

Installare e configurare il provider di identità OpenAM (IdP) per Cisco Identity Service (IdS) per abilitare l'SSO

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Install](#)

[Requisiti di sistema](#)

[Sistemi operativi](#)

[Ambiente Java](#)

[Requisiti del contenitore dell'applicazione Web](#)

[Browser supportati](#)

[Requisiti per l'archivio dati](#)

[Requisiti hardware minimi](#)

[Install](#)

[Software OpenAM](#)

[Prerequisiti](#)

[Installa applicazione Web OpenAM](#)

[Esegui servizio OpenAM](#)

[Configurazione](#)

[OpenAM Configurator](#)

[Configura OpenAM come IdP](#)

[Configurazione Circle of Trust](#)

[Crea provider di identità ospitato](#)

[Configura chiave di firma](#)

[Importa entità provider di servizi](#)

[Firma richiesta/risposta](#)

[Mapping attributi](#)

[Modifica Circle of Trust](#)

[Scarica metadati OpenAM IdP](#)

[Ulteriore configurazione per SSO:](#)

Introduzione

In questo documento viene descritta la configurazione di OpenAM Identity Provider (IdP) per abilitare Single Sign-On (SSO).

Modelli di distribuzione Cisco IdS

Prodotto	Implementazione
UCCX	Coresidente
PCCE	Coresidente con CUIC (Cisco Unified Intelligence Center) e LD (Live Data)
UCCE	Coresidenti con CUIC e LD per installazioni 2k. Standalone per installazioni a 4k e 12k.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Contact Center Express (UCCX) versione 11.6 o Cisco Unified Contact Center Enterprise versione 11.6 o Packaged Contact Center Enterprise (PCCE) versione 11.6, a seconda dei casi.

Nota: Questo documento fa riferimento alla configurazione rispetto a Cisco Identity Service (IdS) e al provider di identità (IdP). Il documento fa riferimento a UCCX nelle schermate e negli esempi, ma la configurazione è simile per quanto riguarda Cisco Identity Service (UCCX/UCCE/PCCE) e l'IdP.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Install

Nota: Questo documento fa riferimento a OpenAM release 10.0.1 come parte della qualifica con SSO

Requisiti di sistema

Sistemi	Ambiente	Requisiti del	Browser supportati	Requisiti per	Requisiti
---------	----------	---------------	--------------------	---------------	-----------

operativi	Java	contenitore dell'applicazione Web		l'archivio dati	hardware minimi
<ul style="list-style-type: none"> • Microsoft Windows Server 2003, 2008 R2 • Linux 2.6, 3.0 • Oracle Solaris 10 	<p>La release 10.0.1 di OpenAM richiede Java Development Kit 1.6, almeno la versione 1.6.0_10. ForgeRock consiglia di utilizzare almeno la versione 1.6.0_27 a causa delle correzioni apportate alla protezione. ForgeRock ha testato questa release di OpenAM principalmente con Oracle Java SE JDK. OpenAM Java SDK supporta Java Development Kit 1.5 o 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 • Application Server JBoss 7.x • Jetty 7 • Server Oracle WebLogic 11g • Oracle WebLogic Server 12c <p>Se si esegue come utente non root, il contenitore dell'applicazione Web deve essere in grado di scrivere nella propria home directory, in cui OpenAM memorizza i file di configurazione.</p>	<ul style="list-style-type: none"> • Cromo e cromo 16 e versioni successive • Firefox 3.6 e versioni successive • Internet Explorer (versione 7 e successiva) • Safari 5 e versioni successive 	<ul style="list-style-type: none"> • ForgeRock OpenDJ • Microsoft Active Directory • Server di elenchi in linea Tivoli IBM • OpenDS • Oracle Directory Server Enterprise Edition 	<ul style="list-style-type: none"> • 1 GB di RAM gratuiti per OpenAM <p>È possibile distribuire OpenAM su qualsiasi hardware supportato dalla combinazione del software richiesto.</p>

Install

Software OpenAM

- Scaricate le versioni di OpenAM 10.0.1 da <https://backstage.forgerock.com/downloads/OpenAM/OpenAM%20Enterprise/10.0.1/OpenAM%20>

- Per ogni versione dei servizi di base OpenAM, è possibile scaricare l'intero pacchetto come archivio .zip, solo il file .war OpenAM, solo gli strumenti di amministrazione come archivio .zip
- Dopo aver decompresso l'archivio dell'intero pacchetto, si ottiene una directory opensso con un file README, un set di file di licenza e le directory

Prerequisiti

Prima dell'installazione, accertarsi di disporre del software necessario per i servizi di base OpenAM,

- Un ambiente di runtime Java 6
- Installa Apache Tomcat come contenitore di applicazioni Web
- I servizi di base OpenAM richiedono una dimensione heap JVM (Java Virtual Memory) minima di 1 GB e una dimensione di generazione permanente di 256 MB. Applicare le opzioni JVM quando si imposta JAVA_OPTS nel file catalina prima dell'avvio dell'application server Tomcat - -Xmx1024m -XX:MaxPermSize=256m

Ad esempio, set JAVA_OPTS=%JAVA_OPTS% -Xmx1024m -XX:MaxPermSize=256m -Xms512m

- Installare Microsoft Active Directory come archivio dati con pochi utenti.

Installa applicazione Web OpenAM

Il file deployable-war/opensso.war contiene tutti i componenti e gli esempi del server OpenAM nella directory opensso.

Distribuisce OpenAM su Tomcat Container

Copiare il file opensso.war nella directory in cui sono archiviate le applicazioni Web tomcat. Rinominare il file opensso.war come openam.war. Riavviare il servizio Tomcat.

Verificare la schermata di configurazione iniziale nel browser all'indirizzo

<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.

Esegui servizio OpenAM

Openam è una semplice applicazione Web ospitata in un server Tomcat. Quindi, è sufficiente lanciare il vostro server tomcat e quindi essere in grado di accedere al servizio Web OpenAM.

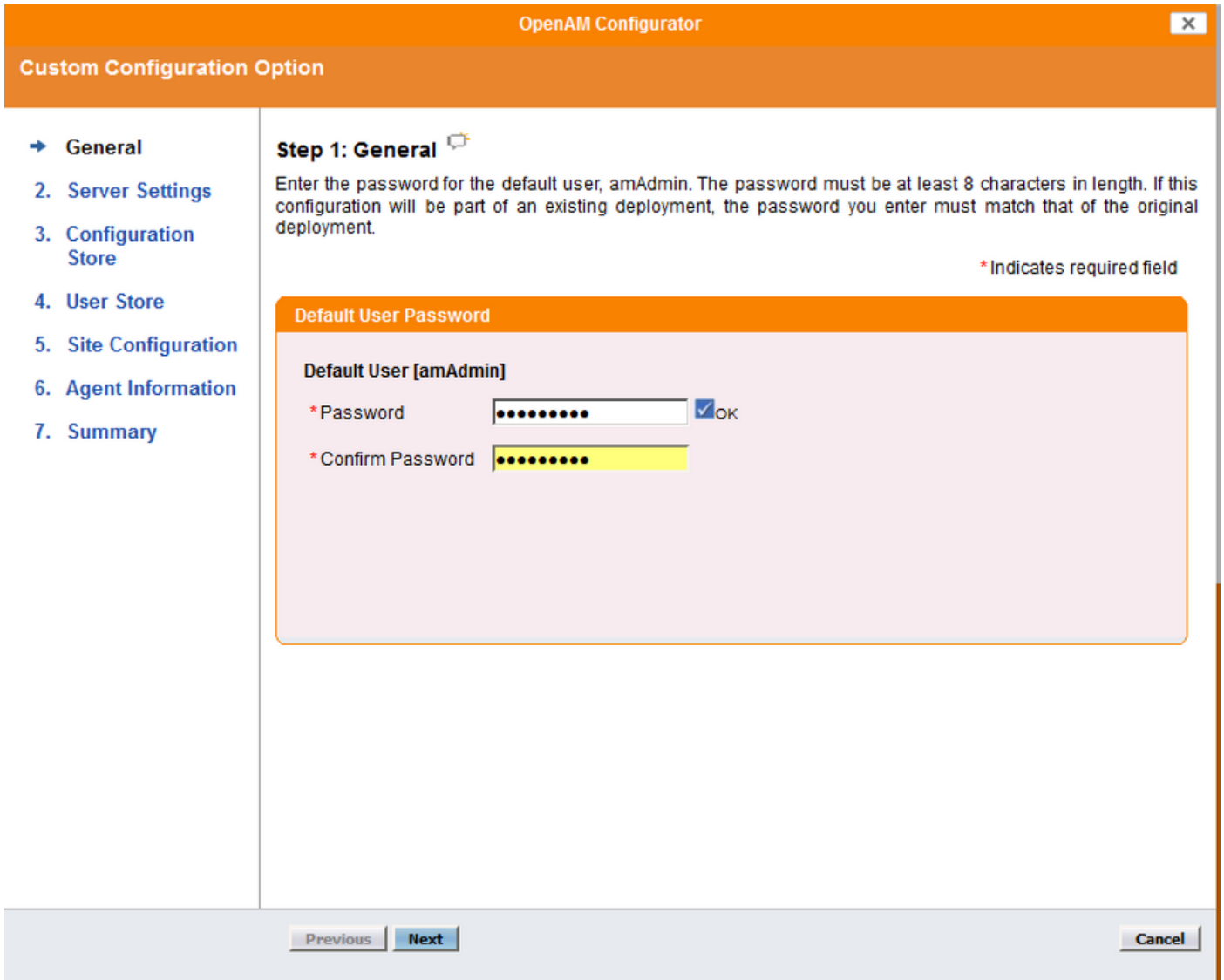
Configurazione

OpenAM Configurator

Il processo di configurazione personalizzata di OpenAM consente di impostare facilmente molte opzioni di configurazione comuni, in modo da risparmiare più tempo prima della configurazione e salvare i passaggi di configurazione richiesti in seguito.

Impostazioni generali

Fare clic su Crea nuova configurazione e scegliere la password per l'account amministratore predefinito (amAdmin). La password deve contenere almeno 8 caratteri.



Dopo aver immesso due volte una password valida, viene visualizzato il pulsante Next (Avanti) e la configurazione può continuare.

Impostazioni server


Per impostazione predefinita, l'URL del server è il nome di dominio completo del server.

Nota: È importante che l'utente che esegue Apache Tomcat disponga dell'accesso in scrittura alla directory Configuration. Ne consegue che ~/openam/config è appropriato per questo scopo. Le versioni locali della piattaforma supportate sono en_US (inglese), de (tedesco), es (spagnolo), fr (francese), ja (giapponese), zh_CN (cinese semplificato) o zh_TW (cinese tradizionale).

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 2: Server Settings 

Confirm the following settings to use for the server.

* Indicates required field

Server Settings

* Server URL	<input type="text" value="http://openamserver.cisco.com:8080"/>
* Cookie Domain	<input type="text" value=".cisco.com"/>
* Platform Locale	<input type="text" value="en_US"/>
* Configuration Directory	<input type="text" value="C:/Users/Administrator/openam"/>

Previous Next Cancel


Impostazioni archivio dati di configurazione

Per la configurazione a server singolo, non è necessario modificare queste impostazioni.

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

Previous Next Cancel

Impostazioni archivio dati utente

Le impostazioni dell'archivio dati utente connettono OpenAM all'archivio dati di Microsoft Active Directory.

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
 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

- Tipo archivio dati utente: Active Directory con host e porta
- SSL/TLS abilitato: Non abilitato
- Nome directory: <Nome dominio del server AD>
- Port: 389
- Suffisso radice: dc=cisco,dc=com
- ID di accesso: cn=<nome utente AD>,cn=users,dc=cisco,dc=com
- Password: <Password utente AD>

Nota: Configurator non offre l'opzione di continuare finché tutte le impostazioni non sono state specificate correttamente e la connessione all'istanza di Active Directory non è riuscita.


Configurazione sito

Nella schermata Configurazione sito è possibile configurare OpenAM come parte di un sito in cui il carico viene bilanciato tra più server OpenAM. Per la prima installazione di OpenAM, accettare le impostazioni predefinite.

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

Previous Next Cancel

Informazioni sull'agente

Nella schermata Informazioni sull'agente, fornire una password di almeno 8 caratteri che gli agenti dei criteri devono utilizzare per connettersi a 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

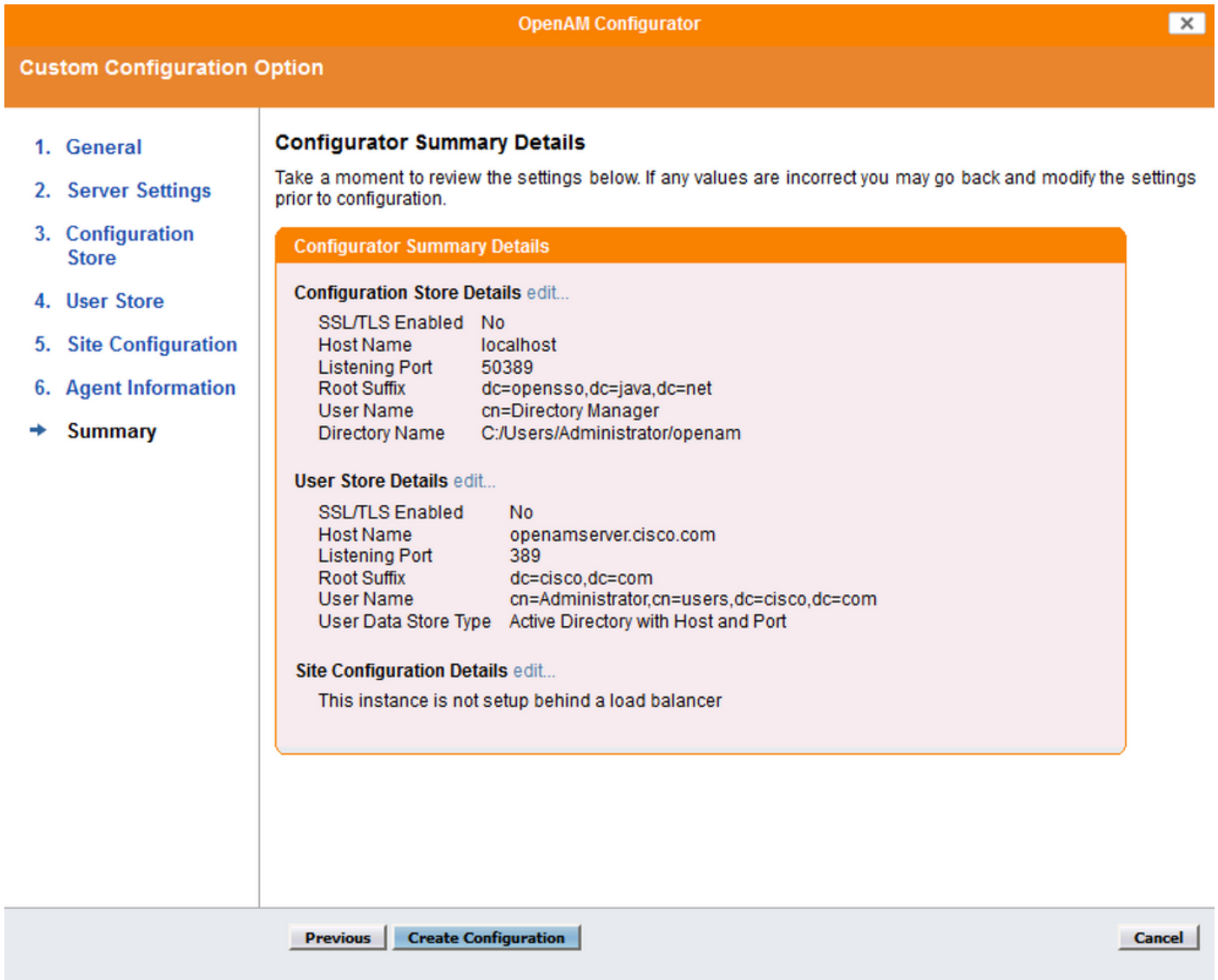
Default Policy Agent [UriAccessAgent]

* Password OK

* Confirm Password

Riepilogo

Esaminare le informazioni e fare clic su Crea configurazione



Stato configurazione

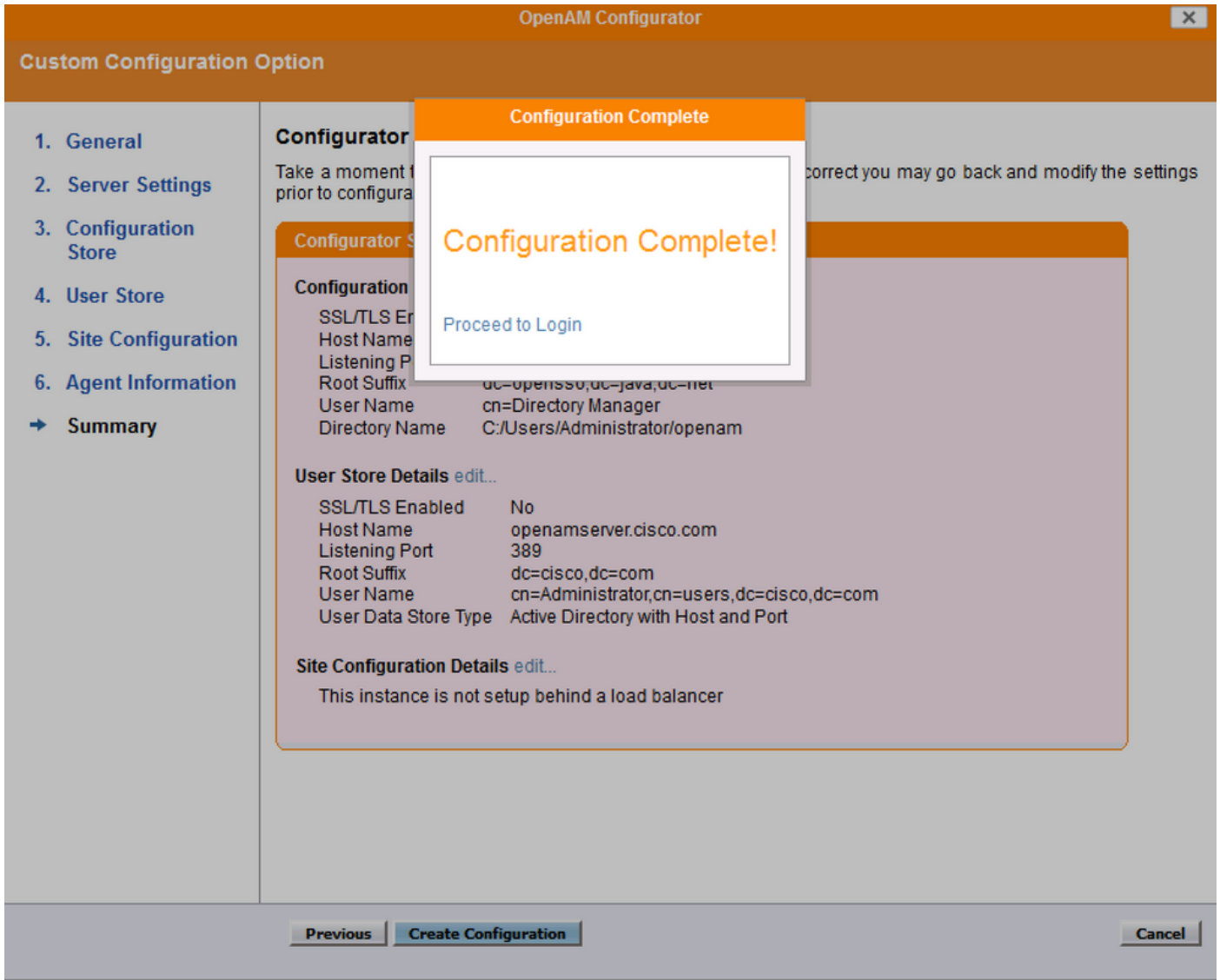
Nella schermata di avanzamento della configurazione viene visualizzato lo stato di avanzamento dell'installazione. Tutto l'output visualizzato in questa schermata e gli errori vengono scritti nel file: `~/openam/config/install.log`.

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  
/opends/config/config.ldif --doNotStart --hostname openamserver.cisco.com OpenDJ 2.4.5  
Please wait while the setup program initializes...
```

Configurazione completata



Configura OpenAM come IdP

- Fare clic su Accedi o accedi all'URL <http://<FQDN di OpenAM>:8080/openam>, quindi accedere come amministratore di OpenAM
- Quando si accede a OpenSSO Enterprise per la prima volta, si viene indirizzati al Configurator per eseguire la configurazione iniziale di OpenSSO Enterprise
- Seleziona configurazione predefinita
- È necessario configurare le password per OpenAMserver
- Configurare le password e accedere all'interfaccia utente del server OpenAM

Sign in to OpenAM

User Name:

Password:

Log In

Copyright © 2010-2011 ForgeRock AS, Phillip 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.

Configurazione Circle of Trust

Passare alla scheda Federazione e fare clic sul pulsante Nuovo nella sezione Cerchio di fiducia

The screenshot shows the OpenAM Administration Console. The top navigation bar includes 'Common Tasks', 'Access Control', 'Federation', 'Web Services', 'Configuration', and 'Sessions'. Under the 'Federation' tab, there are sub-sections for 'Circle of Trust Configuration' and 'SAML 1.x Configuration'. The 'Circle of Trust Configuration' section contains a heading 'Circle of Trust (1 Item(s))' and two buttons: 'New...' and 'Delete'.

Creare un cerchio di fiducia con un nome univoco per il cerchio di fiducia IdP e fare clic su OK

The screenshot shows the 'Create Circle of Trust' form. At the top right, there are 'OK' and 'Cancel' buttons. A note indicates that an asterisk (*) denotes a required field. The form fields are as follows:

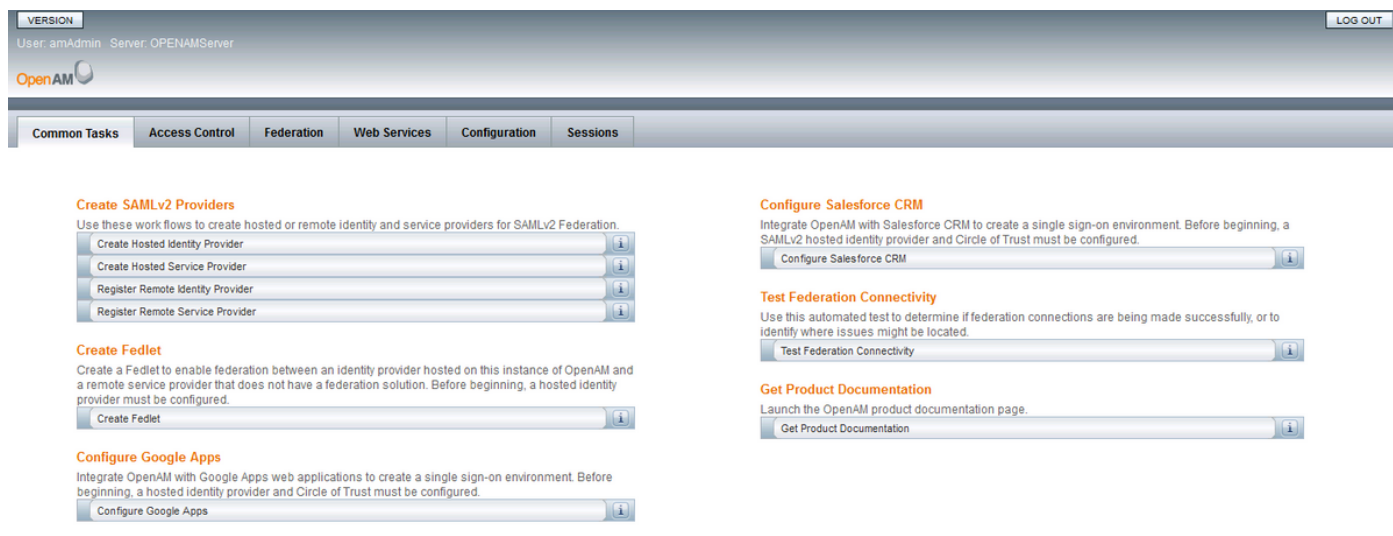
- Name:** (required)
- Description:**
- IDFF Writer Service URL:** (Location of the IDFF Writer service that writes the cookie to the Common Domain.)
- IDFF Reader Service URL:** (Location of the IDFF Reader service that reads the cookie from the Common Domain.)
- SAML2 Writer Service URL:** (Location of the SAML2 Writer service that writes the cookie to the Common Domain.)
- SAML2 Reader Service URL:** (Location of the SAML2 Reader service that reads the cookie from the Common Domain.)
- Status:** Active, Inactive
- Realm:** (The name of the realm where this cot will be created.)

Entity Providers
Minimum requirements for a circle of trust are one identity provider and one service provider. Providers will be assigned to the realm that is specified above.

Nota: Affinché l'SSO SAML funzioni, è necessario che il provider di servizi e l'IdP si trovino nello stesso Circle of Trust(CoT).

Crea provider di identità ospitato

Passare alla scheda Attività comuni e fare clic su Crea provider di identità ospitato e creare un provider di identità ospitato (lasciare i valori configurati predefiniti e salvare le impostazioni).



The screenshot shows the OpenAM Administration Console 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 bar with tabs: 'Common Tasks', 'Access Control', 'Federation', 'Web Services', 'Configuration', and 'Sessions'. The 'Configuration' tab is active. The main content area displays several task cards, each with a title, a brief description, and a button with an information icon (i):

- 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.

Viene elencato il Circle of Trust creato in precedenza

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:

Configura chiave di firma

Passare alla scheda Federazione e fare clic su Provider di identità ospitato aggiunto nella sezione Provider di entità. Passare alla sezione Contenuto asserzione e configurare il valore del campo Firma come test nella sezione Alias certificato. Certificato che verrebbe utilizzato per firmare l'asserzione SAML.

- ✘ 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.

Importa entità provider di servizi

Passare alla scheda Federazione e fare clic sul pulsante Importa entità... nella sezione Provider di entità.

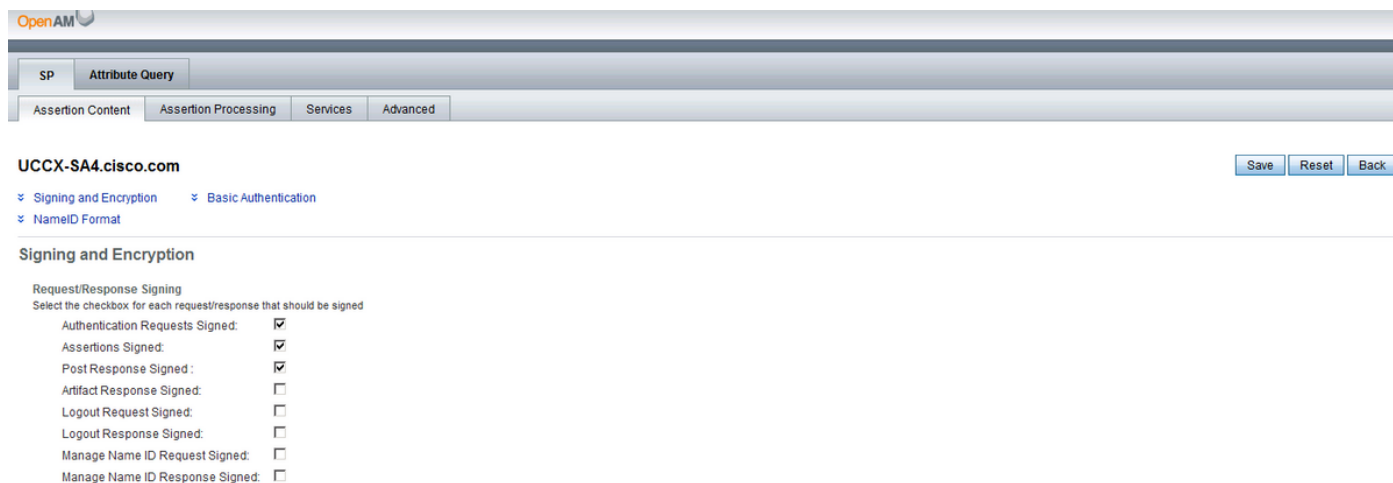
The screenshot shows the OpenAM interface with the 'Federation' tab selected. Under 'Circle of Trust Configuration', there is a table for 'Circle of Trust (1 Item(s))' with one entry: 'IDP_COT' with realm '/' and status 'Active'. Below it, the 'Entity Providers (3 Item(s))' section has an 'Import Entity...' button.

Caricare il file di entità del provider di servizi (sp.xml) e salvare la pagina.

The screenshot shows the 'Import Entity Provider' form. It includes fields for 'Realm Name' (dropdown), 'Where does the metadata file reside?' (radio buttons for URL and File), 'URL where metadata is located' (with an 'Upload...' button), 'Where does the extended data file reside?' (radio buttons for URL and File), and 'URL where extended data is located' (text input). There are 'OK' and 'Cancel' buttons at the top right.

Firma richiesta/risposta

Fare clic sull'entità importata e abilitare la firma per richiesta/risposta



The screenshot shows the OpenAM configuration interface for the entity 'UCCX-SA4.cisco.com'. The 'Attribute Query' tab is active, and the 'Advanced' sub-tab is selected. Under the 'Signing and Encryption' section, the 'Request/Response Signing' options are visible. The following checkboxes are checked: Authentication Requests Signed, Assertions Signed, and Post Response Signed. The other checkboxes (Artifact Response Signed, Logout Request Signed, Logout Response Signed, Manage Name ID Request Signed, and Manage Name ID Response Signed) are unchecked.

Mapping attributi

Passare a Elaborazione asserzioni e aggiungere un attributo di mapping per uid e user_principal in base alle impostazioni Directory e OpenAM. Fare clic su Save (Salva).



The screenshot shows the OpenAM configuration interface for the entity 'UCCX-SA4.cisco.com'. The 'Attribute Mapper' tab is active, and the 'Artifact Message Encoding' sub-tab is selected. Under the 'Attribute Map' section, the 'Current Values' list contains two entries: 'uid=sAMAccountName' and 'user_principal=userPrincipalName'. A 'Remove' button is next to the list. Below the list, there 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.'

Nota: entrambi gli attributi uid e user_principal sono obbligatori, in quanto il provider di servizi (SP) identifica l'identità di un utente autenticato tramite questi attributi. Verificare inoltre che gli attributi sAMAccountName e userPrincipalName siano mappati anche nell'Editor attributi delle proprietà utente di Active Directory.

Modifica Circle of Trust

Passare alla scheda Federazione e fare clic su Cerchio di attendibilità aggiunto e assicurarsi di spostare l'entità IdP (server OpenAm) e Service Provider dalle sezioni Disponibili a Selezionati nella sezione Provider di entità. In questo modo IdP e provider di servizi vengono assegnati allo stesso Circle of Trust.


```
<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>
            MIICcTCCAdggAwIBAgIEEe4zDANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJTTjESMBAGA1UE
            CBMja2FybmlF0YWhcMRlW5nYXVvcmluYXVjAUBgNVBAQTDW5pc2NvIHNSc3RlbXNl
            DTALBgNVBAS TBGNjYnUxZzAdBgNVBAMTFm9wZm9udG9wZm9udG9wZm9udG9wZm9udG9w
            MDcyMjYyYWhcMRlW5nYXVvcmluYXVjAUBgNVBAQTDW5pc2NvIHNSc3RlbXNlDTALBgNV
            BAsTBGNjYnUxZzAdBgNVBAMTFm9wZm9udG9wZm9udG9wZm9udG9wZm9udG9wZm9udG9w
            MRIwEAYDVQQHEwliYXVjAUBgNVBAQTDW5pc2NvIHNSc3RlbXNlDTALBgNVBAS TBGNj
            YnUxZzAdBgNVBAMTFm9wZm9udG9wZm9udG9wZm9udG9wZm9udG9wZm9udG9wZm9udG9w
            MIGJAoBAKvnlKKeu0A1+V2YdfyuiFKQWXdM6E0c/1fmig94cGdNXxw13KxzjUF2Vv4r364rTFi
            73eIduF6e1/M481ECYed24LxKpgcSFm1jAbDQ17Ae0gyzPnWQJODf850guGVQhZUUt0RKYYP/d0
            bgvaRrWxGIvoIRJ+8ky+zLV0T7nAgMBAEEwDQYJKoZIhvcNAQEFBQADGAEAM7NSup7MOHYCLF1
            i7hK99EMUJxmeYvAvAjea85TH7Ba5d0Z1+R/bnXTS/9/pBET15knuKd+Q59P19je2W7L36vFHoF1Q
            jLLAGn3JOVEm0tImcGZGc3m77Thlqn0LIcyjnrXclVQ10m75yfiMFeeHdFPgBuzTsXjkIKjmHF9
            +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/IDPniRedirect/metaAlias/idp1"
      ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPniRedirect/metaAlias/idp1" />
    <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://openamserver.cisco.com:8443/openam/IDPniPOST/metaAlias/idp1"
      ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPniPOST/metaAlias/idp1" />
    <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://openamserver.cisco.com:8443/openam/IDPniSoap/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/NIMSsoap/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>
```

Ulteriore configurazione per SSO:

In questo documento viene descritta la configurazione dell'elemento IdP per l'SSO da integrare con Cisco Identity Service. Per ulteriori informazioni, consultare le guide alla configurazione dei singoli prodotti:

- [UCCX](#)
- [UCCE](#)
- [PCCE](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).