Qualys Certificate View

User Guide

October 09, 2023

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

Table of Contents

About this Guide

Welcome to Qualys Certificate View! Certificate View provides discovery, assessment, and management of all your SSL/TLS certificates across your enterprise and cloud hosted assets. Get instant visibility on all your certificates in one place!

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.

Get Started with Certificate View

Qualys Certificate View gives you a comprehensive view of all the SSL/TLS certificates across your enterprise and cloud hosted assets.

Just add assets, set up your issuing certificate authorities, and that's it! Start discovering certificates that are present on your cloud assets.

Add Assets

Start monitoring assets on your hosts by adding external (public) and internal sites to Certificate View.

If you have a Certificate View Free subscription then you can add only external sites. To add and monitor internal sites simply upgrade to Certificate View Full subscription.

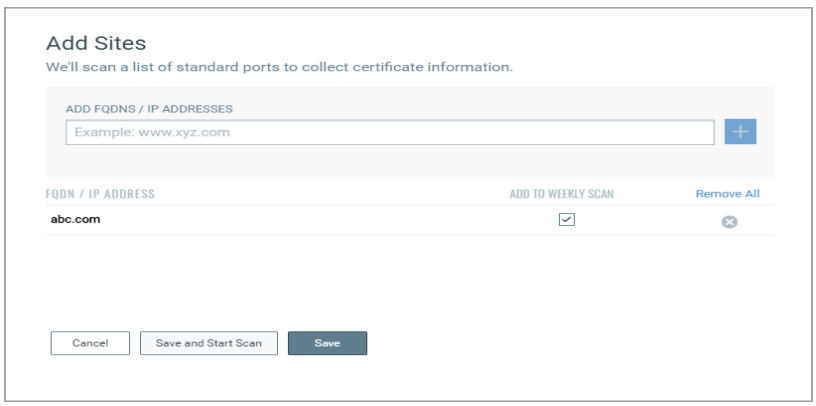
Add External Sites

Go to **Assets** > **External Sites** and click **Add Sites**.

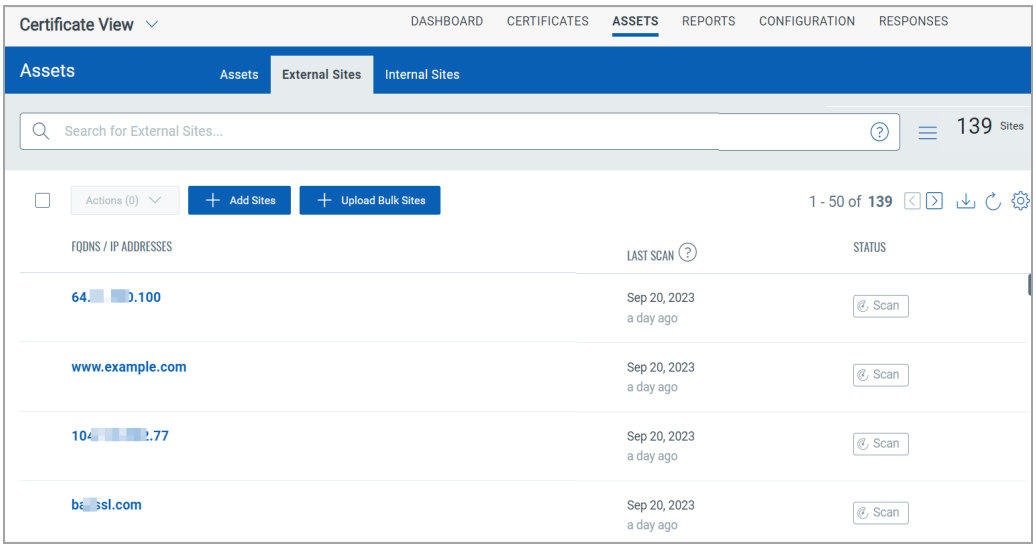
Provide either FQDNs or IP Addresses of public sites that you want to scan for certificates. Certificate View scan a list of standard ports to collect certificate information on the sites provided by you.

Select the **ADD TO WEEKLY SCAN** to either include or exclude the site from the weekly scheduled scan.

Click **Save** to scan the sites at a later time or click **Save** and Start Scan to immediately scan the site.



Once the site is added, it is listed in the External Sites tab. Here you can view details about the sites like when it was last scanned, the status of the scan (Finished, Canceled, Waiting, Queued, Running, or Error). The external sites on the External Sites tab display based on the last scan date. You can also sort the information as per the last scan date.



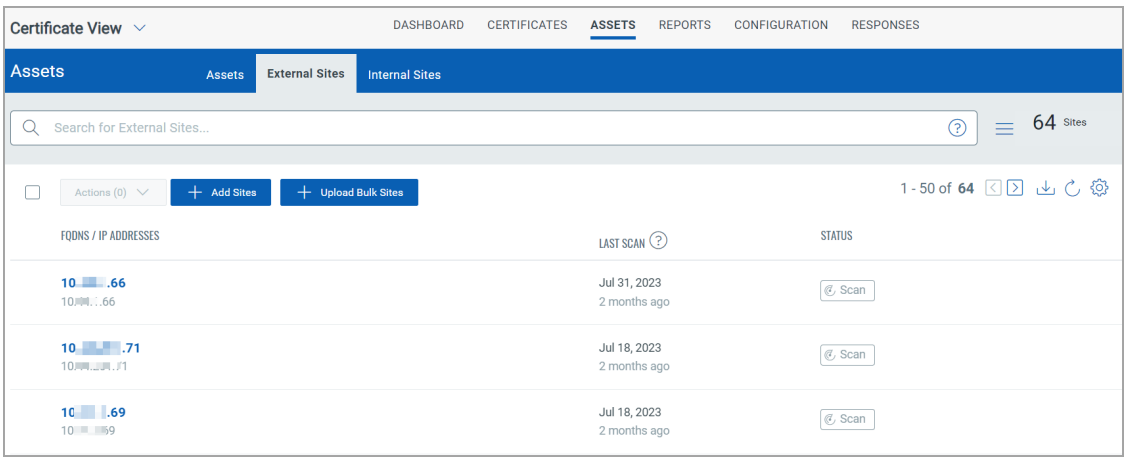
Upload Bulk Sites

You can add external sites with the Upload Bulk Sites functionality. Bulk uploading of external sites is possible with the use of a CSV file.

Note: You can add up to 1000 external site in one CSV file. External sites cannot be added in Certificate View using IPv6 addresses and FQDNs.

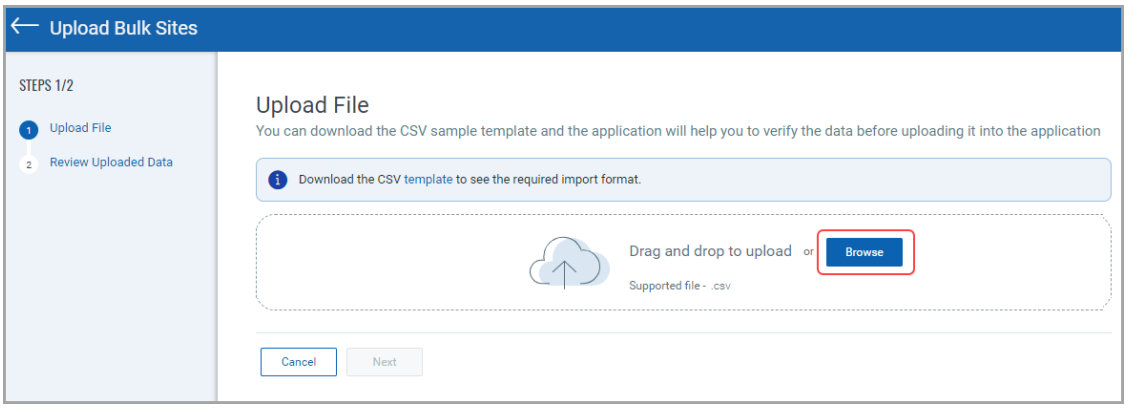
Follow these steps to add external sites. .

1. Go to **Assets** > **External Sites** and click **Upload Bulk Sites**.



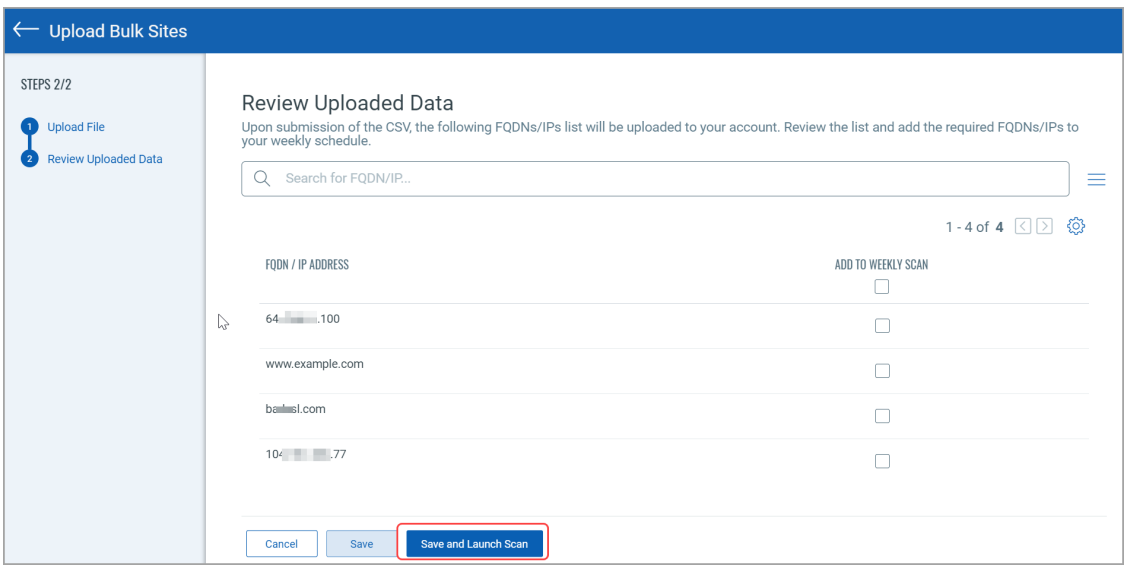
2. Browse your CSV file from your local machine and click Next.

You can download the sample CSV template and use it to add up to 1000 of your preferred sites.

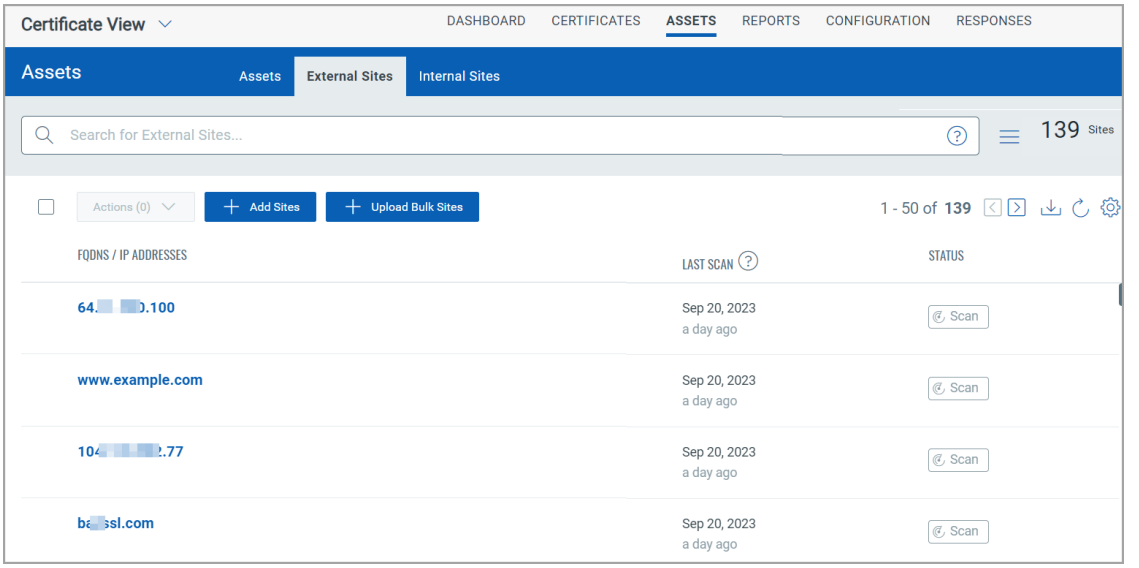


3. Review your uploaded data, click Save or Save and Launch Scan.

Manager users can add these sites to weekly scans as per the requirement.



Your added sites are displayed in External Sites tab.



Add Internal Sites

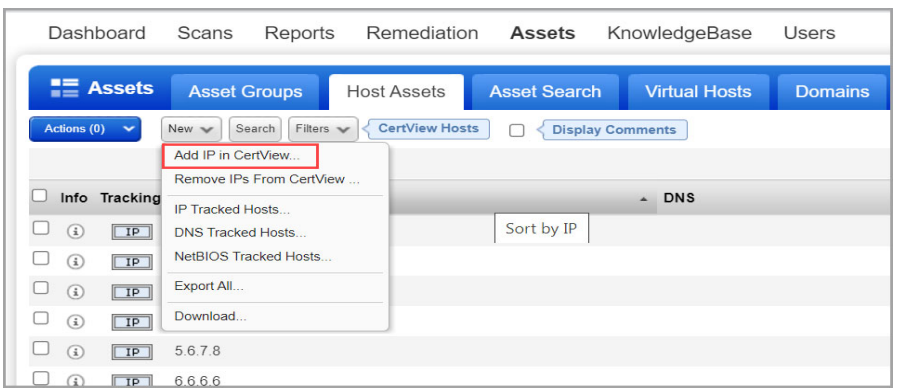
You can monitor FQDNs and IP addresses of internal sites if you have the Certificate View Full subscription.

Following is the list of private IP addresses you can use while adding internal sites.

- 172.16.0.0...172.31.255.255
- 192.168.0.0...192.168.255.255
- 10.0.0.0...10.255.255.255
- 240.0.0.0...255.255.255.255

To add Assets from VM/VMDR, go to **VM/VMDR** > **Assets** > **Host Assets.**

From the **New** menu, select **Add IP in CertView.** .



Review the number of hosts you can add, enter the new IPs/ranges, and click Add. You can see the IPs currently added to CertView by selecting **Filters** > **CertView Hosts**.

Run Scans to Discover Certificates

Scan your assets to discover certificates that are installed on the host assets in your environment. Certificates can be discovered using VM/VMDR . Qualys Cloud Agent is used to scan certificates on the registry or certificate manager console.

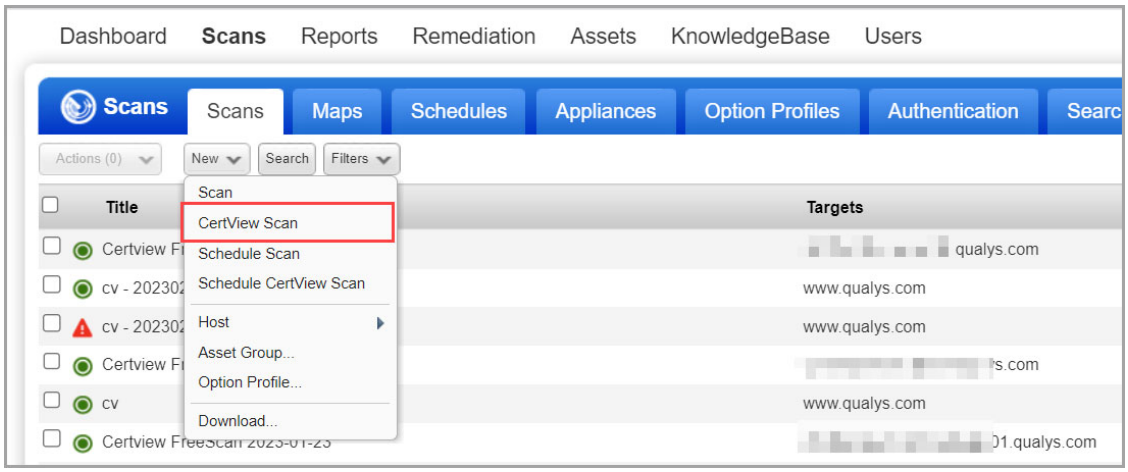
To initiate a scan, go to **Assets** > **External Sites** and click **Scan** corresponding to the desired FQDN or IP Address.

Scan is run for all saved sites periodically and fetch data. In the Last Scan column you can view when the site was last scanned.

To run scans from VM/VMDR

You can run scans or schedule scans from VM/VMDR only if you have a trial or a full subscription of Certificate View.

Go to **VM/VMDR** > **Scans** > **Scans** > **New** > **CertView Scan** and choose your scan settings.



We recommend the SSL Certificates profile to get started. You can easily configure a profile with the various scan options, i.e. what ports to scan, whether to use authentication, and more.

Cloud Agent Configuration to Discover Certificates

Using Qualys Cloud Agent, you can retrieve the leaf certificate present on your target machine in the registry or certificate manager console. Qualys Cloud Agent scans the certificates, and you get the certificate details. For more details on installing the cloud agent, refer to Cloud Agent for Windows guide.

Pre-requisite

- Contact your Technical Account Manager or Qualys Support to activate this feature.

- Install Windows Agent.

Note:

- Currently, Certificate View supports Windows Agent only.

- Certificate View displays certificates that are installed on the Windows machine only.

Following are the steps to run scans from Cloud Agent:

1. Download the Agent installer

2. Install the Agent

3. View the certificates in Certificates Tab

Follow these steps for detailed procedure:

Download the Agent installer

1. Log into the Qualys Cloud Platform and select CA for the Cloud Agent module.

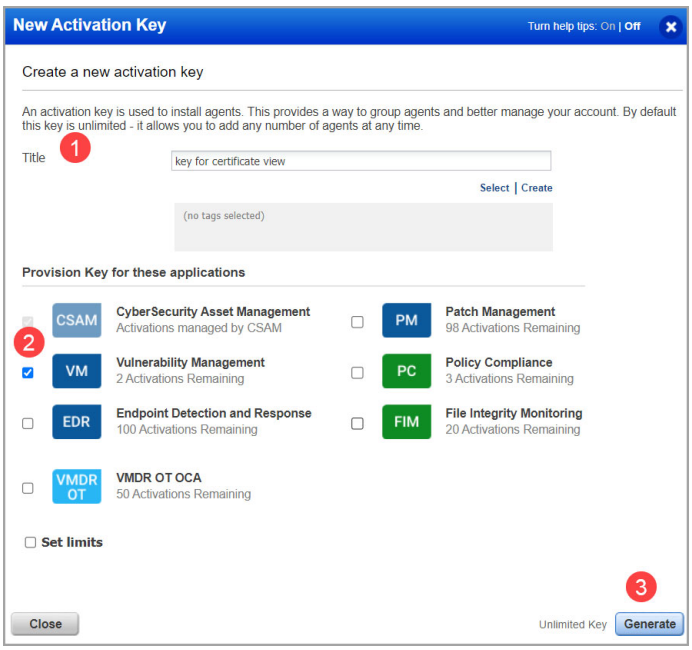
2. Choose an activation key (create one if needed) and select Install Agent from the Quick Actions menu.

To create an activation key.

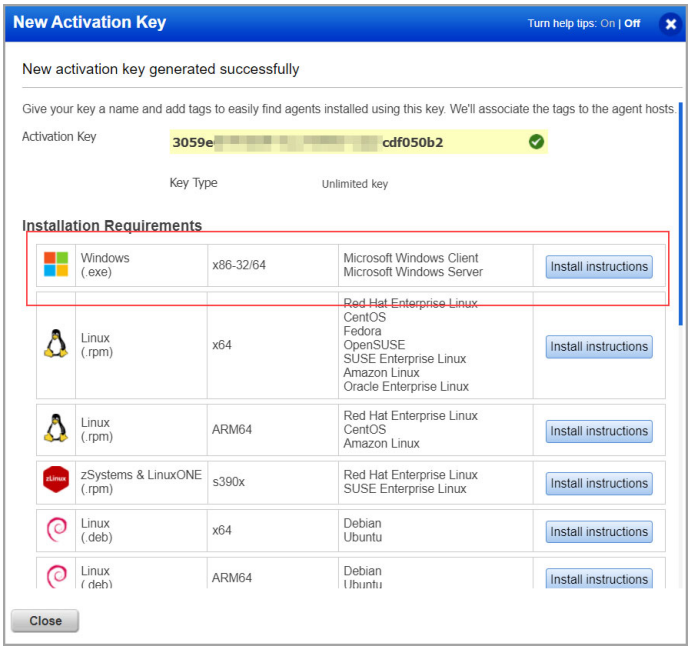
Go to **Cloud Agent** > **Agent Management** > **New Key.**

You can also generate New Key from the Activation Keys tab.

Provide a **Title**, select the Vulnerability Management module from **Provision Key for these applications** section, and click **Generate**.



3. Click **Install instructions** next to Windows (.exe).



The Agent installer is downloaded to your local system, and in the UI, you can see the associated Activation key ID and Customer ID.

4. Copy and paste this to a safe place; you need it to complete the installation manually or through software distribution tools.

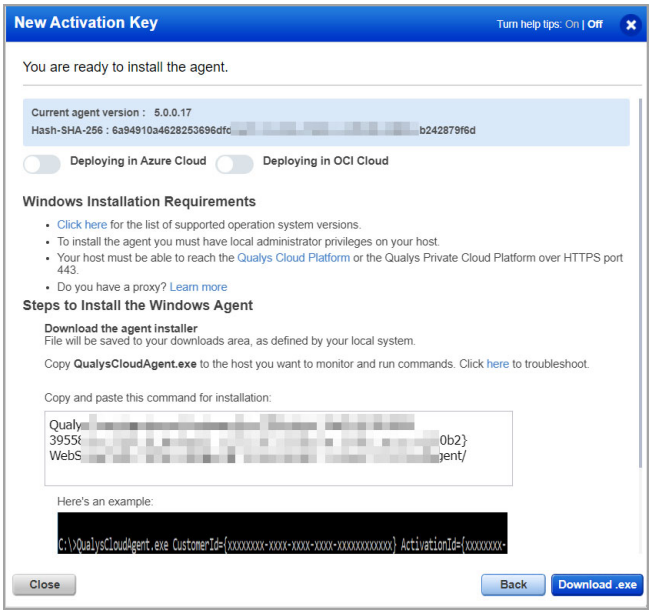
For more details on activation keys, refer to Manage Activation Keys.

Install the Agent

1. Copy the Qualys Cloud Agent installer onto the host where you want to install the agent.

2. Run the command or use a systems management tool to install the agent as per your organization's standard process to install the software.

```
> QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx}
ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}
WebServiceUri=<platform_url>/CloudAgent/2.
```



Once installed, an agent connects to the Qualys Cloud Platform and provisions itself.

The agent is now listed in the Agents tab.

By default, the agent runs the scan every 4 hours, and you can view the scans performed in the Certificates tab of Certificate View.

Note: You can create a customized Configuration Profile and assign the profile to your Cloud Agent. For more details on assigning configuration profiles, refer to Cloud Agent Online help.

View the certificates in Certificates Tab

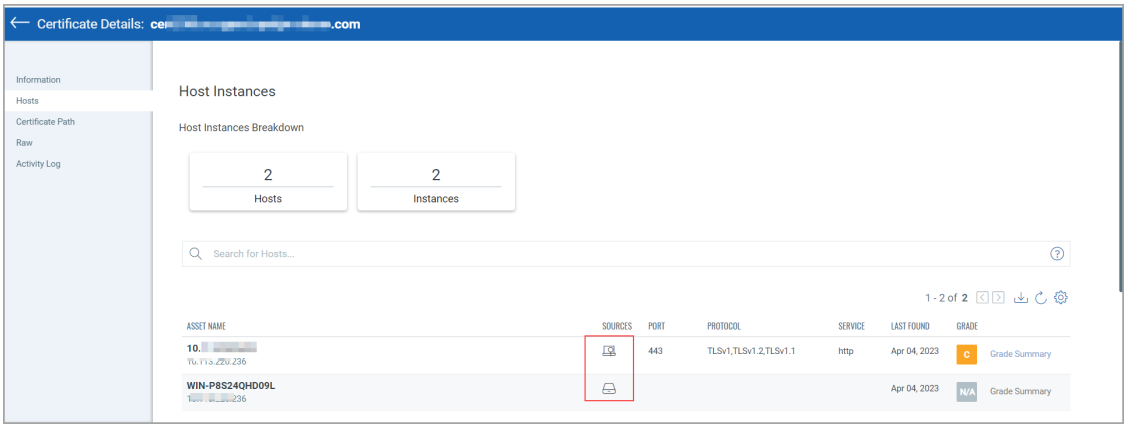
You can use a search query to find the certificates that are scanned through VM (Vulnerability Management) or Qualys Cloud Agent.

For example, `instance:(sources: QAGENT)`

To view the certificate details, go to **View Details** from the Quick Actions menu. Go to the **Hosts** tab.

You can view the details of assets with sources as VM or Qualys Agent. The certificate scanned through VM has  icon. The certificate scanned through Qualys Agent has  icon.

Cloud Agent scans do not support remote discovery, and hence the discovery of ports, protocols, services, grade, and grade summary are shown empty for certificates scanned through Qualys Agent.



QID is the unique Qualys ID number assigned to the vulnerability. A set of SSL certificate QIDs is always used for CertView scans. To get a complete list of the QIDs refer to Vulnerability Tests (QIDs) for CertView Scans.

Tip - To know more about running and scheduling CertView scans from VM/VMDR, go to **VM/VMDR** > **Scans** > **Scans** and look up CertView scans in online help.

Vulnerability Tests (QIDs) for CertView Scans

CertView scans always use these QIDs.

QID	Vulnerability Title	Severity
38116	SSL Server Information Retrieval	Informational
38139	SSL Server Has SSLv2 Enabled Vulnerability	Vulnerability - level 3
38142	SSL Server Allows Anonymous Authentication Vulnerability	Vulnerability - level 4
38167	SSL Certificate - Expired	Vulnerability - level 2
38168	SSL Certificate - Future Start Date	Vulnerability - level 2
38169	SSL Certificate - Self-Signed Certificate	Vulnerability - level 2
38170	SSL Certificate - Subject Common Name Does Not Match Server FQDN	Vulnerability - level 2
38171	SSL Certificate - Server Public Key Too Small	Vulnerability - level 2
38172	SSL Certificate - Improper Usage Vulnerability	Vulnerability - level 2
38173	SSL Certificate - Signature Verification Failed Vulnerability	Vulnerability - level 2
38174	SSL Certificate - Will Expire Soon	Vulnerability - level 1
38182	Webmin Static SSL Key Vulnerability	Vulnerability - level 5
38224	OpenSSL ASN.1 Parsing Vulnerabilities	Vulnerability - level 5
38356	OpenSSL RSA Timing Attack Vulnerability	Vulnerability - level 4
38477	SSL Insecure Protocol Negotiation Weakness	Vulnerability - level 2
38596	TLS Protocol Session Renegotiation Security Vulnerability	Potential Vulnerability - level 5
38597	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance	Informational
38598	Deprecated Public Key Length	PotentialVulnerability - level 2
38599	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Compression Algorithm Information Leakage Vulnerability	Vulnerability - level 3
38600	SSL Certificate will expire within next six months	Informational
38601	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)	Vulnerability - level 3
38602	OpenSSL Multiple Remote Security Vulnerabilities	Potential Vulnerability - level 4

38603	SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)	Vulnerability - level 3
38604	TLS CBC Incorrect Padding Abuse Vulnerability Secure Sockets Layer/Transport Layer Security (SSL/TLS)	Vulnerability - level 3
38605	Server Factoring RSA_EXPORT Keys Vulnerability (FREAK)	Vulnerability - level 4
38607	SSL Server Diffie-Hellman passive listening attack Vulnerability	Vulnerability - level 4
38608	SSL Server Diffie-Hellman Weak Encryption Vulnerability (Logjam)	Potential Vulnerability - level 4
38609	SSL Server default Diffie-Hellman prime information	Informational
38610	SSL/TLS Server supports TLS_FALLBACK_SCSV	Informational
38626	OpenSSL oracle padding vulnerability (CVE-2016-2107)	Vulnerability - level 4
38659	F5 BIG-IP TLS Vulnerability (Ticketbleed)	Vulnerability - level 4
38695	TLS ROBOT Vulnerability Detected	Vulnerability - level 4
38704	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods	Informational
38706	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties	Informational
38764	TLS Padding Oracle Vulnerability (Zombie POODLE and GOLDENDOODLE)	Vulnerability - level 3
42007	Debian OpenSSL Package Random Number Generator Weakness	Vulnerability - level 5
42012	X.509 Certificate MD5 Signature Collision Vulnerability	Vulnerability - level 2
42350	TLS Secure Renegotiation Extension Support Information	Informational
42366	SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)	Vulnerability - level 3
42430	OpenSSL Memory Leak Vulnerability (Heartbleed Bug)	Vulnerability - level 4
45218	Authenticated Certificate Retrieval - Information	Informational
45231	Trusted Digital Certificates Enumerated From Windows Registry	Informational
48143	Qualys Correlation ID Detected	Informational
86000	Web Server Version	Informational
86001	SSL Web Server Version	Informational
86002	SSL Certificate - Information	Informational
86137	HTTP Strict Transport Security (HSTS) Support Detected	Informational
105737	EOL/Obsolete Hardware: Cisco Application Control Engine (ACE) 30/4710 Secure Sockets Layer (SSL) Software Development Kit (SDK) Bleichenbacher Attack Information Disclosure Vulnerability (ROBOT)	Potential Vulnerability - level 5

120604	Oracle Java SE Critical Patch Update - October 2012 (ROBOT)	Vulnerability - level 5
316174	Cisco ASA Bleichenbacher attack on TLS Information Disclosure Vulnerability(ROBOT)	Vulnerability - level 4
370661	F5 BIG-IP OpenSSL Man in the Middle Vulnerability (K21905460) (ROBOT)	Vulnerability - level 4
370683	Citrix NetScaler ADC and Gateway TLS Padding Oracle Vulnerability (CTX230238) (ROBOT)	Vulnerability - level 4
38685	SSL Certificate - Invalid Maximum Validity Date Detected	Vulnerability - level 2
38716	Secure Sockets Layer (SSL) Certificate - Revoked	Vulnerability - level 2
38717	Secure Sockets Layer (SSL) Certificate Online Certificate Status Protocol (OCSP) Information	Informational
38718	Secure Sockets Layer (SSL) Certificate Transparency Information	Informational
45039	Host Names Found	Informational
42041	Detection of certificates with vulnerable keys 1 (ROCA)	Vulnerability - level 4

User Permissions

Depending on the roles and permissions assigned, the user can perform actions like creating, approving or rejecting certificate enrollment and renewal requests.

Certificate View user needs to be created in the VM/VMDR module and roles and permissions are assigned to the user from the Administrator module.

We have provided some pre-created user roles for Certificate View. Depending on the role you choose you get the associated set of permissions.

- **Manager**

  A user with Manager role is considered a super user and has all the available permissions.

- **Certificate View Administrator**

  User with the Administrator role is responsible for Administrating the CA. User can Submit and Approve certificate requests at the CA level and can submit Certificate Enrollment, Renewal, and Revocation Requests. This user also has all permissions on dashboards created by them or other users.

- **Certificate View Approver**

  User with Approver role can approve Certificate Requests at the company level and can submit Certificate Enrollment, Renewal, and Revocation Requests.

- **Certificate View Requester**

  User with Requester role can only submit Certificate Enrollment, Renewal, and Revocation Requests.

- **Certificate View Scan**

  User with Scan role can add External sites in Certificate View and run on-demand scans in the Certificate View -> Assets -> External Sites sub-tab.

- **Certificate View User**

  User with the Certificate View user role gets access to the Certificate View UI. This user also has permissions to create, edit, and delete dashboards created by them.

Tag-based User Scoping

Tag-based user scoping (TBUS) allows a manger user to scope a sub-user's access to assets based on tags. A manager user can restrict a sub-user's access to assets and certificates based on Tag-based User Scope.

Note: By default, the manager user has access to all the assets and tags.

Asset Tagging provides a flexible way to organize the assets in your environment. An asset tag is a tag assigned to one or more assets and allows sub-users to access those assets by assigning the same tag in their scope. If you have assigned a parent tag to a user, then the user has access to assets from the parent tag and all its child tags. If a user is assigned only a child tag, then the user can view assets with only the child tag.

For example, the manager user has 1000k assets. The manager user has assigned the Windows tag to 50k assets. The manager has assigned Windows tag to a sub user. In this case, the sub-user can view only 50k assets in the Assets tab and in Dashboard. In the Certificates tab, sub-user can view certificates found on those 50k assets.

You can apply tags manually or configure rules to automatically classify your assets. For more details on tagging asset, refer to Asset Tag of VM/VMDR Online help.

For more detail on Tag-based User Scoping, refer to VM/VMDR Online help.

View Certificates

Once you launch CertView scans you start getting up to date view on your certificates and security posture using Qualys Certificate View.

Note: The CertView scan option in VM/VMDR is visible only if CertView is turned on in your subscription.

Certificate View helps you

- Discover, inventory, monitor certificates, host configurations & vulnerabilities

- Vulnerability analysis and grading makes all relevant info available to you (host/port/service/certificate)

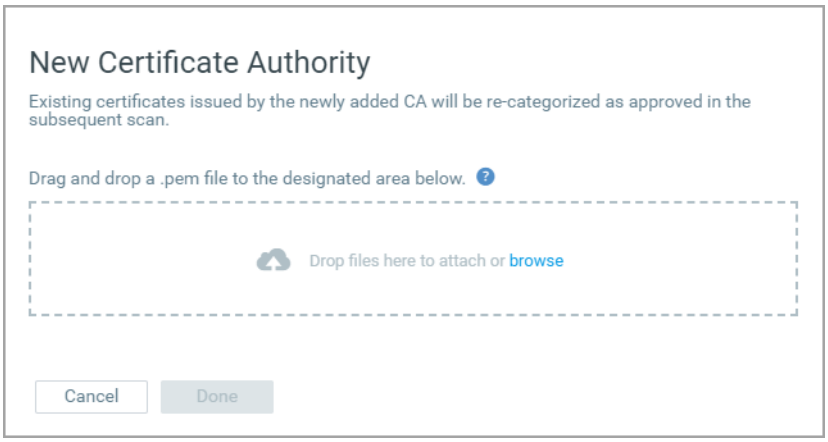
Configure Certificate Authorities

Add Certificate Authorities to better categorize and identify if the certificates are coming from approved or unapproved CAs.

Go to **Configuration** > **Approved CAs** > **New CA** and add a .pem file.

Note: We do not support the Binary format. The supported file format for a certificate is Base64 encoded ASCII. We recommend you to convert the file to Base64 encoded ASCII format before uploading.

Once a CA is added all existing and new certificates will be categorized in subsequent scan.



Add a DigiCert API Key

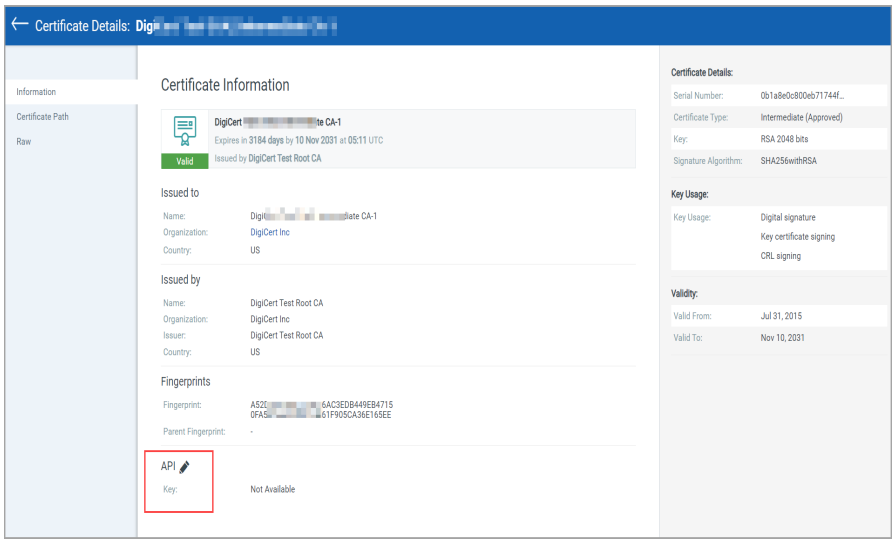
Qualys uses the DigiCert API key to communicate with DigiCert to enroll or renew certificates. You can choose to add an API key to an existing approved DigiCert CA.

To add an API Key to an approved CA in Certificate View

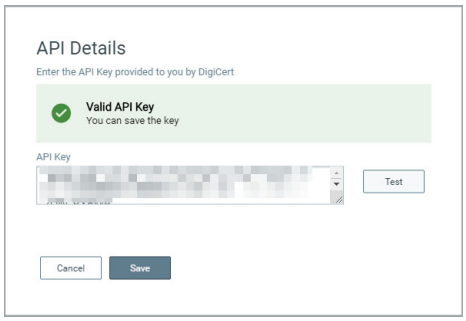
1) Get your API Key from DigiCert. You can get more information here.

2) Navigate to **Configuration** > **Approved CAs** and choose the CA you want to add the API key to.

3) From the **Quick Actions** menu click **View Certificate** and in the **Information** tab of Certificate Details, click the pencil icon next to API Key field.



4) In the **API Key** field copy the key you got from DigiCert. You can also test if the key is valid before saving the key for this CA.



Grades Calculation

We refer to the SSL Labs rating guide to explain how we calculate grades.

https://www.ssllabs.com/projects/rating-guide/index.html

There are a few differences in the way we assign grades:

- CertView will not penalize the grade under the following conditions:

  • Certificate hostnames don't match the site hostname (SSL Labs drops the grade to T)

  • Certificate has been revoked (SSL Labs drops the grade to F)

- SSL Labs runs browser simulation checks and may not penalize the server for using weaker ciphers if the browser simulations determine that the weaker ciphers are not negotiated when establishing the SSL connections. You may therefore see different grades in CertView for the following:

  • use of legacy 64-bit block ciphers (CertView drops the grade to C)

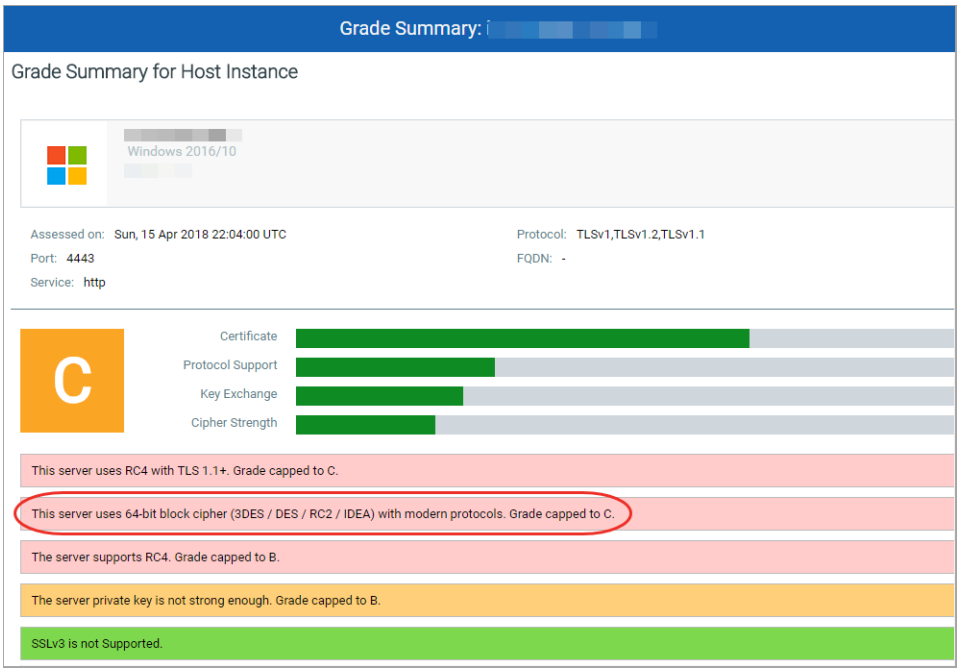
  • use of ciphers that theoretically support forward secrecy (CertView does not reward the server for using these ciphers)

  • use of CBC ciphers with TLS 1.2 or below (CertView drops the grade to F due to the GoldenDoodle vulnerability)

- CertView does not test for forward secrecy and will not penalize a server if it doesn't support forward secrecy.

  SSL Labs caps grades to B and penalizes sites if the server does not support forward secrecy. This assessment is made primarily based on the 60+ browser handshake simulations performed during the SSL Labs assessment.

  SSL Labs, however, does not penalize sites that use suites that are not capable of providing forward secrecy as long as they are not negotiated during browser handshake simulations Forward secrecy depends on a lot of information that cannot be detected remotely, such as the server caching policy of session tickets or the reuse of DH/ECDH keys. While CertView detects the ciphers that theoretically support forward secrecy, merely having such ciphers configured does not actually guarantee forward secrecy.

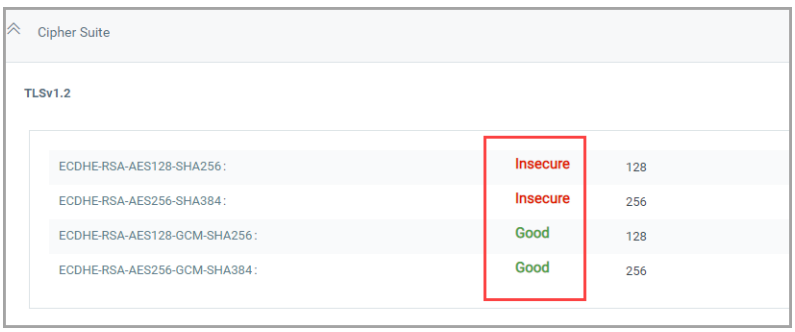


Color Coding and Labels in Cipher Suites

You can view the label and color code for the different Cipher Suites.

Color	Label
Green	Good
Orange	Weak
Red	Insecure
Default (Black)	Neutral

To view the Cipher Suites go to **Certificates** > select Certificate > **Hosts** > **Grades Summary** > **Cipher Suite** and click + icon present in front of protocol.

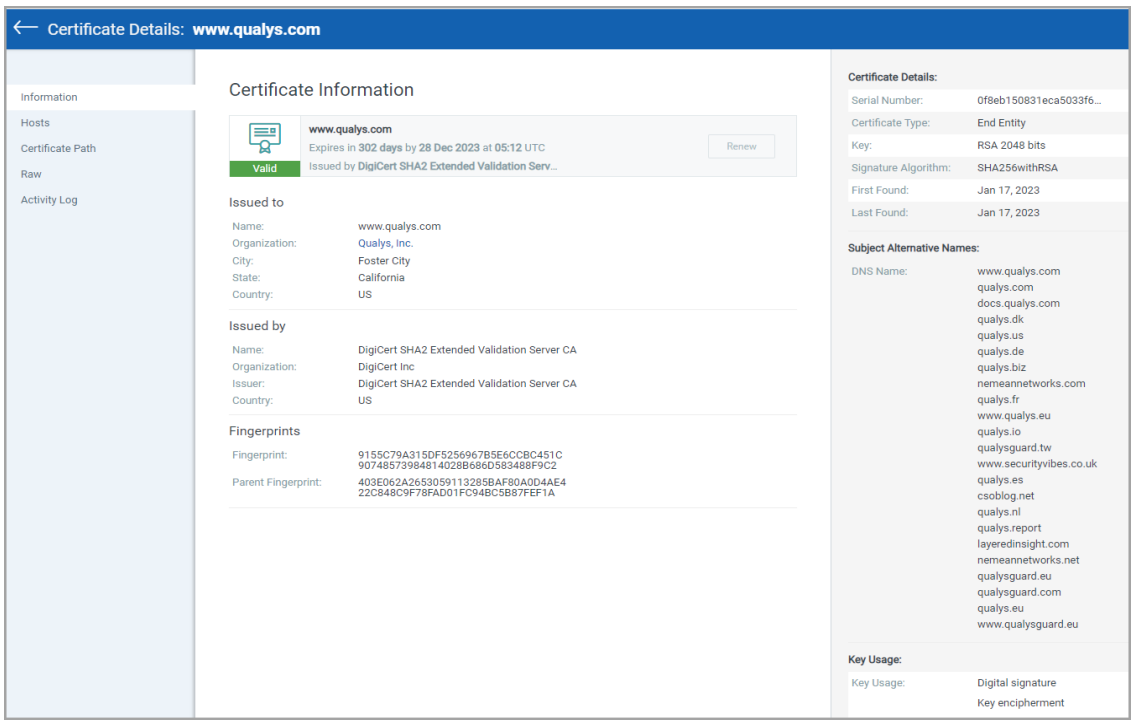


View Certificate Details

After your sites are scanned and if the sites are using certificates then those certificates are listed under the Monitored tab.

You can easily view details like issuer information, grading, host instances and certificate path of certificates discovered on your assets.

To view details of your certificate, simply go to **Certificates** > **Monitored** and from the **Quick Actions** menu select **View Details** of the desired certificate.



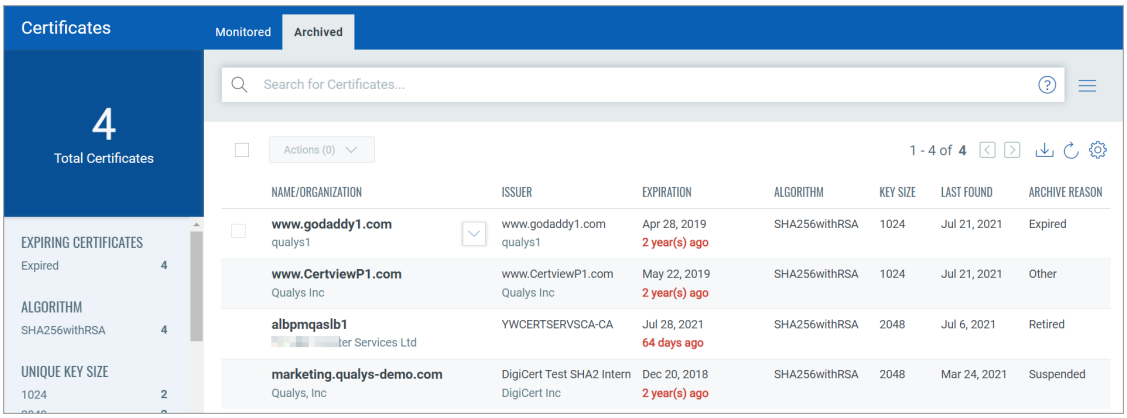
Archived Certificates

In case you do not want a specific certificate to appear in any reports, Dashboards, or list of certificates then you can Archive that certificate.

Go to **Certificates** > **Monitored** tab and from **Quick Actions** of the selected certificate, select Archive. You can choose to apply labels when you archive a certificate.

Once you archive the certificate, the certificate moves to the Archived tab, you can view the reason why certificate is archived.

Note: Archiving a certificate detaches the instances and assets that the certificate was found on. Rescan the asset after restoring the certificate to view the details on dashboards, reports or alerts.



Enroll Certificates

You can enroll or renew your certificates if your Certificate Authority is DigiCert, To enroll for certificates, you must have one of these permissions:

- Certificate View Administrator

- Certificate View Approver

- Certificate View Requestor

For more details, refer to User Permissions section.

To enroll for a new certificate navigate to **Certificates** > **Monitored** > **New** and choose **Enroll**. Follow the wizard to provide information required to help us create an enrollment request.

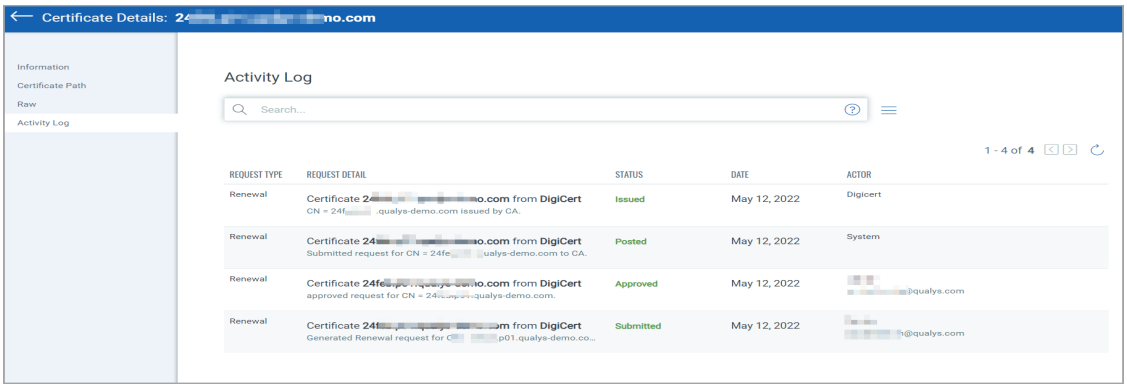
Currently, we can create enroll request for only if the CAs are hosted by DigiCert.

From the list of users, select an approver who will approve this enrollment request before it is sent to DigiCert.

View Progress of Renewal Request

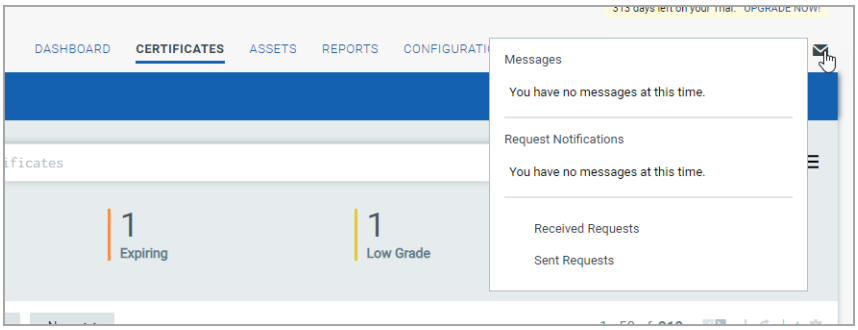
You can monitor the activity log and progress of your renewal request in the Activity log tab.

Choose the certificate you have sent for renewal from the **Monitored** tab and from **Quick Actions** menu ,select View **Details**. Navigate to the **Activity Log** tab to view progress and status of the renewal request.



View Request Status

To view the status of all the enrollment and renewal requests that you sent and received, click the Messages icon in the top right corner to view all the requests.



Renew Your Certificates

You can renew your certificates that are about to expire. Certificate View helps you send a renewal request to DigiCert. You can renew certificates from other issuing entities acquired by DigiCert, such as Twathe, Mocana, GeoTrustand so on.

Navigate to **Certificates** > **Monitored** and choose the certificate you want to renew. From **Quick Actions** menu, select **Renew**.

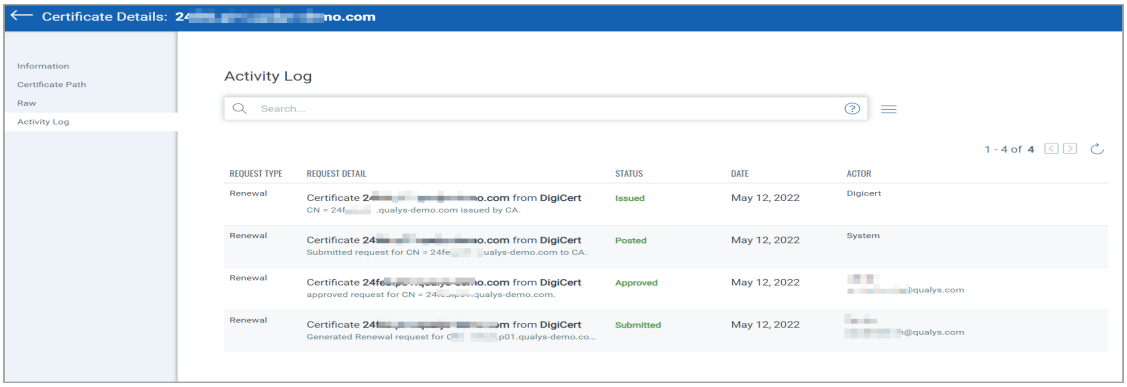
All existing information about the certificate is pre-filled in the wizard. Make sure you provide the accurate Order Id. In case the order id is incorrect, DigiCert rejects the renewal request.

Once you submit the request it is sent for approval to the user you selected.

View Progress of Renewal Request

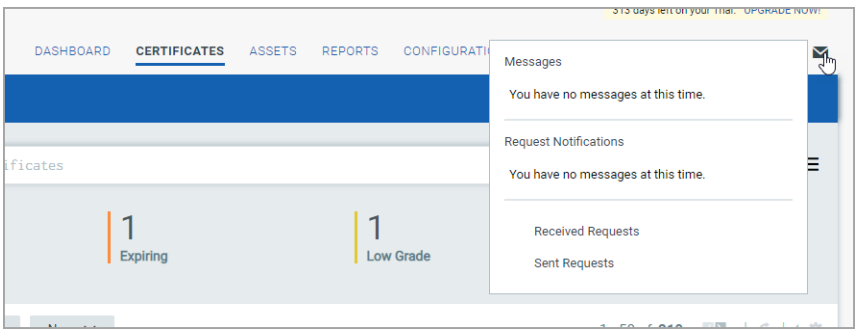
You can monitor the activity log and progress of your renewal request in the Activity log tab.

Choose the certificate you have sent for renewal from the **Monitored** tab and from **Quick Actions** menu ,select View **Details**. Navigate to the **Activity Log** tab to view progress and status of the renewal request.



View Request Status

To view the status of all the enrollment and renewal requests that you sent and received, click the Messages icon in the top right corner to view all the requests.



Import Leaf Certificates

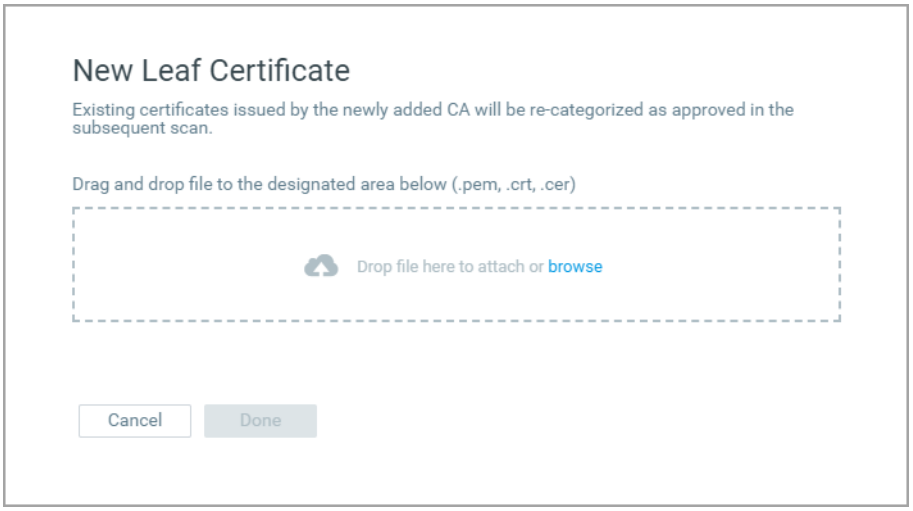
You can import end-entity or leaf certificates in your account. These non-CA certificates are listed as unapproved certificates. If new CAs are added then on subsequent scans these certificates will be re-categorized as approved certificates.

Importing a leaf certificate

Navigate to **Certificates** > **Monitored** > **New** and select Import Leaf Certificate. Upload a .pem, .crt, or .cer file to import the certificates.

You can also choose to import multiple leaf certificates in the same file. All these certificates gets listed in the certificates list of the Monitored tab.

Note: We do not support the Binary format. The supported file format for a certificate is Base64 encoded ASCII. We recommend you to convert the file to Base64 encoded ASCII format before uploading.



Manage Assets

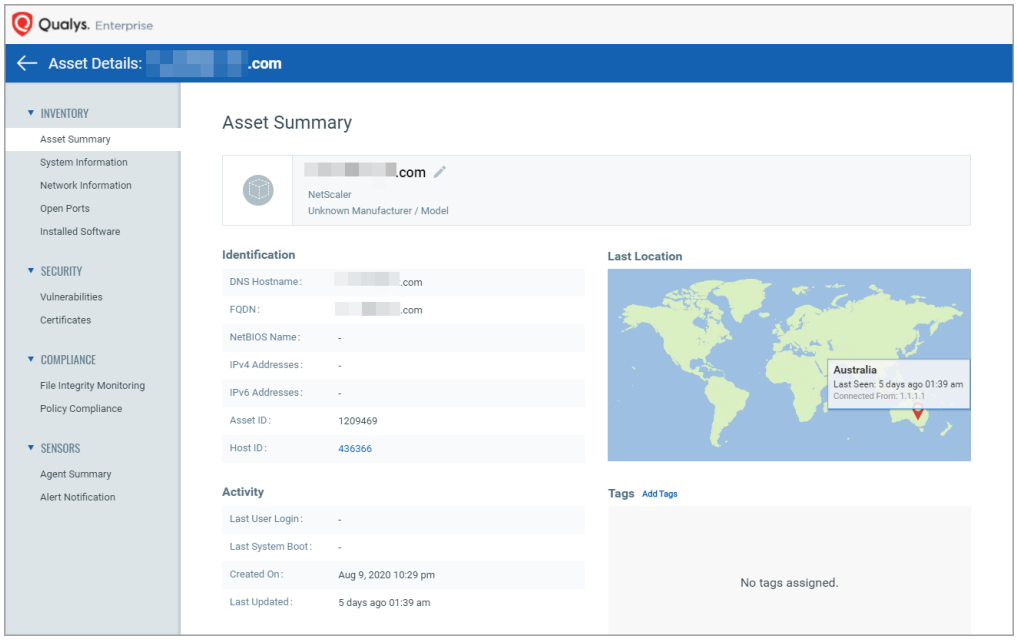
You can view the details of assets and delete assets from **Assets** tab.

View Asset Details

You can view details of assets associated with the certificates once your host sites are resolved and scanned in Asset Details.

All assets are listed in the Assets tab. You can view details like ports, vulnerability, certificates, installed software etc, of the assets on which the certificates were discovered.

To view details, go to **Assets** > **Assets** and from **Quick Actions** menu, select **View Details** for the selected asset.



Delete Assets and External Sites

You can delete assets and external sites from the Assets tab.

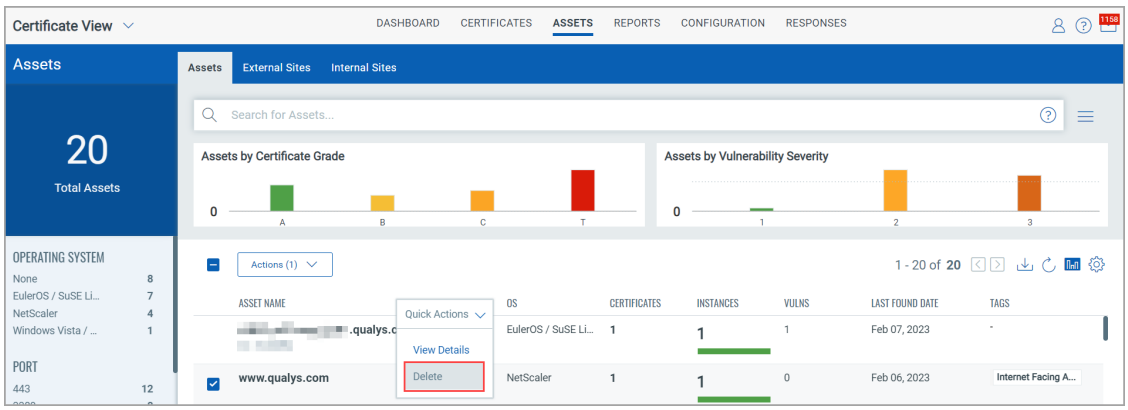
Delete Assets

When you delete the assets, associated mappings, such as external sites and certificates, also get deleted.

Note: Assets with external sites in the running state are not deleted.

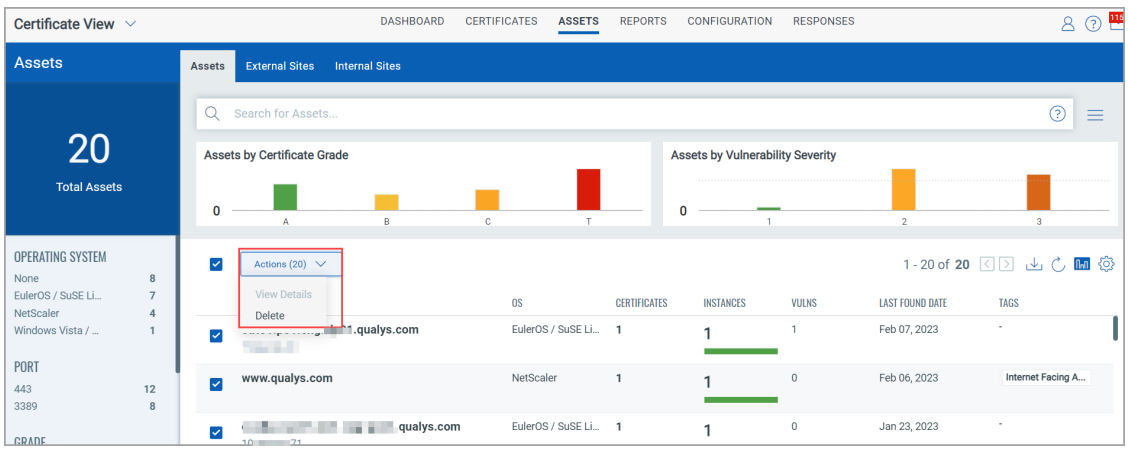
Delete a Single Asset

Select the asset you want to delete and select **Delete** from the **Quick Actions** menu.



Delete Assets in Bulk

Select all the assets you want to delete and click **Delete** from the **Actions** menu.



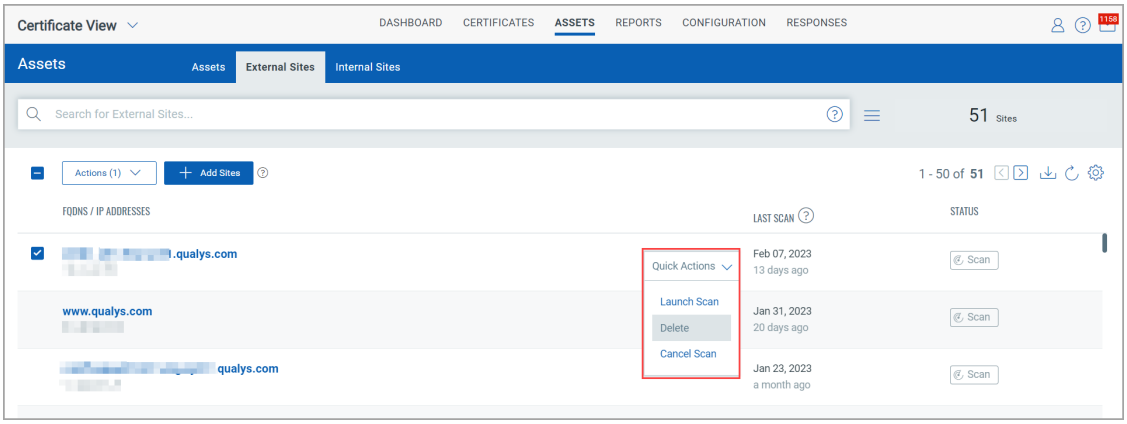
Delete External Sites

When you delete external sites, associated assets and certificates also get deleted.

Note: The external sites with scans in the running state are not deleted.

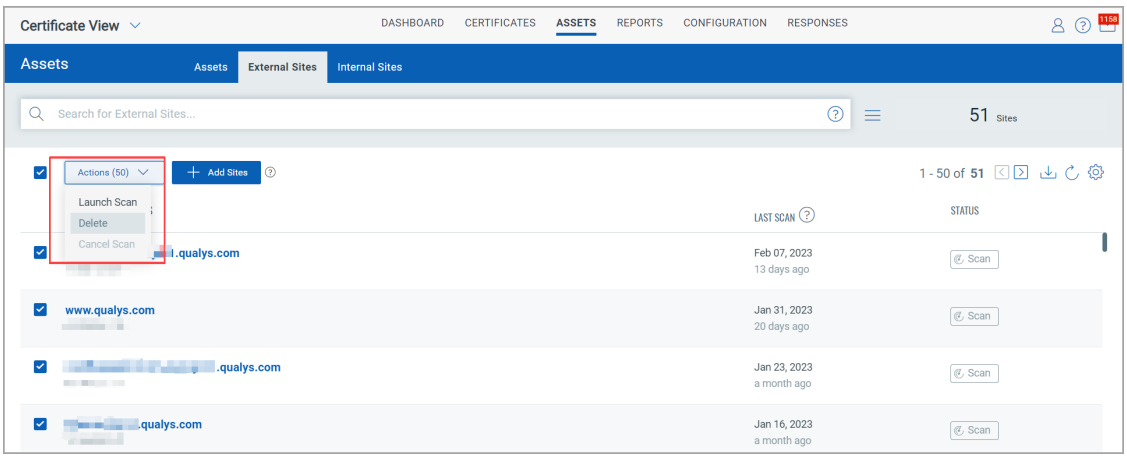
Delete a Single External Site

Select the external site you want to delete and select **Delete** from the **Quick Actions** menu.



Delete External Sites in Bulk

Select all the external sites you want to delete and click **Delete** from the **Actions** menu.



Rule-based Alerts

You can define the conditions, significant findings, or events that should trigger the rules and send you alerts. The alert is generated based on the Rules Query and you get the notification when the query criteria is matched.

For example, you can set up alerts for:

- Certificates expiring in 30/60/90 days

- Self-signed certificates

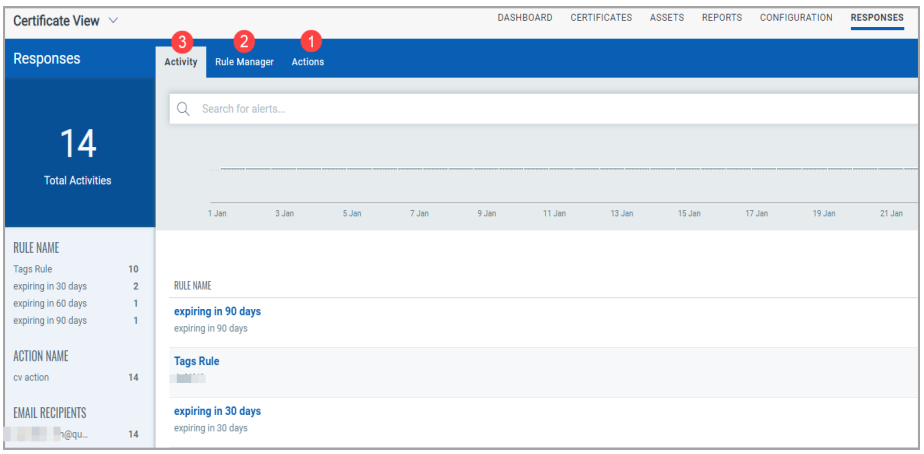
- Certificates from unapproved CAs

- Certificate instances with low grades

- Certificates with weak key lengths or hashing algorithms

Configure Rule-based Alerts

Just tell us what you consider to be a significant finding or event and the mechanism in which you want to be alerted.



Step 1 - Define actions that the rule must take in response to the alert

Create and Manage Actions

Step 2 - Set up your rules in the Rule Manager tab

Create and Manage Rules

Step 3 - Monitor all the alerts that were sent after the rules were triggered

Manage Alerts

You are all set to start being alerted about your certificate findings.

Create and Manage Actions

Define the method in which you want to be alerted once any rule is triggered.

Create an Action

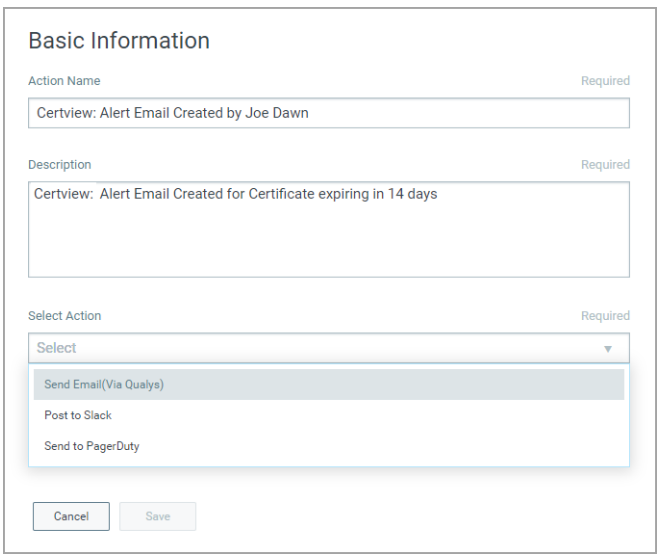
Navigate to **Responses** > **Actions** > **New Action** and provide details to create a new action:

- In the Basic Information section, provide name and description of the action in the Action name and Description fields respectively.

- Select an action from the Select Action list and provide the settings for configuring the messaging system that we will use to send alerts.

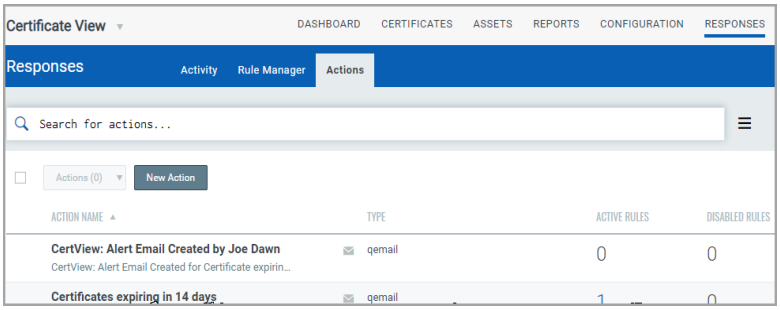
- We support three actions: Send Email (Via Qualys), Post to Slack and Send to Pager Duty for alerts.

  - Select **Send Email (Via Qualys)** to receive email alerts. Specify the recipients' email ID who will receive the alerts, subject of the alert message and the customized alert message.
  - Select **Send to PagerDuty** to send alerts to your PagerDuty account. Provide the service key that is required to connect to your PagerDuty account. In Default Message Settings, specify the subject and the customized alert message.
  - Select **Post to Slack** to post alert messages to your Slack account. Provide the Webhook URI that will be used to connect to your slack account to post alert messages. In Default Message Settings, specify the subject of the alert message and the customized alert message.



Manage Actions

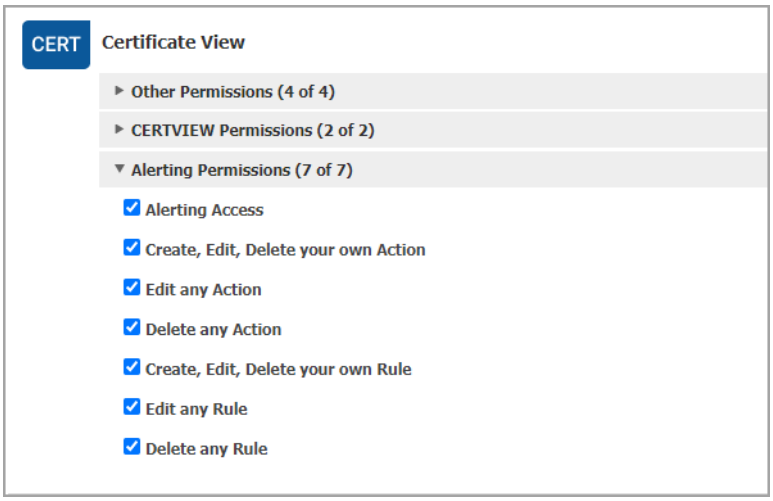
View the newly created actions in the Actions tab with details such as name of the action, type of the action, the number of rules for which this action is chosen are active or inactive, etc. Use the Actions menu or Quick Actions menu to edit or delete actions. You can also save an existing action along with its configurations to create a new action. Use the search bar to search for specific actions using the search tokens



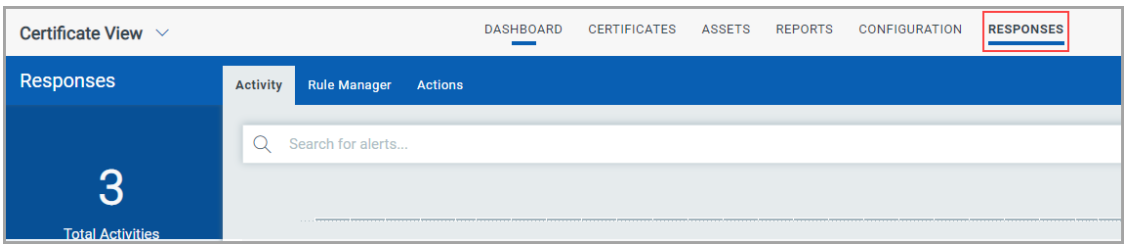
Alerting Permissions

Assign permissions related to alerting to your user. Depending on the permissions assigned, the user can perform actions like creating, editing, or deleting rules and actions.

Using the Administration module, the Manager user for that subscription can assign these permissions to other users.



Only the user having the Alerting Access permission can view the Responses tab on the Certificate View UI.



Create and Manage Rules

You can define the conditions, significant findings, or events that should trigger the rules and send you alerts. The alert is generated based on the Rules Query and you get the notification when the query criteria is matched.

For example, you can set an alert for certificates that are detected with low-grade summary like C or D or you can set an alert for certificates expiring in 30 days to ensure timely certificate renewal.

You can provide a Rule Query while creating an alert you get the notification every time the query criteria are matched.

Note: When you use the Expiry token as your Rule Query, the alert feature will only notify you once when a rule query is matched, regardless of how many scans are performed. Alert for Expiry token is not dependent on scans you perform on the assets.

Let us consider a case where you want alerts for expiring certificates frequently. To make sure you receive timely notifications for upcoming certificate expirations, you can create multiple rules with specific search criteria. This ensures that no renewal deadlines are missed, and allows for easy management at a time convenient for you.

To receive alerts for certificates that will expire in 30, 15, or 5 days, you can create multiple rules with queries like certificate(expiryGroup: "In 30 days"), certificate(expiryGroup: "In 15 days"), certificate(expiryGroup: "In 5 days"). This will ensure you receive timely notifications.

Here is an example of how to set up a rule for certificates that will expire in 30 days. You can also create rules for certificates that will expire in 15 days, 5 days, or any other timeframe you prefer.

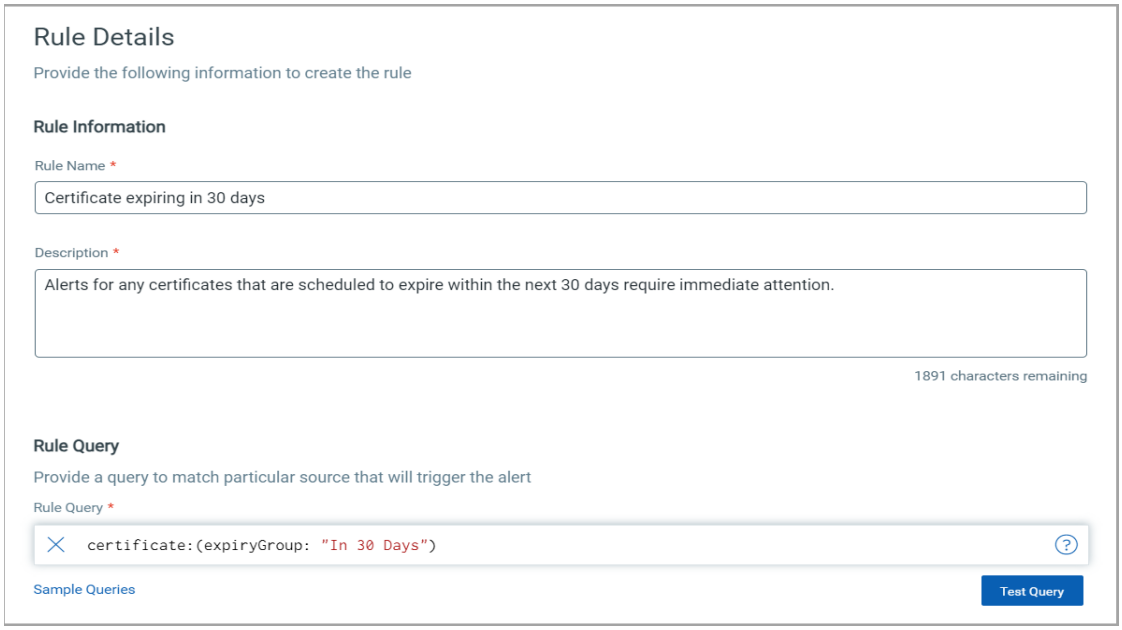
Create a Rule

Navigate to **Repsponses tab**> **Rule Manager** > **New Rule** and provide required details in the respective sections to create a new rule:

- In the Rule Information section, provide a name and description of the new rule.

- In the Rule Query section, specify a query for the rule. The system uses this query to search for events. Use the Test Query to test your query.

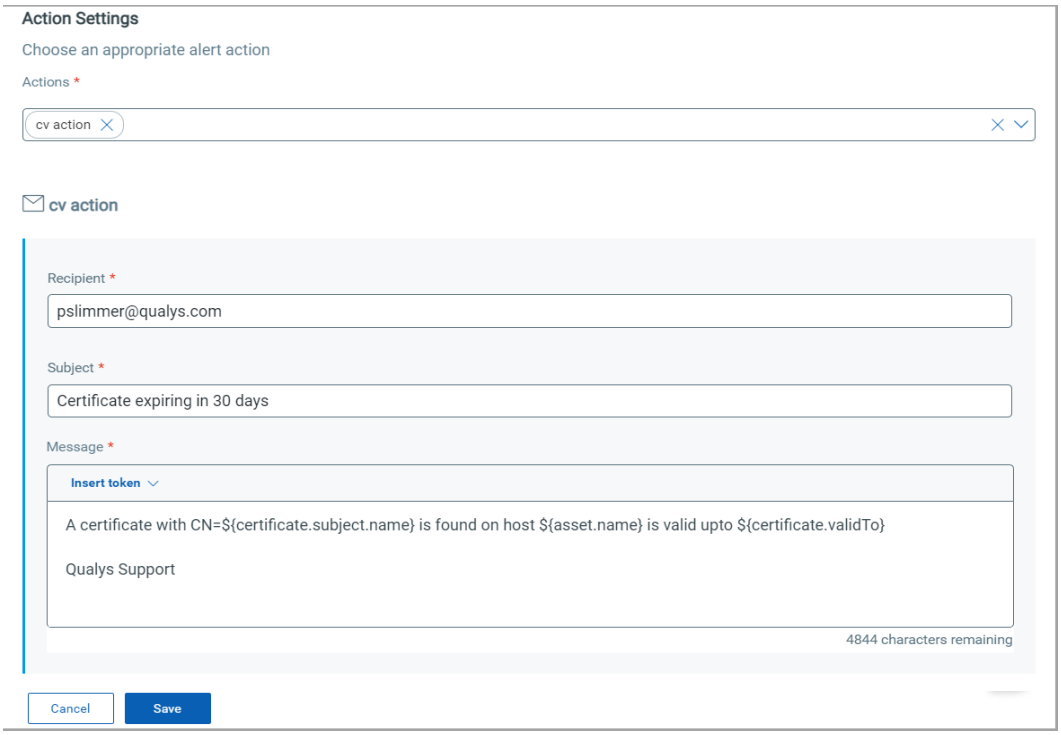
Click **Sample Queries** to select from predefined queries.



- In the Action Settings section, choose the actions that you want the system to perform when an alert is triggered.

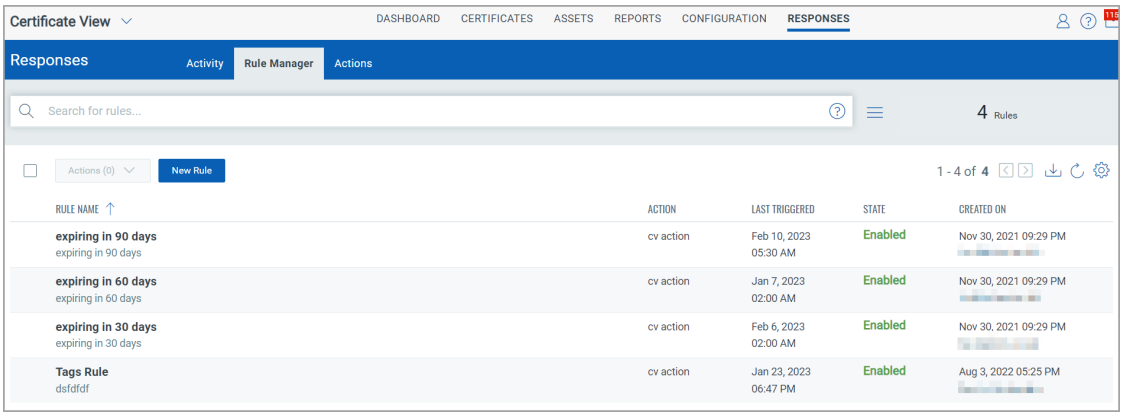
You can also customize the message text by inserting tokens to the alert message.

Note: For customizing message certificate:(expiryGroup is not applicable in the Insert token field, use certificate:(validTo token to view the certificate to view expiration date of the certificates.



Manage Rules

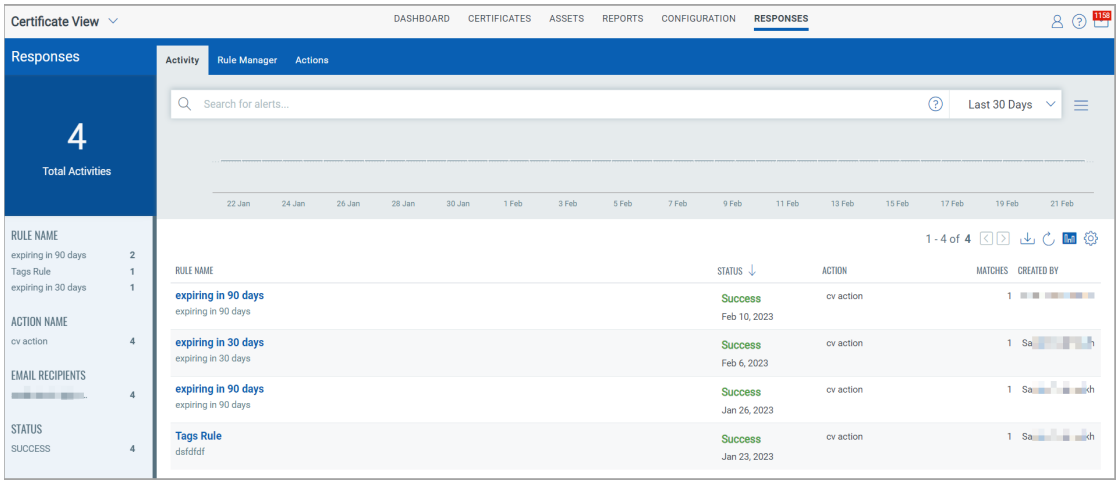
View all the rules created in the Responses tab with details such as trigger criteria selected for the rule, action chosen for the rule, state of the rule, whether the rule is enabled or disabled, etc. Use the Actions menu or Quick Actions menu to perform quick actions on rules, such as, edit, delete rule, enable, disable, delete and save an existing rule along with its configurations to create a new rule. Use the search bar to search for rules using the search tokens.



Manage Alerts

Once a rule condition is met an action is triggered and the stakeholders are alerted. These alerts are listed in the Activity tab for you view. Here you will see for each alert, rule name, success or failure in sending the alert message, action chosen for the rule, matches found for the rule etc.

You can easily search for alerts using search tokens, select a period to view the rules triggered during that time frame, click a bar to jump to the alerts triggered in a certain time frame, use filters listed on left to group the alerts by rule name, action name, etc.



Create Reports in Certificate View

You can generate on-demand or scheduled reports to view the certificates detected on specific assets.

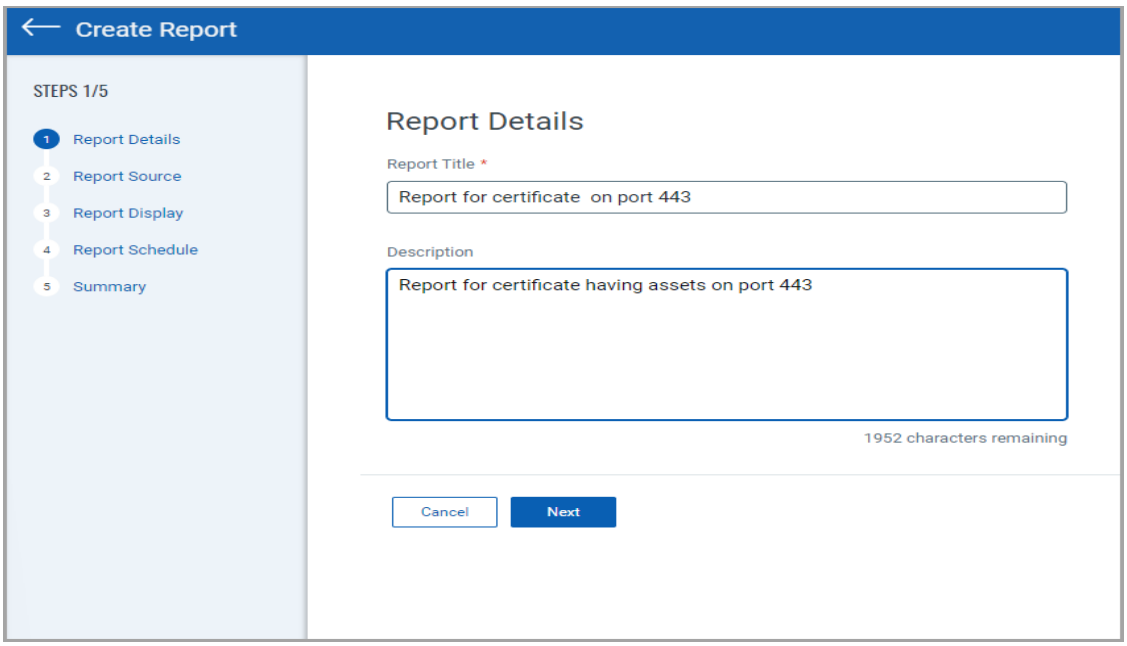
For example, you can create a report to view all certificates available on a specific port or detected on a specific operating system Currently, you can download a report only in CSV format.

Create a Report

Go to **Reports** > **Create Report** and provide required information in the wizard to create a report.

The following example shows a report created for certificates detected on port 443.

1. In the **Create Report** wizard, define the assets.

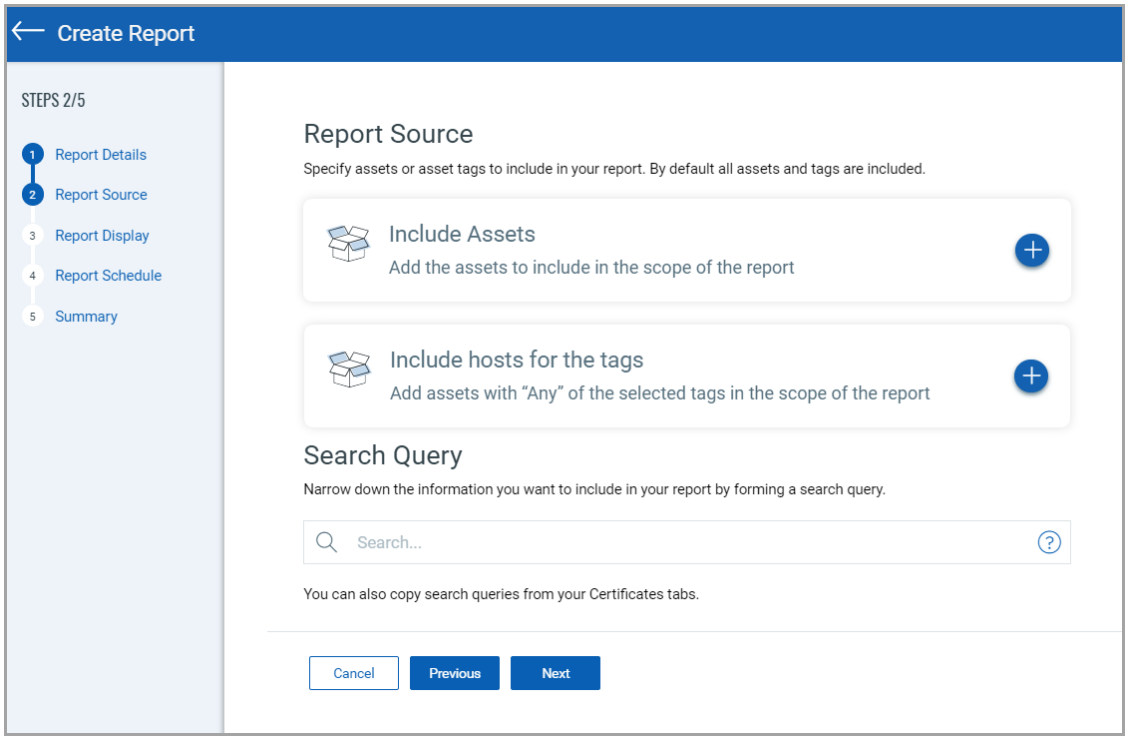


2. Add a source for the report.

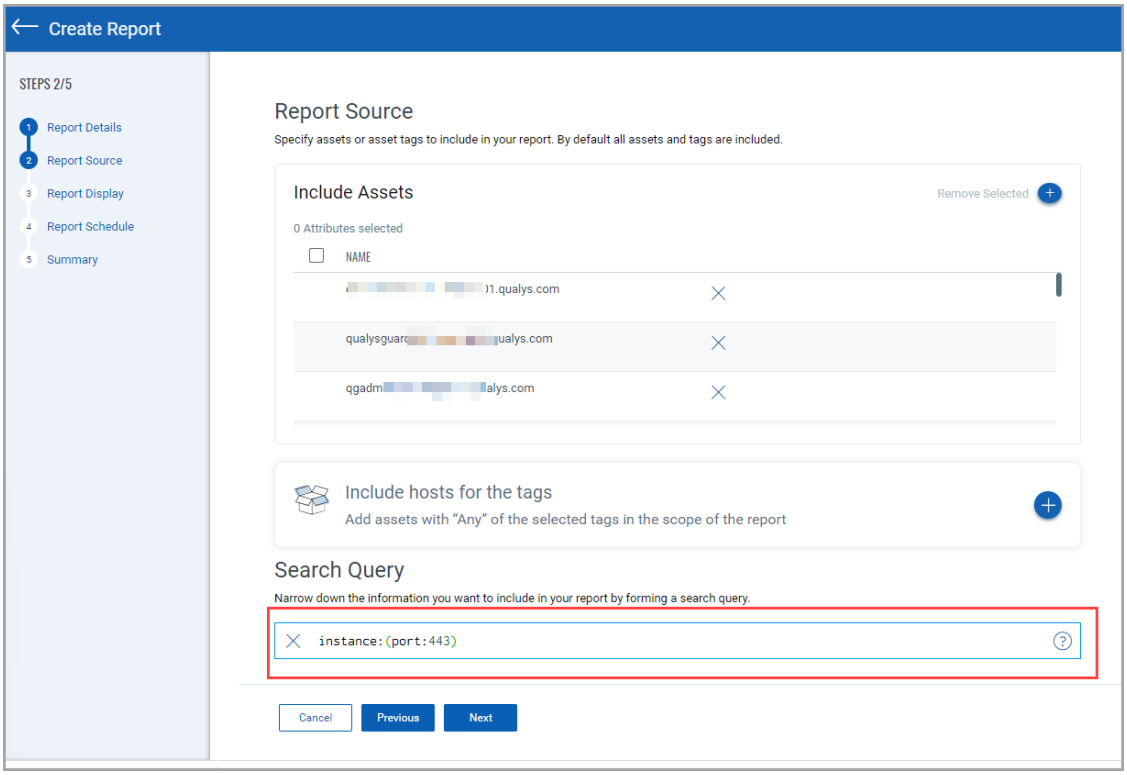
You can include the assets in the scope of the report from **Include Assets**. You can select a maximum of 250 assets. If you have more than 250 assets, you can use Include hosts for the tags. You can group the assets in tags and select the tag to include the assets in the scope. The feature **Include hosts for the tags** is available to the users who have either of the following permissions

- TAGGING.CREATE_USER_TAG

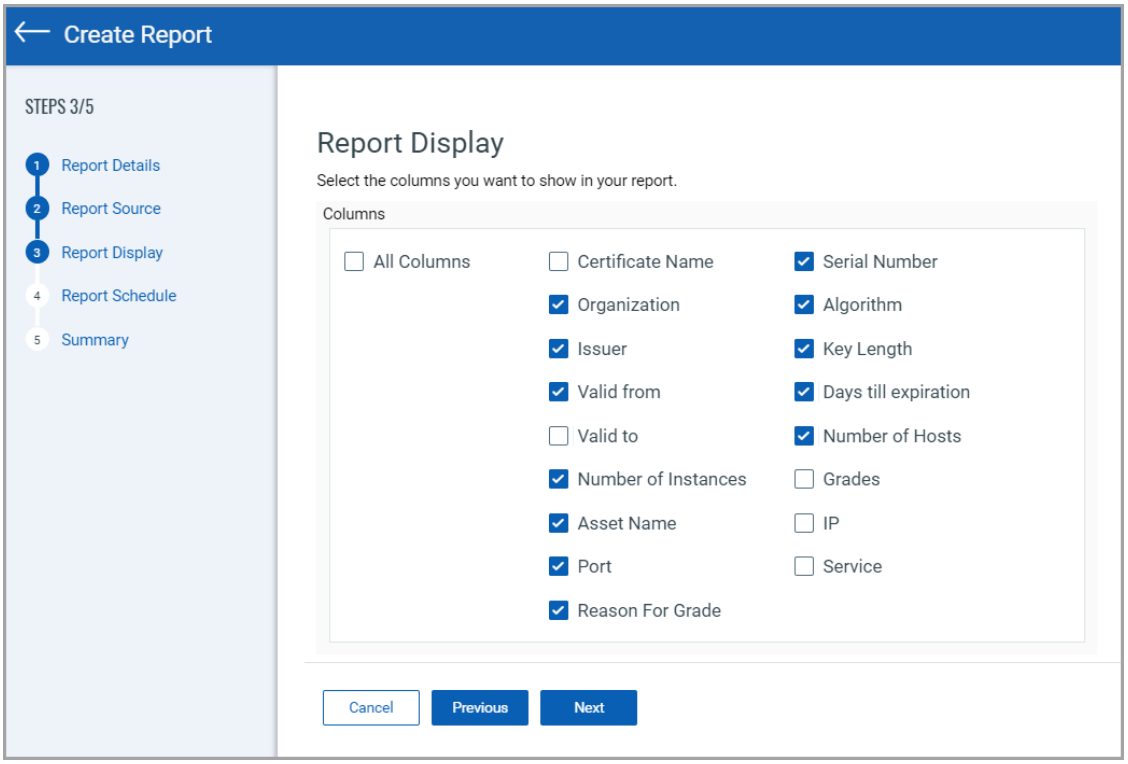
- TAGGING.ADD_REMOVE_TAG


Create Report
STEPS 2/5
1 Report Details
2 Report Source
3 Report Display
4 Report Schedule
5 Summary
Report Source
Specify assets or asset tags to include in your report. By default all assets and tags are included.
Include Assets
Add the assets to include in the scope of the report
Include hosts for the tags
Add assets with "Any" of the selected tags in the scope of the report
Search Query
Narrow down the information you want to include in your report by forming a search query.
Search...
You can also copy search queries from your Certificates tabs.
Cancel
Previous
Next

3. Provide the **Search Query** for instances on port 443 and click **Next.**



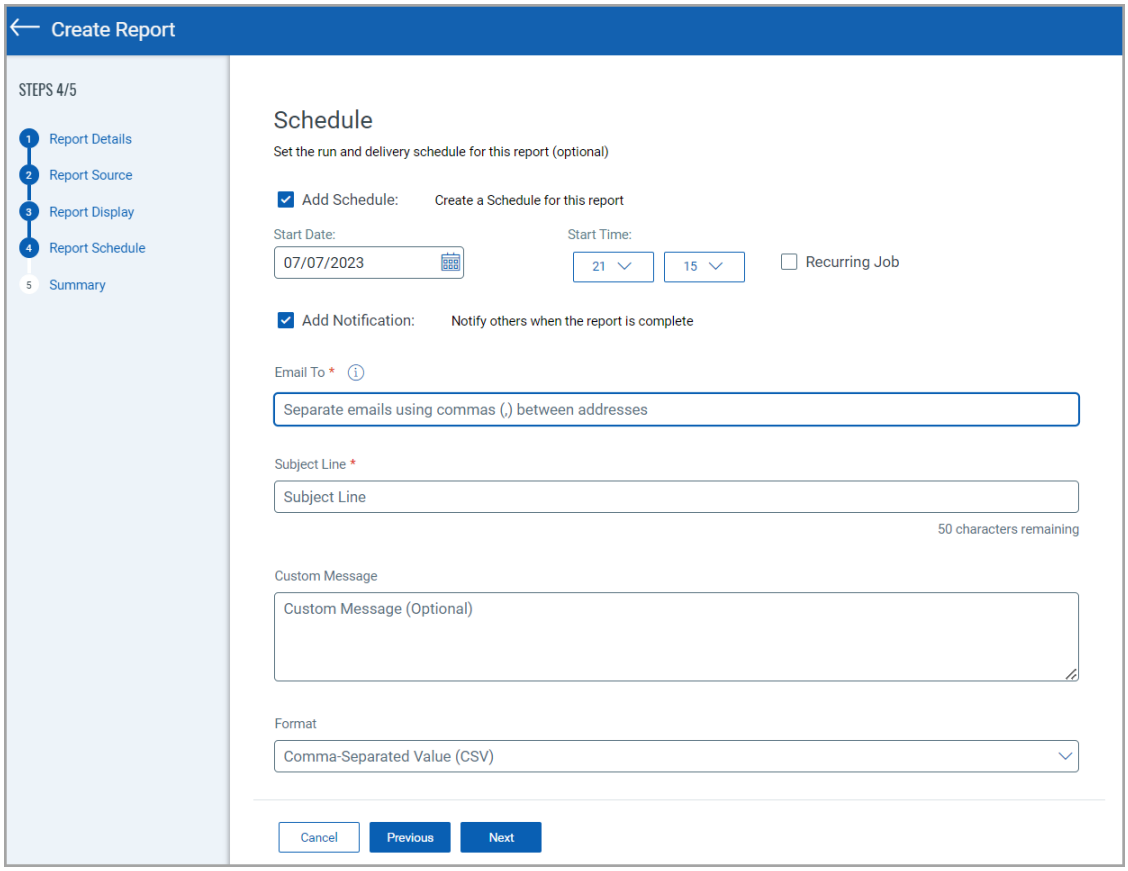
4. Choose the information you want to display. You can select the columns you need in the report.



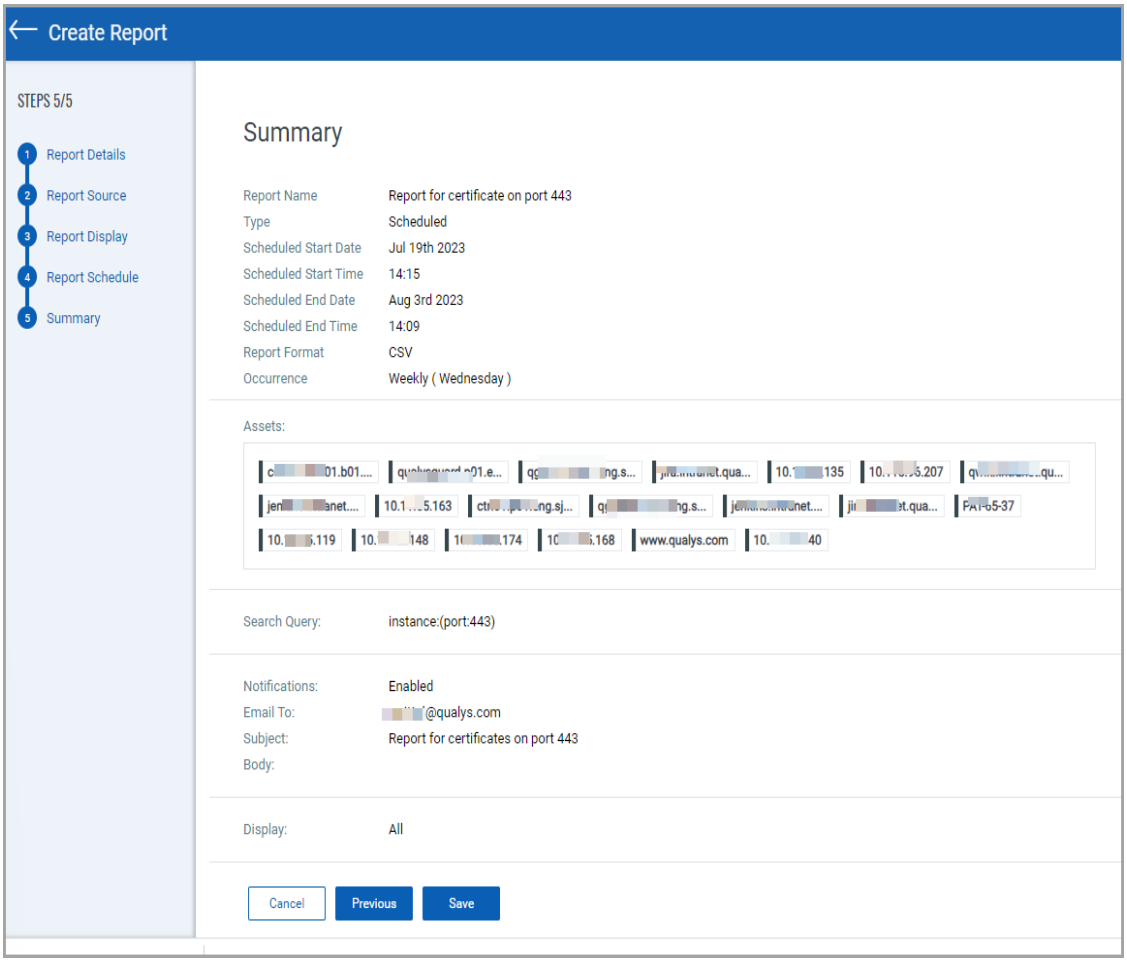
5. Schedule the report as per your requirement.

- Add **Schedule** to your report by providing Start Date and Start Time.
- Select the **Recurring Job** checkbox to make it recurring.
- Select **Add Notifications** checkbox to notify other users.
- Provide the **Email** addresses separated by commas and Subject Line.

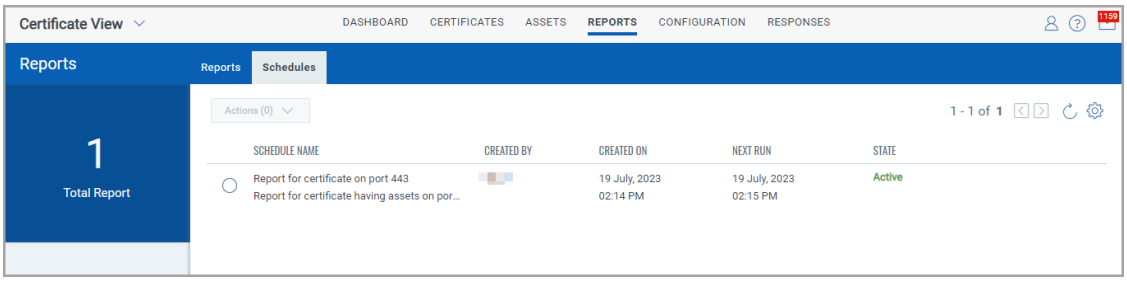
5. Click **Next** to view the Summary of the report.


Create Report
STEPS 4/5
1 Report Details
2 Report Source
3 Report Display
4 Report Schedule
5 Summary
Schedule
Set the run and delivery schedule for this report (optional)
Add Schedule:
Create a Schedule for this report
Start Date:
07/07/2023
Start Time:
21
15
Recurring Job
Add Notification:
Notify others when the report is complete
Email To *
Separate emails using commas (,) between addresses
Subject Line *
Subject Line
50 characters remaining
Custom Message
Custom Message (Optional)
Format
Comma-Separated Value (CSV)
Cancel
Previous
Next

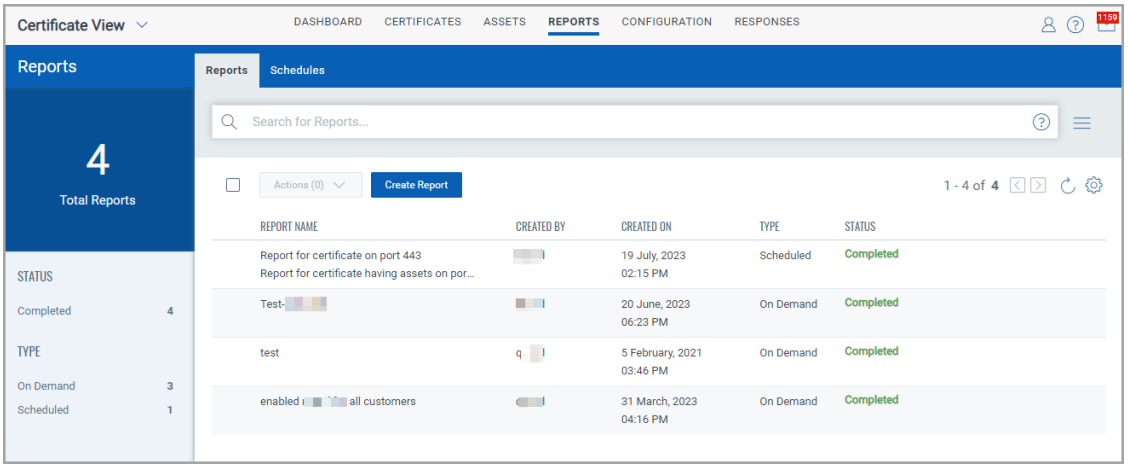
7. Review the summary of your Report and click **Save**.



You can view the report in the **Schedules** tab, as you have created a scheduled report.

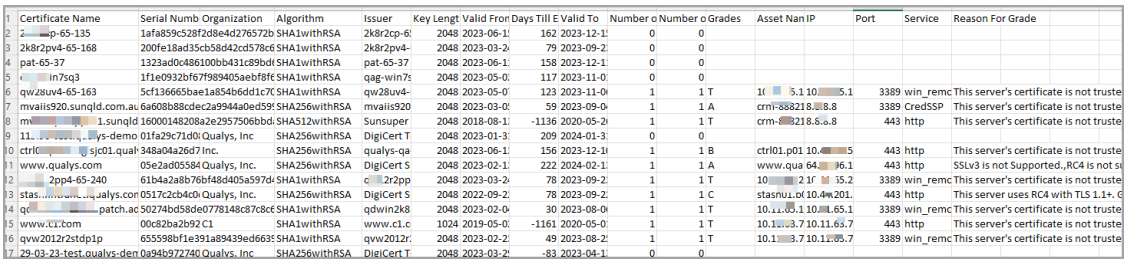


Once the report is generated, you can view the report in the **Reports** tab.



You can download the reports from the Quick Actions menu.

Refer to the following screenshot for a sample report.



Certificate Dashboards

To visualize your certificate posture across your assets, simply use our Unified Dashboard. A default dashboard is provided to get you started, however you can create a custom dashboard to customize the way you view your information.

Unified Dashboard (UD) brings information from all Qualys applications into a single place for visualization. UD provides a powerful new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

You can use dashboards to convey relevant information to any audience at any time and in any place. The dashboards can be customized and shared with their intended end-users.

UD provides greater agility and enriches capabilities of dashboards. You can visualize data from other applications at a central place and get a better understanding of your data. You can use widget builder and improvise dashboards to make it uniform across all products.

Benefits

- Powerful platform to enhance your dashboards

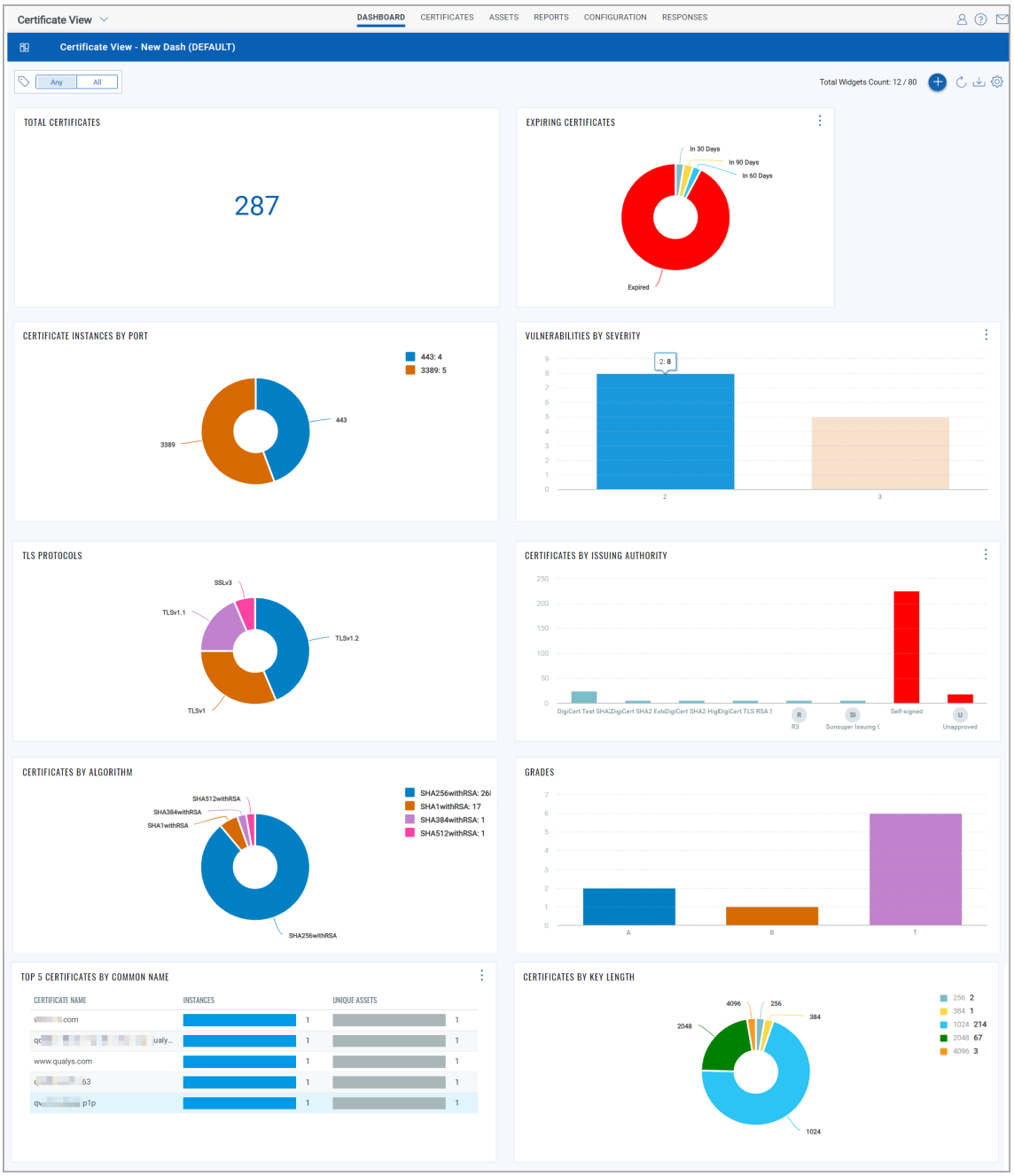
- Capability to pull information from all Qualys applications

- Central place to visualize your data from different Qualys applications

- Enhanced widget builder capabilities for uniform widgets across all products

Create multiple dashboards and switch between them for different views of your data.

For example, you can see the list of expired or expiring certificates, certificates with less than 2048-bit keys or certificate with SHA1 algorithms by clicking on the corresponding widget. The assets that host these certificates can then be listed within 2 clicks.



You can use the default Certificate View dashboard provided by Qualys or easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your certificate posture view.

Know more here

Refresh your view

You might want to see the latest data for a single widget on your dashboard. Just click Refresh from the widget menu. To refresh all widgets in one go, choose Refresh Dashboard from the tools menu.