

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

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Install](#)

[Systemanforderungen](#)

[Betriebssysteme](#)

[Java-Umgebung](#)

[Anforderungen an den Webanwendungscontainer](#)

[Unterstützte Browser](#)

[Anforderungen an den Datenspeicher](#)

[Hardware-Mindestanforderungen](#)

[Install](#)

[OpenAM-Software beziehen](#)

[Voraussetzungen](#)

[Installieren der OpenAM-Webanwendung](#)

[OpenAM-Dienst ausführen](#)

[Konfigurieren](#)

[OpenAM-Konfigurator](#)

[Konfigurieren von OpenAM als IdP](#)

[Kreis der Vertrauenskonfiguration](#)

[Hosted Identity Provider erstellen](#)

[Signatur Schlüssel konfigurieren](#)

[Entität des Diensteanbieters importieren](#)

[Signieren von Anfragen/Antworten](#)

[Attributzuordnung](#)

[Kreis des Vertrauens bearbeiten](#)

[OpenAM IdP-Metadaten herunterladen](#)

[Weitere Konfiguration für SSO:](#)

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
<ul style="list-style-type: none"> • Microsoft Windows Server 2003, 2008 R2 • Linux 2.6, 3.0 • Oracle Solaris 10 	<p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> • 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 <p>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.</p>	<ul style="list-style-type: none"> • Chrom und Chrom 16 und höher • Firefox 3.6 und höher • Internet Explorer (Version 7 und höher) • Safari 5 und höher 	<ul style="list-style-type: none"> • F • 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%2010.0.1.zip> 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>.



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-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.

The screenshot shows the 'OpenAM Configurator' window with the 'Custom Configuration Option' dialog. The 'General' step is active, requiring the user to enter a password for the default user 'amAdmin'. The password must be at least 8 characters long. The dialog includes a sidebar with navigation options and a main area with two password input fields: 'Password' and 'Confirm Password', both marked as required. A 'Next' button is visible at the bottom.

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).

The screenshot shows the 'OpenAM Configurator' window with the 'Custom Configuration Option' selected. The 'Server Settings' step is active, showing a list of required fields for server configuration. The fields are: Server URL (http://openamserver.cisco.com:8080), Cookie Domain (.cisco.com), Platform Locale (en_US), and Configuration Directory (C:/Users/Administrator/openam). The 'Next' button is highlighted, indicating the user can proceed to the next step.

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

Einstellungen für den Konfigurationsdatenspeicher

Bei Einzelserverkonfigurationen müssen diese Einstellungen nicht geändert werden.

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

Einstellungen für den Benutzerdatenspeicher

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

✕
OpenAM Configurator

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
 OpenDJ
 AD with Domain Name
 IBM Tivoli Directory Server
 Active Directory Application Mode

* SSL/TLS Enabled

* Directory Name

* Port

* Root Suffix

* Login ID

* Password OK

Previous
Next
Cancel

- 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.

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

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.

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

Zusammenfassung

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

OpenAM Configurator ✕

Custom Configuration Option

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

Configurator Summary Details

Take a moment to review the settings below. If any values are incorrect you may go back and modify the settings prior to configuration.

Configurator Summary Details

Configuration Store Details [edit...](#)

SSL/TLS Enabled	No
Host Name	localhost
Listening Port	50389
Root Suffix	dc=opensso,dc=java,dc=net
User Name	cn=Directory Manager
Directory Name	C:/Users/Administrator/openam

User Store Details [edit...](#)

SSL/TLS Enabled	No
Host Name	openamserver.cisco.com
Listening Port	389
Root Suffix	dc=cisco,dc=com
User Name	cn=Administrator,cn=users,dc=cisco,dc=com
User Data Store Type	Active Directory with Host and Port

Site Configuration Details [edit...](#)

This instance is not setup behind a load balancer

Previous Create Configuration Cancel

Konfigurationsfortschritt

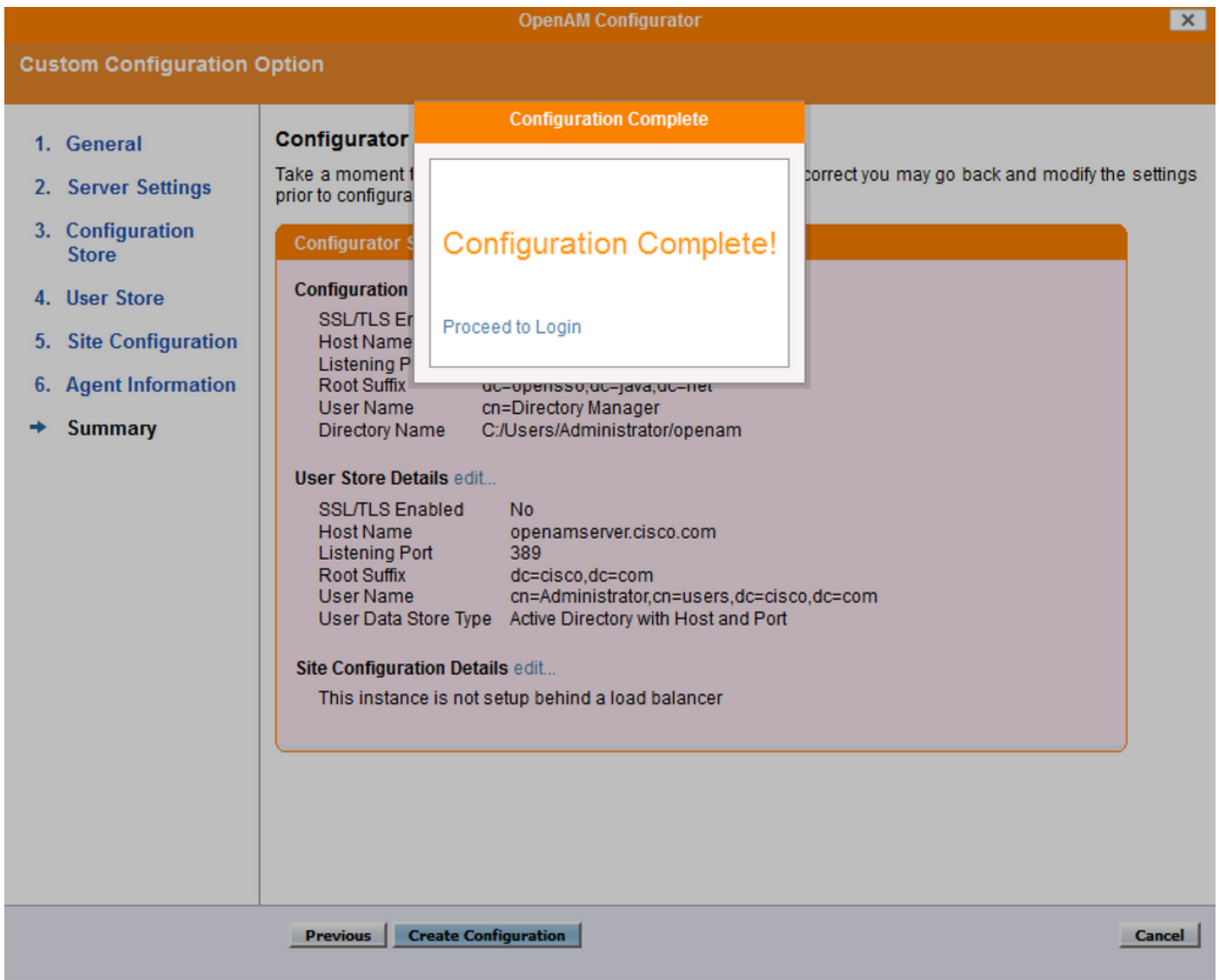
Der Bildschirm "Configuration Progress" (Konfigurationsfortschritt) zeigt den Fortschritt der Installation an. Die gesamte Ausgabe auf diesem Bildschirm und alle Fehler werden in die Datei geschrieben: `~/openam/config/install.log`.

Please wait... configuration in progress...



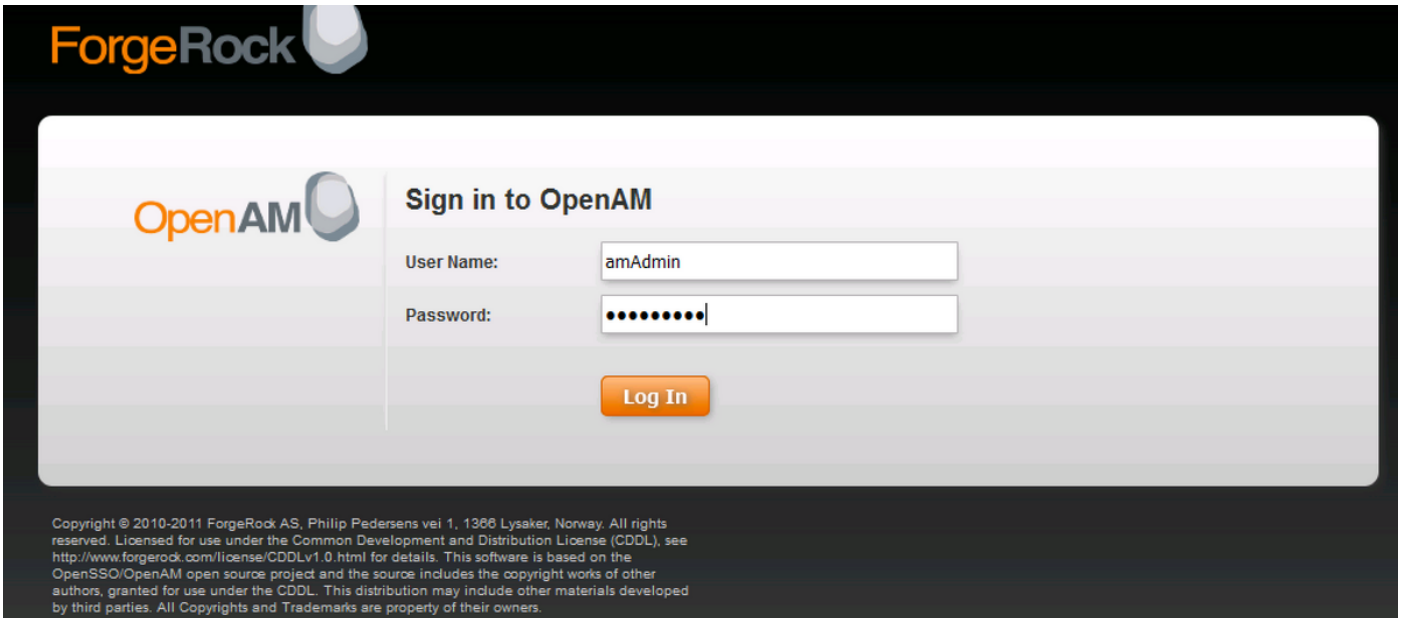
```
Checking configuration directory C:/Users/Administrator/openam....Success.  
Installing OpenAM configuration store...Success RSA/ECB/OAEPWithSHA1AndMGF1Padding.  
Extracting OpenDJ, please wait...Complete  
Running OpenDJ setupSetup command: --cli --adminConnectorPort 4444 --baseDN  
dc=openesso,dc=java,dc=net --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...
```

Konfiguration abgeschlossen



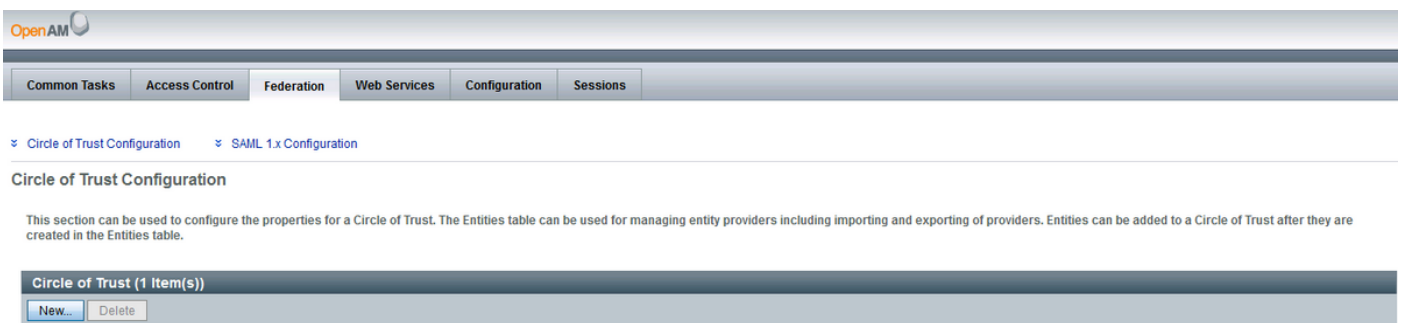
Konfigurieren von OpenAM als IdP

- 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 OpenAM-Servers an.

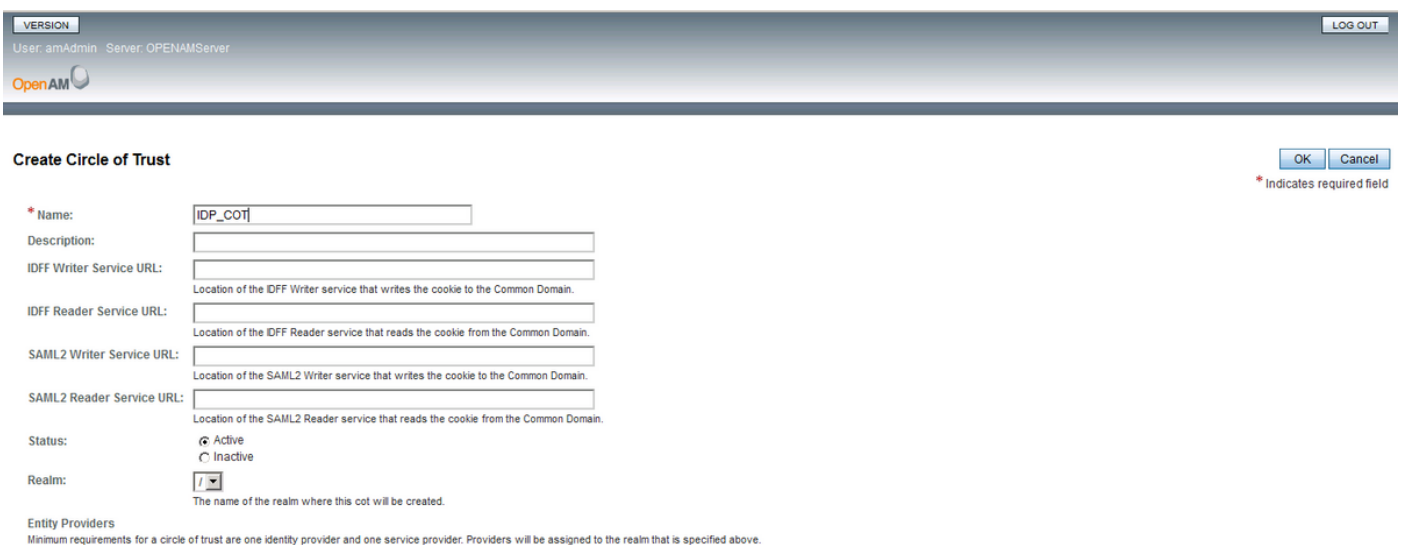


Kreis der Vertrauenskonfiguration

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



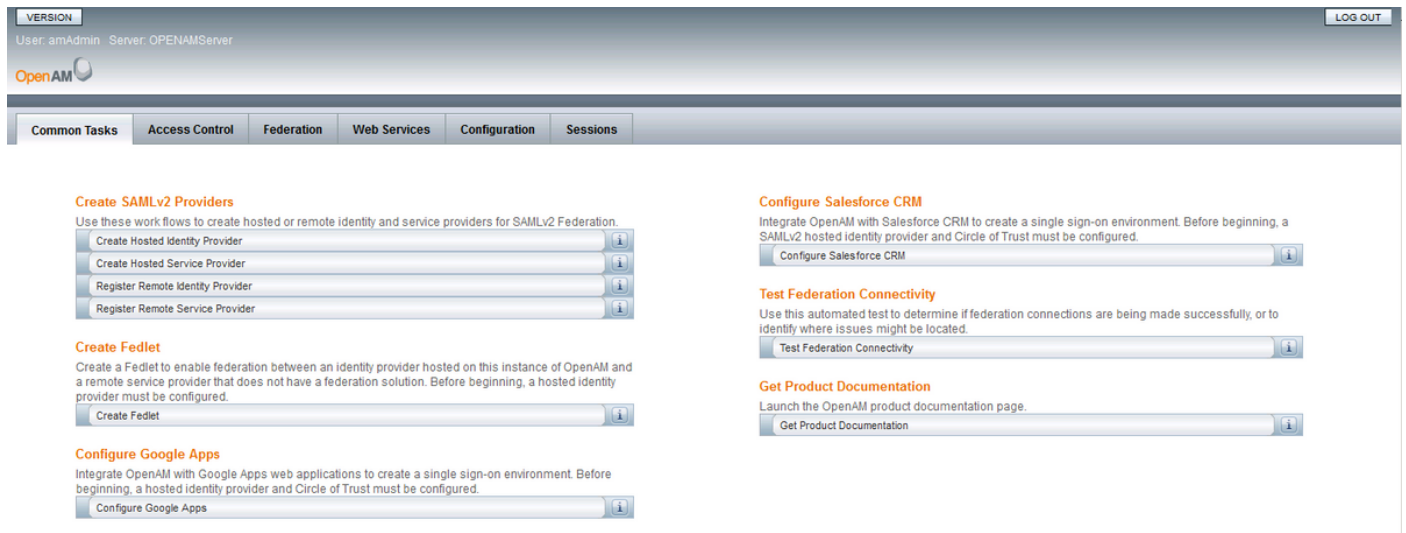
Erstellen Sie einen Vertrauenskreis mit einem eindeutigen Namen für den IdP-Vertrauenskreis, und klicken Sie auf OK.



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).



The screenshot shows the OpenAM administration interface. At the top, it displays 'VERSION', 'User: amAdmin', 'Server: OPENAMServer', and a 'LOG OUT' button. Below this 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.

Der zuvor erstellte Vertrauenskreis wird aufgeführt.

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:

Signatur Schlüssel 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.

- ✘ 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.

Entität des Diensteanbieters importieren

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

The screenshot shows the OpenAM configuration interface. At the top, there are navigation tabs: Common Tasks, Access Control, Federation, Web Services, Configuration, and Sessions. Below these, there are sub-sections for Circle of Trust Configuration and SAML 1.x Configuration. The main content area is titled "Circle of Trust Configuration" and contains a table with one item, "IDP_COT". Below this table is a section for "Entity Providers (3 Item(s))" with a table that is currently empty.

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

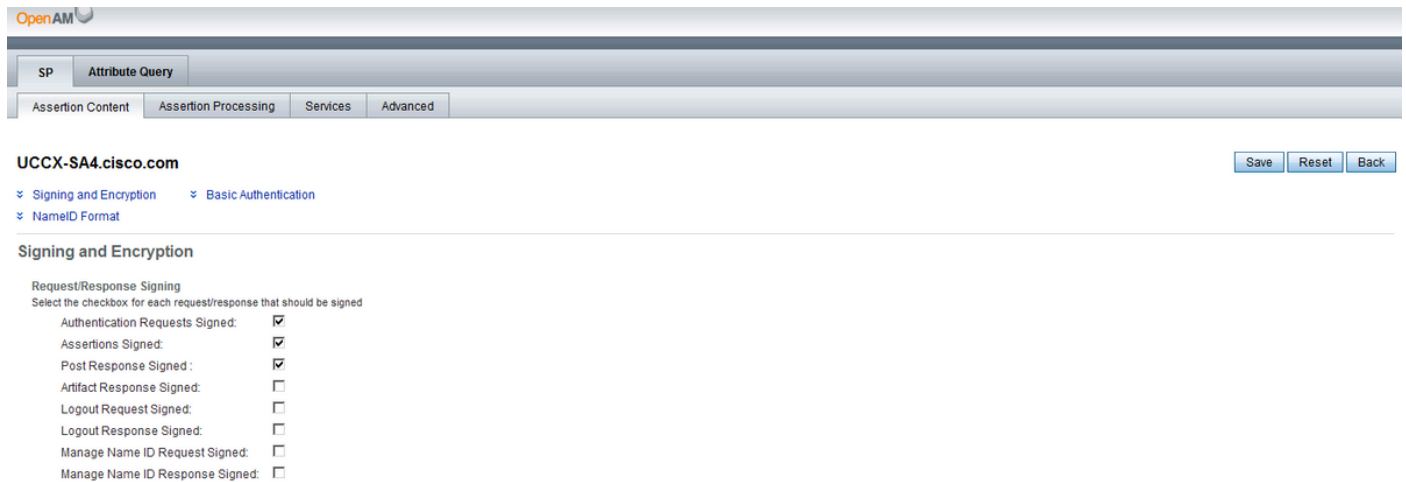
The screenshot shows the "Import Entity Provider" form in OpenAM. It includes a title bar with "OK" and "Cancel" buttons. Below the title bar, there is a paragraph of text explaining the purpose of the form. The form contains several fields:

- * Realm Name: A dropdown menu with a slash (/) selected.
- Where does the metadata file reside?: Radio buttons for "URL" and "File", with "File" selected.
- * URL where metadata is located: A text input field with an "Upload..." button next to it.
- Where does the extended data file reside?: Radio buttons for "URL" and "File", with "File" selected.
- URL where extended data is located: A text input field.

 A legend at the bottom right indicates that an asterisk (*) denotes a required field.

Signieren von Anfragen/Antworten

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



OpenAM

SP Attribute Query

Assertion Content Assertion Processing Services Advanced

UCCX-SA4.cisco.com Save Reset Back

Signing and Encryption

Request/Response Signing

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

- Authentication Requests Signed:
- Assertions Signed:
- Post Response Signed:
- Artifact Response Signed:
- Logout Request Signed:
- Logout Response Signed:
- Manage Name ID Request Signed:
- Manage Name ID Response Signed:

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.



OpenAM

SP Attribute Query

Assertion Content Assertion Processing Services Advanced

UCCX-SA4.cisco.com Save Reset Back

Attribute Mapper

Attribute Map

Current Values

- uid=sAMAccountName Remove
- user_principal=userPrincipalName

New Value Add

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.

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)

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.