



Tenable Cloud Security Quick Reference Guide: Onboarding AWS Accounts in Tenable Cloud Security

Last Revised: July 21, 2023



Table of Contents

Onboarding AWS Accounts	3
Create a Project	5
Set Up Read-Only Access to the AWS Account	6
Onboard an AWS Organization	15
Onboard an AWS Account	20
Configure a Cloud Scan	21
Create a Scan Profile	22
Schedule a Scan	24
Run a Cloud Scan	25



Onboarding AWS Accounts

This Quick Reference Guide provides the sequence of tasks required to onboard AWS cloud accounts to Tenable Cloud Security (formerly known as Tenable.cs) and to perform a cloud scan. Tenable Cloud Security assesses your cloud infrastructure at runtime and identifies security and compliance violations.

Before you begin:

You must have the following:

- Credentials for your Tenable Vulnerability Management user account.
- AWS user account with permissions to create Identity and Access Management (IAM) roles.

Overview

You can onboard your Amazon Web Services (AWS) accounts in Tenable Cloud Security in the following two ways:

- **Onboard an AWS organization:** Use this recommended method to secure multiple AWS accounts and start the security assessment. Tenable Cloud Security can connect to your AWS organization's management account to discover all the member accounts that are under that account. Provide a Role ARN and an optional External ID for the management account. Ensure that you have [read-only permission](#) to deploy a CloudFormation stack to set up access roles in each of the member accounts.
- **Onboard a single AWS account:** Use this method if you want to onboard each AWS account manually without deploying a CloudFormation Stack. Provide a Role ARN and an optional External ID for the AWS account.

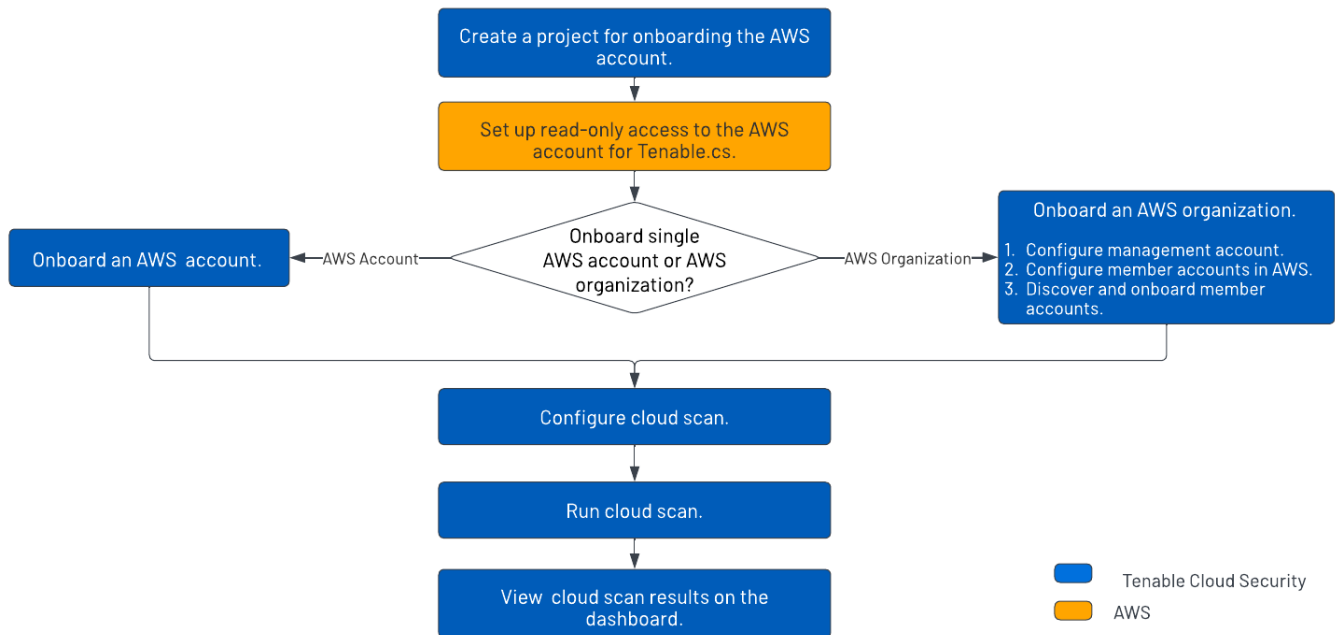
To onboard AWS accounts in Tenable Cloud Security, you must configure an Identity and Access Management (IAM) role so that Tenable Cloud Security can read the resources in the connected AWS accounts. When onboarding an AWS organization account, create an IAM role for the management account.

After connecting your cloud accounts, configure your cloud resources and then scan these cloud resources for any violations.



Workflow

The following workflow provides the high-level tasks required for onboarding AWS accounts.



Video

Video: [Onboarding AWS accounts with Tenable Cloud Security](#)

Other Resources

- [Tenable Cloud Security User Guide](#)

Provides conceptual information and instructions for using Tenable Cloud Security.

- [Getting Started with Tenable Cloud Security](#)


Provides video resources in [Tenable Product Education](#).



Create a Project

In Tenable Cloud Security Console, you can group resources, such as repositories and cloud accounts, into projects. Projects allow you to monitor, analyze, and manage all your resources at once.

To create a project:

1. [Log in](#) to Tenable Vulnerability Management.
2. In the left navigation bar, click **Cloud Security**.
The Tenable Cloud Security home page appears.
3. In the left navigation bar, click  > **Project**.
4. In the **Give the project a name** section, type a name for your project. For example, **AWS-Project**.

Note: A project name can have a maximum of 25 characters.

5. Click **Continue**.
6. In the **Choose provider** section, select **AWS** as the cloud service provider.
7. Click **Create**.

A confirmation message appears and Tenable Cloud Security creates the project. You can view the new project on the **Projects & Connections** page.



Set Up Read-Only Access to the AWS Account

To read the resources in the Amazon Web Services (AWS) cloud account, Tenable Cloud Security requires appropriate permissions. Tenable Cloud Security recommends provisioning an IAM (Identity and Access Management) role in the target AWS cloud account and configuring it for Tenable Cloud Security to read the resources in the same account. When onboarding an AWS organization account, create an IAM role for the management account.

You can create the role in the following ways:

- [Create a read-only role manually](#)
- [Create a read-only role using a script](#)
- [Create a read-only role using a CloudFormation Template](#)

Create a read-only role manually

You can create a read-only role manually from the AWS management console.

Before you begin:

- Log in to the AWS web console with a user account with permission to create IAM roles.

For more information about IAM roles, see Amazon's [AWS Identity and Access Management User Guide](#).

To create a read-only role manually:

1. In the AWS web console, go to **Identity and Access Management (IAM)**.
2. On the left navigation pane, click **Roles**.

The **Roles** page appears.

3. Click **Create Role**.

The Create Role wizard appears.

4. In the **Select trusted entity** page, do the following:



- a. In the **Trusted entity type** section, select **AWS Account**.
- b. In the **An AWS Account** section, select **Another AWS Account**.
- c. In the **Account ID** box, type **012615275169**.

Note: 012615275169 is the account ID of the Tenable AWS account that you are establishing a trust relationship with to support AWS role delegation.

- d. Under **Options**, click the **Require External ID** check box and type your Tenable Vulnerability Management Container UUID in the External ID box.

Note: In Tenable Vulnerability Management, navigate to **Settings > License** to get your container UUID. For more information, see [View Information about Your Tenable Vulnerability Management Instance](#).

- e. Click **Next**.

Step 2
Add permissions

Step 3
Name, review, and create

Trusted entity type

- AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

- This account (576993307204)
- Another AWS account

Account ID
Identifier of the account that can use this role

012615275169

Account ID is a 12-digit number.

Options

- Require external ID (Best practice when a third party will assume this role)**
You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. [Learn more](#)

External ID

<insertTicContainerUUID>

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. [Learn more](#)

- Require MFA**
Requires that the assuming entity use multi-factor authentication.

5. On the **Add permissions** page, perform the following:



- a. Search for **ReadOnlyAccess** in the search box.

Tip: Filtering for "ReadOnlyAccess" by role name might return many entries. Apply the "Used as: Used as permissions policy" filter along with the role name "ReadOnlyAccess" to narrow down the search results.

- b. Select the **ReadOnlyAccess** check box.

Add permissions

Permissions policies (Selected 1/878)
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter 11 matches

ReadOnlyAccess x Used as: Used as permissions policy x Clear filters

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	ADM-POL-ArtifactReadOnlyAccess	Customer managed	This policy gives read-only access to pull reports from artifact
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed	Provides read only access to Amazon EC2 via the AWS Management Console.
<input type="checkbox"/>	AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon VPC via the AWS Management Console.
<input checked="" type="checkbox"/>	ReadOnlyAccess	AWS managed	Provides read-only access to AWS services and resources.
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all buckets via the AWS Management Console.
<input type="checkbox"/>	ResourceGroupsandTagEditorReadOnlyAc...	AWS managed	Provides access to use Resource Groups and Tag Editor, but does not allow editing of tags via the Tag Editor.
<input type="checkbox"/>	AWSCloudFormationReadOnlyAccess	AWS managed	Provides access to AWS CloudFormation via the AWS Management Console.

For the list of permissions and AWS resources scanned by Tenable Cloud Security with this policy, see [Permissions and Supported Resources for AWS ReadOnlyAccess Policy](#).

- c. For vulnerability scanning with Agentless Assessment, create an inline policy with the following JSON to provide Elastic Block Store permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ebs:List*",
        "ebs:Get*"
      ],
      "Resource": "*"
    }
  ]
}
```




- d. Select the required policies for the IAM role and click **Next**.

Note: The new policy might take some time to get created. Refresh your browser if you do not see the policy in the list of policies.

For information about creating IAM policies, see the [AWS documentation](#).

6. In the **Name, review, and create** page, do the following:
 - a. In the **Role Details** section, type a **Role Name** for the role.
 - b. (Optional) Add a role description in the **Description** box.
 - c. (Optional) Click **Add Tags** to add key-value pairs to AWS resources.
 - d. Click **Create Role**.

The screenshot shows the 'Name, review, and create' page in the AWS IAM console. It is divided into several sections:

- Role details:** Includes a 'Role name' field with the value 'TenableReadOnlyTrustRole' and a 'Description' field.
- Step 1: Select trusted entities:** Shows a JSON policy snippet for 'sts:AssumeRole' with a condition for 'sts:ExternalId'.
- Step 2: Add permissions:** Displays a table of attached permissions.
- Tags:** Shows 'Add tags (Optional)' with a note that no tags are currently associated.

Policy name	Type	Attached as
ReadOnlyAccess	AWS managed	Permissions policy

At the bottom right, there are buttons for 'Cancel', 'Previous', and 'Create role'.

Tenable Cloud Security now has read-only access to your AWS account.

7. To get the **Role ARN** and **External ID** of this new role for Tenable Cloud Security, do the following:



- a. On the left navigation pane, click **Roles**.
- b. Search for the role that you created.
- c. In the **Summary** section, note the **Role ARN** value.
- d. Click the **Trust Relationships** tab and note the value of the **ExternalId** field.

IAM > Roles > TenableReadOnlyTrustRole

TenableReadOnlyTrustRole

Summary

Creation date
January 27, 2022, 03:39 (UTC+05:30)

Last activity
14 days ago

ARN
[Redacted]

Maximum session duration
1 hour

Permissions | **Trust relationships** | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Principal": {
7-         "AWS": "[Redacted]"
8-       },
9-       "Action": "sts:AssumeRole",
10-      "Condition": {
11-        "StringEquals": {
12-          "sts:ExternalId": "[Redacted]"
13-        }
14-      }
15-    }
16-  ]
17- }
```

8. Note down the following values:

- **Role ARN**
- **External ID**

You need these values when onboarding AWS accounts in Tenable Cloud Security.

Create a Read-Only Role Using a Script

You can run the script provided by Tenable Cloud Security to create an AWS read-only role.



Before you begin:

- You must have the following:
 - Terraform version 12 or higher
 - AWS access key
 - AWS secret key

To create a read-only role using a script:

1. Run the following command:

```
/bin/bash -c "$(curl https://downloads.accurics.com/downloads/io/create_tcs_aws_readonly_role.sh)"
```

2. Provide values for the following parameters, when prompted:

- (Required) **AWS_ACCESS_KEY_ID**: Access key of the AWS account.
- (Required) **AWS_SECRET_ACCESS_KEY**: Secret key of the AWS account.
- (Optional) **Role name suffix**: By default, Tenable Cloud Security creates a role with the name *TenableReadOnlyTrustRole*. Provide an optional suffix to append to this role name. For example, if you provide ACME, the role name is *TenableReadOnlyTrustRoleACME*.
- (Required) **ExternalId**: Provide an alphanumeric string to be used as the External ID of the role. The External ID can contain a minimum of 4 chars and a maximum of 1224 characters. Tenable recommends providing your Tenable Vulnerability Management Container UUID for the External ID.

3. When prompted "**Do you want to perform these actions?**", type **yes** to continue.

Tenable Cloud Security executes the script and creates the read-only role.



```
Do you want to perform these actions?
Terraform will perform the actions described above.
Only 'yes' will be accepted to approve.

Enter a value: yes

aws_iam_role.read_only: Creating...
aws_iam_role.read_only: Creation complete after 3s [id=TenableReadOnlyTrustRoleTEST]
aws_iam_role_policy_attachment.read_only: Creating...
aws_iam_role_policy_attachment.read_only: Creation complete after 0s [id=TenableReadOnlyTrustRoleTEST-20220930064810139700000001]

Apply complete! Resources: 2 added, 0 changed, 0 destroyed.

Outputs:
CustomerExternalId = "XXXXXXX"
role_arn = "arn:aws:iam::XXXXXXXXXXXX:role/TenableReadOnlyTrustRole"
-e \Read Only AWS Role Creation Successful.

Please use the ARN and CUSTOMER_EXTERNAL_ID printed in the terraform output to enable Tenable.cs Cloud Scan.
```

4. Note down the following values:

- Role ARN
- External ID

You need these values when onboarding accounts in AWS.

Create a read-only role using a CloudFormation Template

You can deploy the Tenable Cloud Security stackset to create a read-only role.

Before you begin:

- Log in to the AWS web console.

To create a read-only role using a CloudFormation Template:

1. Click [here](#) to open the CloudFormation template to deploy a read-only role in AWS.
Tenable Cloud Security redirects you to the **Quick create stack** page in AWS.
2. Review the parameters in the stack template and update, if required.
3. In the **Capabilities** section, select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names.** check box to confirm creating the IAM resources with required permissions.
4. Click **Create stack**.



Wait for the stack to get created and its status to become **CREATE_COMPLETE**.

5. Note down the following values:

- **Role ARN:** Copy the stack ARN of the deployed stack from the **Outputs** tab.

Key	Value	Description	Export name
TenableRoleArn	arn:aws:iam::[redacted]:role/[redacted]	IAM role for Tenable.cs access	tenable-read-only-access:Te[redacted]

- **External ID:** Copy the **ExternalID** from the **Parameters** tab.

Key	Value
AllowEBSReadAccess	false
EBSReadPolicyName	TenableEBSRead2
ExternalID	[redacted]
TenableRoleName	Te[redacted]

You need these values when onboarding AWS accounts in Tenable Cloud Security.

What to do next:

[Onboard AWS Accounts](#)

You must have the following values for onboarding the AWS account in Tenable Cloud Security:



- Role ARN
- External ID



Onboard an AWS Organization

Tenable Cloud Security can connect to your AWS organization's management account to discover all the member accounts under that account. This is the recommended method when you want to onboard all of your AWS accounts in Tenable Cloud Security for security assessment. You must have the required permissions to deploy a CloudFormation stack for setting up access roles in each of the member accounts.

Tip: For more information about AWS organizations, see Amazon's [AWS Organizations User Guide](#).


Before you begin:

You must have the following details for the read-only role in your AWS account:

- Role ARN
- External ID

For more information, see [Set Up Read-Only Access to the AWS Account](#).

To connect to an AWS organization account:

1. In the left navigation bar, click  > **Connection** > **AWS account**.
2. In the **Choose a workflow to discover AWS account(s)** section, select **Onboard AWS organization**.
3. Click **Continue**.

The **Configure management account** section appears.

4. Type the appropriate **Read Only Role ARN** and **External ID**.
5. Click **Continue**.

The **Configure member accounts** section appears.

6. Configure member accounts by performing the following actions:



- a. In the **Configure member accounts** section, in the first step, click **here**.

Tenable Cloud Security redirects you to the **Create StackSet** wizard in the AWS Management Console. Follow these steps to [deploy the stackset](#) that creates the role for all member accounts.

To deploy the StackSet to create a read-only role for a member account:

- a. Sign in to the AWS management account of the target organization.
- b. Copy the appropriate URL from the **Configure member accounts** section.
- c. On the **Choose a template** page, do the following:
 - i. In the **Permissions** section, ensure that the **Service-managed permissions** option is selected.
 - ii. In the **Prerequisite - Prepare template** section, ensure that the **Template is ready** option is selected.
 - iii. In the **Template source** section, click **Amazon S3 URL**.
 - iv. In the **Amazon S3 URL** box, copy the template URL from the Tenable Cloud Security Console and paste it.
 - v. Click **Next**.
- d. On the **Specify StackSet details** page, do the following:
 - i. In the **StackSet name** section, type a name for the StackSet.

Tip: Choose a meaningful name because the Tenable Cloud Security role name is used for all the member accounts of the organization.
 - ii. In the **StackSet description** section, type a description for the current StackSet.
 - iii. In the **Parameters** section, type the appropriate management account ID.
 - iv. Click **Next**.
- e. On the **Configure StackSet Options** page, do the following:



- i. (Optional) In the **Tags** section, click **Add new tag** and provide a **Key** and a **Value** to specify the tag.

Tags are arbitrary key-value pairs that can be used to identify your stack. Tags that you apply to stack sets are applied to all resources created by your stacks.

- ii. For **Execution configuration**, choose **Active** so that StackSets performs non-conflicting operations concurrently and queues conflicting operations. After conflicting operations finish, StackSets starts queued operations in request order.
- iii. Click **Next**.

- f. On the **Set deployment options** page, do the following:

- i. In the **Deployment targets** section, click one of the following:

- **Deploy to organization** – Creates the role in all the member AWS accounts for the organization.
- **Deploy to organizational units (OUs)** – Creates the role in all the member AWS accounts for selected organizations.

- ii. In **Automatic deployment**, click **Enabled**.

- iii. In **Account removal behavior**, click the required option.

- g. In the **Specify regions** section, add a region available across all member accounts.

Caution: Select only one region. If you specify multiple regions, stack deployment succeeds only for one region and fails for others and can cause issues.

Note: If the selected region is not available under a particular member account, the stackset deployment fails.

- h. In the **Deployment options** section, do the following:



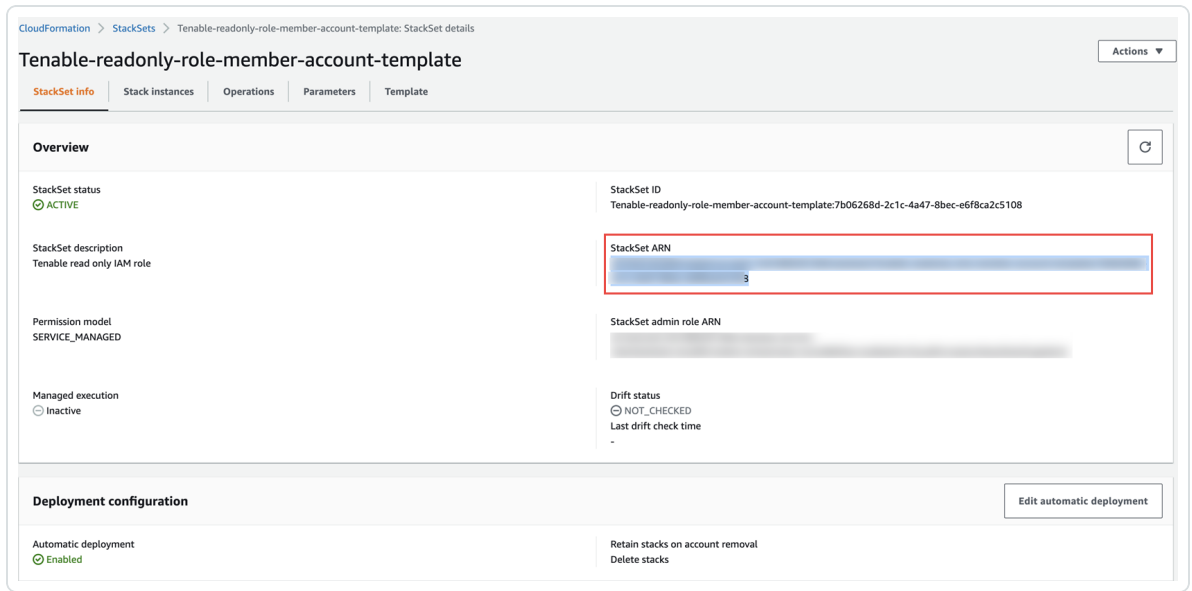
- i. In the **Maximum concurrent accounts - optional** drop-down box, select **Percentage**, and set the value to **100**.
- ii. In the **Failure tolerance - optional** drop-down box, select **Percentage**, and set the value to **100**.
- iii. In the **Regional Concurrency** section, click **Sequential**.
- iv. Click **Next**.
- i. In the **Capabilities** section, select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names**.check box to confirm.
- j. Click **Submit**.

The **StackSet details** page appears. Wait for the status of the StackSet to change to **Succeeded**.

The screenshot shows the AWS CloudFormation console for a StackSet named 'Tenable-readonly-role-member-account-template'. The 'Operations' tab is selected, displaying a table with one operation that has succeeded.

Operation ID	Type	Status	Created time	Completed time
1778681c-fd4a-8d0d-4fd5-46b0da2556d0	CREATE	SUCCEEDED	2022-06-29 18:00:11 UTC+0530	2022-06-29 18:01:36 UTC+0530

- k. Click the **StackSet Info** tab and copy the **StackSet ARN**.



- b. In the Tenable Cloud Security Console, paste the Stacksets ARN copied in the previous step in the **Stacksets ARN** box.
- c. Click **Continue**.

The **Discover and onboard member accounts** section appears. Tenable Cloud Security deploys the StackSet used to create a Tenable Cloud Security role for each member account.

7. Onboard member accounts.

- a. In the **Discover and onboard member accounts** section, in the list, select the cloud member accounts that you want to onboard.

Tip: You can also search for specific cloud accounts and filter the list by organizations.

- b. (Optional) To create a new project automatically for the AWS organization, select the **Map accounts automatically** check box.

Tenable Cloud Security creates a new project for the AWS organization and links all AWS member accounts with the project.

- c. Click **Onboard accounts**.

On the **Projects & Connections** page, the AWS project links to the connected AWS organization's account and the selected VPCs.



Onboard an AWS Account

You can connect your Amazon Web Services (AWS) account as part of your AWS project. Use this method if you want to onboard each of your AWS account manually without deploying a CloudFormation template.


Before you begin:

You must have the following details for the read-only role in for your AWS account:

- Role ARN
- External ID

For more information, see [Set Up Read-Only Access to the AWS Account](#).

To connect an AWS account:

1. In the left navigation bar of the Tenable Cloud Security page, click  > **Connection > AWS account**.
2. In the **Choose a workflow to discover AWS accounts** section, click **Onboard AWS account**.
3. Click **Continue**.

The **Configure AWS account** section appears.

4. Type the appropriate **Read Only Role ARN** and **External ID**.
5. Click **Continue**.
6. In the **Choose projects to add the AWS account(s) to** section, select the project that you created for the AWS account.

For more information, see [Create a Project](#).

7. Click **Connect Cloud Account**.

You can view the AWS project linked to the connected AWS account and the selected VPCs on the **Projects & Connections** page.



Configure a Cloud Scan

To run a cloud scan after onboarding your cloud accounts, you must select and run a scan profile. Tenable Cloud Security provides a default scan profile for each cloud provider. You can also create your custom scan profiles. After creating a scan profile, you can run the following types of cloud scans:

- **Misconfiguration Scan:** Scans for policy violations in IaC repositories and cloud resources. You can view the scan results on the **Findings > [Misconfigurations](#)** page. The Misconfigurations Scan is supported for all cloud providers - AWS, Azure, and GCP.
- **Vulnerability Scan:** Scans for known vulnerabilities (CVEs) in workloads, such as operating systems, images, containers, and software based on plugins. Currently, Tenable Cloud Security supports vulnerability scans only for AWS EC2 instances. You can view these vulnerabilities on the **Findings > [Vulnerabilities](#)** page in Tenable Cloud Security and the **Findings** page in Tenable Vulnerability Management. For more information, see [Configure Vulnerability Scan for Agentless Assessment](#).

To configure a cloud scan:

1. [Create a Scan Profile](#).
2. (Optional) [Schedule a Scan](#).



Create a Scan Profile

Scan profiles allow you to group the scan operations of different cloud resources and schedule scans according to your needs. You can create different scan profiles to run scans targeting different resources.

Note: You can create a maximum of 10 scan profiles.

Before you begin:

To run a vulnerability scan using Agentless Assessment, see the following:

- [Configure Vulnerability Scan using Agentless Assessment for AWS](#)
- [Configure Vulnerability Scan using Agentless Assessment for Azure](#)

To create a scan profile:

1. Click **Projects & Connections**.

Tenable Cloud Security lists all the projects in the **Projects** tab.

2. In the row for the project for which you are creating the scan profile, click **⋮ > Manage cloud scan profiles**.

The **Manage scan profiles** window appears with the default scan profile.

Note: You can use the default scan profile to perform a scan. Click the default scan profile to view the resources that get scanned. Vulnerability scan with agentless assessment is enabled by default for the default scan profile.

3. Click **New Scan Profile**.

The **Create new scan profile for cloud** window appears.

Note: To create a scan profile from an existing scan profile, create a copy of the scan profile and then edit the profile.

4. In the **Scan profile name** box, type a name for the scan profile or retain the default name.



- In **Step 1 Cloud config assessment options**, retain the default selections or do one of the following:
 - Select the check box next to the option to select all the resources within a category.
 - Click the drop-down arrow \vee to show all the available resources in the category. Select the check boxes as needed.

Note: The count next to the drop-down arrow \vee shows: Number of resources available / Number of resources selected.

- Select a resource by searching for it in the **Search resources** box.
- (Optional) In **Step 2**, click the **Enable Vulnerability Scan** toggle to enable vulnerability assessment.

Note: The vulnerability scan option is available only for AWS EC2 Instances and Azure Virtual Machines. When you enable vulnerability scan, Tenable Cloud Security starts scanning for vulnerabilities after the misconfiguration scan completes.

- Click **Preview** to view the resources selected in the cloud scan profile.
- Click **Create Scan Profile**.

Tenable Cloud Security creates the scan profile and displays it in the **Manage scan profiles** window.

What to do next:

Initiate the scan for the scan profile. For more information, see [Run a Cloud Scan](#).



Schedule a Scan

You can add a scan schedule to your scan profile and run scans at regular intervals. Tenable Cloud Security starts immediately after the duration since the schedule was submitted. For example, if you set the scan schedule to 6 hours now, Tenable Cloud Security starts the scan exactly after 6 hours from now. Tenable Cloud Security runs scheduled scans with the default scan profile.

Note: You can add only one schedule for a scan profile.

To schedule a scan for a scan profile:

1. On the home page, click **Projects & Connections**.

Tenable Cloud Security displays the list of projects in the **Projects** tab.

2. In the row for the project that you want to scan, click **⋮ > Manage cloud scan profiles**.

The **Manage scan profiles** window appears.

3. In the row of the scan profile for which you want to schedule a scan, click **⋮ > Schedule scan**.

The **Schedule scan** window appears.

4. In the **Select interval** drop-down box, select the required schedule to run the scan: Every 6 hours, 12 hours, or 24 hours.

5. Click **Schedule Scan**.

Tenable Cloud Security schedules the scan for the selected interval and displays a confirmation message.

Note: To delete a scheduled scan, in the row for the project, click **⋮ > Delete scheduled scan**.



Run a Cloud Scan

You can [create](#) a scan profile to include the resource types that you want to scan and trigger a scan for that profile.

To start a scan:

1. Click **Projects & Connections**.

Tenable Cloud Security displays the list of projects in the **Projects** tab.

2. In the row for the project for the cloud scan, click **:** and do one of the following:
 - **Run default scan profile** – Select this option to run a scan on the default scan profile. If there are no other scan profiles, Tenable Cloud Security runs a scan on the system default scan profile.

Note: Vulnerability scan with agentless assessment is enabled by default for the default scan profile.

- **Manage cloud scan profiles** – Select this option to create a new scan profile or use a scan profile that you created earlier.

The **Manage scan profile** window appears and lists all the scan profiles.

Tenable Cloud Security runs the scan and updates the scan status column of the project on completion of the scan.

Note: You can view or edit other scan profiles of a project when the cloud scan is running with one of the scan profiles.

What to do next:

After running a cloud scan, you can view a summary of issues, critical security insights, remediation insights, number of cloud and IaC drifts, failing policies, and impacted resources for your project. For more information, see [View Tenable Cloud Security Dashboards and Reports](#).