

# 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

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[インストール](#)

[設定](#)

[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](#)

[Webtops](#)

[バーチャル ポリシー エディタ](#)

[サービスプロバイダー \( SP \) メタデータ交換](#)

[確認](#)

[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](#)

[関連情報](#)

## 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。

UCCE 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 Identify 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 Identify 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

Main Help About System >> Resource Provisioning

Configuration License

Current Resource Allocation

CPU MGMT TMM(88%)

Disk (97GB) MGMT

Memory (3.8GB) MGMT TMM APM

Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small	N/A	0	1070
Carrier Grade NAT (CGNAT)	Disabled	Licensed	0	0
Local Traffic (LTM)	Nominal	Licensed	0	884
Application Security (ASM)	None	Licensed	20	1492
Fraud Protection Service (FPS)	None	N/A	12	416
Global Traffic (DNS)	None	Licensed	0	148
Link Controller (LC)	None	Unlicensed	0	148
Access Policy (APM)	Nominal	Licensed	12	494
Application Visibility and Reporting (AVR)	None	Licensed	16	576
Policy Enforcement (PEM)	None	Unlicensed	16	1223
Advanced Firewall (AFM)	None	Licensed	16	1043
Application Acceleration Manager (AAM)	None	Licensed	32	2050
Secure Web Gateway (SWG)	None	Unlicensed	24	4096
iRules Language Extensions (iRulesLX)	None	Licensed	0	748
URLDB Minimal (URLDB)	None	Unlicensed	36	2048
DDOS Protection (DOS)	None	Unlicensed	20	1650

Revert Submit

- ネットワークの下で新しい VLAN を-> VLAN 作成して下さい

The screenshot displays the F5 Network Management interface. At the top left, the F5 logo is shown next to the status 'ONLINE (ACTIVE) Standalone'. The main navigation bar includes 'Main', 'Help', and 'About'. The breadcrumb trail indicates the current location: 'Network >> VLANs : VLAN List >> external'. Below this, there are tabs for 'Properties' and 'Layer 2 Static Forwarding Table'. The left sidebar contains various system management categories: Statistics, iApps, Wizards, DNS, SSL Orchestrator, Local Traffic, Traffic Intelligence, Acceleration, Access, Device Management, and Network. The 'Network' category is expanded, showing a list of items including Interfaces, Routes, Self IPs, Packet Filters, Trunks, Tunnels, Route Domains, VLANs (highlighted), Service Policies, Network Security, Class of Service, ARP, IPsec, WCCP, DNS Resolvers, and Rate Shaping. The main content area is titled 'General Properties' and contains a table with the following data:

Name	external
Partition / Path	Common
Description	<input type="text"/>
Tag	4093

Below the 'General Properties' section is the 'Resources' section, which includes an 'Interfaces' table:

Interface:	1.2
Tagging:	Select...
<input type="button" value="Add"/>	
1.1 (untagged)	
<input type="button" value="Edit"/> <input type="button" value="Delete"/>	

The 'Configuration' section is set to 'Basic' and includes the following settings:

Source Check	<input type="checkbox"/>
MTU	1500
Auto Last Hop	Default

The 'sFlow' section includes the following settings:

Polling Interval	Default	Default Value: 10 seconds
Sampling Rate	Default	Default Value: 2048 packets

At the bottom of the configuration area, there are buttons for 'Update', 'Cancel', and 'Delete'.

- 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



## Configuration

Name	10.78.93.61
Partition / Path	Common
IP Address	10.78.93.61
Netmask	<input type="text" value="255.255.255.0"/>
VLAN / Tunnel	<input type="text" value="external"/>
Port Lockdown	<input type="text" value="Allow Default"/>
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path <input type="text" value="traffic-group-local-only (non-floating)"/>
Service Policy	<input type="text" value="None"/>

- 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

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	<input type="checkbox"/>
Use HTTP Status 503 for Error Pages	<input type="checkbox"/>

Configurations	
Logout URI Include	URI <input type="text"/> Add <input type="text"/> 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	<table border="0"> <thead> <tr> <th>Accepted Languages</th> <th>Factory BuiltIn Languages</th> </tr> </thead> <tbody> <tr> <td>English (en)</td> <td>Japanese (ja)</td> </tr> <tr> <td></td> <td>Chinese (Simplified) (zh-cn)</td> </tr> <tr> <td></td> <td>Chinese (Traditional) (zh-tw)</td> </tr> <tr> <td></td> <td>Korean (ko)</td> </tr> <tr> <td></td> <td>Spanish (es)</td> </tr> <tr> <td></td> <td>French (fr)</td> </tr> </tbody> </table>	Accepted Languages	Factory BuiltIn Languages	English (en)	Japanese (ja)		Chinese (Simplified) (zh-cn)		Chinese (Traditional) (zh-tw)		Korean (ko)		Spanish (es)		French (fr)
Accepted Languages	Factory BuiltIn Languages														
English (en)	Japanese (ja)														
	Chinese (Simplified) (zh-cn)														
	Chinese (Traditional) (zh-tw)														
	Korean (ko)														
	Spanish (es)														
	French (fr)														

- 仮想サーバを作成して下さい

**General Properties**

Name	ldp_Test
Partition / Path	Common
Description	<input type="text"/>
Type	Standard ▾
Source Address	<input type="text" value="0.0.0.0"/>
Destination Address/Mask	<input type="text" value="10.78.93.62"/>
Service Port	<input type="text" value="443"/> HTTPS ▾
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
Availability	<input type="checkbox"/> 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 ▾

SSL Profile (Client)	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <p style="text-align: center; margin: 0;">Selected</p> <p>/Common clientssl</p> </div> <div style="text-align: center; width: 10%;"> <p>&lt;&lt;</p> <p>&gt;&gt;</p> </div> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <p style="text-align: center; margin: 0;">Available</p> <p>/Common clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl splitsession-default-clientssl</p> </div> </div>
SSL Profile (Server)	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <p style="text-align: center; margin: 0;">Selected</p> <p>/Common serverssl</p> </div> <div style="text-align: center; width: 10%;"> <p>&lt;&lt;</p> <p>&gt;&gt;</p> </div> <div style="border: 1px solid gray; padding: 5px; width: 45%;"> <p style="text-align: center; margin: 0;">Available</p> <p>/Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl-insecure-compatible</p> </div> </div>
SMTSPS Profile	None ▾
Client LDAP Profile	None ▾
Server LDAP Profile	None ▾
SMTP Profile	None ▾
VLAN and Tunnel Traffic	All VLANs and Tunnels ▾
Source Address Translation	None ▾
<b>Content Rewrite</b>	
Rewrite Profile	+ None ▾
HTML Profile	None ▾
<b>Access Policy</b>	
Access Profile	profileLDAP ▾
Connectivity Profile	+ None ▾
Per-Request Policy	None ▾
VDI Profile	None ▾
Application Tunnels (Java & Per-App VPN)	<input type="checkbox"/> Enabled
OAM Support	<input type="checkbox"/> Enabled
PingAccess Profile	None ▾
<b>Acceleration</b>	
Rate Class	None ▾
OneConnect Profile	None ▾
NTLM Conn Pool	None ▾
HTTP Compression Profile	None ▾
Web Acceleration Profile	None ▾
HTTP/2 Profile	None ▾
<input type="button" value="Update"/> <input type="button" value="Delete"/>	

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



## General Properties

Name	adfs
Partition / Path	Common
Type	Active Directory

## Configuration

Domain Name	<input type="text" value="cisco.com"/>
Server Connection	<input checked="" type="radio"/> Use Pool <input type="radio"/> Direct
Domain Controller Pool Name	<input type="text" value="/Common/pool"/>
Domain Controllers	<p>IP Address: <input type="text"/></p> <p>Hostname: <input type="text"/></p> <p><input type="button" value="Add"/></p> <div style="border: 1px solid #ccc; padding: 5px;"><p>10.78.93.153   adfsserver.cisco.com</p></div> <p><input type="button" value="Edit"/> <input type="button" value="Delete"/></p>
Server Pool Monitor	<input type="text" value="none"/> ▾
Admin Name	<input type="text" value="Administrator"/>
Admin Password	<input type="password" value="....."/>
Verify Admin Password	<input type="password" value="....."/>
Group Cache Lifetime	<input type="text" value="30"/> Days <input type="button" value="Clear Cache"/>
Password Security Object Cache Lifetime	<input type="text" value="30"/> Days <input type="button" value="Clear Cache"/>
Kerberos Preauthentication Encryption Type	<input type="text" value="None"/> ▾
Timeout	<input type="text" value="15"/> seconds

- 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

IdP Service Name\*:  
/Common/smart-86-idpservice

IdP Entity ID\*:

**IdP Name Settings**

Scheme :  Host :

Description :

Log Setting :

# 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

### Edit IdP Service

- General Settings
- SAML Profiles
- Endpoint Settings
- Assertion Settings**
- SAML Attributes
- Security Settings

Assertion Subject Type :  
Transient Identifier

Assertion Subject Value\*:  
%{session.logon.last.username}

Authentication Context Class Reference :  
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

Assertion Validity (in seconds) :  
600

Enable encryption of Subject

Encryption Strength :  
AES128

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。

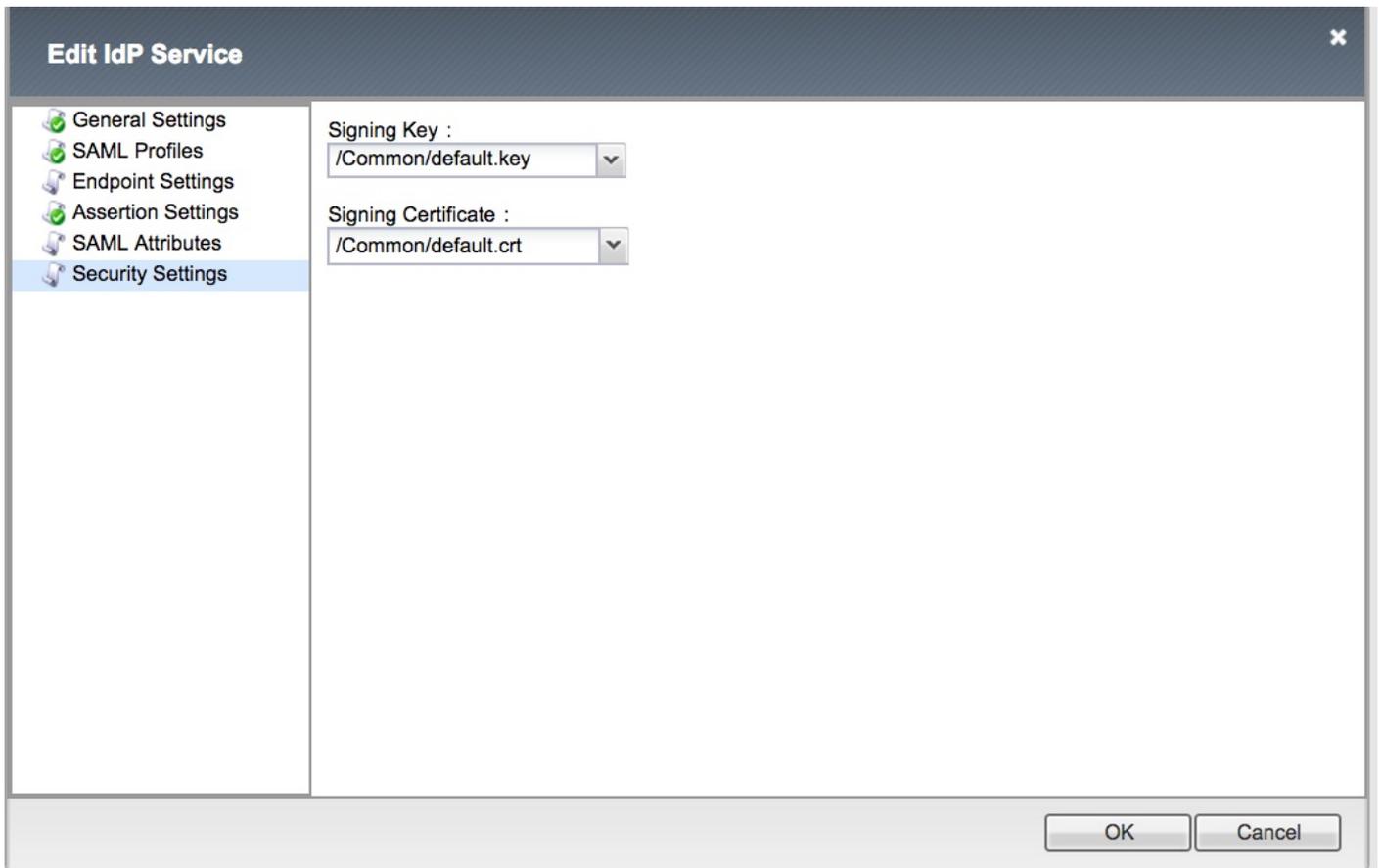
[Name] : uid

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



Properties

General Properties

Name	smart-86-samlresource
Partition / Path	Common
Description	<input type="text"/>
Publish on Webtop	<input type="checkbox"/> Enable

Configuration

SSO Configuration	smart-86-idpservice
-------------------	---------------------

Customization Settings for English

Language	English
Caption	<input type="text" value="smart-86-samlresource"/>
Detailed Description	<input type="text"/>
Image	<input type="button" value="Choose file"/> No file chosen <a href="#">View/Hide</a>

Webtops

- アクセスの下で webtop を -> Webtops 作成して下さい



Properties

General Properties

Name	Smart-86-Webtop
Partition / Path	Common
Type	Full

Configuration

Minimize To Tray	<input checked="" type="checkbox"/> Enabled
Show a warning message when the webtop window close	<input checked="" type="checkbox"/> Enabled
Show URL Entry Field	<input checked="" type="checkbox"/> Enabled
Show Resource Search	<input checked="" type="checkbox"/> Enabled

Fallback Section

Initial State	Expanded ▾
---------------	------------

Update

Delete

## 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

Access >> Profiles / Policies : Access Profiles (Per-Session Policies)

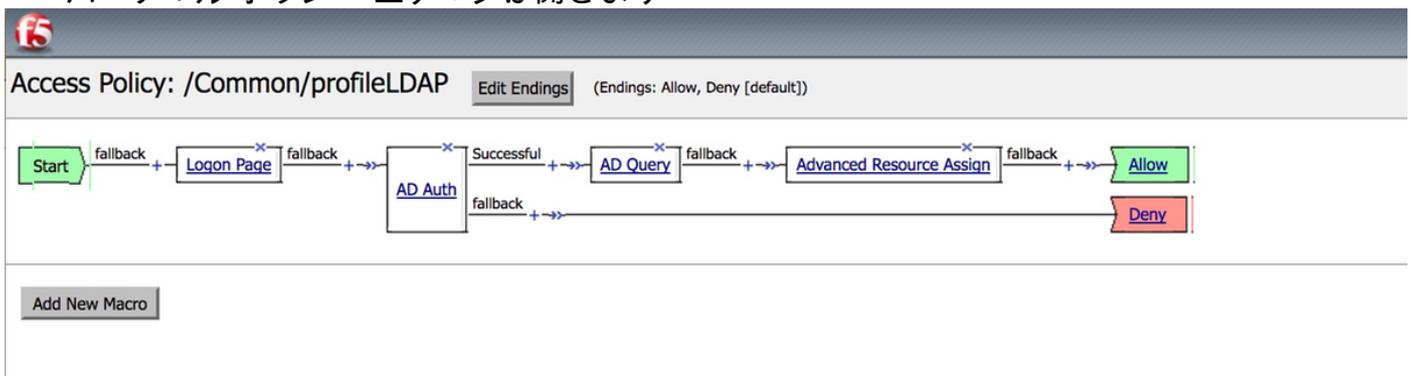
Access Profiles | Per-Request Policies | Policy Sync | Customization

Search

✓	▼	Status	▲ Access Profile Name	◆ Application	◆ Profile Type	Per-Session Policy	Export	Copy	Logs	Virtual Servers	◆ Partition / Path
<input type="checkbox"/>		🟢	LDAPAccessProfile		SSO				default-log-setting	LdapVS	Common
<input type="checkbox"/>		🟢	Name		All		Export...	Copy...	default-log-setting		Common
<input type="checkbox"/>		🟢	Smart-86-AccessProfile		LTM-APM		Export...	Copy...	default-log-setting		Common
<input type="checkbox"/>		🟢	Test		SSO				default-log-setting		Common
<input type="checkbox"/>		🟢	access		All	(none)	(none)	(none)			Common
<input type="checkbox"/>		🟢	profile2		SSL-VPN		Export...	Copy...	default-log-setting		Common
<input type="checkbox"/>		🟢	profile3		LTM-APM		Export...	Copy...	default-log-setting		Common
<input type="checkbox"/>		🟢	profileLDAP		All		Export...	Copy...	default-log-setting	IdP Idp_Test	Common

Delete... | Apply

- バーチャル ポリシー エディタは開きます



- アイコンを<sup>+</sup>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。

Properties

Branch Rules

Name: AD Auth

**Active Directory**

Type	Authentication ↕
Server	/Common/adfs ↕
Cross Domain Support	Disabled ↕
Complexity check for Password Reset	Disabled ↕
Show Extended Error	Disabled ↕
Max Logon Attempts Allowed	3 ↕
Max Password Reset Attempts Allowed	3 ↕

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。

Properties **Branch Rules**

Name:

---

**Active Directory**

Type	Query
Server	/Common/adfs
SearchFilter	sAMAccountName=%{session.logon.last.username}
Fetch Primary Group	Disabled
Cross Domain Support	Disabled
Fetch Nested Groups	Disabled
Complexity check for Password Reset	Disabled
Max Password Reset Attempts Allowed	3
Prompt user to change password before expiration	none 0

---

Add new entry Insert Before: 1

Required Attributes (optional)		
1	<input type="text" value="cn"/>	▼ ×
2	<input type="text" value="displayName"/>	▲ ▼ ×
3	<input type="text" value="distinguishedName"/>	▲ ▼ ×
4	<input type="text" value="dn"/>	▲ ▼ ×
5	<input type="text" value="employeeID"/>	▲ ▼ ×
6	<input type="text" value="givenName"/>	▲ ▼ ×
7	<input type="text" value="homeMDB"/>	▲ ▼ ×
8	<input type="text" value="mail"/>	▲ ▼ ×

Cancel Save Help

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。

Properties **Branch Rules**

Name:

---

**Resource Assignment**

[Add new entry](#) Ins

---

**Expression:** *Empty* [change](#)

---

1 **SAML:** /Common/ids\_pipeline, /Common/smart-86-samlresource  
**Webtop:** /Common/Smart-86-Webtop  
[Add/Delete](#)

## 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	

- 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
IdSSAMLAyncServlet.java:465 - retrievefrom : user_principal
YYYY-MM-DD hh: mm: SS.sss GMT(-0000) [IdSEndPoints-SAML-59] com.cisco.ccbu.ids
IdSSAMLAyncServlet.java:298 - com.sun.identity.saml.common.SAMLException
responseprocessingfailed SAML: saml user_principal
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributeFromAttributesMap(IdSSAMLAyncServlet.java:4
66)
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet.java:263
)
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet.java:17
6)
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](#)