Instale y configure el proveedor de la identidad F5 (IdP) para el servicio de la identidad de Cisco (IdS) para habilitar el SSO

Contenido

Introducción

Este documento describe la configuración en el proveedor de la identidad F5 BIG-IP (IdP) para habilitar la sola muestra encendido (SSO).

Modelos de despliegue del Cisco IDS

Producto	Despliegue
UCCX	Coresidente
PCCE	Coresidente con CUIC (centro unificado Cisco de la inteligencia) y LD (datos vivos)
UCCE	Coresidente con CUIC y el LD para las implementaciones 2k. Independiente para las implementaciones 4k y 12k.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Versión 11.6 del Cisco Unified Contact Center Express (UCCX) o versión 11.6 del Cisco Unified Contact Center Enterprise o versión embalada 11.6 de la empresa del Centro de

contacto (PCCE) como aplicables.

Note: Este documento se refiere a la configuración en cuanto al servicio de Cisco Identitify (IdS) y al proveedor de la identidad (IdP). El documento se refiere a UCCX al screenshots y a los ejemplos, no obstante la configuración es similar en cuanto al servicio de Cisco Identitify (UCCX/UCCE/PCCE) y al IdP.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Instalar

El Grande-IP es una solución embalada que tiene características múltiples. Administrador de la política de acceso (APM) que co-se relaciona con el servicio del proveedor de la identidad.

Grande-IP como APM:

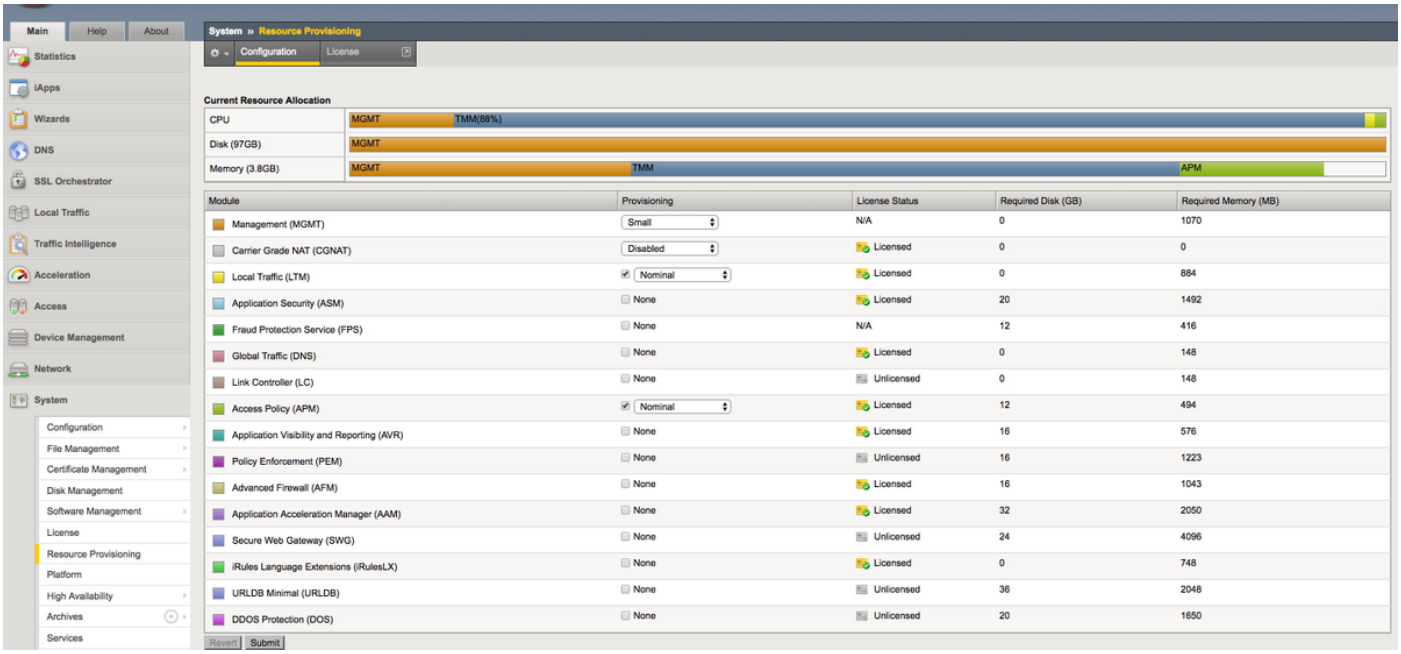
Versión	13.0
Tipo	Edition(OVA) virtual
IP	Dos IP en diversas subredes. Uno para el IP de administración y uno para el servidor virtual de IdP

Descargue la imagen virtual de la edición del sitio web Grande-IP y despliegue los HUEVOS para crear una máquina virtual (VM) se instale previamente que. Obtenga la licencia y instalela con los requisitos básicos.

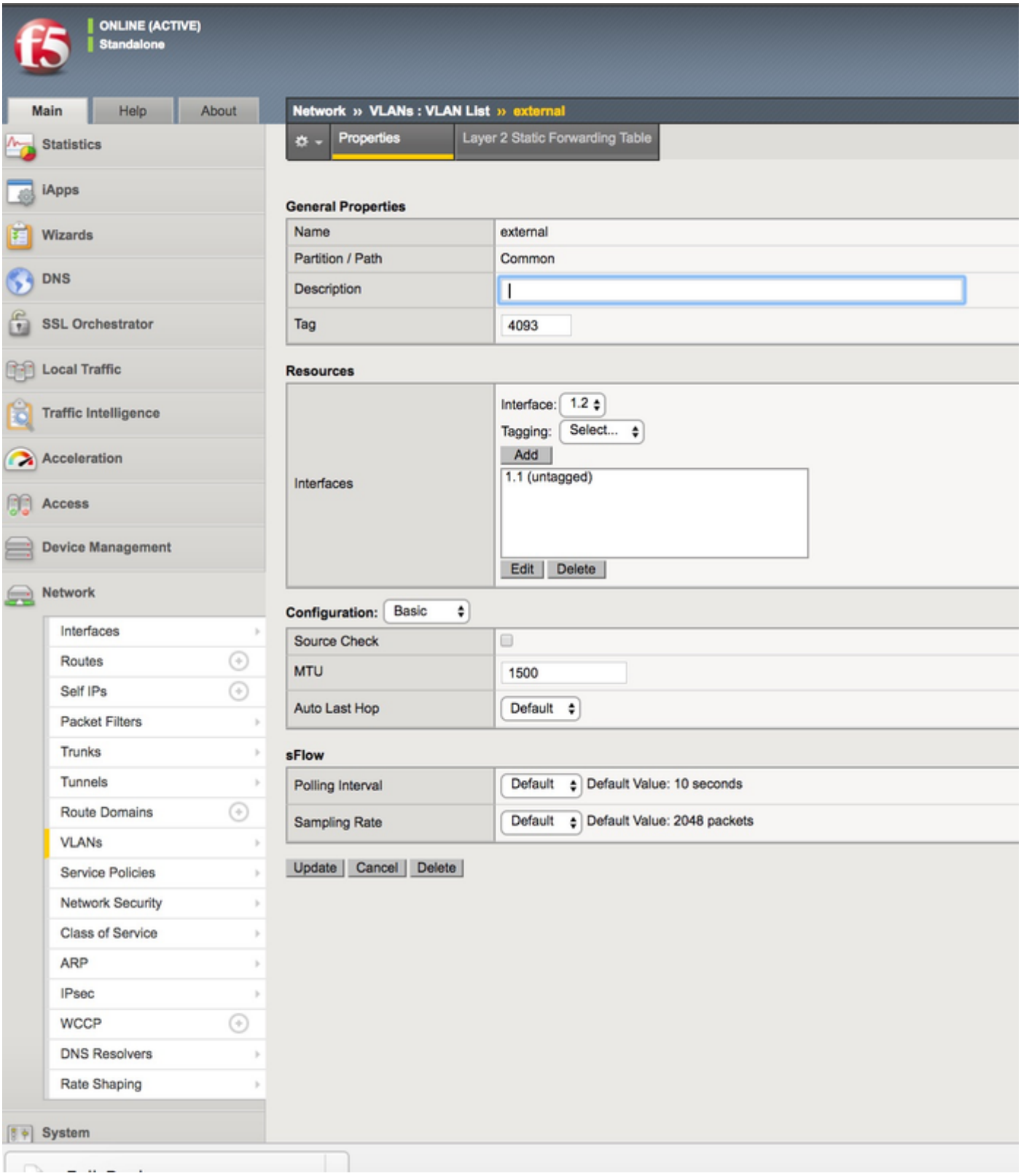
Note: Para la información de la instalación, refiera a la guía de instalación Grande-IP.

Configurar

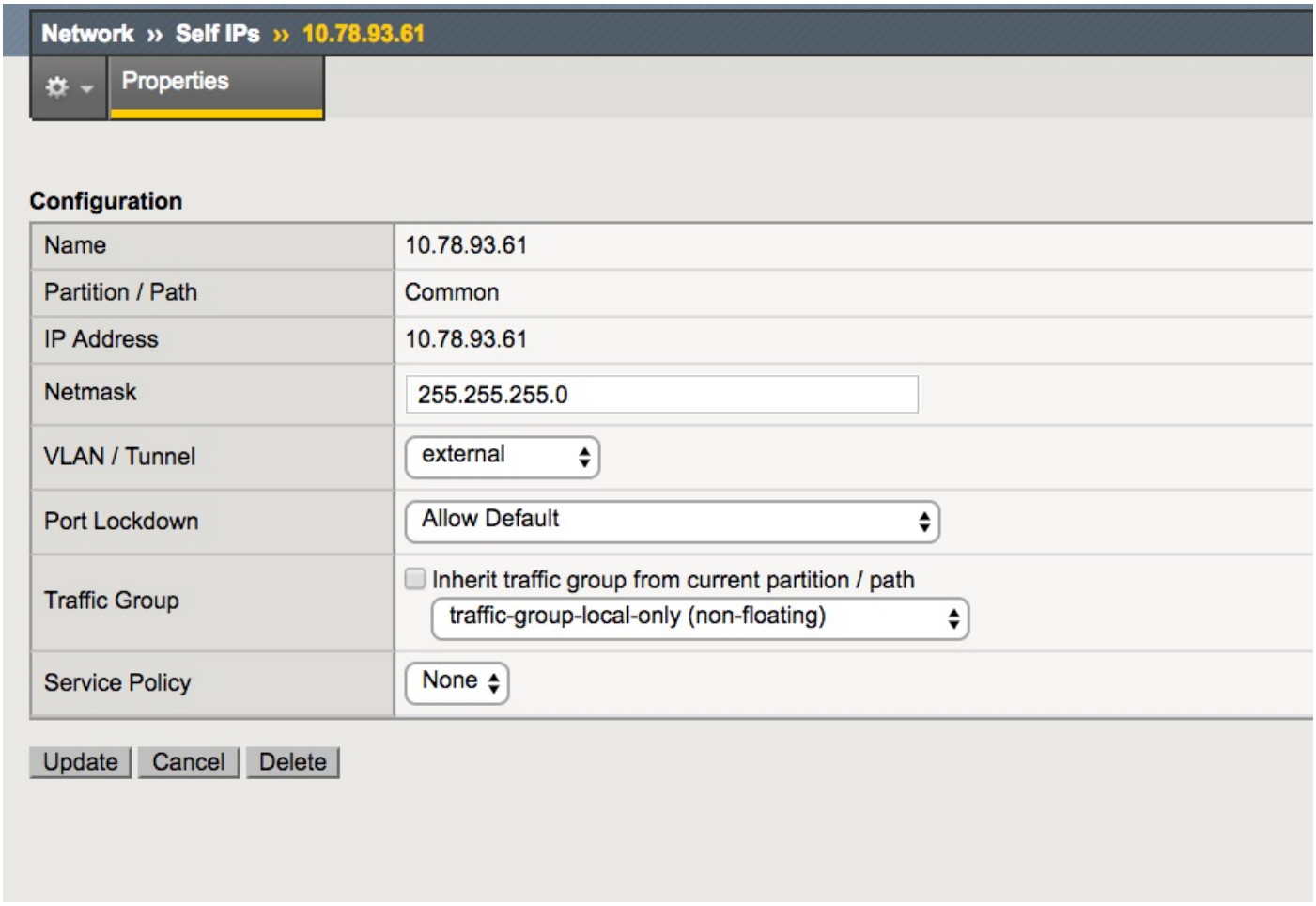
- Navegue al aprovisionamiento del recurso y habilite la **política de acceso**, fije el aprovisionamiento al **nominal**



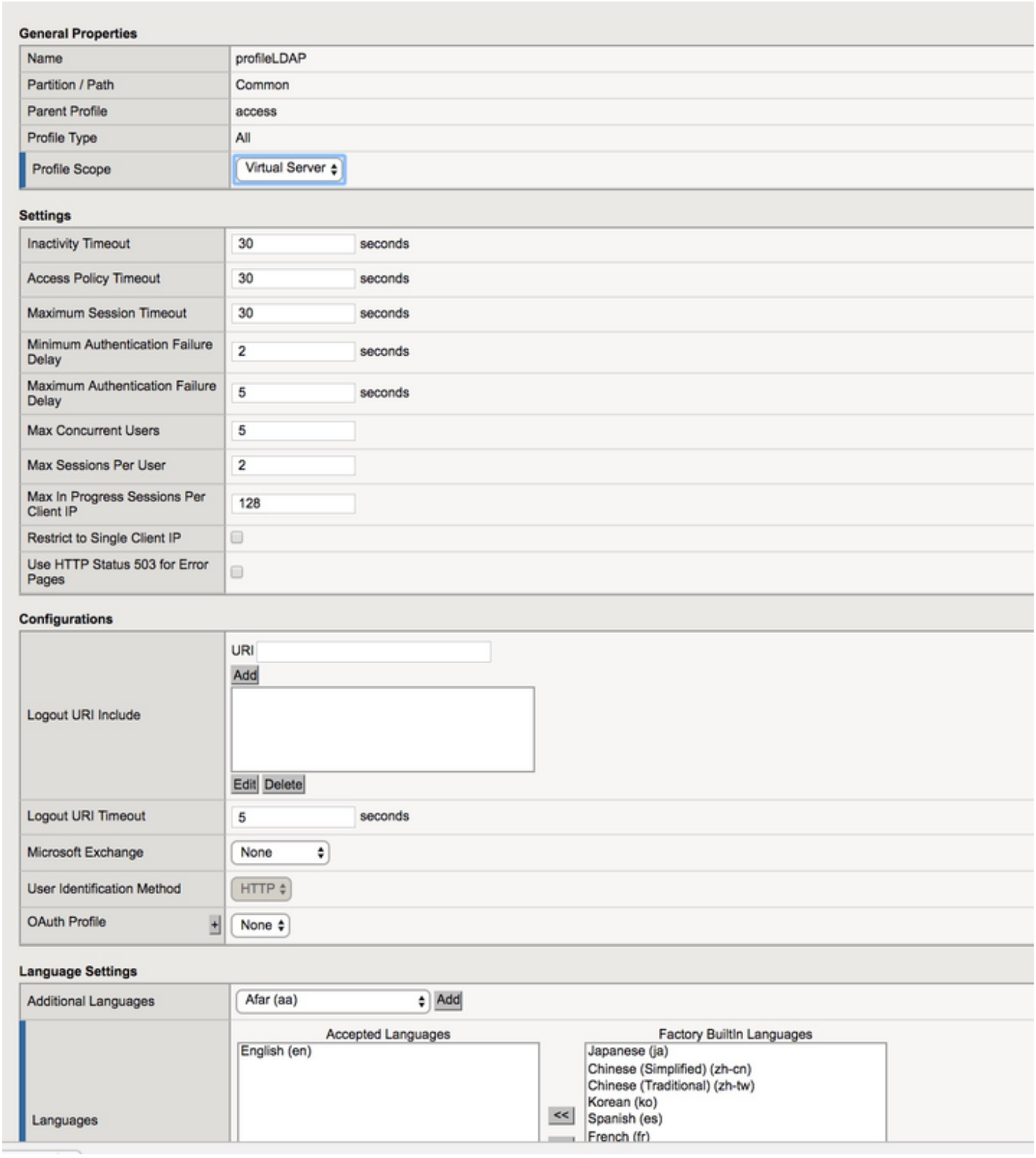
- Cree un nuevo VLA N bajo **red** - > los **VLA N**



- Cree una nueva entrada para el IP que se utiliza para el IdP bajo **red - > el uno mismo IP**



- Cree un perfil bajo **acceso** - **> perfil/las directivas** - > los **perfiles del acceso**

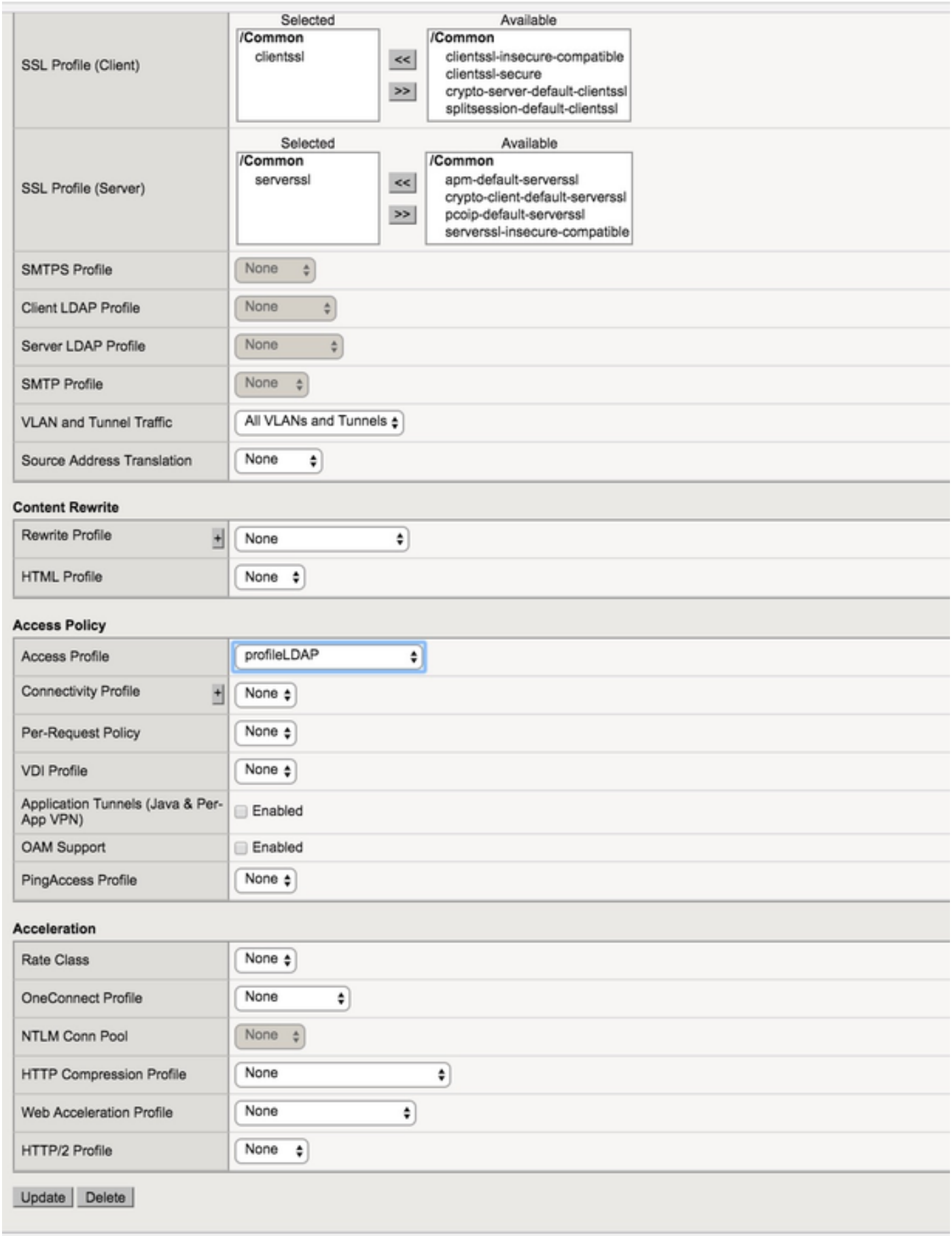


- Cree a un servidor virtual

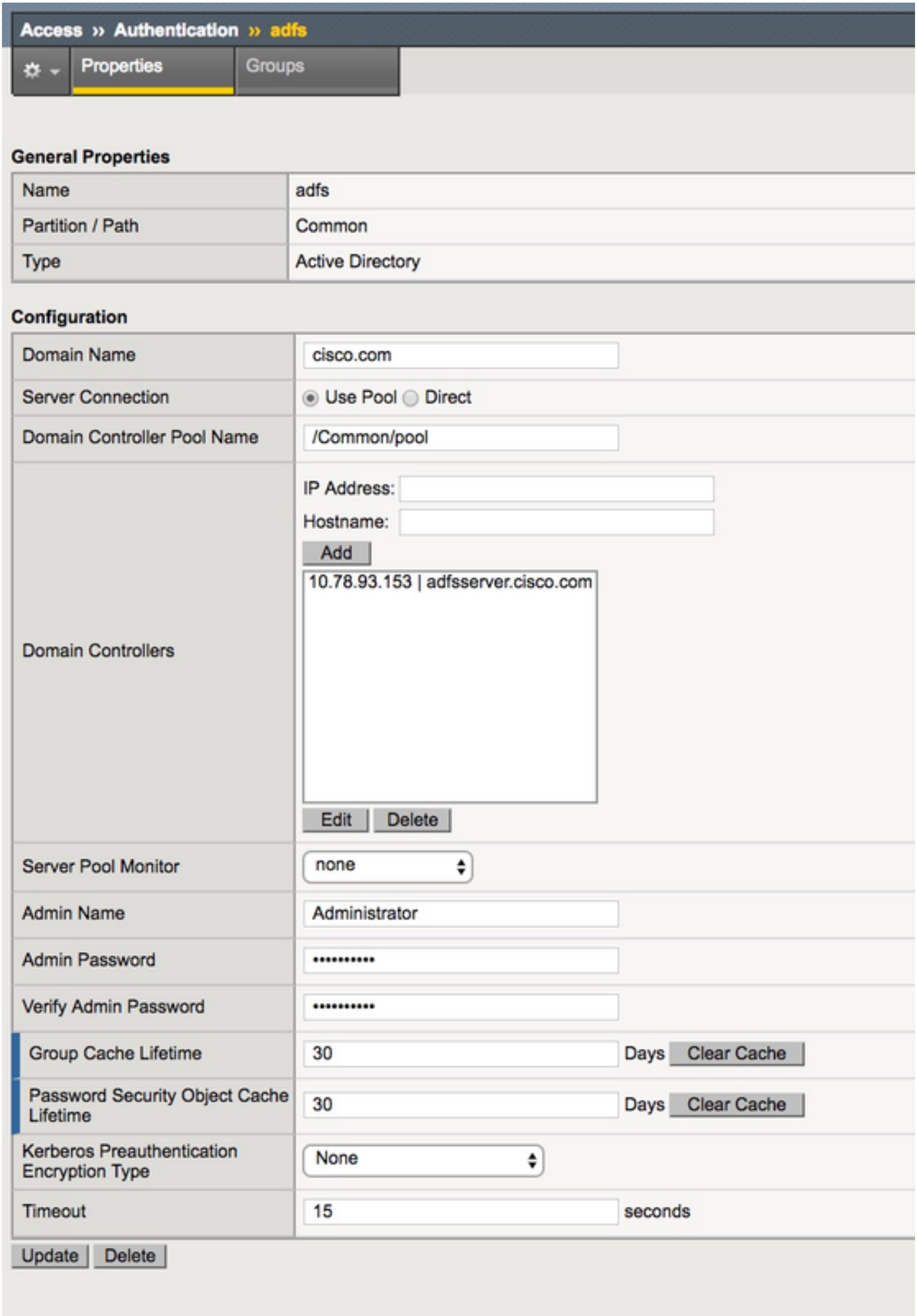
General Properties

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

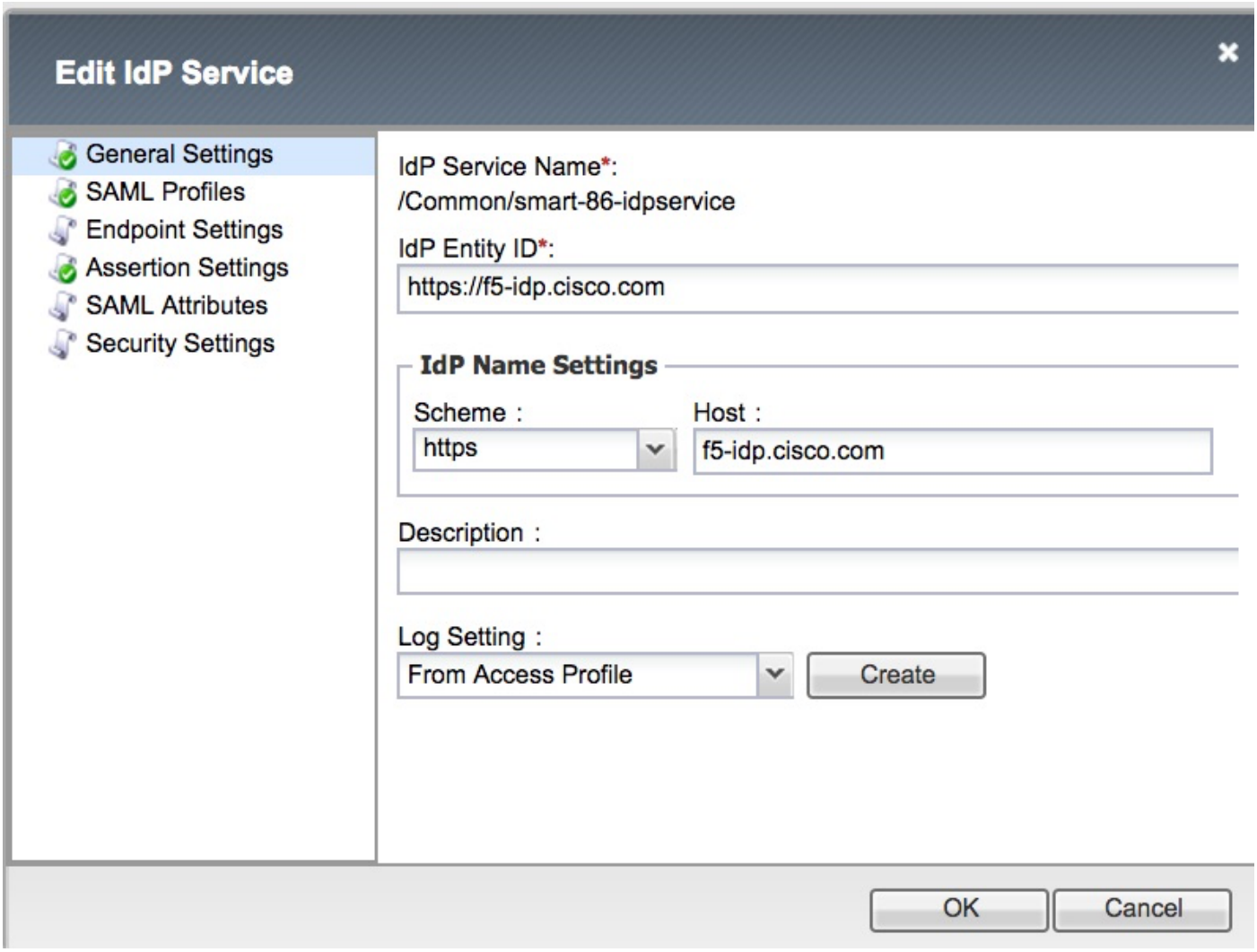
Configuration: Basic

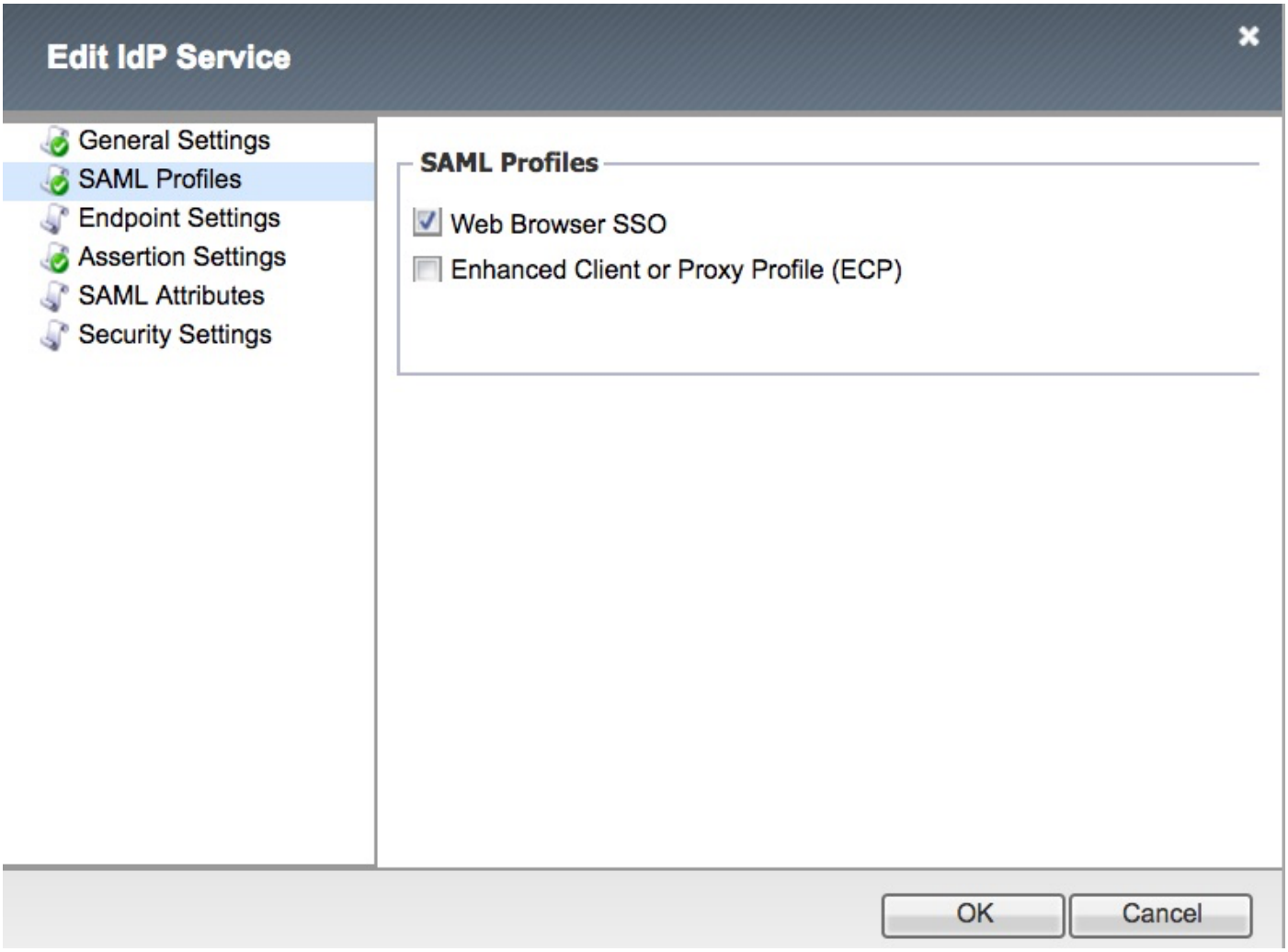


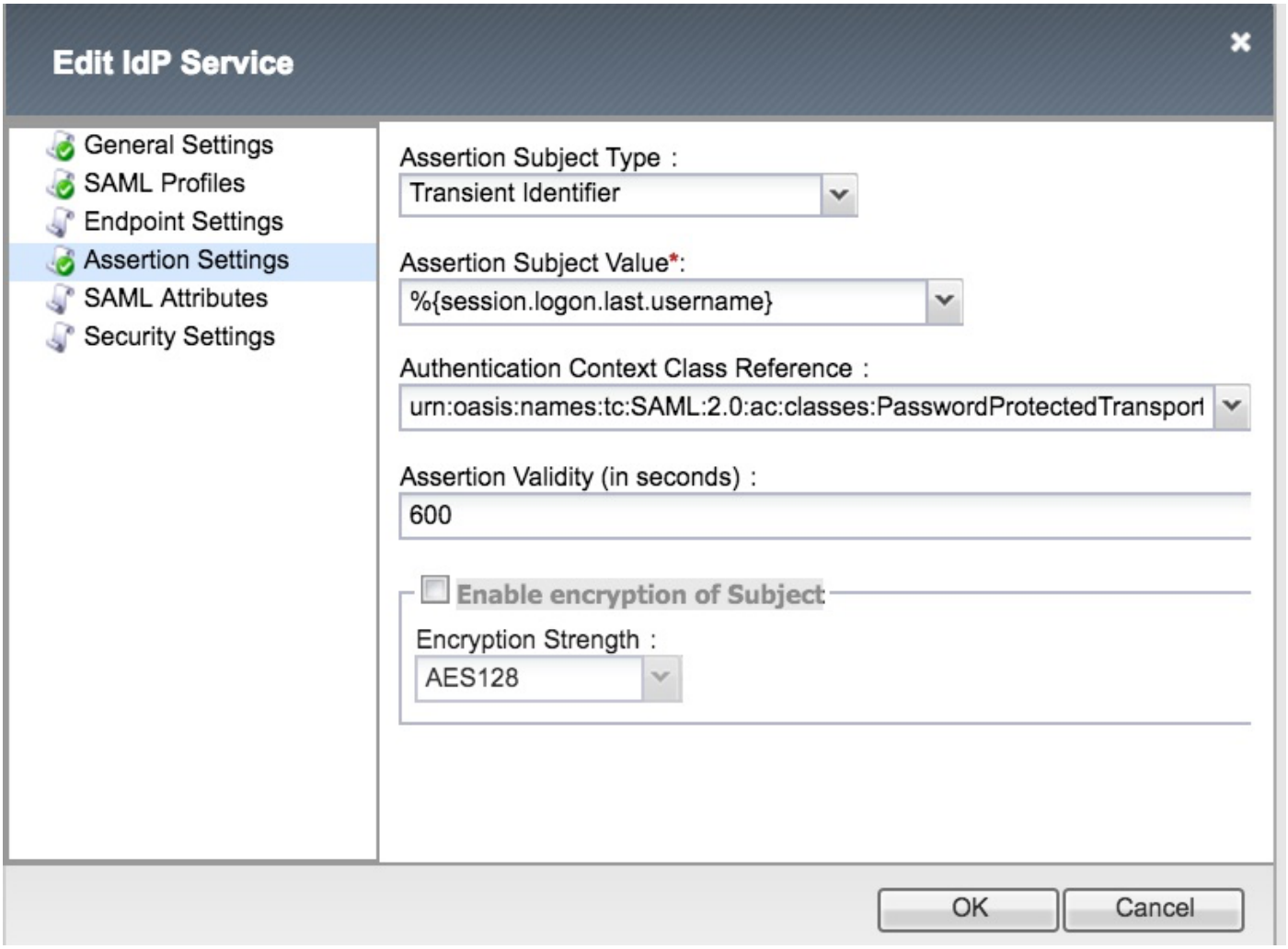
- Agregue los detalles del Active Directory (AD) bajo **acceso** - > **autenticación** - > **Active Directory**


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

- Cree un nuevo servicio de IdP bajo **acceso - > federación - > SAML proveedor de la identidad - > los servicios locales de 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



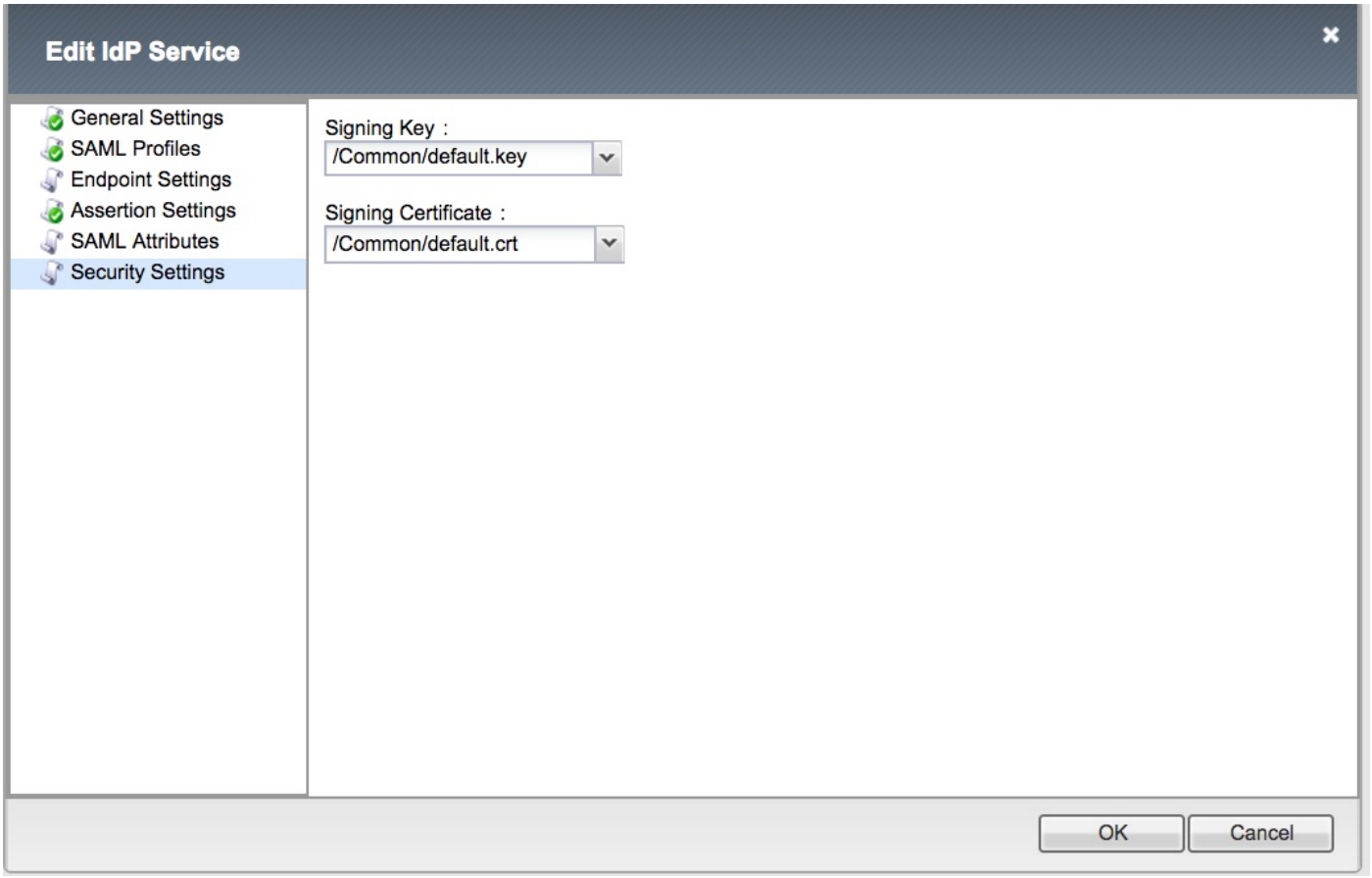
Note: Si un indicador luminoso LED amarillo de la placa muestra gravedad menor común del acceso (CAC) se utiliza para la autenticación, estos atributos necesitan ser agregados en la sección de configuración de los **atributos de SAML**:

Paso 1. Cree el atributo del **uid.**

Nombre: uid
Valor: % {session.ldap.last.attr.sAMAccountName}

Paso 2. Cree el atributo **user_principal**.

Nombre: user_principal
Valor: % {session.ldap.last.attr.userPrincipalName}

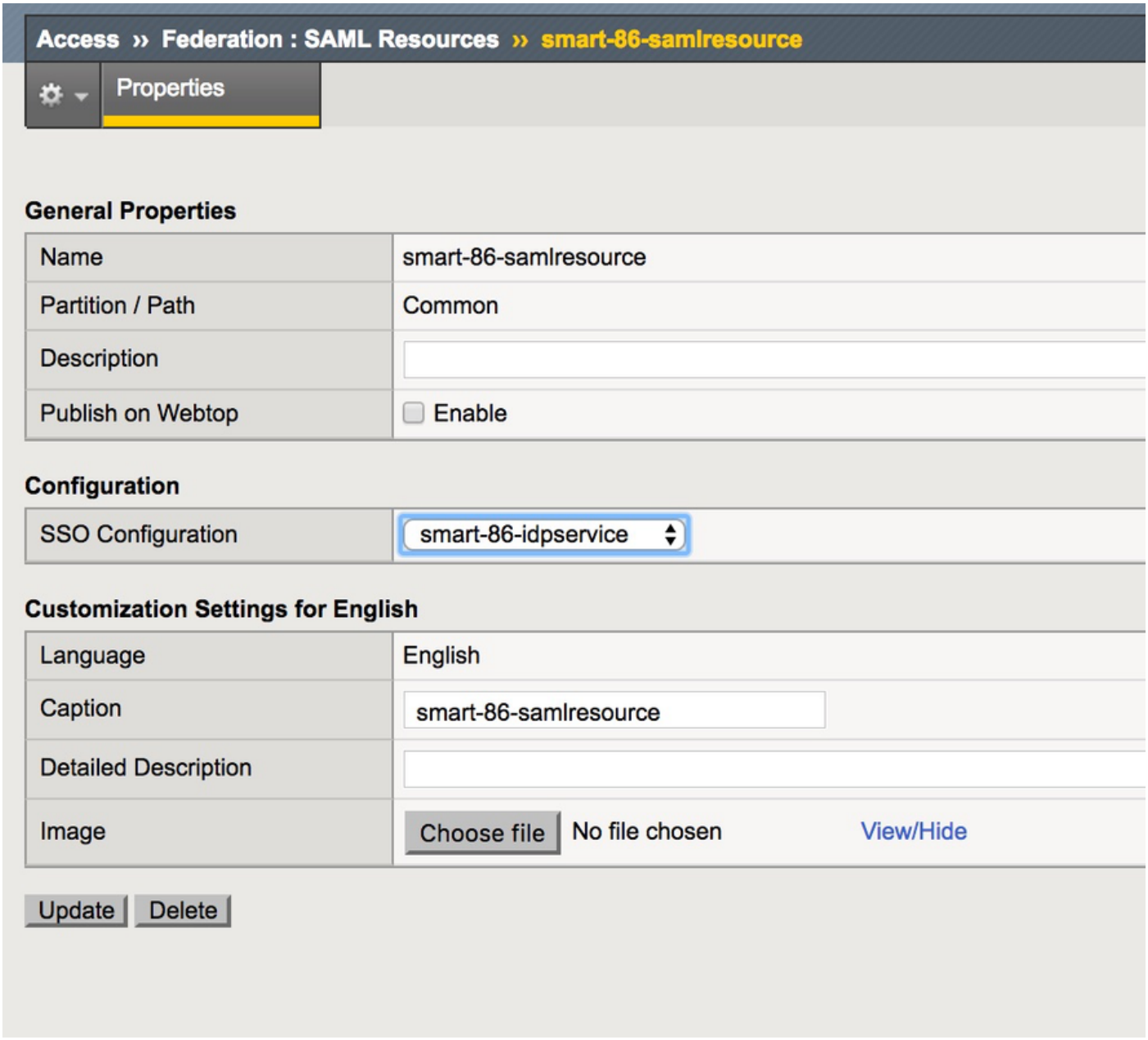


Note: Una vez que el servicio de IdP se crea, hay una opción para descargar los meta datos con los **meta datos de una exportación del** botón bajo **acceso** - **> federación** - **> SAML proveedor de la identidad** - > los **servicios locales de IdP**

Creación del lenguaje de marcado de la aserción de la Seguridad (SAML)

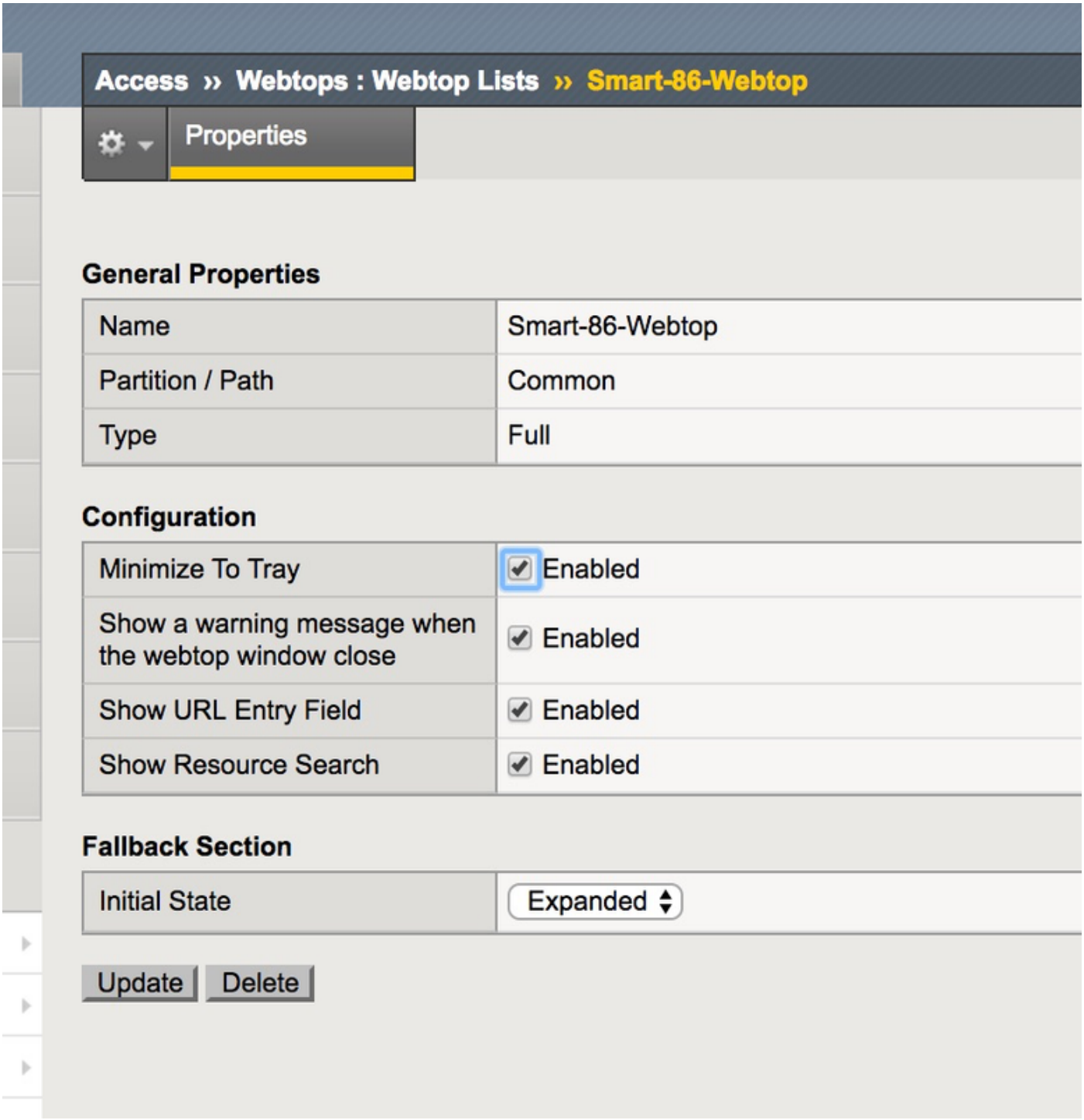
SAML recursos

- Navegue **para acceder** - **> federación** - **> SAML los recursos** y para crear un recurso del saml para asociarse al servicio de IdP que fue creado anterior



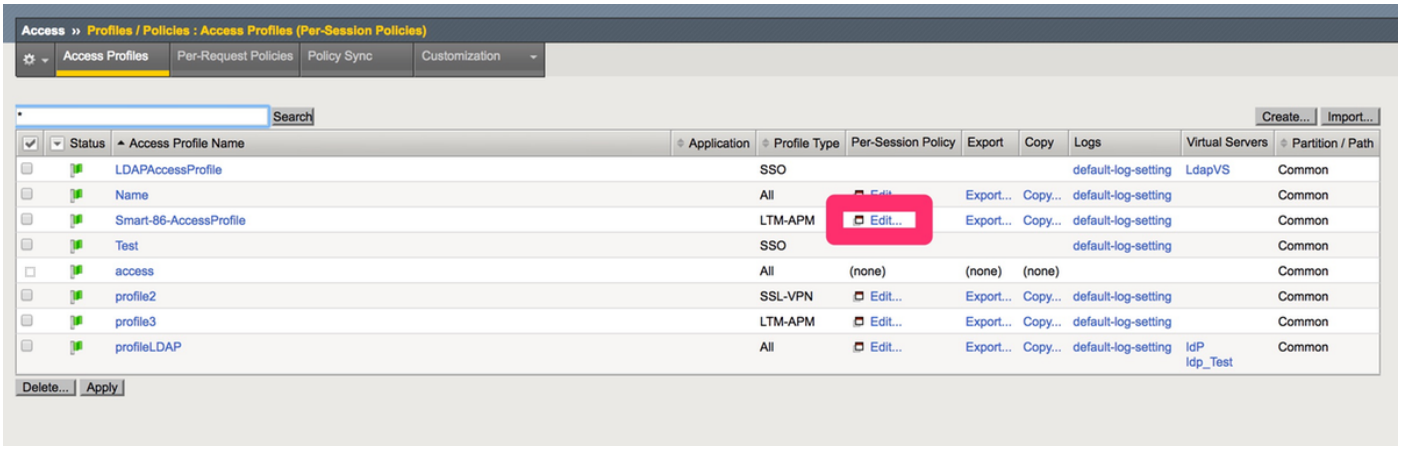
Webtops

- Cree un webtop bajo **acceso** - > **Webtops**

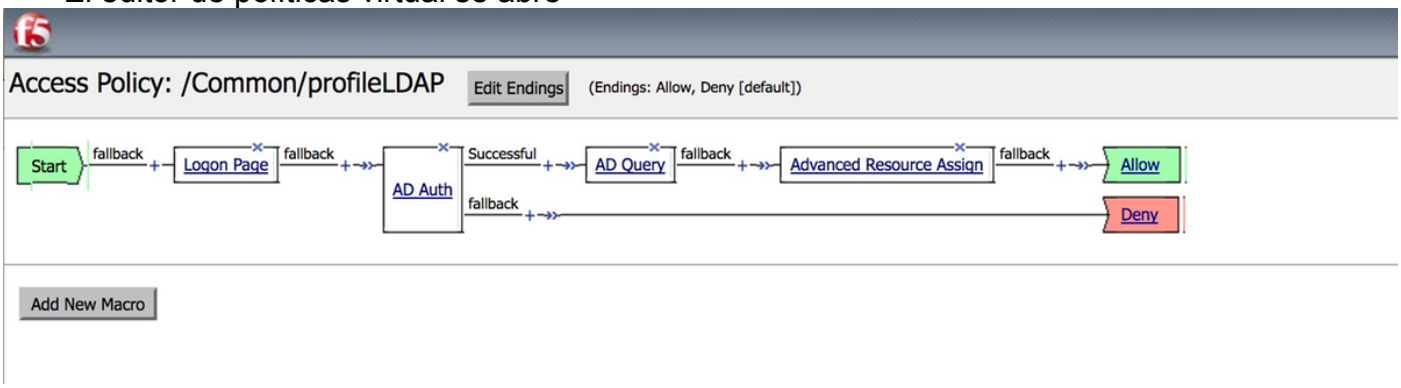


Editor de políticas virtual

- Navegue a la directiva creada anterior y haga clic en editan el link



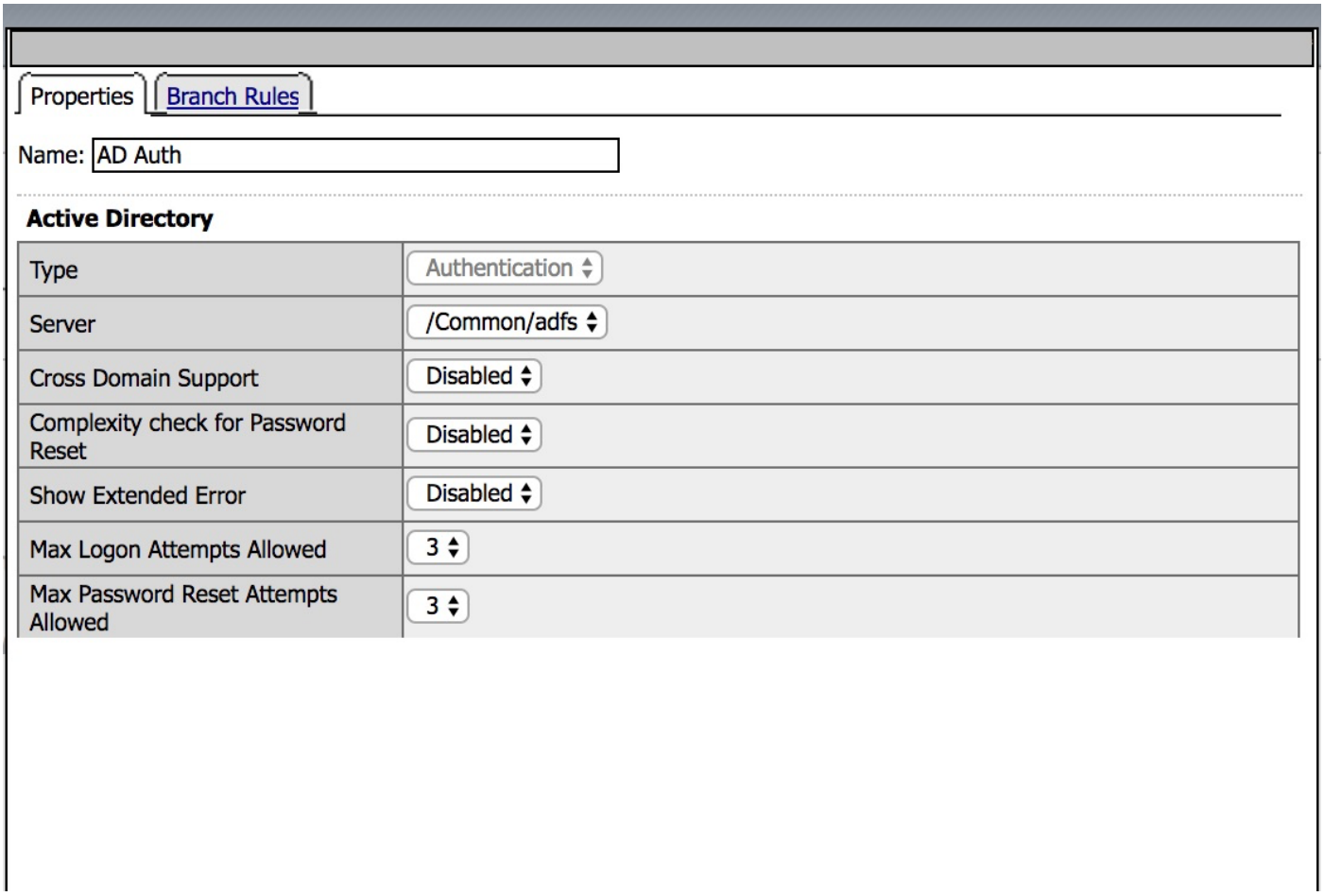
- El editor de políticas virtual se abre



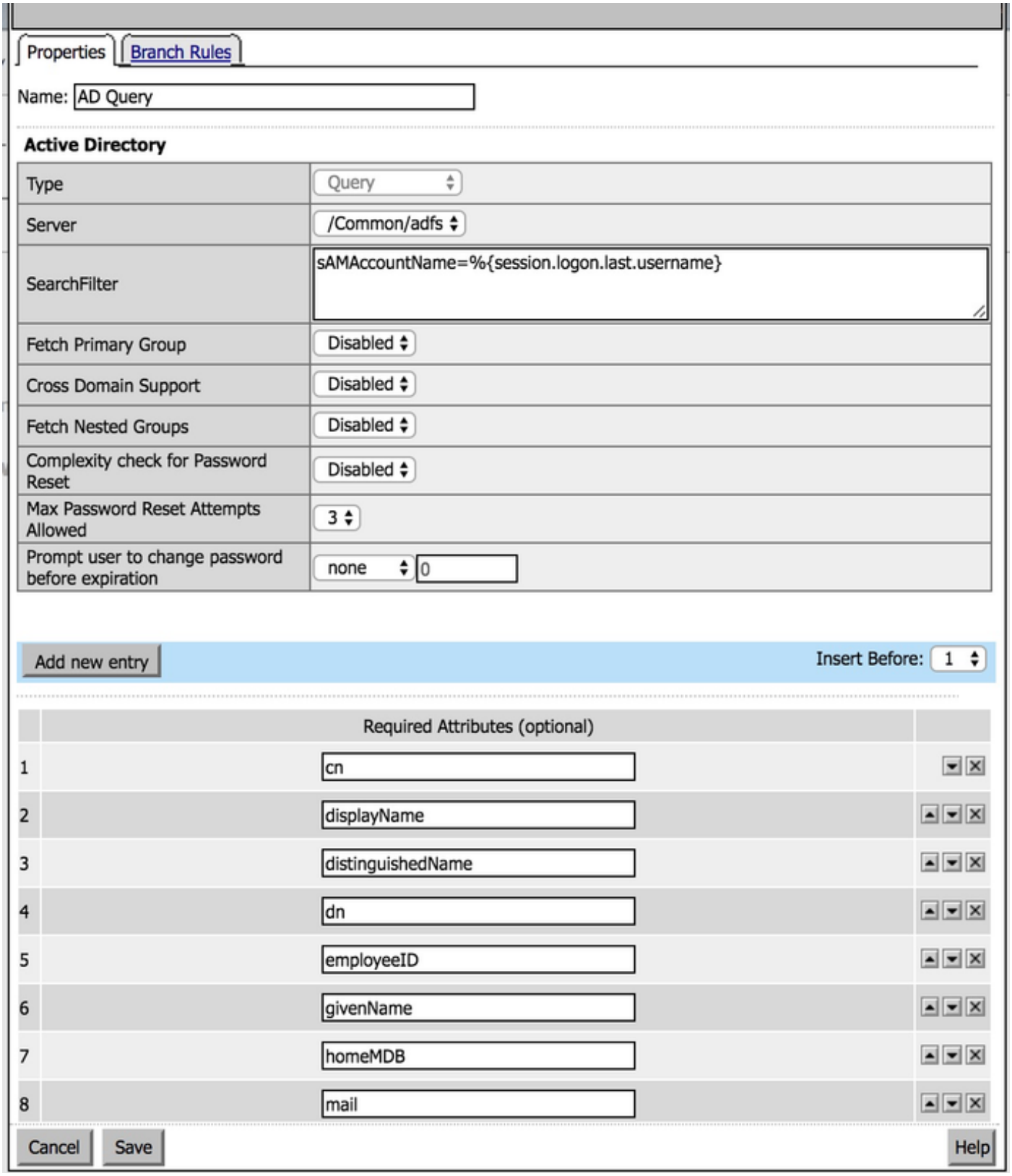
- Haga clic en el icono y agregue los elementos según lo descrito

Paso 1. **Elemento de la página del inicio** - Deje todos los elementos para omitir.

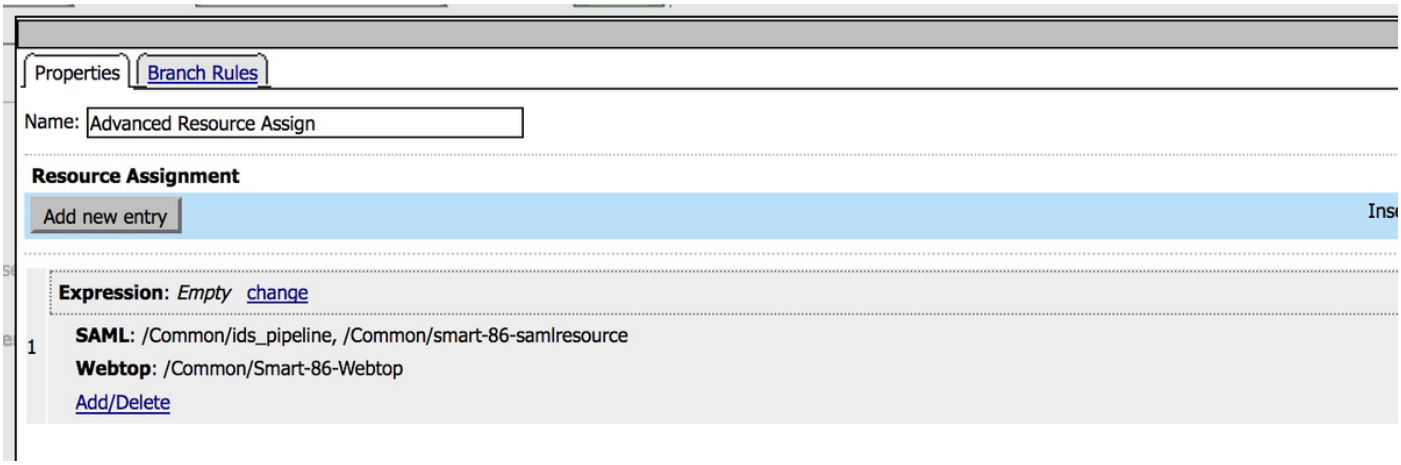
Paso 2. **Auth AD** - > elija la configuración ADFS creada anterior.



Paso 3. **Elemento de la interrogación AD** - Asigne los detalles necesarios.



Paso 4. **El recurso anticipado asigna - Asocie el recurso del saml y el webtop creados anterior.**



Intercambio de los meta datos del proveedor de servicio (SP)

- Importe manualmente el certificado de los IdS al Grande-IP a través del **sistema** - Certificate Management (Administración de certificados) - > Traffic Management

  Note: Asegúrese de que el certificado consista en COMIENCE las etiquetas del CERTIFICADO y del CERTIFICADO del EXTREMO.

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

- Cree una nueva entrada de sp.xml bajo el **proveedor de** Access-> Federation-> SAMLIDENTITY **- > los conectores de** ExternalSP
- Ate el conector SP al servicio de IdP bajo **acceso** - **> federación** - **> SAML proveedor de la identidad** - > los **servicios locales de IdP**

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Falla de autenticación común del indicador luminoso LED amarillo de la placa muestra gravedad menor del acceso (CAC)

Si la autenticación SSO falla para los usuarios CAC, marque el UCCX ids.log para verificar los

atributos de SAML fueron fijados correctamente.

Si hay un problema de configuración, un error de SAML ocurre. Por ejemplo, en este snippet del registro, el atributo user_principal de SAML no se configura en el IdP.

Hh YYYY-MM-DD: milímetro: ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:465 SS.sss GMT(-0000) [IdSEndPoints-SAML-59] - No podría la **correspondencia de los atributos del** retrievefrom**: user_principal**
Hh YYYY-MM-DD: milímetro: ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 SS.sss GMT(-0000) [IdSEndPoints-SAML-59] - SAML **responseprocessingfailed con la excepción com.sun.identity.saml.common.SAMLException: No podía extraer user_principal de la respuesta del saml**
en com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributeFromAttributesMap(IdSSAMLAsyncServlet.java:466)
en com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet.java:263)
en com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServlet.java:176)
en com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)
en java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
en java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
en java.lang.Thread.run(Thread.java:745)

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems