

# 為Cisco Identity Service(IdS)安裝和配置 OpenAM身份提供程式(IdP)以啟用SSO

## 目錄

---

### [簡介](#)

### [必要條件](#)

[需求](#)

[採用元件](#)

### [安裝](#)

[系統要求](#)

[作業系統](#)

[Java環境](#)

[Web應用程式容器要求](#)

[支援的瀏覽器](#)

[資料儲存要求](#)

[最低硬體要求](#)

### [安裝](#)

[獲取OpenAM軟體](#)

[前提條件](#)

[安裝OpenAM Web應用程式](#)

[運行OpenAM服務](#)

### [設定](#)

[OpenAM配置器](#)

[將OpenAM配置為IdP](#)

[信任配置循環](#)

[建立託管身份提供程式](#)

[配置簽名金鑰](#)

[匯入服務提供商實體](#)

[請求/響應簽名](#)

[屬性對映](#)

[編輯信任圈](#)

[下載OpenAM IdP後設資料](#)

[SSO的進一步配置：](#)

---

## 簡介

本檔案介紹OpenAM身份提供程式(IdP)上啟用單一登入(SSO)的配置。

Cisco IdS部署模式

產品	部署
UCCX	共住者

PCCE	與CUIC ( 思科統一情報中心 ) 和LD ( 即時資料 ) 共存
UCCE	與CUIC和LD共駐以進行2k部署。 獨立式，適用於4k和12k部署。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco Unified Contact Center Express(UCCX)版本11.6或Cisco Unified Contact Center Enterprise版本11.6或Packaged Contact Center Enterprise(PCCE)版本11.6 ( 如果適用 )。

附註：本檔案會引用有關思科識別服務(IdS)和身份提供者(IdP)的組態。文檔在螢幕截圖和示例中引用了UCCX，但是在Cisco Identification Service(UCCX/UCCE/PCCE)和IdP方面配置相似。

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 安裝

附註：本文檔引用OpenAM 10.0.1版作為SSO資格認證的一部分

### 系統要求

作業系統	Java環境	Web應用程式容器要求	支援的瀏覽器	資料儲存要求	最低硬體要求
<ul style="list-style-type: none"> <li>• Microsoft Windows Server 2003、</li> </ul>	OpenAM版本10.0.1要求使用Java Development Kit 1.6 ( 至少1.6.0_10 )。由	<ul style="list-style-type: none"> <li>• Apache Tomcat 6.0.x、7.0.x</li> </ul>	<ul style="list-style-type: none"> <li>• 鉻和鉻16及更高版本</li> <li>• Firefox 3.6及更高版本</li> </ul>	<ul style="list-style-type: none"> <li>• ForgeRock OpenDJ</li> <li>• Microsoft Active</li> </ul>	<ul style="list-style-type: none"> <li>• 用於OpenAM 1 GB可RAM</li> </ul>

<p>2008 R2</p> <ul style="list-style-type: none"> <li>Linux 2.6、3.0</li> <li>Oracle Solaris 10</li> </ul>	<p>於進行了安全修復，ForgeRock建議您至少使用1.6.0_27版。ForgeRock已主要通過Oracle Java SE JDK測試此版本的OpenAM。OpenAM Java SDK支援Java Development Kit 1.5或1.6。</p>	<ul style="list-style-type: none"> <li>GlassFish v2</li> <li>JBoss企業應用平台4.x、5.x</li> <li>JBoss應用伺服器7.x</li> <li>碼頭7</li> <li>Oracle WebLogic Server 11g</li> <li>Oracle WebLogic Server 12c</li> </ul> <p>如果以非root使用者身份運行，則Web應用程式容器必須能夠寫入其自己的主目錄（OpenAM在其中儲存配置檔案）。</p>	<ul style="list-style-type: none"> <li>Internet Explorer（版本7及更高版本）</li> <li>Safari 5及更高版本</li> </ul>	<p>Directory</p> <ul style="list-style-type: none"> <li>IBM Tivoli目錄伺服器</li> <li>OpenDS</li> <li>Oracle Directory Server企業版</li> </ul>	<p>您可以在支援需軟體組合的何硬體上部署OpenAM。</p>
---	---	---	--	--	----------------------------------

## 安裝

### 獲取OpenAM軟體

- 從 <https://backstage.forgerock.com/downloads/OpenAM/OpenAM%20Enterprise/10.0.1/OpenAM%2010.0.1> 下載OpenAM 10.0.1版
- 對於每個版本的OpenAM核心服務，您可以將整個軟體包下載為.zip存檔，僅下載OpenAM .war檔案，僅下載管理工具作為.zip存檔
- 解壓縮整個軟體包的存檔檔案後，您將獲得一個包含自述檔案的opensso目錄、一組許可證檔案和目錄

### 前提條件

確保在安裝之前，您擁有OpenAM核心服務所需的必備軟體，

- Java 6運行時環境
- 安裝Apache Tomcat作為Web應用程式容器
- OpenAM核心服務要求最小的Java虛擬記憶體(JVM)堆大小為1 GB，永久生成大小為256 MB。在tomcat應用程式伺服器啟動之前在catalina檔案中設定JAVA\_OPTS時應用JVM選項 — `-Xmx1024m -XX:MaxPermSize=256m`

示例集 `JAVA_OPTS=%JAVA_OPTS% -Xmx1024m -XX:MaxPermSize=256m -Xms512m`

- 安裝Microsoft Active Directory作為具有少量使用者的資料儲存。

## 安裝OpenAM Web應用程式

`deployable-war/opensso.war`檔案包含opensso目錄下的所有OpenAM伺服器元件和示例。

在Tomcat容器上部署OpenAM

將`opensso.war`檔案複製到儲存tomcat Web應用程式的目錄。將`opensso.war`檔案重新命名為`openam.war`。重新啟動tomcat服務。

在瀏覽器中驗證初始配置螢幕，網址為<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.

## 運行OpenAM服務

Openam是一個託管在tomcat伺服器中的簡單Web應用程式。因此，只需啟動tomcat伺服器，即可訪問OpenAM Web服務。

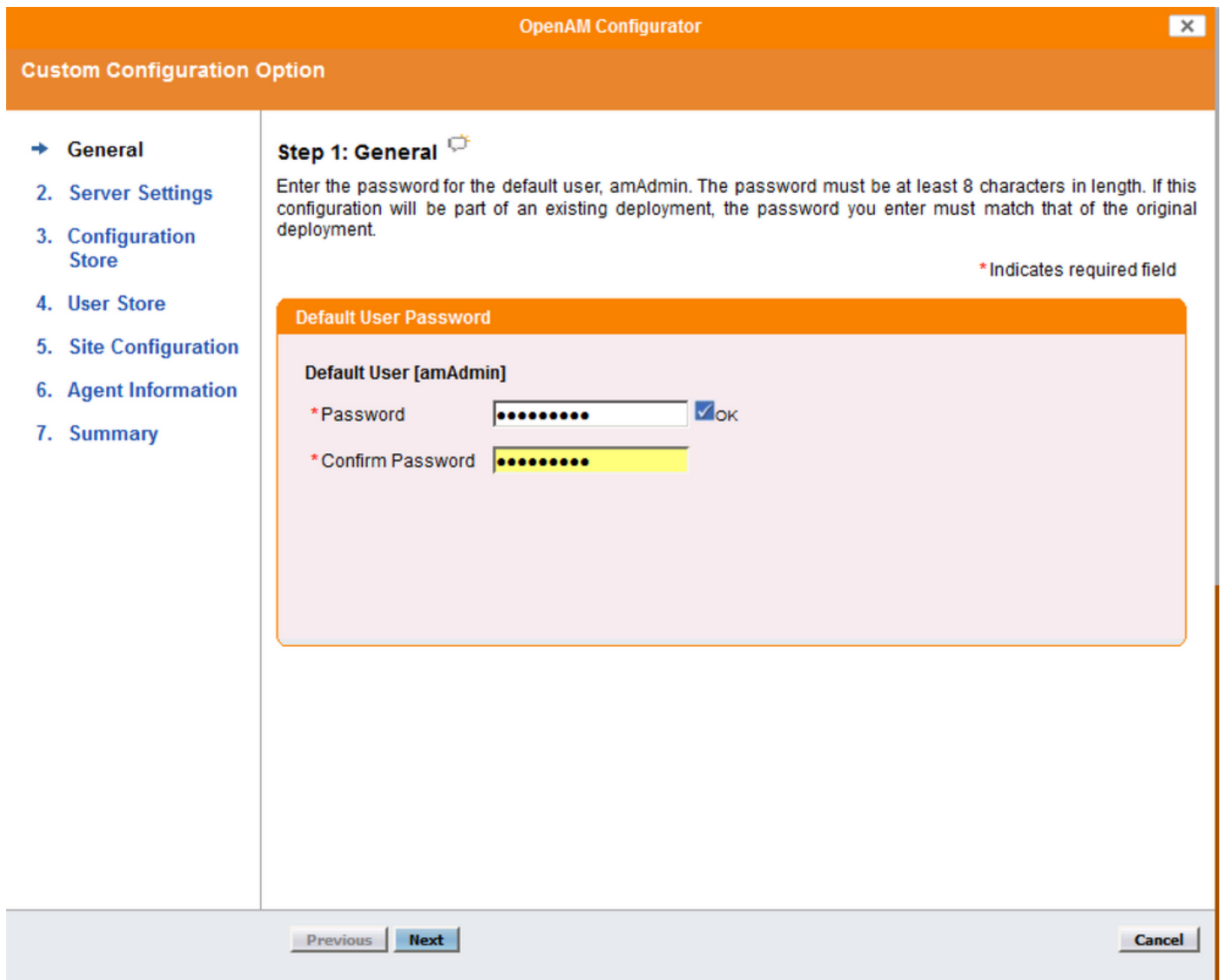
## 設定

## OpenAM配置器

OpenAM自定義配置過程允許輕鬆設定許多常見配置選項，因此在配置之前投入更多精力，可以節省以後所需的配置步驟。

### 常規設定

按一下Create New Configuration選項，然後選擇預設管理員帳戶(amAdmin)的密碼。密碼的長度至少需要為8個字元。



OpenAM Configurator

Custom Configuration Option

→ General

2. Server Settings

3. Configuration Store

4. User Store

5. Site Configuration

6. Agent Information

7. Summary

**Step 1: General**

Enter the password for the default user, amAdmin. The password must be at least 8 characters in length. If this configuration will be part of an existing deployment, the password you enter must match that of the original deployment.

\* Indicates required field

**Default User Password**

Default User [amAdmin]

\* Password   OK

\* Confirm Password

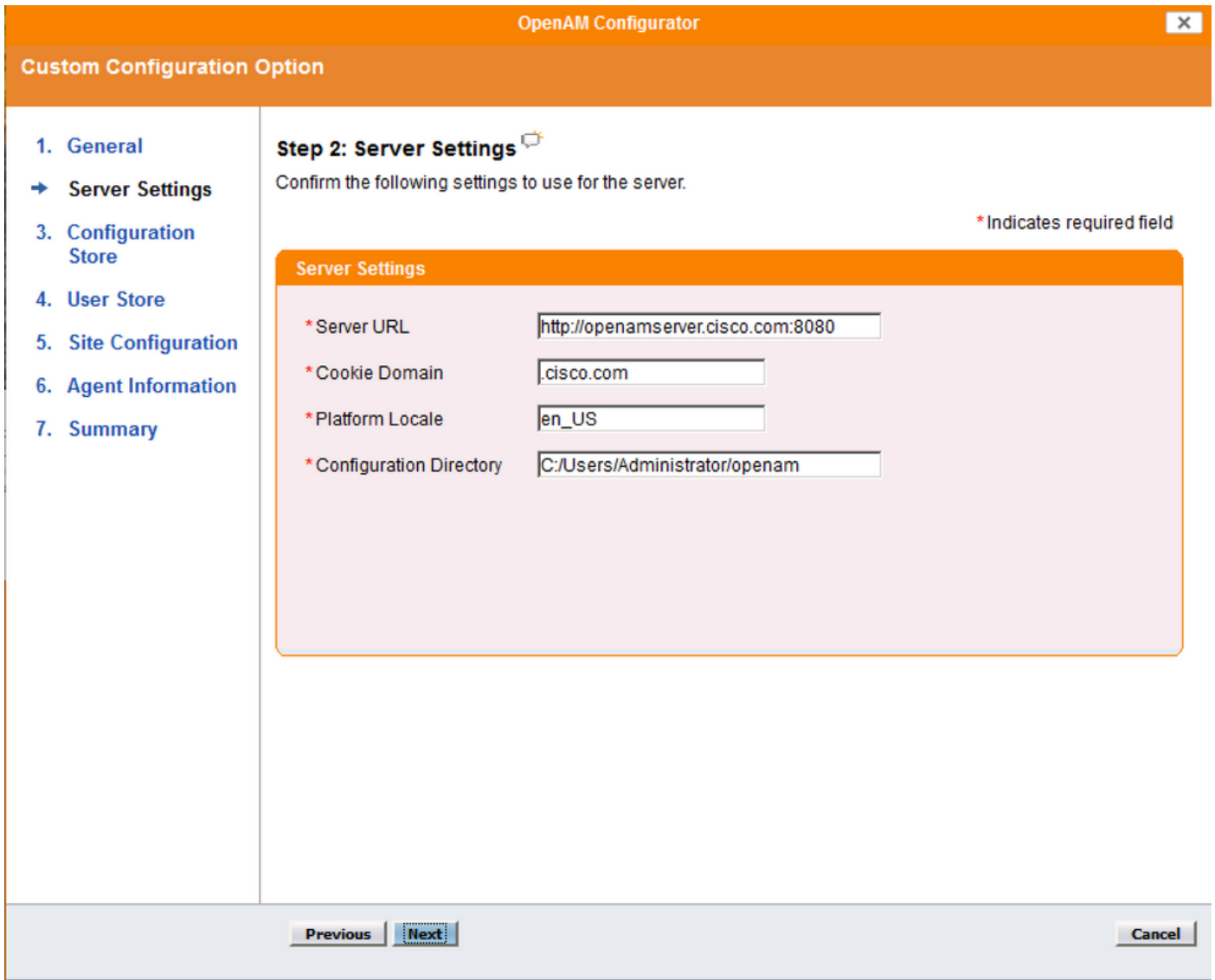
Previous Next Cancel

一旦輸入了兩次有效密碼，就會出現「next ( 下一步 )」按鈕，配置可以繼續。

### 伺服器設定

預設情況下，伺服器URL是伺服器的完全限定域名。

附註：運行Apache Tomcat的使用者必須擁有對Configuration目錄的寫入訪問許可權。因此~/openam/config適用於此目的。支援的平台語言環境為en\_US ( 英語 )、de ( 德語 )、es ( 西班牙語 )、fr ( 法語 )、ja ( 日語 )、zh\_CN ( 簡體中文 ) 或zh\_TW ( 繁體中文 )。



配置資料儲存設定

對於單伺服器配置，無需更改這些設定。

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

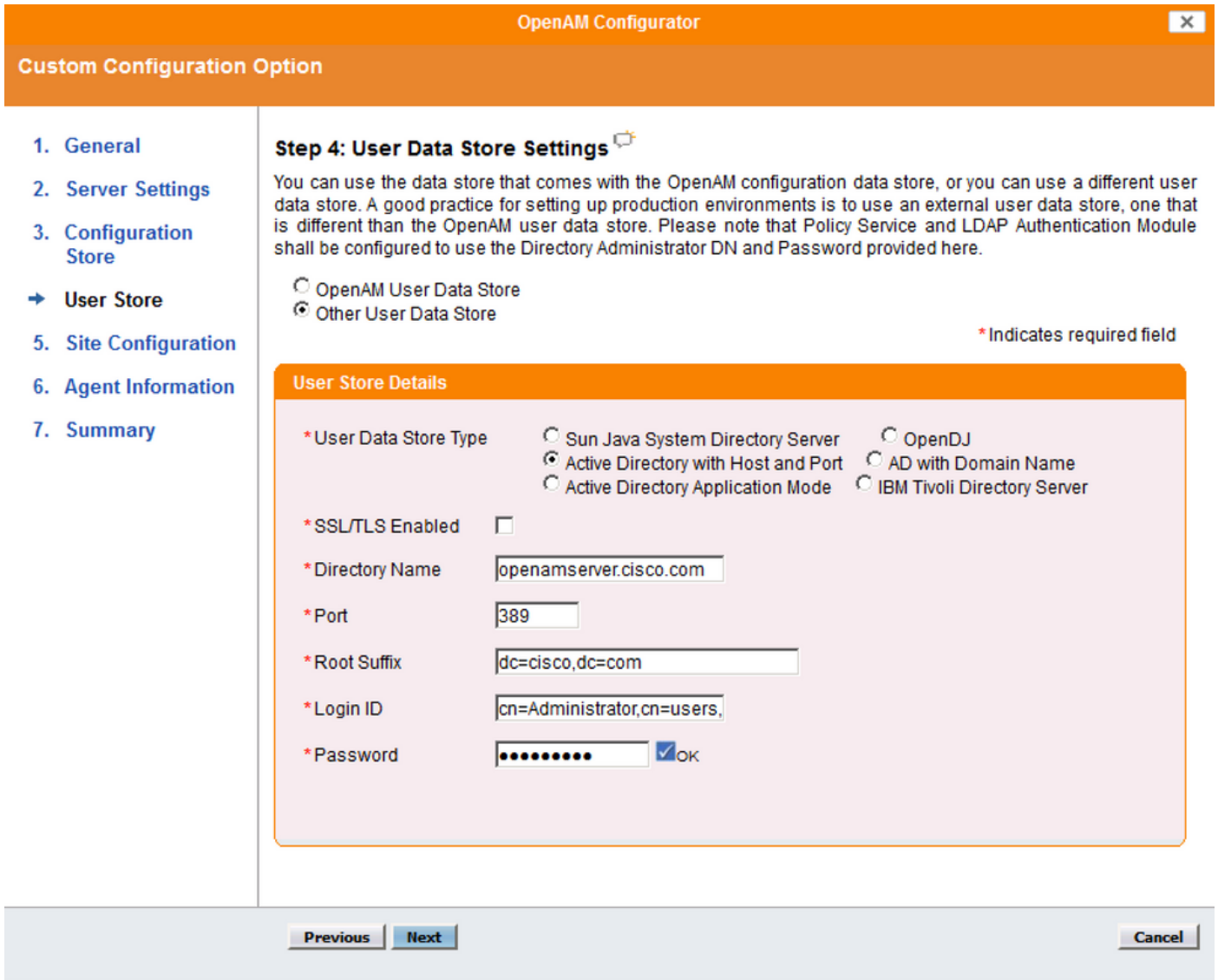
\* Encryption Key

\* Root Suffix

Previous Next Cancel

使用者資料儲存設定

使用者資料儲存設定將OpenAM連線到Microsoft Active Directory資料儲存區。



- 使用者資料儲存型別：帶有主機和埠的Active Directory
- 已啟用SSL/TLS:未啟用
- 目錄名稱：<AD伺服器的域名>
- 連接埠：389
- 根字尾：dc=cisco , dc=com
- 登入ID:cn=<AD使用者名稱>,cn=users , dc=cisco , dc=com
- 密碼：<AD使用者密碼>

附註：在正確指定所有設定並且成功連線到Active Directory例項之前，配置器不會提供繼續操作的選項。

#### 站點配置

在「站點配置」螢幕中，可以將OpenAM設定為站點的一部分，在此站點中，負載將在多個OpenAM伺服器之間均衡。對於第一次OpenAM安裝，請接受預設值。

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

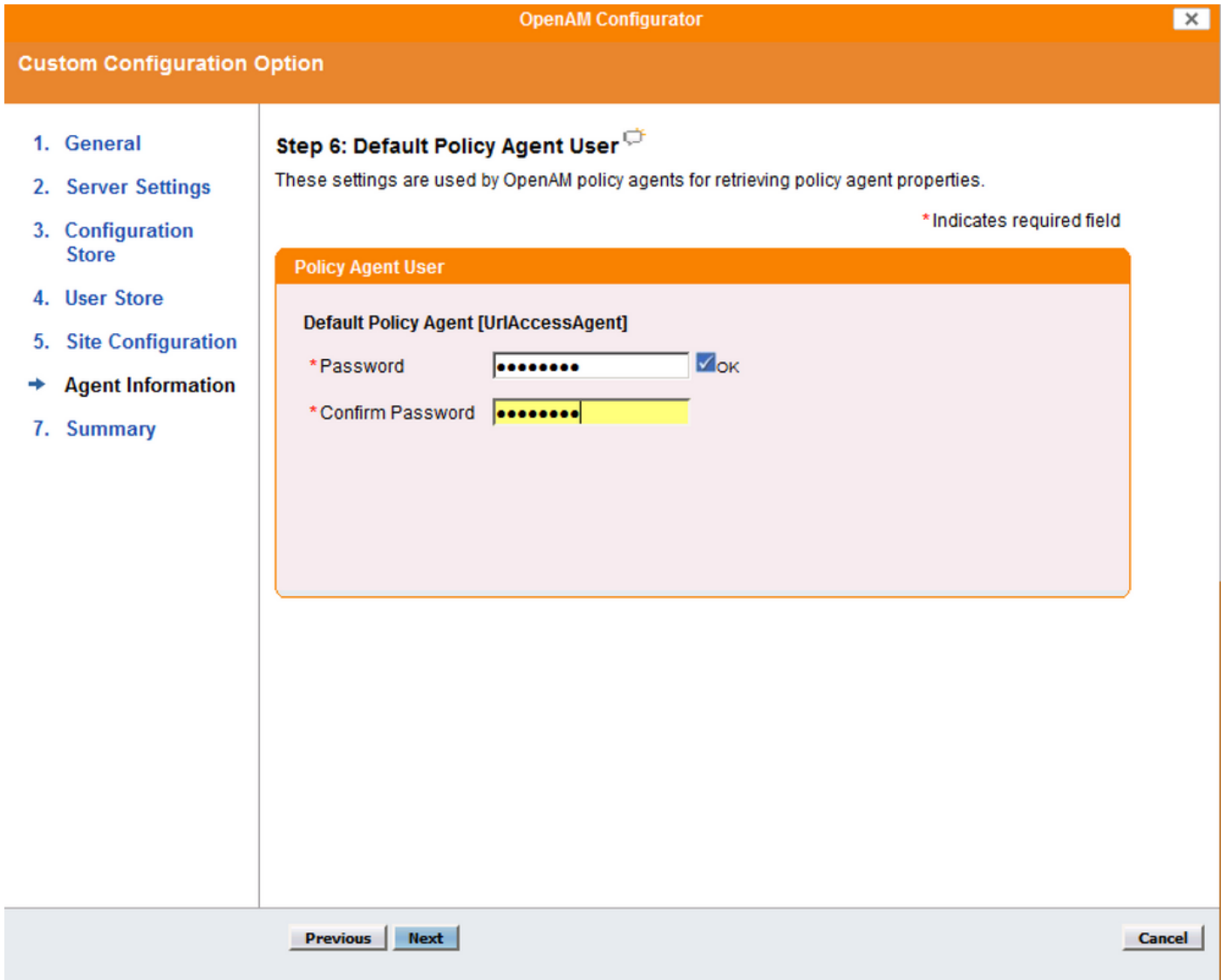
This is the first instance of OpenAM, and no site configurations currently exist. To create a new site configuration, provide the following information

\* Site Name

\* Load Balancer URL

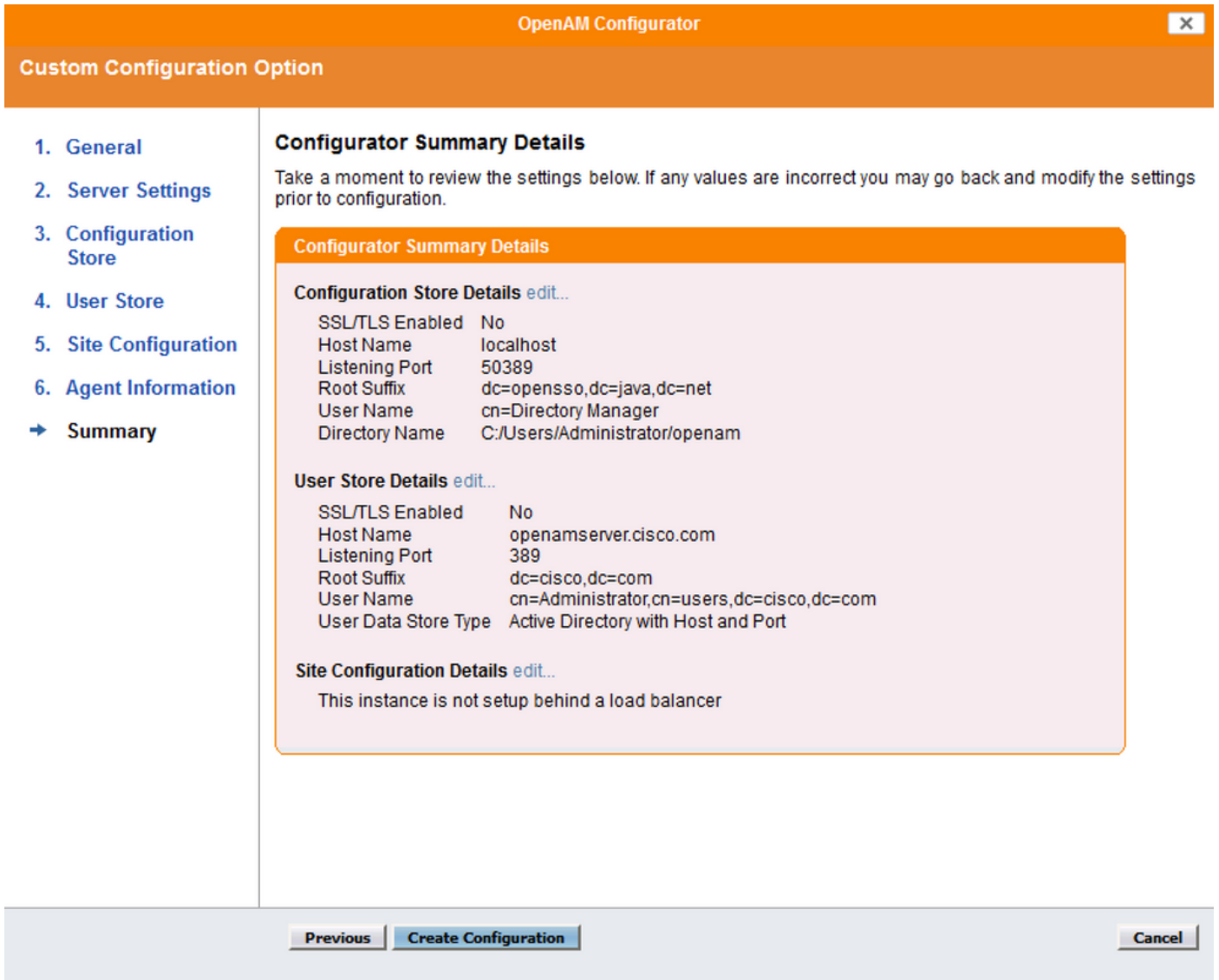
座席資訊

在Agent Information ( 代理資訊 ) 螢幕中，提供至少8個字元的密碼，以供策略代理連線到 OpenAM時使用。



摘要

檢視資訊並按一下Create Configuration



### 配置進度

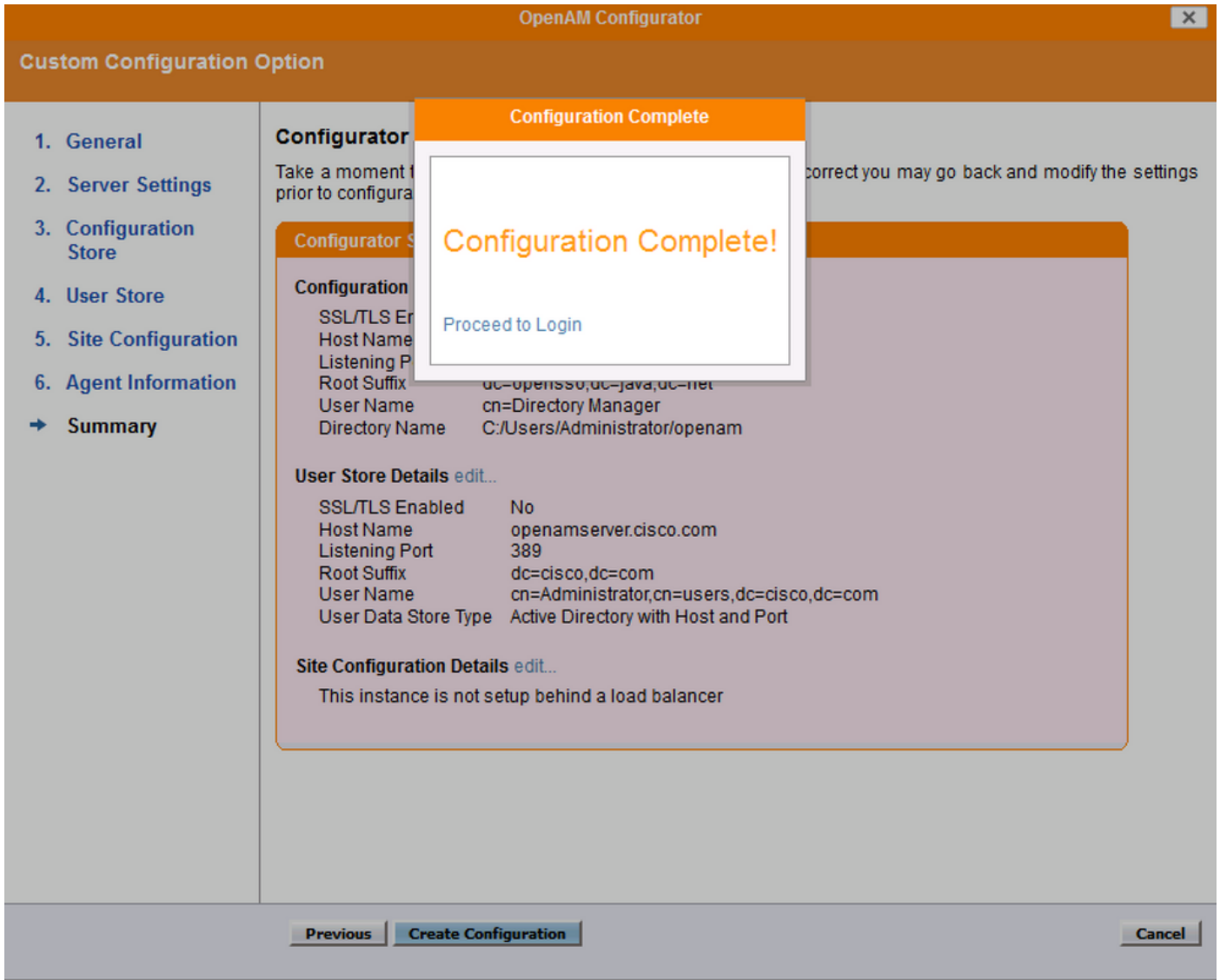
配置進度螢幕顯示安裝進度。此螢幕上的所有輸出和錯誤都會寫入檔案：  
~/openam/config/install.log。

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...
```

配置完成



## 將OpenAM配置為IdP

- 按一下Proceed to Login or Access through URL <http://<FQDN of OpenAM>:8080/openam>，然後以OpenAM管理員身份登入
- 首次訪問OpenSSO Enterprise時，系統會將您引導至配置器以執行OpenSSO Enterprise初始配置
- 選擇預設配置
- 您需要配置OpenAMserver的密碼
- 配置密碼並登入到OpenAM伺服器UI

## 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.

## 信任配置循環

導航到「聯合」頁籤，然後按一下「信任圈」部分下的「新建」按鈕

The screenshot shows the OpenAM Administration Console interface. The 'Federation' tab is selected in the top navigation bar. Below it, there are sub-tabs for 'Circle of Trust Configuration' and 'SAML 1.x Configuration'. The 'Circle of Trust Configuration' section is active, displaying a table with one item and buttons for 'New...' and 'Delete'.

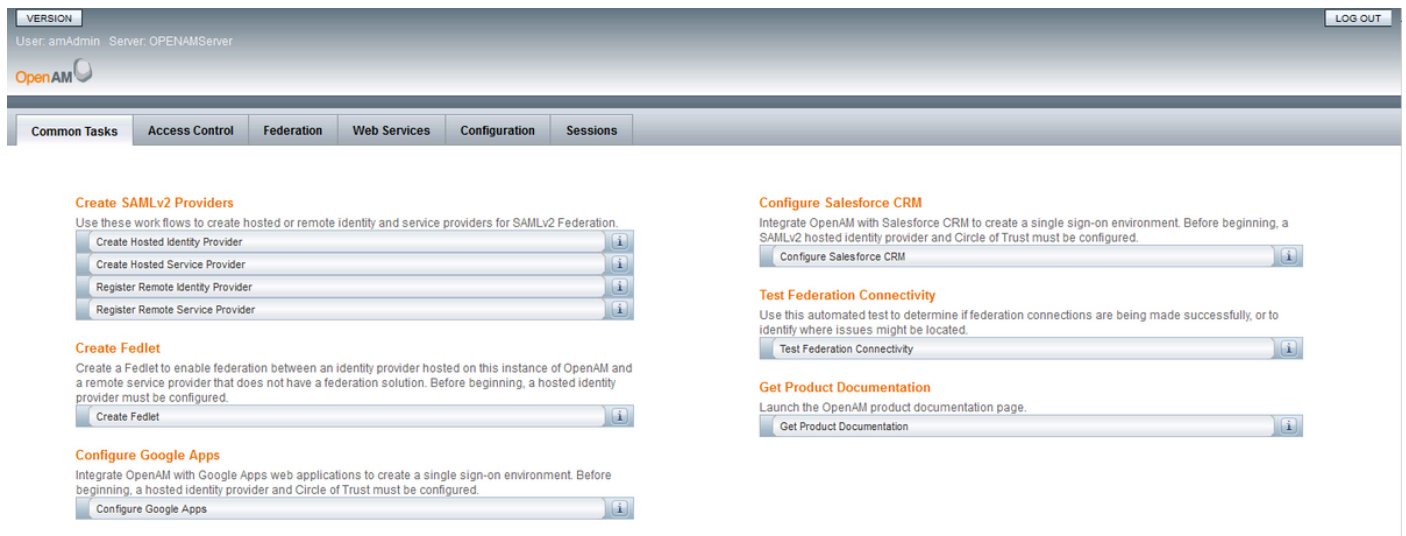
為IdP Circle of trust建立具有唯一名稱的信任圈，然後按一下「確定」

The screenshot shows the 'Create Circle of Trust' form. The 'Name' field is filled with 'IDP\_COT'. The 'Status' is set to 'Active'. The 'Realm' is set to 'I'. The form includes fields for IDFF and SAML2 Writer and Reader Service URLs, with descriptive text below each. There are 'OK' and 'Cancel' buttons at the top right, and a note that '\*' indicates a required field.

附註：服務提供商和IdP必須位於同一信任圈(CoT)中，SAML SSO才能正常工作。

## 建立託管身份提供程式

導航到「常見任務」頁籤，然後點選「建立託管身份提供程式」並建立託管的IdP（保留預設配置值並儲存設定）。



VERSION

User: amAdmin Server: OPENAMServer

LOG OUT

OpenAM

Common Tasks Access Control Federation Web Services Configuration Sessions

**Create SAMLv2 Providers**  
Use these work flows to create hosted or remote identity and service providers for SAMLv2 Federation.

- 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.

- 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.

- 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.

- 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.

- Test Federation Connectivity

**Get Product Documentation**  
Launch the OpenAM product documentation page.

- Get Product Documentation

此處列出了之前建立的信任圈



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: IDP\_COT

## 配置簽名金鑰

導航到聯合頁籤，然後按一下在實體提供程式部分中新增的託管身份提供程式。導航到斷言內容部分，然後在證書別名部分下將Signing欄位值配置為test。這是將用於對SAML斷言進行簽名的證書

。

- ✖ 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.

## 匯入服務提供商實體

導航到聯合頁籤，然後在實體提供程式部分下按一下匯入實體..... 按鈕。

上載服務提供商的實體檔案(sp.xml)並儲存頁面。

## 請求/響應簽名

按一下匯入的實體並啟用請求/響應簽名

The screenshot shows the OpenAM configuration interface for the service 'UCCX-SA4.cisco.com'. The 'Attribute Query' tab is selected, and the 'Advanced' sub-tab is active. The 'Signing and Encryption' section is expanded, showing a list of request and response signing options. The following table summarizes the checked and unchecked options:

Request/Response	Checked
Authentication Requests Signed	<input checked="" type="checkbox"/>
Assertions Signed	<input checked="" type="checkbox"/>
Post Response Signed	<input checked="" type="checkbox"/>
Artifact Response Signed	<input type="checkbox"/>
Logout Request Signed	<input type="checkbox"/>
Logout Response Signed	<input type="checkbox"/>
Manage Name ID Request Signed	<input type="checkbox"/>
Manage Name ID Response Signed	<input type="checkbox"/>

## 屬性對映

導航到斷言處理，然後根據Directory和OpenAM設定新增uid 和user\_principal 的對映屬性。按一下 Save。

The screenshot shows the OpenAM configuration interface for the service 'UCCX-SA4.cisco.com'. The 'Attribute Mapper' section is expanded, showing a list of current values for the attribute map. The following table summarizes the current values:

Current Value
uid=sAMAccountName
user_principal=userPrincipalName

Below the current values, there is a 'New Value' input field and an 'Add' button. A 'Remove' button is also present next to the current values.

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.

註: 屬性uid 和user\_principal 都是強制的 — 因為服務提供商(SP)藉助這些屬性標識經過身份驗證的使用者的身份。此外，請確保屬性sAMAccountName和userPrincipalName也對映在 Active Directory使用者屬性的屬性編輯器中。

## 編輯信任圈

導航到聯合頁籤，然後按一下已新增的信任圈，並確保將IdP ( OpenAm伺服器 ) 和服務提供商實體從實體提供程式部分下的可用部分移動到選定部分。這會將IdP和服務提供商分配到同一個信任圈中

。



```
<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>
            MIICcTCCAdggAwIBAgIEEe4zDANBgkqhkiG9w0BAQUFAADB9MQswCQYDVQQGEwJ1JESMBAGA1UE
            CBMja2FybmF0YWhhMHRlEAYDVQQHEw11Yw5nYXVvcmluZjAUBG9NVBAoTDW5pc2NvIHNSc3RlbXN1
            DTALBgNVBAsTBGNjYnUxZmZAdBgNVBAMTFm9wZXIzLjE5aXNjby5jb20wHhcNMjYxMjA3
            MDCyMjUyMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYx
            MRIwEAYDVQQHEw11Yw5nYXVvcmluZjAUBG9NVBAoTDW5pc2NvIHNSc3RlbXN1DTALBgNVBAsTBGNj
            YnUxZmZAdBgNVBAMTFm9wZXIzLjE5aXNjby5jb20wDQYJKoZIhvcNAQEBBQADgY8A
            MIGJAoGBAKvnlKou0mAl+V2YdfyuiFKQWkdM6E0c/1fmig94cGdNXxw13KxzjUF2Vv4r364rTFi
            73eIduF6e1/M481ECYed24LxKpgcSFm1jAbDQ17Ae0gyzPmWQJODf850guGVQhZUUt0RKYYP/d0
            bgvaRrWxGIvoLRJ+8ky+zLV0T7nAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAh7MNSup7MOHYCLF1
            i7hK99EMUJxemyvAvAjea85TH7Ba5d0Z1+R/bnXTS/9/pBET15knuKd+Q59P19je2W7L36vFHoF1Q
            jLLAGnPJ0VEm0tImcGZGc3m77Thlqn0LIcyjnrXclVQ10m75yfiMFeeHdFPgBuzTsXjkIKjmHF9
            +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>
```

## SSO的進一步配置：

本文檔從SSO的IdP方面描述了要與Cisco身份服務整合的配置。有關詳細資訊，請參閱各個產品配置指南：

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

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。