

# 安装并且配置F5身份供应商(IdP) Cisco身份服务的(ID)对enable (event) SSO

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[安装](#)

[Configure](#)

[安全主张标记语言\(SAML\)创建](#)

[SAML资源](#)

[Webtops](#)

[虚拟策略编辑器](#)

[服务提供商\(SP\)元数据Exchange](#)

[Verify](#)

[Troubleshoot](#)

[普通的访问卡\(CAC\)认证失败](#)

[Related Information](#)

## Introduction

本文描述在F5 BIG-IP身份供应商(IdP)的配置对enable (event)单个符号(SSO)。

### Cisco IDS部署模型

#### 产品 配置

UCCX coresident

PCCE 与CUIC (Cisco Unified智力中心)和LD (实际数据)的共同驻留

与CUIC和LD的共同驻留2k配置的。

UCCE 独立为4k和12k配置。

## Prerequisites

## Requirements

Cisco 建议您了解以下主题：

- Cisco Unified Contact Center Express (UCCX)版本11.6或Cisco Unified Contact Center Enterprise Release 11.6或者被包的联系中心企业(PCCE)版本11.6如可适用。

**Note:**本文参考配置关于Cisco Identity服务(ID)和身份供应商(IdP)。本文参考UCCX屏幕画面和示例，然而配置是类似的关于Cisco Identity服务(UCCX/UCCE/PCCE)和IdP。

## Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. 如果您的网络实际，请保证您了解所有命令的潜在影响。

## 安装

大IP是有多个功能的一个包的解决方案。与身份供应商服务CO涉及的访问策略管理器(APM)。

大IP作为APM：

version 13.0

类型 虚拟Edition(OVA)

IP 两IP用不同的子网。一管理IP的  
并且一IdP虚拟服务器的

从大IP事先装配的网站下载虚拟版本镜像并且配置卵创建虚拟机。获得许可证并且安装与基本需求。

Note:安装信息，请参见大[IP安装指南](#)。


## Configure

- 连接对资源提供，并且enable (event)访问策略，设置设置为名义上

The screenshot displays the FortiGate configuration page for Resource Provisioning. The left sidebar shows the navigation menu with 'System' selected. The main content area shows the 'Current Resource Allocation' section with three progress bars: CPU (MGMT, TMM, 88%), Disk (97GB, MGMT), and Memory (3.8GB, MGMT, TMM, APM). Below this is a table of modules with their provisioning status, license status, and resource requirements.

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

- 创建新的VLAN在Network-> VLAN下


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

- 创建使用在Network->自己IP下的IdP的IP的一个新的条目

**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

- 创建一个配置文件在访问下->配置文件/策略->Access配置文件

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)														

- 创建一个虚拟服务器

**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 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 splitssession-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"/>	

- 添加激活目录(AD)详细资料在访问下->认证->激活目录



## 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



- 创建一项新的IdP服务在访问下->联邦->SAML身份供应商->本地IdP服务

### 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:** 如果一个普通的访问卡(CAC)使用认证，这些属性需要被添加在SAML归因于配置部分：

步骤1. 创建uid属性。

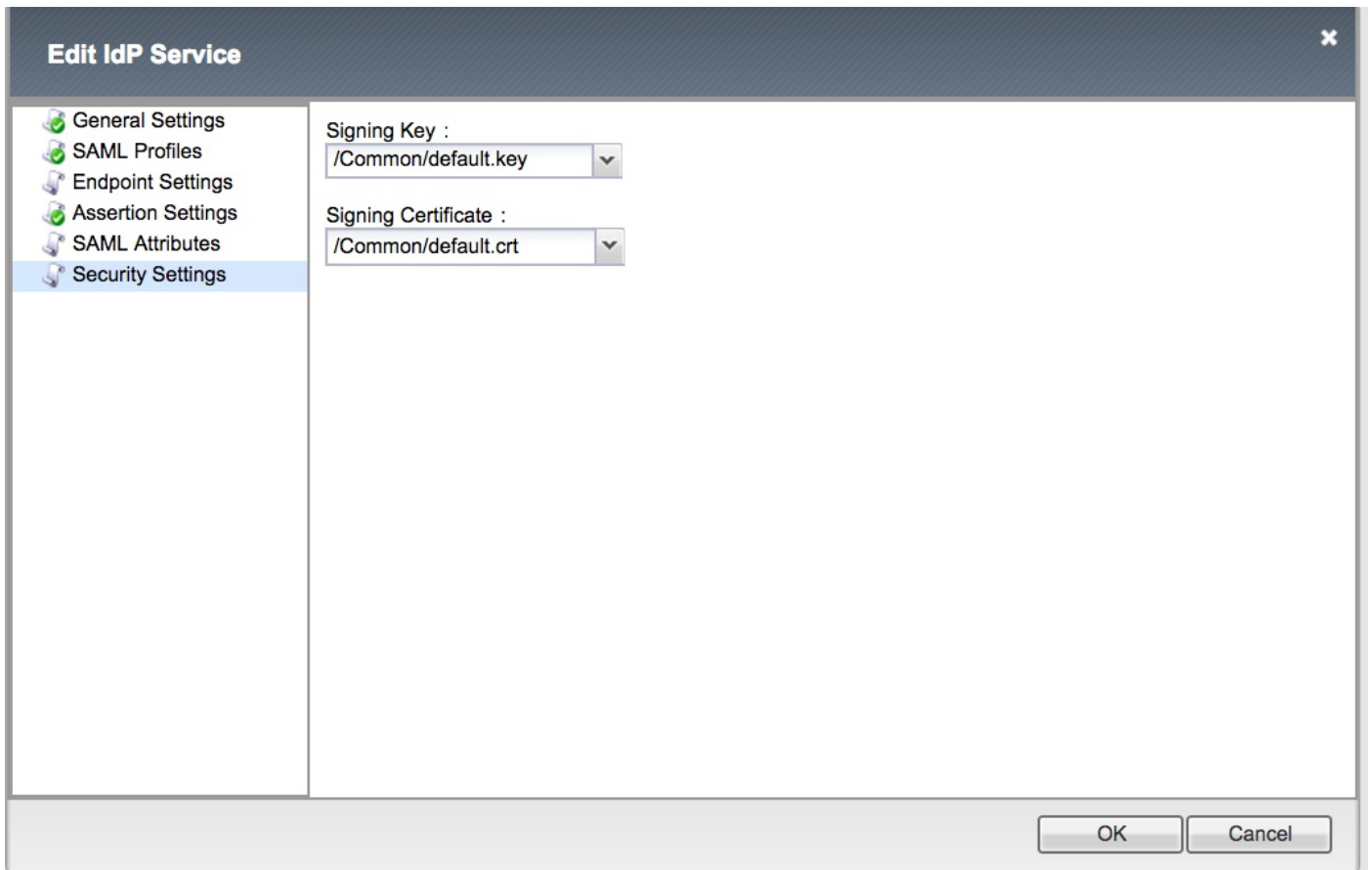
名字：uid

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

步骤2. 创建user\_principal属性。

名字：user\_principal

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



**Note:**一旦IdP服务被创建，有下载与Export按钮元数据的元数据的选项在访问下- >联邦- > SAML身份供应商- >本地IdP服务

## 安全主张标记语言(SAML)创建

### SAML资源

- 连接访问- >联邦- > SAML资源和创建saml资源与被创建前的IdP服务产生关联



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

- 创建一webtop在访问下- > 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

**虚拟策略编辑器**

- 连接对及早被创建的策略并且点击编辑链路

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

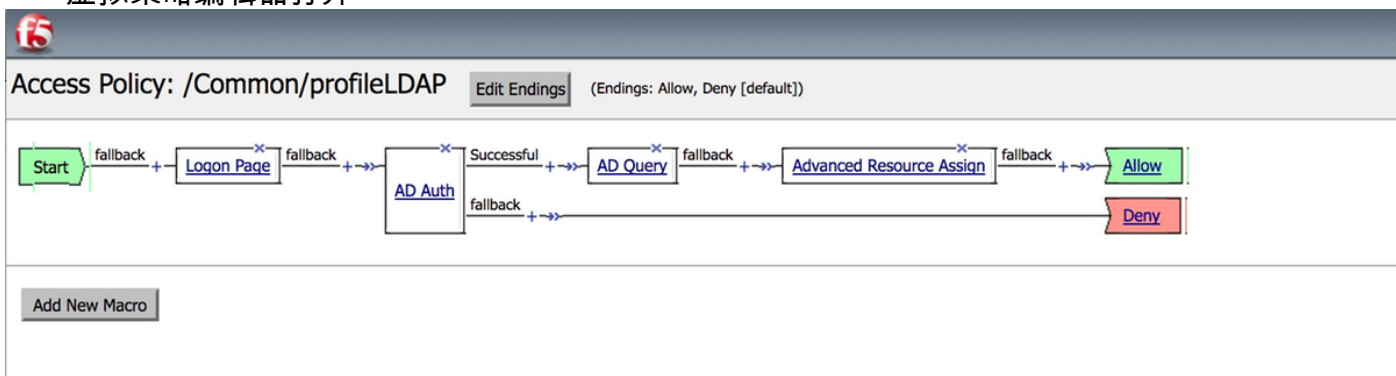
Access Profiles | Per-Request Policies | Policy Sync | Customization

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

• 虚拟策略编辑器打开



• 点击 图标并且添加元素如所描述

步骤1. 登录页元素-留下所有元素默认。

步骤2. AD Auth ->请选择被创建的ADFS配置前。

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 ↕

步骤3. AD查询元素-分配必要的详细资料。



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

步骤4. 预先的资源分配-关联被创建的saml资源和webtop前。

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](#)

## 服务提供商(SP)元数据Exchange

- 请手工导入ID的认证大IP通过系统 -> Certificate Management -> Traffic Management

**Note:**保证认证包括开始认证和END认证标记。

## 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

- 创建从sp.xml的一个新的条目在Access-> Federation-> SAMLIDENTITY供应商下-> ExternalSP连接器
- 捆绑SP连接器对IdP服务在访问下->联邦-> SAML身份供应商->本地IdP服务

## Verify

当前没有可用于此配置的验证过程。

## Troubleshoot

### 普通的访问卡(CAC)认证失败

如果SSO认证为CAC用户失效，请检查UCCX ids.log验证适当地设置SAML属性。

如果有配置问题，SAML故障发生。例如，在此日志片断，user\_principal SAML属性在IdP没有被

配置。

```
YYYY-MM-DD hh mm:SS.sss GMT(-0000) [IdSEndPoints-SAML-59]com.cisco.ccbu.ids  
IdSSAMLAyncServlet.java:465 -retrievefromuser_principal  
YYYY-MM-DD hh mm:SS.sss GMT(-0000) [IdSEndPoints-SAML-59]com.cisco.ccbu.ids  
IdSSAMLAyncServlet.java:298 - SAML responseprocessingfailed  
com.sun.identity.saml.common.SAMLException samluser_principal
```

```
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributeFromAttributesMap(IdSSAMLAyncServlet.java:4  
66)
```

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

```
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet.java:17  
6)
```

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

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

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

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

## Related Information

- [Technical Support & Documentation - Cisco Systems](#)