Service d'authentification fédérée

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

Contents

Federated Authentication Service 2206 9

Service d'authentification fédérée 2206 10

- Problèmes résolus 10
- Problèmes connus 10
- Avis de tiers 11

Configuration système requise 12

Installer et configurer 13

- Séquence d'installation et de configuration 13
- Installer le service d'authentification fédérée 13
  - Mise à niveau de FAS 14
- Activer le plug-in FAS sur les magasins StoreFront 14
- Configurer le Delivery Controller™ 15
- Configurer la stratégie de groupe 15
  - Comportement en session 19
    - Portée de l'invite 20
    - Délai d'expiration du consentement 21
    - Déconnexion au verrouillage 21
- Utilisation de la console d’administration du service d’authentification fédérée 21
- Déployer des modèles de certificat 22
- Configurer les services de certificats Active Directory 24
- Autoriser le service d'authentification fédérée 25
- Configurer les règles 27
- Se connecter à Citrix Cloud 32
  - Se déconnecter de Citrix Cloud 37

Configuration avancée 38

- Informations connexes 38

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

Configuration de l'autorité de certification 38
Configurer plusieurs serveurs d'autorité de certification pour une utilisation dans FAS 38
Modifications de comportement attendues 39
Configurer l'autorité de certification Microsoft pour l'accès TCP 40
Pré-générer les certificats utilisateur 41
Obtenir une liste d'utilisateurs Active Directory 41
Serveur FAS 42
Renouveler les certificats d'autorité d'enregistrement 44
Informations connexes 45
Protection des clés privées 45
Introduction 45
Paramètres de configuration des clés privées 46
Exemples de scénarios de configuration 49
Exemple 1 49
Exemple 2 50
Exemple 3 61
Stockage des certificats FAS 63
Informations connexes 65
Sécurité et configuration réseau 65
Architecture réseau 65
Pare-feu et sécurité réseau 66
Connexions entre le service d'authentification fédérée Citrix et Citrix Cloud™ 67
Considérations de sécurité 68
Agents d'inscription délégués 68
Configuration de la liste de contrôle d'accès 69
Paramètres du pare-feu 69
Surveillance du journal des événements 69
Modules de sécurité matériels 69

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

Responsabilités d'administration 70
Paramètres de stratégie de groupe 71
Modèles de certificat 71
Renommer un modèle de certificat 71
Modifier les propriétés générales 72
Modifier les propriétés de gestion des requêtes 72
Modifier les propriétés de cryptographie 72
Modifier les propriétés d'attestation de clé 72
Modifier les propriétés des modèles remplacés 72
Modifier les propriétés des extensions 72
Modifier les propriétés de sécurité 72
Modifier les propriétés du nom du sujet 73
Modifier les propriétés du serveur 73
Modifier les propriétés des exigences d'émission 73
Modifier les propriétés de compatibilité 74
Administration de l'autorité de certification 74
Publication de modèles 74
Paramètres du pare-feu 75
Enregistrement restreint 75
Modules de stratégie et audit 75
Administration de FAS 76
Restreindre StoreFront, les utilisateurs et les VDA via une ACL 76
Configurer les règles 76
Configurer l'autorité de certification et les modèles 77
Certificats de session et d'authentification 77
Protection de la clé privée et longueur de la clé 77
Journaux d'événements 77
Accès administratif et outils d'administration 77

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

Administrateurs Citrix Virtual Apps, Citrix Virtual Desktops et VDA 77
Sécurité générale du serveur Windows 78
Informations connexes 78
Compteurs de performance 78
Dépanner les problèmes de connexion Windows 80
Certificats et infrastructure à clé publique 80
Nom UPN et mappage de certificat 82
Noms UPN dans Active Directory 82
Service de mappage de certificats 82
Contrôler la sélection du contrôleur de domaine de connexion 83
Contrôler la sélection du contrôleur de domaine 83
Identifier le contrôleur de domaine utilisé 83
Activer les événements d'audit de compte 83
Journaux de validation de certificat 84
Vérifier la validité du certificat 84
Activer la journalisation CAPI 84
Journaux CAPI 85
Messages d'erreur 85
Journaux Kerberos 85
Journaux du contrôleur de domaine et du poste de travail 86
Journal CAPI2 du contrôleur de domaine 86
Journal de sécurité du contrôleur de domaine 87
Journal de sécurité du VDA 88
Journal CAPI du VDA 89
Journal système du VDA 90
Surveillance de FAS à l’aide du journal d’événements Windows 90
Le service FAS est-il en cours d’exécution ? 91
Événements d’intégrité de FAS 91

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

Événements FAS connectés au cloud 93
Événements de sécurité 94
Journaux d'événements FAS 95
Événements d'administration 95
Création d'assertions d'identité 98
Agir en tant que partie de confiance 98
Serveur de certificats en session 99
Plug-in d'assertion FAS 99
FAS activé pour Workspace 100
Ouverture de session 102
Certificats de session 103
Demande de certificat et génération de paires de clés 103
Messages d'erreur de l'utilisateur final 104
Informations connexes 104
Applets de commande PowerShell 105
Architectures de déploiement 106
Introduction 106
Vue d'overview de l'architecture 106
Déploiement interne 107
Déploiement de Citrix Gateway 110
Déploiement ADFS SAML 113
Mappage de comptes B2B 114
Windows 10 Azure AD Join 115
Déploiement ADFS 117
Introduction 117
Présentation de SAML 119
URL de redirection 119
Identifiant 119

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

Adresse de retour 119

Certificat de signature 119

URL de déconnexion unique 120

Configuration 120

Remplir la politique SAML 120

Informations connexes 121

Intégration d'Azure AD 121

Introduction 121

Architecture 123

Créer une zone DNS 125

Créer un service cloud 126

Créer des machines virtuelles Windows 126

Contrôleur de domaine 127

Contrôleur ADFS et serveur proxy d'application web 127

Citrix Virtual Desktops™ Delivery Controller et VDA 128

Configurer un DNS interne 128

Configurer une adresse DNS externe 129

Configurer les groupes de sécurité 130

Créer un certificat ADFS 130

Configurer Azure AD 131

Créer un nouveau répertoire 131

Créer un utilisateur administrateur global (AzureAdmin) 133

Enregistrer votre domaine auprès d'Azure AD 134

Installer Azure AD Connect 135

Activer la jonction Azure AD 145

Installer Citrix Virtual Apps ou Citrix Virtual Desktops 148

Installer le service d'authentification fédérée 149

Configurer StoreFront 149

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

Configurer StoreFront pour utiliser Citrix Gateway 150
Configurer une nouvelle application Azure AD pour l'authentification unique à StoreFront 151
Configurer une icône 152
Configurer l'authentification SAML 152
Attribuer l'application aux utilisateurs 154
Page MyApps 155
URL d'authentification unique 156
Installer et configurer Citrix Gateway 156
Exécuter l'assistant de configuration de Citrix Virtual Apps and Desktops 156
Configurer le contrôleur de domaine pour la gestion des comptes AD 158
Configurer l'adresse StoreFront 158
Vérifier le déploiement de Citrix Gateway 159
Activer la prise en charge de l'authentification SAML de Citrix Gateway 160
Vérifier le système de bout en bout 161
Annexe 162
Fournir une adresse IP publique et une adresse DNS 162
Configurer les règles de pare-feu (groupe de sécurité) 163
Informations associées 164
Historique des documents du service d'authentification fédérée 2206 165

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

Federated Authentication Service 2206

Cette version de Federated Authentication Service (FAS) inclut les nouvelles fonctionnalités suivantes :

- **Enregistrement pour les serveurs FAS.** Le flux d’enregistrement Citrix Cloud™ pour les serveurs Federated Authentication Service (FAS) a été mis à jour afin d’offrir une expérience utilisateur cohérente et d’améliorer la posture de sécurité des serveurs FAS.

  Le nouveau service d’enregistrement pour FAS élimine la nécessité d’ouvrir un nouveau navigateur sur le serveur. Le service d’enregistrement offre une expérience utilisateur sur site cohérente avec les autres produits Citrix sur site, améliore la posture de sécurité des serveurs FAS et réduit la configuration de l’administrateur sur les serveurs FAS. Pour plus d’informations, consultez Se connecter à Citrix Cloud.
- **Améliorations des journaux d’événements.** De nouveaux journaux d’événements FAS ont été ajoutés. Pour plus de détails sur ces journaux d’événements, consultez Journaux d’événements FAS.

Pour plus d’informations sur les correctifs, consultez Problèmes résolus.

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

Service d'authentification fédérée 2206

Cette version du Service d'authentification fédérée (FAS) inclut les nouvelles fonctionnalités suivantes :

- **Enregistrement pour les serveurs FAS.** Mise à jour du flux d'enregistrement Citrix Cloud™ pour les serveurs du Service d'authentification fédérée (FAS) afin d'offrir une expérience utilisateur cohérente et d'améliorer la posture de sécurité des serveurs FAS.

  Le nouveau service d'enregistrement pour FAS élimine la nécessité d'ouvrir un nouveau navigateur sur le serveur. Le service d'enregistrement offre une expérience utilisateur sur site cohérente avec les autres produits Citrix sur site, améliore la posture de sécurité des serveurs FAS et réduit la configuration administrateur sur les serveurs FAS. Pour plus d'informations, consultez Se connecter à Citrix Cloud.
- **Améliorations des journaux d'événements.** Ajout de nouveaux journaux d'événements FAS. Pour plus de détails sur ces journaux d'événements, consultez Journaux d'événements FAS.

Pour plus d'informations sur les corrections de bogues, consultez Problèmes résolus.

Problèmes résolus

Aucun problème n'a été résolu dans Federated Authentication Service 2206.

Problèmes connus

Il n’y a aucun problème connu dans Federated Authentication Service 2206.

L’avertissement suivant s’applique à toute solution de contournement suggérant de modifier une entrée de registre :

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

AVERTISSEMENT :

Toute utilisation incorrecte de l’Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller votre système d’exploitation. Citrix ne peut garantir que les problèmes résultant d’une mauvaise utilisation de l’Éditeur du Registre puissent être résolus. Vous utilisez l’Éditeur du Registre à vos propres risques. Veillez à sauvegarder le registre avant de le modifier.

Avis de tiers

Cette version du service d'authentification fédérée peut inclure des logiciels tiers sous licence selon les termes définis dans les documents suivants :

- Avis de tiers de Citrix Virtual Apps and Desktops(/fr-fr/citrix-virtual-apps-desktops/downloads/third-party-notices-apps-and-desktops.pdf) (Téléchargement PDF)
- Divulgations de logiciels non commerciaux pour FlexNet Publisher 2017 (11.15.0.0)(/fr-fr/citrix-virtual-apps-desktops/downloads/fnp-licensing-11-15-0-ncsd-summary.pdf) (Téléchargement PDF)
- Supplément de documentation FlexNet Publisher Logiciels tiers et open source utilisés dans FlexNet Publisher 11.15.0(/fr-fr/citrix-virtual-apps-desktops/downloads/fnp-licensing-11-15-0-opensource.pdf) (Téléchargement PDF)

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

Configuration système requise

- Le service d'authentification fédérée (FAS) est pris en charge sur les versions suivantes de Windows Server :
  - Windows Server 2022, éditions Standard et Datacenter
  - Windows Server 2019, éditions Standard et Datacenter, et avec l'option Server Core
  - Windows Server 2016, éditions Standard et Datacenter, et avec l'option Server Core
- Citrix recommande d'installer FAS sur un serveur qui ne contient pas d'autres composants Citrix.
- Le serveur Windows doit être sécurisé. Il aura accès à un certificat d'autorité d'enregistrement et à une clé privée lui permettant d'émettre automatiquement des certificats pour les utilisateurs du domaine, et il aura accès à ces certificats d'utilisateur et clés privées.
- Les (/fr-fr/federated-authentication-service/2206/config-manage/ps-sdk.html) FAS nécessitent l'installation de Windows PowerShell 64 bits sur le serveur FAS.
- Une autorité de certification d'entreprise Microsoft (racine ou subordonnée) est requise pour émettre des certificats d'utilisateur.

Dans le site Citrix Virtual Apps ou Citrix Virtual Desktops™ :

- Les Delivery Controllers, les Virtual Delivery Agents (VDA) et le serveur StoreFront™ doivent tous être des versions prises en charge.
- Avant de créer le catalogue de machines, la configuration de la stratégie de groupe du service d'authentification fédérée doit être appliquée correctement aux VDA. Consultez la section (/fr-fr/federated-authentication-service/2206/install-configure.html#configure-group-policy) pour plus de détails.

Lors de la planification du déploiement de ce service, consultez la section (/fr-fr/federated-authentication-service/2206/config-manage/security.html#security-considerations).

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

Installer et configurer

Séquence d'installation et de configuration

1. Installer le service d'authentification fédérée (FAS)
2. Activer le plug-in FAS sur les magasins StoreFront
3. Configurer le Delivery Controller
4. Configurer la stratégie de groupe
5. Utilisez la console d'administration FAS pour :
    a. Déployer des modèles de certificat
    b. Configurer les autorités de certification
    c. Autoriser FAS à utiliser vos autorités de certification
    d. Configurer les règles
    e. Connecter FAS à Citrix Cloud (facultatif)

Installer le service d'authentification fédérée

Pour des raisons de sécurité, Citrix recommande d'installer le service d'authentification fédérée (FAS) sur un serveur dédié sécurisé de la même manière qu'un contrôleur de domaine ou une autorité de certification. FAS peut être installé à partir de :

- l'installeur Citrix Virtual Apps and Desktops™ (à partir du bouton **Federated Authentication Service** sur l'écran de démarrage automatique lorsque l'ISO est inséré), ou
- le fichier d'installation autonome de FAS (disponible sous forme de fichier MSI sur Citrix Downloads).

Ceux-ci installent les composants suivants :

- Service d'authentification fédérée
- Applets de commande du composant logiciel enfichable PowerShell pour la configuration avancée de FAS
- Console d'administration FAS

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

- Modèles de stratégie de groupe FAS (CitrixFederatedAuthenticationService.admx/adml)
- Fichiers de modèle de certificat
- Compteurs de performance et journaux d'événements

Mise à niveau de FAS

Vous pouvez mettre à niveau FAS vers une version plus récente à l'aide d'une mise à niveau sur place. Avant la mise à niveau, tenez compte des éléments suivants :

- Tous les paramètres du serveur FAS sont conservés lorsque vous effectuez une mise à niveau sur place.
- Assurez-vous que la console d'administration FAS est fermée avant de mettre à niveau FAS.
- Assurez-vous qu'au moins un serveur FAS est toujours disponible. Si aucun serveur n'est accessible par un serveur StoreFront™ activé pour le service d'authentification fédérée, les utilisateurs ne peuvent pas se connecter ou démarrer d'applications.

Pour démarrer une mise à niveau, installez FAS à partir de l'installateur Citrix Virtual Apps and Desktops ou à partir du fichier d'installation autonome de FAS.

Activer le plug-in FAS sur les magasins StoreFront

REMARQUE :

Cette étape n’est pas nécessaire si vous utilisez FAS uniquement avec Citrix Cloud.

Pour activer l’intégration FAS sur un StoreFront Store, exécutez les cmdlets PowerShell suivantes en tant que compte Administrateur. Si le magasin a un nom différent, modifiez `$StoreVirtualPath`.

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

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

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

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

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

Pour arrêter d'utiliser FAS, utilisez le script PowerShell suivant :

```
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 ""
```

Configurer le Delivery Controller™

REMARQUE :

Cette étape n'est pas nécessaire si vous utilisez FAS uniquement avec Citrix Cloud.

Pour utiliser FAS, configurez le Delivery Controller Citrix Virtual Apps ou Citrix Virtual Desktops™ pour qu'il approuve les serveurs StoreFront qui peuvent s'y connecter : exécutez la cmdlet PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true**. Cette opération ne doit être effectuée qu'une seule fois par site, quel que soit le nombre de Delivery Controllers dans le site.

Configurer la stratégie de groupe

Après avoir installé FAS, vous devez spécifier les noms de domaine complets (FQDN) des serveurs FAS dans la stratégie de groupe à l'aide des modèles de stratégie de groupe fournis lors de l'installation.

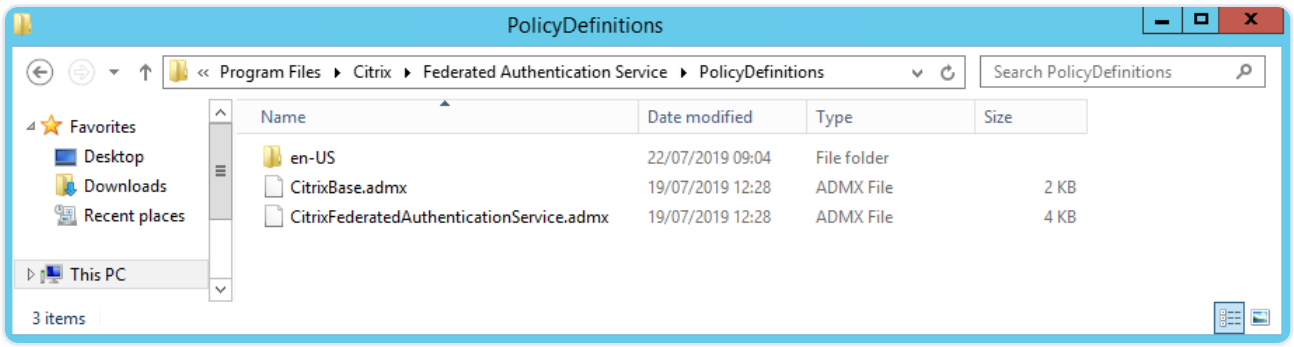
© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT :

Assurez-vous que les serveurs StoreFront demandant des tickets et les Virtual Delivery Agents (VDA) échangeant des tickets ont une configuration identique des FQDN, y compris la numérotation automatique des serveurs appliquée par l'objet de stratégie de groupe.

Par souci de simplicité, les exemples suivants configurent une seule stratégie au niveau du domaine qui s'applique à toutes les machines. Cependant, ce n'est pas obligatoire. FAS fonctionne tant que les serveurs StoreFront, les VDA et la machine exécutant la console d'administration FAS voient la même liste de FQDN. Voir l'étape 6.

Étape 1. Sur le serveur où vous avez installé FAS, localisez les fichiers C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx et CitrixBase.admx, ainsi que le dossier en-US.

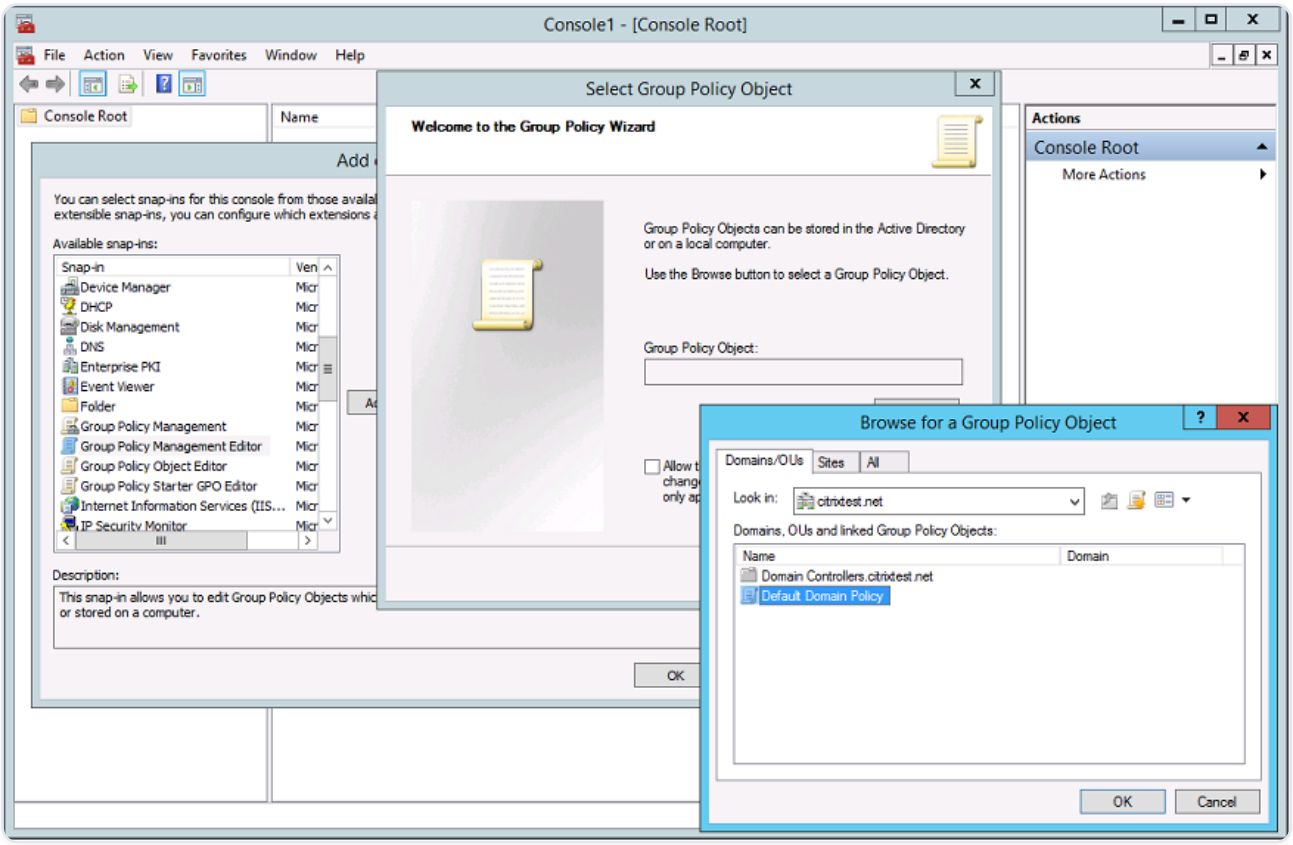


Étape 2. Copiez-les sur vos contrôleurs de domaine et placez-les dans les sous-dossiers C:\Windows\PolicyDefinitions et en-US.

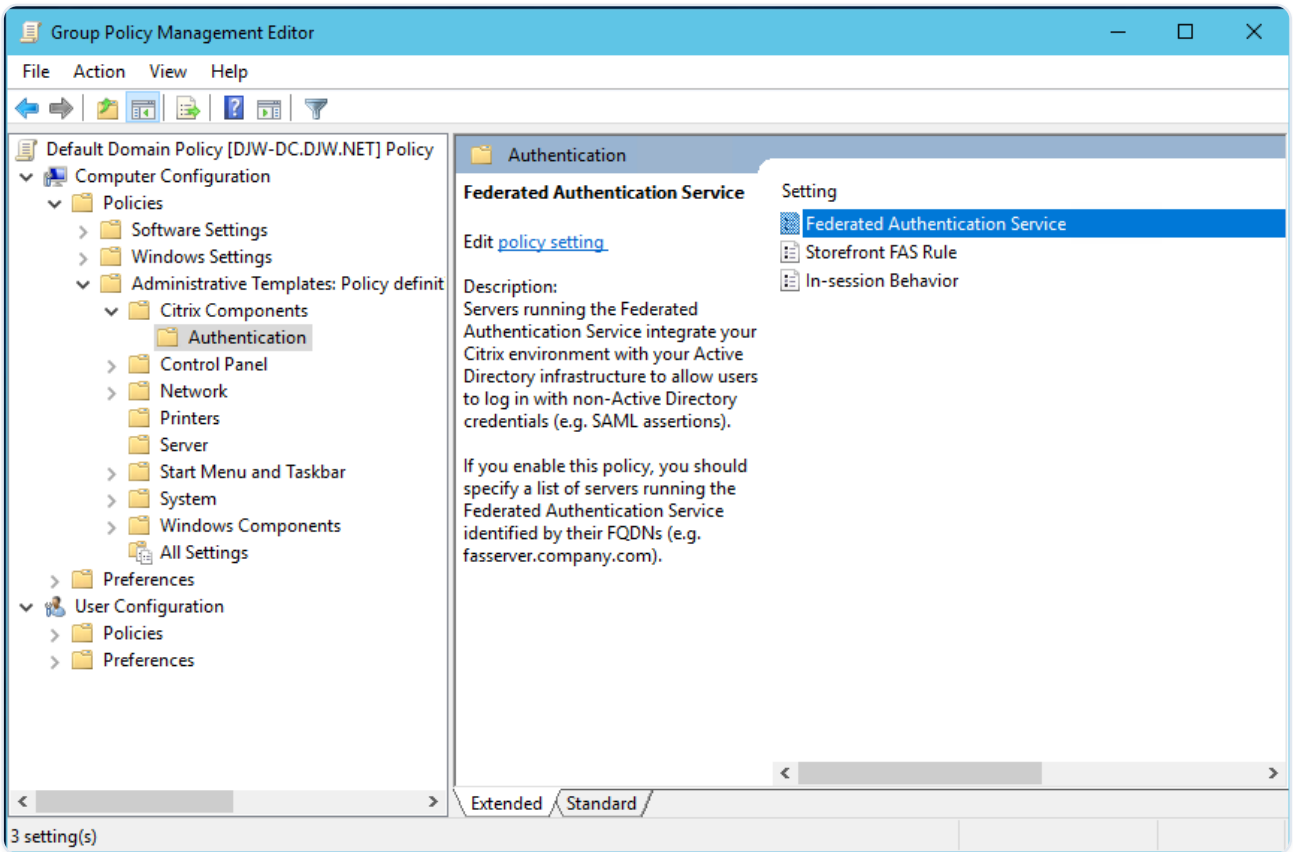
Étape 3. Exécutez la console de gestion Microsoft (mmc.exe à partir de la ligne de commande). Dans la barre de menus, sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**. Ajoutez l'**Éditeur de gestion des stratégies de groupe**.

Lorsque vous êtes invité à sélectionner un objet de stratégie de groupe, sélectionnez **Parcourir**, puis **Stratégie de domaine par défaut**. Vous pouvez également créer et sélectionner un objet de stratégie approprié pour votre environnement, à l'aide des outils de votre choix. La stratégie doit être appliquée à toutes les machines exécutant les logiciels Citrix concernés (VDA, serveurs StoreFront, outils d'administration).

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



Étape 4. Accédez à la stratégie *Service d'authentification fédérée* située dans Configuration ordinateur/Stratégies/Modèles d'administration/Composants Citrix/Authentification.

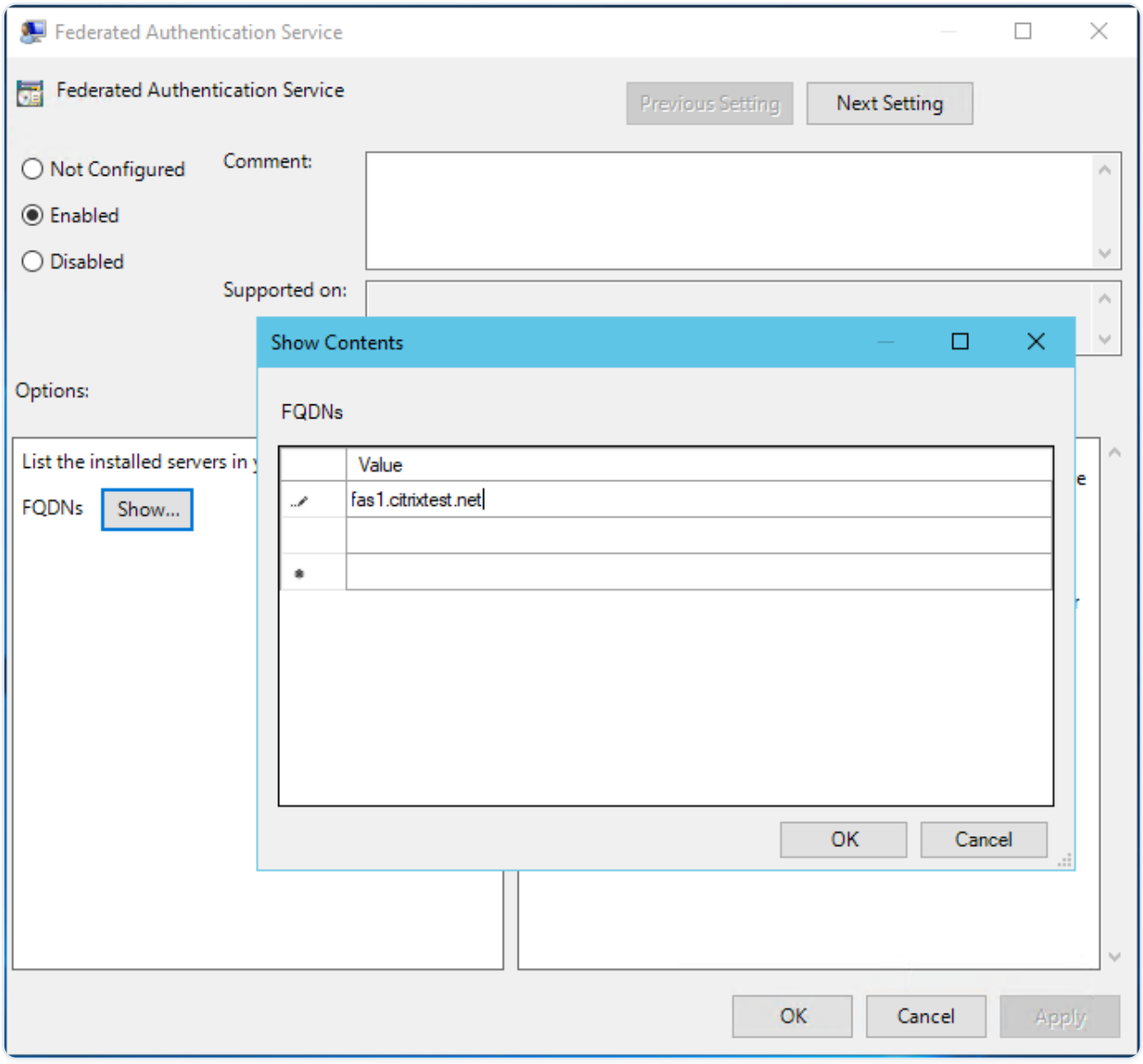


© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Le paramètre de stratégie du Service d'authentification fédérée est disponible uniquement sur l'objet de stratégie de groupe de domaine lorsque vous ajoutez le fichier de modèle CitrixBase.admx/CitrixBase.adml au dossier PolicyDefinitions. Après l'étape 3, le paramètre de stratégie du Service d'authentification fédérée est répertorié dans le dossier **Modèles d'administration > Composants Citrix > Authentification**.

Étape 5. Ouvrez la stratégie du Service d'authentification fédérée et sélectionnez **Activé**. Cela vous permet de sélectionner le bouton **Afficher**, où vous configurez les FQDN de vos serveurs FAS.



Étape 6. Entrez les FQDN des serveurs FAS.

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

IMPORTANT :

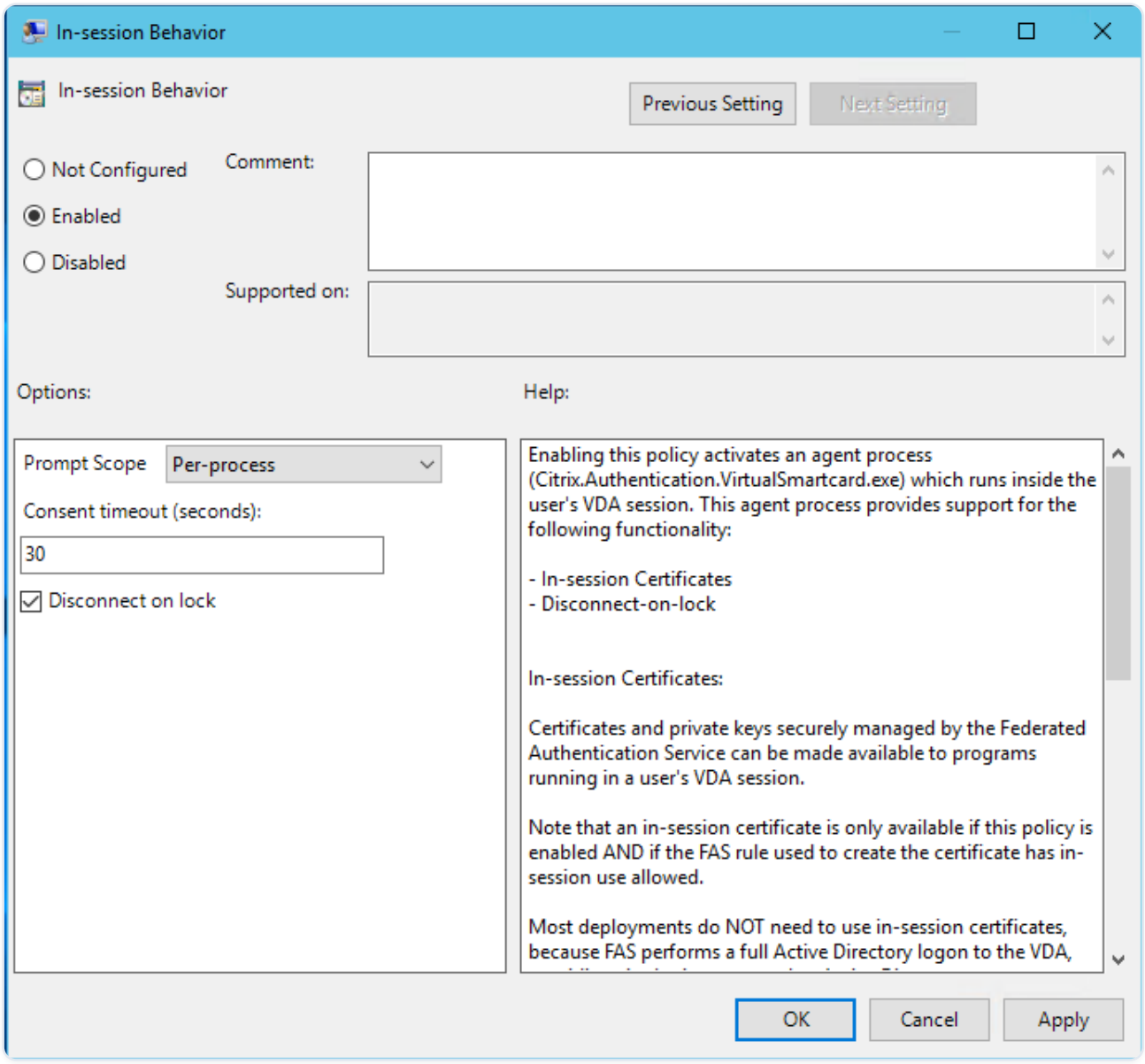
Si vous entrez plusieurs FQDN, l'ordre de la liste doit être cohérent tel qu'il est vu par les VDA, les serveurs StoreFront (le cas échéant) et les serveurs FAS. Consultez Paramètres de stratégie de groupe.

Étape 7. Cliquez sur **OK** pour quitter l'assistant Stratégie de groupe et appliquer les modifications de stratégie de groupe. Vous devrez peut-être redémarrer vos machines (ou exécuter **gpupdate /force** à partir de la ligne de commande) pour que la modification prenne effet.

Comportement en session

Cette stratégie active un processus d'agent dans la session VDA de l'utilisateur qui prend en charge les certificats en session, le consentement et la déconnexion au verrouillage. Les certificats en session ne sont disponibles que si cette stratégie est activée *et* si la règle FAS utilisée pour créer le certificat autorise l'utilisation en session, voir Configurer les règles.

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



Activer active cette stratégie et permet à un processus d'agent FAS de s'exécuter dans la session VDA de l'utilisateur.

Désactiver désactive la stratégie et empêche le processus d'agent FAS de s'exécuter.

Portée de l'invite

Si cette stratégie est activée, **Portée de l'invite** contrôle la manière dont les utilisateurs sont invités à donner leur consentement pour autoriser une application à utiliser un certificat en session. Il existe trois options :

- **Aucun consentement requis**—Cette option désactive l'invite de sécurité et les clés privées sont utilisées silencieusement.
- **Consentement par processus**—Chaque programme en cours d'exécution demande individuellement le consentement.

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

- **Consentement par session**—Une fois que l'utilisateur a cliqué sur **OK**, cela s'applique à tous les programmes de la session.

Délai d'expiration du consentement

Si cette stratégie est activée, **Délai d'expiration du consentement** contrôle la durée (en secondes) du consentement. Par exemple, avec 300 secondes, les utilisateurs voient une invite toutes les cinq minutes. Une valeur de zéro invite les utilisateurs pour chaque opération de clé privée.

Déconnexion au verrouillage

Si cette stratégie est activée, la session de l'utilisateur est automatiquement déconnectée lorsqu'il verrouille l'écran. Cette fonctionnalité offre un comportement similaire à la stratégie de « déconnexion au retrait de la carte à puce » et est utile dans les situations où les utilisateurs ne disposent pas d'informations d'identification de connexion Active Directory.

REMARQUE :

La stratégie de déconnexion au verrouillage s'applique à toutes les sessions sur le VDA.

Utilisation de la console d’administration du service d’authentification fédérée

REMARQUE :

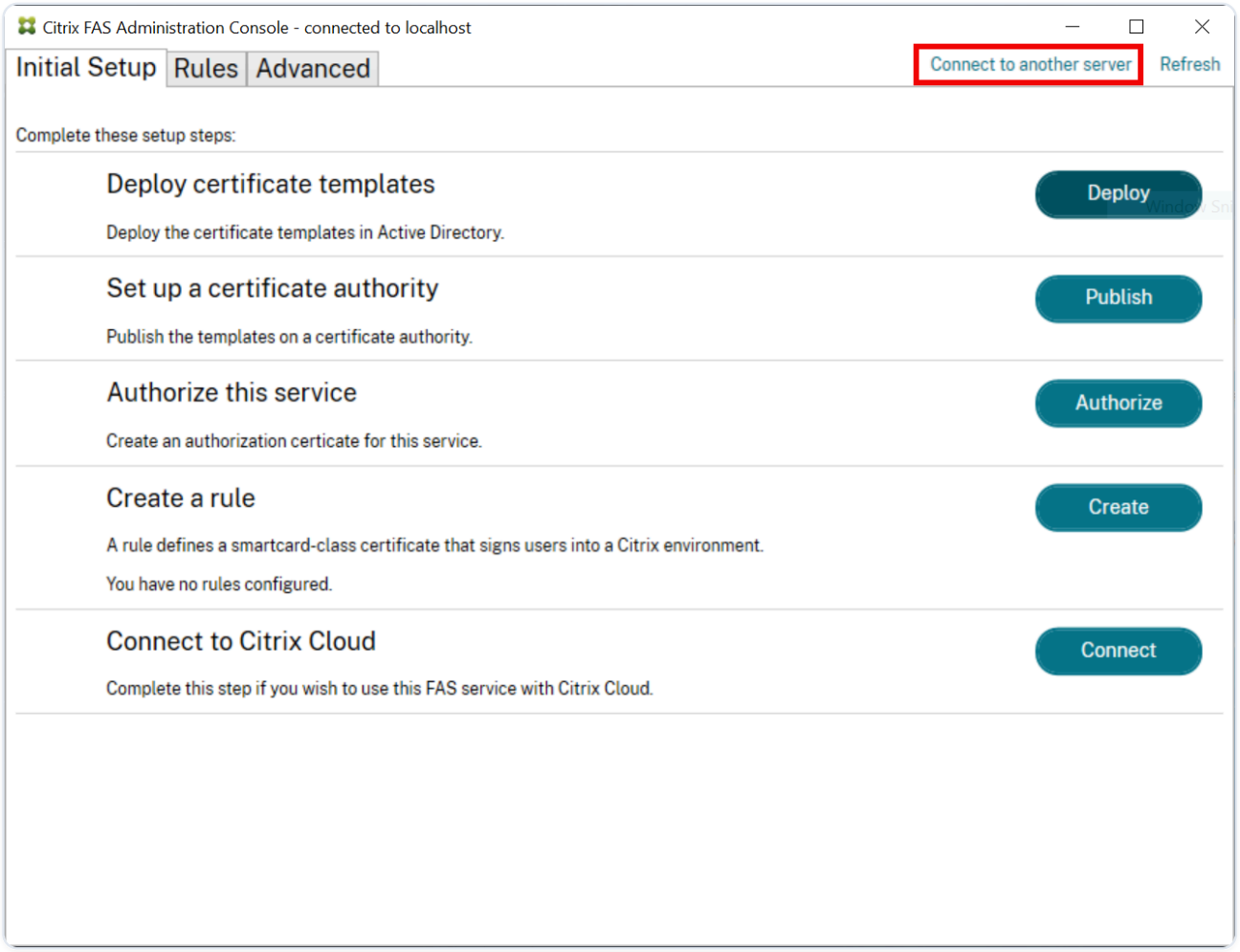
Bien que la console d’administration FAS convienne à la plupart des déploiements, l’interface PowerShell offre des options plus avancées. Pour plus d’informations sur les cmdlets PowerShell FAS, consultez la section Cmdlets PowerShell.

La console d’administration FAS est installée dans le cadre de FAS. Une icône (Citrix Federated Authentication Service) est placée dans le menu Démarrer.

La première fois que la console d’administration est utilisée, elle vous guide à travers un processus qui déploie des modèles de certificat, configure l’autorité de certification et autorise FAS à utiliser l’autorité de certification. Certaines étapes peuvent également être effectuées manuellement à l’aide des outils de configuration du système d’exploitation.

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

La console d'administration FAS se connecte au service FAS local par défaut. Si nécessaire, vous pouvez vous connecter à un service distant en utilisant **Connecter à un autre serveur** en haut à droite de la console.



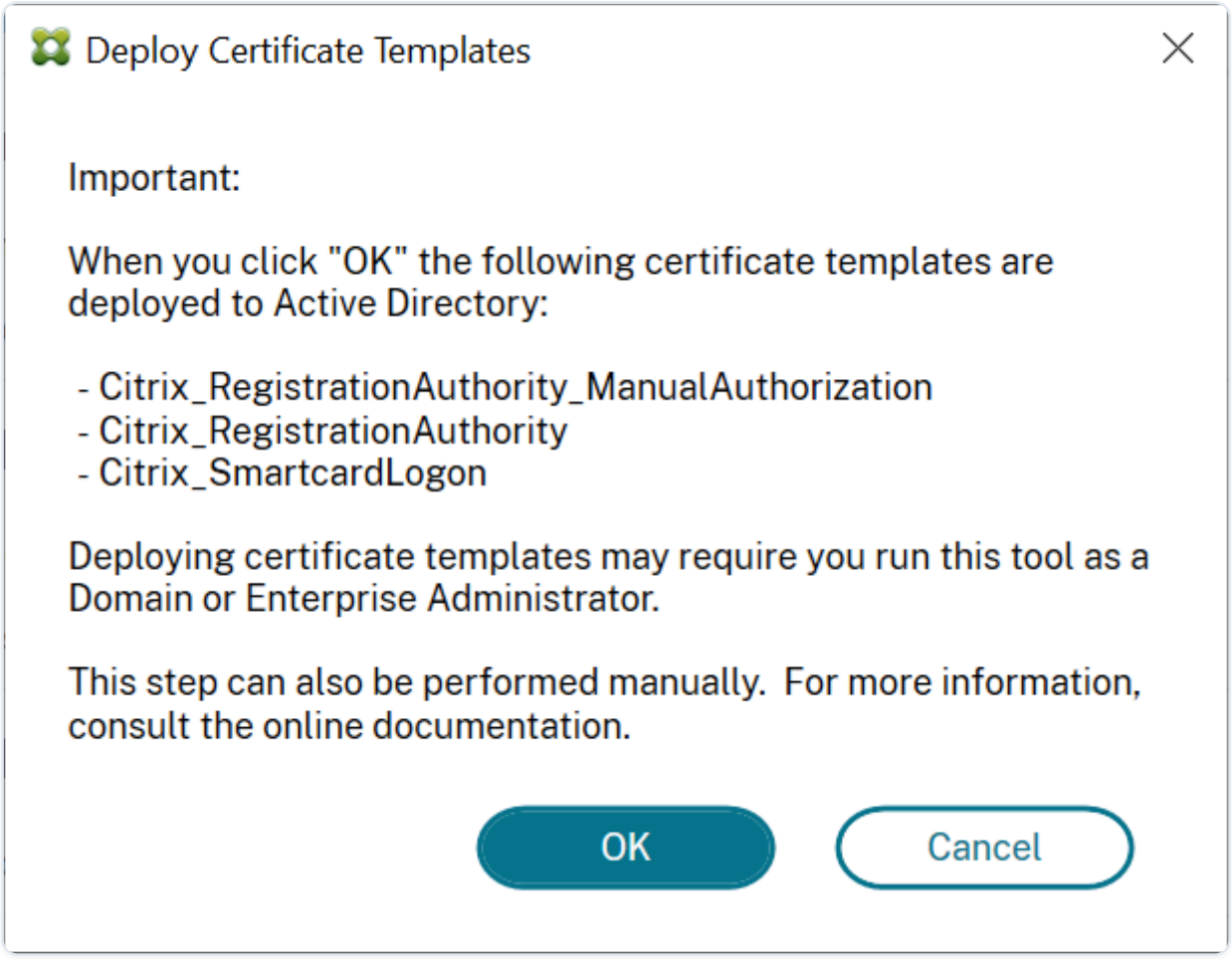
Déployer des modèles de certificat

Pour éviter les problèmes d'interopérabilité avec d'autres logiciels, FAS fournit trois modèles de certificat Citrix pour son propre usage.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

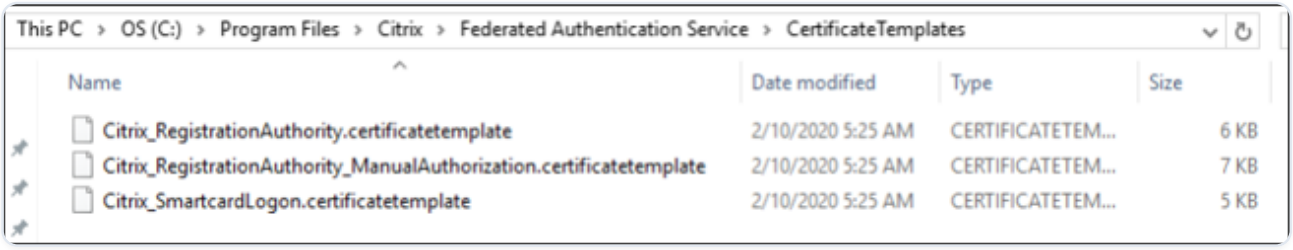
Ces modèles doivent être enregistrés avec Active Directory. Cliquez sur le bouton **Déployer**, puis sur **OK**.

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



La configuration des modèles se trouve dans les fichiers XML avec l'extension .certificatetemplate qui sont installés avec FAS dans :

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



Si vous n'avez pas l'autorisation d'installer ces fichiers de modèle, transmettez-les à votre administrateur Active Directory.

Pour installer manuellement les modèles, vous pouvez exécuter les commandes PowerShell suivantes à partir du dossier contenant les modèles :

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

$CertEnrol = New-Object -ComObject
```

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

```
X509Enrollment.CX509EnrollmentPolicyWebService

$CertEnrol.InitializeImport($template)

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

$writabletemplate = New-Object -ComObject
X509Enrollment.CX509CertificateTemplateADWritable

$writabletemplate.Initialize($comtemplate)

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

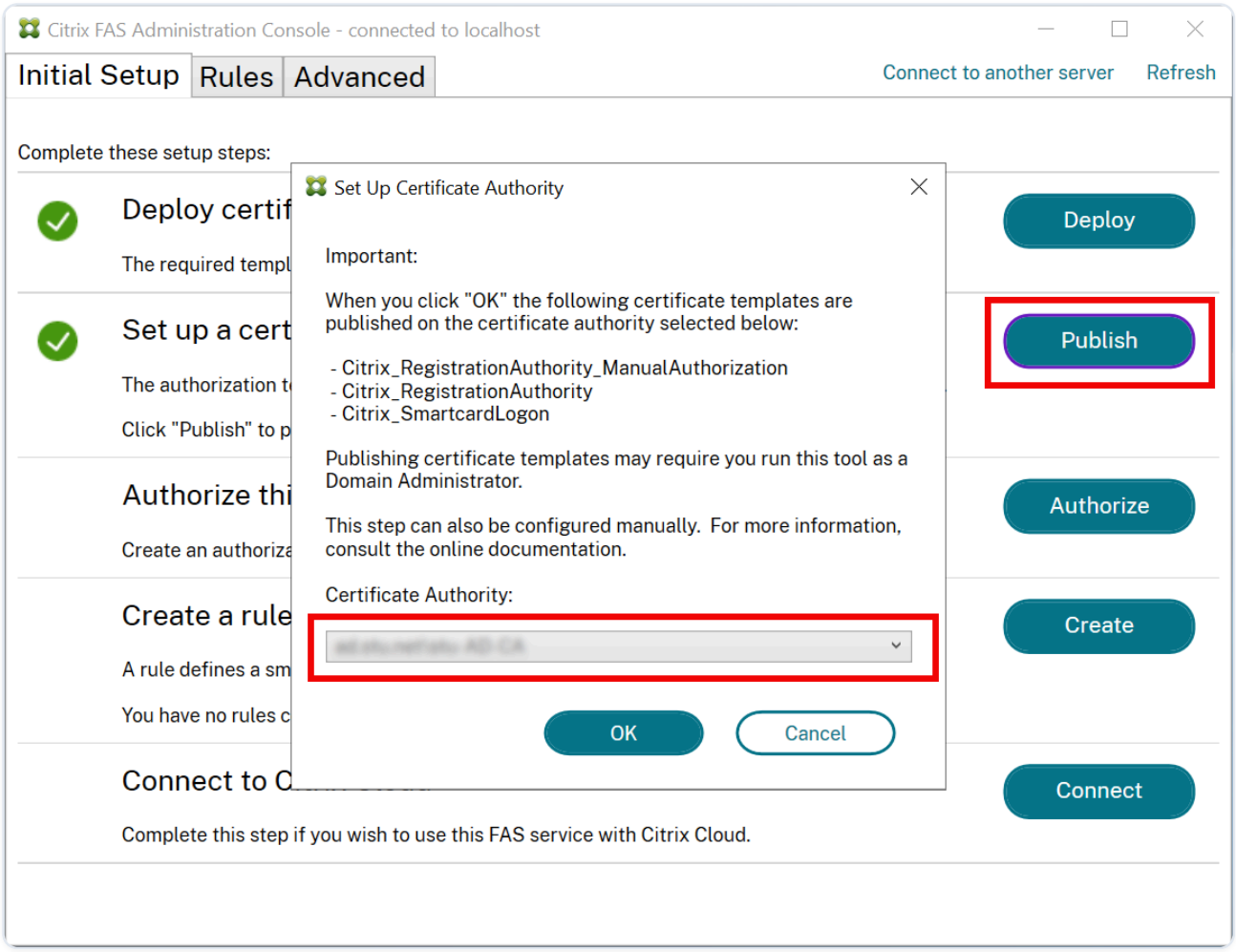
Configurer les services de certificats Active Directory

Après l'installation des modèles de certificat Citrix, ils doivent être publiés sur un ou plusieurs serveurs d'autorité de certification Microsoft Enterprise. Reportez-vous à la documentation Microsoft pour savoir comment déployer les services de certificats Active Directory.

Si les modèles ne sont pas publiés sur au moins un serveur, utilisez **Configurer l'autorité de certification** pour les publier. Vous devez effectuer cette opération en tant qu'utilisateur disposant des autorisations nécessaires pour administrer l'autorité de certification.

(Les modèles de certificat peuvent également être publiés à l'aide de la console d'autorité de certification Microsoft.)

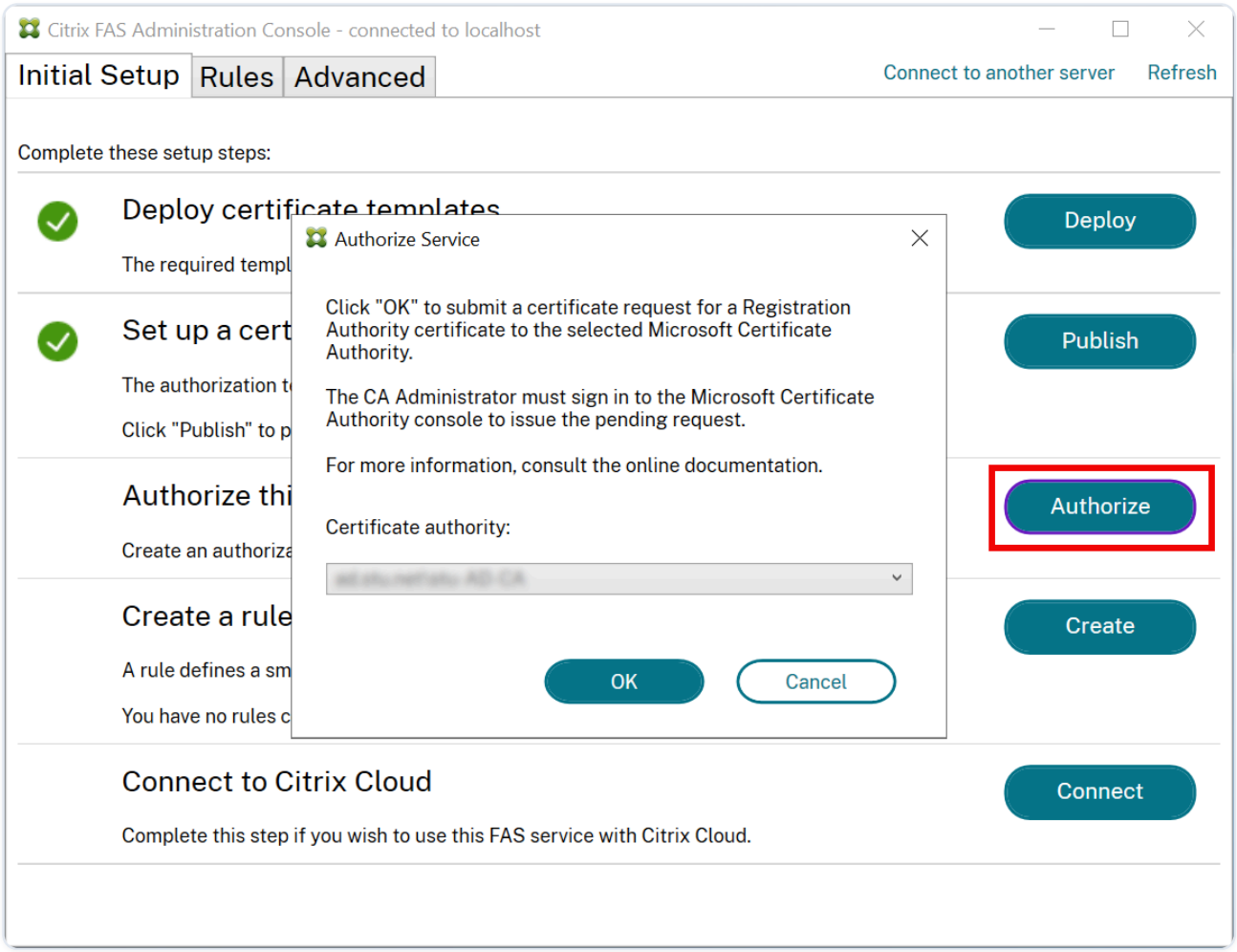
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Autoriser le service d'authentification fédérée

Cette étape initialise l'autorisation de FAS. La console d'administration utilise le modèle Citrix_RegistrationAuthority_ManualAuthorization pour générer une demande de certificat, puis l'envoie à l'une des autorités de certification qui publient ce modèle.

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

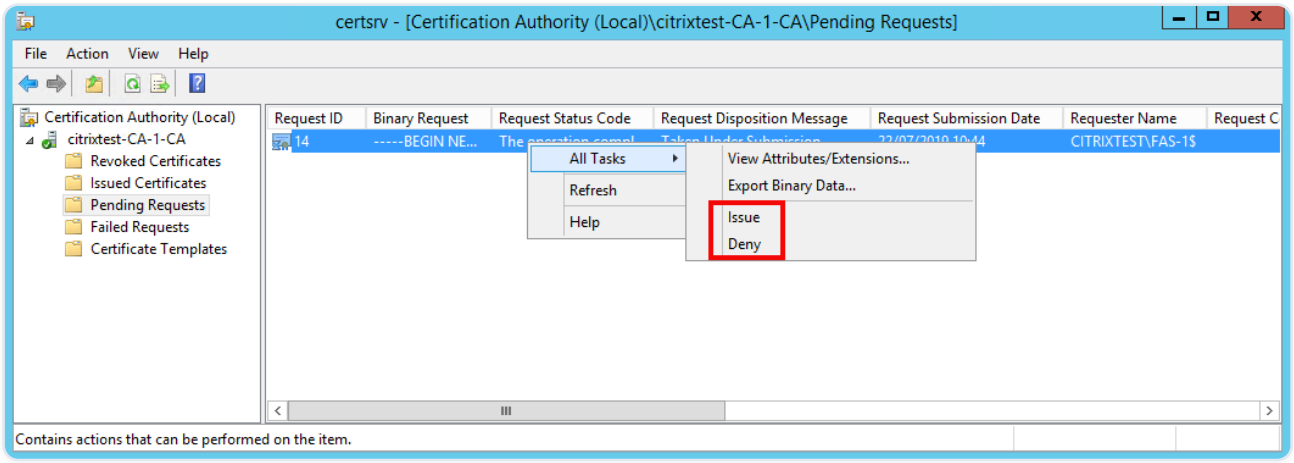


Une fois la demande envoyée, elle apparaît dans la liste **Demandes en attente** de la console d'autorité de certification Microsoft en tant que demande en attente du compte machine FAS. L'administrateur de l'autorité de certification doit émettre ou refuser la demande avant que la configuration de FAS puisse se poursuivre.

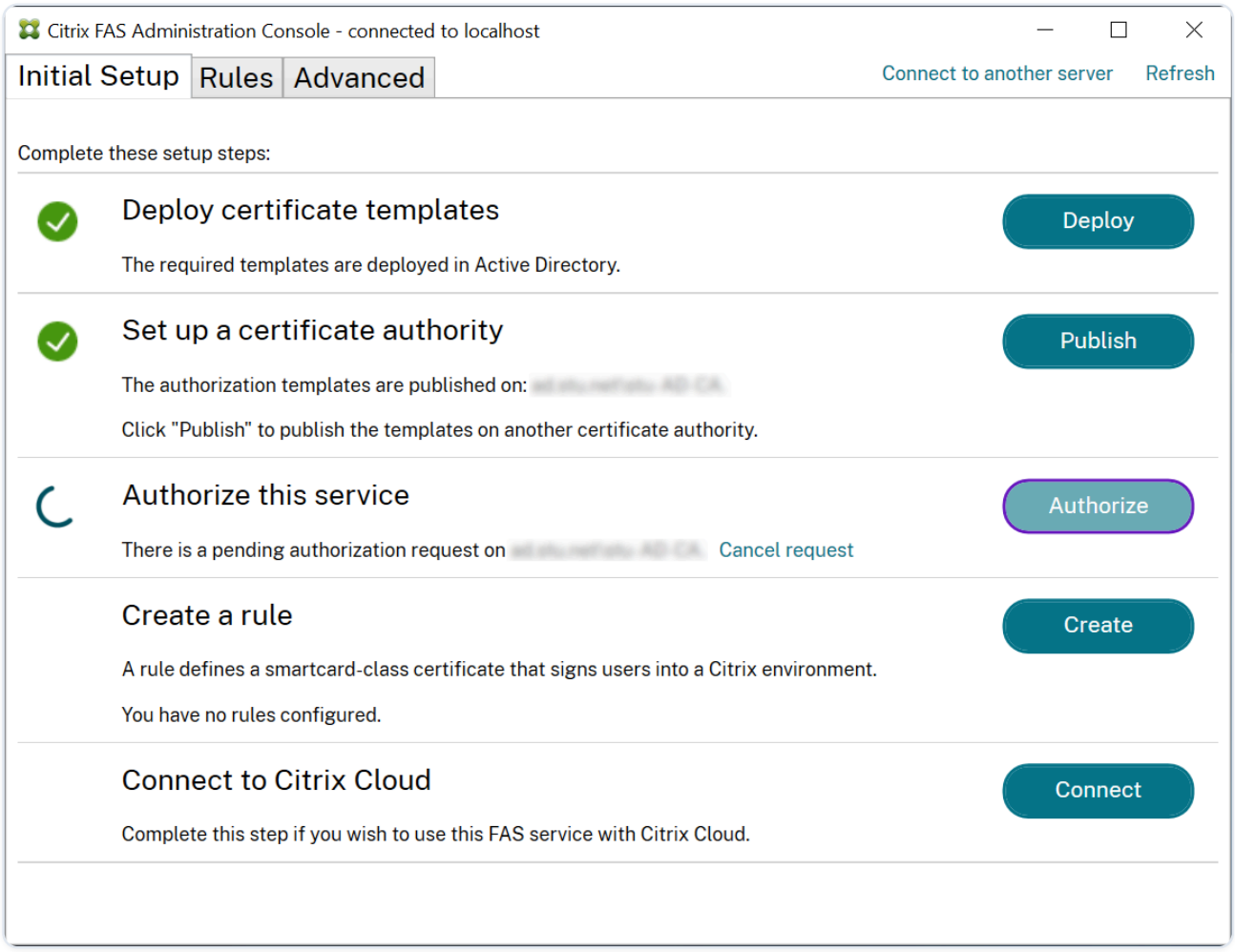
La console d'administration FAS affiche un indicateur de chargement jusqu'à ce que l'administrateur choisisse **Émettre** ou **Refuser**.

Dans la console d'autorité de certification Microsoft, cliquez avec le bouton droit sur **Toutes les tâches**, puis sélectionnez **Émettre** ou **Refuser** pour la demande de certificat. Si vous choisissez **Émettre**, la console d'administration FAS affiche le certificat d'autorisation. Si vous choisissez **Refuser**, la console affiche un message d'erreur.

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



La console d'administration FAS détecte automatiquement la fin de ce processus. Cela peut prendre quelques minutes.



Configurer les règles

FAS utilise les règles pour autoriser l'émission de certificats pour l'ouverture de session VDA et l'utilisation en session, comme indiqué par StoreFront. Chaque règle spécifie les serveurs

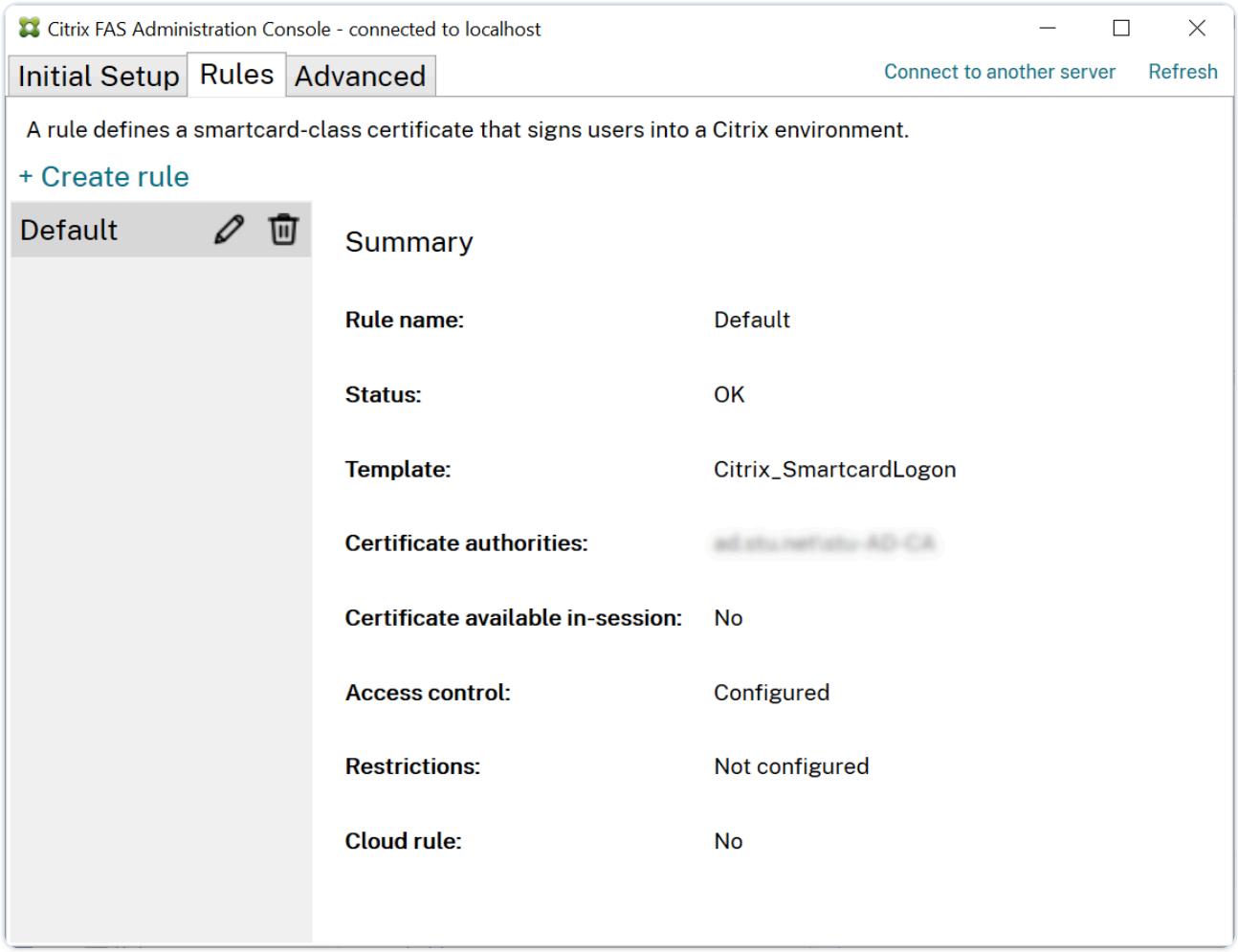
© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFront qui sont approuvés pour demander des certificats, l'ensemble des utilisateurs pour lesquels ils peuvent être demandés, et l'ensemble des machines VDA autorisées à les utiliser.

FAS nécessite qu'au moins une règle soit créée et configurée. Nous vous recommandons de créer une règle nommée « default », car par défaut, StoreFront demande la règle nommée « default » lors de la communication avec FAS.

Vous pouvez créer des règles personnalisées supplémentaires pour référencer différents modèles de certificat et autorités de certification, et les configurer pour qu'elles aient des propriétés et des autorisations différentes. Ces règles peuvent être configurées pour être utilisées par différents serveurs StoreFront ou par Workspace. Configurez les serveurs StoreFront pour qu'ils demandent la règle personnalisée par son nom à l'aide des options de configuration de la stratégie de groupe.

Cliquez sur **Créer** (ou **Créer une règle** dans l'onglet « Règles ») pour démarrer l'assistant de création de règle qui recueille les informations nécessaires à la création de la règle. L'onglet « Règles » affiche un résumé de chaque règle.



Les informations suivantes sont recueillies par l'assistant :

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

Modèle: Le modèle de certificat utilisé pour émettre les certificats utilisateur. Il doit s'agir du modèle Citrix_SmartcardLogon, ou d'une copie modifiée de celui-ci (voir Modèles de certificat).

Autorité de certification: L'autorité de certification qui émet les certificats utilisateur. Le modèle doit être publié par l'autorité de certification. FAS prend en charge l'ajout de plusieurs autorités de certification pour le basculement et l'équilibrage de charge. Assurez-vous que le statut indique « Modèle disponible » pour l'autorité de certification que vous choisissez. Voir Administration de l'autorité de certification.

Utilisation en session: L'option **Autoriser l'utilisation en session** contrôle si un certificat peut être utilisé après l'ouverture de session sur le VDA.

- **Autoriser l'utilisation en session** non sélectionné (par défaut, *recommandé*)—le certificat est utilisé uniquement pour l'ouverture de session ou la reconnexion, et les utilisateurs n'ont pas accès au certificat après l'authentification.
- **Autoriser l'utilisation en session** sélectionné—les utilisateurs ont accès au certificat après l'authentification. La plupart des clients ne devraient pas sélectionner cette option. Les ressources accessibles depuis la session VDA, telles que les sites web intranet ou les partages de fichiers, peuvent être accédées à l'aide de l'authentification unique Kerberos, et par conséquent, un certificat en session n'est pas requis.

  Si vous sélectionnez **Autoriser l'utilisation en session**, la stratégie de groupe Comportement en session doit également être activée et appliquée au VDA. Les certificats sont ensuite placés dans le magasin de certificats personnel de l'utilisateur après l'ouverture de session pour l'utilisation des applications. Par exemple, si vous avez besoin d'une authentification TLS pour les serveurs web au sein de la session VDA, le certificat peut être utilisé par Internet Explorer.

Contrôle d'accès : Liste des machines de serveur StoreFront approuvées qui sont autorisées à demander des certificats pour l'ouverture de session ou la reconnexion des utilisateurs. Pour toutes ces autorisations, vous pouvez ajouter des objets ou des groupes AD individuels.

IMPORTANT :

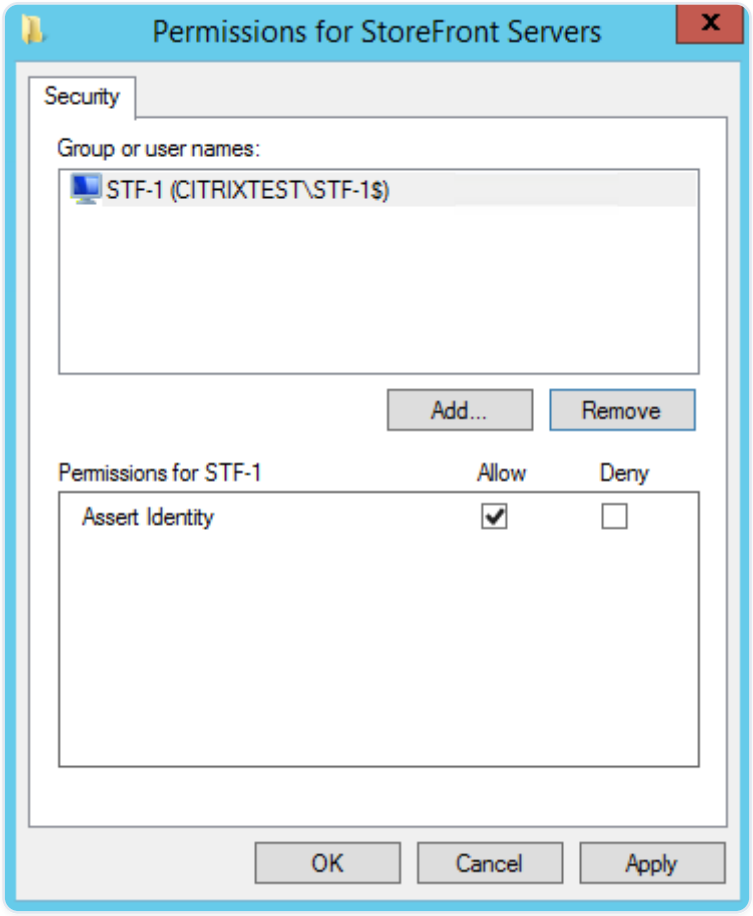
Le paramètre **Contrôle d'accès** est critique pour la sécurité et doit être géré avec soin.

Remarque :

Si vous utilisez le serveur FAS uniquement avec Citrix Cloud, vous n'avez pas besoin de configurer le contrôle d'accès. Lorsqu'une règle est utilisée par Citrix Cloud, les autorisations d'accès StoreFront sont ignorées. Vous pouvez utiliser la même règle avec Citrix Cloud et avec un

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

déploiement StoreFront sur site. Les autorisations d'accès StoreFront sont toujours appliquées lorsque la règle est utilisée par un StoreFront sur site.
L'autorisation par défaut ("Affirmer l'identité" autorisée) refuse tout. Par conséquent, vous devez autoriser explicitement vos serveurs StoreFront.



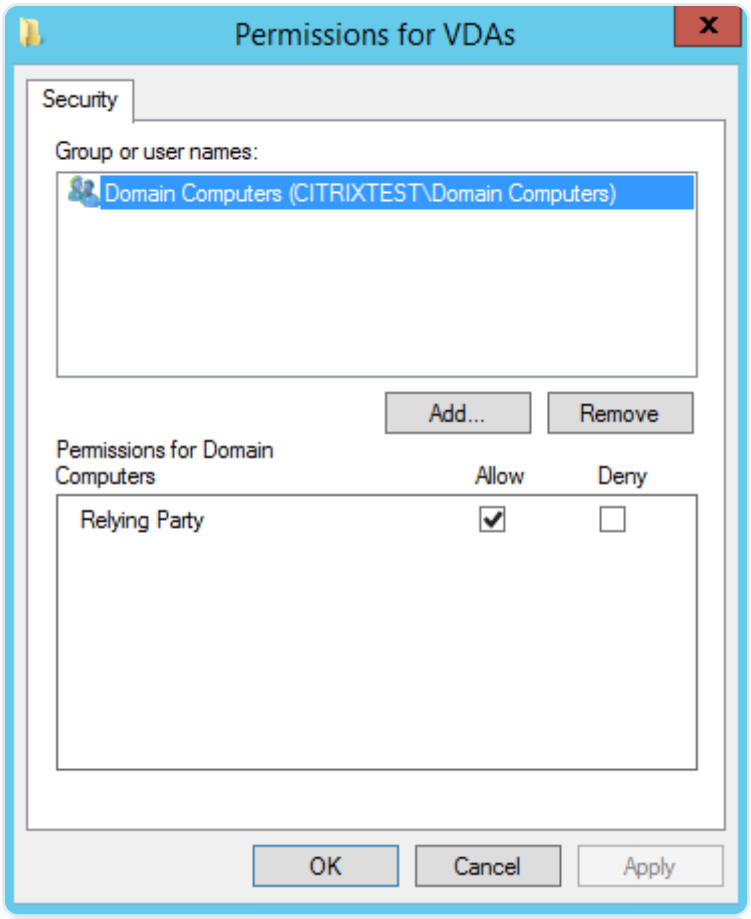
Restrictions : Liste des machines VDA qui peuvent connecter les utilisateurs à l'aide de FAS et liste des utilisateurs auxquels des certificats peuvent être délivrés via FAS.

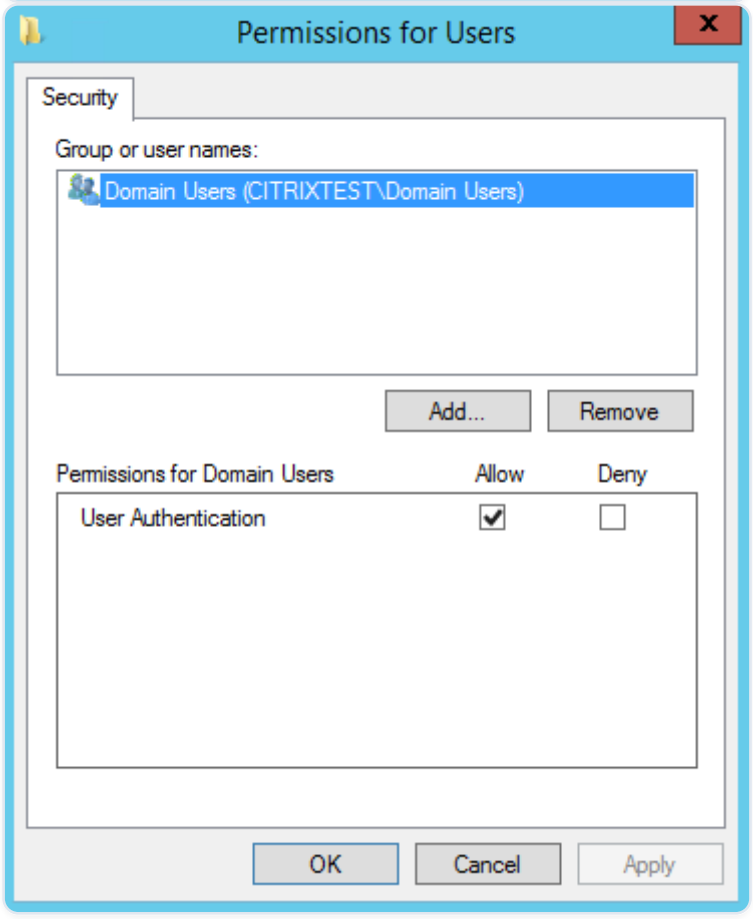
- **Gérer les autorisations VDA** vous permet de spécifier quels VDA peuvent utiliser FAS pour connecter l'utilisateur. La liste des VDA est par défaut sur Ordinateurs du domaine.
- **Gérer les autorisations utilisateur** vous permet de spécifier quels utilisateurs peuvent utiliser FAS pour se connecter à un VDA. La liste des utilisateurs est par défaut sur Utilisateurs du domaine.

REMARQUE :

Si le serveur FAS se trouve dans un domaine différent de celui des VDA et des utilisateurs, les restrictions par défaut doivent être modifiées.

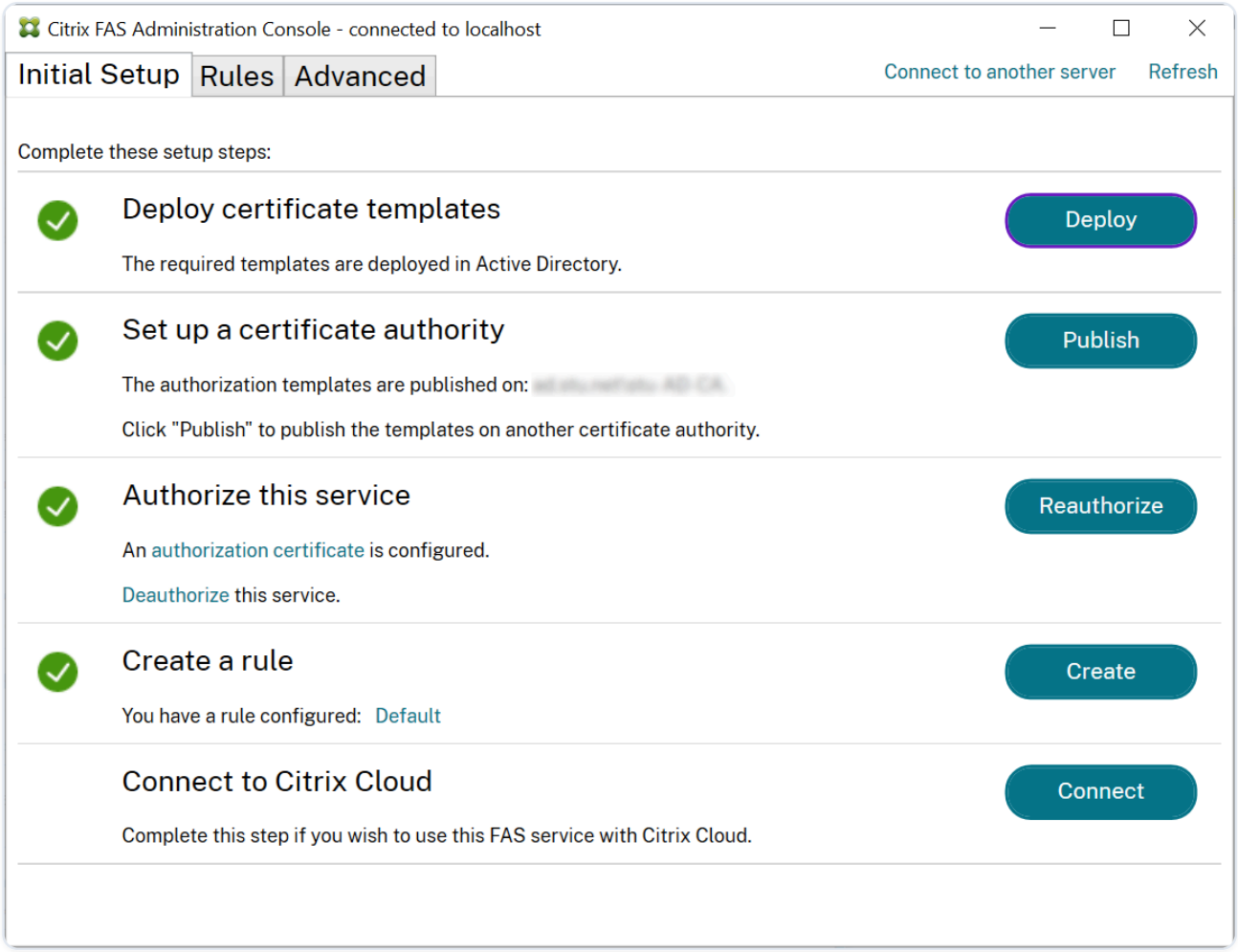
© 1997–2026 Citrix Systems, Inc. All rights reserved.





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

Règle de cloud : Indique si la règle est appliquée lorsque des assertions d'identité sont reçues de Citrix Workspace. Lorsque vous vous connectez à Citrix Cloud, vous choisissez la règle à utiliser pour Citrix Cloud. Vous pouvez également modifier la règle après vous être connecté à Citrix Cloud à partir d'un lien dans la section **Se connecter à Citrix Cloud**.

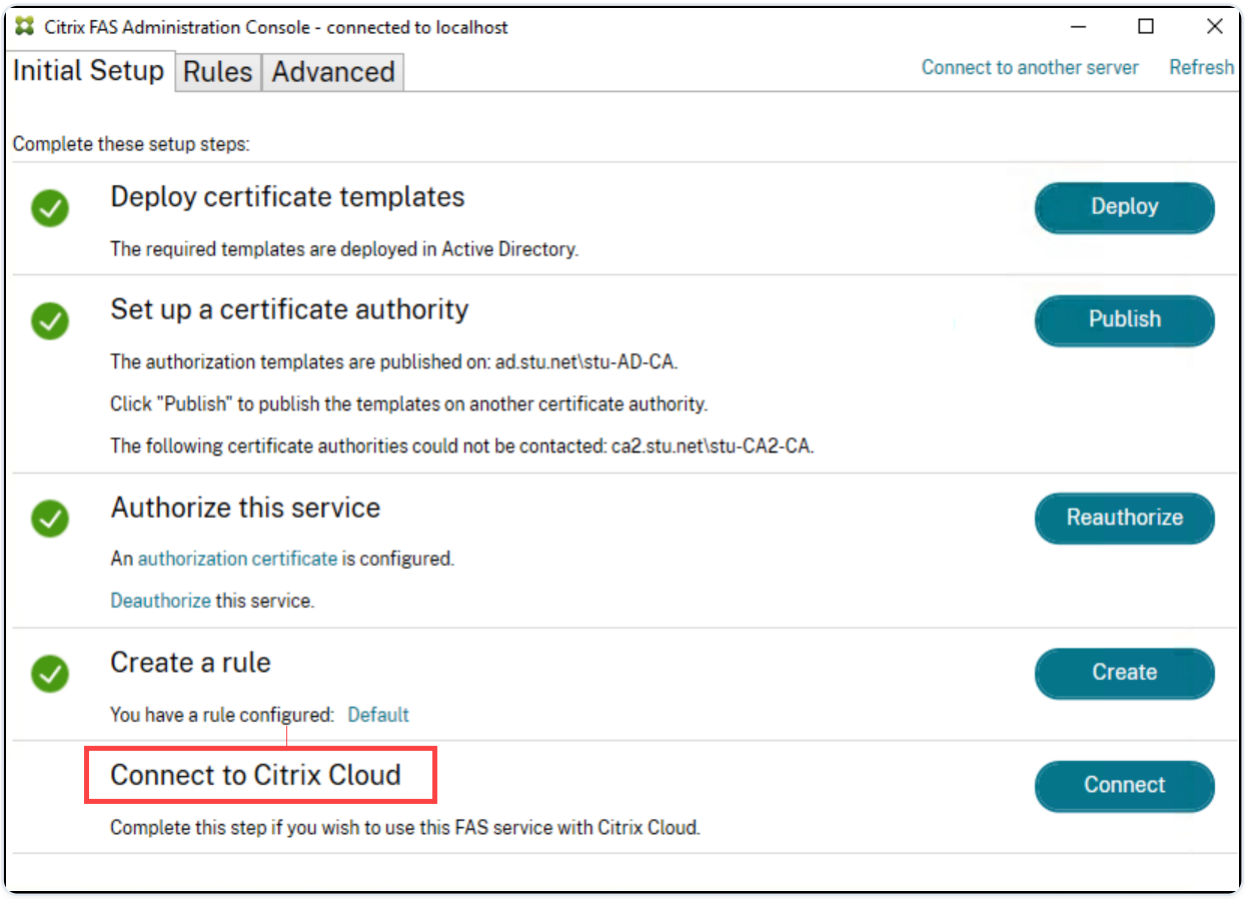


Se connecter à Citrix Cloud

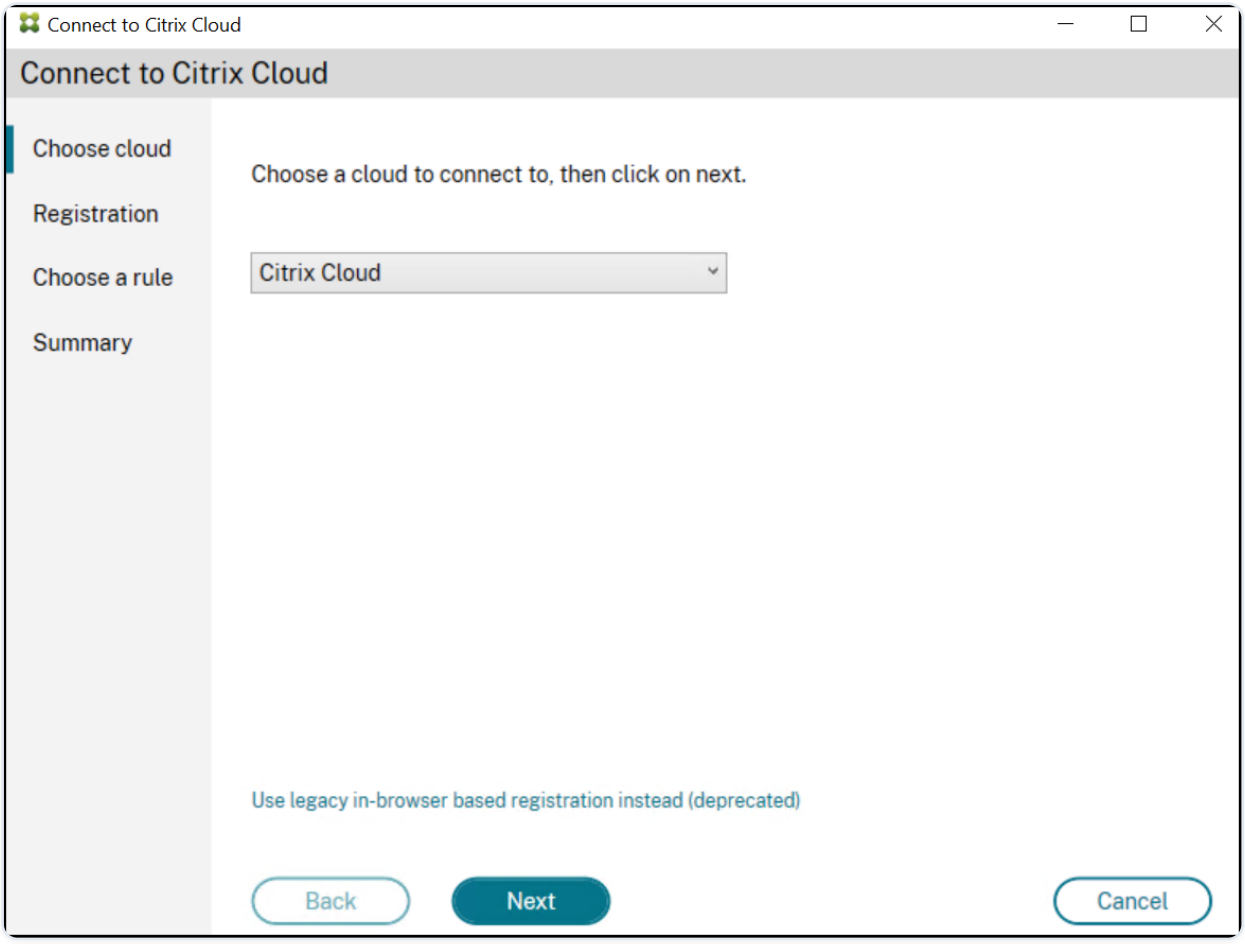
Vous pouvez connecter le serveur FAS à Citrix Cloud avec Citrix Workspace. Consultez cet article de Citrix Workspace.

1. Dans l'onglet Configuration initiale, sous **Se connecter à Citrix Cloud**, cliquez sur **Connecter**.

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



2. Sélectionnez le cloud auquel vous souhaitez vous connecter et cliquez sur **Suivant**.

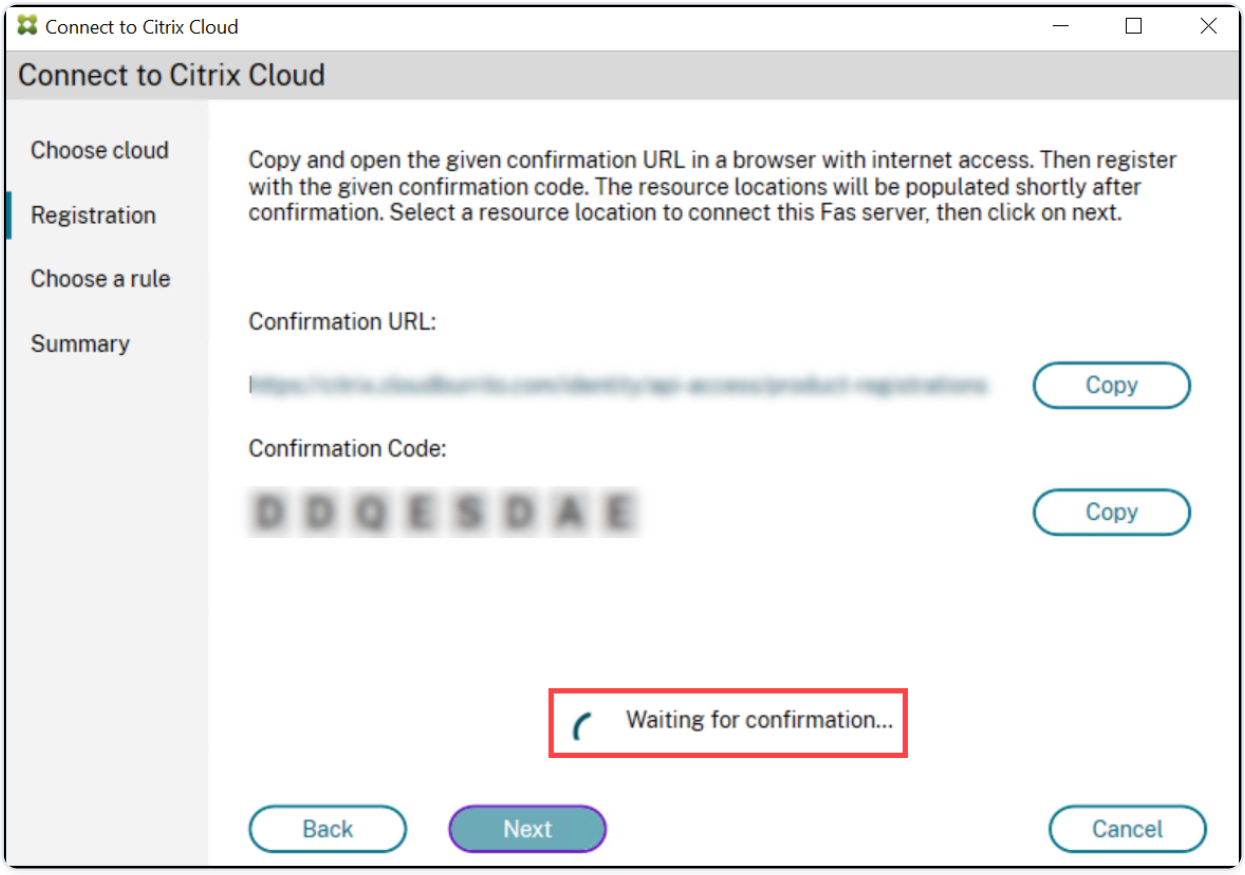


© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

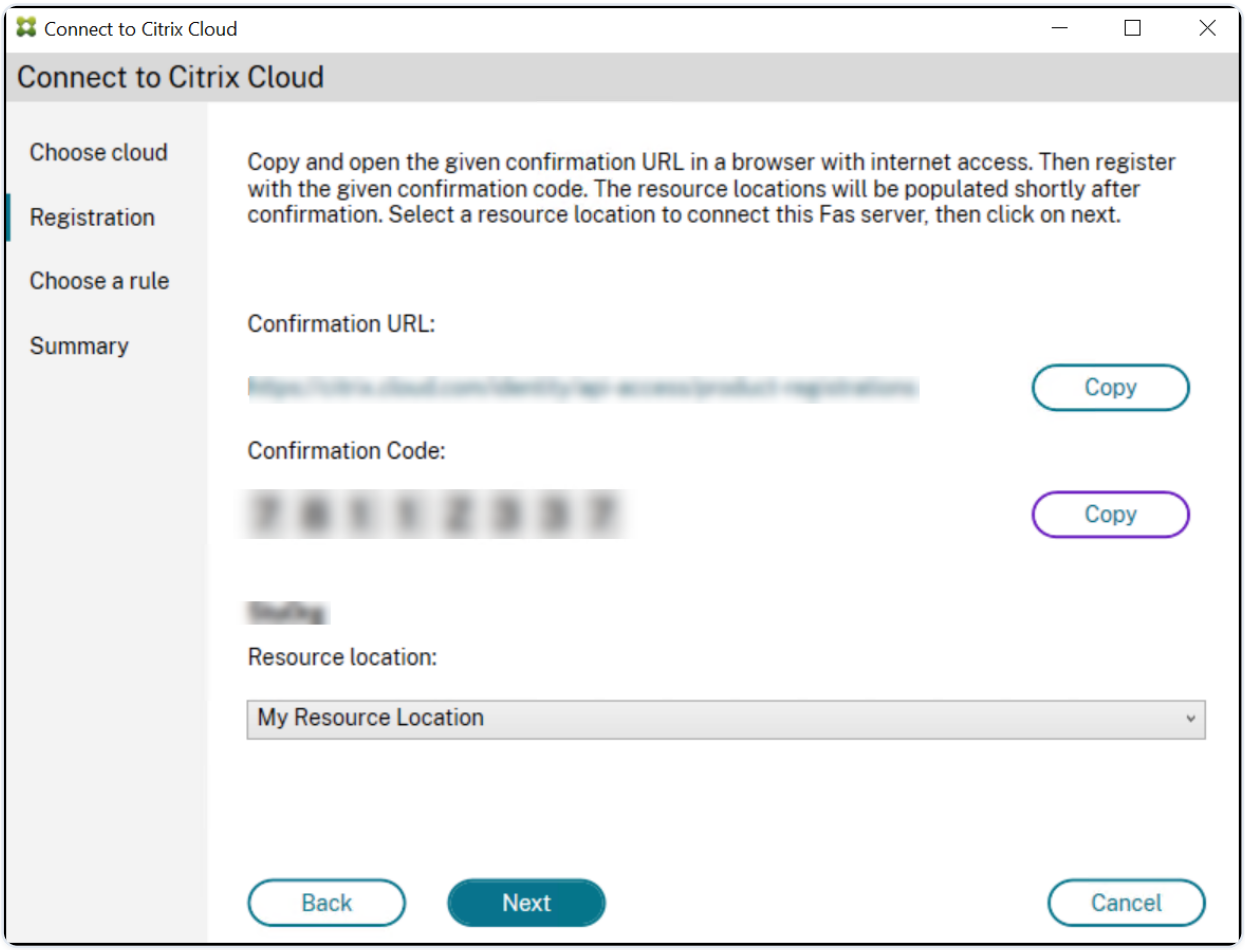
Seul **Citrix Cloud** est disponible dans l'aperçu.

3. La fenêtre affiche un code d'enregistrement unique, qui doit être approuvé dans Citrix Cloud. Pour plus d'informations, consultez Enregistrer les produits sur site auprès de Citrix Cloud.



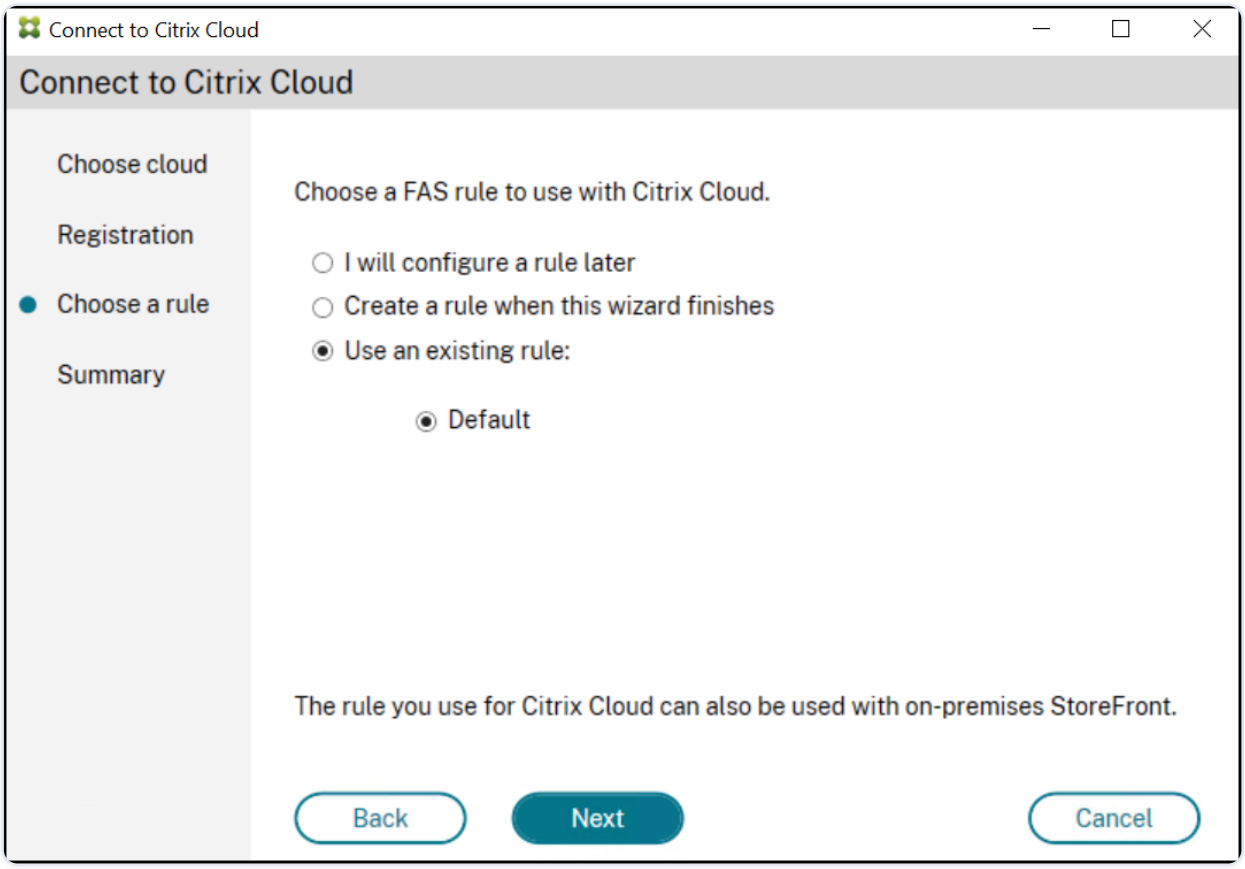
4. Une fois le code d'enregistrement validé, sélectionnez l'**emplacement des ressources** souhaité dans la liste déroulante.

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

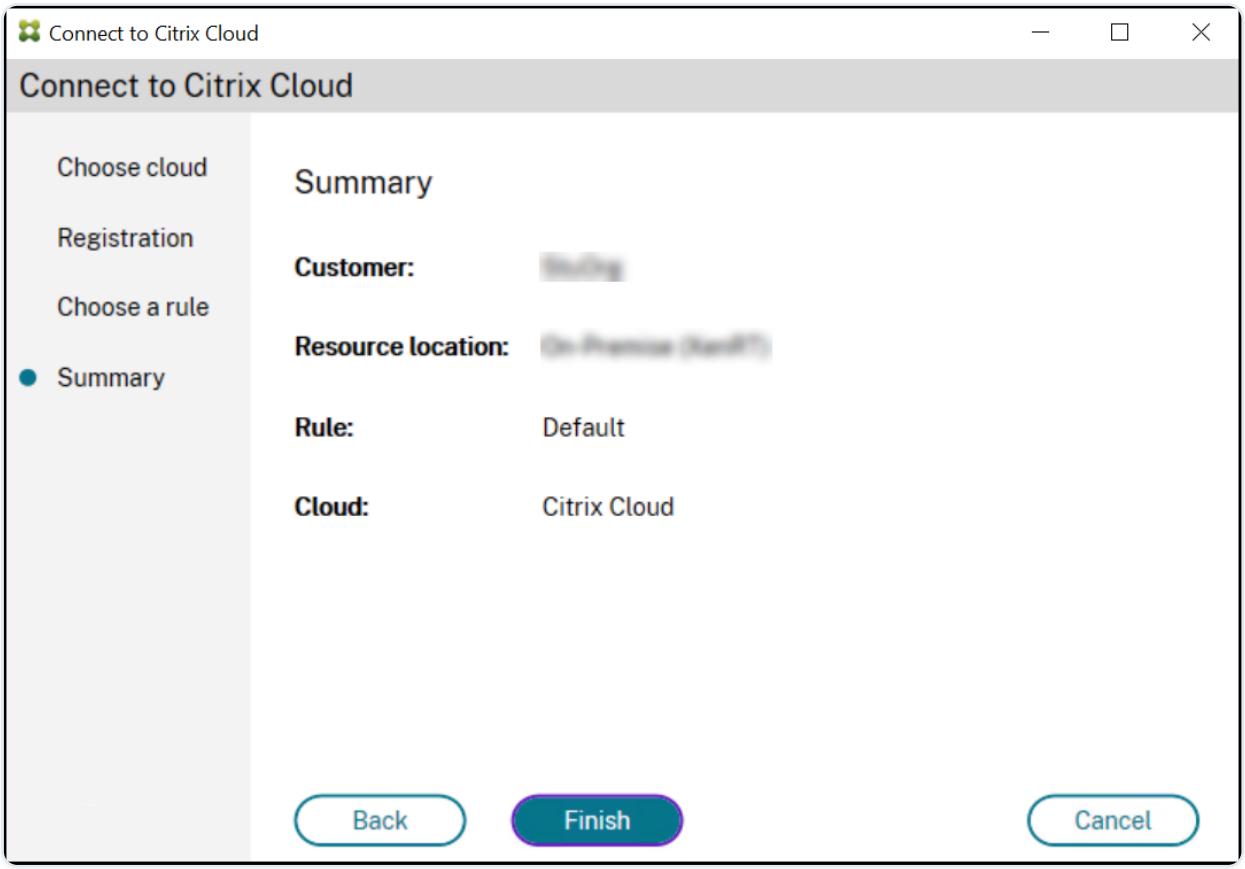


5. Sélectionnez le compte client, le cas échéant, et sélectionnez l'emplacement des ressources où vous souhaitez connecter le serveur FAS. Cliquez sur **Continuer**, puis fermez la fenêtre de confirmation.
6. Dans la section **Choisir une règle**, utilisez une règle existante ou créez-en une. Cliquez sur **Suivant**.

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



7. Dans la section **Résumé**, cliquez sur **Terminer** pour finaliser la connexion à Citrix Cloud.



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

Citrix Cloud enregistre le serveur FAS et l'affiche sur la page Emplacements des ressources de votre compte Citrix Cloud.

Se déconnecter de Citrix Cloud

Après avoir supprimé le serveur FAS de votre emplacement de ressources Citrix Cloud, comme décrit dans cet article de Citrix Workspace, dans **Se connecter à Citrix Cloud**, sélectionnez **Désactiver**.

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

Configuration avancée

Les articles de cette section fournissent des conseils de configuration et de gestion avancés pour le service d’authentification fédérée (FAS).

Informations connexes

- La référence principale pour l’installation et la configuration initiale de FAS est l’article Installer et configurer.
- L’article Architectures de déploiement fournit des résumés des principales architectures FAS, ainsi que des liens vers d’autres articles sur les architectures plus complexes.

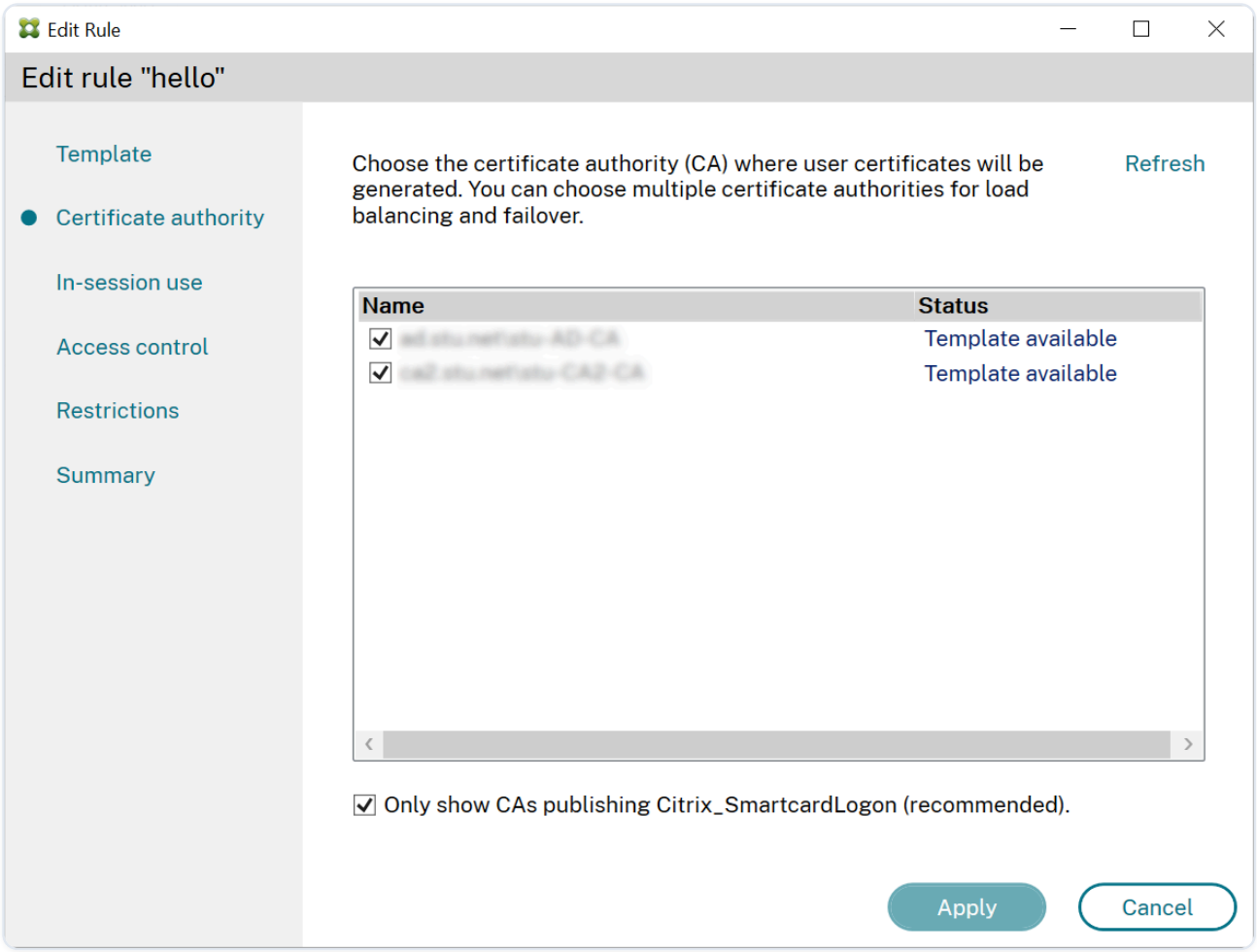
Configuration de l'autorité de certification

Cet article décrit la configuration avancée du service d'authentification fédérée (FAS) pour l'intégration avec les serveurs d'autorité de certification (CA). La plupart de ces configurations ne sont pas prises en charge par la console d'administration FAS. Les instructions utilisent les API PowerShell fournies par FAS. Vous devez avoir une connaissance de base de PowerShell avant d'exécuter les instructions de cet article.

Configurer plusieurs serveurs d'autorité de certification pour une utilisation dans FAS

Vous pouvez utiliser la console d'administration FAS pour configurer FAS avec plusieurs autorités de certification lors de la création ou de la modification d'une règle :

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



Toutes les autorités de certification que vous sélectionnez doivent publier le modèle de certificat Citrix_SmartcardLogon (ou tout autre modèle que vous avez choisi dans votre règle).

Si l'une des autorités de certification que vous souhaitez utiliser ne publie pas le modèle souhaité, effectuez l'étape Configurer une autorité de certification pour cette autorité de certification.

REMARQUE :

Vous n'avez pas besoin d'effectuer l'étape Autoriser ce service pour chaque autorité de certification, car le certificat d'autorisation configuré à cette étape peut être utilisé sur n'importe laquelle de vos autorités de certification.

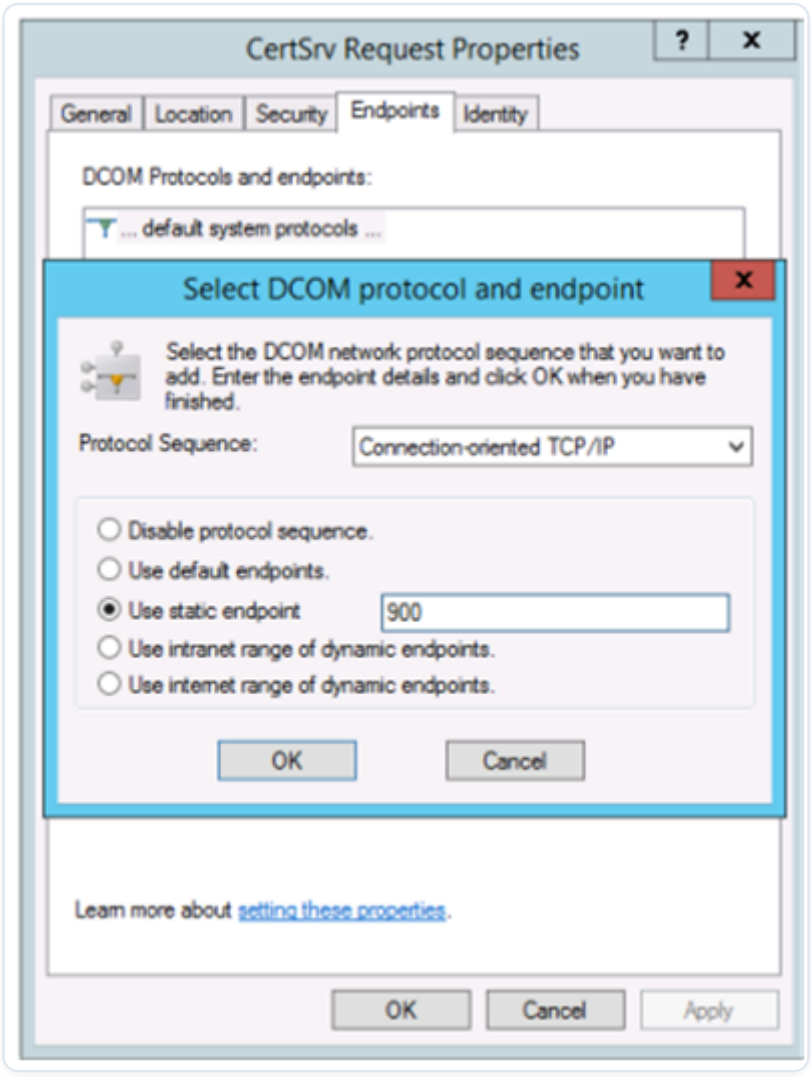
Modifications de comportement attendues

Après avoir configuré le serveur FAS avec plusieurs serveurs d'autorité de certification, la génération de certificats utilisateur est répartie entre tous les serveurs d'autorité de certification configurés. De plus, si l'un des serveurs d'autorité de certification configurés tombe en panne, le serveur FAS basculera vers un autre serveur d'autorité de certification disponible.

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

Configurer l'autorité de certification Microsoft pour l'accès TCP

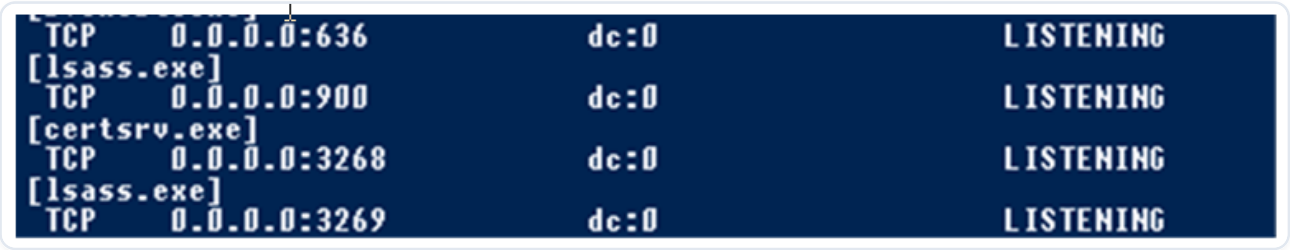
Par défaut, l'autorité de certification Microsoft utilise DCOM pour l'accès. Cela peut entraîner des complexités lors de la mise en œuvre de la sécurité du pare-feu, c'est pourquoi Microsoft a prévu de passer à un port TCP statique. Sur l'autorité de certification Microsoft, utilisez **Démarrer>Exécuter>dcomcnfg.exe** pour ouvrir le panneau de configuration DCOM, développez *Ordinateurs>Mon ordinateur>Configuration DCOM* pour afficher le nœud **CertSrv Request**, puis modifiez les propriétés de l'application DCOM CertSrv Request :



Modifiez les « Points de terminaison » pour sélectionner un point de terminaison statique et spécifiez un numéro de port TCP (900 dans le graphique ci-dessus).

Redémarrez l'autorité de certification Microsoft et soumettez une demande de certificat. Si vous exécutez `netstat –a –n –b`, vous devriez voir que certsvr écoute maintenant sur le port 900 :

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



Il n'est pas nécessaire de configurer le serveur FAS (ou toute autre machine utilisant l'autorité de certification), car DCOM dispose d'une étape de négociation utilisant le port RPC. Lorsqu'un client doit utiliser DCOM, il se connecte au service DCOM RPC sur le serveur de certificats et demande l'accès à un serveur DCOM particulier. Cela déclenche l'ouverture du port 900, et le serveur DCOM indique au serveur FAS comment se connecter.

Pré-générer les certificats utilisateur

Le temps de connexion des utilisateurs s'améliorera considérablement lorsque les certificats utilisateur seront pré-générés au sein du serveur FAS. Les sections suivantes décrivent comment cela peut être fait, que ce soit pour un seul ou plusieurs serveurs FAS.

Obtenir une liste d'utilisateurs Active Directory

Vous pouvez améliorer la génération de certificats en interrogeant l'AD et en stockant la liste des utilisateurs dans un fichier (par exemple, un fichier .csv), comme le montre l'exemple suivant.

```
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 {
```

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

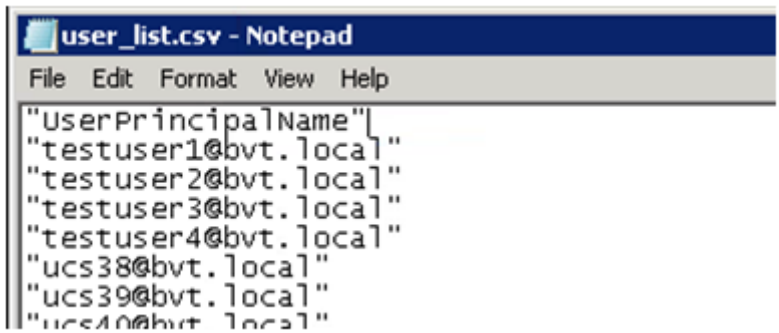
```
    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq
"true")} -Properties UserPrincipalName | Select UserPrincipalName |
Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename

}
```

Get-ADUser est une cmdlet standard pour interroger une liste d'utilisateurs. L'exemple ci-dessus contient un argument de filtre pour lister uniquement les utilisateurs ayant un UserPrincipalName et un statut de compte « activé ».

L'argument SearchBase restreint la partie de l'AD à rechercher pour les utilisateurs. Vous pouvez l'omettre si vous souhaitez inclure tous les utilisateurs de l'AD. Remarque : Cette requête peut renvoyer un grand nombre d'utilisateurs.

Le fichier CSV ressemble à ceci :



Serveur FAS

Le script PowerShell suivant prend la liste d'utilisateurs précédemment générée et crée une liste de certificats utilisateur.

```
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 )

{
```

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

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

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

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

    }

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

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

    }

}
```

Si vous avez plus d'un serveur FAS, le certificat d'un utilisateur particulier sera généré deux fois : une fois sur le serveur principal et une autre sur le serveur de basculement.

Le script ci-dessus est conçu pour une règle nommée « default ». Si vous avez un nom de règle différent (par exemple, « hello »), modifiez simplement la variable $rule dans le script.



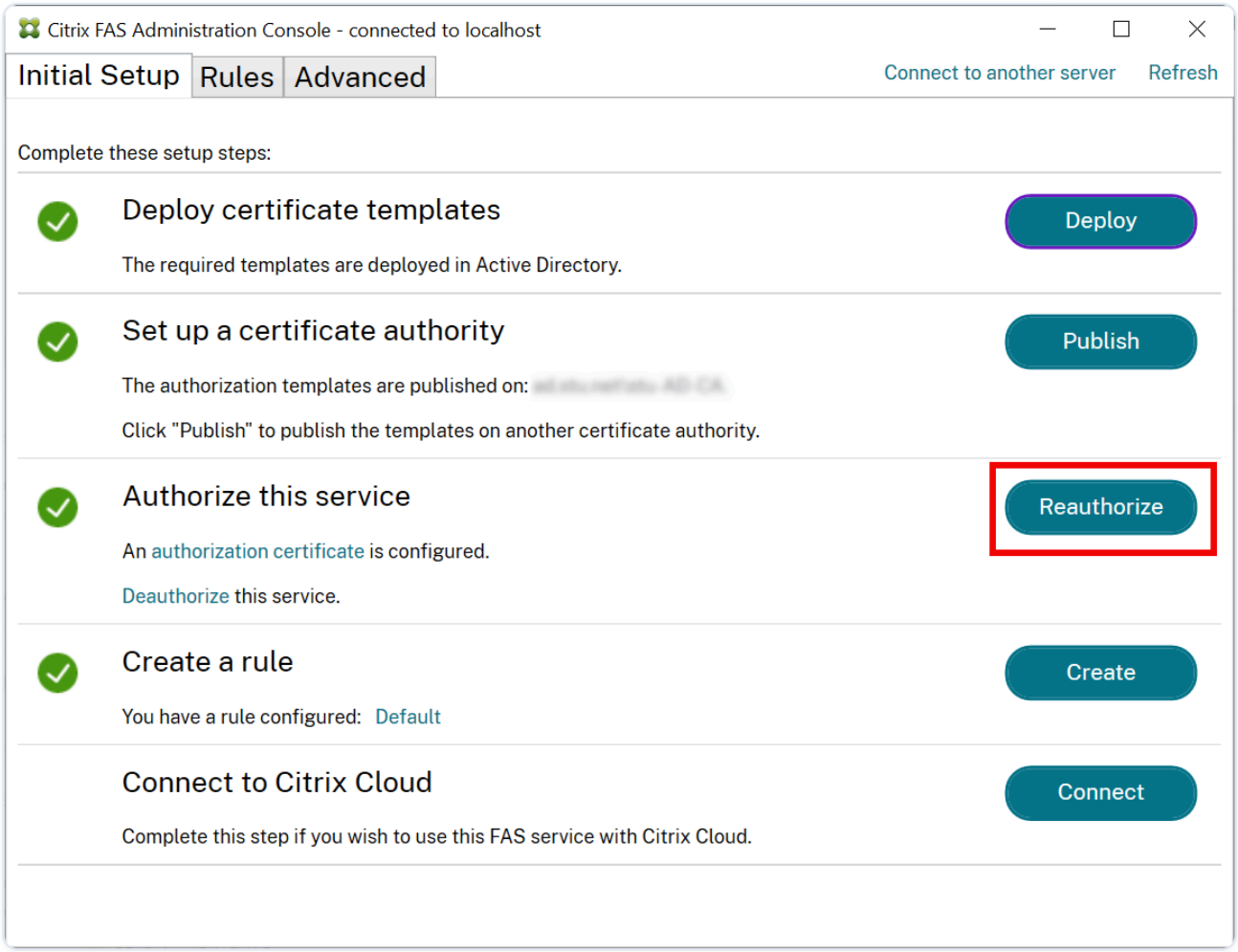
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Renouveler les certificats d'autorité d'enregistrement

Si plusieurs serveurs FAS sont utilisés, vous pouvez renouveler un certificat d'autorisation FAS sans affecter les utilisateurs connectés.

REMARQUE :

Vous pouvez également utiliser l'interface graphique pour réautoriser FAS :



Effectuez la séquence suivante :

1. Créer un nouveau certificat d'autorisation : `New-FasAuthorizationCertificate`
2. Notez le GUID du nouveau certificat d'autorisation, tel que renvoyé par : `Get-FasAuthorizationCertificate`
3. Mettre le serveur FAS en mode maintenance : `Set-FasServer –Address <FAS server> -MaintenanceMode $true`
4. Échanger le nouveau certificat d'autorisation : `Set-FasCertificateDefinition –AuthorizationCertificate <GUID>`

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

5. Retirer le serveur FAS du mode maintenance : `Set-FasServer –Address <FAS server> -MaintenanceMode $false`
6. Supprimer l'ancien certificat d'autorisation : `Remove-FasAuthorizationCertificate`

Informations connexes

- L'article Installer et configurer est la référence principale pour l'installation et la configuration de FAS.
- Les déploiements courants du service d'authentification fédérée sont résumés dans l'article Architectures de déploiement.
- D'autres articles pratiques sont présentés dans l'article Configuration avancée.

Protection des clés privées

Introduction

Les certificats sont stockés dans une base de données intégrée sur le serveur FAS. Les clés privées associées sont stockées via le compte Service réseau du serveur FAS et sont marquées comme non exportables par défaut.

Il existe deux types de clés privées :

- La clé privée associée au certificat d'autorité d'enregistrement, à partir du modèle de certificat Citrix_RegistrationAuthority.
- Les clés privées associées aux certificats utilisateur, à partir du modèle de certificat Citrix_SmartcardLogon.

Il existe en fait deux certificats d'autorité d'enregistrement : Citrix_RegistrationAuthority_ManualAuthorization (valide pendant 24 heures par défaut) et Citrix_RegistrationAuthority (valide pendant deux ans par défaut).

Au cours de l'étape 3 de l'onglet **Configuration initiale** de la console d'administration du service d'authentification fédérée (FAS), lorsque vous cliquez sur **Autoriser**, le serveur FAS génère une paire de clés et envoie une demande de signature de certificat à l'autorité de certification pour le certificat Citrix_RegistrationAuthority_ManualAuthorization. Il s'agit d'un certificat temporaire, valide pendant 24 heures par défaut. L'autorité de certification n'émet pas automatiquement ce certificat ; son émission doit être autorisée manuellement sur l'autorité de certification par un administrateur. Une fois le certificat émis sur le serveur FAS, FAS utilise le certificat Citrix_RegistrationAuthority_ManualAuthorization pour obtenir automatiquement le certificat

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

Citrix_RegistrationAuthority (valide pendant deux ans par défaut). Le serveur FAS supprime le certificat et la clé pour Citrix_RegistrationAuthority_ManualAuthorization dès qu'il obtient le certificat Citrix_RegistrationAuthority.

La clé privée associée au certificat d'autorité d'enregistrement est particulièrement sensible, car la politique de certificat d'autorité d'enregistrement permet à quiconque possède la clé privée d'émettre des demandes de certificat pour l'ensemble des utilisateurs configurés dans le modèle. Par conséquent, quiconque contrôle cette clé peut se connecter à l'environnement en tant que n'importe quel utilisateur de l'ensemble.

Vous pouvez configurer le serveur FAS pour protéger les clés privées d'une manière qui correspond aux exigences de sécurité de votre organisation, en utilisant l'une des options suivantes :

- Fournisseur de services cryptographiques Microsoft Enhanced RSA et AES ou fournisseur de stockage de clés logicielles Microsoft pour le certificat d'autorité d'enregistrement et les clés privées des certificats utilisateur.
- Fournisseur de stockage de clés de plateforme Microsoft avec une puce de module de plateforme sécurisée (TPM) pour la clé privée du certificat d'autorité d'enregistrement, et fournisseur de services cryptographiques Microsoft Enhanced RSA et AES ou fournisseur de stockage de clés logicielles Microsoft pour les clés privées des certificats utilisateur.
- Service cryptographique ou fournisseur de stockage de clés d'un fournisseur de module de sécurité matérielle (HSM) avec le périphérique HSM pour le certificat d'autorité d'enregistrement et les clés privées des certificats utilisateur.

Paramètres de configuration des clés privées

Configurez FAS pour utiliser l'une des trois options. Utilisez un éditeur de texte pour modifier le fichier Citrix.Authentication.FederatedAuthenticationService.exe.config. L'emplacement par défaut du fichier est dans le dossier Program Files\Citrix\Federated Authentication Service sur le serveur FAS.

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

```
<?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 lit le fichier de configuration uniquement lorsque le service démarre. Si des valeurs sont modifiées, FAS doit être redémarré avant que les nouveaux paramètres ne soient pris en compte.

Définissez les valeurs pertinentes dans le fichier Citrix.Authentication.FederatedAuthenticationService.exe.config comme suit :

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (basculer entre les API CAPI et CNG)

VALEUR	COMMENTAIRE
vrai	Utiliser les API CAPI
false (par défaut)	Utiliser les API CNG

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (nom du fournisseur à utiliser)

VALEUR	COMMENTAIRE
Fournisseur de services cryptographiques Microsoft Enhanced RSA et AES	Fournisseur CAPI par défaut
Fournisseur de stockage de clés logicielles Microsoft	Fournisseur CNG par défaut
Fournisseur de stockage de clés de plateforme Microsoft	Fournisseur TPM par défaut. Notez que le TPM n'est pas recommandé pour les clés utilisateur. Utilisez le TPM uniquement pour la

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

VALEUR	COMMENTAIRE
	clé de l'autorité d'enregistrement. Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, vérifiez auprès de votre fournisseur TPM et d'hyperviseur si la virtualisation est prise en charge.
Fournisseur CSP/de stockage de clés HSM_Vendor	Fourni par le fournisseur HSM. La valeur diffère selon les fournisseurs. Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, vérifiez auprès de votre fournisseur HSM si la virtualisation est prise en charge.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (Requis uniquement en cas d'API CAPI)

VALEUR	COMMENTAIRE
24	Par défaut. Fait référence à la propriété Microsoft KeyContainerPermissionAccessEntry.ProviderType PROV_RSA_AES 24. Doit toujours être 24, sauf si vous utilisez un HSM avec CAPI et que le fournisseur HSM spécifie le contraire.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (Lorsque FAS doit effectuer une opération de clé privée, il utilise la valeur spécifiée ici) Contrôle l'indicateur « exportable » des clés privées. Permet l'utilisation du stockage de clés TPM, si pris en charge par le matériel.

VALEUR	COMMENTAIRE
NoProtection	La clé privée peut être exportée.
GenerateNonExportableKey	Par défaut. La clé privée ne peut pas être exportée.
GenerateTPMProtectedKey	La clé privée sera gérée à l'aide du TPM. La clé privée est stockée via le ProviderName que vous avez spécifié dans ProviderName (par

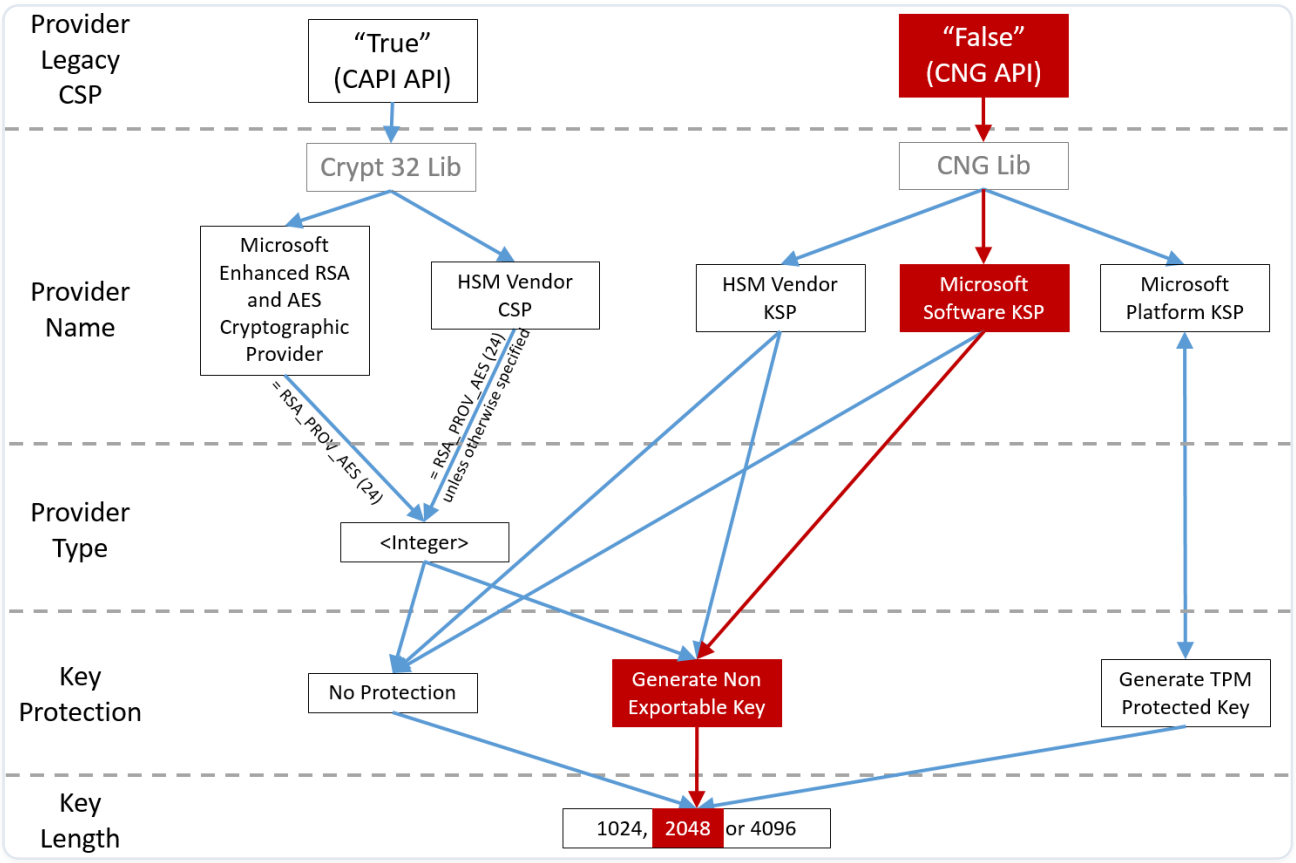
© 1997–2026 Citrix Systems, Inc. All rights reserved.

VALEUR	COMMENTAIRE
	exemple, Microsoft Platform Key Storage Provider)

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (Spécifiez la taille de la clé privée en bits)

VALEUR	COMMENTAIRE
2048	Par défaut. 1024 ou 4096 peuvent également être utilisés.

Les paramètres du fichier de configuration sont représentés graphiquement comme suit (les valeurs par défaut de l'installation sont affichées en rouge) :



Exemples de scénarios de configuration

Exemple 1

Cet exemple couvre la clé privée du certificat de l'autorité d'enregistrement et les clés privées des certificats utilisateur stockées à l'aide du fournisseur de stockage de clés logicielles Microsoft.

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

Il s'agit de la configuration par défaut après l'installation. Aucune configuration supplémentaire de clé privée n'est requise.

Exemple 2

Cet exemple montre la clé privée du certificat de l'autorité d'enregistrement stockée dans le TPM matériel de la carte mère du serveur FAS via le fournisseur de stockage de clés de plateforme Microsoft, et les clés privées des certificats utilisateur stockées à l'aide du fournisseur de stockage de clés logicielles Microsoft.

Ce scénario suppose que le TPM de la carte mère de votre serveur FAS a été activé dans le BIOS conformément à la documentation du fabricant du TPM, puis initialisé dans Windows ; voir `<https://docs.microsoft.com/fr-fr/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)>`.

Utilisation de la console d'administration FAS

La console d'administration FAS ne peut pas effectuer de demande de signature de certificat hors ligne, son utilisation n'est donc pas recommandée à moins que votre organisation n'autorise les demandes de signature de certificat en ligne pour les certificats d'autorité d'enregistrement.

Lors de la configuration initiale de FAS, après le déploiement des modèles de certificat et la configuration de l'autorité de certification, mais avant d'autoriser le service (étape 3 de la séquence de configuration) :

Étape 1 : Modifiez le fichier de configuration en changeant la ligne suivante comme suit :

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

Le fichier doit maintenant apparaître comme suit :

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

```
<?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>
```

Certains TPM limitent la longueur de clé. La longueur de clé par défaut est de 2048 bits. Assurez-vous de spécifier une longueur de clé prise en charge par votre matériel.

Étape 2 : Redémarrez le service d'authentification fédérée Citrix pour lire les valeurs du fichier de configuration.

Étape 3 : Autorisez le service.

Étape 4 : Émettez manuellement la demande de certificat en attente à partir du serveur d'autorité de certification. Une fois le certificat de l'autorité d'enregistrement obtenu, l'étape 3 de la séquence de configuration dans la console d'administration sera verte. À ce stade, la clé privée du certificat de l'autorité d'enregistrement aura été générée dans le TPM. Le certificat sera valide pendant 2 ans par défaut.

Pour confirmer que la clé privée du certificat de l'autorité d'enregistrement est correctement stockée dans le TPM, utilisez les commandes PowerShell suivantes. Le champ PrivateKeyProvider sera défini sur *Microsoft Platform Crypto Provider* si la clé privée du certificat de l'autorité d'enregistrement est stockée dans le TPM :

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

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

Étape 5 : Modifiez le fichier de configuration pour qu'il corresponde à ce qui suit :

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

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

REMARQUE :

Bien que FAS puisse générer des certificats utilisateur avec des clés protégées par TPM, le matériel TPM peut être trop lent pour les déploiements importants.

Étape 6 : Redémarrez FAS. Cela force le service à relire le fichier de configuration et à refléter les valeurs modifiées. Les opérations automatiques de clé privée suivantes affecteront les clés de certificat utilisateur ; ces opérations ne stockeront pas les clés privées dans le TPM, mais utiliseront le fournisseur de stockage de clés logicielles Microsoft.

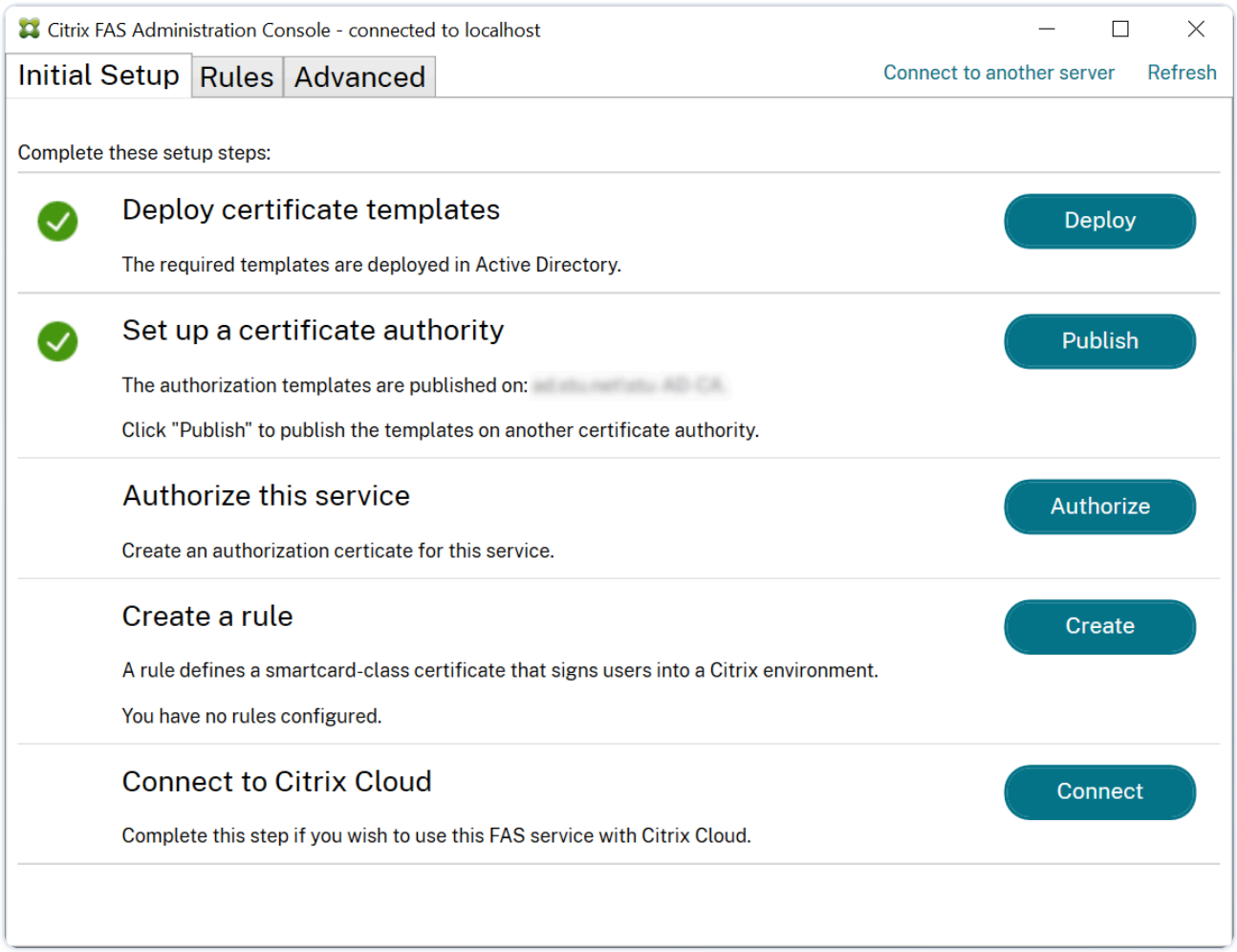
Étape 7 : Sélectionnez l'onglet **Règles** dans la console d'administration FAS et modifiez les paramètres comme décrit dans Installer et configurer.

Utilisation de PowerShell

Le certificat de l'autorité d'enregistrement peut être demandé hors ligne à l'aide de PowerShell. Cela convient aux organisations qui ne souhaitent pas que leur autorité de certification émette un certificat d'autorité d'enregistrement via une demande de signature de certificat en ligne. Vous ne pouvez pas effectuer une demande de signature de certificat d'autorité d'enregistrement hors ligne à l'aide de la console d'administration FAS.

Étape 1 : Lors de la configuration initiale de FAS à l'aide de la console d'administration, ne complétez que les deux premières étapes : « Déployer les modèles de certificat » et « Configurer une autorité de certification ».

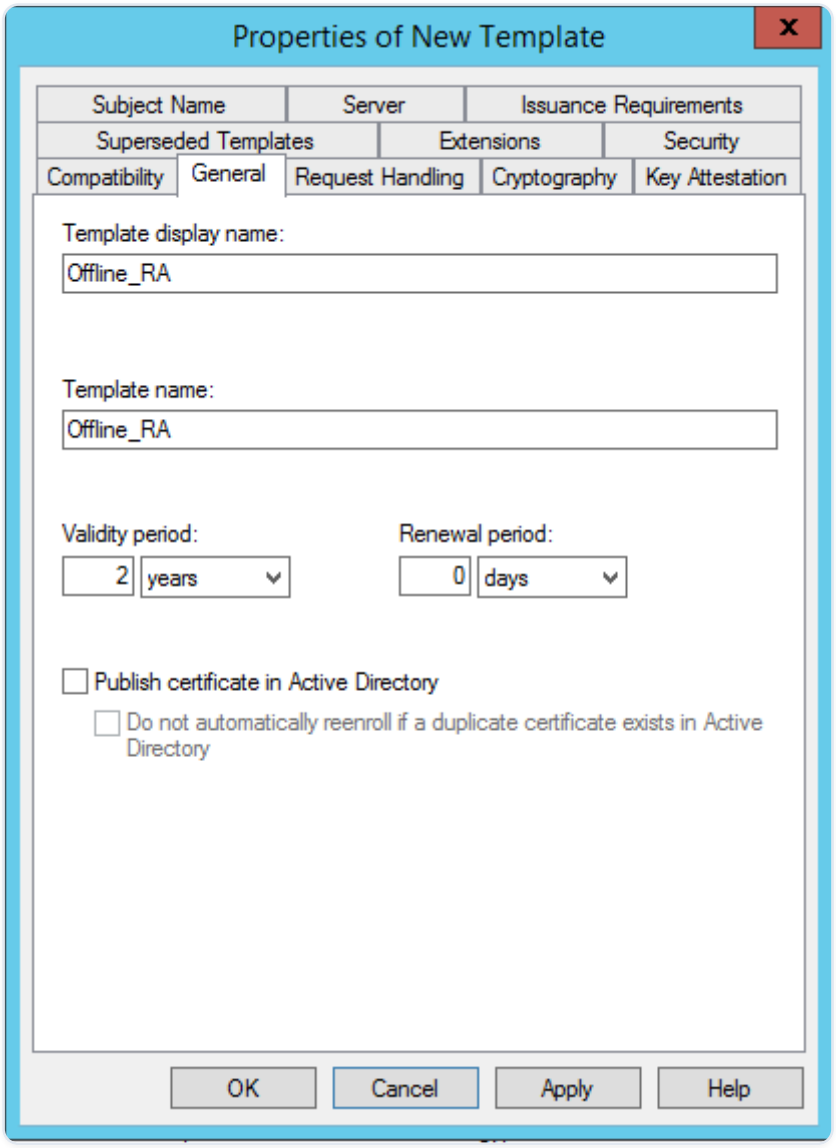
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Étape 2 : Sur votre serveur d'autorité de certification, ajoutez le composant logiciel enfichable MMC Modèles de certificats. Cliquez avec le bouton droit sur le modèle **Citrix_RegistrationAuthority_ManualAuthorization** et sélectionnez **Dupliquer le modèle**.

Sélectionnez l'onglet **Général**. Modifiez le nom et la période de validité. Dans cet exemple, le nom est *Offline_RA* et la période de validité est de 2 ans :

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



Étape 3 : Sur votre serveur d'autorité de certification, ajoutez le composant logiciel enfichable MMC Autorité de certification. Cliquez avec le bouton droit sur **Modèles de certificats**. Sélectionnez **Nouveau**, puis cliquez sur **Modèle de certificat à émettre**. Choisissez le modèle que vous venez de créer.

Étape 4 : Chargez les applets de commande PowerShell suivantes sur le serveur FAS :

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

Étape 5 : Générez la paire de clés RSA à l'intérieur du TPM du serveur FAS et créez la demande de signature de certificat en entrant l'applet de commande PowerShell suivante sur le serveur FAS. **Remarque :** Certains TPM limitent la longueur de clé. La longueur de clé par défaut est de 2048 bits. Assurez-vous de spécifier une longueur de clé prise en charge par votre matériel.

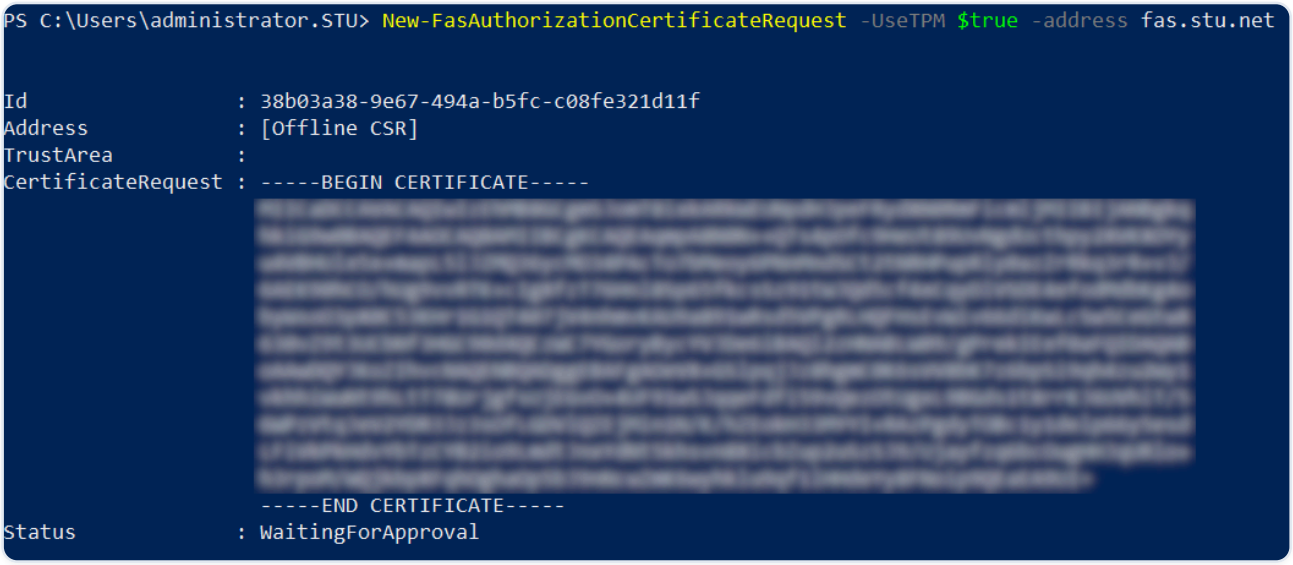
```
New-FasAuthorizationCertificateRequest -UseTPM $true -address \<FQDN of FAS Server>
```

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

Par exemple :

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

Le résultat suivant s'affiche :

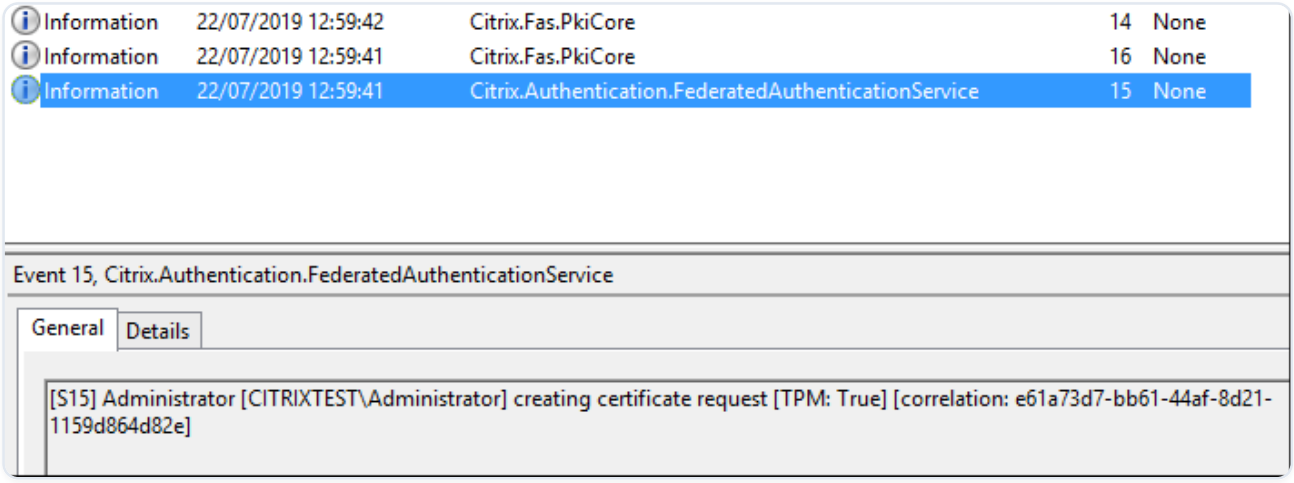


© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES :

- Le GUID d'ID (dans cet exemple, « 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 ») est requis à une étape ultérieure.
- Considérez cette applet de commande PowerShell comme une « substitution » unique utilisée pour générer la clé privée du certificat d'autorité d'enregistrement.
- Lors de l'exécution de cette applet de commande, les valeurs lues à partir du fichier de configuration au démarrage de FAS sont vérifiées pour déterminer la longueur de clé à utiliser (la valeur par défaut est 2048).
- Étant donné que -UseTPM est défini sur $true dans cette opération manuelle de clé privée de certificat d'autorité d'enregistrement initiée par PowerShell, le système ignore les valeurs du fichier qui ne correspondent pas aux paramètres requis pour utiliser un TPM.
- L'exécution de cette applet de commande ne modifie aucun paramètre dans le fichier de configuration.
- Lors des opérations ultérieures automatiques de clé privée de certificat utilisateur initiées par FAS, les valeurs lues à partir du fichier au démarrage de FAS sont utilisées.
- Il est également possible de définir la valeur KeyProtection dans le fichier de configuration sur GenerateTPMProtectedKey lorsque le serveur FAS émet des certificats utilisateur pour générer des clés privées de certificat utilisateur protégées par le TPM.

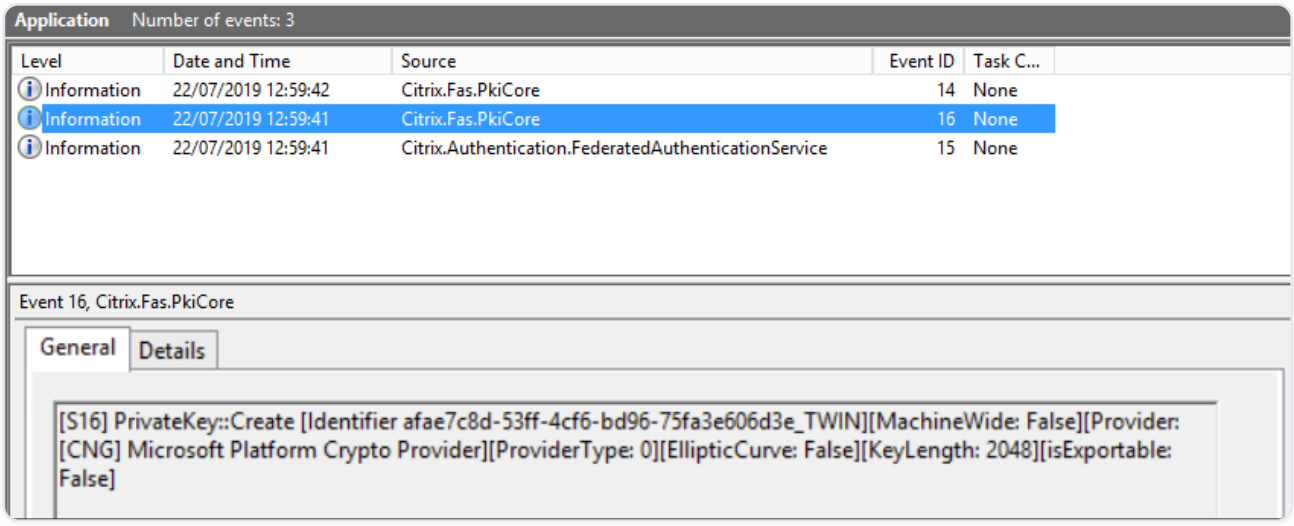
Pour vérifier que le TPM a été utilisé pour générer la paire de clés, consultez le journal des applications dans l'Observateur d'événements Windows sur le serveur FAS, au moment où la paire de clés est générée.



Remarque : « »

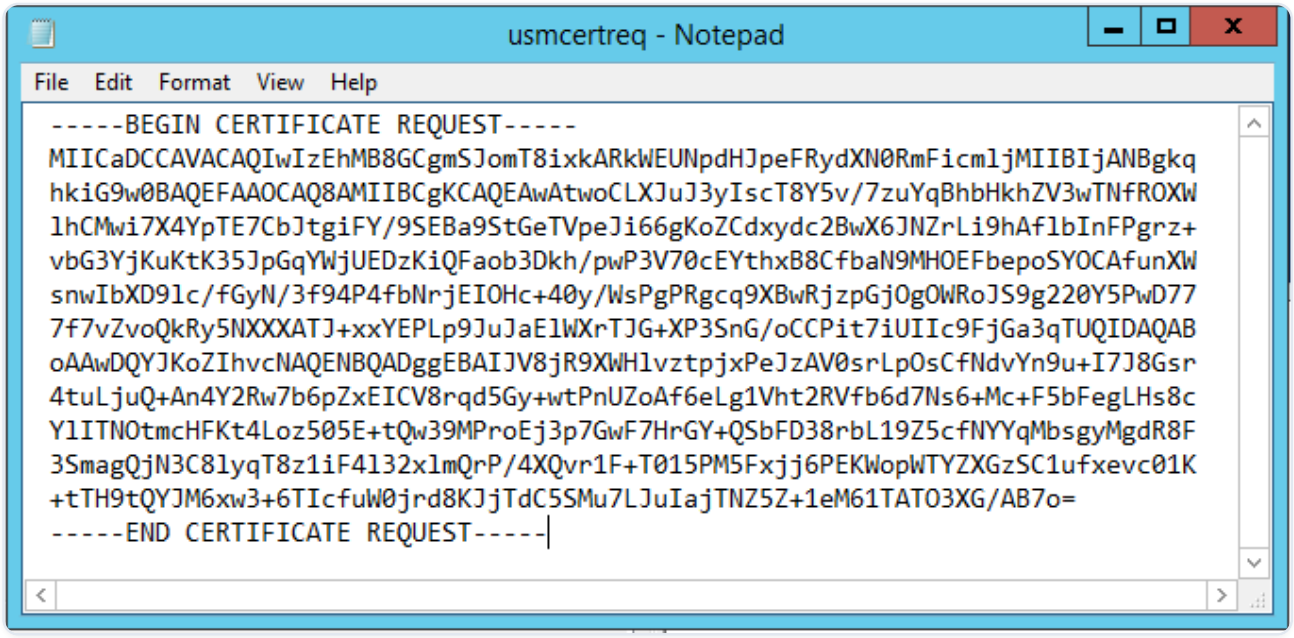
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Suivi de :



Remarque : « Fournisseur : Microsoft Platform Crypto Provider »

Étape 6 : Copiez la section de demande de certificat dans un éditeur de texte et enregistrez-la sur le disque en tant que fichier texte.



Étape 7 : Soumettez la demande de signature de certificat à votre autorité de certification en tapant ce qui suit dans PowerShell sur le serveur FAS :

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

Par exemple :

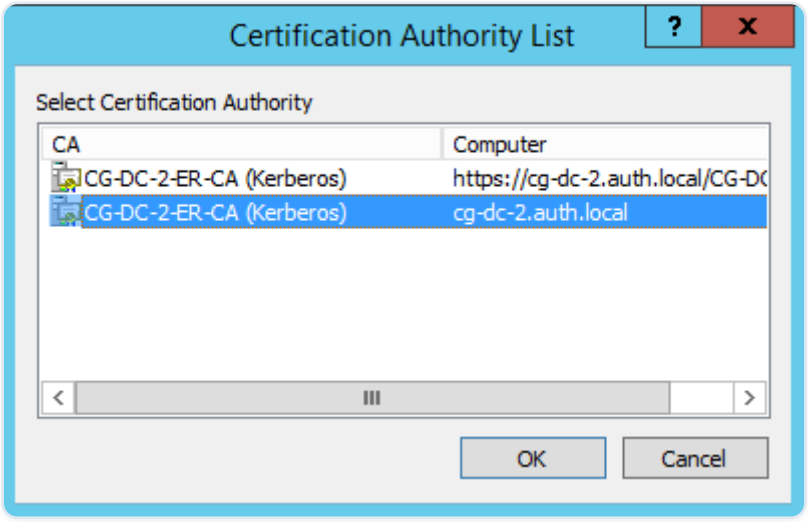
```
certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
```

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

Ce qui suit s'affiche :

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DBDC-4D21-A4FD-2E29502177C2}
  ldap:
```

À ce stade, une fenêtre de liste d'autorités de certification peut apparaître. L'autorité de certification dans cet exemple a l'inscription http (en haut) et DCOM (en bas) activée. Sélectionnez l'option DCOM, si disponible :



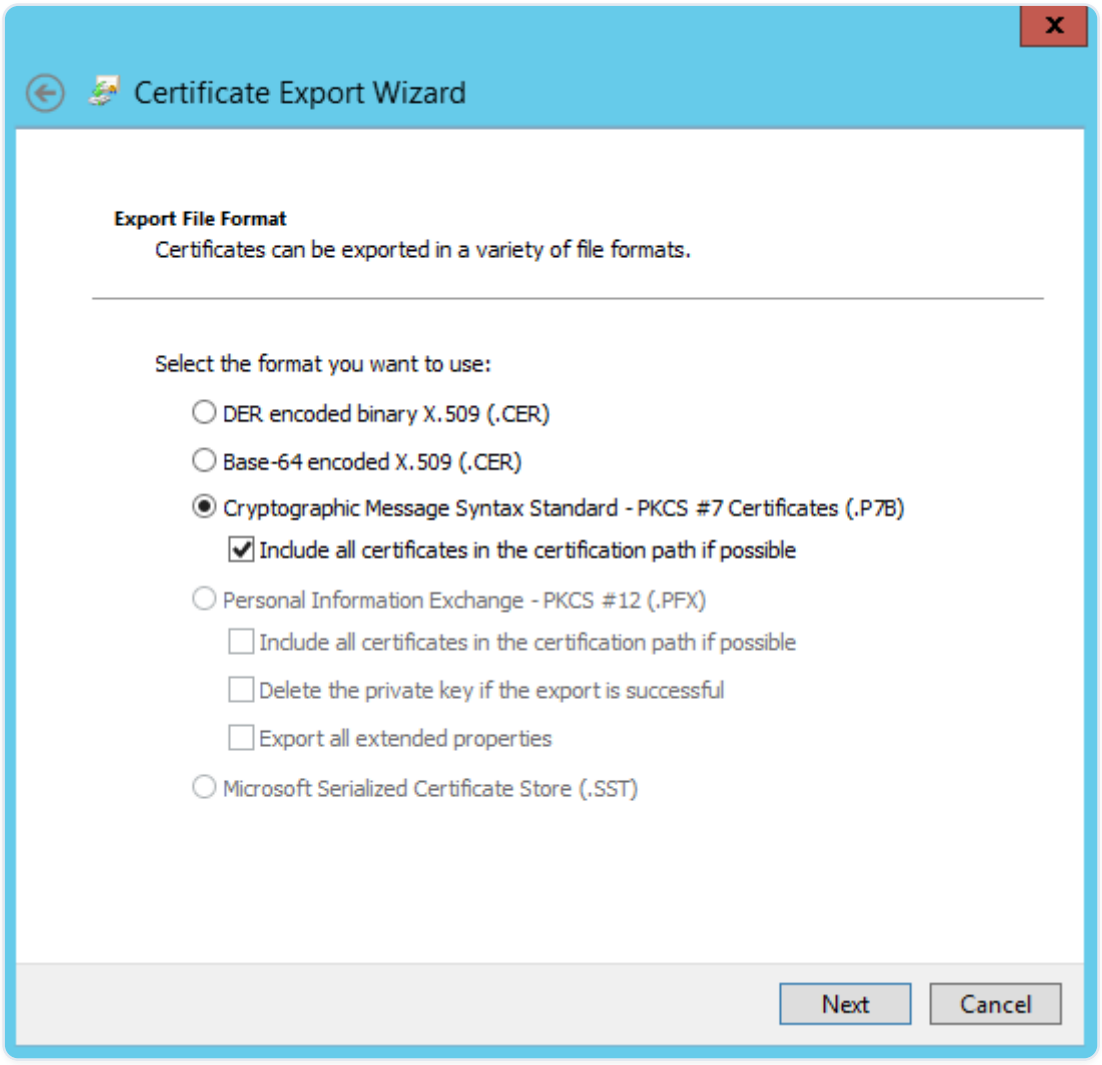
Une fois l'autorité de certification spécifiée, PowerShell affiche le RequestID :

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

Étape 8 : Sur le serveur d'autorité de certification, dans le composant logiciel enfichable MMC de l'autorité de certification, cliquez sur **Demandes en attente**. Notez l'ID de demande. Ensuite, cliquez avec le bouton droit sur la demande et choisissez **Émettre**.

Étape 9 : Sélectionnez le nœud **Certificats émis**. Recherchez le certificat qui vient d'être émis (l'ID de demande doit correspondre). Double-cliquez pour ouvrir le certificat. Sélectionnez l'onglet **Détails**. Cliquez sur **Copier dans un fichier**. L'Assistant Exportation de certificat se lance. Cliquez sur **Suivant.** Choisissez les options suivantes pour le format de fichier :

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



Le format doit être "**Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**" et "**Inclure tous les certificats dans le chemin de certification si possible**" doit être sélectionné.

Étape 10 : Copiez le fichier de certificat exporté sur le serveur FAS.

Étape 11 : Importez le certificat de l'autorité d'enregistrement sur le serveur FAS en saisissant la cmdlet PowerShell suivante sur le serveur FAS :

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

Par exemple :

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

Ce qui suit s'affiche :

© 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

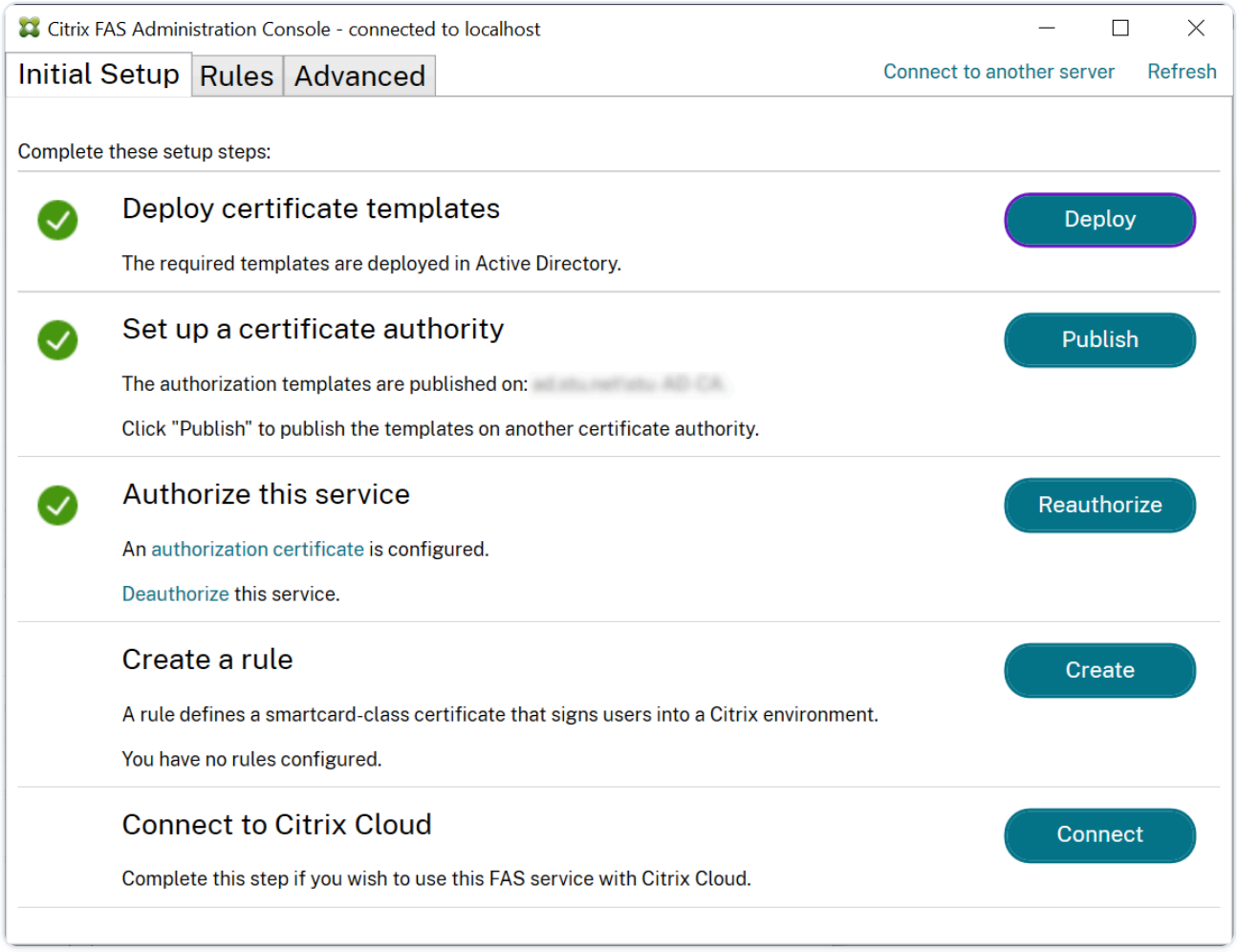

Id                : 74d427ff-c55b-4d6d-87ae-1ff98b0c2705
Address           : [Offline CSR]
TrustArea         : 978816cd-8b2f-4695-8c5d-08bb7df1816b
CertificateRequest :
Status            : Ok
```

Pour confirmer que la clé privée du certificat de l'autorité d'enregistrement est correctement stockée dans le TPM, utilisez les commandes PowerShell suivantes. Le champ PrivateKeyProvider sera défini sur *Microsoft Platform Crypto Provider* si la clé privée du certificat de l'autorité d'enregistrement est stockée dans le TPM :

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

Get-FasAuthorizationCertificate -FullCertInfo -Address localhost
```

Étape 12 : Fermez la console d'administration FAS, puis redémarrez-la.



Remarque : L'étape « Autoriser ce service » est cochée en vert.

Étape 13 : Sélectionnez l'onglet **Règles** dans la console d'administration FAS et modifiez les paramètres décrits dans Installer et configurer.

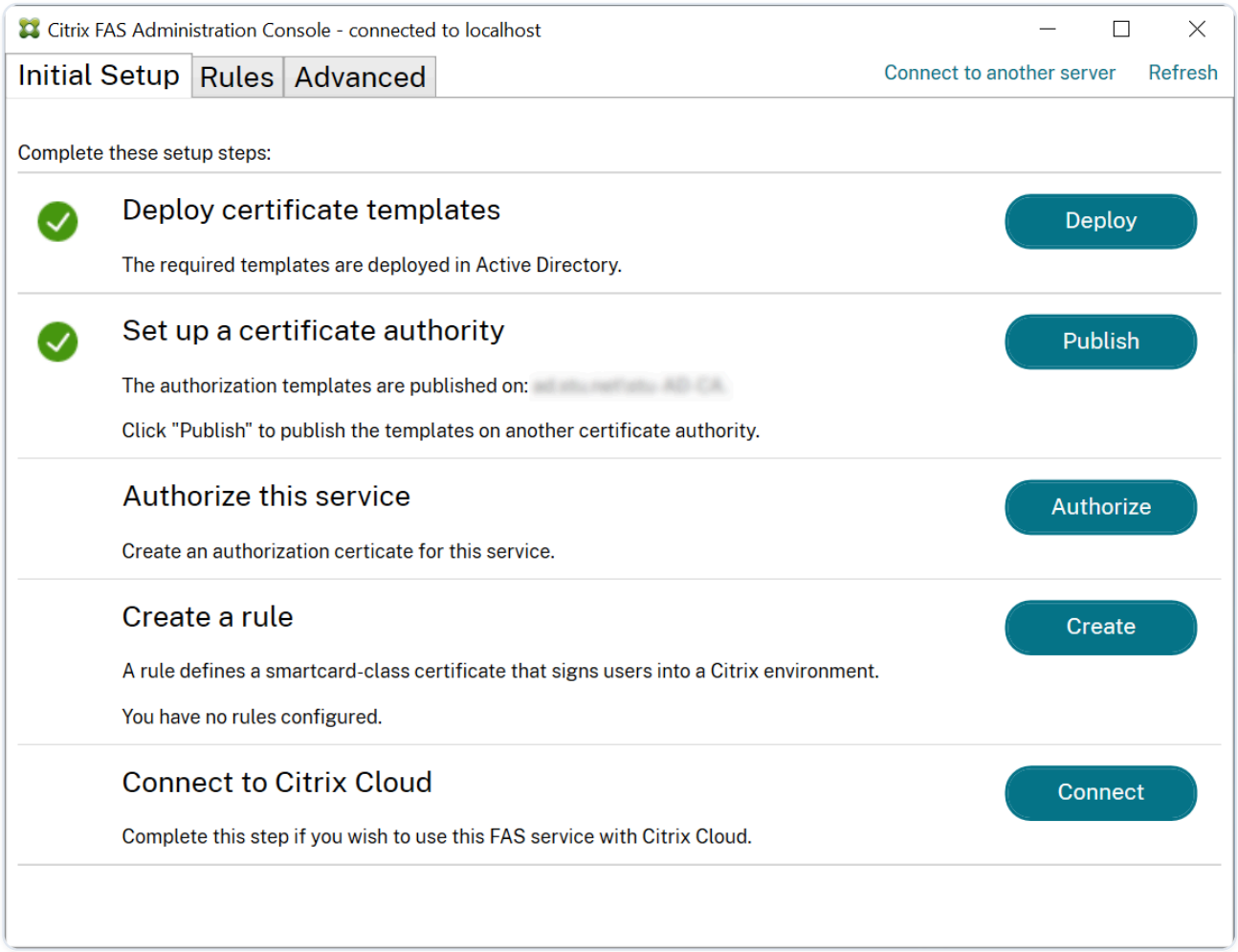
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple 3

Cet exemple couvre une clé privée de certificat d'autorité d'enregistrement et des clés privées de certificats d'utilisateur stockées dans un HSM. Cet exemple suppose un HSM configuré. Votre HSM aura un nom de fournisseur, par exemple « HSM_Vendor's Key Storage Provider ».

Si vous prévoyez d'exécuter votre serveur FAS dans un environnement virtualisé, vérifiez auprès de votre fournisseur HSM la prise en charge de l'hyperviseur.

Étape 1. Lors de la configuration initiale de FAS à l'aide de la console d'administration, ne complétez que les deux premières étapes : « Déployer les modèles de certificat » et « Configurer une autorité de certification ».



Étape 2 : Consultez la documentation de votre fournisseur HSM pour déterminer la valeur ProviderName de votre HSM. Si votre HSM utilise CAPI, le fournisseur peut être désigné dans la documentation comme un Cryptographic Service Provider (CSP). Si votre HSM utilise CNG, le fournisseur peut être désigné comme un Key Storage Provider (KSP).

Étape 3 : Modifiez le fichier de configuration comme suit :

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

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

Le fichier devrait maintenant apparaître comme suit :

```
<?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>
```

Ce scénario suppose que votre HSM utilise CNG, de sorte que la valeur ProviderLegacyCsp est définie sur false. Si votre HSM utilise CAPI, la valeur ProviderLegacyCsp doit être définie sur true. Consultez la documentation de votre fournisseur HSM pour déterminer si votre HSM utilise CAPI ou CNG. Consultez également la documentation de votre fournisseur HSM sur les longueurs de clé prises en charge pour la génération de clés RSA asymétriques. Dans cet exemple, la longueur de clé est définie par défaut sur 2048 bits. Assurez-vous que la longueur de clé que vous spécifiez est prise en charge par votre matériel.

Étape 4 : Redémarrez le service d'authentification fédérée Citrix pour lire les valeurs du fichier de configuration.

Étape 5 : Générez la paire de clés RSA à l'intérieur du HSM et créez la demande de signature de certificat en cliquant sur **Autoriser** dans l'onglet **Configuration initiale** de la console d'administration FAS.

Étape 6 : Pour vérifier que la paire de clés a été générée dans le HSM, vérifiez les entrées d'application dans le journal des événements Windows :

```
[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]
```

Remarque : [Fournisseur : Fournisseur de stockage de clés du fournisseur HSM]

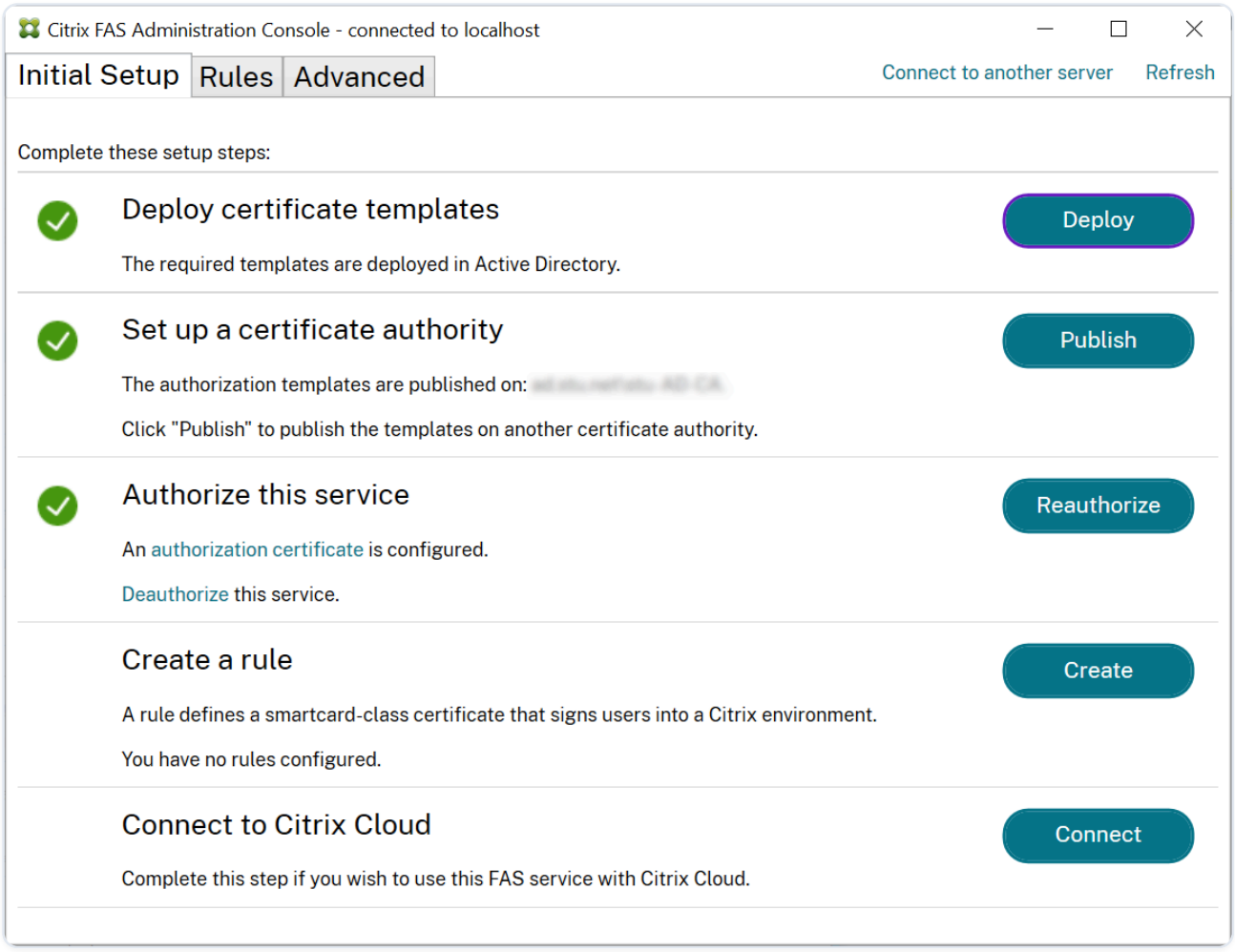
Étape 7 : Sur le serveur d'autorité de certification, dans la console MMC de l'autorité de certification, sélectionnez le nœud **Demandes en attente** :

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

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$	

Cliquez avec le bouton droit sur la demande et sélectionnez **Émettre**.

Remarque : L'étape « Autoriser ce service » est cochée en vert.



Étape 8 : Sélectionnez l'onglet **Règles** dans la console d'administration FAS et modifiez les paramètres comme décrit dans Installer et configurer.

Stockage des certificats FAS

FAS n'utilise pas le magasin de certificats Microsoft sur le serveur FAS pour stocker ses certificats. Il utilise une base de données intégrée.

Pour déterminer le GUID du certificat de l'autorité d'enregistrement, entrez les cmdlets PowerShell suivantes sur le serveur FAS :

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

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

Par exemple, **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>
```

Pour obtenir une liste des certificats utilisateur, saisissez :

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

Par exemple, **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
```

REMARQUE :

Lors de l'utilisation d'un HSM pour stocker des clés privées, les conteneurs HSM sont identifiés par un GUID. Le GUID de la clé privée dans le HSM peut être obtenu à l'aide de :

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

Par exemple :

```
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
```

Informations connexes

- (/fr-fr/federated-authentication-service/2206/install-configure.html) est la référence principale pour l'installation et la configuration de FAS.
- Les déploiements FAS courants sont résumés dans l'article (/fr-fr/federated-authentication-service/2206/deployment-architectures.html).
- D'autres articles pratiques sont présentés dans l'article (/fr-fr/federated-authentication-service/2206/config-manage.html).

Sécurité et configuration réseau

Le service d’authentification fédérée (FAS) est étroitement intégré à Microsoft Active Directory et à l’autorité de certification Microsoft. Il est essentiel de s’assurer que le système est géré et sécurisé de manière appropriée, en élaborant une politique de sécurité comme vous le feriez pour un contrôleur de domaine ou toute autre infrastructure critique.

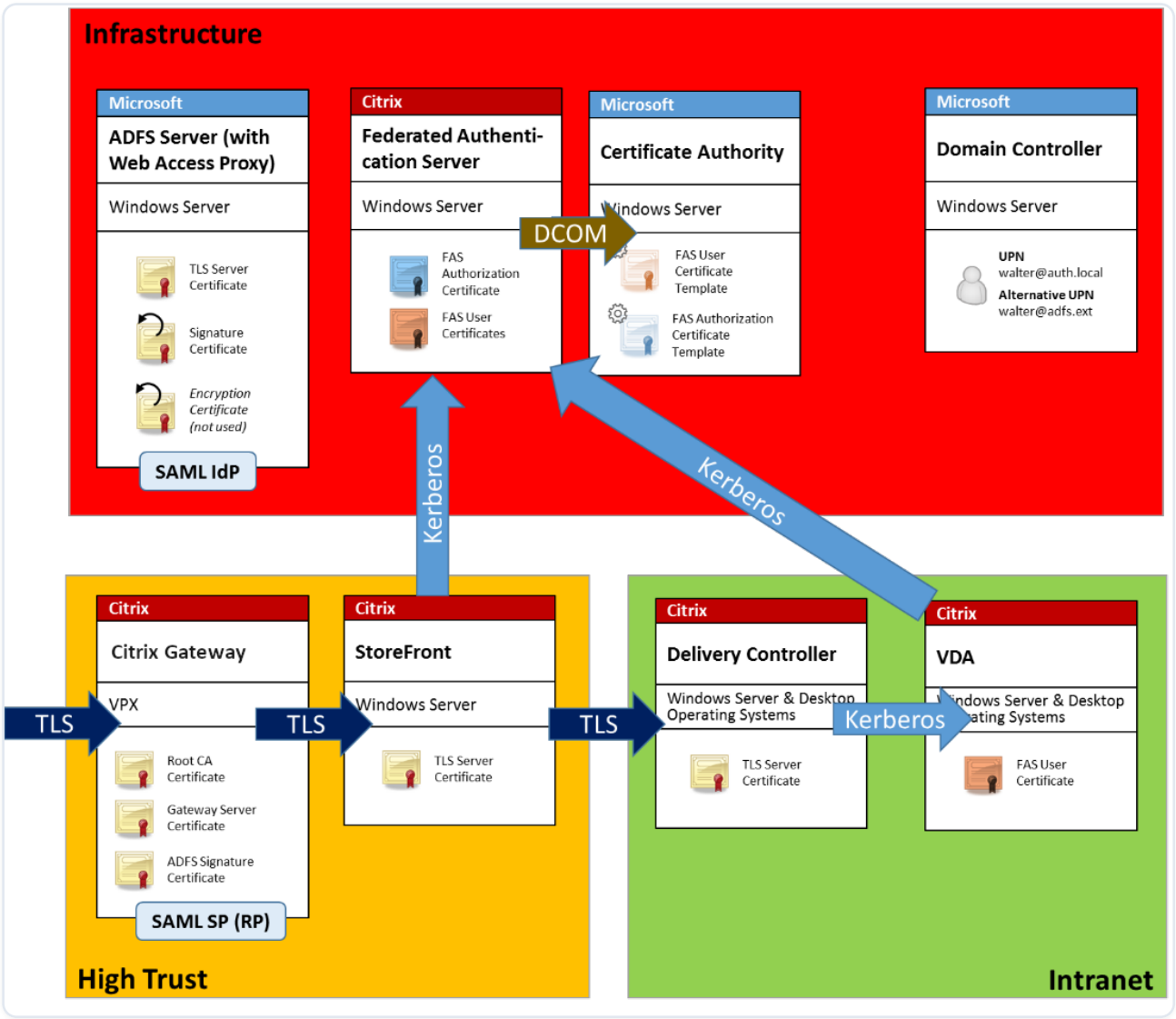
Ce document fournit un aperçu des problèmes de sécurité à prendre en compte lors du déploiement de FAS. Il fournit également un aperçu des fonctionnalités disponibles qui peuvent vous aider à sécuriser votre infrastructure.

Architecture réseau

Le diagramme suivant présente les principaux composants et les limites de sécurité utilisés dans un déploiement FAS.

Le serveur FAS doit être traité comme faisant partie de l’infrastructure critique pour la sécurité, au même titre que l’autorité de certification et le contrôleur de domaine. Dans un environnement fédéré, Citrix Gateway et Citrix StoreFront sont des composants qui effectuent l’authentification des utilisateurs. Les autres composants Citrix Virtual Apps and Desktops™ ne sont pas affectés par l’introduction de FAS.

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



Pare-feu et sécurité réseau

Le protocole TLS sur le port 443 protège la communication entre Citrix Gateway, StoreFront et les composants Delivery Controller™. Le serveur StoreFront n'effectue que des connexions sortantes, et Citrix Gateway n'accepte que les connexions via Internet à l'aide du port HTTPS 443.

Le serveur StoreFront contacte le serveur FAS sur le port 80 à l'aide de Kerberos authentifié mutuellement. L'authentification utilise l'identité Kerberos HOST/fqdn du serveur FAS et l'identité du compte machine Kerberos du serveur StoreFront. Cela génère un « handle d'informations d'identification » à usage unique nécessaire au Citrix Virtual Delivery Agent (VDA) pour connecter l'utilisateur.

Lorsqu'une session HDX est connectée au VDA, le VDA contacte également le serveur FAS sur le port 80. L'authentification utilise l'identité Kerberos HOST/fqdn du serveur FAS et l'identité machine Kerberos du VDA. De plus, le VDA doit fournir le « handle d'informations d'identification » pour accéder au certificat et à la clé privée.

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

L’autorité de certification Microsoft accepte la communication à l’aide de DCOM authentifié par Kerberos, qui peut être configuré pour utiliser un port TCP fixe. L’autorité de certification exige également que le serveur FAS fournisse un paquet CMC signé par un certificat d’agent d’inscription de confiance.

SERVEUR	PORTS DE PARE-FEU
Service d’authentification fédérée	[in] Kerberos sur HTTP depuis StoreFront™ et les VDA, [out] DCOM vers l'autorité de certification Microsoft
Citrix Gateway	[in] HTTPS depuis les machines clientes, [in/out] HTTPS vers/depuis le serveur StoreFront, [out] HDX vers le VDA
StoreFront	[in] HTTPS depuis Citrix Gateway, [out] HTTPS vers le Delivery Controller, [out] Kerberos HTTP vers FAS
Delivery Controller	[in] HTTPS depuis le serveur StoreFront, [in/out] Kerberos sur HTTP depuis les VDA
VDA	[in/out] Kerberos sur HTTP depuis le Delivery Controller, [in] HDX depuis Citrix Gateway, [out] Kerberos HTTP vers FAS
Autorité de certification Microsoft	[in] DCOM et signé depuis FAS

Connexions entre le service d'authentification fédérée Citrix et Citrix Cloud™

La console et FAS accèdent aux adresses suivantes en utilisant respectivement le compte de l'utilisateur et le compte Service réseau.

- Console d'administration FAS, sous le compte de l'utilisateur
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - Adresses requises par un fournisseur d'identité tiers, si l'un est utilisé dans votre environnement
- Service FAS, sous le compte Service réseau :

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

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

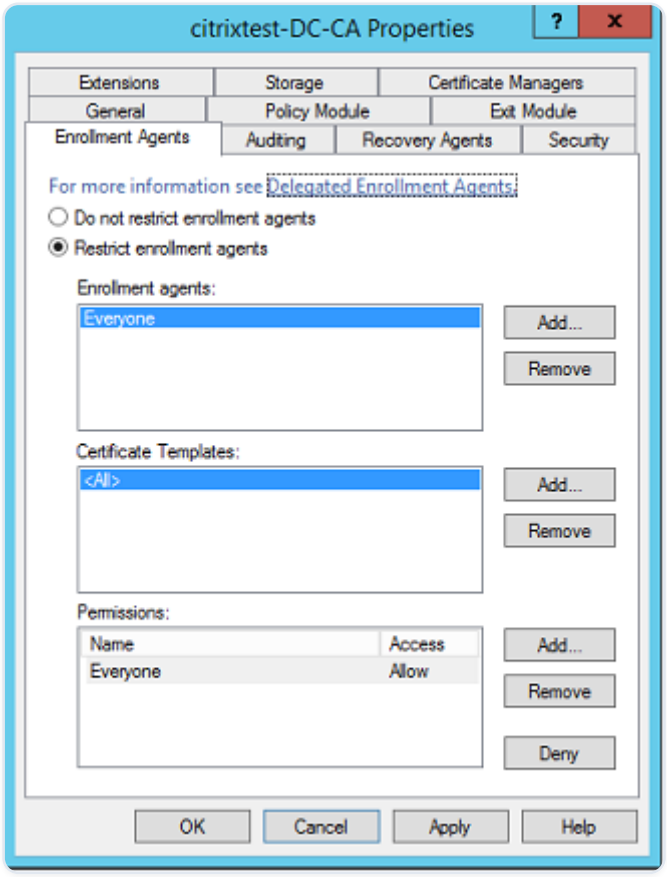
Si votre environnement inclut des serveurs proxy, configurez le proxy utilisateur avec les adresses de la console d'administration FAS. Assurez-vous également que l'adresse du compte Service réseau est configurée à l'aide de netsh ou d'un outil similaire.

Considérations de sécurité

FAS dispose d'un certificat d'autorité d'enregistrement qui lui permet d'émettre des certificats de manière autonome au nom de vos utilisateurs de domaine. À ce titre, il est important de développer et de mettre en œuvre une politique de sécurité pour protéger les serveurs FAS et pour restreindre leurs autorisations.

Agents d'inscription délégués

FAS émet des certificats utilisateur en agissant comme agent d'inscription. L'autorité de certification Microsoft vous permet de restreindre les agents d'inscription, les modèles de certificat et les utilisateurs pour lesquels les agents d'inscription peuvent émettre des certificats.



Vous pouvez utiliser cette boîte de dialogue pour vous assurer que :

- La liste *Agents d'inscription* contient uniquement les serveurs FAS.

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

- La liste *Modèles de certificat* contient uniquement les modèles FAS.
- La liste *Autorisations* contient uniquement les utilisateurs autorisés à utiliser FAS. Par exemple, il est recommandé d'empêcher FAS d'émettre des certificats aux utilisateurs d'un groupe Administration ou Utilisateurs protégés.

Configuration de la liste de contrôle d'accès

Comme décrit dans la section Configurer les règles, vous devez configurer une liste de serveurs StoreFront approuvés pour affirmer les identités des utilisateurs auprès de FAS lors de l'émission de certificats. De même, vous pouvez restreindre les utilisateurs auxquels des certificats seront délivrés, et les machines VDA auprès desquelles ils peuvent s'authentifier. Cette fonctionnalité s'ajoute à toutes les fonctionnalités de sécurité standard d'Active Directory ou d'autorité de certification que vous configurez.

Paramètres du pare-feu

Toutes les communications vers les serveurs FAS utilisent des connexions réseau Kerberos Windows Communication Foundation (WCF) mutuellement authentifiées sur le port 80.

Surveillance du journal des événements

FAS et le VDA écrivent des informations dans le journal des événements Windows. Ce journal peut être utilisé pour la surveillance et l'audit des informations. La section Journaux d'événements répertorie les entrées de journal d'événements qui peuvent être générées.

Modules de sécurité matériels

Toutes les clés privées, y compris les clés de certificat utilisateur émises par FAS, sont stockées en tant que clés privées non exportables par le compte Service réseau. FAS prend en charge l'utilisation d'un module de sécurité matériel cryptographique, si votre politique de sécurité l'exige.

La configuration cryptographique de bas niveau est disponible dans le fichier FederatedAuthenticationService.exe.config. Ces paramètres s'appliquent lors de la première création des clés privées. Par conséquent, différents paramètres peuvent être utilisés pour les clés privées de l'autorité d'enregistrement (par exemple, 4096 bits, protégées par TPM) et les certificats utilisateur d'exécution.

PARAMÈTRE	DESCRIPTION
ProviderLegacyCsp	Lorsqu'il est défini sur true, FAS utilise l'API Microsoft CryptoAPI (CAPI). Sinon, FAS utilise

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

PARAMÈTRE	DESCRIPTION
	l'API Microsoft Cryptography Next Generation (CNG).
ProviderName	Nom du fournisseur CAPI ou CNG à utiliser.
ProviderType	Fait référence à la propriété Microsoft KeyContainerPermissionAccessEntry.ProviderType PROV_RSA_AES 24. Doit toujours être 24, sauf si vous utilisez un HSM avec CAPI et que le fournisseur HSM spécifie le contraire.
KeyProtection	Contrôle l'indicateur « Exportable » des clés privées. Permet également l'utilisation du stockage de clés du module de plateforme sécurisée (TPM), si pris en charge par le matériel.
KeyLength	Longueur de clé pour les clés privées RSA. Les valeurs prises en charge sont 1024, 2048 et 4096 (par défaut : 2048).

Responsabilités d'administration

L'administration de l'environnement peut être divisée en les groupes suivants :

NOM	RESPONSABILITÉ
Administrateur d'entreprise	Installer et sécuriser les modèles de certificat dans la forêt
Administrateur de domaine	Configurer les paramètres de stratégie de groupe
Administrateur d'autorité de certification	Configurer l'autorité de certification
Administrateur FAS	Installer et configurer le serveur FAS
Administrateur StoreFront/Citrix Gateway	Configurer l'authentification utilisateur
Administrateur Citrix Virtual Desktops™	Configurer les VDA et les contrôleurs

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

Chaque administrateur contrôle différents aspects du modèle de sécurité global, ce qui permet une approche de défense en profondeur pour sécuriser le système.

Paramètres de stratégie de groupe

Vous pouvez identifier les machines FAS approuvées à l'aide d'une table de correspondance « numéro d'index -> FQDN » configurée via la stratégie de groupe. Lors de la connexion à un serveur FAS, les clients vérifient l'identité Kerberos `HOST\<fqdn>` du serveur FAS. Tous les serveurs qui accèdent au serveur FAS doivent avoir des configurations FQDN identiques pour le même index ; sinon, StoreFront et les VDA peuvent contacter différents serveurs FAS.

Citrix recommande d'appliquer une seule stratégie à toutes les machines de l'environnement afin d'éviter toute erreur de configuration. Soyez prudent lors de la modification de la liste des serveurs FAS, en particulier lors de la suppression ou du réordonnancement des entrées.

Le contrôle de cette GPO doit être limité aux administrateurs FAS (et/ou aux administrateurs de domaine) qui installent et désactivent les serveurs FAS. Veillez à ne pas réutiliser le nom FQDN d'une machine peu de temps après la désactivation d'un serveur FAS.

Modèles de certificat

Si vous ne souhaitez pas utiliser le modèle de certificat Citrix_SmartcardLogon fourni avec FAS, vous pouvez en modifier une copie. Les modifications suivantes sont prises en charge.

Renommer un modèle de certificat

Si vous souhaitez renommer Citrix_SmartcardLogon pour qu'il corresponde à la norme de dénomination de votre modèle organisationnel, vous devez :

- Créez une copie du modèle de certificat et renommez-la pour qu'elle corresponde à la norme de dénomination de votre modèle organisationnel.
- Utilisez les commandes PowerShell de FAS pour administrer FAS, plutôt que l'interface utilisateur administrative. (L'interface utilisateur administrative est uniquement destinée à être utilisée avec les noms de modèles par défaut de Citrix.)
    - Utilisez le composant logiciel enfichable Modèles de certificats MMC de Microsoft ou la commande Publish-FasMsTemplate pour publier votre modèle, et
    - Utilisez la commande New-FasCertificateDefinition pour configurer FAS avec le nom de votre modèle.

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

Modifier les propriétés générales

Vous pouvez modifier la période de validité dans le modèle de certificat.

Ne modifiez pas la période de renouvellement. FAS ignore ce paramètre dans le modèle de certificat. FAS renouvelle automatiquement le certificat à mi-parcours de sa période de validité.

Modifier les propriétés de gestion des requêtes

Ne modifiez pas ces propriétés. FAS ignore ces paramètres dans le modèle de certificat. FAS désélectionne toujours **Autoriser l'exportation de la clé privée** et désélectionne **Renouveler avec la même clé**.

Modifier les propriétés de cryptographie

Ne modifiez pas ces propriétés. FAS ignore ces paramètres dans le modèle de certificat.

Reportez-vous à Protection de la clé privée pour les paramètres équivalents fournis par FAS.

Modifier les propriétés d'attestation de clé

Ne modifiez pas ces propriétés. FAS ne prend pas en charge l'attestation de clé.

Modifier les propriétés des modèles remplacés

Ne modifiez pas ces propriétés. FAS ne prend pas en charge les modèles remplacés.

Modifier les propriétés des extensions

Vous pouvez modifier ces paramètres pour qu'ils correspondent à la politique de votre organisation.

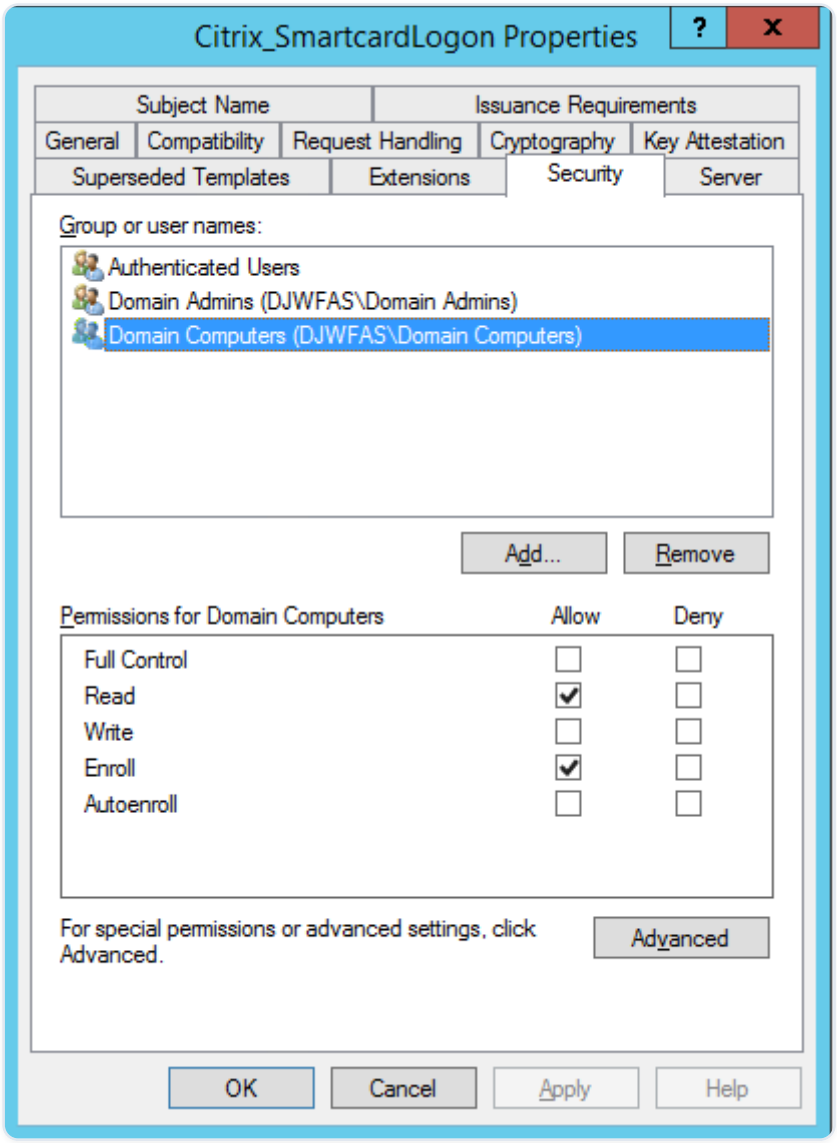
Remarque : Des paramètres d'extension inappropriés peuvent entraîner des problèmes de sécurité ou des certificats inutilisables.

Modifier les propriétés de sécurité

Citrix recommande de modifier ces paramètres pour autoriser les autorisations **Lecture** et **Inscription** uniquement pour les comptes d'ordinateur des serveurs FAS. Le service FAS ne nécessite aucune autre autorisation. Cependant, comme pour les autres modèles de certificat, vous pouvez :

- autoriser les administrateurs à lire ou écrire le modèle
- autoriser les utilisateurs authentifiés à lire le modèle

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



Modifier les propriétés du nom du sujet

Citrix recommande de ne pas modifier ces propriétés.

Le modèle a l'option *Construire à partir de ces informations Active Directory* sélectionnée, ce qui amène l'autorité de certification à inclure le SID de l'utilisateur dans une extension de certificat. Cela fournit un mappage fort vers le compte Active Directory de l'utilisateur.

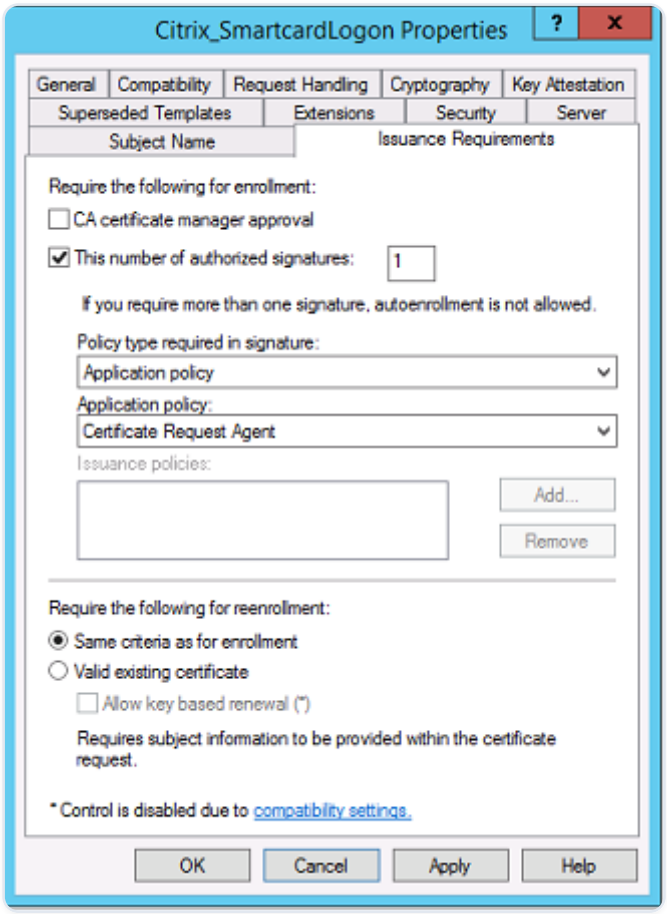
Modifier les propriétés du serveur

Bien que Citrix ne le recommande pas, vous pouvez modifier ces paramètres pour qu'ils correspondent à la politique de votre organisation, si nécessaire.

Modifier les propriétés des exigences d'émission

Ne modifiez pas ces paramètres. Ces paramètres doivent être tels qu'indiqués :

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



Modifier les propriétés de compatibilité

Vous pouvez modifier ces paramètres. Le paramètre doit être au moins **Autorités de certification Windows Server 2003** (version de schéma 2). Cependant, FAS ne prend en charge que les autorités de certification Windows Server 2008 et ultérieures. De plus, comme expliqué ci-dessus, FAS ignore les paramètres supplémentaires disponibles en sélectionnant **Autorités de certification Windows Server 2008** (version de schéma 3) ou **Autorités de certification Windows Server 2012** (version de schéma 4).

Administration de l'autorité de certification

L'administrateur de l'autorité de certification est responsable de la configuration du serveur d'autorité de certification et de l'émission de la clé privée de certificat qu'il utilise.

Publication de modèles

Pour qu'une autorité de certification puisse émettre des certificats basés sur un modèle fourni par l'administrateur d'entreprise, l'administrateur de l'autorité de certification doit choisir de publier ce modèle.

Une pratique de sécurité simple consiste à publier uniquement les modèles de certificat d'autorité d'enregistrement lors de l'installation des serveurs FAS, ou à insister sur un processus d'émission

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

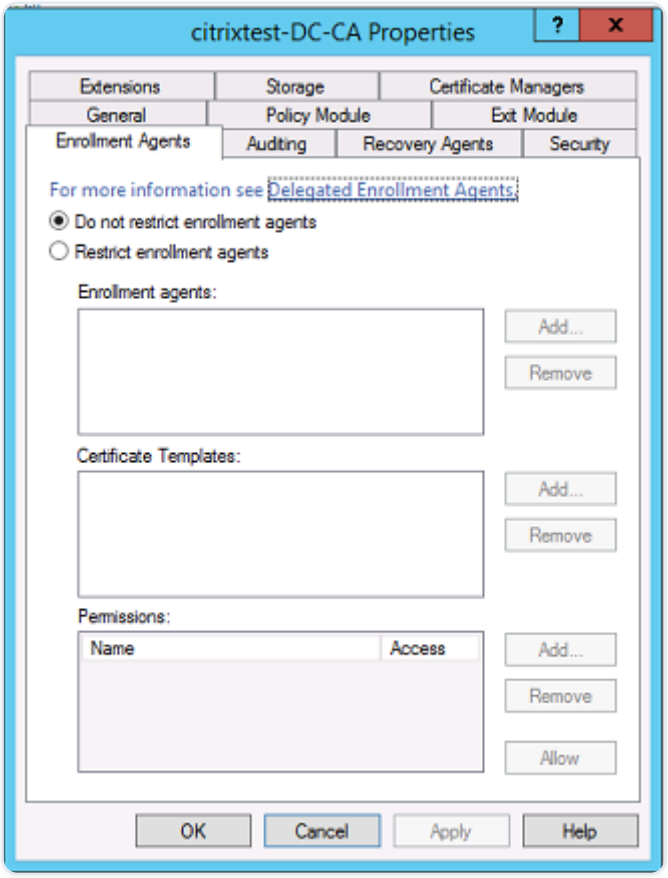
entièrement hors ligne. Dans les deux cas, l'administrateur de l'autorité de certification doit conserver un contrôle total sur l'autorisation des demandes de certificat d'autorité d'enregistrement et disposer d'une politique pour autoriser les serveurs FAS.

Paramètres du pare-feu

L'administrateur de l'autorité de certification contrôle les paramètres du pare-feu réseau de l'autorité de certification, permettant ainsi de contrôler les connexions entrantes. L'administrateur de l'autorité de certification peut configurer les règles DCOM TCP et de pare-feu de manière à ce que seuls les serveurs FAS puissent demander des certificats.

Enregistrement restreint

Par défaut, tout détenteur d'un certificat d'autorité d'enregistrement peut émettre des certificats à tout utilisateur, en utilisant n'importe quel modèle de certificat qui autorise l'accès. Cette fonctionnalité doit être limitée à un groupe d'utilisateurs non privilégiés en utilisant la propriété d'autorité de certification « Restreindre les agents d'inscription ».



Modules de stratégie et audit

Pour les déploiements avancés, des modules de sécurité personnalisés peuvent être utilisés pour suivre et refuser l'émission de certificats.

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

Administration de FAS

FAS dispose de plusieurs fonctionnalités de sécurité.

Restreindre StoreFront, les utilisateurs et les VDA via une ACL

Au centre du modèle de sécurité FAS se trouve le contrôle des comptes Kerberos autorisés à accéder aux fonctionnalités :

VECTEUR D'ACCÈS	DESCRIPTION
StoreFront [IdP]	Ces comptes Kerberos sont considérés comme fiables pour déclarer qu'un utilisateur a été correctement authentifié. Si l'un de ces comptes est compromis, des certificats peuvent être créés et utilisés pour les utilisateurs autorisés par la configuration de FAS.
VDA [Relying party]	Ce sont les machines autorisées à accéder aux certificats et aux clés privées. Un handle d'informations d'identification récupéré par l'IdP est également nécessaire, de sorte qu'un compte VDA compromis dans ce groupe a une portée limitée pour attaquer le système.
Utilisateurs	Cette option contrôle quels utilisateurs peuvent être attestés par l'IdP. Notez qu'il y a un chevauchement avec les options de configuration de l'« agent d'inscription restreint » au niveau de l'autorité de certification. En général, il est conseillé d'inclure uniquement des comptes non privilégiés dans cette liste. Cette fonctionnalité empêche un compte StoreFront compromis d'élever ses privilèges à un niveau administratif supérieur. En particulier, les comptes d'administrateur de domaine ne doivent pas être autorisés par cette ACL.

Configurer les règles

Les règles sont utiles si plusieurs déploiements indépendants de Citrix Virtual Apps™ ou Citrix Virtual Desktops utilisent la même infrastructure de serveur FAS. Chaque règle dispose d'un

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

ensemble distinct d'options de configuration ; en particulier, les listes de contrôle d'accès (ACL) Kerberos peuvent être configurées indépendamment.

Configurer l'autorité de certification et les modèles

Différents modèles de certificat et autorités de certification peuvent être configurés pour différents droits d'accès. Les configurations avancées peuvent choisir d'utiliser des certificats moins ou plus puissants, selon l'environnement. Par exemple, les utilisateurs identifiés comme « externes » peuvent avoir un certificat avec moins de privilèges que les utilisateurs « internes ».

Certificats de session et d'authentification

L'administrateur FAS peut contrôler si le certificat utilisé pour l'authentification est disponible pour une utilisation dans la session de l'utilisateur. Par exemple, cette fonctionnalité pourrait être utilisée pour n'avoir que des certificats de « signature » disponibles en session, le certificat de « connexion » plus puissant n'étant utilisé qu'à la connexion.

Protection de la clé privée et longueur de la clé

L'administrateur FAS peut configurer FAS pour stocker les clés privées dans un module de sécurité matérielle (HSM) ou un module de plateforme sécurisée (TPM). Citrix recommande de stocker la clé privée du certificat de l'autorité d'enregistrement dans un TPM pour des raisons de sécurité. Cette option est fournie dans le cadre du processus de demande de certificat « hors ligne ».

De même, les clés privées des certificats utilisateur peuvent être stockées dans un TPM ou un HSM. Toutes les clés doivent être générées comme « non exportables » et avoir une longueur d'au moins 2048 bits.

Journaux d'événements

Le serveur FAS fournit des journaux d'événements de configuration et d'exécution détaillés, qui peuvent être utilisés pour l'audit et la détection d'intrusion.

Accès administratif et outils d'administration

FAS inclut des fonctionnalités et des outils d'administration à distance (Kerberos authentifié mutuellement). Les membres du « groupe des administrateurs locaux » ont un contrôle total sur la configuration de FAS. Cette liste doit être soigneusement gérée.

Administrateurs Citrix Virtual Apps, Citrix Virtual Desktops et VDA

L'utilisation de FAS ne modifie pas le modèle de sécurité des administrateurs de Delivery Controller et de VDA, car le « handle d'informations d'identification » de FAS remplace simplement

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

le « mot de passe Active Directory ». Les groupes d'administration de Controller et de VDA ne doivent contenir que des utilisateurs de confiance. L'audit et les journaux d'événements doivent être tenus à jour.

Sécurité générale du serveur Windows

Tous les serveurs doivent être entièrement mis à jour et disposer d'un pare-feu standard et d'un logiciel antivirus. Les serveurs d'infrastructure critiques pour la sécurité doivent être conservés dans un emplacement physiquement sécurisé, avec une attention particulière portée au chiffrement des disques et aux options de maintenance des machines virtuelles.

Les journaux d'audit et d'événements doivent être stockés en toute sécurité sur une machine distante.

L'accès RDP doit être limité aux administrateurs autorisés. Dans la mesure du possible, les comptes d'utilisateur doivent exiger une connexion par carte à puce, en particulier pour les comptes d'autorité de certification et d'administrateur de domaine.

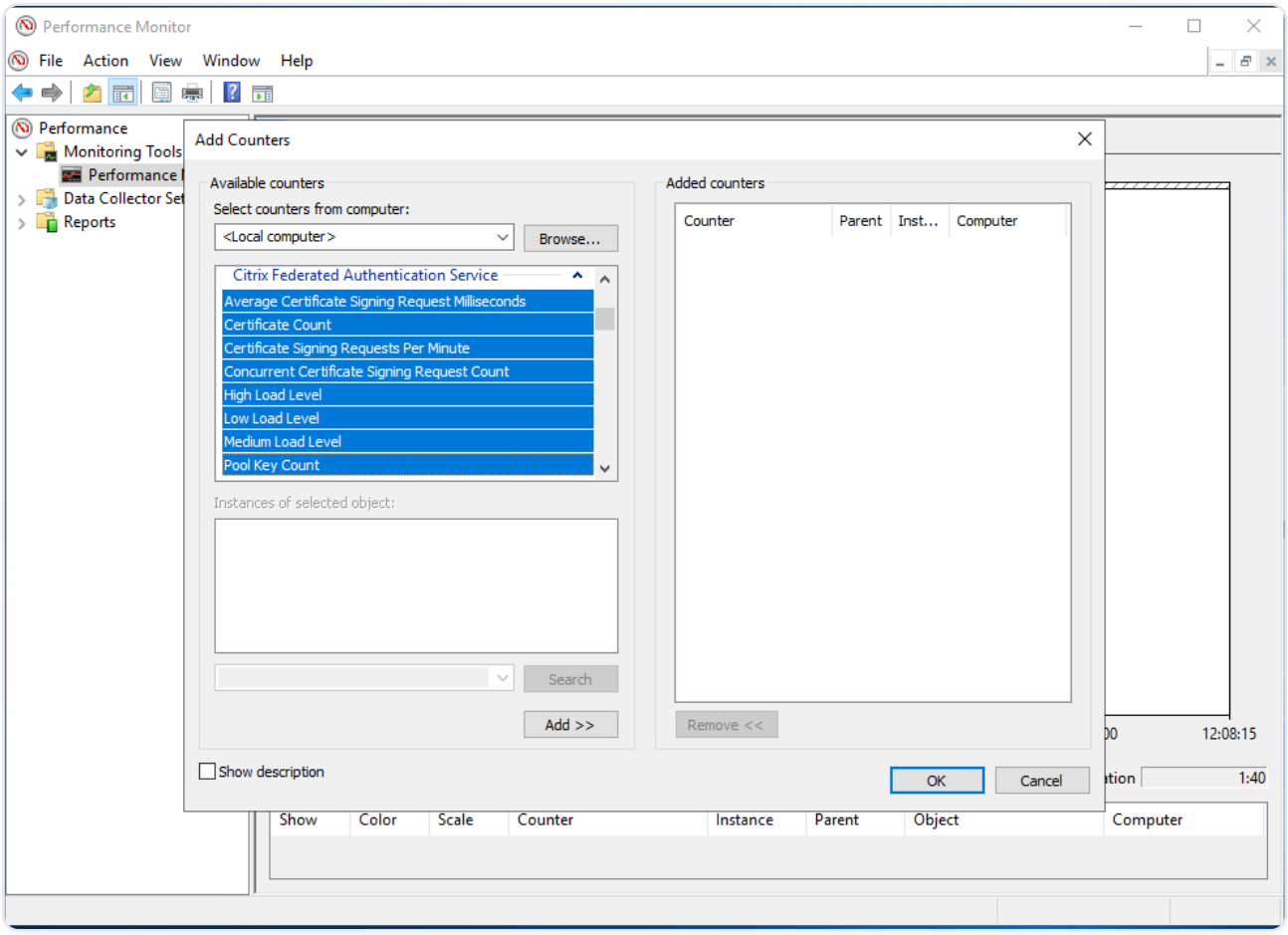
Informations connexes

- Installer et configurer est la référence principale pour l'installation et la configuration de FAS.
- Les architectures FAS sont présentées dans l'article Architectures de déploiement.
- D'autres articles « comment faire » sont présentés dans l'article Configuration avancée.

Compteurs de performance

FAS inclut un ensemble de compteurs de performance à des fins de suivi de charge.

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



Le tableau suivant répertorie les compteurs disponibles. Sauf indication contraire, chaque compteur est mis à jour toutes les 10 secondes.

NOM	DESCRIPTION
Moyenne des millisecondes de demande de signature de certificat	Durée moyenne (en millisecondes) des demandes de signature de certificat, calculée à l'aide des données de la minute précédente.
Nombre de certificats	Le nombre de certificats gérés par le service d'authentification fédérée.
Demandes de signature de certificat par minute	Le nombre de demandes de signature de certificat émises par le service d'authentification fédérée par minute, calculé à l'aide des données de la minute précédente.
Nombre de demandes de signature de certificat simultanées	Le nombre de demandes de signature de certificat simultanées traitées par le service d'authentification fédérée.

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

NOM	DESCRIPTION
Nombre de clés de pool	Le nombre de paires de clés pré-générées dans le pool de clés qui peuvent être utilisées pour les demandes de signature de certificat.
Opérations de clé privée par minute	Le nombre d'opérations de clé privée de certificat effectuées par le service d'authentification fédérée par minute, calculé à l'aide des données de la minute précédente.
Nombre de sessions	Le nombre de sessions VDA suivies par le service d'authentification fédérée.
Niveau de charge faible/moyen/élevé	Estimations de la charge que le service d'authentification fédérée peut accepter en termes de demandes de signature de certificat par minute. Les estimations sont mises à jour chaque minute, à l'aide des données de la minute précédente. Le dépassement du seuil de « charge élevée » peut entraîner l'échec des lancements d'applications ou de bureaux publiés.

Dépanner les problèmes de connexion Windows

Cet article décrit les journaux et les messages d'erreur que Windows fournit lorsqu'un utilisateur se connecte à l'aide de certificats et/ou de cartes à puce. Ces journaux fournissent des informations que vous pouvez utiliser pour dépanner les échecs d'authentification.

Certificats et infrastructure à clé publique

Windows Active Directory gère plusieurs magasins de certificats qui gèrent les certificats pour les utilisateurs qui se connectent.

- **Magasin de certificats NTAuth** : Pour s'authentifier auprès de Windows, l'autorité de certification qui émet directement les certificats utilisateur (c'est-à-dire qu'aucune chaîne n'est prise en charge) doit être placée dans le magasin NTAuth. Pour afficher ces certificats, à partir du programme certutil, saisissez : certutil –viewstore –enterprise NTAuth.
- **Magasins de certificats racine et intermédiaires :** Généralement, les systèmes de connexion par certificat ne peuvent fournir qu'un seul certificat, donc si une chaîne est utilisée,

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

le magasin de certificats intermédiaires sur toutes les machines doit inclure ces certificats. Le certificat racine doit se trouver dans le magasin de racines de confiance (Trusted Root Store), et l'avant-dernier certificat doit se trouver dans le magasin NTAuth.

- **Extensions de certificat de connexion et stratégie de groupe :** Windows peut être configuré pour appliquer la vérification des EKU et d'autres stratégies de certificat. Consultez la documentation Microsoft : `<https://docs.microsoft.com/fr-fr/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)>`.

STRATÉGIE DE REGISTRE	DESCRIPTION
AllowCertificatesWithNoEKU	Lorsqu'elle est désactivée, les certificats doivent inclure l'utilisation étendue de clé (EKU) de connexion par carte à puce.
AllowSignatureOnlyKeys	Par défaut, Windows filtre les clés privées de certificats qui n'autorisent pas le déchiffrement RSA. Cette option annule ce filtre.
AllowTimeInvalidCertificates	Par défaut, Windows filtre les certificats expirés. Cette option annule ce filtre.
EnumerateECCCerts	Active l'authentification par courbe elliptique.
X509HintsNeeded	Si un certificat ne contient pas de nom d'utilisateur principal (UPN) unique, ou s'il peut être ambigu, cette option permet aux utilisateurs de spécifier manuellement leur compte de connexion Windows.
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	Désactive la vérification de la révocation (généralement définie sur le contrôleur de domaine).

- **Certificats de contrôleur de domaine** : Pour authentifier les connexions Kerberos, tous les serveurs doivent disposer de certificats de « contrôleur de domaine » appropriés. Ceux-ci peuvent être demandés à l'aide du menu du composant logiciel enfichable MMC « Magasin personnel de certificats de l'ordinateur local ».

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

Nom UPN et mappage de certificat

Il est recommandé que les certificats utilisateur incluent un nom d'utilisateur principal (UPN) unique dans l'extension Nom alternatif du sujet.

Noms UPN dans Active Directory

Par défaut, chaque utilisateur dans Active Directory possède un UPN implicite basé sur le modèle \<samUsername>@\<domainNetBios> et \<samUsername>@\<domainFQDN>. Les domaines et FQDN disponibles sont inclus dans l'entrée RootDSE de la forêt. Notez qu'un seul domaine peut avoir plusieurs adresses FQDN enregistrées dans le RootDSE.

De plus, chaque utilisateur dans Active Directory possède un UPN explicite et des altUserPrincipalNames. Ce sont des entrées LDAP qui spécifient l'UPN pour l'utilisateur.

Lors de la recherche d'utilisateurs par UPN, Windows recherche d'abord dans le domaine actuel (en fonction de l'identité du processus qui recherche l'UPN) les UPN explicites, puis les UPN alternatifs. S'il n'y a pas de correspondance, il recherche l'UPN implicite, qui peut se résoudre à différents domaines de la forêt.

Service de mappage de certificats

Si un certificat n'inclut pas d'UPN explicite, Active Directory a la possibilité de stocker un certificat public exact pour chaque utilisation dans un attribut « x509certificate ». Pour résoudre un tel certificat à un utilisateur, un ordinateur peut interroger directement cet attribut (par défaut, dans un seul domaine).

Une option est fournie à l'utilisateur pour spécifier un compte utilisateur qui accélère cette recherche, et permet également d'utiliser cette fonctionnalité dans un environnement inter-domaines.

S'il existe plusieurs domaines dans la forêt et que l'utilisateur ne spécifie pas explicitement de domaine, le rootDSE d'Active Directory spécifie l'emplacement du service de mappage de certificats. Celui-ci est généralement situé sur une machine de catalogue global et dispose d'une vue en cache de tous les attributs x509certificate de la forêt. Cet ordinateur peut être utilisé pour trouver efficacement un compte utilisateur dans n'importe quel domaine, en se basant uniquement sur le certificat.

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

Contrôler la sélection du contrôleur de domaine de connexion

Lorsqu'un environnement contient plusieurs contrôleurs de domaine, il est utile de voir et de restreindre le contrôleur de domaine utilisé pour l'authentification, afin que les journaux puissent être activés et récupérés.

Contrôler la sélection du contrôleur de domaine

Pour forcer Windows à utiliser un contrôleur de domaine Windows particulier pour la connexion, vous pouvez définir explicitement la liste des contrôleurs de domaine qu'une machine Windows utilise en configurant le fichier lmhosts : \Windows\System32\drivers\etc\lmhosts.

Il y a généralement un exemple de fichier nommé « lmhosts.sam » à cet emplacement. Incluez simplement une ligne :

1.2.3.4 dcnetbiosname #PRE #DOM:mondomaine

Où « 1.2.3.4 » est l'adresse IP du contrôleur de domaine nommé « dcnetbiosname » dans le domaine « mydomain ».

Après un redémarrage, la machine Windows utilise ces informations pour se connecter à mydomain. Notez que cette configuration doit être annulée une fois le débogage terminé.

Identifier le contrôleur de domaine utilisé

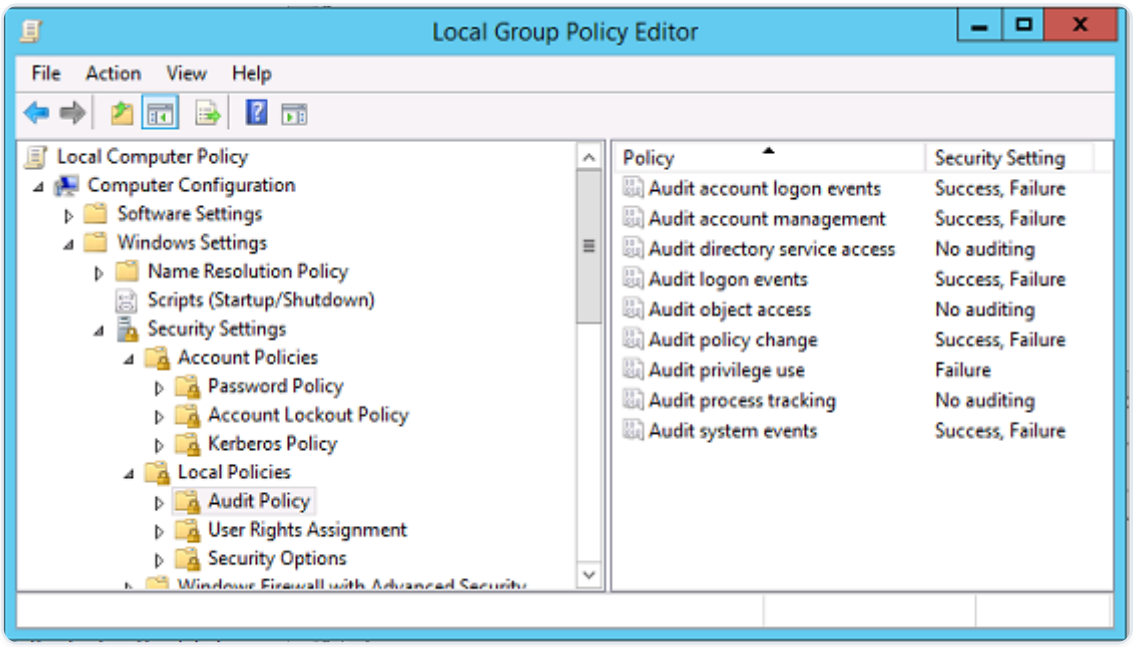
Lors de la connexion, Windows définit une variable d'environnement MSDOS avec le contrôleur de domaine qui a connecté l'utilisateur. Pour le voir, démarrez l'invite de commande avec la commande : **echo %LOGONSERVER%**.

Les journaux relatifs à l'authentification sont stockés sur l'ordinateur renvoyé par cette commande.

Activer les événements d'audit de compte

Par défaut, les contrôleurs de domaine Windows n'activent pas les journaux d'audit de compte complets. Cela peut être contrôlé via les stratégies d'audit dans les paramètres de sécurité de l'éditeur de stratégie de groupe. Une fois activés, le contrôleur de domaine produit des informations de journal d'événements supplémentaires dans le fichier journal de sécurité.

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



Journaux de validation de certificat

Vérifier la validité du certificat

Si un certificat de carte à puce est exporté en tant que certificat DER (aucune clé privée requise), vous pouvez le valider avec la commande : certutil –verify user.cer

Activer la journalisation CAPI

Sur le contrôleur de domaine et la machine des utilisateurs, ouvrez l'observateur d'événements et activez la journalisation pour Microsoft/Windows/CAPI2/Operational Logs.

Vous pouvez contrôler la journalisation CAPI avec les clés de registre à l'emplacement : CurrentControlSet\Services\crypt32.

VALEUR	DESCRIPTION
Niveau de diagnostic (DWORD)	Niveau de verbosité (0 à 5)
Masque de correspondance (QUADWORD)	Filtre d'événements (utiliser 0xffffff pour tout)
Nom du processus de diagnostic (MULTI_SZ)	Filtrer par nom de processus (par exemple, LSASS.exe)

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

Journaux CAPI

MESSAGE	DESCRIPTION
Chaîne de construction	LSA a appelé CertGetCertificateChain (inclut le résultat)
Vérifier la révocation	LSA a appelé CertVerifyRevocation (inclut le résultat)
Objets X509	En mode détaillé, les certificats et les listes de révocation de certificats (CRL) sont vidés dans AppData\LocalLow\Microsoft\X509Objects
Vérifier la politique de chaîne	LSA a appelé CertVerifyChainPolicy (inclut les paramètres)

Messages d'erreur

CODE D'ERREUR	DESCRIPTION
Certificat non approuvé	Le certificat de carte à puce n'a pas pu être créé à l'aide des certificats des magasins de certificats intermédiaires et racines de confiance de l'ordinateur.
Erreur de vérification de la révocation du certificat	La CRL de la carte à puce n'a pas pu être téléchargée à partir de l'adresse spécifiée par le point de distribution CRL du certificat. Si la vérification de la révocation est obligatoire, cela empêche la connexion de réussir. Consultez la section Certificats et infrastructure à clé publique.
Erreurs d'utilisation du certificat	Le certificat n'est pas adapté à la connexion. Par exemple, il peut s'agir d'un certificat de serveur ou d'un certificat de signature.

Journaux Kerberos

Pour activer la journalisation Kerberos, sur le contrôleur de domaine et la machine de l'utilisateur final, créez les valeurs de registre suivantes :

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

RUCHE	NOM DE LA VALEUR	VALEUR [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

La journalisation Kerberos est générée dans le journal des événements système.

- Les messages tels que « certificat non approuvé » devraient être faciles à diagnostiquer.
- Deux codes d'erreur sont informatifs et peuvent être ignorés en toute sécurité :
  - KDC_ERR_PREAUTH_REQUIRED (utilisé pour la compatibilité descendante avec les contrôleurs de domaine plus anciens)
  - Erreur inconnue 0x4b

Journaux du contrôleur de domaine et du poste de travail

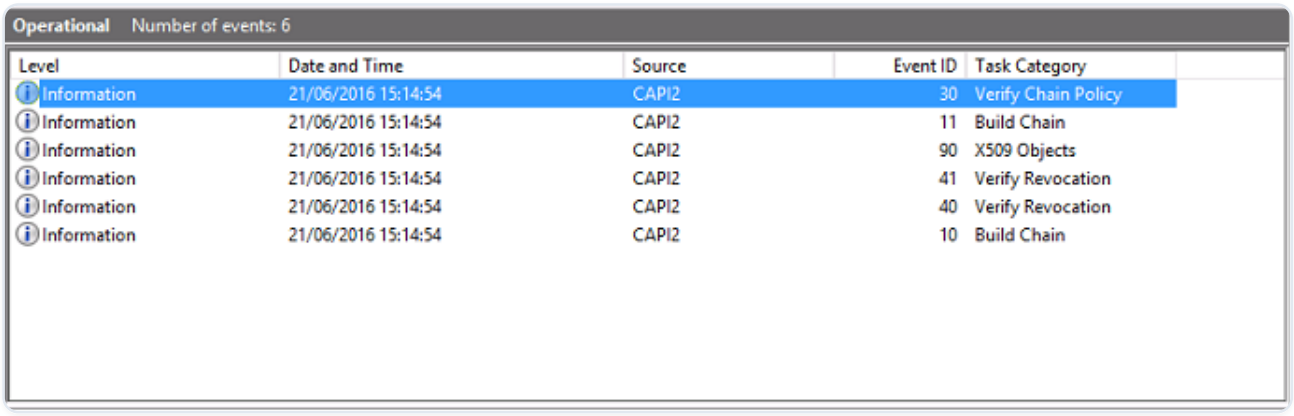
Cette section décrit les entrées de journal attendues sur le contrôleur de domaine et le poste de travail lorsque l'utilisateur se connecte avec un certificat.

- Journal CAPI2 du contrôleur de domaine
- Journaux de sécurité du contrôleur de domaine
- Journal de sécurité du Virtual Delivery Agent (VDA)
- Journal CAPI du VDA
- Journal système du VDA

Journal CAPI2 du contrôleur de domaine

Lors d'une ouverture de session, le contrôleur de domaine valide le certificat de l'appelant, produisant une séquence d'entrées de journal sous la forme suivante.

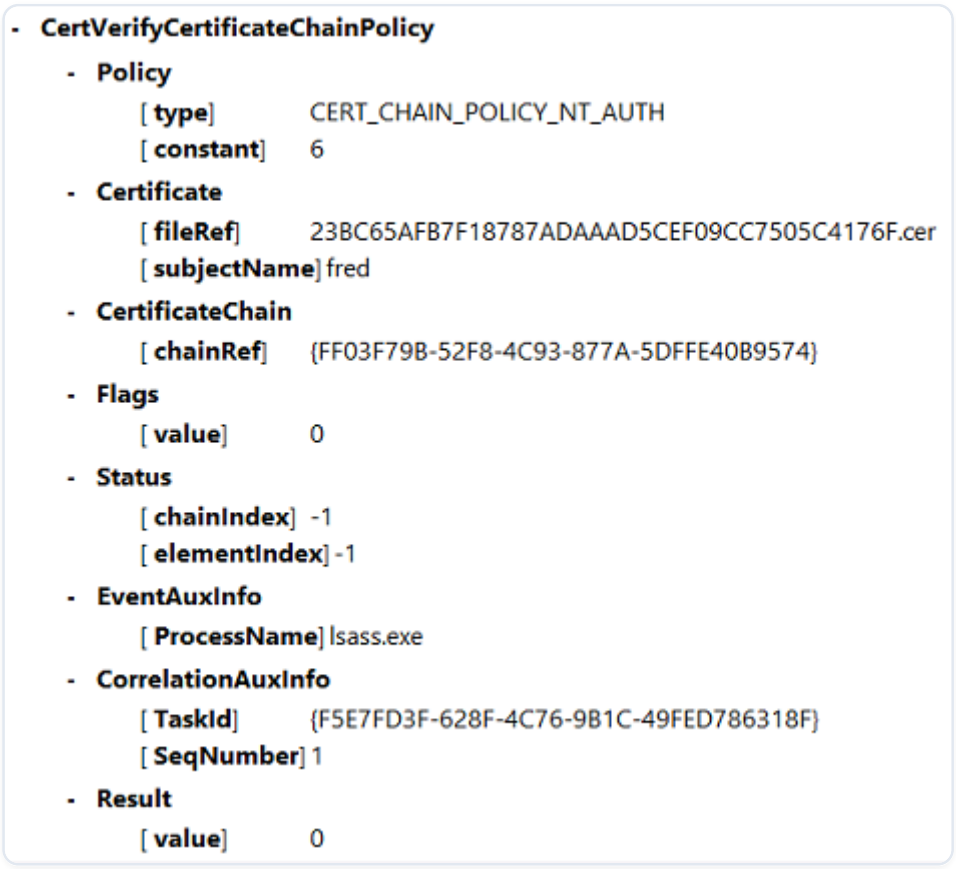
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Operational Number of events: 6

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

Le message final du journal d'événements montre lsass.exe sur le contrôleur de domaine construisant une chaîne basée sur le certificat fourni par le VDA, et la vérifiant pour sa validité (y compris la révocation). Le résultat est renvoyé comme « ERROR_SUCCESS ».



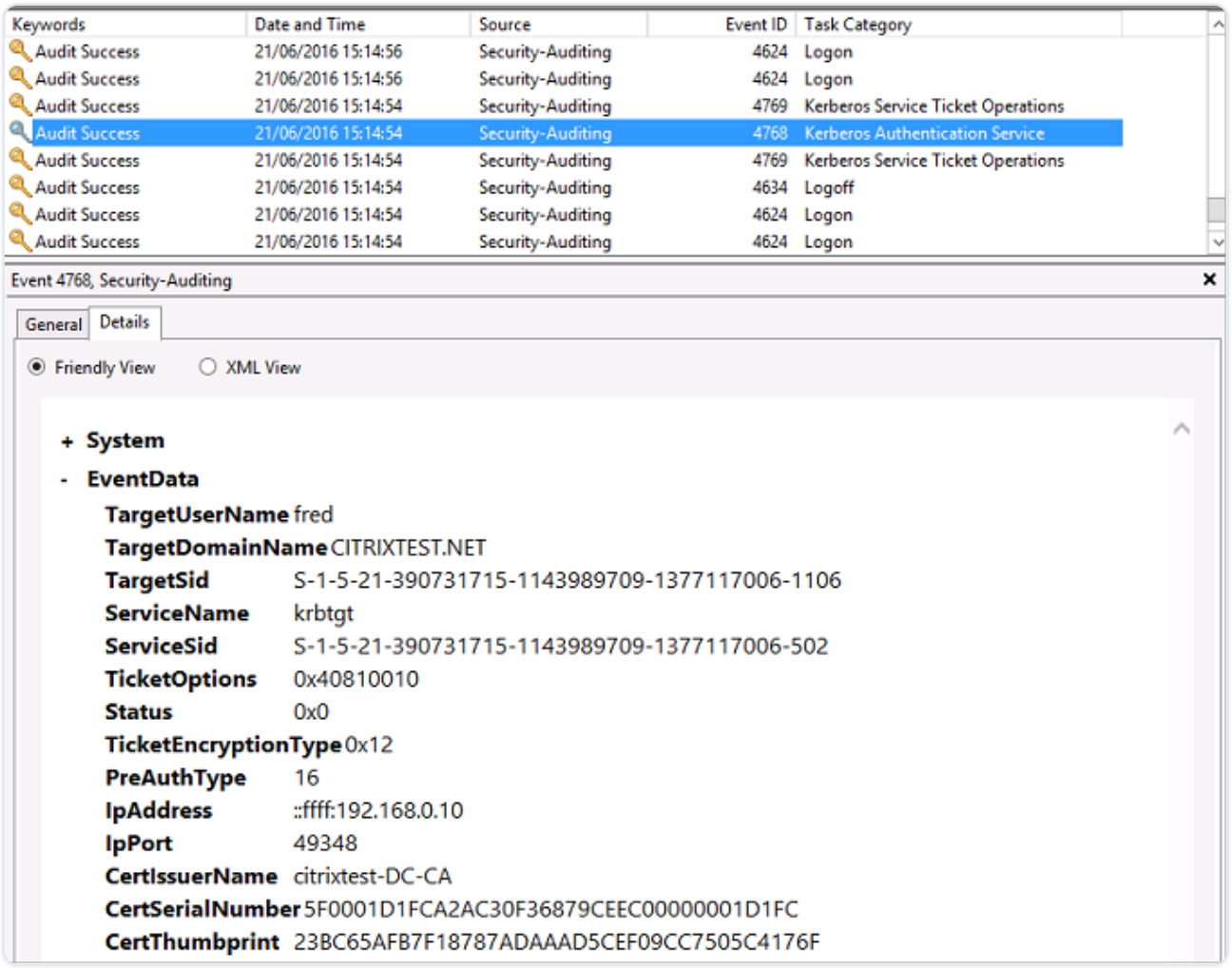
- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [**type**] CERT_CHAIN_POLICY_NT_AUTH
    - [**constant**] 6
  - **Certificate**
    - [**fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [**subjectName**] fred
  - **CertificateChain**
    - [**chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}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

Journal de sécurité du contrôleur de domaine

Le contrôleur de domaine affiche une séquence d'événements d'ouverture de session, l'événement clé étant 4768, où le certificat est utilisé pour émettre le Ticket d'octroi de ticket Kerberos (krbtgt).

Les messages précédents montrent le compte machine du serveur s'authentifiant auprès du contrôleur de domaine. Les messages suivants montrent le compte utilisateur appartenant au nouveau krbtgt étant utilisé pour s'authentifier auprès du contrôleur de domaine.

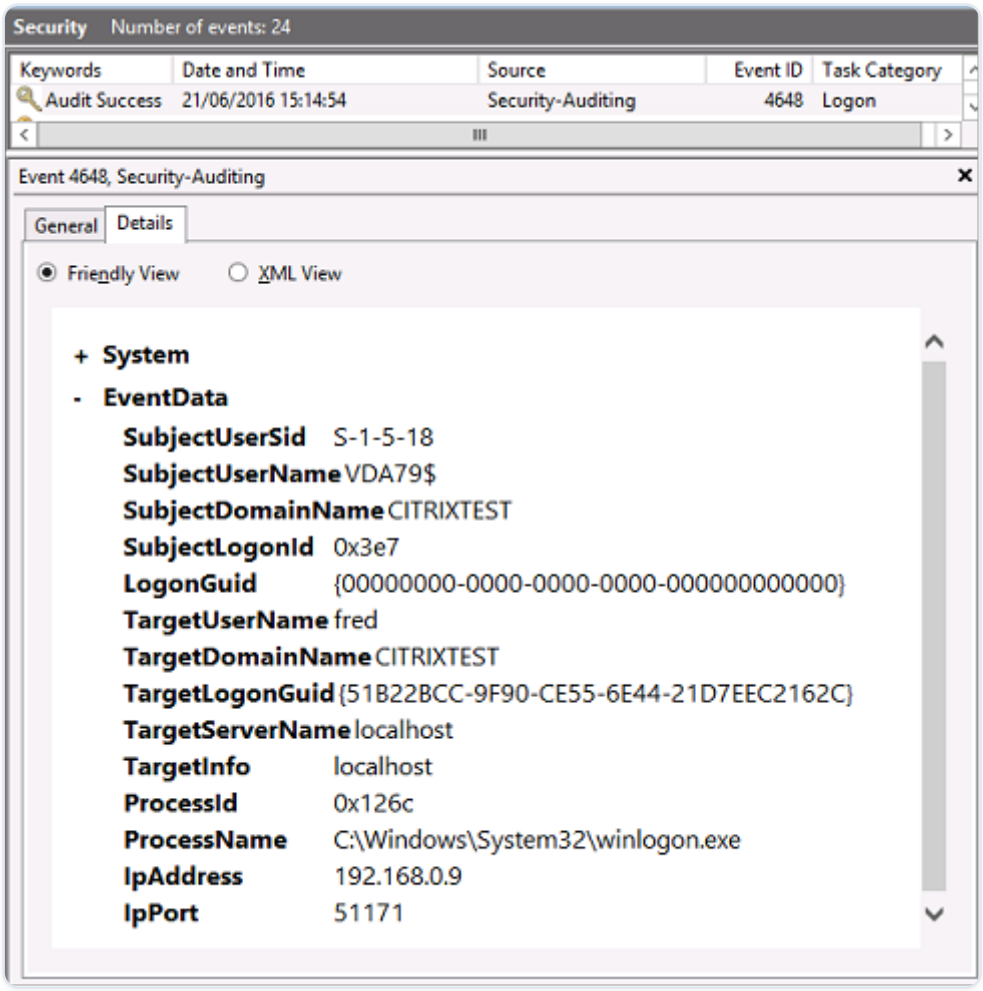
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Journal de sécurité du VDA

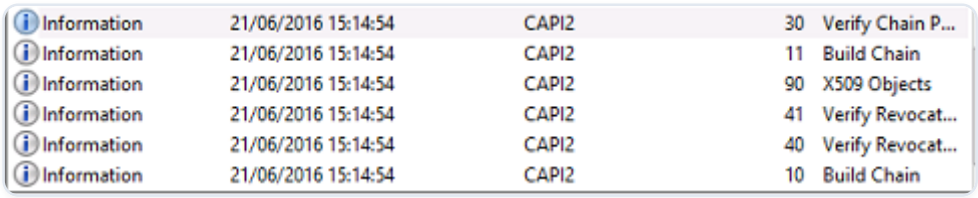
Le journal d'audit de sécurité du VDA correspondant à l'événement d'ouverture de session est l'entrée avec l'ID d'événement 4648, provenant de winlogon.exe.

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

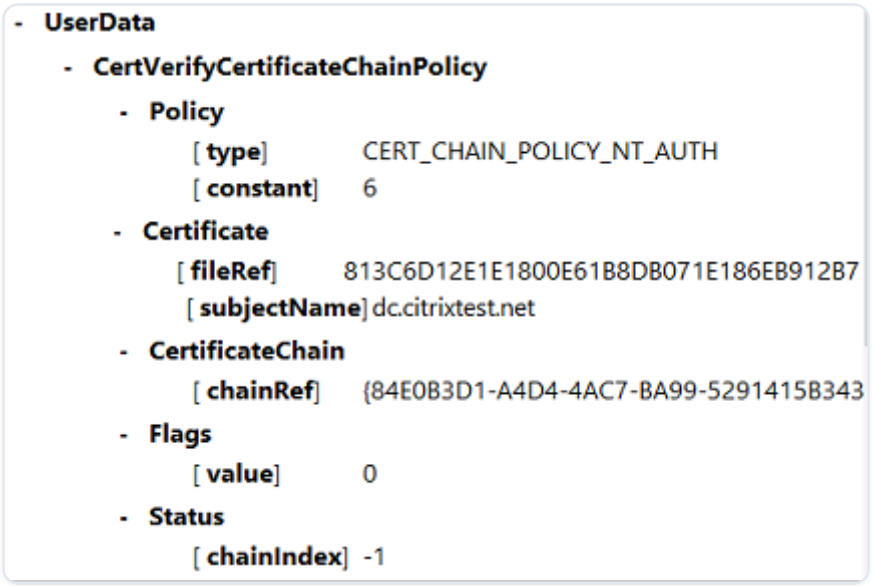


Journal CAPI du VDA

Cet exemple de journal CAPI du VDA montre une séquence unique de construction et de vérification de chaîne à partir de lsass.exe, validant le certificat du contrôleur de domaine (dc.citrixtest.net).

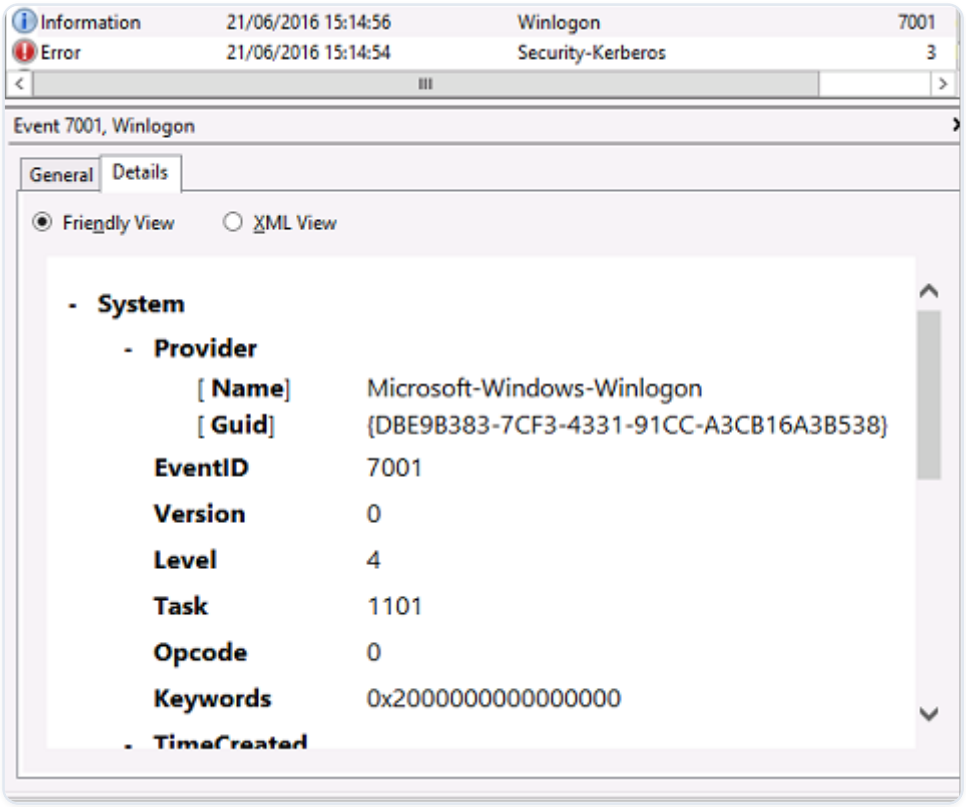


© 1997–2026 Citrix Systems, Inc. All rights reserved.



Journal système du VDA

Lorsque la journalisation Kerberos est activée, le journal système affiche l'erreur KDC_ERR_PREAUTH_REQUIRED (qui peut être ignorée) et une entrée de Winlogon indiquant que l'ouverture de session Kerberos a réussi.



Surveillance de FAS à l'aide du journal d'événements Windows

Tous les événements FAS sont écrits dans le journal d'événements d'application Windows. Vous pouvez utiliser des produits tels que System Center Operations Manager (SCOM) pour surveiller l'état de votre service FAS à l'aide des processus et des événements décrits ici.

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

Le service FAS est-il en cours d’exécution ?

Pour déterminer si le service FAS est en cours d’exécution, surveillez le processus Citrix.Authentication.FederatedAuthenticationService.exe.

Seuls les événements les plus importants pour la surveillance du service FAS sont décrits dans cette section. Pour la liste complète des codes d’événements FAS, consultez Journaux d’événements FAS.

Événements d’intégrité de FAS

Les événements suivants indiquent si votre service FAS est sain.

La source de l'événement est **Citrix.Authentication.FederatedAuthenticationService**.

ÉVÉNEMENT	TEXTE DE L'ÉVÉNEMENT	EXPLICATION	REMARQUES
[S003]	Administrateur [{0}] définissant le mode de maintenance sur [{1}]	Le service FAS a été mis en mode maintenance ou en est sorti.	En mode maintenance, le serveur FAS n'est pas utilisable pour l'authentification unique.
[S022]	Administrateur [{0}] définissant le mode de maintenance sur Désactivé	Le service FAS est sorti du mode maintenance.	Disponible à partir de FAS 10.7 / CVAD 2109.
[S023]	Administrateur [{0}] définissant le mode de maintenance sur Activé	Le service FAS a été mis en mode maintenance.	Disponible à partir de FAS 10.7 / CVAD 2109.
[S123]	Échec de l'émission d'un certificat pour [upn: {0} role: {1}] [exception: {2}]	Cet événement se produit après [S124] si aucune des autorités de certification configurées avec FAS n'a émis de certificat utilisateur avec succès.	Cet événement peut indiquer que toutes les autorités de certification configurées ne fonctionnent pas. Si FAS est configuré pour utiliser un HSM, cela peut également

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

ÉVÉNEMENT	TEXTE DE L'ÉVÉNEMENT	EXPLICATION	REMARQUES
		L'authentification unique échouera pour cet utilisateur.	indiquer que le HSM ne fonctionne pas.
[S124]	Échec de l'émission d'un certificat pour [upn: {0} role: {1}] à [certifcate authority: {2}] [exception: {3}]	Une erreur s'est produite lorsque FAS a tenté de demander un certificat utilisateur à l'autorité de certification donnée. Si FAS est configuré avec plusieurs autorités de certification, FAS tentera la demande auprès d'une autre autorité de certification.	Cet événement peut indiquer que l'autorité de certification ne fonctionne pas ou n'est pas joignable. Si FAS est configuré pour utiliser un HSM, cela peut également indiquer que le HSM ne fonctionne pas. L'exception peut être utilisée pour aider à identifier la cause du problème.
[S413]	Le certificat d'autorisation expire bientôt (il reste {0} jours). Détails du certificat : {1}	Cet événement est généré périodiquement lorsque le certificat d'autorisation FAS est proche de l'expiration. Par défaut, l'événement est généré tous les jours si le certificat d'autorisation expire dans les 30 jours.	Les paramètres par défaut peuvent être ajustés à l'aide de la cmdlet **Set-FasRaCertificateMonitor** ; consultez cmdlets PowerShell.
[S414]	Le certificat d'autorisation a expiré. Détails du certificat : {0}	Cet événement est généré périodiquement lorsque le certificat d'autorisation FAS a expiré. Par défaut, l'événement est	Une fois expiré, FAS n'est plus en mesure de générer de nouveaux certificats utilisateur et l'authentification

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

ÉVÉNEMENT	TEXTE DE L'ÉVÉNEMENT	EXPLICATION	REMARQUES
		généré tous les jours.	unique commence à échouer.

Événements FAS connectés au cloud

Si vous utilisez FAS conjointement avec Citrix Cloud™, les événements suivants indiquent si votre service FAS est sain.

La source de l'événement est **Citrix.Fas.Cloud**.

ÉVÉNEMENT	TEXTE DE L'ÉVÉNEMENT	EXPLICATION	REMARQUES
[S012]	Le service FAS est disponible pour l'authentification unique depuis Citrix Cloud	Cet événement indique que l'authentification unique depuis Workspace (c'est-à-dire Citrix Cloud) devrait fonctionner.	Avant d'émettre cet événement, FAS vérifie (1) qu'il est configuré, (2) qu'il n'est pas en mode maintenance et (3) qu'il est connecté à Citrix Cloud.
[S013]	Le service FAS n'est pas disponible pour l'authentification unique depuis Citrix Cloud. [{0}] Des détails supplémentaires sont disponibles dans la console d'administration.	Cet événement indique que FAS n'est pas en mesure de fournir l'authentification unique depuis Workspace (c'est-à-dire Citrix Cloud). Le message inclut la raison pour laquelle l'authentification unique ne fonctionne pas.	FAS maintient une connexion persistante à Citrix Cloud. De temps à autre, cette connexion peut se terminer pour diverses raisons (telles qu'un problème réseau ou une politique de durée de vie de la connexion sur un serveur proxy). Lorsque cela se produit, le texte de l'événement contient « Le service n'est

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

ÉVÉNEMENT	TEXTE DE L'ÉVÉNEMENT	EXPLICATION	REMARQUES
			pas connecté au cloud ». **Ceci est un comportement normal, et FAS tente immédiatement de rétablir une connexion à Citrix Cloud**.

Événements de sécurité

Les événements suivants indiquent qu'une entité non autorisée a tenté d'utiliser FAS.

La source de l'événement est **Citrix.Authentication.FederatedAuthenticationService**.

ÉVÉNEMENT	TEXTE DE L'ÉVÉNEMENT	EXPLICATION
[S001]	ACCÈS REFUSÉ : L'utilisateur [{0}] n'est pas membre du groupe Administrateurs	Une tentative a été faite pour afficher ou modifier la configuration de FAS, mais l'appelant n'était pas un administrateur FAS.
[S002]	ACCÈS REFUSÉ : L'utilisateur [{0}] n'est pas un administrateur du rôle [{1}]	Une tentative a été faite pour afficher ou modifier la configuration d'une règle FAS, mais l'appelant n'était pas un administrateur FAS.
[S101]	Le serveur [{0}] n'est pas autorisé à affirmer des identités dans le rôle [{1}]	Une tentative a été faite pour affirmer des identités d'utilisateur, mais l'appelant n'est pas autorisé à le faire. Seuls les serveurs StoreFront™ qui ont été autorisés dans la configuration des règles FAS (et Workspace, le cas échéant) sont autorisés à

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

ÉVÉNEMENT	TEXTE DE L'ÉVÉNEMENT	EXPLICATION
		affirmer des identités d'utilisateur.
[S104]	Le serveur [{0}] n'a pas réussi à affirmer l'UPN [{1}] (UPN non autorisé par le rôle [{2}])	Une tentative a été faite pour affirmer une identité d'utilisateur, mais le compte de l'utilisateur n'est pas autorisé selon la configuration des règles FAS.
[S205]	Accès du tiers de confiance refusé - le compte appelant [{0}] n'est pas un tiers de confiance autorisé de la règle [{1}]	Un VDA a tenté d'effectuer une authentification unique avec FAS, mais le VDA n'est pas autorisé selon la configuration des règles FAS.

Journaux d'événements FAS

Les tableaux suivants répertorient les entrées du journal d'événements générées par FAS.

Événements d'administration

Ces événements sont enregistrés en réponse à une modification de configuration dans le serveur FAS.

CODES DE JOURNAL
[S001] ACCÈS REFUSÉ : L'utilisateur [{0}] n'est pas membre du groupe Administrateurs
[S002] ACCÈS REFUSÉ : L'utilisateur [{0}] n'est pas un administrateur du rôle [{1}]
[S003] L'administrateur [{0}] définit le mode de maintenance sur [{1}]
[S004] L'administrateur [{0}] demande un certificat d'autorisation à l'autorité de certification [{1}] en utilisant les modèles [{2} and {3}]
[S005] L'administrateur [{0}] désautorise l'autorité de certification [{1}]
[S006] L'administrateur [{0}] crée une nouvelle définition de certificat [{1}]
[S007] L'administrateur [{0}] met à jour la définition de certificat [{1}]

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

CODES DE JOURNAL
[S008] L'administrateur [{0}] supprime la définition de certificat [{1}]
[S009] L'administrateur [{0}] crée une nouvelle règle [{1}]
[S010] L'administrateur [{0}] met à jour la règle [{1}]
[S011] L'administrateur [{0}] supprime la règle [{1}]
[S012] L'administrateur [{0}] crée un certificat [upn: {1} sid: {2} rule: {3}][Certificate Definition: {4}] [Security Context: {5}]
[S013] L'administrateur [{0}] supprime les certificats [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}]
[S015] L'administrateur [{0}] crée une demande de certificat [TPM: {1}]
[S016] L'administrateur [{0}] importe le certificat d'autorisation [Reference: {1}]
[S022] Administrateur [{0}] définissant le mode maintenance sur Désactivé
[S023] Administrateur [{0}] définissant le mode maintenance sur Activé
[S024] Administrateur [{0}] définissant le moniteur d'intégrité du système
[S025] Administrateur [{0}] définissant le moniteur d'intégrité du système
[S026] Administrateur [{0}] définissant le moniteur de certificat RA
[S027] Administrateur [{0}] réinitialisant le moniteur de certificat RA
[S050] Administrateur [{0}] créant une nouvelle configuration cloud : [{1}]
[S051] Administrateur [{0}] mettant à jour la configuration cloud : [{1}]
[S052] Administrateur [{0}] supprimant la configuration cloud
[S060] Administrateur [{0}] Demande d'enregistrement cloud. Instance : {1}
[S060] Administrateur [{0}] Demande d'enregistrement cloud Direct Trust. Instance : {1} CloudServiceUrlFormat: {2}

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

CODES DE JOURNAL
[S061] Administrateur [{0}] Achèvement de l'enregistrement cloud. Emplacement de la ressource : {1}, Nom de la règle : {2}
[S062] Administrateur [{0}] Enregistrement cloud terminé. Emplacement de la ressource : {1} ({2}), Nom de la règle : {3}, Client : {4} ({5})
[S063] Une erreur KRS s'est produite lors de l'enregistrement cloud. L'exception était {0}
[S063] [S064] Une erreur inconnue s'est produite lors de l'enregistrement cloud. L'exception était {0}

CODES DE JOURNAL
[S401] Mise à niveau de la configuration en cours -- [Depuis la version {0}][to version {1}]
[S402] ERREUR : Le service d'authentification fédérée Citrix doit être exécuté en tant que service réseau [currently running as: {0}]
[S404] Suppression forcée de la base de données du service d'authentification fédérée Citrix
[S405] Une erreur s'est produite lors de la migration des données du registre vers la base de données : [{0}]
[S406] La migration des données du registre vers la base de données est terminée (remarque : les certificats utilisateur ne sont pas migrés)
[S407] Les données basées sur le registre n'ont pas été migrées vers une base de données car une base de données existait déjà
[S408] Impossible de rétrograder la configuration -- [Depuis la version {0}][to version {1}]
[S409] Configuration du pool de threads réussie - MinThreads ajusté de [workers: {0} completion: {1}] à : [workers: {2} completion: {3}]
[S410] Échec de la configuration du pool de threads - impossible d'ajuster MinThreads de [workers: {0} completion: {1}] à : [workers: {2} completion: {3}] ; cela peut impacter l'évolutivité du serveur FAS
[S411] Erreur lors du démarrage du service FAS : [{0}]
[S412] Mise à niveau de la configuration terminée -- [Depuis la version {0}][to version {1}]

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

CODES DE JOURNAL
[S413] Le certificat d'autorisation expire bientôt (il reste {0} jours). Détails du certificat : {1}
[S414] Le certificat d'autorisation a expiré. Détails du certificat : {0}
[S415] Vérification du certificat d'autorisation terminée. {0} problèmes ont été enregistrés. La prochaine vérification est prévue dans {1}

Création d'assertions d'identité

Ces événements sont enregistrés à l'exécution sur le serveur FAS lorsqu'un serveur approuvé affirme une ouverture de session utilisateur.

CODES DE JOURNAL
[S101] Le serveur [{0}] n'est pas autorisé à affirmer des identités dans le rôle [{1}]
[S102] Le serveur [{0}] n'a pas réussi à affirmer l'UPN [{1}] (Exception : {2}{3})
[S103] Le serveur [{0}] a demandé l'UPN [{1}] SID {2}, mais la recherche a renvoyé le SID {3}
[S104] Le serveur [{0}] n'a pas réussi à affirmer l'UPN [{1}] (UPN non autorisé par le rôle [{2}])
[S105] Le serveur [{0}] a émis une assertion d'identité [upn : {1}, rôle {2}, Contexte de sécurité : [{3}]]
[S120] Émission du certificat à [upn : {0} rôle : {1} Contexte de sécurité : [{2}]]
[S121] Certificat émis à [upn: {0} role: {1}] par [certifcate authority: {2}]
[S122] Avertissement : Le serveur est surchargé [upn : {0} rôle : {1}][Requêtes par minute {2}].
[S123] Échec de l'émission d'un certificat pour [upn: {0} role: {1}] [exception: {2}]
[S124] Échec de l'émission d'un certificat pour [upn: {0} role: {1}] à [certifcate authority: {2}] [exception: {3}]

Agir en tant que partie de confiance

Ces événements sont enregistrés lors de l'exécution sur le serveur FAS lorsqu'un VDA connecte un utilisateur.

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

CODES JOURNAL
[S201] La partie de confiance [{0}] n'a pas accès à un mot de passe.
[S202] La partie de confiance [{0}] n'a pas accès à un certificat.
[S203] La partie de confiance [{0}] n'a pas accès au CSP de connexion
[S204] La partie de confiance [{0}] accédant au CSP de connexion pour [upn: {1}] dans le rôle : [{2}] [Operation: {3}] tel qu'autorisé par [{4}]
[S205] Accès de la partie de confiance refusé - le compte appelant [{0}] n'est pas une partie de confiance autorisée de la règle [{1}]
[S206] Le compte appelant [{0}] n'est pas une partie de confiance
[S208] L'opération de clé privée a échoué [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}] [Error {4} {5}].

Serveur de certificats en session

Ces événements sont enregistrés sur le serveur FAS lorsqu'un utilisateur utilise un certificat en session.

CODES JOURNAL
[S301] Accès refusé : L'utilisateur [{0}] n'a pas accès à une carte à puce virtuelle
[S302] L'utilisateur [{0}] a demandé une carte à puce virtuelle inconnue [thumbprint: {1}]
[S303] Accès refusé : L'utilisateur [{0}] ne correspond pas à la carte à puce virtuelle [upn: {1}]
[S304] L'utilisateur [{0}] exécute le programme [{1}] sur l'ordinateur [{2}] à l'aide de la carte à puce virtuelle [upn: {3} role: {4} thumbprint: {5}] pour l'opération de clé privée [{6}]
[S305] L'opération de clé privée a échoué [Opération : {0}][upn : {1} rôle : {2} containerName {3}] [Error {4} {5}].

Plug-in d'assertion FAS

Ces événements sont enregistrés par le plug-in d'assertion FAS.

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

CODES DE JOURNAL
[S500] Aucun plug-in d'assertion FAS n'est configuré
[S501] Le plug-in d'assertion FAS configuré n'a pas pu être chargé [exception:{0}]
[S502] Plug-in d'assertion FAS chargé [pluginId={0}] [assembly={1}] [location={2}]
[S503] Le serveur [{0}] n'a pas pu affirmer l'UPN [{1}] (des preuves d'ouverture de session ont été fournies mais le plug-in [{2}] ne les prend pas en charge)
[S504] Le serveur [{0}] n'a pas pu affirmer l'UPN [{1}] (des preuves d'ouverture de session ont été fournies mais aucun plug-in FAS n'est configuré)
[S505] Le serveur [{0}] n'a pas pu affirmer l'UPN [{1}] (le plug-in [{2}] a rejeté les preuves d'ouverture de session avec le statut [{3}] et le message [{4}])
[S506] Le plug-in [{0}] a accepté les preuves d'ouverture de session du serveur [{1}] pour l'UPN [{2}] avec le message [{3}]
[S507] Le serveur [{0}] n'a pas pu affirmer l'UPN [{1}] (le plug-in [{2}] a levé l'exception [{3}] pendant la méthode [{4}])
[S507] Le serveur [{0}] n'a pas pu affirmer l'UPN [{1}] (le plug-in [{2}] a levé l'exception [{3}])
[S508] Le serveur [{0}] n'a pas pu affirmer l'UPN [{1}] (une disposition d'accès a été fournie mais le plug-in [{2}] ne la prend pas en charge)
[S509] Le serveur [{0}] n'a pas pu affirmer l'UPN [{1}] (une disposition d'accès a été fournie mais aucun plug-in FAS n'est configuré)
[S510] Le serveur [{0}] n'a pas pu affirmer l'UPN [{1}] (la disposition d'accès a été jugée invalide par le plug-in [{2}])

FAS activé pour Workspace

Ces événements sont enregistrés lorsque FAS est utilisé conjointement avec Workspace.

CODES DE JOURNAL
[S001] Clé d'autorisation Citrix Cloud pivotée [fas id: {0}] [old key id:{1}] [new key id:{2}]
[S002] Le module de support cloud démarre. URL du service cloud FasHub : {0}

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

CODES DE JOURNAL
[S003] FAS enregistré auprès du cloud [fas id: {0}] [transaction id: {1}]
[S004] FAS n'a pas pu s'enregistrer auprès du cloud [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S005] FAS a envoyé sa configuration actuelle au cloud [fas id: {0}] [transaction id: {1}]
[S006] FAS n'a pas pu envoyer sa configuration actuelle au cloud [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S007] FAS désenregistré du cloud [fas id: {0}] [transaction id: {1}]
[S009] FAS n'a pas pu se désenregistrer du cloud [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S010] Le service FAS est connecté à l'URL de messagerie cloud : {0}
[S011] Le service FAS n'est pas connecté au cloud
[S012] Le service FAS est disponible pour l'authentification unique depuis Citrix Cloud
[S013] Le service FAS n'est pas disponible pour l'authentification unique depuis Citrix Cloud. [{0}] Plus de détails sont disponibles dans la console d'administration
[S014] Un appel au service cloud `<service name>` a échoué [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S015] Un message de Citrix Cloud a été bloqué car l'appelant n'est pas autorisé [message ID {0}] [transaction ID {1}] [caller {2}]
[S016] Un appel au service cloud `<service name>` a réussi [fas id: {0}] [transaction id: {1}]
[S019] FAS a téléchargé sa configuration depuis le cloud [fas id: {0}] [transaction id: {1}]
[S020] FAS n'a pas pu télécharger sa configuration depuis le cloud [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S021] Le module de support cloud n'a pas pu démarrer. Exception : {0}
[S022] Le module de support cloud s'arrête
[S023] Échec de la rotation de la clé d'autorisation Citrix Cloud [fas id: {0}] [current key id:{1}] [new key id:{2}] [keys in cloud:{3}]

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

CODES DE JOURNAL
[S024] Initialisation de la rotation de la clé d'autorisation Citrix Cloud [fas id: {0}] [current key id:{1}] [new key id:{2}]
[S025] La clé d'autorisation de ce service est présente dans Citrix Cloud [current key: {0}] [keys in cloud: {1}]
[S026] La clé d'autorisation de ce service n'est pas présente dans Citrix Cloud [current key: {0}] [keys in cloud: {1}]
[S027] Mise à niveau du format de stockage de la clé d'autorisation Citrix Cloud [fas id: {0}]

Ouverture de session

Ces événements sont enregistrés sur le VDA pendant la phase d'ouverture de session.

CODES DE JOURNAL
[S101] Échec de l'ouverture de session par assertion d'identité. Service d'authentification fédérée non reconnu [id: {0}]
[S102] Échec de l'ouverture de session par assertion d'identité. Impossible de rechercher le SID pour {0} [Exception: {1}{2}]
[S103] Échec de l'ouverture de session par assertion d'identité. L'utilisateur {0} a le SID {1}, SID attendu {2}
[S104] Échec de l'ouverture de session par assertion d'identité. Échec de la connexion au service d'authentification fédérée : {0} [Error: {1} {2}]
[S105] Ouverture de session par assertion d'identité. Connexion en cours [Nom d'utilisateur : {0}] [Domain: {1}]
[S106] Ouverture de session par assertion d'identité.\n\nService d'authentification fédérée : {0}\n\nConnexion en cours [Certificate: {1}]
[S107] Échec de l'ouverture de session par assertion d'identité. [Exception: {0}{1}]
[S108] Sous-système d'assertion d'identité. ACCÈS_REFUSÉ [Caller: {0}]

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

Certificats de session

Ces événements sont enregistrés sur le VDA lorsqu'un utilisateur tente d'utiliser un certificat de session.

CODES DE JOURNAL
[S201] Accès à la carte à puce virtuelle autorisé par [{0}] pour [PID : {1} Nom du programme : {2}] [Certificate thumbprint: {3}]
[S203] Sous-système de carte à puce virtuelle. Accès refusé [caller: {0}, session {1}]
[S204] Sous-système de carte à puce virtuelle. Prise en charge de la carte à puce désactivée

Demande de certificat et génération de paires de clés

Ces événements sont enregistrés lorsque le serveur FAS effectue des opérations cryptographiques de bas niveau.

CODES DE JOURNAL
[S001] TrustArea::TrustArea : Certificat installé [TrustArea: {0}] [Certificate {1}] [TrustAreaJoinParameters{2}
[S014] Pkcs10Request::Create : Demande PKCS10 créée [Distinguished Name {0}]
[S016] PrivateKey::Create [Identifier {0}][MachineWide: {1}][Provider: {2}][ProviderType: {3}] [EllipticCurve: {4}][KeyLength: {5}][isExportable: {6}]
[S017] PrivateKey::Delete [CspName: {0}, Identifier {1}]

CODES JOURNAL
[S104] MicrosoftCertificateAuthority::GetCredentials : Autorisé à utiliser {0}
[S105] MicrosoftCertificateAuthority::SubmitCertificateRequest Erreur lors de la soumission de la réponse [{0}]
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest Certificat émis [{0}]
[S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - En attente d'approbation [CR_DISP_UNDER_SUBMISSION] [Reference: {0}]

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

Messages d'erreur de l'utilisateur final

Cette section répertorie les messages d'erreur courants affichés à un utilisateur sur la page de connexion Windows.

MESSAGE D'ERREUR AFFICHÉ	DESCRIPTION ET RÉFÉRENCE
Nom d'utilisateur ou mot de passe invalide	L'ordinateur estime que vous disposez d'un certificat et d'une clé privée valides, mais le contrôleur de domaine Kerberos a rejeté la connexion. Consultez la section *Journaux Kerberos* de cet article.
Le système n'a pas pu vous connecter. Vos informations d'identification n'ont pas pu être vérifiées. / La demande n'est pas prise en charge	Le contrôleur de domaine ne peut pas être contacté, ou le contrôleur de domaine n'a pas été configuré avec un certificat pour prendre en charge l'authentification par carte à puce. Enregistrez le contrôleur de domaine pour un certificat « Authentification Kerberos », « Authentification de contrôleur de domaine » ou « Contrôleur de domaine ». Cela vaut généralement la peine d'être essayé, même lorsque le certificat existant semble valide.
Le système n'a pas pu vous connecter. Le certificat de carte à puce utilisé pour l'authentification n'était pas approuvé.	Les certificats intermédiaires et racine ne sont pas installés sur l'ordinateur local. Voir Certificats et infrastructure à clé publique.
Requête incorrecte	Cela indique généralement que les extensions du certificat ne sont pas configurées correctement, ou que la clé RSA est trop courte (<2048 bits).

Informations connexes

- Configuration d'un domaine pour l'ouverture de session par carte à puce : `<http://support.citrix.com/article/CTX206156>`
- Stratégies d'ouverture de session par carte à puce : `<https://docs.microsoft.com/fr-fr/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)>`
- Activation de la journalisation CAPI : `<http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx>`

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

- Activation de la journalisation Kerberos : `<https://support.microsoft.com/fr-fr/kb/262177>`
- Directives pour l'activation de l'ouverture de session par carte à puce avec des autorités de certification tierces : `<https://support.microsoft.com/fr-fr/kb/281245>`

Applets de commande PowerShell

Vous pouvez utiliser la console d’administration du service d’authentification fédérée (FAS) pour les déploiements simples ; toutefois, l’interface PowerShell offre des options plus avancées. Si vous prévoyez d’utiliser des options qui ne sont pas disponibles dans la console, Citrix recommande d’utiliser uniquement PowerShell pour la configuration.

La commande suivante ajoute les applets de commande PowerShell FAS :

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

Dans une fenêtre PowerShell, vous pouvez utiliser Get-Help \<*cmdlet name*> pour afficher l’aide de l’applet de commande.

Pour plus d’informations sur les applets de commande du SDK PowerShell FAS, consultez `<https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/>`.

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

Architectures de déploiement

Introduction

Le service d'authentification fédérée (FAS) est un composant Citrix® qui s'intègre à votre autorité de certification Active Directory, permettant aux utilisateurs d'être authentifiés de manière transparente dans un environnement Citrix. Ce document décrit diverses architectures d'authentification qui peuvent être appropriées pour votre déploiement.

Lorsqu'il est activé, FAS délègue les décisions d'authentification des utilisateurs aux serveurs StoreFront approuvés. StoreFront dispose d'un ensemble complet d'options d'authentification intégrées basées sur les technologies web modernes, et est facilement extensible à l'aide du SDK StoreFront ou de plugins IIS tiers. L'objectif de conception de base est que toute technologie d'authentification capable d'authentifier un utilisateur sur un site web peut désormais être utilisée pour se connecter à un déploiement Citrix Virtual Apps ou Citrix Virtual Desktops™.

Ce document décrit des exemples d'architectures de déploiement de haut niveau, par ordre de complexité croissante.

- Déploiement interne
- Déploiement Citrix Gateway
- ADFS SAML
- Mappage de compte B2B
- Jonction Azure AD Windows 10

Des liens sont fournis vers des articles FAS connexes. Pour toutes les architectures, l'article Installer et configurer est la référence principale pour la configuration de FAS.

Vue d'overview de l'architecture

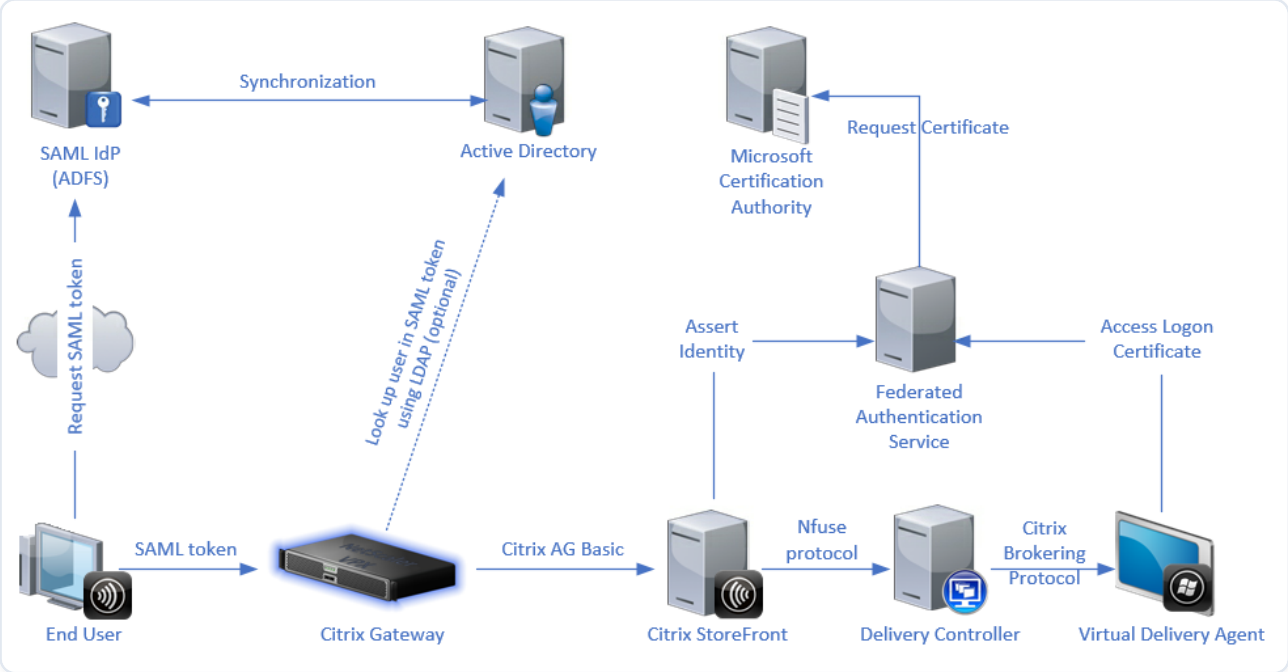
FAS est autorisé à émettre automatiquement des certificats de classe carte à puce au nom des utilisateurs Active Directory authentifiés par StoreFront. Cela utilise des API similaires à celles des outils qui permettent aux administrateurs de provisionner des cartes à puce physiques. Lorsqu'un utilisateur est acheminé vers un agent de livraison virtuel (VDA) Citrix Virtual Apps™ ou Citrix

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

Virtual Desktops, le certificat est attaché à la machine, et le domaine Windows considère la connexion comme une authentification par carte à puce standard.

Les serveurs StoreFront™ approuvés contactent FAS lorsque les utilisateurs demandent l'accès à l'environnement Citrix. FAS accorde un ticket qui permet à une seule session Citrix Virtual Apps ou Citrix Virtual Desktops de s'authentifier avec un certificat pour cette session. Lorsqu'un VDA doit authentifier un utilisateur, il se connecte à FAS et utilise le ticket. Seul FAS a accès à la clé privée du certificat utilisateur ; le VDA doit envoyer chaque opération de signature et de déchiffrement qu'il doit effectuer avec le certificat à FAS.

Le diagramme suivant montre FAS s'intégrant à une autorité de certification Microsoft et fournissant des services de support à StoreFront et aux agents de livraison virtuels (VDA) Citrix Virtual Apps and Desktops™.



Déploiement interne

FAS permet aux utilisateurs de s'authentifier en toute sécurité auprès de StoreFront à l'aide de diverses options d'authentification (y compris l'authentification unique Kerberos) et de se connecter à une session Citrix HDX™ entièrement authentifiée.

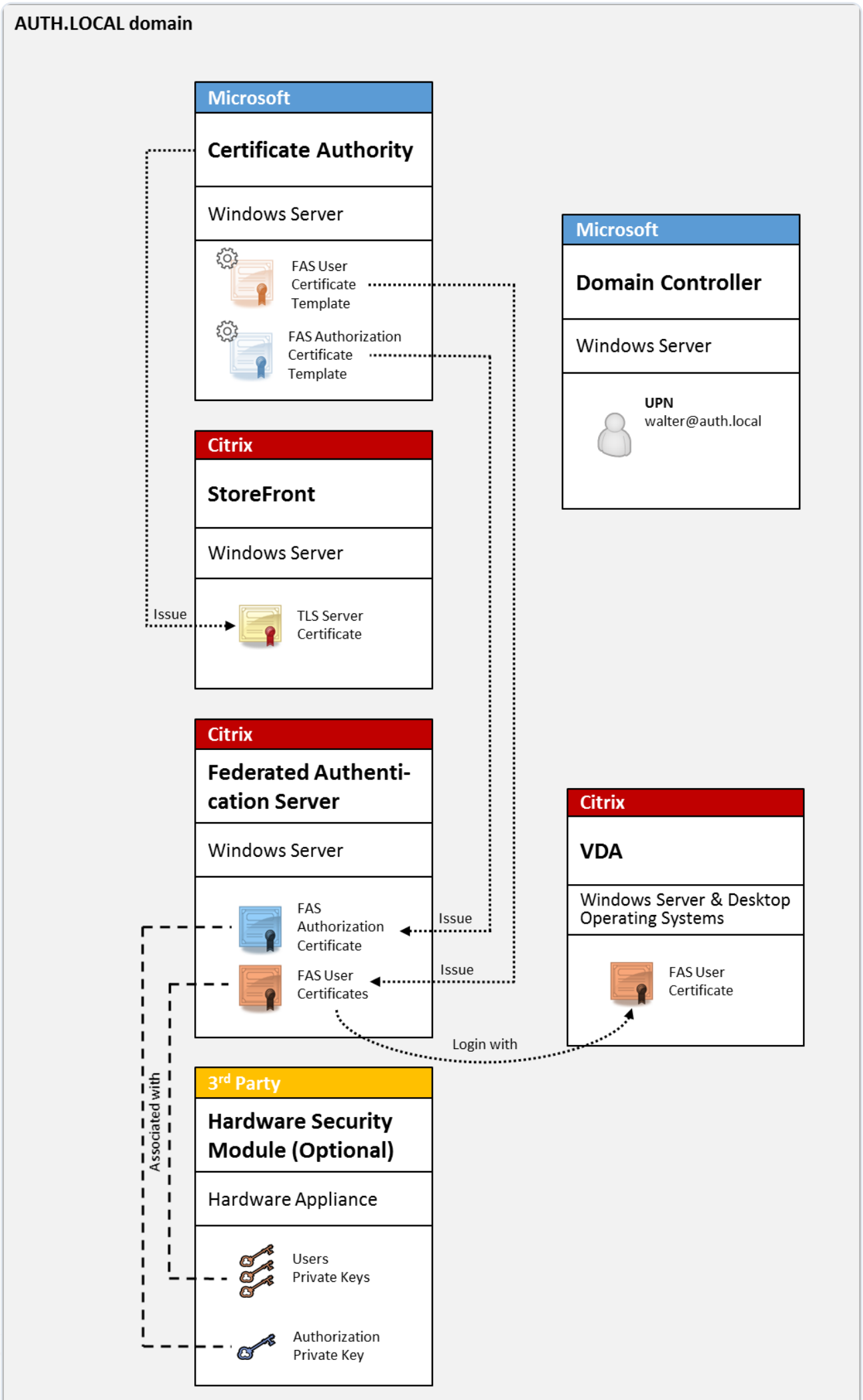
Cela permet l'authentification Windows sans invites de saisie des informations d'identification de l'utilisateur ou des codes PIN de carte à puce, et sans utiliser les fonctionnalités de « gestion des mots de passe enregistrés » telles que le service d'authentification unique. Ceci peut être utilisé pour remplacer les fonctionnalités de connexion par délégation contrainte Kerberos disponibles dans les versions antérieures de Citrix Virtual Apps.

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

Tous les utilisateurs ont accès aux certificats d'infrastructure à clé publique (PKI) au sein de leur session, qu'ils se connectent ou non aux périphériques de point de terminaison avec une carte à puce. Cela permet une migration en douceur vers des modèles d'authentification à deux facteurs, même à partir de périphériques tels que les smartphones et les tablettes qui ne disposent pas de lecteur de carte à puce.

Ce déploiement ajoute un nouveau serveur exécutant FAS, qui est autorisé à émettre des certificats de classe carte à puce au nom des utilisateurs. Ces certificats sont ensuite utilisés pour se connecter aux sessions utilisateur dans un environnement Citrix HDX comme si une connexion par carte à puce avait été utilisée.

© 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

L'environnement Citrix Virtual Apps ou Citrix Virtual Desktops doit être configuré de manière similaire à la connexion par carte à puce, ce qui est documenté dans CTX206156.

Dans un déploiement existant, cela implique généralement de s'assurer qu'une autorité de certification Microsoft jointe au domaine est disponible, et que des certificats de contrôleur de domaine ont été attribués aux contrôleurs de domaine. (Consultez la section « Émission de certificats de contrôleur de domaine » dans CTX206156.)

Informations connexes :

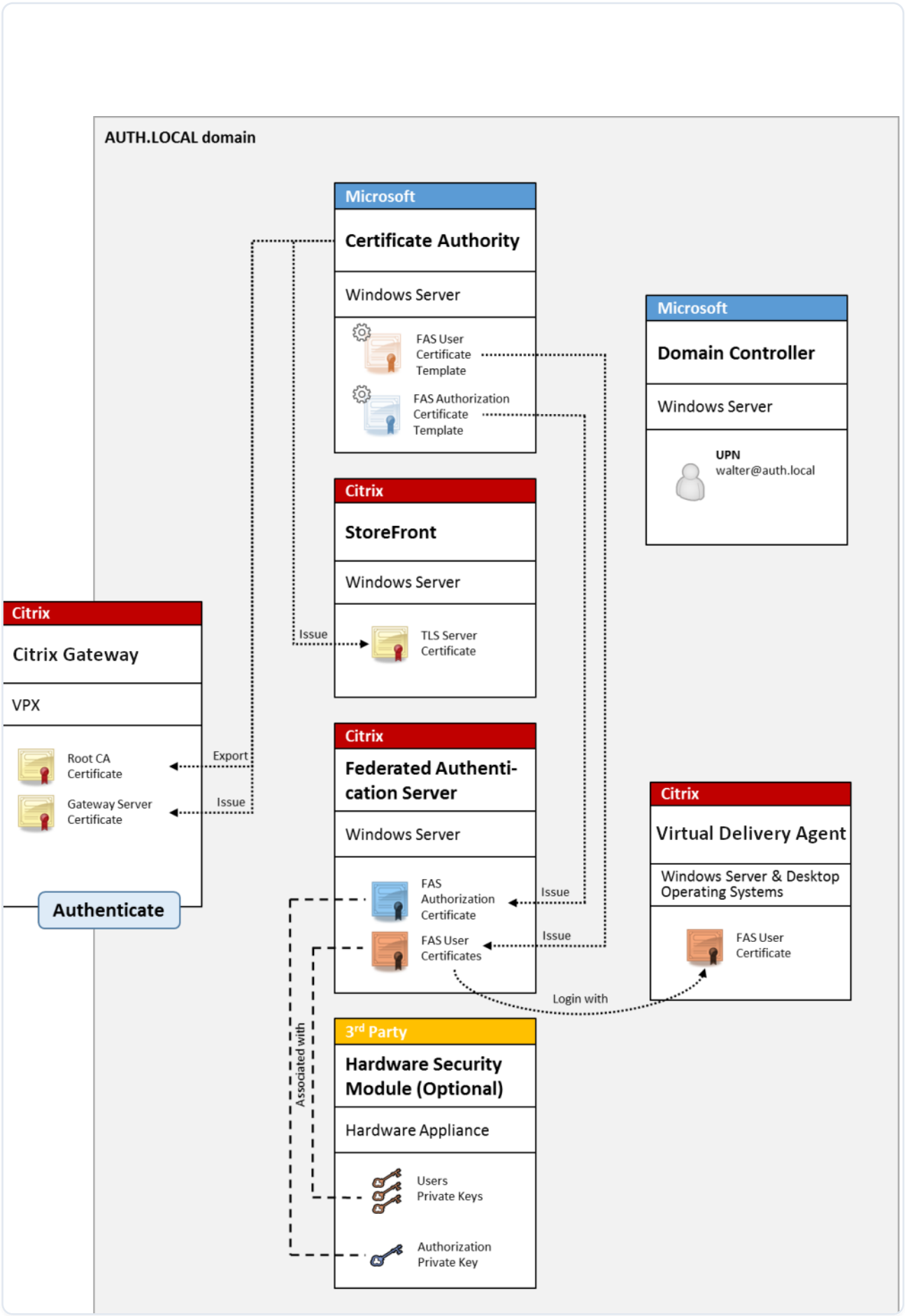
- Les clés peuvent être stockées dans un module de sécurité matérielle (HSM) ou un module de plateforme sécurisée (TPM) intégré. Pour plus de détails, consultez l'article Protection des clés privées.
- L'article Installer et configurer décrit comment installer et configurer FAS.

Déploiement de Citrix Gateway

Le déploiement de Citrix Gateway est similaire au déploiement interne, mais ajoute Citrix Gateway associé à StoreFront, déplaçant le point d'authentification principal vers Citrix Gateway lui-même. Citrix Gateway inclut des options d'authentification et d'autorisation sophistiquées qui peuvent être utilisées pour sécuriser l'accès à distance aux sites Web d'une entreprise.

Ce déploiement peut être utilisé pour éviter les multiples invites de code PIN qui se produisent lors de l'authentification initiale auprès de Citrix Gateway, puis de la connexion à une session utilisateur. Il permet également l'utilisation de technologies d'authentification avancées de Citrix Gateway sans nécessiter en plus des mots de passe AD ou des cartes à puce.

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

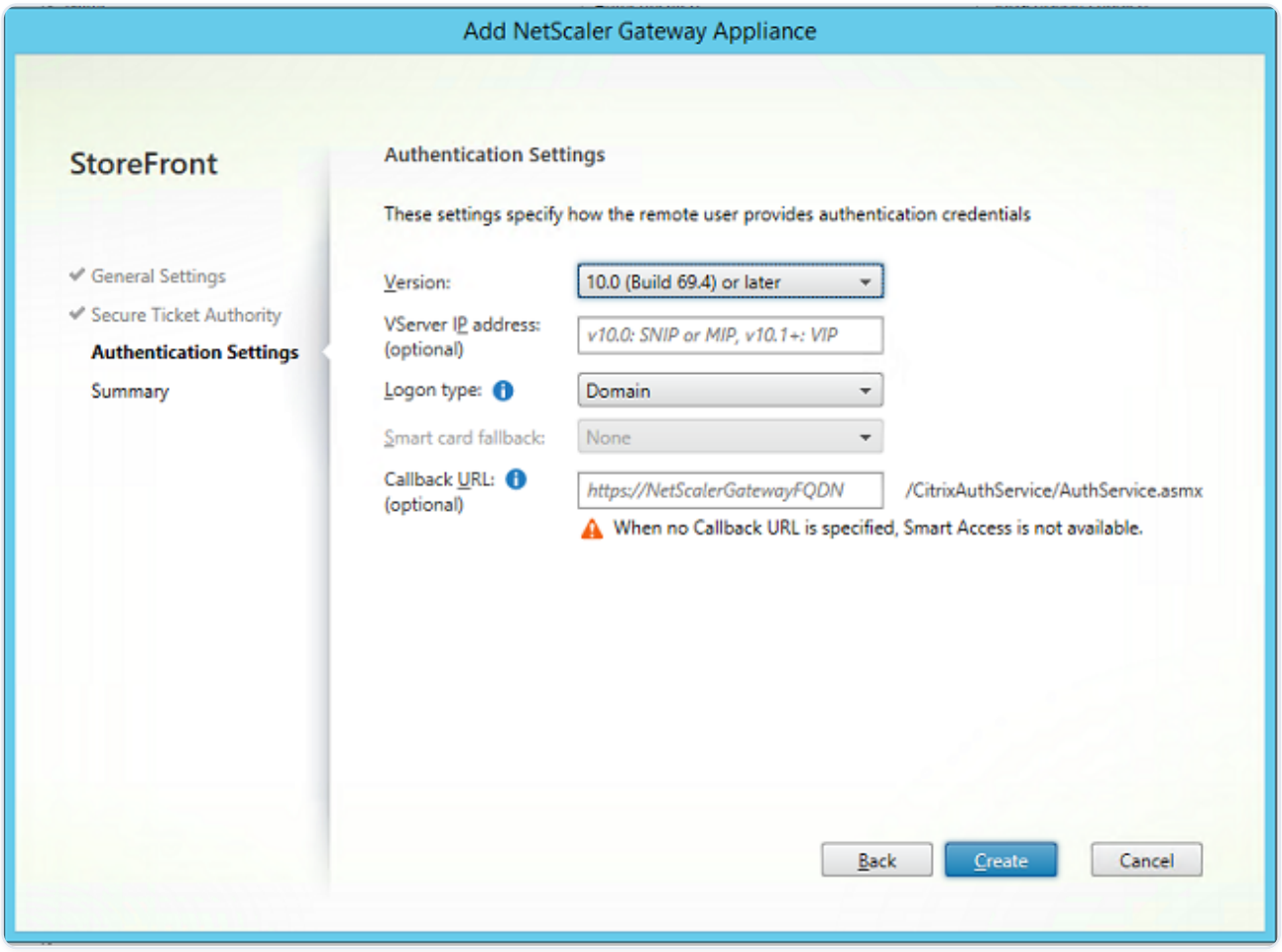


© 1997–2026 Citrix Systems, Inc. All rights reserved.

L'environnement Citrix Virtual Apps ou Citrix Virtual Desktops doit être configuré de la même manière que l'ouverture de session par carte à puce, ce qui est documenté dans CTX206156.

Dans un déploiement existant, cela implique généralement de s'assurer uniquement qu'une autorité de certification Microsoft jointe au domaine est disponible et que des certificats de contrôleur de domaine ont été attribués aux contrôleurs de domaine. (Consultez la section « Émission de certificats de contrôleur de domaine » dans CTX206156).

Lors de la configuration de Citrix Gateway en tant que système d'authentification principal, assurez-vous que toutes les connexions entre Citrix Gateway et StoreFront sont sécurisées avec TLS. En particulier, assurez-vous que l'URL de rappel (Callback Url) est correctement configurée pour pointer vers le serveur Citrix Gateway, car cela peut être utilisé pour authentifier le serveur Citrix Gateway dans ce déploiement.



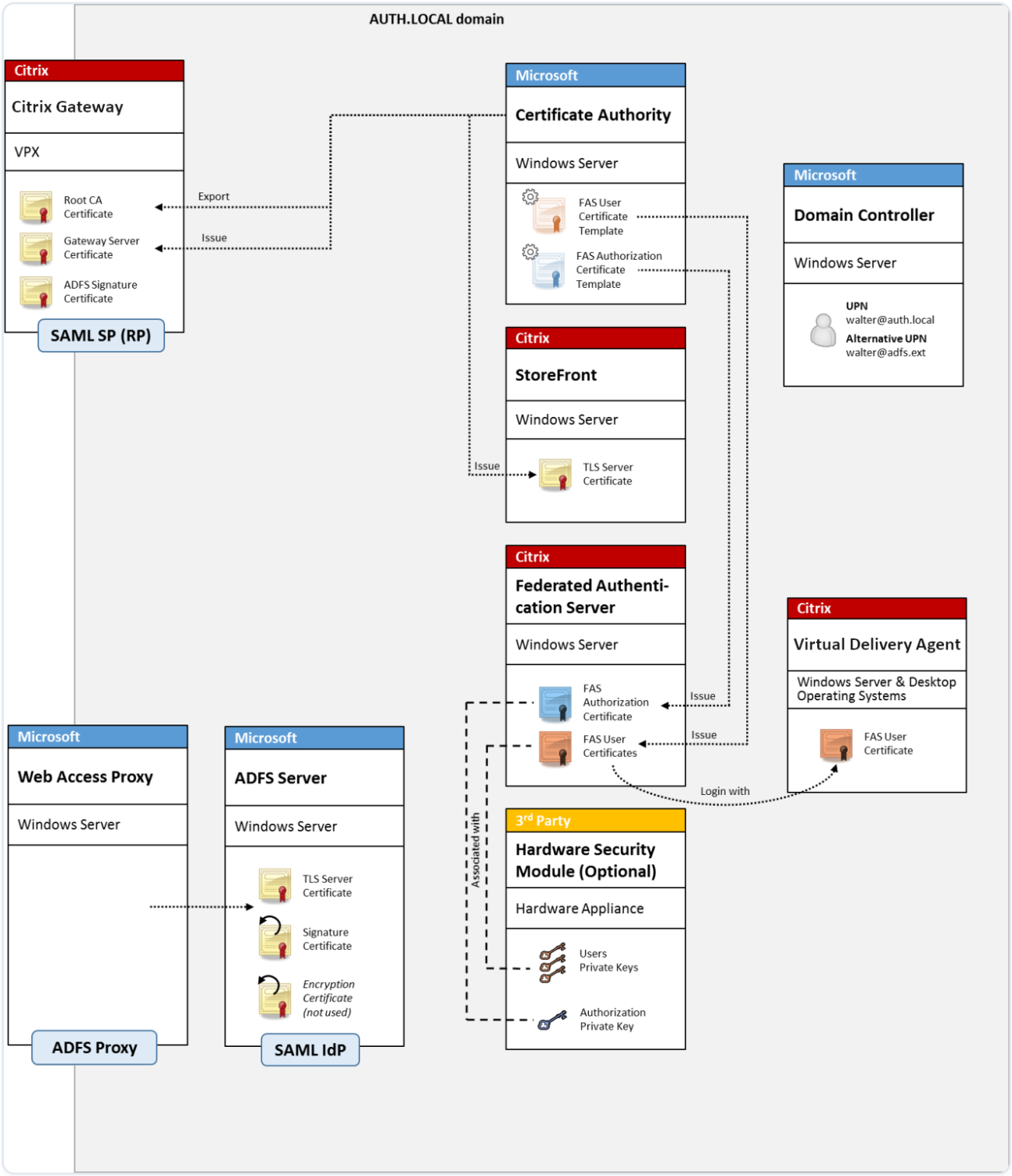
Informations connexes :

- Pour configurer Citrix Gateway, consultez « How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and Citrix Virtual Desktops 7.6. »
- Install and configure décrit comment installer et configurer FAS.

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

Déploiement ADFS SAML

Une technologie d'authentification clé de Citrix Gateway permet l'intégration avec Microsoft ADFS, qui peut agir en tant que fournisseur d'identité SAML (IdP). Une assertion SAML est un bloc XML signé cryptographiquement émis par un IdP de confiance qui autorise un utilisateur à se connecter à un système informatique. Cela signifie que le serveur FAS permet de déléguer l'authentification d'un utilisateur au serveur Microsoft ADFS (ou à un autre IdP compatible SAML).



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

ADFS est couramment utilisé pour authentifier de manière sécurisée les utilisateurs aux ressources d'entreprise à distance via Internet ; par exemple, il est souvent utilisé pour l'intégration d'Office 365.

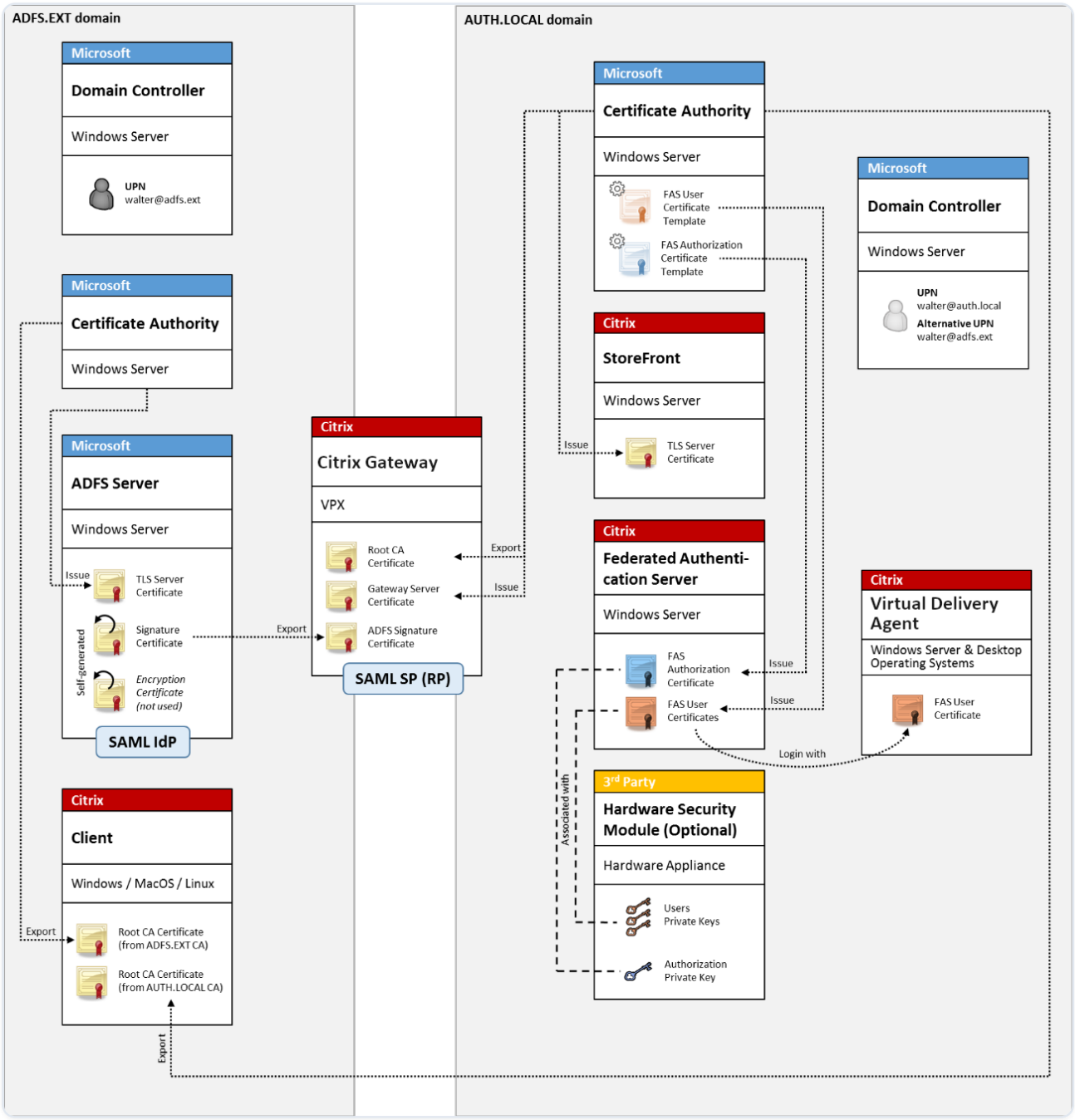
Informations connexes :

- L'article ADFS deployment contient des détails.
- L'article Install and configure décrit comment installer et configurer FAS.
- La section (/fr-fr/federated-authentication-service/2206/deployment-architectures.html#citrix-gateway-deployment) de cet article contient des considérations de configuration.

Mappage de comptes B2B

Si deux entreprises souhaitent utiliser les systèmes informatiques l'une de l'autre, une option courante consiste à configurer un serveur Active Directory Federation Service (ADFS) avec une relation de confiance. Cela permet aux utilisateurs d'une entreprise de s'authentifier de manière transparente dans l'environnement Active Directory (AD) d'une autre entreprise. Lors de la connexion, chaque utilisateur utilise ses propres informations d'identification de connexion d'entreprise ; ADFS mappe automatiquement cela à un « compte fantôme » dans l'environnement AD de l'entreprise partenaire.

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



Informations associées :

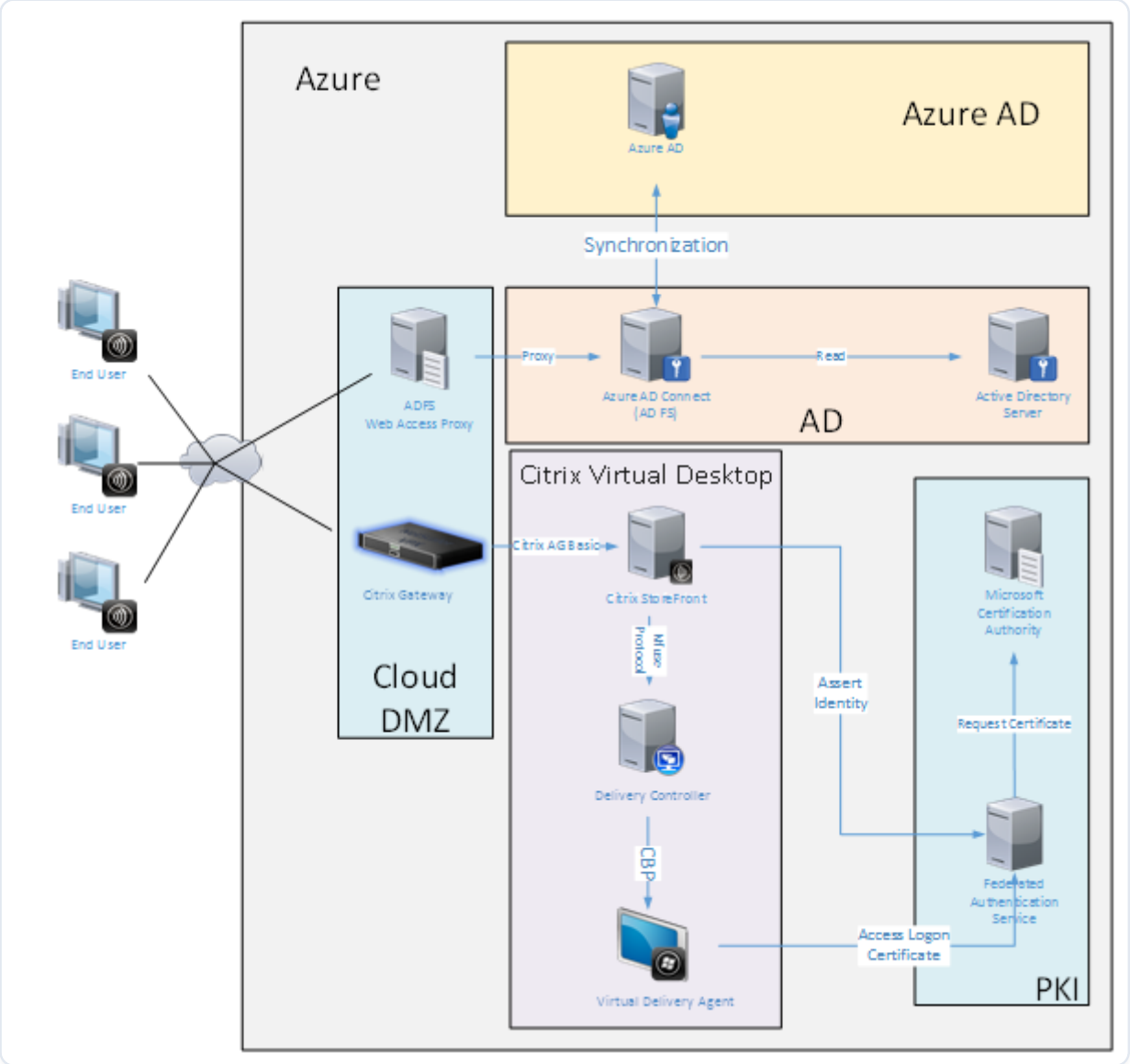
- L'article (/fr-fr/federated-authentication-service/2206/install-configure.html) décrit comment installer et configurer FAS.

Windows 10 Azure AD Join

Windows 10 a introduit le concept de « Azure AD Join », qui est conceptuellement similaire à la jonction de domaine Windows traditionnelle mais ciblé sur les scénarios « via Internet ». Cela fonctionne bien avec les ordinateurs portables et les tablettes. Comme pour la jonction de domaine Windows traditionnelle, Azure AD dispose de fonctionnalités permettant des modèles d'authentification unique pour les sites web et les ressources d'entreprise. Ceux-ci sont tous «

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

compatibles Internet », ils fonctionneront donc depuis n'importe quel emplacement connecté à Internet, et pas seulement le réseau local du bureau.



Ce déploiement est un exemple où il n'y a effectivement aucun concept d'« utilisateurs finaux au bureau ». Les ordinateurs portables sont inscrits et s'authentifient entièrement via Internet à l'aide des fonctionnalités modernes d'Azure AD.

Notez que l'infrastructure de ce déploiement peut s'exécuter partout où une adresse IP est disponible : sur site, chez un fournisseur hébergé, dans Azure ou chez un autre fournisseur de cloud. Le synchroniseur Azure AD Connect se connectera automatiquement à Azure AD. Le graphique d'exemple utilise des machines virtuelles Azure pour des raisons de simplicité.

Informations associées :

- L'article (/fr-fr/federated-authentication-service/2206/install-configure.html) décrit comment installer et configurer FAS.

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

- L'article (/fr-fr/federated-authentication-service/2206/deployment-architectures/azure-ad.html) contient des détails.

Déploiement ADFS

Introduction

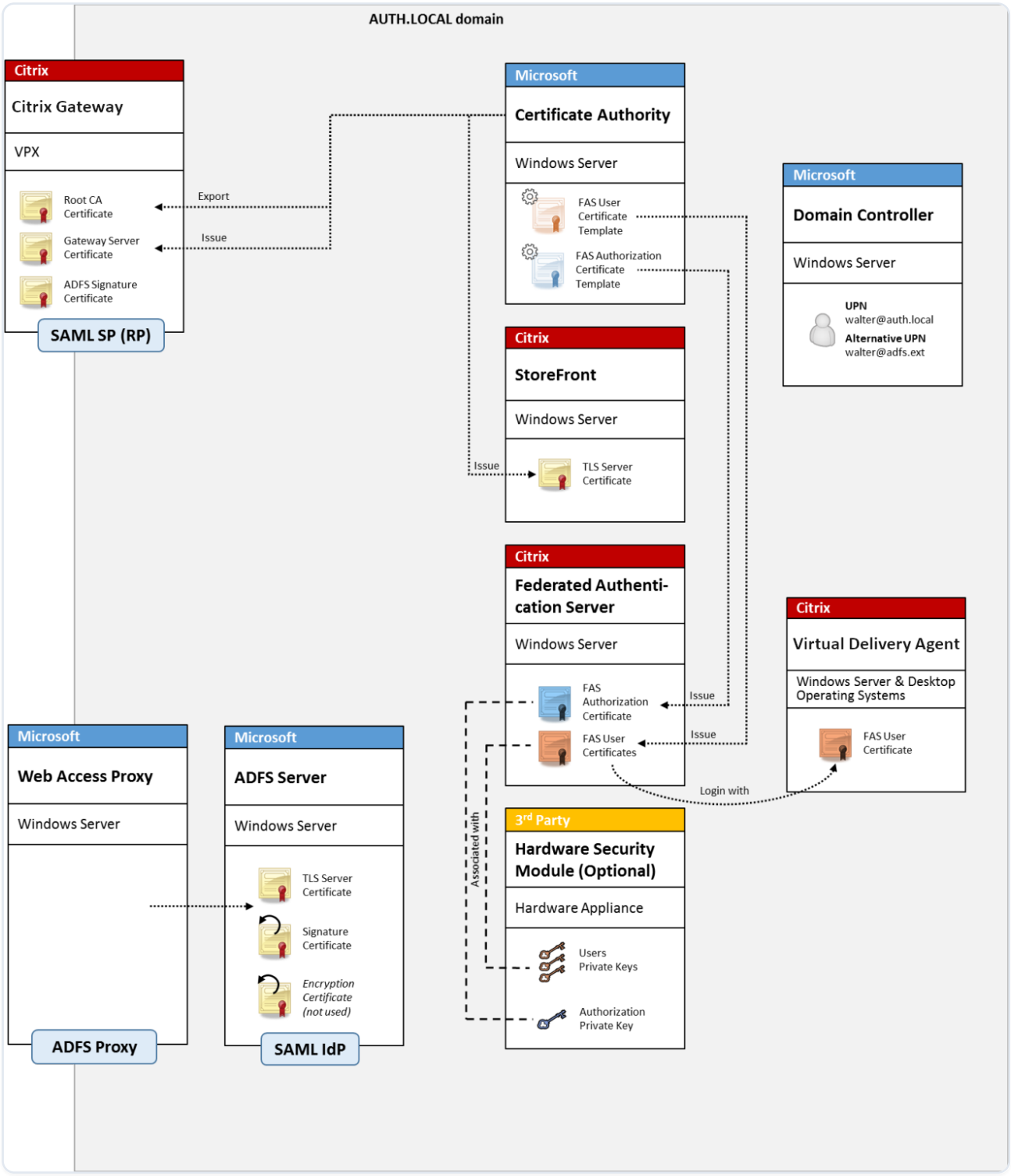
Ce document décrit comment intégrer un environnement Citrix avec Microsoft ADFS.

De nombreuses organisations utilisent ADFS pour gérer l'accès sécurisé des utilisateurs aux sites web qui nécessitent un point d'authentification unique. Par exemple, une entreprise peut avoir du contenu et des téléchargements supplémentaires disponibles pour les employés ; ces emplacements doivent être protégés par des informations d'identification de connexion Windows standard.

Le service d'authentification fédérée (FAS) permet également d'intégrer Citrix Gateway et Citrix StoreFront™ au système de connexion ADFS, réduisant ainsi la confusion potentielle pour le personnel de l'entreprise.

Ce déploiement intègre Citrix Gateway en tant que partie de confiance à Microsoft ADFS.

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



REMARQUE :

Il n'y a pas de différences si la ressource back-end est un VDA Windows ou un VDA Linux.

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

Présentation de SAML

Security Assertion Markup Language (SAML) est un système de connexion par navigateur web simple de type « redirection vers une page de connexion ». La configuration comprend les éléments suivants :

URL de redirection

Lorsque Citrix Gateway découvre qu'un utilisateur doit être authentifié, il demande au navigateur web de l'utilisateur d'effectuer une requête HTTP POST vers une page web de connexion SAML sur le serveur ADFS. Il s'agit généralement d'une adresse `https://` de la forme : `https://adfs.mycompany.com/adfs/ls`.

Cette requête POST de page web inclut d'autres informations, y compris l'« adresse de retour » où ADFS renverra l'utilisateur une fois la connexion terminée.

Identifiant

L'EntityId est un identifiant unique que Citrix Gateway inclut dans ses données POST vers ADFS. Cela informe ADFS du service auquel l'utilisateur tente de se connecter et permet d'appliquer différentes politiques d'authentification, le cas échéant. Si émis, le XML d'authentification SAML ne sera approprié que pour la connexion au service identifié par l'EntityId.

Habituellement, l'EntityID est l'URL de la page de connexion du serveur Citrix Gateway, mais il peut généralement être n'importe quoi, tant que Citrix Gateway et ADFS sont d'accord sur ce point : `https://ns.mycompany.com/application/logonpage`.

Adresse de retour

Si l'authentification est réussie, ADFS demande au navigateur web de l'utilisateur d'envoyer un XML d'authentification SAML à l'une des URL de réponse configurées pour l'EntityId. Il s'agit généralement d'une adresse `https://` sur le serveur Citrix Gateway d'origine, sous la forme : `https://ns.mycompany.com/cgi/samlauth`.

S'il y a plus d'une adresse URL de réponse configurée, Citrix Gateway peut en choisir une dans son POST initial vers ADFS.

Certificat de signature

ADFS signe cryptographiquement les objets XML d'authentification SAML à l'aide de sa clé privée. Pour valider cette signature, Citrix Gateway doit être configuré pour vérifier ces signatures à l'aide de la clé publique incluse dans un fichier de certificat. Le fichier de certificat sera généralement un fichier texte obtenu du serveur ADFS.

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

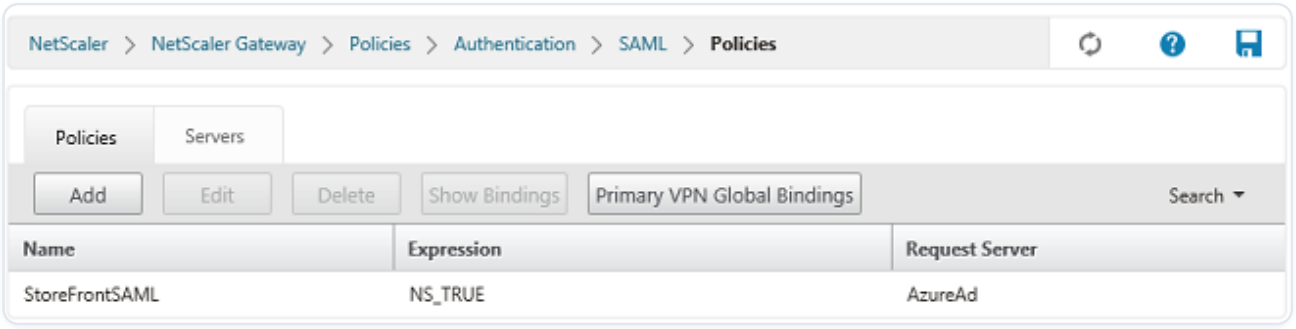
URL de déconnexion unique

ADFS et Citrix Gateway prennent en charge un système de « déconnexion centralisée ». Il s'agit d'une URL que Citrix Gateway interroge occasionnellement pour vérifier que l'objet XML d'authentification SAML représente toujours une session actuellement connectée.

Il s'agit d'une fonctionnalité facultative qui n'a pas besoin d'être configurée. Il s'agit généralement d'une adresse `https://` sous la forme `https://adfs.mycompany.com/adfs/logout`. (Notez qu'elle peut être la même que l'URL de connexion unique.)

Configuration

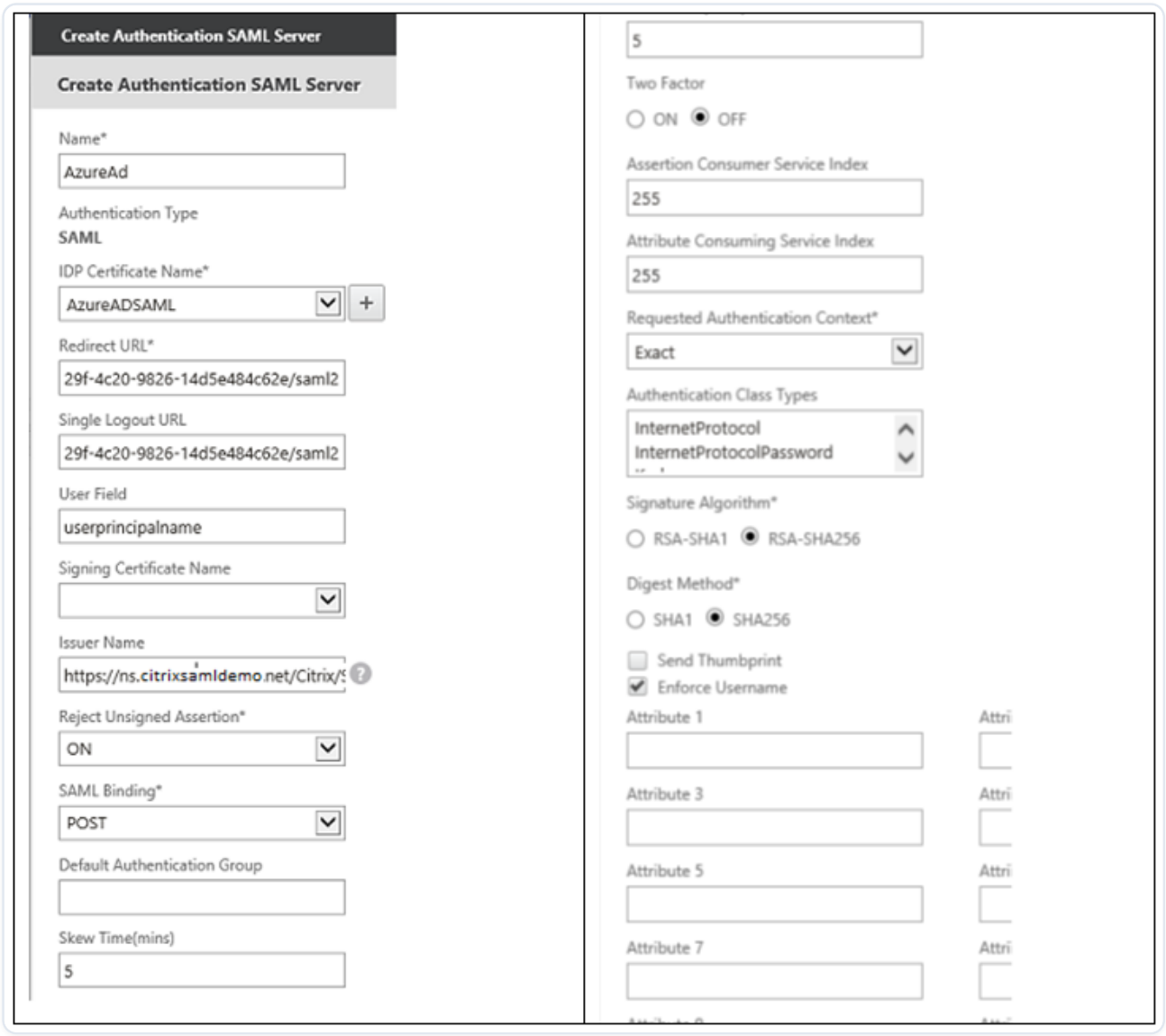
La section Déploiement de Citrix Gateway décrit comment configurer Citrix Gateway pour gérer les options d'authentification LDAP standard. Une fois cette étape terminée avec succès, vous pouvez créer une nouvelle politique d'authentification sur Citrix Gateway qui autorise l'authentification SAML. Celle-ci peut alors remplacer la politique LDAP par défaut utilisée par l'assistant Citrix Gateway.



Remplir la politique SAML

Configurez le nouveau serveur IdP SAML en utilisant les informations obtenues précédemment depuis la console de gestion ADFS. Lorsque cette politique est appliquée, Citrix Gateway redirige l'utilisateur vers ADFS pour la connexion et accepte en retour un jeton d'authentification SAML signé par ADFS.

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



Informations connexes

- Installer et configurer est la référence principale pour l'installation et la configuration de FAS.
- Les déploiements FAS courants sont résumés dans l'article Architectures de déploiement.
- Les articles de procédure sont présentés dans l'article Configuration avancée.

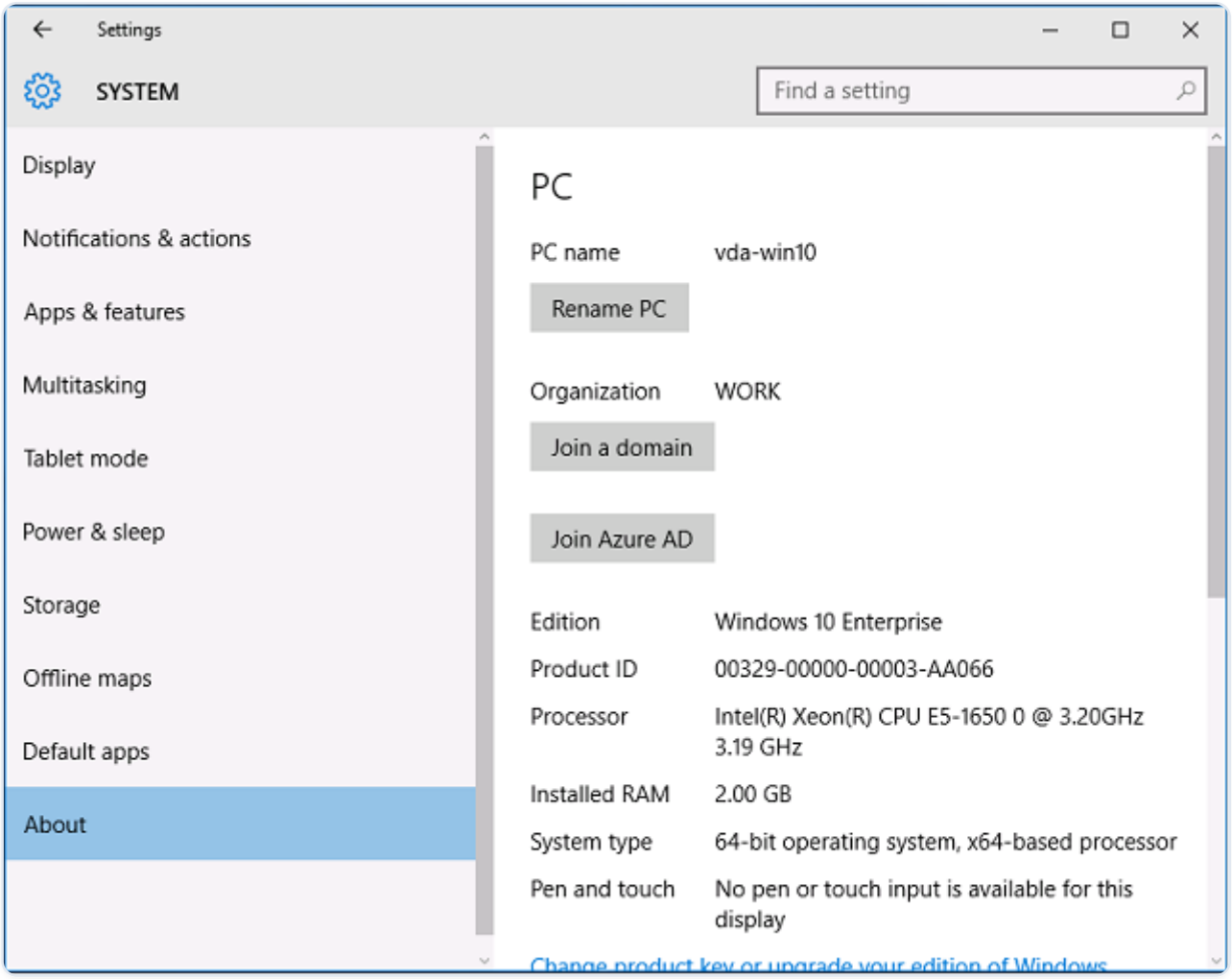
Intégration d'Azure AD

Introduction

Ce document décrit comment intégrer un environnement Citrix à la fonctionnalité Azure AD de Windows 10. Windows 10 a introduit Azure AD, qui est un nouveau modèle de jonction de domaine où les ordinateurs portables itinérants peuvent être joints à un domaine d'entreprise via Internet à des fins de gestion et d'authentification unique.

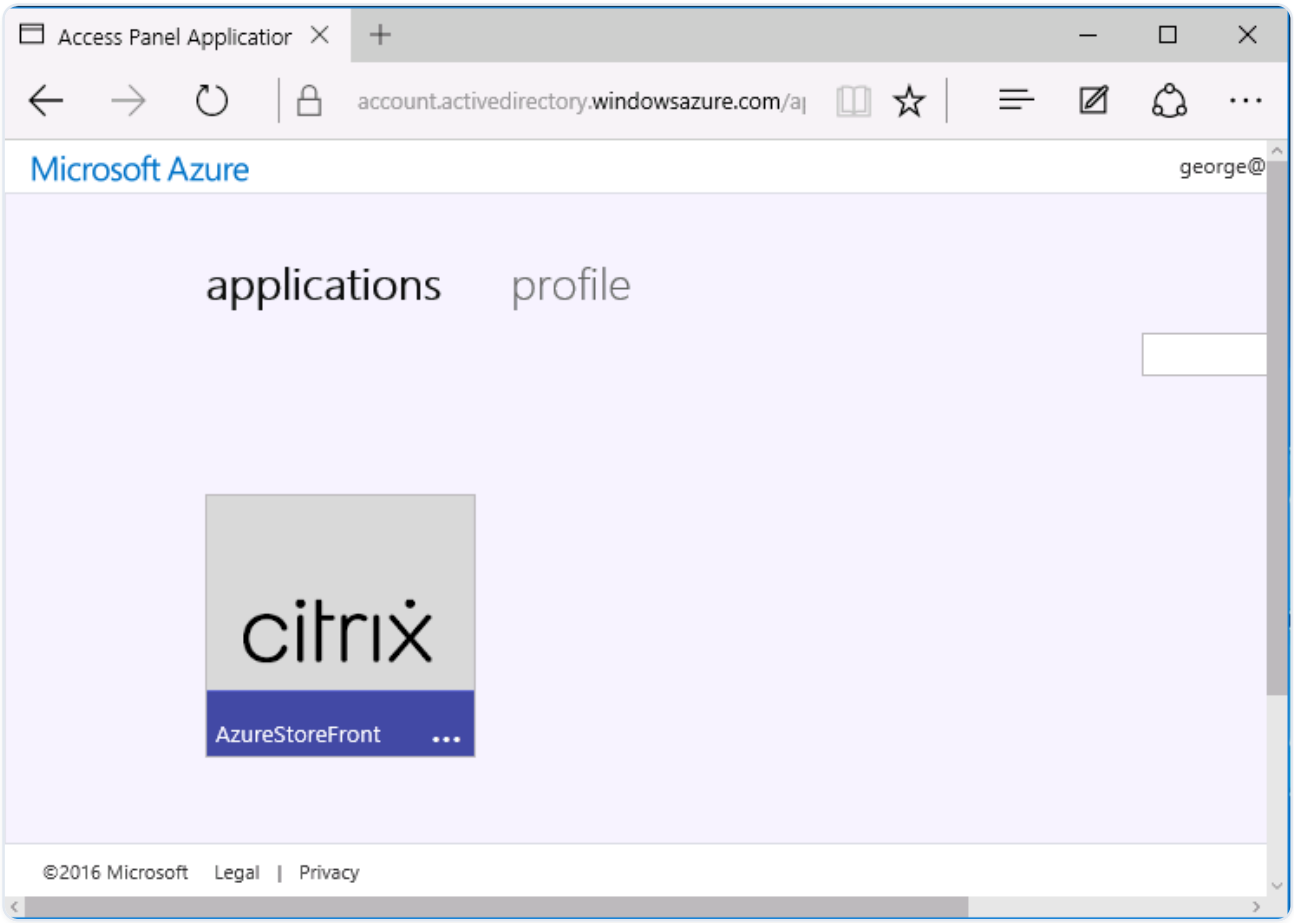
© 1997–2026 Citrix Systems, Inc. All rights reserved.

L'exemple de déploiement dans ce document décrit un système où le service informatique fournit aux nouveaux utilisateurs une adresse e-mail d'entreprise et un code d'inscription pour leurs ordinateurs portables Windows 10 personnels. Les utilisateurs accèdent à ce code via l'option **Système > À propos > Rejoindre Azure AD** dans le panneau **Paramètres**.



Une fois l'ordinateur portable inscrit, le navigateur web Microsoft Edge se connecte automatiquement aux sites web de l'entreprise et aux applications publiées Citrix via la page web des applications SaaS Azure, avec d'autres applications Azure telles qu'Office 365.

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

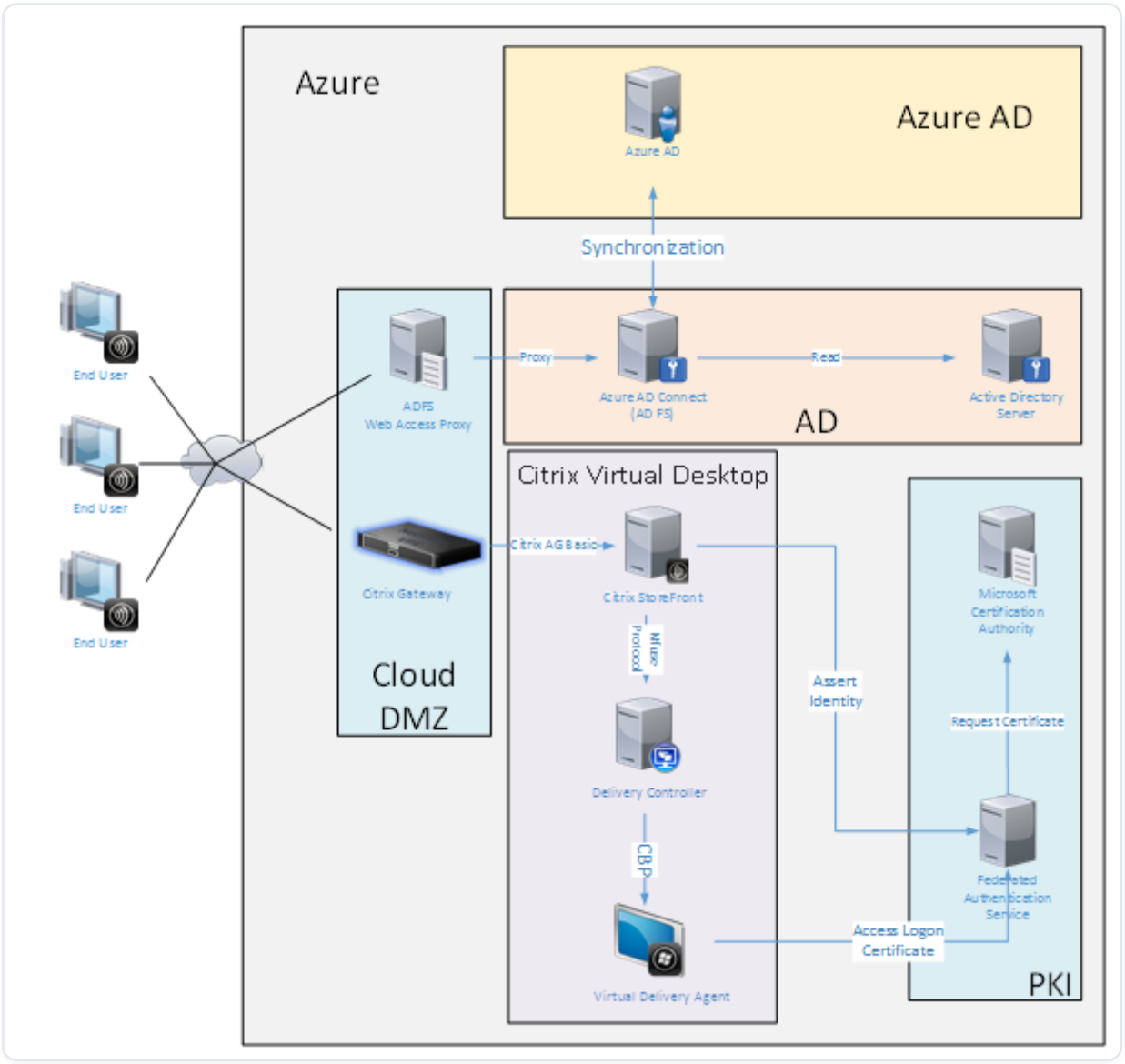


Architecture

Cette architecture réplique un réseau d'entreprise traditionnel entièrement au sein d'Azure, en s'intégrant aux technologies cloud modernes telles qu'Azure AD et Office 365. Tous les utilisateurs finaux sont considérés comme des travailleurs à distance, sans notion d'être sur un intranet de bureau.

Le modèle peut être appliqué aux entreprises disposant de systèmes sur site existants, car la synchronisation Azure AD Connect peut établir un pont vers Azure via Internet.

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



Les connexions sécurisées et l'authentification unique, qui auraient traditionnellement été une authentification LAN pare-feu et Kerberos/NTLM, sont remplacées dans cette architecture par des connexions TLS à Azure et SAML. Les nouveaux services sont construits comme des applications Azure jointes à Azure AD. Les applications existantes qui nécessitent Active Directory (telles qu'une base de données SQL Server) peuvent être exécutées à l'aide d'une VM de serveur Active Directory standard dans la partie IAAS du service cloud Azure.

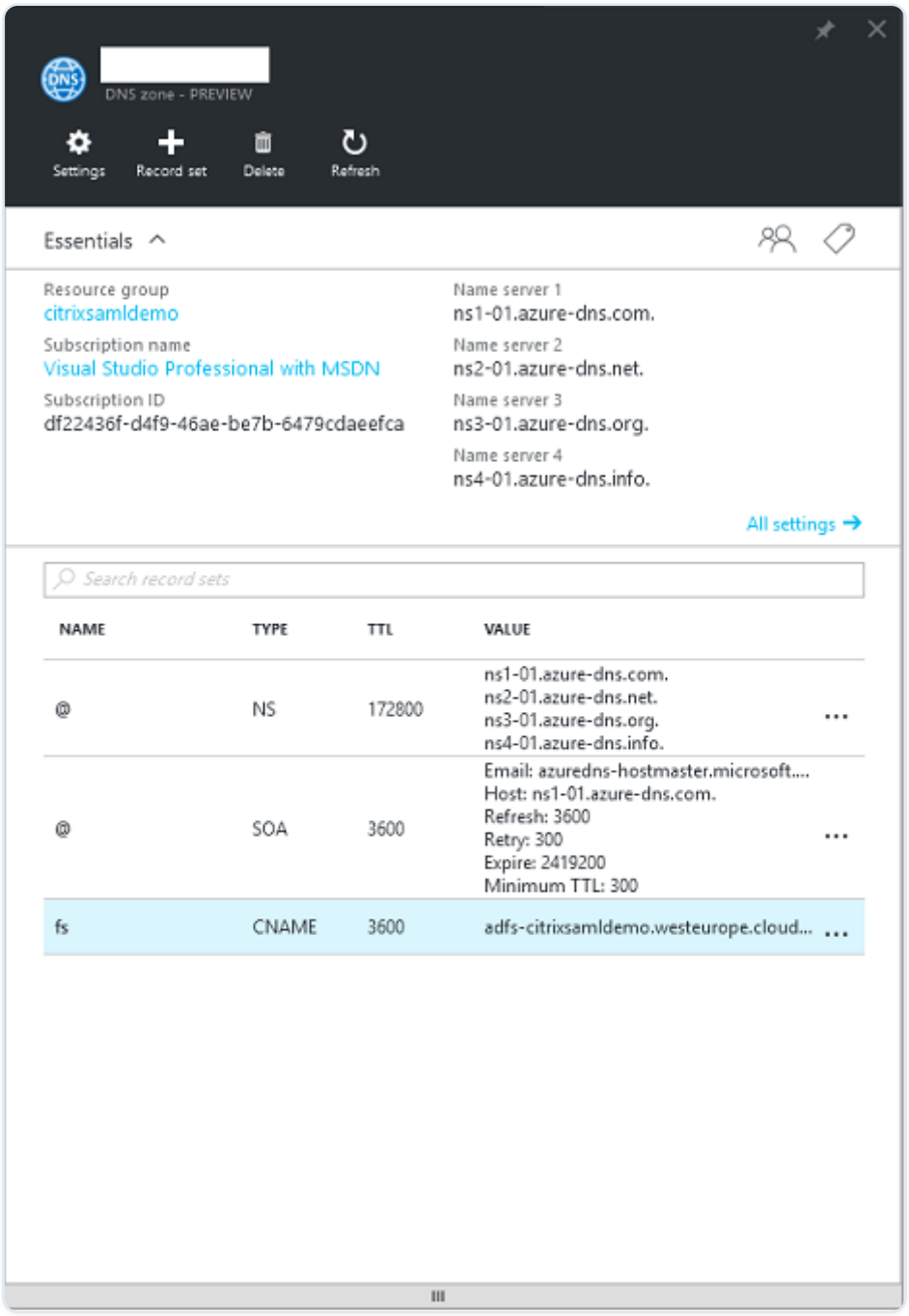
Lorsqu'un utilisateur lance une application traditionnelle, celle-ci est accessible à l'aide des applications publiées Citrix Virtual Apps and Desktops™. Les différents types d'applications sont regroupés via la page **Applications Azure** de l'utilisateur, en utilisant les fonctionnalités d'authentification unique de Microsoft Edge. Microsoft fournit également des applications Android et iOS qui peuvent énumérer et lancer des applications Azure.

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

Créer une zone DNS

Azure AD exige que l'administrateur ait enregistré une adresse DNS publique et contrôle la zone de délégation pour le suffixe du nom de domaine. Pour ce faire, l'administrateur peut utiliser la fonctionnalité de zone DNS Azure.

Cet exemple utilise le nom de zone DNS *citrixsamldemo.net*.



La console affiche les noms des serveurs de noms DNS Azure. Ceux-ci doivent être référencés dans les entrées NS du bureau d'enregistrement DNS pour la zone (par exemple, `citrixsamldemo.net. NS n1-01.azure-dns.com`)

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

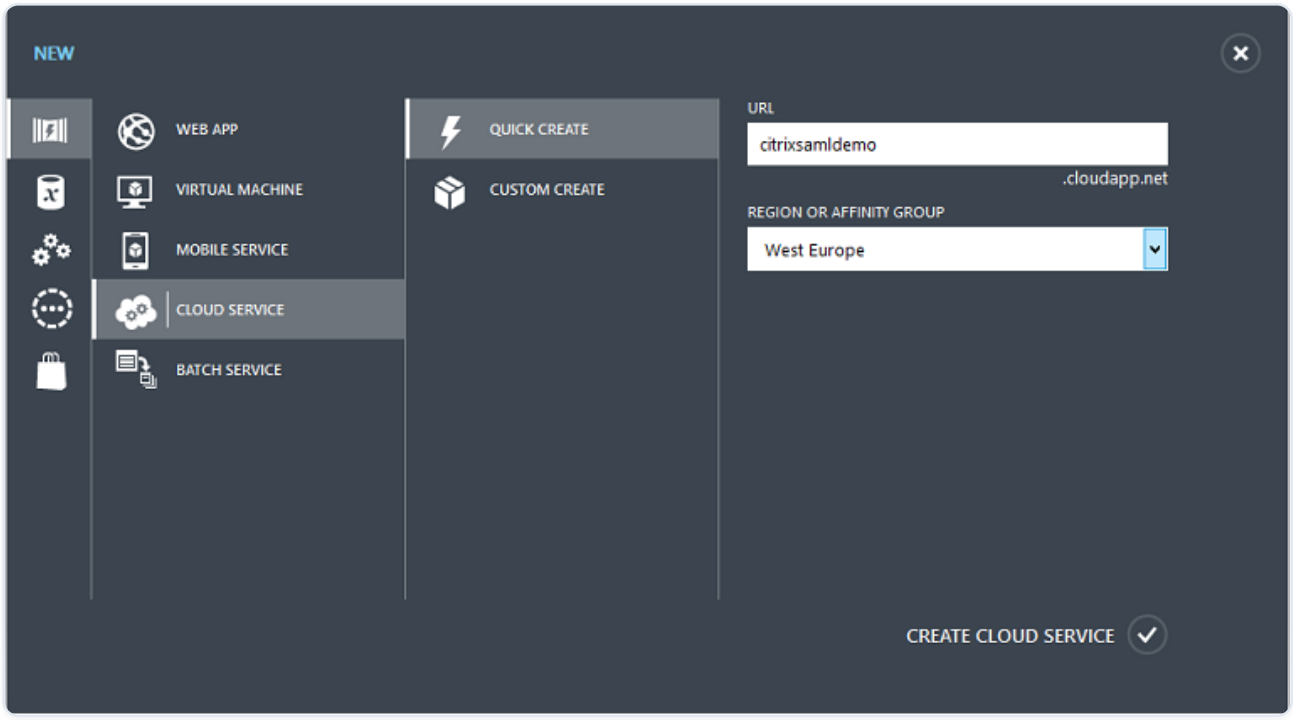
Lors de l'ajout de références à des machines virtuelles exécutées dans Azure, il est plus facile d'utiliser un pointeur CNAME vers l'enregistrement DNS géré par Azure pour la machine virtuelle. Si l'adresse IP de la machine virtuelle change, vous n'aurez pas besoin de mettre à jour manuellement le fichier de zone DNS.

Les suffixes d'adresse DNS internes et externes correspondront pour ce déploiement. Le domaine est citrixsamldemo.net et utilise un DNS fractionné (10.0.0.* en interne).

Ajoutez une entrée « fs.citrixsamldemo.net » qui référence le serveur proxy d'application Web. Il s'agit du service de fédération pour cette zone.

Créer un service cloud

Cet exemple configure un environnement Citrix, y compris un environnement AD avec un serveur ADFS exécuté dans Azure. Un service cloud est créé, nommé « citrixsamldemo ».

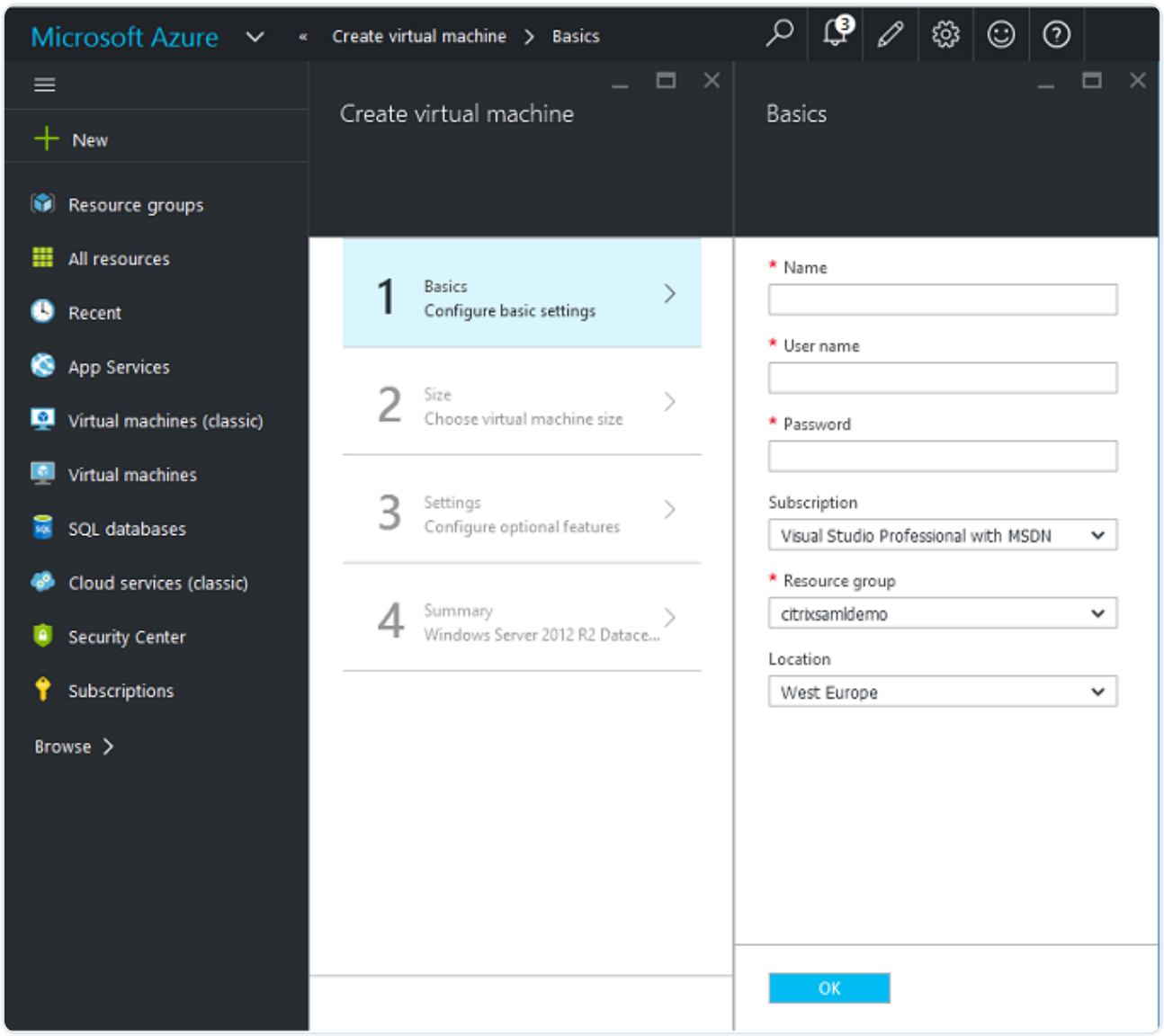


Créer des machines virtuelles Windows

Créez cinq machines virtuelles Windows exécutées dans le service cloud :

- Contrôleur de domaine (domaincontrol)
- Serveur ADFS Azure Connect (adfs)
- Proxy d'accès Web ADFS (proxy d'application Web, non joint au domaine)
- Contrôleur de livraison Citrix Virtual Apps and Desktops
- Citrix Virtual Apps and Desktops Agent de livraison virtuel (VDA)

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



Contrôleur de domaine

- Ajoutez les rôles **Serveur DNS** et **Services de domaine Active Directory** pour créer un déploiement Active Directory standard (dans cet exemple, citrixsamldemo.net). Une fois la promotion de domaine terminée, ajoutez le rôle **Services de certification Active Directory**.
- Créez un compte utilisateur normal pour les tests (par exemple, George@citrixsamldemo.net).
- Étant donné que ce serveur exécutera un DNS interne, tous les serveurs doivent se référer à ce serveur pour la résolution DNS. Cela peut être fait via la page **Paramètres DNS Azure**. (Pour plus d'informations, consultez l'Annexe de ce document.)

Contrôleur ADFS et serveur proxy d'application web

- Joignez le serveur ADFS au domaine citrixsamldemo. Le serveur proxy d'application web doit rester dans un groupe de travail isolé, donc enregistrez manuellement une adresse DNS auprès du DNS AD.

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

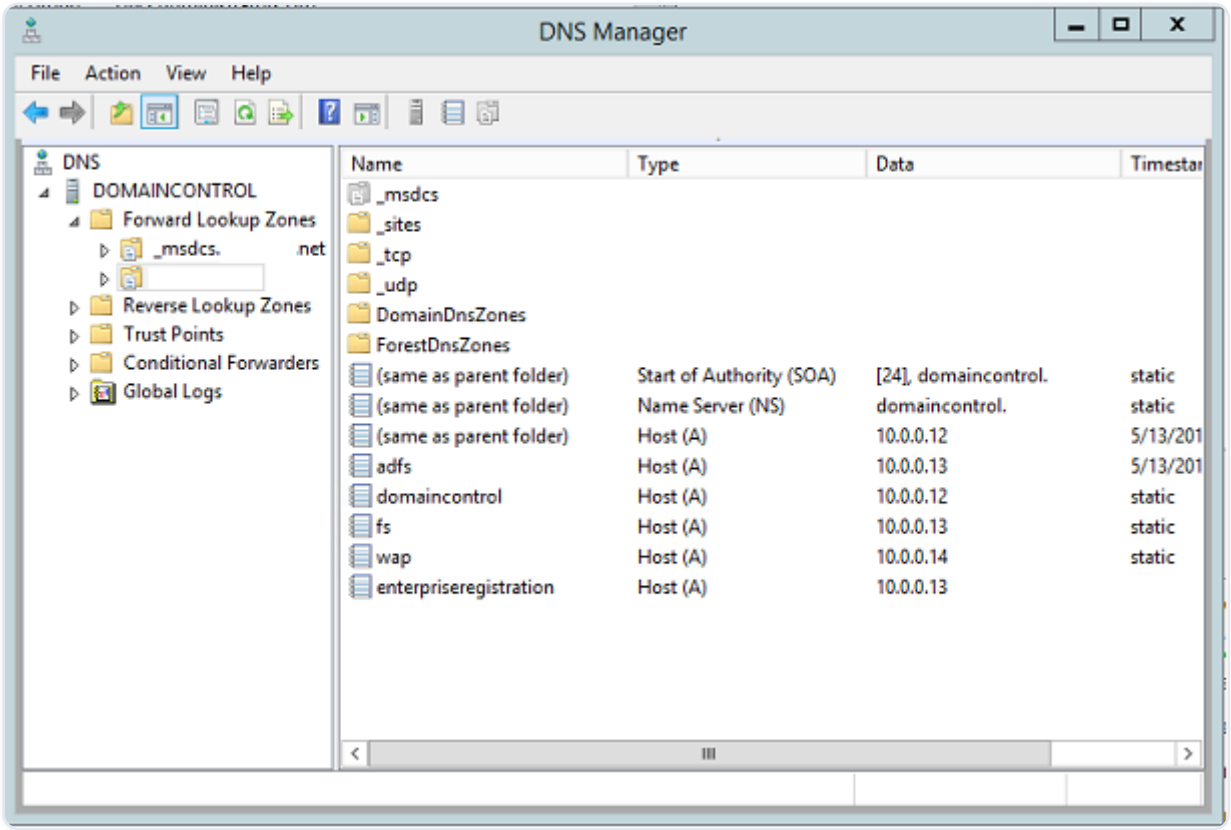
- Exécutez l'applet de commande **Enable-PSRemoting –Force** sur ces serveurs, pour autoriser la communication à distance PS via les pare-feu à partir de l'outil AzureAD Connect.

Citrix Virtual Desktops™ Delivery Controller et VDA

- Installez le Citrix Virtual Apps ou Citrix Virtual Desktops Delivery Controller™ et le VDA sur les deux serveurs Windows restants joints à citrixsamldemo.

Configurer un DNS interne

Une fois le contrôleur de domaine installé, configurez le serveur DNS pour gérer la vue interne de citrixsamldemo.net et agir comme un redirecteur vers un serveur DNS externe (par exemple : 8.8.8.8).

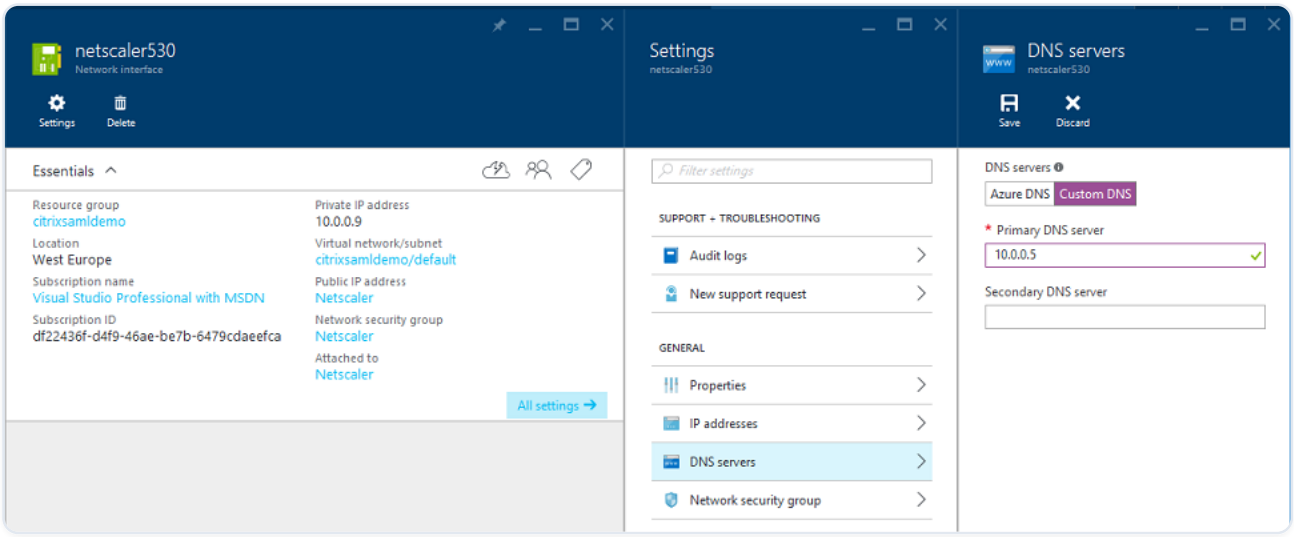


Ajoutez un enregistrement statique pour :

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

Toutes les machines virtuelles exécutées dans Azure doivent être configurées pour utiliser uniquement ce serveur DNS. Vous pouvez le faire via l'interface graphique de l'interface réseau.

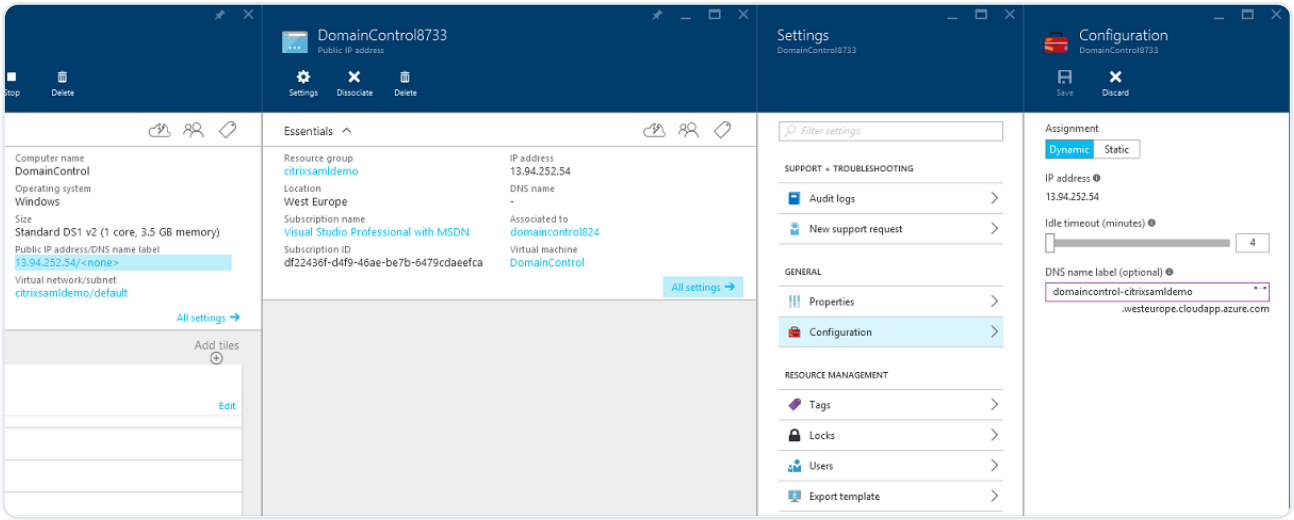
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Par défaut, l'adresse IP interne (10.0.0.9) est allouée dynamiquement. Vous pouvez utiliser le paramètre d'adresses IP pour attribuer l'adresse IP de manière permanente. Cela doit être fait pour le serveur proxy d'application Web et le contrôleur de domaine.

Configurer une adresse DNS externe

Lorsqu'une machine virtuelle est en cours d'exécution, Azure maintient son propre serveur de zone DNS qui pointe vers l'adresse IP publique actuelle attribuée à la machine virtuelle. Il s'agit d'une fonctionnalité utile à activer car Azure attribue des adresses IP au démarrage de chaque machine virtuelle, par défaut.



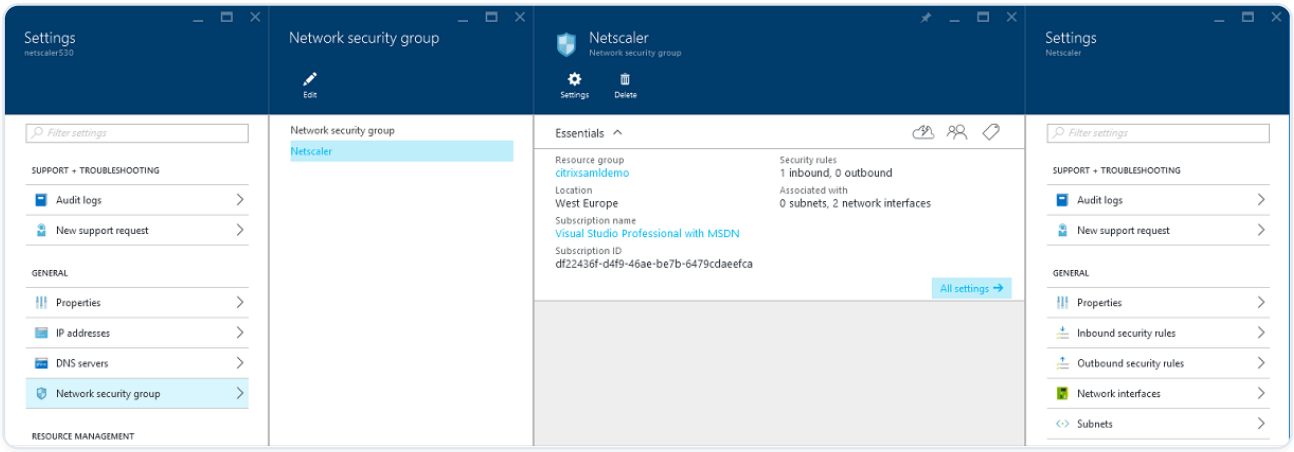
Cet exemple attribue une adresse DNS de domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com au contrôleur de domaine.

Notez que lorsque la configuration à distance est terminée, seules les machines virtuelles du proxy d'application Web et de Citrix Gateway doivent avoir des adresses IP publiques activées. (Pendant la configuration, l'adresse IP publique est utilisée pour l'accès RDP à l'environnement).

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

Configurer les groupes de sécurité

Le cloud Azure gère les règles de pare-feu pour l'accès TCP/UDP aux machines virtuelles depuis Internet à l'aide de groupes de sécurité. Par défaut, toutes les machines virtuelles autorisent l'accès RDP. Les serveurs Citrix Gateway et proxy d'application Web doivent également autoriser TLS sur le port 443.



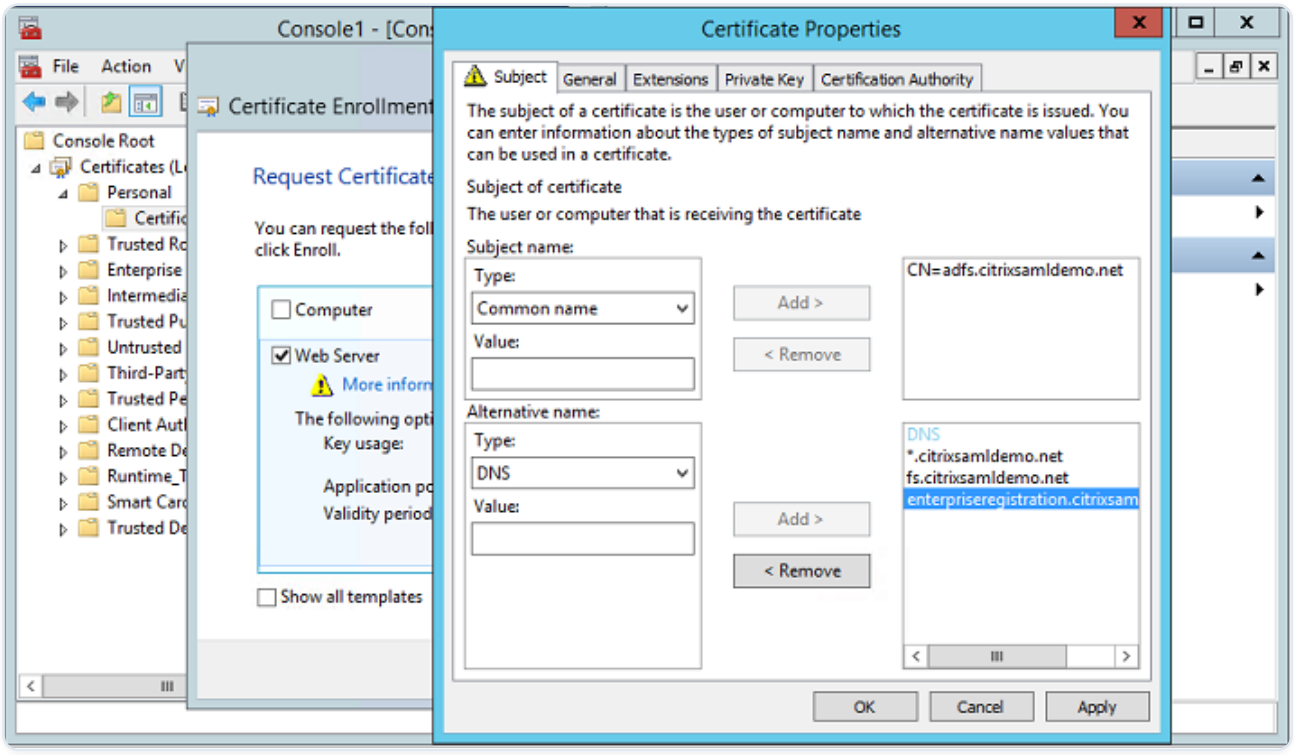
Créer un certificat ADFS

Activez le modèle de certificat **Serveur Web** sur l'autorité de certification Microsoft. Cela permet la création d'un certificat avec des adresses DNS personnalisées qui peut être exporté (y compris la clé privée) vers un fichier pfx. Vous devez installer ce certificat sur les serveurs ADFS et Web Application Proxy, le fichier PFX est donc l'option préférée.

Émettez un certificat de serveur Web avec les noms d'objet suivants :

- Nom commun :
  - adfs.citrixsamldemo.net
- Nom alternatif du sujet :
  - *.citrixsamldemo.net
  - fs.citrixsamldemo. réseau
  - enterpriseregistration.citrixsamldemo.net

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



Exportez le certificat vers un fichier pfx, y compris une clé privée protégée par mot de passe.

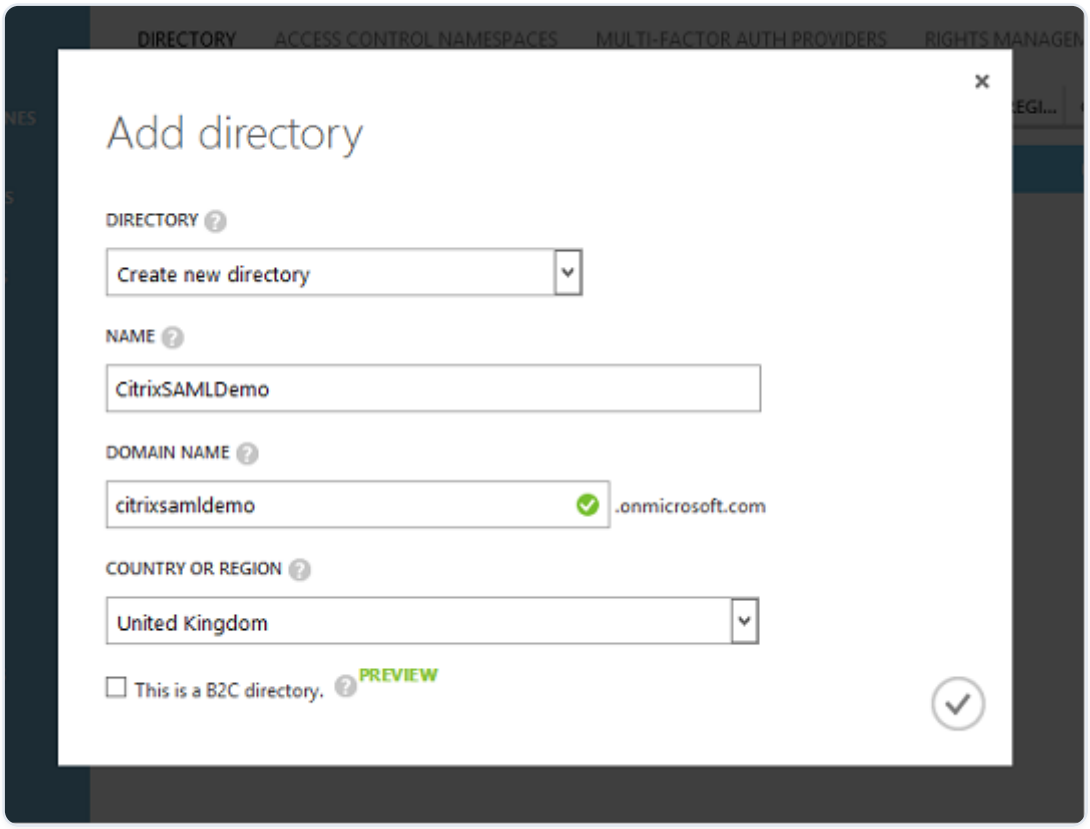
Configurer Azure AD

Cette section détaille le processus de configuration d'une nouvelle instance Azure AD et de création d'identités d'utilisateur pouvant être utilisées pour joindre Windows 10 à Azure AD.

Créer un nouveau répertoire

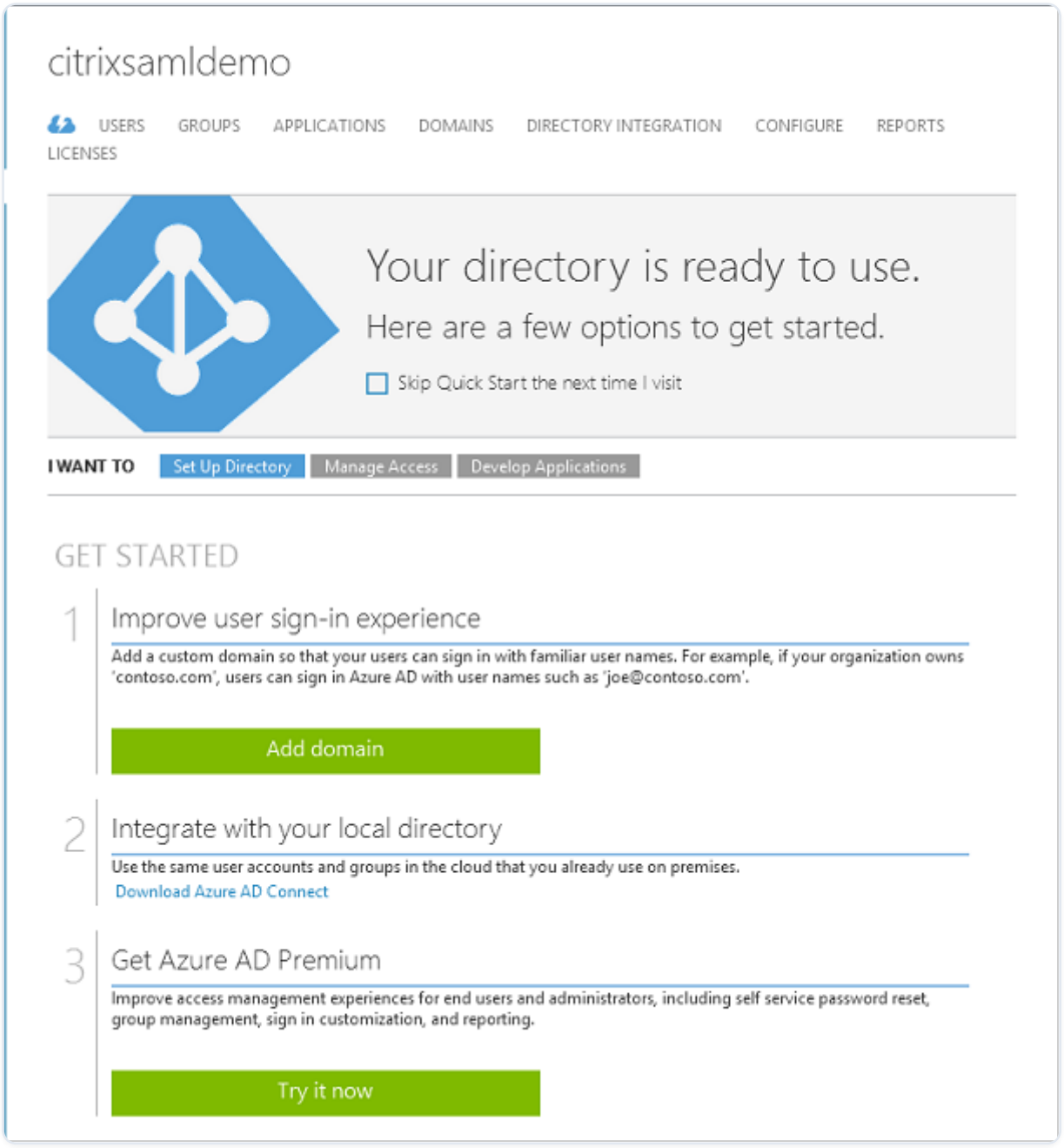
Connectez-vous au portail Azure classique et créez un nouveau répertoire.

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



Une fois terminé, une page de résumé apparaît.

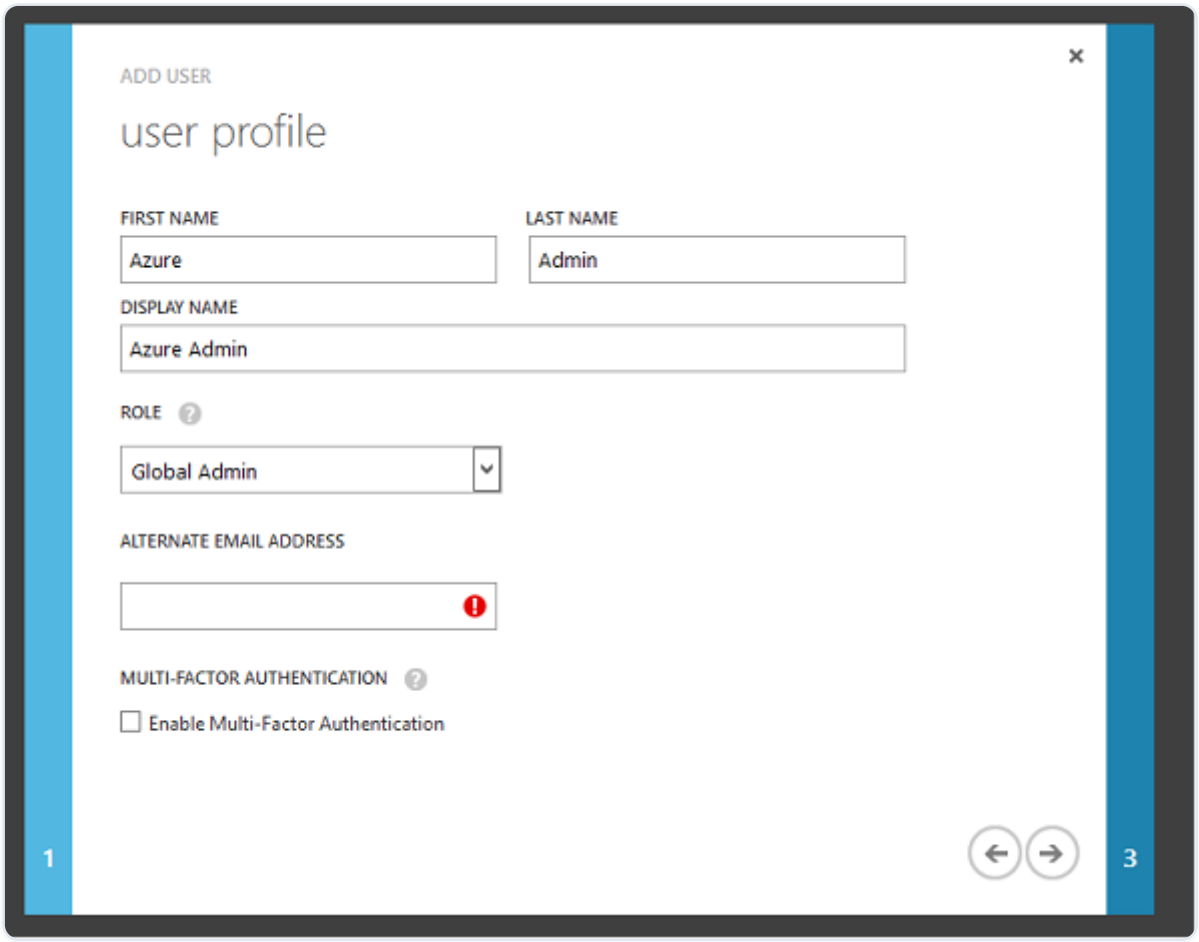
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Créer un utilisateur administrateur global (AzureAdmin)

Créez un administrateur global dans Azure (dans cet exemple, `AzureAdmin@citrixsamldemo.onmicrosoft.com`) et connectez-vous avec le nouveau compte pour définir un mot de passe.

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



Enregistrer votre domaine auprès d'Azure AD

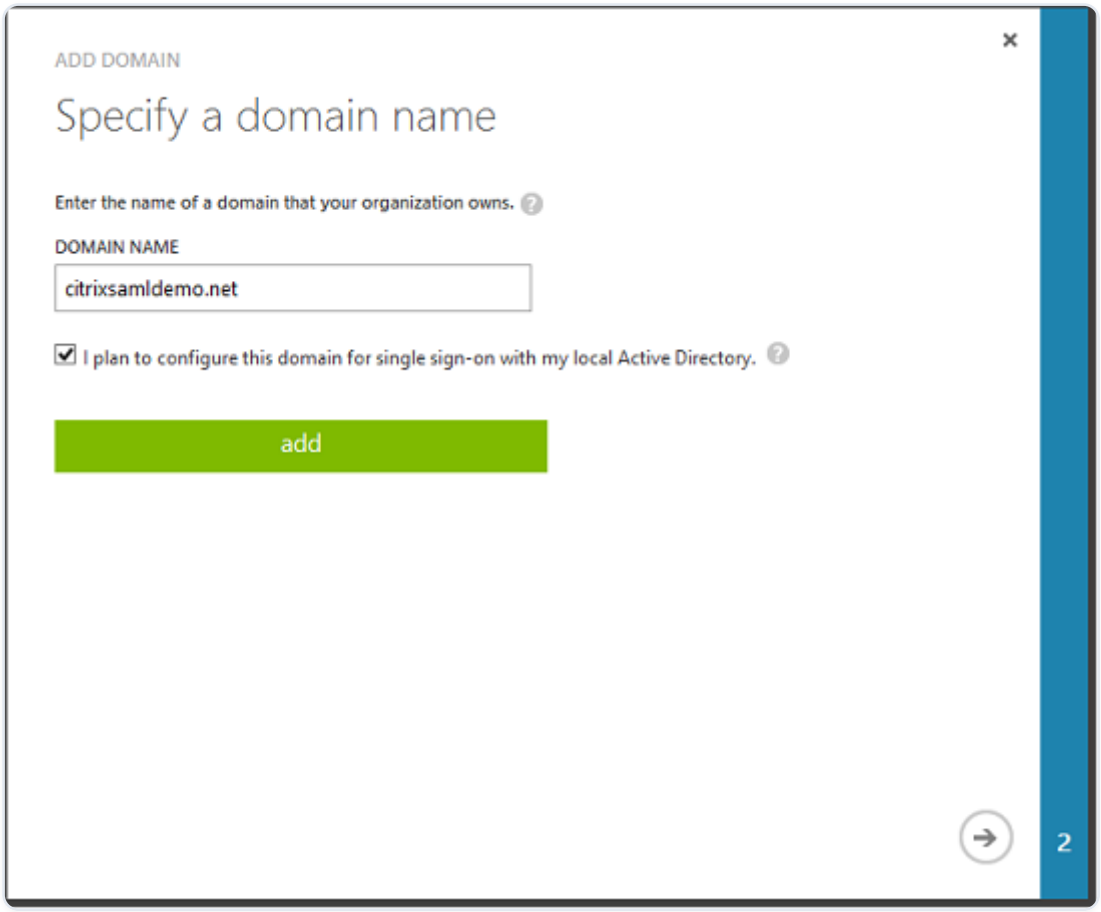
Par défaut, les utilisateurs sont identifiés par une adresse e-mail sous la forme : `<user.name>@<company>.onmicrosoft.com`.

Bien que cela fonctionne sans configuration supplémentaire, une adresse e-mail au format standard est préférable, idéalement une qui corresponde au compte de messagerie de l'utilisateur final : `<user.name>@<company>.com`.

L'action **Ajouter un domaine** configure une redirection depuis le domaine réel de votre entreprise. L'exemple utilise `citrixsamldemo.net`.

Si vous configurez ADFS pour l'authentification unique, cochez la case.

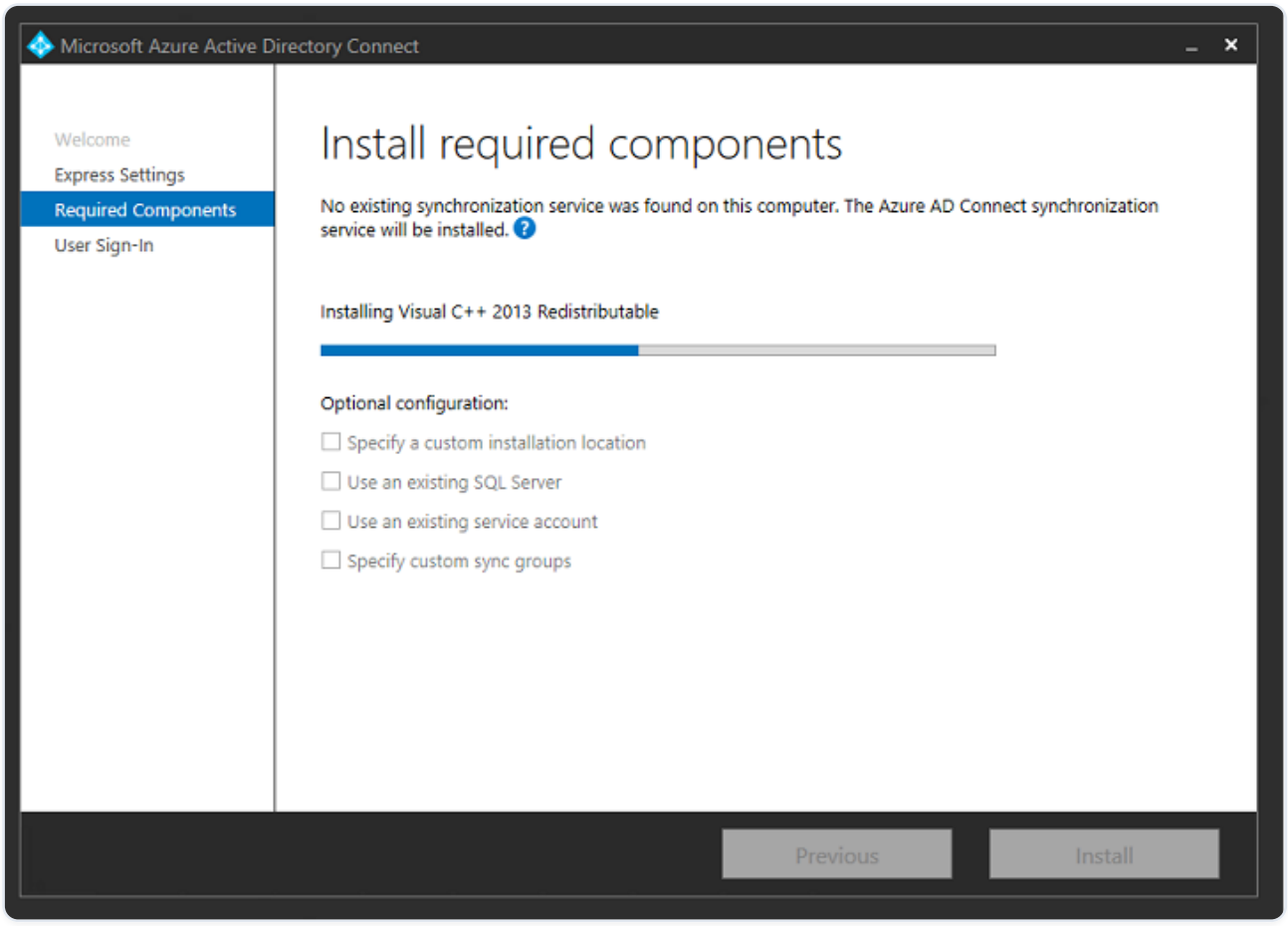
© 1997–2026 Citrix Systems, Inc. All rights reserved.



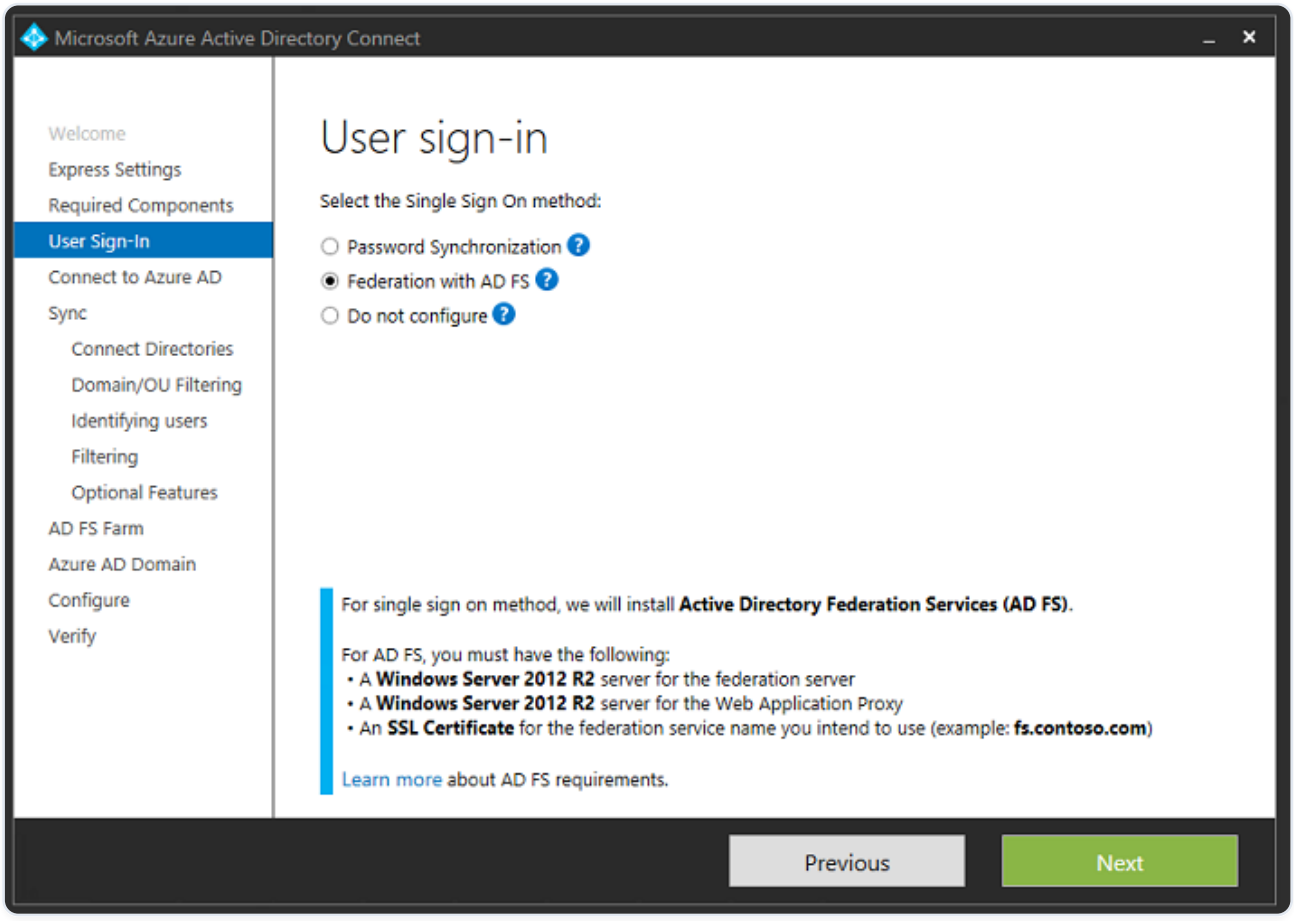
Installer Azure AD Connect

L'étape 2 de l'interface graphique de configuration d'Azure AD redirige vers la page de téléchargement Microsoft pour Azure AD Connect. Installez-le sur la VM ADFS. Utilisez **Installation personnalisée** plutôt que **Paramètres express**, afin que les options ADFS soient disponibles.

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

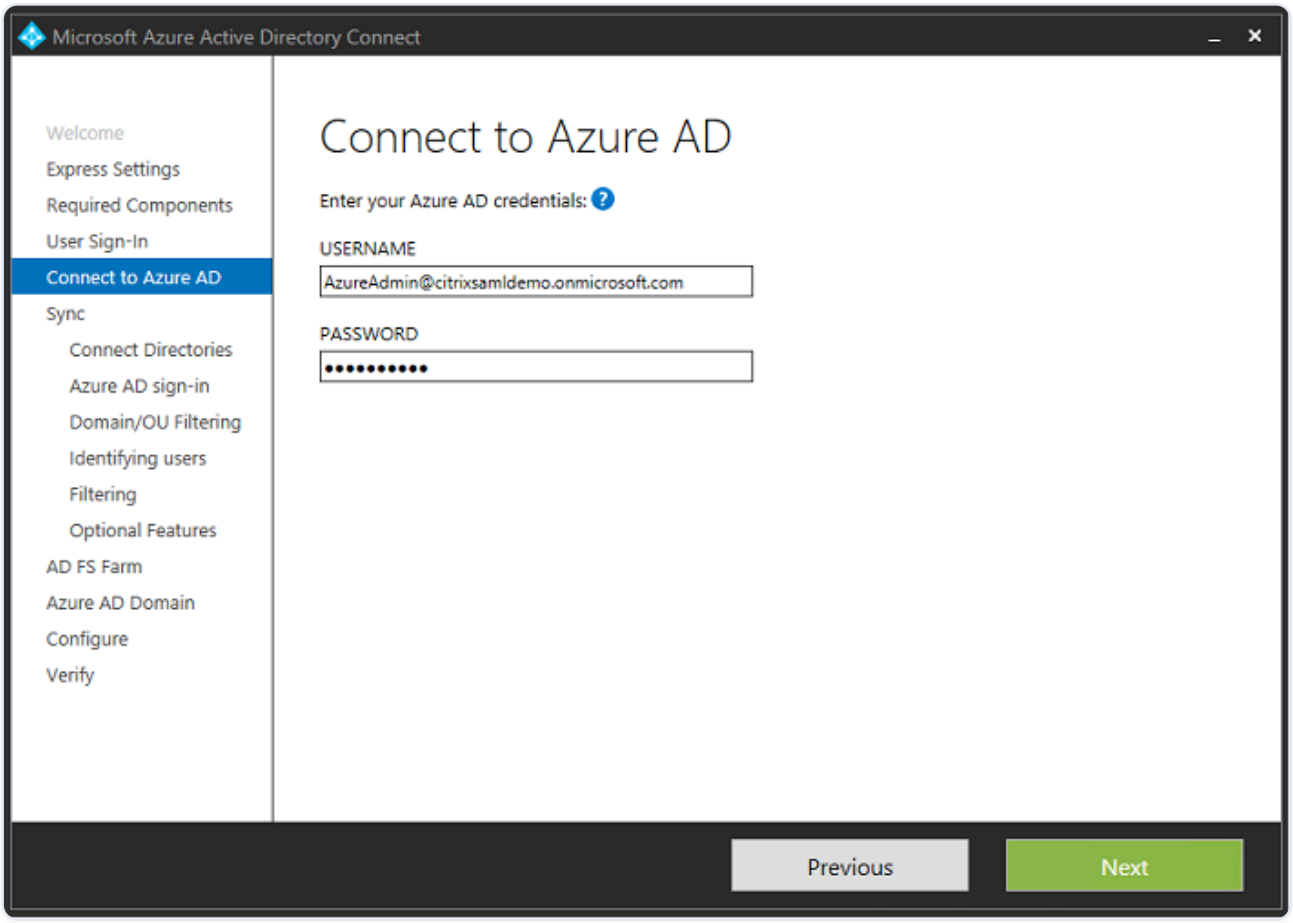


Sélectionnez l'option d'authentification unique **Fédération avec AD FS**.



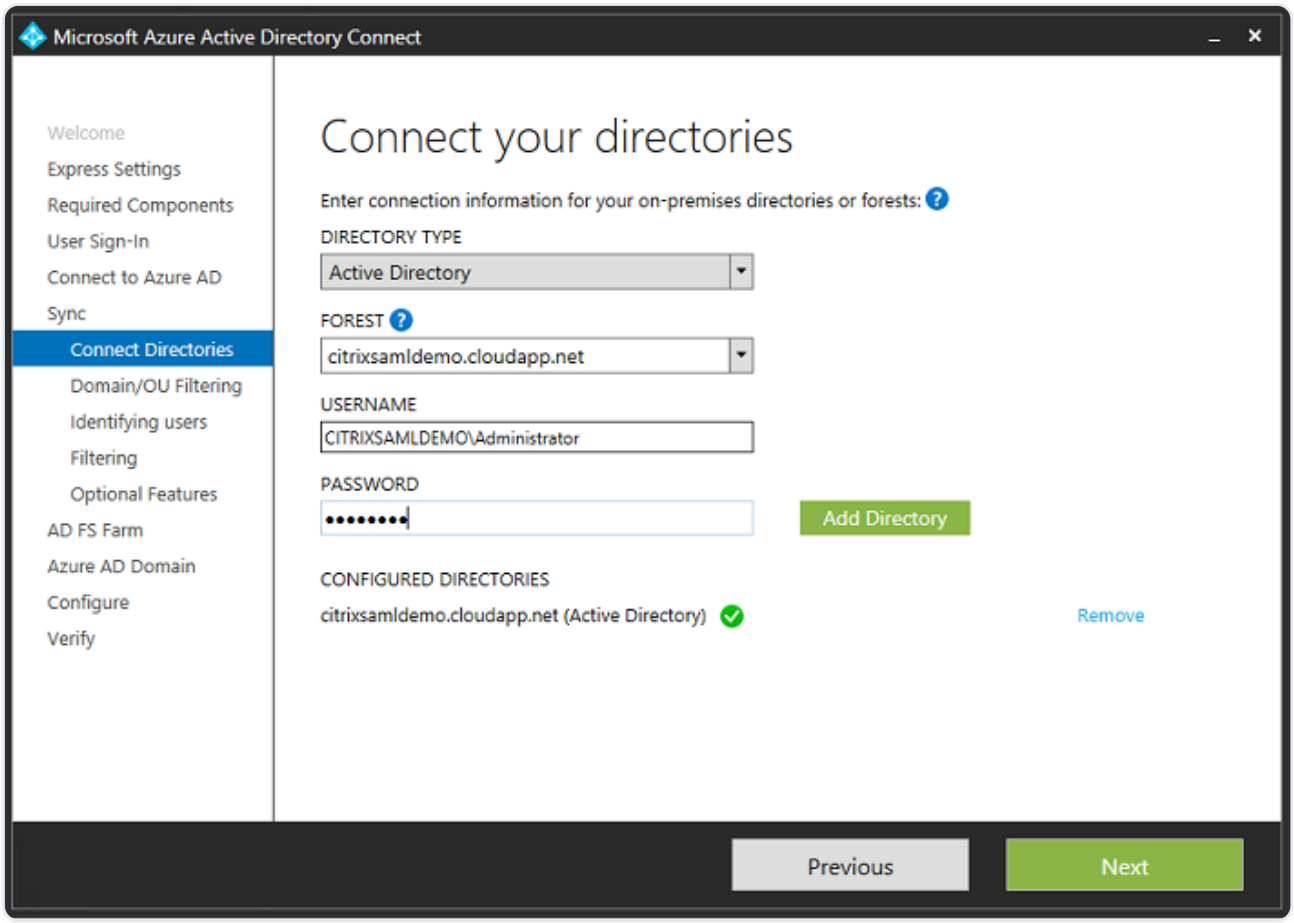
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connectez-vous à Azure avec le compte administrateur que vous avez créé précédemment.

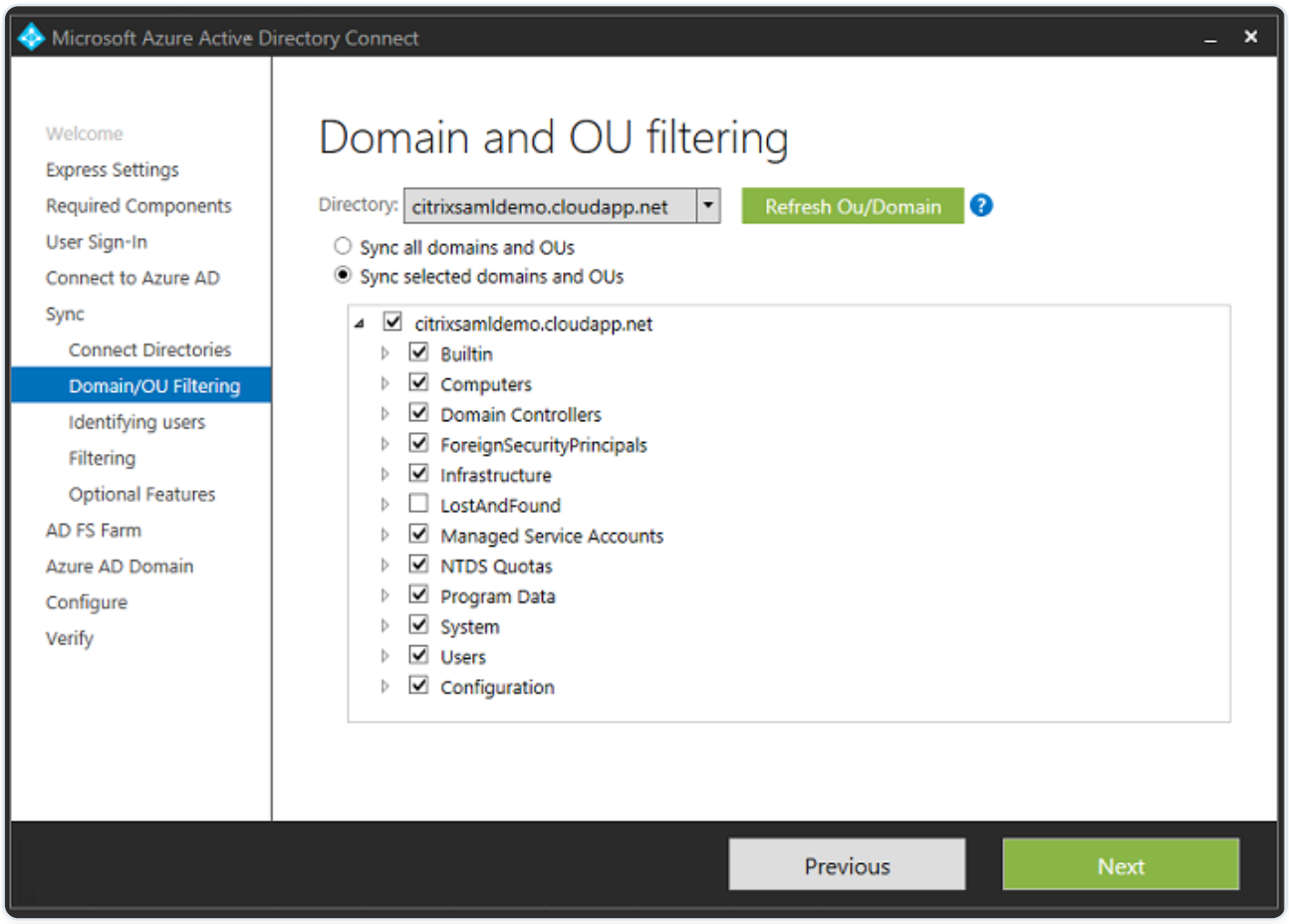


Sélectionnez la forêt AD interne.

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

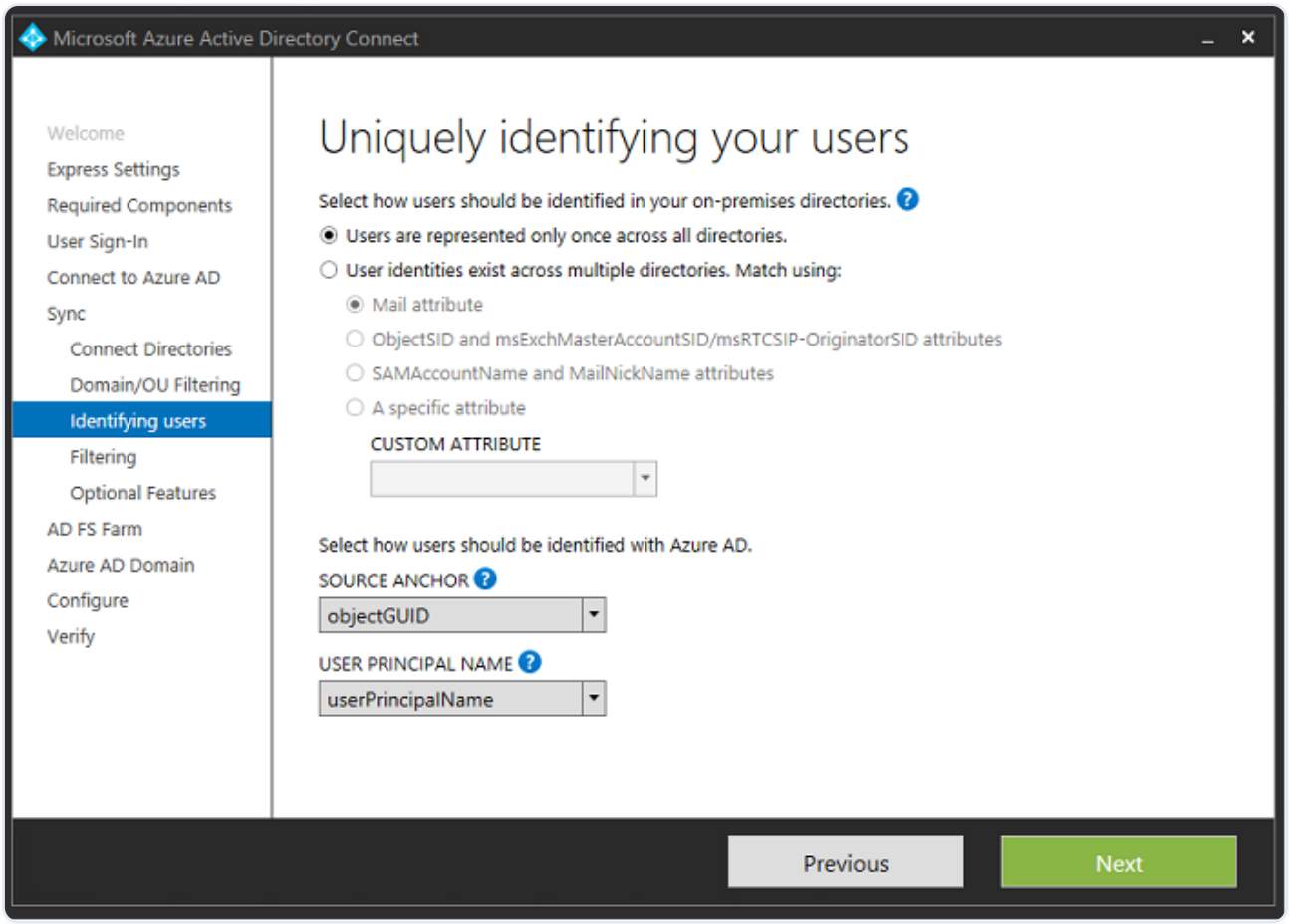


Synchronisez tous les objets Active Directory hérités avec Azure AD.



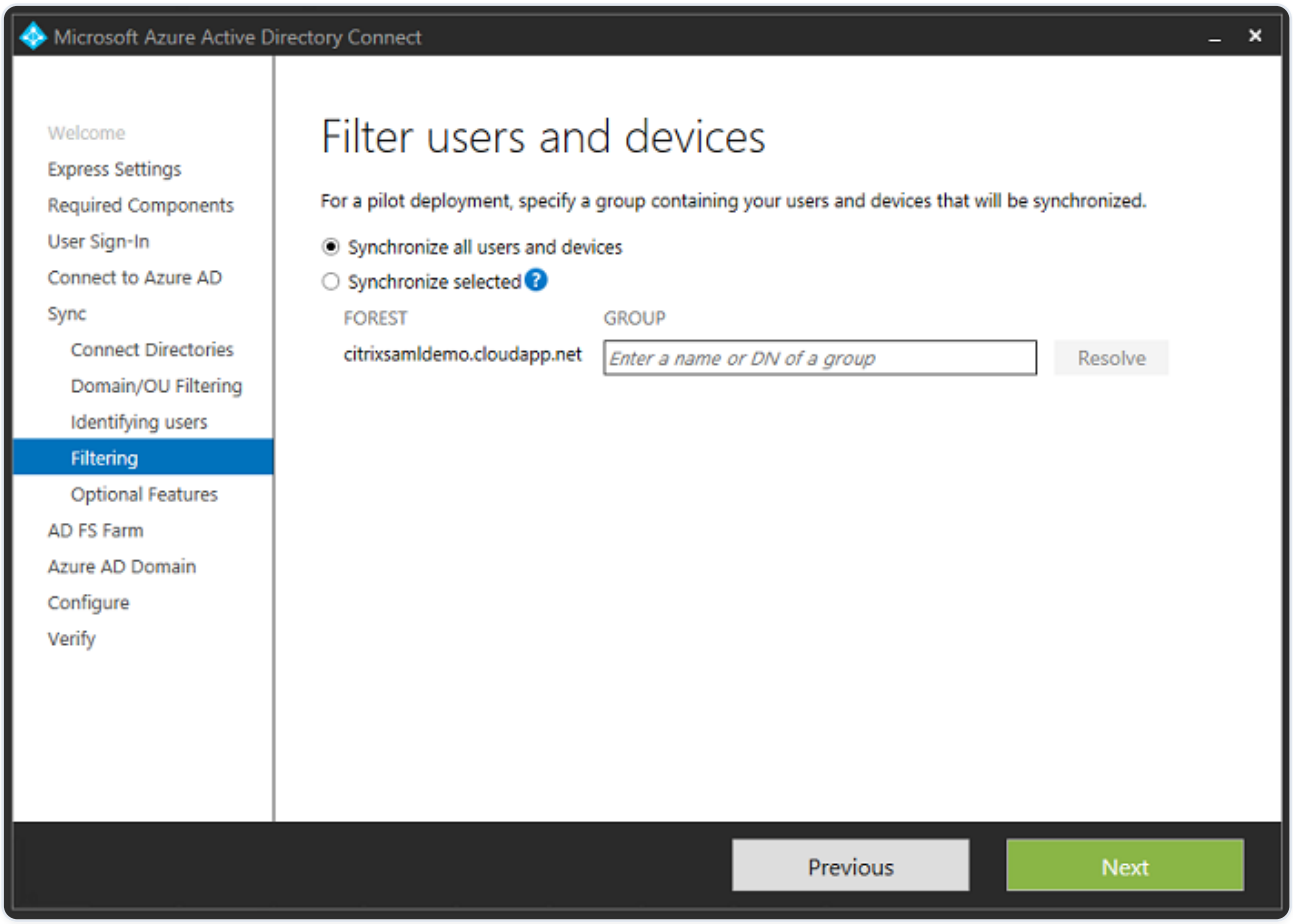
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si la structure de l'annuaire est simple, vous pouvez vous fier à l'unicité suffisante des noms d'utilisateur pour identifier un utilisateur qui se connecte.



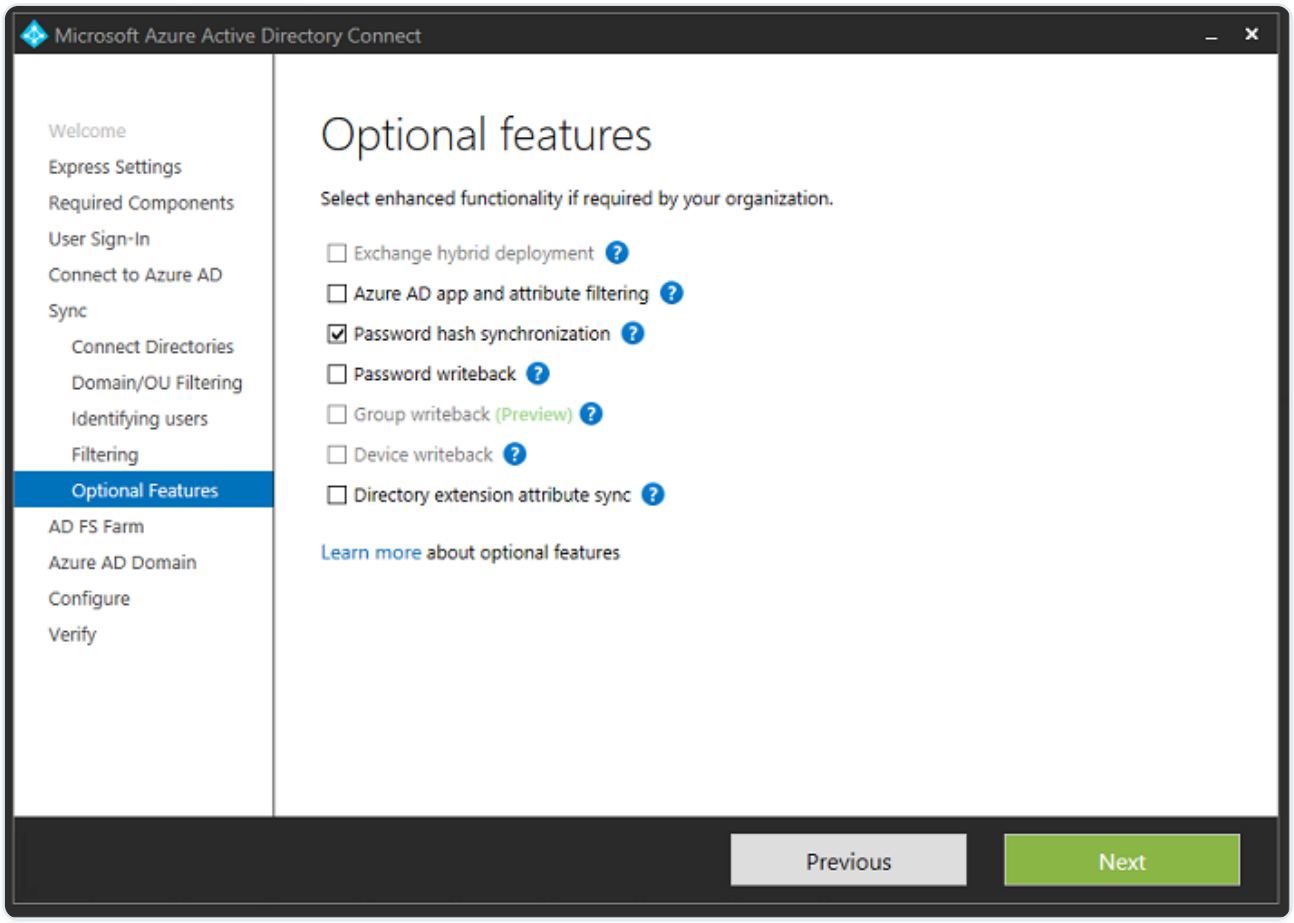
Acceptez les options de filtrage par défaut, ou restreignez les utilisateurs et les appareils à un ensemble de groupes particulier.

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



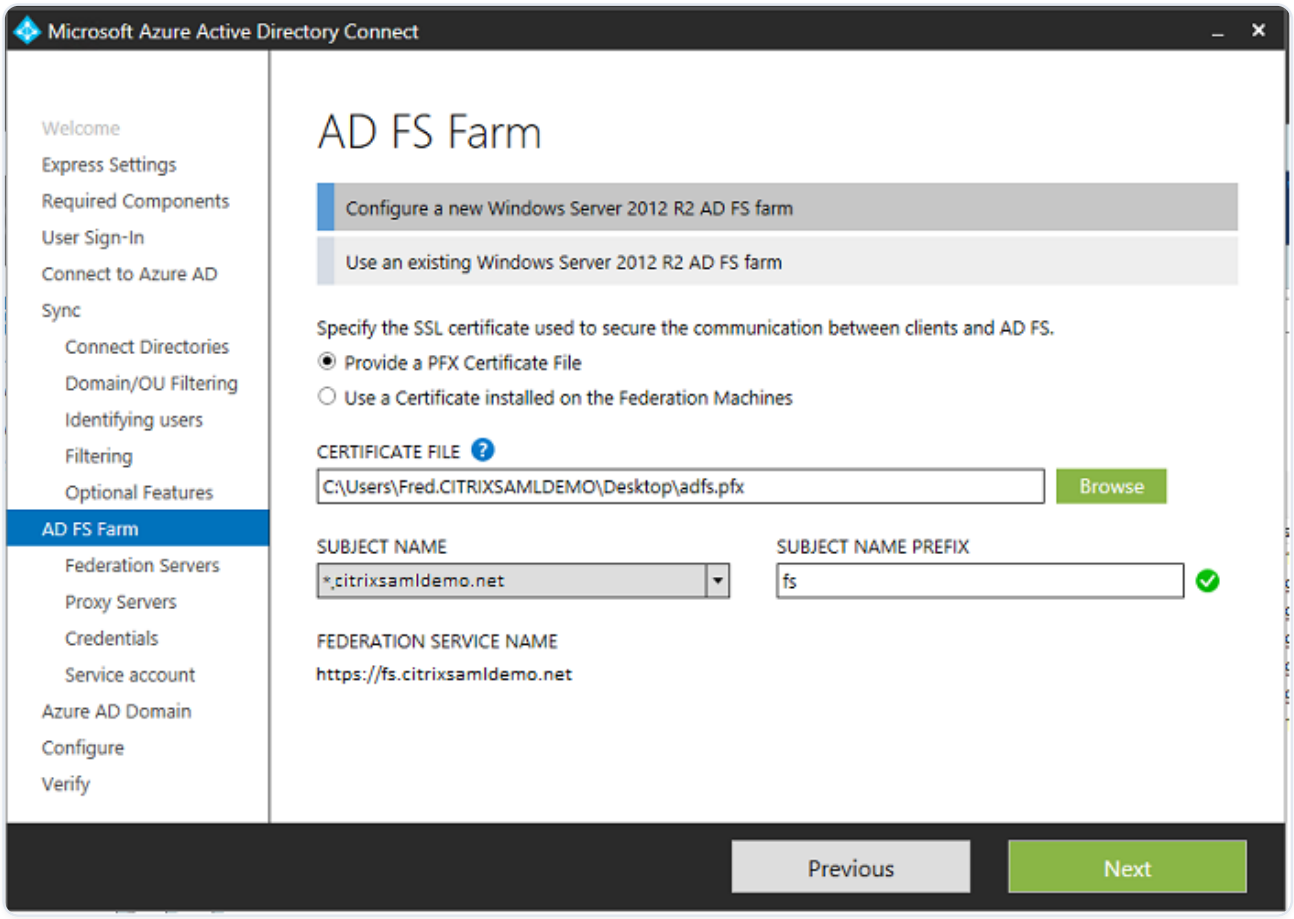
Si vous le souhaitez, vous pouvez synchroniser les mots de passe Azure AD avec Active Directory. Cela n'est généralement pas nécessaire pour l'authentification basée sur ADFS.

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



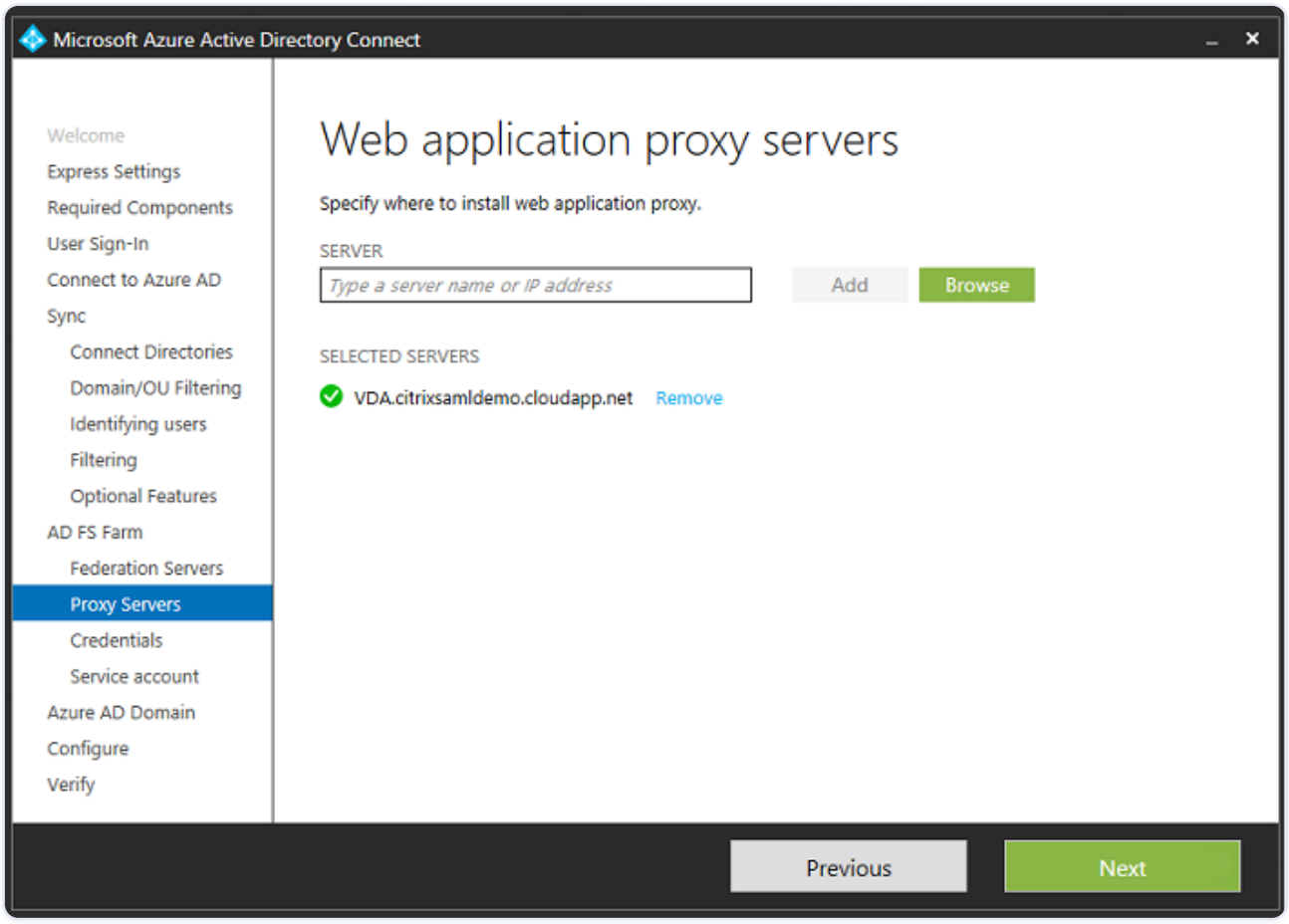
Sélectionnez le fichier PFX du certificat à utiliser dans AD FS, en spécifiant fs.citrixsamldemo.net comme nom DNS.

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



Lorsque vous êtes invité à sélectionner un serveur proxy, entrez l'adresse du serveur wap.citrixsamldemo.net. Vous devrez peut-être exécuter l'applet de commande **Enable-PSRemoting –Force** en tant qu'administrateur sur le serveur proxy d'application Web, afin qu'Azure AD Connect puisse le configurer.

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

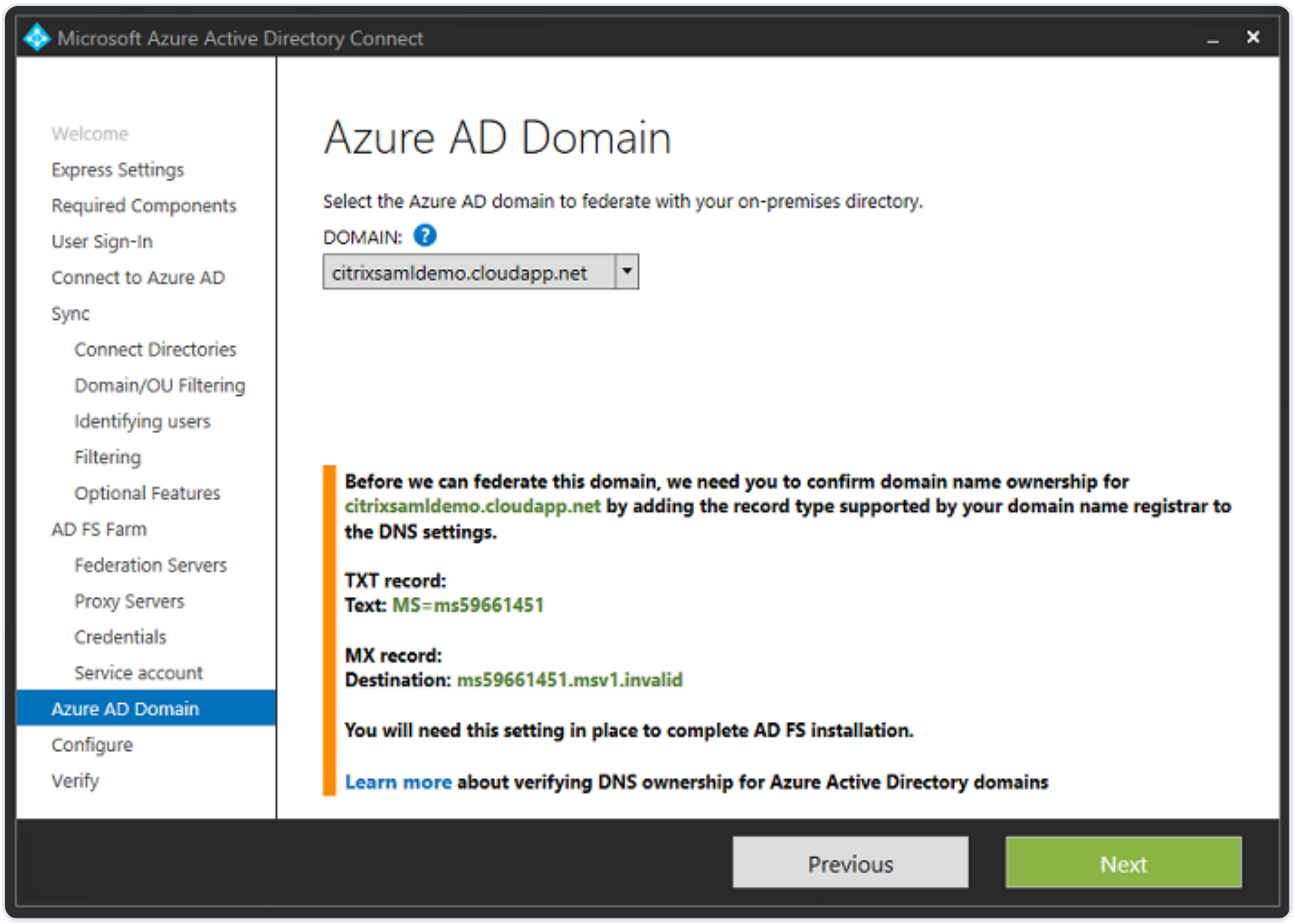


REMARQUE :

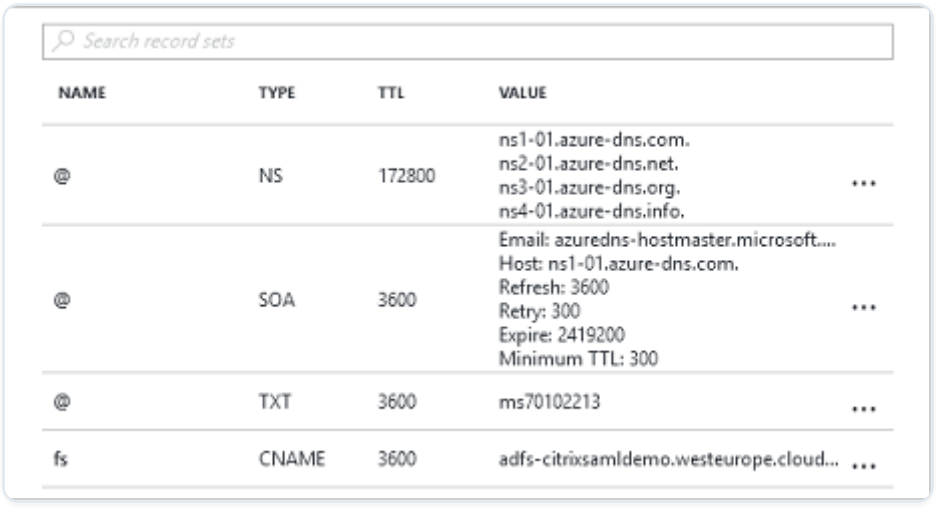
Si cette étape échoue en raison de problèmes de confiance de Remote PowerShell, essayez de joindre le serveur proxy d'application Web au domaine.

Pour les étapes restantes de l'assistant, utilisez les mots de passe administrateur standard et créez un compte de service pour ADFS. Azure AD Connect vous invitera ensuite à valider la propriété de la zone DNS.

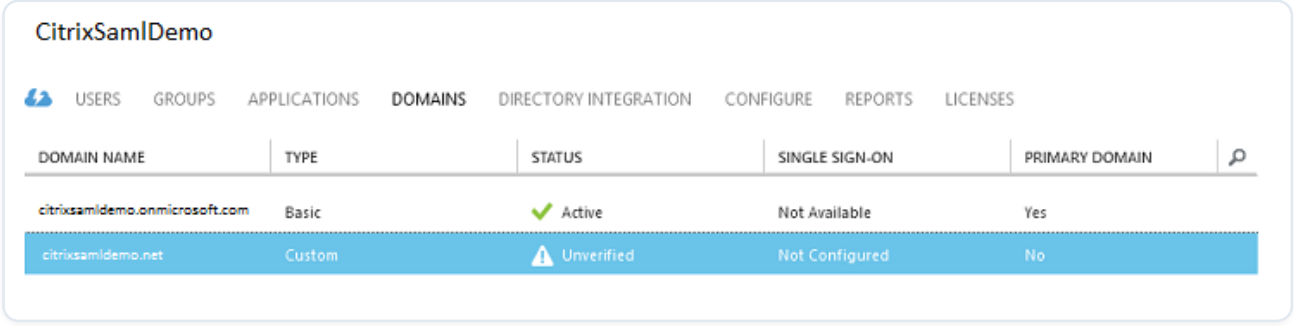
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Ajoutez les enregistrements TXT et MX aux enregistrements d'adresse DNS dans Azure.



Cliquez sur **Vérifier** dans la console de gestion Azure.

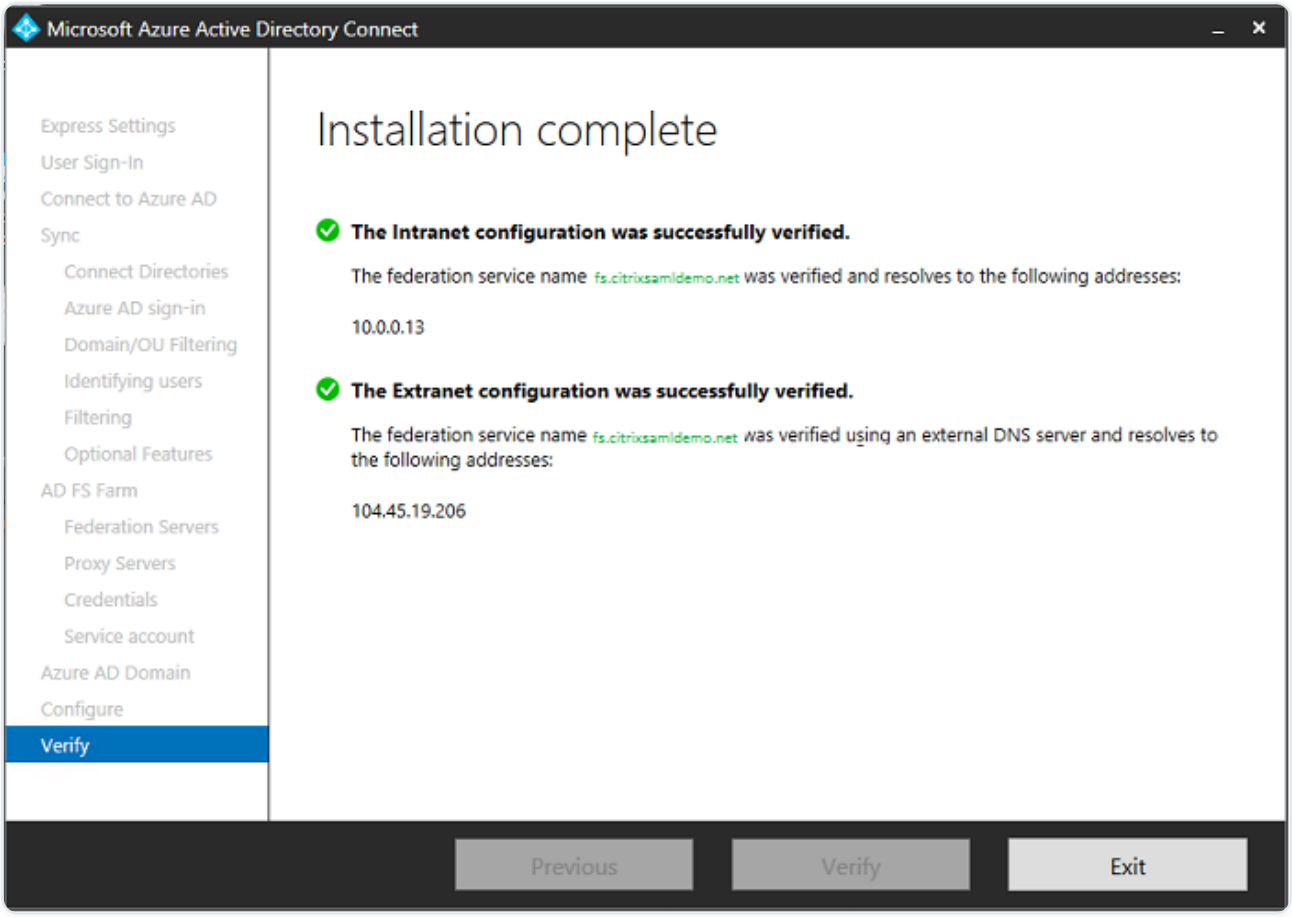


© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Si cette étape échoue, vous pouvez vérifier le domaine avant d'exécuter Azure AD Connect.

Une fois terminé, l'adresse externe fs.citrixsamldemo.net est contactée via le port 443.

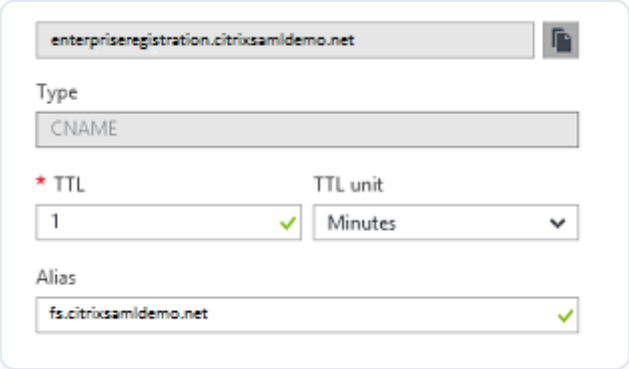


Activer la jonction Azure AD

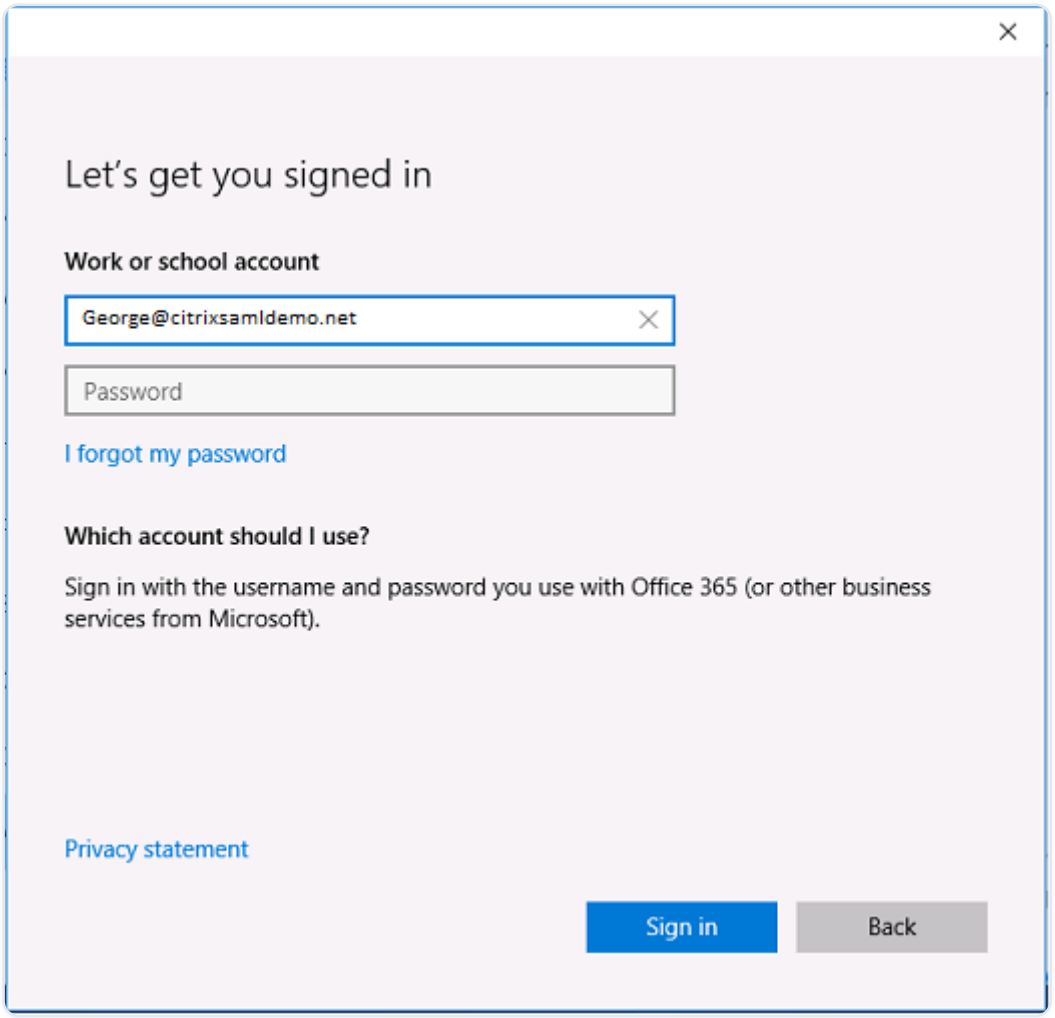
Lorsqu'un utilisateur saisit une adresse e-mail afin que Windows 10 puisse effectuer une jonction Azure AD, le suffixe DNS est utilisé pour construire un enregistrement DNS CNAME qui doit pointer vers ADFS : enterpriseregistration.\<*upnsuffix*>.

Dans l'exemple, il s'agit de `fs.citrixsamldemo.net`.

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

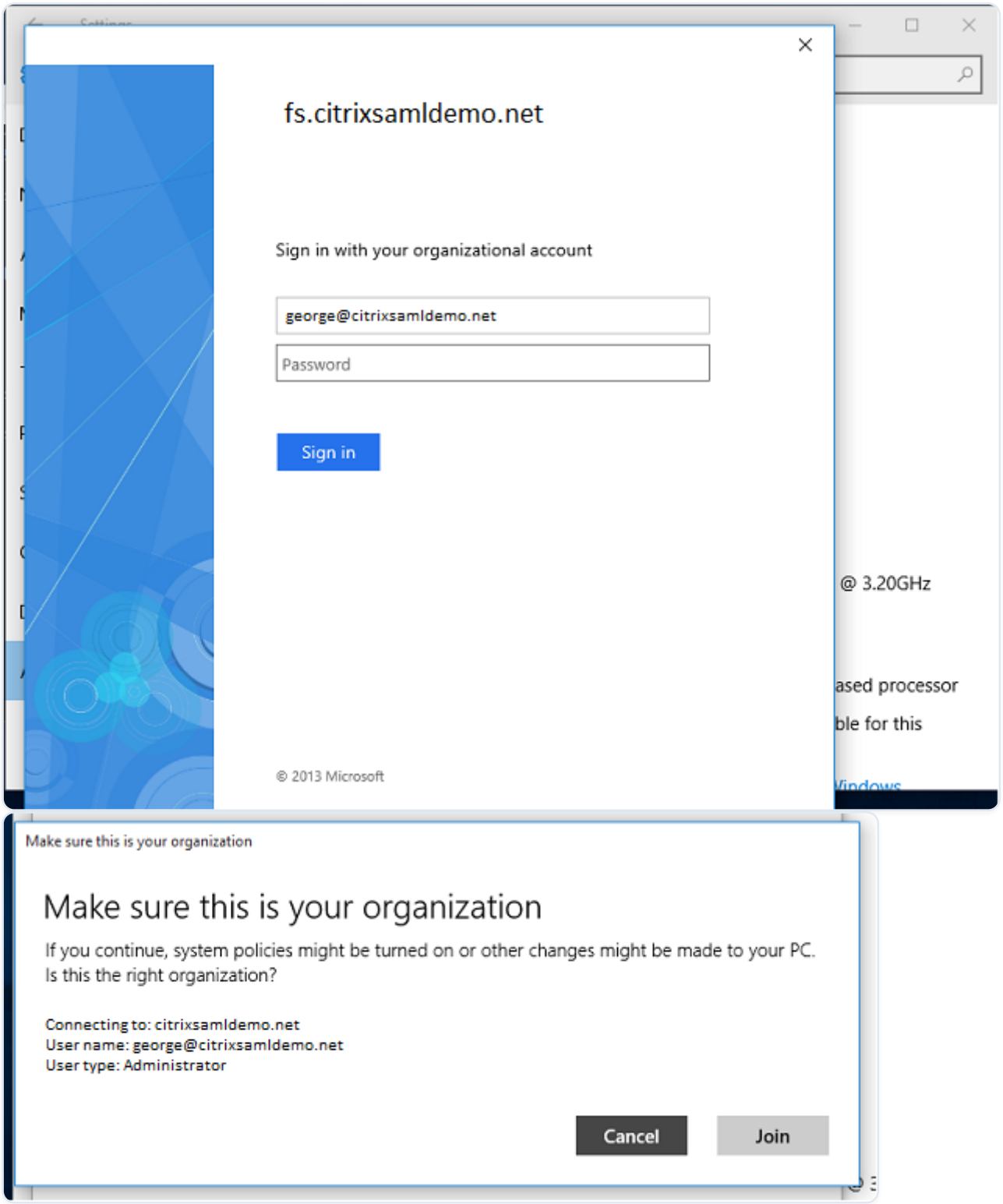


Si vous n'utilisez pas d'autorité de certification publique, assurez-vous que le certificat racine ADFS est installé sur l'ordinateur Windows 10 afin que Windows fasse confiance au serveur ADFS. Effectuez une jonction de domaine Azure AD à l'aide du compte utilisateur standard généré précédemment.

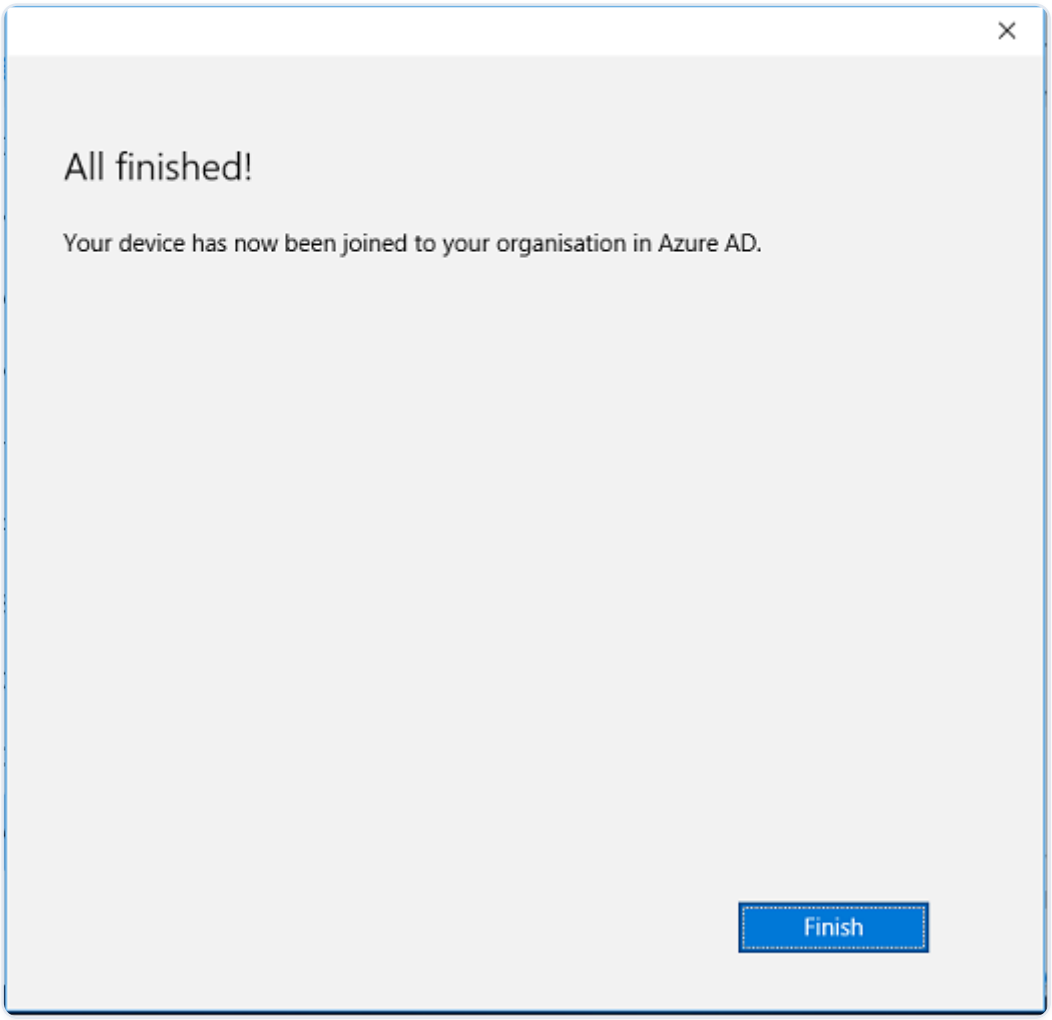


Notez que l'UPN doit correspondre à l'UPN reconnu par le contrôleur de domaine ADFS.

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



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



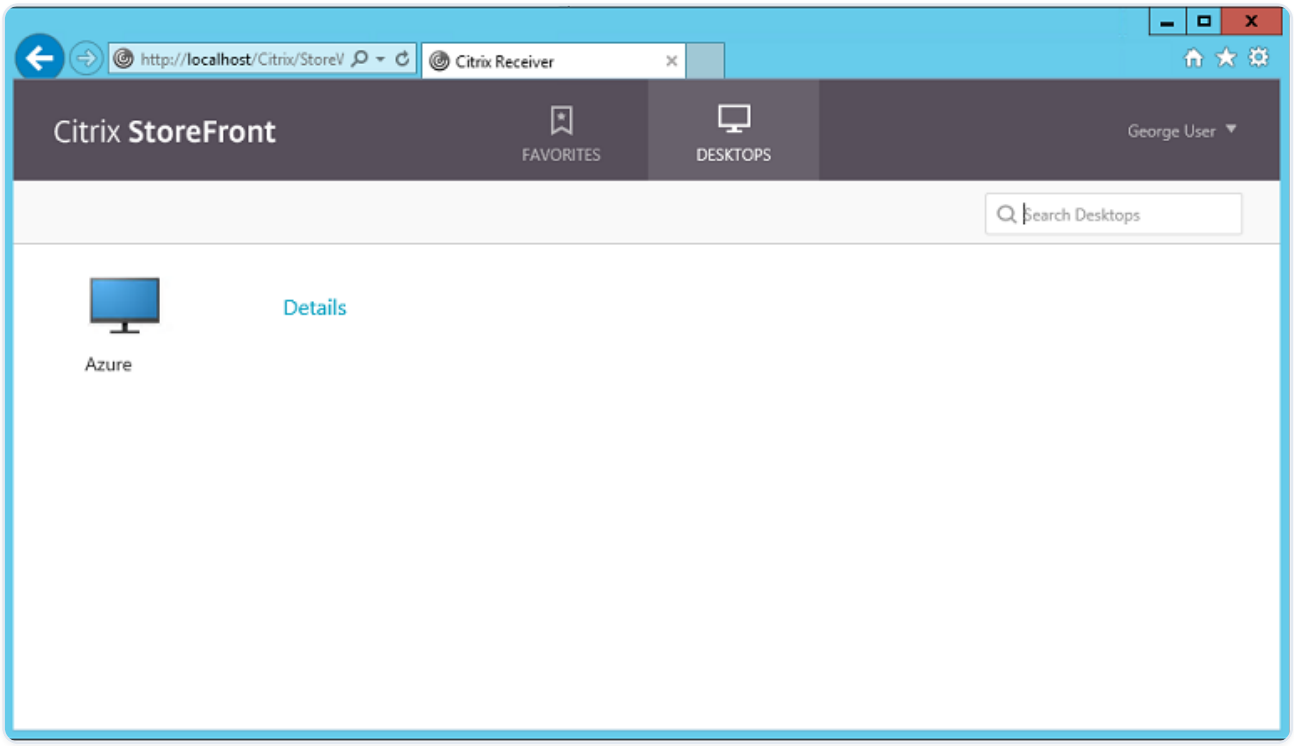
Vérifiez que la jonction Azure AD a réussi en redémarrant la machine et en vous connectant à l'aide de l'adresse e-mail de l'utilisateur. Une fois connecté, lancez Microsoft Edge et connectez-vous à `<http://myapps.microsoft.com>`. Le site Web devrait utiliser l'authentification unique automatiquement.

Installer Citrix Virtual Apps ou Citrix Virtual Desktops

Vous pouvez installer les machines virtuelles Delivery Controller et VDA dans Azure directement à partir de l'ISO de Citrix Virtual Apps ou Citrix Virtual Desktops de la manière habituelle.

Dans cet exemple, StoreFront est installé sur le même serveur que le Delivery Controller. Le VDA est installé en tant que travailleur RDS Windows 2012 R2 autonome, sans intégration avec Machine Creation Services (bien que cela puisse être configuré en option). Vérifiez que l'utilisateur George@citrixsamldemo.net peut s'authentifier avec un mot de passe avant de continuer.

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



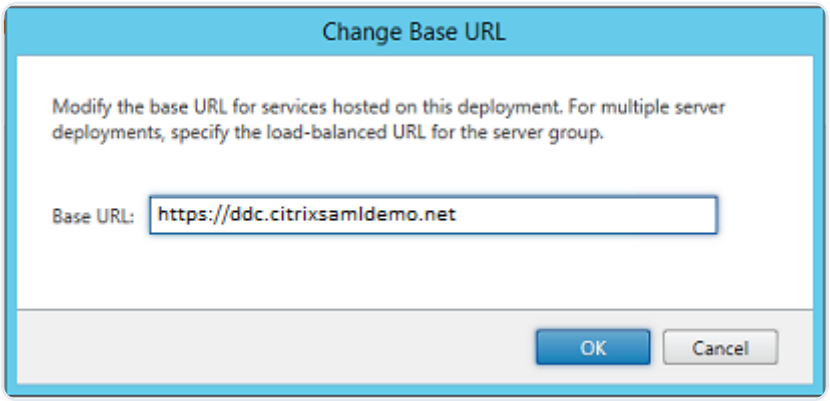
Exécutez la cmdlet PowerShell **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** sur le Controller pour permettre à StoreFront™ de s'authentifier sans les informations d'identification des utilisateurs.

Installer le service d'authentification fédérée

Installez FAS sur le serveur ADFS et configurez une règle pour que le Delivery Controller agisse comme un StoreFront de confiance (puisque, dans cet exemple, StoreFront est installé sur la même VM que le Delivery Controller). Voir Installer et configurer.

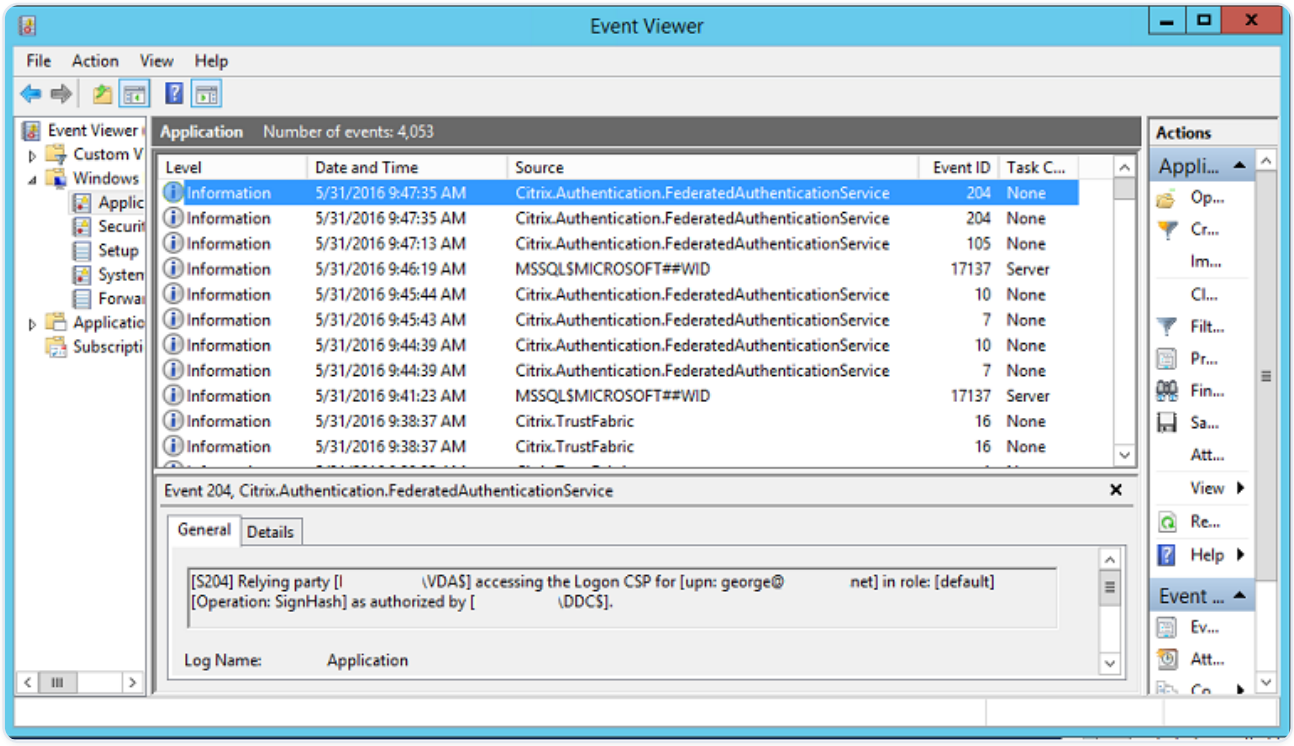
Configurer StoreFront

Demandez un certificat d'ordinateur pour le Delivery Controller, et configurez IIS et StoreFront pour utiliser HTTPS en définissant une liaison IIS pour le port 443, et en modifiant l'adresse de base de StoreFront en https:.



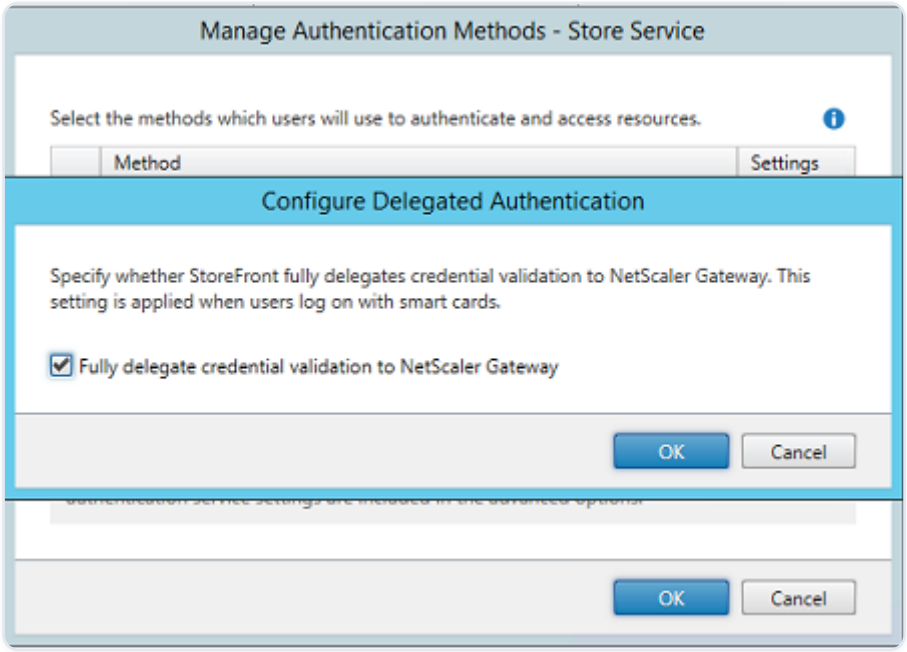
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurez StoreFront pour utiliser le serveur FAS (utilisez le script PowerShell dans Installer et configurer), et testez en interne dans Azure, en vous assurant que la connexion utilise FAS en vérifiant l'observateur d'événements sur le serveur FAS.



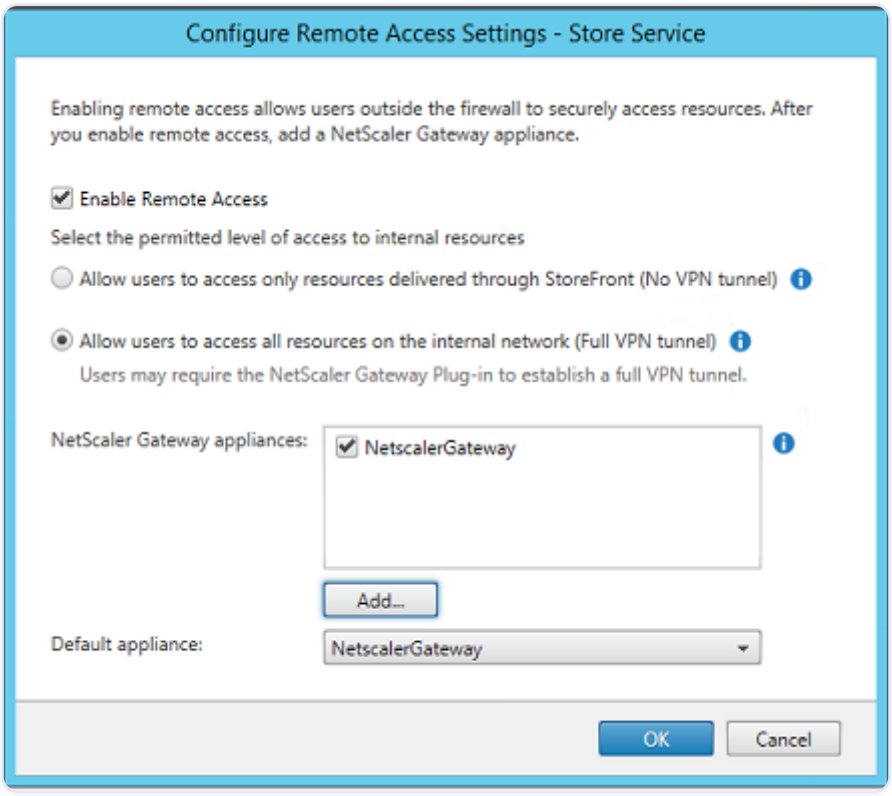
Configurer StoreFront pour utiliser Citrix Gateway

À l'aide de l'interface graphique **Gérer les méthodes d'authentification** dans la console de gestion StoreFront, configurez StoreFront pour utiliser Citrix Gateway afin d'effectuer l'authentification.



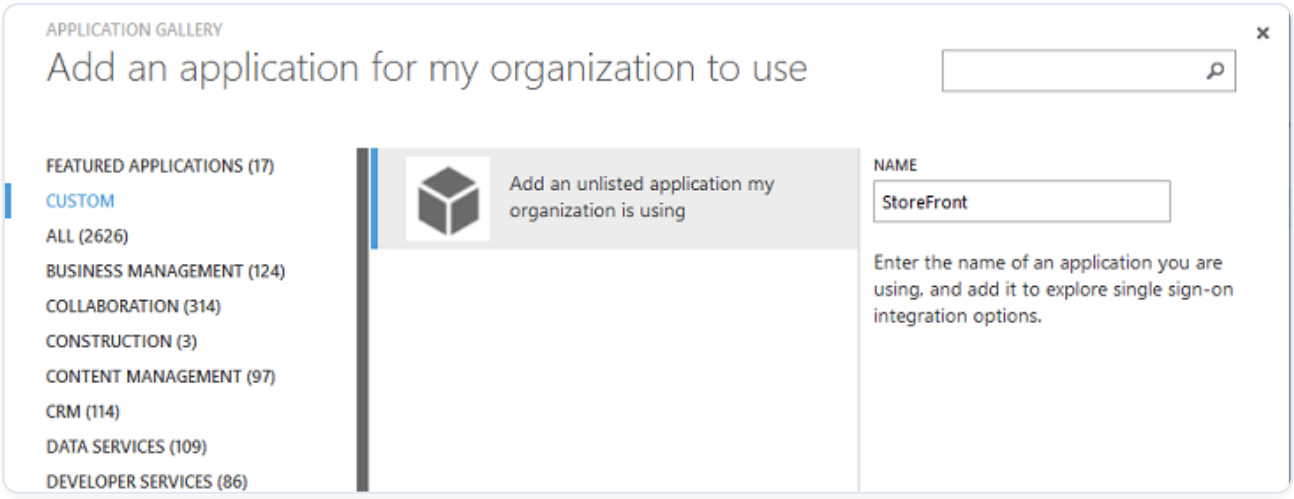
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour intégrer les options d'authentification de Citrix Gateway, configurez une Secure Ticket Authority (STA) et configurez l'adresse de Citrix Gateway.



Configurer une nouvelle application Azure AD pour l'authentification unique à StoreFront

Cette section utilise les fonctionnalités d'authentification unique SAML 2.0 d'Azure AD, qui nécessitent actuellement un abonnement Azure Active Directory Premium. Dans l'outil de gestion Azure AD, sélectionnez **Nouvelle application**, en choisissant **Ajouter une application depuis la galerie**.

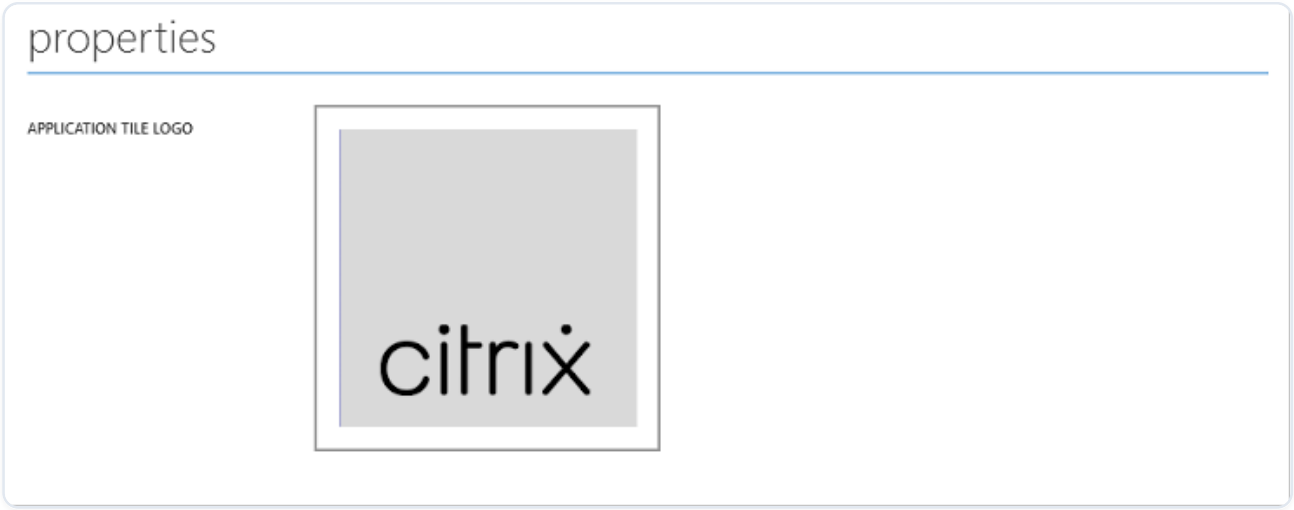


Sélectionnez **PERSONNALISÉ > Ajouter une application non répertoriée utilisée par mon organisation** pour créer une nouvelle application personnalisée pour vos utilisateurs.

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

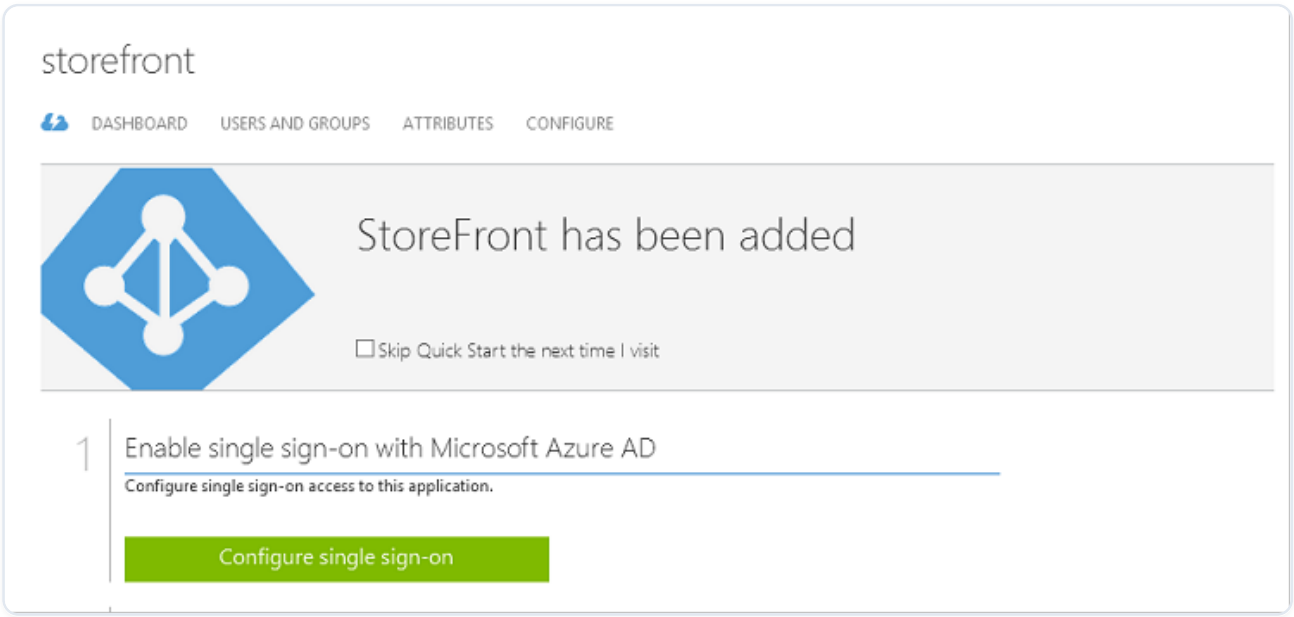
Configurer une icône

Créez une image de 215 par 215 pixels et téléchargez-la sur la page CONFIGURER pour l'utiliser comme icône pour l'application.



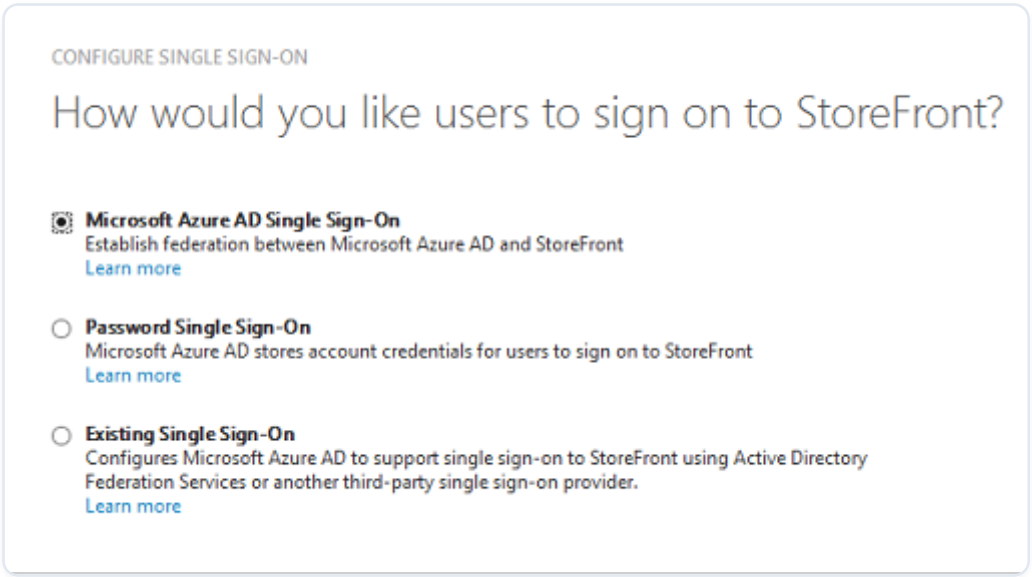
Configurer l'authentification SAML

Retournez à la page de présentation du tableau de bord de l'application et sélectionnez **Configurer l'authentification unique**.

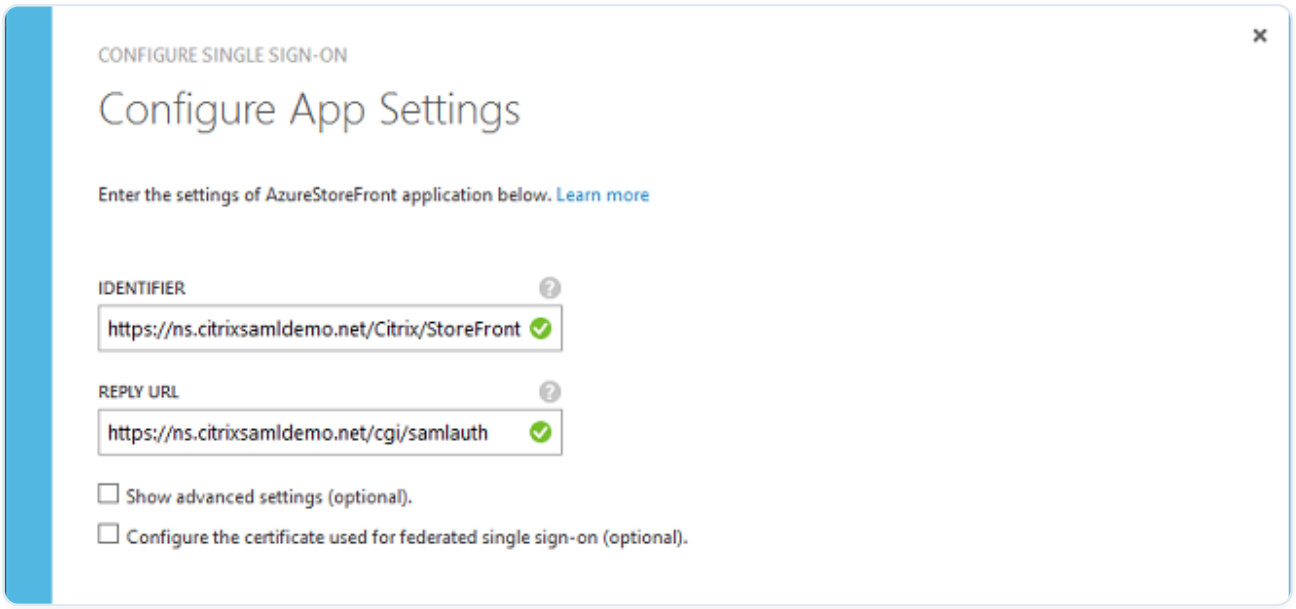


Ce déploiement utilisera l'authentification SAML 2.0, qui correspond à **Microsoft Azure AD Single Sign-On**.

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

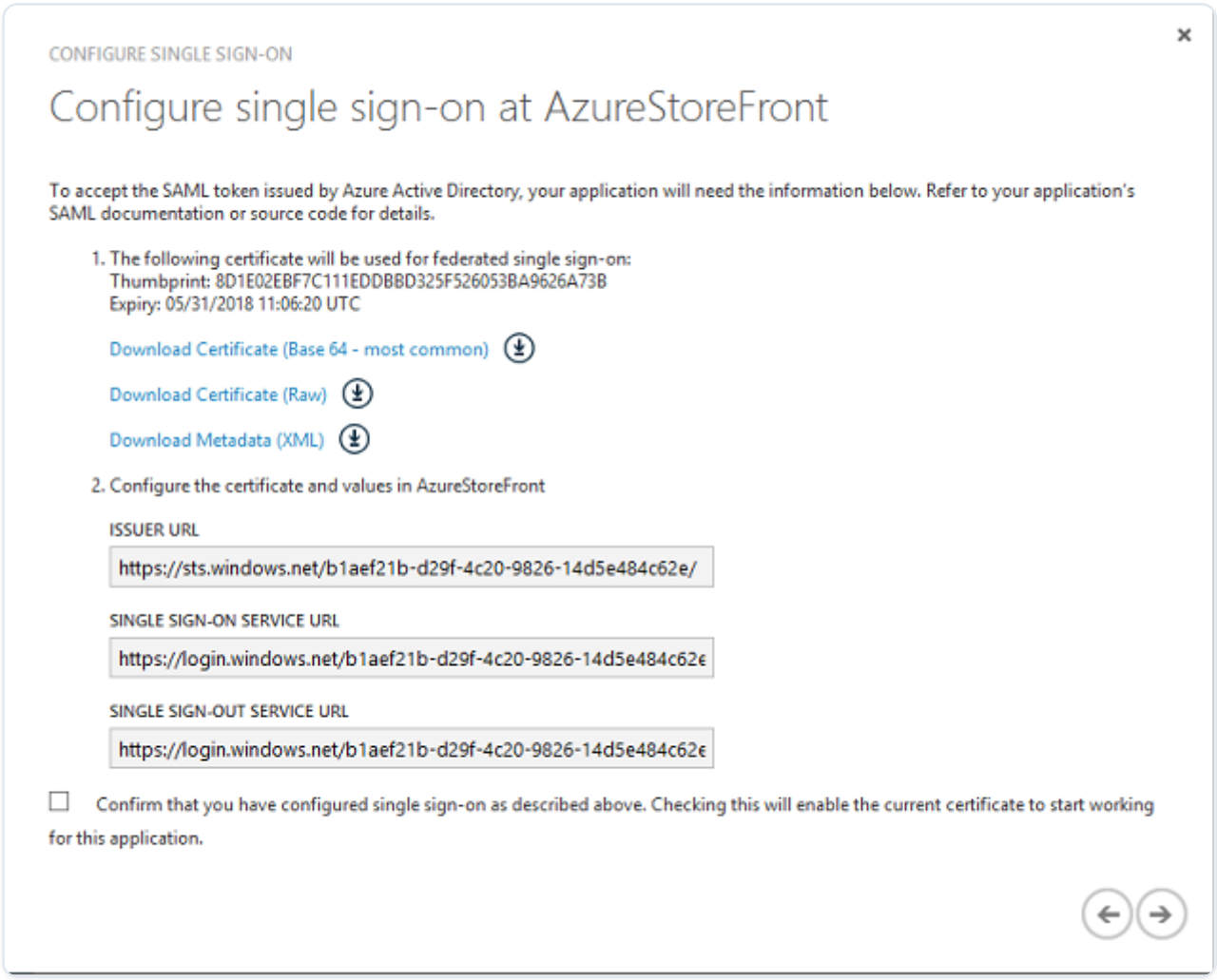


L'**identifiant** peut être une chaîne arbitraire (il doit correspondre à la configuration fournie à Citrix Gateway) ; dans cet exemple, l'**URL de réponse** est */cgi/samlauth* sur le serveur Citrix Gateway.



La page suivante contient des informations utilisées pour configurer Citrix Gateway en tant que partie de confiance pour Azure AD.

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



Téléchargez le certificat de signature approuvé en base 64 et copiez les URL de connexion et de déconnexion. Vous les collerez ultérieurement dans les écrans de configuration de Citrix Gateway.

Attribuer l'application aux utilisateurs

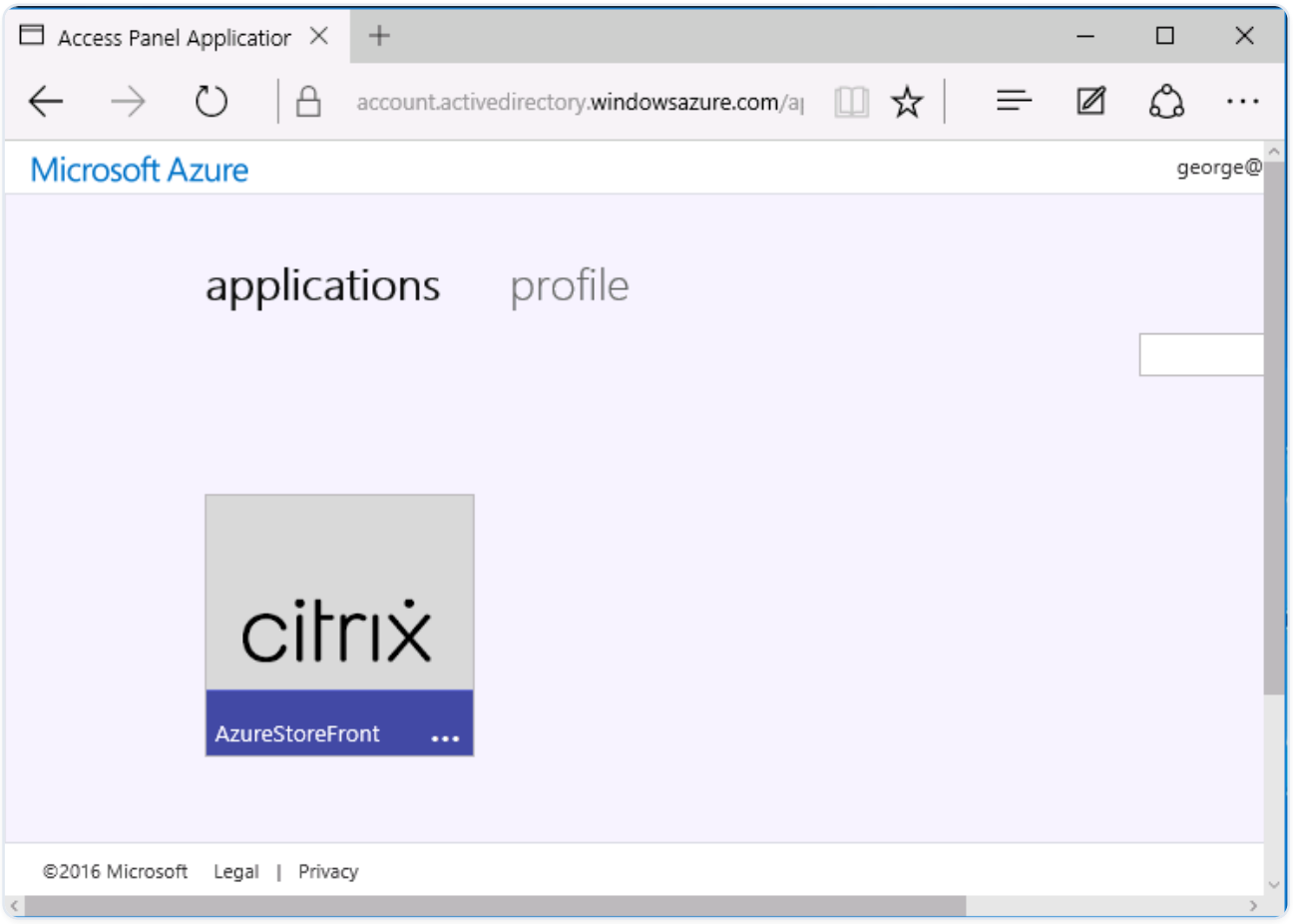
La dernière étape consiste à activer l'application afin qu'elle apparaisse sur la page de contrôle « myapps.microsoft.com » des utilisateurs. Cela se fait sur la page UTILISATEURS ET GROUPES. Attribuez l'accès aux comptes d'utilisateurs de domaine synchronisés par Azure AD Connect. D'autres comptes peuvent également être utilisés, mais ils doivent être explicitement mappés car ils ne sont pas conformes au modèle \<user>@\<domain>.

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



Page MyApps

Lorsque l'application a été configurée, elle apparaît dans les listes d'applications Azure des utilisateurs lorsqu'ils visitent `<https://myapps.microsoft.com>`.

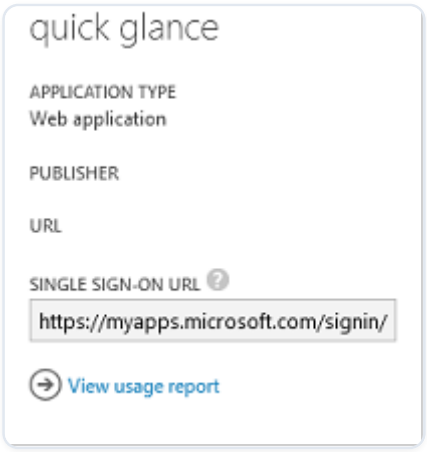


Lorsqu'il est joint à Azure AD, Windows 10 prend en charge l'authentification unique aux applications Azure pour l'utilisateur qui se connecte. Cliquer sur l'icône dirige le navigateur vers la page web SAML cgi/samlauth qui a été configurée précédemment.

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

URL d'authentification unique

Retournez à l'application dans le tableau de bord Azure AD. Une URL d'authentification unique est maintenant disponible pour l'application. Cette URL est utilisée pour fournir des liens de navigateur web ou pour créer des raccourcis du menu Démarrer qui dirigent les utilisateurs directement vers StoreFront.



Collez cette URL dans un navigateur web pour vous assurer que vous êtes redirigé par Azure AD vers la page web Citrix Gateway cgi/samlauth configurée précédemment. Cela ne fonctionne que pour les utilisateurs auxquels l'accès a été attribué, et ne fournira l'authentification unique que pour les sessions de connexion Windows 10 jointes à Azure AD. (Les autres utilisateurs seront invités à saisir leurs informations d'identification Azure AD.)

Installer et configurer Citrix Gateway

Pour accéder à distance au déploiement, cet exemple utilise une VM distincte exécutant NetScaler (maintenant Citrix Gateway). Celle-ci peut être achetée sur l'Azure Store. Cet exemple utilise la version "Bring your own License" de NetScaler 11.0.

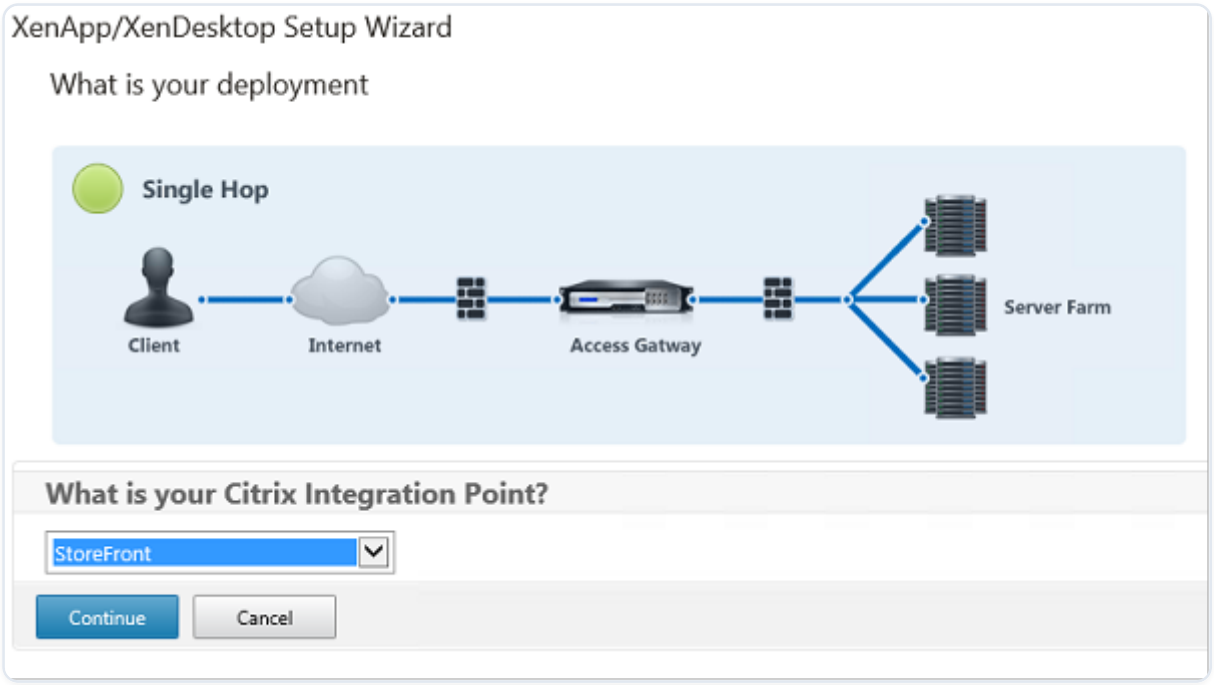
Connectez-vous à la VM NetScaler®, en pointant un navigateur web vers l'adresse IP interne, en utilisant les informations d'identification spécifiées lors de l'authentification de l'utilisateur. Notez que vous devez modifier le mot de passe de l'utilisateur nsroot dans une VM Azure AD.

Ajoutez les licences, en sélectionnant **redémarrer** après l'ajout de chaque fichier de licence, et pointez le résolveur DNS vers le contrôleur de domaine Microsoft.

Exécuter l'assistant de configuration de Citrix Virtual Apps and Desktops

Cet exemple commence par la configuration d'une intégration StoreFront simple sans SAML. Une fois ce déploiement fonctionnel, il ajoute une stratégie d'ouverture de session SAML.

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

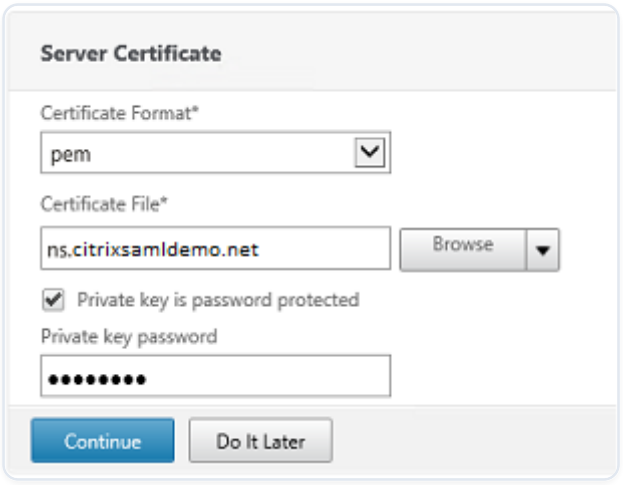


Sélectionnez les paramètres standard de Citrix Gateway StoreFront. Pour une utilisation dans Microsoft Azure, cet exemple configure le port 4433, plutôt que le port 443. Vous pouvez également rediriger ou remapper le site web administratif de Citrix Gateway.



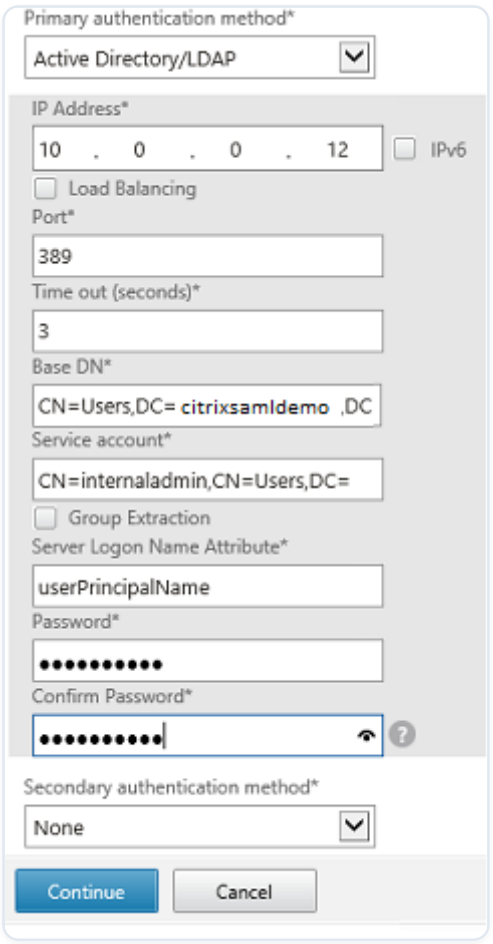
Par souci de simplicité, l'exemple télécharge un certificat de serveur et une clé privée existants stockés dans un fichier.

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



Configurer le contrôleur de domaine pour la gestion des comptes AD

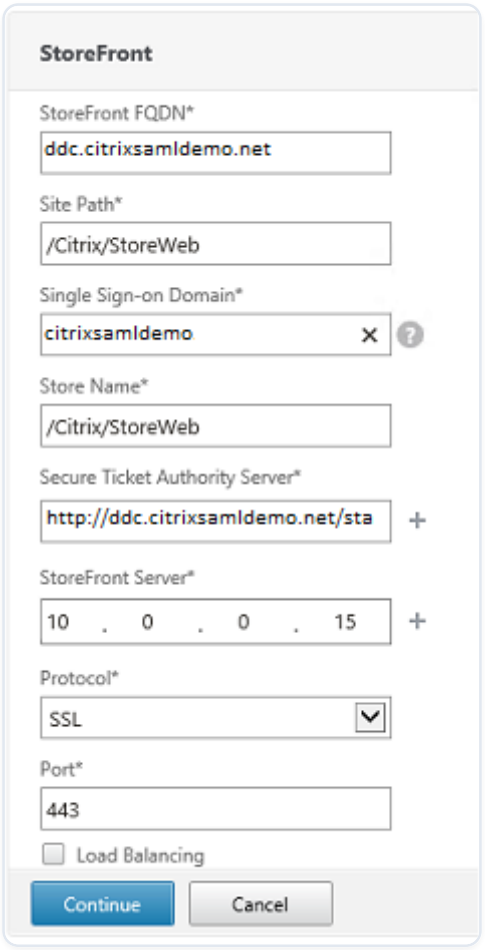
Le contrôleur de domaine sera utilisé pour la résolution des comptes, ajoutez donc son adresse IP à la méthode d'authentification principale. Notez les formats attendus dans chaque champ de la boîte de dialogue.



Configurer l'adresse StoreFront

Dans cet exemple, StoreFront a été configuré à l'aide de HTTPS, sélectionnez donc les options du protocole SSL.

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



Vérifier le déploiement de Citrix Gateway

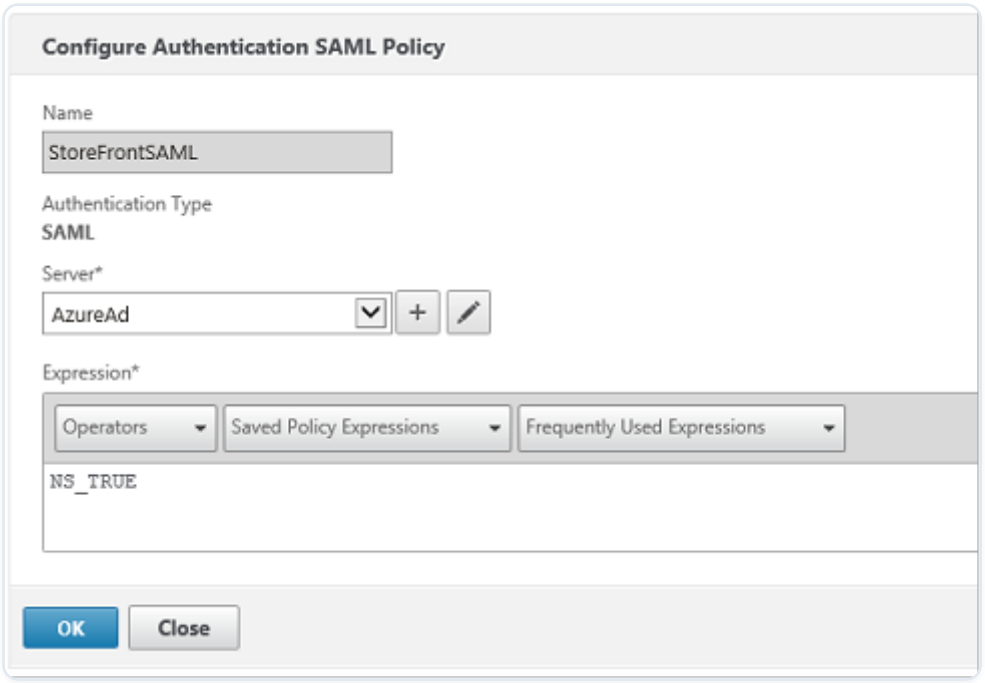
Connectez-vous à Citrix Gateway et vérifiez que l'authentification et le lancement sont réussis avec le nom d'utilisateur et le mot de passe.



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

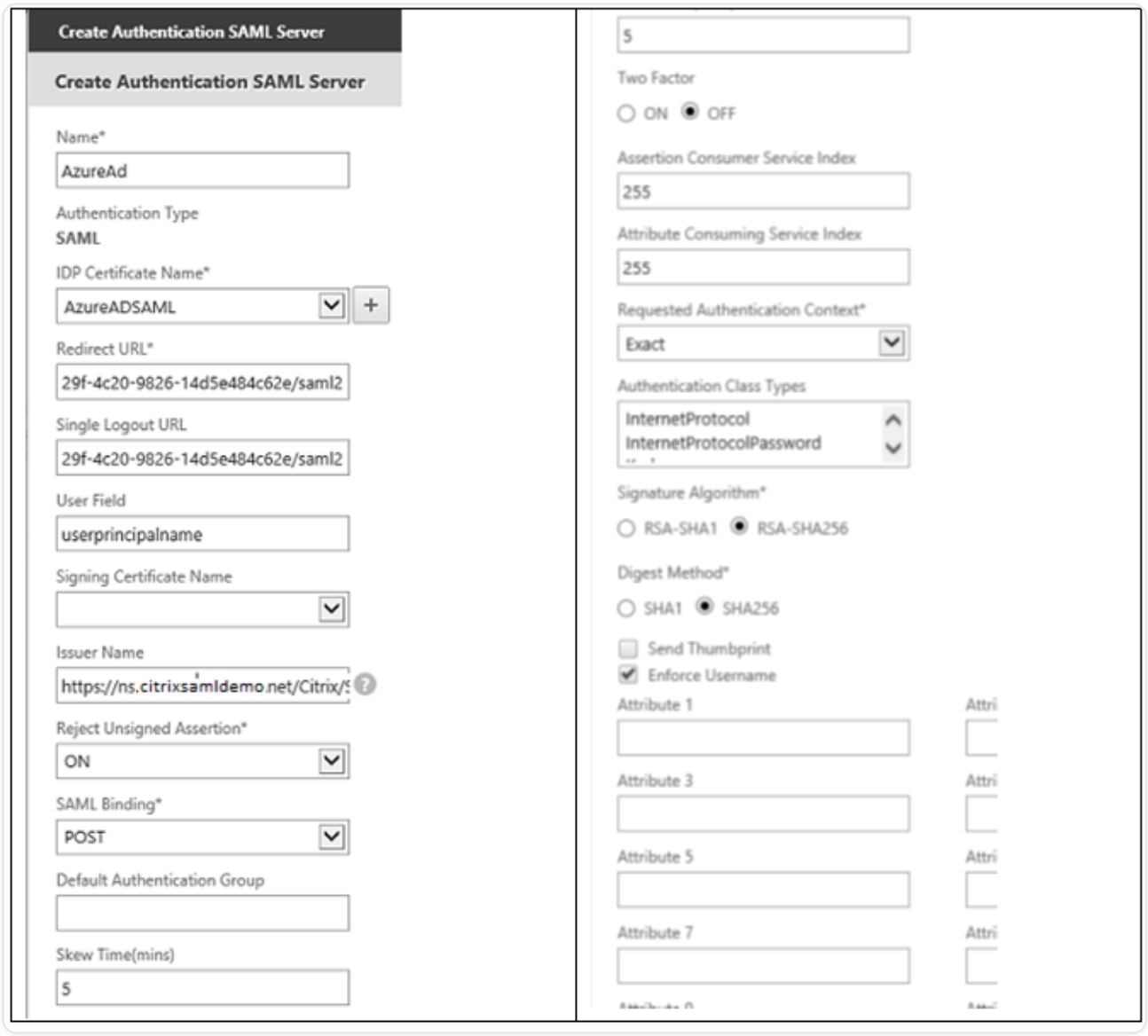
Activer la prise en charge de l'authentification SAML de Citrix Gateway

L'utilisation de SAML avec StoreFront est similaire à l'utilisation de SAML avec d'autres sites web. Ajoutez une nouvelle stratégie SAML, avec une expression de **NS_TRUE**.



Configurez le nouveau serveur IdP SAML, en utilisant les informations obtenues précédemment auprès d'Azure AD.

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

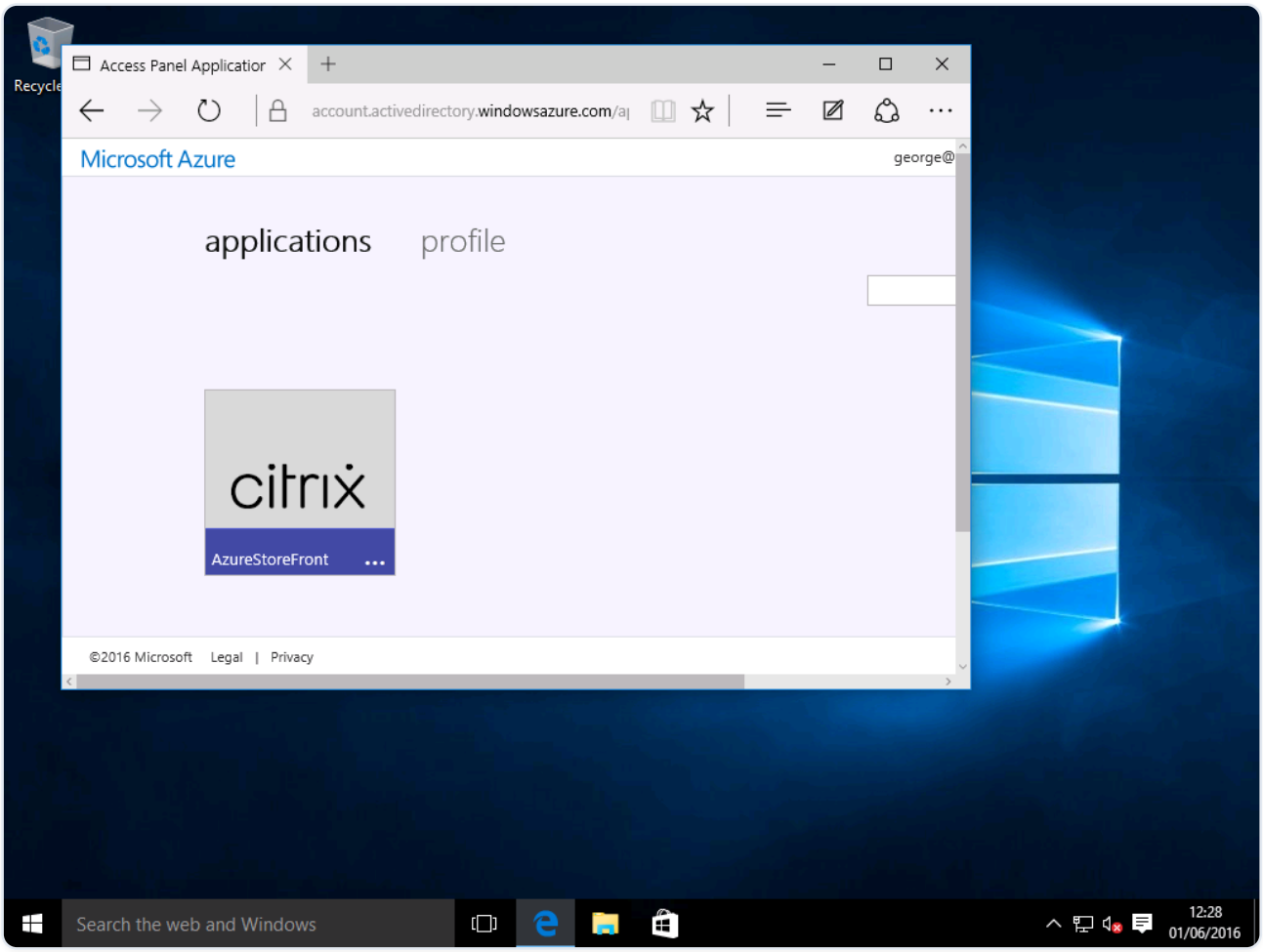


Vérifier le système de bout en bout

Connectez-vous à un bureau Windows 10 joint à Azure AD, en utilisant un compte enregistré dans Azure AD. Lancez Microsoft Edge et connectez-vous à : `<https://myapps.microsoft.com>`.

Le navigateur web doit afficher les applications Azure AD pour l'utilisateur.

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



Vérifiez que le fait de cliquer sur l'icône vous redirige vers un serveur StoreFront authentifié.

De même, vérifiez que les connexions directes utilisant l'URL d'authentification unique et une connexion directe au site Citrix Gateway vous redirigent vers Microsoft Azure et inversement.

Enfin, vérifiez que les machines non jointes à Azure AD fonctionnent également avec les mêmes URL (bien qu'il y aura une seule connexion explicite à Azure AD pour la première connexion).

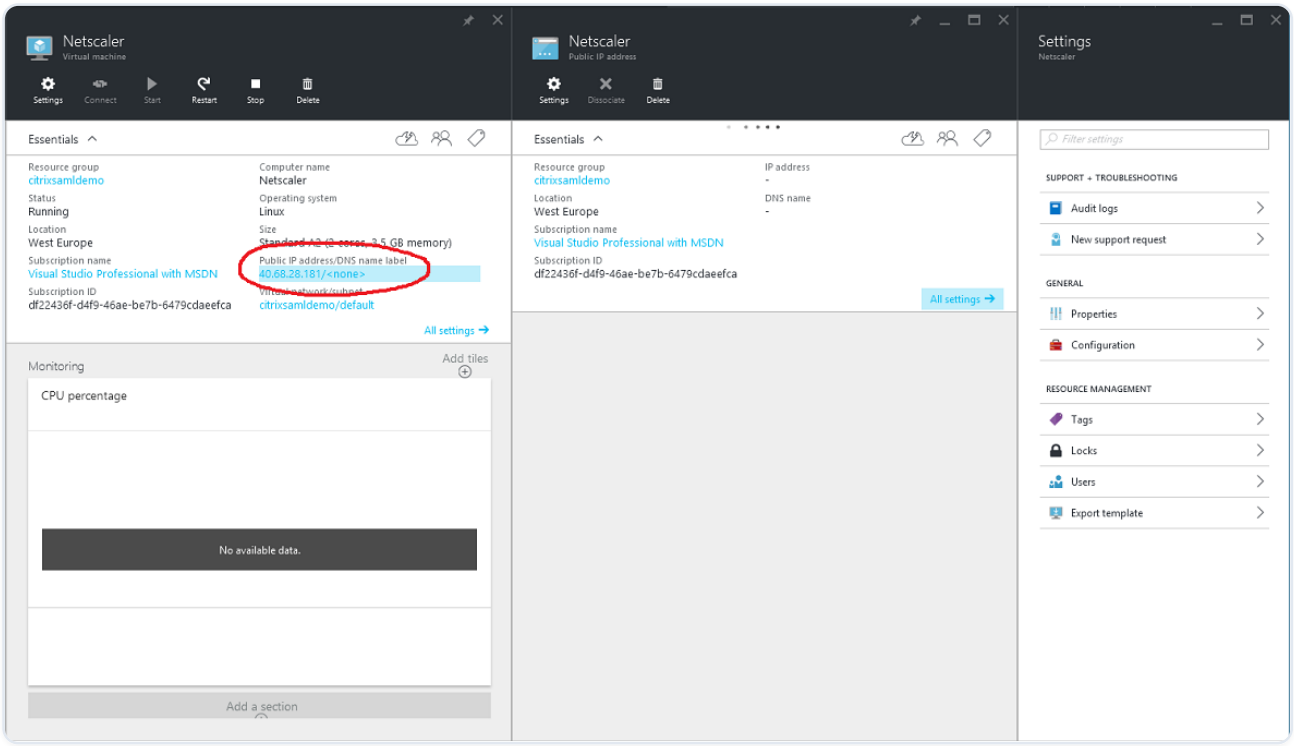
Annexe

Vous devez configurer les options standard suivantes lorsque vous configurez une machine virtuelle dans Azure.

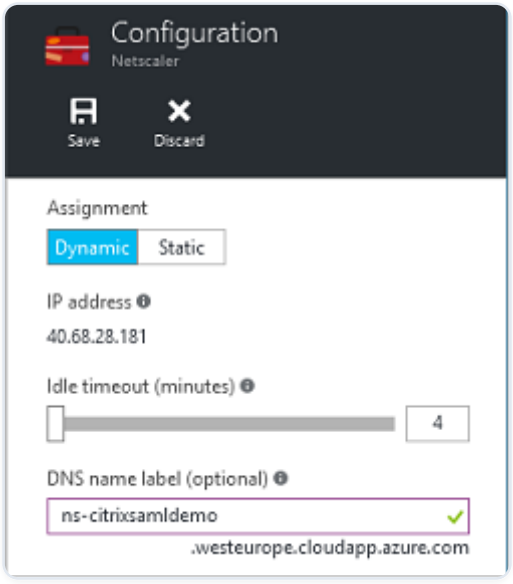
Fournir une adresse IP publique et une adresse DNS

Azure attribue à toutes les machines virtuelles une adresse IP sur le sous-réseau interne (10.*.*.* dans cet exemple). Par défaut, une adresse IP publique est également fournie, qui peut être référencée par une étiquette DNS mise à jour dynamiquement.

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



Sélectionnez **Configuration** de l'**adresse IP publique/étiquette de nom DNS**. Choisissez une adresse DNS publique pour la machine virtuelle. Celle-ci peut être utilisée pour les références CNAME dans d'autres fichiers de zone DNS, garantissant que tous les enregistrements DNS continuent de pointer correctement vers la machine virtuelle, même si l'adresse IP est réattribuée.



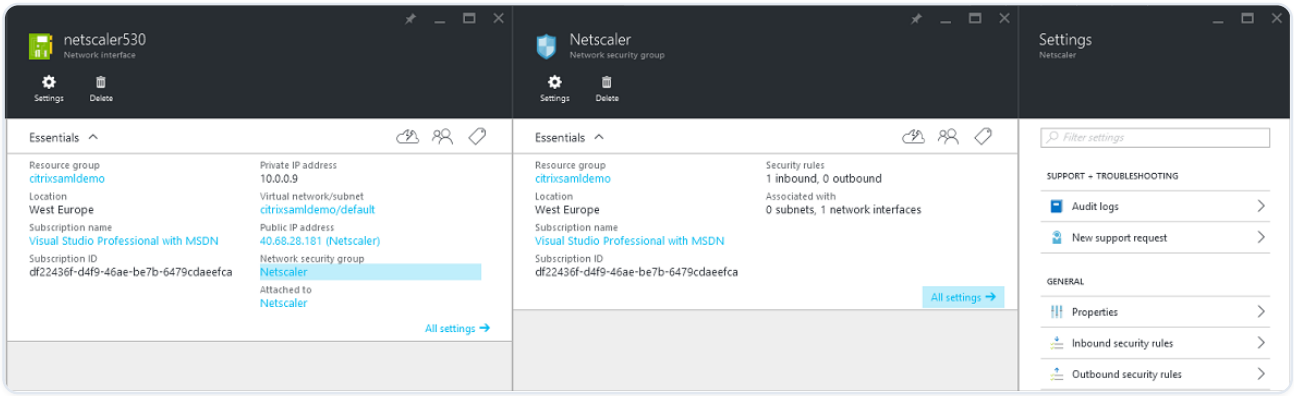
Configurer les règles de pare-feu (groupe de sécurité)

Chaque machine virtuelle dans un cloud dispose d'un ensemble de règles de pare-feu appliquées automatiquement, appelé groupe de sécurité. Le groupe de sécurité contrôle le trafic transféré de l'adresse IP publique vers l'adresse IP privée. Par défaut, Azure autorise le transfert RDP vers

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

toutes les machines virtuelles. Les serveurs Citrix Gateway et ADFS doivent également transférer le trafic TLS (443).

Ouvrez **Interfaces réseau** pour une machine virtuelle, puis cliquez sur l'étiquette **Groupe de sécurité réseau**. Configurez les **Règles de sécurité entrantes** pour autoriser le trafic réseau approprié.



Informations associées

- Installer et configurer est la référence principale pour l'installation et la configuration de FAS.
- Les déploiements FAS courants sont résumés dans l'article Architectures de déploiement.
- Les articles « Comment faire » sont présentés dans l'article Configuration avancée.

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

Historique des documents du service d'authentification fédérée 2206

Le tableau suivant décrit les modifications importantes apportées à la documentation du service d'authentification fédérée 2206. Pour recevoir des notifications concernant ces mises à jour, abonnez-vous au flux RSS.

DATE	MODIFICATION	DESCRIPTION
13 Jun 2022	Version initiale du service d'authentification fédérée 2206	Version initiale du service d'authentification fédérée 2206. Pour plus d'informations, consultez Nouveautés.

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