

Instale e configurar o fornecedor da identidade F5 (IdP) para o serviço da identidade de Cisco (IdS) para permitir o SSO

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Instalação](#)

[Configurar](#)

[Criação do linguagem de marcação da afirmação da Segurança \(SAML\)](#)

[Recursos de SAML](#)

[Webtops](#)

[Editor de política virtual](#)

[Troca dos Metadata do provedor de serviços \(SP\)](#)

[Verificar](#)

[Troubleshooting](#)

[Falha de autenticação comum do cartão do acesso \(CAC\)](#)

[Informações Relacionadas](#)

Introdução

Este original descreve a configuração no fornecedor da identidade F5 BIG-IP (IdP) para permitir sobre o único sinal (SSO).

Modelos de distribuição do Cisco IDS

Produto Desenvolvimento

UCCX Co-residente

PCCE Co-residente com CUIIC (centro unificado Cisco da inteligência) e LD (dados vivos)

UCCE Co-residente com CUIIC e LD para as disposições 2k.

Autônomo para as disposições 4k e 12k.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Liberação 11.6 do Cisco Unified Contact Center Express (UCCX) ou liberação 11.6 do Cisco Unified Contact Center Enterprise ou liberação empacotada 11.6 da empresa do centro de contato (PCCE) como aplicáveis.

Note: Este original provê a configuração no que diz respeito ao serviço de Cisco Identity (IdS) e ao fornecedor da identidade (IdP). O original provê UCCX nos screenshots e nos exemplos, porém a configuração é similar no que diz respeito ao serviço de Cisco Identity (UCCX/UCCE/PCCE) e ao IdP.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Instalação

O Grande-IP é uma solução empacotada que tenha características múltiplas. Gerente da política de acesso (APM) que co-se relaciona ao serviço do fornecedor da identidade.

Grande-IP como o APM:

Versão 13.0

Tipo Edition(OVA) virtual

IPs Dois IPs em sub-redes diferentes. Um para o IP de gerenciamento e um para o servidor virtual de IdP

Transfira a imagem virtual da edição do Web site Grande-IP e distribua os ÓVULOS para criar uma máquina virtual (VM) que seja instalada. Obtenha a licença e instale-a com as requisições básico.

Note: Para a informação de instalação, refira o [Guia de Instalação Grande-IP](#).

Configurar

- Navegue ao abastecimento do recurso e permita a **política de acesso**, ajuste o abastecimento ao **substantivo**

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

- Crie um VLAN novo sob a rede - > VLAN

ONLINE (ACTIVE)
Standalone

Main Help About

Network » VLANs : VLAN List » external

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

Properties Layer 2 Static Forwarding Table

General Properties

Name	external
Partition / Path	Common
Description	
Tag	4093

Resources

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

- Crie uma entrada nova para o IP que é usado para o IdP sob a rede -> o auto 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"/>

- Crie um perfil sob o acesso - > perfil/políticas - > perfis do acesso

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	Accepted Languages
	English (en)
	Factory BuiltIn Languages
	Japanese (ja)
	Chinese (Simplified) (zh-cn)
	Chinese (Traditional) (zh-tw)
	Korean (ko)
	Spanish (es)
	French (fr)

- Crie um 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"/>
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 #ccc; 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 #ccc; padding: 5px; width: 45%;"> <p style="text-align: center; margin: 0;">Available</p> <p>/Common 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 #ccc; 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 #ccc; 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"/>	

- Adicionar detalhes do diretório ativo (AD) sob o acesso -> autenticação -> diretório ativo



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

- Crie um serviço novo de IdP sob o **acesso - > federação - > fornecedor da identidade de SAML - > serviços locais 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: Se um cartão comum do acesso (CAC) é usado para a autenticação, estes atributos precisam de ser adicionados na seção de configuração dos **atributos de SAML**:

Etapa 1. Crie o atributo do **uid**.

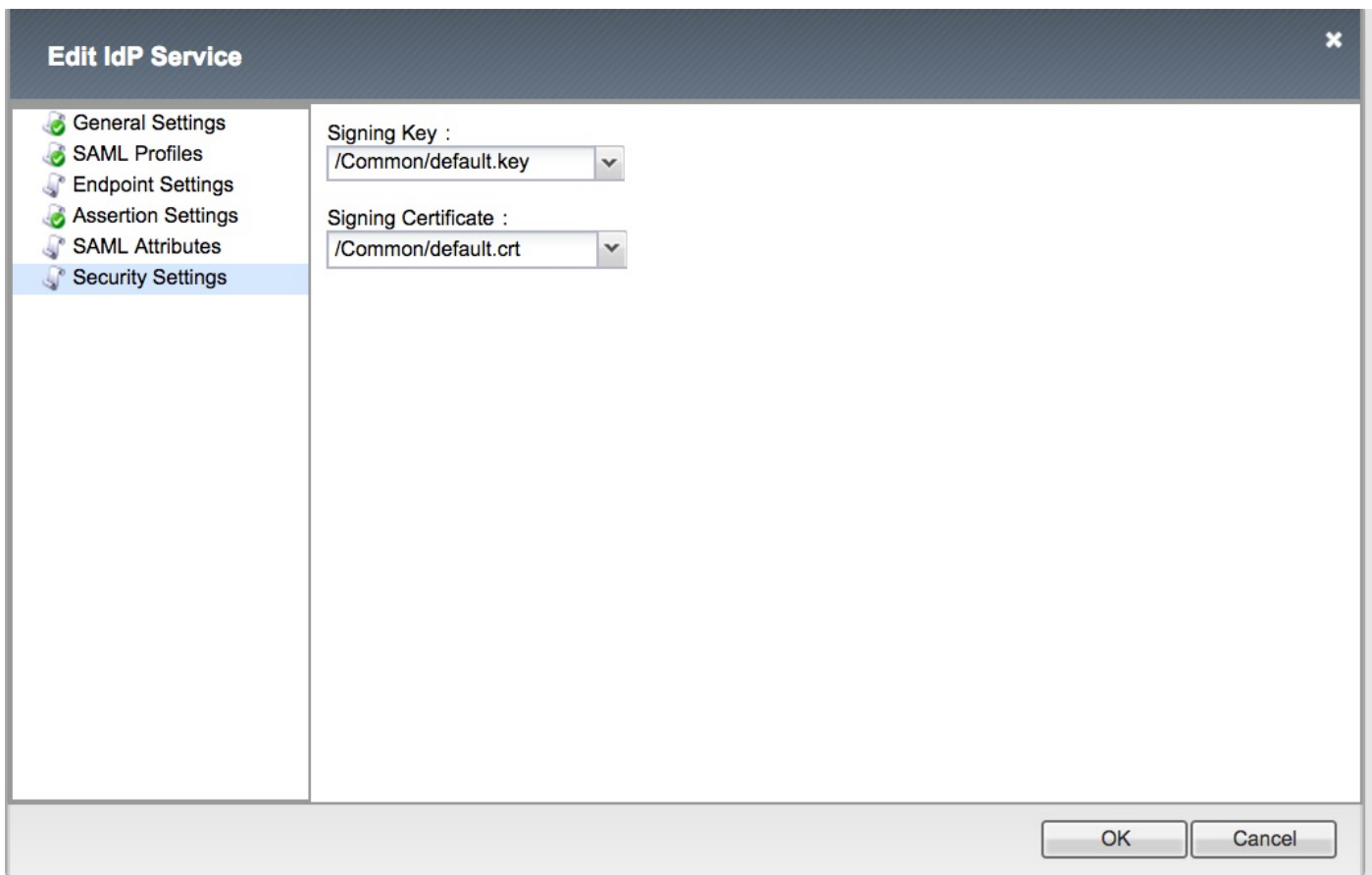
Nome: uid

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

Etapa 2. Crie o atributo **user_principal**.

Nome: user_principal

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



Note: Uma vez que o serviço de IdP é criado, há uma opção para transferir os metadata com **Metadata de uma exportação** do botão sob o **acesso - > federação - > fornecedor da identidade de SAML - > serviços locais de IdP**

Criação do linguagem de marcação da afirmação da Segurança (SAML)

Recursos de SAML

- Navegue para **alcançar - > federação - > recursos de SAML** e para criar um recurso do saml para associar com o serviço de IdP que foi criado mais cedo



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

- Crie um webtop sob o acesso - > 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 política virtual

- Navegue à política criada mais cedo e clique editam sobre o link

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

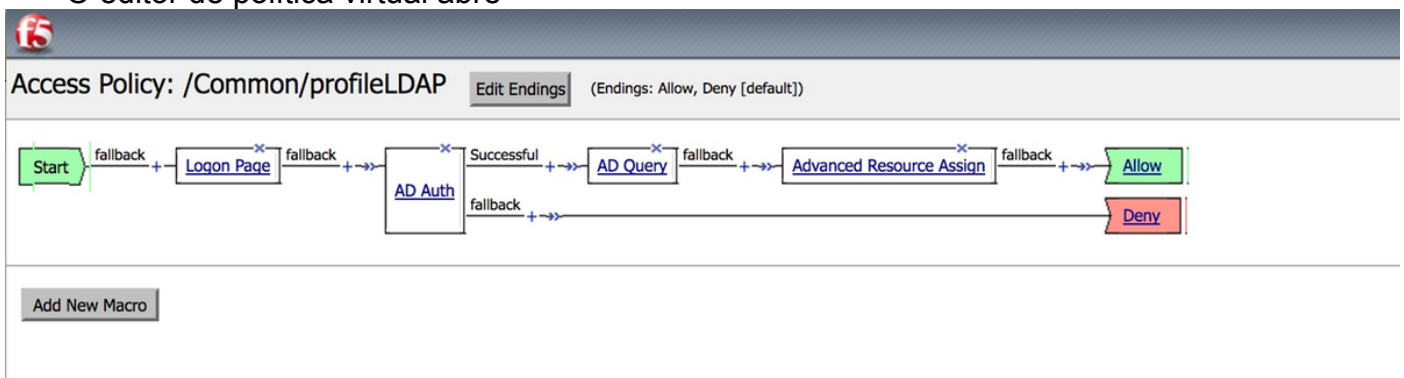
Access Profiles | Per-Request Policies | Policy Sync | Customization

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

- O editor de política virtual abre



- Clique sobre o ícone e adicionar elementos como descritos

Etapa 1. Elemento da página do fazer logon - Deixe todos os elementos para optar.

Etapa 2. AUTH AD - > escolha a configuração ADFS criada mais cedo.

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 ↕

Etapa 3. Elemento da pergunta AD - Atribua os detalhes necessários.

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

Etapa 4. O recurso avançado atribui - Associe o recurso do saml e o webtop criados mais cedo.

The screenshot shows a web interface with two tabs: 'Properties' and 'Branch Rules'. The 'Branch Rules' tab is active. Below the tabs, there is a text input field labeled 'Name:' containing the text 'Advanced Resource Assign'. Below this is a section titled 'Resource Assignment'. Inside this section, there is a light blue bar with the text 'Add new entry' on the left and 'Ins' on the right. Below the bar, there is a section titled 'Expression: Empty' with a 'change' link. Below this, there is a list of items: 'SAML: /Common/ids_pipeline, /Common/smart-86-samlresource', 'Webtop: /Common/Smart-86-Webtop', and 'Add/Delete'.

Troca dos Metadata do provedor de serviços (SP)

- Importe manualmente o certificado dos IdS ao Grande-IP através do **sistema** - > gerenciamento de certificado - > **gerência do tráfego**

Note: Assegure-se de que o certificado consista COMECE O CERTIFICADO e TERMINE-SE etiquetas do CERTIFICADO.

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

- Crie uma entrada nova de sp.xml sob o **fornecedor de Access-> Federation-> SAMLIDENTITY - > conectores de ExternalSP**
- Ligue o conector SP ao serviço de IdP sob o **acesso - > federação - > fornecedor da identidade de SAML - > serviços locais de IdP**

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Falha de autenticação comum do cartão do acesso (CAC)

Se a autenticação SSO falha para usuários CAC, verifique o UCCX ids.log para verificar que os atributos de SAML estiveram ajustados corretamente.

Se há um problema de configuração, uma falha de SAML ocorre. Por exemplo, neste snippet do log, o atributo user_principal de SAML não é configurado no IdP.

```
YYYY-MM-DD HH: milímetro: ERRO com.cisco.ccbu.ids.IdSSAMLAyncServlet.java:465 SS.sss GMT(-0000)
[IdSEndPoints-SAML-59] - Não poderia o mapa dos atributos do retrievefrom: user_principal
YYYY-MM-DD HH: milímetro: ERRO com.cisco.ccbu.ids.IdSSAMLAyncServlet.java:298 SS.sss GMT(-0000)
[IdSEndPoints-SAML-59] - SAML responseprocessingfailed com exceção
com.sun.identity.saml.common.SAMLException: Não podia recuperar user_principal da resposta do
saml
em
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributeFromAttributesMap(IdSSAMLAyncServlet.java:4
66)
em
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet.java:263
)
em
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet.java:17
6)
em com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)
em java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
em java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
em java.lang.Thread.run(Thread.java:745)
```

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)