# Table of Contents

## About this guide

- About Qualys ................................................................. 3
- Qualys Support ............................................................... 3

## Welcome to Qualys VMDR for ServiceNow

- Qualys VMDR ................................................................. 4
- Key Features ................................................................. 4
- Pre-requisites ............................................................... 5
- User Roles and Permissions ...................................... 5

## Get Started

- Install the App ............................................................ 9
- Upgrade the App ........................................................ 10

## Qualys Core

- Configure Basic Authentication Credential .................. 13
- Configure Connection to Qualys Applications .............. 14
  - Associate Import Configuration to Connector ............. 17
- Configure Data Import ............................................... 19
- Import Configurations ............................................... 19
  - Schedule Import ..................................................... 20
  - View Jobs ................................................................. 22
  - View Chunks ............................................................. 23
- Import Row Tables ...................................................... 23
- Data Tables ............................................................... 24
- Configure Detection Event Rule .................................. 25
  - One-to-One Rules .................................................... 25
  - Detection Event Field Maps .................................. 28
  - Grouping Rules ......................................................... 29
- Configure Assignment Rules .................................... 35
- View SLA Definition .................................................. 38
  - Examples of SLA definitions .................................. 39
  - SLA definition for Internet-facing assets ................ 40
  - Activate SLA .............................................................. 41
- Configure Patch Deployment Settings ....................... 41
- Customize Data List Columns ..................................... 42

## Qualys VMDR

- Hosts/Assets .......................................................... 44
- Find CI ................................................................. 45
About this guide

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

Qualys VMDR for ServiceNow 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. You can also configure detection rules for qualys-patchable vulnerabilities that reflects in automatic creation of change requests, creation of patch jobs in Qualys Patch Management. This helps in faster remediation and thus helps to meet the SLAs to reduce risk within the organization.

Qualys VMDR

The Qualys VMDR 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, and avoids manual intervention by creating automated workflows.

Note: Both Qualys VMDR 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 application, click here.

Key Features

- Bi-directional integration between Qualys and ServiceNow, where findings from Qualys are pulled by ServiceNow and push mechanism that provides information on critical vulnerabilities with real time mapping of threat indicators.

- Automated data import from Qualys VMDR, File Integrity Monitoring (FIM), and Patch Management with predefined criteria- 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.

- Automated ticket creation, identification or matching of CIs with ServiceNowCMDB, assignment to rightful owners, and closure on remediation.

- Vulnerability grouping based on multiple parameters, such as, operating system, severity, Qualys TruRisk score, and so on. This helps in reducing number of tasks for the IT teams to track and remediate.

- Custom SLA can be defined for open vulnerabilities based on Qualys real-time threat indicators (RTIs) and Qualys VMDR 2.0 with TruRisk.

- Automated Change request creation, approval enforcement and integration with Qualys patch management.
- Integrated Exception Management and false positive process to offer a comprehensive and complete VM solution.
- The rescan feature 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.
- Dynamic 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.

**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 and Qualys VMDR applications

**Note:** Qualys Core application is a prerequisite for installing Qualys VMDR.

- 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 applications is restricted based on the user roles.
The following table presents the user groups and associated roles and permissions for Qualys Core application:

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>x_qual5_core.admin</td>
<td>Administrative user of the application. Create, Write, Read, and Delete access to all aspects of the application.</td>
</tr>
<tr>
<td>x_qual5_core.kb_read</td>
<td>Read access to the Qualys - KnowledgeBase records.</td>
</tr>
<tr>
<td>x_qual5_core.create_ci_from_host</td>
<td>Can see the &quot;Create CI&quot; UI action from host records.</td>
</tr>
<tr>
<td>x_qual5_core.api_data_receiver</td>
<td>Grants access to any Data Receiver API Endpoints that are available &quot;globally&quot; across the Qualys for ServiceNow app and add-ins. These endpoints are used for Pushing data from Qualys into ServiceNow. This role would need to be given to the ServiceNow Service Account that is being used by Qualys for API Authentication.</td>
</tr>
<tr>
<td></td>
<td># API Endpoints</td>
</tr>
<tr>
<td></td>
<td>- /api/x_qual5_core/v1/data_receiver/{connector_sys_id}/vmdr/host_asset</td>
</tr>
<tr>
<td></td>
<td>- /api/x_qual5_core/v1/data_receiver/{connector_sys_id}/vmdr/host_detection</td>
</tr>
<tr>
<td>x_qual5_core.connector_user</td>
<td>This role grants access to create, modify and delete Connector Records.</td>
</tr>
<tr>
<td>x_qual5_core.qualys_fim_incident_user</td>
<td>Has access to FIM Incidents and information related to them.</td>
</tr>
<tr>
<td>x_qual5_core.general_settings</td>
<td>Has access to read/write the General Settings values of the application.</td>
</tr>
<tr>
<td>x_qual5_core.import_user</td>
<td>Has access to the import_set tables for debugging and API Calls.</td>
</tr>
<tr>
<td>x_qual5_core.host_user</td>
<td>Has Read access to Host Asset Records and related information such as Asset Tags and Asset Groups</td>
</tr>
<tr>
<td>x_qual5_core.launch_vm_scan</td>
<td>Role required to see / interact with Launching VM Scans</td>
</tr>
<tr>
<td>x_qual5_core.patch_deployment_user</td>
<td>This role grants access to view and management patch deployments for Change Request</td>
</tr>
<tr>
<td>x_qual5_core.view_vm_scan</td>
<td>This role grants access to view VM Scans and related data such as Option Profiles and Scanner Appliances</td>
</tr>
</tbody>
</table>
The following table presents the user groups and associated roles and permissions for Qualys VMDR application.

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>x_qual5_core.user</td>
<td>This role grants basic access to the Data Tables within Qualys CORE and basic information within those tables. Typically this role is not granted directly to users, and will be auto-granted based on the add-on application roles that come with Applications such as Qualys VMDR. &lt;br&gt; # Access to read the following &lt;br&gt; - Qualys Tags / Asset Tags &lt;br&gt; - Detection Event Rules &lt;br&gt; - Specifically the Name, and Description attributes (and nothing else) &lt;br&gt; - Qualys Asset Groups &lt;br&gt; - Basic Information to Connectors, such as Name. &lt;br&gt; - Access to ancillary functionality used by various functions of other applications.</td>
</tr>
<tr>
<td>x_qual5_core.qualys_knowledgebase_user</td>
<td>This role grants READ Only access to the Qualys KnowledgeBase.</td>
</tr>
<tr>
<td>x_qual5_vmdr.dashboard_viewer</td>
<td>Can Access / View Dashboard from VMDR Application</td>
</tr>
<tr>
<td>x_qual5_vmdr.admin</td>
<td>Can create/read/write/delete items within this application scope.</td>
</tr>
<tr>
<td>x_qual5_vmdr.exception_approver</td>
<td>Can read vulnerability tasks where they are the &quot;Exception approver&quot; or if the task is assigned directly to them.</td>
</tr>
<tr>
<td>x_qual5_vmdr.false_positive_approver</td>
<td>Has access to read Vulnerability Tasks where they are involved in the approval process for it (regardless of which approval step). Has additional access to edit fields required to be filled by the False Positive Approver on the vulnerability task, when they are involved in the approval for that vulnerability task.</td>
</tr>
<tr>
<td>Role</td>
<td>Permissions</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>x_qual5_vmdr.remediation_owner</td>
<td>This is the role intended for Remediation Owners that need to perform work on VMDR Task or VMDR Task Group records that belong to a Support/Assignment group that they are a member of.</td>
</tr>
<tr>
<td></td>
<td><strong>## VMDR Task</strong>&lt;br&gt;- Grants Read/Write access to VMDR Tasks and Related Functions where the logged in user is a member of the Assignment Group for that Task</td>
</tr>
<tr>
<td></td>
<td><strong>## VMDR Task Group</strong>&lt;br&gt;- Grants Read/Write access to VMDR Task Group Records and Related Functions where the logged in user is a member of the Assignment Group for that Task</td>
</tr>
<tr>
<td>x_qual5_vmdr.vulnerability_analyst</td>
<td>This is the role intended for Security Analysts that need to perform work or oversee all VMDR Task and VMDR Task Group records, regardless of which Assignment Group they are associated to.</td>
</tr>
<tr>
<td></td>
<td><strong>## VMDR Task</strong>&lt;br&gt;- Grants Read/Write/Create access to all VMDR Tasks and Related Functions</td>
</tr>
<tr>
<td></td>
<td><strong>## VMDR Task Group</strong>&lt;br&gt;- Grants Read/Write/Create access to all VMDR Task Group and Related Functions</td>
</tr>
</tbody>
</table>
Get Started

Follow the steps to install Qualys Core and Qualys VMDR 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 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 from the left pane.

After you are done, the new modules appear in the ServiceNow instance as displayed in the following image:

![ServiceNow interface with Qualys Core and Qualys VMDR modules](image)

**Note:** The options in the Qualys Core and Qualys VMDR 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 and upgrade the new version of the application:

In ServiceNow application, navigate to **System Applications > All Available Applications > All**.

Search for the application you want to update. You can see the version of the application that is installed currently.
If there is a new version available, it is displayed in the drop-down list. Select the version you want to upgrade to 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 for creating tasks.

- You can define one-to-one rules for creating the vulnerability tasks from the detections and you can also define grouping rules to group the vulnerability tasks based on different criteria. You can define the detection event rule to create change requests which can be used to apply patches to the host assets for remediation.

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

Configure Patch Deployment Settings - Define default settings for the patch deployment jobs.

Configure Basic Authentication Credential

You need to set up a basic authentication credentials record in ServiceNow for authenticating a connection to Qualys system. You must have a Service account with Manager privilege and API access in Qualys subscription to setup basic authentication credentials.
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 domain separation that separates data between service providers, partners, and sub-organizations. Support for domain separation allows Managed Service Providers (MSPs), Managed Security Services Providers (MSSPs) and Qualys Partners to customize business process definitions and user interfaces for each domain – a form of delegated administration.
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/](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. This is an optional field.

**VMDR Healthy, FIM Healthy, PM Healthy** check boxes indicate whether the last test connection with respective applications was successful for this connector.

**Note**: These check boxes are not available while configuring a new connector. Once create a connector and click Test the connector, the check boxes are selected based on the successful connection.

**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.

<table>
<thead>
<tr>
<th>Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection Re-Scan</td>
<td></td>
</tr>
<tr>
<td>Default Scanner Appliance</td>
<td>ADCZ Pass-Thru RAS Scanner</td>
</tr>
<tr>
<td>Default Option Profile</td>
<td>Copy of All Authentication - UIX</td>
</tr>
<tr>
<td>Web Portal URL</td>
<td><a href="https://exampleplatformurl.com">https://exampleplatformurl.com</a></td>
</tr>
</tbody>
</table>

**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.

**Web Portal URL** - Enter Qualys platform URL. Using this URL, you can view the patch deployment job directly in Qualys Patch Management application. See Reports and Dashboards.

To identify the endpoint URL, refer to the API URLs in https://www.qualys.com/platform-identification/

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.
**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, 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:

Click **Save**.
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, the following import configurations are available by default.

- Host Asset Import
- Host Detection Import
- KnowledgeBase Import
- Option Profiles
- Scanner Appliance

Review the import configurations to check what data is being imported. For example, Import Configuration: Host Detection, review the **Detection Filters, Vulnerability Filters, Host Filters** tabs, modify the values as required, click **Update** to update configuration.

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

**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.

In the default import schedules, review the following sections:
If you want to copy the default import schedule, modify, and create a new schedule, open the default import schedule, click make changes to the same, right-click the toolbar, and click **Insert and Stay**.

Review the following fields:

**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** - Indicates 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.

For the chunk size and chunk data load timeout fields, the default values for each type of import schedules are as below

<table>
<thead>
<tr>
<th>Type of import schedule</th>
<th>Default Chunk Size value</th>
<th>Default Chunk Data Load Timeout value</th>
</tr>
</thead>
<tbody>
<tr>
<td>host asset</td>
<td>2500</td>
<td>300</td>
</tr>
<tr>
<td>host detection</td>
<td>50</td>
<td>300</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>1000</td>
<td>300</td>
</tr>
</tbody>
</table>

By default the Qualys VMDR subscription includes the Standard API service level. For the default Qualys API rate limits, refer to [https://www.qualys.com/docs/qualys-api-limits.pdf](https://www.qualys.com/docs/qualys-api-limits.pdf).

**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. You can also create detection event rules for creating change request in the ServiceNow Change Request.

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

There are two types of detection event rules that you can create.

- **One-to-One Rules:** The one-to-one Rules create a separate vulnerability task for each detection. You must set the one-to-one detection event rules for creation of grouping rules.

- **Grouping Rules:** The Grouping Rules use the vulnerability tasks created by the one-to-one rules and group the tasks based on different criteria.

**One-to-One Rules**

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

**Note:** We have created a separate destination table: **Qualys - VMDR Task** for the Qualys VMDR vulnerabilities. However, you can change the destination table to create a incident task or request task.

You can use the **Copy this Rule** option to clone the detection rule, modify the required field, and save the rule with a new name. See **Clone a detection rule**.
Review the existing values in the fields and modify as required:

**Source table** - Select the source table from where the detections are retrieved, that is, host detection table.

**Destination table** - Select **Qualys - VMDR Task** from the list of tables. This table is created for Qualys VMDR vulnerabilities.

For change request creation, select **Change Request** in the Destination table.
**Description** - Enter description for detection event rule.

The **Trigger Criteria** tab defines when this detection event rule runs.

**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.

**Trigger when** - 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.
For change request creation, the **Trigger Criteria** can be set as displayed in the following image:

![Trigger Criteria Image](image)

The **Assignment** tab defines how the vulnerability tasks are assigned once this detection event rule is triggered.

- If the **Assignment group based on ServiceNow Assignment Rules** is selected, the tasks are assigned based on the rules set in the **Reprocess the detection event rules**.

- If the **Assignment based on Detection Event Rule** is selected, you can select a value in the Assignment Group field. This assignment group will be applicable only for this rule.

- If the **Assignment based on Group by** field is selected, you can select a value in the Assignment Group field. This assignment group will be applicable only for this rule.

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.

![Image of field mappings](image)

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.

**Grouping Rules**

With grouping rules, you can group individual vulnerability tasks in a group based on different criteria. This results in reducing the number of tasks making the remediation easier.

To define the grouping rules, you must have one-to-one detection rules configured in Qualys Core. The grouping rules use the tasks from the Qualys - VMDR Task table and group them based on the rules that are defined.

Go to **Configuration > Detection Event Rules > Grouping Rules** to view the grouping rules that are available by default. However, you can update an existing rule or create a new rule.

![Image of grouping rules](image)

You can use the **Copy this Rule** option to clone the detection rule, modify the required field, and save the rule with a new name. See **Clone a detection rule**.
Review the existing values in the fields and modify as required:

Source table - Select the Qualys - VMDR Task table, where the tasks are created when the one-to-one detection rules are triggered.

Destination table - Select Qualys - VMDR Task Group. This is where the group task are created when this rule is triggered.

For change request creation, select Change Request in the Destination table.

The Trigger Criteria tab defines the condition in which the detection event rule is triggered.

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.
The **Grouping** defines how grouping is performed.

<table>
<thead>
<tr>
<th>Trigger Criteria</th>
<th>Grouping</th>
<th>Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grouping Configuration</td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
</tr>
</tbody>
</table>

**Group by** - Select which field from the Source table should be used as a criteria for grouping the tasks. You can select a criteria for grouping from the list.

You can define up to 4 criteria for grouping.

For details, on how the task grouping works, see **Example of Grouping**.

**Note:** Once you select a value in the Group by field, you cannot edit the value in the field. To change value in the Group by field, click **Clear Group By Fields**. This clears values in the Group by field.

The **Clear Group By Fields** option is available only if you have the required privileges.
You can also define when the task grouping should be stopped. For example, the following image displays that the task should not be included in a group if the state of the task matches any of the selected values.

The Assignment tab defines how the assignment groups are assigned.

- If the Assignment group based on ServiceNow Assignment Rules is selected, the tasks are assigned based on the rules set in the Configure Assignment Rules.

If the Assignment based on Detection Event Rule is selected, you can select a value in the Assignment Group field. This assignment group will be applicable only for this rule.

If the Assignment based on Group by field is selected, you can select a value in the Assignment Group field. This assignment group will be applicable only for this rule.

Click Submit to create a new detection event grouping rule.

Detection Event Field Maps

Once the detection event rule is created, add field mappings. Click the detection event group rule that you created, and go to Detection event field maps.

You must add the following field mappings:
Example of Grouping
This example presents how the Group by feature works. The grouping criteria is defined as:
- **Group by:** Configuration Item.Support Group
- **Then group by:** Configuration Item.Business Criticality
- **Then group by:** Configuration Item.Operating System

There are 12 VMDR tasks with unique Configuration Item categorized as:
- Configuration Item support groups: Group A, Group B, and Group C
- Configuration Items with criticality: High and Low
- Operating Systems: Windows Server 2008 R2, RedHat, and Windows 11 22h02

The following scenarios explain how the task grouping is created. This explains how the task groups are created in this example.

The tasks are first grouped by support groups as it is the first grouping criteria.

**Scenario 1: Support Group A**

Out of 12 VMDR tasks, the following four tasks belong to Configuration Item Group A.


In this case, the following task groups will be created:

<table>
<thead>
<tr>
<th>Group</th>
<th>Tasks included</th>
</tr>
</thead>
</table>

**Scenario 2: Support Group B**

Out of remaining tasks, the following two tasks belong to Configuration Item Support Group B.


In this case, the following task group will be created:

<table>
<thead>
<tr>
<th>Group</th>
<th>Tasks included</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMDRGRPTSK0004</td>
<td>VMDRTSK0005, VMDRTSK0006</td>
</tr>
<tr>
<td>VMDRTSK0005</td>
<td></td>
</tr>
<tr>
<td>VMDRTSK0006</td>
<td></td>
</tr>
</tbody>
</table>

**Scenario 3: Support Group C**

Remaining 6 tasks belong to Configuration Item support group C.

VMDRTSK0007 - CI.Support Group = Support Group C, AND a Business Criticality of High, AND a CI Operating System of Windows 11 22h02


VMDRTSK0012 - CI.Support Group = Support Group C, AND a Business Criticality of High, AND a CI Operating System of Windows 11 22h02

In this case, the following task groups will be created:

<table>
<thead>
<tr>
<th>Group</th>
<th>Tasks included</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMDRGRPTSK0005</td>
<td>VMDRTSK0007, VMDRTSK0012</td>
</tr>
<tr>
<td>VMDRGRPTSK0006</td>
<td>VMDRTSK0008, VMDRTSK0010</td>
</tr>
<tr>
<td>VMDRGRPTSK0007</td>
<td>VMDRTSK0009</td>
</tr>
<tr>
<td>VMDRGRPTSK0008</td>
<td>VMDRTSK0012</td>
</tr>
<tr>
<td>VMDRGRPTSK0009</td>
<td></td>
</tr>
</tbody>
</table>
Reprocess the detection event rules
For importing new vulnerabilities, you need to process one-to-one detection rules manually and subsequently the grouping rules also need to be processed again.

To reprocess the grouping rules and one-to-one rules manually, in the detection event rule, click Reprocess Detection Event.

The Reprocess Detection Event option is available only if you have the required privileges. If you cannot view this option, contact your ServiceNow administrator.

Clone a detection rule
You can create a clone of a grouping rule or one-to-one rule. Click Copy this Rule to create a copy of the rule with all the defined settings along with detection event field maps.

You can provide a new name or save the rule with the default name. In this case, prefix COPY is added to the existing name.

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.

The following image displays the assignment rules available by default.
For example, the assignment rule for the Windows team:

The assignment rule criteria for cloud assets:
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, 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.

**Examples of SLA definitions**

SLA based on Asset Risk Score
SLA definition for Internet-facing assets
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.

Configure Patch Deployment Settings

You can configure settings for the patch deployment jobs, such as, maximum number of assets that can be included in the patch deployment job, percentage of completion that can be considered for job completion.

To configure Patch job deployment, go to Qualys Core > Configuration > General Settings.

- Percentage of completed items to consider Patch Deployment completed - If the percentage of assets where the patch job is deployed reaches the defined number, the patch job is considered as completed.

- Maximum Number of Assets Per Job - Define the number of assets to be included in a single patch deployment job. For example, this field is set to 50. If there are 100 assets per change ticket, two patch jobs are created for 50 assets each to ensure that only specific number of assets are added to the patch jobs.

- Duration Past Start Date to Auto Complete - The time elapsed after the patch job has started. After the time defined in this field, the patch job is considered as stale and the state of the patch job changes to Completed - Stale.
The default settings are available in the **Patch Deployment Configuration**. However, you can modify the values and click **Update**.

**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 in the main pane. The **Personalize List Columns** pop-up appears.

![Image of 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.

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

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

**In Summary**
- **Hosts/Assets**: View details of assets and match or create CI records.
- **VMDR Task Groups**: View details of vulnerability task groups created.
- **VMDR Tasks**: View details of all vulnerability tasks created.
- **Launch a VM Scan**: Launch a VM scan from Qualys VMDR application.
- **Exceptions**: View details of initiating exception request and approval workflow.
- **False Positive**: View details of initiating false positive request and approval workflow.
- **Scan Executions**: List of scan executions that are initiated from this application.
- **Detections**: List of all vulnerability detections categorized based on status.
- **Qualys Patch Management Workflow**: View change request management process.
- **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 Qualys VMDR 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** - The host or asset is categorized as unmatched CI in one of the following conditions:
  - IP address or host that is scanned in Qualys is not available in CMDB
  - IRE scripts attributes do not match
  - Duplicate records of IP address or host are found in CMDB.

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, IP address, 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.

To find the CI, a script is used that is available under **System Definition - Script Includes** - QualysAssetIRE.

```js
IRE CMDB_CI_hardware cirteria: (Script Includes, under System Definition & look for QualysAssetIREvar ireData = {
  items: [{
    className: "cmdb_ci_hardware",
    values: {
      os: host.getValue('operating_system') || undefined,
      name: host.getValue('name') || undefined,
      asset_tag: host.getValue('asset_id') || undefined,
      dns_domain: host.getValue('domain') || undefined,
      fqdn: host.getValue('fqdn') || undefined,
      ip_address: host.getValue('ip_address') || undefined,
    }
  }]
});
```

You can modify the IRE parameters and the script with additional parameters if you have required privileges.
**Note:** Ensure that you have defined the Hardware Rule in the Identification and Reconciliation Engine and the criteria to be matched are set to true.

To check the hardware rule, go to **Identification/ Reconciliation > CI Identifiers > Hardware Rule.**

![Hardware Rule Interface](image)

**Note:** The CI matching can be enhanced with the Qualys CMDB Sync app available on the ServiceNow store. The Qualys CMDB Sync app is part of Qualys CyberSecurity Asset Management (CSAM). 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 or task groups are created for the host detections that are imported. You can view and update the vulnerability tasks that are created.
VMDR 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.

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.

You can check 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.

Launch a VM Scan
You can launch vulnerability scans from the Qualys VMDR 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.

  ![Launch a Qualys VM Scan](image)

  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 Qualys VM Scan](image)

- For multiple vulnerability tasks

![Vulnerability Tasks](image)

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

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

For effective management of vulnerability tasks, you can group the individual vulnerability tasks based on multiple factors, such as, Vuln Severity, multiple Qualys Knowledgebase fields, Qualys Detection Score (QDS), QDS Severity, Asset Risk Score (ARS), Asset Criticality Score (ACS), Operating System, Qualys Asset Tags, Assignment Group, Configuration Item, and so on. Qualys VMDR creates tasks groups based on the Grouping Rules configured in Qualys Core and assigns them to the remediation team based on the defined assignment rules.

Vulnerability task grouping provides better visibility to the remediation owners to track remediation with fewer tasks and quicker remediations, organizes vulnerability tasks, and analyze them in bulk.

You can view vulnerability task groups that are assigned to you and your group as a remediation owner.

For each task group, you can view the state and priority of the task group, the assignment group, the number of vulnerability tasks included in the task group, percentage of remediation, and so on.
For each vulnerability task group, you can view the following details:

You can view the basic information of a vulnerability group task, such as, task number and status, assignment group and priority.

The **Remediation Status** provides remediation status as number of tasks, including and excluding the deferred tasks and percentage of tasks remediated.

The **Group Definition** displays the detection event rule that was applied for creating this group task.
The task groups also display details about the deferred and resolved tasks, host assets involved in the group task, QIDs associated with the this group task.

**Deferred Tasks**

**Resolved Tasks**

**Host Assets**
QIDs

For the tasks to be grouped under a specific group, you can configure the detection rules for vulnerability task groups in Qualys Core. Infrastructure and Security teams can view all the tasks.

General Settings

You can define the default approval behavior for the exception management and false positive reporting process.

For exception management and false positive reporting, you need three approvals - first from the infrastructure/application group and two security approvals from security team and security board. However, you can modify this to the customized approval.

Approval Configuration Default

The Approval Configuration Default tab | Infrastructure / Application Owner Approval Defaults section, define the following fields:

Infrastructure / App Owner Approval Type - Select Vulnerability Task Field for the built-in approval process based on the field value from a vulnerability task.
Select **Custom** to disable the built-in approval step for Infrastructure / Application Owner Approval.

**Approval Group: Infrastructure / App Owner Task Field** - Select a field to use as a default for the Infrastructure Approval, when utilized.

**Infrastructure/ App Owner Default Approval Group** - Select the group to use for Infrastructure Approval if the automated selection does not resolve to a valid group.

In the **Security Approval Defaults** section, define the group of users responsible for security review of a vulnerability task.

In the **Security Approval Defaults** section, define the group of users responsible for security review of a vulnerability task.

- **Approval Group: Security Team** - Group of users responsible for approval whenever a Vulnerability Task requires review by the Security Team.

- **Approval Group: Security Board** - Group of users responsible for approval whenever a Vulnerability Task requires review by the Security Board.

**Exception Process**

In the Exception Process tab, select the template that should be used by default when the state of the vulnerability task changes to Exception - Identified.

You can select the template from the available templates or create a new template that includes the exception reason.

**False Positive Process**

In the Exception Process tab, select the template that should be used by default when the state of the vulnerability task changes to Exception - Identified.

You can select the template from the available templates or create a new template that includes the exception reason.
Exceptions
The remediation owners can seek exception for an individual vulnerability task or for a vulnerability task group if the vulnerability cannot be remediated for various reasons, such as, not enough downtime available, patch not available, or applications not compatible with updates.

This section presents how a remediation owner can initiate an exception, inputs that needs to added while requesting exception approval and the state of the ticket during exception management. This section also presents how the approver can approve or reject the exception requested.

Exception Initiation
To initiate an exception:

Go to VMDR Tasks or VMDR Task Groups > Assigned to My Group (Open).
Click an open task.
Right-click in the title bar, and click Exception - Initiate.

The State is changed to Exception - Identified.
In the vulnerability task, scroll down to the Exception tab.
In the Exception tab, select Exception Business Risk and enter exception reason in the Reason for exception.

Click Approval Configuration tab, select the approval group in the Infrastructure/ App Owner Approval Group.

Click Exception - Request Approval.

The State changes to Exception - Awaiting Approval.

The exception is submitted for approval. The approver group approves or rejects the exception. See Exception Approval.

After the exception is approved or rejected, go to the task for which exception was requested, and click VMDR Approvals tab.

You can view the approver and the state of exception approval.
You can also view the additional approvers after initial application infrastructure approval. The other approvers need to follow the exception approval workflow.

If the approver rejects the exception, it reflects in the task record | VMDR Approvals tab.

Exception Approval

Once the exception is requested, the designated approvers or approver group members can approve or reject the exception based on the business risks involved and reason for exception. The following sections present the workflow for exception approval and rejection.

The exception request could include three or four stages of approvers and can be approved/rejected by any of the assigned group members.

**Note:** This workflow is available only for the approver groups.

Approval Workflow

Log on to the application and go to Qualys VMDR.

Click **Exceptions | Pending My Approval.**

The right pane displays the exceptions requested for approval.

Click the **State** column.
Click the icon besides the **Approving** field | **Open Record**.

The task record opens. In the task record, **Exception** tab, add dates and exception recommendation, and click **Update**.
You are back on the approval record.

Click **Approve**.

**Rejection Workflow**

Log on to the application and go to Qualys VMDR.

Click **Exceptions | Pending My Approval**.

The right pane displays the exceptions requested for approval.

Click the **State** column.
Click the icon besides the **Approving field** | **Open Record**.

The task record opens. In the task record, add reason for exception rejection in the **Comments** field, and click **Reject**.

A message is displayed that confirms the exception rejection.
False Positive

A remediation owner can mark a vulnerability task or a vulnerability task group as false positive in a scenario where the vulnerability has already been remediated. The remediation owner provides the reasons and required artifacts while confirming the false positive request so that the approver team can investigate for request approval.

Once a vulnerability is marked as false positive, it goes through an approval process by assigned approvers. If the false positive request is approved, no further action is needed. If the false positive request is rejected, the remediation owner needs to follow the remediation steps.

You can track the State of the vulnerability task and VMDR Approvals tab to understand the status.

False Positive Initiation

To initiate a false positive request:

Go to VMDR Tasks or VMDR Task Group > Assigned to My Group (Open).

Click an open task.

Right-click in the title bar, and click False Positive - Initiate.
The **State** is changed to **False Positive- Identified**.

In the vulnerability task, scroll down to the **False Positive** tab.

In the **False Positive** tab, enter a reason for marking this vulnerability task as false positive.

Click **Approval Configuration** tab, and select the approval group in the **Infrastructure/ App Owner Approval Group**.

Click **False Positive- Request Confirmation**.

The **State** changes to **False Positive- Awaiting Approval**.
The false positive request is submitted for approval. The approver group approves or rejects the false positive request. See False Positive Approval.

After the false positive request is approved or rejected, go to the task for which false positive request is sent, and click VMDR Approvals tab.

You can view the approver and the state of approval. You can also view the additional approvers after initial application infrastructure approval. The other approvers need to follow the false positive approval workflow.

If the approver rejects the false positive request, it reflects in the task record | VMDR Approvals tab.

If all the approvers approve the false positive request, the state of the task changes to False Positive - Confirmed.

False Positive Approval

Once the false positive request is initiated, the designated approvers or approver group members can approve or reject the false positive request based on the proofs provided. The following sections present the workflow for false positive approval and rejection.

Note: This workflow is available only for the approver groups.

Approval Workflow

Log on to the application and go to Qualys VMDR.
Click **False Positive | Pending My Approval.**
The right pane displays the false positive requested for approval.

Click the State column.
Click the icon besides the **Approving** field | **Open Record.**

The task record opens. In the task record, **False Positive** tab to view the reason why a remediation owner has marked this as false positive.
You are back on the approval record.

Click **Approve**.

A message is displayed that confirms the approval.

Alternatively, you can add a message and click **Reject**.
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.

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.

Qualys Patch Management Workflow
With Qualys VMDR application, automatic change tickets are created to track the remediation action for the detected vulnerabilities. The change requests can create automated patch deployment jobs in Qualys Patch Management, which helps to reduce risk faster.

Note: This application is available for remediation owners.
The change management process included the following steps:

- When a vulnerability is detected, it is pulled in the Qualys VMDR with the detection event rule and a vulnerability task is created.

- With a detection event rule for change requests, a new change ticket is created with vulnerability details and CIs associated with it. This is applicable if the CIs are part of the ServiceNow CMDB.

- When the change is approved, a deployment job is created within ServiceNow and later in the Qualys Patch Management.

- The job status and result will then be monitored, and the updates will be logged into the change ticket under the deployment job.

- Once the job is created in Qualys Patch Management, the status of the change ticket is updated.

- After the vulnerability is remediated and the next VM scan runs, it will close the vulnerability task in ServiceNow and the change manager can then review the change and close the change ticket manually.

**Change Request - Review, Assessment and Approval**

In the application navigator, go to **Change Request > New**.

Click the change request in a New state.

In the **Schedule** section, set the **Planned start date** and **Planned end date**.
The **Affected CIs** tab displays the CIs that were automatically added based on VMDR tasks associated with this change request.

The **Qualys - VMDR Tasks** tab displays associated VMDR tasks.

In the **State** field, select **Assess** state, and click **Save**.

The **Qualys PM - Deployment Jobs** tab displays the patch deployment jobs that are created.
**Note:** A unique job is created for each connector. For each connector, up to 50 hosts can be added to one patch deployment job.

### Review Patch Jobs with Errors

Click the patch job with error state to view the job details. Click the **Log** tab to review the possible errors. The possible cause of the error is some or many hosts that do not have UUID value required for patch deployments.

Scroll down to view the entries indicating that have no UUID in ServiceNow stored for the host.

You can perform two actions:

- To ignore a specific entry for patch deployment, right-click the entry, and click **Cancel - Ignore**. To ignore multiple entries, select the corresponding check boxes, and select **Cancel - Ignore** from the list of available action.
Check whether UUID or patching is enabled on the host since the job was created or after the hosts were last imported into ServiceNow. Click **Check UUID in Qualys**.

When checking UUID in Qualys is completed, the status changes either to Pending - Start Date or Pending - Task Approval based on whether the task (Change Request) has been approved or not.

Navigate back to your change request > Approvers tab, to review the approvals needed and approve it.

Select the check box for the approver, and click **Approve** from the list of available actions.

The change request is approved and the state changes to **Scheduled**.
View Patch Deployment Jobs in Qualys Patch Management

You can view the status of patch management job in Qualys Patch Management application.

Go to the patch job item, and in the Configuration tab, click View in Qualys.

![Image of patch job configuration](image)

Note: If the View in Qualys button is not available:
- Qualys Job ID is not populated and there is no job in the Qualys application.
- The connector is not configured with Web Portal URL. See Configure Connection to Qualys Applications.

You are redirected to the Qualys Cloud Platform > Patch Management application > patch job.

![Image of Qualys Cloud Platform](image)

If you have not logged on to the application already, log on to Qualys Cloud Platform. Then, go back to the patch job item, and click View in Qualys. You are directed to the patch job in Qualys.
Create a new patch job manually

A remediation owner can also create a patch job in the Change Request.

Go to Change Request > Open, click a change request in Assess or Scheduled state.

In the Change Request > Qualys PM - Deployment Job, open the job in Error status.

In the Configuration tab, click Create Patch Job.

Once the job is created, the state of the deployment job changes to Waiting - For Next Scheduled Status Check, and the Qualys Job ID is updated.

The state and patch information for each job item is updated periodically (every 4 hours) by the automated status checking.

Refresh the Patch Job Status

To refresh the patch job status manually, go to the patch job item, and in the Configuration tab, click Refresh Status.
The system refreshes the status at a regular interval automatically. Once a particular percentage (Configured in the General Settings of the Qualys Core application) of patch deployment jobs items are completed, the status of the patch job changes to Complete or Complete - Partial depending on the number of items completed.
Reports and Dashboards

Go to Qualys VMDR App > **Overview**.

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

![Detections Tab Example](image)

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 Qualys VMDR application.

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**.
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.