

# Installez et configurez le fournisseur de l'identité F5 (IDP) pour la gestion d'identité de Cisco (id) pour activer SSO

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Installez](#)

[Configurer](#)

[Création du Langage SAML \(SAML\)](#)

[Ressources SAML](#)

[Webtops](#)

[Éditeur de stratégie virtuel](#)

[Échange de métadonnées de fournisseur de services \(fournisseur de services\)](#)

[Vérifier](#)

[Dépanner](#)

[Échec d'authentification commun de la carte d'accès \(CAC\)](#)

[Informations connexes](#)

## Introduction

Ce document décrit la configuration sur le fournisseur d'identité F5 BIG-IP (IDP) pour activer simple se connectent (SSO).

### Modèles de déploiement d'id de Cisco

#### Produit Déploiement

UCCX Co-résident

PCCE Co-résident avec CUIC (centre d'intelligence de Cisco Unified) et LD (données vivantes)

UCCE Co-résident avec CUIC et LD pour les déploiements 2k.

Autonome pour les déploiements 4k et 12k.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Version 11.6 de version 11.6 ou de Cisco Unified Contact Center Enterprise du Cisco Unified Contact Center Express (UCCX) ou version 11.6 emballée du Contact Center Enterprise (PCCE) comme applicable.

**Note:** Ce document met en référence la configuration en ce qui concerne le service de Cisco Identity (id) et le fournisseur d'identité (IDP). Le document met en référence UCCX dans les captures d'écran et les exemples, toutefois la configuration est semblable en ce qui concerne le service de Cisco Identity (UCCX/UCCE/PCCE) et l'IDP.

## Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

## Installez

Le Grand-IP est une solution emballée qui a de plusieurs caractéristiques. Accédez au Policy Manager (APM) qui Co-associe au service de fournisseur d'identité.

Grand-IP comme APM :

Version 13.0

**Type** Edition(OVA) virtuel

**IPS** Deux IPS dans les différents sous-réseaux. Un pour l'IP de Gestion et un pour le serveur virtuel d'IDP

Téléchargez l'image virtuelle d'édition du site Web Grand-IP et déployez les OVULES pour créer un virtual machine (VM) qui est préinstallé. Obtenez le permis et l'installez avec les exigences de base.

**Note:** Pour les informations d'installation, référez-vous au [guide d'installation Grand-IP](#).

## Configurer

- Naviguez vers le ravitaillement de ressource et activez la **stratégie d'Access**, placez le ravitaillement au **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

Revert Submit

- Créez un nouveau VLAN sous le réseau - > des VLAN

 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

- Créez une nouvelle entrée pour l'IP qui est utilisé pour l'IDP sous le réseau -> l'individu 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"/>

- Créez un profil sous **Access** - > **profil/stratégies** - > **des profils d'Access**

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)														

- Créez un serveur virtuel

**General Properties**

Name	ldp_Test
Partition / Path	Common
Description	<input type="text"/>
Type	Standard ▾
Source Address	0.0.0.0/0 <input type="text"/>
Destination Address/Mask	10.78.93.62 <input type="text"/>
Service Port	443 <input type="text"/> 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"/>	

- Ajoutez les détails de Répertoire actif (AD) sous **Access** - > **authentification** - > **Répertoire actif**



## 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 gray; 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

- Créez un nouveau service d'IDP sous **Access - > fédération - > fournisseur d'identité SAML - > des services locaux d'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 une carte d'accès commune (CAC) est utilisée pour l'authentification, ces attributs doivent être ajoutés dans la section de configuration d'**attributs SAML** :

Étape 1. Créez l'attribut d'**uid**.

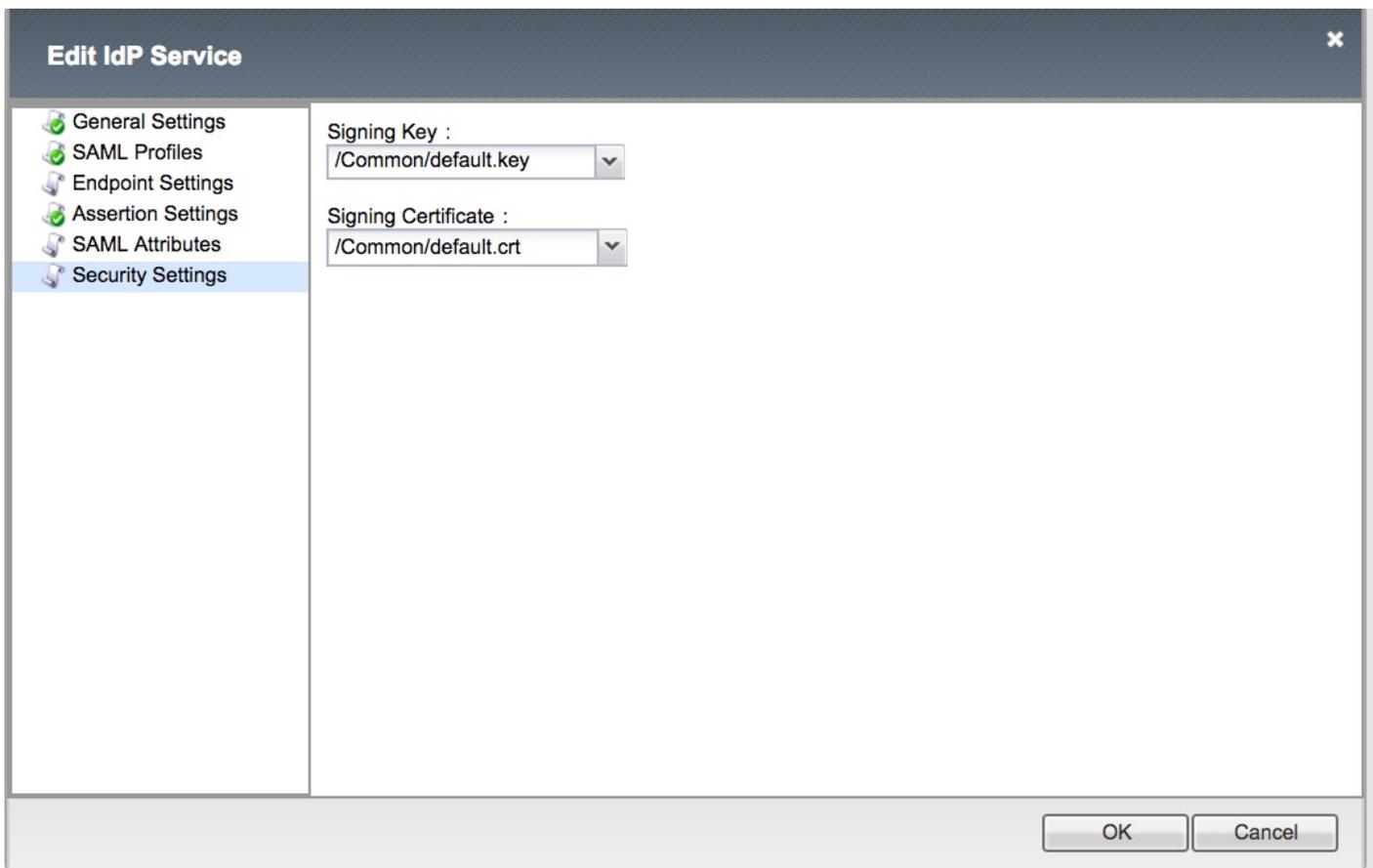
**Nom** : uid

**Valeur** : % {session ldap.last.attr.sAMAccountName}

Étape 2. Créez l'attribut **user\_principal**.

**Nom** : user\_principal

**Valeur** : % {session ldap.last.attr.userPrincipalName}



**Note:** Une fois que le service d'IDP est créé, il y a une option de télécharger les métadonnées avec des **métadonnées d'une exportation de bouton** sous **Access** - > **fédération** - > **fournisseur d'identité SAML** - > **des services locaux d'IDP**

## Création du Langage SAML (SAML)

### Ressources SAML

- Naviguez **pour accéder à** - > **fédération** - > **des ressources SAML** et pour créer une ressource en saml pour s'associer avec le service d'IDP qui a été créé plus tôt



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

- Créez un webtop sous 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

**Éditeur de stratégie virtuel**

- Naviguez vers la stratégie créée plus tôt et cliquez sur éditer en fonction le lien

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

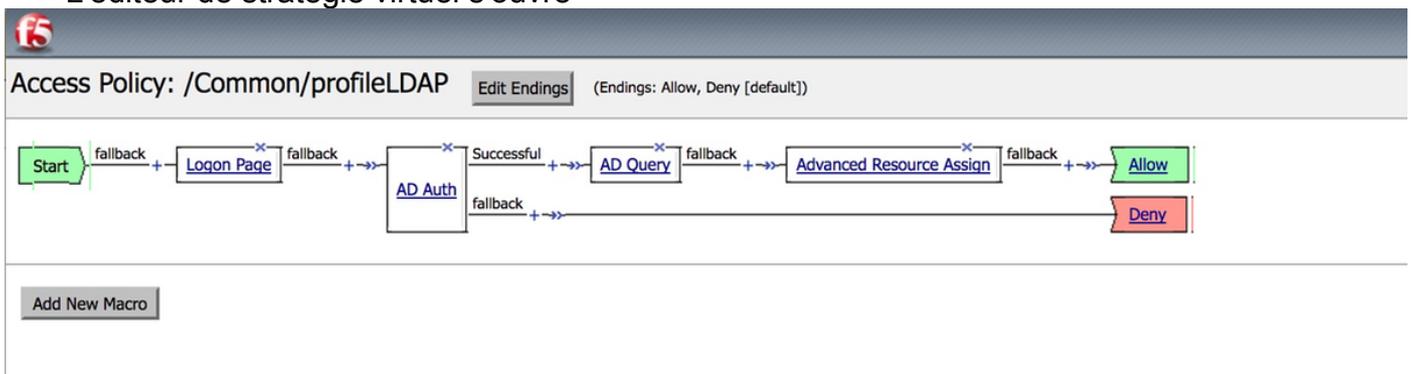
Access Profiles | Per-Request Policies | Policy Sync | Customization

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

- L'éditeur de stratégie virtuelle s'ouvre



- Cliquez sur en fonction l'icône et ajoutez les éléments comme décrit
- Étape 1. **Élément de page de connexion** - Laissez tous les éléments pour se transférer.
- Étape 2. **AD authentique** - > choisissez la configuration ADFS créée plus tôt.

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 ↕

Étape 3. **Élément de requête d'AD** - Assignez les détails nécessaires.

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

Étape 4. La ressource anticipée assignent - Associez la ressource en saml et le webtop créés plus tôt.

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](#)

## Échange de métadonnées de fournisseur de services (fournisseur de services)

- Importez manuellement le certificat des id au Grand-IP par le système - > **Gestion de certificat**  
- > **gestion de trafic**

**Note:** Assurez-vous que le certificat se compose COMMENCENT des balises de CERTIFICAT et de CERTIFICAT d'EXTRÉMITÉ.

## 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

- Créez une nouvelle entrée de sp.xml sous le **fournisseur d'Access**-> Federation-> SAMLIDENTITY - > **des connecteurs d'ExternalSP**
- Liez le connecteur de fournisseur de services au service d'IDP sous **Access** - > **fédération** - > **fournisseur d'identité SAML** - > **des services locaux d'IDP**

## Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépanner

### Échec d'authentification commun de la carte d'accès (CAC)

Si l'authentification SSO échoue pour des utilisateurs CAC, vérifiez l'UCCX ids.log pour vérifier les attributs SAML ont été placés correctement.

S'il y a une question de configuration, une panne SAML se produit. Par exemple, dans cet extrait de log, l'attribut user\_principal SAML n'est pas configuré sur l'IDP.

```
Hh YYYY-MM-DD : millimètre : ERREUR com.cisco.ccbu.ids.IdSSAMLAyncServlet.java:465 SS.sss GMT(-0000) [IdSEndPoints-SAML-59] - Ne pourrait pas la carte d'attributs de retrievefrom : user_principal
```

```
Hh YYYY-MM-DD : millimètre : ERREUR com.cisco.ccbu.ids.IdSSAMLAyncServlet.java:298 SS.sss GMT(-0000) [IdSEndPoints-SAML-59] - SAML responseprocessingfailed à l'exception
```

```
com.sun.identity.saml.common.SAMLException : N'a pas pu récupérer user_principal de la réponse de saml
```

```
àcom.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributeFromAttributesMap(IdSSAMLAyncServlet.java:466)
```

```
àcom.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet.java:263)
```

```
àcom.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet.java:176)
```

```
àcom.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)
```

```
àjava.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
```

```
àjava.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
```

```
àjava.lang.Thread.run(Thread.java:745)
```

## [Informations connexes](#)

- [Support et documentation techniques - Cisco Systems](#)