

# Instale y configure el proveedor de la identidad F5 (IdP) para el servicio de la identidad de Cisco (IdS) para habilitar el SSO

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Instalar](#)

[Configurar](#)

[Creación del lenguaje de marcado de la aserción de la Seguridad \(SAML\)](#)

[SAML recursos](#)

[Webtops](#)

[Editor de políticas virtual](#)

[Intercambio de los meta datos del proveedor de servicio \(SP\)](#)

[Verificación](#)

[Troubleshooting](#)

[Falla de autenticación común del indicador luminoso LED amarillo de la placa muestra gravedad menor del acceso \(CAC\)](#)

[Información Relacionada](#)

## Introducción

Este documento describe la configuración en el proveedor de la identidad F5 BIG-IP (IdP) para habilitar la sola muestra encendido (SSO).

### Modelos de despliegue del Cisco IDS

#### Producto Despliegue

UCCX Coresidente

PCCE Coresidente con CUIIC (centro unificado Cisco de la inteligencia) y LD (datos vivos)

UCCE Coresidente con CUIIC y el LD para las implementaciones 2k.

Independiente para las implementaciones 4k y 12k.

## Prerrequisitos

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Versión 11.6 del Cisco Unified Contact Center Express (UCCX) o versión 11.6 del Cisco Unified Contact Center Enterprise o versión embalada 11.6 de la empresa del Centro de

contacto (PCCE) como aplicables.

**Note:** Este documento se refiere a la configuración en cuanto al servicio de Cisco Identity (IdS) y al proveedor de la identidad (IdP). El documento se refiere a UCCX al screenshots y a los ejemplos, no obstante la configuración es similar en cuanto al servicio de Cisco Identity (UCCX/UCCE/PCCE) y al IdP.

## Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

## Instalar

El Grande-IP es una solución embalada que tiene características múltiples. Administrador de la política de acceso (APM) que co-se relaciona con el servicio del proveedor de la identidad.

Grande-IP como APM:

Versión 13.0

Tipo Edition(OVA) virtual

IP Dos IP en diversas subredes. Uno para el IP de administración y uno para el servidor virtual de IdP

Descargue la imagen virtual de la edición del sitio web Grande-IP y despliegue los HUEVOS para crear una máquina virtual (VM) se instale previamente que. Obtenga la licencia y instalela con los requisitos básicos.

**Note:** Para la información de la instalación, refiera a la [guía de instalación Grande-IP](#).

## Configurar

- Navegue al aprovisionamiento del recurso y habilite la **política de acceso**, fije el aprovisionamiento al **nominal**

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

Reverse Submit

- Cree un nuevo VLA N bajo red - > los VLA N

ONLINE (ACTIVE)  
Standalone

Main Help About

Network » VLANs : VLAN List » external

Properties Layer 2 Static Forwarding Table

### General Properties

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

### Resources

Interfaces

Interface: 1.2  
Tagging: Select...  
Add

1.1 (untagged)

Edit Delete

Configuration: Basic

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

### sFlow

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

Update Cancel Delete

System

Statistics  
iApps  
Wizards  
DNS  
SSL Orchestrator  
Local Traffic  
Traffic Intelligence  
Acceleration  
Access  
Device Management  
Network  
Interfaces  
Routes  
Self IPs  
Packet Filters  
Trunks  
Tunnels  
Route Domains  
VLANs  
Service Policies  
Network Security  
Class of Service  
ARP  
IPsec  
WCCP  
DNS Resolvers  
Rate Shaping

- Cree una nueva entrada para el IP que se utiliza para el IdP bajo red - > el uno mismo IP

**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"/>

- Cree un perfil bajo acceso - > perfil/las directivas - > los perfiles del acceso

General Properties	
Name	profileLDAP
Partition / Path	Common
Parent Profile	access
Profile Type	All
Profile Scope	Virtual Server ▾

Settings	
Inactivity Timeout	30 <input type="text"/> seconds
Access Policy Timeout	30 <input type="text"/> seconds
Maximum Session Timeout	30 <input type="text"/> seconds
Minimum Authentication Failure Delay	2 <input type="text"/> seconds
Maximum Authentication Failure Delay	5 <input type="text"/> seconds
Max Concurrent Users	5 <input type="text"/>
Max Sessions Per User	2 <input type="text"/>
Max In Progress Sessions Per Client IP	128 <input type="text"/>
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 <input type="text"/> 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)														

- Cree a un servidor virtual

**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 splitssession-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"/>	

- Agregue los detalles del Active Directory (AD) bajo acceso - > autenticación - > 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	<p>IP Address: <input type="text"/></p> <p>Hostname: <input type="text"/></p> <p><input type="button" value="Add"/></p> <div><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

- Cree un nuevo servicio de IdP bajo acceso - > federación - > SAML proveedor de la identidad - > los servicios locales de IdP

### 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:** Si un indicador luminoso LED amarillo de la placa muestra gravedad menor común del acceso (CAC) se utiliza para la autenticación, estos atributos necesitan ser agregados en la sección de configuración de los **atributos de SAML**:

Paso 1. Cree el atributo del **uid**.

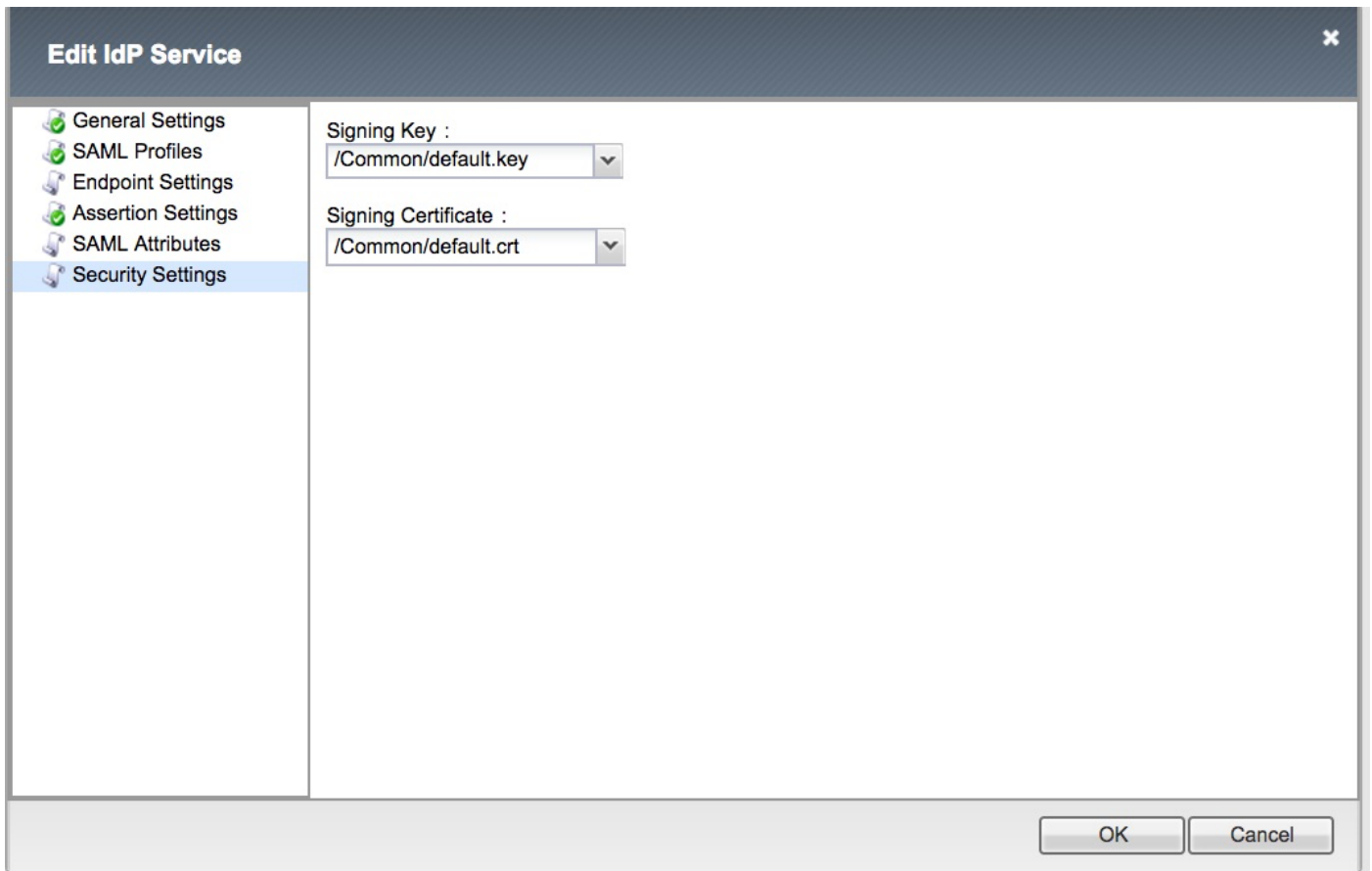
**Nombre:** uid

**Valor:** % {session.Idap.last.attr.sAMAccountName}

Paso 2. Cree el atributo **user\_principal**.

**Nombre:** user\_principal

**Valor:** % {session.Idap.last.attr.userPrincipalName}



**Note:** Una vez que el servicio de IdP se crea, hay una opción para descargar los meta datos con los **meta datos de una exportación del botón bajo acceso - > federación - > SAML proveedor de la identidad - > los servicios locales de IdP**

## Creación del lenguaje de marcado de la aserción de la Seguridad (SAML)

### SAML recursos

- Navegue **para acceder - > federación - > SAML los recursos** y para crear un recurso del saml para asociarse al servicio de IdP que fue creado anterior



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**

- Cree un webtop bajo acceso - > 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

**Editor de políticas virtual**

- Navegue a la directiva creada anterior y haga clic en editan el link

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

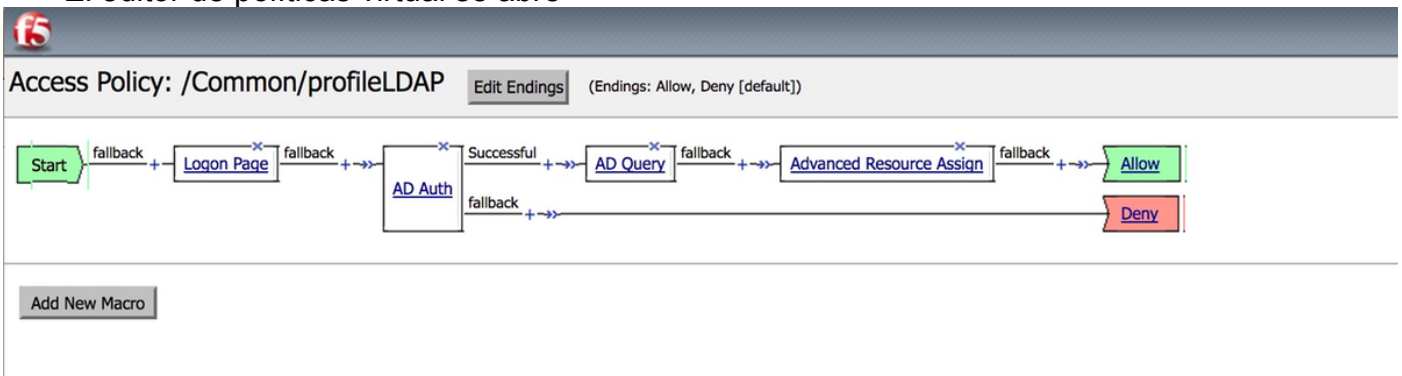
Access Profiles | Per-Request Policies | Policy Sync | Customization

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)			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

- El editor de políticas virtual se abre



- Haga clic en el icono y agregue los elementos según lo descrito

Paso 1. **Elemento de la página del inicio** - Deje todos los elementos para omitir.

Paso 2. **Auth AD** - > elija la configuración ADFS creada anterior.



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 ↕

Paso 3. Elemento de la interrogación AD - Asigne los detalles necesarios.

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

Paso 4. El recurso anticipado asigna - Asocie el recurso del saml y el webtop creados anterior.

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](#)

## Intercambio de los meta datos del proveedor de servicio (SP)

- Importe manualmente el certificado de los IdS al Grande-IP a través del **sistema** - Certificate Management (Administración de certificados) - > Traffic Management

**Note:** Asegúrese de que el certificado consista en COMIENZE las etiquetas del CERTIFICADO y del CERTIFICADO del EXTREMO.

## 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

- Cree una nueva entrada de sp.xml bajo el **proveedor de Access**-> Federation-> SAMLIDENTITY - > **los conectores de ExternalSP**
- Ate el conector SP al servicio de IdP bajo **acceso** - > **federación** - > **SAML proveedor de la identidad** - > **los servicios locales de IdP**

## Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

## Troubleshooting

**Falla de autenticación común del indicador luminoso LED amarillo de la placa muestra gravedad menor del acceso (CAC)**

Si la autenticación SSO falla para los usuarios CAC, marque el UCCX ids.log para verificar los

atributos de SAML fueron fijados correctamente.

Si hay un problema de configuración, un error de SAML ocurre. Por ejemplo, en este snippet del registro, el atributo user\_principal de SAML no se configura en el IdP.

```
Hh YYYY-MM-DD: milímetro: ERROR com.cisco.ccbu.ids.IdSSAMLAyncServlet.java:465 SS.sss GMT(-0000)
[IdSEndPoints-SAML-59] - No podría la correspondencia de los atributos del retrievefrom: user_principal
Hh YYYY-MM-DD: milímetro: ERROR com.cisco.ccbu.ids.IdSSAMLAyncServlet.java:298 SS.sss GMT(-0000)
[IdSEndPoints-SAML-59] - SAML responseprocessingfailed con la excepción
com.sun.identity.saml.common.SAMLException: No podía extraer user_principal de la respuesta del
saml
en
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributeFromAttributesMap(IdSSAMLAyncServlet.java:4
66)
en
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet.java:263
)
en
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet.java:17
6)
en com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)
en java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
en java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
en java.lang.Thread.run(Thread.java:745)
```

## Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)