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

Sommario

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 Identify 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 Identify 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	Requisit

operativi	Java	contenitore dell'applicazione Web		l'archivio dati	hardware minimi
• Microsoft Windows Server 2003, 2008 R2 • Linux 2.6, 3.0 • Oracle Solaris 10	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.	• 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 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.	• Cromo e cromo 16 e versioni successive • Firefox 3.6 e versioni successive • Internet Explorer (versione 7 e successiva) • Safari 5 e versioni successive	• ForgeRock OpenDJ • Microsoft Active Directory • Server di elenchi in linea Tivoli IBM • OpenDS • Oracle Directory Server Enterprise Edition	• 1 GB RAM gratuit per OpenA È possibile distribuire OpenAM su qualsiasi hardware supportato dalla combinazion del software richiesto.

Install

Software OpenAM

- Scaricate le versioni di OpenAM 10.0.1 da https://backstage.forgerock.com/downloads/OpenAM/OpenAM%20Enterprise/10.0.1/OpenAM%201

- 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.

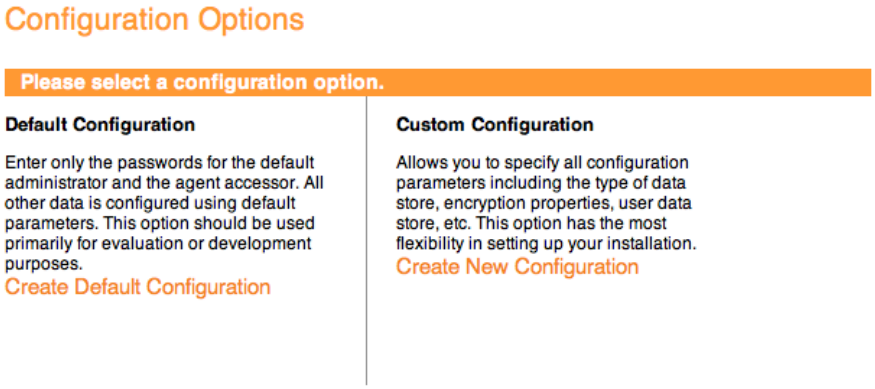
Installa applicazione Web OpenAM

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

Distribuisci 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



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.

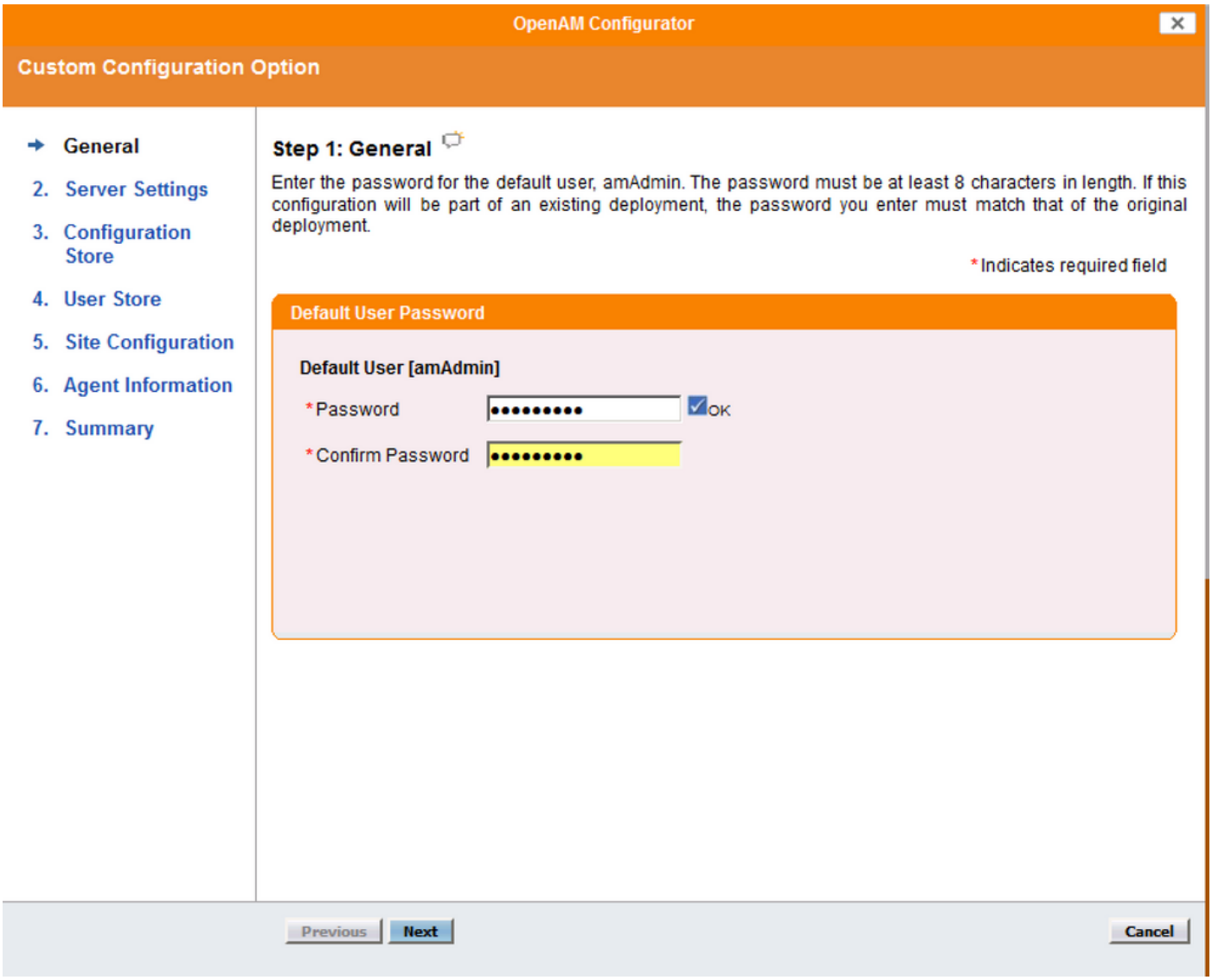
Configurazione

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.

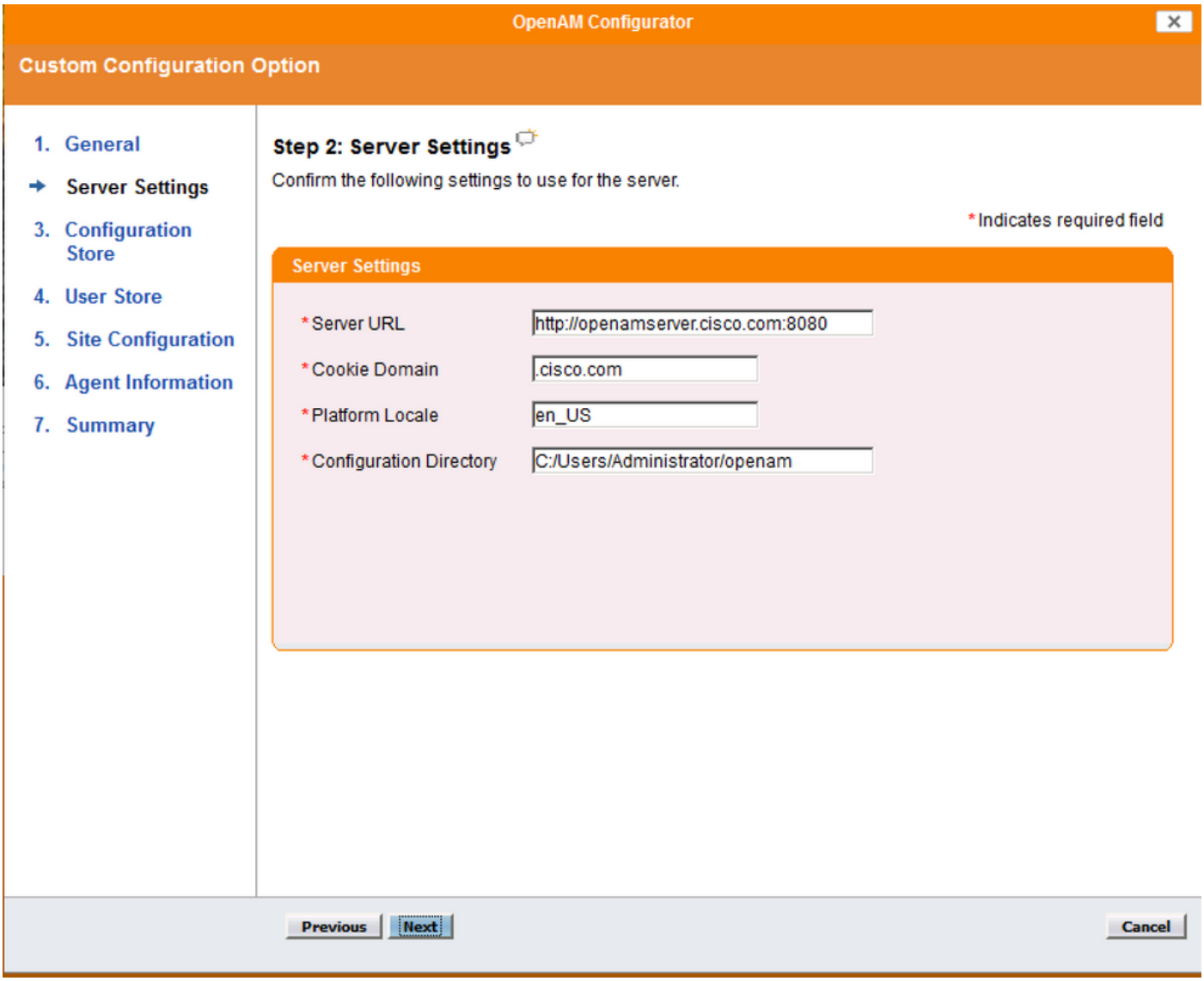


Dopo aver immesso due volte una password valida, viene visualizzato il pulsante Next (Avanti) e la configurazione può continuare.

Impostazioni server

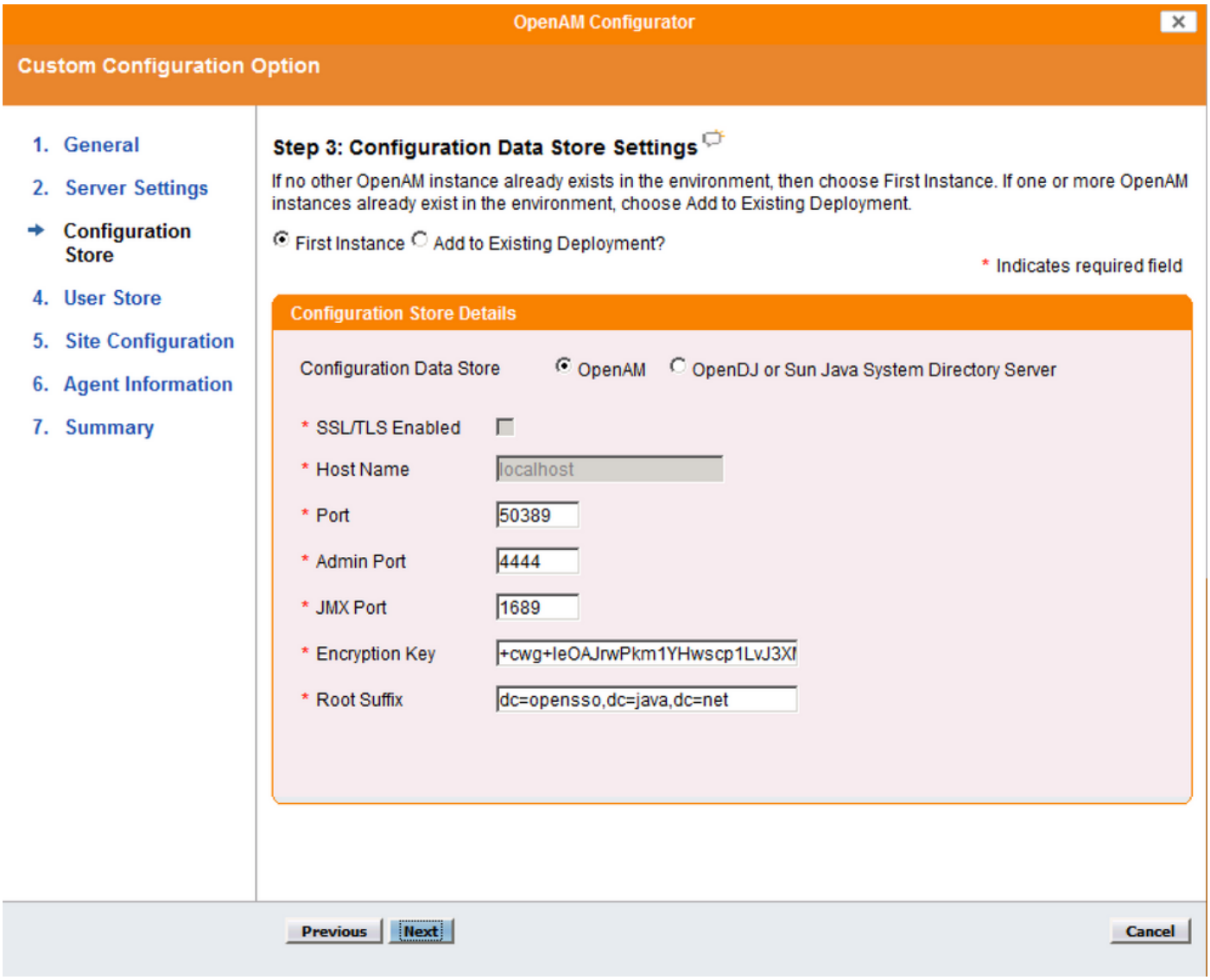
Per impostazione predefinita, l'URL del server è il nome di dominio completo del server.

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).



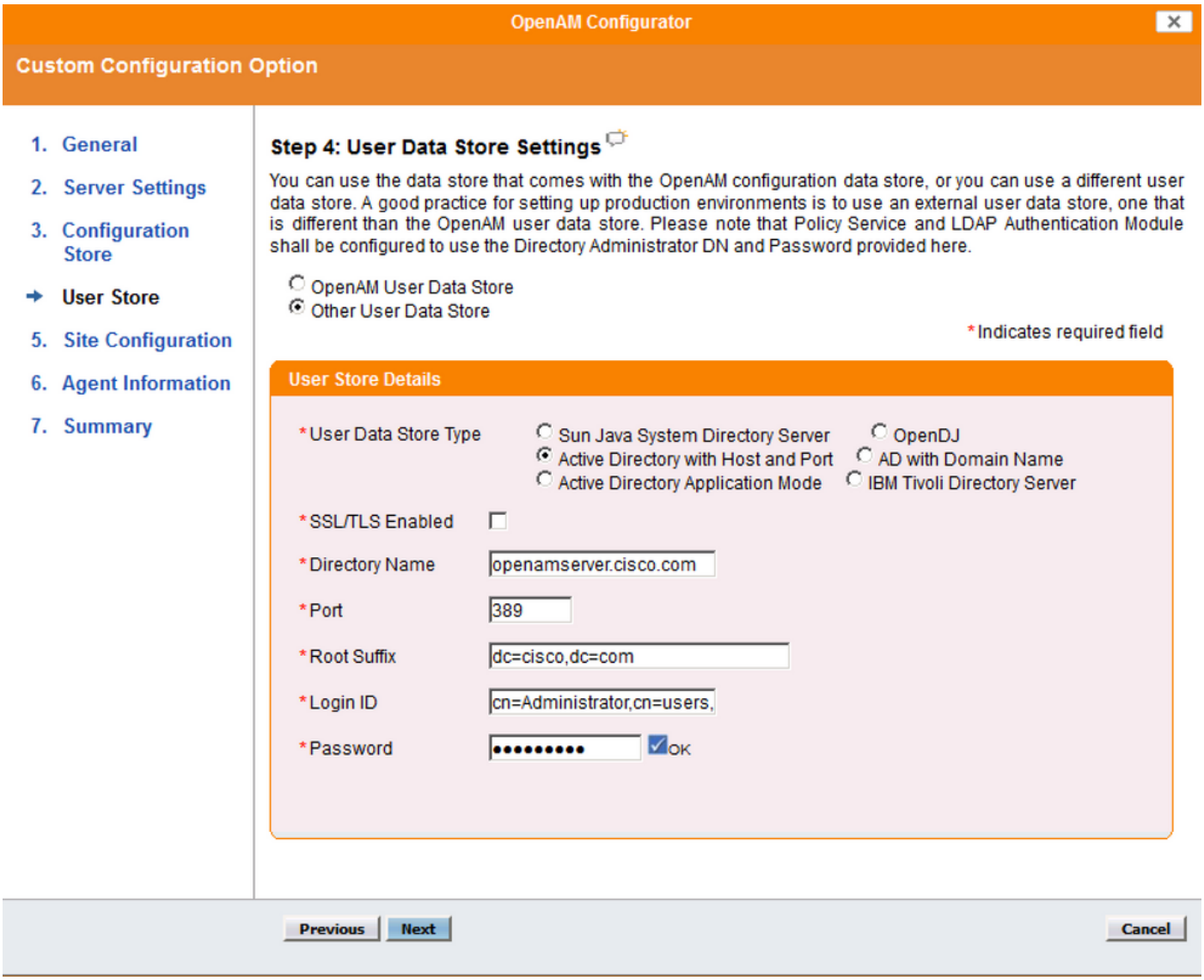
Impostazioni archivio dati di configurazione

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



Impostazioni archivio dati utente

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

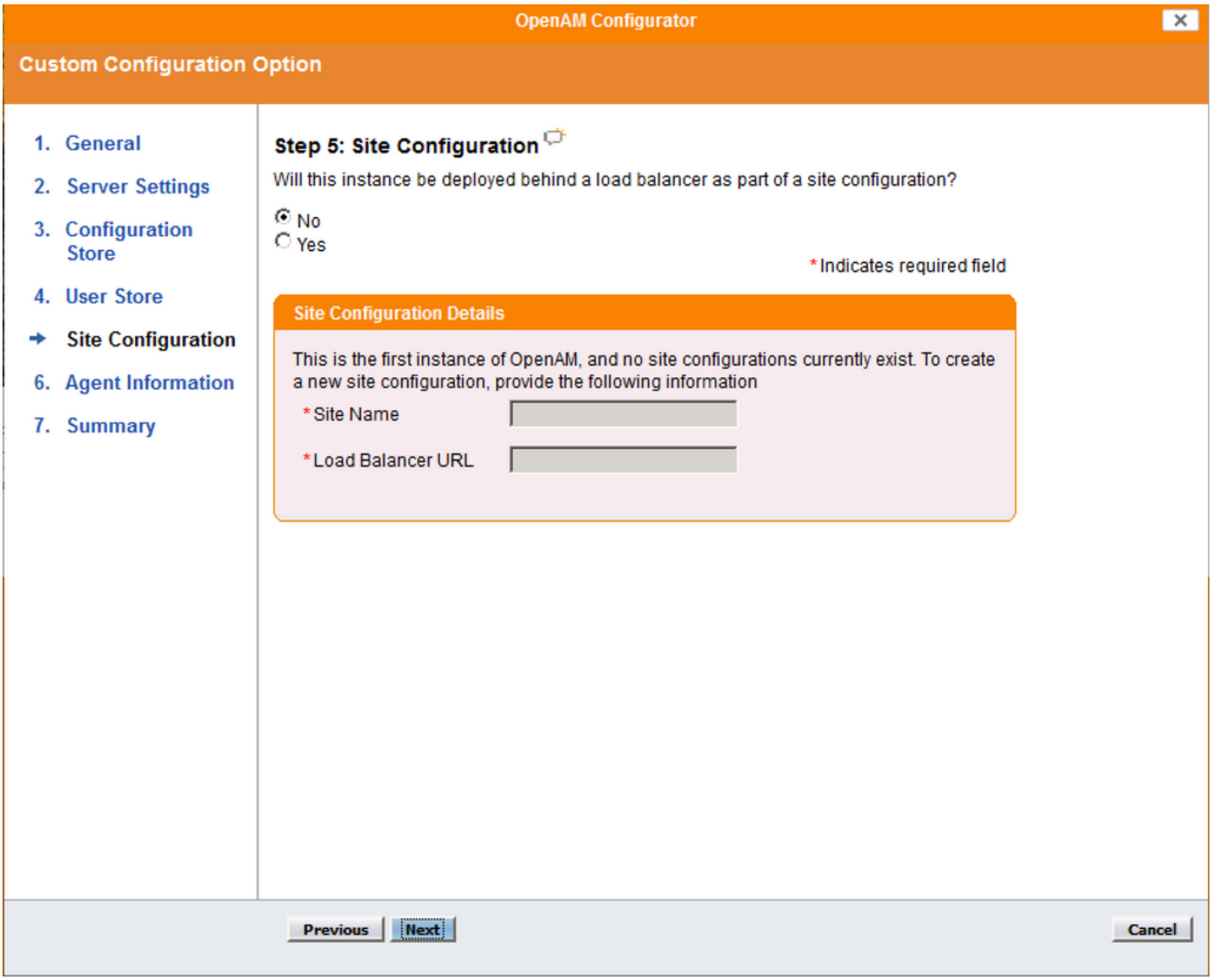


- Tipo archivio dati utente: Active Directory con host e porta
- SSL/TLS abilitato: Non abilitato
- Nome directory: <Nome dominio del server AD>
- Port: 389
- Suffisso radice: dc=cisco,dc=com
- ID di accesso: cn=<nome utente AD>,cn=users,dc=cisco,dc=com
- Password: <Password utente AD>

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.

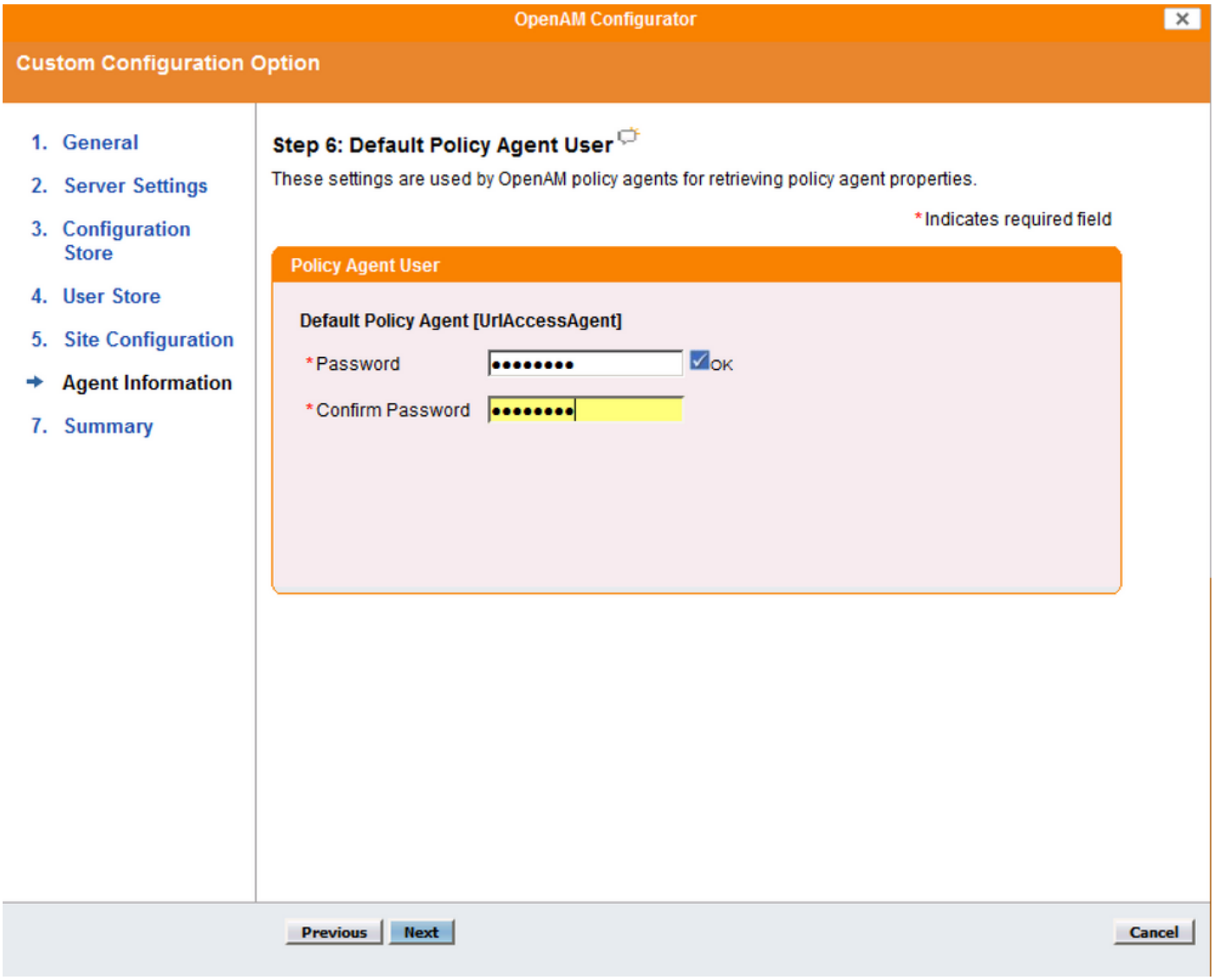
Configurazione sito

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.



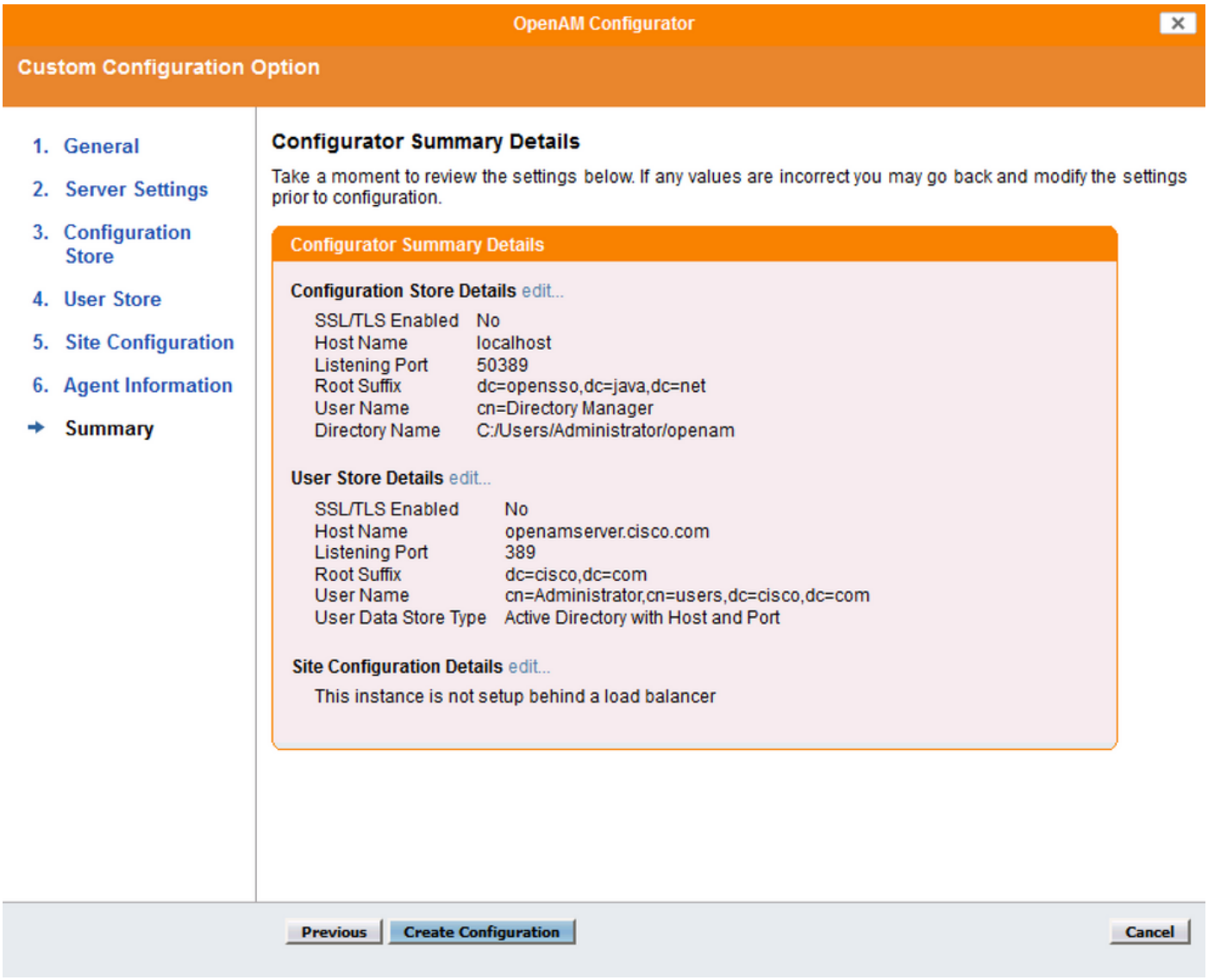
Informazioni sull'agente

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



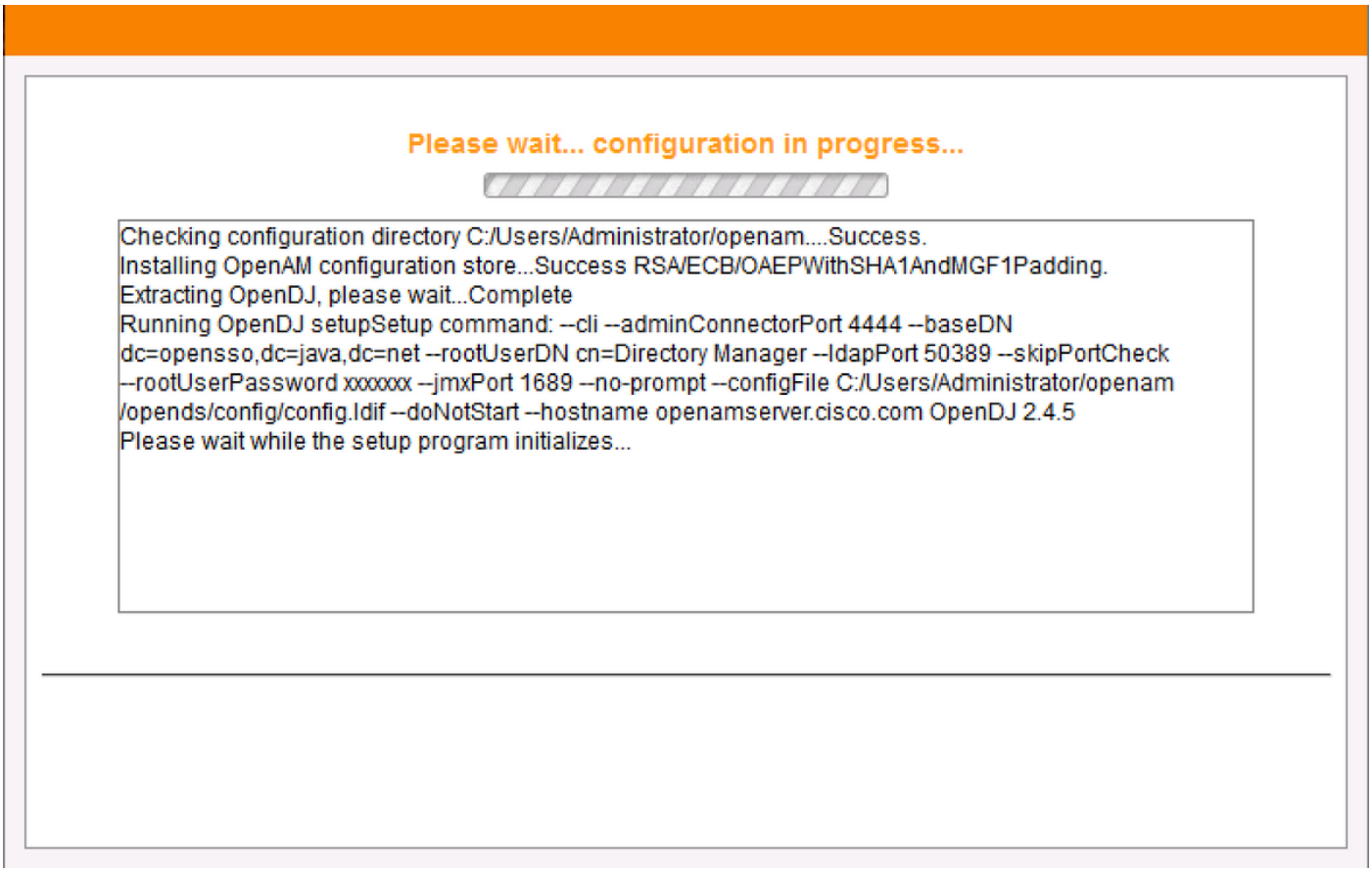
Riepilogo

Esaminare le informazioni e fare clic su Crea configurazione

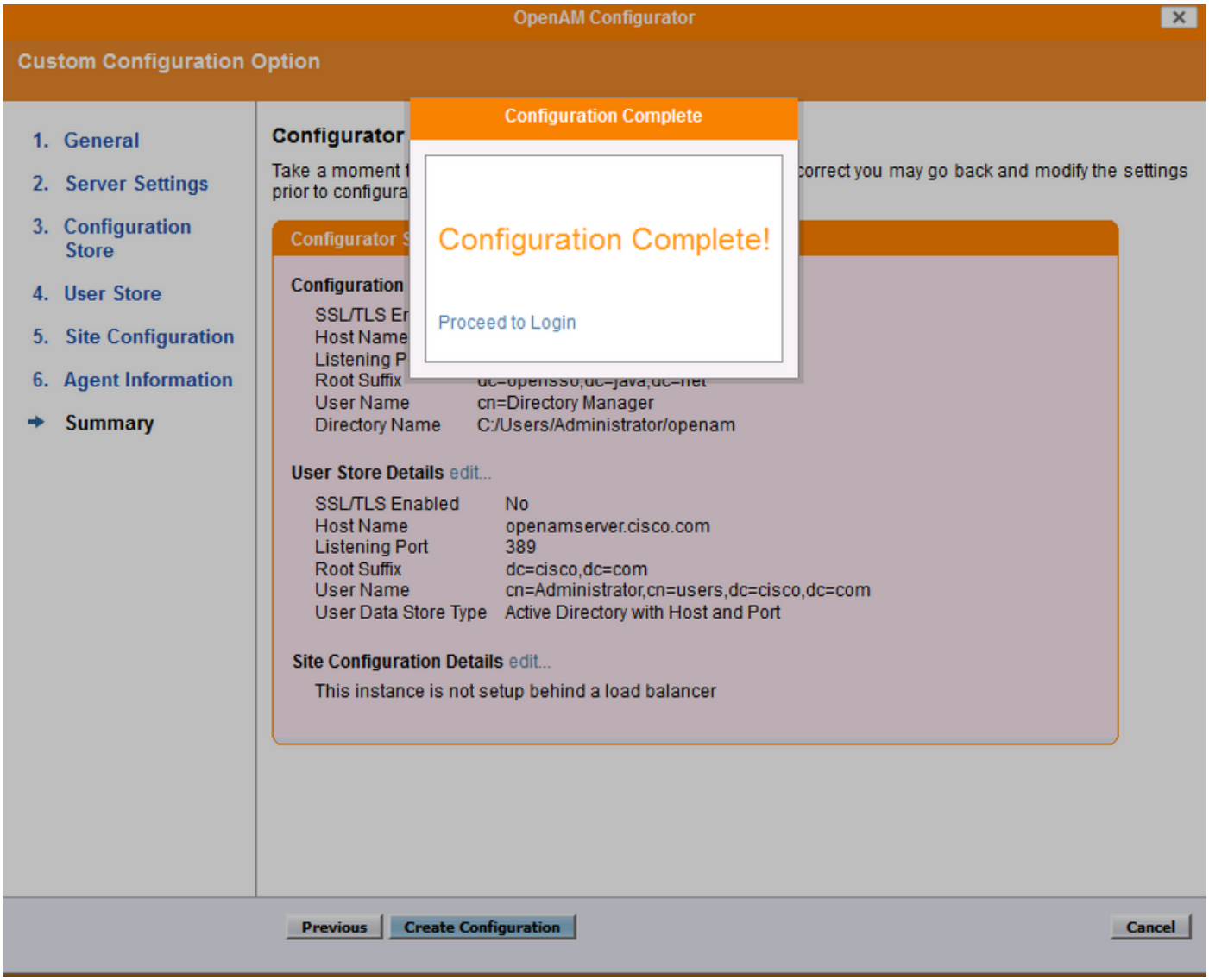


Stato configurazione

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.

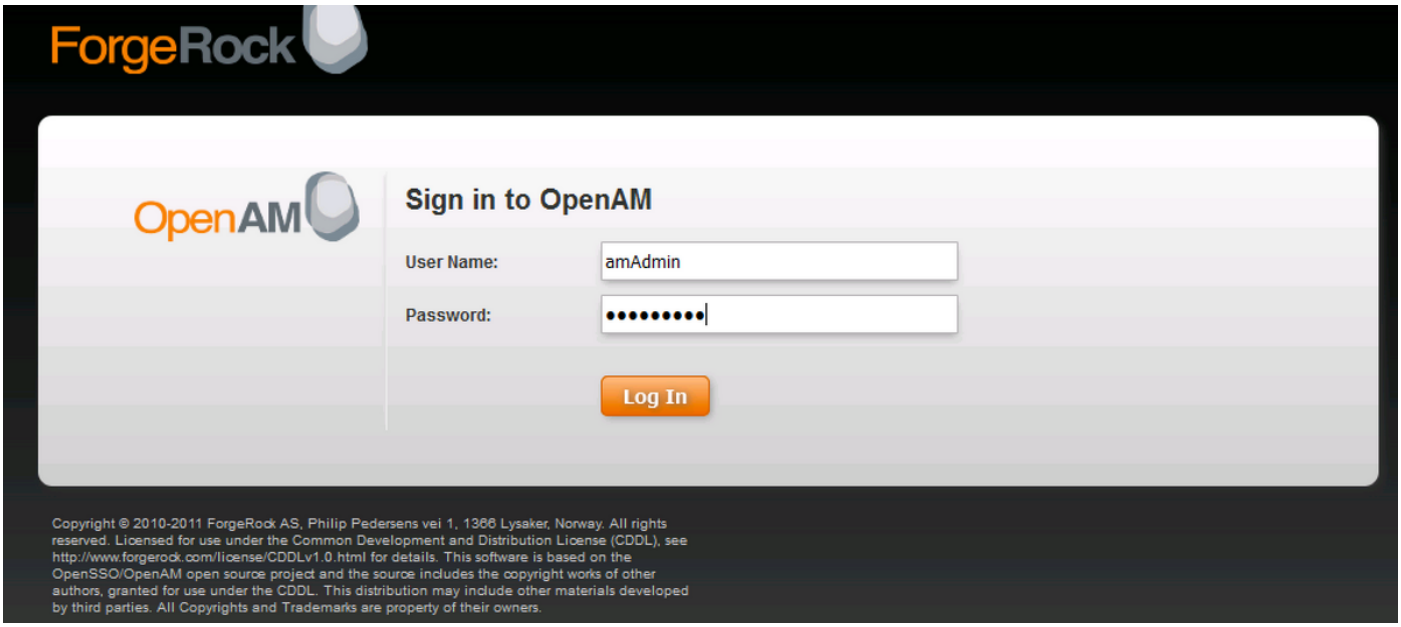


Configurazione completata



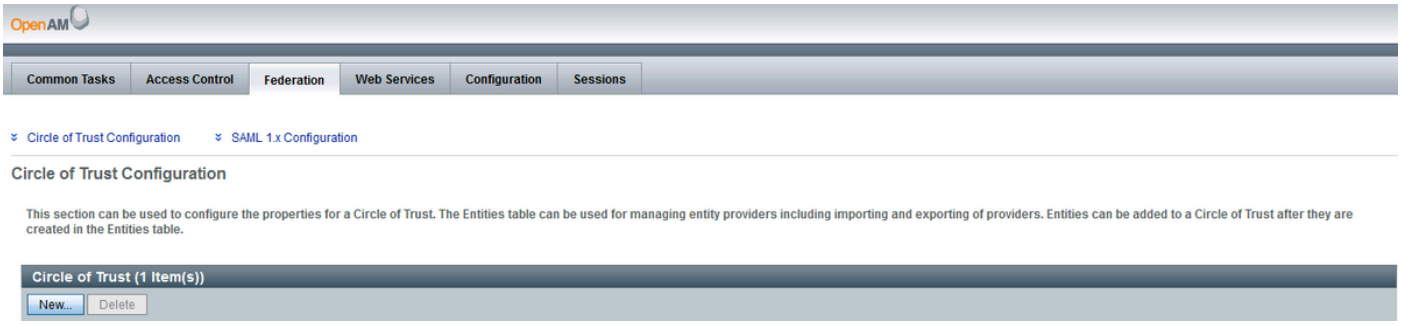
Configura OpenAM come IdP

- 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 OpemAM

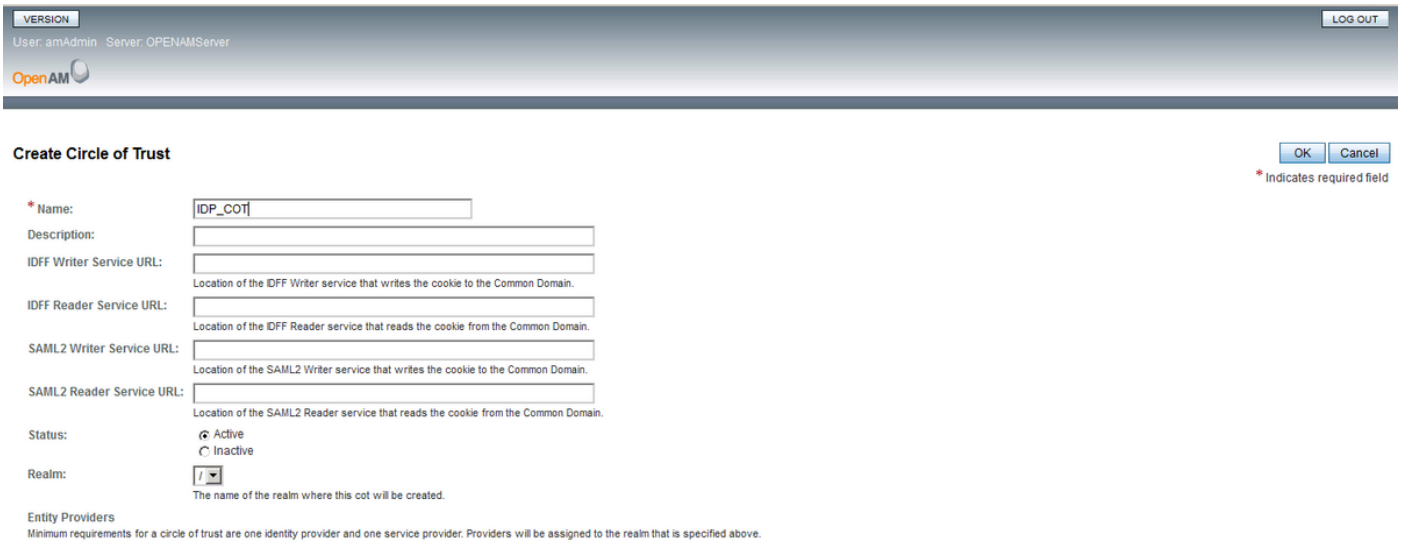


Configurazione Circle of Trust

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



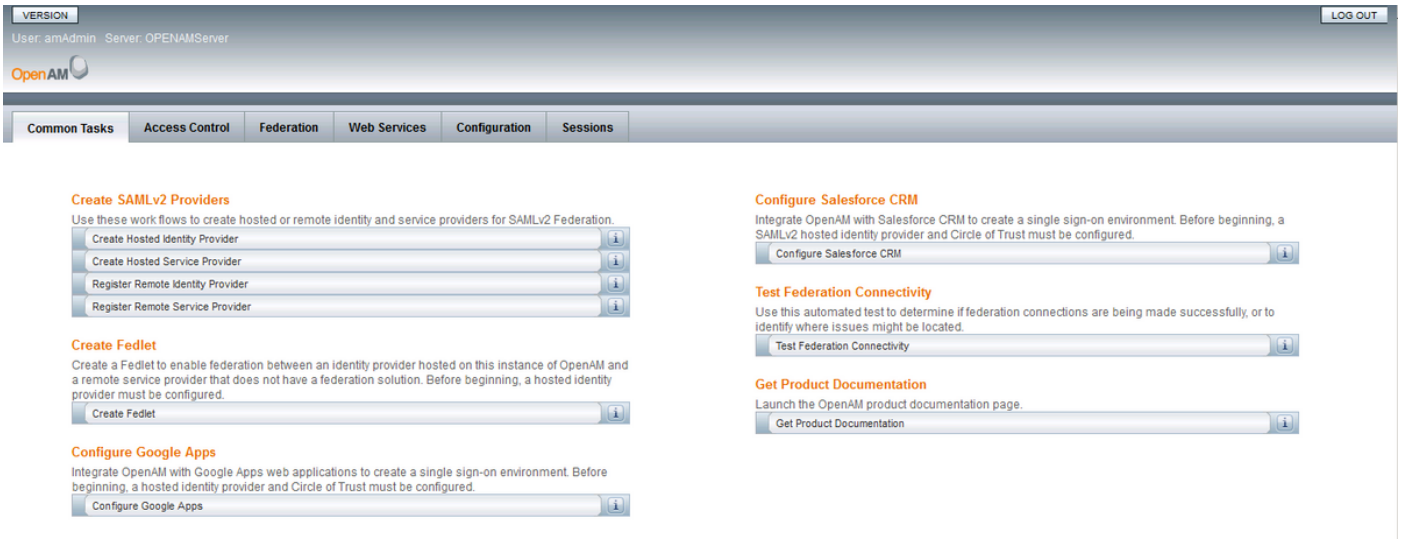
Creare un cerchio di fiducia con un nome univoco per il cerchio di fiducia IdP e fare clic su OK



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

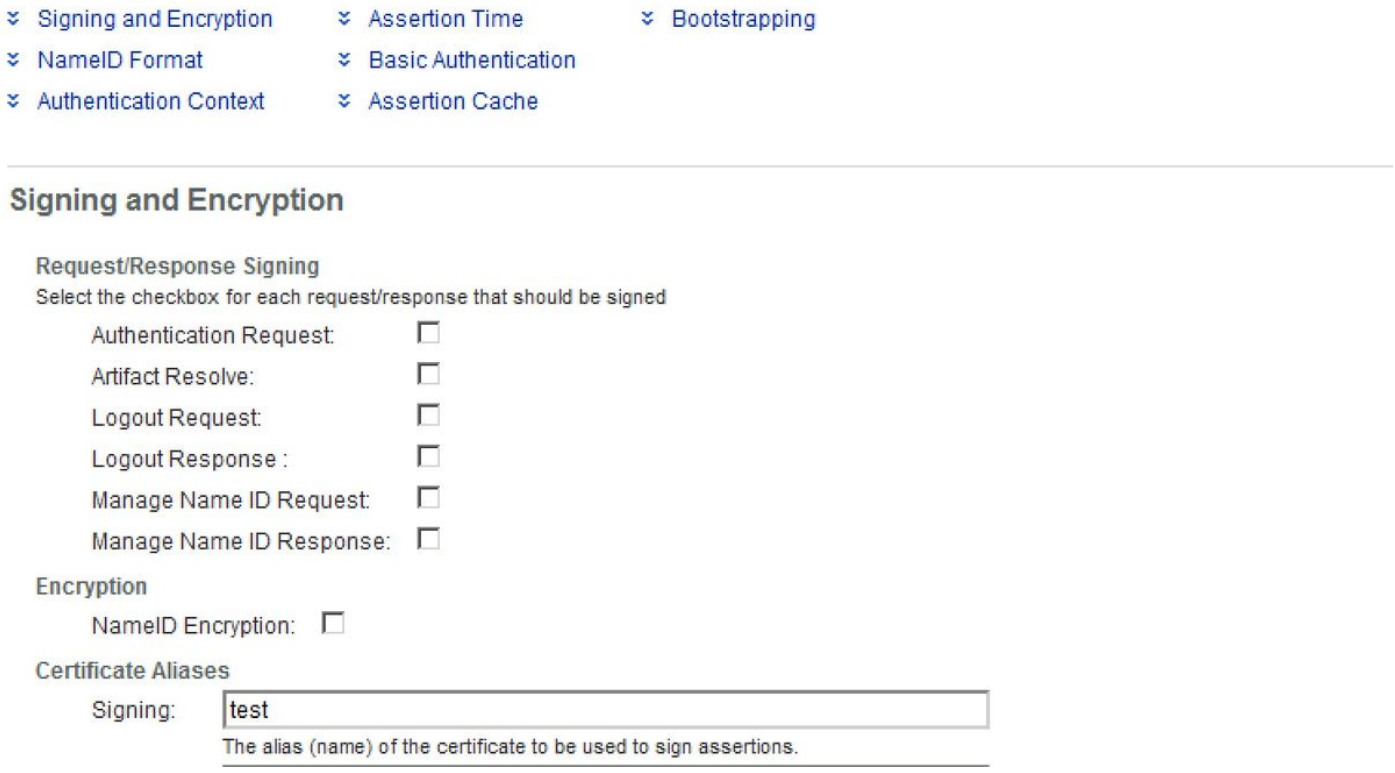
Passare alla scheda Attività comuni e fare clic su Crea provider di identità ospitato e creare un provider di identità ospitato (lasciare i valori configurati predefiniti e salvare le impostazioni).



Viene elencato il Circle of Trust creato in precedenza

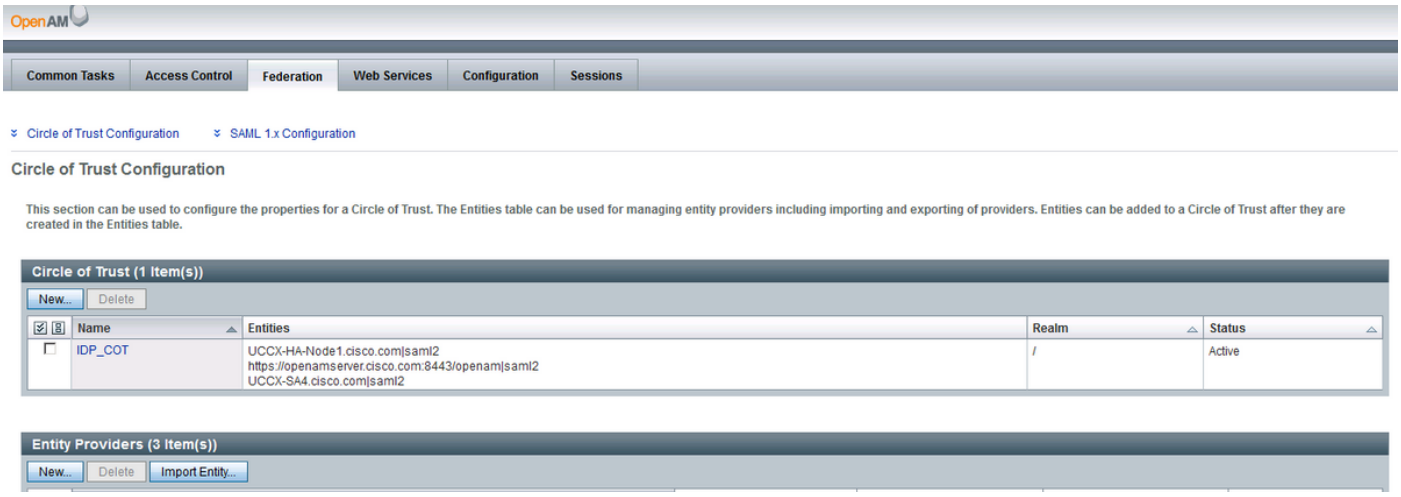
Configura chiave di firma

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.

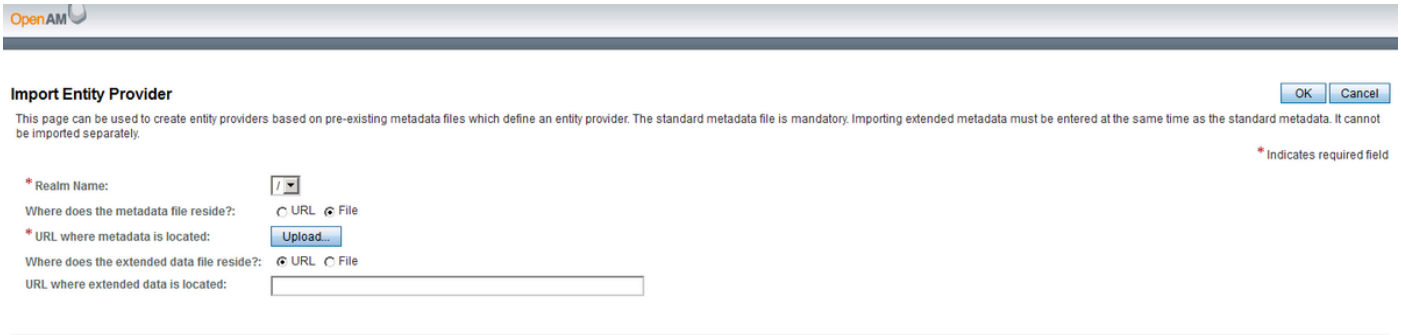


Importa entità provider di servizi

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

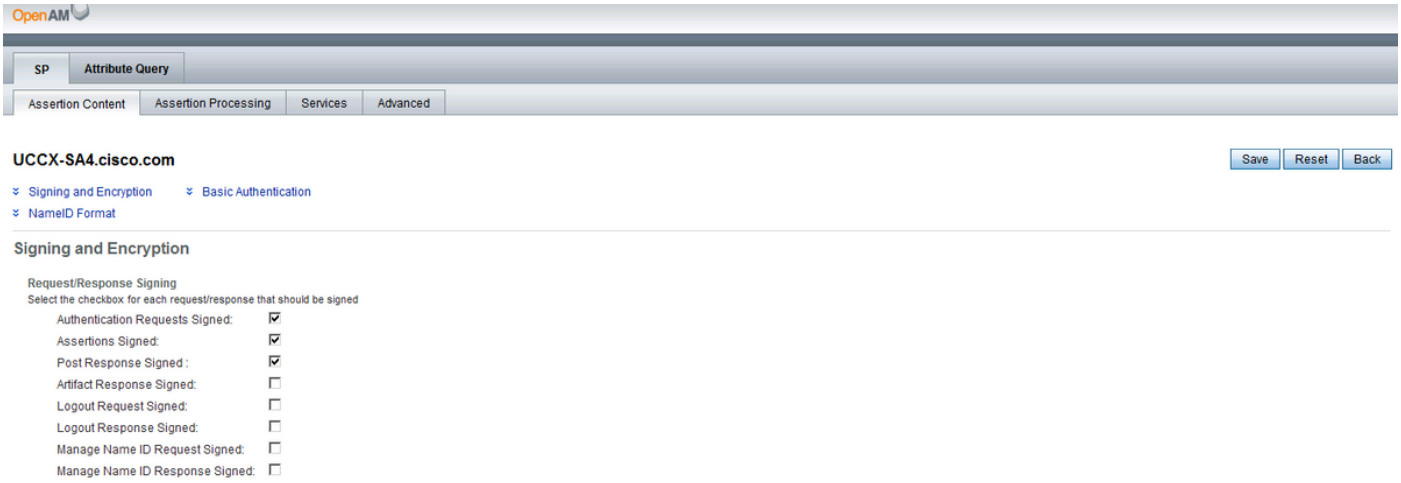


Caricare il file di entità del provider di servizi (sp.xml) e salvare la pagina.



Firma richiesta/risposta

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



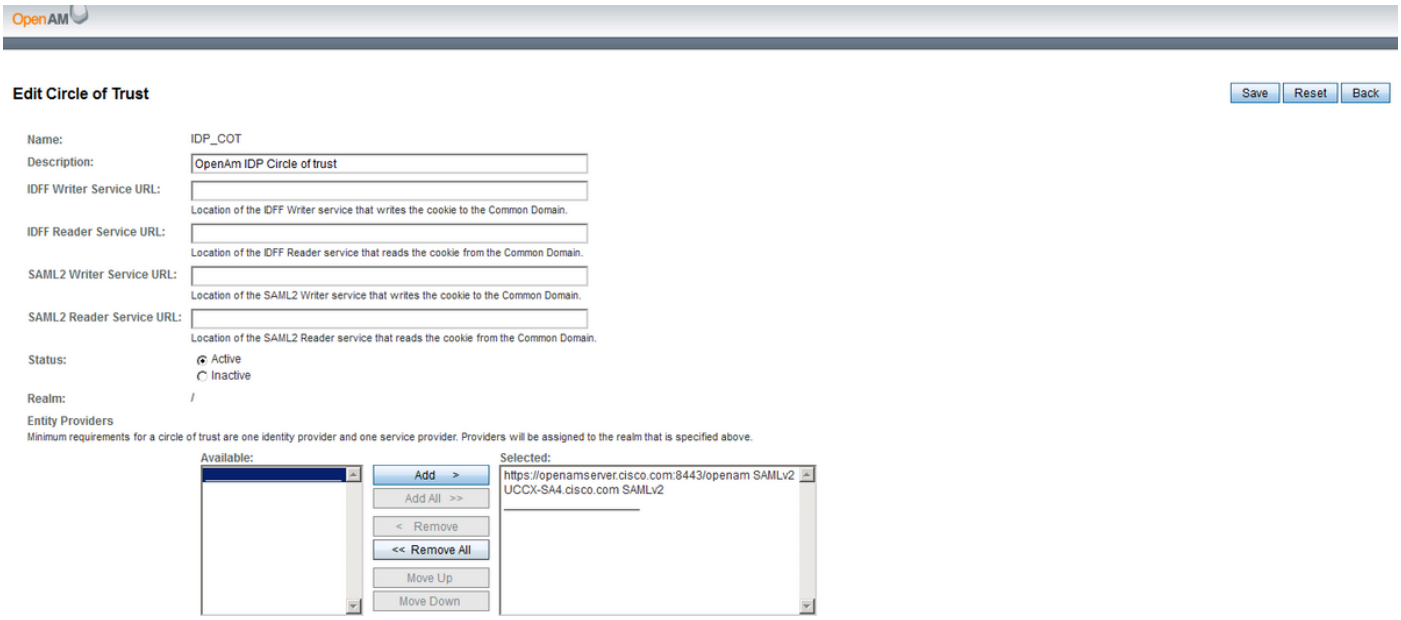
Mapping attributi

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).

> 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.



Scarica metadati OpenAM IdP

È possibile scaricare l'IdPmetadatafile del server OpenAM con l'URL [http://<FQDN di OpenAM>:8080/openam/saml2/jsp/exportmetadata.jsp?entityid=http://<FQDN di 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
```

Esempio di XML dei metadati OpenAM

```
<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>
```

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).