

# Installare e configurare il provider di identità federativa ping per il servizio identità Cisco per abilitare l'SSO

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Install](#)

[Requisiti di sistema](#)

[Sistemi operativi](#)

[Ambiente Java](#)

[Browser supportati per gli utenti finali](#)

[Browser supportati per la console di amministrazione](#)

[Integrazione archivio dati](#)

[\(per la ricerca di attributi utente\)](#)

[Requisiti hardware minimi](#)

[Requisiti hardware minimi](#)

[Install](#)

[Installa PingFederate con file ZIP di distribuzione](#)

[Installa PingFederate con file EXE di distribuzione](#)

[Avviare PingFederate per la prima volta](#)

[Installazione guidata iniziale](#)

[Accetta contratto di licenza](#)

[Account PingOne](#)

[Licenza](#)

[Informazioni di base](#)

[Abilita ruoli](#)

[Configurazione provider di identità](#)

[Account amministratore](#)

[Conferma](#)

[Completa](#)

[Configura federazione ping](#)

[Configurazione server](#)

[Chiavi e certificati di decrittografia XML \(Digital Signing and Extensible Markup Language\)](#)

[Archivi dati](#)

[Convalide credenziali password](#)

[Impostazioni server](#)

[Configurazione provider di identità](#)

[Adattatori](#)

[Connessioni SP](#)

---

[Esporta metadati PingFederate](#)

[Esportazione metadati](#)

[Modalità metadati](#)

[Metadati connessione](#)

[Firma metadati](#)

[Esportazione e riepilogo](#)

[Metadati di esempio](#)

[Risoluzione dei problemi](#)

[Ulteriore configurazione per SSO:](#)

---

## Introduzione

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

Modelli di distribuzione Cisco IdS

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

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

---

Nota: Questo documento fa riferimento alla configurazione di Cisco Identity Service (IdS) e del provider di identità (IdP). Il documento fa riferimento a UCCX negli screenshot ed esempi, tuttavia la configurazione è simile a quella di Cisco Identity Service (UCCX/UCCE/PCCE) e dell'IdP.

---

### Componenti usati

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

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

## Install

### Requisiti di sistema

Sistemi operativi	Ambiente Java	Browser supportati per gli utenti finali	Browser supportati per la console di amministrazione	Integrazione archivio dati (per la ricerca di attributi utente)	R ha
<ul style="list-style-type: none"> <li>• Microsoft Windows Server 2008 R2 SP (Service Pack)</li> <li>• Microsoft Windows Server 2012 Standard</li> <li>• Microsoft Windows Server 2012 R2 Datacenter</li> <li>• Oracle Enterprise Linux 6.5 (kernel compatibile con Red Hat)</li> <li>• Oracle Solaris 10</li> <li>• Red Hat</li> </ul>	<ul style="list-style-type: none"> <li>• Oracle Java SE Runtime Environment (Server JRE) 7 aggiornamento 79 (64 bit)</li> <li>• Oracle Java SE Runtime Environment (Server JRE) 8 aggiornamento 45 (64 bit)</li> </ul>	<ul style="list-style-type: none"> <li>• Cromatura</li> <li>• Firefox</li> <li>• Internet Explorer (versione 9 e successiva)</li> <li>• Safari</li> </ul>	<ul style="list-style-type: none"> <li>• Cromatura</li> <li>• Firefox</li> <li>• Internet Explorer (versione 9 e successiva)</li> </ul>	<ul style="list-style-type: none"> <li>• Microsoft Active Directory (2008 R2 e 2012)</li> <li>• Oracle Directory Server Enterprise Edition 11g</li> <li>• Server Microsoft SQL (Structured Query Language) (2012 e 2014)</li> <li>• Database Oracle (10g e 11g R2)</li> <li>• Oracle MySQL 5.6</li> </ul>	<ul style="list-style-type: none"> <li>•</li> <li>•</li> <li>•</li> </ul>

Enterprise Linux ES 6.6 • Red Hat Enterprise Linux ES 7.0 • SUSE Linux Enterprise 11 SP 3					
---	--	--	--	--	--

## Install

Estrarre il file ZIP di distribuzione o utilizzare un programma di installazione specifico della piattaforma per installare PingFederate.

- Richiedere una chiave di licenza nella pagina Web delle licenze Ping Identity ([www.pingidentity.com/support-and-downloads/licensing.cfm](http://www.pingidentity.com/support-and-downloads/licensing.cfm))
- Verificare di aver eseguito l'accesso al sistema con i privilegi appropriati per installare ed eseguire un'applicazione
- Verificare che Server Java Runtime Environment (JRE) sia installato e che le variabili di ambiente e PATH siano impostate correttamente

## Installa PingFederate con file ZIP di distribuzione

Estrarre il file ZIP di distribuzione in una directory di installazione.

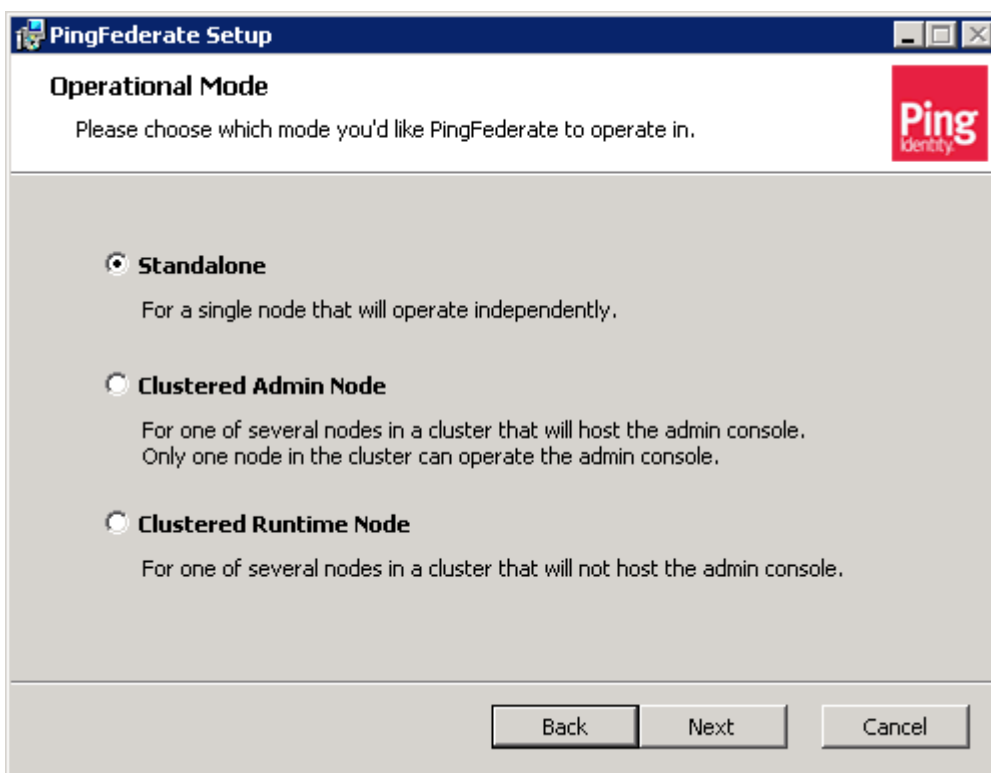
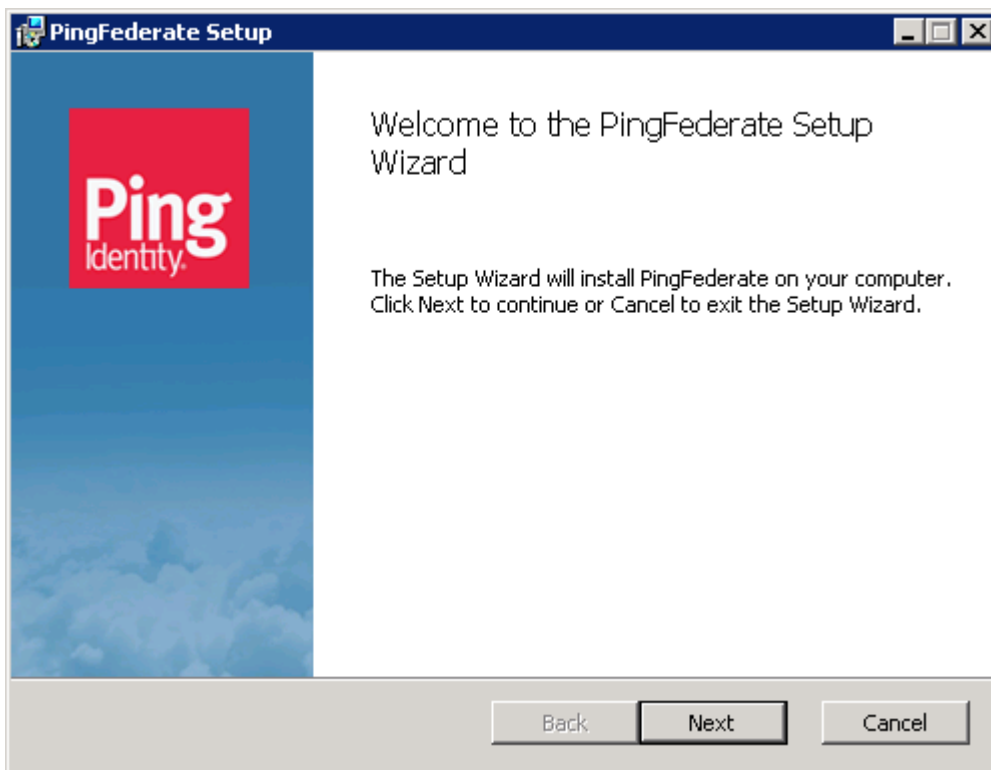
---

Avviso: Per evitare problemi futuri con gli aggiornamenti automatici, non rinominare la cartella pingfederate installata. Se si installano più istanze di PingFederate nello stesso computer, ad esempio in determinati scenari di clustering del server, installare ogni istanza in un percorso diverso o rinominare la cartella padre per installare una struttura di file parallela nello stesso percorso.

---

## Installa PingFederate con file EXE di distribuzione


Fare doppio clic sul file exe e seguire le istruzioni di installazione



**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.

**PingFederate Setup**

### Engine Settings

Enter the ports that PingFederate will use.

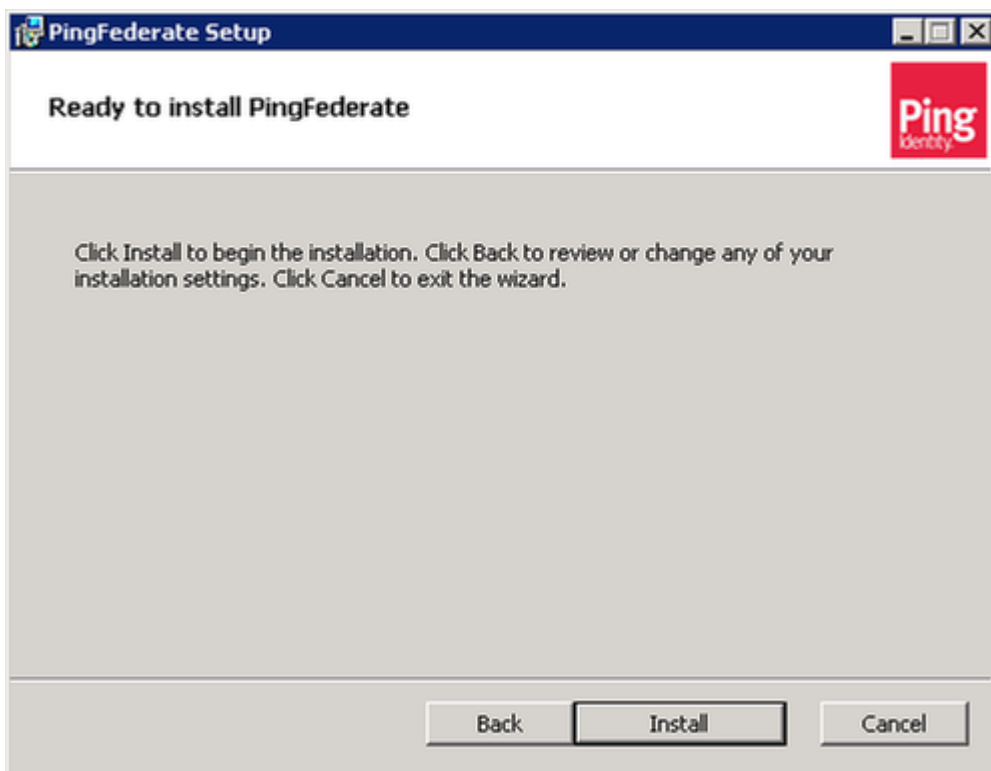
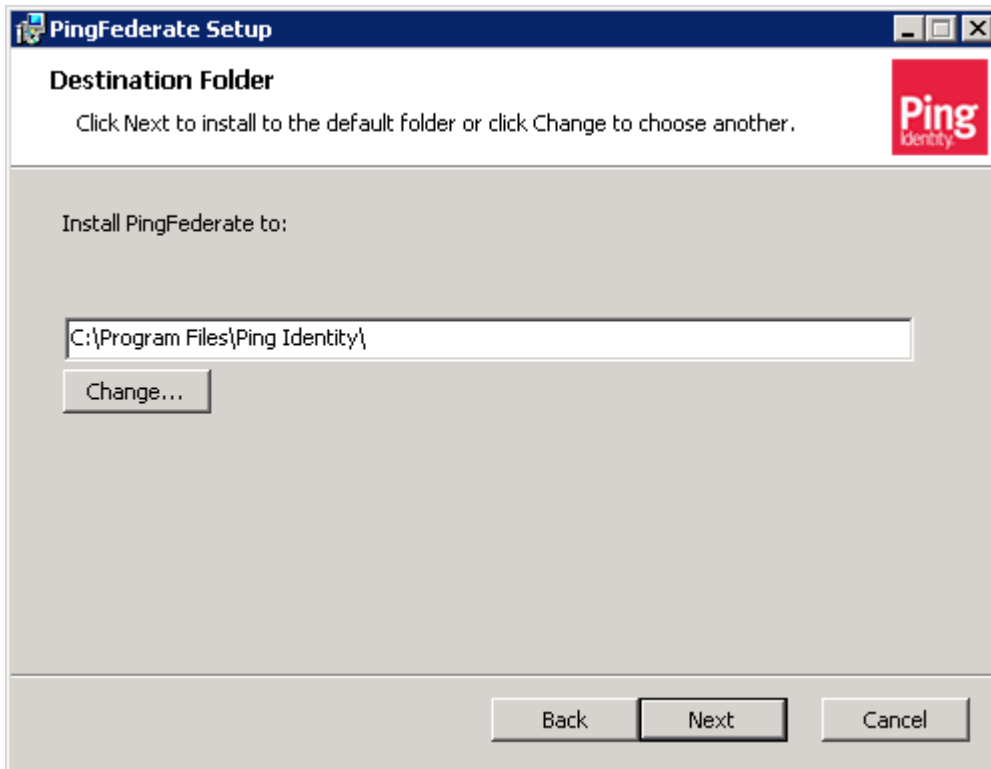


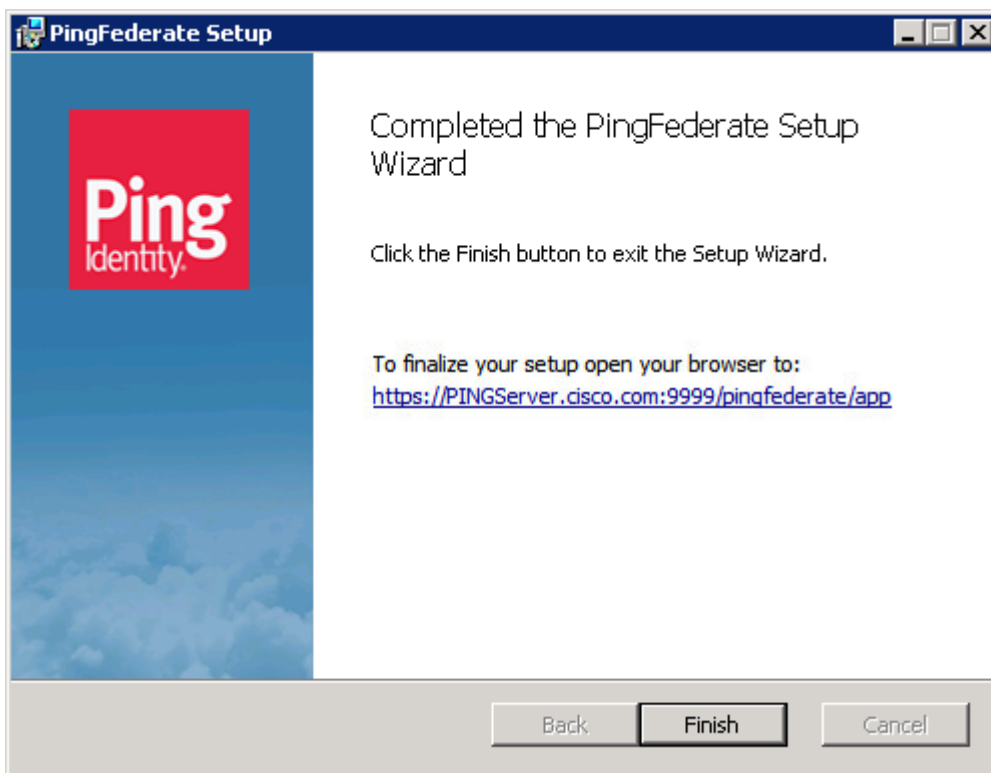
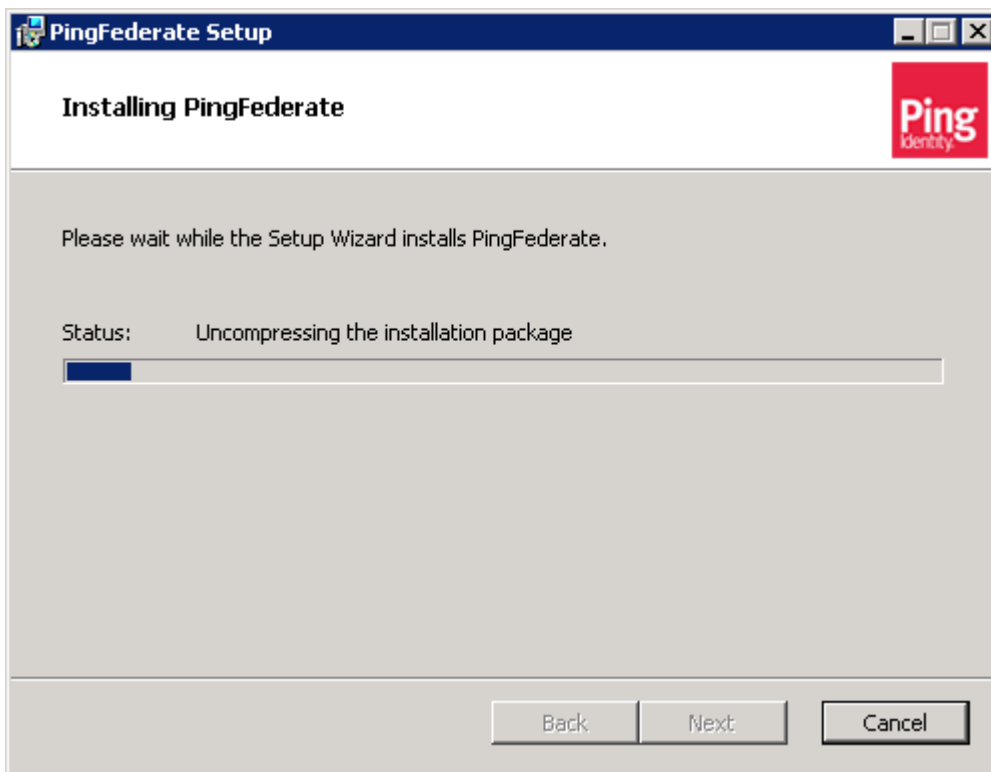
**HTTPS Port**

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.





## Avviare PingFederate per la prima volta

Se si installa PingFederate con uno dei programmi di installazione specifici della piattaforma, PingFederate viene configurato per l'esecuzione come servizio e viene avviato automaticamente al termine del processo di installazione.

Se si installa PingFederate con un file ZIP di distribuzione, eseguire lo script per avviare PingFederate manualmente.

(Windows) <pf\_install>/pingfederate/bin/run.bat  
(Unix/Linux) <pf\_install>/pingfederate/bin/run.sh

Attendi il completamento dello script - il processo di avvio viene completato quando viene visualizzato questo messaggio vicino alla fine della sequenza:

PingFederate avviato tra <X>s:<Y>ms

## Installazione guidata iniziale

L'interfaccia utente dell'amministratore di PingFederate, la console di amministrazione, è basata su un sistema di schermate di controllo simili a procedure guidate. Avviare la console di amministrazione PingFederate e utilizzare l'installazione guidata iniziale per completare la configurazione delle impostazioni di federazione delle identità. È inoltre possibile connettere PingFederate a PingOne per installare una potente soluzione ibrida in sede e basata su cloud.

Per accedere alla console di amministrazione:

Avviare il browser e passare a <https://<FQHN>.9999/pingfederate/app> (dove <FQHN> è il nome host completo del server in cui è installato PingFederate).

---

Nota: il numero di porta 9999 è impostato per default. È possibile modificare questa impostazione tramite le proprietà PingFederate.

---

## Accetta contratto di licenza

**Ping Identity** PingFederate

License Agreement

For more information on commercial licensing or support, contact Ping Sales at [sales@pingidentity.com](mailto: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

## Account PingOne

**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 © 2003-2018  
Ping Identity Corporation  
All rights reserved  
Version 11.2.2.0

## Fare clic su Avanti.

### Licenza

**Ping** PingFederate

PingOne Account License Basic Information Enable Roles Administrator Account Confirmation Complete

Please upload a valid PingFederate license file.

License File

No file selected

Choose file

Previous Next

Copyright © 2003-2018  
Ping Identity Corporation  
All rights reserved  
Version 11.2.2.0

È necessario acquistare o richiedere una licenza di sviluppo all'indirizzo pingidentity.com, caricare il file della licenza e fare clic su Avanti

## Informazioni di base

The screenshot shows the 'Basic Information' step of the PingFederate setup wizard. The breadcrumb trail includes: PingOne Account, License, **Basic Information**, Enable Roles, Administrator Account, Confirmation, and Complete! The main instruction reads: 'Welcome to PingFederate. To set up your enterprise identity bridge, let's first confirm your Base URL and Entity ID.' There are two input fields: 'BASE URL' containing 'https://pingserver.cisco.com:9031' and 'ENTITY ID' containing 'pingserver'. 'Previous' and 'Next' navigation buttons are located at the bottom right. A copyright notice at the bottom left states: 'Copyright © 2003-2018 Ping Identity Corporation. All rights reserved. Version 11.2.2.0'.

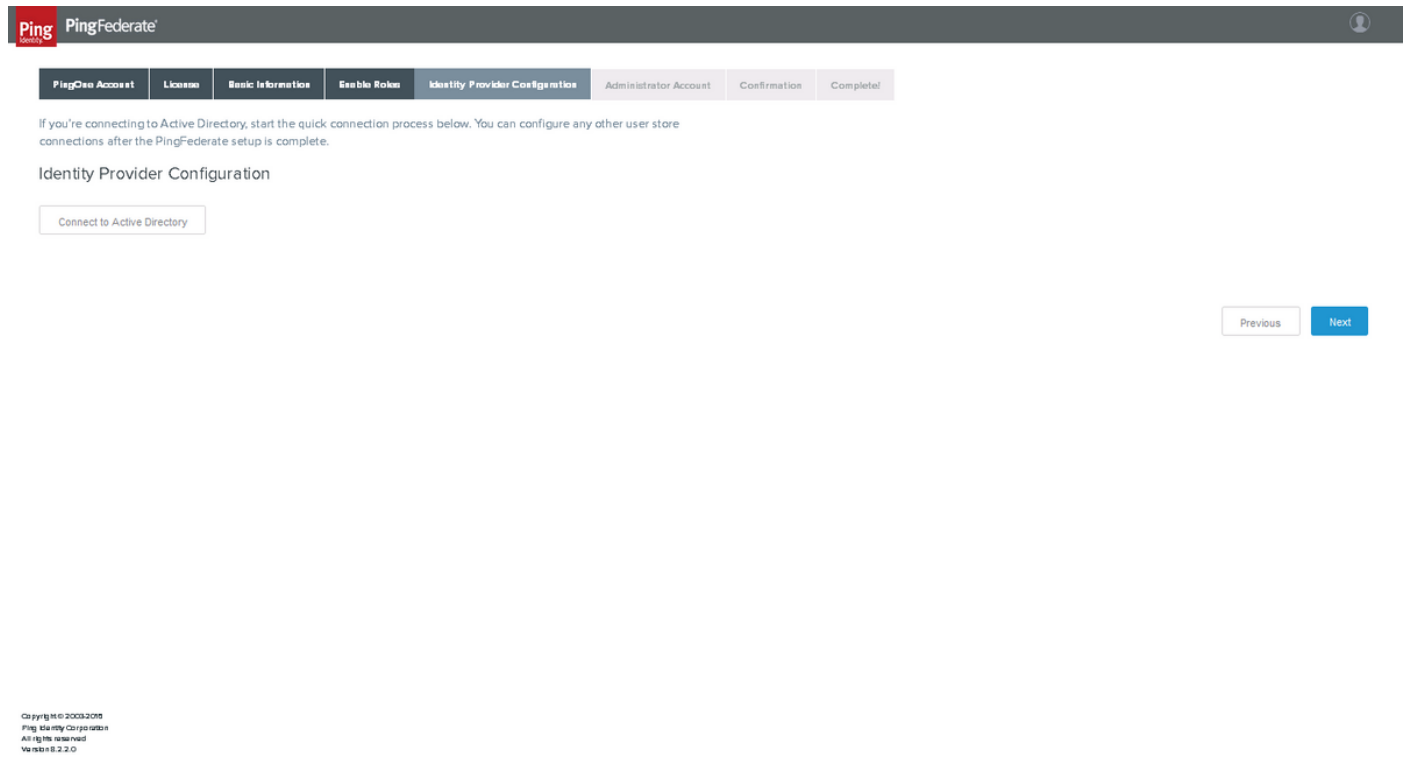
## Impostare URL BASE e ID ENTITÀ e fare clic su Avanti

### Abilita ruoli

The screenshot shows the 'Enable Roles' step of the PingFederate setup wizard. The breadcrumb trail includes: PingOne Account, License, Basic Information, **Enable Roles**, Identity Provider Configuration, Administrator Account, Confirmation, and Complete! The main instruction reads: 'Please select the roles you expect PingFederate to play.' Under the 'ROLES' section, there are three checkboxes: 'IDENTITY PROVIDER' (checked), 'SERVICE PROVIDER' (unchecked), and 'OAUTH AUTHORIZATION SERVER' (unchecked). 'Previous' and 'Next' navigation buttons are located at the bottom right. A copyright notice at the bottom left states: 'Copyright © 2003-2018 Ping Identity Corporation. All rights reserved. Version 11.2.2.0'.

## Selezionare IDENTITY PROVIDER e fare clic su Avanti

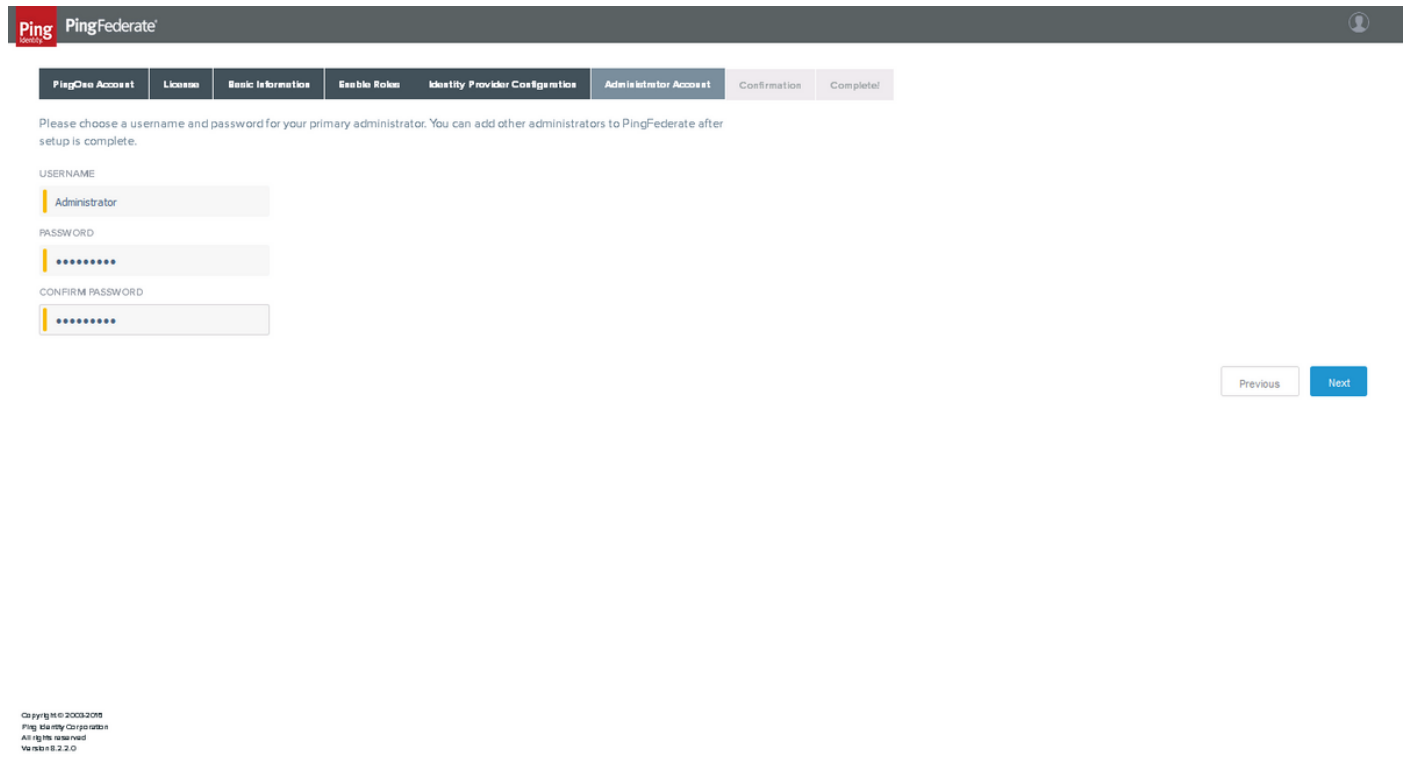
## Configurazione provider di identità



The screenshot shows the 'Identity Provider Configuration' step of the PingFederate setup wizard. The breadcrumb trail includes: PingOne Account, License, Basic Information, Enable Roles, Identity Provider Configuration, Administrator Account, Confirmation, and Complete. The main content area contains a button labeled 'Connect to Active Directory'. Below the button, there are 'Previous' and 'Next' navigation buttons. At the bottom left, there is a copyright notice: 'Copyright © 2003-2019 Ping Identity Corporation. All rights reserved. Version 8.2.2.0'.

La connessione ad Active Directory può essere eseguita in un secondo momento. Fare clic su **Avanti**


### Account amministratore



The screenshot shows the 'Administrator Account' step of the PingFederate setup wizard. The breadcrumb trail includes: PingOne Account, License, Basic Information, Enable Roles, Identity Provider Configuration, Administrator Account, Confirmation, and Complete. The main content area contains a text prompt: 'Please choose a username and password for your primary administrator. You can add other administrators to PingFederate after setup is complete.' Below this are three input fields: 'USERNAME' with the value 'Administrator', 'PASSWORD' with masked characters, and 'CONFIRM PASSWORD' with masked characters. At the bottom right, there are 'Previous' and 'Next' navigation buttons. At the bottom left, there is a copyright notice: 'Copyright © 2003-2019 Ping Identity Corporation. All rights reserved. Version 8.2.2.0'.

Impostare la password dell'amministratore e fare clic su **Avanti**

## Conferma

User icon

[PingOne Account](#) | [License](#) | [Basic Information](#) | [Enable Roles](#) | [Identity Provider Configuration](#) | [Administrator Account](#) | [Confirmation](#) | [Completed](#)

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](#)

Copyright © 2003-2018  
Ping Identity Corporation  
All rights reserved  
Version 5.2.2.0

## Confermare e fare clic su Avanti

## Completa

User icon

[PingOne Account](#) | [License](#) | [Basic Information](#) | [Enable Roles](#) | [Identity Provider Configuration](#) | [Administrator Account](#) | [Confirmation](#) | [Completed](#)

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](#)

Copyright © 2003-2018  
Ping Identity Corporation  
All rights reserved  
Version 5.2.2.0

## Fare clic su Fine

# Configura federazione ping

## Configurazione server

The screenshot shows the PingFederate web interface. The top navigation bar includes the PingFederate logo and a user profile icon. A sidebar on the left contains a menu with 'MAIN', 'IdP Configuration', and 'Server Configuration' (which is selected). The main content area is titled 'Server Configuration' and features a 'License Warning: Approaching expiration date' banner. Below this, the page is organized into three columns: 'SYSTEM SETTINGS' (with links for Server Settings, Connect to PingOne, Data Stores, and Redirect Validation), 'ADMINISTRATIVE FUNCTIONS' (with links for Metadata Export, XML File Signatures, Configuration Archive, Account Management, License Management, and Virtual Host Names), 'CERTIFICATE MANAGEMENT' (with links for Trusted CAs, SSL Server Certificates, SSL Client Keys & Certificates, Signing & Decryption Keys & Certificates, Certificate Revocation Checking, and Metadata URLs), and 'AUTHENTICATION' (with links for Application Authentication, Password Credential Validators, and Active Directory Domains/Kerberos Realms). A footer at the bottom left contains copyright information for Ping Identity Corporation, version 8.2.2.0.

Chiavi e certificati di decrittografia XML (Digital Signing and Extensible Markup Language)

Fare clic su Configurazione server > Gestione certificati > Firma e certificati XML

The screenshot shows the PingFederate web interface for Certificate Management. The top navigation bar and sidebar are consistent with the previous screenshot. The main content area is titled 'Certificate Management' and includes a 'License Warning: Approaching expiration date' banner. Below the banner, there is a descriptive paragraph: 'Establish and maintain your server's signing certificates, which may be used to sign assertions, security tokens, requests, and responses. These certificates may also be used for decryption.' A table with the following columns is displayed: 'Serial', 'Subject DN', 'Expires', 'Key Details', 'Status', and 'Action'. Below the table, there are two buttons: 'Create New' and 'Import'. At the bottom right of the page, there are 'Cancel' and 'Save' buttons.

Fare clic su Crea nuovo

Crea certificato

Ping Identity PingFederate

License Warning: Approaching expiration date

MAIN

- IdP Configuration
- Server Configuration

### Certificate Management | Create Certificate

Create Certificate Summary

Create a new Certificate and Private Key.

COMMON NAME: SSO

ORGANIZATION: CISCO

ORGANIZATIONAL UNIT: CBABU

CITY: Bangalore

STATE: Karnataka

COUNTRY: IN

VALIDITY (DAYS): 365

KEY ALGORITHM: RSA

KEY SIZE (BITS): 2048

SIGNATURE ALGORITHM: RSA SHA256

Cancel Next

Copyright © 2008-2018 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

Fare clic su Avanti.

Esporta certificato

Ping Identity PingFederate

License Warning: Approaching expiration date

MAIN

- IdP Configuration
- Server Configuration

### Certificate Management | Export Certificate

Export Certificate Export & Summary

You have a choice of exporting the certificate and the key or just the certificate.

CERTIFICATE ONLY

CERTIFICATE AND PRIVATE KEY

Esportazione e riepilogo

Ping Federate

License Warning: Approaching expiration date

MAIN

IdP Configuration

Server Configuration

### Certificate Management | Export Certificate

Export Certificate | Export & Summary

Click the Export button to export this certificate to the file system.

Export Certificate	
Subject DN	CN=SSO, OU=CBABU, O=CISCO, L=Bengalore, ST=Karnataka, CHN
Issuer DN	CN=SSO, OU=CBABU, O=CISCO, L=Bengalore, ST=Karnataka, CHN
Serial Number	015867 E2988D
Expires	Wed Nov 15 17:37:33 IST 2017

Export

Cancel Previous Done

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

Fare clic su Esporta

Archivi dati

Fare clic su Configurazione server > IMPOSTAZIONI DI SISTEMA > Archivi dati

Ping Federate

License Warning: Approaching expiration date

MAIN

IdP Configuration

Server Configuration

### Manage Data Stores

Manage data store definitions for use with attribute lookups.

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

Add New Data Store

Cancel Save

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

Fare clic su Aggiungi nuovo archivio dati

## Configurazione LDAP

**PingFederate**

License Warning: Approaching expiration date

### Manage Data Stores | Data Store

Data Store Type | LDAP Configuration | Summary

Please select a type of data store.

DATABASE

LDAP

CUSTOM

Cancel Next

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

## Scegliere LDAP e fare clic su Avanti

**PingFederate**

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) 10.78.93.148:389

LDAP TYPE Active Directory

BIND ANONYMOUSLY

USER DN cn=Administrator,cn=u

PASSWORD

USE LDAPS

MASK VALUES IN LOG

Advanced

Cancel Previous Next

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

## Immettere i valori e fare clic su Avanti

## Riepilogo

The screenshot shows the PingFederate Admin Console interface. At the top, there is a 'License Warning: Approaching expiration date' banner. Below it, 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. Below the tabs, there is a heading 'Data Store' and a sub-heading 'Data Store Type'. The configuration details are as follows:

Property	Value
Type of Data Store	LDAP
<b>LDAP Configuration</b>	
Hostname(s)	10.78.93.148:389
Username	cn=Administrator,cn=users,dc=cisco,dc=com

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

Copyright © 2008-2018 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

Fare clic su Save (Salva) dopo la verifica.

Convalide credenziali password

Fare clic su Configurazione server > AUTENTICAZIONE > Convalide credenziali password

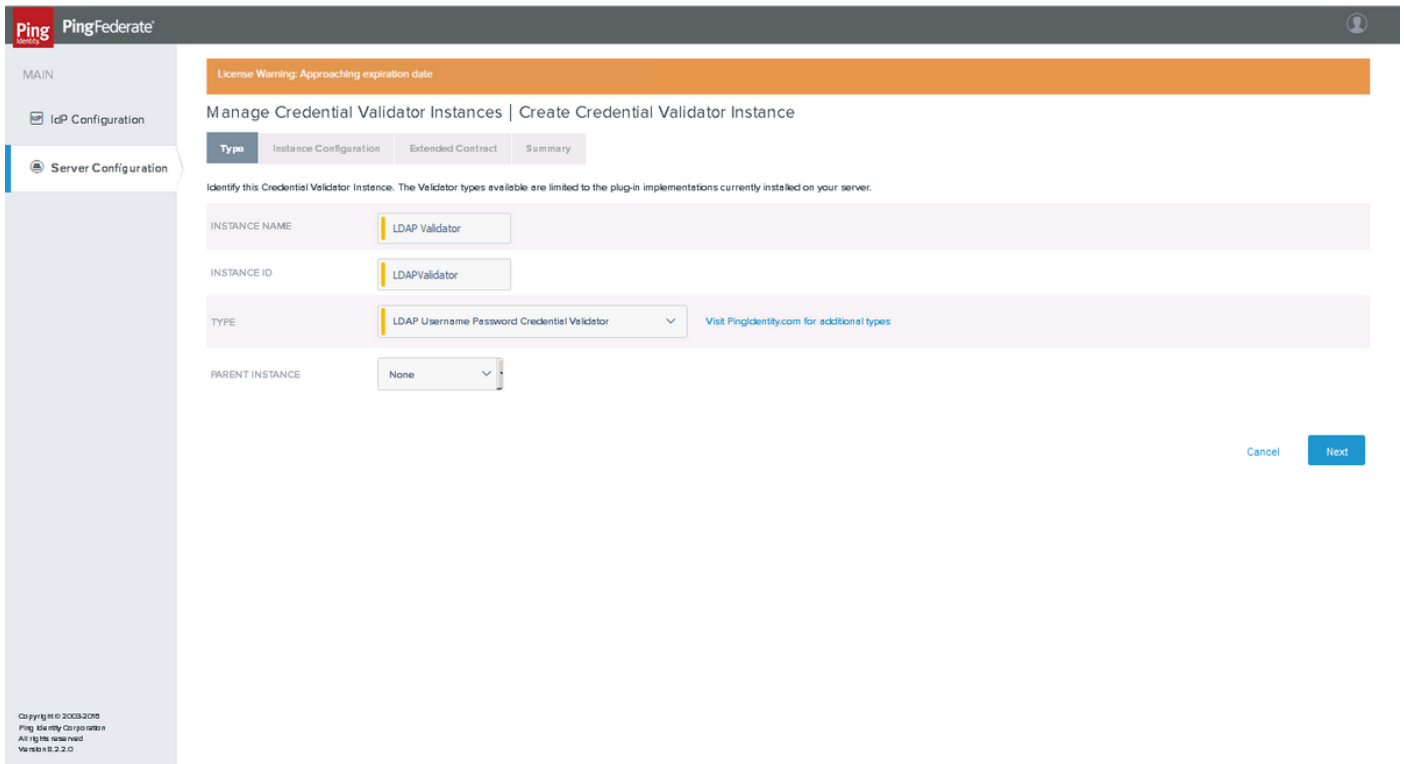
The screenshot shows the PingFederate Admin Console interface. At the top, there is a 'License Warning: Approaching expiration date' banner. Below it, the page title is 'Manage Credential Validator Instances'. There is a descriptive paragraph: 'Credential Validators are plug-ins used to verify username and password pairs in various contexts throughout the system. The actual application of a Validator instance must be configured in the appropriate context as needed (e.g., OAuth Resource Owner Credentials Mapping)'. Below the text, there is a table with the following columns: 'Instance Name', 'Instance Id', 'Type', 'Parent Name', and 'Action'. There is a 'Create New Instance' button below the table. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Instance Name	Instance Id	Type	Parent Name	Action
---------------	-------------	------	-------------	--------

Copyright © 2008-2018 Ping Identity Corporation. All rights reserved. Version 8.2.2.0

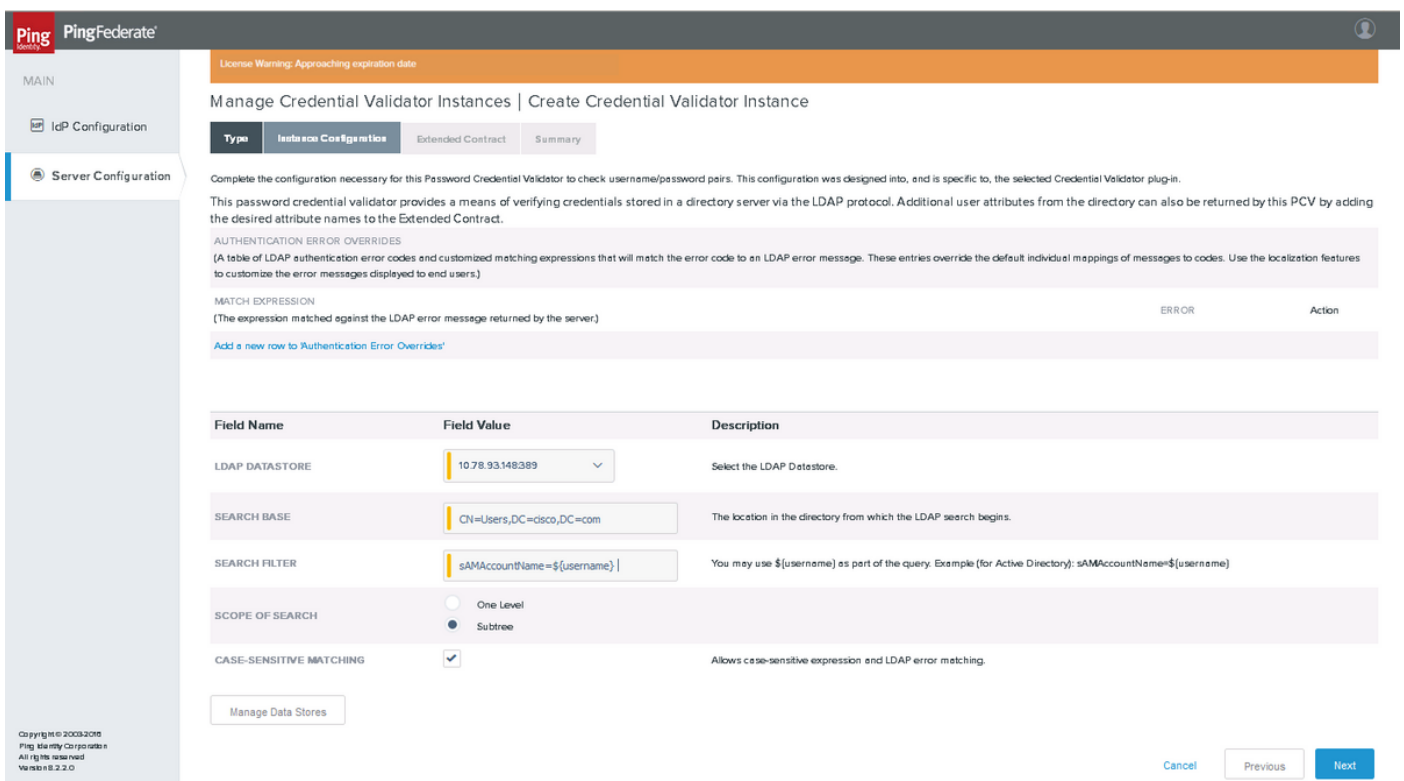
Fate clic su Crea nuova variante (Create New Instance).

Tipo



Selezionare Convalida credenziali password nome utente LDAP come TYPE. Fare clic su Next (Avanti).

### Configurazione istanza



Selezionare l'archivio dati LDAP e immettere la base di ricerca, il filtro di ricerca e l'ambito di ricerca. Fare clic su Next (Avanti).

## Contratto esteso

The screenshot shows the 'Create Credential Validator Instance' page in PingFederate. At the top, there is a license warning: 'License Warning: Approaching expiration date'. Below this, the page title is 'Manage Credential Validator Instances | Create Credential Validator Instance'. There are four tabs: 'Type', 'Instance Configuration', 'Extended Contract', and 'Summary'. The 'Extended Contract' tab is active. The text below the tabs reads: 'You can extend the attribute contract of this Password Credential Validator instance.' Under the heading 'Core Contract', there are three input fields for 'DN', 'givenName', and 'mail'. Below these is a section titled 'Extend the Contract' with an 'Add' button. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons. The footer contains copyright information: 'Copyright © 2003-2016 Ping Identity Corporation. All rights reserved. Version 8.2.2.0'.

## Fare clic su Avanti.

## Riepilogo

The screenshot shows the 'Create Credential Validator Instance' page in PingFederate, specifically the 'Summary' tab. At the top, there is a license warning: 'License Warning: Approaching expiration date'. Below this, the page title is 'Manage Credential Validator Instances | Create Credential Validator Instance'. There are four tabs: 'Type', 'Instance Configuration', 'Extended Contract', and 'Summary'. The 'Summary' tab is active. The text below the tabs reads: 'Password Credential Validator configuration summary.' Under the heading 'Create Credential Validator Instance', there is a table with the following data:

Type	
Instance Name	LDAP Validator
Instance Id	LDAPValidator
Type	LDAP Username Password Credential Validator
Class Name	org.sourceid.sem120.domain.LDAPUsernamePasswordCredentialValidator
Parent Instance Name	None

Below the table, there is a section titled 'Instance Configuration' with the following data:

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

Below this, there is a section titled 'Extended Contract' with the following data:

Attribute	mail
Attribute	givenName
Attribute	DN
Attribute	username

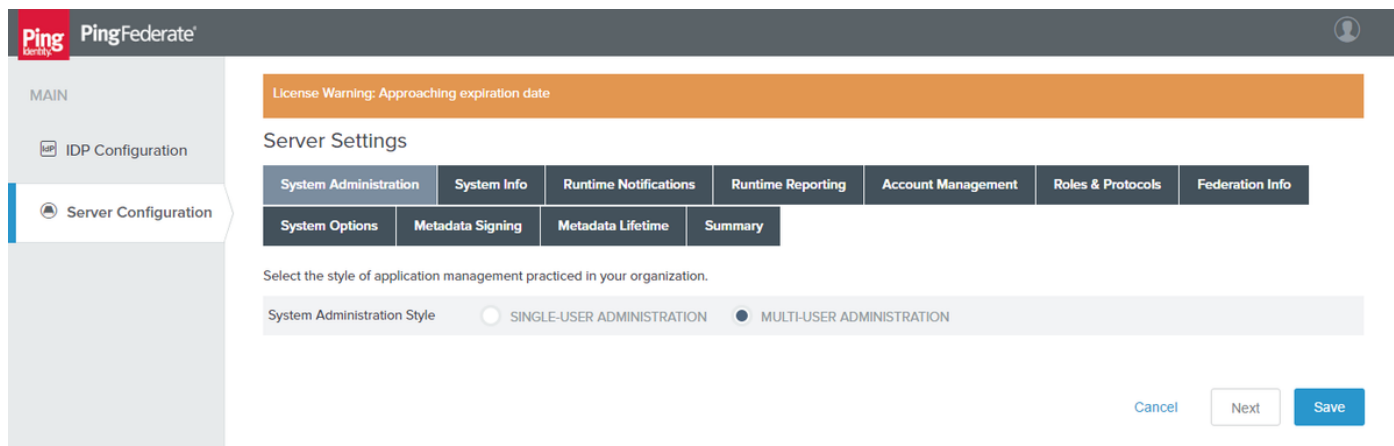
At the bottom right, there are 'Cancel', 'Previous', and 'Done' buttons. The footer contains copyright information: 'Copyright © 2003-2016 Ping Identity Corporation. All rights reserved. Version 8.2.2.0'.

## Verificate le impostazioni e fate clic su Fine (Done).

## Impostazioni server

### Amministrazione del sistema

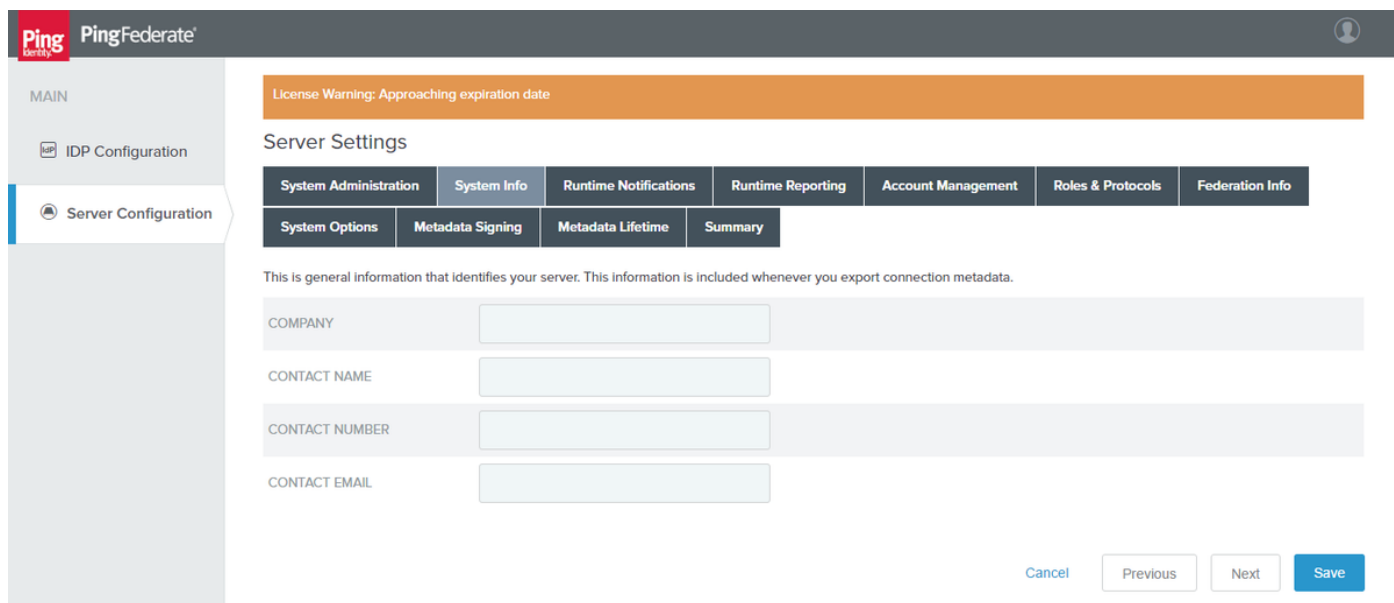
Fare clic su Configurazione server > IMPOSTAZIONI DI SISTEMA > Impostazioni server



The screenshot shows the PingFederate administration interface. At the top left is the PingFederate logo. A navigation menu on the left includes 'MAIN', 'IDP Configuration', and 'Server Configuration'. The main content area is titled 'Server Settings' and contains a 'License Warning: Approaching expiration date' banner. Below the banner are 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 'System Administration' tab is active. Below the tabs, there is a section for 'System Administration Style' with two radio buttons: 'SINGLE-USER ADMINISTRATION' (unselected) and 'MULTI-USER ADMINISTRATION' (selected). At the bottom right, there are 'Cancel', 'Next', and 'Save' buttons.

Fare clic su Next (Avanti).

### Informazioni sul sistema



The screenshot shows the PingFederate administration interface for system information. The navigation menu on the left is the same as in the previous screenshot. The main content area is titled 'Server Settings' and contains the same 'License Warning' banner. Below the banner are the same tabs as in the previous screenshot. The 'System Info' tab is active. Below the tabs, there is a section for 'System Information' with the text: 'This is general information that identifies your server. This information is included whenever you export connection metadata.' Below this text are four input fields: 'COMPANY', 'CONTACT NAME', 'CONTACT NUMBER', and 'CONTACT EMAIL'. At the bottom right, there are 'Cancel', 'Previous', 'Next', and 'Save' buttons.

Fare clic su Next (Avanti).

### Notifiche di runtime

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

Fare clic su Next (Avanti).

Report runtime

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

Fare clic su Next (Avanti).

Gestione account

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"/>	<input checked="" type="checkbox"/>	Deactivate   <a href="#">Change Password</a>

Create User

NOTIFY USER OF PASSWORD CHANGE

Cancel Previous Next Save

Fare clic su Next (Avanti).

Nota: in questa sezione è possibile aggiungere o modificare la password dell'utente.

## Ruoli e protocolli

The screenshot shows the PingFederate administration interface. The left sidebar has 'Server Configuration' selected. The main content area is titled 'Server Settings' and has a tab for 'Roles & Protocols'. A license warning banner is at the top. Below the tabs, there are several checkboxes for enabling roles and protocols. The 'ENABLE IDENTITY PROVIDER (IDP) ROLE AND SUPPORT THE FOLLOWING:' section is checked, with 'SAML 2.0' also checked. Other options like 'ENABLE OAUTH 2.0 AUTHORIZATION SERVER (AS) ROLE', 'SAML 1.1', 'SAML 1.0', 'WS-FEDERATION', 'OUTBOUND PROVISIONING', 'WS-TRUST', 'ENABLE SERVICE PROVIDER (SP) ROLE AND SUPPORT THE FOLLOWING:', and 'ENABLE IDP DISCOVERY ROLE (SAML 2.0 ONLY)' are unchecked. At the bottom right, there are buttons for 'Cancel', 'Previous', 'Next', and 'Save'.

Copyright © 2003-2016 Ping Identity Corporation

Selezionare i ruoli e i protocolli appropriati. Fare clic su Next (Avanti).

## Informazioni federazione

The screenshot shows the PingFederate administration interface. The left sidebar has 'Server Configuration' selected. The main content area is titled 'Server Settings' and has a tab for 'Federation Info'. A license warning banner is at the top. Below the tabs, there is a 'Summary' section with a text box for 'BASE URL' containing 'https://pingserver.cisco.com:9031' and a text box for 'SAML 2.0 ENTITY ID' containing 'pingserver'. At the bottom right, there are buttons for 'Cancel', 'Previous', 'Next', and 'Save'.

Fare clic su Next (Avanti).

## Opzioni di sistema

Ping Identity PingFederate

License Warning: Approaching expiration date

MAIN

- IDP Configuration
- Server Configuration

### 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](#)

Fare clic su Next (Avanti).

Firma metadati

Ping Identity PingFederate

License Warning: Approaching expiration date

MAIN

- IDP Configuration
- Server Configuration

### 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](#)

Selezionare il certificato di firma e l'algoritmo di firma creato in precedenza come parte della configurazione del certificato. Fare clic su Next (Avanti).

Durata metadati

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

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

Fare clic su Next (Avanti).

Riepilogo

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

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

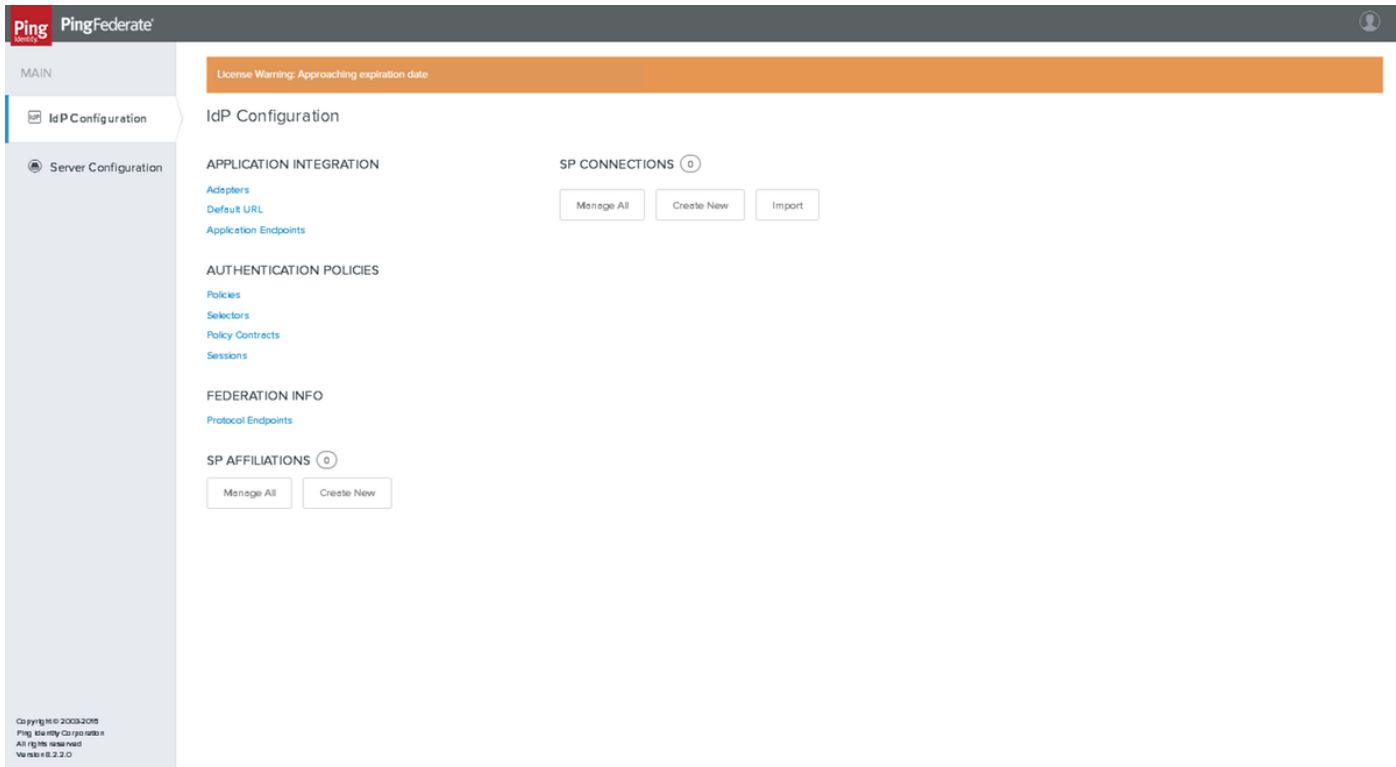
Username

Retry Attempt 2

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

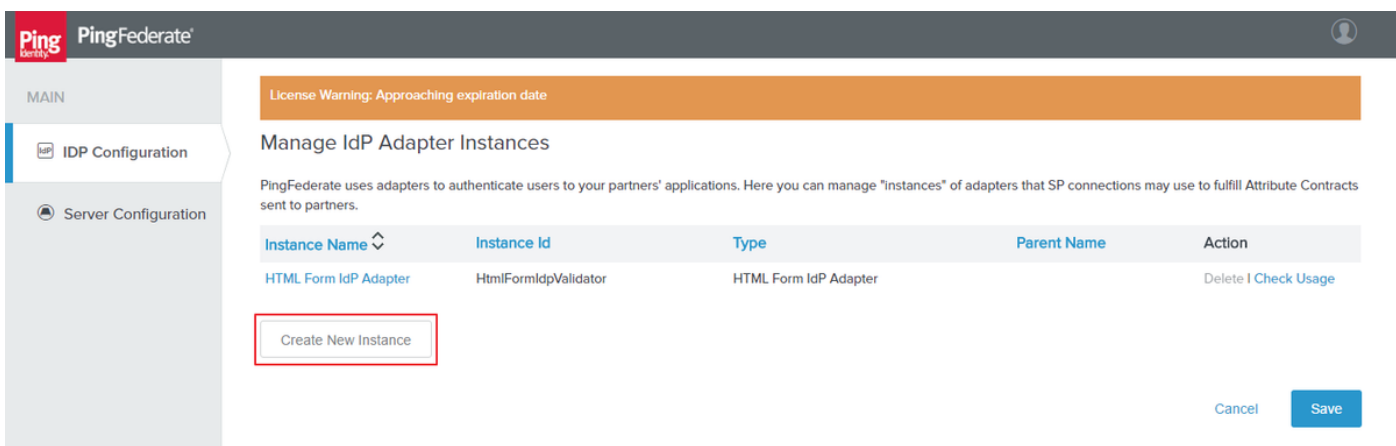
Verificare le impostazioni e fare clic su Salva.

Configurazione provider di identità



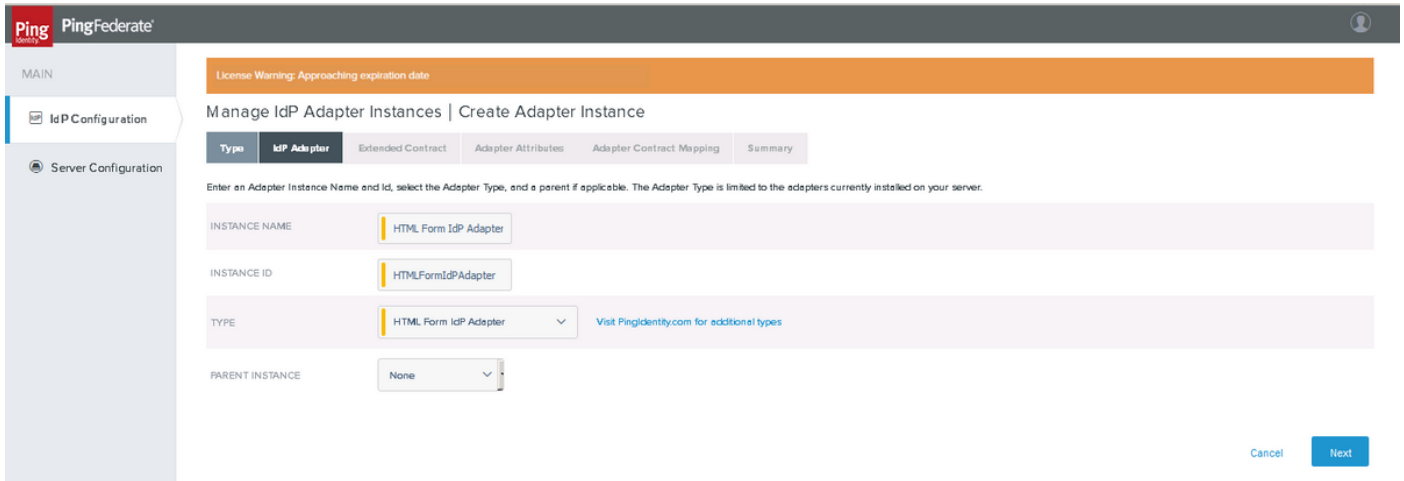
## Adattatori

Fare clic su IdP Configuration > APPLICATION INTEGRATION > Adapters



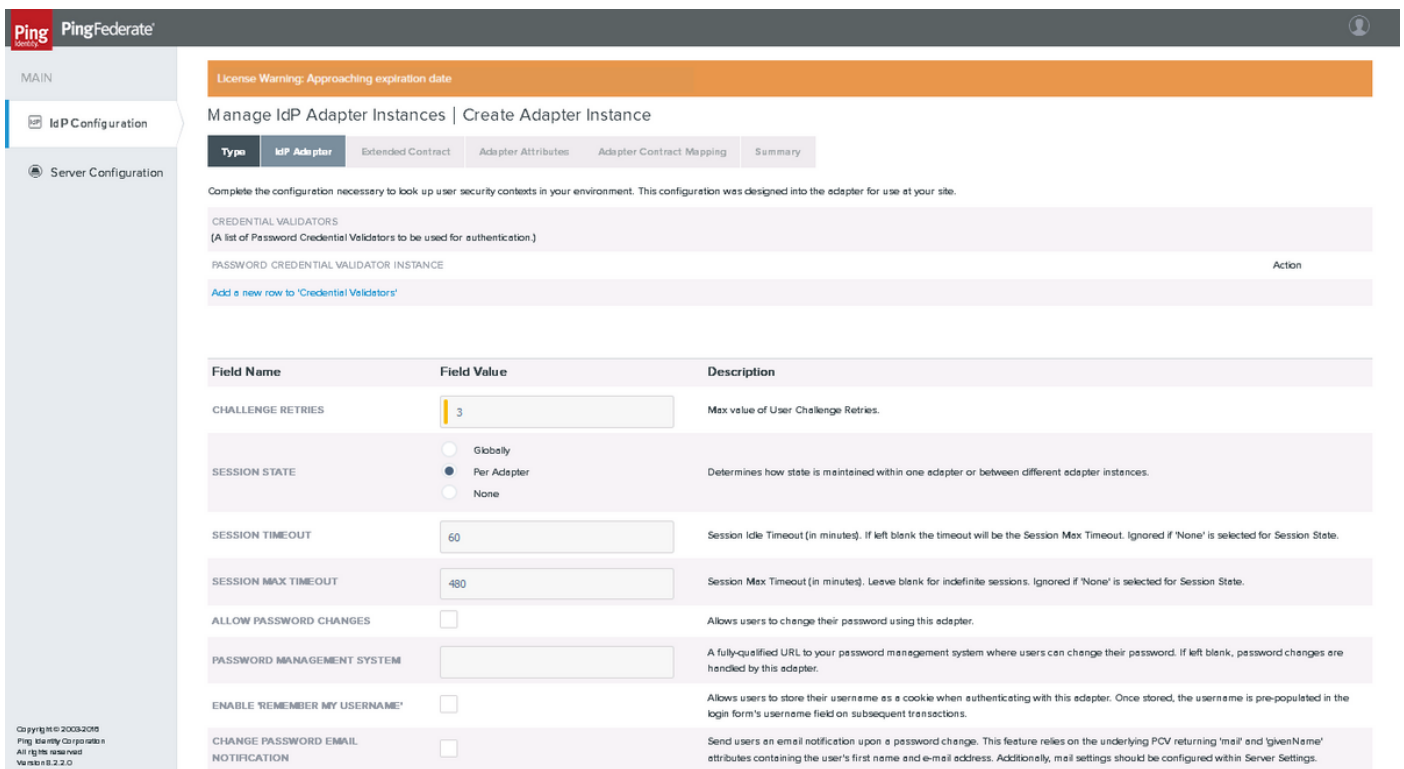
Fate clic su Crea nuova variante (Create New Instance).

Tipo



Scegliere HTML Form IDP Adapter. Fare clic su Next (Avanti).

### Adattatore IDP



Fare clic su Aggiungi una nuova riga a 'Convalida credenziali' e selezionare la Convalida LDAP creata in precedenza come ISTANZA CONVALIDA CREDENZIALI PASSWORD e fare clic su Aggiorna. Fare clic su Avanti.

### Contratto esteso

Ping Federate

License Warning: Approaching expiration date

Manage IdP Adapter Instances | Create Adapter Instance

Type | IdP Adapter | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

This adapter type supports the creation of an Extended Adapter Contract after initial deployment of the adapter instance. This Adapter Contract may be used to fulfill the Attribute Contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.

**Core Contract**

username

**Extend the Contract**      **Action**

email	<a href="#">Edit</a>   <a href="#">Delete</a>
firstname	<a href="#">Edit</a>   <a href="#">Delete</a>
lastname	<a href="#">Edit</a>   <a href="#">Delete</a>
uid	<a href="#">Edit</a>   <a href="#">Delete</a>
updatetimestamp	<a href="#">Edit</a>   <a href="#">Delete</a>
user_principal	<a href="#">Edit</a>   <a href="#">Delete</a>

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

Aggiungere i contratti come illustrato. Fare clic su Next (Avanti).

Attributi adattatore

Ping Federate

License Warning: Approaching expiration date

Manage IdP Adapter Instances | Create Adapter Instance

Type | IdP Adapter | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

Attribute	Pseudonym	Mask Log Values
email	<input checked="" type="checkbox"/>	<input type="checkbox"/>
firstname	<input checked="" type="checkbox"/>	<input type="checkbox"/>
lastname	<input checked="" type="checkbox"/>	<input type="checkbox"/>
uid	<input checked="" type="checkbox"/>	<input type="checkbox"/>
updatetimestamp	<input checked="" type="checkbox"/>	<input type="checkbox"/>
user_principal	<input checked="" type="checkbox"/>	<input type="checkbox"/>
username	<input checked="" type="checkbox"/>	<input type="checkbox"/>

MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES

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

Fare clic su Next (Avanti).

Mapping contratto scheda

The screenshot shows the 'Configure Adapter Contract' step in the PingFederate interface. The breadcrumb trail is 'Manage IdP Adapter Instances | Create Adapter Instance'. The current step is 'Adapter Contract Mapping', with other steps being 'Type', 'IdP Adapter', 'Extended Contract', 'Adapter Attributes', and 'Summary'. A license warning banner is at the top. Below the breadcrumb, there is explanatory text: '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 navigation buttons: 'Cancel', 'Previous', 'Next', and 'Done'.

Fare clic su Configura contratto scheda.

Origini attributi e ricerca utente

The screenshot shows the 'Adapter Contract Mapping' step in the PingFederate interface. The breadcrumb trail is 'Manage IdP Adapter Instances | Create Adapter Instance | Adapter Contract Mapping'. The current step is 'Adapter Contract Mapping', with other steps being 'Attribute Sources & User Lookup', 'Adapter Contract Fulfillment', 'Issuance Criteria', and 'Summary'. A license warning banner is at the top. Below the breadcrumb, there is explanatory text: '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 text 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 navigation buttons: 'Cancel', 'Next', and 'Done'.

Aggiungere un'origine attributo e selezionare l'archivio LDAP creato in precedenza. Fare clic su Next (Avanti).

Adeguamento esecuzione contratto

PingFederate

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

Mappare gli attributi. Fare clic su Next (Avanti).

Criteri di rilascio

PingFederate

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

Fare clic su Next (Avanti).

Riepilogo

**LDAP Directory Search**

Data Store	10.78.93.148:389
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)
-----------	--------

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

Cancel Previous Done

Verificate le impostazioni e fate clic su Fine (Done).

## Connessioni SP

### Creazione di nuove connessioni SP

#### Tipo di connessione

**License Warning: Approaching expiration date**

**SP Connection**

CONNECTION TYPE: **Browser SSO Profiles** | CONNECTION OPTIONS: **Browser SSO Profiles** | IMPORT METADATA: **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

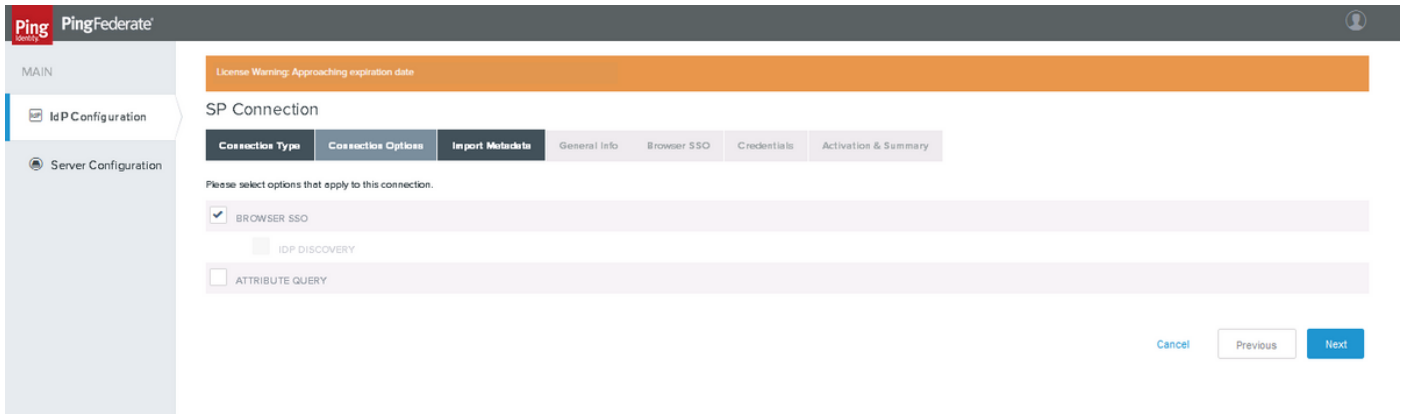
WS-TRUST STS

OUTBOUND PROVISIONING

Cancel Next

Fare clic su Next (Avanti).

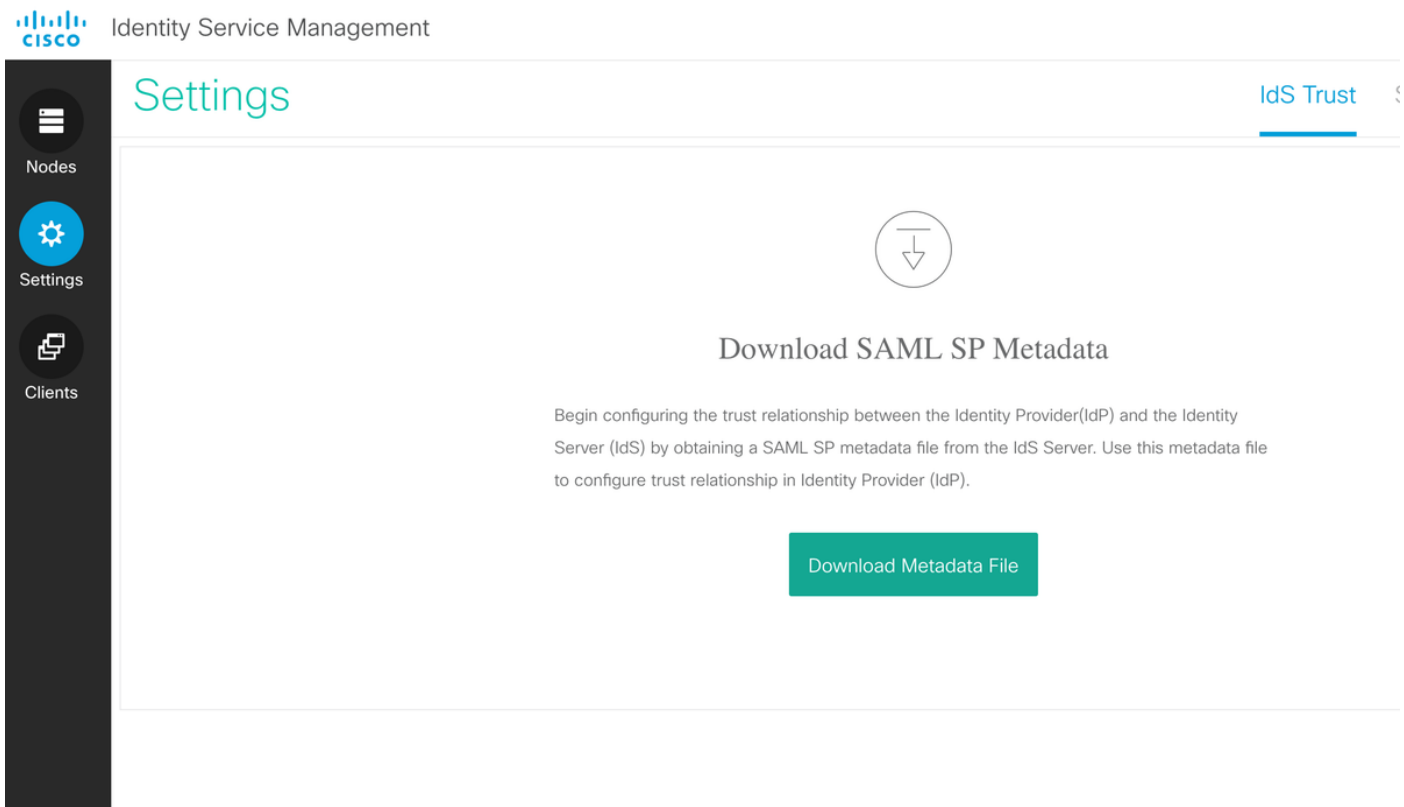
#### Opzioni di connessione



Fare clic su Avanti.

Importa metadati

Scarica il file xml dei metadati del provider di servizi da Cisco Identity Service Admin > Impostazioni > Attendibilità IdS > Scarica metadati



Caricare il file XML dei metadati del provider di servizi in PingFederate.

The screenshot shows the 'SP Connection' configuration page in PingFederate, specifically the 'Import Metadata' tab. At the top, there is a license warning: 'License Warning: Approaching expiration date'. Below this, the page title is 'SP Connection'. There are several tabs: 'Connection Type', 'Connection Options', 'Import Metadata' (active), 'General Info', 'Browser SSO', 'Credentials', and 'Activation & Summary'. A text block explains: 'To populate many connection settings automatically, you can upload the partner's metadata file, or specify a URL where PingFederate can download it. To periodically reload the connection settings from the URL, select Enable Automatic Reloading.' Below this, there are radio buttons for 'METADATA' with options 'NONE', 'FILE' (selected), and 'URL'. A file input field contains 'sp.xml' and a 'Choose file' button. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

Scegliere il file xml scaricato e fare clic su Avanti

Riepilogo metadati

The screenshot shows the 'SP Connection' configuration page in PingFederate, specifically the 'Metadata Summary' tab. The page title is 'SP Connection'. The tabs are: 'Connection Type', 'Connection Options', 'Import Metadata', 'Metadata Summary' (active), 'General Info', 'Browser SSO', 'Credentials', and 'Activation & Summary'. A text block says: 'Use the information below to evaluate the authenticity of the imported metadata.' Below this, there is a table with two rows: 'Entity Id' with the value 'UCCX-SA1.cisco.com' and 'Metadata Signature Status' with the value 'unsigned'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

Fare clic su Avanti.

Informazioni generali

The screenshot shows the 'SP Connection' configuration page in PingFederate, specifically the 'General Info' tab. The page title is 'SP Connection'. The tabs are: 'Connection Type', 'Connection Options', 'Import Metadata', 'Metadata Summary', 'General Info' (active), 'Browser SSO', 'Credentials', and 'Activation & Summary'. A text block explains: 'This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain-language identifier for this connection. Optionally, you can specify multiple virtual server IDs for your own server to use when communicating with this partner. If set, these virtual server IDs will be used in place of the unique protocol identifier configured for your server in Server Settings. The Base URL may be used to simplify configuration of partner endpoints.' Below this, there are several input fields: 'PARTNER'S ENTITY ID (CONNECTION ID)' with value 'UCCX-SA1.cisco.com', 'CONNECTION NAME' with value 'UCCX-SA1.cisco.com', 'VIRTUAL SERVER IDS' with an 'Add' button, 'BASE URL' with value 'https://UCCX-SA1.cisco.com:8553', 'COMPANY', 'CONTACT NAME', 'CONTACT NUMBER', 'CONTACT EMAIL', 'APPLICATION NAME', and 'APPLICATION ICON URL'. At the bottom, there are radio buttons for 'LOGGING MODE' with options 'NONE', 'STANDARD' (selected), 'ENHANCED', and 'FULL'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

Fare clic su Avanti.

## SSO browser

The screenshot shows the PingFederate interface for configuring an SP Connection. The left sidebar contains 'MAIN', 'IdP Configuration', and 'Server Configuration'. The main content area has a 'License Warning: Approaching expiration date' banner. Below it, the 'SP Connection' title is followed by a breadcrumb trail: 'Connection Type', 'Connection Options', 'Import Metadata', 'Metadata Summary', 'General Info', 'Browser SSO', 'Credentials', and 'Activation & Summary'. The 'Browser SSO' tab is active. A text block explains that this task provides connection-endpoint and other configuration information for secure browser-based SSO. Below this is a 'BROWSER SSO CONFIGURATION' section with a 'Configure Browser SSO' button. At the bottom right, there are 'Cancel', 'Save Draft', 'Previous', and 'Next' buttons.

Fare clic su Configura SSO browser

## Profili SAML (Security Assertion Markup Language)

The screenshot shows the 'SAML Profiles' tab within the 'Browser SSO' configuration. The breadcrumb trail is 'SAML Profiles', 'Assertion Lifetime', 'Assertion Creation', 'Protocol Settings', and 'Summary'. A text block explains that a SAML Profile defines message exchange between an IdP and a Service Provider. Below this are two sections: 'Single Sign-On (SSO) Profiles' and 'Single Logout (SLO) Profiles'. Under SSO, 'IDP-INITIATED SSO' and 'SP-INITIATED SSO' are both checked. Under SLO, 'IDP-INITIATED SLO' and 'SP-INITIATED SLO' are unchecked. At the bottom right, there are 'Cancel', 'Save Draft', and 'Next' buttons.

Fare clic su Avanti.

Nota: Il logout singolo (SLO) non è supportato da Cisco Identity Service (IdS) nella versione 11.6 e non è selezionato.

## Durata asserzione

The screenshot shows the 'Assertion Creation' tab within the 'Browser SSO' configuration. The breadcrumb trail is 'SAML Profiles', 'Assertion Lifetime', 'Assertion Creation', 'Protocol Settings', and 'Summary'. A text block explains that when an assertion is issued to the SP, there is a timeframe of validity before and after issuance. Below this are two input fields: 'MINUTES BEFORE' with a value of 5, and 'MINUTES AFTER' with a value of 5. At the bottom right, there are 'Cancel', 'Previous', 'Next', 'Done', and 'Save' buttons.

Fare clic su Avanti.

Creazione di asserzioni

The screenshot shows the 'Assertion Creation' step in the 'Browser SSO' configuration. The page has a left sidebar with 'IDP Configuration' and 'Server Configuration'. The main content area has a breadcrumb 'SP Connection | Browser SSO' and a tabbed interface with 'Assertion Creation' selected. Below the tabs is a table for 'Assertion Configuration' with the following data:

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

At the bottom of the configuration area, a button labeled 'Configure Assertion Creation' is highlighted with a red box. To the right of the configuration area are navigation buttons: 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

Fare clic su Configura creazione asserzioni

Mapping identità

The screenshot shows the 'Identity Mapping' step in the 'Browser SSO' configuration. The page has a left sidebar with 'IDP Configuration' and 'Server Configuration'. The main content area has a breadcrumb 'SP Connection | Browser SSO | Assertion Creation' and a tabbed interface with 'Identity Mapping' selected. Below the tabs is a text description: 'Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the SP. Select the type of name identifier that you will send to the SP. Your selection may affect the way that the SP will look up and associate the user to a specific local account.'

There are three radio button options:

- 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.

At the bottom right of the configuration area are navigation buttons: 'Cancel', 'Next', 'Done', and 'Save'.

Fare clic su Avanti.

Contratto attributo

← → ↻ ⚠ Not Secure https://pingserver.cisco.com:9999/pingfederate/app ☆ 📄 🗄

**Ping** PingFederate

MAIN

- IdP Configuration
- Server Configuration

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	<a href="#">Edit</a> <a href="#">Delete</a>
SAML_NAME_FORMAT	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	<a href="#">Edit</a> <a href="#">Delete</a>
uid	urn:oasis:names:tc:SAML:2.0:attrname-format:uri	<a href="#">Edit</a> <a href="#">Delete</a>
user_principal	urn:oasis:names:tc:SAML:2.0:attrname-format:uri	<a href="#">Edit</a> <a href="#">Delete</a>

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

Copyright © 2003-2016 Ping Identity Corporation

Avviso: Questi attributi sono obbligatori per l'interoperabilità di Cisco Identity Service (IdS) con PingFederate.

Contratto attributo	Scopo
SAML_OGGETTO	Utilizzato dal filtro di ricerca PingFederate per verificare se il valore mappato è soddisfatto
SAML_AUTHN_CTX	Utilizzato nella risposta SAML per indicare il contesto di autenticazione 'PasswordProtectedTransport'
FORMATO_NOME_SAML	Utilizzato nella risposta SAML per indicare il formato ID nome transitorio SAML 2.0
uid	Utilizzato da Cisco IdS per identificare l'utente autenticato
user_principal	Utilizzato da Cisco IdS per identificare il nome completo (ad esempio ID + dominio) dell'utente autenticato

L'amministratore può personalizzare le alternative al formato del nome tramite il file di configurazione custom-name-formats.xml disponibile in questa directory: <pf\_install>/pingfederate/server/default/data/config-store.

Per eseguire l'SSO con l'identificatore del nome transitorio, aggiungere l'elemento xml nella sezione saml2-subject-name-formats: <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>

Fare clic su Avanti.

Mapping origine autenticazione

Ping Federate

License Warning: Approaching expiration date

SP Connection | Browser SSO | Assertion Creation

Identify Mapping | **Attribute Contract** | Authentication Source Mapping | Summary

PingFederate uses IdP adapters, partner IdPs or Authentication Policies to authenticate users to your SP. Users may be authenticated by one of several different adapters or authentication policy contracts, so map an adapter instance for each IDM system or an authentication policy contract for each policy.

Adapter Instance Name	Virtual Server IDs	Action

Authentication Policy Contract Name	Virtual Server IDs	Action

Map New Adapter Instance    Map New Authentication Policy

Cancel    Save Draft    Previous    Next

Fare clic su Mappa nuova istanza adattatore

Ping Federate

License Warning: Approaching expiration date

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

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

Select an IdP adapter instance that may be used to authenticate users for this partner. Attributes returned by the adapter instance you choose (the Adapter Contract) may be used to fulfill the Attribute Contract with your partner.

ADAPTER INSTANCE: HTML Form IdP Adapter

**Adapter Contract**

email

firstname

lastname

uid

updateTimestamp

user\_principal

username

OVERRIDE INSTANCE SETTINGS

Manage Adapter Instances

Cancel    Save Draft    Next

Mappare l'adattatore IdP del modulo HTML creato in precedenza. Fare clic su Avanti.

Mapping, metodo

Ping Federate

License Warning: Approaching expiration date

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

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

You can choose to fulfill the Attribute Contract with your partner using either the values provided by the "HTML Form IdP Adapter" adapter, or you can use these values plus additional attributes retrieved from local data stores.

**Adapter Contract**

email

firstname

lastname

uid

updateTimestamp

user\_principal

username

RETRIEVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING  
 RETRIEVE ADDITIONAL ATTRIBUTES FROM A DATA STORE - INCLUDES OPTIONS TO USE ALTERNATE DATA STORES AND/OR A FAILSAFE MAPPING  
 USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION

Cancel    Previous    Next    Done    Save

Fare clic su Avanti.

### Attributo Evasione contratto

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

Cancel Previous Next Done Save

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

Assicurarsi che i valori siano impostati su

Contratto attributo	Origine	Valore
SAML_OGGETTO	Adattatore	username Nota molto importante: Il valore utilizzato per questa impostazione deve corrispondere a quello utilizzato nell'impostazione del filtro LI (sezione #3.1.3.2. Configurazione istanza) Nota: 'username' è utilizzato perché il filtro utilizzato era sAMAccountName=\${username}
SAML_AUTHN_CTX	testo	urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTrans
FORMATO_NOME_SAML	testo	urn:oasis:names:tc:SAML:2.0:nameid-format:transient
uid	Adattatore	uid
user_principal	Adattatore	user_principal

Fare clic su Avanti.

### Criteri di rilascio

Ping Federate

License Warning: Approaching expiration date

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

Adapter Instance | Mapping Method | Attribute 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 Save

## Riepilogo

Ping Federate

License Warning: Approaching expiration date

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

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

Click a heading link to edit a configuration setting.

**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)

**Issuance Criteria**

Criterion: (None)

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

Cancel Previous Done Save

Verificate le impostazioni e fate clic su Fine (Done)

Impostazioni protocollo

**Ping Federate**

License Warning: Approaching expiration date

SP Connection | Browser SSO

SAML Profiles | Assertion Lifetime | Assertion Creation | Protocol Settings | Summary

This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.

**Protocol Settings**

OUTBOUND SSO BINDINGS	POST
OUTBOUND SLO BINDINGS	Redirect
INBOUND BINDINGS	POST, Redirect, SOAP
SIGNATURE POLICY	SAML-standard, SAML Assertion, Authn requests over POST & Redirect
ENCRYPTION POLICY	No Encryption

Configure Protocol Settings

Cancel Previous Next Done Save

Fare clic su Configura impostazioni protocollo

URL servizio consumer asserzione

**Ping Federate**

License Warning: Approaching expiration date

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | Allowable SAML Bindings | Signature Policy | Encryption Policy | Summary

As the IdP, you send SAML assertions to the SP's Assertion Consumer Service. The SP may request that the SAML assertion be sent to one of several URLs, via different bindings. Please provide the possible assertion consumer URLs below and select one to be the default.

Default	Index	Binding	Endpoint URL	Action
default	0	POST	/ids/saml/response	Edit   Delete
<input type="checkbox"/>	<input type="text"/>	- SELECT -	<input type="text"/>	Add

Cancel Next Done Save

Aggiungere l'endpoint SSO di binding POST. Fare clic su Avanti.

Associazioni SAML consentite

**Ping Federate**

License Warning: Approaching expiration date

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | Allowable SAML Bindings | Signature Policy | Encryption Policy | Summary

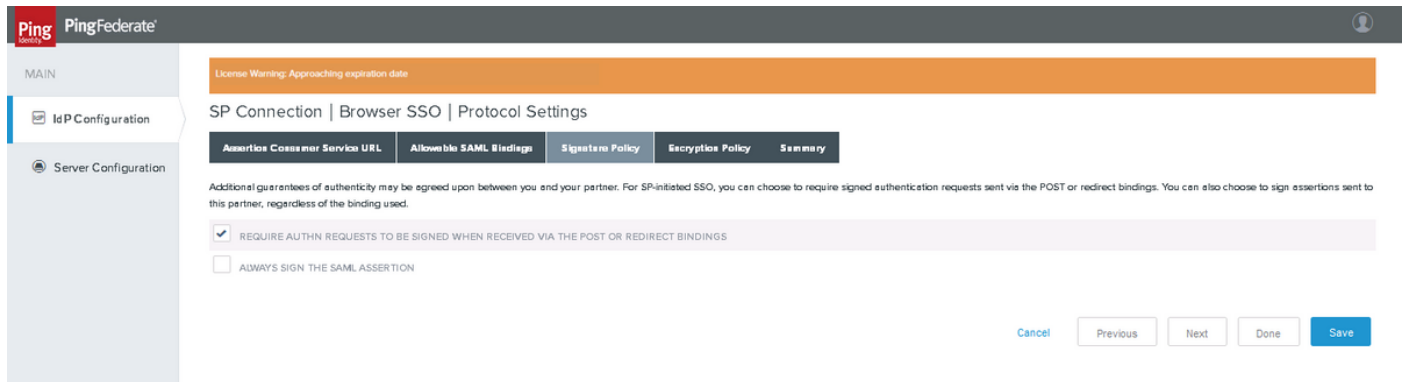
When the SP sends messages, what SAML bindings do you want to allow?

- ARTIFACT
- POST
- REDIRECT
- SOAP

Cancel Previous Next Done Save

Fare clic su Avanti.

## Critero firma

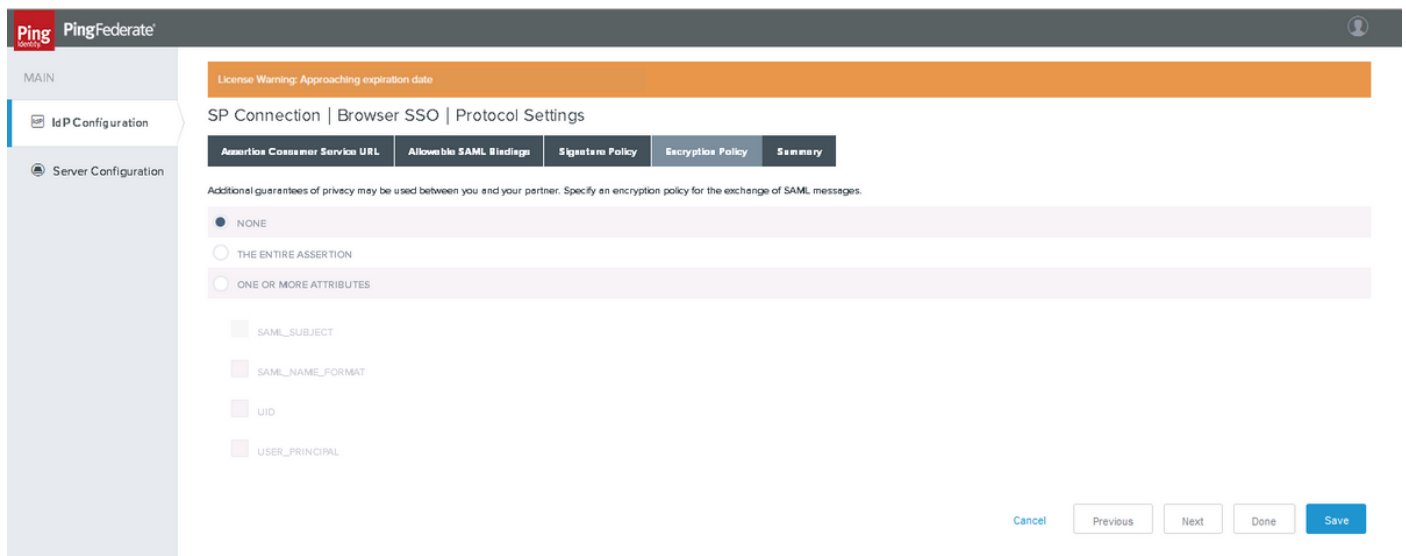


The screenshot shows the PingFederate administration interface. The left sidebar has 'Server Configuration' selected. The main content area is titled 'SP Connection | Browser SSO | Protocol Settings' and has the 'Signatures Policy' tab active. A license warning banner is at the top. Below it, there are tabs for 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signatures Policy', 'Encryption Policy', and 'Summary'. The 'Signatures Policy' section contains the text: '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'.

Nota: Cisco IdS garantisce che il messaggio SAML sia 'firmato' e quindi non selezionare 'FIRMA SEMPRE L'ASSERZIONE SAML'. PingFederate firmerebbe 'SAML assertion' o 'SAML response', ma non entrambi.

Fare clic su Avanti.

## Critero crittografia



The screenshot shows the PingFederate administration interface. The left sidebar has 'Server Configuration' selected. The main content area is titled 'SP Connection | Browser SSO | Protocol Settings' and has the 'Encryption Policy' tab active. A license warning banner is at the top. Below it, there are tabs for 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signatures Policy', 'Encryption Policy', and 'Summary'. The 'Encryption Policy' section contains the text: '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 button options: 'NONE' (selected), 'THE ENTIRE ASSERTION', and 'ONE OR MORE ATTRIBUTES'. Under 'ONE OR MORE ATTRIBUTES', there are four checkboxes: 'SAML\_SUBJECT', 'SAML\_NAME\_FORMAT', 'UID', and 'USER\_PRINCIPAL'. At the bottom right are buttons for 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

Nota: Cisco IdS non supporta il flusso SAML crittografato. Scegliere 'NONE' per l'impostazione 'Crittografia'.

Fare clic su Avanti.

## Riepilogo

Ping Federate

License Warning: Approaching expiration date

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | Allowable SAML Bindings | Signature Policy | Encryption Policy | Summary

Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.

**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
--------	----------

Cancel Previous Done Save

Verificate le impostazioni e fate clic su Fine (Done)

Credenziali

Ping Federate

License Warning: Approaching expiration date

SP Connection

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

For each credential shown here, configure the necessary settings.

**Credential Requirement**

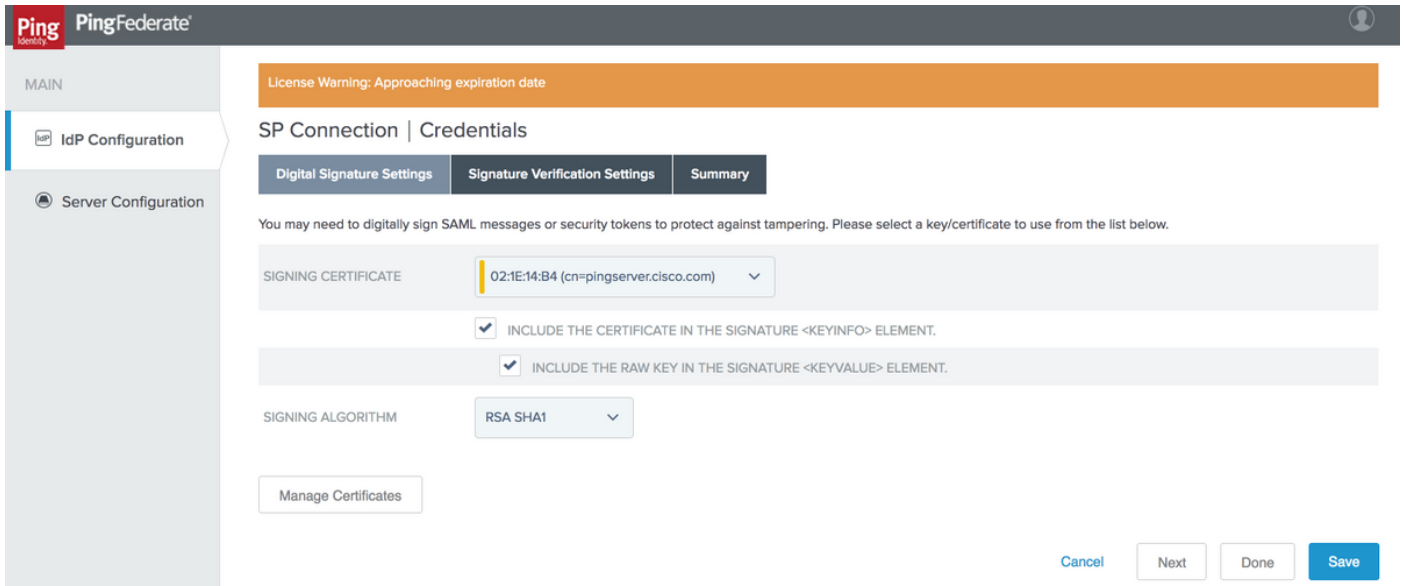
DIGITAL SIGNATURE	CN=SSO
SIGNATURE VERIFICATION SETTINGS	Unanchored Certificate (Primary CN=UCCX-SA1.cisco.com, Secondary Not Configured)

Configure Credentials

Cancel Previous Next Save

Scegliere Configura credenziali

Impostazioni firma digitale



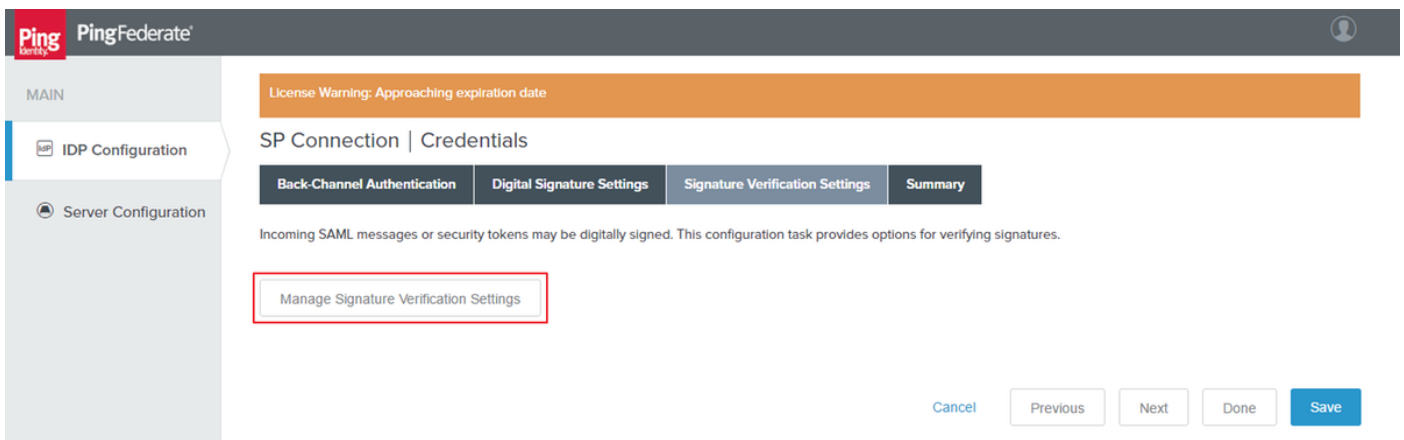
The screenshot shows the 'Digital Signature Settings' tab in the 'SP Connection | Credentials' section. At the top, there is an orange banner with the text 'License Warning: Approaching expiration date'. Below this, the page title is 'SP Connection | Credentials'. There are three tabs: 'Digital Signature Settings' (active), 'Signature Verification Settings', and 'Summary'. A message states: '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.' The 'SIGNING CERTIFICATE' dropdown is set to '02:1E:14:B4 (cn=pingserver.cisco.com)'. There are two checked checkboxes: 'INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.' and 'INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE> ELEMENT.'. The 'SIGNING ALGORITHM' dropdown is set to 'RSA SHA1'. A 'Manage Certificates' button is located at the bottom left. At the bottom right, there are buttons for 'Cancel', 'Next', 'Done', and 'Save'.

Selezionare CERTIFICATO DI FIRMA creato in precedenza. In caso contrario, è possibile fare clic su Gestisci certificati per creare un certificato.

Nota: Cisco IdS non supporta RSA SHA256 per la firma della risposta SAML e pertanto viene utilizzato 'RSA SHA1'.

Fare clic su Avanti.

Impostazioni verifica firma



The screenshot shows the 'Signature Verification Settings' tab in the 'SP Connection | Credentials' section. At the top, there is an orange banner with the text 'License Warning: Approaching expiration date'. Below this, the page title is 'SP Connection | Credentials'. There are four tabs: 'Back-Channel Authentication', 'Digital Signature Settings', 'Signature Verification Settings' (active), and 'Summary'. A message states: 'Incoming SAML messages or security tokens may be digitally signed. This configuration task provides options for verifying signatures.' A 'Manage Signature Verification Settings' button is highlighted with a red rectangle. At the bottom right, there are buttons for 'Cancel', 'Previous', 'Next', 'Done', and 'Save'.

Fare clic su Gestisci impostazioni verifica firma

Modello di trust

License Warning: Approaching expiration date

SP Connection | Credentials | Signature Verification

Trust Model | Signature Verification Certificate | Summary

Select the Trust Model to be used for verifying digital signatures received from this partner.

ANCHORED The verification certificate must be signed by a Trusted CA and included in the incoming message.

UNANCHORED The verification certificate is self-signed, or you wish to trust a specific certificate.

Cancel Next Done Save

Fare clic su Avanti.

Certificato di verifica della firma

License Warning: Approaching expiration date

SP Connection | Credentials | Signature Verification

Trust Model | Signature Verification Certificate | Summary

Please select the certificate(s) to use when verifying these digital signatures. When multiple certificates are chosen, each certificate is tried from the top of the list down until the signature is verified.

PRIMARY 2A7B5D5B (cn=UCDX-SA1.cisco.com)

SECONDARY - SELECT -

Manage Certificates

Cancel Previous Next Done Save

Fare clic su Gestisci certificati per importare i certificati dall'SP.

License Warning: Approaching expiration date

SP Connection | Credentials | Signature Verification | Certificate Management

Manage Digital Verification Certificates

Use this screen to manage the certificates PingFederate needs to verify digital signatures from connection partners or other sources. These certificates may also be used for encryption.

Serial	Subject DN	Expires	Key Details	Status	Active	Action
2A7B5D5B	CN=UCDX-SA1.cisco.com	Sun Nov 24 17:03:42 IST 2019	RSA 2048	Valid	<input checked="" type="checkbox"/>	<a href="#">Activate</a> - Certificate already active <a href="#">Export</a> <a href="#">Delete</a> - Certificate in use

Import

Cancel Done

Fare clic su Importa per importare un certificato.

Riepilogo

License Warning: Approaching expiration date

SP Connection | Credentials | Signature Verification

Trust Model | Signature Verification Certificate | Summary

Summary information for your Signature Verification configuration. Click a heading link to edit a configuration setting.

Signature Verification

<b>Trust Model</b>	
Trust Model	Unanchored
<b>Signature Verification Certificate</b>	
Selected Certificate	CN=UCCX-SA1.cisco.com

Cancel Previous Done Save

Fare clic su Fine

Riepilogo

License Warning: Approaching expiration date

SP Connection | Credentials

Digital Signature Settings | Signature Verification Settings | Summary

Summary information for your Credentials configuration. Click a heading link to edit a configuration setting.

Credentials

<b>Digital Signature Settings</b>	
Selected Certificate	CN=SSO, OU=CBABU, O=CISCO, L=Bangalore, ST=Karnataka, C=IN
Include Certificate in KeyInfo	true
Include Raw Key in KeyValue	true
Selected Signing Algorithm	RSA SHA256
<b>Signature Verification</b>	
<b>Trust Model</b>	
Trust Model	Unanchored
<b>Signature Verification Certificate</b>	
Selected Certificate	CN=UCCX-SA1.cisco.com

Cancel Previous Done Save

Verificate il riepilogo e fate clic su Fine (Done)

Attivazione e riepilogo

MAIN

IdP IdP Configuration

Server Configuration

Copyright © 2003-2016 Ping Identity Corporation

## 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

MAIN

IdP IdP Configuration

Server Configuration

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

### 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**

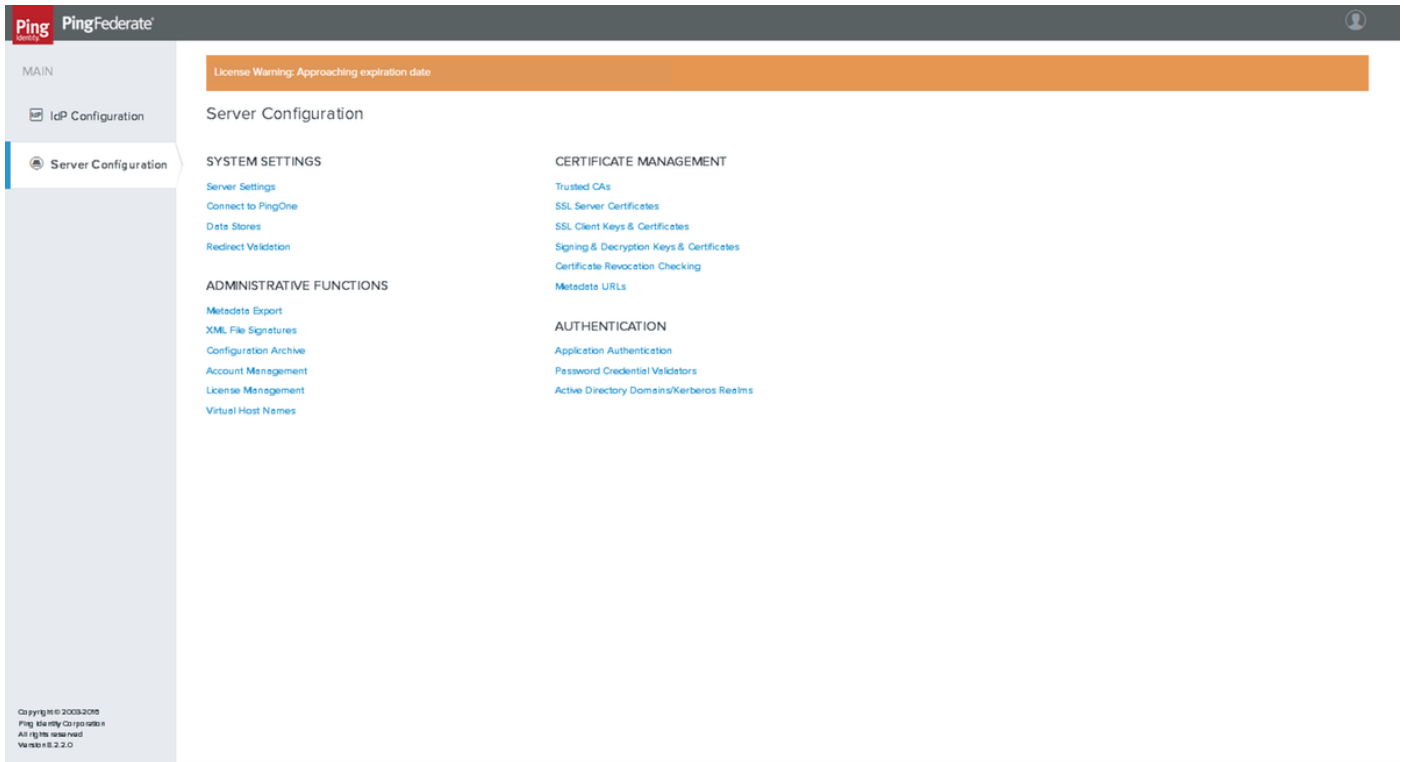
Selected Certificate	CN=UCCX-SA1.cisco.com
----------------------	-----------------------

Cancel Previous Save

Verificare il riepilogo e fare clic su Salva.

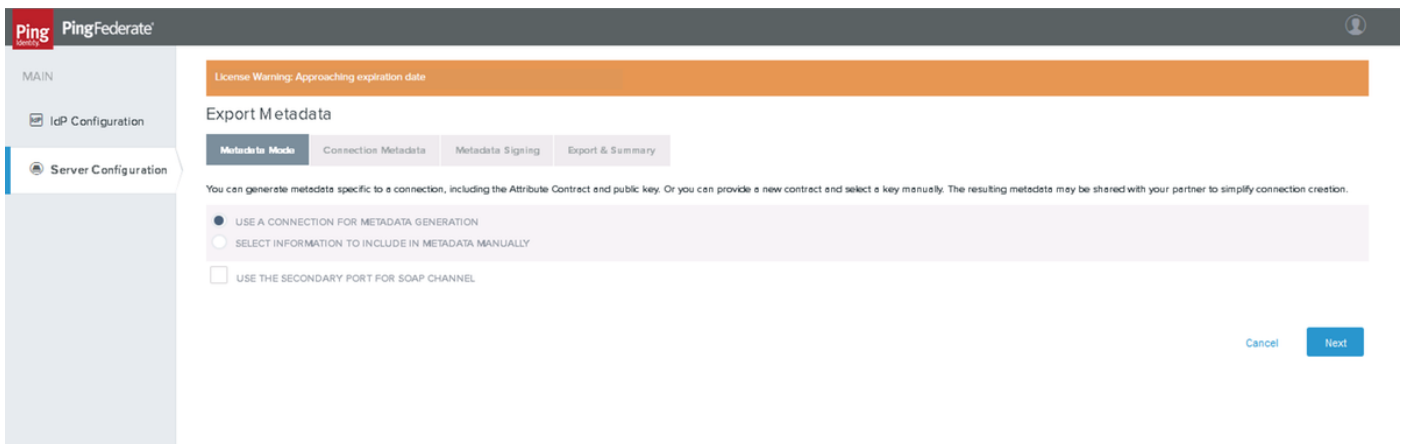
## Esporta metadati PingFederate

### Esportazione metadati



## Modalità metadati

Fare clic su Configurazione server > FUNZIONI AMMINISTRATIVE > Esportazione metadati



Fare clic su Avanti.

## Metadati connessione

## 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**

Selezionare la connessione SP creata e fare clic su Avanti

## Firma metadati

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=SSO)

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**

Selezionare il certificato metadati creato e ALGORITMO DI FIRMA come RSA SHA256. Fare clic su Avanti

## Esportazione e riepilogo

**Export Metadata**

Click the Export button to export this metadata to the file system.

Export Metadata	
<b>Metadata Mode</b>	
Metadata mode	Use connection
Use the secondary port for SOAP channel	false
<b>Connection Metadata</b>	
Selected connection	UCCX-SA1.cisco.com
Attribute	uid
Attribute	SAML_AUTHN_CTX
Attribute	user_principal
Attribute	SAML_NAME_FORMAT
Digital Signature Key	CN=pingserver.cisco.com, OU=cisco, O=ccbu, L=bangalore, ST=Karnataka, C=IN
<b>Metadata Signing</b>	
Signing 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 SHA256

Export

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

Fare clic su Esporta e salva il file nel sistema locale.

- Modificare il file XML dei metadati scaricato per rimuovere le voci dello spazio dei nomi 'md' e salvarlo
- Caricare quindi il file di metadati salvato in IdS dalla pagina idsadmin per stabilire l'attendibilità IDP

## Metadati di esempio

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<md:Metadata xmlns:md="http://www.pingidentity.com/2008/08/metadata" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.pingidentity.com/2008/08/metadata http://www.pingidentity.com/2008/08/metadata.xsd">
  <md:MetadataMode>Use connection</md:MetadataMode>
  <md:UseSecondaryPortForSOAPChannel>false</md:UseSecondaryPortForSOAPChannel>
  <md:ConnectionMetadata>
    <md:SelectedConnection>UCCX-SA1.cisco.com</md:SelectedConnection>
    <md:Attribute>uid</md:Attribute>
    <md:Attribute>SAML_AUTHN_CTX</md:Attribute>
    <md:Attribute>user_principal</md:Attribute>
    <md:Attribute>SAML_NAME_FORMAT</md:Attribute>
    <md:DigitalSignatureKey>CN=pingserver.cisco.com, OU=cisco, O=ccbu, L=bangalore, ST=Karnataka, C=IN</md:DigitalSignatureKey>
  </md:ConnectionMetadata>
  <md:MetadataSigning>
    <md:SigningCertificate>CN=pingserver.cisco.com, OU=cisco, O=ccbu, L=bangalore, ST=Karnataka, C=IN</md:SigningCertificate>
    <md:IncludeCertificateInKeyInfo>true</md:IncludeCertificateInKeyInfo>
    <md:IncludeRawKeyInKeyValue>true</md:IncludeRawKeyInKeyValue>
    <md:SelectedSigningAlgorithm>RSA SHA256</md:SelectedSigningAlgorithm>
  </md:MetadataSigning>
</md:Metadata>
```

## Risoluzione dei problemi

Problema	Strumento	Possibile causa
Caricamento dei metadati PingFederate non riuscito nella pagina	editor di file di testo	Verificare che il file XML dei metadati non contenga le voci dello spazio dei nomi 'md'.

Problema	Strumento	Possibile causa
IdS Admin		
Flusso SAML non riuscito	Tracer SAML	<p>Verificare se 'StatusCode' indica 'Success', ad esempio  <code>&lt;samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" /&gt;</code></p> <ul style="list-style-type: none"> <li>In caso contrario, verificare se indica 'Richiedente' o 'Risponditore' <ul style="list-style-type: none"> <li>'Richiedente' indica un problema con la richiesta SAML, ad esempio se Cisco IdS non ha inviato correttamente la richiesta. Controllare i log di Cisco IdS nella cartella <code>/opt/cisco/ids/log/</code></li> <li>'Risponditore' indica un problema con l'IdP. Controllare i registri PingFederate</li> </ul> </li> </ul>
Flusso SAML non riuscito	Tracer SAML	<p>Controllare l'elemento <code>&lt;saml:AuthnContextClassRef&gt;</code> - il relativo valore deve essere <code>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</code></p> <p>Se il relativo valore è impostato su <code>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</code>, verificare se il contratto <code>SAML_AUTHN_CTXcontract</code> è configurato e mappato correttamente.</p>
Flusso SAML non riuscito	Tracer SAML	<p>Controllare l'elemento <code>&lt;saml:AttributeStatement&gt;</code>. Deve essere presente e contenere elementi figlio che corrispondono a 'uid' e 'user_principal'</p> <p>Se non viene trovato, controllare le impostazioni 'Creazione asserzioni' seguite dalle impostazioni 'Evasione contratto' per verificare che gli attributi del contratto siano definiti e mappati correttamente</p>
Flusso SAML non riuscito	Tracer SAML	<p>Verificare la presenza di un messaggio 'Firma non valida' nei log Cisco IdS o PingFederate.</p> <p>Se confermato, ristabilire il trust metadati tra IdS e PingFederate</p>
Flusso SAML non riuscito	Tracer SAML	<p>Controllare le condizioni temporali, l'ora in cui Cisco IdS ha ricevuto la risposta SAML deve essere compresa tra i tempi indicati in <code>&lt;saml:Conditions NotBefore="2016-12-18T07:24:10.191Z" NotOnOrAfter="2016-12-18T07:34:10.191"&gt;</code></p>

Ulteriore configurazione per SSO:

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

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

## Informazioni su questa traduzione

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