



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	1
Step 2 – Set up a certificate bucket	2
Step 3 – Add an assignment rule to the bucket	4
Step 4 – Configure a cloud-discovery scan	7
Step 5 – Run a manual scan	11
Step 6 – View your scan results	14
Step 7 – View your discovered certificates in SCM	17



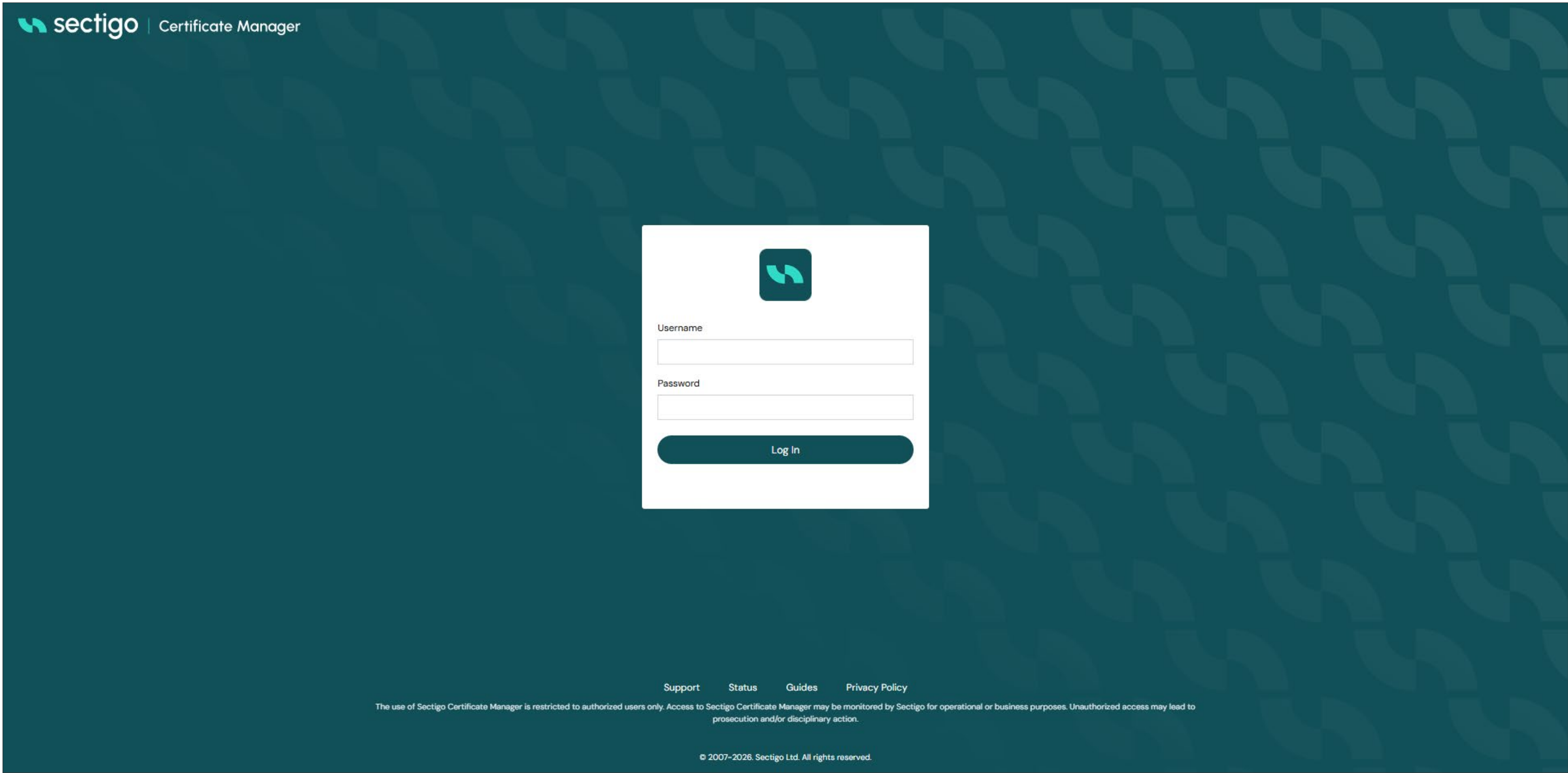


STEP 1

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.





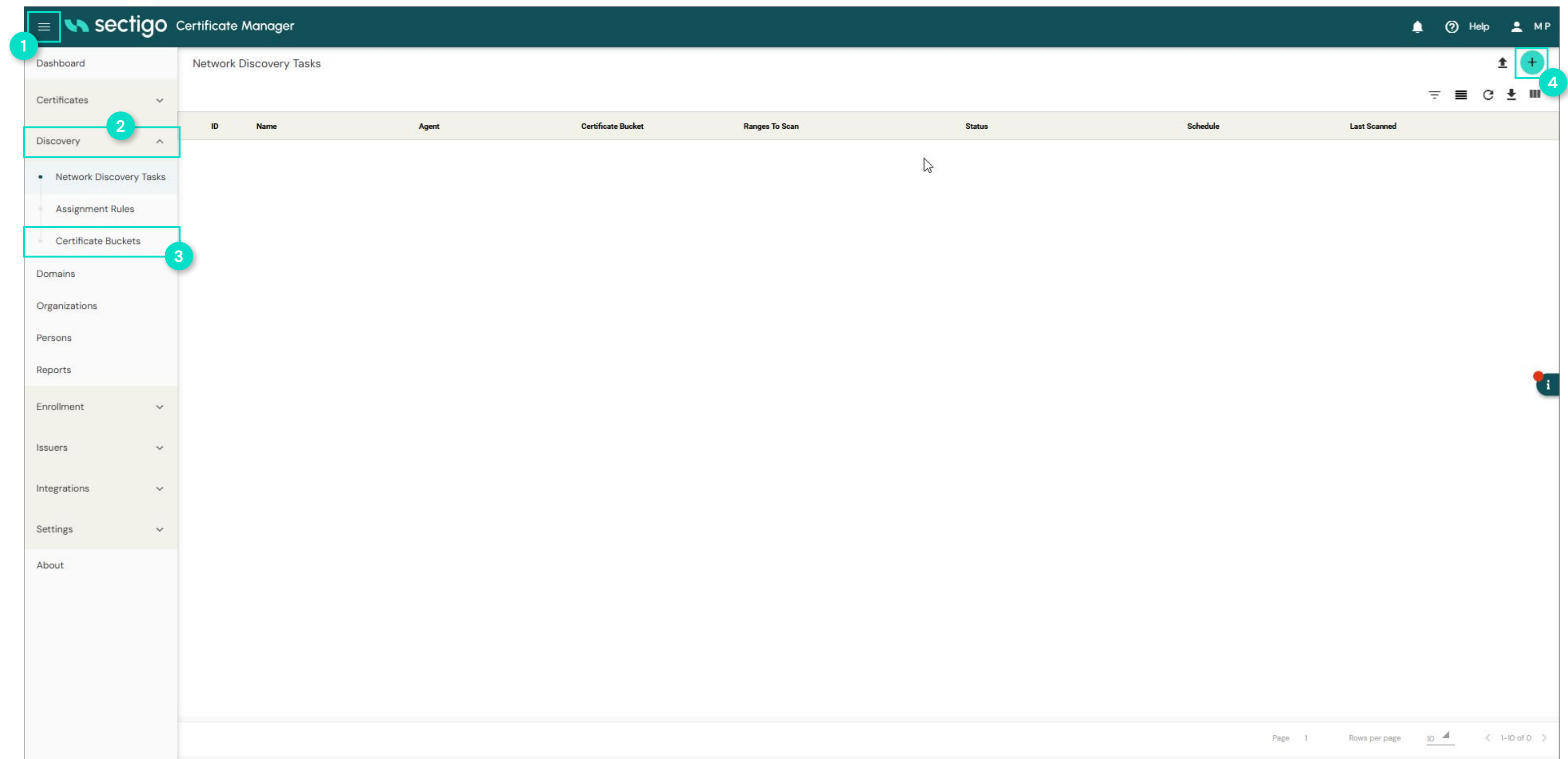
STEP 2

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.

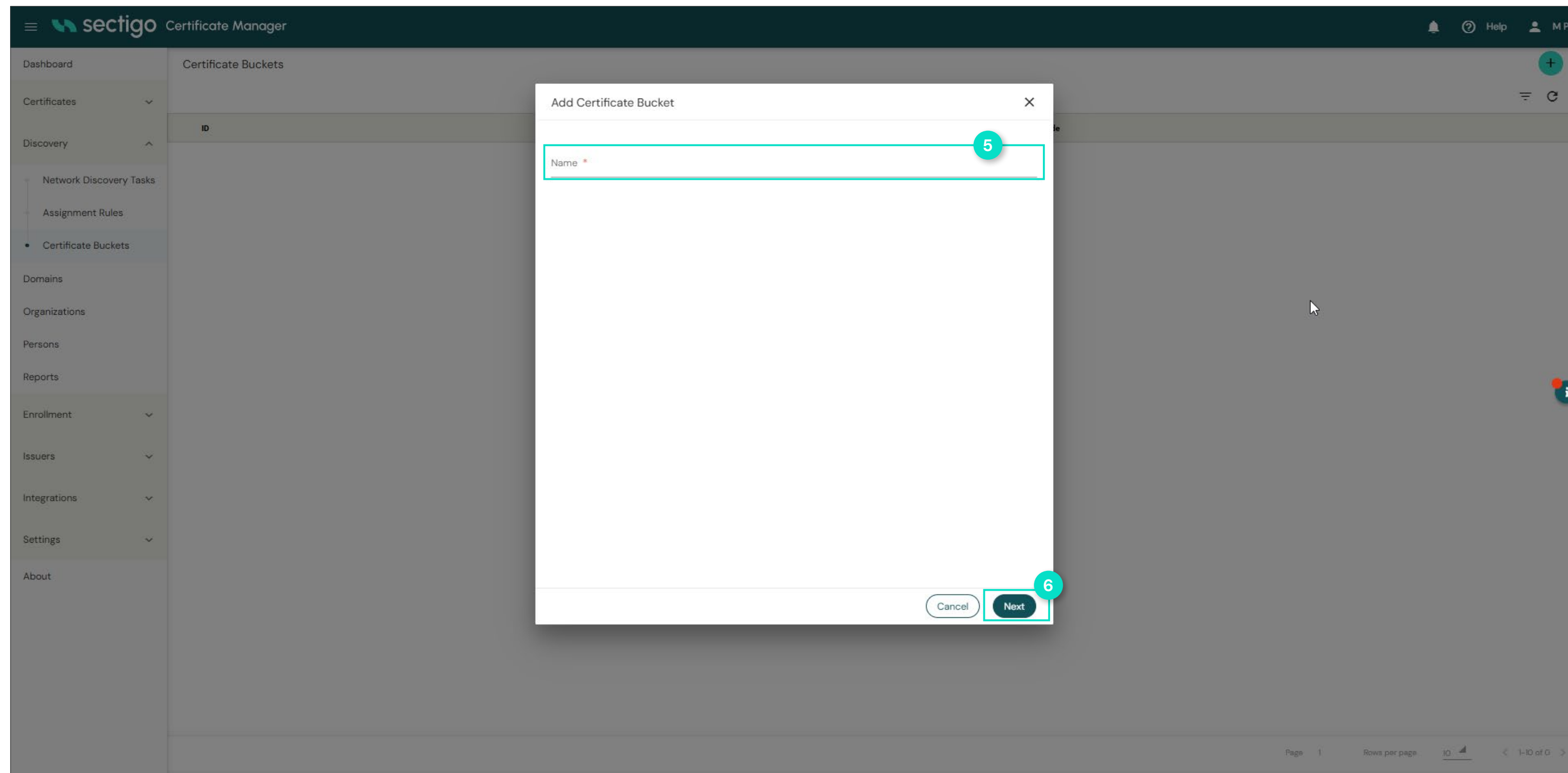
To create a bucket:

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

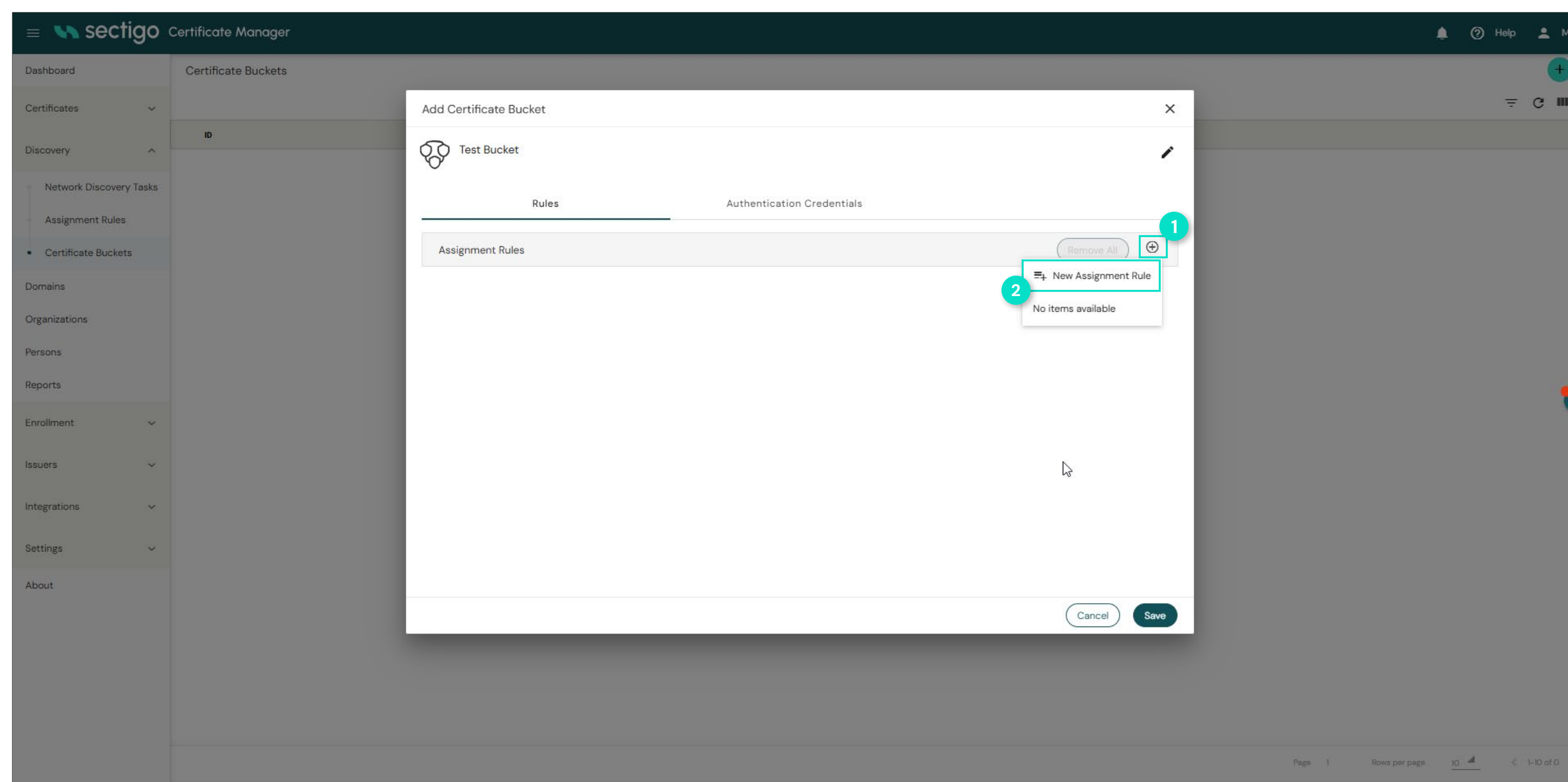
Next, it's time to define the assignment rule.

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.

The screenshot shows the 'Create New Assignment Rule' dialog in the Sectigo Certificate Manager. The dialog is titled 'Create New Assignment Rule' and has a close button (X) in the top right corner. It contains the following fields and sections:

- Name ***: A text input field, highlighted with a red circle and labeled '3'.
- If certificate discovered meets all conditions below**: A section header.
- Conditions**: A section with a 'Remove All' button and a plus icon (+).
- Assign to ...**: A section with three dropdown menus, highlighted with a red circle and labeled '4':
 - Organization**: A dropdown menu with 'Mohit's Test Company' selected.
 - Department**: A dropdown menu with 'None' selected.
 - Certificate Type ***: A dropdown menu with 'SSL Certificate' selected.
- Buttons**: 'Cancel' and 'Save' buttons at the bottom right.





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.

The screenshot shows the 'Create New Assignment Rule' dialog box in the Sectigo Certificate Manager interface. The dialog has a dark header with the Sectigo logo and 'Certificate Manager' text. The main content area is white and contains the following fields and controls:

- Name ***: A text input field.
- If certificate discovered meets all conditions below**: A heading for the conditions section.
- Conditions**: A section with a 'Remove All' button and an 'Add (+)' button (highlighted with a red circle and number 5). Below this is a table with one row: 'Port' matches '443'.
- Assign to ...**: A section with three dropdown menus: 'Organization' (selected: 'Mohit's Test Company'), 'Department' (selected: 'None'), and 'Certificate Type *' (selected: 'SSL Certificate').
- Buttons**: 'Cancel' and 'Save' buttons at the bottom right. The 'Save' button is highlighted with a red circle and number 6.

The background shows the 'Assignment Rules' page in the Certificate Manager, with a sidebar on the left containing links to Dashboard, Certificates, Discovery, Network Discovery Tasks, Assignment Rules, Certificate Buckets, Domains, Organizations, Persons, Reports, Enrollment, Issuers, Integrations, Settings, and About.



**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.

The screenshot shows the Sectigo Certificate Manager interface. The left sidebar contains a menu with items: Dashboard, Certificates, Discovery, Network Discovery Tasks (highlighted with a red circle and a '1' callout), Assignment Rules, Certificate Buckets, Domains, Organizations, Persons, Reports, Enrollment, Issuers, Integrations, Settings, and About. The main content area is titled 'Network Discovery Tasks' and displays a table with the following columns: ID, Name, Agent, Certificate Bucket, Ranges To Scan, Status, Schedule, and Last Scanned. In the top right corner of the table, there is a '+ Add' button (highlighted with a red circle and a '2' callout) and a 'Filter' icon. The bottom of the interface shows a footer with 'Page 1', 'Rows per page 10', and '1-10 of 0'.





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**.

The screenshot shows the 'Add Network Discovery Task' dialog in the Sectigo Certificate Manager. The dialog is divided into two tabs: 'General' and 'Schedule'. The 'General' tab is selected. It contains three input fields: 'Name' (with a red asterisk), 'Agent' (with 'Cloud' selected), and 'Certificate Bucket' (with 'Select...' selected). Below these is a 'Ranges to Scan' section with a table and an 'Add' button (a square with a plus sign). The 'Add' button is highlighted with a red circle and the number 6. The other three input fields are also highlighted with red circles and numbers 3, 4, and 5 respectively. The background shows the 'Network Discovery Tasks' table with columns 'ID' and 'Name'. The bottom of the dialog has 'Cancel' and 'Save' buttons.





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**.

The screenshot shows the Sectigo Certificate Manager interface. The left sidebar contains navigation links: Dashboard, Certificates, Discovery, Network Discovery Tasks, Assignment Rules, Certificate Buckets, Domains, Organizations, Persons, Reports, Enrollment, Issuers, Integrations, Settings, and About. The main content area is titled 'Network Discovery Tasks' and shows a table with columns 'ID' and 'Name'. A modal dialog 'Add Network Discovery Task' is open, with a 'General' tab. It includes fields for 'Name', 'Where to Discover', 'Agent' (set to 'Cloud'), 'Certificate Bucket', and 'Test Bucket'. Below these is a 'Ranges to Scan' section. A sub-dialog 'Add Scan Range' is also open, showing three radio button options: 'CIDR', 'IP or IP range', and 'Host name'. The 'Host name' option is selected. Below the radio buttons are two input fields: one for the host name (e.g., 'host1.domain.com') and one for ports (e.g., '443, 8443-9000'). The 'Save' button in the 'Add Scan Range' dialog is highlighted with a red circle and the number 7.





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.

The screenshot shows the 'Add Network Discovery Task' dialog in the Sectigo Certificate Manager. The 'General' tab is selected, and the 'Schedule' tab is also visible. The 'Where to Discover' field is empty. The 'Agent' is set to 'Cloud'. The 'Certificate Bucket' is set to 'Test Bucket'. The 'Ranges to Scan' table has one entry: 'www.sectigo.com : 443'. A plus icon (+) is in the bottom right of the table. At the bottom of the dialog are 'Cancel' and 'Save' buttons. Red callout boxes with numbers 8, 9, and 10 highlight the plus icon, the 'Schedule' tab, and the 'Save' button respectively.





STEP 5

Run a manual scan

To run the scan manually:

- 1. Select the scan you created.
- 2. Click **Scan**.

Dashboard

Certificates

Discovery

Network Discovery Tasks

Assignment Rules

Certificate Buckets

Domains

Organizations

Persons

Reports

Enrollment

Issuers

Integrations

Settings

About

sectigo Certificate Manager

Network Discovery Tasks

Edit

Scan

History

View Audit

ID	Name	Agent	Certificate Bucket	Ranges To Scan	Status	Schedule	Last Scanned
☒	5327	Where to Discover	Cloud	Test Bucket	www.sectigo.com	Manual	

Page 1 Rows per page 10 1 of 1





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.

Dashboard

Certificates

Discovery

Network Discovery Tasks

Assignment Rules

Certificate Buckets

Domains

Organizations

Persons

Reports

Enrollment

Issuers

Integrations

Settings

About

sectigoCertificate Manager

Network Discovery Tasks

Edit

Cancel

History

View Audit

ID	Name	Agent	Certificate Bucket	Ranges To Scan	Status	Schedule	Last Scanned
5327	Where to Discover	Cloud	Test Bucket	www.sectigo.com	Scan in Progress	Manual	07/02/2026 12:08:22

Page 1 Rows per page 10 1 of 1

Scan has started.

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





3. Click the **Refresh icon** to update the status. Once the scan is complete, the status will change to **Successful**.

Dashboard

Certificates

Discovery

Network Discovery Tasks

Assignment Rules

Certificate Buckets

Domains

Organizations

Persons

Reports

Enrollment

Issuers

Integrations

Settings

About

sectigo

Certificate Manager

Network Discovery Tasks

Edit

Scan

History

View Audit

ID	Name	Agent	Certificate Bucket	Ranges To Scan	Status	Schedule	Last Scanned
5327	Where to Discover	Cloud	Test Bucket	www.sectigo.com	Successful	Manual	07/02/2026 12:08:47

Page 1 Rows per page 10 1 of 1



**STEP 6**

View your scan results

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

1. Click the **History** button.

The screenshot shows the Sectigo Certificate Manager interface. The left sidebar contains a navigation menu with items: Dashboard, Certificates, Discovery, Network Discovery Tasks, Assignment Rules, Certificate Buckets, Domains, Organizations, Persons, Reports, Enrollment, Issuers, Integrations, Settings, and About. The main content area is titled 'Network Discovery Tasks' and features a table with columns: ID, Name, Agent, Certificate Bucket, Ranges To Scan, Status, Schedule, and Last Scanned. A single row is visible with ID 5327, Name 'Where to Discover', Agent 'Cloud', Certificate Bucket 'Test Bucket', Ranges To Scan 'www.sectigo.com', Status 'Successful', Schedule 'Manual', and Last Scanned '07/02/2026 12:08:47'. Above the table are buttons for 'Edit', 'Scan', 'History' (highlighted with a red circle and the number 1), and 'View Audit'. The top header bar includes the Sectigo logo, 'Certificate Manager', and user information 'M P'.

ID	Name	Agent	Certificate Bucket	Ranges To Scan	Status	Schedule	Last Scanned
5327	Where to Discover	Cloud	Test Bucket	www.sectigo.com	Successful	Manual	07/02/2026 12:08:47





2. Select your scan from the list.

The screenshot shows the Sectigo Certificate Manager interface. A modal window titled 'History of scan 'Where to Discover'' is open, displaying a table of scan history. The table has two columns: 'Date' and 'Status'. There are two rows of scan data. The first row is dated '07/02/2026 12:08:47' with a status of 'Successful'. The second row is dated '07/02/2026 12:08:22' with a status of 'Successful'. A red circle with the number '2' highlights the second row. A red box highlights the 'Details' button in the top left corner of the modal. The background interface shows a sidebar with navigation options like 'Dashboard', 'Certificates', 'Discovery', 'Network Discovery Tasks', 'Assignment Rules', 'Certificate Buckets', 'Domains', 'Organizations', 'Persons', 'Reports', 'Enrollment', 'Issuers', 'Integrations', 'Settings', and 'About'. The main content area shows 'Network Discovery Tasks' with a table of tasks, including one with ID '5327' and name 'Where to Discover'.

Date	Status
07/02/2026 12:08:47	Successful
07/02/2026 12:08:22	Successful





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**.

The screenshot displays the Sectigo Certificate Manager interface. A modal window titled "Certificates for operation 2c9c92929ef06c6f019f2396a19b0058" is open, showing a table of certificates. The table has columns: Common Name, Valid To, Valid From, Key Algorithm, Key Size/Curve, Signature Algorithm, Inventory, Found Date, IP Address, and Port. One certificate is listed with the Common Name "sectigo.com". The modal includes buttons for "Details" (circled with a red 4) and "Hide" (circled with a red 3). A "Download" icon (circled with a red 5) is also present. At the bottom right of the modal, there is a "Close" button (circled with a red 6). The background interface shows a sidebar with navigation options like Dashboard, Certificates, Discovery, and Reports, and a main area with "Network Discovery Tasks".

Common Name	Valid To	Valid From	Key Algorithm	Key Size/Curve	Signature Algorithm	Inventory	Found Date	IP Address	Port
sectigo.com	09/04/2026	06/05/2026	RSA	2048	SHA256withRSA		07/02/2026 12:12	104.18.228.224	443





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.

Dashboard

Certificates

SSL Certificates

Client Certificates

Code Signing Certificates

Device Certificates

Mark Certificates

Discovery

Network Discovery Tasks

Assignment Rules

Certificate Buckets

Domains

Organizations

Persons

Reports

Enrollment

Issuers

Integrations

Settings

About

sectigo Certificate Manager

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	Renewed
90591	Issued	sectigo.com		Imported	Mohit's Test Company		M P	09/04/2026	74:AB:77:3A:91:AA:98:06:D2:81:BB:43:F6:AF:9B:30	
72500	Applied	mohitspandey.com	Sectigo Enterprise ...	Admin	Mohit's Test Company		M P			
72499	Expired	mohitpandey.work	Sectigo Enterprise ...	Admin	Mohit's Test Company		M P	05/25/2026	1F:71:73:CB:08:8D:76:CA:4E:EF:BA:D2:4A:ED:89:B3	
72498	Expired	mohitpandey.work	Sectigo Enterprise ...	Admin	Mohit's Test Company		M P	05/25/2026	65:AF:69:7D:EC:9E:81:12:27:B1:57:96:3E:76:B2:81	

Page 1 Rows per page 10 1-4 of 4





2. To see more details, select any certificate and click **View**.

Dashboard

Certificates

SSL Certificates

Client Certificates

Code Signing Certificates

Device Certificates

Mark Certificates

Discovery

Network Discovery Tasks

Assignment Rules

Certificate Buckets

Domains

Organizations

Persons

Reports

Enrollment

Issuers

sectigo Certificate Manager

SSL Certificates

Search by ID or Common Name or Subject Alt Name

2 View Renew Mark Renewed View Audit

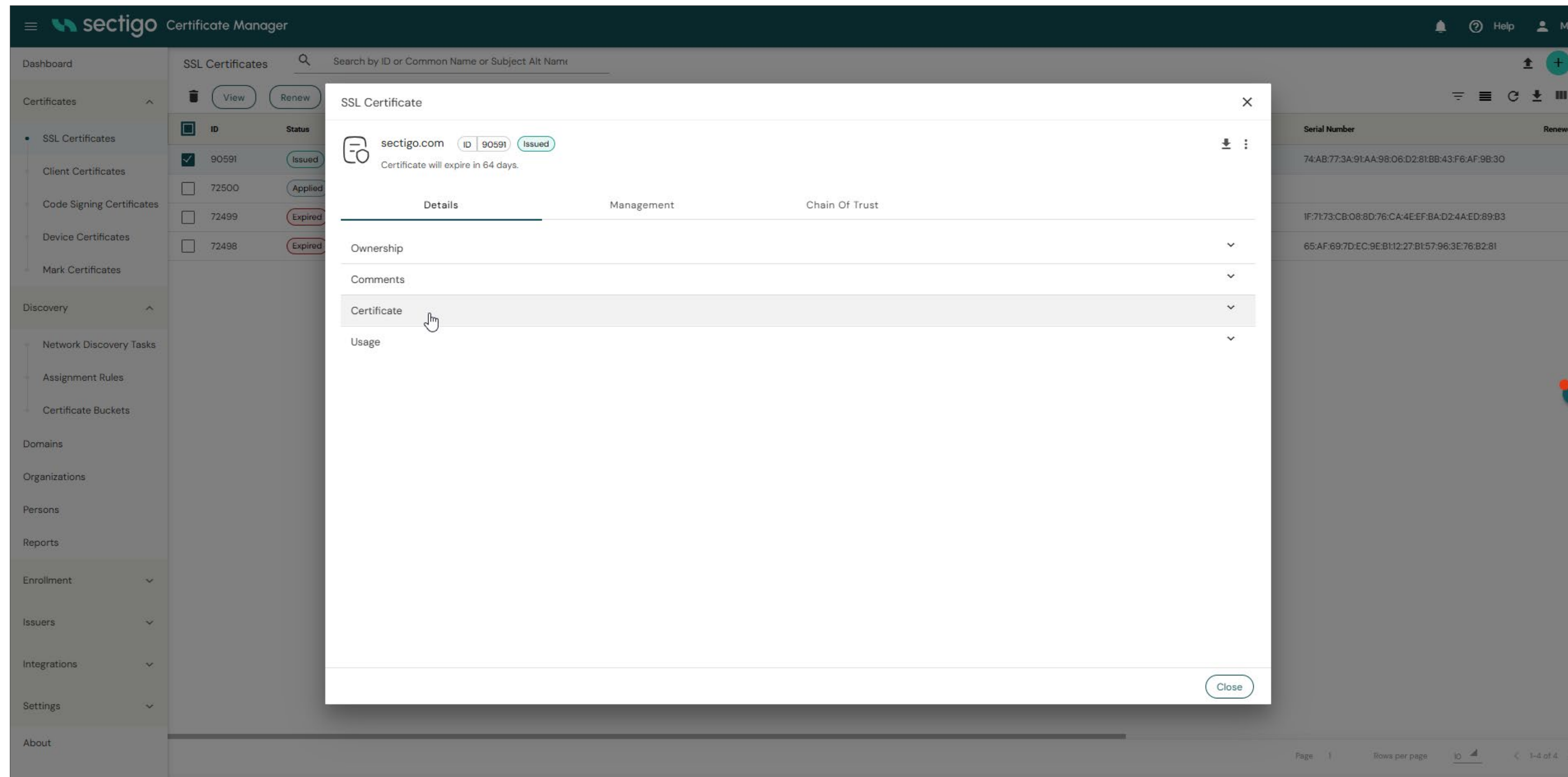
ID	Status	Common Name	Certificate Profile	Requested Via	Organization	Department	Requester	Expires	Serial Number
90770	Issued	sectigo.com		Imported	Mohit's Test Company		Mohit P	01/24/2027	1A:9C:3A:9D:58:98
90769	Issued	sectigo.com		Discovery	Mohit's Test Company			09/04/2026	74:AB:77:3A:91:AA:3
72500	Applied	mohitspandey.com	Sectigo Enterpris...	Admin	Mohit's Test Company		M P		
72499	Expired	mohitpandey.work	Sectigo Enterpris...	Admin	Mohit's Test Company		M P	05/25/2026	1F:71:73:CB:08:8D:7
72498	Expired	mohitpandey.work	Sectigo Enterpris...	Admin	Mohit's Test Company		M P	05/25/2026	65:AF:69:7D:EC:9E

Page 1 Rows per page 10 1-5 of 5





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.

