Qualys Certificate View

User Guide

March 4, 2019

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

Qualys AssetView 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.

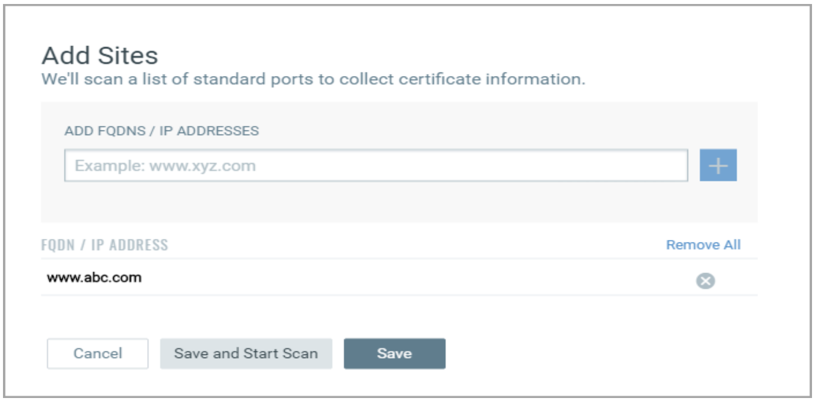
If you have a Certificate View Free subscription then you can add only external sites. To add and monitor internal sites simply upgrade to Certificate View Full subscription.

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.

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

www.abc.com

Add Internal Sites

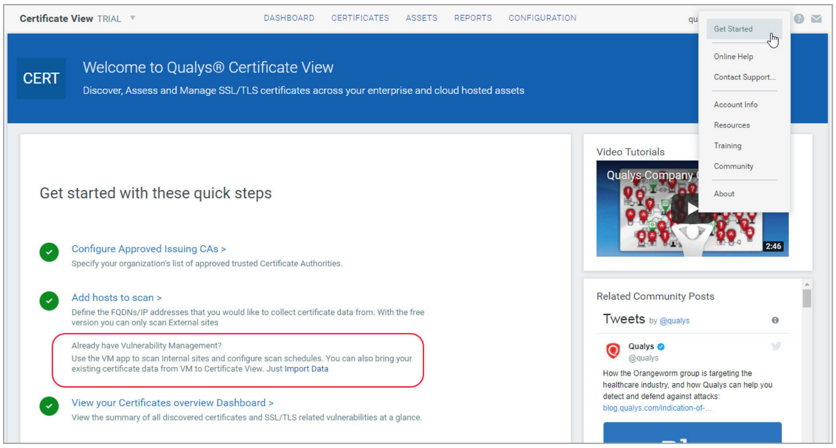
You can monitor FQDNs and IP addresses of internal sites if you have the Certificate View Full subscription.

To add Assets from VM, go to VM > 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.

Import Data

You can import certificate data for your assets from VM as a one time activity if you are an existing VM user.

Go to the Get Started page and click Import Data. Select IPs and asset tags, define the time frame for which you want the data and click Import.



Welcome to Qualys® Certificate View

Discover, Assess and Manage SSL/TLS certificates across your enterprise and cloud hosted assets

Get started with these quick steps

✓ Configure Approved Issuing CAs >
Specify your organization's list of approved trusted Certificate Authorities.

✓ Add hosts to scan >
Define the FQDNs/IP addresses that you would like to collect certificate data from. With the free version you can only scan External sites

Already have Vulnerability Management?
Use the VM app to scan Internal sites and configure scan schedules. You can also bring your existing certificate data from VM to Certificate View. Just Import Data

✓ View your Certificates overview Dashboard >
View the summary of all discovered certificates and SSL/TLS related vulnerabilities at a glance.

How the Orangeworm group is targeting the healthcare industry, and how Qualys can help you detect and defend against attacks: blog.qualys.com/indication-of-...

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

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

Simply go to VM > 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 Certificate View online help.

Tip - To know more about running and scheduling CertView scans from VM, go to VM > Scans > Scans and look up CertView scans in 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 that CertView scan option in VM will be visible only if CertView is turned on in your subscription.

Certificate View helps you

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

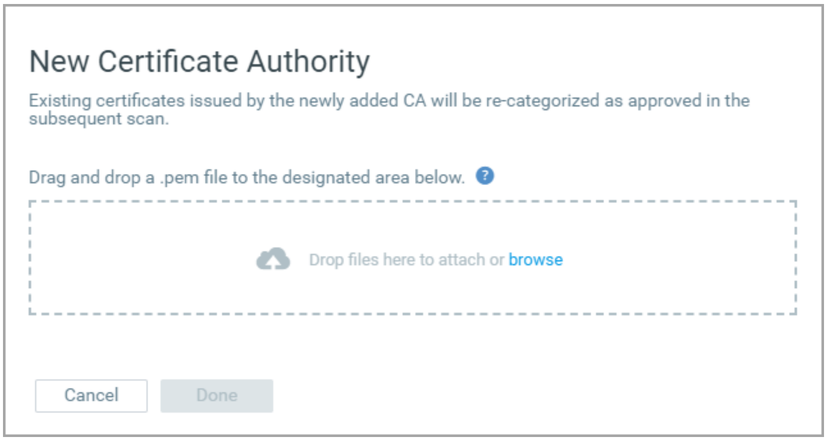
- Vulnerability analysis and grading makes all relevant info available to you (host/port/service/certificate)

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.

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.

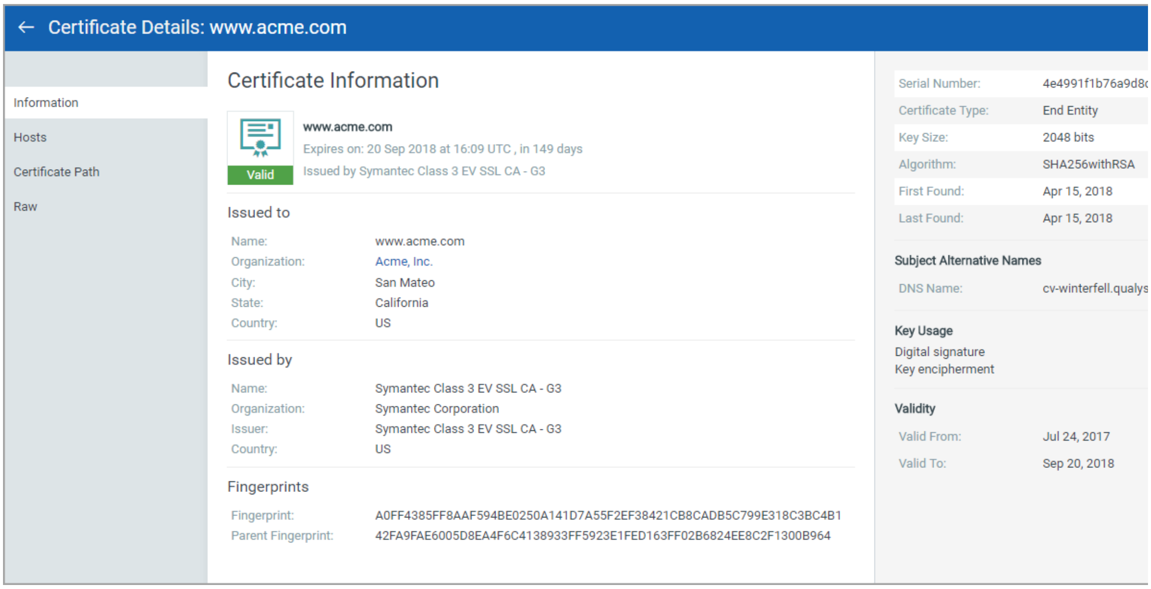
View Certificate details

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 Details: www.acme.com

Certificate Information

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.

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 Vulnerability Management 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 have you get the associated set of permissions.

- Certview PKI Administrator

- Certview Approver

- Certview Requester

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.

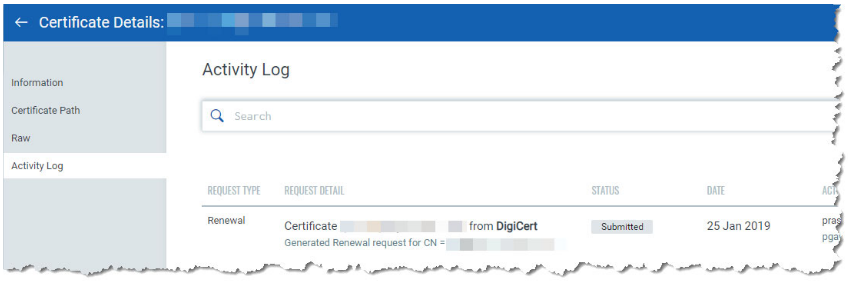
All existing information about the certificate is pre-filled in the wizard. Make sure you provide the accurate Order Id. In case the order id is incorrect, DigiCert rejects the renewal request.

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.



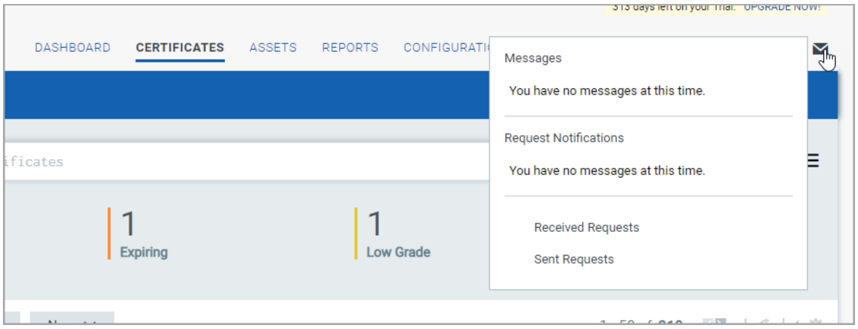
Certificate Details: [redacted]

Activity Log

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

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.



Messages

You have no messages at this time.

Request Notifications

You have no messages at this time.

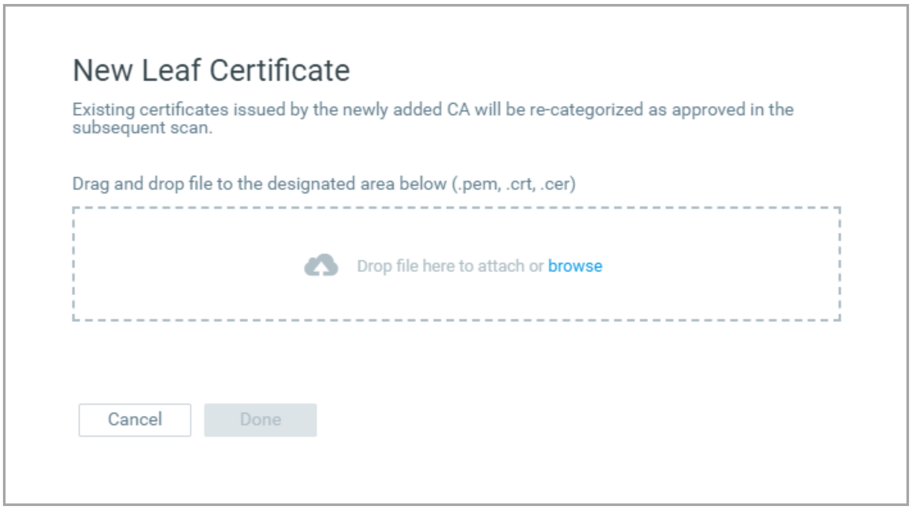
Import Leaf Certificates

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.



New Leaf Certificate

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

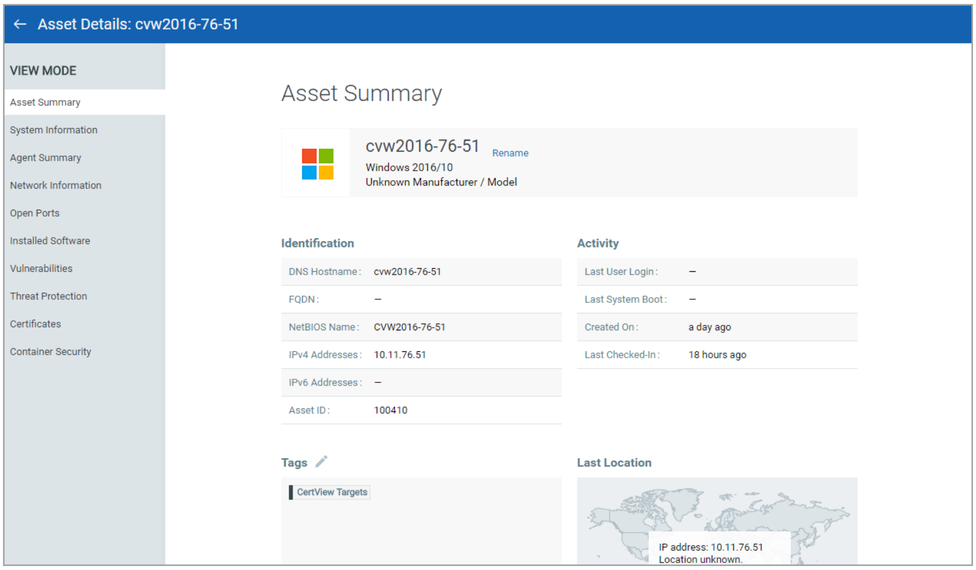
Drag and drop file to the designated area below (.pem, .crt, .cer)

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 Summary

cvw2016-76-51
Windows 2016/10
Unknown Manufacturer / Model

Identification

DNS Hostname :	cvw2016-76-51
FQDN :	–
NetBIOS Name :	CVW2016-76-51
IPv4 Addresses :	10.11.76.51
IPv6 Addresses :	–
Asset ID :	100410

Activity

Last User Login :	–
Last System Boot :	–
Created On :	a day ago
Last Checked-In :	18 hours ago

Tags

CertView Targets

Last Location

IP address: 10.11.76.51
Location unknown.

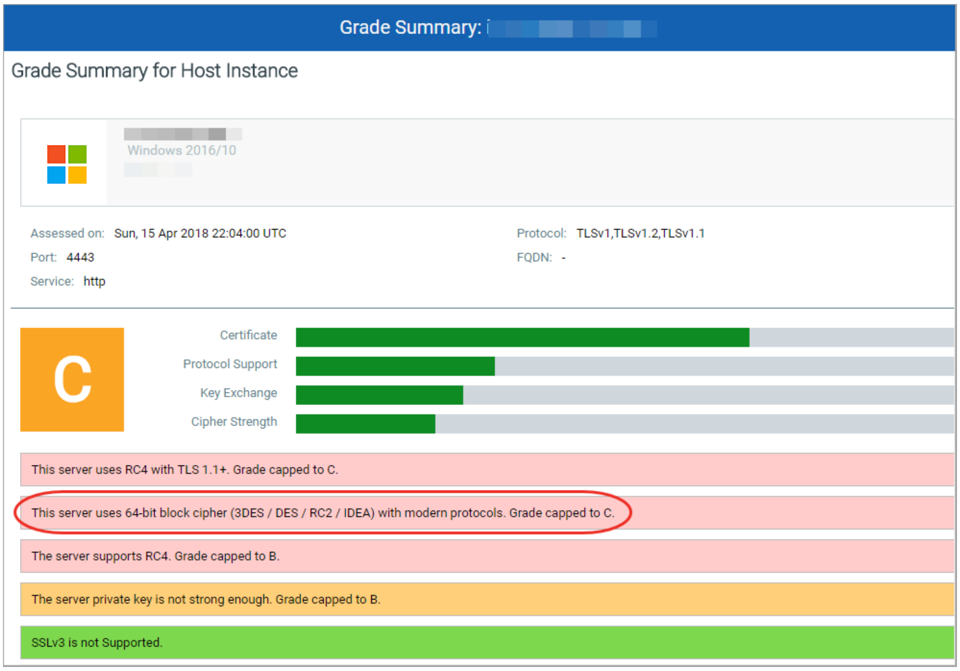
How are grades calculated?

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:

- SSL Labs assigns a zero score to the certificate inspection portion if there is a domain name mismatch or the certificate is revoked. Certificate View does not assign a zero score for these criteria. However, the certificate score does not affect the overall grade.
- Both SSL Labs and CertView detect the use of legacy 64-bit block ciphers. However, SSL Labs lowers the severity of this vulnerability if it detects that these legacy ciphers are only used with older browsers. Where as Certificate View considers it to be a confirmed Severity 3 vulnerability (regardless of the browser used) and caps the grade to C.



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.

Create Reports

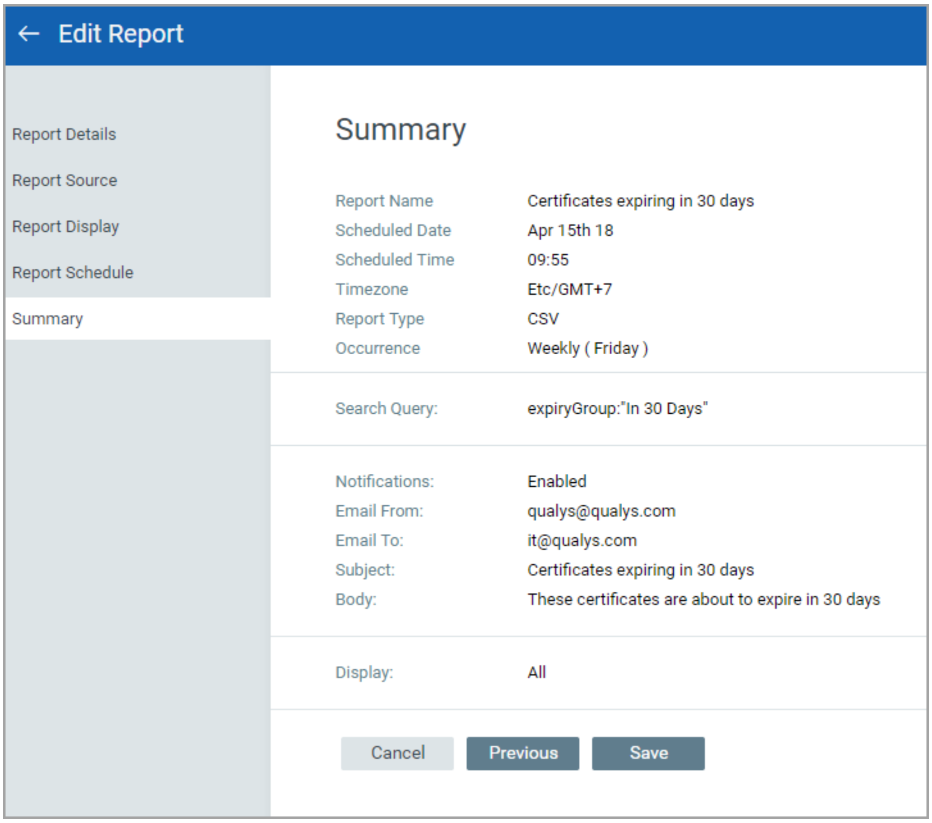
Create reports to generate on-demand or scheduled reports that can be used to alert you on the security posture of both certificates and assets in your network that need immediate attention or remediation actions. Currently you can download a report only in CSV format.

To 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.



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

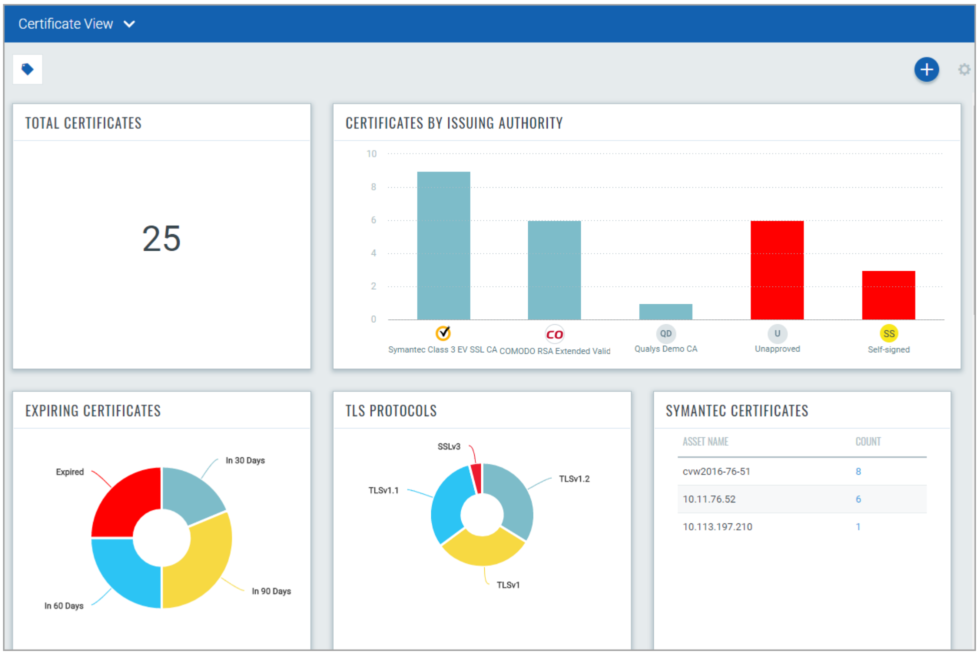
To visualize your certificate posture across your assets, simply use our dynamic Dashboard. We provide you with a default dashboard to get you started, however you can create a custom dashboard to customize the way you view your information.

Add widgets with search queries to see exactly what you're interested in. You can also export and import Dashboard and Widget configurations.

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

Add new widgets

1) Start by clicking the Add Widget button on your dashboard.

2) Pick one of our widget templates - there are many to choose from - or create your own.

3) Each widget is unique. You'll enter a query for the data to display in the widget and the layout - count, table,column, pie chart.

4) When you're ready, click Add to Dashboard.

Tip - Wondering how we created the widgets on the default dashboard? Choose Edit for any widget to see the settings.

Import/Export widgets

You can import and export widget configurations to a file in a json format, allowing you to share the widgets between accounts or within the Qualys community.

To Import a widget, choose Import Widget from the tools menu. Browse to your json file and click Import.

To export a widget, choose Export this Widget from the widget menu. Give your file a name, choose whether to hide sensitive information, and click Export.

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.