Qualys Certificate View

User Guide

April 25, 2022

Copyright 2022 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

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. We'll help you 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! We'll start discovering certificates that are present on your cloud assets.

What assets are included?

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.

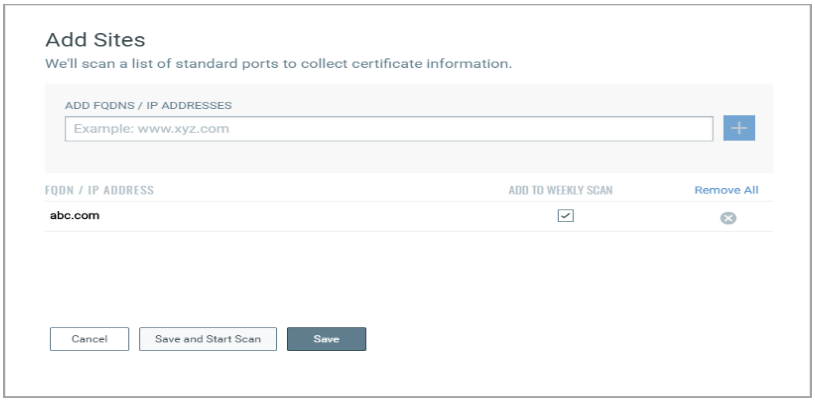
Add External Sites

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. We'll scan a list of standard ports to collect certificate information on the sites provided by you.

Select the Add to Weekly Scan option 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.



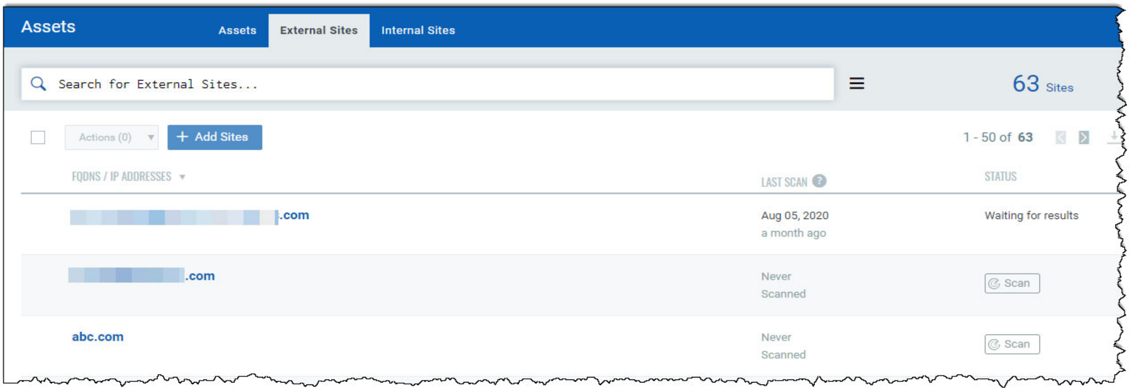
Add Sites

We'll scan a list of standard ports to collect certificate information.

ADD FQDNS / IP ADDRESSES: Example: www.xyz.com

FQDN / IP ADDRESS	ADD TO WEEKLY SCAN	Remove All
abc.com	☑	⊗

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, status of the scan (Queued, Running, Waiting for results, Finished), etc.



FQDNS / IP ADDRESSES	LAST SCAN	STATUS
[redacted].com	Aug 05, 2020 a month ago	Waiting for results
[redacted].com	Never Scanned	Scan
abc.com	Never Scanned	Scan

Add Internal Sites

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

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.

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

We will run scans 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.

Simply 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.

A limited 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

38116	38356	38608	42430
38139	38477	38609	45218
38142	38596	38610	45231
38167	38597	38626	48143
38168	38598	38659	86000
38169	38599	38695	86001
38170	38600	38704	86002
38171	38601	38706	86137
38172	38602	38764	105737
38173	38603	42007	120604
38174	38604	42012	316174
38182	38605	42350	370661
38224	38607	42366	370683

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 will be 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)

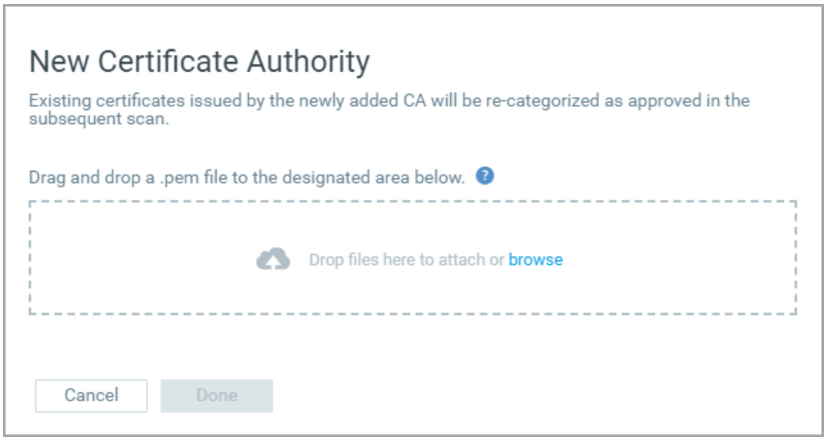
Configure Certificate Authorities

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.



New Certificate Authority

Existing certificates issued by the newly added CA will be re-categorized as approved in the subsequent scan.

Drag and drop a .pem file to the designated area below.

Add a DigiCert API Key

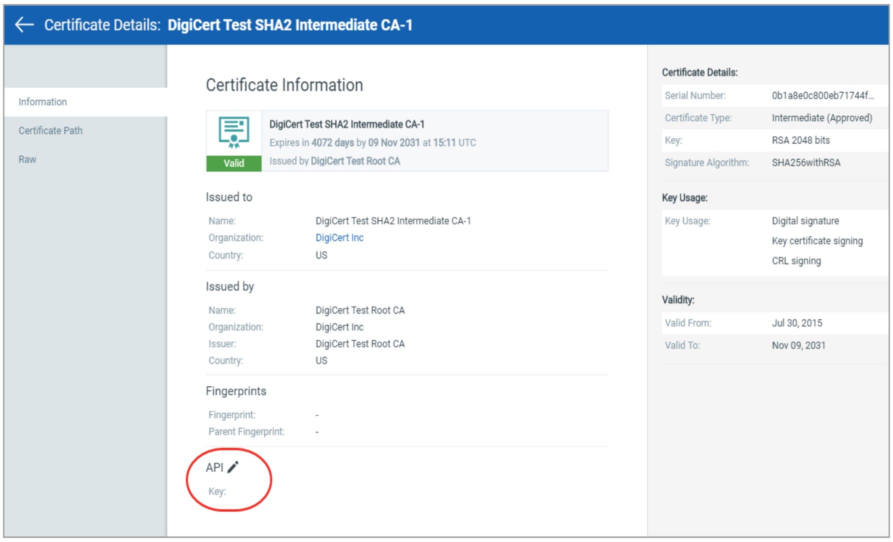
Qualys uses the DigiCert API key to communicate with DigiCert to enroll or renew certificates. You can choose to add an API key to an existing approved DigiCert CA.

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. .



Certificate Details: **DigiCert Test SHA2 Intermediate CA-1**

Certificate Information

DigiCert Test SHA2 Intermediate CA-1
Expires in 4072 days by 09 Nov 2031 at 15:11 UTC
Issued by DigiCert Test Root CA
Valid

Issued to

Name:	DigiCert Test SHA2 Intermediate CA-1
Organization:	DigiCert Inc
Country:	US

Issued by

Name:	DigiCert Test Root CA
Organization:	DigiCert Inc
Issuer:	DigiCert Test Root CA
Country:	US

Fingerprints

Fingerprint:	-
Parent Fingerprint:	-

API
Key:

Certificate Details:

Serial Number:	0b1a8e0c800eb71744f...
Certificate Type:	Intermediate (Approved)
Key:	RSA 2048 bits
Signature Algorithm:	SHA256withRSA

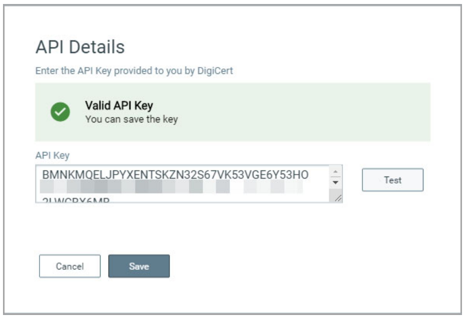
Key Usage:

Key Usage:	Digital signature Key certificate signing CRL signing

Validity:

Valid From:	Jul 30, 2015
Valid To:	Nov 09, 2031

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..



API Details

Enter the API Key provided to you by DigiCert

Valid API Key
You can save the key

API Key: BMNKMQELJPYXENTSKZN32S67VK53VGE6Y53HO [redacted]

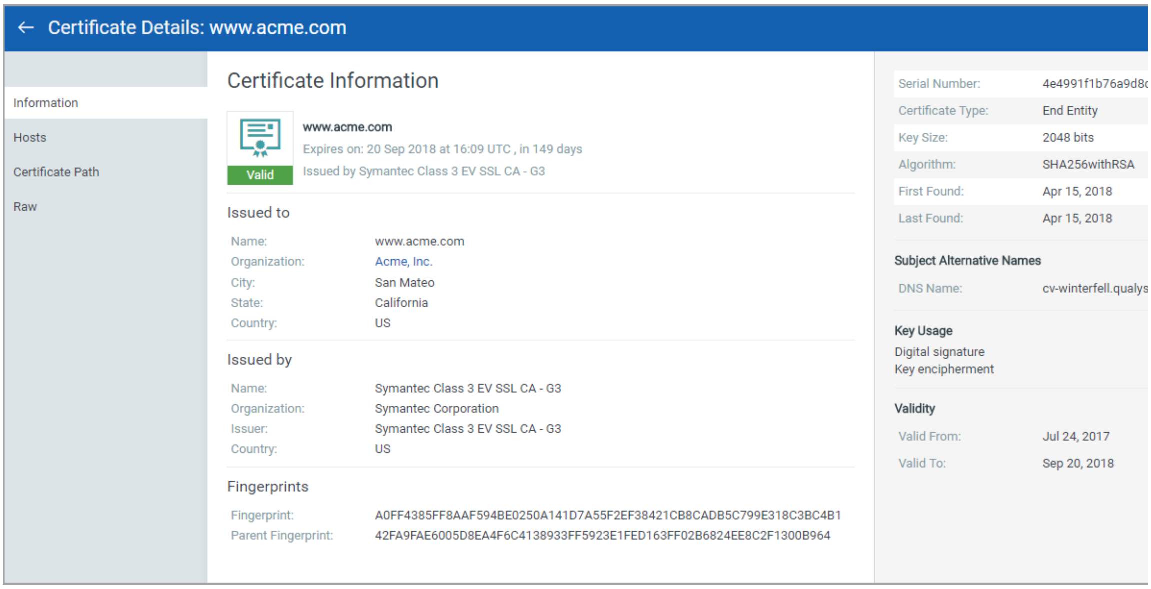
View Certificate Details

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.

How are grades calculated?

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



Certificate Information

Valid

www.acme.com
Expires on: 20 Sep 2018 at 16:09 UTC , in 149 days
Issued by Symantec Class 3 EV SSL CA - G3

Issued to

Name:	www.acme.com
Organization:	Acme, Inc.
City:	San Mateo
State:	California
Country:	US

Issued by

Name:	Symantec Class 3 EV SSL CA - G3
Organization:	Symantec Corporation
Issuer:	Symantec Class 3 EV SSL CA - G3
Country:	US

Fingerprints

Fingerprint:	A0FF4385FF8AAF594BE0250A141D7A55F2EF38421CB8CADB5C799E318C3BC4B1
Parent Fingerprint:	42FA9FAE6005D8EA4F6C4138933FF5923E1FED163FF02B6824EE8C2F1300B964

Serial Number:	4e4991f1b76a9d8
Certificate Type:	End Entity
Key Size:	2048 bits
Algorithm:	SHA256withRSA
First Found:	Apr 15, 2018
Last Found:	Apr 15, 2018

Subject Alternative Names

DNS Name:	cv-winterfell.qualys

Key Usage
Digital signature
Key encipherment

Validity

Valid From:	Jul 24, 2017
Valid To:	Sep 20, 2018

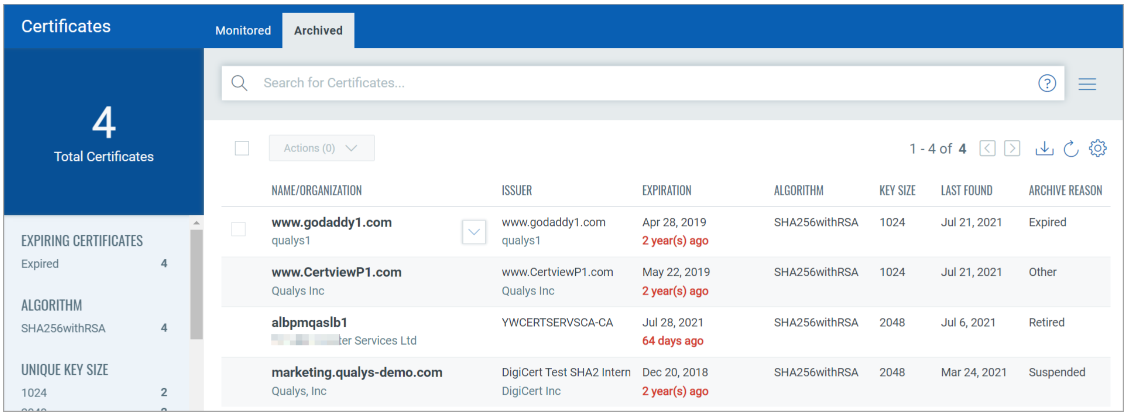
Archived Certificates

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 desired 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.



EXPIRING CERTIFICATES	
Expired	4
ALGORITHM	
SHA256withRSA	4
UNIQUE KEY SIZE	
1024	2

NAME/ORGANIZATION	ISSUER	EXPIRATION	ALGORITHM	KEY SIZE	LAST FOUND	ARCHIVE REASON
www.godaddy1.com qualys1	www.godaddy1.com qualys1	Apr 28, 2019 2 year(s) ago	SHA256withRSA	1024	Jul 21, 2021	Expired
www.CertviewP1.com Qualys Inc	www.CertviewP1.com Qualys Inc	May 22, 2019 2 year(s) ago	SHA256withRSA	1024	Jul 21, 2021	Other
albpmqaslb1 [redacted]ler Services Ltd	YWCERTSERVSCA-CA	Jul 28, 2021 64 days ago	SHA256withRSA	2048	Jul 6, 2021	Retired
marketing.qualys-demo.com Qualys, Inc	DigiCert Test SHA2 Intern DigiCert Inc	Dec 20, 2018 2 year(s) ago	SHA256withRSA	2048	Mar 24, 2021	Suspended

Enroll or Renew Your Certificates

If your Certificate Authority is DigiCert we can help enroll or renew your certificates.

To enroll for certificates you must have one of these permissions: Certview PKI Administrator, Certview Approver, Certview Requestor

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.

Enroll for a certificate

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.

Renew a certificate

You can renew your certificates that are about to expire. We will help you send a renewal request to DigiCert.

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

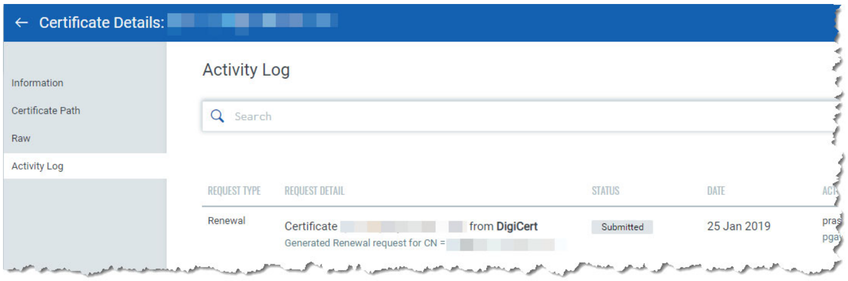
All existing information about the certificate is pre-filled in the wizard. Make sure you provide the accurate Order Id. In case the order id is incorrect, DigiCert rejects the renewal request.

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.

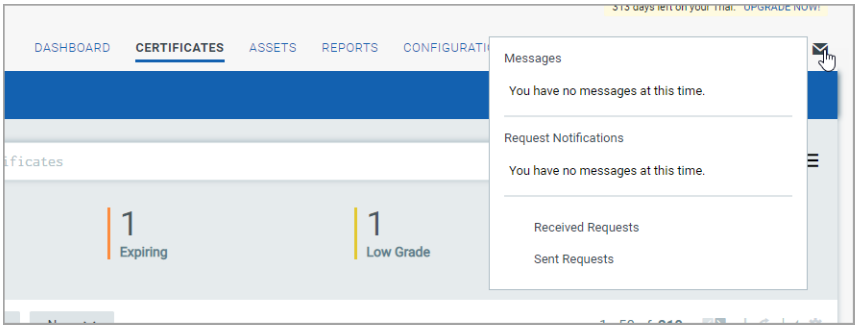
Choose the certificate you have sent for renewal from the Monitored tab and from Quick Actions menu select View Details. Navigate to the Activity Log tab to view progress and status of the renewal request.



REQUEST TYPE	REQUEST DETAIL	STATUS	DATE	ACT
Renewal	Certificate [redacted] from DigiCert Generated Renewal request for CN = [redacted]	Submitted	25 Jan 2019	pras pga

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.



You have no messages at this time.

You have no messages at this time.

Import Leaf Certificates

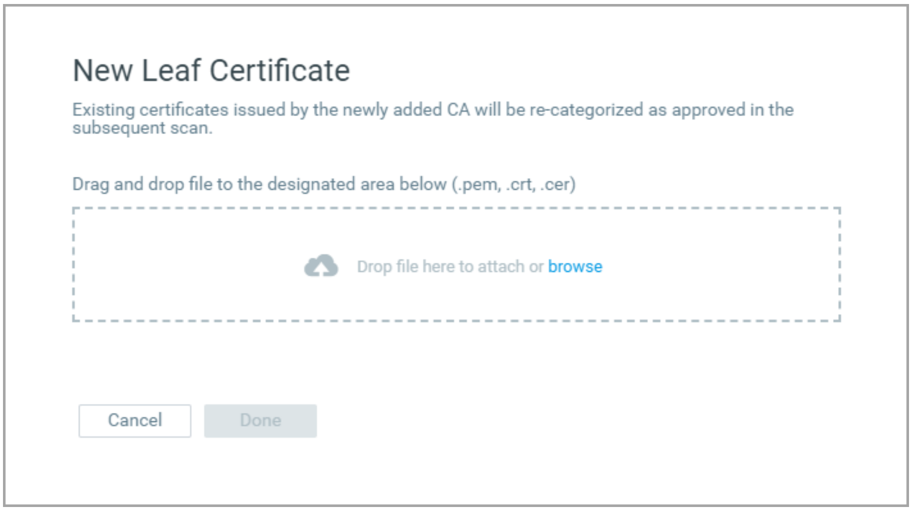
You can import end-entity or leaf certificates in your account. These non-CA certificates are listed as unapproved certificates. If new CAs are added then on subsequent scans these certificates will be re-categorized as approved certificates.

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 will be 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.



New Leaf Certificate

Existing certificates issued by the newly added CA will be re-categorized as approved in the subsequent scan.

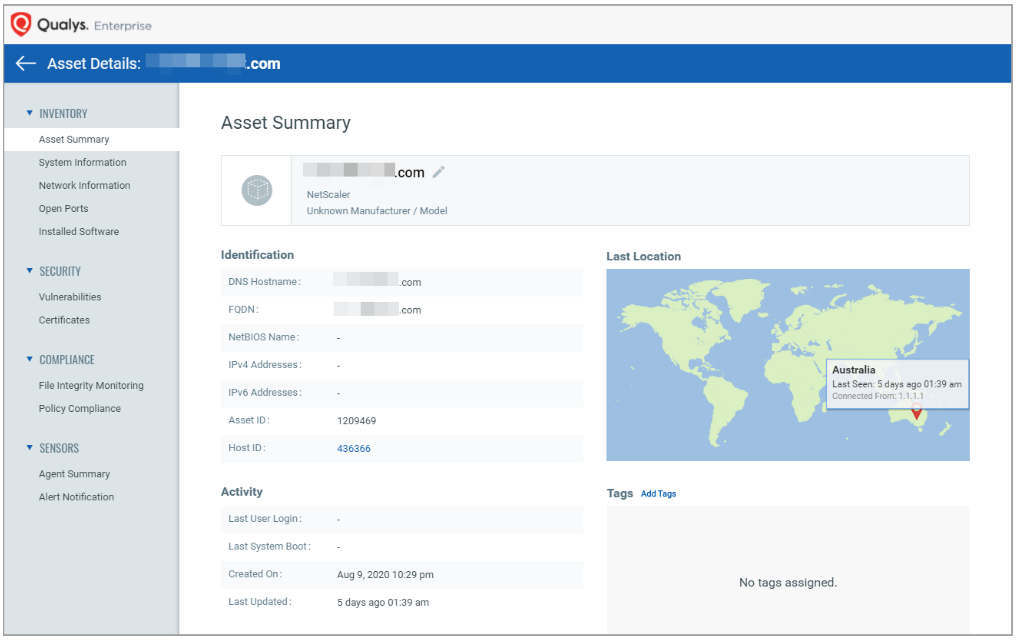
Drag and drop file to the designated area below (.pem, .crt, .cer)

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 desired asset.



Asset Details: [redacted].com

Asset Summary

[redacted].com
NetScaler
Unknown Manufacturer / Model

Identification

DNS Hostname :	[redacted].com
FQDN :	[redacted].com
NetBIOS Name :	-
IPv4 Addresses :	-
IPv6 Addresses :	-
Asset ID :	1209469
Host ID :	436366

Last Location

Australia
Last Seen: 5 days ago 01:39 am
Connected From: 1.1.1.1

Activity

Last User Login :	-
Last System Boot :	-
Created On :	Aug 9, 2020 10:29 pm
Last Updated :	5 days ago 01:39 am

Tags

No tags assigned.

How are grades calculated?

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)

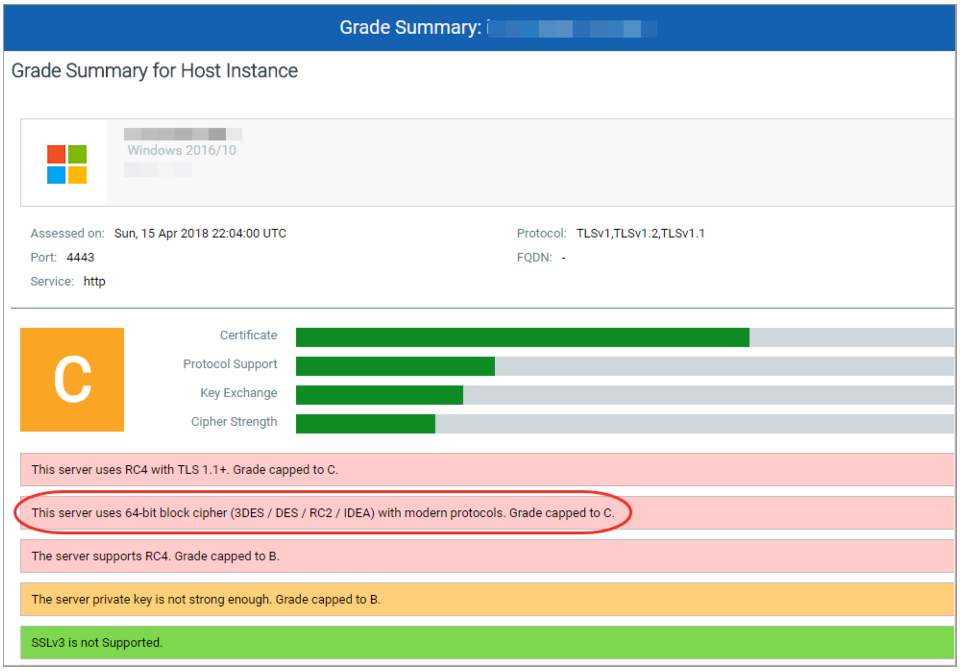
- SSL Labs runs browser simulation checks and may not penalize the server for using weaker ciphers if the browser simulations determine that the weaker ciphers are not negotiated when establishing the SSL connections. You may therefore see different grades in CertView for the following:

  - 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.



Grade Summary: [redacted]

Grade Summary for Host Instance

[redacted]
Windows 2016/10
[redacted]

Assessed on: Sun, 15 Apr 2018 22:04:00 UTC
Port: 4443
Service: http

Protocol: TLSv1,TLSv1.2,TLSv1.1
FQDN: -

This server uses RC4 with TLS 1.1+. Grade capped to C.

This server uses 64-bit block cipher (3DES / DES / RC2 / IDEA) with modern protocols. Grade capped to C.

The server supports RC4. Grade capped to B.

The server private key is not strong enough. Grade capped to B.

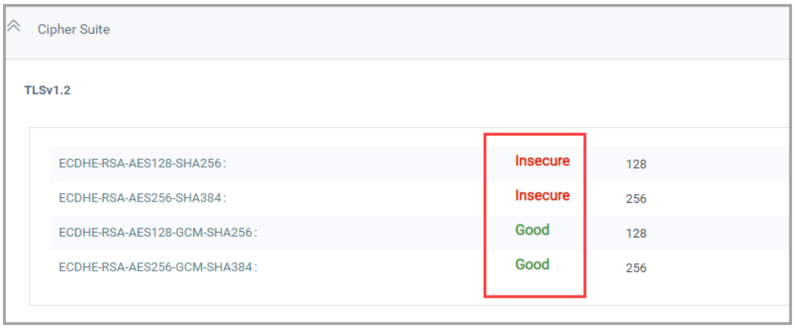
SSLv3 is not Supported.

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.



Cipher Suite

TLSv1.2

ECDHE-RSA-AES128-SHA256 :	Insecure	128
ECDHE-RSA-AES256-SHA384 :	Insecure	256
ECDHE-RSA-AES128-GCM-SHA256 :	Good	128
ECDHE-RSA-AES256-GCM-SHA384 :	Good	256

Rule-based Alerts

You can set up rules to alert you and keep you aware of certificate or TLS related vulnerabilities and allow for quick remediation. Instead of having to actively monitor the system, these alerts ask for attention and intervention only when necessary, and make you aware of changes or significant findings as soon as the rules are met.

For example, you can set up alerts for:

- Certificates expiring in 30/60/90 days

- Self-signed certificates

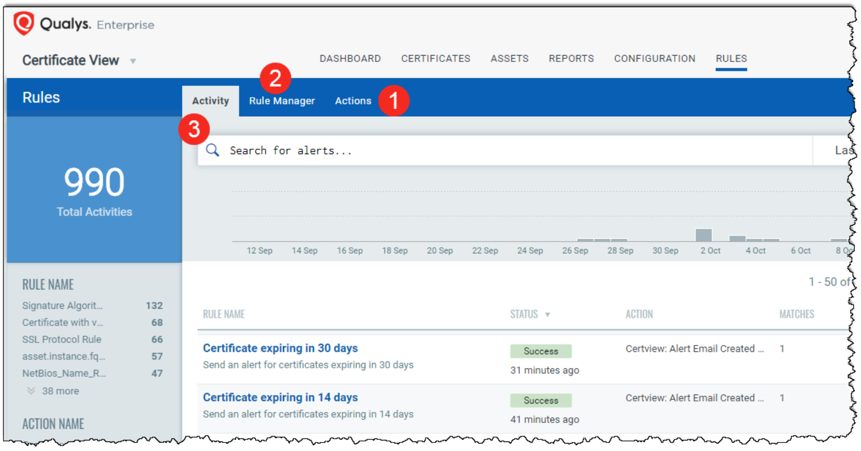
- Certificates from unapproved CAs

- 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.



RULE NAME	
Signature Algorit...	132
Certificate with v...	68
SSL Protocol Rule	66
asset.instance.fq...	57
NetBios_Name_R...	47

RULE NAME	STATUS	ACTION	MATCHES
Certificate expiring in 30 days Send an alert for certificates expiring in 30 days	Success 31 minutes ago	Certview: Alert Email Created ...	1
Certificate expiring in 14 days Send an alert for certificates expiring in 14 days	Success 41 minutes ago	Certview: Alert Email Created ...	1

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

That's it! 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

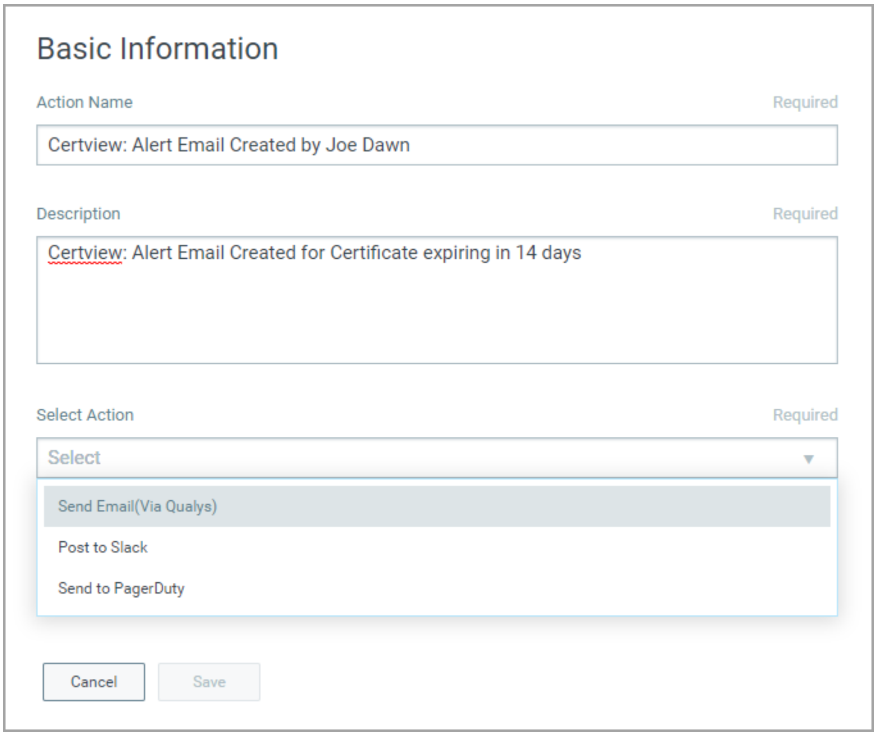
Navigate to Rules > Actions > New Action and provide details to create a new action:

- 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 drop-down 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.



Basic Information

Action Name Required

Certview: Alert Email Created by Joe Dawn

Description Required

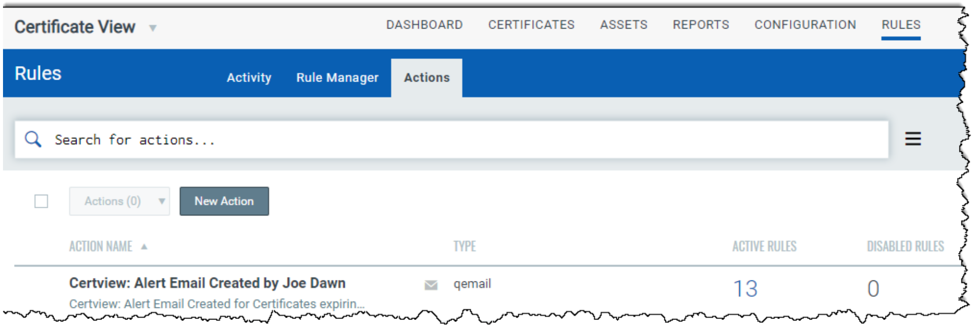
Certview: Alert Email Created for Certificate expiring in 14 days

Select Action Required

Select

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.

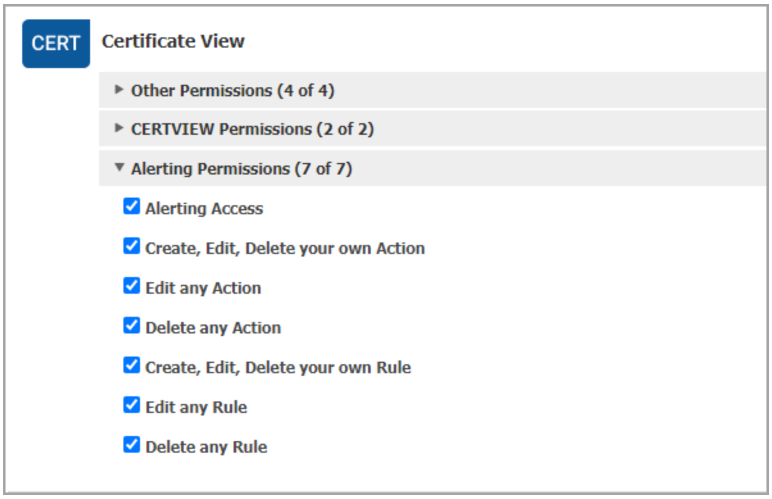


ACTION NAME	TYPE	ACTIVE RULES	DISABLED RULES
Certview: Alert Email Created by Joe Dawn Certview: Alert Email Created for Certificates expirin...	qemail	13	0

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.



CERT Certificate View

▸ Other Permissions (4 of 4)

▸ CERTVIEW Permissions (2 of 2)

▾ Alerting Permissions (7 of 7)

☑ Alerting Access

☑ Create, Edit, Delete your own Action

☑ Edit any Action

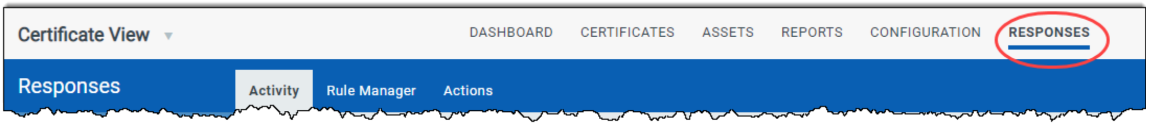
☑ Delete any Action

☑ Create, Edit, Delete your own Rule

☑ Edit any Rule

☑ Delete any Rule

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



Create and Manage Rules

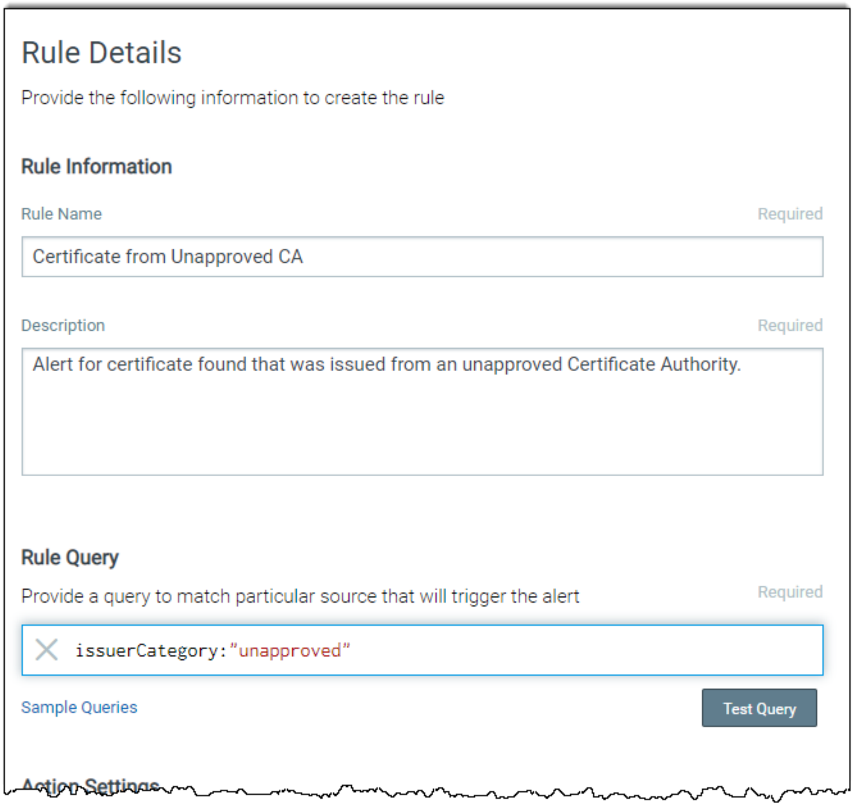
Define the conditions, significant finding or event that should trigger the rules and send you alerts.

Create a rule

Navigate to Rules > 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 button to test your query. Click Sample Queries to select from predefined queries.



Rule Details

Provide the following information to create the rule

Rule Information

Rule Name — Required

Certificate from Unapproved CA

Description — Required

Alert for certificate found that was issued from an unapproved Certificate Authority.

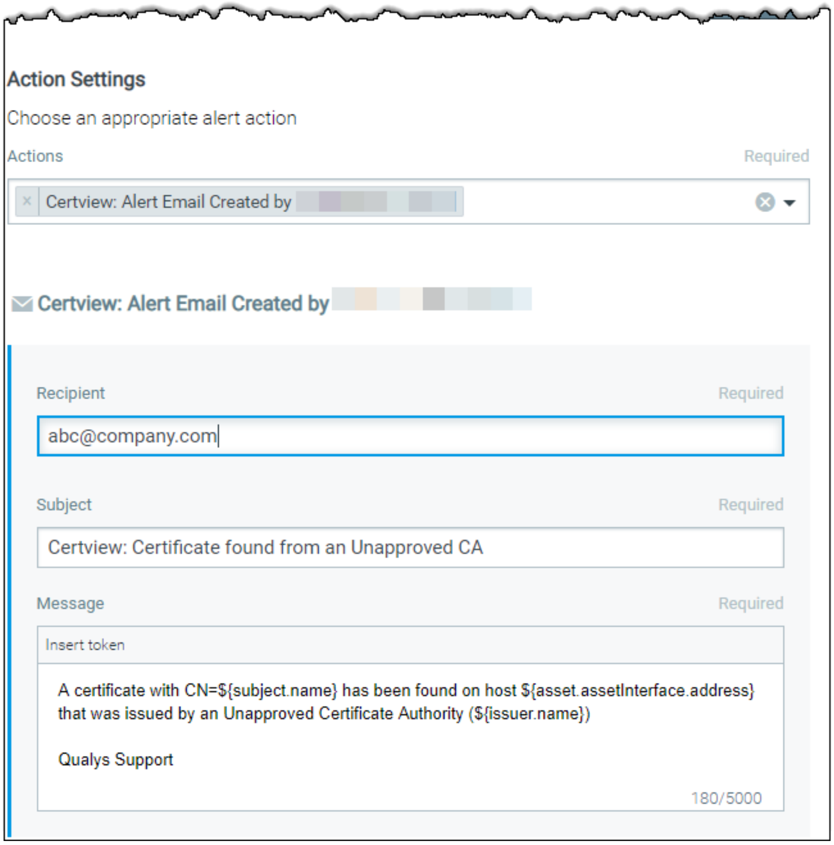
Rule Query

Provide a query to match particular source that will trigger the alert — Required

```
issuerCategory:"unapproved"
```

- 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: Currently, the "validTo" and "ValidFrom" tokens in the alert message display the date as a number (UNIX Epoch time). In order to view the date in a legible format in your alert email, you can manually change the tokens "validTo" to "validToDate" and "validFrom" to "validFromDate" when you compose your alert message.



Action Settings

Choose an appropriate alert action

Actions — Required

× Certview: Alert Email Created by [redacted]

Certview: Alert Email Created by [redacted]

Recipient — Required

abc@company.com

Subject — Required

Certview: Certificate found from an Unapproved CA

Message — Required

Insert token

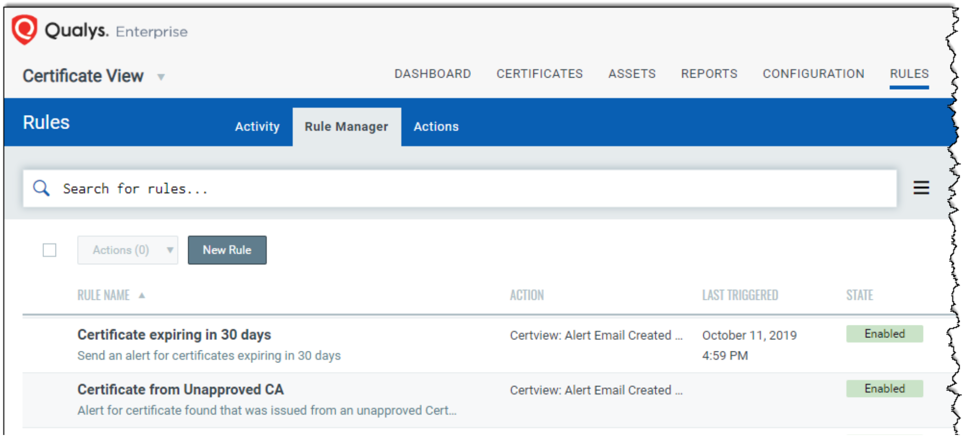
A certificate with CN=${subject.name} has been found on host ${asset.assetInterface.address} that was issued by an Unapproved Certificate Authority (${issuer.name})

Qualys Support

180/5000

Manage rules

View all the rules created in the Rule Manager 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.

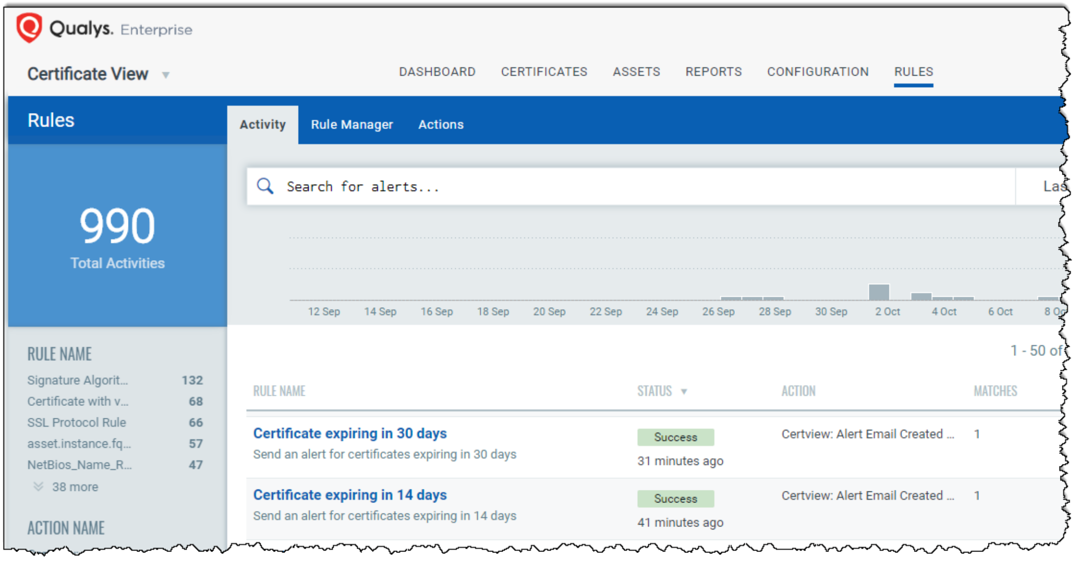


RULE NAME	ACTION	LAST TRIGGERED	STATE
Certificate expiring in 30 days Send an alert for certificates expiring in 30 days	Certview: Alert Email Created ...	October 11, 2019 4:59 PM	Enabled
Certificate from Unapproved CA Alert for certificate found that was issued from an unapproved Cert...	Certview: Alert Email Created ...		Enabled

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.



RULE NAME	
Signature Algorit...	132
Certificate with v...	68
SSL Protocol Rule	66
asset.instance.fq...	57
NetBios_Name_R...	47

38 more

ACTION NAME

RULE NAME	STATUS	ACTION	MATCHES
Certificate expiring in 30 days Send an alert for certificates expiring in 30 days	Success 31 minutes ago	Certview: Alert Email Created ...	1
Certificate expiring in 14 days Send an alert for certificates expiring in 14 days	Success 41 minutes ago	Certview: Alert Email Created ...	1

Create Reports in Certificate View

Create reports to generate on-demand or scheduled reports that can be used to alert you on the security posture of both certificates and assets in your network that need immediate attention or remediation actions. Currently you can download a report only in CSV format.

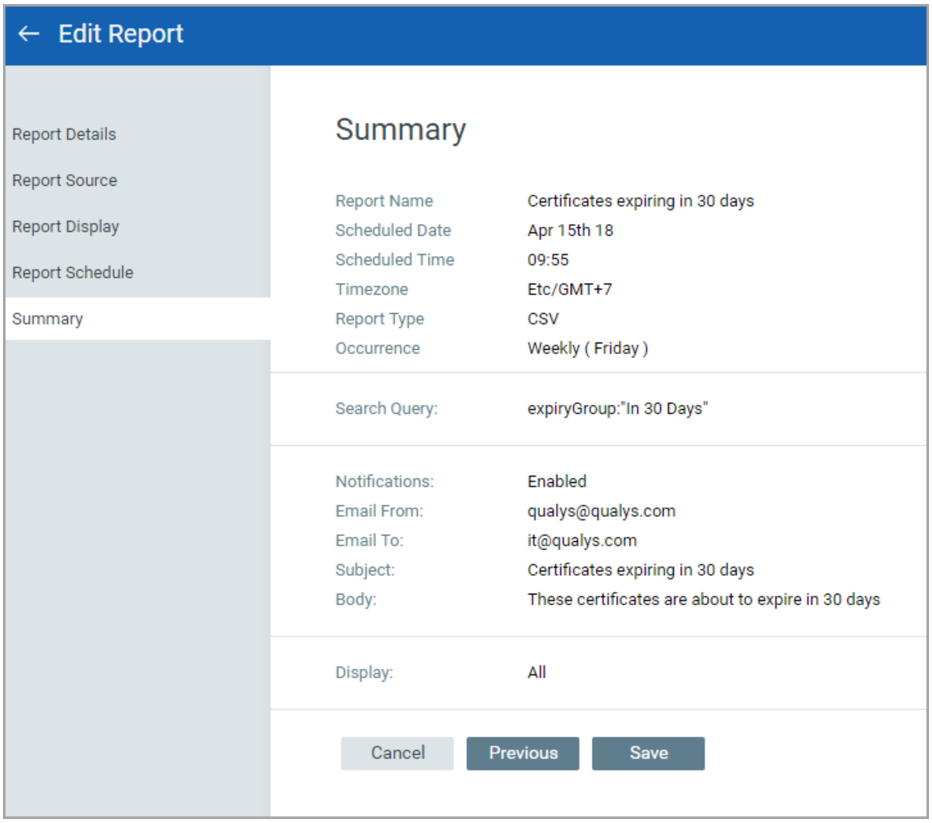
Create a report

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

For example, you want to be alerted about all certificates expiring in the next 30 days.

In the Create Report wizard define assets and tags you want to report on, choose the information you want to display, schedule the report as desired and run the report.

Note: If you want to create a report for more than 10000 certificates, use scheduled reports.



Summary

Report Name	Certificates expiring in 30 days
Scheduled Date	Apr 15th 18
Scheduled Time	09:55
Timezone	Etc/GMT+7
Report Type	CSV
Occurrence	Weekly (Friday)
Search Query:	expiryGroup:"In 30 Days"
Notifications:	Enabled
Email From:	qualys@qualys.com
Email To:	it@qualys.com
Subject:	Certificates expiring in 30 days
Body:	These certificates are about to expire in 30 days
Display:	All

Certificate Dashboards

To visualize your certificate posture across your assets, simply use our Unified Dashboard. We provide you with a default dashboard 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

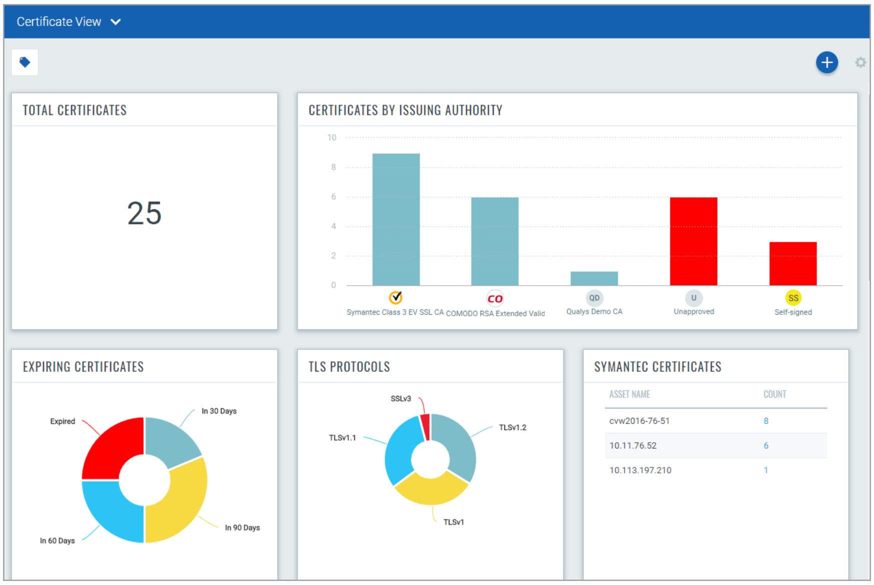
-Capability to pull information from all Qualys applications

-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.



ASSET NAME	COUNT
cvw2016-76-51	8
10.11.76.52	6
10.113.197.210	1

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.