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

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）
• 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	• Oracle Java SE Runtime Environment(Server JRE)7 update 79（64位） • Oracle Java SE Runtime Environment(Server JRE)8 update 45（64位）	• 鉻合金 • Firefox • Internet Explorer（版本9及更高版本） • Safari	• 鉻合金 • Firefox • Internet Explorer（版本9及更高版本）	• Microsoft Directory R2和2012 • Oracle Dir Server企業 11g • Microsoft SQL（結構詢語言）伺（2012和2014） • Oracle資料（10g和1 R2） • Oracle My 5.6

11 SP 3				

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

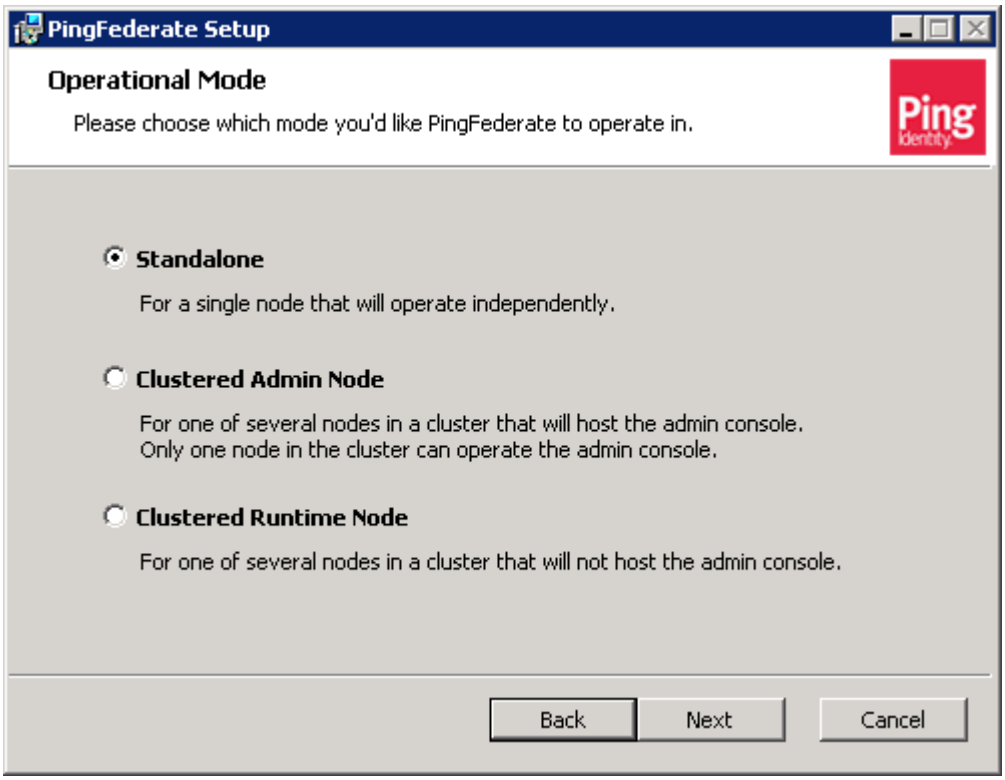
使用分發ZIP檔案安裝PingFederate

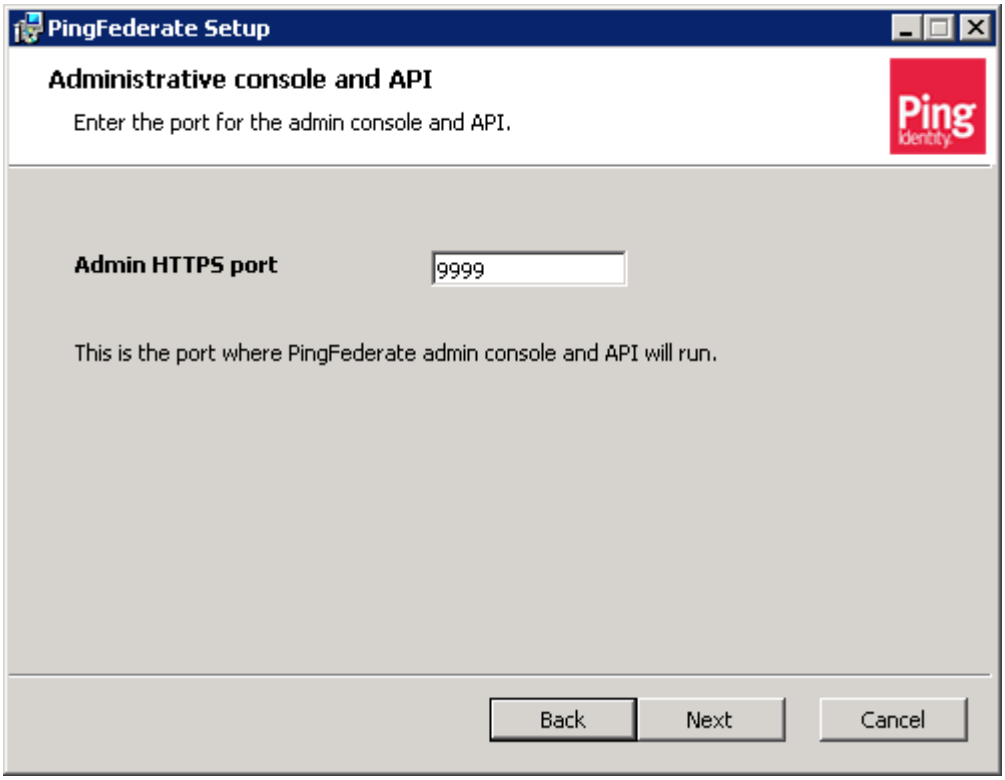
將分發ZIP檔案解壓縮到安裝目錄中。

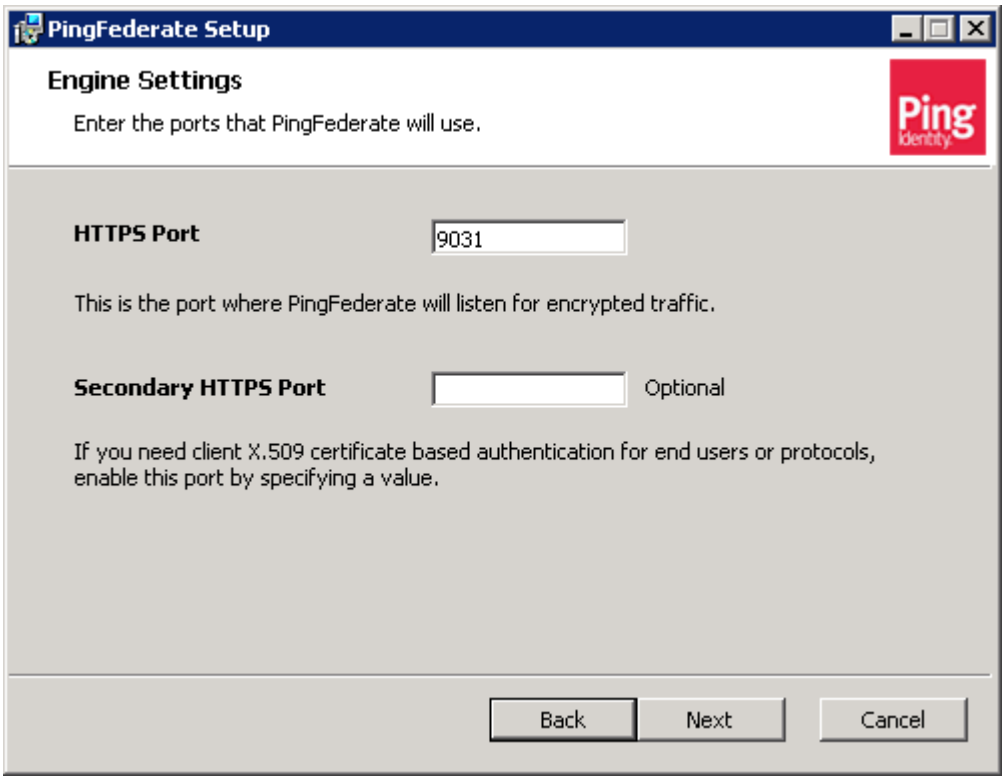
> 警告：為避免將來出現自動升級問題，請不要重新命名已安裝的pingfederate資料夾。如果要在同一台電腦上安裝PingFederate的多個例項（例如，在某些伺服器群集情況下），請在不同的位置安裝每個例項，或者重新命名父資料夾，以在相同的位置安裝並行檔案結構。

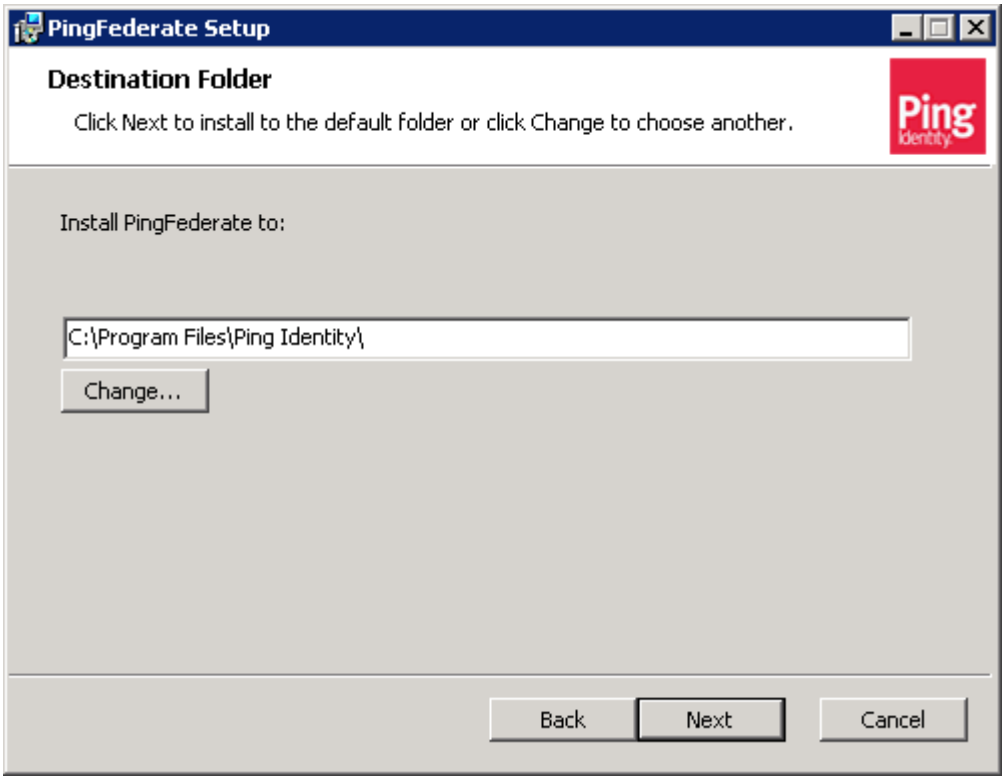
使用分發EXE檔案安裝PingFederate

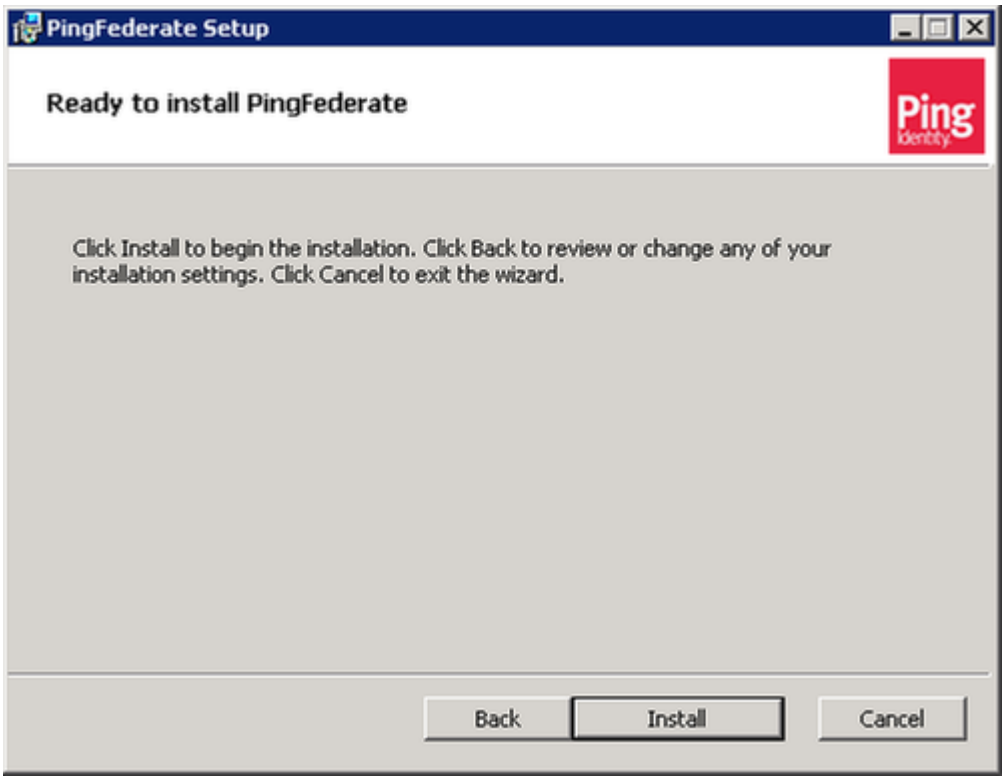
按兩下exe檔案，然後執行安裝步驟

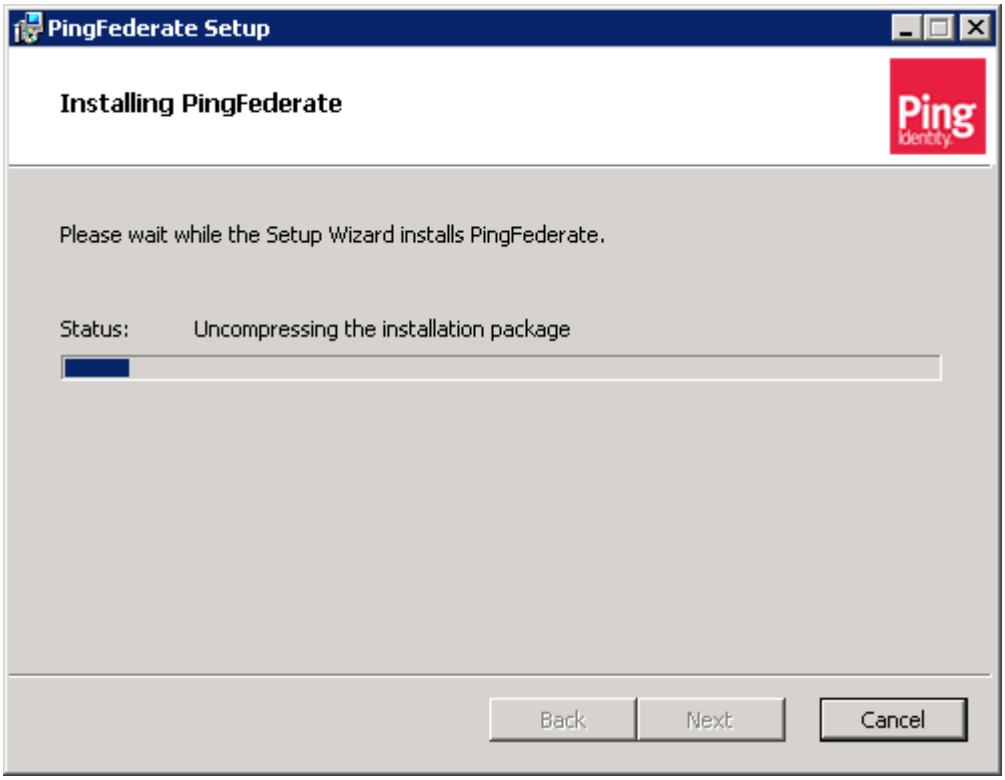

PingFederate Setup
Operational Mode
Please choose which mode you'd like PingFederate to operate in.
Ping identity
Standalone
For a single node that will operate independently.
Clustered Admin Node
For one of several nodes in a cluster that will host the admin console.
Only one node in the cluster can 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

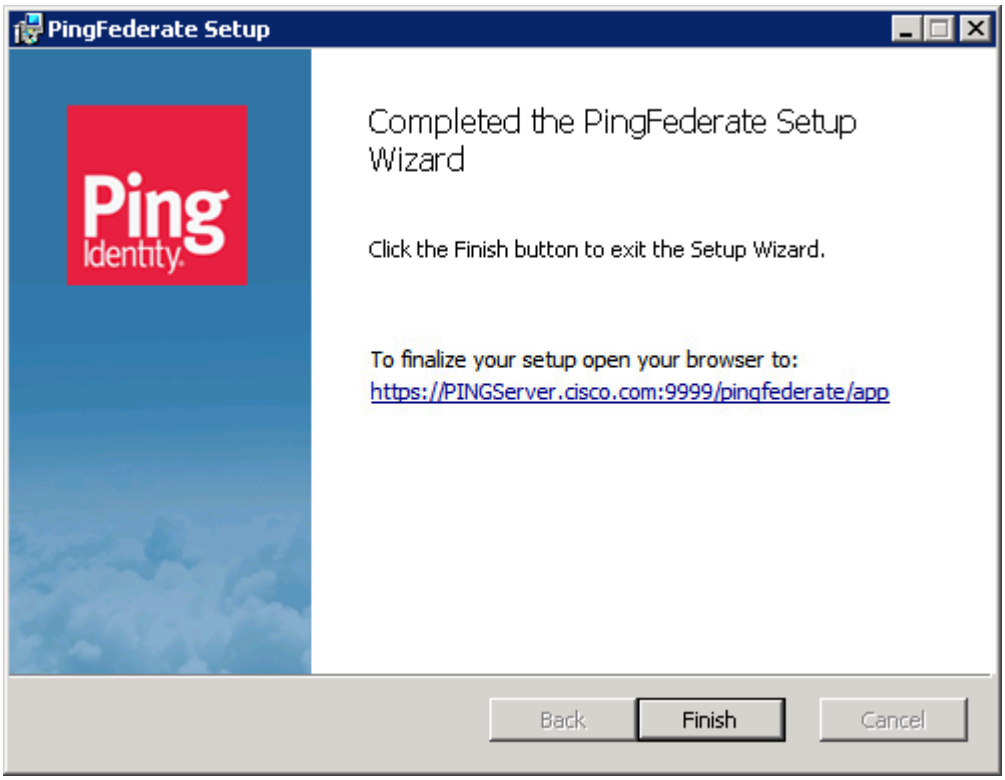

PingFederate Setup
Administrative console and API
Enter the port for the admin console and API.
Ping identity
Admin HTTPS port
9999
This is the port where PingFederate admin console and API will run.
Back
Next
Cancel


PingFederate Setup
Engine Settings
Enter the ports that PingFederate will use.
Ping identity
HTTPS Port
9031
This is the port where PingFederate will listen for encrypted traffic.
Secondary HTTPS Port
Optional
If you need client X.509 certificate based authentication for end users or protocols, enable this port by specifying a value.
Back
Next
Cancel


PingFederate Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Ping identity
Install PingFederate to:
C:\Program Files\Ping Identity\
Change...
Back
Next
Cancel


PingFederate Setup
Ready to install PingFederate
Ping identity
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel


PingFederate Setup
Installing PingFederate
Ping identity
Please wait while the Setup Wizard installs PingFederate.
Status: Uncompressing the installation package
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

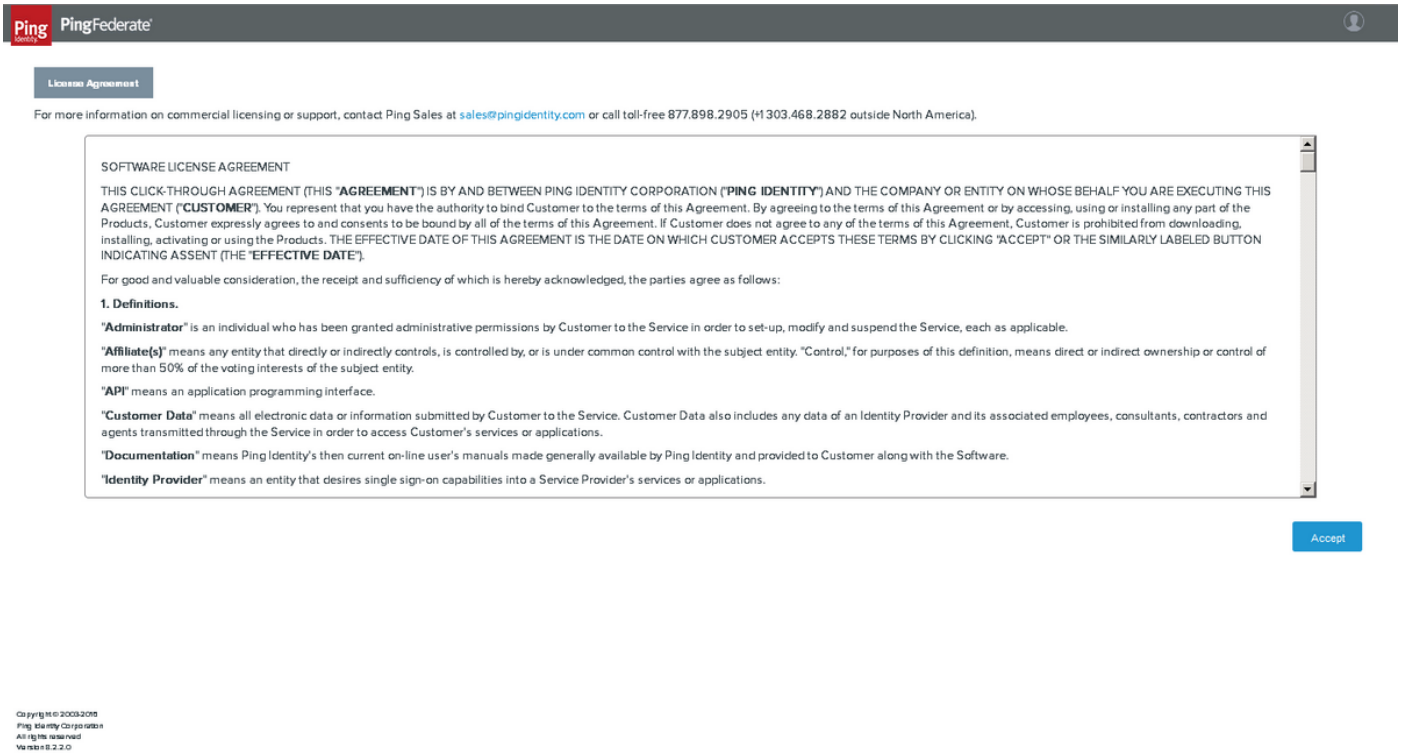
PingFederate管理員的使用者介面（管理控制檯）圍繞一個類似於嚮導的控制螢幕系統而構建。啟動PingFederate管理控制檯並使用初始設定嚮導完成身份聯合設定的配置。您還可以將PingFederate連線到PingOne，以部署強大的內部和基於雲的混合解決方案。

若要存取管理主控台：

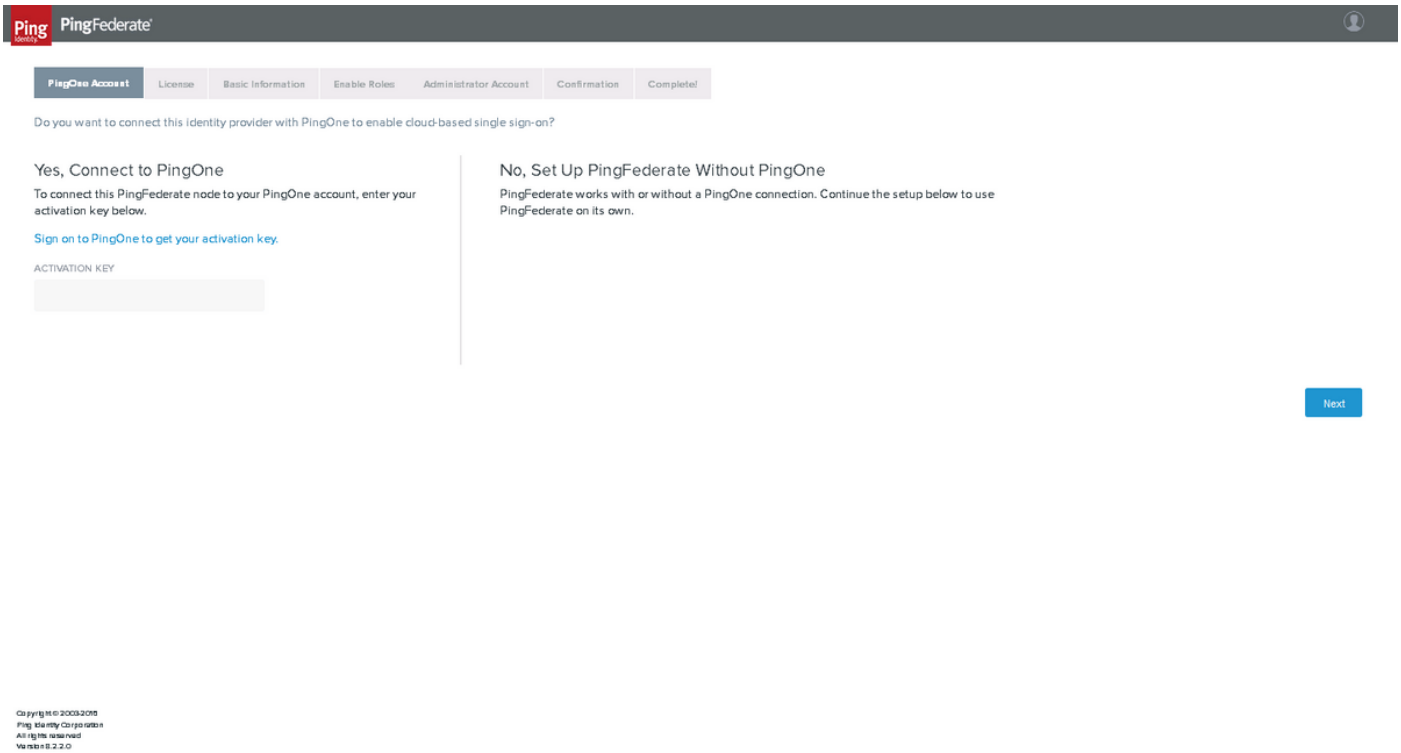
啟動瀏覽器並導航到https://<FQHN>:9999/pingfederate/app (其中<FQHN>是安裝PingFederate的伺服器的完全限定主機名)。

註:埠號9999預設設定。這可透過PingFederate屬性變更。

接受許可協定

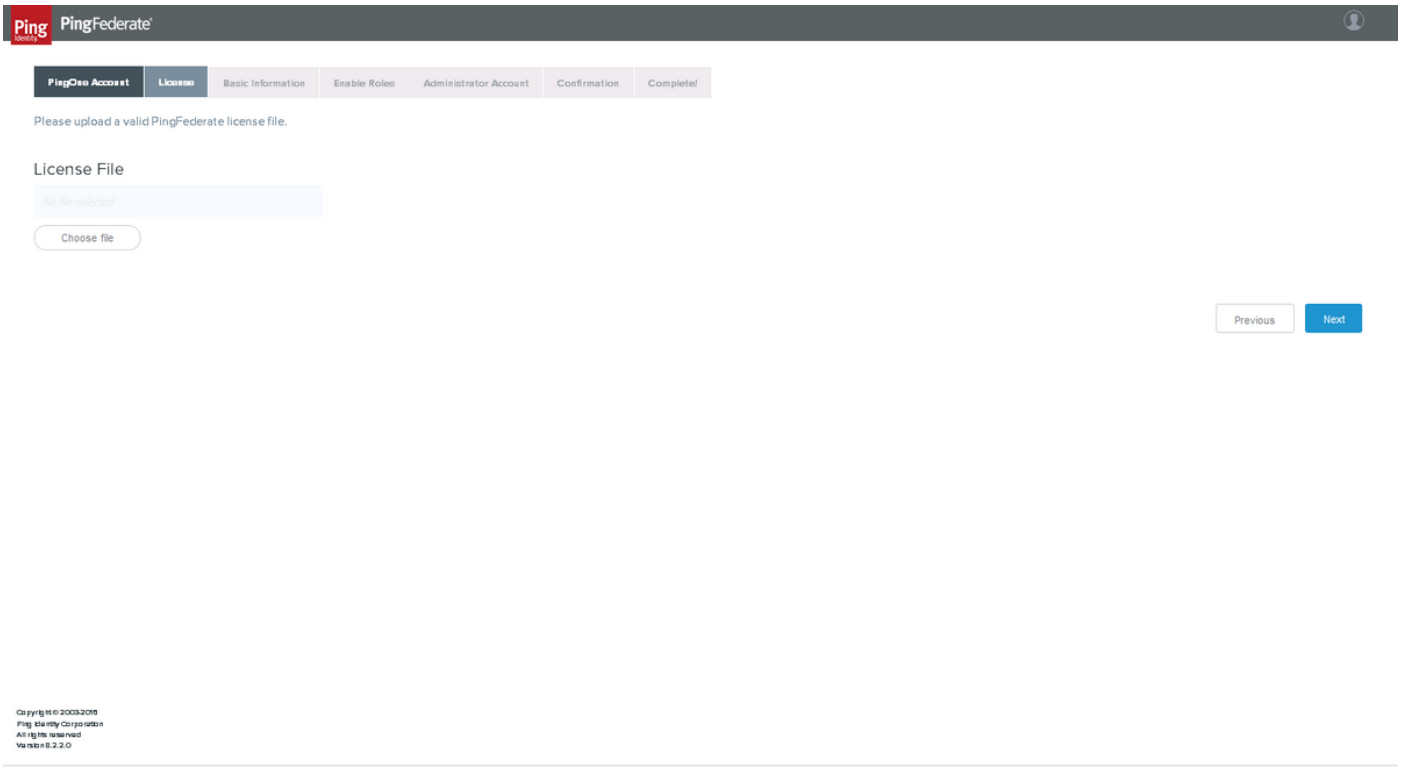


PingOne帳戶



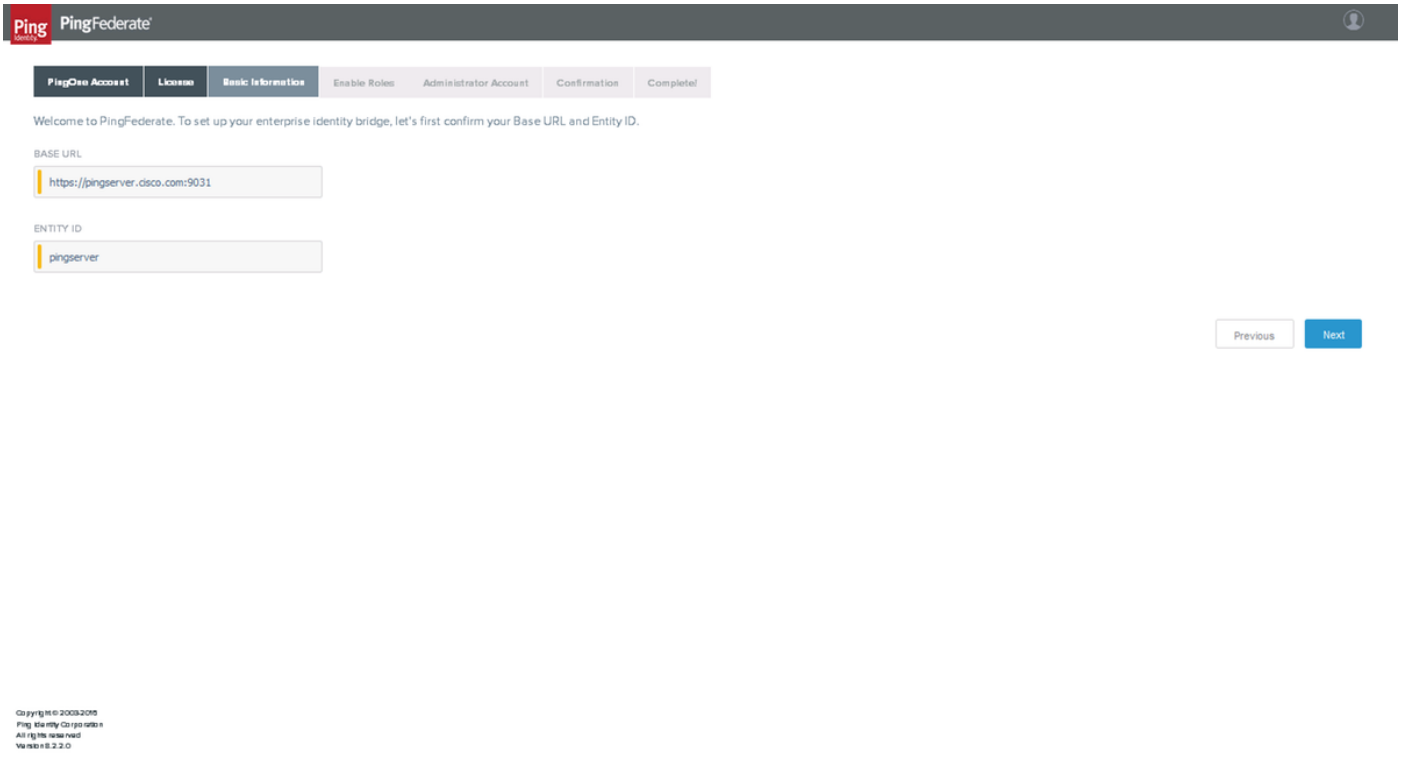
按一下下一步

授權



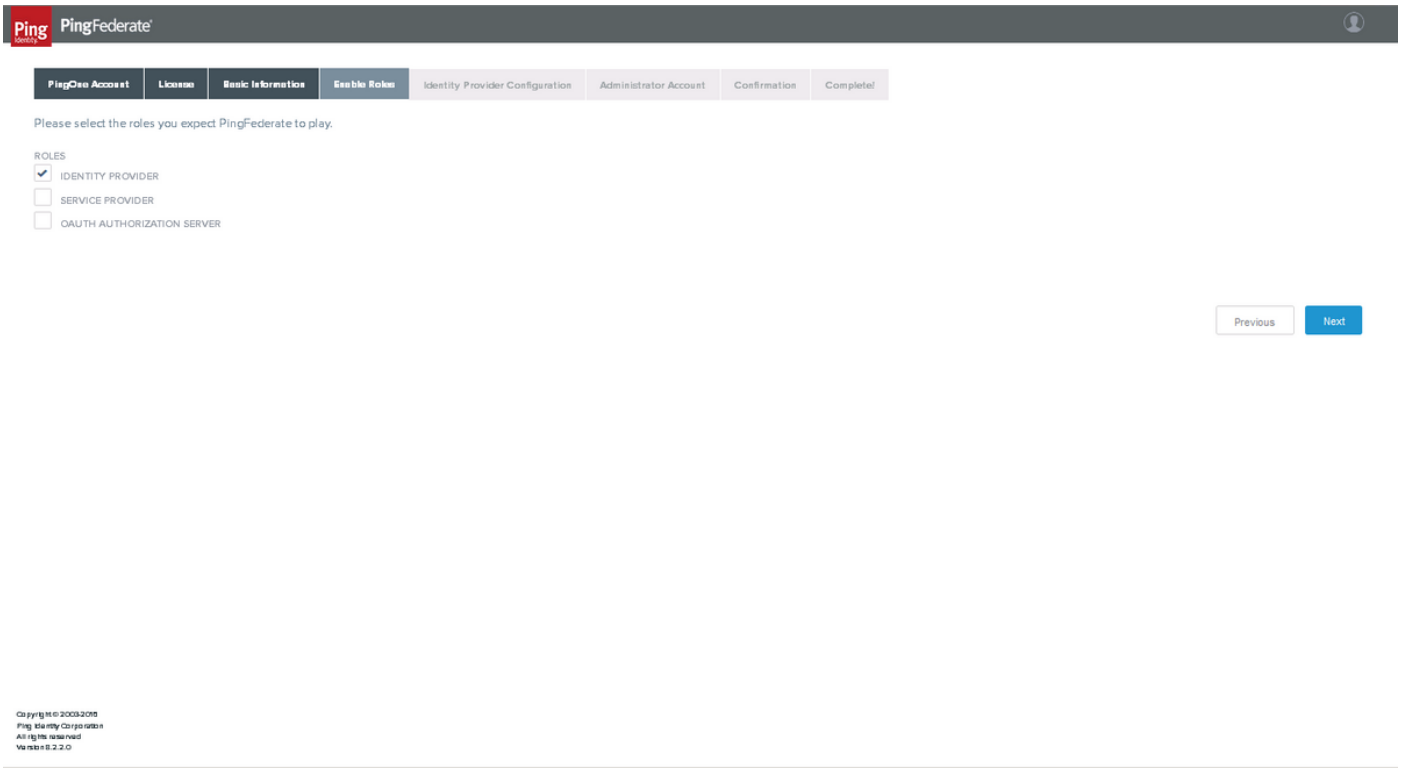
您必須從pingidentity.com購買或請求開發許可證，上傳許可證檔案，然後點選下一步

基本資訊



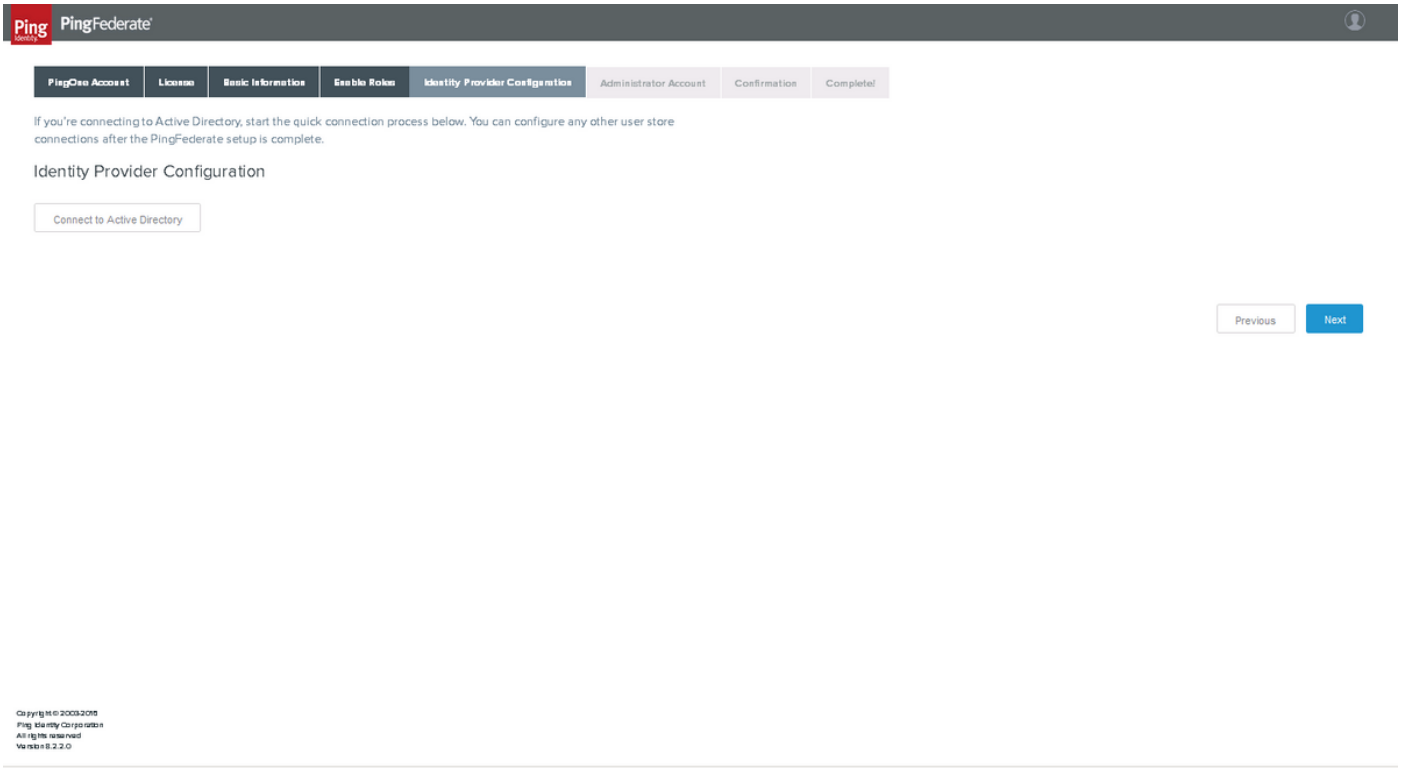
設定基本URL和實體ID，然後點選下一步

啟用角色



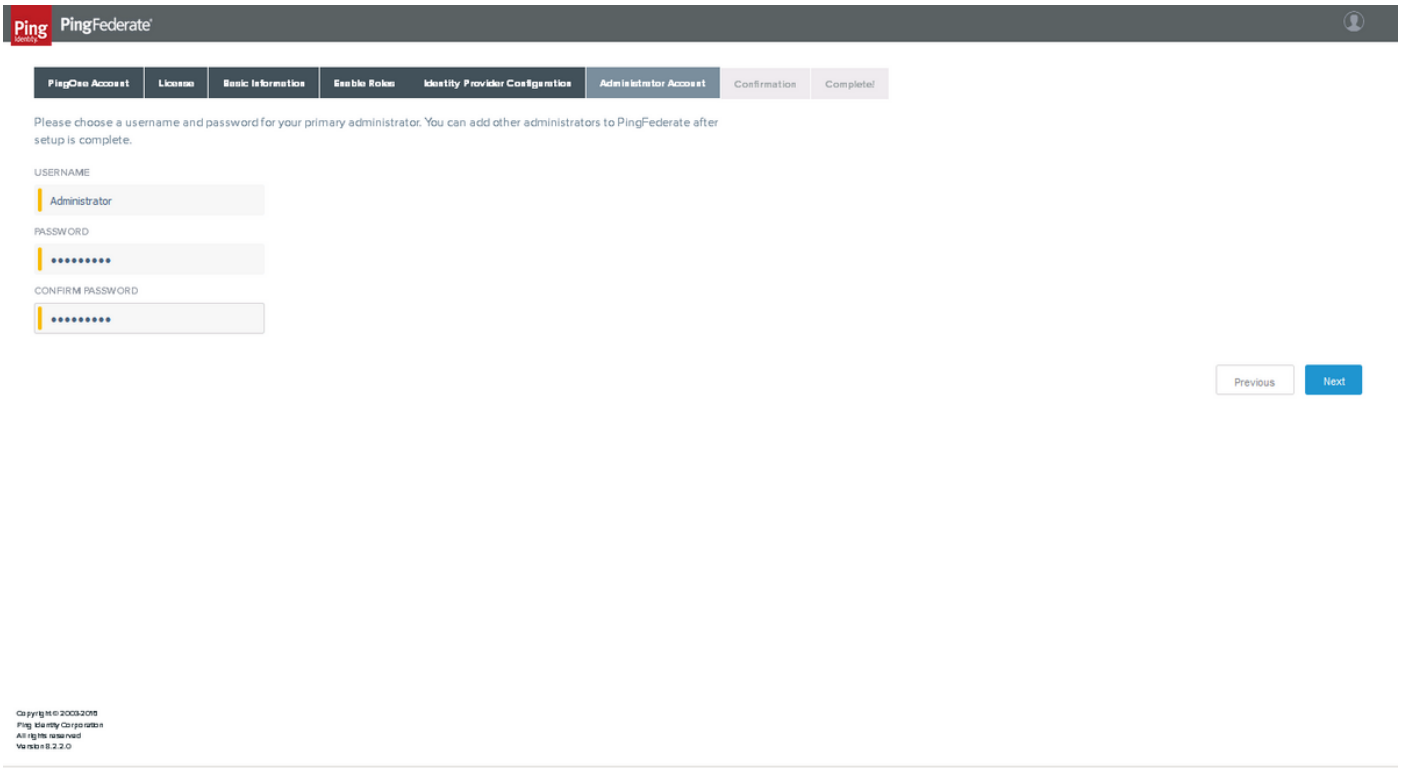
選擇IDENTITY PROVIDER並按一下Next

身份提供程式配置



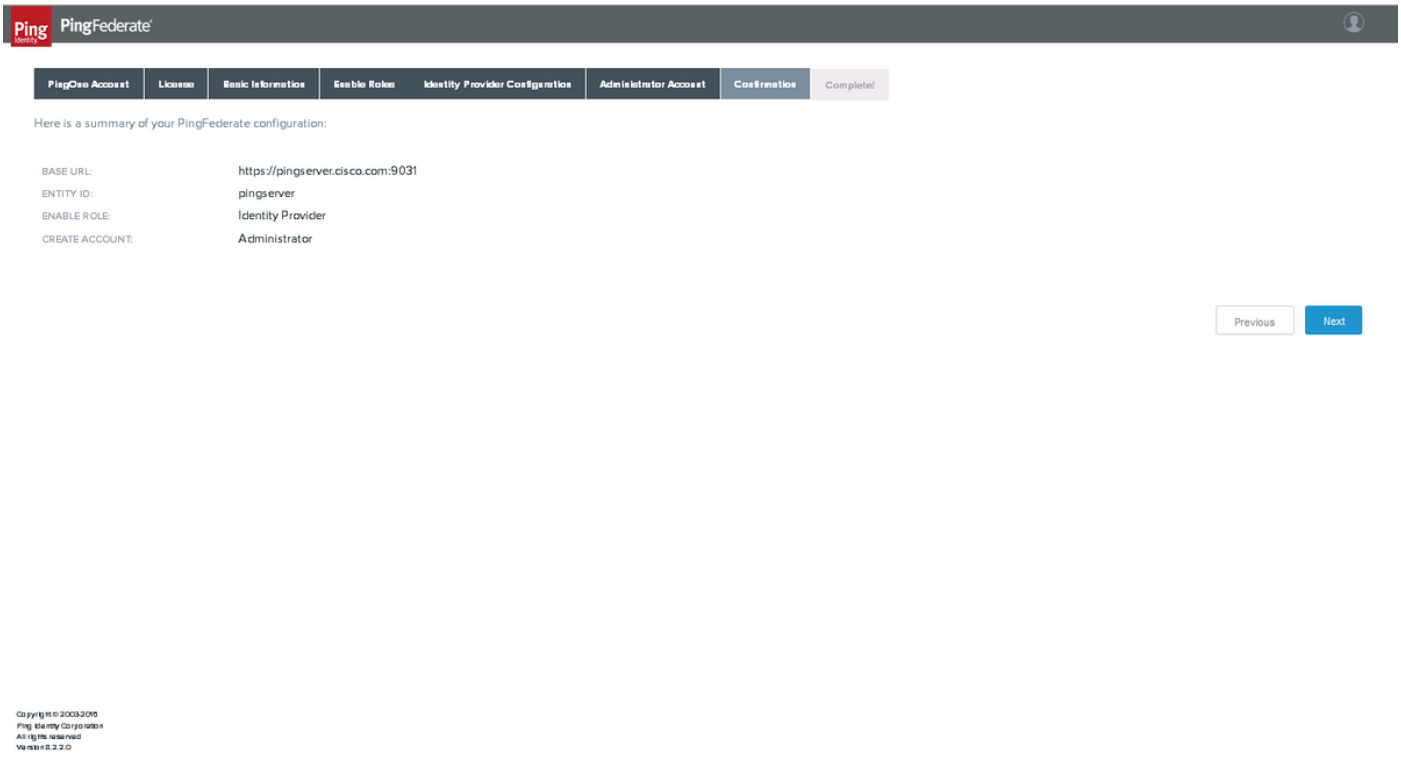
以後可以執行到Active Directory的連線，按一下下一步

管理員帳戶



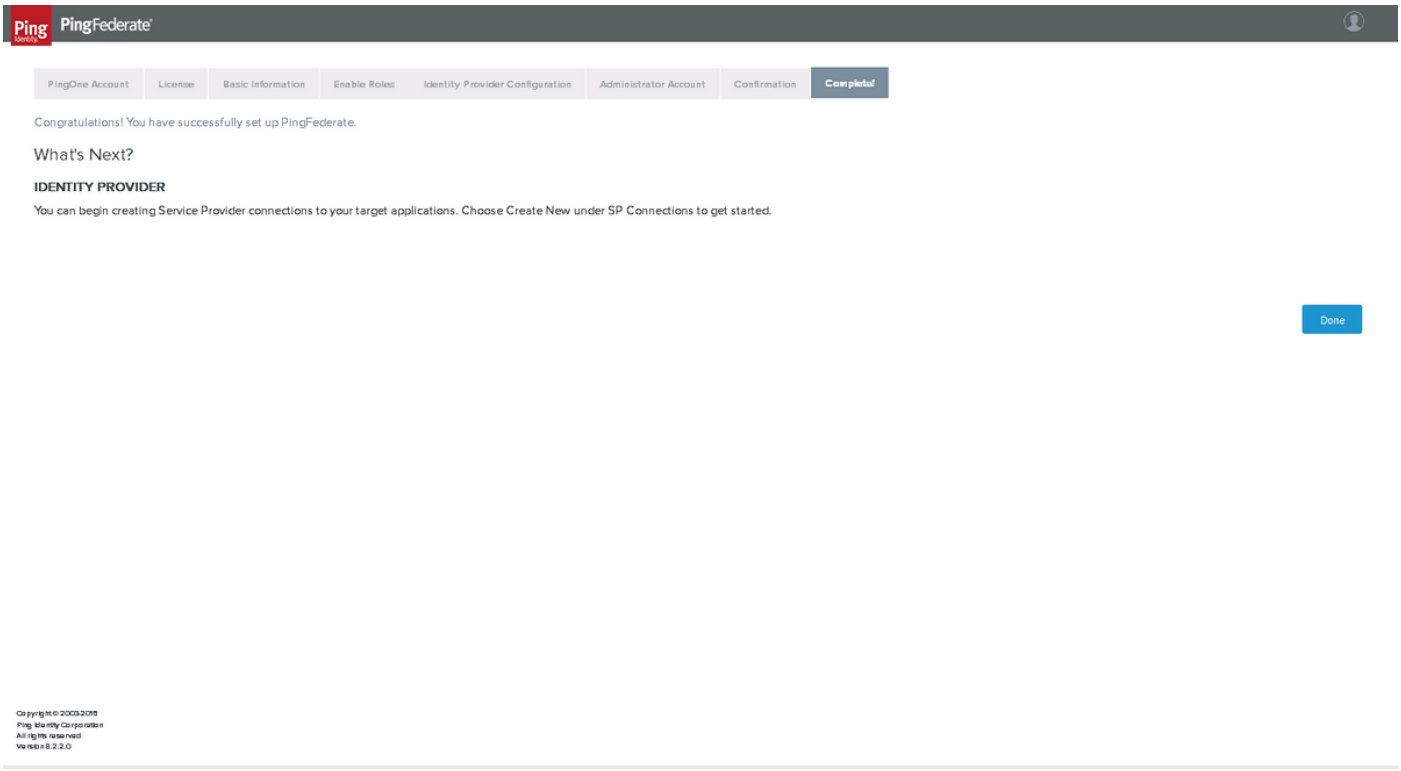
設定管理員的密碼，然後按一下Next（下一步）

確認



確認並按一下下一步

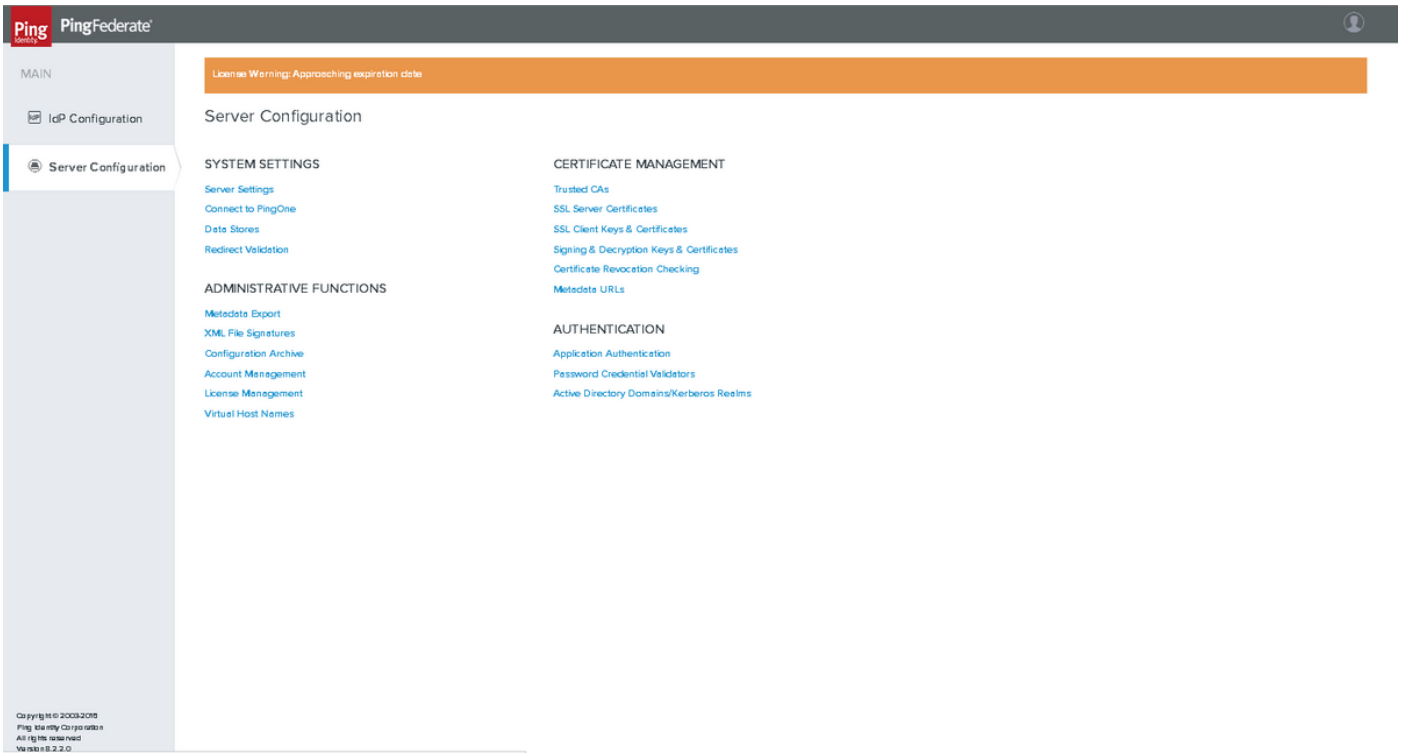
完成



按一下完成

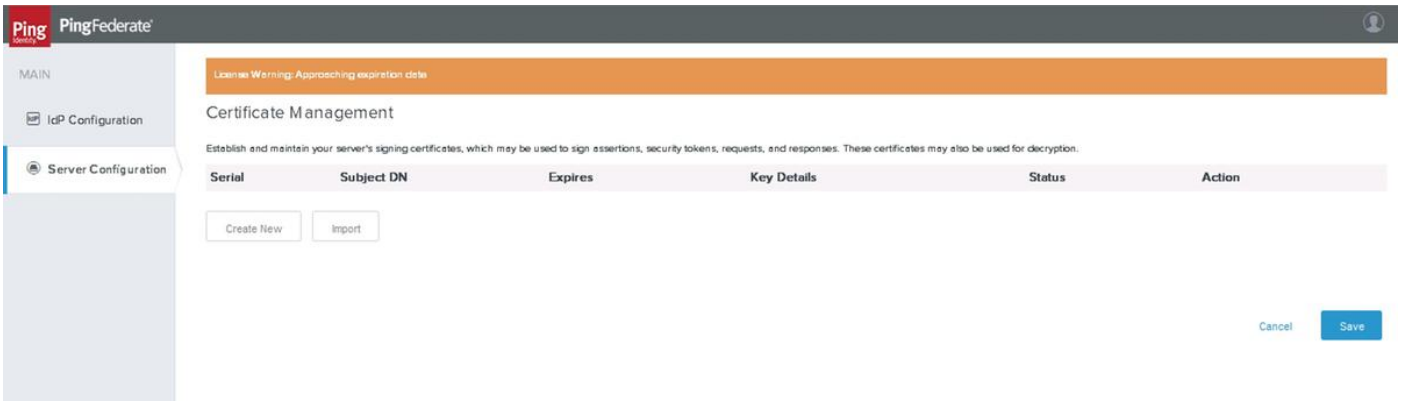
配置PingFederate

伺服器配置



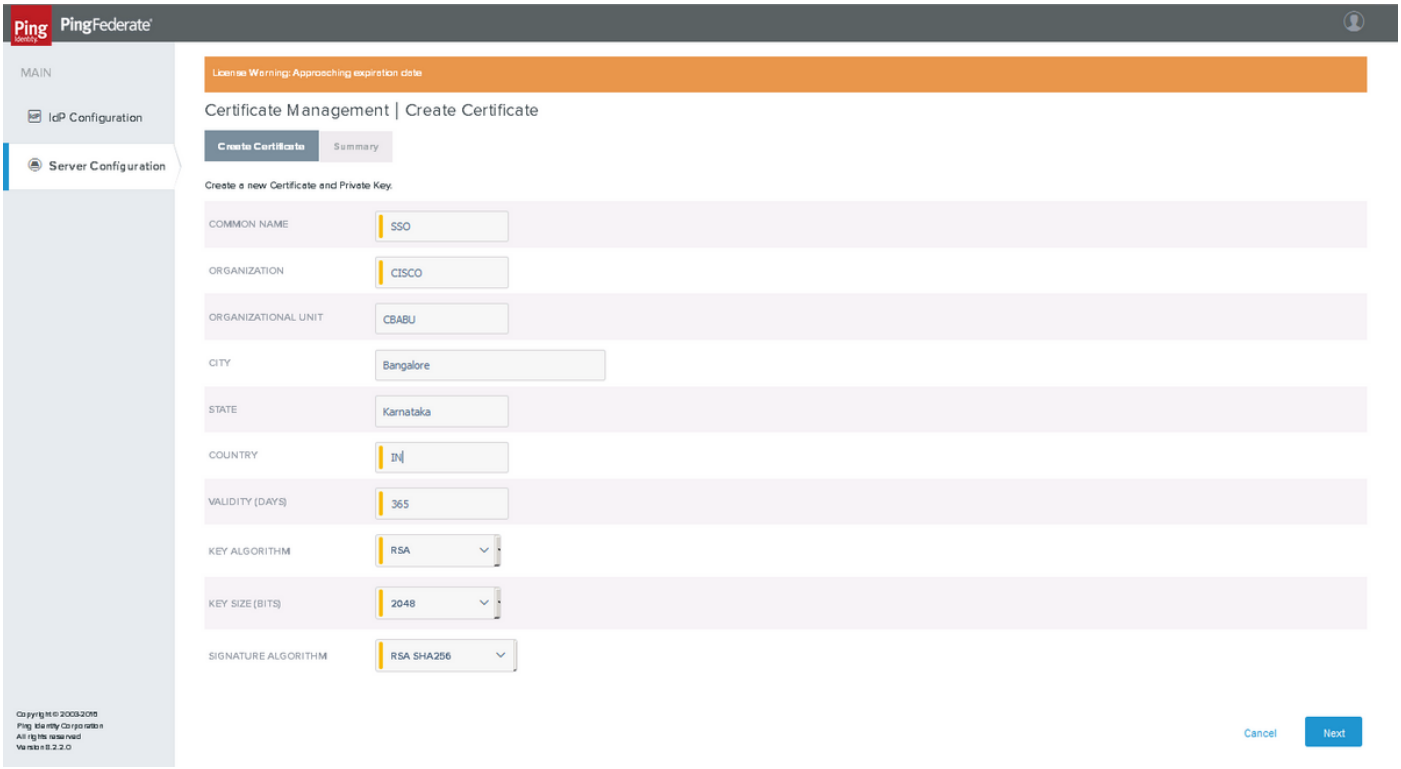
數位簽署和可擴充標籤語言(XML)解密金鑰和憑證

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



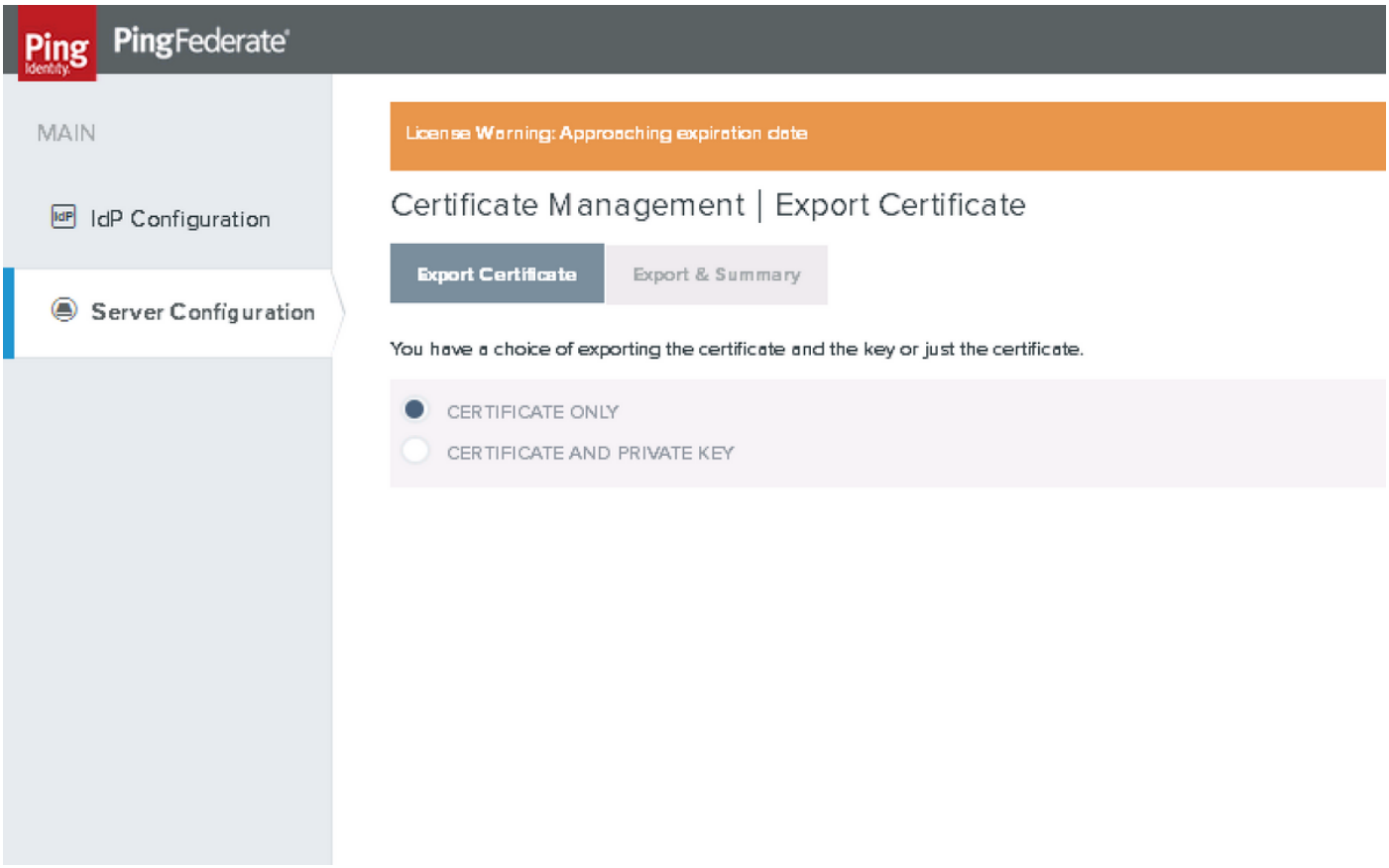
按一下「Create New」

建立證書

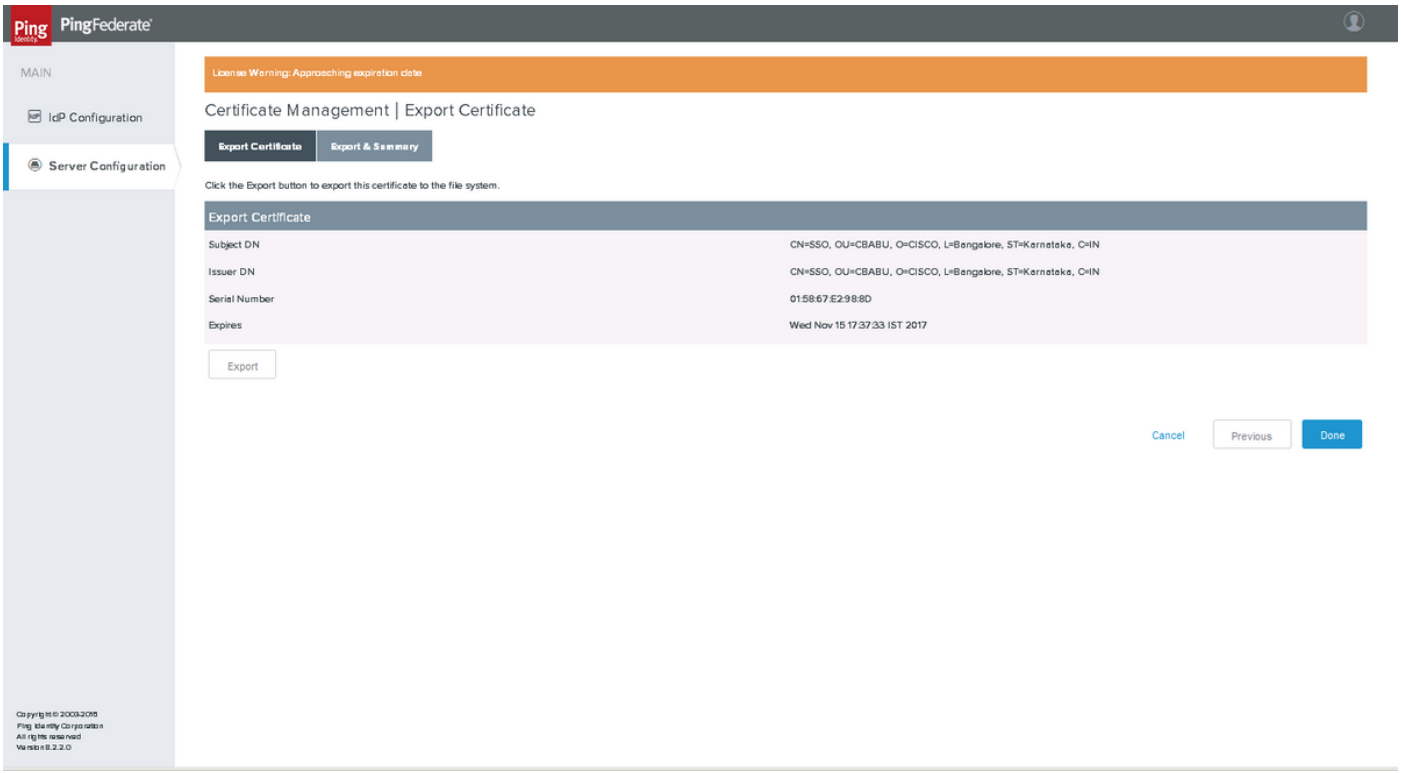


按一下下一步

匯出證書



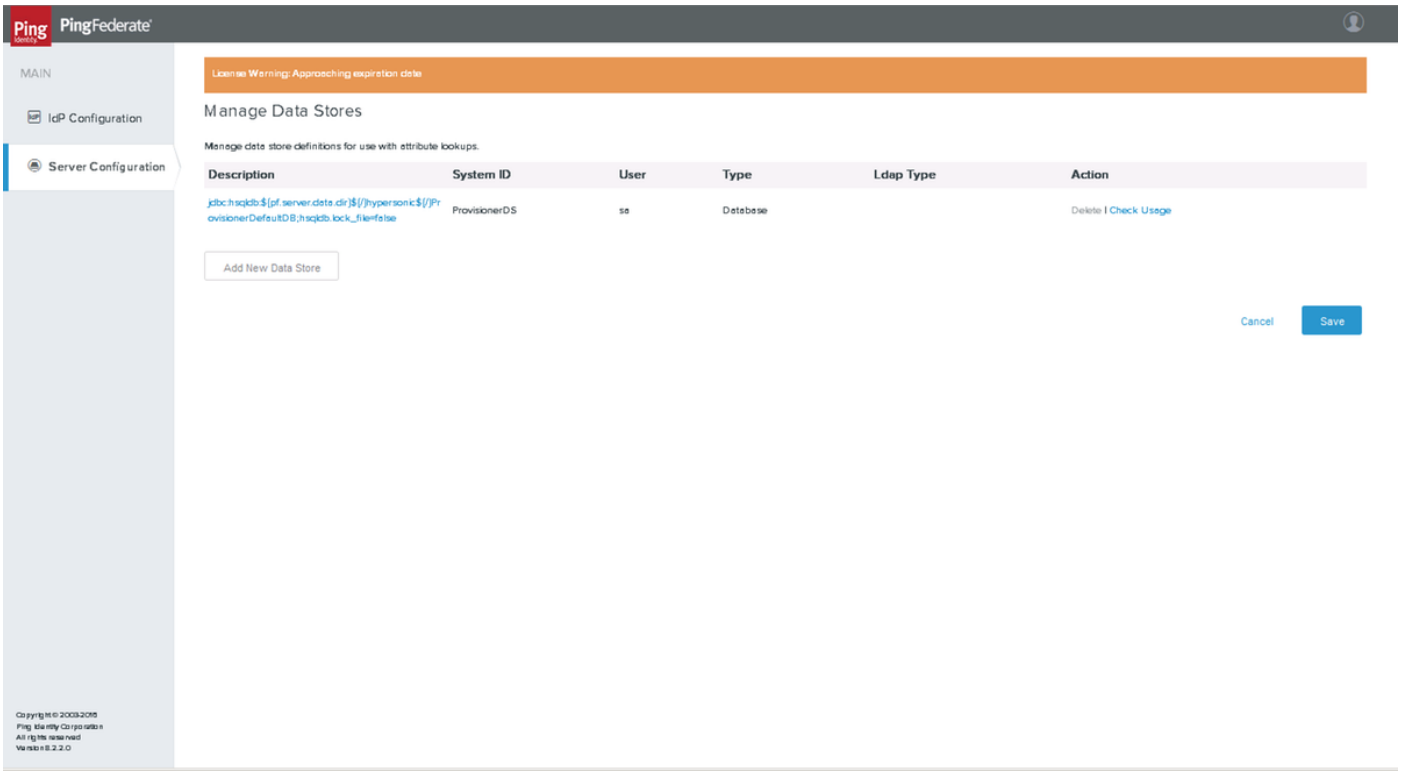
匯出與摘要



按一下「Export」

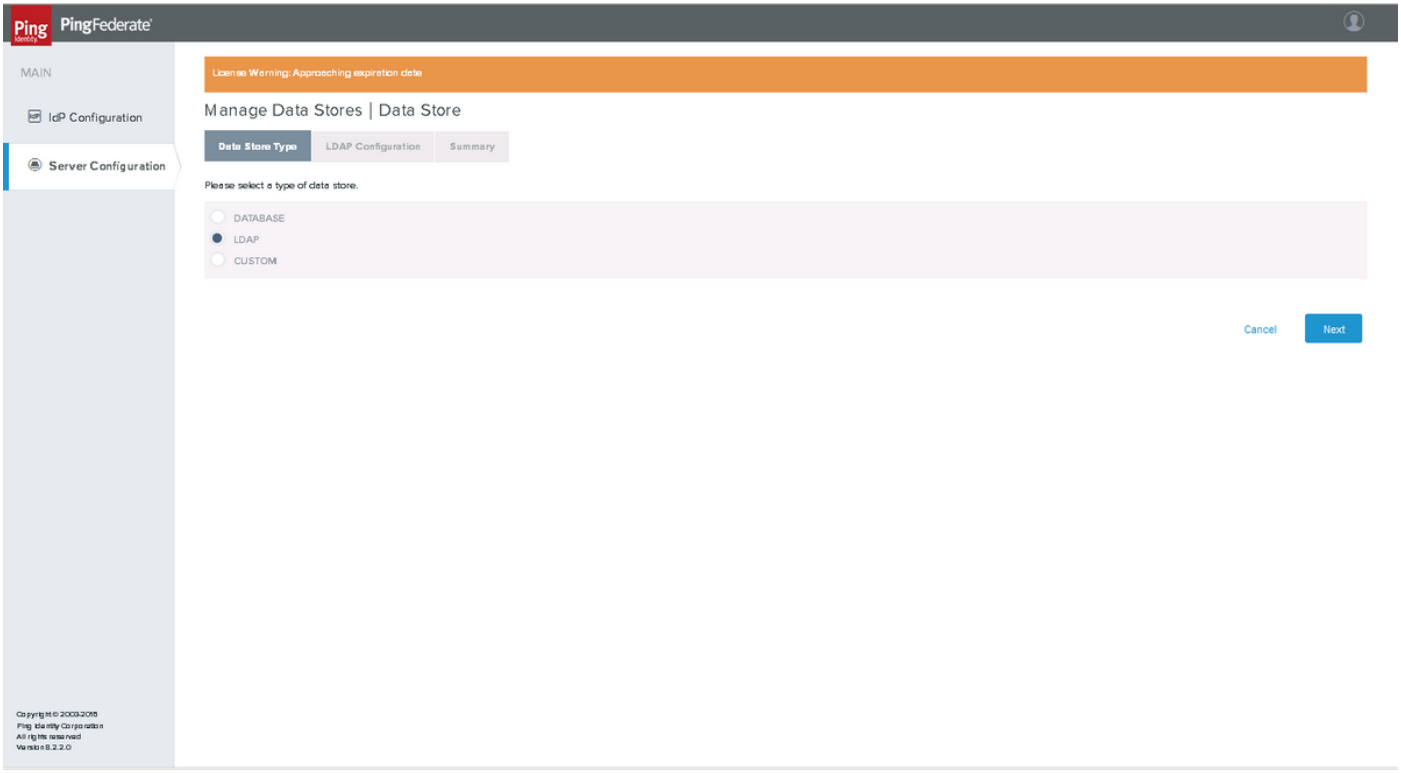
資料儲存

按一下Server Configuration > SYSTEM SETTINGS > Data Stores

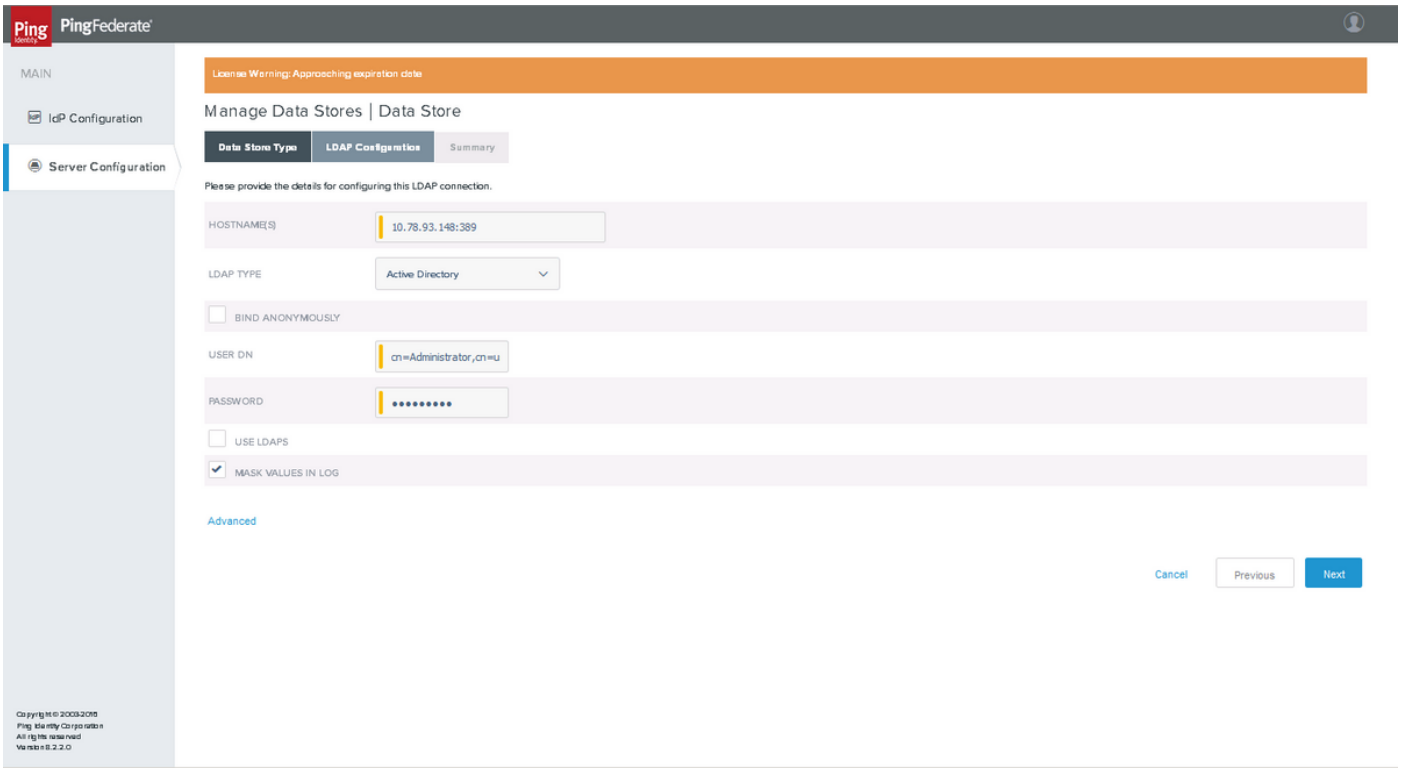


按一下Add New Data Store

LDAP配置

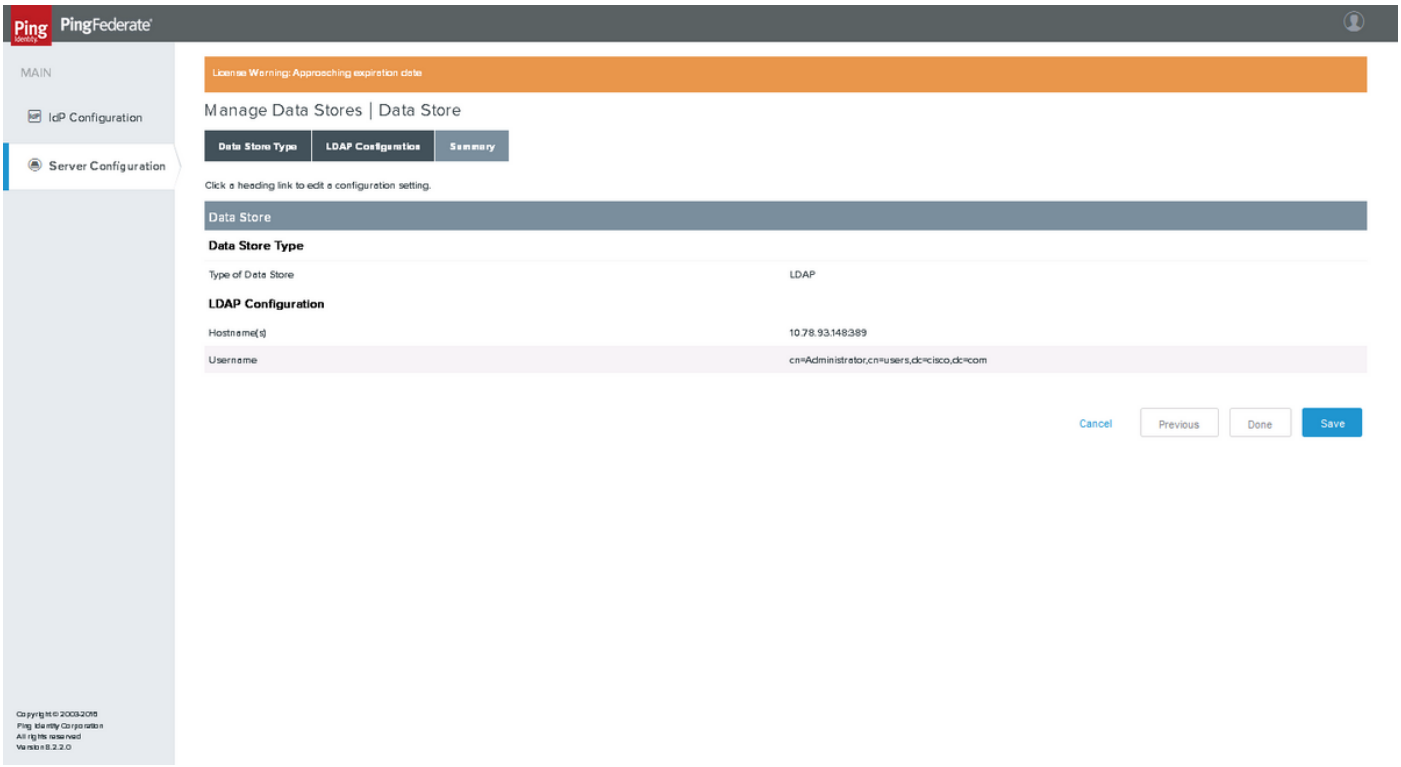


選擇LDAP並按一下Next



輸入值，然後按一下下一步

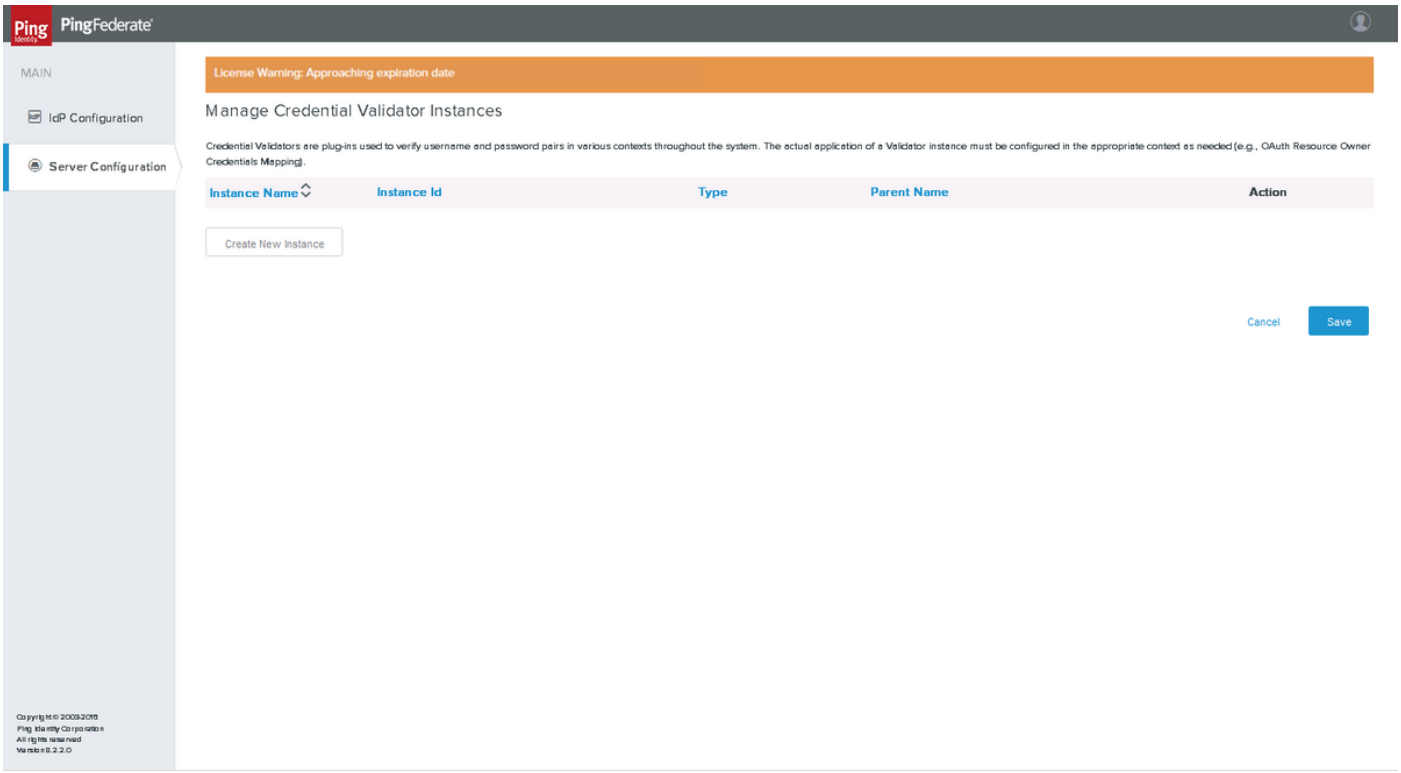
摘要



驗證後按一下「Save」。

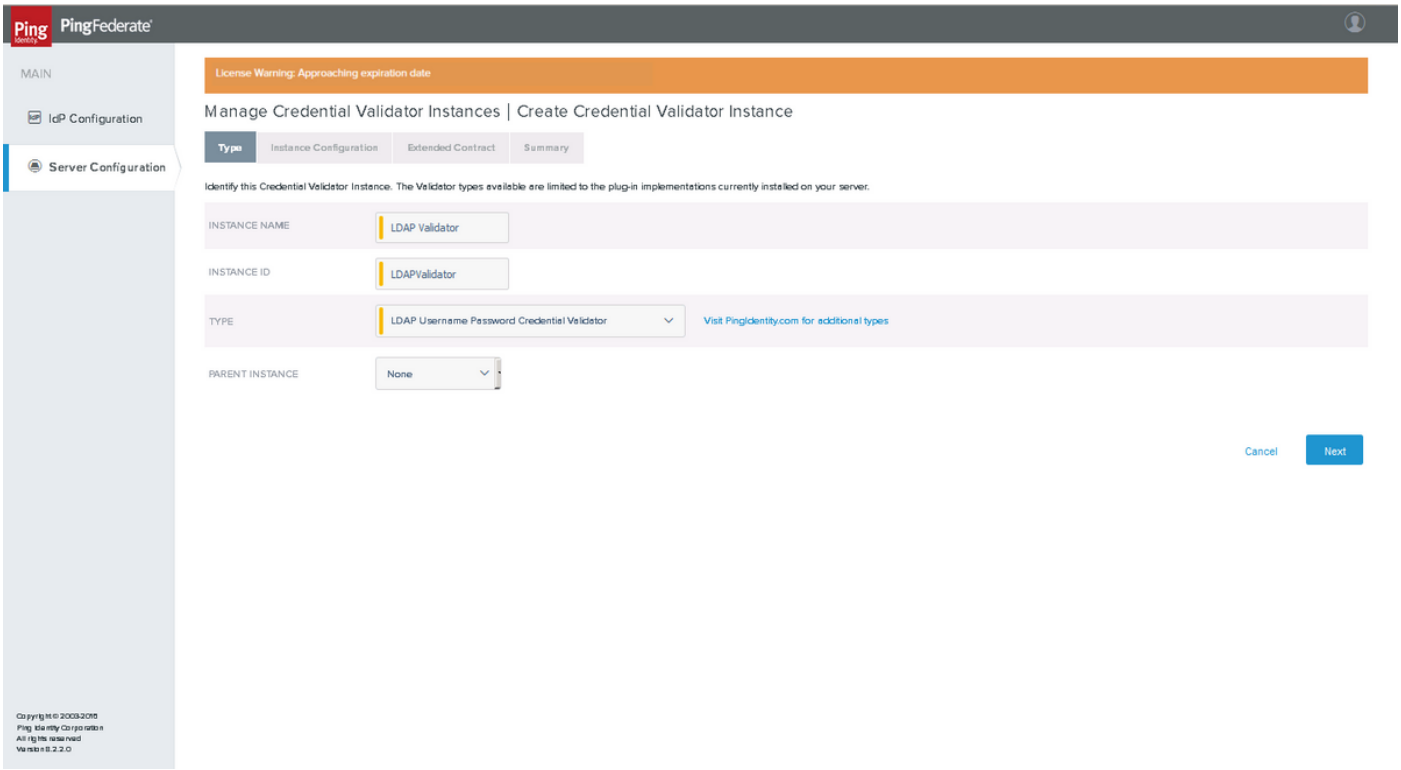
密碼憑據驗證程式

按一下Server Configuration > AUTHENTICATION > Password Credential Validators



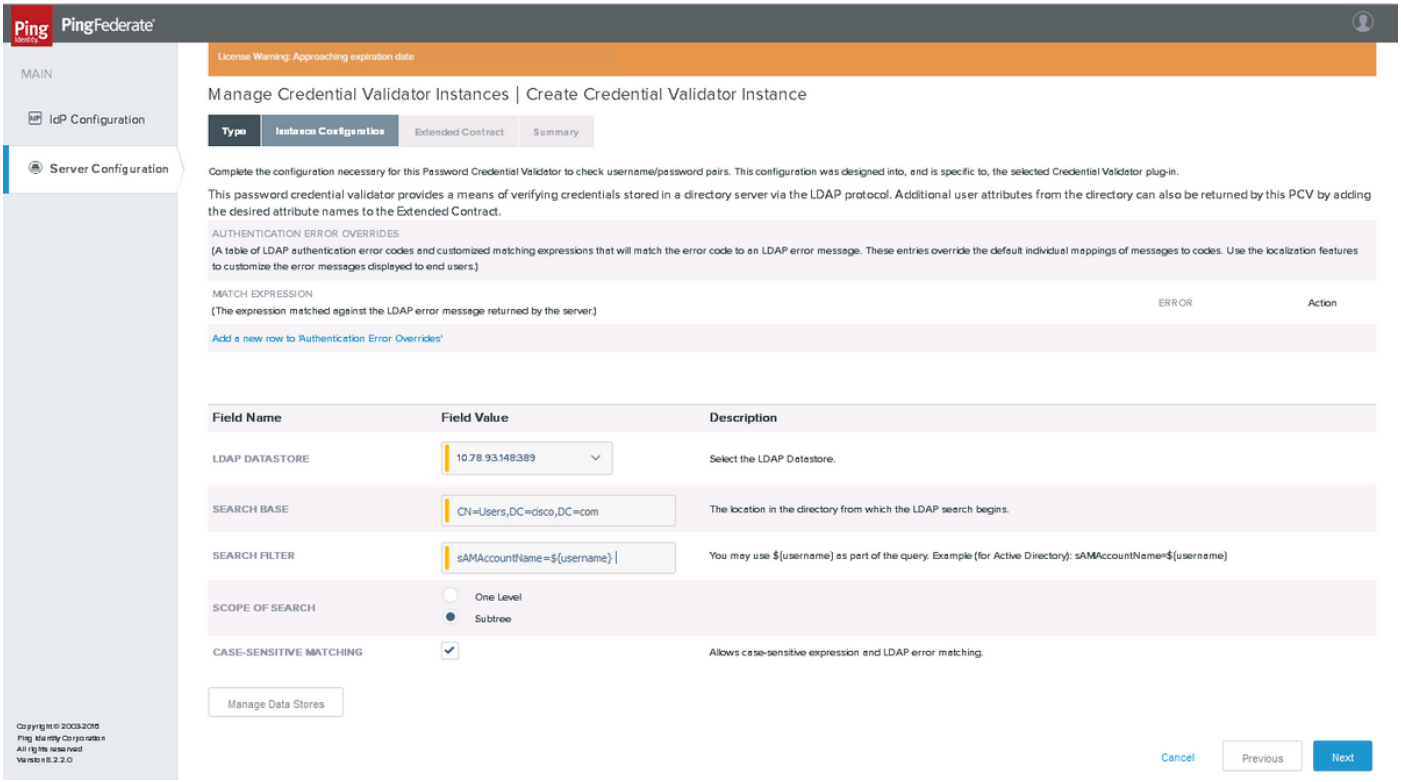
按一下Create New Instance。

類型



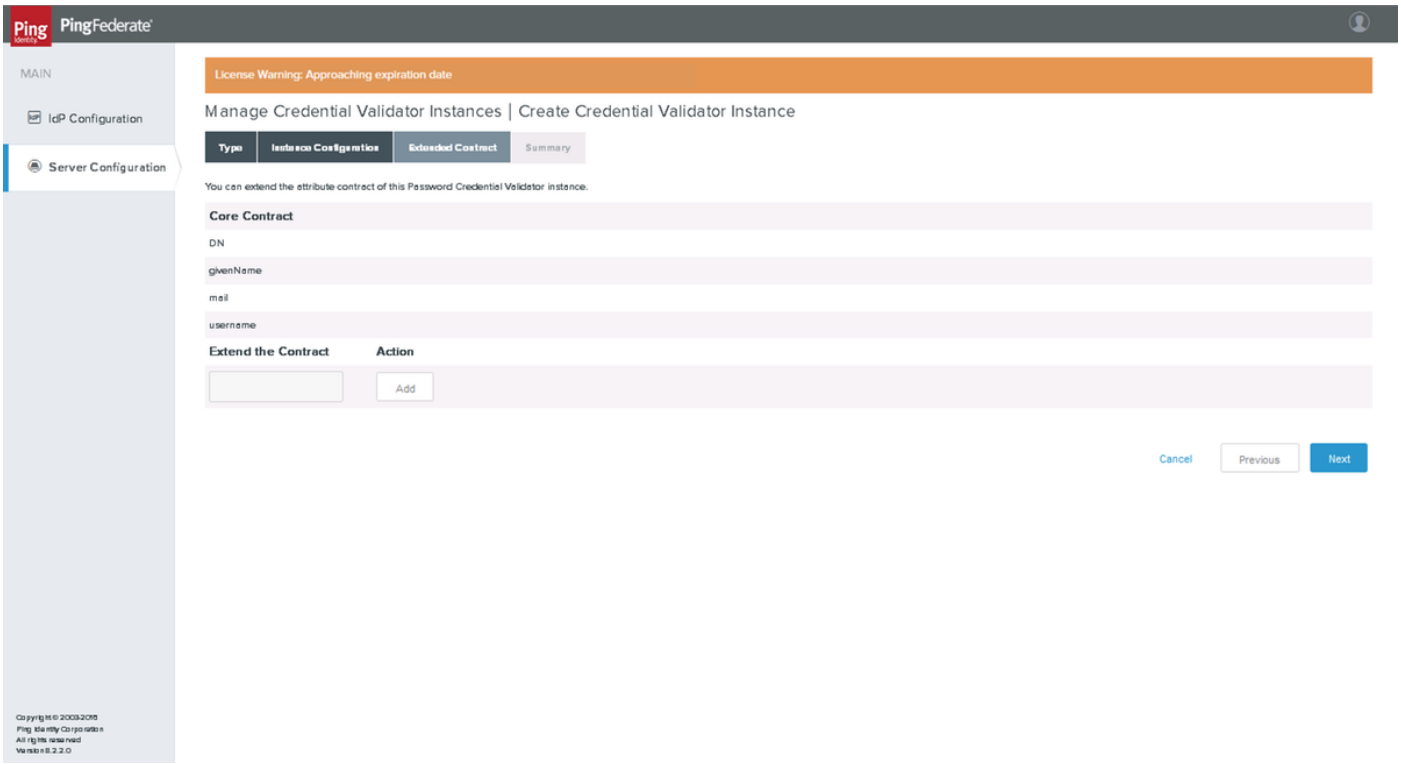
選擇LDAP Username Password Credential Validator作為型別。按「Next」（下一步）。

例項配置



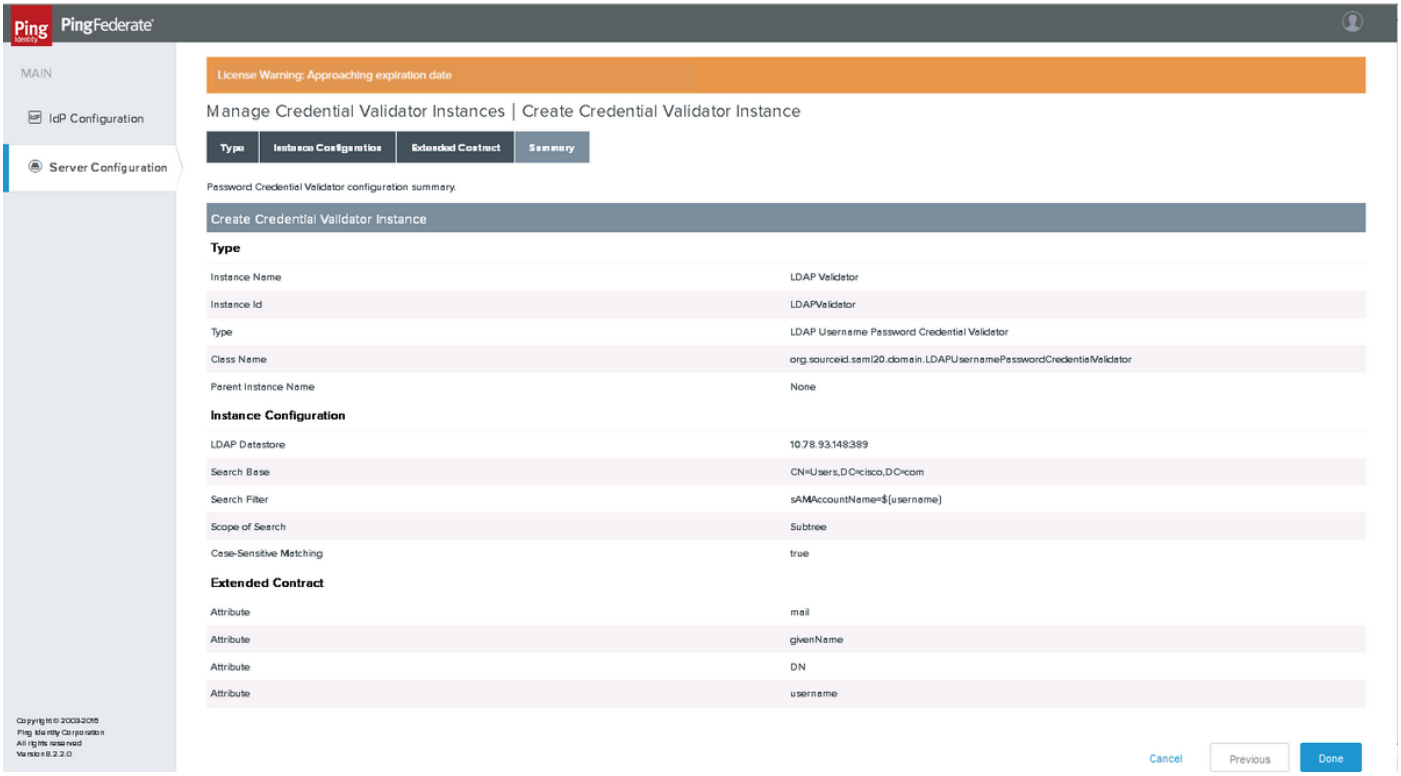
選擇LDAP資料儲存區並輸入搜尋庫、搜尋過濾器和搜尋範圍。按「Next」（下一步）。

延伸合約



按一下下一步

摘要

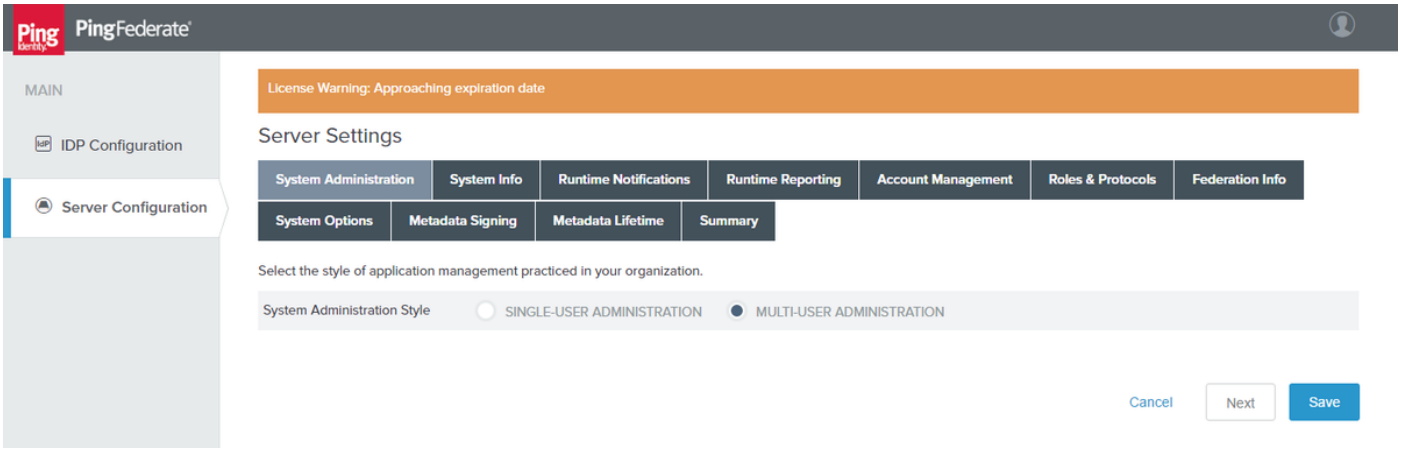


驗證設定並按一下「Done(完成)」。

伺服器設定

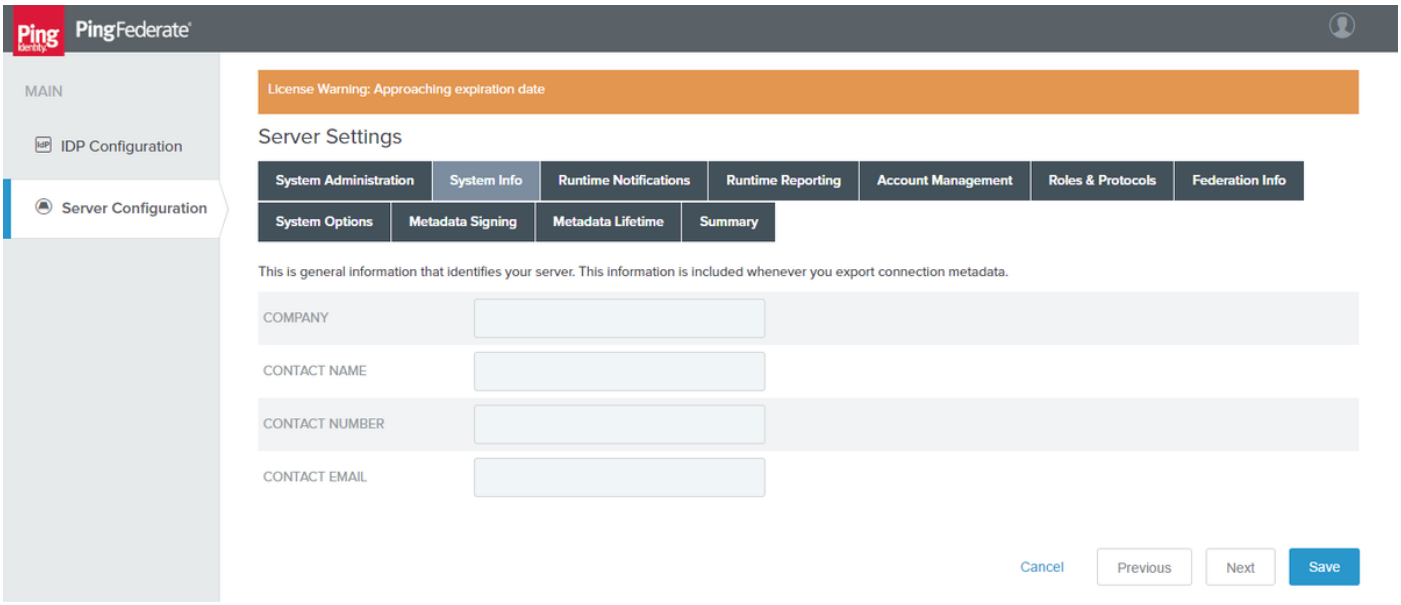
系統管理

按一下Server Configuration>SYSTEM SETTINGS>Server Settings



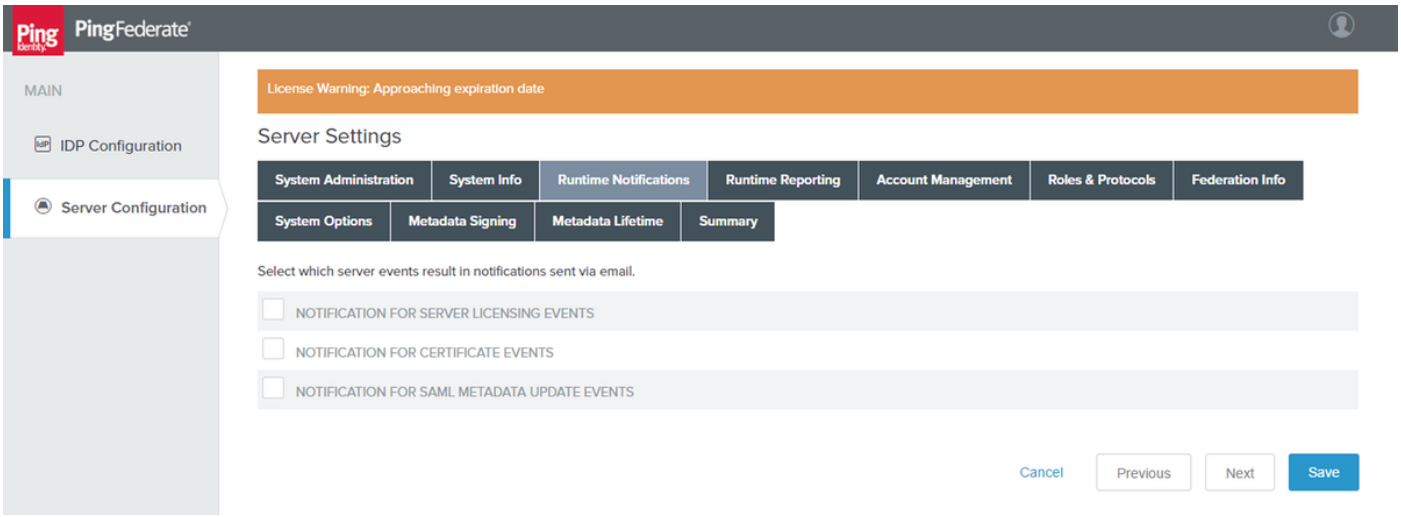
按「Next」（下一步）。

系統資訊



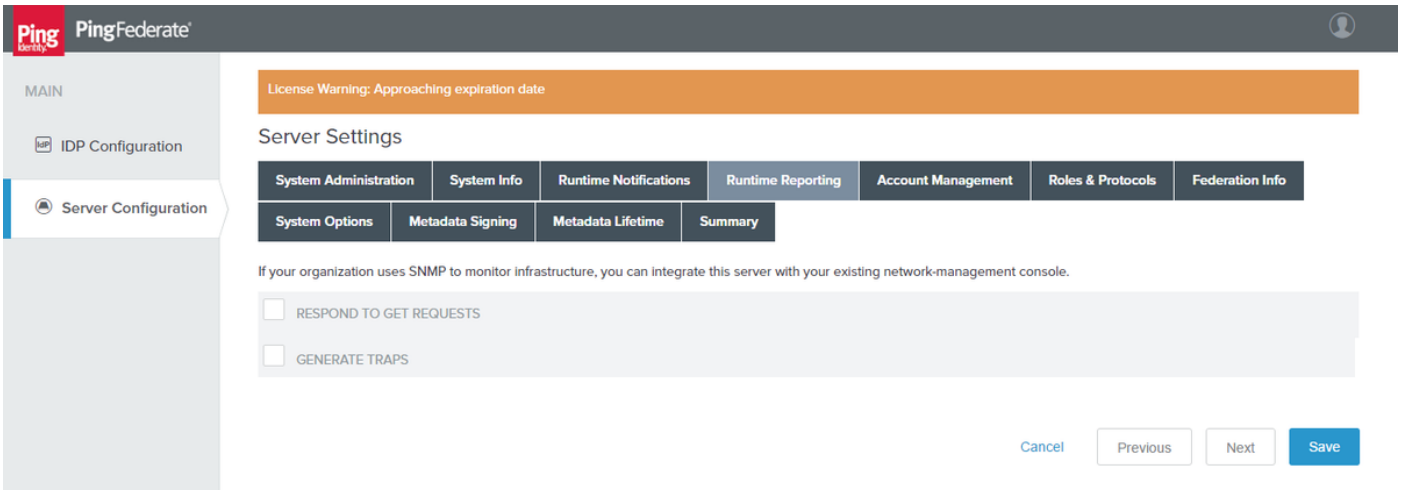
按「Next」（下一步）。

運行時通知



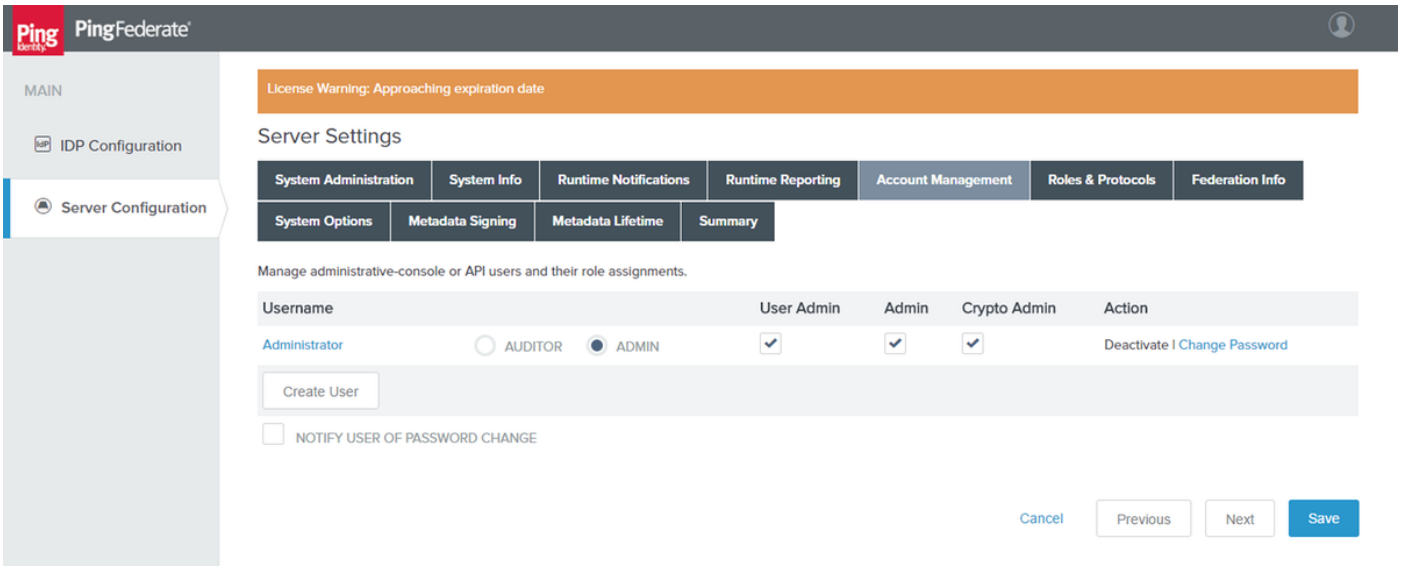
按「Next」（下一步）。

運行時報告



按「Next」（下一步）。

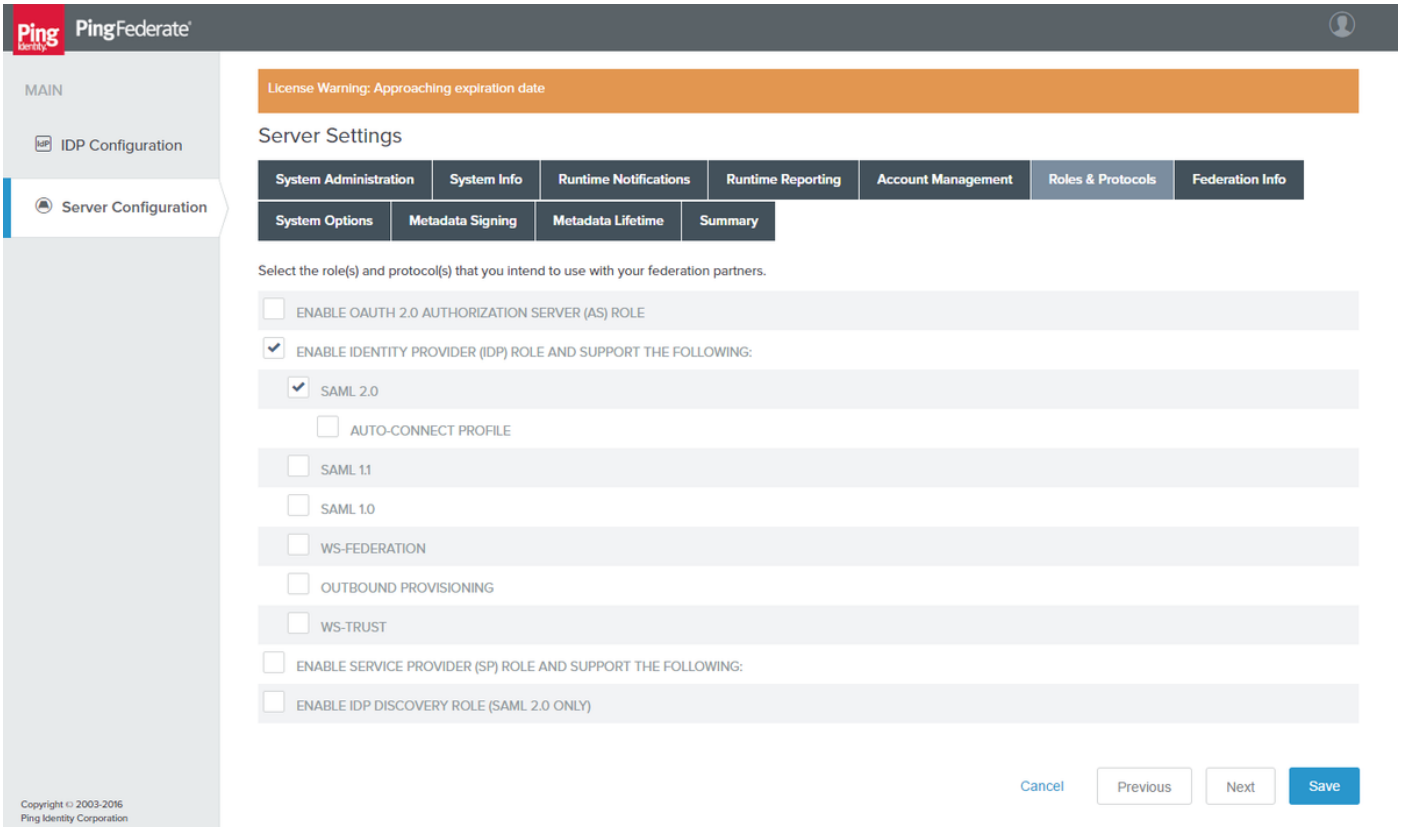
帳戶管理



按「Next」（下一步）。

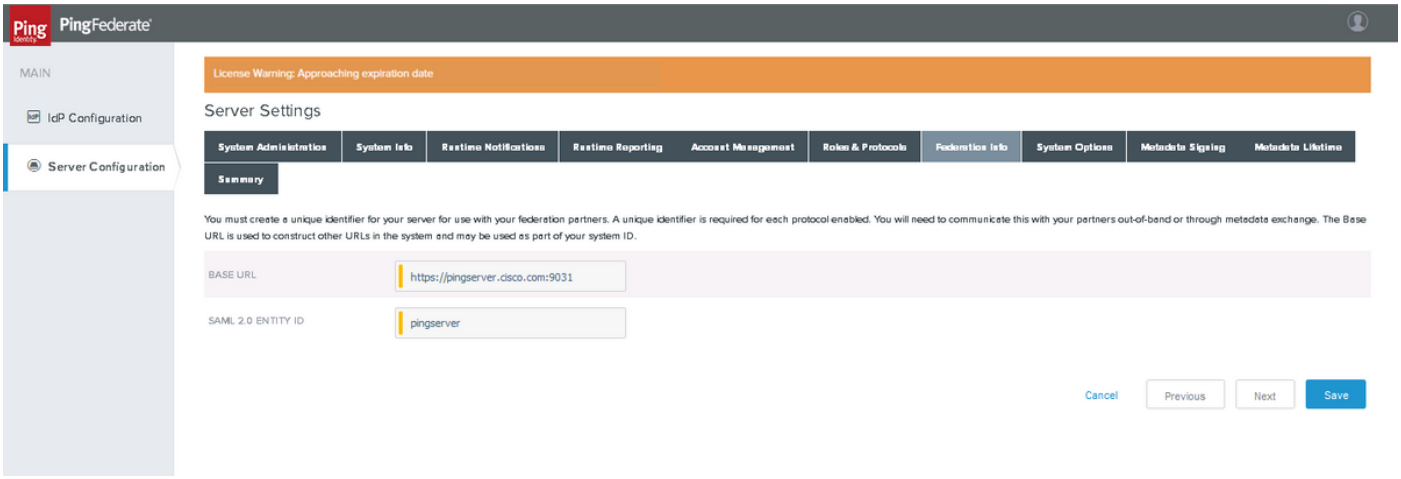
注意：您可以在此部分中新增使用者或更改使用者的密碼。

角色和協定



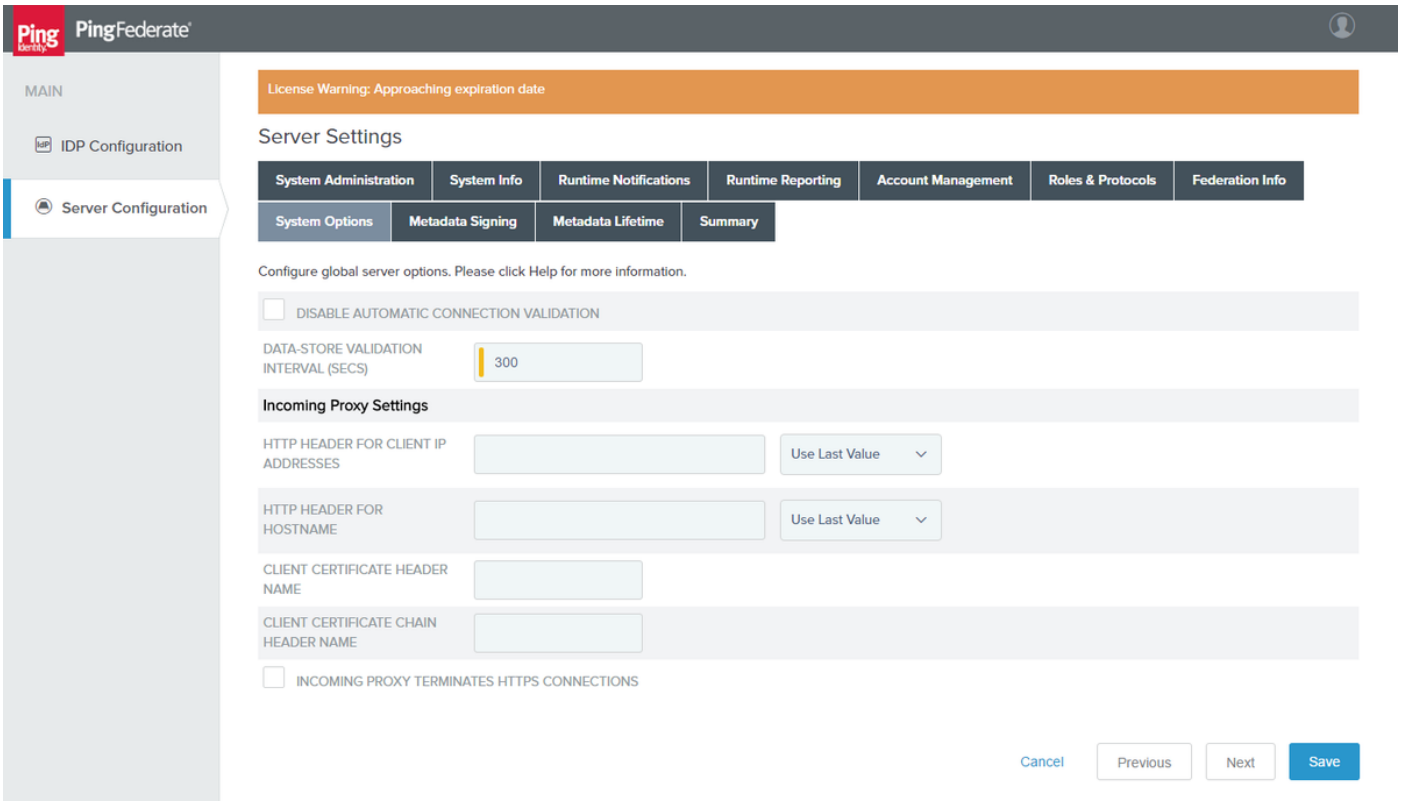
選擇適當的角色和協定。按「Next」（下一步）。

聯合資訊



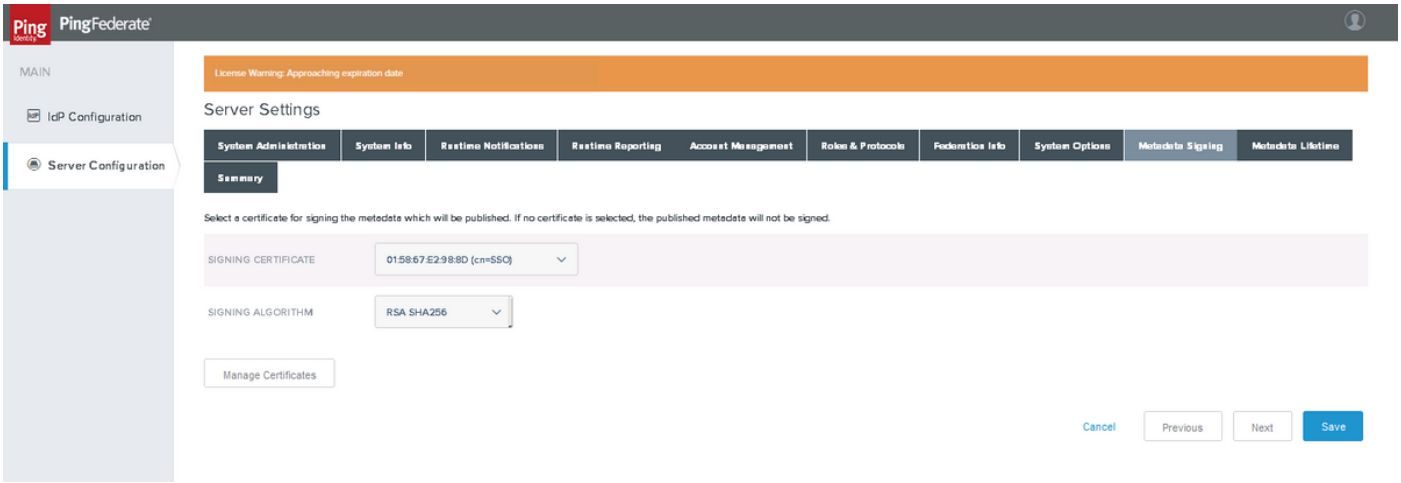
按「Next」（下一步）。

系統選項



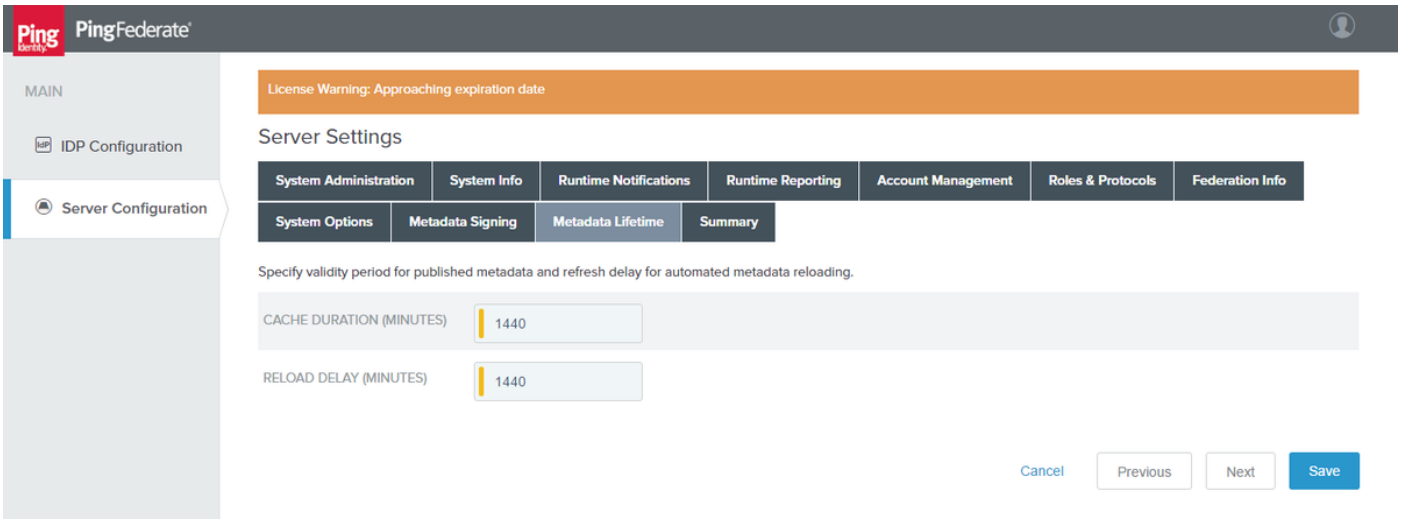
按「Next」（下一步）。

後設資料簽名



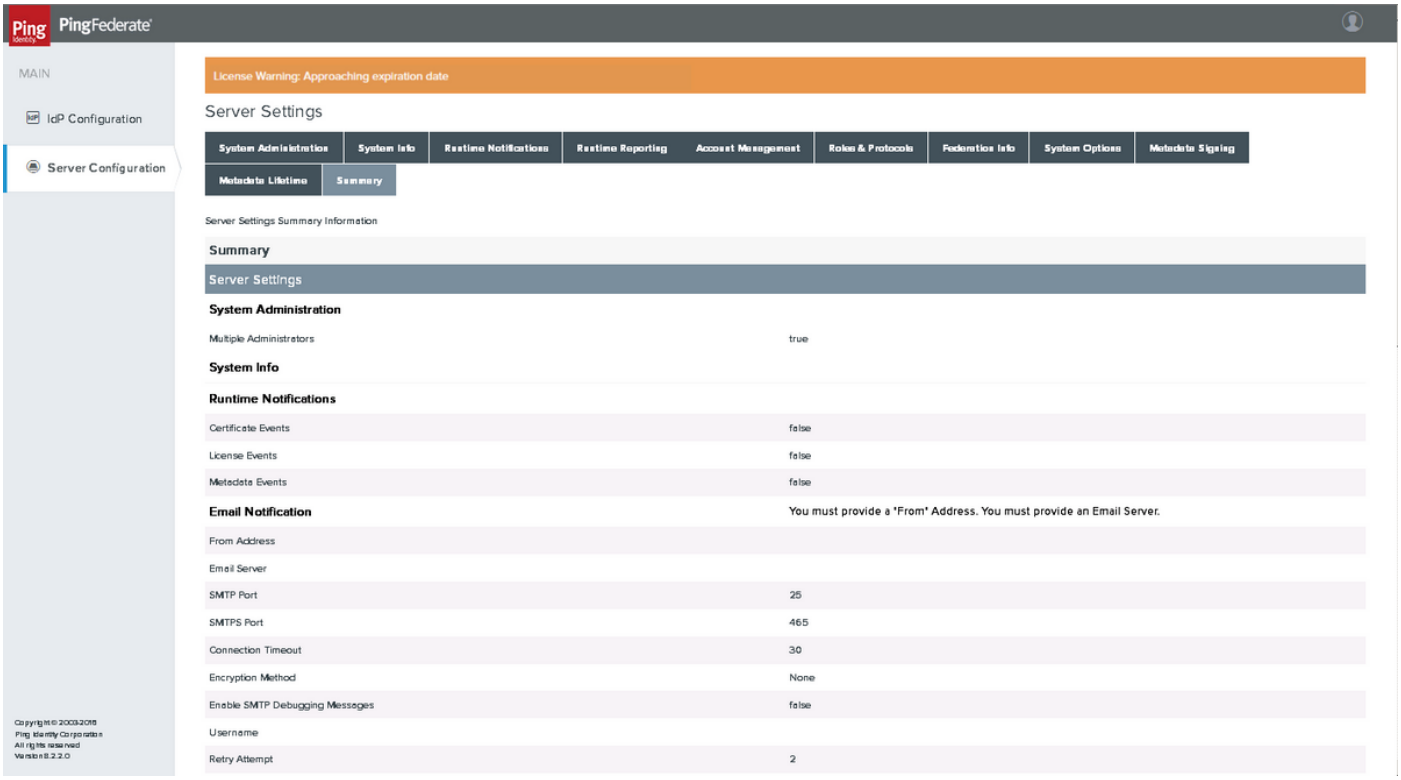
選擇之前建立的簽名證書和簽名演算法作為證書配置的一部分。按「Next」（下一步）。

後設資料生存期



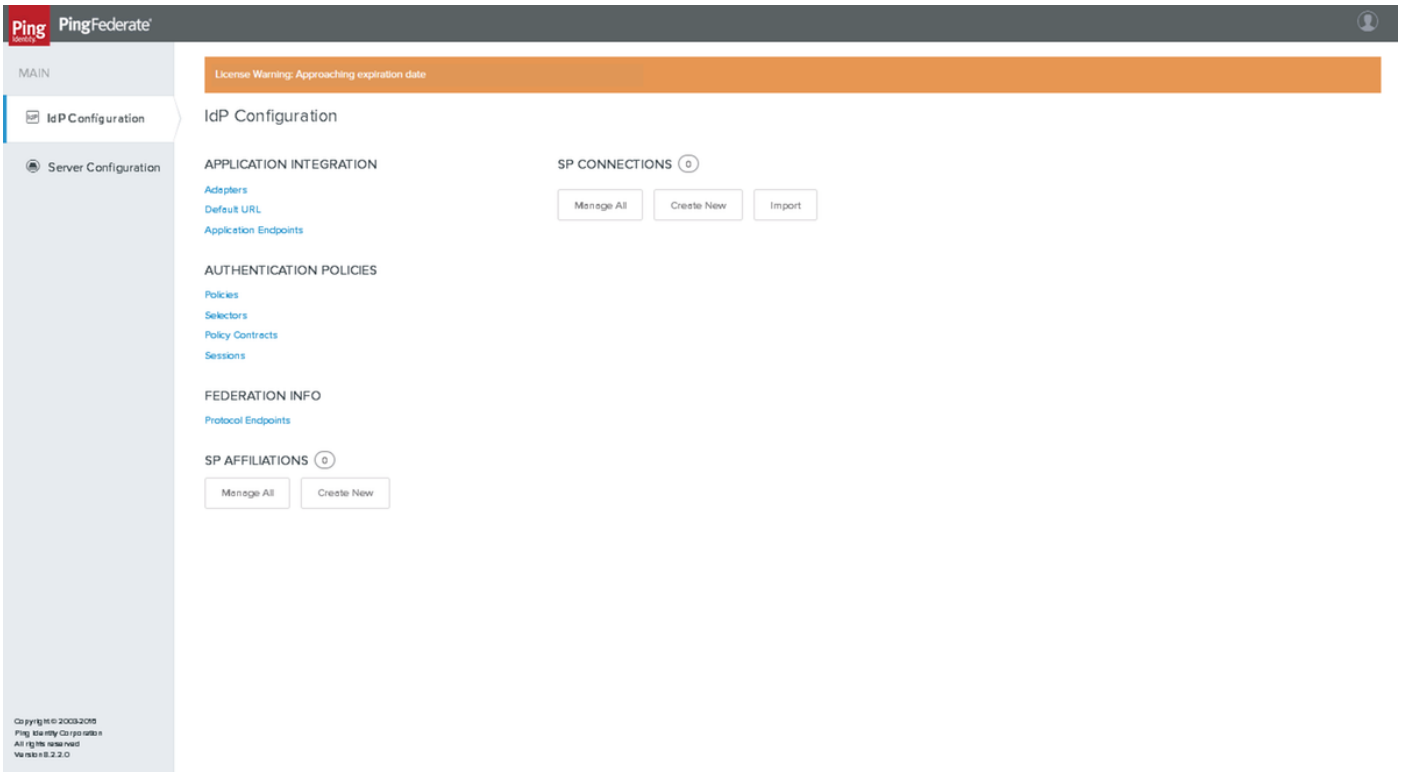
按「Next」（下一步）。

摘要



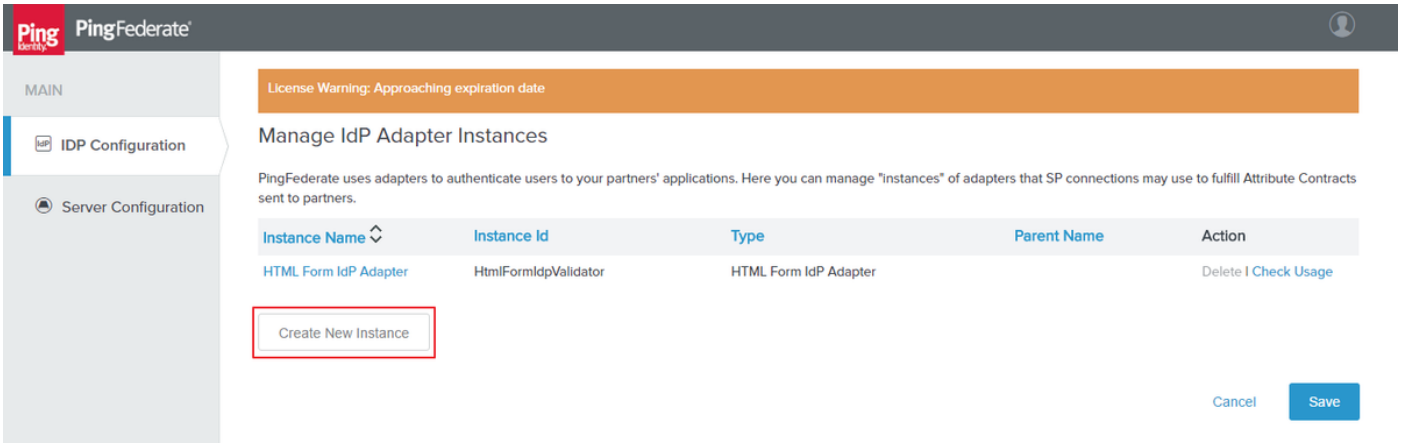
驗證設定並按一下Save。

身份提供程式(IdP)配置



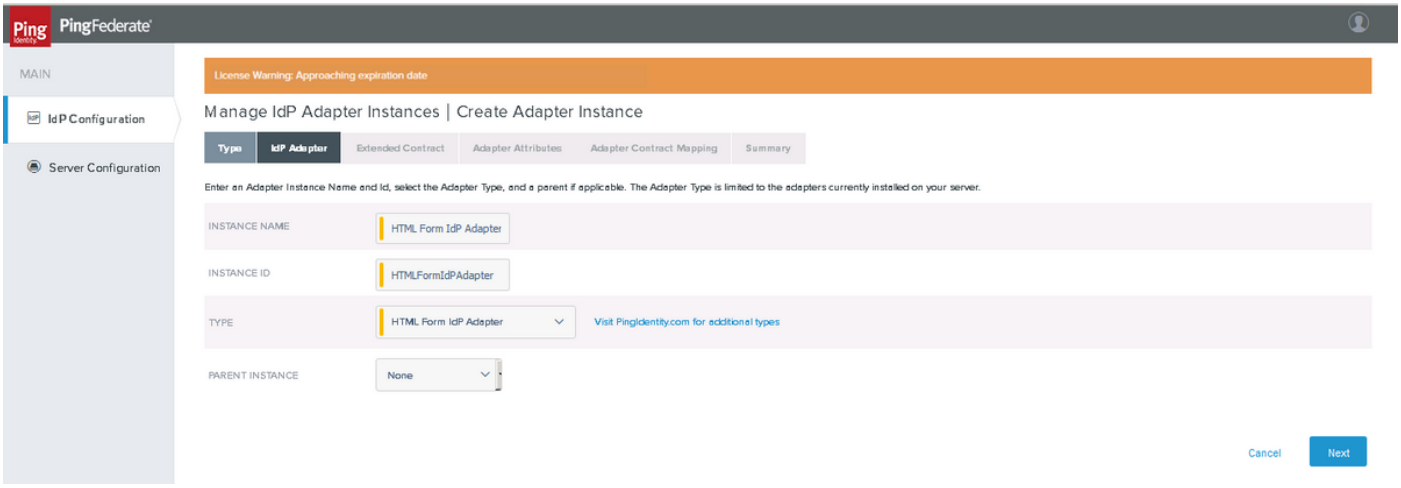
介面卡

按一下IdP Configuration > APPLICATION INTEGRATION > Adapters



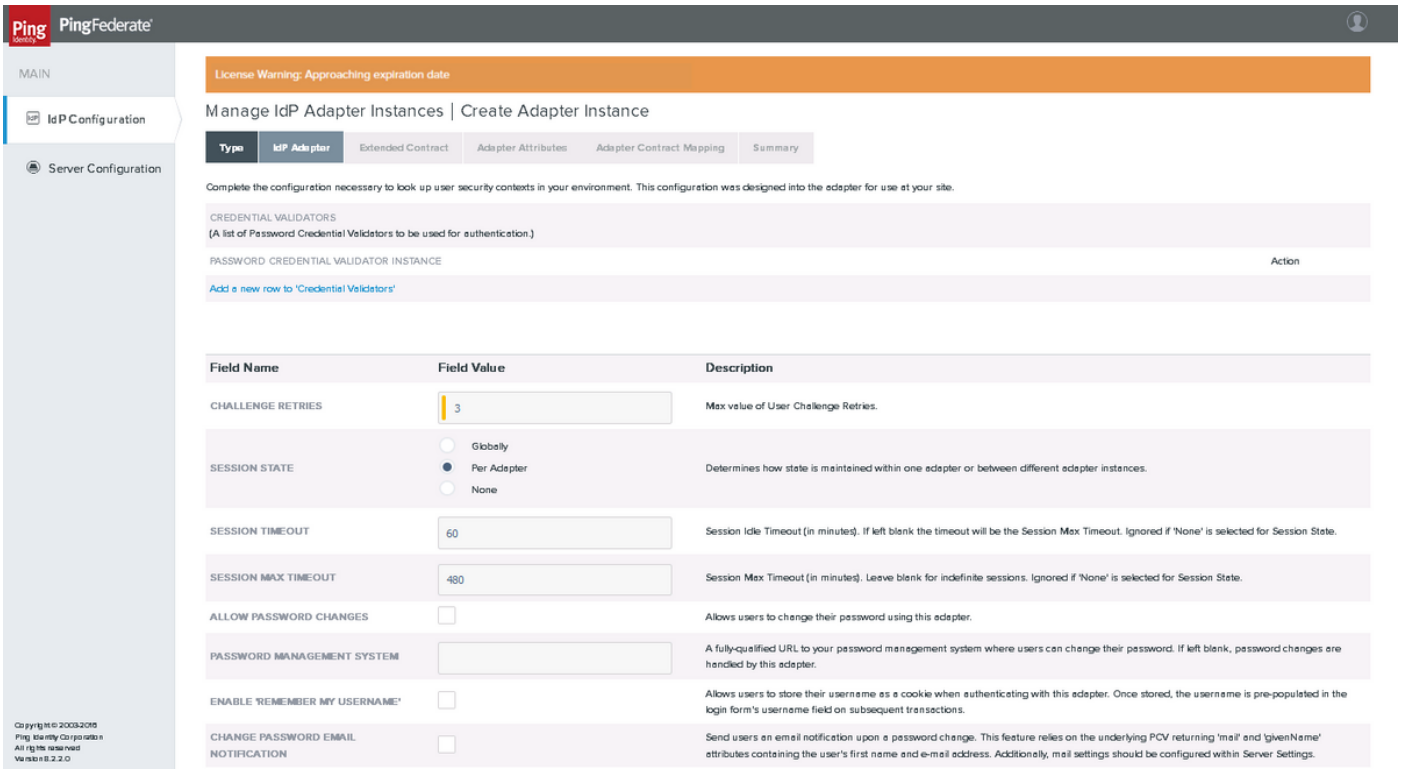
按一下Create New Instance。

類型



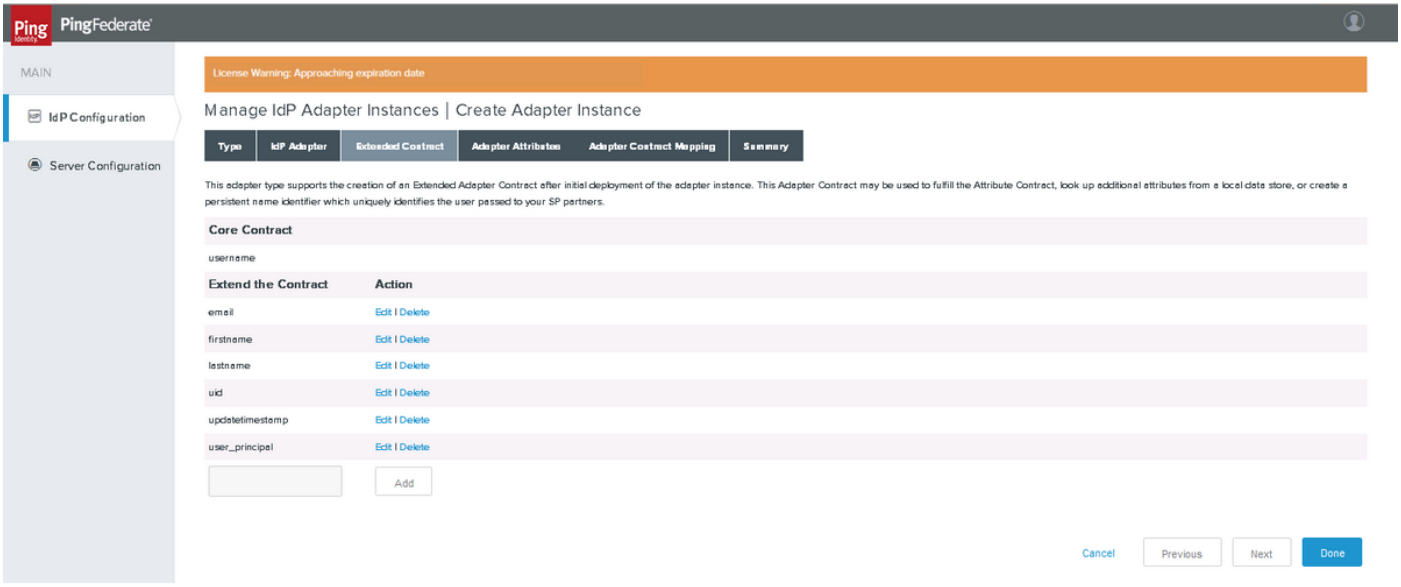
選擇HTML表單IDP介面卡。按「Next」（下一步）。

IdP介面卡



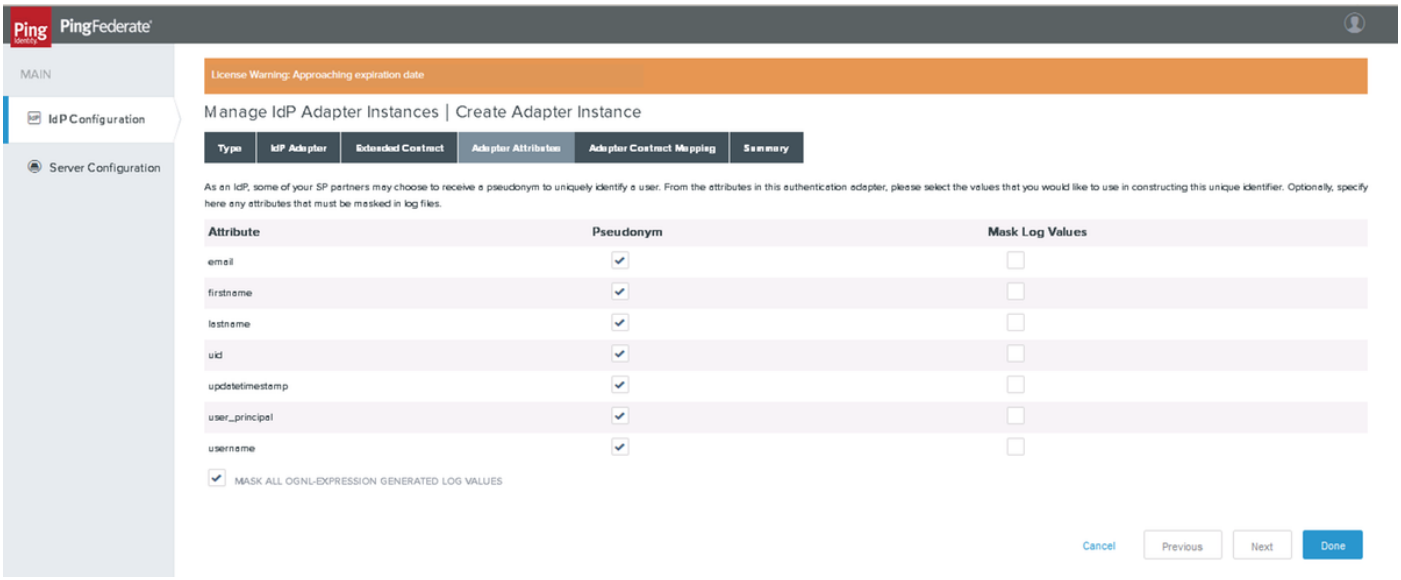
按一下Add a new row to 'Credential Validators'（向「憑據驗證程式」新增新行），然後選擇先前作為PASSWORD CREDENTIAL VALIDATOR INSTANCE建立的LDAP驗證程式，然後按一下Update（更新）。按一下Next（下一步）。

延伸合約



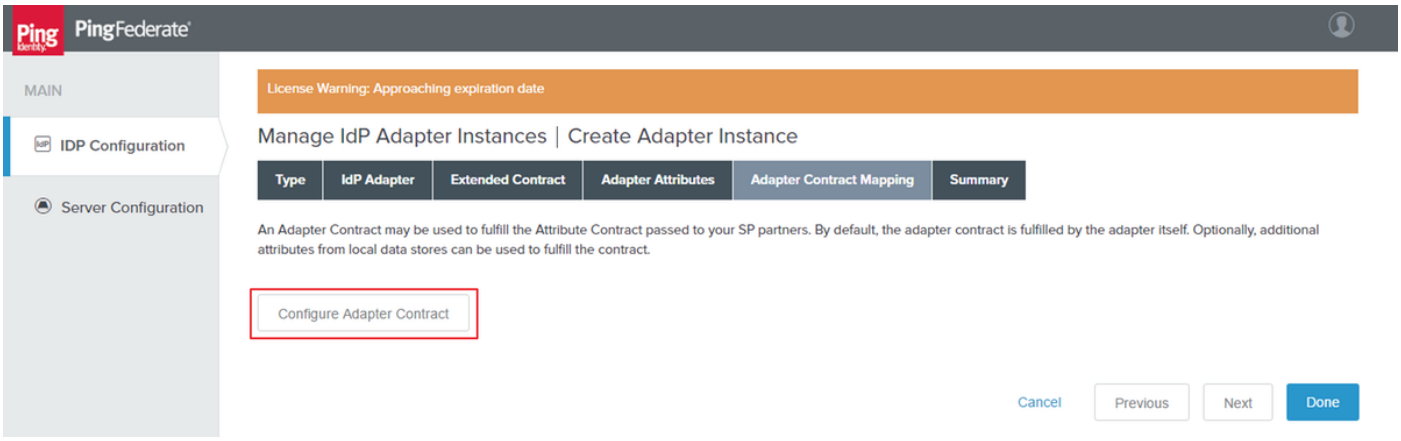
新增合約，如圖所示。按「Next」（下一步）。

介面卡屬性



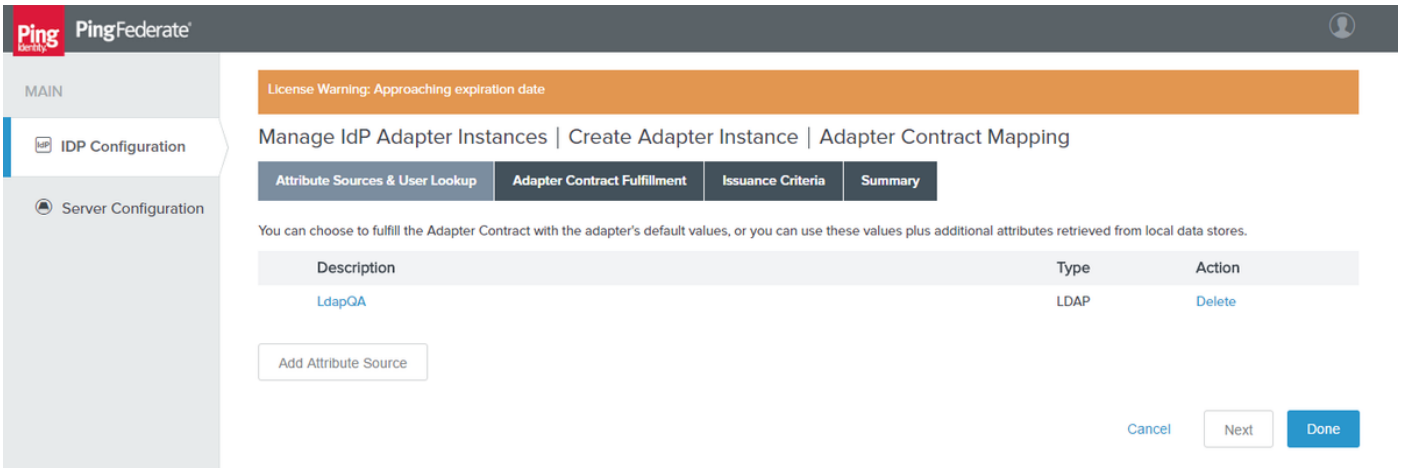
按「Next」（下一步）。

介面卡合約對映



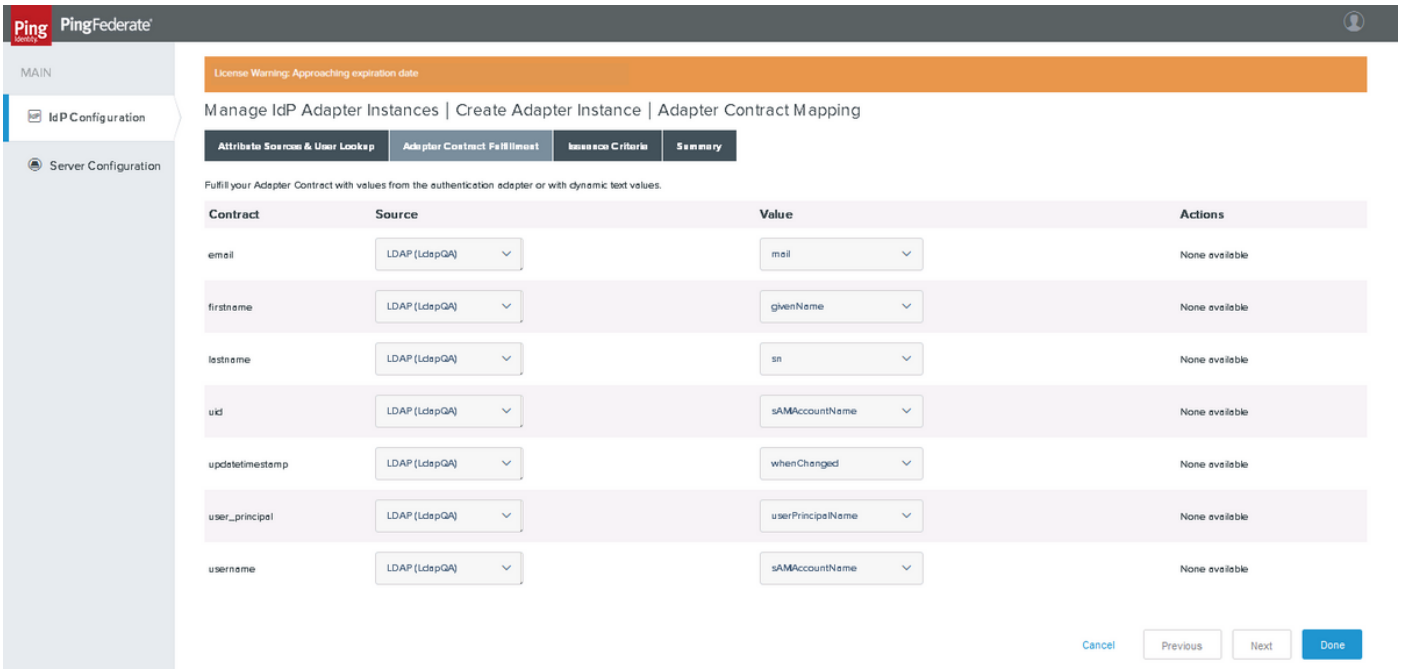
按一下「Configure Adapter Contract」。

屬性源和使用者查詢



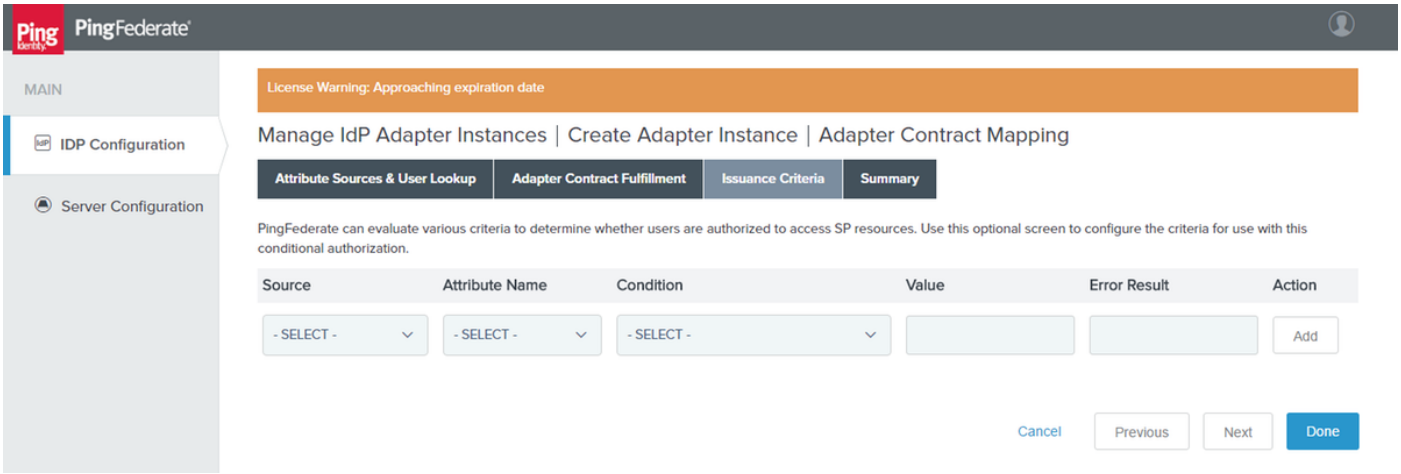
新增屬性源並選擇之前建立的LDAP儲存。按「Next」（下一步）。

介面卡合約履行



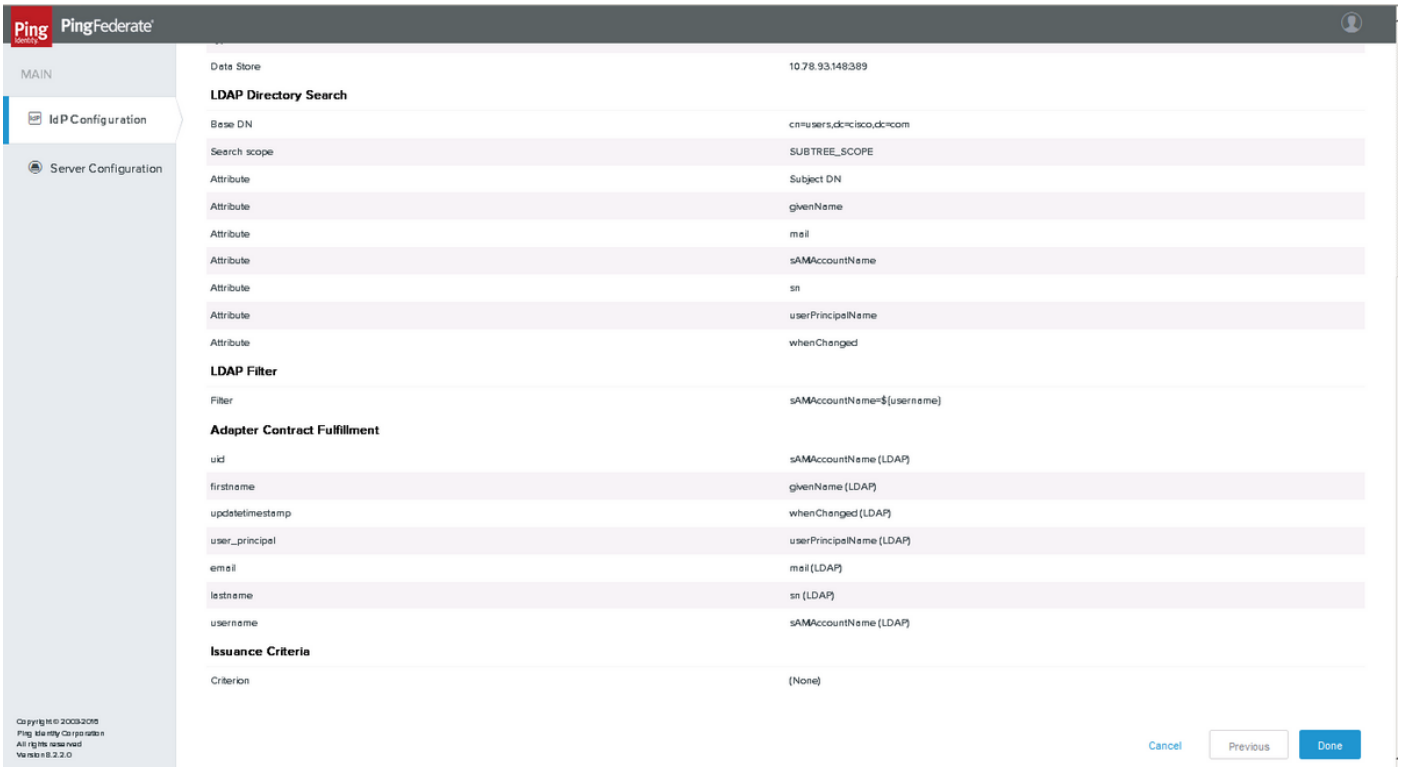
對映屬性。按「Next」（下一步）。

發佈標準



按「Next」（下一步）。

摘要

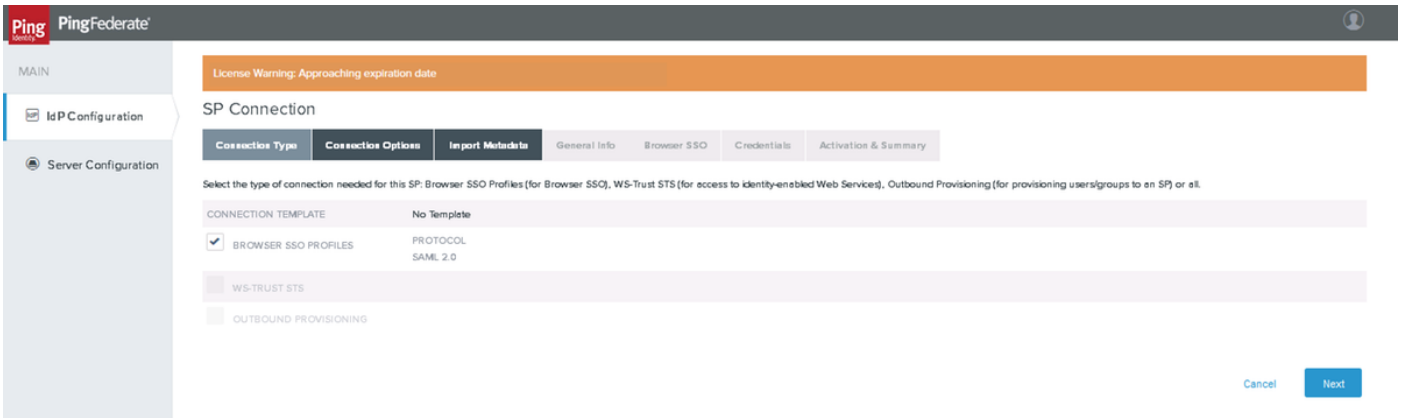


驗證設定並按一下「Done(完成)」。

SP連線

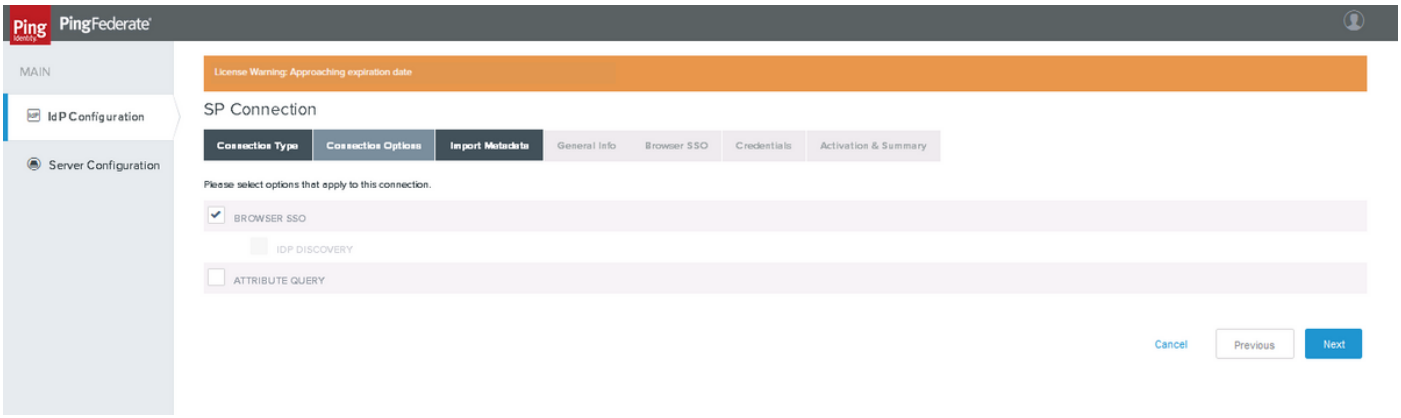
建立新的SP連線

連線型別



按「Next」（下一步）。

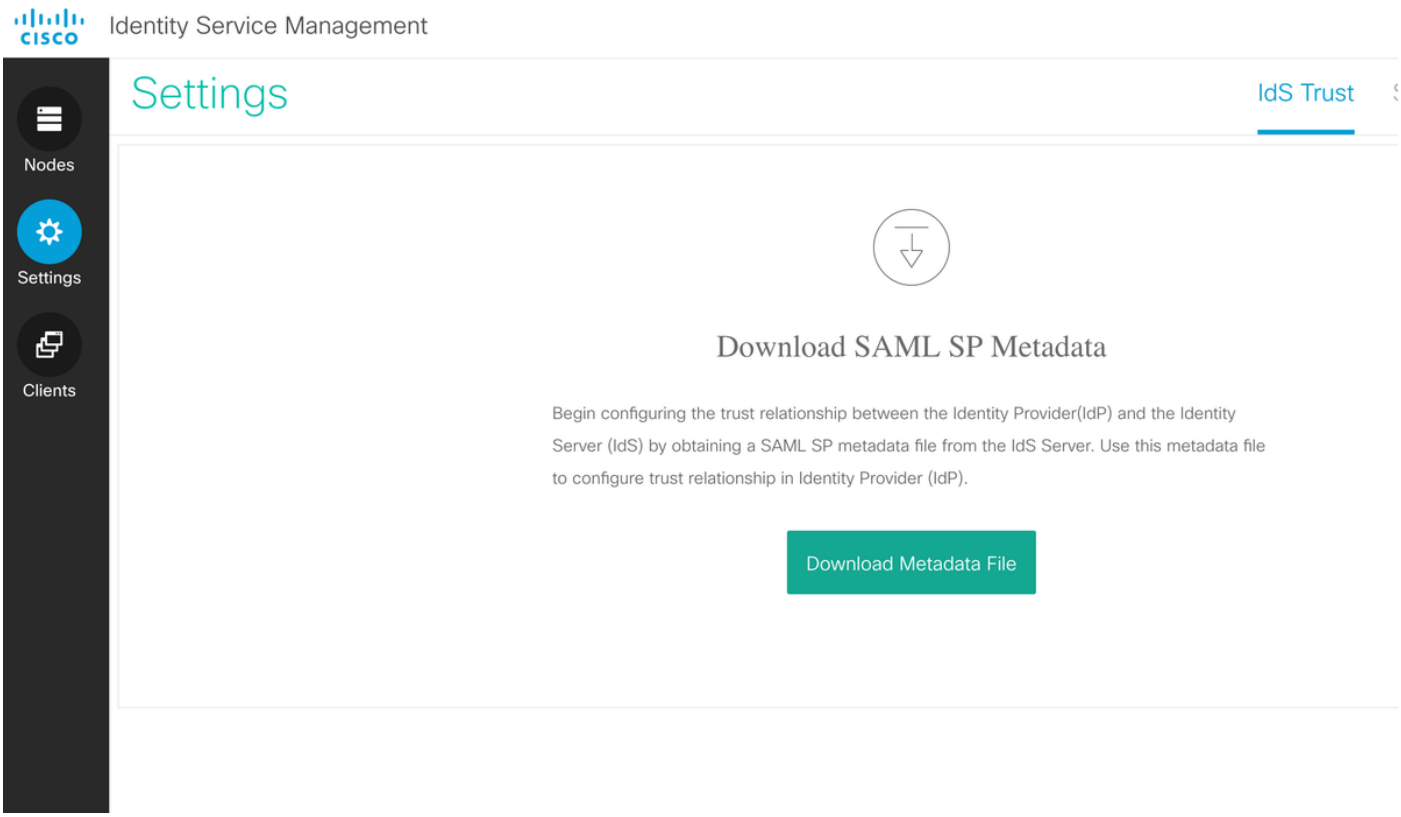
連線選項



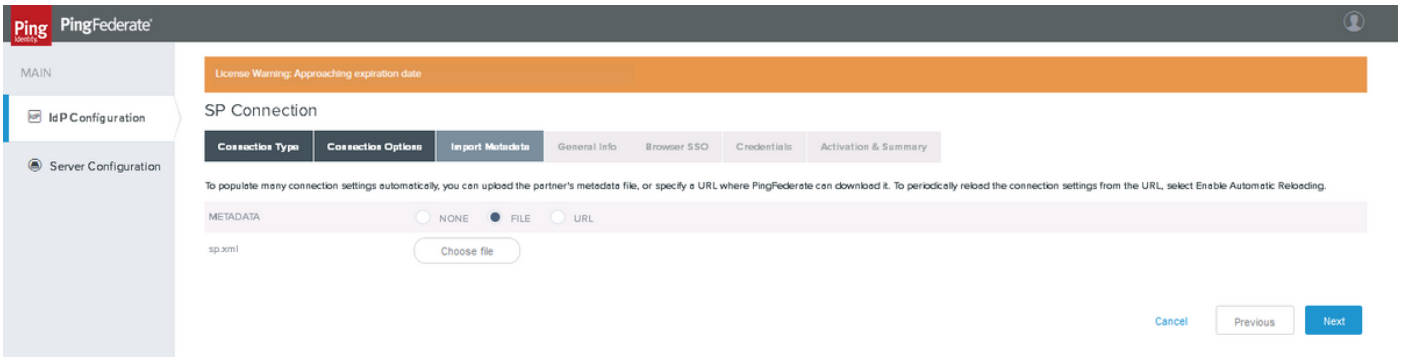
按一下下一步

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

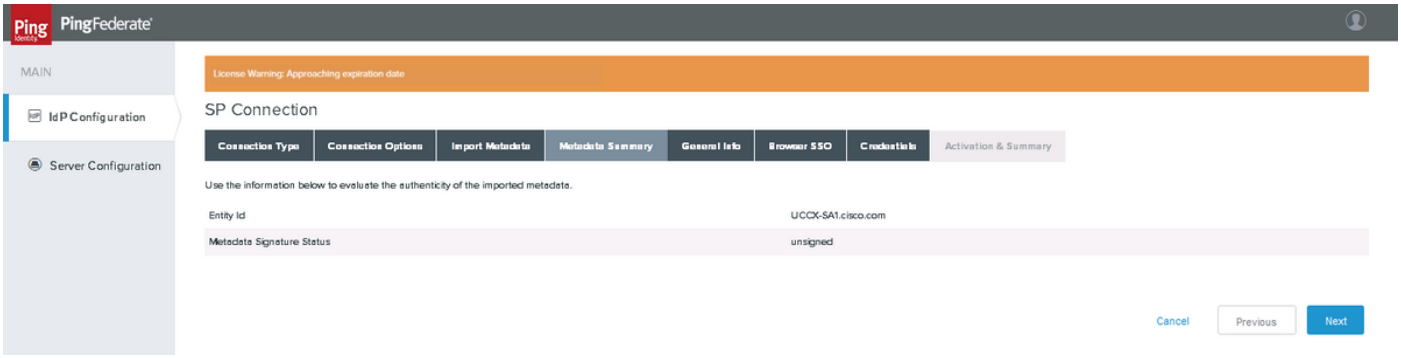


將服務提供程式的後設資料xml檔案上載到PingFederate。



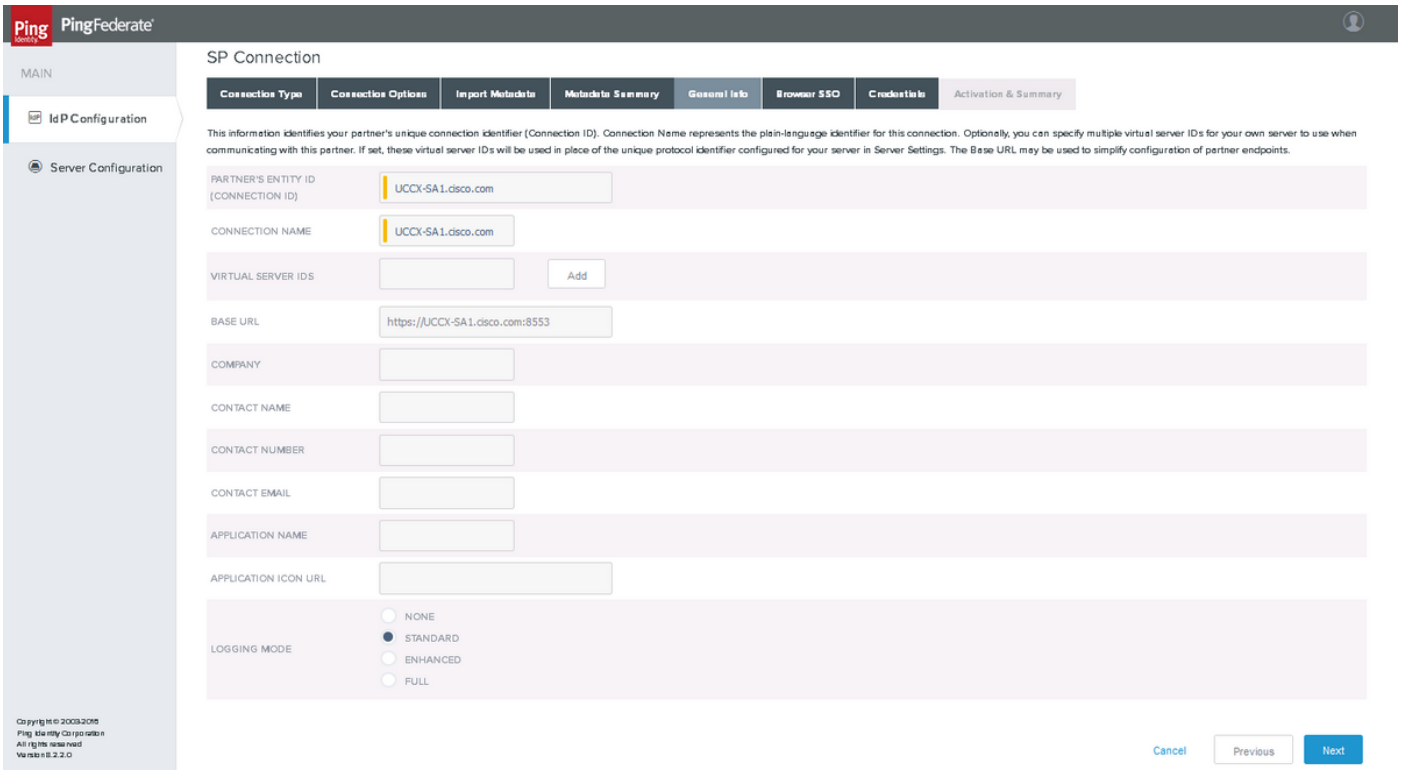
選擇下載的xml檔案，然後按一下「下一步」

後設資料摘要



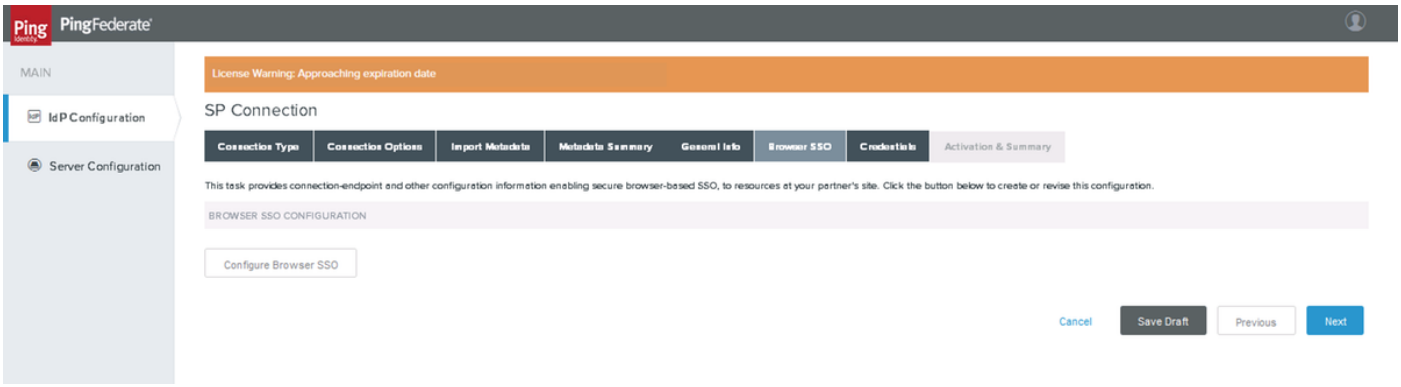
按一下下一步

一般資訊



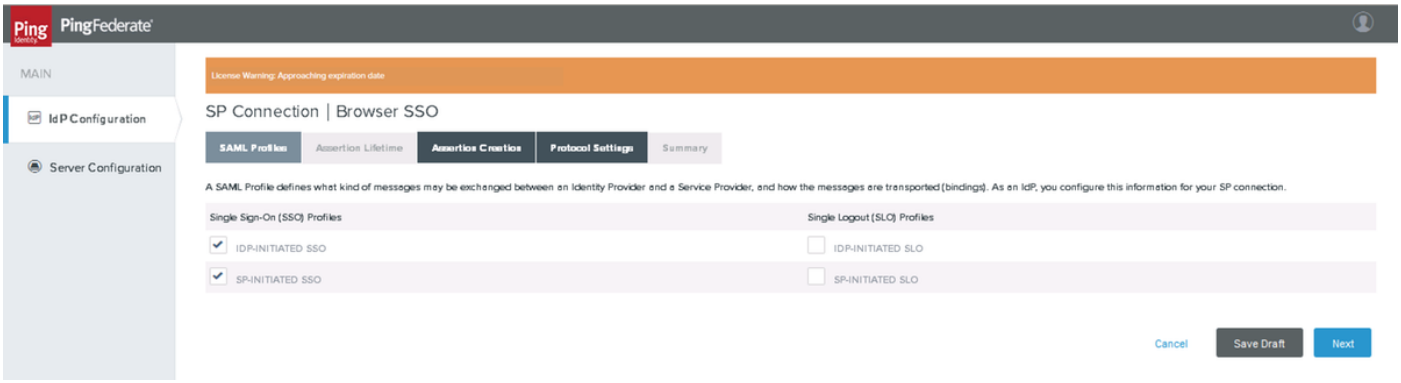
按一下下一步

瀏覽器SSO



按一下Configure Browser SSO

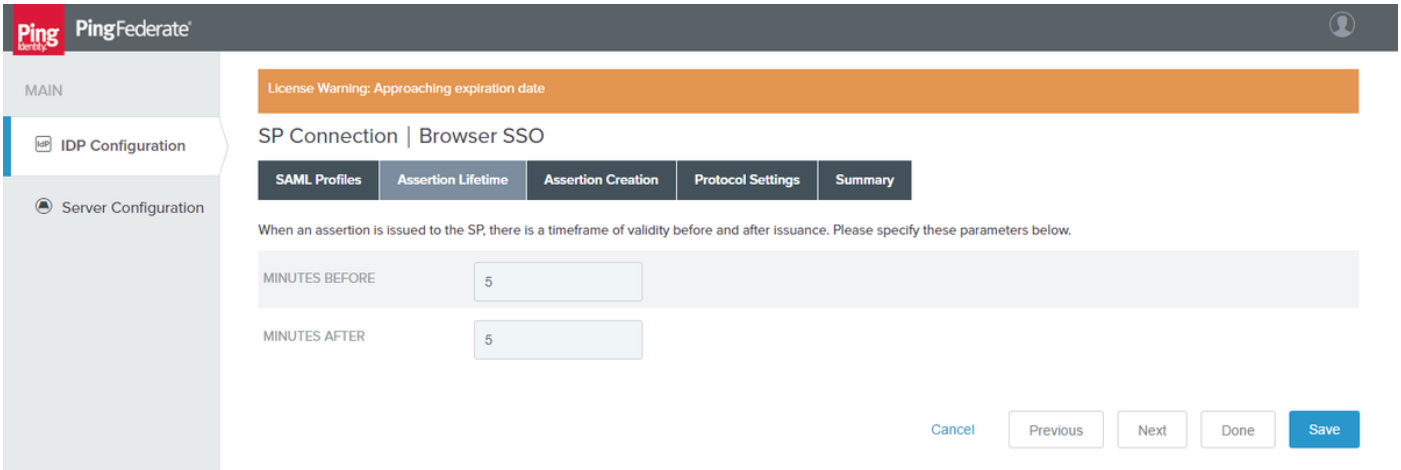
安全斷言標籤語言(SAML)配置檔案



按一下下一步

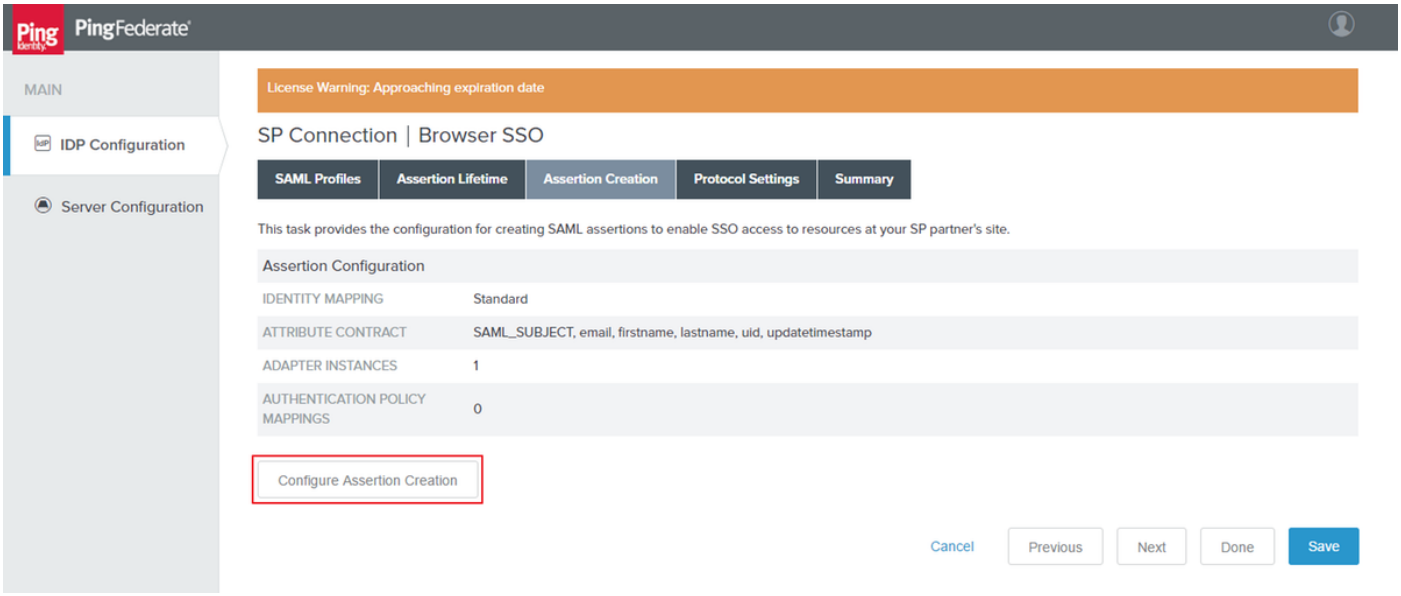
> 附註：思科身份服務(IdS)在11.6中不支援單一註銷(SLO)，並且未選擇此選項。

斷言生存期



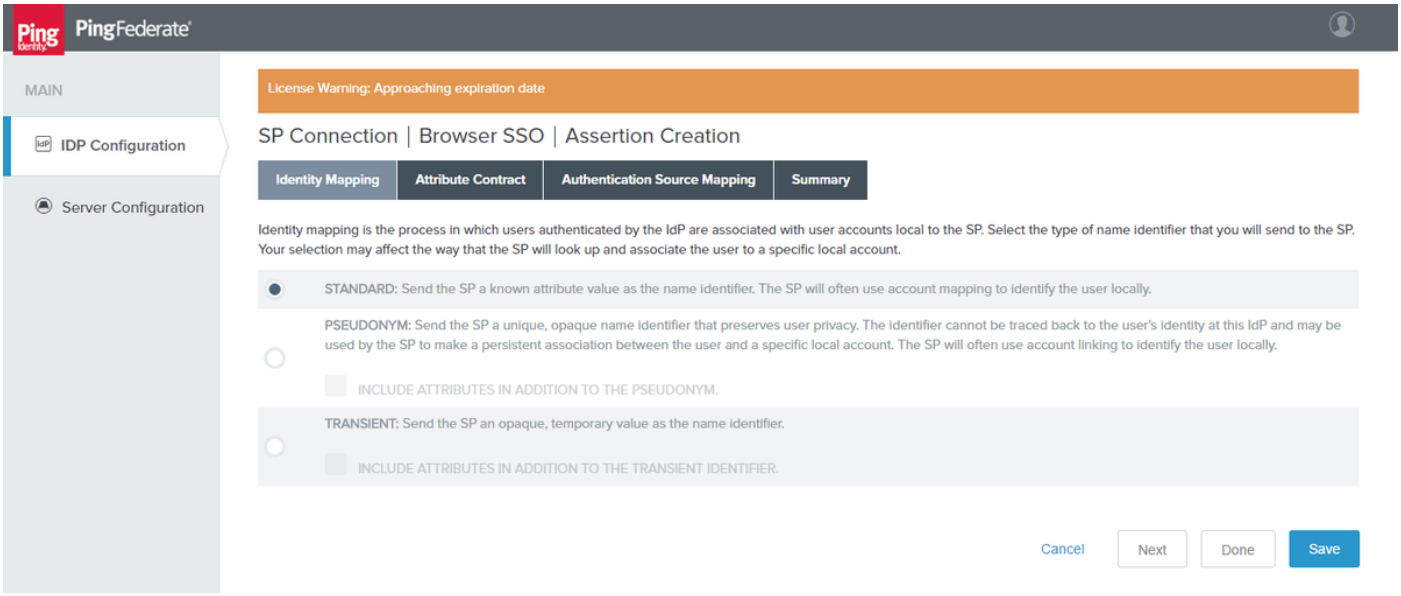
按一下下一步

斷言建立



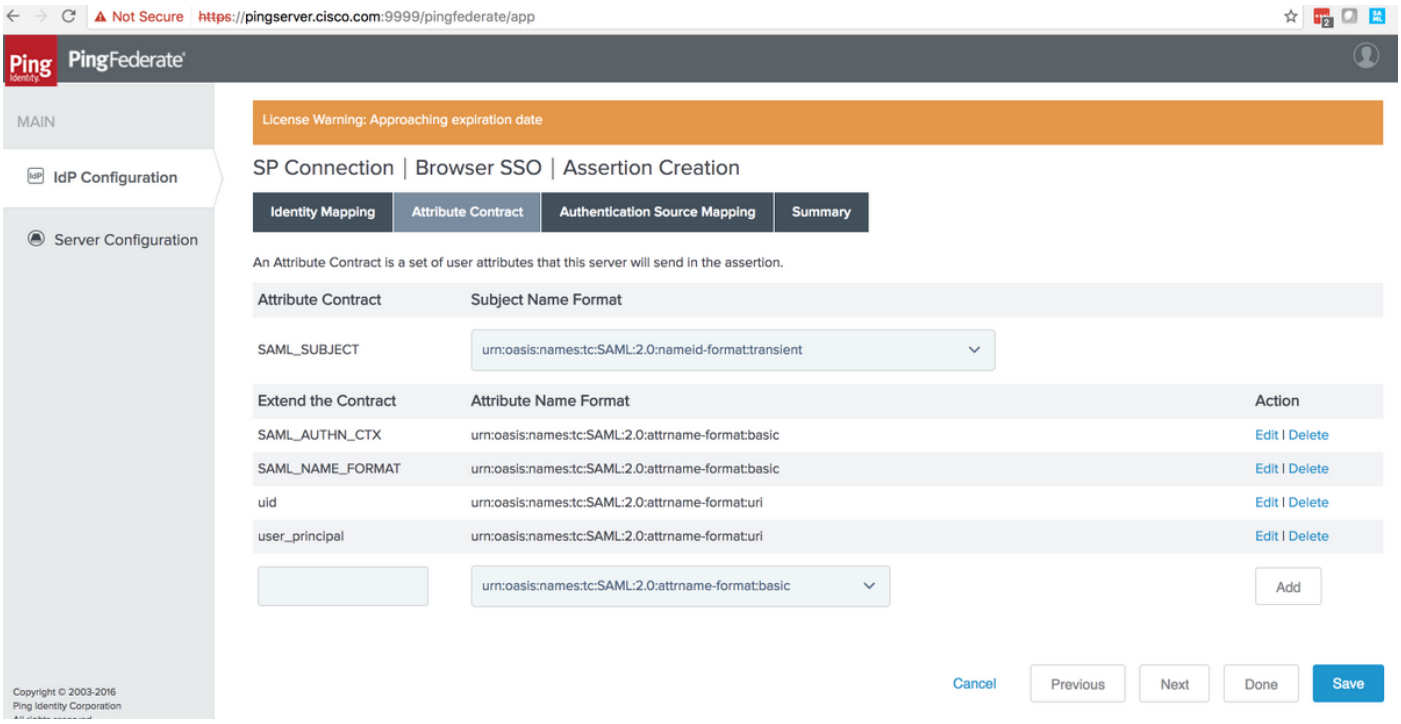
按一下配置斷言建立

身份對映



按一下下一步

屬性合約



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

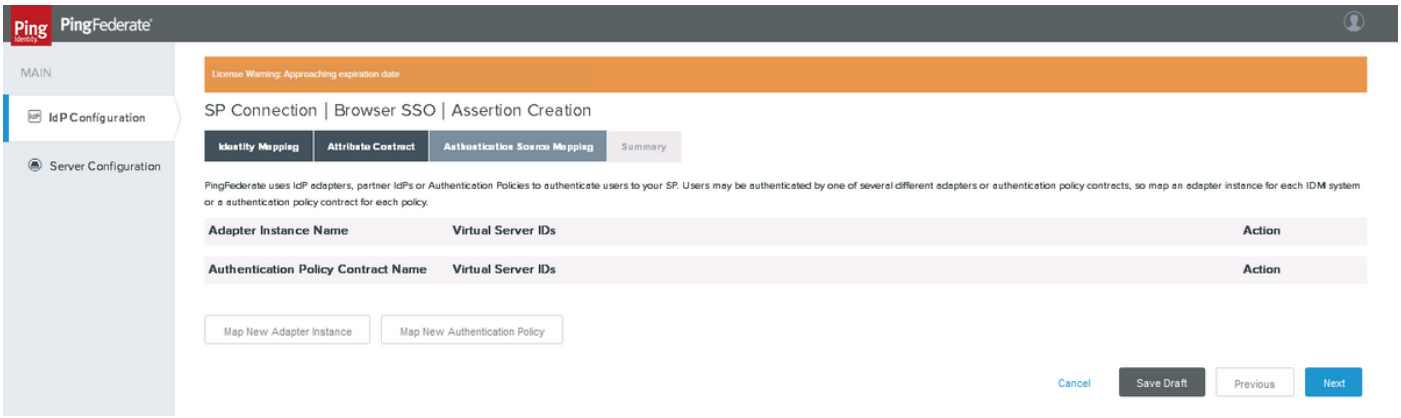
屬性合約	目的
SAML_SUBJECT	PingFederate搜尋過濾器用於檢查是否滿足對映值
SAML_AUTHN_CTX	在SAML響應中用於指示「PasswordProtectedTransport」身份驗證內容
SAML名稱格式	用於SAML響應以指示SAML 2.0臨時名稱ID格式
uid	由Cisco IdS用於識別經過身份驗證的使用者
user_principal	由Cisco IdS用來識別通過身份驗證的使用者的完整名稱（即id +域）

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。

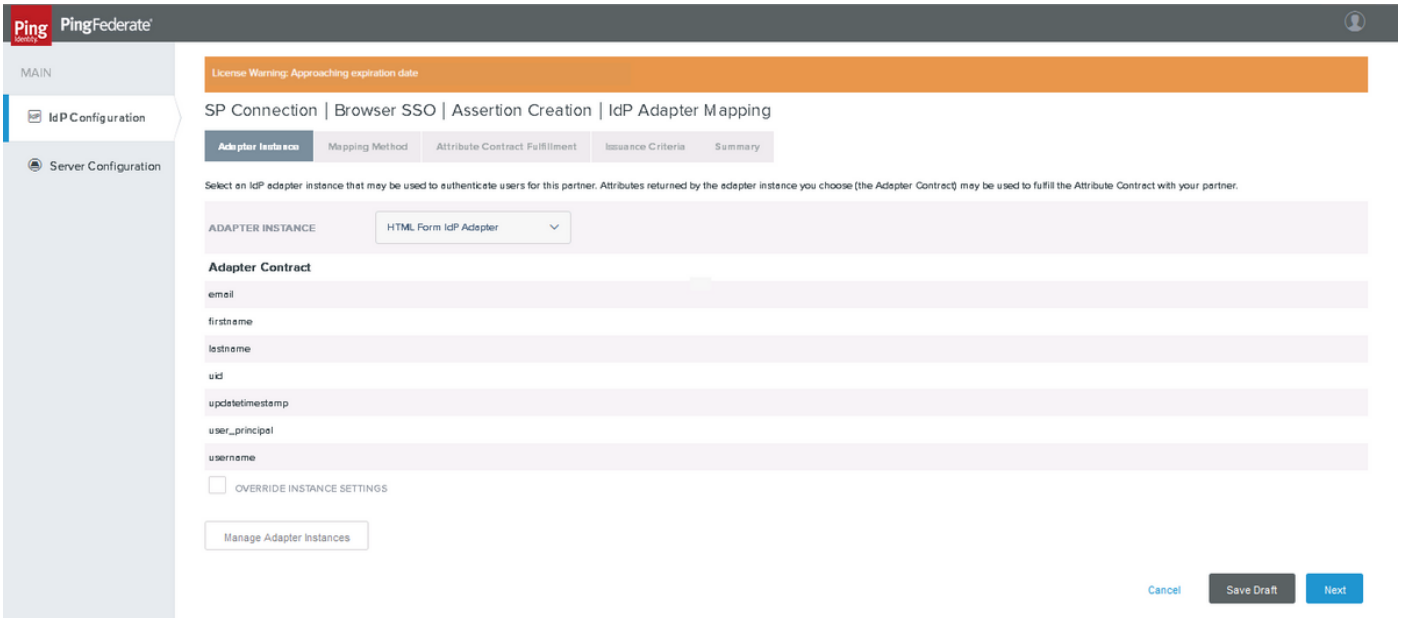
要使用瞬態作為名稱識別符號的SSO操作，請在saml2-subject-name-formats部分下新增xml項：<con:item name="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">urn:oasis:names:tc:SAML:2.0:nameid-format:transient</con:item>

按一下下一步

驗證來源對應

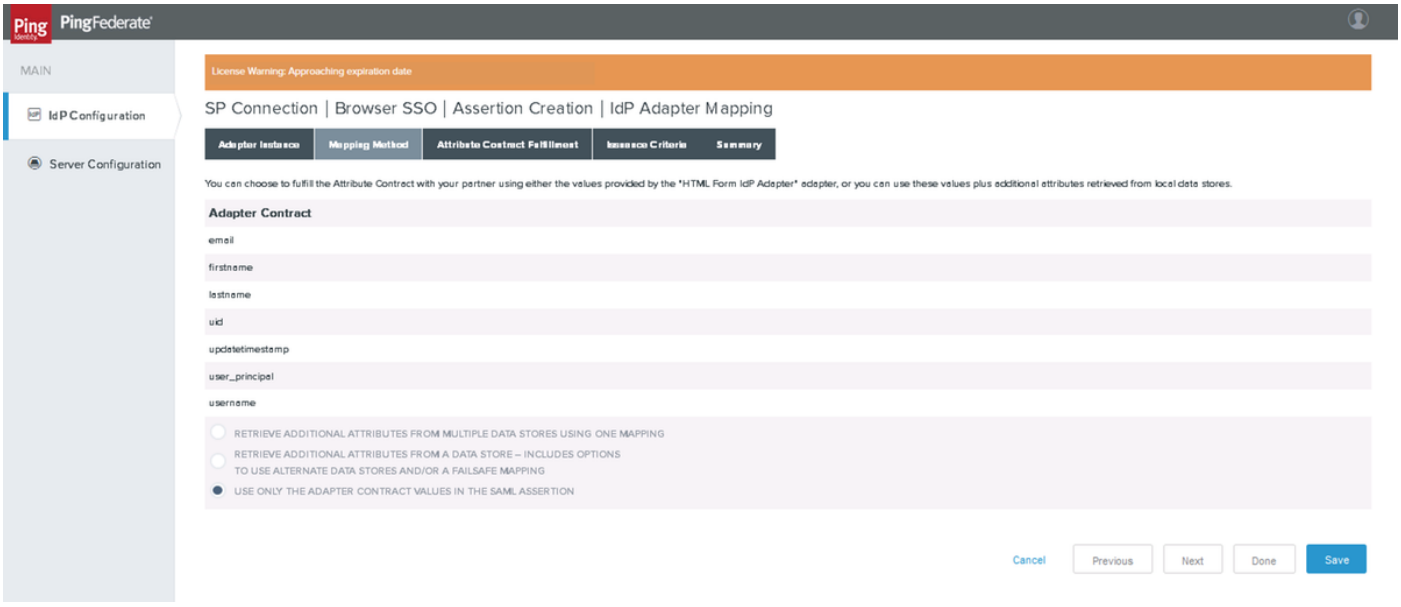


按一下Map New Adapter Instance



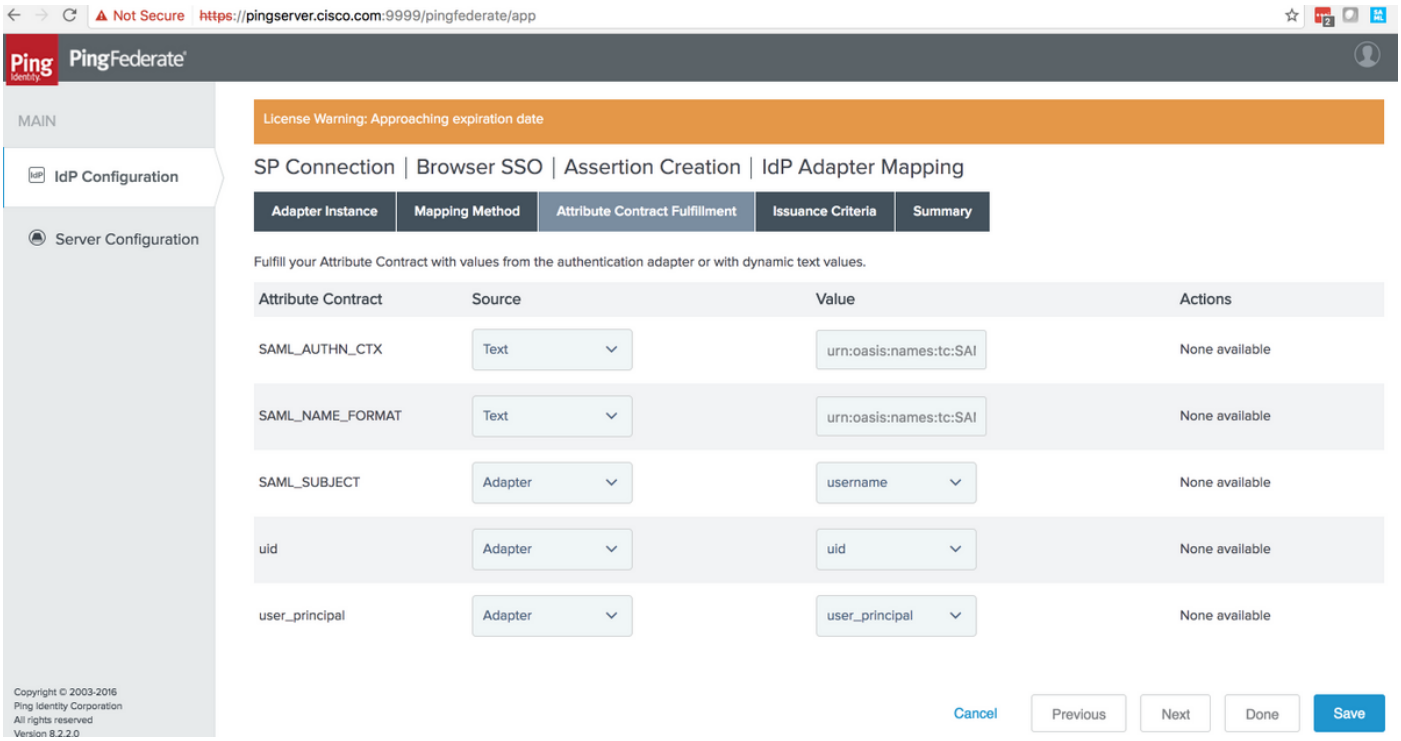
對映之前建立的HTML表單IdP介面卡。按一下下一步

對映方法



按一下下一步

屬性合約履行

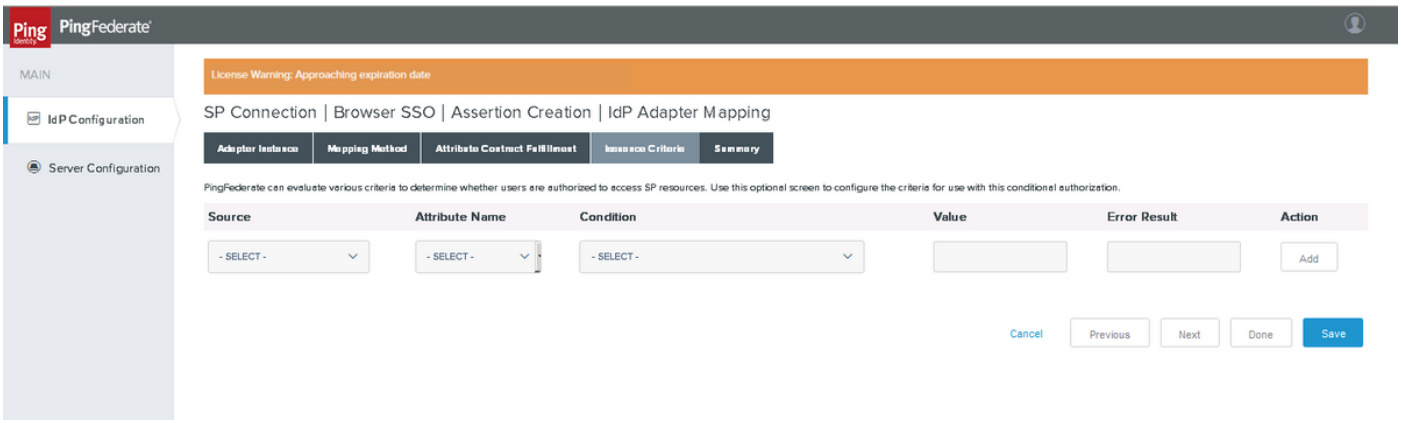


確保將值設定為

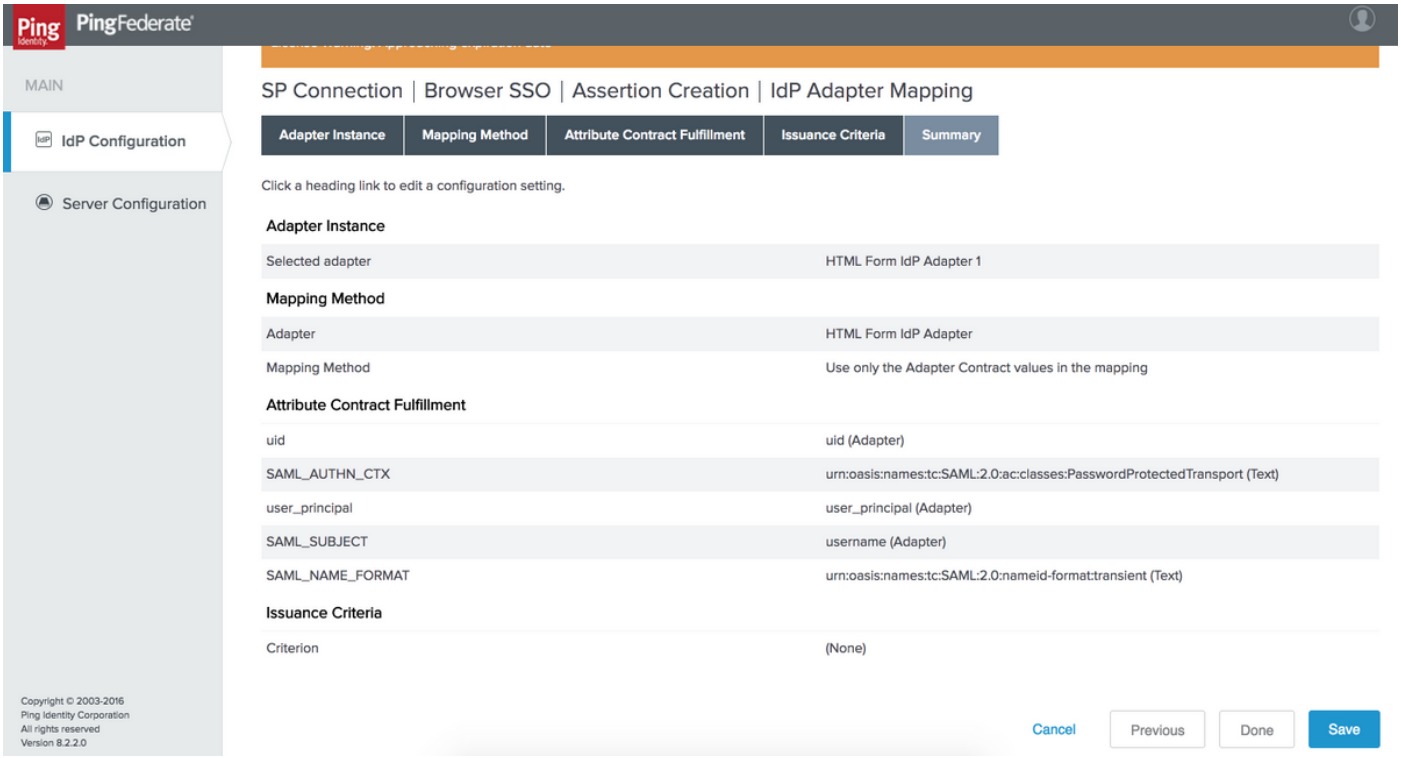
屬性合約	來源	價值
SAML_SUBJECT	介面卡	使用者名稱 非常重要附註：用於此設定的值必須與LDAP過濾器設定中使用的值相匹配（節#3.1.3.2。例項配置） 附註：此處使用了「username」，因為此處使用了sAMAccountName=${username}
SAML_AUTHN_CTX	文本	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
SAML名稱格式	文本	urn:oasis:names:tc:SAML:2.0:nameid-format:transient
uid	介面卡	uid
user_principal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

按一下下一步

發佈標準

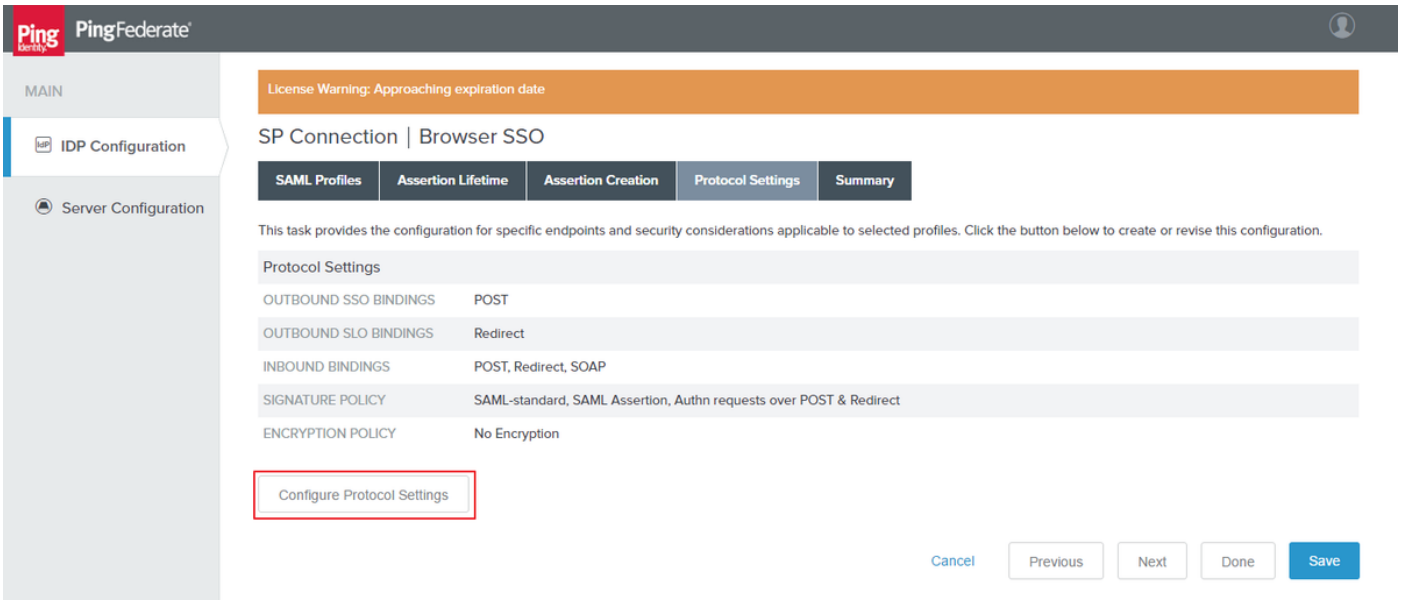


摘要



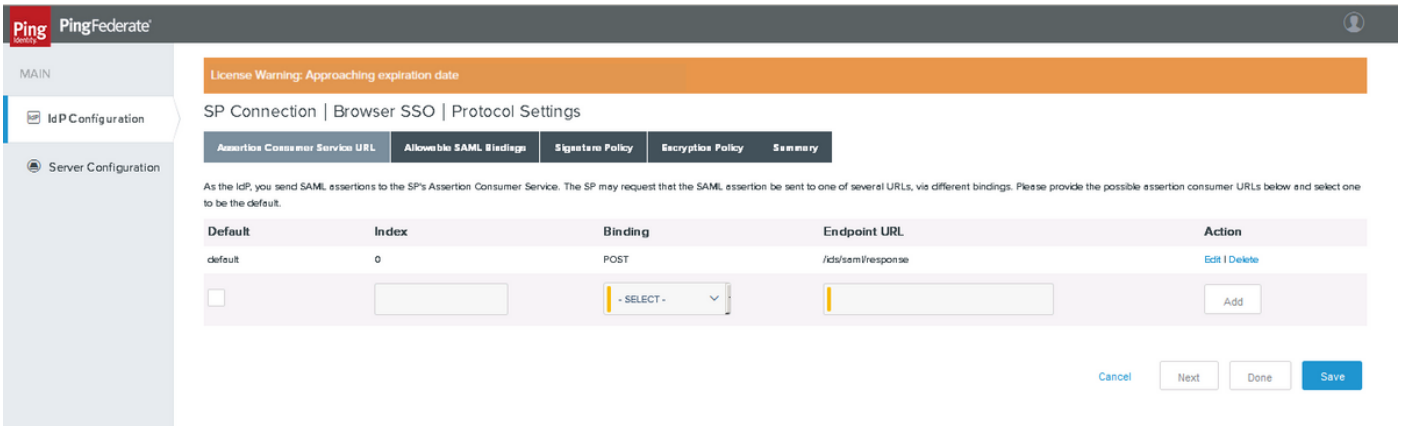
驗證設定並按一下Done

協定設定



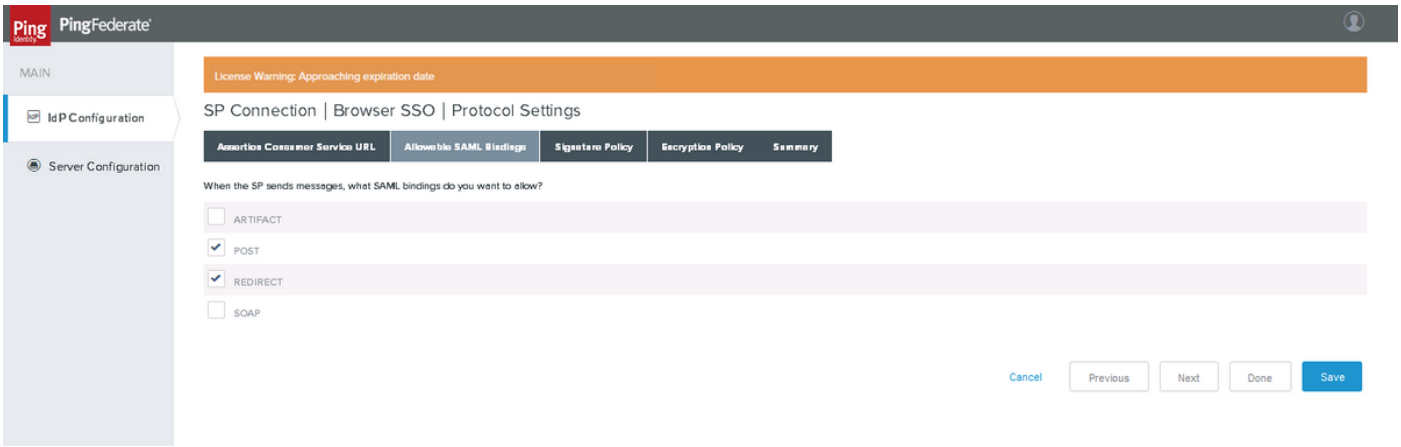
按一下Configure Protocol Settings

斷言使用者服務URL



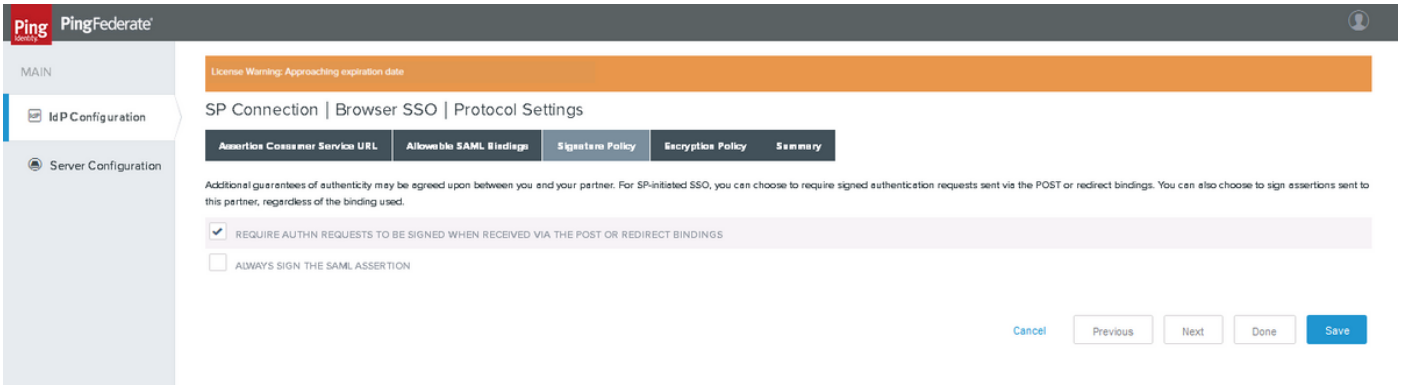
新增POST繫結SSO終結點。按一下下一步

允許的SAML繫結



按一下下一步

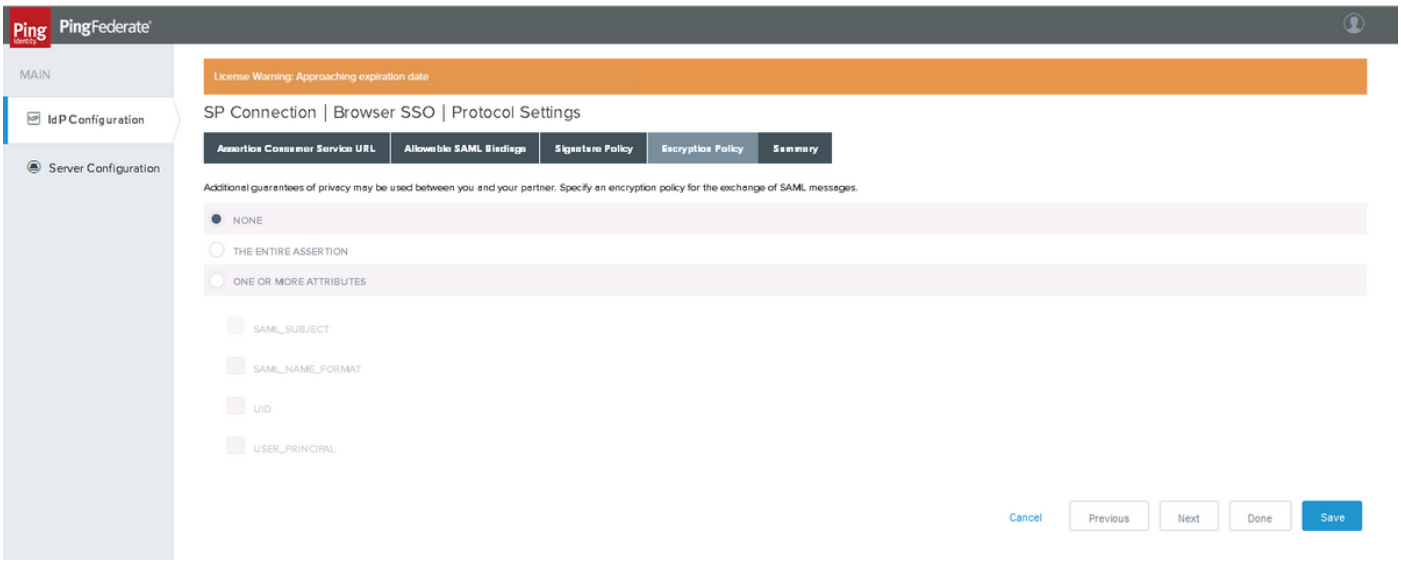
簽名策略



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

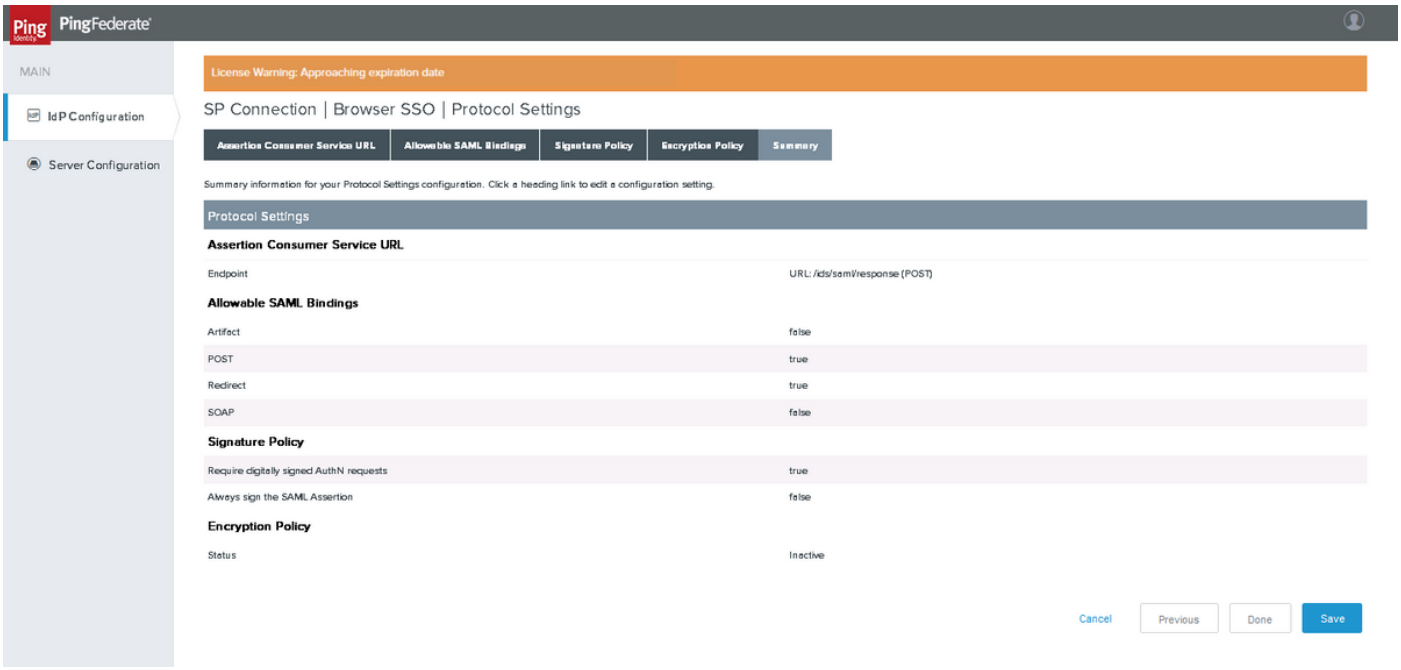
加密策略



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

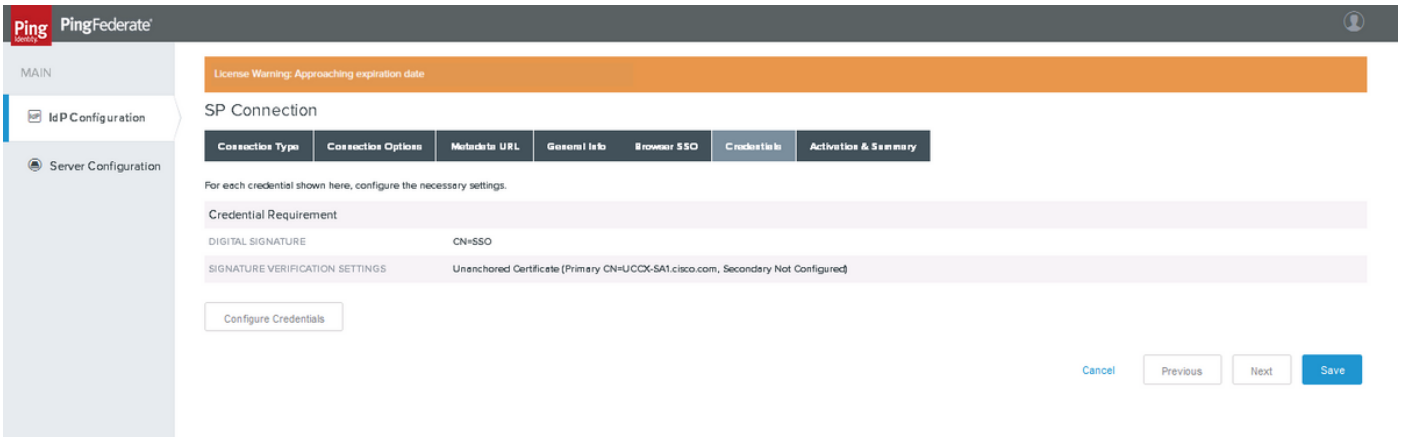
按一下下一步

摘要



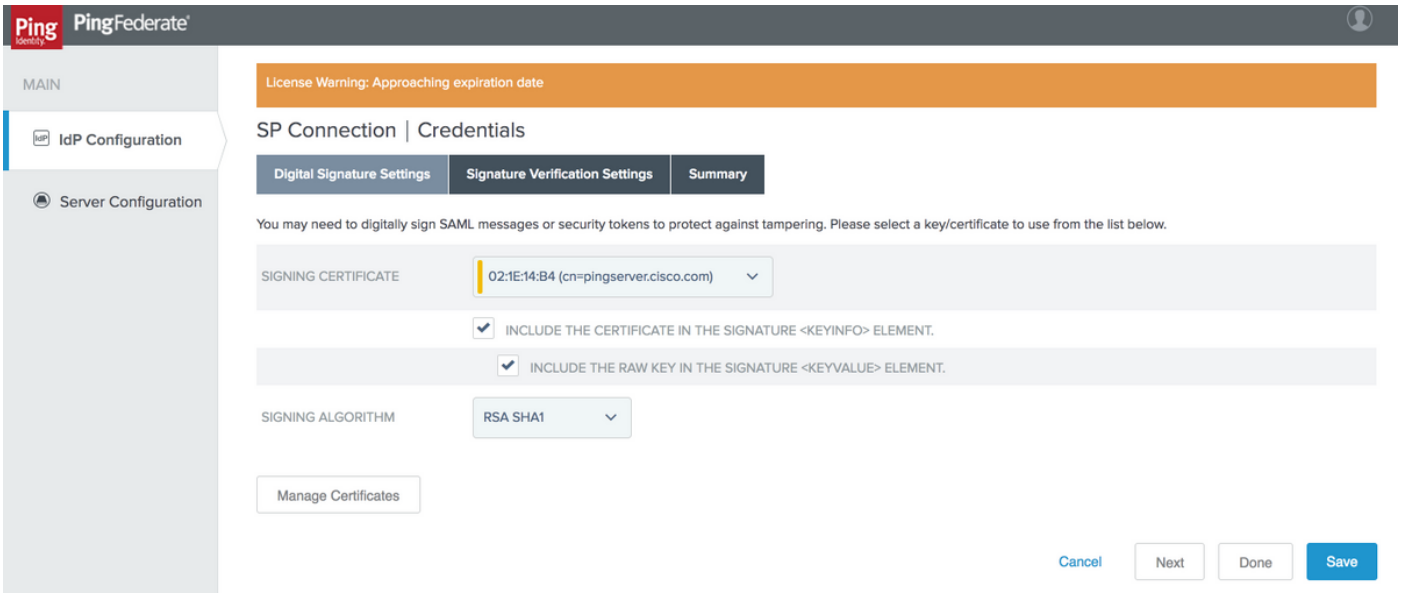
驗證設定並按一下Done

憑證



按一下Configure Credentials

數位簽章設定

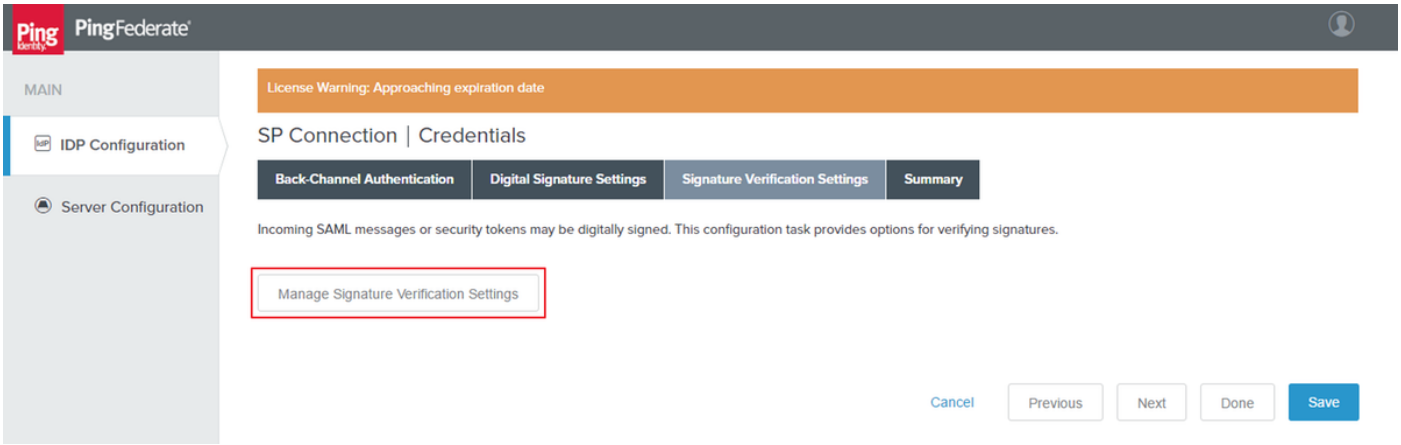


選擇SIGNING CERTIFICATE CREATED Early。如果沒有，您可以按一下Manage Certificates以建立證書。

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

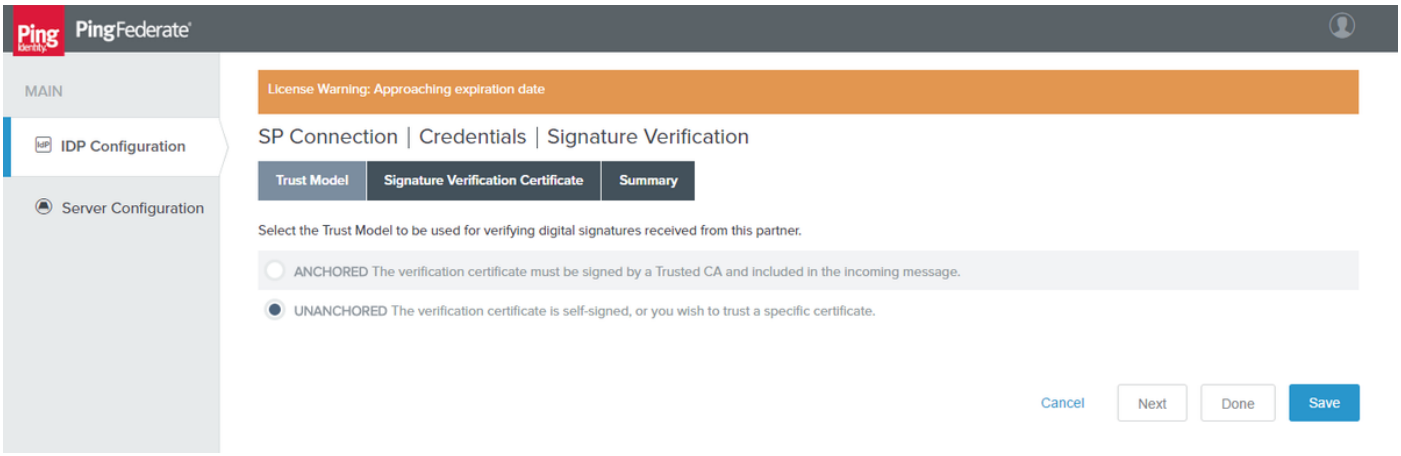
按一下下一步

簽名驗證設定



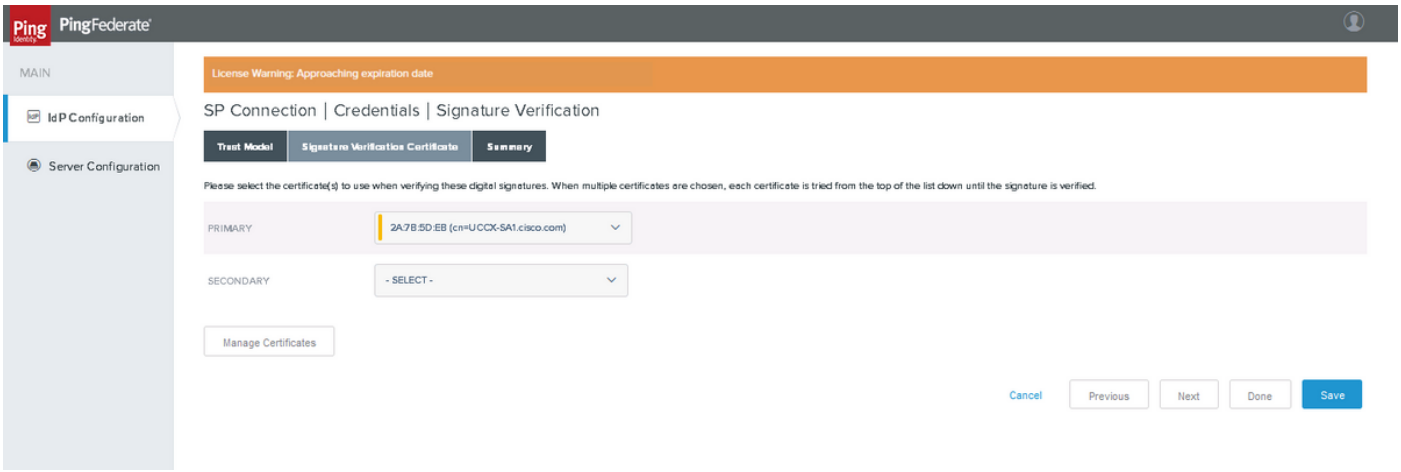
按一下管理簽名驗證設定

信任模型

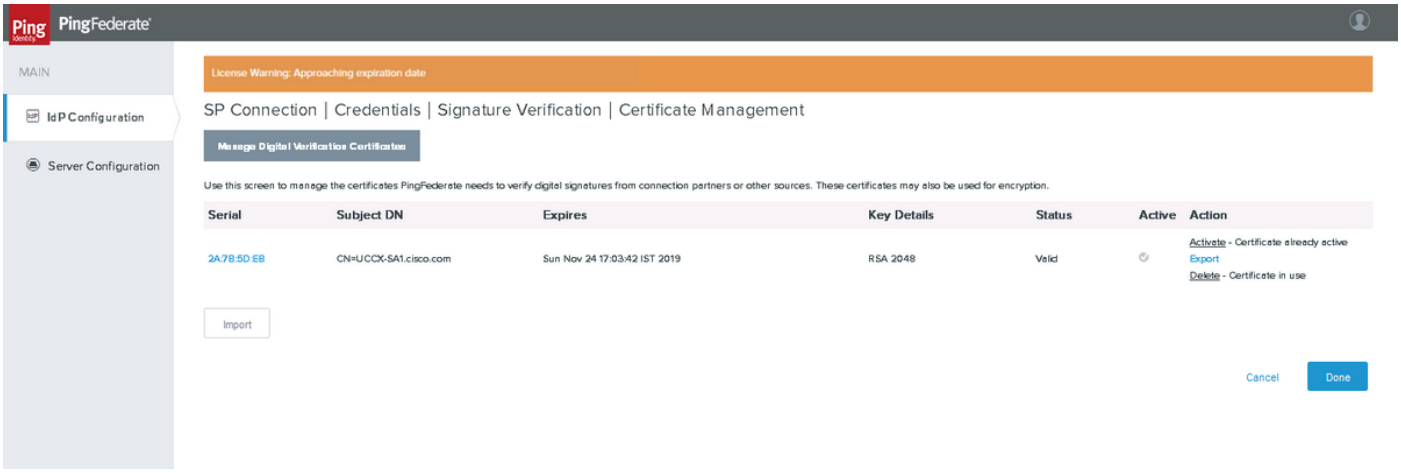


按一下下一步

簽名驗證證書

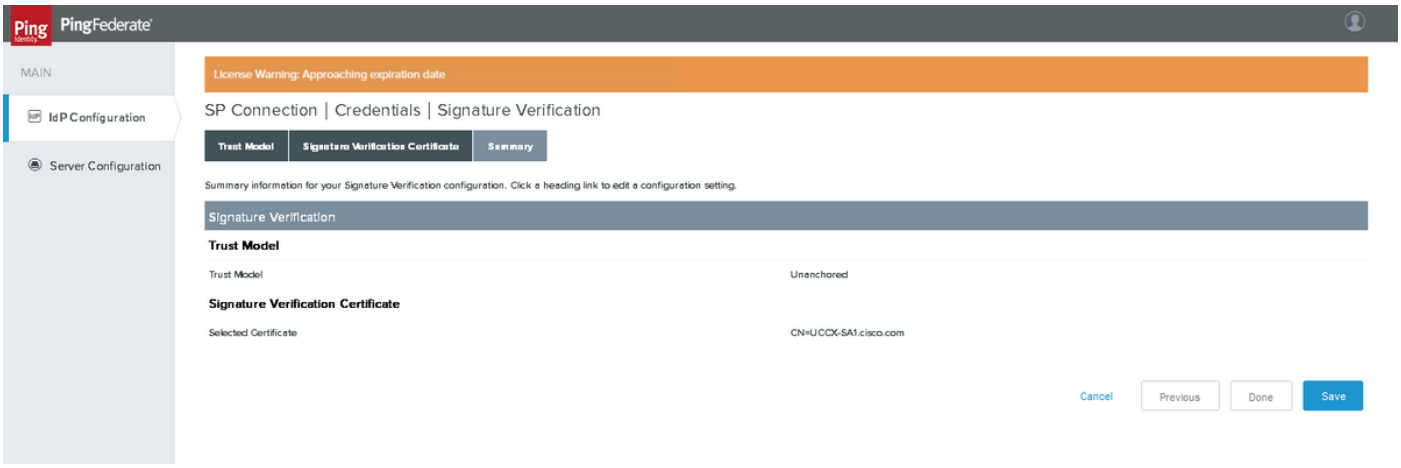


按一下Manage Certificates以從SP匯入證書。



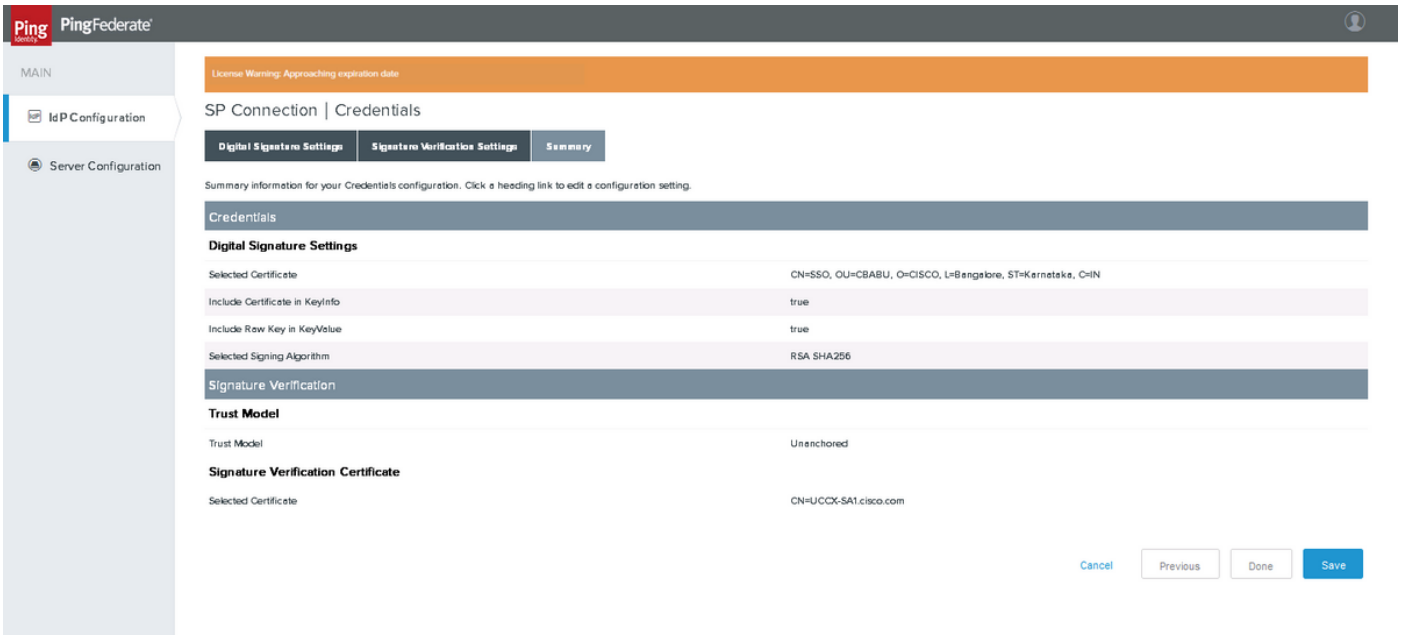
按一下「Import」以匯入憑證。

摘要



按一下完成

摘要



驗證摘要並按一下Done

啟用與摘要

PingFederate

MAIN

IdP Configuration

Server Configuration

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	ACTIVE / 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

Copyright © 2003-2016
Ping Identity Corporation

PingFederate

MAIN

IdP Configuration

Server Configuration

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

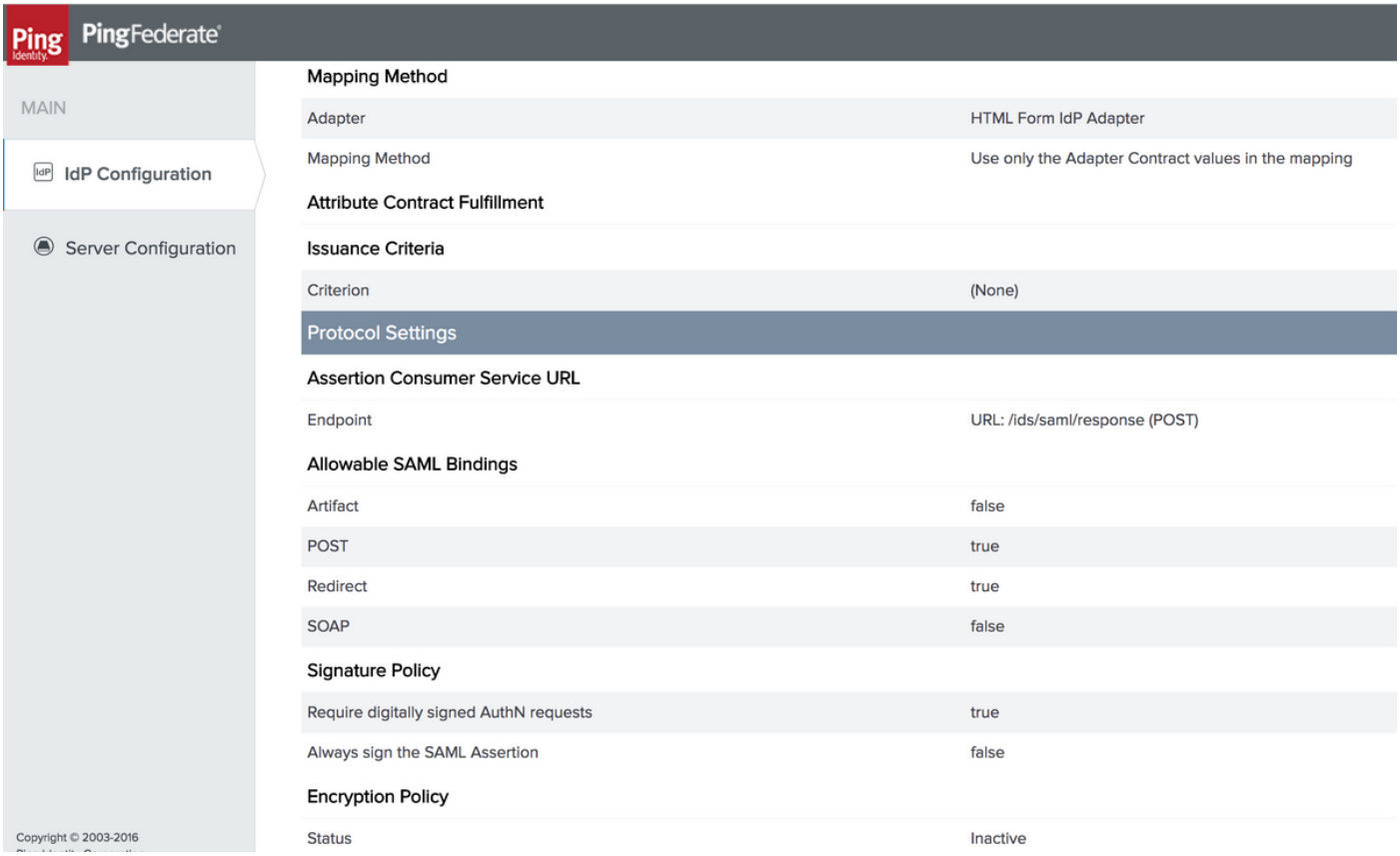
Authentication Source Mapping

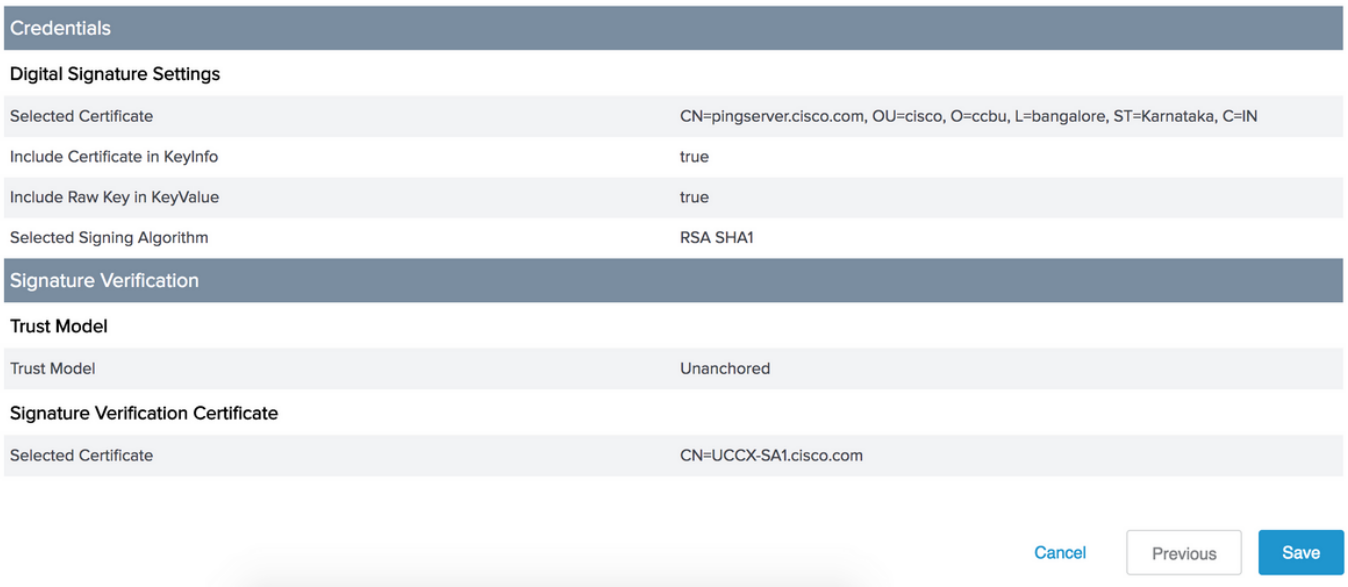
Adapter instance name	HTML Form IdP Adapter 1

Adapter Instance

Selected adapter	HTML Form IdP Adapter 1

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

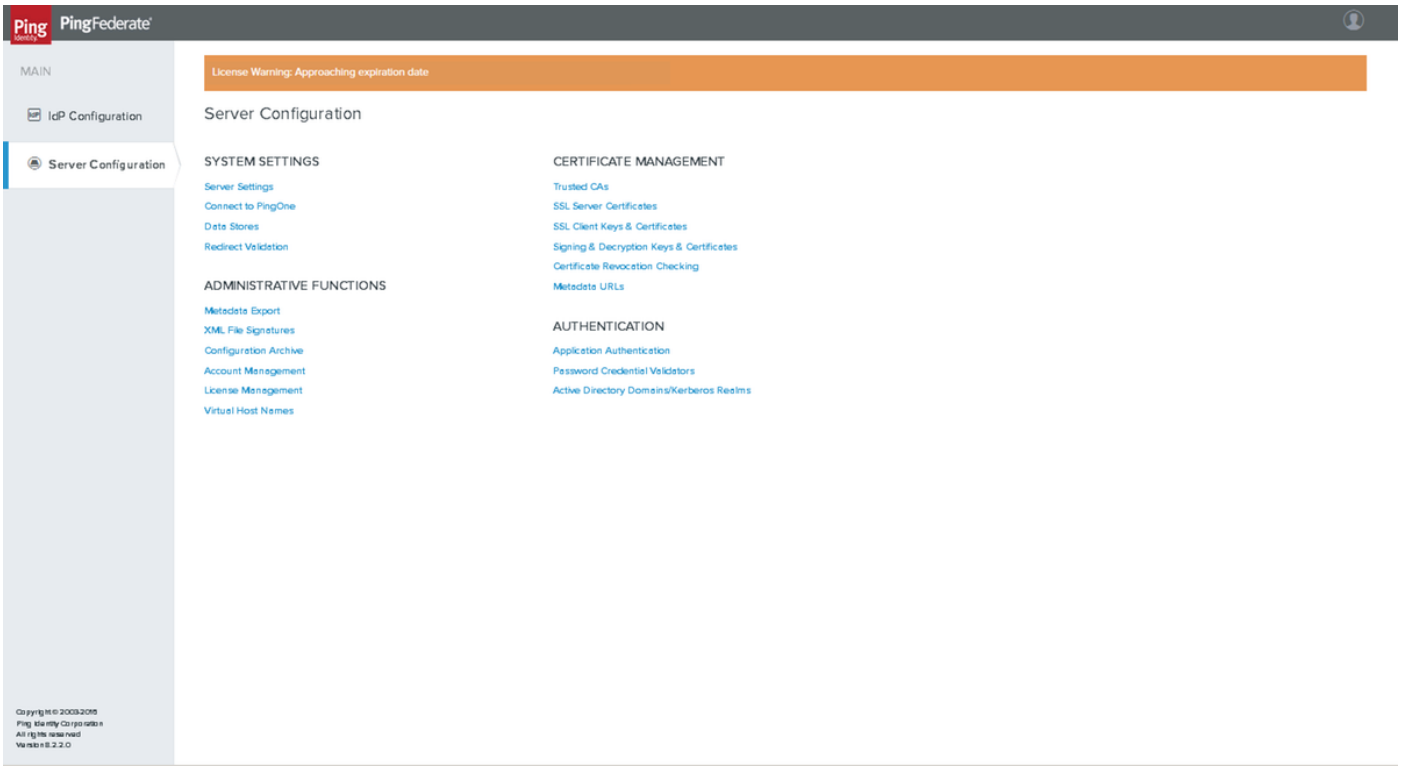




驗證摘要並按一下Save。

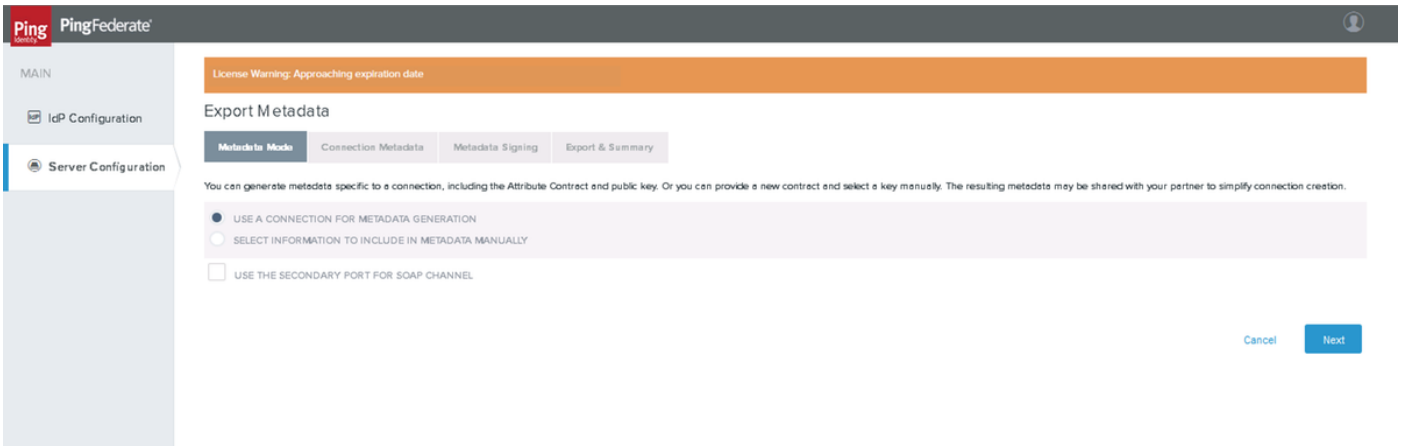
匯出PingFederate後設資料

後設資料匯出



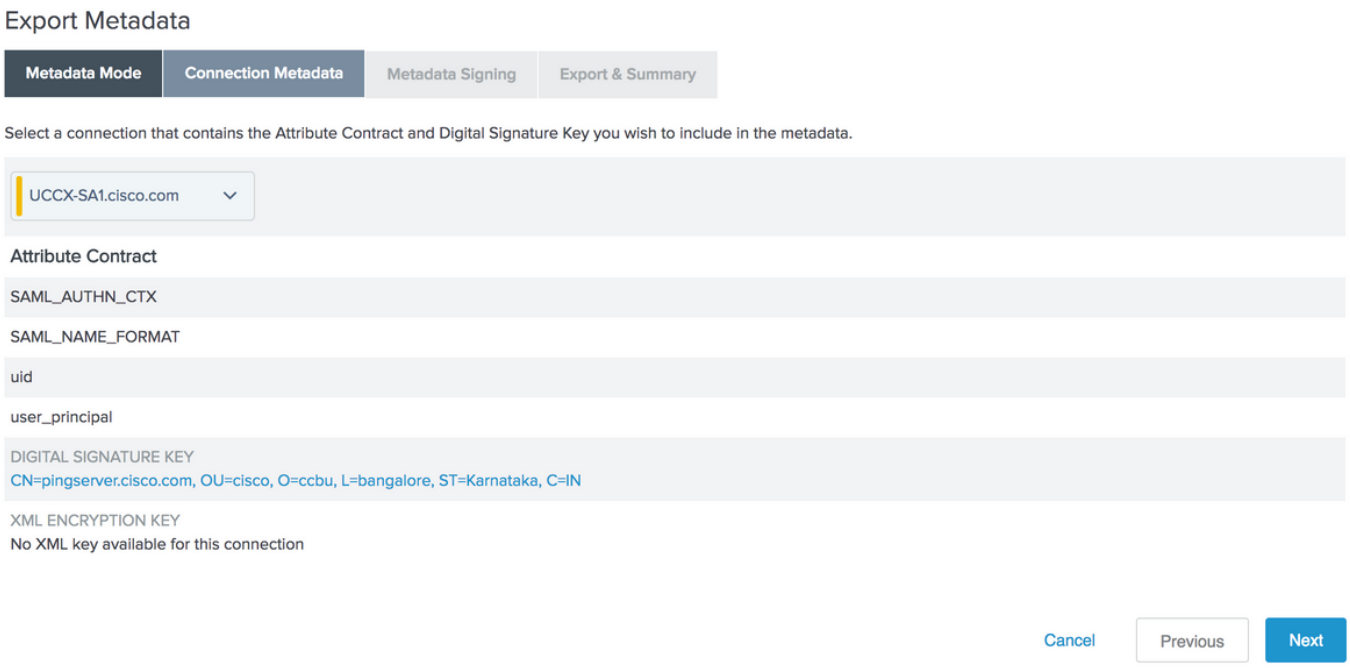
後設資料模式

按一下Server Configuration > ADMINISTRATIVE FUNCTIONS > Metadata Export



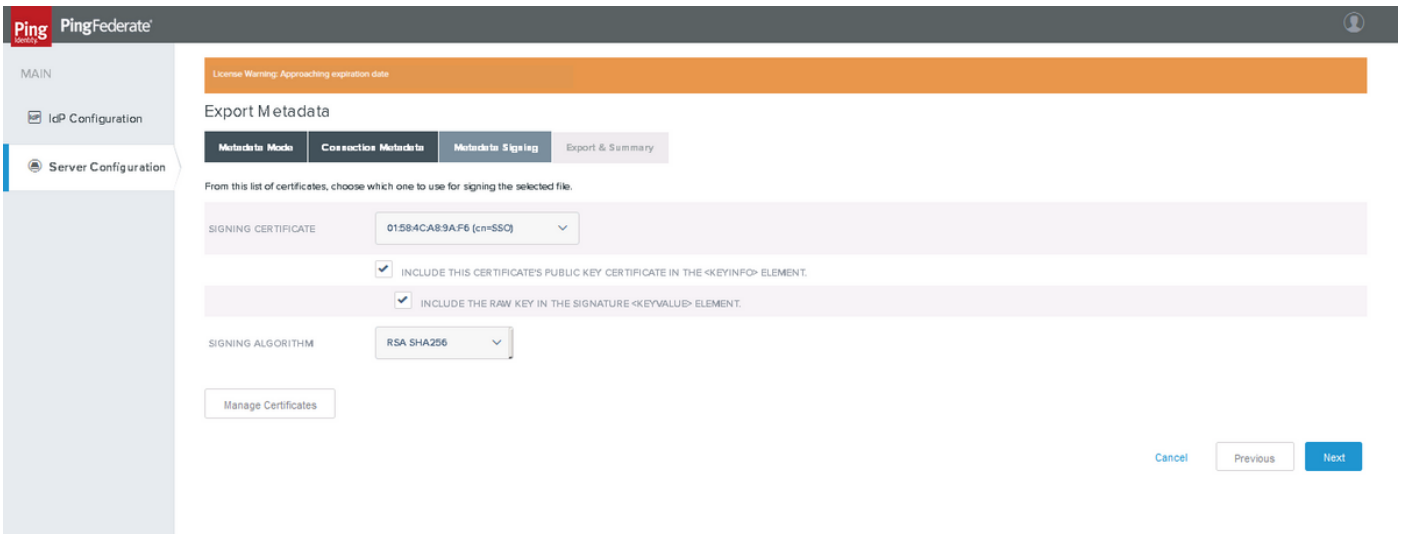
按一下下一步

連線後設資料



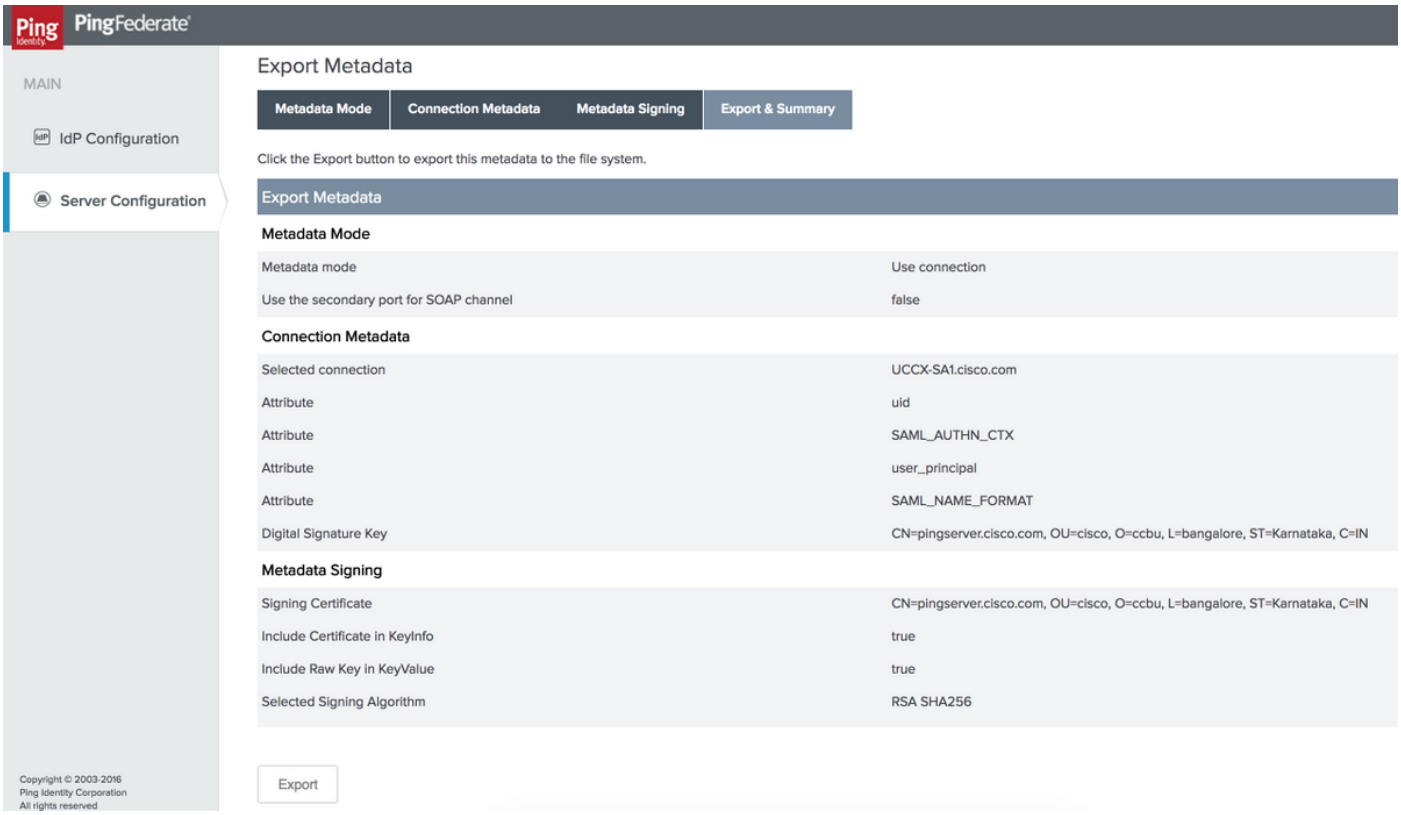
選擇已建立的SP連線，然後按一下下一步

後設資料簽名



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
		• 如果不是，請檢查它是否指示「Requester」或「Responder」 ◦ 「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	檢查<saml:AuthnContextClassRef>元素 — 其值必須是urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport 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。
SAML流失敗	SAML跟蹤器	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 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
SAML流失敗	SAML跟蹤器	檢查Cisco Id或PingFederate日誌中是否存在「Invalid Signature」（無效簽名）消息。 如果確認，請在Id和PingFederate之間重新建立後設資料信任
SAML流失敗	SAML跟蹤器	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

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）。