Implementation Guide:

OneLogin / AWS Control Tower with AWS SSO
Table of Contents

Table of Contents 2
Foreword 3
Solution overview and features 4
Architecture diagram 4
Pre-requisites 6
Deployment and Configuration Steps 6
  Step 1.1: Subscribe to OneLogin on AWS Marketplace. 6
  Step 1.2: Guidance on Contract Duration, Renewal and Contract Options 6
  Step 1.3: Create the Contract and Pay 7
  Step 1.4: Set up Account 7
Connect OneLogin & AWS Control Tower with AWS SSO 8
  AWS Control Tower 8
  OneLogin Administration 9
  AWS Control Tower 10
  Assigning a user to the AWS account 11
  Test Your SSO 11
    Log in to AWS SSO via OneLogin to access the newly Control Tower managed account 12
Best Practices 13
Solution Estimated Pricing 13
FAQ 13
Additional Resources 13
Partner contact information 14
Foreword

OneLogin is an Identity Federation solution that performs Identity and Access Management (IAM) on the AWS cloud. Implementing this solution, you can seamlessly provide appropriate identity safeguards and automation as you scale your AWS Multi-Account environment.

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

As you build out your AWS environment, cloud user and account setup and access management quickly become cumbersome and complex. AWS Control Tower provides the easiest path to build a baseline environment based on best industry practices. OneLogin Identity and Access Management (IAM) integrates seamlessly to ensure that your organization has the appropriate identity safeguards and automation as you scale your multi-account, multi-role environment.

OneLogin can help scale your AWS infrastructure securely and seamlessly with:

✔ **Identity Federation** - OneLogin’s best-in-class directory connectors can integrate AWS with multiple user stores, including Active Directory, LDAP, Google and more, in real-time. Integrate in minutes, not days or weeks, depending on your environment and provide your users with seamless federation from the cloud.

✔ **Strong & Adaptive Authentication** - Secure access and allow users to use their master credentials to login to AWS and all their corporate SaaS applications. Prevent password theft and orphaned AWS accounts with Single Sign-On (SSO) and Contextual Multi-Factor Authentication (MFA).

✔ **Automated User and Access Provisioning** - OneLogin’s intuitive rules engine easily maps multiple roles per user for comprehensive access assertion. Automate and manage least privileged access based on directory attributes, such as account and role (e.g. Amazon RDS Power User, Amazon S3 Power User, Amazon EC2 Power User, etc.). Provision users in real-time with appropriate role privileges with JIT provisioning.

✔ **Centralize Access Management** - Create and enforce customized security policies such as multi-factor authentication, password complexity, session timeout, and more. Easily apply those policies based on user attributes or other identifiers such as IP address to help prevent unauthorized application access.

✔ **Decrease Administration and Support Costs** - Free up IT’s time and resources with built-in self-service password reset and automated user provisioning and deprovisioning. Spend time and money focused on other infrastructure, IT, or development initiatives.

✔ **Accelerate Your Cloud Migration** - Equip your baseline AWS environment with identity guardrails such as access controls, Smartfactor multi-factor authentication, and automated security policies. Automatically replicate as you create additional AWS accounts, roles, and tenants. You can also integrate OneLogin with AWS Organizations, AWS IAM, and Session Tags.

Architecture diagram

Implementing strong, scalable Identity and Access Management (IAM) is a best practice for security and scalability. OneLogin’s Trusted Experiences Platform is built to seamlessly manage all digital identities for your workforce and customers from the cloud. With OneLogin’s powerful authentication and role-based user provisioning engine, quickly enable single sign-on (SSO) across mobile, web and desktop, enforce multi-factor authentication (MFA) and security policies like password complexity and IP restriction, and automate user account provisioning across your corporate applications. OneLogin’s automated AWS role provisioning enables organizations to streamline the most complicated of user policies and assign least-privileged policies to hundreds or thousands of permissions. OneLogin also enhances AWS’s native security capabilities and is commonly used alongside AWS STS, AWS Organizations, AWS Session Tags, AWS Control Tower, AWS IAM, and Amazon EventBridge.

OneLogin integrates with AWS Control Tower in two ways:

1. OneLogin and AWS Control Tower with AWS SSO
2. OneLogin and AWS Control Tower with SAML
In this document, you can find the implementation guidelines for scenario where OneLogin and AWS Control Tower are integrated using AWS SSO. OneLogin provides a sample CloudFormation Template that is used to set up identity federation with OneLogin, as well as to provide guidance on sample AWS IAM Roles and permissions in the different AWS accounts. After AWS Control Tower creates the various AWS accounts, OneLogin can perform identity federation via AWS SSO or directly to the accounts themselves.

In this scenario, OneLogin performs identity federation with AWS SSO. An end user would then sign in to the various AWS accounts using AWS SSO.

You can refer to this [document](#) for the guidelines to implement second scenario where OneLogin performs identity federation directly with the AWS Control Tower created accounts.
Pre-requisites

To get started, you’ll need the following items:

1. OneLogin account
   - OneLogin is available on the AWS Marketplace at https://aws.amazon.com/marketplace/pp/B0764C2TJS. Instructions for the AWS Marketplace are in the following section.
   - OneLogin Developer Accounts are available at https://www.onelogin.com/developer-signup

2. Provide a work email for your OneLogin Account (e.g., yourAlias@domain.com, confirm email, set up MFA if required, and sign in as administrator)
   - For example, yourAlias@domain.com
   - MFA should be set up on the OneLogin account if required
   - You should have Super User (Administrator) access to your OneLogin account

3. AWS Control Tower should be setup on your AWS account and you should have Administrator access to your AWS Control Tower Master Account

Deployment and Configuration Steps

**Step 1.1: Subscribe to OneLogin on AWS Marketplace.**


Click on the **Continue to Subscribe** button.

**Step 1.2: Guidance on Contract Duration, Renewal and Contract Options**

In the new screen, you can configure your contract. You can select the **Contract Duration**, **Renewal Settings** and **Contract Options**.
Step 1.3: Create the Contract and Pay

Once you have configured your contract, you can click on the Create contract button. You will be prompted to confirm the contract. If you agree to the pricing, select the Pay Now button.

You will be prompted to confirm the contract. If you agree to the pricing, select the Pay Now button.

Step 1.4: Set up Account

Once you agree to Pay Now, you will be redirected to a sign-up form. Once the form is complete, a OneLogin account will be automatically generated for you. You can then sign in.
Connect OneLogin & AWS Control Tower with AWS SSO

This topic describes how to configure OneLogin to provide SSO for AWS Control Tower using AWS SSO.

1. Log in to OneLogin and go to Applications > Applications.
2. Search for saml test, then choose SAML Test Connector (Advanced).

3. On the initial Configuration tab, rename the app to AWS Control Tower Demo, then click Save.

AWS Control Tower

Open a second tab and navigate to the AWS Control Tower console. Click on User and Access on the left-hand side and click on View in AWS Single Sign-On to open up AWS SSO.
On the **Settings** page, choose **Change** next to **Identity Source**.

On the **Change directory** page, choose **External Identity Provider**.

In the **Service provider metadata** section, click **Show Individual Metadata Values**.

Click the **Copy** icon next to **AWS SSO ACS URL**.

Switch back to the OneLogin configuration tab and select **Configuration** in the left-hand navigation pane.

Paste the AWS SSO ACS URL from AWS SSO (copied from previous section) into the **Recipient**, **ACS (Consumer) URL Validator**, and **ACS (Consumer) URL** fields.

**Important note:** you MUST modify the URL in the ACS (Consumer) URL Validator using Regular Expressions code. Specifically:

- Add a “^” character (no quotes) at the beginning.
- Escape all forward-slashes with a leading backslash.

Your ACS (Consumer) URL Validator address will look similar to this:

```
https://Vv.us-east-1.signin.aws.amazon.com/Vplatform\/saml\/acs\/d4969c98-b269-43c4-a58c-3c
```

Return to your AWS Control Tower tab and copy the **AWS SSO issuer URL**.

1. Paste the AWS SSO issuer URL value into the **Audience** field on OneLogin.
2. Scroll down and confirm that SAML **nameID** format is set to **Email**, then click **Save** in upper right.
3. Under More Actions, click SAML Metadata. This will download the OneLogin SAML metadata file from OneLogin to your computer’s downloads folder.

AWS Control Tower

Switch back to the AWS Control Tower console, click on User and Access on the left, and click View in AWS Single Sign-On to open up AWS SSO.

1. Choose Settings in the left panel. Next to Identity source, choose Change to open Change identity source page
2. In the Identity provider metadata section, choose Browse. Search for and upload for the metadata file that you downloaded from the OneLogin Portal.
3. Choose Next: Review, then type CONFIRM in the text box to confirm that you want to change the directory. Click Finish.
4. Return to your open OneLogin tab and select Users in the top navigation bar, then click on your test user. In the left-hand navigation pane, select Applications and click the blue + button to add a new application for this user.

5. Select AWS Control Tower Demo from the drop-down and click Continue, then confirm that the nameID value shown matches the email address of your test user.

6. Click Save, then Save User.
Switch back to the AWS Control Tower console. Click on User and Access on the left-hand side and click on View in AWS Single Sign-On to open AWS SSO.

In the left navigation pane, choose Users, then choose Add User.

1. In the Username field, enter the email address associated with your OneLogin test user.
2. In the Email and Confirm Email Address fields, enter the same email as in the previous step.
3. Enter any value you like for First Name and Last Name.
4. Ensure Display Name field is populated.
5. Choose Next: Groups and select AWSControlTowerAdmins and AWSLogArchiveAdmins for testing purposes.
6. Click Add User.

Assigning a user to the AWS account

1. On the AWS Accounts page in the left navigation pane, select the AWS organization tab and select the AWS account you want to assign to the user and choose Assign users.
2. In the Assign Users page, select the user you created and choose Next: Permission sets.
3. Under the Select Permission Sets section, select the permission set you want to assign to the user. If you don’t have an existing permission set, choose Create New Permission Set. Click Finish.

Test Your SSO

1. Return to your OneLogin browser window, and select Profile -> App Portal/Home from top-right
2. Switch to the Company: Everything tab
3. Click on the AWS Control Tower Demo application. If it doesn’t appear, re-confirm that your test user is assigned to the AWS Control Tower Demo application in OneLogin.
4. Following a set of browser redirects, the AWS Single Sign-On User Portal page appears and you are able to access your AWS Control Tower master or log account based on the OneLogin user authentication.

Optional: Create a new managed account in Control Tower via account Factory and associate it with OneLogin User.

1. Open the Control Tower console from your master account, navigate to Account Factory, and click Enroll Account.
2. Select **AWS Control Tower Account Factory** as the product name and click **Launch Product**, then provide a name for the product and click **Next**.

3. Type in a new SSO user email, account email, and managed OneLogin user details, then click **Next**.

4. Click **Next** and **Launch**. This step takes about 15-20 minutes to complete; your status will update to **SUCCEEDED** when it's done.

5. Check the email you provided for an **invitation email** from no-reply@login.awsapps.com, then click **Accept Invitation**.

6. Note your **User portal URL** (example: [https://d-xxxxx.awsapps.com/start](https://d-xxxxx.awsapps.com/start)) and your **Username**. You can move on to the steps below as the above step is in progress.

**Log in to AWS SSO via OneLogin to access the newly Control Tower managed account**

1. Open a fresh browser or incognito window and paste **Your User Portal URL** into the address bar. You'll see a series of redirects on your browser to take you to OneLogin.

2. Enter the OneLogin username created in the previous step. This redirects you to AWS SSO.
Best Practices

- Aim for least privileged access to AWS
  - Think through your AWS IAM roles and permissions
  - Determine how you would want your AWS IAM structure to look like for the Control Tower created accounts and your production AWS accounts

Solution Estimated Pricing

- AWS: Refer to AWS estimated pricing for the different AWS services
- OneLogin
  - Single Application: $12/user/year
  - Unlimited Plan: $96/user/year
  - Custom plans: contact partners@onelogin.com

FAQ

- Before you implement this solution, we recommend that you become familiar with OneLogin. More information is available in the Additional Resources section
- If you are new to AWS, see Getting Started with AWS
  - https://aws.amazon.com/getting-started/
- For additional information on AWS Marketplace, visit
- To get started with AWS Control Tower, visit

Additional Resources

- OneLogin for AWS
  - https://www.onelogin.com/partners/technology-partners/aws
- OneLogin Support Documentation for AWS
  - https://onelogin.service-now.com/support?id=kb_category&kb_category=2009a1b0db185340d5505ee4b96194e
- OneLogin on the AWS Marketplace
- OneLogin Developer Documentation
  - https://developers.onelogin.com
Partner contact information

For questions, contact partners@onelogin.com