Configuring Single Sign-on from the VMware Identity Manager Service to Amazon Web Services

VMware Identity Manager

OCTOBER 2015 V1

vmware®

Table of Contents

Overview

This document provides information about configuring SAML-based single sign-on from the VMware Identity Manager service to the Amazon Web Services Management Console.

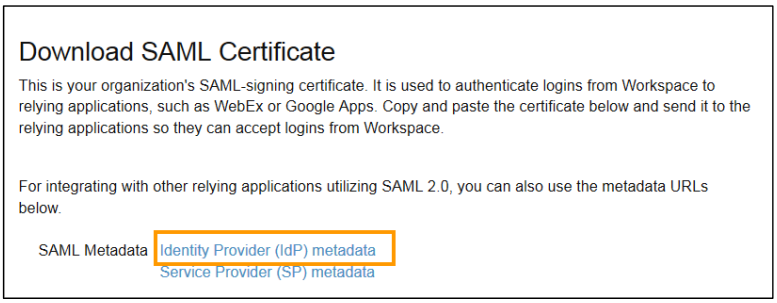
When VMware Identity Manager is configured as the identity provider for AWS, users can sign on to the AWS Management Console without you having to create an identity and access management (IAM) user in AWS for everyone in your organization. Users sign in to their VMware Identity Manager Apps Portal, select the AWS app, and they are redirected to the AWS console without having to provide additional sign on details.

You must have an administrator account for the VMware Identity Manager service, as well as an administrator account for Amazon Web Services. In AWS you, create VMware Identity Manager as a SAML provider and upload the identity provider SAML metadata file. You also create an IAM role that establishes a trust relationship between VMware Identity Manager and AWS IAM. The role also defines what users are allowed to do in AWS. In the VMware Identity Manager administration console, you add AWS to the catalog, add the values of the AWS application parameters, and entitle users to the AWS application.

Save the Identity Provider SAML Metadata

You must have the VMware identity provider metadata xml file to configure Amazon Web Services.

1. Log in to the VMware Identity Manager administration console.
2. In the Catalog tab, click **Settings > SAML Metadata**.
3. In the SAML Metadata section, click **Identity Provider (IdP) metadata** to display the metadata content. Save the metadata content as an .xml file.



Setting up Amazon Web Service for Single Sign-on

To set up AWS for single sign-on from the service, you configure VMware Identity Manager as the SAML identity provider in AWS, add the metadata xml file, and create an AWS identity and access management (IAM) single sign-on role to the AWS management console.

Find Your Amazon Web Services Account ID Number

1. Sign in to the AWS Management Console as the admin user.
2. In the upper-right on the Amazon Web Services page, click **Support > Support Center**.

The account ID number displays below the Support menu.

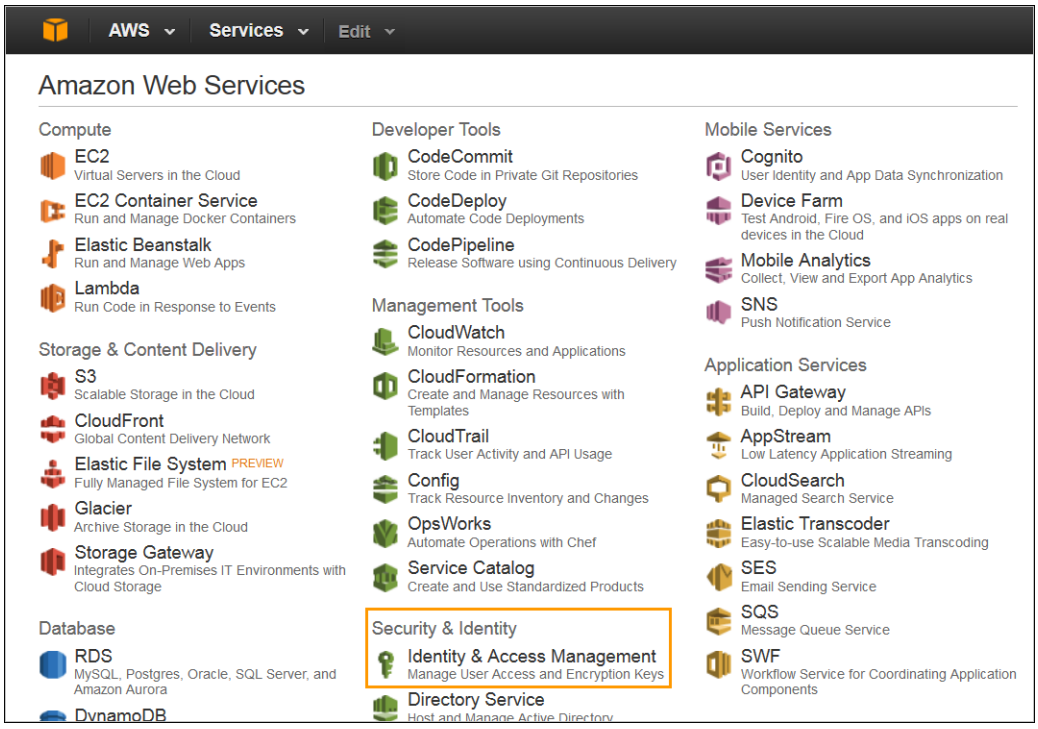
3. Copy and save the AWS account ID number.

   This account ID number is configured later in the VMware Identity Manager.

Create Identity Provider in Amazon Web Services

When you create the identity provider, you add the VMware identity provider metadata xml file that you saved earlier.

1. Sign in to the AWS Management Console as the admin user and navigate to the **Amazon Web Services > Security & Identity > Identity & Access Management** page.



2. In the Dashboard Details navigation pane, click **Identity Providers** and then click **Create Provider**.
3. From the **Provider Type > Choose a provider type** drop-down menu, select **SAML**.
4. In the **Provider Name** text box, enter a name for the identity provider.

   Remember the provider name, as it is configured in the VMware Identity Manager Catalog.
5. In the **Metadata Document** row, click **Choose File** and navigate to the SAML metadata file you saved.

Click **Open**. Click **Next Step**.

6. Verify that the information is correct and click **Create**.

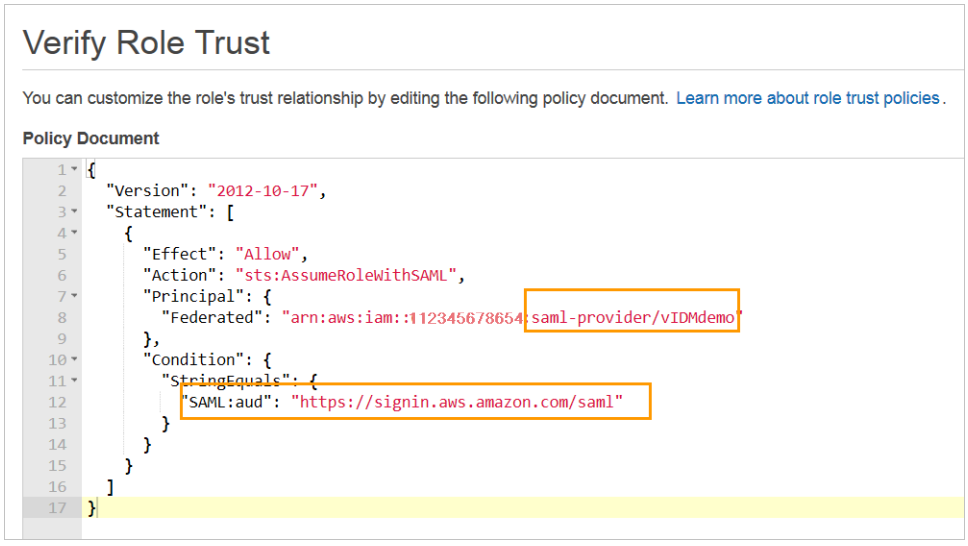
Create a Role for Identity Provider Access in Amazon Web Services

You create a role for identity provider access to permit your users to access the AWS Management Console. The role grants users permissions to carry out tasks in the AWS console.

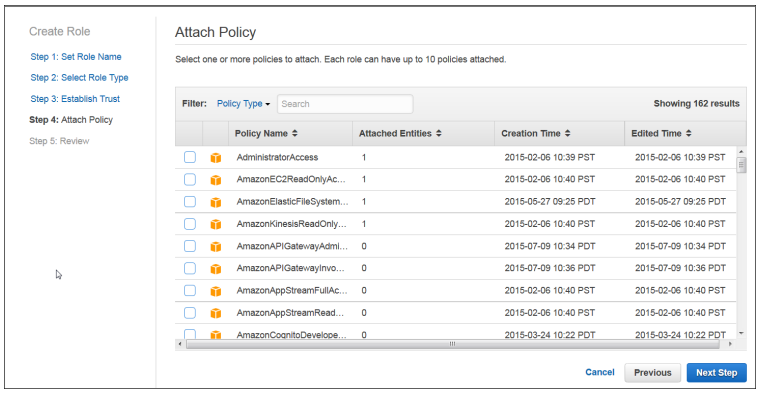
Before you create the role, the SAML provider must be created in AWS.

1. Sign in to the AWS Management Console as the admin user and navigate to the **Amazon Web Services > Security & Identity > Identity & Access Management** page.
2. In the Details navigation pane, click **Roles** and then click **Create New Role**.
3. In the **Set Role Name** page, enter the role name that can help you identify the purpose of this role. Click **Next Step**.

   Remember the role name, as it is configured in the VMware Identity Manager Catalog.
4. Click **Role for Identity Provider Access.**
5. Select **Grant Web Single Sign-On (WebSSO) access to SAML providers**.
6. Select the SAML identity provider you created in AWS. Click **Next Step**.
7. The trust policy for the role displays showing the SAML identity provider you created previously along with the SAML attributes that a user must match to assume the role. Review the policy that was created to verify the information. You can edit this page. Click **Next Step**.



8. Select the AWS access policies users inherit when using this role.



9. Review the settings and click **Create Role**.

Next you configure AWS in the VMware Identity Manager catalog.

Adding Amazon Web Services to VMware Identity Manager Catalog

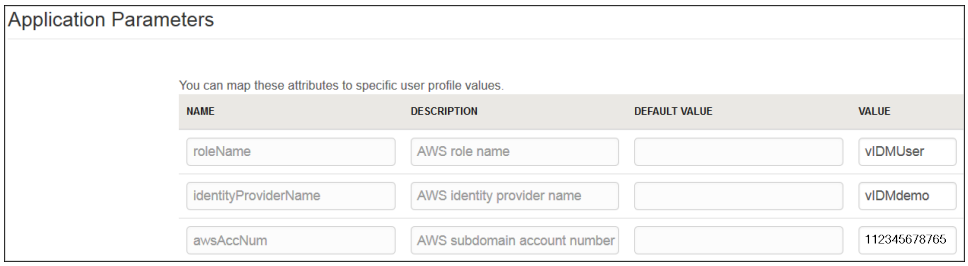
To configure AWS in VMware, make sure you have the following AWS information.

- AWS account number saved from Step 2 when you set up the SAML identity provider in AWS
- SAML identity provider name you configured in AWS
- The name of the role you created in AWS

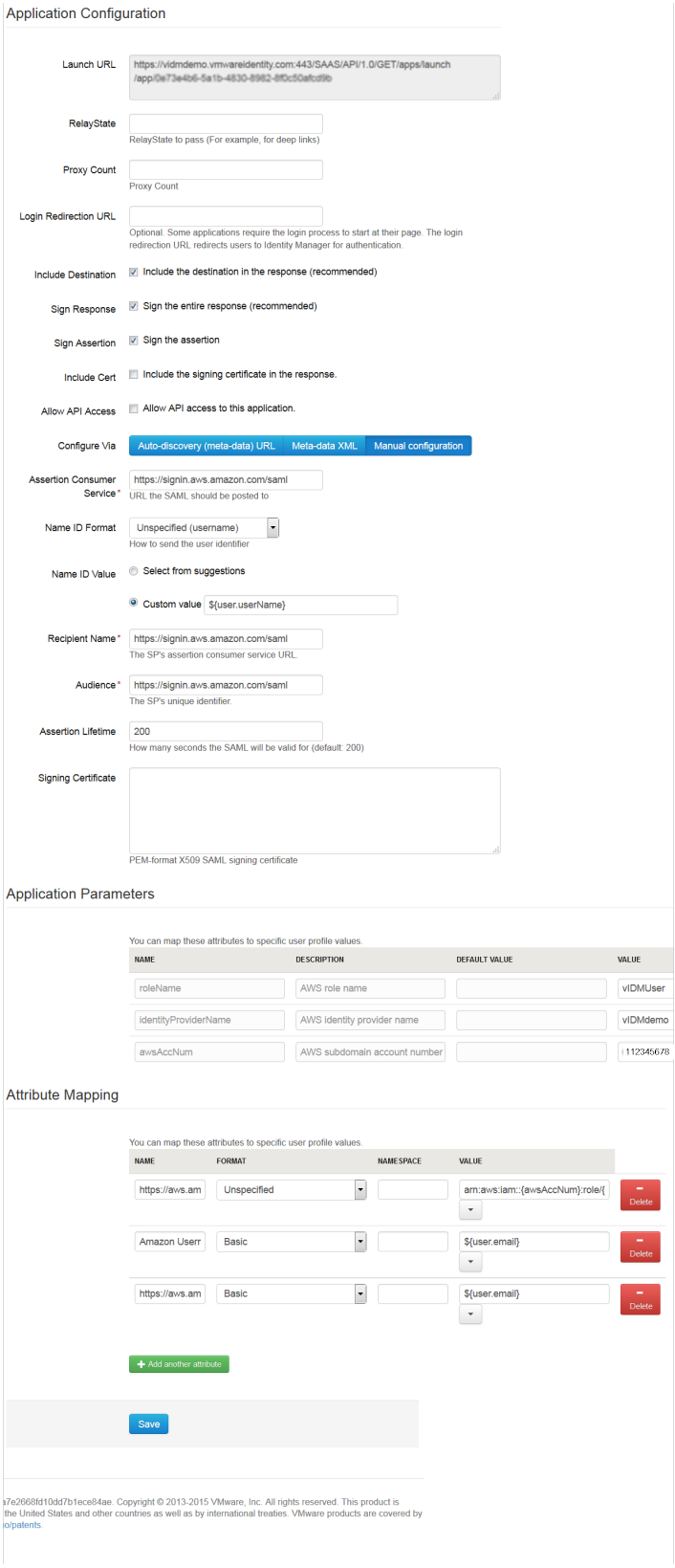
Add Amazon Web Services to the Catalog

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Add Application > ...from the cloud application catalog**.
3. Click the **Amazon Web Services** icon.

   The modify application page appears.
4. Click **Configuration**.
5. In the Application Parameters section map the attributes in the name column with the AWS profile. Enter the name of the role, the SAML identity provider name and the AWS account number.



6. Click **Save**.


Application Configuration
Launch URL
https://vidmdemo.vmwareidentity.com:443/SAAS/API/1.0/GET/apps/launch
/app/0e73e4b6-5a1b-4830-8962-8f0c50afcd9b
RelayState
RelayState to pass (For example, for deep links)
Proxy Count
Proxy Count
Login Redirection URL
Optional. Some applications require the login process to start at their page. The login redirection URL redirects users to Identity Manager for authentication.
Include Destination
Include the destination in the response (recommended)
Sign Response
Sign the entire response (recommended)
Sign Assertion
Sign the assertion
Include Cert
Include the signing certificate in the response.
Allow API Access
Allow API access to this application.
Configure Via
Auto-discovery (meta-data) URL
Meta-data XML
Manual configuration
Assertion Consumer Service *
https://signin.aws.amazon.com/saml
URL the SAML should be posted to
Name ID Format
Unspecified (username)
How to send the user identifier
Name ID Value
Select from suggestions
Custom value
${user.userName}
Recipient Name *
https://signin.aws.amazon.com/saml
The SP's assertion consumer service URL.
Audience *
https://signin.aws.amazon.com/saml
The SP's unique identifier.
Assertion Lifetime
200
How many seconds the SAML will be valid for (default: 200)
Signing Certificate
PEM-format X509 SAML signing certificate
Application Parameters
You can map these attributes to specific user profile values.
NAME
DESCRIPTION
DEFAULT VALUE
VALUE
roleName
AWS role name
vIDMUser
identityProviderName
AWS identity provider name
vIDMdemo
awsAccNum
AWS subdomain account number
112345678
Attribute Mapping
You can map these attributes to specific user profile values.
NAME
FORMAT
NAMESPACE
VALUE
https://aws.am
Unspecified
arn:aws:iam::{awsAccNum}:role/{
Delete
Amazon Userr
Basic
${user.email}
Delete
https://aws.am
Basic
${user.email}
Delete
Add another attribute
Save
b7e2668fd10dd7b1ece84ae. Copyright © 2013-2015 VMware, Inc. All rights reserved. This product is
the United States and other countries as well as by international treaties. VMware products are covered by
o/patents.

Testing Single Sign-on Configuration

Test your single sign-on configuration with a small number of users before deploying the application across your organization.

Set up User in VMware Identity Manager for Testing

1. Log in to the VMware Identity Manager administration console.
2. In the **Users & Groups** page, click **Users** and ensure that the user you are testing is in the list of users.
3. In the **Catalog** page, click on the **Amazon Web Services** application.
4. Click **Entitlements**.
5. Click +**Add user entitlement**.
6. Select the test user and change the **DEPLOYMENT** field value for the user to **Automatic**. For example:

7. Click **Save**, then click **Done**.
8. In the top-right corner of the page, click your user name and select **Logout**.

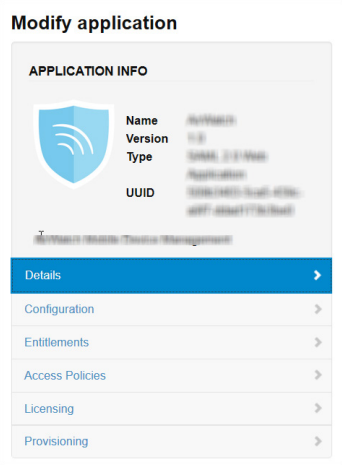
Verify Test-User can Sign into Amazon Web Services

1. Sign in to the user portal as the test user.
2. Click the **Amazon Web Services** icon on the My Apps page.

   You should now have single sign-on access to Amazon Web Services.

Completing the Configuration in the Catalog

In addition to configuring the Web application for single sign-on to the service, you can configure additional settings to add an access policy, set up app licensing requirements, and entitle users and groups to the app.



Entitlements After you configure a Web application, you can add group entitlements and entitle individual users to the Web app.

Access Policies The VMware Identity Manager service includes a default policy that is automatically assigned to the Web app when you add the app to the Catalog. If you do not want to use the default access policy, create a new access policy and in the Access Policies link, select the access policy to use for this Web application.

For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required. See the VMware Identity Manager documentation at http://pubs.vmware.com.

Licensing Licensing can be used to require users to request license approval before they can access the application. You can add additional information, including pricing, license type, cost per license and the number of licenses. You can run the Resource Usage report to see the licensing information for the application.

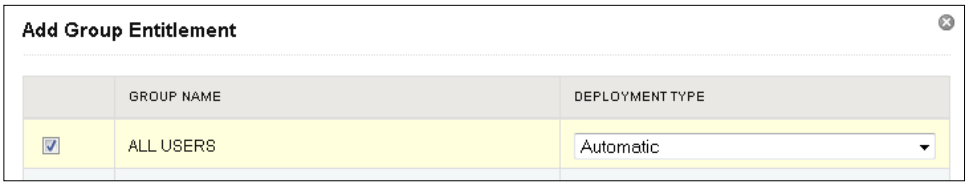
Provisioning Provisioning provides automatic application user-management from a single location. Provisioning adapters allow the Web application to retrieve specific information from VMware Identity Manager, as required. The provisioning adapters that can be selected are either Google Apps, Mozy, or Vchs. If you configure these applications, you can select the appropriate provisioning adapter.

Entitle Users to Amazon Web Services

You can activate single sign-on for all users. Before you do so, ensure that all the user accounts are provisioned in Amazon Web Services.

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Amazon Web Services**.
3. In the **Modify application** page, click **Entitlements**.
4. Click +**Add group entitlement**.

5. Select **ALL USERS** and change the **DEPLOYMENT TYPE** field value to **Automatic**.



6. Click **Save,** then click **Done**.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com