



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 2407	10
以前のリリース	10
参照	11
フェデレーテッド認証サービス 2407	12
Federated Authentication Service KSPリモート処理 (プレビュー)	12
Windows Server 2025のサポート	12
修正された問題	12
既知の問題	12
サードパーティ通知	13
システム要件	14
インストールと構成	16
インストールとセットアップの順序	16
フェデレーション認証サービスをインストールする	16
FASのアップグレード	17
StoreFrontストアでFASプラグインを有効にする	17
Delivery Controller™を構成する	18
グループポリシーを構成する	18
セッション内の動作	22
プロンプトスコープ	23
同意タイムアウト	24
ロック時の切断	24
Federated Authentication Service 管理コンソールの使用	24
証明書テンプレートを展開する	25
Active Directory証明書サービスをセットアップする	26
フェデレーション認証サービスを承認する	27
ルールの構成	28

Citrix Cloudへの接続	31
Citrix Cloudから切断する	35
高度な構成	36
関連情報	36
テナント顧客向けにフェデレーション認証サービスを有効にする	36
前提条件	36
MSP 顧客を構成する	36
既知の問題	39
Azure Active Directory シングルサインオン	39
ドメイン参加済み VDA	40
ハイブリッド参加済みVDA	41
認証局の構成	43
FAS で使用する複数の CA サーバーをセットアップする	43
予期される動作の変更	43
TCP アクセス用に Microsoft 認証局を構成する	43
ユーザー証明書を事前生成する	44
Active Directoryユーザーのリストを取得する	44
FASサーバー	45
登録機関証明書を更新する	47
関連情報	48
秘密キーの保護	49
はじめに	49
秘密キーの構成設定	50
構成シナリオの例	53
例 1	53
例 2	53
例 3	63
FAS証明書ストレージ	65

関連情報	67
キー ストレージ プロバイダー (KSP) リモーティング (プレビュー)	67
はじめに	67
KSP リモーティングを有効にする	68
KSPリモート処理が有効になっているかを確認する	68
既知の制限事項	69
セキュリティとネットワーク構成	69
ネットワークアーキテクチャ	69
ファイアウォールとネットワークセキュリティ	70
シトリックス フェデレーテッド認証サービスとシトリックス クラウド™間の接続	71
シトリックス クラウド	71
Citrix Cloud 日本	72
セキュリティに関する考慮事項	72
委任された登録エージェント	72
アクセス制御リストの構成	73
ファイアウォール設定	73
イベントログの監視	74
ハードウェアセキュリティモジュール	74
管理者の責任	75
グループポリシー設定	75
証明書テンプレート	76
証明書テンプレートの名前を変更する	76
一般プロパティを変更する	76
要求処理プロパティの変更	76
暗号化プロパティの変更	76
キー構成証明プロパティの変更	77
廃止されたテンプレートプロパティの変更	77
拡張機能プロパティの変更	77

セキュリティプロパティの変更	77
サブジェクト名のプロパティを変更する	78
サーバーのプロパティを変更する	78
発行要件のプロパティを変更する	78
互換性プロパティを変更する	79
証明機関の管理	79
テンプレートの公開	79
ファイアウォール設定	80
登録の制限	80
ポリシーモジュールと監査	80
FAS管理	80
ACLを介してStoreFront、ユーザー、VDAを制限する	81
ルールの構成	81
証明機関とテンプレートの構成	81
セッション内証明書と認証証明書	82
秘密鍵の保護と鍵長	82
イベントログ	82
管理アクセスと管理ツール	82
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	82
者	
一般的なWindowsサーバーのセキュリティ	82
関連情報	83
パフォーマンスカウンター	83
Windowsログオンの問題のトラブルシューティング	84
証明書と公開鍵インフラストラクチャ	84
UPN 名と証明書のマッピング	85
アクティブディレクトリのユーピーエヌ名	85
証明書マッピングサービス	86

ログオンドメインコントローラーの選択を制御する	86
ドメインコントローラーの選択を制御する	86
使用中のドメインコントローラーを特定する	87
アカウント監査イベントを有効にする	87
証明書検証ログ	87
証明書の有効性を確認する	87
CAPIログを有効にする	87
CAPIログ	88
エラーメッセージ	88
Kerberosログ	89
ドメインコントローラーとワークステーションのログ	89
ドメインコントローラー CAPI2 ログ	90
ドメインコントローラー セキュリティログ	90
VDA セキュリティログ	90
VDA CAPIログ	91
VDAシステムログ	91
Windowsイベントログを使用したFASの監視	91
FASサービスは実行中ですか?	91
FASヘルスイベント	91
クラウド接続FASイベント	93
セキュリティイベント	94
FASイベントログ	95
管理イベント	95
IDアサーションの作成	98
依頼当事者として機能する	98
セッション内証明書サーバー	99
FASアサーションプラグイン	99
ワークスペース対応FAS	100

ログオン	102
インセッション証明書	102
証明書要求とキーペア生成	103
エンドユーザーのエラーメッセージ	103
関連情報	104
PowerShell コマンドレット	105
展開アーキテクチャ	106
はじめに	106
アーキテクチャの概要	106
内部展開	107
Citrix Gateway の展開	110
ADFS SAML展開	111
B2Bアカウントマッピング	111
Windows 10 Azure AD ジョイン	112
ADFS 展開	114
はじめに	114
SAML の概要	116
リダイレクトURL	116
識別子	116
戻りアドレス	116
署名証明書	116
シングルサインアウト URL	117
構成	117
SAML ポリシーの入力	117
関連情報	117
Azure AD統合	118
はじめに	118
アーキテクチャ	119

DNSゾーンを作成する	120
クラウドサービスを作成する	122
Windows仮想マシンを作成する	122
ドメインコントローラー	123
ADFSコントローラーとWebアプリケーションプロキシサーバー	123
Citrix Virtual Desktops™ デリバリーコントローラーとVDA	124
内部DNSの構成	124
外部DNSアドレスを構成する	125
セキュリティグループを構成する	125
ADFS証明書を作成する	125
Azure ADのセットアップ	126
新しいディレクトリの作成	126
グローバル管理者ユーザー (AzureAdmin) を作成する	128
Azure AD にドメインを登録する	129
Azure AD Connect をインストールする	130
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	136
Federated Authentication Service のインストール	137
StoreFrontの構成	137
StoreFrontがCitrix Gatewayを使用するように構成する	138
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	139
アイコンを構成する	140
SAML認証を構成する	140
アプリケーションをユーザーに割り当てる	142
MyAppsページ	143
シングルサインオンURL	144
Citrix Gatewayのインストールと構成	144
Citrix Virtual Apps and Desktopsセットアップウィザードの実行	144

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	146
StoreFrontアドレスを構成する	146
Citrix Gatewayの展開を検証する	147
Citrix Gateway SAML認証サポートを有効にする	148
エンドツーエンドシステムを検証する	149
付録	150
パブリックIPアドレスとDNSアドレスを提供する	150
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	151
関連情報	152
フェデレーション認証サービス2407ドキュメント履歴	153

フェデレーション認証サービス 2407

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

フェデレーション認証サービス 2407 は、FAS の最新の Current Release バージョンです。この記事には、この最新リリースにおける機能と構成が反映されています。

以前のリリース

以前の FAS リリースのドキュメントについては、以下を参照してください:

- [フェデレーション認証サービス 2402 LTSR](#)
- [フェデレーション認証サービス 2311](#)
- [フェデレーション認証サービス 2308](#)
- [フェデレーション認証サービス 2305](#)
- [フェデレーション認証サービス 2303](#)
- [フェデレーション認証サービス 2212](#)
- [フェデレーション認証サービス 2209](#)
- [フェデレーション認証サービス 2206](#)
- [フェデレーション認証サービス 2203](#)
- [フェデレーション認証サービス 2112](#)
- [フェデレーション認証サービス 2109](#)
- [フェデレーション認証サービス 2106](#)
- [フェデレーション認証サービス 2103](#)
- [フェデレーション認証サービス 1912 LTSR](#)
- [XenApp and XenDesktop 7.15 長期サービスリリース](#)

現在のリリース (CR) および長期サービスリリース (LTSR) の製品ライフサイクル戦略については、[Lifecycle Milestones](#)で説明されています。

参照

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

フェデレーテッド認証サービス 2407

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。

Federated Authentication Service KSPリモート処理 (プレビュー)

- Windows VDAからFASサーバーへの暗号化操作のリモート処理は、VDA上で実行される一対の暗号化サービスプロバイダー (CSP) を使用して実現されます。このプレビューでは、一対のキー記憶域プロバイダー (KSP) を使用して暗号化操作のリモート処理も実現できます。KSP は、Windowsアプリケーションに暗号化操作を公開する最新の方法であり、より多くの機能をサポートしています。詳細については、[KSPリモート処理](#)を参照してください。

Windows Server 2025のサポート

- FASはWindows Server 2025をサポートするようになりました。Windows Server 2025の詳細については、Microsoftドキュメントの[Windows Server 2025の新機能](#)を参照してください。

バグ修正については、[修正された問題](#)を参照してください。

修正された問題

Federated Authentication Service 2407には、修正された問題はありません。

既知の問題

Federated Authentication Service 2407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た問題が解決でき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 \(11.15.0.0\) 用 非商用ソフトウェア開示 \(PDFダウンロード\)](#)
- [FlexNet Publisher ドキュメント補足: FlexNet Publisher 11.15.0 で使用されているサードパーティおよびオープンソースソフトウェア \(PDFダウンロード\)](#)

システム要件

- フェデレーション認証サービス (FAS) は、以下のWindows Serverバージョンでサポートされています。
 - Windows Server 2025、StandardおよびDatacenterエディション
 - Windows Server 2022、StandardおよびDatacenterエディション
 - Windows Server 2019、StandardおよびDatacenterエディション、およびServer Coreオプション
 - Windows Server 2016、StandardおよびDatacenterエディション、およびServer Coreオプション
- Citrixは、他のCitrixコンポーネントがインストールされていないサーバーにFASをインストールすることを推奨します。
- Windows Serverは、登録機関証明書と秘密キーにアクセスできるため、保護されている必要があります。証明書と秘密キーにより、サーバーはドメインユーザー用の証明書を発行できます。サーバーは、発行されたドメインユーザー証明書と秘密キーにもアクセスできます。
- FASの[PowerShellコマンドレット](#)には、FASサーバーにWindows PowerShell 64ビットがインストールされている必要があります。
- ユーザー証明書を発行するには、Microsoft Enterprise証明機関またはその他の検証済み証明機関 (CA) が必要です。以下の非Microsoft PKIプロバイダーは、FASで使用するためのソリューションを検証済みです。これらの検証に関するサポートについては、ベンダーにお問い合わせください。
 - キーファクター コマンド
 - セクティゴ サーティフィケート マネージャー
 - ベナフィ ゼロタッチ PKI
 - HDI PKIaaS (ベナフィ)
 - エントラスト WNES
 - AppViewX
 - エバートラスト ホライズン CLM
 - オープントラスト PKI

- IDノミック PKI-3
- デジサート オートエンロールメント サーバー
- Microsoft以外のCAでFASを使用する場合のサポートとガイダンスについては、関連するPKIプロバイダーにお問い合わせください。
- Microsoft以外の認証局の場合、以下を確認してください。
 - 認証局 (CA) が登録サービスとしてActive Directoryに登録されていること。
 - CA証明書がドメインコントローラーのNTAuthストアにあること。詳細については、[サードパーティの認証局 \(CA\) 証明書をエンタープライズNTAuthストアにインポートする方法](#)を参照してください。
- 詳細については、[展開ガイド: Citrix Federated Authentication ServiceとSectigo MS Agent](#)を参照してください。

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

- 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をVDAに適用します。詳細については、「グループポリシーの構成」([/ja-jp/federated-authentication-service/2407/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、「セキュリティに関する考慮事項」([/ja-jp/federated-authentication-service/2407/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をインストールする (FAS)
2. StoreFrontストアでFASプラグインを有効にする
3. Delivery Controllerを構成する
4. グループポリシーを構成する
5. FAS管理コンソールを使用して、次の操作を行います。
 - a. 証明書テンプレートを展開する
 - b. 証明機関をセットアップする
 - c. FASが証明機関を使用することを承認する
 - d. ルールを構成する
 - e. FASをCitrix Cloudに接続する (オプション)

フェデレーション認証サービスをインストールする

セキュリティのため、Citrixではフェデレーション認証サービス (FAS) を専用サーバーにインストールすることをお勧めします。このサーバーは、ドメインコントローラーまたは証明機関と同様の方法で保護する必要があります。FASは、次のいずれかから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
- スタンドアロンのFASインストーラーファイル（[Citrix Downloads](#)でMSIファイルとして入手可能）。

これらは次のコンポーネントをインストールします。

- フェデレーション認証サービス
- 高度なFAS構成のためのPowerShellスナップインコマンドレット
- FAS管理コンソール
- FASグループポリシーテンプレート (CitrixFederatedAuthenticationService.admx/adml)

- 証明書テンプレートファイル
- パフォーマンスカウンターとイベントログ

FASのアップグレード

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

- インプレースアップグレードを実行すると、すべてのFASサーバー設定が保持されます。
- FASをアップグレードする前に、FAS管理コンソールを必ず閉じてください。
- 常に少なくとも1つのFASサーバーが利用可能であることを確認してください。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インストーラーまたはスタンドアロンのFASインストーラーファイルからFASをインストールします。

StoreFrontストアでFASプラグインを有効にする

注:

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

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以下の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、以下のPowerShellスクリプトを使用します。

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

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

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

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

Delivery Controller™を構成する

注:

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

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

グループポリシーを構成する

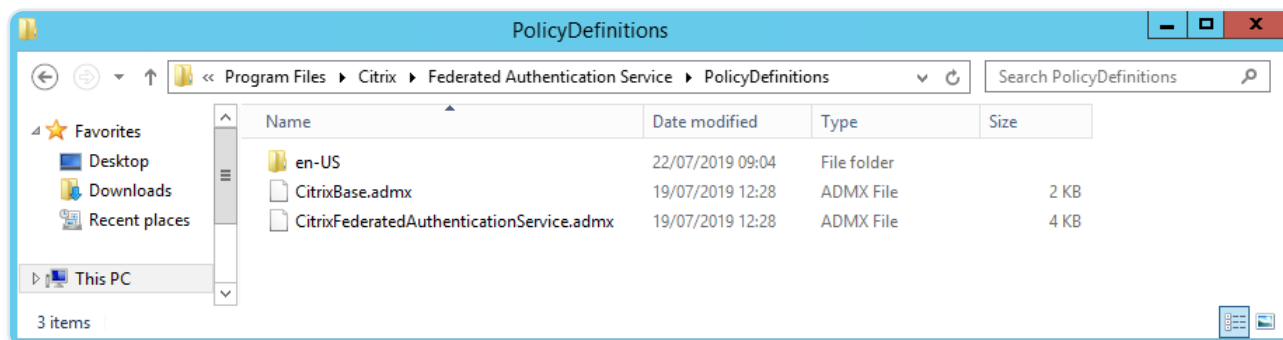
FASをインストールした後、インストールで提供されるグループポリシーテンプレートを使用して、グループポリシー内のサーバーの完全修飾ドメイン名 (FQDN) を指定します。

重要:

チケットを要求するStoreFrontサーバーと、チケットを引き換えるVirtual Delivery Agents (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の構成が同一である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の単一ポリシーを構成します。ただし、これは必須ではありません。StoreFrontサーバー、VDA、およびFAS管理コンソールを実行しているマシンが同じFQDNのリストを参照している限り、FASは機能します。ステップ6を参照してください。

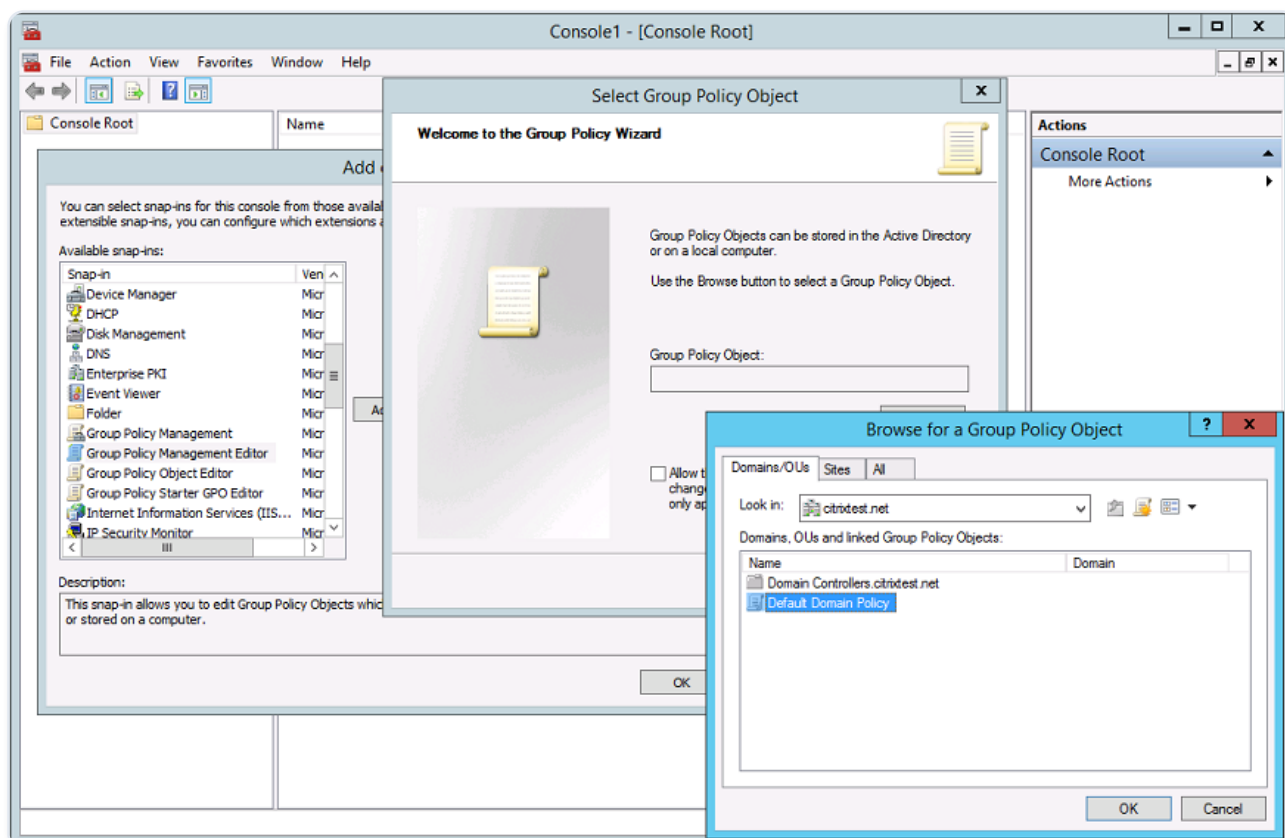
ステップ1. FASをインストールしたサーバーで、C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admxおよびCitrixBase.admxファイルと、en-USフォルダーを見つけます。



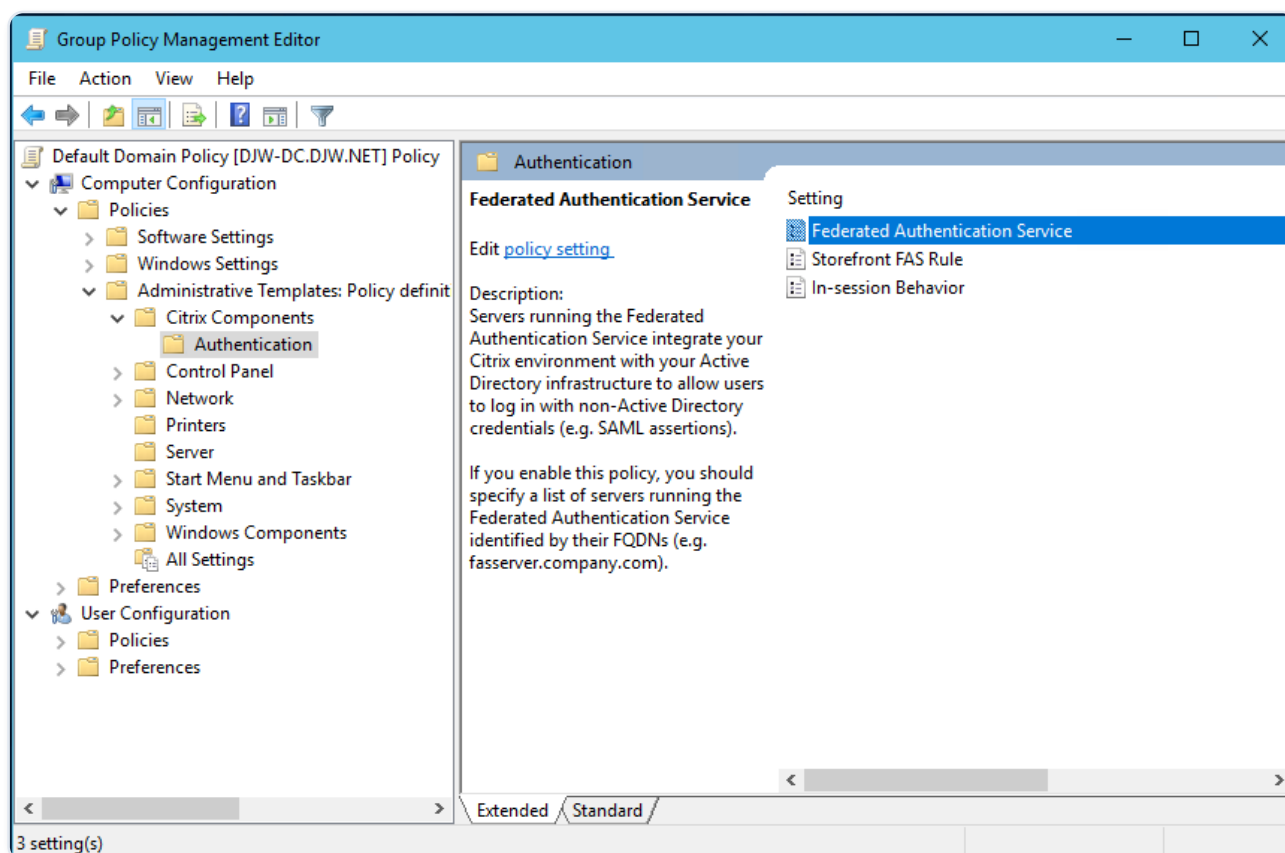
ステップ2. これらのファイルをドメインコントローラーにコピーし、C:\Windows\PolicyDefinitionsおよびen-USサブフォルダーに配置します。

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

グループポリシーオブジェクトの入力を求められたら、**参照**を選択し、**既定のドメインポリシー**を選択します。または、任意のツールを使用して、環境に適したポリシーオブジェクトを作成して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。



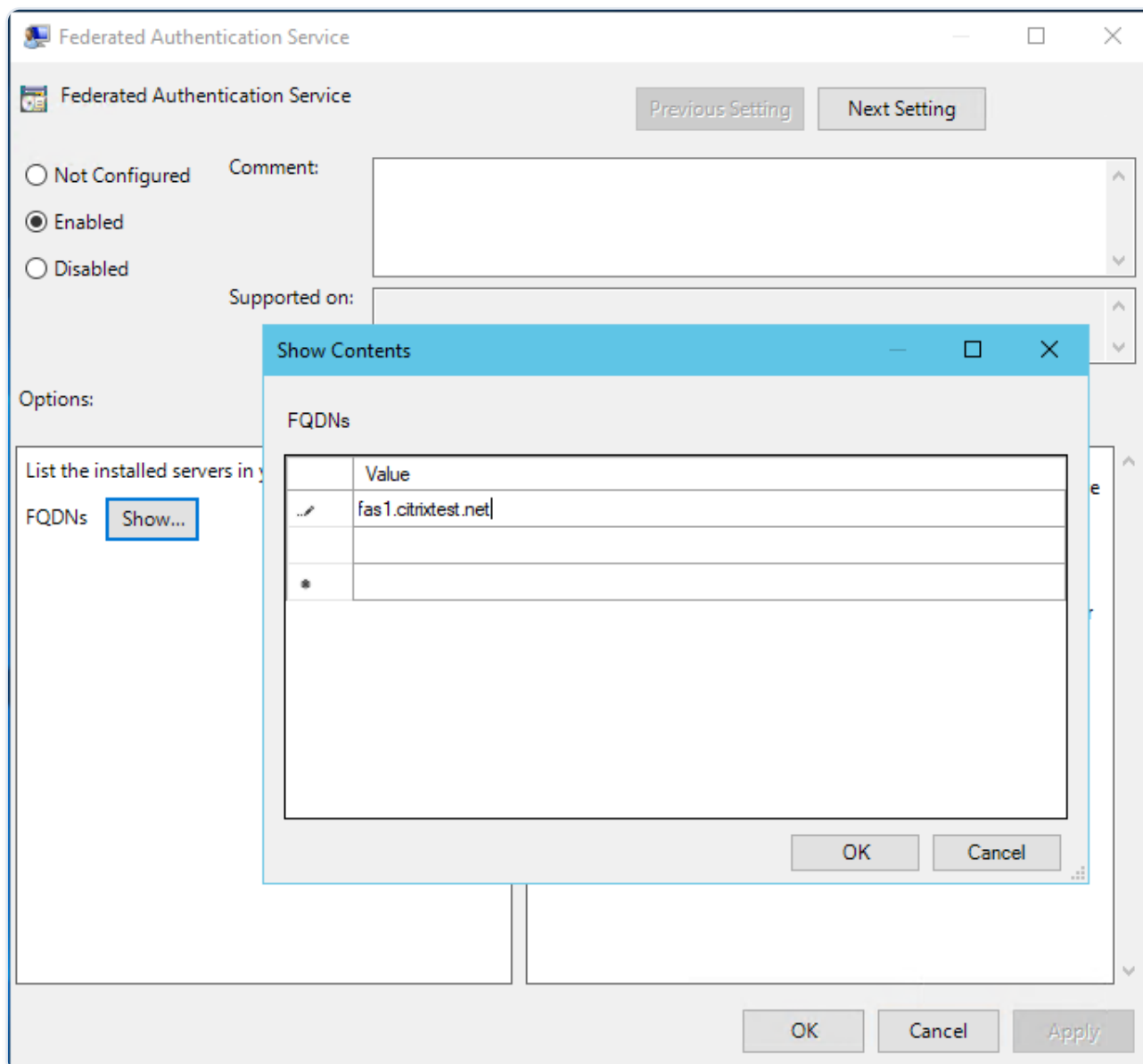
ステップ4. コンピューターの構成/ポリシー/管理用テンプレート/Citrixコンポーネント/認証にあるフェデレーション認証サービスポリシーに移動します。



注：

フェデレーション認証サービスポリシー設定は、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、フェデレーション認証サービスポリシー設定は、**管理用テンプレート > Citrixコンポーネント > 認証フォルダー**に表示されます。

ステップ5. フェデレーション認証サービスポリシーを開き、**有効**を選択します。これにより、表示ボタンを選択できるようになり、FASサーバーのFQDNを構成します。



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

セッション内の動作

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、インセッション証明書、同意、およびロック時の切断をサポートします。インセッション証明書は、このポリシーが有効になっている場合かつ、証明書の作成に使用されたFASルールでインセッション使用が許可されている場合にのみ利用できます。「[ルールを構成する](#)」を参照してください。

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の実行が停止します。

プロンプトスコープ

このポリシーが有効になっている場合、**プロンプトスコープ**は、アプリケーションがインセッション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。3つのオプションがあります。

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

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

同意タイムアウト

このポリシーが有効になっている場合、**同意タイムアウト**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になっている場合、ユーザーが画面をロックすると、ユーザーのセッションは自動的に切断されます。この動作は、「スマートカード取り外し時の切断」ポリシーに似ています。ユーザーがActive Directoryログオン資格情報を持っていない場合に、この機能を使用します。

注：

ロック時の切断ポリシーは、VDA上のすべてのセッションに適用されます。

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インターフェイスはより高度なオプションを提供します。FAS PowerShellコマンドレットの詳細については、[PowerShellコマンドレット](#)を参照してください。

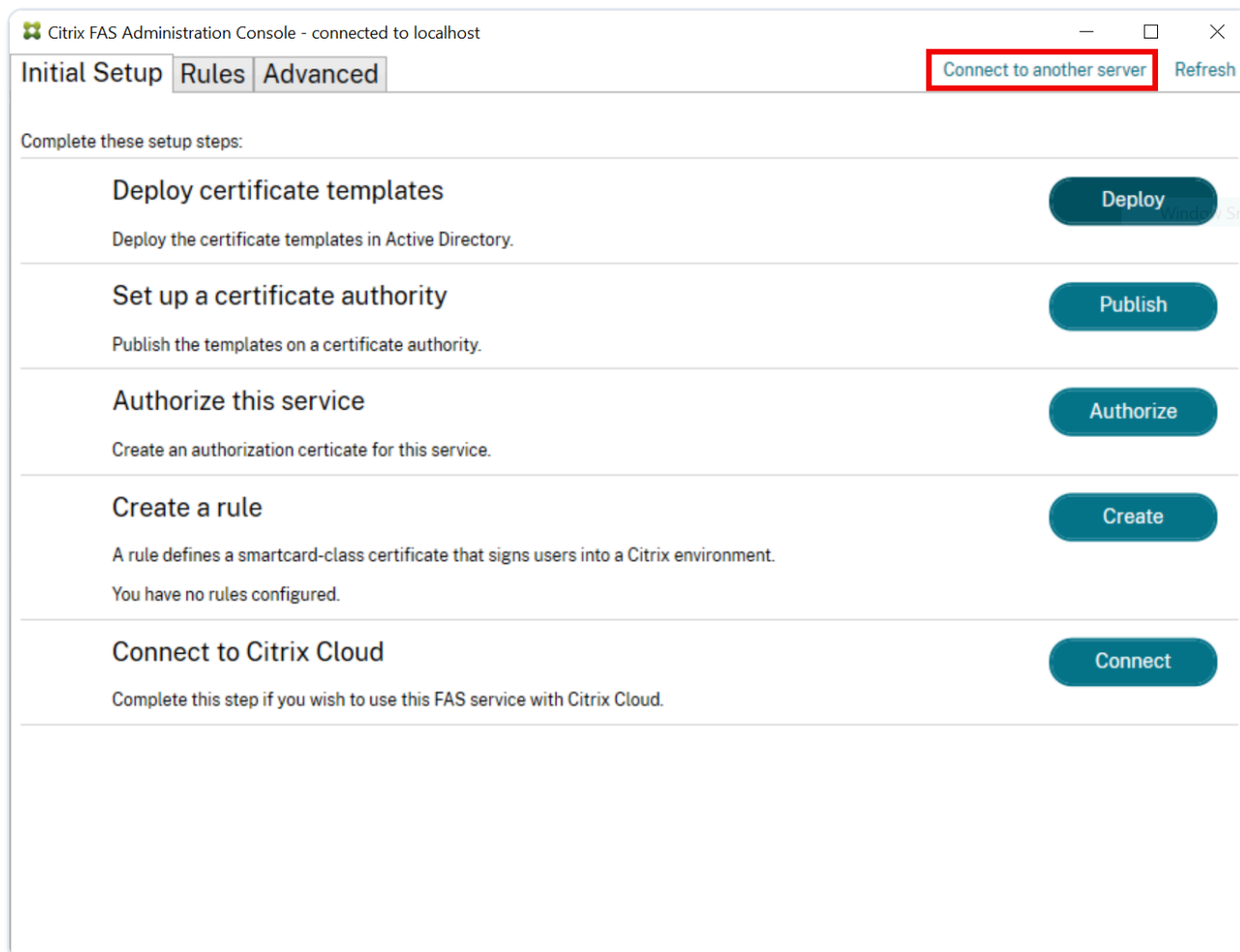
FAS管理コンソールはFASの一部としてインストールされます。アイコン（Citrix Federated Authentication Service）はスタートメニューに配置されます。

管理コンソールを初めて使用する際には、以下のプロセスを実行するようにガイドされます。

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

OS構成ツールを使用して、一部の手順を手動で完了することもできます。

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



証明書テンプレートを展開する

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

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

これらのテンプレートはActive Directoryに登録する必要があります。**Deploy**ボタンをクリックし、次に**OK**をクリックします。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/deploy-cert-templates.png)

テンプレートの設定は、FASとともにインストールされる拡張子.certificatetemplateを持つXMLファイルにあります。

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

証明書テンプレートフォルダー。(/en-us/federated-authentication-service/2407/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次のPowerShellコマンドを実行できます。

```
$template =  
[System.IO.File]::ReadAllBytes("$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証明書サービスを展開する方法については、Microsoftのドキュメントを参照してください。

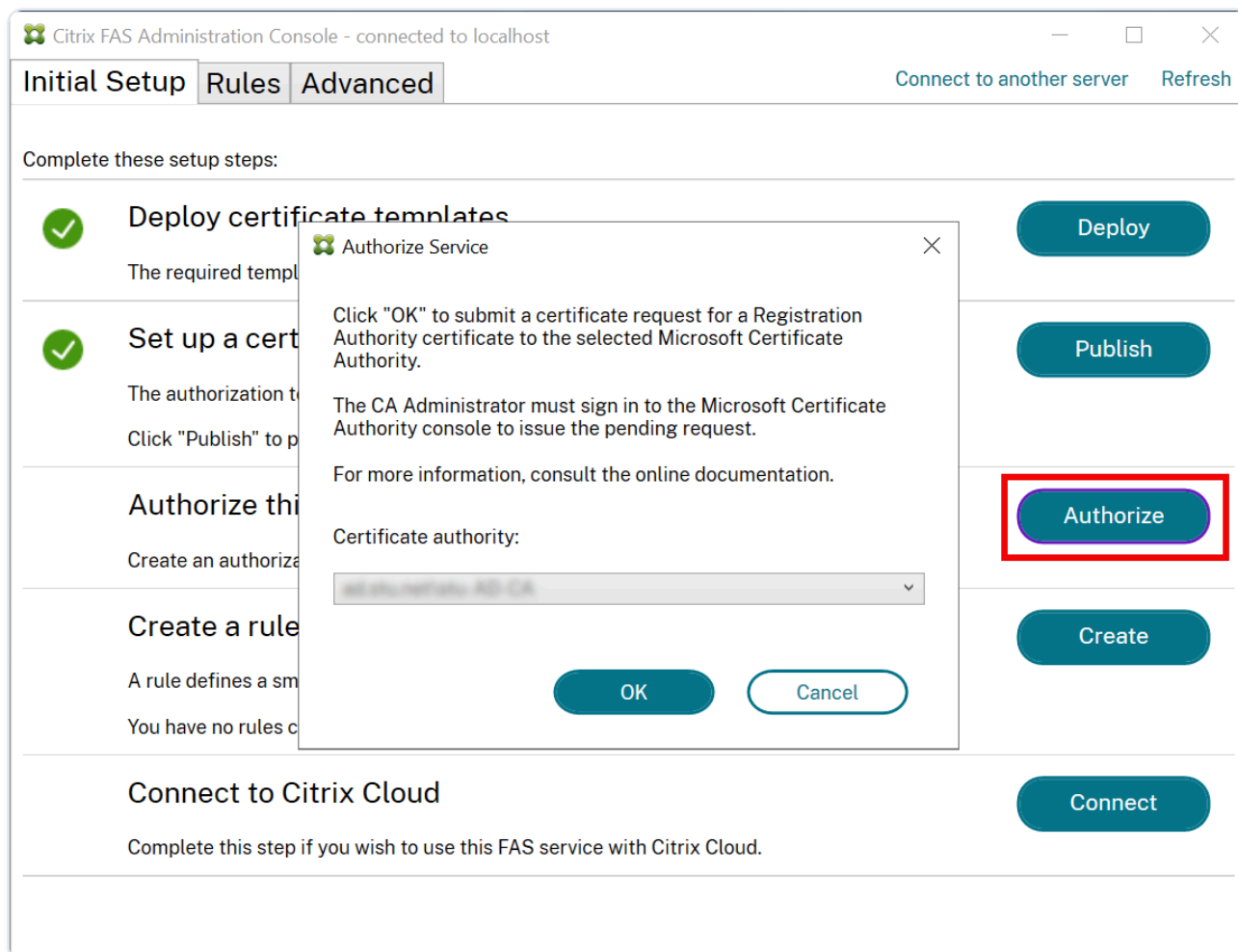
証明機関を管理する権限を持つユーザーは、少なくとも1つのサーバーにテンプレートを公開する必要があります。それらを公開するには、**証明機関のセットアップ**を使用します。

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/setup-cert-authority.png)

フェデレーション認証サービスを承認する

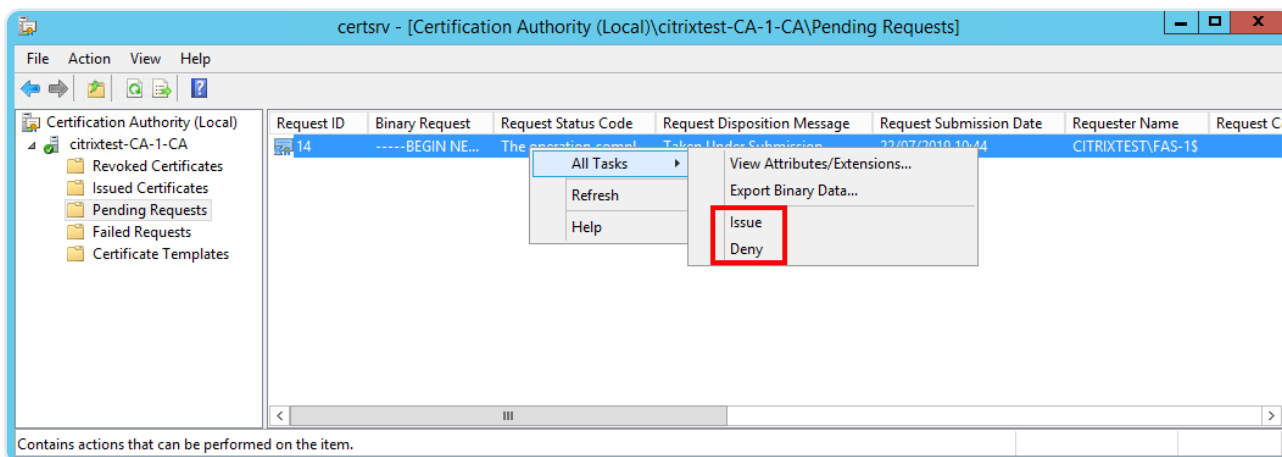
この手順により、FASの承認が開始されます。管理コンソールは Citrix_RegistrationAuthority_ManualAuthorization テンプレートを使用して証明書要求を生成し、その後、そのテンプレートを公開している証明機関のいずれかに送信します。



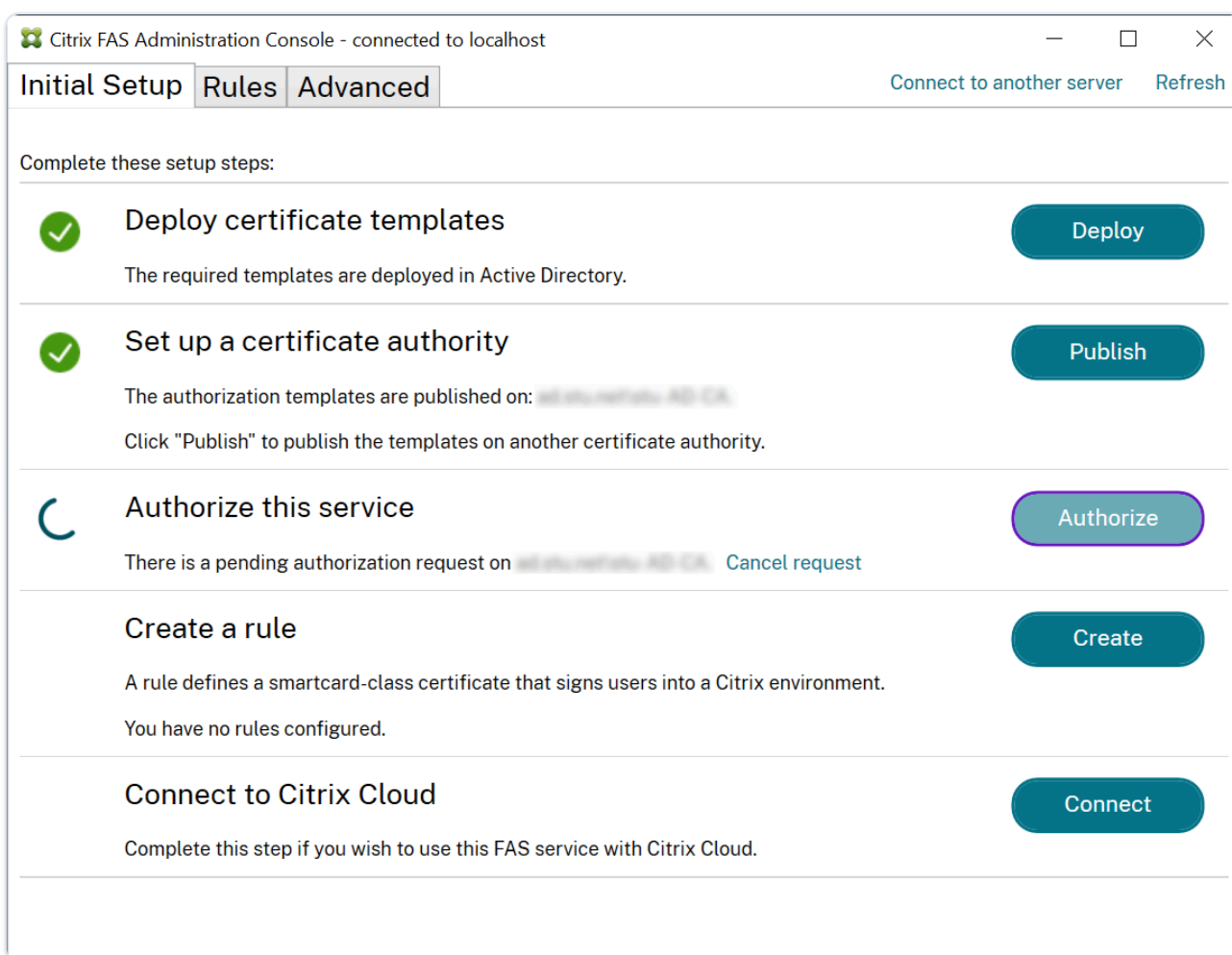
リクエストが送信されると、Microsoft Certification Authority コンソールの **Pending Requests** リストに、FAS マシン アカウントからの保留中のリクエストとして表示されます。FAS の構成を続行する前に、証明機関管理者はそのリクエストを発行または拒否する必要があります。

管理者が **Issue** または **Deny** を選択するまで、FAS 管理コンソールにはビジー状態の「スピナー」が表示されます。

Microsoft Certification Authority コンソールで、**All Tasks** を右クリックし、証明書要求に対して **Issue** または **Deny** を選択します。**Issue** 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。**Deny** を選択すると、コンソールにエラーメッセージが表示されます。



FAS管理コンソールは、このプロセスが完了したことを自動的に検出します。これには数分かかる場合があります。



ルールの構成

FASは、StoreFrontの指示に従って、VDAログオンおよびセッション内使用の証明書の発行を承認するためにルールを使用します。

各ルールは以下を指定します。

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

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

異なる証明書テンプレートや証明機関を参照するカスタムルールをさらに作成し、異なるプロパティと権限を持つように構成できます。これらのルールは、異なるStoreFrontサーバーまたはWorkspaceで使用するように構成できます。Group Policy Configuration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**」をクリックして（または「ルール」タブで「**ルールの作成**」をクリックして）、ルール作成ウィザードを開始し、ルールを作成するための情報を収集します。「ルール」タブには、各ルールの概要が表示されます。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/user-rules.png)

ウィザードは次の情報を収集します。

テンプレート: ユーザー証明書の発行に使用される証明書テンプレートです。これはCitrix_SmartcardLogonテンプレート、またはその変更されたコピーである必要があります（[証明書テンプレート](#)を参照）。

証明機関: ユーザー証明書を発行し、テンプレートを公開する証明機関です。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「テンプレート利用可能」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場合（デフォルト、*推奨*）—証明書はログオンまたは再接続にのみ使用され、ユーザーは認証後に証明書にアクセスできません。
- **セッション内使用を許可**が選択されている場合—ユーザーは認証後に証明書にアクセスできます。ほとんどのお客様は、このオプションを選択すべきではありません。イントラネットの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セッション内のWebサーバーへのTLS認証が必要な場合、Internet Explorerはその証明書を使用できます。

アクセス制御: 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た、信頼できるStoreFrontサーバーマシンのリストです。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:

「**アクセス制御**」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、アクセス制御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」許可）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。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/storefront-servers.png)

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を介して証明書を発行できるユーザーのリスト。

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

注:

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/vdas.png)

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/allowed-users.png)

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/rule-created.png)

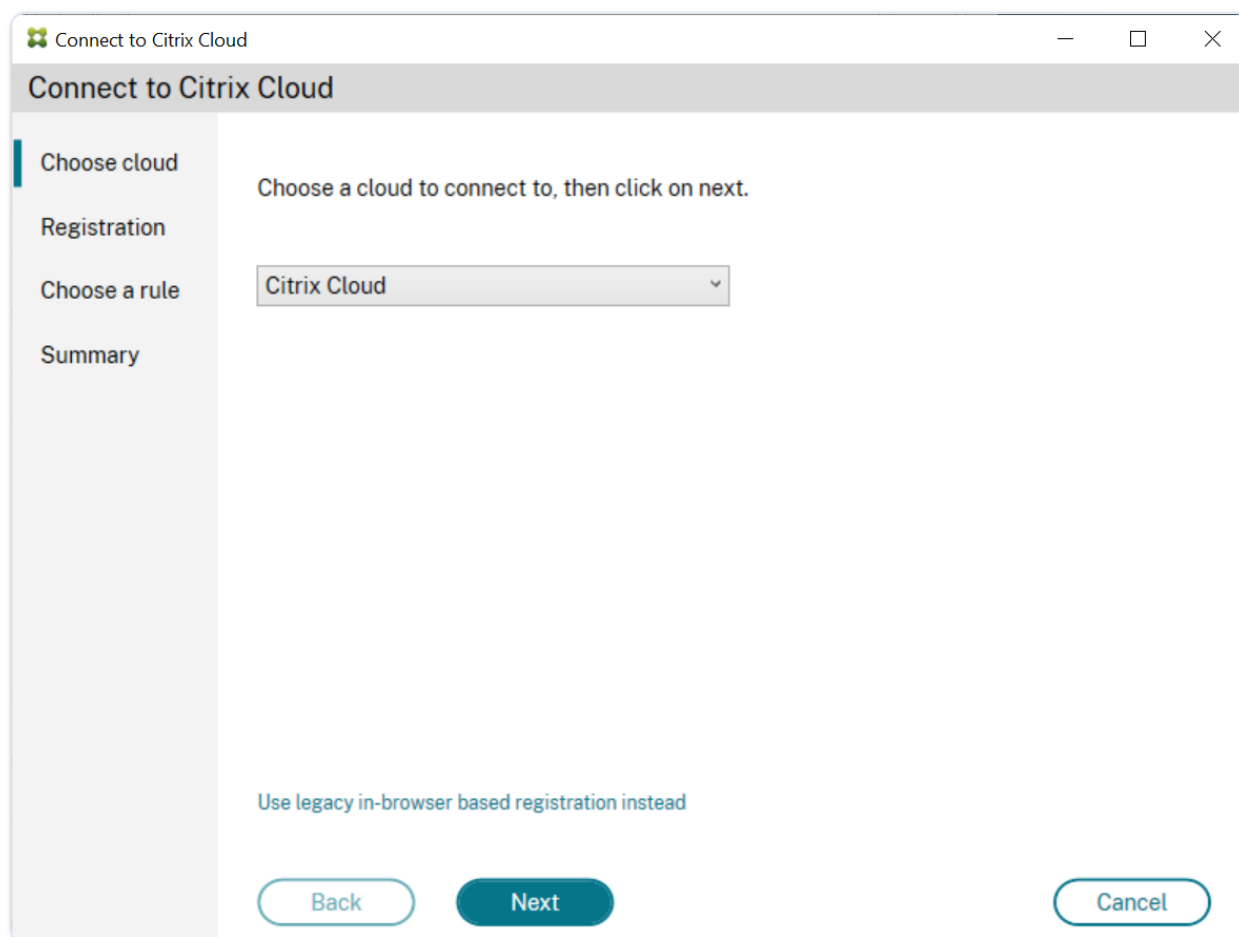
Citrix Cloudへの接続

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

初期設定(/en-us/federated-authentication-service/2407/media/connect-cloud-initial-setup.png)

2. 接続するクラウドを選択し、**次へ**をクリックします。



Connect to Citrix Cloud

Connect to Citrix Cloud

Choose cloud

Registration

Choose a rule

Summary

Choose a cloud to connect to, then click on next.

Citrix Cloud

Use legacy in-browser based registration instead

Back Next Cancel

注

プレビューでは、**Citrix Cloud**のみが利用可能です。

3. ウィンドウに一意的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。

Connect to Citrix Cloud

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.cloudconnect.citrix.com/identity/api/access/product-registration> Copy

Confirmation Code:

DDQESDAE Copy

Waiting for confirmation...

Back Next Cancel

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

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:

Copy

Confirmation Code:

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。続行をクリックし、確認ウィンドウを閉じます。
6. **ルール**の**選択**セクションで、既存のルールを使用するか、新しいルールを作成します。次へをクリックします。

Connect to Citrix Cloud

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

Connect to Citrix Cloud

Choose cloud

Registration

Choose a rule

Summary

Summary

Customer: [blurred]

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Resource Locationsページに表示します。

注

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

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。

テナント顧客向けにフェデレーション認証サービスを有効にする

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

前提条件

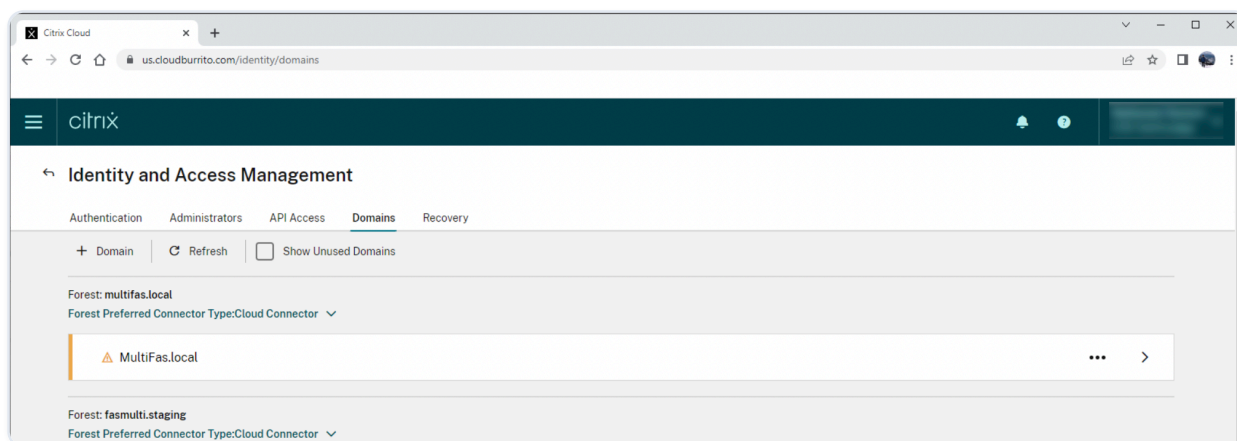
- Citrix Cloud のドメインとリソースの場所に管理者アクセス権があること。詳細については、「[管理者権限の変更](#)」を参照してください。
- テナントと MSP の関係が設定されていること。詳細については、「[Citrix Service Provider 向け Citrix DaaS](#)」を参照してください。

MSP 顧客を構成する

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

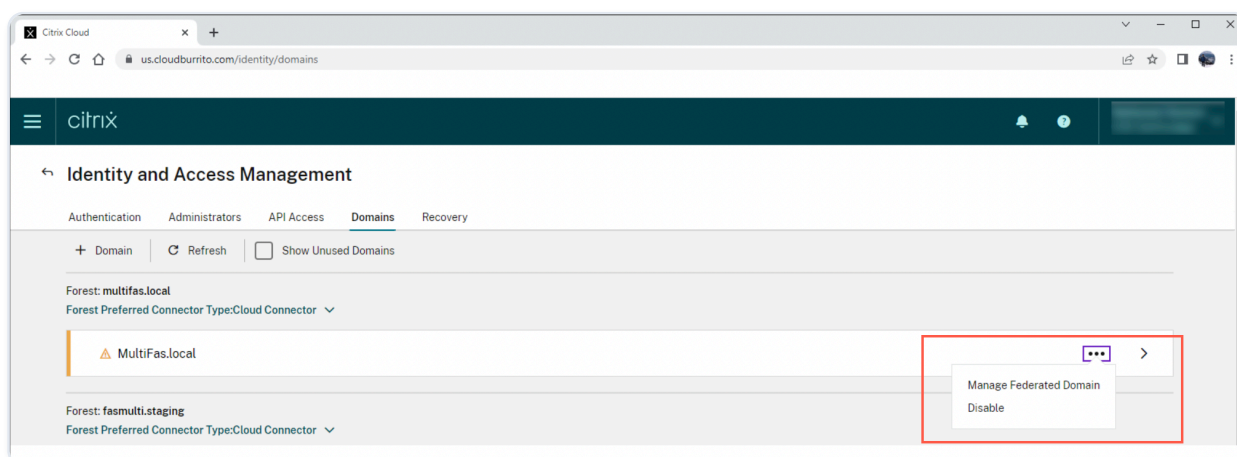
[Cloud Connector](#) をインストールして、オンプレミスインフラストラクチャを Citrix Cloud に接続します。

オンプレミスのドメインコントローラーに関連付けられているドメインが、**[ID とアクセス管理]** > **[ドメイン]** で利用可能であることを確認します。



2. ドメインをテナントにフェデレートします。

ドメインを選択し、ドロップダウンメニュー (...) をクリックして、**「フェデレーションドメインの管理」** をクリックします。



テナントを見つけて + をクリックします。次に、**「適用」** をクリックします。

Add or remove customers to create a federated domain

1 available customers [Add all](#)

Search... Q

FAS Tenant1 with service profile. +

0 federated customers [Remove all](#)

Search... Q

Cancel Apply

3. 関連付けられているドメインがテナントに存在することを確認します。

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

関連付けられているドメインがテナントに存在することを確認します(/en-us/federated-authentication-service/2407/media/fas-verify-domains.png)

MSP顧客に戻ります。

4. FASサーバーをCitrix Cloudにインストールして登録します。

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

5. テナント顧客を構成する

テナント顧客向けにFASを有効にする

- IDプロバイダー (IdP) を構成する

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

- テナント向けにFASを有効にする

Workspace Configuration > Authentication に移動します。設定した認証を選択し、FASを有効にします。

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

既知の問題

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

Azure Active Directory シングルサインオン

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

AD と AAD 間で同期を行い、ユーザーとコンピューターの両方にハイブリッド ID を作成する Azure Active Directory (AAD) の実装は一般的です。この記事では、FAS を使用している場合に VDA セッション内から AAD への SSO を実現するために必要な追加構成について説明します。これにより、ユーザーは再認証なしで AAD で保護されたアプリケーションにアクセスできるようになります。

注:

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

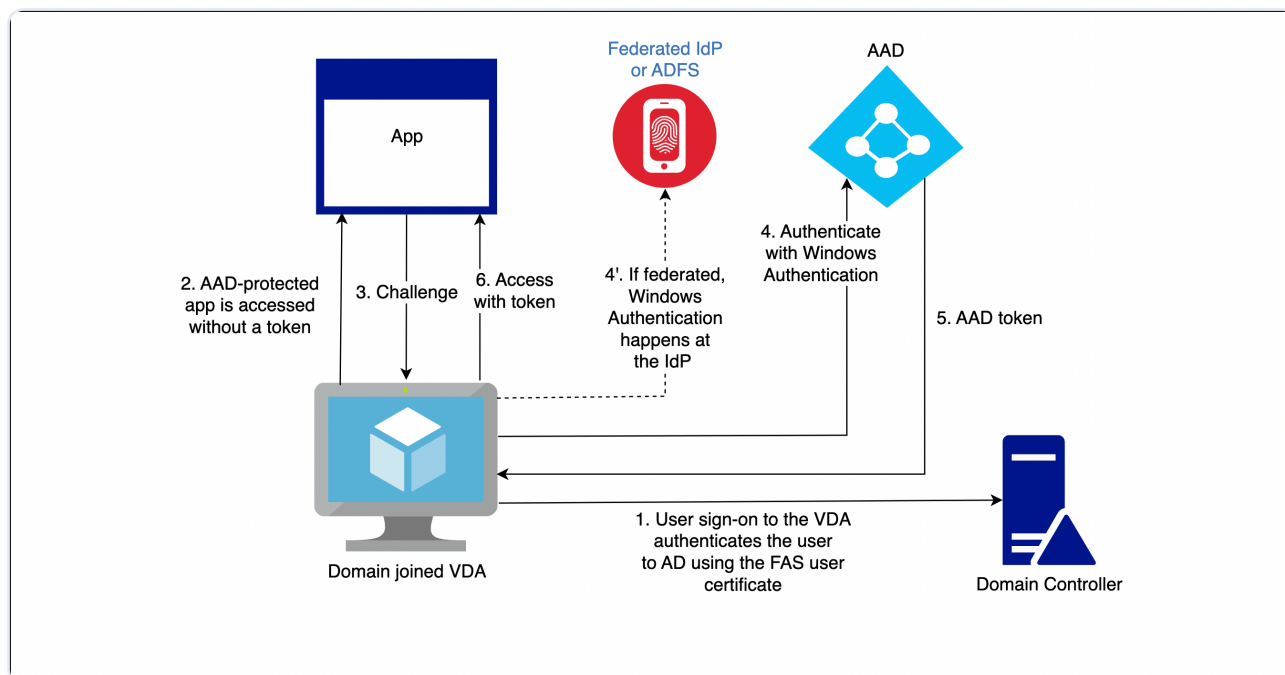
AAD SSO の手法を次の表にまとめます。

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

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

ドメイン参加済み VDA

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



詳細な内容は、AAD ドメインがマネージドであるかフェデレーションされているかによって異なります。

マネージド AAD ドメインの設定については、[シームレスシングルサインオン](#) を参照してください。

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

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

注:

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

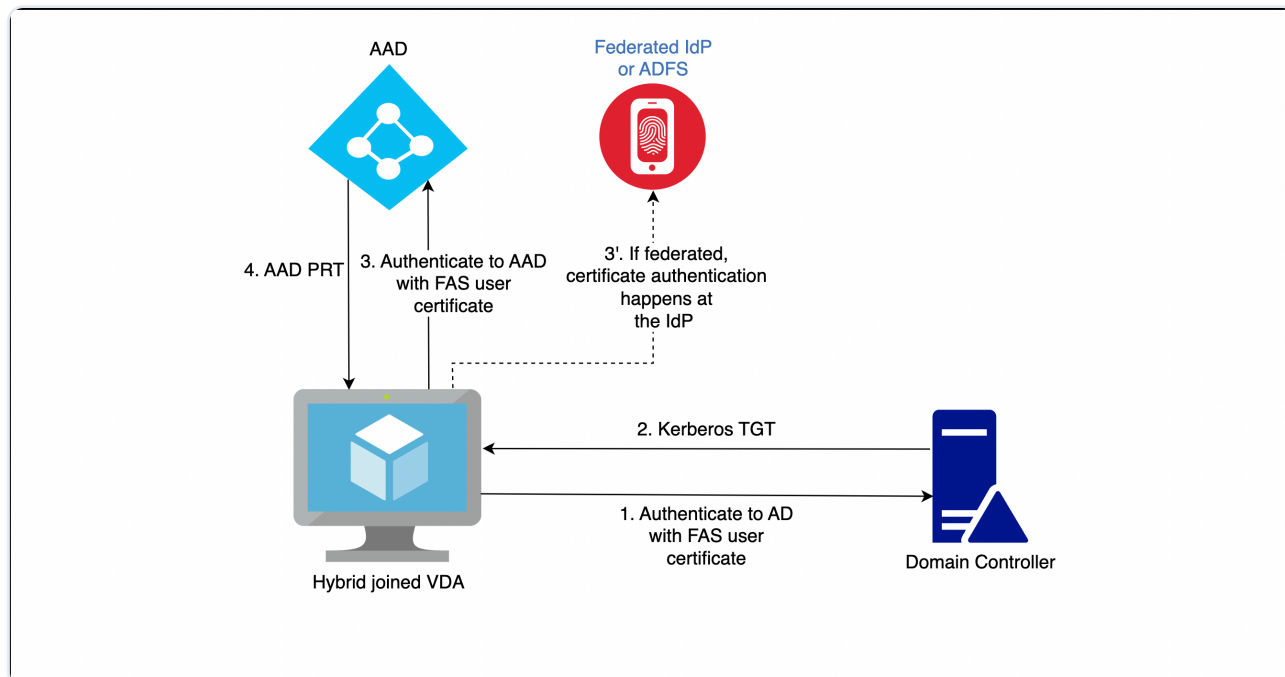
ハイブリッド参加済み VDA

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

- AD リソースへの認証のための Kerberos チケット保証チケット (TGT)
- AAD リソースへの認証のための プライマリ更新トークン (PRT)

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

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



詳細については、AADドメインが管理されているかフェデレーションされているかによって異なります。

管理対象のAADドメインの場合、AAD CBAを構成します。詳細については、「[Azure AD 証明書ベースの認証の概要](#)」を参照してください。VDAは、ユーザーのFAS証明書を使用してAAD CBAでユーザーをAADに認証します。

注:

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

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

サードパーティのIDプロバイダーにフェデレーションされたAADドメインの場合、同様のソリューションが存在する可能性があります。IDプロバイダーはWS-Trust *certificatemixed* エンドポ

イントを実装する必要があります。サポートについては、IDプロバイダーにお問い合わせください。

認証局の構成

この記事では、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 の基本的な知識が必要です。

FAS で使用する複数の CA サーバーをセットアップする

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

2つのCAを持つルールを編集します。(/en-us/federated-authentication-service/2407/media/edit-rule-2cas.png)

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）を公開している必要があります。

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

注:

すべてのCAに対して[このサービスを承認する](#)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 認証局を構成する

FAS は DCOM を使用して Microsoft CA にアクセスします。DCOM はポート 135 を使用して、サービスがリッスンしているポートを検出します。デフォルトでは、リッスンポートは動的に割り当てられます。これにより、ファイアウォールセキュリティを実装する際に複雑さが生じる可能性があります。そのため、Microsoft は静的ポートを構成する機能を提供しています。Microsoft

CAで静的ポートを構成するには、**スタート > ファイル名を指定して実行 > dcomcnfg.exe** を選択して DCOM 構成パネルを開きます。コンピューター > マイ コンピューター > **DCOM の構成** を展開して、CertSrv Request ノードを表示します。次に、CertSrv Request DCOM アプリケーションのプロパティを編集します。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-caconfig-select-dcom-protocol.png)

「**エンドポイント**」を変更して静的エンドポイントを選択し、TCPポート番号（上記のグラフィックでは900）を指定します。

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

変更を適用するには、Microsoft証明機関を再起動します。

DCOMはRPCポート135を使用してネゴシエーション段階を持つため、FASサーバー（または証明機関を使用する他のマシン）を構成する必要はありません。クライアントがDCOMを使用する必要がある場合、サーバー上のDCOM RPCサービスに接続し、特定のDCOMサーバーへのアクセスを要求します。これにより、ポート900（この例では）が開かれ、DCOMサーバーはクライアントにそのポートへの接続を指示します。

ユーザー証明書を事前生成する

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

Active Directoryユーザーのリストを取得する

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

```
Import-Module ActiveDirectory
```

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

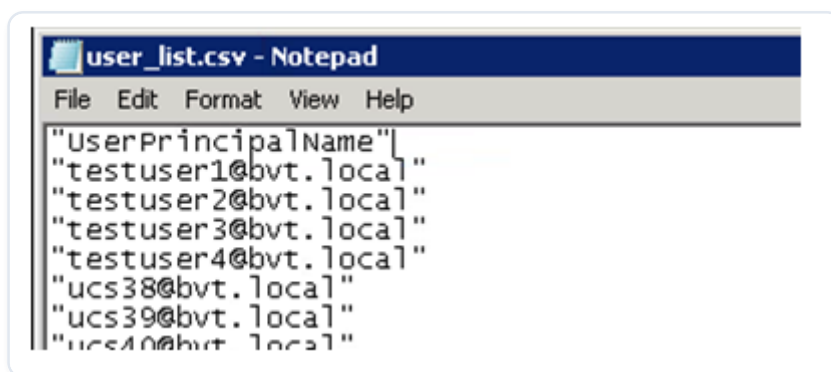
```
$filename = "user_list.csv" # Filename to save
```

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

Get-ADUserは、ユーザーのリストをクエリするための標準的なコマンドレットです。上記の例には、UserPrincipalNameを持ち、アカウントステータスが「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

以下の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 t

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

+ Create rule

Default
hello

Summary

Rule name:hello

Status:OK

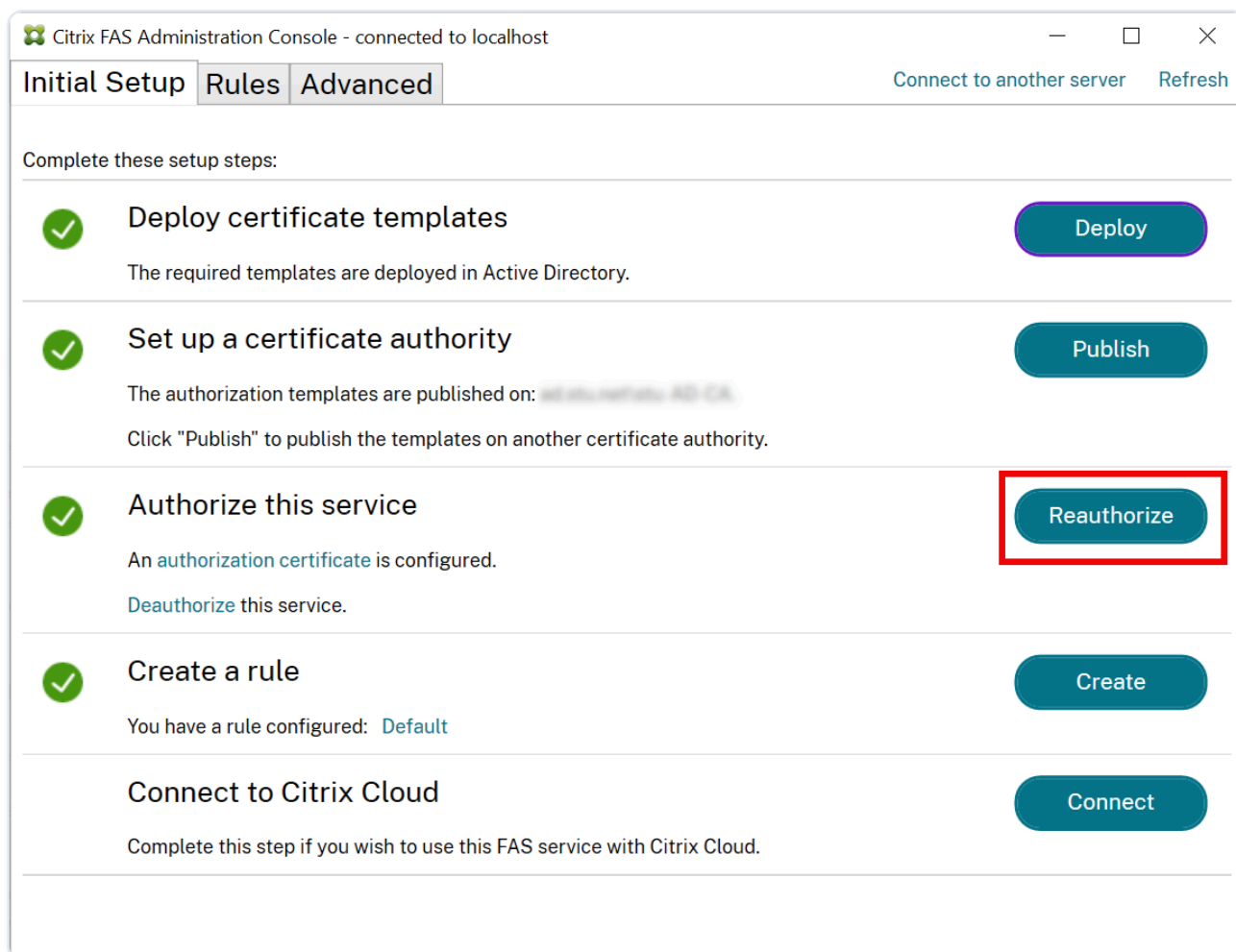
Template:Citrix_SmartcardLogon

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。これは以下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」([/ja-jp/federated-authentication-service/2407/deployment-architectures.html](https://ja-jp/federated-authentication-service/2407/deployment-architectures.html))の記事にまとめられています。
- その他の「ハウツー」記事については、「高度な構成」([/ja-jp/federated-authentication-service/2407/config-manage.html](https://ja-jp/federated-authentication-service/2407/config-manage.html))の記事で紹介されています。

秘密キーの保護

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。関連する秘密キーは、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。

秘密キーには次の2種類があります。

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

実際には、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）の2つの登録機関証明書があります。

フェデレーション認証サービス (FAS) 管理コンソールの「初期セットアップ」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証明書に対する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あり、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、管理者が証明機関で手動で承認する必要があります。証明書がFASサーバーに発行されると、FASはCitrix_RegistrationAuthority_ManualAuthorization証明書を使用して、Citrix_RegistrationAuthority証明書（デフォルトで2年間有効）を自動的に取得します。FASサーバーは、Citrix_RegistrationAuthority証明書を取得するとすぐに、Citrix_RegistrationAuthority_ManualAuthorizationの証明書とキーを削除します。

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

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

- 登録機関証明書とユーザー証明書の秘密キーの両方に対して、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キーには、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キーには、Microsoft Enhanced RSA and AES Cryptographic ProviderまたはMicrosoft Software Key Storage Providerを使用します。
- 登録機関証明書とユーザー証明書の秘密キーの両方に対して、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。

秘密キーの構成設定

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

```
<?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="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>
</configuration>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

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

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

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

値	コメント
トゥルー	CAPI API を使用する
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 Enhanced 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	既定の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	既定のTPMプロバイダー。TPMはユーザーキーには推奨されません。TPMは登録機関キーにのみ使用してください。仮想化環境でFASサーバーを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。仮想化環境でFASサーバーを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の場合にのみ必要)

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

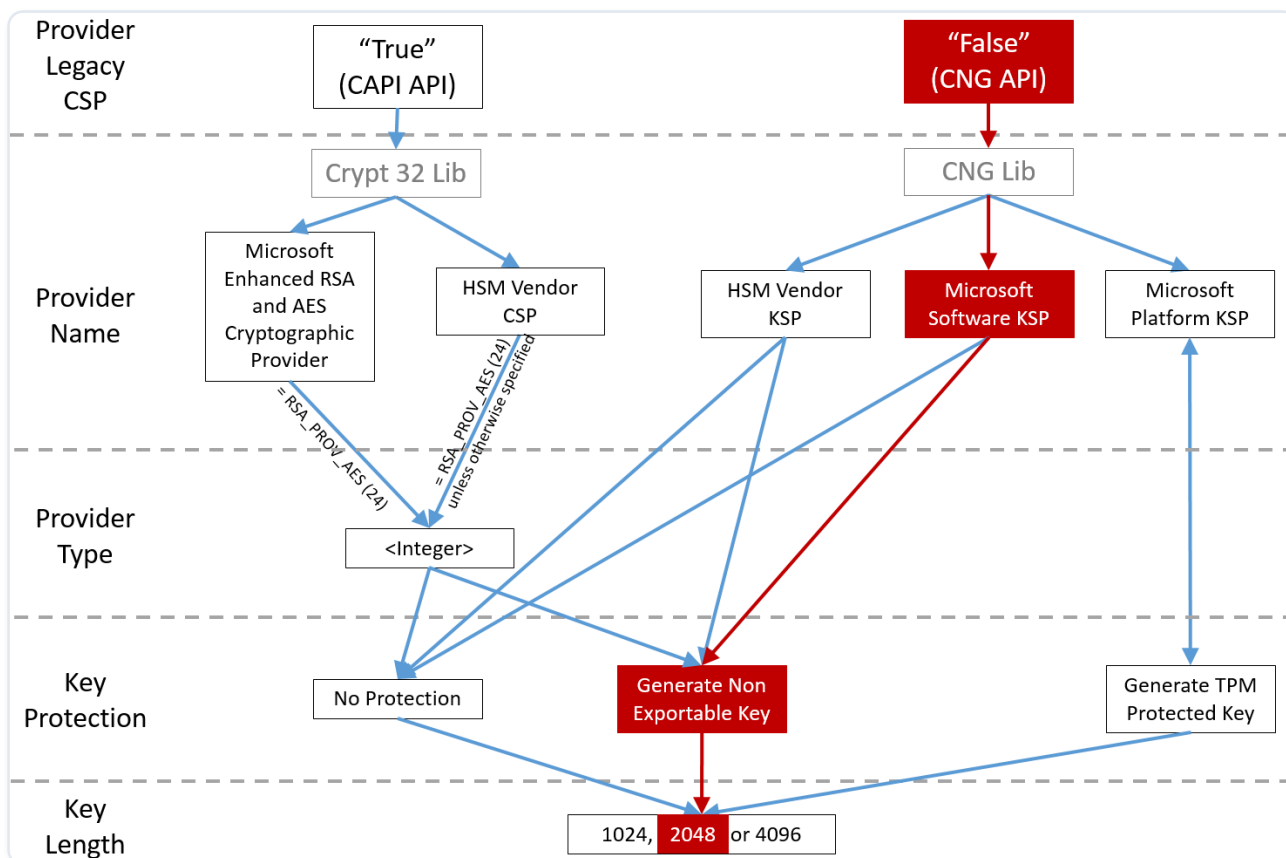
Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (FASが秘密鍵操作を実行する必要がある場合、ここで指定された値を使用します) 秘密鍵の「エクスポート可能」フラグを制御します。ハードウェアでサポートされている場合、TPMキーの保存を許可します。

値	コメント
保護なし	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されています）。



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の構成です。追加の秘密鍵構成は必要ありません。

例 2

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

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

FAS管理コンソールの使用

FAS管理コンソールはオフラインの証明書署名要求を実行できないため、組織が登録機関証明書に対してオンラインの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、証明機関を設定した後、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: 以下の行を次のように変更して、構成ファイルを編集します。

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

ファイルは次のようになります。

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

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

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

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

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

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

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

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value="" / -->
  </appSettings>
</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、次のPowerShellコマンドを使用します。登録機関証明書の秘密キーがTPMに保存されている場合、PrivateKeyProviderフィールドは*Microsoft Platform Crypto Provider*に設定されます。

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

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

手順5： 構成ファイルを次のように編集し直します。

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

注：

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

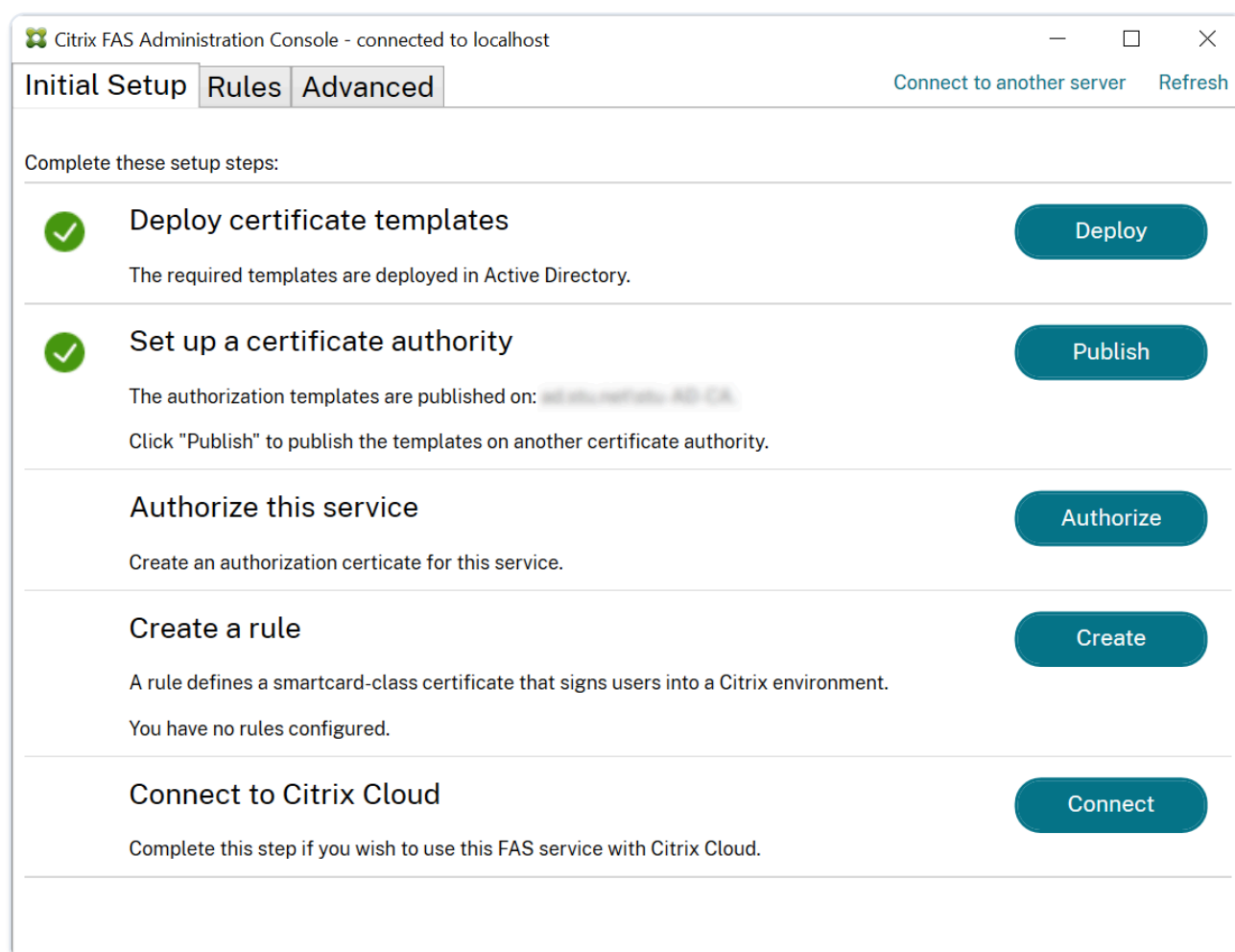
手順6： FASを再起動します。これにより、サービスは構成ファイルを再読み込みし、変更された値を反映します。その後の自動秘密キー操作は、ユーザー証明書キーに影響を与えます。これらの操作は秘密キーをTPMに保存せず、Microsoft Software Key Storage Providerを使用します。

手順7： FAS管理コンソールで**ルールタブ**を選択し、(</ja-jp/federated-authentication-service/2407/install-configure.html>)に記載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の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。

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



手順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

手順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。作成したテンプレートを選択します。

ステップ4: FASサーバーで次のPowerShellコマンドレットを読み込みます。

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

ステップ5: FASサーバーのTPM内でRSAキーペアを生成し、FASサーバーで次のPowerShellコマンドレットを入力して証明書署名要求を作成します。**注:** 一部のTPMはキー長を制限します。デフォルトのキー長は2048ビットです。お使いの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-----
                  [Blurred Certificate Content]
                  -----END CERTIFICATE-----
Status            : WaitingForApproval
```

注:

- ID GUID（この例では「5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39」）は、後続のステップで必要になります。
- このPowerShellコマンドレットは、登録機関証明書の秘密キーを生成するために使用される1回限りの「上書き」として考えてください。
- 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、使用するキー長を決定するためにチェックされます（デフォルトは2048です）。
- この手動のPowerShellによって開始された登録機関証明書の秘密キー操作では、-UseTPMが\$trueに設定されているため、システムはTPMを使用するため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。

キーペアの生成にTPMが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のFASサーバーのWindowsイベントビューアーのアプリケーションログを確認してください。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-privatekeys-eventviewer-applog.png)

注: 「

以下に続きます。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-privatekeys-eventviewer-applog2.png)

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

ステップ 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。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-privatekeys-usmcertreq-notepad.png)

ステップ 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に以下を入力します。

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

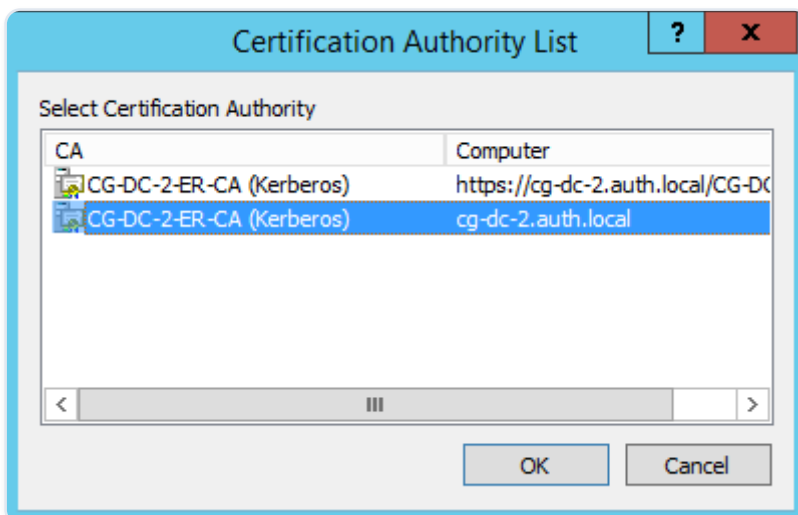
例:

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

次のように表示されます。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-privatekeys-certreq-submit-display.png)

この時点で、認証局リストウィンドウが表示される場合があります。この例の認証局では、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。

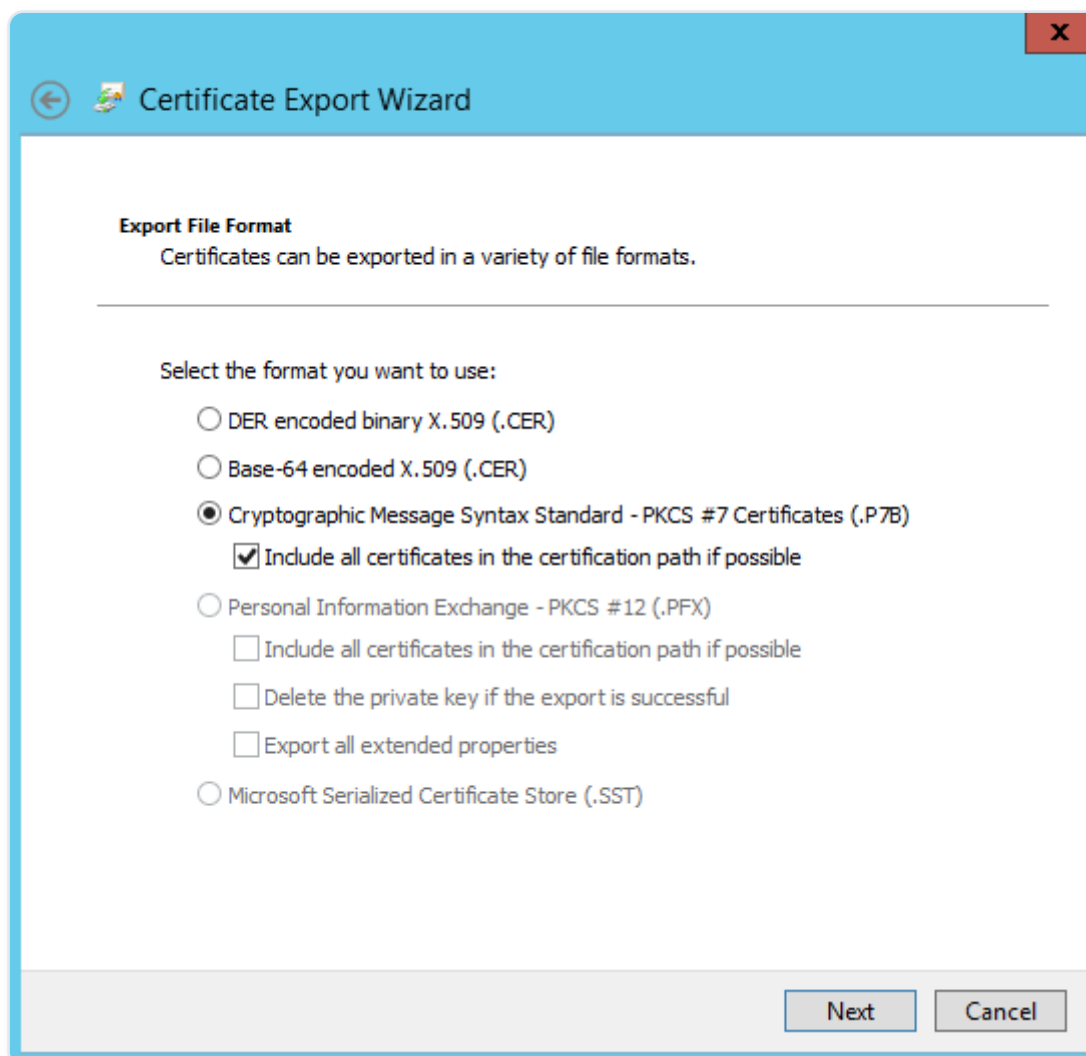


認証局が指定されると、PowerShellにRequestIDが表示されます。

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
{4F76160E-DB0C-4D21-A4FD-2E295D2177C2}
ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

ステップ8： 認証局サーバーで、認証局MMCスナップインの**保留中の要求**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**発行**を選択します。

ステップ9： **発行済み証明書**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。**詳細**タブを選択します。**ファイルへコピー**をクリックします。証明書のエクスポートウィザードが起動します。**次へ**をクリックします。ファイル形式について、以下のオプションを選択します。



形式は「**Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**」である必要があり、「可能な場合は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。

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

例：

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

以下が表示されます。

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

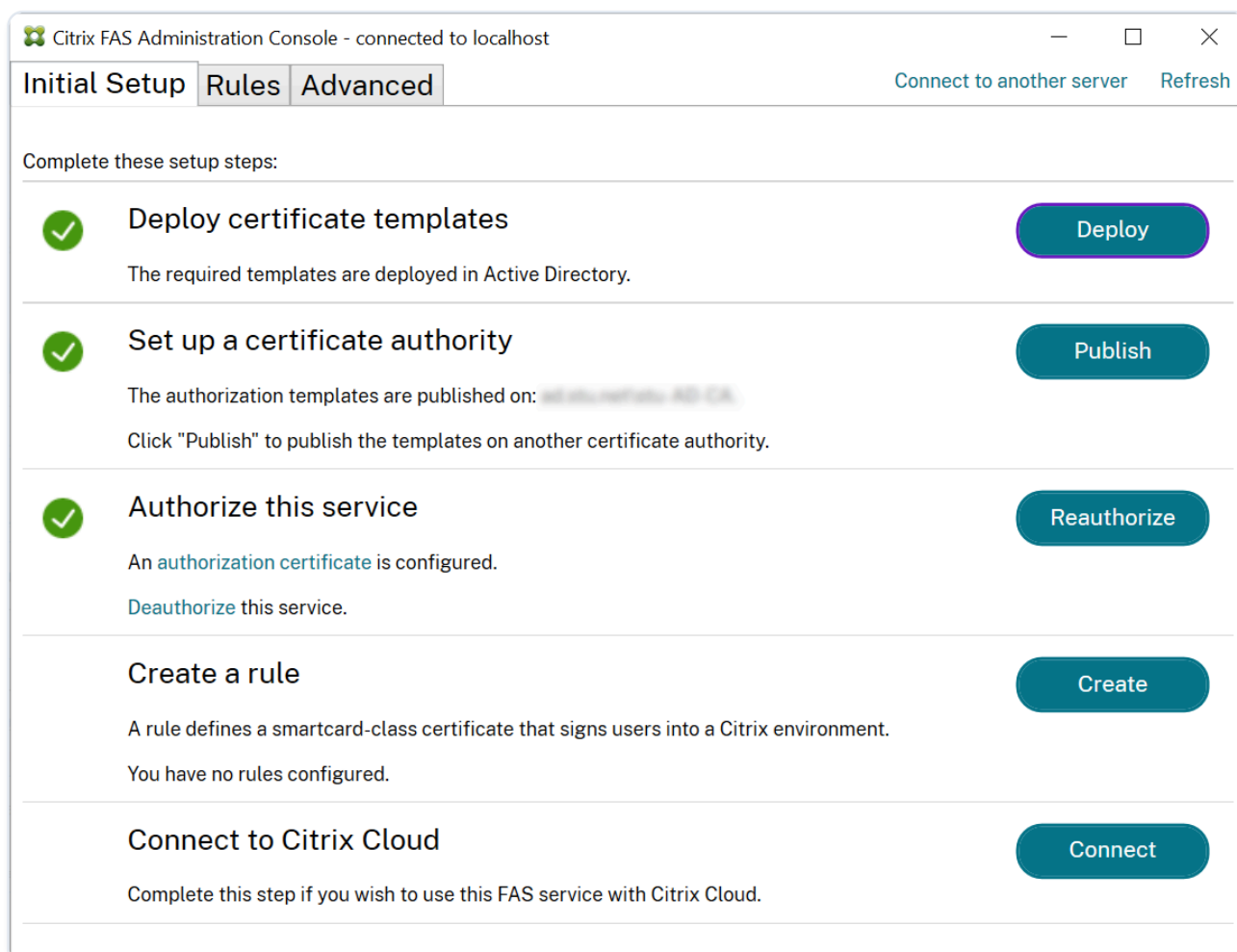
Id                : 74d427ff-c55b-4d6d-87ae-1ff98b0c2705
Address           : [Offline CSR]
TrustArea         : 978816cd-8b2f-4695-8c5d-08bb7df1816b
CertificateRequest :
Status            : Ok
```

登録機関証明書の秘密キーがTPMに正しく保存されていることを確認するには、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 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。

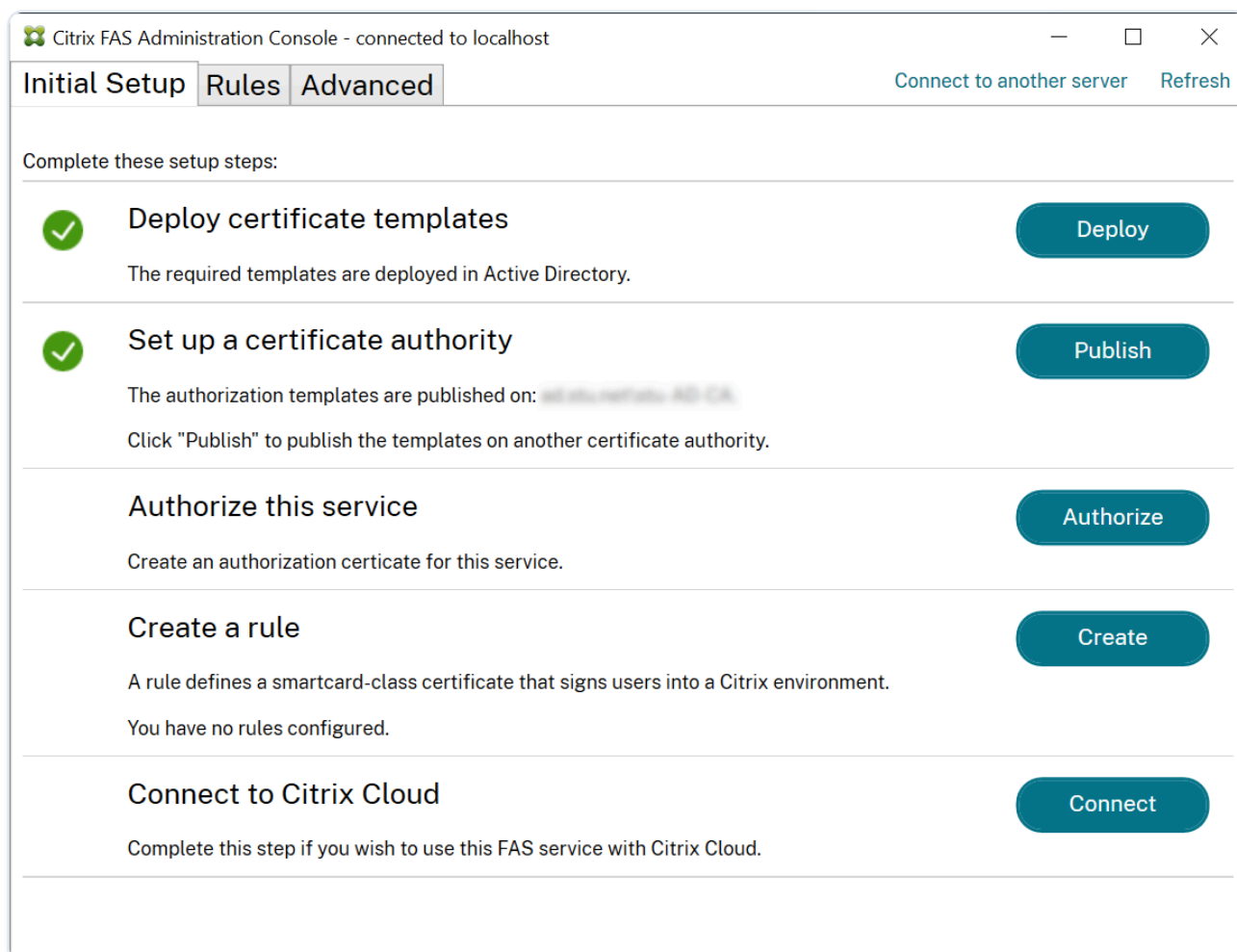
ステップ 13: FAS 管理コンソールで **Rules** タブを選択し、インストールと構成で説明されている設定を編集します。

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、最初の2つのステップ「Deploy certificate templates」と「Set up a certificate authority」のみを完了します。



The screenshot shows the Citrix FAS Administration Console interface. At the top, it says 'Citrix FAS Administration Console - connected to localhost'. Below this are three tabs: 'Initial Setup', 'Rules', and 'Advanced'. To the right of the tabs are two links: 'Connect to another server' and 'Refresh'. Under the 'Initial Setup' tab, there is a section titled 'Complete these setup steps:'. This section contains five items, each with a green checkmark icon, a title, a description, and a button:

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

ステップ 2: HSMのProviderName値が何であるべきかを判断するには、HSMベンダーのドキュメントを参照してください。HSMがCAPIを使用している場合、プロバイダーはドキュメントでCryptographic Service Provider (CSP) と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: 構成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"/></configuration>
```

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

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

ステップ 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。

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

```
[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]
```

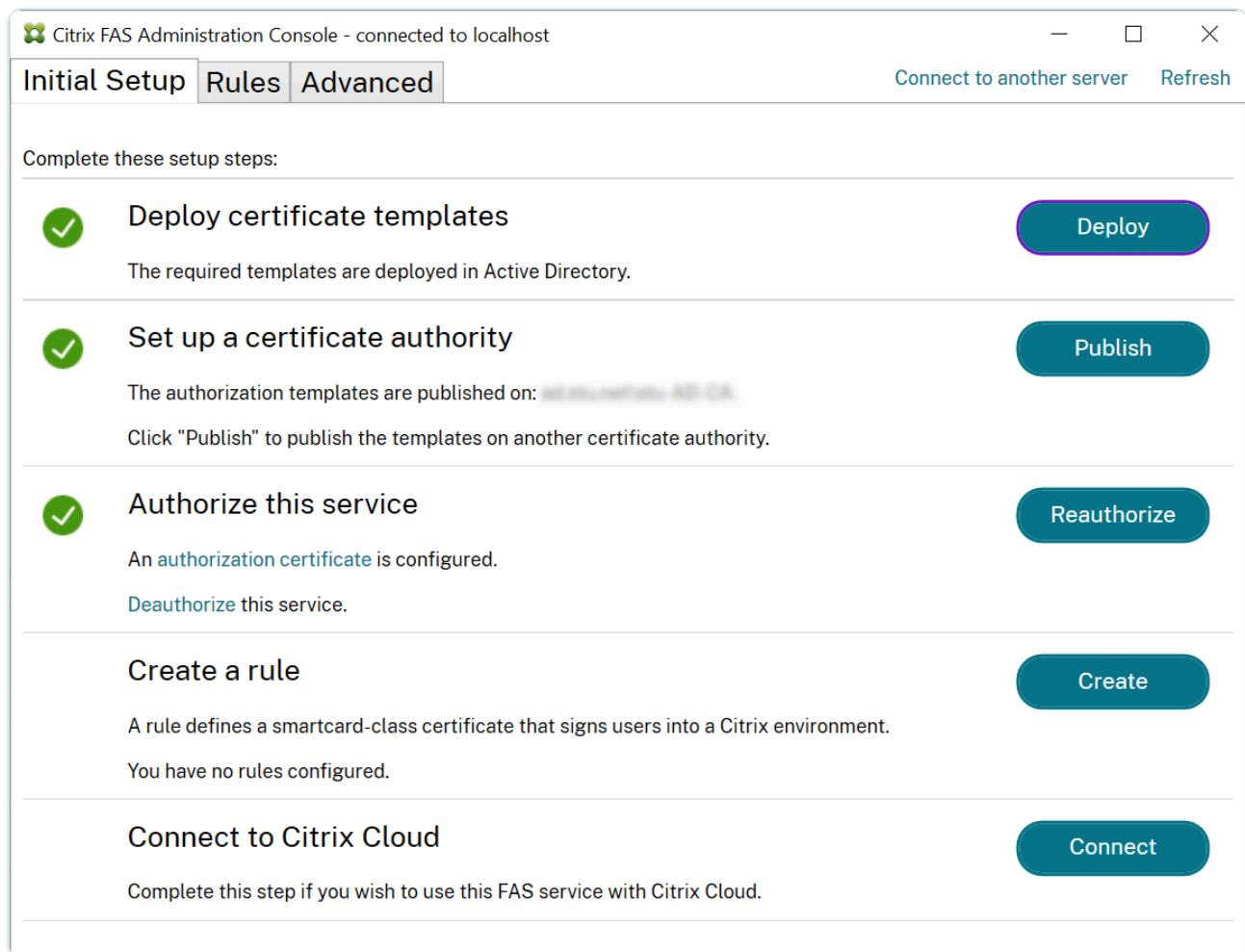
注: [プロバイダー: HSM_Vendor's Key Storage Provider]

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

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\UCSHMS\$	

要求を右クリックし、**発行**を選択します。

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 8: FAS管理コンソールでルールタブを選択し、インストールと構成に記載されているとおり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** :

[illegible]

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。

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

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

```
PS C:\Users\administrator.STU> Get-FasUserCertificate -Address fas.stu.net

ThumbPrint      : 2A81185BBF8B696180F5FDE6FAC0FB8FBAEB99C5
UserPrincipalName : stuart
Role            : default
CertificateDefinition : default_Definition
SecurityContext   :
ExpiryDate       : 15/07/2021 16:34:50
```

注：

HSMを使用して秘密キーを保存する場合、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。

```
Get-FasUserCertificate -address \<FAS server FQDN> -KeyInfo $true
```

例えば：

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

```
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

- FASのインストールと構成に関する主要な参照は、[インストールと構成](#)です。
- 一般的なFASの展開については、[Federated Authentication Services architectures overview](#)の記事にまとめられています。
- その他の「ハウツー」記事は、[Advanced configuration](#)の記事で紹介されています。

キー ストレージ プロバイダー (KSP) リモータリング (レビュー)

はじめに

以前は、Windows VDA から FAS サーバーへの暗号化操作のリモータリングは、VDA で実行される一対の暗号化サービスプロバイダー (CSP) を使用して実現されていました。

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

この機能により、暗号化操作のリモータリングは、一対の KSP を使用しても実現できます。

- `CitrixLogonKsp.dll` - VDA への SSO 用
- `CitrixVirtualSmartcardKsp.dll` - セッション内証明書用

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

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

注:

FAS で ECC キーを有効にする方法はありません。

KSP リモートティグを有効にする

KSP リモートティグは、次のレジストリキーを作成することで有効になります。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication\UserCredentialService\RemoteKsp

種類: string

値: on

- FASサーバーとVDAソフトウェアの両方でCVAD 2407ソフトウェアが実行されている必要があります。
- KSPリモート処理は、FASサーバーとVDAの両方にレジストリキーを作成することで有効になります。
- 変更を有効にするには、FASサーバーとVDAを再起動します。

上記の条件のいずれかが満たされない場合、VDAはCSPリモート処理の使用にフォールバックします。

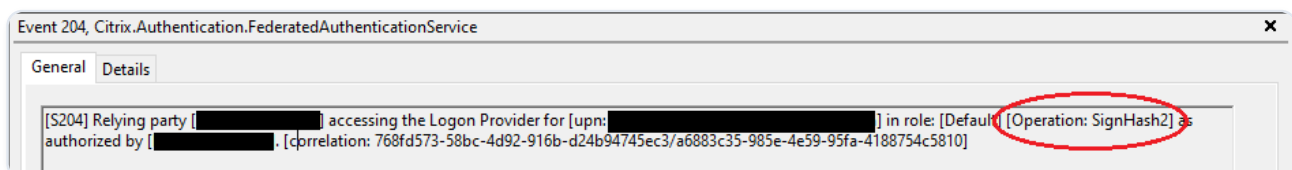
KSPリモート処理が有効になっているかを確認する

FASサーバーで、Powershellを使用してKSPリモート処理が有効になっているかを確認できます。

```
PS C:\> Get-FasServer -Address localhost

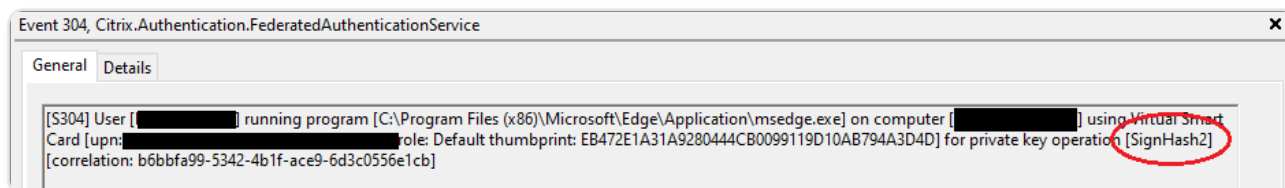
Address      : localhost
Index        :
Version      : 3
MaintenanceMode : True
AdministrationACL : O:BAG:DUD:P(A;OICI;SW;;;BA)
Capabilities  : AuthCertificateDetails,Cloud2,CloudKeyInfo,CloudRegistration,RaCertificateMonitor,RemoteKsp,RemoveA
                uthorization
```

VDA SSOにKSPリモート処理が使用されたかどうかを確認するには、FASサーバーのWindowsアプリケーションログで次のイベントを探します。



操作 SignHash2 はKSPリモート処理の使用を示し、SignHash はCSPリモート処理を示します。

同様に、TLSクライアント認証などの暗号化にセッション内証明書が使用される場合、FASサーバーで次のイベントを探します。



既知の制限事項

KSPリモート処理は、FAS自体がKSPを使用するように構成されている場合にのみサポートされます。これはデフォルトの構成です。FASがCSPを使用するように構成されている場合、KSPリモート処理は機能しません。

関連する設定は次のとおりです。

```
ファイル %programfiles%\Citrix\Federated Authentication
Service\Citrix.Authentication.FederatedAuthenticationService.exe.config 内の
<add
key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp"
value="false" />
```

ここで、`False` はFASがKSPで構成されており、したがってKSPリモート処理がサポートされていることを示します。

セキュリティとネットワーク構成

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

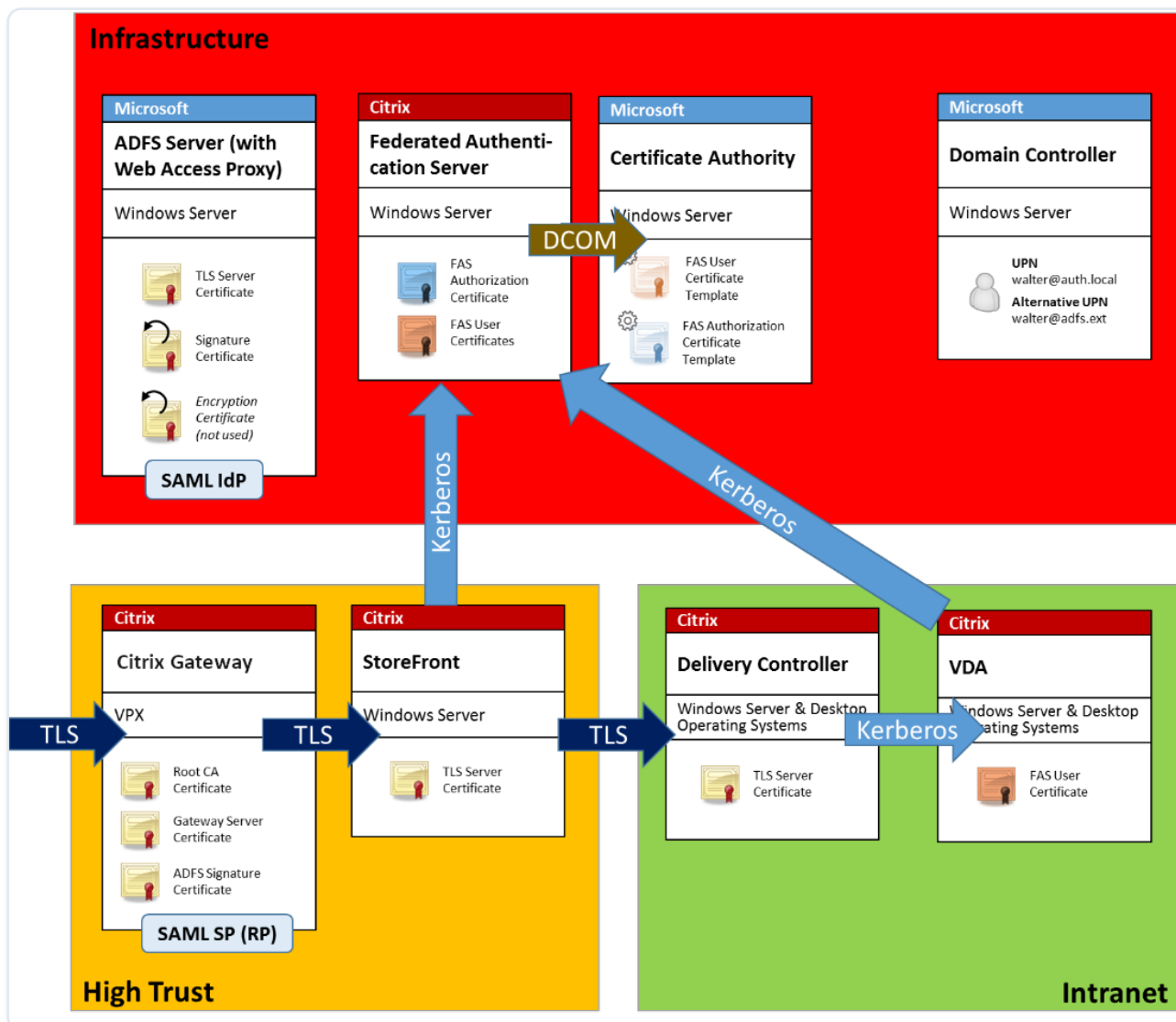
このドキュメントでは、FAS を展開する際に考慮すべきセキュリティ問題の概要を説明します。また、インフラストラクチャの保護に役立つ可能性のある利用可能な機能の概要も説明します。

ネットワークアーキテクチャ

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

FAS サーバーは、証明機関およびドメインコントローラーとともに、セキュリティ上重要なインフラストラクチャの一部です。フェデレーション環境では、Citrix Gateway と Citrix StoreFront が

ユーザー認証を実行するコンポーネントです。その他の Citrix Virtual Apps and Desktops™ コンポーネントは、FAS の導入による影響を受けません。



ファイアウォールとネットワークセキュリティ

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

StoreFront サーバーは、相互認証された Kerberos を使用してポート 80 経由で FAS サーバーに接続します。認証には、FAS サーバーの Kerberos HOST/fqdn ID と、StoreFront サーバーの Kerberos マシンアカウント ID が使用されます。この認証方法により、Citrix Virtual Delivery Agent (VDA) がユーザーをログオンするために必要な、1 回限りの「資格情報ハンドル」が生成されます。

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

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

サーバー	ファイアウォールポート
フェデレーション認証サービス	[in] StoreFront™およびVDAからの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および署名済み

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

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

シトリックス クラウド

- ユーザーアカウントで実行される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で実行されるFASサービス:
 - *.citrixworkspacesapi.net
 - *.citrixnetworkapi.net

Citrix Cloud 日本

- ユーザーアカウントで実行されるFAS管理コンソール
 - *.citrixcloud.jp
 - *.citrixworkspacesapi.jp
 - 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で実行されるFASサービス:
 - *.citrixworkspacesapi.jp
 - *.citrixnetworkapi.jp

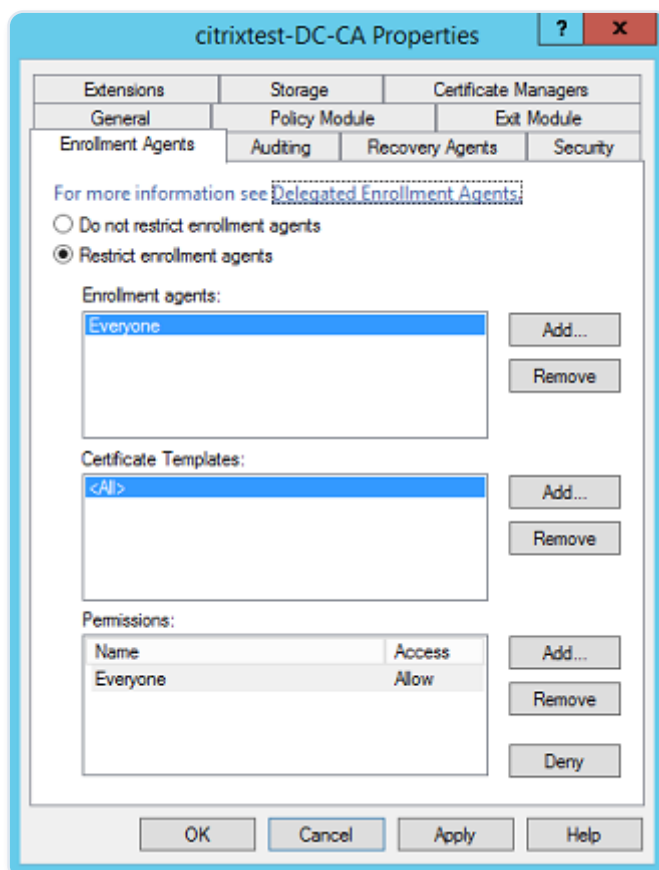
環境にプロキシサーバーが含まれている場合、FAS管理コンソールのアドレスを使用してユーザープロキシを構成します。また、ネットワークサービスアカウントのアドレスが**Netsh**または同様のツールを使用して構成されていることを確認してください。

セキュリティに関する考慮事項

FASには、ドメインユーザー向けに自律的に証明書を発行できる登録機関証明書があります。これは、FASサーバーを保護し、その権限を制限するためのセキュリティポリシーの開発と実装に役立ちます。

委任された登録エージェント

FASは、登録エージェントとして機能することでユーザー証明書を発行します。Microsoft証明機関を使用すると、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。



提示されたダイアログを使用して、以下を確実にすることができます。

- 「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。
- 「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。
- 「アクセス許可」リストには、FASの使用が許可されているユーザーが含まれている。たとえば、管理者または保護されたユーザーグループに証明書を発行しないことを推奨します。

アクセス制御リストの構成

(/ja-jp/federated-authentication-service/2407/install-configure.html#configure-rules)セクションで説明されているように、StoreFrontサーバーのリストを構成する必要があります。これらのStoreFrontサーバーは、証明書が発行されるときにFASにユーザーIDをアサートします。同様に、どのユーザーに証明書が発行されるか、およびどのVDAマシンに認証できるかを制限できます。この機能は、構成する標準のActive Directoryまたは証明機関のセキュリティ機能に追加されるものです。

ファイアウォール設定

FASサーバーへのすべての通信は、ポート80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。(/[ja-jp/federated-authentication-service/2407/config-manage/troubleshoot-logon.html#fas-event-logs](#))セクションには、生成可能なイベントログエントリがリストされています。

ハードウェアセキュリティモジュール

FASによって発行されたユーザー証明書キーを含むすべての秘密キーは、ネットワークサービスアカウントによってエクスポート不可能な秘密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（例：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せん。

パラメーター	説明
ProviderLegacyCsp	trueに設定されている場合、FASはMicrosoft CryptoAPI (CAPI)を使用します。それ以外の場合、FASはMicrosoft Cryptography Next Generation API (CNG)を使用します。
ProviderName	使用するCAPIまたはCNGプロバイダーの名前。
ProviderType	Microsoft KeyContainerPermissionAccessEntry.ProviderType プロパティ PROV_RSA_AES 24 を参照します。CAPIでHSMを使用しており、HSMベンダーが別途指定しない限り、常に24である必要があります。
KeyProtection	秘密キーの「エクスポート可能」フラグを制御します。また、ハードウェアでサポートされている場合、トラステッドプラットフォームモジュール (TPM) キー格納の使用も許可します。

パラメーター	説明
KeyLength	RSA秘密キーのキー長。サポートされている値は1024、2048、4096です（デフォルト：2048）。

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

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

グループポリシー設定

信頼されたFASマシンは、グループポリシーを通じて構成された「インデックス番号 -> FQDN」のルックアップテーブルによって識別されます。FASサーバーに接続する際、クライアントはFASサーバーの `HOST\<fqdn>` Kerberos IDを検証します。FASサーバーにアクセスするすべてのサーバーは、同じインデックスに対して同一のFQDN構成を持っている必要があります。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、誤設定を避けるために、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、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）に限定する必要があります。FASサーバーの廃止後すぐにマシンのFQDN名を再利用しないように注意してください。

証明書テンプレート

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

証明書テンプレートの名前を変更する

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

- 証明書テンプレートのコピーを作成し、組織のテンプレート命名標準に合わせて名前を変更します。
- 管理者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。（管理者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意図しています。）
 - Microsoft MMC証明書テンプレートスナップインまたはPublish-FasMsTemplateコマンドのいずれかを使用してテンプレートを公開し、
 - New-FasCertificateDefinitionコマンドを使用して、テンプレート名でFASを構成します。

一般プロパティを変更する

デフォルトでは、ユーザー証明書の有効期間は7日間です。証明書テンプレートで有効期間を変更できます。

更新期間は変更しないでください。FASは証明書テンプレートのこの設定を無視します。FASは、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。

廃止されたテンプレートプロパティの変更

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

拡張機能プロパティの変更

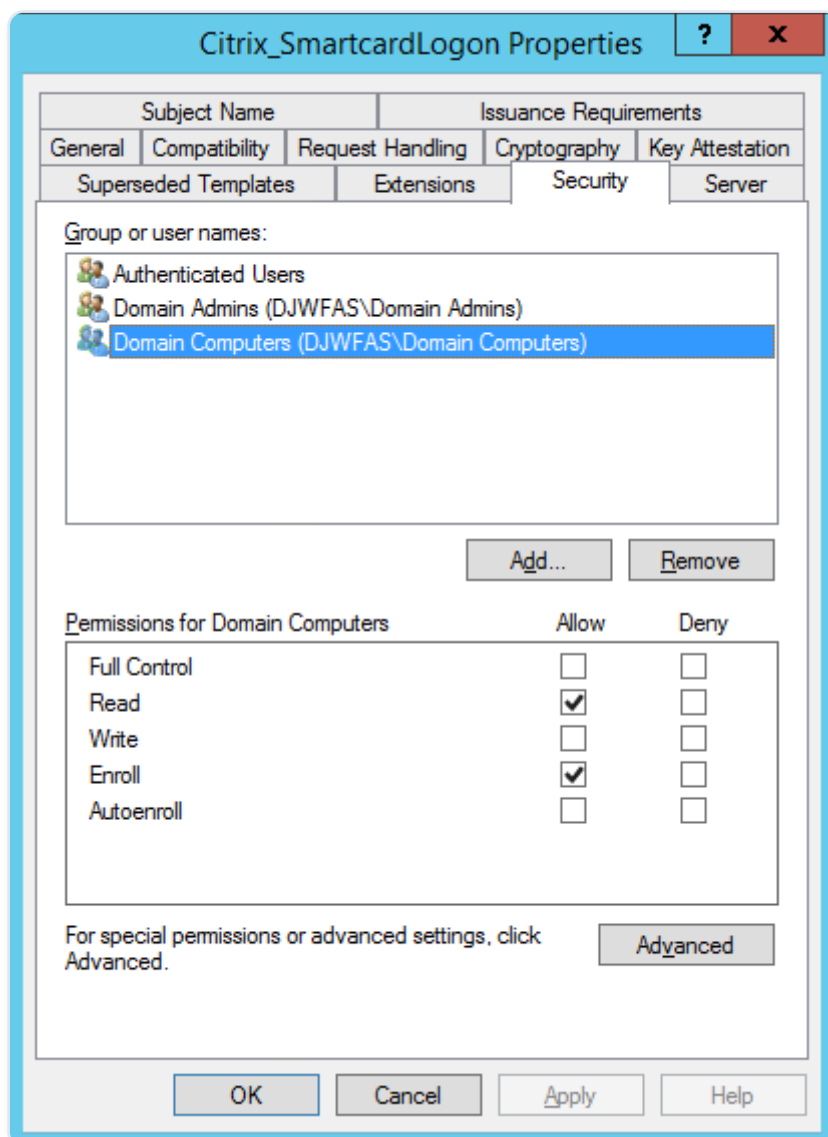
これらの設定は、組織のポリシーに合わせて変更できます。

注：不適切な拡張機能設定は、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る可能性があります。

セキュリティプロパティの変更

Citrix は、FAS サーバーのマシンアカウントのみに **読み取り** および **登録** 権限を許可するように、これらの設定を変更することを推奨します。FAS サービスは、他の権限を必要としません。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。

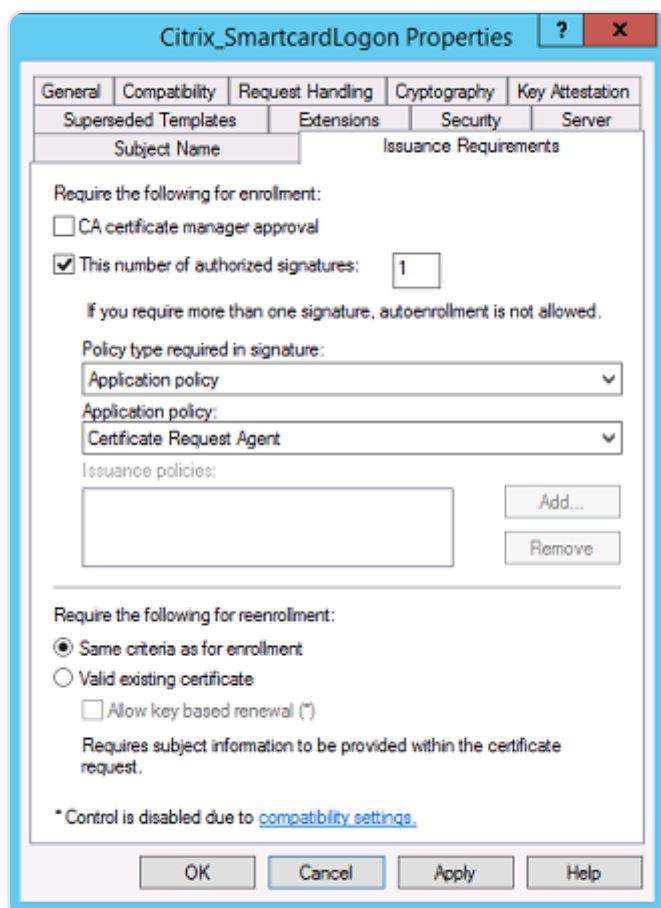
テンプレートには、この *Active Directory* 情報から構築するが選択されており、証明機関がユーザーの SID を証明書拡張機能に含めるようにします。これにより、ユーザーの *Active Directory* アカウントへの強力なマッピングが提供されます。

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。

発行要件のプロパティを変更する

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



互換性プロパティを変更する

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、それが使用する発行証明書の秘密鍵に責任を負います。

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。

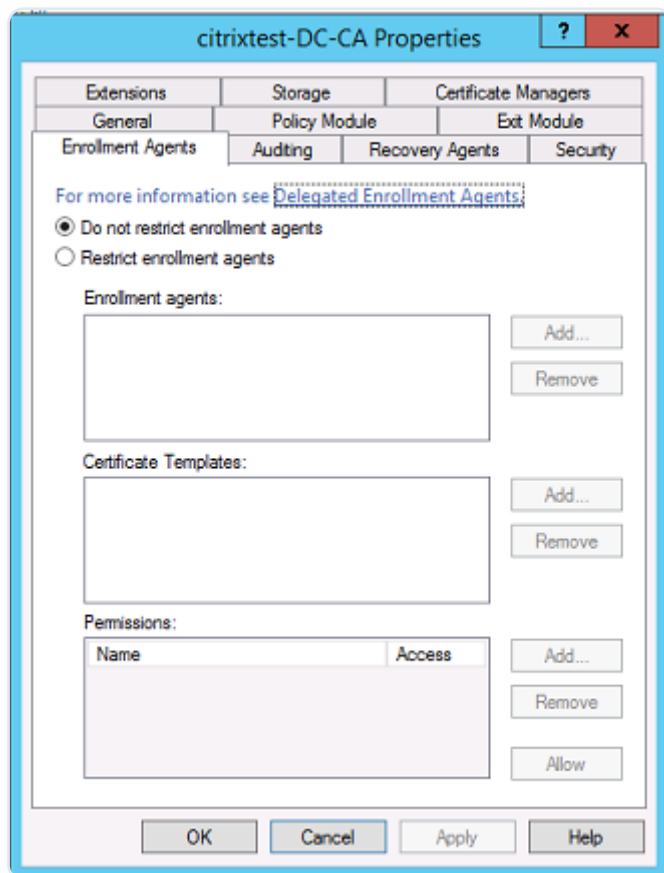
簡単なセキュリティ対策としては、FASサーバーのインストール時に登録機関証明書テンプレートのみを公開するか、完全にオフラインの発行プロセスを徹底することです。いずれの場合でも、証明機関管理者は登録機関証明書要求の承認を完全に制御し、FASサーバーを承認するためのポリシーを持つ必要があります。

ファイアウォール設定

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

登録の制限

デフォルトでは、登録機関証明書の所有者は、アクセスを許可する任意の証明書テンプレートを使用して、任意のユーザーに証明書を発行できます。この証明書の発行は、「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を介してStoreFront、ユーザー、VDAを制限する

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

アクセスベクター	説明
StoreFront [IdP]	これらのKerberosアカウントは、ユーザーが正しく認証されたことを宣言するために信頼されています。これらのアカウントのいずれかが侵害された場合、FASの構成によって許可されたユーザー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、証明書と秘密鍵へのアクセスが許可されているマシンです。IdPによって取得された資格情報ハンドルも必要であるため、このグループ内の侵害されたVDAアカウントがシステムを攻撃できる範囲は限られています。
ユーザー	このオプションは、どのユーザーがIdPによってアサートされるかを制御します。証明機関の「制限付き登録エージェント」構成オプションと重複があることに注意してください。一般的に、このリストには非特権アカウントのみを含めることをお勧めします。これにより、侵害されたStoreFrontアカウントがより高い管理レベルに特権を昇格させることを防ぎます。特に、ドメイン管理者アカウントは、このACLによって許可されてはなりません。

ルールの構成

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

証明機関とテンプレートの構成

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

セッション内証明書と認証証明書

FAS管理者は、認証に使用される証明書がユーザー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、ユーザーはセッション内で「署名」証明書のみを使用でき、より強力な「ログオン」証明書はログオン時にのみ使用できます。

秘密鍵の保護と鍵長

FAS管理者は、秘密キー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では、少なくとも登録機関証明書の秘密キーをTPMに保存して保護することを推奨しています。FASは、「オフライン」証明書要求プロセスの一部として、秘密キーをTPMに保存するオプションを提供します。

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

イベントログ

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

管理アクセスと管理ツール

FASには、リモート管理機能（相互認証Kerberos）とツールが含まれています。「ローカル管理者グループ」のメンバーは、FAS構成を完全に制御できます。FAS構成は適切に維持する必要があります。

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

FASの「資格情報ハンドル」は単に「Active Directoryパスワード」を置き換えるだけであるため、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。ControllerおよびVDA管理グループには、信頼できるユーザーのみを含める必要があります。監査およびイベントログは維持する必要があります。

一般的なWindowsサーバーのセキュリティ

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

監査およびイベントログは、リモートマシンに安全に保存する必要があります。

RDPアクセスは、承認された管理者のみに制限する必要があります。Citrix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推奨しています。

関連情報

- [インストールと構成](#)は、FASのインストールと構成に関する主要なリファレンスです。
- FASアーキテクチャについては、[展開アーキテクチャ](#)の記事で紹介しています。
- その他の「ハウツー」記事は、[高度な設定](#)記事で紹介されています。

パフォーマンスカウンター

FASには、負荷追跡のために一連のパフォーマンスカウンターが含まれています。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/performance-counters.png)

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	Federated Authentication Service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	Federated Authentication Service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	Federated Authentication Service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。
1分あたりの秘密鍵操作	Federated Authentication Serviceによって1分あたりに実行されている証明書秘密鍵操作の数。前の1分間のデータを使用して計算されません。

名前	説明
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分あたりの証明書署名要求の観点から受け入れ可能な負荷の推定値。推定値は、前の1分間のデータを使用して毎分更新されます。「高負荷」のしきい値を超えると、公開されたアプリまたはデスクトップの起動が失敗する可能性があります。

Windowsログオンの問題のトラブルシューティング

この記事では、ユーザーが証明書またはスマートカード、あるいはその両方を使用してログオンする際にWindowsが提供するログとエラーメッセージについて説明します。これらのログは、認証失敗のトラブルシューティングに役立つ情報を提供します。

証明書と公開鍵インフラストラクチャ

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

- **NTAuth 証明書ストア**：Windowsに認証するには、ユーザー証明書を直接発行する証明機関（つまり、チェーンはサポートされていません）をNTAuthストアに配置する必要があります。これらの証明書を表示するには、certutilプログラムから次のように入力します：`certutil -viewstore -enterprise NTAuth`
- **ルートおよび中間証明書ストア**：通常、証明書ログオンシステムは単一の証明書しか提供できないため、チェーンが使用されている場合、すべての中間証明書ストアにこれらの証明書を含める必要があります。ルート証明書は信頼されたルートストアに、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\(v=ws.10\)>`。

レジストリポリシー	説明
AllowCertificatesWithNoEKU	無効にすると、証明書にはスマートカードログオンの拡張キー使用法 (EKU) を含める必要があります。
AllowSignatureOnlyKeys	既定では、Windowsは、RSA復号化を許可しない証明書の秘密鍵を除外します。このオプションはそのフィルターを上書きします。
AllowTimeInvalidCertificates	既定では、Windowsは期限切れの証明書を除外します。このオプションはそのフィルターを上書きします。
EnumerateECCerts	楕円曲線認証を有効にします。
X509ヒントニーデッド	証明書に一意のユーザープリンシパル名 (UPN) が含まれていない場合、または曖昧な場合、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 (ドメインコントローラーで設定)。

- **ドメインコントローラー証明書:** Kerberos 接続を認証するには、すべてのサーバーが適切な「ドメインコントローラー」証明書を持っている必要があります。これらは、「ローカルコンピュータ証明書個人ストア」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のユービーエヌ名

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

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

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

証明書マッピングサービス

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

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

フォレスト内に複数のドメインがあり、ユーザーが明示的にドメインを指定しない場合、Active Directory の rootDSE は証明書マッピングサービスの場所を指定します。これはグローバルカタログマシンにあり、フォレスト内のすべての x509certificate 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、ログを有効にして取得できるように、認証に使用されるドメインコントローラーを確認し、制限することが役立ちます。

ドメインコントローラーの選択を制御する

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

通常、その場所には「lmhosts.sam」という名前のサンプルファイルがあります。単純に次の行を含めます。

1.2.3.4 dcnetbiosname #PRE #DOM:mydomai

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

再起動後、Windows マシンはその情報を使用して mydomain にログオンします。この構成は、デバッグが完了したら元に戻す必要があります。

使用中のドメインコントローラーを特定する

ログオン時、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 **echo %LOGONSERVER%** コマンドで起動します。

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

アカウント監査イベントを有効にする

デフォルトでは、Windows ドメインコントローラーは完全なアカウント監査ログを有効にしていません。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。グループポリシーエディターを開くには、ドメインコントローラーで `gpedit.msc` を実行します。監査ポリシーが有効になると、ドメインコントローラーはセキュリティログに追加のイベントログ情報を生成します。

アカウント監査イベントを有効にする(/en-us/federated-authentication-service/2407/media/fas-troubleshoot-logon-auditpolicy.png)

証明書検証ログ

証明書の有効性を確認する

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

CAPIログを有効にする

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

ドメインコントローラーとVDAマシンで、イベントビューアーを開き、**Applications and Services Logs > Microsoft > Windows > CAPI2 > Operational** に移動します。**Operational** を右クリックし、**Enable Log** を選択します。

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

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

CAPIログ

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

エラーメッセージ

エラーコード	説明
証明書が信頼されていません	スマートカード証明書を、コンピューターの 中間証明書ストアおよび信頼されたルート証 明書ストアにある証明書を使用して構築でき ませんでした。
証明書失効チェックエラー	スマートカードのCRLを、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ま せん。 (/ja-jp/federated-authentication-service/ 2407/config-manage/troubleshoot- logon.html#certificates-and-public-key-

エラーコード	説明
	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目的であり、安全に無視できます。
 - KDC_ERR_PREAUTH_REQUIRED (古いドメインコントローラーとの下位互換性のために使用されます)
 - 不明なエラー 0x4b

ドメインコントローラーとワークステーションのログ

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に、ドメインコントローラーとワークステーションで予想されるログエントリについて説明します。

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

ドメインコントローラー CAPI2 ログ

ログオン中、ドメインコントローラーは呼び出し元の証明書を検証し、次の形式でログエントリのシーケンスを生成します。

ドメインコントローラー CAPI2 ログ (/en-us/federated-authentication-service/2407/media/fas-troubleshoot-logon-capi2-log.png)

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

ドメインコントローラー CAPI2 ログ 2 (/en-us/federated-authentication-service/2407/media/fas-troubleshoot-logon-capi2-chainpolicy.png)

ドメインコントローラー セキュリティログ

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

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

ドメインコントローラー セキュリティログ (/en-us/federated-authentication-service/2407/media/fas-troubleshoot-logon-dc-security-log.png)

VDA セキュリティログ

ログオンイベントに対応する VDA セキュリティ監査ログは、winlogon.exe を起点とするイベント ID 4648 のエントリです。

VDA セキュリティログ (/en-us/federated-authentication-service/2407/media/fas-troubleshoot-logon-vda-security-log.png)

VDA CAPIログ

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

VDA CAPIログ (/en-us/federated-authentication-service/2407/media/fas-troubleshoot-logon-capi-log.png)

VDA CAPIログ 2 (/en-us/federated-authentication-service/2407/media/fas-troubleshoot-logon-capi-chainpolicy.png)

VDAシステムログ

Kerberosログが有効になっている場合、システムログにはエラー KDC_ERR_PREAUTH_REQUIRED（無視可能）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。

VDAシステムログ (/en-us/federated-authentication-service/2407/media/fas-troubleshoot-logon-vda-system-log.png)

Windowsイベントログを使用したFASの監視

すべてのFASイベントはWindowsアプリケーションイベントログに書き込まれます。System Center Operations Manager（SCOM）などの製品を使用して、ここで説明す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、Citrix.Authentication.FederatedAuthenticationService.exeプロセスを監視します。

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

FASヘルスイベント

以下のイベントは、FASサービスが正常であるかどうかを示します。

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

イベント	イベントテキスト	説明	注
[S003]	管理者 [{0}] がメンテナンスモードを [{1}] に設定	FASサービスがメンテナンスモードに設定されたか、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 / Citrix Virtual Apps and Desktops 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サービスがメンテナンスモードになりました。	FAS 10.7 / Citrix Virtual Apps and Desktops 2109 から利用可能。
[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]	[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	FASが指定されたCAからユーザー証明書を要求しようとしたときに、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。	このイベントは、CAが機能していないか、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。

イベント	イベントテキスト	説明	注
[S413]	承認証明書の有効期限が間もなく切れます ({0} 日残っています)。証明書の詳細: {1}	このイベントは、FAS承認証明書の有効期限が近づくとき定期的に生成されます。デフォルトでは、承認証明書の有効期限が30日以内である場合、このイベントは毎日生成されます。	既定の設定は、cmdlet Set-FasRaCertificateMonitor を使用して調整できます。 PowerShell cmdlet 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™でFASを使用している場合、次のイベントは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するはずであることを示しています。	このイベントを発行する前に、FASは(1)設定されていること、(2)メンテナンスモードではないこと、および(3)Citrix Cloudに接続されていることを確認します。
[S013]	FASサービスはCitrix Cloudからのシングルサインオンに利用	このイベントは、FASがWorkspace（つまりCitrix	FASはCitrix Cloudへの永続的な接続を維持します。この接続

イベント	イベントテキスト	説明	注記
	できません。[{0}] 詳細については、管理コンソールで確認できます。	Cloud) からのシングルサインオンを提供できないことを示します。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。	は、ネットワークの不具合やプロキシサーバーの接続ライフタイムポリシーなど、さまざまな理由で時折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。これは通常の動作であり、FASはCitrix Cloudへの接続を直ちに再確立しようとします。

セキュリティイベント

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

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

イベント	イベントテキスト	説明
[S001]	アクセス拒否: ユーザー[{0}]はAdministratorsグループのメンバーではありません	FASの構成を表示または変更しようとしたましたが、呼び出し元はFAS管理者ではありませんでした。
[S002]	アクセス拒否: ユーザー[{0}]はロール[{1}]の管理者ではありません	FASルールの構成を表示または変更しようとしたましたが、呼び出し元はFAS管理者ではありませんでした。
[S101]	サーバー [{0}] は、ロール [{1}] でIDをアサートする権限がありません。	ユーザーIDをアサートしようとしたましたが、呼び出し元にはその権限がありません。FASルール構成で許可されているStoreFront™サーバー（および該当する場合は

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

FASイベントログ

次の表は、FASによって生成されるイベントログエントリを示しています。

管理イベント

これらのイベントは、FASサーバーの構成変更に応じてログに記録されます。

ログコード
[S001] アクセス拒否: ユーザー [{0}] は Administrators グループのメンバーではありません
[S002] アクセス拒否: ユーザー [{0}] はロール [{1}] の管理者ではありません
[S003] 管理者 [{0}] がメンテナンスモードを [{1}] に設定しています
[S004] 管理者 [{0}] が CA [{1}] からテンプレート [{2} and {3}] を使用して承認証明書を要求しています
[S005] 管理者 [{0}] が CA [{1}] の承認を取り消しています
[S006] 管理者 [{0}] が証明書定義 [{1}] を作成しています
[S007] 管理者 [{0}] が証明書定義 [{1}] を更新しています
[S008] 管理者 [{0}] が証明書定義 [{1}] を削除しています
[S009] 管理者 [{0}] がルール [{1}] を作成しています

ログコード
[S010] 管理者 [{0}] がルール [{1}] を更新しています
[S011] 管理者 [{0}] がルール [{1}] を削除しています
[S012] 管理者 [{0}] が証明書 [upn: {1} sid: {2} rule: {3}] を作成しています [Certificate Definition: {4} Security Context: {5}]
[S013] 管理者 [{0}] が証明書 [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}] を削除しています
[S015] 管理者 [{0}] が証明書要求 [TPM: {1}] を作成しています
[S016] 管理者 [{0}] 承認証明書をインポートしています [Reference: {1}]
[S022] 管理者 [{0}] メンテナンスモードをオフに設定しています
[S023] 管理者 [{0}] メンテナンスモードをオンに設定しています
[S024] 管理者 [{0}] システムヘルスマニターを設定しています
[S025] 管理者 [{0}] システムヘルスマニターを設定しています
[S026] 管理者 [{0}] RA証明書モニターを設定しています
[S027] 管理者 [{0}] RA証明書モニターをリセットしています
[S050] 管理者 [{0}] クラウド構成を作成しています: [{1}]
[S051] 管理者 [{0}] クラウド構成を更新しています: [{1}]
[S052] 管理者 [{0}] クラウド構成を削除しています
[S060] 管理者 [{0}] 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}] 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}] クラウド登録を完了しています。リソースの場所: {1}, ルール名: {2}
[S062] 管理者 [{0}] クラウド登録が完了しました。リソースの場所: {1} ({2}), ルール名: {3}, 顧客: {4} ({5})

ログコード
[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
[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] 構成のアップグレードを実行しています - [From version {0} to version {1}]
[S402] エラー: Citrix Federated Authentication Service は Network Service として実行する必要があります [currently running as: {0}]
[S404] Citrix Federated Authentication Service データベースを強制的に消去しています
[S405] レジストリからデータベースへのデータ移行中にエラーが発生しました: [{0}]
[S406] レジストリからデータベースへのデータ移行が完了しました (注: ユーザー証明書は移行されません)
[S407] データベースが既に存在するため、レジストリベースのデータはデータベースに移行されませんでした
[S408] 構成をダウングレードできません -- [From version {0} to version {1}]
[S409] ThreadPool 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
[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。これは FAS サーバーのスケーラビリティに影響を与え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] 構成のアップグレードが完了しました -- [From version {0} to version {1}]
[S413] 承認証明書の有効期限が間もなく切れます (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] 認証証明書のチェックが完了しました。{0}件の問題がログに記録されました。次回のチェックは{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] [upn: {0} role: {1} Security Context: [{2}]] に証明書を発行しています
[S121] [certificate authority: {2}] によって [upn: {0} role: {1}] に証明書が発行されました
[S122] 警告: サーバーが過負荷状態です [upn: {0} role: {1}][1分あたりのリクエスト数 {2}]。
[S123] [upn: {0} role: {1}] [exception: {2}] の証明書の発行に失敗しました
[S124] [certificate authority: {2}] [exception: {3}] で [upn: {0} role: {1}] の証明書の発行に失敗しました

依頼当事者として機能する

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

ログコード
[S201] 依頼当事者 [{0}] はパスワードにアクセスできません。
[S202] 依頼当事者 [{0}] は証明書にアクセスできません。
[S203] 依頼当事者 [{0}] はLogon CSPにアクセスできません

ログコード
[S204] 依頼当事者 [{0}] は、[{4}] によって承認された役割: [{2}] [Operation: {3}] で [upn: {1}] の Logon CSPにアクセスしています
[S205] 依頼当事者アクセスが拒否されました - 呼び出し元アカウント [{0}] は、ルール [{1}] の許可された依頼当事者ではありません
[S206] 呼び出し元アカウント [{0}] は依頼当事者ではありません
[S208] 秘密キー操作が失敗しました [操作: {0} UPN: {1} 役割: {2} certificateDefinition {3} エラー {4} {5}]。

セッション内証明書サーバー

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

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

ログコード
[S502] FASアサーションプラグインがロードされました [pluginId={0}] [assembly={1}] [location={2}]
[S503] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (ログオン証拠が提供されましたが、プラグイン [{2}] はそれをサポートしていません)
[S504] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (ログオン証拠が提供されましたが、構成されたFASプラグインがありません)
[S505] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (プラグイン [{2}] はログオン証拠をステータス [{3}] とメッセージ [{4}] で拒否しました)
[S506] プラグイン [{0}] は、サーバー [{1}] から UPN [{2}] のログオン証拠をメッセージ [{3}] とともに受け入れました
[S507] サーバー [{0}] は UPN [{1}] をアサートできませんでした (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}] をアサートできませんでした (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}] をアサートできませんでした (アクセスディスポジションが提供されましたが、プラグイン [{2}] はそれをサポートしていません)
[S509] サーバー [{0}] は UPN [{1}] をアサートできませんでした (アクセスディスポジション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}] をアサートできませんでした (アクセスディスポジションはプラグイン [{2}] によって無効と見なされました)

ワークスペース対応FAS

FASがWorkspaceで使用される場合、これらのイベントがログに記録されます。

ログコード
[S001] Citrix Cloud認証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}]

ログコード
[S004] FASは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は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 は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 はクラウドから登録解除されました [fas id: {0}] [transaction id: {1}]
[S009] FAS は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できます
[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
[S014] クラウドサービス <service name> への呼び出しが失敗しました [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S015] 呼び出し元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 <service name> への呼び出しが成功しました [fas id: {0}] [transaction id: {1}]
[S019] FAS は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 はクラウドから構成をダウンロードできませんでした [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S021] クラウドサポートモジュールの起動に失敗しました。例外: {0}
[S022] クラウドサポートモジュールが停止しています
[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}]

ログコード
[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
[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 {0} への接続に失敗しました [Error: {1} {2}]
[S105] IDアサーションログオン。ログオンしています [Username: {0} Domain: {1}]
[S106] IDアサーションログオン。フェデレーション認証サービス: {0} ログオンしています [Certificate: {1}]
[S107] IDアサーションログオンに失敗しました。 [Exception: {0}{1}]
[S108] IDアサーションサブシステム。アクセス拒否 [Caller: {0}]

インセッション証明書

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

ログコード
[S201] 仮想スマートカードアクセスは [PID: {1} Program Name: {2}Certificate thumbprint: {3}] のために [{0}] によって承認されました
[S203] 仮想スマートカードサブシステム。アクセス拒否 [caller: {0}, session {1}]
[S204] 仮想スマートカードサブシステム。スマートカード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するときにログ記録されます。

ログコード
[S001] TrustArea::TrustArea: 証明書がインストールされました [TrustArea: {0} Certificate {1} TrustAreaJoinParameters {2}]
[S014] Pkcs10Request::Create: PKCS10要求が作成されました [Distinguished Name {0}]
[S016] 秘密鍵::作成 [Identifier {0}MachineWide: {1} Provider: {2} ProviderType: {3} EllipticCurve: {4} KeyLength: {5} isExportable: {6}]
[S017] 秘密鍵::削除 [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 応答の送信エラー [{0}]
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest 証明書が発行されました [{0}]
[S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - 承認待ち [CR_DISP_UNDER_SUBMISSION] [Reference: {0}]

エンドユーザーのエラーメッセージ

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

表示されたエラーメッセージ	説明と参照
無効なユーザー名またはパスワード	コンピューターは有効な証明書と秘密鍵を持っていると認識していますが、Kerberosドメインコントローラーが接続を拒否しました。この記事の「 Kerberos ログ 」セクションを参照してください。
システムはログオンできませんでした。資格情報を確認できませんでした。/ リクエスト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。ドメインコントローラーに「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、これを試す価値はあります。
システムはログオンできない可能性があります。認証に使用されたスマートカード証明書は信頼されていませんでした。	中間証明書とルート証明書がローカルコンピューターにインストールされていません。 「証明書と公開鍵インフラストラクチャ」(/ja-jp/federated-authentication-service/2407/config-manage/troubleshoot-logon.html#certificates-and-public-key-infrastructure)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) ことを示しています。

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](#)
- [スマートカードログオンポリシー](#)
- [CAPIログの有効化](#)
- [Kerberosログの有効化](#)
- [サードパーティの認証局でスマートカードログオンを有効にするためのガイドライン](#)

PowerShell コマンドレット

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

次のコマンドは、FAS PowerShell コマンドレットを追加します。

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

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

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

展開アーキテクチャ

はじめに

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

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

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

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

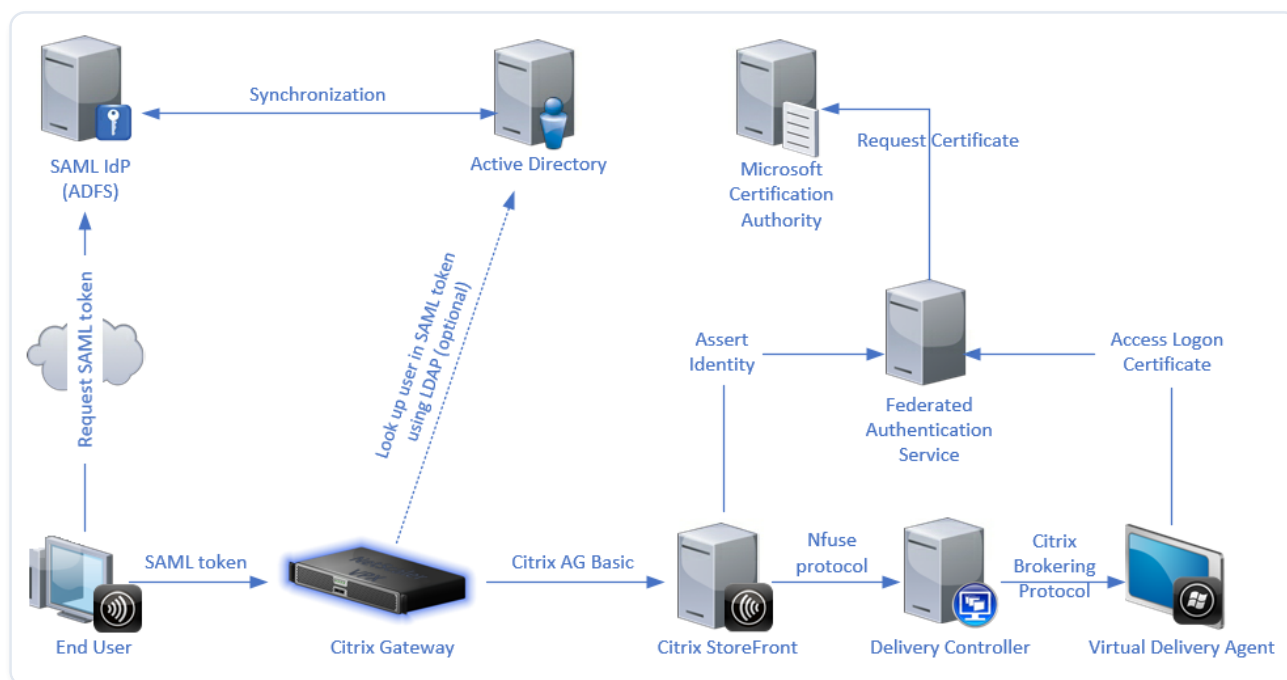
関連する FAS 記事へのリンクが提供されています。すべてのアーキテクチャにおいて、[インストールと構成](#) の記事は FAS のセットアップに関する主要なリファレンスです。

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許可されています。これは、管理者が物理スマートカードをプロビジョニングできるツールと同様の API を使用します。ユーザーが Citrix Virtual Apps™ または Citrix Virtual Desktops Virtual Delivery Agent (VDA) に仲介されると、証明書がマシンにアタッチされ、Windows ドメインはログオンを標準のスマートカード認証として認識します。

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™ サーバーが FAS に接続します。FAS は、単一の Citrix Virtual Apps または Citrix Virtual Desktops セッションがそのセッションの証明書で認証することを許可するチケットを発行します。VDA がユーザーを認証する必要がある場合、FAS に接続してチケットを引き換えます。ユーザー証明書の秘密キーにアクセスできるのは FAS のみです。VDA は、証明書で実行する必要がある署名および復号化の各操作を FAS に送信する必要があります。

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



内部展開

FAS 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、ユーザーが StoreFront に安全に認証し、完全に認証された Citrix HDX™ セッションに接続できるようにします。

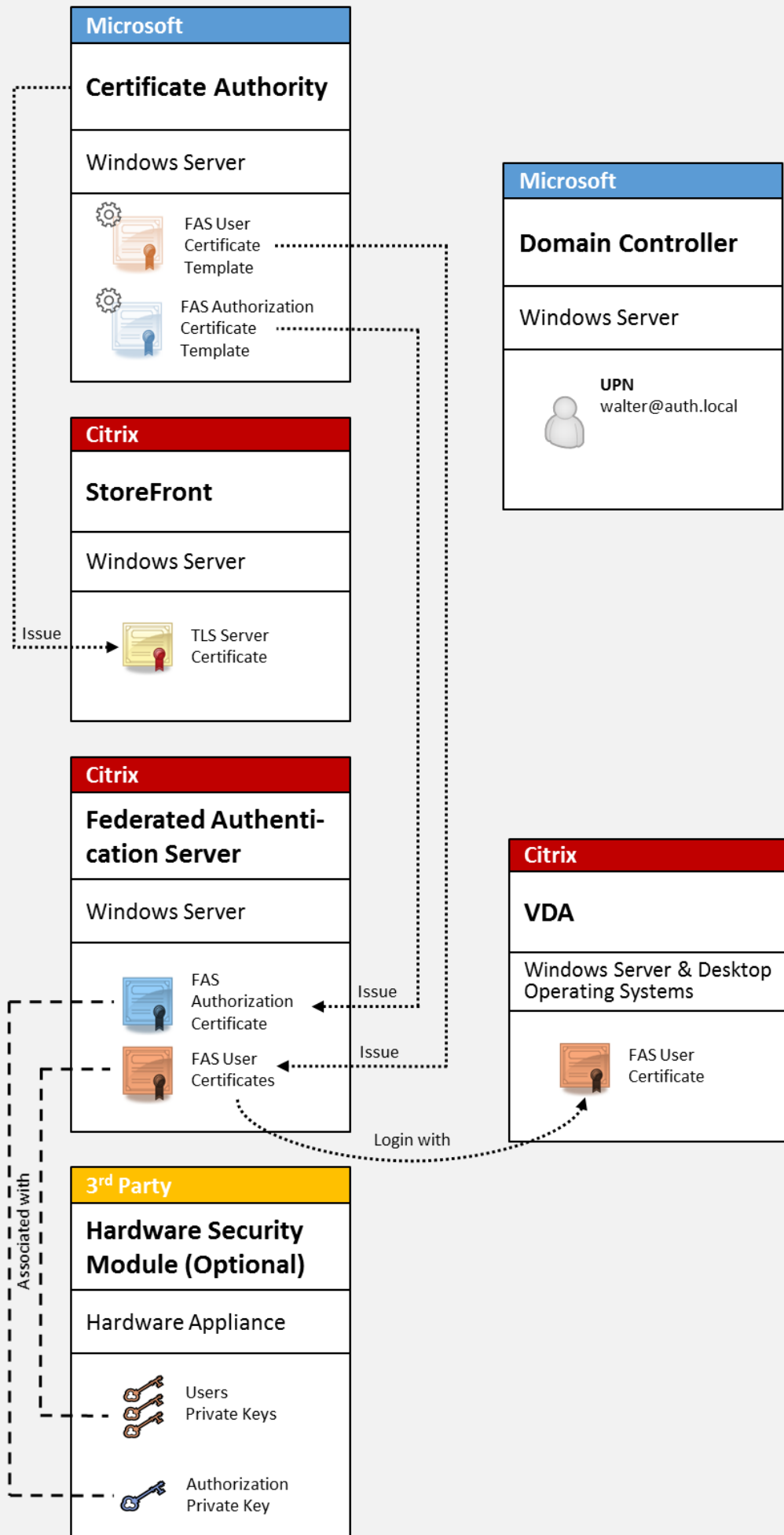
これにより、ユーザー資格情報やスマートカードの PIN を入力するプロンプトなしで Windows 認証が可能になり、シングルサインオンサービスなどの「保存されたパスワード管理」機能を使用する必要がなくなります。これは、以前のバージョンの Citrix Virtual Apps で利用可能だった Kerberos 制限付き委任ログオン機能を置き換えるために使用できます。

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

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

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

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。これについては、[CTX206156](#) に記載されています。

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

関連情報:

- キーは、ハードウェアセキュリティモジュール (HSM) または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 のインストールと構成方法について説明しています。

Citrix Gateway の展開

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

この展開は、最初に Citrix Gateway に認証し、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必要とせずに、高度な Citrix Gateway 認証テクノロジーを使用することもできます。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-architectures-netscaler.png)

Citrix Virtual Apps または Citrix Virtual Desktops 環境は、[CTX206156](#) に記載されている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。

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

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/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のインストール方法と構成方法について説明しています。

ADFS SAML展開

主要なCitrix Gateway認証テクノロジーは、SAML IDプロバイダー (IdP) として機能できるMicrosoft ADFSとの統合を可能にします。SAMLアサーションは、信頼されたIdPによって発行され、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する、暗号署名されたXMLブロックです。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/2407/media/fas-architectures-adfs-saml.png)

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

関連情報:

- [ADFS展開](#)の記事に詳細が記載されています。
- [インストールと構成](#)の記事では、FASのインストール方法と構成方法について説明しています。
- このアートの(/ja-jp/federated-authentication-service/2407/deployment-architectures.html#citrix-gateway-deployment)セクションには、構成に関する考慮事項が含まれています。

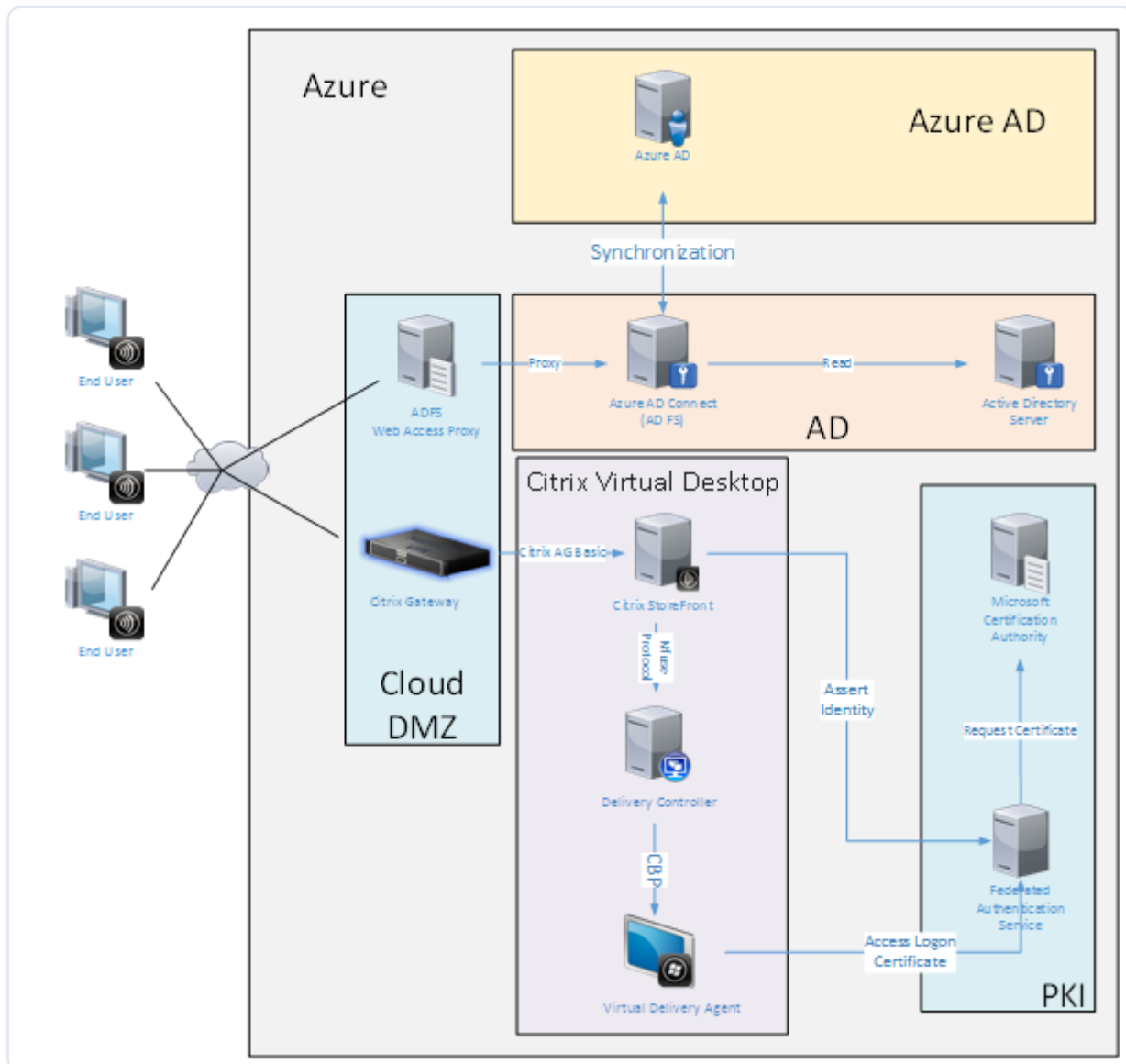
B2Bアカウントマッピング

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

- (ja-jp/federated-authentication-service/2407/install-configure.html)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。

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

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



この展開は、「オフィスにエンドユーザーがいない」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ることに注意してください。オンプレミス、ホスト型プロバイダー、Azure、またはその他のクラウドプロバイダーです。Azure AD Connectシンクロナイザーは、Azure ADに自動的に接続します。例のグラフィックでは、簡素化のためにAzure VMを使用しています。

関連情報:

- ([/ja-jp/federated-authentication-service/2407/install-configure.html](https://aka.ms/federated-authentication-service/2407/install-configure.html))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。

- ([/ja-jp/federated-authentication-service/2407/deployment-architectures/azure-ad.html](https://ja-jp.federated-authentication-service/2407/deployment-architectures/azure-ad.html))の記事には詳細が記載されています。

ADFS 展開

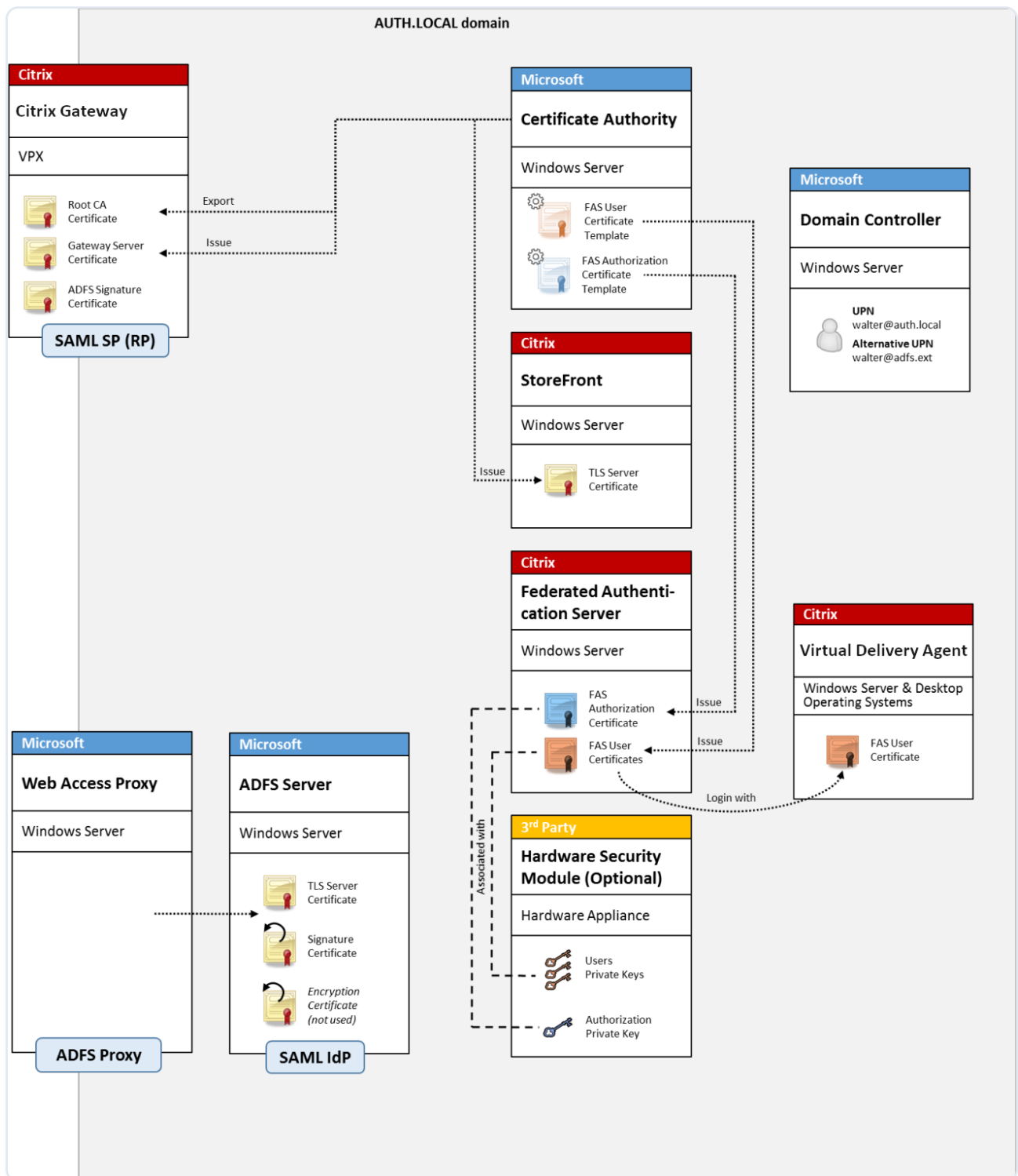
はじめに

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

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

Federated Authentication Service (FAS) は、Citrix Gateway と Citrix StoreFront™ を ADFS ログオンシステムと統合することも可能にし、従業員の混乱を軽減します。

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



注：

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

SAML の概要

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

リダイレクトURL

Citrix Gateway 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を実行するよう指示します。これは通常、`https://adfs.mycompany.com/adfs/ls` の形式の `https://` アドレスです。

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

識別子

EntityId は、Citrix Gateway が ADFS への POST データに含める一意の識別子です。これにより、ユーザーがログオンしようとしているサービスを ADFS に通知し、必要に応じて異なる認証ポリシーを適用します。発行された場合、SAML 認証 XML は EntityId 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 ブラウザーに、EntityId 用に構成されている応答 URL のいずれかに SAML 認証 XML を POST するよう指示します。これは通常、元の Citrix Gateway サーバー上の `https://` アドレスで、形式は次のとおりです。`https://ns.mycompany.com/cgi/samlauth`。

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

署名証明書

ADFS は、秘密キーを使用して SAML 認証 XML BLOB 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キーを使用してこれらの署名をチェックするように構成されている必要があります。証明書ファイルは通常、ADFS サーバーから取得したテキストファイルです。

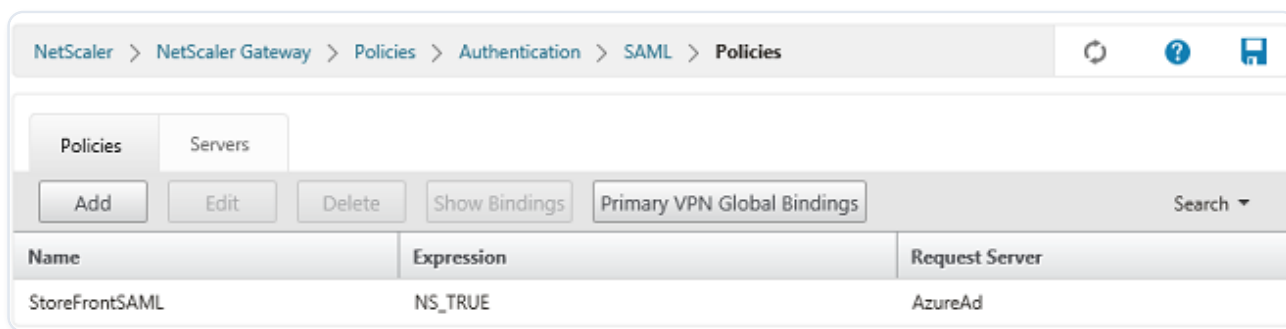
シングルサインアウト URL

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

これは、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できます)。

構成

セクション [Citrix Gateway の展開](#) では、標準の LDAP 認証オプションを処理するように Citrix Gateway を設定する方法について説明します。これが正常に完了したら、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

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-adfs-create-auth-saml-server.png)

関連情報

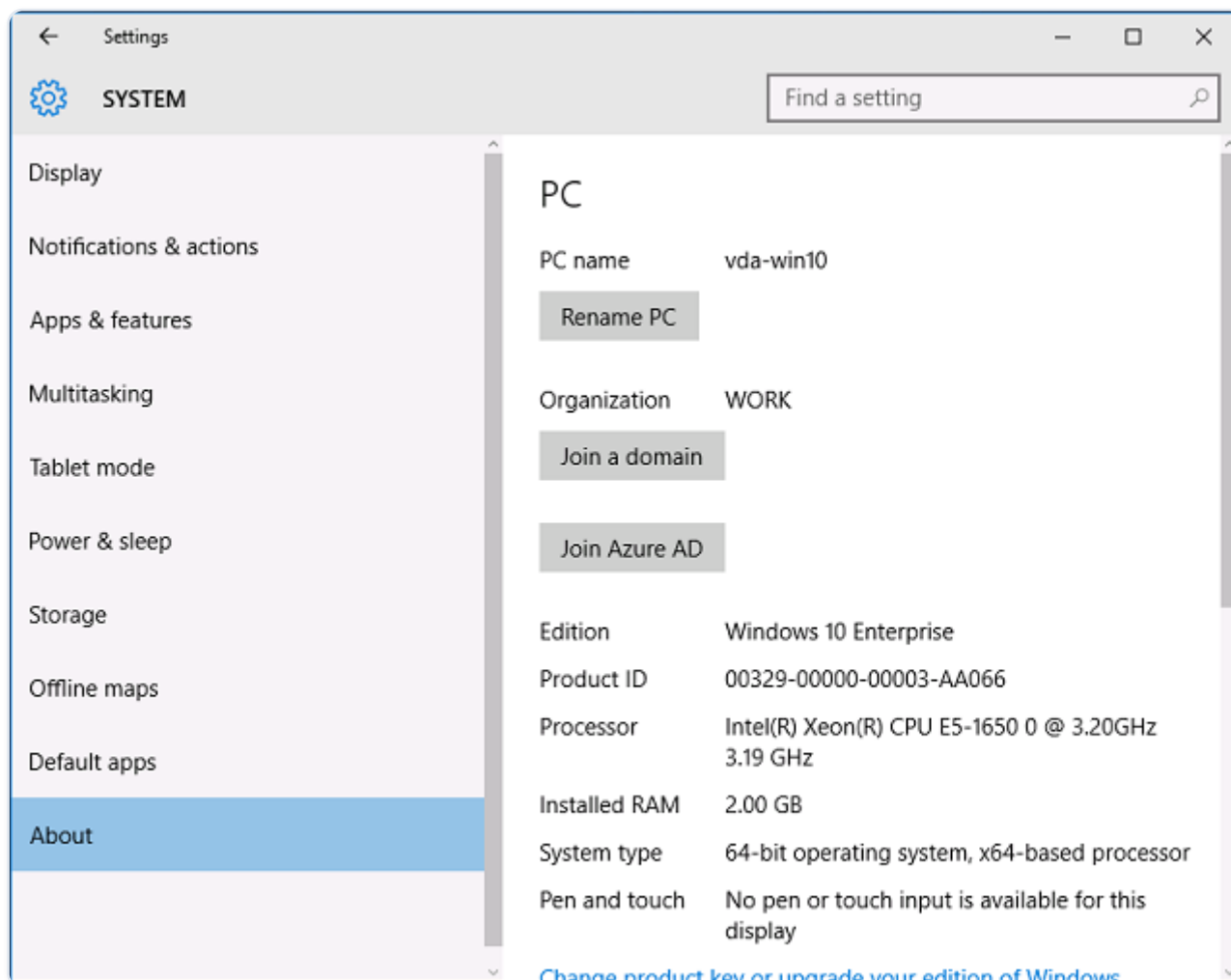
- [インストールと構成](#) は、FAS のインストールと構成に関する主要なリファレンスです。
- 一般的な FAS 展開は、[展開アーキテクチャ](#) の記事にまとめられています。
- 「ハウツー」記事は、[高度な構成](#) の記事で紹介されています。

Azure AD統合

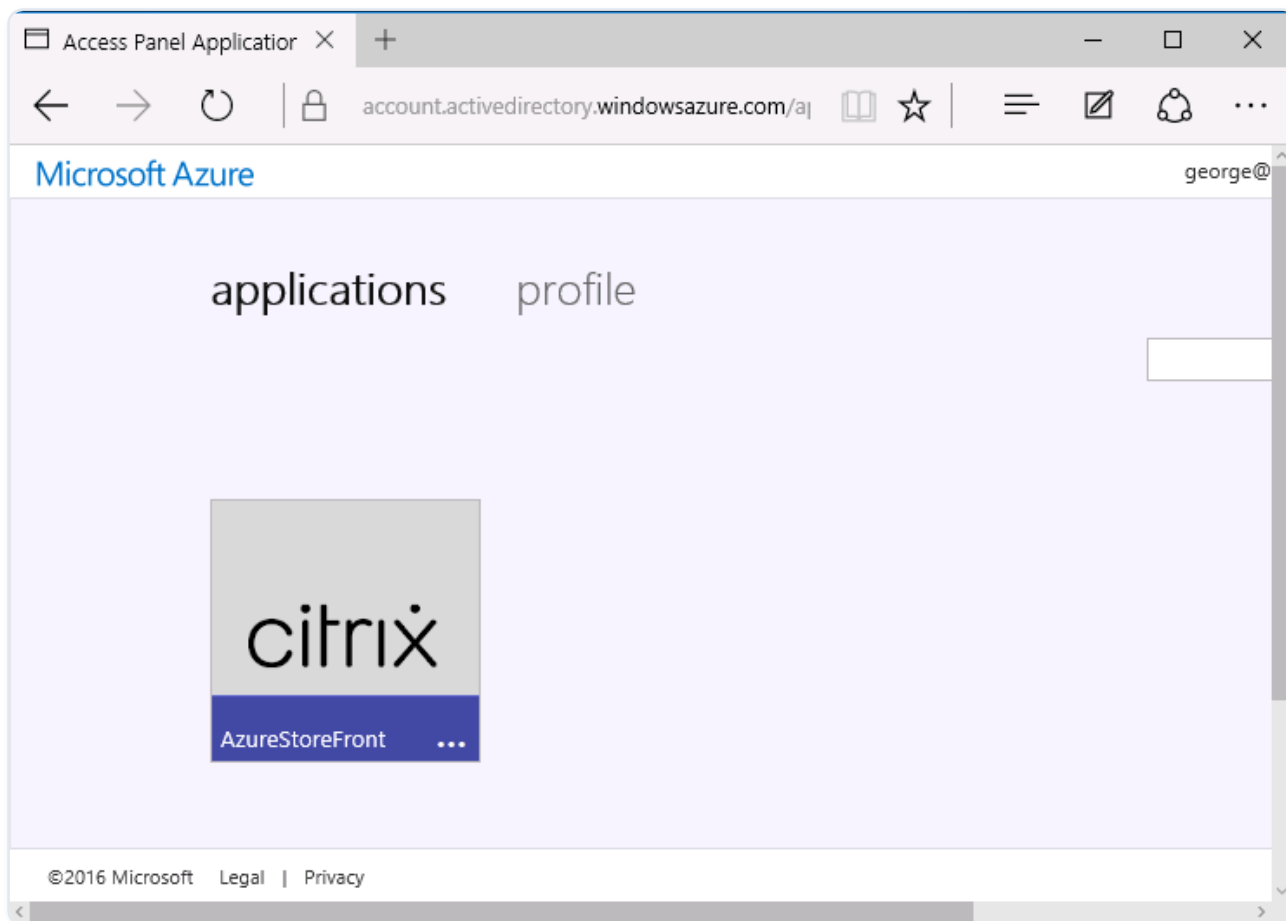
はじめに

このドキュメントでは、Citrix環境をWindows 10 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、管理とシングルサインオンのために、ローミング中のラップトップをインターネット経由で企業ドメインに参加させることができる新しいドメイン参加モデルです。

このドキュメントの展開例では、IT部門が新規ユーザーに企業メールアドレスと、個人の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。



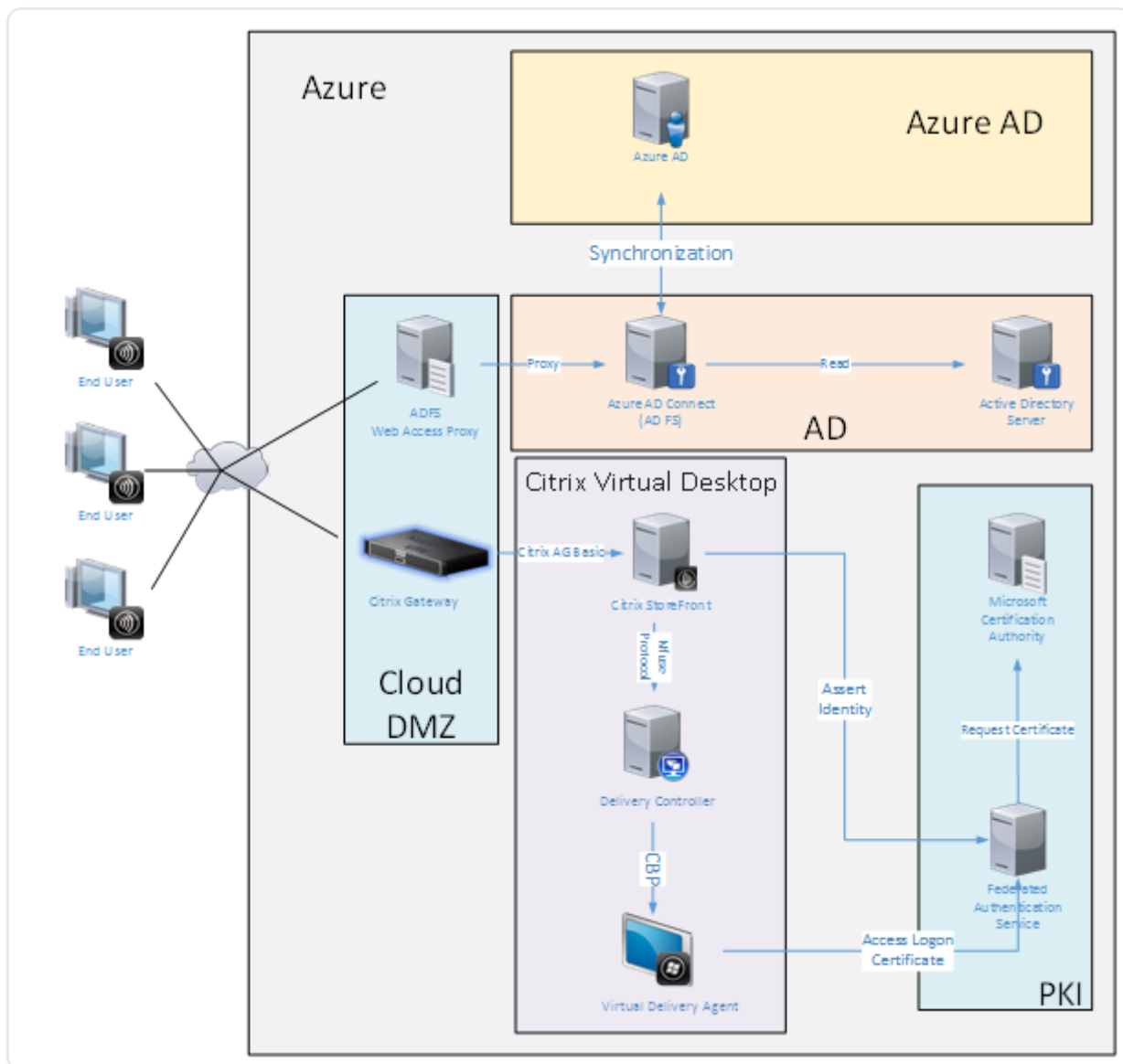
ラップトップが登録されると、Microsoft Edge Webブラウザは、Azure SaaSアプリケーションのWebページを介して、会社のWebサイトやCitrix公開アプリケーションに自動的にサインオンします。これには、Office 365などの他のAzureアプリケーションも含まれます。



アーキテクチャ

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

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



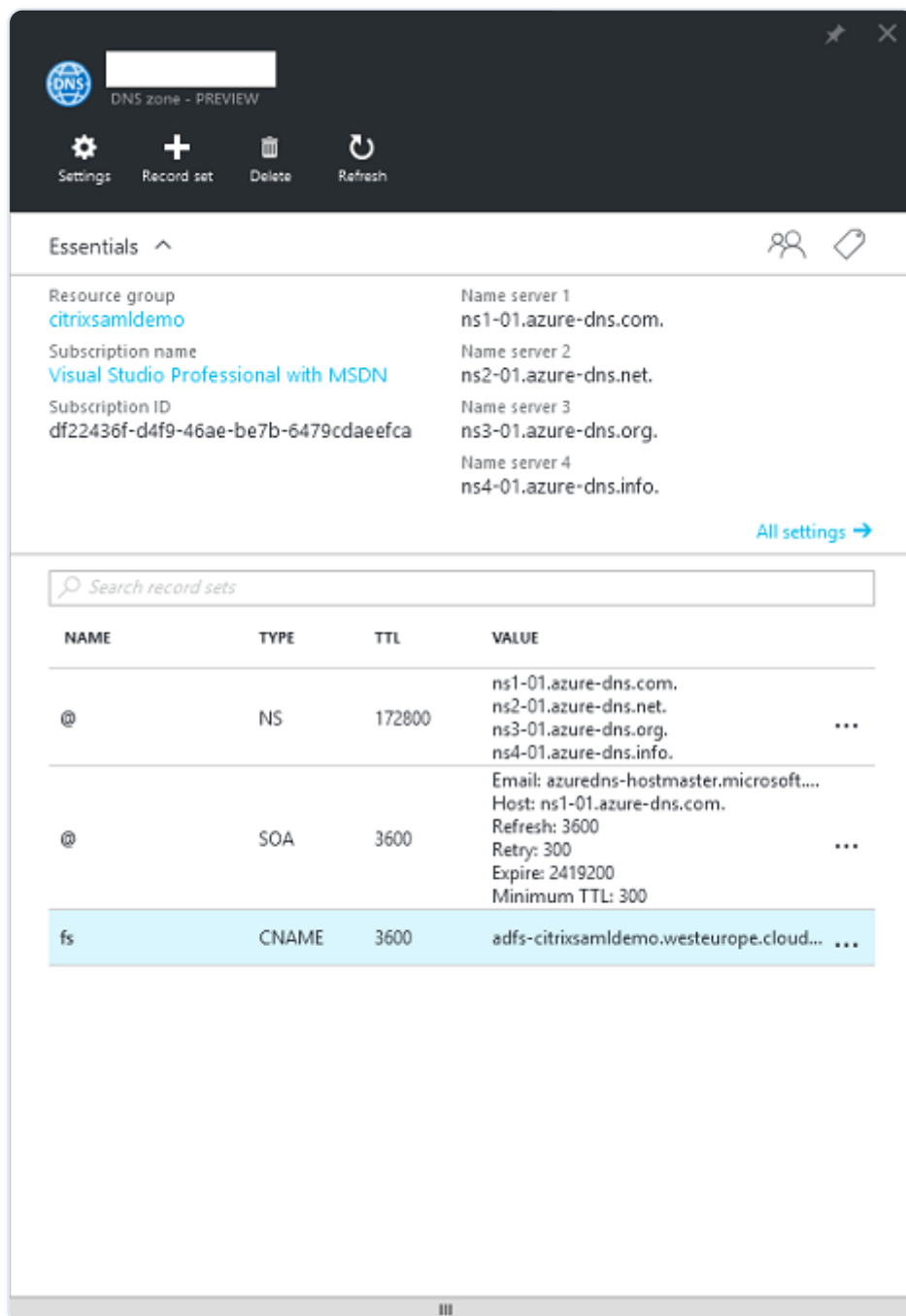
従来、ファイアウォールで保護されたLANとKerberos/NTLM認証であったセキュアな接続とシングルサインオンは、このアーキテクチャではAzureへのTLS接続とSAMLに置き換えられます。新しいサービスは、Azure ADに参加するAzureアプリケーションとして構築されます。Active Directoryを必要とする既存のアプリケーション（SQL Serverデータベースなど）は、Azure Cloud ServiceのIAAS部分で標準のActive Directory Server VMを使用して実行できます。

ユーザーが従来のアプリケーションを起動すると、Citrix Virtual Apps and Desktops™公開アプリケーションを使用してアクセスされます。さまざまな種類のアプリケーションは、Microsoft Edgeのシングルサインオン機能を使用して、ユーザーの**Azure 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ゾーンを作成する

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

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



コンソールにはAzure DNSネームサーバーの名前が表示されます。これらは、ゾーンのDNSレジストラのNSエントリで参照される必要があります（例： `citrixsamldemo.net. NS n1-01.azure-dns.com` ）。

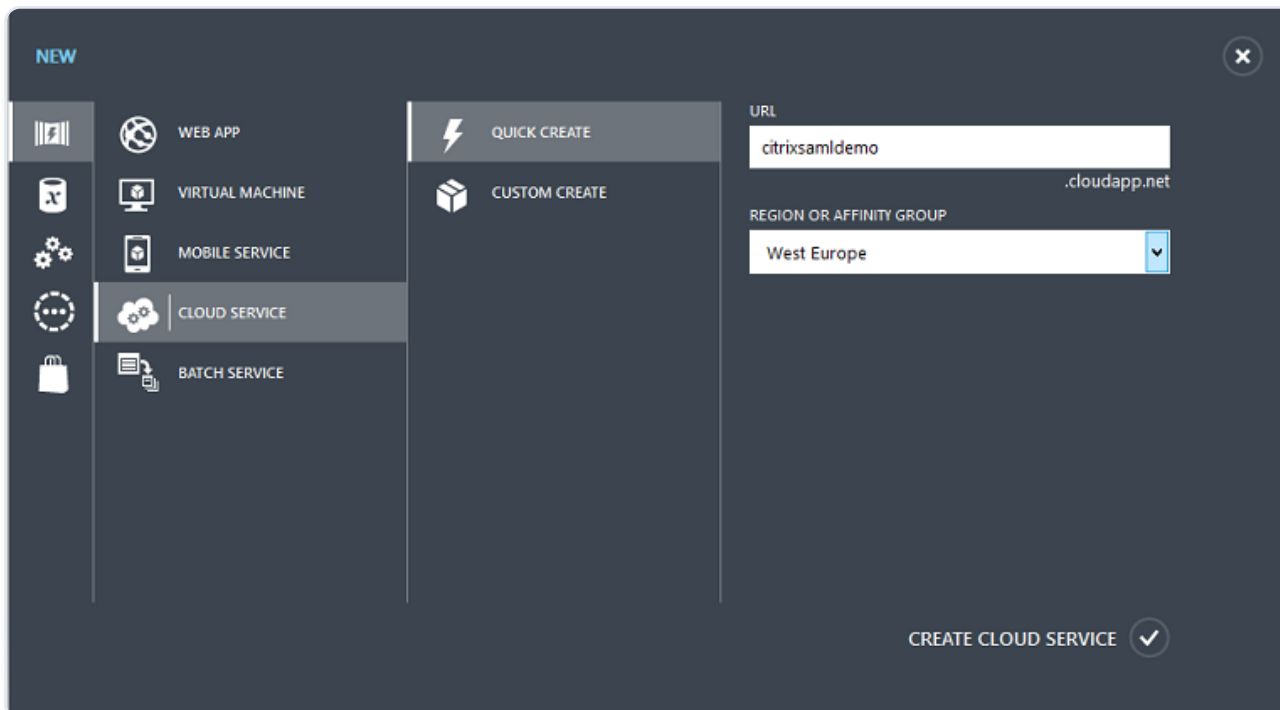
Azureで実行されているVMへの参照を追加する場合、VMのAzure管理DNSレコードへのCNAMEポインターを使用するのが最も簡単です。VMのIPアドレスが変更されても、DNSゾーンファイルを手動で更新する必要はありません。

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

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

クラウドサービスを作成する

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



Windows仮想マシンを作成する

クラウドサービスで実行されている5つのWindows VMを作成します。

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

The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The left sidebar contains navigation links: New, Resource groups, All resources, Recent, App Services, Virtual machines (classic), Virtual machines, SQL databases, Cloud services (classic), Security Center, and Subscriptions. The main area is titled 'Create virtual machine' and 'Basics'. A progress bar shows four steps: 1 Basics (Configure basic settings), 2 Size (Choose virtual machine size), 3 Settings (Configure optional features), and 4 Summary (Windows Server 2012 R2 Datacenter). The 'Basics' step is active, displaying a form with the following fields: Name (text input), User name (text input), Password (password input), Subscription (dropdown menu showing 'Visual Studio Professional with MSDN'), Resource group (dropdown menu showing 'citrixsaml-demo'), and Location (dropdown menu showing 'West Europe'). An 'OK' button is located at the bottom right of the form.

ドメインコントローラー

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

ADFSコントローラーとWebアプリケーションプロキシサーバー

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

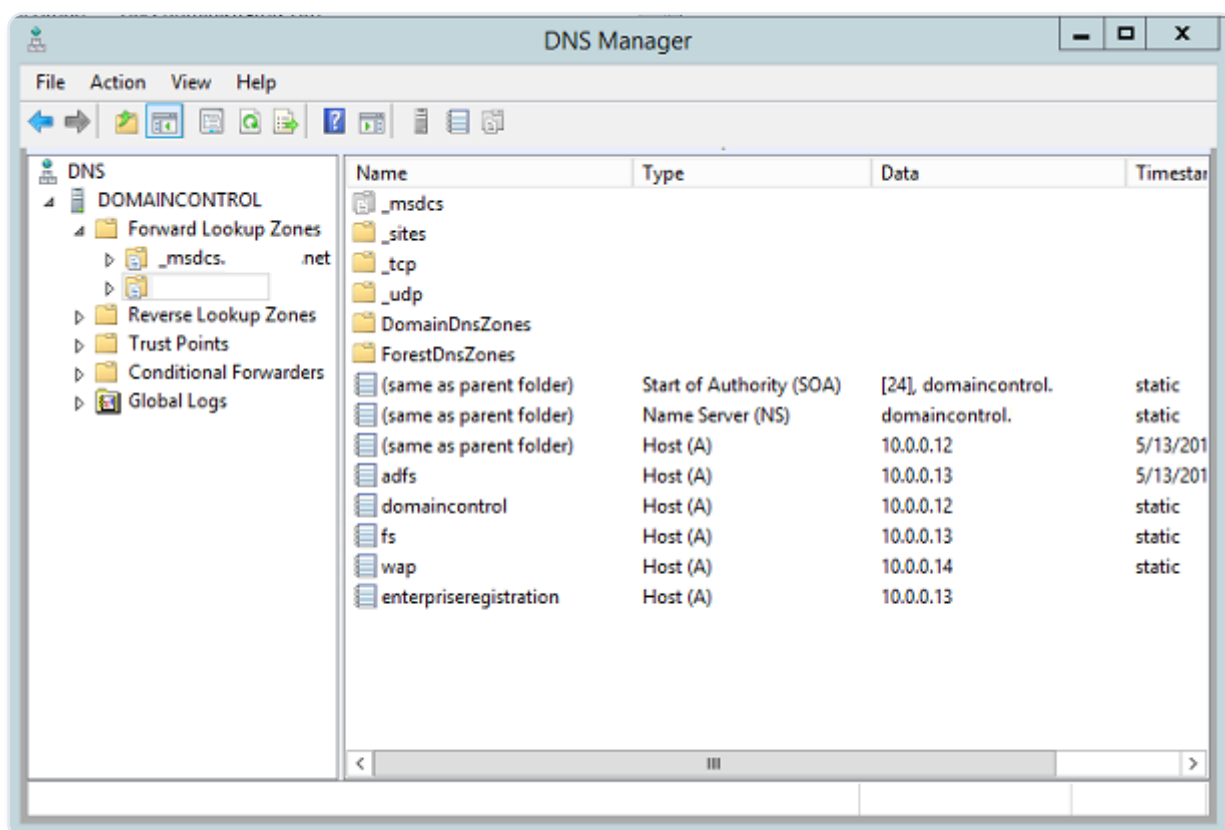
- AzureAD Connectツールからのファイアウォール経由のPSリモート処理を許可するために、これらのサーバーで**Enable-PSRemoting -Force**コマンドレットを実行します。

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

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



静的レコードを追加します。

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

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-config-internal-dns-dnsservers.png)

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

外部DNSアドレスを構成する

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-config-external-dns-configuration.png)

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

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ることに注意してください。(構成中は、パブリックIPアドレスが環境へのRDPアクセスに使用されます)。

セキュリティグループを構成する

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-config-security-groups.png)

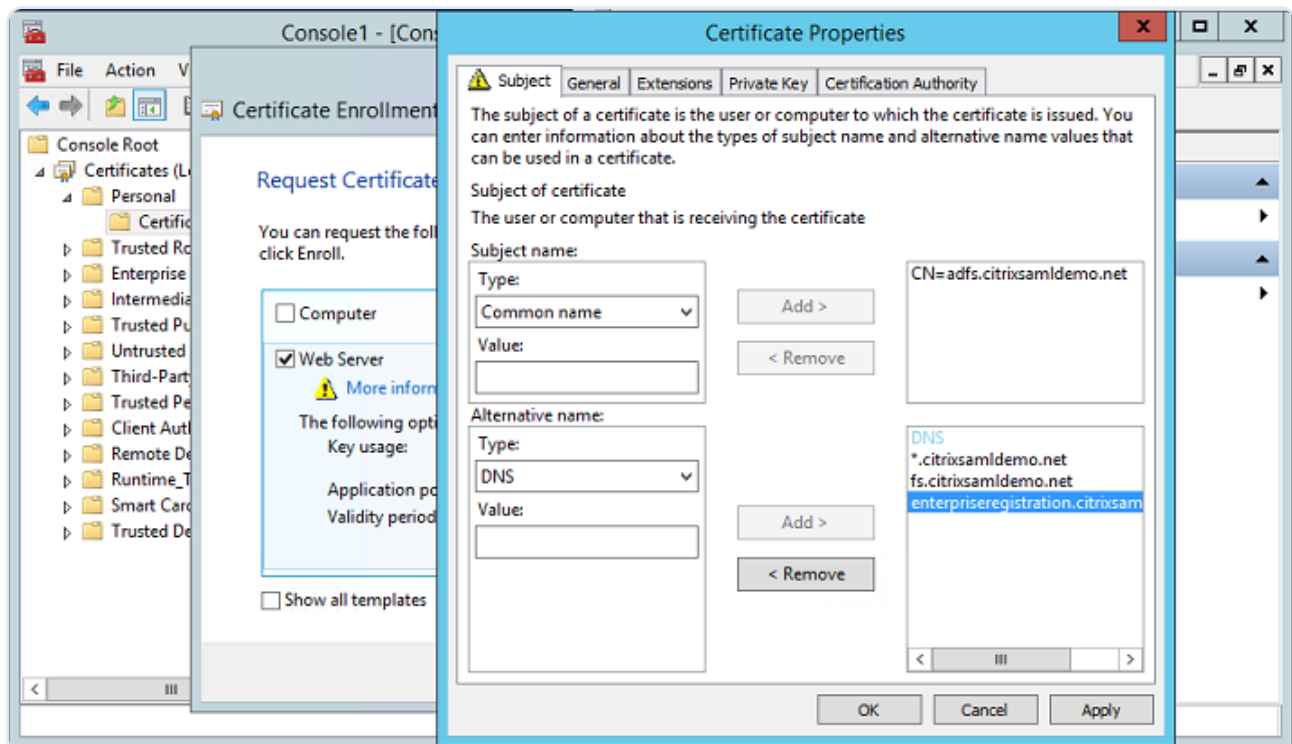
ADFS証明書を作成する

Microsoft証明機関で**Webサーバー**証明書テンプレートを有効にします。これにより、カスタムDNSアドレスを持つ証明書を作成し、pfxファイルにエクスポート（秘密鍵を含む）できるようになります。この証明書はADFSサーバーとWebアプリケーションプロキシサーバーの両方にインストールする必要があるため、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.citrixsamldemo.net

- サブジェクト代替名:
 - *.citrixsamldemo.net
 - fs.citrixsamldemo. ネット
 - enterpriseregistration.citrixsamldemo.net



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

Azure ADのセットアップ

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

新しいディレクトリの作成

クラシックAzureポータルにログインし、新しいディレクトリを作成します。

ADD DIRECTORY

DIRECTORY ⓘ

Create new directory ▼

NAME ⓘ

CitrixSAMLdemo

DOMAIN NAME ⓘ

citrixsaml demo ✓ .onmicrosoft.com

COUNTRY OR REGION ⓘ

United Kingdom ▼

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

✓

完了すると、概要ページが表示されます。

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

Azure AD にドメインを登録する

既定では、ユーザーは次の形式のメールアドレスで識別されます:

`<user.name>@<company>.onmicrosoft.com`。

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

Add domain 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構成します。この例では `citrixsamldemo.net` を使用します。

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

ADD DOMAIN

Specify a domain name

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

DOMAIN NAME

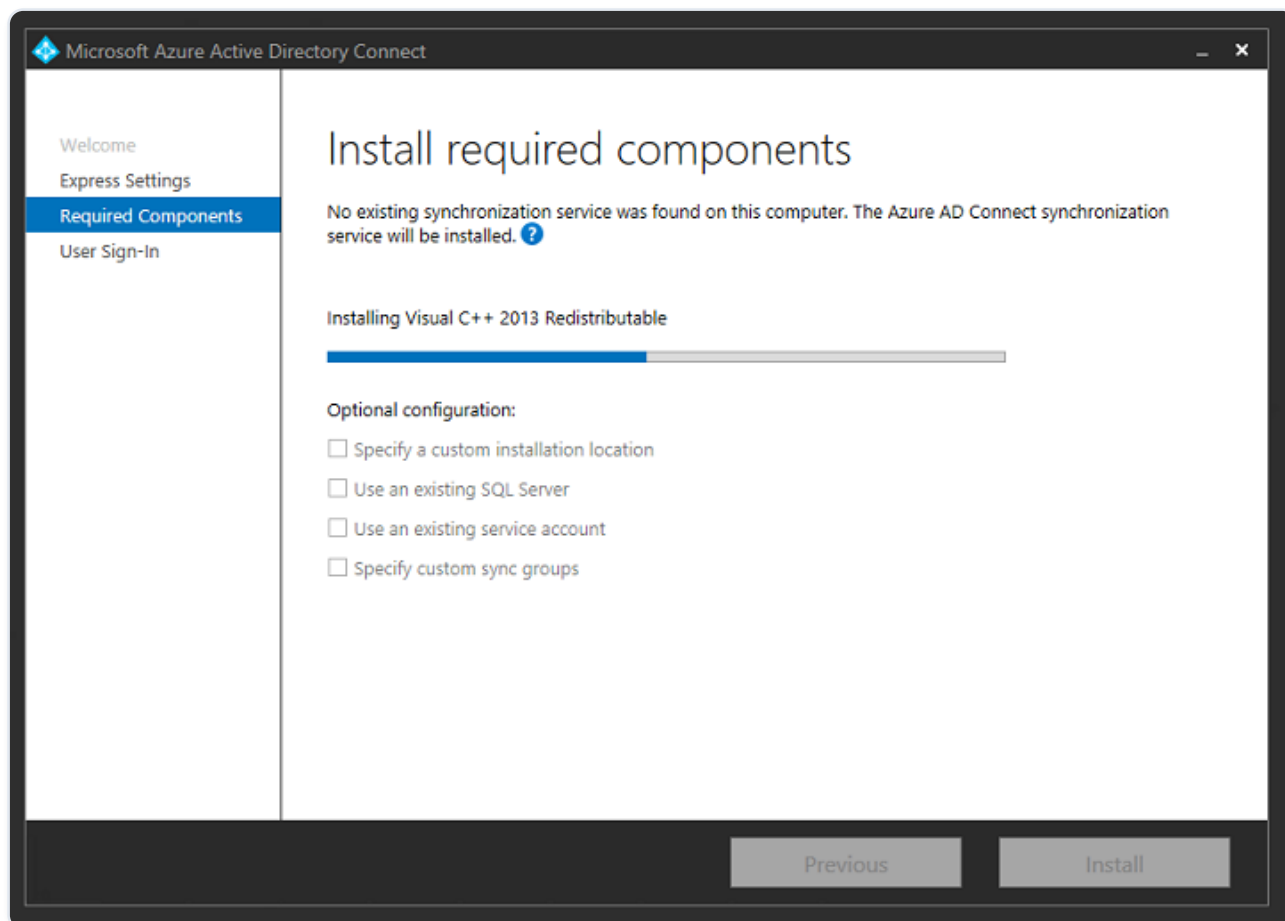
☒ I plan to configure this domain for single sign-on with my local Active Directory. ?

add

2

Azure AD Connect をインストールする

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



Federation with AD FS シングルサインオンオプションを選択します。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-setup-azure-usersignin.png)

以前に作成した管理者アカウントでAzureに接続します。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-setup-azure-connect.png)

内部ADフォレストを選択します。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-setup-azure-connect-dirs.png)

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-setup-azure-domain-ou-filter.png)

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-setup-azure-unique-id-users.png)

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-setup-azure-filter-users-devices.png)

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-setup-azure-optional-features.png)

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

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-setup-azure-adfs-farm.png)

プロキシサーバーの選択を求められたら、wap.citrixsamldemo.net サーバーのアドレスを入力します。Azure AD Connect が構成できるように、Web 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/2407/media/fas-azure-setup-azure-wap-servers.png)

注：

リモートPowerShellの信頼性の問題によりこの手順が失敗した場合は、Web 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/2407/media/fas-azure-setup-azure-azure-ad-domain.png)

TXTおよびMXレコードをAzureのDNSアドレスレコードに追加します。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-setup-azure-txt-mx.png)

Azure Management Console 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/2407/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。

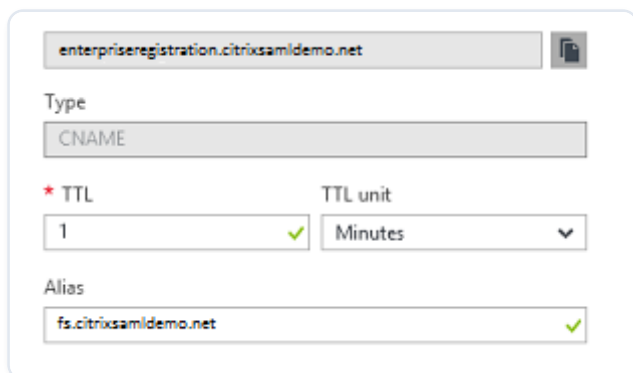
完了すると、外部アドレス fs.citrixsamldemo.net がポート 443 経由で接続されます。

ローカライズされた画像(/en-us/federated-authentication-service/2407/media/fas-azure-setup-azure-install-complete.png)

Azure AD Join を有効にする

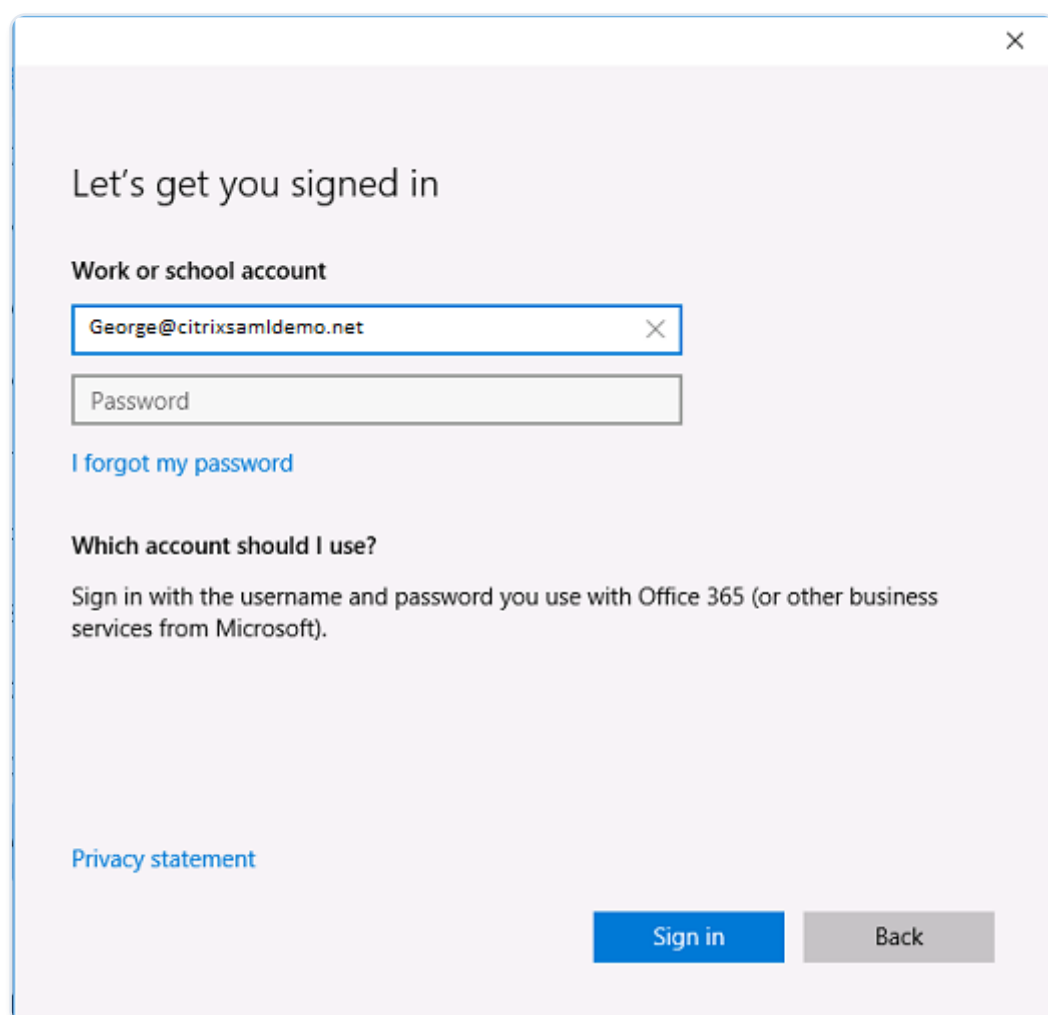
ユーザーが Windows 10 で Azure AD 参加を実行するためにメールアドレスを入力すると、DNS サフィックスが CNAME DNS レコードの構築に使用されます。このレコードは ADFS: enterpriseregistration.\<upnsuffix>を指す必要があります。

この例では、これは fs.citrixsamldemo.net です。



The screenshot shows a DNS record configuration interface. At the top, the domain 'enterpriseregistration.citrixsamldemo.net' is entered in a text box with a copy icon to its right. Below this, the 'Type' is set to 'CNAME'. The 'TTL' is set to '1' with a green checkmark, and the 'TTL unit' is set to 'Minutes' with a dropdown arrow. The 'Alias' is set to 'fs.citrixsamldemo.net' with a green checkmark.

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



Let's get you signed in

Work or school account

George@citrixsamldemo.net X

Password

[I forgot my password](#)

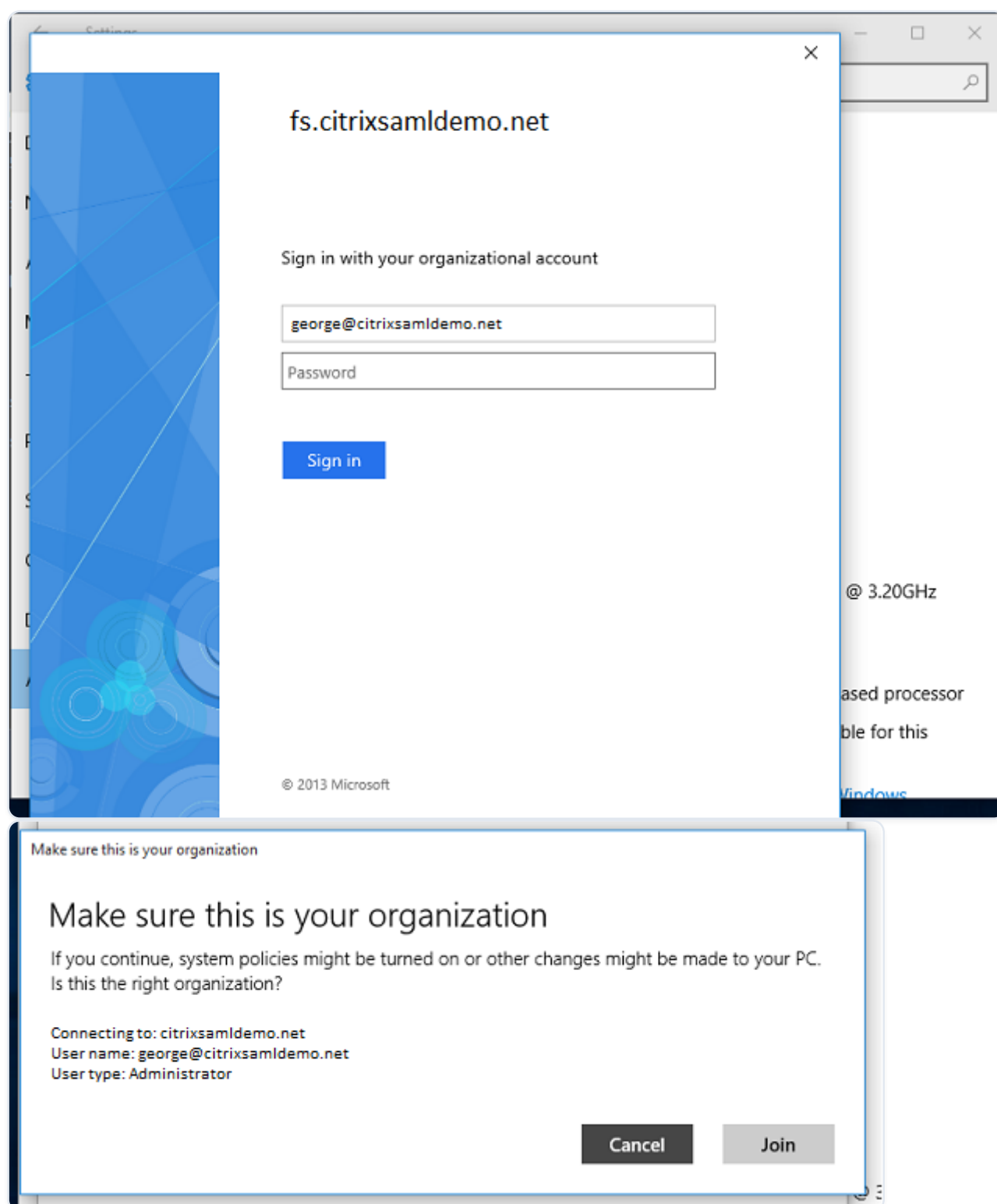
Which account should I use?

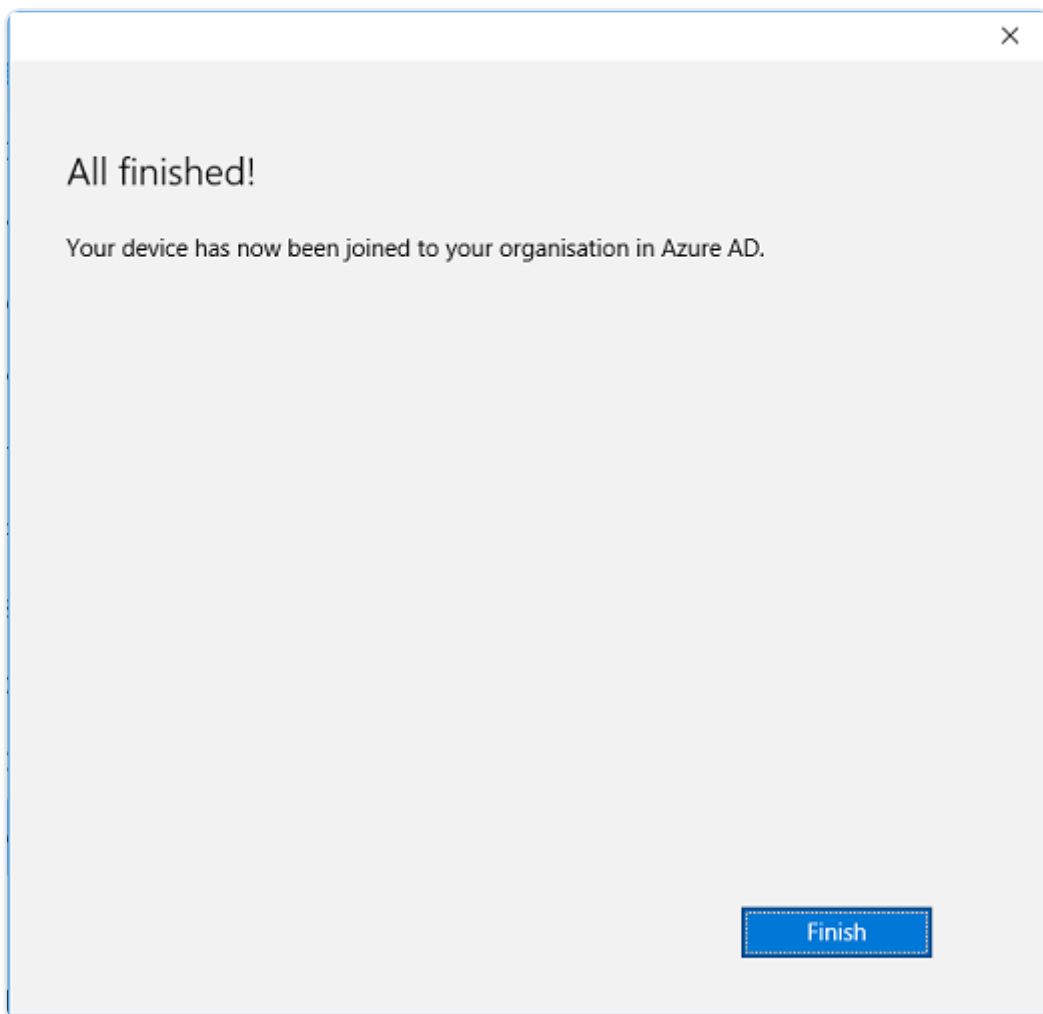
Sign in with the username and password you use with Office 365 (or other business services from Microsoft).

[Privacy statement](#)

Sign in Back

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



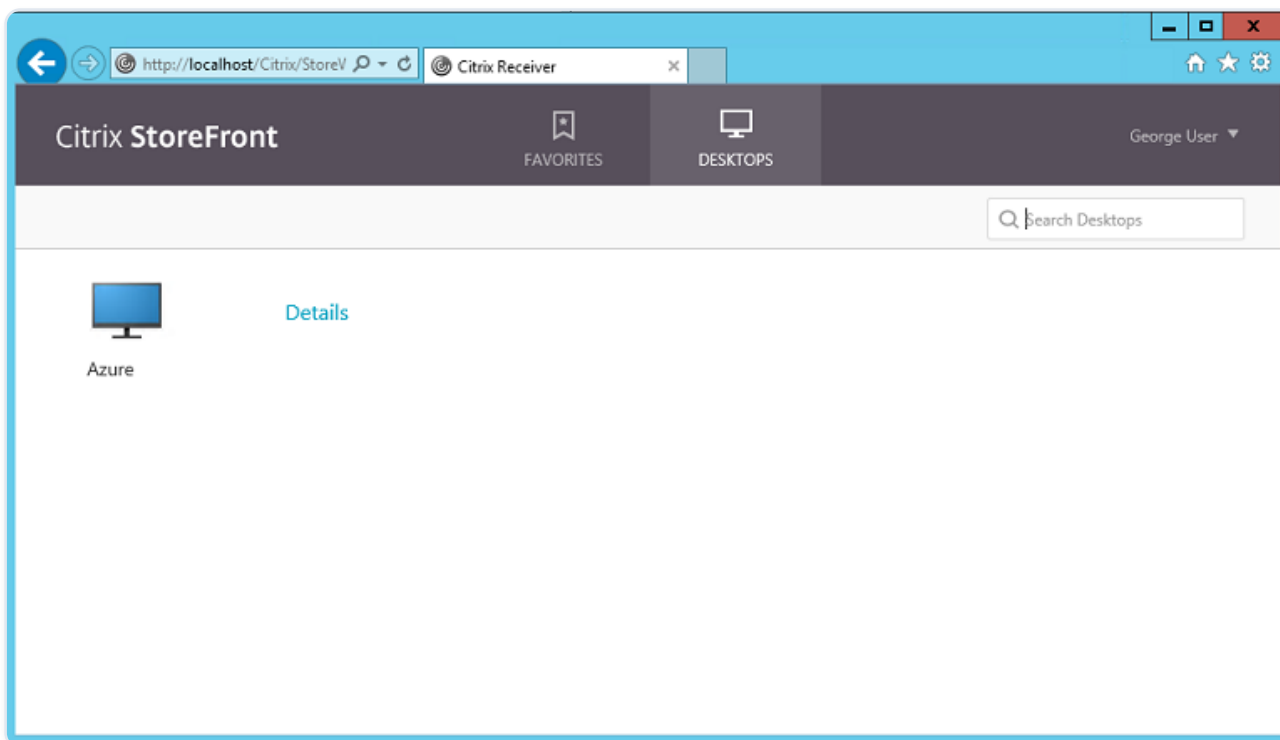


マシンを再起動し、ユーザーのメールアドレスを使用してログオンすることで、Azure AD参加が成功したことを確認します。ログオンしたら、Microsoft Edgeを起動し、`<http://myapps.microsoft.com>` に接続します。ウェブサイトは自動的にシングルサインオンを使用するはずです。

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

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

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



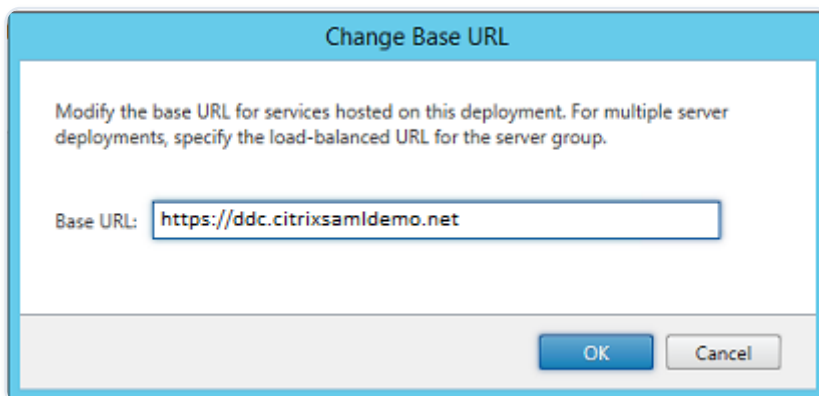
ユーザーの資格情報なしでStoreFront™が認証できるように、Controllerで **Set-BrokerSite - TrustRequestsSentToTheXmlServicePort \$true** PowerShellコマンドレットを実行します。

Federated Authentication Service のインストール

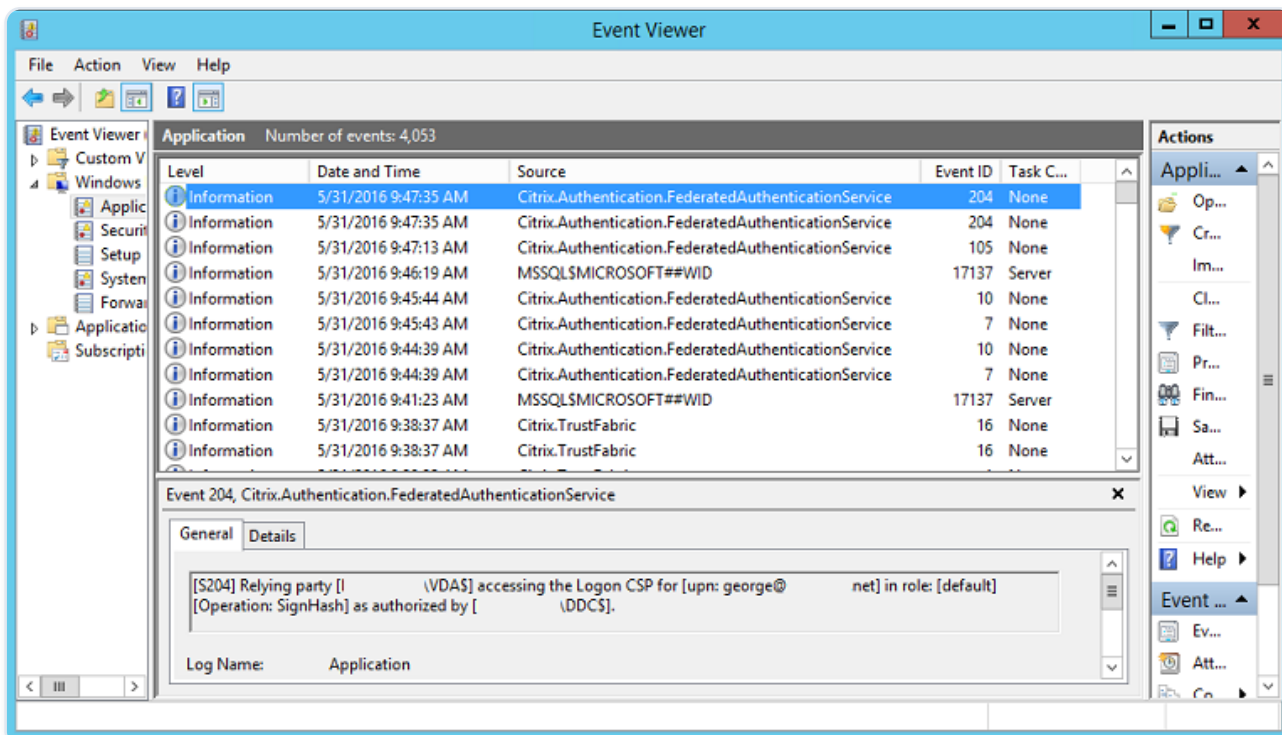
ADFSサーバーにFASをインストールし、Delivery Controllerが信頼されたStoreFrontとして機能するためのルールを構成します（この例では、StoreFrontはDelivery Controllerと同じVMにインストールされているため）。「インストールと構成」(</ja-jp/federated-authentication-service/2407/install-configure.html>)を参照してください。

StoreFrontの構成

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

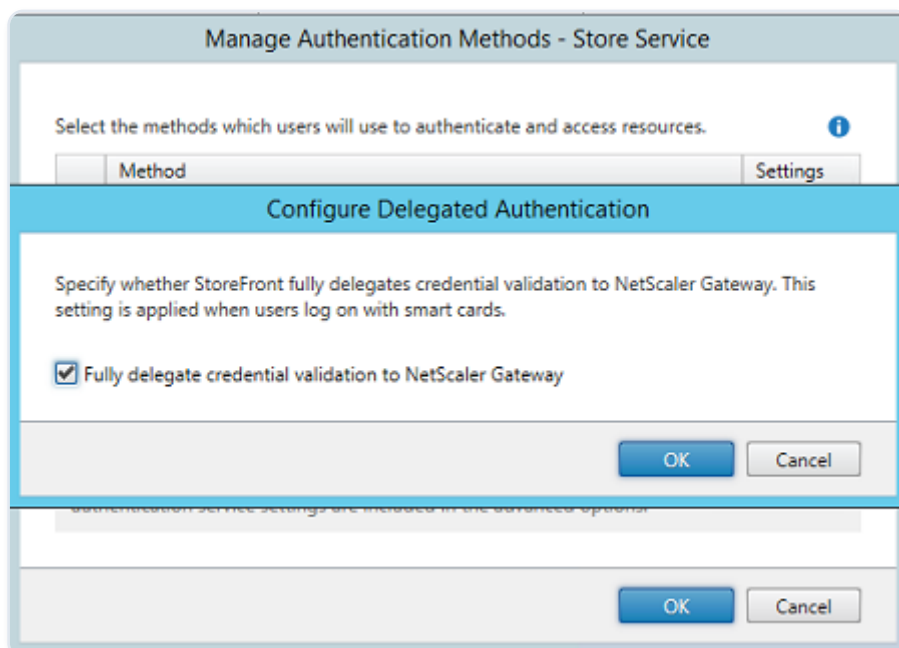


StoreFrontがFASサーバーを使用するように構成し（「インストールと構成」(/ja-jp/federated-authentication-service/2407/install-configure.html)のPowerShellスクリプトを使用）、Azure内で内部的にテストして、FASサーバーのイベントビューアーを確認することでログオンがFASを使用していることを確認します。

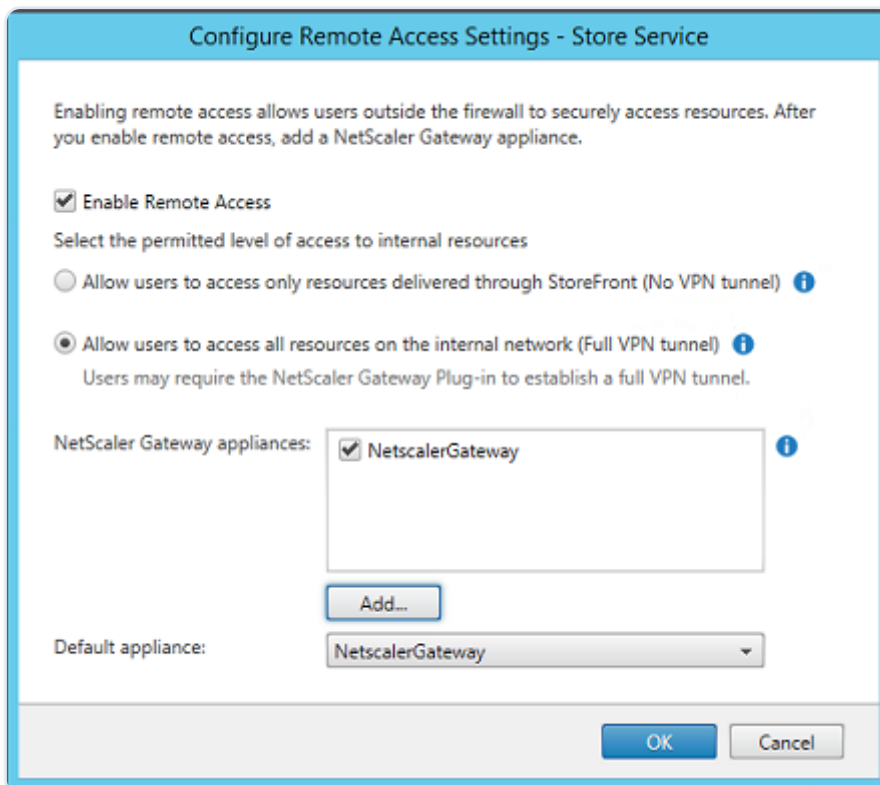


StoreFrontがCitrix Gatewayを使用するように構成する

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

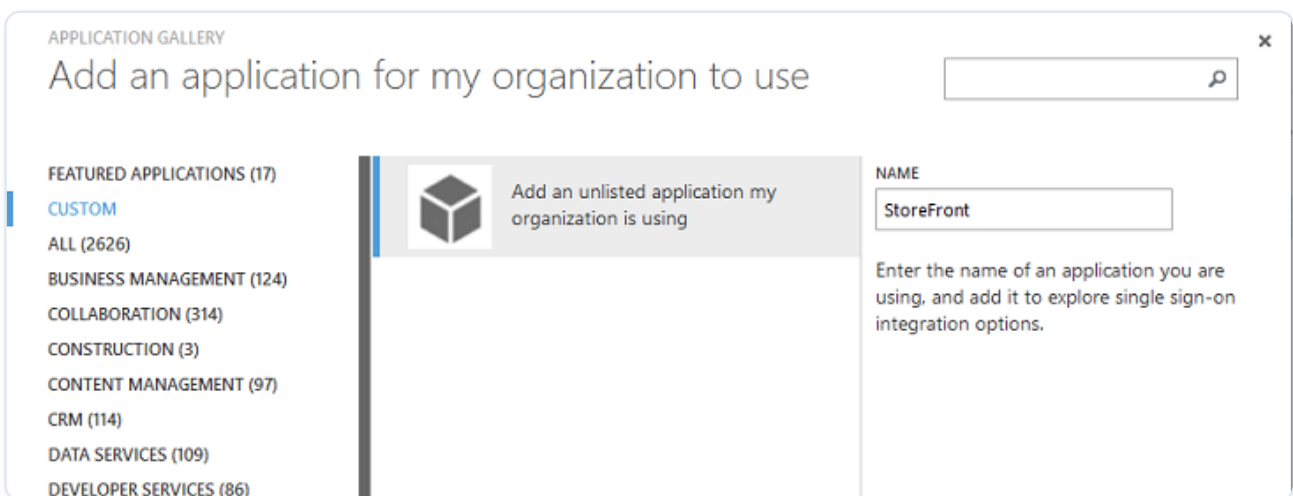


Citrix Gateway認証オプションを統合するには、Secure Ticket Authority（STA）を構成し、Citrix Gatewayアドレスを構成します。



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

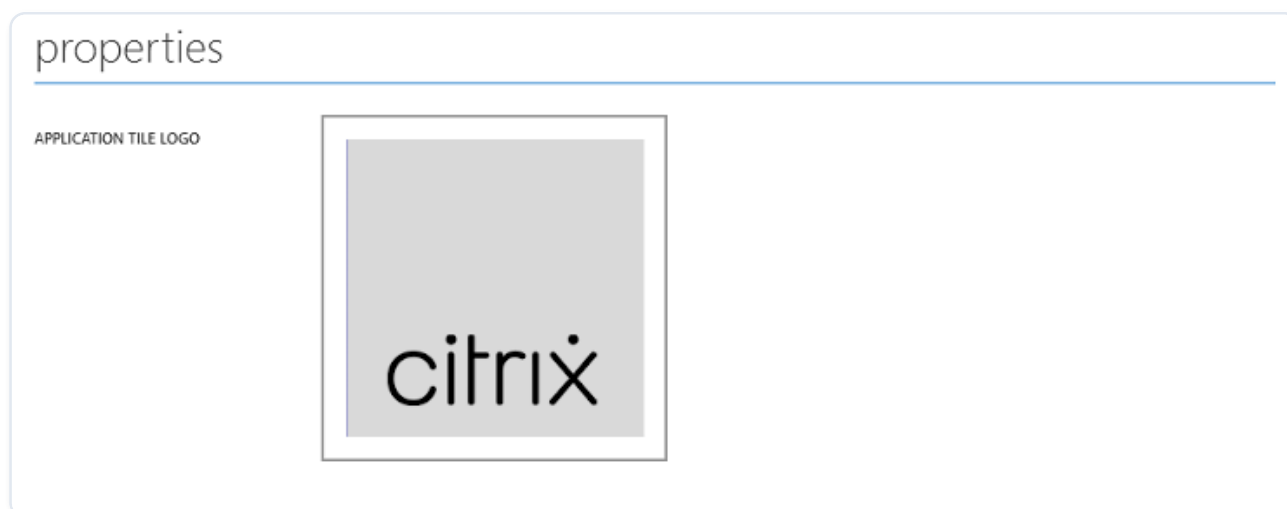
このセクションでは、現在Azure Active Directory Premiumサブスクリプションを必要とするAzure AD SAML 2.0シングルサインオン機能を使用します。Azure AD管理ツールで、**新しいアプリケーション**を選択し、**ギャラリーからアプリケーションを追加**を選択します。



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、「**カスタム > 組織が使用している一覧にないアプリケーションを追加**」を選択します。

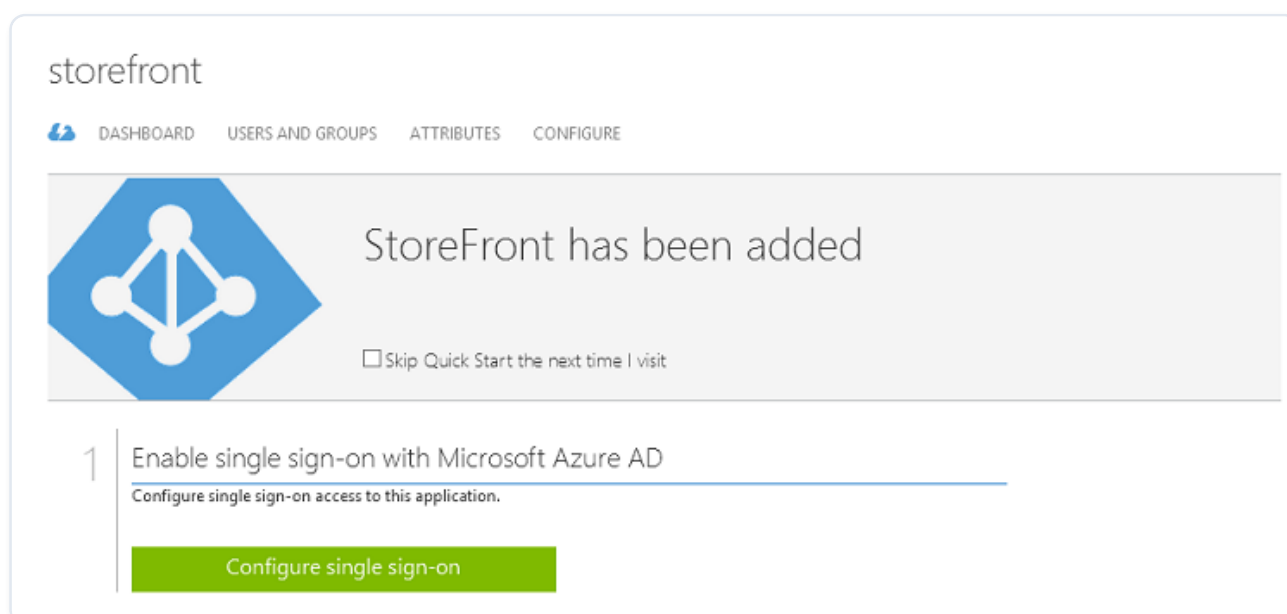
アイコンを構成する

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



SAML認証を構成する

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



この展開ではSAML 2.0認証を使用します。これは「**Microsoft Azure ADシングルサインオン**」に対応しています。

CONFIGURE SINGLE SIGN-ON

How would you like users to sign on to StoreFront?

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

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

CONFIGURE SINGLE SIGN-ON

Configure App Settings

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

IDENTIFIER ?
 ✓

REPLY URL ?
 ✓

☐ Show advanced settings (optional).

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

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

CONFIGURE SINGLE SIGN-ON

Configure single sign-on at AzureStoreFront

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

1. The following certificate will be used for federated single sign-on:
Thumbprint: 8D1E02EBF7C111EDDBBD325F5260538A9626A73B
Expiry: 05/31/2018 11:06:20 UTC

[Download Certificate \(Base 64 - most common\)](#)

[Download Certificate \(Raw\)](#)

[Download Metadata \(XML\)](#)

2. Configure the certificate and values in AzureStoreFront

ISSUER URL

SINGLE SIGN-ON SERVICE URL

SINGLE SIGN-OUT SERVICE URL

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

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

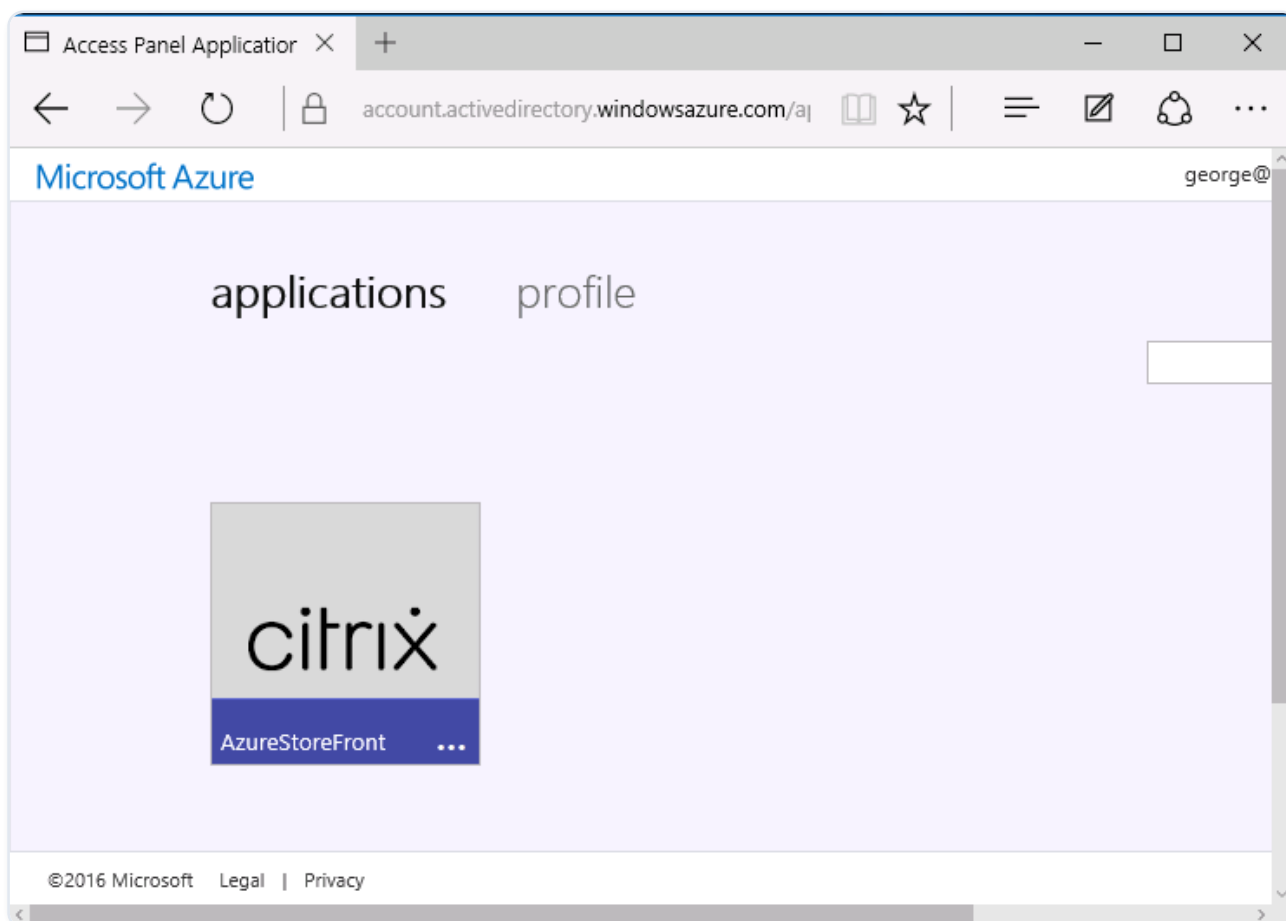
アプリケーションをユーザーに割り当てる

最後のステップは、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、ページで行います。Azure AD Connectによって同期されたドメインユーザーアカウントにアクセスを割り当てます。他のアカウントも使用できますが、それらは<user>@<domain>パターンに準拠していないため、明示的にマッピングする必要があります。

storefront						
DASHBOARD USERS AND GROUPS ATTRIBUTES CONFIGURE						
SHOW All Users						
DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT	ACCESS	METHOD	
Azure Admin	AzureAdmin@citrixsamld..			No	Unassigned	
George User	george@citrixsamldemo.net			No	Unassigned	
On-Premises Directory Sy...	Sync_ADFS_21a7e8060dcf...			No	Unassigned	

MyAppsページ

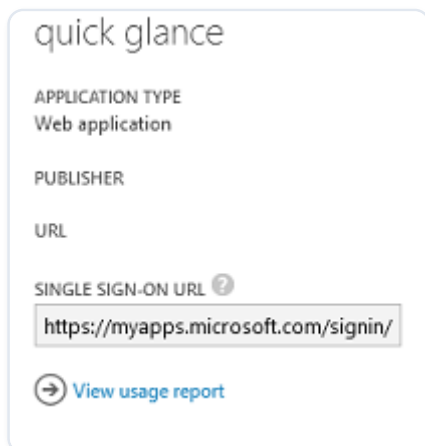
アプリケーションが構成されると、ユーザーが <https://myapps.microsoft.com> にアクセスしたときに、Azureアプリケーションのユーザーリストに表示されます。



Azure ADに参加している場合、Windows 10は、ログオン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ダッシュボードでアプリケーションに戻ります。アプリケーションでシングルサインオンURLが利用可能になりました。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対してのみ機能し、Windows 10 Azure AD参加済みログオンセッションに対してのみシングルサインオンを提供します。（他のユーザーはAzure AD資格情報の入力を求められます。）

Citrix Gatewayのインストールと構成

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

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

ライセンスを追加し、各ライセンスファイルを追加した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設定します。

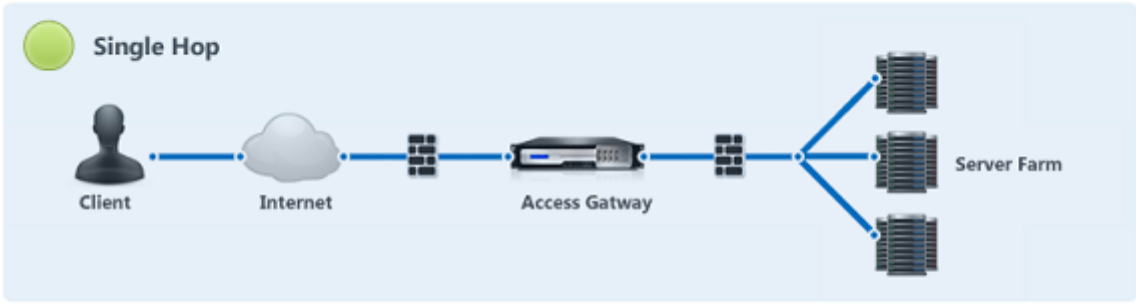
Citrix Virtual Apps and Desktopsセットアップウィザードの実行

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

XenApp/XenDesktop Setup Wizard

What is your deployment

Single Hop



The diagram illustrates a 'Single Hop' deployment architecture. It shows a 'Client' (represented by a person icon) connecting to the 'Internet' (cloud icon). From the Internet, the connection goes through an 'Access Gateway' (server rack icon) and then to a 'Server Farm' (multiple server rack icons). The components are connected in a linear fashion from Client to Internet to Access Gateway to Server Farm.

What is your Citrix Integration Point?

StoreFront

Continue Cancel

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

NetScaler Gateway Settings

NetScaler Gateway IP Address*

10 . 0 . 0 . 18

Port*

4433

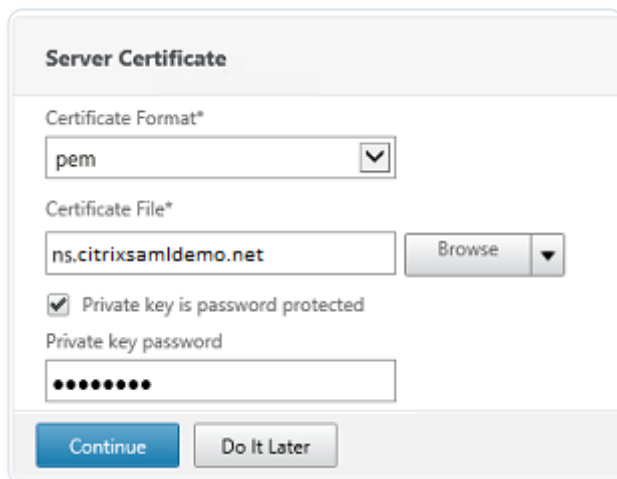
Virtual Server Name*

ns.citrixsaml demo.net

☐ Redirect requests from port 80 to secure port

Continue Cancel

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



Server Certificate

Certificate Format*
pem

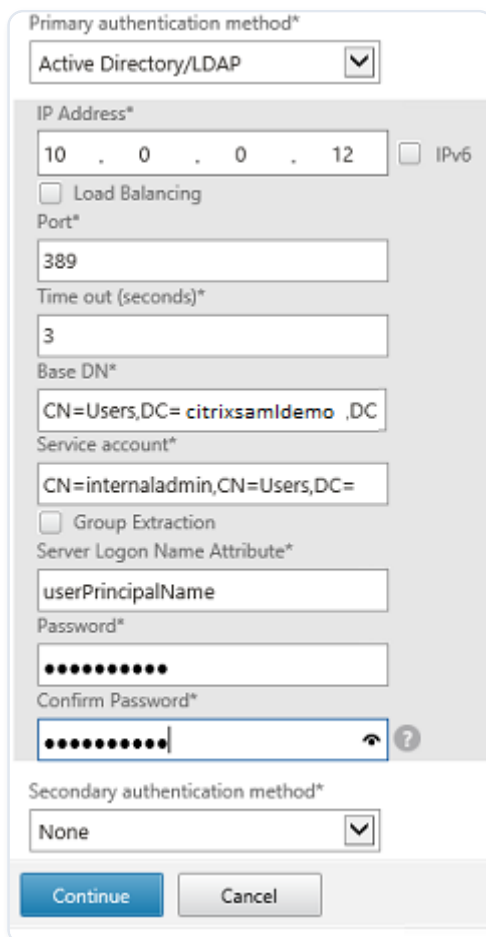
Certificate File*
ns.citrixsamldemo.net Browse

☒ Private key is password protected
Private key password
.....

Continue Do It Later

ADアカウント管理のためにドメインコントローラーを構成する

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



Primary authentication method*
Active Directory/LDAP

IP Address*
10 . 0 . 0 . 12 ☐ IPv6

☐ Load Balancing

Port*
389

Time out (seconds)*
3

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

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

☐ Group Extraction

Server Logon Name Attribute*
userPrincipalName

Password*
.....

Confirm Password*
..... ?

Secondary authentication method*
None

Continue Cancel

StoreFrontアドレスを構成する

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

StoreFront

StoreFront FQDN*

ddc.citrixsamldemo.net

Site Path*

/Citrix/StoreWeb

Single Sign-on Domain*

citrixsamldemo

Store Name*

/Citrix/StoreWeb

Secure Ticket Authority Server*

http://ddc.citrixsamldemo.net/sta

StoreFront Server*

10 . 0 . 0 . 15

Protocol*

SSL

Port*

443

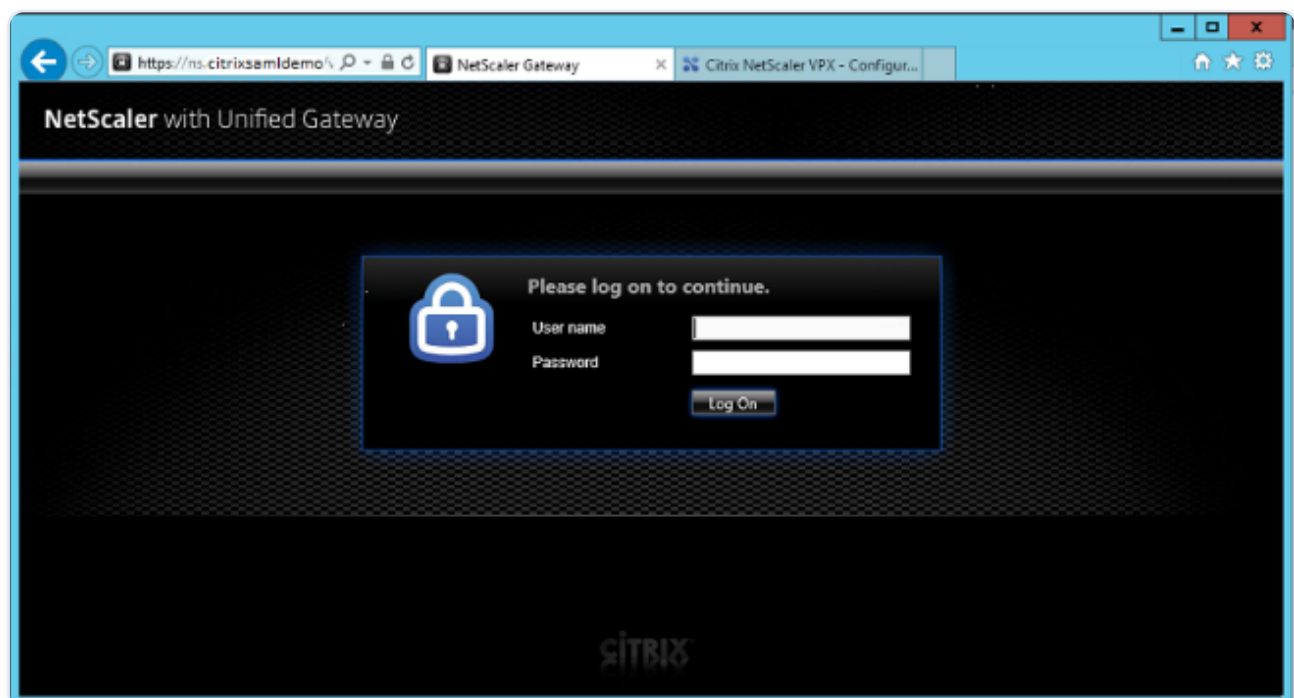
☐ Load Balancing

Continue

Cancel

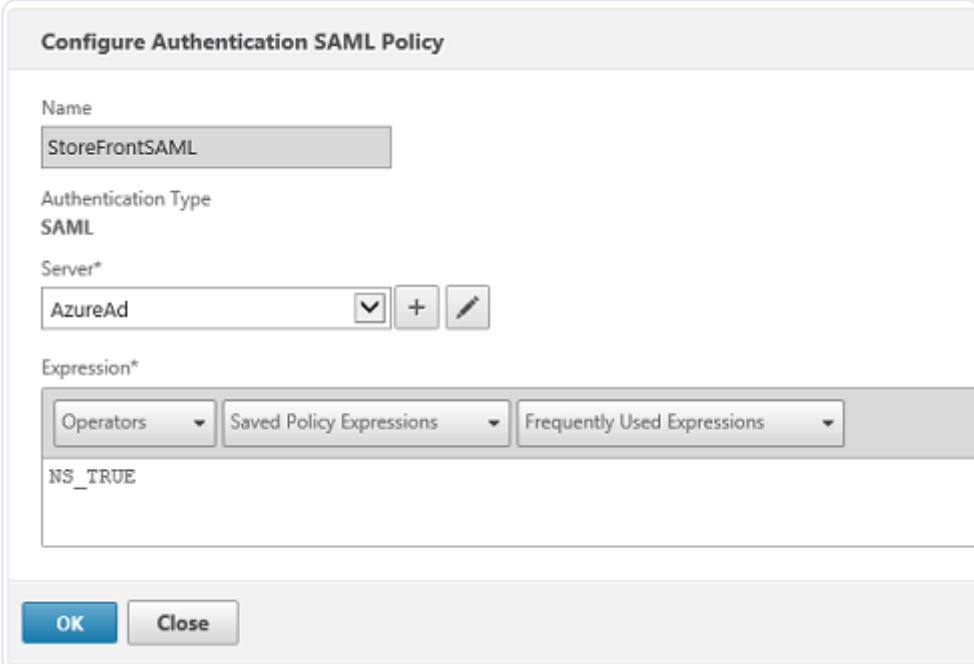
Citrix Gatewayの展開を検証する

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



Citrix Gateway SAML認証サポートを有効にする

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



The screenshot shows a dialog box titled "Configure Authentication SAML Policy". It contains the following fields and controls:

- Name:** A text box containing "StoreFrontSAML".
- Authentication Type:** A dropdown menu set to "SAML".
- Server*:** A dropdown menu set to "AzureAd", with a checkmark icon, a plus icon, and an edit icon.
- Expression*:** A section with three dropdown menus: "Operators", "Saved Policy Expressions", and "Frequently Used Expressions". Below these, a text box contains the expression "NS_TRUE".
- Buttons:** "OK" and "Close" buttons at the bottom left.

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

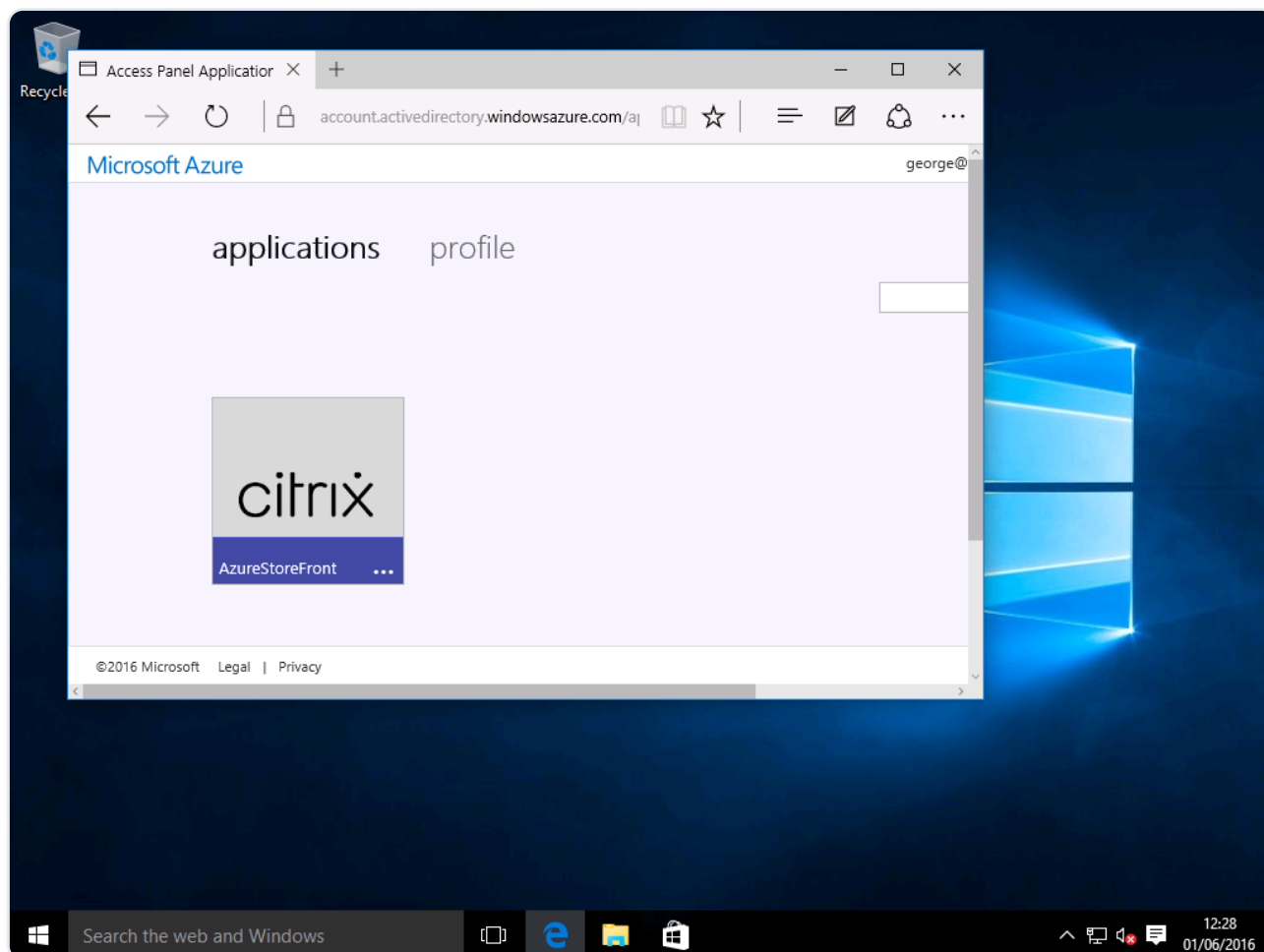
Attribute 1
Attribute 3
Attribute 5
Attribute 7

Attri
Attri
Attri
Attri

エンドツーエンドシステムを検証する

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

Webブラウザに、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。



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によって、Microsoft Azureにリダイレクトされ、元に戻ることを確認します。

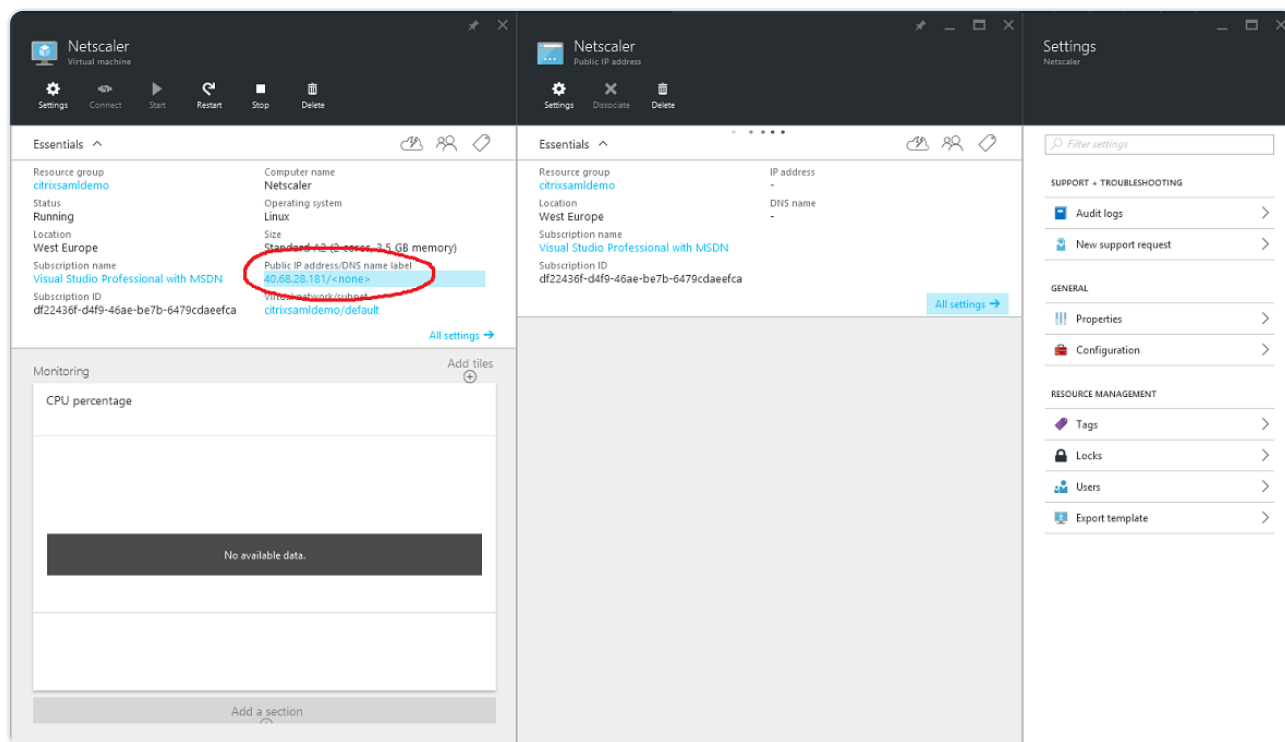
最後に、Azure ADに参加していないマシンでも同じURLで機能することを確認します（ただし、最初の接続ではAzure ADへの明示的なシングルサインオンが1回発生します）。

付録

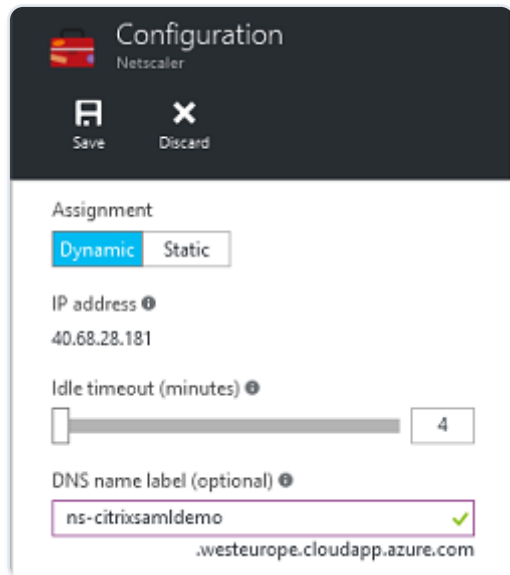
AzureでVMをセットアップする際には、以下の標準オプションを構成する必要があります。

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。



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

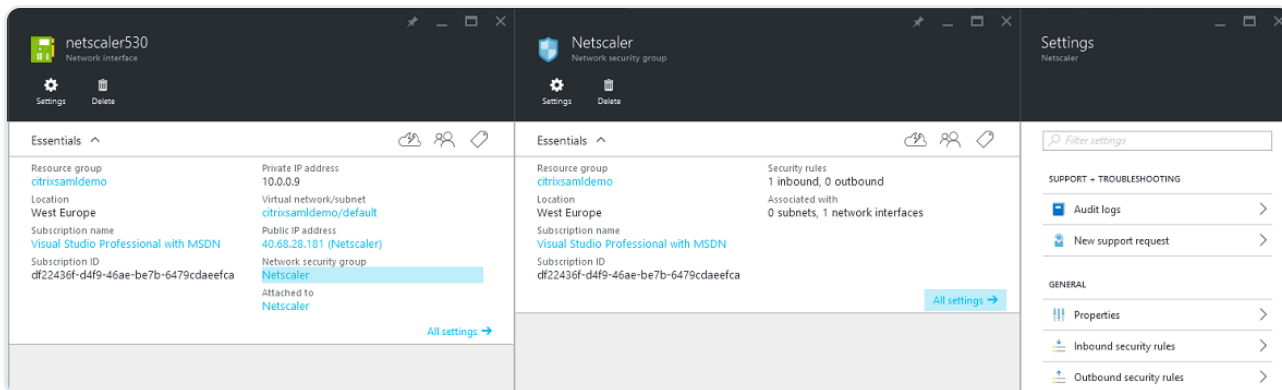


ファイアウォールルール (セキュリティグループ) を設定する

クラウド内の各 VM には、セキュリティグループとして知られる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 はすべての VM への

RDP 転送を許可します。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。



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。

フェデレーション認証サービス2407ドキュメント履歴

次の表に、フェデレーション認証サービス2407のドキュメントに対する重要な変更点を示します。これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

日付	変更	説明
31 Jul 2024	Citrixフェデレーション認証サービス2407の初期リリース	詳しくは、「 新機能 」を参照してください。