



Qualys VMDR for ServiceNow

User Guide

March 6, 2023

Copyright 2022- 2023 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100



Table of Contents

About this guide.....	3
About Qualys	3
Qualys Support	3
Welcome to Qualys VMDR for ServiceNow	4
Qualys VMDR	4
Key Features	4
Pre-requisites	5
User Roles and Permissions	5
Get Started	9
Install the App	9
Upgrade the App	10
Qualys Core	13
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	44
Hosts/Assets	44
Find CI	45

Create CI	48
View and Manage Vulnerability Tasks	48
VMDR Tasks	49
Launch a VM Scan	53
VMDR Task Groups	56
General Settings	59
Approval Configuration Default	59
Exception Process	60
False Positive Process	60
Exceptions	61
Exception Initiation	61
Exception Approval	63
False Positive	67
False Positive Initiation	67
False Positive Approval	69
Scan Executions	72
Detections	72
Qualys Patch Management Workflow	72
Change Request - Review, Assessment and Approval	73
Review Patch Jobs with Errors	75
View Patch Deployment Jobs in Qualys Patch Management	77
Create a new patch job manually	78
Refresh the Patch Job Status	78
Reports and Dashboards	80
Create a new report	82
Add a Report to Dashboard	88
Share the report	90
KnowledgeBase	91
Debugging and Troubleshooting.....	92
How to debug	92
Configure logging	92
View Logs	92
Known Issues	93

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:

Role	Permissions
x_qual5_core.admin	Administrative user of the application. Create, Write, Read, and Delete access to all aspects of the application.
x_qual5_core.kb_read	Read access to the Qualys - KnowledgeBase records.
x_qual5_core.create_ci_from_host	Can see the "Create CI" UI action from host records.
x_qual5_core.api_data_receiver	Grants access to any Data Receiver API Endpoints that are available "globally" 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. # API Endpoints - /api/x_qual5_core/v1/data_receiver/{connector_sys_id}/vmdr/host_asset - /api/x_qual5_core/v1/data_receiver/{connector_sys_id}/vmdr/host_detection
x_qual5_core.connector_user	This role grants access to create, modify and delete Connector Records.
x_qual5_core.qualys_fim_incident_user	Has access to FIM Incidents and information related to them.
x_qual5_core.general_settings	Has access to read/write the General Settings values of the application.
x_qual5_core.import_user	Has access to the import_set tables for debugging and API Calls.
x_qual5_core.host_user	Has Read access to Host Asset Records and related information such as Asset Tags and Asset Groups
x_qual5_core.launch_vm_scan	Role required to see / interact with Launching VM Scans
x_qual5_core.patch_deployment_user	This role grants access to view and management patch deployments for Change Request
x_qual5_core.view_vm_scan	This role grants access to view VM Scans and related data such as Option Profiles and Scanner Appliances

Role	Permissions
x_qual5_core.user	<p>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</p> <p># Access to read the following</p> <ul style="list-style-type: none"> - Qualys Tags / Asset Tags - Detection Event Rules <ul style="list-style-type: none"> - Specifically the Name, and Description attributes (and nothing else) - Qualys Asset Groups - Basic Information to Connectors, such as Name. - Access to ancillary functionality used by various functions of other applications.
x_qual5_core.qualys_knowledgebase_user	This role grants READ Only access to the Qualys KnowledgeBase

The following table presents the user groups and associated roles and permissions for Qualys VMDR application.

Role	Permissions
x_qual5_vmdr.dashboard_viewer	Can Access / View Dashboard from VMDR Application
x_qual5_vmdr.admin	Can create/read/write/delete items within this application scope.
x_qual5_vmdr.exception_approver	Can read vulnerability tasks where they are the "Exception approver" or if the task is assigned directly to them.
x_qual5_vmdr.false_positive_approver	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.

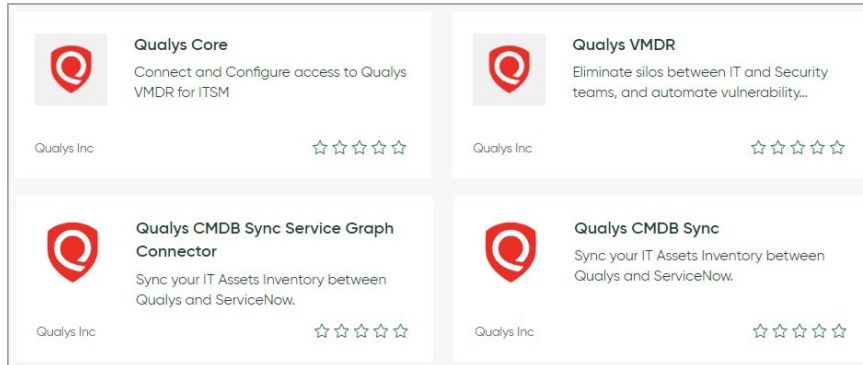
Role	Permissions
x_qual5_vmdr.remediation_owner	<p>This is the role intended for Remediation Owners that need to perform work on VMDR Task or VMDR Task Group records that belong to a Support/Assignment group that they are a member of.</p> <p>## VMDR Task</p> <ul style="list-style-type: none">- Grants Read/Write access to VMDR Tasks and Related Functions where the logged in user is a member of the Assignment Group for that Task <p>## VMDR Task Group</p> <ul style="list-style-type: none">- 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
x_qual5_vmdr.vulnerability_analyst	<p>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.</p> <p>## VMDR Task</p> <ul style="list-style-type: none">- Grants Read/Write/Create access to all VMDR Tasks and Related Functions <p>## VMDR Task Group</p> <ul style="list-style-type: none">- Grants Raad/Write/Create access to all VMDR Task Group and Related Functions

Get Started

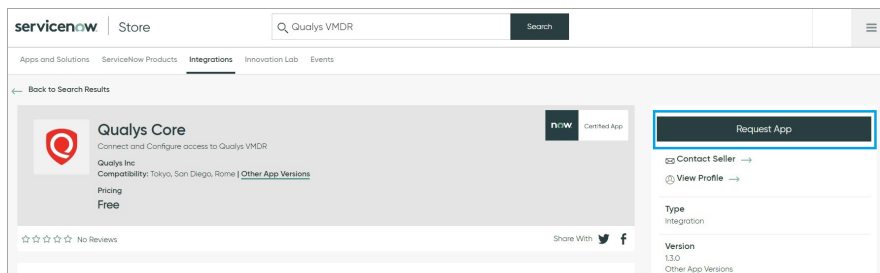
Follow the steps to install Qualys Core and Qualys VMDR applications.

Install the App

Visit the [ServiceNow Online Store](#) and search for **Qualys** apps.

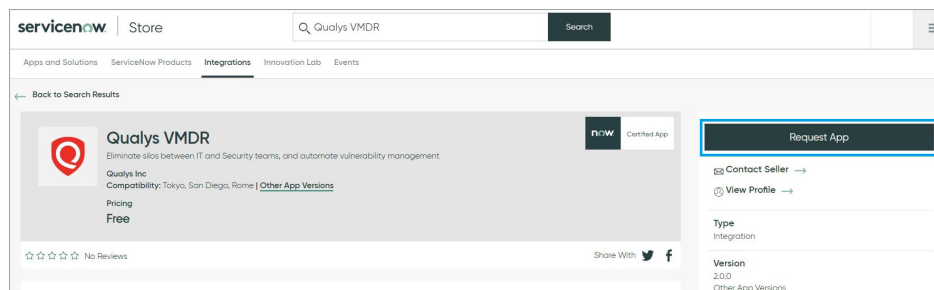


- Go to [Qualys Core](#) app, and click Request App.



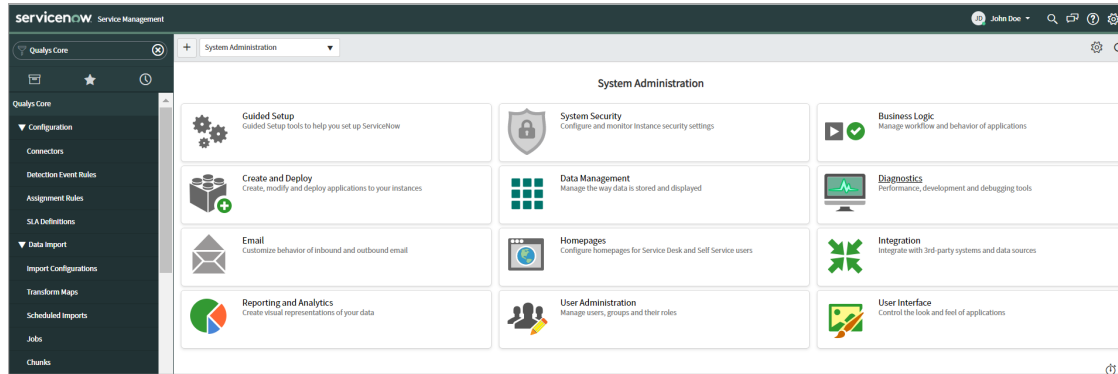
Your Qualys representative will enable the application for you if you have Qualys VMDR subscription. The app then appears in the “Downloads” list of your instance. Click “Install” to start install the app.

- 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:



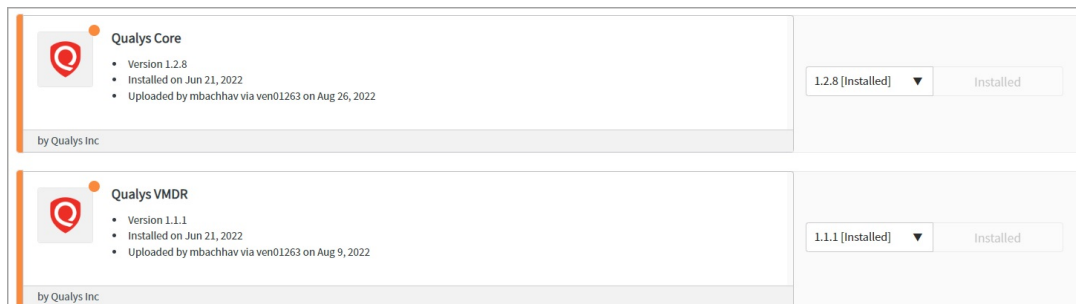
Note: The options in the Qualys Core and Qualys VMDR applications that you can view are different based on the user group to which you belong. For information on user roles, see [User Roles and Permissions](#).

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**.

<div>Qualys Core<ul style="list-style-type: none">• Version 1.3.103• Created on Feb 14, 2023• Uploaded by nate.anderson via ven04911 on Feb 14, 2023<div>by Qualys Inc</div><div>Show More</div></div>	<div>1.3.103 ▼</div> <div>Update</div>
<div>Qualys VMDR<ul style="list-style-type: none">• Version 2.0.1• Created on Feb 03, 2023• Uploaded by nate.anderson via ven04911 on Feb 3, 2023<div>by Qualys Inc</div><div>Show More</div></div>	<div>2.0.1 ▼</div> <div>Update</div>

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.

Edit User Launch Help

Information: Users must be employees or contractors of your company who are bound to confidentiality obligations as protective as those contained in the Qualys® Service Agreement.

General Information **User Role**

Locale **User Role**

User Role: *

Allow access to: ☐ GUI ☒ API

Business Unit: * [New Business Unit](#)

User configurations to transfer:

Changing the user's business unit or user role will result in the **removal of personal configurations and asset groups from the user**. Select the options below if you wish to transfer those configurations and asset groups to the user's Manager/Unit Manager. [Learn more](#)

☐ Transfer personal configurations
Includes option profiles, report templates, scheduled tasks, distribution groups, search lists, web applications and compliance policies.

☐ Transfer Asset Groups
If not selected, configurations may become inactive (e.g. report templates, schedules) and you'll need to manually update them.

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 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/>.

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.

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:

-- choose field --
 -- oper --
 -- value --

Collection

Default: FIM Incident Event Import - All
 Default: FIM Incident Import - All

>
 <

Import Configurations List

Qualys ITSM Demo

Default: Host Asset Import - All
 Default: Host Detection Import - All
 Default: Knowledge Base Import - All
 Default: Option Profiles - All
 Default: Scanner Appliance - All

Name Default: Host Asset Import - All

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

The screenshot displays a configuration window with the following elements:

- Filter Section:** Includes buttons for "Add Filter", "Run filter", and a help icon (?). Below these are three dropdown menus labeled "-- choose field --", "-- oper --", and "-- value --".
- Collection List:** A search bar with a magnifying glass icon is positioned above a list of collections:
 - Default: Host Asset Import - All
 - Default: Host Detection Import - All
 - Default: Knowledge Base Import - All
 - Default: Option Profiles - All
 - Default: Scanner Appliance - All
- Import Configurations List:** A list titled "Qualys ITSM Demo" containing:
 - Default: FIM Incident Event Import - All (highlighted with a blue background)
 - Default: FIM Incident Import - All
- Navigation and Action:** Between the two lists are right (>) and left (<) arrow buttons. At the bottom are "Cancel" and "Save" buttons.
- Status Bar:** At the very bottom, it reads "Name Default: FIM Incident Event Import - All".

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.

Import Configurations		Active
<input type="checkbox"/>	Default: FIM Incident Event Import - All	● true
<input type="checkbox"/>	Default: FIM Incident Import - All	● true
<input type="checkbox"/>	Default: Host Asset Import - All	● true
<input type="checkbox"/>	Default: Host Detection Import - All	● true
<input type="checkbox"/>	Default: Knowledge Base Import - All	● true
<input type="checkbox"/>	Default: Option Profiles - All	● true
<input type="checkbox"/>	Default: Scanner Appliance - All	● true

If you want to configure Qualys Core to work with Qualys VMDR, the following import configurations are available by default.

- Host Asset 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

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.

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.

Name	Active	Connector	Source Table	Update Frequency (minutes)	Latest Change Synced	Updated
Default: FIM Incident Event Import - Every 1 Min	true	(empty)		30	(empty)	2022-09-06 22:32:36
Default: FIM Incident Import - Nightly	true	(empty)		30	(empty)	2022-09-08 20:00:21
Default: Host Asset Import - Nightly	true	(empty)		30	(empty)	2022-09-10 20:00:50
Default: Host Detection Import - Nightly	true	(empty)		30	(empty)	2022-06-21 02:06:08
Default: Knowledge Base Import - Nightly	true	(empty)		30	(empty)	2022-09-10 00:38:55
Default: Option Profiles - Every 4 hours	true	(empty)		30	(empty)	2022-08-09 00:00:30
Default: Scanner Appliance - Nightly	true	(empty)		30	(empty)	2022-08-09 01:00:20

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

Type of import schedule	Default Chunk Size value	Default Chunk Data Load Timeout value
host asset	2500	300
host detection	50	300
KnowledgeBase	1000	300

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>.

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

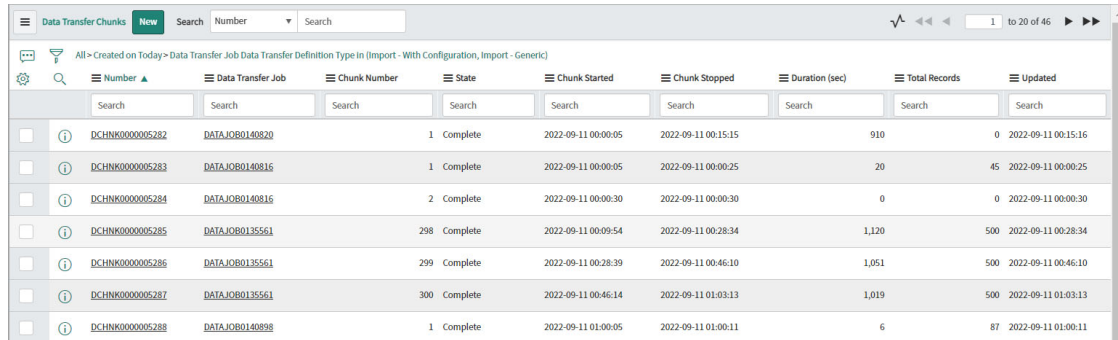
After scheduled import execution, data transfer jobs are processed. You can view details of data transfer jobs - job number, status, start and stop time, completion percentage, associated connector, and so on.

Number	Data Transfer Definition	State	Job Started	Total Records	Percent Complete	Job Stopped	Duration (seconds)	Updated
DATAJOB0135561	Default: FIM Incident Event Import - Eve...	In Progress	2022-09-08 05:07:55		99%	(empty)		2022-09-11 11:01:30
DATAJOB0140816	Default: Option Profiles - Every 4 hours	Complete	2022-09-11 00:00:05	45	100%	2022-09-11 00:00:35	30	2022-09-11 00:00:35
DATAJOB0140820	Default: Knowledge Base Import - Nightly	Complete	2022-09-11 00:00:05	0	100%	2022-09-11 00:15:20	915	2022-09-11 00:15:20
DATAJOB0140898	Default: Scanner Appliance - Nightly	Complete	2022-09-11 01:00:05	87	100%	2022-09-11 01:00:20	15	2022-09-11 01:00:20
DATAJOB0141125	Default: Option Profiles - Every 4 hours	Complete	2022-09-11 04:00:00	45	100%	2022-09-11 04:00:20	20	2022-09-11 04:00:20
DATAJOB0141431	Default: Option Profiles - Every 4 hours	Complete	2022-09-11 08:00:05	45	100%	2022-09-11 08:00:25	20	2022-09-11 08:00:25

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.

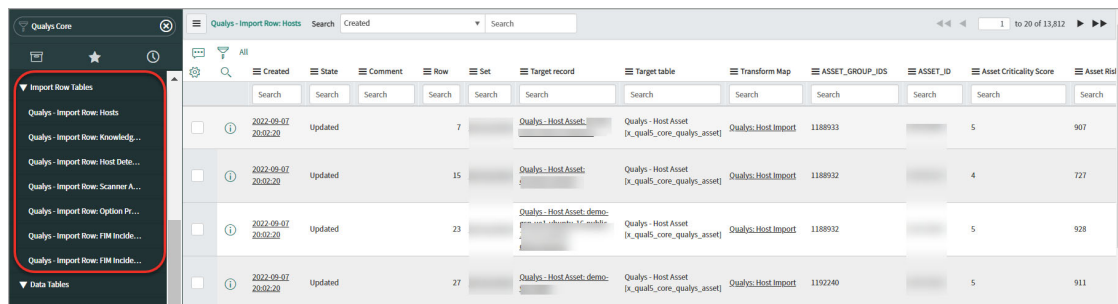


	Number	Data Transfer Job	Chunk Number	State	Chunk Started	Chunk Stopped	Duration (sec)	Total Records	Updated
<input type="checkbox"/>	①	DCHNK0000005282	DATAJOB0140820	1 Complete	2022-09-11 00:00:05	2022-09-11 00:15:15	910	0	2022-09-11 00:15:16
<input type="checkbox"/>	①	DCHNK0000005283	DATAJOB0140816	1 Complete	2022-09-11 00:00:05	2022-09-11 00:00:25	20	45	2022-09-11 00:00:25
<input type="checkbox"/>	①	DCHNK0000005284	DATAJOB0140816	2 Complete	2022-09-11 00:00:30	2022-09-11 00:00:30	0	0	2022-09-11 00:00:30
<input type="checkbox"/>	①	DCHNK0000005285	DATAJOB0135561	298 Complete	2022-09-11 00:09:54	2022-09-11 00:28:34	1,120	500	2022-09-11 00:28:34
<input type="checkbox"/>	①	DCHNK0000005286	DATAJOB0135561	299 Complete	2022-09-11 00:28:39	2022-09-11 00:46:10	1,051	500	2022-09-11 00:46:10
<input type="checkbox"/>	①	DCHNK0000005287	DATAJOB0135561	300 Complete	2022-09-11 00:46:14	2022-09-11 01:03:13	1,019	500	2022-09-11 01:03:13
<input type="checkbox"/>	①	DCHNK0000005288	DATAJOB0140898	1 Complete	2022-09-11 01:00:05	2022-09-11 01:00:11	6	87	2022-09-11 01:00:11

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.



	Created	State	Comment	Row	Set	Target record	Target table	Transform Map	ASSET_GROUP_ID	ASSET_ID	Asset Criticality Score	Asset Risk
<input type="checkbox"/>	2022-09-07 20:02:20	Updated		7		Qualys - Host Asset	Qualys - Host Asset	Qualys Host Import	1188933		5	907
<input type="checkbox"/>	2022-09-07 20:02:20	Updated		15		Qualys - Host Asset	Qualys - Host Asset	Qualys Host Import	1188932		4	727
<input type="checkbox"/>	2022-09-07 20:02:20	Updated		23		Qualys - Host Asset	Qualys - Host Asset	Qualys Host Import	1188932		5	928
<input type="checkbox"/>	2022-09-07 20:02:20	Updated		27		Qualys - Host Asset	Qualys - Host Asset	Qualys Host Import	1192240		5	911

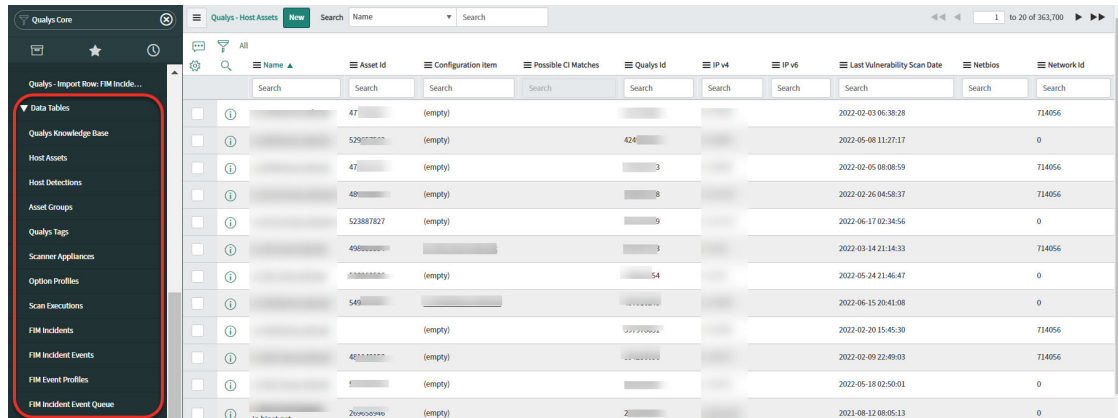
The import row tables for hosts, host detection, scanner appliance, option profiles, and knowledgebase present data imported from Qualys VMDR application.

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.



The screenshot shows the Qualys Core interface. On the left, a sidebar menu lists various data sources, with 'Data Tables' highlighted. The main area displays a table of host assets. The table has columns for Name, Asset ID, Configuration Item, Possible CI Matches, Qualys ID, IP v4, IP v6, Last Vulnerability Scan Date, Netbios, and Network ID. The data is filtered to show 10 rows out of 363,700 total records.

Name	Asset ID	Configuration Item	Possible CI Matches	Qualys ID	IP v4	IP v6	Last Vulnerability Scan Date	Netbios	Network ID
[Redacted]	47	(empty)					2022-02-03 06:38:28		714056
[Redacted]	529	(empty)	424				2022-05-08 11:27:17	0	
[Redacted]	47	(empty)	3				2022-02-05 08:08:59		714056
[Redacted]	48	(empty)	8				2022-02-26 04:58:37		714056
[Redacted]	523887827	(empty)	9				2022-06-17 02:34:56	0	
[Redacted]	496888888		3				2022-03-14 21:14:33		714056
[Redacted]	[Redacted]	(empty)	54				2022-05-24 21:46:47	0	
[Redacted]	549						2022-06-15 20:41:08	0	
[Redacted]		(empty)					2022-02-20 15:45:30		714056
[Redacted]	401111111	(empty)					2022-02-09 22:49:03		714056
[Redacted]	5	(empty)					2022-05-18 02:50:01	0	
[Redacted]	201010101	(empty)	2				2021-08-12 08:05:13	0	

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.

Name	Active	Trigger when	Description	Destination table	Order	Stop processing
Create Vulnerability Tasks for Confirmed Vulnerabilities (Sec 4 or higher)	true	Type = Confirmed and QID Severity level in (4 - High, 5 - Critical) and Qualys detection score > 70 and QID Threat Intelligence contains Cisa_Known_Exploited_Vulns and Qualys Host Qualys Asset Tags CONTAINS Critical Assets	Create a Vulnerability Task for every de...	Qualys - VMDR Task [x_qual5_vmdr_vuln_task_item]	1,000	true
Ticket Creation Policy	false	Qualys Host Qualys Asset Tags CONTAINS Internet Facing Assets and Qualys detection score > 90 or QID Threat Intelligence contains cisaknownexploitedvulns and QID Vulnerability Type = Confirmed Vulnerability	Shared Content for IT & Security to crea...	Qualys - VMDR Task [x_qual5_vmdr_vuln_task_item]	203	false
COPY - Create Vulnerability Tasks for Confirmed Vulnerabilities (Sec 4 or higher)	false	Type = Confirmed and QID Severity level in (4 - High, 5 - Critical) and Qualys detection score > 80 and QID Threat Intelligence contains Cisa_Known_Exploited_Vulns and Qualys Host Qualys Asset Tags CONTAINS PCI Scope	Create a Vulnerability Task for every de...	Qualys - VMDR Task [x_qual5_vmdr_vuln_task_item]	1,000	true
COPY - Create Vulnerability Tasks for Confirmed Vulnerabilities (Sec 4 or higher)	false	Type = Confirmed and QID Severity level in (4 - High, 5 - Critical) and Qualys detection score > 80 and QID Threat Intelligence contains Cisa_Known_Exploited_Vulns and Qualys Host Qualys Asset Tags CONTAINS PCI Scope	Create a Vulnerability Task for every de...	Qualys - VMDR Task [x_qual5_vmdr_vuln_task_item]	1,000	true
Certificate Rule with SSL Certificates QID	true	QID QID in 38116, 38142, 38167, 38169, 38170, 38171, 38172, 38173, 38174, [...]	Certificate Rule with SSL Certificates Q...	Qualys - VMDR Task [x_qual5_vmdr_vuln_task_item]		false
Internet Facing Assets	true	Qualys Host Qualys Asset Tags CONTAINS Internet Facing Assets and Qualys detection score > 85 and Qualys Host TrustRisk Criticality Score > 4 and Qualys Host TrustRisk Score > 850 and QID Severity level = 5 - Critical and Type = Confirmed and Qualys Host Qualys Asset Tags CONTAINS	Internet Facing Assets rule to Incident ...	Qualys - VMDR Task [x_qual5_vmdr_vuln_task]		false
Example: Create Problem Rule	false	QID Severity level = 5 - Critical	This is an example rule for documentatio...	Problem [problem]	100	false
Testing Incident?	true	Qualys Host Configuration item is not empty		Incident [incident]		false
Patchable Tasks	false	QID Patchable = true and Qualys Host Operating System contains Windows and Qualys detection score >= 90		Change Request [change_request]	102	false

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](#).

Detection Event Rule
New record

Detection Event Rules
The detection event rules allow specifying what records to create a record is inserted or updated on the source table specified.

- **Name:** A name to reference this rule by
- **Active:** Is this rule active or not?
- **Source table:** The source table to watch for record changes and run this rule of the Trigger Criteria are met
- **Destination Table:** The table to create a record in when this rule is triggered.
- **Destination Form View:** When enabled, will allow specifying the form view of the destination record. This is to help for scenarios when you need to show different information based on the groupings performed.
- **Description:** A long description to provide more detail about the purpose of this rule.

Name: Certificate Rule with SSL Certificates QIDs

Active: ☒

Logging level: Errors

Source table: Import Configuration: Host Detection [x_qual5_core_host_det...]

Destination table: Qualys - VMDR Task [x_qual5_vmdr_vuln...]

Source field to set to Destination Record: -- None --

Description:

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.

Detection Event Rule
Create Vulnerability Tasks for Confirmed Detections (Sev 4 or higher)

Name: Create Vulnerability Tasks for Confirmed Detections (Sev 4 or higher)

Active: ☒

Logging level: Errors

Source table: Qualys - Host Detection [x_qual5_core_host_det...]

Destination table: Qualys - VMDR Task [x_qual5_vmdr_vuln_task_it...]

Source field to set to Destination Record: -- None --

Description:

Trigger Criteria
Below you can specify the criteria in which this rule is triggered.

- Qualys VMDR Task [x_qual5_vmdr_vuln_task_item]
- Qualys VMDR Task Group [x_qual5_vmdr_vuln_task_group]
- Qualys Asset Details [x_qual5_item_app_qualys_asset_details]
- Qualys Asset Groups [x_qual5_item_app_qualys_asset_groups]
- Qualys Asset Tags

record in th Source table as they are processed.

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

Detection Event Rule
Patchable Tasks

Detection Event Rules
The detection event rules allow specifying what records to create a record is inserted or updated on the source table specified.

- **Name:** A name to reference this rule by
- **Active:** Is this rule active or not?
- **Source table:** The source table to watch for record changes and run this rule of the Trigger Criteria are met
- **Destination Table:** The table to create a record in when this rule is triggered.
- **Destination Form View:** When enabled, will allow specifying the form view of the destination record. This is to help for scenarios when you need to show different information based on the groupings performed.
- **Description:** A long description to provide more detail about the purpose of this rule.

Name: Patchable Tasks

Active: ☐

Logging level: Errors

Source table: Qualys - Host Detection [x_qual5_core_host_det...]

Destination table: Change Request [change_request]

Source field to set to Destination Record: -- None --

Description:

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:

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.

Source field	Destination field	Coalesce
sys_id	host_detection	false
cmdb_ci	cmdb_ci	false
[script]	priority	false
[script]	short_description	false
[script]	source	false
sys_id	correlation_id	true
[script]	state	false

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 tasks making the remediation easier remediation.

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.

Name	Active	Trigger when	Description	Destination table	Order	Stop processing
COPY - Group Rule Based on QDS Severity	false	Qualys Detection QDS detection score > 80 .and. Qualys Detection QDS Host TruRisk Score > 700 .and. State = Open .and. Qualys Detection Connector = Qualys Demo Account .and. Host asset Operating System contains Windows .and. QID Patchable = true	Group Tickets by QDS Severity for QDS=80...	Qualys - VMDR Task Group [x_qual5_vmdr_vuln_task_group]		false
Critical & High Vulnerability Tasks by Configuration Item	false	Configuration Item Support group is not empty .and. QID Severity level in (4 - High, 5 - Critical) .and. Qualys Detection QDS detection score > 70 .and. QID Vulnerability Type = Confirmed Vulnerability .and. Host asset Qualys Asset Tags CONTAINS Windows Assets		Qualys - VMDR Task Group [x_qual5_vuln_task_group]	100	false
Assets Tagged with Production and Tasks with Critical QDS Severity	true	Qualys Detection QDS Severity = CRITICAL .and. Qualys Detection QDS Host Qualys Asset Tags CONTAINS Production	Group Tickets by QDS Severity	Qualys - VMDR Task Group [x_qual5_vmdr_vuln_task_group]		false
Group Rules Based on QDS Severity	true	Qualys Detection QDS detection score > 80 .and. Host asset TruRisk Score > 700 .and. State = Open	Group Rules based on QDS Severity	Qualys - VMDR Task Group [x_qual5_vmdr_vuln_task_group]	10	false
Group Rule Based on QDS Severity	true	Qualys Detection QDS detection score > 80 .and. Qualys Detection QDS Host TruRisk Score > 700 .and. State = Open	Group Tickets by QDS=80...	Qualys - VMDR Task Group [x_qual5_vmdr_vuln_task_group]		false
Critical & High Vulnerability Tasks by CI Support Group	true	Configuration Item Support group is not empty .and. QID Severity level in (4 - High, 5 - Critical) .and. Qualys Detection QDS detection score > 90 .and. Host asset Qualys Asset Tags CONTAINS Windows Assets		Qualys - VMDR Task Group [x_qual5_vuln_task_group]	100	false
Change Request by Assignment Group, High and Critical Patchable Vulnerabilities by Operating System	true	Change request is empty .and. State not in (Awaiting Change Request, Under Implementation, Change Implemented, Exception - [...]) .and. Qualys Detection QID Patchable = true .and. Qualys Detection QID Severity level in (4 - High, 5 - Critical) .and. Qualys Detection QDS Host Operating System contains windows		Change Request [change_request]	10	false
Change Request - Patchable Vulnerabilities with CI UUIDs	false	Host asset Qualys UUID is not empty .and. QID Patchable = true		Change Request [change_request]		false

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:

Detection Event Rule
Assets Tagged with Production and Tasks with Critical QOS Severity

The detection event rules allow specifying what records to create a record is inserted or updated on the source table specified.

- **Name:** A name to reference this rule by
- **Active:** Is this rule active or not?
- **Source table:** The source table to watch for record changes and run this rule of the Trigger Criteria are met
- **Destination Table:** The table to create a record in when this rule is triggered.
- **Destination Form View:** When enabled, will allow specifying the form view of the destination record. This is to help for scenarios when you need to show different information based on the groupings performed.
- **Description:** A long description to provide more detail about the purpose of this rule.

Name: Assets Tagged with Production and Tasks with Critical QOS Severity

Active: ☒

Source table: Qualys - VMDR Task [x_qual5_vmdr_task_8...]

Destination table: Qualys - VMDR Task Group [x_qual5_vmdr_task_8...]

Source field to set to Destination Record: -- None --

Description: Group Tickets by QOS Severity

Logging level: Errors

Enable grouping: ☒

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.

Trigger Criteria

Below you can specify the criteria in which this rule should execute. This is based on data on each individual record in the Source table as they are processed.

- **Order:** The order in which this rule should run, in relation to the other rules for the same Source table
- **Stop Processing:** When this rule is triggered, should we stop processing rules that are ordered after this one?
- **Trigger when:** This rule will be triggered the source record being inserted or Updated matches the condition criteria specified.

Order: 100

Stop processing: ☐

Trigger when: 5 records match condition

Add Filter Condition Add "OR" Clause

All of these conditions must be met

Configuration Item.Support group is not empty AND OR X

QID.Severity level is one of 1 - Negligible 2 - Low 3 - Medium 4 - High AND OR X

Qualys Detection.Qualys detection ... is greater than 70 AND OR X

QID.Vulnerability Type is Confirmed Vulnerability AND OR X

Host asset.Qualys Asset Tags contains Windows Assets AND OR X

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.

The screenshot shows the 'Grouping' tab of a configuration interface. It includes a 'Grouping Configuration' section with instructions and two bullet points: 'Group by: What field from the Source table should we group records by. Once a grouping is selected, additional fields will show if more grouping is needed up to 4.' and 'Stop grouping when: Specify a condition for the Destination record (Grouping Record) in which we should stop grouping and create a New grouping record. For example: if you want to create a new Vulnerability Task when the original grouping task is closed.' Below this, there are three dropdown menus for 'Group by', 'Then group by', and 'Then group by'. The 'Stop Grouping When' section includes buttons for 'Add Filter Condition' and 'Add "OR" Clause', followed by a dropdown for 'State' and a list of conditions: 'Is one of', 'Open', 'Re Opened', 'In Progress', and 'Under Investigation'. There are also buttons for 'AND', 'OR', and 'X'.

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

This screenshot shows the 'Grouping' tab with a dropdown menu open for the 'Group by' field. The dropdown is titled 'Select the element from the tree' and lists various fields from the Source table, including 'Active', 'Activity due', 'Actual end', 'Actual start', 'Additional assignee list', 'Additional comments', 'Approval', 'Approval history', 'Approval set', 'Archive on', 'Assigned to', 'Assignment group', 'Business duration', and 'Change request'. The background shows the same configuration interface as the previous screenshot, but with the 'Group by' field set to 'Configuration Item Support group'.

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.

VMDRTSK0001 - CI.Support Group = Support Group A, AND a Business Criticality of High, AND a CI Operating System of Windows Server 2008 R2

VMDRTSK0002 - CI.Support Group = Support Group A, AND a Business Criticality of Low, AND a CI Operating System of Windows Server 2008 R2

VMDRTSK0003 - CI.Support Group = Support Group A, AND a Business Criticality of High, AND a CI Operating System of Windows Server 2008 R2

VMDRTSK0004 - CI.Support Group = Support Group A, AND a Business Criticality of High, AND a CI Operating System of RedHat

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

Group	Tasks included
<u>VMDGRPTSK0001</u> - CI.Support Group = Support Group A, AND a Business Criticality of High, AND a CI Operating System of Windows Server 2008 R2	VMDRTSK0001 VMDRTSK0003
<u>VMDGRPTSK0002</u> - CI.Support Group = Support Group A, AND a Business Criticality of Low, AND a CI Operating System of Windows Server 2008 R2	VMDRTSK0002
<u>VMDGRPTSK0003</u> - CI.Support Group = Support Group A, AND a Business Criticality of High, AND a CI Operating System of RedHat	VMDRTSK0004

Scenario 2: Support Group B

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

VMDRTSK0005 - CI.Support Group = Support Group B, AND a Business Criticality of Low, AND a CI Operating System: RedHat

VMDRTSK0006 - CI.Support Group = Support Group B, AND a Business Criticality of Low, AND a CI Operating System: RedHat

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

Group	Tasks included
<u>VMDRGRPTSK0004</u> - CI.Support Group = Support Group B, AND a Business Criticality of Low, AND a CI Operating System: RedHat	VMDRTSK0005 VMDRTSK0006

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

VMDRTSK0008 - CI.Support Group = Support Group C, AND a Business Criticality of Low, AND a CI Operating System of Windows Server 2008 R2

VMDRTSK0009 - CI.Support Group = Support Group C, AND a Business Criticality of High, AND a CI Operating System of Windows Server 2008 R2

VMDRTSK0010 - CI.Support Group = Support Group C, AND a Business Criticality of Low, AND a CI Operating System of Windows Server 2008 R2

VMDRTSK0011 - CI.Support Group = Support Group C, AND a Business Criticality of Low, AND a CI Operating System of RedHat

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:

Group	Tasks included
<u>VMDRGRPTSK0005</u> - CI.Support Group = Support Group C, AND a Business Criticality of High, AND a CI Operating System of Windows 11 22h02	VMDRTSK0007 VMDRTSK0012
<u>VMDRGRPTSK0006</u> - CI.Support Group = Support Group C, AND a Business Criticality of Low, AND a CI Operating System of Windows Server 2008 R2	VMDRTSK0008 VMDRTSK0010
<u>VMDRGRPTSK0007</u> - CI.Support Group = Support Group C, AND a Business Criticality of High, AND a CI Operating System of Windows Server 2008 R2	VMDRTSK0009
<u>VMDRGRPTSK0008</u> - CI.Support Group = Support Group C, AND a Business Criticality of Low, AND a CI Operating System of RedHat	VMDRTSK0007

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.

	Name	Execution Order	User	Group	Updated
<input type="checkbox"/>	x_qualys_vmdr_vuln_task	Windows Team	100 (empty)	(empty)	2023-01-31 08:42:15
<input type="checkbox"/>	x_qualys_vmdr_vuln_task	Linux Vuln	100 (empty)	Linux Server Team	2023-01-31 08:42:15
<input type="checkbox"/>	x_qualys_vmdr_vuln_task	App Teams	100 (empty)	(empty)	2023-01-31 08:42:15
<input type="checkbox"/>	x_qualys_vmdr_vuln_task	Azure Infra	100 (empty)	(empty)	2023-01-31 08:42:15
<input type="checkbox"/>	x_qualys_vmdr_vuln_task	Security Team	100 (empty)	(empty)	2023-01-31 08:42:14
<input type="checkbox"/>	x_qualys_vmdr_vuln_task	AWS Infra Team	100 (empty)	(empty)	2023-01-31 08:42:15
<input type="checkbox"/>	x_qualys_vmdr_vuln_task	App - Database Teams	100 (empty)	(empty)	2023-01-31 08:42:15
<input type="checkbox"/>	x_qualys_vmdr_vuln_task	WKS - Agent	100 (empty)	(empty)	2023-01-31 08:42:14
<input type="checkbox"/>	x_qualys_vmdr_vuln_task	test	100 (empty)	(empty)	2023-02-06 14:30:37

For example, the assignment rule for the Windows team:

Assignment Rule
Windows Assignment

You are editing a record in the Global application (cancel)

Use Assignment Rules to automatically assign tasks to users and groups. [More Info](#)

Name: Application: ⓘ

Execution Order: Active: ☒

Applies To: Assign To Script

Select a Table and specify the Conditions that must be met before the task is assigned to the user or group. The rule is applied only if the task is not already assigned to another user or group.

Table:

Conditions:

The assignment rule criteria for cloud assets:

Assignment Rule
Cloud Assets

Use Assignment Rules to automatically assign tasks to users and groups. [More Info](#)

Name: Application: ⓘ

Execution Order: Active: ☒

Applies To: Assign To Script

Select a Table and specify the Conditions that must be met before the task is assigned to the user or group. The rule is applied only if the task is not already assigned to another user or group.

Table:

Conditions:

All of these conditions must be met

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.

Use Assignment Rules to automatically assign tasks to users and groups. [More info](#)

Name: Application:

Active: ☒

Applies To | Assign To | Script

Enter a script to further customize the assignment rule. Scripts provide access to `current`, `variable`, `pool` variables.

Script

```
/**
 * Example:
 * The following script requires personalizing the instance to add the Malware category and the Security assignment group.
 * If (current.category == "Hardware")
 *   current.assignment_group.setDisplayValue("Hardware");
 * else if (current.category == "Software")
 *   current.assignment_group.setDisplayValue("Software");
 * else if (current.category == "Malware")
 *   current.assignment_group.setDisplayValue("Security");
 *
 * Another Example:
 * Release Planning Example, which assigns the last person assigned to a release to the current release.
 * current.release.product.service.assigned_to;
 */
```

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.

SLA Definitions <input type="button" value="New"/> <input type="text" value="Search"/> Name <input type="text" value="Search"/>						
All > Table = x_qual5_vmdr_vuln_task						
	Name	Type	Target	Duration	Table	Updated
	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="x_qual5_vmdr_vuln_task"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	ARS Criteria	SLA	Resolution	4 Days	Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]	2022-06-21 05:22:59
<input type="checkbox"/>	Asset Risk Score	SLA	Resolution	4 Days	Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]	2022-06-21 05:23:14
<input type="checkbox"/>	Crit Sev(4)_No RTI_Crit Buss Asset	SLA	Resolution	10 Days	Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]	2022-06-21 04:13:02
<input type="checkbox"/>	Crit Sev(4)_RTI-AT_High Buss Asset	SLA	Resolution	30 Days	Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]	2022-06-21 04:14:34
<input type="checkbox"/>	Crit Sev(4)_RTI-AT_Low Buss Asset	SLA	Resolution	120 Days	Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]	2022-06-21 04:19:44
<input type="checkbox"/>	Crit Sev(4)_RTI-AT_Med Buss Asset	SLA	Resolution	60 Days	Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]	2022-06-21 04:15:28
<input type="checkbox"/>	Crit Sev(4)_RTI-AT_Min Buss Asset	SLA	Resolution	90 Days	Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]	2022-06-21 04:18:16
<input type="checkbox"/>	Crit Sev(5)_No RTI_Crit Buss Asset	SLA	Resolution	5 Days	Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]	2022-06-21 04:11:36
<input type="checkbox"/>	Crit Sev(5)_RTI-AT_Crit Buss Asset	SLA	Resolution	5 Days	Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]	2022-06-21 04:12:35
<input type="checkbox"/>	Crit Sev(5)_RTI-AT_High Buss Asset	SLA	Resolution	20 Days	Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]	2022-06-21 04:14:02

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.

The screenshot shows the 'SLA Definition' page for 'ARS Criteria'. The top section contains basic configuration: Name (ARS Criteria), Type (SLA), Target (Resolution), Table (Qualys - Vulnerability Task [x_qual5_vmdr_vu...]), and Flow (Default SLA flow). There are checkboxes for 'Enable logging' and 'Active'. The 'Start condition' tab is selected, showing a list of conditions: 'Qualys Detection.QDS Severity' is one of 'CRITICAL, HIGH, LOW, MEDIUM'; 'Qualys Detection.Qualys Host.Asse...' is '5'; and 'Qualys Detection.Qualys Host.Asse...' is 'greater than' '900'. There are also buttons for 'Add Filter Condition' and 'Add OR Clause'.

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
Asset Risk Score

Name: Asset Risk Score

Type: SLA

Target: Resolution

Table: Qualys - Vulnerability Task [x_qual5_vmdr_vuln_...]

Flow: Default SLA flow

Enable logging: ☐

Active: ☒

Application: Qualys Core

Duration type: User specified duration

* Duration: Days 4 Hours 00 00 00

Schedule source: SLA definition

* Schedule: 24 x 7

Timezone source: The caller's time zone

Start condition | **Pause condition** | Stop condition | Reset condition

The conditions under which the new SLA will be attached and canceled

Start condition

Add Filter Condition Add "OR" Clause

All of these conditions must be met

Qualys Detection.QID.Severity level is one of 1 - Negligible 2 - Low 3 - Medium 4 - High

Qualys Detection.Qualys Host.Asse... greater than 850

Qualys Detection.Qualys Host.Asse... is 5

Qualys Detection.Qualys detection ... greater than 90

Qualys Detection.Qualys Host.Qual... contains Internet Facing Assets

SLA definition for Internet-facing assets

SLA Definition
Internet Facing Asset

Name: Internet Facing Asset

Type: SLA

Target: Resolution

Table: Qualys - Vulnerability Task [x_qual5_vmdr_vuln_...]

Flow: Default SLA flow

Enable logging: ☐

Active: ☒

Application: Qualys Core

Duration type: User specified duration

* Duration: Days 2 Hours 00 00 00

Schedule source: SLA definition

* Schedule: 24 x 7

Timezone source: The caller's time zone

Start condition | **Pause condition** | Stop condition | Reset condition

The conditions under which the new SLA will be attached and canceled

Start condition

Add Filter Condition Add "OR" Clause

All of these conditions must be met

Qualys Detection.Qualys detection ... greater than 90

Qualys Detection.Qualys Host.Qual... contains Internet Facing Assets

Qualys Detection.Qualys Host.Asse... greater than 850

Qualys Detection.QDS Severity is one of CRITICAL HIGH LOW MEDIUM

Qualys Detection.Qualys Host.Asse... greater than 4

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**.

The screenshot shows the 'SLA Definition' form for 'Crit Sev(4), RT1-A1, Min Buss Asset'. The form includes fields for Name, Type (SLA), Table (Qualys - Vulnerability Task [x_qualys_vmdr_vuln...]), Workflow (None), Active (checked), and Enable logging (unchecked). On the right, there are fields for Application (sys_scope) set to 'Qualys VMDR for ServiceNow ITSM', Duration type (User specified duration), Duration (Days: 90, Hours: 00, Minutes: 00, Seconds: 00), Schedule source (SLA definition), Schedule (24 x 7), and Timezone source (The caller's time zone). A notification at the top states: 'An SLA starting now will breach on 07-18-2022 15:37:18 (Actual elapsed time: 90 Days)'.

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**.

The screenshot shows the 'General Settings' page in Qualys Core. The left sidebar contains a navigation menu with options like Configuration, General Settings, Connectors, Assignment Rules, SLA Definitions, Detection Event Rules, Grouping Rules, One-to-One Rules, All, Regenerating Histories, Data Import, Import Configurations, and Scheduled Imports. The main content area is titled 'Patch Deployment Configuration' and contains instructions on how to configure the behavior of the Patch Deployment Jobs and Related Functionality. It lists three key settings: 1. Percentage of completed items to consider Patch Deployment completed (set to 50), 2. Maximum Number of Assets Per Job (set to 50), and 3. Duration Past Start Date to Auto Complete (set to 1 Day, 00 Hours, 00 Minutes, 00 Seconds). An 'Update' button is at the bottom.

- **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.

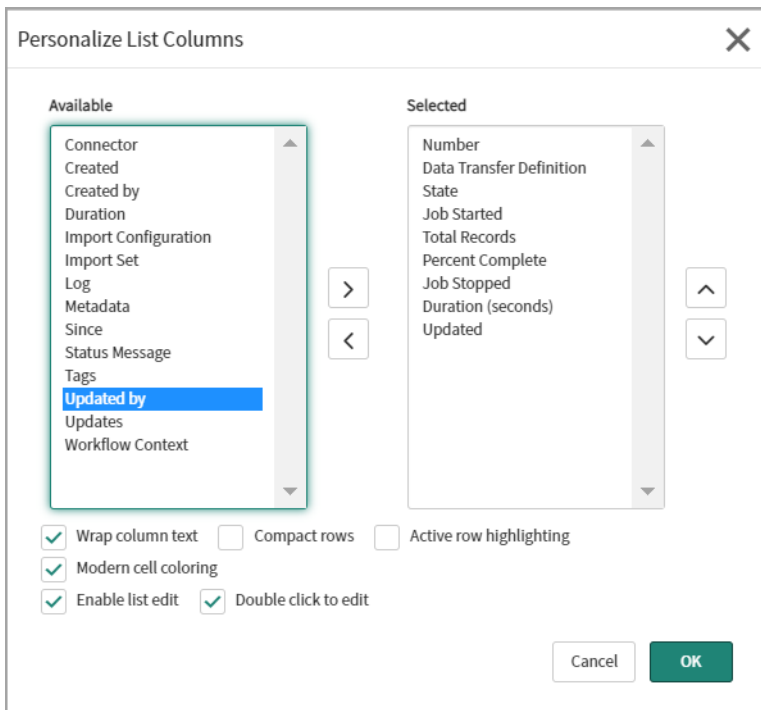
- **Duration Past Start Date to Auto Complete** - The time elapsed after the patch job has started. After the time defined in this field, the patch job is considered as stale and the state of the patch job changes to Completed - Stale.

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.



The dialog box titled "Personalize List Columns" has a close button (X) in the top right corner. It contains two main sections: "Available" and "Selected".

Available: A list of columns that are currently hidden. The columns are: Connector, Created, Created by, Duration, Import Configuration, Import Set, Log, Metadata, Since, Status Message, Tags, **Updated by** (highlighted in blue), Updates, and Workflow Context. There are up and down arrow buttons next to this list.

Selected: A list of columns that are currently displayed. The columns are: Number, Data Transfer Definition, State, Job Started, Total Records, Percent Complete, Job Stopped, Duration (seconds), and Updated. There are up and down arrow buttons next to this list.

Between the two lists are left and right arrow buttons. Below the lists are several checkboxes:

- ☒ Wrap column text
- ☐ Compact rows
- ☐ Active row highlighting
- ☒ Modern cell coloring
- ☒ Enable list edit
- ☒ Double click to edit

At the bottom right are "Cancel" and "OK" buttons.

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.

	Name	Asset Id	Configuration Item	Qualys Id	IP v4	IP v6	Last Vulnerability Scan Date	Netbios	Network Id	Host name
<input type="checkbox"/>	(empty)	406933792	(empty)			(empty)			47223	
<input type="checkbox"/>	(empty)	417179677	(empty)			(empty)			47223	
<input type="checkbox"/>	(empty)	416905670	(empty)			(empty)			47223	
<input type="checkbox"/>	(empty)	408719516	(empty)			(empty)			47223	
<input type="checkbox"/>	(empty)	436572773	(empty)			(empty)			47223	
<input type="checkbox"/>	(empty)	192610746	(empty)			(empty)			47223	
<input type="checkbox"/>	(empty)	402843144	(empty)			(empty)			47223	
<input type="checkbox"/>	(empty)	437887960	(empty)			(empty)			47223	
<input type="checkbox"/>	(empty)	403222935	(empty)			(empty)			47223	
<input type="checkbox"/>	(empty)	458400765	(empty)			(empty)			47223	

- **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 hosts 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**.

The screenshot displays the 'Qualys - Host Asset' form. At the top, there's a header with a back arrow, a menu icon, the title 'Qualys - Host Asset', and a sub-header 'xpsp2chs-26-112'. To the right of the header are icons for edit, view, and a list of three dots, followed by buttons: 'Update', 'Create CI', 'Find CI', and 'Delete'. Below the header, the form is organized into sections. The first section contains 'Name' (a text field), 'Tracking method' (a dropdown menu set to 'IP'), 'Asset Id' (a text field), 'Configuration item' (a text field with a search icon), 'Qualys id' (a text field), and 'Operating System' (a dropdown menu set to 'Windows XP'). The second section is 'Qualys Asset Tags' with a lock icon and a text area containing a long string of tags. The third section is 'Asset Groups' with a lock icon and a text area containing a list of groups. Below these is a tabbed interface with four tabs: 'Network' (selected), 'Scan Dates', 'Cloud', and 'ARS Factors'. The 'Network' tab shows fields for 'Host name', 'DNS Name', 'FQDN', 'Domain', 'Netbios', 'Network Id' (set to '0'), 'IP v4', and 'IP v6'. The 'Find CI' button is located in the top right corner of the form.

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**.

```
IRE CMDB_CI_hardware criteria: (Script Includes, under System
Definition & look for QualysAssetIREvar ireData = {
items: [{
className: "cldb_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.**

Identifier: cmdb_ci_hardware

Name: Hardware Rule Active ☒

* Applies to: Hardware [cmdb_ci_hardware]

Description: Identifier for hardware.

Independent ☒

Update Delete

Identifier Entries (10) Related Entries (8)

Identifier = cmdb_ci_hardware

Active	Search on table	Criterion attributes	Allow null attribute	Optional condition	Priority
<input type="checkbox"/>	Hardware [cmdb_ci_hardware]	ip_address,mac_address	false		500
<input type="checkbox"/>	Hardware [cmdb_ci_hardware]	name	false		300
<input type="checkbox"/>	Network Adapter [cmdb_ci_network_adapter]	mac_address,name	false	install_status!=100^EQ	400

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.

Qualys - Host Asset
10.115.1

Name: 10.115.1

Tracking method: IP

Configuration Item: [Search]

Asset Id: [Field]

Qualys Id: [Field]

Qualys UUID: [Field]

Operating System: EulerOS / Ubuntu / Fedora / Tiny Core Linux / L

Qualys Asset Tags: [Icon]

Asset Groups: [Icon] BU-NET-RDLABS_INDIA

No NetBIOS Name, p1_Operational, Scan Time (>15m), IP: 10.0.0.0_8, SW: EOL EOS Software, Status:Operational, Crash_TCP_Unknown, Authentication Not Attempted, EOL, Scanned in 180-D, Scan Time (>45m), OS: Unidentified, CPE Tag Example, Scanned in 90-D, Scan Time (>30m), Scanned in 30-D, BU-NET-RDLABS_INDIA, No Hostname, not_scanned_x_days, TM: IP Tracking

Asset Groups: [Icon] BU-NET-RDLABS_INDIA

Network | Scan Dates | Cloud | TruRisk

Host name: [Field]

DNS Name: [Field]

FQDN: [Field]

Domain: [Field]

Netbios: [Field]

Network Id: 777124

IP v4: 10.115.1

IP v6: [Field]

Update | Create CI | Find CI | Delete

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

Qualys

Qualys VMDR for ServiceNow ITSM

Overview

Vulnerability Tasks

Open

Assigned to My Group (Open)

Assigned to My Group (Fixed)

Assigned to Me (Open)

All

Qualys - Vulnerability Tasks

New

Search

State

Search

1 to 20 of 55,065

All

Number

State

Severity level

Priority

IP v4

Vulnerability Status

Assignment group

Assigned to

Operating System

QID

Search

Search

Search

Search

Search

Search

Search

Search

Search

Search

YTASK0079682

Open

4 - High

2 - High

Active

Vulnerability Routing

(empty)

Solaris 9-11

120356

YTASK0020803

Open

3 - Medium

3 - Moderate

Fixed

Vulnerability Routing

(empty)

Ubuntu Linux 16.04.6

197917

YTASK0053632

Open

4 - High

2 - High

Active

Vulnerability Routing

(empty)

Windows 2003 Server AD Service Pack 2

100232

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.

Qualys - Vulnerability Tasks

New

Search

State

Search

All

Number

State

Severity level

Priority

IP v4

Vulnerability Status

Assignment group

Assigned to

Operating System

QID

Title

Search

Search

Search

Search

Search

Search

Search

Search

Search

Search

Search

VTASK0079682

Open

4 - High

2 - High

Active

Vulnerability Routing

(empty)

Solaris 9-11

Solaris 9-11 Remote C-Service Vi

VTASK0020803

Open

3 - Medium

3 - Moderate

Fixed

Vulnerability Routing

(empty)

Ubuntu Linux 16.04.6

Ubuntu S Notificati Linux-awr aws-hwe, azure, Lin 4.15, Linu (USN-439)

VTASK0053632

Open

4 - High

2 - High

Active

Vulnerability Routing

(empty)

Windows 2003 Server AD Service Pack 2

Microsoft Explorer (Security I (MS15-04)

VTASK0061192

Open

4 - High

2 - High

Fixed

Vulnerability Routing

(empty)

Windows XP Service Pack 3

Apple Saf 5.1 and 5. Vulnerabi (APPLE-S 20-1)

VTASK0049094

Open

3 - Medium

3 - Moderate

Active

Vulnerability Routing

(empty)

Windows Server 2003 64 bit Edition Servi...

Microsoft Explorer ("express Denial of

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.

Qualys - VMDR Task
VTITM0012378

Follow

Update

Delete

Number	VTITM0012378	State	Awaiting Change Request
Connector	Qualys Demo Account	Vulnerability Status	Active
* Qualys Detection	HDETC098699	Severity level	4 - High
Creation Source	Automated - Qualys Integration	* Change request	CHG1821422
Configuration Item		Assignment group	
Class	.NET Application	Assigned to	
Status	-- None --	QDS Severity	HIGH
		Qualys detection score	87

Host Information provides host and host network information.

Host Information

Host Network Information

Operating System	Windows 11 Pro 64 bit Edition Version 21H2	IP v4	10.115
Cloud Resource ID		IP v6	
Asset Id	52618	Host name	desktop-1
Qualys Id	42267	Netbios	DESKTOP-1
TruRisk Criticality Score	2	FQDN	desktop-k
TruRisk Score	349	DNS Name	desktop-k
		Domain	europa.

Vulnerability Details provides details of a vulnerability that is available from Qualys VMDR.

Qualys - Vulnerability Task
VTASK0079682

Vulnerability Details | Detection | Notes / Activity

Title: Solaris SCTP and IPv6 Remote Denial of Service Vulnerability

Vulnerability Type: Confirmed Vulnerability QID: 120356

CVSS

CVSS v3

CVSS Base: 7.8 CVSS v3 Base: 7.5

CVSS Temporal: 5.8 CVSS v3 Temporal: 6.5

Threat: Unspecified vulnerability in Oracle Solaris SCTP and IPv6 component allows remote attacker to cause a denial of service. Affected Versions: Solaris 8, 9, 10 on the SPARC and x86 platforms are affected.

Impact: Successfully exploiting these vulnerabilities might allow remote attacker to cause denial of service.

Solution: Refer to [Oracle CPU Jul 2012 for Sun Products](#) and Oracle Sun Products Suite Executive Summary Section at [Oracle CPU JUL 2012](#) to address this issue and obtain more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
[Oracle Solaris CPU Jul 2012: Solaris 8, 9, 10](#)

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

Qualys - Vulnerability Task
VTASK0079682

Vulnerability Details | Detection | Notes / Activity

Qualys Asset Tags: DECOM Asset+365days, TestIP to remove, MMC Test Environment, ScanTimeMin-0-30, MCW - AT Not Seen in 180 Days, PB - 10/8, Qualys - QA Lab - Solaris 10, MAK Groovy, MCW - Not Scanned in 30 Days, MCW - Auth Not Attempted Windows, External facing ports, MSC-LAB, hs-Service-SQL-Tag, Unix - PP, Not Scanned in 365 days, MEP - QA, ScanTimeMin-0-10, SMC - Default Demo Assets, MCW - Not 38601, 1 AC Demo Business Unit, MCW - Test OS CPE, Public DMZ, YK-Threat Protect, ServerOS, Test Purging - GTD, (TVL) Linux

Asset Groups: Public DMZ, MEP - QA, TM - Global Network, TestIP to remove, SMC - Default Demo Assets, Unix - PP, YK-Threat Protect, PB - 10/8, MMC Test Environment, Qualys - QA Lab - Solaris 10, MSC-LAB

Detection Detail

Tracking method: IP

Service:

Port:

Protocol:

Type: Confirmed

Affect Exploitable Config: -- None --

Affect Running Kernel: -- None --

Affect Running Service: -- None --

Is disabled: ☐

Is ignored: ☒

Detected over SSL: ☐

Results: SUNWcsl is installed
147441-15 is missing.

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

Scan Dates

Last Vulnerability Scan Date
2019-10-02 01:02:42

Last Authenticated scan date
2019-08-19 11:07:17

Last Authed Scan Date
Duration
0 00 00 00

Last Unauthenticated scan date
2019-10-02 01:02:42

Last VM (UnAuthed) Scan
Duration
0 00 00 00

Last Compliance Scan
Date/Time
2020-03-23 07:58:49

Last Compliance Scap Scan
Date/Time

Update Delete

Related Links

[Launch VM Scan](#)
[Show SLA Timeline](#)

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.

Qualys - Vulnerability Task
VTASK0079682

Follow Update Delete

Vulnerability Details Detection **Notes / Activity**

Work notes

Post

Activities: 1

System

Impact 3 - Low
Opened by [Empty]
Priority 2 - High
State Open

Field changes • 2021-11-01 15:53:17

Update Delete

Related Links

[Launch VM Scan](#)
[Show SLA Timeline](#)

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.

Recent VM Scans for Host Open Tasks for Host (51) Open Tasks for Vulnerability (1) **Task SLAs (1)**

Open Tasks for Vulnerability New Search State Search

Qualys - Vulnerability Tasks

Number State Severity level IP v4 Vulnerability Status Configuration item Class Status Assignment group Assigned to

<input type="checkbox"/>		VTASK0074064	Open	5 - Critical	Fixed	(empty)	Vulnerability Routing	(empty)	AD
--------------------------	--	------------------------------	------	---	--	---------	-----------------------	---------	----

☐ Actions on selected rows...

1 to 1 of 1

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

Host Information

Please review the host information and details before launching your scan

Name

ai61-30-211

IP v4

10.10.30.211

Tracking method

IP

Qualys Asset Tags

DECOM Asset+365days, JM Asset Group 2, TestIP to remove, ScanTimeI

Asset Groups

Public DMZ, AIX, MEP - QA, TM - Global Network, TestIP to remove, DC -

Scan Configuration

Please select the Scanner Appliance and Option Profile for this can. **Note:** The defaults have been loaded for the Connector associated to these hosts.

Scanner Appliance

is_quays_ma58_2

×

▼

Option Profile

MCW - Std VM Scan - No Auth - Fast - Web QIDs Only

×

▼

Start Scan

Cancel

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

Host Information

Please review the host information and details before launching your scan

1 Valid Hosts for Scan

The following Hosts are valid to launch a VM Scan against.

- 64.41.200.250 | demo20.s02.sjc01.qualys.com | IP

1 Invalid Hosts for Scan

The following Hosts are not valid targets to Launch a VM Scan from ServiceNow. This is typically due to the Tracking Method as only IP based Tracking methods are currently supported. Please consider refining your List Filter

- 64.41.200.250 | demo20.s02.sjc01.qualys.com | DNS

Scan Configuration

Please select the Scanner Appliance and Option Profile for this can. **Note:** The defaults have been loaded for the Connector associated to these hosts.

Scanner Appliance
is_qualys_ma58_2

Option Profile
MCW - Std VM Scan - No Auth - Fast - Web QIDs Only

Start Scan
Cancel

- For multiple vulnerability tasks

Qualys - Vulnerability Tasks

New

Search

State

1

to 20 of 55,065

Number

State

Severity level

Priority

IP v4

Vulnerability Status

Assignment group

Assigned to

Operating System

QID

Title

VTASK0042530

Open

3 - Medium

3 - Moderate

Fixed

Vulnerability Routing

(empty)

Windows XP Service Pack 3

90508

Microsoft Print Spo
Allow file
Executor

VTASK0089474

Open

3 - Medium

3 - Moderate

42

Fixed

Vulnerability Routing

(empty)

Ubuntu Linux 16.04.6

198108

Ubuntu S
Notifica
Freetype
Vulnerabi
4593-1)

3 - Medium

3 - Moderate

Fixed

Vulnerability Routing

(empty)

Windows XP 64 bit
Edition Service Pack 2

119314

Adobe Fl
Cross-Siti
Vulnerabi
(APSB11-

5 - Critical

1 - Critical

Fixed

Vulnerability Routing

(empty)

Windows Server 2008 R2
Enterprise 64 bit...

91029

Microsoft
Shell Ren
Executor
Vulnerabi
020)

3 - Medium

3 - Moderate

Active

Vulnerability Routing

(empty)

Solaris 9-11

120149

Solaris In
Input Vali
Vulnerabi
Apache H
2.0

Actions on selected rows...

Add to Update Set

Delete

Follow on Live Feed

Launch VM Scan

VALA Show Matching Checked

Repair SLAs

Add to Visual Task Board

Create Application File

Assign Tag

New Tag

Performance Analytics and Reporting

IT Service Management

Customer Service

IT Operations Management

Software Asset Management

Cannot determine code change

Other

Includes code

More...

Actions on selected rows...

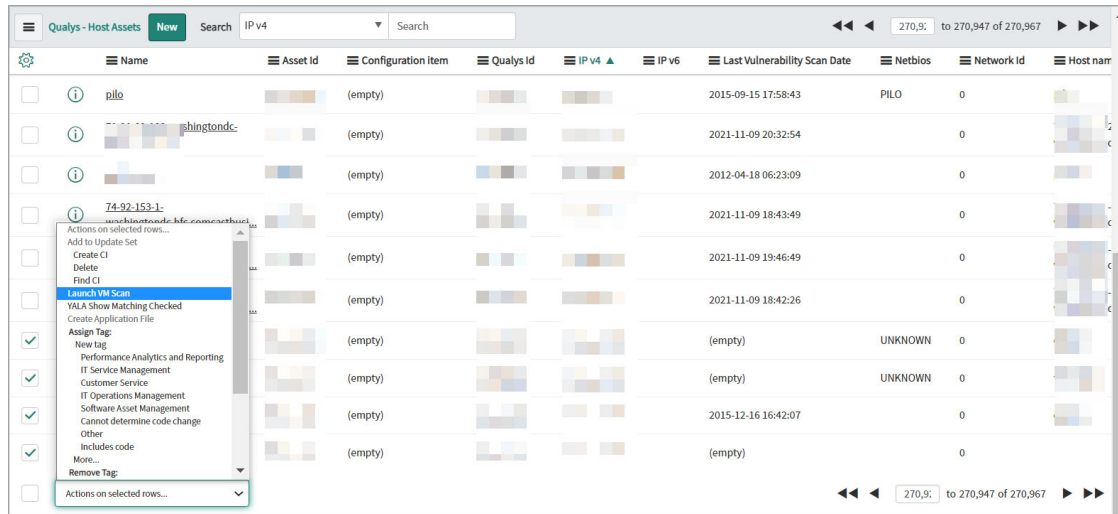
1

to 20 of 55,065

Response time(ms): 1164, Network: 4, server: 1027, browser: 133

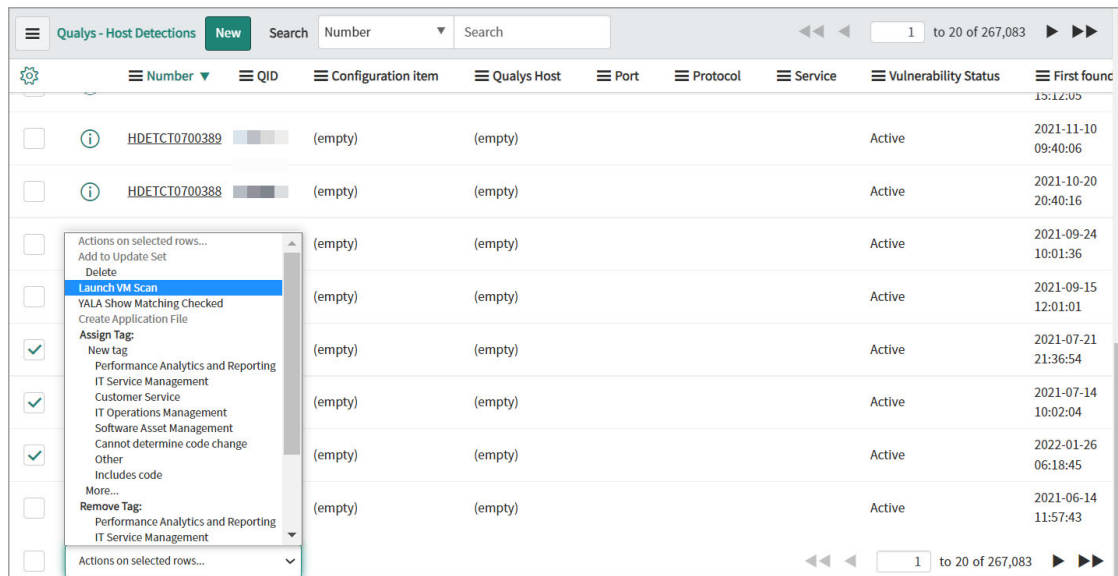
You can select multiple vulnerability tasks and select **Launch VM Scan** from the list of available actions.

- 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 task 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.

Qualys - VMDR Task Groups									
New Search % Vulnerability Tasks remediated Search									
All Active = true									
	Number	State	Assignment group	Detection event	% Vulnerability Tasks remediated	Vulnerability Tasks	Total Vulnerability Tasks	Total	
	Search	Search	Search	Search	Search	Search	Search	Search	Search
<input type="checkbox"/>	① YTGPR0021525	Awaiting Change Request	Developer	Critical & High Vulnerability Tasks by CI Support Group	100%	<div></div>	3	0	
<input type="checkbox"/>	① YTGPR0126100	Open	Developer	Critical & High Vulnerability Tasks by CI Support Group	100%	<div></div>	1	0	
<input type="checkbox"/>	① YTGPR0021514	False Positive - Awaiting Confirmation	VMOR Windows Vulnerability Team	Critical & High Vulnerability Tasks by CI Support Group	94.16%	<div></div>	290	233	
<input type="checkbox"/>	① YTGPR0021513	Awaiting Change Request	Team Firewall Comets	Critical & High Vulnerability Tasks by CI Support Group	90.26%	<div></div>	343	39	
<input type="checkbox"/>	① YTGPR0022134	Open	Apache Support Group	Critical & High Vulnerability Tasks by CI Support Group	85.71%	<div></div>	1	6	
<input type="checkbox"/>	① YTGPR0021666	Awaiting Change Request	Windows Server support	Critical & High Vulnerability Tasks by CI Support Group	70%	<div></div>	7	3	
<input type="checkbox"/>	① YTGPR0021556	Exception - Identified	App-Sec Manager	Critical & High Vulnerability Tasks by CI Support Group	68.57%	<div></div>	22	48	
<input type="checkbox"/>	① YTGPR0021527	Exception - Identified	VMDR Remediation Analysts	Critical & High Vulnerability Tasks by CI Support Group	54.97%	<div></div>	68	83	
<input type="checkbox"/>	① YTGPR0021538	Awaiting Change Request	Application Security	Critical & High Vulnerability Tasks by CI Support Group	53.85%	<div></div>	7	6	
<input type="checkbox"/>	① YTGPR0137551	Open	VMDR Admins	Critical & High Vulnerability Tasks by CI Support Group	33.33%	<div></div>	4	4	
<input type="checkbox"/>	① YTGPR0168295	Open	VMDR Admins	Critical & High Vulnerability Tasks by CI Support Group	11.61%	<div></div>	99	13	
<input type="checkbox"/>	① YTGPR0168465	Open	Developer	Critical & High Vulnerability Tasks by CI Support Group	10.81%	<div></div>	198	24	

For each vulnerability task group, you can view the following details:

The screenshot shows the 'Qualys - VMDR Task Group - VTGRP00' interface. At the top, there are fields for 'Number' (VTGRP00), 'Priority' (1 - Critical), 'State' (Awaiting Change Request), 'Change request', 'Assignment group' (Windows Server support), and 'Assigned to'. Below these are 'Short description' and 'Description' fields. The 'Remediation Status' tab is active, showing 'Include Deferred' and 'Exclude Deferred' sections. Each section has 'Vulnerability Tasks' and 'Total Vulnerability Tasks' counts, along with a '% Vulnerability Tasks remediated' progress bar.

Category	Vulnerability Tasks	Total Vulnerability Tasks	% Vulnerability Tasks remediated
Include Deferred	7	10	70
Exclude Deferred	0	3	0

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.

This screenshot is a closer view of the 'Remediation Status' tab from the previous image. It shows the 'Include Deferred' and 'Exclude Deferred' sections with their respective task counts and remediation percentages. An 'Update' button is visible at the bottom left.

Category	Vulnerability Tasks	Total Vulnerability Tasks	% Vulnerability Tasks remediated
Include Deferred	7	10	70
Exclude Deferred	0	3	0

The **Group Definition** displays the detection event rule that was applied for creating this group task.

The task groups also displays details about the deferred and resolved tasks, host assets involved in the group task, QIDs associated with the this group task.

Deferred Tasks

Open Tasks (6)

Deferred Tasks (1)

Resolved Tasks (3)

Host Assets (Unique) (1)

QIDs (Unique) (10)

Approvals

Task SLAs

Deferred Tasks

Search

Number

Search

1 to 1 of 1

Grouped Vulnerability Task

Number

State

Priority

Configuration item

Host asset

QID

Port

Operating System

Assignment group

Assigned to

Detection event

VTASK000

False Positive - Confirmed

1 - Critical

demonstrator

ymdr

105972

Windows Server 2008 R2 Enterprise 64 bit...

VMDR Windows Vulnerability Team

(empty)

Critical & High Vulnerability Tasks by CI...

Actions on selected rows...

1 to 1 of 1

Resolved Tasks

Open Tasks (6)

Deferred Tasks (1)

Resolved Tasks (3)

Host Assets (Unique) (1)

QIDs (Unique) (10)

Approvals

Task SLAs

Resolved Tasks

Search

Number

Search

<<<

<

1

>

>>>

Grouped Vulnerability Task

		Number	State	Priority	Configuration Item	Host asset	QID	Port	Operating System	Assignment group	Assigned to	Detection event
<input type="checkbox"/>		VTASK000	Resolved	1 - Critical	demonstrator	ymdr			Windows Server 2008 R2 Enterprise 64 bit...	Vulnerability Routing	(empty)	Critical & High Vulnerability Tasks by CI...
<input type="checkbox"/>		VTASK001	Resolved	2 - High	demonstrator	ymdr			Windows Server 2008 R2 Enterprise 64 bit...	VMDR Windows Vulnerability Team	(empty)	Critical & High Vulnerability Tasks by CI...
<input type="checkbox"/>		VTASK002	Resolved	1 - Critical	demonstrator	ymdr			Windows Server 2008 R2 Enterprise 64 bit...	Vulnerability Routing	(empty)	Critical & High Vulnerability Tasks by CI...

☐ Actions on selected rows...

<<< < 1 > >>>

Host Assets

Open Tasks (6)

Deferred Tasks (1)

Resolved Tasks (3)

Host Assets (Unique) (1)

QIDs (Unique) (10)

Approvals

Task SLAs

Host Assets (Unique)

Search

Name

Search

1 to 1 of 1

Qualys - Host Assets

Name

Asset Id

Configuration Item

Possible CI Matches

Qualys Id

IP v4

IP v6

Last Vulnerability Scan Date

Netbios

Network Id

1

demon

:

1492

10.

2023-02-01 21:48:00

DEMC

0

Actions on selected rows...

1 to 1 of 1

QIDs

Open Tasks (6)	Deferred Tasks (1)	Resolved Tasks (3)	Host Assets (Unique) (1)	QIDs (Unique) (10)	Approvals	Task SLAs
<div>QIDs (Unique) Search Title Search</div> <div>Qualys - KnowledgeBases</div> <div> <div>QID</div> <div>Title</div> <div>Vulnerability Type</div> <div>Category</div> <div>Severity level</div> <div>Patchable</div> <div>PCI Compliance</div> </div>						
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				EOL/Obsolete Operating System: Microsoft Windows Server 2008 R2 Detected	Confirmed Vulnerability	Security Policy
				EOL/Obsolete Software: Apache Tomcat 7.0.x Detected	Vulnerability or Potential Vulnerability	Security Policy
				EOL/Obsolete Software: Microsoft .NET Framework 4 - 4.5.1 Detected	Confirmed Vulnerability	Security Policy
				EOL/Obsolete Software: Microsoft Internet Explorer 8 Detected	Confirmed Vulnerability	Security Policy
				EOL/Obsolete Software: Microsoft SQL Server 2012 Service Pack 2 (SP2) Detected	Vulnerability or Potential Vulnerability	Security Policy
				EOL/Obsolete Software: Microsoft Visual C++ 2008 Redistributable Package Detected	Confirmed Vulnerability	Security Policy
				EOL/Obsolete Software: Winamp Media Player Detected	Confirmed Vulnerability	Security Policy
				EOL/Obsolete Software: WireShark 3.0 Detected	Confirmed Vulnerability	Security Policy
				TeamViewer Desktop Privilege Escalation Vulnerability	Confirmed Vulnerability	Local
				Windows Print Spooler Remote Code Execution Vulnerability	Confirmed Vulnerability	Windows

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:

Filter navigator

Knowledge Base

Confirmed

All

Configuration

General Settings

Benchmarks

Content Taxonomy

Couchbase Cluster

Interaction

Now Experience Framework

Qualys Core

General Settings

global (VMDR for ITSM General Settings view)

Approval Configuration Defaults

Exception Process

False Positive Process

Below you will find fields to specify the default approval behavior for the built-in flows for Exception Management and False Positive Reporting process.

Infrastructure / Application Owner Approval Defaults

Configure how the Infrastructure / Application Owner Approvals are requested when a Vulnerability Task enters the "Exception Approval" step

- Infrastructure / App Owner Approval Type:
 - Task Field: Based on a field value from Vulnerability Task. Must select a field that references the Group List Table.
 - Custom: Disable the Built-in Approval step for Infrastructure / Application Owner Approval. You must provide your own flow if you wish to have this approval step still.
- Approval Group: Infrastructure / App Owner Task Field: Select the field we should use to default the value for the Infrastructure Approval when utilized. Note: Final field selected must reference a Group [sys_user_group]
- Infrastructure / App Owner Default Approval Group: Select the group to use for Infrastructure Approval when the automated selection does not resolve to a valid group.

Infrastructure / App Owner Approval Type

Vulnerability Task Field

Approval Group: Infrastructure / App Owner Task Field

Configuration Item Approval group

Infrastructure / App Owner Default Approval Group

Application Exception Approver - Level 1

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.

Security Approval Defaults

Configure the groups of users that will be asked for approval during Security Review of Vulnerability Tasks.

- **Approval Group: Security Team:** This group of users will be asked for approval whenever a Vulnerability Task requires review by the Security Team.
- **Approval Group: Security Board:** This is the group of users whom will be asked for approval whenever a Vulnerability Task requires review by the Security Board.

Approval Group: Security Team	VMDR Security Team	Q	+
Approval Group: Security Board	VMDR Security Board	Q	+

- **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.

Approval Configuration Defaults | **Exception Process** | False Positive Process

Configure details regarding the Exception Process for Vulnerability Tasks.

- **Template: Exception Identified:** Please select the template you would like applied to a Vulnerability Task when the state changes to *Exception - Identified*. **NOTE:** The template must only have the Exception Reason field specified.

Template: Exception Identified	EXAMPLE: Exception Identified	Q	+
--------------------------------	-------------------------------	---	---

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.

Approval Configuration Defaults | Exception Process | **False Positive Process**

Configure details regarding the False Positive Process for Vulnerability Tasks.

- **Template: False Positive Identified:** Please select the template you would like applied to a Vulnerability Task when the state changes to *False Positive - Identified*. **NOTE:** The template must only have the False Positive Reason field specified.

Template: False Positive Identified	EXAMPLE: False Positive Identified	Q	+
-------------------------------------	------------------------------------	---	---

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 screenshot displays the Qualys VMDR interface for a specific task titled 'Qualys - VMDR Task - VTASK0000233'. On the left, a sidebar lists various task categories under 'VMDR Tasks' and 'Exceptions'. The main panel shows task details including 'Number' (VTASK0000), 'Connector', 'Qualys Detection', 'Creation Source' (Automated - Qualys Integration), 'Configuration Item', 'Class', and 'Status' (None). A right-hand panel contains fields for 'State' (Open), 'Vulnerability Status' (Active), 'Severity level' (5 - Critical), 'Assignment group' (VMDR Windows Vulnerability Team), 'Assigned to', 'QDS Severity' (HIGH), and 'Qualys detection score' (81). A context menu is open over the title bar, with 'Exception - Initiate' highlighted. Below the main task details, there are sections for 'Host Information' (Operating System: CentOS Linux 7.3.1611, Cloud Resource ID, Asset Id, Qualys Id, TruRisk Criticality Score, TruRisk Score) and 'Host Network Information' (IP v4, IP v6, Host name, Netbios, FQDN, DNS Name, Domain).

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.

Recent VM Scans for Host Open Tasks for Host (405) Open Tasks for Vulnerability (1) Task SLAs (1) VMDR Approvals (3) Vulnerability Task Groupings					
VMDR Approvals					
	Approver	State	Comments	Approving	Group
<input type="checkbox"/>	Cloud Application Owner	Approved		Qualys - VMDR Task: VTASK0000223	GAPRV0010048
<input type="checkbox"/>	Security Person	Requested		Qualys - VMDR Task: VTASK0000223	GAPRV0010049
<input type="checkbox"/>	Security Person	Requested		Qualys - VMDR Task: VTASK0000223	GAPRV0010049

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.

Approver	State	Comments	Approving	Group
Cloud Application Owner	Approved		Qualys - VMDR Task: VTASK00000233	GAPRV0010048
Security Person	Rejected	2023-01-30 09:09:21 - Security Person (Comments) This is not something we can make an exception to, as the vulnerability is to critical and the business system contains customer data.	Qualys - VMDR Task: VTASK00000233	GAPRV0010048

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.

State	Approver	Comments	Approval for	Created
Requested	Cloud Application Owner		VTASK00000233	2023-01-30 04:47:47

Click the **State** column.

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

The screenshot displays the 'Approval - Qualys - VMDR Task: VTASK000' form. The 'Approving' field is set to 'Qualys - VMDR Task: VTASK000'. Below this, the 'Qualys - VMDR Task' record is shown with the following details:

Qualys - VMDR Task	
Number	VTASK0000
Connector	Qualys - POD 1
Qualys Detection	Automated - Qualys Integration
Creation Source	Automated - Qualys Integration
State	Exception - Awaiting Approval
Approval	Requested
Vulnerability Status	Active
Severity level	S - Critical
Change request	
Assignment group	VMDR Windows Vulnerability Team
Assigned to	
QDS Severity	HIGH
Qualys detection score	81

Below the task details, the 'Host Information' and 'Host Network Information' sections are visible:

Host Information		Host Network Information	
Operating System	CentOS Linux 7.3.1611	IP v4	
Cloud Resource ID		IP v6	
Asset Id		Host name	
Qualys Id		Netbios	
TruRisk Criticality Score		FQDN	
TruRisk Score		DNS Name	
		Domain	

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.

Approval - Qualys - VMDR Task: VTASK000

Approver: Cloud Application Owner
State: Requested

Comments: Comments

Activities: 1

System: Approvers: Cloud Application Owner, State: Requested

Update Approve Reject Delete

Summary of Item being approved

Qualys - VMDR Task

Number: VTASK000
Connector: Qualys - POD 1
Qualys Detection: [Progress Bar]
Creation Source: Automated - Qualys Integration

Qualys - VMDR Task

Number: VTASK000
Connector: Qualys - POD 1
Qualys Detection: [Progress Bar]
Creation Source: Automated - Qualys Integration

Host Information

Operating System: CentOS Linux 7.3.1611
Cloud Resource ID: [Redacted]
Asset Id: [Redacted]
Qualys Id: [Redacted]
TruRisk Criticality Score: [Redacted]
TruRisk Score: [Redacted]

Host Network Information

IP v4: [Redacted]
IP v6: [Redacted]
Host name: [Redacted]
Netbios: [Redacted]
FQDN: [Redacted]
DNS Name: [Redacted]
Domain: [Redacted]

Exception - Awaiting Approval
Approval: Requested
Vulnerability Status: Active
Severity level: 5 - Critical
Change request: [Redacted]
Assignment group: VMDR Windows Vulnerability Team
Assigned to: [Redacted]
QDS Severity: HIGH
Qualys detection score: 81

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.

Filter navigator

Qualys VMDR

- Exceptions
 - Pending My Approval
 - False Positive Requests
 - Pending My Approval
 - Knowledge Base
 - Confirmed
 - All

Approvals Search State Search

All > Approval for Task type is a (Qualys - VMDR Task, Qualys - VMDR Task Group, Qualys - VMDR Task) > State = Requested > Approval for State = Exception - Awaiting Approval > Approver = John Security Person

State	Approver	Approval for	Created
Requested	Security Person	VTASK0000233	2023-01-30 08:32:27
Requested	Security Person	VTGAP0021528	2022-11-16 10:40:28

Actions on selected rows...

1 to 2 of 2

Click the **State** column.

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

The screenshot shows the 'Qualys - VMDR Task' record page. The 'Approving' field is highlighted in yellow and has an information icon. The 'Open Record' button is located in the top right corner of the record view. The record details include:

- Number: VTASK0000
- Connector: Qualys - POD 1
- Qualys Detection: [Redacted]
- Creation Source: Automated - Qualys Integration
- State: Exception - Awaiting Approval
- Approval: Requested
- Vulnerability Status: Active
- Severity level: 5 - Critical
- Change request: [Redacted]
- Assignment group: VMDR Windows Vulnerability Team
- Assigned to: [Redacted]
- QDS Severity: HIGH
- Qualys detection score: 81

Host Information:

- Operating System: CentOS Linux 7.3.1611
- Cloud Resource ID: [Redacted]
- Asset Id: [Redacted]
- Qualys Id: [Redacted]
- TruRisk Criticality Score: [Redacted]
- TruRisk Score: [Redacted]

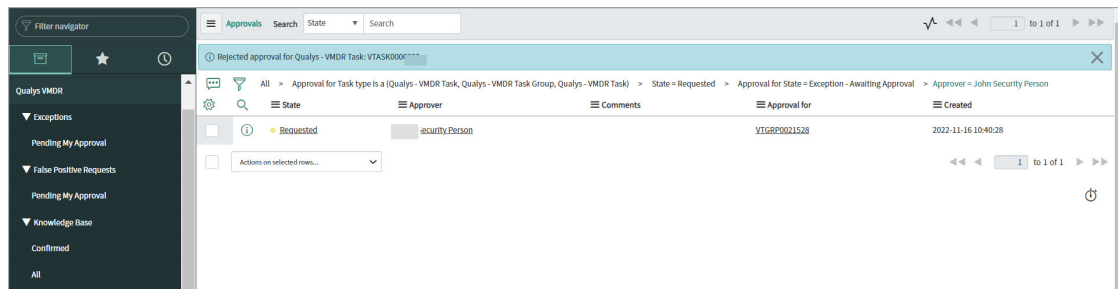
Host Network Information:

- IP v4: [Redacted]
- IP v6: [Redacted]
- Host name: [Redacted]
- Netbios: [Redacted]
- FQDN: [Redacted]
- DNS Name: [Redacted]
- Domain: [Redacted]

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

The screenshot shows the 'Qualys - VMDR Task' record page after adding a comment. The 'Comments' field contains the text: "This is not something we can make an exception to, as the vulnerability is to critical and the business system contains customer data." The 'Reject' button is highlighted. The record details are the same as in the previous screenshot.

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**.

Number: VTASK000

Connector: Qualys - POD 1

Qualys Detection: [Field]

Creation Source: Manual

Configuration Item: [Field]

Class: [Field]

Status: -- None --

State: Open

Vulnerability Status: Re-Opened

Severity level: 4 - High

Assignment group: VMDR Windows Vulnerability Team

Assigned to: [Field]

QDS Severity: -- None --

Qualys detection score: [Field]

Host Information

Operating System: FreeBSD 5.x / AIX 5.1-5.3 / MacOS

Cloud Resource ID: [Field]

Asset id: [Field]

Qualys id: [Field]

TruRisk Criticality Score: [Field]

TruRisk Score: [Field]

Host Network Information

IP v4: [Field]

IP v6: [Field]

Host name: [Field]

Netbios: [Field]

FQDN: [Field]

DNS Name: [Field]

Domain: [Field]

The **State** is changed to **False Positive- Identified**.

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

False Positive Reason

Documentation required to capture reasons

- logs
- screenshots

Update False Positive - Request Confirmation Delete

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**.

Domain: [Field]

Infrastructure / App Owner Approval Group: VMDR Cloud Application Approvers

Update False Positive - Request Confirmation Delete

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.

VMDR Approvals	Search	Approver	State	Comments	Approving	Group
<input type="checkbox"/>		cloud Application Owner	Approved		Qualys - VMDR Task-VTASKU	GAPRV0010050
<input type="checkbox"/>		Person	Requested		Qualys - VMDR Task-VTASKU	GAPRV0010051
<input type="checkbox"/>		Person	Requested		Qualys - VMDR Task-VTASKU	GAPRV0010051

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**.

Qualys - VMDR Tasks	Search	Number	State	Priority	Configuration item	Host asset	IP v4	QID	Title	Assignment group	Assigned to	Opened
<input type="checkbox"/>		VTAS*	False Positive - Confirmed	2 - High	(empty)			216108	VMware ESXi 3.5 Patch Release ESX350-200912401-BG Missing (KB1016657)	VMDR Windows Vulnerability Team	(empty)	2021-11-01 15:05:31
<input type="checkbox"/>		VTASK0	Open	3 - Moderate	(empty)			91709	Microsoft Sploitw64 Windows Elevation of Privilege Vulnerability	VMDR Windows Vulnerability Team	(empty)	2021-11-01 15:10:22
<input type="checkbox"/>		VTASKC	Exception - Awaiting Approval	3 - Moderate	(empty)			38657	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	VMDR Windows Vulnerability Team	(empty)	2021-11-01 15:16:01
<input type="checkbox"/>		VTAS	Exception - Awaiting Approval	2 - High	(empty)			100202	Microsoft Internet Explorer Multiple Remote Code Execution Vulnerabilities (MS14-035)	VMDR Windows Vulnerability Team	(empty)	2021-11-01 15:16:55

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.

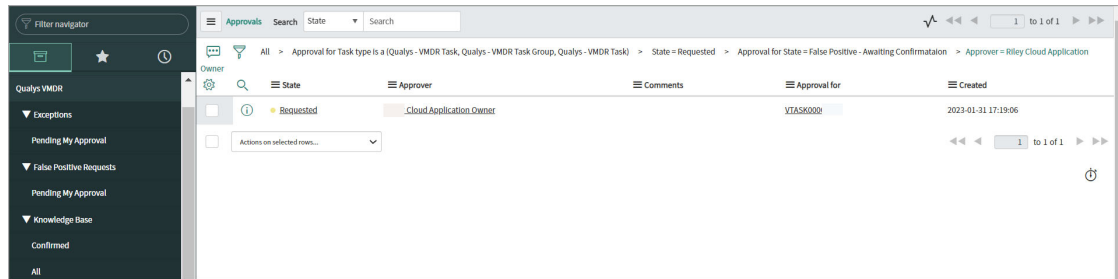
Note: This workflow is available only for the approver groups.

Approval Workflow

Log on to the application and go to Qualys VMDR.

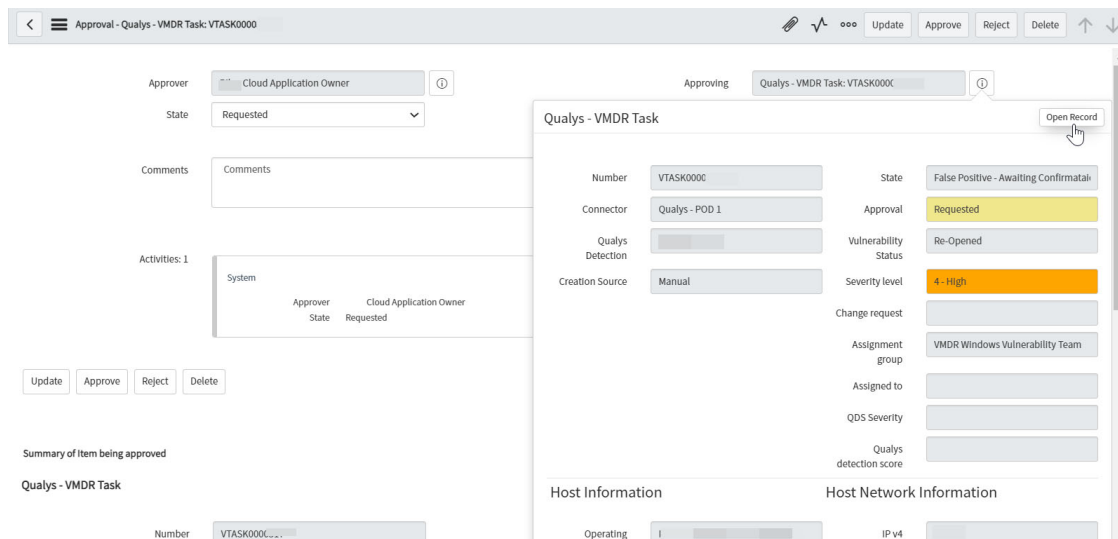
Click **False Positive** | **Pending My Approval**.

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.

The screenshot shows the 'Approval - Qualys - VMDR Task: VTASK0000' form. At the top right, there are buttons for 'Update', 'Approve', 'Reject', and 'Delete'. The 'Approve' button is highlighted with a mouse cursor. The form fields include:

- Approver:** Cloud Application Owner
- State:** Requested
- Comments:** Recorded as false positive. Confirmed.
- Activities:** 1
- System:** Qualys - VMDR Task: VTASK0000
- Field changes:** 2023-01-31 17:19:06

 At the bottom left, there are buttons for 'Update', 'Approve', 'Reject', and 'Delete'.

Click **Approve**.

A message is displayed that confirms the approval.

The screenshot shows the 'Approvals' list in the Qualys VMDR interface. A confirmation message is displayed at the top: 'Approved Qualys - VMDR Task: VTASK0000'. Below the message, the breadcrumb trail reads: 'All > Approval for Task type is a (Qualys - VMDR Task, Qualys - VMDR Task Group, Qualys - VMDR Task) > State = Requested > Approval for State = False Positive - Awaiting Confirmation > Approver = Riley Cloud Application'. The table below the message is empty, with the text 'No records to display' centered.

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.

	Title	Scanner	Option profile	Executed by	Executed on	Scan Status	Integration status
<input type="checkbox"/>	[SCNEXC00000003] launched from veno4911.s...	SNOWApp_Testing	2008 SANS20.Options	Nate Anderson	2021-10-27 18:52:49	Finished	Completed
<input type="checkbox"/>	[SCNEXC00000004] launched from veno4911.s...	SNOWApp_Testing	Initial Options	Nate Anderson	2021-10-28 13:22:40	Finished	Completed
<input type="checkbox"/>	[SCNEXC00000005] launched from veno4911.s...	SNOWApp_Testing	Initial Options	Nate Anderson	2021-10-28 13:35:39	Queued	Error
<input type="checkbox"/>	[SCNEXC00000006] launched from veno4911.s...	is_qualys_ma58_2	MCW_Sid VM Scan - No Auth - Fast - Web...	Nate Anderson	2021-10-29 08:59:20		Waiting - For Other Status Check
<input type="checkbox"/>	[SCNEXC00000007] launched	SNOWApp_Testing	Initial Options	David Granov...	2021-11-15 06:13:45	Finished	Completed

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

Detections

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

	Number	QID	Configuration Item	Qualys Host	Port	Protocol	Service	Vulnerability Status	First found	Last found	S
<input type="checkbox"/>	HDETECT0273478	20000	(empty)						2020-07-03 00:47:08	2020-07-03 00:47:08	1
<input type="checkbox"/>	HDETECT0273497		(empty)						2020-07-03 17:35:50	2020-07-03 17:35:50	1

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 withing 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.

The screenshot shows the 'Change Request' form in the 'New' state. The form is divided into several sections:

- Header:** Includes a navigation bar with tabs: New, Assess, Authorize, Scheduled, Implement, Review, Closed, and Canceled. The 'New' tab is active.
- Form Fields:**
 - Left Column:** Number (CHG1), Requested by (searchable), Category (Other), Service (searchable), Service offering (searchable), Configuration item (searchable), Priority (4 - Low), Risk (Moderate), Impact (3 - Low), Short description (Windows Patches for 2023-01-16), and Description.
 - Right Column:** Model (Normal), Type (Normal), State (New), Conflict status (Not Run), Conflict last run (searchable), Assignment group (T), and Assigned to (searchable).
- Planning Section:**
 - Planned start date and Planned end date are the requested change window:** A blue banner.
 - Planned start date:** 2023-01-16 17:44:33
 - Planned end date:** (empty)
 - CAB required:** (checkbox)
 - Actual start date:** (empty)
 - Actual end date:** (empty)
 - CAB delegate:** (searchable)
 - CAB recommendation:** (empty)

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.

Qualys PM - Deployment Job

Windows Patches for as of 2023-01-16

Update

Check UUIDs in Qualys

Create Patch Job

Name	Windows Patches for as of 2023-01-16		
Number	DPLVJ0R	Status	Error
Qualys - Job ID		Start Date/Time	2023-01-16 17:44:33
Task	CHG1I		
Connector	Qualys qg3 (mndra3sa)		

Configuration | Patches Information | Log

Activities: 7

System

Log • 2023-02-12 23:09:26

```
[0000005] - ERROR: [QualysPatchManagementAPI : getAssetUUIDs] - resp.getStatusCode():403  
[0000006] - ERROR: [QualysPatchManagementAPI : getAssetUUIDs] - resp.getBody() ["error":{"code":"403","errorCode":"","message":"'Access denied due to invalid license.'"}]  
[0000007] - ERROR: [QualysPatchManagementAPI : getAssetUUIDs] - resp.getErrorMessage(Method failed) (java.lang.IllegalStateException: Forbidden username/password combo)  
[0000008] - ERROR: [QualysPatchManagementAPI : getAssetUUIDs] - EXCEPTION THROWN IN (getAssetUUIDs) (message) An error occurred attempting to create the patch job. Please review the logs for details!  
[name]: Error  
[0000070] - ERROR: [Business rule : Create Patch Job] - EXCEPTION THROWN IN (Create Patch Job) (message): Was unable to make API Call or a Failure Occurred attempting to get UUIDs for assets([name]): Error
```

System

Field changes • 2023-02-12 23:09:26

Status Error was API Call In Progress - UUID Check

System

Field changes • 2023-02-12 23:09:25

Status API Call In Progress - UUID Check was Queued - UUID Check

System

Field changes • 2023-02-12 23:09:25

Status Queued - UUID Check was Error

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.

Job Items

Search

Number

▼

Search

Job - Windows Patches for 1

s of 2023-01-16

Number

▲

Host Asset

Qualys UID

QIDs

Actual start

Actual end

Status

Status code

Failed patches

Installed patches

Success patches

DPLVIT

demowin

370405, 30620, 100232, 91634, 91254, 90740, 91038, 91495, 100114, 91642, 375718, 91674, 120274, 91653, 121843, 370427, 372247, 121279, 372020, 91560, 374531

(empty)

(empty)

Error - No UID Found in ServiceNow

DPLVIT

demow

100413, 373156, 100359, 91408, 91182, 91405, 91099, 370297, 91461, 100381, 91151, 91333, 91449, 91758, 91481, 91395, 91359, 100317

(empty)

(empty)

Error - No UID Found in ServiceNow

DPLVIT

DEM

91485, 100399, 100408, 91353, 91771, 91443, 91563, 91453, 91605, 100412, 100359, 91591, 91340

(empty)

(empty)

Error - No UID Found in ServiceNow

Show Matching

Filter Out

Copy URL to Clipboard

Assign Tag

Cancel - ignore

YL Row

- 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**.

The screenshot shows the 'Qualys PM - Deployment Job' configuration page for 'Windows Patches'. The page has a top navigation bar with 'Update', 'Refresh Status', and 'View in Qualys' buttons. The main content area is divided into two tabs: 'Configuration' (selected) and 'Patches Information'. Under the 'Configuration' tab, there are fields for 'Name' (Windows Patches), 'Number' (DPLVJOBK), 'Status' (Waiting - For Next Scheduled Status Check), 'Qualys - Job ID' (8197a91f-...), 'Start Date/Time' (2023-02-23 17:47:03), 'Task' (CHGL), and 'Connector' (Qualys Demo Account). Below these fields, there are sections for 'Platform' (Windows), 'Schedule type' (Once), 'Opportunistic downloads' (checked), and 'Time zone type' (Agent time zone). At the bottom, there are 'Update', 'Refresh Status', and 'View in Qualys' buttons.

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.

The screenshot shows the 'Qualys Cloud Platform' interface for 'Job Details: Windows Patches Vulnerability Team'. The page has a left sidebar with a 'VIEW MODE' dropdown and a list of tabs: 'Basic Information' (selected), 'Assets', 'Pre-actions', 'Patches', 'Post-actions', 'Options', and 'Job Access'. The main content area is divided into two sections: 'Basic Information' and 'Identification'. The 'Basic Information' section shows the job name 'Windows Patches Vulnerability Team', its status 'Enabled', and job type 'Install'. The 'Identification' section shows the job's GUID, description 'Windows Patches Vulnerability Team', scheduled time 'Once, Feb 17, 2023 01:46 am', created on 'Feb 7, 2023 11:05 PM', time zone 'Default Agent Timezone', modified on '-', owner 'quays2nh56', patch window 'None', and next schedule 'Feb 17, 2023 04:16 AM' with a run time of 'Runs in 2 days 6 hours 27 minutes 40 seconds'. A 'Show All...' link is also present.

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.

The screenshot shows the 'Qualys PM - Deployment Job' configuration page. The job is titled 'Windows Patches for 1' and is in an 'Error' status. The configuration details are as follows:

Field	Value
Name	Windows Patches for 1 as of 2023-01-16
Number	DPLVJOB00
Qualys - Job ID	
Task	CHG1805324
Connector	Qualys - POD 1
Platform	Windows
Schedule type	Once
Time zone type	Agent time zone
Opportunistic downloads	<input checked="" type="checkbox"/>

Buttons at the bottom: Update, Create Patch Job.

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 screenshot shows the 'Qualys PM - Deployment Job' configuration page after the job has been created. The status has changed to 'Waiting - For Next Scheduled Status Check'. The configuration details are as follows:

Field	Value
Name	Windows Patches for 1 2023-01-16
Number	DPLVJOB00
Qualys - Job ID	7b0b301
Task	CHG1
Connector	Qualys Demo Account
Platform	Windows
Schedule type	Once
Time zone type	Agent time zone
Opportunistic downloads	<input checked="" type="checkbox"/>

Buttons at the bottom: Update, Check UUIDs in Qualys, Create Patch Job.

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 screenshot shows the 'Qualys PM - Deployment Job' configuration page. The job is titled 'Windows Patches for 1' and is in a 'Waiting - For Next Scheduled Status Check' status. The configuration details are as follows:

Field	Value
Name	Windows Patches for 1 as of 2023-01-16
Number	DPLVJOB00
Qualys - Job ID	c7b5b5af
Task	CHG18
Connector	Qualys Demo Account
Platform	Windows
Schedule type	Once
Time zone type	Agent time zone
Opportunistic downloads	<input checked="" type="checkbox"/>

Buttons at the bottom: Update, Refresh Status, View in Qualys.

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

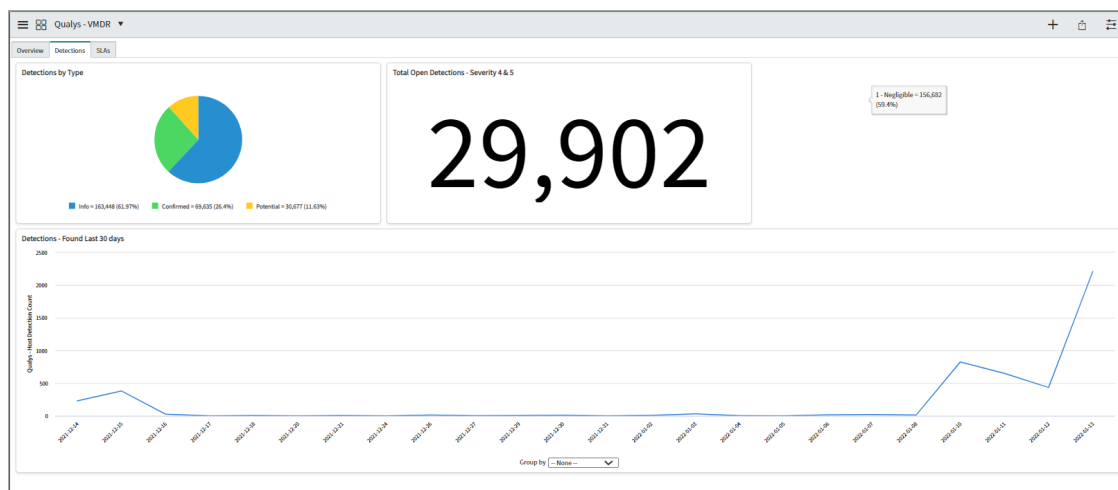
Go to Qualys VMDR App > **Overview**.



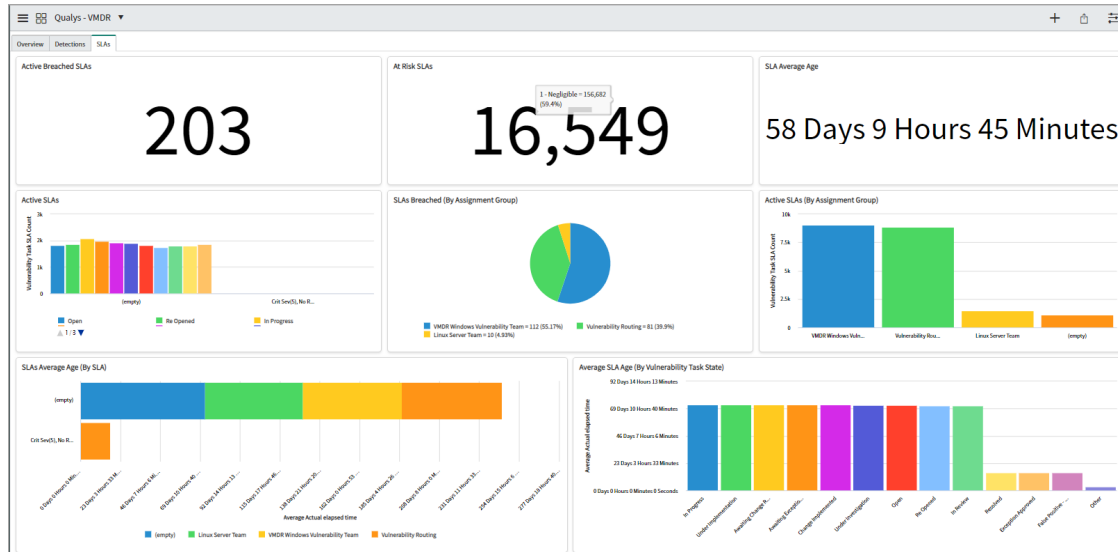
The **Overview** page displays a consolidated view of all the reports for vulnerabilities, detection, hosts, and so on.



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.



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**.

The screenshot shows the 'Create a report' form with the following sections:

- Report Title:** A field for entering the report title.
- Report name:** A field for entering the report name.
- Source type:** A dropdown menu with 'Data source' selected.
- Data source:** A dropdown menu with 'No data source selected'.
- Next:** A button to proceed to the next step.
- Analytics Q&A:** A section titled 'Create your report with Analytics Q&A' with a text input field 'What do you want to see?' and an 'Ask' button.
- How can I improve my results?:** A link to improve results.

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.

The screenshot shows the 'Create a report' interface with the 'Data' tab selected. The form includes the following fields:

- Report name:** Log4j New
- Source type:** Table
- Table:** Qualys - Vulnerability Task [x_qual5_vmdr_vuln_t...]
- Description:** There is no description for this table. To add a description, please contact your admin.

A 'Next' button is located at the bottom of the form.

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.

The screenshot shows the 'Create a report' interface with the 'Type' tab selected. The form includes the following elements:

- Filter the visualizations:** A dropdown menu with 'Bars' selected.
- Report Title:** Log4j New
- Table:** Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]
- Visualizations:** A section titled 'Log4j New' showing a table of vulnerability data.

Number	State	Severity level	Priority	IP v4	Vulnerability Status	Assignment group	Assig
VTASK0189381	Open	4 - High	2 - High		Active	Vulnerability Routing	(err
VTASK0189973	Open	3 - Medium	3 - Moderate		Active	Vulnerability Routing	(err

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.

Create a report

Save Run

Data > Type > **Configure** > Style

Report Title : Log4j New

What do you want to see? Ask How can I improve my results?

To modify the current report, use the left panel or [Edit Condition](#).

Table: Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]

All

Log4j New

Number	State	Severity level	Priority	IP v4 ▲	Vulnerability Status	Assignment group	Assign
VTASK0189381	Open	4 - High	2 - High		Active	Vulnerability Routing	(err
VTASK0189973	Open	3 - Medium	3 - Moderate		Active	Vulnerability Routing	(err

Back Next

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 the 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.

Table: Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]

All

Add Sort

Clear All

CONDITIONS

All of these conditions must be met

Qualys Detect...

OR

AND

Qualys

Qualys Detection → Qualys Detection Fields

Qualys Detection

Qualys Host

Results

Service

Sys ID

Tags

Times found

Type

Updated

Updated by

Updates

Vulnerability Status

status

Assignment gr

Vulnerability

Routing

- Select the operator and appropriate values.

Table: Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]

All

Add Sort

Clear All

▼

CONDITIONS

All of these conditions must be met

Qualys Detect...

▼

is one of

▼

New

Active

Re-Opened

Fixed

⊖

OR

AND

or

New Criteria

▶

RELATED LIST CONDITIONS

?

- 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.

Table: Qualys - Vulnerability Task [x_qual5_vmdr_vuln_task]

All > Qualys Detection Vulnerability Status in (New, Active, Re-Opened) >

Qualys Detection QID QID in , [...]

Add Sort Clear All

CONDITIONS

All of these conditions must be met

Qualys Detect... is one of New Active Re-Opened Fixed

Qualys Detect... is one of , , ,

or

New Criteria

RELATED LIST CONDITIONS

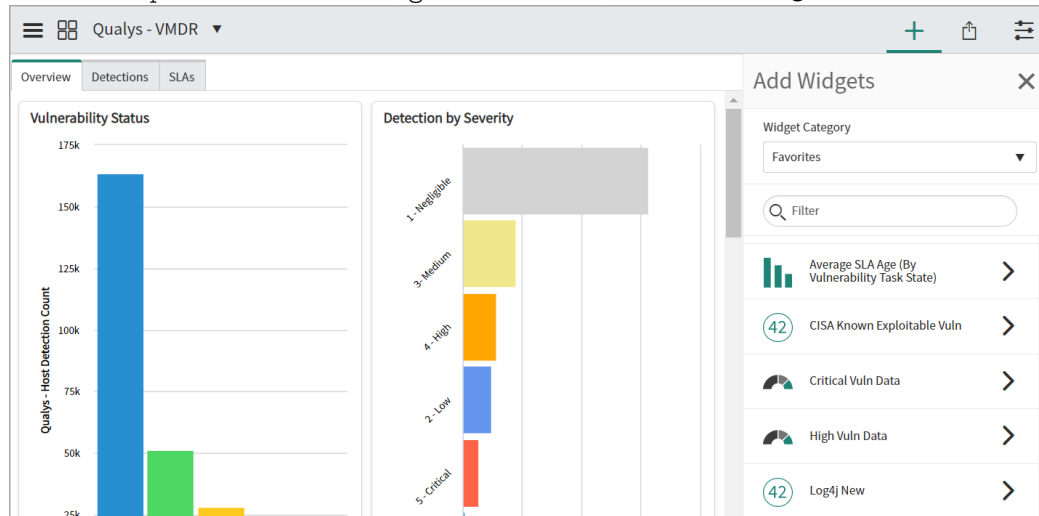
The filter conditions are added. Click **Run** to apply the conditions.

Add a Report to Dashboard

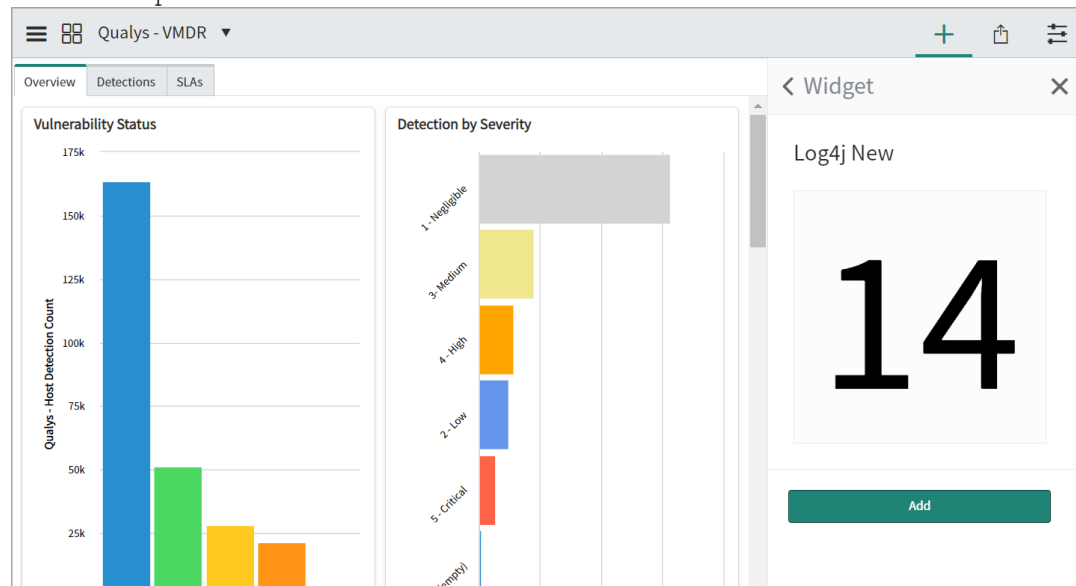
Once you add a report to the dashboard, you can view the report in the in the **Overview** and track the change in the report data at a glance.

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.

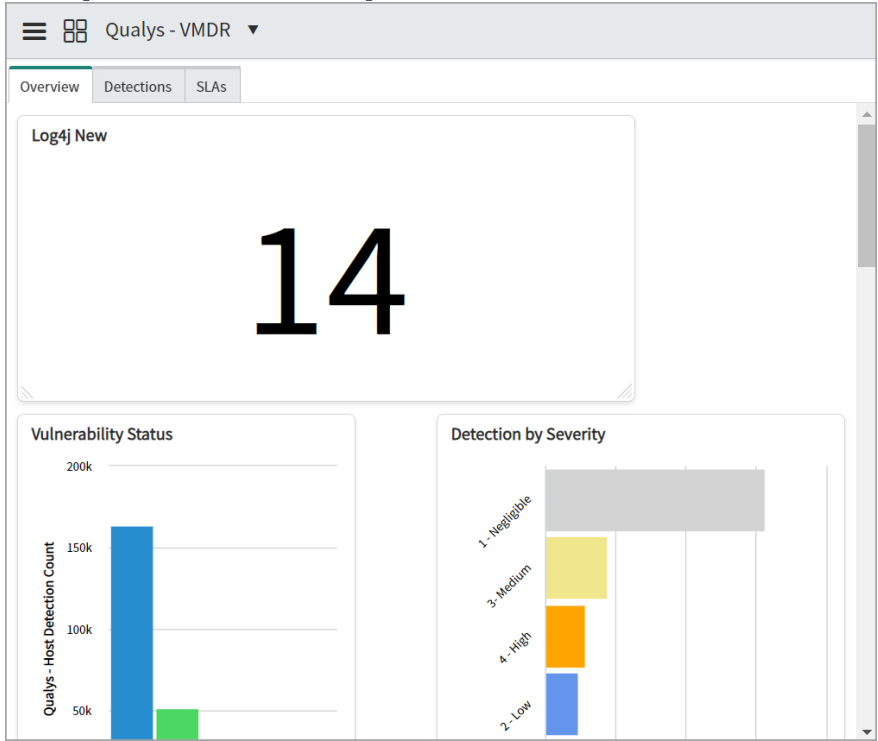
To add a report the dashboard, go to **Overview**, click **Add Widgets** icon.



Click the report to be added and click **Add**.



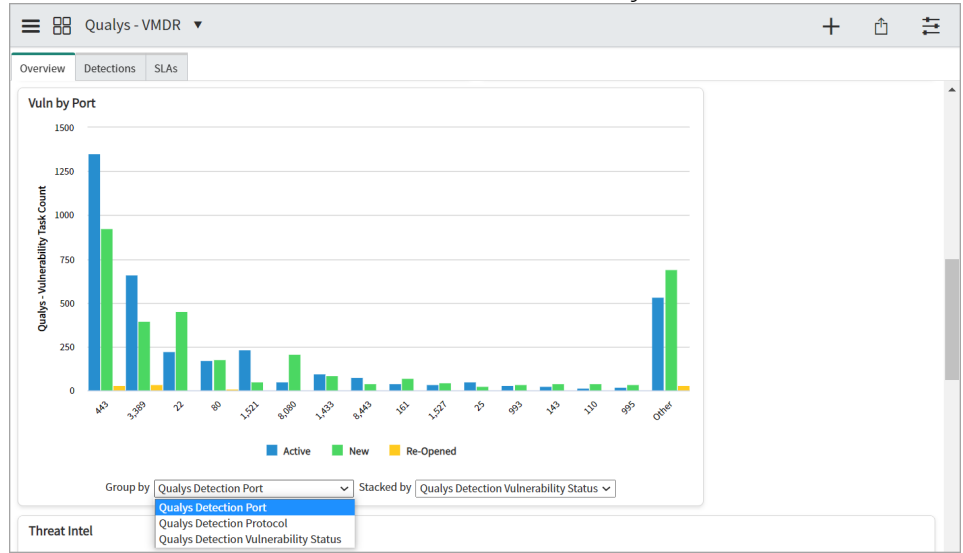
The report is added to the top of the dashboard.



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.

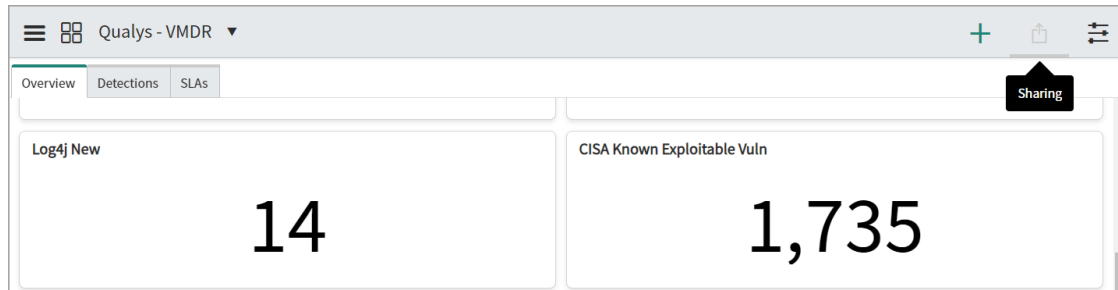


Share the report

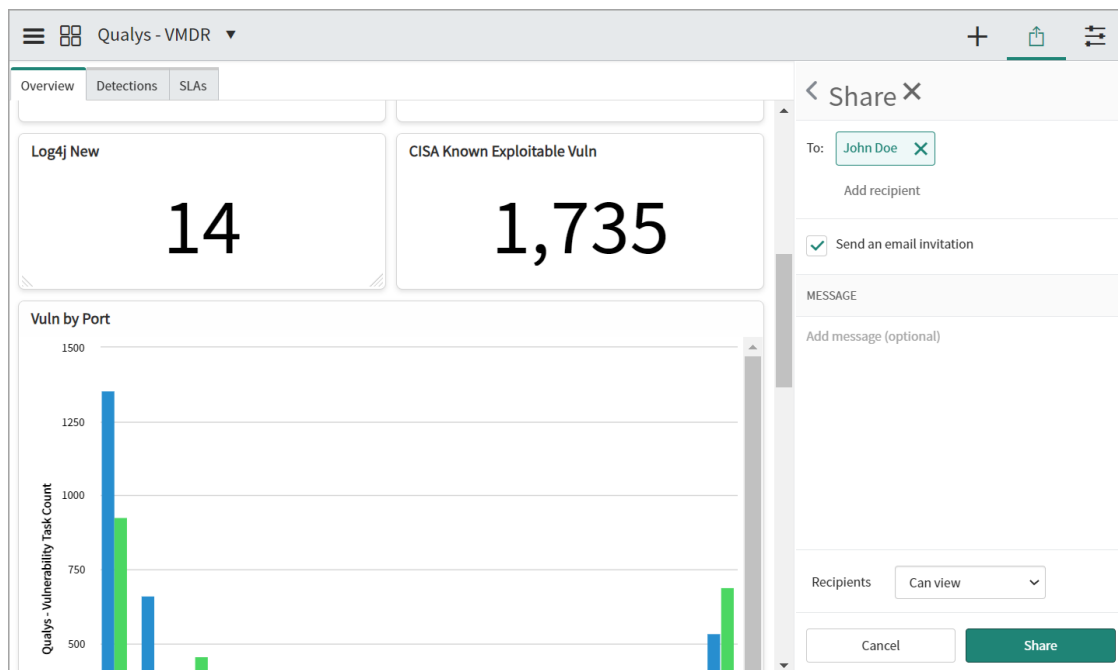
Once you add a report that you have created to the dashboard, only you can view it on the dashboard.

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.



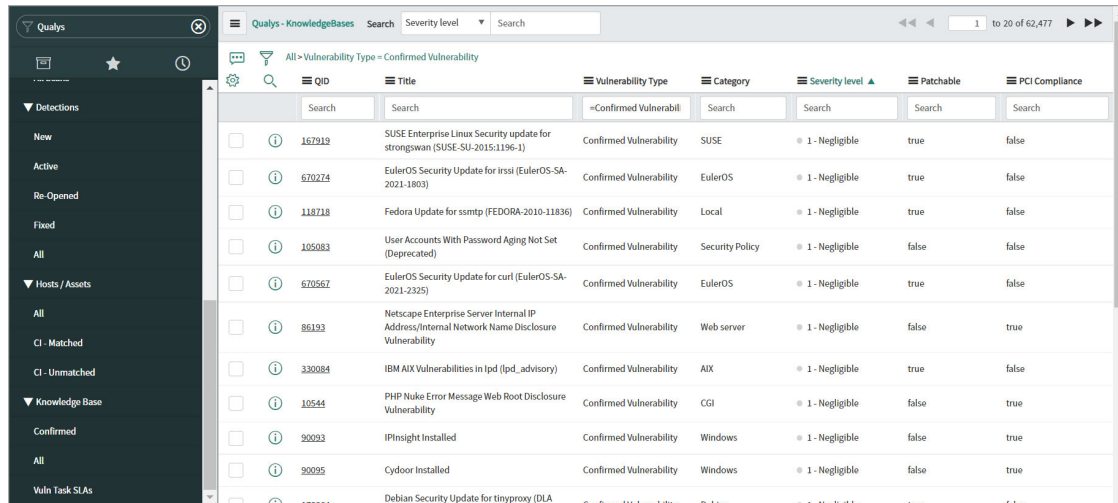
In the **Share** form, add a user name in the recipients, and click **Share**.



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

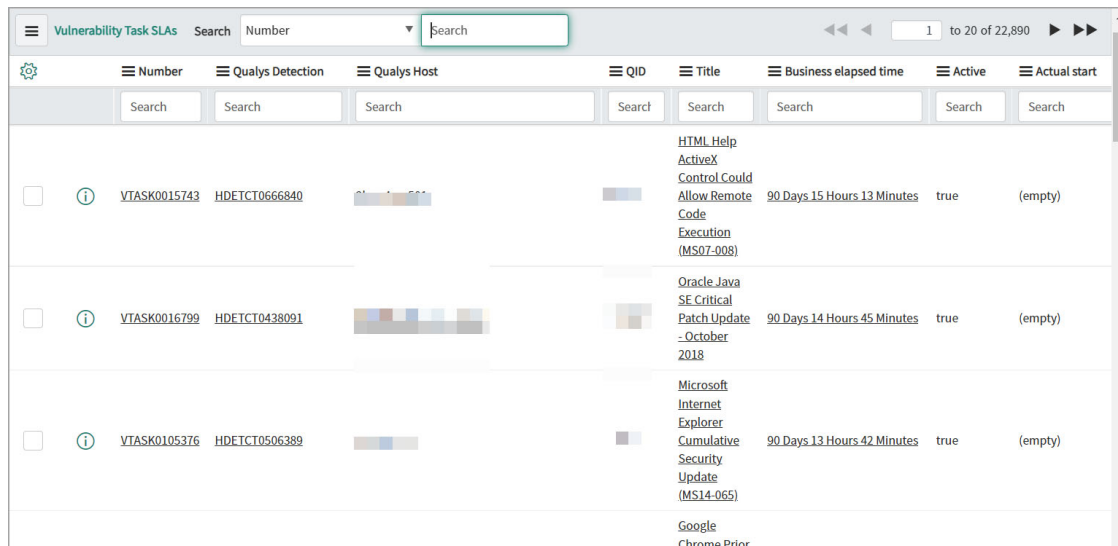
You can view Qualys KnowledgeBase in the Qualys VMDR application.



The screenshot shows the Qualys KnowledgeBase interface. On the left is a sidebar with navigation options: Detections (New, Active, Re-Opened, Fixed, All), Hosts / Assets (All, C1 - Matched, C1 - Unmatched), and Knowledge Base (Confirmed, All, Vuln Task SLAs). The main panel displays a table of vulnerabilities filtered by 'All - Vulnerability Type = Confirmed Vulnerability'. The table has columns for QID, Title, Vulnerability Type, Category, Severity level, Patchable, and PCI Compliance. The first few rows show updates for SUSE, EulerOS, Fedora, and User Accounts.

QID	Title	Vulnerability Type	Category	Severity level	Patchable	PCI Compliance
167919	SUSE Enterprise Linux Security update for strongswan (SUSE-SU-2015:1196-1)	Confirmed Vulnerability	SUSE	1 - Negligible	true	false
670274	EulerOS Security Update for irssi (EulerOS-SA-2021-1803)	Confirmed Vulnerability	EulerOS	1 - Negligible	true	false
118718	Fedora Update for ssmtp (FEDORA-2010-11836)	Confirmed Vulnerability	Local	1 - Negligible	true	false
105083	User Accounts With Password Aging Not Set (Deprecated)	Confirmed Vulnerability	Security Policy	1 - Negligible	false	false
670567	EulerOS Security Update for curl (EulerOS-SA-2021-2325)	Confirmed Vulnerability	EulerOS	1 - Negligible	true	false
86193	Netscape Enterprise Server Internal IP Address/Internal Network Name Disclosure Vulnerability	Confirmed Vulnerability	Web server	1 - Negligible	false	true
330084	IBM AIX Vulnerabilities in lpd (lpd_advisory)	Confirmed Vulnerability	AIX	1 - Negligible	true	false
10544	PHP Nuke Error Message Web Root Disclosure Vulnerability	Confirmed Vulnerability	CGI	1 - Negligible	false	true
90093	IPinsight Installed	Confirmed Vulnerability	Windows	1 - Negligible	false	true
90095	Cydoor Installed	Confirmed Vulnerability	Windows	1 - Negligible	false	true
128364	Debian Security Update for tinyproxy (DLA-2021-128364)	Confirmed Vulnerability	Debian	1 - Negligible	true	false

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.



The screenshot shows the 'Vulnerability Task SLAs' interface. It features a sidebar with a search bar and a main table. The table has columns for Number, Qualys Detection, Qualys Host, QID, Title, Business elapsed time, Active, and Actual start. The first three rows show tasks for HTML Help ActiveX Control, Oracle Java SE Critical Patch Update, and Microsoft Internet Explorer Cumulative Security Update.

Number	Qualys Detection	Qualys Host	QID	Title	Business elapsed time	Active	Actual start
VTASK0015743	HDETECT0666840			HTML Help ActiveX Control Could Allow Remote Code Execution (MS07-008)	90 Days 15 Hours 13 Minutes	true	(empty)
VTASK0016799	HDETECT0438091			Oracle Java SE Critical Patch Update - October 2018	90 Days 14 Hours 45 Minutes	true	(empty)
VTASK0105376	HDETECT0506389			Microsoft Internet Explorer Cumulative Security Update (MS14-065)	90 Days 13 Hours 42 Minutes	true	(empty)
				Google Chrome Prior			

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.

System Configuration

Qualys for ServiceNow Logging

Logging Level
Level of logging in the Apps

Debug

Max Cumulative Log Entries
Max number of log entries in a cumulative log before it writes to the log file

200

Max Cumulative Log Size
The general max string size of a log before it triggers the app logger to write the cumulative log to the System Log

20000

Save

View Logs

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

App Log **New** **Search** **Created** **Search**

All > Created on Today > App Scope Name starts with Qualys Core

Created **Level** **Message** **App Scope** **Source Script**

Search Search Search

Qualys Core SystemLogHelper

```
[0000001] - INFO: [SchedDataImp.JobUtils: preScript] - ENTERING
[0000002] - DEBUG: [SchedDataImp.JobUtils: preScript] - schedDataImpId: bd83caa3871374507bb3a86e0ebb3542
[0000003] - DEBUG: [SchedDataImp.JobUtils: preScript] - cancel: false
[0000004] - DEBUG: [SchedDataImp.JobUtils: preScript] - data_source: [object GlideRecord]
[0000005] - DEBUG: [SchedDataImp.JobUtils: preScript] - import_set: [object GlideRecord]
[0000006] - INFO: [DataTransferChunkHelper: initialize] - ENTERING/EXITING
[0000007] - INFO: [ImportDefinitionHelper: getFirstActiveDefinitionUsingSchedDataImportAsThread] - ENTERING
[0000008] - DEBUG: [ImportDefinitionHelper: getFirstActiveDefinitionUsingSchedDataImportAsThread] - schedDataImpId: bd83caa3871374507bb3a86e0ebb3542
[0000009] - INFO: [ImportDefinitionHelper: getFirstActiveDefinitionUsingSchedDataImportAsThread] - res.getEncodedQuery():
active=true*import_threads*CONTAINS*bd83caa3871374507bb3a86e0ebb3542
[0000010] - DEBUG: [ImportDefinitionHelper: getFirstActiveDefinitionUsingSchedDataImportAsThread] - Definition record was found
[0000011] - INFO: [ImportDefinitionHelper: getFirstActiveDefinitionUsingSchedDataImportAsThread] - LEAVING
[0000012] - INFO: [SchedDataImp.JobUtils: preScript] - Found a definition record: true
[0000013] - INFO: [SchedDataImp.JobUtils: preScript] - Found no active jobs
[0000014] - DEBUG: [SchedDataImp.JobUtils: preScript] - definition: [object GlideRecord]
[0000015] - DEBUG: [SchedDataImp.JobUtils: preScript] - res.getEncodedQuery():
sys_idInId3caa3871374507bb3a86e0ebb3542*active=true
[0000016] - INFO: [SchedDataImp.JobUtils: preScript] - LEAVING
[0000017] - INFO: [DataTransferJobHelper: getActiveJobForDefinition] - ENTERING
[0000018] - DEBUG: [DataTransferJobHelper: getActiveJobForDefinition] - definition: [object GlideRecord]
[0000019] - INFO: [DataTransferJobHelper: getActiveJobForDefinition] - Found no active jobs
[0000020] - INFO: [DataTransferJobHelper: getActiveJobForDefinition] - LEAVING
[0000021] - INFO: [SchedDataImp.JobUtils: preScript] - No active job was found
[0000022] - INFO: [SchedDataImp.JobUtils: preScript] - Major Decisions in this Execution:
{
  "Working with definition record: true",
  "No active job was found. Exit and Slow the Threads Down."
}
```

Known Issues

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