

## **Implementation Guide:**

### **Ping Identity Workforce360**

**November 2020**



## Table of Contents

Foreword .....	3
Solution overview and features .....	4
Architecture diagram.....	4
Pre-requisites .....	6
Subscribe to Workforce 360.....	7
Deployment and configuration steps.....	8
Best practices .....	16
Solution estimated pricing.....	16
FAQs.....	16
Additional resources.....	17
Partner contact information.....	17

## Foreword

Ping Identity is a leader in identity access and management that provides a comprehensive suite of identity services on the AWS Cloud. Implementing this solution helps ensure that enterprise customers, employees, and partners have real-time, intelligent access to resources from anywhere, making their digital business initiatives more agile with a centralized control point for security.

The purpose of the AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure the Ping Identity Workforce360 solution in AWS Control Tower environment. Additionally, it allows them to take full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

## Solution overview and features

Ping Identity's Workforce360 solution provides central authentication services to connect employees across different applications, directories, and situations. By providing broad authentication, it can help eliminate authentication silos. The result is a centrally managed authentication hub that provides a seamless, consistent experience for your workforce. When deployed in an AWS Control Tower environment, users can optimize identity and access management in a multi-account environment with standards based single sign-on, multi-factor authentication, user directory, and provisioning for their AWS environments.

With Ping Identity Workforce360, features include:

- ✓ Workforce authentication authority
- ✓ Single sign-on (SSO) for employees, partners, and more
- ✓ Multi-factor authentication (MFA) with contextual and adaptive policies
- ✓ Centralized management and delegated administration
- ✓ Real-time user and group provisioning to hundreds of cloud applications

## Architecture diagram

Ping Identity offers two Workforce360 configurations to integrate with AWS Control Tower via AWS Single Sign-On (AWS SSO). The first is the Workforce360 Express option, which leverages the PingOne SaaS platform to perform the user provisioning and single sign-on to AWS SSO. The second is the Workforce360 Advanced option which leverages PingFederate Cloud Native solution to perform the user provisioning and single sign-on to AWS SSO.

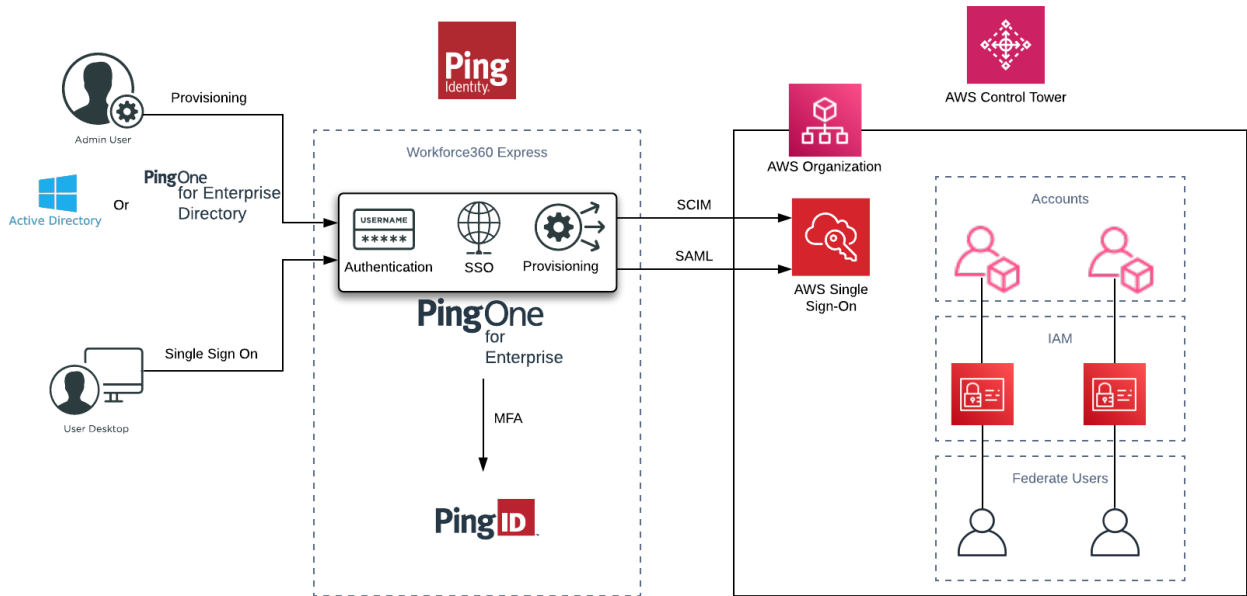


Figure 1. Ping Identity Workforce Express with PingOne for Enterprise Architecture Diagram

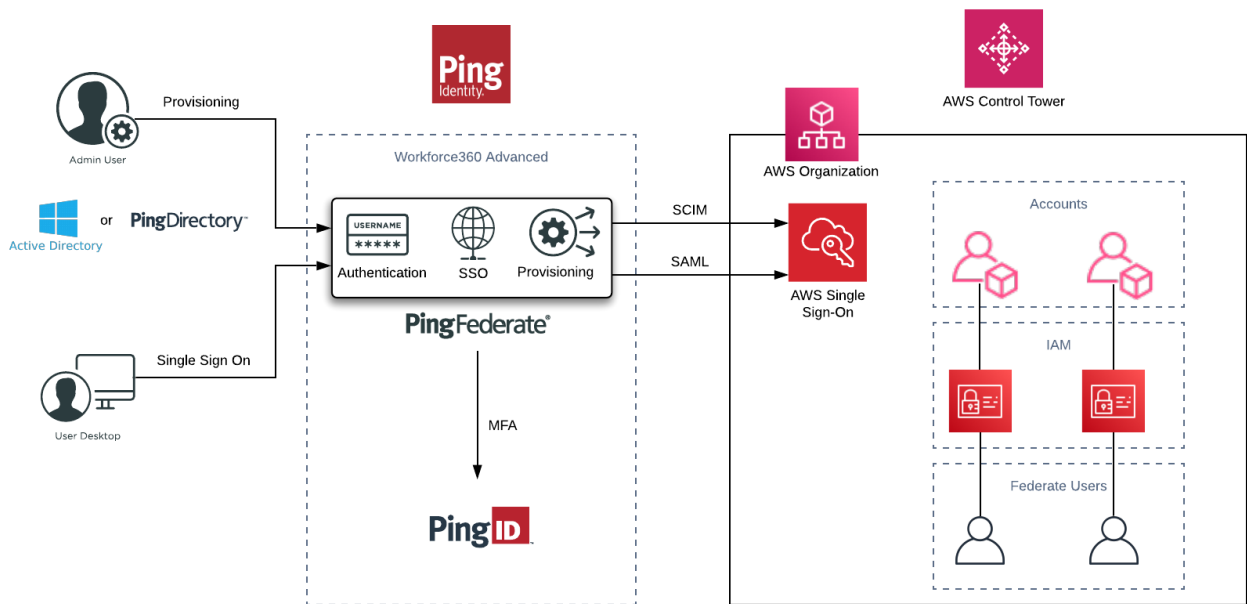


Figure 2. Ping Identity Workforce Advanced with PingFederate Architecture Diagram

## Pre-requisites

### **Workforce360 Express (PingOne)**

You will need the following before you can get started:

- A PingOne subscription or free trial, with both federated authentication and provisioning capabilities. For more information about how to obtain a free trial, see the [Ping Identity](#) website. Ensure the IdP
- An AWS SSO-enabled account ([free](#)). For more information, see [Enable AWS SSO](#).
- Download the AWS SSO metadata file from the External Identity provider configuration in AWS account. For more information, see [How to Connect to an External Identity Provider](#).
- The PingOne AWS Single Sign-On application added to your PingOne admin portal. You can obtain the PingOne AWS Single Sign-On application from the PingOne Application Catalog. For general information, see [Add an application from the Application Catalog](#) on the Ping Identity website.

### **Workforce360 Advanced (PingFederate)**

You will need the following before you can get started:

- A working PingFederate server. If you do not have an existing PingFederate server, you may be able to obtain a free trial or developer account including licenses and software downloads and associated documentation from the [Ping Identity](#) website.
- A copy of the PingFederate AWS Single Sign-On Connector software installed on your PingFederate server. For more information about how to obtain this software, see [AWS Single Sign-On Connector](#) on the Ping Identity website.
- An AWS SSO-enabled account ([free](#)). For more information, see [Enable AWS SSO](#) and a downloaded copy the AWS SSO SAML Metadata file.

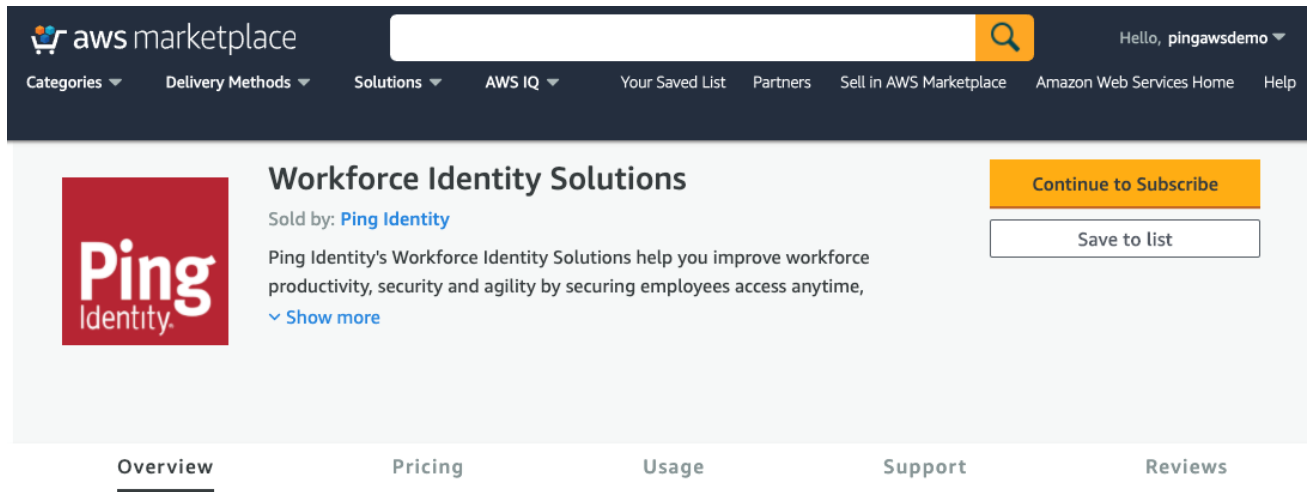
### **System requirements:**

- PingFederate 9.0 or later.
- An AWS Single Sign-On administrator account.
- To allow PingFederate to make outbound connections to the AWS Single Sign-On API, you might need to allow the following domain in your firewall:
  - <https://aws.amazon.com>

# Subscribe to Workforce 360

1. Navigate to Ping Identity's Workforce 360 listing in the AWS Marketplace

(<https://aws.amazon.com/marketplace/pp/B0877CGKF9>)



The screenshot shows the AWS Marketplace product page for 'Workforce Identity Solutions' by Ping Identity. The page includes a search bar, navigation menu, and product details. The 'Continue to Subscribe' button is highlighted in orange.

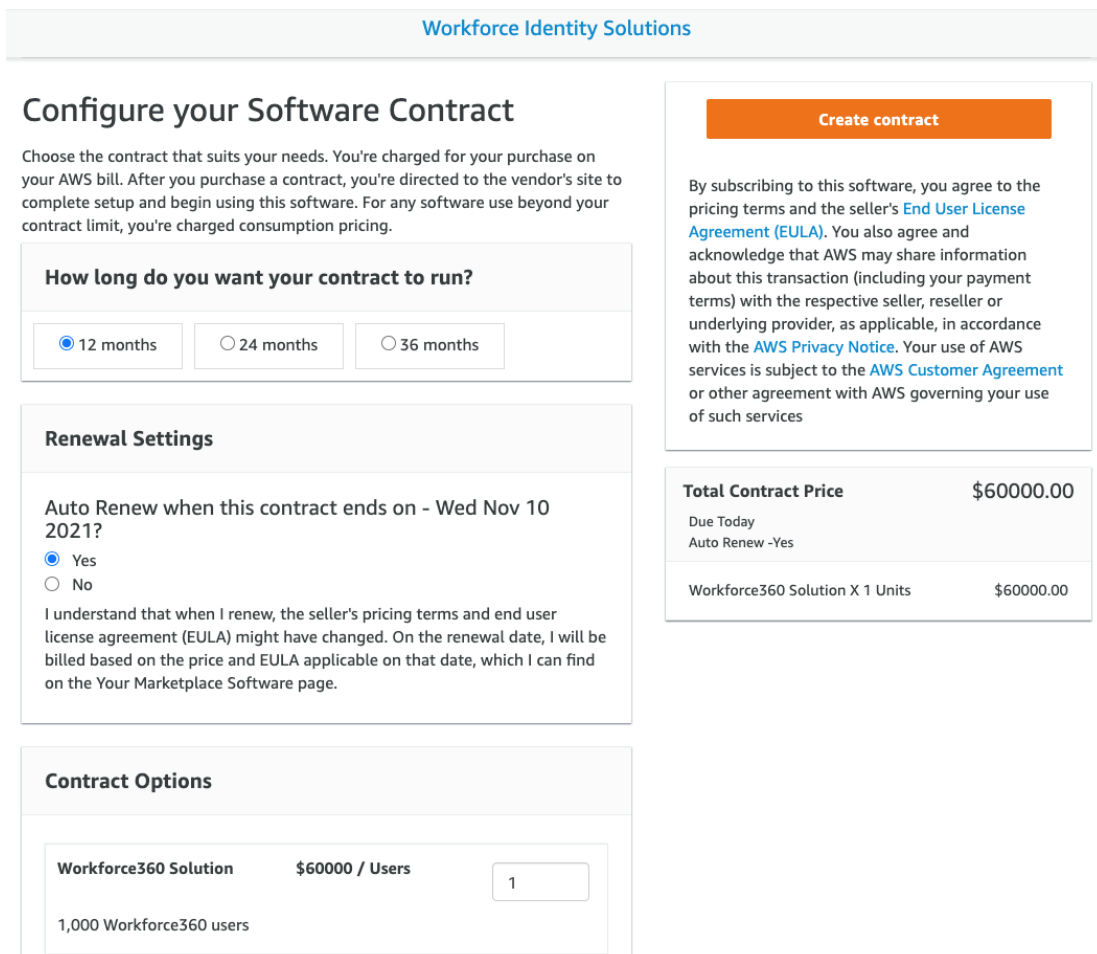
**Workforce Identity Solutions**  
Sold by: [Ping Identity](#)  
Ping Identity's Workforce Identity Solutions help you improve workforce productivity, security and agility by securing employees access anytime, [Show more](#)

**Continue to Subscribe**  
Save to list

Overview Pricing Usage Support Reviews

Click **Continue to Subscribe**

2. Next, select the **Contract Duration**, **Renewal** and **Contract Options** and click **Create Contract**.



The screenshot shows the 'Configure your Software Contract' page. It includes a 'Create contract' button, a 'How long do you want your contract to run?' section with radio buttons for 12, 24, and 36 months, a 'Renewal Settings' section with a 'Yes' radio button selected, and a 'Contract Options' section with a quantity of 1 selected. A summary table on the right shows a total contract price of \$60,000.00.

**Workforce Identity Solutions**

### Configure your Software Contract

Choose the contract that suits your needs. You're charged for your purchase on your AWS bill. After you purchase a contract, you're directed to the vendor's site to complete setup and begin using this software. For any software use beyond your contract limit, you're charged consumption pricing.

**How long do you want your contract to run?**

12 months  24 months  36 months

**Renewal Settings**

Auto Renew when this contract ends on - Wed Nov 10 2021?

Yes  No

I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.

**Contract Options**

Workforce360 Solution	\$60000 / Users	<input type="text" value="1"/>
-----------------------	-----------------	--------------------------------

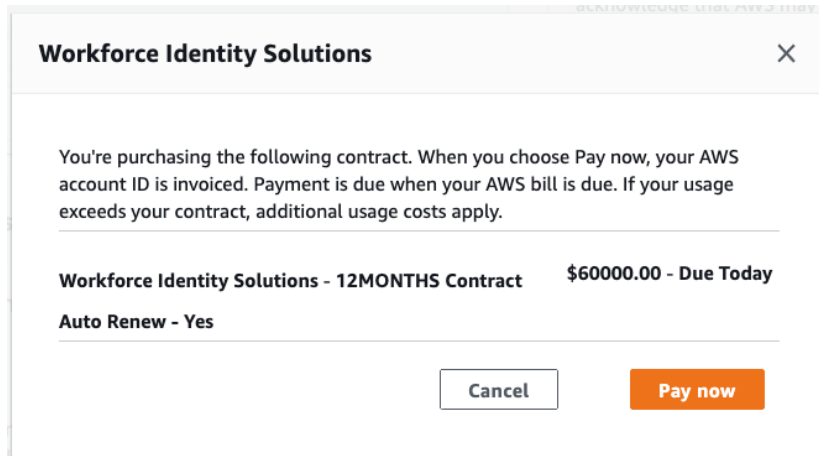
1,000 Workforce360 users

**Create contract**

By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services is subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services

<b>Total Contract Price</b>	\$60000.00
Due Today	
Auto Renew -Yes	
Workforce360 Solution X 1 Units	\$60000.00

3. The summary screen will appear indicating the total pricing of the offering. Click **Pay Now** to finalize the contract.



## Deployment and Configuration Steps

### Workforce360 Express (PingOne)

#### 1. Create the AWS SSO application

In this step, you will create the AWS SSO application from the PingOne Application catalog.

1. Go to **Applications** → **Application Catalog**.
2. In the Search field, search for the **AWS Single Sign-On** application by typing **AWS** in the search box and selecting the AWS Single Sign-On (SAML with Provisioning) entry.
3. Click **Setup** to begin. The SSO Instructions page for the application is displayed.
4. No requires changes on the SSO Instructions page. Click **Continue to Next Step**.
5. For the Upload Metadata field, click Select File and locate your AWS SSO SAML Metadata file downloaded in as part of the pre-requisites. Click **Continue to Next Step**.
6. For the SAML\_SUBJECT attribute mapping, click the Name or Literal field and select **Email (Work)**. Click **Continue to Next Step**.
7. For PingOne App Customizations – customize the icon image, name and description as necessary. Click **Continue to Next Step**.
8. Make the AWS SSO application available to your users by assigning the groups authorized to use the application. All members of the selected group or groups will be able to use the application. When the application supports user provisioning, user provisioning to this application is also enabled for members of the assigned groups.

- Click **Add** for each group you want to authorize to use the application.
- Click **Continue to Next Step**

The summary information for the application configuration is then displayed on a new page.

9. On the Review Setup page, click Download beside the SAML Metadata to download the PingOne application metadata. In your AWS tenant, upload the PingOne SAML Metadata to your AWS SSO External IdP configuration under the Change Identity Source screen for the IdP SAML metadata required field.
10. Once the AWS SSO External IdP configuration is complete, the Initiate Single Sign-On (SSO) URL on the Review Setup page can be used to initiate an authentication to test the IdP initiated SSO.

## 2. Enable provisioning in AWS SSO

In this first step, you will use the AWS SSO console to enable automatic provisioning.

### To enable automatic provisioning in AWS SSO

1. After you have completed the prerequisites, open the [AWS SSO console](#).
2. Choose **Settings** in the left navigation pane.
3. On the **Settings** page, under **Identity source > Provisioning**, choose **Enable automatic provisioning**. This immediately enables automatic provisioning in AWS SSO and displays the necessary endpoint and access token information.
4. In the **Inbound automatic provisioning** dialog box, copy each of the values for the following options. You will need to paste these in later when you configure provisioning in your IdP.
  - a. **SCIM endpoint**
  - b. **Access token**
5. Choose **Close**.

## 3. Configure provisioning in PingOne

Use the following procedure in the PingOne AWS Single Sign-On application to enable provisioning with AWS SSO. This procedure assumes that you have already added the PingOne AWS Single Sign-On application to your PingOne admin portal completed in Step 1 above.

### To configure provisioning in PingOne

1. Open the PingOne AWS Single Sign-On application you installed as part of configuring SAML for PingOne (**Applications > My Applications**).

2. Scroll to the bottom of the page. Under **User Provisioning**, click the **complete** link which will jump you to the user provisioning configuration of your connection.
3. On the **Provisioning Instructions** page, click **Continue to Next Step**.
4. In the previous procedure you copied the **SCIM endpoint** value in AWS SSO. Paste that value into the **SCIM URL** field in the PingOne AWS Single Sign-On application. Make sure that you remove the trailing forward slash at the end of the URL. Also, in the previous procedure you copied the **Access token** value in AWS SSO. Paste that value into the **ACCESS\_TOKEN** field in the PingOne AWS Single Sign-On application.
5. For **REMOVE\_ACTION**, select either **Disabled** or **Deleted** (see the description text on the page for more details).
6. On the **Attribute Mapping** page, select a value to use for the **SAML\_SUBJECT** (NameId) assertion, following guidance from [Additional Considerations](#) earlier on this page, and click **Continue to Next Step**.
7. On the **PingOne App Customization - AWS Single Sign-On** page, make any desired customization changes (optional), and click **Continue to Next Step**.
8. On the **Group Access** page, select the groups containing the users you would like to enable for provisioning and single sign-on to AWS SSO. Click **Continue to Next Step**.
9. Scroll to the bottom of the page, and click **Finish**. At this point, provisioning will start.
10. To verify that users have been successfully synchronized to AWS SSO, return to the AWS SSO console and select **Users**. Synchronized users from PingOne will appear on the **Users** page. These users can now be selected for assignment to accounts and applications within AWS SSO.

As a reminder, PingOne does not support provisioning of groups or group memberships via SCIM. Please contact Ping for more information.

#### 4. Testing provisioning

To test provisioning of an user to AWS SSO within AWS Control Tower move or create an account in the PingOne configured external data source (Active Directory or PingOne for Enterprise Directory). The account will be automatically provisioned and available to view in AWS SSO under Users.

#### 5. Testing Single Sign-On

1. Open a browser and navigate to the AWS SSO User Portal URL.
2. A series of redirects will navigate to the PingOne user credentials form.
3. Enter the username created in the previous provisioning step. This will redirect to the AWS SSO user portal.

## Workforce360 Advanced (PingFederate)

### 1. Overview of the AWS Single Sign-On Connector for PingFederate

The AWS Single Sign-On Connector allows PingFederate to integrate with AWS Single Sign-On for user and group provisioning and single sign-on (SSO).

#### Features:

- Manages users
  - Creates, updates, disables, and deletes users.
  - Allows you to enable the create, update, disable, and delete capabilities independently.
  - Allows you to choose whether to disable or delete users when deprovisioning.
  - Allows you to provision disabled users.
- Manages groups
  - Creates and deletes groups.
  - Updates group memberships.
- Enables browser-based SSO initiated by the service provider (SP) or identity provider (IdP).
- Pre-populates some connection settings with the included quick connection template.

### 2. Configure PingFederate for AWS Control Tower with AWS SSO

The AWS Single Sign-On Connector allows PingFederate to integrate with AWS Single Sign-On for user and group provisioning and single sign-on (SSO).

Your external datastore acts as the source of data for provisioning. PingFederate also uses an internal datastore to store the state of synchronization between the source datastore and the target datastore. For more information, see [Datastores](#) and [Configuring](#) outbound provisioning settings in the PingFederate documentation.

1. Configure the data store that PingFederate will use as the source of user data. For instructions, see [Managing datastores](#) in the PingFederate documentation.

**ATTENTION:** When targeting users and groups for provisioning, exclude the user account that you will use to administer users in your connection to AWS Single Sign-On. This prevents the

PingFederate provisioning engine from interfering with the account that provisions users and groups.

2. Do one of the following:
  - For PingFederate 10.1 or later: go to **System** → **Server** → **Protocol Settings**.
  - For PingFederate 10.0 or earlier: enable the identity provider and outbound provisioning roles.
    1. Go to **System** → **Server** → **Roles & Protocols**.
    2. Select **Enable Identity Provider IdP Role and Support the Following**.
    3. Select **SAML 2.0** and **Outbound Provisioning**. Click **Next**.
3. On the **Federation Info** tab, in the **SAML 2.0 Entity ID** field, enter a name for PingFederate to use to identify itself to SAML partners.
4. On the **Outbound Provisioning** tab, select the PingFederate internal datastore. Click **Save**. For help, see [Configuring outbound provisioning settings in the PingFederate documentation](#).

### 3. Exporting SAML metadata from PingFederate

Export a metadata file that describes your PingFederate identity provider configuration.

For general information about these steps, see [Metadata export in the PingFederate documentation](#).

1. In the PingFederate administrative console, open the Metadata Export window.
  - For PingFederate 10.1 or later: go to **System** → **Protocol Metadata** → **Metadata Export**.
  - For PingFederate 10.0 or earlier: go to **System** → **Metadata Export**.
2. If you see the **Metadata Role** tab, select **I am the identity provider (IdP)**. Click **Next**.
3. On the **Metadata Mode** tab, select **Select information to include in metadata manually**. Click **Next**.
4. On the **Protocol** tab, ensure SAML 2.0 is selected, click **Next**.
5. On the **Attribute Contract** tab, click **Next**.
6. On the **Signing Key** tab, select a signing certificate. Click **Next**.
7. **Optional:** On the **Metadata Signing** tab, select a certificate to sign the metadata XML file. Click **Next**.
8. On the **XML Encryption Certificate** tab, click **Next**.
9. On the **Export & Summary** tab, click **Export**.
10. Save metadata.xml.
11. Click Done.

#### 4. Registering PingFederate as an identity provider in AWS Single Sign-On

To allow PingFederate to communicate with AWS Single Sign-On, exchange the two metadata files between the two systems and note the provisioning details from AWS.

1. Sign on to the [AWS SSO Console](#) as the root user for the AWS account.
2. Go to **Settings**. In the **Identity source** section, on the **Identity source** row, click **Change**.
3. On the "Choose where your identities are sourced page, click **External identity provider**.
4. In the **Service provider metadata** section, click **Download metadata file**. Save the sp-saml-metadata.xml file.
5. In the **Identity provider metadata** section, upload the PingFederate metadata file that you exported in [Exporting SAML metadata from PingFederate](#).
6. Click **Next: Review**.
7. In the **Review and confirm** section, enter ACCEPT. Click **Save identity source**.
8. Note your provisioning SCIM URL and access token ID.
  1. On the Settings window, in the **Identity source** section, on the **Provisioning** row, click **View details**.
  2. On the Automatic Provisioning window, note the **SCIM endpoint** and **Access token ID**. You will use these in [Creating a connection](#).

## 5. Creating a connection

To allow PingFederate to act as an identity provider and manage users in AWS Single Sign-On, create a service provider (SP) connection.

### Steps

1. On the PingFederate administrator console, create a new SP connection.
  - For PingFederate 10.1 or later: go to **Applications** → **Integration** → **SP Connections**. Click **Create Connection**.
  - For PingFederate 10.0 or earlier: go to **Identity Provider** → **SP Connections**. Click **Create Connection**.
2. Configure the basic connection details with the AWS Single Sign-On quick connection template.
  1. On the **Connection Template** tab, select **Use a template for this connection**.
  2. From the **Connection Template** list, select **AWS SSO Cloud Connector**.
  3. On the **Metadata File** row, upload the sp-saml-metadata.xml file that you saved in [Registering PingFederate as an identity provider in AWS Single Sign-On](#). Click **Next**.
  4. On the **Connection Type** tab select **Browser SSO Profiles** and **Outbound Provisioning**. Click **Next**.
  5. On the **Connection Options** tab, click **Next**.
  6. On the **General Info** tab, in the **Connection Name** field, enter a name of your choosing. Click **Next**.
3. On the **Browser SSO** tab, configure browser SSO with the following details. For help, see [Configuring IdP Browser SSO in the PingFederate documentation](#).

#### Attribute Creation -> Configure Assertion Creation

1. Click **Map New Authentication Policy**
2. Select the **Authentication Policy Contract** used in your system. Click **Next**.
3. On **Mapping Method** click **Next**
4. On **Attribute Contract Fulfillment**, **Source** is Authentication Policy Contract and **Value** is mail
5. On **Issuance Criteria** click **Next**. Click **Done**.
6. Back on Authentication Source Mapping click **Done**.
7. **Attribute Contract** – change attribute Contract to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**. Click **Done**.
8. Back on Assertion Creation click **Next**

## Protocol Settings -> Configure Protocol Settings

9. **Assertion Consumer Service URL** – there's default URL – do I need to modify this to add AWS SSO ACS URL?
10. Click **Done**
4. On the **Credentials** tab, configure the connection credentials as shown in Configuring credentials in the PingFederate documentation. Click **Next**.
5. On the **Outbound Provisioning** tab, configure provisioning with the following details. For help, see Configuring outbound provisioning in the PingFederate documentation.
  - On the **Target** tab, complete the **SCIM URL** and **Access Token** fields with the values that you noted in [Registering PingFederate as an identity provider in AWS Single Sign-On](#).
  - Under **Provisioning Options**, customize the provisioning connector behavior by referring to [Provisioning options reference](#). Click **Next**.
  - On the **Manage Channels** → **Attribute Mapping** tab, at the bottom of the attribute list, click **Refresh Fields** to get fields and specifications from your AWS Single Sign-On site. Complete the attribute mappings by referring to [Supported attributes reference](#). For help, see Managing channels in the PingFederate documentation.
6. On the **Activation and Summary** tab, above the **Summary** section, turn on the connection. Click **Save**.

## 6. Testing provisioning

To test provisioning of a user to AWS SSO within AWS Control Tower move or create an account in the PingFederate configured external datastore. The account will be automatically provisioned and available to view in AWS SSO under Users.

## 7. Testing single sign-on

1. Open a browser and navigate to the AWS SSO User Portal URL.
2. A series of redirects will navigate to the PingFederate user credentials form.
3. Enter the username created in the previous provisioning step. This will redirect to the AWS SSO user portal.

## Best practices

The following are important considerations about PingOne that can affect how you implement provisioning with AWS SSO.

- As of October 2020, PingOne does not support provisioning of groups via System for Cross-domain Identity Management (SCIM).
- If using the PingOne for Enterprise Directory, ensure the optional displayName attribute is configured and populated as it is required by AWS SSO.
- Users may continue to be provisioned from PingOne after disabling provisioning in the PingOne admin portal. If you need to terminate provisioning immediately, delete the relevant SCIM bearer token, and/or disable [Automatic Provisioning](#) in AWS SSO.
- If an attribute for a user is removed from the data store configured in PingOne, that attribute will not be removed from the corresponding user in AWS SSO. This is a known limitation in PingOne's provisioner implementation. If an attribute is modified, the change will be synchronized to AWS SSO.
- The following are important notes regarding your SAML configuration in PingOne:
  - AWS SSO only supports emailAddress as a NameId format. This means you will need to select a user attribute that is unique within your directory in PingOne, non-null, and formatted as an email/UPN (for example, user@domain.com) for your **SAML\_SUBJECT** mapping in PingOne. **Email (Work)** is a reasonable value to use for test configurations with the PingOne built-in directory.
  - Users in PingOne with an email address containing a + character may be unable to sign in to AWS SSO, with errors such as 'SAML\_215' or 'Invalid input'. To fix this, in PingOne, select the **Advanced** option for the **SAML\_SUBJECT** mapping in **Attribute Mappings**, and set **Name ID Format to send to SP:** to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** in the drop-down menu.

## Solution estimated pricing

Below are the total costs for these different subscription durations. Additional taxes or fees may apply.

Workforce Identity Solutions				
Users	Description	12 MONTHS	24 MONTHS	36 MONTHS
Workforce360 Solution	1,000 Workforce360 users	\$60,000	\$120,000	\$180,000

## FAQs

Before you start, you should be familiar with the following:

- AWS Single Sign-On documentation:
  - [What is AWS Single Sign-On?](#)
  - [Understanding key AWS Single Sign-On concepts](#)
  - [Users, groups, and provisioning](#)
  - [SCIM Profile and SAML 2.0 implementation](#)
  - [Automatic provisioning](#)
- PingFederate documentation:
  - [Identity provider SSO configuration](#)
  - [Datastores](#)
  - [Managing digital signing certificates and decryption keys](#)
  - [SP connection management](#)
  - [Configuring outbound provisioning](#)

## Additional resources

- Ping Identity for AWS
  - <https://www.pingidentity.com/en/lp/e/aws-ping-identity.html>
- Ping Identity support documentation for AWS
  - <https://docs.pingidentity.com/bundle/integrations/page/kun1563994988131.html>
- Ping Identity on AWS Marketplace
  - <https://aws.amazon.com/marketplace/pp/B0877CGKF9>
- Ping Identity developer documentation
  - <https://developer.pingidentity.com/en.html>

## Partner contact information

For questions, contact [tap-global@pingidentity.com](mailto:tap-global@pingidentity.com)