

Installieren und Konfigurieren des F5 Identity Providers (IdP) für Cisco Identity Service (IDs) zur Aktivierung von SSO

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Installieren](#)

[Konfigurieren](#)

[Erstellung von Security Assertion Markup Language \(SAML\)](#)

[SAML-Ressourcen](#)

[Webtops](#)

[Virtueller Richtlinien-Editor](#)

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

[Überprüfen](#)

[Fehlerbehebung](#)

[CAC-Authentifizierungsfehler \(Common Access Card\)](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird die Konfiguration des BIG-IP Identity Providers (IDP) F5 zur Aktivierung der einmaligen Anmeldung (Single Sign On, SSO) beschrieben.

Cisco IDS-Bereitstellungsmodelle

Produkt Bereitstellung

UCCX Co-Resident

PCCE Co-Resident mit CUIC (Cisco Unified Intelligence Center) und LD (Live-Daten)

UCCE Resident gemeinsam mit CUIC und LD für 2.000 Bereitstellungen.

Standalone für 4.000- und 12.000-Bereitstellungen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Contact Center Express (UCCX) Version 11.6 oder Cisco Unified Contact Center Enterprise Release 11.6 oder Packaged Contact Center Enterprise (PCCE) Release 11.6.

Hinweis: Dieses Dokument bezieht sich auf die Konfiguration des Cisco Identity Service (IDs) und des Identitätsanbieters (IdP). Das Dokument verweist in den Screenshots und Beispielen auf UCCX, die Konfiguration ähnelt jedoch dem Cisco Identity Service (UCCX/UCCE/PCCE) und der IdP.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Installieren

Big-IP ist eine Paketlösung mit mehreren Funktionen. Zugriffsrichtlinien-Manager (APM), der sich auf den Identity Provider-Service bezieht.

Big-IP als APM:

Version 13,0

Typ Virtual Edition (OVA)

IPs Zwei IPs in verschiedenen Subnetzen. Eine für die Verwaltungs-IP und eine für den virtuellen IDP-Server

Laden Sie das virtuelle Edition-Image von der Big-IP-Website herunter, und stellen Sie die OVA bereit, um ein vorinstalliertes virtuelles System (VM) zu erstellen. Erwerben Sie die Lizenz, und installieren Sie sie mit den grundlegenden Anforderungen.

Hinweis: Informationen zur Installation finden Sie in der [Big-IP-Installationsanleitung](#).

Konfigurieren

- Navigieren Sie zu Ressourcenbereitstellung, aktivieren Sie **Zugriffsrichtlinien**, und legen Sie die Bereitstellung auf **Nominal fest**.

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

Reset Submit

- Erstellen eines neuen VLAN unter **Netzwerk** -> **VLANs**

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

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
System

- Erstellen Sie einen neuen Eintrag für die IP, der für die IDP unter **Netzwerk -> Self IPs** verwendet wird.

**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"/>

- Erstellen Sie ein Profil unter **Access -> Profile/Policies -> Access-Profile**.

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)														

- Erstellen eines virtuellen Servers

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 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>/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"/>	

- Hinzufügen von Active Directory (AD)-Details unter **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	<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

- Erstellen Sie einen neuen IDP-Service unter **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

Hinweis: Wenn eine Common Access Card (CAC) für die Authentifizierung verwendet wird, müssen diese Attribute im Konfigurationsabschnitt **SAML Attributes** hinzugefügt werden:

Schritt 1: Erstellen des **uid**-Attributs.

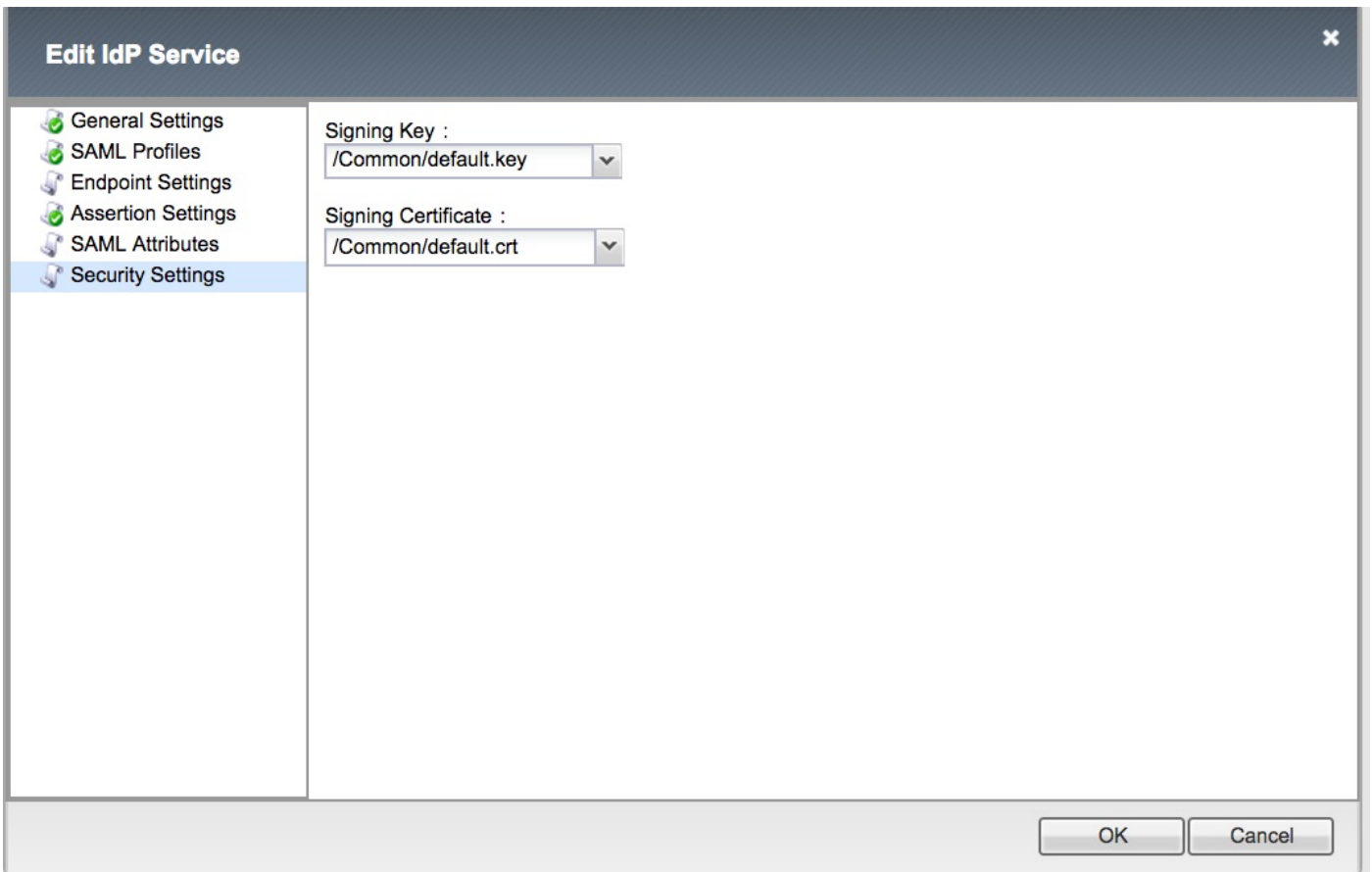
Name: uid

Wert: %{session.Idap.last.attr.sAMAccountName}

Schritt 2: Erstellen Sie das **user_main**-Attribut.

Name: Benutzer_Principal

Wert: %{session.Idap.last.attr.userPrincipalName}



Hinweis: Nach dem Erstellen des IDP-Service gibt es eine Option zum Herunterladen der Metadaten mit einer Schaltfläche **Metadaten exportieren** unter **Access -> Federation -> SAML Identity Provider -> Local IdP Services**.

Erstellung von Security Assertion Markup Language (SAML)

SAML-Ressourcen

- Navigieren Sie zu **Access -> Federation -> SAML Resources**, und erstellen Sie eine einfache Ressource für die Verknüpfung mit dem zuvor erstellten IDP-Dienst.



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

- Erstellen Sie einen Webtop unter 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

Virtueller Richtlinien-Editor

- Navigieren Sie zur zuvor erstellten Richtlinie, und klicken Sie auf den Link Bearbeiten.

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

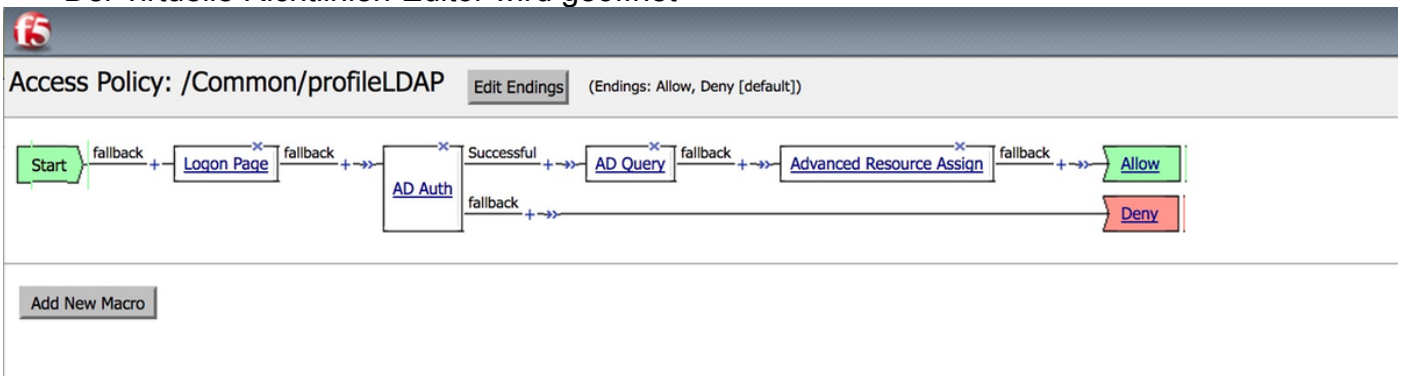
Access Profiles | Per-Request Policies | Policy Sync | Customization

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

- Der virtuelle Richtlinien-Editor wird geöffnet



- Klicken Sie auf Symbol und fügen Sie Elemente wie beschrieben hinzu.

Schritt 1: **Logon page element** (Seite anmelden): Behalten Sie die Standardeinstellung für alle Elemente bei.

Schritt 2: **AD Auth** -> Wählen Sie die zuvor erstellte ADFS-Konfiguration aus.

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 ↕

Schritt 3: AD Query-Element - Weisen Sie die erforderlichen Details zu.

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

Schritt 4: **Erweiterte Ressourcenzuweisung** - Verknüpfen Sie die gleiche Ressource mit dem zuvor erstellten Webtop.

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

- Importieren Sie das Zertifikat der IDS manuell in Big-IP über **System -> Zertifikatsverwaltung -> Datenverkehrsmanagement**.

Hinweis: Stellen Sie sicher, dass das Zertifikat aus den Tags BEGIN CERTIFICATE und END CERTIFICATE besteht.

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	

- Erstellen Sie einen neuen Eintrag aus sp.xml unter **Access -> Federation -> SAML Identity Provider -> External SP Connectors**.
- Binden Sie den SP-Anschluss unter **Access -> Federation -> SAML Identity Provider -> Local IdP Services an den IDP-Service**.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

CAC-Authentifizierungsfehler (Common Access Card)

Wenn die SSO-Authentifizierung für CAC-Benutzer fehlschlägt, überprüfen Sie das Feld UCCX ids.log, um zu überprüfen, ob die SAML-Attribute korrekt eingestellt wurden.

Bei einem Konfigurationsproblem tritt ein SAML-Fehler auf. In diesem Protokollausschnitt ist das user_Principal-SAML-Attribut z. B. auf dem IdP nicht konfiguriert.

```
JJJJ-MM-DD hh:mm:ss.sss GMT(-0000) [IdSEndPoints-SAML-59] ERROR
com.cisco.ccbu.ids IdSSAMLAyncServlet.java:465 - Kann nicht aus der Attributzuordnung abgerufen werden: Benutzer_Principal
JJJJ-MM-DD hh:mm:ss.sss GMT(-0000) [IdSEndPoints-SAML-59] ERROR
com.cisco.ccbu.ids IdSSAMLAyncServlet.java:298 - SAML-Antwortverarbeitung fehlgeschlagen mit exception com.sun.identity.saml.common.SAMLException: user_Principal konnte nicht aus der Antwort "SAL" abgerufen werden.
unter
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributeFromAttributesMap(IdSSAMLAyncServlet.java:466)
unter
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet.java:263)
)
unter
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet.java:176)
unter 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)
```

Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)