# Table of Contents

**About this guide**........................................................................................................... 3  
   About Qualys .................................................................................................................. 3  
   Qualys Support ............................................................................................................. 3  

**Welcome to Qualys for ITSM**................................................................................... 4  
   Qualys VMDR for ITSM .................................................................................................. 4  
   Key Features of Qualys Core ......................................................................................... 4  
   Pre-requisites ................................................................................................................... 4  
   User Roles and Permissions ............................................................................................ 5  

**Get Started**.................................................................................................................. 7  
   Install the App ................................................................................................................ 7  
   Upgrade the App ............................................................................................................. 7  

**Qualys Core**.............................................................................................................. 9  
   Configure Basic Authentication Credential .................................................................... 9  
   Configure Connection to Qualys Applications ................................................................ 10  
   Configure Data Import .................................................................................................. 12  
   Import Configurations .................................................................................................... 12  
      Associate Import Configuration to Connector ............................................................. 13  
      Schedule Import ......................................................................................................... 14  
      View Jobs .................................................................................................................... 17  
      View Chunks ............................................................................................................... 17  
   Import Row Tables ........................................................................................................ 18  
   Data Tables .................................................................................................................... 18  
   Configure Detection Event Rule .................................................................................... 19  
      Detection Event Field Maps ....................................................................................... 20  
   Configure Assignment Rules ......................................................................................... 21  
   View SLA Definition ...................................................................................................... 23  
      Activate SLA ............................................................................................................... 25  
   Customize Data List Columns ......................................................................................... 25  

**Qualys VMDR for ITSM**............................................................................................ 28  
   Key Features ................................................................................................................... 28  
   Hosts/Assets .................................................................................................................. 28  
      Find CI ........................................................................................................................ 29  
      Create CI ..................................................................................................................... 32  
   View and Manage Vulnerability Tasks .......................................................................... 32  
      View Vulnerability Task Details ............................................................................... 33  
      Update Task ................................................................................................................ 36
Launch a VM Scan .............................................................................................................. 39
Scan Executions .................................................................................................................. 41
Detections .......................................................................................................................... 41
Reports and Dashboards .................................................................................................... 42
  Create a new report .......................................................................................................... 43
  Add a Report to Dashboard ............................................................................................. 49
  Share the report .............................................................................................................. 51
KnowledgeBase ................................................................................................................ 52

**Debugging and Troubleshooting** .................................................................................. 54

  How to debug ................................................................................................................. 54
  Configure logging .......................................................................................................... 54
  View Logs ...................................................................................................................... 54
Known Issues ................................................................................................................... 55
About this guide

Welcome to Qualys Cloud Platform! We’ll show you how to use the Qualys Core and Qualys VMDR for ITSM applications.

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 a 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 support information at www.qualys.com/support/
Welcome to Qualys for ITSM

Qualys ITSM application comprises of an application that manages connection between ServiceNow and Qualys - Qualys Core. Once the connection is configured, you can define import configurations, import schedules, incidents and related event detection rules, and service-level agreement (SLA) definition in the Qualys Core application.

Qualys VMDR for ITSM

The Qualys VMDR for IT Service Management (ITSM) is an application that manages tracking of open vulnerabilities and mapping of remediation tickets to the respective resolver groups. The applications acts as a bridge between Security and IT teams, uses the ServiceNow ITSM platform, and avoids manual intervention by creating automated workflows.

Note: Both Qualys VMDR for ITSM and the Qualys Core app are included with a Qualys Vulnerability Management, Detection and Response (VMDR) 2.0 subscription.

For quick introduction to the Qualys Core and Qualys VMDR for ITSM application, click here.

Key Features of Qualys Core

- ServiceNow ITSM is integrated bi-directionally with Qualys Core, where findings from Qualys are pulled by ServiceNow ITSM.
- Data from Qualys VMDR and File Integrity Monitoring (FIM) with predefined criteria are automatically imported on demand or through a defined schedule.

Note: FIM incidents and related events can be configured from Qualys Core version 1.2.0 and later.

- Vulnerability tasks are automatically created for the imported vulnerability findings.
- Tasks are automatically assigned to the concerned groups for remediation and are closed upon resolution.
- Custom SLA can be defined for open vulnerabilities based on Qualys real-time threat indicators (RTIs) and Qualys VMDR 2.0 with TruRisk.

Pre-requisites

- Service account with Manager privilege and API access in Qualys subscription
- ServiceNow IT Service Management (ITSM) test instance (recommended) and production instance.
**Note:** Request an instance size based on the following guidelines:
- Instance size XL for less than 1 million vulnerabilities
- Instance size XXL for 1 - 2.5 million vulnerabilities
- Instance size Ultra for more than 2.5 million vulnerabilities

- Up-to-date ServiceNow Configuration Management Database (CMDB) with reconciliation process enabled for newly-identified assets

- Qualys Core application 1.0.0
  **Note:** This is a prerequisite for installing Qualys VMDR for ITSM.

- Qualys subscription with Vulnerability Management, Detection and Response (VMDR) 2.0
- Qualys FIM subscription
  **Note:** Contact your ServiceNow representative to set up and install the applications on a test instance first and then on the production instance.

## User Roles and Permissions

The access to the Qualys Core and Qualys VMDR for ITSM applications is restricted based on the user roles.

The following table presents the user groups and associated roles and permissions:

<table>
<thead>
<tr>
<th>ServiceNow admin</th>
<th>Remediation owner</th>
<th>VMDR owner and Vulnerability analyst</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete access to Qualys Core and Qualys VMDR application</td>
<td>View and update Vulnerable task (VT) including – Vulnerability description, threats, remediation steps</td>
<td>Read-only access to Qualys Core</td>
</tr>
<tr>
<td>Configure automation rules (Assignment Rule, Detection Events, Schedule Import, SLA Definition)</td>
<td>Write access to the internal notes field</td>
<td>Monitor remediation progress - SLA of open tasks</td>
</tr>
<tr>
<td>Manage third-party Integrations (Qualys Connector)</td>
<td>Update the status of vulnerability tasks</td>
<td>Identify remediation challenges (Assign remediation tasks)</td>
</tr>
<tr>
<td>Manage VMDR user access</td>
<td>Submit Re-Scan</td>
<td>Coordinate with CMDB team (Infrastructure team) for unmatched items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Qualys Integration Checks (Connector Status)</td>
</tr>
</tbody>
</table>
Get Started

Follow the steps to install Qualys Core and Qualys VMDR for ITSM applications.

Install the App

Visit the ServiceNow Online Store and search for Qualys apps.
- Go to Qualys Core app, and click Request App. Your Qualys representative will enable the application for you if you have Qualys VMDR subscription. The app then appears in the “Downloads” list of your instance. Click “Install” to start install the app.
- Go to Qualys VMDR for ITSM app and perform the same steps that you followed to install the Qualys Core application.

In the Search field, type Qualys, and then select Qualys Core and Qualys VMDR for ITSM from the left pane.

After you are done, the new modules appear in the ServiceNow instance that looks like this for a Vulnerability Admin group:

![ServiceNow Interface with Qualys Core and Qualys VMDR for ITSM modules]

**Note:** The options in the Qualys Core and Qualys VMDR for ITSM applications that you can view are different based on the user group to which you belong. For information on user roles, see User Roles and Permissions.

Upgrade the App

To view if you have a new version of the application available, navigate to System Application > My Company Application > Installed.
If there is a new version available, it is displayed in the drop-down list. Select the version and click **Update**.
Qualys Core

Qualys Core application manages connection between ServiceNow and Qualys Vulnerability Management, Detection and Response (VMDR), data import, import schedules, vulnerability detection rules, and service-level agreement (SLA) definition.

In Summary

Configure Basic Authentication Credential - Create basic authentication credential record in ServiceNow to authenticate the connection.

Configure Connection to Qualys Applications - Configure the connection with Qualys and use Test Connection to know if the connection between ServiceNow and the Qualys is working fine.

Configure Data Import - Provide details of import configuration and schedule imports.

Configure Detection Event Rule - Provide details to define which vulnerabilities should be added to ServiceNow ITSM for creating tasks.

Configure Assignment Rules - Provide details to create rules for assignment of tasks to appropriate groups.

Customize Data List Columns - Provide details of import configuration and schedule imports.

Configure Basic Authentication Credential

You need to set up a basic authentication credentials record in ServiceNow for authenticating a connection.

Note: Contact your Qualys administrator for your account to get service account details.

To configure basic authentication credential:

In the application navigator, go to Connection & Credentials > Credentials, and click New.

Click Basic Auth Credentials from the list.

Enter required details to create an authentication record:

Name - Provide a name for the authentication record.
User name - User name to be associated with the authentication record.
Password - Password for the user name.

Click Submit. This record is available while selecting credentials for authenticating connection to Qualys.

Configure Connection to Qualys Applications

Once you install the Qualys Core app, you need to configure a connection with Qualys.

Note: Qualys Core supports multiple Qualys VMDR subscriptions to import findings into Qualys VMDR for ITSM.

To add a new connector, go to Qualys Core > Configuration > Connectors, and click New.

Enter required details to create the connector:
Name - Provide a name for the connector.
Active - Select this option to activate the connector that you create.
Endpoint - Enter primary URL for the Qualys server that this connector will connect to get data from Qualys. To identify the endpoint URL, refer to the API URLs in https://www.qualys.com/platform-identification/.
MID Server - The MID server can work as a proxy server/middleman between ServiceNow and Qualys pod, wherein the ServiceNow instance work with limited reachability to outside sources.

VMDR Healthy and FIM Healthy check boxes indicate whether the last test connection with VMDR and FIM was successful for this connector.

Note: These check boxes are not available while configuring a new connector.
Authentication

Credentials - Select appropriate credentials that you have created for authentication. For details on how to create basic auth credentials, see Configure Basic Authentication Credential.

Settings

Enter the required details for rescanning a host.

Default Scanner Appliance - Select default scanner to be used for rescanning from the Qualys Scanner Appliances list.

Default Option Profiles - Select default option profile to be used while rescanning from the Qualys Option Profiles list.

Note: The list scanner appliance and option profile will be available only when the import configurations are run and cannot be selected while creating a new connector. Contact your Qualys representative for setting up default scanner appliance and option profile.

Click Submit to create the connector.

Then, after configuring and saving the connector, click the connector you have created from the Connectors list, and click Test the Connector from the Related Links.

If the connection is healthy, proceed to import data. Else, use the error message and the system logs to resolve the error.
Configure Data Import

After configuring a connection to Qualys, you can view data imported from Qualys for VMDR and FIM - KnowledgeBase, option profiles, scanner appliance, host assets for VMDR and FIM incidents and incident events for FIM.

Qualys Core imports data from Qualys by using the import configurations, where you need to associate a defined import configuration to a connector to execute importing data from Qualys.

Import Configurations

Go to Data Import > Import Configurations to review the data import configured by default.

If you want to configure Qualys Core to work with Qualys VMDR for ITSM, review and ensure that the following import configurations are active:

- Host Asset Import
- Host Detection Import

**Note:** Configure the host detection event rules before you import host detections. For host detection rules, see Configure Detection Event Rule.

- KnowledgeBase Import
- Option Profiles
- Scanner Appliance

If you want to configure Qualys Core to work with FIM application, review and ensure that the following import configurations are active:

- FIM Incident Event Import
- FIM Incident Import

If you are not using FIM application, you can deactivate the FIM-related import configurations.
Associate Import Configuration to Connector

You must associate the import configuration to a connector so that you can execute the import.

To associate import configuration to a connector:

Go to Configuration > Connectors, and select the connector for which you wish to configure imports.

Navigate to Import Configurations, and click Edit.

From the Collection list, select the import configuration and move to the Import Configuration List.

- If you want to configure Qualys Core to work with Qualys VMDR for ITSM, select the import configurations, as shown in the following image:
- If you want to configure Qualys Core to work with FIM application, select the following import configurations, as shown in the following image:

![Image of import configurations](image.png)

Click **Save**.

**Schedule Import**

You can define schedules to import each type of data at a specified frequency to automate data import. You have default import schedule associated with every import configuration. Go to **Data Import > Scheduled Imports** to view the schedules defined by default.
The following image displays the default schedules for each import configuration defined for FIM and VMDR.

**Note:** We recommend to import each type of data at least once everyday. However, you can define to import data multiple times a day depending on your infrastructure and scanning frequency.

To define a new schedule, click **New**.

Enter required details to create a schedule:

**Name** - Provide name for the new schedule.

**Import Configuration** - Select the entity for which this import schedule will be applied.

**Active** - Select this check box to activate the import schedule.
**Type** - Select one of the following values:

- **Import - With Configuration**: Select this option to schedule data import with the import configuration defined in the Import Configurations.

- **Import - Generic**: Select this option to schedule data import with customized import configuration.

**Delta Timestamp** - Indicates the date and time when this scheduled import was last run.

*Note:* If the **Delta Timestamp** field is populated, the data import is executed as delta. For the first import execution, clear the value in the **Delta Timestamp** field to perform full import.

**Chunk Size** - Provide the number of records to be imported in a chunk.

**Chunk Data Load Timeout (sec)** - Provide the time limit in seconds between the time when the chunk import record is created and the time when loading of data is completed. If it exceeds the defined time, the chunk is marked with an error.

**Import only when all data is received** - Select this check box if you want to import data when all chunks are executed and data is loaded in the import table. In this case, the data transformation is performed at the job level. If this check box is clear, the data transformation is performed at the chunk level, which may be useful if the total number of records at the job level can take long time to import.

**Stop processing on Chunk Error** - Select this check box if you want the scheduled import operation to stop when a chunk is marked as an error.

**Schedule**

**Run** - Select the frequency of import from the list. The related fields change based on the value you select in the **Run** field.

**Run as tz** - Select the time zone to be followed for this import schedule.

**Run as** - Select the user or user group.

**Conditional** - Select this check box to add more conditions on the import schedule.
Script - You can enter a script to customize the import schedule.

**Note:** There is a default import schedule associated with every import configuration. We recommend you to retain the default values for all the fields except, **Delta Timestamp** and **Schedule** fields.

View Jobs

After scheduled import execution, data transfer jobs are processed. You can view details of data transfer jobs - job number, status, start and stop time, completion percentage, associated connector, and so on.

The data transfer jobs track the higher-level batch of data that is being transferred. When the data transfer jobs are processed, data chunks are created. Those chunks are associated to the job.

View Chunks

You can view details of the data chunks in each data transfer job, such as, chunk number, the associated data transfer job, status, start and stop time, and so on.

You can monitor progress of data transfer chunks based on the **State** - Errors, In Progress (Making API Call), Importing (Import Set and Transformation), Completed (All done, move onto next check).
Import Row Tables

The import tables present the data imported from Qualys through scheduled import operations from VMDR and FIM.

The import row tables for hosts, host detection, scanner appliance, option profiles, and knowledgebase present data imported from Qualys VMDR application.

The import row tables for FIM incidents and FIM incidents events present data imported from Qualys FIM application.

The tables are automatically updated after the scheduled import runs for each type of data. Click the information icon or value in the first column to view the details.

Data Tables

The data imported is transformed based on the field mapping and is presented in the data tables.

You can view data tables for hosts, host detections, scanner appliances, option profiles, and knowledgebase as well as for Qualys tags, asset groups (created from host assets import), and scan executions (generated based on scans launched) for VMDR data.

You can view data tables for FIM incidents, FIM incident events, FIM event profiles, and FIM incident event queue for FIM data.
Configure Detection Event Rule

You can define the rules for detection of events for which the tickets will be created based on type and severity of vulnerabilities, asset tags, RTI’s, and Qualys Risk Score.

**Note:** This section is applicable only if you want to work with Qualys VMDR for ITSM application.

Go to **Configuration > Detection Event Rules** to view the detection rule that is added by default. However, you can update an existing rule or create a new rule.

To create a new host detection event rule, go to **Configuration > Detection Event Rule**, and click **New**.

Enter required details to create the detection event rule:

- **Name** - Provide a name of detection rule.
- **Active** - Select the Active check box to activate the detection rule that you create.
**Destination table** - Select **Qualys - Vulnerability Task** from the list of tables. This table is created for Qualys VMDR vulnerabilities.

**Description** - Enter description for detection event rule.

**Order** - Provide the number that indicates the order of priority for running this detection event rule. The value in the **Order** field is a relative value and the detection event rules are executed in ascending order, that is, lowest to highest. The order assigned to a rule helps decide the priority when multiple rules exist for the same table.

**Stop processing** - Select this check box to stop processing the rules ordered after this rule once the detection conditions are met.

**Detection condition** - Define criteria on the host detection record that should trigger this detection event rule and create a record in the destination table. You can use single or multiple attributes and filters.

You may need to use the **Show Related Fields** option at the bottom of the field list to allow you to get to reference data such as **QID => Severity** to validate the severity level of a detection record.

Click **Submit** to create the detection event rule.

**Detection Event Field Maps**

Once the detection event rule is created, add field mappings. Click the detection event rule that you created, and go to **Detection event field maps**.
You must add the following three fields mappings.

You can add any additional field mappings as per your requirement.

**Note:** We recommend to set the **Coalesce** field as mentioned in the example to avoid creation of duplicate entries.

### Configure Assignment Rules

The assignment rule defines the group to which the vulnerability task will be assigned based on the group responsible for the remediation of the detected vulnerability. The tasks are automatically assigned to the appropriate team based on the criteria defined.

Currently, all tasks are assigned to the Infrastructure team.

**Note:** We have provided an example of how an assignment rule is created. However, you may not view this option as the permissions to create the assignment rule are restricted. To get the assignment rules created, contact your ServiceNow representative.

To create a new assignment rule, go to **Configuration > Assignment Rules**, and click **New**.

Enter required details to create the assignment rule:
Name - Provide a name for the assignment rule.

Active - Select the Active check box to activate the assignment rule that you create.

Applies To - Define the conditions for the detected vulnerability for the task to be assigned to the user or group.

Note: The assignment rule is applied only if the task is not already assigned to any other user or group.

Table - Select Qualys - Vulnerability Task from the list.

Conditions - Define conditions using single or multiple attributes and filter for this assignment rule.

The conditions can be selected based on your CMDB attributes such as, CI class (Windows, Linux), CI OS type, CI location and zone, CI IP address range/CIDR, CI assignment group, and so on.

Assign To - Select User or Group from the list to whom the task will be assigned.

Script - You can enter a script to customize the assignment rules.

Click Submit to create the assignment rule.
View SLA Definition

You can view the service-level agreements (SLAs) defined for the different tasks. Go to Configuration > SLA Definitions to view SLAs defined for different tasks created for vulnerabilities detected by Qualys VMDR.

The SLA definition is based on the Asset Criticality, Vulnerability Severity, Threat Exposure, Qualys Real-Time Threat Indicators (RTIs), and CI mapping. The remediation timelines are automatically measured according to the SLA definition.

**Note:** The SLA values are recommended values. To update the SLAs, contact your ServiceNow representative.
The SLA Definition page displays the conditions in which the SLA is triggered, paused, stopped, and reset.

These conditions are based on Vulnerability Status (New, Active, Fixed, Reopened) and Vulnerability State (Open, In progress, In review, Change implemented, Resolved, and so on).

- The vulnerability states included in the Start condition are Open, In-Progress, In-Review, Under Investigation, and Reopened.
- The vulnerability states included in the Pause condition are Awaiting Change Request, Under Implementation, Change Implemented, Awaiting Exception Approval, Exception Approved, and False Positive – Approved.
- The vulnerability states included in the Stop condition are Closed and Resolved.
Activate SLA

By default, the SLAs are not activated. To activate an SLA, click an SLA definition, set the **Duration Type** and **Schedule** fields, and click **Update**.

![Activate SLA](image)

Customize Data List Columns

We display few columns in the data lists. You can customize which columns appear and change the column sequence. The following example presents how to add a column to the displayed list of columns.

1) Click the ![icon](image) icon in the main pane. The **Personalize List Columns** pop-up appears.

![Personalize List Columns](image)

2) The **Available** list includes columns that are currently hidden. From this list, select the column you want to display. For example, double-click the column "**Updated by**" and you will see it moved to the **Selected** list.

![Available and Selected](image)
3) Enable or disable other settings like **Wrap column text**, **Double click to edit**, and so on.
4) Click OK.

You’ll start seeing the Updated by column. If for some columns, the data is not available, the value in the column will be empty.
Qualys VMDR for ITSM

Qualys VMDR for ITSM application manages tracking of open vulnerabilities and mapping of remediation tickets to the respective resolver groups.

Key Features

- Qualys VMDR and ServiceNow ITSM are integrated bi-directionally, where findings from Qualys are pulled by ServiceNow ITSM.

- The rescan feature can be used by the resolver groups to measure the impact of patching. If the vulnerability is identified by Qualys as Fixed, based on the outcome of the consecutive scan or agent data, the task will be automatically closed.

- Host Assets data from Qualys is compared with ServiceNow CMDB and hosts are classified as Matched and Unmatched.
  - Assets matching a CI in the SNOW CMDB are marked as Matched.
  - Assets not matching a CI in the SNOW CMDB are categorized as Unmatched. You can use the ServiceNow Identification Reconciliation Engine (IRE) to find the CI for these assets or can create a new CI record. With this, you can review the asset prior to creating CI entries.

- Multiple dashboard and reports can be created to display data and status based on status of vulnerability, SLA monitoring, critical assets with RTIs and Asset Risk Scoring.

In Summary

Hosts/Assets: View details of assets and match or create CI records.

View and Manage Vulnerability Tasks: View details of all vulnerability tasks created.

Launch a VM Scan: Launch a VM scan from Qualys VMDR for ITSM application.

Scan Executions: List of scan executions that are initiated from this application.

Detections: List of all vulnerability detections categorized based on status.

Reports and Dashboards: View different reports and dashboards.

KnowledgeBase: View Qualys knowledgebase.

Hosts/Assets

When data is imported as a part of the integration, the VMDR for ITSM automatically uses host (asset) data to search for matches in the ServiceNow Configuration Management Database (CMDB).
CI lookup rules are used to identify CI and add them to host detection records when vulnerability tasks are created to help you with remediation.

- **CI-Matched** - If the IP address or host that is scanned in Qualys is part of ServiceNow CMDB, the same is categorized as matched CI. The vulnerability task created for this host or assets is assigned according to the defined assignment rules.

- **CI-Unmatched** - If the IP address or host that is scanned in Qualys is not available in CMDB, the host or asset is categorized as unmatched CI. The vulnerability task is created for this host or asset and is assigned to your Security team.

**Note:** To maximize the Host Asset records matching with CMDB CI records, enable the CI re-classification during IRE processing. For Identification and Reconciliation, following properties are used to control the re-classification, and to identify the CI records:

- glide.class.upgrade.enabled
- glide.class.downgrade.enabled
- glide.class.switch.enabled

For more information, click [here](#).

Set these properties as True to maximize the Host Asset records matching with CMDB CI records.

**Find CI**

For unmatched CI, you can find the CI availability by using the ServiceNow functionality - Identification and Reconciliation Engine (IRE).

The Identification and Reconciliation Engine (IRE) tries to find the associated CI based on other matching criteria, such as, Host Name, DNS Name, FQDN, Domain, and Netbios.
To find associated CI, open an unmatched CI record, and click **Find CI**.

If any parameter matches the corresponding values in CMDB, the **Configuration item** field is automatically populated. Click **Update** to update the record.

**Note:** Ensure that you have defined the Hardware Rule in the Identification and Reconciliation Engine.
To check the hardware rule, go to **Identification/ Reconciliation > CI Identifiers > Hardware Rule.**

**Note:** The CI matching can be enhanced with the Qualys CMDB Sync app available on the ServiceNow store. For more information on Qualys CMDB Sync app, contact your Qualys representative.
Create CI

If there is no matching CI found in CMDB by using the IRE, you can create a new CI record. To create a new CI record, open an unmatched CI record, and click Create CI. The Configuration item field is populated with the CI value.

Click Update to save the record.

View and Manage Vulnerability Tasks

When the detection event rule provided in the Qualys Core application is processed, vulnerability tasks are created for the host detections that are imported. You can view and update the vulnerability tasks that are created.

Infrastructure and Security teams can view all the tasks.
You can view the tasks categorized based on task assignment, that is, tasks assigned to you and your group, based on status of the tasks, that is, open or fixed.

**Note:**
- The administrators can view all vulnerability tasks in all statuses.
- If you are a part of a remediation team, you can view only the tasks that are assigned to your own group.

**View Vulnerability Task Details**

You can view list of all the vulnerability tasks that are created in the application.

You can click a vulnerability task number to view details of the vulnerability task. You can view the basic information of a vulnerability task, such as, task number and status, Qualys detection ID, associated connector, status of the vulnerability, and assignment details.
Host Information provides host and host network information.

Vulnerability Details provides details of a vulnerability that is available from Qualys VMDR.
The **Detection** tab provides the detection logic, type of vulnerability, tracking method and results of the detection.

---

The **Detection** tab also provides details of scan dates.

---

The **Detection** tab provides the detection logic, type of vulnerability, tracking method and results of the detection.

---

The **Detection** tab also provides details of scan dates.
You can add notes to the ticket in the **Notes/Activity** tab. Any changes or updates in the task is also seen in the **Notes/Activity** tab.

On the vulnerability task page, you can also view additional details, such as, recent vulnerability scans, other open tasks on the same host, open tasks for the vulnerability that is selected, and SLA for the selected task.

**Update Task**

You can update the state of the task to Resolved. When the status of the vulnerability is fixed, the task state is automatically updated to Closed.

**Note:** You can use your internal Exception Management workflow for Vulnerability exception for any open tasks and update the vulnerability task **State** to **Exception Approved**, **Awaiting Exception Approved**, and **False Positive - Approved** as appropriate. If the task is updated to the exception state, the SLA is paused, and the **Exception** tab is available to add the details of the exception.
You understand whether the vulnerability is remediated completely in the following ways.

- If the vulnerability is detected by the Qualys agent, the agent keeps polling every four hours. If the vulnerability is remediated, the status of the vulnerability is updated to Fixed.

- If the vulnerability is detected by a virtual scanner, the change in the vulnerability status is updated in the next scanning.

You can click **Launch VM Scan** from Related Links to launch a Qualys VM scan.
You can select the **Scanner Appliance** and **Option Profile** from the list and click **Start Scan**. We recommend you to use the default option profile that is configured and populated. If authentication is missed, vulnerability detection may not be accurate. If the vulnerability status is changed to Fixed in the scan, the task will get closed automatically.

**Note:** If the tracking method for the host is Cloud Agent, Cloud Assets, DNS tracked, NetBIOS tracked, or FQDN, you cannot launch a VM scan.
Launch a VM Scan

You can launch vulnerability scans from the Qualys VMDR for ITSM application to verify whether a vulnerability is fixed.

**Note:** Currently, we perform scans for detection of all QIDs. We are not supporting scan for a selected vulnerability at the QID level.

We can launch a Qualys VM scan in following ways:

- For a single vulnerability task

  You can click **Launch VM Scan** from the **Related Links** in the vulnerability task.

- For multiple vulnerability tasks

  ![](image-url)

  You can select multiple vulnerability tasks and select **Launch VM Scan** from the list of available actions.
- For Hosts/ Assets

![Image of Host Assets]

You can select multiple host assets from Host Assets or from Host/ Assets and select Launch VM Scan from the list of available actions.

- For Host Detections

![Image of Host Detections]

You can select multiple host assets from Host Detection or from Detections and select Launch VM Scan from the list of available actions.
Scan Executions

You can view details of all scans launched through ServiceNow here. The scans are also categorized as pending scans and scans with errors.

You can view all the scans that you have initiated.

Click the options in the left pane to view required scan executions.

Detections

You can view details of all vulnerabilities detected by Qualys VMDR.

You can click the options in the left pane to view vulnerabilities based on its status, that is, New, Active, Fixed, and Re-opened.

For each detected vulnerability, you can view vulnerability details, such as, detection ID, type and status of vulnerability, results of the vulnerability and other details, such as, host details, related knowledgebase, and scan dates.
Reports and Dashboards

Go to Qualys VMDR for ITSM App > Overview.

The Overview page displays a consolidated view of all the reports for vulnerabilities, detection, hosts, and so on.
The **Detections** tab provides reports on detections based on different criteria, such as, type of detections, status of detections, number of detections.

![](image1.png)

The **SLAs** tab provides reports on SLAs based on different criteria, such as, active SLAs, SLAs for each assignment group, average age of SLAs, and so on.

You can edit the existing dashboard, add new reports to the dashboard or create a new dashboard.

**Create a new report**

You can create new reports for the data that you want to view. For example, report for open tasks for a specific vulnerability type. You can also select the format in which the data is presented, that is, bar chart, pie chart, time series, and so on.

To create a new report, in application navigator, go to **Reports > Create New.**
In **Create a report** > **Data**, enter the required details for a new report.

**Report name**: Provide a name for the new report.

**Source type**: Select **Table** from the list that is used as a source of the data.

**Table**: Enter **Qualys** to populate the Qualys import tables and select the relevant table from the list.

Click **Next**.

In the **Type** form, select the way in which you want to present the report. For example, bar chart, pie chart, time series report, and so on.

Click **Next**.
In the **Configure** form, the fields that are displayed depend on the type of report that you have selected.

By default, the report is created in a tabular format. In the following image, you can see the options for configuring your report in a tabular format.

In the right pane, all the data from the selected Qualys table is displayed.

For example, in this image, all tasks from the Qualys Vulnerability Tasks table are displayed irrespective of the vulnerability status.

Click **Edit Condition** to filter the data for which you want are creating a report.
Define the criteria to filter the data for creating a report. You can use single or multiple attributes and filters.

For details on how to define conditions for a report, refer to the Define Conditions. Click Next.

In the Style form, select the style for your report.

Click Run to apply the defined condition.
Click **Save** to save the report.

**Define Conditions**

In this example, you can see how to add the conditions for filtering tasks logged for Log4j vulnerability, where the vulnerability status is are New, Active or Reopened.

- Select and expand the **Qualys Detection** table, and select **Vulnerability Status** field.
- Select the operator and appropriate values.

- Click **AND** to add another condition.

- Select and expand the **Qualys Detection** table, and select QID.

- Select the operator and add all QIDs for log4j vulnerability.
The filter conditions are added. Click **Run** to apply the conditions.

**Add a Report to Dashboard**

Once you add a report to the dashboard, you can view the report in the **Overview** and track the change in the report data at a glance.

For example, if you add a report for active tasks for a specific vulnerability count to the dashboard, you can track whether the count shows increasing or decreasing trend.

To add a report to the dashboard, go to **Overview**, click **Add Widgets** icon.

Click the report to be added and click **Add**.
The report is added to the top of the dashboard.

You can resize the widgets and move the positions of the widgets in the dashboard.

You can update the presentation data presented in the report that you have created.

For example, in the Vulnerability by Port report, data can be grouped by Qualys Detection Port, Detection Protocol, or Detection Vulnerability Status.
Share the report

Once you add a report that you have created to the dashboard, only you can view it on the dashboard.

If you want the report to be visible to a user or group of users, you can share the report with other users. For example, a report on open tasks for a specific vulnerability can be shared with the respective remediation team.

To share a report or dashboard with a user, go to **Overview**, click the **Sharing** icon.

In the **Share** form, add a user name in the recipients, and click **Share**.

You can select the **Send an email invitation** to send an email notification to the selected user, and add a message for the user. In the **Recipients** list, you can select the permissions for the user to indicate whether the user should have view or edit permissions to the report.
KnowledgeBase

You can view Qualys KnowledgeBase in the VMDR for ITSM.

You can click the options in the left pane to view knowledge base items for the confirmed vulnerabilities, all vulnerabilities and SLAs for all vulnerability tasks.
Debugging and Troubleshooting

How to debug

In case of any unexpected application behavior, you can check the application logs. The application log has four different levels of logging: Information, Error, Warning, Debug. The application writes log entries after important transitions.

Configure logging

From the Qualys Core application, click **Diagnostics > Logging Configuration**. In the **Qualys for ServiceNow Logging** page, select **Debug** in the **Logging Level** field.

View Logs

To view the logs, navigate to System Logs > All, and filter with **Qualys Core** as **App Scope**.

![Qualys VMDR for ServiceNow ITSM Debugging and Troubleshooting](image)
Known Issues

FIM API does not support the 'updatedDate' filter. Hence, currently Qualys Core app cannot show the state transition of the synced incident on the Qualys UI.