Cisco 識別サービス（ID）のための F5 識別プロバイダ（IdP）をインストールし、SSO を有効に するために設定して下さい

目次

概要

この資料は単一 サインを有効に するために F5 BIG-IP 識別プロバイダ（IdP）の設定を説明したものです（SSO）。

Cisco IdS 導入モデル

製品	導入
UCCX	共存
PCCE	CUIC（Cisco Unified Intelligence Center）と LD（ライブ データ）の共存
UCCE	2k 導入用の CUIC と LD の共存。 4k および 12k 導入用のスタンドアロン。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Unified Contact Center Express （UCCX）リリース 11.6 か Cisco Unified Contact Center Enterprise リリース 11.6 または適当 Packaged Contact Center Enterprise （PCCE）リリース 11.6。

注: この資料は Cisco Identitify サービス（ID）および識別プロバイダ（IdP）に関して設定を参照します。 資料はスクリーン ショットおよび例で設定が Cisco Identitify サービス（UCCX/UCCE/PCCE）および IdP に関して類似したであるどんなに、UCCX を参照します。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

インストールするもの

複数の機能がある大きい IP は実装されたソリューションです。 識別プロバイダ サービスに共同関連付けるアクセスポリシー マネージャ（APM）。

APM として大きい IP:

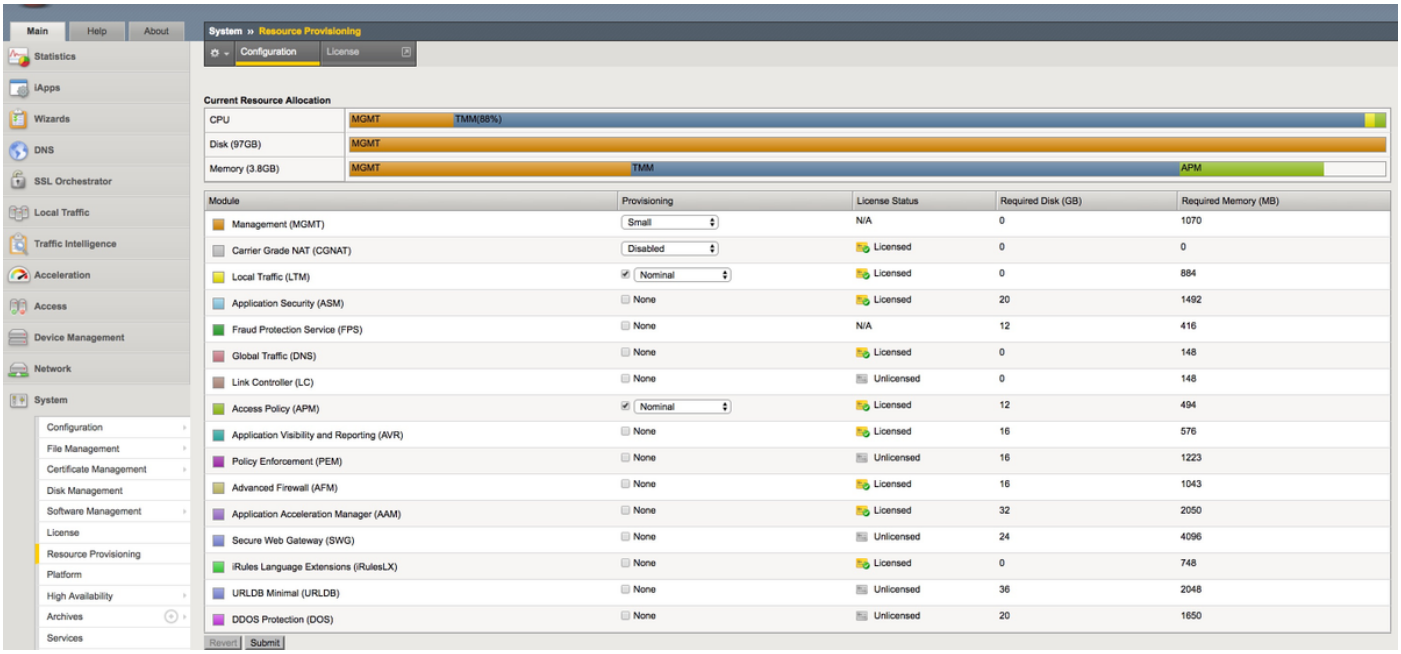
バージョン	13.0
タイプ	バーチャル Edition（OVA）
IP	異なるサブネットの 2 IP。 管理 IP のための 1 つ そして IdP 仮想サーバのための 1 つ

バーチャル版イメージをプレインストールされる大きい IP Webサイトからダウンロードし、Virtual Machine（VM）を作成するために OVUM を展開して下さい。 ライセンスを得、基本要件とインストールして下さい。

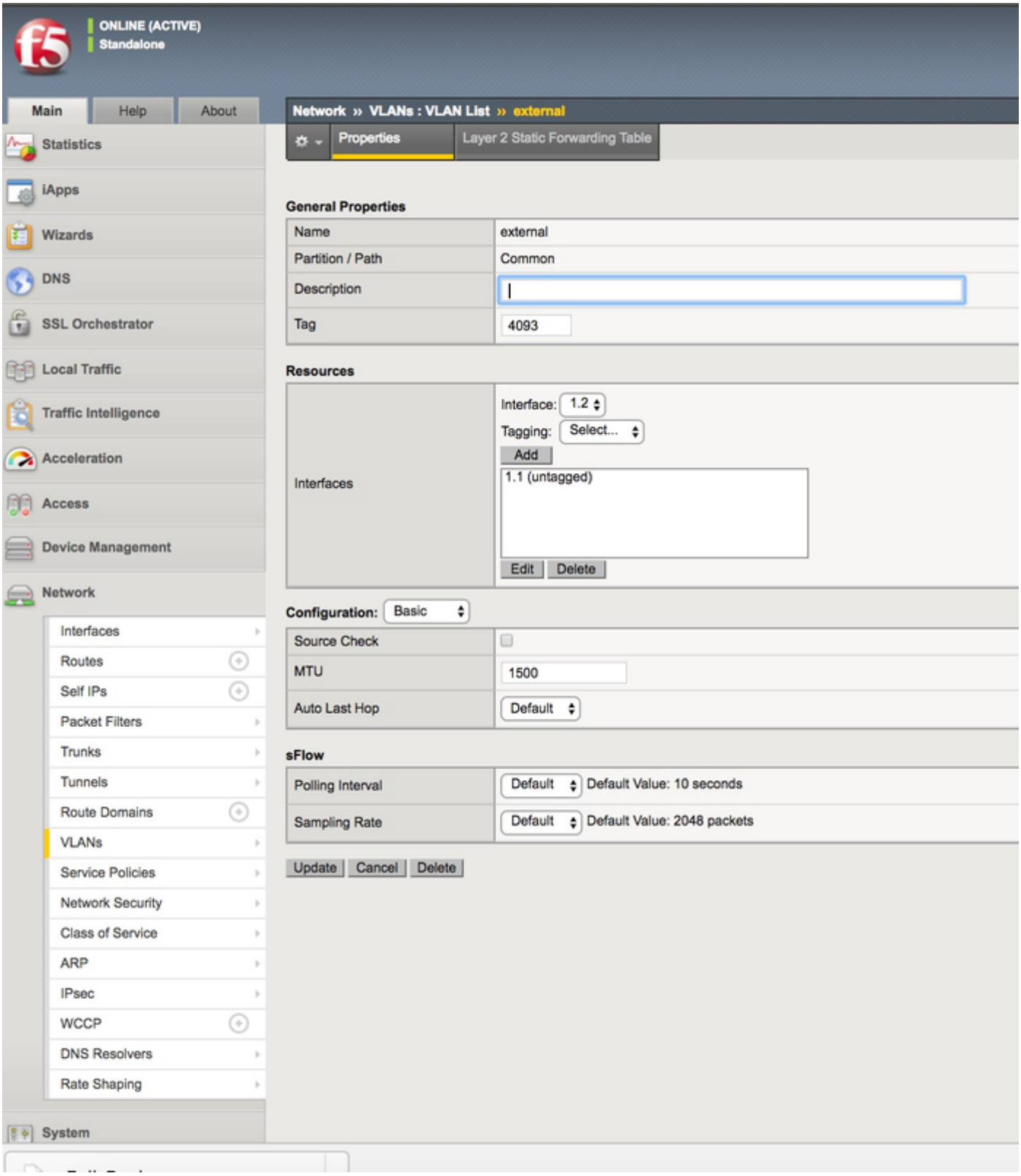
注: インストール情報に関しては、大きい IP インストール ガイドを参照して下さい。

設定

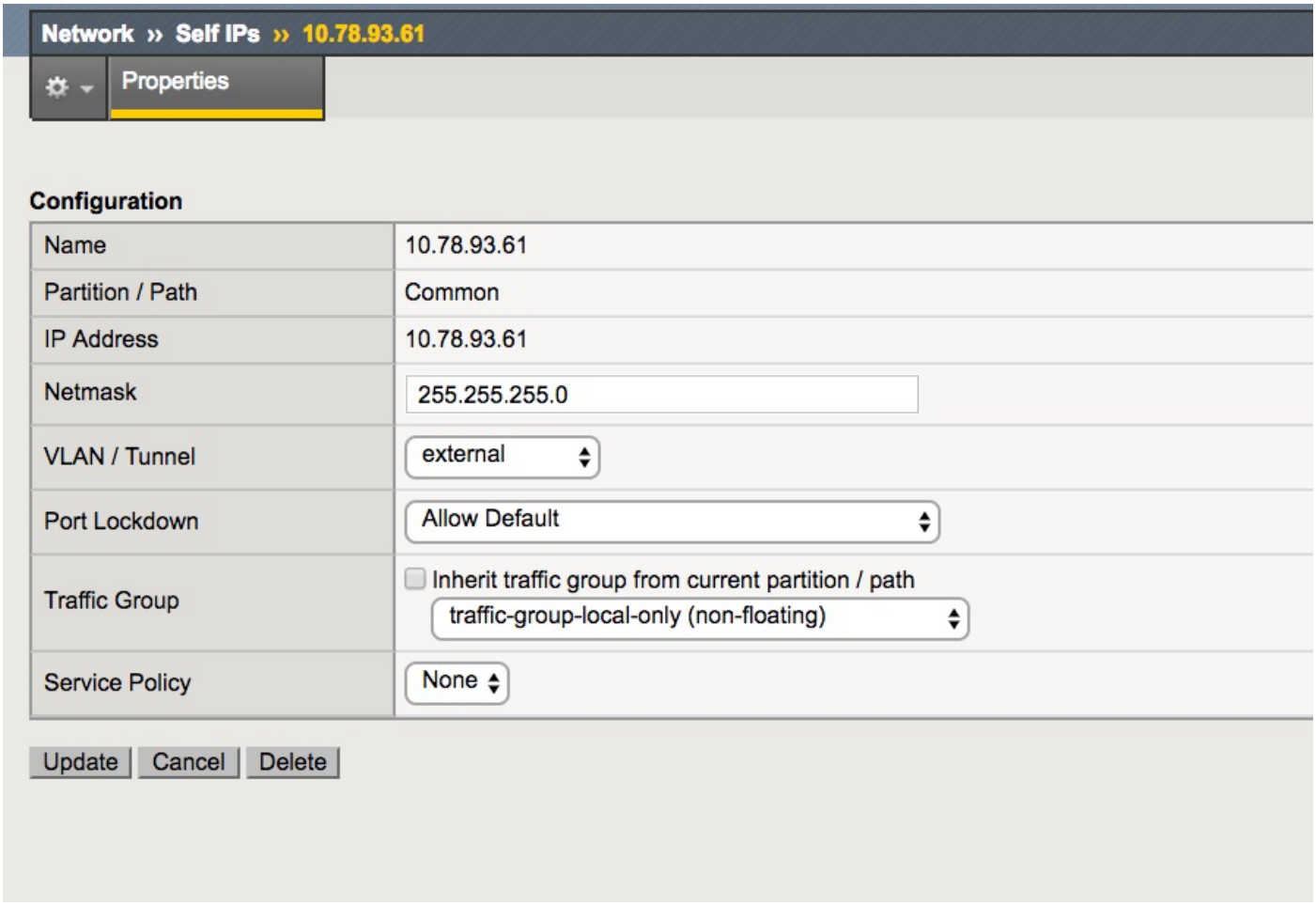
- リソー スのプロビジョニングにナビゲートし、**アクセスポリシーを**有効に して下さい、**公称**にプロビジョニングを設定 して下さい



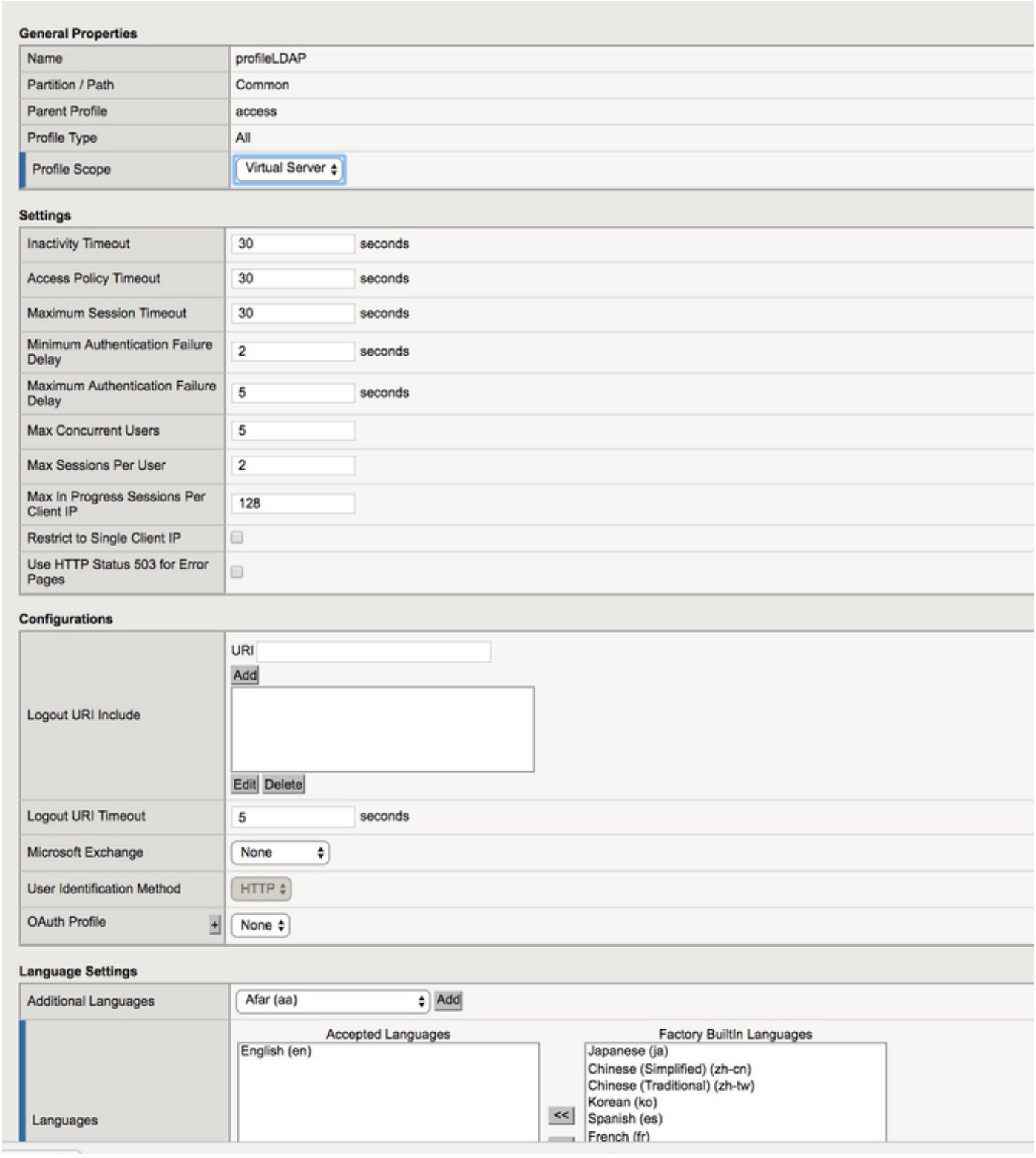
- ネットワークの下で新しい VLAN を- > VLAN 作成して下さい



- **ネットワーク**の下の IdP のために- > **自己 IP** 使用される IP のための New エントリを作成して下さい



- **アクセス**の下でプロファイルを- > **プロファイル/ポリシー**- > **アクセス プロファイル**作成して下さい

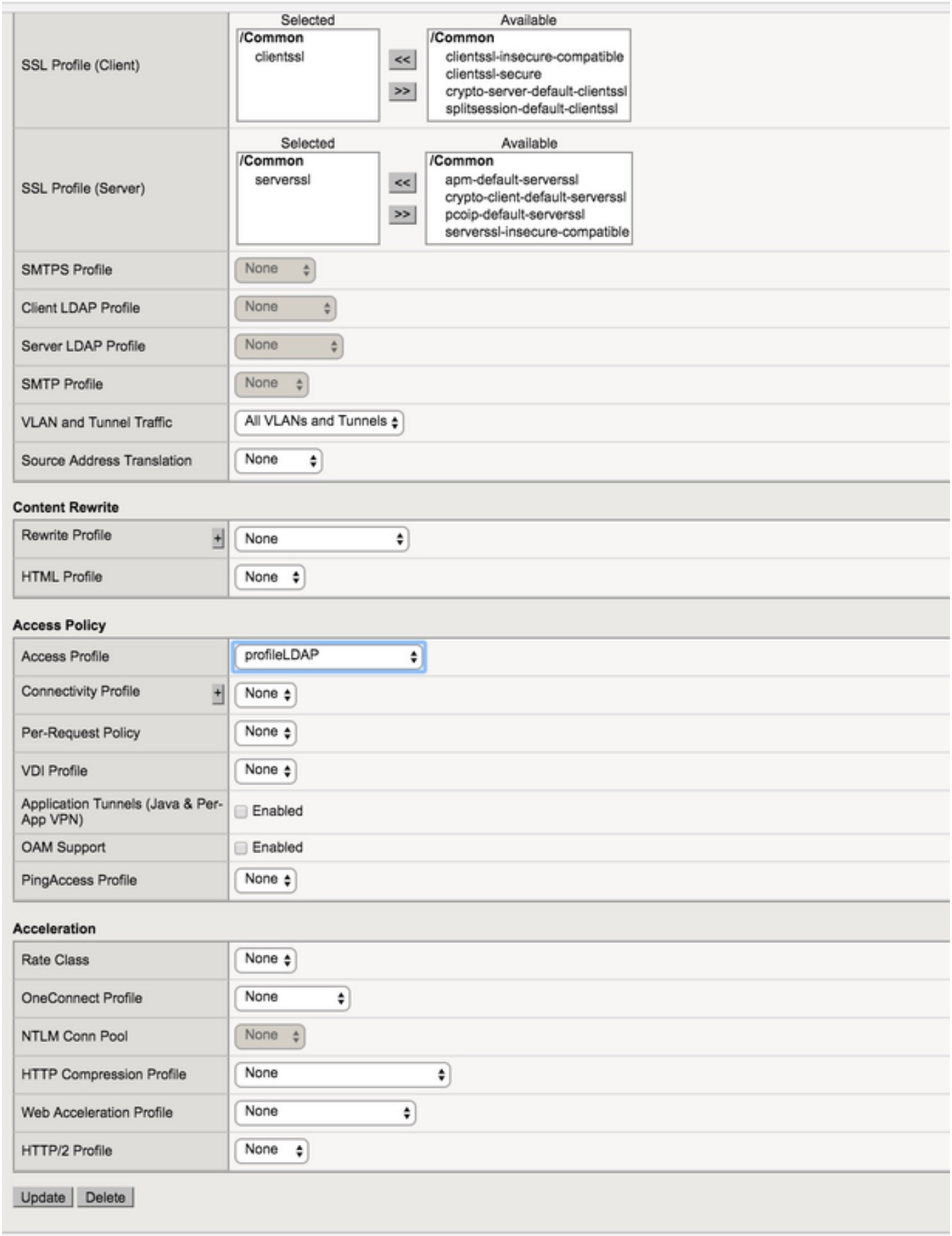


- 仮想サーバを作成して下さい

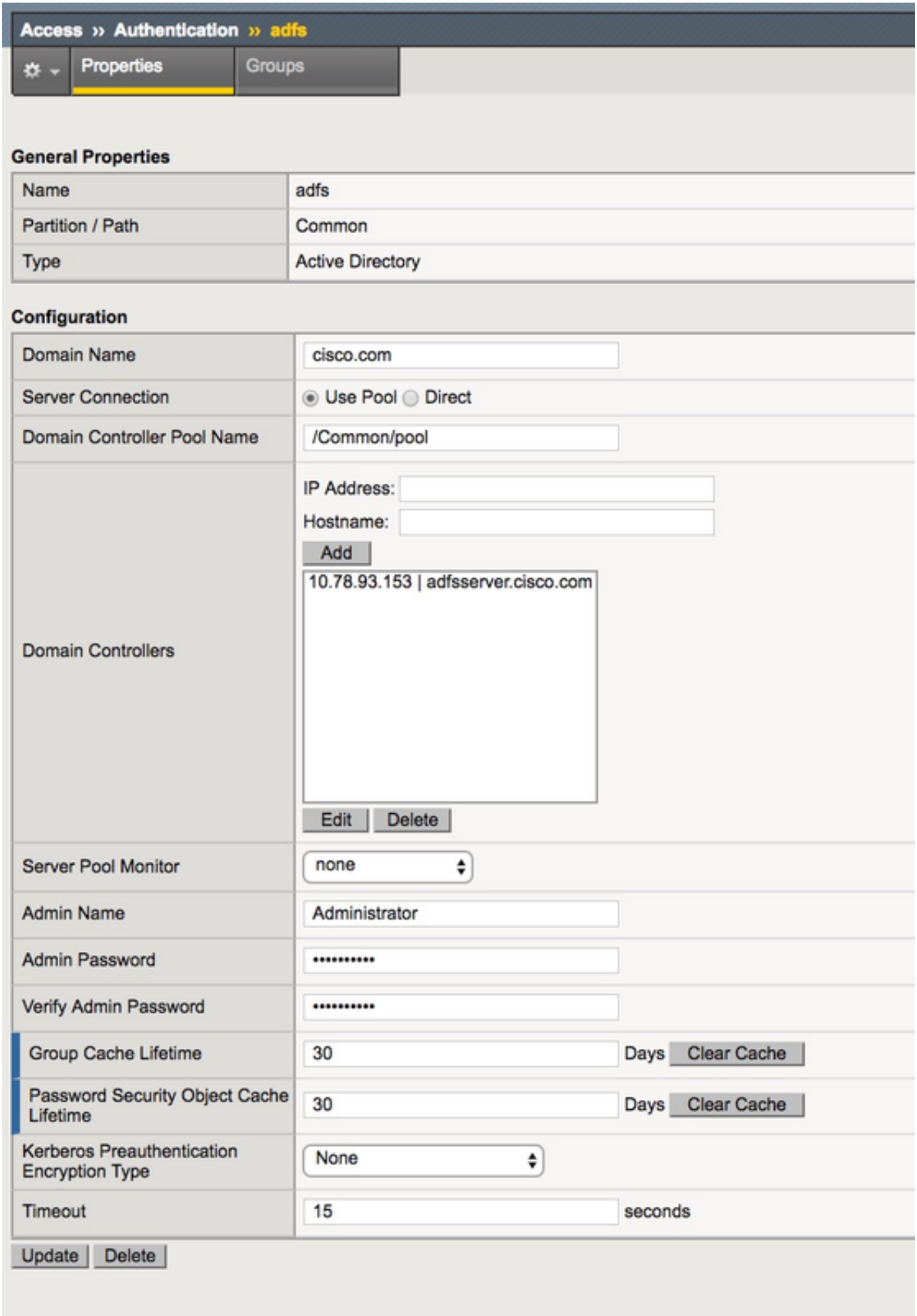
General Properties

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

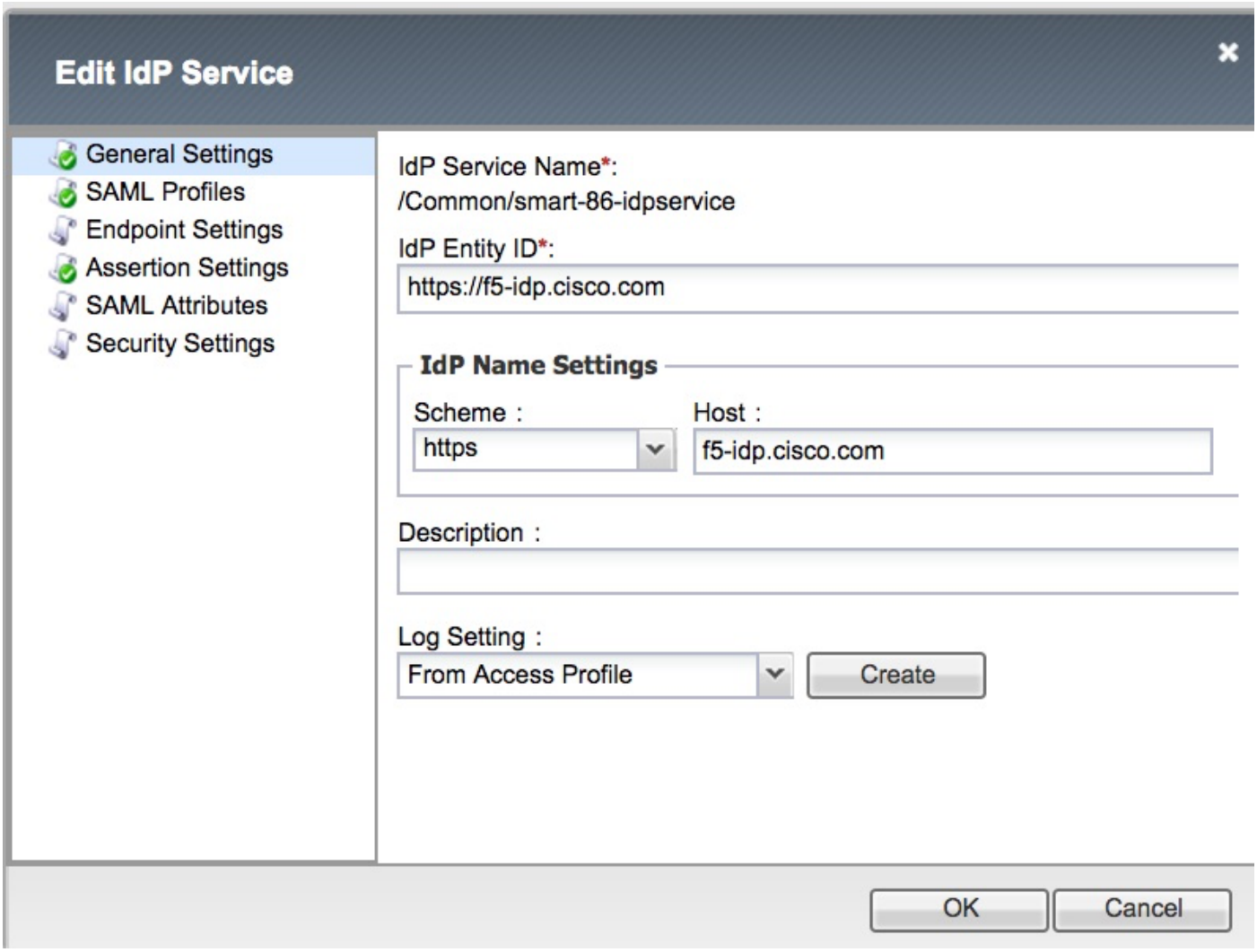
Configuration: Basic

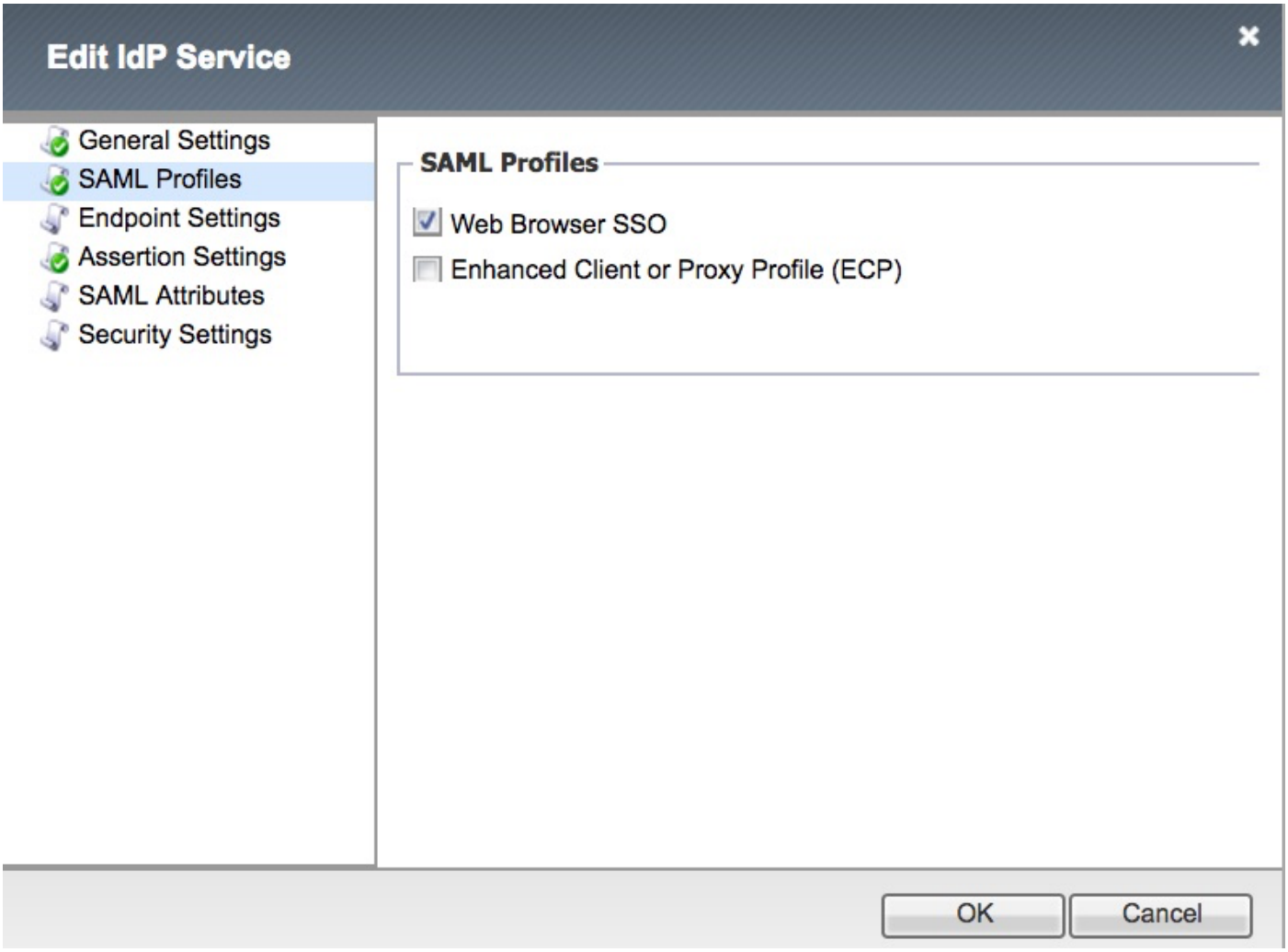


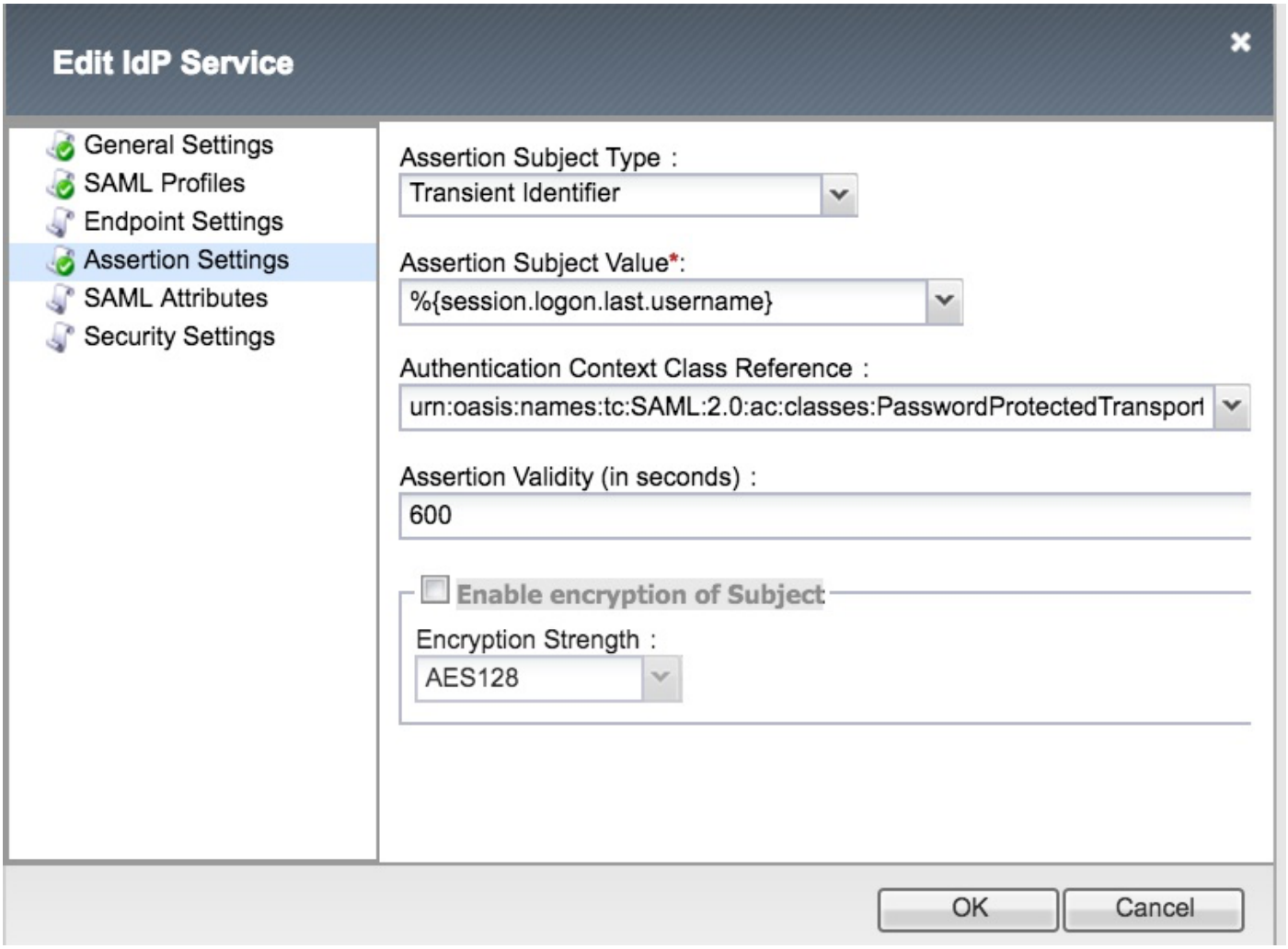
- アクセスの下で Active Directory （ AD ） 詳細を- > 認証- > Active Directory 追加して下さい


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

- **アクセス**の下で IdP 新しいサービスを- > **フェデレーション**- > **SAML 識別プロバイダ**- > **IdP ローカル サービス**作成して下さい




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



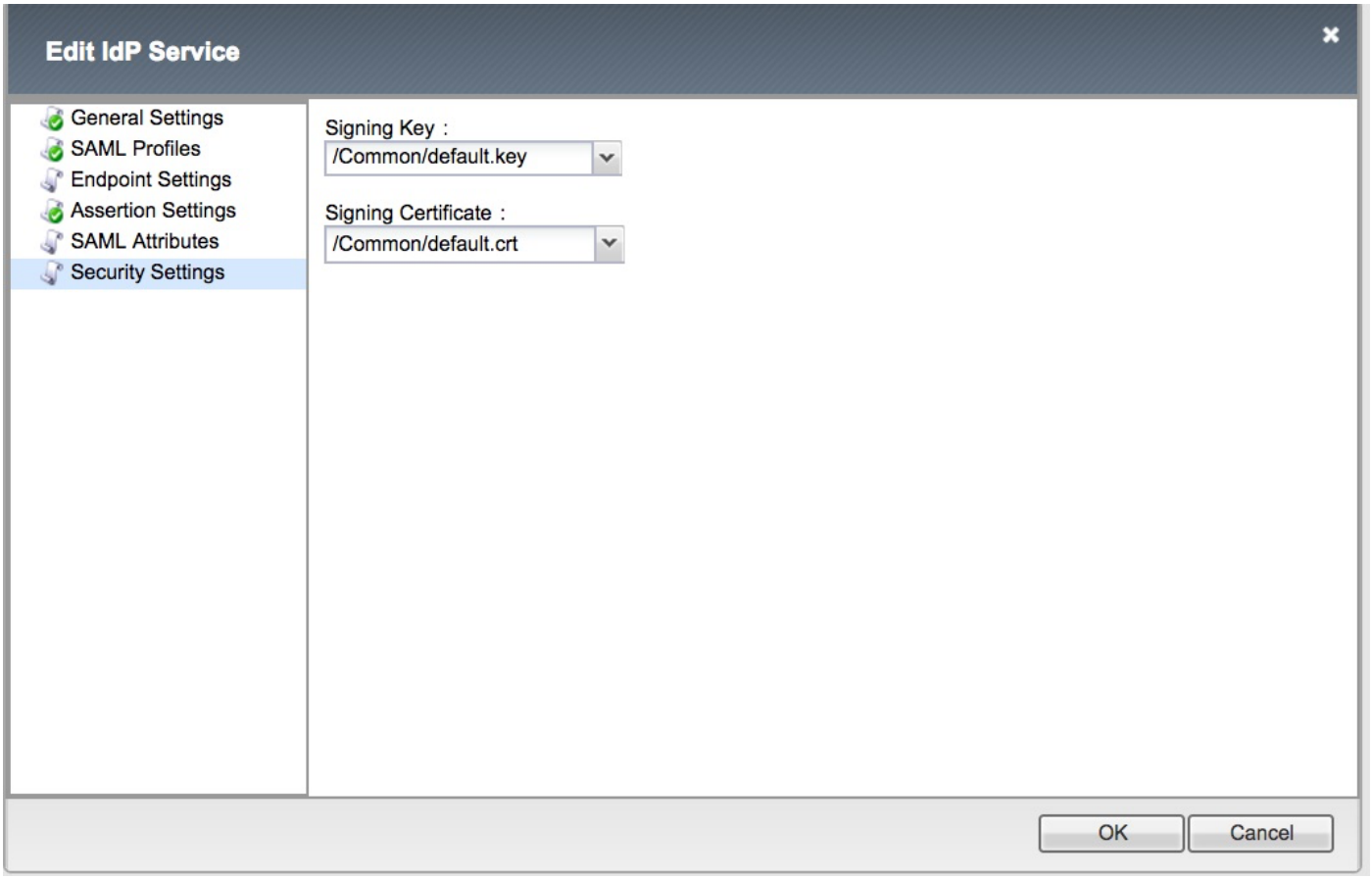
注: よくあるアクセス カード（CAC）が認証のために使用される場合、**SAML** に追加されるこれらの属性必要はコンフィギュレーションセクションを**帰因させます**:

ステップ 1. **uid** アトリビュートを作成して下さい。

[Name]： uid
Value % {session.ldap.last.attr.sAMAccountName}

ステップ 2. **user_principal** アトリビュートを作成して下さい。

[Name]： user_principal
Value % {session.ldap.last.attr.userPrincipalName}

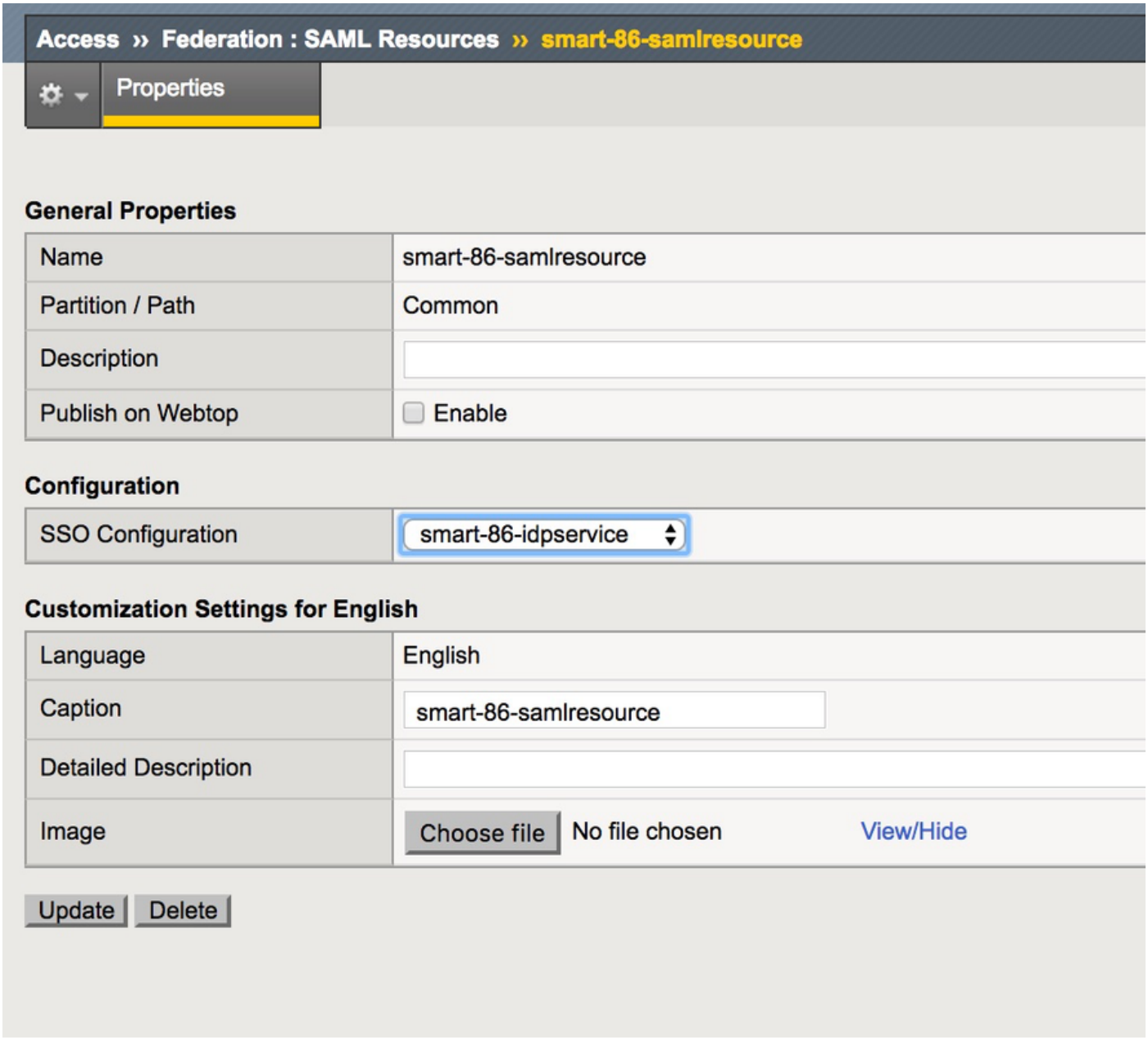


注: IdP サービスが作成されたり、**アクセス**の下でボタン **エクスポート メタデータ**のメタデータをダウンロードするオプションが- > **フェデレーション**- > **SAML 識別プロバイダ**- > **IdP ローカル サービス**あります

セキュリティ アサーション マークアップ言語 (SAML) 作成

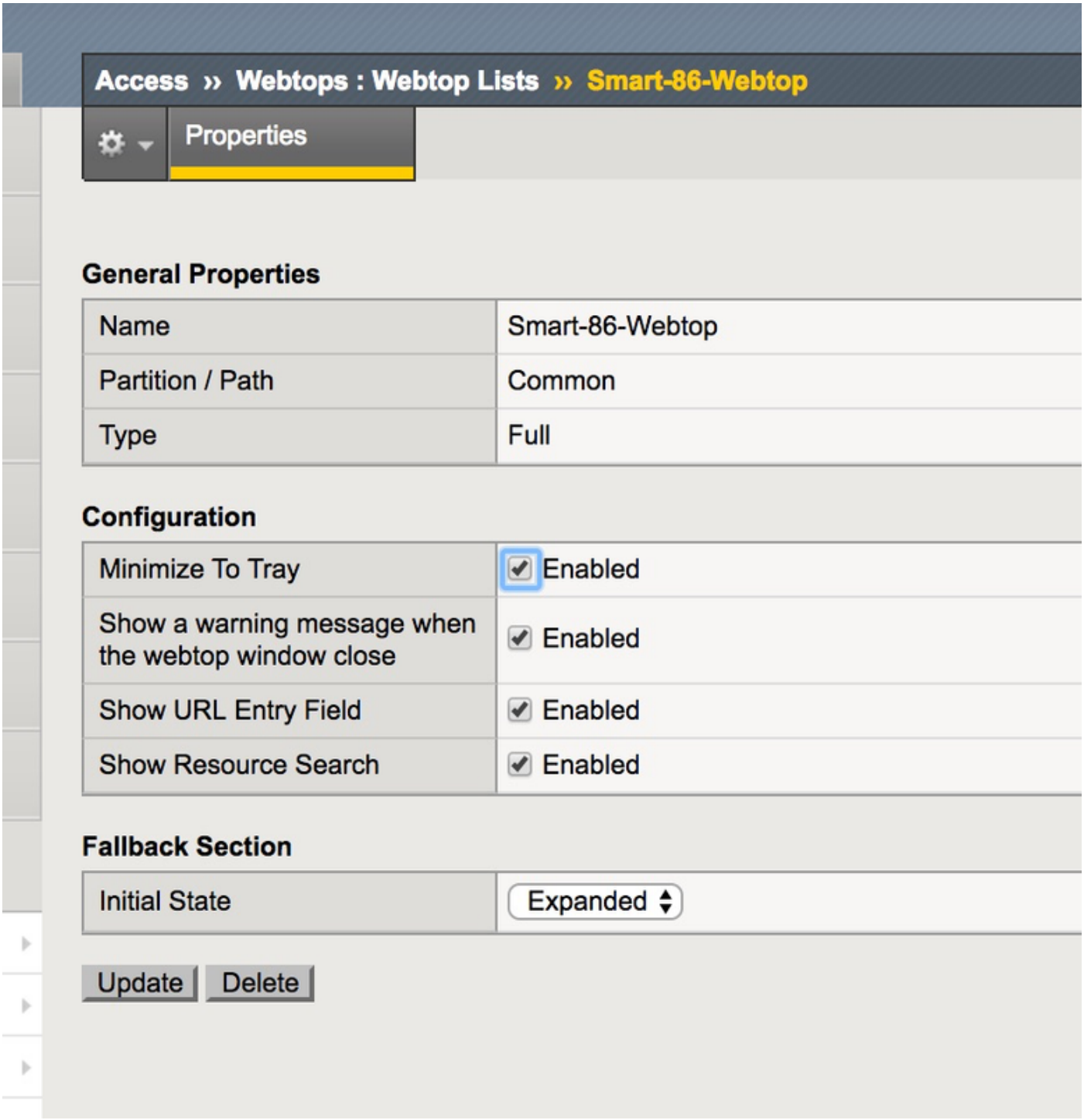
SAML リソース

- - > **フェデレーション**- > **SAML リソース アクセス**し、先に作成された IdP サービスと関連付けるために saml リソースを作成するためにナビゲートして下さい



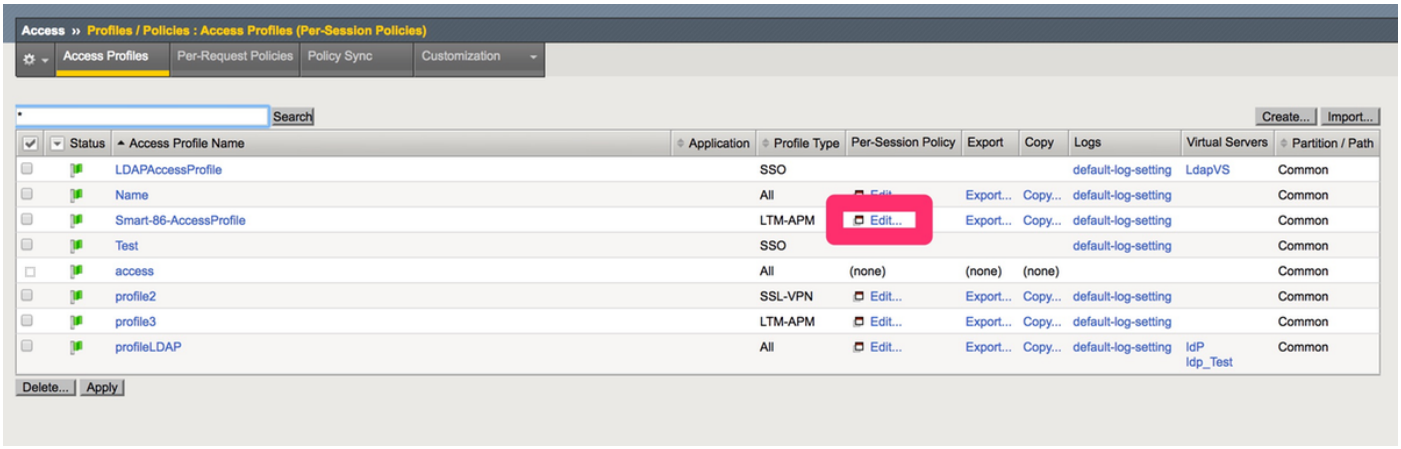
Webtops

- アクセスの下で webtop を- > Webtops 作成して下さい

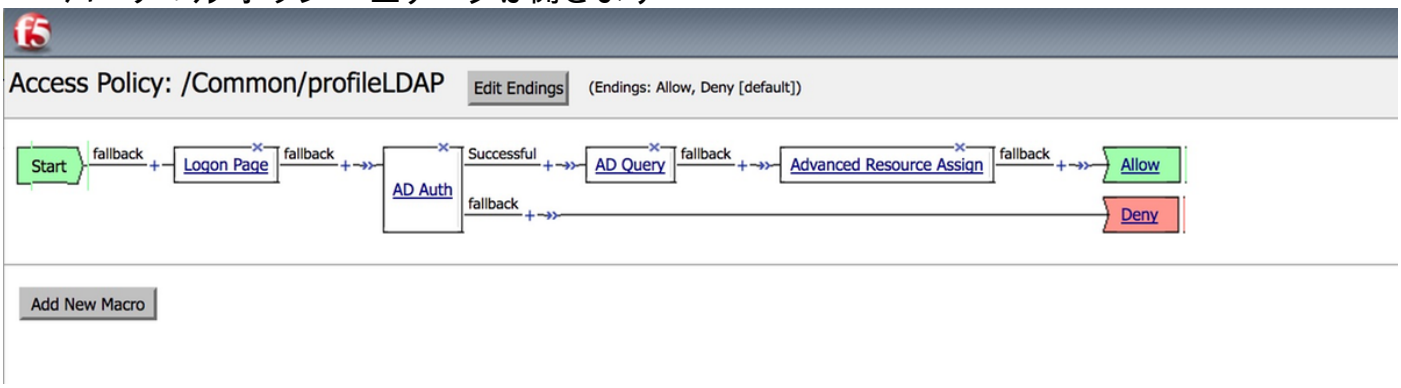


バーチャル ポリシー エディタ

- 先に作成されるポリシーにナビゲートし、リンクを『Edit』 をクリック して下さい



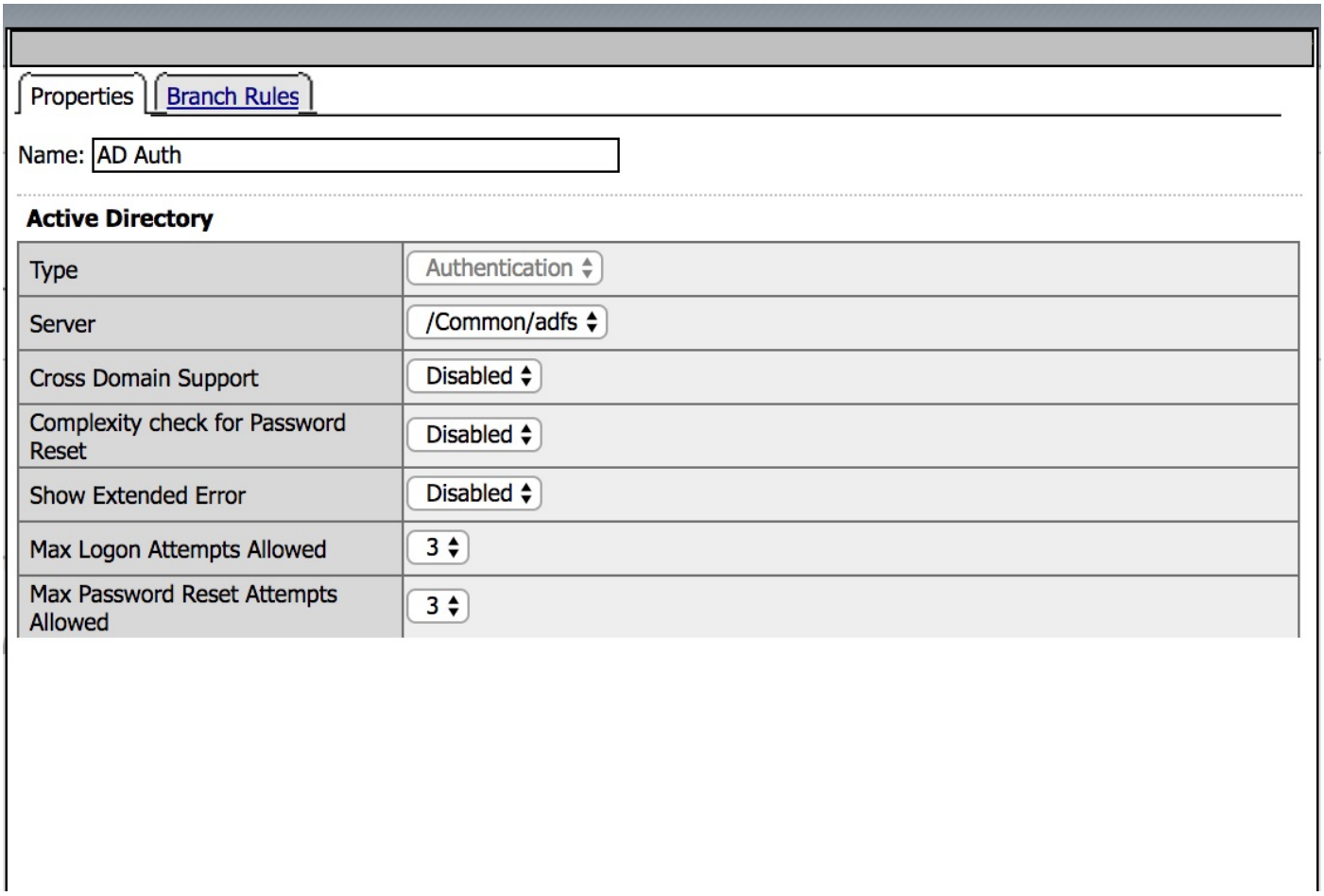
- バーチャル ポリシー エディタは開きます



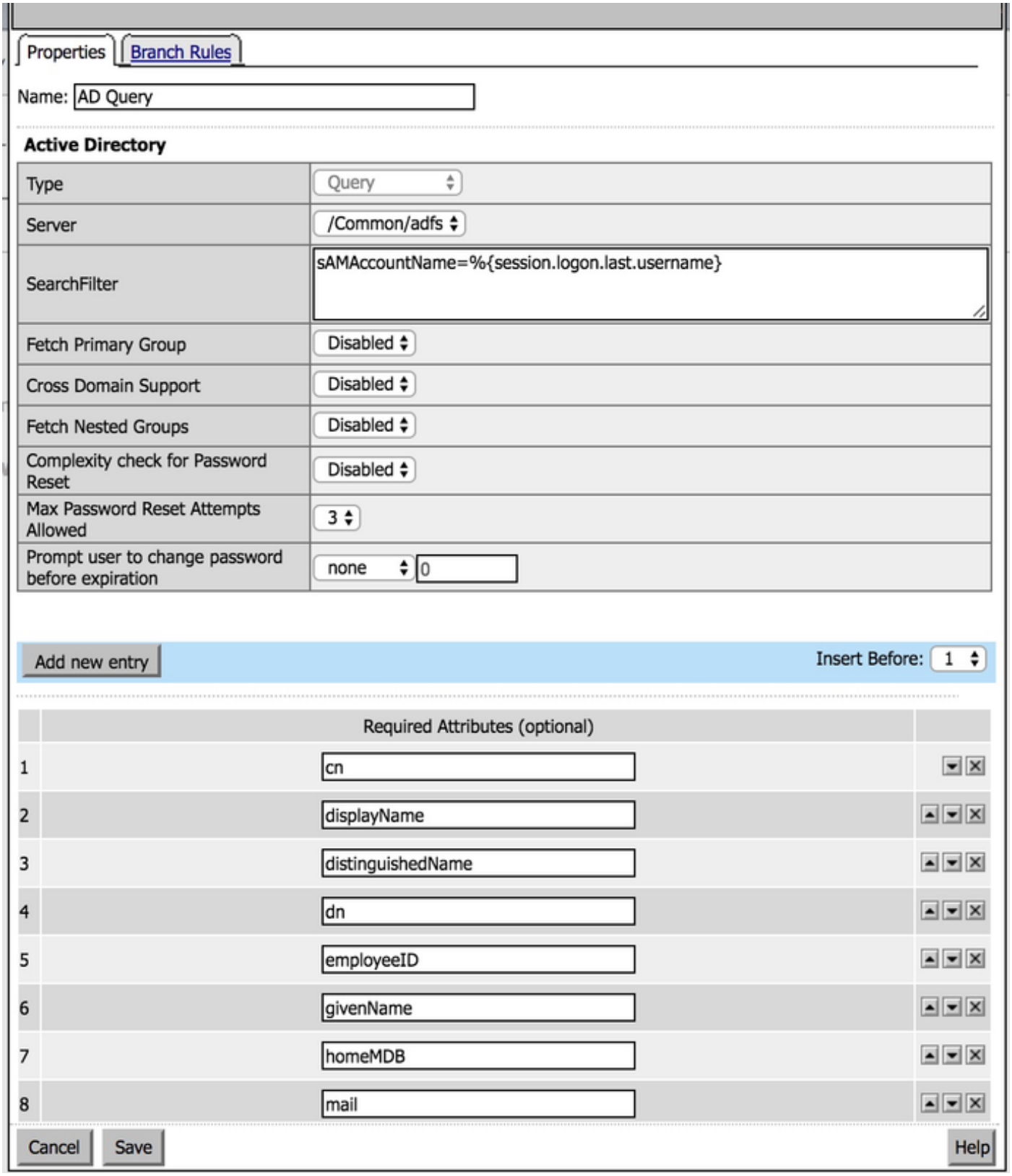
- アイコンを  クリックし、記述されているように要素を追加して下さい

ステップ 1.**ログオン ページ要素**-ディフォルトするためにすべての要素を残して下さい。

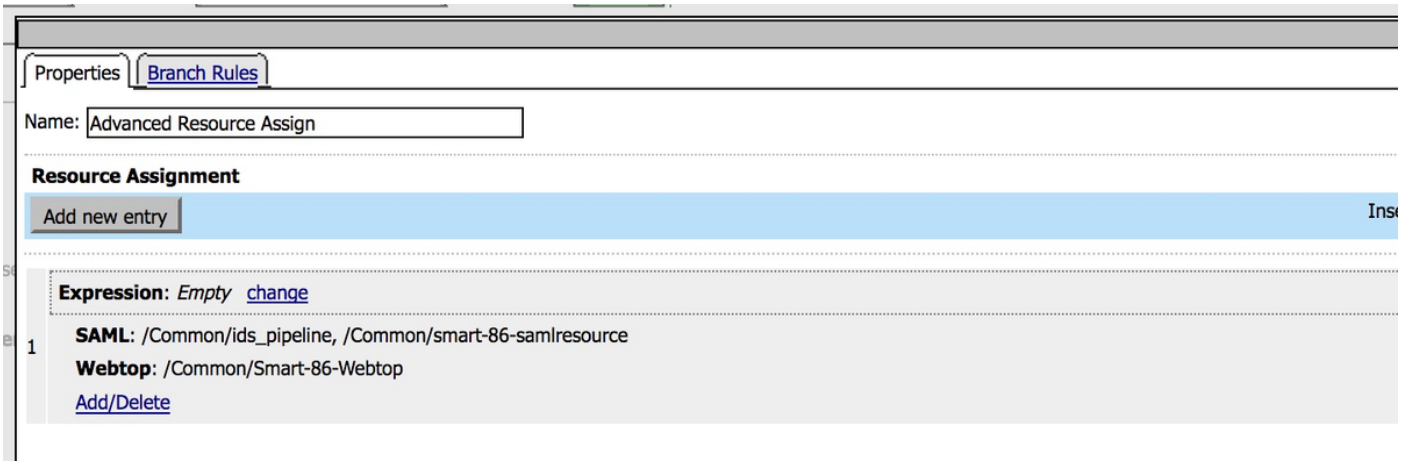
ステップ 2. **AD Auth** - > 先に作成される ADFS 設定を選択して下さい。



ステップ 3. **AD クエリ要素**-必要な詳細を割り当てて下さい。



ステップ 4.先発リソースは割り当てます-先に作成される saml リソースおよび webtop を関連付けて下さい。



サービス プロバイダー（SP）メタデータ交換

- 手動で **システム**によって大きい IP に ID の証明書を- > Certificate Management - > Traffic Management インポートして下さい

  注: 証明書が BEGIN 証明書および END 証明書タグで構成されているようにして下さい。

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

- Access-> Federation-> SAMLIDENTITY **プロバイダ**の下で sp.xml からの New エントリを**- >** ExternalSP **コネクタ**作成して下さい
- **アクセス**の下で IdP サービスに SP コネクタを- > **フェデレーション**- > **SAML 識別プロバイダ**- > **IdP ローカル サービス** バインドして下さい

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

よくあるアクセス カード（CAC）認証失敗

SSO 認証が CAC ユーザ向けに失敗した場合、SAML 属性がきちんと設定 されたことを確認するために UCCX ids.log をチェックして下さい。

設定 に関する 問題がある場合、SAML 失敗は発生します。 たとえば、このログ 断片で、user_principal SAML アトリビュートは IdP で設定されません。

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 - **com.sun.identity.saml.common.SAMLException responseprocessingfailed** SAML**: saml user_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)

関連情報

- テクニカル サポートとドキュメント – Cisco Systems