フェデレーション認証サービス

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

フェデレーション認証サービス 2305 9
フェデレーション認証サービス 2305 10
修正された問題 10
既知の問題 10
サードパーティ通知 10
システム要件 11
インストールと構成 12
インストールとセットアップの順序 12
フェデレーション認証サービスをインストールする 12
FASのアップグレード 13
StoreFrontストアでFASプラグインを有効にする 13
Delivery Controller™を構成する 14
グループポリシーを構成する 15
セッション内の動作 18
プロンプトの範囲 19
同意のタイムアウト 20
ロック時の切断 20
フェデレーション認証サービス管理コンソールの使用 20
証明書テンプレートを展開する 21
Active Directory証明書サービスをセットアップする 22
フェデレーション認証サービスを承認する 23
ルールを構成する 23
Citrix Cloudへの接続 26
Citrix Cloud から切断する 28
高度な構成 29
関連情報 29

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

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 29
前提条件 29
MSP顧客を構成する 29
既知の問題 32
Azure Active Directory シングルサインオン 32
ドメイン参加済み VDA 33
ハイブリッド参加済みVDA 34
証明機関の構成 35
FASで使用する複数のCAサーバーをセットアップする 36
予期される動作の変更 36
TCPアクセス用にMicrosoft証明機関を構成する 36
ユーザー証明書の事前生成 37
Active Directoryユーザーのリストを取得する 37
FASサーバー 38
登録機関証明書を更新する 39
関連情報 40
秘密鍵の保護 41
はじめに 41
秘密鍵の構成設定 42
構成シナリオの例 45
例1 45
例 2 45
例3 56
FAS 証明書ストレージ 58
関連情報 60
セキュリティとネットワーク構成 60
ネットワークアーキテクチャ 60
ファイアウォールとネットワークセキュリティ 61

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

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 62
セキュリティに関する考慮事項 63
委任された登録エージェント 63
アクセス制御リストの構成 63
ファイアウォール設定 63
イベントログの監視 64
ハードウェアセキュリティモジュール 64
管理者の責任 65
グループポリシー設定 65
証明書テンプレート 65
証明書テンプレートの名前を変更する 66
一般プロパティの変更 66
要求処理プロパティの変更 66
暗号化プロパティの変更 66
キー構成証明プロパティの変更 66
「廃止されたテンプレート」プロパティの変更 67
「拡張機能」プロパティの変更 67
「セキュリティ」プロパティの変更 67
「サブジェクト名」プロパティの変更 67
「サーバー」プロパティの変更 67
発行要件プロパティの変更 67
互換性プロパティの変更 68
証明機関の管理 68
テンプレートの公開 68
ファイアウォール設定 69
登録の制限 69
ポリシーモジュールと監査 69
FAS管理 69

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

ACLによるStoreFront、ユーザー、およびVDAの制限 70
ルールの構成 70
証明機関とテンプレートを構成する 70
セッション内および認証証明書 71
秘密鍵の保護と鍵長 71
イベントログ 71
管理アクセスと管理ツール 71
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 71
一般的なWindowsサーバーセキュリティ 71
関連情報 72
パフォーマンスカウンター 72
Windowsログオンの問題のトラブルシューティング 74
証明書と公開鍵インフラストラクチャ 74
UPN名と証明書マッピング 75
Active DirectoryにおけるUPN名 75
証明書マッピングサービス 76
ログオンドメインコントローラーの選択を制御する 76
ドメインコントローラーの選択を制御する 76
使用中のドメインコントローラーを特定する 77
アカウント監査イベントを有効にする 77
証明書検証ログ 77
証明書の有効性を確認する 77
CAPIログを有効にする 77
CAPIログ 78
エラーメッセージ 78
Kerberosログ 79
ドメインコントローラーおよびワークステーションログ 79

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

ドメインコントローラー CAPI2 ログ 80
ドメインコントローラー セキュリティログ 80
VDA セキュリティログ 80
VDA CAPIログ 80
VDAシステムログ 81
Windowsイベントログを使用したFASの監視 81
FASサービスは実行中ですか? 81
FASヘルスイベント 81
クラウド接続FASイベント 83
セキュリティイベント 84
FASイベントログ 85
管理イベント 85
IDアサーションの作成 87
依拠当事者として機能する 88
セッション内証明書サーバー 89
FASアサーションプラグイン 89
Workspace対応のFAS 90
ログオン 92
セッション内証明書 92
証明書要求とキーペア生成 93
エンドユーザーのエラーメッセージ 93
関連情報 94
PowerShell コマンドレット 94
展開アーキテクチャ 96
はじめに 96
アーキテクチャの概要 96
内部展開 97
シトリックス ゲートウェイ 展開 100

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

ADFS SAML展開 101
B2Bアカウントマッピング 101
ウィンドウズ 10 アジュール AD ジョイン 102
ADFS展開 104
はじめに 104
SAMLの概要 106
リダイレクトURL 106
識別子 106
戻りアドレス 106
署名証明書 106
シングルサインアウト URL 107
構成 107
SAML ポリシーの入力 107
関連情報 107
Azure AD 統合 108
はじめに 108
アーキテクチャ 109
DNSゾーンの作成 111
クラウドサービスの作成 112
Windows仮想マシンの作成 112
ドメインコントローラー 113
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 113
Citrix Virtual Desktops™ デリバリーコントローラーおよびVDA 114
内部DNSの構成 114
外部 DNS アドレスを構成する 115
セキュリティグループを構成する 116
ADFS 証明書を作成する 116
Azure ADをセットアップする 117

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

新しいディレクトリを作成する 117
グローバル管理者ユーザー (AzureAdmin) を作成する 119
ドメインを Azure AD に登録する 120
Azure AD Connect をインストールする 121
Azure AD Join を有効にする 131
Citrix Virtual AppsまたはCitrix Virtual Desktopsをインストールする 134
Federated Authentication Serviceをインストールする 135
StoreFrontを構成する 135
StoreFrontがCitrix Gatewayを使用するように構成する 136
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 137
アイコンの構成 138
SAML認証の構成 138
アプリケーションをユーザーに割り当てる 138
MyAppsページ 139
シングルサインオンURL 139
Citrix Gatewayのインストールと構成 139
Citrix Virtual Apps and Desktopsセットアップウィザードを実行する 140
ADアカウント管理のためにドメインコントローラーを構成する 141
StoreFrontアドレスを構成する 141
Citrix Gatewayの展開を確認する 142
Citrix Gateway SAML認証サポートを有効にする 143
エンドツーエンドシステムを検証する 144
付録 145
パブリックIPアドレスとDNSアドレスを提供する 145
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 146
関連情報 147
フェデレーション認証サービス 2303 ドキュメント履歴 148

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

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 (FAS) は、Active Directory証明書サービスと統合するように設計された特権コンポーネントです。これは、ユーザーに証明書を動的に発行し、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ます。

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

フェデレーション認証サービス 2305

この Federated Authentication Service のリリースには、新機能は含まれていません。

バグ修正に関する情報については、修正された問題を参照してください。

修正された問題

Federated Authentication Service 2305 には、修正された問題はありません。

既知の問題

Federated Authentication Service 2305には既知の問題はありません。

レジストリエントリの変更を推奨する回避策には、以下の警告が適用されます。

警告：

レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターの使用は自己責任で行ってください。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

Federated Authentication Service の本リリースには、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る場合があります。

- Citrix Virtual Apps and Desktops サードパーティ通知 (PDF ダウンロード)
- FlexNet Publisher 2017 (11.15.0.0) の非商用ソフトウェア開示 (PDF ダウンロード)
- FlexNet Publisher 11.15.0 で使用されている FlexNet Publisher ドキュメント補足 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)

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

システム要件

- Federated Authentication Service (FAS) は、以下の Windows Server バージョンでサポートされています。
  - Windows Server 2022、Standard および Datacenter エディション
  - Windows Server 2019、Standard および Datacenter エディション、および Server Core オプション
  - Windows Server 2016、Standard および Datacenter エディション、および Server Core オプション
- Citrix では、他の Citrix コンポーネントを含まないサーバーに FAS をインストールすることをお勧めします。
- Windows Server はセキュリティで保護されている必要があります。ドメインユーザーに証明書を自動的に発行できる登録機関証明書と秘密キーにアクセスでき、それらのユーザー証明書と秘密キーにもアクセスできます。
- FAS の 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 Certification Authority (ルートまたは下位) が必要です。

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

- Delivery Controller、Virtual Delivery Agent (VDA)、および StoreFront™ サーバーはすべて、サポートされているバージョンである必要があります。
- マシンカタログを作成する前に、Federated Authentication Service のグループポリシー構成が VDA に正しく適用されている必要があります。詳細については、「グループポリシーの構成」セクションを参照してください。

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

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

インストールと構成

インストールとセットアップの順序

1. フェデレーション認証サービス (FAS) をインストールする
2. StoreFrontストアでFASプラグインを有効にする(/ja-jp/federated-authentication-service/2305/install-configure.html#enable-the-fas-plug-in-on-storefront-stores)
3. Delivery Controllerを構成する(/ja-jp/federated-authentication-service/2305/install-configure.html#configure-the-delivery-controller)
4. グループポリシーを構成する(/ja-jp/federated-authentication-service/2305/install-configure.html#configure-group-policy)
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(/ja-jp/federated-authentication-service/2305/install-configure.html#deploy-certificate-templates)
    b. 証明機関をセットアップする(/ja-jp/federated-authentication-service/2305/install-configure.html#set-up-active-directory-certificate-services)
    c. FASが証明機関を使用することを承認する(/ja-jp/federated-authentication-service/2305/install-configure.html#authorize-federated-authentication-service)
    d. ルールを構成する(/ja-jp/federated-authentication-service/2305/install-configure.html#configure-rules)
    e. FASをCitrix Cloudに接続する(/ja-jp/federated-authentication-service/2305/install-configure.html#connect-to-citrix-cloud) (オプション)

フェデレーション認証サービスをインストールする

セキュリティのため、Citrixではフェデレーション認証サービス (FAS) を専用サーバーにインストールすることをお勧めします。このサーバーは、ドメインコントローラーまたは証明機関と同様の方法で保護する必要があります。FASは次のいずれかの方法でインストールできます。

- Citrix Virtual Apps and Desktops™インストーラー (ISO挿入時の自動実行スプラッシュ画面にある**Federated Authentication Service**ボタンから)、または

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

- 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）。

これらは以下のコンポーネントをインストールします。

- フェデレーション認証サービス
- 高度なFAS構成のためのPowerShellスナップインコマンドレット
- FAS管理コンソール
- FASグループポリシーテンプレート (CitrixFederatedAuthenticationService.admx/adml)
- 証明書テンプレートファイル
- パフォーマンスカウンターとイベントログ

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。Federation Authentication Serviceが有効なStoreFront™サーバーからサーバーに到達できない場合、ユーザーはログオンしたりアプリケーションを起動したりできません。

アップグレードを開始するには、Citrix Virtual Apps and Desktopsインストーラーまたはスタンドアロンの 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は、この手順は必要ありません。

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` を変更してください。

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

$StoreVirtualPath = "/Citrix/Store"
```

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

```
$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は、この手順は必要ありません。

FASを使用するには、Citrix Virtual AppsまたはCitrix Virtual Desktops™ Delivery Controllerが接続する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。

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

グループポリシーを構成する

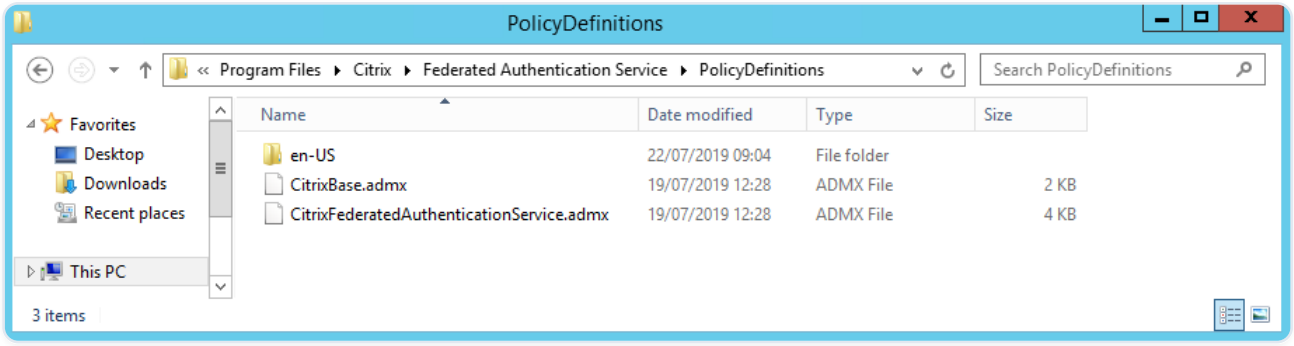
FASをインストールした後、インストールで提供されるグループポリシーテンプレートを使用して、グループポリシー内のサーバーの完全修飾ドメイン名 (FQDN) を指定します。

重要：

チケットを要求するStoreFrontサーバーと、チケットを引き換えるVirtual Delivery Agent (VDA) が、グループポリシーオブジェクトによって適用される自動サーバー番号付けを含め、FQDNの同一構成になってい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で単一のポリシーを構成します。ただし、これは必須ではありません。FASは、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。

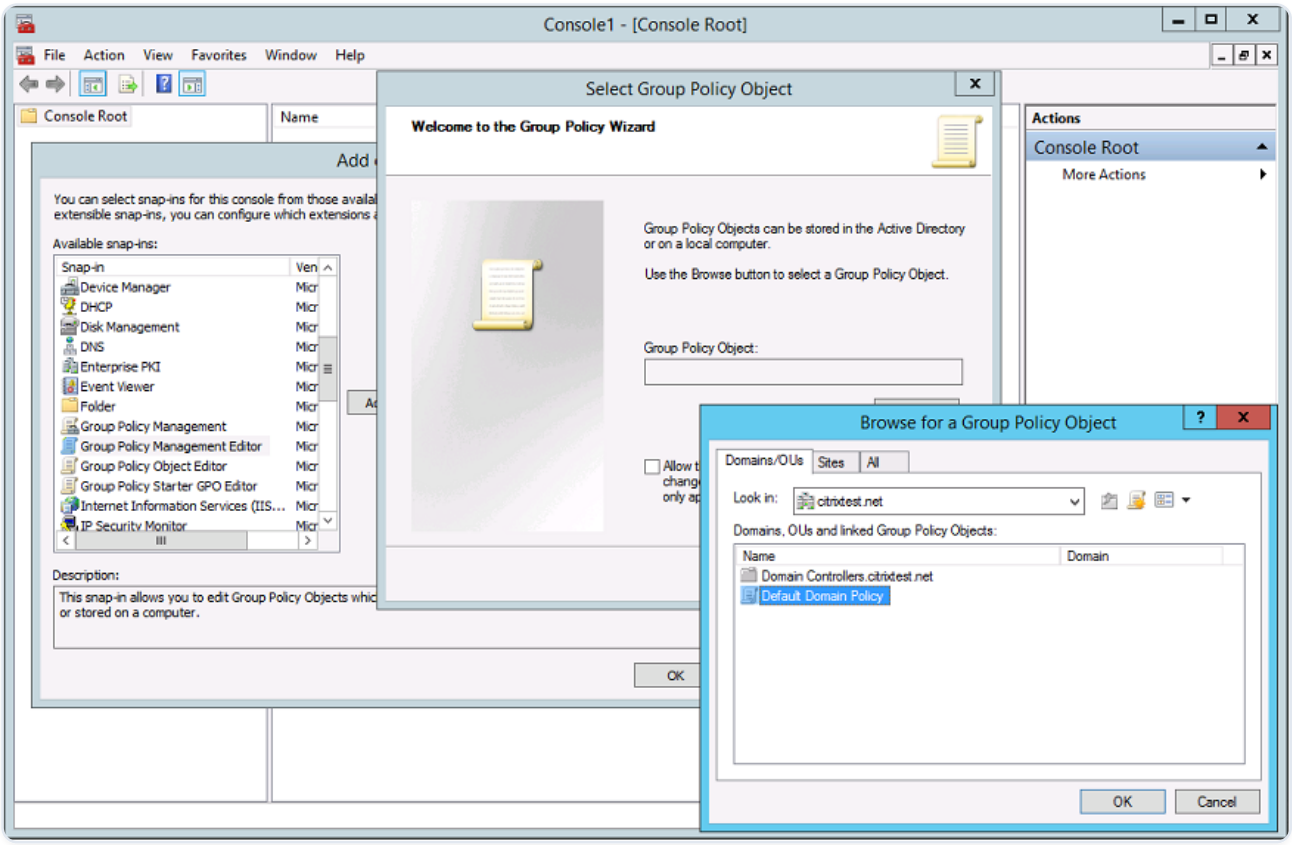


手順 2. これらのファイルをドメインコントローラーにコピーし、C:\Windows\PolicyDefinitionsおよびen-USサブフォルダーに配置します。

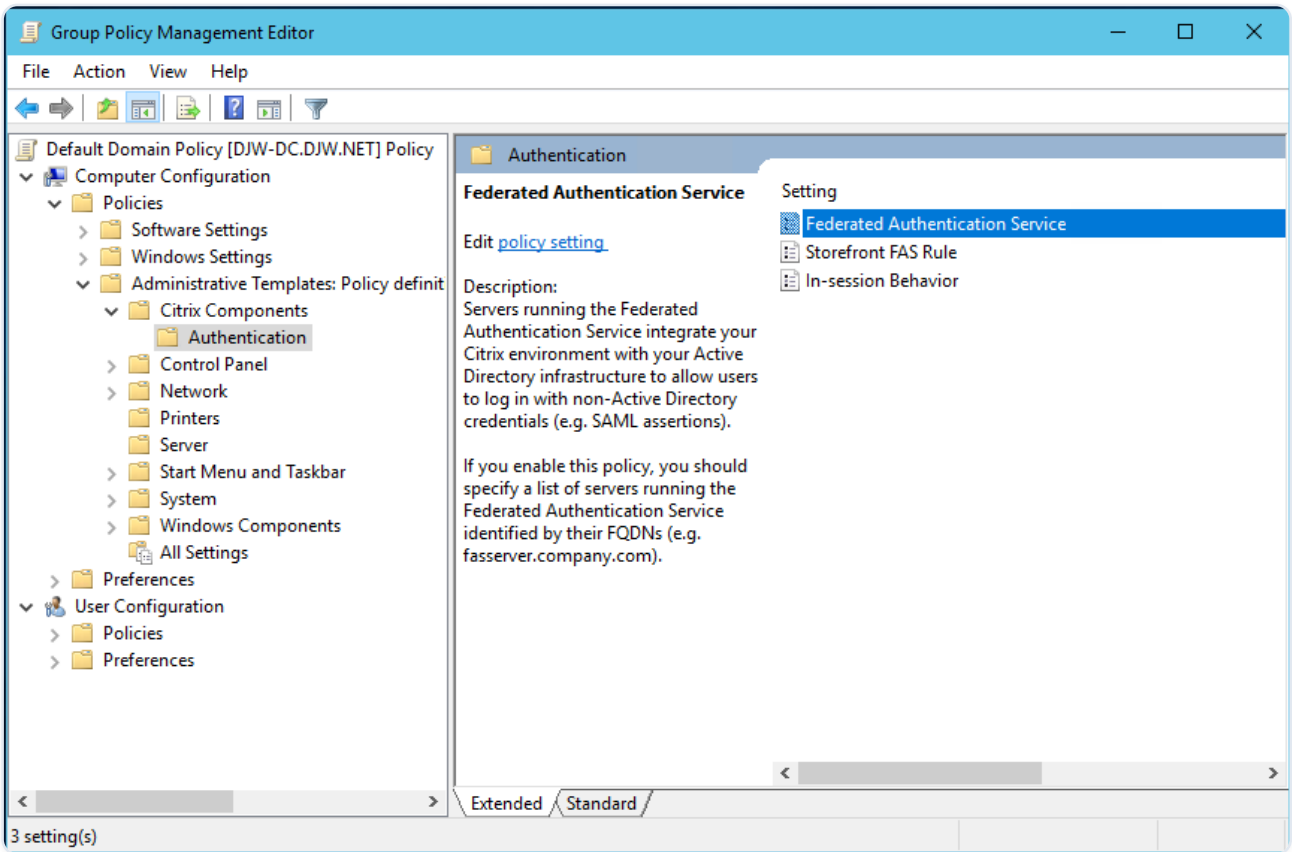
手順 3. Microsoft Management Console（コマンドラインからmmc.exe）を実行します。メニューバーから、**ファイル > スナップインの追加と削除**を選択します。**グループポリシー管理エディター**を追加します。

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および選択することもできます。このポリシーは、影響を受けるCitrixソフトウェア（VDAs、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。

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



手順 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。

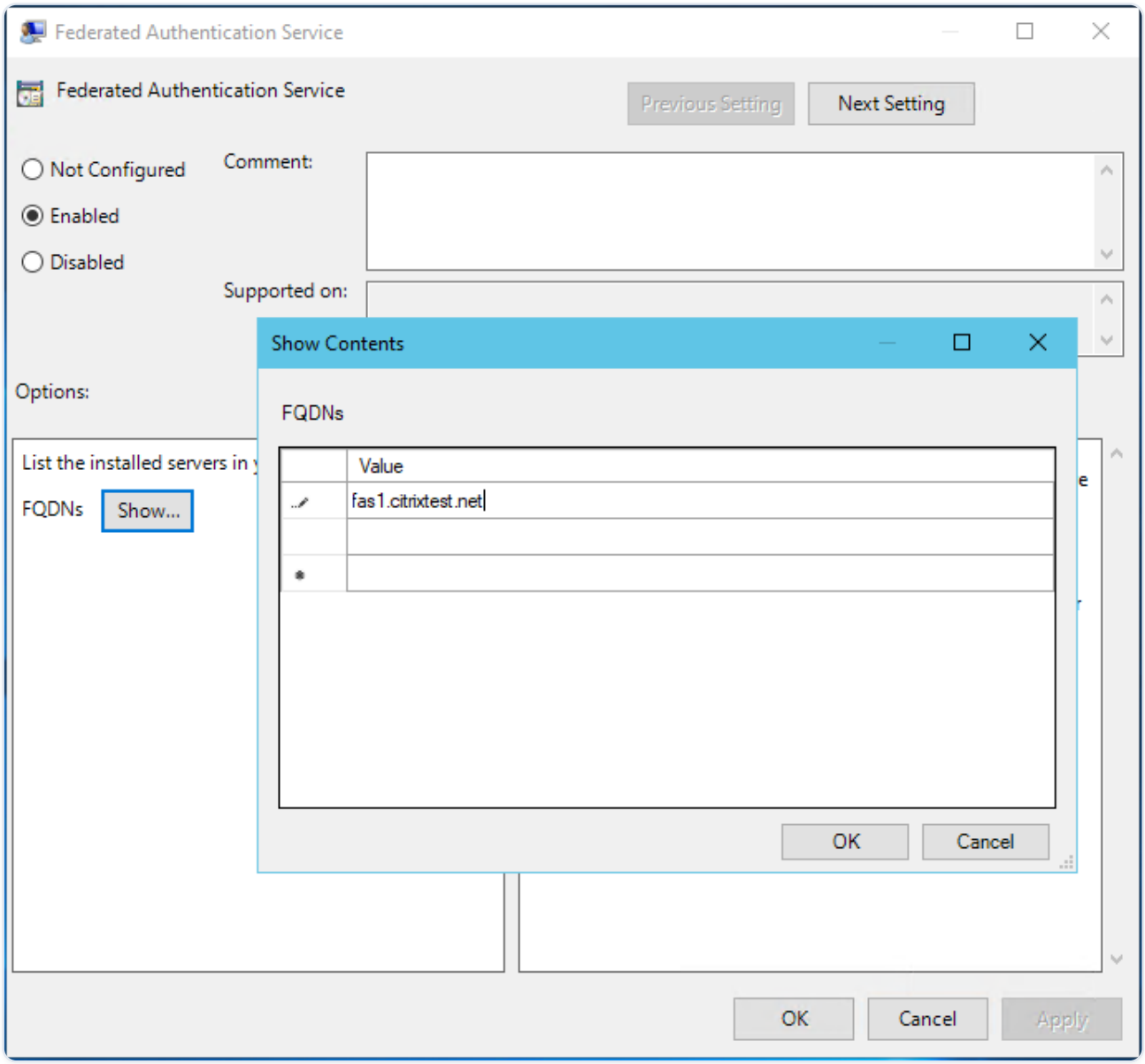


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。手順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。

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



手順 6. FASサーバーのFQDNを入力します。

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

重要：

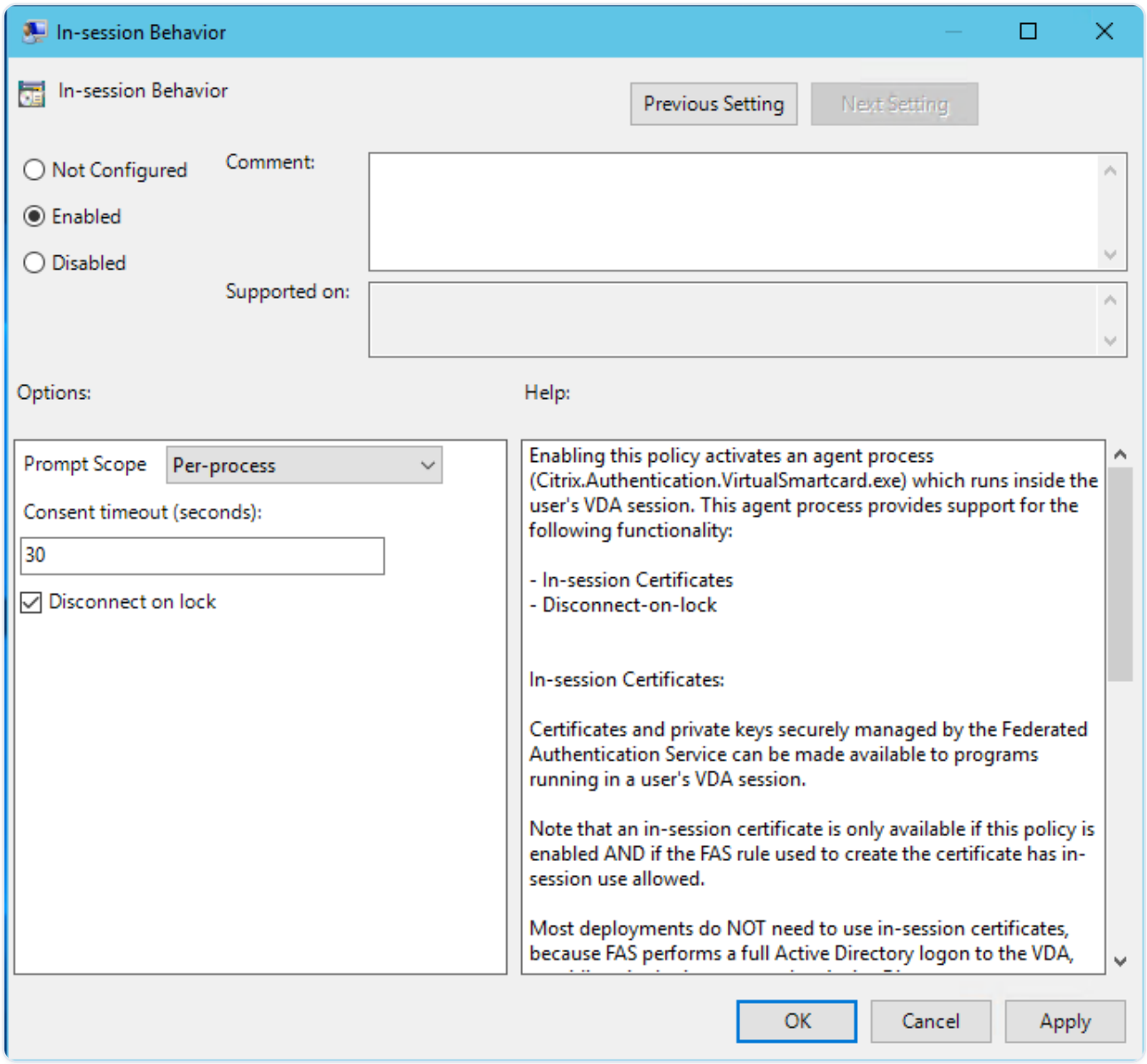
複数のFQDNを入力する場合、リストの順序は、VDAs、StoreFrontサーバー（存在する場合）、およびFASサーバーから見て一貫している必要があります。(/ja-jp/federated-authentication-service/2305/config-manage/security.html#group-policy-settings)を参照してください。

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

セッション内の動作

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

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



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

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

プロンプトの範囲

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

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

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

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

同意のタイムアウト

このポリシーが有効になっている場合、**同意のタイムアウト**は、同意が持続する期間（秒単位）を制御します。たとえば、300秒に設定すると、ユーザーは5分ごとにプロンプトが表示されます。値がゼロの場合、秘密鍵の操作ごとにユーザーにプロンプトが表示されます。

ロック時の切断

このポリシーが有効になっている場合、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。

フェデレーション認証サービス管理コンソールの使用

注：

FAS管理コンソールはほとんどの展開に適していますが、PowerShellインターフェイスはより高度なオプションを提供します。FAS PowerShellコマンドレットの詳細については、「PowerShellコマンドレット」を参照してください。

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

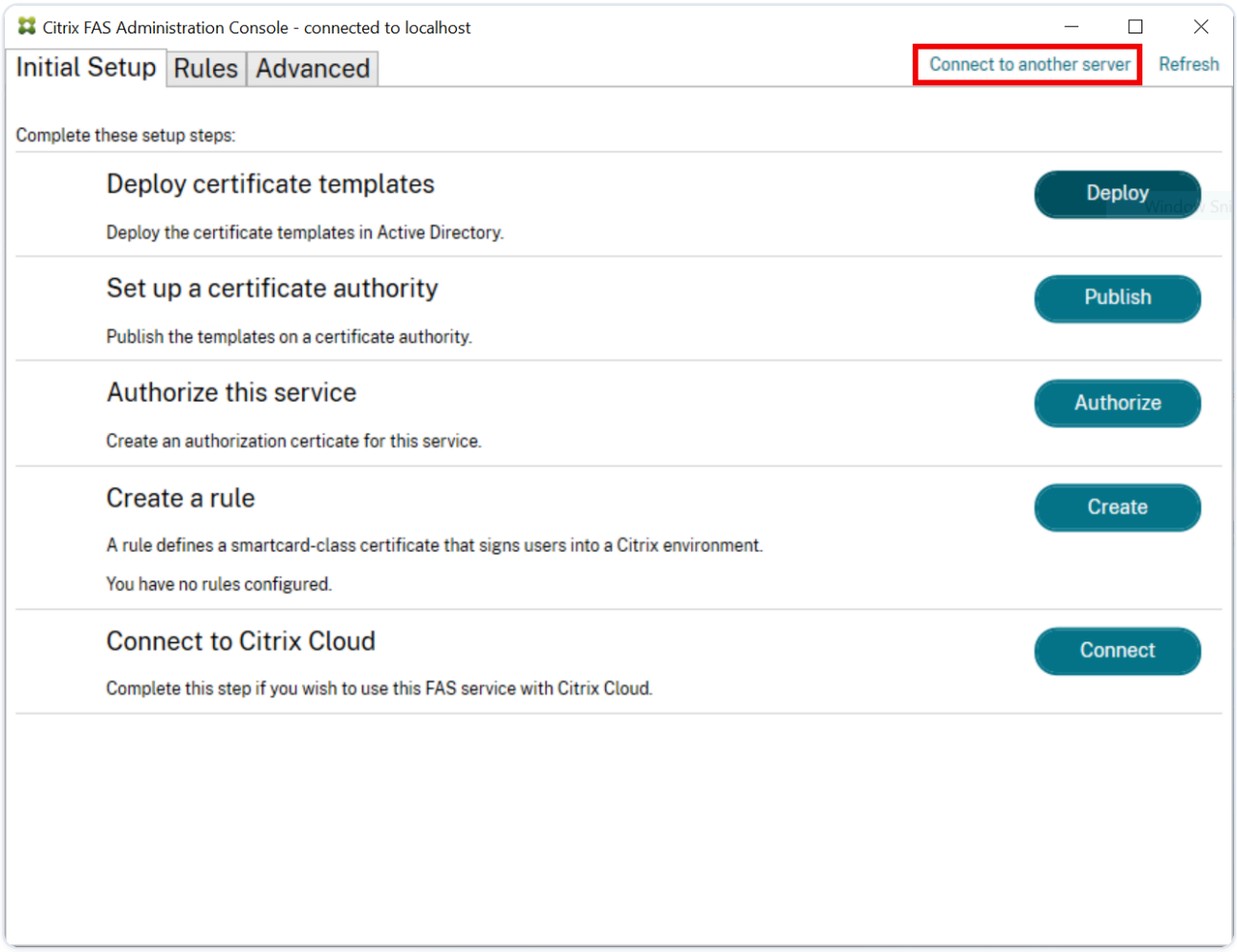
管理コンソールを初めて使用するときは、次のプロセスを実行するようにガイドされます。

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

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。

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

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



証明書テンプレートを展開する

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

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/deploy-cert-templates.png)

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

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

C:\プログラムファイル\Citrix\フェデレーション認証サービス\証明書テンプレート

証明書テンプレートフォルダー。(/en-us/federated-authentication-service/2305/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.certificatetemp
late")

$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する必要があります。Active Directory証明書サービスの展開方法については、Microsoftのドキュメントを参照してください。

証明機関を管理する権限を持つユーザーは、少なくとも1つのサーバーにテンプレートを公開する必要があります。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。)

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/setup-cert-authority.png)

フェデレーション認証サービスを承認する

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/authorize-service.png)

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

管理者が**発行**または**拒否**を選択するまで、FAS 管理コンソールには処理中の「スピナー」が表示されます。

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/pending-request.png)

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。

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/waiting-approval.png)

ルールを構成する

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

各ルールは以下を指定します。

- 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。

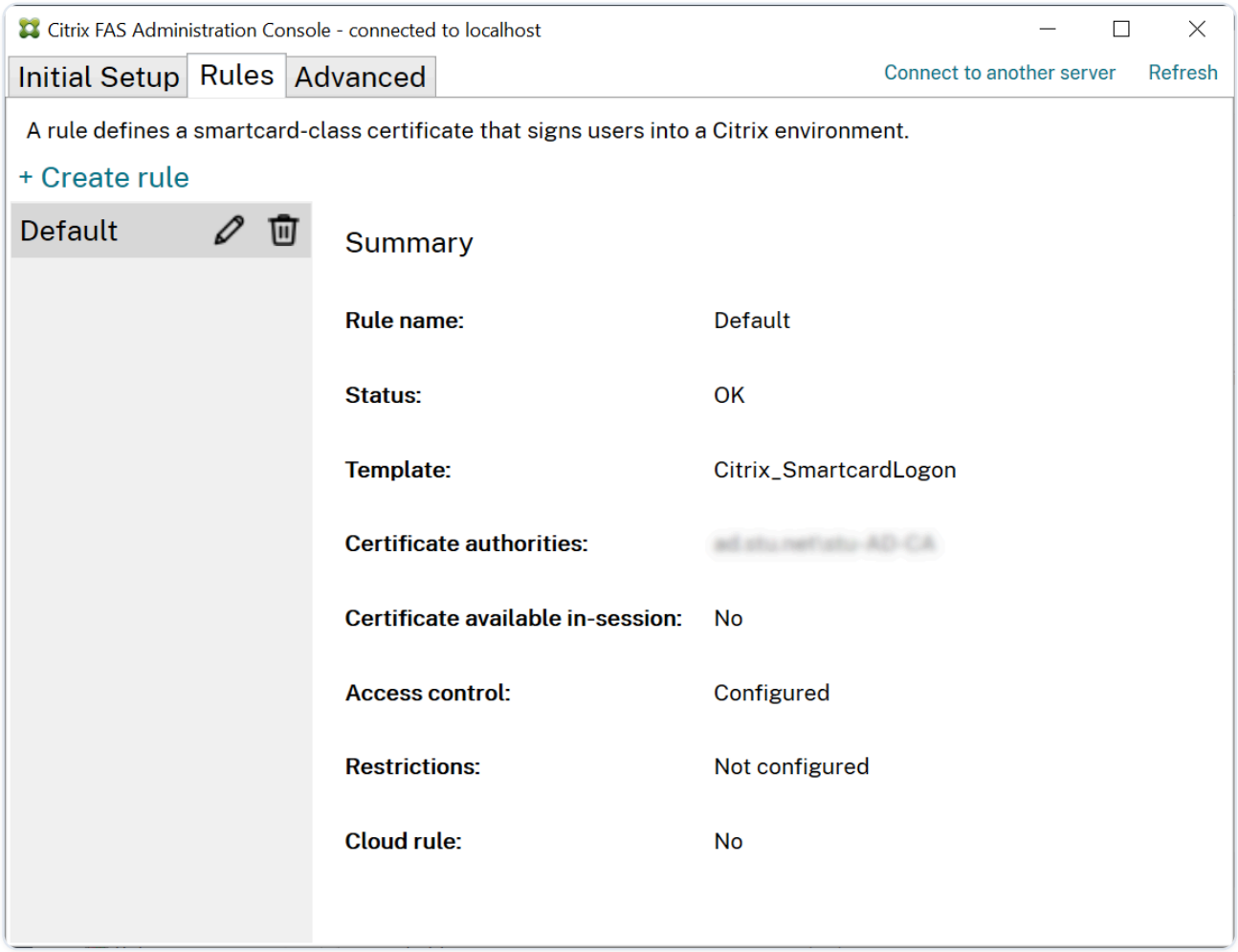
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 証明書の使用が許可されている VDA マシンセット。

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

さらにカスタムルールを作成して、異なる証明書テンプレートと証明機関を参照し、異なるプロパティと権限を持つように構成できます。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。グループポリシー構成オプションを使用して、StoreFront サーバーがカスタムルールを名前で要求するように構成します。

「**作成**」をクリックするか、「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、ルールの作成に必要な情報を収集します。「ルール」タブには、各ルールの概要が表示されます。



ウィザードは以下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）。

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

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。

アクセスコントロール: ユーザーのログオンまたは再接続のために証明書を要求することを許可されている、信頼されたStoreFrontサーバーマシンのリストです。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:

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

注:
FASサーバーをCitrix Cloudでのみ使用している場合、アクセスコントロールを設定する必要はありません。ルールがCitrix Cloudによって使用される場合、StoreFrontのアクセス許可は無視されます。同じルールをCitrix CloudとオンプレミスのStoreFront展開の両方で使用できます。ルールがオンプレミスのStoreFrontによって使用される場合、StoreFrontのアクセス許可は引き続き適用されます。
デフォルトの権限（「Assert Identity」が許可されている）はすべてを拒否します。したがって、StoreFrontサーバーを明示的に許可する必要があります。

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/storefront-servers.png)

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

制限: FASを使用してユーザーをログオンできるVDAマシンの一覧と、FASを介して証明書を発行できるユーザーの一覧。

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

注:

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/vdas.png)

ローカライズされた画像(/en-us/federated-authentication-service/2305/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。**Citrix Cloudへの接続**セクションのリンクから、Citrix Cloudに接続した後で規則を変更することもできます。

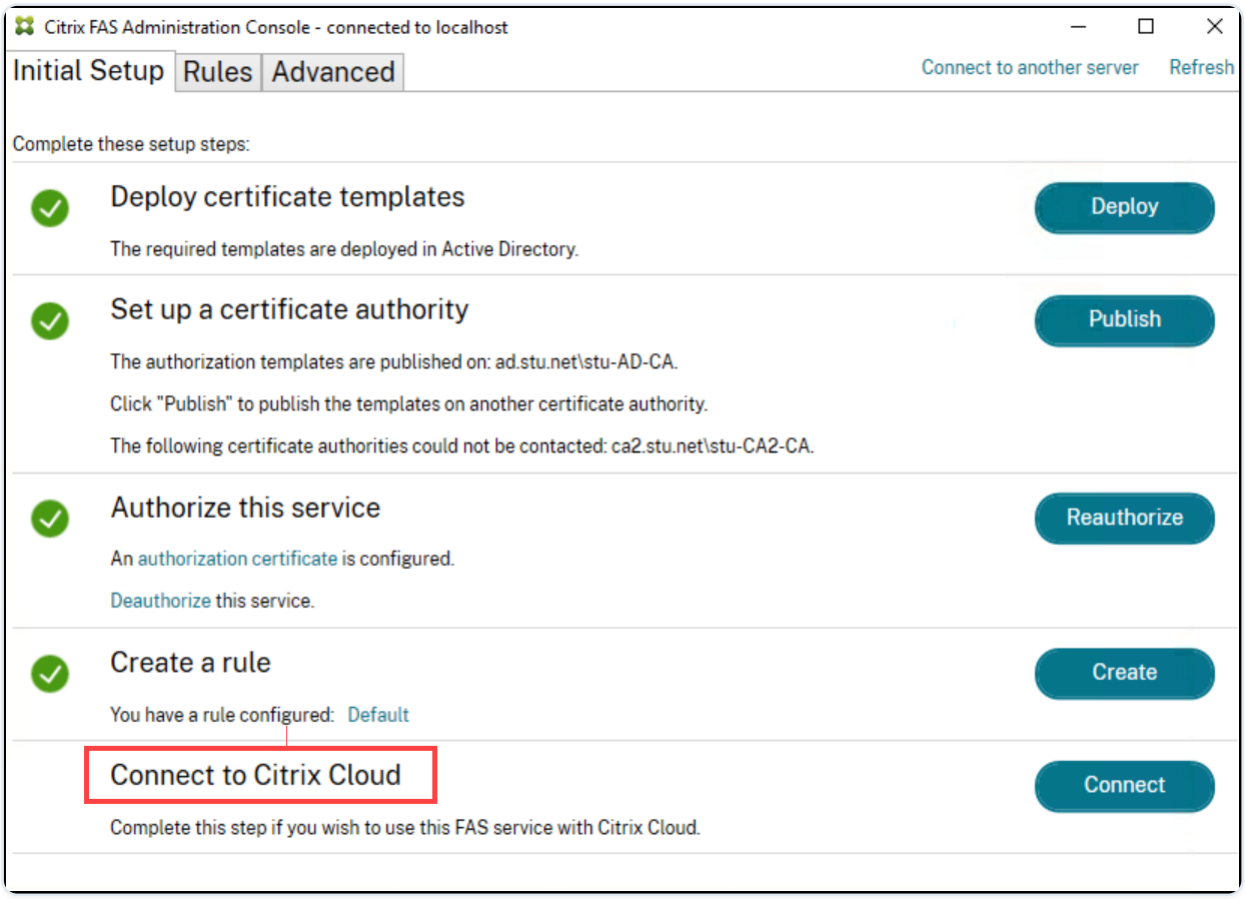
ローカライズされた画像(/en-us/federated-authentication-service/2305/media/rule-created.png)

Citrix Cloudへの接続

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

1. 初期設定タブの**Citrix Cloudへの接続**で、**接続**をクリックします。

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



2. 接続するクラウドを選択し、**次へ**をクリックします。

   「Citrix Cloudの選択」(/en-us/federated-authentication-service/2305/media/connect-cloud-choose-citrix-cloud.png)

   「

   注

   」

   プレビューでは、**Citrix Cloud**のみが利用可能です。

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

   「確認」(/en-us/federated-authentication-service/2305/media/connect-cloud-confirmation.png)

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。

   「リソースの場所」(/en-us/federated-authentication-service/2305/media/connect-cloud-resource-location.png)

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

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。

   「ルールの選択」(/en-us/federated-authentication-service/2305/media/connect-cloud-choose-rule.png)
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。

   「Cloud接続の概要」(/en-us/federated-authentication-service/2305/media/connect-cloud-summary.png)

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

注

> オンプレミスのFASサーバーは、Citrix Cloudおよび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、**Connect to Citrix Cloud** で **Disable** を選択します。

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

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ています。

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の関係を設定していること。詳細については、「Citrix Service Provider 向け Citrix DaaS」を参照してください。

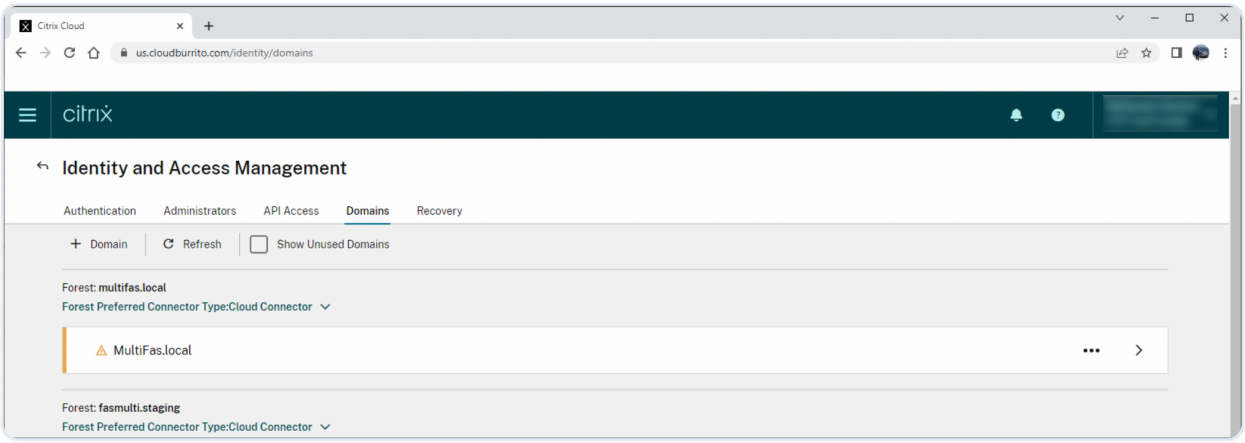
MSP顧客を構成する

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。

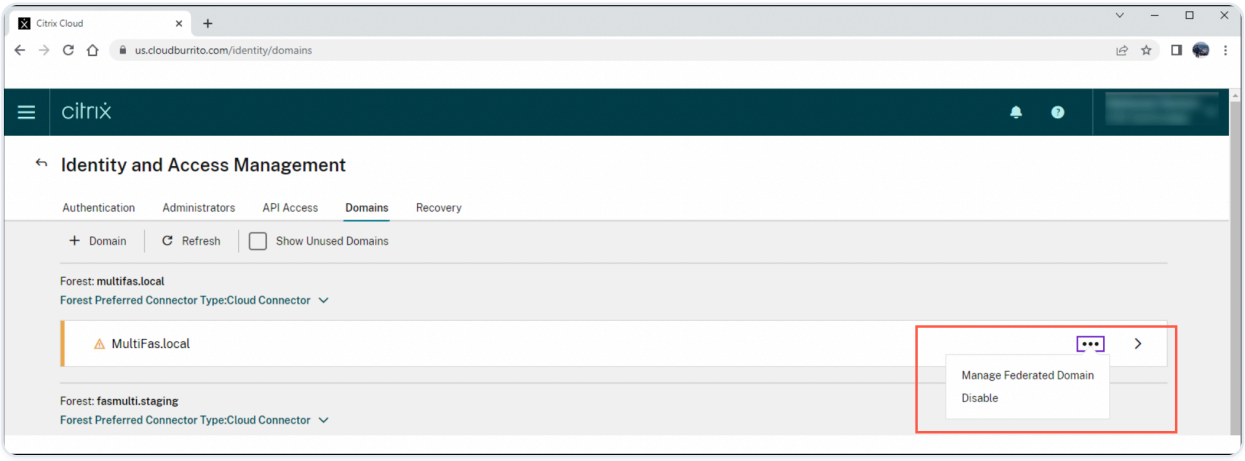
   オンプレミスドメインコントローラーに関連付けられているドメインが、 > の下に表示されていることを確認します。

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



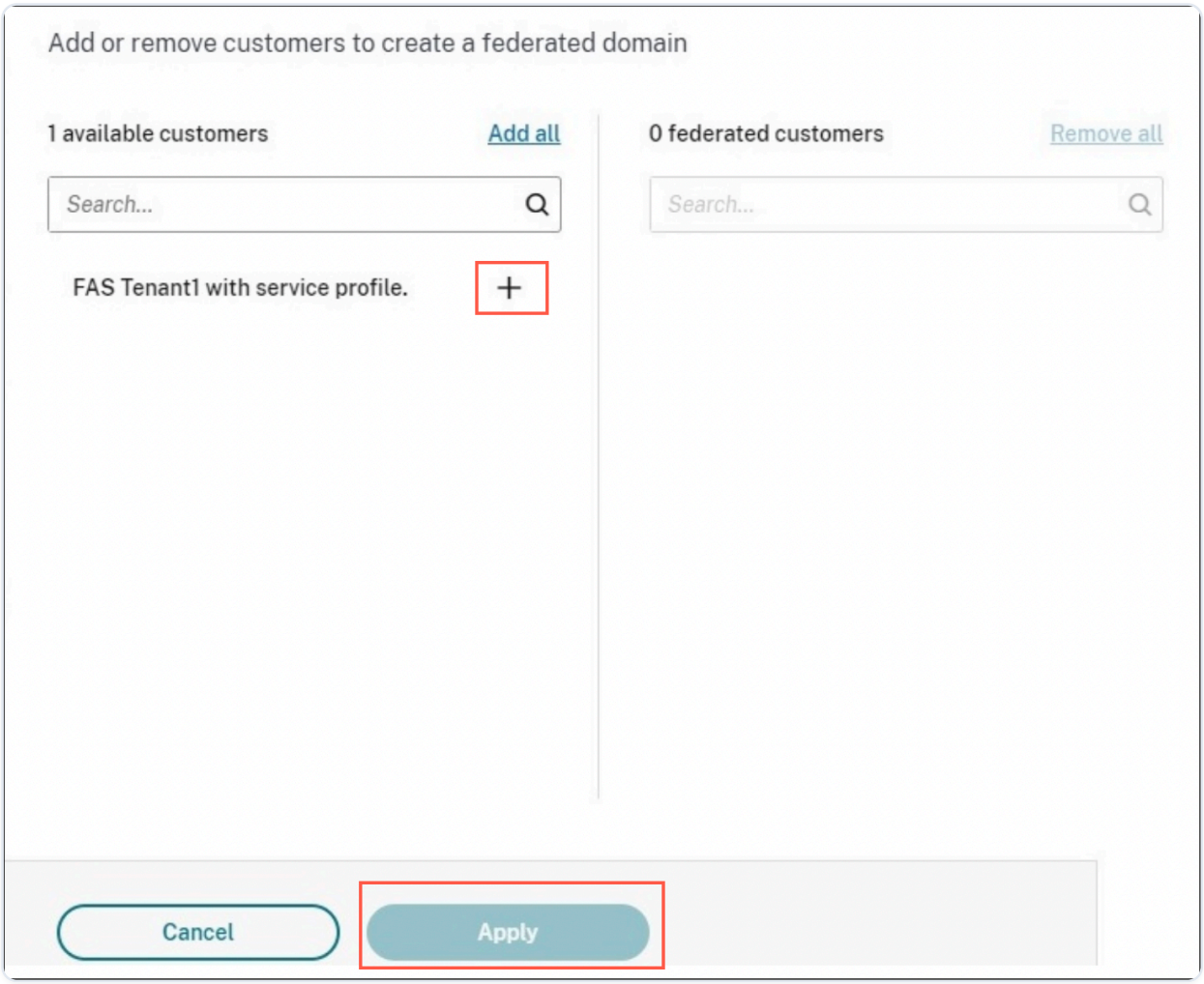
2. ドメインをテナントにフェデレーションします。

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



   テナントを見つけて + をクリックします。次に、 をクリックします。

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



3. 関連付けられた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。

   関連付けられた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/2305/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たクラウドのリソースロケーションに接続します。FASサーバーのインストールについては、「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

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

- 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/2305/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。

Azure Active Directory (AAD) は、AD と AAD の間で同期を行い、ユーザーとコンピューターの両方にハイブリッド ID を作成して実装されるのが一般的です。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。

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

AAD SSO の手法を次の表にまとめます。

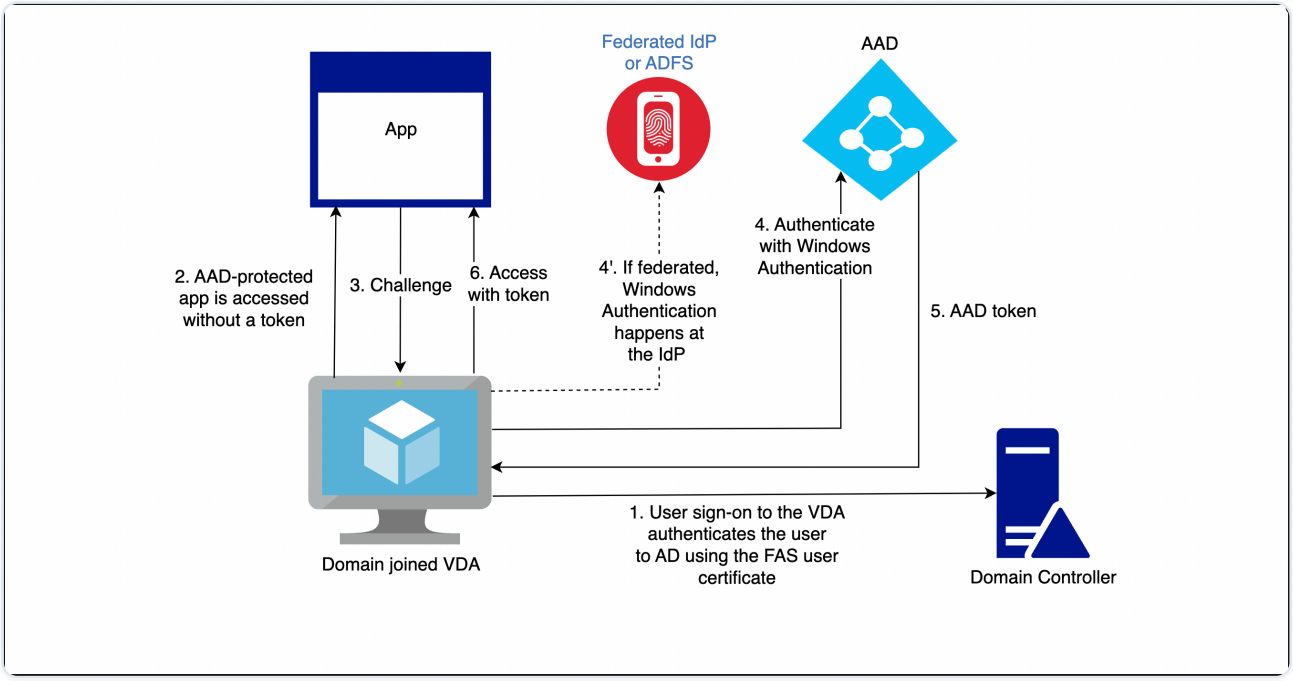
AAD 認証タイプ	VDA はドメイン参加済み	VDA はハイブリッド参加済み
マネージド	AAD シームレス SSO を使用	AAD 証明書ベース認証を使用
Active Directory Federation Services (ADFS) にフェデレーション済み	ADFS で Windows 認証を有効にする	WS-Trust の *certificatemixed* エンドポイントが有効になっていることを確認する
サードパーティの ID プロバイダーにフェデレーション済み	サードパーティのソリューションを使用する	サードパーティのソリューションを使用する

- 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 と呼ばれていました）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。

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



詳細については、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 ドメインのセットアップについては、シームレスシングルサインオンを参照してください。

ADFS にフェデレーションされている 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。詳細については、IDプロバイダーにお問い合わせください。

注：

ハイブリッド参加済みVDA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を使用することもできます。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チケット許可チケット（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）

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

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。

ハイブリッド参加済みVDAの図(/en-us/federated-authentication-service/2305/media/hybrid-joined-vdas.png)

詳細については、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証明書ベース認証の概要」を参照してください。VDAはAAD CBA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。

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ている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の*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。

証明機関の構成

この記事では、Federated Authentication Service (FAS) と証明機関 (CA) サーバーを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。この記事の指示を実行する前に、PowerShellの基本的な知識が必要です。

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

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/2305/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に対して証明機関をセットアップするの手順を実行してください。

> **注:**
>
> このステップで構成された承認証明書は、どのCAでも使用できるため、すべてのCAに対してこのサービスを承認するステップを実行する必要はありません。

予期される動作の変更

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

TCPアクセス用にMicrosoft証明機関を構成する

デフォルトでは、Microsoft CAはアクセスにDCOMを使用します。これはファイアウォールセキュリティを実装する際に複雑さをもたらす可能性があるため、Microsoftは静的TCPポートに切り替えるための規定を設けています。Microsoft CAで、**スタート>ファイル名を指定して実行>dcomcnfg.exe**を使用してDCOM構成パネルを開き、*コンピューター>マイコンピューター>DCOM構成*を展開して**CertSrv Request**ノードを表示し、CertSrv Request DCOMアプリケーションのプロパティを編集します。

ローカライズされた画像(/en-us/federated-authentication-service/2305/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。

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

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-caconfig-netstat.png)

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

ユーザー証明書の事前生成

FASサーバー内でユーザー証明書を事前生成すると、ユーザーのログオン時間が大幅に改善されます。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

ADをクエリし、ユーザーのリストをファイル（例：.csvファイル）に保存することで、証明書生成を改善できます。以下の例を参照してください。

```
Import-Module ActiveDirectory



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

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



if ($searchbase -ne ""){

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

} else {

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

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

```
}
```

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

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

CSVは次のようになります。

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-caconfig-get-aduser-csv.png)

FASサーバー

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

```
Add-PSSnapin Citrix.A*

$csv = "user_list.csv"

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

$users = Import-Csv -encoding utf8 $csv

foreach ( $user in $users )

{

    $server = Get-FasServerForUser -UserPrincipalNames
$user.UserPrincipalName

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

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

    }
```

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

```
    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（例：「hello」）を使用する場合は、スクリプト内の$rule変数を変更してください。



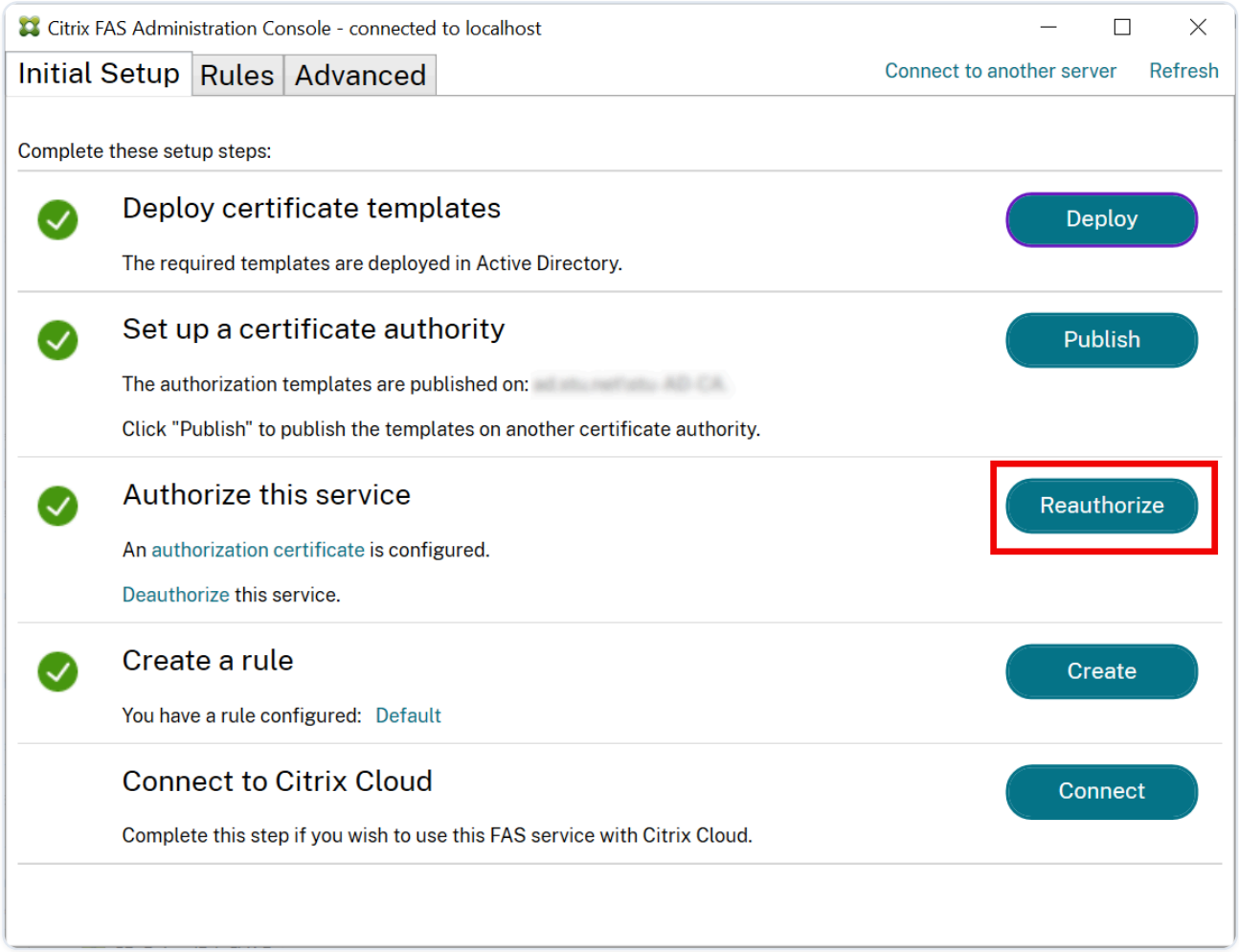
登録機関証明書を更新する

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。

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



次の手順を完了します。

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

関連情報

- インストールと構成の記事は、FASのインストールと構成に関する主要な参照資料です。

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

- 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記事にまとめられています。
- その他の「ハウツー」記事は、高度な構成記事で紹介されています。

秘密鍵の保護

はじめに

証明書はFASサーバー上の組み込みデータベースに保存されます。関連する秘密鍵は、FASサーバーのネットワークサービスアカウントによって保存され、デフォルトでエクスポート不可としてマークされます。

秘密鍵には2種類あります。

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

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

Federated Authentication Service (FAS) 管理コンソールの **Initial Setup** タブのステップ3で、**Authorize** をクリックすると、FASサーバーはキーペアを生成し、Citrix_RegistrationAuthority_ManualAuthorization証明書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、デフォルトで24時間有効です。証明機関はこの証明書を自動的に発行しません。その発行は、証明機関で管理者によって手動で承認される必要があります。証明書がFASサーバーに発行されると、FASはCitrix_RegistrationAuthority_ManualAuthorization証明書を使用して、Citrix_RegistrationAuthority証明書（デフォルトで2年間有効）を自動的に取得します。FASサーバーは、Citrix_RegistrationAuthority証明書を取得するとすぐに、Citrix_RegistrationAuthority_ManualAuthorizationの証明書とキーを削除します。

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

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

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

- 登録機関証明書とユーザー証明書の秘密鍵の両方に、Microsoft Enhanced RSA and AES Cryptographic ProviderまたはMicrosoft Software Key Storage Providerを使用する。
- 登録機関証明書の秘密鍵にはTrusted Platform Module (TPM) チップを備えたMicrosoft Platform Key Storage Providerを使用し、ユーザー証明書の秘密鍵にはMicrosoft Enhanced RSA and AES Cryptographic ProviderまたはMicrosoft Software Key Storage Providerを使用する。
- 登録機関証明書とユーザー証明書の秘密鍵の両方に、HSMデバイスを備えたHardware Security Module (HSM) ベンダーのCryptographic ServiceまたはKey Storage Providerを使用する。

秘密鍵の構成設定

FASを3つのオプションのいずれかを使用するように構成します。テキストエディターを使用してCitrix.Authentication.FederatedAuthenticationService.exe.configファイルを編集します。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.Supress" 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>
```

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)

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

値	コメント
真	CAPI API を使用
false (デフォルト)	CNG API を使用

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

値	コメント
マイクロソフト拡張RSAおよびAES暗号化プロバイダー	デフォルトの CAPI プロバイダー
Microsoft ソフトウェア キー ストレージ プロバイダー	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の場合にのみ必須)

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。

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

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

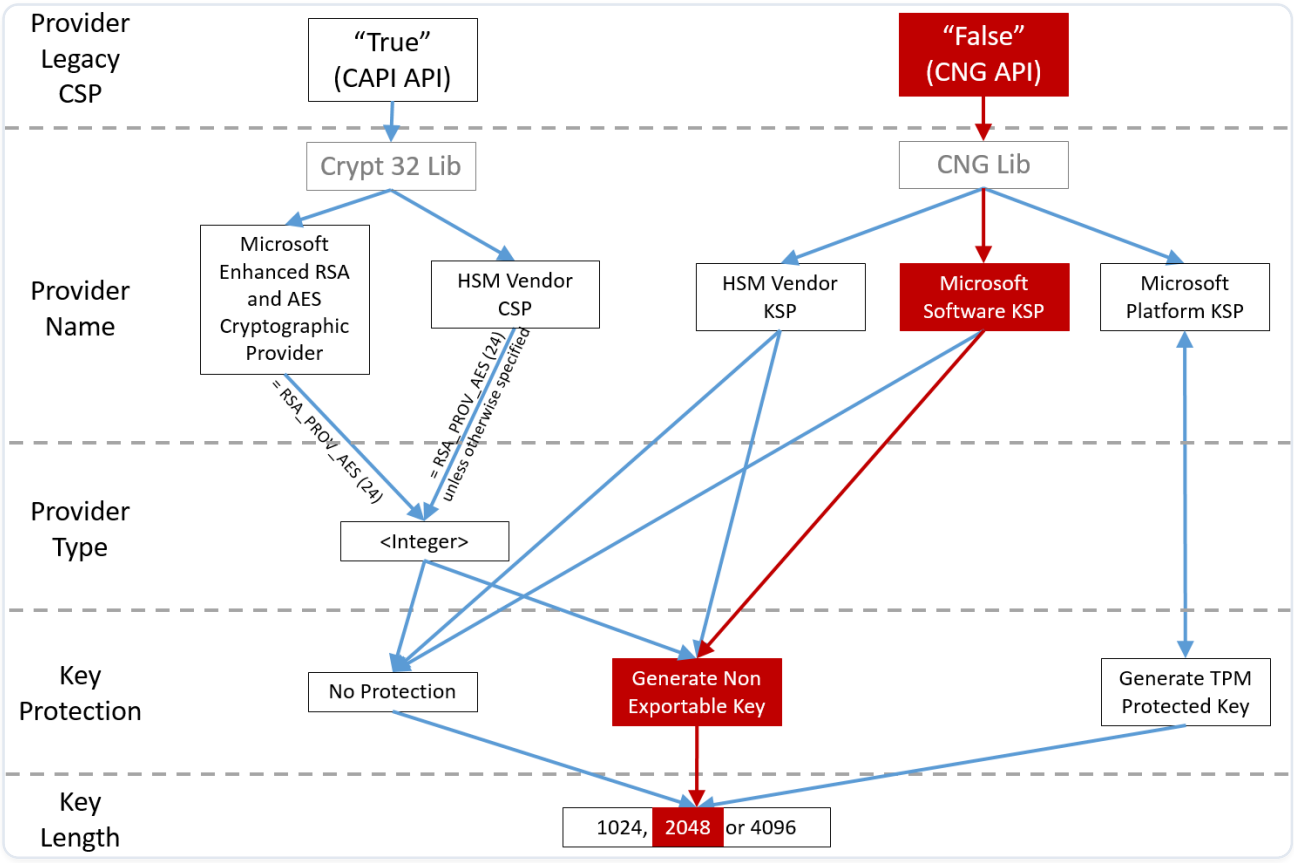
値	コメント
保護なし	秘密キーはエクスポート可能です。
GenerateNonExportableKey	デフォルト。秘密キーはエクスポートできません。
GenerateTPMProtectedKey	秘密キーはTPMを使用して管理されます。秘密キーは、ProviderNameで指定したProviderName（例：Microsoft Platform Key Storage Provider）を介して保存されます。

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）。

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



構成シナリオの例

例1

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

これはデフォルトのインストール後構成です。追加の秘密鍵構成は不要です。

例 2

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

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

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

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: 構成ファイルを編集し、以下の行を次のように変更します。

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

ファイルは次のようになります。

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

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

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

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

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

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

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" 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はTPMで生成されています。証明書はデフォルトで2年間有効です。

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

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

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

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

手順5： 設定ファイルを以下のように編集し直します。

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

注：

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

手順6： FASを再起動します。これにより、サービスは設定ファイルを再読み込みし、変更された値を反映します。その後の自動秘密キー操作は、ユーザー証明書キーに影響します。これらの操作は秘密キーをTPMに保存せず、Microsoftソフトウェアキー記憶プロバイダーを使用します。

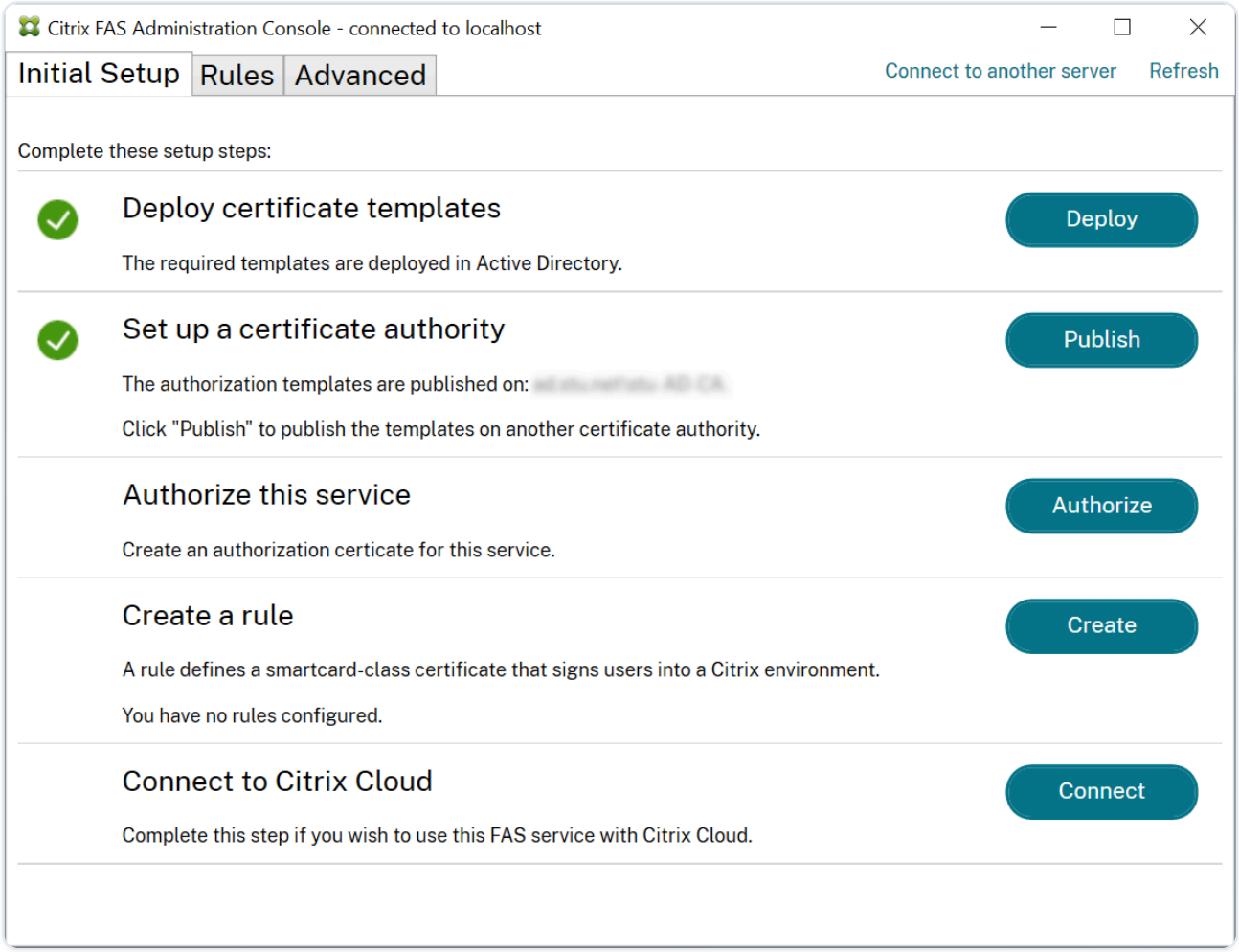
手順7： FAS管理コンソールで**ルール**タブを選択し、インストールと構成で説明されているように設定を編集します。

PowerShellの使用

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

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に、最初の2つの手順（「証明書テンプレートの展開」と「証明機関のセットアップ」）のみを完了します。

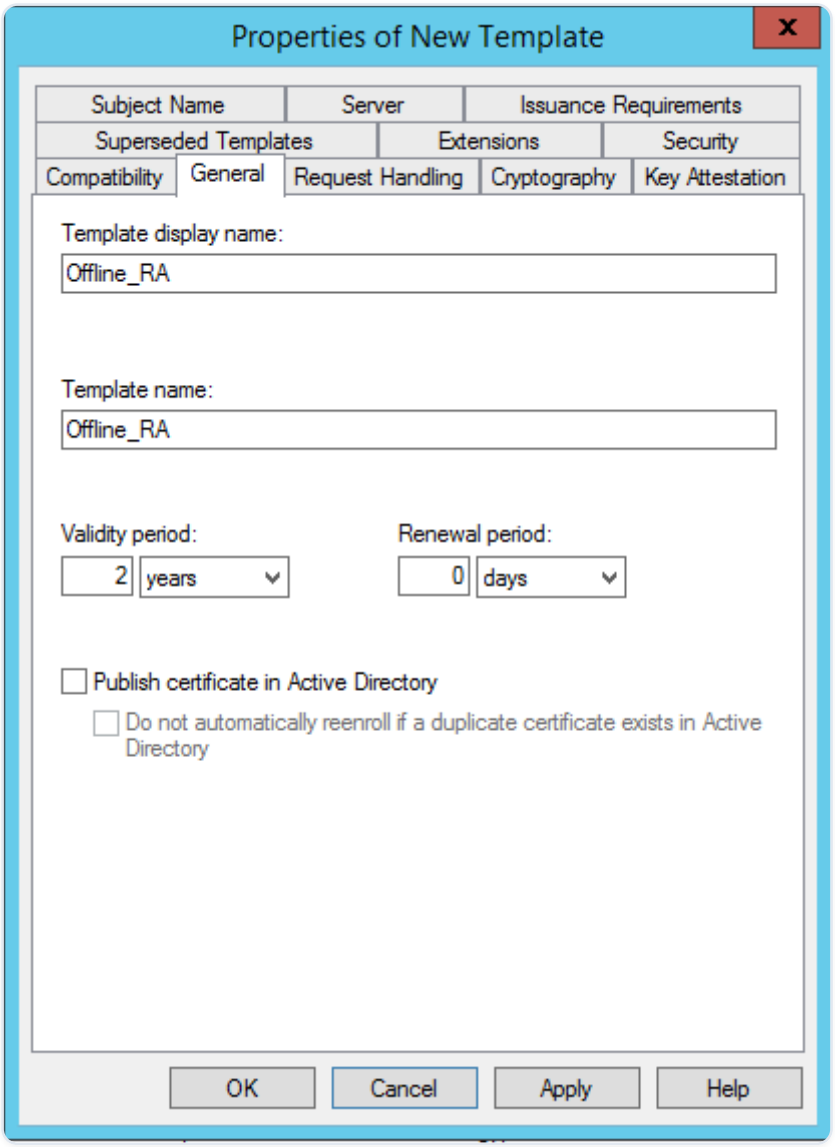
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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。

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



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。作成したばかりのテンプレートを選択します。

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

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

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

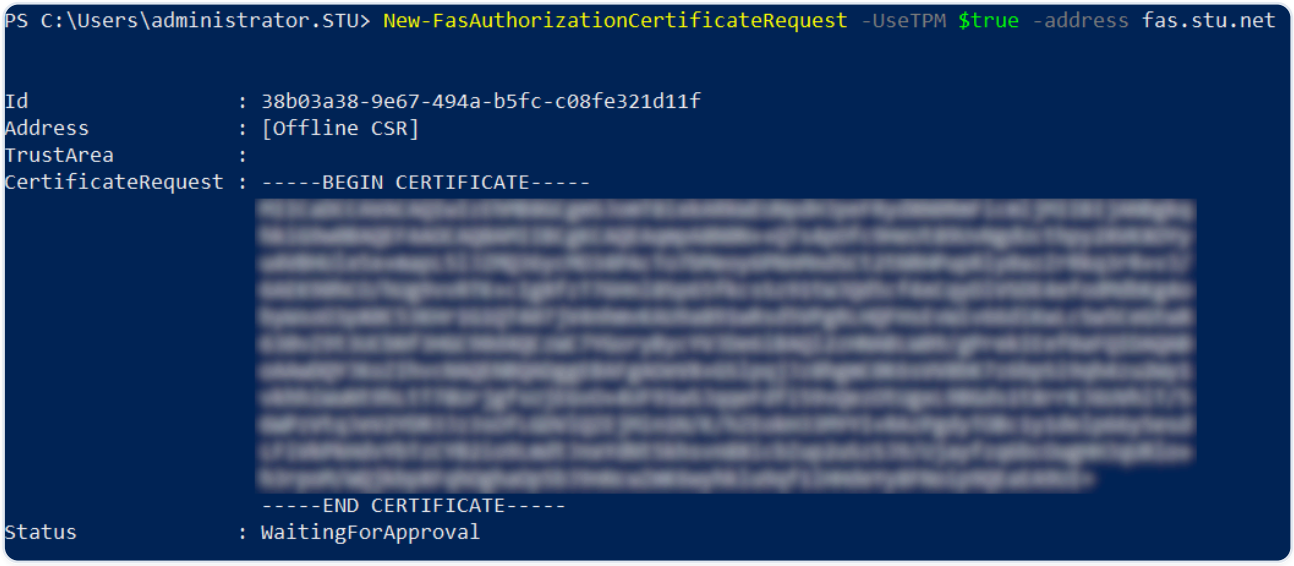
```
New-FasAuthorizationCertificateRequest -UseTPM $true -address \<FQDN of FAS Server>
```

例:

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

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

次のように表示されます。

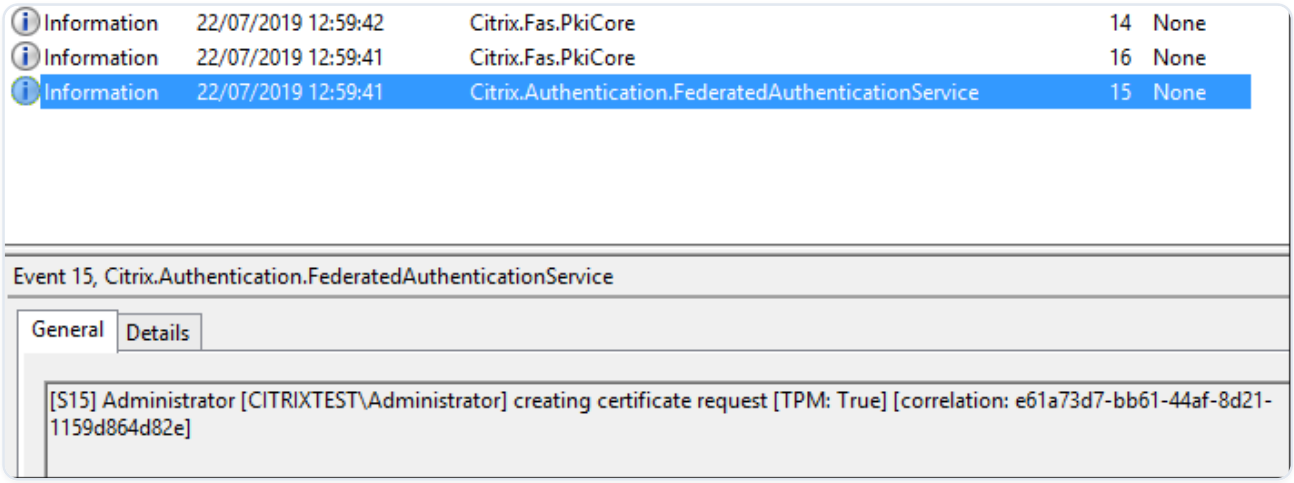


注:

- 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」と考えてください。
- このコマンドレットを実行すると、FASの起動時に構成ファイルから読み取られた値がチェックされ、使用するキー長が決定されます（デフォルトは2048）。
- この手動のPowerShell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。
- 後続の自動FASによって開始されたユーザー証明書の秘密キー操作では、FASの起動時にファイルから読み取られた値が使用されます。
- FASサーバーがユーザー証明書を発行して、TPMによって保護されたユーザー証明書秘密キーを生成する場合、構成ファイルでKeyProtection値をGenerateTPMProtectedKeyに設定することも可能です。

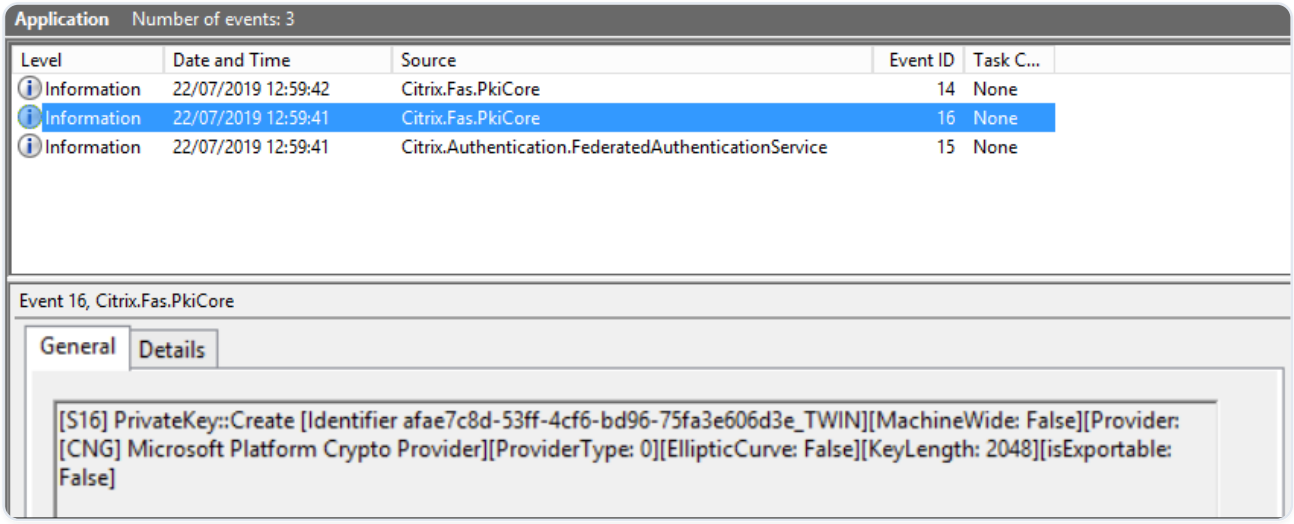
キーペアの生成にTPMが使用されたことを確認するには、キーペアが生成されたときに、FASサーバーのWindowsイベントビューアーのアプリケーションログを確認します。

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



注：「」

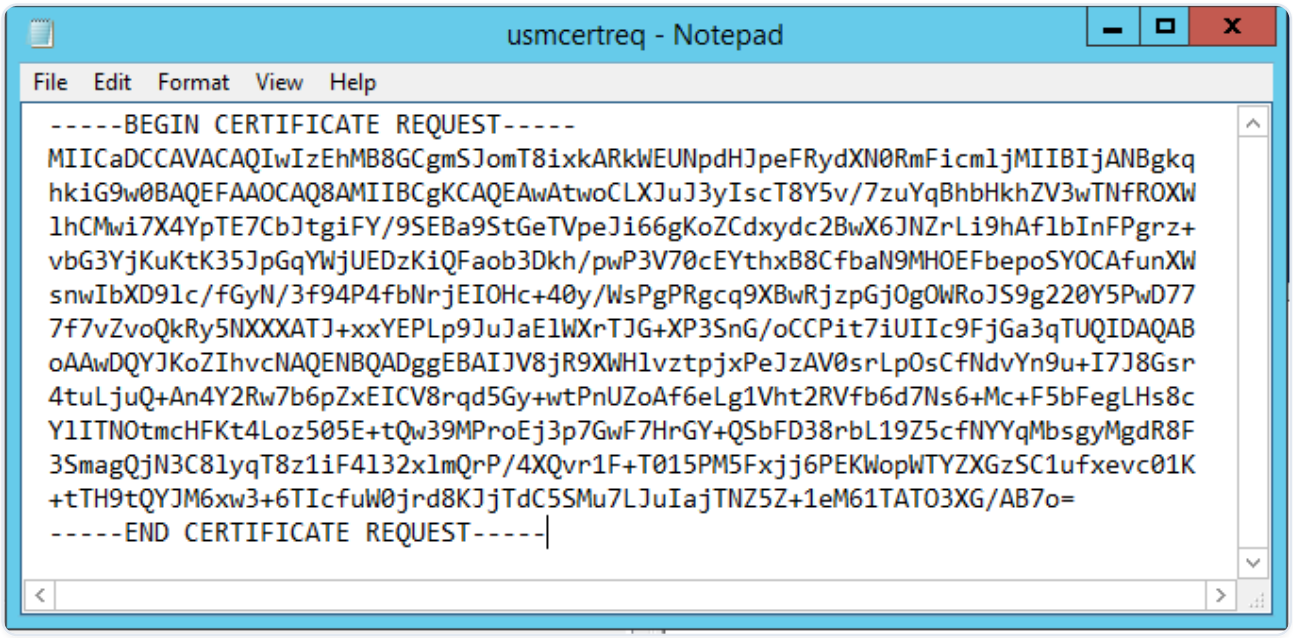
続いて：



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

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

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



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

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

例：

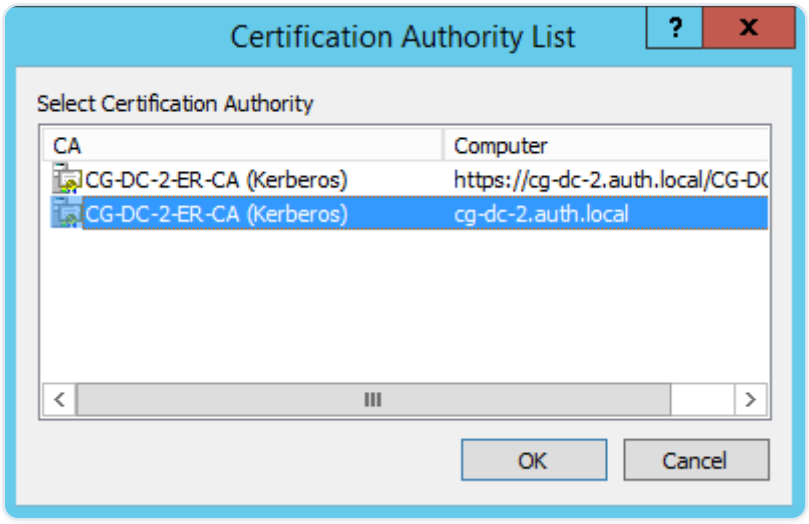
```
certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
```

次のように表示されます：



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

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



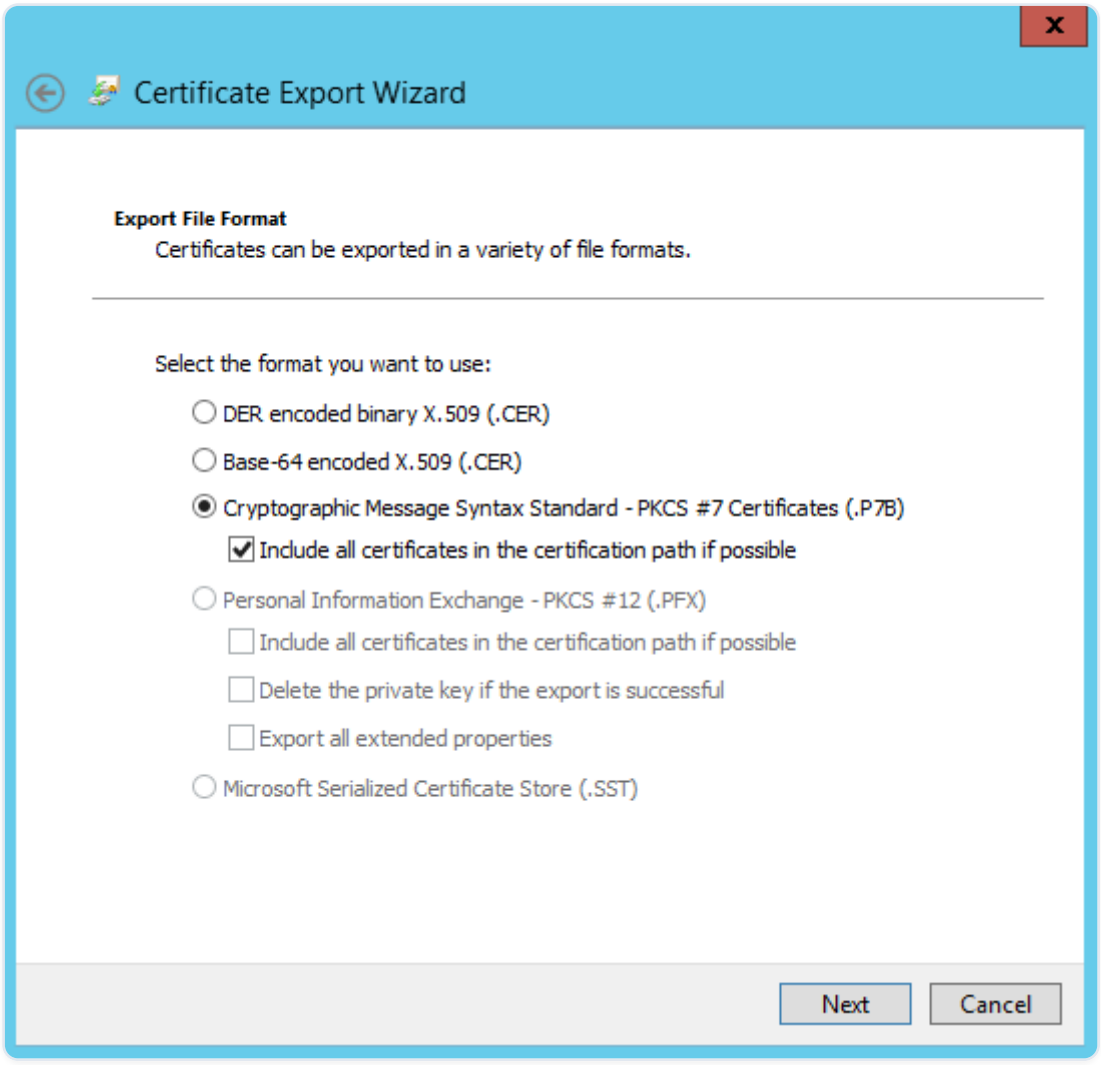
証明機関が指定されると、PowerShellはRequestIDを表示します。

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-0B0C-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

手順8： 証明機関サーバーで、証明機関MMCスナップインの**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。

手順9： **発行された証明書**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。

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



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

手順10： エクスポートした証明書ファイルをFASサーバーにコピーします。

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

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

例：

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

以下が表示されます。

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

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

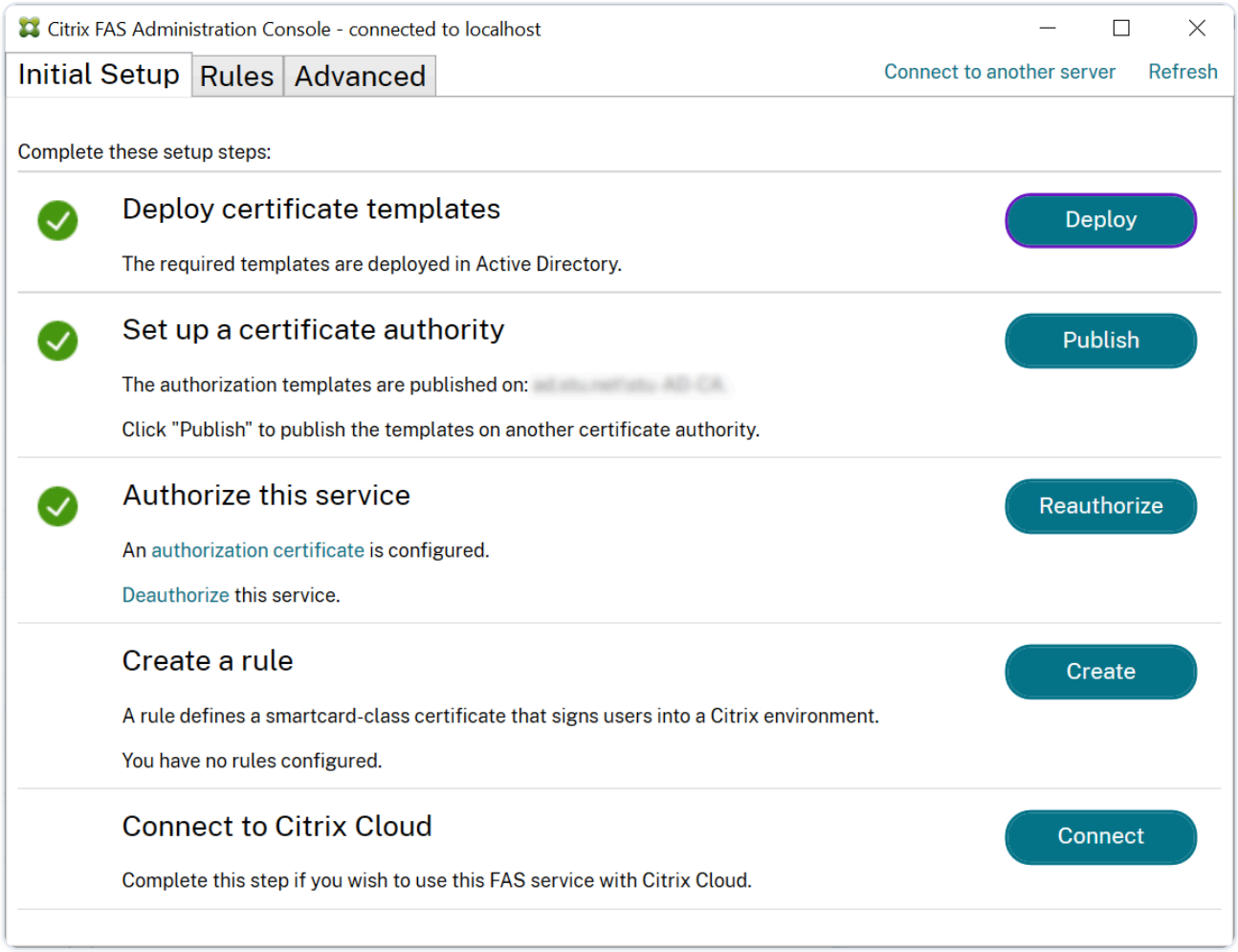

Id                : 74d427ff-c55b-4d6d-87ae-1ff98b0c2705
Address           : [Offline CSR]
TrustArea         : 978816cd-8b2f-4695-8c5d-08bb7df1816b
CertificateRequest :
Status            : Ok
```

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: 「このサービスを承認する」のステップに緑色のチェックマークが表示されます。

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

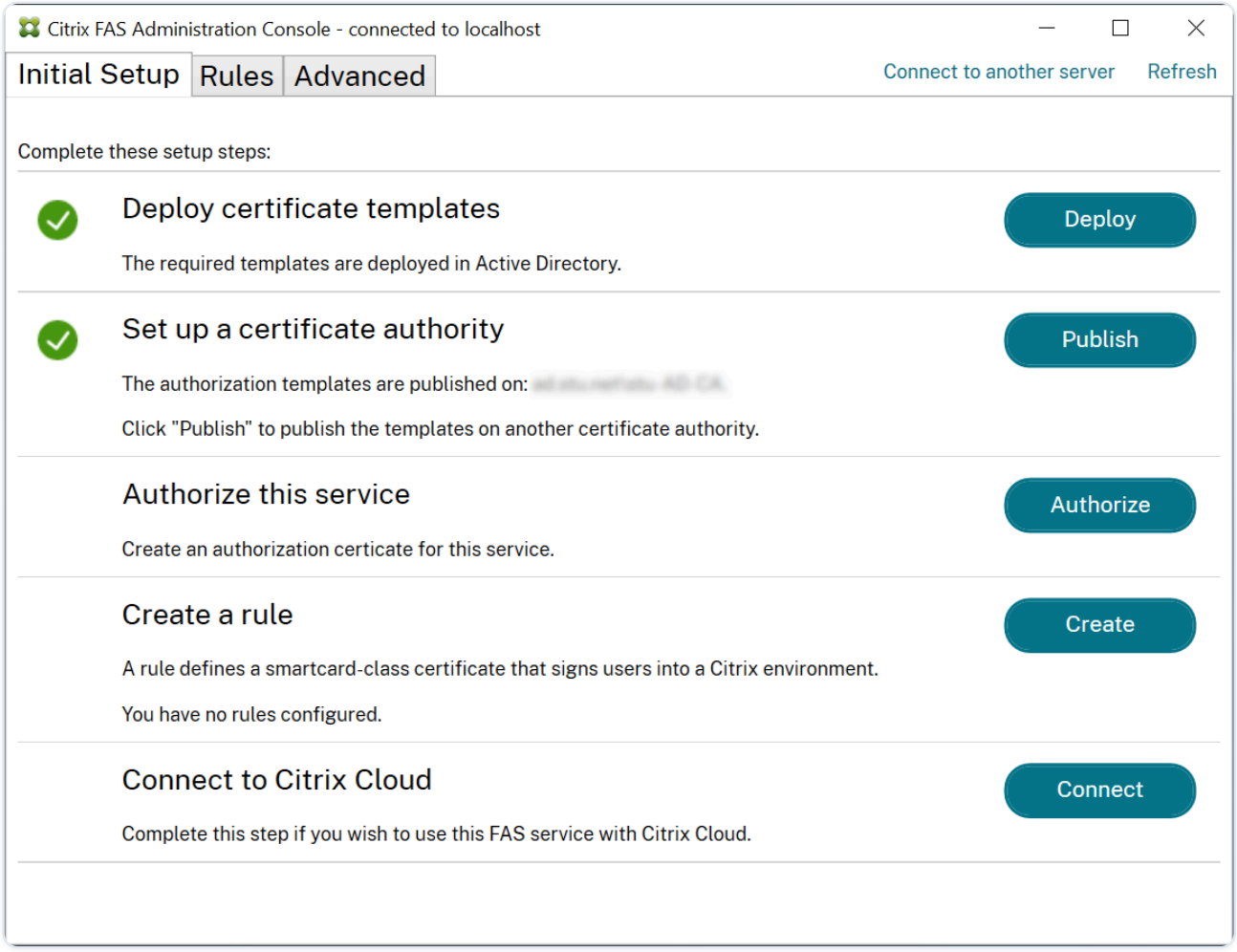
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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が構成済みであ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は、「証明書テンプレートの展開」と「証明機関のセットアップ」の最初の2つのステップのみを完了してください。



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

ステップ3: 設定ファイルを次のように編集します。

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

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

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.Supress" value="" / -->

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

このシナリオでは、HSM が CNG を使用しているため、ProviderLegacyCsp 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。

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

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

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

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

注：[プロバイダー: HSM ベンダーのキーストレージプロバイダー]

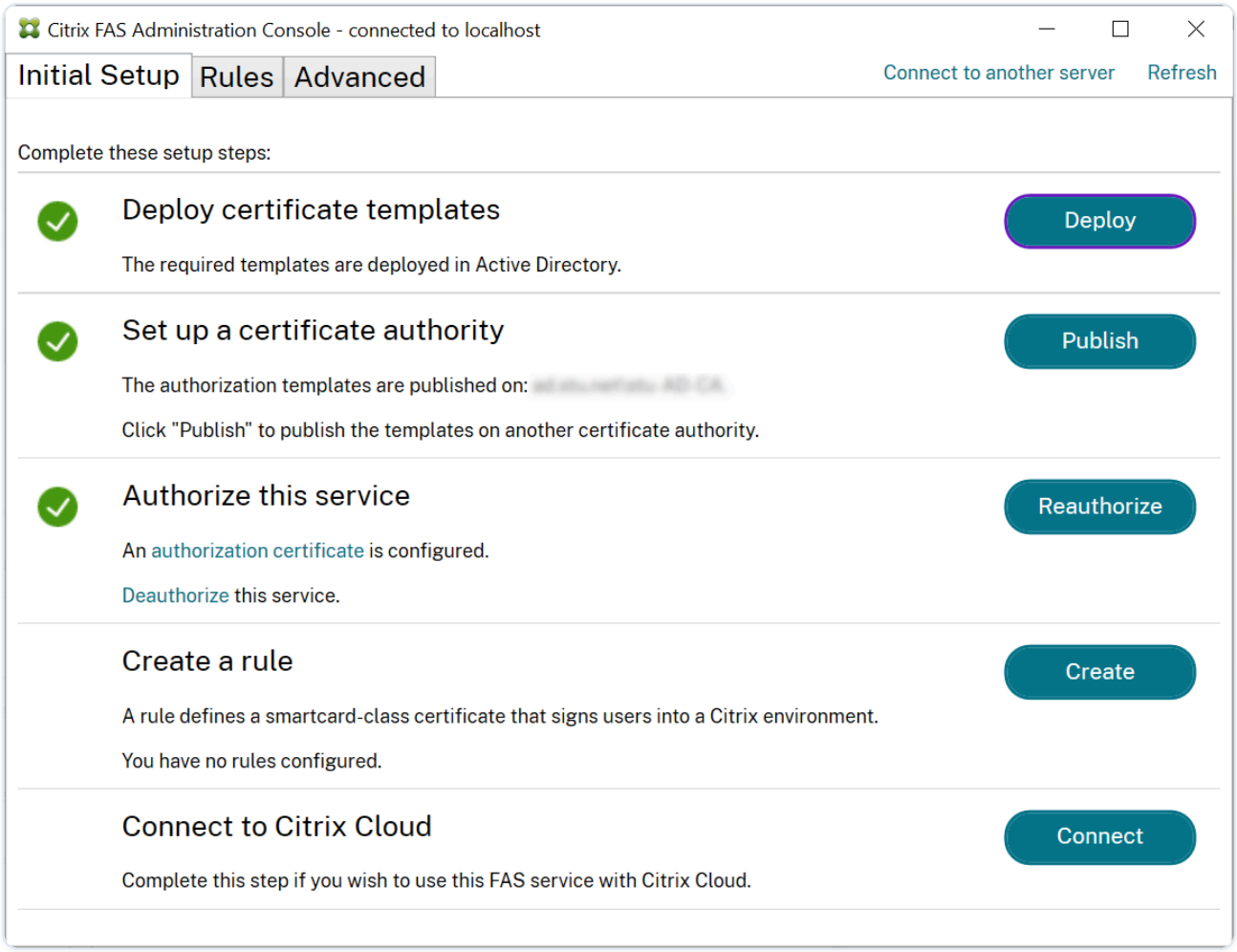
手順 7: 証明機関サーバーで、証明機関 MMC の ノードを選択します。

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\UCSHSM$	

要求を右クリックし、 を選択します。

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

注：「このサービスを承認する」の手順に緑色のチェックマークが付いています。



手順 8: FAS 管理コンソールで タブを選択し、「インストールと構成」の説明に従って設定を編集します。

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**:

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

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


Id                : e3044634-6790-4de0-a8ee-d599bb047ad7
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE-----
                    [redacted]
                    -----END CERTIFICATE-----
Status            : WaitingForApproval


PS C:\Users\administrator.STU>
```

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、以下を使用して取得できます。

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

例:

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

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

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


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

関連情報

- 「インストールと構成」(/ja-jp/federated-authentication-service/2305/install-configure.html)は、FASのインストールと構成に関する主要なリファレンスです。
- 一般的なFAS展開については、「フェデレーション認証サービスアーキテクチャの概要」(/ja-jp/federated-authentication-service/2305/deployment-architectures.html)の記事にまとめられています。
- その他の「ハウツー」記事は、「高度な構成」(/ja-jp/federated-authentication-service/2305/config-manage.html)の記事で紹介されています。

セキュリティとネットワーク構成

Federated Authentication Service (FAS) は、Microsoft Active Directory および Microsoft 認証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の場合と同様に、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るようにしてください。

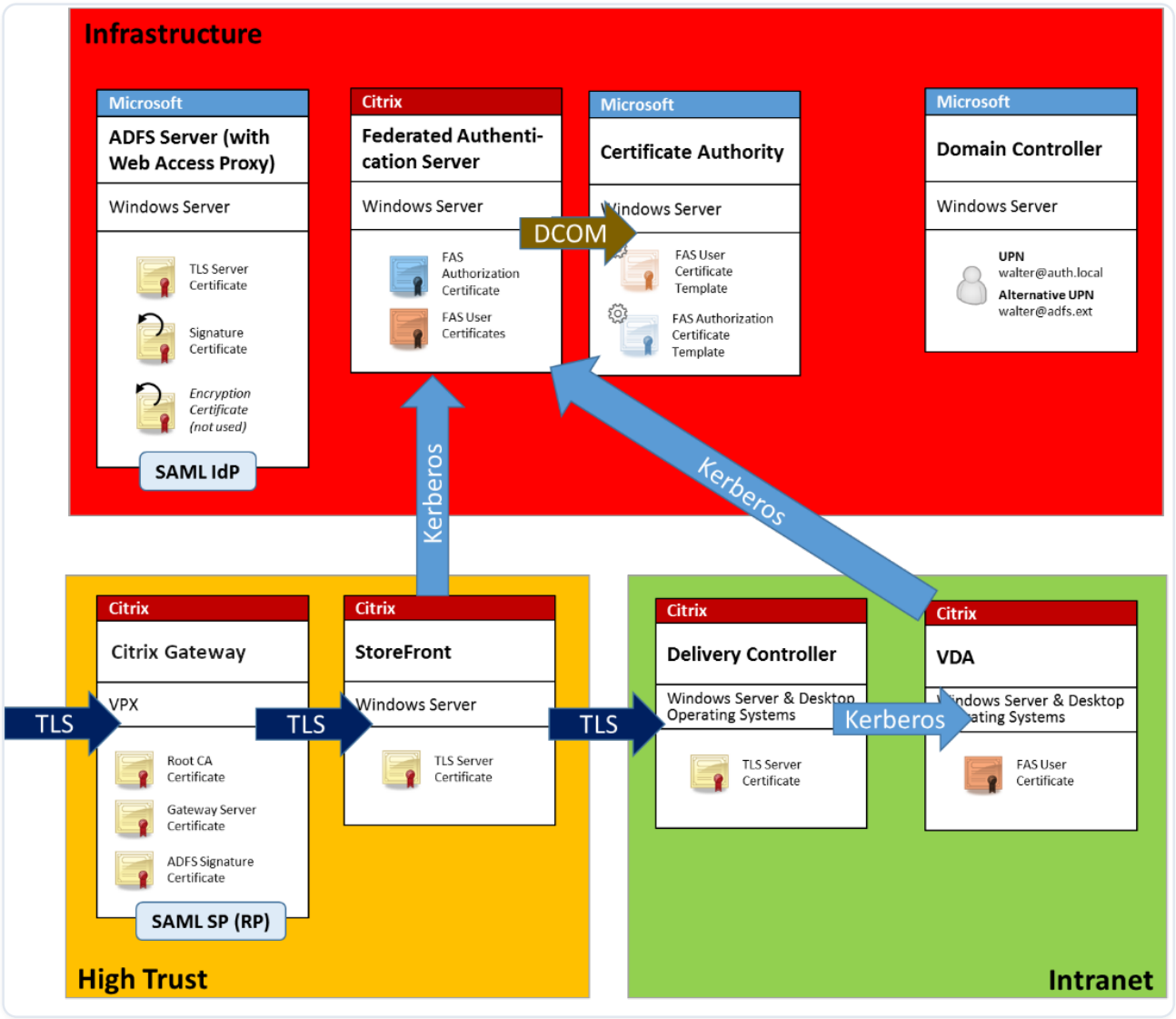
このドキュメントでは、FAS を展開する際に考慮すべきセキュリティ上の考慮事項の概要を説明します。また、インフラストラクチャの保護に役立つ可能性のある機能の概要も説明します。

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、認証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。

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



ファイアウォールとネットワークセキュリティ

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

StoreFront サーバーは、相互認証された Kerberos を使用してポート 80 経由で FAS サーバーに接続します。認証では、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 を使用します。この認証方法により、Citrix Virtual Delivery Agent (VDA) がユーザーをログオンさせるために必要な、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。認証では、FAS サーバーの Kerberos HOST/fqdn ID と、VDA の Kerberos マシン ID を使用します。また、VDA は証明書と秘密キーにアクセスするために「資格情報ハンドル」を提供する必要があります。

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

Microsoft 認証機関は、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。認証機関は、FAS サーバーが信頼された登録エージェント証明書によって署名された CMC パケットを提供することを要求します。

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

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

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

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

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

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

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

セキュリティに関する考慮事項

FASには、ドメインユーザーに自律的に証明書を発行できる登録機関証明書があります。これは、FASサーバーを保護し、その権限を制限するためのセキュリティポリシー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証明機関では、登録エージェント、証明書テンプレート、および登録エージェントが証明書を発行できるユーザーを制限できます。

登録エージェントダイアログ(/en-us/federated-authentication-service/2305/media/delegated-enrollment-agents.png)

提示されたダイアログを使用して、以下を確認できます。

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

アクセス制御リストの構成

ルールを構成するセクションで説明されているように、StoreFrontサーバーのリストを構成する必要があります。これらのStoreFrontサーバーは、証明書が発行される際にFASにユーザーIDをアサートします。同様に、証明書が発行されるユーザー、および認証できるVDAマシンを制限できます。この機能は、構成する標準のActive Directoryまたは証明機関のセキュリティ機能に追加されるものです。

ファイアウォール設定

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

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

イベントログの監視

FASとVDAは、Windowsイベントログに情報を書き込みます。このログは、監視および監査情報に使用できます。イベントログセクションには、生成可能なイベントログエントリが一覧表示されます。

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（たとえば、4096ビット、TPM保護）とランタイムユーザー証明書には、異なる設定を使用できます。

パラメーター	説明
ProviderLegacyCsp	trueに設定すると、FASはMicrosoft CryptoAPI (CAPI)を使用します。それ以外の場合、FASはMicrosoft Cryptography Next Generation API (CNG)を使用します。
ProviderName	使用するCAPIまたはCNGプロバイダーの名前。
プロバイダーの種類	Microsoft KeyContainerPermissionAccessEntry.ProviderType プロパティ PROV_RSA_AES 24 を指します。CAPIでHSMを使用しており、HSMベンダーが別途指定しない限り、常に24である必要があります。
キー保護	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は、トラステッドプラットフォームモジュール (TPM) キー ストレージの使用も許可します。
キー長	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 (既定値: 2048)。

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

管理者の責任

環境の管理は、次のグループに分けられます。

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

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

グループポリシー設定

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

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

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

証明書テンプレート

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

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

証明書テンプレートの名前を変更する

Citrix_SmartcardLogonの名前を組織のテンプレート命名標準に合わせる場合は、次の操作を行う必要があります。

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

一般プロパティの変更

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

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

要求処理プロパティの変更

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。

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

「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ったりする可能性があります。

「セキュリティ」プロパティの変更

Citrixでは、これらの設定を変更して、FASサーバーのマシンアカウントのみに**読み取り**および**登録**のアクセス許可を付与することをお勧めします。FASサービスには、その他のアクセス許可は必要ありません。ただし、他の証明書テンプレートと同様に、次のことができます。

- 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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-security-props-security.png)

「サブジェクト名」プロパティの変更

Citrixでは、これらのプロパティを変更しないことをお勧めします。

テンプレートには、*このActive Directory情報から構築*が選択されており、証明機関がユーザーのSIDを証明書拡張機能に含めるように設定されています。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。

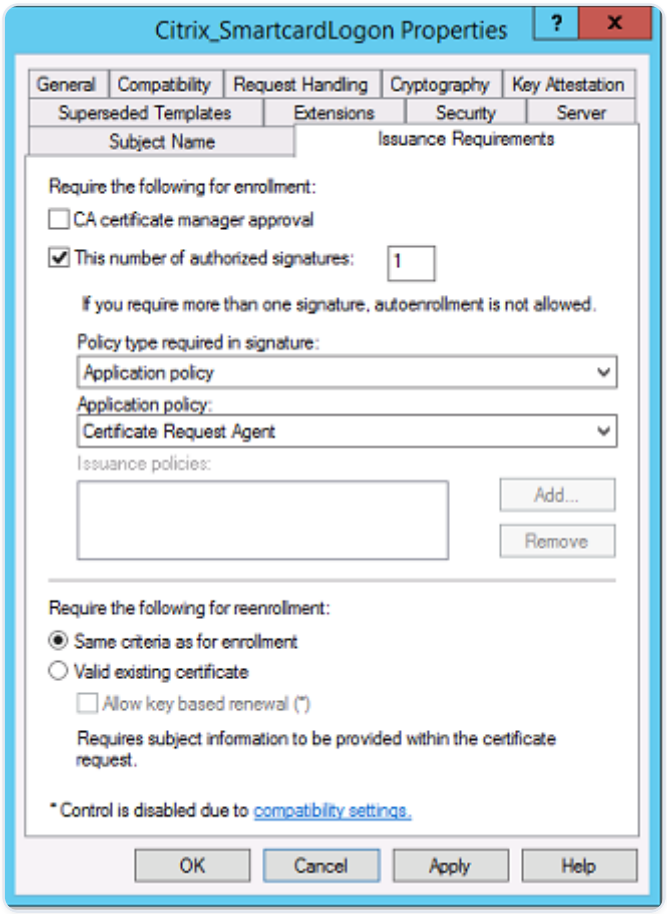
「サーバー」プロパティの変更

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

発行要件プロパティの変更

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

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



互換性プロパティの変更

これらの設定は変更できます。設定は少なくとも **Windows Server 2003 CA** (スキーマバージョン 2) である必要があります。ただし、FAS は Windows Server 2008 以降の CA のみをサポートしています。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秘密鍵の責任を負います。

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は、FAS サーバーのインストール時に登録機関証明書テンプレートのみを公開するか、完全にオフラインの発行プロセスを要求することです。いずれの場合も、証明機関管理者は登録機関証明書要求の承認を完全に管理し、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。

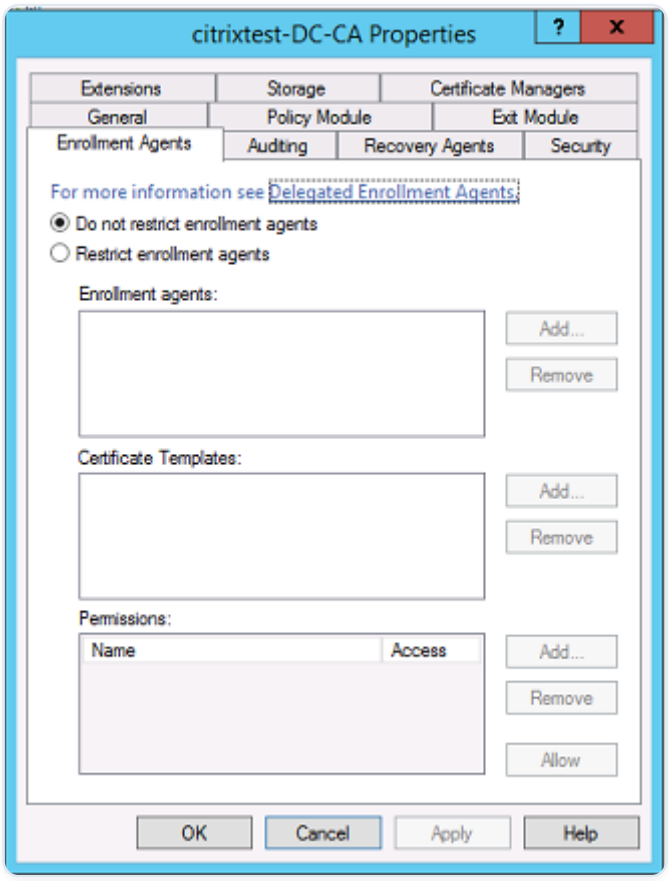
© 1997–2026 Citrix Systems, Inc. All rights reserved.

ファイアウォール設定

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

登録の制限

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

高度な展開では、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。

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

ACLによるStoreFront、ユーザー、およびVDAの制限

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

アクセスベクター	説明
StoreFront [IdP]	これらのKerberosアカウントは、ユーザーが正しく認証されたことを宣言するために信頼されています。これらのアカウントのいずれかが侵害された場合、FASの構成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、証明書と秘密キーへのアクセスが許可されているマシンです。IdPによって取得された資格情報ハンドルも必要であるため、このグループ内の侵害されたVDAアカウントがシステムを攻撃できる範囲は限られています。
ユーザー	このオプションは、どのユーザーがIdPによってアサートできるかを制御します。証明機関の「制限付き登録エージェント」構成オプションと重複することに注意してください。一般に、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

ルールは、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に役立ちます。各ルールには個別の構成オプションセットがあり、特にKerberosアクセス制御リスト（ACL）は個別に構成できます。

証明機関とテンプレートを構成する

異なるアクセス権限に対して、異なる証明書テンプレートとCAを構成できます。高度な構成では、環境に応じて、より強力な証明書またはより強力でない証明書を使用することを選択できま

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

す。たとえば、「外部」として識別されたユーザーは、「内部」ユーザーよりも少ない権限を持つ証明書を持つことができます。

セッション内および認証証明書

FAS管理者は、認証に使用される証明書がユーザーのセッション内で使用可能であるかどうかを制御できます。 たとえば、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、秘密鍵をハードウェアセキュリティモジュール（HSM）またはトラステッドプラットフォームモジュール（TPM）に保存するようにFASを構成できます。Citrixは、少なくとも登録機関証明書の秘密鍵をTPMに保存して保護することを推奨しています。FASは、「オフライン」証明書要求プロセスの一部として、秘密鍵を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鍵はTPMまたはHSMに保存できます。すべての鍵は「エクスポート不可」として生成され、長さは2048ビット以上である必要があります。

イベントログ

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

管理アクセスと管理ツール

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

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

FASの使用は、FASの「資格情報ハンドル」が「Active Directoryパスワード」を単に置き換えるため、Delivery ControllerおよびVDA管理者のセキュリティモデルを変更しません。ControllerおよびVDA管理グループには、信頼できるユーザーのみを含める必要があります。監査およびイベントログは維持する必要があります。

一般的なWindowsサーバーセキュリティ

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と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

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

は、物理的に安全な場所に保管し、ディスク暗号化と仮想マシンのメンテナンスオプションに注意を払う必要があります。

監査ログとイベントログは、リモートマシンに安全に保存する必要があります。

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

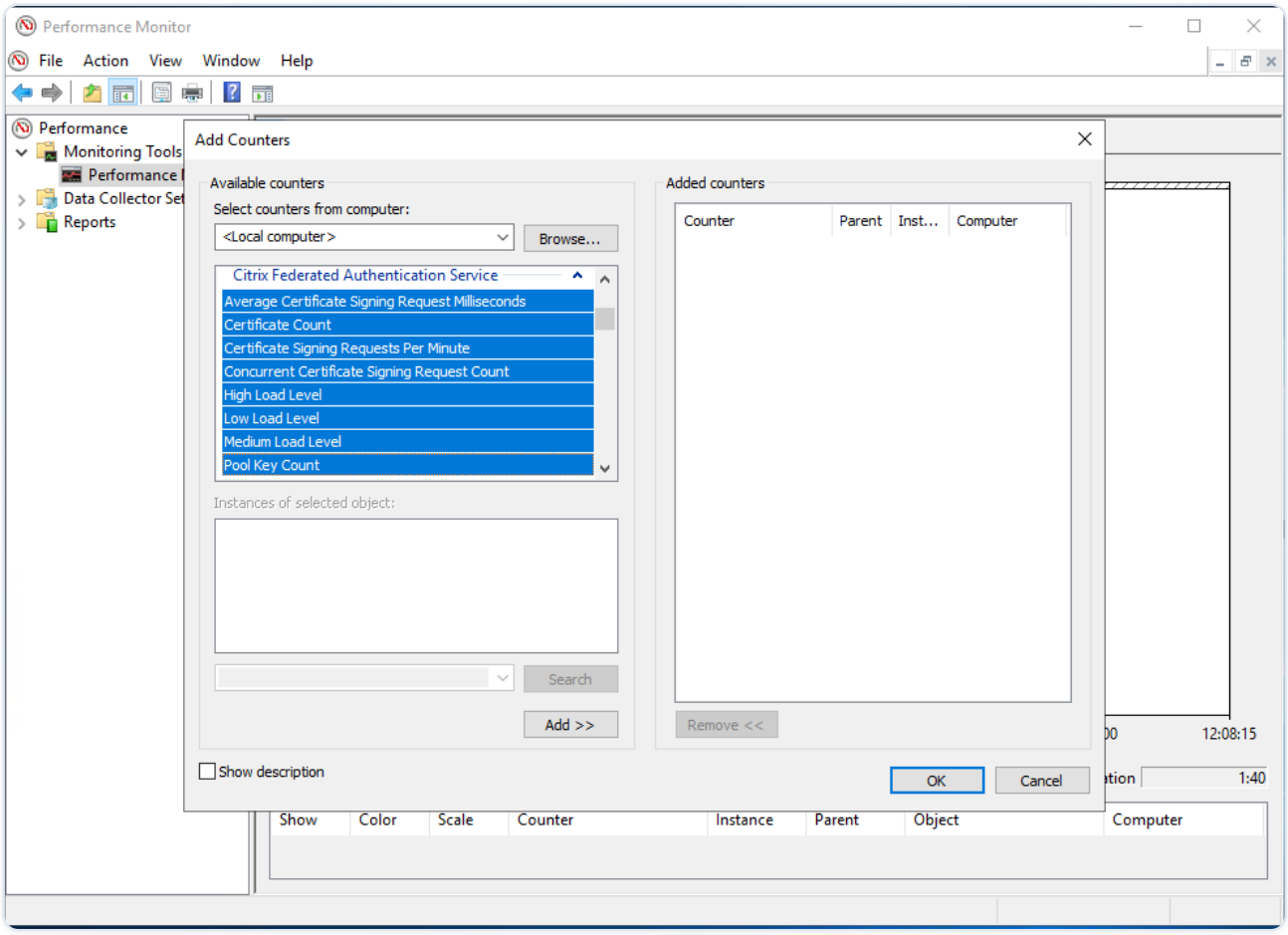
関連情報

- (/ja-jp/federated-authentication-service/2305/install-configure.html)は、FASのインストールと構成に関する主要なリファレンスです。
- FASアーキテクチャについては、(/ja-jp/federated-authentication-service/2305/deployment-architectures.html)の記事で紹介されています。
- その他の「ハウツー」記事については、(/ja-jp/federated-authentication-service/2305/config-manage.html)の記事で紹介されています。

パフォーマンスカウンター

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

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



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

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

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

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

Windowsログオンの問題のトラブルシューティング

この記事では、ユーザーが証明書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利用できる情報を提供します。

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ています。

- **NTAuth証明書ストア**: Windowsに認証するには、ユーザー証明書を直接発行する認証局（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、最後から2番目の証明書はNTAuthストアになければなりません。
- **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)>`。

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

レジストリポリシー	説明
AllowCertificatesWithNoEKU	無効にすると、証明書にはスマートカードログオン拡張鍵使用 (EKU) を含める必要があります。
AllowSignatureOnlyKeys	デフォルトでは、WindowsはRSA復号化を許可しない証明書の秘密鍵をフィルタリングします。このオプションはそのフィルタを上書きします。
AllowTimeInvalidCertificates	デフォルトでは、Windowsは期限切れの証明書をフィルタリングします。このオプションはそのフィルタを上書きします。
EnumerateECCCerts	楕円曲線認証を有効にします。
X509ヒンツニーデッド	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、すべてのサーバーに適切な「ドメインコントローラー」証明書が必要です。これらは、「ローカルコンピューター証明書個人ストア」MMCスナップインメニューを使用して要求できます。

UPN名と証明書マッピング

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

Active DirectoryにおけるUPN名

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

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

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

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

証明書マッピングサービス

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

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

フォレスト内に複数のドメインがあり、ユーザーがドメインを明示的に指定しない場合、Active Directory 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x509証明書属性のキャッシュされたビューを持っています。このコンピューターは、証明書のみに基づいて、任意のドメイン内のユーザーアカウントを効率的に見つけるために使用できます。

ログオンドメインコントローラーの選択を制御する

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

ドメインコントローラーの選択を制御する

Windowsが特定のWindowsドメインコントローラーをログオンに使用するように強制するには、lmhostsファイルを構成して、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: \Windows\System32\drivers\etc\lmhosts。

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

1.2.3.4 dcnetbiosname #PRE #DOM: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。

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

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

使用中のドメインコントローラーを特定する

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

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

アカウント監査イベントを有効にする

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

アカウント監査イベントを有効にする(/en-us/federated-authentication-service/2305/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、**アプリケーションとサービスログ** > **Microsoft** > **Windows** > **CAPI2** > **Operational** に移動します。**Operational** を右クリックし、**ログの有効化** を選択します。

さらに、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。

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

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0xffffff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は、コンピューターの中間証明書ストアおよび信頼されたルート証明書ストアにある証明書を使用して構築できませんでした。
証明書失効チェックエラー	スマートカードのCRLは、証明書のCRL配布ポイントで指定されたアドレスからダウンロードできませんでした。失効チェックが必須の場合、これによりログオンが成功しません。証明書と公開鍵インフラストラクチャセクションを参照してください。

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

エラーコード	説明
証明書使用エラー	この証明書はログオンに適していません。たとえば、サーバー証明書または署名証明書である可能性があります。

Kerberosログ

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

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

Kerberosログはシステムイベントログに出力されます。

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

ドメインコントローラーおよびワークステーションログ

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

- ドメインコントローラー CAPI2 ログ
- ドメインコントローラー セキュリティログ

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

- Virtual Delivery Agent (VDA) セキュリティログ
- VDA CAPI ログ
- VDA システムログ

ドメインコントローラー CAPI2 ログ

ログオン中に、ドメインコントローラーは呼び出し元の証明書を検証し、次の形式で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/2305/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/2305/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ログオンイベントのシーケンスを表示し、主要なイベントは4768です。このイベントでは、証明書がKerberos Ticket Granting Ticket (krbtgt) の発行に使用されます。

これより前のメッセージは、サーバーのマシンアカウントがドメインコントローラーに対して認証を行っていることを示しています。これに続くメッセージは、新しい krbtgt に属するユーザーアカウントがドメインコントローラー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/2305/media/fas-troubleshoot-logon-dc-security-log.png)

VDA セキュリティログ

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

VDAセキュリティログ(/en-us/federated-authentication-service/2305/media/fas-troubleshoot-logon-vda-security-log.png)

VDA CAPIログ

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

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

VDA CAPIログ(/en-us/federated-authentication-service/2305/media/fas-troubleshoot-logon-capi-log.png)

VDA CAPIログ 2(/en-us/federated-authentication-service/2305/media/fas-troubleshoot-logon-capi-chainpolicy.png)

VDAシステムログ

Kerberosログが有効になっている場合、システムログにはエラーKDC_ERR_PREAUTH_REQUIRED（これは無視できます）と、Kerberosログオンが成功したことを示すWinlogonからのエントリが表示されます。

VDAシステムログ(/en-us/federated-authentication-service/2305/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、ここで説明されているプロセスとイベントを使用してFASサービスの健全性を監視できます。

FASサービスは実行中ですか?

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

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

FASヘルスイベント

以下のイベントは、FASサービスが正常であるかどうかを示します。

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

イベント	イベントテキスト	説明	注
[S003]	管理者 [{0}] がメンテナンスモードを [{1}] に設定	FASサービスがメンテナンスモードに移行したか、メンテナンスモードから解除されました。	メンテナンスモード中は、FASサーバーはシングルサインオンに使用できません。

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

イベント	イベントテキスト	説明	注
[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以降で利用可能です。
[S123]	[upn: {0} role: {1}] [exception: {2}] の証明書の発行に失敗しました	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、このイベントは [S124] の後に発生します。そのユーザーのシングルサインオンは失敗します。	このイベントは、構成されているすべてのCAが機能していないことを示します。FASがHSMを使用するように構成されている場合、HSMが機能していないことも示している可能性があります。
[S124]	[certificate authority: {2}] [exception: {3}] で [upn: {0} role: {1}] の証明書の発行に失敗しました	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、障害が発生しました。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、連絡不能であることを示している可能性があります。FASがHSMを使用するように構成されている場合、HSMが機能していないことも示している可能性があります。例外は、問題の原因を特定するのに役立ちます。
[S413]	承認証明書の有効期限が間もなく切れます（残り{0}日）。証明書の詳細: {1}	このイベントは、FAS承認証明書の有効期限が近づくと定期的に生成されます。デフォルトでは、承認証明書の有	既定の設定は、コマンドレット **Set-FasRaCertificateMonitor** を使用して調整できます。PowerShell コマンド

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

イベント	イベントテキスト	説明	注
		効期限が30日以内である場合、毎日イベントが生成されます。	レット を参照してください。
[S414]	認証証明書の有効期限が切れました。証明書の詳細: {0}	このイベントは、FAS認証証明書の有効期限が切れると定期的に生成されます。デフォルトでは、このイベントは毎日生成されます。	有効期限が切れると、FASは新しいユーザー証明書を生成できなくなり、シングルサインオンが失敗し始めます。

クラウド接続FASイベント

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

イベントソースは**Citrix.Fas.Cloud**です。

イベント	イベントテキスト	説明	注記
[S012]	FASサービスはCitrix Cloudからのシングルサインオンに利用可能です	このイベントは、Workspace（つまりCitrix Cloud）からのシングルサインオンが機能しているはずであることを示します。	このイベントを発行する前に、FASは(1)構成されていること、(2)メンテナンスモードではないこと、および(3)Citrix Cloudに接続されていることを確認します。
[S013]	FASサービスはCitrix Cloudからのシングルサインオンに利用できません。[{0}] 詳細については、管理コンソールで確認できます。	このイベントは、FASがWorkspace（つまりCitrix Cloud）からのシングルサインオンを提供できないことを示しています。メッセージには、シングルサインオンが機能	FASはCitrix Cloudへの永続的な接続を維持します。この接続は、ネットワークの不具合やプロキシサーバーの接続寿命ポリシーなど、さまざまな理由で時々切断されることがあり

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

イベント	イベントテキスト	説明	注記
		しない理由が含まれています。	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

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

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

イベント	イベントテキスト	説明
[S001]	アクセス拒否: ユーザー [{0}] はAdministratorsグループのメンバーではありません	FASの構成を表示または変更しようとしましたが、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ましたが、呼び出し元がFAS管理者ではありませんでした。
[S101]	サーバー [{0}] は、役割 [{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	ユーザーIDをアサートしようとしましたが、FASルール構

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

イベント	イベントテキスト	説明
	（UPNは役割 [{2}] で許可されていません）	成に従ってユーザーアカウントが許可されていません。
[S205]	証明書利用者アクセスが拒否されました - 呼び出し元アカウント [{0}] は、ルール [{1}] の許可された証明書利用者ではありません	VDAがFASでシングルサインオンを実行しようとしましたが、FASルール構成に従ってVDAは許可されていません。

FASイベントログ

次の表に、FASによって生成されるイベントログエントリを示します。

管理イベント

これらのイベントは、FASサーバー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
[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

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

ログコード
[S012] 管理者 [{0}] が証明書 [upn: {1} sid: {2} rule: {3}]Certificate Definition: {4} Security Context: {5}] を作成しています
[S013] 管理者 [{0}] が証明書 [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}] を削除しています
[S015] 管理者 [{0}] が証明書要求 [TPM: {1}] を作成しています
[S016] 管理者 [{0}] が承認証明書をインポート中 [Reference: {1}]
[S022] 管理者 [{0}] がメンテナンスモードをオフに設定中
[S023] 管理者 [{0}] がメンテナンスモードをオンに設定中
[S024] 管理者 [{0}] がシステムヘルスモニターを設定中
[S025] 管理者 [{0}] がシステムヘルスモニターを設定中
[S026] 管理者 [{0}] がRA証明書モニターを設定中
[S027] 管理者 [{0}] がRA証明書モニターをリセット中
[S050] 管理者 [{0}] がクラウド構成を作成中: [{1}]
[S051] 管理者 [{0}] がクラウド構成を更新中: [{1}]
[S052] 管理者 [{0}] がクラウド構成を削除中
[S060] 管理者 [{0}] がクラウド登録を要求中。インスタンス: {1}
[S060] 管理者 [{0}] がダイレクトトラストクラウド登録を要求中。インスタンス: {1} CloudServiceUrlFormat: {2}
[S061] 管理者 [{0}] がクラウド登録を完了中。リソースの場所: {1}、ルール名: {2}
[S062] 管理者 [{0}] がクラウド登録を完了しました。リソースの場所: {1} ({2})、ルール名: {3}、顧客: {4} ({5})
[S063] クラウド登録中にKRSエラーが発生しました。例外は {0} でした
[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。

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

ログコード
[S401] 構成のアップグレードを実行中 - [From version {0} to version {1}]
[S402] エラー: Citrix Federated Authentication Service は Network Service として実行する必要があります [currently running as: {0}]
[S404] Citrix Federated Authentication Service データベースを強制的に消去しています
[S405] レジストリからデータベースへのデータ移行中にエラーが発生しました: [{0}]
[S406] レジストリからデータベースへのデータ移行が完了しました (注: ユーザー証明書は移行されません)
[S407] データベースが既に存在するため、レジストリベースのデータはデータベースに移行されませんでした
[S408] 構成をダウングレードできません -- [From version {0} to version {1}]
[S409] ThreadPool 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。これにより FAS サーバーのスケーラビリティに影響が出る可能性があります
[S411] FAS サービスの開始中にエラーが発生しました: [{0}]
[S412] 構成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。

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

ログコード
[S101] サーバー [{0}] は、ロール [{1}] でIDをアサートする権限がありません。
[S102] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (例外: {2}{3})
[S103] サーバー [{0}] はUPN [{1}] SID {2} を要求しましたが、ルックアップはSID {3} を返しました。
[S104] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (UPNはロール [{2}] で許可されていません)
[S105] サーバー [{0}] はIDアサーションを発行しました [upn: {1}, role {2}, Security Context: [{3}]]
[S120] 証明書を発行中 [upn: {0} role: {1} Security Context: [{2}]]
[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

依拠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] 依拠当事者 [{0}] はパスワードにアクセスできません。
[S202] 依拠当事者 [{0}] は証明書にアクセスできません。
[S203] 依拠当事者 [{0}] はLogon CSPにアクセスできません
[S204] 依拠当事者 [{0}] が、[{4}] によって承認されたロール: [{2}] [Operation: {3}] で [upn: {1}] の Logon CSPにアクセスしています
[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

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

ログコード
[S206] 呼び出し元アカウント [{0}] は依拠当事者ではありません
[S208] 秘密キー操作が失敗しました [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}]。

セッション内証明書サーバー

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

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

FASアサーションプラグイン

これらのイベントはFASアサーションプラグインによってログに記録されます。

ログコード
[S500] FASアサーションプラグインが構成されていません
[S501] 構成されたFASアサーションプラグインをロードできませんでした [exception:{0}]
[S502] FASアサーションプラグインがロードされました [pluginId={0}] [assembly={1}] [location={2}]
[S503] サーバー [{0}] はUPN [{1}] をアサートできませんでした (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)

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

ログコード
[S504] サーバー [{0}] はUPN [{1}] をアサートできませんでした (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}] をアサートできませんでした (プラグイン [{2}] はステータス [{3}] とメッセージ [{4}] でログオン証拠を拒否しました)
[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}] のアサートに失敗しました (プラグイン [{2}] がメソッド [{4}] の実行中に例外 [{3}] をスローしました)
[S507] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (プラグイン [{2}] が例外 [{3}] をスローしました)
[S508] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (アクセス処理が提供されましたが、プラグイン [{2}] はそれをサポートしていません)
[S509] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (アクセス処理が提供されましたが、構成済みの FAS プラグインがありません)
[S510] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (アクセス処理はプラグイン [{2}] によって無効と見なされました)

Workspace対応のFAS

これらのイベントは、FAS が Workspace とともに使用されるときにログに記録されます。

ログコード
[S001] Citrix Cloud 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}]
[S004] FAS がクラウドへの登録に失敗しました [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S005] FAS が現在の構成をクラウドに送信しました [fas id: {0}] [transaction id: {1}]
[S006] FAS 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}]

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

ログコード
[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: {0} に接続されています
[S011] FAS サービスはクラウドに接続されていません
[S012] FAS サービスは Citrix Cloud からのシングルサインオンに利用できます
[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 はクラウドからの構成のダウンロードに失敗しました [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S021] クラウドサポートモジュールの起動に失敗しました。例外: {0}
[S022] クラウドサポートモジュールが停止しています
[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}]
[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}]

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

ログコード
[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} でした
[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。ログオン中 [Username: {0} Domain: {1}]
[S106] IDアサーションログオン。\n\nフェデレーション認証サービス: {0}\n\nログオン中 [Certificate: {1}]
[S107] IDアサーションログオンに失敗しました。 [Exception: {0}{1}]
[S108] IDアサーションサブシステム。アクセス拒否 [Caller: {0}]

セッション内証明書

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

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

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

ログコード
[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記録されます。

ログコード
[S001] TrustArea::TrustArea: インストールされた証明書 [TrustArea: {0} Certificate {1} TrustAreaJoinParameters {2}]
[S014] Pkcs10Request::Create: PKCS10要求を作成しました [Distinguished Name {0}]
[S016] プライベートキー::生成 [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

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

表示されたエラーメッセージ	説明と参照
	た。この記事の「***Kerberos ログ***」セクションを参照してください。
システムはログオンできませんでした。資格情報を確認できませんでした。 / 要求はサポートされていません	ドメインコントローラーに接続できないか、ドメインコントローラーがスマートカード認証をサポートする証明書で構成されていません。「Kerberos認証」、「ドメインコントローラー認証」、または「ドメインコントローラー」証明書のためにドメインコントローラーを登録してください。既存の証明書が有効に見える場合でも、これ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。証明書と公開キー基盤を参照してください。
不正な要求	これは通常、証明書の拡張機能が正しく設定されていないか、RSAキーが短すぎる（<2048ビット）ことを示します。

関連情報

- スマートカードログオン用にドメインを構成する
- 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
- サードパーティの証明機関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

シンプルな展開には、Federated Authentication Service (FAS) 管理コンソールを使用できます。ただし、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。

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

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

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

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

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

展開アーキテクチャ

はじめに

フェデレーション認証サービス (FAS) は、Active Directory証明機関と統合し、ユーザーがCitrix環境内でシームレスに認証されることを可能にするCitrix® コンポーネントです。このドキュメントでは、展開に適したさまざまな認証アーキテクチャについて説明します。

有効にすると、FASはユーザー認証の決定を信頼されたStoreFrontサーバーに委任します。StoreFrontには、最新のWebテクノロジーに基づいて構築された包括的な組み込み認証オプションがあり、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™の展開にログインするために使用できるようになったことです。

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

- 内部展開
- Citrix Gateway のデプロイ
- ADFS SAML
- B2Bアカウントマッピング
- Windows 10 Azure AD ジョイン

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

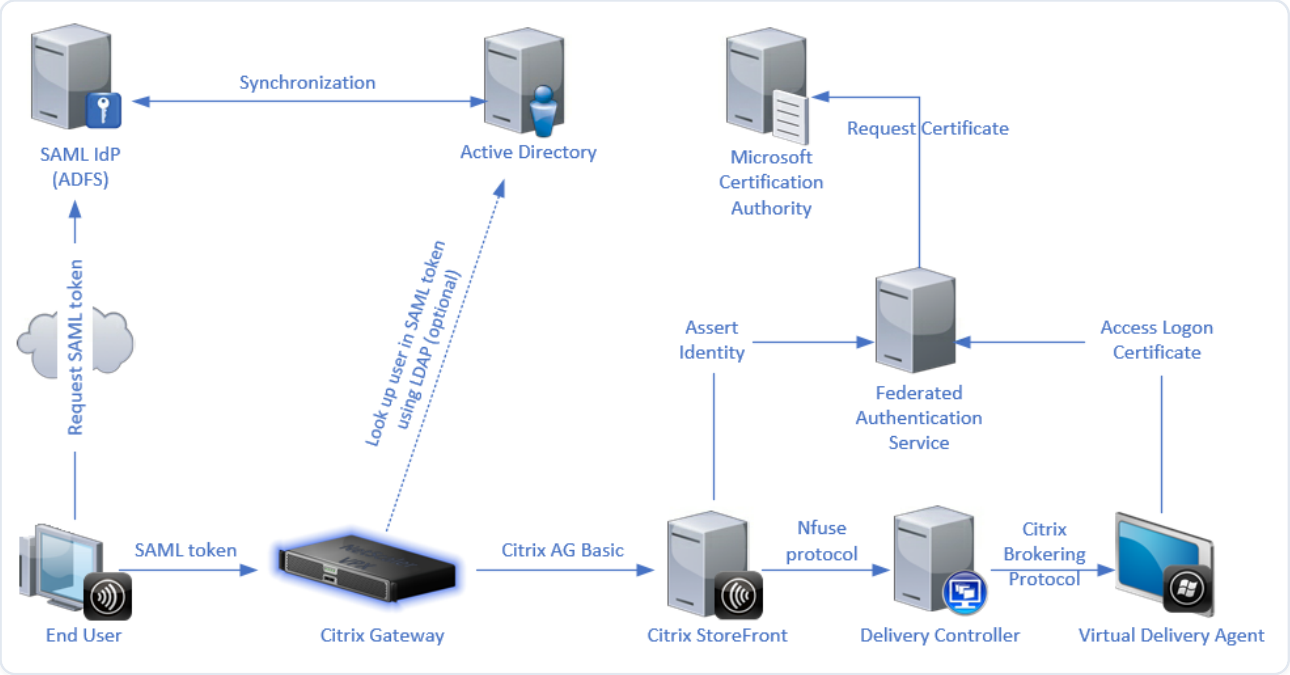
アーキテクチャの概要

FASは、StoreFrontによって認証されたActive Directoryユーザーに代わって、スマートカードクラスの証明書を自動的に発行することを承認されています。これは、管理者が物理スマートカードをプロビジョニングできるツールと同様のAPIを使用します。ユーザーがCitrix Virtual Apps™またはCitrix Virtual Desktops Virtual Delivery Agent (VDA) に仲介されると、証明書がマシンにアタッチされ、Windowsドメインはログオンを標準のスマートカード認証として認識します。

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

ユーザーがCitrix環境へのアクセスを要求すると、信頼されたStoreFront™サーバーはFASに接続します。FASは、単一のCitrix Virtual AppsまたはCitrix Virtual Desktopsセッションがそのセッションの証明書で認証することを許可するチケットを付与します。VDAがユーザーを認証する必要がある場合、FASに接続してチケットを引き換えます。FASのみがユーザー証明書の秘密鍵にアクセスできます。VDAは、証明書で実行する必要がある署名および復号化操作をすべてFASに送信する必要があります。

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



内部展開

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

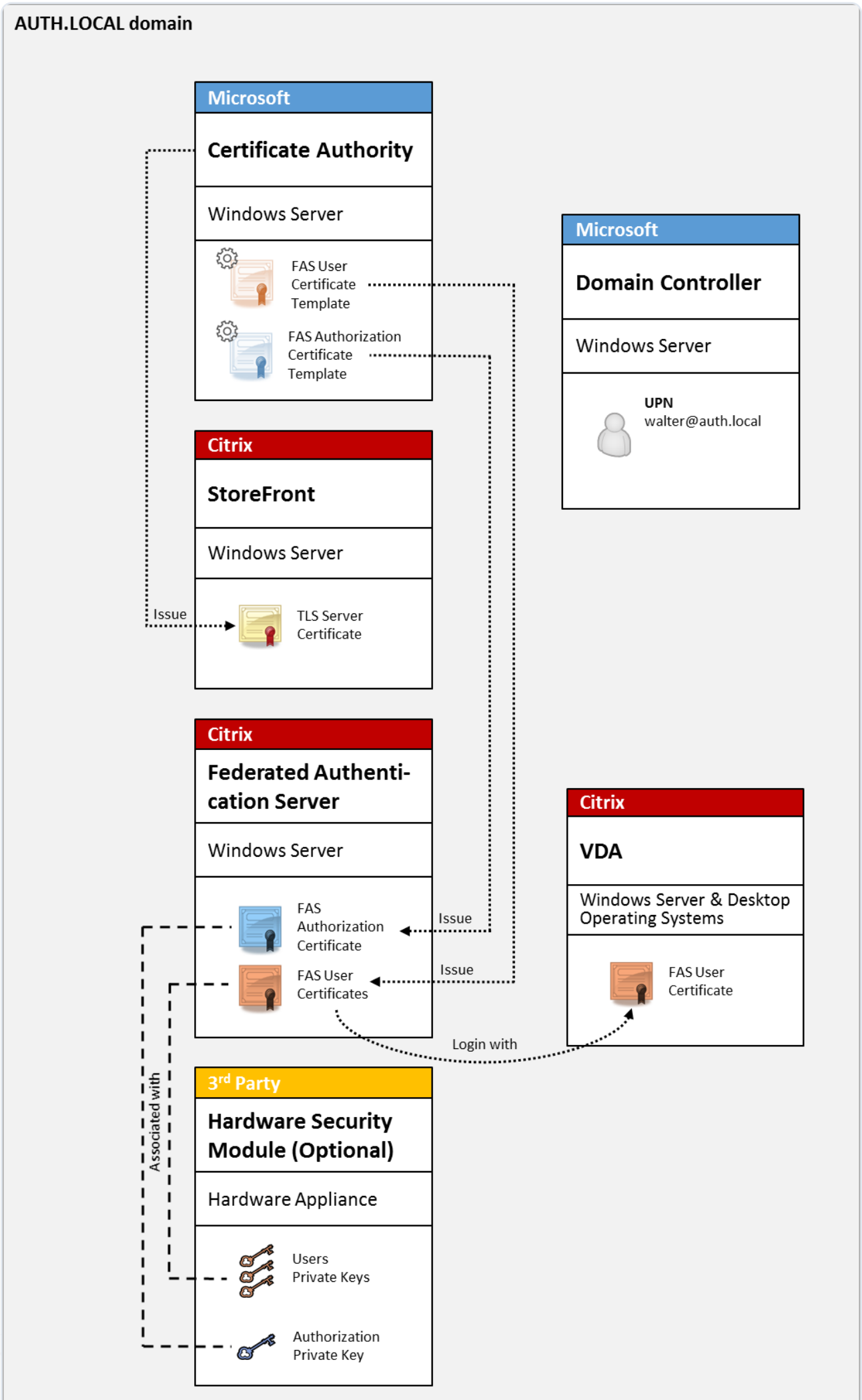
これにより、ユーザー資格情報やスマートカードPINの入力を求めるプロンプトなしでWindows認証が可能になり、シングルサインオンサービスなどの「保存されたパスワード管理」機能を使用する必要もありません。これは、以前のバージョンのCitrix Virtual Appsで利用可能だったKerberos制約付き委任ログオン機能を置き換えるために使用できます。

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

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

この展開では、FASを実行する新しいサーバーが追加され、このサーバーはユーザーに代わってスマートカードクラスの証明書を発行する権限を持っています。これらの証明書は、スマートカードログオンが使用されたかのように、Citrix HDX環境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。

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


AUTH.LOCAL domain
Microsoft
Certificate Authority
Windows Server
FAS User Certificate Template
FAS Authorization Certificate Template
Microsoft
Domain Controller
Windows Server
UPN
walter@auth.local
Citrix
StoreFront
Windows Server
Issue
TLS Server Certificate
Citrix
Federated Authenti-cation Server
Windows Server
FAS Authorization Certificate
FAS User Certificates
Issue
Issue
Citrix
VDA
Windows Server & Desktop Operating Systems
FAS User Certificate
Login with
3rd Party
Hardware Security Module (Optional)
Hardware Appliance
Users Private Keys
Authorization Private Key
Associated with

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

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

関連情報:

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

シトリックス ゲートウェイ 展開

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

この展開は、最初にCitrix Gatewayに認証し、次にユーザーセッションにログオンする際に発生する複数のPINプロンプトを回避するために使用できます。また、ADパスワードやスマートカードを別途必要とせずに、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/2305/media/fas-architectures-netscaler.png)

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

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

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

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-architectures-netscaler-auth-settings.png)

関連情報:

- Citrix Gatewayを構成するには、「How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and Citrix Virtual Desktops 7.6」を参照してください。
- Install and configureは、FASのインストールと構成方法について説明しています。

ADFS SAML展開

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/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。

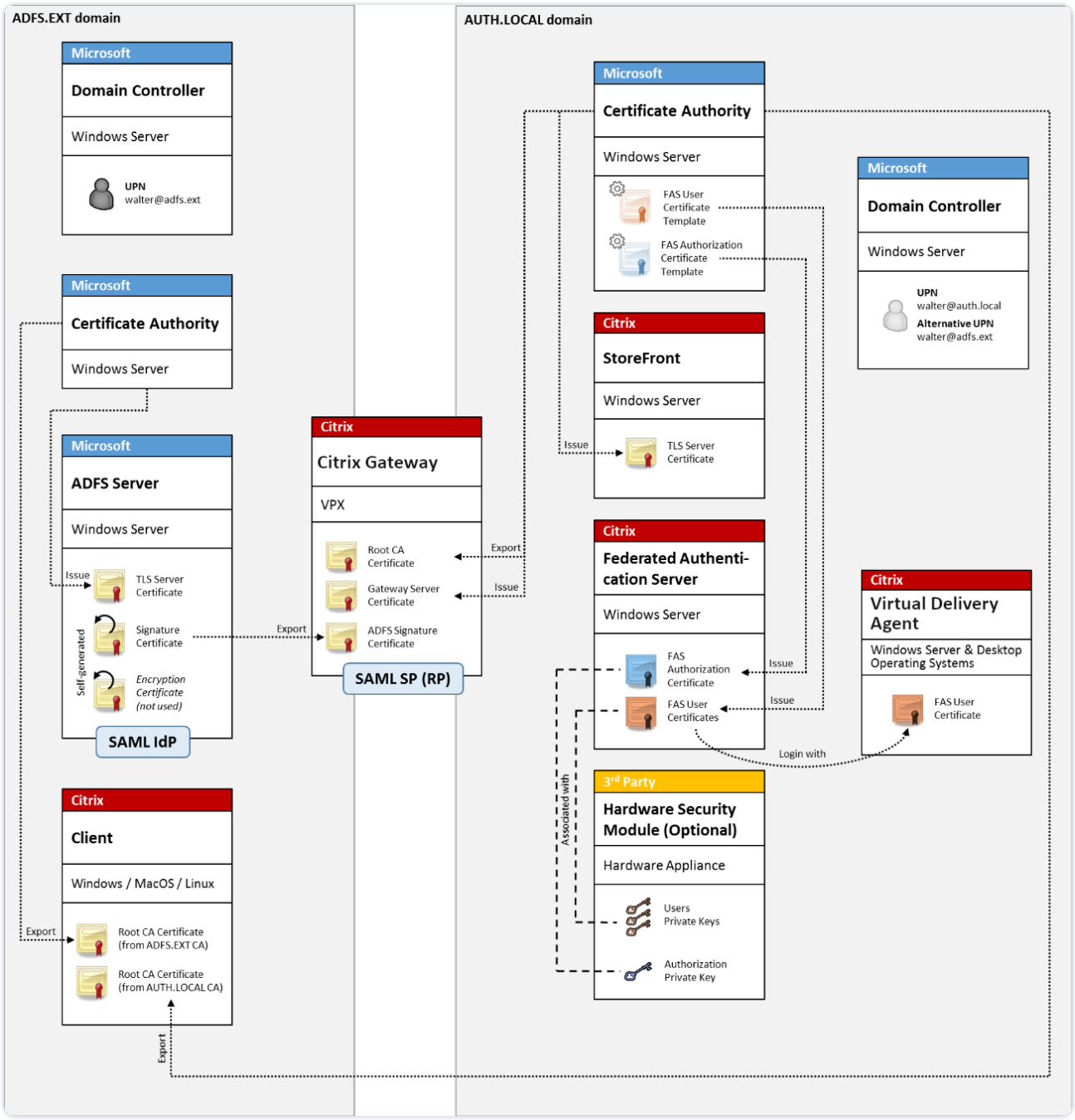
関連情報:

- ADFS展開の記事には詳細が含まれています。
- インストールと構成の記事は、FASのインストールと構成方法について説明しています。
- このアーティクルの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環境の「シャドウアカウント」に自動的にマッピングします。

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



関連情報:

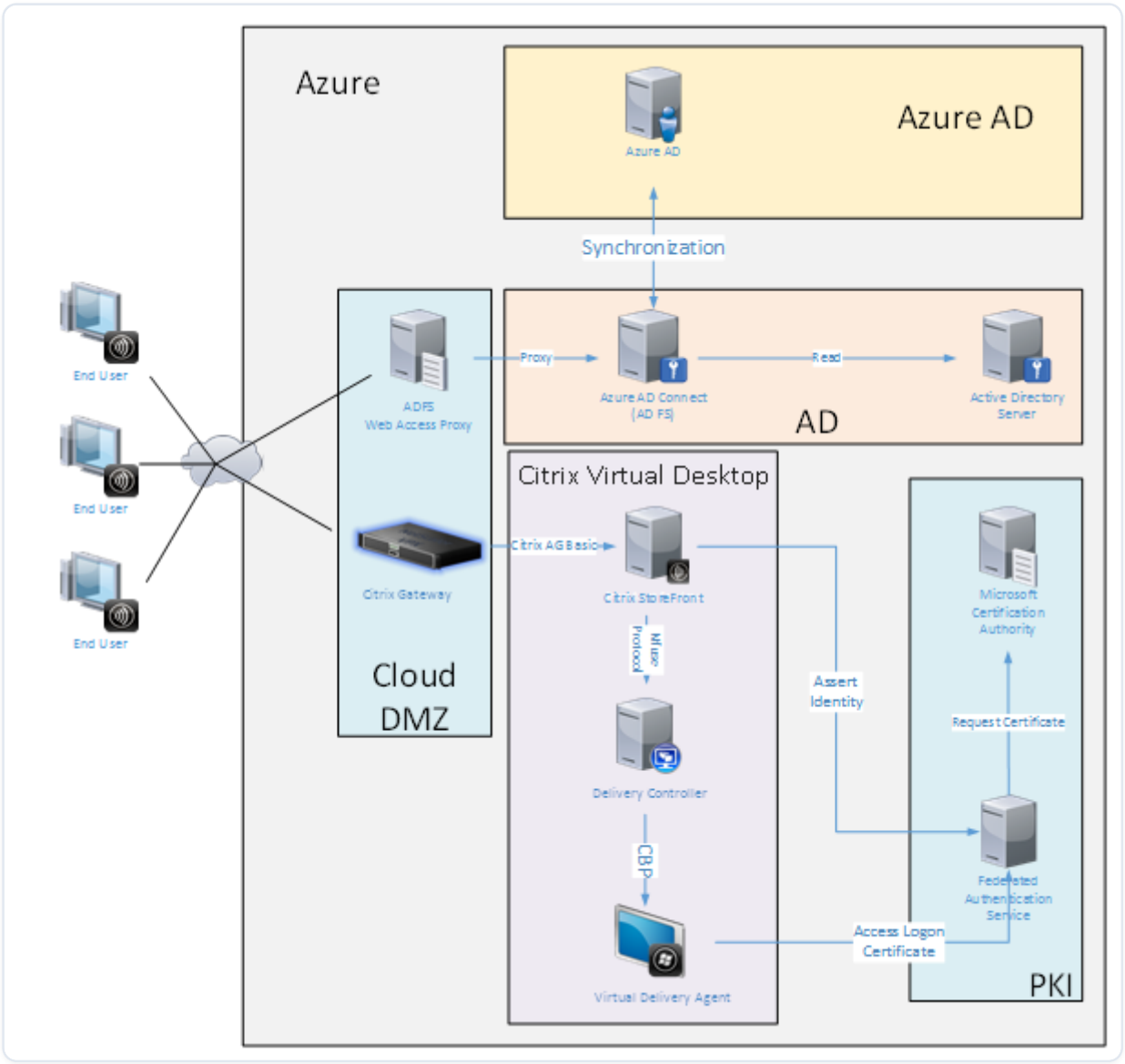
- (/ja-jp/federated-authentication-service/2305/install-configure.html)の記事では、FASのインストール方法と構成方法について説明しています。

ウィンドウズ 10 アジュール AD ジョイン

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

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

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

この展開のインフラストラクチャは、IPアドレスが利用可能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。この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/2305/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。

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

- (/ja-jp/federated-authentication-service/2305/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

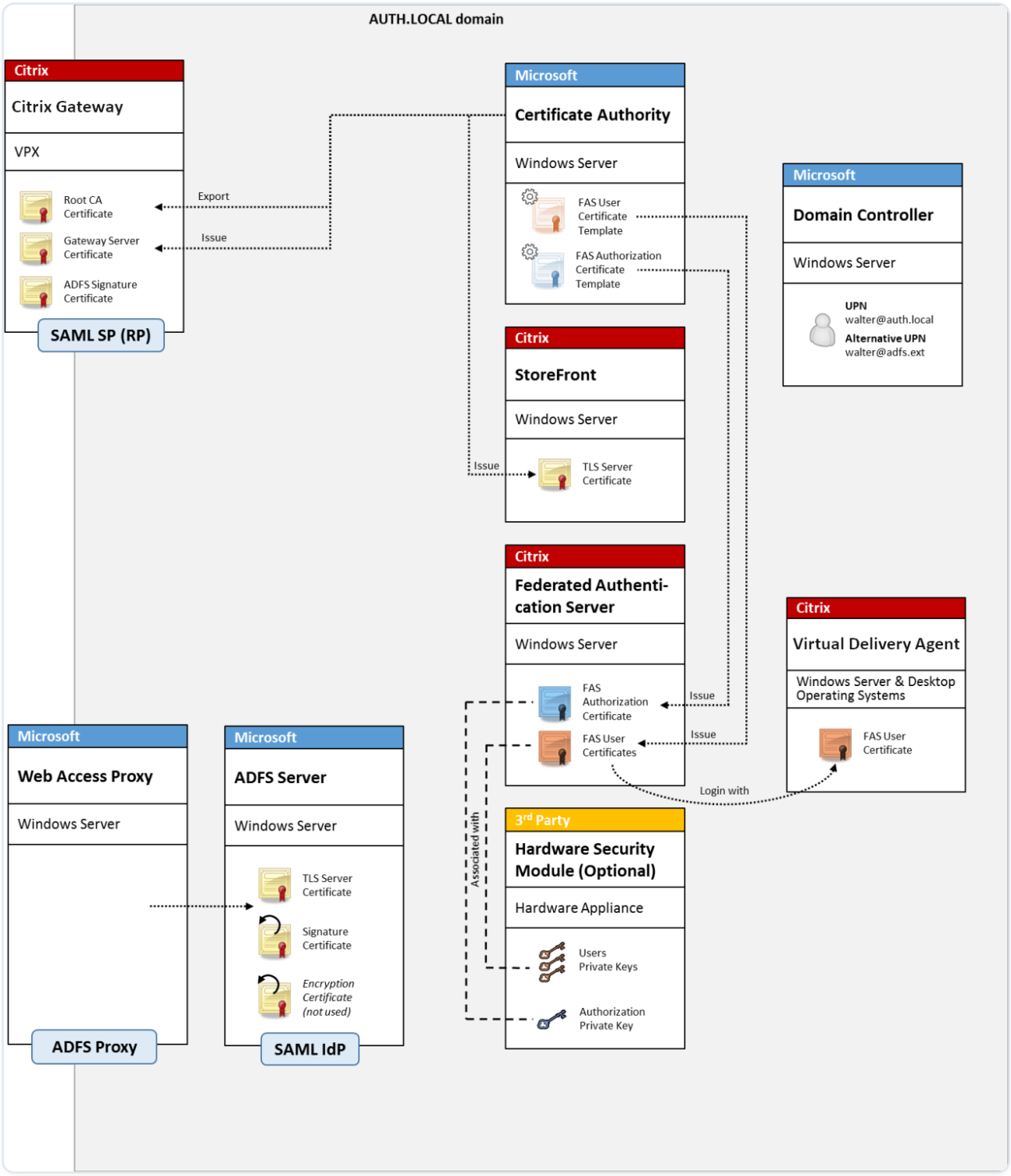
このドキュメントでは、Citrix環境をMicrosoft ADFSと統合する方法について説明します。

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。

フェデレーテッド認証サービス (FAS) は、Citrix Gateway および Citrix StoreFront™ を ADFS ログオンシステムと統合することも可能にし、従業員の潜在的な混乱を軽減します。

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

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



注：

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

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

SAMLの概要

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

リダイレクトURL

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

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

識別子

EntityId は、Citrix Gateway が ADFS への POST データに含める一意の識別子です。これにより、ADFS はユーザーがどのサービスにログオンしようとしているかを認識し、必要に応じて異なる認証ポリシーを適用します。発行された場合、SAML 認証 XML は EntityId によって識別されるサービスへのログオンにのみ適しています。

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

戻りアドレス

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

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

署名証明書

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

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

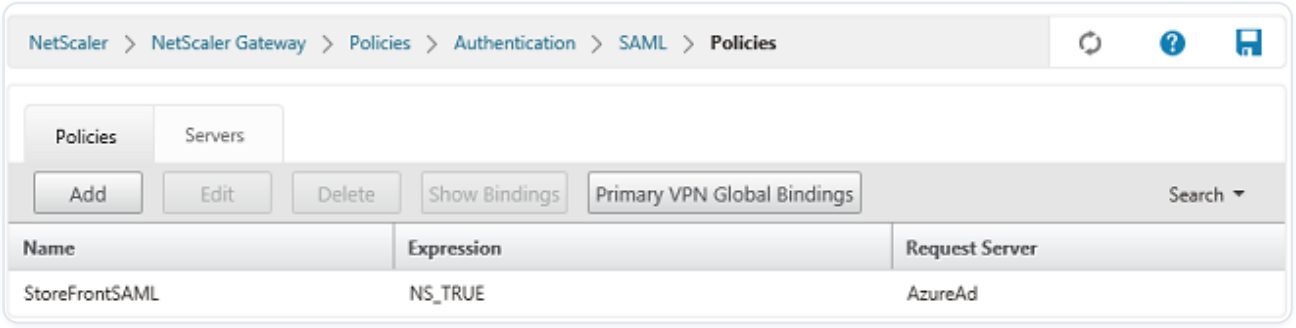
シングルサインアウト URL

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 が時折ポーリングして、SAML 認証 XML ブロブが現在ログオン中のセッションをまだ表しているかを確認するための 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://` 形式の `https://adfs.mycompany.com/adfs/logout` アドレスです。(シングルログオン URL と同じである場合もあります。)

構成

セクション Citrix Gateway の展開 では、標準の LDAP 認証オプションを処理するように Citrix Gateway を設定する方法について説明しています。それが正常に完了した後、SAML 認証を許可する新しい認証ポリシーを Citrix Gateway 上に作成できます。これは、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、その見返りとして ADFS 署名付き SAML 認証トークンを受け入れます。

ローカライズされた画像(/en-us/federated-authentication-service/2305/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の展開は、展開アーキテクチャの記事にまとめられています。
- 「ハウツー」記事は、高度な構成の記事で紹介されています。

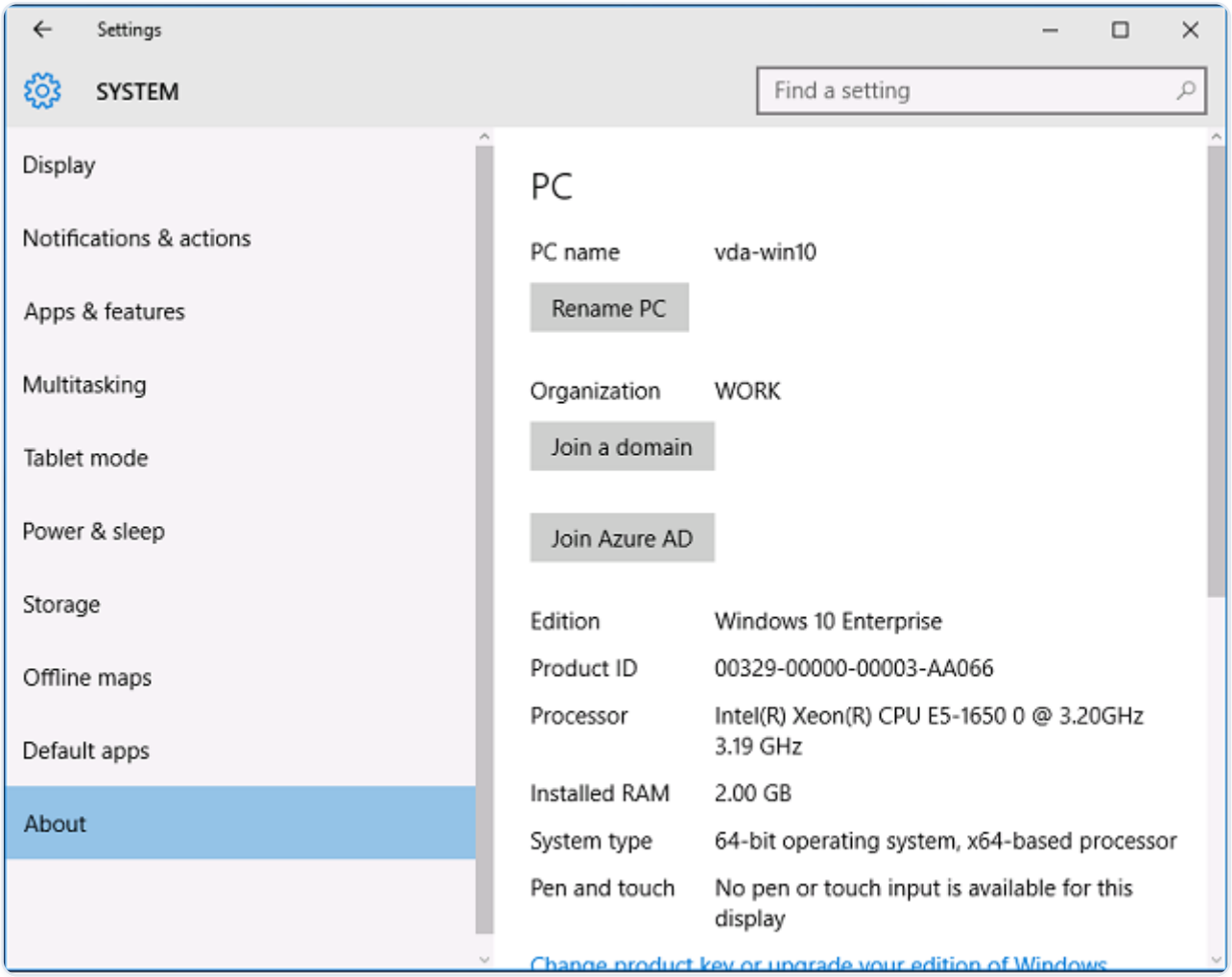
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure AD 統合

はじめに

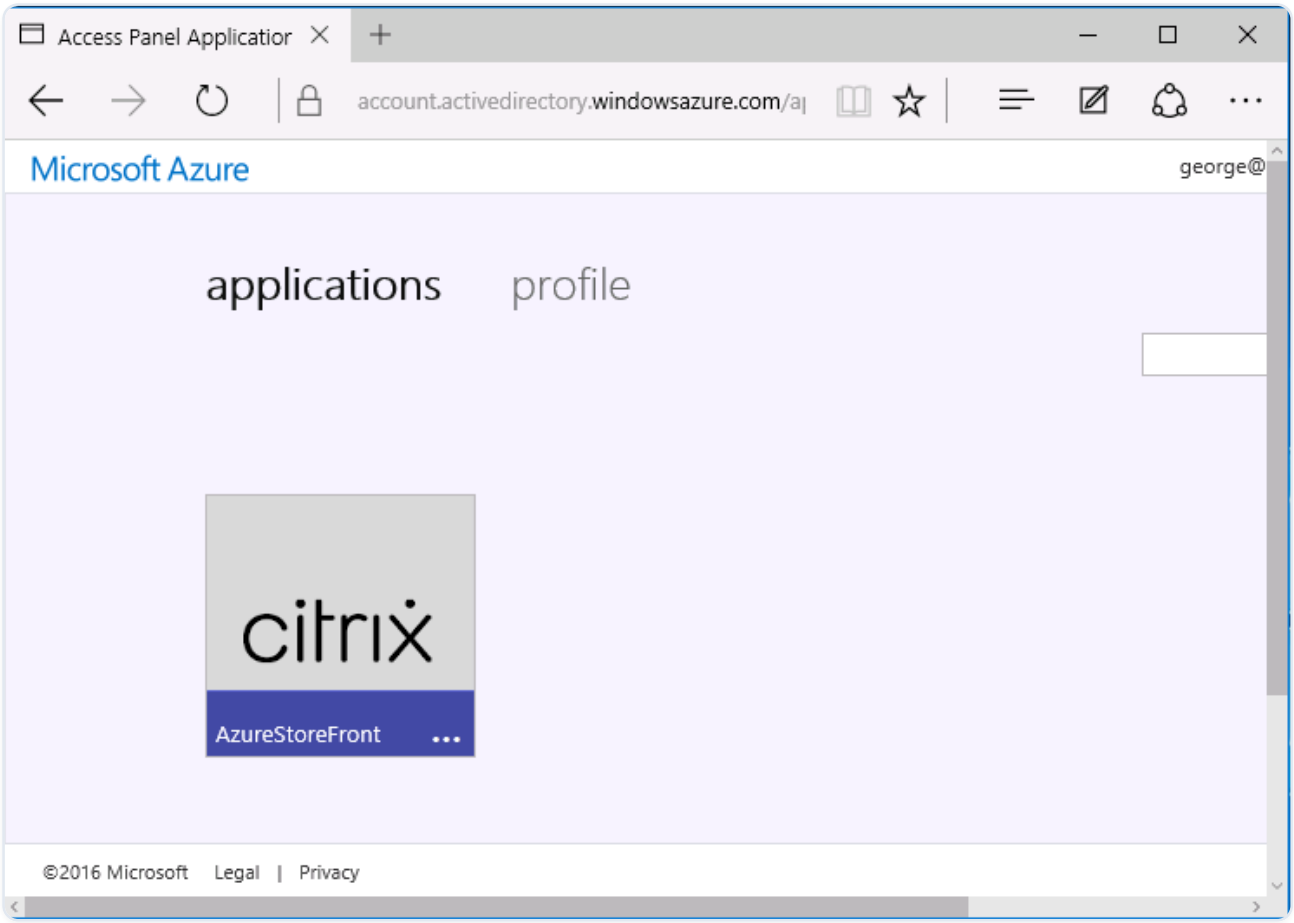
このドキュメントでは、Citrix環境をWindows 10のAzure AD機能と統合する方法について説明します。Windows 10ではAzure ADが導入されました。これは、管理とシングルサインオンのために、ローミング中のラップトップをインターネット経由で企業ドメインに参加させることができる新しいドメイン参加モデルです。

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ています。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。これは、Office 365などの他のAzureアプリケーションと同様です。

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

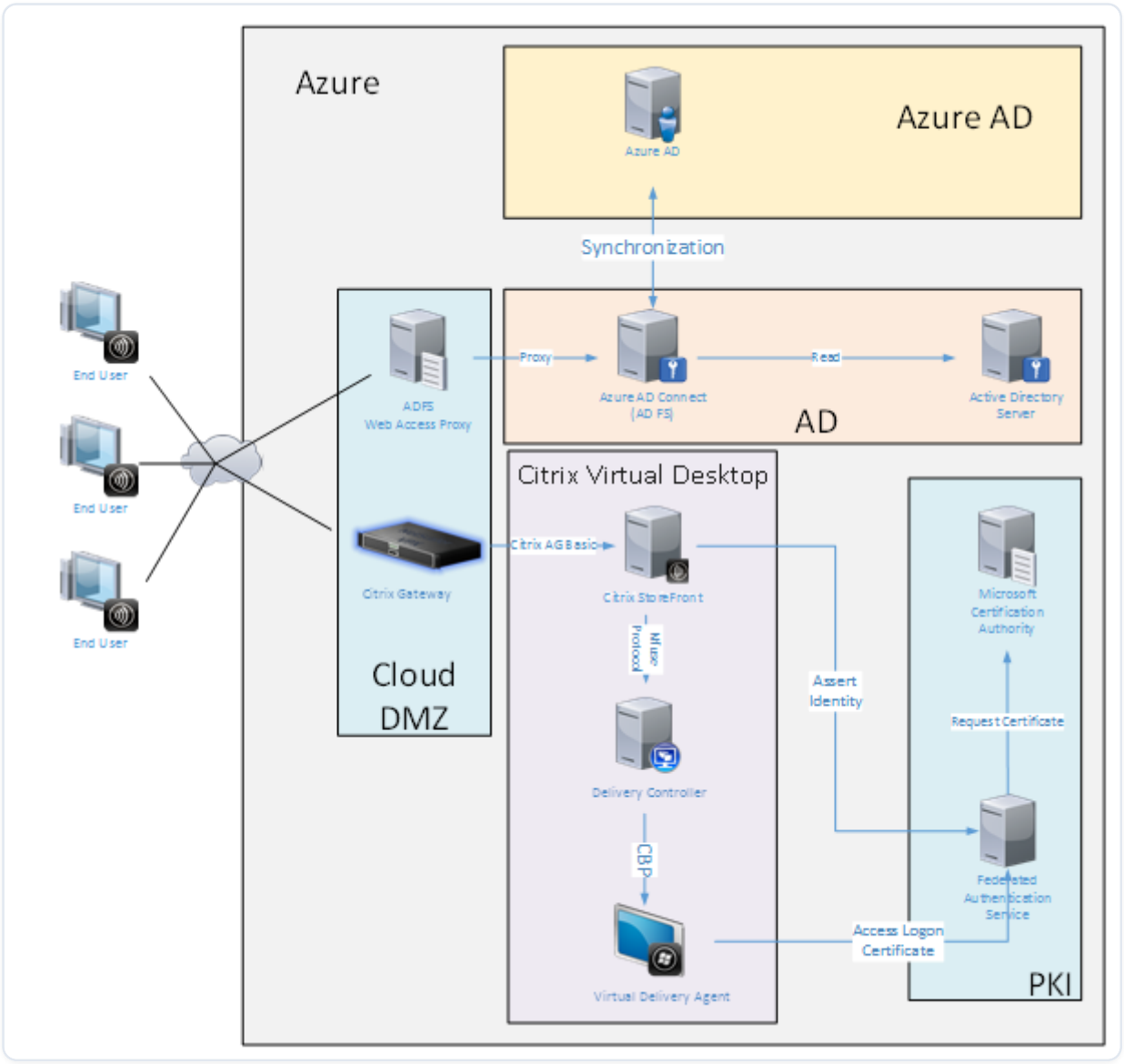


アーキテクチャ

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

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

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



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

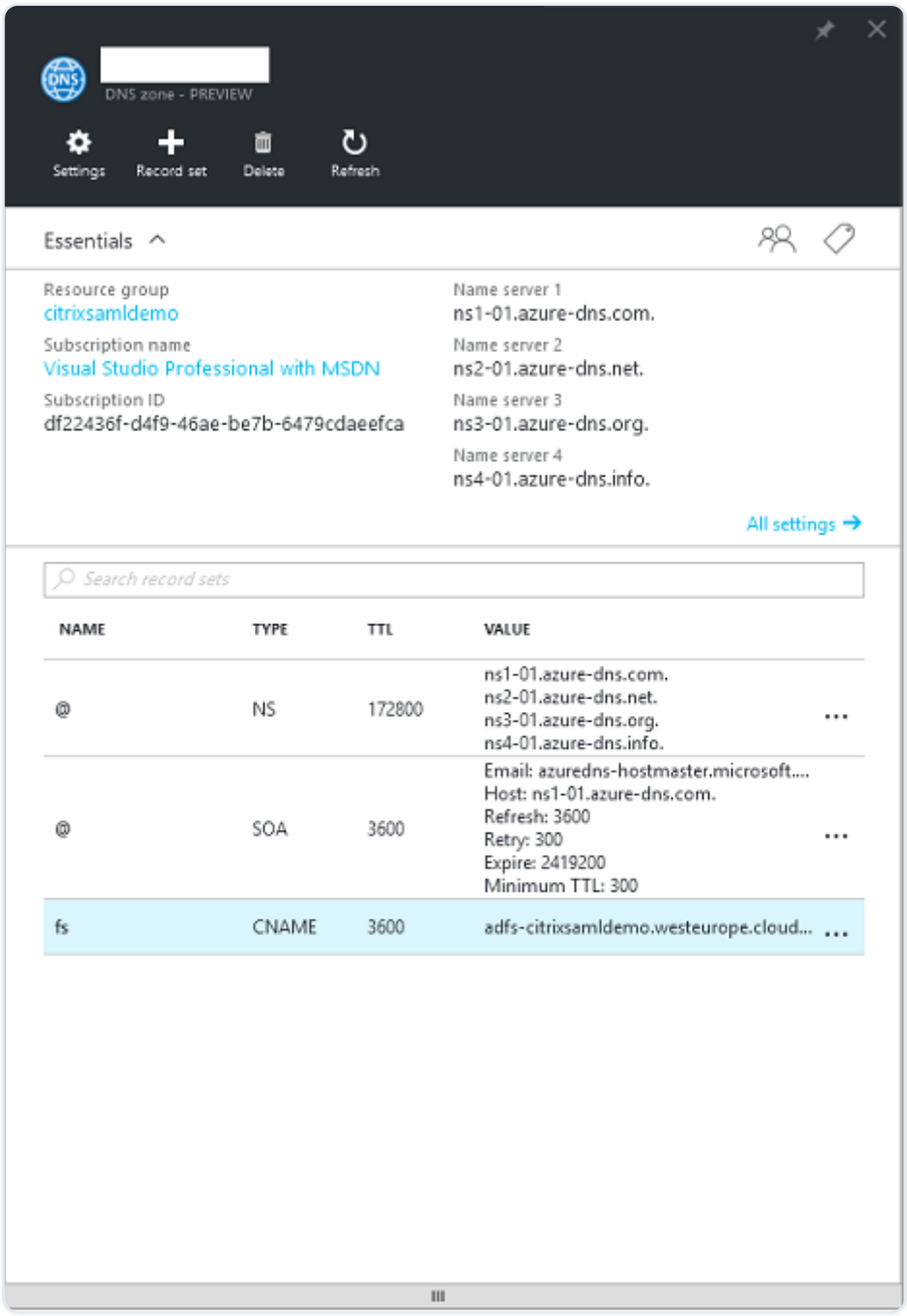
ユーザーが従来のアプリケーションを起動すると、Citrix Virtual Apps and Desktops™公開アプリケーションを使用してアクセスされます。さまざまな種類のアプリケーションは、Microsoft Edgeのシングルサインオン機能を使用して、ユーザーの**Azure Applications**ページを通じて照合されます。Microsoftは、Azureアプリケーションを列挙して起動できるAndroidおよびiOSアプリも提供しています。

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

DNSゾーンの作成

Azure ADでは、管理者がパブリックDNSアドレスを登録し、ドメイン名サフィックスの委任ゾーンを制御している必要があります。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`）。

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

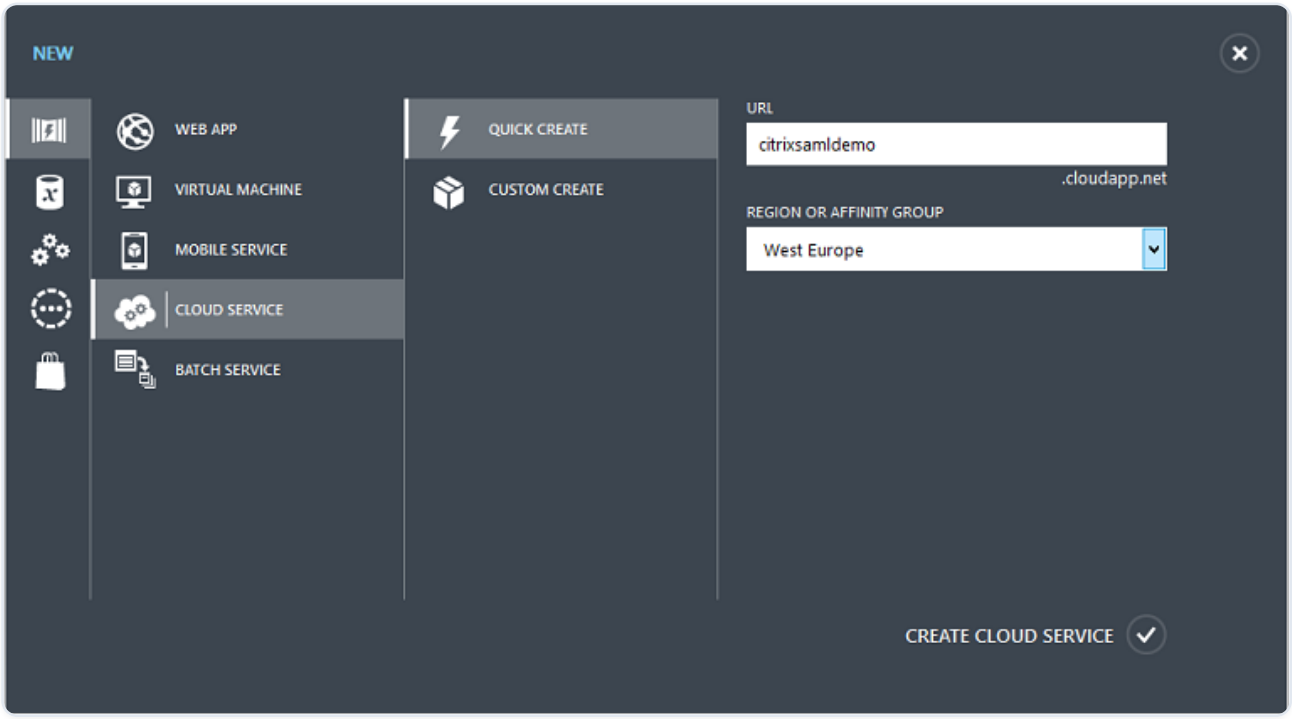
Azureで実行されているVMへの参照を追加する場合、VMのAzure管理DNSレコードへのCNAMEポインタを使用するのが最も簡単です。VMのIPアドレスが変更されても、DNSゾーンファイルを手動で更新する必要はありません。

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

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

クラウドサービスの作成

この例では、Azureで実行されているADFSサーバーを含むAD環境を備えた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。

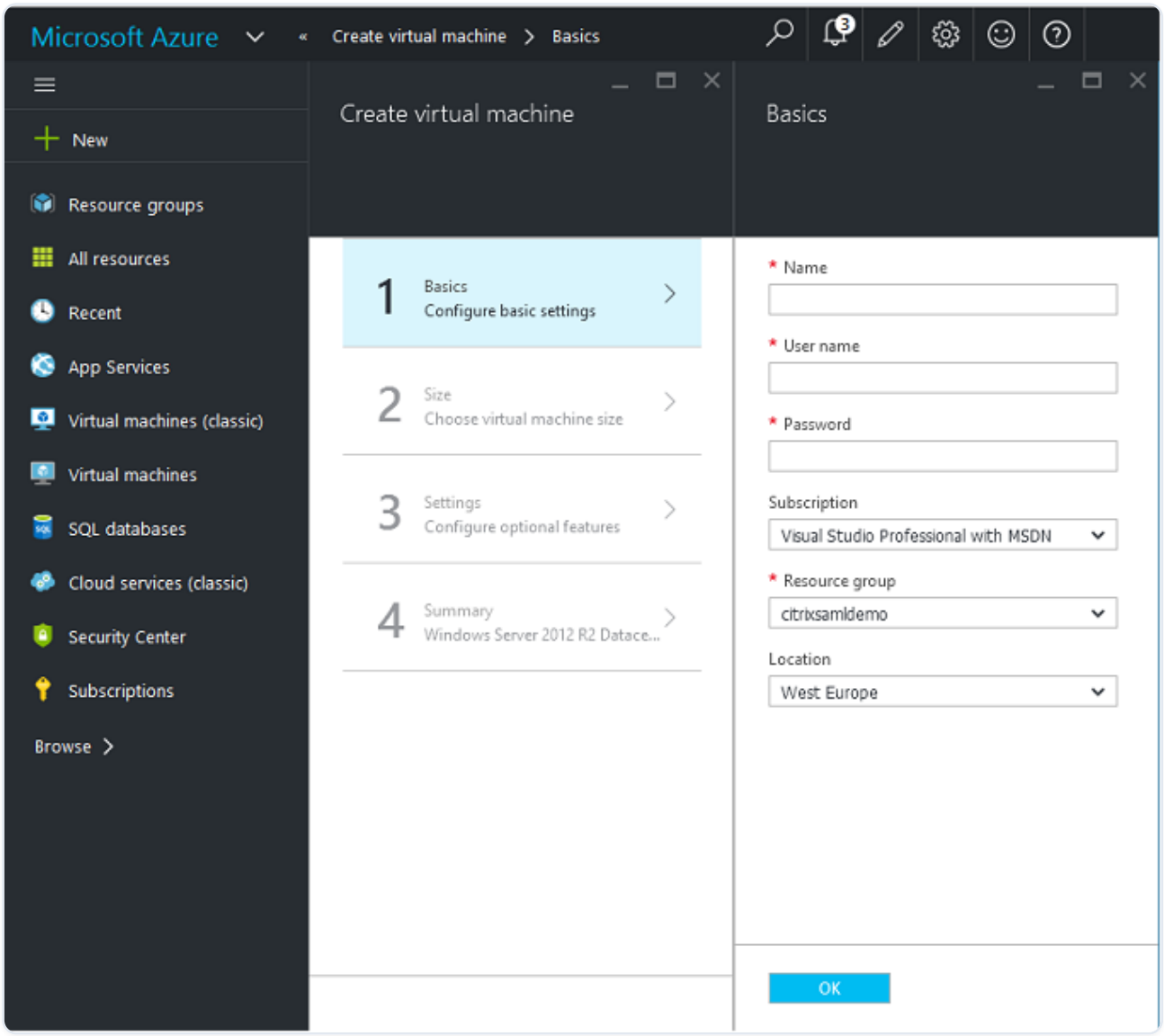


Windows仮想マシンの作成

クラウドサービスで実行される5つのWindows VMを作成します。

- ドメインコントローラー (domaincontrol)
- アジュール コネクト エーディーエフエス サーバー (adfs)
- ADFS Webアクセスプロキシ (Web Application Proxy、ドメイン参加なし)
- シトリックス バーチャル アプリケーションズ アンド デスクトップ 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)

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



ドメインコントローラー

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

ADFSコントローラーとWebアプリケーションプロキシサーバー

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

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

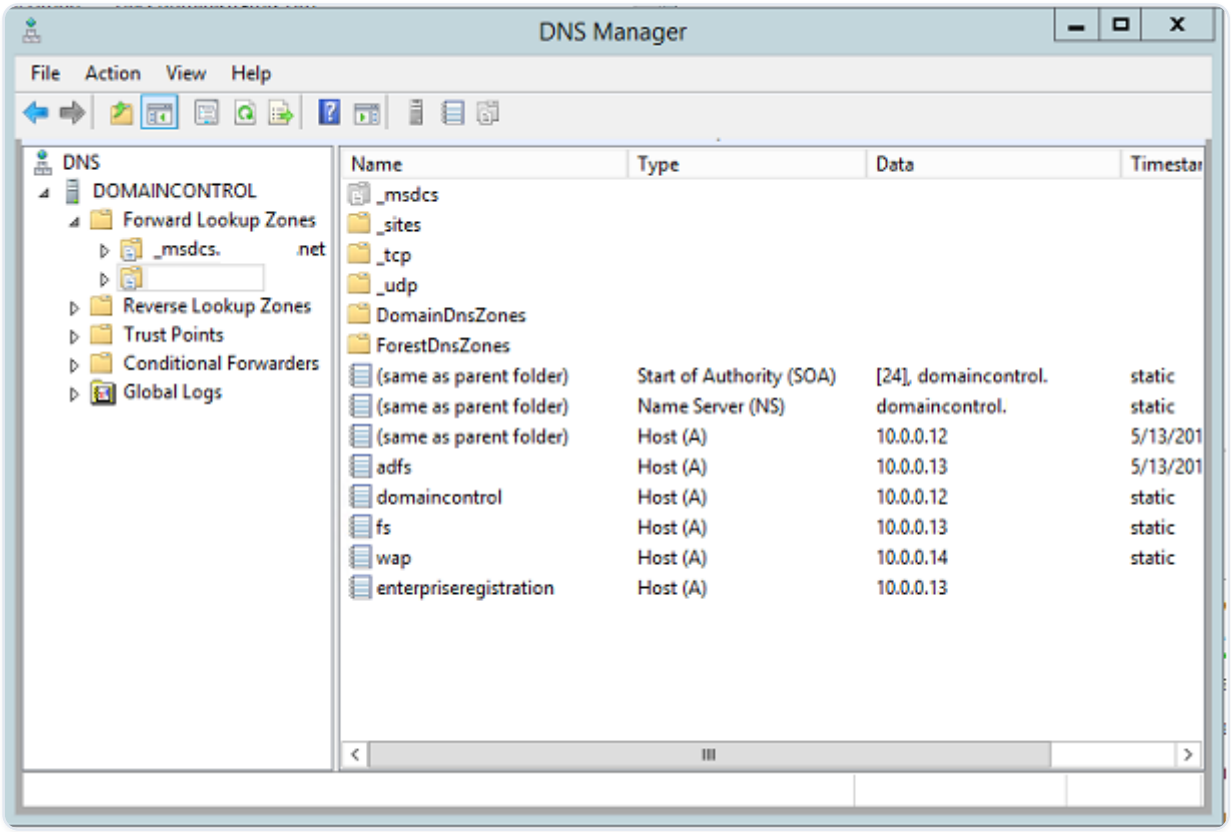
- AzureAD Connectツールからの PSリモート処理をファイアウォール経由で許可するために、これらのサーバーで**Enable-PSRemoting –Force**コマンドレットを実行します。

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

- 残りの2台のcitrixsamldemoに参加している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。

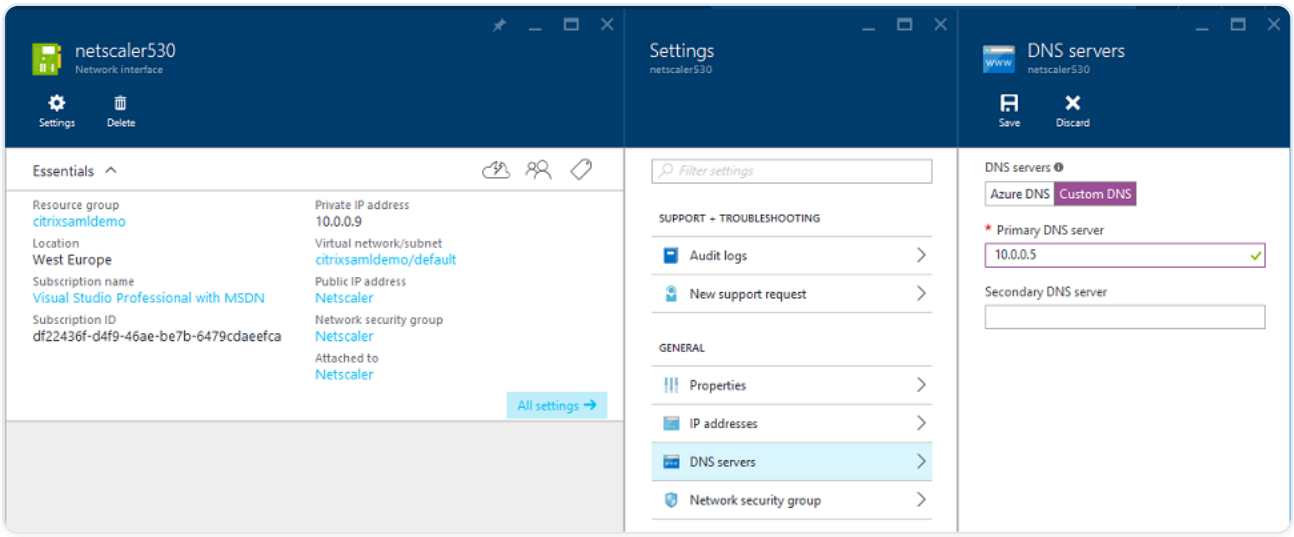


静的レコードを追加します:

- 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の GUI を介して行うことができます。

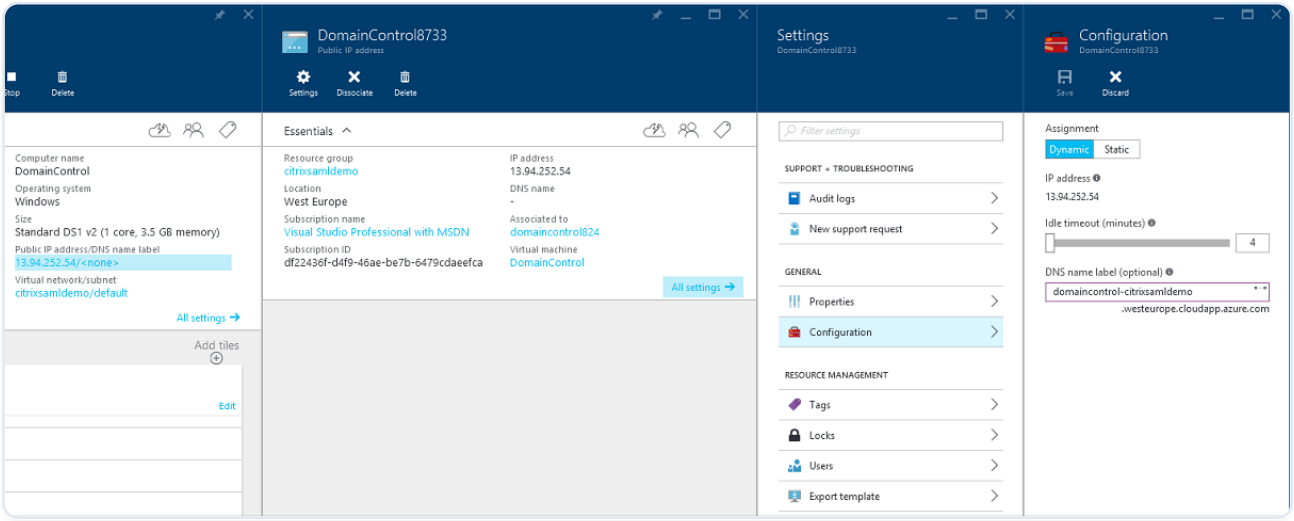
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

外部 DNS アドレスを構成する

VM 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。



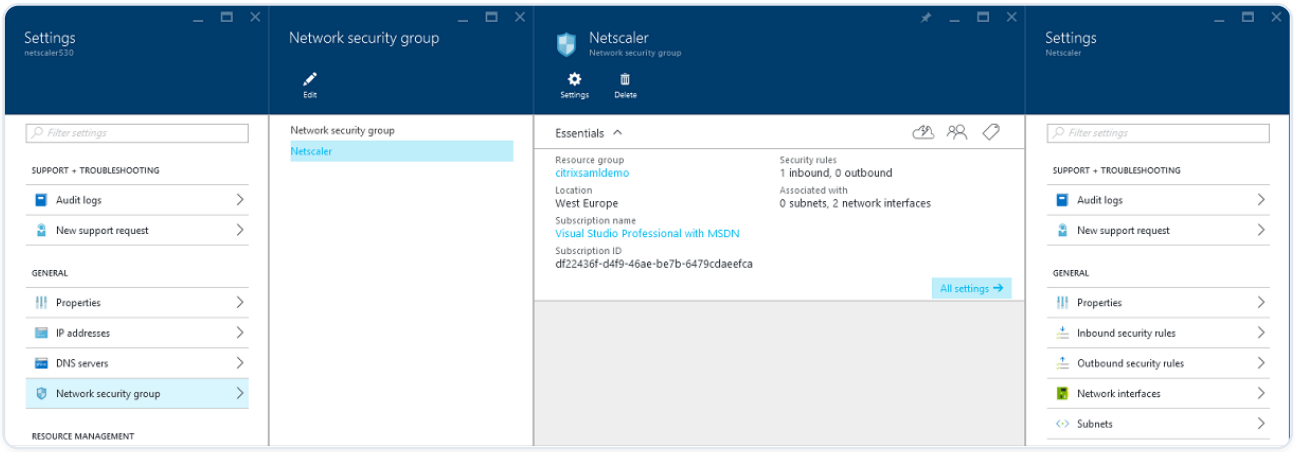
この例では、domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com の DNS アドレスをドメインコントローラーに割り当てます。

リモート構成が完了すると、Web アプリケーションプロキシと Citrix Gateway VM のみがパブリック IP アドレスを有効にする必要があることに注意してください。(構成中は、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)。

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

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 アクセスのファイアウォールルールを管理します。デフォルトでは、すべての VM が RDP アクセスを許可します。Citrix Gateway および Web アプリケーションプロキシサーバーも、ポート 443 で TLS を許可する必要があります。



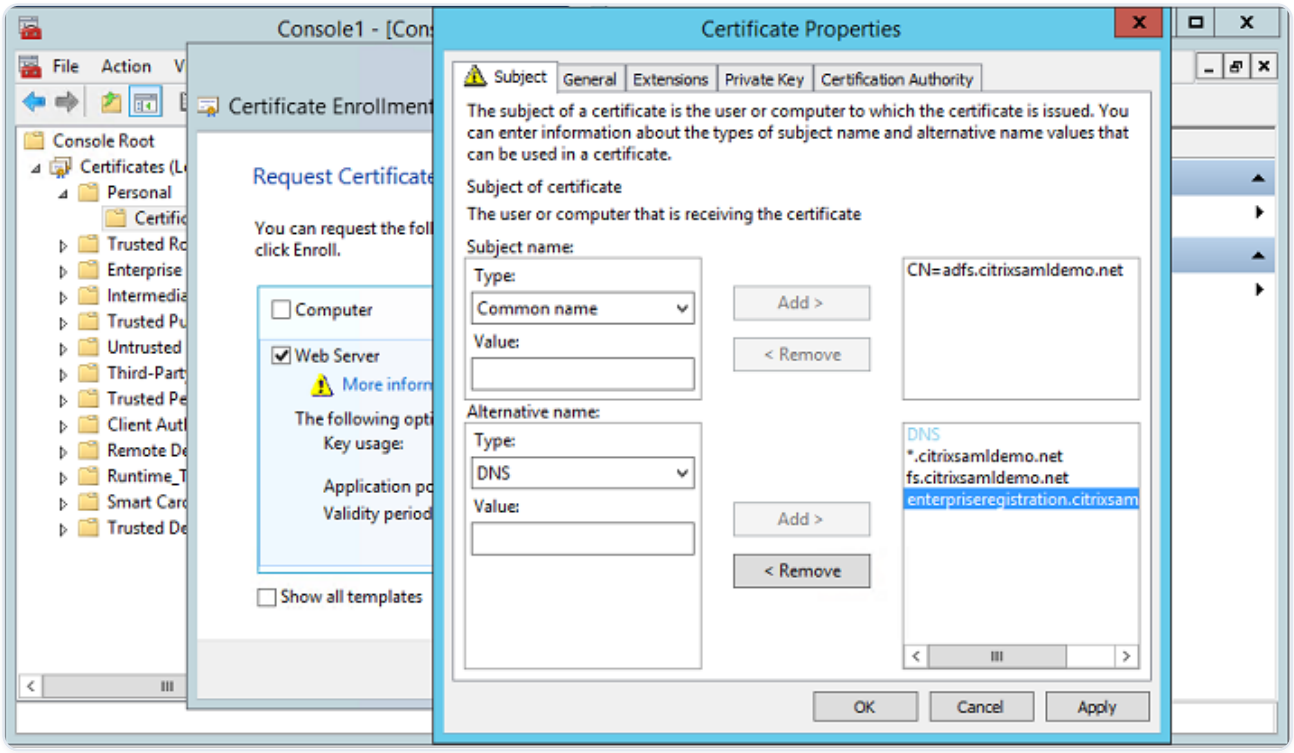
ADFS 証明書を作成する

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

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



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。

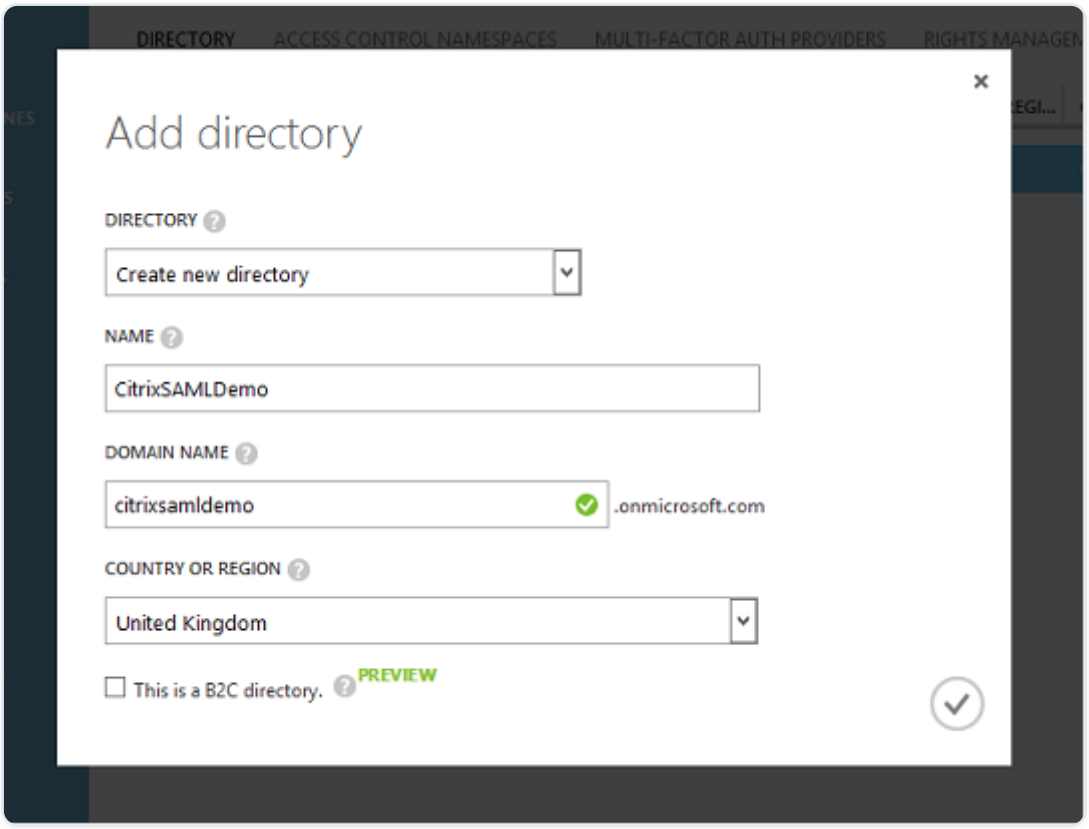
Azure ADをセットアップする

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

新しいディレクトリを作成する

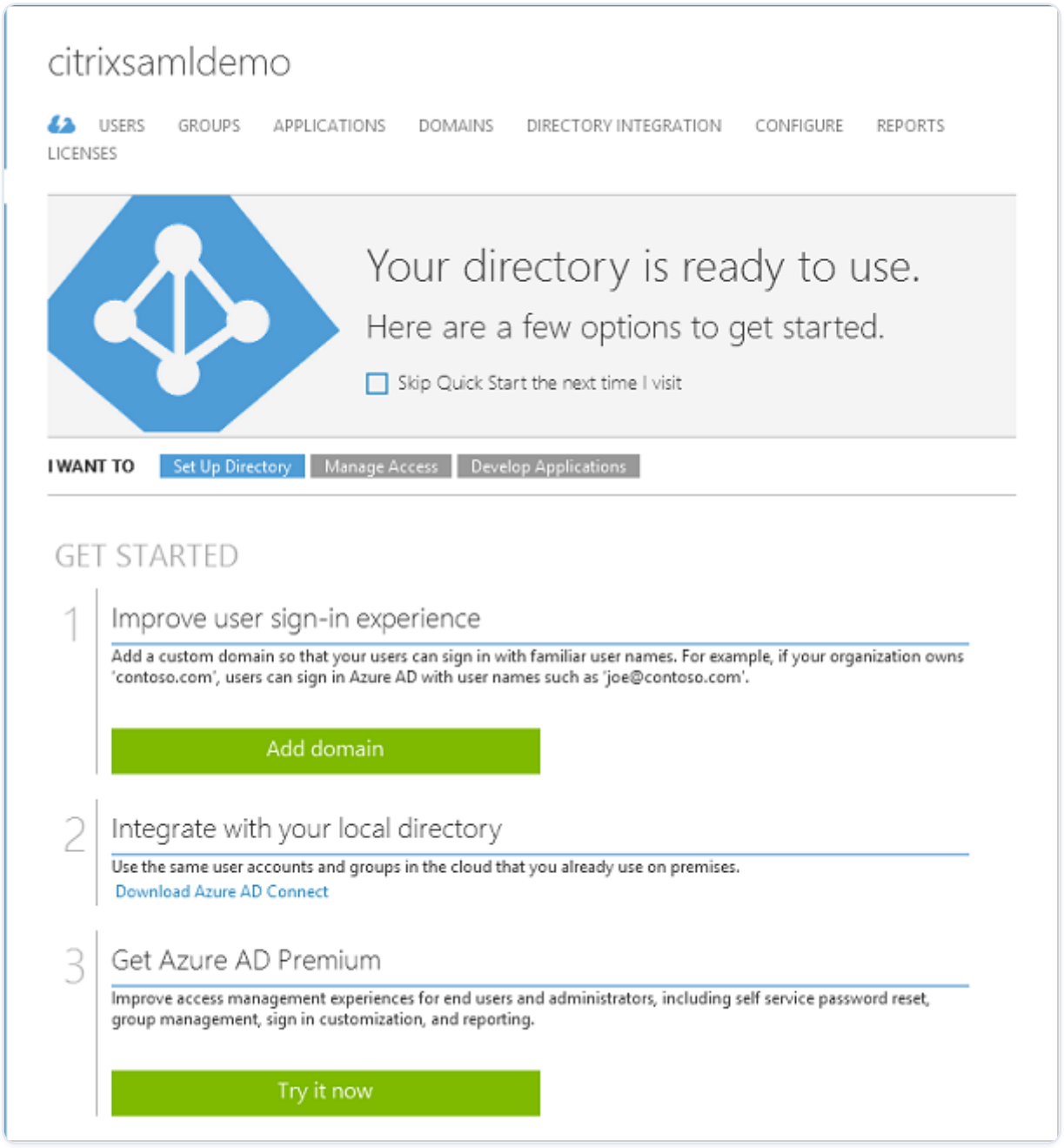
クラシックAzureポータルにログオンし、新しいディレクトリを作成します。

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



完了すると、概要ページが表示されます。

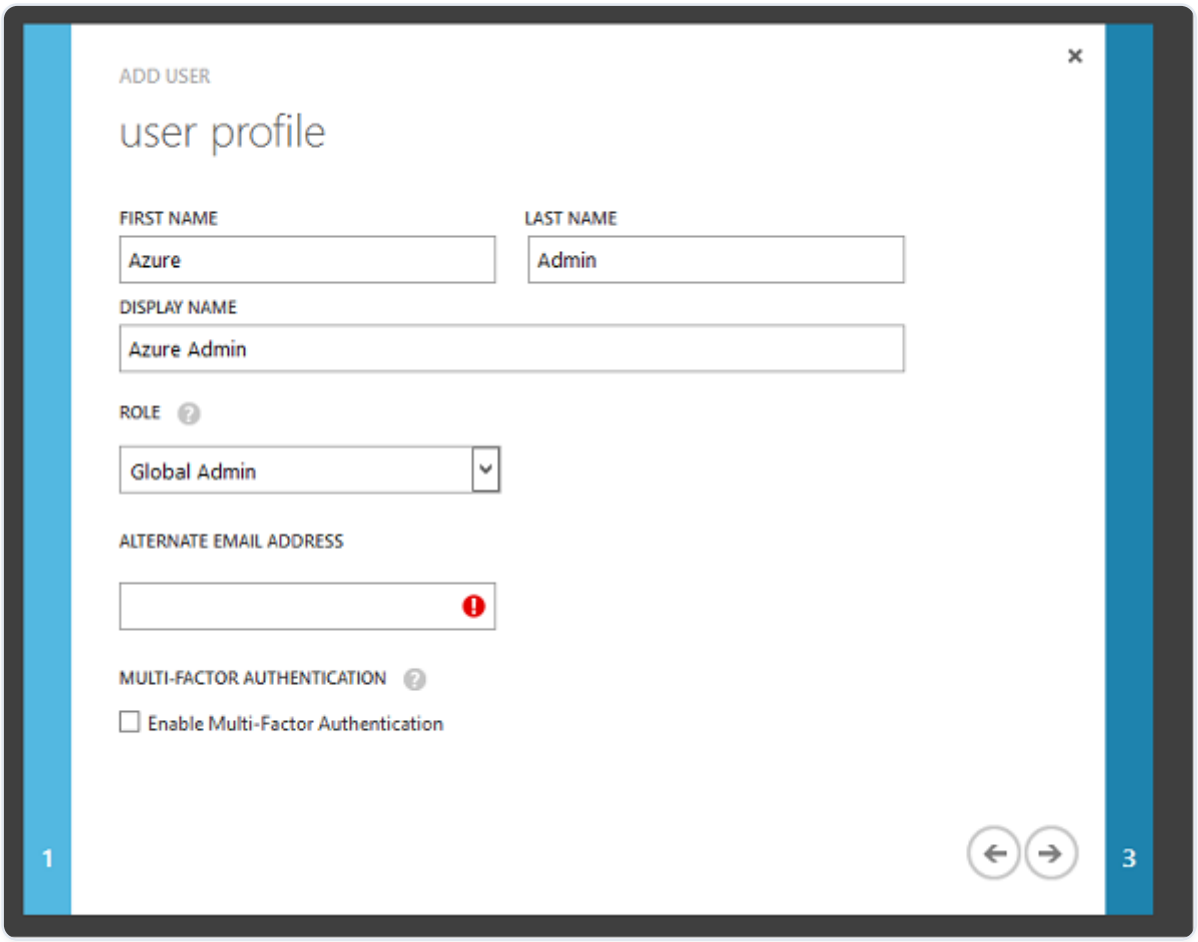
© 1997–2026 Citrix Systems, Inc. All rights reserved.



グローバル管理者ユーザー (AzureAdmin) を作成する

Azure でグローバル管理者 (この例では `AzureAdmin@citrixsamldemo.onmicrosoft.com`) を作成し、新しいアカウントでログオンしてパスワードを設定します。

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



ドメインを Azure AD に登録する

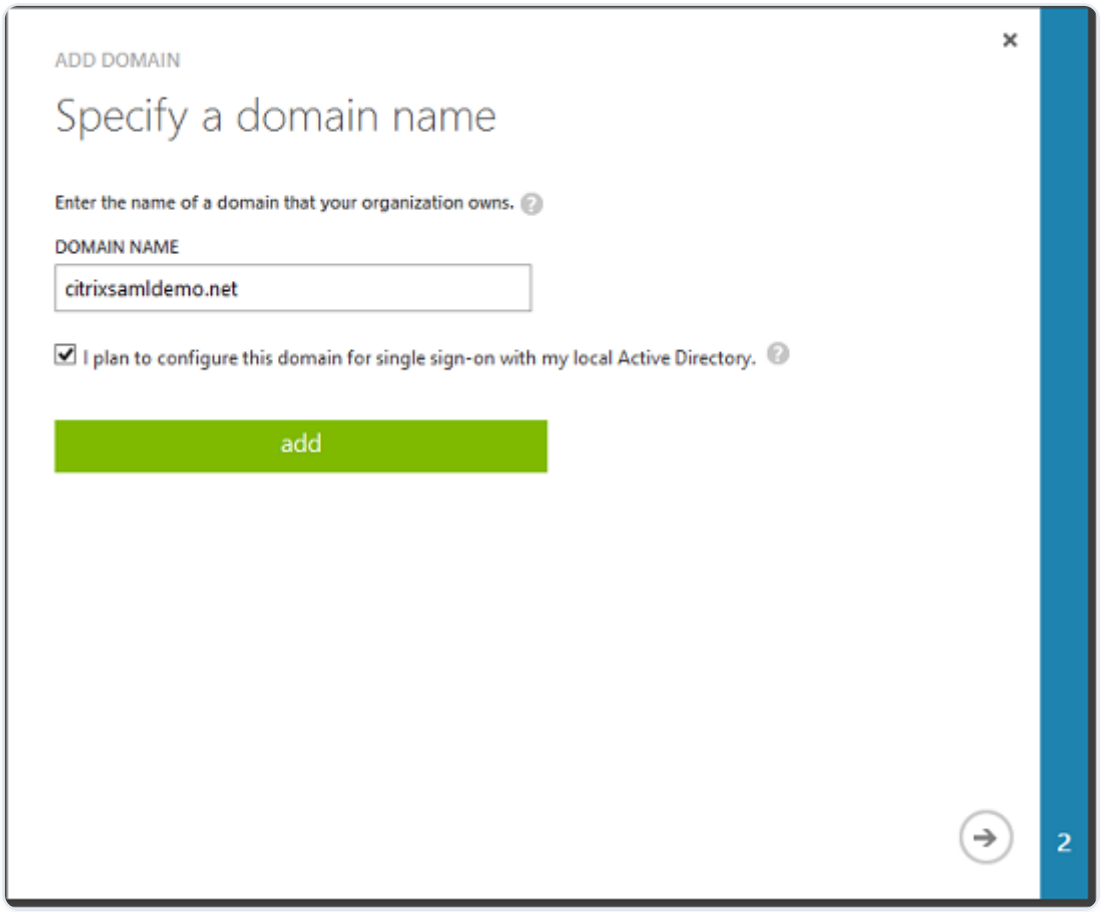
デフォルトでは、ユーザーは `<user.name>@<company>.onmicrosoft.com` の形式のメールアドレスで識別されます。

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

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

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

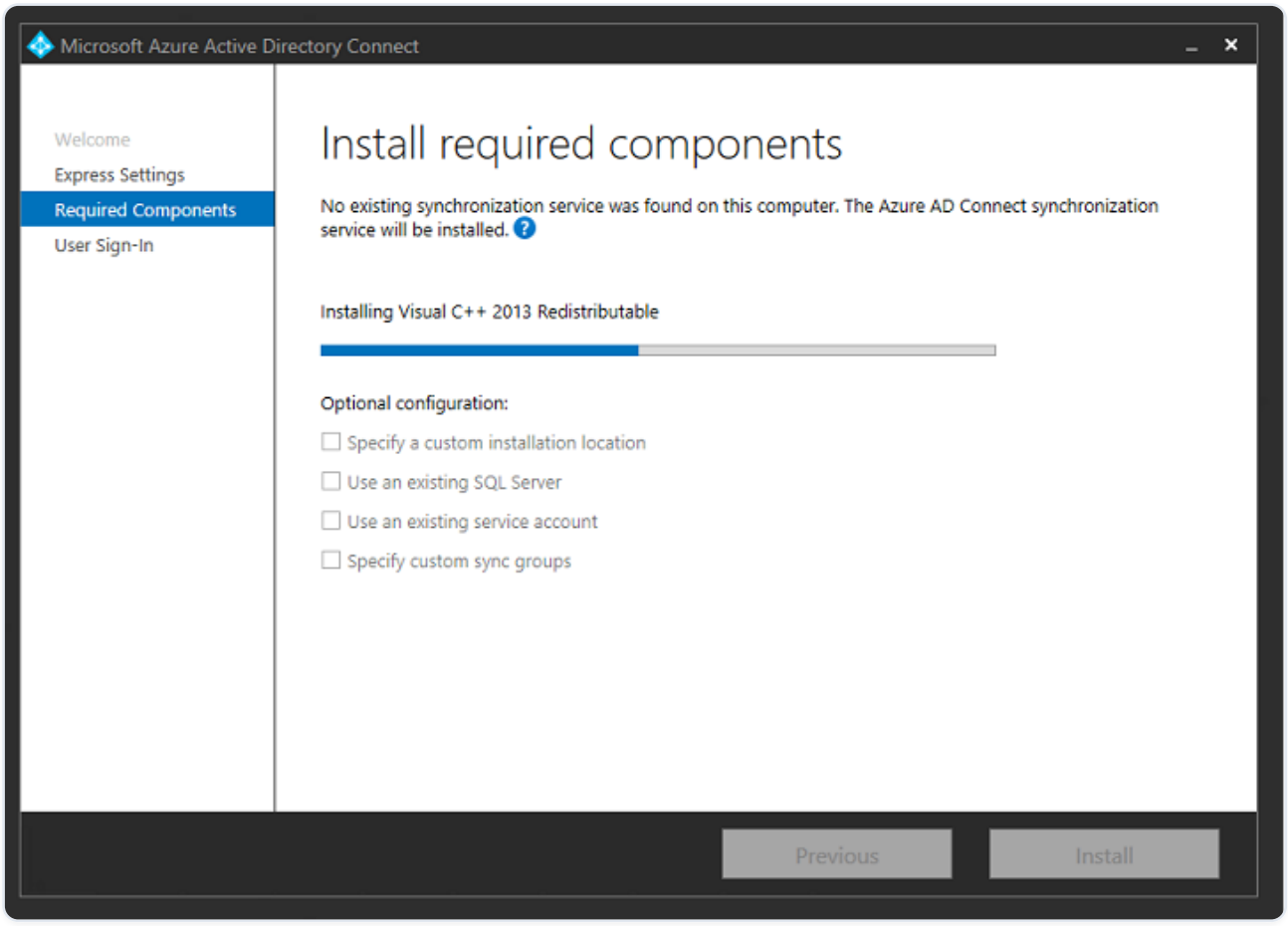
© 1997–2026 Citrix Systems, Inc. All rights reserved.



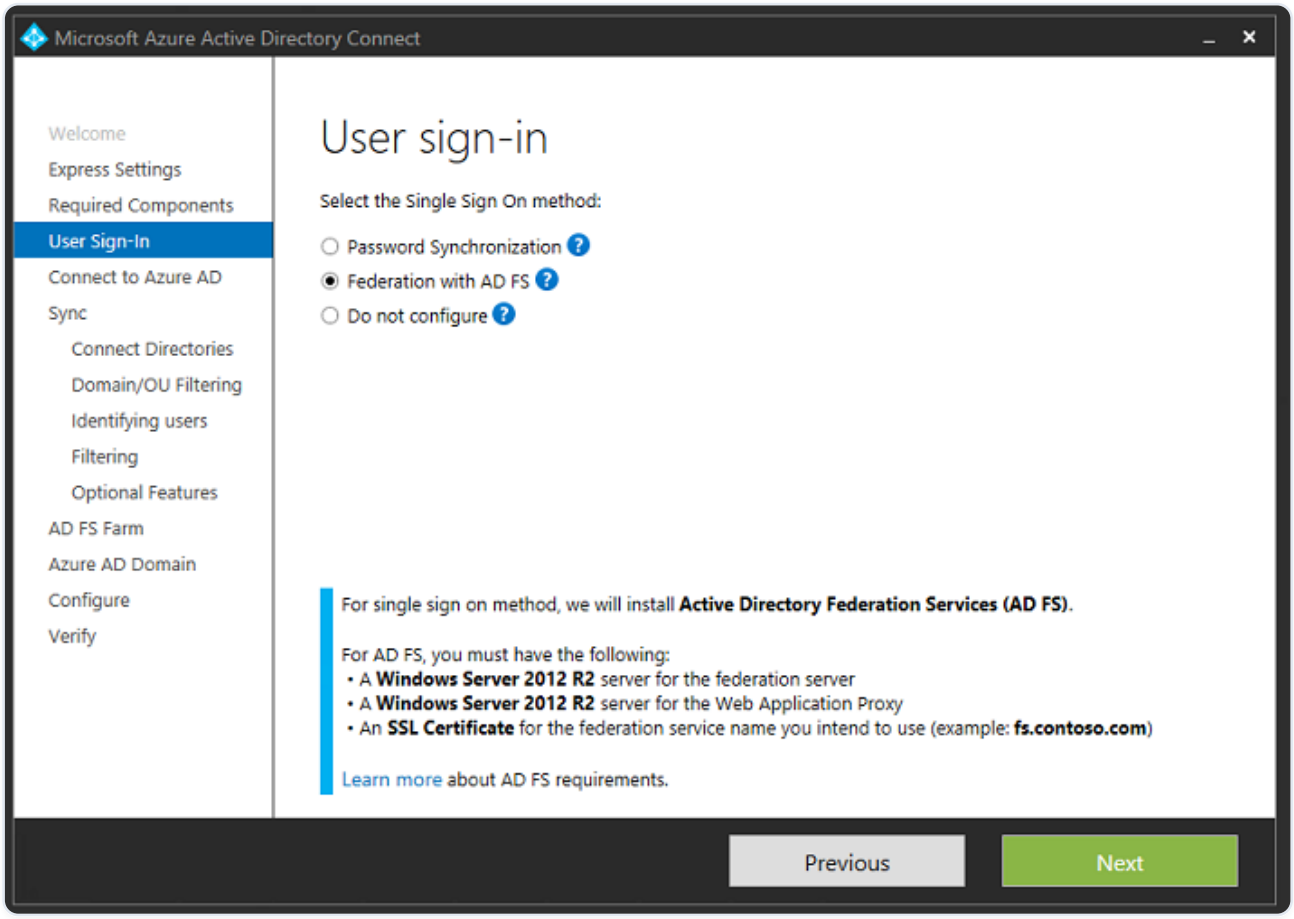
Azure AD Connect をインストールする

Azure AD 構成 GUI のステップ 2 は、Azure AD Connect の Microsoft ダウンロードページにリダイレクトされます。これを ADFS VM にインストールします。ADFS オプション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。

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

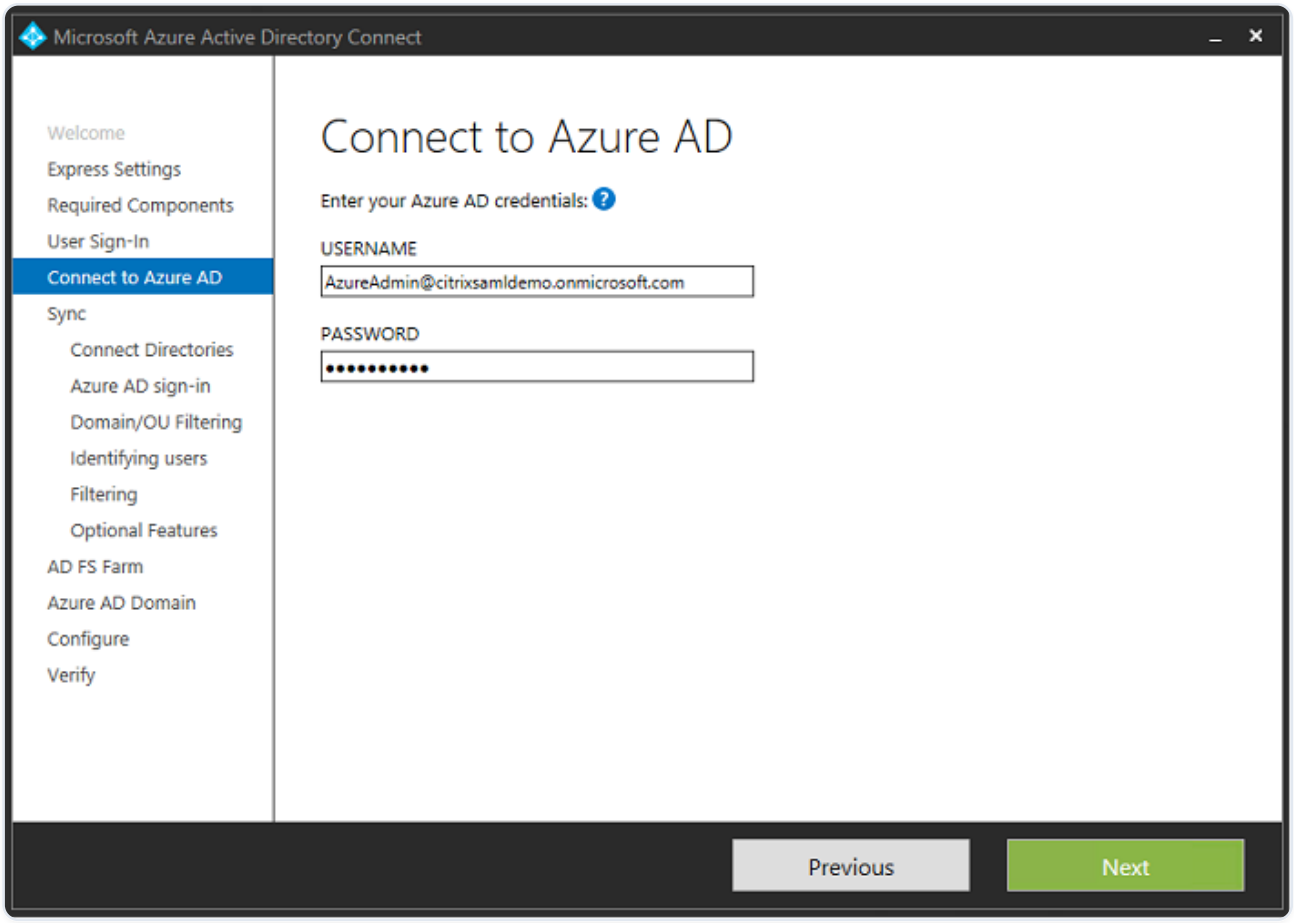


Federation with AD FS シングルサインオンオプションを選択します。



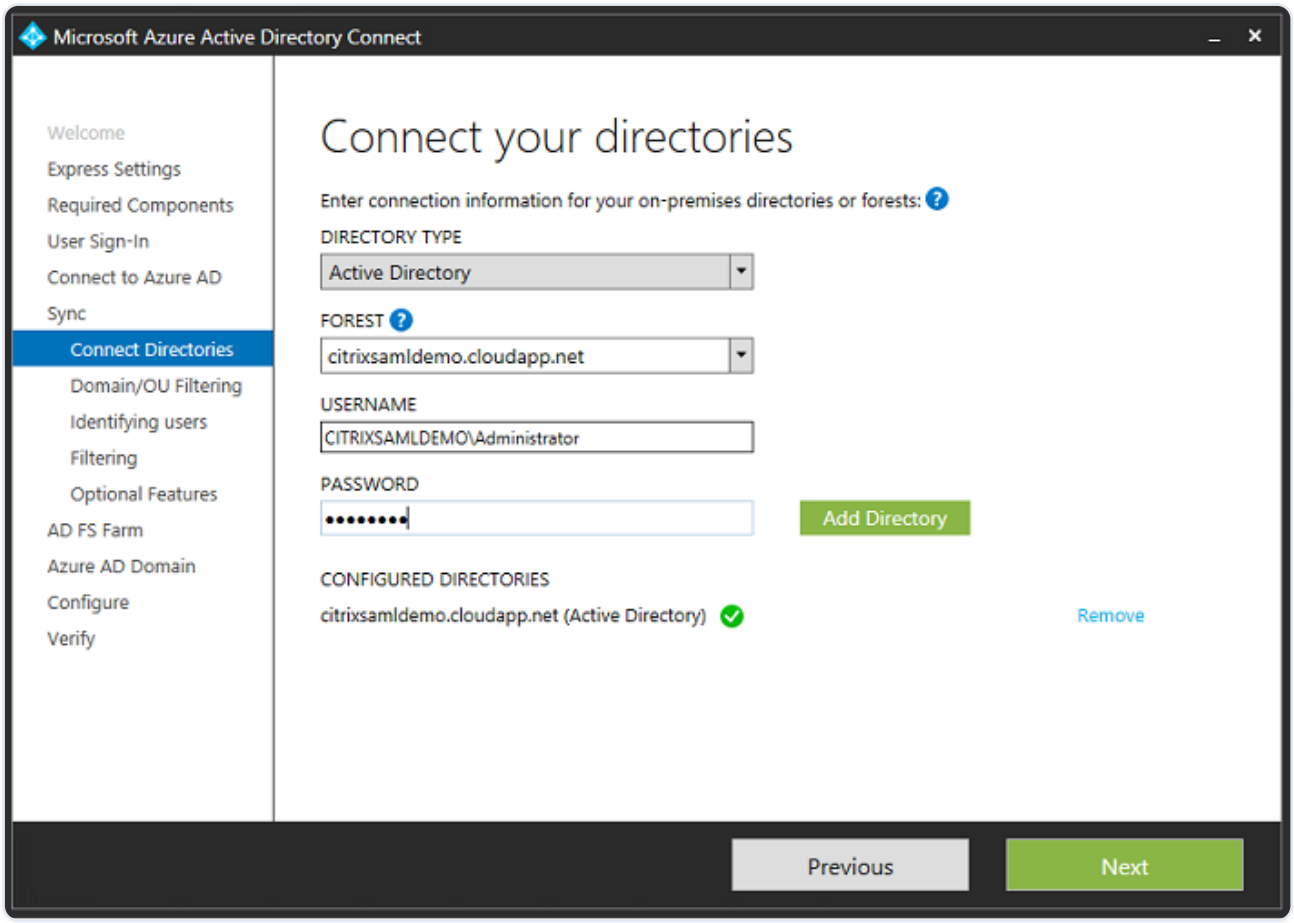
© 1997–2026 Citrix Systems, Inc. All rights reserved.

以前に作成した管理者アカウントでAzureに接続します。

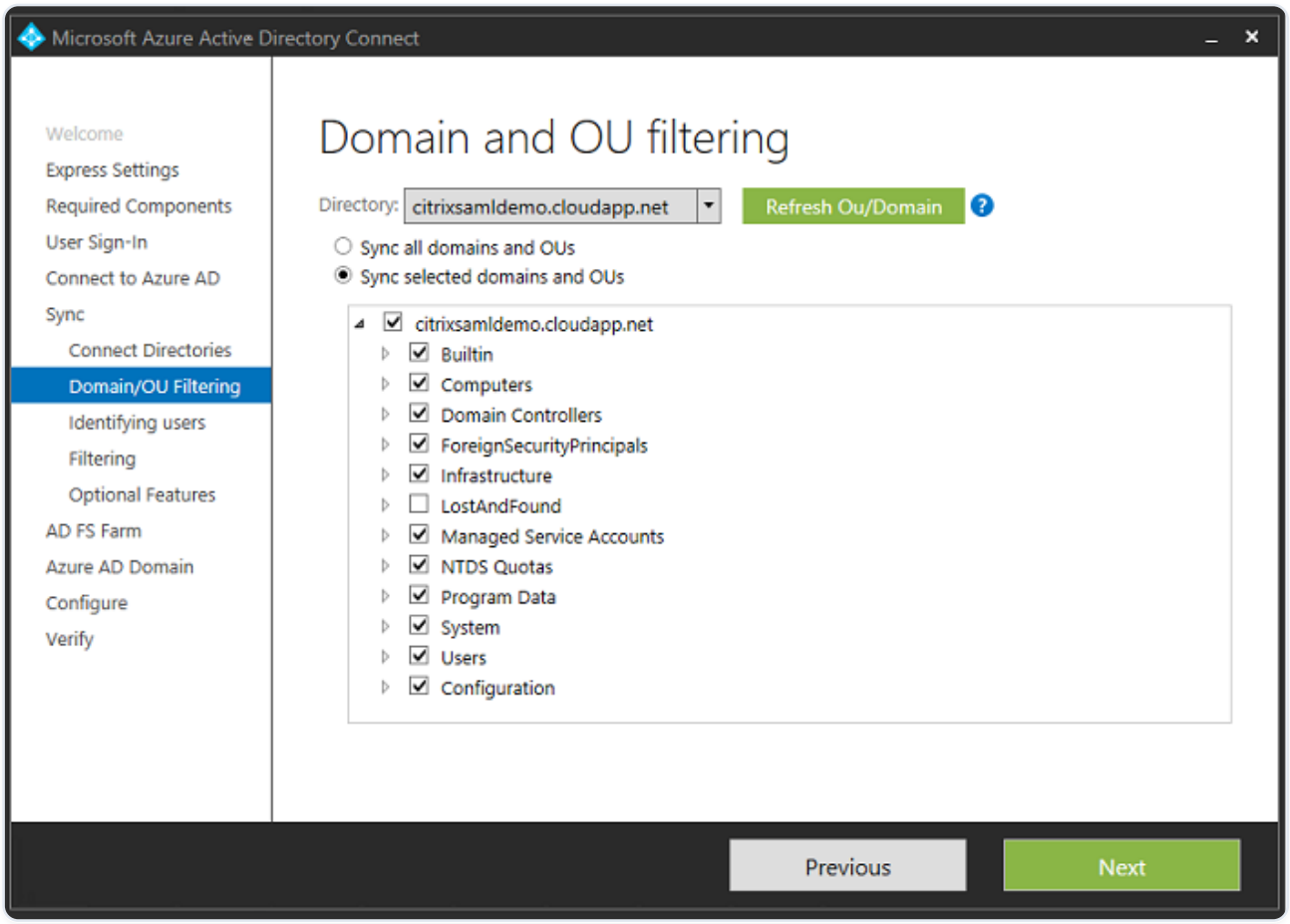


内部ADフォレストを選択します。

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

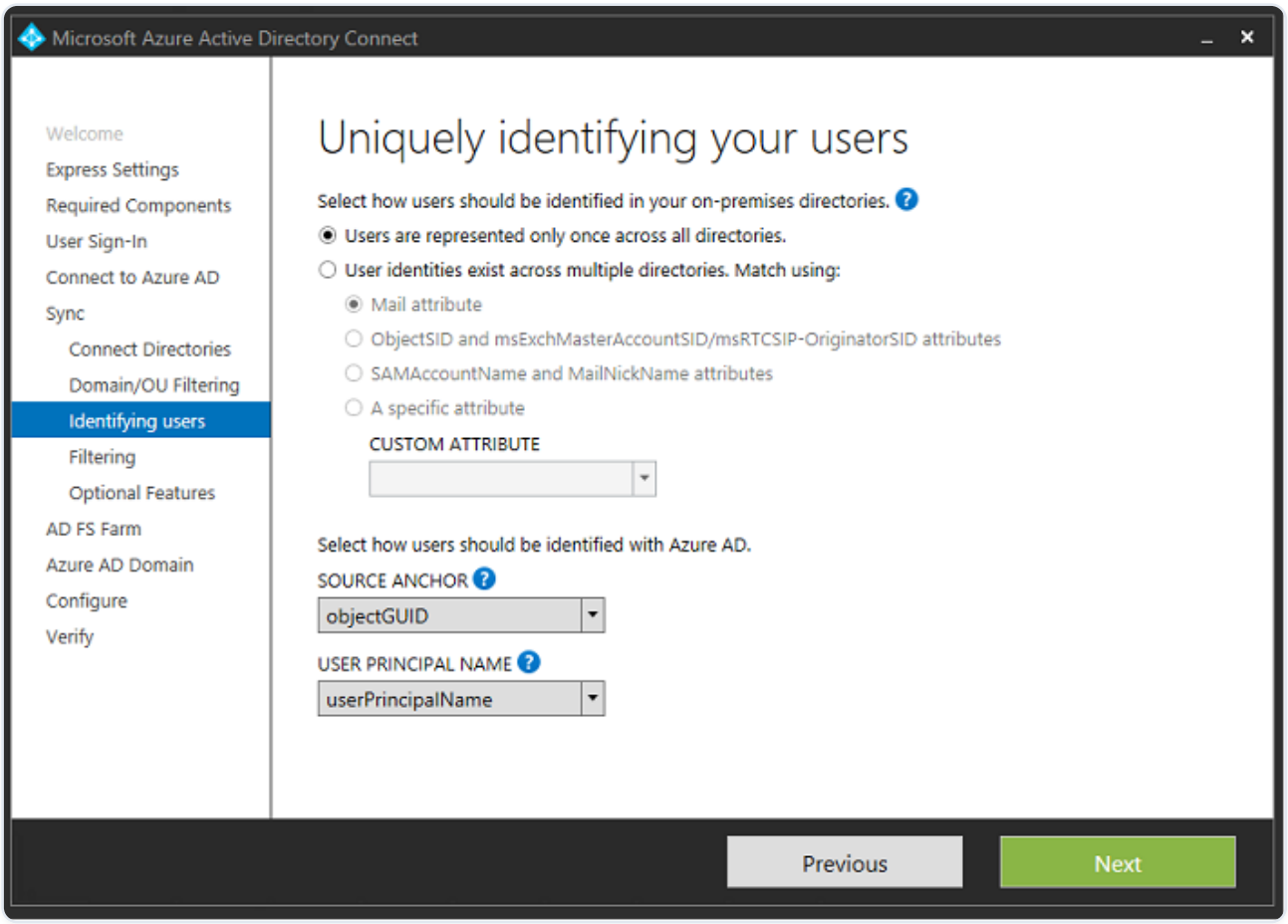


すべてのレガシーActive Directoryオブジェクトを Azure ADと同期します。



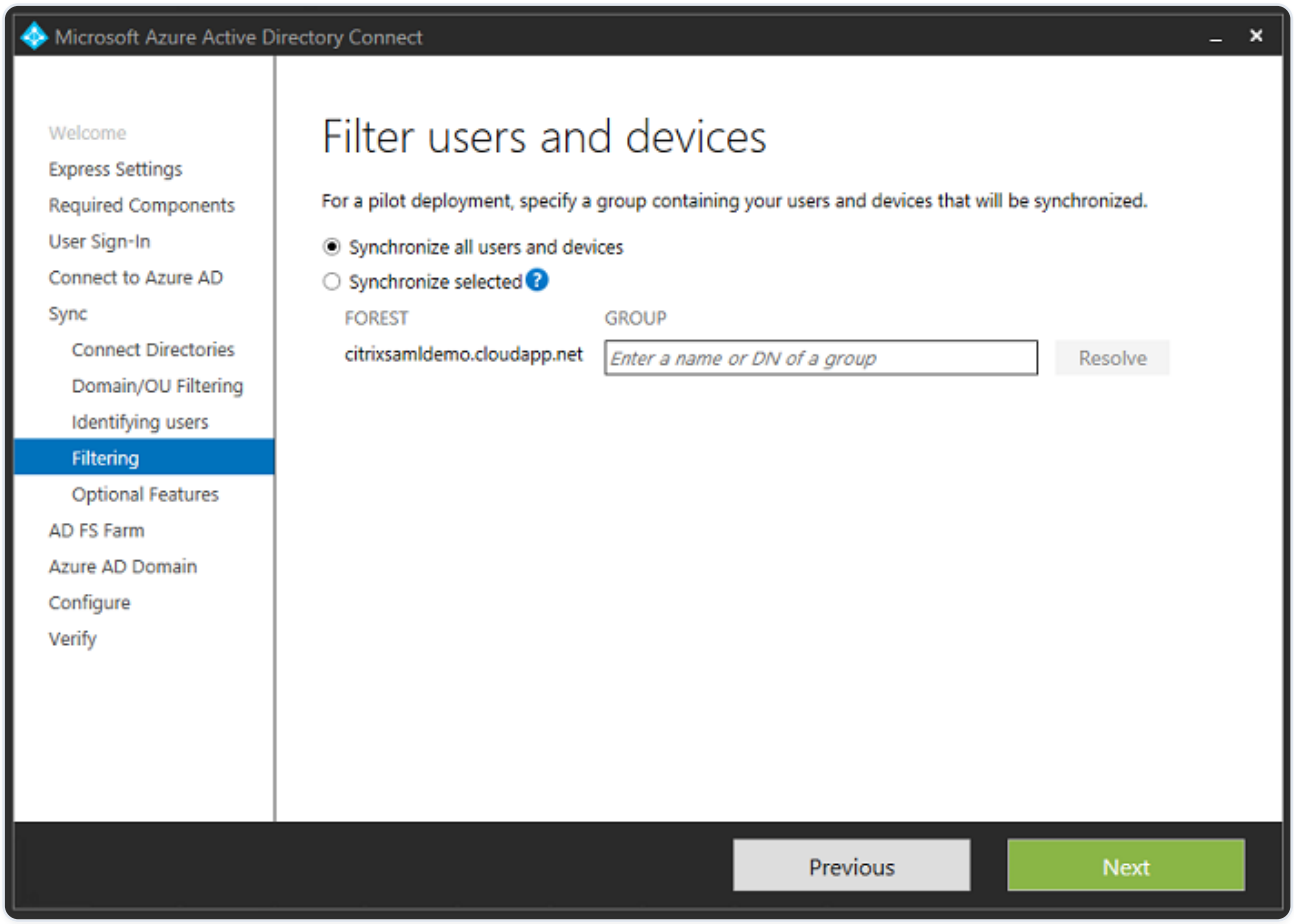
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。



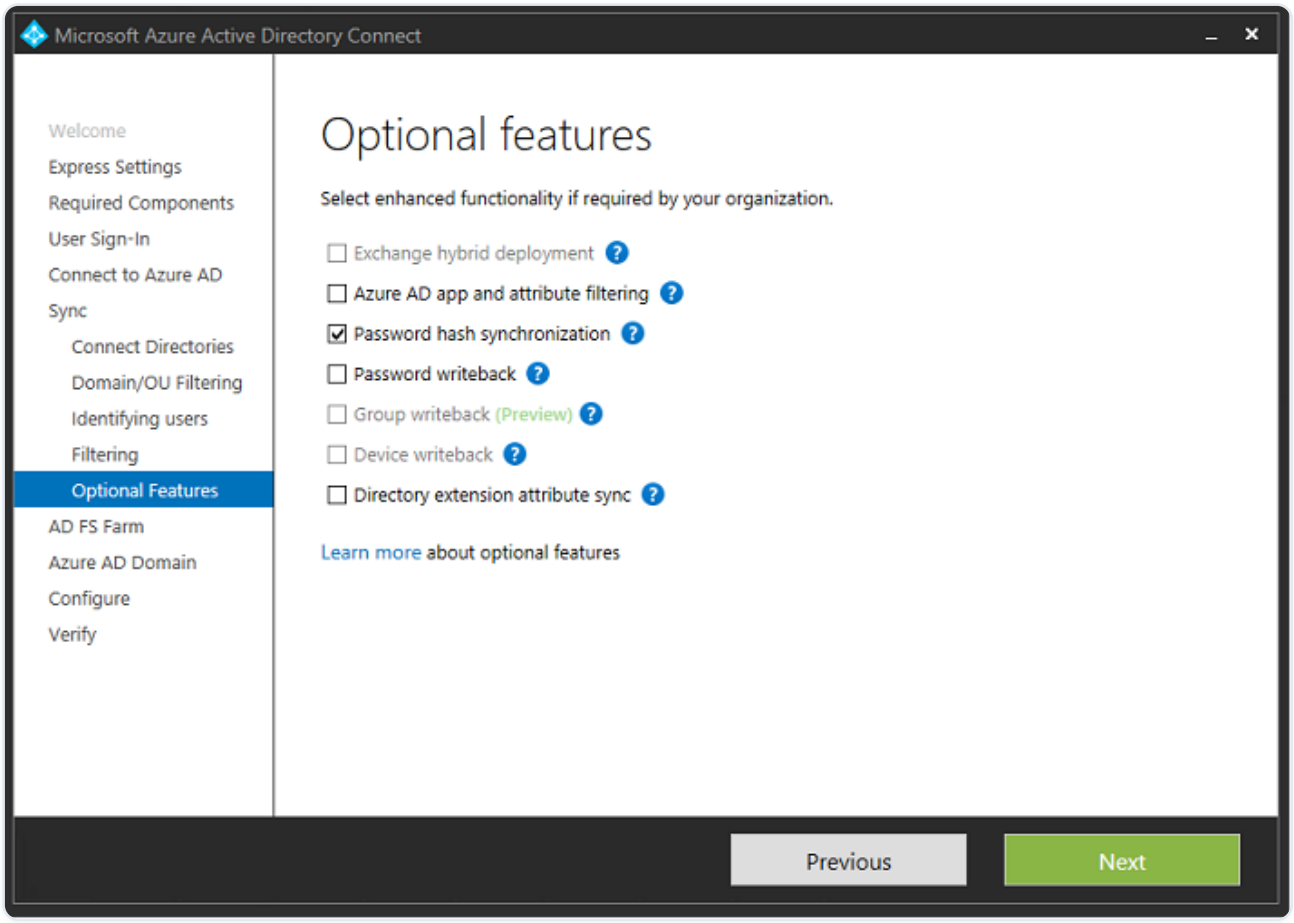
デフォルトのフィルタリングオプションを受け入れるか、ユーザーとデバイスを特定のグループセットに制限します。

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



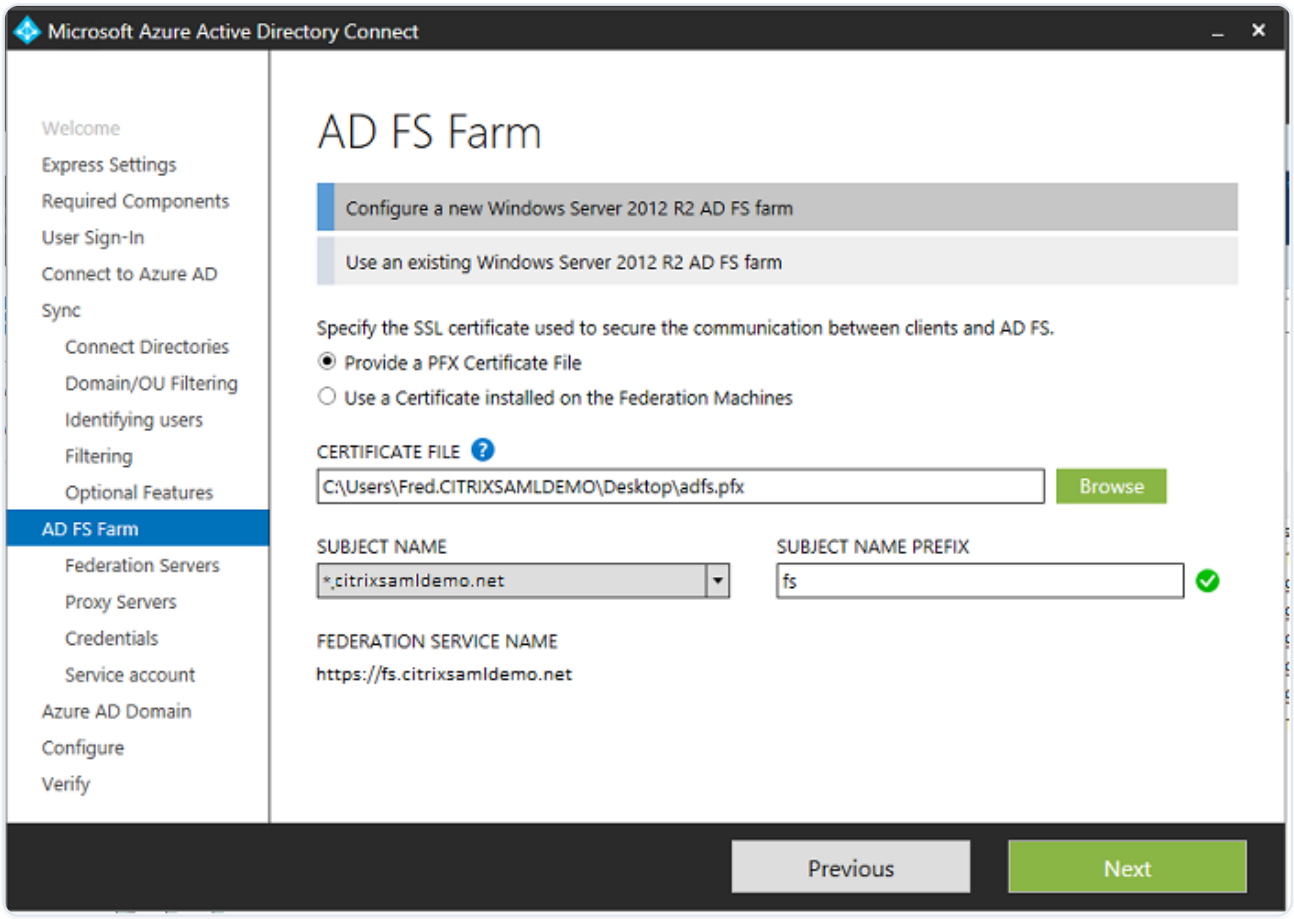
必要に応じて、Azure ADパスワードをActive Directoryと同期できます。これは通常、ADFSベースの認証には必要ありません。

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



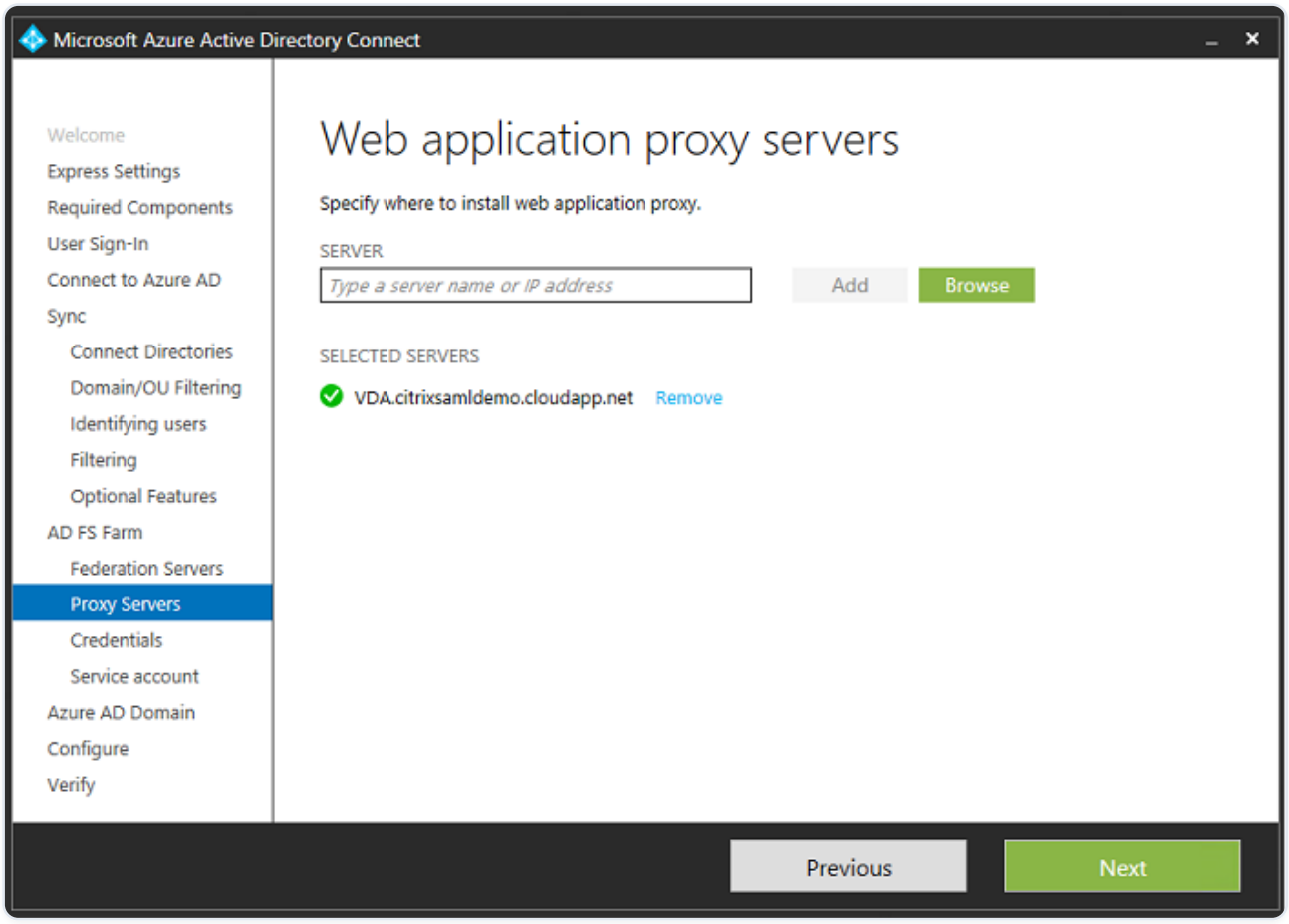
AD FSで使用する証明書PFXファイルを選択し、DNS名としてfs.citrixsamldemo.netを指定します。

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



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

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

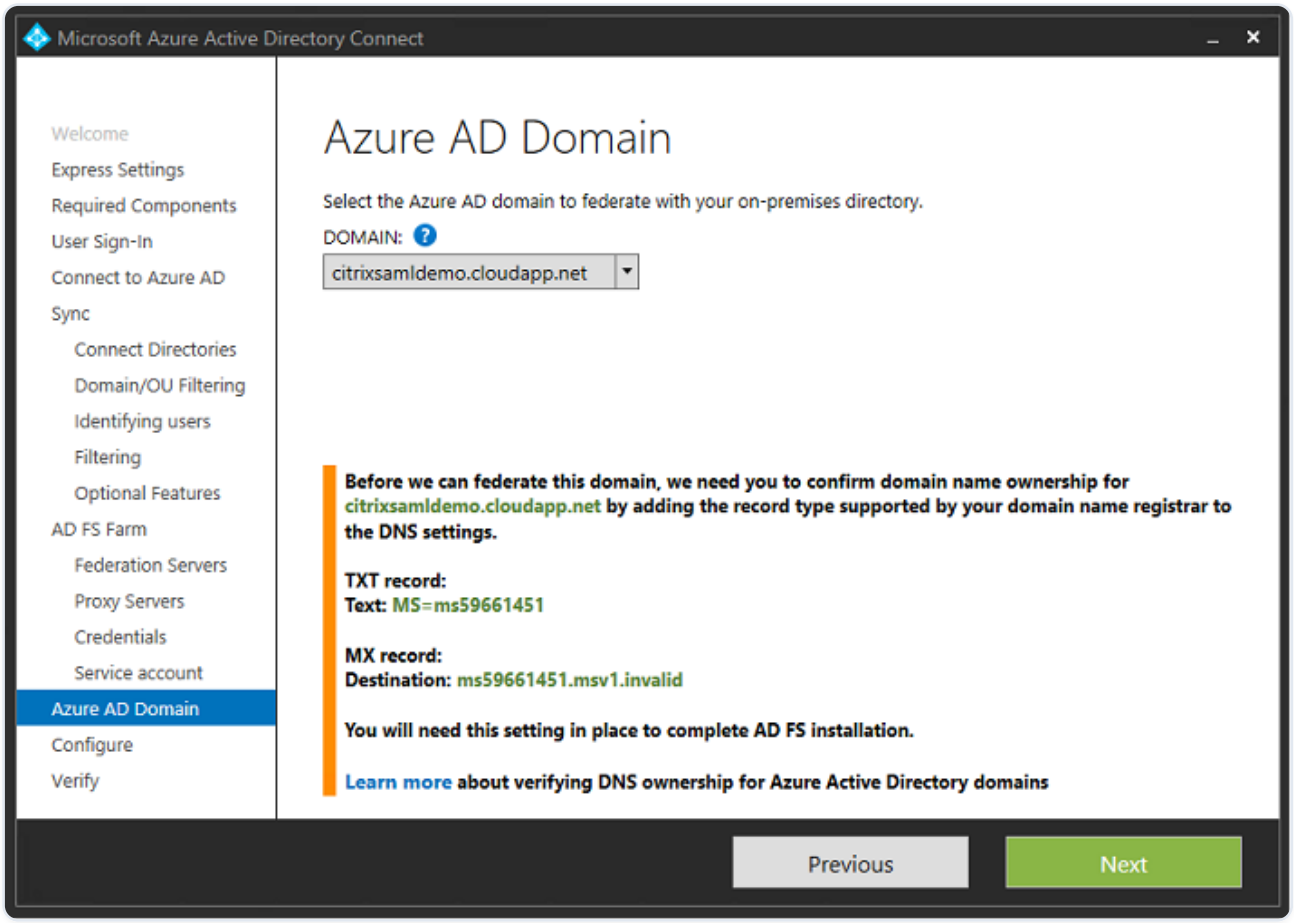


注：

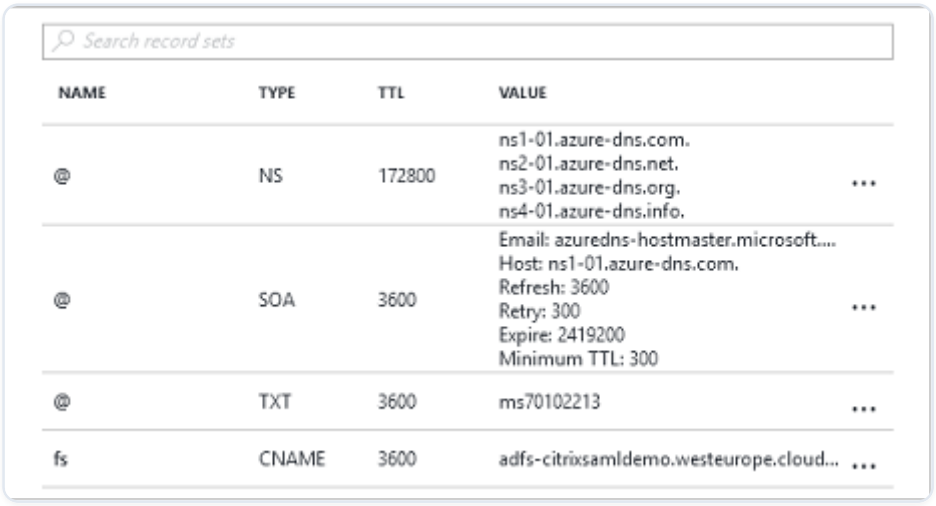
リモートPowerShellの信頼性の問題によりこの手順が失敗した場合は、Webアプリケーションプロキシサーバーをドメインに参加させてみてください。

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

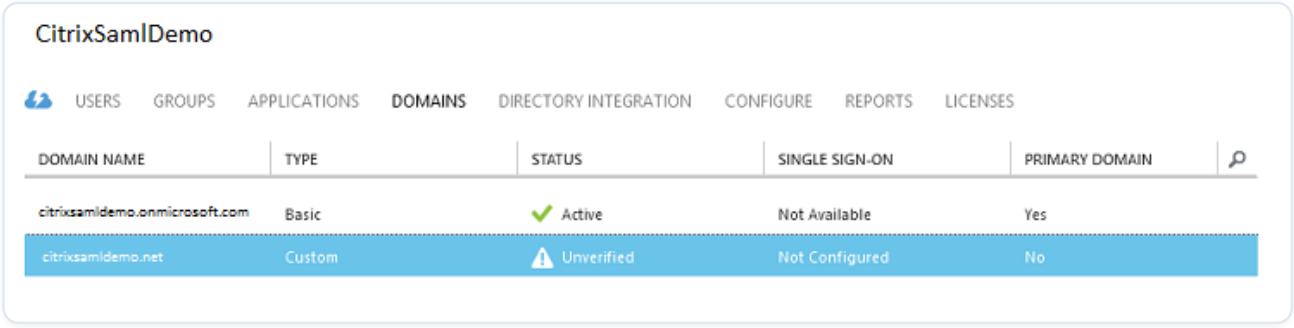
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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。



Azure 管理コンソールで をクリックします。

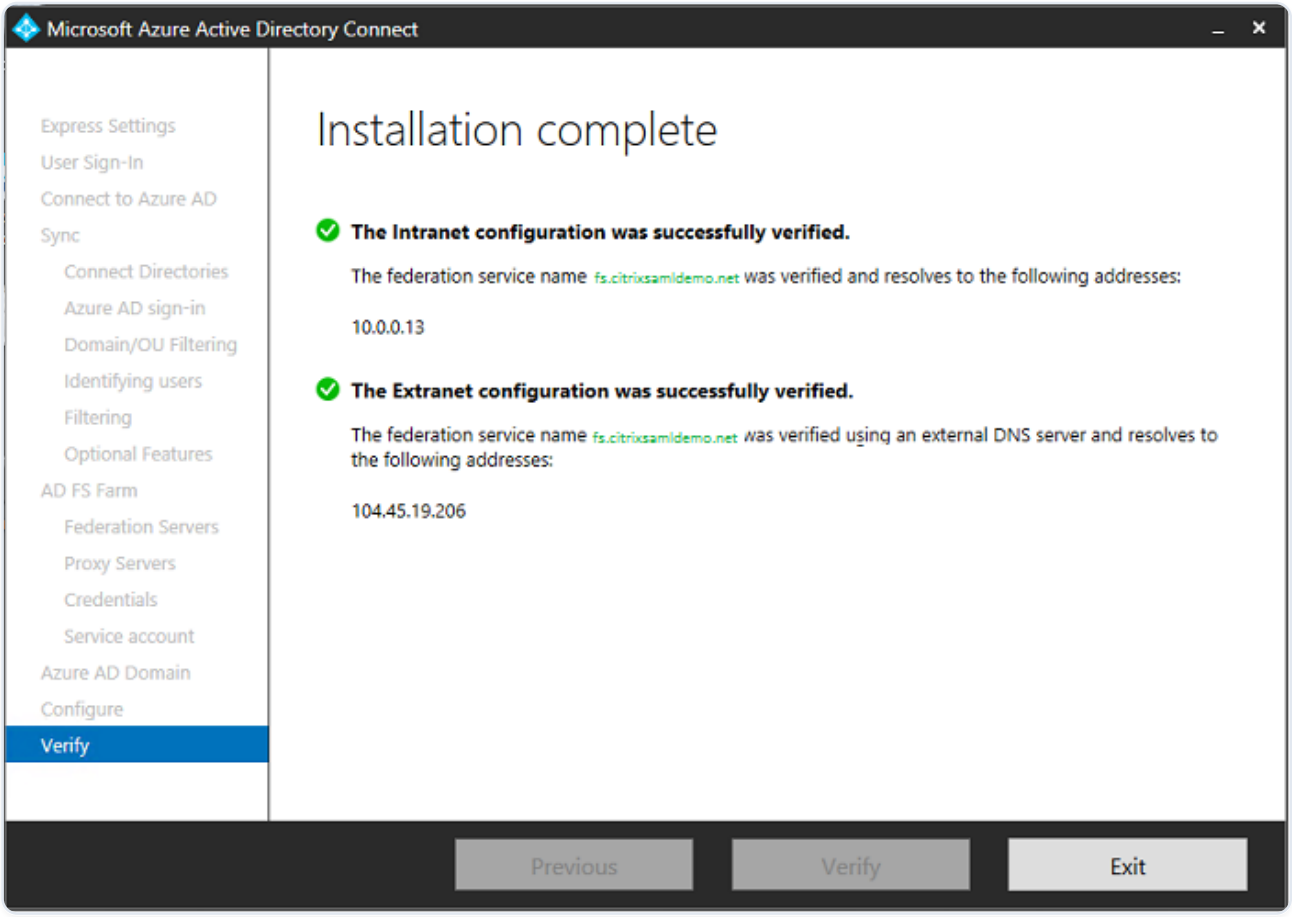


© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

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

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

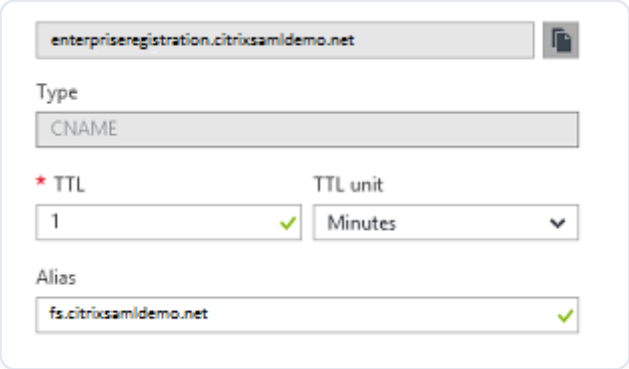


Azure AD Join を有効にする

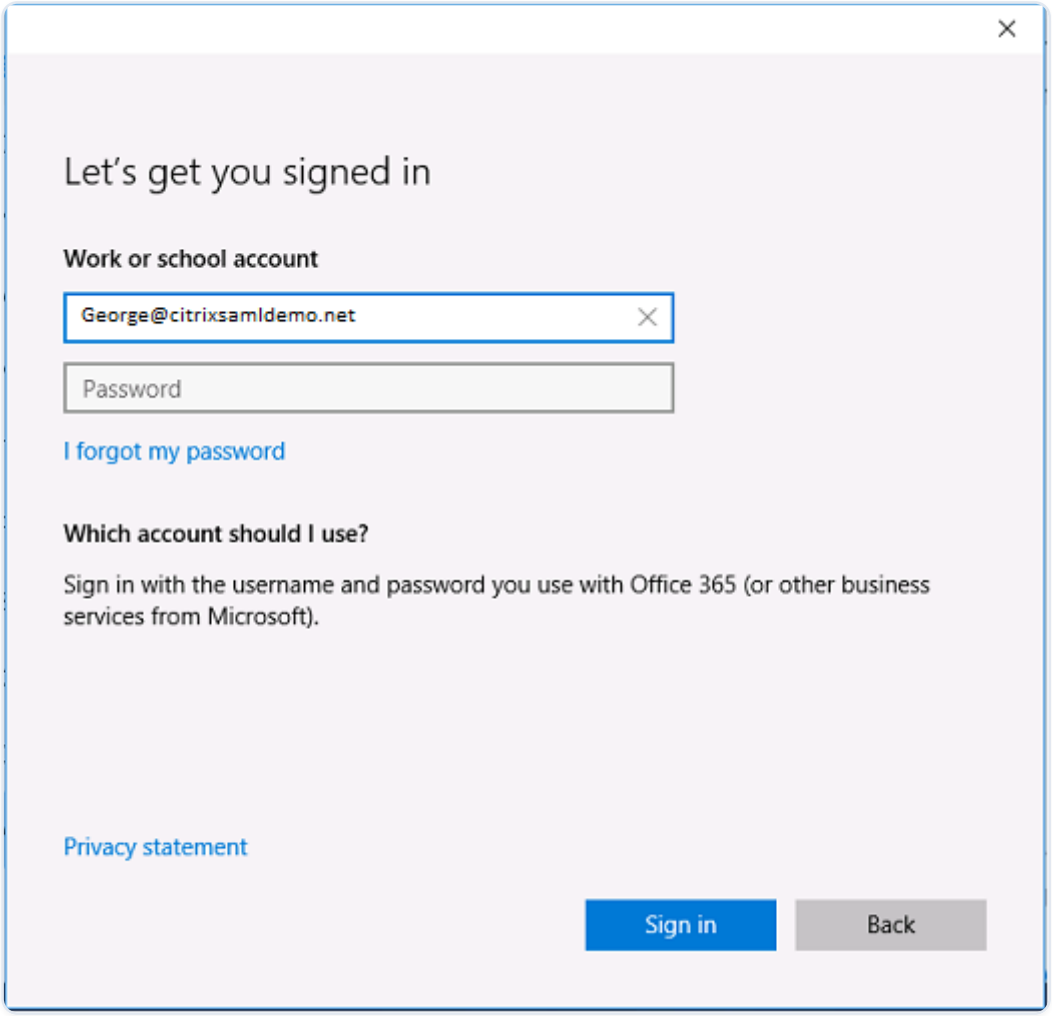
ユーザーがメールアドレスを入力してWindows 10がAzure AD参加を実行できるようにすると、DNSサフィックスがADFSを指すCNAME DNSレコード（enterpriseregistration.\<*upnsuffix*>）を構築するために使用されます。

この例では、これは`fs.citrixsamldemo.net`です。

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

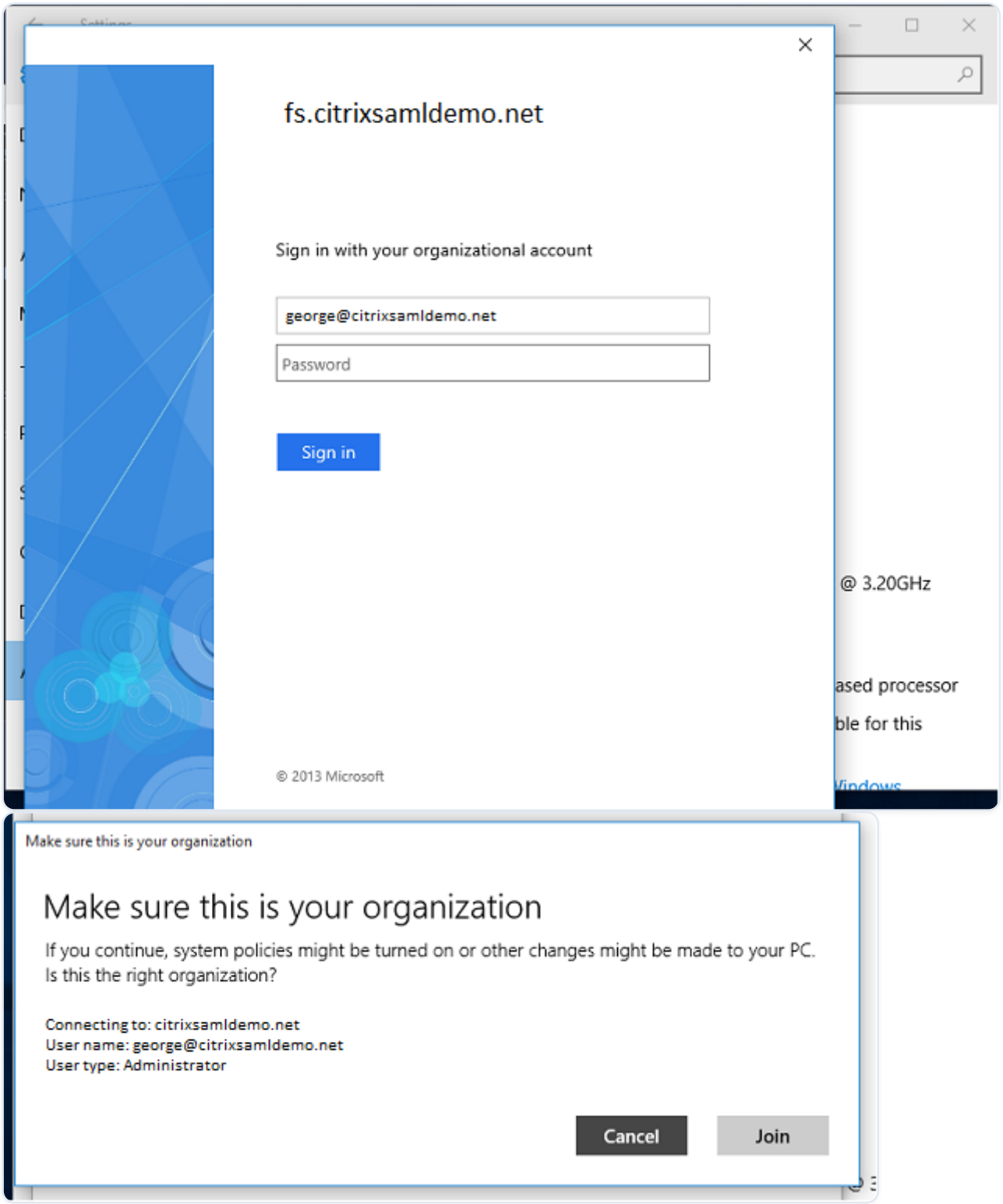


公開証明機関を使用していない場合は、WindowsがADFSサーバーを信頼するように、ADFSルート証明書がWindows 10コンピューターにインストールされていることを確認してください。以前に生成した標準ユーザーアカウントを使用して、Azure ADドメイン参加を実行します。

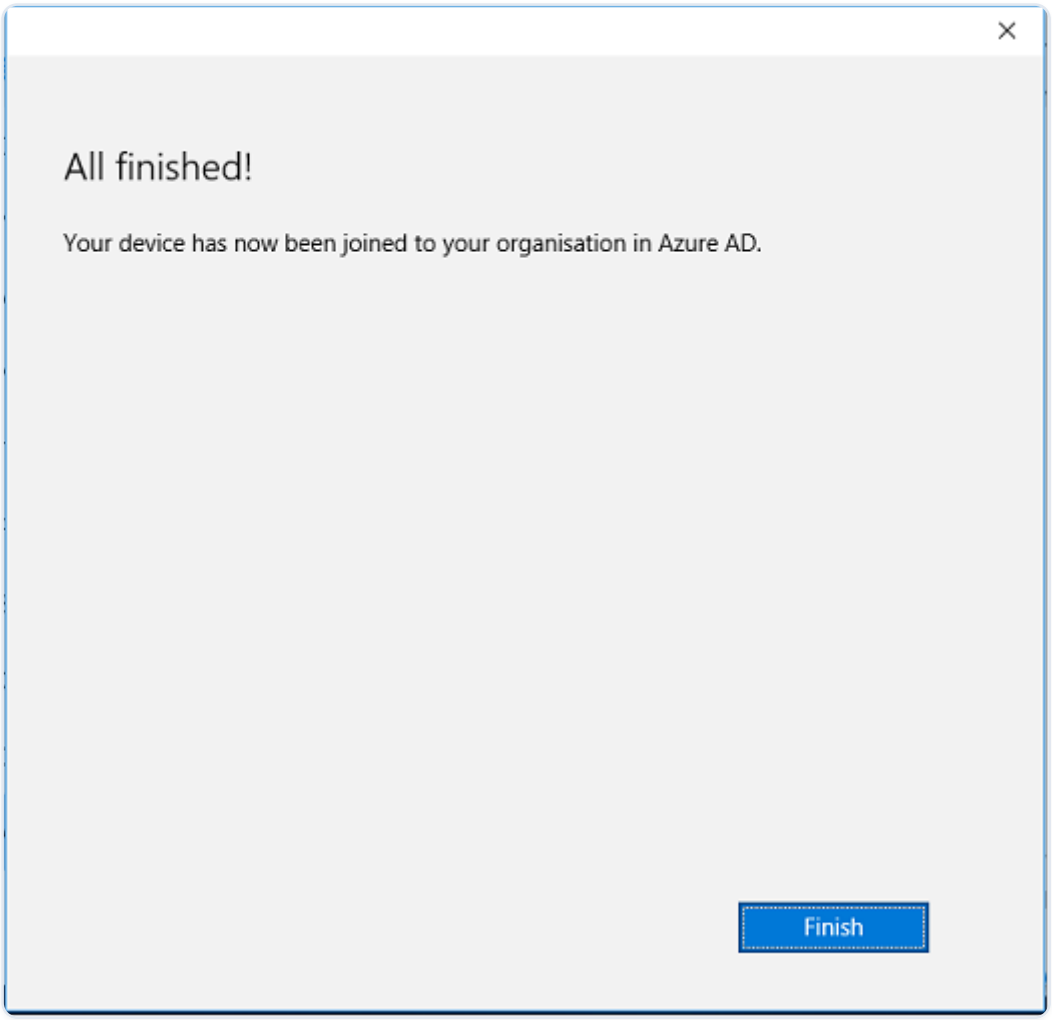


UPNは、ADFSドメインコントローラーによって認識されるUPNと一致する必要があることに注意してください。

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



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



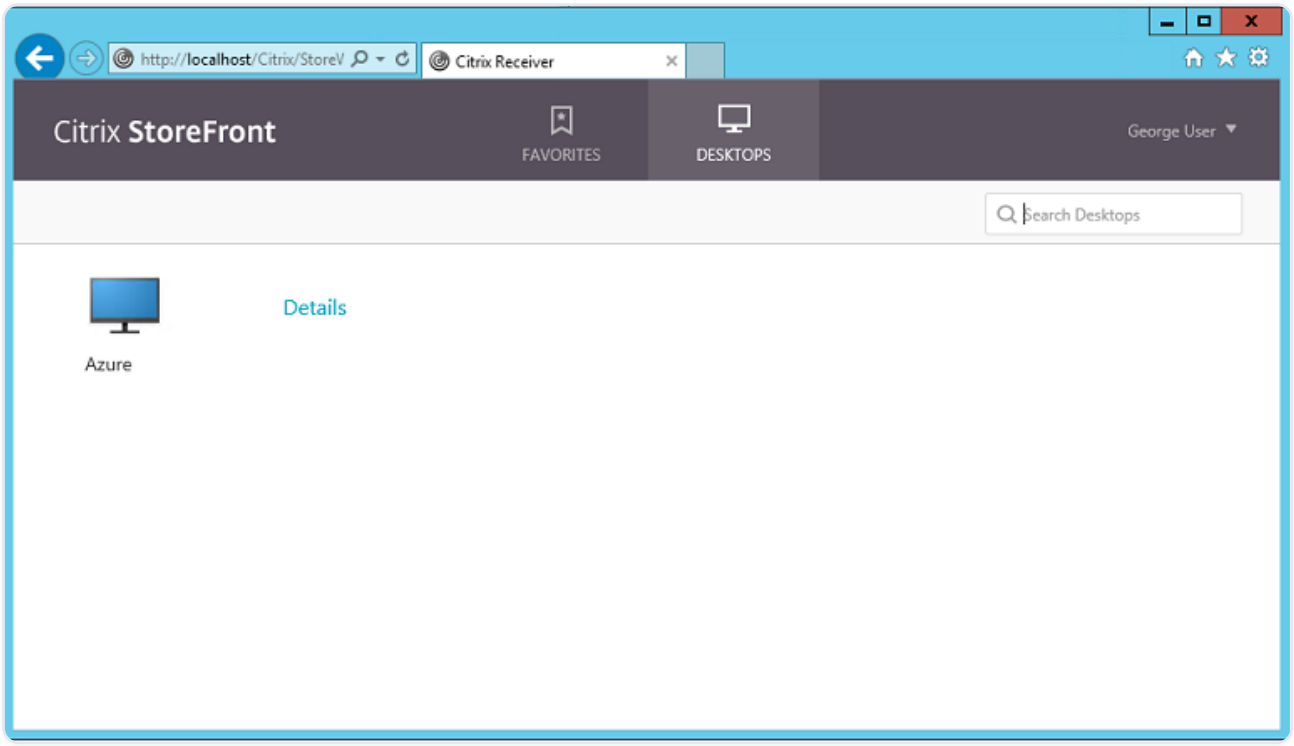
マシンを再起動し、ユーザーのメールアドレスを使用してログオンすることで、Azure AD参加が成功したことを確認します。ログオンしたら、Microsoft Edgeを起動して`<http://myapps.microsoft.com>`に接続します。ウェブサイトは自動的にシングルサインオンを使用するはずです。

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

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

この例では、StoreFrontはDelivery Controllerと同じサーバーにインストールされています。VDAは、Machine Creation Servicesと統合せずに（オプションで構成可能ですが）、スタンドアロンのWindows 2012 R2 RDSワーカーとしてインストールされています。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。

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



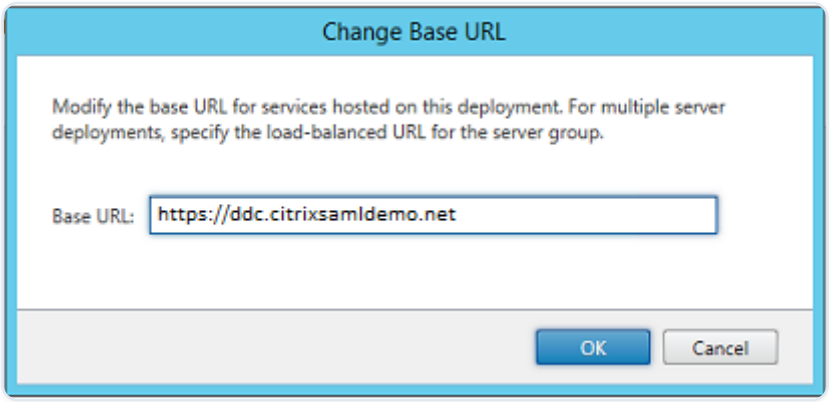
ユーザーの資格情報なしでStoreFront™が認証できるように、Controllerで**Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** PowerShellコマンドレットを実行します。

Federated Authentication Serviceをインストールする

ADFSサーバーにFASをインストールし、Delivery Controllerが信頼されたStoreFrontとして機能するようにルールを構成します (この例では、StoreFrontはDelivery Controllerと同じVMにインストールされているため)。「インストールと構成」を参照してください(/ja-jp/federated-authentication-service/2305/install-configure.html)。

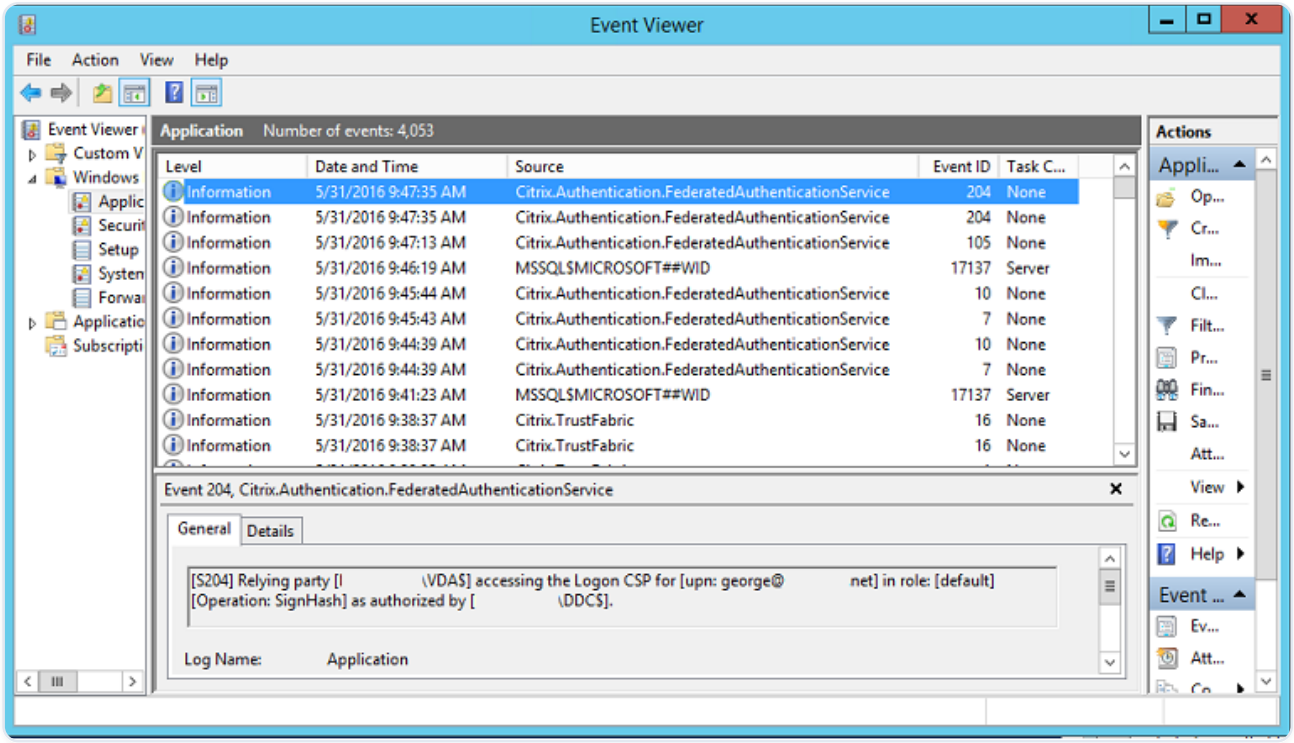
StoreFrontを構成する

Delivery Controllerのコンピューター証明書を要求し、ポート443のIISバインディングを設定して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。



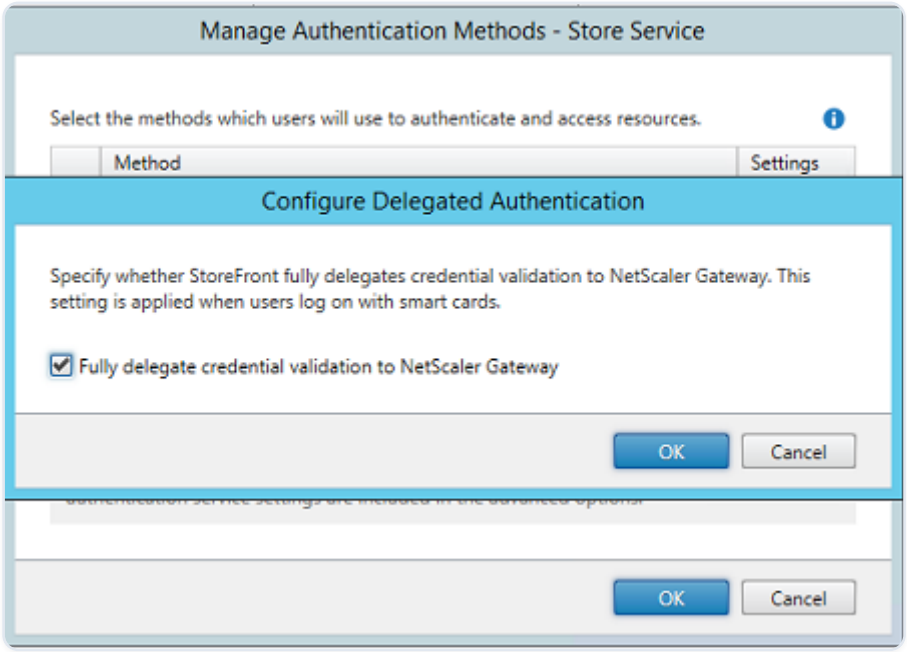
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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/2305/install-configure.html)のPowerShellスクリプトを使用します)、Azure内で内部的にテストし、FASサーバーのイベントビューアーを確認してログオンがFASを使用していることを確認します。



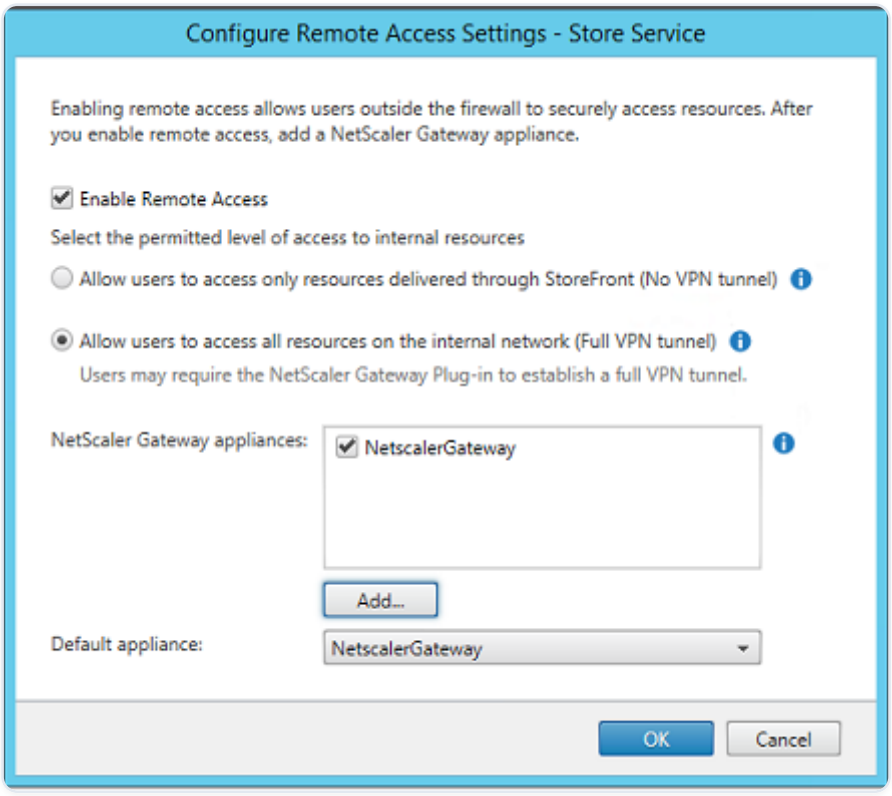
StoreFrontがCitrix Gatewayを使用するように構成する

StoreFront管理コンソールで**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。



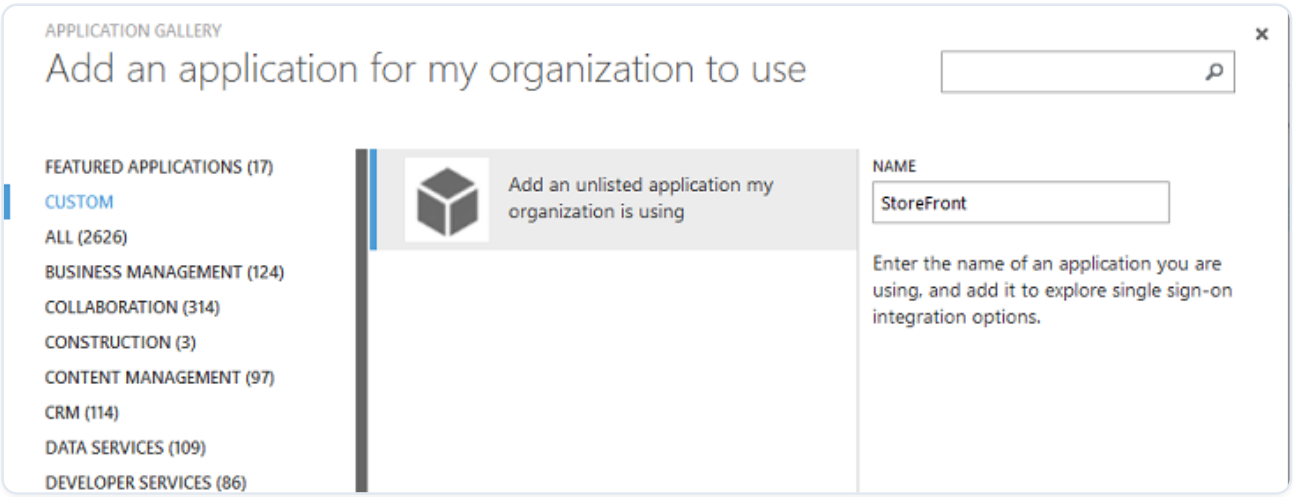
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

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

アイコンの構成

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-azure-config-app-add-app-icon.png)

SAML認証の構成

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-azure-config-app-add-configsso.png)

この展開ではSAML 2.0認証を使用します。これは「**Microsoft Azure AD Single Sign-On**」に対応しています。

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-azure-config-app-add-ad-sso.png)

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-azure-config-app-add-id-replyurl.png)

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。

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-azure-config-app-add-relyparty.png)

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

アプリケーションをユーザーに割り当てる

最終ステップは、アプリケーションを有効にして、ユーザーの「myapps.microsoft.com」コントロールページに表示されるようにすることです。これは「USERS AND GROUPS」ページで行います。Azure AD Connectによって同期されたドメインユーザーアカウントにアクセスを割り当て

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

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。

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-azure-config-app-add-assign-users.png)

MyAppsページ

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-azure-appls-access-page.png)

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

シングルサインオンURL

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

ローカライズされた画像(/en-us/federated-authentication-service/2305/media/fas-azure-config-app-add-sso-url.png)

このURLをWebブラウザに貼り付けて、Azure ADによって以前に構成されたCitrix Gateway cgi/samlauth Webページにリダイレクトされることを確認します。これは、割り当てられたユーザーにのみ機能し、Windows 10 Azure AD参加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

デプロイメントにリモートで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ストアから購入できます。この例では、NetScaler 11.0の「Bring your own License」バージョンを使用します。

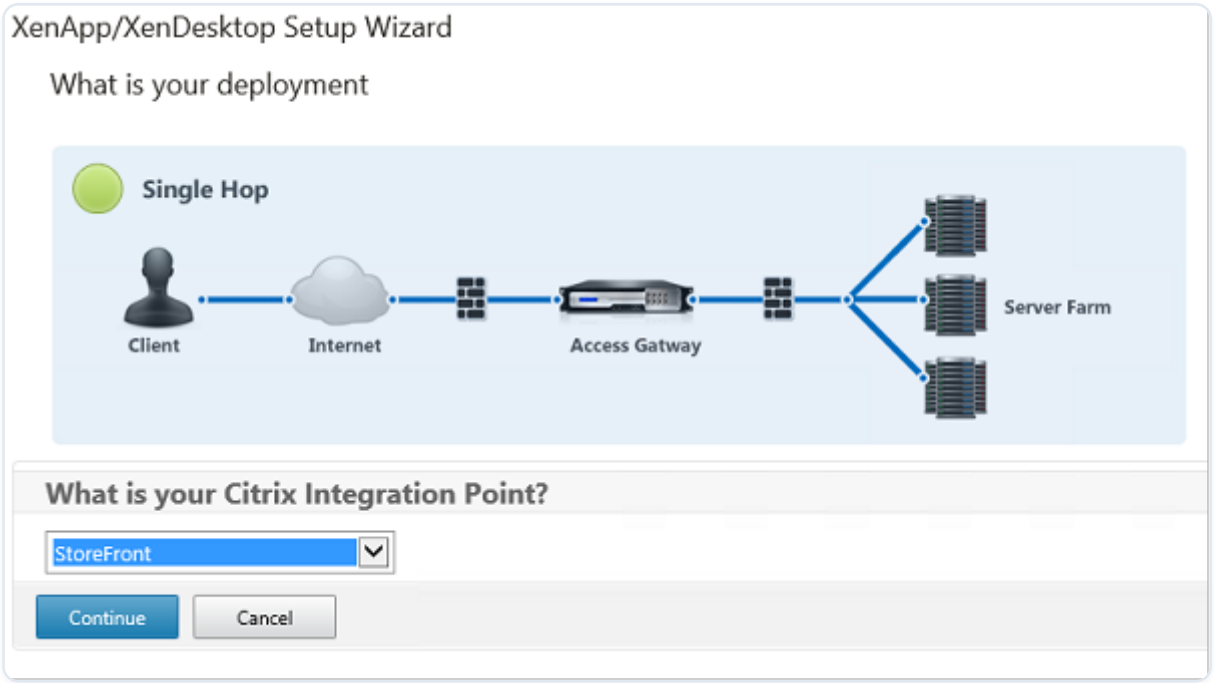
ユーザーが認証したときに指定された資格情報を使用して、Webブラウザを内部IPアドレスにポイントし、NetScaler® VMにログオンします。Azure AD VMでは、nsrootユーザーのパスワードを変更する必要があることに注意してください。

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

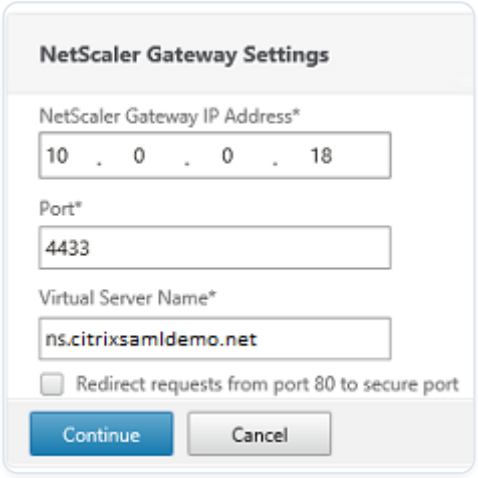
ライセンスを追加し、各ライセンスファイルの追加後に**再起動**を選択し、DNSリゾルバーをMicrosoftドメインコントローラーにポイントします。

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

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

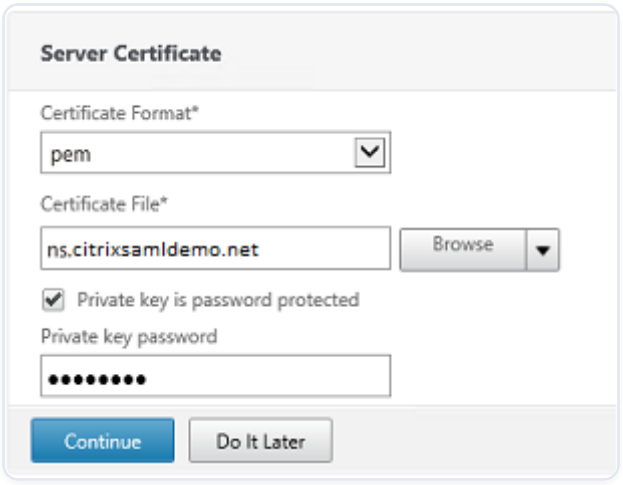


標準のCitrix Gateway StoreFront設定を選択します。Microsoft Azureで使用する場合、この例ではポート443ではなくポート4433を構成します。または、Citrix Gateway管理Webサイトをポート転送または再マッピングすることもできます。



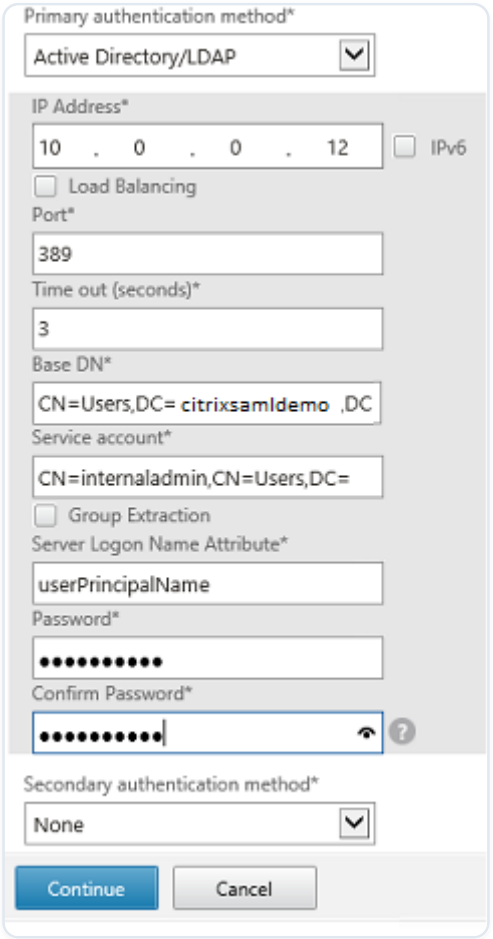
簡素化のため、この例ではファイルに保存されている既存のサーバー証明書と秘密キーをアップロードします。

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



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

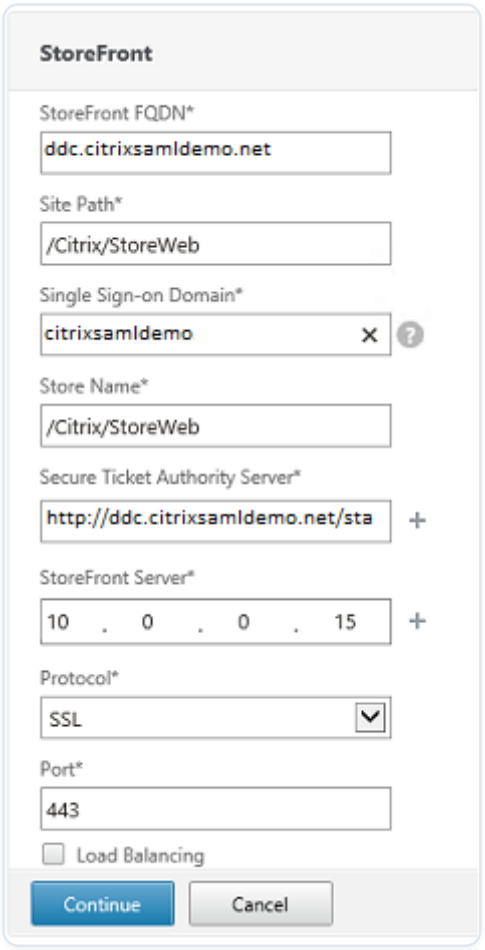
ドメインコントローラーはアカウント解決に使用されるため、そのIPアドレスをプライマリ認証方法に追加します。ダイアログボックスの各フィールドで期待される形式に注意してください。



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。

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



Citrix Gatewayの展開を確認する

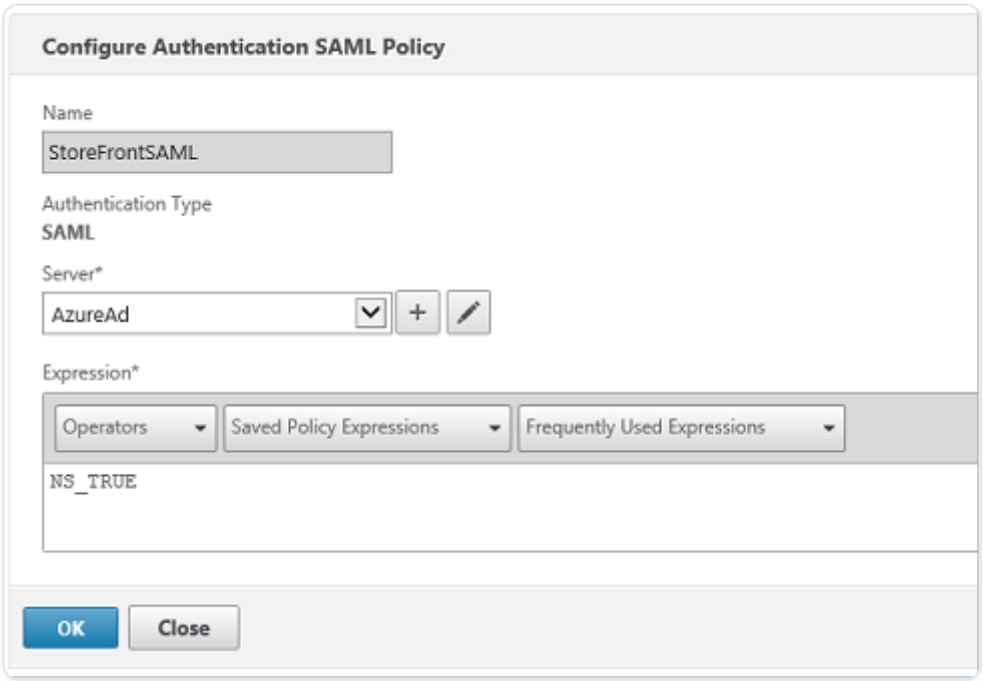
Citrix Gatewayに接続し、ユーザー名とパスワードで認証と起動が成功することを確認します。



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

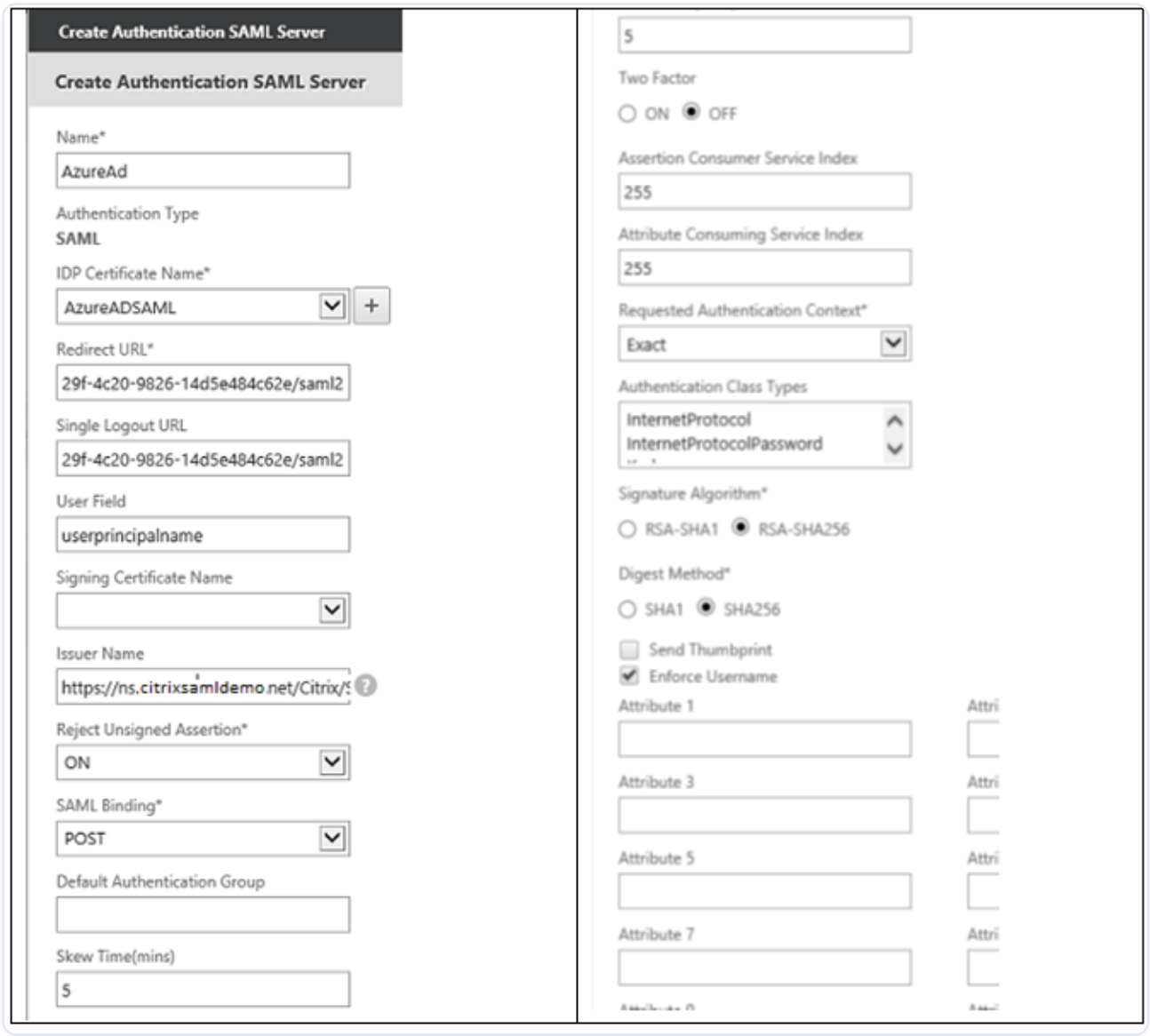
Citrix Gateway SAML認証サポートを有効にする

StoreFrontでSAMLを使用することは、他のWebサイトでSAMLを使用することと似ています。**NS_TRUE**の式を持つ新しいSAMLポリシーを追加します。



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

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

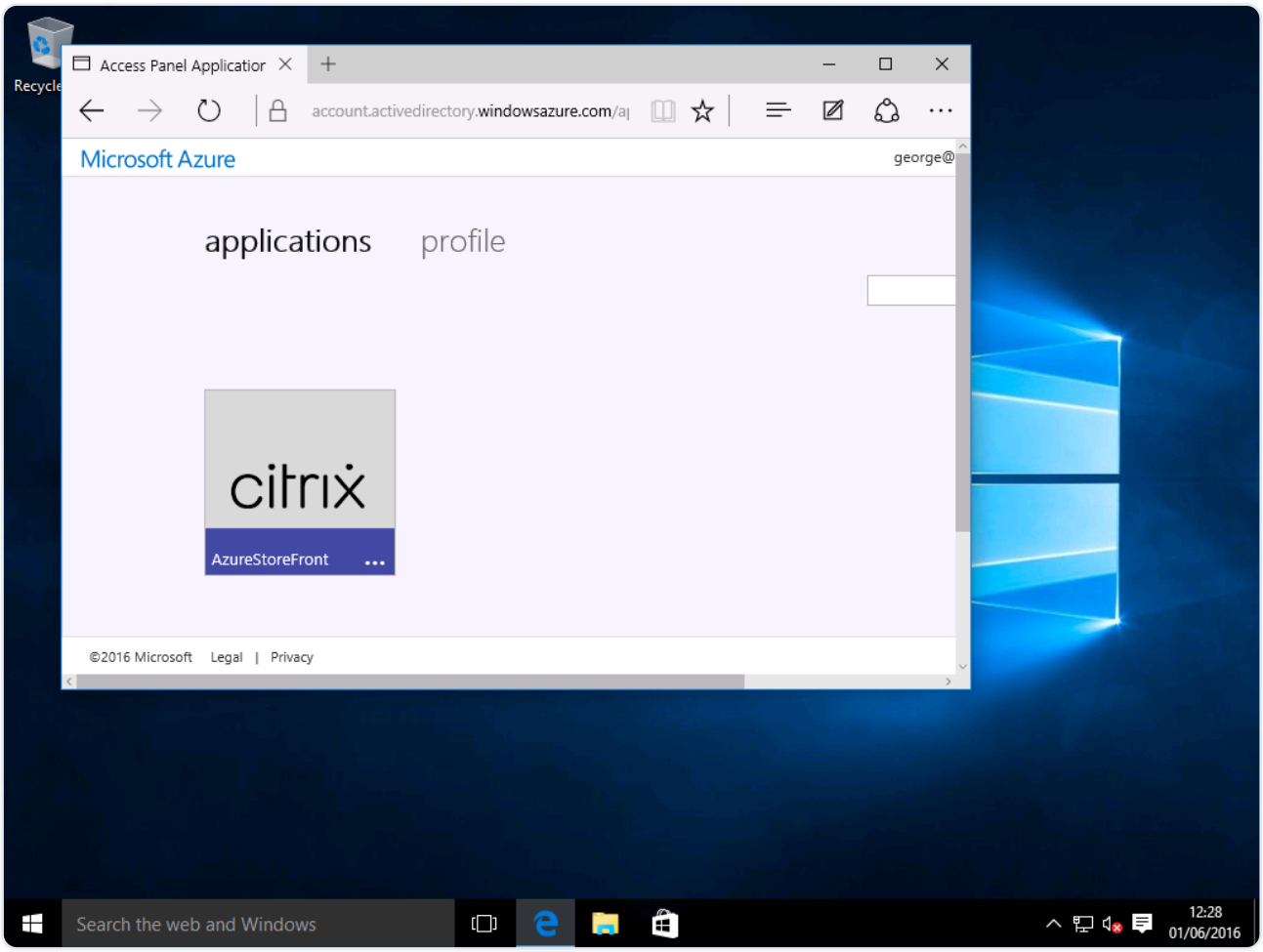


エンドツーエンドシステムを検証する

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

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

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



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

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

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

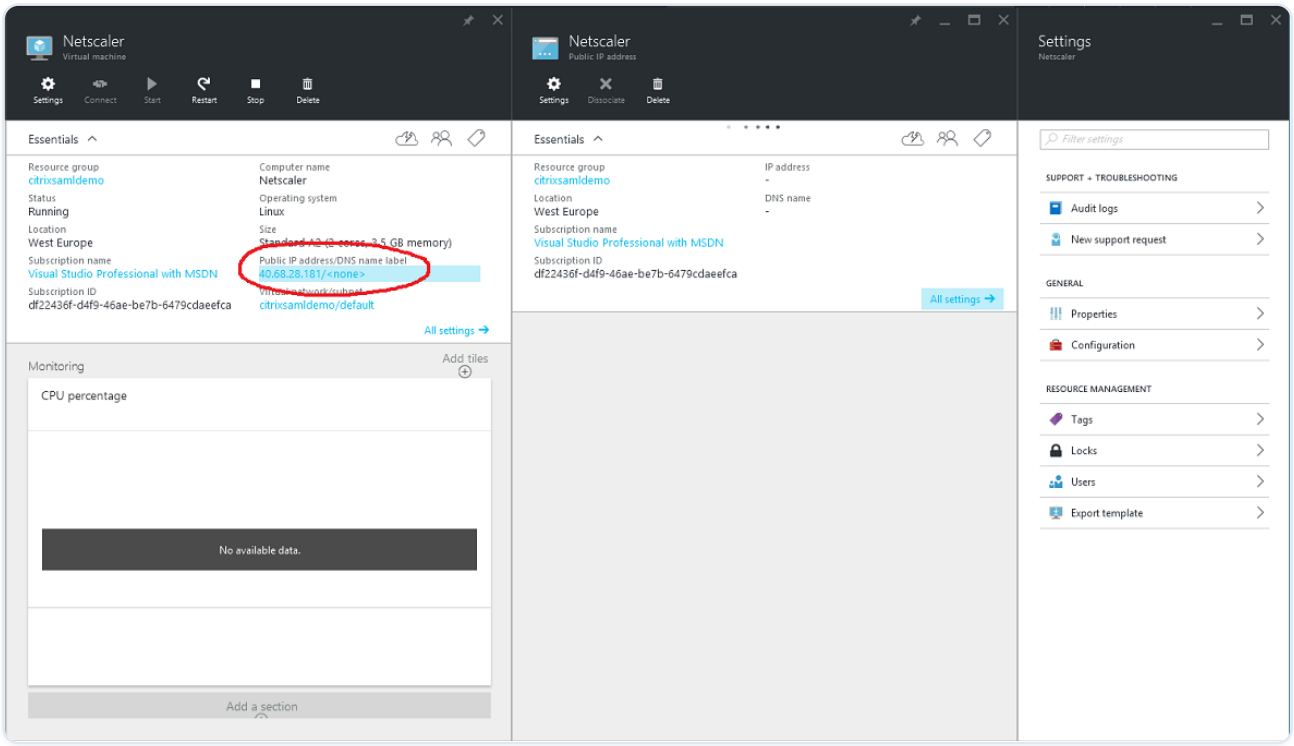
付録

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

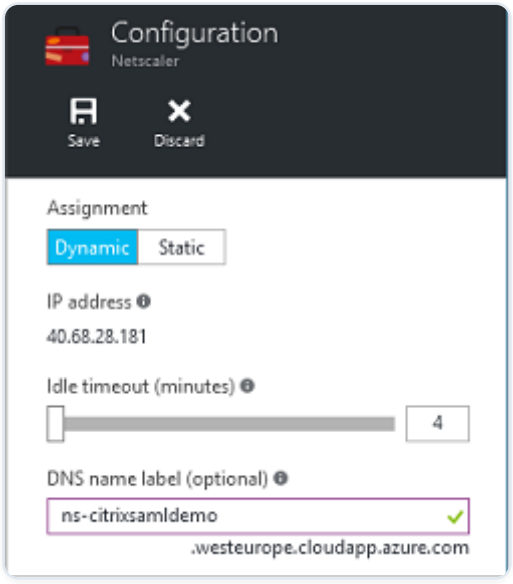
パブリックIPアドレスとDNSアドレスを提供する

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

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



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。



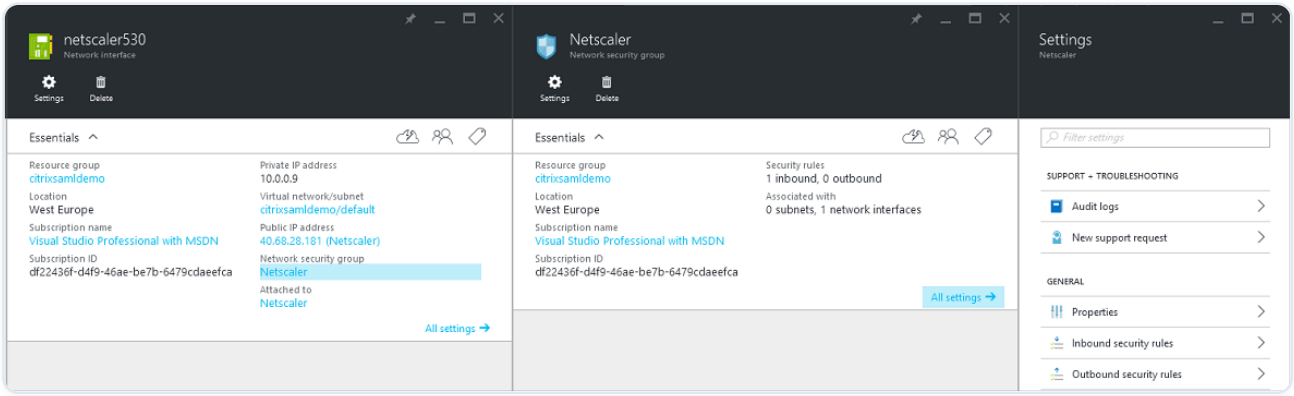
ファイアウォールルール（セキュリティグループ）を設定する

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

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

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。

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

フェデレーション認証サービス 2303 ドキュメント履歴

以下の表は、フェデレーション認証サービス 2303 ドキュメントの重要な変更点について説明しています。これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

日付	変更点	説明
30 May 2023	フェデレーション認証サービス 2305 の初回リリース	フェデレーション認証サービス 2305 の初回リリース。詳細については、新機能を参照してください。

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