Amazon WorkSpaces SAML Authentication Implementation Guide

First published November 18, 2022

Last updated April 26, 2024



Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

© 2024 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

Introduction and Requirements 5

Introduction 5

Requirements 5

Prerequisites 5

Step 1: Generate SAML 2.0 metadata manifest in your identity provider 6

ADFS 7

Auth0 7

Azure AD 8

Duo Single Sign-On 9

JumpCloud 9

Keycloak 10

Okta 11

OneLogin 11

PingFederate 12

PingOne for Enterprise 13

Step 2: Create a SAML 2.0 identity provider in AWS IAM 13

Step 3: Create a SAML 2.0 federation IAM role and policy 14

Step 4: Configure your SAML 2.0 identity provider 17

ADFS 19

Auth0 23

Azure AD 24

Duo Single Sign-On 26

JumpCloud 27

Keycloak 28

Okta 30

OneLogin 33

PingFederate 34
PingOne for Enterprise 38
Step 5: Enable SAML 2.0 integration on your WorkSpaces directory 39
Conclusion 41
Contributors 41
Further reading 42
Document revisions 42

Introduction and Requirements

Introduction

Integrating SAML 2.0 with your WorkSpaces for desktop session authentication allows your users to use their existing SAML 2.0 identity provider (IdP) credentials and authentication methods through their default web browser. By using your IdP to authenticate users for WorkSpaces, you can protect WorkSpaces by employing IdP features like multi-factor authentication and contextual access policies.

This guild walks you through the process of setting up SAML 2.0 authentication in your WorkSpaces environment. It contains both general guidance as well as IdP specific instructions. If your IdP is included, you may skip directly to that section in steps 1 and 4. You will learn how to create the trust between your IdP and AWS and create the required AWS Identity and Access Management roles and policies. You will then learn how to configure your identity provider for WorkSpaces. Finally, you will learn how to enable SAML 2.0 authentication on your WorkSpaces directory.

Requirements

- SAML 2.0 for WorkSpaces is being configured in a supported region. See official service documentation for a complete list.
- To use SAML 2.0 authentication with WorkSpaces, the IdP must support unsolicited IdP-initiated SSO with a deep link target resource or relay state endpoint URL. Examples of IdPs include ADFS, Azure AD, Duo Single Sign-On, JumpCloud, Keycloak, Okta, PingFederate, and PingOne for Enterprise. Consult your IdP documentation for more information.
- SAML 2.0 authentication will function with WorkSpaces launched using Simple AD, but this isn't recommended as Simple AD doesn't integrate with SAML 2.0 IdPs.
- SAML 2.0 authentication is supported on the following WorkSpaces clients. Open Amazon WorkSpaces Client Downloads to find the latest versions. Other client versions won't be able to connect to WorkSpaces enabled for SAML 2.0 authentication unless fallback is enabled. For more information, see Enable SAML 2.0 authentication on the WorkSpaces directory:
    - Windows client application version 5.1.0.3029 or later
    - macOS client version 5.x or later
    - Web Access

Prerequisites

Complete the following prerequisites before configuring your SAML 2.0 identity provider (IdP) connection to a WorkSpaces directory.

- Configure your IdP to integrate user identities from the Microsoft Active Directory that is used with the WorkSpaces directory. For a user with a WorkSpace, the **sAMAccountName** and **email** attributes for the Active Directory user and the IdP user must match for the user to sign in to WorkSpaces using the IdP. For more information about integrating Active Directory with your IdP, consult your IdP documentation.
- Configure your IdP to establish a trust relationship with AWS.
    - See Integrating third-party SAML solution providers with AWS for more information on configuring AWS federation. Relevant examples include IdP integration with AWS IAM to access the AWS management console.
    - Use your IdP to generate and download a federation metadata document that describes your organization as an IdP. This signed XML document is used to establish the relying party trust. Save this file to a location that you can access from the IAM console later.
- Create or register a directory for WorkSpaces by using the WorkSpaces management console. For more information, see Manage directories for WorkSpaces. SAML 2.0 authentication for WorkSpaces is supported for the following directory types:
    - AD Connector
    - AWS Managed Microsoft AD
- Create a WorkSpace for a user who can sign in to the IdP using a supported directory type. You can create a WorkSpace using the WorkSpaces management console, AWS CLI, or WorkSpaces API. For more information, see Launch a virtual desktop using WorkSpaces.

Step 1: Generate SAML 2.0 metadata manifest in your identity provider

Before you can create an IAM SAML identity provider, you need the SAML metadata document that you get from your identity provider. This document includes the information to setup a trust relationship between the IdP and AWS. For more information, see Creating and managing a SAML identity provider (Amazon Web Services Management Console). For information about working with SAML IdPs in AWS GovCloud (US-West), see AWS Identity and Access Management in the AWS GovCloud (US) User Guide.

To generate the required metadata document, follow the instructions below for your identity provider. If your identity provider is not listed, please check with your provider's documentation.

Note: When defining sign-in endpoints, it is requisite to use the correct region-specific endpoint. Please refer to https://docs.aws.amazon.com/general/latest/gr/signin-service.html to see a list of all the service endpoints.

ADFS

In this step you download the Active Directory Federation Services (ADFS) metadata file unique to your environment. The metadata file is a signed document that is used later in this guide to establish the relying party trust. Do not edit or reformat this file.

1. Log into your ADFS server.
2. Navigate to the following location, replace <ADFS_HOSTNAME> with your ADFS server name:

```
https://<ADFS_HOSTNAME>/FederationMetadata/2007-
06/FederationMetadata.xml
```

3. Download the XML file to your desktop. This file will be used in Step 2.

Auth0

In this step you create a generic Auth0 SAML 2.0 application for WorkSpaces and download the associated metadata file. You will finish the configuration in a later step.

1. Log into your Auth0 administrative portal.
2. Choose **Applications**, then **Applications**.
3. Choose **+ Create Application** and select S**ingle page application**.
4. Enter a name for the application and choose S**ave Changes**.
5. Select the **Addons** tab, then enable **SAML2 Web App**.
6. Select the new SAML2 Web App.
7. On the **Settings** tab, for **Application Callback URL**, enter `https://signin.aws.amazon.com/saml`.
8. For **Settings**, enter the following JSON code:

```
{
  "audience": "https://signin.aws.amazon.com/saml",
  "mappings": {
    "email":
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/sAMAccountNa
me",
```

```
    "name":
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
  },
  "createUpnClaim": false,
  "passthroughClaimsWithNoMapping": false,
  "mapUnknownClaimsAsIs": false,
  "mapIdentities": false,
  "nameIdentifierFormat": "urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent",
  "nameIdentifierProbes": [
    "http://schemas.auth0.com/sAMAccountName"
  ]
}
```

9. Scroll to the bottom, select S**ave** then **Enable**.
10. On the **Usage** tab, next to **Identity Provider Metadata**, choose **Download** to save the metadata XML file. This file will be used in Step 2.

Azure AD

In this step you create a generic Azure Enterprise Application SAML 2.0 application for WorkSpaces and download the associated metadata file. You will finish the configuration in Azure AD in a later step.

1. In your Azure Admin Directory admin center, choose **Enterprise applications**.
2. Choose **+ New Application**.
3. Choose **+ Create your own application**.
4. For **What's the name of your app?**, enter `WorkSpaces`.
5. For **What are you looking to do with your application?**, select **Integrate any other application you don't find in the gallery (Non-gallery).**
6. Choose **Create**.
7. When the app is created, in the **Manage** section, choose **Single sign-on**.
8. Select **SAML**.
9. For **Identifier (Entity ID)** enter `urn:amazon:webservices`.
10. For **Reply URL (Assertion Consumer Service URL)** enter `https://signin.aws.amazon.com/saml`.

11. In the **SAML Certificates** section, download the **Federation Metadata XML** file for your application. If there is no download link, create a certificate by choosing the pencil icon and then **New Certificate**. This file will be used in Step 2.

Duo Single Sign-On

In this step you create a generic Duo SAML 2.0 application for WorkSpaces and download the associated metadata file. You will finish the configuration in Duo in a later step.

1. Log into your Duo administrative portal.
2. Choose **Applications** then **Protect an Application**.
3. Enter `Generic SAML` in the search box and choose **Protect** next to **Generic SAML Service Provider**.
4. In the **Downloads** section, choose **Download XML**. Save the .xml to your desktop. This file will be used in Step 2.
5. In the **Service Provider** section, for **Entity ID**, enter `urn:amazon:webservices`.
6. For **Assertion Consumer Service (ACS) URL**, enter `https://signin.aws.amazon.com/saml`.
7. In the **Settings** section, enter a **Name** for the application.
8. Choose **Save** to complete the preliminary setup. We will complete the SAML configuration after the required components are setup within AWS IAM.

JumpCloud

In this step you create a generic SAML 2.0 application tile for WorkSpaces and download the associated metadata file. You will finish the configuration in JumpCloud in a later step.

1. Create an SSO application in JumpCloud.
2. Navigate to the SSO option on the left tab menu, select **Get Started**.
3. Choose **Custom SAML App** at the bottom of the page. Give the application a Name, Description and add a Logo if needed.
4. Under **Single Sign-On Configuration**, add the values below and select **Activate**.
    - For **IdP Entity ID**, enter `urn:amazon:webservices`.

- For **SP Entity ID**, enter `urn:amazon:webservices`.
- For **ACS URLs**, enter `https://signin.aws.amazon.com/saml`.

5. Select the created application, choose the **SSO** tab and select **Export Metadata**. This will download an XML file. This file will be used in Step 2.

Keycloak

In this step you create a generic Keycloak SAML 2.0 client for WorkSpaces and download the associated SAML 2.0 Identity Provider metadata file for the Keycloak Realm. You will finish the configuration in Keycloak in a later step.

1. Log into the Keycloak admin console.
2. Under the **Master** real drop-down list, select **Create Realm**. (A realm is a space where you manage users, applications, roles, and groups.)
3. Enter a **Realm name**: `AWS`.
4. Select **Clients**, then **Create Client**.

   - For **Client type**, select **SAML**.
   - For **Client ID**, enter `urn:amazon:webservices`.
   - For **Name**, enter `WorkSpaces`.
   - For **Description**, enter a description of your choice.

5. Choose **Next**.
6. Select **Clients**, then **Create Client**.

   - For **Root URL**, enter the hostname of you Keycloak server with port 8080. (`https://hostname:8080`)
   - For **Home URL**, enter `realms/AWS/protocol/saml/client/WorkSpaces`. This should match the realm and client names configured in the previous steps.
   - For **idP-initiated SSO URL name**, enter `WorkSpaces`.
   - For **Master SAML Processing URL**, enter `https://signin.aws.amazon.com/saml`.

7. Select **Ream Settings**.
8. On the **General** tab, select **SAML 2.0 Identity Provider Metadata** to download metadata file. This file will be used in Step 2.

Okta

In this step you create a generic Okta SAML 2.0 application tile for WorkSpaces and download the associated metadata file. You will finish the configuration in Okta in a later step.

1. Log into your Okta administrative portal.
2. Choose **Applications** then **Applications**.
3. Choose **Create App Integration**.
4. Select **SAML 2.0** and choose **Next**.
5. Enter an **App name** and choose **Next**.
6. For **Single sign on URL**, enter `https://signin.aws.amazon.com/saml`.
7. For **Audience URL (SP Entity ID)**, enter `urn:amazon:webservices`.
8. Choose **Next**.
9. Select **I'm an Okta customer adding an internal app**.
10. Choose **Finish**.
11. Choose the **Sign On** tab, then under **SAML Setup** choose **View SAML setup instructions**.
12. Under **Optional**, select all of the XML inside the box, paste into a text editor, and save as an XML file on your desktop for later. This file will be used in Step 2.

OneLogin

In this step you create a generic OneLogin SAML 2.0 application tile for WorkSpaces and download the associated metadata file. You will finish the configuration in OneLogin in a later step.

1. Login into your OneLogin administrative portal.
2. Choose **Applications** and then select **Applications**.
3. Choose **Add App**.
4. Search **for SAML Custom Connector (Advanced)** and then select it.
5. Enter a display name for the application, add description and choose **Save**.
6. Choose **Configuration**.
7. For **Audience (EntitiyID)**, enter `urn:amazon:webservices`.
8. For **Recipient**, enter `https://signin.aws.amazon.com/saml`.

9. For **ACS (Consumer) URL Validator***, enter `^https:\/\/signin\.aws\.amazon\.com\/saml$`.
10. For **ACS (Consumer) URL***, enter `https://signin.aws.amazon.com/saml`.
11. Select **Sign SLO Request** and **Sign SLO Response**.
12. Choose **Save**.
13. Choose **More Actions** and then **SAML Metadata**.
14. Metadata XML file will be downloaded. This file will be used in Step 2.

PingFederate

In this step you create a generic PingFederate SAML 2.0 application for WorkSpaces and download the associated metadata file. You will finish the configuration in PingFederate in a later step.

NOTE: If you are enabling certificate-based authentication, and an LDAP authentication source is used, ensure the additional Binary attribute `objectSid` is included (Data Store) with 'Attribute Encoding Type' set to `SID` in **IdP Adapters**.

1. Log into your PingFederate administrative portal.
2. Choose **SP Connections**.
3. Choose **Creation Connection**.
4. Choose the connection type **Browser SSO Profiles** and leave the default for SAML 2.0.
5. Select the Metadata URL for AWS and choose **Load Metadata**.
6. For **Partner's Entity ID**, enter `urn:amazon:webservices`.
7. For **Connection Name**, enter `urn:amazon:webservices`.
8. In the **Configure Browser SSO** section, select both **IDP-Initiated SSO** and **SP-Initiated SSO**.
9. Leave the **Attribute Contract** section as is for now. We will complete the SAML attribution assignment after the required components are setup within AWS IAM.
10. In the **Adapter Instance** section, add an authentication IdP Adapter that includes attributes for mail, userPrincipalName, and username (sAMAccountname).
11. For **Assertion Consumer Service URL**, enter `https://signin.aws.amazon.com/saml`.
12. For **Allowable SAML Bindings**, unselect **Artifact**, **SOAP**, and **Redirect,** leaving only **POST** selected.
13. For **Signature Policy**, select **Always Sign Assertion** and **Sign Response As Required**.
14. Leave **Encryption Policy** set to **None**.

15. Assign the **Digital Signature Settings** for your PingFederate portal.
16. Choose **Save** in the **Summary** to complete the preliminary setup.
17. From the **Action** menu in the newly created Connection, choose the option for **Export Metadata**.
18. Choose **Export** to download the associated metadata file. This file will be used in Step 2.

PingOne for Enterprise

In this step you create a generic PingOne SAML 2.0 application for WorkSpaces and download the associated metadata file. You will finish the configuration in PingOne in a later step.

1. Log into your PingOne administrative portal.
2. Choose **My Applications** and then click the **Add Application** dropdown menu.
3. Select **New SAML Application**.
4. Enter an **Application Name**, **Application Description** and **Category**, then choose **Continue to Next Step**.
5. For **Assertion Consumer Service (ACS)**, enter `https://signin.aws.amazon.com/saml`.
6. For **Entity ID**, enter `urn:amazon:webservices`.
7. Choose **Continue to Next Step**, then **Save & Exit** to complete the preliminary setup. We will complete the SAML configuration after the required components are setup within AWS IAM.
8. From the **My Application** dashboard, select the application created and choose **Download** beside **SAML Metadata**. This file will be used in Step 2.

Step 2: Create a SAML 2.0 identity provider in AWS IAM

Next, create an IAM identity provider using the manifest .xml file generated in the previous step.

1. Navigate to the IAM console.
2. In the navigation pane, choose **Identity providers**.
3. Choose **Add provider**.
4. Ensure **SAML** is selected under **Provider type**.
5. Enter a **Provider name**.

6. Under **Metadata document**, choose **Choose file** and select the.xml file downloaded to your desktop in the previous step.
7. Choose **Add provider**.
8. Choose **View provider**.
9. Copy the provider **ARN** for use in Step 4: Configure your SAML 2.0 identity provider.
10. For Duo, Okta, and OneLogin copy the **SSO service location** for use in as the UserAccessUrl in Step 5: Enable SAML 2.0 integration on your WorkSpaces directory.

Step 3: Create a SAML 2.0 federation IAM role and policy

Next, create a SAML 2.0 federation IAM role. This step establishes a trust relationship between IAM and your organization's IdP, which identifies your IdP as a trusted entity for federation.

1. Navigate to the IAM console.
2. In the navigation pane, choose **Roles**.
3. Choose **Create role**.
4. For **Trusted entity type**, choose **SAML 2.0 federation**.
5. For **SAML 2.0-based provider**, select the SAML IdP that you created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.

> Important
>
> Do not choose either of the two SAML 2.0 access methods, **Allow programmatic access only** or **Allow programmatic and Amazon Web Services Management Console access**.

6. For **Attribute**, choose **SAML:sub_type**.
7. For **Value**, enter `persistent`. This value restricts role access to SAML user streaming requests that include a SAML subject type assertion with a value of persistent. If the SAML:sub_type is persistent, your IdP sends the same unique value for the NameID element in all SAML requests from a particular user. For more information about the SAML:sub_type assertion, see the **Uniquely identifying users in SAML-based federation section** in Using SAML-based federation for API access to AWS.
8. Choose **Next**.
9. On the **Add permissions** page, choose **Next**.

10. For **Role name**, enter a name that identifies the purpose of this role. Because multiple entities might reference the role, you can't edit the role's name once it is created.
11. (Optional) For **Role description**, enter a description for the new role.
12. (Optional) Choose **Add tags** and enter a key and value for each tag that you want to add. For more information, see Tagging IAM users and roles.
13. Review the role details and choose **Create role**.
14. Choose **View role** or select the **Role name** from the list for the role you just created.
15. Choose the **Trust relationships** tab, and then choose **Edit trust policy**.
16. Under **Edit statement**, for **1. Add actions for STS**, enter `tagsession` to filter the statement list.
17. Under **Access level - read or write**, select **TagSession**. This will add the sts:TagSession action to the trust policy.
18. Your updated policy should now appear as follows:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-
provider/IDENTITY-PROVIDER"
      },
      "Action": [
        "sts:AssumeRoleWithSAML",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "SAML:sub_type": "persistent"
        }
      }
    }
  ]
}
```

Replace `IDENTITY-PROVIDER` with the name of the SAML IdP you created in Step 1: Generate SAML 2.0 metadata manifest in your identity provider. Replace `ACCOUNT-ID-WITHOUT-HYPHENS` with your AWS account number.

19. Once complete, choose **Update policy**.

Next, embed an inline IAM policy for the role that you created. When you embed an inline policy, the permissions in that policy can't be accidentally attached to the wrong principal entity. The inline policy provides federated users with access to the WorkSpaces directory.

20. In the details for the IAM role that you created, choose the **Permissions tab**.
21. Choose **Add permissions**, then **Create inline policy**. The Create policy wizard will start.
22. In **Create policy**, choose the **JSON** tab.
23. Copy and paste the following JSON policy into the JSON window, replacing what is already there. In the following policy, `"Action": "workspaces:Stream"` is the action that provides your WorkSpaces users with permissions to connect to their desktop sessions in the WorkSpaces directory.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-
WITHOUT-HYPHENS:directory/DIRECTORY-ID",
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

Replace `REGION-CODE` with the AWS Region code where your WorkSpaces directory exists. Replace `ACCOUNT-ID-WITHOUT-HYPHENS` with your AWS account number. Replace `DIRECTORY-ID` with the WorkSpaces directory ID, which can be found in the WorkSpaces management console. For resources in AWS GovCloud (US-West), use the following format for the ARN: `arn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID`.

24. When you're done, choose **Review policy**. The Policy Validator will report any syntax errors.
25. Under **Review policy**, for **Name**, enter a name that identifies the purpose of this policy.
26. Review the policy details and choose **Create policy**.

27. Under **Summary**, copy the role **ARN** for use in Step 4: Configure your SAML 2.0 identity provider.

Step 4: Configure your SAML 2.0 identity provider

Next, configure the information that your IdP sends to AWS as SAML attributes in its authentication response. Depending on your IdP, some of these attributes may be already configured.

The following SAML attributes are generic descriptions and may be used as a guide when configuring a SAML provider not specifically described later in this section.

- **SAML Subject NameID** – The unique identifier for the user who is signing in. The value must match the WorkSpaces user name, and is typically the **sAMAccountName** attribute for the Active Directory user.
- **SAML Subject Type** (with a value set to `persistent`) – Setting the value to `persistent` ensures that your IdP sends the same unique value for the `NameID` element in all SAML requests from a particular user. Make sure that your IAM policy includes a condition to only allow SAML requests with a SAML sub_type set to `persistent`, as described in Step 2: Create a SAML 2.0 identity provider in AWS IAM.
- **`Attribute`** element with the **`Name`** attribute set to **`https://aws.amazon.com/SAML/Attributes/Role`** – This element contains one or more `AttributeValue` elements that list the IAM role and SAML IdP to which the user is mapped by your IdP. The role and IdP are specified as a comma-delimited pair of ARNs.
- **`Attribute`** element with the **`Name`** attribute set to **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** – This element contains one `AttributeValue` element that provides an identifier for the AWS temporary credentials that are issued for SSO. The value in the `AttributeValue` element must be between 2 and 64 characters long, can contain only alphanumeric characters, underscores, and **`. , + = @ -`** characters. It can't contain spaces. The value is typically an email address or a user principal name (UPN). It shouldn't be a value that includes a space, such as a user's display name.
- **`Attribute`** element with the **`Name`** attribute set to **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`** – This element contains one `AttributeValue` element that provides the email address of the user. The value must match the WorkSpaces user email address as defined in the WorkSpaces directory. Tag values may include combinations of letters, numbers, spaces, and **`_ . : / , + = @ -`** characters. For more information, see Rules for tagging in IAM and AWS STS in the IAM User Guide.

- **`Attribute`** element with the **`Name`** attribute set to **`https://aws.amazon.com/SAML/Attributes/SessionDuration`** (optional) – This element contains one `AttributeValue` element that specifies the maximum amount of time in seconds that a federated streaming session for a user can remain active before reauthentication is required. The default value is 3600 seconds (60 minutes). For more information, see the SAML SessionDurationAttribute section of the *IAM User Guide*.

> **Note**
>
> Although `SessionDuration` is an optional attribute, we recommend that you include it in the SAML response. If you don't specify this attribute, the session duration is set to a default value of 60 minutes. WorkSpaces desktop sessions are disconnected after their session duration expires.

- *(Optional) Use in environments requiring username to the Amazon WorkSpace Client as UPN in place of sAMAccountName*: **`Attribute`** element with the **`Name`** attribute set to **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName`** – This element contains one `AttributeValue` element that provides an alternative username format. Use this attribute if you have use cases that require user name formats such as `corp\username`, `corp.example.com\username`, or `username@corp.example.com` to login using the WorkSpaces client. Tag keys and values can include any combination of letters, numbers, spaces, and Tag values may include combinations of letters, numbers, spaces, and **`_ . : / , + = @ -`** characters. For more information, see Rules for tagging in IAM and AWS STS in the *IAM User Guide*. To claim `corp\username` or `corp.example.com\username` formats, replace **`\`** with **`/`** in the SAML assertion.

- *(Optional) Use when implementing certificate-based authentication for Amazon WorkSpaces*: **`Attribute`** element with the `Name` attribute set to **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`** – This element contains one `AttributeValue` element that provides the Active Directory `userPrincipalName` for the user who is signing in. The value must be provided in the format of `username@domain.com`. This parameter is used with certificate-based authentication as the Subject Alternative Name in the end user certificate. For more information, see Certificate-Based Authentication.

- *(Optional) Use when implementing certificate-based authentication for Amazon WorkSpaces*: **`Attribute`** element with the **`Name`** attribute set to **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`**– This element contains one `AttributeValue` element that provides the Active Directory security identifier (SID) for the user who is signing in. This parameter is used with certificate-based authentication to enable strong mapping to the Active Directory user. For more information, see Certificate-Based Authentication.

For more information about how to configure these elements, see Configuring SAML assertions for the authentication response in the *IAM User Guide*. For information about specific configuration requirements for your IdP, see your IdP's documentation.

ADFS

Next you return to the ADFS console to complete the configuration of the SAML application for WorkSpaces.

Configure relying party trust

1. Open ADFS console on your ADFS server.
2. In the left menu, open the context (right-click) menu for **Relying Party Trusts**, and then choose **Add Relying Party Trust**.
3. Select **Claims aware** and choose **Star**t.
4. For **Select Data Source**, **select Import data about the relying party published online or on a local network**.
5. For **Federation metadata address**, enter `https://signin.aws.amazon.com/static/saml-metadata.xml` and choose **Next**.
6. For **Display name**, enter `Amazon Web Services` and choose **Next**.
7. For **Choose Access Control Policy**, select **Permit Everyone** and choose **Next**.
8. On the Ready to Add Trust page, choose **Next**.
9. Leave the box selected to configure claims policy, and choose **Close**.

Configure the ADFS claim rules

1. Rule 1: NameID
    a. Choose **Add Rule**.

b. For **Claim rule template**, choose **Send Claims Using a Custom Rule**.

c. Choose **Next**.

d. For **Claim rule name**, enter `NameID`.

e. For **Custom rule**, enter the following claim rule:

```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]=>
issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifi
er", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value =
RegExReplace(c.Value, "@[^\n]*", ""), ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimpro
perties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent");
```

2. Rule 2: RoleSessionName

   a. Choose **Add Rule**.

   b. For **Claim rule template**, choose **Send LDAP Attributes as Claims**.

   c. Choose **Next**.

   d. For **Claim rule name**, enter `RoleSessionName`.

   e. For **Attribute store**, select **Active Directory**.

   f. In the table, for **LDAP Attribute**, select **E-Mail-Addresses**.

   g. For **Outgoing Claim Type**, enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.

   h. Choose **Finish**.

3. Rule 3: Role

   a. Choose **Add Rule**.

   b. For **Claim rule template**, choose **Send Claims Using a Custom Rule**.

   c. Choose **Next**.

   d. For **Claim rule name**, enter `Role`.

   e. For **Custom rule**, enter the following claim rule:

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role",
Value = " arn:aws:iam:: ACCOUNT-ID-WITHOUT-HYPHENS:role/ROLE-
```

```
NAME,arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/IDP-
NAME");
```

NOTE: Replace `ROLE-NAME` with the name of the role created in Step 3: Create a SAML 2.0 federation IAM role and policy. Replace `IDP-NAME` with the name of the identity provider created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.

f. Choose **Finish**.

4. Rule 4: PrincipalTag:Email

   a. Choose **Add Rule**.

   b. For **Claim rule template**, choose **Send LDAP Attributes as Claims**.

   c. Choose **Next**.

   d. For **Claim rule name**, enter `PrincipalTag-Email`.

   e. For **Attribute store**, select **Active Directory**.

   f. In the table, for **LDAP Attribute**, select **E-Mail-Addresses**.

   g. For **Outgoing Claim Type**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`.

   h. Choose **Finish**.

5. Rule 5: SessionDuration

   a. Choose **Add Rule**.

   b. For **Claim rule template**, choose **Send Claims Using a Custom Rule**.

   c. Choose **Next**.

   d. For **Claim rule name**, enter `SessionDuration`.

   e. For **Custom rule**, enter the following claim rule:

```
=> issue(Type =
"https://aws.amazon.com/SAML/Attributes/SessionDuration", Value =
"28800");
```

For **Value** enter a value between `900` and `43200` seconds. WorkSpaces desktop sessions are disconnected after their session duration expires.

   f. Choose **Finish**.

6. (Certificate-based authentication) Rule 6: PrincipalTag:UserPrincipalName

   a. Choose **Add Rule**.

b. For **Claim rule template**, choose **Send LDAP Attributes as Claims**.

c. Choose **Next**.

d. For **Claim rule name**, enter `PrincipalTag-UPN`.

e. For **Attribute store**, select **Active Directory**.

f. In the table, for **LDAP Attribute**, select **User-Principal-Name**.

g. For **Outgoing Claim Type**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`.

h. Choose **Finish**.

Generate relay state URL

You now need to generate the RelayState URL that is used in Section 5 of this guide. This URL is added to the WorkSpaces directory configuration as the UserAccessURL and directs the WorkSpaces client directly to the application you just configured in ADFS. The RelayState URL must be in URL-encoded format.

You can use this PowerShell script to generate the encoded URL and automatically copy it into your clipboard. When prompted enter the fully qualified external hostname for your ADFS server, the relay state endpoint where your WorkSpaces reside, and your WorkSpaces directory registration code.

```
cls
Add-Type -AssemblyName System.Web

#Federartion service name
$hostName = Read-Host -Prompt 'Enter fully qualified ADFS server
name'

#Relying party identifier
$rpID ="urn:amazon:webservices"

#Worskspace region
$regionRelayState = Read-Host -Prompt 'Enter WorkSpaces Relay state
endpoint'

#Worskspace registration code
$wsRegCode = Read-Host -Prompt 'Enter Amazon WorkSpaces
registration code'

$idpURL ="https://"+$hostName+"/adfs/ls/idpinitiatedsignon.aspx?"
```

```
$relayState ="https://"+$regionRelayState+"/sso-
idp?registrationCode="+$wsRegCode



#The below code is used to encode the URL
$encodedRPID = [System.Web.HttpUtility]::UrlEncode($rpID)

$encodedRelayState =
[System.Web.HttpUtility]::UrlEncode($relayState)

$doubleEncode =
[System.Web.HttpUtility]::UrlEncode('='+$encodedRPID+"&RelayState="
+$encodedRelayState)

$encodedURL = $idpURL+"RelayState=RPID"+$doubleEncode

$encodedURL | Set-Clipboard

Write-Host "The encoded RelayState URL:" $encodedURL -
ForegroundColor Green
Write-Host "The RelayState URL has been copied to your clipboard."
-ForegroundColor Cyan
```

Auth0

Next you return to the Auth0 management console to complete the configuration of the SAML application for WorkSpaces.

1. In the Auth0 console, choose **Actions** then **Library**.
2. Choose **Create Action**, then **Build from Scratch**.
3. Enter a **Name** for the action.
4. For **Trigger**, select **Login/Post Login**.
5. For **Runtime**, select **Node 18**.
6. Choose **Create**.
7. Paste the following code.

Replace APP-NAME with the name of the application created in Step 1: Generate SAML 2.0 metadata manifest in your identity provider. Replace ROLE-NAME with the name of the role created in Step 3: Create a SAML 2.0 federation IAM role and policy. Replace IDP-NAME with the name of the identity provider created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.

```
exports.onExecutePostLogin = async (event, api) => {
  if (event.client.name === "APP-NAME") {
    const awsRole = ' arn:aws:iam::ACCOUNT-ID-
WITHOUTHYPHENS:role/ROLE-NAME,arn:aws:iam::ACCOUNT-ID-
WITHOUTHYPHENS:saml-provider/IDP-NAME';
    const awsRoleSession = event.user.sAMAccountName;
    const email = event.user.emails[0];

api.samlResponse.setDestination('https://signin.aws.amazon.com/saml
');

api.samlResponse.setAttribute('https://aws.amazon.com/SAML/Attribut
es/Role', awsRole)

api.samlResponse.setAttribute('https://aws.amazon.com/SAML/Attribut
es/RoleSessionName', awsRoleSession)

api.samlResponse.setAttribute('https://aws.amazon.com/SAML/Attribut
es/PrincipalTag:Email', email)
}
return;
};
```

8. Choose **Deploy** to save the SAML configuration.
9. Navigate back to **Actions**, then choose **Flows** then **Login**.
10. On the right side, under **Add Action**, choose **Custom.**
11. Drag the custom library actions created in the previous step between **Start** and **Complete**.
12. Choose **Apply**.

Azure AD

Next you return to the Azure AD Enterprise Application console to complete the configuration of the SAML application for WorkSpaces.

1. In the Azure AD console, choose **All applications**.
2. Choose the WorkSpaces SAML service provider created in Step 1: Generate SAML 2.0 metadata manifest in your identity provider.
3. Choose **Single sign-on**.
4. In the **Basic SAML Configuration** section, for **Default Relay State**, enter `https://RELAY-STATE-URL/sso-idp?registrationCode=DIRECTORY-REGISTRATION-CODE`.

   Replace `RELAY-STATE-URL` with the appropriate relay state endpoint where your WorkSpaces exist. Replace `DIRECTORY-REGISTRATION-CODE` with the registration code for the WorkSpaces directory which will have SAML enabled on it.
5. In the **Attribute & Claims** section, under **Required claim**, select **Unique User Identifier (Name ID)**.
6. For **NameID format** select **Persistent**.
7. For **Source attribute**, select `user.onpremisessamaccountname`.
8. In the **Attributes & Claims** section, under **Additional claims**, remove the four default claims Azure AD populates by selecting the three dots next to each, and choosing **Delete**.
9. In the **Attribute & Claims** section, under **Additional claims**, create four new attributes.
10. For the first IdP Attribute, choose **+ Add new claim**.
    - For **Name**, enter `PrincipalTag:Email`.
    - For **Namespace**, `enter https://aws.amazon.com/SAML/Attributes`.
    - For **Source attribute**, choose `user.mail`.
11. For the second IdP Attribute, choose **+ Add new claim**.
    - For **Name**, enter `RoleSessionName`.
    - For **Namespace**, enter `https://aws.amazon.com/SAML/Attributes`.
    - For **Source attribute**, choose `user.userprincipalname`.
12. For the third IdP Attribute, choose **+ Add new claim**.
    - For **Name**, enter `Role`.
    - For **Namespace**, enter `https://aws.amazon.com/SAML/Attributes`.
    - For **Source attribute**, enter `arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:role/ROLE-NAME,arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/IDP-NAME`.

Replace `ROLE-NAME` with the name of the role created in Step 3: Create a SAML 2.0 federation IAM role and policy. Replace `IDP-NAME` with the name of the identity provider created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.

13. For the fourth IdP Attribute, choose **+ Add new claim**.
    - For **Name**, enter SessionDuration.
    - For **Namespace**, enter `https://aws.amazon.com/SAML/Attributes`.
    - For **Source attribute**, enter a value between `900` and `43200`. This value is the number of seconds the SAML authentication is valid for a user's session. If you do not include this attribute, the session will disconnect in 60 minutes.

Now that the application has been fully configured, you can add assign users to make it available in user's My Apps portal.

1. In the Azure AD enterprise apps console, choose **Users and groups**.
2. Choose **+ Add user/group**.
3. Select the user or group for the users with WorkSpaces.
4. Choose **Assign**.

Duo Single Sign-On

Next you return to the Duo administration console to complete the configuration of the SAML application for WorkSpaces.

1. In the Duo console, choose **Applications**.
2. Choose the WorkSpaces SAML service provider created in Step 1: Generate SAML 2.0 metadata manifest in your identity provider.
3. In the **Service Provider** section, for **Default Relay State**, enter `https://RELAY-STATE-URL/sso-idp?registrationCode=DIRECTORY-REGISTRATION-CODE`.

   Replace `RELAY-STATE-URL` with the appropriate relay state endpoint where your WorkSpaces exist. Replace `DIRECTORY-REGISTRATION-CODE` with the registration code for the WorkSpaces directory which will have SAML enabled on it.
4. In the **SAML Response** section, for **NameID format** select **urn:oasis:name:tc:SAML:1.1:nameid-format:unspecified**.
5. For **NameID attribute**, remove <Email Address> then enter `sAMAccountName`.
6. Under **Map attributes**, create two attributes:

- For the first **IdP Attribute**, enter `<Email Address>` and for **SAML Response Attribute** enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`.
- For the second **IdP Attribute**, enter `<Username>` and for **SAML Response Attribute** enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.

7. Under **Create attributes**, create two attributes:
   - For the first **Name**, enter `https://aws.amazon.com/SAML/Attributes/Role` and for **Value** enter `arn:aws:iam:: ACCOUNT-ID-WITHOUT-HYPHENS:role/ROLE-NAME,arn:aws:iam:: ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/IDP-NAME`.

     Replace `ROLE-NAME` with the name of the role created in Step 3: Create a SAML 2.0 federation IAM role and policy. Replace `IDP-NAME` with the name of the identity provider created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.
   - For the second **Name**, enter `https://aws.amazon.com/SAML/Attributes/SessionDuration` and for **Value** enter a value between `900` and `43200`. This value is the number of seconds the SAML authentication is valid for a user's session. If you do not include this attribute, the session will disconnect in 60 minutes.

Now that the application has been fully configured, you can add it to Duo Central to make it available to users.

1. In the Duo console, choose **Single Sign-On**.
2. Choose **Duo Central**, then **Add tile**.
3. Choose **Add application tile**.
4. Select the box next to the name of the WorkSpaces application created previously, then choose **Add tile**.

JumpCloud

1. Navigate to the JumpCloud administrative console. On the SSO tab, select the WorkSpaces SAML application created in step 1 of this guide.
2. Under **SP Certificate**, add the following attributes:

- SAMLSubject NameID: username (The unique identifier for the user who is signing in. The value must match the WorkSpaces user name)
- SAMLSubject NameID Format: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- Select the **Sign Assertion** box.
- Default RelayState: `https://RELAY-STATE-URL/sso-idp?registrationCode=DIRECTORY-REGISTRATION-CODE`.

  Replace `RELAY-STATE-URL` with the appropriate relay state endpoint where your WorkSpaces exist. Replace `DIRECTORY-REGISTRATION-CODE` with the registration code for the WorkSpaces directory which will have SAML enabled on it.

3. Under **Attributes**, add the following:

User Attributes:
- **https://aws.amazon.com/SAML/Attributes/RoleSessionName:** email
- **https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email:** email

Constant Attributes:
- **https://aws.amazon.com/SAML/Attributes/Role:** `arn:aws:iam:: ACCOUNT-ID-WITHOUT-HYPHENS:role/ROL-NAME,arn:aws:iam:: ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/IDP-NAME`.

  Replace `ROLE-NAME` with the name of the role created in Step 3: Create a SAML 2.0 federation IAM role and policy. Replace `IDP-NAME` with the name of the identity provider created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.

- **https://aws.amazon.com/SAML/Attributes/SessionDuration:** This is optional, but the default is 60 minutes.

Keycloak

Return to the Keycloak administration console to complete the configuration of the SAML application for Workspaces.

1. Select the **AWS** realm from the drop-down menu.
2. From the **Clients** menu, select the **WorkSpaces** client created in Step 1.
3. Navigate to the **Client Scopes** tab, select the **urn:amazon:webservices-dedicated** client scope.
4. Select **Add Mapper** from the drop-down list, choose **By Configuration**.
   - Select **Hardcoded attribute**.
   - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/Role`.

- For **SAML Attribute Name**, enter `https://aws.amazon.com/SAML/Attributes/Role`.
- For **Attribute Value**, enter `arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:role/ROLE-NAME,arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/IDP-NAME`.

  Replace `ROLE-NAME` with the name of the role created in Step 3: Create a SAML 2.0 federation IAM role and policy. Replace `IDP-NAME` with the name of the identity provider created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.
- Choose **Save**.

5. Select **Add Mapper** from the drop-down list, choose **By Configuration**.
   - Select **User Property**.
   - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`.
   - For **Property**, enter `email`.
   - For **SAML Attribute Name**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`.
   - For **SAML Attribute NameFormat**, enter `Unspecified`.
   - Choose **Save**.
6. Select **Add Mapper** from the drop-down list, choose **By Configuration**.
   - Select **User Property**.
   - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.
   - For **Property**, enter `email`.
   - For **SAML Attribute Name**, enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.
   - For **SAML Attribute NameFormat**, enter `Unspecified`.
   - Choose **Save**.

   To ensure we pass **sAMAccountName** in the **NameID** field in the SAML response create a User Federation Mapper (alternatively, you can modify the IAM role as detailed above and remove the condition to only allow SAML requests with a SAML **sub_type** set to persistent).
7. Select **User Federation**.
8. Select the LDAP provider you use to integrate Keycloak with your Active Directory.

9. Navigate to the **Mappers** tab, choose **Add Mapper**.
10. For **Name**, enter `saml.persistent.name.id.for.urn:amazon:webservices`.
11. For **LDAP Attribute**, enter `sAMAccountName`.
12. Choose **Save**.

Okta

Next you return to the Okta administration console to complete the configuration of the SAML application for WorkSpaces.

1. In the Okta console, choose **Applications** then **Applications** again.
2. Choose the WorkSpaces SAML app created in Step 1: Generate SAML 2.0 metadata manifest in your identity provider.
3. Choose the **General** tab.
4. Under **SAML Settings**, choose **Edit**.
5. Choose **Next**.
6. For **Default Relay State**, enter `https://RELAY-STATE-URL/sso-idp?registrationCode=DIRECTORY-REGISTRATION-CODE`.

   Replace `RELAY-STATE-URL` with the appropriate relay state endpoint where your WorkSpaces exist. Replace `DIRECTORY-REGISTRATION-CODE` with the registration code for the WorkSpaces directory which will have SAML enabled on it.
7. For **Name ID format**, select **Persistent**.
8. For **Application username**, select **AD SAM account name**.
9. Under **Attributes Statements (optional),** choose **Add Another** 3 times. There should now be four rows to configure four attributes.
10. Configure the first attribute:
    - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`.
    - For **Name Format**, select **Unspecified**.
    - For **Value**, enter `user.email`.
11. Configure the second attribute:

- For **Name**, enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.
- For **Name Format**, select **URI Reference**.
- For **Value**, enter `userName`.

12. Configure the third attribute:
    - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/Role`.
    - For **Name Format**, select **URI Reference**.
    - For **Value** enter `arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:role/ROLE-NAME,arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/IDP-NAME`.

    Replace `ROLE-NAME` with the name of the role created in Step 3: Create a SAML 2.0 federation IAM role and policy. Replace `IDP-NAME` with the name of the identity provider created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.
13. Configure the fourth attribute:
    - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/SessionDuration`.
    - For **Name Format**, select **Basic**.
    - For **Value** enter a value between `900` and `43200`.This value is the number of seconds the SAML authentication is valid for a user's session. If you do not include this attribute, the session will disconnect in 60 minutes.
14. Choose **Next**.
15. Choose **Finish**.
16. Now that the application has been fully configured, you can make it available to users. Choose the **Assignment** tab.
17. Choose **Assign**, then **Assign to People** or **Assign to Groups** based on your organization's needs.

If you are not enabling certificate-based authentication on your WorkSpaces directory, you may skip the following steps and move on to Step 5: Enable SAML 2.0 integration on your WorkSpaces directory.

18. In the Okta console, choose **Directory** then **Profile Editor**.
19. Under **Profile** choose **User (default)**.
20. Under **Attributes**, choose **+ Add Attribute**.
    - For **Display name**, enter `wsp_sid`.

- For **Variable name**, enter `wsp_sid`.
- For **Attribute length**, select **Greater than** and enter `1`.
- Select **Attribute required**.
- Choose **Save**.

21. In the Okta console, choose **Directory** then **Profile Integrations**.
22. Choose the active Active Directory source name.
23. Choose the **Provisioning** tab.
24. Under **Settings**, choose **To Okta**.
25. Under **Okta Attribute Mappings**, choose the pencil icon next to `wsp_sid` to edit the mapping.
26. For **Attribute value**, select **Map from *your_domain* Profile**.
27. Select **objectSid | string**.
28. Choose **Save**.
29. Under **Okta Attribute Mappings**, choose **Force Sync** to have the new attribute mapping populated for users.
30. In the Okta console, choose **Applications** then **Applications** again.
31. Choose the WorkSpaces SAML app created in Step 1: Generate SAML 2.0 metadata manifest in your identity provider.
32. Choose the **General** tab.
33. Under **SAML Settings**, choose **Edit**.
34. Choose **Next**.
35. Under **Attributes Statements (optional),** choose **Add Another** 2 more times. There should now be two new rows to configure two more attributes.
36. Configure the first attribute:
    - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`.
    - For **Name Format**, select **URI Reference**.
    - For **Value**, enter `appuser.wsp_sid`.
37. Configure the second attribute:

- For **Name**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`.
- For **Name Format**, select **URI Reference**.
- For **Value**, enter `user.login`.

38. Choose **Next**.
39. Choose **Finish**.

OneLogin

Next you return to the OneLogin administration console to complete the configuration of the SAML application for WorkSpaces.

1. In the OneLogin Admin console, choose **Applications** then **Applications** again.
2. Choose the WorkSpaces SAML app created in Step 1: Generate SAML 2.0 metadata manifest in your identity provider.
3. Choose the **Configuration** tab.
4. For **Relay State**, enter `https://RELAY-STATE-URL/sso-idp?registrationCode=DIRECTORY-REGISTRATION-CODE`.

   Replace `RELAY-STATE-URL` with the appropriate relay state endpoint where your WorkSpaces exist. Replace `DIRECTORY-REGISTRATION-CODE` with the registration code for the WorkSpaces directory which will have SAML enabled on it.
5. For **SAML nameID format**, select **Persistent**.
6. For **SAML signature element**, select **Both**.
7. Choose the **Parameters** tab.
8. Under **SAML Custom Connector (Advanced) Field**, select existing **Name ID** attribute, modify the value to be `AD sAMAccountName` and choose **Save**.
9. Configure the second attribute by selecting the **(+)** option.
   - For **Field Name**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`.
   - Select **Include in SAML assertion**, and choose **Save**.
   - For **Value**, select **Email** and choose **Save**.
10. Configure the third attribute by selecting the **(+)** option.

- For **Field Name**, enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.
- Select **Include in SAML assertion**, and choose **Save**.
- For **Value**, select **UserName** and choose **Save**.

11. Configure the fourth attribute by selecting the **(+)** option.
    - For **Field Name**, enter `https://aws.amazon.com/SAML/Attributes/Role`.
    - Select **Include in SAML assertion**, and choose **Save**.
    - For **Value**, choose **-Macro-**.
    - For **Value field**, enter `arn:aws:iam:: ACCOUNT-ID-WITHOUT-HYPHENS:role/ROLE-NAME,arn:aws:iam:: ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/IDP-NAME`.

      Replace `ROLE-NAME` with the name of the role created in Step 3: Create a SAML 2.0 federation IAM role and policy. Replace `IDP-NAME` with the name of the identity provider created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.
    - Choose **Save**.
12. Configure the fifth attribute by selecting the **(+)** option.
    - For **Field Name**, enter `https://aws.amazon.com/SAML/Attributes/SessionDuration`.
    - Select **Include in SAML assertion**, and choose **Save**.
    - For **Value**, choose **-Macro-**.
    - For **Value field**, enter a value between `900` and `43200`. This value is the number of seconds the SAML authentication is valid for a user's session. If you do not include this attribute, the session will disconnect in 60 minutes.
    - Choose **Save**.
13. Save all the Configuration and Parameter settings by choosing **Save**.

PingFederate

Next you return to the PingFederate administration console to complete the configuration of the SAML application for WorkSpaces.

1. In the PingFederate administrative console, choose **SP Connections**.

2. Choose the **Connection** for the WorkSpaces SAML app created in Step 1: Generate SAML 2.0 metadata manifest in your identity provider.
3. Scroll down the Summary and choose the **Attribute Contract** section.
4. Configure the first attribute:
    - For **Contract**, enter `SAML_SUBJECT`.
    - For **Name Format**, select **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**.
5. Configure the first extended attribute:
    - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`.
    - For **Name Format**, select **urn:oasis:names:tc:SAML:2.0:attrname-format:basic**.
6. Configure the second extended attribute:
    - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.
    - For **Name Format**, select **urn:oasis:names:tc:SAML:2.0:attrname-format:basic**.
7. Configure the third extended attribute:
    - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/Role`.
    - For **Name Format**, select **urn:oasis:names:tc:SAML:2.0:attrname-format:basic**.
8. Configure the fourth extended attribute:
    - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/SessionDuration`.
    - For **Name Format**, select **urn:oasis:names:tc:SAML:2.0:attrname-format:basic**.
9. Configure the fifth extended attribute:
    - For **Name**, enter `SAML_NAME_FORMAT`.
    - For **Name Format**, select **urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified**.
10. (Optional) Configure an optional sixth extended attribute. Use in environments requiring the username passed to the Amazon WorkSpace Client as UPN in place of sAMAccountName
    - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUsername`.
    - For **Name Format**, select **urn:oasis:names:tc:SAML:2.0:attrname-format:basic**.
11. (Certificate-based authentication) Configure the optional extended attribute for certificate-based authentication:

- For **Name**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`.
- For **Name Format**, select **urn:oasis:names:tc:SAML:2.0:attrname-format:basic**.

12. (Certificate-based authentication) Configure the additional optional extended attribute for certificate-based authentication:
    - For **Name**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`.
    - For **Name Format**, select **urn:oasis:names:tc:SAML:2.0:attrname-format:basic**.
13. Choose **Next** to proceed to the **IdP Adapter Mapping** section.
14. Configure the first attribute:
    - For **Attribute Contract**, enter `SAML_NAME_FORMAT`.
    - For **Source**, select **Text**.
    - For **Value**, enter `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.
15. Configure the second attribute:
    - For **Attribute Contract**, enter `SAML_SUBJECT`.
    - For **Source**, select **Adapter**.
    - For **Value**, select **username**.
16. Configure the third attribute:
    - For **Attribute Contract**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`.
    - For **Source**, select **Adapter**.
    - For **Value**, select **mail**.
17. Configure the fourth attribute:
    - For **Attribute Contract**, enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.
    - For **Source**, select **Adapter**.
    - For **Value**, select **userPrincipalName.**
18. Configure the fifth attribute:

- For **Attribute Contract**, enter `https://aws.amazon.com/SAML/Attributes/Role`.
- For **Source**, select **Text**.
- For **Value** enter `arn:aws:iam:: ACCOUNT-ID-WITHOUT-HYPHENS:role/ROLE-NAME,arn:aws:iam:: ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/IDP-NAME`.

  Replace `ROLE-NAME` with the name of the role created in Step 3: Create a SAML 2.0 federation IAM role and policy. Replace `IDP-NAME` with the name of the identity provider created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.

19. Configure the sixth attribute:
    - For **Attribute Contract**, enter `https://aws.amazon.com/SAML/Attributes/SessionDuration`.
    - For **Source**, select **Text**.
    - For **Value** enter a value between `900` and `43200`. This value is the number of seconds the SAML authentication is valid for a user's session. If you do not include this attribute, the session will disconnect in 60 minutes.
20. (Optional) Configure the optional attribute:
    - For **Attribute Contract**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUsername`.
    - For **Source**, select **Adapter**.
    - For **Value**, select **userPrincipalName**.
21. (Certificate-based authentication) Configure the optional attribute for certificate-based authentication:
    - For **Attribute Contract**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`.
    - For **Source**, select **Adapter**.
    - For **Value**, select **userPrincipalName**.
22. (Certificate-based authentication) Configure the additional optional attribute for certificate-based authentication:
    - For **Attribute Contract**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`.

- For **Source**, select **Adapter**.
- For **Value**, select **objectSid**.

23. Choose **Save**.

PingOne for Enterprise

Next you return to the PingOne administration console to complete the configuration of the SAML application for WorkSpaces.

1. In the PingOne administrative console, select **Applications**.
2. From the **My Applications** tab select the Workspaces SAML application created in step 1 of this guide and choose **Edit**.
3. Choose **Continue to Next Step** to take you to the **Application Configuration** page.
4. For **Application URL**, enter `https://RELAY-STATE-URL/sso-idp?registrationCode=DIRECTORY-REGISTRATION-CODE`.

   Replace `RELAY-STATE-URL` with the appropriate relay state endpoint where your WorkSpaces exist. Replace `DIRECTORY-REGISTRATION-CODE` with the registration code for the WorkSpaces directory which will have SAML enabled on it.
5. Choose **Continue to Next Step**.
6. Configure the first attribute:
   - For **Application Attribute**, enter `https://aws.amazon.com/SAML/Attributes/Role`.
   - For **Identity Bridge Attribute or Literal Value**, select **As Literal**. Enter `arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:role/ROL-NAME,arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/IDP-NAME`.

     Replace `ROLE-NAME` with the name of the role created in Step 3: Create a SAML 2.0 federation IAM role and policy. Replace `IDP-NAME` with the name of the identity provider created in Step 2: Create a SAML 2.0 identity provider in AWS IAM.
7. Configure the second attribute:
   - For **Application Attribute**, enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.
   - For **Identity Bridge Attribute or Literal Value**, enter `mail`.
8. Configure the third attribute:

- For **Application Attribute**, enter `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`.
- For **Identity Bridge Attribute or Literal Value**, enter `mail`.

9. Configure the fourth attribute:
   - For **Application Attribute**, enter `https://aws.amazon.com/SAML/Attributes/SessionDuration`.
   - For **Identity Bridge Attribute or Literal Value**, enter a value between `900` and `43200`. This value is the number of seconds the SAML authentication is valid for a user's session. If you do not include this attribute, the session will disconnect in 60 minutes.
10. Configure the fifth attribute:
    - For **Application Attribute**, enter `SAML_SUBJECT`.
    - In the **Identity Bridge Attribute or Literal Value**, enter `sAMAccountName`.
    - Choose **Advanced**.
    - For **Name ID Format to send to SP**, select **urn:oasis:names:tc:SAML:2.0.nameid-format:persistent**.
11. Choose **Continue to Next Step**, then **Finish** to save changes.

Step 5: Enable SAML 2.0 integration on your WorkSpaces directory

The final step to allowing SAML authentication into WorkSpaces is to enable it on the WorkSpaces directory. Once this step is completed, you can use the IdP-initiated and client application-initiated flows to register WorkSpaces client applications and sign in to WorkSpaces.

Once SAML integration is complete, you can utilize the additional authentication factors of your IdP to provide multi-factor authentication (MFA) to your users. In most scenarios, if you were utilizing WorkSpaces RADIUS based MFA, you can revisit disabling that feature to prevent your users from being prompted for MFA more than once.

1. Navigate to the WorkSpaces console.
2. In the navigation pane, choose **Directories**.
3. Choose the **Directory ID** of the directory that will have SAML authentication enabled.
4. Under **Authentication**, choose **Edit authentication**.
5. Under **SAML 2.0 Identity Provider**, choose **Edit SAML 2.0 Identity Provider**.

6. Select **Enable SAML 2.0 authentication**.
7. Enter your **User access URL**. Typically, the user access URL is the URL a user would navigate to in their web browser to federate and directly access the application, without any SAML 2.0 service provider (SP) bindings. For many IdPs this is the SSO service location saved from the IAM console in Step 2: Create a SAML 2.0 identity provider in AWS IAM. For ADFS, this is the RelayState generated in Step 4: Configure your SAML 2.0 identity provider. Ensure the URL you enter matches the pattern below for your IdP.

Table 1 – IdP relay state parameters and URL template

Identity Provider	Parameter	UserAccessURL
ADFS	RelayState	`https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri>`
Azure AD	RelayState	`https://launcher.myapps.microsoft.com/api/signin/<app id>?tenantId=<tenant id>`
Duo	RelayState	`https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app i`
JumpCloud	RelayState	`https://sso.jumpcloud.com/saml2/<workspaces description>`
Keycloak	RelayState	`https://<fqdn>/realms/<realm name>/protocols/saml/clients/<client name>`
Okta	RelayState	`https://<sub_domain>.okta.com/app/<app_name>/<app id>/sso/saml`
OneLogin	RelayState	`https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/<app-id>`
PingFederate	TargetResource	`https://<host>/idp/startSSO.ping?PartnerSpId=<sp id>`
PingOne for Enterprise	TargetResource	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<app_id>&idpid=<idp_id>`

8. (Optional) Enter your IdP's **Relay state parameter name**. The default value is `RelayState`. Refer to the table above or your IdP's documentation if the default value does not work.
9. Choose **Test** to test the user access URL and parameter values for your IdP.

Copy and paste the test URL to a private window in your current browser or another browser to test SAML 2.0 logon without disrupting your current AWS management console session. This should result in the IdP-initiated flow, opening and registering the WorkSpaces client.

10. (Optional) Select **Allow clients that do not support SAML 2.0 to login** if you wish to allow users to bypass SAML 2.0 authentication if their client does not support it. Enable this setting if your users need to continue accessing WorkSpaces using client types or versions that do not support SAML 2.0, or if you want to get started with SAML 2.0 authentication and your users need time to upgrade to the latest client version.

    > Note: This setting allows users to bypass SAML 2.0 and login using Directory authentication using older client versions.

11. Choose **Save**. Your WorkSpaces directory is now enabled with SAML 2.0 integration. You can use the IdP-initiated and client application-initiated flows to register WorkSpaces client applications and sign in to WorkSpaces.

Conclusion

In this guide you integrated SAML 2.0 authentication with Amazon WorkSpaces. You first established the trust between AWS IAM and your identity provider. Next you configured the required IAM role and policy. Then you configured your identity provider for WorkSpaces. Last you enabled SAML authentication on your WorkSpaces directory.

Contributors

Contributors to this document include:

- Justin Grego, Sr. EUC Solutions Architect, Amazon Web Services
- Andrew DeFoe, Principal Product Manager, EUC, Amazon Web Services
- Pete Fergus, Sr. EUC Solutions Architect, Amazon Web Services
- Stephen Stetler, Sr. EUC Solutions Architect, Amazon Web Services
- Ajay Saini, EUC Solutions Architect, Amazon Web Services
- Jeremy Schiefer, Sr. Solutions Architect, Amazon Web Services
- Muni Doddala, Solutions Architect, Amazon Web Services
- Mulalo Matamela, Cloud Infrastructure Architect, Amazon Web Services

- Tushar Dhanani, Sr. EUC Solutions Architect, Amazon Web Services
- Shantanu Padhye, Sr. Cloud Support Engineer, Amazon Web Services

Further reading

For additional information, refer to:

- Amazon WorkSpaces SAML 2.0 Integration Documentation
- Amazon WorkSpaces Certificate-based Authentication Documentation
- Amazon WorkSpaces Documentation
- *Best Practices for Deploying Amazon WorkSpaces* (AWS whitepaper)

Document revisions

Date	Description
April 26, 2024	Added Auth0 as an Identity Provider
January 17, 2024	Added Keycloak as an Identity Provider
August 31, 2023	Added JumpCloud as an Identity Provider
May 16, 2023	Fixed inconsistencies between IdP steps
December 12, 2022	Added optional CBA assertions
November 18, 2022	First publication