Installation und Konfiguration des OpenAM Identity Provider (IdP) für Cisco Identity Service (IdS) zur Aktivierung von SSO

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des OpenAM Identity Providers (IdP) zur Aktivierung von Single Sign On (SSO) beschrieben.

Cisco IDs-Bereitstellungsmodelle

Produkt	Bereitstellung
UCCX	Mitansässig
PCCE	Co-Resident mit CUIC (Cisco Unified Intelligence Center) und LD (Live-Daten)
UCCE	Gleichzeitige Implementierung mit CUIC und LD für 2k-Bereitstellungen Standalone für Bereitstellungen der Serien 4000 und 12000.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Contact Center Express (UCCX) Version 11.6 oder Cisco Unified Contact Center Enterprise Version 11.6 bzw. Packaged Contact Center Enterprise (PCCE) Version 11.6

Anmerkung: In diesem Dokument wird die Konfiguration in Bezug auf den Cisco Identification Service (IdS) und den Identity Provider (IdP) beschrieben. In den Screenshots und Beispielen wird auf UCCX verwiesen. Die Konfiguration ist jedoch in Bezug auf den Cisco Identification Service (UCCX/UCCE/PCCE) und die IdP ähnlich.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Install

Anmerkung: Dieses Dokument bezieht sich im Rahmen der Qualifizierung mit SSO auf OpenAM Release 10.0.1

Systemanforderungen

Betriebssysteme	Java-Umgebung	Anforderungen an den	Unterstützte	Anfor

		Webanwendungscontainer	Browser	den D
• Microsoft Windows Server 2003, 2008 R2 • Linux 2.6, 3.0 • Oracle Solaris 10	Version 10.0.1 von OpenAM erfordert Java Development Kit 1.6, mindestens 1.6.0_10. ForgeRock empfiehlt aufgrund von Sicherheitskorrekturen, mindestens Version 1.6.0_27 zu verwenden. ForgeRock hat diese Version von OpenAM hauptsächlich mit Oracle Java SE JDK getestet. OpenAM Java SDK unterstützt Java Development Kit 1.5 oder 1.6.	• Apache Tomcat 6.0.x, 7.0.x • GlassFish v2 • JBoss Enterprise Application Platform 4.x, 5.x • JBoss-Anwendungsserver 7.x • Jetty 7 • Oracle WebLogic Server 11g • Oracle WebLogic Server 12c Wenn Sie als Nicht-Root-Benutzer ausgeführt werden, muss der Webanwendungscontainer in der Lage sein, in sein eigenes Stammverzeichnis zu schreiben, in dem OpenAM Konfigurationsdateien speichert.	• Chrom und Chrom 16 und höher • Firefox 3.6 und höher • Internet Explorer (Version 7 und höher) • Safari 5 und höher	• Fo O • M D • IB V • O • O S E

Install

OpenAM-Software beziehen

- Laden Sie die OpenAM 10.0.1-Versionen unter https://backstage.forgerock.com/downloads/OpenAM/OpenAM%20Enterprise/10.0.1/OpenAM%201 herunter.
- Für jede Version der OpenAM-Kerndienste können Sie das gesamte Paket als ZIP-Archiv herunterladen, nur die OpenAM-Datei .war, nur die Verwaltungstools als ZIP-Archiv
- Nachdem Sie das Archiv des gesamten Pakets entpackt haben, erhalten Sie ein OpenSso-Verzeichnis mit einer README, einer Reihe von Lizenzdateien und den Verzeichnissen

Voraussetzungen

Stellen Sie vor der Installation sicher, dass Sie über die erforderliche erforderliche Software für die OpenAM-Kernservices verfügen.

- Eine Java 6-Laufzeitumgebung

- Apache Tomcat als Webanwendungscontainer installieren
- OpenAM-Core-Services erfordern eine Java Virtual Memory (JVM)-Heap-Größe von mindestens 1 GB und eine permanente Generationsgröße von 256 MB. Wenden Sie die JVM-Optionen an, wenn Sie JAVA_OPTS vor dem Start des Tomcat-Anwendungsservers in der Catalina-Datei festlegen - -Xmx1024m -XX:MaxPermSize=256m

Zum Beispiel Set JAVA_OPTS=%JAVA_OPTS% -xmx1024m -XX:MaxPermSize=256m -Xms512m

- Installieren Sie Microsoft Active Directory als Datenspeicher mit wenigen Benutzern.

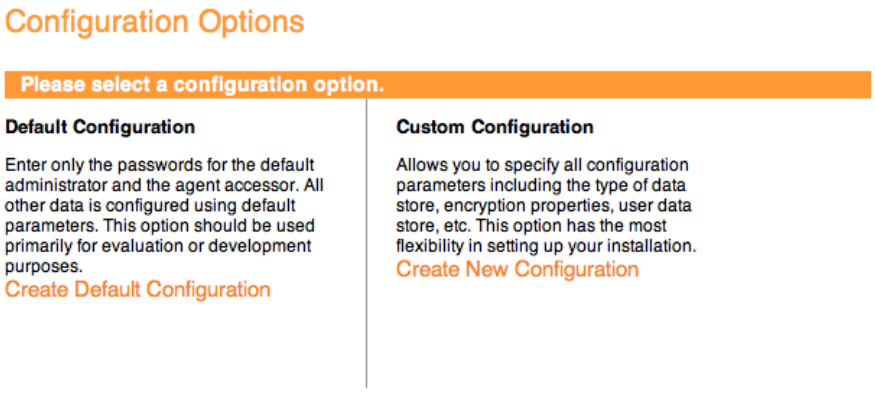
Installieren der OpenAM-Webanwendung

Die Datei deployable-war/opensso.war enthält alle OpenAM-Serverkomponenten und Beispiele im OpenAM-Verzeichnis.

Bereitstellen von OpenAM auf Tomcat Container

Kopieren Sie die Datei opensso.war in das Verzeichnis, in dem die Tomcat-Webanwendungen gespeichert sind. Benennen Sie die Datei opensso.war in openam.war um. Starten Sie den Tomcat-Dienst neu.

Überprüfen Sie den Bildschirm für die Erstkonfiguration in Ihrem Browser unter http://<FQHN>:8080/openam.



OpenAM-Dienst ausführen

Openam ist eine einfache Web-Anwendung, die auf einem Tomcat-Server gehostet wird. Starten Sie einfach Ihren Tomcat-Server und können Sie so auf den OpenAM-Webdienst zugreifen.

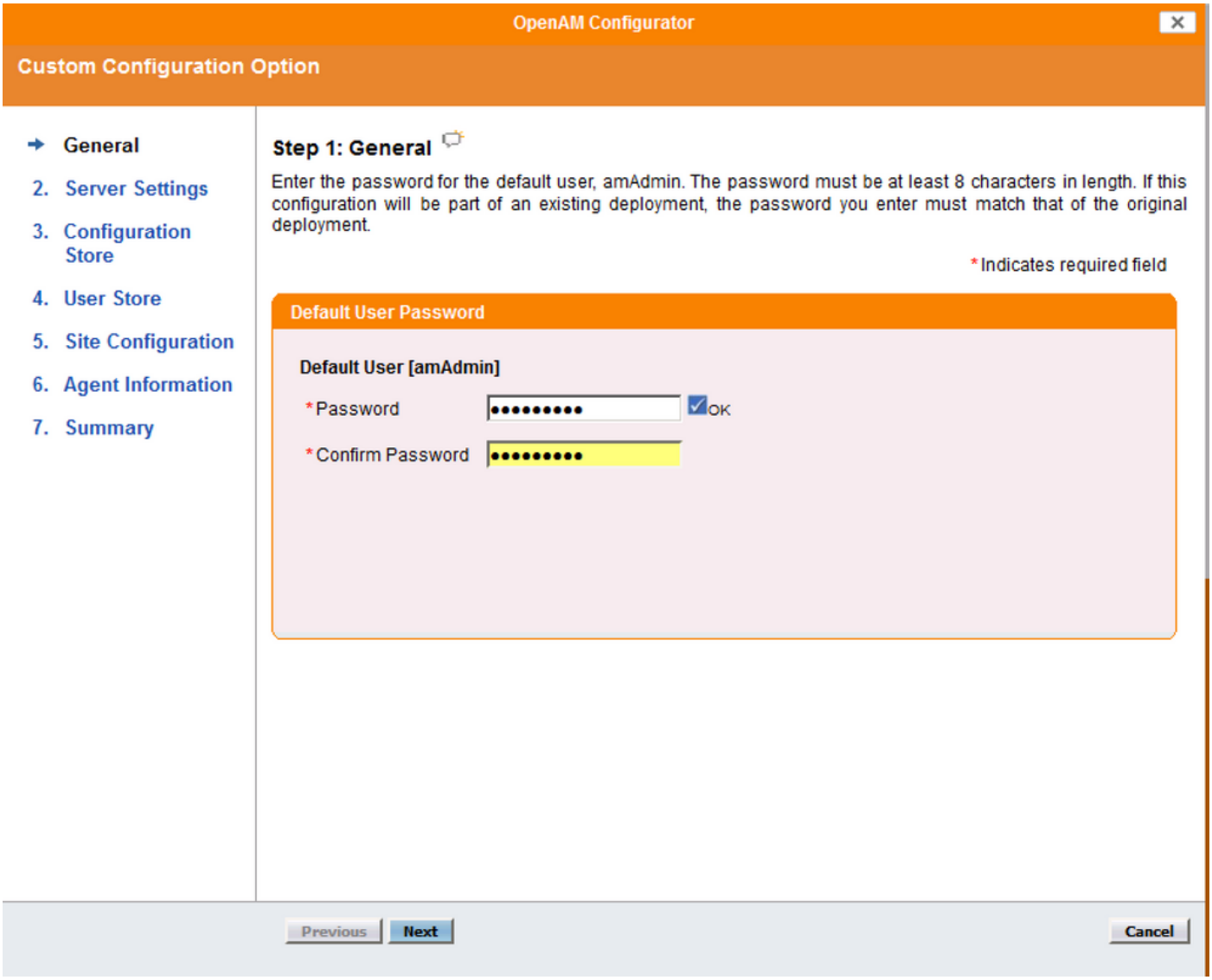
Konfigurieren

OpenAM-Konfigurator

Der benutzerdefinierte OpenAM-Konfigurationsprozess ermöglicht das einfache Festlegen einer Vielzahl gängiger Konfigurationsoptionen. So werden Konfigurationsschritte, die später erforderlich sind, vor der Konfiguration mit größerem Aufwand eingespart.

Allgemeine Einstellungen

Klicken Sie auf die Option Create New Configuration (Neue Konfiguration erstellen), und wählen Sie das Kennwort für das Standardadministratorkonto (amAdmin) aus. Das Kennwort muss mindestens 8 Zeichen lang sein.

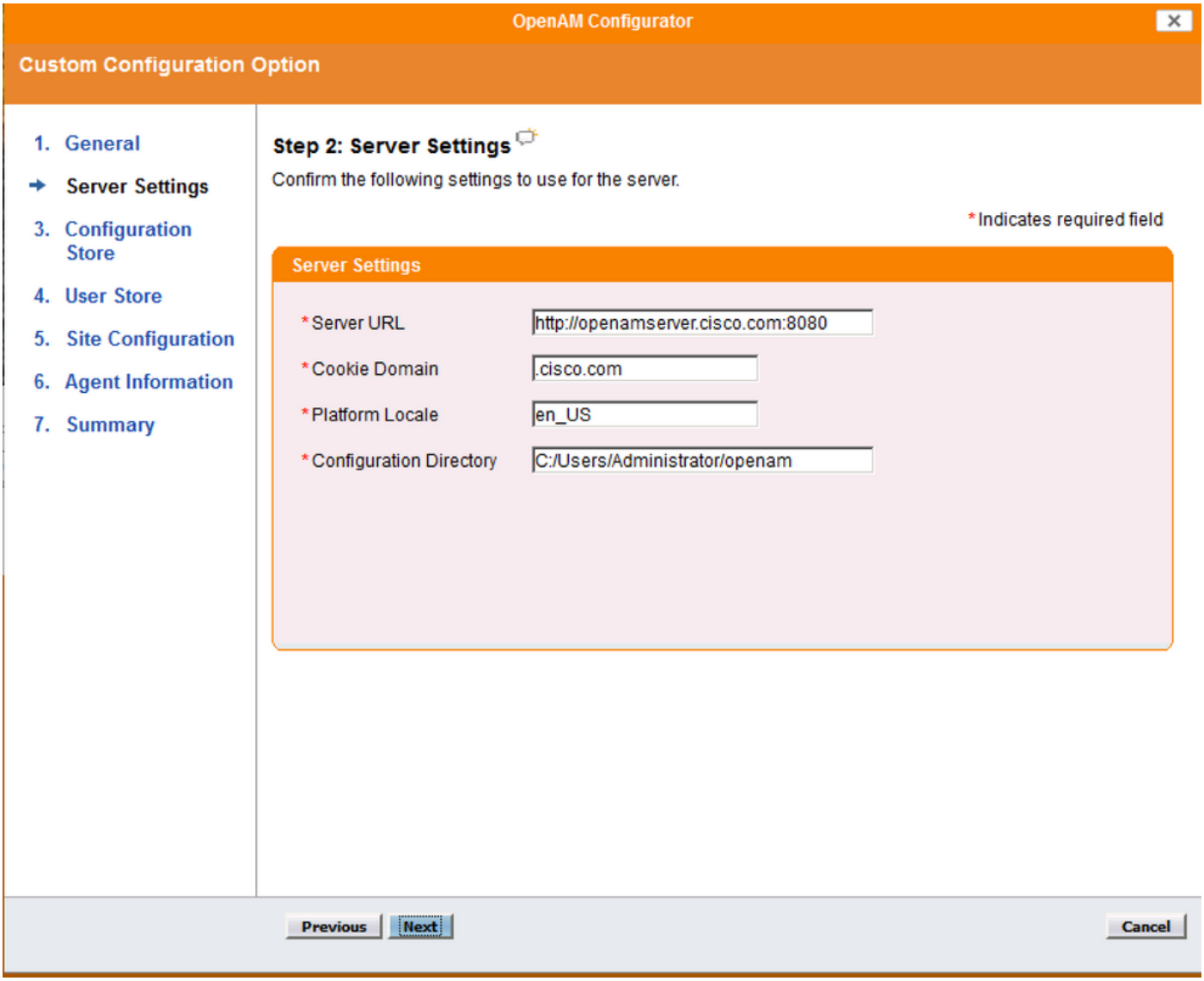


Nach zweimaliger Eingabe eines gültigen Kennworts wird die nächste Schaltfläche angezeigt, und die Konfiguration kann fortgesetzt werden.

Servereinstellungen

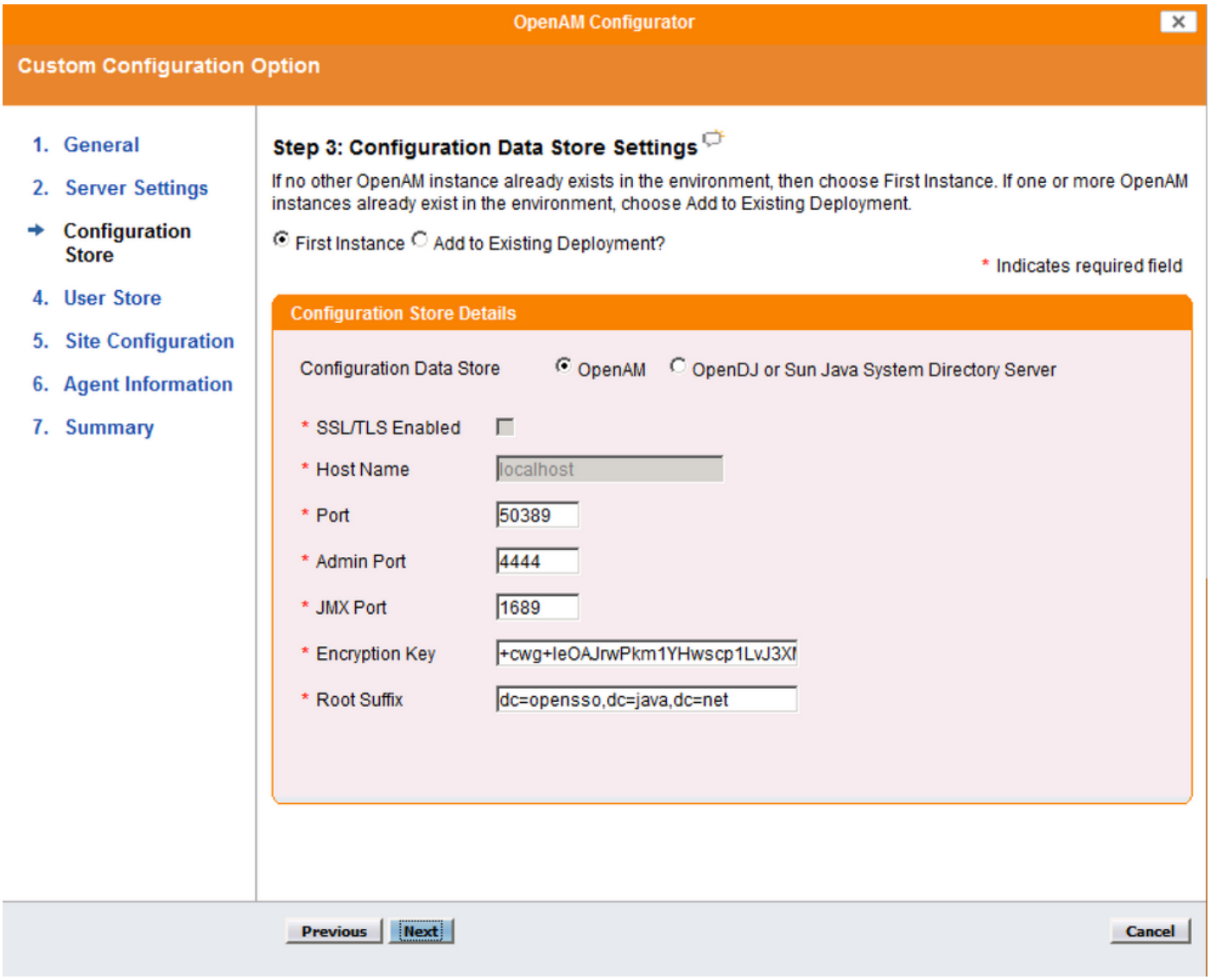
Standardmäßig ist die Server-URL der vollqualifizierte Domänenname des Servers.

Anmerkung: Es ist wichtig, dass der Benutzer, der Apache Tomcat ausführt, Schreibzugriff auf das Konfigurationsverzeichnis hat. Daher ist ~/openam/config für diesen Zweck geeignet. Unterstützte Plattform-Gebietsschemas sind en_US (Englisch), de (Deutsch), es (Spanisch), fr (Französisch), ja (Japanisch), zh_CN (Vereinfachtes Chinesisch) oder zh_TW (Traditionelles Chinesisch).



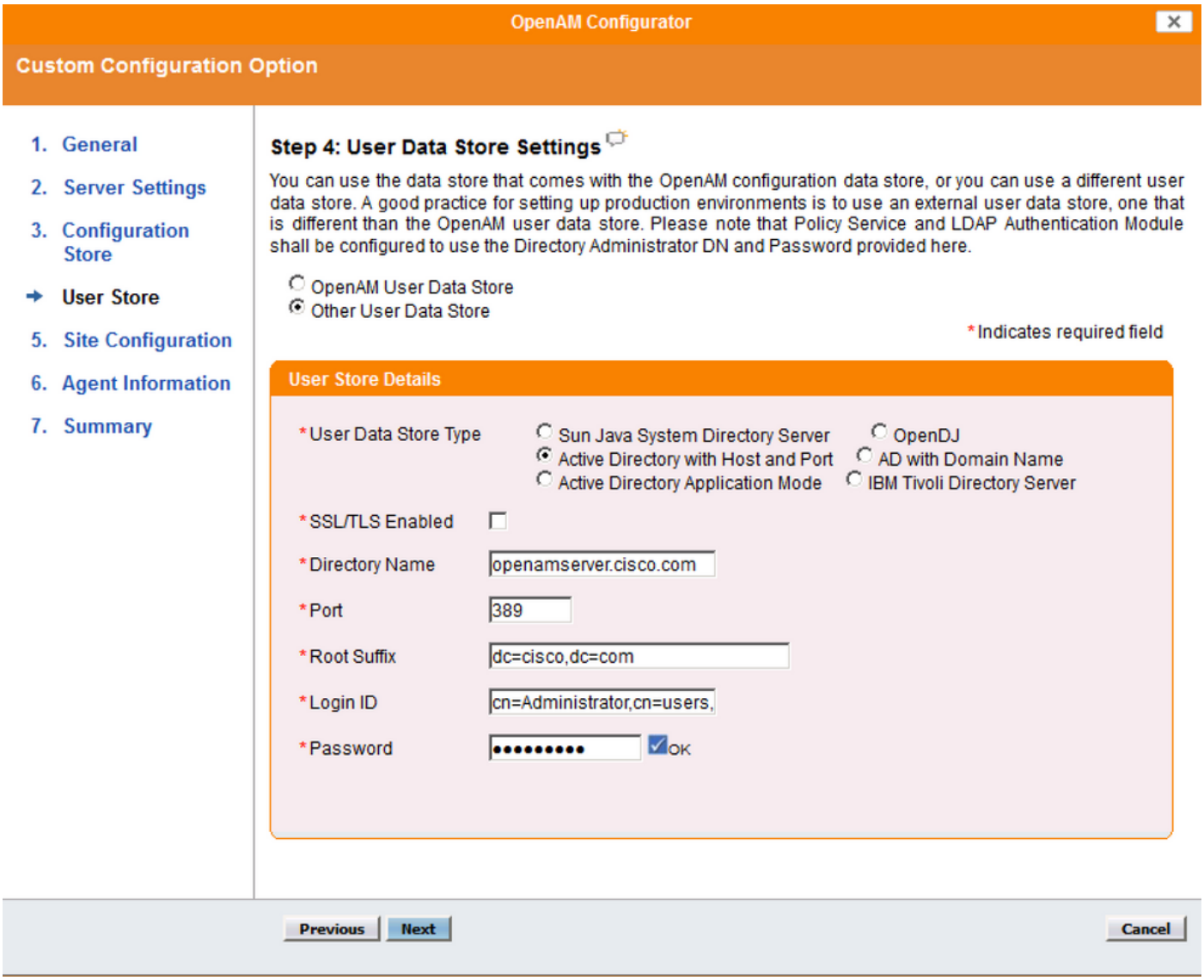
Einstellungen für den Konfigurationsdatenspeicher

Bei Einzelserverkonfigurationen müssen diese Einstellungen nicht geändert werden.



Einstellungen für den Benutzerdatenspeicher

Die Benutzerdatenspeichereinstellungen verbinden OpenAM mit dem Microsoft Active Directory-Datenspeicher.

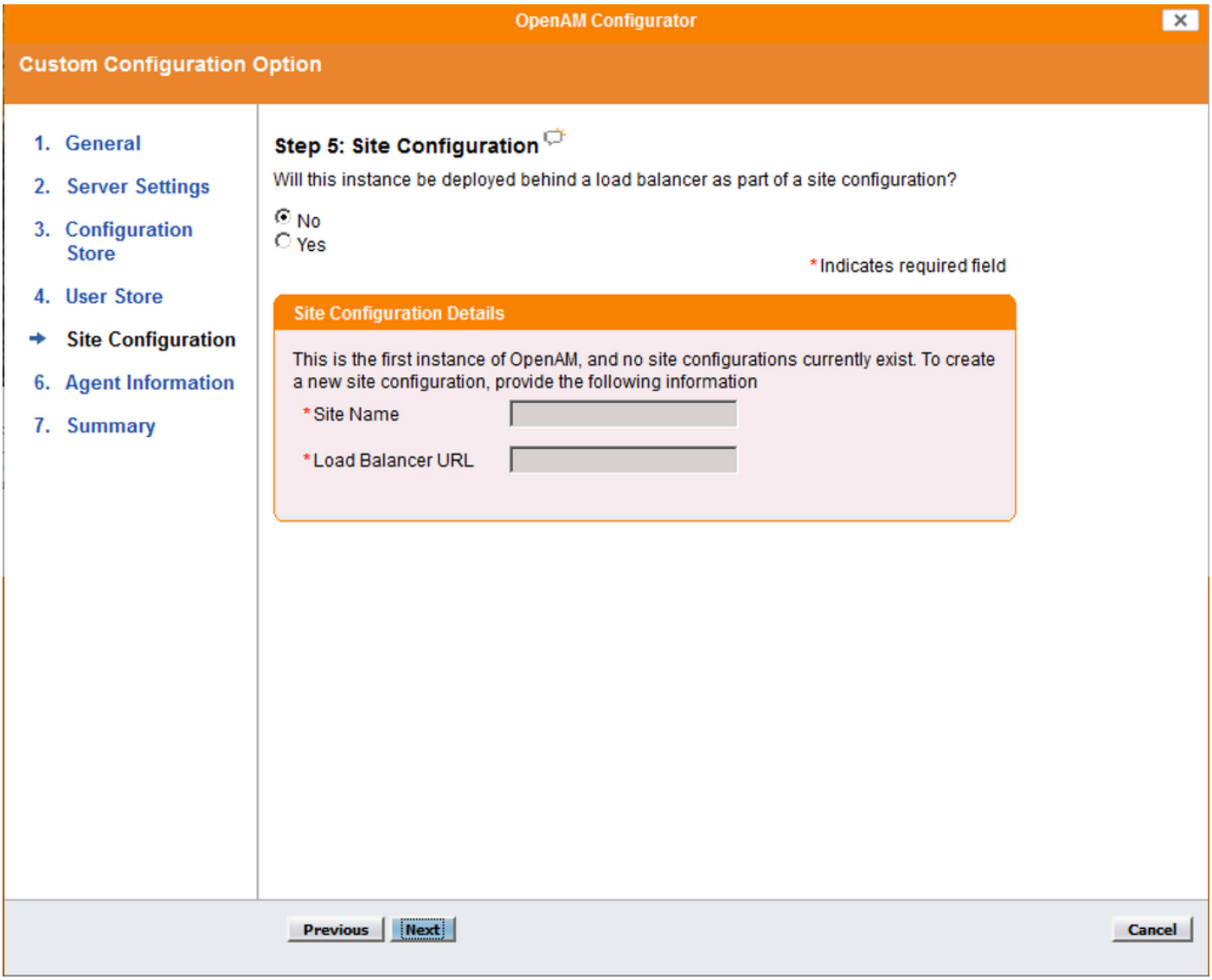


- Benutzerdatenspeichertyp: Active Directory mit Host und Port
- SSL/TLS aktiviert: Nicht aktiviert
- Verzeichnisname: <Domänenname des AD-Servers>
- Anschluss: 389
- Stammsuffix: dc=cisco,dc=com
- Anmelde-ID: cn=<AD-Benutzername>,cn=users,dc=cisco,dc=com
- Kennwort: <AD-Benutzerkennwort>

Anmerkung: Der Konfigurator stellt erst dann eine Option zum Fortfahren bereit, wenn alle Einstellungen korrekt angegeben wurden und eine Verbindung zur Active Directory-Instanz hergestellt wurde.

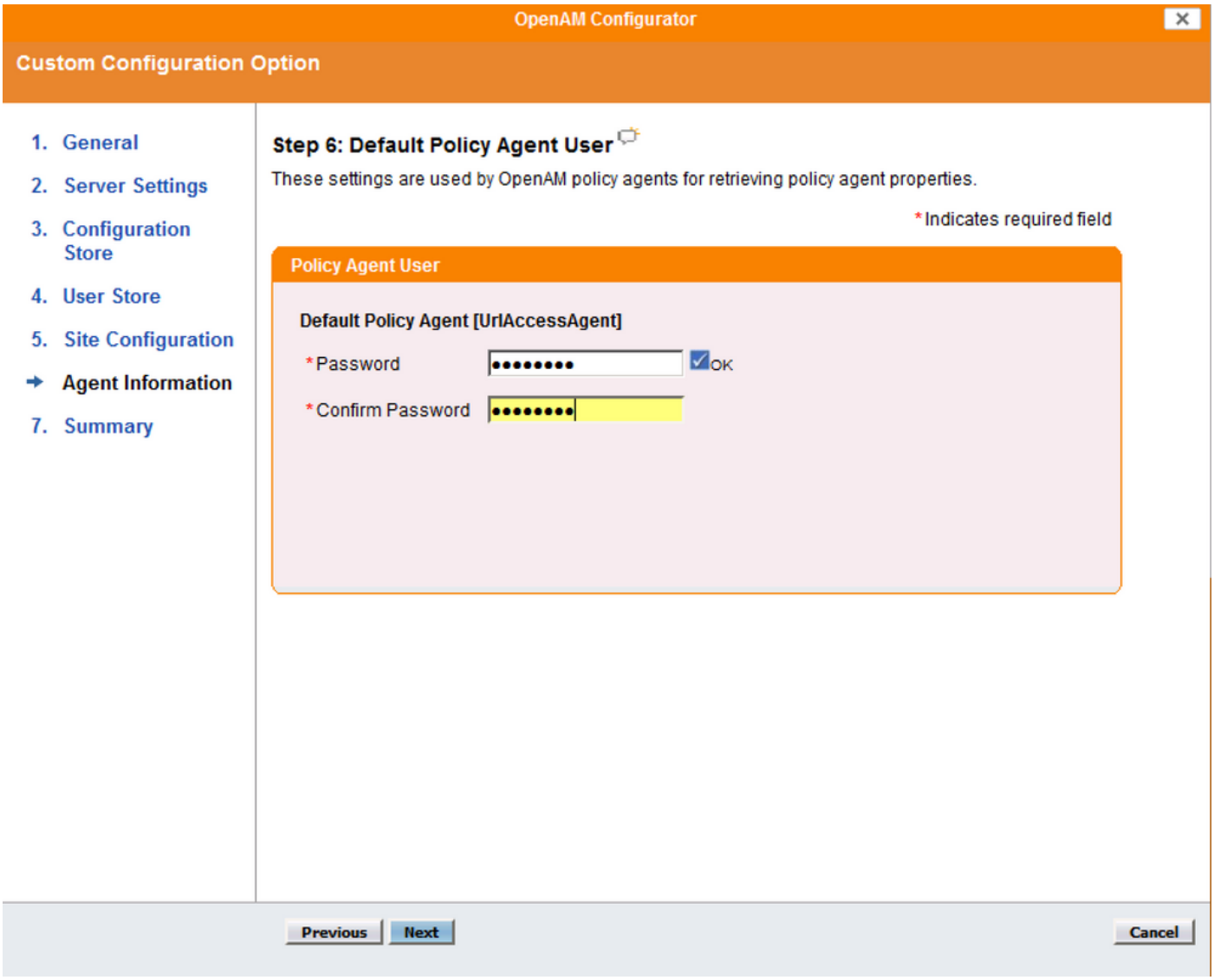
Standortkonfiguration

Im Bildschirm "Site Configuration" können Sie OpenAM als Teil eines Standorts einrichten, bei dem die Last auf mehrere OpenAM-Server verteilt wird. Akzeptieren Sie für die erste OpenAM-Installation die Standardeinstellungen.



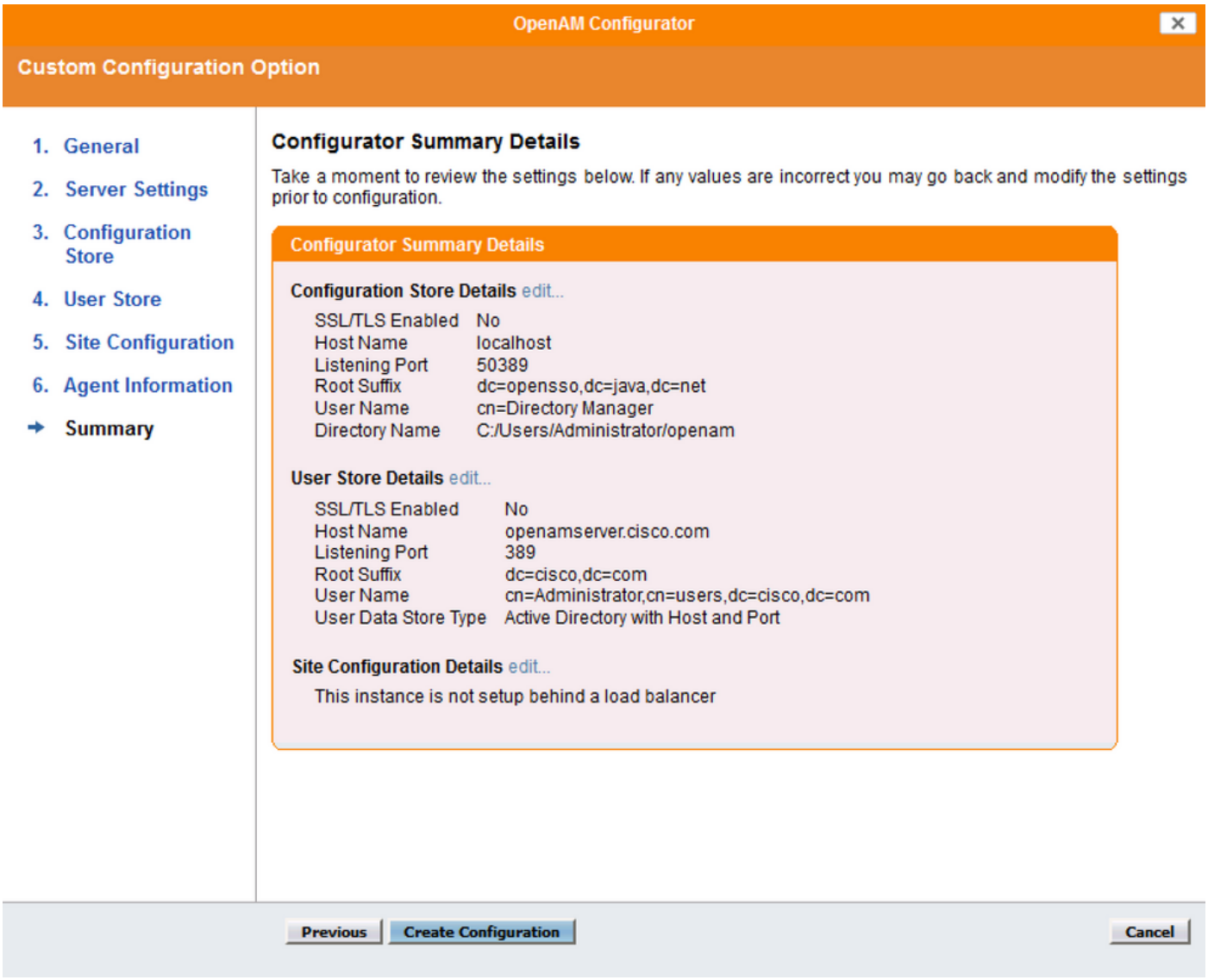
Agenteninformationen

Geben Sie im Bildschirm Agent Information (Agenteninformationen) ein Kennwort von mindestens 8 Zeichen an, das von Richtlinien-Agents verwendet werden soll, um eine Verbindung mit OpenAM herzustellen.



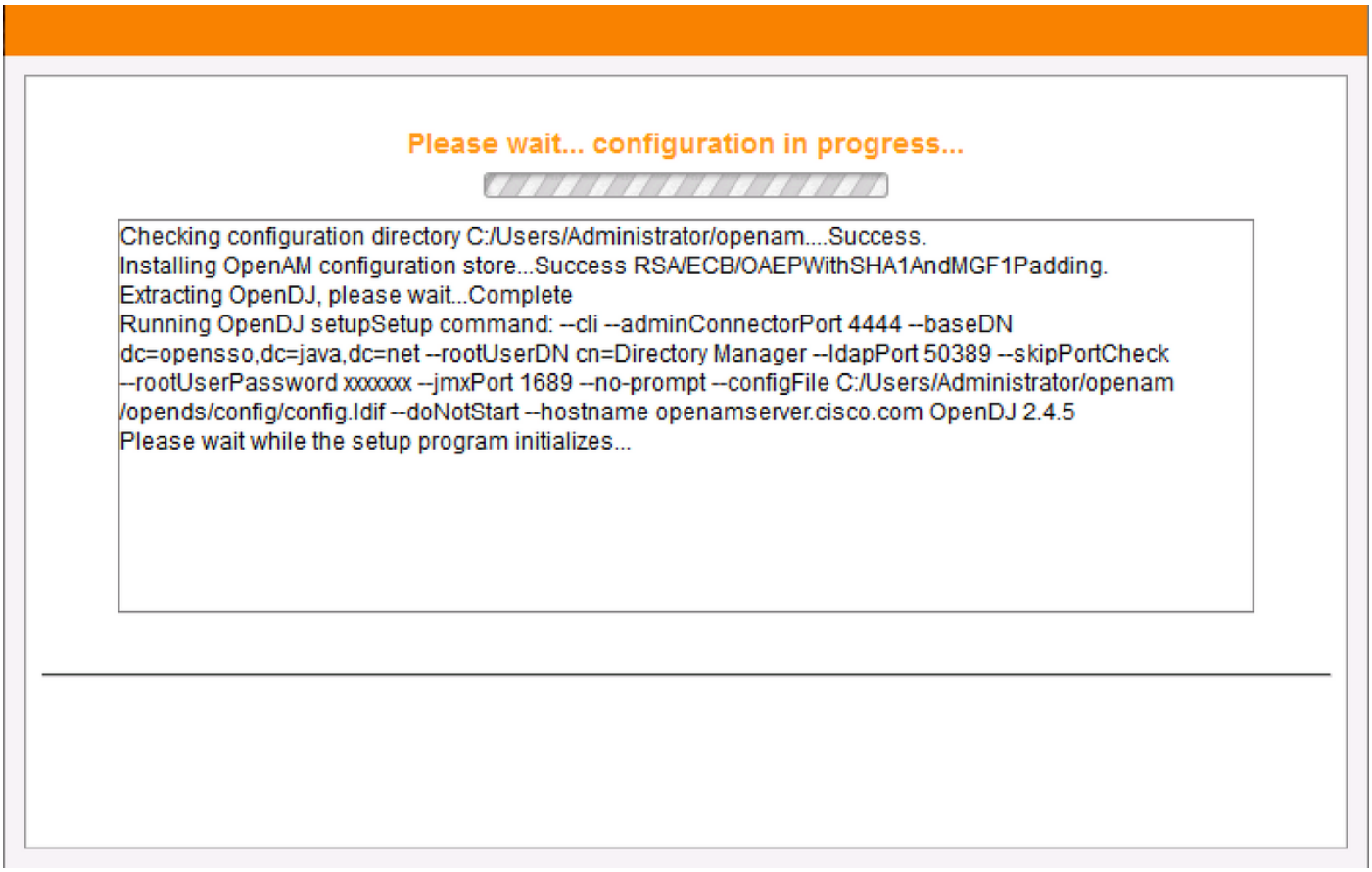
Zusammenfassung

Überprüfen Sie die Informationen, und klicken Sie auf Konfiguration erstellen.

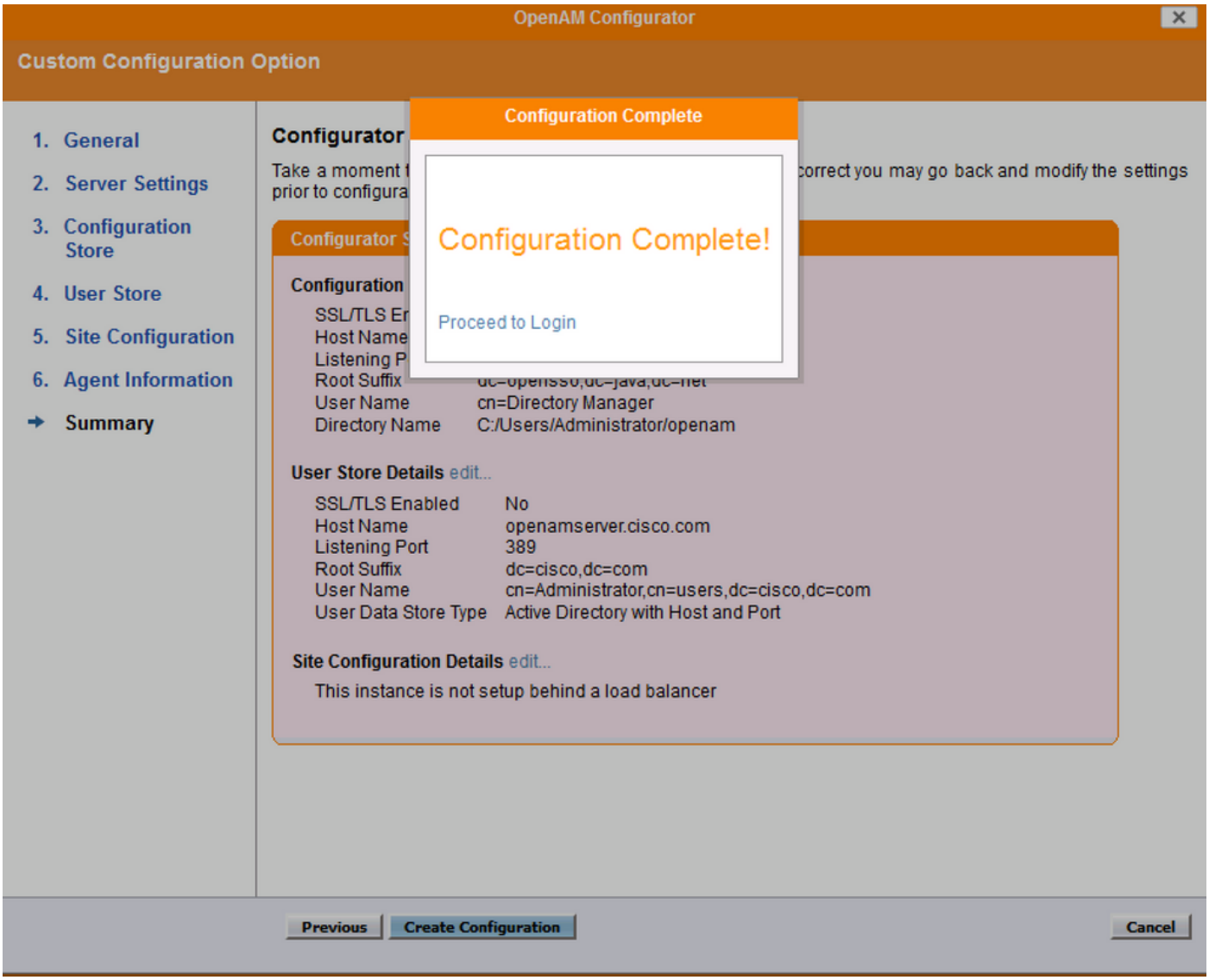


Konfigurationsfortschritt

Der Bildschirm "Configuration Progress" (Konfigurationsfortschritt) zeigt den Fortschritt der Installation an. Die gesamte Ausgabe auf diesem Bildschirm und alle Fehler werden in die Datei geschrieben: ~/openam/config/install.log.

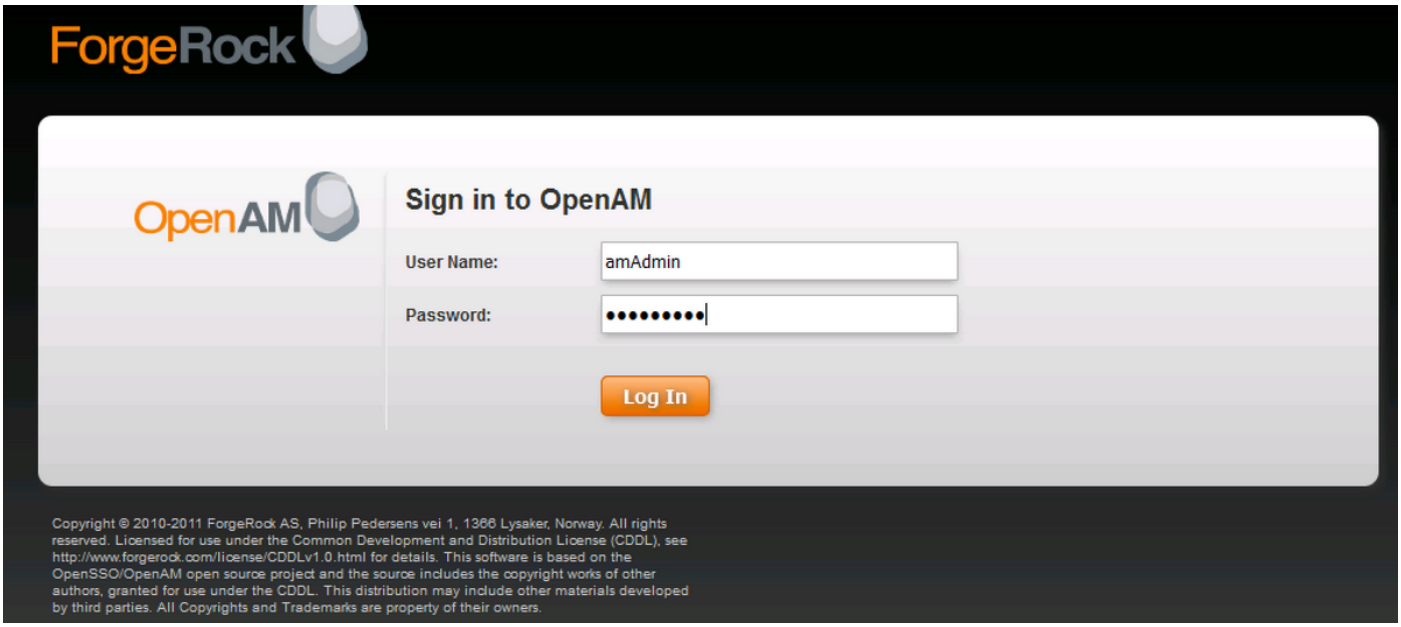


Konfiguration abgeschlossen



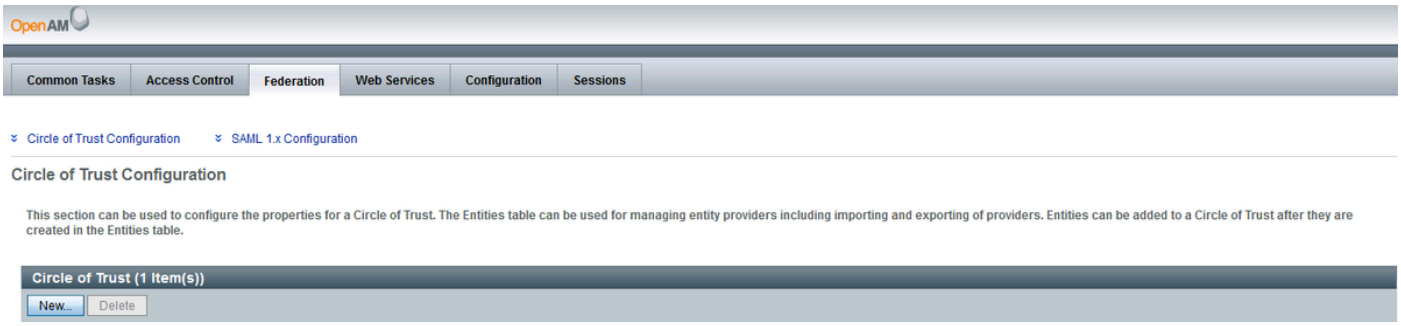
Konfigurieren von OpenAM als IdP

- Klicken Sie auf Proceed to Login (Anmelden) oder Access via URL http://<FQDN of OpenAM>:8080/openam, und melden Sie sich dann als OpenAM-Administrator an.
- Wenn Sie zum ersten Mal auf OpenSSO Enterprise zugreifen, werden Sie zum Konfigurator geleitet, um die Erstkonfiguration von OpenSSO Enterprise durchzuführen
- Standardkonfiguration auswählen
- Sie müssen die Kennwörter für OpenAMserver konfigurieren.
- Konfigurieren Sie die Kennwörter, und melden Sie sich bei der Benutzeroberfläche des OpemAM-Servers an.

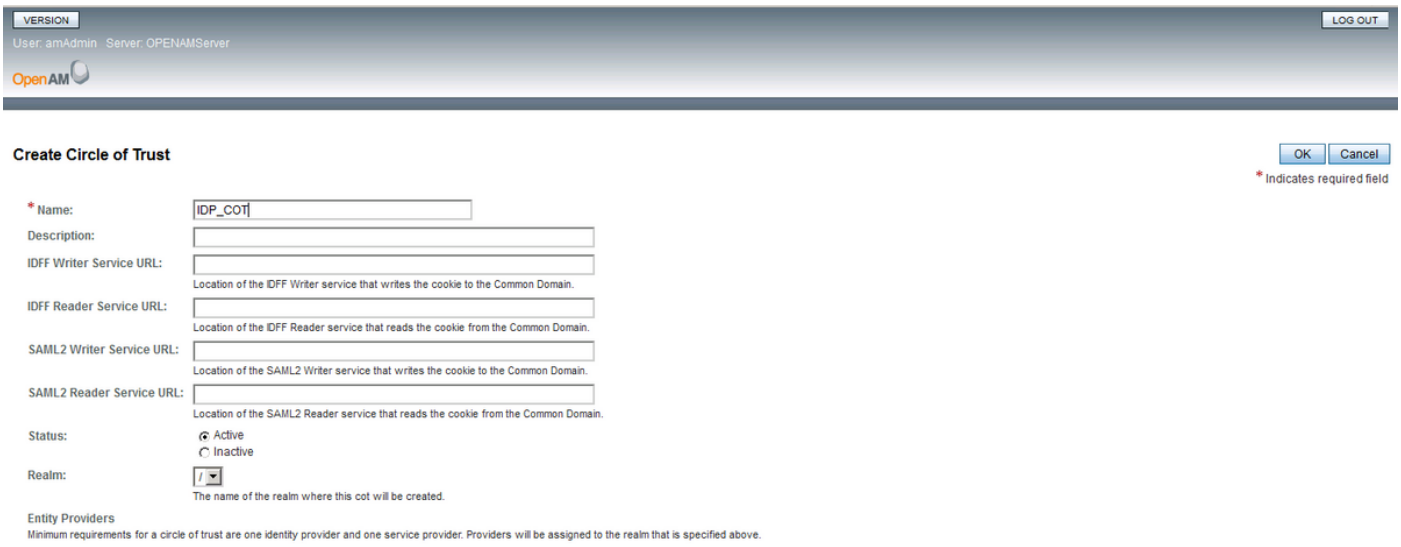


Kreis der Vertrauenskonfiguration

Navigieren Sie zur Registerkarte "Federation", und klicken Sie im Abschnitt "Circle of Trust" auf die Schaltfläche "New".



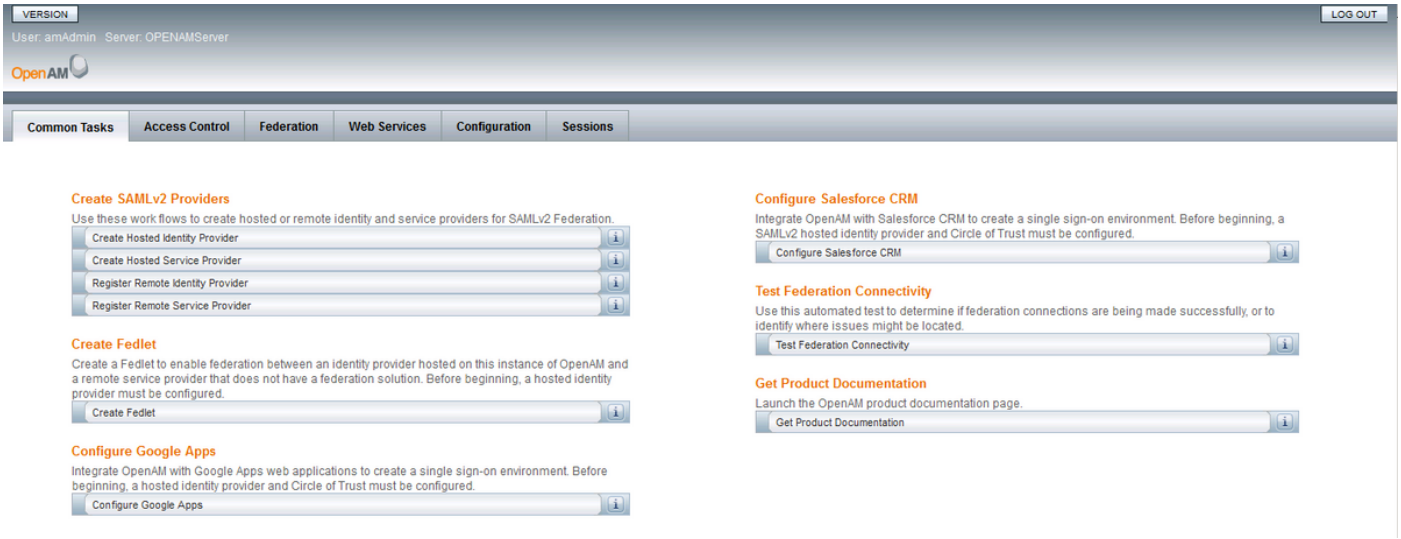
Erstellen Sie einen Vertrauenskreis mit einem eindeutigen Namen für den IdP-Vertrauenskreis, und klicken Sie auf OK.



Anmerkung: Damit SAML SSO funktioniert, müssen sich Service Provider und IdP im selben Circle of Trust (CoT) befinden.

Hosted Identity Provider erstellen

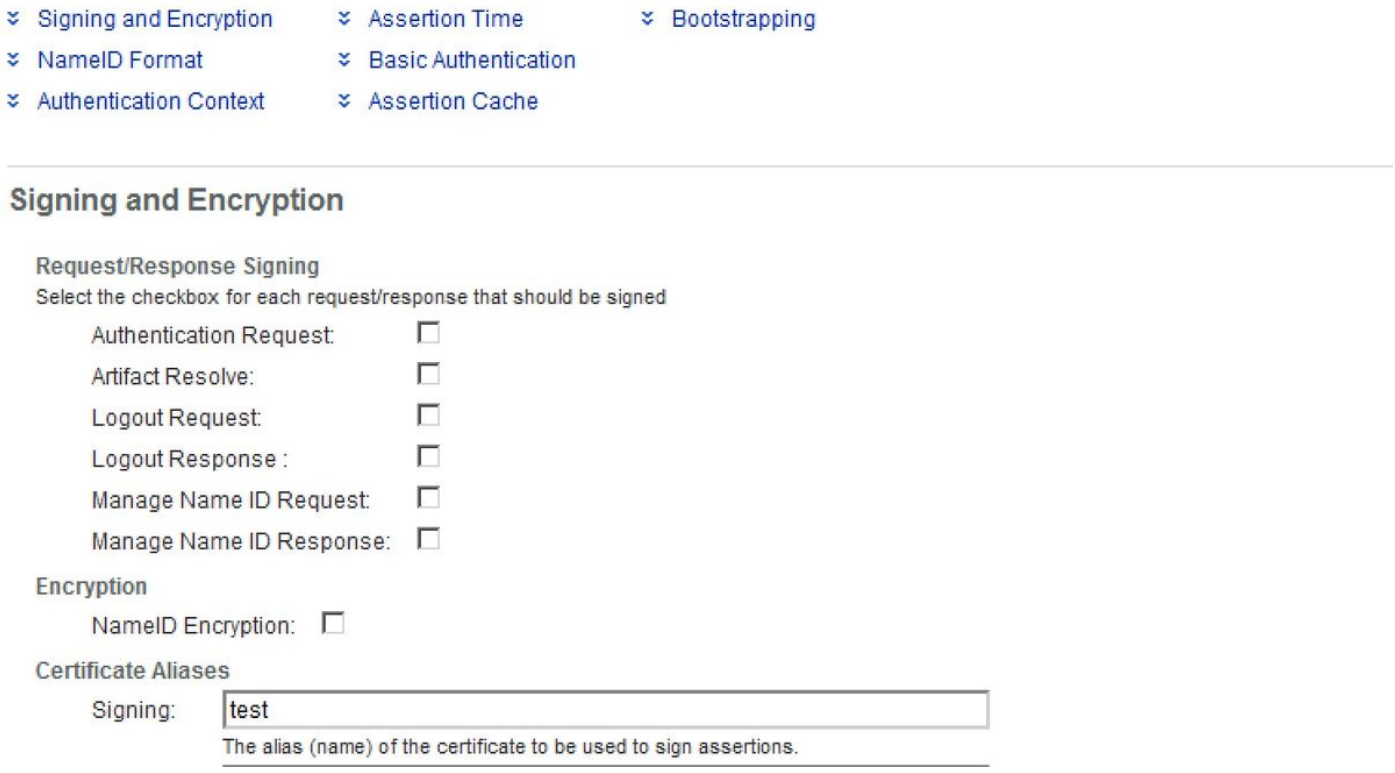
Navigieren Sie zur Registerkarte Allgemeine Aufgaben, und klicken Sie auf Gehosteten Identitätsanbieter erstellen, und erstellen Sie eine gehostete ID (belassen Sie die konfigurierten Standardwerte, und speichern Sie die Einstellungen).



Der zuvor erstellte Vertrauenskreis wird aufgeführt.

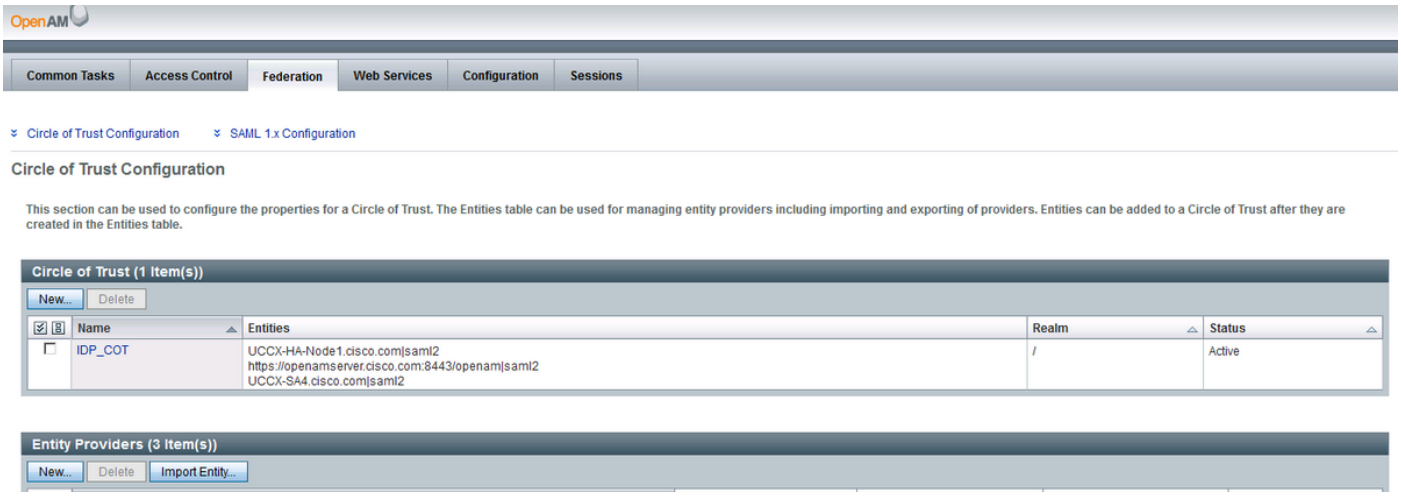
Signaturschlüssel konfigurieren

Navigieren Sie zur Registerkarte Verbund und klicken Sie im Abschnitt "Entitätsanbieter" auf den Anbieter der gehosteten Identität. Navigieren Sie zum Abschnitt Assertion Content, und konfigurieren Sie den Wert des Signaturfelds unter Certificate Aliases als Test. Dies ist das Zertifikat, das zum Signieren der SAML-Assertion verwendet wird.

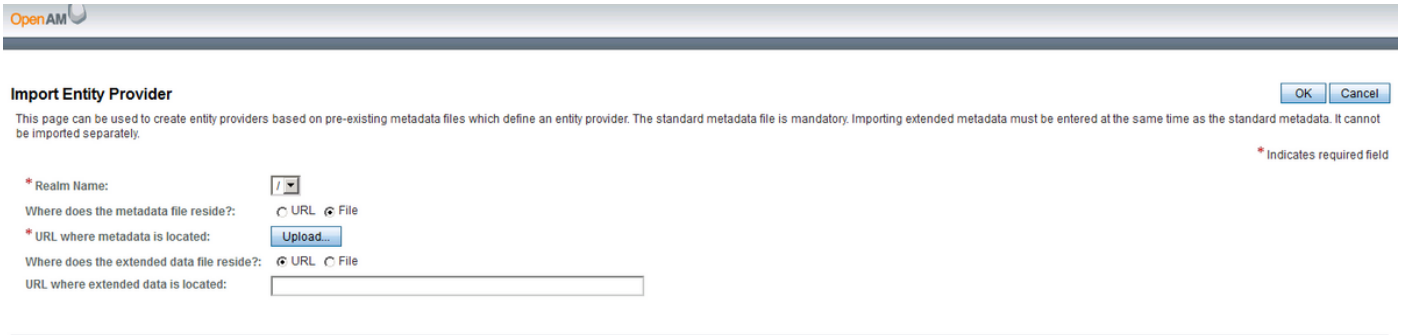


Entität des Dienstanbieters importieren

Navigieren Sie zur Registerkarte "Verbund", und klicken Sie im Abschnitt "Entitätsanbieter" auf die Schaltfläche Entität importieren.

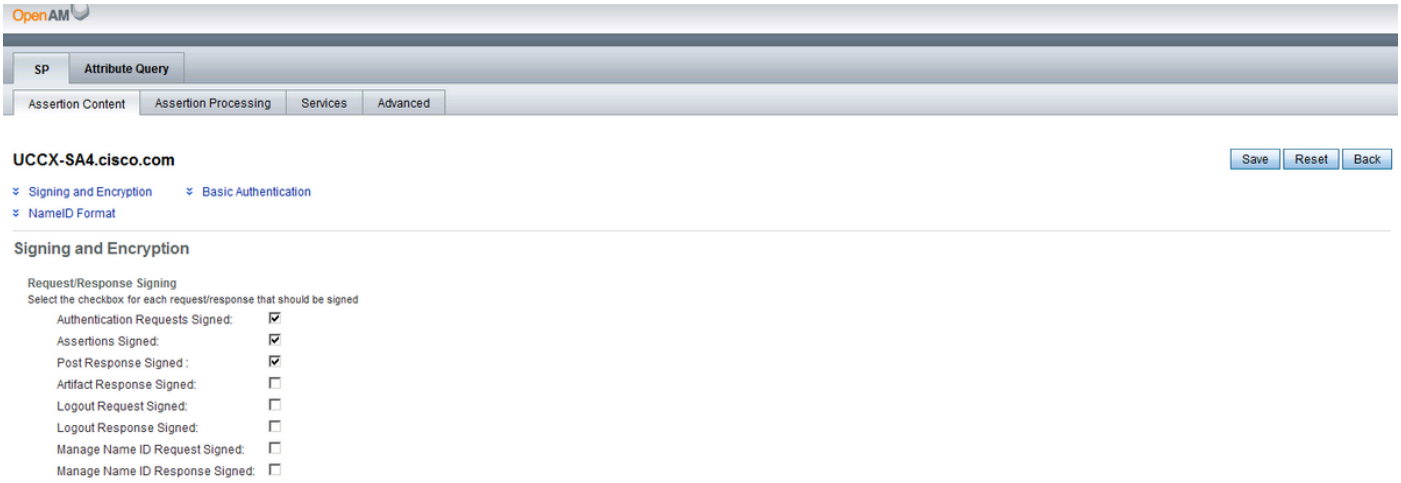


Laden Sie die Entitätsdatei (sp.xml) des Dienstanbieters hoch, und speichern Sie die Seite.



Signieren von Anfragen/Antworten

Klicken Sie auf die importierte Entität, und aktivieren Sie die Signatur für Anforderung/Antwort.



Attributzuordnung

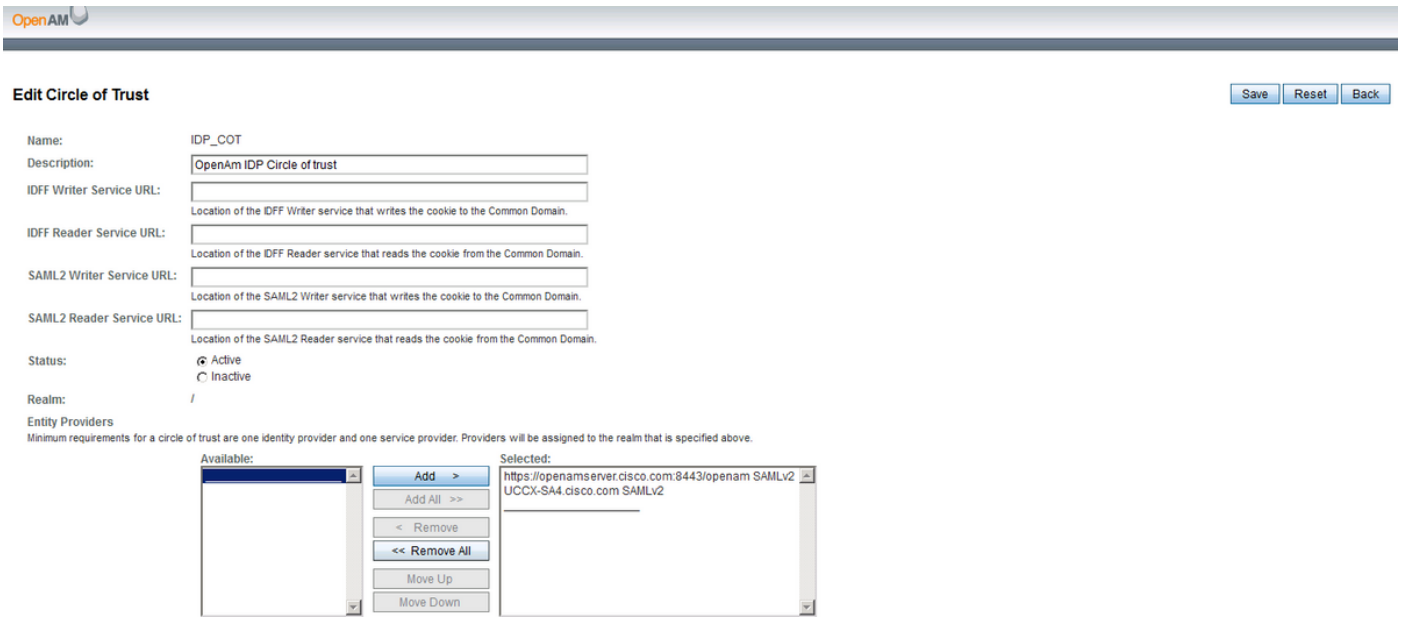
Navigieren Sie zu Assertion Processing, und fügen Sie ein Zuordnungsattribut für uid und user_principale gemäß den Directory- und OpenAM-Einstellungen hinzu. Klicken Sie auf Speichern.

Hinweis: Sowohl die Attribute uid als auch user_principale sind obligatorisch, da der Service Provider (SP) mithilfe dieser Attribute die Identität eines authentifizierten Benutzers identifiziert. Stellen Sie außerdem sicher, dass die Attribute sAMAccountName und userPrincipalName auch im Attribut-Editor der Active Directory-Benutzereigenschaften zugeordnet sind.

Kreis des Vertrauens bearbeiten

Navigieren Sie zur Registerkarte Federation, und klicken Sie auf Circle of Trust (Vertrauenswürdiger Kreis) hinzugefügt, und stellen Sie sicher, dass Sie die IdP-(OpenAm-Server)

und die Service Provider-Entität im Abschnitt Entity Providers aus den Abschnitten Available in Selected (Verfügbar) verschieben. Damit gehören IdP und Service Provider demselben Vertrauenskreis an.



OpenAM IdP-Metadaten herunterladen

Sie können die IdPmetadatafile des OpenAM-Servers unter folgender URL herunterladen: [http://<FQDN of OpenAM>:8080/openam/saml2/jsp/exportmetadata.jsp?entityid=http://<FQDN of 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
```

Beispiel für OpenAM-Metadaten-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>
```

Weitere Konfiguration für SSO:

In diesem Dokument wird die IdP-Konfiguration für SSO zur Integration in den Cisco Identity Service beschrieben. Weitere Informationen finden Sie in den jeweiligen Produktkonfigurationsanleitungen:

- UCCX
- UCCE
- PCCE

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.