Implementation Guide:

Okta & AWS Control Tower Configuration with AWS SSO

November 2020
Table of Contents

Foreword ............................................................................................................................. 3
Solution overview and features ....................................................................................... 4
Architecture diagram ....................................................................................................... 4
Pre-requisites ................................................................................................................... 5
Subscribe to Okta from AWS Marketplace ..................................................................... 6
Configure Okta with AWS SSO & AWS Control Tower for Single Sign-On ..................... 8
  Configure AWS CLI for Federated Authentication with Okta ...................................... 13
  Configure Okta with AWS SSO and AWS Control Tower for User and Group Provisioning .............................................................. 15
Solution Estimated Pricing ............................................................................................ 18
FAQs ............................................................................................................................... 18
Additional resources ..................................................................................................... 18
Partner contact information ............................................................................................ 18
Foreword

Okta is an Identity and Access Management (IAM) platform that enables teams to manage access and entitlements on the AWS cloud with AWS Single Sign-on (AWS SSO).

Implementing this solution, Okta allows you to securely and centrally manage identity and access by providing federated SSO to AWS Control Tower and AWS Management Console, federated authentication for AWS Command Line Interface (AWS CLI), and automatic provisioning using the System for Cross-domain Identity Management (SCIM) v2.0 protocol.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure Okta in AWS Control Tower environment while taking full advantage of the resources pre-configures by AWS Control Tower as part of the initialization.
Solution overview and features

Okta is a modern Identity and Access Management platform that enables teams to securely and seamlessly manage AWS SSO entitlements at scale. Okta’s AWS Control Tower integration eases the burden of managing multi-account environment. By allowing IT to effectively provision, monitor and secure accounts, Okta helps organization get up and running faster with AWS.

The combination of Okta and AWS SSO provides:

- **Federation with AWS SSO** for single-click access to the AWS SSO user portal and its entitlements
- **Multi-factor and Adaptive authentication** to secure access to Amazon Workspace and AWS applications including AWS Control Tower
- **Seamless AWS CLI access** through federated authentication with Okta
- **Automated provisioning** to keep AWS SSO identities synchronized with Okta – providing synchronization between AWS and other user sources connected to Okta including HR systems, Active Directory(s) and LDAP(s).
- **Entitlement management** through group synchronization directly with Okta
- **Centralized reporting & auditing** of user access across all apps & systems

Architecture diagram

Okta acts as the federated Identity Provider for AWS Control Tower through integration with AWS SSO.

As an identity provider, Okta can be used as the authoritative user source for AWS SSO. While AWS SSO allows users, groups and user authentication to be managed within AWS SSO, for most enterprise customers, an external identity provider is preferred as it allows identities to be centrally managed. With Okta, identities can be consolidated from multiple sources including Active Directory, LDAP and HR systems such as Workday and SuccessFactors. By integrating with Okta, AWS SSO has clear visibility of all the enterprise users needing access.

SSO is achieved by configuring Okta as the external SAML identity provider in AWS SSO. This eliminates the need to manage user information as well as user authentication within AWS SSO.
Furthermore, AWS customers can benefit from Okta’s advanced authentication, multi-factor authentication and adaptive authentication capabilities to further secure access for AWS access.

Another key benefit with Okta and AWS SSO is the support for AWS CLI. The new CLI tool allows user to trigger a federated authentication flow from the command line to bootstrap authentication. The same level of security for web access through Okta can now be applied to all AWS CLI access as well.

Automated Provisioning can be enabled in AWS SSO to automatically synchronize user and group information from Okta using the SCIM protocol. This allows Okta to create, update and disable users automatically within AWS. User attributes such as first name, last name, display name and email can also be synchronized. Group management allows enterprise groups from Okta to be used in the context of AWS with synchronization in place for group and group membership.

![Okta and AWS Control Tower with AWS SSO](image)

**Figure 1 Okta and AWS Control Tower with AWS SSO**

**Pre-requisites**

This guide assumes two things:

AWS Control Tower is already enabled in your AWS Management Account. To get started with AWS Control Tower, view the documentation:

1) Sign up for a free okta developer account at https://developer.okta.com/signup/ to try this solution if needed.

2) If you are new to AWS, see Getting Started with AWS: https://aws.amazon.com/getting-started

3) For additional information on AWS Marketplace, see see https://aws.amazon.com/marketplace/help/about-us?ref=footer_nav_about_aws_marketplace

Subscribe to Okta from AWS Marketplace


2. Click on Continue to Subscribe

3. In the new screen, you can configure your software contract. Select appropriate Contract Duration, Renewal Settings, and Contract Options
4. Once you have configured your contract, you can click on the **Create contract** button.

5. You will be prompted to confirm the contract. If you agree to the pricing, select the **Pay Now** button.
6. To complete registration and start using your software, choose Set up your account. You will be redirected to Okta portal to complete the registration.

You successfully completed subscribing to Okta Identity Platform and registered your account. Continue to next steps to extend Okta Identity Platform to AWS Control Tower.

Configure Okta with AWS SSO & AWS Control Tower for Single Sign-On

In order to set up Okta with AWS SSO, the administrator will need admin access to both AWS Control Tower and Okta.

1. Log in to Okta as an admin. On the admin dashboard, select the Applications dropdown and go to Applications.

2. Click on the Add Application button and start typing in “AWS Single Sign-On”. The auto-fill should show “AWS Single Sign-On” in the search results. Click on that.
3. Click the green **Add** button on the left to add the AWS Single Sign-on app.

4. Provide an **Application Label**. This will be the display name of the app on the end user homepage. It will also be used as the display name of the app in the admin console. The pre-populated default value is “AWS Single Sign-On”. Click **Done** when finished.

5. On the next page, click the **Sign On** tab to configure SAML. You will see that SAML 2.0 is selected by default. Click the **Identity Provider metadata** link to download and save the metadata XML which will be needed later. (NOTE: The **View Setup Instructions** will walk you through similar set of steps as described here with less details)

6. Now scroll down to **Advanced Sign-On Settings**. Leave this tab open.

We now need to log into AWS Control Tower to fetch the values of these two fields from AWS SSO Identity Provider configuration.

7. Log into AWS Control Tower and select **Users and access** on the left pane. Click on the **View in AWS Single Sign-On** button on the right and a new tab will take you directly into AWS Single Sign-On.
8. Click on step 1 – **Choose your identity source**. On the next page, click **Change** next to **Identity Source**.

9. On the next page, select **External Identity Provider** which will expand the section. Under **Service Provider Metadata**, click on **Show individual metadata values** to reveal the metadata values.
10. Go back to the open tab in step 5 and copy the **AWS SSO ACS URL** and **AWS SSO issuer URL** into the corresponding fields in Okta. Click Save.

11. Now go back to **Change Identity Source page** in step 9. Under **IDP SAML metadata***, browse and upload the previously saved identity provider metadata XML file from Okta in step 5.

The SSO configuration is now complete. To verify the setup, you now need to assign the AWS Single Sign-On app in Okta to a user. Before we do that, make sure there is a user created in AWS SSO that you can SSO into. For example, here we have added a user “Test Admin1” with the username “testadmin2” in AWS SSO.

To assign this user to the app in Okta for testing:

1. Go back to the AWS Single Sign-on app and select the **Assignment** tab. On the left, click the **Assign** dropdown and select **Assign to People**.

2. Choose a user to assign the app to. The easiest way is to use your Okta admin user and assign the app to yourself. You will be asked to enter a **User Name**. This will be the username (i.e. NameID used in SAML) of your AWS test user. In the sample AWS SSO setup
shown above, this would be the username “testadmin1”. Click Save and Go Back, then Done on the pop-up window. You have now assigned the app to yourself.

3. You should test the end-to-end experience using the User Portal URL. In AWS Control Tower, under Users and access, you will see the value of your User Portal URL that ends with /start. You can also find this at the bottom of the AWS Single Sign-On Dashboard page.

4. Go to private browsing or a new browser (since you are likely already in an AWS session) and go to the URL. You should see some URL redirects with a quick flash of the page below which then redirects you to the Okta login page.
5. Log into Okta and you should be logged into AWS. Depending on your AWS setup, your landing screen may differ slightly. In this example, the user has 2 AWS accounts to choose from upon login.

Configure AWS CLI for Federated Authentication with Okta

1. Install AWS CLI. Make sure you install AWS CLI version 2. Version 1 does not support federated authentication. Follow the instructions here -
   https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

2. Once you have completed the installation, test that you can launch “aws” on the command line. Run “aws configure sso”. You should be prompted for **SSO start URL**. Enter the **User Portal URL** that you had just used to test SSO with (step 3 in the test instructions.) – and hit Enter.

3. You will then be prompted for the **SSO Region**. Enter your region. AWS CLI will give you a dropdown of selection. At this point, your screen should look something like this.

4. A browser should open when you hit Enter. If you need to use a different browser, follow the instructions on the command line. If a browser had popped up, you should now see the following prompt:
5. You will be redirected to Okta to authenticate. If you are already authenticated into Okta as the proper user, it will immediately jump to the success screen as shown here.

6. Going back to AWS CLI - if you have multiple accounts, you will be prompted to select one, similar to the browser experience. Complete the rest of the set up for **CLI default client Region**, **CLI default output format**, and **CLI profile name** to reuse the profile.

To log out of an authenticated session, simply type “aws sso logout”. This will require you to re-configure using the “aws configure sso” command again.

If you encounter an “invalid_grant” error in the browser when trying to authenticate, it could be due to an incorrect region. The error is shown here.

Select the correct region during the setup (step 3) and try again.
Configure Okta with AWS SSO and AWS Control Tower for User and Group Provisioning

Now that you have SSO configured with Okta, the next step is to configure User and Group Provisioning. With Okta integrated with various authoritative sources of users, automated provisioning based on Okta user lifecycle is a powerful tool to streamline user management within AWS Control Tower.

To enable provisioning,

1. Go to the AWS Single Sign-On app in the Okta admin console and select the **Provisioning** tab. Hit **Configure API Integration** button and select the **Enable API** integration option. You will be prompted for the **Base URL** and **API Token**.

2. In your AWS SSO Dashboard Settings page, click **Enable automatic provisioning** next to the **Provisioning** option. A pop-up will show you the **SCIM Endpoint** as well as the **Access Token** (click **Show token** to see the value).
3. Copy these values and enter them in the Okta app configuration in step 1. **SCIM Endpoint** goes to the Base URL field. **Access Token** goes to the API Token field. Note that for the Base URL, make sure there is no trailing “/” at the end of the URL.

4. Under **Settings** on the left pane, select **To App** to modify Okta-to-AWS provisioning settings. Click **Edit** and select provisioning operations that are applicable. In most cases, all 3 options (Create Users, Update User Attributes and Deactivate Users) should be selected to capture the full user lifecycle.
The basic SCIM provisioning setup is complete. From now on, any changes to a user who is assigned the AWS Single Sign-On app in Okta will be automatically synchronized with AWS. To test this, assign the app to a new user who does not exist in AWS – and the user will be created. Unassigning a user from the app will lead to disablement of the user in AWS.

The Default Attribute mapping only covers the mandatory attributes needed to create an AWS user. You can learn more about Okta profile mapping and profile editor here.
Solution Estimated Pricing

Please visit www.okta.com/pricing.

FAQs

- I’m new to Control Tower, where do I start?
  - Please visit Getting started with Control Tower.
- Can I get an Okta tenant to test?
  - Yes, you can create a free Okta developer account here.
- Where can I learn more about Okta and AWS integrations?
  - Please visit the AWS Partner webpage on Okta website.

Additional resources

- AWS partner webpage on Okta website
- Okta/AWS SSO/CLI Datasheet
- Okta/AWS SSO/CLI Demo
- Okta/AWS SSO/CLI Blog Post

Partner contact information

If you’re new to Okta, please contact aws@okta.com. If you are an existing customer, please contact your Okta support.