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

Inhoud

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 Identitify 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 Identitify 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	geg
• Microsoft Windows Server 2003, 2008 R2 • Linux 2.6, 3.0 • Oracle Solaris 10	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.	• Apache Tomcat 6.0.x, 7.0.x • GlassFish v2 • JBoss Enterprise Application Platform 4.x, 5.x • JBoss Application Server 7.x • steiger 7 • Oracle WebLogic Server 11g • Oracle WebLogic Server 12c Als u als een niet-rootgebruiker uitvoert, moet de webtoepassingscontainer kunnen schrijven naar zijn eigen hoofddirectory, waar OpenAM configuratiebestanden opslaat.	• Chroom en chroom 16 en hoger • Firefox 3.6 en hoger • Internet Explorer (versie 7 en hoger) • Safari 5 en later	

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.

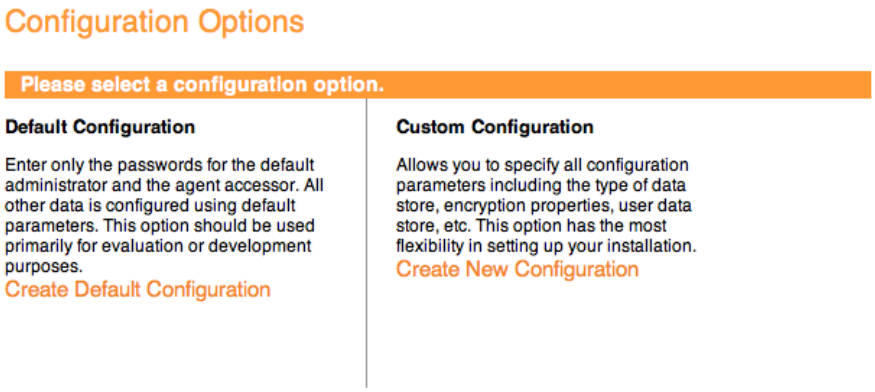
OpenAM-webtoepassing installeren

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



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.

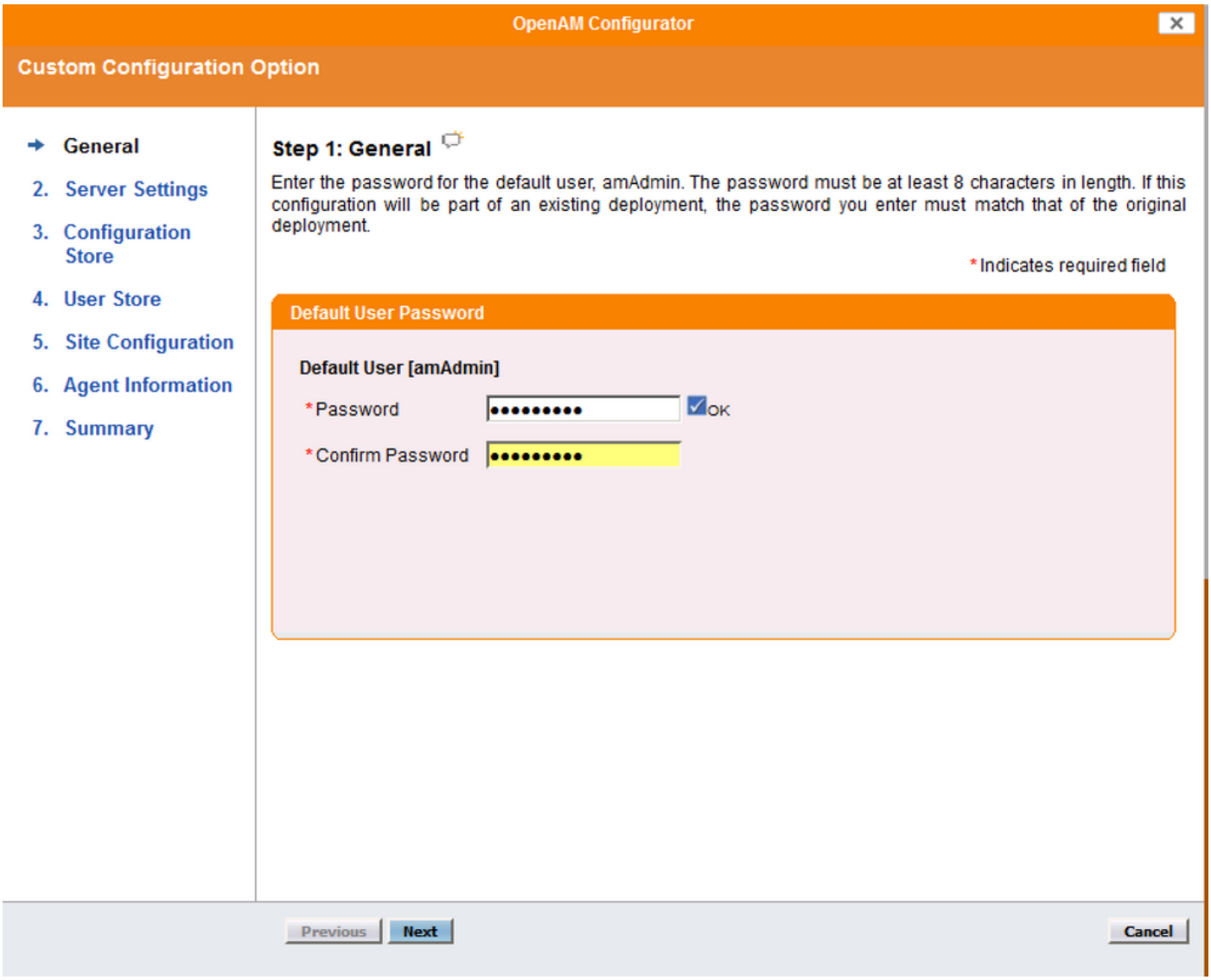
Configureren

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.



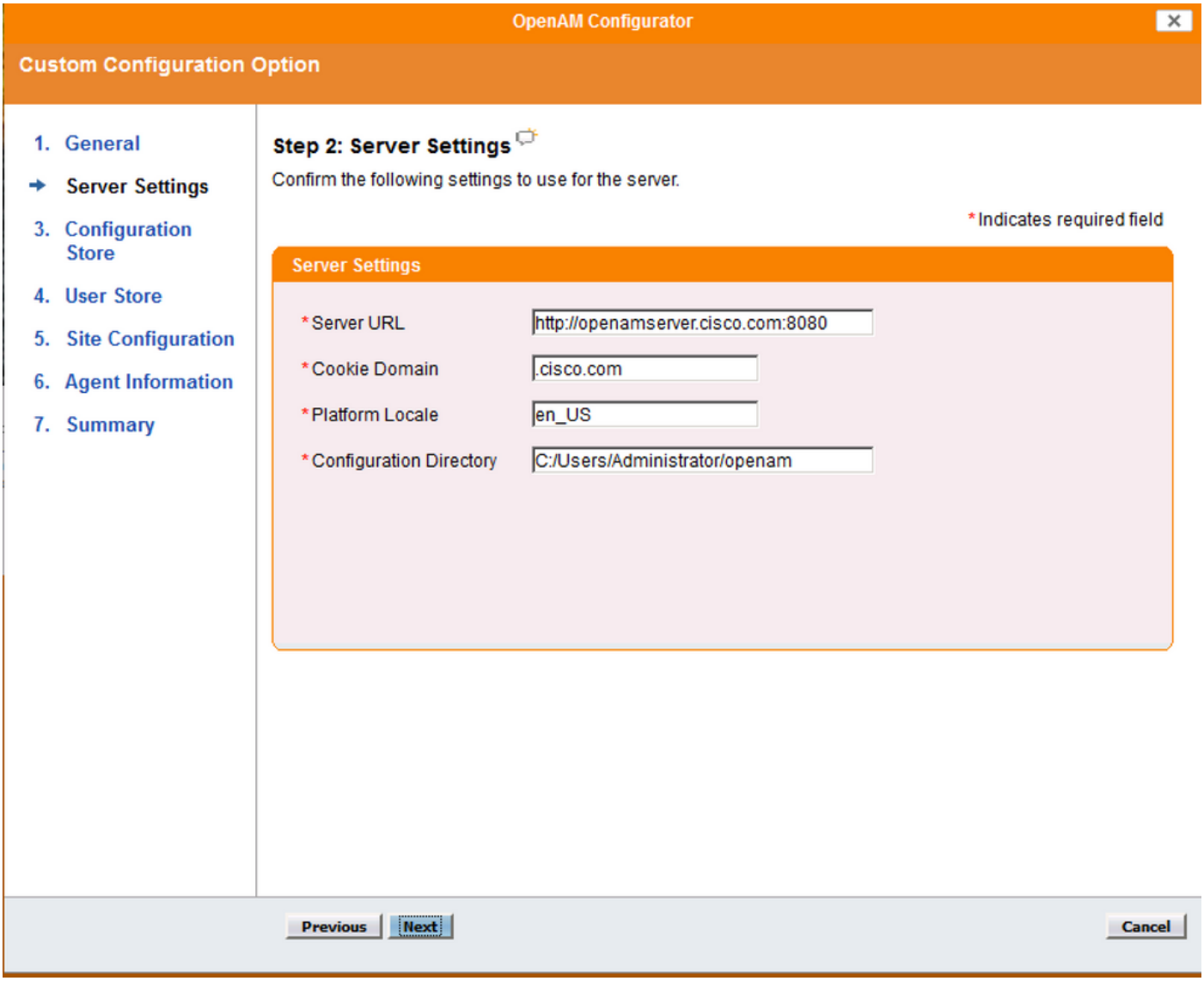
Zodra een geldig wachtwoord tweemaal is ingevoerd, verschijnt de knop Volgende en kan de configuratie worden voortgezet.

Serverinstellingen

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

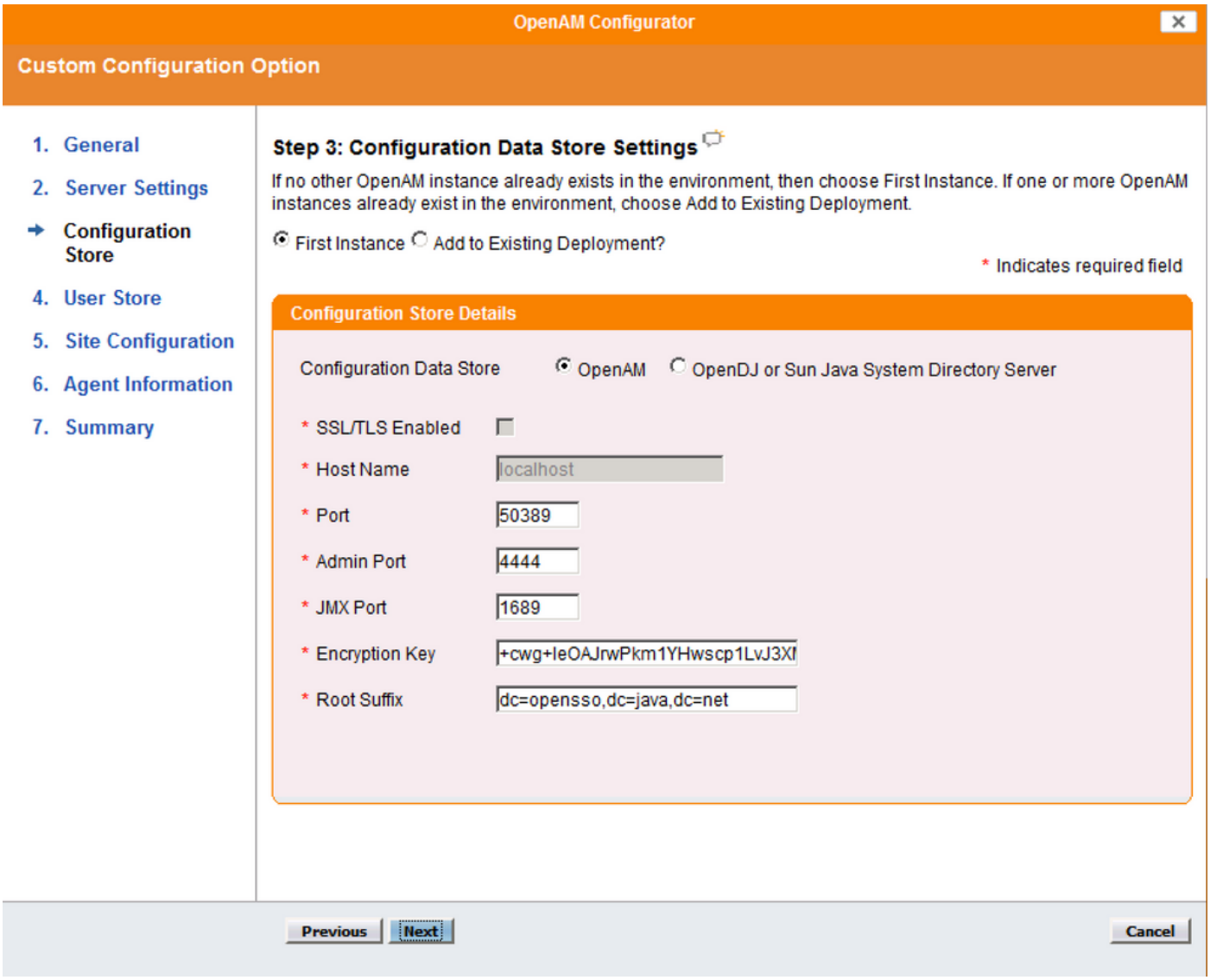
Opmerking: Het is belangrijk dat de gebruiker die Apache Tomcat uitvoert, schrijftoegang

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).



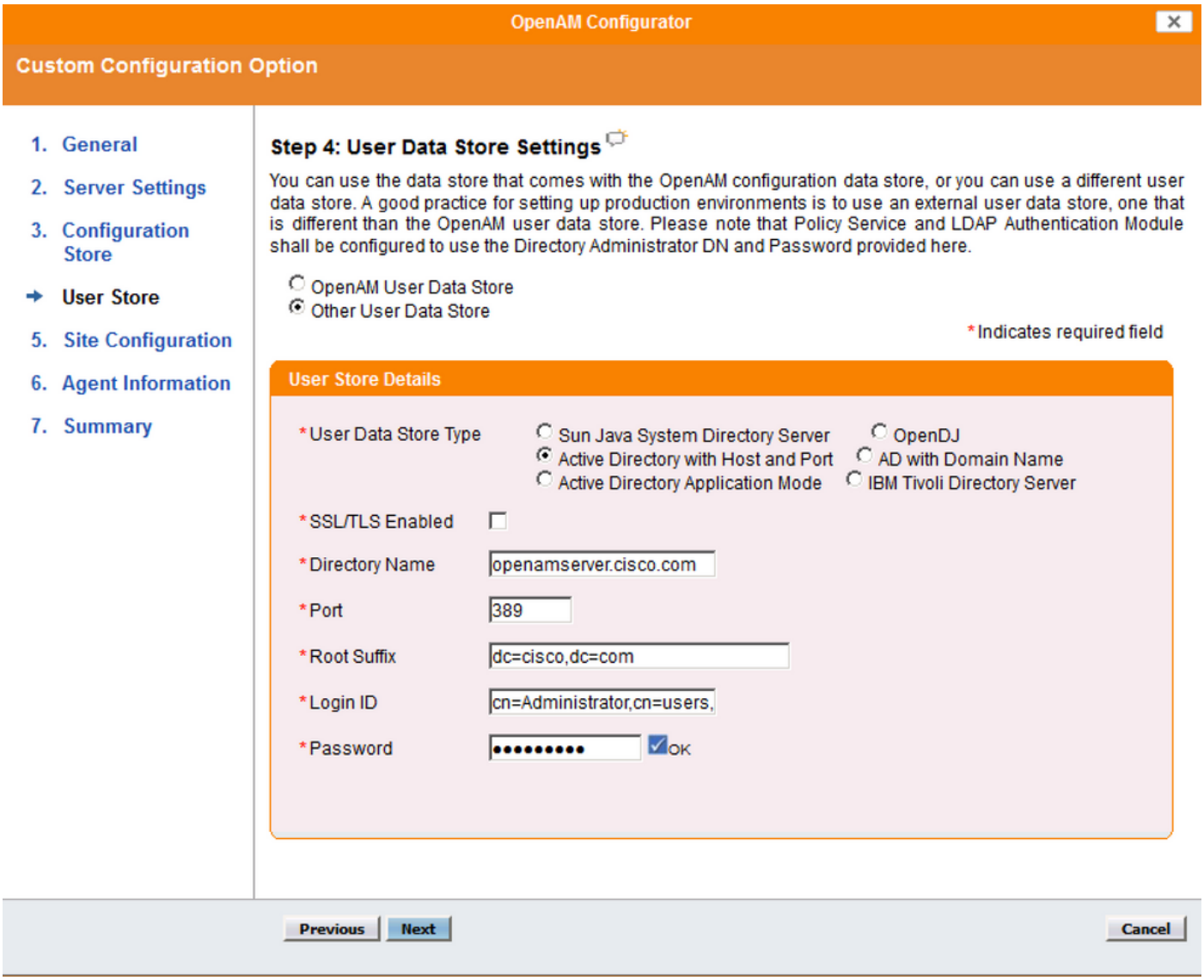
Instellingen voor de Configuration Data Store

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



Instellingen voor opslag van gebruikersgegevens

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

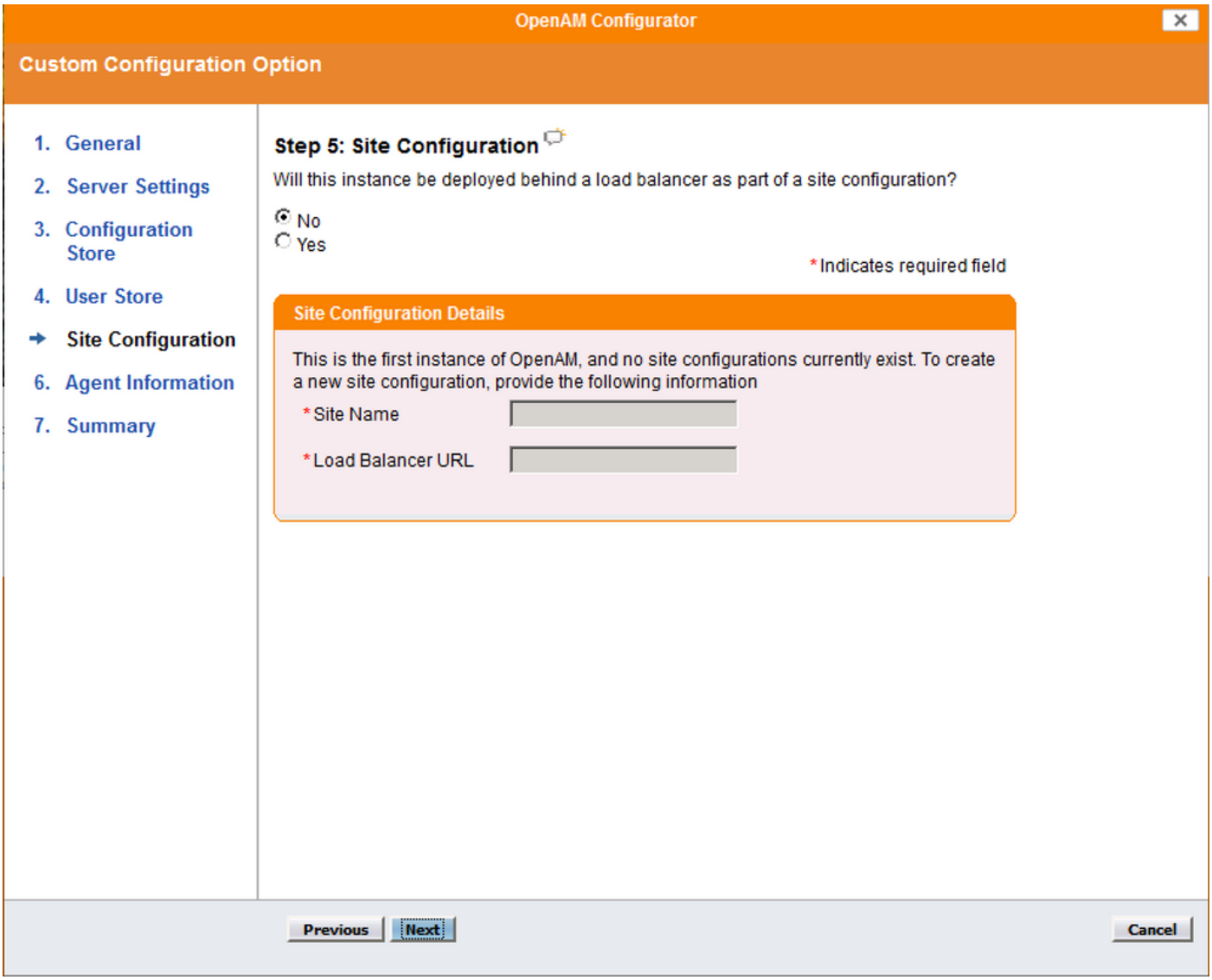


- Type gebruikersgegevensopslag: Active Directory met host en poort
- SSL/TLS ingeschakeld: niet ingeschakeld
- Directory-naam: <Domeinnaam van AD-server>
- Poort: 389
- Achtervoegsel wortel: dc=cisco, dc=com
- Inlog-ID: cn=<AD-gebruikersnaam>, cn=gebruikers, dc=cisco, dc=com
- Wachtwoord: <AD-gebruikerswachtwoord>

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.

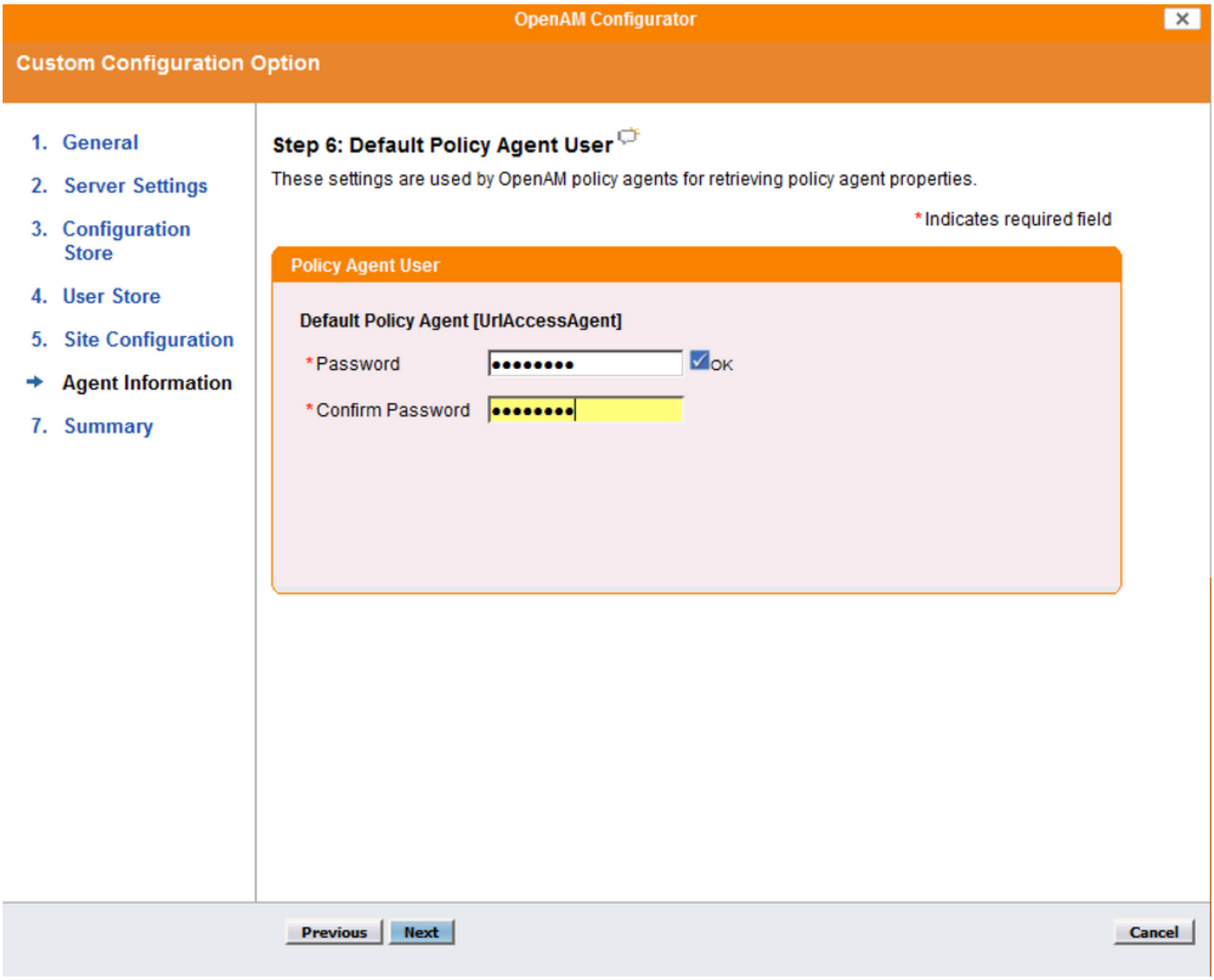
Siteconfiguratie

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.



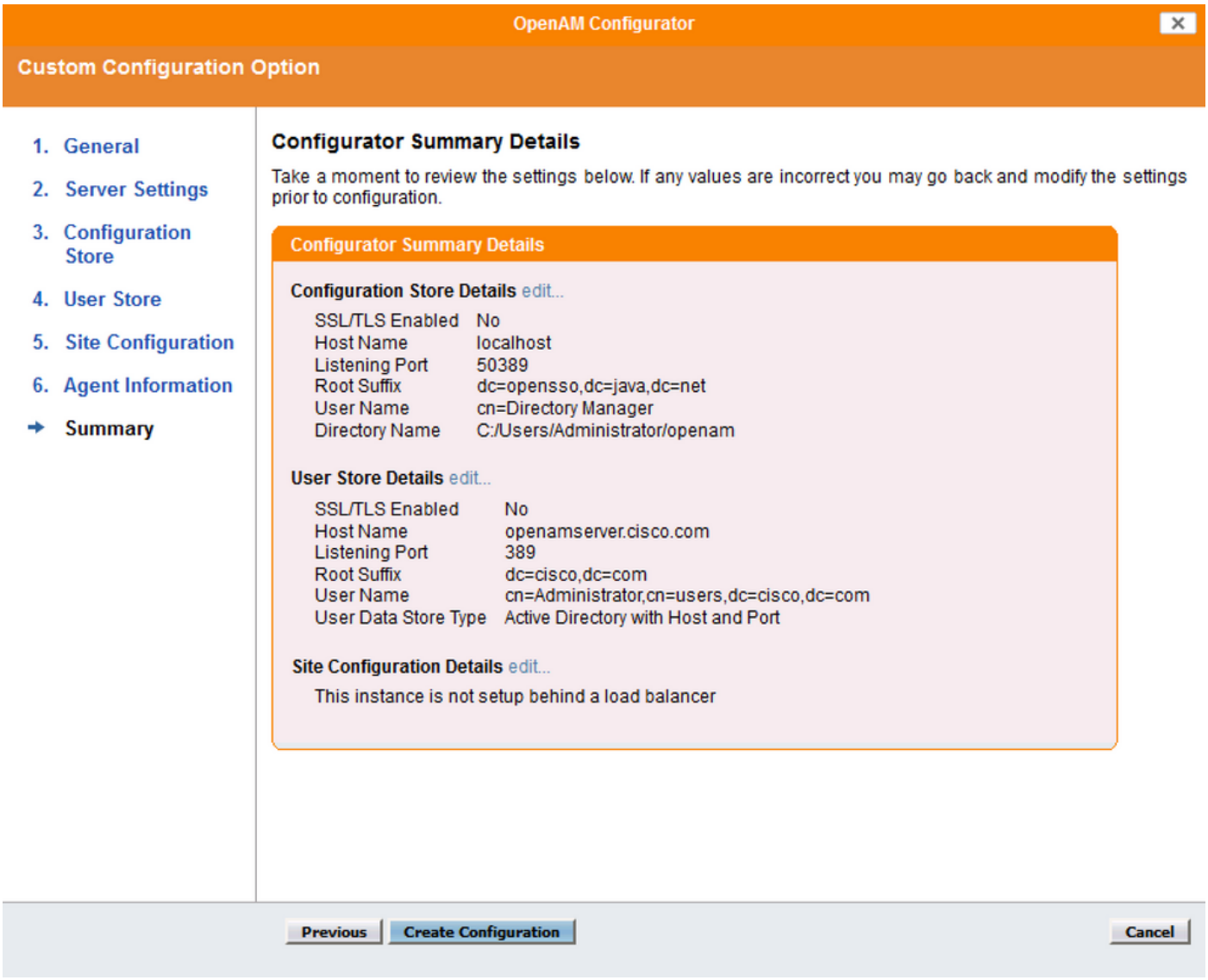
Agentgegevens

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.



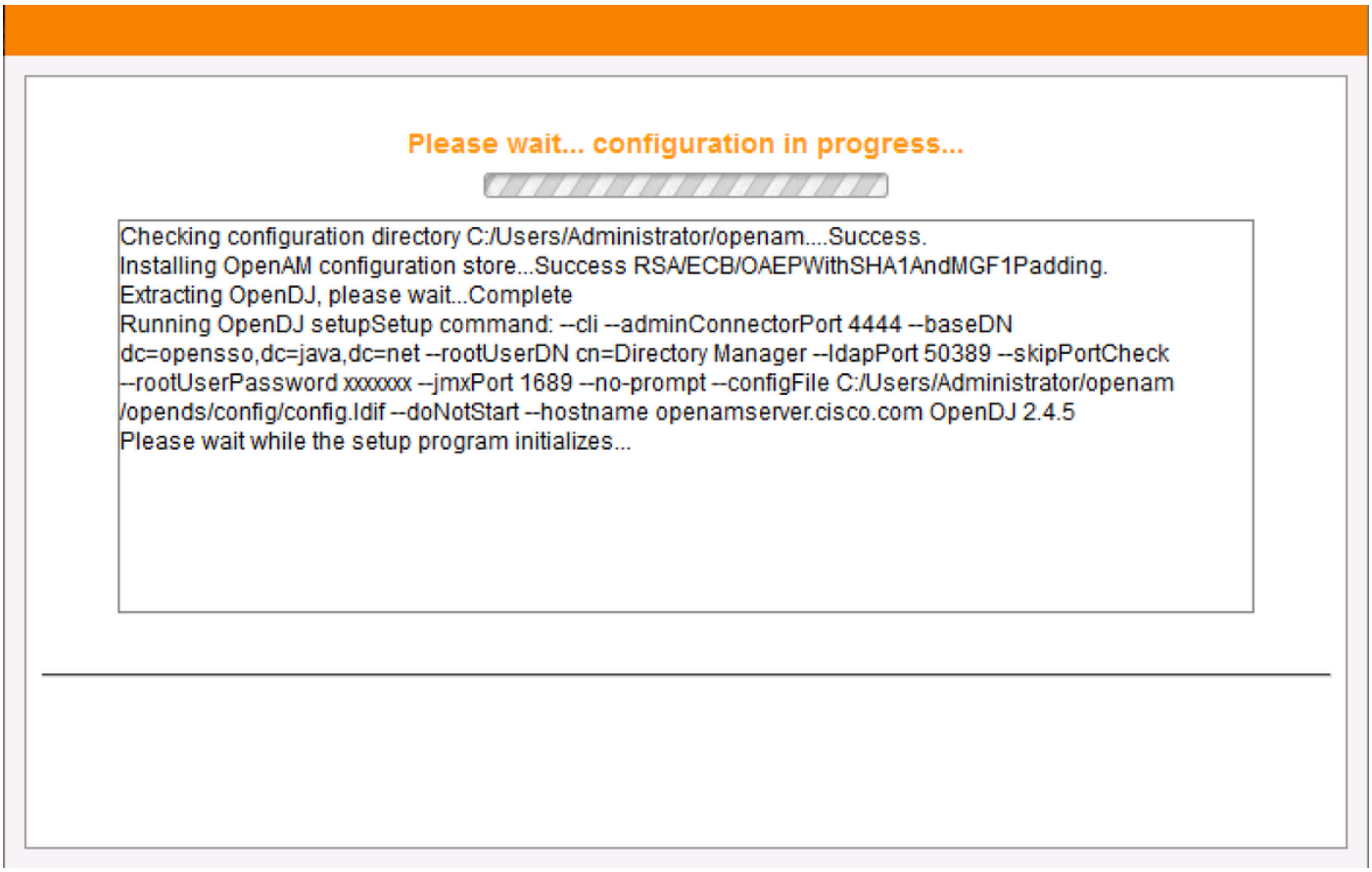
Samenvatting

Controleer de informatie en klik op Configuratie maken

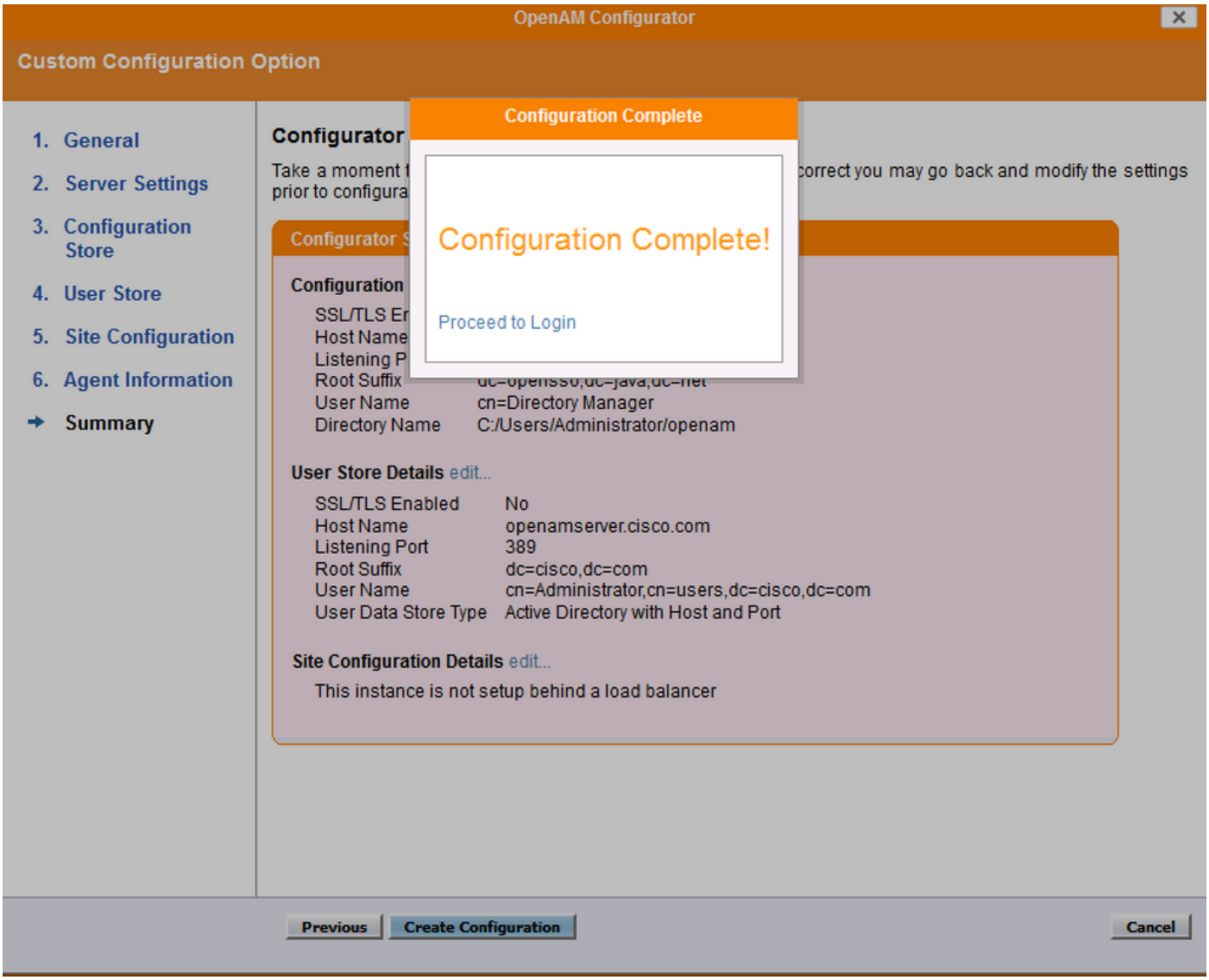


Configuratievoortgang

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.

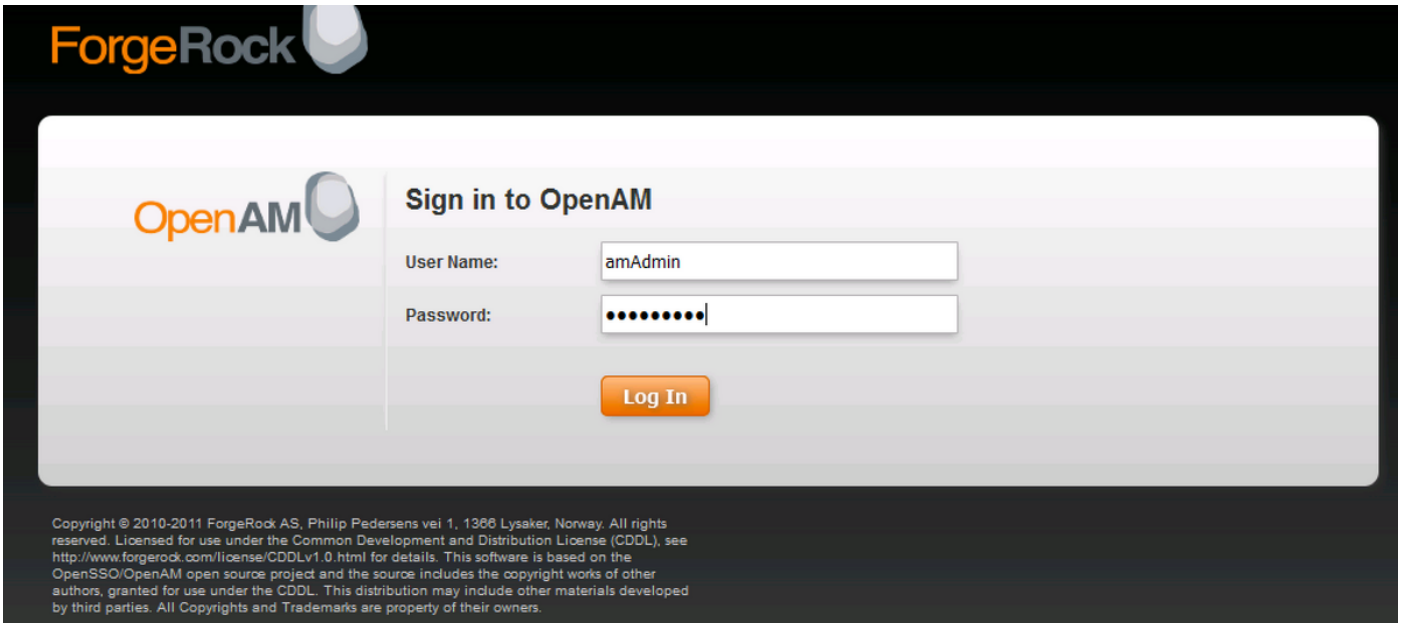


Configuratie voltooid



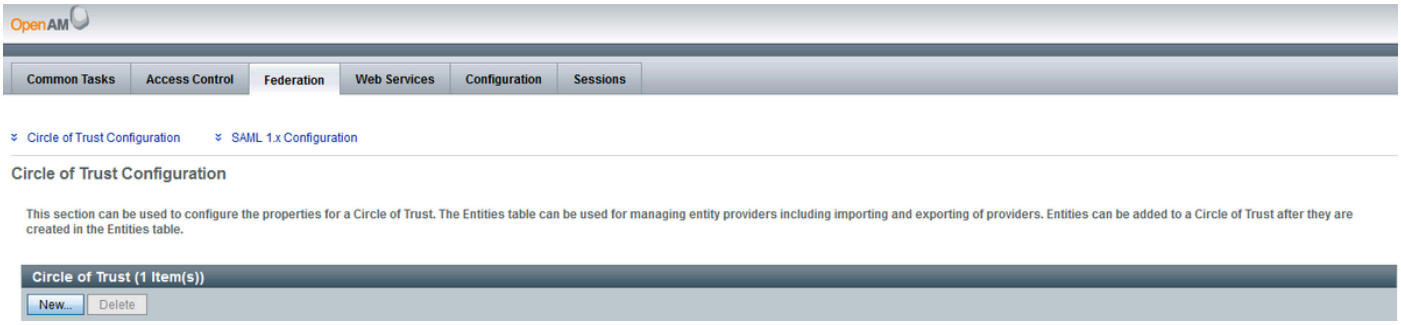
OpenAM configureren als IdP

- 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

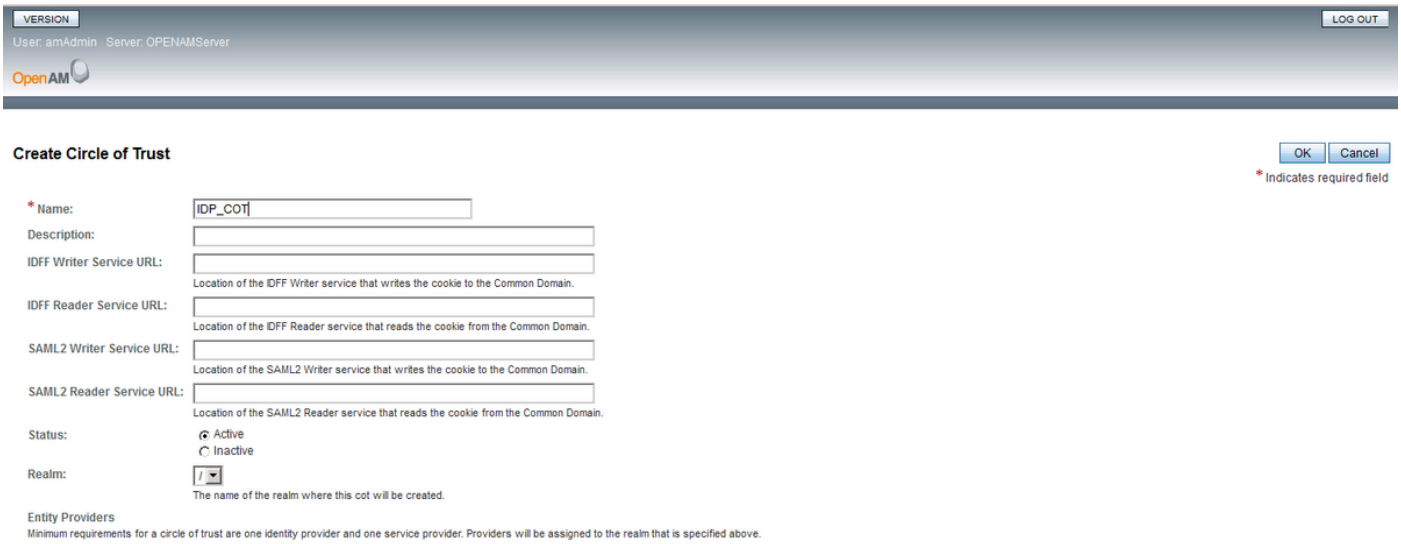


Configuratie Circle of Trust

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



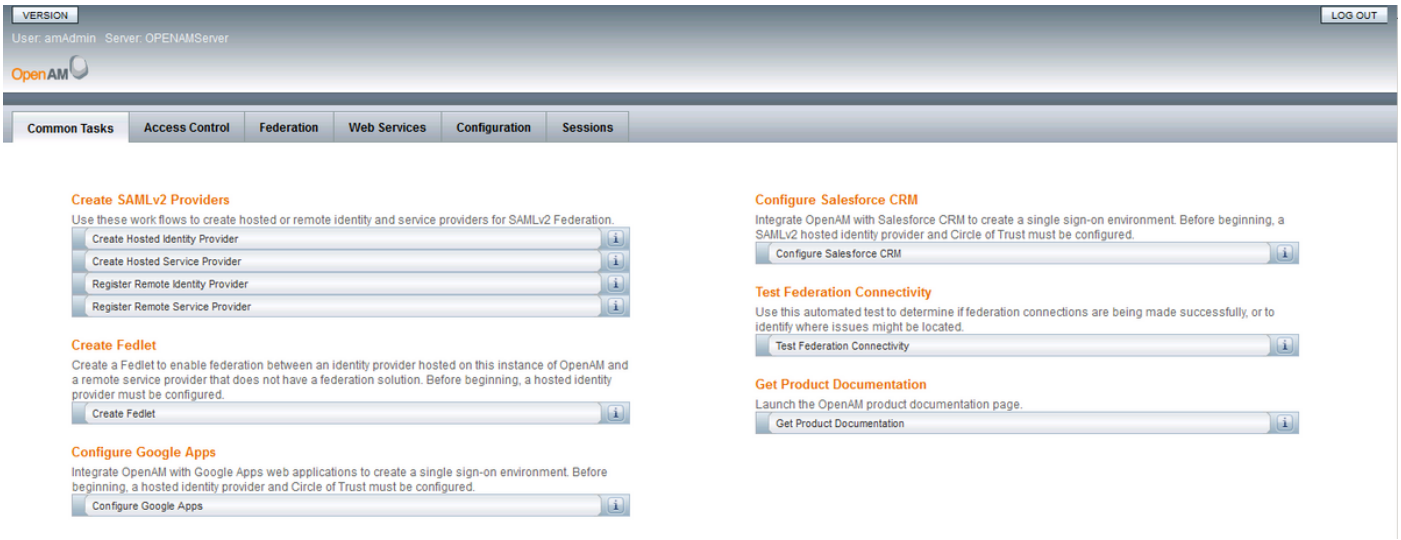
Maak een vertrouwenscirkel met een unieke naam voor de IdP-vertrouwenscirkel en klik op OK



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

Hosted Identity Provider maken

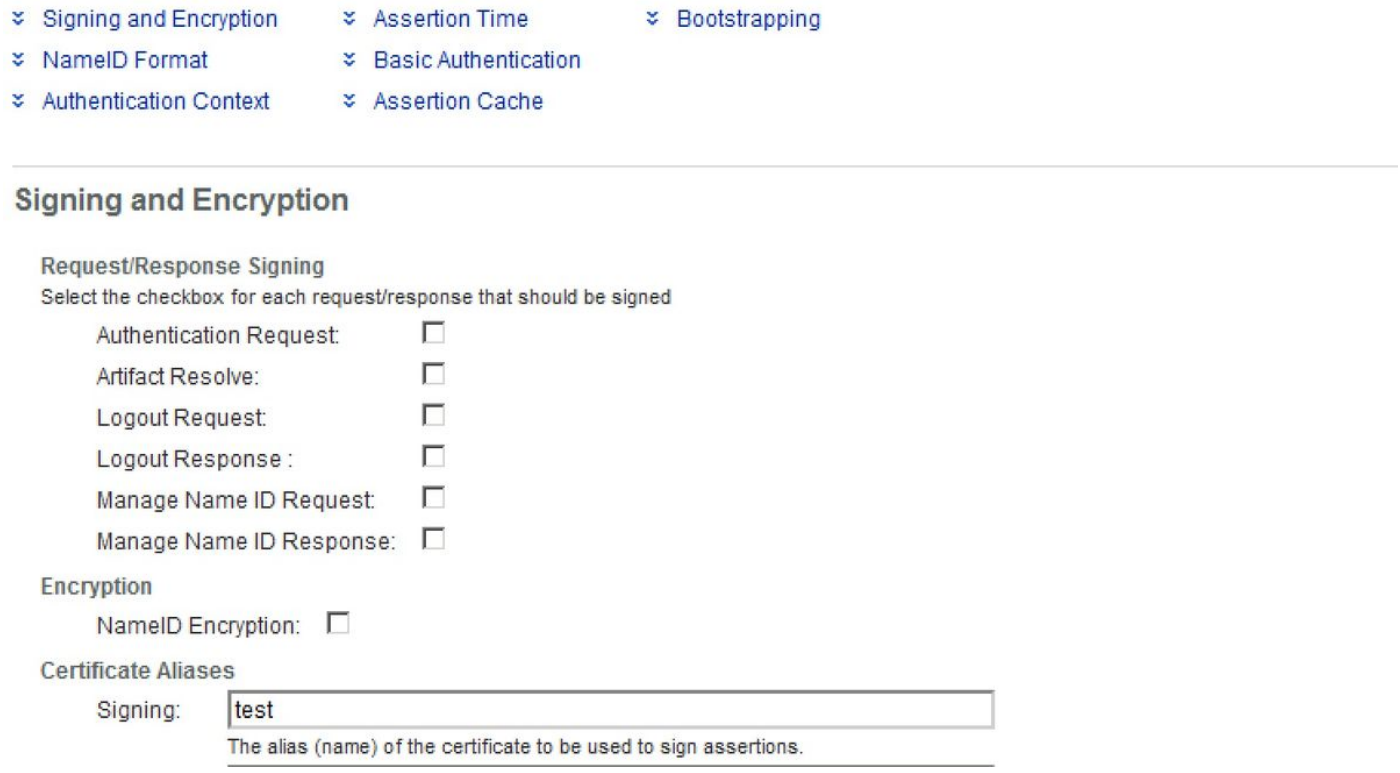
Navigeer naar het tabblad Algemene taken en klik op Gehoste identiteitsprovider maken en maak een gehoste IdP (laat de standaard geconfigureerde waarden en sla de instellingen op).



De Circle of Trust die eerder is gemaakt, wordt vermeld

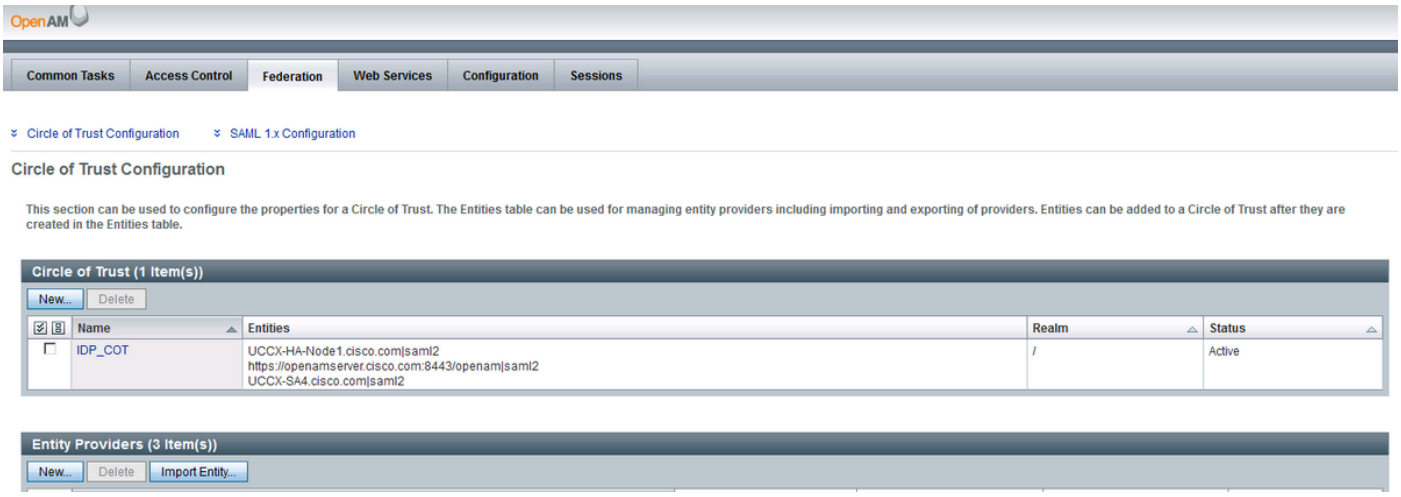
Ondertekeningssleutel configureren

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.

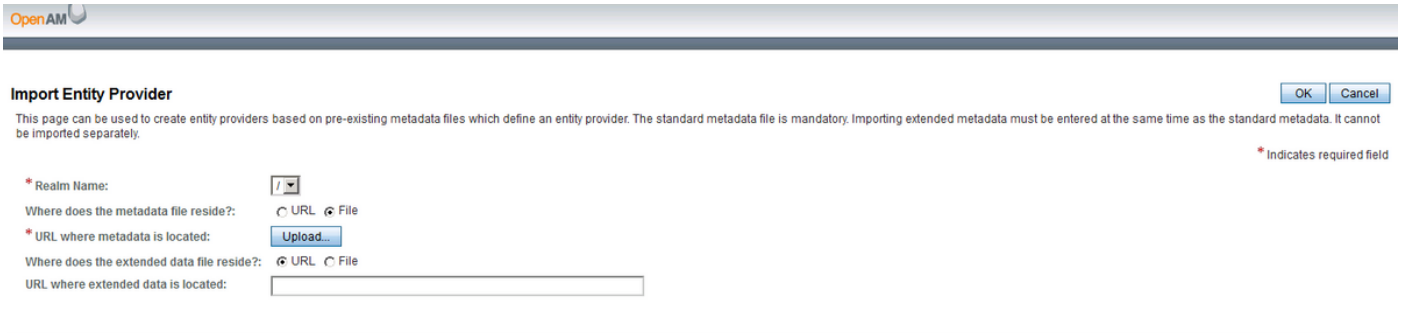


entiteit van importserviceprovider

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

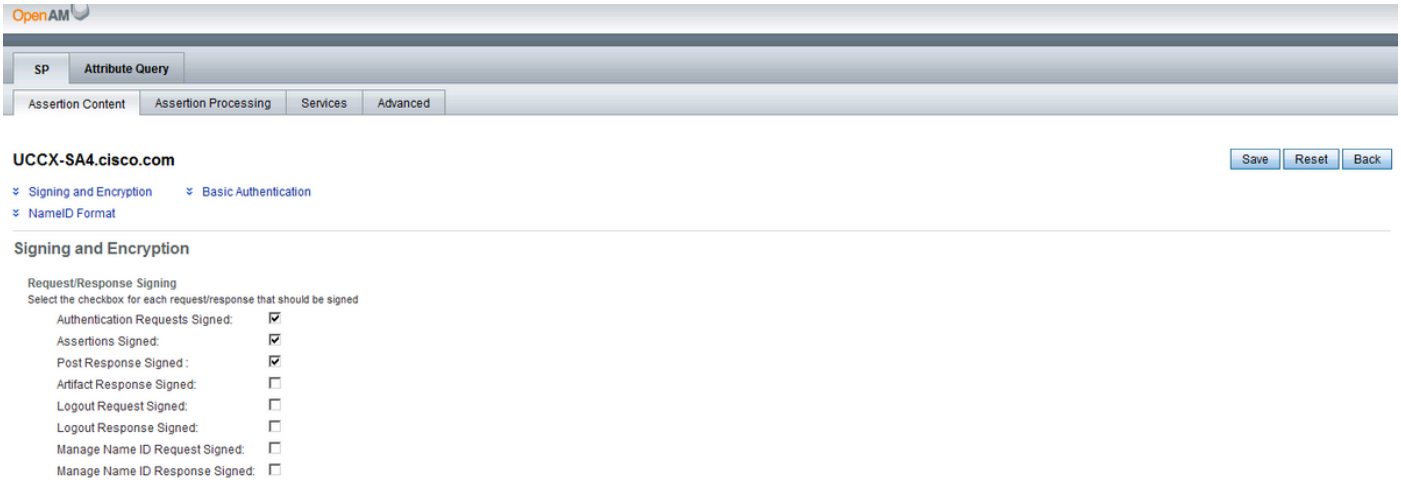


Upload het Entiteitsbestand van de Serviceverlener (sp.xml) en sla de pagina op.



Aanvraag-/antwoordondertekening

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



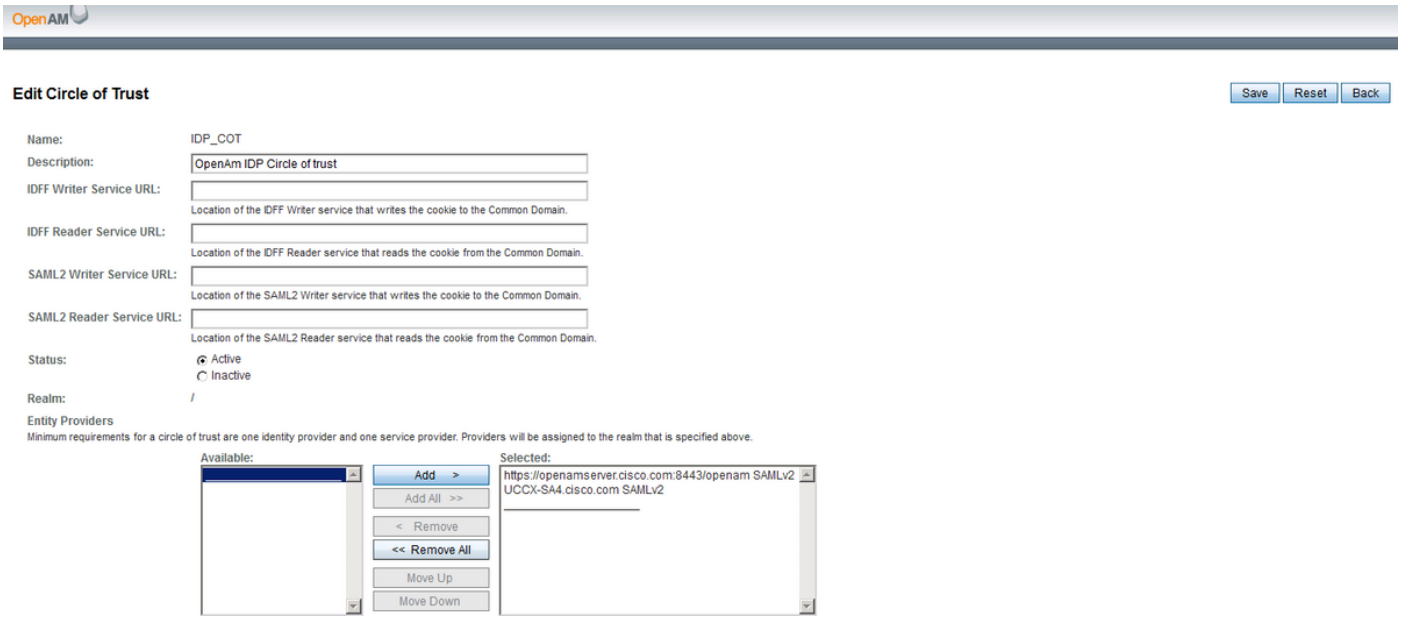
attribuuttoewijzing

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

> 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 sAMAaccountName en userPrincipalName ook zijn toegewezen in de Attribuuteditor 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.



OpenAM IdP-metagegevens downloaden

U kunt het IdPmetadatafile van OpenAM server downloaden met de URL [http://<FQDN van OpenAM>:8080/openam/saml2/jsp/exportmetadata.jsp?entityid=http://<FQDN van OpenAM>:8080/openam&realm=]

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://openamserver.cisco.com:8443/openam">
    <IDPSSODescriptor WantAuthnRequestsSigned="false"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
                        MIICcTCCAdqgAwIBAgIEWEe4zDANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJJTjESMBAGA1UE
                        CBMJa2FybmF0YWthMRIwEAYDVQQHEwliYW5nYWxvcmUxFjAUBgNVBAoTDWNpc2NvIHN5c3RlbXMx
                        DTALBgNVBAsTBGNjYnUxHzAdBgNVBAMTFm9wZW5hbXNlcnZlci5jaXNjby5jb20wHhcNMTYxMjA3
                        MDcyMjUyWhcNMTgxMjA3MDcyMjUyWjB9MQswCQYDVQQGEwJJTjESMBAGA1UECBMJa2FybmF0YWth
```

Voorbeeld van OpenAM Metadata XML

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://openamserver.cisco.com:8443/openam">
    <IDPSSODescriptor WantAuthnRequestsSigned="false"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
                        MIICcTCCAdqgAwIBAgIEWEe4zDANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJJTjESMBAGA1UE
                        CBMJa2FybmF0YWthMRIwEAYDVQQHEwliYW5nYWxvcmUxFjAUBgNVBAoTDWNpc2NvIHN5c3RlbXMx
                        DTALBgNVBAsTBGNjYnUxHzAdBgNVBAMTFm9wZW5hbXNlcnZlci5jaXNjby5jb20wHhcNMTYxMjA3
                        MDcyMjUyWhcNMTgxMjA3MDcyMjUyWjB9MQswCQYDVQQGEwJJTjESMBAGA1UECBMJa2FybmF0YWth
                        MRIwEAYDVQQHEwliYW5nYWxvcmUxFjAUBgNVBAoTDWNpc2NvIHN5c3RlbXMxDTALBgNVBAsTBGNj
                        YnUxHzAdBgNVBAMTFm9wZW5hbXNlcnZlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
                        MIGJAoGBAKvhLKeu0mA1+V2YdfyuiFKQWXdM6EOc/1fmig94cGdNXxvW13KxzjUF2Vv4r364rTFi
                        73eIduF6e1/M481ECYed24LxKpgcSFMijaBdQl7AeQgyzPnWQCJODf85OguGVQhZUUt0RKKYP/d0
                        bgvarRrwXGIvoURJ+8Wy+zLV0T7nAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAM7MNSup7MOHYCLFl
                        i7hK89EMUIxmeywvAjEa8STH7Ba5d0Z1+R/bnXTS/9/pBETi5knuKd+Q59Pl9je2W7l36vFHoF1Q
                        jLlAGnPJOVEmOtimcGZGCj3m7ThlqnOlICyjnrXcLvQ10m75yfimFeeHdFPGbuzTsXjkIKjmhMF9
                        +cc=
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </KeyDescriptor>
        <ArtifactResolutionService index="0"
            isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/ArtifactResolver/metaAlias/idp1" />
        <SingleLogoutService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://openamserver.cisco.com:8443/openam/IDPSloRedirect/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPSloRedirect/metaAlias/idp1" />
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://openamserver.cisco.com:8443/openam/IDPSloPOST/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPSloPOST/metaAlias/idp1" />
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/IDPSloSoap/metaAlias/idp1" />
        <ManageNameIDService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://openamserver.cisco.com:8443/openam/IDPMniRedirect/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPMniRedirect/metaAlias/idp1" />
        <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://openamserver.cisco.com:8443/openam/IDPMniPOST/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPMniPOST/metaAlias/idp1" />
        <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/IDPMniSoap/metaAlias/idp1" />
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
        </NameIDFormat>
        <SingleSignOnService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://openamserver.cisco.com:8443/openam/SSORedirect/metaAlias/idp1" />
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://openamserver.cisco.com:8443/openam/SSOPOST/metaAlias/idp1" />
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/SSOSoap/metaAlias/idp1" />
        <NameIDMappingService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/NIMSoap/metaAlias/idp1" />
        <AssertionIDRequestService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/AIDReqSoap/IDPRole/metaAlias/idp1" />
        <AssertionIDRequestService Binding="urn:oasis:names:tc:SAML:2.0:bindings:URI"
            Location="https://openamserver.cisco.com:8443/openam/AIDReqUri/IDPRole/metaAlias/idp1" />
    </IDPSSODescriptor>
</EntityDescriptor>
```

Verdere configuratie voor SSO:

Dit document beschrijft de configuratie van het IdP-aspect voor SSO om te integreren met de Cisco Identity Service. Voor meer informatie raadpleegt u de afzonderlijke productconfiguratiehandleidingen:

- UCCX
- UCCE
- PCCE

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.