ADフォレストを選択します。

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。

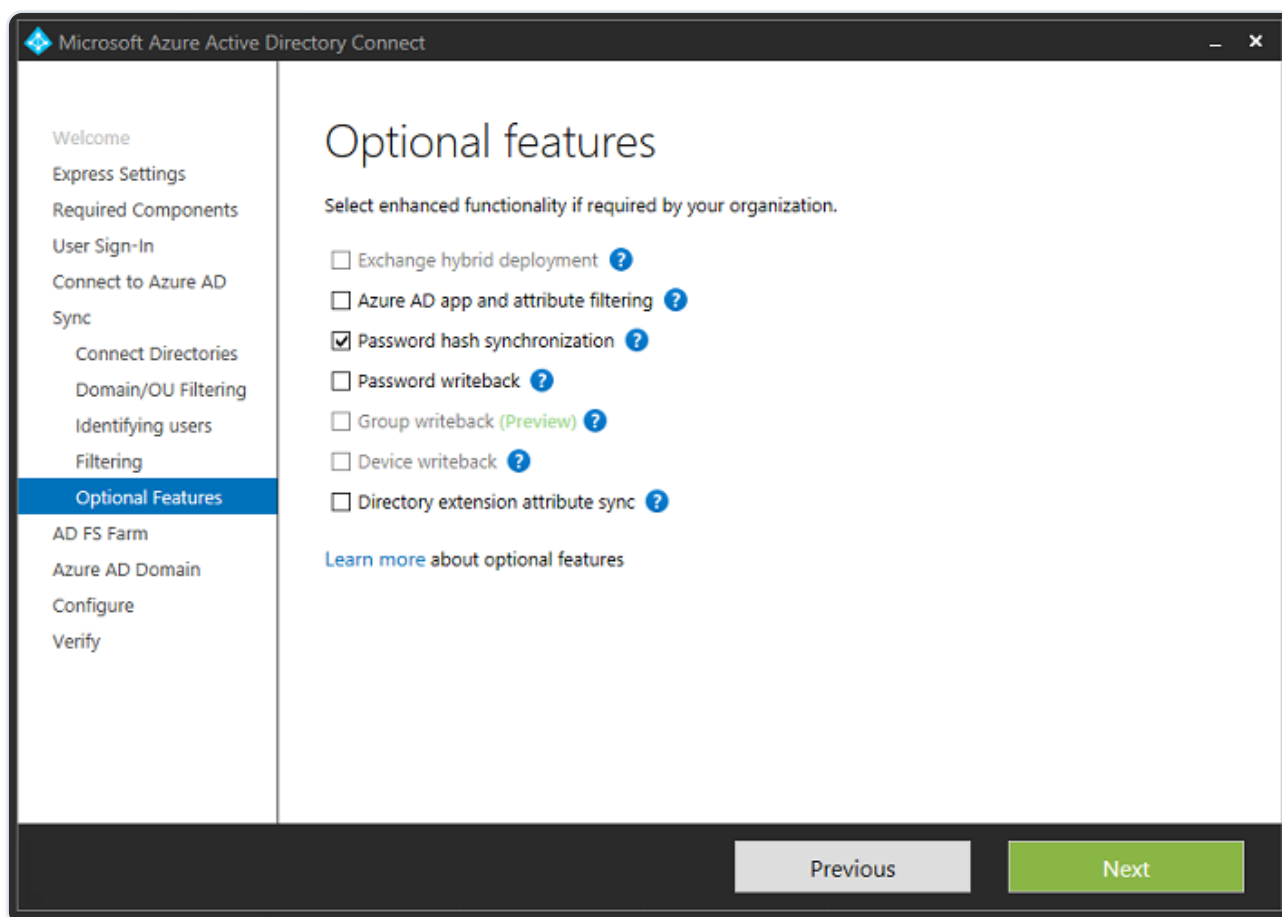
ディレクトリ構造が単純な場合は、ユーザー名が十分に一意であるため、ログオンするユーザーを識別できます。

The screenshot shows the 'Uniquely identifying your users' configuration window in Microsoft Azure Active Directory Connect. The window has a dark title bar and a sidebar on the left with navigation links: 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 two sections. The first section, 'Select how users should be identified in your on-premises directories.', has a help icon and two radio button options. The first option, 'Users are represented only once across all directories.', is selected. The second option, 'User identities exist across multiple directories. Match using:', is unselected and has four sub-options: 'Mail attribute' (selected), 'ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes', 'SAMAccountName and MailNickName attributes', and 'A specific attribute'. Below these is a 'CUSTOM ATTRIBUTE' label and a text input field. The second section, 'Select how users should be identified with Azure AD.', has a help icon and two dropdown menus. The first dropdown, labeled 'SOURCE ANCHOR', has 'objectGUID' selected. The second dropdown, labeled 'USER PRINCIPAL NAME', has 'userPrincipalName' selected. At the bottom of the window 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 Application Proxy 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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-setup-azure-wap-servers.png)

注:

この手順がリモート PowerShell の信頼性の問題で失敗した場合は、Web Application Proxy 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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-setup-azure-azure-ad-domain.png)

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

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-setup-azure-txt-mx.png)

Azure 管理コンソールで **Verify** をクリックします。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-setup-azure-verify.png)

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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-setup-azure-install-complete.png)

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CNAME DNSレコードを構築するために使用されます。このレコードは ADFS: enterpriseregistration.\<upnsuffix>を指す必要があります。

この例では、これは fs.citrixsamldemo.net です。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-enable-azureadjoin-cname.png)

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

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-enable-azureadjoin-signin.png)

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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-enable-azureadjoin-upn1.png)

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-enable-azureadjoin-upn2.png)

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-enable-azureadjoin-finish.png)

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、`<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

Delivery ControllerとVDA仮想マシンは、Citrix Virtual AppsまたはCitrix Virtual DesktopsのISOから、通常の方法でAzureに直接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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-install-xaxd-sf.png)

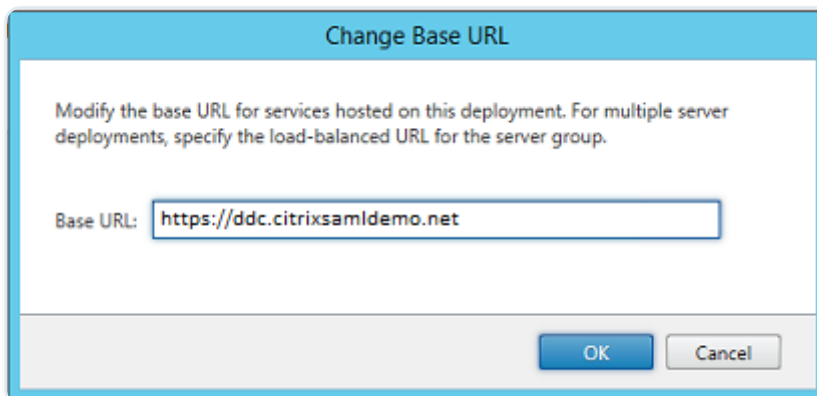
Controllerで **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** PowerShell コマンドレットを実行して、StoreFront™がユーザーの資格情報なしで認証できるようにします。

フェデレーション認証サービスをインストールする

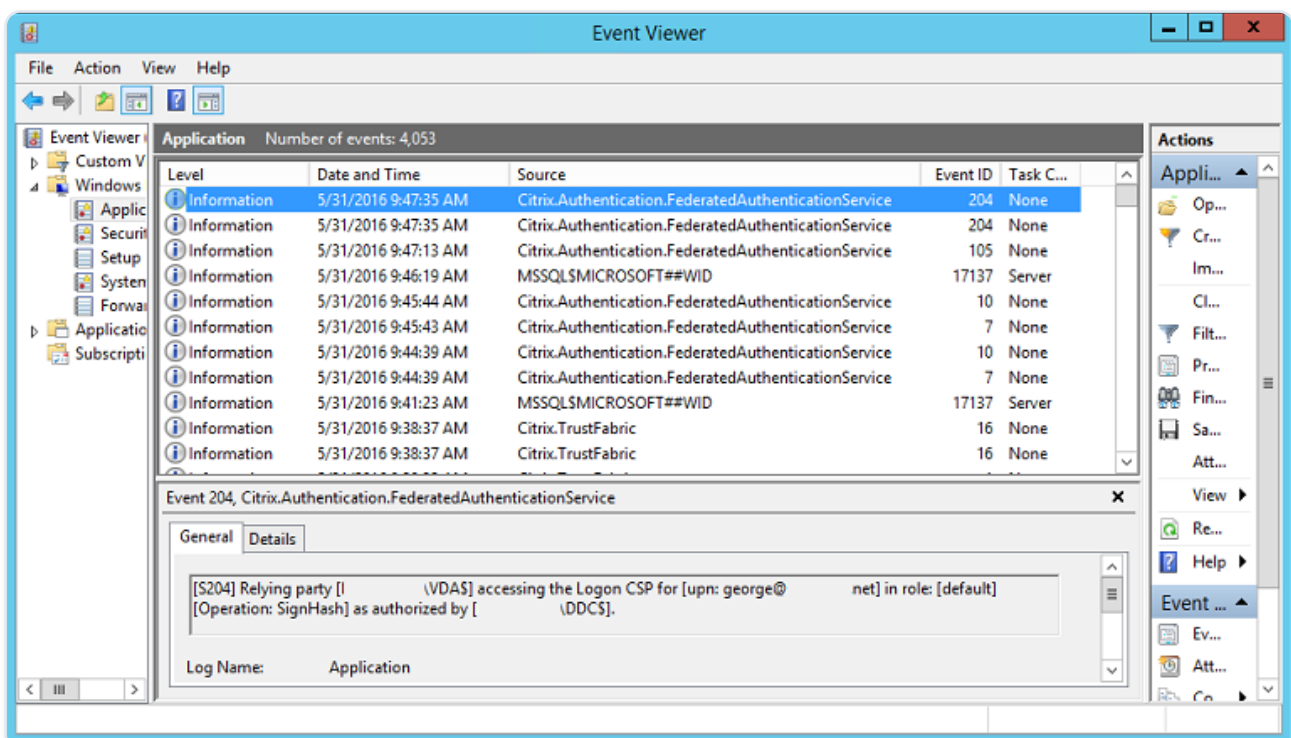
ADFSサーバーにFASをインストールし、Delivery Controllerが信頼されたStoreFrontとして機能するためのルールを構成します（この例では、StoreFrontはDelivery Controllerと同じVMにインストールされているため）。[インストールと構成](#)を参照してください。

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

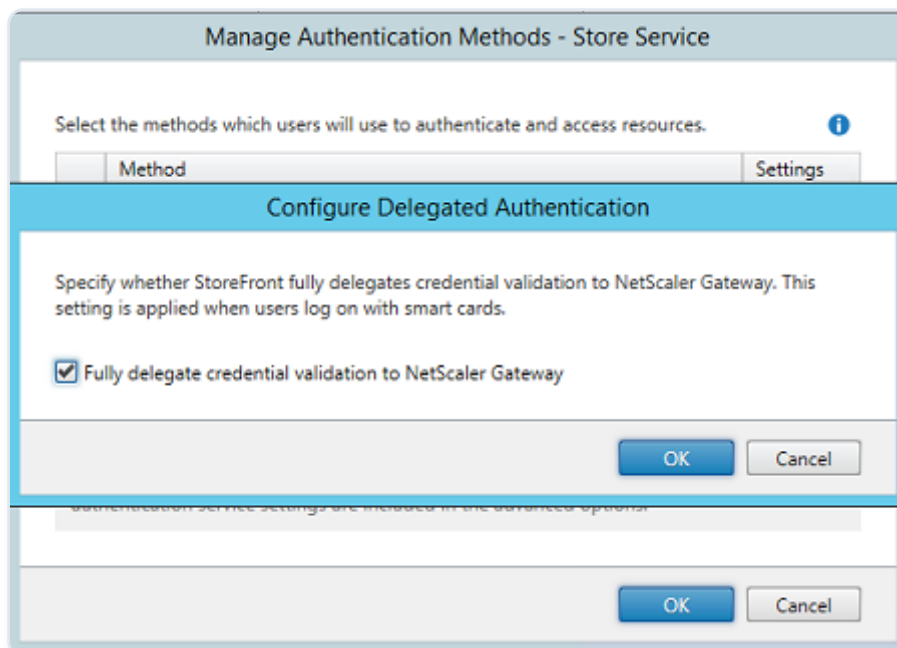


StoreFrontがFASサーバーを使用するように構成し（インストールと構成のPowerShellスクリプトを使用）、Azure内で内部的にテストし、FASサーバーのイベントビューアーを確認してログオンがFASを使用していることを確認します。

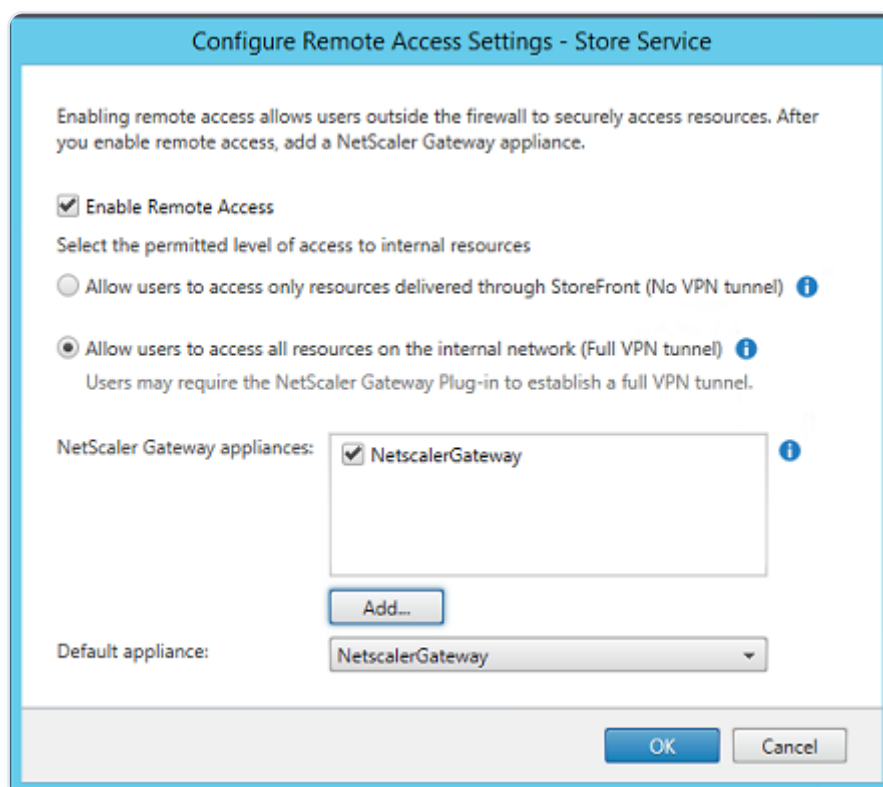


StoreFrontでCitrix Gatewayを使用するように構成する

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。

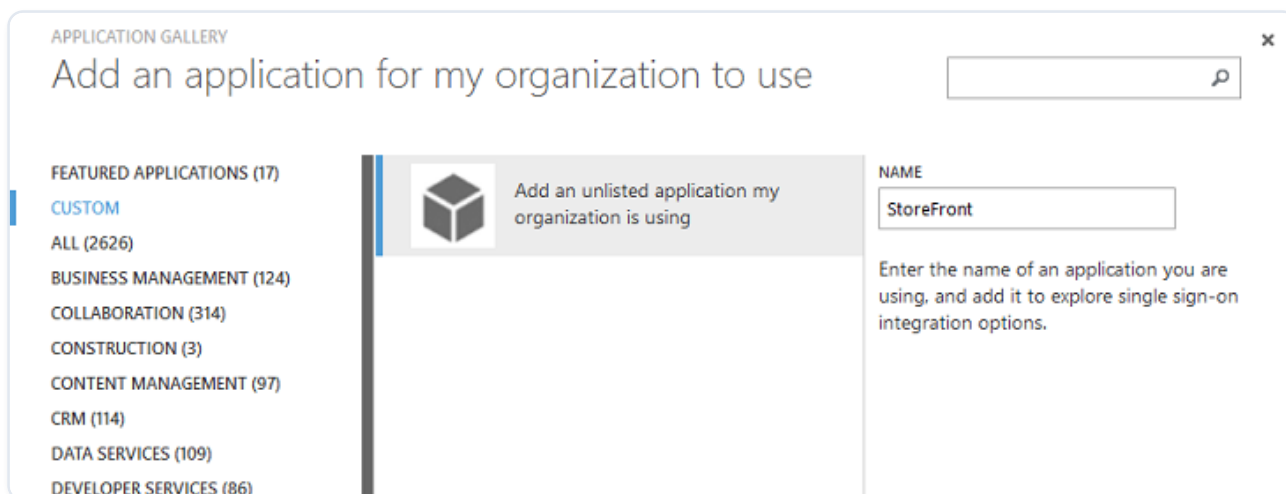


Citrix Gateway認証オプションを統合するには、Secure Ticket Authority (STA) を構成し、Citrix Gatewayアドレスを構成します。



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。



ユーザー向けの新しいカスタムアプリケーションを作成するには、> を選択します。

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には、215 x 215 ピクセルの画像を作成し、ページにアップロードします。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-config-app-add-app-icon.png)

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、 を選択します。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-config-app-add-configsso.png)

この展開では、**Microsoft Azure AD Single Sign-On** に対応する SAML 2.0 認証を使用します。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-config-app-add-ad-sso.png)

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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-config-app-add-id-replyurl.png)

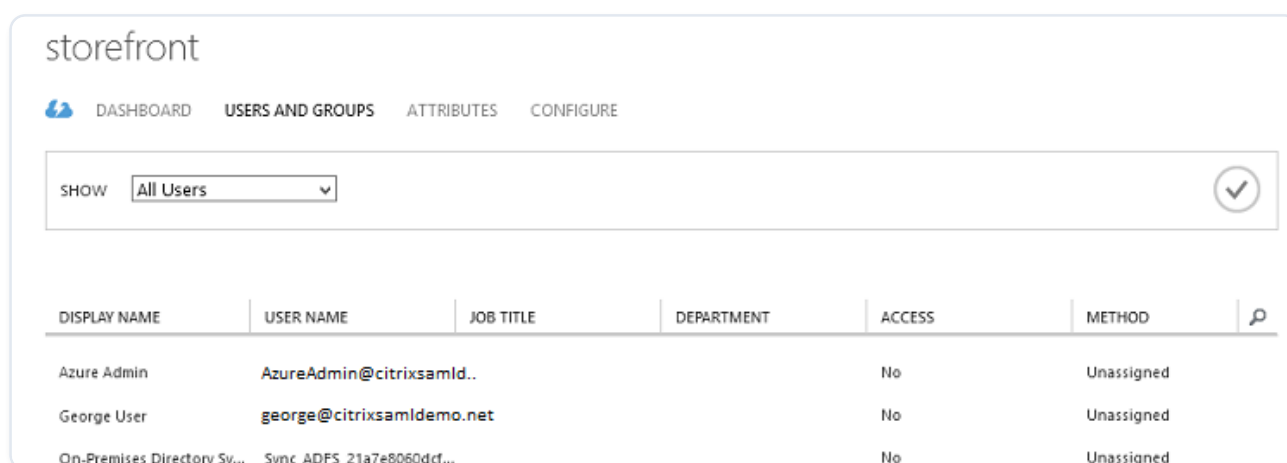
次のページには、Citrix Gateway を Azure AD の証明書利用者として構成するために使用される情報が含まれています。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-config-app-add-relyparty.png)

Base 64 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。



storefront

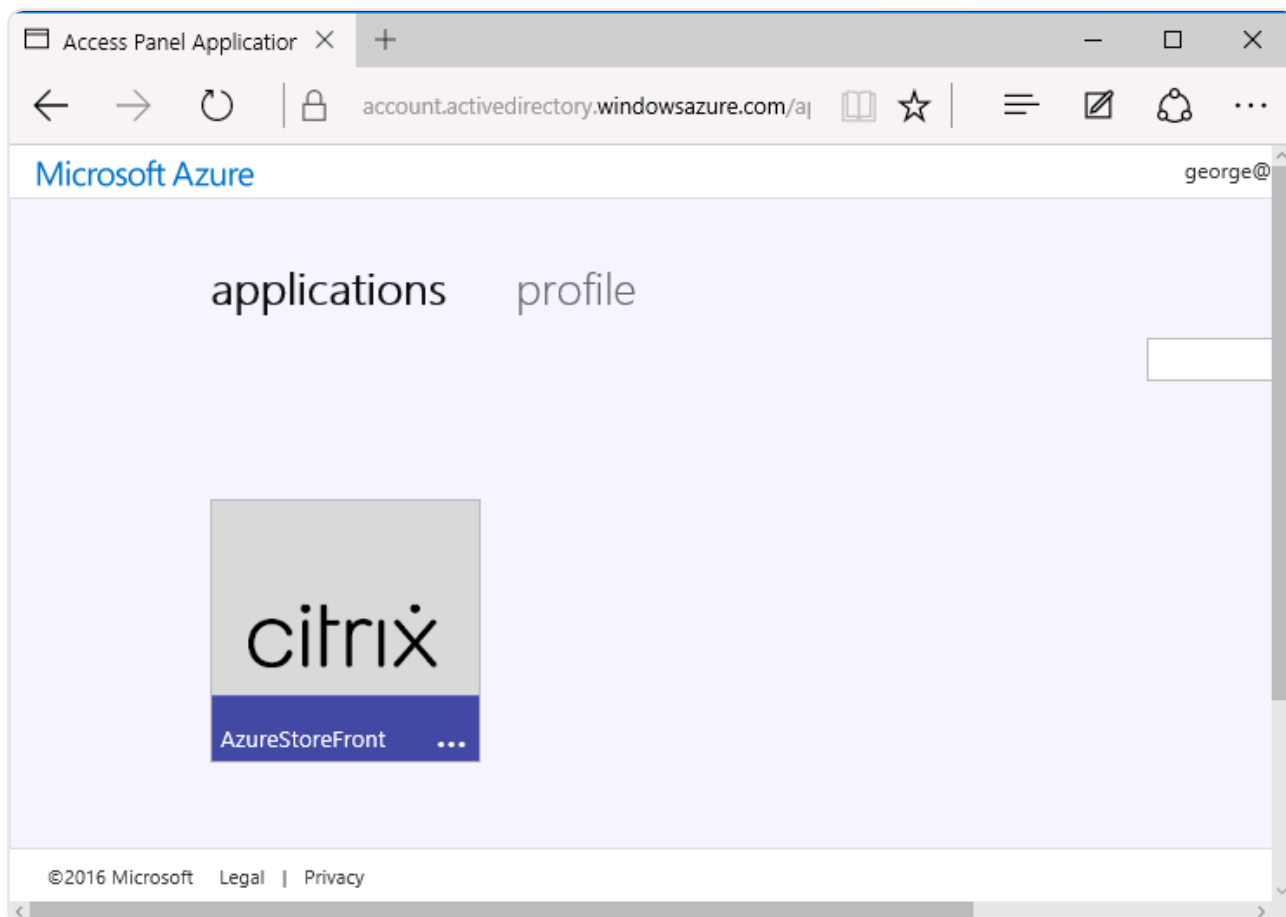
DASHBOARD USERS AND GROUPS ATTRIBUTES CONFIGURE

SHOW All Users

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

MyAppsページ

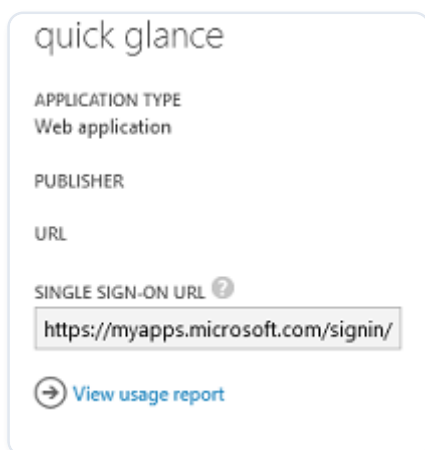
アプリケーションが構成されると、ユーザーが <https://myapps.microsoft.com> にアクセスしたときに、Azureアプリケーションのリストに表示されます。



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

シングルサインオンURL

Azure ADダッシュボードのアプリケーションに戻ります。アプリケーションで利用可能なシングルサインオンURLが作成されています。このURLは、Webブラウザリンクを提供したり、ユーザーをStoreFrontに直接誘導するスタートメニュー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のみ機能し、Windows 10 Azure AD参加ログオンセッションに対してのみシングルサインオンを提供します。（他のユーザーはAzure AD資格情報の入力を求められます。）

Citrix Gatewayのインストールと構成

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

NetScaler® VMにログオンし、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て、Webブラウザを内部IPアドレスに向けます。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。

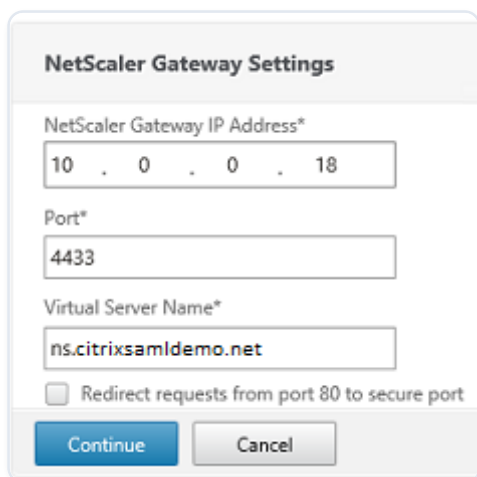
ライセンスを追加し、各ライセンスファイルの追加後に**再起動**を選択し、DNSリゾルバーをMicrosoftドメインコントローラーに向けます。

Citrix Virtual Apps and Desktopsセットアップウィザードの実行

この例では、まずSAMLなしでシンプルなStoreFront統合を構成します。そのデプロイが機能した後、SAMLログオンポリシーを追加します。

The screenshot shows the 'XenApp/XenDesktop Setup Wizard' window. The first section, 'What is your deployment', features a 'Single Hop' option (indicated by a green circle) and a network diagram showing a Client connecting through the Internet to an Access Gateway, which then connects to a Server Farm. The second section, 'What is your Citrix Integration Point?', has a dropdown menu with 'StoreFront' selected. At the bottom are 'Continue' and 'Cancel' buttons.

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

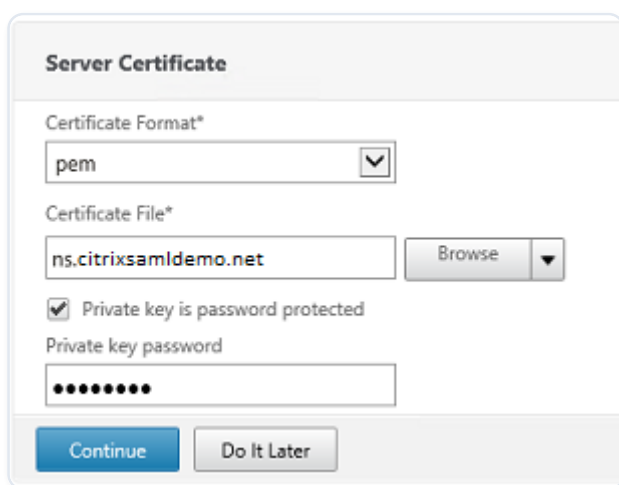
Virtual Server Name*

ns.citrixsamldemo.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= citrixsaml demo ,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

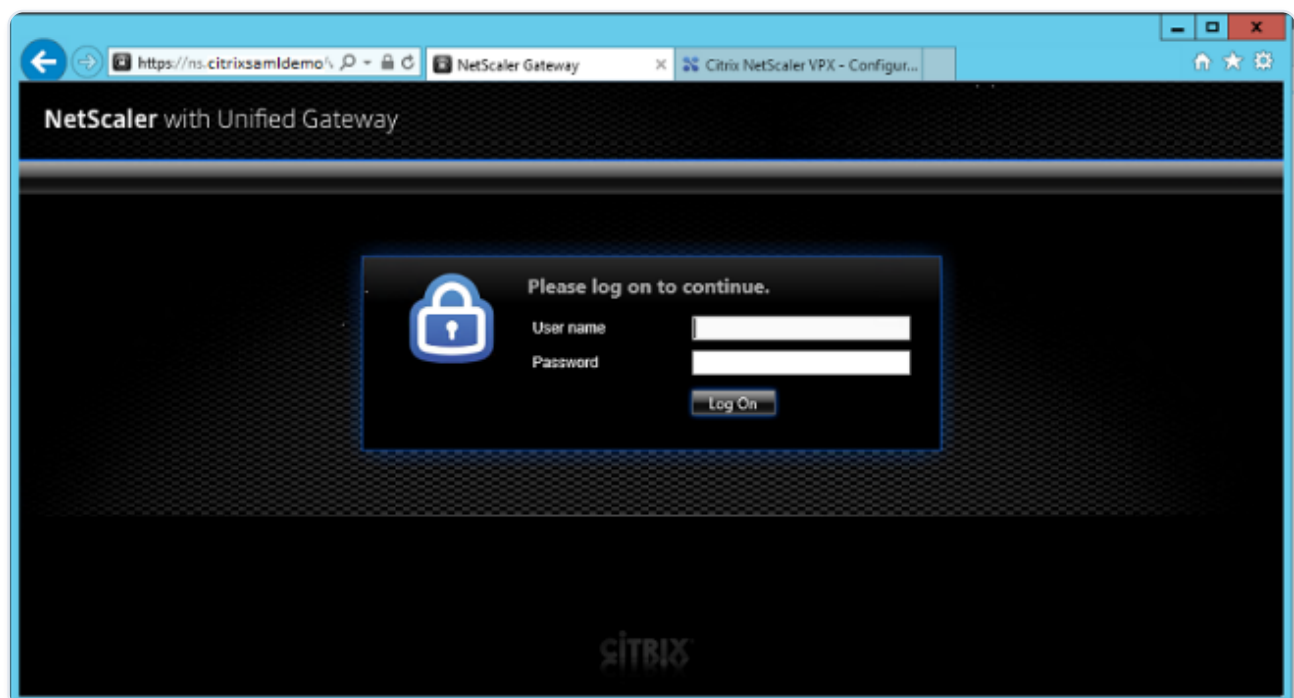
☐ Load Balancing

Continue

Cancel

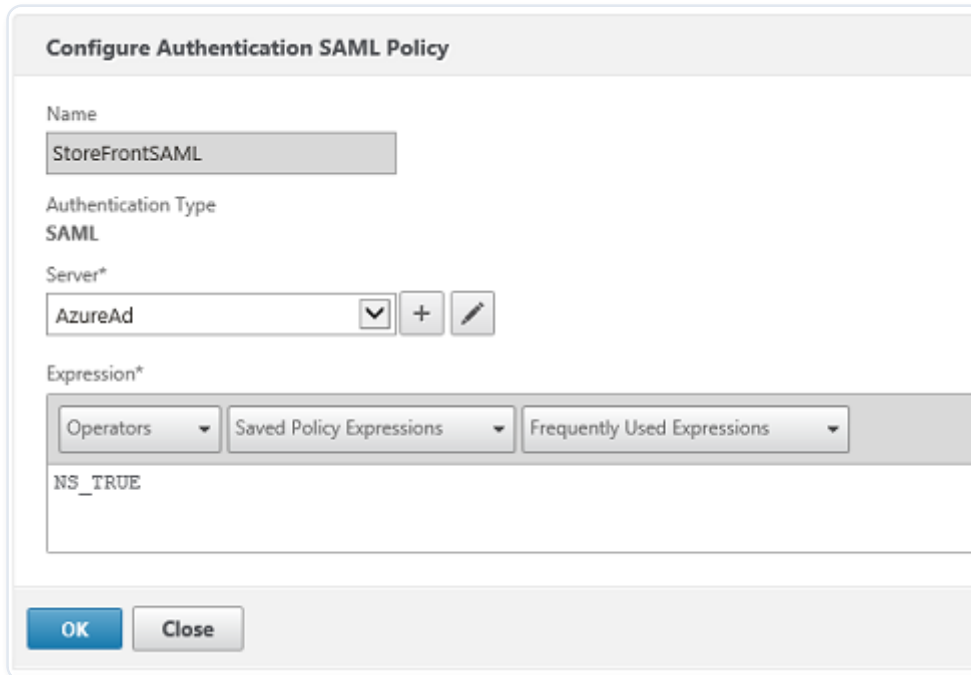
Citrix Gatewayの展開を確認する

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



Citrix Gateway SAML 認証サポートを有効にする

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



Configure Authentication SAML Policy

Name
StoreFrontSAML

Authentication Type
SAML

Server*
AzureAd

Expression*
Operators Saved Policy Expressions Frequently Used Expressions
NS_TRUE

OK Close

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

Create Authentication SAML Server

Create Authentication SAML Server

Name*
AzureAd

Authentication Type
SAML

IDP Certificate Name*
AzureADSAML

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

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

User Field
userprincipalname

Signing Certificate Name

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

Reject Unsigned Assertion*
ON

SAML Binding*
POST

Default Authentication Group

Skew Time(mins)
5

5

Two Factor
☐ ON ☒ OFF

Assertion Consumer Service Index
255

Attribute Consuming Service Index
255

Requested Authentication Context*
Exact

Authentication Class Types
InternetProtocol
InternetProtocolPassword

Signature Algorithm*
☐ RSA-SHA1 ☒ RSA-SHA256

Digest Method*
☐ SHA1 ☒ SHA256

☐ Send Thumbprint
☒ Enforce Username

Attribute 1
Attri

Attribute 3
Attri

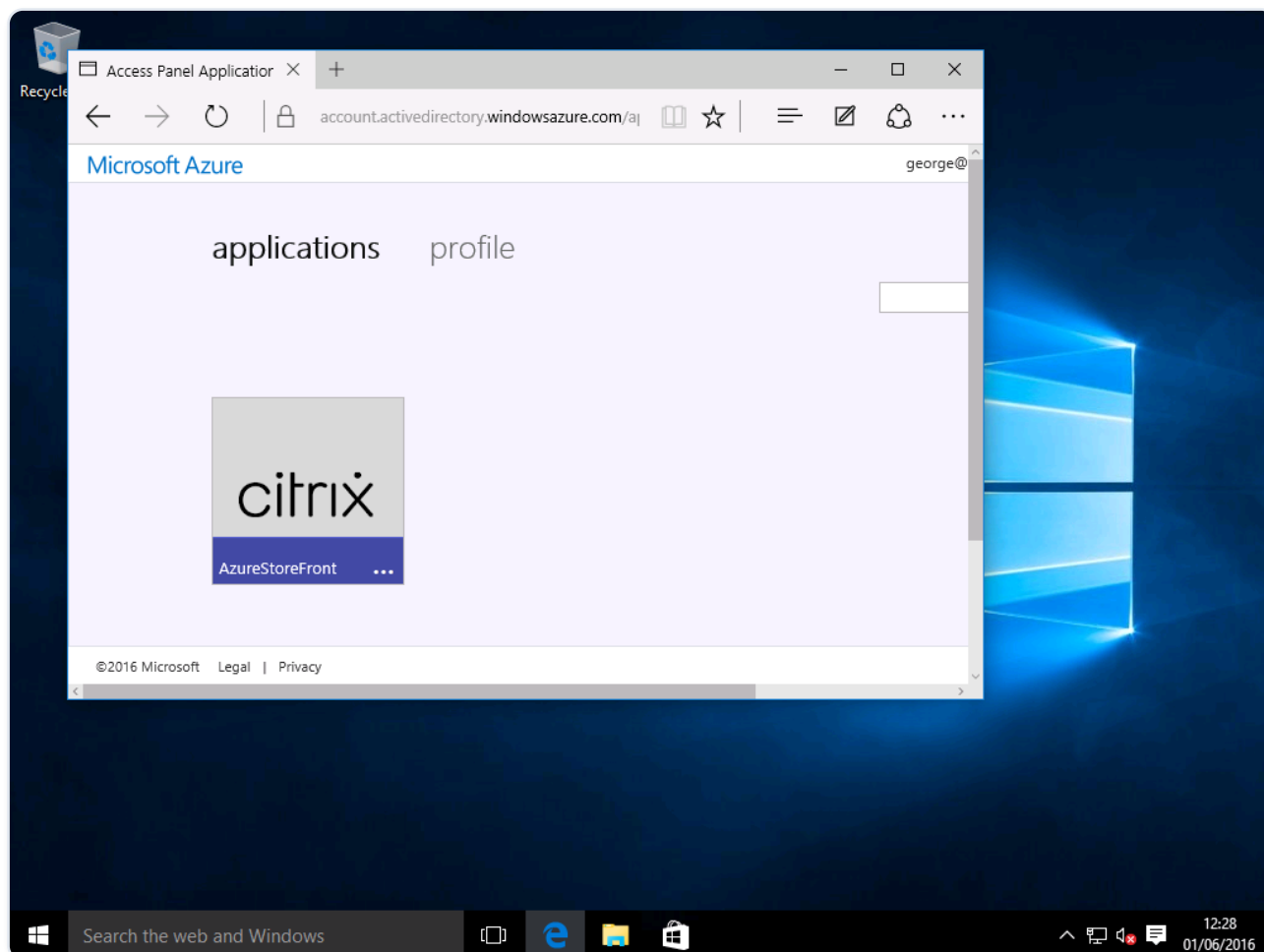
Attribute 5
Attri

Attribute 7
Attri

エンドツーエンドシステムを確認する

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

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



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

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

最後に、Azure AD に参加していないマシンも同じ URL で機能することを確認します（ただし、最初の接続では Azure AD への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 アドレスを割り当てます。デフォルトでは、パブリック IP アドレスも提供され、動的に更新される DNS ラベルで参照できます。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-vm-options-public-ip-dns-adds.png)

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。

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-vm-options-public-ip-dns-label.png)

ファイアウォールルール (セキュリティグループ) を設定する

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

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

ローカライズされた画像(/en-us/federated-authentication-service/2206/media/fas-azure-vm-options-inbound-sec-rules.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。

Federated Authentication Service 2206 ドキュメント履歴

以下の表は、Federated Authentication Service 2206 ドキュメントの重要な変更点について説明しています。これらの更新に関する通知を受け取るには、RSS フィードを購読してください。

日付	変更点	説明
13 Jun 2022	Federated Authentication Service 2206 の初回リリース	Federated Authentication Service 2206 の初回リリースです。詳細については、「 新機能 」を参照してください。