安装并且配置F5身份供应商(IdP) Cisco身份服务的(ID)对enable (event) SSO

Contents

Introduction

本文描述在F5 BIG-IP身份供应商(IdP)的配置对enable (event)单个符号(SSO)。

Cisco IDS部署模型

产品	配置
UCCX	coresident
PCCE	与CUIC (Cisco Unified智力中心)和LD (实际数据)的共同驻留
UCCE	与CUIC和LD的共同驻留2k配置的。 独立为4k和12k配置。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Cisco Unified Contact Center Express (UCCX)版本11.6或Cisco Unified Contact Center Enterprise Release 11.6或者被包的联系中心企业(PCCE)版本11.6如可适用。

  Note:本文参考配置关于Cisco Identitify服务(ID)和身份供应商(IdP)。 本文参考UCCX屏幕画面和示例，然而配置是类似的关于Cisco Identitify服务(UCCX/UCCE/PCCE)和IdP。

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.如果您的网络实际，请保证您了解所有命令的潜在影响。

安装

大IP是有多个功能的一个包的解决方案。与身份供应商服务CO涉及的访问策略管理器(APM)。

大IP作为APM ：

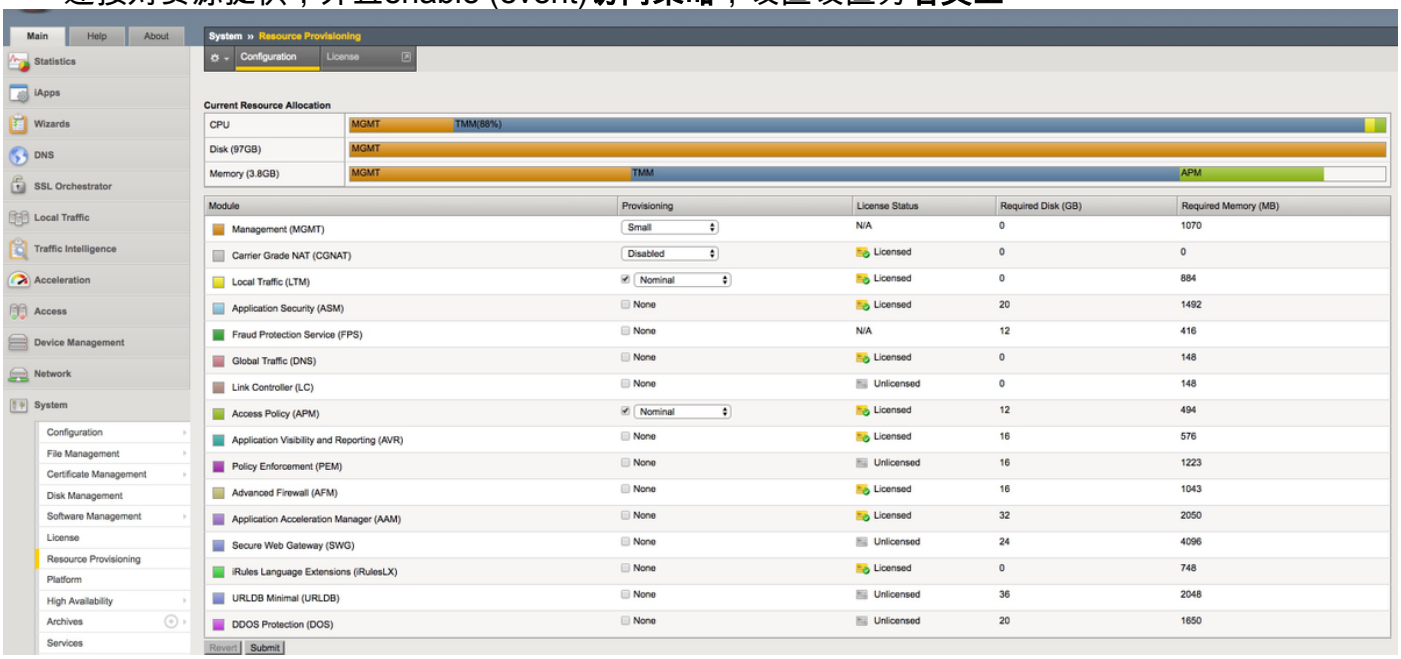
version 13.0	
类型	虚拟Edition(OVA)
IP	两IP用不同的子网。一管理IP的 并且一IdP虚拟服务器的

从大IP事先装配的网站下载虚拟版本镜像并且配置卵创建虚拟机。获得许可证并且安装与基本需求。

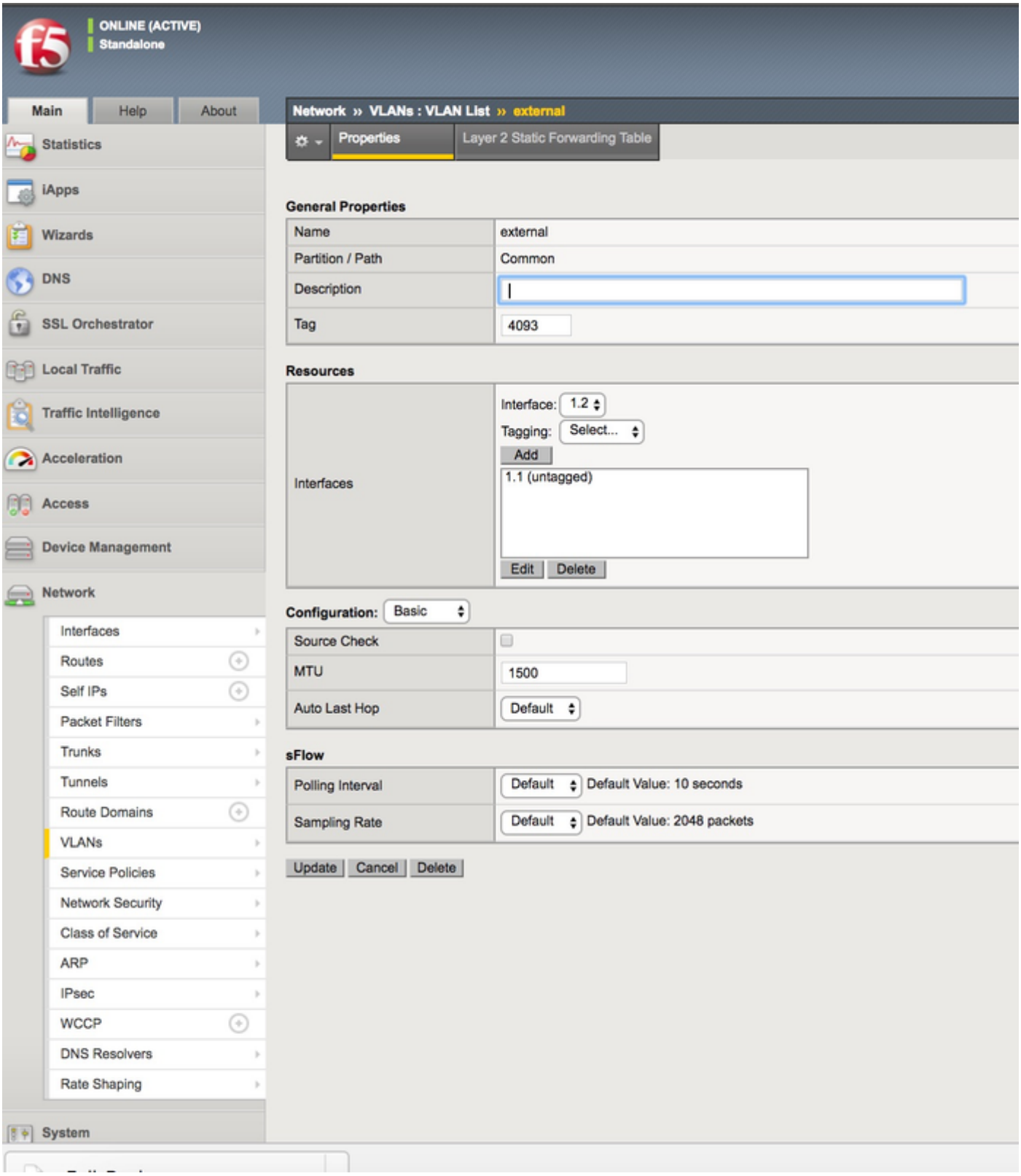
Note:安装信息，请参见大IP安装指南。

Configure

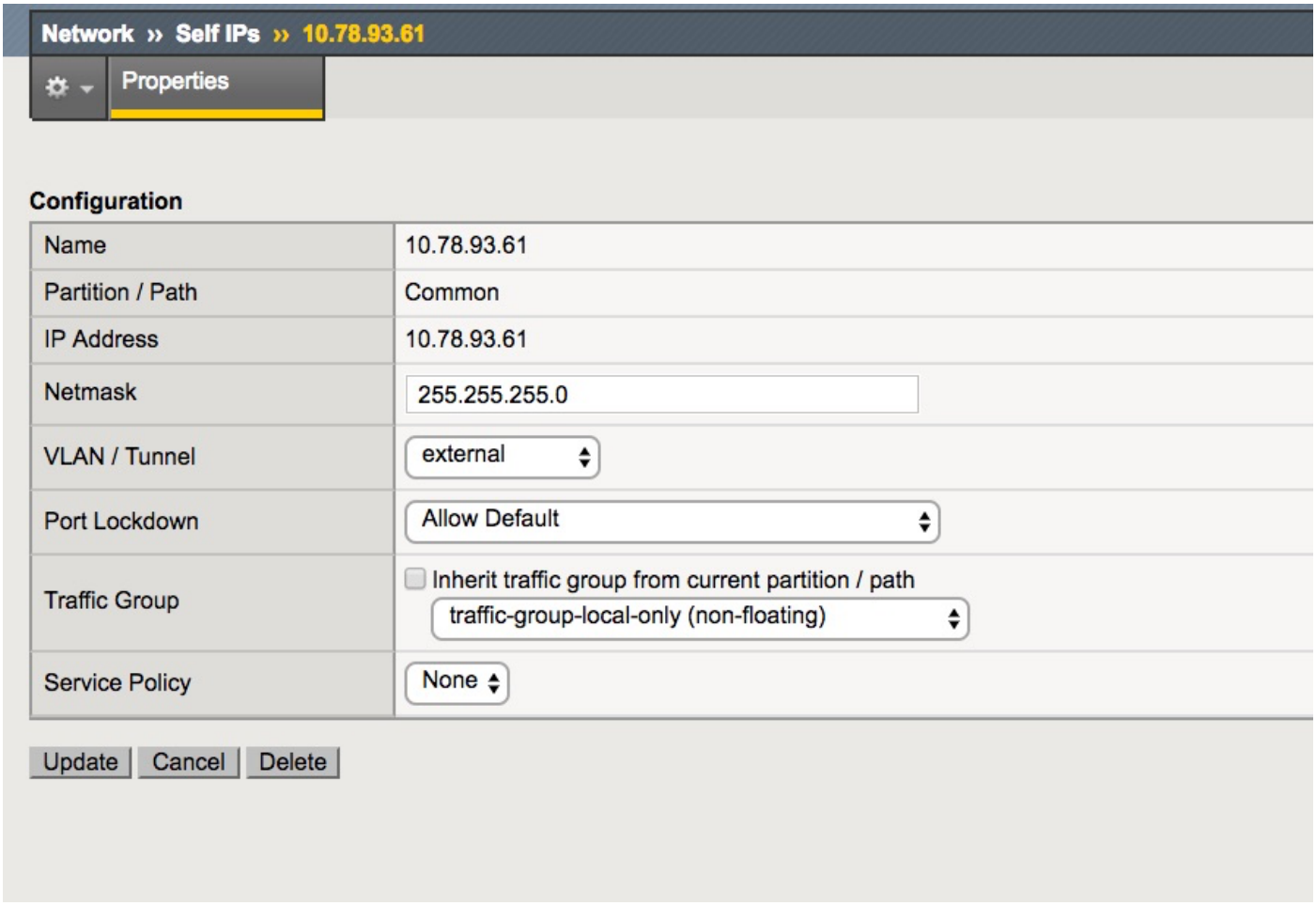
- 连接对资源提供，并且enable (event)**访问策略**，设置设置为**名义上**



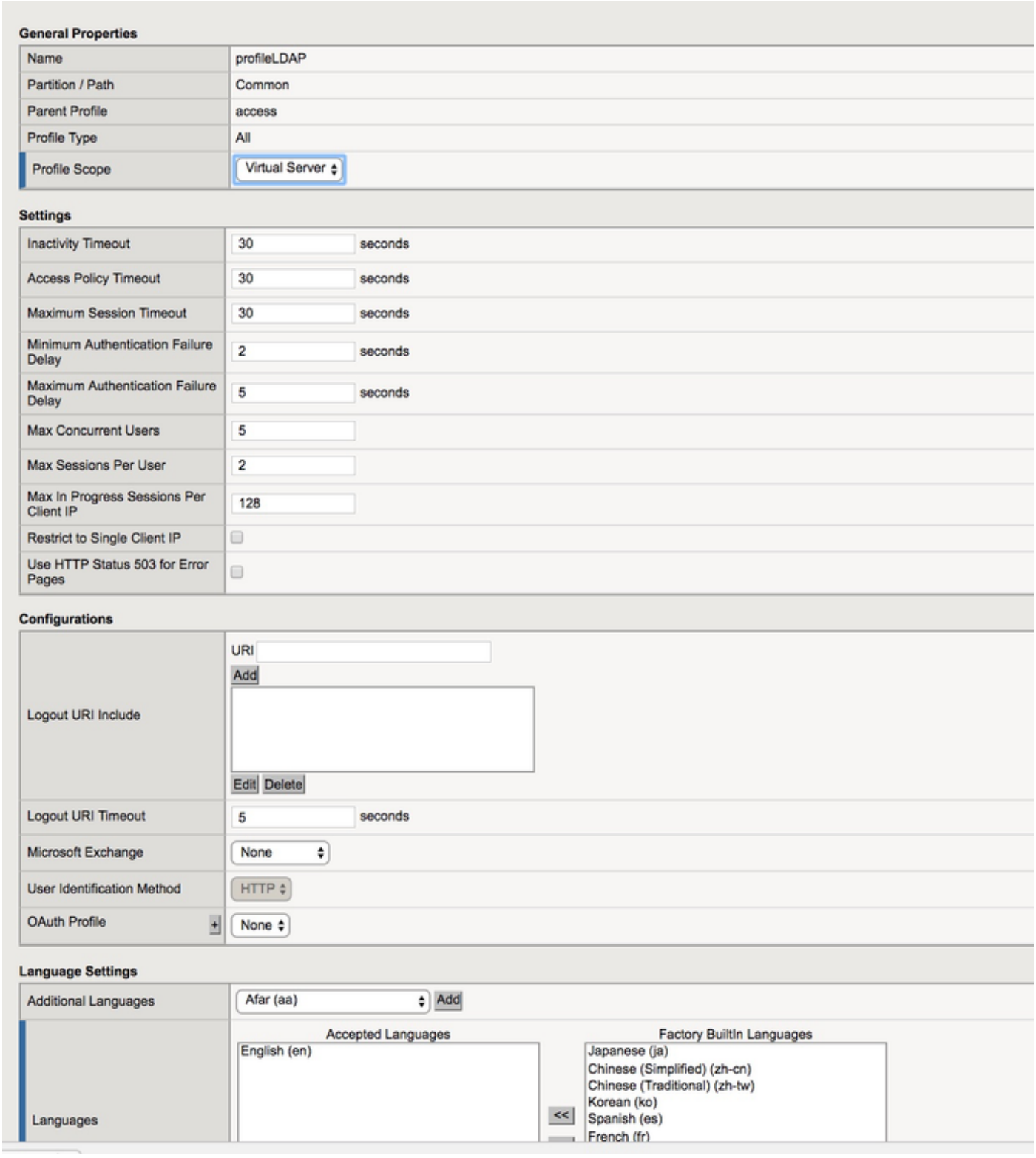
- 创建新的VLAN在**Network-> VLAN**下



- 创建使用在**Network->自己IP下的**IdP的IP的一个新的条目



- 创建一个配置文件在**访问下- >配置文件/策略**- >Access**配置文件**

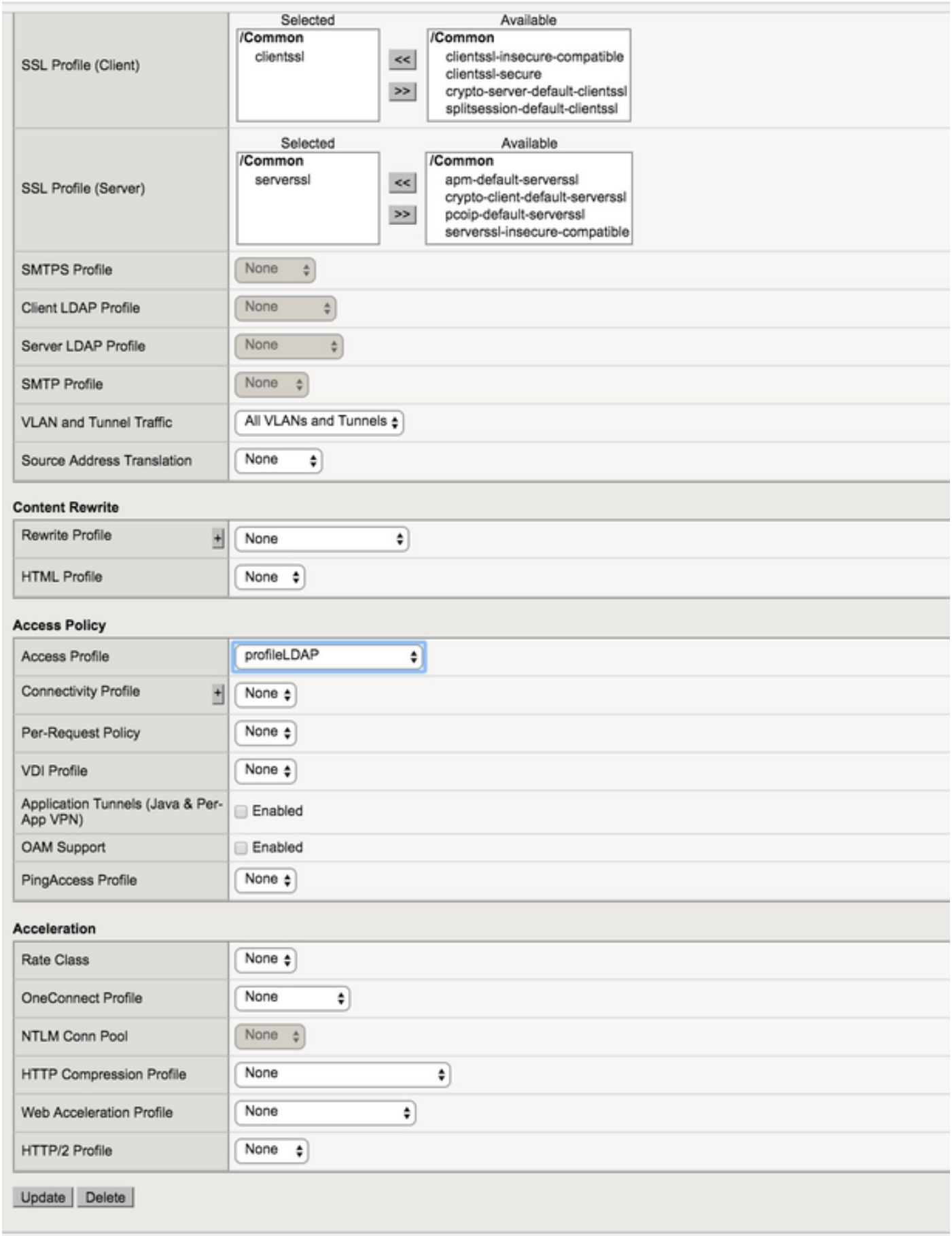

General Properties
Name
profileLDAP
Partition / Path
Common
Parent Profile
access
Profile Type
All
Profile Scope
Virtual Server
Settings
Inactivity Timeout
30
seconds
Access Policy Timeout
30
seconds
Maximum Session Timeout
30
seconds
Minimum Authentication Failure Delay
2
seconds
Maximum Authentication Failure Delay
5
seconds
Max Concurrent Users
5
Max Sessions Per User
2
Max In Progress Sessions Per Client IP
128
Restrict to Single Client IP
Use HTTP Status 503 for Error Pages
Configurations
Logout URI Include
URI
Add
Edit
Delete
Logout URI Timeout
5
seconds
Microsoft Exchange
None
User Identification Method
HTTP
OAuth Profile
None
Language Settings
Additional Languages
Afar (aa)
Add
Languages
Accepted Languages
English (en)
<<
Factory Builtin Languages
Japanese (ja)
Chinese (Simplified) (zh-cn)
Chinese (Traditional) (zh-tw)
Korean (ko)
Spanish (es)
French (fr)

- 创建一个虚拟服务器

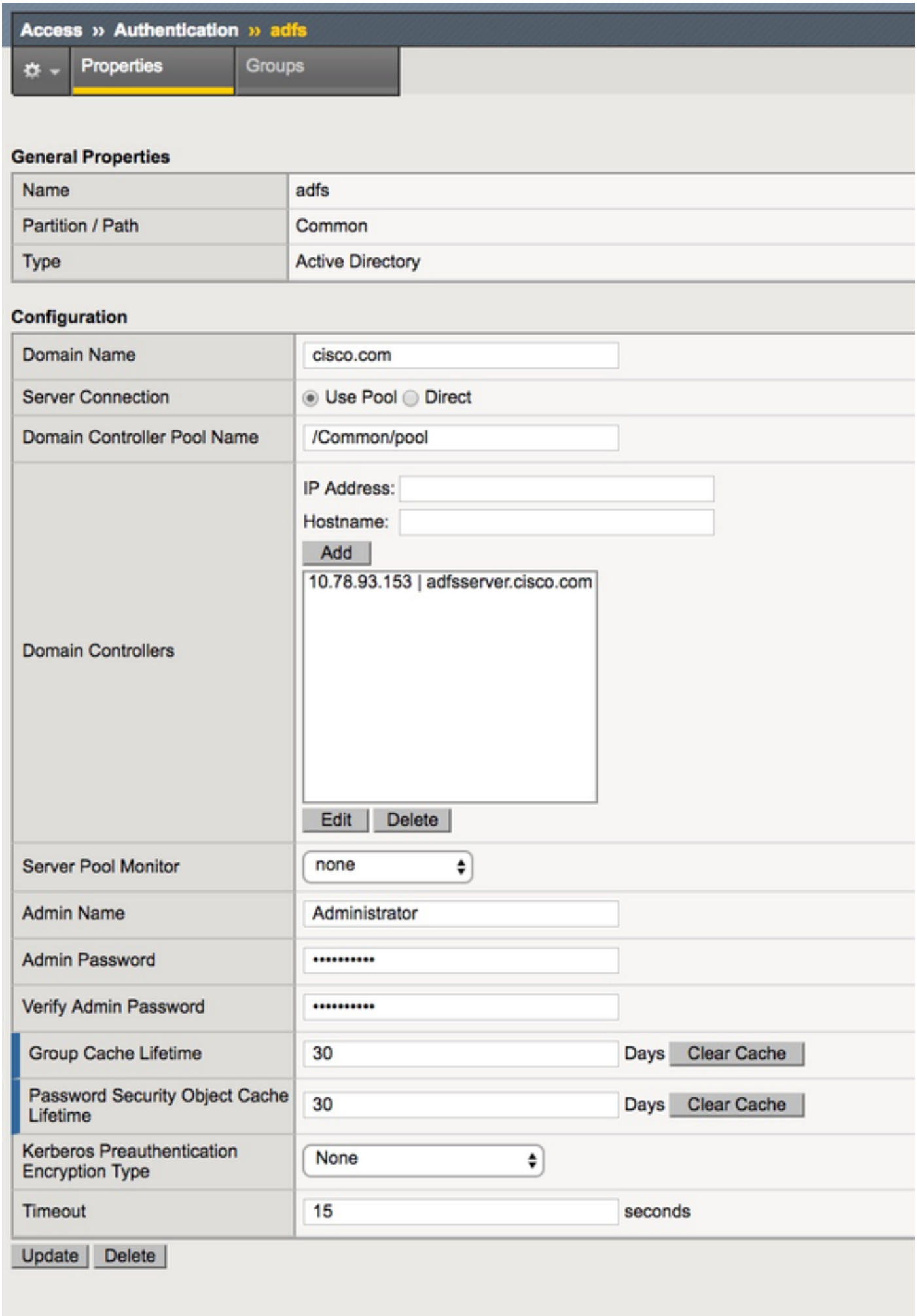
General Properties

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

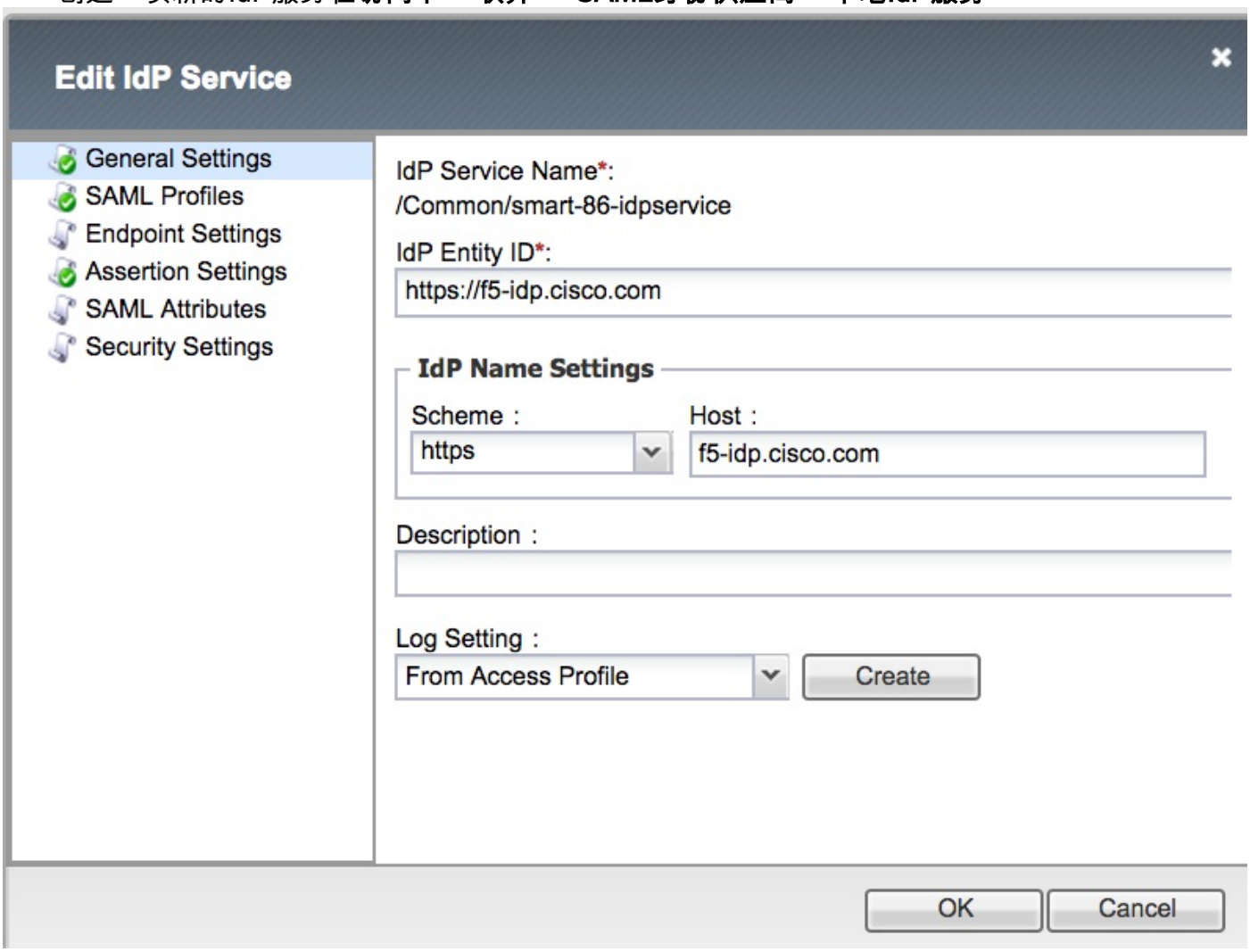
Configuration: Basic

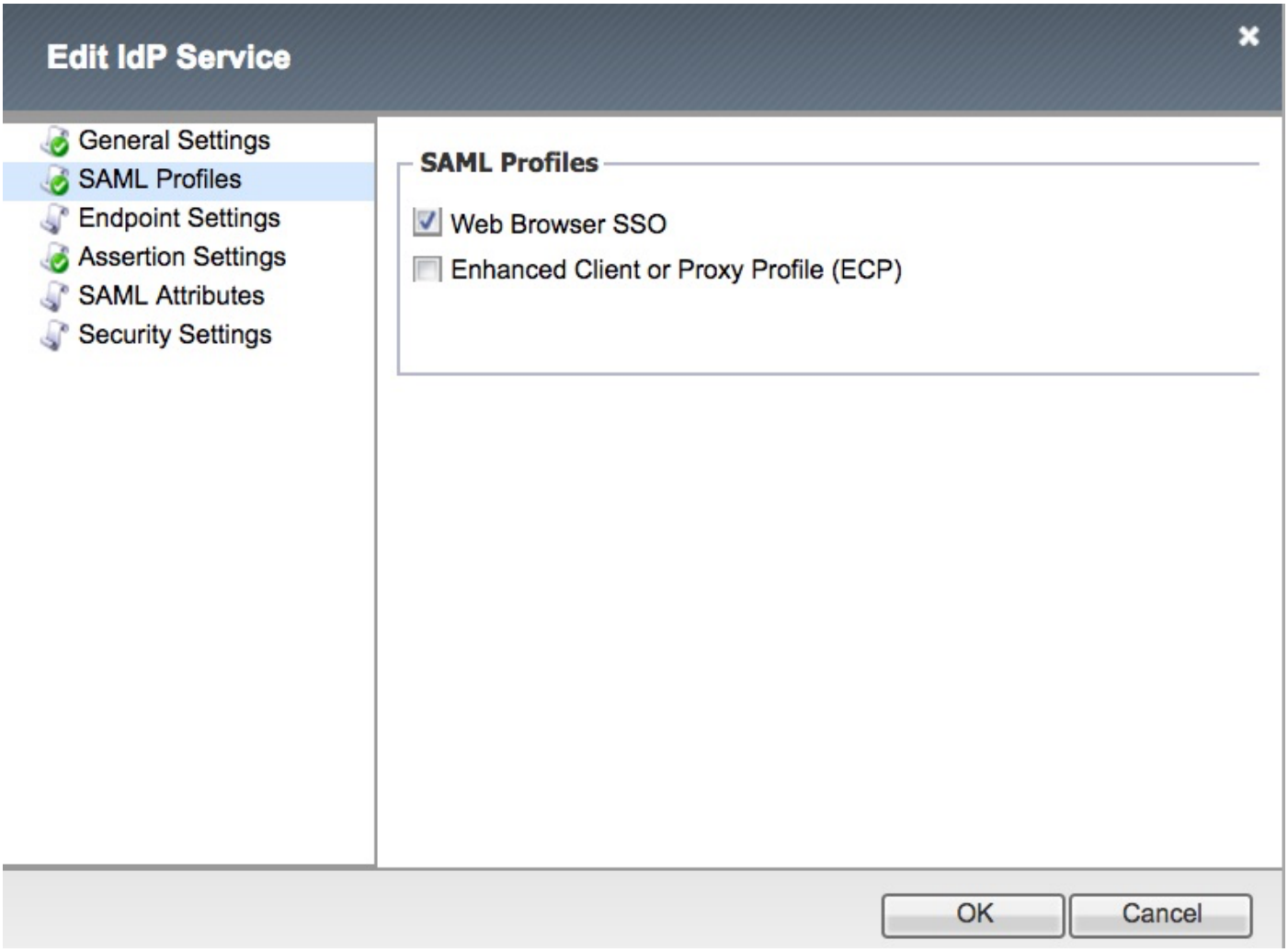


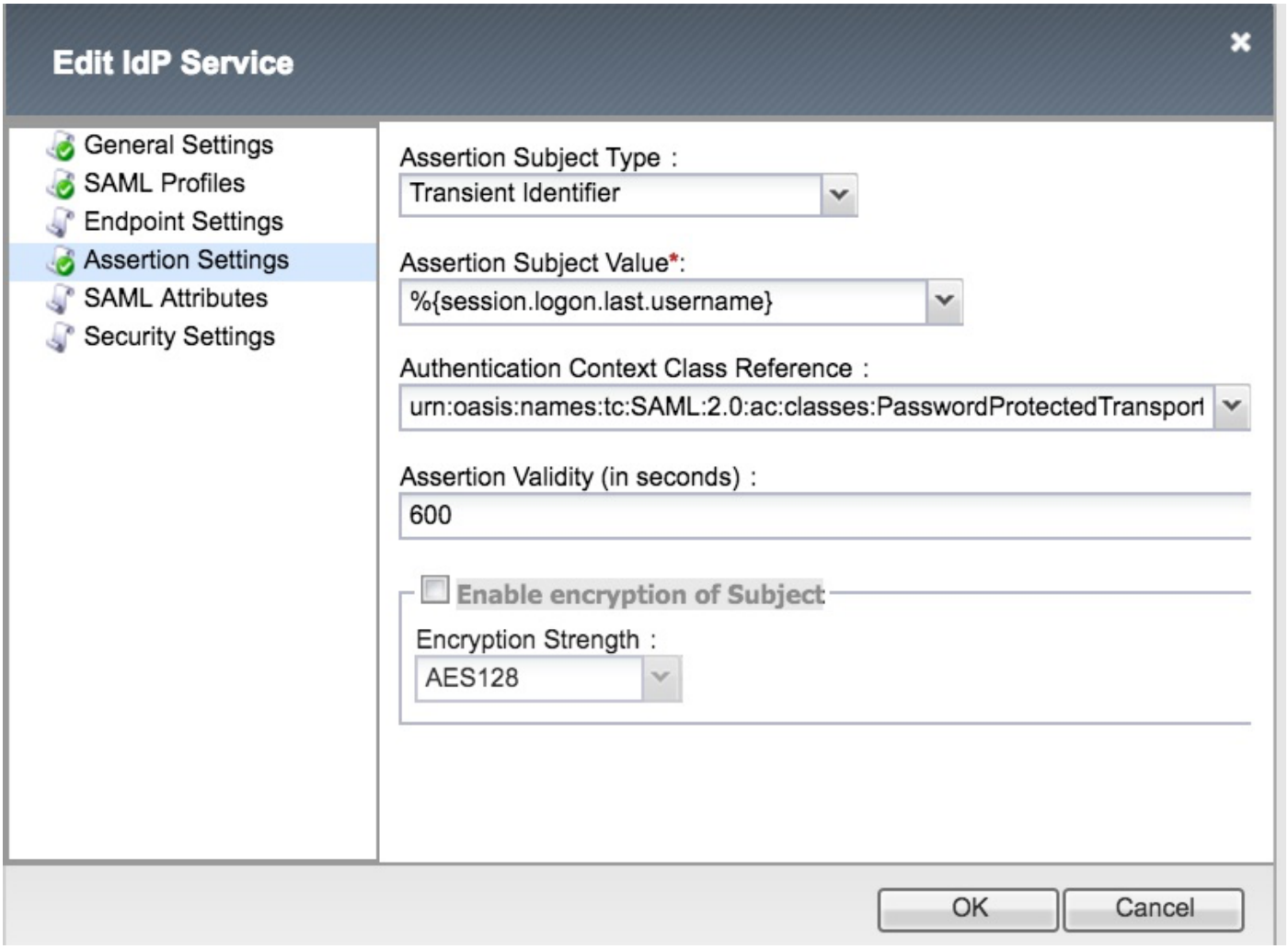
- 添加激活目录(AD)详细资料在**访问下- >认证- >激活目录**


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

- 创建一项新的IdP服务在**访问下- >联邦- > SAML身份供应商- >本地IdP服务**




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



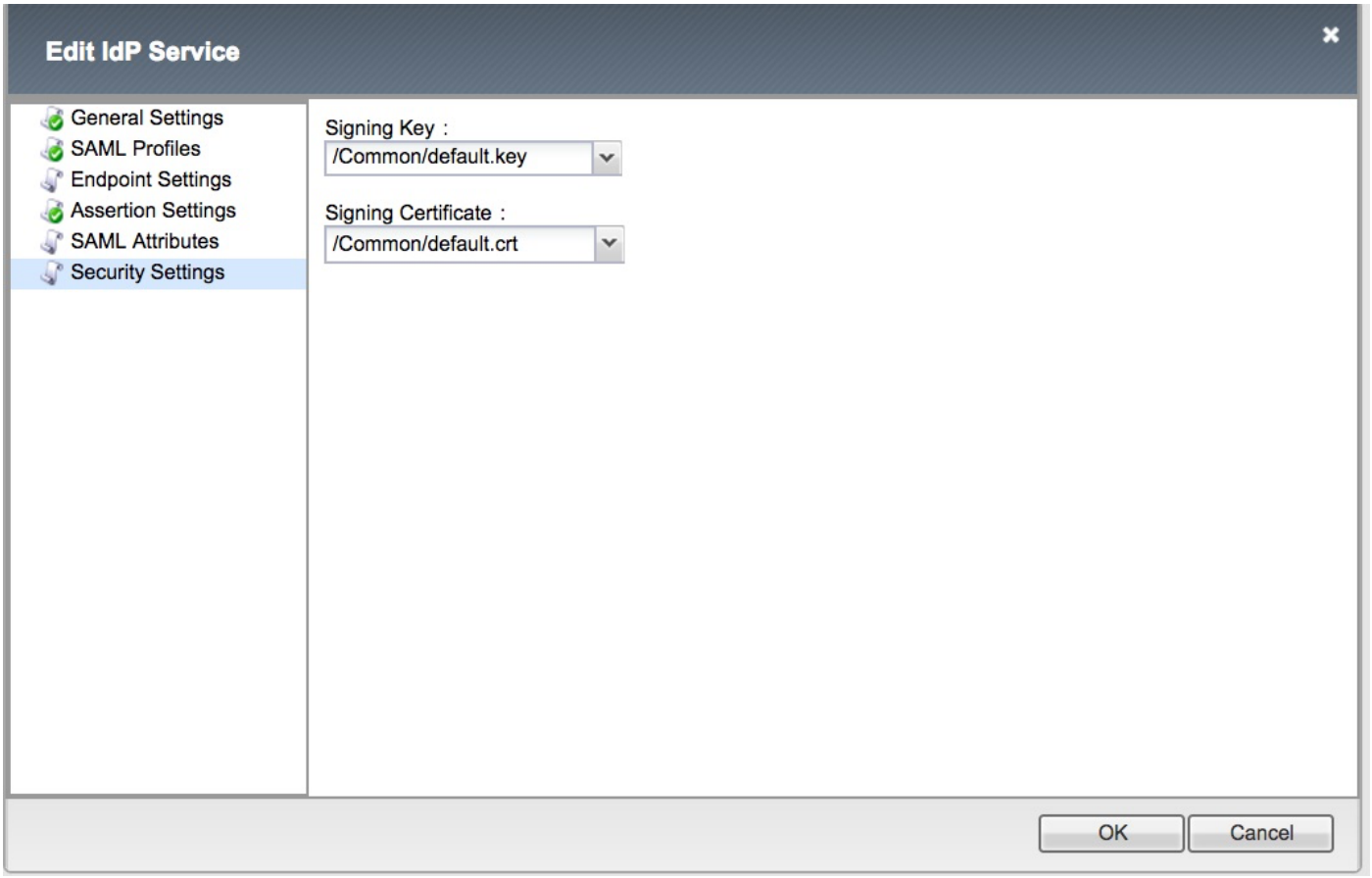
Note:如果一个普通的访问卡(CAC)使用认证，这些属性需要被添加在**SAML归因于**配置部分：

步骤1.创建**uid**属性。

名字：uid
值：% {session.ldap.last.attr.sAMAccountName}

步骤2.创建**user_principal**属性。

名字：user_principal
值：% {session.ldap.last.attr.userPrincipalName}

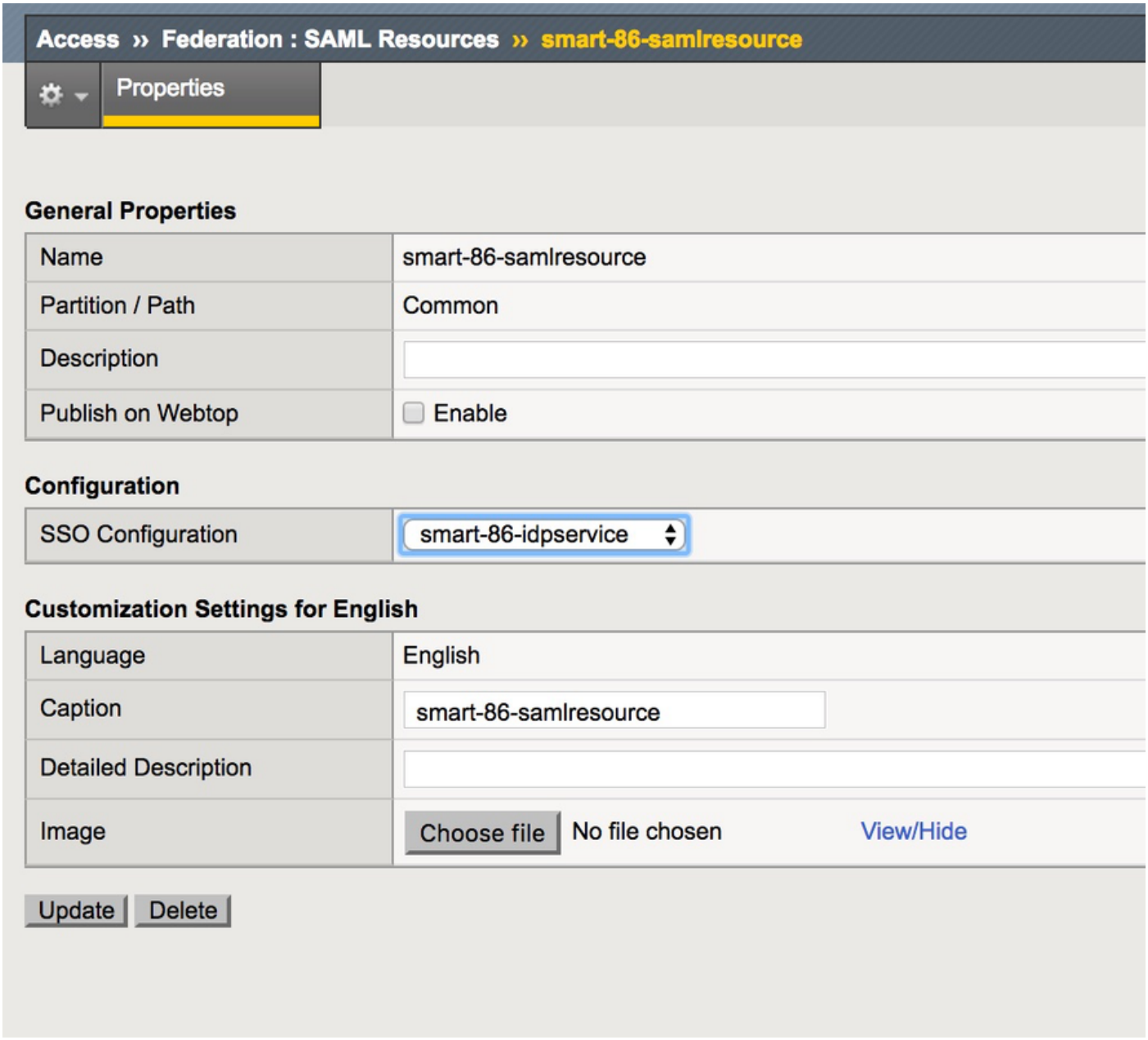


Note:一旦IdP服务被创建，有下载与Export按钮**元数据的**元数据的选项在**访问下- >联邦- > SAML身份供应商- >本地IdP服务**

安全主张标记语言(SAML)创建

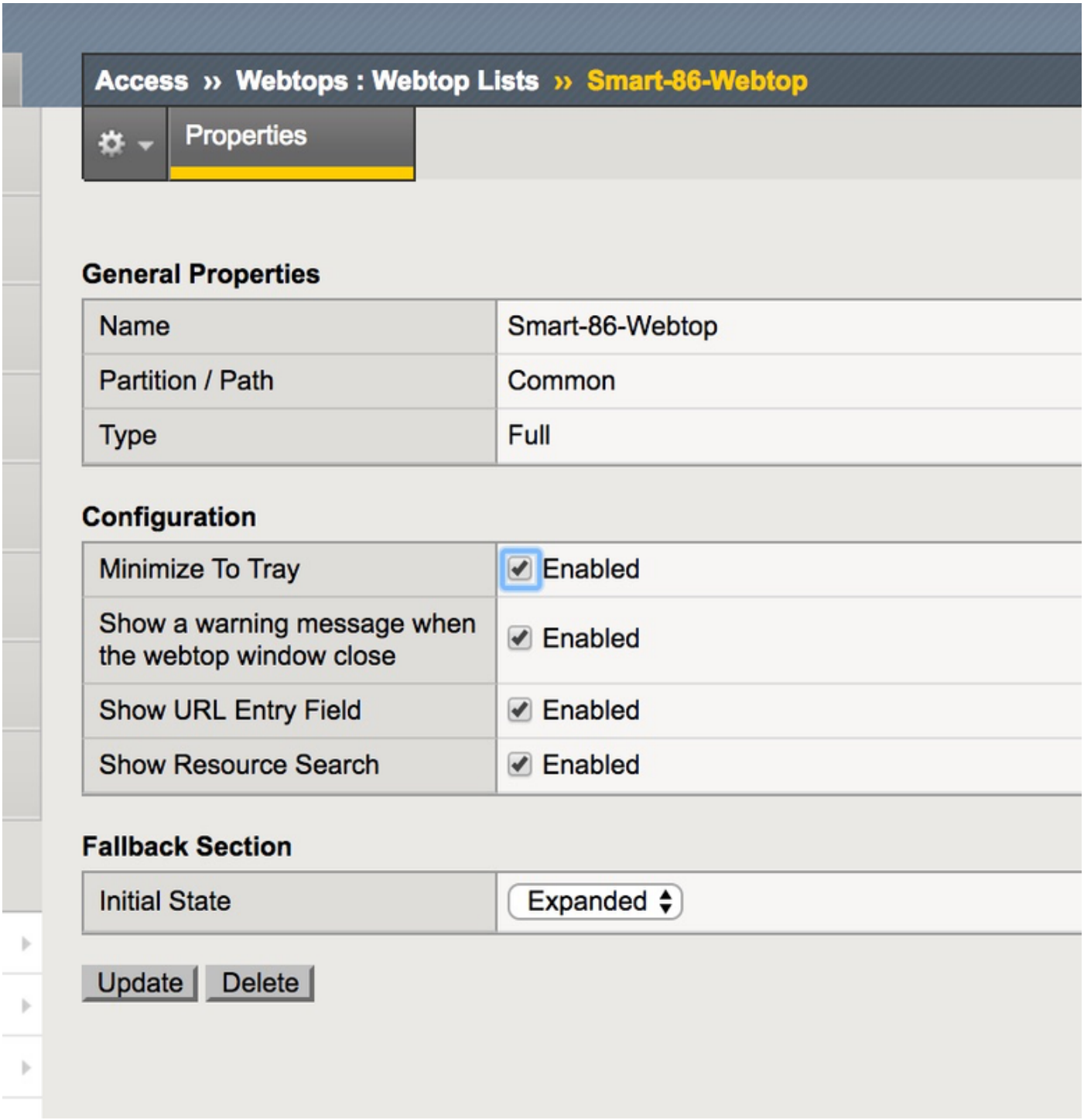
SAML资源

- 连接**访问- >联邦- > SAML资源**和创建saml资源与被创建前的IdP服务产生关联



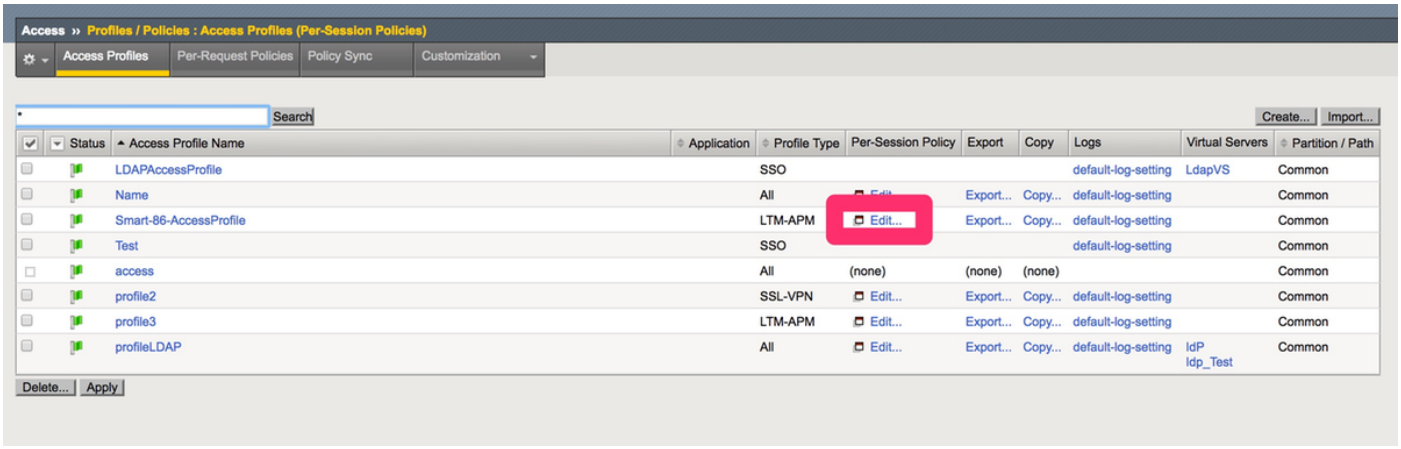
Webtops

- 创建一webtop在**访问下- > Webtops**

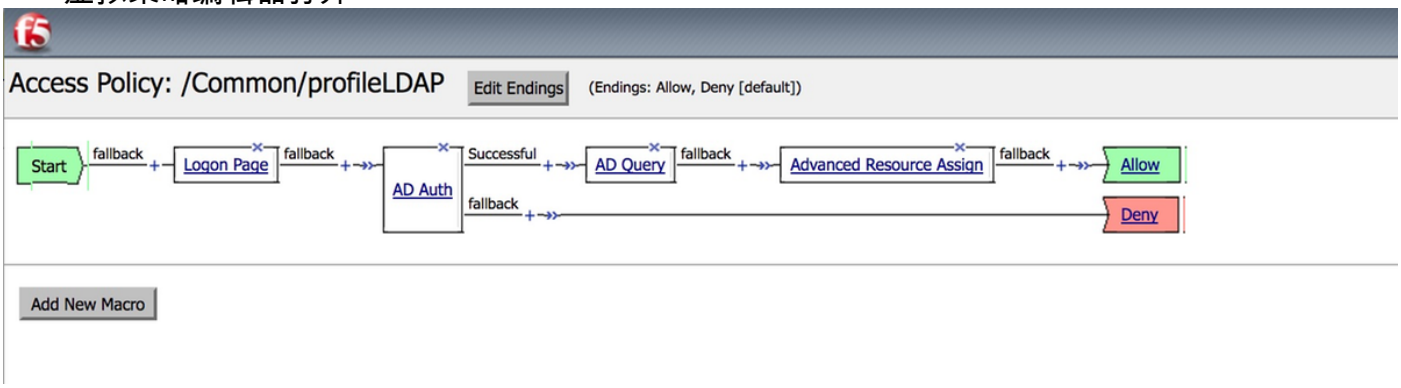


虚拟策略编辑器

- 连接对及早被创建的策略并且点击编辑链路



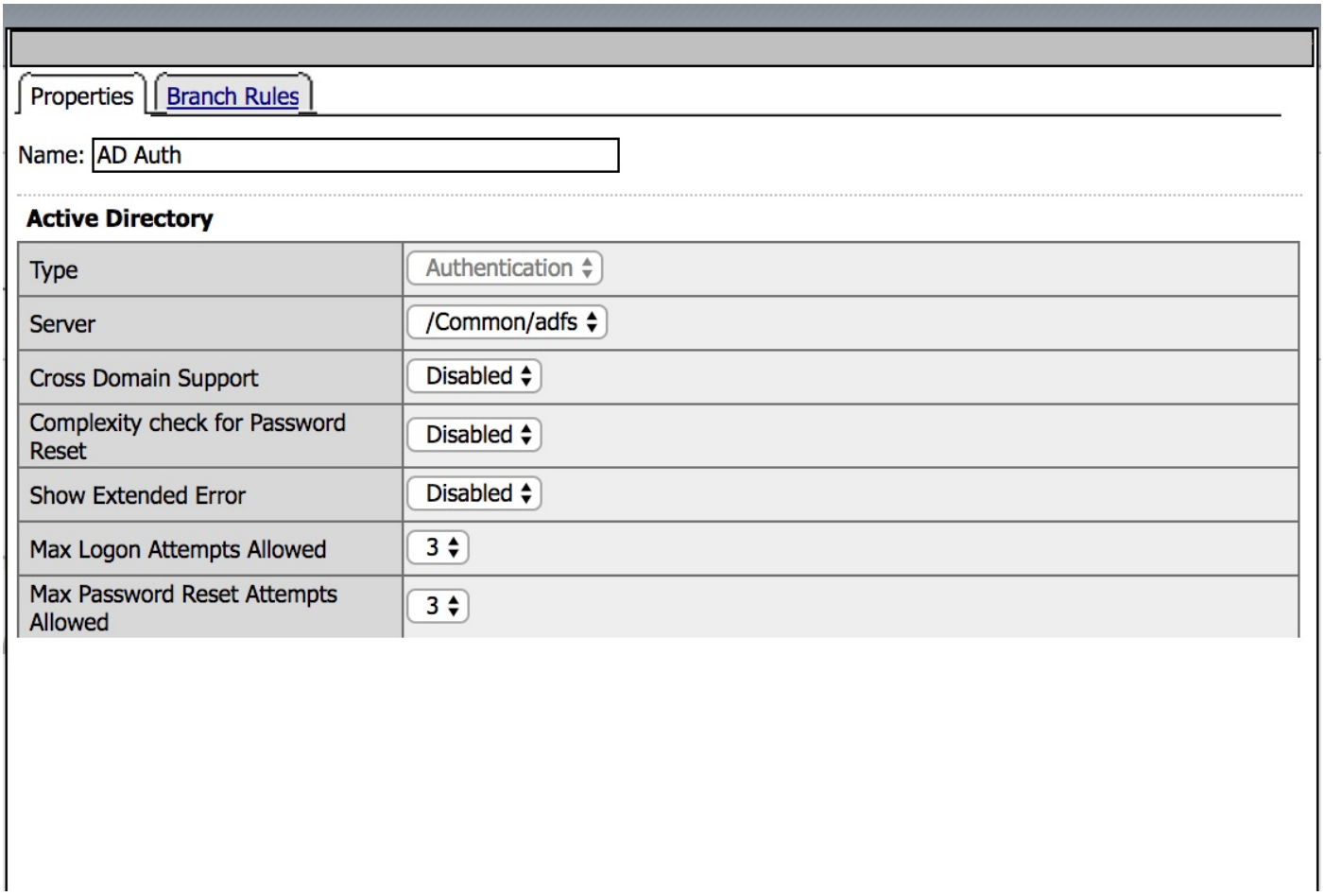
- 虚拟策略编辑器打开



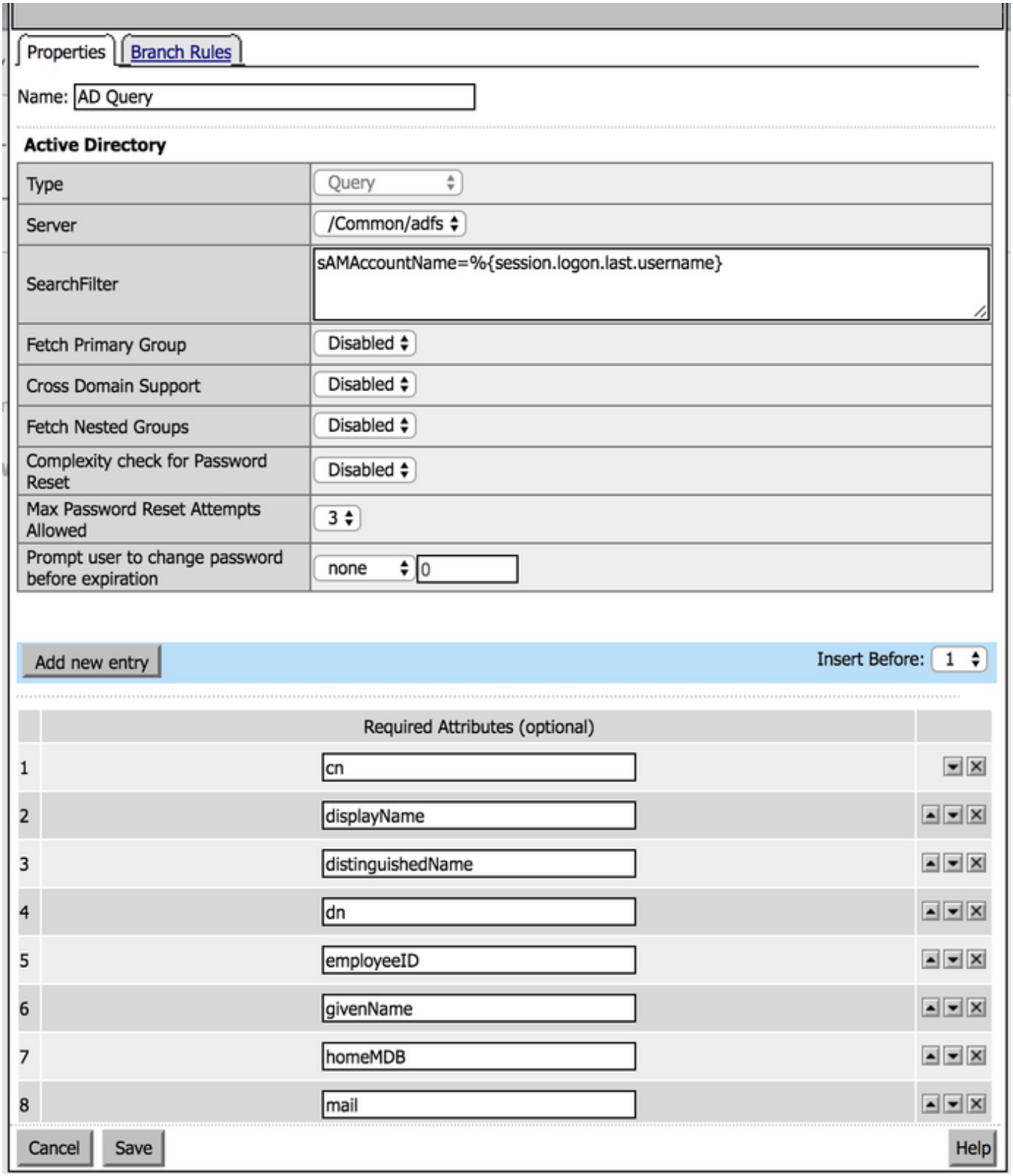
- 点击  图标并且添加元素如所描述

步骤1.**登录页元素**-留下所有元素默认。

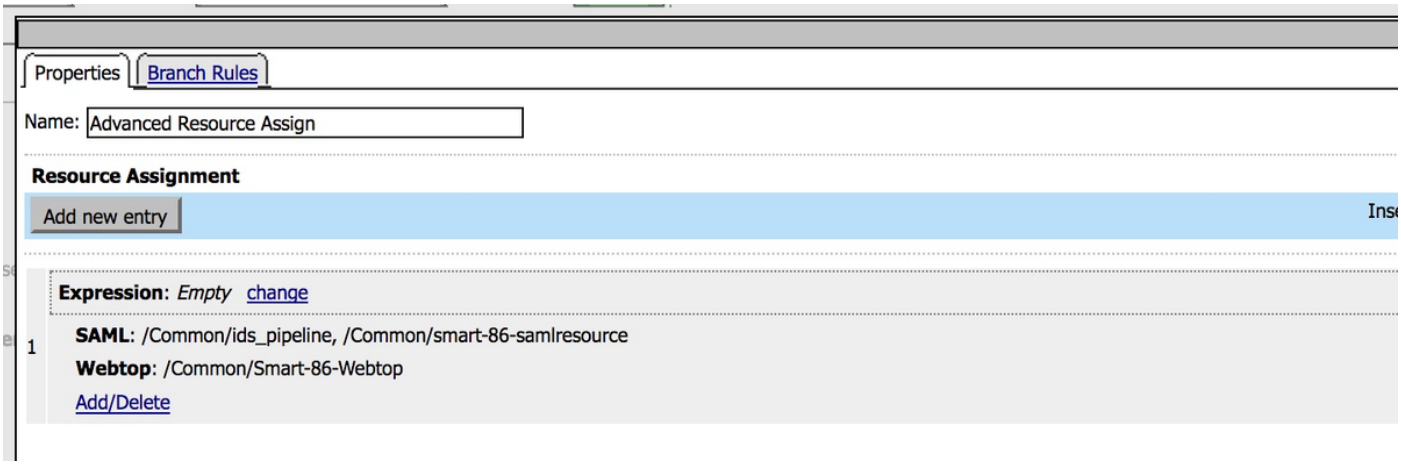
步骤2. **AD Auth** - >请选择被创建的ADFS配置前。



步骤3. **AD查询元素**-分配必要的详细资料。



步骤4.**预先的资源分配-关联被创建的saml资源和webtop前。**



服务提供商(SP)元数据Exchange

- 请手工导入ID的认证大IP通过**系统**- > Certificate Management - > Traffic Management

  Note:保证认证包括开始认证和END认证标记。

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

- 创建从sp.xml的一个新的条目在Access-> Federation-> SAMLIDENTITY**供应商下- >** ExternalSP**连接器**
- 捆绑SP连接器对IdP服务在**访问下- >联邦- > SAML身份供应商- >本地IdP服务**

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

普通的访问卡(CAC)认证失败

如果SSO认证为CAC用户失效，请检查UCCX ids.log验证适当地设置SAML属性。

如果有配置问题， SAML故障发生。例如，在此日志片断， user_principal SAML属性在IdP没有被

配置。

YYYY-MM-DD hh **mm:**SS.sss GMT(-0000) [IdSEndPoints-SAML-59]com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:465 -retrievefrom**user_principal**

YYYY-MM-DD hh **mm:**SS.sss GMT(-0000) [IdSEndPoints-SAML-59]com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - SAML **responseprocessingfailed com.sun.identity.saml.common.SAMLException samluser_principal**

com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributeFromAttributesMap(IdSSAMLAsyncServlet.java:466)

com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet.java:263)

com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServlet.java:176)
com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
java.lang.Thread.run(Thread.java:745)

Related Information

- Technical Support & Documentation - Cisco Systems