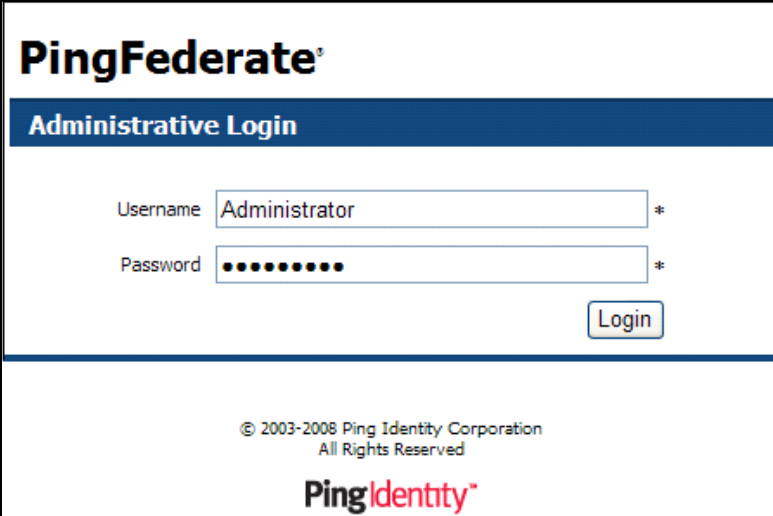


SETUP GUIDE FOR PING AS IDP

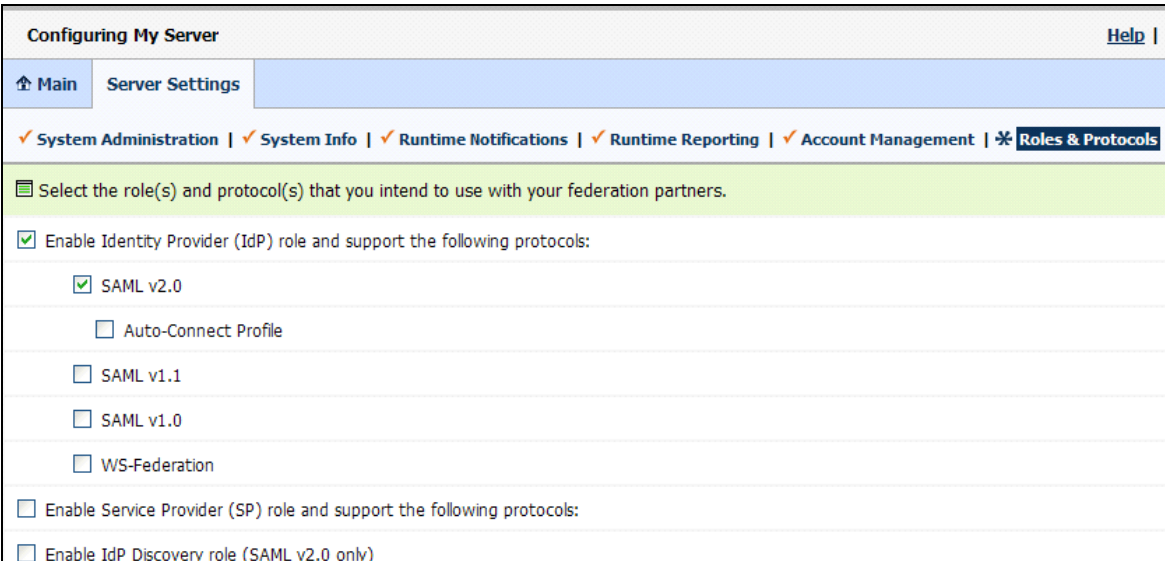
STEP 1:

- Login to your PingFederate environment as the administrator.



The image shows the PingFederate Administrative Login page. At the top is the PingFederate logo. Below it is a dark blue header with the text "Administrative Login". The main area contains two input fields: "Username" with the value "Administrator" and "Password" with masked characters. Both fields have an asterisk (*) to their right. A "Login" button is positioned to the right of the password field. At the bottom, there is a copyright notice: "© 2003-2008 Ping Identity Corporation All Rights Reserved" and the PingIdentity logo.

- Once you have logged into your PingFederate portal, click on the Roles & Protocols under Server Settings and enable the Identity Provider role with the SAML 2.0 protocol.



The image shows the "Configuring My Server" page in the PingFederate portal. The page has a navigation bar with "Main" and "Server Settings". Under "Server Settings", there is a sub-navigation bar with "System Administration", "System Info", "Runtime Notifications", "Runtime Reporting", "Account Management", and "Roles & Protocols". The "Roles & Protocols" section is active. Below the navigation bar, there is a green banner with the text "Select the role(s) and protocol(s) that you intend to use with your federation partners." The main content area has a checkbox labeled "Enable Identity Provider (IdP) role and support the following protocols:". This checkbox is checked. Below it, there are several checkboxes for protocols: "SAML v2.0" (checked), "Auto-Connect Profile" (unchecked), "SAML v1.1" (unchecked), "SAML v1.0" (unchecked), and "WS-Federation" (unchecked). There are also two unchecked checkboxes for "Enable Service Provider (SP) role and support the following protocols:" and "Enable IdP Discovery role (SAML v2.0 only)".

- In order to integrate with Confluence, create a new SP (Service Provider) connection. When creating the new connection, supply Confluence' EntityID and base URL:

Summary	
SP Connection	
Role & Protocol	
Connection Type	SP
Protocol	SAML v2.0
General Info	
Partner's Entity ID (Connection ID)	http://localhost:8096/wordpress4/wp-content/plugins/miniorange-saml-20-single-sign-on/
Base URL	http://localhost:8096/wordpress4/

- Choose SP-initiated SSO under SAML Profiles:

Main SP Connection	
✓ Role & Protocol ✓ General Info ✓ Assertion Lifetime ✖ SAML Profiles ✓ Assertion Creation ✓ Web SSO	
<p>A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider. Configure this information for your SP connection.</p>	
Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
<input type="checkbox"/> IdP-Initiated SSO	<input type="checkbox"/> IdP-Initiated SLO
<input checked="" type="checkbox"/> SP-Initiated SSO	<input type="checkbox"/> SP-Initiated SLO

- Go To Web SSO and select Summary tab. Set Assertion Consumer Service URL (ACS URL) and also specify the binding type (POST or ARTIFACT).

Main SP Connection Web SSO	
✓ Assertion Consumer Service URL ✓ Signature Policy ✓ Encryption Policy ✖ Summary	
<p>Summary information for your Web SSO configuration. Click a heading link to edit a configuration setting.</p>	
Summary Info	
Web SSO	
Assertion Consumer Service URL	
Endpoint	URL: /a/pingidentity.com/acs (POST)

- Go to Credentials screen. Create a signing certificate.

* **Create Certificate** | Summary

Create a new Certificate and Private Key.

Common Name	Ping Identity Signing *
Organization	Ping Identity *
Organizational Unit	Global Client Services
City	Boston
State	MA
Country	US *
Validity (days)	365 *
Key Algorithm	RSA ▾ *
Key Size (bits)	1024 ▾ *

STEP 2

- Copy the following URL/Endpoints. These will be required while configuring the plugin.

Copy the X.509 Certificate textarea value and keep it handy.

- Go to **Configure SP** Tab in **miniOrange SAML Plugin** and enter the following details:

IDP Entity ID	Entity ID from the Single Sign On tab in Ping Federate
Single Sign On URL	Login URL from the Single Sign On tab in Ping Federate
Single Logout URL	Logout URL from the Single Sign On tab in Ping Federate
X.509 Certificate	Paste the X.509 Certificate value from Single Sign On tab in Ping Federate

STEP 3:

In miniOrange SAML plugin, go to **Attribute Mapping** tab. Enter the following values:

- Username:** Name of the username attribute from IDP (Keep NameID by default)
- Email:** Name of the email attribute from IDP (Keep NameID by default)

- **FirstName:** Name of the firstname attribute from IDP
- **LastName:** Name of the lastname attribute from IDP

Account	Configure IDP	Configure SP	Attribute Mapping	Role Mapping	Sign In Settings	Certificates	Support
---------	---------------	--------------	-------------------	--------------	------------------	--------------	---------

Attribute Mapping

Username: *
Enter the Attribute Name that contains Confluence Username. Use *NameID* if Username is in Subject element.

Email: *
Enter the Attribute Name that contains Email. Use *NameID* if Email is in Subject element.

Full Name Attribute:
Enter the Attribute Name that contains Full Name.

Separate Name ☐ (Select this if your IDP is sending First name and Last name as separate attributes.)
 Attributes:

First Name:
Enter the Attribute Name that contains First Name.

Last Name:
Enter the Attribute Name that contains Last Name.

STEP 4:

Go to **Role Mapping** tab. Enter the following values:

- **Role Mapping:** Name of the Role attribute from IDP

You can check the ***Test Configuration Results*** to get a better idea as to which values to map here.

Under the Role Mapping Section configure which GROUP value coming in the SAML response needs to be mapped to which role. The Group value coming in the SAML response will be mapped to the Role assigned here and the user will be assigned that role.

Account	Configure IDP	Configure SP	Attribute Mapping	Role Mapping	Sign In Settings	Certificates	Support
---------	---------------	--------------	-------------------	--------------	------------------	--------------	---------

Role Mapping

Role Attribute:

Enter the Attribute Name that contains Roles of the User.

Create Users: ☐ If checked, Users will be created only if roles are mapped.

Default Group:

Select Default Group to assign to new Users.

confluence-administrators:

confluence-users:

Note: Enter semi-colon separated list of role values in the textbox.

Save

STEP 5:

Go to **Sign In Settings** tab. Enable auto-redirect to IDP using **Disable Confluence login** option.

Account	Configure IDP	Configure SP	Attribute Mapping	Role Mapping	Sign In Settings	Certificates	Support
---------	---------------	--------------	-------------------	--------------	------------------	--------------	---------

Sign In Settings

Login Button Text:

Disable Confluence login: ☒

Enable backdoor: ☒ Use `http://localhost:8091/login.action?saml_sso=false`
For administrative tasks use `http://localhost:8091/authenticate.action?saml_sso=false`

Save