Installez et configurez le fournisseur de l'identité F5 (IDP) pour la gestion d'identité de Cisco (id) pour activer SSO

Contenu

Introduction

Ce document décrit la configuration sur le fournisseur d'identité F5 BIG-IP (IDP) pour activer simple se connectent (SSO).

Modèles de déploiement d'id de Cisco

Produit	Déploiement
UCCX	Co-résident
PCCE	Co-résident avec CUIC (centre d'intelligence de Cisco Unified) et LD (données vivantes)
UCCE	Co-résident avec CUIC et LD pour les déploiements 2k. Autonome pour les déploiements 4k et 12k.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Version 11.6 de version 11.6 ou de Cisco Unified Contact Center Enterprise du Cisco Unified Contact Center Express (UCCX) ou version 11.6 emballée du Contact Center Enterprise (PCCE) comme applicable.

Note: Ce document met en référence la configuration en ce qui concerne le service de Cisco Identitify (id) et le fournisseur d'identité (IDP). Le document met en référence UCCX dans les captures d'écran et les exemples, toutefois la configuration est semblable en ce qui concerne le service de Cisco Identitify (UCCX/UCCE/PCCE) et l'IDP.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Installez

Le Grand-IP est une solution emballée qui a de plusieurs caractéristiques. Accédez au Policy Manager (APM) qui Co-associe au service de fournisseur d'identité.

Grand-IP comme APM :

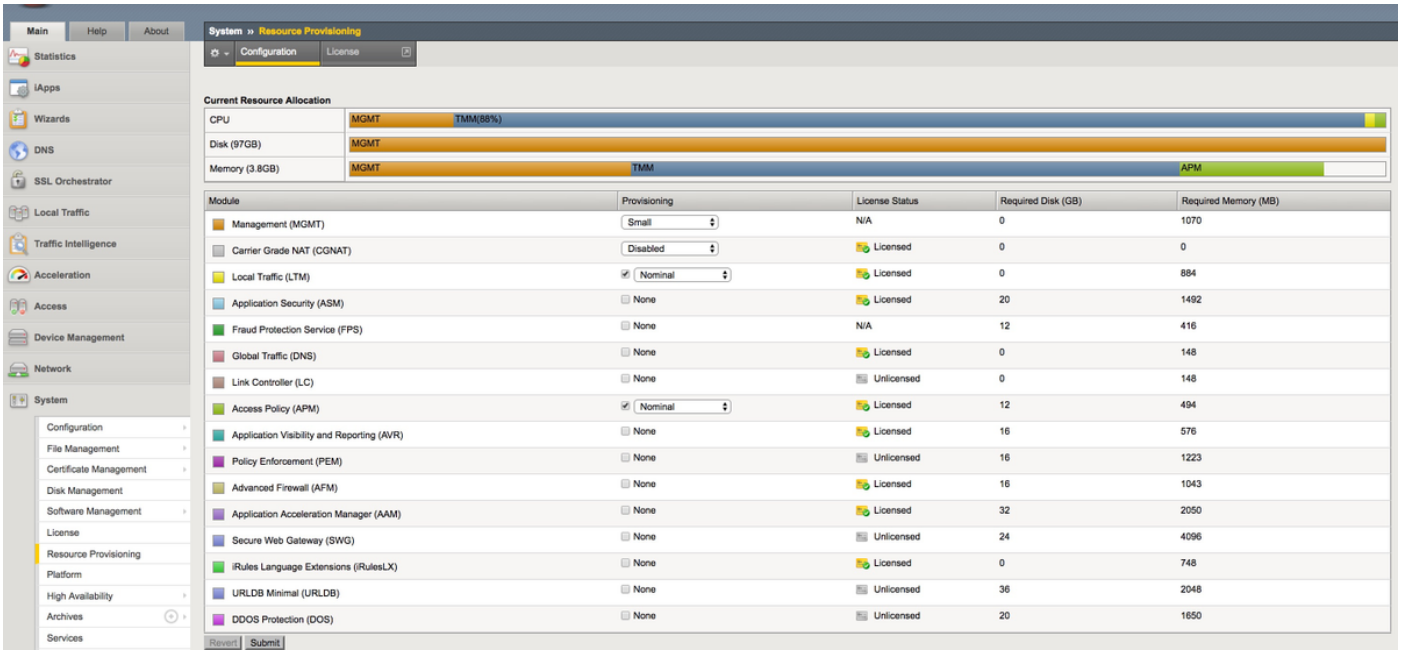
Version 13.0	
Type	Edition(OVA) virtuel
IPS	Deux IPS dans les différents sous-réseaux. Un pour l'IP de Gestion et un pour le serveur virtuel d'IDP

Téléchargez l'image virtuelle d'édition du site Web Grand-IP et déployez les OVULES pour créer un virtual machine (VM) qui est préinstallé. Obtenez le permis et l'installez avec les exigences de base.

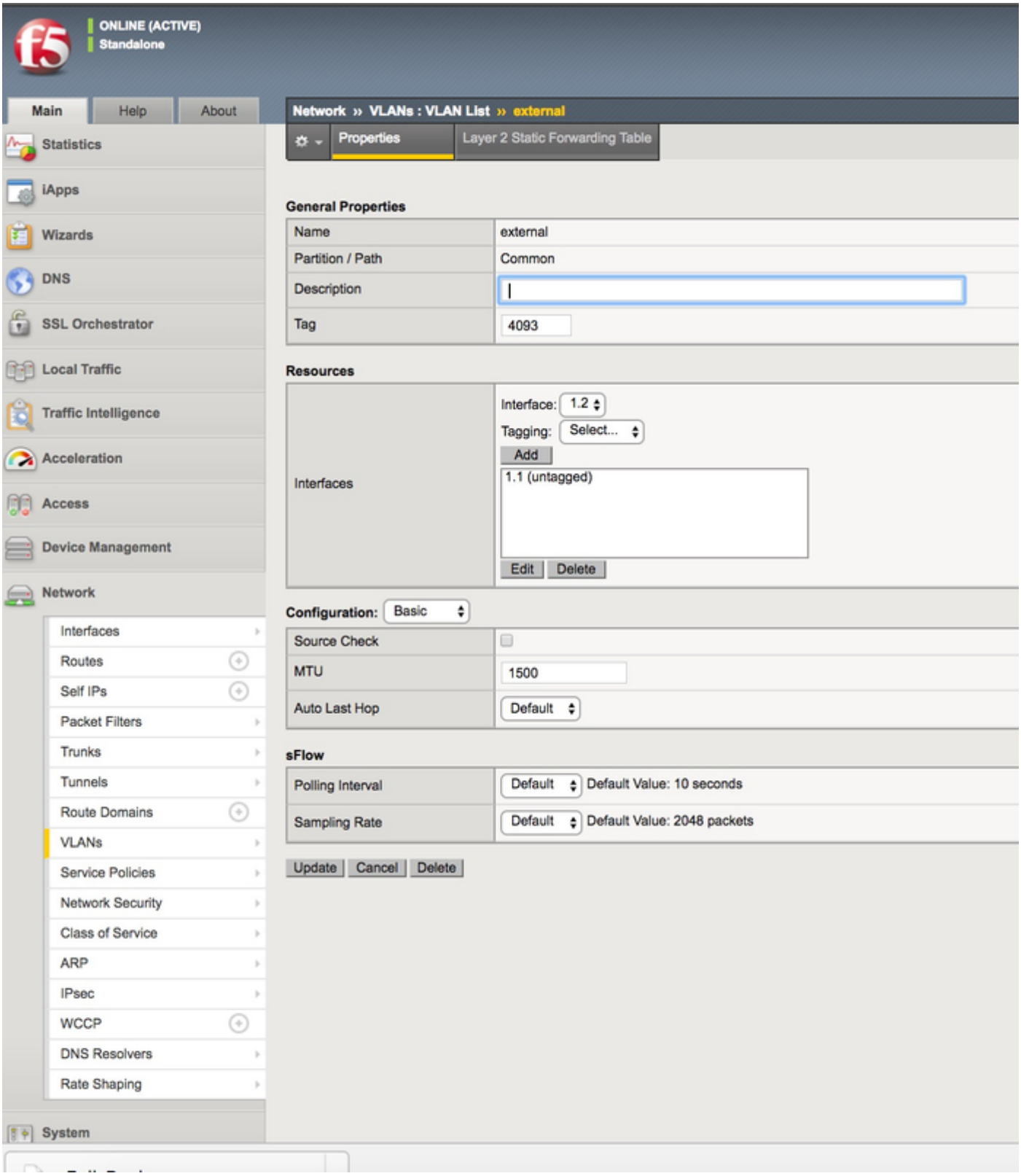
Note: Pour les informations d'installation, référez-vous au guide d'installation Grand-IP.

Configurer

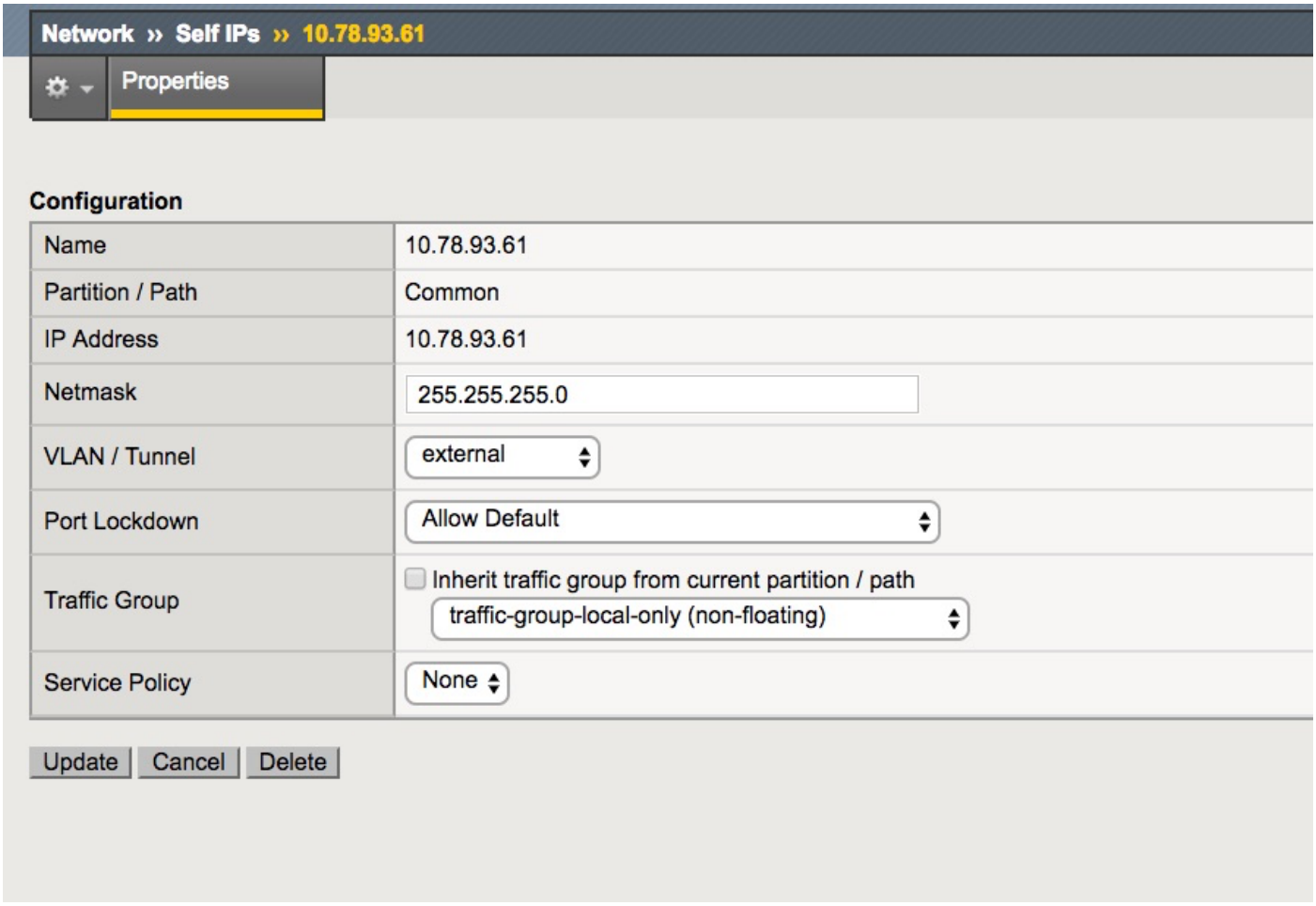
- Naviguez vers le ravitaillement de ressource et activez la **stratégie d'Access**, placez le ravitaillement au **nominal**



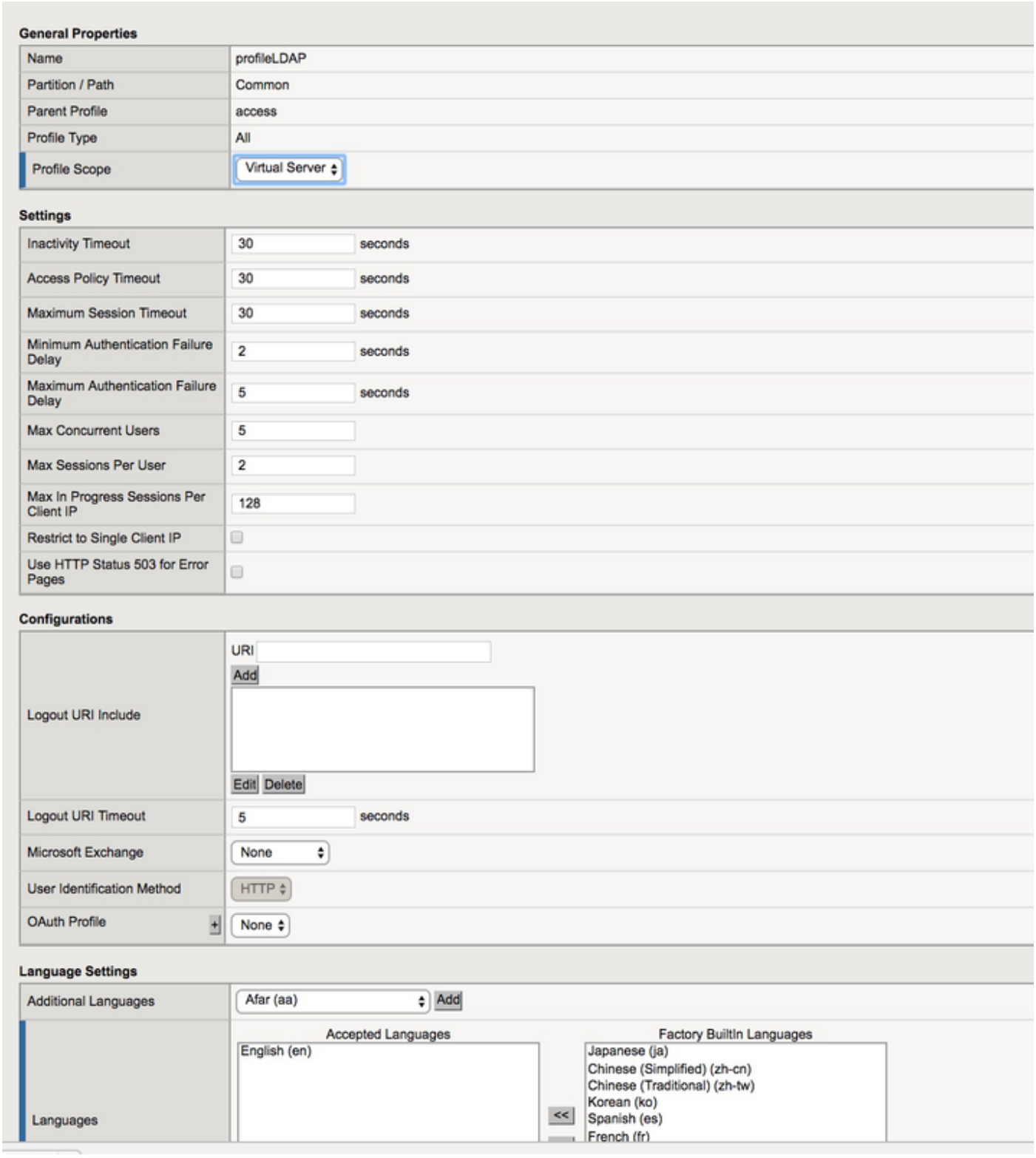
- Créez un nouveau VLAN sous le **réseau** - > des **VLAN**



- Créez une nouvelle entrée pour l'IP qui est utilisé pour l'IDP sous le **réseau - > l'individu IPS**



- Créez un profil sous **Access** - > **profil/stratégies** - > des **profils d'Access**

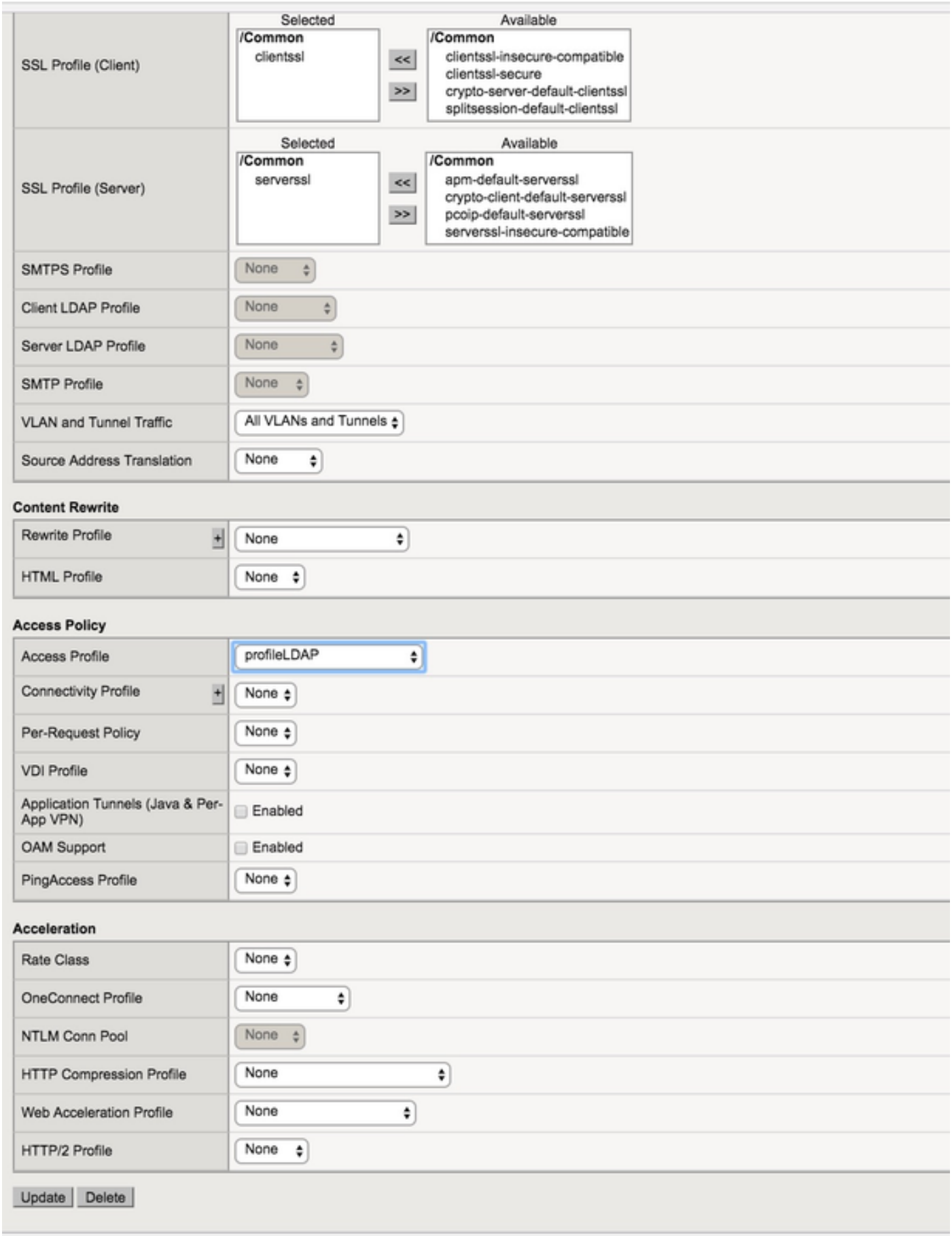


- Créez un serveur virtuel

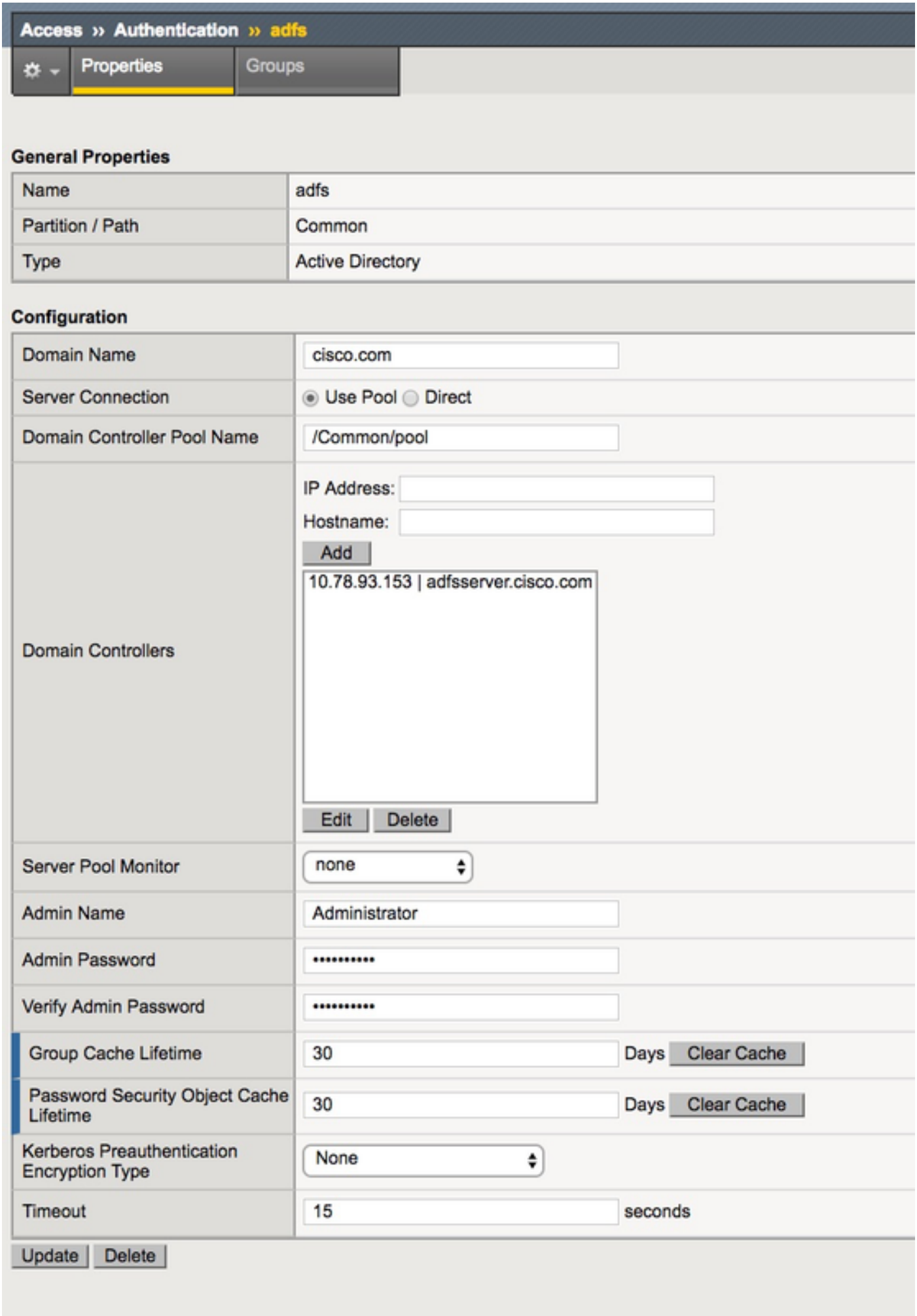
General Properties

Name	ldp_Test
Partition / Path	Common
Description	
Type	Standard
Source Address	0.0.0.0/0
Destination Address/Mask	10.78.93.62
Service Port	443 HTTPS
Notify Status to Virtual Address	☑
Availability	Unknown (Enabled) - The children pool member(s) either don't have service checking enabled, or service check results are not available yet
Syncookie Status	Off
State	Enabled

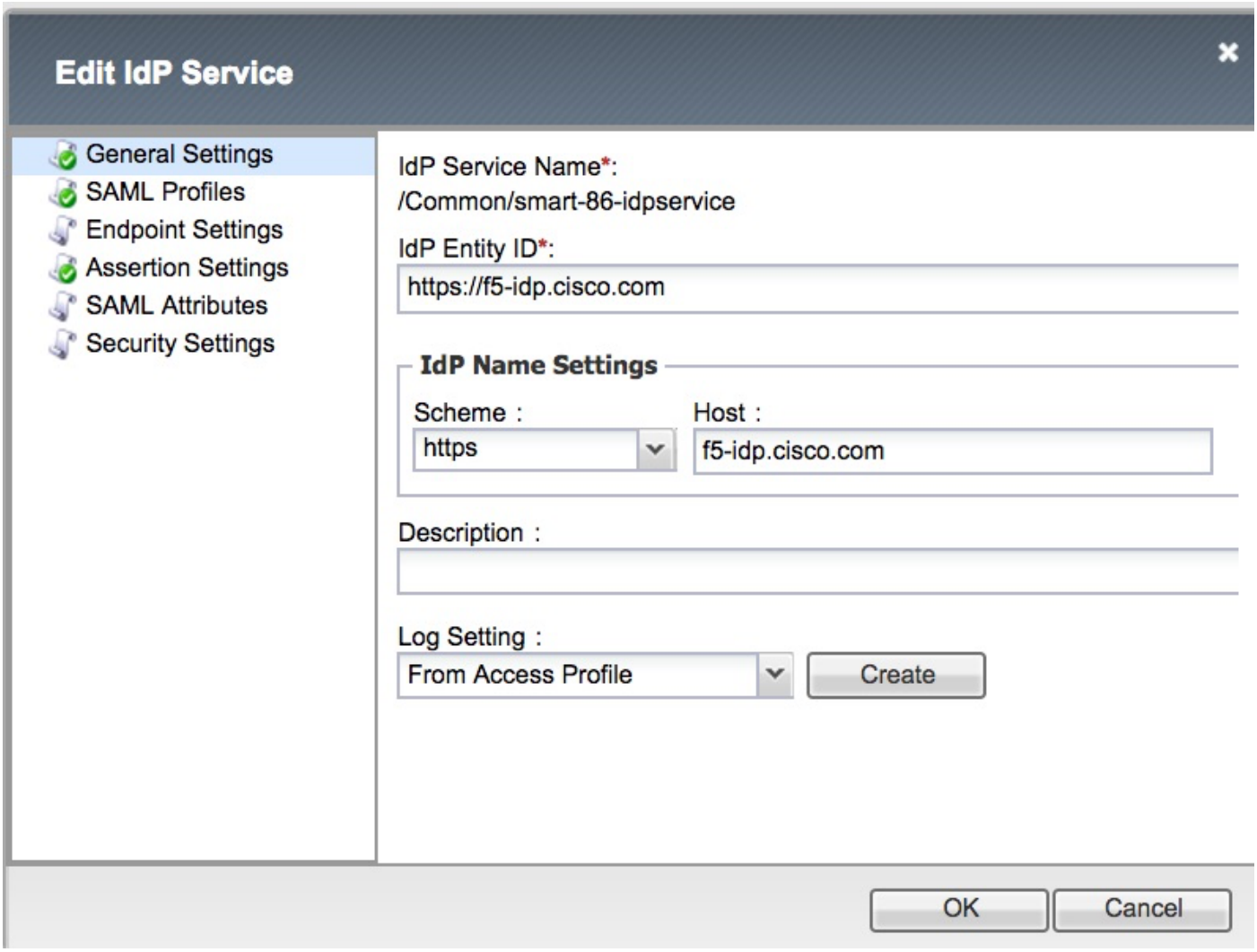
Configuration: Basic

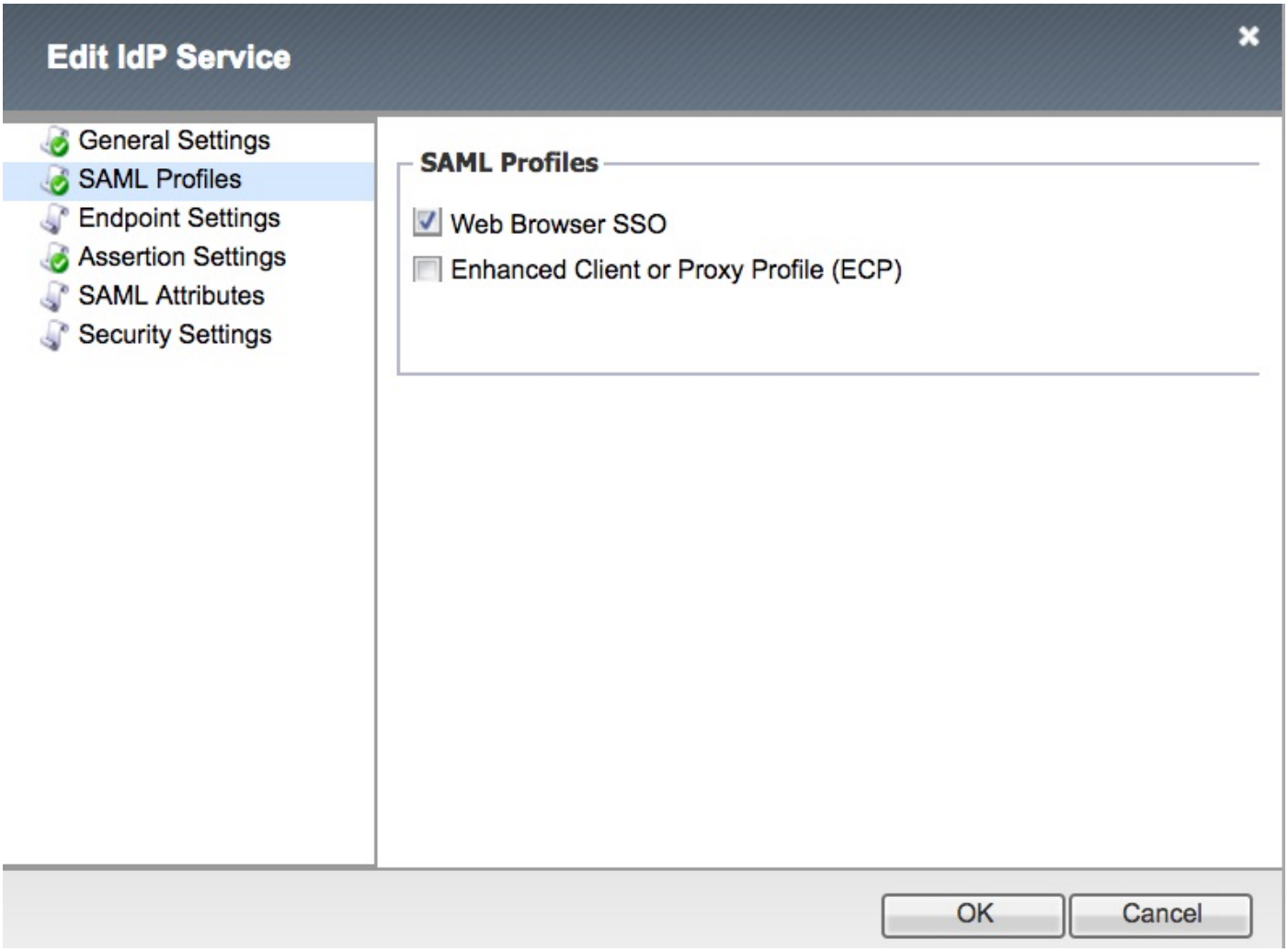


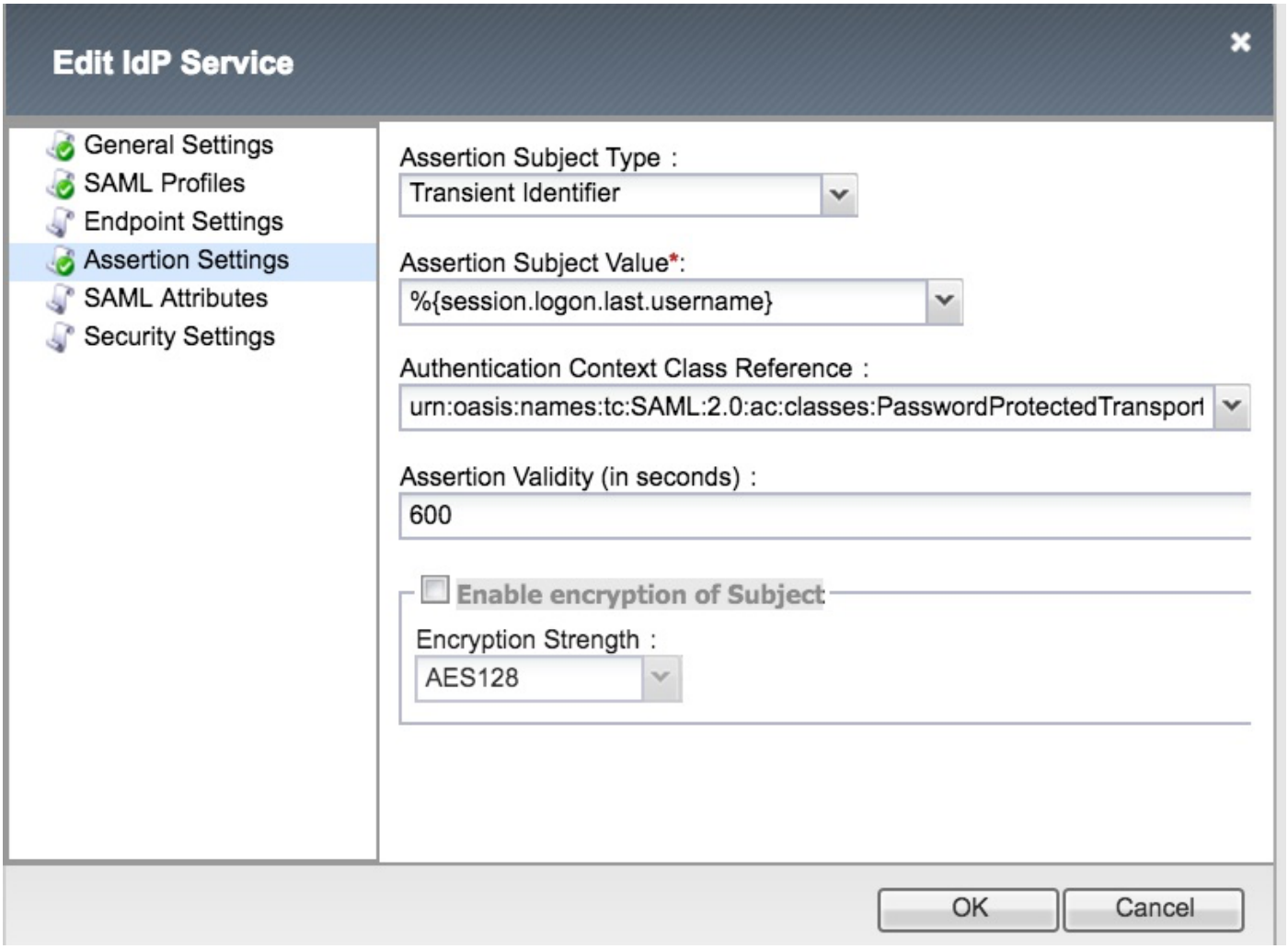
- Ajoutez les détails de Répertoire actif (AD) sous **Access** - > **authentification** - > **Répertoire actif**


Access » Authentication » adfs
Properties
Groups
General Properties
Name
adfs
Partition / Path
Common
Type
Active Directory
Configuration
Domain Name
cisco.com
Server Connection
Use Pool
Direct
Domain Controller Pool Name
/Common/pool
Domain Controllers
IP Address:
Hostname:
Add
10.78.93.153 | adfsserver.cisco.com
Edit
Delete
Server Pool Monitor
none
Admin Name
Administrator
Admin Password
Verify Admin Password
Group Cache Lifetime
30
Days
Clear Cache
Password Security Object Cache Lifetime
30
Days
Clear Cache
Kerberos Preauthentication Encryption Type
None
Timeout
15
seconds
Update
Delete

- Créez un nouveau service d'IDP sous **Access - > fédération - > fournisseur d'identité SAML - > des services locaux d'IDP**




Edit IdP Service
General Settings
SAML Profiles
Endpoint Settings
Assertion Settings
SAML Attributes
Security Settings
SAML Profiles
Web Browser SSO
Enhanced Client or Proxy Profile (ECP)
OK
Cancel



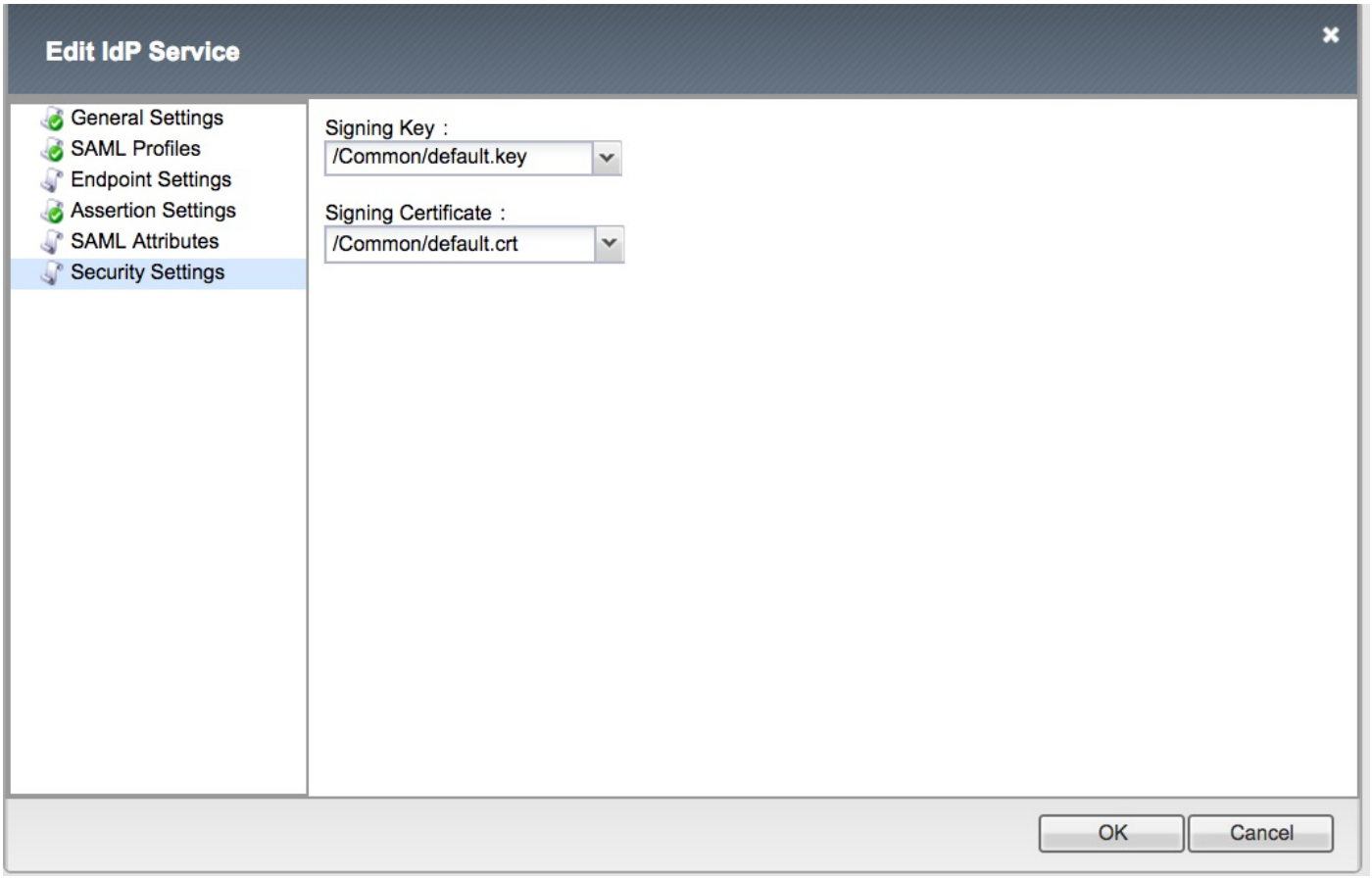
Note: Si une carte d'accès commune (CAC) est utilisée pour l'authentification, ces attributs doivent être ajoutés dans la section de configuration d'**attributs SAML** :

Étape 1. Créez l'attribut d'**uid.**

Nom : uid
Valeur : % {session.ldap.last.attr.sAMAccountName}

Étape 2. Créez l'attribut **user_principal**.

Nom : user_principal
Valeur : % {session.ldap.last.attr.userPrincipalName}

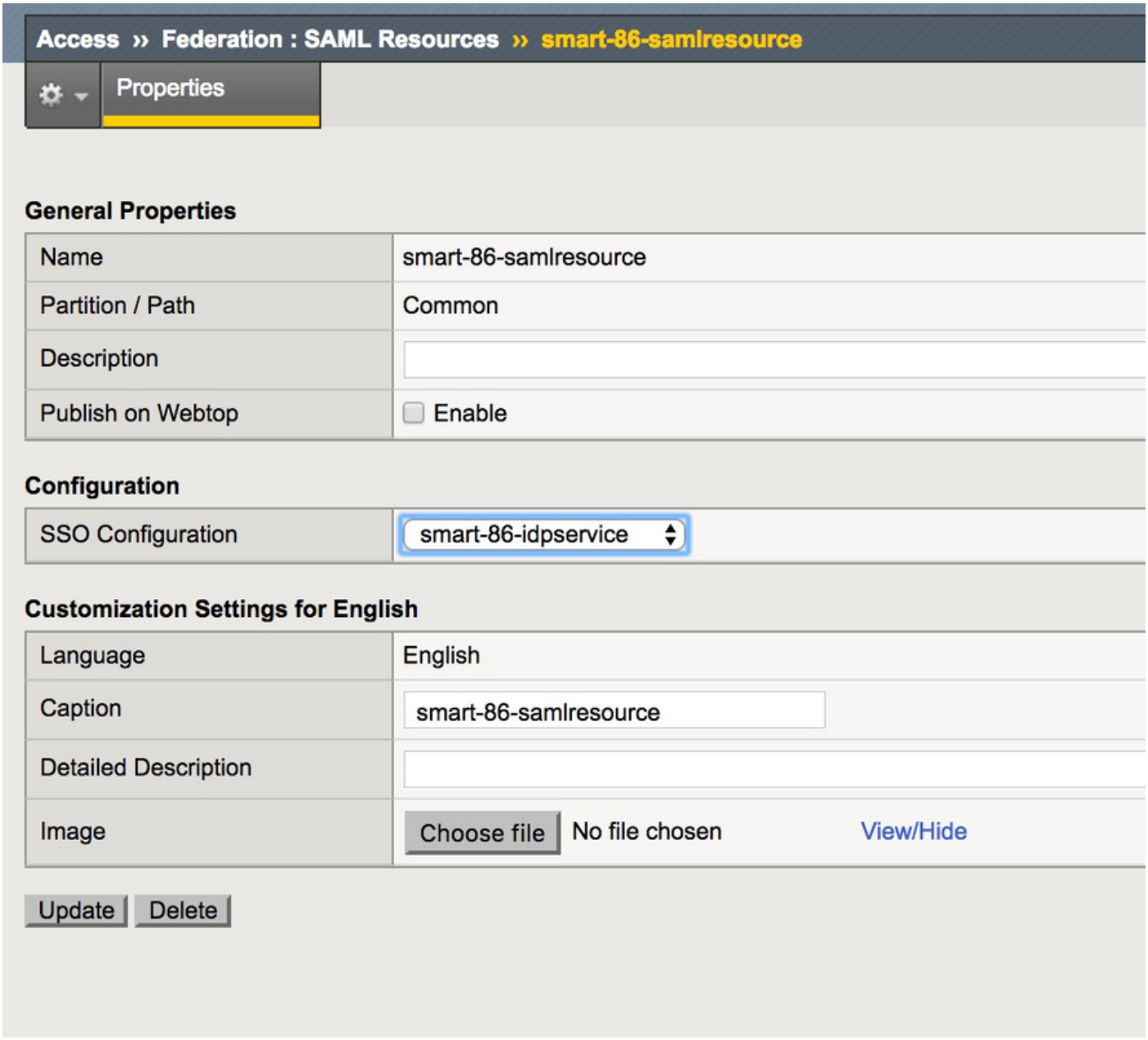


Note: Une fois que le service d'IDP est créé, il y a une option de télécharger les métadonnées avec des **métadonnées d'une exportation de** bouton sous **Access** - > **fédération** - > **fournisseur d'identité SAML** - > des **services locaux d'IDP**

Création du Langage SAML (SAML)

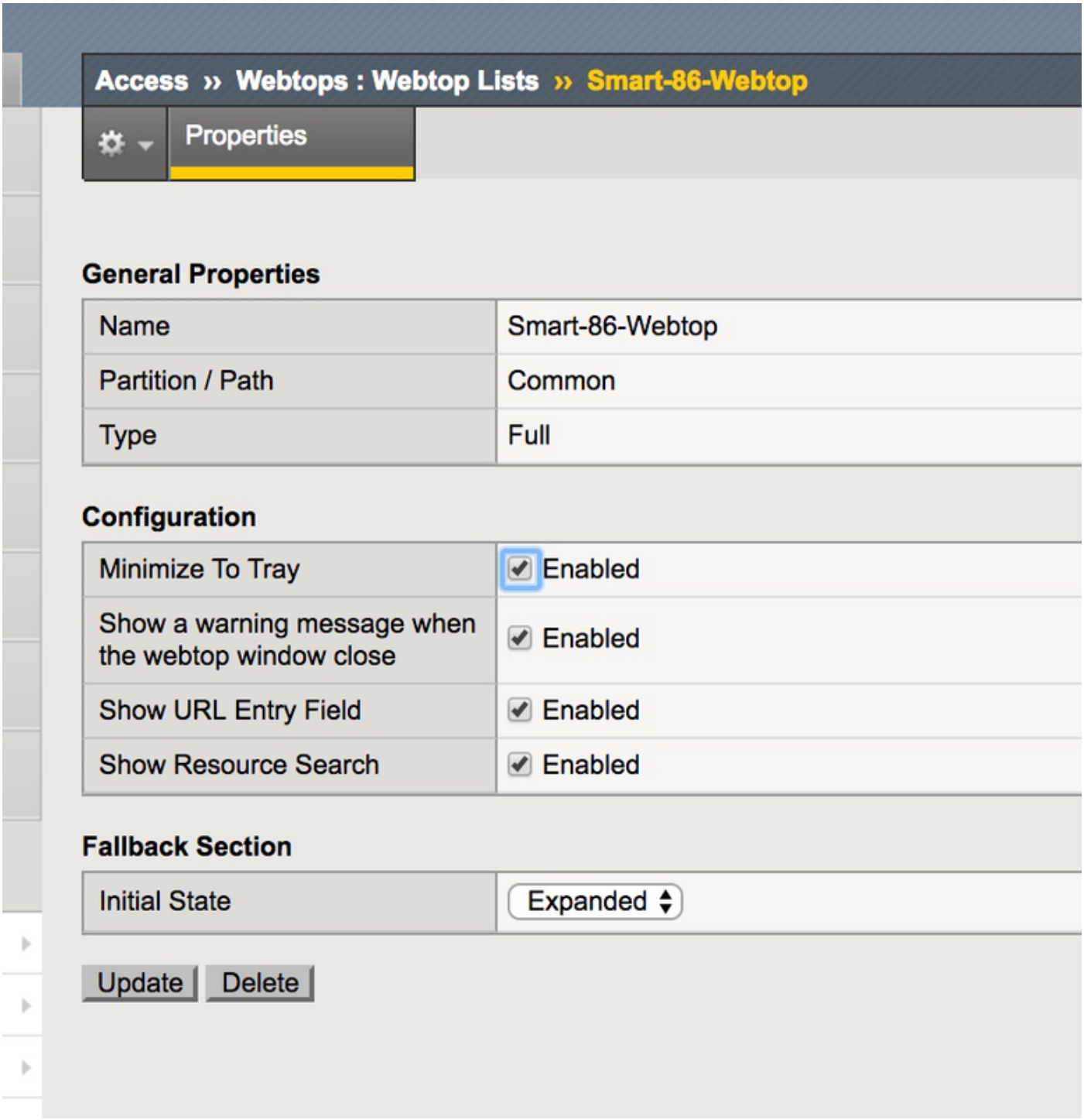
Ressources SAML

- Naviguez **pour accéder à** - > **fédération** - > des **ressources SAML** et pour créer une ressource en saml pour s'associer avec le service d'IDP qui a été créé plus tôt



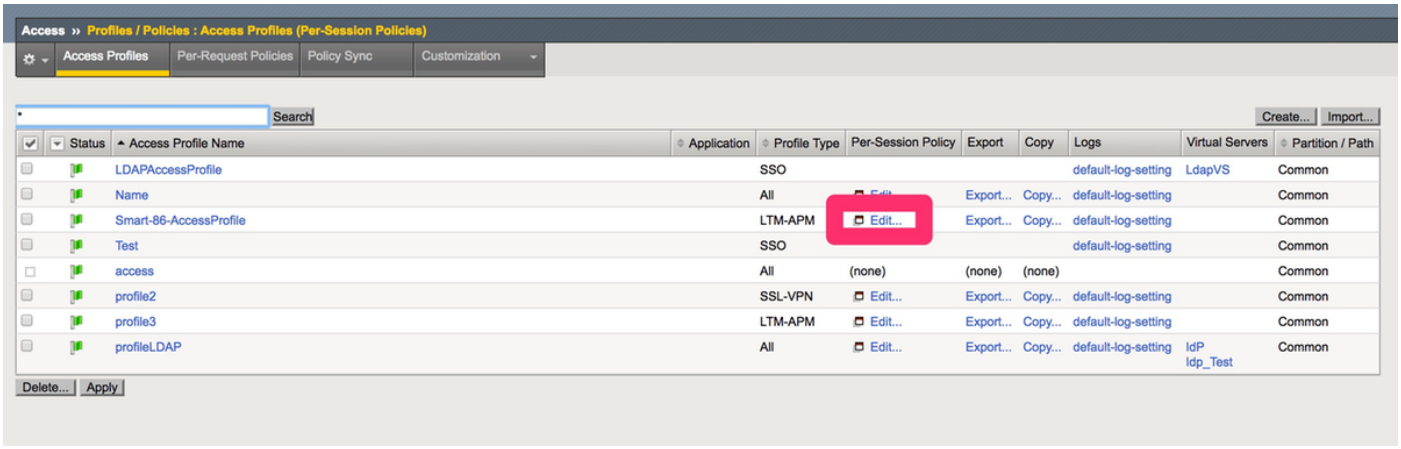
Webtops

- Créez un webtop sous **Access** - > **Webtops**

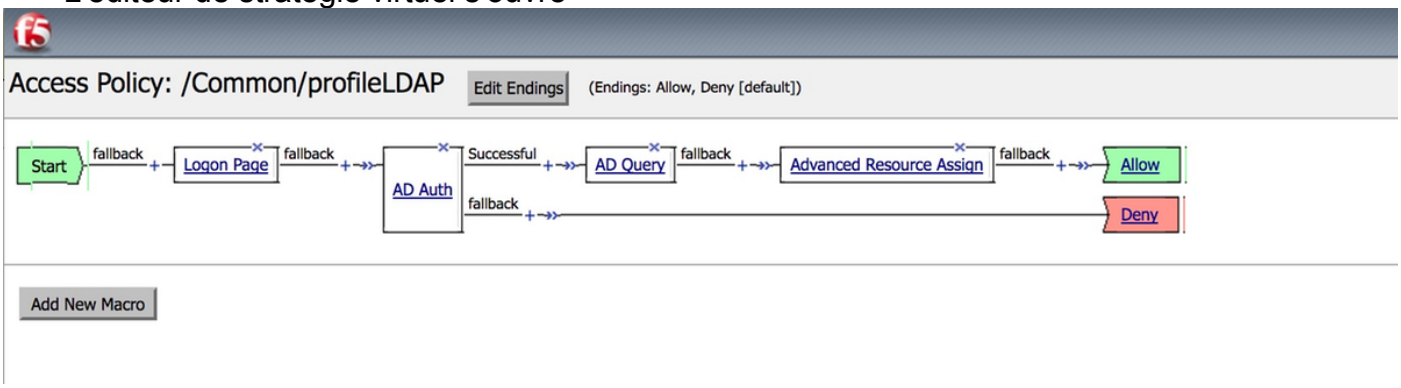


Éditeur de stratégie virtuel

- Naviguez vers la stratégie créée plus tôt et cliquez sur éditent en fonction le lien



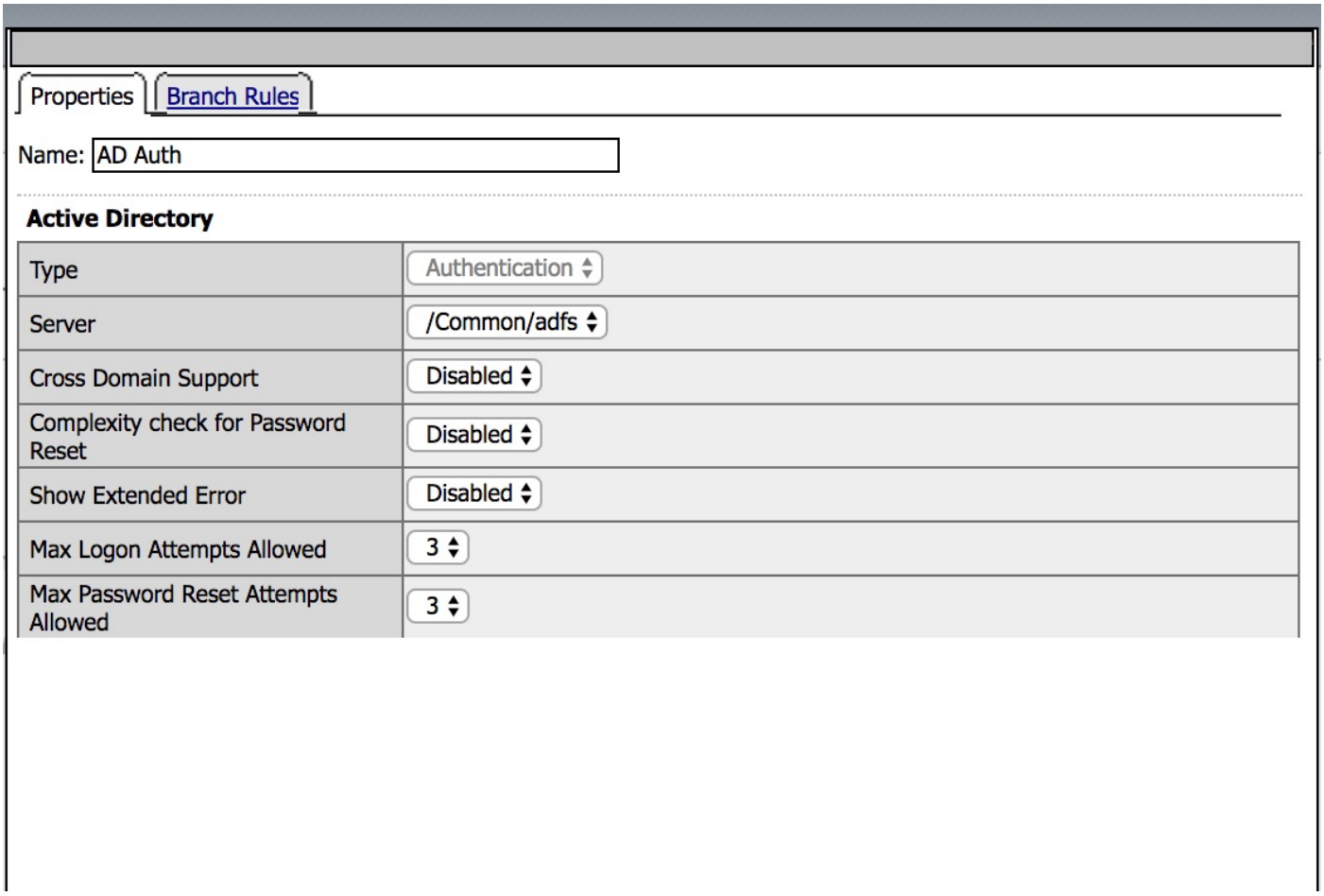
- L'éditeur de stratégie virtuel s'ouvre



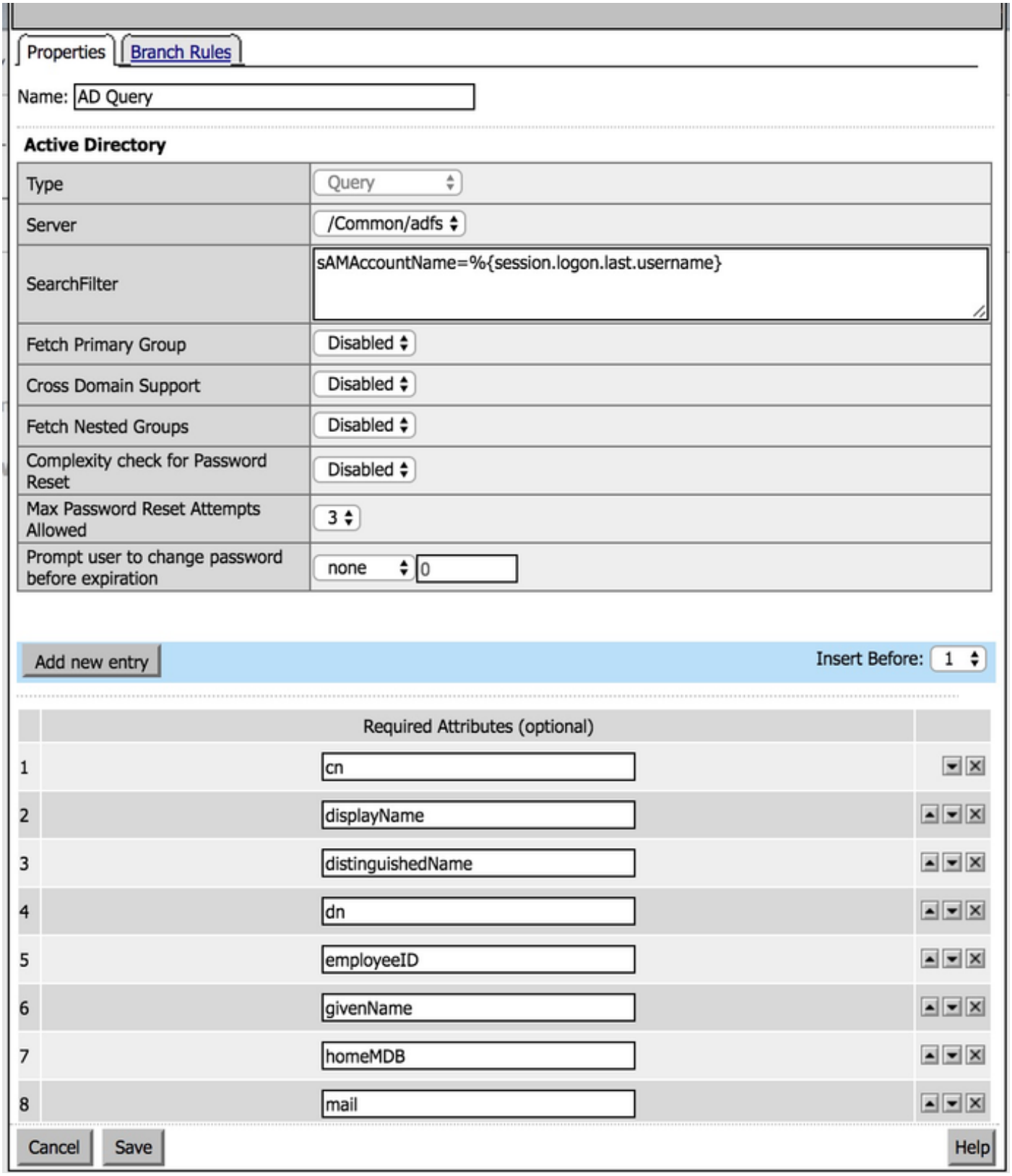
- Cliquez sur en fonction l'icône et ajoutez les éléments comme décrit

Étape 1. **Élément de page de connexion** - Laissez tous les éléments pour se transférer.

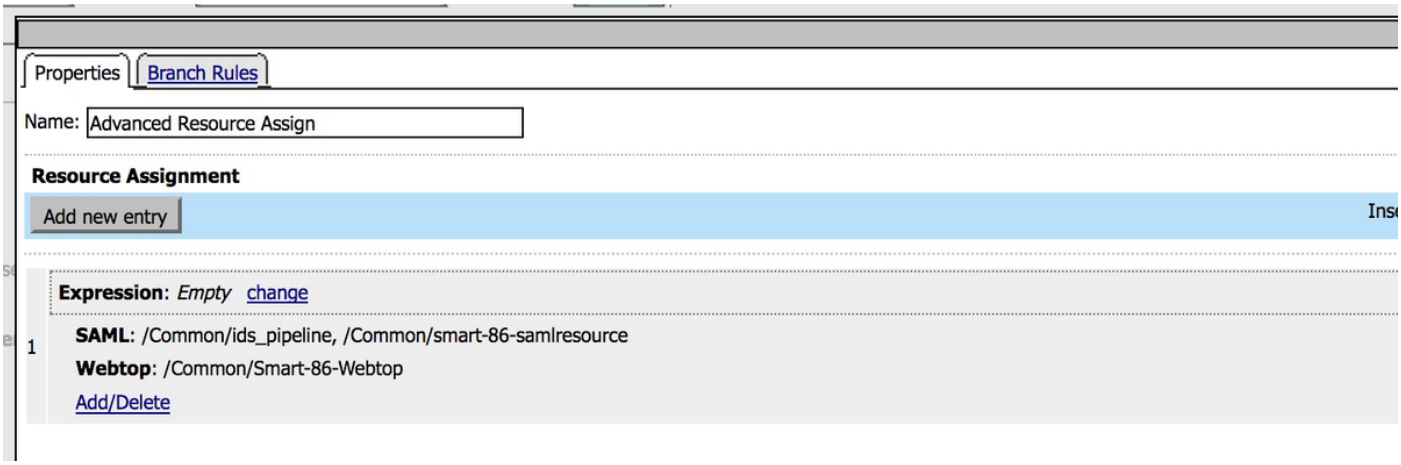
Étape 2. **AD authentique** - > choisissez la configuration ADFS créée plus tôt.



Étape 3. **Élément de requête d'AD** - Assignez les détails nécessaires.



Étape 4. **La ressource anticipée assignent - Associez la ressource en saml et le webtop créés plus tôt.**



Échange de métadonnées de fournisseur de services (fournisseur de services)

- Importez manuellement le certificat des id au Grand-IP par le **système** - > **Gestion de certificat** - > **gestion de trafic**

  Note: Assurez-vous que le certificat se compose COMMENCENT des balises de CERTIFICAT et de CERTIFICAT d'EXTRÉMITÉ.

General Properties

Name	smart88crt.crt
Partition / Path	Common
Certificate Subject(s)	smart-88.cisco.com

Certificate Properties

Public Key Type	RSA
Public Key Size	2048 bits
Expires	Nov 17 2019 21:10:10 GMT
Version	3
Serial Number	915349505
Subject	Common Name: smart-88.cisco.com Organization: Division: Locality: State Or Province: Country:
Issuer	Self
Email	
Subject Alternative Name	

Import... Export... Delete

- Créez une nouvelle entrée de sp.xml sous le **fournisseur d'**Access-> Federation-> SAMLIDENTITY **- > des connecteurs d'**ExternalSP
- Liez le connecteur de fournisseur de services au service d'IDP sous **Access** - **> fédération** - **> fournisseur d'identité SAML** - > des **services locaux d'IDP**

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépanner

Échec d'authentification commun de la carte d'accès (CAC)

Si l'authentification SSO échoue pour des utilisateurs CAC, vérifiez l'UCCX ids.log pour vérifier les attributs SAML ont été placés correctement.

S'il y a une question de configuration, une panne SAML se produit. Par exemple, dans cet extrait de log, l'attribut user_principal SAML n'est pas configuré sur l'IDP.

Hh YYYY-MM-DD : millimètre : ERREUR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:465 SS.sss GMT(-0000) [IdSEndPoints-SAML-59] - Ne pourrait pas la **carte d'attributs de** retrievefrom **: user_principal**
Hh YYYY-MM-DD : millimètre : ERREUR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 SS.sss GMT(-0000) [IdSEndPoints-SAML-59] - SAML **responseprocessingfailed à l'exception com.sun.identity.saml.common.SAMLException : N'a pas pu récupérer user_principal de la réponse de saml**
àcom.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributeFromAttributesMap(IdSSAMLAsyncServlet.java:466)
àcom.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet.java:263)
àcom.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServlet.java:176)
àcom.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)
àjava.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
àjava.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
àjava.lang.Thread.run(Thread.java:745)

Informations connexes

- Support et documentation techniques - Cisco Systems