To scan a repository in **CoreOS Quay**, create a new registry scan setting.

### Create a new registry scan

**Prerequisites:**

* You have [installed a Defender](https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma/prisma-cloud/prisma-cloud-admin-compute/install/deploy-defender/defender_types.html) somewhere in your environment.

**STEP 1:** Log in to Console, and select **Defend > Vulnerabilities > Images > Registry settings**.

**STEP 2:** Select **Add Registry**.

**STEP 3:** in the dialog, enter the following:

1. From the **Version** drop-down list, select CoreOS Quay
2. In **Registry**, enter the URL for the registry.
3. In **Repository**, enter the repository to scan.  
   If you leave this field blank or enter a wildcard, Prisma Cloud finds and scans all repositories in the registry.  
   If you specify a partial string that ends with a wildcard, Prisma Cloud finds and scans all repositories that start with the partial string.  
   If you specify an exact match, Prisma Cloud scans just the specified repository.
4. In **Tag**, enter an image tag. Leave this field blank to scan all tags.
5. In **Credential**, Select a credential from the drop-down list. If there are no credentials in the list, click **Add new**, and create a **Basic authentication** credential with the service account username and password.
6. In **OS type**, specify whether the repo holds **Linux** or **Windows** images.
7. In **Scanners scope**, specify the collections of defenders to use for the scan.
8. In **Number of scanners**, enter the number of Defenders across which scan jobs can be distributed
9. **Cap** the number of images to scan.  
   Specify the maximum number of images to scan in the given repository, sorted according to last modified date. To scan all images in a repository, set **Cap** to 0.
10. Save Add

**STEP 4: Select Save and scan.**

1. Verify that the images in the repository are being scanned under **Monitor > Vulnerabilities > Images > Registries**.