Qualys Certificate View
User Guide

September 16, 2020
# Table of Contents

**About this Guide** .................................................................................................................. 4  
  - About Qualys .................................................................................................................. 4  
  - Qualys Support ............................................................................................................ 4  

**Get Started** ..................................................................................................................... 5  
  - What assets are included? .............................................................................................. 5  
  - Run Scans to Discover Certificates ............................................................................. 7  

**View Certificates** ............................................................................................................. 8  
  - Configure Certificate Authorities ................................................................................ 8  
  - Add a DigiCert API Key ................................................................................................. 8  
  - View Certificate details ............................................................................................... 10  
  - Enroll or Renew your Certificates ............................................................................. 10  
  - Import Leaf Certificates .............................................................................................. 12  
  - View Asset Details ....................................................................................................... 14  
  - How are grades calculated? ......................................................................................... 15  

**Rule-based Alerts** ......................................................................................................... 16  
  - Configure rule-based alerts ....................................................................................... 16  

**Create Reports** .............................................................................................................. 22  
  - Create a report ............................................................................................................. 22  

**Certificate Dashboards** ................................................................................................... 23  
  - Add new widgets .......................................................................................................... 23  
  - Import/Export widgets ................................................................................................. 24  
  - Refresh your view ........................................................................................................ 24
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 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.
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.

**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.

**Import Data**

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

It is recommended that you choose relevant assets to import certificate data (only leaf certificates are imported). An asset’s certificates are imported only once and will not be imported again even if the asset is included in a subsequent target list.

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.
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 Certificate View online help.

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.
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/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.

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.
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.

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 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.

- 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.

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.

**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 will be listed in the certificates list of the Monitored 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 desired asset.
How are grades calculated?

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

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.
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.

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.
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.
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.

- 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.
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.
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

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.
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.

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.