



Qualys OCI Vulnerability Scanning Service BYOL

Onboarding Guide

March 13, 2023

Copyright 2023 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Introduction to OCI BYOL Support	4
Pre-requisites.....	4
Deploying Qualys Agent on OCI Platform	4
Generate Qualys Cloud Agent License Code	5
Create a Vault to Store the Qualys License Information	6
Define a Secret for Scan Recipe	6
Create a Scan Recipe for Host Instances	8
Create a Target to Assign a Scan Recipe.....	11
Appendix A: Permissions and Policies	13
Grant Access to the VSS Service	13
Grant Permission to Group of Administrators to Access to VSS Service	13
Set up the Policies and Dynamic Groups for VSS – Qualys BYOL.....	14

Introduction to OCI BYOL Support

BYOL is a Bring Your Own License. With this feature users can use Oracle Cloud Infrastructure (OCI) with their Own Qualys License. BYOL enables Qualys VM scanning for instances on OCI. OCI Vulnerability Scanning Service (VSS) is integrated with Qualys. VSS can set up Qualys Agent on OCI instances.

Users can configure a Qualys Agent based scan from the OCI console. Qualys agents collect the instances data and push it to Qualys VMDR where scanning is performed. The count of unique vulnerabilities out of the identified or detected vulnerability and then forward the result to VSS.

VSS displays the results in the VSS application and forwards the result to Cloud Guard for global alerting of security problems. Qualys VMDR, VSS and Cloud Guard provides the complete security posture of the instances.

Pre-requisites

For using BYOL feature, following are the pre-requisites:

- Ensure that Oracle has enabled the OCI BYOL features for your account. Oracle VSS is required for the functionality of this feature.
- Ensure VSS agent is installed.
- Set up policies:
 - Grant access to the VSS service.
 - Grant permission to group of administrators to access to VSS.For more details on policies, refer to [Appendix A](#).

Deploying Qualys Agent on OCI Platform

Users can create one scan recipe, one target and start viewing findings about their host (compute) instances. For implementing integration between the OCI platform and Qualys platform, follow these steps:

1. [Generate Qualys Cloud Agent License Code](#)
2. [Create a Vault to Store the Qualys License Information](#)
3. [Define a Secret for Scan Recipe](#)
4. [Create a Scan Recipe for Host Instances](#)
5. [Create a Target to Assign a Scan Recipes](#)

Generate Qualys Cloud Agent License Code

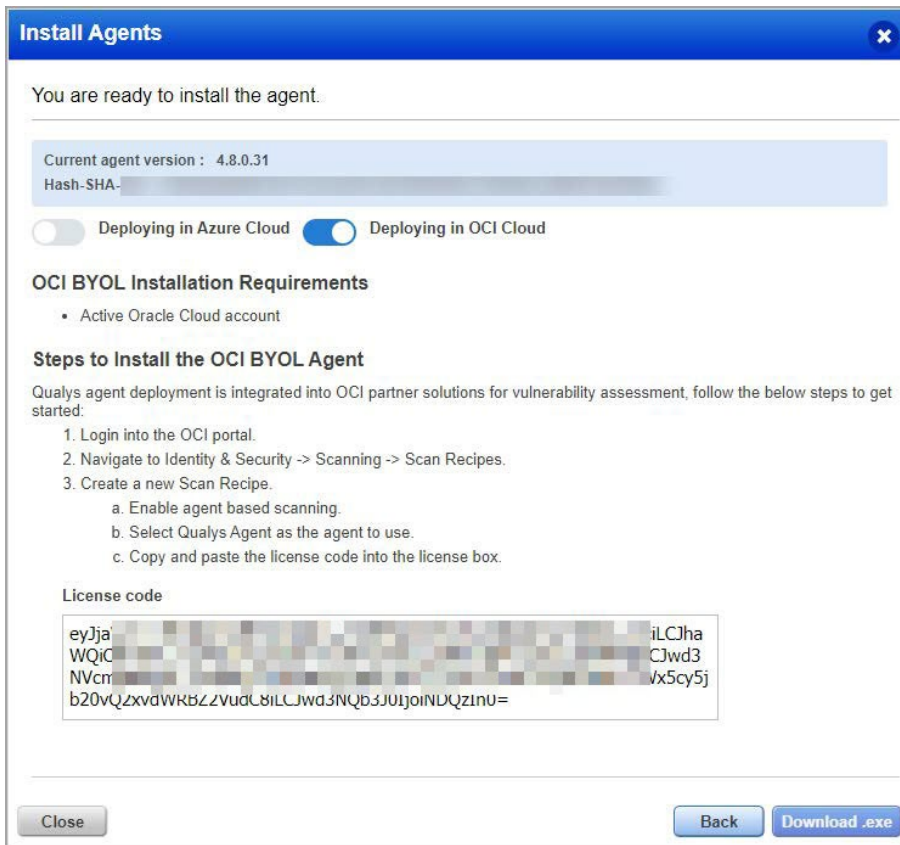
You need to generate the license code. To generate a license, you must generate a Cloud Agent Activation Key and enable OCI for the Qualys cloud agent. Perform these tasks using the Cloud Agent application.

Follow these steps to generate a license code:

1. Login to **Cloud Agent** (CA) application.
2. Navigate to **Agent Management > Activation Keys** (or go to the Activation Keys tab).
3. Select **New Key** to create a new activation key.

An activation key is used to install agents.

4. Select the activation key and click **Install Agent** from the **Actions** menu.
5. In the **Install Agents** screen, click **Install instructions** for the required agent > **Deploying in OCI Cloud**.



6. Copy the **License code**.

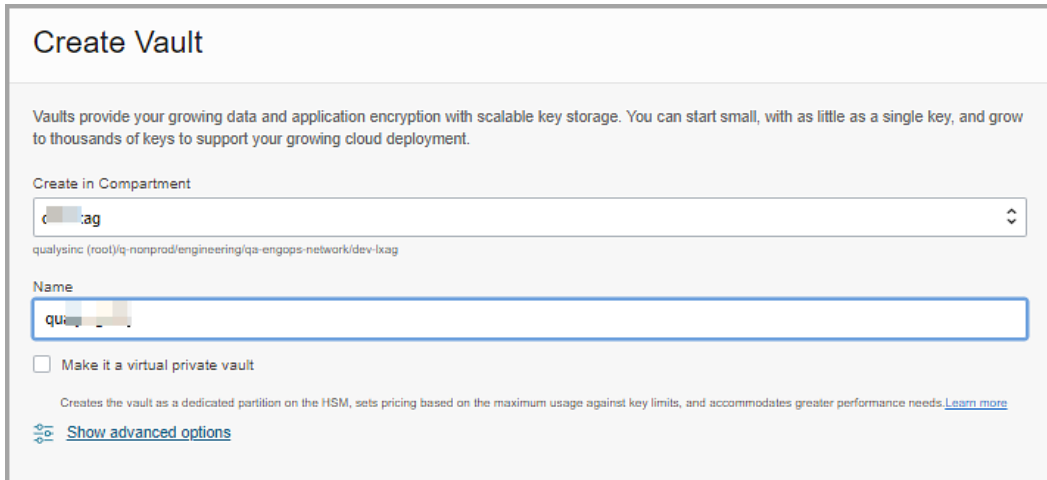
You have license code now, you need this license code while creating a vault and secret.

Create a Vault to Store the Qualys License Information

You can store your Qualys License information in a vault secret. You need to create the vault, define the secret. Follow these steps to create a vault.

1. Log in to **Oracle Cloud > Vault > Create Vault**.
2. From **Create in Compartment**, select the compartment and provide the **Name** for the vault.

Note: Ensure you have vault permissions.



The vault is created. A listing page with all the vaults is displayed.

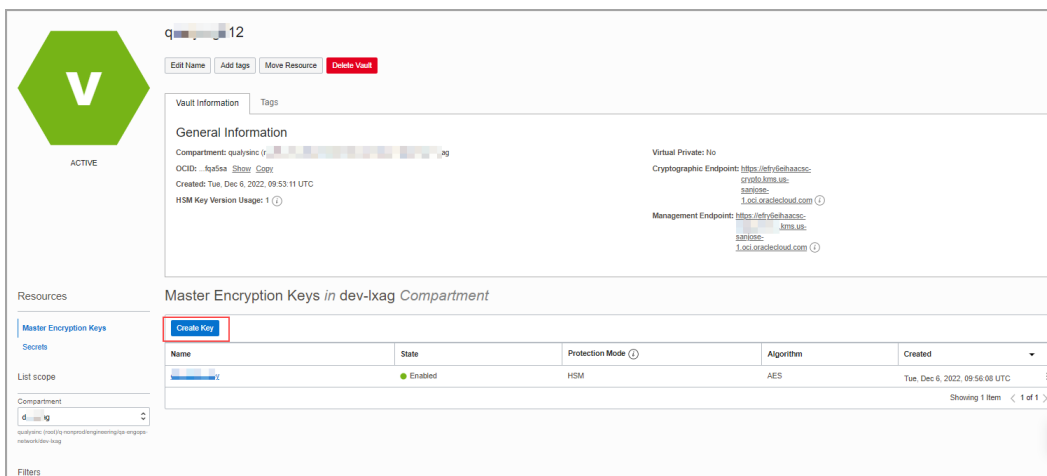
Define a Secret for Scan Recipe

You need to define a secret for scan recipe. Secret is used to store the Qualys license information in the vault.

Follow these steps to create a secret:

Before creating a secret, create a secret key.

1. From the vault detail, click **Create Key**.



The Create Key window is displayed.

- From **Create in Compartment**, select the compartment, **Protection Mode** as HSM and provide the **Name** of the key.

Create Key

Create in Compartment
de...g
qualysinc (root)/q-nonprod/engineering/qa-engops-network/dev-ixag

Protection Mode ⓘ
HSM

Name
gk...-key

Key Shape: Algorithm ⓘ
AES (Symmetric key used for Encrypt and Decrypt)

Key Shape: Length
256 bits

Import External key

Create a new key by importing a wrapped file containing key data that matches the specified key shape. For more information, see [Importing Keys](#).

[Show advanced options](#)

- To encrypt the key, go to **Secrets** and click **Create Secret**.

Identity & Security > Vaults > Vault Details

qu...12

Edit Name Add tags Move Resource Delete Vault

Vault Information Tags

ACTIVE

General Information

Compartment: qualysinc (root)/q-nonprod/engineering/qa-engops-network/dev-ixag

OCID: ...tqa0sa [Show Copy](#)

Created: Tue, Dec 6, 2022, 09:53:11 UTC

HSM Key Version Usage: 4 ⓘ

Virtual Private: No

Cryptographic Endpoint: <https://efry6eihaacsc-crypto.kms.us-sanjose-1.oci.oraclecloud.com> ⓘ

Management Endpoint: <https://efry6eihaacsc-management.kms.us-sanjose-1.oci.oraclecloud.com> ⓘ

Resources

Master Encryption Keys

Secrets

List scope

Secrets in dev-ixag Compartment

Create Secret

Name	Status	Created
...	Active	Tue, Dec 6, 2022, 09:59:46 UTC

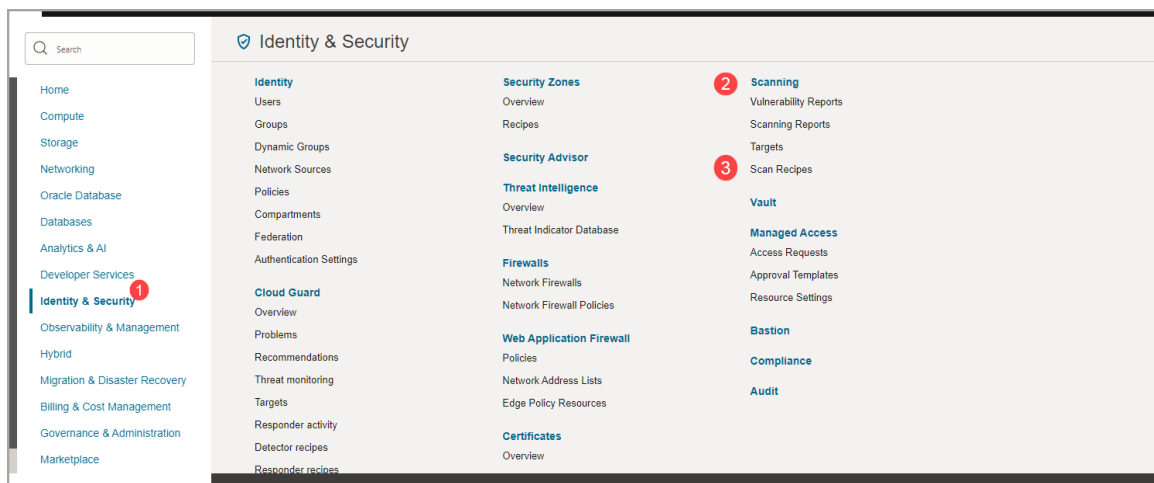
- From **Create in Compartment**, provide **Name** and **Description**, and select the **Encryption Key**.
- Select the **Secret Type Template** from the list and paste the license code you copied into the **Secret Contents**.
- To store the information, click **Crete Secret**.

The Secret is created for scan recipe.

Create a Scan Recipe for Host Instances

Oracle Cloud Infrastructure Vulnerability Scanning Service creates recipes that scan target host's instances. To create a scan recipe, follow these steps:

- Go to **Identity & Security > Scanning > Scan Recipes**.



- From the Hosts tab, click **Create**.

Scanning

- Vulnerability Reports
- Scanning Reports
- Targets
- Scan Recipes**

List scope

Compartment

qualysinc (root)/q-nonprod/engineering/qa-engops-network/dev-ixag

Filters

State

Tag filters [add](#) | [clear](#)

no tag filters applied

Scan Recipes in **ig** Compartment

Create a recipe to control how resources are scanned. After creating a recipe, assign it to targets. [Learn more](#)

i Qualys BYOL option now available. See the agent option in host [scan recipe](#)

Hosts | Container image

Create

Name	Status	Created	
...au5	● Active	Wed, Jan 11, 2023, 08:08:11 UTC	⋮
gk6:...an_recipe	● Active	Tue, Jan 10, 2023, 11:45:54 UTC	⋮
BYOL...tag	● Active	Wed, Dec 7, 2022, 10:54:27 UTC	⋮
BY...cipe	● Active	Tue, Dec 6, 2022, 10:04:32 UTC	⋮

Showing 4 items < Page 1

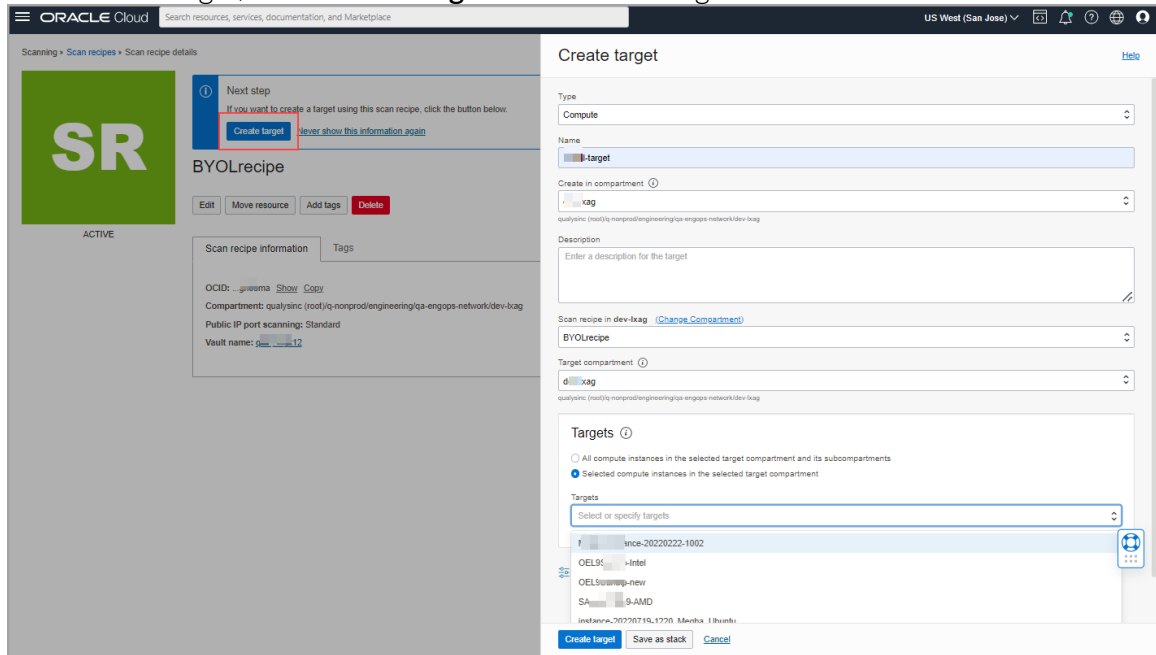
3. Enter the **Name** for the recipe.
 4. From **Create in compartment**, select the compartment where you want to store the recipe.
 5. Select Qualys for the **Agent based scanning**, and select the vault and secret that you stored your Qualys license.
- Note:** You can enter the license information directly into a new secret
6. Click **Create scan recipe** to save the information.

Scan recipe to scan target host instances is created.

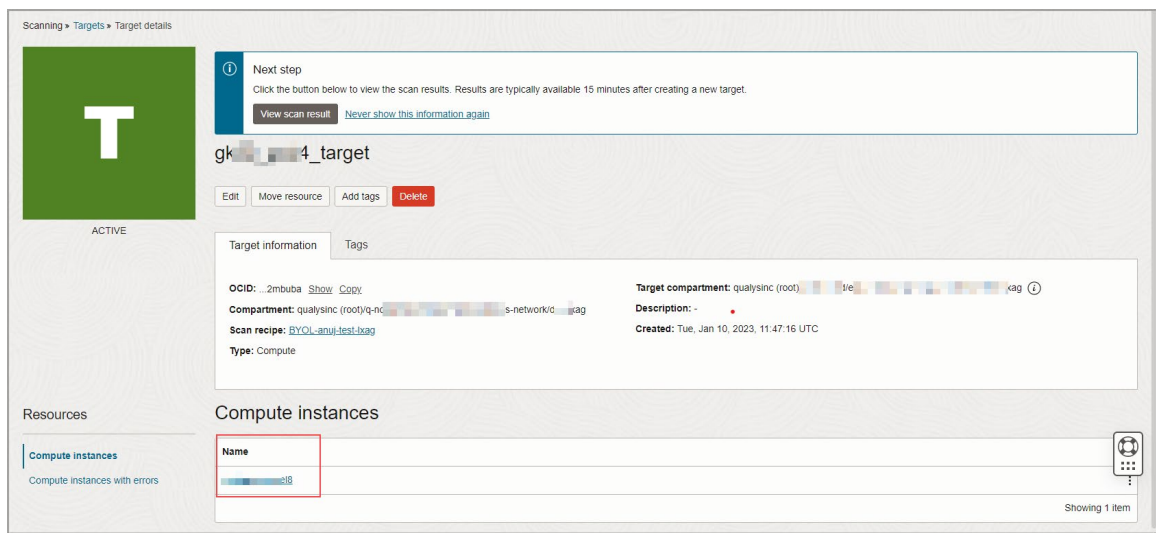
Create a Target to Assign a Scan Recipe

A target is a group of cloud resources you want to be scanned for vulnerabilities. Create a target for assigning it to scan recipe.

1. Click **Create target** from the Scan recipe details window.
This new target uses the scan recipe that you have just created.
2. Enter **Name** of the target.
3. From **Create in compartment**, select the compartment.
4. Provide **Description** and select scan recipe from the list.
5. Select the **Target compartment**, and scan all or a subset of your instances as required.
6. To save the target, click **Create target** from Create target window.



You can view the target Target Information tab's details and status in Computer instances.



You have completed the set up now, you can see the results in VSS (Vulnerability Scanning Service).

Appendix A: Permissions and Policies

To use the BYOL feature, you must set up policies in VSS (Vulnerability Scanning Service). Refer the following policies and permission required:

- Grant the following:
 - [Permission access to the VSS service](#)
 - [Permission to group of administrators to access to VSS service](#)
- [Set up the policies and dynamic groups for VSS – Qualys BYOL](#)

Grant Access to the VSS Service

- Allow VSS access in tenancy OR compartment.
- Allow to manage instances.
- Allow to read compartments, vnics, vnics-attachements.
- Allow to read repos for VSS OCIR container image scans.

Grant Permission to Group of Administrators to Access to VSS Service

- Allow groups access to VSS in the tenancy OR compartment.
- Allow admins to manage vss-family to allow all scan settings.
- Allow admins to read repos for container image scanning.

Statements
Edit Policy Statements
Allow Service vulnerability-scanning-service to manage instances in tenancy
Allow Service vulnerability-scanning-service to read compartments in tenancy
Allow service vulnerability-scanning-service to read vnics in tenancy
Allow service vulnerability-scanning-service to read vnic-attachments in tenancy
Allow Group VSS_Admins to manage vss-family in tenancy
Allow Group VSS_Admins to read repos in tenancy

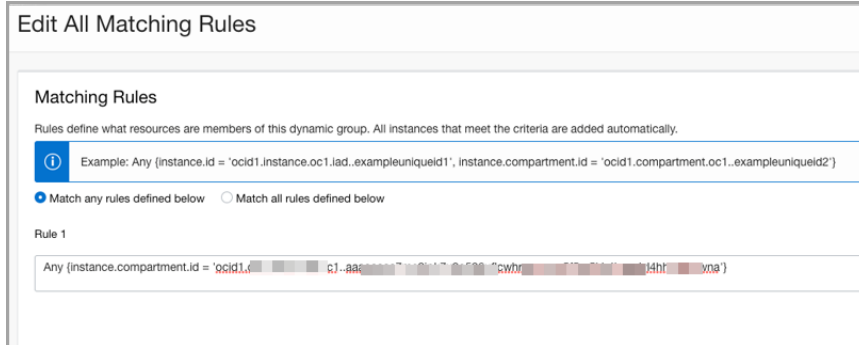
Set up the Policies and Dynamic Groups for VSS - Qualys BYOL

Create a dynamic group of instances that you want to scan.

For example:

The dynamic group includes instances that meet the criteria defined by any of the following rules. (Select - Match any rules defined)

```
Any {instance.compartment.id = '<compartment-ocid-of-your-instances-or-This-could-even-be-the-whole-tenancy>' }
```



Policy for granting permission for the instances to access secrets

This allows the Qualys agents to get the Qualys license data and send that in communications to the Qualys data center.

- Allow dynamic-group <your-qualys-instances-group> to read vaults in the tenancy
- Allow dynamic-group <your-qualys-instances-group> to read keys in the tenancy.
- Allow dynamic-group <your-qualys-instances-group> to read secret-family in the tenancy

Need to get access to the data sent back from Qualys

- Define tenancy ocivssprod as
ocid1.tenancy.oc1..aaaaaaaa6zt5ejxod5pgthsq4apr5z2uzde7dmbpduc5ua3mic4z
v3g5ttma
- Endorse dynamic-group <your-qualys-instances-group> to read objects in tenancy ocivssprod

Following screenshot shows policies set up for dynamic group of instances.

