



# Your guided setup for cloud discovery in Sectigo Certificate Manager (SCM)

This guide helps you explore how Sectigo Certificate Manager simplifies cloud certificate discovery. In just a few steps, you'll learn how to set up a scan, organize discovered certificates into buckets, apply assignment rules, and gain complete visibility across your environment, without the manual overhead.

Want to see it in action? [Watch the step-by-step walkthrough on YouTube](#)

## Quick Navigation

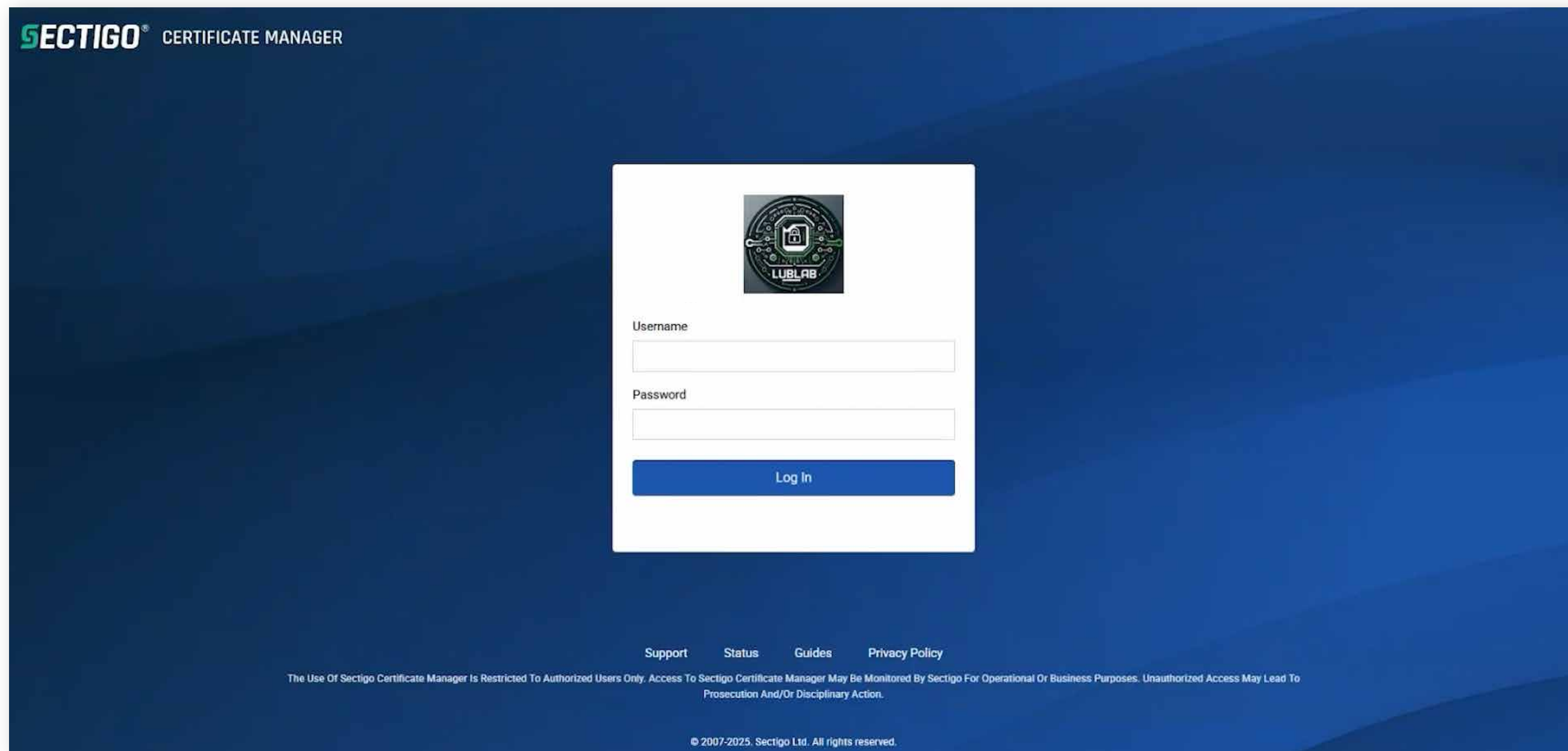
Step 1 - Log in	03
Step 2 - Set up a certificate bucket	04
Step 3 - Add an assignment rule to the bucket	06
Step 4 - Configure a cloud-discovery scan	09
Step 5 - Run a manual scan	13
Step 6 - View your scan results	16
Step 7 - View your discovered certificates in SCM	19



## Step 1 - Log in

Start by logging in to your Sectigo Certificate Manager account.

Sign in using your email, single sign-on (SSO), or Sectigo's authentication service.



The image shows the Sectigo Certificate Manager login page. The background is a dark blue gradient. In the top left corner, the 'SECTIGO' logo is in green and white, followed by 'CERTIFICATE MANAGER' in white. In the center, there is a white login box. Inside this box, at the top, is a circular logo for 'LUBLAB' with a padlock icon. Below the logo are two input fields: 'Username' and 'Password'. Below these fields is a blue 'Log In' button. At the bottom of the page, there are links for 'Support', 'Status', 'Guides', and 'Privacy Policy'. Below these links is a small line of text: 'The Use Of Sectigo Certificate Manager Is Restricted To Authorized Users Only. Access To Sectigo Certificate Manager May Be Monitored By Sectigo For Operational Or Business Purposes. Unauthorized Access May Lead To Prosecution And/Or Disciplinary Action.' At the very bottom, there is a copyright notice: '© 2007-2025. Sectigo Ltd. All rights reserved.'

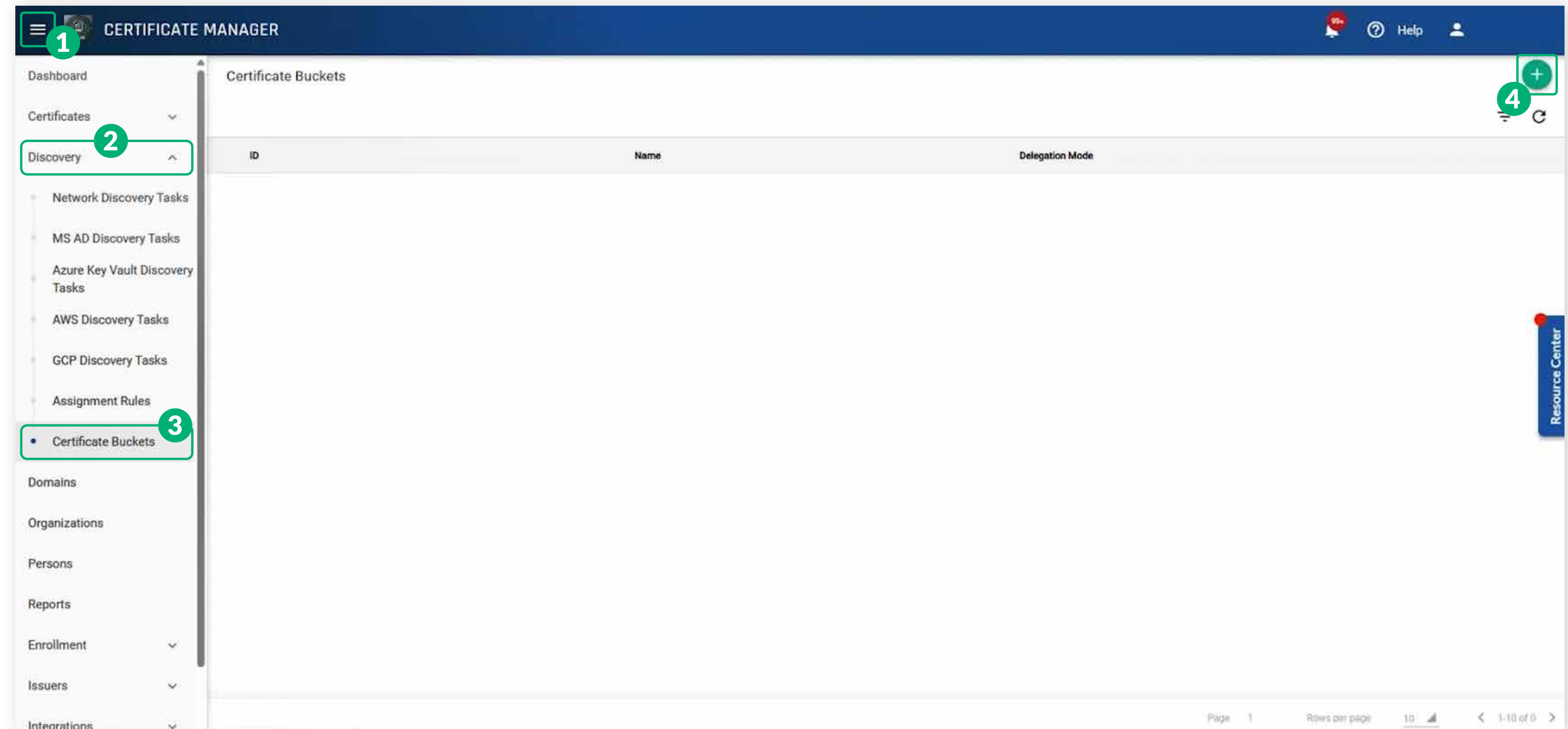


## Step 2 - Set up a certificate bucket

Buckets help you organize certificates found during a scan. Every certificate will be automatically assigned to the bucket linked to the task that discovered it, so it's helpful to create one before scanning.

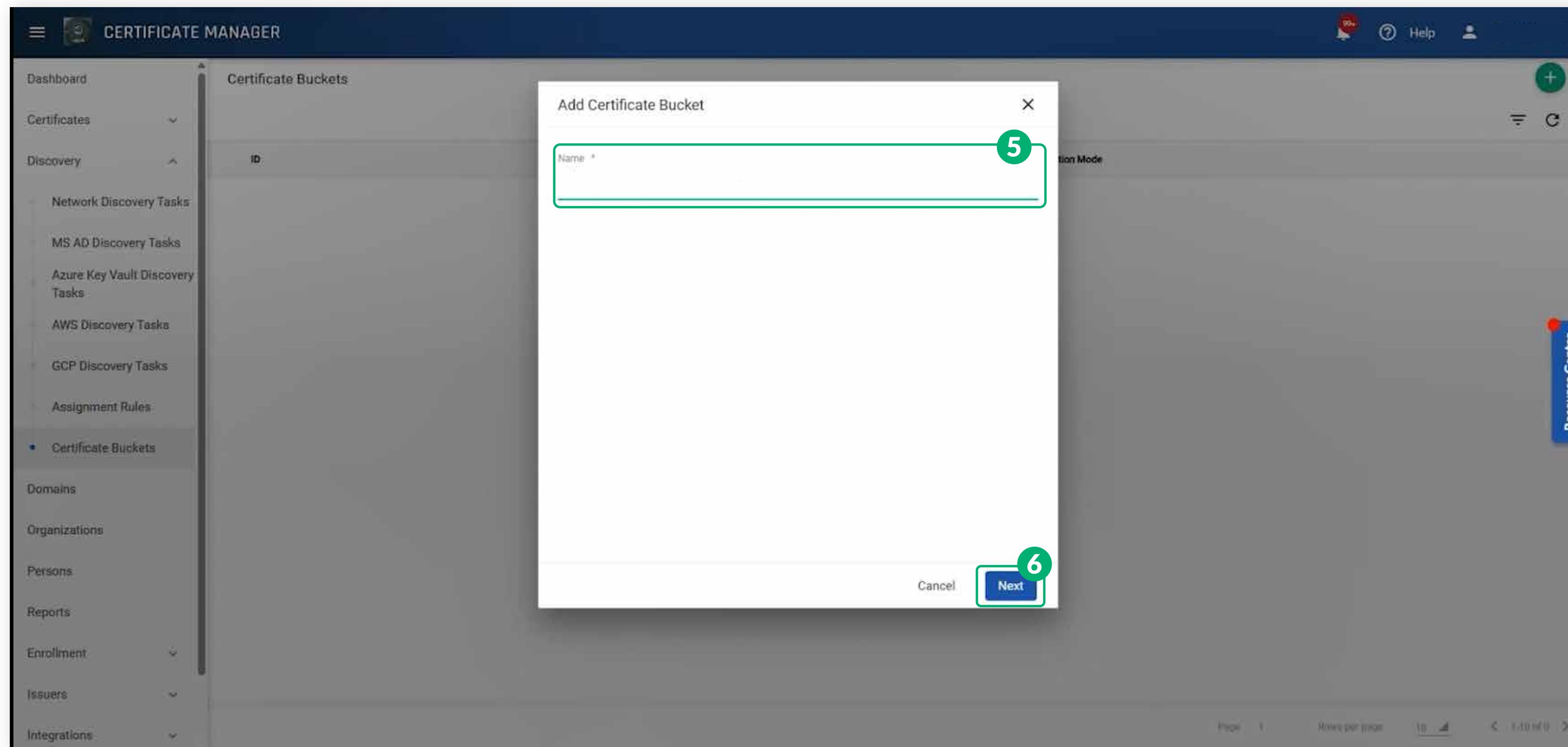
To create a bucket:

1. Click the [Menu](#) icon.
2. Go to [Discovery](#) tab.
3. Click [Certificate Buckets](#).
4. Click the [Add \(+\)](#) icon to create a new bucket.





5. Give your bucket **a name** (e.g. “Cloud Scan - Prod”).
6. Click **Next** to continue.





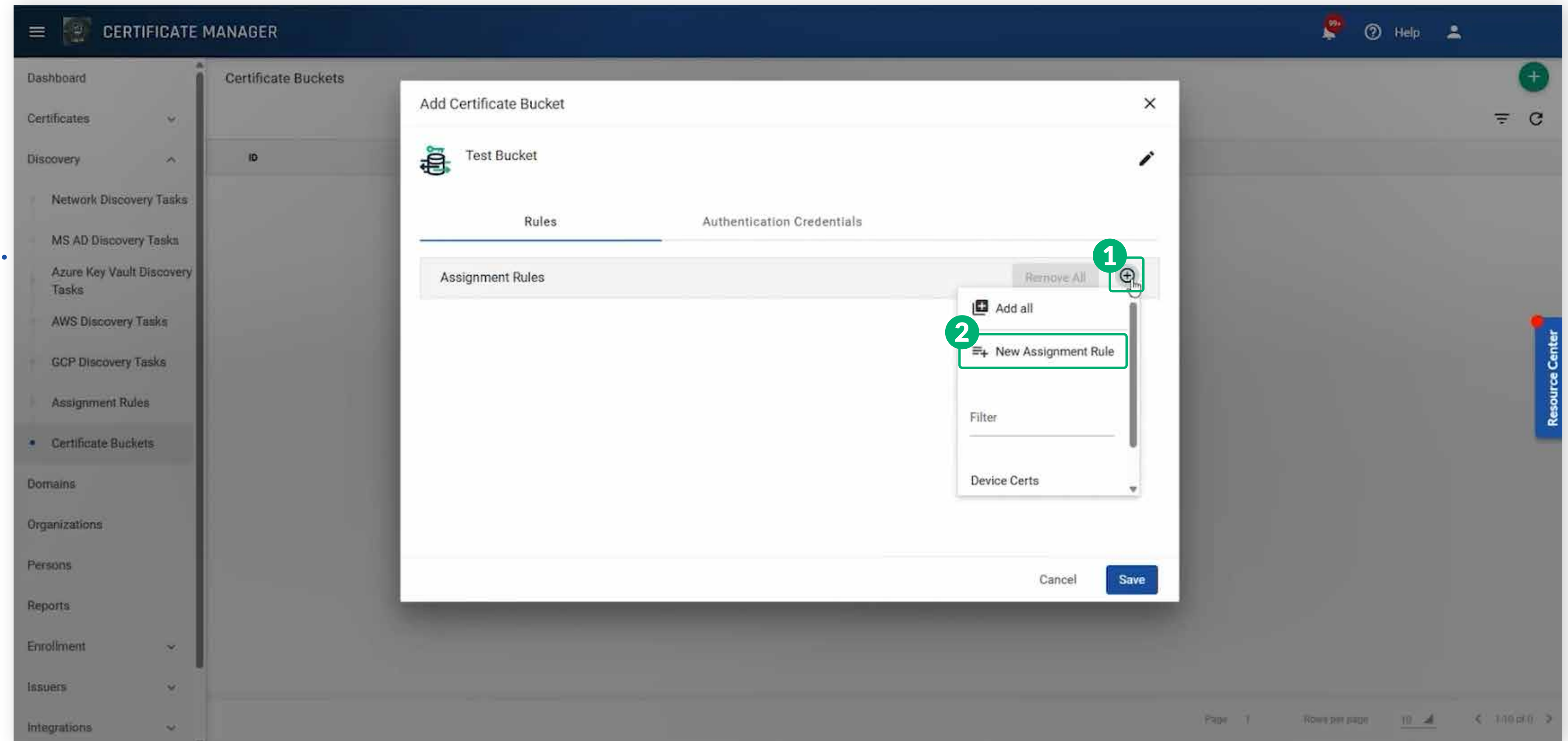
## Step 3 - Add an assignment rule to the bucket

Next, it's time to define the assignment rule.

Assignment rules help SCM know where to route discovered certificates, either by department, region, environment, or any logic you define. This helps keep your certificate inventory organized and easy to manage.

To create a rule (continuing from Step 2):

1. Click the **Add (+)** icon
2. Select **New Assignment Rule**.





3. **Give your rule a name.** This rule will apply to the bucket you're setting up and can be reused across multiple buckets.
4. **Assign the certificates** to a specific organization or department, or leave it as default.

**CREATE NEW ASSIGNMENT RULE**

Name \*

If certificate discovered meets all conditions below

Conditions Remove All +

Assign to ...

Organization  
Lublab

Department  
None

Certificate Type \*  
SSL Certificate

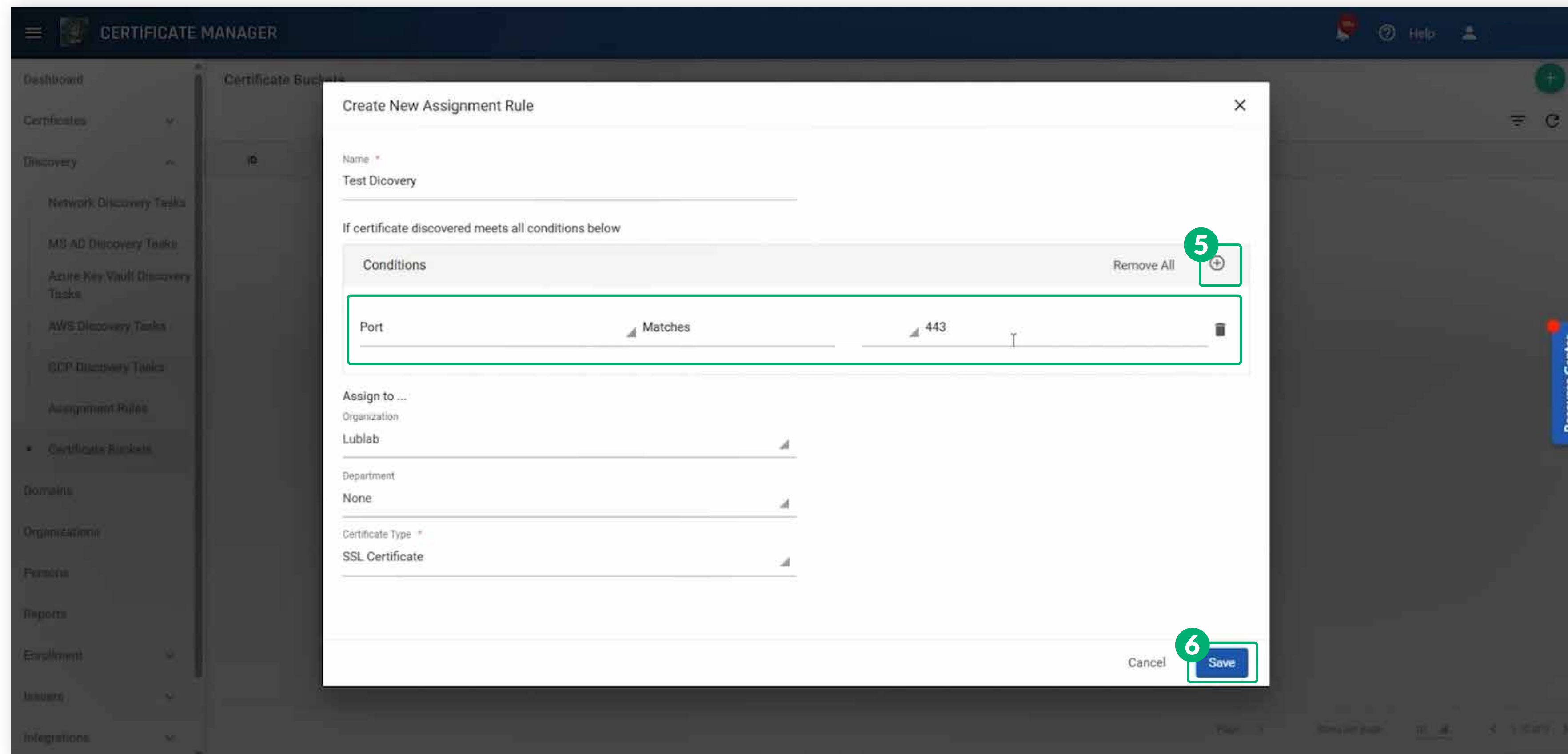
Cancel Save



5. Click the **Add (+)** icon to set conditions. Each rule requires at least one condition.

Add more conditions if needed. These use **AND** logic, so all must be met for a certificate to match.

6. **Click Save** to apply the rule, then click Save again to finalize your bucket.



**Example:** Filter for certificates discovered on port 443; anything else will be excluded.

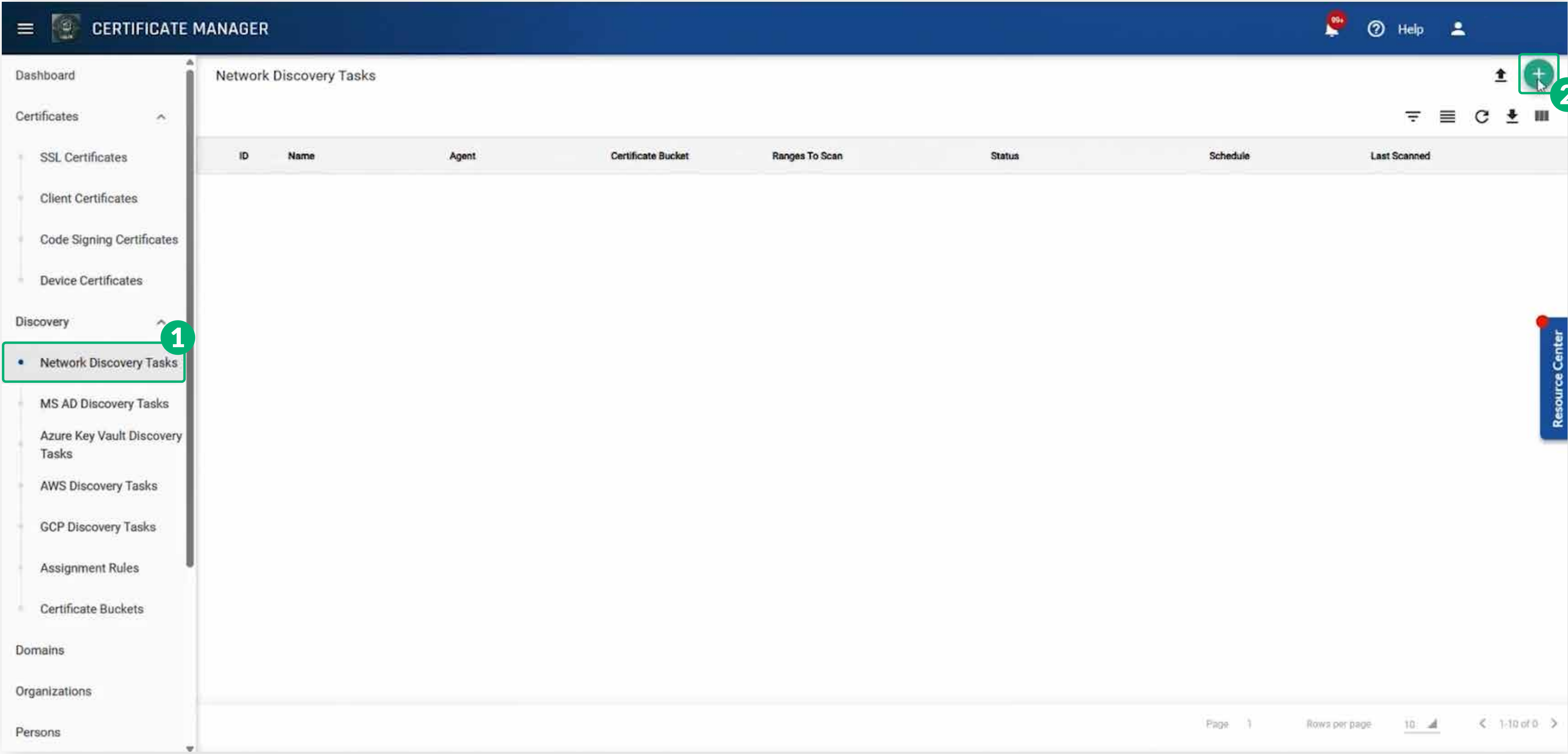


# Step 4 - Configure a cloud-discovery scan

With your bucket ready, it's time to set up the scan to find certificates in your cloud environment.

To set up the scan:

- 1. Go to [Discovery](#) → [Network Discovery Tasks](#).
- 2. Click the [Add \(+\)](#) icon.





3. Give your scan **a name**.
4. Select **Cloud** in the agent field.
5. Choose the **certificate bucket** you just created.
6. Click **Add** next to **Ranges to Scan**.

**CERTIFICATE MANAGER**

Dashboard

Certificates

- SSL Certificates
- Client Certificates
- Code Signing Certificates
- Device Certificates

Discovery

- Network Discovery Tasks
- MS AD Discovery Tasks
- Azure Key Vault Discovery Tasks
- AWS Discovery Tasks
- GCP Discovery Tasks
- Assignment Rules
- Certificate Buckets

Domains

Organizations

Persons

Network Discovery Tasks

ID Name

Add Network Discovery Task

General Schedule

Name \*

Agent

Cloud

Certificate Bucket \*

Select...

Ranges to Scan

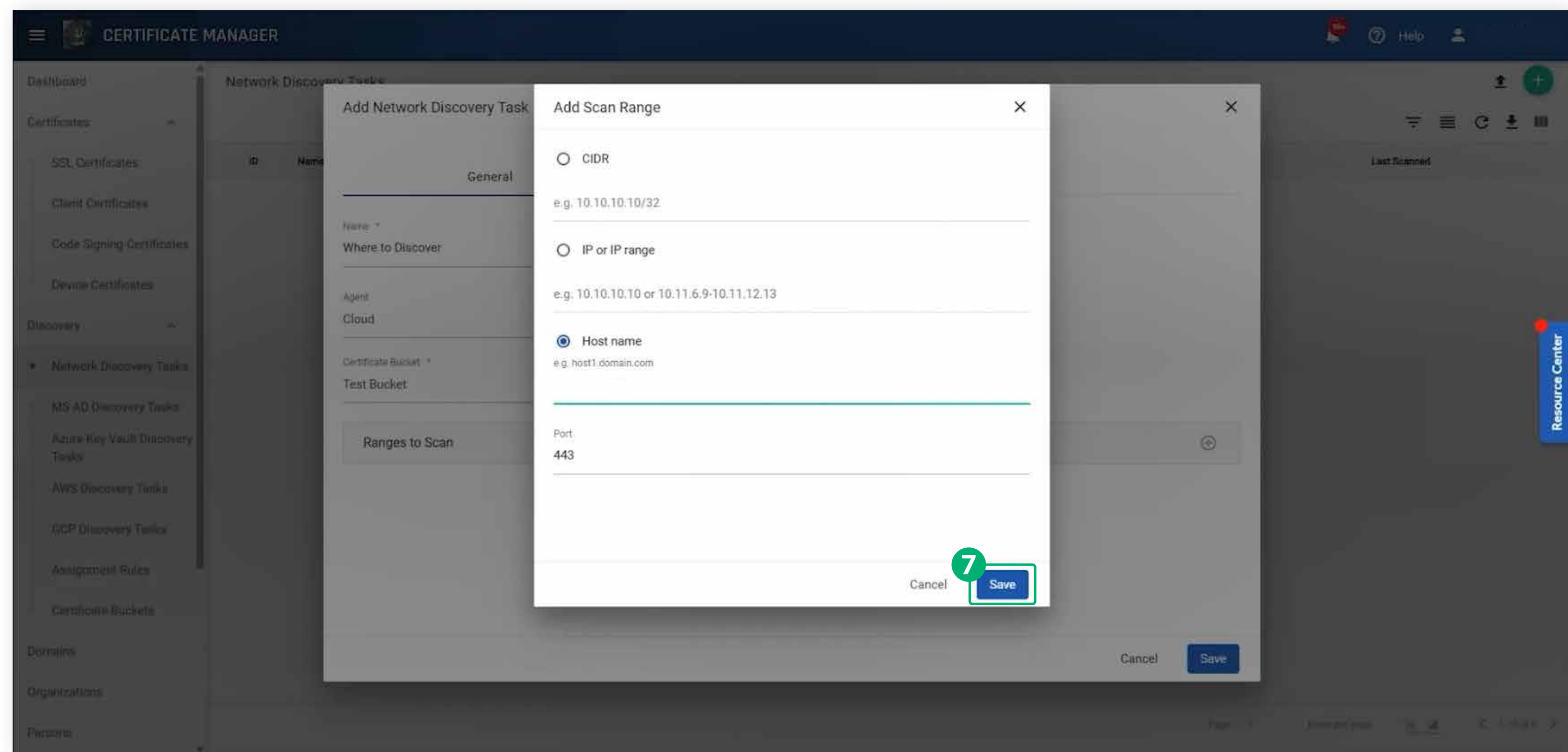
Cancel Save

Resource Center



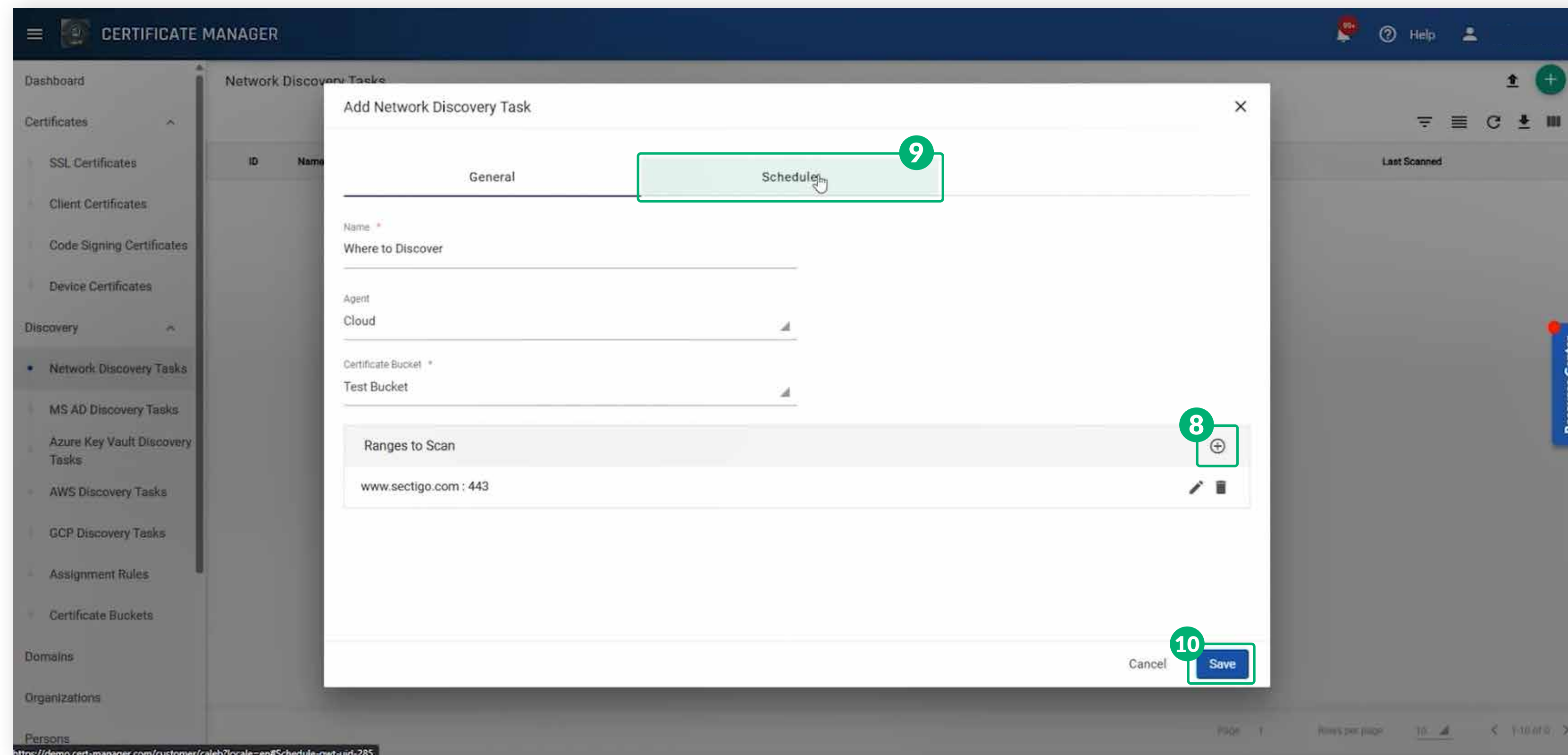
You can define the scan using CIDR, IP, or hostname. For ports, enter a single port, multiple ports separated by commas, or a range using a dash.

7. When finished, click **Save**.





8. To add more ranges, click **Add(+)** again, and repeat these steps.
9. (Optional) Click the **Schedule** tab to set how often the scan runs.
10. When done, click **Save**.

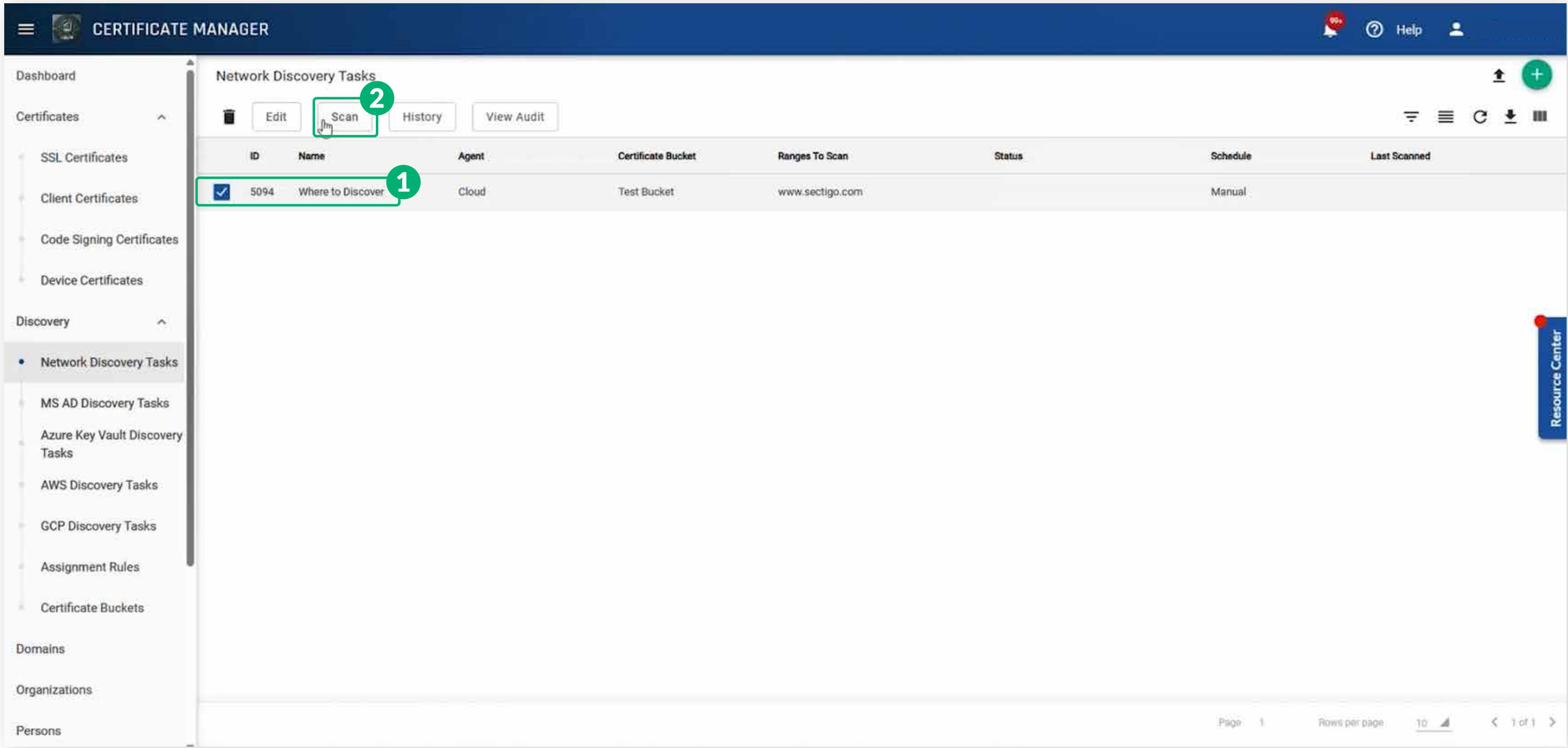




# Step 5 - Run a manual scan

To run the scan manually:

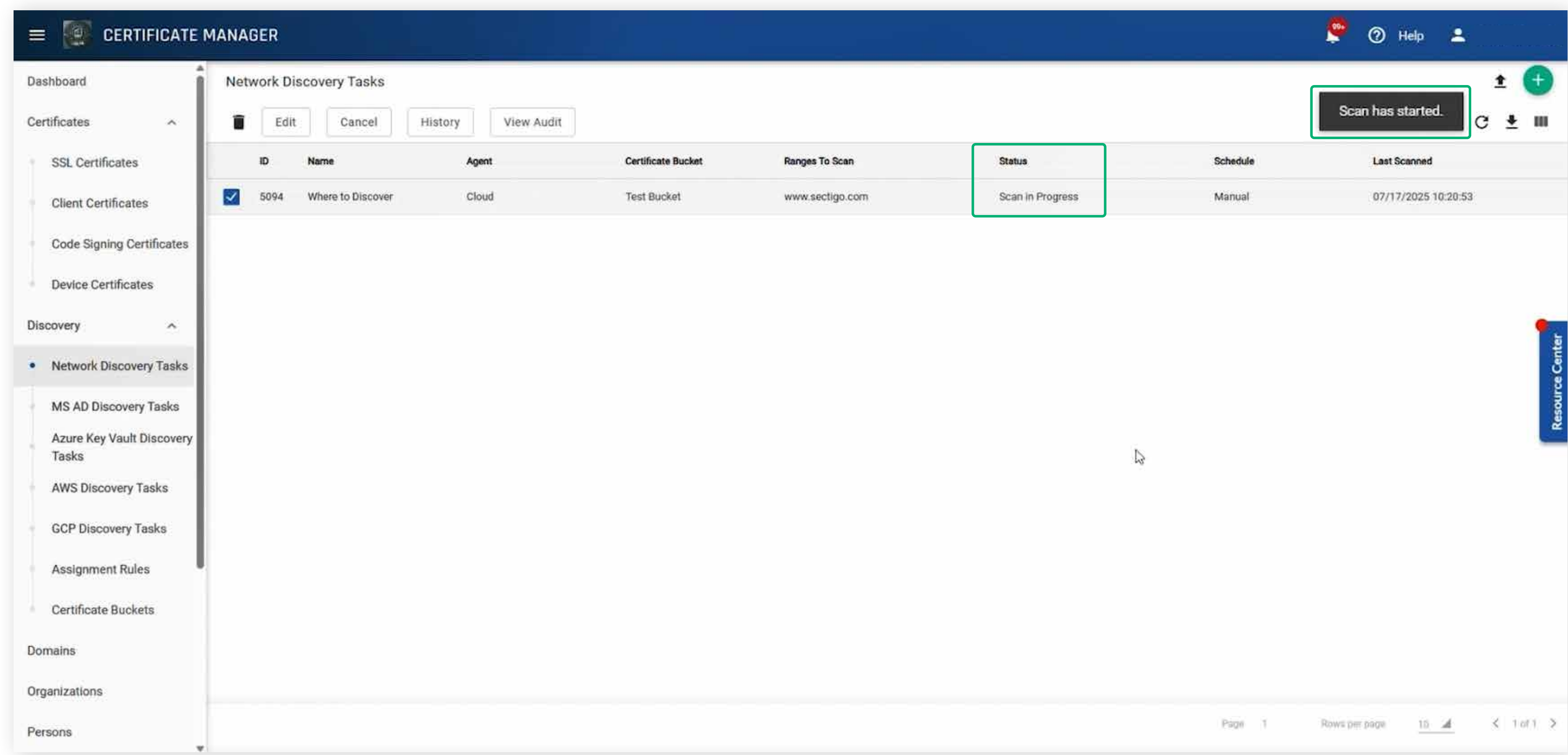
- 1. Select the scan you created.
- 2. Click [Scan](#).





You'll see a confirmation message that the scan has started.

While the scan is in progress, the status will show as [Scan in Progress](#).



Scan time can take anywhere from a few seconds to several hours, depending on the number of addresses and ports you are scanning.

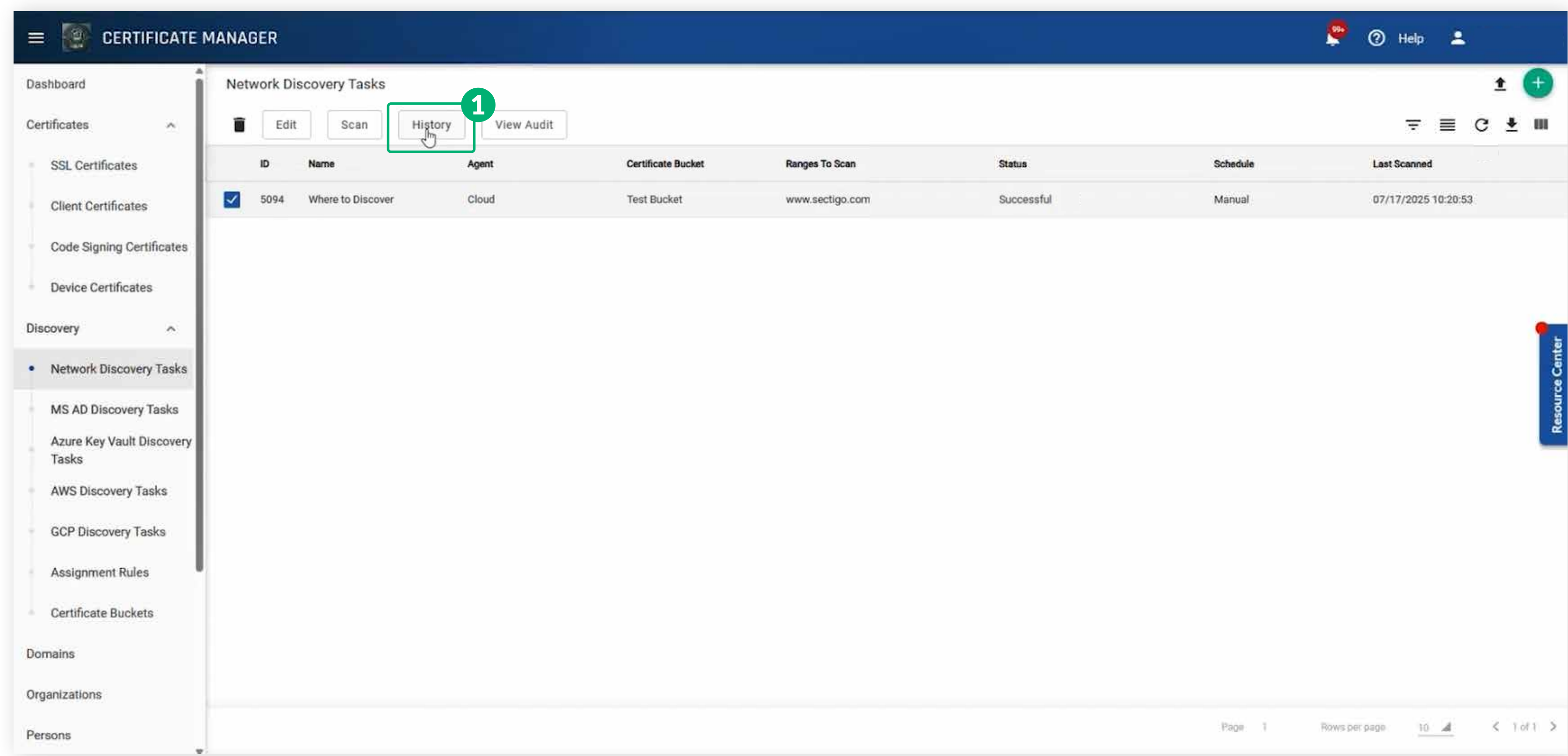




# Step 6 - View your scan results

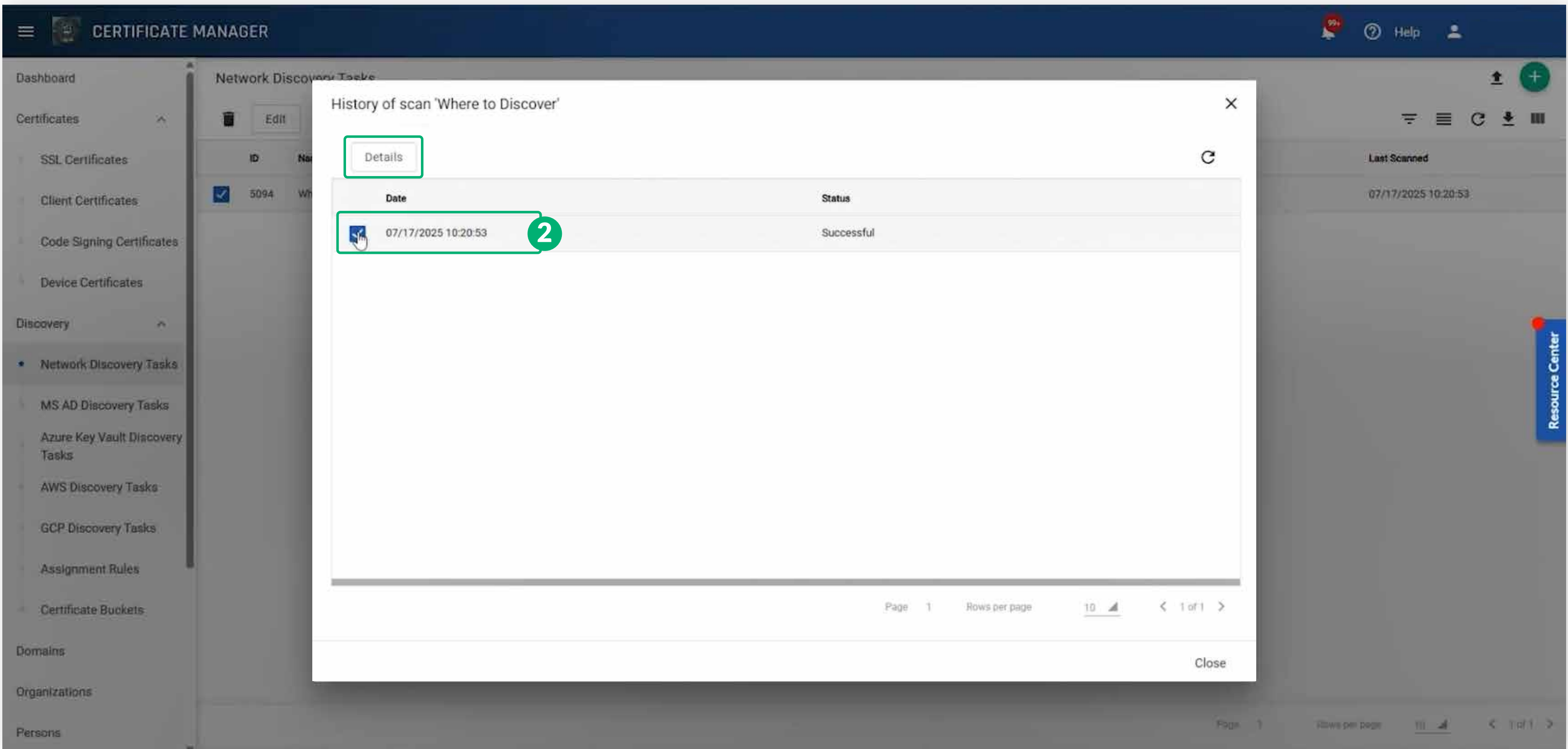
Within the same interface following step 5, to see your scan results:

- 1. Click the [History](#) button.



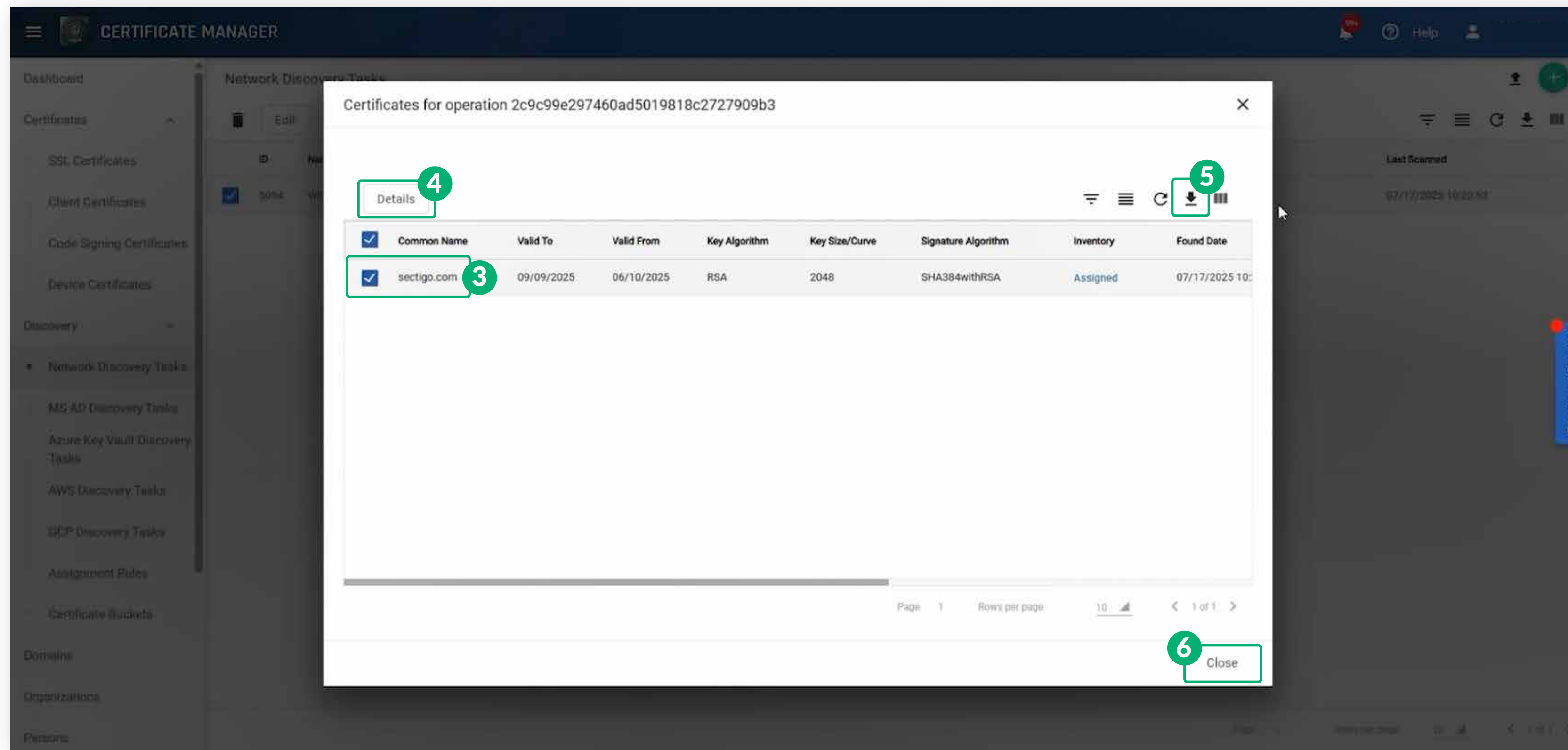


2. Select your scan from the list.





3. Select any certificate you want to inspect.
4. Click [Details](#) to view its metadata.
5. Or click the [Download icon](#) to export the full list as a CSV file.
6. When finished, click [Close](#).





# Step 7- View your discovered certificates in SCM

You can also find any newly discovered certificates under the **Certificates** tab:

- 1. Click **Certificates → SSL Certificates**.

Each certificate includes a status, such as **Issued**, **Imported**, or **External**, and may also indicate if it's **Expired** or **Revoked**.

For example, a certificate marked as **Issued** was created by SCM. A certificate with an **External** status indicates it was found through discovery and issued by a third-party CA.

CERTIFICATE MANAGER

99+

?

Help

Dashboard

Certificates

• SSL Certificates

Client Certificates

Code Signing Certificates

Device Certificates

Discovery

Network Discovery Tasks

MS AD Discovery Tasks

Azure Key Vault Discovery Tasks

AWS Discovery Tasks

GCP Discovery Tasks

Assignment Rules

Certificate Buckets

Domains

Organizations

Persons

SSL Certificates

Search by ID or Common Name or Subject Alt Name

ID

Status

Common Name

Certificate Profile

Requested Via

Organization

Department

Requester

Expires

Serial Number

62314

Issued

sectigo.com

Discovery

Lublab

09/09/2025

F2:9C:CC:FC:90:1E:D

60676

Issued

test.lublab.ca

Private SSL

ACME

Lublab

09/08/2025

62:E1:E7:DA:1B:98:1

60675

Issued

gci.example.com

Private SSL

ACME

Lublab

09/08/2025

27:6B:CF:8E:E9:ES:E

Page 1

Rows per page 10

1-3 of 3

Resource Center

Your guided setup for cloud discovery in Sectigo Certificate Manager (SCM)

www.sectigo.com | 19



2. To see more details, select any certificate and click [View](#).

CERTIFICATE MANAGER

99+

?

Help

Dashboard

Certificates

SSL Certificates

Client Certificates

Code Signing Certificates

Device Certificates

Discovery

Network Discovery Tasks

MS AD Discovery Tasks

Azure Key Vault Discovery Tasks

AWS Discovery Tasks

GCP Discovery Tasks

Assignment Rules

Certificate Buckets

Domains

Organizations

Persons

SSL Certificates

Search by ID or Common Name or Subject Alt Name

2

View

Renew

Mark Renewed

View Audit

ID

Status

Common Name

Certificate Profile

Requested Via

Organization

Department

Requester

Expires

Serial Number

☒

62314

Issued

sectigo.com

Discovery

Lublab

09/09/2025

F2:9C:CC:FC:90:1E

☐

60676

Issued

test.lublab.ca

Private SSL

ACME

Lublab

09/08/2025

62:E1:E7:DA:1B:98

☐

60675

Issued

gci.example.com

Private SSL

ACME

Lublab

09/08/2025

27:6B:CF:8E:E9:E5

Resource Center

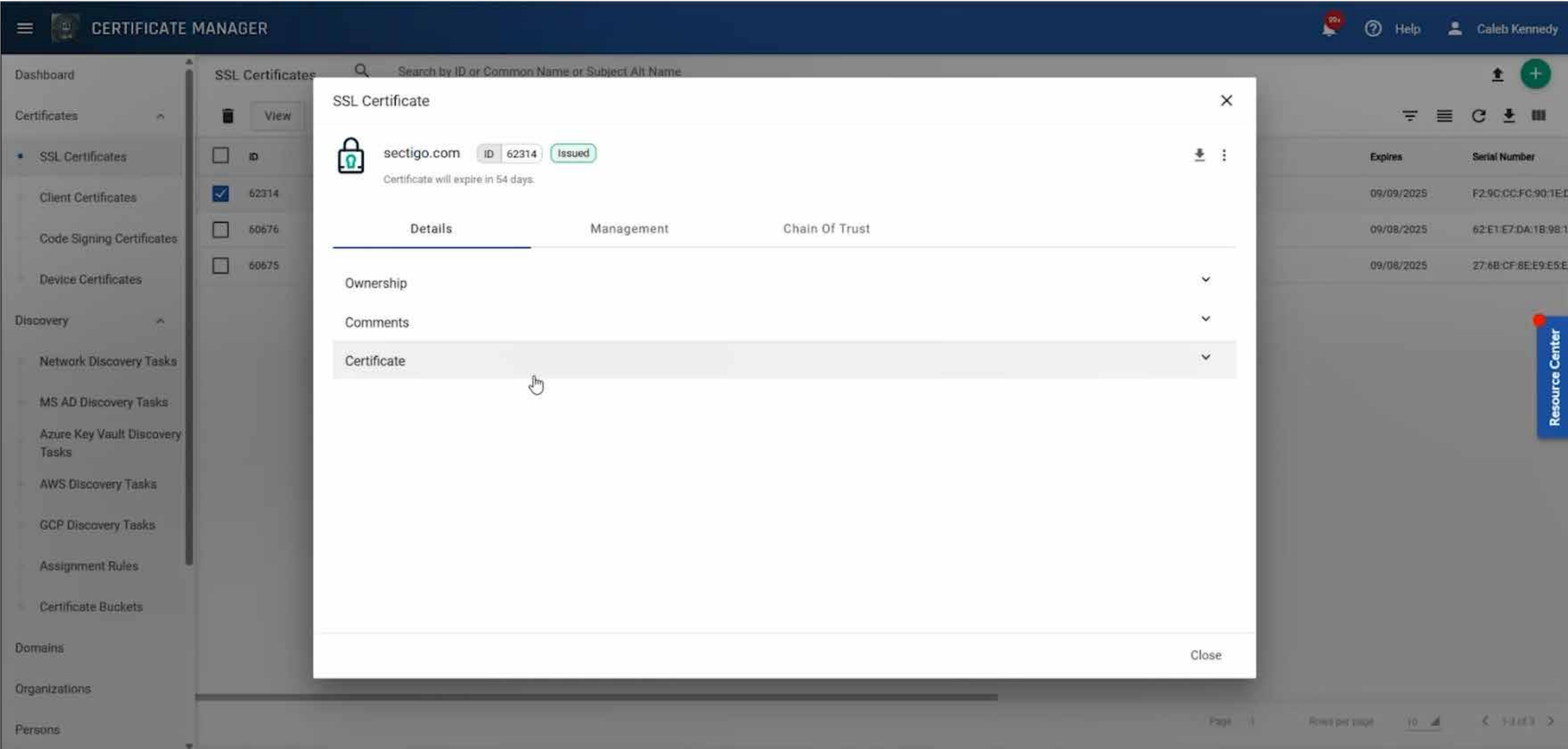
Page: 1

Rows per page: 10

1-3 of 3



You'll get a full overview, including its metadata and the complete certificate chain.



That's how you use discovery scans to pull certificates into SCM for simple, centralized management.