Qualys®

VMDR OT

Getting Started Guide

January 24, 2023

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

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 malfunction 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.

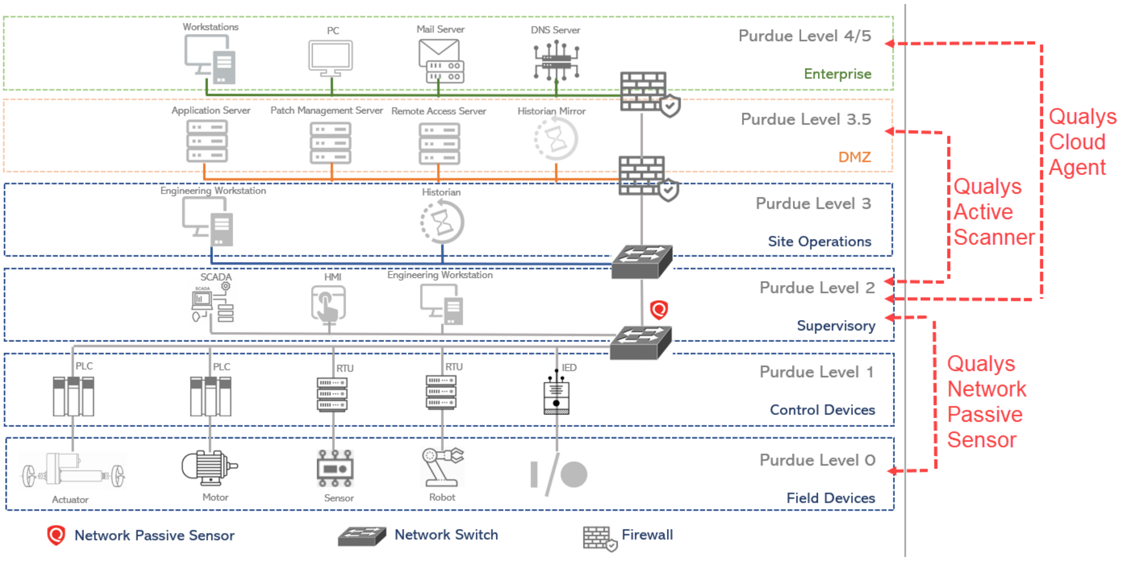
Qualys Network Passive Sensor can latch on the mirrored port of a network switch which can see traffic from assets present in Purdue levels 0, 1 and 2 and passively listen to traffic, dissect the protocol, and build the asset inventory.

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.

Purdue Level	Assets	Feature	Supported by	Available on Qualys Applications
Purdue Levels 0/1/2	Hardware like PLC, RTU, IO, Robots, VFDs etc	Asset Inventory	Qualys Network Passive Sensor	VMDR OT
		Vulnerability Management	VMDR OT Out of band configuration assessment	

Purdue Levels 2 and above	OT/ICS OS-based endpoints hosting ICS Vendor software - (Engineering workstations, Operator Stations, HMI Servers, DCS Servers, etc.)	Asset Inventory	VMDR application (VMDR OT safe active scan support in Qualys Scanner and Cloud Agent)	VMDR CSAM For more details, see OT Device Scan details
		Vulnerability Management	VMDR (OT/ICS OS-based endpoints hosting ICS Vendor software)	VMDR
		Policy Compliance	Policy Compliance application IEC 62443 NERC CIP Policy	Policy Compliance

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.

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

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.

Manager Users	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.
Users	Depending on the permissions assigned to the role, users can be categorized with all privileges or read-only privileges.

New Users: Scope and Permissions

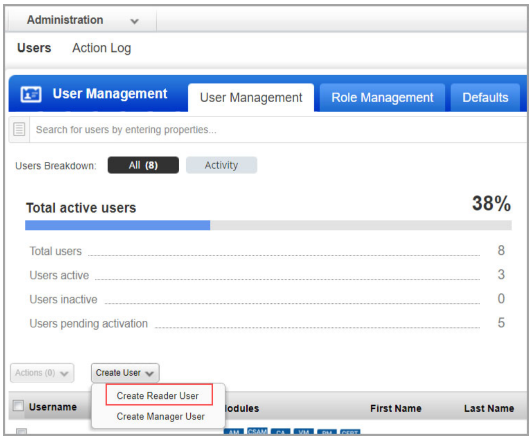
Only Manager users have permissions to create new users and grant them permissions.

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**.

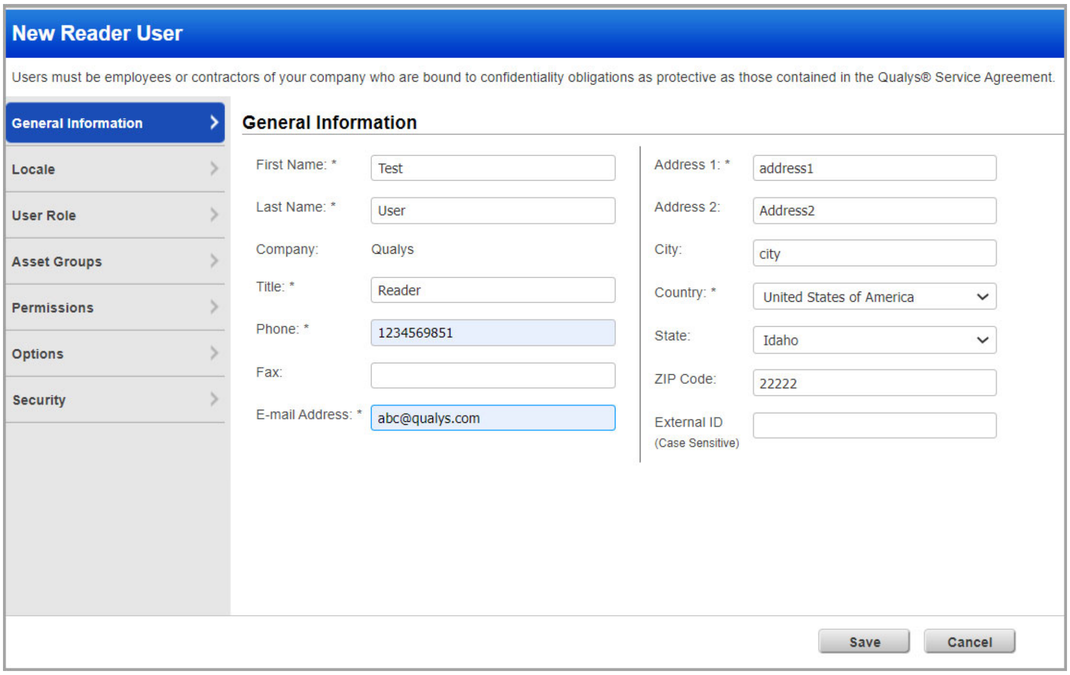


Total active users 38%

Total users 8
Users active 3
Users inactive 0
Users pending activation 5

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.



New Reader User

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

First Name: * Test

Last Name: * User

Company: Qualys

Title: * Reader

Phone: * 1234569851

Fax:

E-mail Address: * abc@qualys.com

Address 1: * address1

Address 2: Address2

City: city

Country: * United States of America

State: Idaho

ZIP Code: 22222

External ID (Case Sensitive)

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.

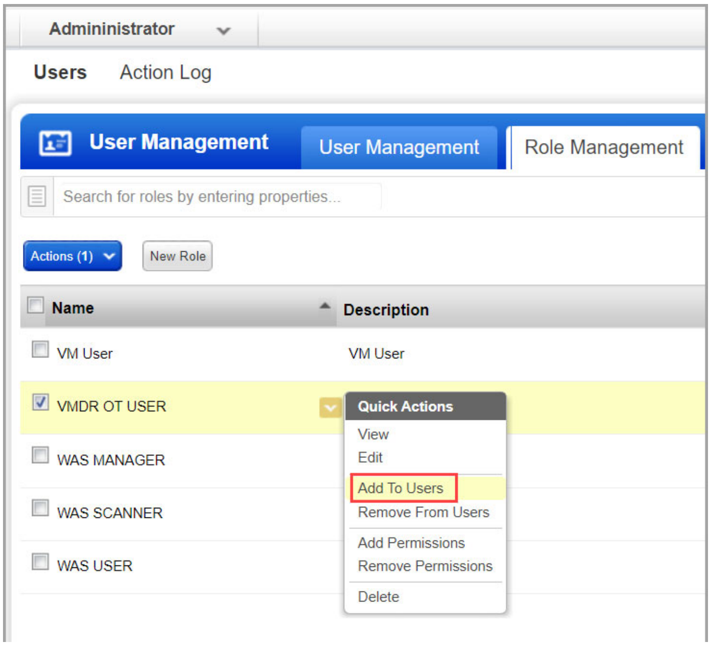
Note: To view the Role Management tab, you need to have full permissions and scope or a role with the Access Role Management Section permission enabled in the Administration utility.

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.



□ Name	Description
□ VM User	VM User
☑ VMDR OT USER	
□ WAS MANAGER	
□ WAS SCANNER	
□ WAS USER	

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.

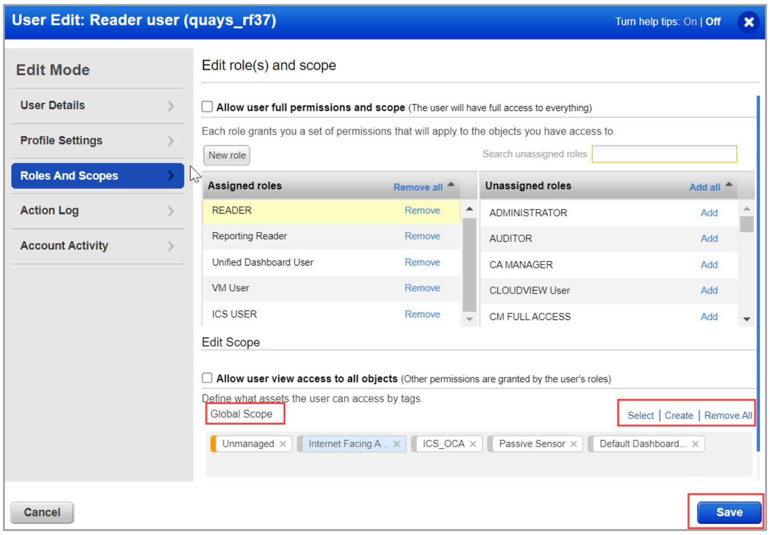
To view the assets, vulnerabilities, and network list view in the scope, a user must have access to the assets. Ensure that the user has access to those assets.

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**.



☐ **Allow user full permissions and scope** (The user will have full access to everything)

Each role grants you a set of permissions that will apply to the objects you have access to.

New role | Search unassigned roles

Assigned roles	Remove all
READER	Remove
Reporting Reader	Remove
Unified Dashboard User	Remove
VM User	Remove
ICS USER	Remove

Unassigned roles	Add all
ADMINISTRATOR	Add
AUDITOR	Add
CA MANAGER	Add
CLOUDVIEW User	Add
CM FULL ACCESS	Add

Edit Scope

☐ **Allow user view access to all objects** (Other permissions are granted by the user's roles)

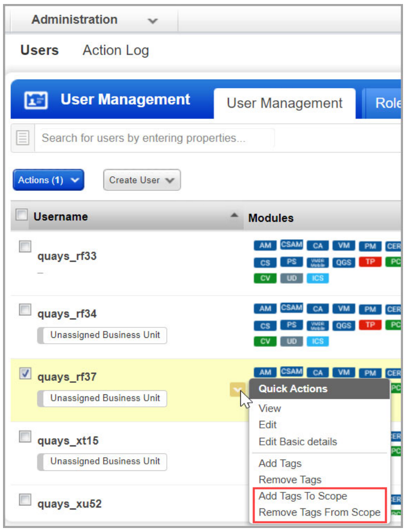
Define what assets the user can access by tags.

Global Scope | Select | Create | Remove All

Unmanaged × | Internet Facing A... × | ICS_OCA × | Passive Sensor × | Default Dashboard... ×

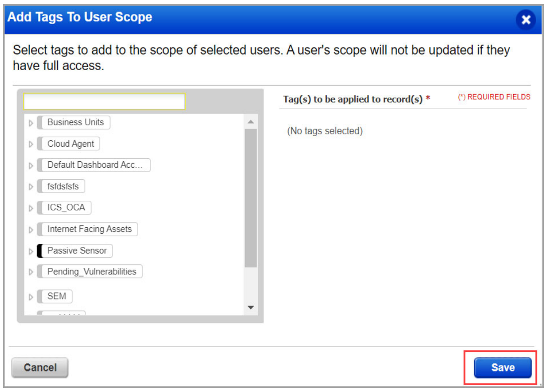
Or

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.



Add Tags To User Scope

Select tags to add to the scope of selected users. A user's scope will not be updated if they have full access.

Tag(s) to be applied to record(s) *

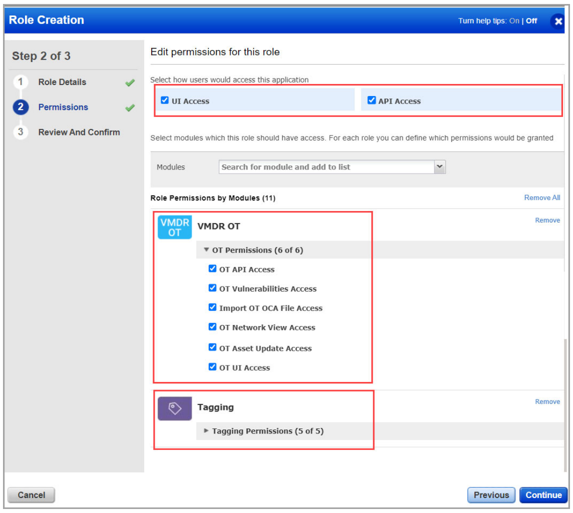
(*) REQUIRED FIELDS

(No tags selected)

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 permission, 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.



Role Creation

Step 2 of 3

Edit permissions for this role

Select how users would access this application

☑ UI Access ☑ API Access

Select modules which this role should have access. For each role you can define which permissions would be granted

Modules: Search for module and add to list

Role Permissions by Modules (11)

VMDR OT

▾ OT Permissions (6 of 6)

☑ OT API Access
☑ OT Vulnerabilities Access
☑ Import OT OCA File Access
☑ OT Network View Access
☑ OT Asset Update Access
☑ OT UI Access

Tagging

▸ Tagging Permissions (5 of 5)

- 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.

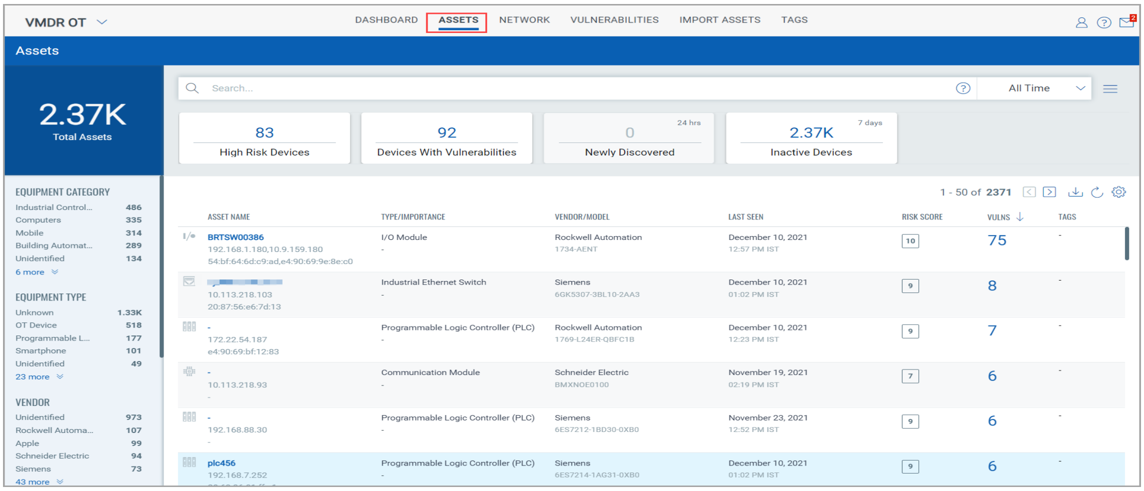
Deploy Qualys Network Passive Sensor in the network and enable it to listen to the mirrored port. For more details, refer to Qualys Network Passive Sensor Getting Start Guide.

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.



2.37K Total Assets

83	92	0 (24 hrs)	2.37K (7 days)
High Risk Devices	Devices With Vulnerabilities	Newly Discovered	Inactive Devices

EQUIPMENT CATEGORY

Industrial Control...	486
Computers	335
Mobile	314
Building Automat...	289
Unidentified	134

6 more

EQUIPMENT TYPE

Unknown	1.33K
OT Device	518
Programmable L...	177
Smartphone	101
Unidentified	49

23 more

VENDOR

Unidentified	973
Rockwell Automa...	107
Apple	99
Schneider Electric	94
Siemens	73

43 more

1 - 50 of 2371

ASSET NAME	TYPE/IMPORTANCE	VENDOR/MODEL	LAST SEEN	RISK SCORE	VULNS	TAGS
BRTSW00386 192.168.1.180,10.9.159.180 54:bf:64:6d:c9:ad,e4:90:69:9e:8e:c0	I/O Module -	Rockwell Automation 1734-AENT	December 10, 2021 12:57 PM IST	10	75	-
[redacted] 10.113.218.103 20:87:56:e6:7d:13	Industrial Ethernet Switch -	Siemens 6GK5307-3BL10-2AA3	December 10, 2021 01:02 PM IST	9	8	-
- 172.22.54.187 e4:90:69:bf:12:83	Programmable Logic Controller (PLC) -	Rockwell Automation 1769-L24ER-QBFC1B	December 10, 2021 12:23 PM IST	9	7	-
- 10.113.218.93 -	Communication Module -	Schneider Electric BMXNOE0100	November 19, 2021 02:19 PM IST	7	6	-
- 192.168.88.30 -	Programmable Logic Controller (PLC) -	Siemens 6ES7212-1BD30-0XB0	November 23, 2021 12:52 PM IST	9	6	-
plc456 192.168.7.252	Programmable Logic Controller (PLC) -	Siemens 6ES7214-1AG31-0XB0	December 10, 2021 01:02 PM IST	9	6	-

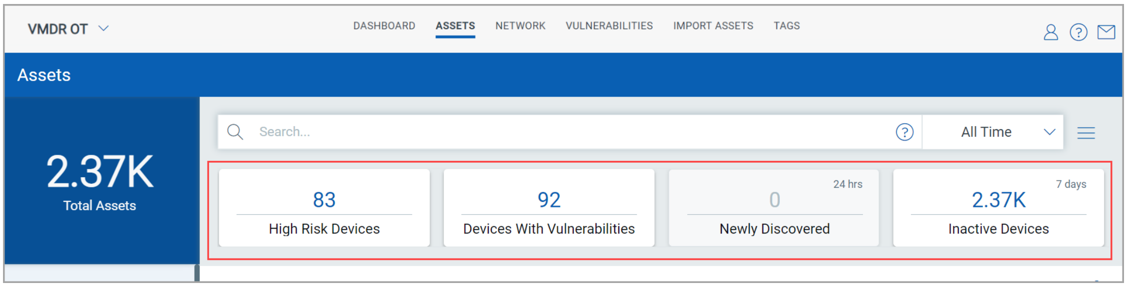
The assets table contains the list of discovered assets with the following details:

- 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

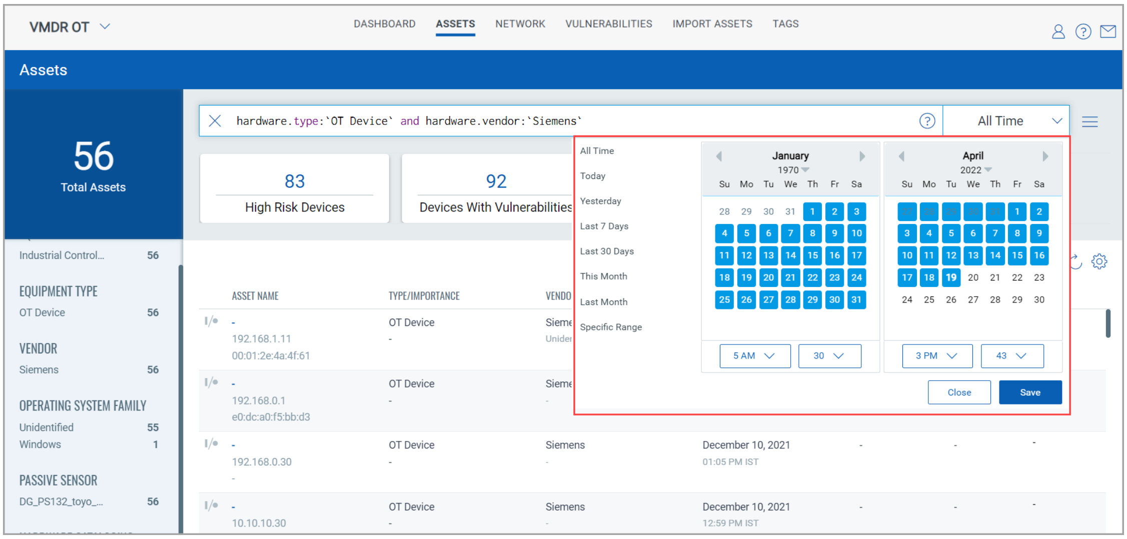
In the search bar, QQL queries can be built to narrow down the scope of the asset search by using the supported search tokens. For more information, see Search Tokens for VMDR OT in VMDR OT Online help.

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.



```
hardware.type:`OT Device` and hardware.vendor:`Siemens`
```

Industrial Control... 56

EQUIPMENT TYPE
OT Device 56

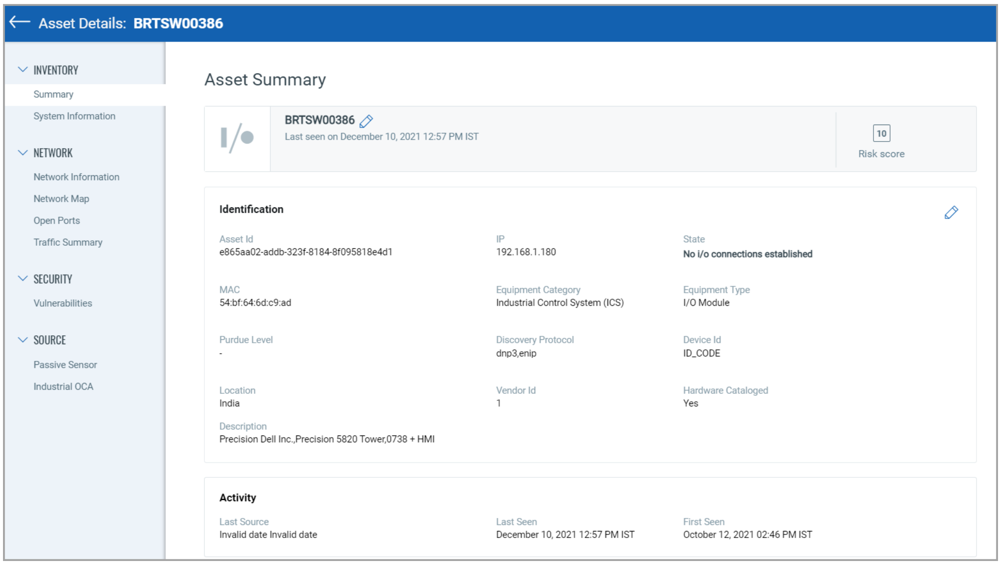
VENDOR
Siemens 56

OPERATING SYSTEM FAMILY
Unidentified 55
Windows 1

PASSIVE SENSOR
DG_PS132_toyo_... 56

ASSET NAME	TYPE/IMPORTANCE	VENDO				
- 192.168.1.11 00:01:2e:4a:4f:61	OT Device -	Sieme Unider				
- 192.168.0.1 e0:dc:a0:f5:bb:d3	OT Device -	Sieme -				
- 192.168.0.30 -	OT Device -	Siemens -	December 10, 2021 01:05 PM IST	-	-	-
- 10.10.10.30	OT Device -	Siemens -	December 10, 2021 12:59 PM IST	-	-	-

To view more details of an asset, click the asset name. The Asset Details page contains asset information divided into various sections.



Asset Summary

BRTSW00386
Last seen on December 10, 2021 12:57 PM IST

10

Identification

Asset Id: e865aa02-addb-323f-8184-8f095818e4d1
IP: 192.168.1.180
State: No i/o connections established
MAC: 54:bf:64:6d:c9:ad
Equipment Category: Industrial Control System (ICS)
Equipment Type: I/O Module
Purdue Level: -
Discovery Protocol: dnp3,enip
Device Id: ID_CODE
Location: India
Vendor Id: 1
Hardware Cataloged: Yes
Description: Precision Dell Inc.,Precision 5820 Tower,0738 + HMI

Activity

Last Source: Invalid date Invalid date
Last Seen: December 10, 2021 12:57 PM IST
First Seen: October 12, 2021 02:46 PM IST

The following table contains details as seen on each tab in each section:

INVENTORY	Summary	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.
	System Information	Manufacturer details, model number, serial number, firmware version, hardware version, product code, add-on details, protocol-specific information etc.
NETWORK	Network Information	Interface details such as IPv4 address, IPv6 address, domain details, DNS server details, and protocols talking to devices on each interface.
	Network Map	View the network map for the selected asset.
	Open Ports	List of open ports and services running on those ports.
	Traffic Summary	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.
SECURITY	Vulnerabilities	Summarized view for potential and confirmed vulnerabilities on the asset.
SENSORS	Passive Sensor	Details of Qualys Network Passive Sensor that discovered the asset.
	Industrial OCA	Details of Industrial OCA information regarding the asset.

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.

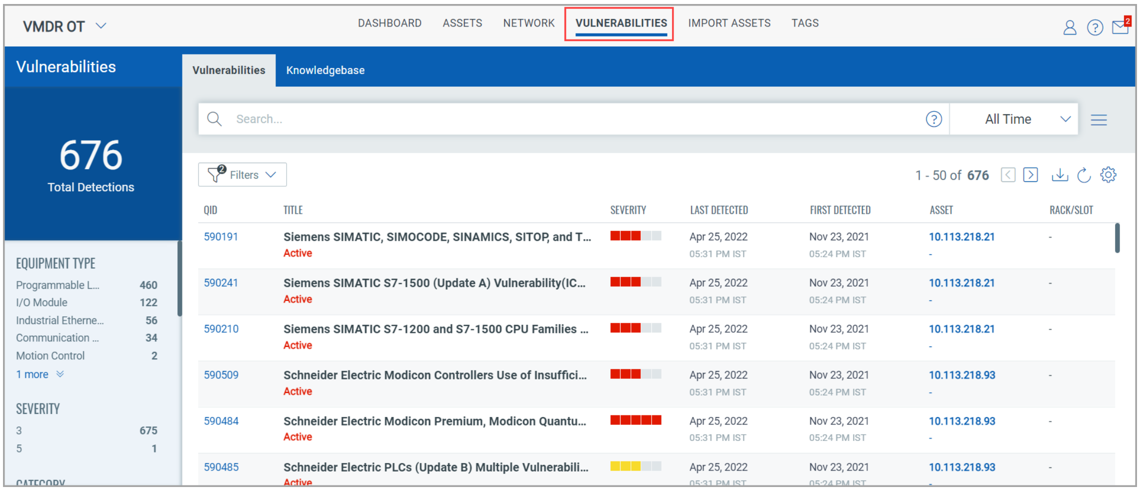
For more details on supported OT protocols, refer to Appendix A - Supported OT Protocols

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.



676
Total Detections

EQUIPMENT TYPE

Programmable L...	460
I/O Module	122
Industrial Etherne...	56
Communication ...	34
Motion Control	2

1 more

SEVERITY

3	675
5	1

CATEGORY

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET	RACK/SLOT
590191	Siemens SIMATIC, SIMOCODE, SINAMICS, SITOP, and T... Active	■■■□□	Apr 25, 2022 05:31 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.21 -	-
590241	Siemens SIMATIC S7-1500 (Update A) Vulnerability(IC... Active	■■■□□	Apr 25, 2022 05:31 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.21 -	-
590210	Siemens SIMATIC S7-1200 and S7-1500 CPU Families ... Active	■■■□□	Apr 25, 2022 05:31 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.21 -	-
590509	Schneider Electric Modicon Controllers Use of Insuffici... Active	■■■□□	Apr 25, 2022 05:31 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.93 -	-
590484	Schneider Electric Modicon Premium, Modicon Quantu... Active	■■■■■	Apr 25, 2022 05:31 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.93 -	-
590485	Schneider Electric PLCs (Update B) Multiple Vulnerabili... Active	■■■□□	Apr 25, 2022 05:31 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.93 -	-

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

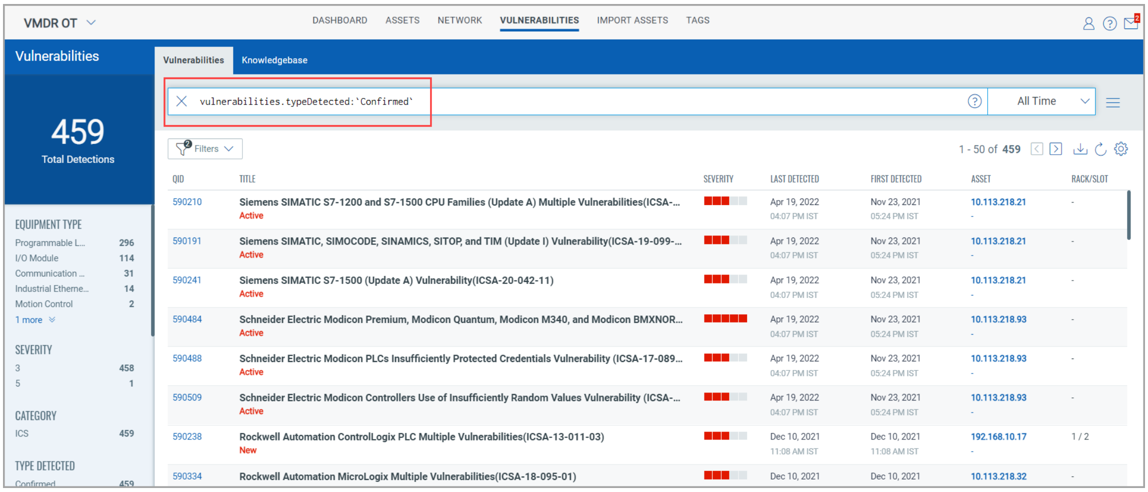
-When the vulnerability was last detected on the asset

-When the vulnerability was first detected on the asset

-Asset on which the vulnerability is detected

- Rack/Slot details

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.



```
vulnerabilities.typeDetected:`Confirmed`
```

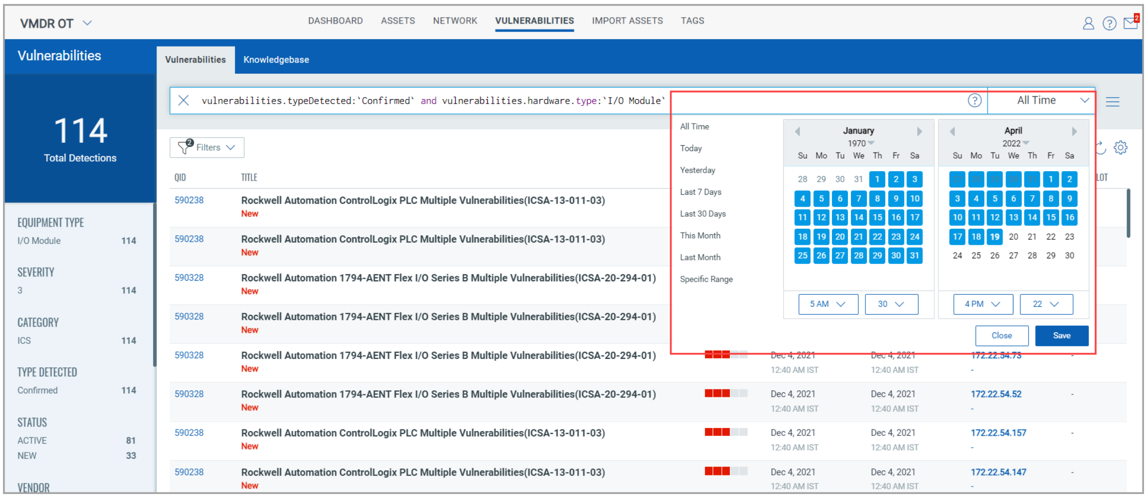
459
Total Detections

EQUIPMENT TYPE	
Programmable L...	296
I/O Module	114
Communication ...	31
Industrial Etherne...	14
Motion Control	2
1 more	
SEVERITY	
3	458
5	1
CATEGORY	
ICS	459
TYPE DETECTED	
Confirmed	459

1 - 50 of 459

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET	RACK/SLOT
590210	Siemens SIMATIC S7-1200 and S7-1500 CPU Families (Update A) Multiple Vulnerabilities(ICSA-... Active	■■■□□	Apr 19, 2022 04:07 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.21 -	-
590191	Siemens SIMATIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update I) Vulnerability(ICSA-19-099-... Active	■■■□□	Apr 19, 2022 04:07 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.21 -	-
590241	Siemens SIMATIC S7-1500 (Update A) Vulnerability(ICSA-20-042-11) Active	■■■□□	Apr 19, 2022 04:07 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.21 -	-
590484	Schneider Electric Modicon Premium, Modicon Quantum, Modicon M340, and Modicon BMXNOR... Active	■■■■■	Apr 19, 2022 04:07 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.93 -	-
590488	Schneider Electric Modicon PLCs Insufficiently Protected Credentials Vulnerability (ICSA-17-089... Active	■■■□□	Apr 19, 2022 04:07 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.93 -	-
590509	Schneider Electric Modicon Controllers Use of Insufficiently Random Values Vulnerability (ICSA-... Active	■■■□□	Apr 19, 2022 04:07 PM IST	Nov 23, 2021 05:24 PM IST	10.113.218.93 -	-
590238	Rockwell Automation ControlLogix PLC Multiple Vulnerabilities(ICSA-13-011-03) New	■■■□□	Dec 10, 2021 11:08 AM IST	Dec 10, 2021 11:08 AM IST	192.168.10.17 -	1 / 2
590334	Rockwell Automation MicroLogix Multiple Vulnerabilities(ICSA-18-095-01)	■■■□□	Dec 10, 2021	Dec 10, 2021	10.113.218.32	-

The date and time range selector next to the search bar can be used choose to view vulnerabilities detected within a specific time period.



```
vulnerabilities.typeDetected:`Confirmed` and vulnerabilities.hardware.type:`I/O Module`
```

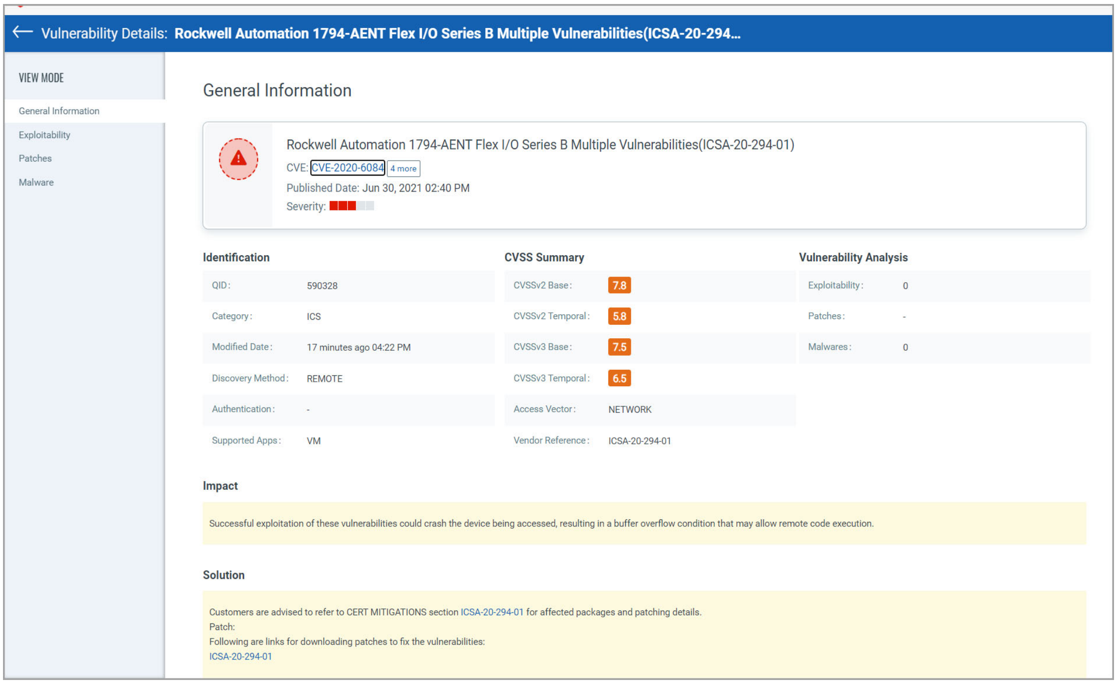
114
Total Detections

EQUIPMENT TYPE	
I/O Module	114
SEVERITY	
3	114
CATEGORY	
ICS	114
TYPE DETECTED	
Confirmed	114
STATUS	
ACTIVE	81
NEW	33
VENDOR	

QID	TITLE					
590238	Rockwell Automation ControlLogix PLC Multiple Vulnerabilities(ICSA-13-011-03) New					
590238	Rockwell Automation ControlLogix PLC Multiple Vulnerabilities(ICSA-13-011-03) New					
590328	Rockwell Automation 1794-AENT Flex I/O Series B Multiple Vulnerabilities(ICSA-20-294-01) New					
590328	Rockwell Automation 1794-AENT Flex I/O Series B Multiple Vulnerabilities(ICSA-20-294-01) New					
590328	Rockwell Automation 1794-AENT Flex I/O Series B Multiple Vulnerabilities(ICSA-20-294-01) New	🟥🟥🟥⬜⬜	Dec 4, 2021 12:40 AM IST	Dec 4, 2021 12:40 AM IST	172.22.54.73 -	-
590328	Rockwell Automation 1794-AENT Flex I/O Series B Multiple Vulnerabilities(ICSA-20-294-01) New	🟥🟥🟥⬜⬜	Dec 4, 2021 12:40 AM IST	Dec 4, 2021 12:40 AM IST	172.22.54.52 -	-
590238	Rockwell Automation ControlLogix PLC Multiple Vulnerabilities(ICSA-13-011-03) New	🟥🟥🟥⬜⬜	Dec 4, 2021 12:40 AM IST	Dec 4, 2021 12:40 AM IST	172.22.54.157 -	-
590238	Rockwell Automation ControlLogix PLC Multiple Vulnerabilities(ICSA-13-011-03) New	🟥🟥🟥⬜⬜	Dec 4, 2021 12:40 AM IST	Dec 4, 2021 12:40 AM IST	172.22.54.147 -	-

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.



Vulnerability Details: **Rockwell Automation 1794-AENT Flex I/O Series B Multiple Vulnerabilities(ICSA-20-294...**

General Information

Rockwell Automation 1794-AENT Flex I/O Series B Multiple Vulnerabilities(ICSA-20-294-01)
CVE: CVE-2020-6084
Published Date: Jun 30, 2021 02:40 PM
Severity: 🟥🟥🟥⬜⬜

Identification		CVSS Summary		Vulnerability Analysis	
QID:	590328	CVSSv2 Base:	7.8	Exploitability:	0
Category:	ICS	CVSSv2 Temporal:	5.8	Patches:	-
Modified Date:	17 minutes ago 04:22 PM	CVSSv3 Base:	7.5	Malwares:	0
Discovery Method:	REMOTE	CVSSv3 Temporal:	6.5		
Authentication:	-	Access Vector:	NETWORK		
Supported Apps:	VM	Vendor Reference:	ICSA-20-294-01		

Impact

Successful exploitation of these vulnerabilities could crash the device being accessed, resulting in a buffer overflow condition that may allow remote code execution.

Solution

Customers are advised to refer to CERT MITIGATIONS section ICSA-20-294-01 for affected packages and patching details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ICSA-20-294-01

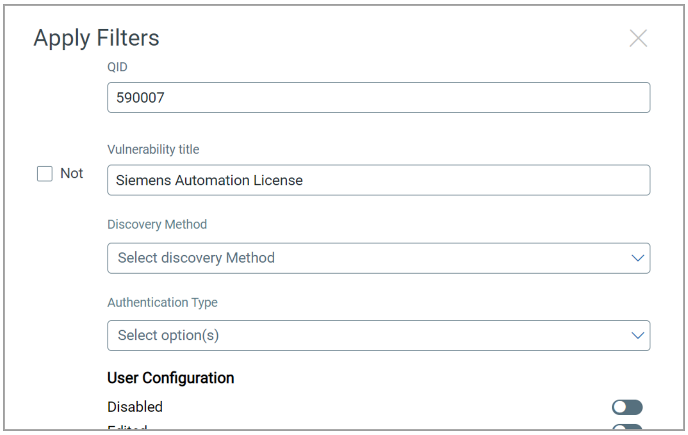
Viewing KnowledgeBase

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**.



Apply Filters

QID: 590007

□ Not — Vulnerability title: Siemens Automation License

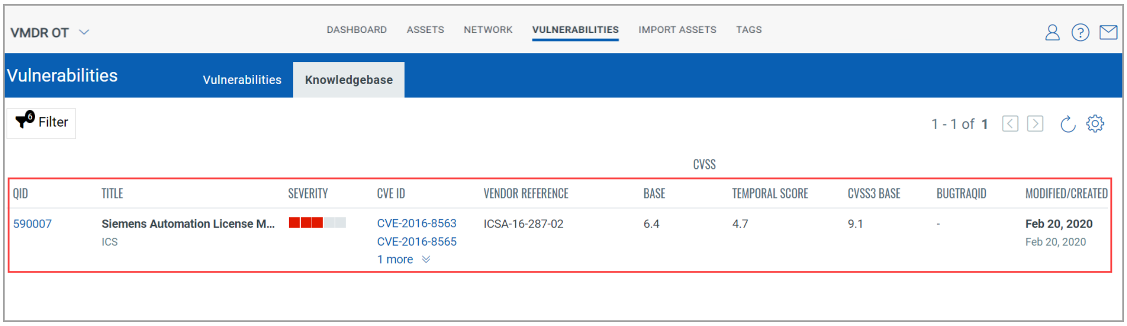
Discovery Method: Select discovery Method

Authentication Type: Select option(s)

User Configuration

Disabled

You get the results based on your search criteria.



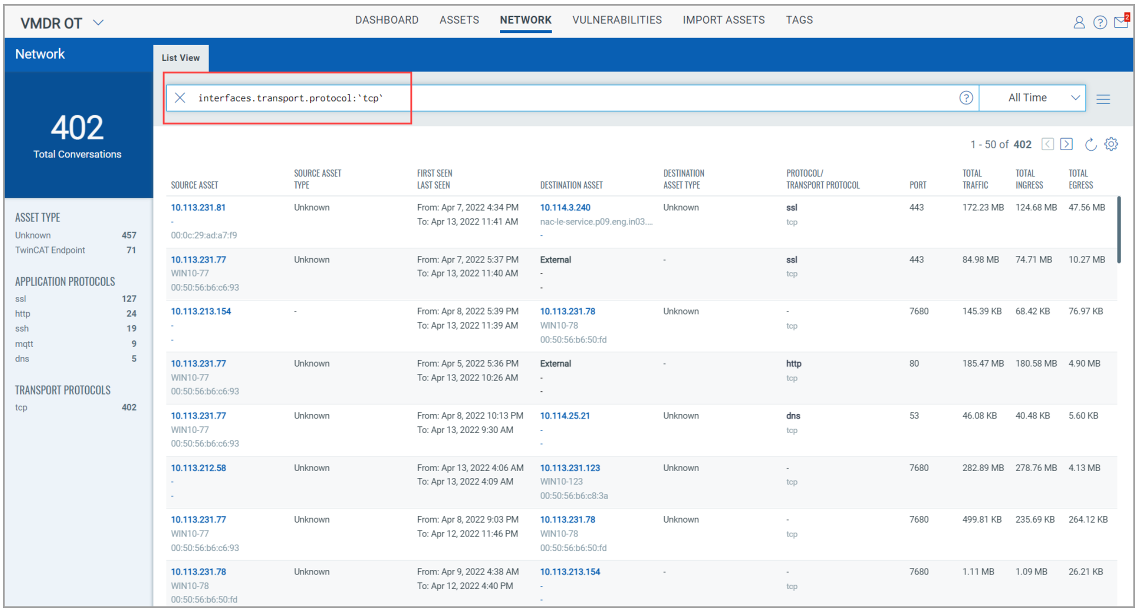
					CVSS				
QID	TITLE	SEVERITY	CVE ID	VENDOR REFERENCE	BASE	TEMPORAL SCORE	CVSS3 BASE	BUGTRAQID	MODIFIED/CREATED
590007	Siemens Automation License M... ICS	🟥🟥🟥⬜⬜	CVE-2016-8563 CVE-2016-8565 1 more	ICSA-16-287-02	6.4	4.7	9.1	-	Feb 20, 2020 Feb 20, 2020

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.



```
interfaces.transport.protocol:`tcp`
```

402
Total Conversations

ASSET TYPE	
Unknown	457
TwinCAT Endpoint	71
APPLICATION PROTOCOLS	
ssl	127
http	24
ssh	19
mqtt	9
dns	5
TRANSPORT PROTOCOLS	
tcp	402

SOURCE ASSET	SOURCE ASSET TYPE	FIRST SEEN LAST SEEN	DESTINATION ASSET	DESTINATION ASSET TYPE	PROTOCOL/ TRANSPORT PROTOCOL	PORT	TOTAL TRAFFIC	TOTAL INGRESS	TOTAL EGRESS
10.113.231.81 - 00:0c:29:ad:a7:f9	Unknown	From: Apr 7, 2022 4:34 PM To: Apr 13, 2022 11:41 AM	10.114.3.240 nac-le-service.p09.eng.in03.... -	Unknown	ssl tcp	443	172.23 MB	124.68 MB	47.56 MB
10.113.231.77 WIN10-77 00:50:56:b6:c6:93	Unknown	From: Apr 7, 2022 5:37 PM To: Apr 13, 2022 11:40 AM	External - -	-	ssl tcp	443	84.98 MB	74.71 MB	10.27 MB
10.113.213.154 - -	-	From: Apr 8, 2022 5:39 PM To: Apr 13, 2022 11:39 AM	10.113.231.78 WIN10-78 00:50:56:b6:50:fd	Unknown	- tcp	7680	145.39 KB	68.42 KB	76.97 KB
10.113.231.77 WIN10-77 00:50:56:b6:c6:93	Unknown	From: Apr 5, 2022 5:36 PM To: Apr 13, 2022 10:26 AM	External - -	-	http tcp	80	185.47 MB	180.58 MB	4.90 MB
10.113.231.77 WIN10-77 00:50:56:b6:c6:93	Unknown	From: Apr 8, 2022 10:13 PM To: Apr 13, 2022 9:30 AM	10.114.25.21 - -	Unknown	dns tcp	53	46.08 KB	40.48 KB	5.60 KB
10.113.212.58 - -	Unknown	From: Apr 13, 2022 4:06 AM To: Apr 13, 2022 4:09 AM	10.113.231.123 WIN10-123 00:50:56:b6:c8:3a	Unknown	- tcp	7680	282.89 MB	278.76 MB	4.13 MB
10.113.231.77 WIN10-77 00:50:56:b6:c6:93	Unknown	From: Apr 8, 2022 9:03 PM To: Apr 12, 2022 11:46 PM	10.113.231.78 WIN10-78 00:50:56:b6:50:fd	Unknown	- tcp	7680	499.81 KB	235.69 KB	264.12 KB
10.113.231.78 WIN10-78 00:50:56:b6:50:fd	Unknown	From: Apr 9, 2022 4:38 AM To: Apr 12, 2022 4:40 PM	10.113.213.154 - -	-	- tcp	7680	1.11 MB	1.09 MB	26.21 KB

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

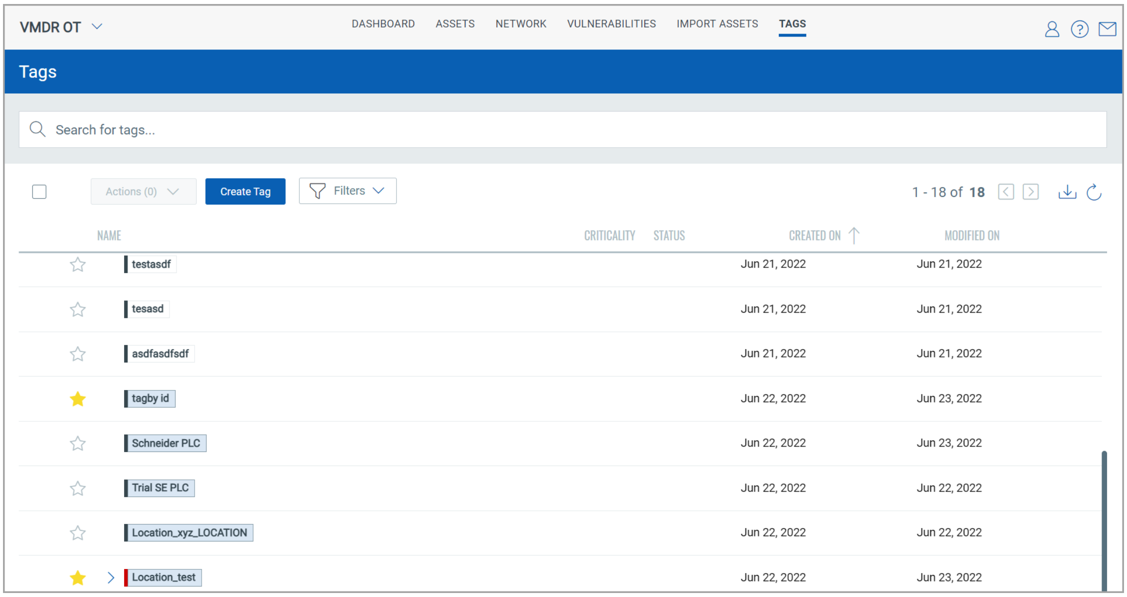
- Source asset
- Source asset type
- When the asset was first and last seen communicating on the network
- Destination Asset
- Destination asset type
- Protocol/Transport protocol used for communication
- Port on which they are communicating
- Total traffic volume for the network
- Ingress traffic volume 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 But isn't automatically classifying 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 list of various tags applied to the assets and option to create new tag.

You can search the tag from the Search for tags.



	NAME	CRITICALITY	STATUS	CREATED ON	MODIFIED ON
☆	testasdf			Jun 21, 2022	Jun 21, 2022
☆	tesasd			Jun 21, 2022	Jun 21, 2022
☆	asdfasdfsdf			Jun 21, 2022	Jun 21, 2022
★	tagby id			Jun 22, 2022	Jun 23, 2022
☆	Schneider PLC			Jun 22, 2022	Jun 23, 2022
☆	Trial SE PLC			Jun 22, 2022	Jun 22, 2022
☆	Location_xyz_LOCATION			Jun 22, 2022	Jun 22, 2022
★	Location_test			Jun 22, 2022	Jun 23, 2022

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).

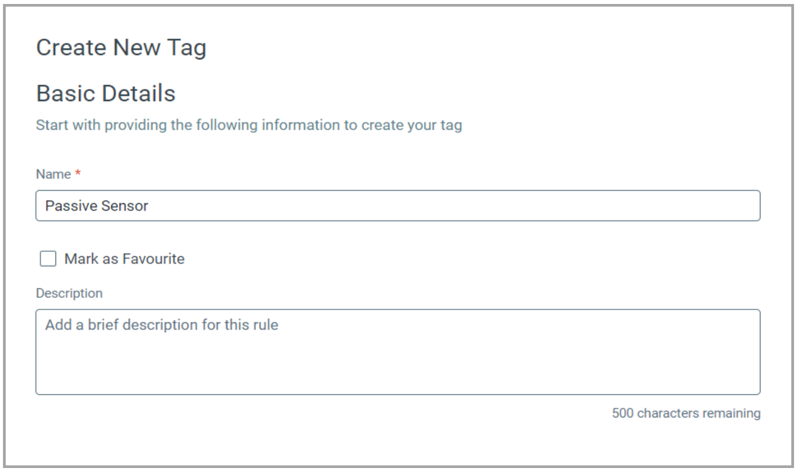
- Tag Properties

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.



Create New Tag

Basic Details

Start with providing the following information to create your tag

Name *

Passive Sensor

□ Mark as Favourite

Description

Add a brief description for this rule

500 characters remaining

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 asses 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 example of a dynamic tag.

Managing Asset Tags

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

Function	Steps
View the Tag details	Go to the **TAGS** tab and click **View** under **Quick Actions** menu of the tag.
Edit the Tag details	Go to the **TAGS** tab and click **Edit** under **Quick Actions** menu of the tag.
Find Assets with the specific tag	Go to the **TAGS** 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.
Move tags to root	Go to the **TAGS** 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
Mark tag as favorites	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
Remove tag from favorites	Go to the **TAGS** tab and click Find Assets under **Quick Actions** menu of the specific tag.

Add Child Tag	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.
Delete a Tag	Go to the **TAGS** tab and click Delete from **Quick Actions** menu for a tag. You can only delete custom created tag
Save the Tags	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.
Save the Static Tag	When you save your static tag, you can apply it to your asset from the Assets tab
Use of tag filters	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.

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.

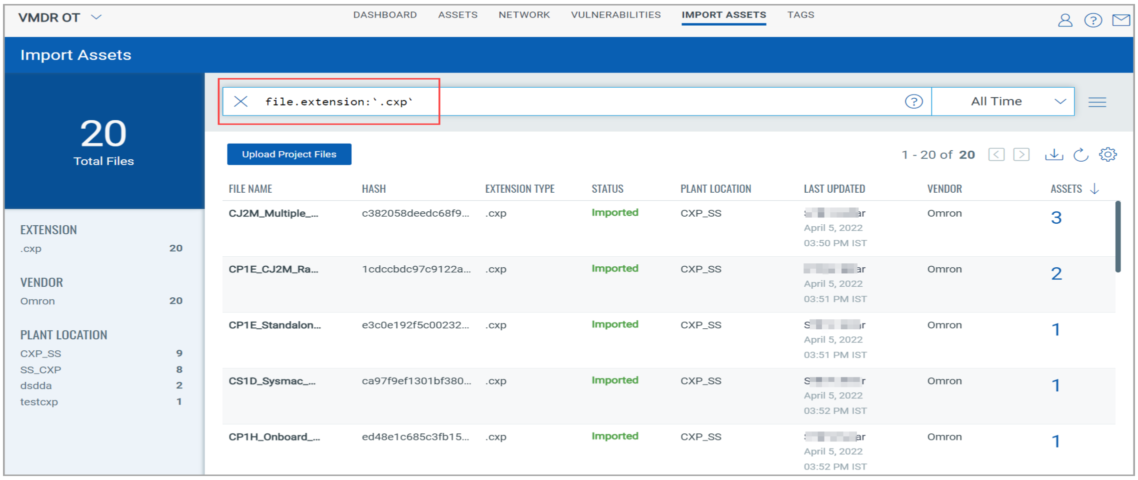
On the Import Assets tab, there is option to upload project files. Project files support extensions like cxp, zip, Xml, RSS and many more.

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.

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.



20
Total Files

```
file.extension:`.cxp`
```

EXTENSION	
.cxp	20
VENDOR	
Omron	20
PLANT LOCATION	
CXP_SS	9
SS_CXP	8
dsdda	2
testcxp	1

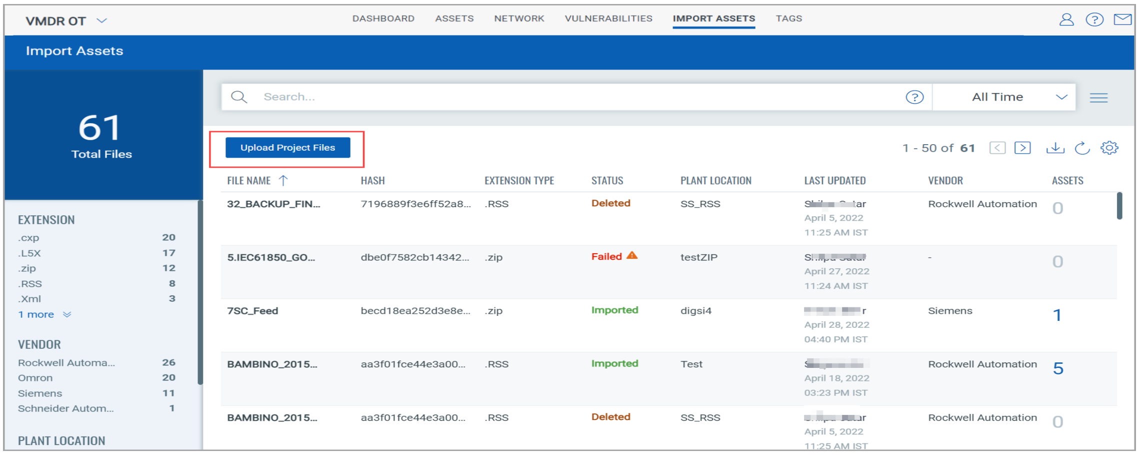
FILE NAME	HASH	EXTENSION TYPE	STATUS	PLANT LOCATION	LAST UPDATED	VENDOR	ASSETS ↓
CJ2M_Multiple_...	c382058deedc68f9...	.cxp	Imported	CXP_SS	[redacted] April 5, 2022 03:50 PM IST	Omron	3
CP1E_CJ2M_Ra...	1cdccbdc97c9122a...	.cxp	Imported	CXP_SS	[redacted] April 5, 2022 03:51 PM IST	Omron	2
CP1E_Standalon...	e3c0e192f5c00232...	.cxp	Imported	CXP_SS	[redacted] April 5, 2022 03:51 PM IST	Omron	1
CS1D_Sysmac_...	ca97f9ef1301bf380...	.cxp	Imported	CXP_SS	[redacted] April 5, 2022 03:52 PM IST	Omron	1
CP1H_Onboard_...	ed48e1c685c3fb15...	.cxp	Imported	CXP_SS	[redacted] April 5, 2022 03:52 PM IST	Omron	1

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

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



61
Total Files

EXTENSION

.cxp	20
.L5X	17
.zip	12
.RSS	8
.Xml	3

1 more

VENDOR

Rockwell Automa...	26
Omron	20
Siemens	11
Schneider Autom...	1

PLANT LOCATION

1 - 50 of 61

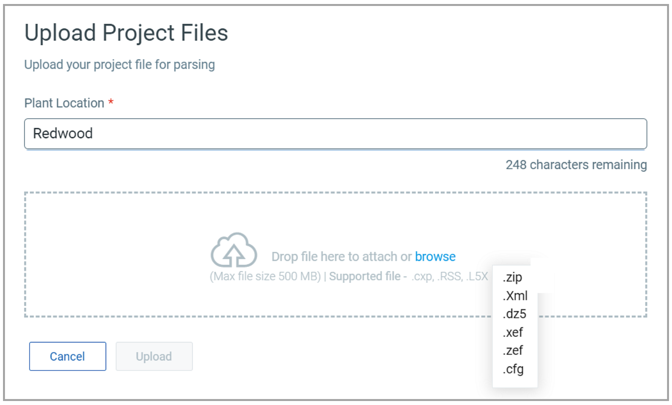
FILE NAME	HASH	EXTENSION TYPE	STATUS	PLANT LOCATION	LAST UPDATED	VENDOR	ASSETS
32_BACKUP_FIN...	7196889f3e6ff52a8...	.RSS	Deleted	SS_RSS	[redacted] April 5, 2022 11:25 AM IST	Rockwell Automation	0
5.IEC61850_GO...	dbe0f7582cb14342...	.zip	Failed ⚠	testZIP	[redacted] April 27, 2022 11:24 AM IST	-	0
7SC_Feed	becd18ea252d3e8e...	.zip	Imported	digsi4	[redacted] April 28, 2022 04:40 PM IST	Siemens	1
BAMBINO_2015...	aa3f01fce44e3a00...	.RSS	Imported	Test	[redacted] April 18, 2022 03:23 PM IST	Rockwell Automation	5
BAMBINO_2015...	aa3f01fce44e3a00...	.RSS	Deleted	SS_RSS	[redacted] April 5, 2022 11:25 AM IST	Rockwell Automation	0

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**.



Upload Project Files

Upload your project file for parsing

Plant Location *

Redwood

248 characters remaining

Drop file here to attach or browse

(Max file size 500 MB) | Supported file - .cxp, .RSS, .L5X

.zip
.Xml
.dz5
.xef
.zef
.cfg

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

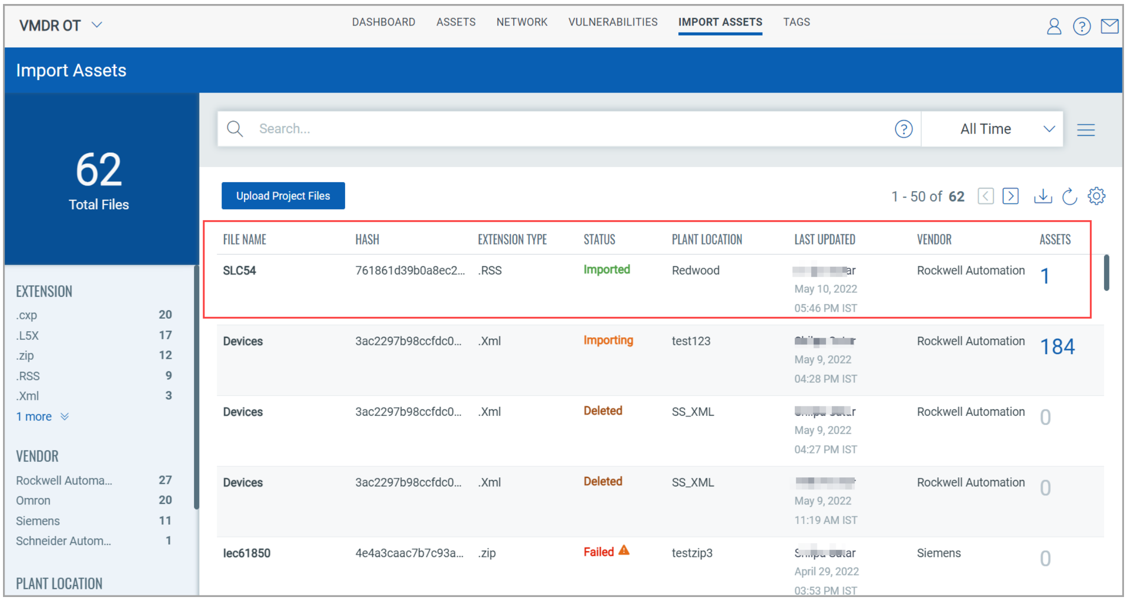
Importing - file is still uploading

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.



62
Total Files

EXTENSION

.cxp	20
.L5X	17
.zip	12
.RSS	9
.Xml	3

1 more

VENDOR

Rockwell Automa...	27
Omron	20
Siemens	11
Schneider Autom...	1

PLANT LOCATION

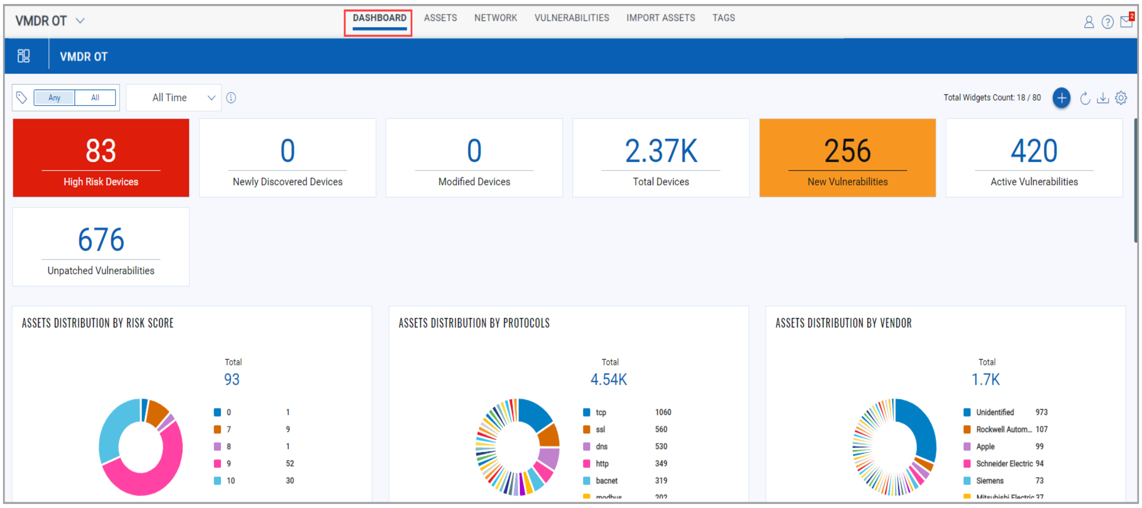
FILE NAME	HASH	EXTENSION TYPE	STATUS	PLANT LOCATION	LAST UPDATED	VENDOR	ASSETS
SLC54	761861d39b0a8ec2...	.RSS	Imported	Redwood	[redacted] May 10, 2022 05:46 PM IST	Rockwell Automation	1
Devices	3ac2297b98ccfdc0...	.Xml	Importing	test123	[redacted] May 9, 2022 04:28 PM IST	Rockwell Automation	184
Devices	3ac2297b98ccfdc0...	.Xml	Deleted	SS_XML	[redacted] May 9, 2022 04:27 PM IST	Rockwell Automation	0
Devices	3ac2297b98ccfdc0...	.Xml	Deleted	SS_XML	[redacted] May 9, 2022 11:19 AM IST	Rockwell Automation	0
Iec61850	4e4a3caac7b7c93a...	.zip	Failed ⚠	testzip3	[redacted] April 29, 2022 03:53 PM IST	Siemens	0

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.

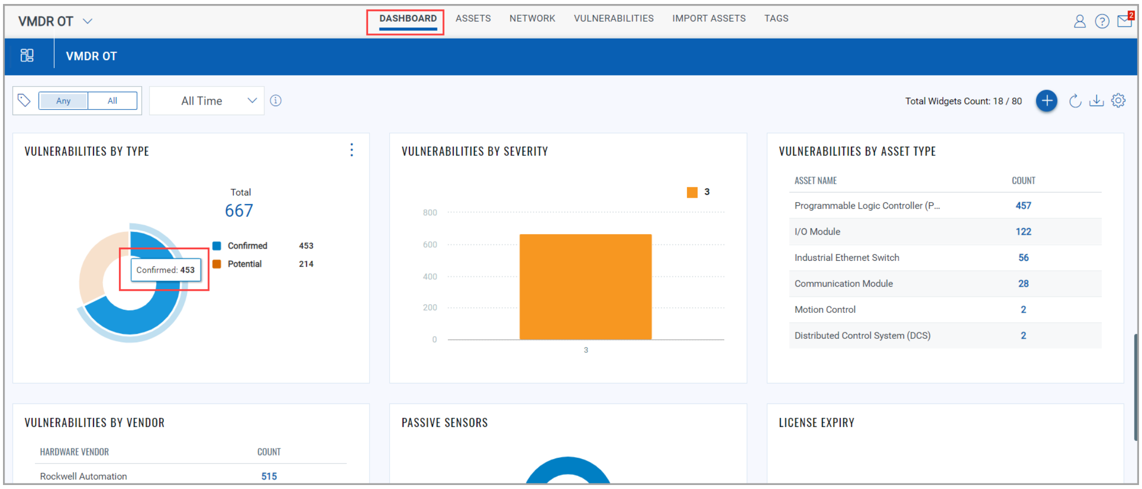
To see the VMDR OT dashboard, select **VMDR OT** from the application selector. On the dashboard, there are count cards like high risk devices, newly discovered devices, new vulnerabilities, active vulnerabilities and so on by default.

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.



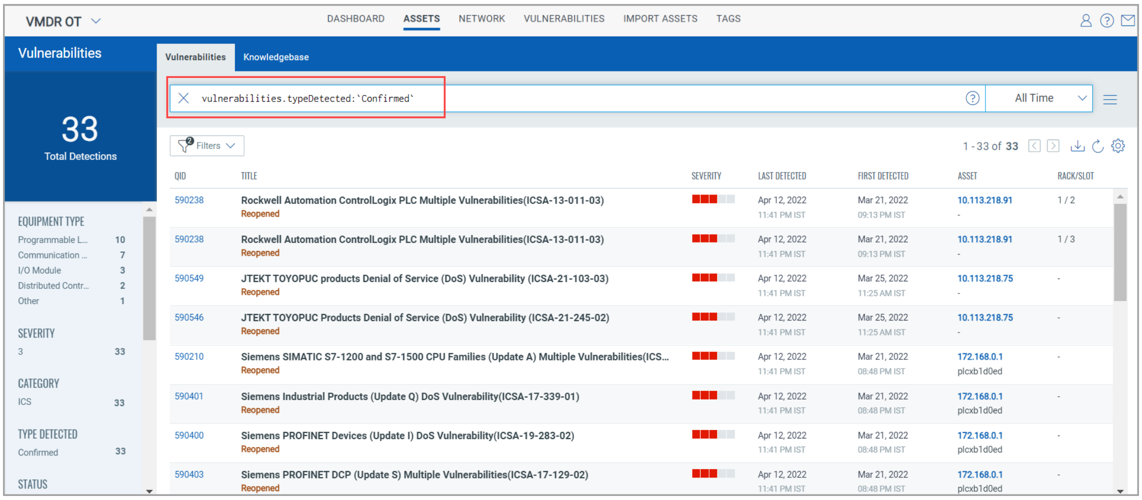
VULNERABILITIES BY ASSET TYPE

ASSET NAME	COUNT
Programmable Logic Controller (P...	457
I/O Module	122
Industrial Ethernet Switch	56
Communication Module	28
Motion Control	2
Distributed Control System (DCS)	2

VULNERABILITIES BY VENDOR

HARDWARE VENDOR	COUNT
Rockwell Automation	515

All the details of the confirmed vulnerability are displayed.



```
vulnerabilities.typeDetected:`Confirmed`
```

EQUIPMENT TYPE	
Programmable L...	10
Communication ...	7
I/O Module	3
Distributed Contr...	2
Other	1
SEVERITY	
3	33
CATEGORY	
ICS	33
TYPE DETECTED	
Confirmed	33
STATUS	

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET	RACK/SLOT
590238	Rockwell Automation ControlLogix PLC Multiple Vulnerabilities(ICSA-13-011-03) Reopened	■■■□□	Apr 12, 2022 11:41 PM IST	Mar 21, 2022 09:13 PM IST	10.113.218.91 -	1 / 2
590238	Rockwell Automation ControlLogix PLC Multiple Vulnerabilities(ICSA-13-011-03) Reopened	■■■□□	Apr 12, 2022 11:41 PM IST	Mar 21, 2022 09:13 PM IST	10.113.218.91 -	1 / 3
590549	JTEKT TOYOPUC products Denial of Service (DoS) Vulnerability (ICSA-21-103-03) Reopened	■■■□□	Apr 12, 2022 11:41 PM IST	Mar 25, 2022 11:25 AM IST	10.113.218.75 -	-
590546	JTEKT TOYOPUC Products Denial of Service (DoS) Vulnerability (ICSA-21-245-02) Reopened	■■■□□	Apr 12, 2022 11:41 PM IST	Mar 25, 2022 11:25 AM IST	10.113.218.75 -	-
590210	Siemens SIMATIC S7-1200 and S7-1500 CPU Families (Update A) Multiple Vulnerabilities(ICS... Reopened	■■■□□	Apr 12, 2022 11:41 PM IST	Mar 21, 2022 08:48 PM IST	172.168.0.1 plcxb1d0ed	-
590401	Siemens Industrial Products (Update Q) DoS Vulnerability(ICSA-17-339-01) Reopened	■■■□□	Apr 12, 2022 11:41 PM IST	Mar 21, 2022 08:48 PM IST	172.168.0.1 plcxb1d0ed	-
590400	Siemens PROFINET Devices (Update I) DoS Vulnerability(ICSA-19-283-02) Reopened	■■■□□	Apr 12, 2022 11:41 PM IST	Mar 21, 2022 08:48 PM IST	172.168.0.1 plcxb1d0ed	-
590403	Siemens PROFINET DCP (Update S) Multiple Vulnerabilities(ICSA-17-129-02) Reopened	■■■□□	Apr 12, 2022 11:41 PM IST	Mar 21, 2022 08:48 PM IST	172.168.0.1 plcxb1d0ed	-

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.

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

Appendix B - Supported IT Protocols

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

- TCP
- UDP
- DHCP
- HTTP
- DNS
- SSH
- SSL
- Kerberos
- CDP
- LLDP
- UPnP
- SMTP
- SNMP
- Netbios
- SIP
- ARP
- IPv6 Neighbor Discovery

Appendix C - Supported OCA

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

Vendor	Engineering Tool	File Extension Type
Beckhoff zip	TwinCAT3	.zip, .tnzip
Emerson	DeltaV Explorer	.fhx
GE Fanuc	Proficy Machine Edition	.zip, .SwxCF
Omron	CX-Programmer	.cxp
Rockwell	RSLogix 500	.RSS
Rockwell	RSLogix 5000/ Studio 5000	.l5x
Rockwell	RS System Ferret	.Xml
Siemens	Digsi4	.zip
Siemens	Digsi5	.zip,.dz5
Siemens	Simatic Manager (Step 7)	.cfg
Siemens	TIA Portal	.zip, .zap(.zap15, .zap15_1, .zap17)
Siemens	LOGO! Soft Comfort	.lnp, .mnp
Siemens	PRONETA	.xml
Schneider	Unity L/XL	.zef, .xef
Schneider	TwidoSuite	.zip, .xtwd
Schneider	Schneider Concept	..ccf, .CCF
Mitsubishi	GX Works3	.gx3
Mitsubishi	GX Works2	.gxw
Red Lion Controls	Crimson	.cd3, .cd31