# Table of Contents

**About this Guide** ............................................................................................................ 4  
About Qualys .................................................................................................................. 4  
Qualys Support ............................................................................................................. 4  

**VMDR OT Overview** .................................................................................................... 5  
Introduction ..................................................................................................................... 5  
Why Qualys VMDR OT? .................................................................................................... 7  
Concepts and Terminologies .............................................................................................. 8  
Know the Requirements .................................................................................................. 8  
How does Qualys VMDR OT work? ................................................................................... 9  

**Get Started with VMDR OT** ....................................................................................... 10  
User Roles and Permissions ............................................................................................. 10  
Deploying Qualys Network Passive Sensors ................................................................... 17  
Viewing Assets Details .................................................................................................... 18  
Generating Traffic Using Device Discovery Method ......................................................... 21  
Viewing Vulnerabilities ..................................................................................................... 21  
Viewing KnowledgeBase ................................................................................................. 24  
Viewing Network Traffic .................................................................................................. 25  
Tagging Assets .................................................................................................................. 26  
Importing Assets ............................................................................................................... 29  

**Managing VMDR OT Dashboards** ............................................................................. 33  

**Appendix A - Supported OT Protocols** ..................................................................... 36  

**Appendix B - Supported IT Protocols** ...................................................................... 37  

**Appendix C - Supported OCA** ................................................................................ 38
About this Guide

Thank you for your interest in Qualys VMDR OT. Qualys VMDR OT provides comprehensive visibility and vulnerability management for critical infrastructure across all industrial network layers - Control, Supervisory, and Site Operations.

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 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/
VMDR OT Overview

Qualys VMDR OT, provides a real-time asset inventory, network visibility, and vulnerability management for industrial control systems. Qualys VMDR OT serves as a powerful tool to reduce the risk of costly and dangerous cyber security breaches with an intuitive interface and a fully automated risk assessment workflow. Qualys provides a single application and a single pane of glass for all IT & OT Asset Inventory, Vulnerabilities Management, Policy Compliance as well as OT Endpoint based Threat Detection and Response.

Introduction

Industrial IoT (IIOT) and smart manufacturing greatly enhance the Overall Equipment Efficiency (OEE) and cost savings. However, they also increase enterprises’ exposure to cyber-attacks due to rapid digitization and newly established interconnectivity between previously air-gapped industrial environments and the enterprise networks. Industrial assets have higher availability and reliability requirements. Their functioning round the clock and malfunctions can potentially lead to significant physical safety incidents. Any downtime incurred by making changes or installing updates to these systems need careful planning to ensure the minimum level of service disruption.

Typically, industrial processes are supported by multiple equipment manufactured by different industrial vendors and powered by varied industrial protocols such as Ethernet/IP, Modbus TCP, Siemens S7 Comm, S7Comm Plus, Profinet, BACnet, and DNP3, among others. Many of these protocols are insecure by design, lacking basic authentication and encryption, so it is even more critical to have visibility and regular risk assessments conducted in these environments.

VMDR OT security is defined as protecting industrial control systems from threats from cyber attackers. It is often referred to as OT security. It includes a wide range of practices including asset inventory and detection and vulnerability management.

Identifying network vulnerabilities is the most crucial step. Qualys VMDR OT identifies the existing vulnerabilities and recommends a cyber risk mitigation solution.

The Purdue model is a reference architecture model for VMDR OT. It divides the system into multiple levels: Purdue level 0 to Purdue level 5.

As shown in the following Purdue level reference model, the VMDR OT provides asset inventory, network visibility, and vulnerability postures at all Purdue levels.

**Qualys Network Passive Sensor** can latch on the mirrored port of a network switch which can see traffic from assets present in Purdue levels 0, 1 and 2 and passively listen to traffic, dissect the protocol, and build the asset inventory.

**Qualys Active Scanner** can be used in safe scanning mode to support the industrial scan. It can safely discover PLC, RTU, and equipment running at the controller layer without disrupting the environment. Qualys Active Scanner can also scan the end points present
in levels 2, 3, and 3.5 to take care of all engineering workstation and SCADA servers, operating stations, site operation equipment like manufacturing execution system, ERP, jump-boxes in RTU.

Launch OT Device scans and start getting up-to-date views on your OT Assets and security posture using Qualys Industrial Control System. You can use OT device scan feature in VM/VMDR. OT Device Scan is provided for the safe active scan. It is a protocol-oriented scan that fetches identity-related attributes. VMDR OT collects the data from VM/VMDR, extracts the information and detects the vulnerability. For more details on OT Device scan refer to Vulnerability Management Online help.

**Qualys Cloud Agents** deployed in these environments can provide continuous visibility and continuous posture of vulnerabilities.

**VMDR OT Out of band Configuration Assessment** can also be used for building asset inventory. This is useful in case of other methods (Qualys Network Passive Sensor or Qualys Cloud Agent) of creating asset inventory is not available.

Refer to the following table to view the VMDR OT features availability on Qualys applications.

<table>
<thead>
<tr>
<th>Purdue Level</th>
<th>Assets</th>
<th>Feature</th>
<th>Supported by</th>
<th>Available on Qualys Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purdue Levels 0/1/2</td>
<td>Hardware like PLC, RTU, IO, Robots, VFDs etc</td>
<td>Asset Inventory, Vulnerability Management</td>
<td>Qualys Network Passive Sensor, VMDR OT Out of band configuration assessment</td>
<td>VMDR OT</td>
</tr>
</tbody>
</table>
Why Qualys VMDR OT?

Real-time VMDR OT Asset Inventory
Qualys VMDR OT builds a comprehensive real-time asset inventory via multiple engines:
- Qualys Network Passive Sensor dissects industrial protocols and gives visibility into various Purdue Levels, especially at Field and Control network layers.
- Qualys extends the scanner capabilities to perform safe VMDR OT discovery for industrial protocols. This new scan is designed to be safe and talks in the same language as industrial protocols querying the devices in the protocol language they understand.
- VMDR OT Out of band Configuration Assessment import the assets from using the project files collected from programming and maintenance software.

Extensive Industrial Protocol Support
Qualys VMDR OT supports a wide range of IT and OT protocols such as S7Comm, S7comm Plus, Profinet, Ethernet IP, BACnet, Modbus TCP, DNP3, MQTT, IEC 104, CIP, IEC 61850-MMS, Beckhoff ADS, Omron, PCCC, Niagara Fox, and many more.

Out of band Configuration Assessment
Qualys supports Out of band Configuration Assessment. You can import the asset information using a project file, collected from programming and maintenance software. The VMDR OT application parses the uploaded file with valuable data and creates assets from the data gathered. Qualys supports different vendors engineering tools such as Omron CX Programmer (.cxp), Rockwell RSLogix 500 (.RSS), Rockwell Studio 5000 (.L5X), Rockwell System Ferret (.Xml), Siemens DIGSI 4 (.zip), Siemens DIGSI 5 (.zip), Siemens DIGSI 5 (.dz5), and many more.
Robust Vulnerability Management
Qualys VMDR OT provides continuous vulnerability assessment on all discovered industrial assets. Hardware and firmware-based vulnerabilities impact PLCs, IOs, HMIs, Drives, etc., and software vulnerabilities affecting SCADA servers, Engineering software, HMI Software, etc., are covered via Passive sensor and Qualys scanner or a Cloud agent combined.

Risk scores are based on asset criticality, severity of vulnerability, and availability of redundancy for the asset to assist with better prioritization and remediation actions.

Broad Industrial Vendor Support
Qualys VMDR OT supports the major industry vendors like Siemens, Rockwell Automation, Schneider Electric, Wago, Johnson Controls, Niagara Fox, Beckhoff, Omron, ABB, and many more.

Concepts and Terminologies
Get familiar with common terms used in the VMDR OT application.

<table>
<thead>
<tr>
<th>Terms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QID</td>
<td>It is a unique Qualys ID number assigned to the vulnerability.</td>
</tr>
<tr>
<td>QQL</td>
<td>Qualys Query Language (QQL) for building search queries are used to fetch information from Qualys databases.</td>
</tr>
<tr>
<td>Severity Score</td>
<td>Qualys assigns every vulnerability in the Knowledge Base a severity score that is determined by the security risk associated with its exploitation.</td>
</tr>
<tr>
<td>CVE ID</td>
<td>CVE (Common Vulnerabilities and Exposures) lists common names for publicly known vulnerabilities and exposures. These are CVE name(s) associated with this vulnerability check.</td>
</tr>
<tr>
<td>Confirmed vulnerabilities</td>
<td>These are the vulnerabilities that are positively identified by QualysGuard.</td>
</tr>
<tr>
<td>Potential vulnerabilities</td>
<td>These are the vulnerabilities that cannot be fully verified. In these cases, at least one necessary condition for the vulnerability is detected.</td>
</tr>
<tr>
<td>CVSS</td>
<td>Common Vulnerability Scoring System is an industry open standard designed to convey vulnerability severity and risk.</td>
</tr>
</tbody>
</table>

Know the Requirements
Industrial Control System application can be accessed with a subscription to VMDR, Cyber Security Asset Management (CSAM) and Qualys Network Passive Sensor (NPS) applications.
How does Qualys VMDR OT work?

VMDR OT is powered by Qualys Network Passive Sensor. It continuously monitors all network traffic and flags any asset activity. It identifies and profiles devices the moment it is connected to the network.

Qualys Network Passive Sensor (NPS) identifies assets in industrial environment that can’t be actively scanned. Qualys Network Passive Sensor (NPS) enriches existing asset inventory with additional details, such as recent open ports, traffic summary, network services and applications in use. Updating the asset inventory helps to gain a deeper understanding of an asset and its activity on the network in real time.

**Asset discovery and collect Inventory** - Once Qualys Network Passive Sensor (NPS) is deployed and configured in the network, it starts passively listening to the network traffic and creating assets based on the information dissected from the traffic. For more details on deployment, refer to Deploying Qualys Network Passive Sensors.

Over the period of time, with various asset activities seen on the wire, the passive sensor will continue to enhance the asset inventory attributes with additional contextual information. The time taken for a complete asset context to be built is based on the type of industrial protocol and type of activities performed in the environment.

To expedite the asset discovery, refer to section Generating Traffic Using Device Discovery Method.

Asset inventory can also be created using VMDR OT Out of band configuration assessment using the project files collected from programming and maintenance software. For more information refer to section Importing Assets.

**Detect and Monitor** - Qualys Network Passive Sensor (NPS) monitors network activity without any active probing of devices to detect active assets in the network. The VMDR OT asset inventory is continuously updated depending on the asset activities flagged by the Qualys Network Passive Sensor (NPS). For information about the VMDR OT asset inventory, see Assets tab.

To view network traffic which displays the communication between server and client refer to section Viewing Network Traffic.

Vulnerabilities on industrial assets are detected and listed on the vulnerabilities tab. For more information refer to section Viewing Vulnerabilities.
Get Started with VMDR OT

Start building VMDR OT inventory by
- Deploying Qualys Network Passive Sensors (NPS).
- Importing Assets using VMDR OT Out of band configuration assessment.
- Generating Traffic Using Device Discovery Method from Programming software for configuring and managing the network devices.

User Roles and Permissions

Users can be created and assign a role to grant access as per the role defined. We support multiple user roles.

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager Users</td>
<td>The most privileged users are Manager users. They have full privileges and access to all resources in the subscription. Only Manager users can create users and assign roles. Manager users can choose how the user can access the application.</td>
</tr>
<tr>
<td>Users</td>
<td>Depending on the permissions assigned to the role, users can be categorized with all privileges or read-only privileges.</td>
</tr>
</tbody>
</table>

New Users: Scope and Permissions

Only Manager users have permissions to create new users and grant them permissions. Let us view the high level steps.

1) Create a User

You need to create a new user using Administration application. Managers can add users, up to the number allowed for the subscription service level. Follow these steps:

1. Navigate to Administration module > User Management > Create User > Create Reader User.
2. Provide the necessary information for the user creation such as General Information, Locale, User Role, Asset Groups (optional), Permissions, Options, and Security.

Ensure that you select at least Reader role for User Role. For all other options you can retain the default settings.

3. Click Save.

2. Grant permissions to the user

You can define a role and then assign this defined role to the user. The role you define decides the permissions assigned to the user. You can do this by editing the user’s account. For example, to create a user with full access, you must enable all the permissions in a role and assign the role to the user. You can assign the role to assign full access to multiple users at one go.

3. Validation after adding a new user

When you create a new user, the user appears on the user accounts list with a status of Pending Activation. The user will receive a registration email with a secure one-time-only link to the credentials for their new account and login instructions. The registration email is sent to the email address defined in the user’s account. The user’s status changes to Active after logging in for the first time.

Note: Users with a Contact user role do not receive login credentials and cannot log in to the application.
4. Assign Roles to Users

(Managers) Use the Administration utility (last option in the application selector) to view and manage users and grant access to the VMDR OT application. On the User Management tab, you can see the applications each user has access to. Access is role based.

You can also refer to the Online help available in the Administration utility for detailed information.

Knowing various roles

You can configure two types of user roles:

- User with all privileges: We provide a predefined role named VMDR OT user. Assign the role to the required user.

- User with Reader privileges: The user with Reader role can only view the data displayed in VMDR OT module. Click New Role. Give the role a name and description, and then select the modules and permissions to privileges be granted to a user when the role is assigned.

Assigning Role to the User

You can create new roles and make changes to the permissions for existing roles. You can also quickly assign roles to users from here.

Note: To view the Role Management tab, you need to have full permissions and scope or a role with the Access Role Management Section permission enabled in the Administration utility.

1. In the Administration utility, go to Users > Role Management.

2. Select the role you want to assign and choose Add To Users from the Quick Actions menu.

3. Select the user from the list to assign the role and click Save.
You can remove roles from users in a similar way - need to select the action Remove From Users.

**Editing a role**

1. Select any role in the list and choose **Edit** from the **Quick Actions** menu.

You can change the role name and description and edit the assigned permissions. Any changes you make to a role will apply to all users assigned that role.

**Warning** - Be careful while removing the UI access permission from a role. A user will not be able to log into the UI if they don't have at least one role with the UI access permission assigned.

**Editing permissions**

While editing the permissions for a role, you can define application access, modules to be accessible, and permissions within the module for the users with the current role. Currently, you can configure two types of users. Depending on the permissions you assign to the role, you can categorize the users with all permissions or read only permissions.

Ensure that you have assigned VMDR OT module to be accessible for the users. Click the title of a group to expand its permissions. Then select the permissions you want to assign to the role.

To view the assets, vulnerabilities, and network list view in the scope, a user must have access to the assets. Ensure that the user has access to those assets.

**Adding tags in the scope of users**
You can provide access to the assets by adding tags to the user scope. Each asset can have some tags associated with it. You can create your own tags and assign them to the asset. Scopes can be assigned to other users by the Manager users. Manager users can log in through the Administration utility to assign the tags to user scope. To know more about tags, refer to Tagging Assets.

1. In the Administration utility, go to the User Management tab, select the user to which you want to assign the permissions and click Edit.

2. In the Edit window, go to the Roles and Scopes tab in the left pane and Select the Tags (Assets for which the user need access) from the Global Scope.

Or

You can also assign the tags to scope from the Quick Actions menu of the user on User Management tab.
3. Select the tag from the list.

4. Click **Save**, and the user permissions are assigned to the required user.

**Note:** You need permissions related to tagging activities. There are various permissions like Create User Tag | Edit User Tag | Delete User Tag | Modify Dynamic Tag Rules | Add/Remove Tags.

For more details on Tagging permissions, refer to the section Steps to assign or remove the Tagging Permissions of the Online help of Administration Utility.

- **All privileges:** User will have all the privileges in VMDR OT except creating and managing other users.

- **Reader privileges:** User with Reader role can only view the data displayed in VMDR OT module.

For more details on Tagging permission, refer to the section Steps to assign or remove the Tagging Permissions of Online help of Administration Utility.

**Adding/Removing Permissions for Multiple Roles**
You can add or remove permissions from multiple roles in a single action. Select the roles you want to change and then select Add Permissions or Remove Permissions from the Quick Actions menu.
Deleting a Role

Select the role and choose **Delete** from the **Quick Actions** menu.

The role you delete will no longer be assigned to users. It is removed automatically from all users' accounts (that had it previously assigned) and those users will no longer have the permissions granted by the role.

**Note:** If you edit permissions for a predefined role or delete a predefined role, the user associated with the roles you edit can experience difference in access behavior.

Deploying Qualys Network Passive Sensors

Upon deploying the Qualys Network Passive Sensor in the network, it starts sniffing the metadata of the network devices after the flow of traffic related to the device identity is generated on the network. Based on the collected device properties, the devices are added as assets to the Qualys VMDR OT inventory.

Deploy Qualys Network Passive Sensor in the network and enable it to listen to the mirrored port. For more details, refer to Qualys Network Passive Sensor Getting Start Guide.
Viewing Assets Details

Assets tab displays a detailed consolidated view of the industrial assets. These are the devices in the industrial network that are discovered and profiled by the Qualys Network Passive Sensor.

This real-time asset inventory provides the details related to asset metadata. It also helps to gauge the security posture of the industrial OT environment and mitigate the risk of potential cyber security threats by managing vulnerabilities well in advance.

In the upper left corner, there is total count of the industrial assets in the network.

The assets table contains the list of discovered assets with the following details:

- Asset name
- Hardware type of the asset
- Vendor/Model number
- When the asset activity was last detected on the network
- Risk score of the asset
- Vulnerabilities detected on the asset
- Asset tags

In the search bar, QQL queries can be built to narrow down the scope of the asset search by using the supported search tokens. For more information, see Search Tokens for VMDR OT in VMDR OT Online help.

Use the left pane filters to search for assets grouped into categories like equipment category, equipment type, vendor and so on. The assets that belong to the selected category are displayed in the assets table.
Below the search bar, assets are grouped under four categories: devices with a high risk score, devices on which vulnerabilities are detected, devices discovered by Qualys Network Passive Sensor (NPS) within the past 24 hours, and devices on which no activity has been detected for the past seven days. Click each of these cards and get the assets listed by the selected category.

The date and time range selector next to the search bar can be used to view assets discovered within a specific time period.
To view more details of an asset, click the asset name. The Asset Details page contains asset information divided into various sections.

<table>
<thead>
<tr>
<th>Section</th>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVENTORY</td>
<td>Summary</td>
<td>Asset metadata such as asset name, ID, IP address, MAC address, equipment type, and industry protocol based on which the Qualys Network Passive sensor discovers the asset, description, assigned location of asset, first passive scan details and last passive scan details etc.</td>
</tr>
<tr>
<td></td>
<td>System Information</td>
<td>Manufacturer details, model number, serial number, firmware version, hardware version, product code, add-on details, protocol-specific information etc.</td>
</tr>
<tr>
<td>NETWORK</td>
<td>Network Information</td>
<td>Interface details such as IPv4 address, IPv6 address, domain details, DNS server details, and protocols talking to devices on each interface.</td>
</tr>
<tr>
<td></td>
<td>Network Map</td>
<td>View the network map for the selected asset.</td>
</tr>
<tr>
<td></td>
<td>Open Ports</td>
<td>List of open ports and services running on those ports.</td>
</tr>
<tr>
<td></td>
<td>Traffic Summary</td>
<td>Traffic flow details for an asset. These may include a date-wise traffic volume summary for the client to server (CTS) and server to client (STC), traffic categorized by family and volume.</td>
</tr>
<tr>
<td>SECURITY</td>
<td>Vulnerabilities</td>
<td>Summarized view for potential and confirmed vulnerabilities on the asset.</td>
</tr>
<tr>
<td>SENSORS</td>
<td>Passive Sensor</td>
<td>Details of Qualys Network Passive Sensor that discovered the asset.</td>
</tr>
<tr>
<td></td>
<td>Industrial OCA</td>
<td>Details of Industrial OCA information regarding the asset.</td>
</tr>
</tbody>
</table>
Generating Traffic Using Device Discovery Method

To speed up the discovery of the assets, device discovery method can also be used. Start generating traffic required for device identity and retrieve device information. The device information is retrieved from the programming software for configuring and managing the network devices.

Refer to the Device Discovery Documents in VMDR OT Online help, which contain the procedure to generate the traffic flow from the network without any additional configuration in the control system. The procedure varies depending on the programming software. Pick up the vendor software, and go ahead with the device discovery.

Once the procedure of device discovery is completed, it triggers the necessary data flow related to device identity on the network. Qualys Network Passive Sensor sniffs and dissects this data to list the discovered devices in Qualys VMDR OT.

For more details on supported OT protocols, refer to Appendix A - Supported OT Protocols. For more details on supported IT protocols, refer to Appendix B - Supported IT Protocols.

Viewing Vulnerabilities

The Vulnerabilities tab gives a complete view of the vulnerability posture of the assets in the industrial network.

In the upper left corner, there is total count of vulnerability detections in the network.
The vulnerabilities table contains the list of detected vulnerabilities and their following details:

- **QID**, the unique Qualys ID assigned to the vulnerability
- **Vulnerability title**
- **Severity level** (1-5) determined by the security risk associated with its exploitation
- **When the vulnerability was first detected on the asset**
- **Asset on which the vulnerability is detected**
- **Rack/Slot details**
- **When the vulnerability was last detected on the asset**

In the search bar, QQL queries can be built to narrow down the scope of the vulnerability search by using the supported search tokens. For more information, see *Search Tokens for VMDR OT* in VMDR OT Online help. Use the left pane filters to search for assets grouped into various categories. After clicking a category in this list, the selection gets translated into a QQL query in the search bar. The vulnerabilities that fit into the selected category are displayed in the vulnerabilities table.
The date and time range selector next to the search bar can be used to choose to view vulnerabilities detected within a specific time period.

To view details of a vulnerability, click the QID.

The detection summary and general information about the detected vulnerability is displayed on the Vulnerability details page. On the Vulnerability Details page, information about known exploits for the vulnerability available from third-party vendors and/or publicly available sources, available patches to fix the vulnerability, and any published malware associated with the vulnerability are displayed.
Viewing KnowledgeBase

We have the most up-to-date KnowledgeBase of vulnerabilities in the security industry and it's continuously getting updated.

To view the KnowledgeBase tab, go to VULNERABILITIES tab and click KnowledgeBase.

The KnowledgeBase tab contains details of vulnerabilities that can be detected in an industrial automation environment. You can use a variety of search filters to find vulnerabilities. Some of these filters include QID, vulnerability title, discovery method, severity level, category, patch availability, CVSS or CVSS v3 scores, published date, etc.

Click Filters, and then in the Apply Filters, select the filters of your choice and click Search.

You get the results based on your search criteria.
Viewing Network Traffic

The Network tab gives a complete view of network traffic in the industrial network. Multiple Qualys Network Passive Sensors (NPS) can be deployed across the network. Each Qualys Network Passive Sensor (NPS) has access to traffic with source and destination details in the flows. The Network tab shows all sources and destinations of the given port and protocol. The network list view displays the different protocols being used in the network and how the assets are communicating.

In the search bar, QQL queries can be built to narrow down the scope of the network traffic search by using the supported search tokens. For more information, see Search Tokens for VMDR OT in VMDR OT Online help.

Use the left pane filters to search for the network traffic grouped into various categories. After clicking a category in this list, selection gets translated into a QQL query in the search bar. The network traffic that fits the selected category is displayed in the network traffic table.

The network table contains the list of network traffic with the following details:

- Source asset
- Source asset type
- When the asset was first and last seen communicating on the network
- Destination Asset
- Destination asset type
- Protocol/Transport protocol used for communication
- Port on which they are communicating
- Total traffic volume for the network
- Ingress traffic volume for the network
- Egress traffic for the network
Tagging Assets

Asset tagging helps to organize assets in your organization. You can apply tags manually or configure rules for automatic classification of your assets in logical, hierarchical, business-contextual groups. The most powerful use of tags is accomplished by creating a dynamic tag. Dynamic tag automatically assigns tags to the assets based on search criteria in the dynamic tagging rule.

On the Tags tab, you can view the list of various tags applied to the assets and option to create a new tag.

You can search the tag from the Search for tags.

![Tagging Assets UI](image)

Configure Tags

Configure tags to apply them to assets. Tags help to organize your assets and to manage user access to them.

1) Go to **TAGS** tab and click **Create Tag**.

2) Enter the basic details and tag properties for your tag.

- **Basic Details**
  - Give your tag a name (up to 1024 characters).
  - Select Mark as Favourite if you want to create a tag as favourite. Favourite is displayed with yellow star in the list.
  - Add a description for your tag (optional).
- **Tag Properties**

Color coding is a great way to organize tags. You can assign different colors to different tag. When creating a child tag, you can select a parent tag from existing tags in your account.

- To select existing tag click **Select** and then choose a tag from **Select Tags** pop up.
- You can also create a new tag for a parent.

- Click **Create** and again similar form to create a tag displays. You can not create a new parent from this new tag.

3) Set up a dynamic tag type (optional). If there is no dynamic rule, then your tag is saved as a static tag.

- **Tag Type**

There are two types of tags - Static and Dynamic.

- By default, static tag is created. Dynamic tag allows you to define Tag Rules.
- You can select Evaluate Rule on Creation check box to evaluate dynamic rule once it is created or updated.

- **Tag Rules**

These are the rules which helps to identify the assets to apply tags.

- No Dynamic Rule - Your tag will be a static tag.
- Asset Name Contains - Applies the tag when any part of the user-definable asset name contains the substring or substrings you enter. Add multiple substrings separated by the "|" (vertical bar) with no spaces before or after.
- Asset Inventory - Applies the tag to assets from VMDR OT.
- IP Address In Range(s) - Applies the tag to assets with an IP in the range you enter (e.g. 172.31.254.0-172.31.254.25 or 172.31.254.0/25).
• IP Address In Range(s) + Network(s) - Applies the tag to assets with an IP in the range you enter and network.

• Open Ports - Applies the tag to assets whose port listing matches the ports you enter (e.g. 80,123).

• Asset Search - Applies the tag to assets based on search criteria defined in the Asset Search field. You can use XML code to define your query.

- Test Rule Applicability on Selected Assets (Optional)

Select assets in your account to test the rule.

A green color Pass tells you the asset matches the rule.

A red color Fail tells you the asset does not match the rule.

4) Click **Create** to save the tag.

When you save your dynamic tag, it is applied to all discovered assets that match your defined rule. You can filter the assets list to show only those that match your new tag rule.

**Note:** When you save your static tag, you can apply it to your asset from the Assets tab. Refer to the Online help for viewing an example of a dynamic tag.

**Managing Asset Tags**

You can perform many actions from the **Quick Actions** menu from the tag.

<table>
<thead>
<tr>
<th>Function</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the Tag details</td>
<td>Go to the <strong>TAGS</strong> tab and click View under Quick Actions menu of the tag.</td>
</tr>
<tr>
<td>Edit the Tag details</td>
<td>Go to the <strong>TAGS</strong> tab and click Edit under Quick Actions menu of the tag.</td>
</tr>
<tr>
<td>Find Assets with the specific tag</td>
<td>Go to the <strong>TAGS</strong> tab and click Find Assets under Quick Actions menu of the specific tag. The Find Assets option takes you to the Asset tab to view the list of assets with the specific tag.</td>
</tr>
<tr>
<td>Move tags to root</td>
<td>Go to the <strong>TAGS</strong> tab and click Move to root under Quick Actions menu for a child tag. Once you perform 'Move to root' action, child tag will be moved to parent tag and carries all the children under it while moving to root.</td>
</tr>
<tr>
<td>Mark tag as favorites</td>
<td>If there are tags you assign frequently, adding them to favorites can save time. You can mark a tag as a favorite when adding a new tag or when editing an existing one. If a tag is already favourite, you can see an option to remove from favourite.</td>
</tr>
<tr>
<td>Remove tag from favorites</td>
<td>Go to the <strong>TAGS</strong> tab and click Find Assets under Quick Actions menu of the specific tag.</td>
</tr>
</tbody>
</table>
### Importing Assets

Asset inventory can also be created using VMDR OT Out of band configuration assessment. Asset can be imported using the project file. Project files are collected from programming and maintenance software, uploaded to the VMDR OT application, and accessible from the account. The VMDR OT application parses the uploaded file with valuable data and creates assets from the data gathered.

On the Import Assets tab, there is option to upload project files. Project files support extensions like cxp, zip, Xml, RSS and many more.

You can view the procedure to generate a project file. The procedure varies depending on the programming software you use. We are supporting different vendors and software tools such as Omron CX Programmer (.cxp), Rockwell RSLogix 500 (.RSS), Rockwell Studio 5000 (.L5X), Rockwell System Ferret (.Xml), Siemens DIGSI 4 (.zip), Siemens DIGSI 5 (.zip), Siemens DIGSI 5 (.dz5) and many more.

For more details on supported OCA, refer to Appendix C - Supported OCA

In the upper left corner, there is total count of project files uploaded. In the search bar, QQL queries can be built to narrow down the scope of the file search by using the supported search tokens. For more information, see Search Tokens for VMDR OT in VMDR OT Online help.

<table>
<thead>
<tr>
<th>Add Child Tag</th>
<th>Go to the TAGS tab and click Add child tag from Quick Actions menu for a tag. You can create maximum 8 tag levels and 100 child tags for a parent tag.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a Tag</td>
<td>Go to the TAGS tab and click Delete from Quick Actions menu for a tag. You can only delete custom created tag.</td>
</tr>
<tr>
<td>Save the Tags</td>
<td>When you save your dynamic tag, we apply it to all discovered assets that match the rule you defined. You can filter the assets list to show only those that match your new tag rule.</td>
</tr>
<tr>
<td>Save the Static Tag</td>
<td>When you save your static tag, you can apply it to your asset from the Assets tab</td>
</tr>
<tr>
<td>Use of tag filters</td>
<td>Go to the TAGS tab and you can see Filters. You can filter the list of tags using favourite and in scope checkbox. You can also filter tags based on the color applied to tags.</td>
</tr>
</tbody>
</table>
Use the left pane filters to search for files grouped into various categories. After clicking a category in this list, the selection gets translated into a QQL query in the search bar. The files that fit into the selected category are displayed in the table.

The import asset table contains the following details:

- File name
- Hash of the file
- Extension type
- Status like Imported, Importing, Failed, and Deleted
- Plant location from where the files are gathered
- When the file was last updated
- Vendor of the file
- Total number of assets in the file
Get Started with VMDR OT
Importing Assets

To upload the file, click **Upload Project Files**.

Provide the **Plant Location** name, select the file from the saved location using **browse**.

Project files support extensions like cxp, RSS, zip, Xml, d5Z, zef, xef, cfg and many more.

**Note:** The file extensions are case sensitive, ensure the extensions you are uploading are supported.

Click **Upload**.

The file is uploaded and shows the status as Imported. Depending on the uploading of the file, there can be different statuses like

- **Importing** - file is still uploading
- **Imported** - file is imported successfully
- **Deleted** - file is deleted
- **Failed** - file could not be imported
For more detail on how to generate the project file from programming and maintenance software, refer to Generating Project File in VMDR OT Online help.
Managing VMDR OT Dashboards

To visualize the assets and vulnerability postures, simply add widgets to dashboard. The dashboard tab is the home page for VMDR OT.

To see the VMDR OT dashboard, select VMDR OT from the application selector. On the dashboard, there are count cards like high risk devices, newly discovered devices, new vulnerabilities, active vulnerabilities and so on by default.

There are different widgets like asset distribution by risk score, asset distribution by protocol, asset distribution by vendors and various widgets based on vulnerabilities by type, vulnerabilities by severity and so on. Add widgets can be used to add VMDR OT related widgets.
The widgets are interactive; clicking the specific part of the widget redirects to the related tab.

For example, here in the above VULNERABILITIES BY TYPE widget, clicking Confirmed takes to the Vulnerability tab for the details of confirmed vulnerabilities.

All the details of the confirmed vulnerability are displayed.

Dynamic dashboards help you customize the way you view your information. Qualys provide a default dashboard to get started.

**Viewing Unified Dashboard**

Dashboards help to visualize the assets, see the threat exposure, leverage saved searches, and quickly fix the priority of vulnerabilities.

Qualys VMDR OT integrates with Unified Dashboard (UD) to bring information from all Qualys applications into a single place for visualization. UD provides a powerful, new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.
Qualys VMDR OT offers several dashboards out-of-the-box. Each dashboard displays a short description of the information it offers. It is easy to configure widgets to pull information from other modules/applications and add them to the dashboard. As per requirement many dashboards can be added to customize the view.

See the Unified Dashboard help for more information.
# Appendix A - Supported OT Protocols

This appendix lists the OT protocols supported by Industrial Control System.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siemens S7 Comm</td>
<td>Omron Fins</td>
</tr>
<tr>
<td>Siemens S7 comm plus</td>
<td>Mitsubishi Melsoft</td>
</tr>
<tr>
<td>Profinet</td>
<td>Mitsubishi CC Link</td>
</tr>
<tr>
<td>Ethernet IP</td>
<td>Mitsubishi SLMP</td>
</tr>
<tr>
<td>CIP (Common Industrial Protocol)</td>
<td>EtherCAT</td>
</tr>
<tr>
<td>PCCC</td>
<td>Emerson Delta-V</td>
</tr>
<tr>
<td>Modbus TCP</td>
<td>Redlion Crimson</td>
</tr>
<tr>
<td>BACnet</td>
<td>Toyopuc</td>
</tr>
<tr>
<td>Niagara Fox</td>
<td>Microsoft Discovery Protocol</td>
</tr>
<tr>
<td>Johnson Controls Metasys</td>
<td>Schneider UMAS</td>
</tr>
<tr>
<td>DNP3</td>
<td>Honeywell CeeNTComm (C200, C300)</td>
</tr>
<tr>
<td>IEC 104</td>
<td>Proconos</td>
</tr>
<tr>
<td>IEC 61850 – MMS</td>
<td>GE-SRTP</td>
</tr>
<tr>
<td>Beckhoff AMS / ADS</td>
<td>MQTT</td>
</tr>
</tbody>
</table>
Appendix B - Supported IT Protocols

This appendix lists the IT protocols supported by Industrial Control System.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>LLDP</td>
</tr>
<tr>
<td>UDP</td>
<td>UPnP</td>
</tr>
<tr>
<td>DHCP</td>
<td>SMTP</td>
</tr>
<tr>
<td>HTTP</td>
<td>SNMP</td>
</tr>
<tr>
<td>DNS</td>
<td>Netbios</td>
</tr>
<tr>
<td>SSH</td>
<td>SIP</td>
</tr>
<tr>
<td>SSL</td>
<td>ARP</td>
</tr>
<tr>
<td>Kerberos</td>
<td>IPv6 Neighbor Discovery</td>
</tr>
<tr>
<td>CDP</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix C - Supported OCA

This appendix lists supported OCA (Out of band Configuration Assessment) by Industrial Control System.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Engineering Tool</th>
<th>File Extension Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beckhoff zip</td>
<td>TwinCAT3</td>
<td>.zip, .tnzip</td>
</tr>
<tr>
<td>Emerson</td>
<td>DeltaV Explorer</td>
<td>.fhn</td>
</tr>
<tr>
<td>Omron</td>
<td>CX-Programmer</td>
<td>.csp</td>
</tr>
<tr>
<td>Rockwell</td>
<td>RSLogix 500</td>
<td>.RSS</td>
</tr>
<tr>
<td>Rockwell</td>
<td>RSLogix 5000/ Studio 5000</td>
<td>.l5x</td>
</tr>
<tr>
<td>Rockwell</td>
<td>RS System Ferret</td>
<td>.Xml</td>
</tr>
<tr>
<td>Siemens</td>
<td>Digi4</td>
<td>.zip</td>
</tr>
<tr>
<td>Siemens</td>
<td>Digi5</td>
<td>.zip, .dz5</td>
</tr>
<tr>
<td>Siemens</td>
<td>Simatic Manager (Step 7)</td>
<td>.cfg</td>
</tr>
<tr>
<td>Siemens</td>
<td>TIA Portal</td>
<td>.zip, .zap(.zap15, .zap15_1, .zap17)</td>
</tr>
<tr>
<td>Siemens</td>
<td>LOGO! Soft Comfort</td>
<td>.lnp, .mnp</td>
</tr>
<tr>
<td>Siemens</td>
<td>PRONETA</td>
<td>.xml</td>
</tr>
<tr>
<td>Schneider</td>
<td>Unity L/XL</td>
<td>.zef, .xef</td>
</tr>
<tr>
<td>Schneider</td>
<td>TwidoSuite</td>
<td>.zip, .xtwd</td>
</tr>
<tr>
<td>Schneider</td>
<td>Schneider Concept</td>
<td>.ccf, .CCF</td>
</tr>
<tr>
<td>Mitsubishi</td>
<td>GX Works3</td>
<td>.gx3</td>
</tr>
<tr>
<td>Mitsubishi</td>
<td>GX Works2</td>
<td>.gxw</td>
</tr>
<tr>
<td>Red Lion Controls</td>
<td>Crimson</td>
<td>.cd3, .cd31</td>
</tr>
</tbody>
</table>