

# SSO를 활성화하기 위해 Cisco Id(Identity Service)용 F5 IdP(Identity Provider)를 설치하고 구성합니다

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[Install](#)

[구성](#)

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

[SAML 리소스](#)

[웹탑](#)

[가상 정책 편집기](#)

[서비스 공급자\(SP\) 메타데이터 교환](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[CAC\(Common Access Card\) 인증 실패](#)

[관련 정보](#)

---

## 소개

이 문서에서는 SSO(Single Sign On)를 활성화하기 위한 F5 BIG-IP IdP(Identity Provider)의 컨피그레이션에 대해 설명합니다.

Cisco Id 구축 모델

제품	구축
UCCX	공동 거주자
PCCE	CUIC(Cisco Unified Intelligence Center) 및 LD(Live Data)와 공동 상주
UCCE	2k 구축을 위해 CUIC 및 LD와 공동 상주 4k 및 12k 구축을 위한 독립형

## 사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco UCCX(Unified Contact Center Express) 릴리스 11.6 또는 Cisco Unified Contact Center Enterprise 릴리스 11.6 또는 PCCE(Packaged Contact Center Enterprise) 릴리스 11.6이 해당됩니다.

 참고: 이 문서는 Cisco Id(Identify Service) 및 IdP(Identity Provider)와 관련된 구성을 참조합니다. 이 문서는 스크린샷과 예에서 UCCX를 참조하지만, Cisco Id Service(UCCX/UCCE/PCCE) 및 IdP와 관련된 구성은 유사합니다.

## 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## Install

Big-IP는 다양한 기능을 갖춘 패키지형 솔루션입니다. 액세스 정책 관리자 (APM) ID 제공자 서비스와 공동 연관.

Big-IP as APM:

버전	13.0
유형	가상 에디션(OVA)
IP	서로 다른 서브넷에 있는 두 개의 IP. 관리 IP용 1개 하나는 IdP 가상 서버용

Big-IP 웹 사이트에서 Virtual Edition 이미지를 다운로드하고 OVA를 구축하여 사전 설치된 VM(Virtual Machine)을 생성합니다. 라이선스를 받은 다음 기본 요구 사항에 따라 설치합니다.

 참고: 설치 정보는 [Big-IP Installation guide](#)를 참조하십시오.

## 구성

- 리소스 프로비저닝으로 이동하여 액세스 정책을 활성화하고 프로비저닝을 명목상으로 설정합니다

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 (RulesLX)	None	Licensed	0	748
URLDB Minimal (URLDB)	None	Unlicensed	36	2048
DDOS Protection (DOS)	None	Unlicensed	20	1650

Reset Submit

- Network -> VLANs(네트워크 -> VLAN)에서 새 VLAN 생성

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**

Interface: 1.2  
Tagging: Select...  
Add

Interfaces

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

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

System

- Network -> Self IPs(네트워크 -> 셀프 IP)에서 IdP에 사용되는 IP에 대한 새 항목 생성

**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"/>

Update

Cancel

Delete

- Access -> Profile/Policies -> Access profiles(액세스 -> 프로파일/정책 -> 액세스 프로파일)에서 프로필을 만듭니다.

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)            Chinese (Simplified) (zh-cn)            Chinese (Traditional) (zh-tw)            Korean (ko)            Spanish (es)            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)				

- 가상 서버 만들기

**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"/>	

- Access -> Authentication -> Active Directory 아래에 AD(Active Directory) 세부 정보 추가





**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;">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

- Access(액세스) -> Federation(페더레이션) -> SAML Identity Provider(SAML ID 공급자) -> Local IdP Services(로컬 IdP 서비스)에서 새 IdP 서비스를 만듭니다



1단계. uid 특성을 생성합니다..

이름: uid

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

2단계. user\_principal 속성을 생성합니다.

이름: 사용자\_계정

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

**Edit IdP Service**

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

Signing Key :  
/Common/default.key

Signing Certificate :  
/Common/default.crt

OK Cancel



참고: IdP 서비스가 생성되면 Access -> Federation -> SAML Identity Provider -> Local IdP Services에서 Export Metadata(메타데이터 내보내기) 버튼과 함께 메타데이터를 다운로드할 수 있는 옵션이 있습니다.

## SAML(Security Assertion Markup Language) 생성

### SAML 리소스

- Access -> Federation -> SAML Resources로 이동하여 이전에 생성한 IdP 서비스와 연결할 saml 리소스를 생성합니다



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>

웹탑

- Access -> Webtops에서 webtop을 만듭니다



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

가상 정책 편집기

- 이전에 생성한 정책으로 이동하고 edit(수정) 링크를 클릭합니다.

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

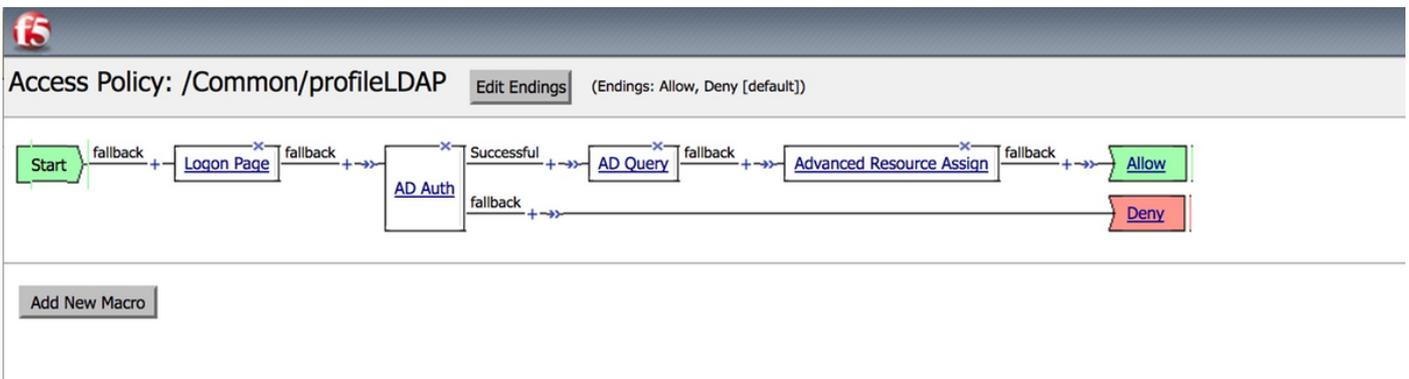
Access Profiles | Per-Request Policies | Policy Sync | Customization

Search

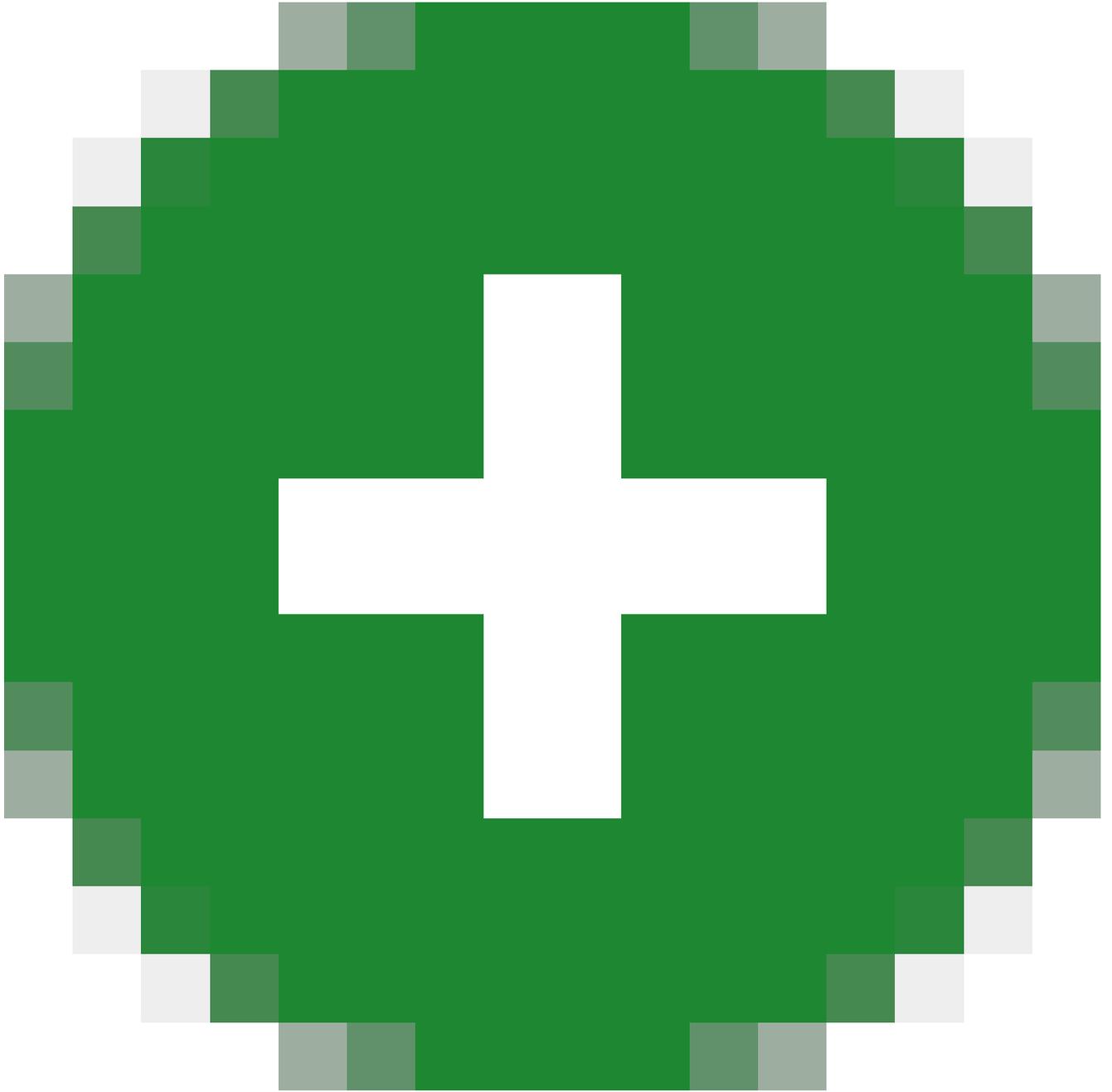
✓	▼	Status	▲ Access Profile Name	◆ Application	◆ Profile Type	Per-Session Policy	Export	Copy	Logs	Virtual Servers	◆ Partition / Path
<input type="checkbox"/>		✔	LDAPAccessProfile		SSO				default-log-setting	LdapVS	Common
<input type="checkbox"/>		✔	Name		All		Export...	Copy...	default-log-setting		Common
<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

- 가상 정책 편집기가 열립니다



- 다음을 클릭합니다.



아이콘 및 설명된 대로 요소 추가

1단계. 로그인 페이지 요소 - 모든 요소를 기본값으로 둡니다.

2단계. AD Auth -> 이전에 생성한 AD FS 컨피그레이션을 선택합니다.

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 ↕

3단계. AD 질의 요소 - 필요한 상세내역을 지정합니다.

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

4단계. 고급 리소스 할당 - saml 리소스와 이전에 작성한 webtop을 연결합니다.



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](#)

## 서비스 공급자(SP) 메타데이터 교환

- System -> Certificate Management -> Traffic Management를 통해 Id의 인증서를 Big-IP로 수동으로 가져옵니다.

 참고: 인증서가 BEGIN CERTIFICATE 및 END CERTIFICATE 태그로 구성되어 있는지 확인합니다.

### 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 -> SAML Identity Provider -> External SP Connectors 아래에서 sp.xml에서 새 항목을 만듭니다.
- Access -> Federation -> SAML Identity Provider -> Local IdP Services의 IdP 서비스에 SP 컨넥터를 바인딩합니다.

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

## 문제 해결

### CAC(Common Access Card) 인증 실패

CAC 사용자에게 대해 SSO 인증이 실패할 경우 UCCX ids.log를 확인하여 SAML Attributes(SAML 특

성)가 제대로 설정되었는지 확인합니다.

컨피그레이션 문제가 있는 경우 SAML 오류가 발생합니다. 예를 들어 이 로그 스니펫에서 user\_principal SAML 특성은 IdP에 구성되지 않습니다.

```
YYYY-MM-DD hh:mm:ss.sss GMT(-0000) [IdSEndPoints-SAML-59] 오류
com.cisco.ccbu.ids IdSSAMLAyncServlet.java:465 - 특성 맵에서 검색할 수 없습니다. 사용자_계정
YYYY-MM-DD hh:mm:ss.sss GMT(-0000) [IdSEndPoints-SAML-59] 오류
com.cisco.ccbu.ids IdSSAMLAyncServlet.java:298 - com.sun.identity.saml.common.SAMLException 예외로 인해
SAML 응답 처리가 실패했습니다. saml 응답에서 user_principal을 검색할 수 없습니다.
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributeFromAttributesMap(IdSSAMLAyncServlet.java:466)에
서
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet.java:263)에서
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet.java:176)에서
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)
```

## 관련 정보

- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.