



Qualys Certificate View

Release Notes

Version 3.3

January 02, 2024

What's New?

[Permission for Deleting Assets and External Sites](#)

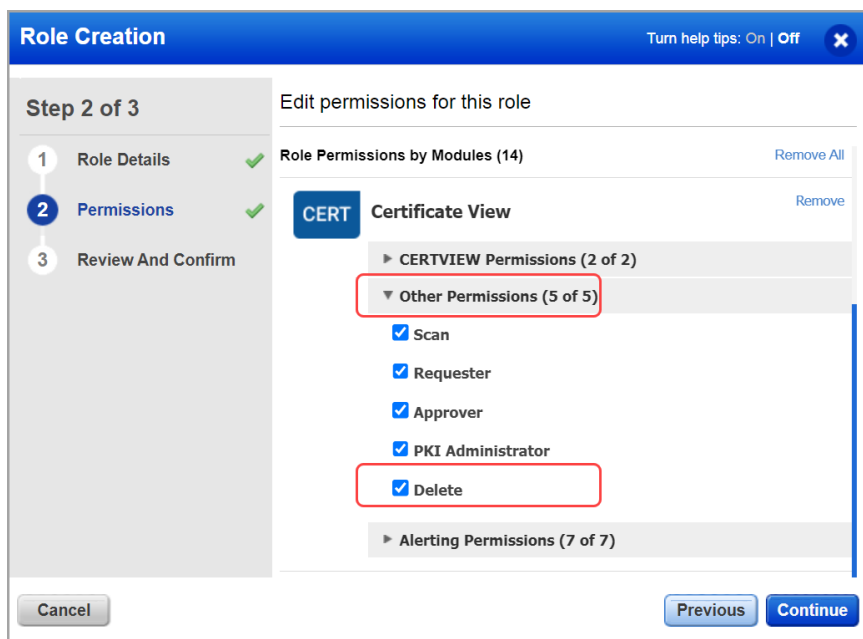
[Addition of Cipher Suites Column in Reports](#)

Qualys Certificate View 3.3 brings you many more improvements and updates! [Learn more](#)

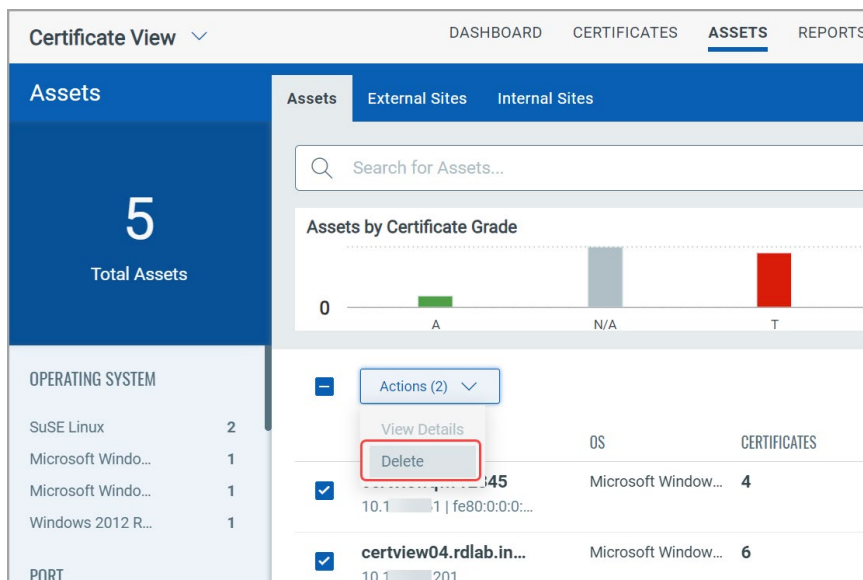
Permission for Deleting Assets and External Sites

With this release, we have added permission to delete assets and external sites in Certificate View. With this permission, the Manager user can assign role-based access for deletion of assets and external sites.

You can assign the Delete permission to an existing user role or to a new user role. To assign the Delete permission, navigate to the **Administration** application from the application selector > **Role Management**. Select the **Delete** permission from **Other Permissions**, as shown in the following image.



The **Delete** option is available in the **Assets** and **External Sites** tabs. For example, refer to the Delete option shown in the following image.



Addition of Cipher Suites Column in Reports

With this release, you can include the Cipher Suites details in the certificate report. To add the Cipher Suites of the certificates in reports, select the **Cipher Suites** check box from the **Report Display** section while creating or editing the reports.

The screenshot shows the 'Edit Report' dialog box with the 'Report Display' section selected. Under 'Columns', the 'Cipher Suites' checkbox is checked and highlighted with a red box. Other checked boxes include Certificate Name, Organization, Issuer, Valid from, Valid to, Number of Instances, Asset Name, Port, Reason For Grade, Serial Number, Algorithm, Key Length, Days till expiration, Number of Hosts, Grades, IP, and Service.

Note: You can view this information for all new reports generated. For old reports, include Cipher Suites information in the reports and run the report again.

A1	Certificate Name																				
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	AC
1	Certificate	Serial Nur	Organizati	Algorithm	Issuer	Key Leng	Valid From	Days Till E	Valid To	Number o	Number o	Grades	Asset Name	IP	Port	Service	Reason For	Cipher Suites			
2	certview05b4409ffc4b8e2974b	SHA1with	certview0	2048	2023-11-2	164	2024-05-2	1	1	T	10.1	201	3389	win_rem	This serve	AES128-SHA,ECDHE-RSA-AES128	S-CBC3-SH				
3	www.cert.00e3efe8r	Qualys, In	SHA256wi	www.cert	1024	2019-08-1	-1554	2019-09-1	1	1	T	10.1	201	636	http	This serve	AES128	S-CBC3-SH			
4	tran.0992a6c49	Qualys, In	SHA256wi	DigiCert G	2048	2023-09-1	274	2024-09-1	1	1	C	www.qualys.com	443	http	This serve	AES128-SHA,AES256-SHA,RC	2048 SHA256				
5	www.qua.0a3869233	Qualys, In	SHA256wi	DigiCert S	2048	2023-10-1	300	2024-10-0	1	1	A	www.qualys.com	443	http	SSLv3 is n	ECDHE-RSA	AES128-SHA,AES256-SHA,RC	2048 SHA256			
6	2k82cp-6i42e8b4925241ac824c	SHA1with	2k82cp-6i	2048	2023-11-1	152	2024-05-1	1	1	T	10.1	135	3389	win_rem	This serve	AES128-SHA,AES256-SHA,RC	2048 SHA256				
7	2k82pva4-113d0fc72ffb3bf4ff	SHA1with	2k82pva4-	2048	2023-08-2	69	2024-02-2	1	1	T	10.1	168	3389	win_rem	This serve	AES1	2048 SHA256				
8	qwki.intr.0e4caefc	Qualys, In	SHA256wi	DigiCert S	2048	2022-09-2	-82	2023-09-2	1	1	B	confluence01.b01.er	443	http	TLS 1.0 Su	AES256-GCM-SHA384,	DHE-RSA-AES128				
9																					

Issues Addressed

- Users encountered an issue where scans initiated on external sites from Certificate View were getting stuck in a Queued state for an extended period of time even though the scans were finished and processed. This issue has now been resolved. We have improved the scan logic, and now the scans reflect the correct status.
- While adding multiple sites using the **Upload Bulk Sites** option, the user received the error: Your FQDN resolve to IPv6 address.
This error occurs because we currently only support IPv4 addresses.
We have improved the error message to include the possible user action as:
Your FQDN resolves to IPv6 address; try adding it with a different FQDN or IP address.
- In some cases, users could see expired certificates in their reports as they were not deleted. We have fixed this issue, and now users do not see expired certificates in their reports.
- Self-assigned certificates were not graded correctly in a few instances. We have improved the grading logic now, and self-signed certificates are graded as T.

- In some cases, if a certificate had multiple assets and instances, the **Certificates** and **Reports** tab displayed inconsistency in the assets and instances count. This inconsistency is resolved with the improved reporting logic.