# Installieren und Konfigurieren des F5 Identity Providers (IdP) für Cisco Identity Service (IDs) zur Aktivierung von SSO

## Inhalt



## Einführung

In diesem Dokument wird die Konfiguration des BIG-IP Identity Providers (IDP) F5 zur Aktivierung der einmaligen Anmeldung (Single Sign On, SSO) beschrieben.

#### Cisco IDS-Bereitstellungsmodelle

| Produkt | Bereitstellung |
|---|---|
| UCCX | Co-Resident |
| PCCE | Co-Resident mit CUIC (Cisco Unified Intelligence Center) und LD (Live-Daten) |
| UCCE | Resident gemeinsam mit CUIC und LD für 2.000 Bereitstellungen.<br>Standalone für 4.000- und 12.000-Bereitstellungen. |

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Contact Center Express (UCCX) Version 11.6 oder Cisco Unified Contact Center Enterprise Release 11.6 oder Packaged Contact Center Enterprise (PCCE) Release 11.6.

**Hinweis**: Dieses Dokument bezieht sich auf die Konfiguration des Cisco Identify Service (IDs) und des Identitätsanbieters (IdP). Das Dokument verweist in den Screenshots und Beispielen auf UCCX, die Konfiguration ähnelt jedoch dem Cisco Identitify Service (UCCX/UCCE/PCCE) und der IdP.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Installieren

Big-IP ist eine Paketlösung mit mehreren Funktionen. Zugriffsrichtlinien-Manager (APM), der sich auf den Identity Provider-Service bezieht.

Big-IP als APM:

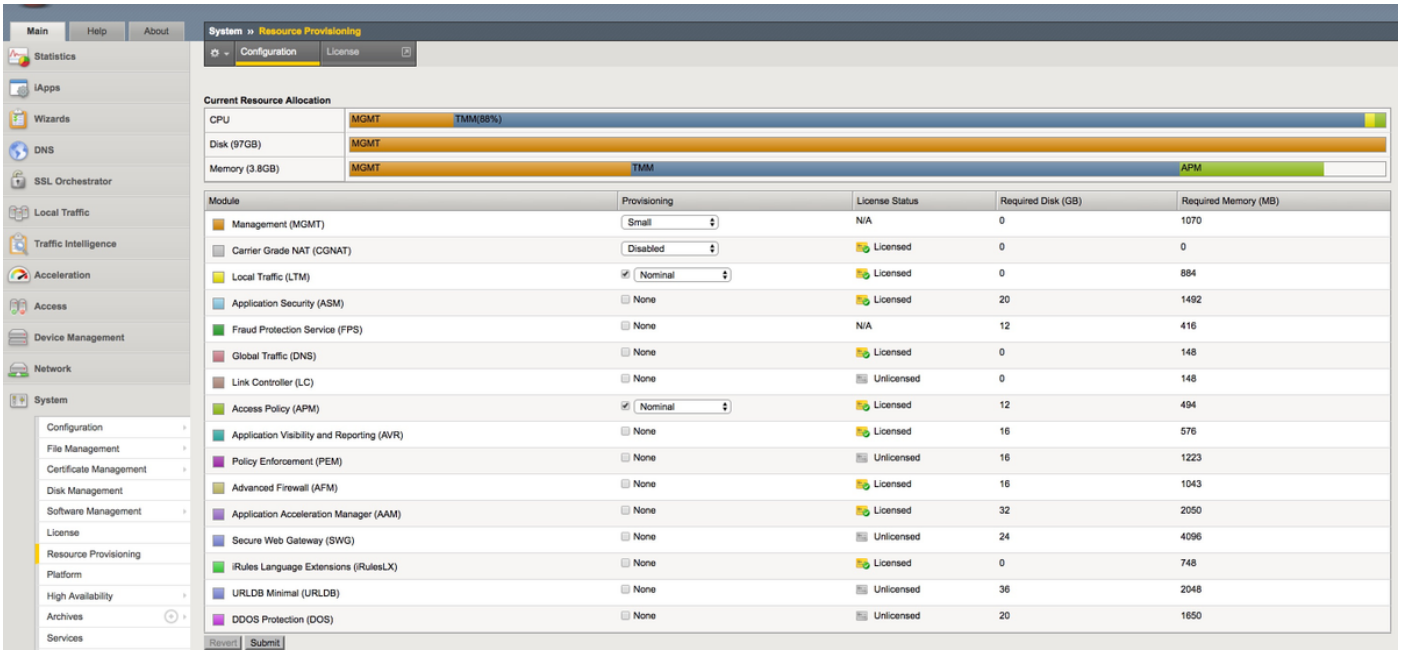
| | |
|---|---|
| Version | 13,0 |
| Typ | Virtual Edition (OVA) |
| IPs | Zwei IPs in verschiedenen Subnetzen. Eine für die Verwaltungs-IP und eine für den virtuellen IDP-Server |

Laden Sie das virtuelle Edition-Image von der Big-IP-Website herunter, und stellen Sie die OVA bereit, um ein vorinstalliertes virtuelles System (VM) zu erstellen. Erwerben Sie die Lizenz, und installieren Sie sie mit den grundlegenden Anforderungen.

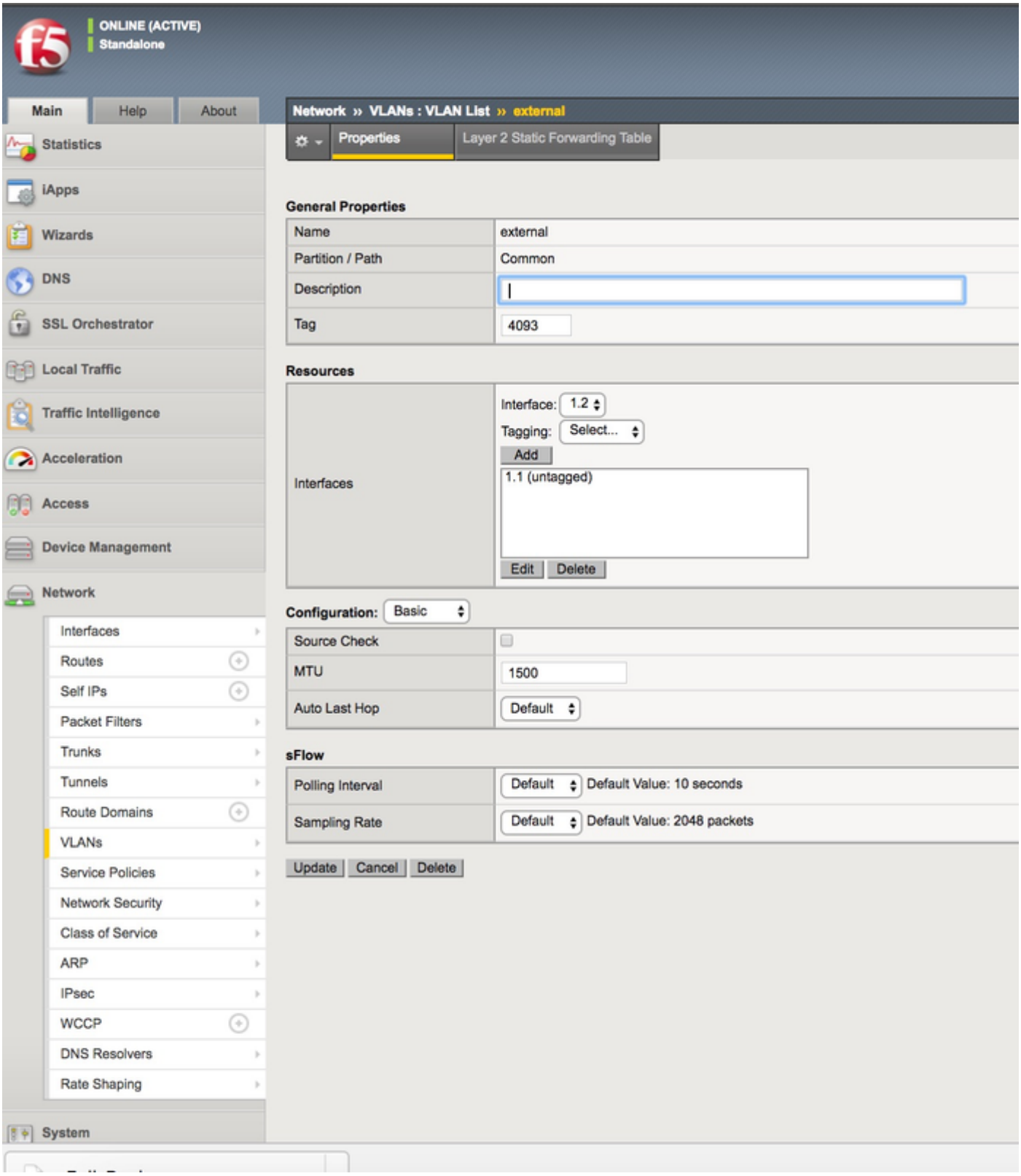
**Hinweis**: Informationen zur Installation finden Sie in der Big-IP-Installationsanleitung.

## Konfigurieren

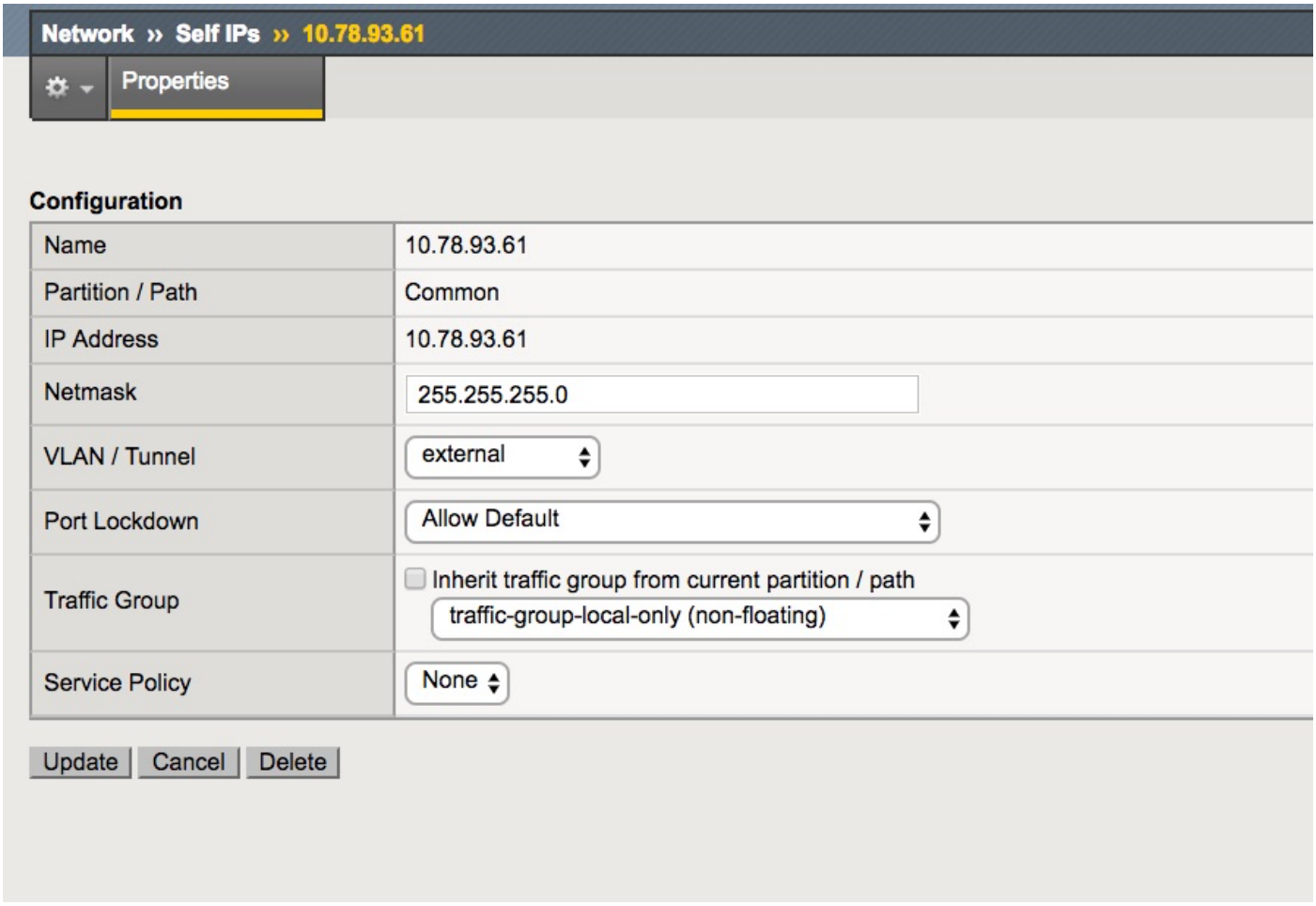
- Navigieren Sie zu Ressourcenbereitstellung, aktivieren Sie **Zugriffsrichtlinien**, und legen Sie die Bereitstellung auf **Nominal fest.**



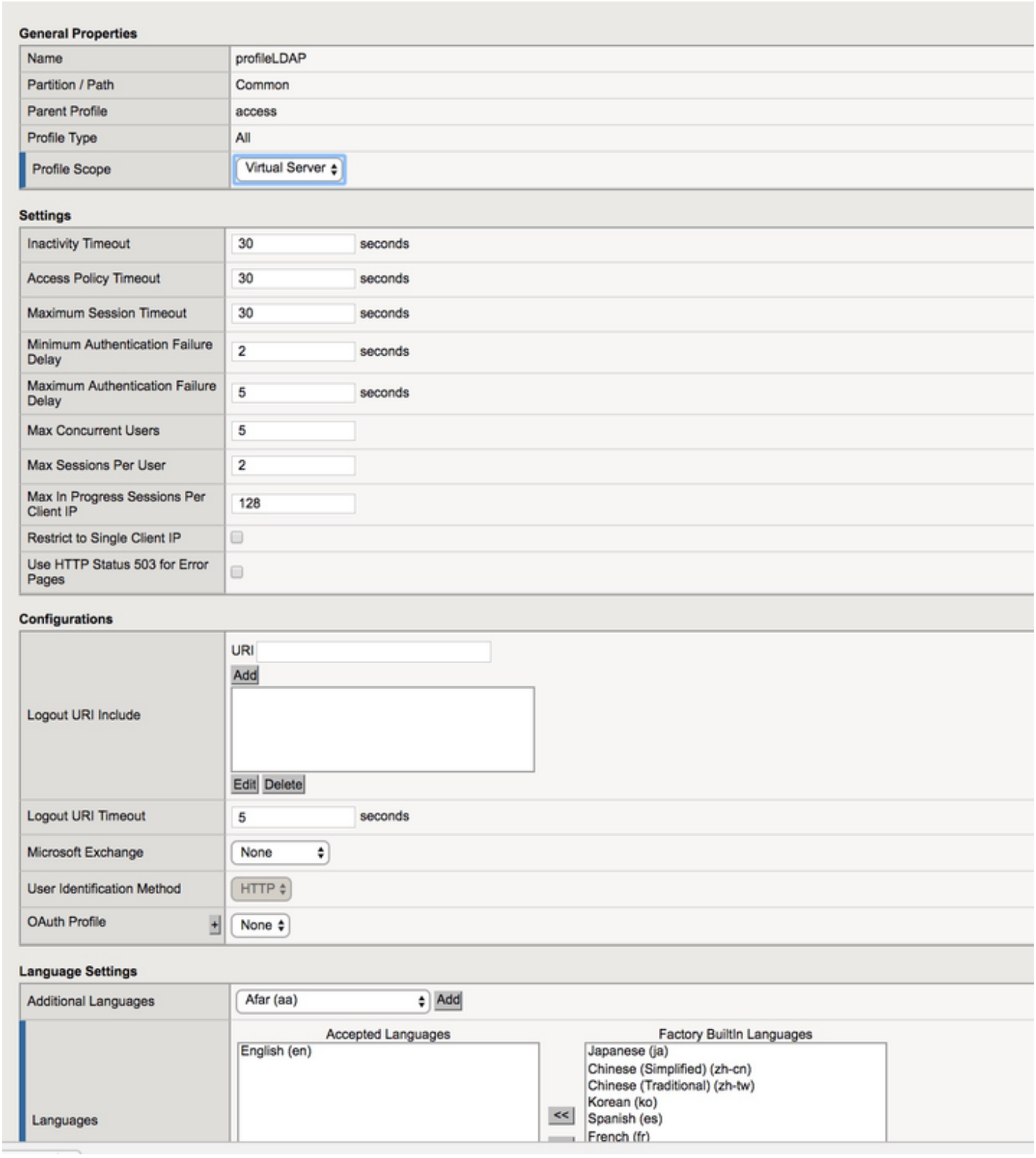

- Erstellen eines neuen VLAN unter **Netzwerk** -> **VLANs**




- Erstellen Sie einen neuen Eintrag für die IP, der für die IDP unter **Netzwerk -> Self IPs** verwendet wird.




- Erstellen Sie ein Profil unter **Access** -> **Profile/Policies** -> **Access-Profile.**

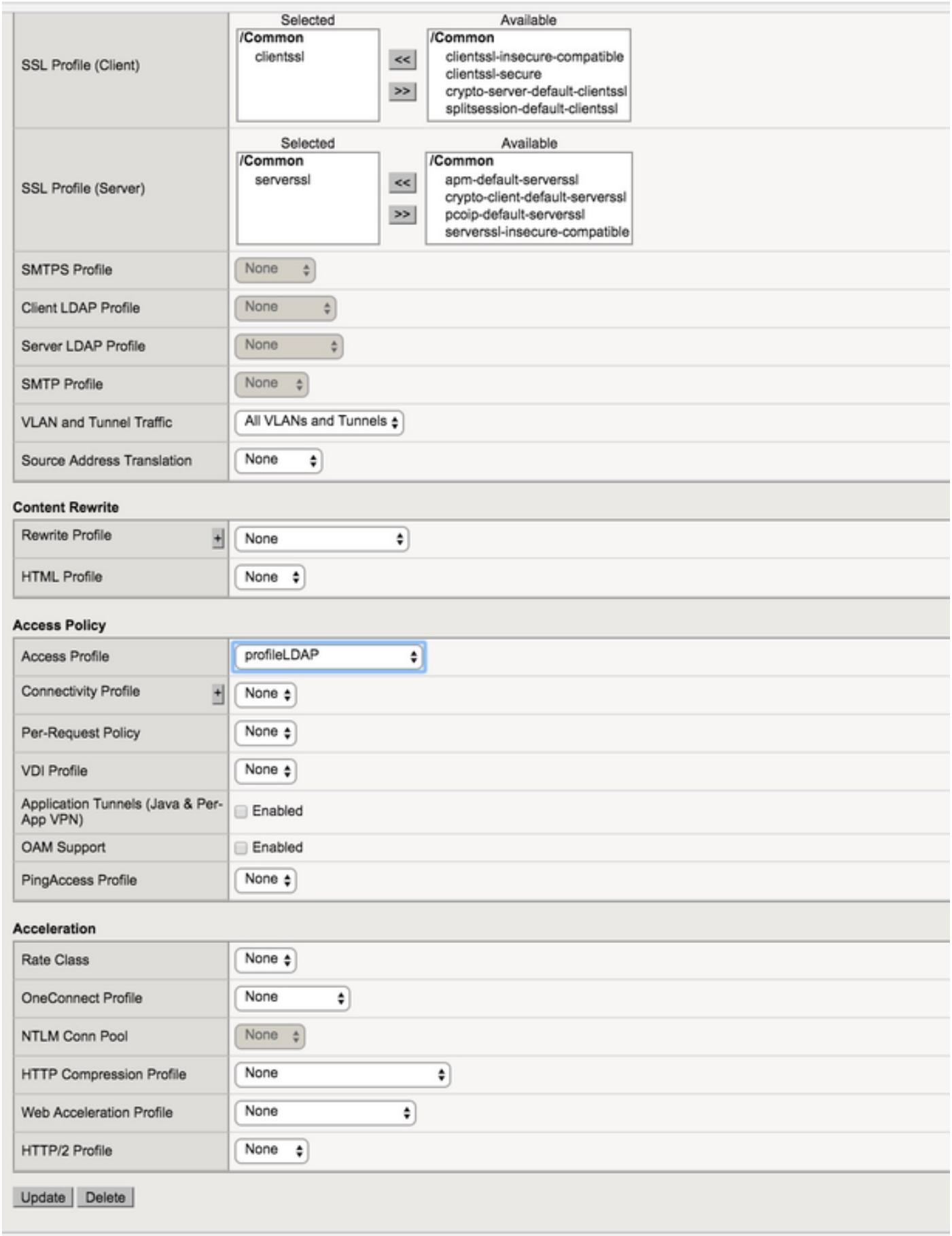



- Erstellen eines virtuellen Servers

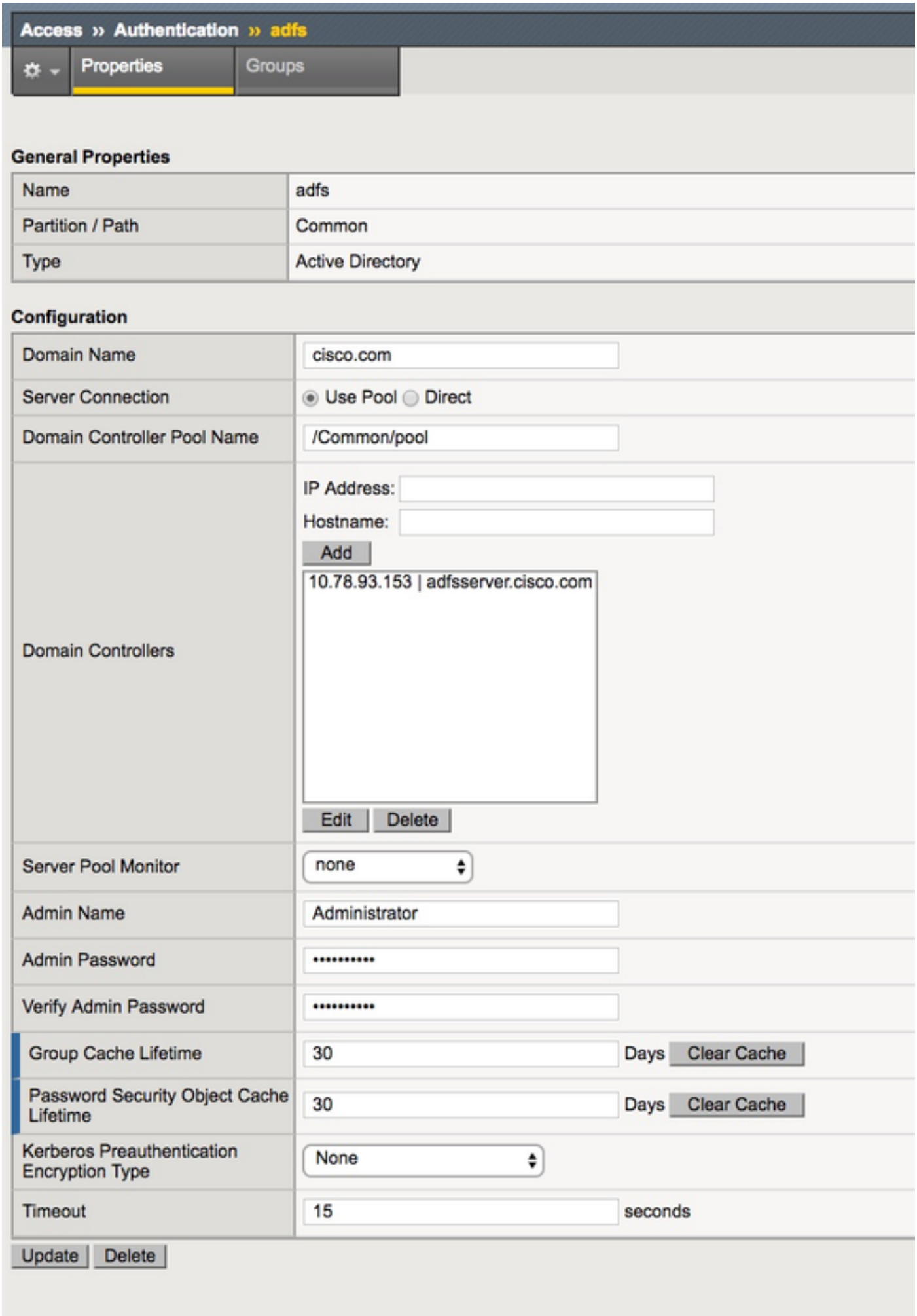
**General Properties**

| | |
|---|---|
| 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 |

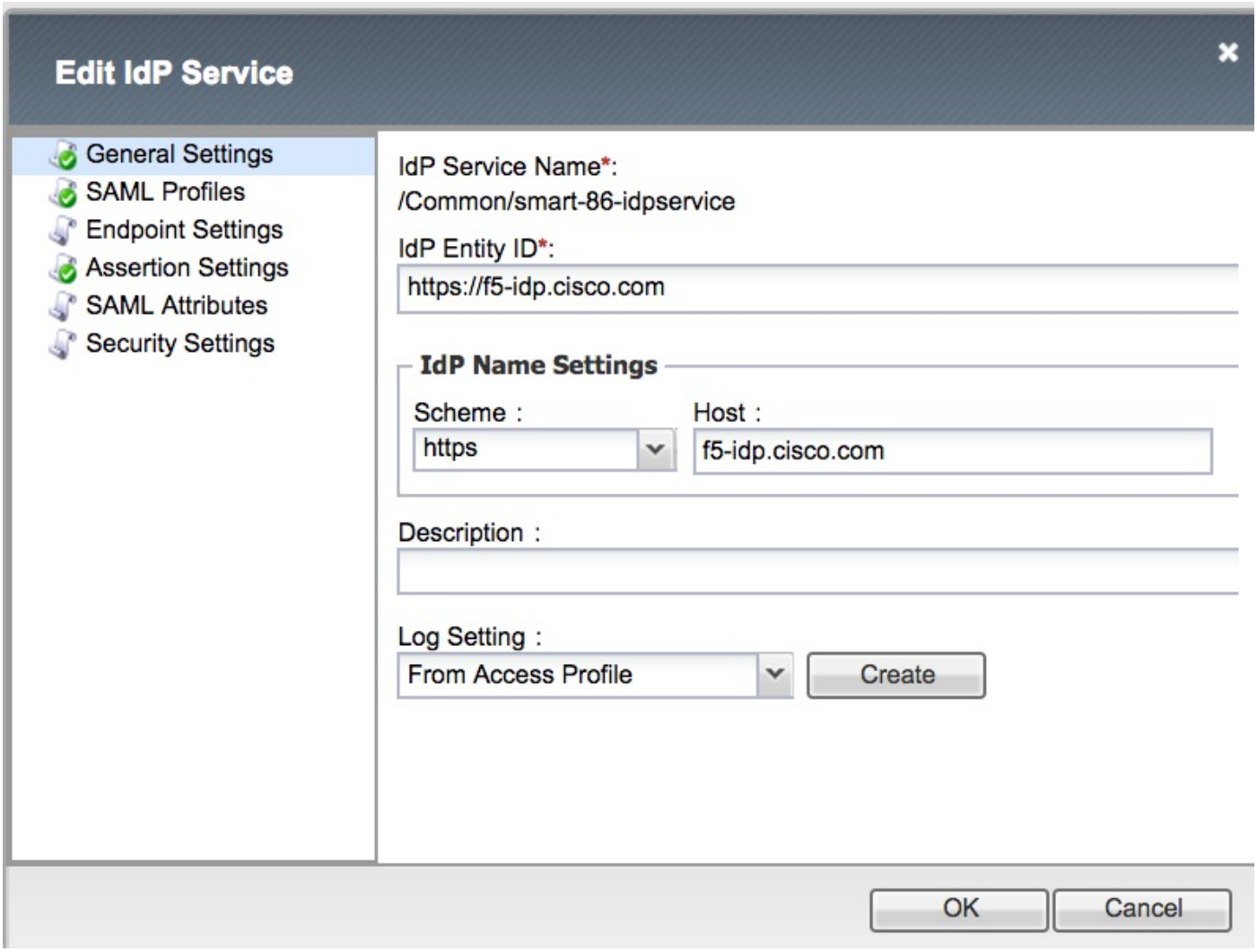
**Configuration:** Basic

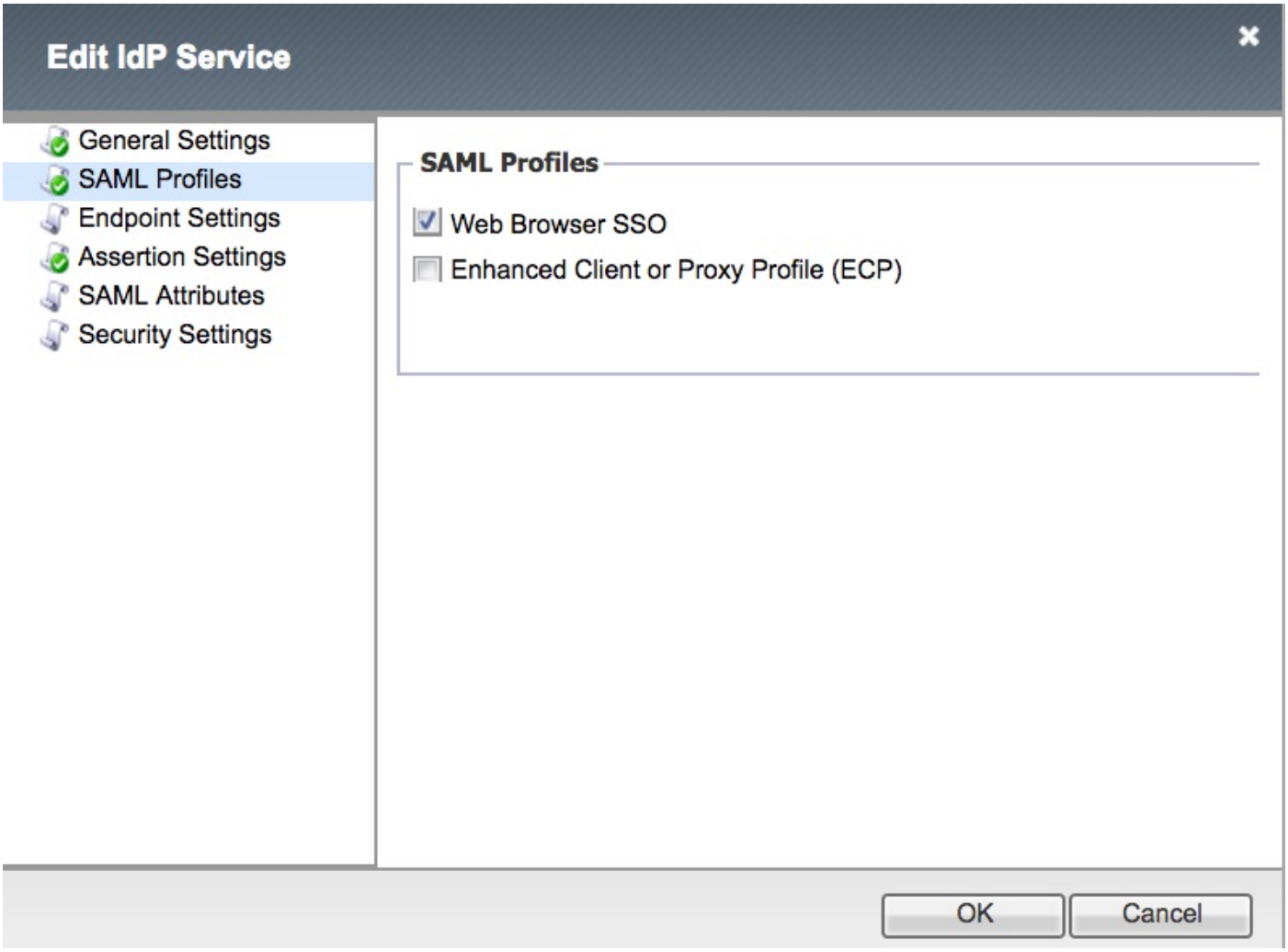


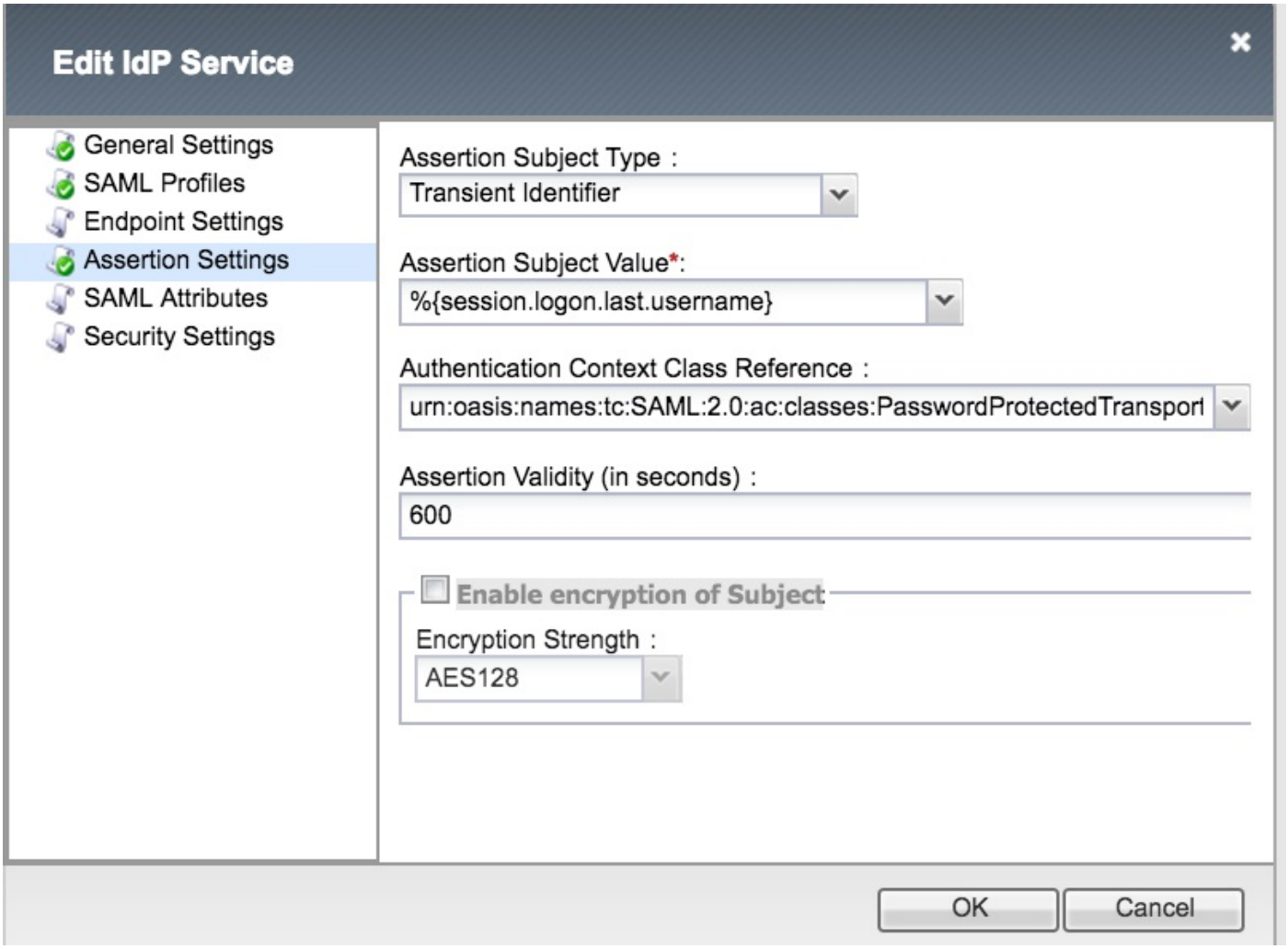

- Hinzufügen von Active Directory (AD)-Details unter **Access** -> **Authentication** -> **Active Directory**


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

- Erstellen Sie einen neuen IDP-Service unter **Access -> Federation -> SAML Identity Provider -> Local IdP Services.**




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



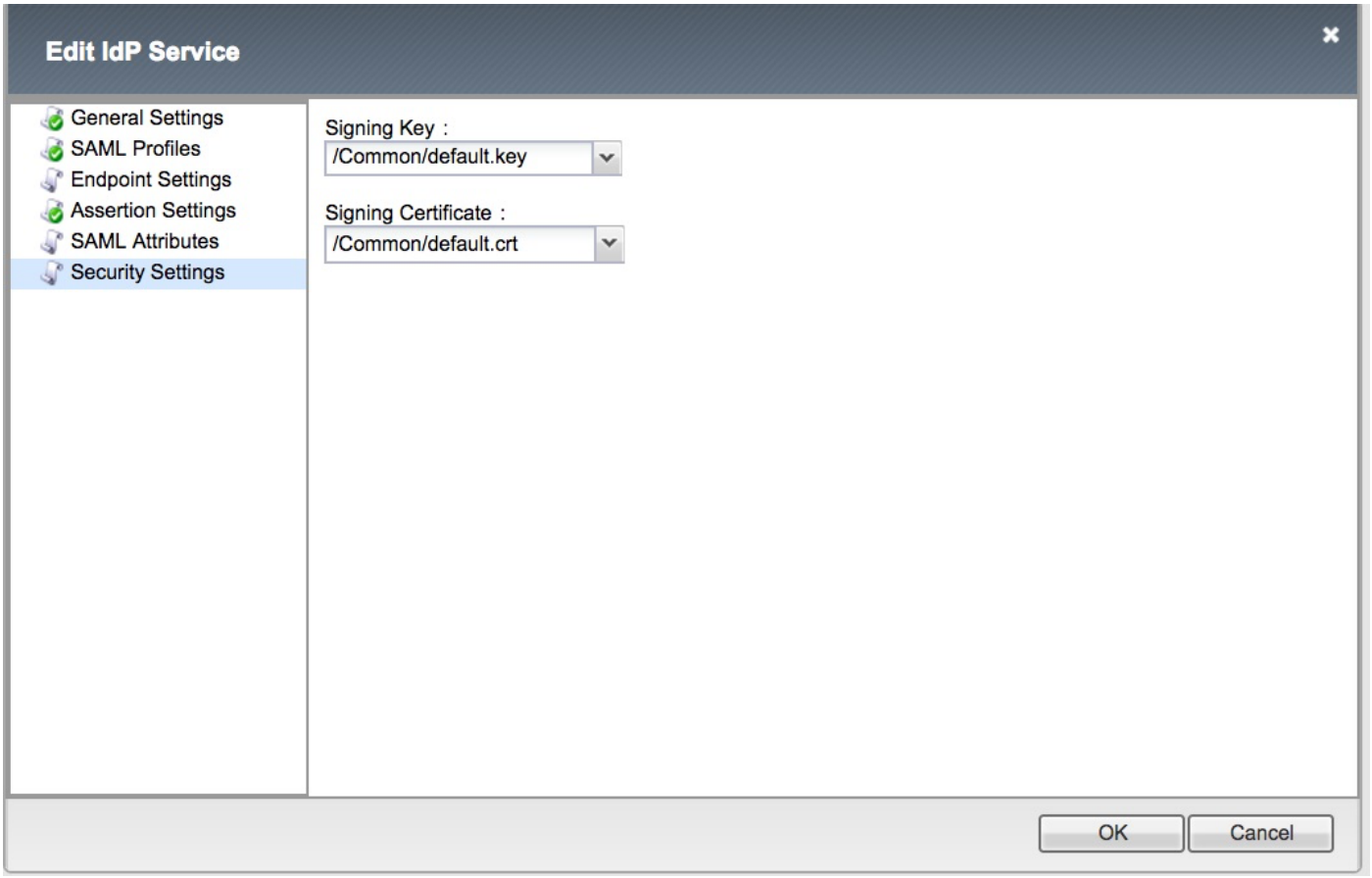

**Hinweis**: Wenn eine Common Access Card (CAC) für die Authentifizierung verwendet wird, müssen diese Attribute im Konfigurationsabschnitt **SAML Attributes** hinzugefügt werden:

Schritt 1: Erstellen des **uid-**Attributs**.**

**Name:** uid
**Wert:** %{session.ldap.last.attr.sAMAccountName}

Schritt 2: Erstellen Sie das **user_main-**Attribut.

**Name:** Benutzer_Principal
**Wert:** %{session.ldap.last.attr.userPrincipalName}

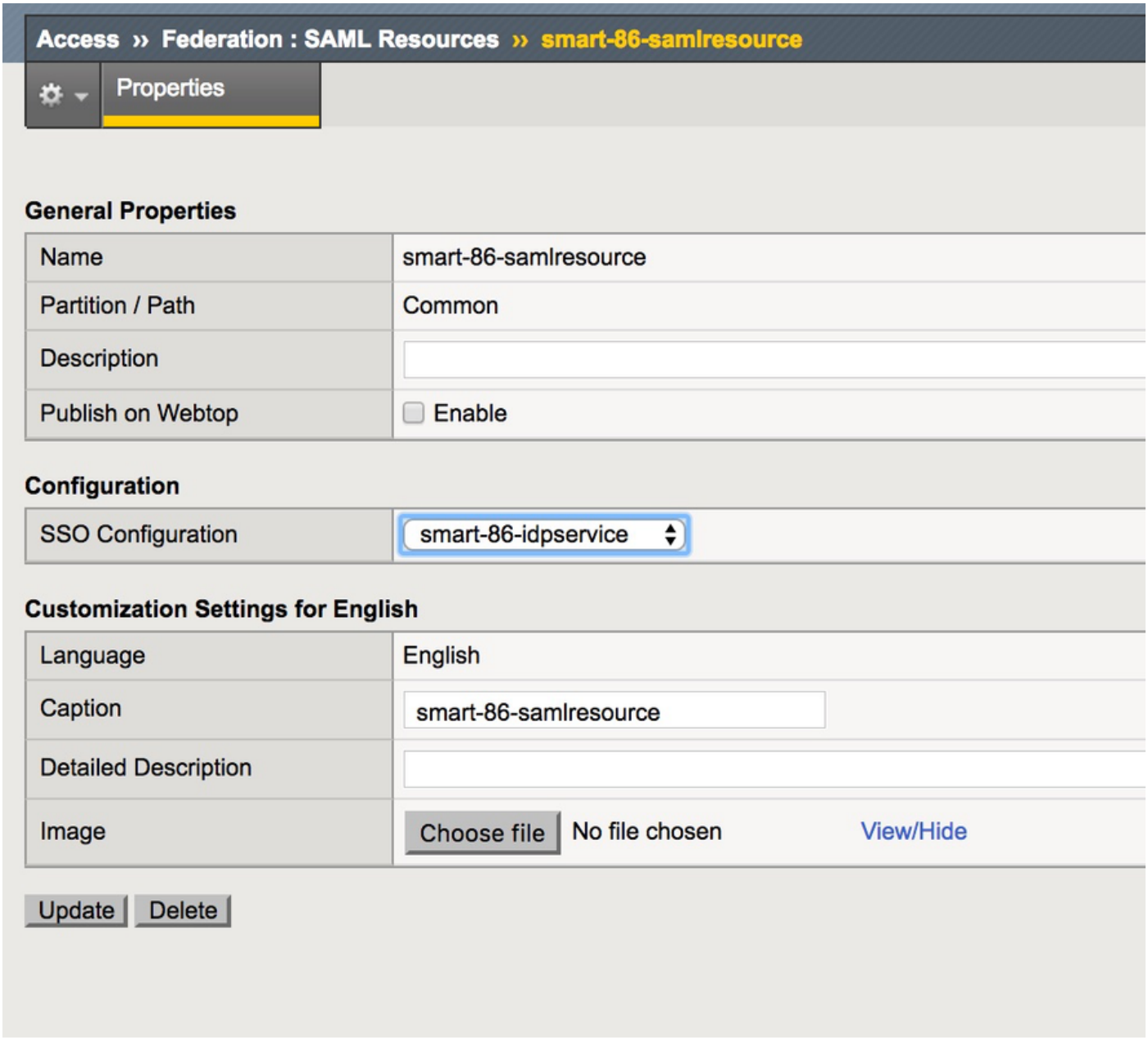



**Hinweis**: Nach dem Erstellen des IDP-Service gibt es eine Option zum Herunterladen der Metadaten mit einer Schaltfläche **Metadaten exportieren** unter **Access** -> **Federation** -> **SAML Identity Provider** -> **Local IdP Services.**

## Erstellung von Security Assertion Markup Language (SAML)

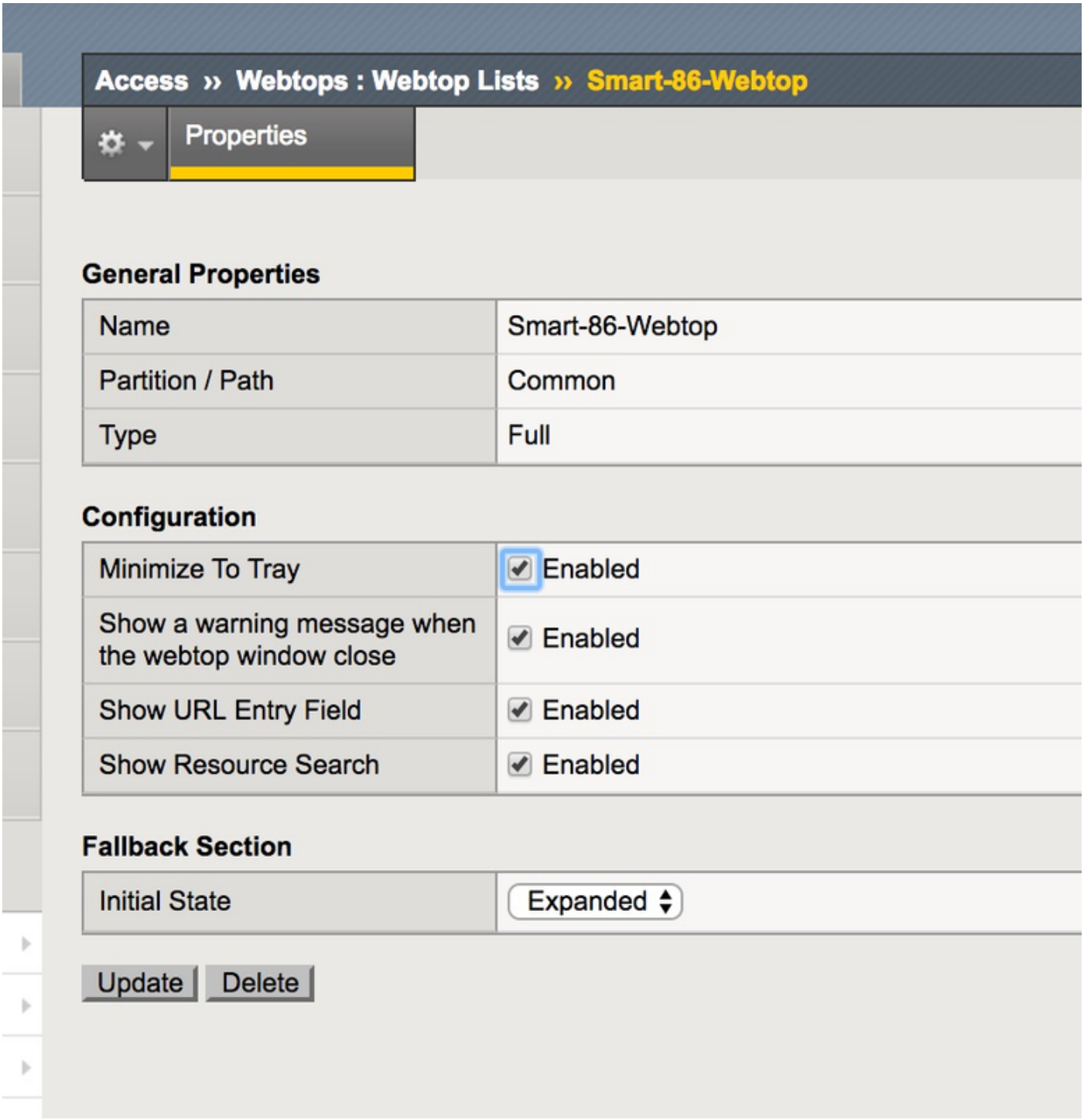
### SAML-Ressourcen

- Navigieren Sie zu **Access** -> **Federation** -> **SAML Resources**, und erstellen Sie eine einfache Ressource für die Verknüpfung mit dem zuvor erstellten IDP-Dienst.



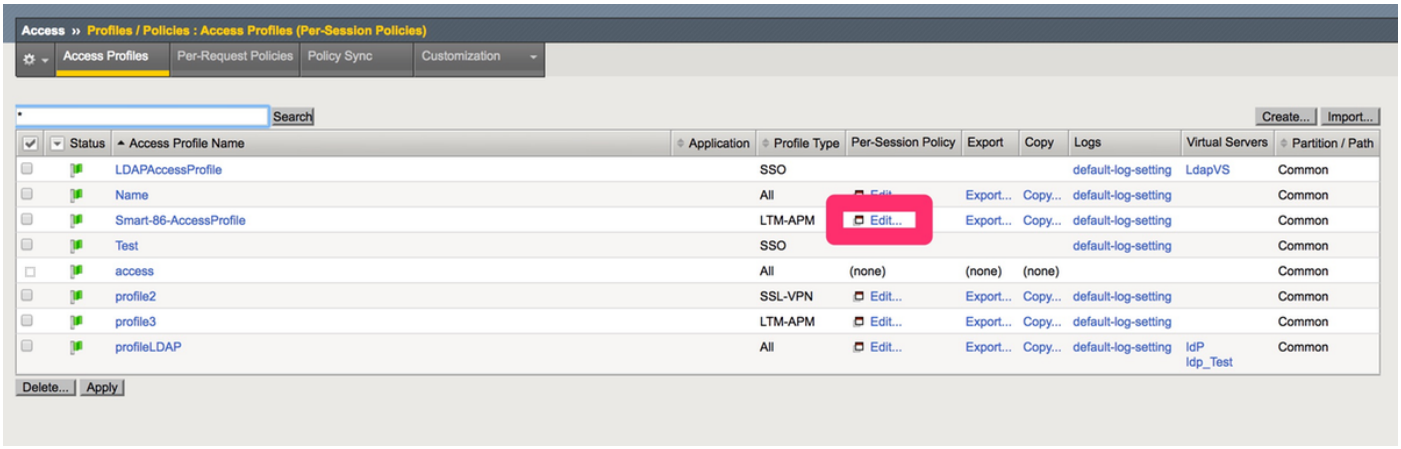

### Webtops

- Erstellen Sie einen Webtop unter **Access** -> **Webtops.**

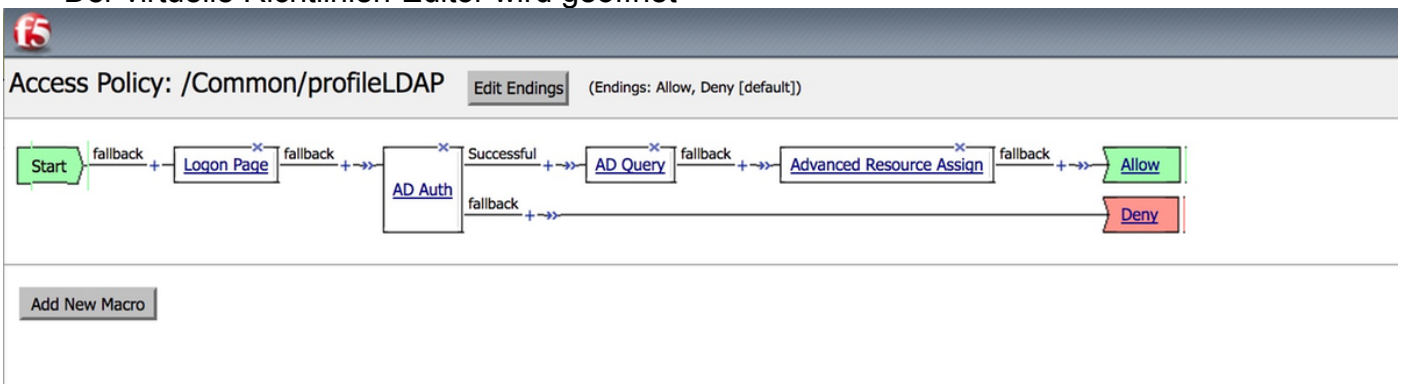



Virtueller Richtlinien-Editor

- Navigieren Sie zur zuvor erstellten Richtlinie, und klicken Sie auf den Link Bearbeiten.



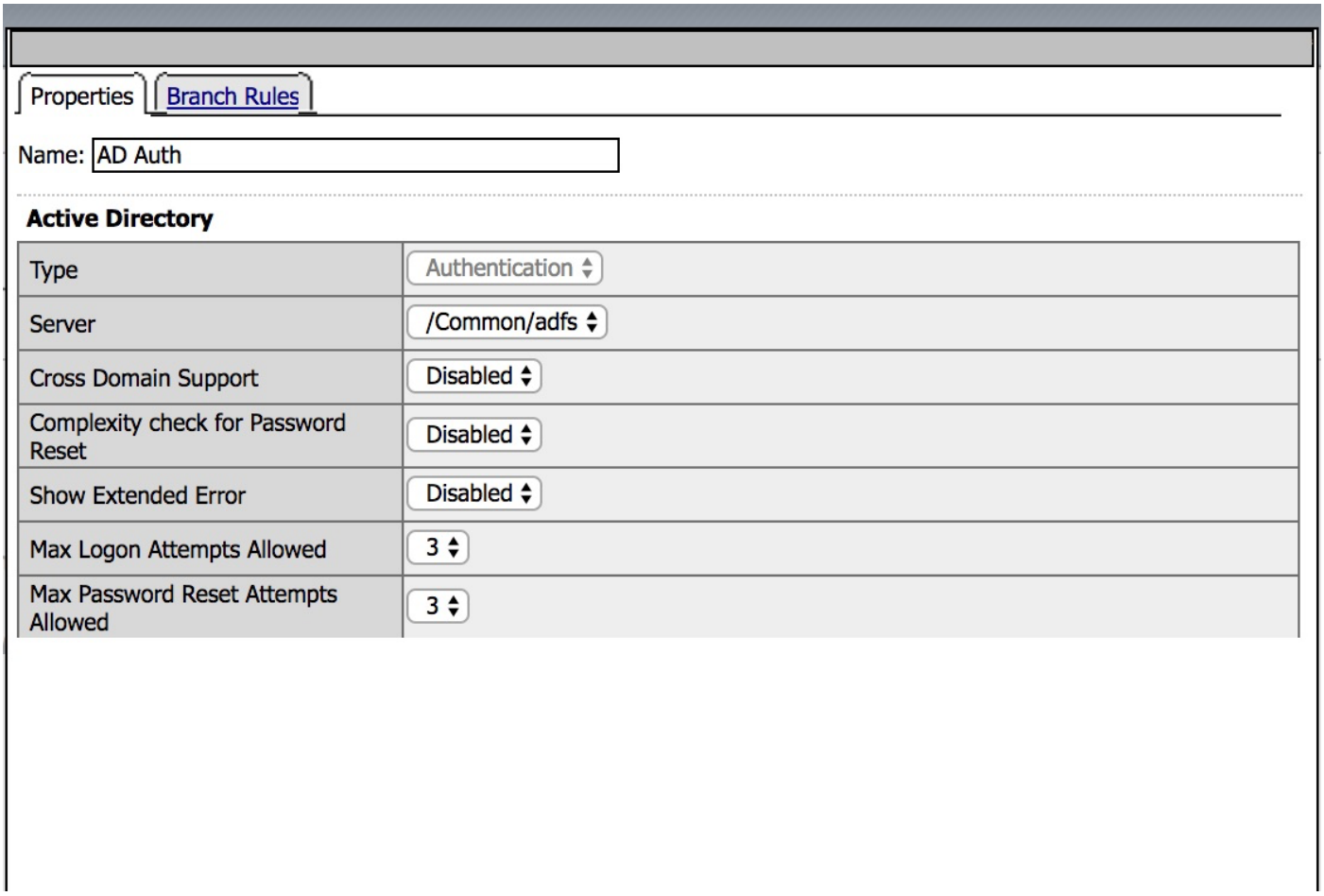

- Der virtuelle Richtlinien-Editor wird geöffnet



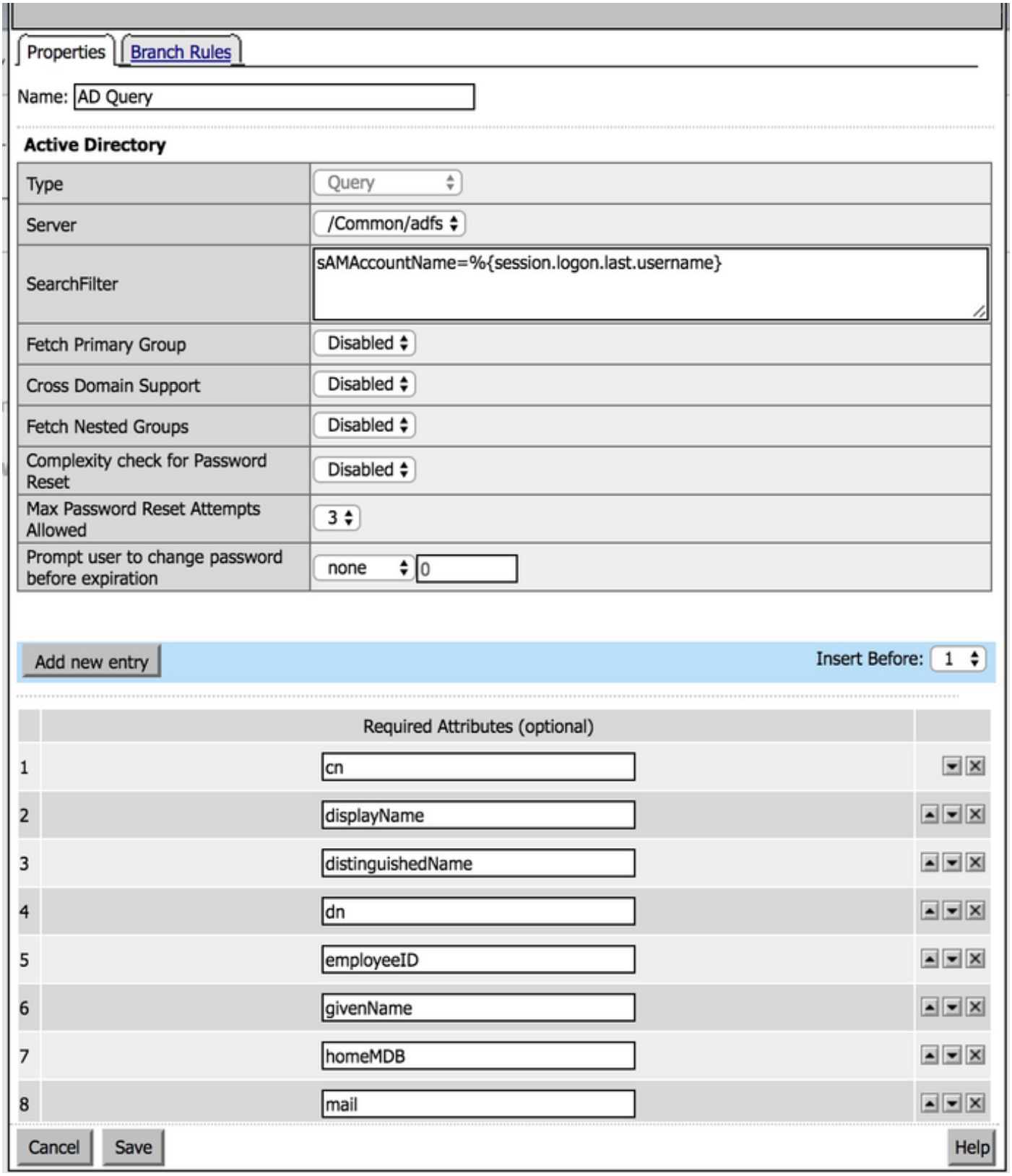

- Klicken Sie auf  Symbol und fügen Sie Elemente wie beschrieben hinzu.

Schritt 1: **Logon page element** (Seite anmelden): Behalten Sie die Standardeinstellung für alle Elemente bei.

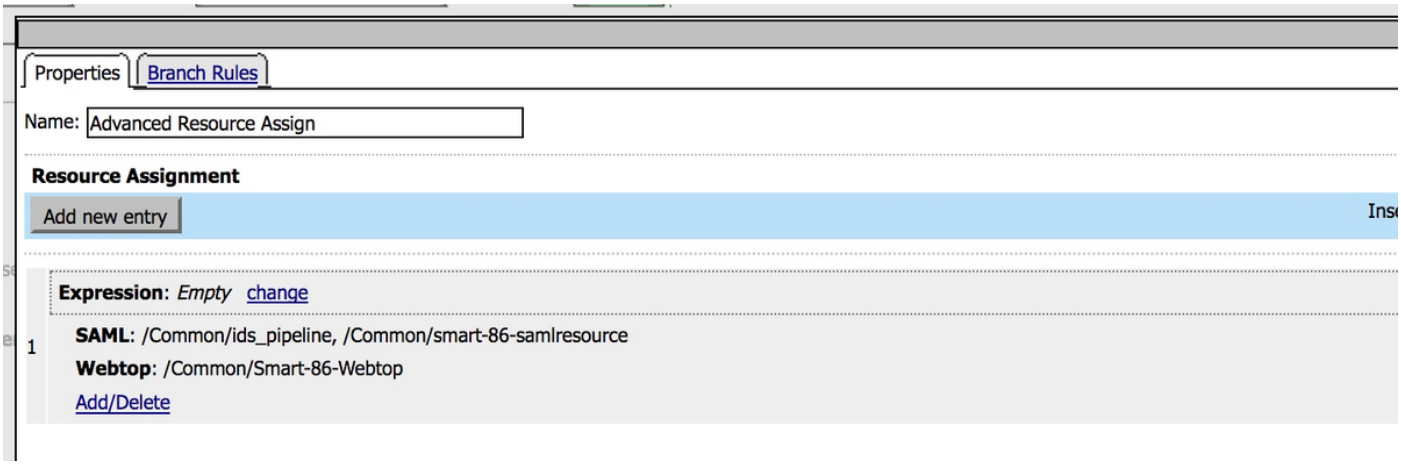
Schritt 2: **AD Auth** -> Wählen Sie die zuvor erstellte ADFS-Konfiguration aus.




Schritt 3: **AD Query-Element** - Weisen Sie die erforderlichen Details zu.



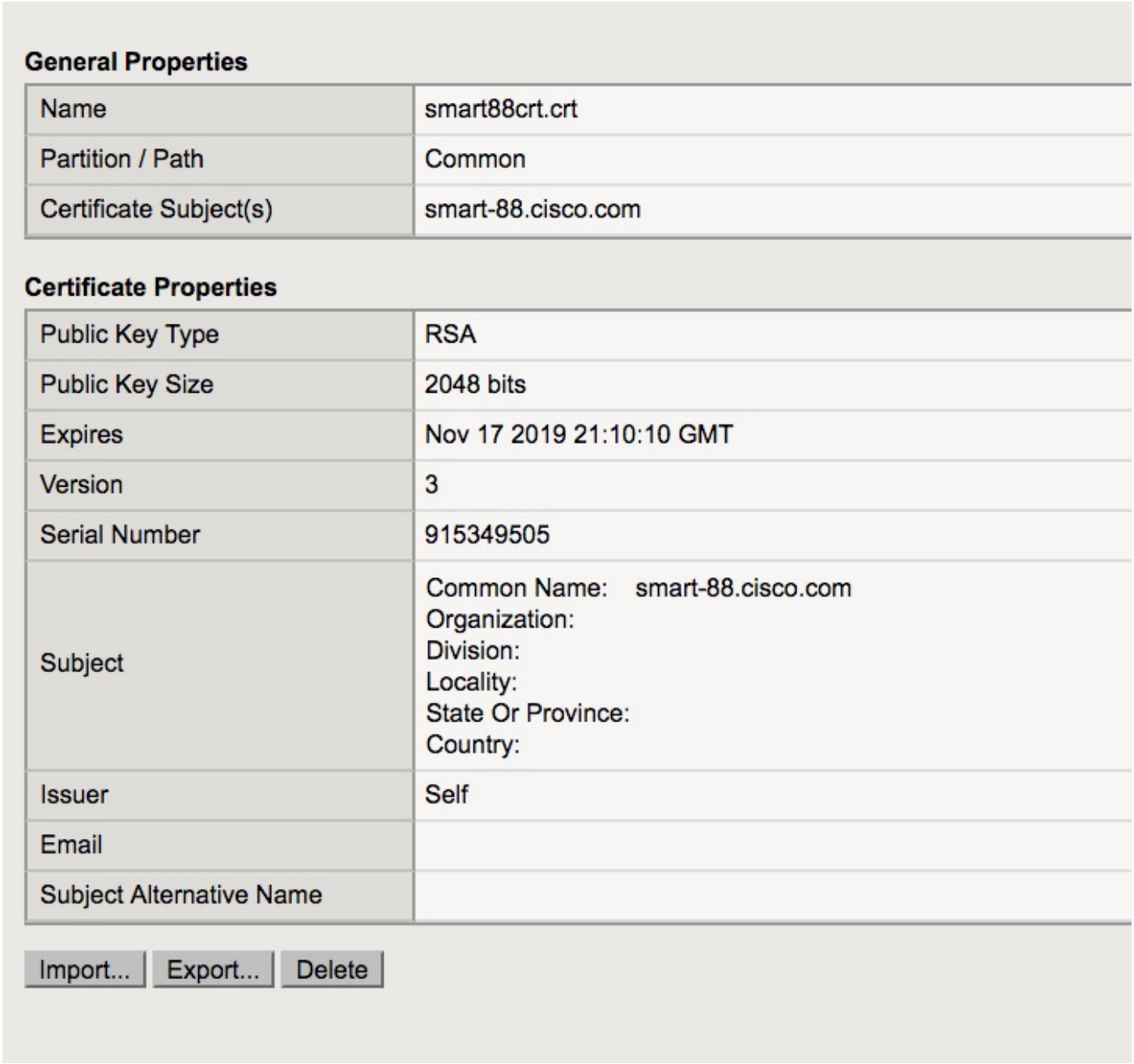

Schritt 4: **Erweiterte Ressourcenzuweisung - Verknüpfen Sie die gleiche Ressource mit dem zuvor erstellten Webtop.**




## Service Provider (SP) Metadata Exchange

- Importieren Sie das Zertifikat der IDS manuell in Big-IP über **System** -> **Zertifikatsverwaltung** -> **Datenverkehrsmanagement.**

  **Hinweis**: Stellen Sie sicher, dass das Zertifikat aus den Tags BEGIN CERTIFICATE und END CERTIFICATE besteht.



**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<br>Organization:<br>Division:<br>Locality:<br>State Or Province:<br>Country: |
| Issuer | Self |
| Email | |
| Subject Alternative Name | |



- Erstellen Sie einen neuen Eintrag aus sp.xml unter **Access -> Federation -> SAML Identity Provider -> External SP Connectors.**
- Binden Sie den SP-Anschluss unter **Access -> Federation -> SAML Identity Provider -> Local IdP Services an den** IDP-Service.

# Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

# Fehlerbehebung

## CAC-Authentifizierungsfehler (Common Access Card)

Wenn die SSO-Authentifizierung für CAC-Benutzer fehlschlägt, überprüfen Sie das Feld UCCX ids.log, um zu überprüfen, ob die SAML-Attribute korrekt eingestellt wurden.

Bei einem Konfigurationsproblem tritt ein SAML-Fehler auf. In diesem Protokollausschnitt ist das user_Principal-SAML-Attribut z. B. auf dem IdP nicht konfiguriert.

JJJJ-MM-DD hh:mm:SS.sss GMT(-0000) [IdSEndPoints-SAML-59] ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:465 - **Kann nicht aus der Attributzuordnung abgerufen werden: Benutzer_Principal**

JJJJ-MM-DD hh:mm:SS.sss GMT(-0000) [IdSEndPoints-SAML-59] ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - **SAML-Antwortverarbeitung fehlgeschlagen mit exception com.sun.identity.saml.common.SAMLException: user_Principal konnte nicht aus der Antwort "SAL" abgerufen werden.**

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

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

unter com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServlet.java:176)

unter com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)

at java.util.current.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)

at java.util.current.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)

at java.lang.Thread.run(Thread.java:745)

# Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems