



Tenable Cloud Security Quick Reference Guide: Onboarding Microsoft Azure Accounts in Tenable Cloud Security

Last Revised: May 18, 2023



Table of Contents

Onboarding Microsoft Azure Accounts	3
Create a Project	5
Create an Azure Service Principal Role	6
Onboard an Azure Account	19
Configure a Cloud Scan	21
Create a Scan Profile	22
Schedule a Scan	23
Run a Cloud Scan	24



Onboarding Microsoft Azure Accounts

This Quick Reference Guide provides the sequence of tasks required to onboard Microsoft Azure cloud accounts to Tenable Cloud Security 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.
- An Azure subscription with sufficient permissions to register an application and assign a role with your Azure Active Directory (AD) tenant.

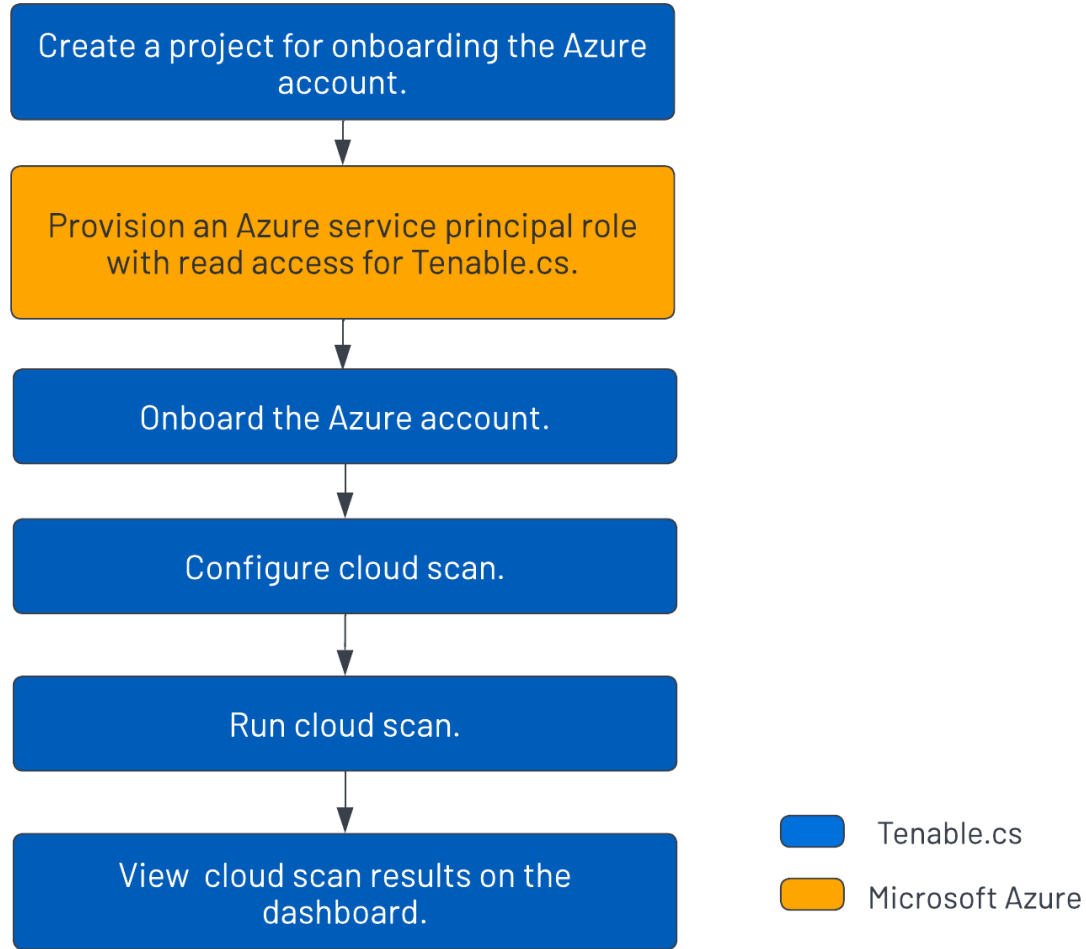
Overview

To establish the connection between Tenable Cloud Security and Azure cloud, Tenable Cloud Security requires an Azure service principal in the Azure subscription with read permissions to access the resources in the subscription. For creating a service principal, register an application through the Azure portal and then assign the **Reader** role to the application. To onboard the Azure service principal in Tenable Cloud Security, provide the tenant ID, application ID, and secret key value of your application for authenticating with Azure.

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 for onboarding Azure accounts.



Video

Video: [Onboarding Azure 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, **Azure-Project**.
5. Click **Continue**.
6. In the **Choose provider** section, select **Azure** 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.



Create an Azure Service Principal Role

Tenable Cloud Security requires adequate permissions to read the resources in your Azure subscription. Provision a service principal role in the target Azure subscription and configure it for Tenable Cloud Security to read the resources in the same account.

Follow these steps to create a service principal and assign a role to it:

1. [Register an application with Azure to create the service principal.](#)
2. Choose one of the following options to assign a role to the service principal for accessing the resources in your subscription:
 - [Create and assign a custom role with expanded Read access \(comprehensive\) to the service principal.](#)
 - [Assign the built-in Reader role \(limited\) to the service principal.](#)
3. [Create a client secret for authenticating the service principal from Tenable Cloud Security.](#)

Register an application with Azure

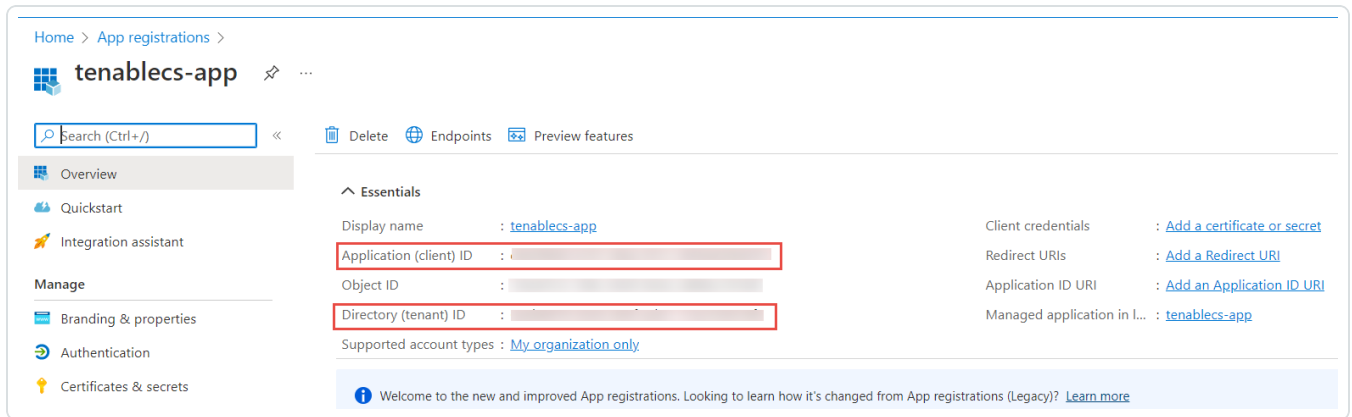
When you register an application through the Azure portal, Azure automatically creates an application object and service principal in your tenant. For more information on the relationship between application registration, application objects, and service principals, see [Application and service principal objects in Azure Active Directory](#).

To create a service principal role in Azure:

1. Log in to the [Microsoft Azure portal](#).
2. In the home page, click **App registrations**.
The **App registrations** page appears.
3. Click **New registration**.
The **Register an application** page appears.
4. Type a name for the application you want to register.
5. Click **Register**.



The application details page appears.



6. Note down the following values. You need these values when onboarding the service account in Tenable Cloud Security:

- **Application (client) ID:** This is the client ID requested by Tenable Cloud Security.
- **Directory (tenant) ID:** This is the Tenant ID requested by Tenable Cloud Security.

Create a custom role and assign it to the service principal

For a comprehensive scan including managed clusters and storage accounts, add a custom role with expanded read access for the service principal you created. The following Azure resources require specific permissions in the access control of that resource:

- **Storage Account** requires one of the following: Owner, Contributor, Storage Account Contributor.
- **Kubernetes Cluster** requires one of the following: Owner, Contributor, Azure Kubernetes Service Cluster Admin Role.
- **Cosmos DB** requires one of the following: Owner, Contributor, DocumentDB Account Contributor.
- **Function App** requires one of the following: Owner, Contributor, Website Contributor.
- **Snapshot** requires the **Disk Snapshot Contributor** role for scanning virtual machine snapshots with Agentless Assessment.

For more information about these permissions, see [Azure built-in roles](#) in Azure documentation.

To create a custom role and assign it to the service principal:



1. On the home page of the Azure portal, click **Subscriptions**.

The **Subscriptions** page appears.

2. On the left navigation bar, click **Access Control (IAM)**.

The **Access control (IAM)** page for your subscription appears.


3. In the **Create a custom role** section, click **Add**.

The **Create a custom role** page appears.



Home > Subscriptions > tenable-acc-test | Access control (IAM) >


Create a custom role ...

 Got feedback?

Basics Permissions Assignable scopes JSON Review + create

To create a custom role for Azure resources, fill out some basic information. [Learn more](#) 

* Custom role name ⓘ

Tenablecs-ReaderPlusStorageAccountRead 

Description


Custom role for Tenable.cs

Baseline permissions ⓘ

Clone a role

Start from scratch

Start from JSON

"tenablecs_customrole.json" 

Review + create

Previous

Next

4. In **Baseline permissions**, select the **Start from JSON** option.


You can create a custom role in the following ways:



- **Clone a role:** Create a custom role by cloning an existing role and modifying the role, as required.
- **Start from scratch:** Create a custom role by using the Azure user interface.
- **Start from JSON:** Create a custom role by uploading a JSON file with the required permissions.

For more information about these methods, see [Create or update Azure custom roles using the Azure portal](#) in Azure documentation.

Note: This procedure describes how to create a custom role using a JSON file.

5. Click  to upload a JSON file that has the required permissions.

Azure validates the JSON file and uploads the file for role creation.

The following sample JSON file creates a role with read permissions along with the list APIs for the Storage Accounts, Kubernetes cluster, Cosmos DB, and Function App services:

```
{
  "properties": {
    "roleName": "Tenablecs-ReaderPlusStorageAccountRead",
    "description": "Custom role for Tenable Cloud Security",
    "assignableScopes": [
      "/subscriptions/<subscription-id>"
    ],
    "permissions": [
      {
        "actions": [
          "*/read",
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.Storage/storageAccounts/listAccountSas/action",
          "Microsoft.Storage/storageAccounts/listServiceSas/action",
          "Microsoft.Storage/storageAccounts/localusers/listKeys/action",
          "Microsoft.ContainerService/managedClusters/accessProfiles/listCredential/a-
action",
          "Microsoft.DocumentDB/databaseAccounts/listKeys/action",
          "Microsoft.DocumentDB/databaseAccounts/readonlykeys/action",
          "Microsoft.DocumentDB/databaseAccounts/listConnectionStrings/action",
          "Microsoft.Web/sites/config/list/action"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```



The following sample JSON file creates a custom role with read permissions along with permissions to the access snapshots, which is required for Agentless Assessment:


```
{
  "properties": {
    "roleName": "Tenablecs-ReaderPlusDiskSnapshotContributor",
    "description": "Custom role for Tenable Cloud Security",
    "assignableScopes": [
      "/subscriptions/<subscription-id>"
    ],
    "permissions": [
      {
        "actions": [
          "*/read",
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.Storage/storageAccounts/listAccountSas/action",
          "Microsoft.Storage/storageAccounts/listServiceSas/action",
          "Microsoft.Storage/storageAccounts/localusers/listKeys/action",
          "Microsoft.Compute/snapshots/beginGetAccess/action"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

where <subscription-id> is your Azure subscription ID.

6. Click **Review + create**.

The **Review + create** tab appears.

Create a custom role ...

 Got feedback?

[Basics](#) [Permissions](#) [Assignable scopes](#) [JSON](#) [Review + create](#)

Basics

Role name Tenablecs-ReaderPlusStorageAccountRead

Role description Custom role for Tenable.cs

Permissions

Action */read

Action Microsoft.Storage/storageAccounts/listkeys/action

Action Microsoft.Storage/storageAccounts/listAccountSas/action

Action Microsoft.Storage/storageAccounts/listServiceSas/action

Action Microsoft.Storage/storageAccounts/localusers/listKeys/action

Action Microsoft.ContainerService/managedClusters/accessProfiles/listCredential/action

Action Microsoft.DocumentDB/databaseAccounts/listKeys/action

Action Microsoft.DocumentDB/databaseAccounts/readonlykeys/action

Action Microsoft.DocumentDB/databaseAccounts/listConnectionStrings/action

[Create](#)

[Previous](#)

7. Click **Create**.

Azure creates the custom role and redirects you to the **Access control (IAM)** page.

8. In the **Grant access to this resource** section, click **Add role assignment** to assign the custom role to the service principal.

The **Add role assignment** page appears.



9. On the **Role** tab, search for the custom role you created.
10. Select the custom role and click **Next**.

The **Members** tab appears.
11. On the **Members** tab, do the following:
 - a. Click **Select Members**.
 - b. In the **Select members** window, search for the application you created.
 - c. Select the application.

The application appears under **Selected members**.
 - d. Click **Select**.

Azure adds the application for assigning the selected custom role.
 - e. Click **Next**.

The **Review + assign** tab appears.
12. Review the details of the role and click **Review + assign**.

Add role assignment ...

Got feedback?

[Role](#) [Members](#) [Review + assign](#)

Role Tenablecs-ReaderPlusStorageAccountRead

Scope /subscriptions/ ████████████████████

Members	Name	Object ID	Type
	tenablecs-app	████████████████████	App

Description No description

Azure assigns the custom role to the service principal of the application and redirects you to the **Access control (IAM)** page.

Assign the Reader role to the service principal



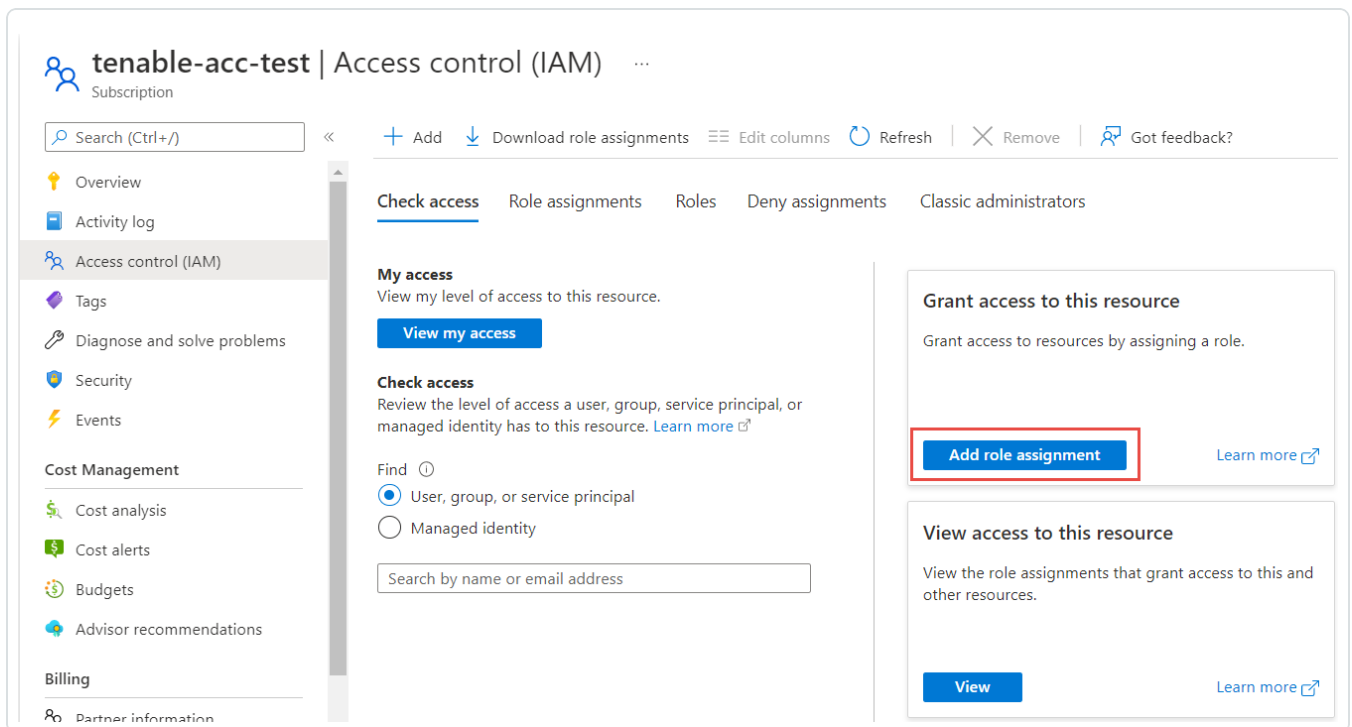
Tenable Cloud Security requires the **Reader** role for accessing the resources for a cloud scan. This role provides limited permissions to the service principal. If you want to perform a comprehensive scan including managed clusters and storage accounts, [create a custom role with expanded read permissions](#).

1. On the home page of the Azure portal, click **Subscriptions**.

The **Subscriptions** page appears.

2. On the left navigation bar, click **Access Control (IAM)**.

The **Access control (IAM)** page for your subscription appears.



3. In the **Grant access to this resource** section, click **Add role assignment**.

The **Add role assignment** page appears.

4. On the **Role** tab, search for the **Reader** role.



Home > Subscriptions > tenable-acc-test >

Add role assignment

Got feedback?

[Role](#) [Members](#) [Review + assign](#)

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Reader Type: All Category: All

Showing 71 of 348 roles

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Disk Backup Reader	Provides permission to backup vault to perform disk backup.	BuiltInRole	Other	View
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View

5. Select the **Reader** role and click **Next**.

The **Members** tab appears.

6. On the **Members** tab, do the following:

- Click **Select Members**.
- In the **Select members** window, search for the application you created.
- Select the application.

The application appears under **Selected members**.

Home > Subscriptions > tenable-acc-test >

Add role assignment

Got feedback?

[Role](#) [Members](#) [Review + assign](#)

Assign access to User, group, or service principal
 Managed identity

Members [+ Select members](#)

Name	Object ID	Type
No members selected		

Description

Select members

Select

- TenableCS
- Tenablecsappreggarnation

Selected members:

- tenablecs-app**

d. Click **Select**.

Azure adds the application for assigning the **Reader** role.



Home > Subscriptions > tenable-acc-test >

Add role assignment

Got feedback?

Role **Members** Review + assign

Assign access to User, group, or service principal
 Managed identity

Members + Select members

Name	Object ID	Type	
tenablecs-app	[REDACTED]	App	

Description Optional

e. Click **Next**.

The **Review + assign** tab appears.

7. Review the details of the role and click **Review + assign**.

Home > Subscriptions > tenable-acc-test >

Add role assignment

Got feedback?

Role Members **Review + assign**

Role Reader

Scope [REDACTED]

Name	Object ID	Type
tenablecs-app	[REDACTED]	App

Description No description

Azure assigns the role to the service principal of the application and redirects you to the **Access control (IAM)** page.

Create a client secret

You can create a new application secret to authenticate the service principal.



1. On the home page of the Azure portal, click **App Registrations**.
2. Click the application that you created for Tenable Cloud Security.
3. On the left navigation bar, click **Certificates & secrets**.

The **Certificates & secrets** page appears.

4. Click **New client secret**.

The **Add a client secret** page appears.

Add a client secret ✕

Description

Expires

5. Provide a relevant description for the secret. For example, Tenable Cloud Security Scan.
6. Set an expiration for the client secret.
7. Click **Add**.

The client secret value and ID appear.

Certificates (0)	Client secrets (1)	Federated credentials (0)	
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.			
+ New client secret			
Description	Expires	Value ⌵	Secret ID
Password uploaded on Wed Jul 27 2022	1/27/2023	<input type="text" value=""/>	<input type="text" value=""/>

8. Record the **Value** of this client secret.

Note: You cannot view this value again because Azure masks this value.

What to do next:

[Onboard an Azure Account](#)

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



- Client ID
- Tenant ID
- Secret value



Onboard an Azure Account


In Tenable Cloud Security, you can connect your Microsoft Azure cloud account using a service principal. In Microsoft Azure, a service principal is an entity that requires access to the resources secured by an Azure Active Directory tenant.

Before you begin:

- Ensure you have the following Azure values:
 - Client ID
 - Secret value
 - Tenant ID

For more information, see [Create an Azure Service Principal Role](#).

To connect an Azure subscription with a service principal:

1. In the left navigation bar, click  > **Connection** > **Azure subscription**.
2. In the **Choose a workflow to discover Azure subscriptions** section, click **Service principal (recommended)**.
3. Click **Continue**.
4. In the **Discover Azure subscription(s)** section, enter your **Client ID**, **Secret value**, and **Tenant ID**.
5. Click **Continue**.

Tenable Cloud Security connects to your Microsoft Azure account using the specified credentials, and displays the list of subscriptions.

6. In the **Choose Azure subscription(s)** section, select the required subscriptions.
7. Click **Continue**.
8. For the selected subscriptions, in the **Choose resource group(s)** section, do one of the following:



- To select all available resource groups, click **All (recommended)**.
- To select specific resource groups, click **Specific**, and select a resource group in the list.

Tip: You can search for specific resource groups, and filter the list by subscriptions.

9. Click **Continue**.
10. (Optional) In the **Choose projects to add the Azure project(s) to** section, create or select a project for the Azure subscription.
 - To create a new project for your Azure account, click **Add a project**. For more information, see [Create a Project](#).
 - Select a project from the list.

Tip: You can also search for specific projects.

11. Click **Connect Cloud Account**.

On the **Projects & Connections** page, you can view the Azure project with the connected Azure account and view the selected VPCs.



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 a misconfiguration scan for your cloud account. A misconfiguration scan scans for policy violations in IaC repositories and cloud resources. You can view the scan results on the **Findings > [Misconfigurations](#)** page.

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.

To create a scan profile:

1. Click **Projects & Connections**.

Tenable Cloud Security displays the list of 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.

3. Click **New Scan Profile**.

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

4. Edit the scan profile name or retain the default name.
5. In **Step 1**, in the **Cloud config assessment options** section, select all applicable resources.

Note: You can search for resources in the **Search resources** box.

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

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

For information about how to initiate the scan for the scan profile, see [Run a Cloud Scan](#).



Schedule a Scan

You can add a scan schedule to your scan profile and run scans at regular intervals.

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.

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](#).