

Install and Configure the F5 Identity Provider (IdP) for Cisco Identity Service (IdS) to enable SSO

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Install](#)

[Configure](#)

[Security Assertion Markup Language \(SAML\) creation](#)

[SAML Resources](#)

[Webtops](#)

[Virtual Policy Editor](#)

[Service Provider \(SP\) Metadata Exchange](#)

[Verify](#)

[Troubleshoot](#)

[Common Access Card \(CAC\) Authentication Failure](#)

[Related Information](#)

Introduction

This document describes the configuration on the F5 BIG-IP Identity Provider (IdP) to enable Single Sign On (SSO).

Cisco IdS Deployment Models

Product Deployment

UCCX Co-resident

PCCE Co-resident with CUIC (Cisco Unified Intelligence Center) and LD (Live Data)

UCCE Co-resident with CUIC and LD for 2k deployments.

Standalone for 4k and 12k deployments.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Contact Center Express (UCCX) Release 11.6 or Cisco Unified Contact Center Enterprise Release 11.6 or Packaged Contact Center Enterprise (PCCE) Release 11.6 as applicable.

Note: This document references the configuration with respect to the Cisco Identify Service (IdS) and the Identity Provider (IdP). The document references UCCX in the screenshots and examples, however the configuration is similar with respect to the Cisco Identify Service (UCCX/UCCE/PCCE) and the 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. If your network is live, ensure that you understand the potential impact of any command.

Install

Big-IP is a packaged solution that has multiple features. Access Policy Manager (APM) which correlates to the Identity Provider service.

Big-IP as APM:

Version 13.0

Type Virtual Edition(OVA)

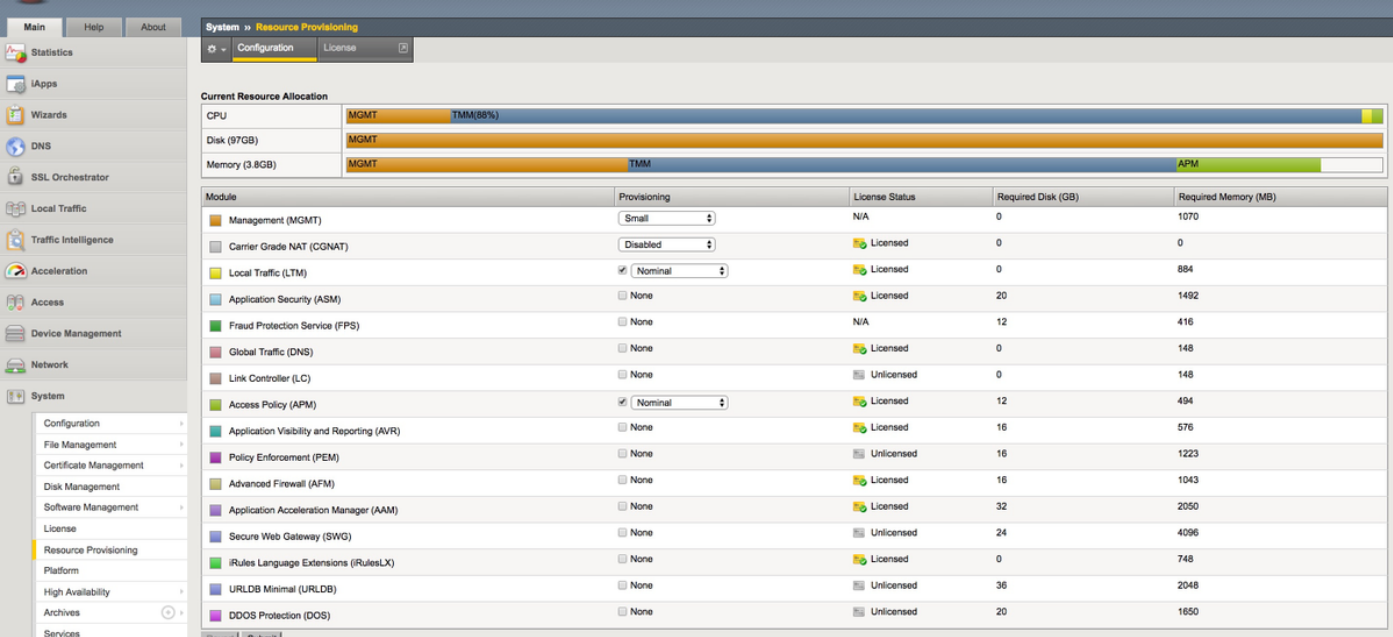
IPs Two IPs in different subnets. One for the management IP and one for the IdP virtual server

Download the virtual edition image from Big-IP website and deploy the OVA to create a Virtual Machine (VM) that is pre-installed. Obtain the license and install with the basic requirements.

Note: For installation information, refer to [Big-IP Installation guide](#).

Configure

- Navigate to resource provisioning and enable **Access Policy**, set provisioning to **Nominal**



The screenshot shows the 'System > Resource Provisioning' configuration page. At the top, there are tabs for 'Configuration' and 'License'. Below this, a 'Current Resource Allocation' section shows three progress bars: CPU (MGMT, TMM:88%), Disk (97GB, MGMT), and Memory (3.8GB, MGMT, TMM, APM). The main part of the page is a table listing various modules 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)	<input checked="" type="checkbox"/> (Nominal)	Licensed	0	884
Application Security (ASM)	<input type="checkbox"/> None	Licensed	20	1492
Fraud Protection Service (FPS)	<input type="checkbox"/> None	N/A	12	416
Global Traffic (DNS)	<input type="checkbox"/> None	Licensed	0	148
Link Controller (LC)	<input type="checkbox"/> None	Unlicensed	0	148
Access Policy (APM)	<input checked="" type="checkbox"/> (Nominal)	Licensed	12	494
Application Visibility and Reporting (AVR)	<input type="checkbox"/> None	Licensed	16	576
Policy Enforcement (PEM)	<input type="checkbox"/> None	Unlicensed	16	1223
Advanced Firewall (AFM)	<input type="checkbox"/> None	Licensed	16	1043
Application Acceleration Manager (AAM)	<input type="checkbox"/> None	Licensed	32	2050
Secure Web Gateway (SWG)	<input type="checkbox"/> None	Unlicensed	24	4096
iRules Language Extensions (RulesLX)	<input type="checkbox"/> None	Licensed	0	748
URLDB Minimal (URLDB)	<input type="checkbox"/> None	Unlicensed	36	2048
DDOS Protection (DOS)	<input type="checkbox"/> None	Unlicensed	20	1650

- Create a new VLAN under **Network -> VLANs**

The screenshot displays the F5 network management console. The top navigation bar shows 'Network >> VLANs : VLAN List >> external'. The left sidebar contains a tree view with 'Network' expanded and 'VLANs' selected. The main content area is titled 'Properties' and 'Layer 2 Static Forwarding Table'. It is divided into several sections: 'General Properties' with fields for Name (external), Partition / Path (Common), Description (empty), and Tag (4093); 'Resources' with 'Interfaces' section showing '1.1 (untagged)' and options for Interface (1.2) and Tagging (Select...); 'Configuration: Basic' with fields for Source Check (unchecked), MTU (1500), and Auto Last Hop (Default); and 'sFlow' with fields for Polling Interval (Default, 10 seconds) and Sampling Rate (Default, 2048 packets). At the bottom are 'Update', 'Cancel', and 'Delete' buttons.

- Create a new entry for the IP which is used for the IdP under **Network -> Self IPs**

**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"/>

- Create a profile under **Access** -> **Profile/Policies** -> **Access profiles**

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	Accepted Languages
	English (en)
	Factory BuiltIn Languages
	Japanese (ja)
	Chinese (Simplified) (zh-cn)
	Chinese (Traditional) (zh-tw)
	Korean (ko)
	Spanish (es)
	French (fr)

- Create a virtual server

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>/Common clientssl</p> </div> <div style="text-align: center; width: 10%;"> <p><<</p> <p>>></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 splitstion-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><<</p> <p>>></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 ▾
Content Rewrite	
Rewrite Profile	+ None ▾
HTML Profile	None ▾
Access Policy	
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 ▾
Acceleration	
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"/>	

- Add Active Directory (AD) details under **Access -> Authentication -> Active Directory**



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	IP Address: <input type="text"/> Hostname: <input type="text"/> <input type="button" value="Add"/> <div style="border: 1px solid gray; padding: 5px; min-height: 100px;"> 10.78.93.153 adfsserver.cisco.com </div> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
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

- Create a new IdP service under **Access -> Federation -> SAML Identity Provider -> Local IdP Services**

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

Note: If a Common Access Card (CAC) is used for authentication, these attributes need to be added in the **SAML Attributes** configuration section:

Step 1. Create the **uid** attribute.

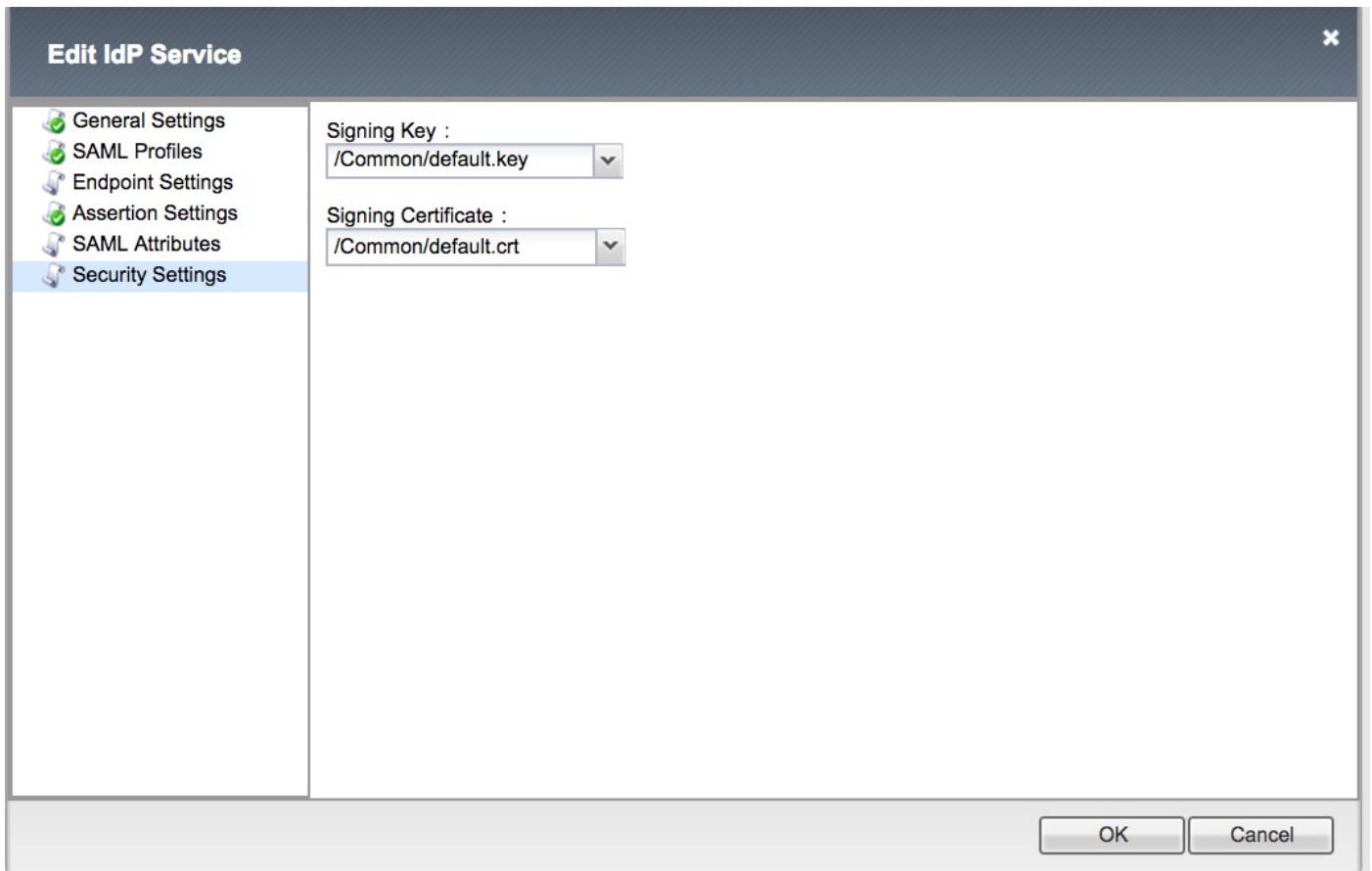
Name: uid

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

Step 2. Create the **user_principal** attribute.

Name: user_principal

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



Note: Once the IdP service is created, there is an option to download the metadata with a button **Export Metadata** under **Access -> Federation -> SAML Identity Provider -> Local IdP Services**

Security Assertion Markup Language (SAML) creation

SAML Resources

- Navigate to **Access -> Federation -> SAML Resources** and create a saml resource to associate with the IdP service that was created earlier



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 View/Hide

Webtops

- Create a webtop under **Access** -> **Webtops**



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

Virtual Policy Editor

- Navigate to the policy created earlier and click on edit link

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

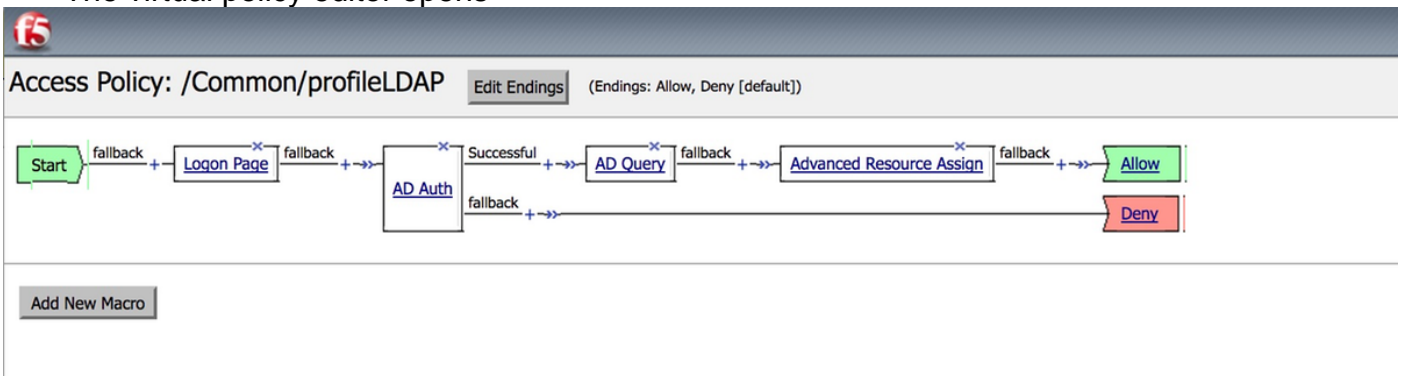
Access Profiles | Per-Request Policies | Policy Sync | Customization


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)	(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

- The virtual policy editor opens



- Click on the  icon and add elements as described
- Step 1. **Logon page element** - Leave all elements to default.
- Step 2. **AD Auth** -> Choose the ADFS configuration created earlier.

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 ↕

Step 3. **AD Query element** - Assign the necessary details.

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

Step 4. **Advance Resource Assign** - Associate the saml resource and the webtop created earlier.

Properties **Branch Rules**

Name:

Resource Assignment

Ins

Expression: *Empty* [change](#)

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

Service Provider (SP) Metadata Exchange

- Manually import the certificate of the IdS to Big-IP through **System -> Certificate Management -> Traffic Management**

Note: Ensure that the certificate consists of BEGIN CERTIFICATE and END CERTIFICATE tags.

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	

- Create a new entry from sp.xml under **Access -> Federation -> SAML Identity Provider -> External SP Connectors**
- Bind the SP connector to the IdP service under **Access -> Federation -> SAML Identity Provider -> Local IdP Services**

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Common Access Card (CAC) Authentication Failure

If SSO authentication fails for CAC users, check the UCCX ids.log to verify the SAML Attributes were set properly.

If there is a configuration issue, a SAML failure occurs. For example, in this log snippet, the user_principal SAML attribute is not configured on the IdP.

```
YYYY-MM-DD hh:mm:ss.sss GMT(-0000) [IdSEndPoints-SAML-59] ERROR
com.cisco.ccbu.ids IdSSAMLAyncServlet.java:465 - Could not retrieve from attributes map: user_principal
YYYY-MM-DD hh:mm:ss.sss GMT(-0000) [IdSEndPoints-SAML-59] ERROR
com.cisco.ccbu.ids IdSSAMLAyncServlet.java:298 - SAML response processing failed with exception
com.sun.identity.saml.common.SAMLException: Could not retrieve user_principal from saml response
at
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributeFromAttributesMap(IdSSAMLAyncServlet.java:4
66)
at
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet.java:263
)
at
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet.java:17
6)
at com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
at java.lang.Thread.run(Thread.java:745)
```

Related Information

- [Technical Support & Documentation - Cisco Systems](#)