# Qualys scanner overview

QRadar® can retrieve vulnerability information from the QualysGuard Host Detection List API or download scan reports directly from a QualysGuard appliance. QRadar supports integration with QualysGuard appliances that use software version 4.7 through 7.10.

### Qualys Detection Scanners

Add a Qualys Detection Scanner if you want to use the QualysGuard Host Detection List API to query multiple scan reports to collect vulnerability data for assets. The data that the query returns contains the vulnerabilities as identification numbers, which QRadar compares against the most recent Qualys Vulnerability Knowledge Base. The Qualys Detection Scanner does not support live scans, but enables the Qualys Detection Scanner to retrieve vulnerability information aggregated across multiple scan reports. QRadar supports key search parameters to filter for the information that you want to collect. You can also configure how frequently QRadar retrieves and caches the Qualys Vulnerability Knowledge Base.

### Qualys Scanners

Add a Qualys scanner if you want to import specific live or imported reports that include scan or asset data. When you add a Qualys scanner, you can choose from the following collection types:

- Scheduled live - Scan Report
- Scheduled Import - Asset Data Report
- Scheduled Import - Scan Report

## Adding a Qualys detection scanner

Add a Qualys detection scanner to use an API to query across multiple scan reports to collect vulnerability data for assets. The Qualys detection scanner uses the QualysGuard Host Detection List API.

### Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

### Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.

3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Qualys detection scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Qualys Detection Scanner**.
7. Configure the following parameters:

| Parameter | Description |
|---|---|
| **Qualys Server Host Name** | The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type `qualysapi.qualys.com` or `qualysapi.qualys.eu`. |
| **Qualys Username** | The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation. |
| **Operating System Filter** | The regular expression (regex) to filter the scan data by the operating system. |
| **Asset Group Names** | A comma-separated list to query IP addresses by the asset group name. |
| **Host Scan Time Filter (Days)** | Host scan times that are older than the specified number of days are excluded from the results that Qualys returns. |
| **Qualys Vulnerability Retention Period (Days)** | The number of days that you want QRadar to store the Qualys Vulnerability Knowledge Base. If a scan is scheduled and the retention period expires, the system downloads an update.<br>**Attention:** After you create this scanner for the first time, subsequent updates to this retention period might not take effect. For this change to take effect after the initial creation, you might need to delete or clear the cache. |
| **Force Qualys Vulnerability Update** | Forces the system to update to the Qualys Vulnerability Knowledge Base for each scheduled scan. |

8. Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
9. Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
10. Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.

    **Restriction:** The QualysGuard Host Detection List API accepts only CIDR ranges to a maximum of a single class A or /8 and does not accept the local host IP address (127.0.0.1).

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**. Changes to the proxy configuration require a **Deploy Full Configuration**.

## Adding a Qualys scheduled live scan

Add a scheduled live scan to start preconfigured scans on the Qualys Scanner and then collect the completed scan results.

### Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

### Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Qualys scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Qualys Scanner**.
7. Configure the following parameters:

| Parameter | Description |
|---|---|
| **Qualys Server Host Name** | The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type `qualysapi.qualys.com` or `qualysapi.qualys.eu`. |
| **Qualys Username** | The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation. |

8. Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
9. Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
10. From the **Collection Type** list, select **Scheduled Live - Scan Report**.
11. Configure the following parameters:

| Parameter | Description |
|---|---|
| **Scanner Name** | To obtain the scanner name, contact your network administrator. Public scanning appliance must clear the name from this field. |
| **Option Profiles** | The name of the option profile that determines which live scan is started. Live scans support only one option profile name for each scanner configuration. |

12. Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.
13. Click **Save**.
14. On the **Admin** tab, click **Deploy Changes**. Changes to the proxy configuration require a **Deploy Full Configuration**.

## Adding a Qualys scheduled import asset data report

Add an asset report data import to schedule QRadar to retrieve a single asset report from your Qualys scanner.

### Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

### Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Qualys scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Qualys Scanner**.
7. Configure the following parameters:

| Parameter | Description |
|---|---|
| **Qualys Server Host Name** | The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type `qualysapi.qualys.com` or `qualysapi.qualys.eu`. |

| Parameter | Description |
|---|---|
| **Qualys Username** | The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation. |

8. Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
9. Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
10. From the **Collection Type** list, select **Scheduled Import - Asset Data Report**.
11. Configure the following parameters:

| Parameter | Description |
|---|---|
| **Report Template Title** | The report template title to replace the default asset data report title. |
| **Max Reports Age (Days)** | Files that are older than the specified days and time stamp on the report file are excluded when the schedule scan starts. |
| **Import File** | The directory path to download and import a single asset report from Qualys. If you specify an import file location, QRadar downloads the contents of the asset report from Qualys to a local directory and imports the file. If you leave this field blank or if the file or directory cannot be found, the Qualys scanner uses the API to retrieve the asset report by using the value in the **Report Template Title** field. |

12. Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.
13. Optional: To enable QRadar to create custom vulnerabilities from the live scan data, select the **Enable Custom Vulnerability Creation** check box and select options that you want to include.
14. Click **Save**.
15. On the **Admin** tab, click **Deploy Changes**. Changes to the proxy configuration require a **Deploy Full Configuration**.

## Adding a Qualys scheduled import scan report

Add a scan report data import to schedule QRadar to retrieve scan reports from your Qualys scanner.

### Before you begin

Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der. To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.

- SSH into the Console or managed host and retrieve the certificate by using the following command: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. A certificate is then downloaded from the specified host name or IP and placed into `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

## Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify your Qualys scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Qualys Scanner**.
7. Configure the following parameters:

| Parameter | Description |
|---|---|
| **Qualys Server Host Name** | The Fully Qualified Domain Name (FQDN) or IP address of the QualysGuard management console. If you type the FQDN, use the host name and not the URL, for example, type `qualysapi.qualys.com` or `qualysapi.qualys.eu`. |
| **Qualys Username** | The user name that you specify must have access to download the Qualys Vulnerability Knowledge Base. For more information about how to update Qualys user accounts, see your Qualys documentation. |

8. Optional: To configure a proxy, select the **Use Proxy** check box and configure the credentials for the proxy server.
9. Optional: To configure a client certificate, select the **Use Client Certificate** check box and configure the **Certificate File Path** field and **Certificate Password** fields.
10. From the **Collection Type** list, select **Scheduled Import - Scan Report**.
11. Configure the following parameters:

| Parameter | Description |
|---|---|
| **Option Profiles** | The name of the option profile to determine which scan to start. QRadar retrieves the completed live scan data after the live scan completes. Live scans support only one option profile name per scanner configuration. |
| **Scan Report Name Pattern** | The regular expression (regex) to filter the list of scan reports. |
| **Max Reports Age (Days)** | Files that are older than the specified days and time stamp on the report file are excluded when the schedule scan starts. |

| Parameter | Description |
|---|---|
| **Import File** | The directory path to download and import a single scan report from Qualys, for example, `/qualys_logs/test_report.xml`. If you specify an import file location, QRadar downloads the contents of the scan report from Qualys to a local directory and imports the file. If you leave this field blank or if the file or directory cannot be found, the Qualys scanner uses the API to retrieve the scan report by using the value in the **Options Profile** field. |

12. Optional: To configure a CIDR range for your scanner, configure the CIDR range parameters and click **Add**.
13. Optional: To enable QRadar to create custom vulnerabilities from the live scan data, select the **Enable Custom Vulnerability Creation** check box and select options that you want to include.
14. Click **Save**.
15. On the **Admin** tab, click **Deploy Changes**. Any changes to the proxy configuration requires a **Deploy Full Configuration**.

## What to do next

You are now ready to create a scan schedule. See Scheduling a vulnerability scan.

# Index