

安裝和配置Cisco身份服務的PingFederate身份提供程式以啟用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](#)

[終端使用者支援的瀏覽器](#)

[管理控制權支援的瀏覽器](#)

[資料儲存整合](#)

[\(用於使用者屬性查詢\)](#)

[最低硬體要求](#)

[最低硬體建議](#)

[安裝](#)

[使用分發ZIP檔案安裝PingFederate](#)

[使用分發EXE檔案安裝PingFederate](#)

[首次啟動PingFederate](#)

[初始安裝嚮導](#)

[接受許可協定](#)

[PingOne帳戶](#)

[授權](#)

[基本資訊](#)

[啟用角色](#)

[身份提供程式配置](#)

[管理員帳戶](#)

[確認](#)

[完成](#)

[配置PingFederate](#)

[伺服器配置](#)

[數位簽署和可擴充標籤語言\(XML\)解密金鑰和憑證](#)

[資料儲存](#)

[密碼憑據驗證程式](#)

[伺服器設定](#)

[身份提供程式\(IdP\)配置](#)

[介面卡](#)

[SP連線](#)

[匯出PingFederate後設資料](#)

[後設資料匯出](#)

[後設資料模式](#)

[連線後設資料](#)

[後設資料簽名](#)

[匯出與摘要](#)

[後設資料示例](#)

[疑難排解](#)

[SSO的進一步配置](#)

簡介

本檔案介紹PingFederate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)。
- Windows伺服器上安裝的PingFederate

附註：本文檔引用有關思科身份識別服務(IdS)和身份提供方(IdP)的配置。文檔在螢幕截圖和示例中引用UCCX，但是配置與思科身份識別服務(UCCX/UCCE/PCCE)和IdP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

系統要求

作業系統	Java環境	終端使用者支援的瀏覽器	管理控制檯支援的瀏覽器	資料儲存整 (用於使用者查詢)
<ul style="list-style-type: none"> • Microsoft Windows Server 2008 R2 SP(Service Pack) • Microsoft Windows Server 2012標準版 • Microsoft Windows Server 2012 R2 Datacenter • Oracle Enterprise Linux 6.5 (與 Red Hat相容的核心) • Oracle Solaris 10 • Red Hat Enterprise Linux ES 6.6 • Red Hat Enterprise Linux ES 7.0 • SUSE Linux Enterprise 	<ul style="list-style-type: none"> • Oracle Java SE Runtime Environment(Server JRE)7 update 79 (64位) • Oracle Java SE Runtime Environment(Server JRE)8 update 45 (64位) 	<ul style="list-style-type: none"> • 鉻合金 • Firefox • Internet Explorer (版本9及更高版本) • Safari 	<ul style="list-style-type: none"> • 鉻合金 • Firefox • Internet Explorer (版本9及更高版本) 	<ul style="list-style-type: none"> • Microsoft Directory R2和2012 • Oracle Directory Server企業 11g • Microsoft SQL (結構查詢語言) 佈 (2012和 2014) • Oracle資料 (10g和1 R2) • Oracle My 5.6

安裝

解壓縮分發ZIP檔案或使用特定於平台的安裝程式安裝PingFederate。

- 通過Ping身份許可證網頁(www.pingidentity.com/support-and-downloads/licensing.cfm)請求許可證 [金鑰](#)
- 確保您以適當許可權登入到系統以安裝和運行應用程式
- 驗證是否已安裝Server Java Runtime Environment(JRE)以及是否已正確設定環境和PATH變數

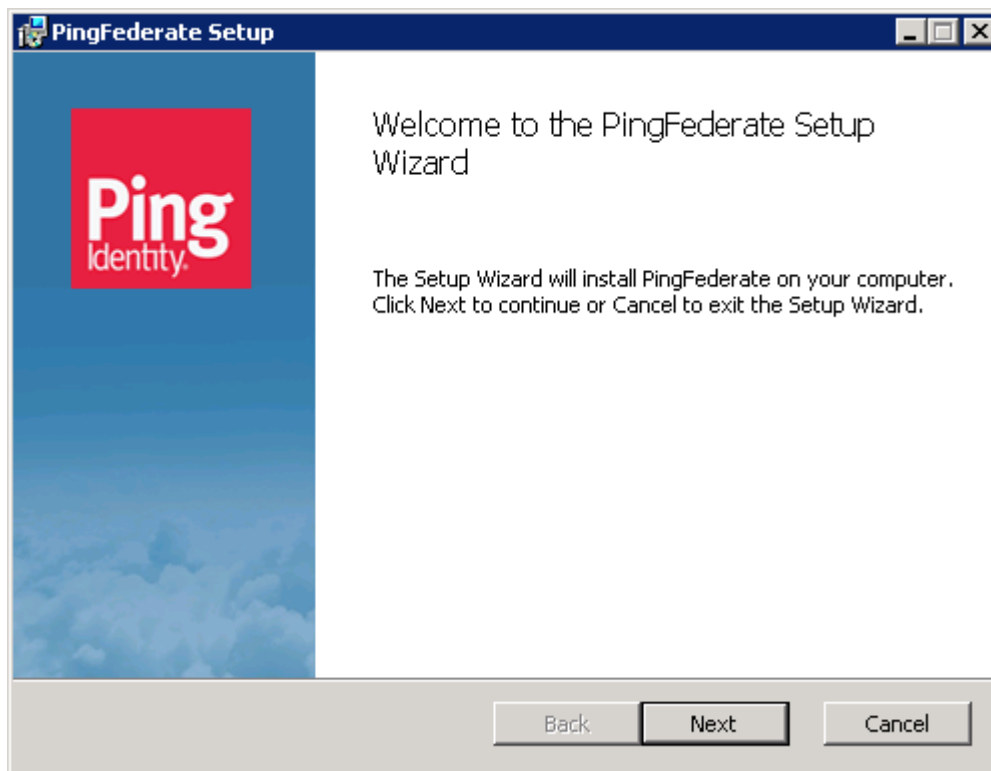
使用分發ZIP檔案安裝PingFederate

將分發ZIP檔案解壓縮到安裝目錄中。

警告：為避免將來出現自動升級問題，請不要重新命名已安裝的pingfederate資料夾。如果要在同一台電腦上安裝PingFederate的多個例項（例如，在某些伺服器群集情況下），請在不同的位置安裝每個例項，或者重新命名父資料夾，以在相同的位置安裝並行檔案結構。

使用分發EXE檔案安裝PingFederate


按兩下exe檔案，然後執行安裝步驟



PingFederate Setup

Operational Mode

Please choose which mode you'd like PingFederate to operate in.




- Standalone**
For a single node that will operate independently.
- Clustered Admin Node**
For one of several nodes in a cluster that will host the admin console.
Only one node in the cluster can operate the admin console.
- Clustered Runtime Node**
For one of several nodes in a cluster that will not host the admin console.

Back Next Cancel

PingFederate Setup

Administrative console and API

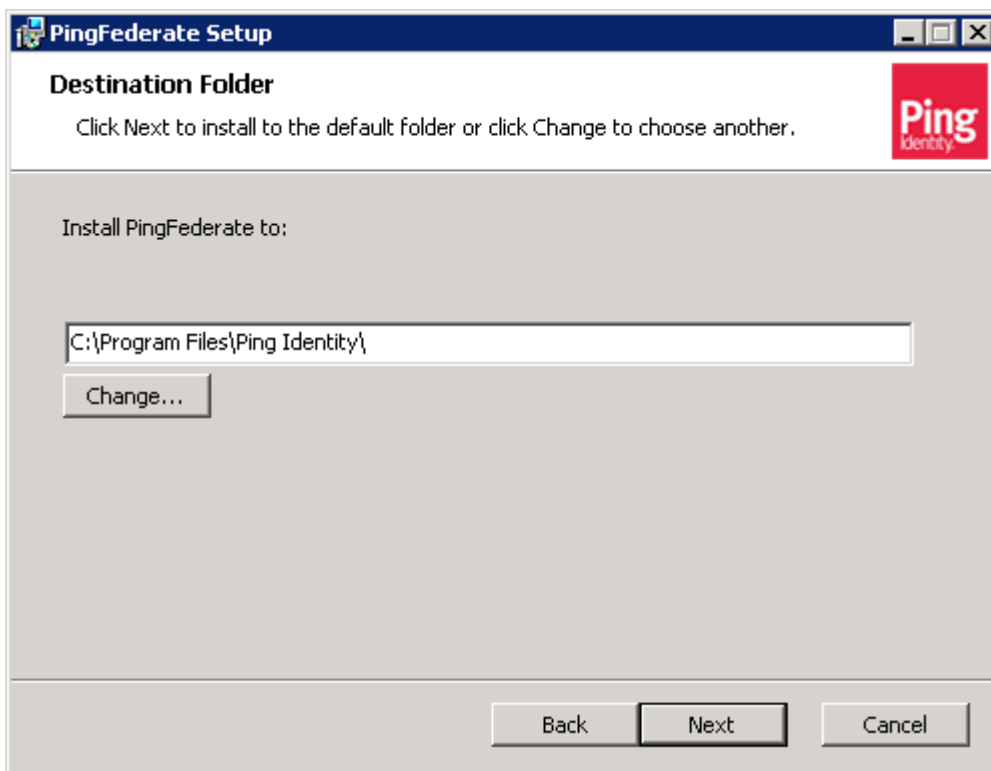
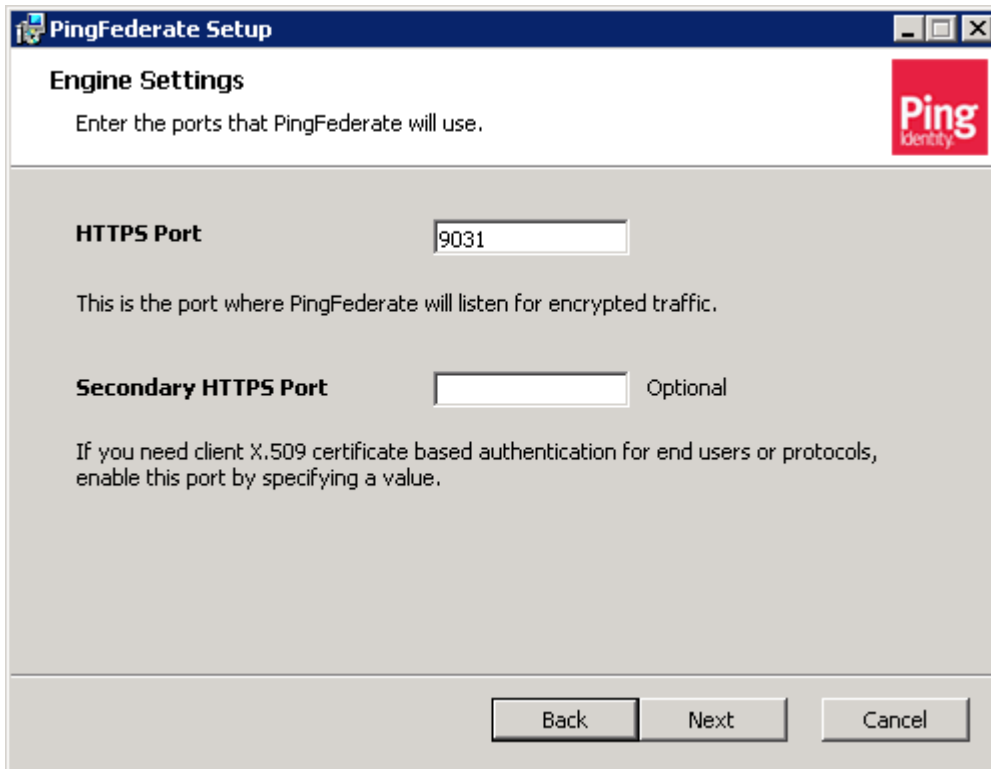
Enter the port for the admin console and API.

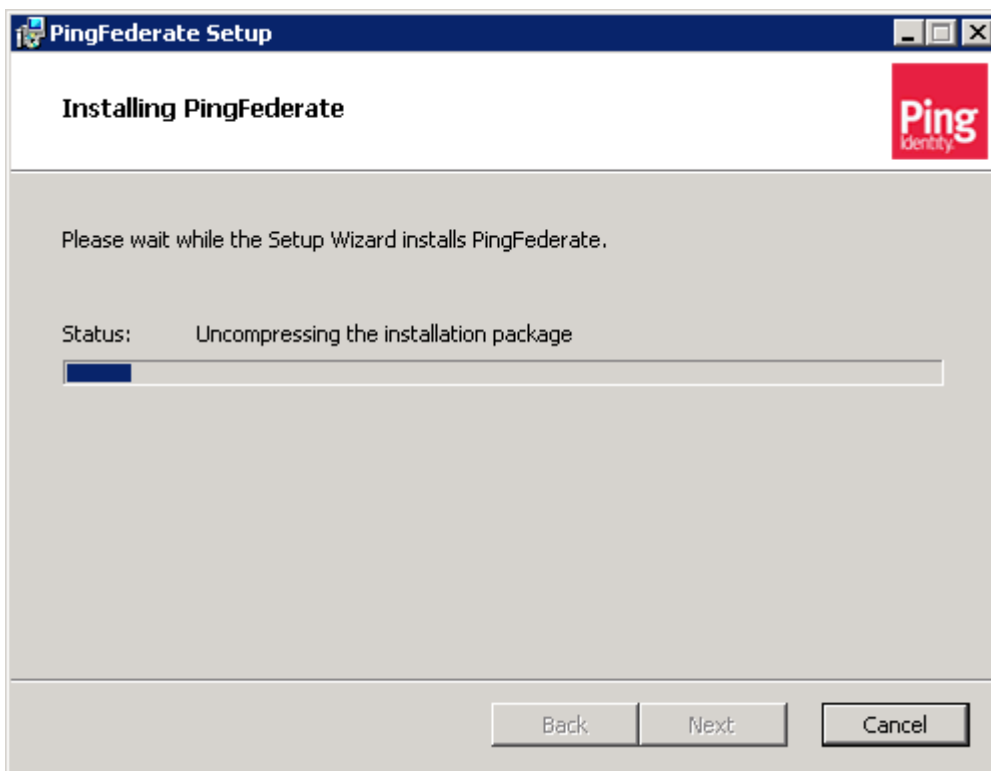
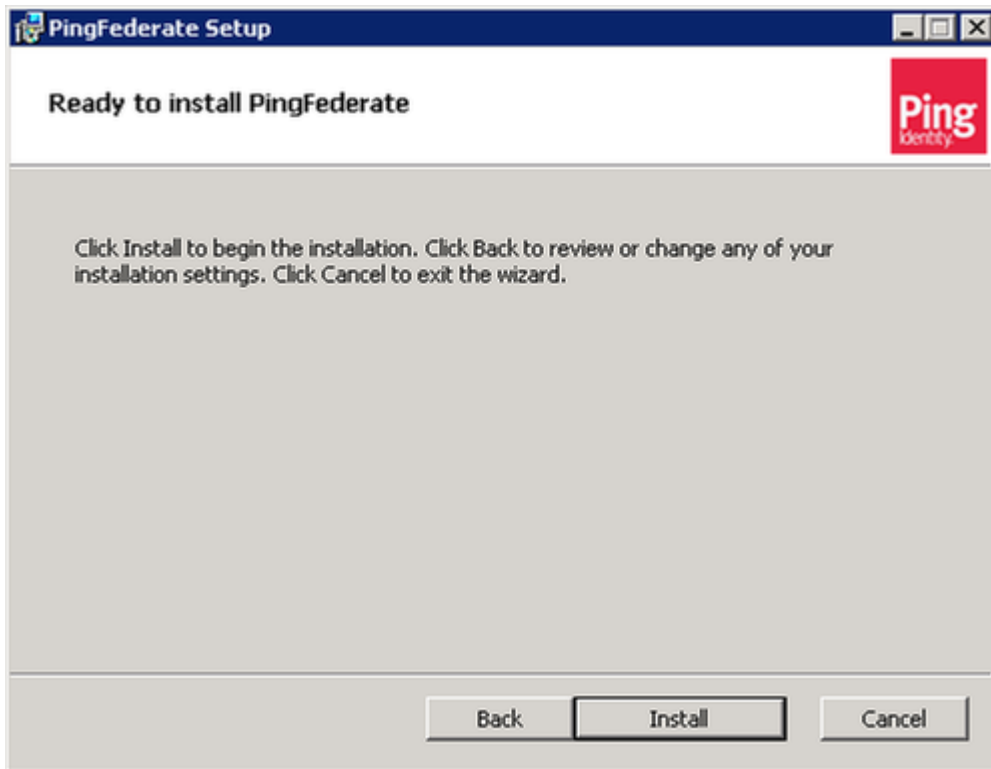


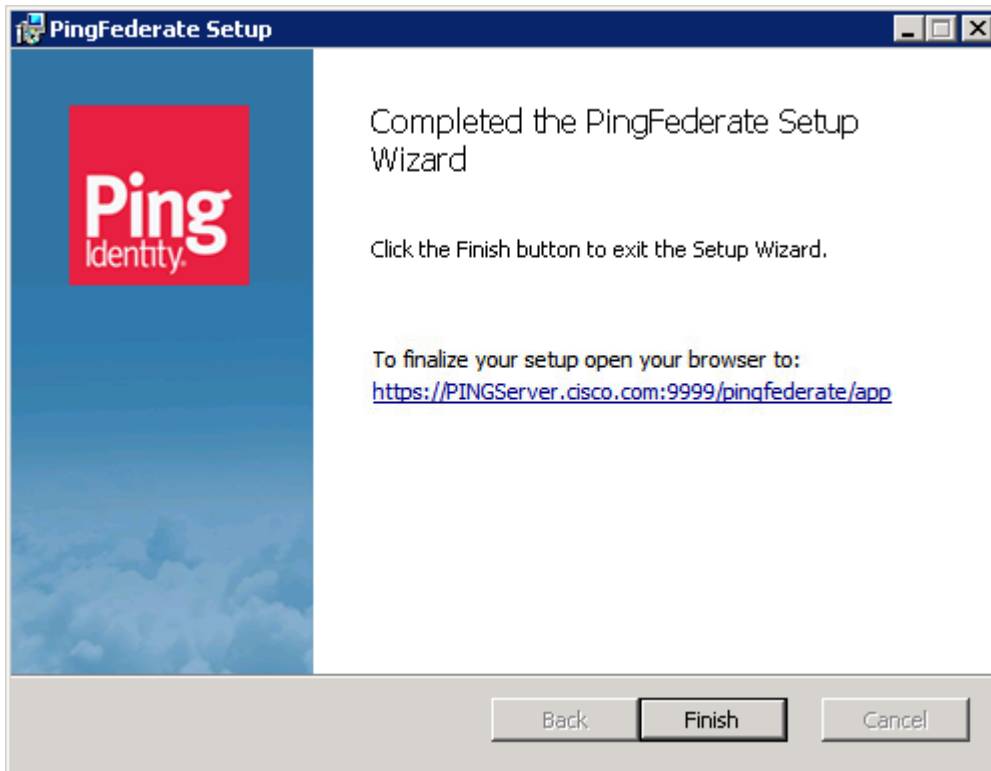
Admin HTTPS port

This is the port where PingFederate admin console and API will run.

Back Next Cancel







首次啟動PingFederate

如果使用某個平台特定的安裝程式安裝PingFederate，則將PingFederate配置為作為服務運行，並在安裝過程結束時自動啟動。

如果使用分發ZIP檔案安裝PingFederate，請運行指令碼以手動啟動PingFederate，

(Windows)<pf_install>/pingfederate/bin/run.bat
(Unix/Linux)<pf_install>/pingfederate/bin/run.sh

等待指令碼完成 — 當此消息出現在序列結尾附近時，啟動過程完成：

PingFederate在<X>s:<Y>ms中啟動

初始安裝嚮導

PingFederate管理員的使用者介面（管理控制檯）圍繞一個類似於嚮導的控制螢幕系統而構建。啟動PingFederate管理控制檯並使用初始設定嚮導完成身份聯合設定的配置。您還可以將PingFederate連線到PingOne，以部署強大的內部和基於雲的混合解決方案。

若要存取管理主控台：

啟動瀏覽器並導航到https://<FQHN>:9999/pingfederate/app (其中<FQHN>是安裝PingFederate的伺服器的完全限定主機名)。

註:埠號9999預設設定。這可透過PingFederate屬性變更。

接受許可協定

Ping PingFederate

License Agreement

For more information on commercial licensing or support, contact Ping Sales at sales@pingidentity.com or call toll-free 877.898.2905 (+1303.468.2882 outside North America).

SOFTWARE LICENSE AGREEMENT

THIS CLICK-THROUGH AGREEMENT (THIS "AGREEMENT") IS BY AND BETWEEN PING IDENTITY CORPORATION ("PING IDENTITY") AND THE COMPANY OR ENTITY ON WHOSE BEHALF YOU ARE EXECUTING THIS AGREEMENT ("CUSTOMER"). You represent that you have the authority to bind Customer to the terms of this Agreement. By agreeing to the terms of this Agreement or by accessing, using or installing any part of the Products, Customer expressly agrees to and consents to be bound by all of the terms of this Agreement. If Customer does not agree to any of the terms of this Agreement, Customer is prohibited from downloading, installing, activating or using the Products. THE EFFECTIVE DATE OF THIS AGREEMENT IS THE DATE ON WHICH CUSTOMER ACCEPTS THESE TERMS BY CLICKING "ACCEPT" OR THE SIMILARLY LABELED BUTTON INDICATING ASSENT (THE "EFFECTIVE DATE").

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. Definitions.

"Administrator" is an individual who has been granted administrative permissions by Customer to the Service in order to set-up, modify and suspend the Service, each as applicable.

"Affiliate(s)" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"API" means an application programming interface.

"Customer Data" means all electronic data or information submitted by Customer to the Service. Customer Data also includes any data of an Identity Provider and its associated employees, consultants, contractors and agents transmitted through the Service in order to access Customer's services or applications.

"Documentation" means Ping Identity's then current on-line user's manuals made generally available by Ping Identity and provided to Customer along with the Software.

"Identity Provider" means an entity that desires single sign-on capabilities into a Service Provider's services or applications.

Accept

Copyright © 2003-2019
Ping Identity Corporation
All rights reserved.
Version 8.2.2.0

PingOne 帳戶

Ping PingFederate

PingOne Account License Basic Information Enable Roles Administrator Account Confirmation Complete

Do you want to connect this identity provider with PingOne to enable cloud-based single sign-on?

Yes, Connect to PingOne

To connect this PingFederate node to your PingOne account, enter your activation key below.

[Sign on to PingOne to get your activation key.](#)

ACTIVATION KEY

No, Set Up PingFederate Without PingOne

PingFederate works with or without a PingOne connection. Continue the setup below to use PingFederate on its own.

Next

Copyright © 2003-2019
Ping Identity Corporation
All rights reserved.
Version 8.2.2.0

按一下下一步

授權

Please upload a valid PingFederate license file.

License File

No file selected

Choose file

Previous

Next

您必須從pingidentity.com購買或請求開發許可證，上傳許可證檔案，然後點選下一步

基本資訊

Welcome to PingFederate. To set up your enterprise identity bridge, let's first confirm your Base URL and Entity ID.

BASE URL

https://pingserver.disco.com:9031

ENTITY ID

pingserver

Previous

Next

設定基本URL和實體ID，然後點選下一步

啟用角色

Please select the roles you expect PingFederate to play.

- ROLES
- IDENTITY PROVIDER
 - SERVICE PROVIDER
 - OAUTH AUTHORIZATION SERVER

Previous Next

選擇IDENTITY PROVIDER並按一下Next

身份提供程式配置

If you're connecting to Active Directory, start the quick connection process below. You can configure any other user store connections after the PingFederate setup is complete.

Identity Provider Configuration

Connect to Active Directory

Previous Next

以後可以執行到Active Directory的連線，按一下下一步

管理員帳戶

Please choose a username and password for your primary administrator. You can add other administrators to PingFederate after setup is complete.

USERNAME

Administrator

PASSWORD

••••••••

CONFIRM PASSWORD

••••••••

Previous Next

設定管理員的密碼，然後按一下Next (下一步)

確認

Here is a summary of your PingFederate configuration:

BASE URL:	https://pingserver.cisco.com:9031
ENTITY ID:	pingserver
ENABLE ROLE:	Identity Provider
CREATE ACCOUNT:	Administrator

Previous Next

確認並按一下下一步

完成

Congratulations! You have successfully set up PingFederate.

What's Next?

IDENTITY PROVIDER

You can begin creating Service Provider connections to your target applications. Choose Create New under SP Connections to get started.

Done

按一下完成

配置PingFederate

伺服器配置

MAIN

IdP Configuration

Server Configuration

License Warning: Approaching expiration date

Server Configuration

SYSTEM SETTINGS

- Server Settings
- Connect to PingOne
- Data Stores
- Redirect Validation

ADMINISTRATIVE FUNCTIONS

- Metadata Export
- XML File Signatures
- Configuration Archive
- Account Management
- License Management
- Virtual Host Names

CERTIFICATE MANAGEMENT

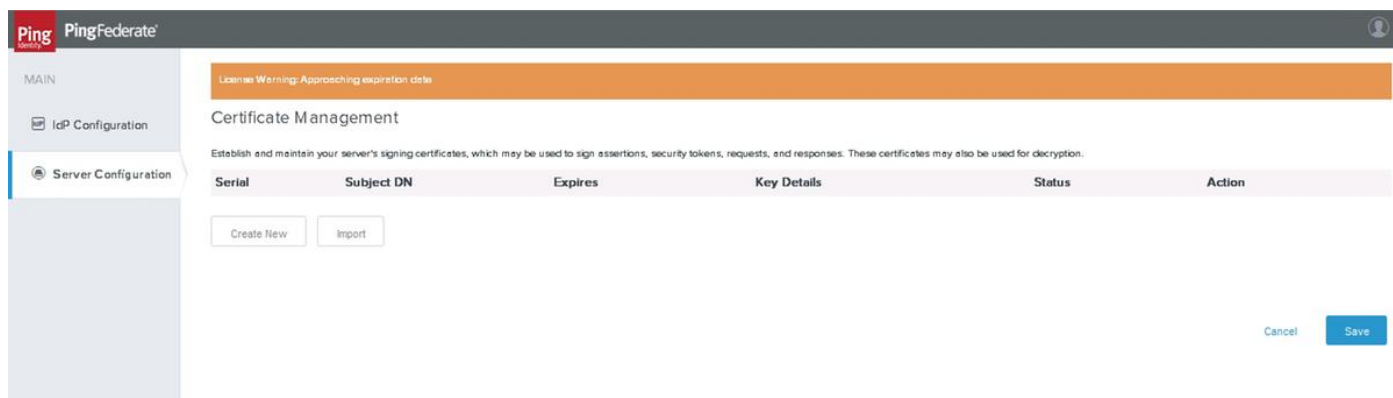
- Trusted CAs
- SSL Server Certificates
- SSL Client Keys & Certificates
- Signing & Decryption Keys & Certificates
- Certificate Revocation Checking
- Metadata URLs

AUTHENTICATION

- Application Authentication
- Password Credential Validators
- Active Directory Domains/Kerberos Realms

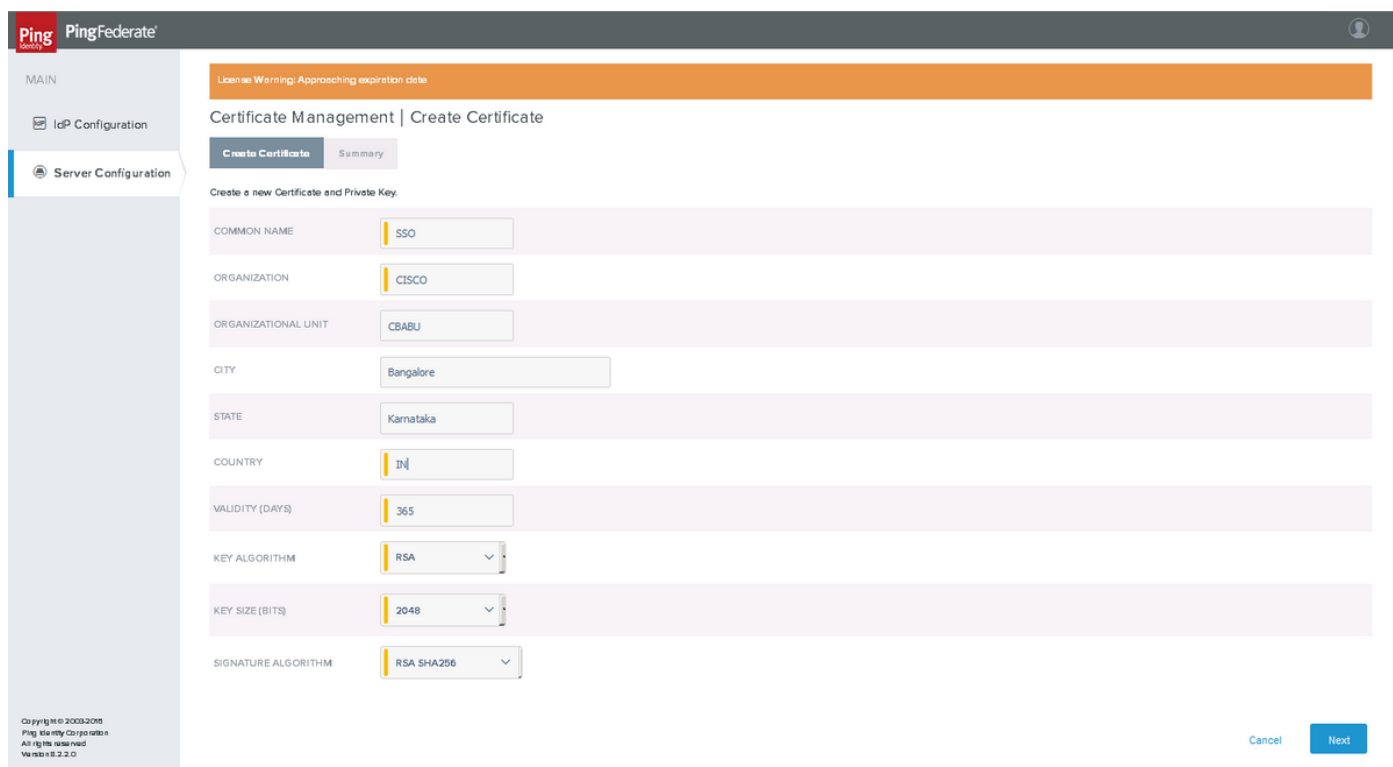
數位簽署和可擴充標籤語言(XML)解密金鑰和憑證

按一下「Server Configuration」>「Certificate Management」>「Signing & XML Decryption Keys & Certificates」



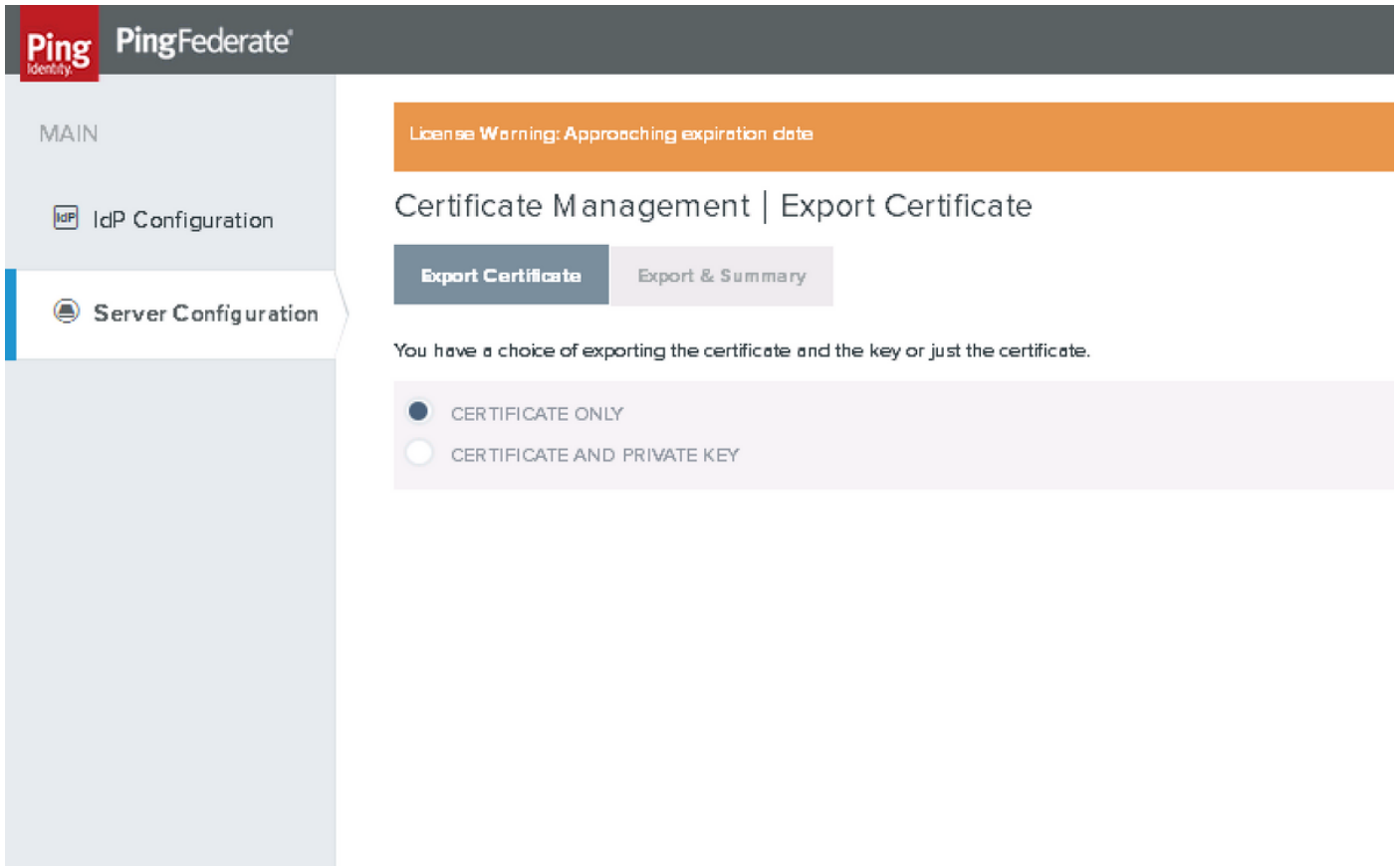
按一下「Create New」

建立證書

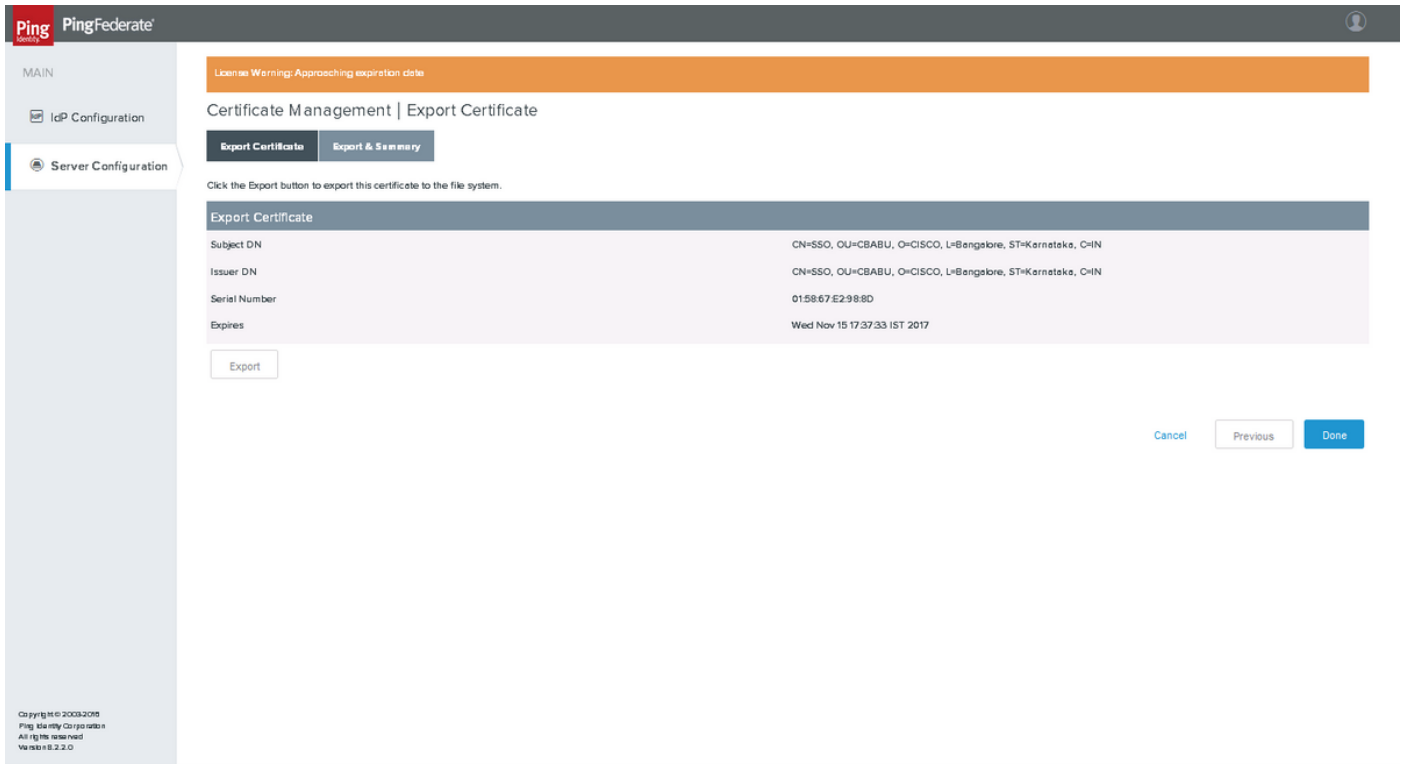


按一下下一步

匯出證書



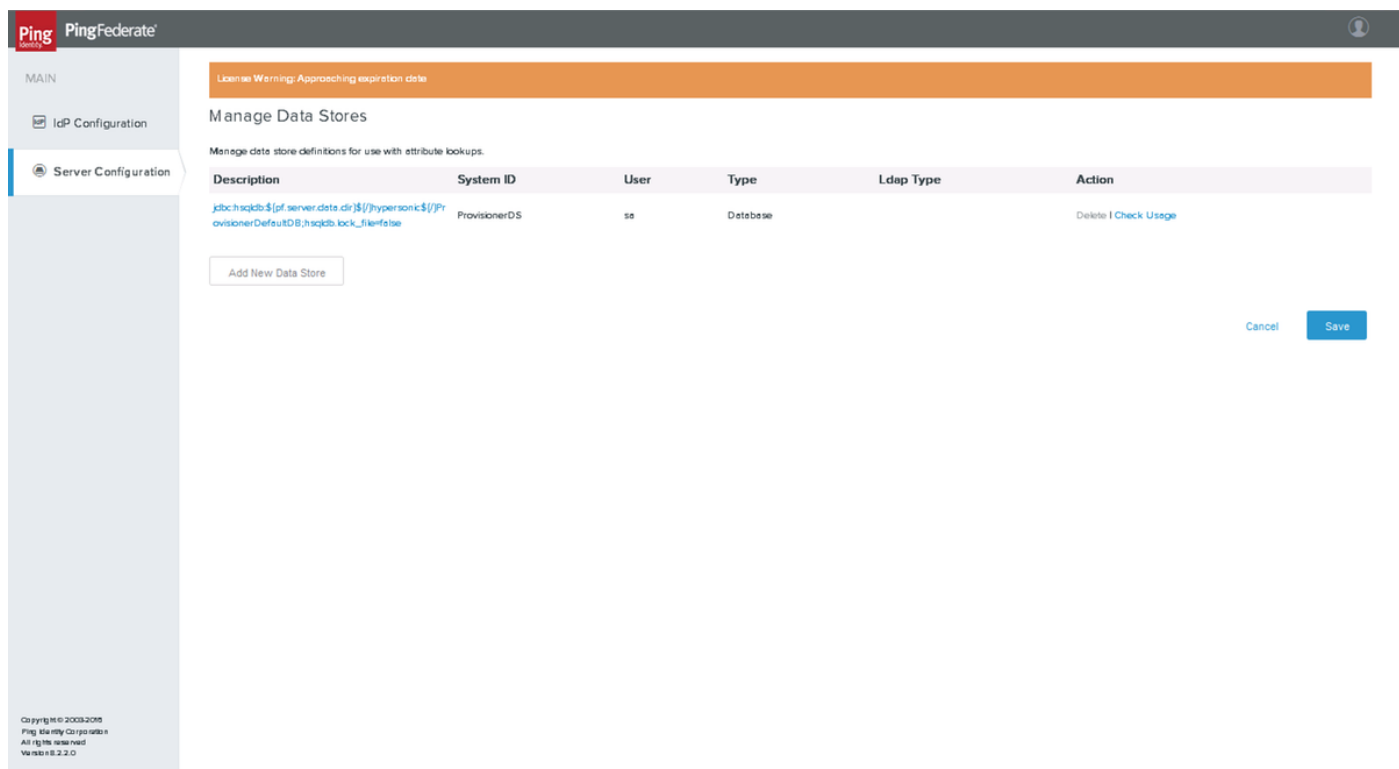
匯出與摘要



按一下「Export」

資料儲存

按一下Server Configuration > SYSTEM SETTINGS > Data Stores



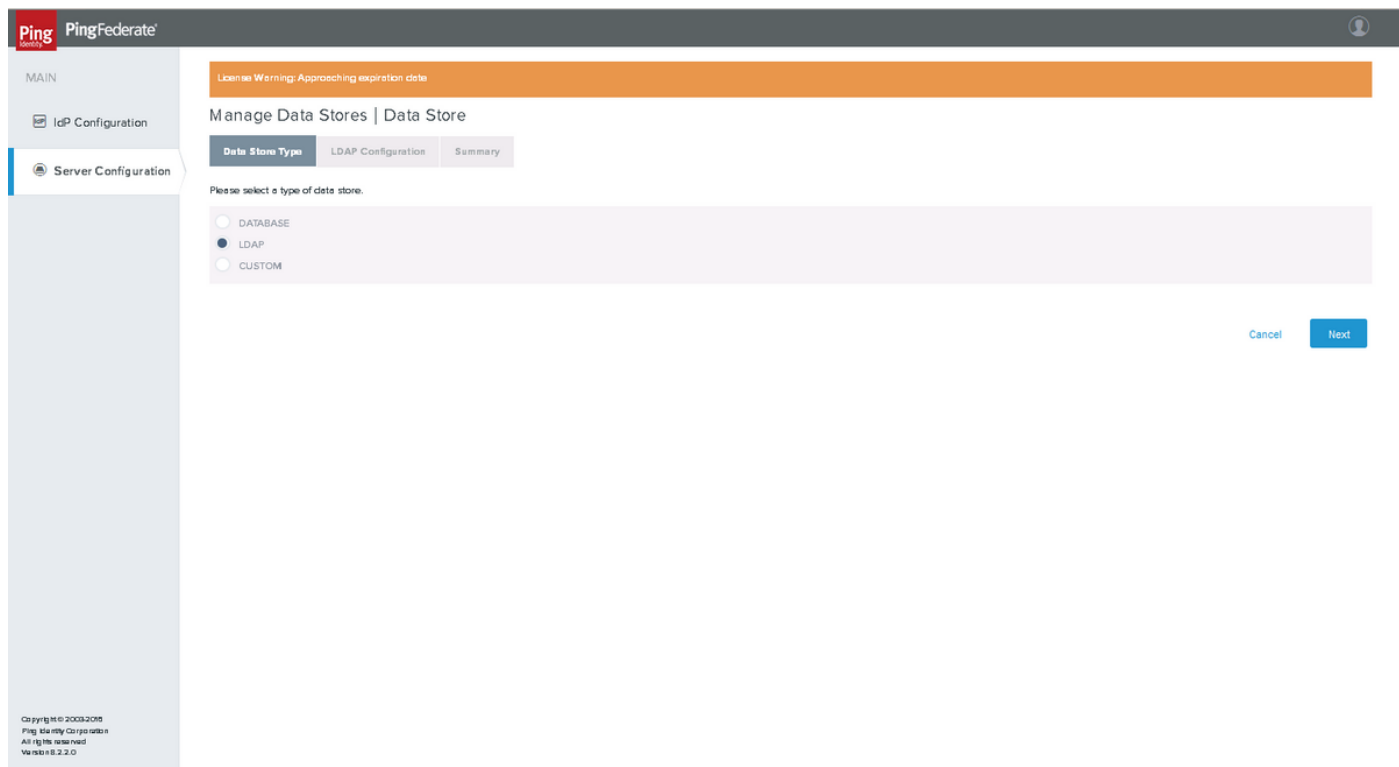
The screenshot shows the 'Manage Data Stores' page in PingFederate. At the top, there is a license warning: 'License Warning: Approaching expiration date'. Below this, the page title is 'Manage Data Stores' with a subtitle 'Manage data store definitions for use with attribute lookups.' A table lists the existing data stores:

Description	System ID	User	Type	Ldap Type	Action
<code>jdbc:hsqldb:\${pf.server.data.dir}/\${hypersonic}/\${ProvisionerDefaultDB;hsqldb.lock_file=false</code>	ProvisionerDS	sa	Database		Delete Check Usage

Below the table is an 'Add New Data Store' button. At the bottom right, there are 'Cancel' and 'Save' buttons. The left sidebar shows the navigation menu with 'Server Configuration' selected. The footer contains copyright information: 'Copyright © 2003-2018 Ping Identity Corporation. All rights reserved. Version 8.2.2.0'.

按一下Add New Data Store

LDAP配置



The screenshot shows the 'Manage Data Stores | Data Store' page in PingFederate. At the top, there is a license warning: 'License Warning: Approaching expiration date'. Below this, the page title is 'Manage Data Stores | Data Store'. There are three tabs: 'Data Store Type', 'LDAP Configuration', and 'Summary'. The 'Data Store Type' tab is active, showing the instruction 'Please select a type of data store.' and three radio button options: 'DATABASE', 'LDAP' (which is selected), and 'CUSTOM'. At the bottom right, there are 'Cancel' and 'Next' buttons. The left sidebar shows the navigation menu with 'Server Configuration' selected. The footer contains copyright information: 'Copyright © 2003-2018 Ping Identity Corporation. All rights reserved. Version 8.2.2.0'.

選擇LDAP並按一下Next

License Warning: Approaching expiration date

Manage Data Stores | Data Store

Data Store Type | **LDAP Configuration** | Summary

Please provide the details for configuring this LDAP connection.

HOSTNAME(S)

LDAP TYPE

BIND ANONYMOUSLY

USER DN

PASSWORD

USE LDAPS

MASK VALUES IN LOG

[Advanced](#)

Cancel Previous **Next**

Copyright © 2003-2018 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

輸入值，然後按一下下一步

摘要

License Warning: Approaching expiration date

Manage Data Stores | Data Store

Data Store Type | **LDAP Configuration** | **Summary**

Click a heading link to edit a configuration setting.

Data Store

Data Store Type

Type of Data Store LDAP

LDAP Configuration

Hostname(s) 10.78.93.148:389

Username cn=Administrator,cn=users,dc=cisco,dc=com

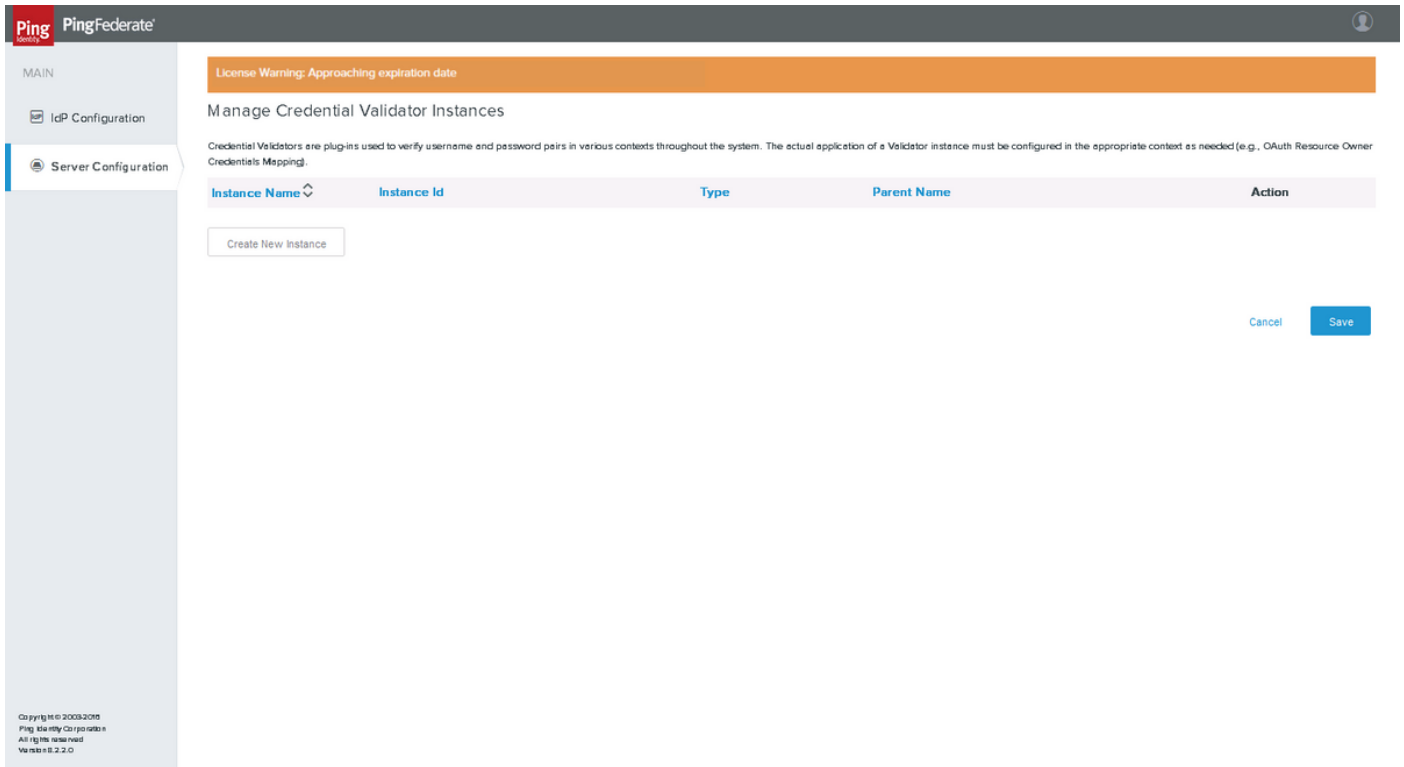
Cancel Previous Done **Save**

Copyright © 2003-2018 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

驗證後按一下「Save」。

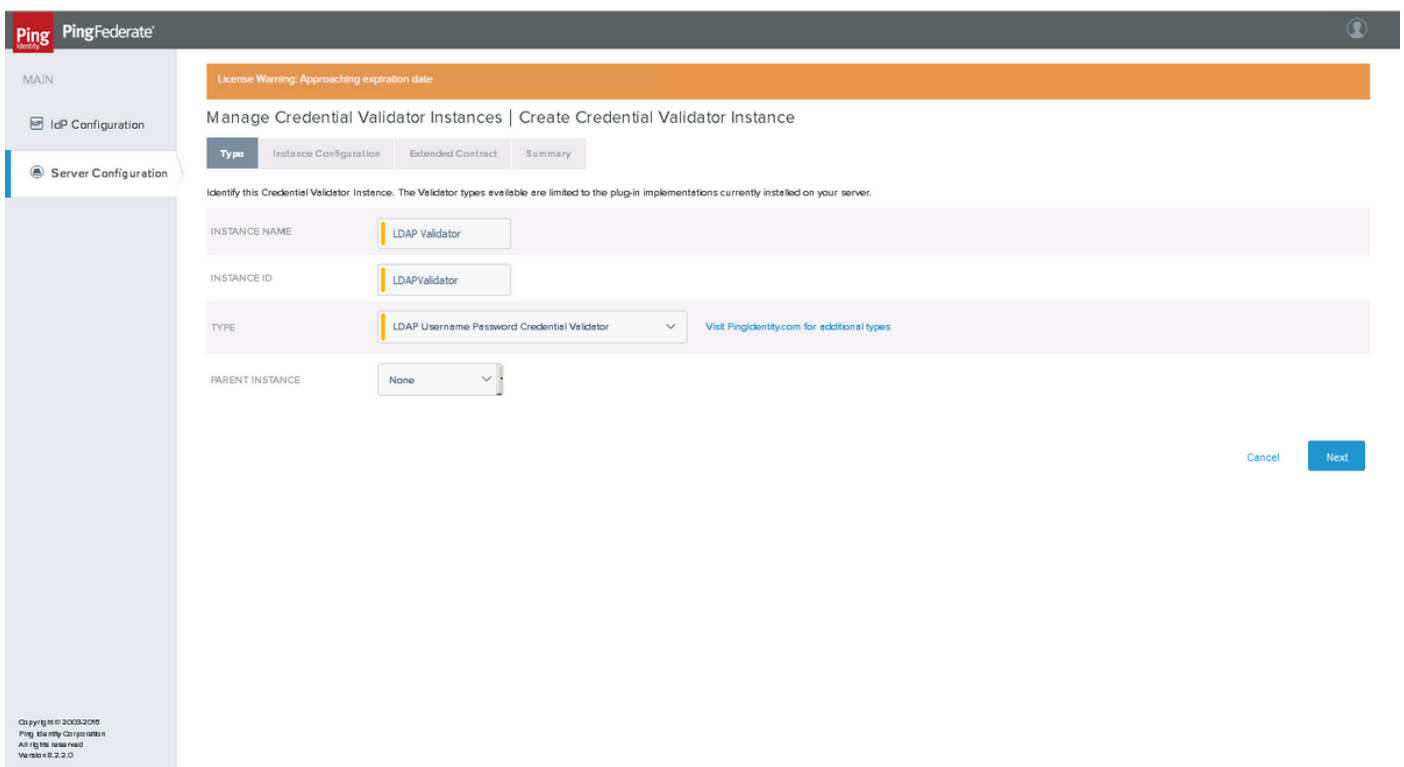
密碼憑據驗證程式

按一下Server Configuration > AUTHENTICATION > Password Credential Validators



按一下Create New Instance。

類型



選擇LDAP Username Password Credential Validator作為型別。按「Next」（下一步）。

例項配置

License Warning: Approaching expiration date

Manage Credential Validator Instances | Create Credential Validator Instance

Type Instance Configuration Extended Contract Summary

Complete the configuration necessary for this Password Credential Validator to check username/password pairs. This configuration was designed into, and is specific to, the selected Credential Validator plug-in.

This password credential validator provides a means of verifying credentials stored in a directory server via the LDAP protocol. Additional user attributes from the directory can also be returned by this PCV by adding the desired attribute names to the Extended Contract.

AUTHENTICATION ERROR OVERRIDES
 [A table of LDAP authentication error codes and customized matching expressions that will match the error code to an LDAP error message. These entries override the default individual mappings of messages to codes. Use the localization features to customize the error messages displayed to end users.]

MATCH EXPRESSION
 [The expression matched against the LDAP error message returned by the server]

MATCH EXPRESSION	ERROR	Action
Add a new row to Authentication Error Overrides!		

Field Name	Field Value	Description
LDAP DATASTORE	1078.93.148.389	Select the LDAP Datastore.
SEARCH BASE	CN=Users,DC=disco,DC=com	The location in the directory from which the LDAP search begins.
SEARCH FILTER	sAMAccountName=\${username}	You may use \${username} as part of the query. Example (for Active Directory): sAMAccountName=\${username}
SCOPE OF SEARCH	<input type="radio"/> One Level <input checked="" type="radio"/> Subtree	
CASE-SENSITIVE MATCHING	<input checked="" type="checkbox"/>	Allows case-sensitive expression and LDAP error matching.

[Manage Data Stores](#)

Cancel Previous **Next**

Copyright © 2003-2016 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

選擇LDAP資料儲存區並輸入搜尋庫、搜尋過濾器 and 搜尋範圍。按「Next」(下一步)。

延伸合約

License Warning: Approaching expiration date

Manage Credential Validator Instances | Create Credential Validator Instance

Type Instance Configuration Extended Contract Summary

You can extend the attribute contract of this Password Credential Validator instance.

Core Contract

DN

givenName

mail

username

Extend the Contract **Action**

Cancel Previous **Next**

Copyright © 2003-2016 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

按一下下一步

摘要

License Warning: Approaching expiration date

Manage Credential Validator Instances | Create Credential Validator Instance

Type Instance Configuration Extended Contract Summary

Password Credential Validator configuration summary.

Create Credential Validator Instance

Type

Instance Name	LDAP Validator
Instance Id	LDAPValidator
Type	LDAP Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.LDAPUsernamePasswordCredentialValidator
Parent Instance Name	None

Instance Configuration

LDAP Dtestore	10.78.93.148:389
Search Base	CN=Users,DC=cisco,DC=com
Search Filter	sAMAccountName=\${username}
Scope of Search	Subtree
Case-Sensitive Matching	true

Extended Contract

Attribute	mail
Attribute	givenName
Attribute	DN
Attribute	username

Copyright © 2003-2016 Ping Identity Corporation. All rights reserved. Version 10.2.2.0

Cancel Previous Done

驗證設定並按一下「Done(完成)」。

伺服器設定

系統管理

按一下Server Configuration>SYSTEM SETTINGS>Server Settings

License Warning: Approaching expiration date

Server Settings

System Administration System Info Runtime Notifications Runtime Reporting Account Management Roles & Protocols Federation Info

System Options Metadata Signing Metadata Lifetime Summary

Select the style of application management practiced in your organization.

System Administration Style SINGLE-USER ADMINISTRATION MULTI-USER ADMINISTRATION

Cancel Next Save

按「Next」(下一步)。

系統資訊

Ping Federate

License Warning: Approaching expiration date

Server Settings

- System Administration
- System Info
- Runtime Notifications
- Runtime Reporting
- Account Management
- Roles & Protocols
- Federation Info

- System Options
- Metadata Signing
- Metadata Lifetime
- Summary

This is general information that identifies your server. This information is included whenever you export connection metadata.

COMPANY

CONTACT NAME

CONTACT NUMBER

CONTACT EMAIL

[Cancel](#) [Previous](#) [Next](#) [Save](#)

按「Next」（下一步）。

運行時通知

Ping Federate

License Warning: Approaching expiration date

Server Settings

- System Administration
- System Info
- Runtime Notifications
- Runtime Reporting
- Account Management
- Roles & Protocols
- Federation Info

- System Options
- Metadata Signing
- Metadata Lifetime
- Summary

Select which server events result in notifications sent via email.

NOTIFICATION FOR SERVER LICENSING EVENTS

NOTIFICATION FOR CERTIFICATE EVENTS

NOTIFICATION FOR SAML METADATA UPDATE EVENTS

[Cancel](#) [Previous](#) [Next](#) [Save](#)

按「Next」（下一步）。

運行時報告

Ping Federate

License Warning: Approaching expiration date

Server Settings

- System Administration
- System Info
- Runtime Notifications
- Runtime Reporting
- Account Management
- Roles & Protocols
- Federation Info

- System Options
- Metadata Signing
- Metadata Lifetime
- Summary

If your organization uses SNMP to monitor infrastructure, you can integrate this server with your existing network-management console.

RESPOND TO GET REQUESTS

GENERATE TRAPS

Cancel Previous Next Save

按「Next」(下一步)。

帳戶管理

Ping Federate

License Warning: Approaching expiration date

Server Settings

- System Administration
- System Info
- Runtime Notifications
- Runtime Reporting
- Account Management
- Roles & Protocols
- Federation Info

- System Options
- Metadata Signing
- Metadata Lifetime
- Summary

Manage administrative-console or API users and their role assignments.

Username	User Admin	Admin	Crypto Admin	Action
Administrator	<input type="radio"/> AUDITOR <input checked="" type="radio"/> ADMIN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Deactivate Change Password

Create User

NOTIFY USER OF PASSWORD CHANGE

Cancel Previous Next Save

按「Next」(下一步)。

注意：您可以在此部分中新增使用者或更改使用者的密碼。

角色和協定

The screenshot shows the PingFederate administration interface. At the top, there is a 'License Warning: Approaching expiration date' banner. The main navigation on the left includes 'MAIN', 'IDP Configuration', and 'Server Configuration'. The 'Server Settings' page has several tabs: 'System Administration', 'System Info', 'Runtime Notifications', 'Runtime Reporting', 'Account Management', 'Roles & Protocols', 'Federation Info', 'System Options', 'Metadata Signing', 'Metadata Lifetime', and 'Summary'. The 'Roles & Protocols' tab is active, displaying a list of roles and protocols with checkboxes. The roles listed are: 'ENABLE OAUTH 2.0 AUTHORIZATION SERVER (AS) ROLE' (unchecked), 'ENABLE IDENTITY PROVIDER (IDP) ROLE AND SUPPORT THE FOLLOWING:' (checked), 'SAML 2.0' (checked), 'AUTO-CONNECT PROFILE' (unchecked), 'SAML 1.1' (unchecked), 'SAML 1.0' (unchecked), 'WS-FEDERATION' (unchecked), 'OUTBOUND PROVISIONING' (unchecked), 'WS-TRUST' (unchecked), 'ENABLE SERVICE PROVIDER (SP) ROLE AND SUPPORT THE FOLLOWING:' (unchecked), and 'ENABLE IDP DISCOVERY ROLE (SAML 2.0 ONLY)' (unchecked). At the bottom right, there are buttons for 'Cancel', 'Previous', 'Next', and 'Save'. A copyright notice 'Copyright © 2003-2016 Ping Identity Corporation' is visible in the bottom left corner.

選擇適當的角色和協定。按「Next」（下一步）。

聯合資訊

The screenshot shows the PingFederate administration interface, now on the 'Federation Info' tab. The 'License Warning' banner is still present. The 'Server Settings' page has tabs for 'System Administration', 'System Info', 'Runtime Notifications', 'Runtime Reporting', 'Account Management', 'Roles & Protocols', 'Federation Info', 'System Options', 'Metadata Signing', and 'Metadata Lifetime'. The 'Federation Info' tab is active, displaying a text area for 'BASE URL' with the value 'https://pingserver.cisco.com:9031' and a text field for 'SAML 2.0 ENTITY ID' with the value 'pingserver'. A note states: 'You must create a unique identifier for your server for use with your federation partners. A unique identifier is required for each protocol enabled. You will need to communicate this with your partners out-of-band or through metadata exchange. The Base URL is used to construct other URLs in the system and may be used as part of your system ID.' At the bottom right, there are buttons for 'Cancel', 'Previous', 'Next', and 'Save'.

按「Next」（下一步）。

系統選項

Ping Identity PingFederate

License Warning: Approaching expiration date

Server Settings

System Administration | System Info | Runtime Notifications | Runtime Reporting | Account Management | Roles & Protocols | Federation Info

System Options | Metadata Signing | Metadata Lifetime | Summary

Configure global server options. Please click Help for more information.

DISABLE AUTOMATIC CONNECTION VALIDATION

DATA-STORE VALIDATION INTERVAL (SECS)

Incoming Proxy Settings

HTTP HEADER FOR CLIENT IP ADDRESSES Use Last Value

HTTP HEADER FOR HOSTNAME Use Last Value

CLIENT CERTIFICATE HEADER NAME

CLIENT CERTIFICATE CHAIN HEADER NAME

INCOMING PROXY TERMINATES HTTPS CONNECTIONS

Cancel Previous Next Save

按「Next」（下一步）。

後設資料簽名

Ping Identity PingFederate

License Warning: Approaching expiration date

Server Settings

System Administration | System Info | Runtime Notifications | Runtime Reporting | Account Management | Roles & Protocols | Federation Info | System Options | Metadata Signing | Metadata Lifetime

Summary

Select a certificate for signing the metadata which will be published. If no certificate is selected, the published metadata will not be signed.

SIGNING CERTIFICATE

SIGNING ALGORITHM

Manage Certificates

Cancel Previous Next Save

選擇之前建立的簽名證書和簽名演算法作為證書配置的一部分。按「Next」（下一步）。

後設資料生存期

License Warning: Approaching expiration date

Server Settings

- System Administration
- System Info
- Runtime Notifications
- Runtime Reporting
- Account Management
- Roles & Protocols
- Federation Info

- System Options
- Metadata Signing
- Metadata Lifetime
- Summary

Specify validity period for published metadata and refresh delay for automated metadata reloading.

CACHE DURATION (MINUTES) 1440

RELOAD DELAY (MINUTES) 1440

Cancel Previous Next Save

按「Next」(下一步)。

摘要

License Warning: Approaching expiration date

Server Settings

- System Administration
- System Info
- Runtime Notifications
- Runtime Reporting
- Account Management
- Roles & Protocols
- Federation Info
- System Options
- Metadata Signing

- Metadata Lifetime
- Summary

Server Settings Summary Information

Summary

Server Settings

System Administration

Multiple Administrators true

System Info

Runtime Notifications

Certificate Events false

License Events false

Metadata Events false

Email Notification You must provide a "From" Address. You must provide an Email Server.

From Address

Email Server

SMTP Port 25

SMTPS Port 465

Connection Timeout 30

Encryption Method None

Enable SMTP Debugging Messages false

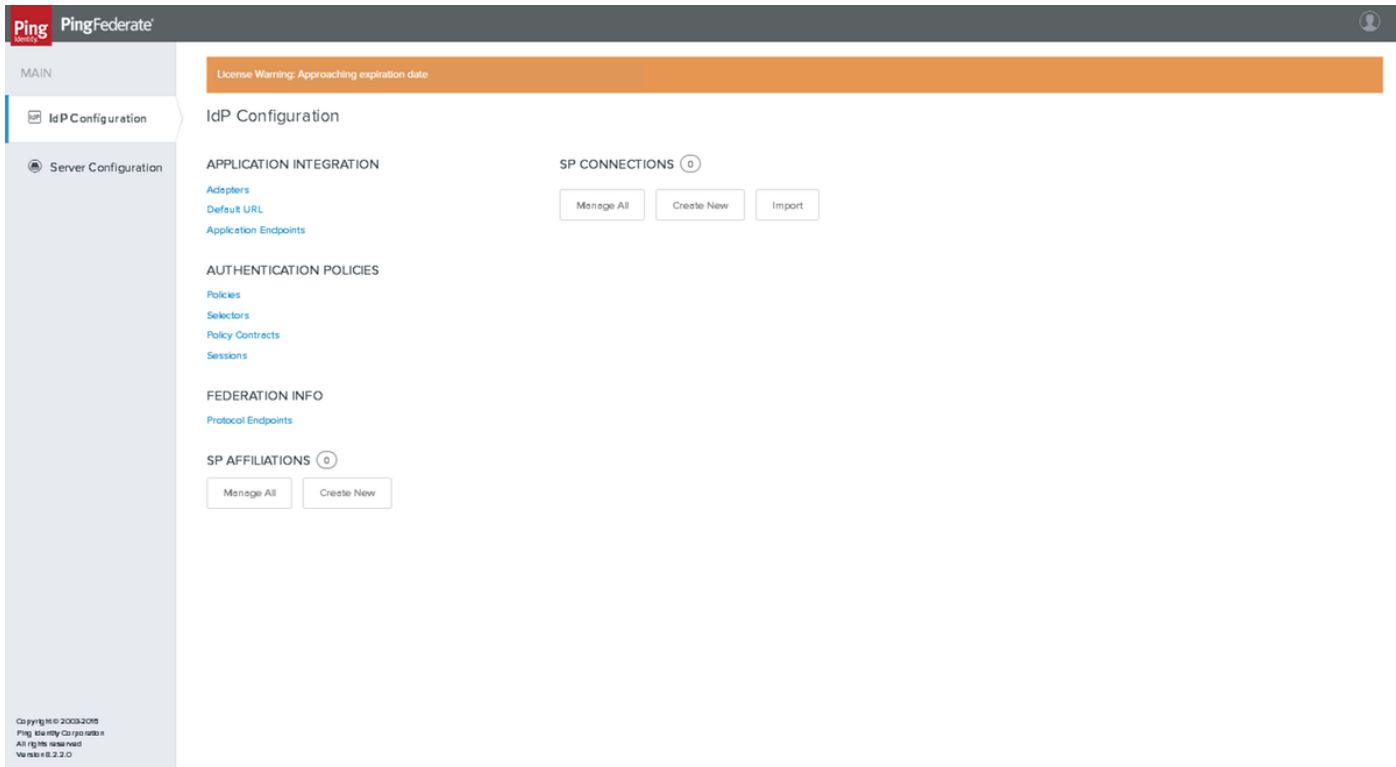
Username

Retry Attempt 2

Copyright © 2009-2019 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

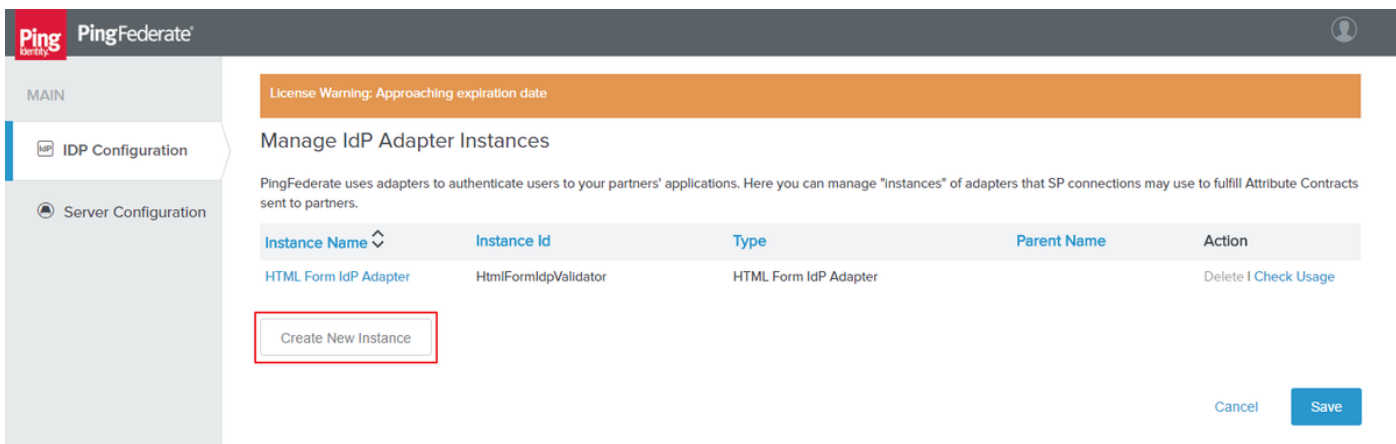
驗證設定並按一下Save。

身份提供程式(IdP)配置



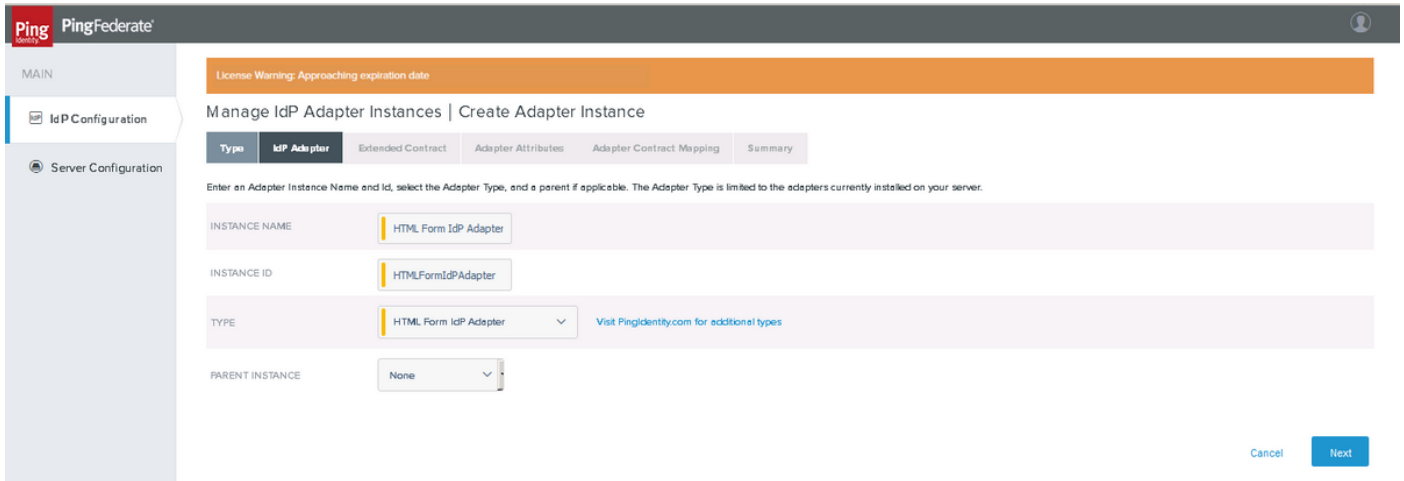
介面卡

按一下 IdP Configuration > APPLICATION INTEGRATION > Adapters



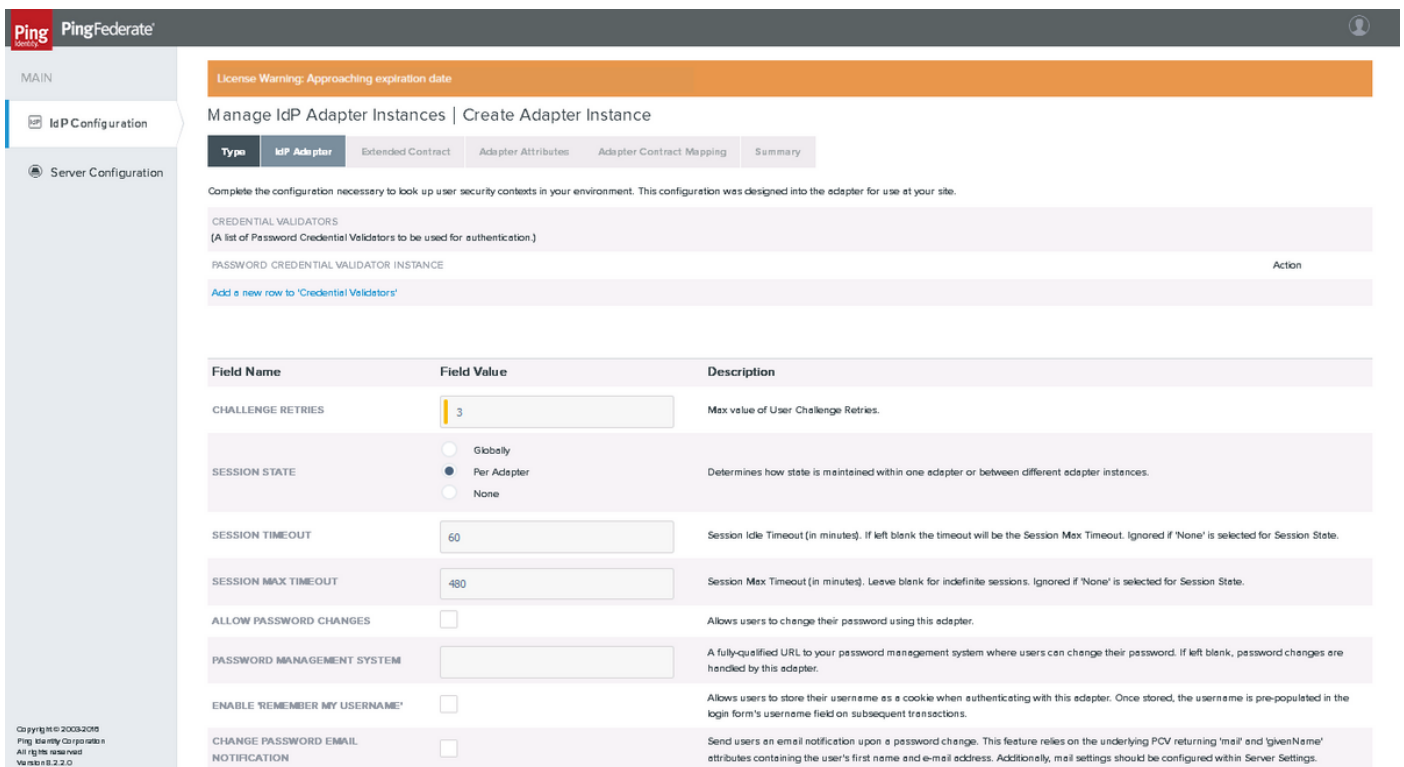
按一下 Create New Instance。

類型



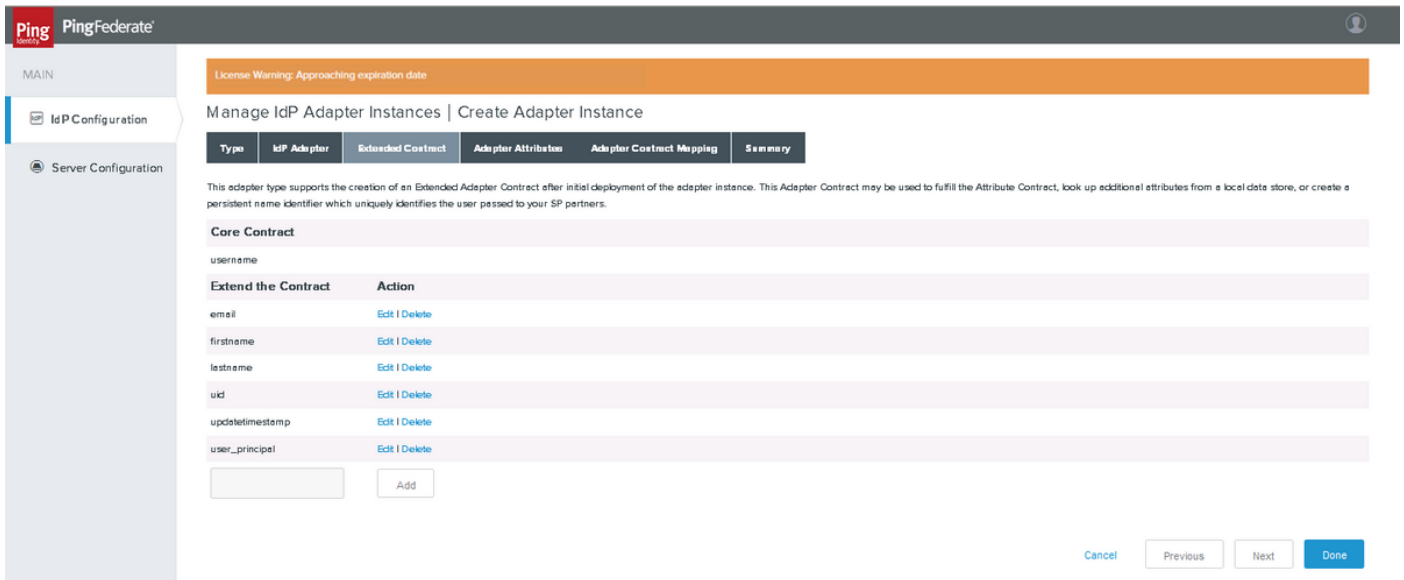
選擇HTML表單IDP介面卡。按「Next」（下一步）。

IdP介面卡



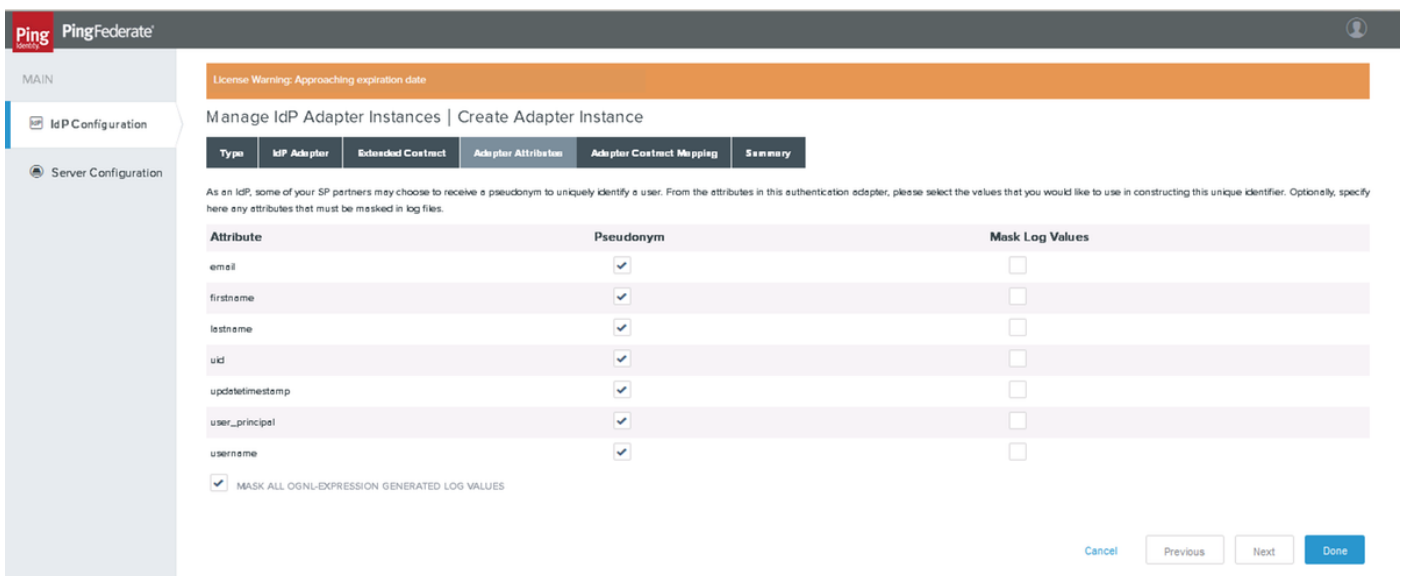
按一下Add a new row to 'Credential Validators'（向「憑據驗證程式」新增新行），然後選擇先前作為PASSWORD CREDENTIAL VALIDATOR INSTANCE建立的LDAP驗證程式，然後按一下Update（更新）。按一下Next（下一步）。

延伸合約



新增合約，如圖所示。按「Next」（下一步）。

介面卡屬性



按「Next」（下一步）。

介面卡合約對映

The screenshot shows the PingFederate interface. At the top, there is a license warning: "License Warning: Approaching expiration date". The main heading is "Manage IdP Adapter Instances | Create Adapter Instance". Below this, there are several tabs: "Type", "IdP Adapter", "Extended Contract", "Adapter Attributes", "Adapter Contract Mapping", and "Summary". The "Adapter Contract Mapping" tab is currently selected. A text block explains: "An Adapter Contract may be used to fulfill the Attribute Contract passed to your SP partners. By default, the adapter contract is fulfilled by the adapter itself. Optionally, additional attributes from local data stores can be used to fulfill the contract." A button labeled "Configure Adapter Contract" is highlighted with a red box. At the bottom right, there are four buttons: "Cancel", "Previous", "Next", and "Done".

按一下「Configure Adapter Contract」。

屬性源和使用者查詢

The screenshot shows the PingFederate interface at the "Adapter Contract Mapping" step. The main heading is "Manage IdP Adapter Instances | Create Adapter Instance | Adapter Contract Mapping". Below this, there are four tabs: "Attribute Sources & User Lookup", "Adapter Contract Fulfillment", "Issuance Criteria", and "Summary". The "Attribute Sources & User Lookup" tab is selected. A text block explains: "You can choose to fulfill the Adapter Contract with the adapter's default values, or you can use these values plus additional attributes retrieved from local data stores." Below this is a table with the following data:

Description	Type	Action
LdapQA	LDAP	Delete

Below the table is an "Add Attribute Source" button. At the bottom right, there are three buttons: "Cancel", "Next", and "Done".

新增屬性源並選擇之前建立的LDAP儲存。按「Next」（下一步）。

介面卡合約履行

Ping Federate

License Warning: Approaching expiration date

Manage IdP Adapter Instances | Create Adapter Instance | Adapter Contract Mapping

Attribute Sources & User Lookup | Adapter Contract Fulfillment | Issuance Criteria | Summary

Fulfill your Adapter Contract with values from the authentication adapter or with dynamic text values.

Contract	Source	Value	Actions
email	LDAP (LdapQA)	mail	None available
firstname	LDAP (LdapQA)	givenName	None available
lastname	LDAP (LdapQA)	sn	None available
uid	LDAP (LdapQA)	sAMAccountName	None available
updateTimestamp	LDAP (LdapQA)	whenChanged	None available
user_principal	LDAP (LdapQA)	userPrincipalName	None available
username	LDAP (LdapQA)	sAMAccountName	None available

Cancel Previous Next Done

對映屬性。按「Next」（下一步）。

發佈標準

Ping Federate

License Warning: Approaching expiration date

Manage IdP Adapter Instances | Create Adapter Instance | Adapter Contract Mapping

Attribute Sources & User Lookup | Adapter Contract Fulfillment | Issuance Criteria | Summary

PingFederate can evaluate various criteria to determine whether users are authorized to access SP resources. Use this optional screen to configure the criteria for use with this conditional authorization.

Source	Attribute Name	Condition	Value	Error Result	Action
- SELECT -	- SELECT -	- SELECT -			Add

Cancel Previous Next Done

按「Next」（下一步）。

摘要

Copyright © 2003-2016
Ping Identity Corporation
All rights reserved
Version 8.2.2.0

10.78.93.148:369

LDAP Directory Search

Base DN: cn=users,dc=cisco,dc=com

Search scope: SUBTREE_SCOPE

Attribute: Subject DN

Attribute: givenName

Attribute: mail

Attribute: sAMAccountName

Attribute: sn

Attribute: userPrincipalName

Attribute: whenChanged

LDAP Filter

Filter: sAMAccountName=\${username}

Adapter Contract Fulfillment

uid: sAMAccountName (LDAP)

firstname: givenName (LDAP)

updateTimestamp: whenChanged (LDAP)

user_principal: userPrincipalName (LDAP)

email: mail (LDAP)

lastname: sn (LDAP)

username: sAMAccountName (LDAP)

Issuance Criteria

Criterion: (None)

Cancel Previous Done

驗證設定並按一下「Done(完成)」。

SP連線

建立新的SP連線

連線型別

License Warning: Approaching expiration date

SP Connection

CONNECTION TYPE: CONNECTION OPTIONS: IMPORT METADATA: GENERAL INFO: BROWSER SSO: CREDENTIALS: ACTIVATION & SUMMARY

Select the type of connection needed for this SP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for access to identity-enabled Web Services), Outbound Provisioning (for provisioning users/groups to an SP) or all.

CONNECTION TEMPLATE: No Template

BROWSER SSO PROFILES: PROTOCOL: SAML 2.0

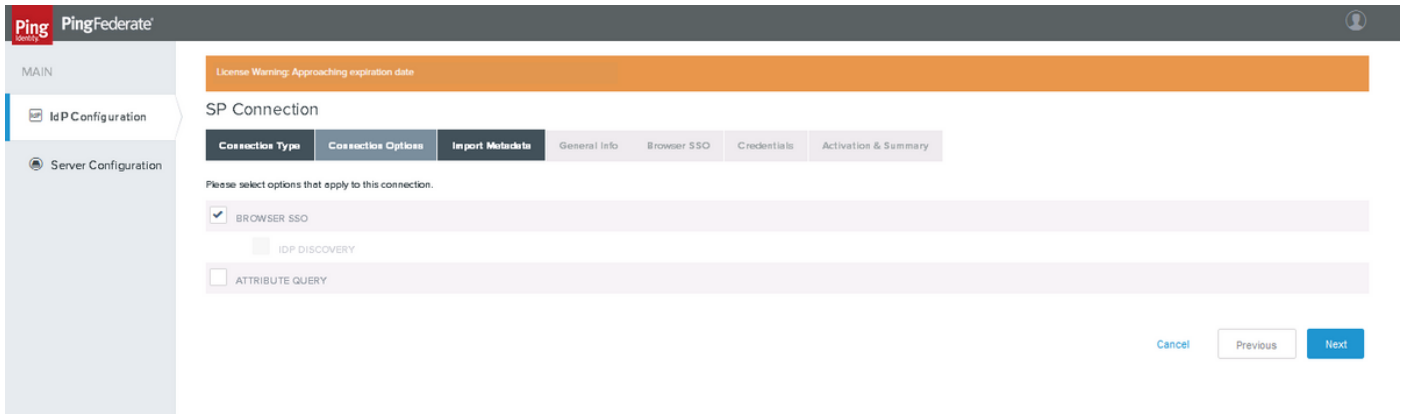
WS-TRUST STS

OUTBOUND PROVISIONING

Cancel Next

按「Next」(下一步)。

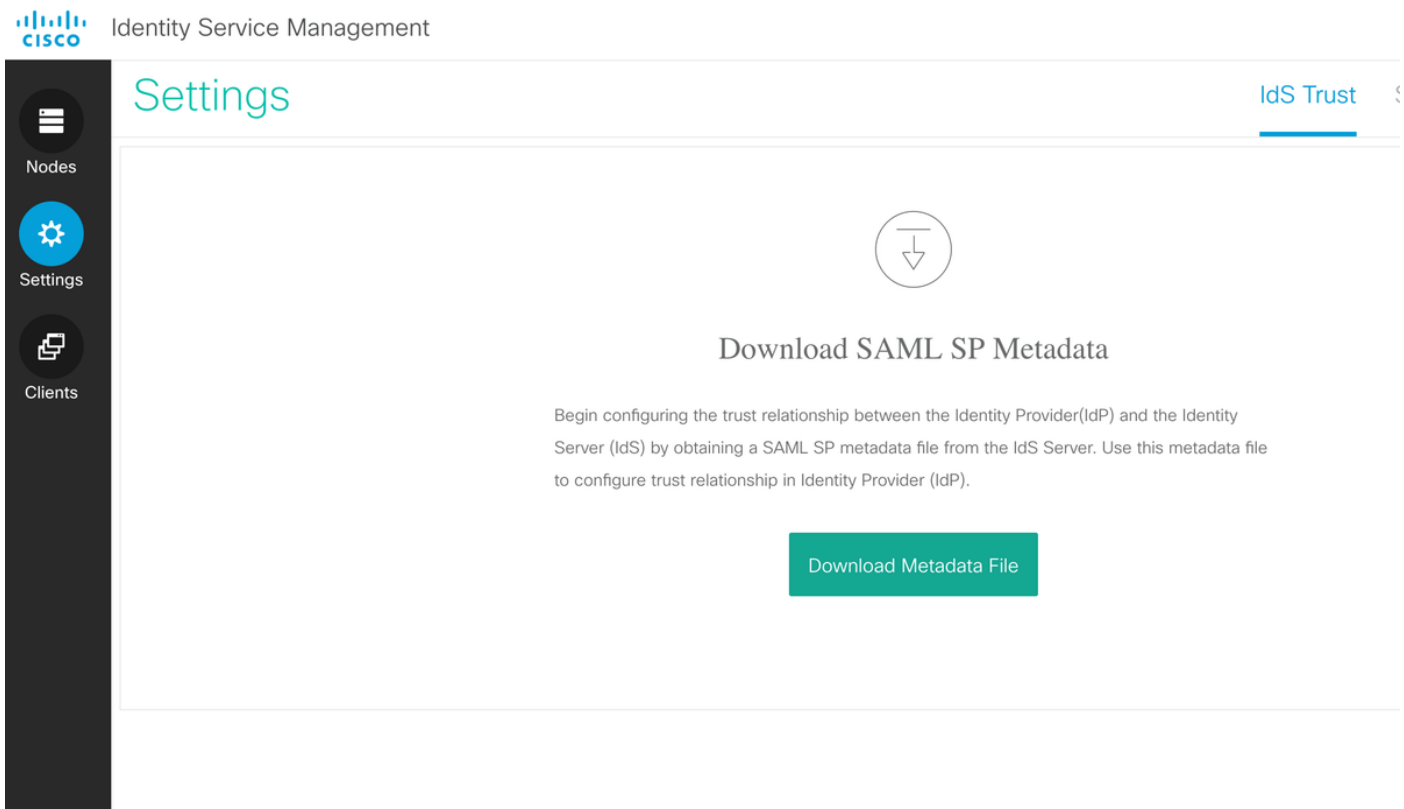
連線選項



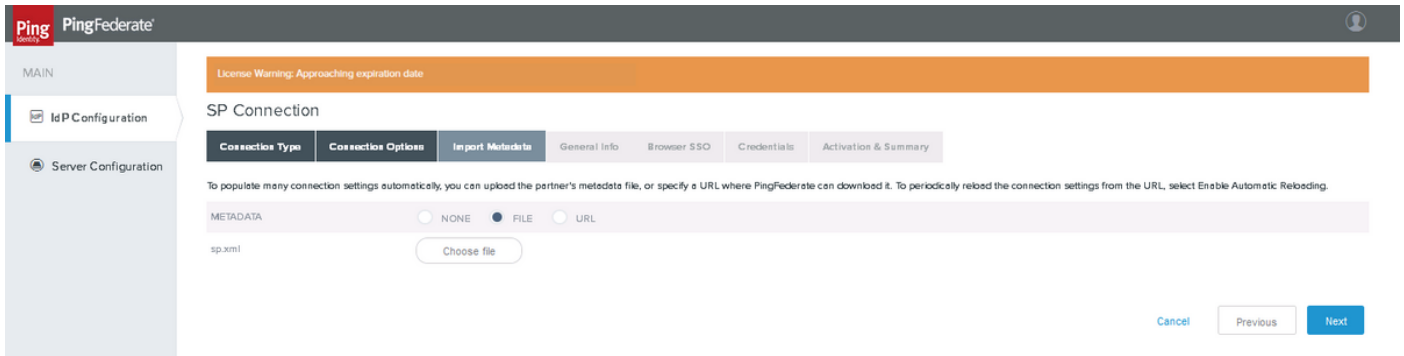
按一下下一步

匯入後設資料

從Cisco Identity Service Admin > Settings > IdS Trust > Download Metadata 下載服務提供程式的後設資料xml檔案

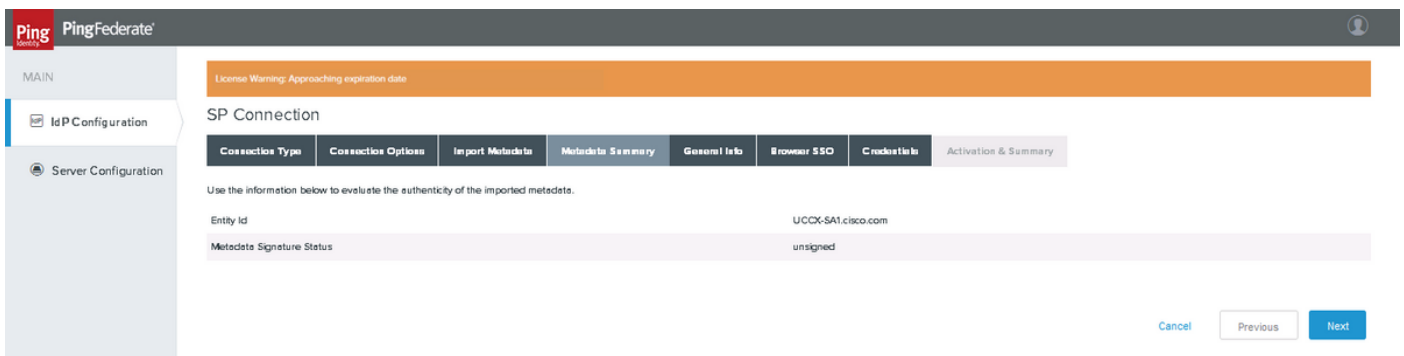


將服務提供程式的後設資料xml檔案上載到PingFederate。



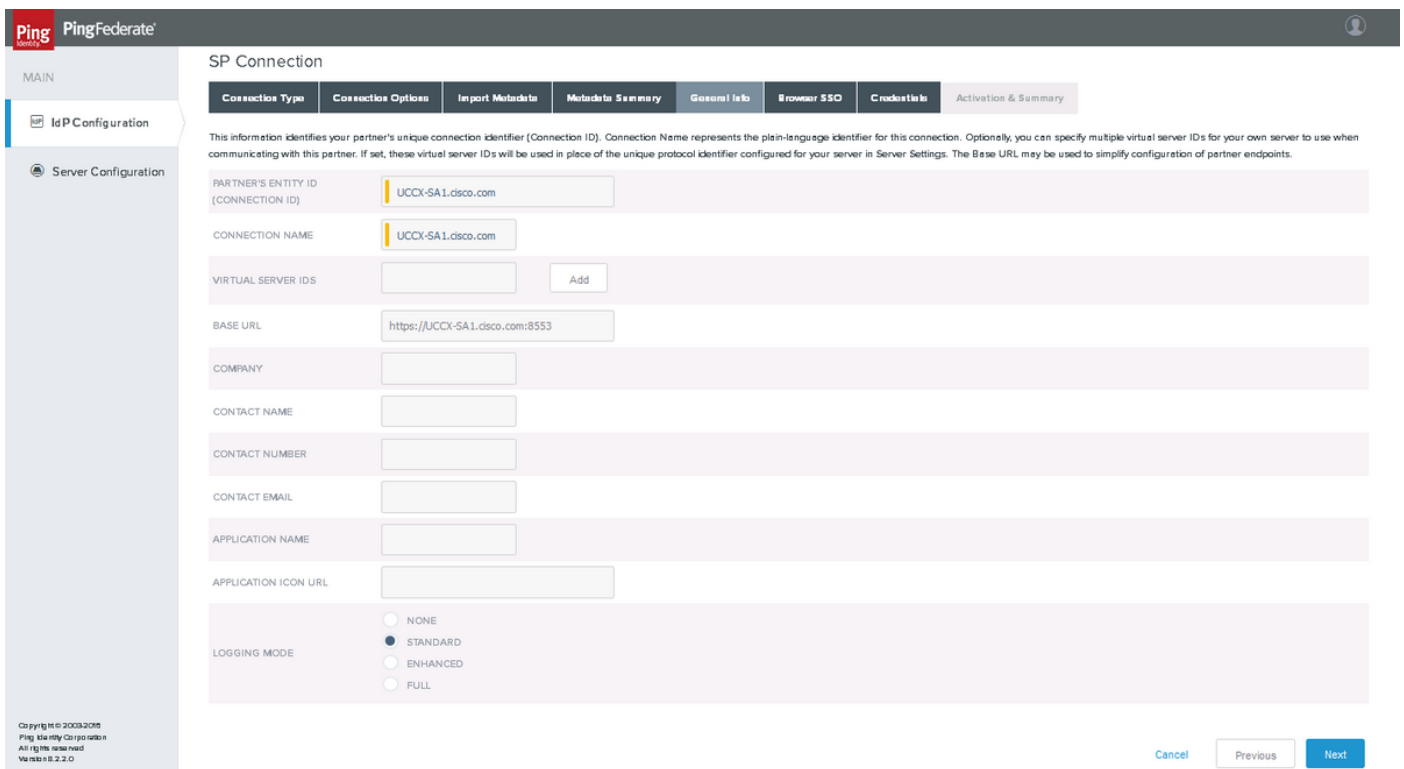
選擇下載的xml檔案，然後按一下「下一步」

後設資料摘要



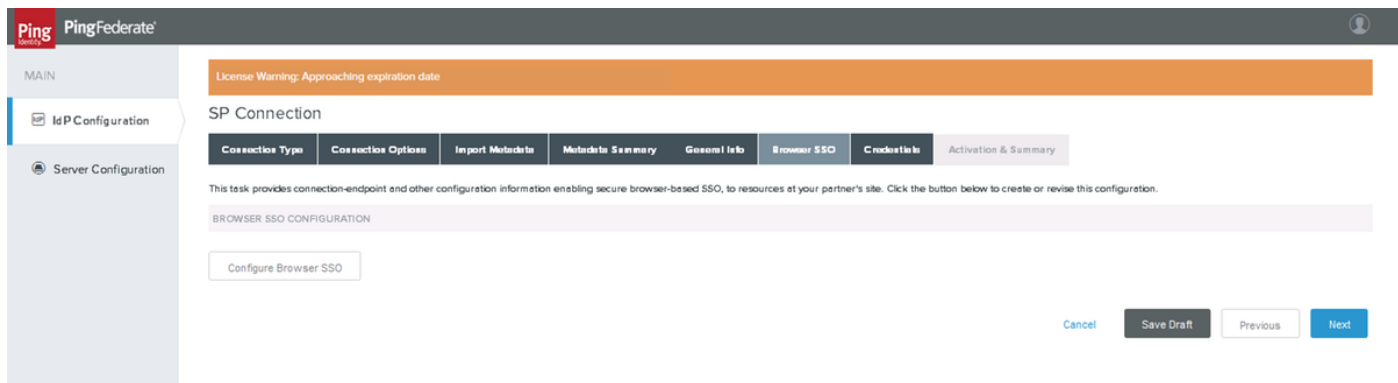
按一下下一步

一般資訊



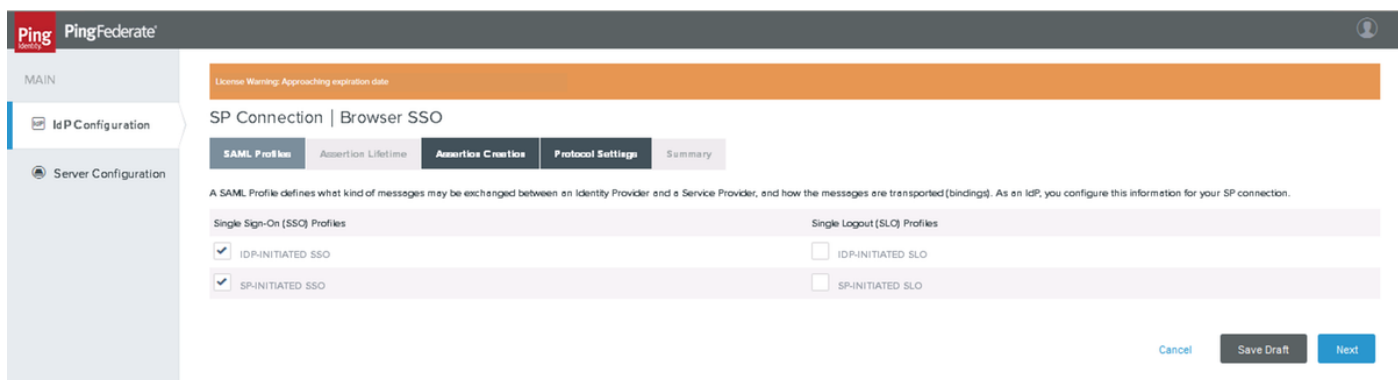
按一下下一步

瀏覽器SSO



按一下Configure Browser SSO

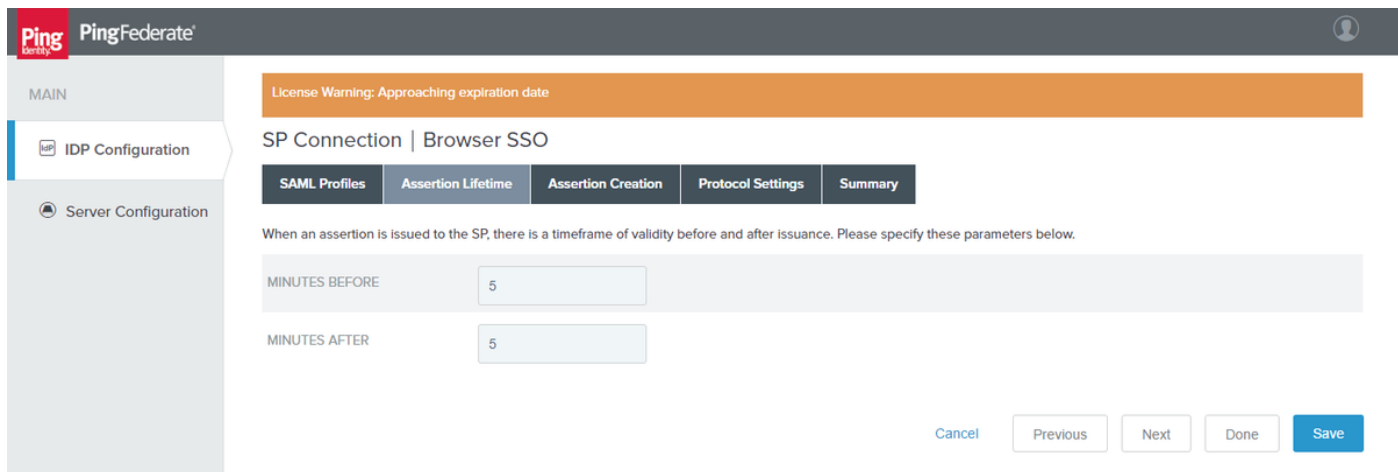
安全斷言標籤語言(SAML)配置檔案



按一下下一步

附註：思科身份服務(IdS)在11.6中不支援單一註銷(SLO)，並且未選擇此選項。

斷言生存期



按一下下一步

斷言建立

The screenshot shows the 'SP Connection | Browser SSO' configuration page in PingFederate. The 'Assertion Creation' tab is selected. The page displays the following configuration details:

Assertion Configuration	
IDENTITY MAPPING	Standard
ATTRIBUTE CONTRACT	SAML_SUBJECT, email, firstname, lastname, uid, updatetimestamp
ADAPTER INSTANCES	1
AUTHENTICATION POLICY MAPPINGS	0

At the bottom, there is a 'Configure Assertion Creation' button highlighted with a red box. Navigation buttons include 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

按一下配置斷言建立

身份對映

The screenshot shows the 'SP Connection | Browser SSO | Assertion Creation' configuration page in PingFederate. The 'Identity Mapping' tab is selected. The page displays the following configuration details:

Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the SP. Your selection may affect the way that the SP will look up and associate the user to a specific local account.

- STANDARD: Send the SP a known attribute value as the name identifier. The SP will often use account mapping to identify the user locally.
 - INCLUDE ATTRIBUTES IN ADDITION TO THE PSEUDONYM.
- PSEUDONYM: Send the SP a unique, opaque name identifier that preserves user privacy. The identifier cannot be traced back to the user's identity at this IdP and may be used by the SP to make a persistent association between the user and a specific local account. The SP will often use account linking to identify the user locally.
 - INCLUDE ATTRIBUTES IN ADDITION TO THE PSEUDONYM.
- TRANSIENT: Send the SP an opaque, temporary value as the name identifier.
 - INCLUDE ATTRIBUTES IN ADDITION TO THE TRANSIENT IDENTIFIER.

Navigation buttons include 'Cancel', 'Next', 'Done', and 'Save'.

按一下下一步

屬性合約

License Warning: Approaching expiration date

SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | Authentication Source Mapping | Summary

An Attribute Contract is a set of user attributes that this server will send in the assertion.

Attribute Contract	Subject Name Format
SAML_SUBJECT	urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Extend the Contract	Attribute Name Format	Action
SAML_AUTHN_CTX	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
SAML_NAME_FORMAT	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit Delete
uid	urn:oasis:names:tc:SAML:2.0:attrname-format:uri	Edit Delete
user_principal	urn:oasis:names:tc:SAML:2.0:attrname-format:uri	Edit Delete

urn:oasis:names:tc:SAML:2.0:attrname-format:basic

Cancel Previous Next Done Save

Copyright © 2003-2016 Ping Identity Corporation

警告：這些屬性是思科身份服務(IdS)與PingFederate互通性所必需的。

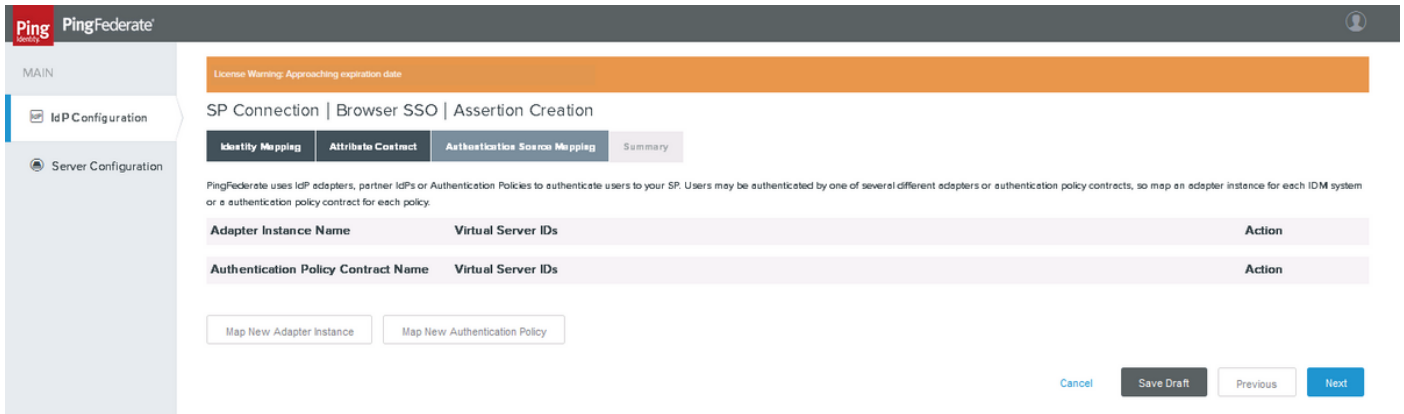
屬性合約	目的
SAML_SUBJECT	PingFederate搜尋過濾器用於檢查是否滿足對映值
SAML_AUTHN_CTX	在SAML響應中用於指示「PasswordProtectedTransport」身份驗證內容
SAML名稱格式	用於SAML響應以指示SAML 2.0臨時名稱ID格式
uid	由Cisco IdS用於識別經過身份驗證的使用者
user_principal	由Cisco IdS用來識別通過身份驗證的使用者的完整名稱 (即id +域)

管理員可以通過位於以下目錄中的custom-name-formats.xml配置檔案自定義名稱格式替代方案：
 <pf_install>/pingfederate/server/default/data/config-store。

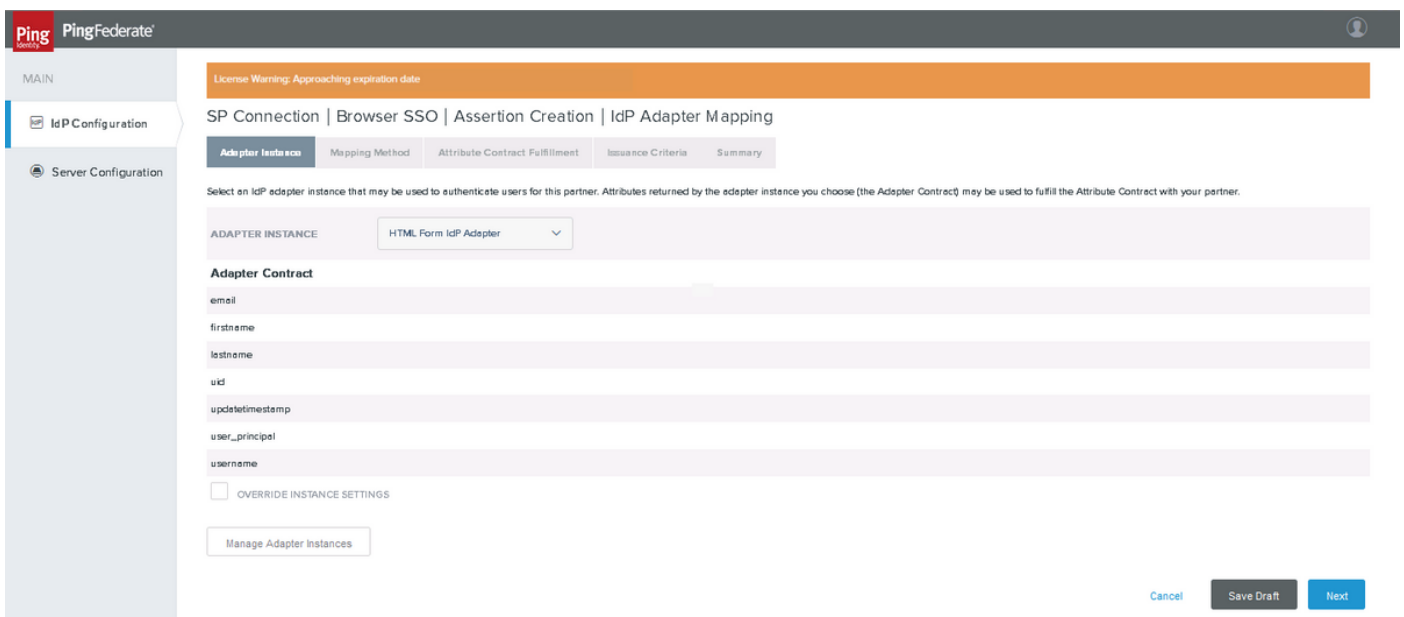
要使用瞬態作為名稱識別符號的SSO操作，請在saml2-subject-name-formats部分下新增xml項：
 <con:item name="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">urn:oasis:names:tc:SAML:2.0:nameid-format:transient</con:item>

按一下下一步

驗證來源對應

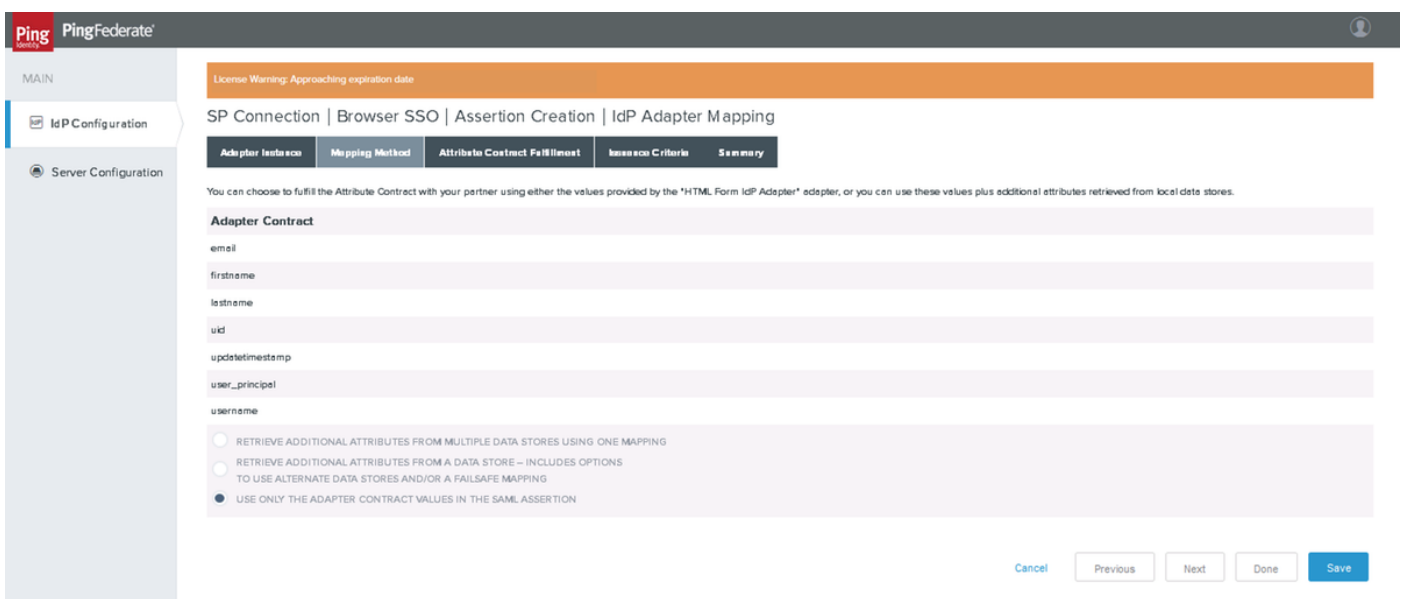


按一下Map New Adapter Instance



對映之前建立的HTML表單IdP介面卡。按一下下一步

對映方法



按一下下一步

屬性合約履行

License Warning: Approaching expiration date

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Adapter Instance | Mapping Method | Attribute Contract Fulfillment | Issuance Criteria | Summary

Fulfill your Attribute Contract with values from the authentication adapter or with dynamic text values.

Attribute Contract	Source	Value	Actions
SAML_AUTHN_CTX	Text	urn:oasis:names:tc:SAI	None available
SAML_NAME_FORMAT	Text	urn:oasis:names:tc:SAI	None available
SAML_SUBJECT	Adapter	username	None available
uid	Adapter	uid	None available
user_principal	Adapter	user_principal	None available

Copyright © 2003-2016 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

Cancel Previous Next Done Save

確保將值設定為

屬性合約	來源	價值
SAML_SUBJECT	介面卡	<p>使用者名稱</p> <p>非常重要附註：用於此設定的值必須與LDAP過濾器設定中使用的值相匹配 (節#3.1.3.2。例項配置)</p> <p>附註：此處使用了「username」，因為此處使用了 sAMAccountName=\${username}</p>
SAML_AUTHN_CTX	文本	urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport
SAML名稱格式	文本	urn:oasis:names:tc:SAML:2.0:nameid-format:transient
uid	介面卡	uid
user_principal	介面卡	user_principal

按一下下一步

發佈標準

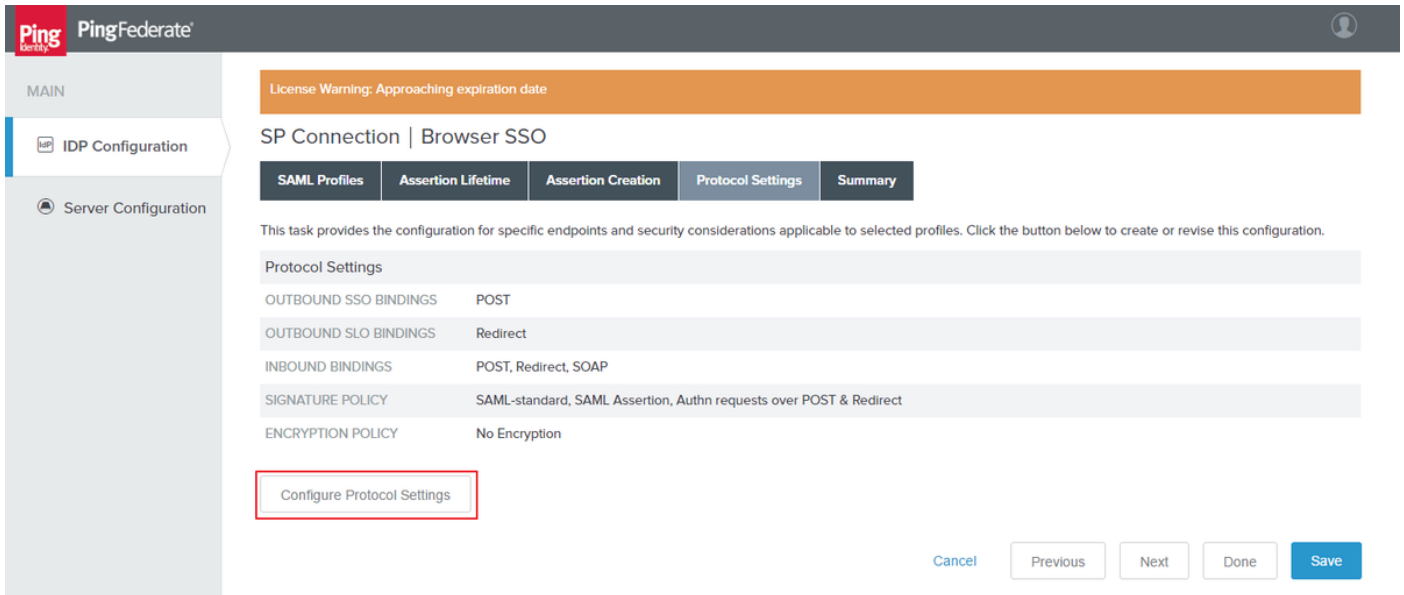
The screenshot shows the 'Attribute Contract Fulfillment' configuration screen in PingFederate. At the top, there is a license warning: 'License Warning: Approaching expiration date'. Below this, the navigation path is 'SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping'. The current step is 'Attribute Contract Fulfillment', with other steps being 'Adapter Instance', 'Mapping Method', 'Issuance Criteria', and 'Summary'. A descriptive text states: 'PingFederate can evaluate various criteria to determine whether users are authorized to access SP resources. Use this optional screen to configure the criteria for use with this conditional authorization.' Below this is a table with columns: Source, Attribute Name, Condition, Value, Error Result, and Action. The table is currently empty, with dropdown menus for Source, Attribute Name, and Condition, and an 'Add' button in the Action column. At the bottom right, there are navigation buttons: Cancel, Previous, Next, Done, and Save.

摘要

The screenshot shows the 'Summary' configuration screen in PingFederate. At the top, there is a license warning: 'License Warning: Approaching expiration date'. Below this, the navigation path is 'SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping'. The current step is 'Summary', with other steps being 'Adapter Instance', 'Mapping Method', 'Attribute Contract Fulfillment', and 'Issuance Criteria'. A note says: 'Click a heading link to edit a configuration setting.' The configuration is organized into sections: 'Adapter Instance' (Selected adapter: HTML Form IdP Adapter 1), 'Mapping Method' (Adapter: HTML Form IdP Adapter, Mapping Method: Use only the Adapter Contract values in the mapping), 'Attribute Contract Fulfillment' (uid: uid (Adapter), SAML_AUTHN_CTX: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport (Text), user_principal: user_principal (Adapter), SAML_SUBJECT: username (Adapter), SAML_NAME_FORMAT: urn:oasis:names:tc:SAML:2.0:nameid-format:transient (Text)), and 'Issuance Criteria' (Criterion: (None)). At the bottom right, there are navigation buttons: Cancel, Previous, Done, and Save.

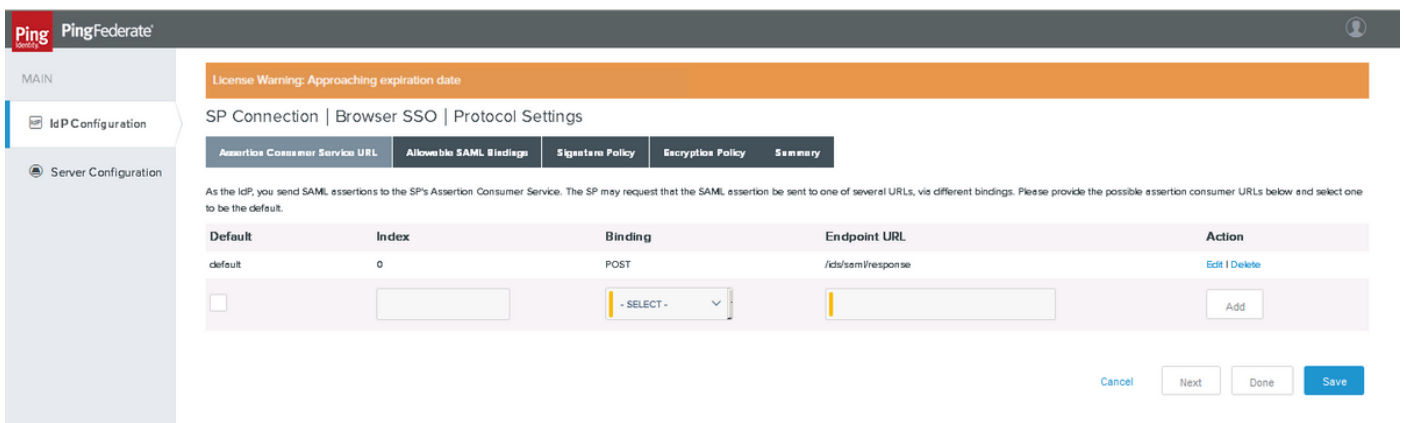
驗證設定並按一下Done

協定設定



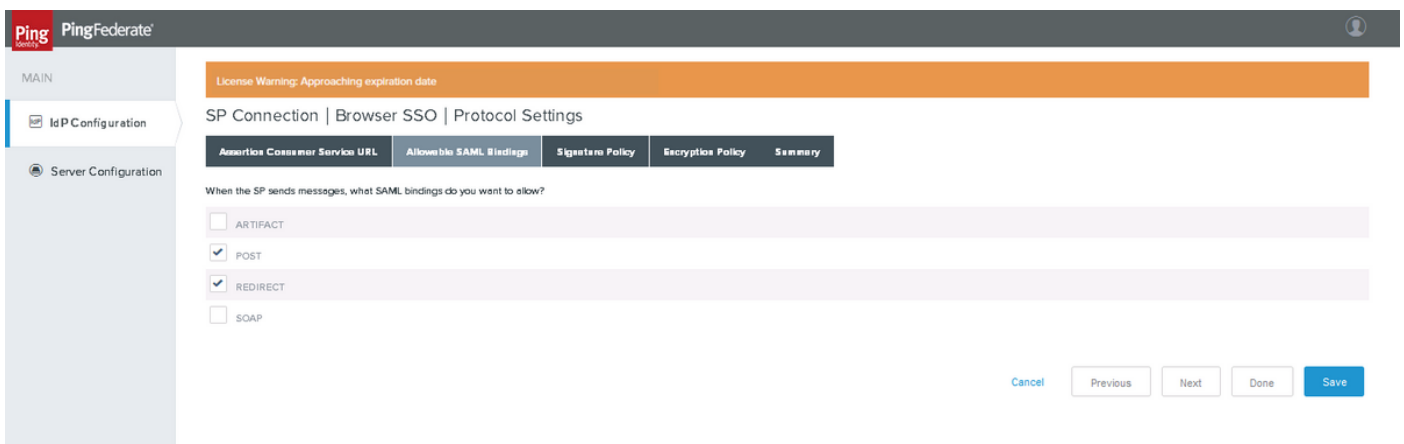
按一下Configure Protocol Settings

斷言使用者服務URL



新增POST繫結SSO終結點。按一下下一步

允許的SAML繫結



按一下下一步

簽名策略

The screenshot shows the PingFederate administration console. The left sidebar has 'MAIN' at the top, followed by 'IdP Configuration' and 'Server Configuration'. The main content area is titled 'SP Connection | Browser SSO | Protocol Settings'. Below the title are tabs for 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signing Policy', 'Encryption Policy', and 'Summary'. The 'Signing Policy' tab is active. A license warning banner is at the top. The text below reads: 'Additional guarantees of authenticity may be agreed upon between you and your partner. For SP-initiated SSO, you can choose to require signed authentication requests sent via the POST or redirect bindings. You can also choose to sign assertions sent to this partner, regardless of the binding used.' There are two checkboxes: 'REQUIRE AUTHN REQUESTS TO BE SIGNED WHEN RECEIVED VIA THE POST OR REDIRECT BINDINGS' (checked) and 'ALWAYS SIGN THE SAML ASSERTION' (unchecked). At the bottom right are buttons for 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

注意: Cisco IdS 保證 SAML 消息為「簽名」，因此不要選擇「始終對 SAML 斷言簽名」。這是因為 PingFederate 會簽署「SAML 斷言」或「SAML 響應」，而不是同時簽署。

按一下下一步

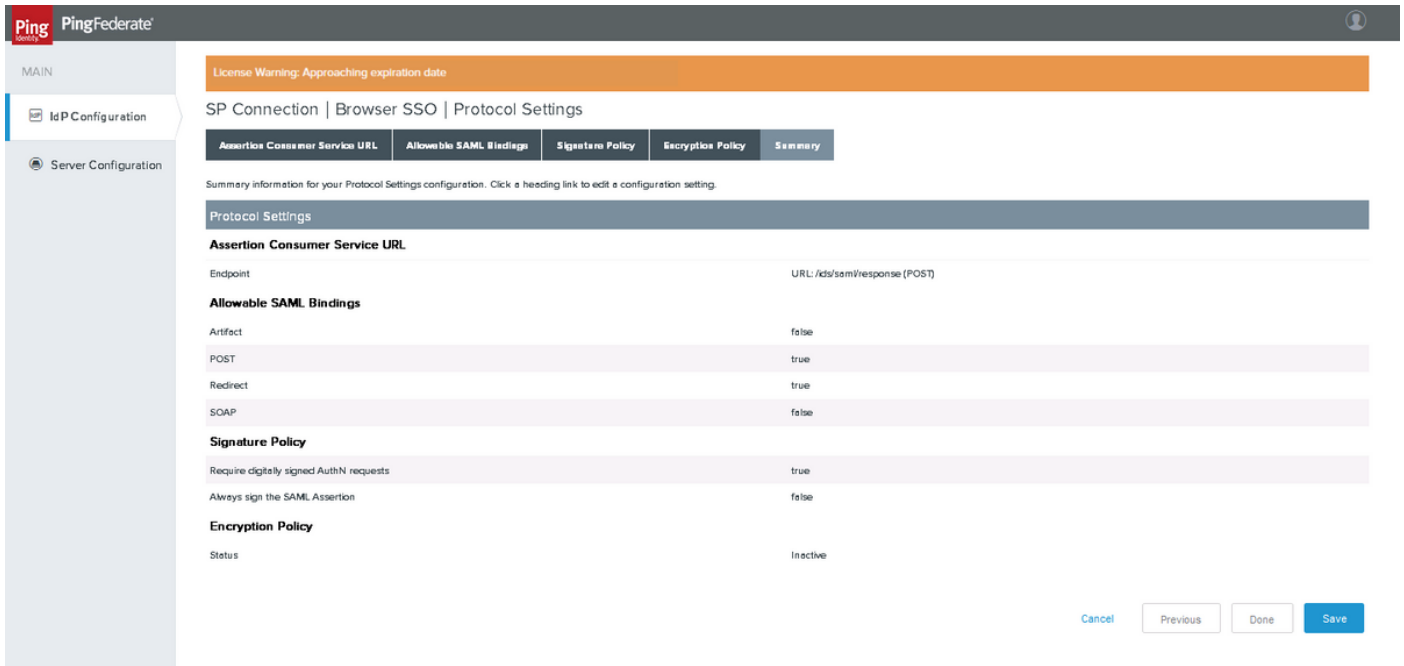
加密策略

The screenshot shows the PingFederate administration console. The left sidebar has 'MAIN' at the top, followed by 'IdP Configuration' and 'Server Configuration'. The main content area is titled 'SP Connection | Browser SSO | Protocol Settings'. Below the title are tabs for 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signing Policy', 'Encryption Policy', and 'Summary'. The 'Encryption Policy' tab is active. A license warning banner is at the top. The text below reads: 'Additional guarantees of privacy may be used between you and your partner. Specify an encryption policy for the exchange of SAML messages.' There are three radio buttons: 'NONE' (selected), 'THE ENTIRE ASSERTION', and 'ONE OR MORE ATTRIBUTES'. Below these are five checkboxes: 'SAML_SUBJECT', 'SAML_NAME_FORMAT', 'UID', and 'USER_PRINCIPAL'. At the bottom right are buttons for 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

註: Cisco IdS 不支援加密的 SAML 流，因此為「Encryption Policy」設定選擇「NONE」。

按一下下一步

摘要



The screenshot shows the 'Protocol Settings' page in PingFederate. At the top, there is a license warning: 'License Warning: Approaching expiration date'. The page title is 'SP Connection | Browser SSO | Protocol Settings'. Below the title are tabs for 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signature Policy', 'Encryption Policy', and 'Summary'. The 'Summary' tab is selected. A summary text reads: 'Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.' The main content area is titled 'Protocol Settings' and contains several sections:

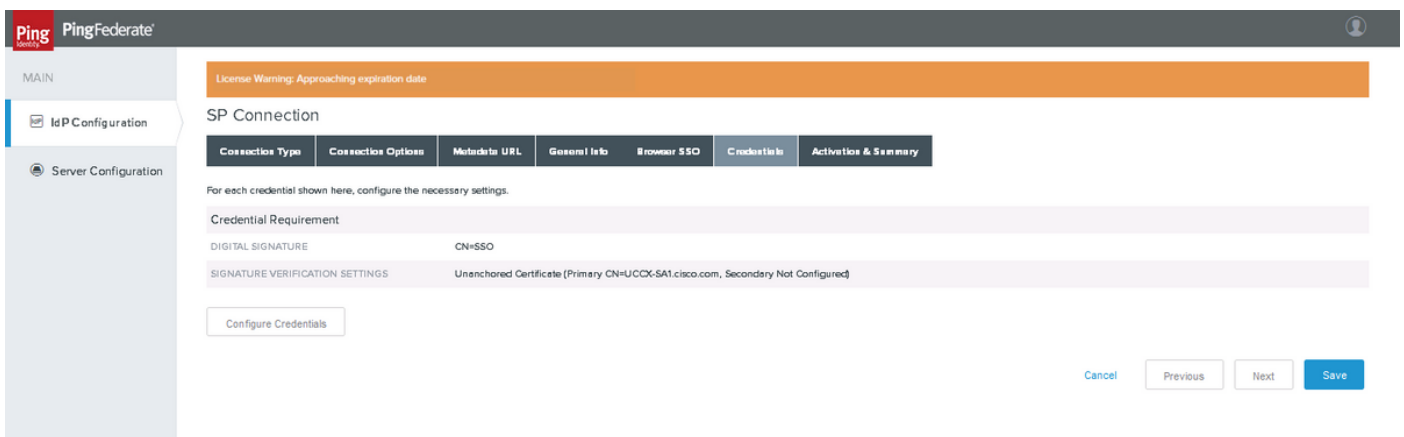
- Assertion Consumer Service URL:** Endpoint is 'URL:/ids/saml/response (POST)'.
- Allowable SAML Bindings:** A table with columns for binding type and a boolean value.

Artifact	false
POST	true
Redirect	true
SOAP	false
- Signature Policy:**
 - Require digitally signed AuthN requests: true
 - Always sign the SAML Assertion: false
- Encryption Policy:**
 - Status: Inactive

 At the bottom right, there are buttons for 'Cancel', 'Previous', 'Done', and 'Save'.

驗證設定並按一下Done

憑證



The screenshot shows the 'Credentials' page in PingFederate. At the top, there is a license warning: 'License Warning: Approaching expiration date'. The page title is 'SP Connection'. Below the title are tabs for 'Connection Type', 'Connection Options', 'Metadata URL', 'General Info', 'Browser SSO', 'Credentials', and 'Activation & Summary'. The 'Credentials' tab is selected. A text block reads: 'For each credential shown here, configure the necessary settings.' The main content area is titled 'Credential Requirement' and contains two rows:

- DIGITAL SIGNATURE:** CN=SSO
- SIGNATURE VERIFICATION SETTINGS:** Unanchored Certificate (Primary CN=UCCX-SA1.cisco.com, Secondary Not Configured)

 Below this is a button labeled 'Configure Credentials'. At the bottom right, there are buttons for 'Cancel', 'Previous', 'Next', and 'Save'.

按一下Configure Credentials

數位簽章設定

License Warning: Approaching expiration date

SP Connection | Credentials

Digital Signature Settings | Signature Verification Settings | Summary

You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.

SIGNING CERTIFICATE: 02:1E:14:B4 (cn=pingserver.cisco.com) ▼

INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.

INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE> ELEMENT.

SIGNING ALGORITHM: RSA SHA1 ▼

Manage Certificates

Cancel Next Done Save

選擇SIGNING CERTIFICATE CREATED Early。如果沒有，您可以按一下Manage Certificates以建立證書。

注意: Cisco IdS不支持SAML響應簽名的RSA SHA256，因此使用了「RSA SHA1」。

按一下下一步

簽名驗證設定

License Warning: Approaching expiration date

SP Connection | Credentials

Back-Channel Authentication | Digital Signature Settings | Signature Verification Settings | Summary

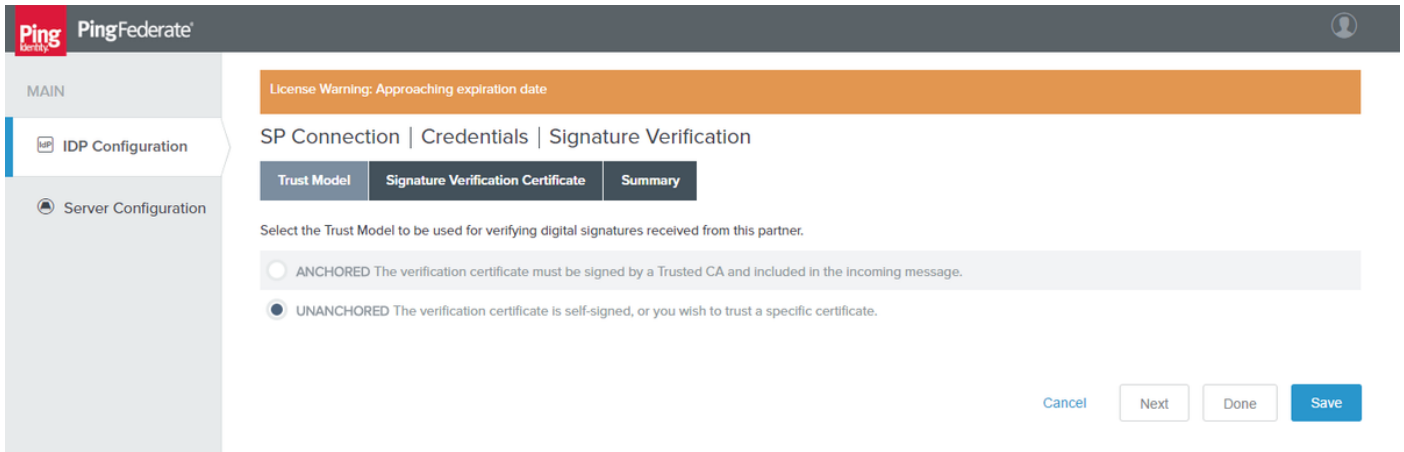
Incoming SAML messages or security tokens may be digitally signed. This configuration task provides options for verifying signatures.

Manage Signature Verification Settings

Cancel Previous Next Done Save

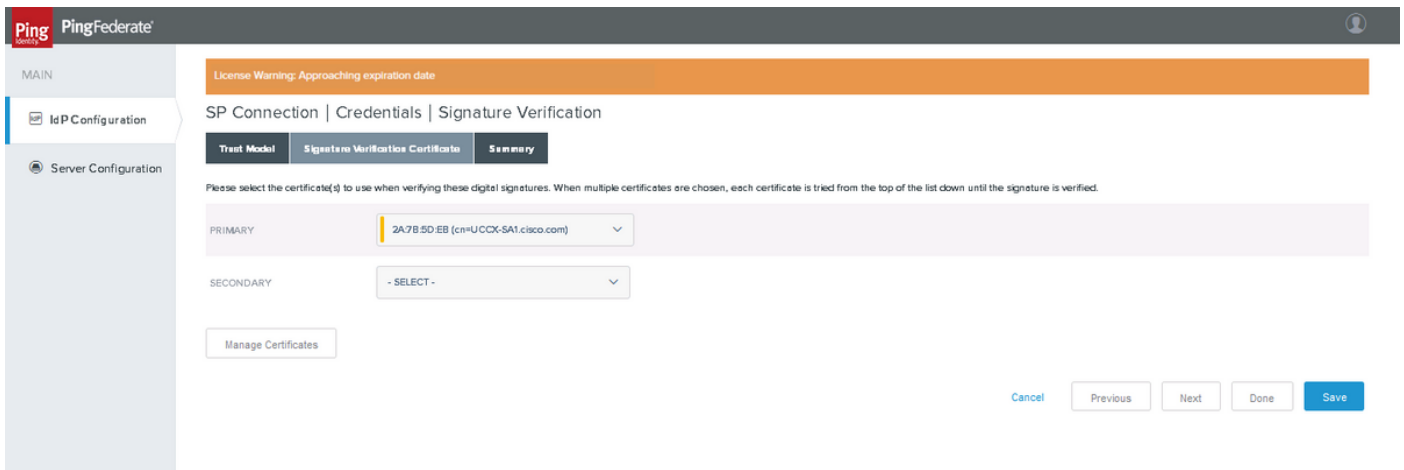
按一下管理簽名驗證設定

信任模型

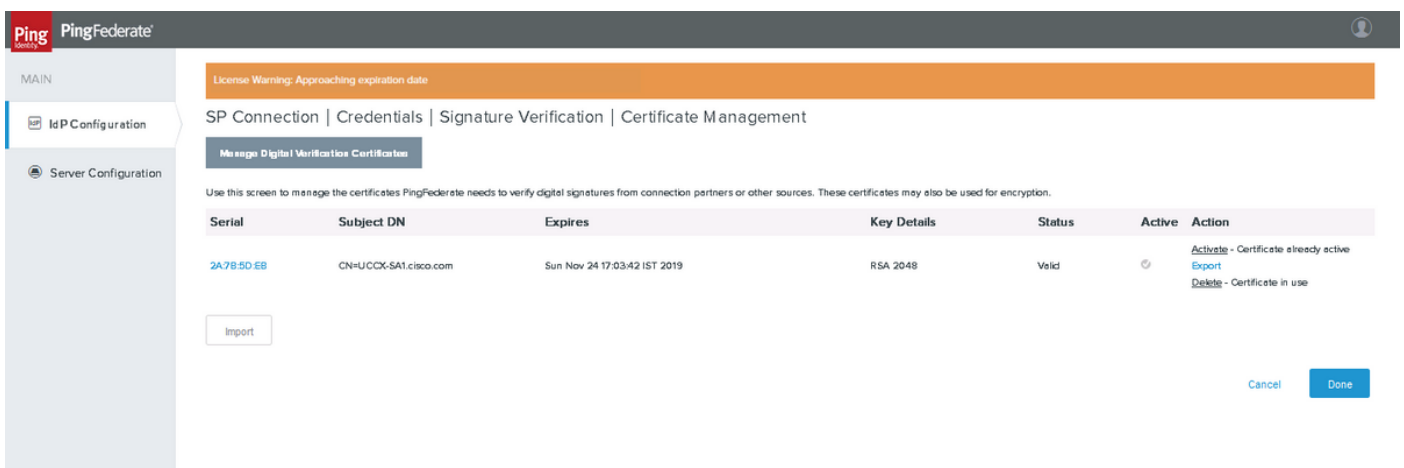


按一下下一步

簽名驗證證書



按一下Manage Certificates以從SP匯入證書。



按一下「Import」以匯入憑證。

摘要

按一下完成

摘要

驗證摘要並按一下Done

啟用與摘要

SP Connection

Connection Type	Connection Options	Metadata URL	General Info	Browser SSO	Credentials	Activation & Summary
-----------------	--------------------	--------------	--------------	-------------	-------------	----------------------

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status	<input checked="" type="radio"/> ACTIVE <input type="radio"/> INACTIVE
SSO Application Endpoint	https://pingserver.cisco.com:9031/idp/startSSO.ping?PartnerSpId=UCCX-SA1.cisco.com

Summary

SP Connection

Connection Type

Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false

Connection Options

Browser SSO	true
IdP Discovery	false
Attribute Query	false

General Info

Partner's Entity ID (Connection ID)	UCCX-SA1.cisco.com
Base URL	https://UCCX-SA1.cisco.com:8553

Browser SSO

SAML Profiles

IdP-Initiated SSO	true
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	false

Assertion Lifetime

Valid Minutes Before	5
Valid Minutes After	5

Assertion Creation

Identity Mapping

Enable Transient Identifier	true
Include additional attributes	false

Authentication Source Mapping

Adapter instance name	HTML Form IdP Adapter 1
-----------------------	-------------------------

Adapter Instance

Selected adapter	HTML Form IdP Adapter 1
------------------	-------------------------

MAIN

- IdP Configuration
- Server Configuration

Copyright © 2003-2016

Mapping Method

Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping

Attribute Contract Fulfillment

Issuance Criteria

Criterion	(None)
-----------	--------

Protocol Settings

Assertion Consumer Service URL

Endpoint	URL: /ids/saml/response (POST)
----------	--------------------------------

Allowable SAML Bindings

Artifact	false
POST	true
Redirect	true
SOAP	false

Signature Policy

Require digitally signed AuthN requests	true
Always sign the SAML Assertion	false

Encryption Policy

Status	Inactive
--------	----------

Credentials

Digital Signature Settings

Selected Certificate	CN=pingserver.cisco.com, OU=cisco, O=ccbu, L=bangalore, ST=Karnataka, C=IN
Include Certificate in KeyInfo	true
Include Raw Key in KeyValue	true
Selected Signing Algorithm	RSA SHA1

Signature Verification

Trust Model

Trust Model	Unanchored
-------------	------------

Signature Verification Certificate

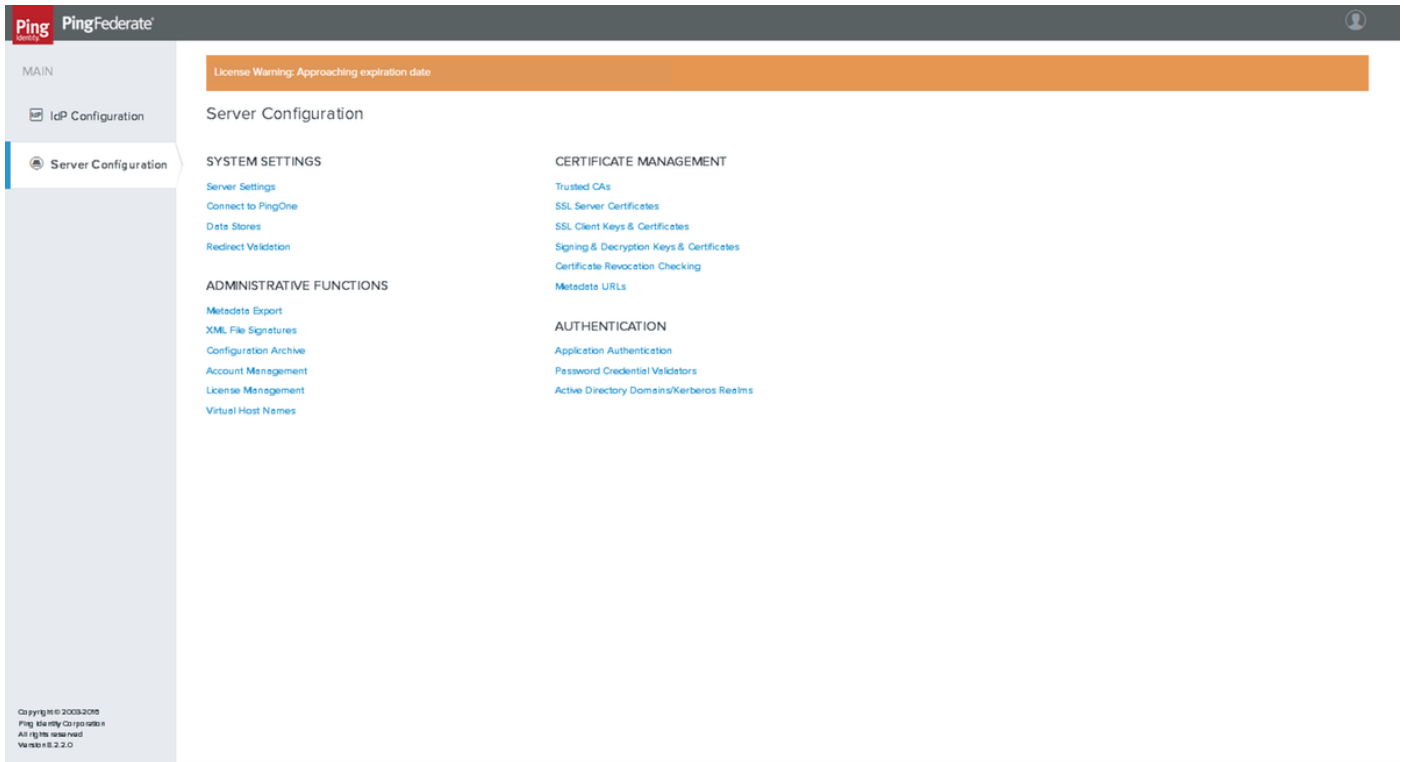
Selected Certificate	CN=UCCX-SA1.cisco.com
----------------------	-----------------------

Cancel Previous Save

驗證摘要並按一下Save。

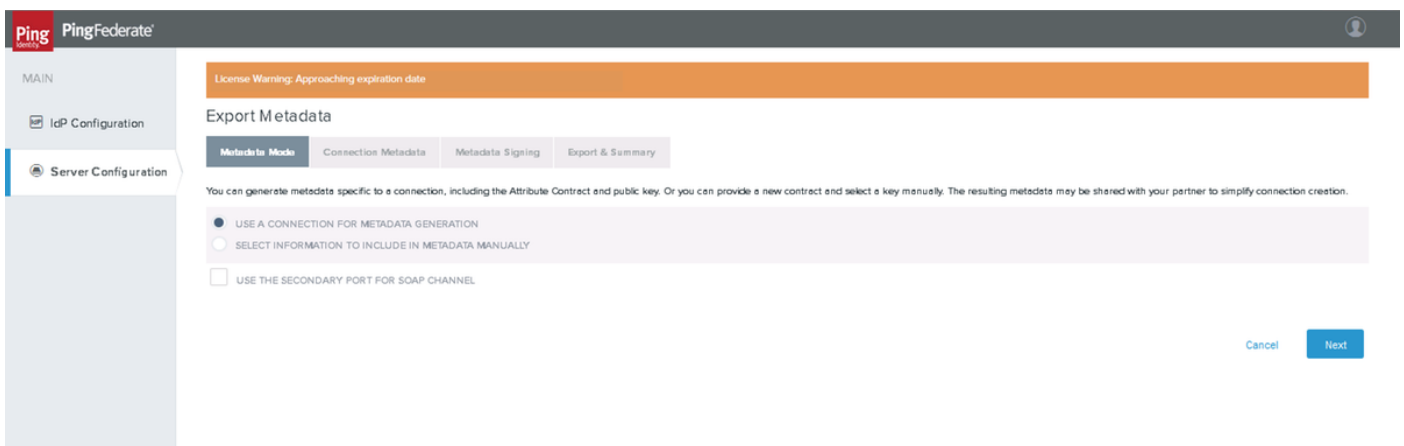
匯出PingFederate後設資料

後設資料匯出



後設資料模式

按一下Server Configuration > ADMINISTRATIVE FUNCTIONS > Metadata Export



按一下下一步

連線後設資料

Export Metadata

Metadata Mode Connection Metadata Metadata Signing Export & Summary

Select a connection that contains the Attribute Contract and Digital Signature Key you wish to include in the metadata.

UCCX-SA1.cisco.com

Attribute Contract

SAML_AUTHN_CTX

SAML_NAME_FORMAT

uid

user_principal

DIGITAL SIGNATURE KEY
CN=pingserver.cisco.com, OU=cisco, O=ccbu, L=bangalore, ST=Karnataka, C=IN

XML ENCRYPTION KEY
No XML key available for this connection

Cancel Previous Next

選擇已建立的SP連線，然後按一下下一步

後設資料簽名

PingFederate

License Warning: Approaching expiration date

Export Metadata

Metadata Mode Connection Metadata Metadata Signing Export & Summary

From this list of certificates, choose which one to use for signing the selected file.

SIGNING CERTIFICATE 01584CA89AF6 (cn=SSC)

INCLUDE THIS CERTIFICATE'S PUBLIC KEY CERTIFICATE IN THE <KEYINFO> ELEMENT.

INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALU> ELEMENT.

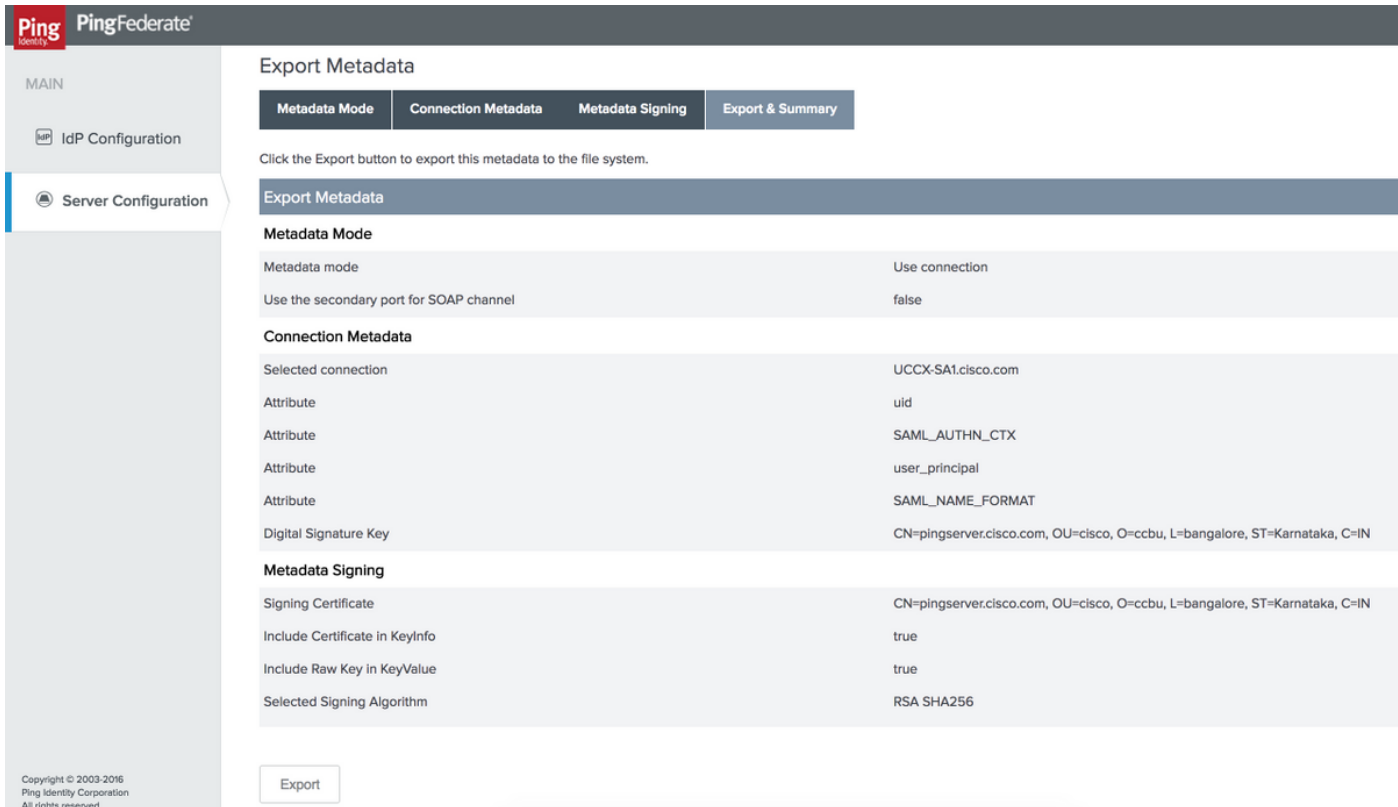
SIGNING ALGORITHM RSA-SHA256

Manage Certificates

Cancel Previous Next

選擇已建立的後設資料證書並將SIGNING ALGORITHM作為RSA SHA256。單擊「下一步」

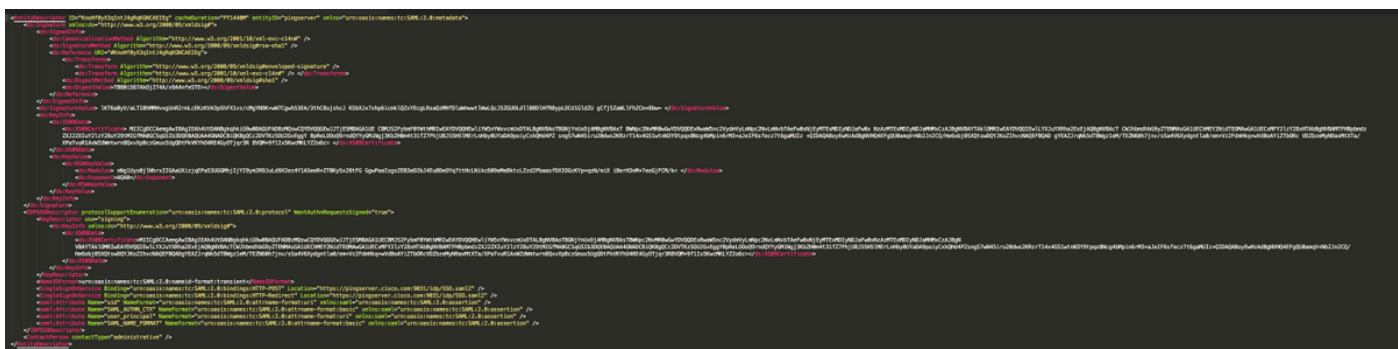
匯出與摘要



按一下Export並在本地系統中儲存檔案。

- 編輯下載的後設資料XML檔案，以刪除「md」名稱空間條目並儲存它
- 然後，將儲存的後設資料檔案從idsadmin頁上載到IdS以建立IDP信任

後設資料示例



疑難排解

問題	工具	可能起因
在IdS管理頁中上傳PingFederate後設資料失敗	文本檔案編輯器	確保後設資料XML檔案沒有「md」名稱空間條目。
SAML流失敗	SAML跟蹤器	檢查「StatusCode」是否表示「Success」，即<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />

問題	工具	可能起因
		<ul style="list-style-type: none"> • 如果不是，請檢查它是否指示「Requester」或「Responder」 <ul style="list-style-type: none"> ◦ 「Requester」意味著SAML請求出現問題，即Cisco IdS未正確傳送請求。檢查/opt/cisco/ids/log/資料夾下的Cisco IdS日誌 ◦ 「Responder」意味著IdP問題 — 因此請檢查PingFederate日誌
SAML流失敗	SAML跟蹤器	<p>檢查<saml:AuthnContextClassRef>元素 — 其值必須是urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport</p> <p>如果其值設定為urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified — 則檢查是否正確配置並對映SAML_AUTHN_CTXcontract。</p>
SAML流失敗	SAML跟蹤器	<p>檢查<saml:AttributeStatement>元素 — 它必須存在並且必須包含與「uid」和「user_principal」對應的子元素</p> <p>如果未找到，請檢查「Assertion Creation」設定後跟「Contract Fulfillment」設定，以確保已正確定義和對映合約屬性</p>
SAML流失敗	SAML跟蹤器	<p>檢查Cisco Id或PingFederate日誌中是否存在「Invalid Signature」（無效簽名）消息。</p> <p>如果確認，請在Id和PingFederate之間重新建立後設資料信任</p>
SAML流失敗	SAML跟蹤器	<p>檢查時間條件，Cisco IdS收到SAML響應的時間必須介於<saml:Conditions NotBefore="2016-12-18T07:24:10.191Z" NotOnOrAfter="2016-12-18T07:34:10.191">中指定的時間之間</p>

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）。