

# De OpenAM Identity Provider (IdP) voor Cisco Identity Service (IdS) installeren en configureren om SSO in te schakelen

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Installeren](#)

[Systeemvereisten](#)

[Besturingssystemen](#)

[Java-omgeving](#)

[Vereisten voor webtoepassingscontainer](#)

[Ondersteunde browsers](#)

[Vereisten voor gegevensopslag](#)

[Minimale hardwarevereisten](#)

[Installeren](#)

[OpenAM-software verkrijgen](#)

[voorwaarden](#)

[OpenAM-webtoepassing installeren](#)

[OpenAM-service uitvoeren](#)

[Configureren](#)

[OpenAM Configurator](#)

[OpenAM configureren als IdP](#)

[Configuratie Circle of Trust](#)

[Hosted Identity Provider maken](#)

[Ondertekeningssleutel configureren](#)

[entiteit van importserviceprovider](#)

[Aanvraag-/antwoordondertekening](#)

[attribuuttoewijzing](#)

[Circle of Trust bewerken](#)

[OpenAM IdP-metagegevens downloaden](#)

[Verdere configuratie voor SSO:](#)

---

## Inleiding

Dit document beschrijft de configuratie op de OpenAM Identity Provider (IdP) om Single Sign On (SSO) in te schakelen.

Cisco IDs-implementatiemodellen

Product	Implementatie
UCCX	medebewoner
PCCE	Medebewoner van CUIC (Cisco Unified Intelligence Center) en LD (Live Data)
UCCE	Co-resident 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) versie 11.6 of Cisco Unified Contact Center Enterprise versie 11.6 of Packaged Contact Center Enterprise (PCCE) versie 11.6, indien van toepassing.

---

Opmerking: Dit document verwijst naar de configuratie met betrekking tot de Cisco Identity 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 de Cisco Identity 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 live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Installeren

---

Opmerking: Dit document verwijst naar OpenAM versie 10.0.1 als onderdeel van de kwalificatie met SSO

---

### Systeemvereisten

Besturingssystemen	Java-omgeving	Vereisten voor	Ondersteunde	Ve
--------------------	---------------	----------------	--------------	----

		webtoepassingscontainer	browsers	ge
<ul style="list-style-type: none"> <li>• Microsoft Windows Server 2003, 2008 R2</li> <li>• Linux 2.6, 3.0</li> <li>• Oracle Solaris 10</li> </ul>	<p>Voor versie 10.0.1 van OpenAM is Java Development Kit 1.6 vereist, ten minste 1.6.0_10. ForgeRock raadt u aan ten minste versie 1.6.0_27 te gebruiken vanwege beveiligingsoplossingen. ForgeRock heeft deze release van OpenAM voornamelijk getest met Oracle Java SE JDK. OpenAM Java SDK ondersteunt Java Development Kit 1.5 of 1.6.</p>	<ul style="list-style-type: none"> <li>• Apache Tomcat 6.0.x, 7.0.x</li> <li>• GlassFish v2</li> <li>• JBoss Enterprise Application Platform 4.x, 5.x</li> <li>• JBoss Application Server 7.x</li> <li>• steiger 7</li> <li>• Oracle WebLogic Server 11g</li> <li>• Oracle WebLogic Server 12c</li> </ul> <p>Als u als een niet-rootgebruiker uitvoert, moet de webtoepassingscontainer kunnen schrijven naar zijn eigen hoofddirectory, waar OpenAM configuratiebestanden opslaat.</p>	<ul style="list-style-type: none"> <li>• Chroom en chroom 16 en hoger</li> <li>• Firefox 3.6 en hoger</li> <li>• Internet Explorer (versie 7 en hoger)</li> <li>• Safari 5 en later</li> </ul>	

## Installeren

### OpenAM-software verkrijgen

- Download OpenAM 10.0.1 releases van <https://backstage.forgerock.com/downloads/OpenAM/OpenAM%20Enterprise/10.0.1/OpenAM%201>
- Voor elke release van de OpenAM-kernservices kunt u het volledige pakket downloaden als een .zip-archief, alleen het OpenAM .war-bestand, alleen de administratieve hulpmiddelen als een .zip-archief
- Nadat u het archief van het hele pakket hebt uitgepakt, krijgt u een openSo-directory met een README, een set licentiebestanden en de directory's

### voorwaarden

Zorg ervoor dat u de vereiste vereiste software voor OpenAM-kernservices hebt voordat u deze installeert,

- Een Java 6 runtime omgeving
- Apache Tomcat installeren als webtoepassingscontainer

- OpenAM-kernservices vereisen een minimale Java Virtual Memory (JVM) heapgrootte van 1 GB en een permanente generatiegrootte van 256 MB. Pas de JVM-opties toe wanneer u JAVA\_OPTS instelt in het Catalina-bestand voordat de tomcat-toepassingsserver wordt gestart - `-Xmx1024m -XX:MaxPermSize=256m`

Bijvoorbeeld set `JAVA_OPTS=%JAVA_OPTS% -Xmx1024m -XX:MaxPermSize=256m -Xms512m`

- Installeer Microsoft Active Directory als een Data Store met weinig gebruikers.

## OpenAM-webtoepassing installeren

Het bestand `deployable-war/opensso.war` bevat alle OpenAM-servercomponenten en -monsters in de directory `openso`.

OpenAM implementeren op Tomcat-container

Kopieer het bestand `opensso.war` naar de directory waar tomcat-webtoepassingen worden opgeslagen. Wijzig de naam van het bestand `opensso.war` in `openam.war`. Start de tomatenservice opnieuw op.

Controleer het scherm voor de eerste configuratie in uw browser op <http://<FQHN>:8080/openam>



## Configuration Options

Please select a configuration option.

### Default Configuration

Enter only the passwords for the default administrator and the agent accessor. All other data is configured using default parameters. This option should be used primarily for evaluation or development purposes.

[Create Default Configuration](#)

### Custom Configuration

Allows you to specify all configuration parameters including the type of data store, encryption properties, user data store, etc. This option has the most flexibility in setting up your installation.

[Create New Configuration](#)

Copyright © 2010-2011 ForgeRock AS, Philip Pedersens vei 1, 1366 Lysaker, Norway. All rights reserved. Licensed for use under the Common Development and Distribution License (CDDL), see <http://www.forgerock.com/license/CDDLv1.0.html> for details. This software is based on the OpenSSO/OpenAM open source project and the source includes the copyright works of other authors, granted for use under the CDDL. This distribution may include other materials developed by third parties. All Copyrights and Trademarks are property of their owners.

## OpenAM-service uitvoeren

Openam is een eenvoudige webapplicatie gehost in een tomcat-server. Dus, start gewoon uw tomcat-server en heb dus toegang tot de OpenAM-webservice.

## Configureren

# OpenAM Configurator

Het aangepaste configuratieproces van OpenAM maakt het mogelijk om veel algemene configuratieopties eenvoudig in te stellen, dus met meer moeite voor de configuratie worden de configuratiestappen die later nodig zijn, opgeslagen.

Algemene instellingen

Klik op Nieuwe configuratie maken en kies het wachtwoord voor de standaardbeheerdersaccount (amAdmin). Het wachtwoord moet minimaal 8 tekens lang zijn.

OpenAM Configurator

Custom Configuration Option

→ General

2. Server Settings

3. Configuration Store

4. User Store

5. Site Configuration

6. Agent Information

7. Summary

**Step 1: General**

Enter the password for the default user, amAdmin. The password must be at least 8 characters in length. If this configuration will be part of an existing deployment, the password you enter must match that of the original deployment.

\* Indicates required field

**Default User Password**

Default User [amAdmin]

\* Password   OK

\* Confirm Password

Previous Next Cancel

Zodra een geldig wachtwoord tweemaal is ingevoerd, verschijnt de knop Volgende en kan de configuratie worden voortgezet.

Serverinstellingen

Standaard is de server-URL de volledig gekwalificeerde domeinnaam van de server.

---

Opmerking: Het is belangrijk dat de gebruiker die Apache Tomcat uitvoert, schrijftoegang

---

heeft tot de configuratiemap. Hierdoor is ~/openam/config geschikt voor dit doel. Ondersteunde platformlocaties zijn en\_US (Engels), de (Duits), es (Spaans), fr (Frans), ja (Japans), zh\_CN (vereenvoudigd Chinees) of zh\_TW (traditioneel Chinees).

The screenshot shows the 'OpenAM Configurator' window with the title 'Custom Configuration Option'. On the left is a navigation menu with seven items: 1. General, 2. Server Settings (highlighted with a blue arrow), 3. Configuration Store, 4. User Store, 5. Site Configuration, 6. Agent Information, and 7. Summary. The main area is titled 'Step 2: Server Settings' and includes a sub-header 'Server Settings'. Below this, there are four text input fields, each preceded by an asterisk indicating it is a required field. The fields are: 'Server URL' with the value 'http://openamserver.cisco.com:8080', 'Cookie Domain' with the value '.cisco.com', 'Platform Locale' with the value 'en\_US', and 'Configuration Directory' with the value 'C:/Users/Administrator/openam'. A legend on the right states '\* Indicates required field'. At the bottom of the window are three buttons: 'Previous', 'Next' (highlighted with a blue border), and 'Cancel'.

Field	Value
* Server URL	http://openamserver.cisco.com:8080
* Cookie Domain	.cisco.com
* Platform Locale	en_US
* Configuration Directory	C:/Users/Administrator/openam

Instellingen voor de Configuration Data Store

Voor configuratie met één server hoeven deze instellingen niet te worden gewijzigd.

OpenAM Configurator

### Custom Configuration Option

- 1. General
- 2. Server Settings
- **Configuration Store**
- 4. User Store
- 5. Site Configuration
- 6. Agent Information
- 7. Summary

#### Step 3: Configuration Data Store Settings

If no other OpenAM instance already exists in the environment, then choose First Instance. If one or more OpenAM instances already exist in the environment, choose Add to Existing Deployment.

First Instance  Add to Existing Deployment? \* Indicates required field

#### Configuration Store Details

Configuration Data Store  OpenAM  OpenDJ or Sun Java System Directory Server

\* SSL/TLS Enabled

\* Host Name

\* Port

\* Admin Port

\* JMX Port

\* Encryption Key

\* Root Suffix

Instellingen voor opslag van gebruikersgegevens

De instellingen voor de gebruikersgegevensopslag verbinden OpenAM met de Microsoft Active Directory-gegevensopslag.

OpenAM Configurator X

**Custom Configuration Option**

1. General
2. Server Settings
3. Configuration Store
- ➔ 4. User Store
5. Site Configuration
6. Agent Information
7. Summary

### Step 4: User Data Store Settings

You can use the data store that comes with the OpenAM configuration data store, or you can use a different user data store. A good practice for setting up production environments is to use an external user data store, one that is different than the OpenAM user data store. Please note that Policy Service and LDAP Authentication Module shall be configured to use the Directory Administrator DN and Password provided here.

OpenAM User Data Store  
 Other User Data Store

\* Indicates required field

**User Store Details**

\* User Data Store Type

Sun Java System Directory Server  
 Active Directory with Host and Port  
 Active Directory Application Mode

OpenDJ  
 AD with Domain Name  
 IBM Tivoli Directory Server

\* SSL/TLS Enabled

\* Directory Name

\* Port

\* Root Suffix

\* Login ID

\* Password   OK

Previous
Next
Cancel

- Type gebruikersgegevensopslag: Active Directory met host en poort
- SSL/TLS ingeschakeld: niet ingeschakeld
- Directory-naam: <Domeinnaam van AD-server>
- Poort: 389
- Achtervoegsel wortel: dc=cisco, dc=com
- Inlog-ID: cn=<AD-gebruikersnaam>, cn=gebruikers, dc=cisco, dc=com
- Wachtwoord: <AD-gebruikerswachtwoord>

Opmerking: De configurator biedt geen optie om door te gaan totdat alle instellingen correct zijn opgegeven en de verbinding met de Active Directory-instantie is voltooid.

#### Siteconfiguratie

In het scherm Siteconfiguratie kunt u OpenAM instellen als onderdeel van een site waar de belasting over meerdere OpenAM-servers wordt verdeeld. Accepteer de standaardinstellingen voor de eerste OpenAM-installatie.

OpenAM Configurator

### Custom Configuration Option

- 1. General
- 2. Server Settings
- 3. Configuration Store
- 4. User Store
- **Site Configuration**
- 6. Agent Information
- 7. Summary

#### Step 5: Site Configuration

Will this instance be deployed behind a load balancer as part of a site configuration?

No  
 Yes

\* Indicates required field

##### Site Configuration Details

This is the first instance of OpenAM, and no site configurations currently exist. To create a new site configuration, provide the following information

\* Site Name

\* Load Balancer URL

Agentgegevens

Geef in het scherm Agentinformatie een wachtwoord van ten minste 8 tekens op dat door de beleidsagenten moet worden gebruikt om verbinding te maken met OpenAM.

OpenAM Configurator ✕

**Custom Configuration Option**

- 1. General
- 2. Server Settings
- 3. Configuration Store
- 4. User Store
- 5. Site Configuration
- ➔ **Agent Information**
- 7. Summary

**Step 6: Default Policy Agent User**

These settings are used by OpenAM policy agents for retrieving policy agent properties.

\* Indicates required field

**Policy Agent User**

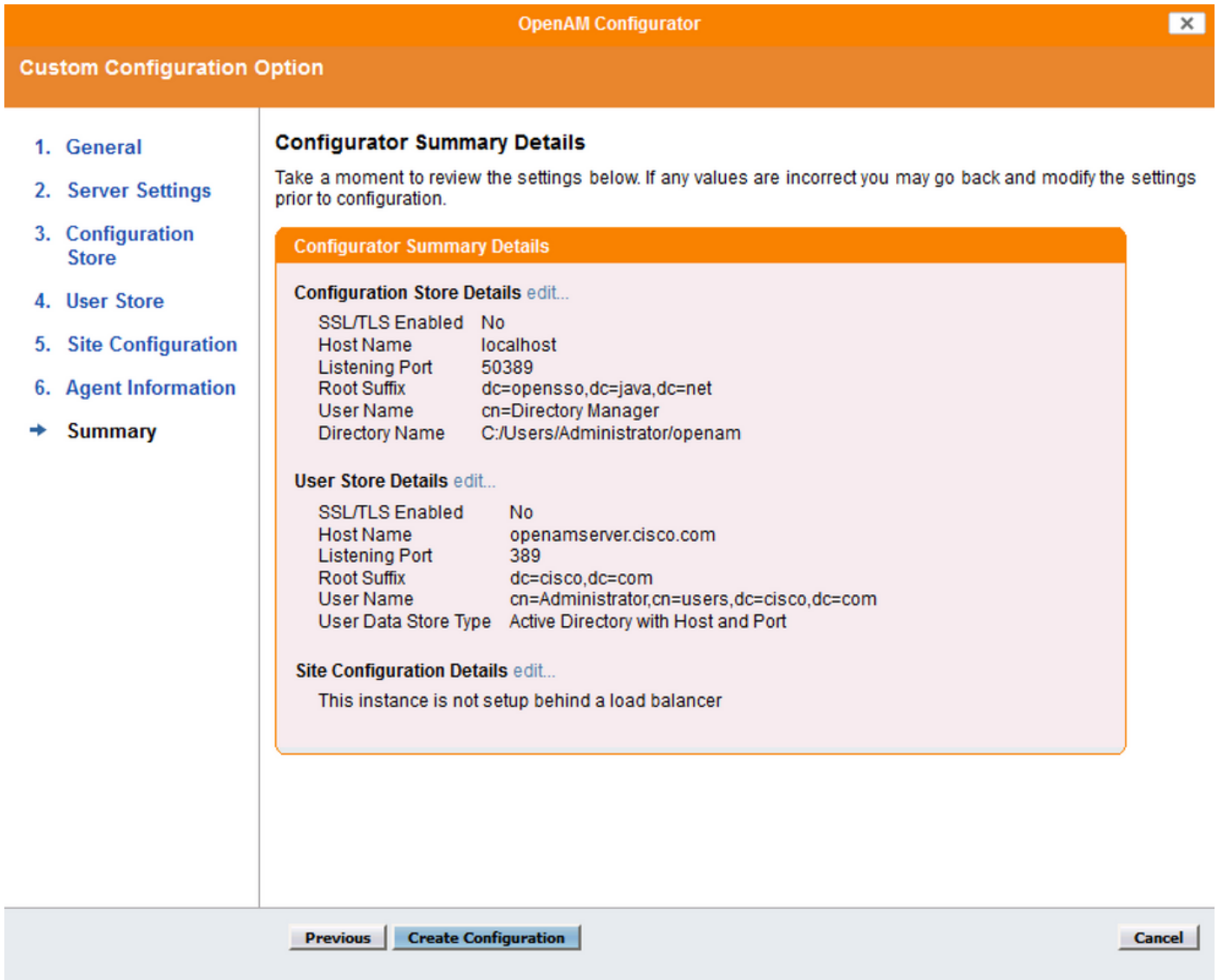
**Default Policy Agent [UriAccessAgent]**

\* Password   OK

\* Confirm Password

Samenvatting

Controleer de informatie en klik op Configuratie maken



## Configuratievoortgang

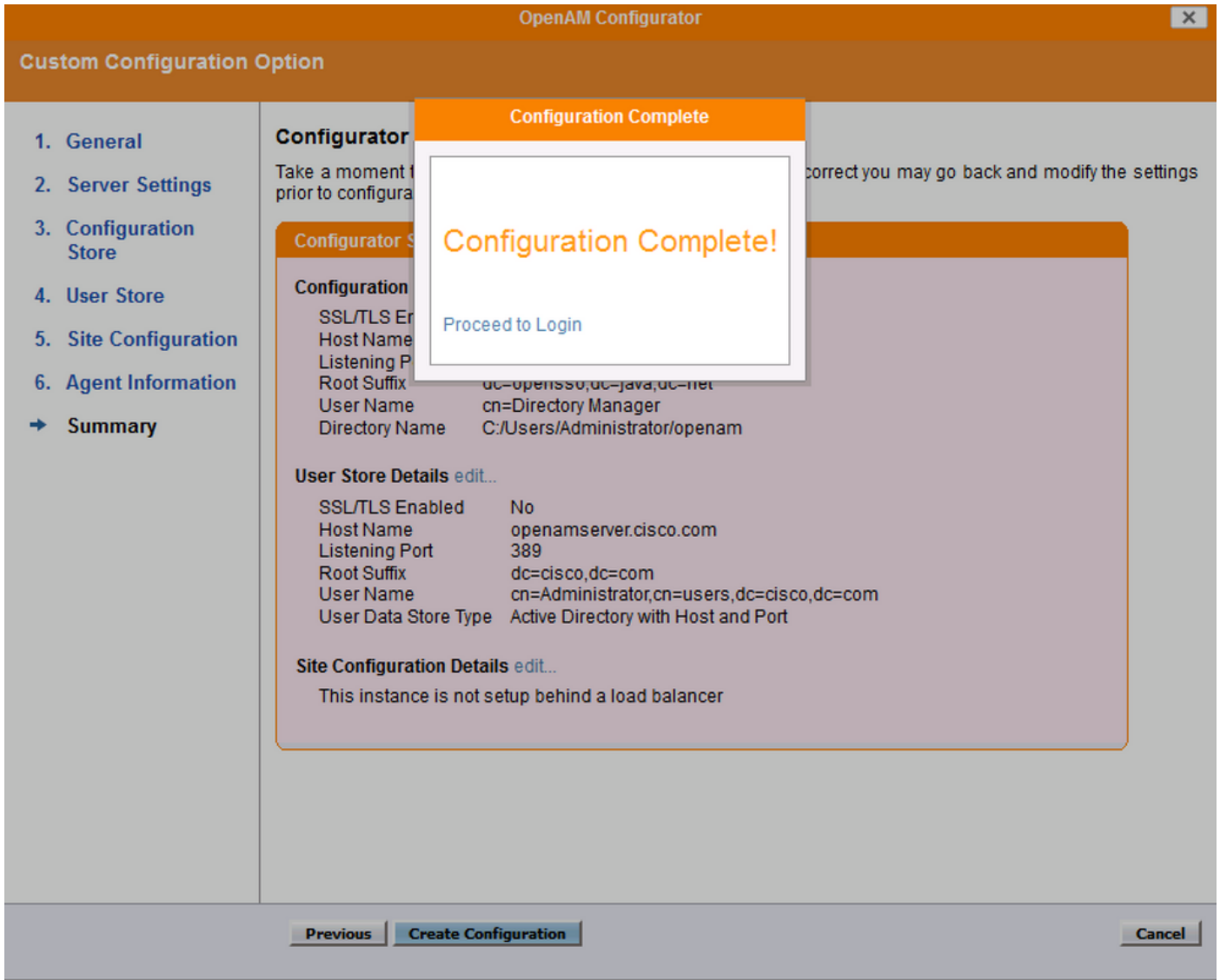
Het scherm Configuration Progress (Configuratievoortgang) geeft de voortgang van de installatie weer. Alle uitvoer op dit scherm en alle fouten worden naar het bestand geschreven: `~/openam/config/install.log`.

Please wait... configuration in progress...



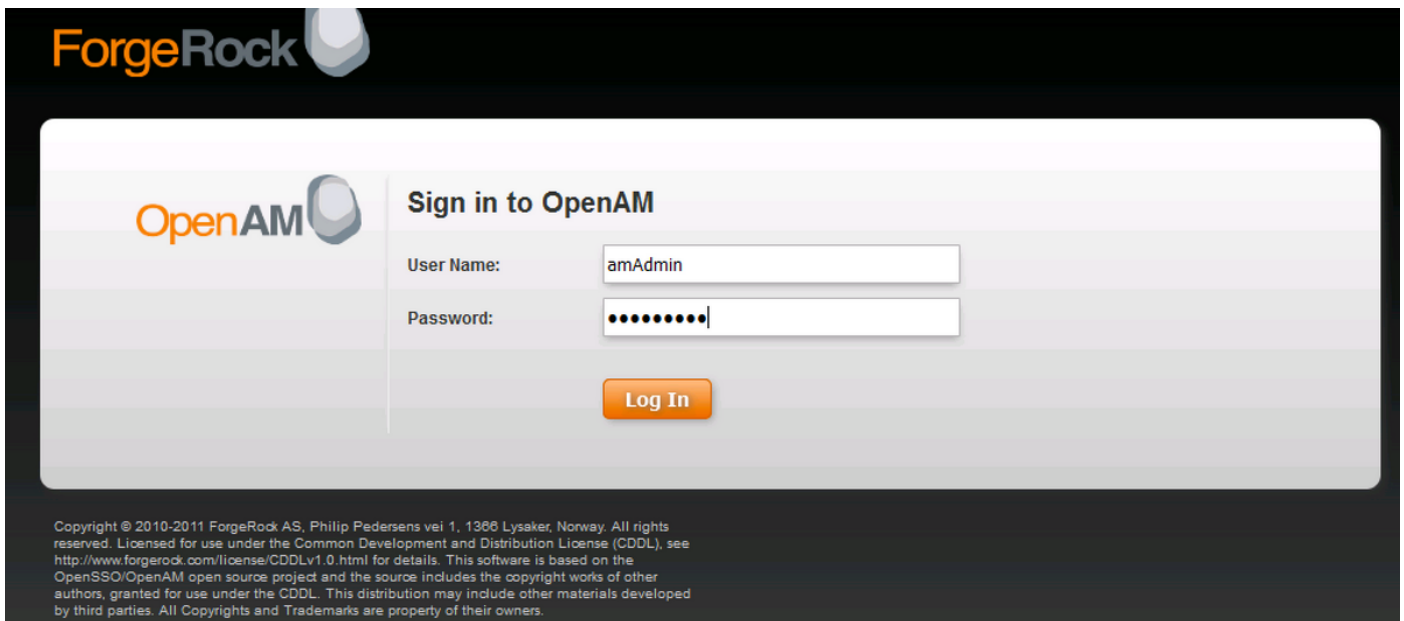
```
Checking configuration directory C:/Users/Administrator/openam....Success.  
Installing OpenAM configuration store...Success RSA/ECB/OAEPWithSHA1AndMGF1Padding.  
Extracting OpenDJ, please wait...Complete  
Running OpenDJ setupSetup command: --cli --adminConnectorPort 4444 --baseDN  
dc=openesso,dc=java,dc=net --rootUserDN cn=Directory Manager --ldapPort 50389 --skipPortCheck  
--rootUserPassword xxxxxx --jmxPort 1689 --no-prompt --configFile C:/Users/Administrator/openam  
/opens/config/config.ldif --doNotStart --hostname openamserver.cisco.com OpenDJ 2.4.5  
Please wait while the setup program initializes...
```

Configuratie voltooid



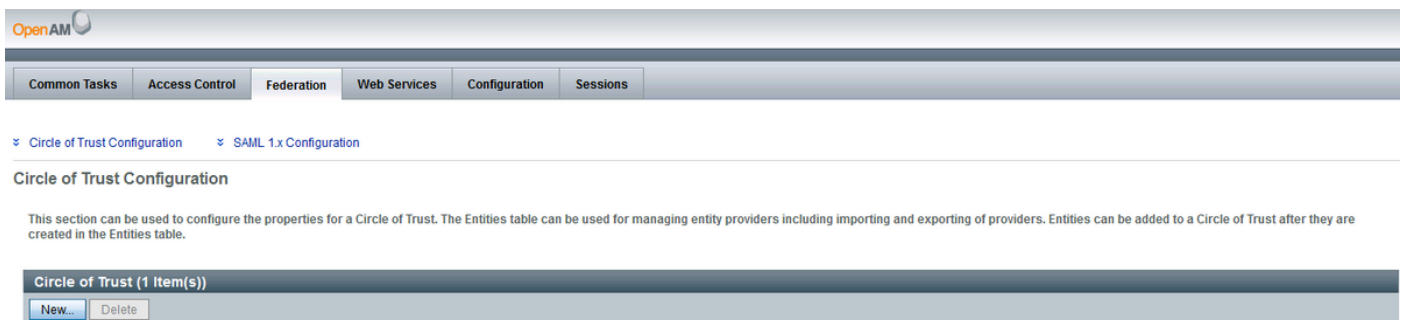
## OpenAM configureren als IdP

- Klik op Doorgaan om in te loggen of toegang te krijgen via URL <http://<FQDN of OpenAM>:8080/openam>, en meld u vervolgens aan als OpenAM-beheerder
- Wanneer u OpenSSO Enterprise voor de eerste keer opent, wordt u doorgestuurd naar de Configurator om de eerste configuratie van OpenSSO Enterprise uit te voeren
- Standaardconfiguratie selecteren
- U moet de wachtwoorden voor OpenAMserver configureren
- Configureer de wachtwoorden en log in op OpenAM server UI

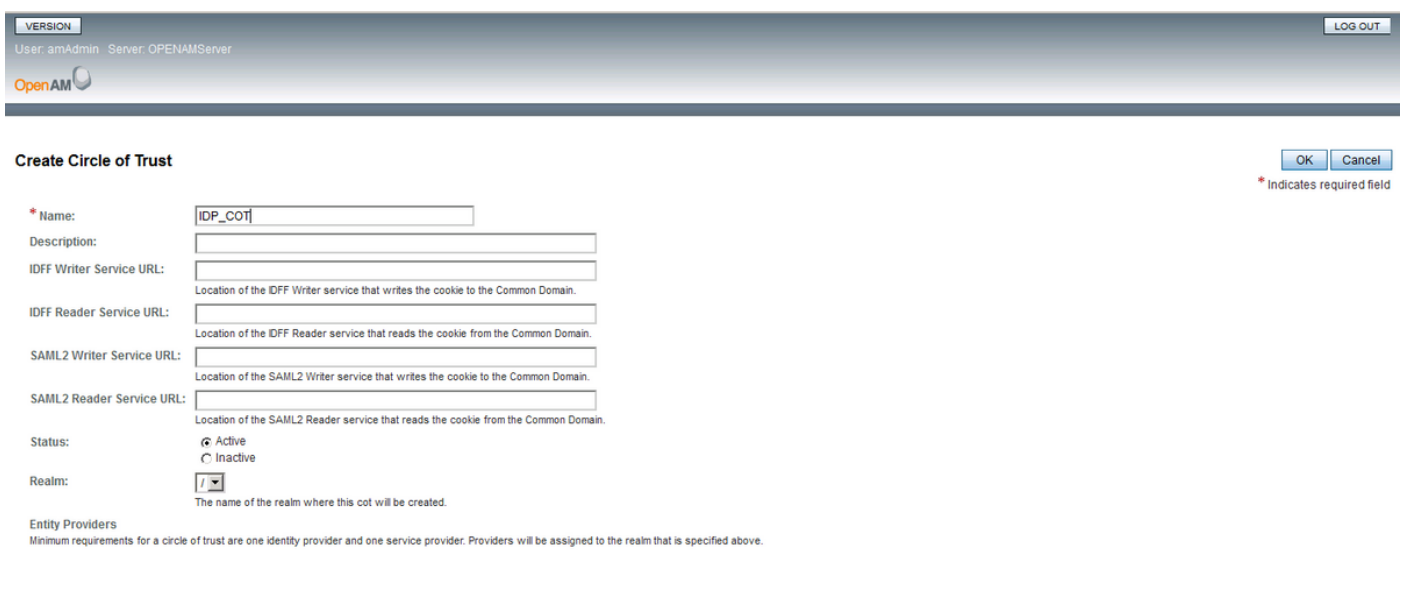


## Configuratie Circle of Trust

Navigeer naar het tabblad Federatie en klik op de knop Nieuw onder de sectie Circle of Trust



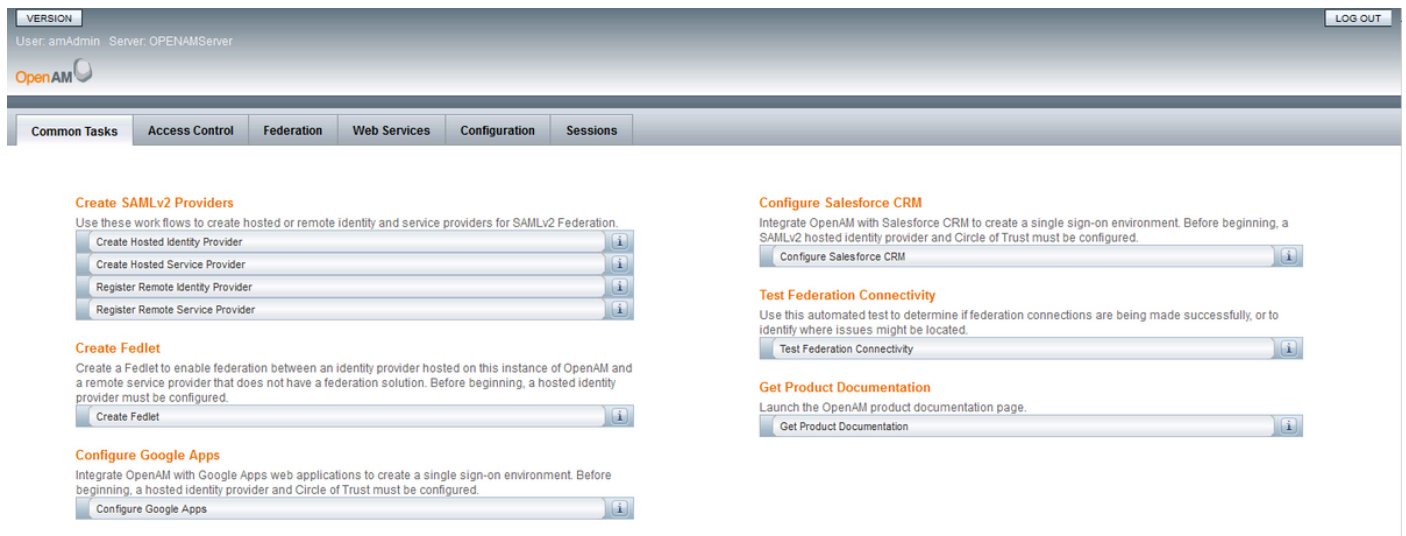
Maak een vertrouwenscirkel met een unieke naam voor de IdP-vertrouwenscirkel en klik op OK



Opmerking: Serviceverlener en IdP moeten zich in dezelfde vertrouwenscirkel (CoT) bevinden om SAML SSO te laten werken.

## Hosted Identity Provider maken

Navigeer naar het tabblad Algemene taken en klik op Gehoste identiteitsprovider maken en maak een gehoste IdP (laat de standaard geconfigureerde waarden en sla de instellingen op).



The screenshot shows the OpenAM administration interface. At the top, there is a header with 'VERSION', 'User: amAdmin', 'Server: OPENAMServer', and a 'LOG OUT' button. Below the header is a navigation menu with tabs for 'Common Tasks', 'Access Control', 'Federation', 'Web Services', 'Configuration', and 'Sessions'. The main content area is divided into several sections, each with a title and a description, followed by a button with an information icon:

- Create SAMLv2 Providers**: Use these work flows to create hosted or remote identity and service providers for SAMLv2 Federation. Buttons: Create Hosted Identity Provider, Create Hosted Service Provider, Register Remote Identity Provider, Register Remote Service Provider.
- Create Fedlet**: Create a Fedlet to enable federation between an identity provider hosted on this instance of OpenAM and a remote service provider that does not have a federation solution. Before beginning, a hosted identity provider must be configured. Button: Create Fedlet.
- Configure Google Apps**: Integrate OpenAM with Google Apps web applications to create a single sign-on environment. Before beginning, a hosted identity provider and Circle of Trust must be configured. Button: Configure Google Apps.
- Configure Salesforce CRM**: Integrate OpenAM with Salesforce CRM to create a single sign-on environment. Before beginning, a SAMLv2 hosted identity provider and Circle of Trust must be configured. Button: Configure Salesforce CRM.
- Test Federation Connectivity**: Use this automated test to determine if federation connections are being made successfully, or to identify where issues might be located. Button: Test Federation Connectivity.
- Get Product Documentation**: Launch the OpenAM product documentation page. Button: Get Product Documentation.

## De Circle of Trust die eerder is gemaakt, wordt vermeld

### Circle of Trust

Choose from existing circles of trust listed or provide one to be created in which to include this IDP. A COT is a group of IDPs and SPs that trust each other and provides the confines within which all SAMLv2 communications are performed.

Circles of Trust:  Add to existing  Add to new

\* Existing Circle of Trust:

## Ondertekeningsleutel configureren

Navigeer naar het tabblad Federatie en klik op gehoste identiteitsprovider toegevoegd onder sectie Entiteitsproviders. Navigeer naar de sectie Assertie-inhoud en configureer de waarde van het ondertekeningsveld als test onder de sectie Certificaat-aliassen. Dit is het certificaat dat zou worden gebruikt om de SAML-verklaring te ondertekenen.

- ✘ Signing and Encryption
- ✘ Assertion Time
- ✘ Bootstrapping
- ✘ NameID Format
- ✘ Basic Authentication
- ✘ Authentication Context
- ✘ Assertion Cache

## Signing and Encryption

### Request/Response Signing

Select the checkbox for each request/response that should be signed

- Authentication Request:
- Artifact Resolve:
- Logout Request:
- Logout Response:
- Manage Name ID Request:
- Manage Name ID Response:

### Encryption

NameID Encryption:

### Certificate Aliases

Signing:

The alias (name) of the certificate to be used to sign assertions.

entiteit van importserviceprovider

Navigeer naar het tabblad Federatie en klik op de knop Entiteit importeren... onder het gedeelte Entiteitsproviders.

The screenshot shows the OpenAM administration interface. The 'Federation' tab is selected. Under 'Circle of Trust Configuration', there is a table for 'Circle of Trust (1 Item(s))' with one entry: 'IDP\_COT' with realm '/' and status 'Active'. Below it is the 'Entity Providers (3 Item(s))' section with a table containing three providers.

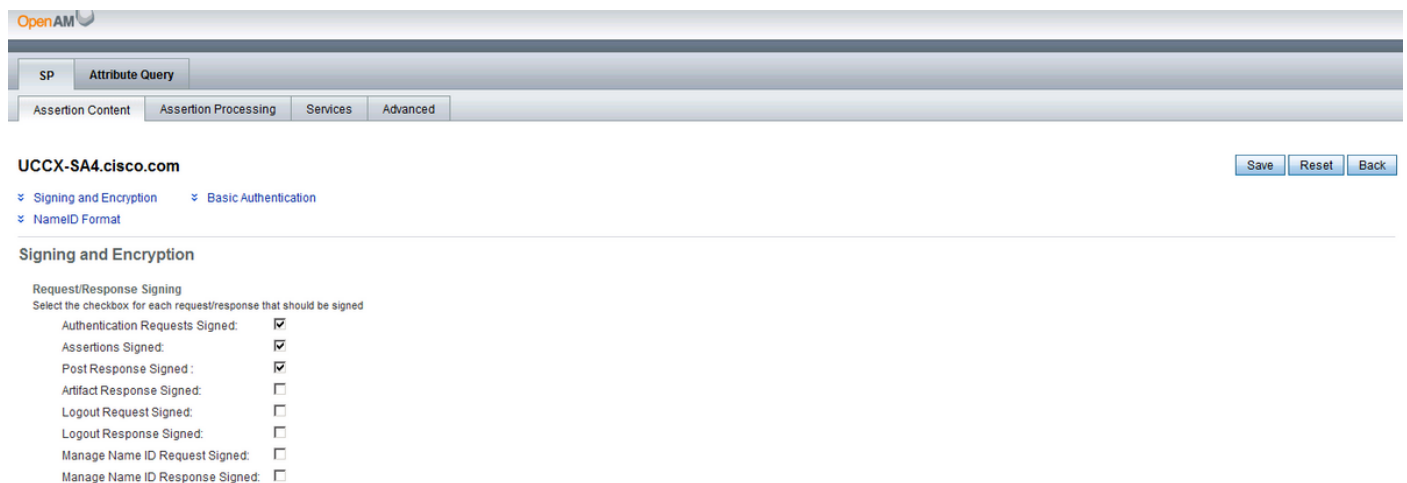
Name	Entities	Realm	Status
IDP_COT	UCCX-HA-Node1.cisco.com saml2 https://openamserver.cisco.com:8443/openam saml2 UCCX-SA4.cisco.com saml2	/	Active

Upload het Entiteitsbestand van de Serviceverlener (sp.xml) en sla de pagina op.

The screenshot shows the 'Import Entity Provider' form. It includes fields for 'Realm Name', 'Where does the metadata file reside?' (URL/File), 'URL where metadata is located' (with an 'Upload...' button), 'Where does the extended data file reside?' (URL/File), and 'URL where extended data is located'.

## Aanvraag-/antwoordondertekening

Klik op de geïmporteerde entiteit en schakel ondertekening in voor Request/Response



The screenshot shows the OpenAM configuration interface for the 'UCCX-SA4.cisco.com' service. The 'Attribute Query' tab is active, and the 'Advanced' sub-tab is selected. The 'Signing and Encryption' section is expanded, showing a list of checkboxes for signing requests and responses. The following table represents the state of these checkboxes:

Request/Response	Checked
Authentication Requests Signed:	<input checked="" type="checkbox"/>
Assertions Signed:	<input checked="" type="checkbox"/>
Post Response Signed:	<input checked="" type="checkbox"/>
Artifact Response Signed:	<input type="checkbox"/>
Logout Request Signed:	<input type="checkbox"/>
Logout Response Signed:	<input type="checkbox"/>
Manage Name ID Request Signed:	<input type="checkbox"/>
Manage Name ID Response Signed:	<input type="checkbox"/>

## attribuuttoewijzing

Navigeer naar Assertion Processing en voeg een toewijzingskenmerk toe voor uid en user\_principal volgens de instellingen Directory en OpenAM. Klik op Opslaan.



The screenshot shows the OpenAM configuration interface for the 'UCCX-SA4.cisco.com' service, specifically the 'Attribute Mapper' section. The 'Artifact Message Encoding' sub-tab is active. The 'Attribute Map' section shows a list of 'Current Values' with a 'Remove' button next to each. The current values are:

- uid=sAMAccountName
- user\_principal=userPrincipalName

Below the list is a 'New Value' input field and an 'Add' button. A note at the bottom states: 'This mapping is the configuration used by the Attribute Mapper. Mapping should be defined as SAML ATTRIBUTE NAME=PROFILE ATTRIBUTE NAME in assertion. Example: EmailAddress=mail, Address=postaladdress.'

Opmerking: Zowel de attributen uid en user\_principal zijn verplicht – omdat Service Provider (SP) de identiteit van een Geverifieerde gebruiker identificeert met behulp van deze. Zorg er ook voor dat de attributen sAMAccountName en userPrincipalName ook zijn toegewezen in de Attribuiteditor van Active Directory-gebruikerseigenschappen.

## Circle of Trust bewerken

Navigeer naar het tabblad Federatie en klik op Circle of Trust toegevoegd en zorg ervoor dat u de IdP (OpenAm-server) en de entiteit van de Serviceverlener verplaatst van Beschikbaar naar Geselecteerde secties onder de sectie Entiteitsproviders. Dit wijst IdP en Serviceverlener toe aan dezelfde Circle of Trust.





## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.