



# Qualys Certificate View

## Release Notes

Version 2.4.0.0

October 18, 2019

Here's what's new in Certificate View!

[Configure Rule-based Alerts](#)

Qualys Certificate View 2.4 brings you many more Improvements and updates! [Learn more](#)

## Configure 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

### How to set up 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.

The screenshot shows the Qualys Certificate View interface under the 'RULES' tab. A search bar at the top has 'Search for alerts...' and a date range from '12 Sep' to '8 Oct'. Three numbered circles point to specific elements: circle 1 points to the 'Actions' tab, circle 2 points to the 'Rule Manager' tab, and circle 3 points to the search bar. Below the search bar, there's a table with two rows of alert rules:

RULE NAME	STATUS	ACTION	MATCHES
Certificate expiring in 30 days	Success	Certview: Alert Email Created ...	1
Certificate expiring in 14 days	Success	Certview: Alert Email Created ...	1

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

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

##### To create an action:

Navigate to Rules > Actions > New Action and provide details required 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 PagerDuty 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.
  - 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.

View and manage the newly created actions in the Actions tab with details such as name of the action, type of the action, etc.

**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 Send Email(Via Qualys) Post to Slack Send to PagerDuty	
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

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

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

### To 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

<input checked="" type="checkbox"/> issuerCategory: "unapproved"
--

[Sample Queries](#) [Test Query](#)

[Action Settings](#)

- 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.

### Action Settings

Choose an appropriate alert action

Actions	Required
<input checked="" type="checkbox"/> Certview: Alert Email Created by	<input type="button" value="x"/>
<input checked="" type="checkbox"/> Certview: Alert Email Created by	
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	

**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.

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

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.

The screenshot shows the Qualys Certificate View interface. The top navigation bar includes links for DASHBOARD, CERTIFICATES, ASSETS, REPORTS, CONFIGURATION, and RULES. The RULES link is underlined, indicating it is the active tab. Below the navigation is a search bar with the placeholder "Search for alerts...". A timeline at the bottom shows dates from 12 Sep to 8 Oct, with a bar for 2 Oct highlighted. To the left, a sidebar displays "990 Total Activities" and lists rule names and their counts: Signature Algorithm (132), Certificate with v... (68), SSL Protocol Rule (66), asset.instance.fq... (57), NetBios\_Name\_R... (47), and a link to "38 more". The main content area shows two rows of alert details:

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

That's it! You are all set to start being alerted about your certificate findings!

## Issues addressed in this release

- A new input parameter “certificateDetails” is now added to the List CertView Certificates API. Using this parameter, you can define the level of certificate attributes you want to list. Default value **basic** is used to fetch commonly used attributes. Use value **extended** to fetch these additional attributes: Serial number, Auth Key Identifier, Subject Key Identifier, Key Usage, Base64 certificate, Enhanced Key Usage
- We have fixed an issue with search tokens and now the filter tokens used with NOT operator return correct results.