Instale e configurar o fornecedor da identidade F5 (IdP) para o serviço da identidade de Cisco (IdS) para permitir o SSO

Índice

Introdução

Este original descreve a configuração no fornecedor da identidade F5 BIG-IP (IdP) para permitir sobre o único sinal (SSO).

Modelos de distribuição do Cisco IDS

Produto	Desenvolvimento
UCCX	Co-residente
PCCE	Co-residente com CUIC (centro unificado Cisco da inteligência) e LD (dados vivos)
UCCE	Co-residente com CUIC e LD para as disposições 2k. Autônomo para as disposições 4k e 12k.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Liberação 11.6 do Cisco Unified Contact Center Express (UCCX) ou liberação 11.6 do Cisco Unified Contact Center Enterprise ou liberação empacotada 11.6 da empresa do centro de contato (PCCE) como aplicáveis.

Note: Este original provê a configuração no que diz respeito ao serviço de Cisco Identitify (IdS) e ao fornecedor da identidade (IdP). O original provê UCCX nos screenshots e nos exemplos, porém a configuração é similar no que diz respeito ao serviço de Cisco Identitify (UCCX/UCCE/PCCE) e ao IdP.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Instalação

O Grande-IP é uma solução empacotada que tenha características múltiplas. Gerente da política de acesso (APM) que co-se relaciona ao serviço do fornecedor da identidade.

Grande-IP como o APM:

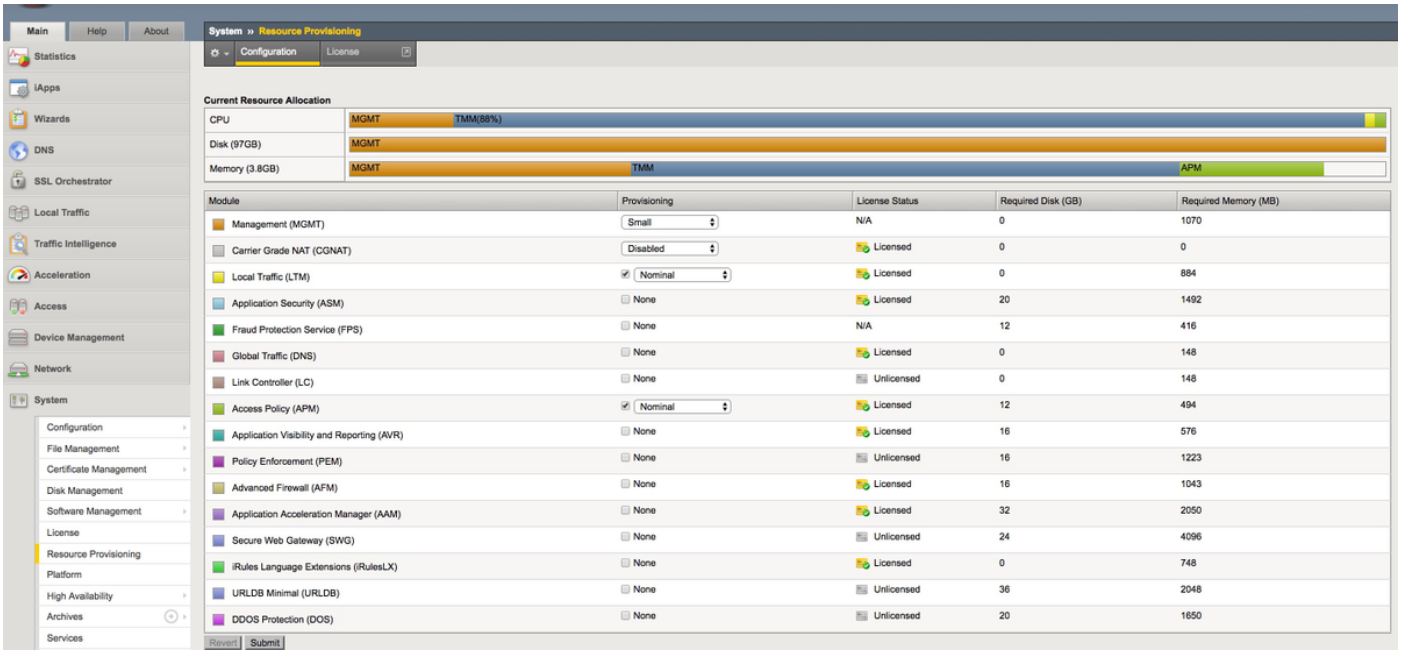
Versão	13.0
Tipo	Edition(OVA) virtual
IPs	Dois IPs em sub-redes diferentes. Um para o IP de gerenciamento e um para o servidor virtual de IdP

Transfira a imagem virtual da edição do Web site Grande-IP e distribua os ÓVULOS para criar uma máquina virtual (VM) que seja instalada. Obtenha a licença e instale-a com as requisições básico.

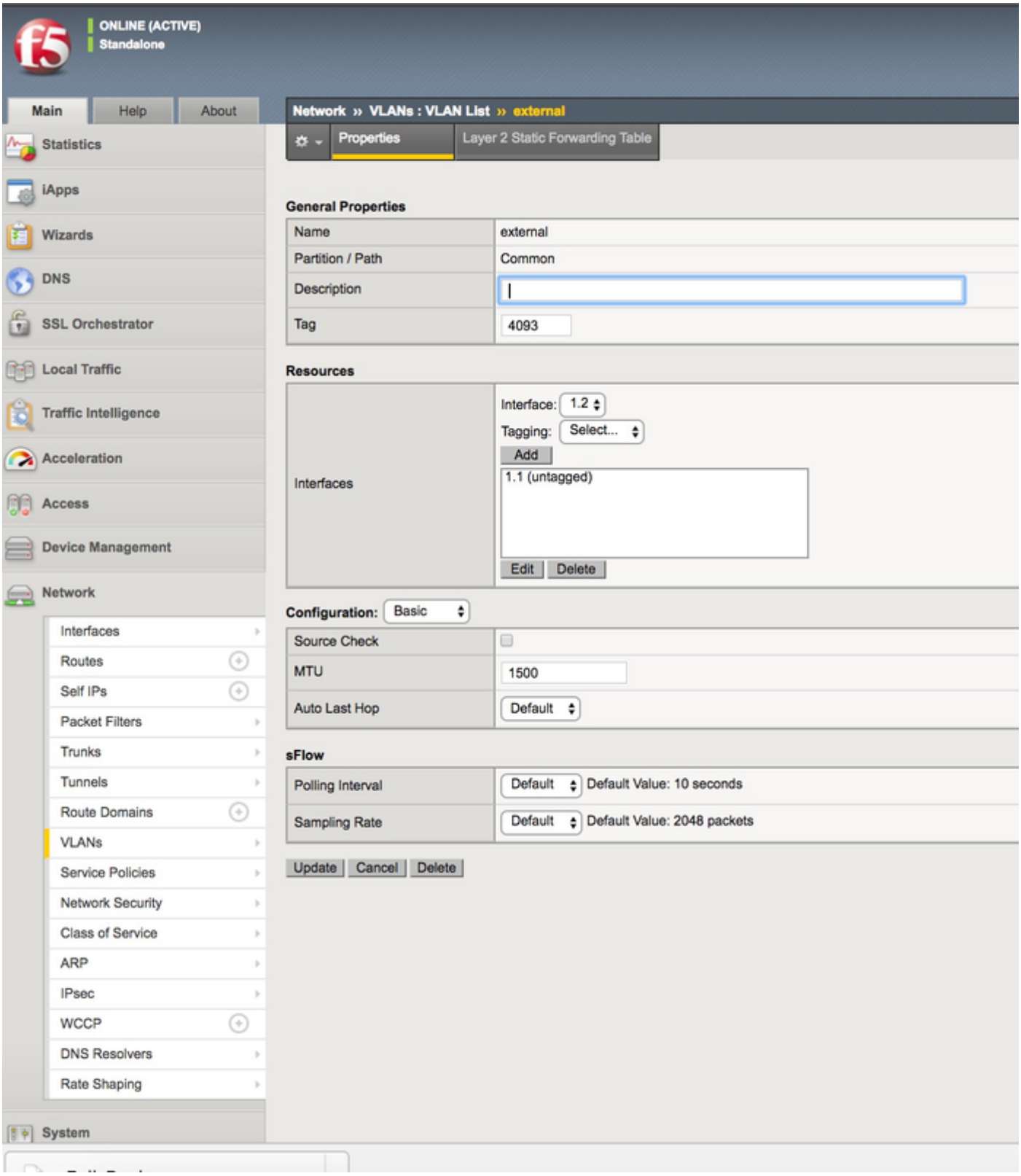
Note: Para a informação de instalação, refira o Guia de Instalação Grande-IP.

Configurar

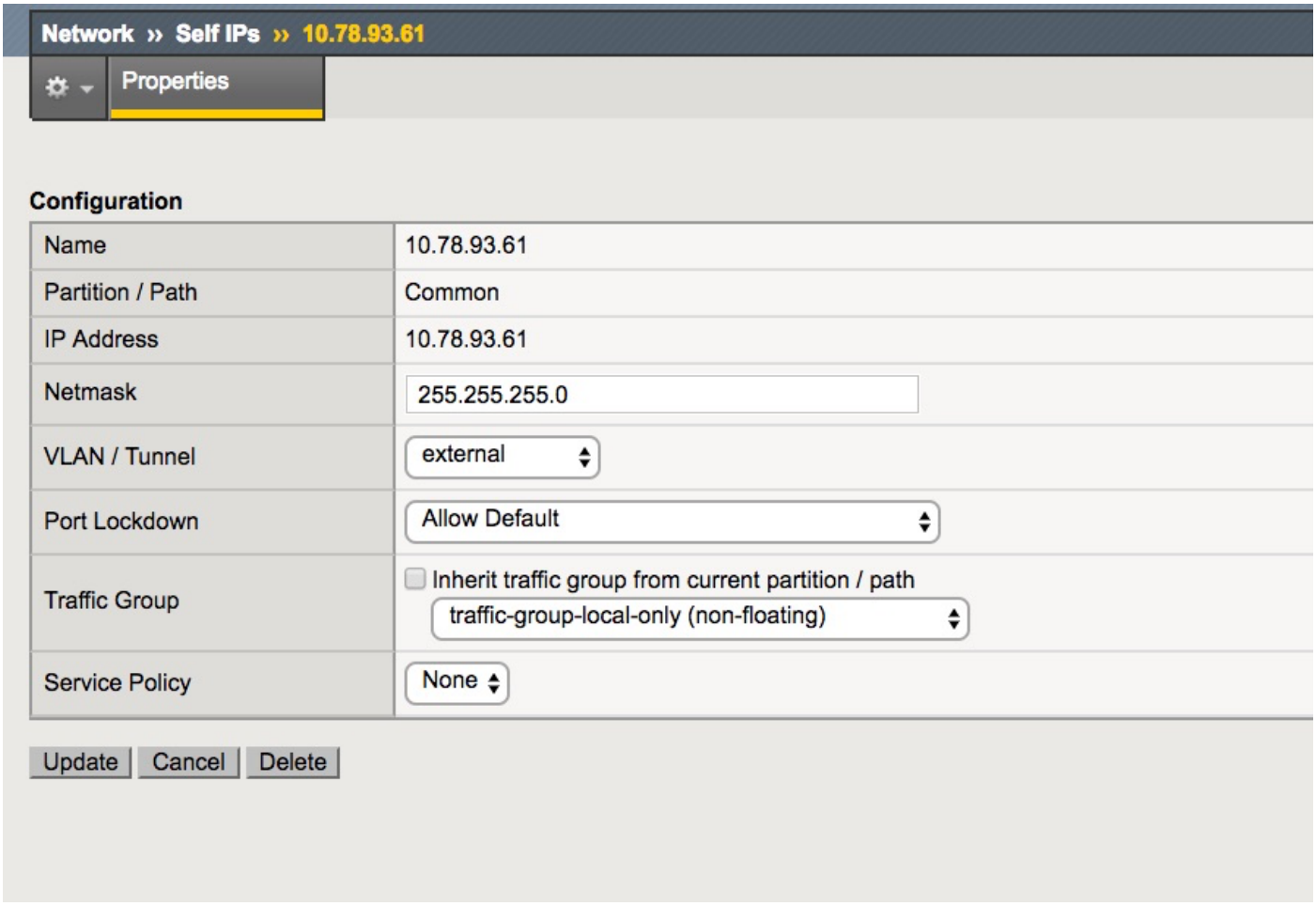
- Navegue ao abastecimento do recurso e permita a **política de acesso**, ajuste o abastecimento ao **substantivo**



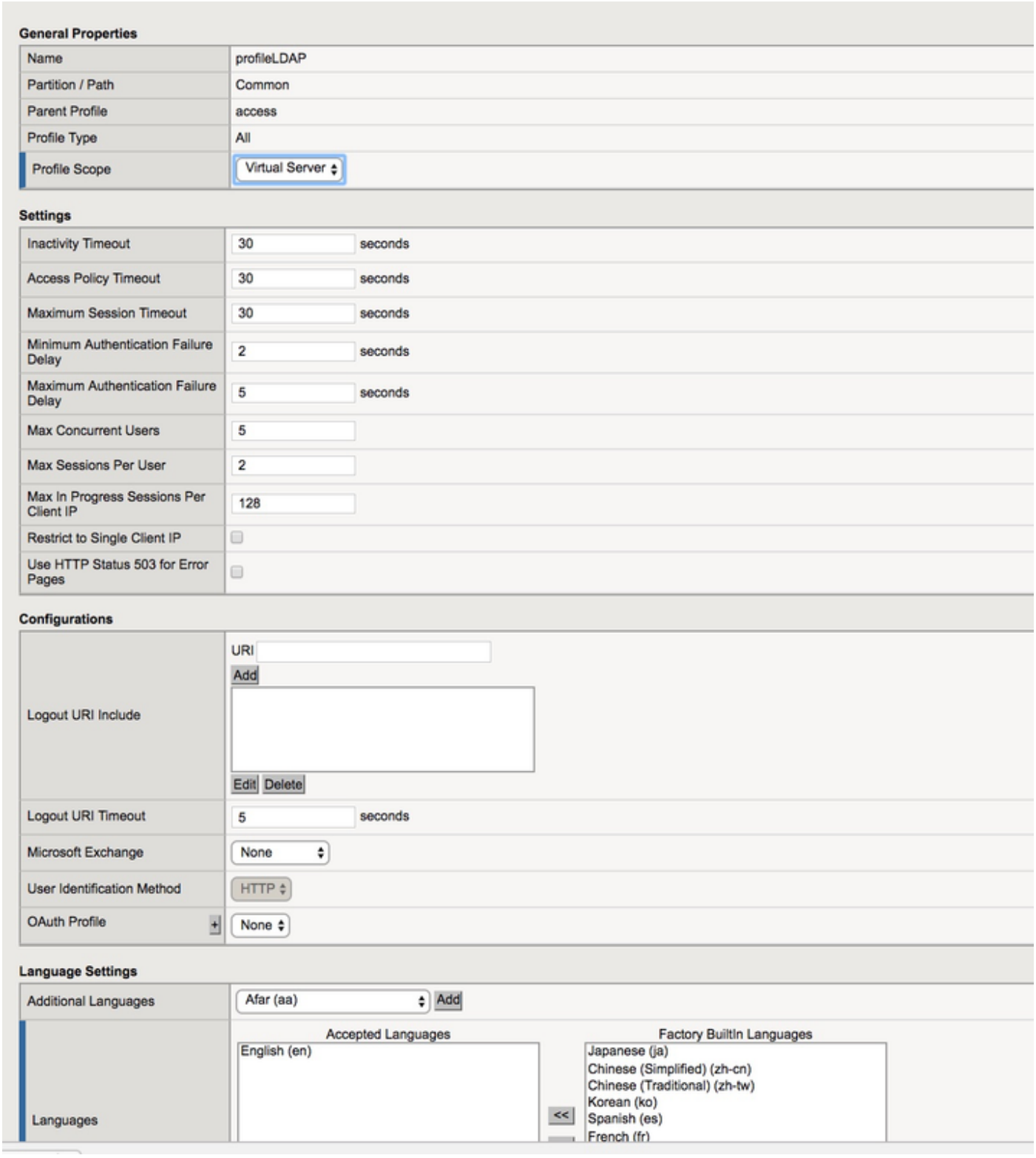
- Crie um VLAN novo sob a **rede** - > **VLAN**



- Crie uma entrada nova para o IP que é usado para o IdP sob a **rede - > o auto IPs**



- Crie um perfil sob o **acesso** - **> perfil/políticas** - **> perfis do acesso**

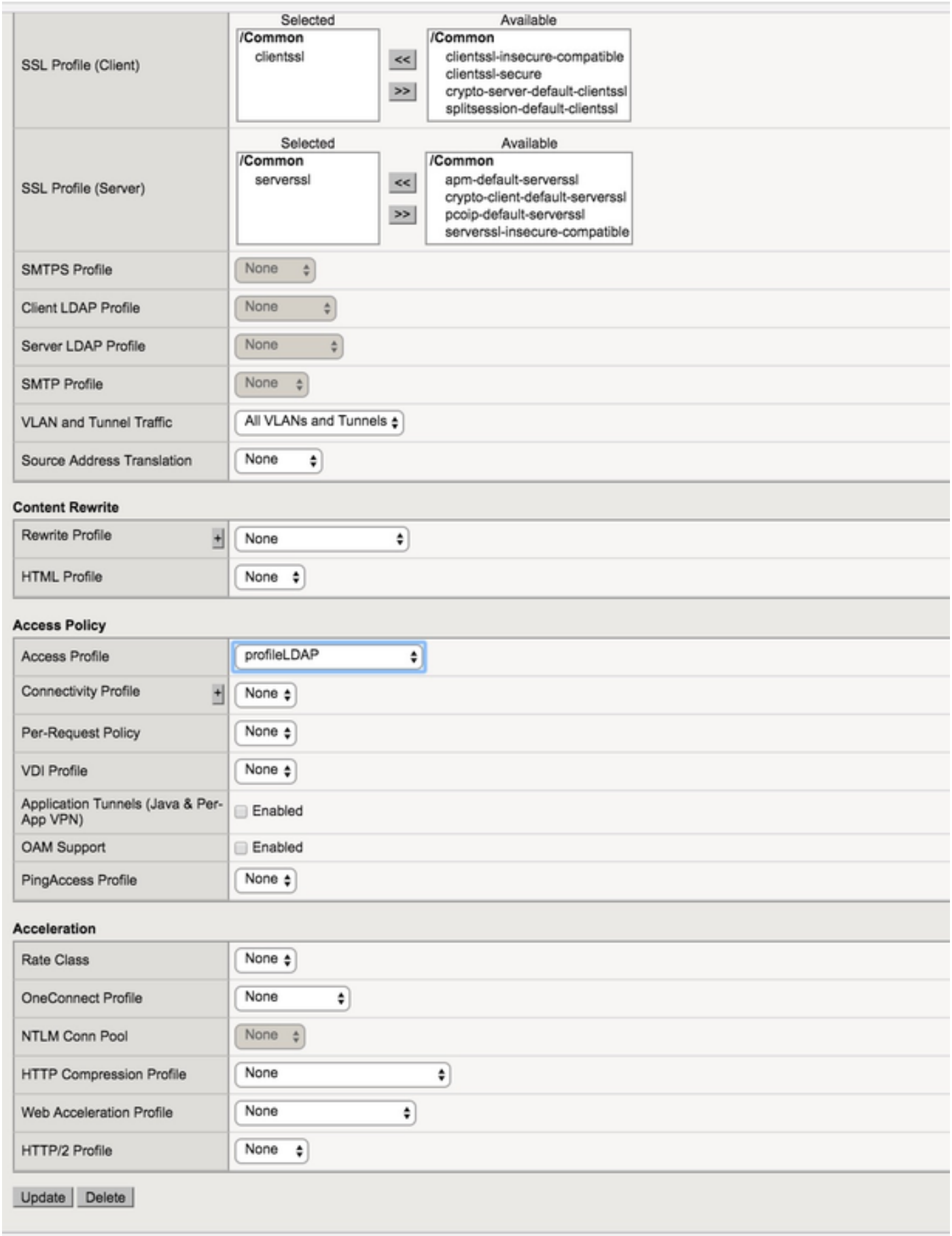


- Crie um servidor virtual

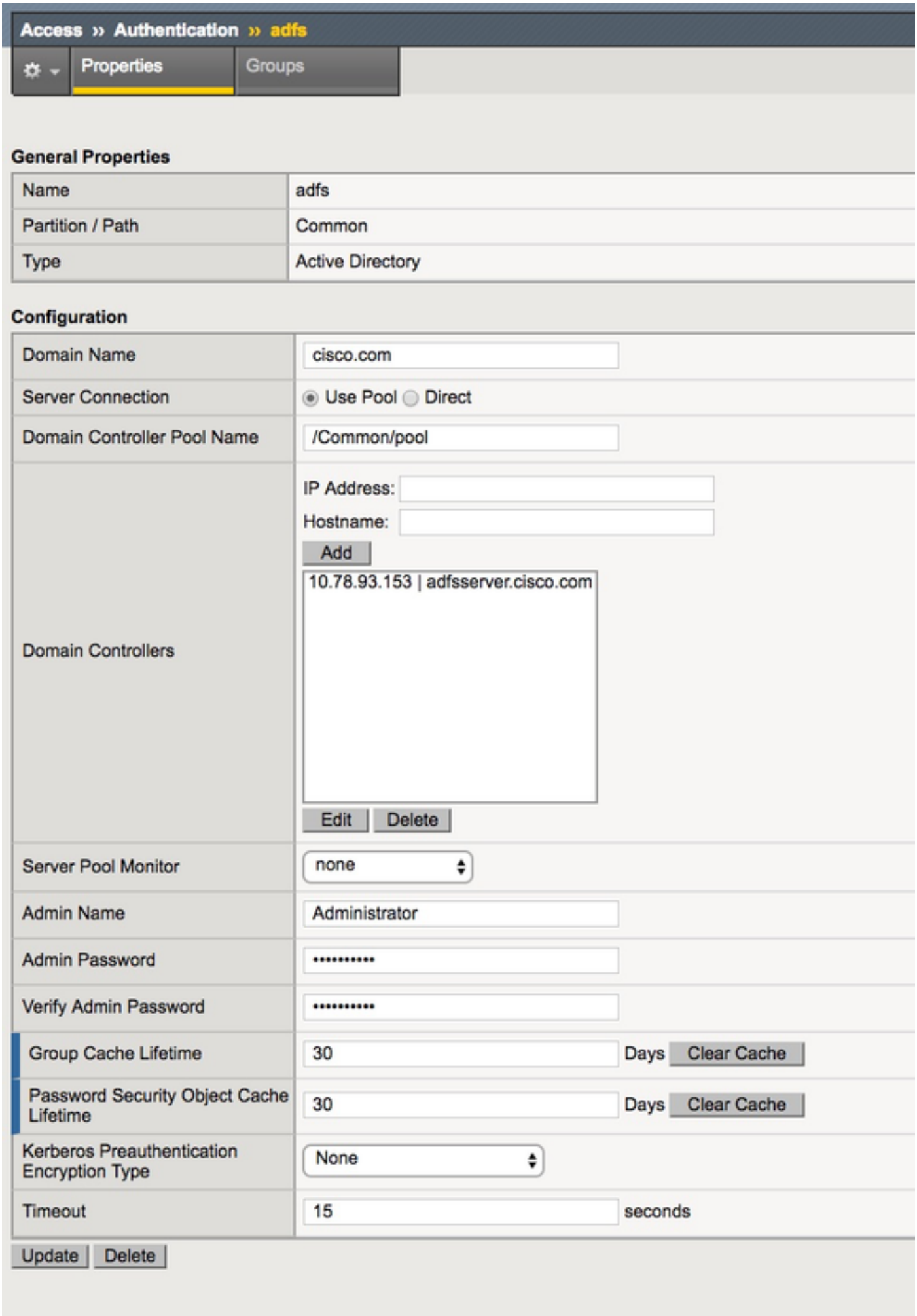
General Properties

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

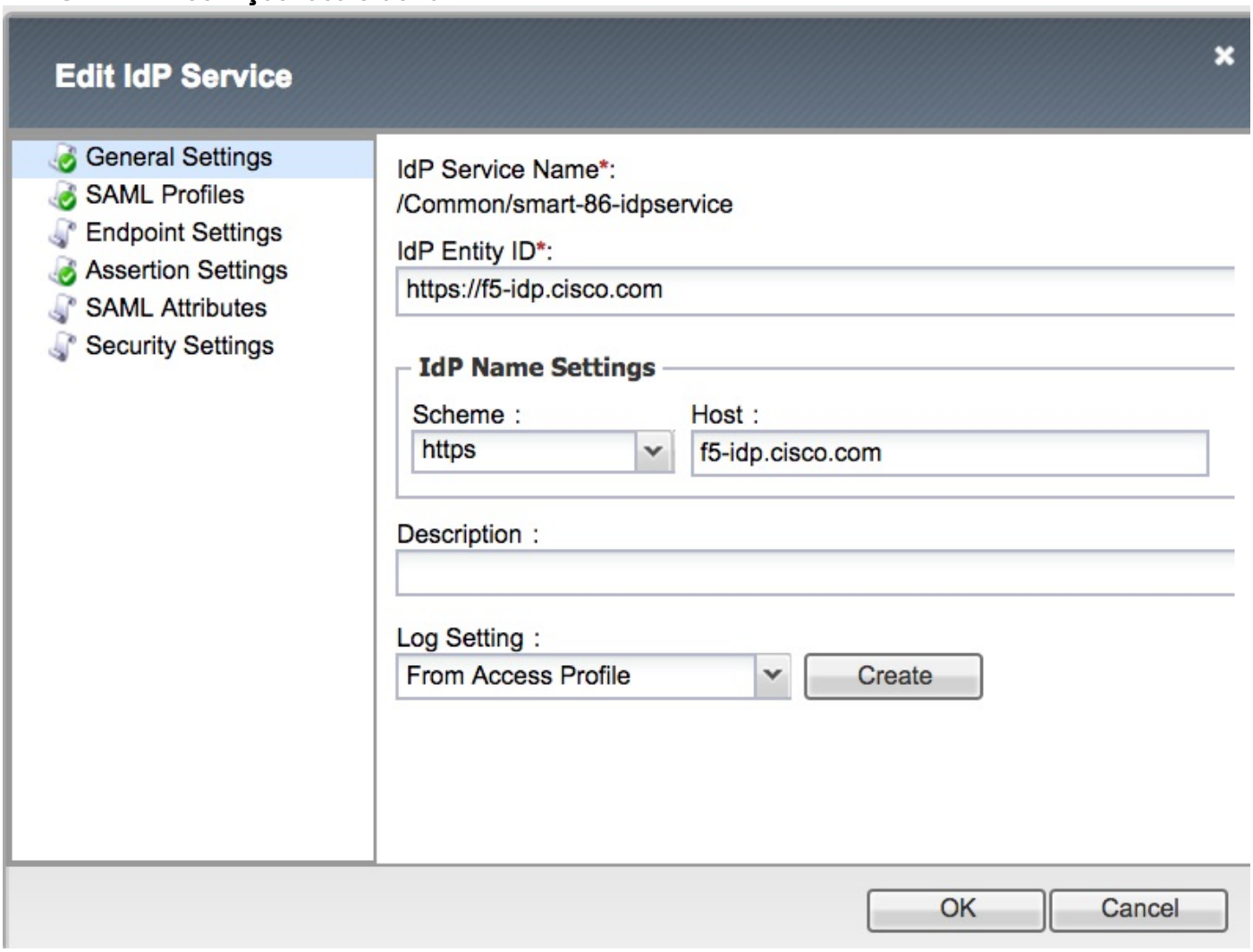
Configuration: Basic

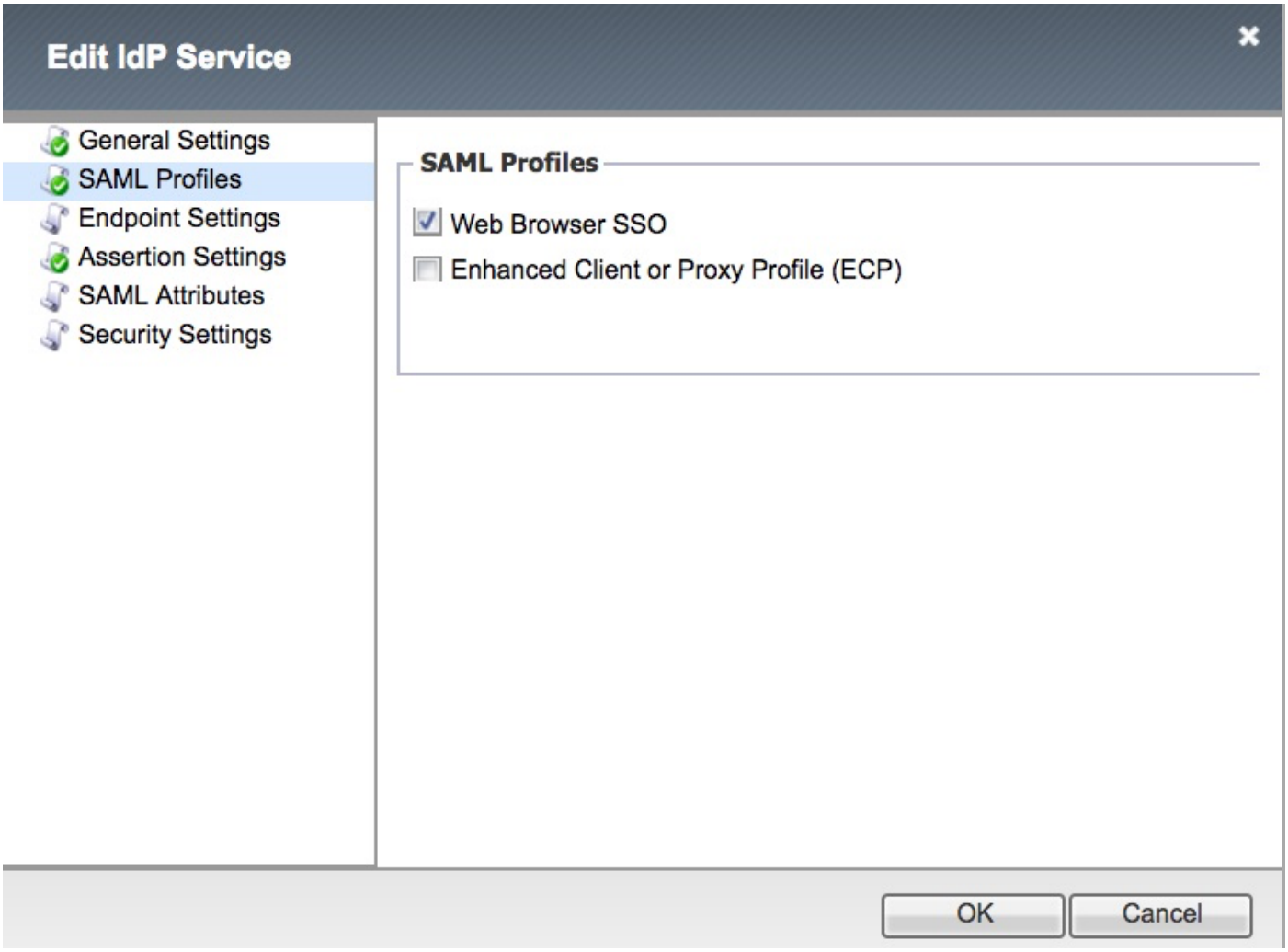


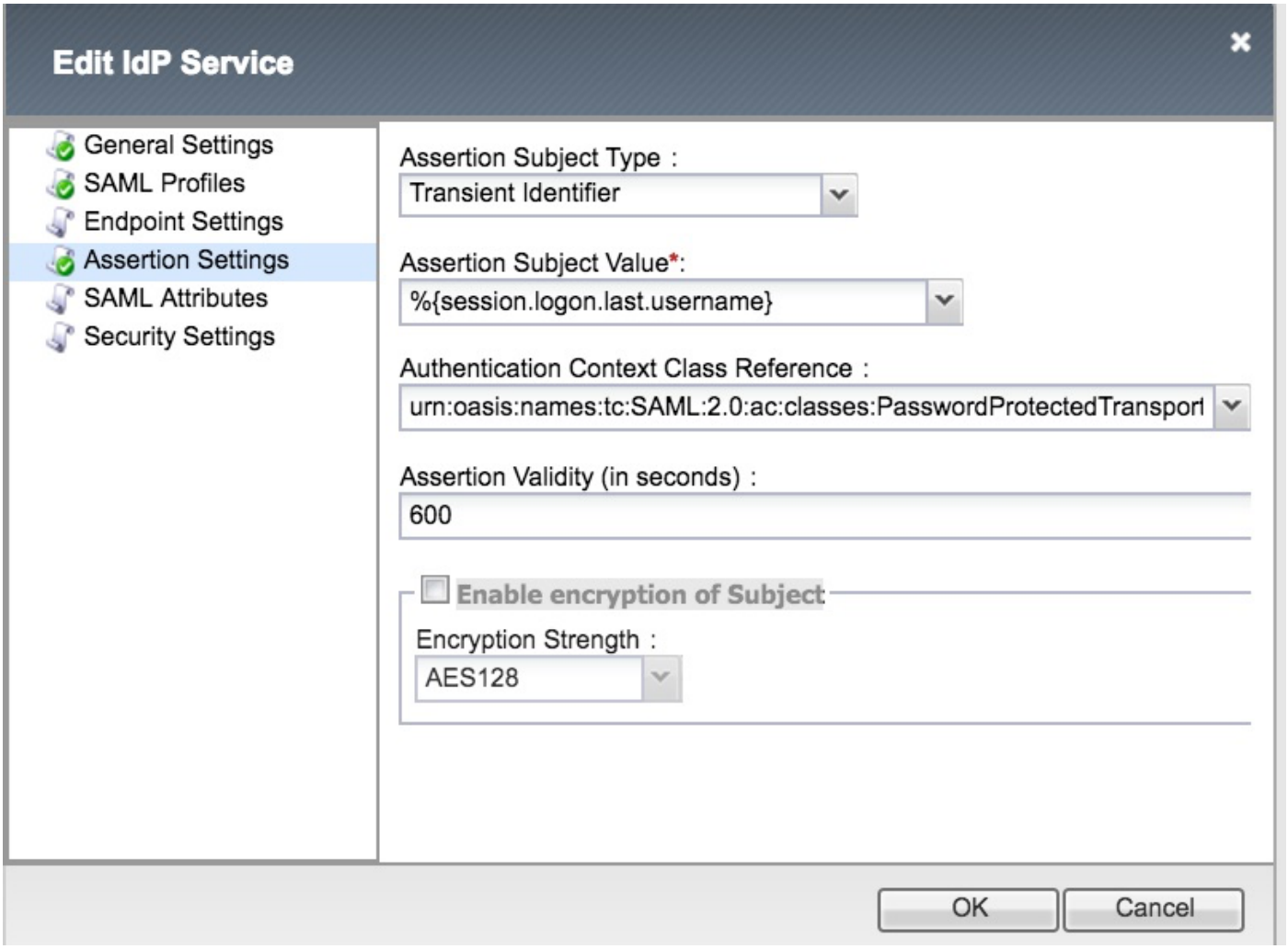
- Adicionar detalhes do diretório ativo (AD) sob o **acesso** - > **autenticação** - > **diretório ativo**


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

- Crie um serviço novo de IdP sob o **acesso - > federação - > fornecedor da identidade de SAML - > serviços locais 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



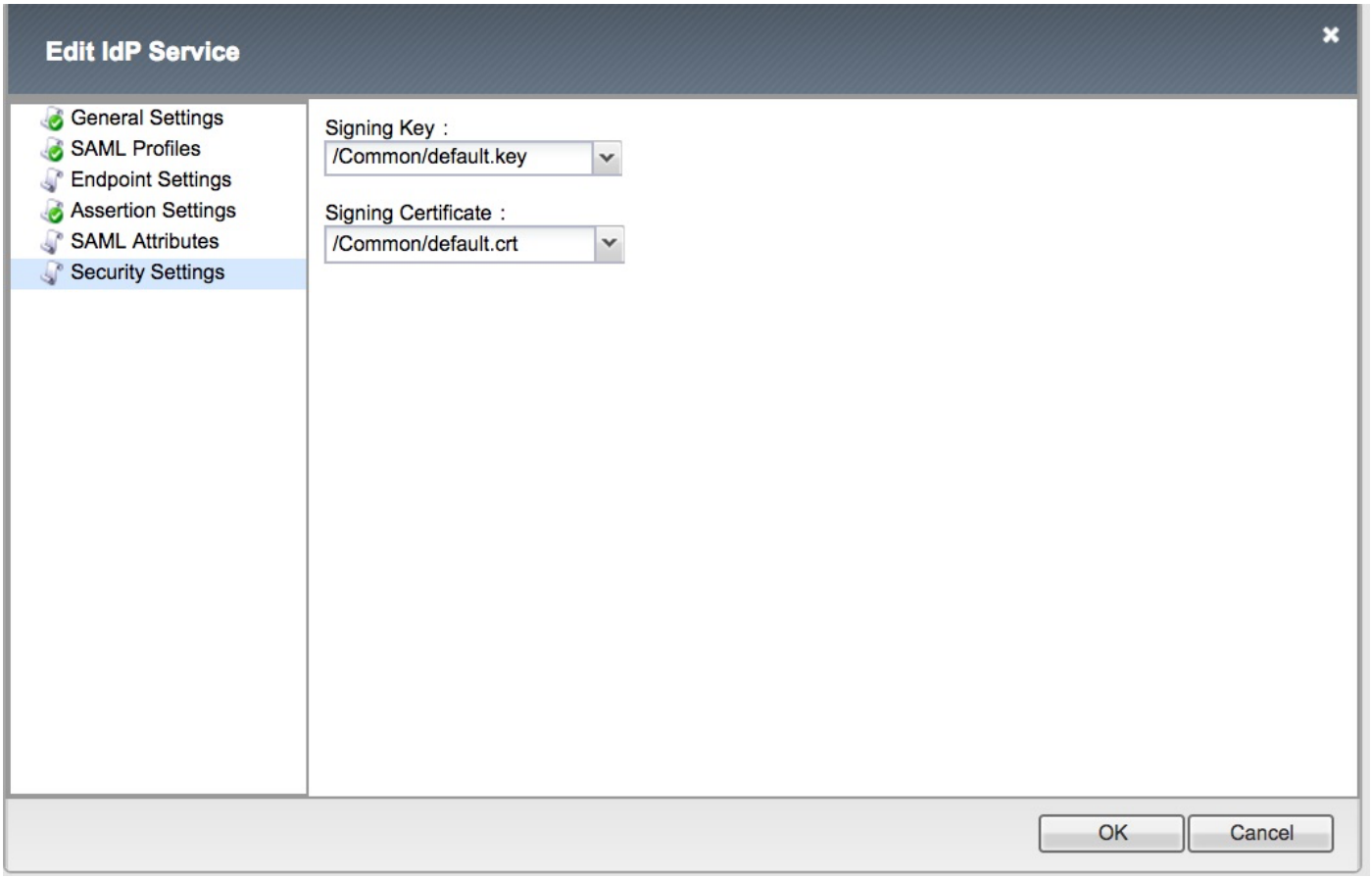
Note: Se um cartão comum do acesso (CAC) é usado para a autenticação, estes atributos precisam de ser adicionados na seção de configuração dos **atributos de SAML**:

Etapa 1. Crie o atributo do **uid.**

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

Etapa 2. Crie o atributo **user_principal**.

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

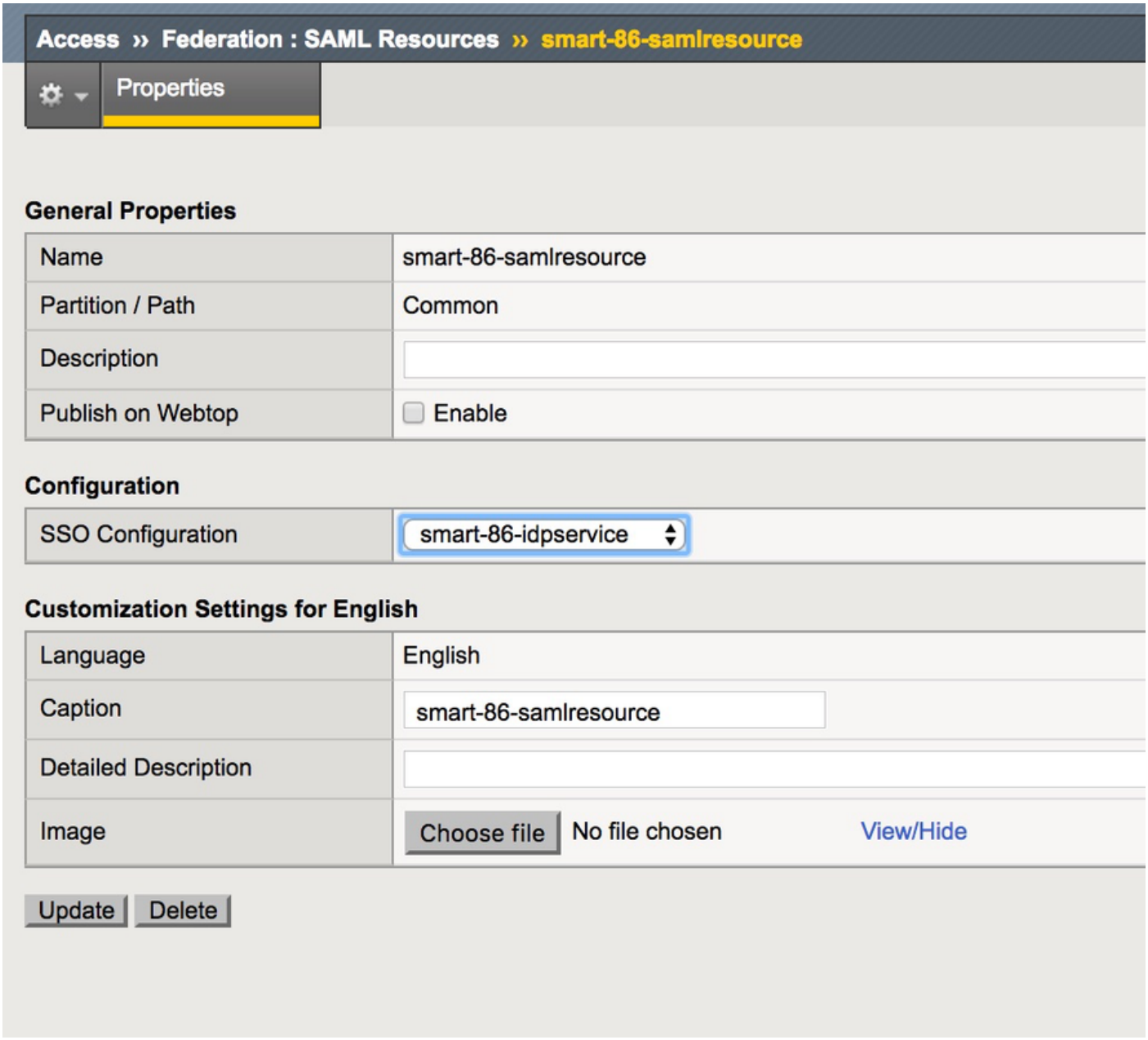


Note: Uma vez que o serviço de IdP é criado, há uma opção para transferir os metadata com **Metadata de uma exportação do** botão sob o **acesso** - **> federação** - **> fornecedor da identidade de SAML** - **> serviços locais de IdP**

Criação do linguagem de marcação da afirmação da Segurança (SAML)

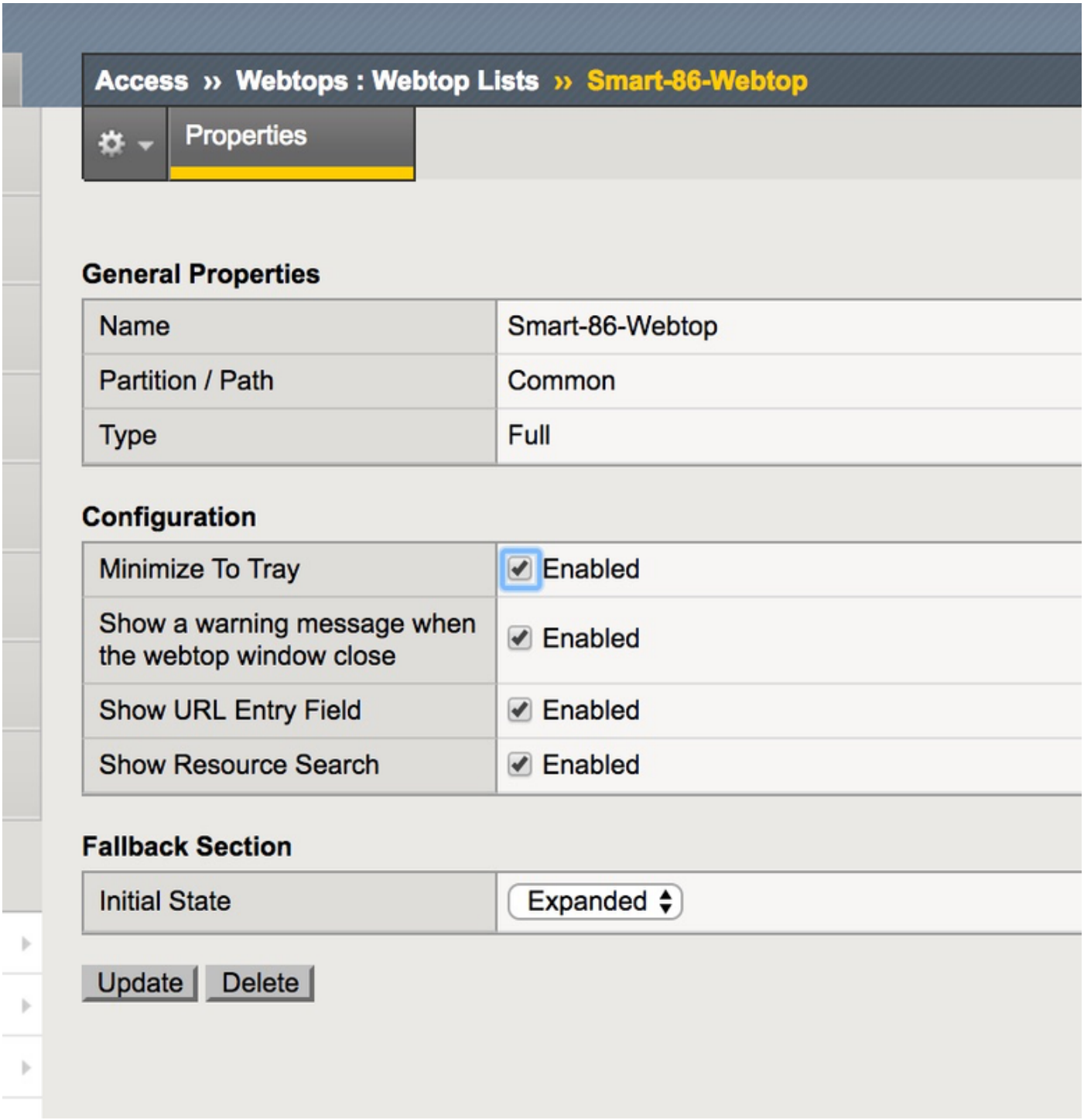
Recursos de SAML

- Navegue **para alcançar** - **> federação** - **> recursos de SAML** e para criar um recurso do saml para associar com o serviço de IdP que foi criado mais cedo



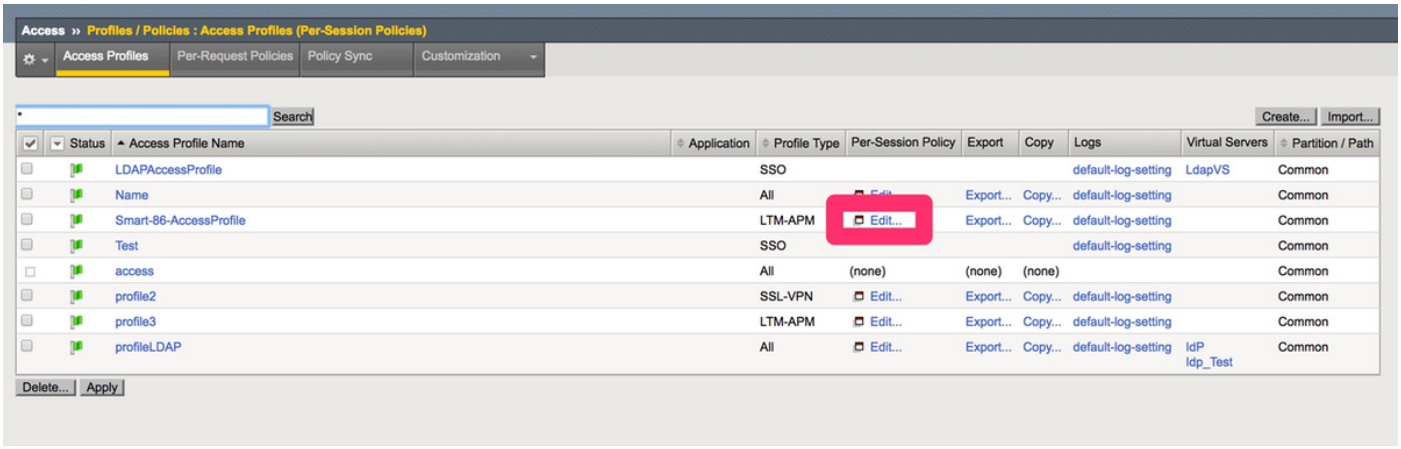
Webtops

- Crie um webtop sob o **acesso** - > **Webtops**

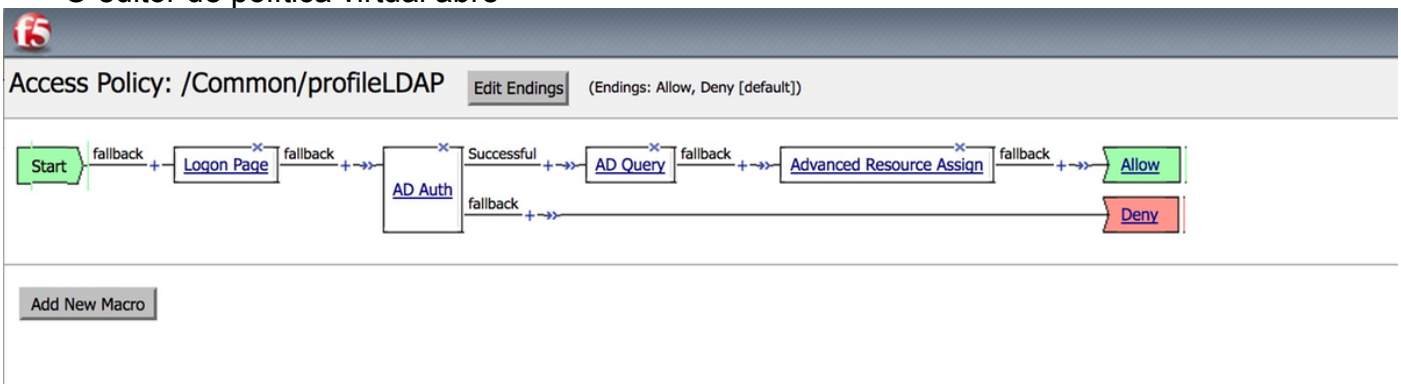


Editor de política virtual

- Navegue à política criada mais cedo e clique editam sobre o link



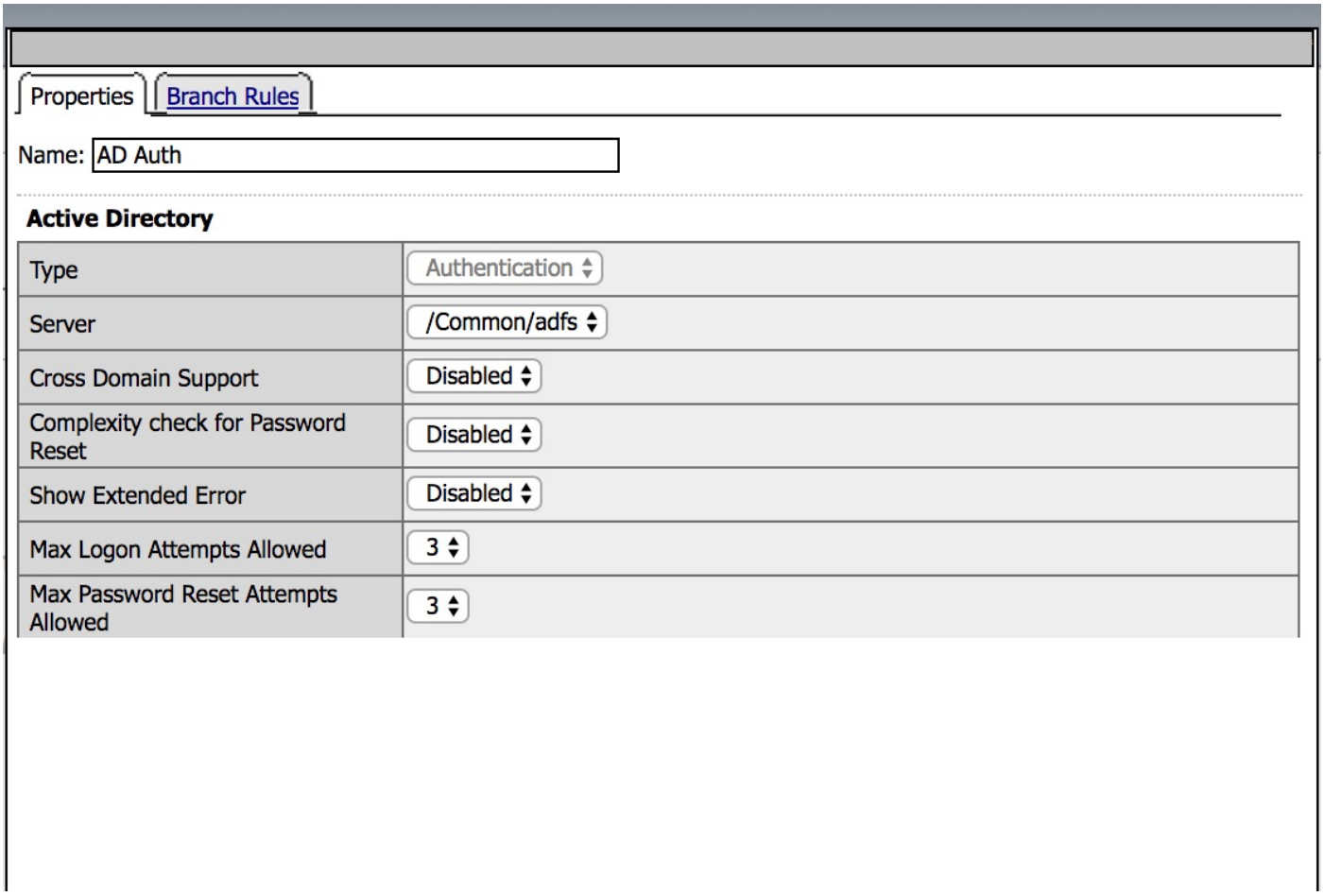
- O editor de política virtual abre



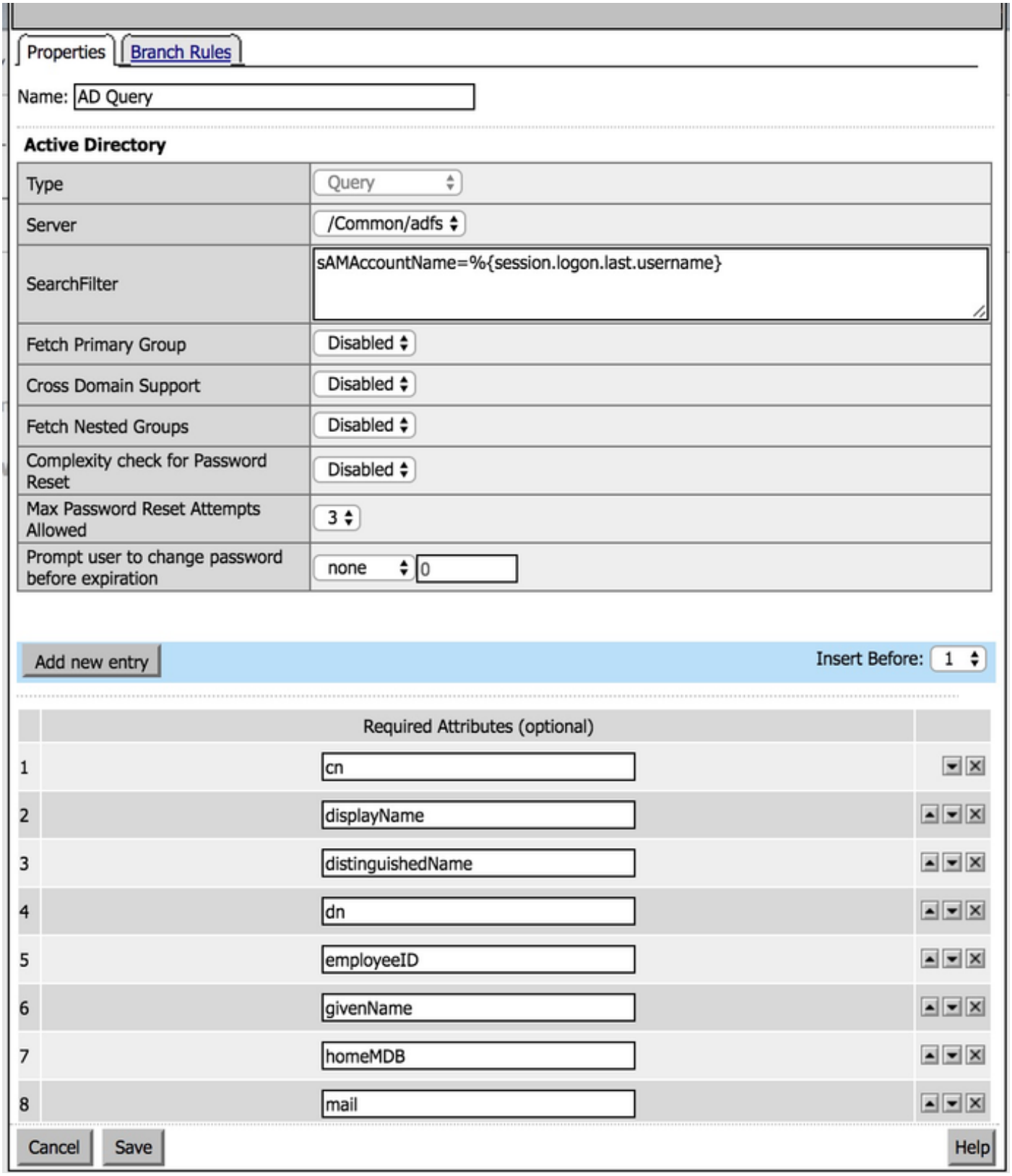
- Clique sobre o ícone e adicionar elementos como descritos

Etapa 1. **Elemento da página do fazer logon** - Deixe todos os elementos para optar.

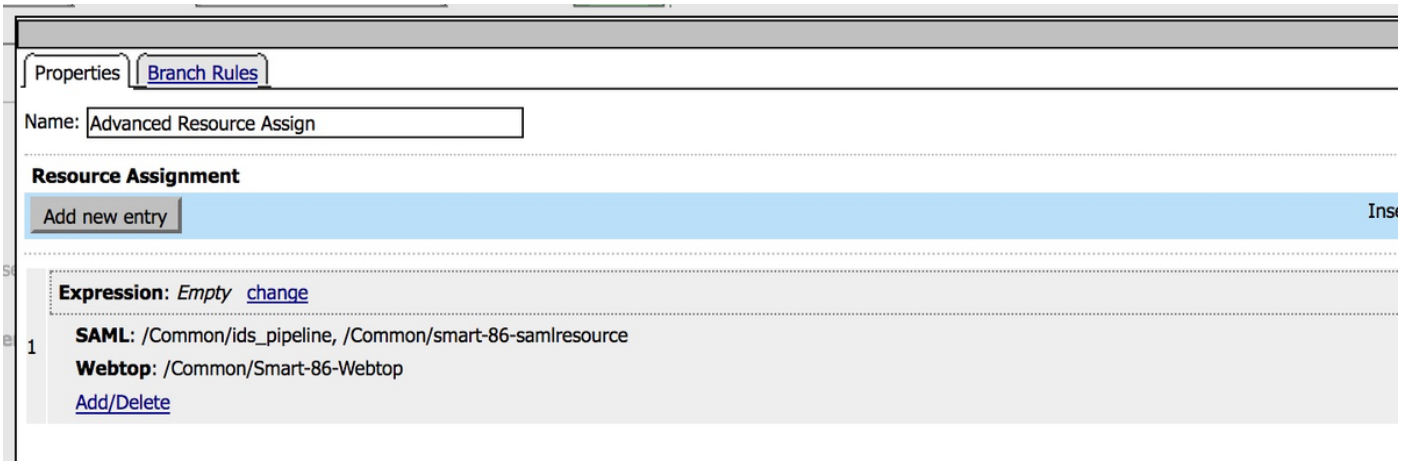
Etapa 2. **AUTH AD** - > escolha a configuração ADFS criada mais cedo.



Etapa 3. **Elemento da pergunta AD** - Atribua os detalhes necessários.



Etapa 4. **O recurso avançado atribui - Associe o recurso do saml e o webtop criados mais cedo.**



Troca dos Metadata do provedor de serviços (SP)

- Importe manualmente o certificado dos IdS ao Grande-IP através do **sistema** - > gerenciamento de certificado - > **gerência do tráfego**

  Note: Assegure-se de que o certificado consista COMECE O CERTIFICADO e TERMINE-SE etiquetas do CERTIFICADO.

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

- Crie uma entrada nova de sp.xml sob o **fornecedor de** Access-> Federation-> SAMLIDENTITY **- > conectores de** ExternalSP
- Ligue o conector SP ao serviço de IdP sob o **acesso** - **> federação** - **> fornecedor da identidade de SAML** - **> serviços locais de IdP**

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Falha de autenticação comum do cartão do acesso (CAC)

Se a autenticação SSO falha para usuários CAC, verifique o UCCX ids.log para verificar que os atributos de SAML estiveram ajustados corretamente.

Se há um problema de configuração, uma falha de SAML ocorre. Por exemplo, neste snippet do log, o atributo user_principal de SAML não é configurado no IdP.

YYYY-MM-DD HH: milímetro: ERRO com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:465 SS.sss GMT(-0000) [IdSEndPoints-SAML-59] - Não poderia o **mapa dos atributos do** retrievefrom**: user_principal**
YYYY-MM-DD HH: milímetro: ERRO com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 SS.sss GMT(-0000) [IdSEndPoints-SAML-59] - SAML **responseprocessingfailed com exceção com.sun.identity.saml.common.SAMLException: Não podia recuperar user_principal da resposta do saml**
em com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributeFromAttributesMap(IdSSAMLAsyncServlet.java:466)
em com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet.java:263)
em com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServlet.java:176)
em com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)
em java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
em java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
em java.lang.Thread.run(Thread.java:745)

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems