

# 為思科身份服務(IdS)安裝和配置F5身份提供程式(IdP)以啟用SSO

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[安裝](#)

[設定](#)

[建立安全斷言標籤語言\(SAML\)](#)

[SAML資源](#)

[Webtops](#)

[虛擬原則編輯器](#)

[服務提供商\(SP\)後設資料交換](#)

[驗證](#)

[疑難排解](#)

[通用存取卡\(CAC\)驗證失敗](#)

[相關資訊](#)

## 簡介

本檔案介紹F5 BIG-IP身份提供程式(IdP)上啟用單一登入(SSO)的配置。

### Cisco IdS部署模式

#### 產品 部署

UCCX 共住者

PCCE 與CUIC ( 思科統一情報中心 ) 和LD ( 即時資料 ) 共存

與CUIC和LD共駐以進行2k部署。

UCCE 獨立式，適用於4k和12k部署。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco Unified Contact Center Express(UCCX)版本11.6或Cisco Unified Contact Center Enterprise版本11.6或Packaged Contact Center Enterprise(PCCE)版本11.6 ( 如果適用 ) 。

**附註：**本文檔引用有關思科身份識別服務(IdS)和身份提供方(IdP)的配置。文檔在螢幕截圖和示例中引用UCCX，但是配置與思科身份識別服務(UCCX/UCCE/PCCE)和IdP相似。

## 採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 安裝

Big-IP是一種具有多種功能的打包解決方案。存取原則管理員 (APM)，與身份提供商服務共同相關。

Big-IP作為APM:

版本 13.0

類型 虛擬版(OVA)

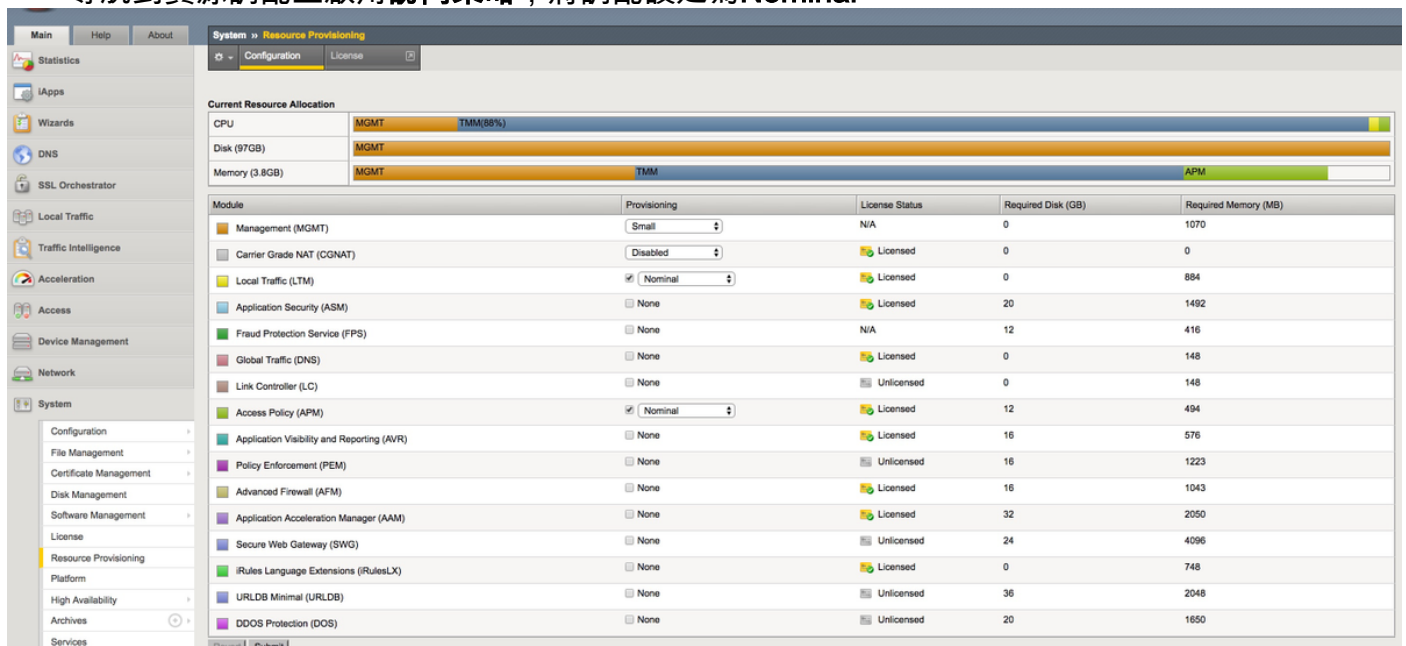
IP 不同子網中的兩個IP。一個用於管理IP  
一個用於IdP虛擬伺服器

從Big-IP網站下載虛擬版映像，並部署OVA以建立預先安裝的虛擬機器(VM)。獲取許可證並按基本要求安裝。

附註：有關安裝資訊，請參閱[Big-IP安裝指南](#)。

## 設定

- 導航到資源調配並啟用訪問策略，將調配設定為Nominal



The screenshot displays the 'Resource Provisioning' configuration page in the Big-IP management interface. The 'Current Resource Allocation' section shows CPU at 88% (MGMT), Disk at 97GB (MGMT), and Memory at 3.8GB (MGMT). The 'Module' table lists various services and their configurations:

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

- 在Network -> VLAN下建立新的VLAN

The screenshot displays the F5 Network Management interface. At the top left, the status is 'ONLINE (ACTIVE) Standalone'. The navigation menu on the left includes 'Main', 'Help', and 'About', followed by various network management tools like 'Statistics', 'iApps', 'Wizards', 'DNS', 'SSL Orchestrator', 'Local Traffic', 'Traffic Intelligence', 'Acceleration', 'Access', 'Device Management', and 'Network'. The 'Network' section is expanded to show 'VLANs', which is further expanded to 'external'. The main content area shows the configuration for this VLAN. Under 'General Properties', the Name is 'external', Partition / Path is 'Common', Description is empty, and Tag is '4093'. The 'Resources' section shows 'Interfaces' with a list containing '1.1 (untagged)'. Below this, the 'Configuration' section is set to 'Basic' and includes 'Source Check' (unchecked), 'MTU' (1500), and 'Auto Last Hop' (Default). The 'sFlow' section shows 'Polling Interval' (Default, 10 seconds) and 'Sampling Rate' (Default, 2048 packets). At the bottom, there are 'Update', 'Cancel', and 'Delete' buttons.

- 在Network -> Self IPs下為IP建立新條目，用於IdP

**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"/>

- 在Access -> Profile/Policies -> Access profiles下建立配置檔案

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)														

- 建立虛擬伺服器

**General Properties**

Name	ldp_Test
Partition / Path	Common
Description	<input type="text"/>
Type	Standard ▾
Source Address	<input type="text" value="0.0.0.0/0"/>
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><b>/Common</b> 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><b>/Common</b> 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><b>/Common</b> 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><b>/Common</b> 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"/>	

- 在Access -> Authentication -> Active Directory下新增Active Directory(AD)詳細資訊



## 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



- 在Access -> Federation -> SAML Identity Provider ->本地IdP服務下建立新的IdP服務

### 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

**附註：** 如果使用通用訪問卡(CAC)進行身份驗證，則需要在**SAML屬性配置**部分新增以下屬性：

步驟1. 建立uid屬性。

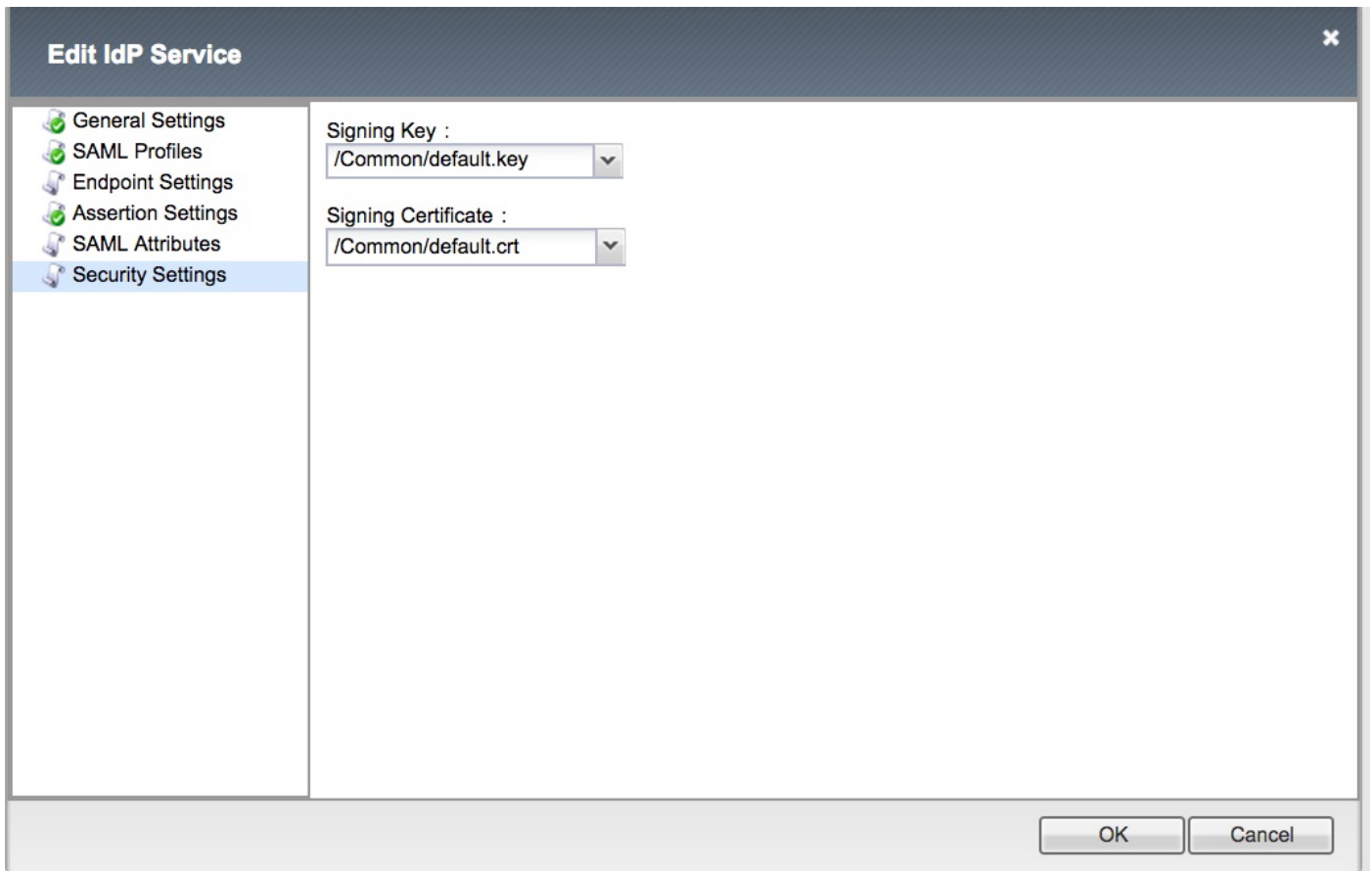
名稱: uid

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

步驟2. 建立user\_principal屬性。

名稱: user\_principal

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



附註：建立IdP服務後，在Access -> Federation -> SAML Identity Provider -> Local IdP Services下，有一個用於下載後設資料的選項，該選項帶有Export Metadata按鈕

## 建立安全斷言標籤語言(SAML)

### SAML資源

- 導航到Access -> Federation -> SAML Resources，然後建立一個saml資源以與之前建立的IdP服務相關聯



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

- 在Access -> Webtop下建立Webtop



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

**虛擬原則編輯器**

- 導航到之前建立的策略，然後按一下編輯連結

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

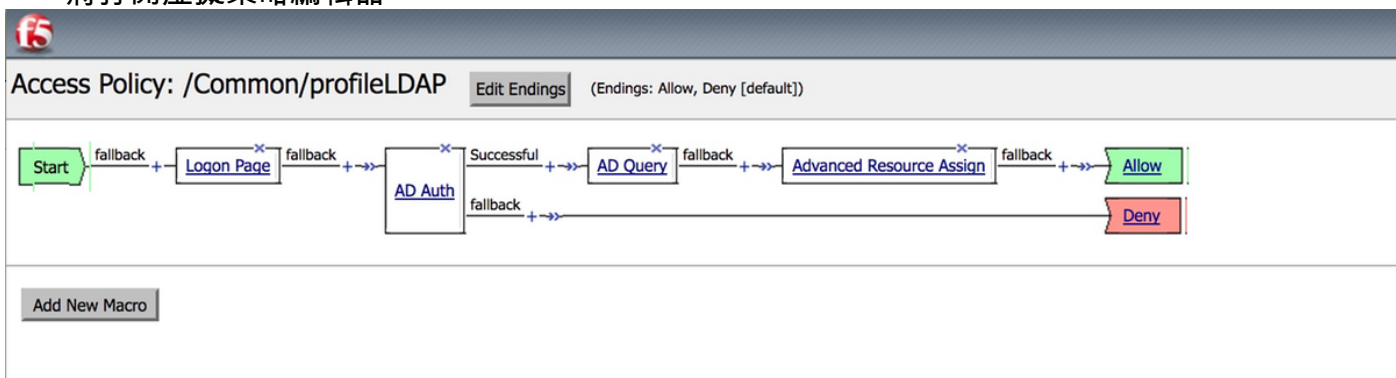
Access Profiles | Per-Request Policies | Policy Sync | Customization

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

- 將打開虛擬策略編輯器



- 按一下 圖示並按所述新增元素

步驟1. Logon page element — 保留所有元素為預設值。

步驟2. AD Auth ->選擇先前建立的ADFS組態。

Properties

Branch Rules

Name:

**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 ↕

步驟3. AD查詢元素 — 分配必要的詳細資訊。



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

步驟4. Advanced Resource Assign — 將saml資源與先前建立的webtop相關聯。

The screenshot shows a web interface with two tabs: 'Properties' and 'Branch Rules'. The 'Branch Rules' tab is active. Below the tabs, there is a 'Name' field containing 'Advanced Resource Assign'. Underneath, there is a section titled 'Resource Assignment' with a blue header bar containing an 'Add new entry' button and the text 'Ins'. Below this, there is a section titled 'Expression: Empty' with a 'change' link. A list of resources is shown, starting with '1 SAML: /Common/ids\_pipeline, /Common/smart-86-samlresource' and 'Webtop: /Common/Smart-86-Webtop'. At the bottom of the list, there is a link 'Add/Delete'.

## 服務提供商(SP)後設資料交換

- 通過System -> Certificate Management -> Traffic Management手動將Id的證書匯入Big-IP

附註：確保證書由BEGIN CERTIFICATE和END CERTIFICATE標籤組成。

## 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	

- 在Access -> Federation -> SAML Identity Provider -> 外部SP聯結器下從sp.xml建立新條目
- 將SP聯結器繫結到Access -> Federation -> SAML Identity Provider -> Local IdP Services下的IdP服務

## 驗證

目前沒有適用於此組態的驗證程序。

## 疑難排解

### 通用存取卡(CAC)驗證失敗

如果CAC使用者的SSO身份驗證失敗，請檢查UCCX ids.log以驗證SAML屬性是否設定正確。

如果存在配置問題，則會發生SAML故障。例如，在此日誌代碼片段中，IdP上未配置user\_principal

SAML屬性。

YYYY-MM-DD hh:mm:ss.sss GMT(-0000)[IdSEndPoints-SAML-59] ERROR

com.cisco.ccbu.ids [IdSSAMLAyncServlet.java:465](#) - **user\_principal**

YYYY-MM-DD hh:mm:ss.sss GMT(-0000)[IdSEndPoints-SAML-59] ERROR

com.cisco.ccbu.ids [IdSSAMLAyncServlet.java:298](#) - **SAMLcom.sun.identity.saml.common.SAMLException:  
samluser\_principal**

com.cisco.cbu.ids.auth.api.IdSSAMLAyncServlet.getAttributeFromAttributesMap(IdSSAMLAyncServlet.java:466)

com.cisco.cbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet.java:263)

com.cisco.cbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet.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)

## 相關資訊

- [技術支援與文件 - Cisco Systems](#)