

Installare e configurare il provider di identità F5 (IdP) per Cisco Identity Service (IdS) per abilitare l'SSO

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Install](#)

[Configurazione](#)

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

[Risorse SAML](#)

[Webtop](#)

[Editor criteri virtuali](#)

[Scambio metadati Service Provider \(SP\)](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Errore di autenticazione CAC \(Common Access Card\)](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive la configurazione su F5 BIG-IP Identity Provider (IdP) per abilitare Single Sign-On (SSO).

Modelli di distribuzione Cisco IdS

Prodotto Implementazione

UCCX Coresidente

PCCE Coresidente con CUIC (Cisco Unified Intelligence Center) e LD (Live Data)

UCCE Coresidenti con CUIC e LD per installazioni 2k.

UCCE Standalone per installazioni a 4k e 12k.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Contact Center Express (UCCX) versione 11.6 o Cisco Unified Contact Center Enterprise versione 11.6 o Packaged Contact Center Enterprise (PCCE) versione 11.6, a seconda dei casi.

Nota: Questo documento fa riferimento alla configurazione di Cisco Identify Service (IdS) e del provider di identità (IdP). Il documento fa riferimento a UCCX negli screenshot ed esempi, tuttavia la configurazione è simile a quella di Cisco Identify Service (UCCX/UCCE/PCCE) e dell'IdP.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Install

Big-IP è una soluzione a pacchetti che ha diverse funzioni. Access Policy Manager (APM) che si riferisce al servizio Identity Provider.

Big-IP come APM:

Version 13.0

Tipo Virtual Edition (OVA)

IP Due IP in subnet diverse. Uno per l'IP di gestione e uno per il server virtuale IdP

Scaricare l'immagine dell'edizione virtuale dal sito Web Big-IP e distribuire l'OAV per creare una macchina virtuale preinstallata. Ottenere la licenza e installarla con i requisiti di base.

Nota: Per informazioni sull'installazione, consultare la [Guida all'installazione di Big-IP](#).

Configurazione

- Passare al provisioning delle risorse e abilitare i **criteri di accesso**, impostare il provisioning su **Nominale**

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

- Creare una nuova VLAN in Rete -> 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

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

- Creare una nuova voce per l'indirizzo IP utilizzato per l'IdP in Rete -> Indirizzi IP autonomi

**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"/>

- Creare un profilo in **Accesso** -> **Profilo/Criteri** -> **Profili di accesso**

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"><tr><td>Accepted Languages</td><td>Factory BuiltIn Languages</td></tr><tr><td>English (en)</td><td>Japanese (ja) Chinese (Simplified) (zh-cn) Chinese (Traditional) (zh-tw) Korean (ko) Spanish (es) French (fr)</td></tr></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)				

- Creare un server virtuale

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"/>	

- Aggiungere i dettagli di Active Directory (AD) in **Accesso** -> **Autenticazione** -> **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 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

- Crea un nuovo servizio IdP in **Accesso** -> **Federazione** -> **Provider di identità SAML** -> **Servizi IdP locali**

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

Nota: Se per l'autenticazione viene utilizzata una scheda CAC (Common Access Card), è necessario aggiungere questi attributi nella sezione di configurazione **Attributi SAML**:

Passaggio 1. Creare l'attributo **uid**.

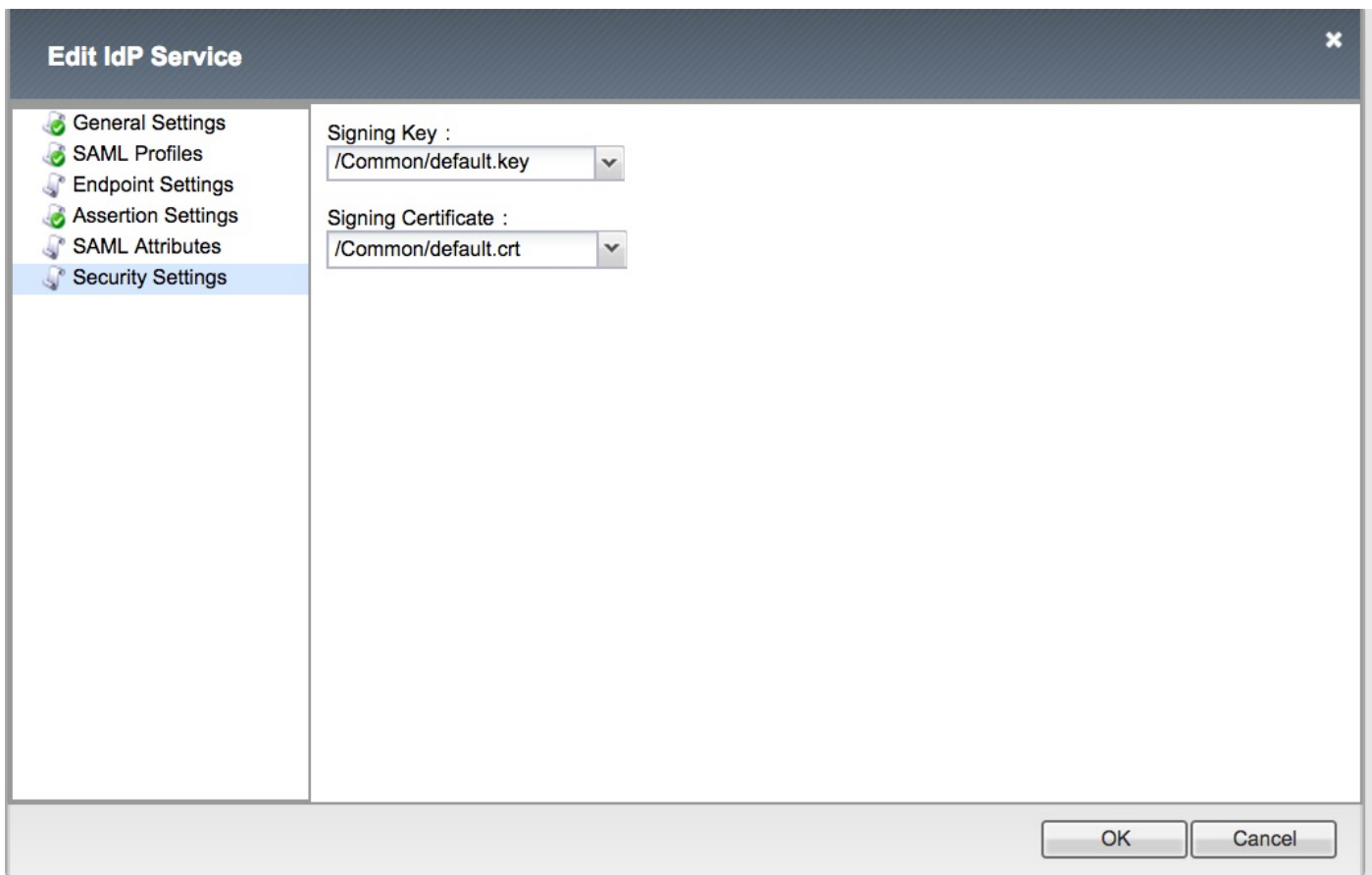
Nome: uid

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

Passaggio 2. Creare l'attributo **user_principal**.

Nome: user_principal

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



Nota: Una volta creato il servizio IdP, è possibile scaricare i metadati con un pulsante **Esporta metadati in Accesso -> Federazione -> Provider di identità SAML -> Servizi IdP locali**

Creazione SAML (Security Assertion Markup Language)

Risorse SAML

- Passare a **Accesso -> Federazione -> Risorse SAML** e creare una risorsa SAML da associare al servizio IdP creato in precedenza



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

Webtop

- Create un WebTop in Access -> Webtop



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 criteri virtuali

- Passare al criterio creato in precedenza e fare clic sul collegamento Modifica

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

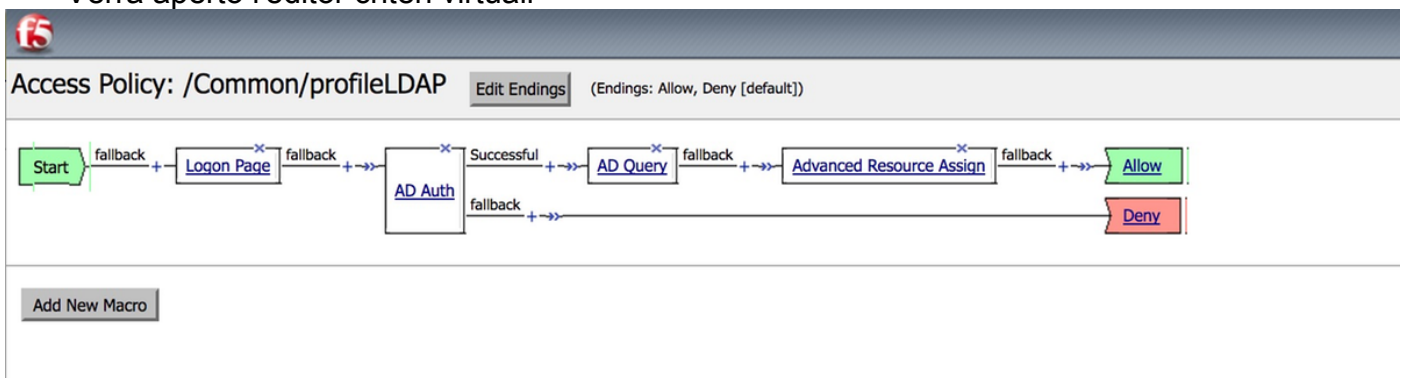
Access Profiles | Per-Request Policies | Policy Sync | Customization

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

- Verrà aperto l'editor criteri virtuali



- Fare clic su e aggiungere gli elementi come descritto

Passaggio 1. **Elemento della pagina di accesso** - Lasciare tutti gli elementi ai valori predefiniti.

Passaggio 2. **Autenticazione AD** -> Scegliere la configurazione ADFS creata in precedenza.

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 ↕

Passaggio 3. Elemento query AD - Assegnare i dettagli necessari.

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

Passaggio 4. Assegnazione anticipata risorse: associare la risorsa saml e il WebTop creato in precedenza.

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](#)

Scambio metadati Service Provider (SP)

- Importa manualmente il certificato degli IdS in Big-IP tramite **System -> Gestione certificati -> Gestione traffico**

Nota: Verificare che il certificato sia costituito da tag BEGIN CERTIFICATE e END CERTIFICATE.

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

- Creare una nuova voce da sp.xml in **Access -> Federation -> SAML Identity Provider -> External SP Connectors**
- Associare il connettore SP al servizio IdP in **Accesso -> Federazione -> Provider di identità SAML -> Servizi IdP locali**

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Errore di autenticazione CAC (Common Access Card)

Se l'autenticazione SSO non riesce per gli utenti CAC, controllare il file UCCX ids.log per verificare che gli attributi SAML siano stati impostati correttamente.

Se si verifica un problema di configurazione, si verifica un errore SAML. Ad esempio, in questo frammento di log, l'attributo SAML user_principal non è configurato in IdP.

```
AAAA-MM-GG hh:mm:ss.sss GMT(-0000) [IdSEndPoints-SAML-59] ERRORE
com.cisco.ccbu.ids IdSSAMLAyncServlet.java:465 - Impossibile recuperare dalla mappa attributi:
user_principal
AAAA-MM-GG hh:mm:ss.sss GMT(-0000) [IdSEndPoints-SAML-59] ERRORE
com.cisco.ccbu.ids IdSSAMLAyncServlet.java:298 - Elaborazione della risposta SAML non riuscita con
eccezione com.sun.identity.saml.common.SAMLException: Impossibile recuperare user_principal dalla
risposta saml
all'indirizzo
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributeFromAttributesMap(IdSSAMLAyncServlet.java:4
66)
all'indirizzo
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet.java:263
)
all'indirizzo
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet.java:17
6)
all'indirizzo com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)
all'indirizzo java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
in java.lang.Thread.run(Thread.java:745)
```

Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems](#)