

Installeer en Configureer de F5 Identity Provider (IDP) voor Cisco Identity Services (IDS) om SDOs in te schakelen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Installeren](#)

[Configureren](#)

[Creatie van SAML-technologieën \(Security Association Markup Language\)](#)

[SAML-bronnen](#)

[Webplaten](#)

[Virtuele beleidseditor](#)

[metagegevens over serviceproviders \(SP\)](#)

[Verifiëren](#)

[Problemen oplossen](#)

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

[Gerelateerde informatie](#)

Inleiding

In dit document wordt de configuratie op de F5 BIG-IP Identity Provider (IDP) beschreven om Single Sign On (SSO) in te schakelen.

Cisco IDs-implementatiemodule

Product Plaatsing

UCCX Medeingezetene

PCCE Gelijktijdige inwoner met CUIC (Cisco Unified Intelligence Center) en LD (Live Data)

UCCES Gelijktijdige inwoner met CUIC en LD voor 2k implementaties.

Standalone voor 4k- en 12k-implementaties.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Contact Center Express (UCCX) release 11.6 of Cisco Unified Contact Center Enterprise release 11.6 of Packaged Contact Center Enterprise (PCCE) release 11.6 indien van toepassing.

Opmerking: Dit document verwijst naar de configuratie met betrekking tot de Cisco Identifier Service (IDS) en de Identity Provider (IDP). Het document verwijst naar UCCX in de screenshots en voorbeelden, maar de configuratie is vergelijkbaar met betrekking tot Cisco Identifier Service (UCCX/UCCE/PCCE) en de IDP.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Installeren

Big-IP is een verpakte oplossing die meerdere eigenschappen heeft. Access Policy Manager (APM) die verband houdt met de dienst Identity Provider.

Big IP als APM:

Versie 13.0

Type Virtual Edition (OVA)

IP's Twee IP's in verschillende subnetten. Eén voor IP-beheer en één voor de virtuele IDP-server

Download de virtuele editieafbeelding van de Big-IP website en gebruik de OVA om een virtuele machine (VM) te maken die vooraf is geïnstalleerd. Verkrijg de licentie en installeer het apparaat met de basisvereisten.

Opmerking: Raadpleeg de [installatiehandleiding](#) van [Big IP voor](#) installatie-informatie.

Configureren

- Navigeer naar resource provisioning en stel **toegangsbeleid in**, stel voorziening in op **Nominaal**

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

- Een nieuw VLAN maken onder **Network** -> VLAN's

 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

- Maakt een nieuw item voor het IP dat voor de IDP onder **Netwerk** -> **Zelf-IP's** wordt gebruikt

**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"/>

- Een profiel maken onder Toegang -> Profile/Policy -> Access-profielen

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)				

- Een virtuele server maken

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;"> Selected / Common clientssl </div> <div style="text-align: center;"> << >> </div> <div style="border: 1px solid gray; padding: 5px;"> Available / Common clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl splitssession-default-clientssl </div> </div>
SSL Profile (Server)	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; padding: 5px;"> Selected / Common serverssl </div> <div style="text-align: center;"> << >> </div> <div style="border: 1px solid gray; padding: 5px;"> Available / Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl-insecure-compatible </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"/>	

- Actieve map toevoegen (AD)-gegevens onder Toegang -> Verificatie -> Actieve map



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

- Een nieuwe IDP-service maken onder **toegang-> Federatie -> 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

Opmerking: Als een Common Access Card (CAC) wordt gebruikt voor echtheidscontrole, moeten deze eigenschappen worden toegevoegd aan het configuratiescherm van **SAML Eigenschappen**:

Stap 1. Maak de **uid**-eigenschap.

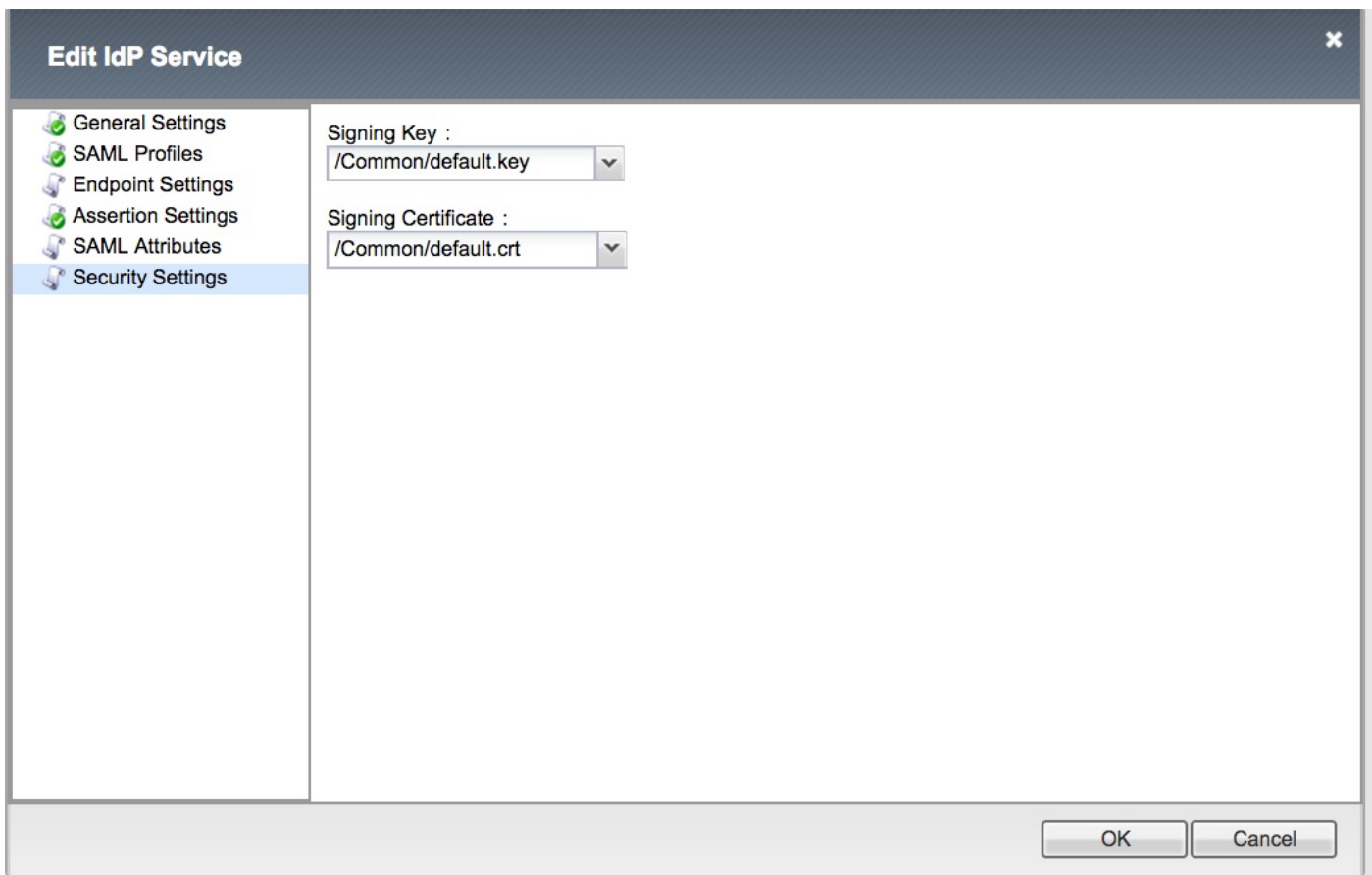
Name: uid

Value: % {sessie.ldap.last.attr.sAMAccountName}

Stap 2. Maak de eigenschap **user_main**.

Name: user_main

Value: % {sessie.ldap.last.attr.userPrincipalName}



Opmerking: Nadat de IDP-service is gecreëerd, kan de metagegevens via een knop **Exporteren** worden gedownload onder **Toegang -> Federatie -> SAML Identity Provider -> Local IDP Services**

Creatie van SAML-technologieën (Security Association Markup Language)

SAML-bronnen

- Navigeren in op **toegang -> Federatie -> SAML-bronnen** en een eenvoudige bron maken om de IDP-service te associëren die eerder is gemaakt



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

Webplaten

- Een webtop maken onder Toegang -> 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

Virtuele beleidseditor

- Navigeren naar het eerder gemaakte beleid en klik op de link bewerken

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

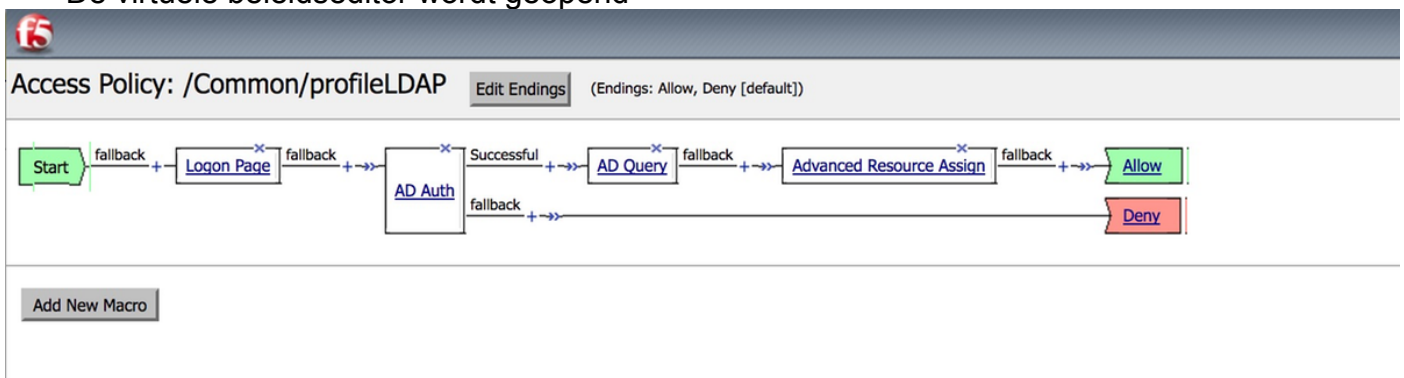
Access Profiles | Per-Request Policies | Policy Sync | Customization

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

- De virtuele beleidseditor wordt geopend



- Klik op de pictogram en voeg elementen toe zoals beschreven
- Stap 1. **Logon-pagina-element** - Laat alle elementen standaard.
- Stap 2. **AD Auth** -> Kies de eerder gemaakte ADFS-configuratie.

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 ↕

Stap 3. AD Query-element - De benodigde gegevens toewijzen.

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

Stap 4. Toewijzing van geavanceerde middelen - associeer de primaire bron en de webtop die eerder is gemaakt.

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](#)

metagegevens over serviceproviders (SP)

- Voer het certificaat van de IDs handmatig in op Big IP via **System** -> **certificaatbeheer** -> **verkeersbeheer**

Opmerking: Zorg ervoor dat het certificaat bestaat uit BEGIN-CERTIFICAAT- en EINDCERTIFICAATtags.

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

- Een nieuw item maken vanuit sp.xml onder **Access** -> **Federatie** -> **SAML Identity Provider** -> **Externe SP connectors**
- Bind de SP-connector naar de IDP-service onder **Toegang** -> **Federatie** -> **SAML Identity Provider** -> **Lokale ID-services**

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

CAC-verificatie (Common Access Card)

Als de verificatie van SSO's voor CAC-gebruikers niet lukt, controleer dan de UCCX id.log om te controleren of de SAML-kenmerken correct zijn ingesteld.

Als er een configuratie probleem is, treedt een SAML-storing op. Bijvoorbeeld, in dit logfragment, wordt de user_main SAML eigenschap niet gevormd op IDP.

```
YYYY-MM-DD hh:mm:ss.sss GMT(-0000) [IDSEndPoint-SAML-59] FOUT
com.cisco.cbu.ids IDSSAMLAsyncServlet.java:465 - Kan geen attributenkaart ophalen: user_main
YYYY-MM-DD hh:mm:ss.sss GMT(-0000) [IDSEndPoint-SAML-59] FOUT
com.cisco.cbu.ids IDSSAMLAsyncServlet.java:298 - SAML-responsverwerking faalde met uitzondering van
com.sun.Identity.saml.common.SAMLException: Kan user_main niet ophalen van saml respons
op com.cisco.cbu.ids.auth.api.idSSAMLAsyncServlet.getAttributesFromAttributesMap
(IDSSAMLAsyncServlet.java:466)
op com.cisco.cbu.ids.auth.api.idSSAMLAsyncServlet.processSamlPostResponse
(IDSSAMLAsyncServlet.java:263)
op
com.cisco.cbu.ids.auth.api.idSSAMLAsyncServlet.procedureIDSEndPointrequest(IDSSAMLAsyncServlet.java:1
76)
op com.cisco.cbu.ids.auth.api.idSEndPoint$1.run (IDSEndPoint.java:269)
op java.util.tegelijkertijd.ThreadPoolExecteur.runWorker(ThreadPoolExec.java:1145)
op java.util.tegelijkertijd.ThreadPoolExec$Worker.run(ThreadPoolExec.java:615)
in java.lang.Thread.run(Thread.java:745)
```

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)