tripwire®

TRIPWIRE®
INDUSTRIAL
VISIBILITY

TRIPWIRE INDUSTRIAL VISIBILITY 4.2.4
USER GUIDE

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

User Guide Revisions

Rev	Date	Owner	Author	Description
Rev 1	April 2021	Moshe Alvoer	Jodie Quinn	Initial Version

Contents

1 About this Document

Tripwire Industrial Visibility (TIV) provides broad visibility across multi-vendor Operational Technology (OT) environments. It uncovers network configuration issues and threats to critical control systems.

1.1 Purpose

This User Guide provides instructions for operating Tripwire Industrial Visibility, version 4.2.4.

1.2 Audience

The intended audience is Tripwire customers (IT and OT professionals): users, representatives, and partners.

> **Note** Functionality for Administrators is marked as *Only Admins* in the section heading.

1.3 Related Documents

Table 1 Related Documents

TIV Quick Installation Guide
TIV Installation Guide
TIV ClarotyOS Guide
TIV Reference Guide
TIV Web API User Guide

2 Introducing TIV

TIV provides agentless security for OT networks providing real-time visibility over assets and systems. It alerts users of known or unknown security incidents.

2.1 Key Benefits

Customers can quickly detect industrial operations risk, enhance cyber resiliency, and minimize unplanned downtime. TIV prevents damage to physical processes, industrial equipment, injury or death. It reduces management costs because it can be quickly deployed and scaled across multiple sites.

TIV has built-in integration with:

- SIEM systems
- Log management systems
- Asset management systems
- Ticketing systems.

The integration of TIV with existing security tools provides Security Operations Center (SOC) teams with real-time alerts and threat hunting capabilities. Its visibility features improve network segmentation. Security Operators monitor the industrial network and can identify network vulnerabilities. This saves time and improves cyber resiliency.

2.1.1 Visibility with Active and Passive Methods

With both active and passive methods, TIV offers visibility of assets within minutes. It actively monitors the entire network and it passively reads network communications without interfering with operations or industrial processes. TIV displays the assets and asset architecture on the web interface dashboard.

In the active mode, TIV uses active querying for asset information. TIV scans and performs queries of the assets. TIV's Active solution is detailed in the *TIV Reference Guide*.

When passively sniffing the network, mapping it, and gathering information, TIV identifies and exposes security threats. TIV uses network behaviors (a "baseline") by examining network communication through a Switched Port Analyzer (SPAN) port. It separates valid communication from security threats.

With Deep Packet Inspection (DPI), TIV identifies:

- The specific assets on the network
- The lines of asset communication
- Communication timing

- Protocols between assets
- The types of commands and registers used
- The values of valid responses.

Baselines may be changed if required.

TIV closely inspects every network communication and collects all events to identify a possible threat. All related events go into a single alert that notifies of a possible threat to the process, such as an operational anomaly or a security attack. One alert per threat rather than one alert per event avoids alert-overload.

You can then

- assign
- address
- handle the alert.

2.1.2 Root Cause Analytics and ML Algorithm

Root cause analytics (RCA) examines each alert based on:

- TIV's machine learning (ML) algorithms
- Indicators
- User preferences.

RCA reduces noise and presents the user with relevant data as alerts.

The ML algorithm distinguishes legitimate minor events from alerts that are a risk to the environment. Every change is logged in the system and classified as an event, but only the highest alerts are shown to the end-user. These alerts are enriched by Claroty's Threat Intelligence (CTI). Risk-based indicators and a proprietary scoring index prioritize these ML-generated alerts within an end-user's queue. Alerting sensitivity is customizable to assist different organizations' risk acceptance criteria.

2.2 Architecture

TIV's scalable architecture supports a variety of hierarchies and use cases:

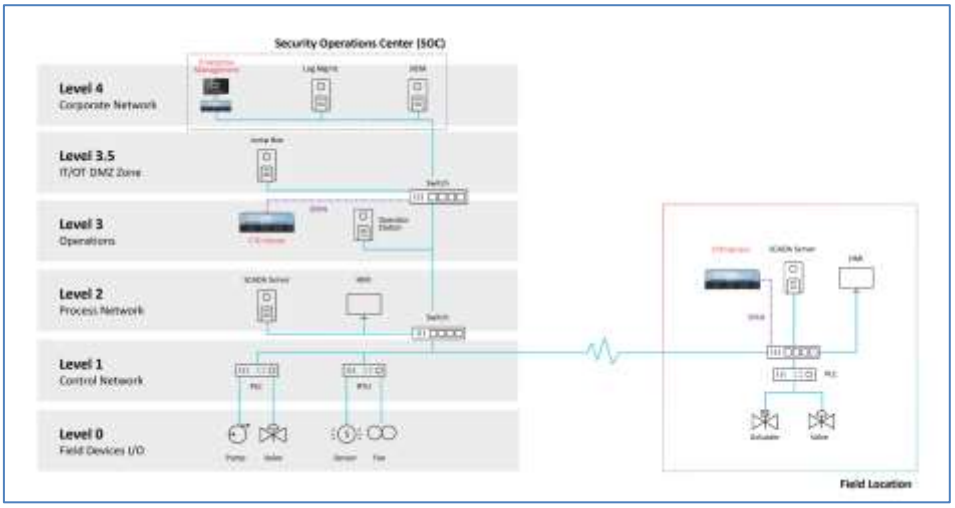


Figure 1 TIV Architecture

TIV can be configured as a simple standalone server or in a distributed model where lower components are connected to an Enterprise Management Console (EMC). It can accommodate widely geographically dispersed environments with a sizeable number of assets across multiple remote sites. It can also be configured to support installations in extreme environments across isolated sites that have low network bandwidth or satellite connectivity.

The TIV solution is made of several components as shown in Figure 1. A TIV Server is located at each site and performs sniffing and DPI. The TIV Server is connected through a span port to sniff the network. Additionally, for isolated network segments, one or more TIV Sensors may be used to collect and process network traffic and send it to the TIV Server for incorporation into its database. Information from all TIV Servers are sent to the Enterprise Management Console. The EMC gathers all the relevant information and displays the security posture of all sites.

2.3 Scalability

TIV is designed with scalable architecture to support deployments in environments across multiple remote sites – often in extreme environmental conditions.

TIV can be configured with

- sensors with limited computing power
- a smaller physical footprint
- virtual environments
- specific scenarios requiring communication over low bandwidth networks.

TIV supports deployments in refineries, power generation, electric transmission grids, oil and gas pipelines, manufacturing, etc. This unique

architecture can be deployed at large, distributed installations, monitoring thousands of devices.

2.4 TIV Server

The TIV Server, also called the TIV Site, is a physical or virtual server that provides real-time cybersecurity and visibility of industrial control networks within distributed network environments and architectures. It exists at each location and is the only mandatory component. Other components are required depending on the use case and type of implementation.

2.4.1 DPI Processing

The TIV Server performs the DPI processing as shown below:

Figure 2 Processes in the TIV Server

The TIV Server performs:

- Sniffing
- Dissection
- Processing
- Correlation
- Visualization.

TIV collects all the data in the network and builds the asset inventory. Based on what the system learned, it creates security and integrity alerts like policy deviation.

It creates a risk assessment report with all the risks and analysis of the network, including:

- Unsecure protocols
- Unpatched vulnerabilities
- Open alerts
- Protocols distribution.

2.4.2 Distributed Configuration

Alternatively, it is possible to split the work done by TIV Server into distributed components (including TIV Sensor, TIV Sensor Light — see section 14), each located in different areas but all communicating to a TIV Server. The TIV server performs correlation and visualization functions.

The distributed configuration is useful for assets not accessible to a TIV Server or to balance the load on a single TIV Server.

2.5 Enterprise Management Console (EMC)

The Enterprise Management Console (EMC) is TIV's central appliance, usually located at the Security Operations Center (SOC) or in the corporate site. It displays information collected from all TIV sites on its web interface.

It displays the:

- network diagram
- statistics
- alerts for each site.

The EMC interface provides a global dashboard that consolidates data from multiple sites, showing their:

- Assets
- Activities
- Alerts
- Access requests.

The EMC also manages the TIV Servers, like upgrading the TIV application on the TIV Servers and if present, their attached TIV Sensors.

The EMC is versatile and integrates with

- SIEM solutions
- firewalls
- Active Directory
- SMTP servers.

2.6 TIV Sensor

A TIV Sensor component performs sniffing, dissection, and part of the processing. When working in operational mode, the TIV Sensor will only send the anomalies it identified and some metadata to the TIV Server, lowering the bandwidth required to the TIV Server.

The TIV Sensor operates as a remote extension of the TIV Server. It is used in sites with limited physical connectivity or across multiple remote sites with limited out-of-band aggregation.

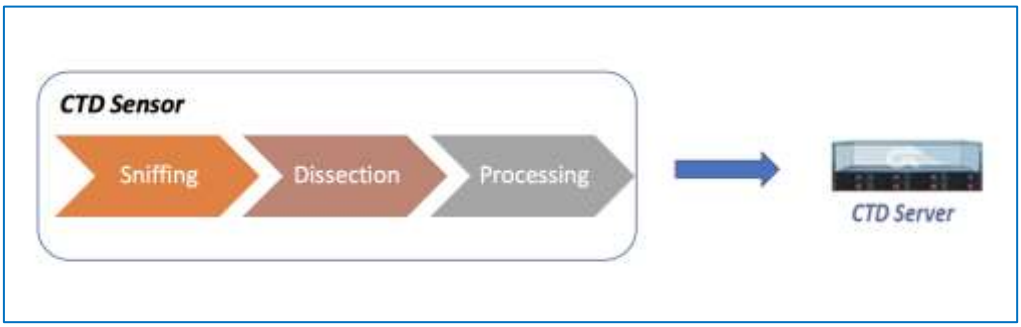


Figure 3 Processes in the TIV Sensor

2.7 TIV Sensor Light

The TIV Sensor Light performs only sniffing and initial compression (typically 50% compression) of the sniffed packets. It does not create alerts or build the asset inventory. It sends the sniffed information to the TIV Server for dissection and processing. TIV Sensor Light is designed primarily for use cases in which a minimal hardware footprint is required.

Figure 4 Processes in the TIV Sensor Light

3 TIV Interface

TIV provides

- extreme visibility
- continuous threat and vulnerability monitoring
- deep insights into ICS networks.

It was designed to ensure safe, secure, and reliable operations in large, complex industrial networks – ensuring zero impact to the operational processes and improved cyber resiliency.

TIV:

- extracts precise details about each asset on the industrial network
- profiles all communications and protocols
- generates a behavioral baseline of legitimate traffic.

It alerts you to

- network changes
- vulnerabilities
- threats.

The alerts the system generates provides the context you need to investigate and respond quickly.

3.1 Login

Login to TIV with your username and password provided by your Administrator, and click **Login**:

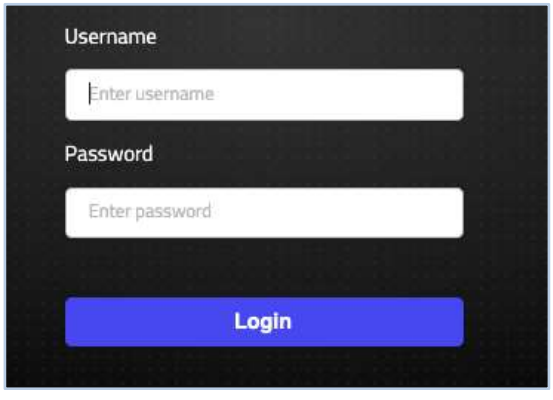


Figure 5 TIV Login screen

- The Dashboard appears:

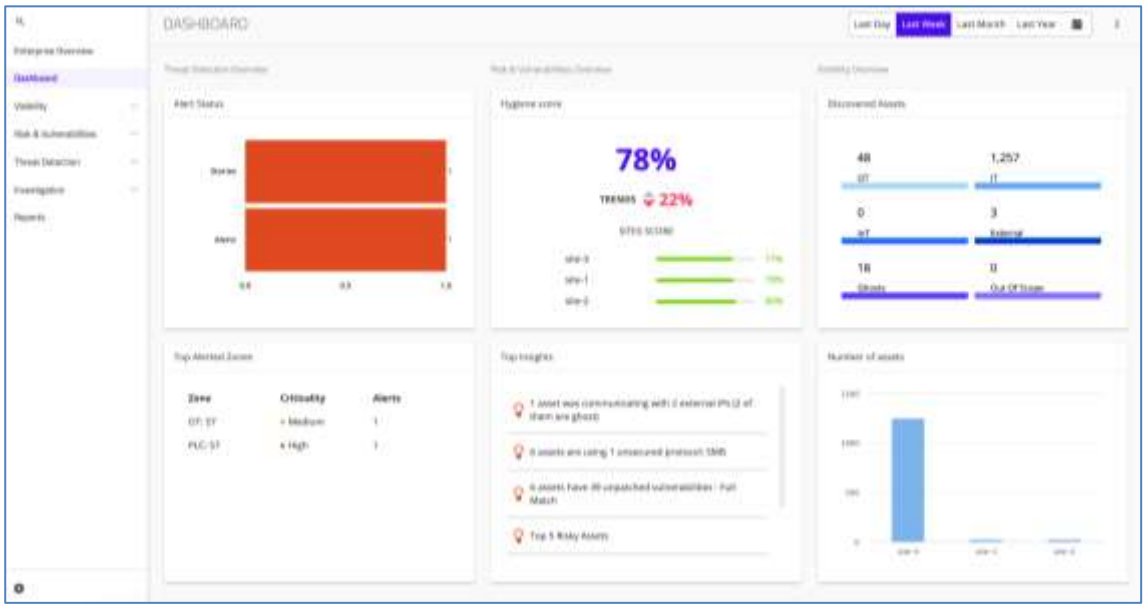


Figure 6 EMC Dashboard

3.2 Navigating the Interface

TIV is based on a hierarchical navigation system that supports finding and navigating to specific information or configurations down to a desired page. Instead of needing to recall the exact hierarchy of a page in the system, you can simply search for it.

This is especially helpful if your role and responsibilities require you to use different parts of TIV at different times.

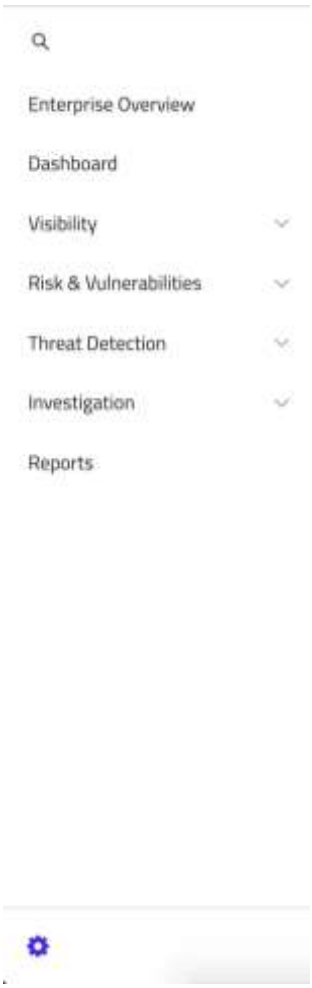
This navigation system, from which all TIV pages can be accessed, includes:

- A hierarchical menu, structured according to the core TIV focus areas: Threat Detection, Risk and Vulnerability, Investigation, Visibility, and System Settings
- Quick page search and navigation
- A Navigation Path for clear indication of your location
- The option to show or hide the menu to save screen space for the main content

■

3.2.1 Main TIV Menu

Click the three-line menu icon ☰ on the top left corner of the interface to hide the **Main Menu** for the TIV Platform. Click again to show it.



Enterprise Overview – A high level overview for all multiple site deployments. Relevant only for Admins. Available on the EMC only. See section 3.3.

Dashboard – Provides an overview of the network with dynamic graphs and metrics; see section 4.1.

Visibility – Gives comprehensive visibility of assets and their exposures.

Risk & Vulnerabilities –Identifies which aspects of the network can be fortified to achieve a more robust network architecture and enhance protection of the system.

Threat Detection – Used to identify threats early in their process. Relying on its in-depth knowledge of protocols, configuration, and communication flows, the system identifies known threat attacks and zero-day attacks as well as ones with sophisticated OT payloads.

Investigation –Used to investigate alerts or events in the network. Gives deeper visibility and tools for understanding the network and its behavior.

Reports – Generates the summarized and configurable Risk Assessment report; see section 9.6.

(Settings) – Primarily used for Admins to set up and customize TIV features as needed; see chapters 10 through 16.

Figure 7: Main Menu

3.2.2 Search in Menu

The search window in the top left corner of the screen makes navigating TIV easy. Type the name of any TIV page, or part of it, and as you type, any matched results are highlighted and clickable as shown below.

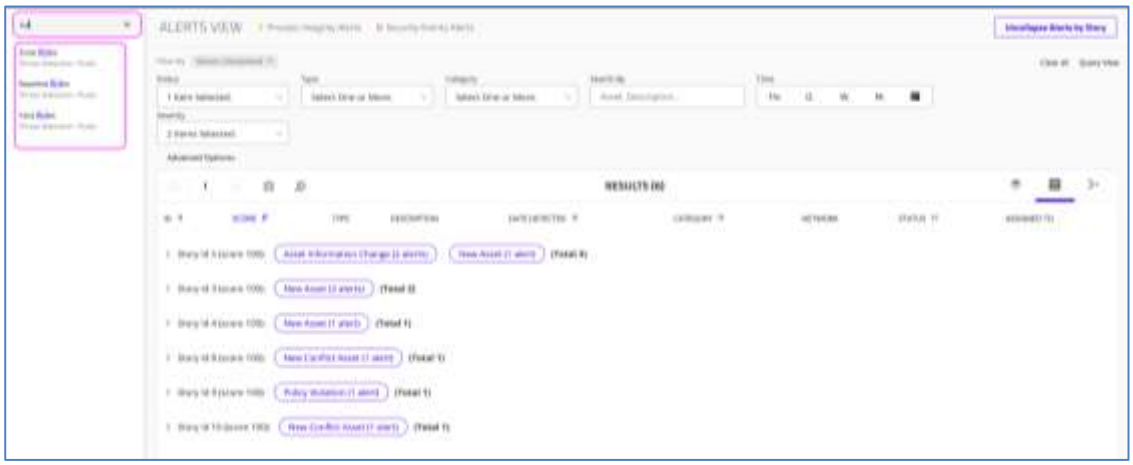


Figure 8: Searching in the menu

3.2.2.1 Search Keyboard Shortcut

You can open the search window from anywhere in TIV by typing **Shift + F**.

3.2.3 Activity Bar

After you log in, the **Activity Bar** appears at the top of your screen:

The Activity Bar consists of the following parts:

1. **Hide/Show Main Menu** – Click to hide or show the Main Menu and search window.
2. **Site Selector** – For sites connected to an EMC, enables you to view and perform TIV functions on an individual site on all sites collectively.
3. **Navigation Path** – Indicates where in the TIV navigational hierarchy you are. Underlined items in the path indicate a table.
   (In the example, you are currently viewing the details of Event #155. Clicking Events in the path brings you one level up to the entire Events list).
4. **System Mode** – When the system is in Training Mode, the Training Mode indicator displays.
5. **Logged-in User Menu** – Opens a menu for viewing and performing functions related to the logged in user.

3.2.3.1 Site Selector

This drop-down menu and search are only available when connected with an EMC:

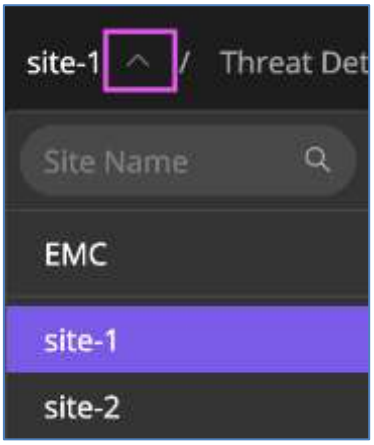


Figure 9 Site Navigation Dropdown

Depending on your configuration, expand the site selector dropdown to select:

- The EMC showing data for all sites in one display
- Individual sites

For organizations with many sites, use the **Site Name** search to find a specific site.

See section 4.2 for details about the EMC and the TIV Site.

3.2.3.2 Logged-in User Menu

Clicking on your **Username** opens this dropdown, displaying the details of your login history including:

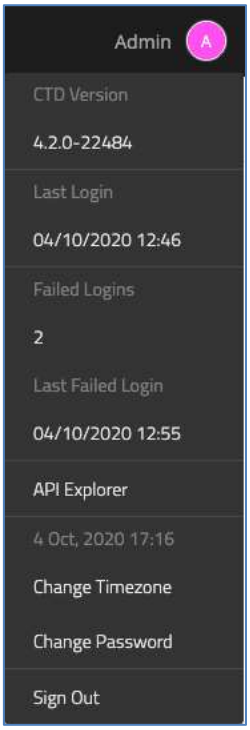


Figure 10 Login, Time Zone, Password & Sign-Out Controls

- **TIV Version** – Currently-installed version of TIV
- **Last Login** - Displays your last login date and time
- **Failed Logins** - The number of failed logins
- **Last Failed Login** - The date and time of the last failed login
- **API Explorer** (Admin user only) – Click on **API Explorer** and it will bring you to the API documentation.
- **Change Time Zone** – For managing sites in a time zone different from where you are physically located. This setting affects only the time zone you see on your browser. Each user can set a different time zone, while the browser time zone is the Default:

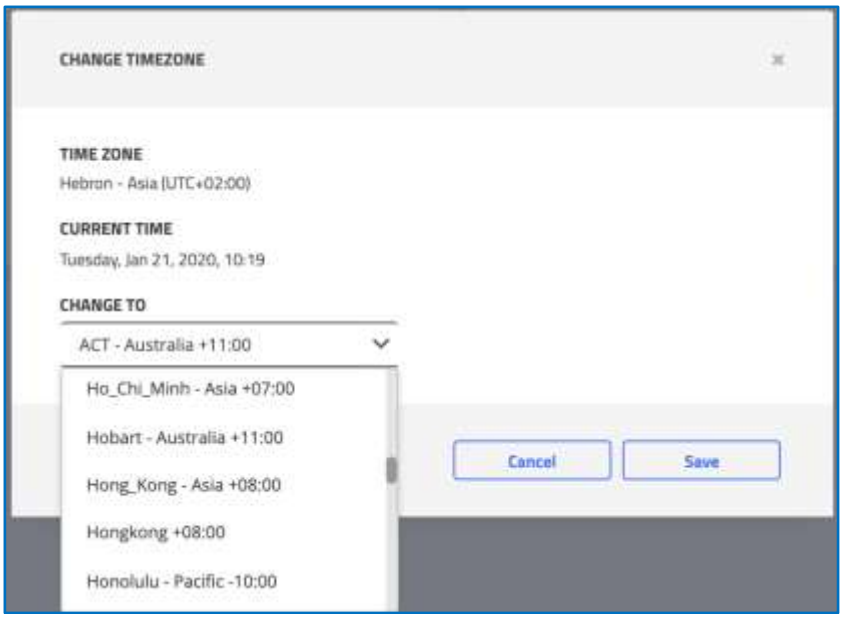


Figure 11 Change Time Zone dialog

6. **Change Password** – Reset your password**.** The Change Password popup opens, and you need to provide your correct current password and your new password:

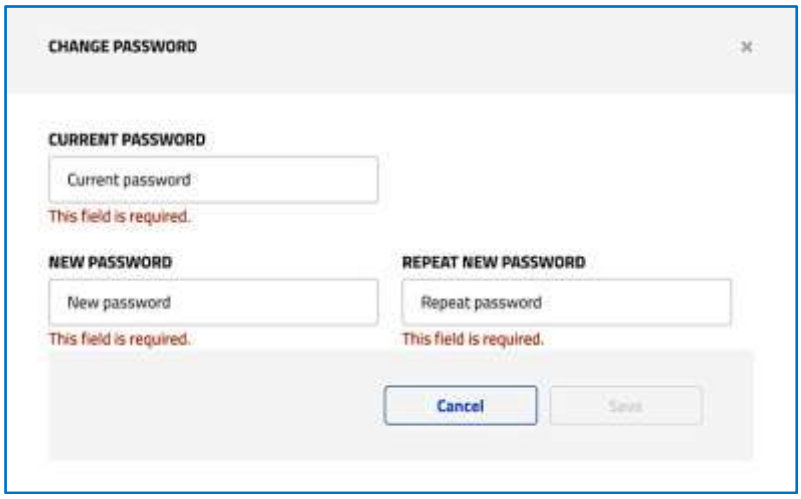


Figure 12 Change Password dialog

7. **Sign Out** – Click to exit your session.

3.3 Browser Back Navigation

You can use the browser's back button to navigate to the previous page.

> Note Internal page changes are not considered for back navigation.

3.4 Enterprise Overview

The EMC **Enterprise Overview** offers a quick overview of all sites in the enterprise. You can observe all the sites in the network and access any specific site down to the level of individual assets (provided you have at least 'Read' System Permissions).

The **Enterprise Overview** provides visibility into your sites, including site status, installed version, IP address, number of assets, and alerts. The top bar of the All Sites page provides the statistics aggregated from all the connected sites.

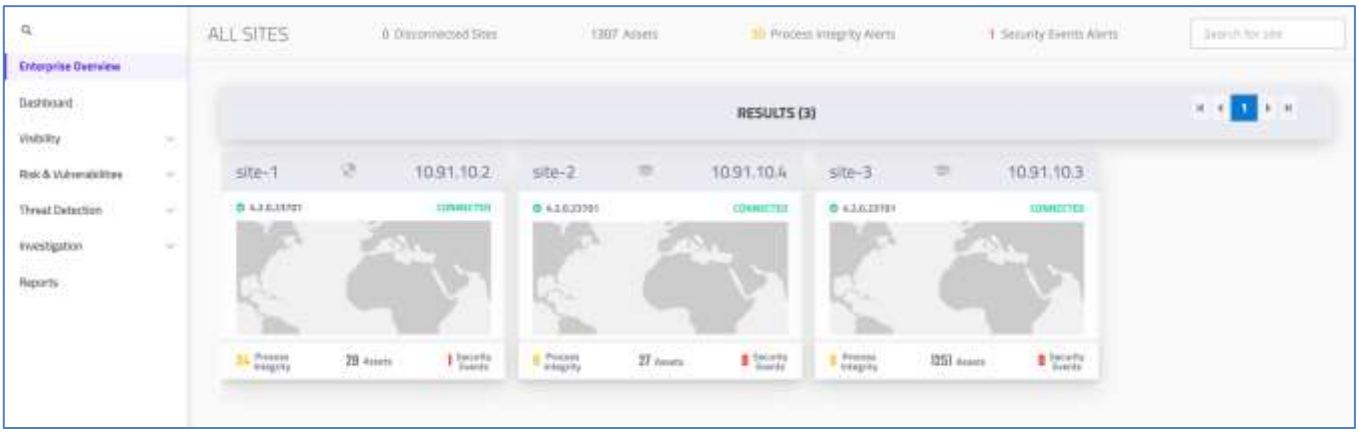


Figure 13 Enterprise Overview: Example

Figure 14 Enterprise Overview - Information per site

Each window displays the following data for its site:

1. Site name
2. The TIV Mode (Training or Operational)
3. Site address

4. TIV version number
5. Connection status
6. A map of the site's geographic location
7. Number of Process Integrity alerts
8. The total number of assets
9. Number of Security Event alerts

Click any information in the window to view more details.

4 Dashboards

4.1 Site Dashboard

The TIV Dashboard provides an at-a-glance assessment of key information for an individual site. (When selecting a specific site from the EMC, the Dashboard displayed is the same as when viewed from the TIV Site directly.)

After logging into the system, the Dashboard appears:

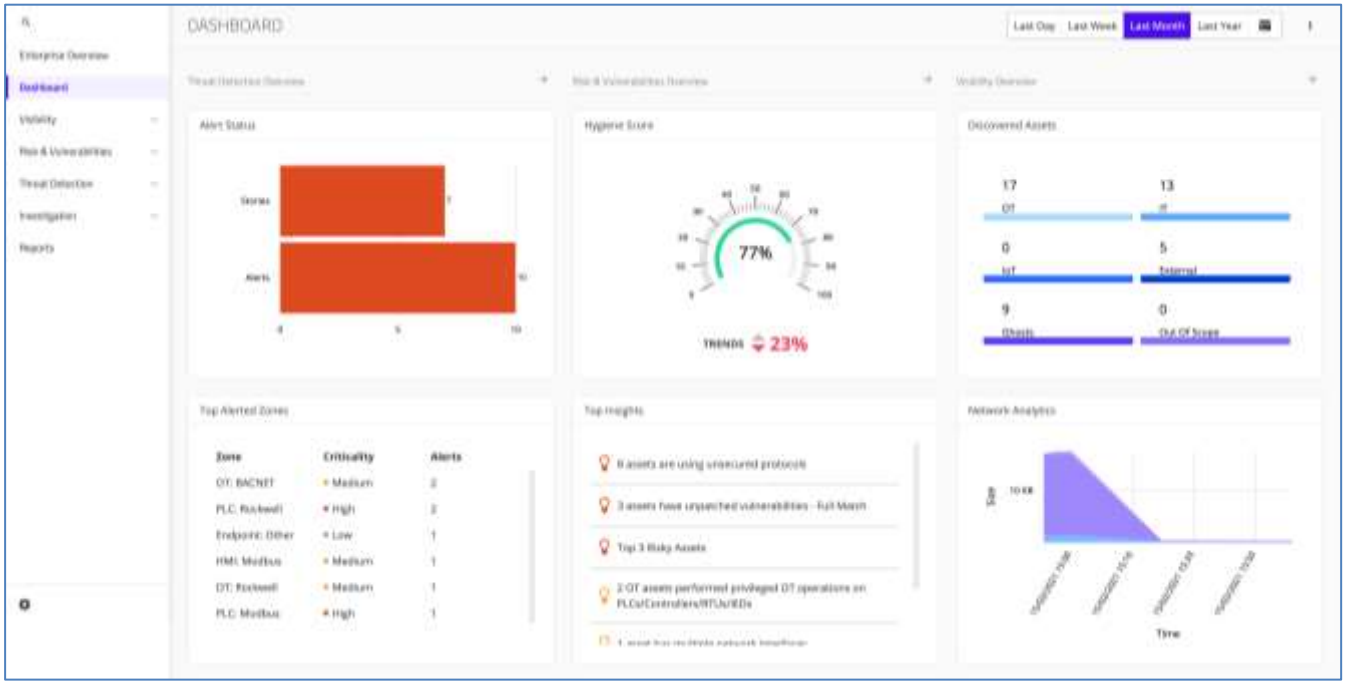


Figure 15 TIV Dashboard

The Dashboard consists of three panels, grouped by the core functions of TIV – Threat Detection, Risk & Vulnerabilities, and Visibility. They emphasize real time characteristics for a standalone site for the last day, week, month, or year, displaying predefined widgets per topic.

Clicking an Overview link opens a page with key information about the core function. Clicking the data in a widget enables you to drill down to deeper levels of detail.

- Threat Detection – Focuses on potential threats to the system, displaying:
  - **Alert Status** - A color-coded bar graph of Alert Stories and Alerts with a count of each alert severity level.
    Clicking the graph opens the Alerts page filtered for the alert count and severity in the graph.

- **Top Alerted Zones** - A list of the top Zones with alerts.
  Clicking a zone opens the Zone View page with details about the selected zone.

- Risk & Vulnerabilities – Highlights the key risks and vulnerabilities, displaying:
  - **Hygiene Score** - The current cumulative risk level posed to the system. This score comprises the critical security insights, CVEs, and anomalies that were detected, as well as how many critical assets were identified. A low score indicates that the system is highly vulnerable to attacks.
    - The Hygiene Score also includes an upward or downward trend over the selected timeframe. See section 4.3 for details.
    - To improve the Hygiene Score, see section 6.3.1.
  - **Top Insights** - Derived from your entire security posture and producing a holistic picture and risk assessment, this window displays the top, critical-level Insights.
    Clicking an Insight opens the Insights page giving you the ability to drill down further to the information contained in the Insight.
- Visibility– Provides a high-level view of assets and network activity
  - **Discovered Assets** – Displays the total number of IT vs. OT vs. IoT assets, as well as the number of external assets, ghost assets, and out of scope assets.
    Clicking a number opens the Assets page filtered by the information clicked in the Dashboard.
  - **Network Analytics** – Shows superimposed graphs of the Top 8 protocols in use, charting their throughput over the selected time frame, broken down and color-coded per protocol. All protocols in use are shown in a stacked popup.
    Clicking an end point in the graph opens the Zone Rules page filtered by the selected protocol.

The Dashboard is also accessible in the Main Menu by clicking **Dashboard**. For the EMC dashboard, see section 4.2.

4.2 EMC Dashboard

The EMC Dashboard aggregates key information from all the sites across the enterprise and displays it in the same manner as for an individual site, with two exceptions:

- Instead of the **Network Analytics** graph in the Site Dashboard, the EMC Dashboard contains a **Number of Assets** graph that displays the total number of assets discovered for each site in the enterprise.

Clicking a site opens its Assets page.

Figure 16 Number of Assets - EMC Dashboard

- The Hygiene Score is calculated according to all sites in the enterprise and the trend is broken down per site. See section 4.3 for details.

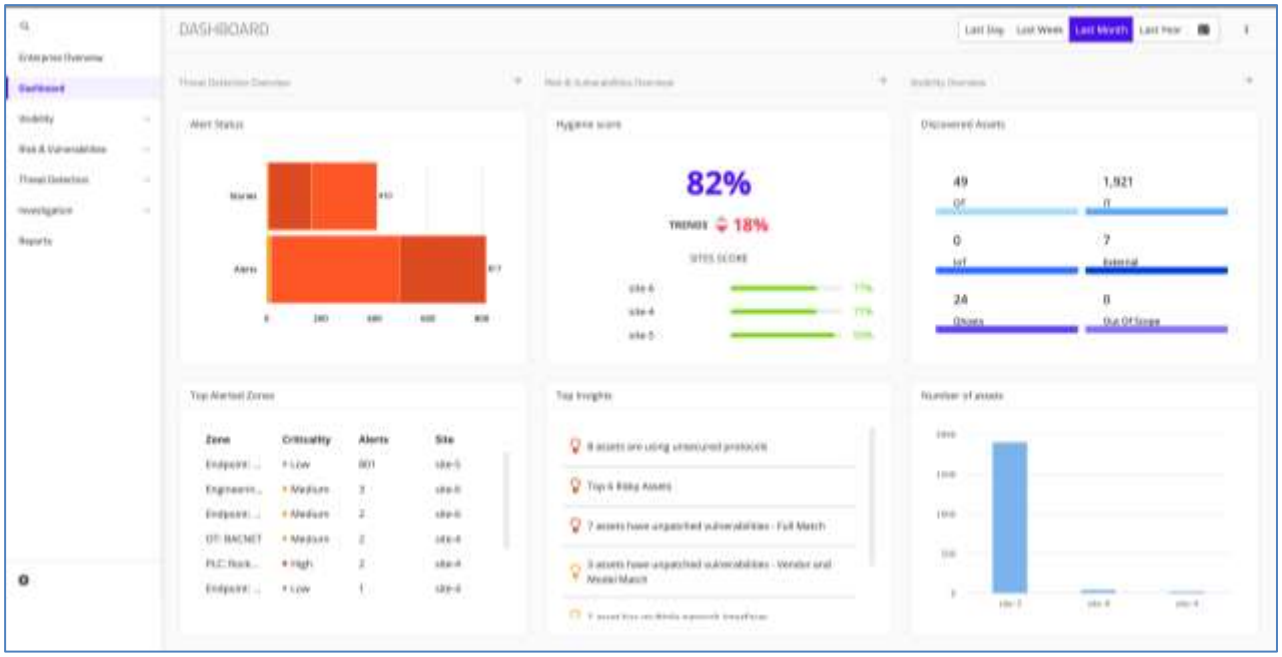


Figure 17 Multiple Site Configuration - EMC Dashboard

4.3 Hygiene Score Trend

The hygiene score trend shows, in percentage, changes based on the timeframe selected in the timeframe selector:

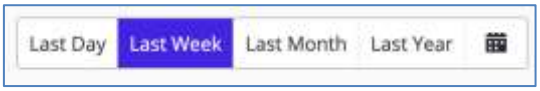


Figure 18 Dashboard Timeframe Selector

The following colors show in the trend:

- **Green** – change was good, and the hygiene score improved.
- **Red** – the network became riskier and the hygiene score decreased.

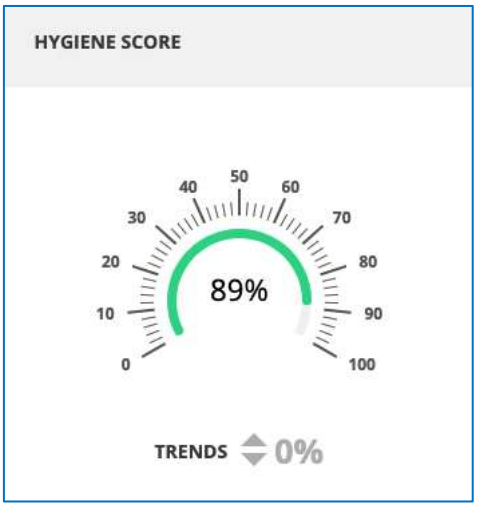


Figure 19: Hygiene Score - Site View

Figure 20: Hygiene Score - EMC View

5 Visibility

5.1 Overview

The Visibility Overview displays TIV's comprehensive visibility of assets and exposures. It allows users to create customized widgets as needed, presenting extreme visibility into your network. TIV manages the assets by monitoring traffic and collecting data passively, actively, and via the App DB. The Visibility tools reveal the entire OT, IT, and IoT inventories in the environment, throughout all layers of the network. They enable deep visibility into the ICS assets, including down to the card/rack slot data where applicable.

The Visibility widgets present the network topology showing the assets and the network analytics. Network-based diagrams show the communication patterns and dataflows. They are according to the Purdue model format, both line and plant level, depending on the deployment architecture. Users can use them to identify all the details of the individual components, as well as their operating systems, firmware, device classifications, and more. Potential misconfiguration issues are flagged quickly. By automatically clustering assets and baselines into virtual zones, users have the advantage of managing them more effectively.

5.2 Visibility Overview

To access the Visibility Overview, click **Visibility > Overview** in the Main Menu.

The Visibility Overview appears as follows for a standalone TIV Server (see section 5.3 for the EMC Overview):

Figure **21** Visibility Overview

1. Use the **Time Frame Selector** to display information based on the time period of your preference (day/week/month/year/date range). All widgets described below represent the results per the selected duration.

Site Visibility Widgets

2. **Visibility Info Bar** – Displays the total assets, zones, IT/OT/IoT assets, new assets and inactive assets.
3. **Discovered Assets** – Displays the breakdown of prominent assets discovered, subdivided into asset types: OT, IT, External, Broadcast/Multicast, Ghosts, etc.
4. **IT vs OT Policies** – This widget presents bar graphs of IT vs. OT policies.
5. **Asset Breakdown**: Types – Pie chart showing each asset breakdown per asset Type.
6. **OT Assets Distribution** – The breakdown of the OT assets per type (e.g. PLC, HMI, Engineering Station).
7. **IT Assets Distribution** – The breakdown of the IT assets per type (e.g. Endpoint, Printer, Networking).
8. **IoT Assets Distribution** – The breakdown of the IoT assets per type (e.g. Camera, VOIP Phone).
9. **DNS Queries Over Time** – A time graph of the number of DNS queries that have occurred.
10. **Most Frequent DNS Queries**– Provides a listing of the most frequent DNS Queries and how often each has occurred.
11. **Most Common Domain Names by Assets**– Provides a listing of the most frequent DNS Queries and how often each has occurred.
12. **Network Analytics** – Graph of bandwidth breakdown per most prevalent protocols.
13. **Summary** – A count of OT Assets, OT Operations, and Write and Execute type OT Operations.
14. **OT Operations by type** – Breaks down the number of alerts for each type of OT operation.
15. **Latest OT Operation** – Lists the top 10 most recent OT asset alerts.
16. **Top Assets by Process Value Requests** – Lists the top 10 assets with the highest Read/Publish or Write counts.

> Note: These Visibility breakdown widgets are not affected by the timeframe. Clicking on any portion of the pie chart leads you to the corresponding filtered Asset Page.

5.3 EMC Visibility Overview

To access the EMC Visibility Overview, with EMC selected, click **Visibility > Overview** in the Main Menu.

The EMC Visibility Overview appears as follows:

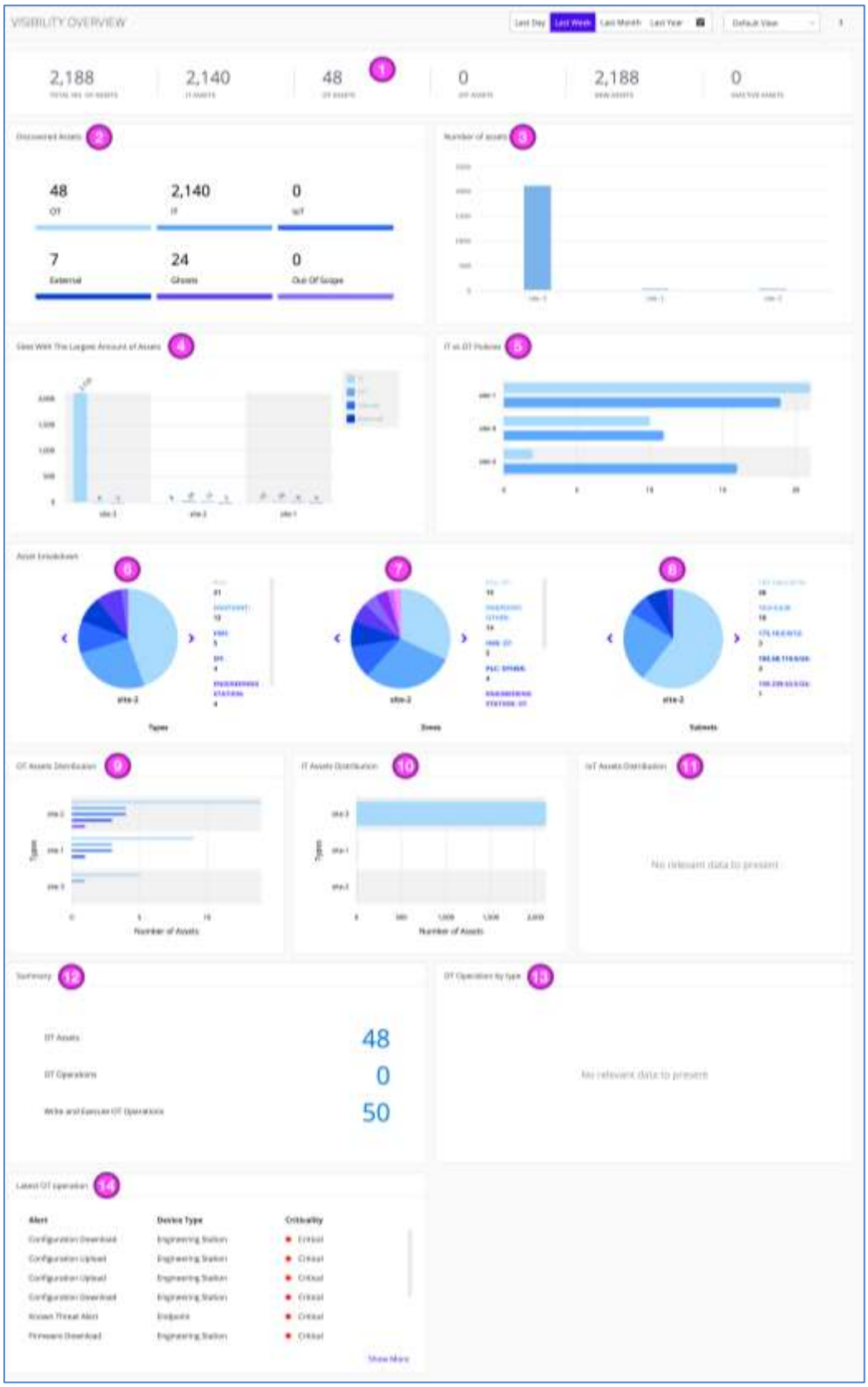


Figure 22 EMC Visibility Overview

EMC Visibility Widgets

1. **Visibility Info Bar** – Displays the total assets, IT/OT/IoT assets, new assets and inactive assets across all sites.
2. **Discovered Assets** – Displays the breakdown of prominent assets discovered, subdivided into asset types: OT, IT, External, Broadcast/Multicast, Ghosts, etc. across all sites.
3. **Number of Assets** – Shows the total number of assets **per site**.
4. **Sites with the Largest Amount of Assets** – Displays up to 10 sites with the largest amount of assets, subdivided into asset types: OT, IT, External, Broadcast/Multicast, Ghosts, etc. The vertical bar graphs are **per site**. A color legend is displayed for distinguishing the most prominent types of assets in each site.
5. **IT vs OT Policies** – Shows horizontal bar graphs of IT vs. OT policies **per site**.
6. **Asset Breakdown: Types** – Pie chart showing each asset breakdown per asset **Type per site**. Use the **< >** arrows to navigate to the **<** Previous or Next **>** sites.
7. **Asset Breakdown: Zones** – Pie chart showing each asset breakdown per asset **Zone per site**. Use the arrows to navigate to the other sites.
8. **Asset Breakdown: Subnets** – Pie chart showing each asset breakdown per asset **Subnet per site**. Use the arrows to navigate to the other sites.

> Note These Visibility breakdown widgets are not affected by the timeframe. Clicking on any portion of the pie chart leads you to the corresponding filtered Asset Page.

9. **OT Assets Distribution** – The breakdown of the OT assets per type (e.g. PLC, HMI, Engineering Station).
10. **IT Assets Distribution** – The breakdown of the IT assets per type (e.g. Endpoint, Printer, Networking) per site.
11. **IoT Assets Distribution** – The breakdown of the IoT assets per type (e.g. Camera, VOIP Phone) per site.
12. **Summary** – A count of OT Assets, OT Operations, and Write and Execute type OT Operations.
13. **OT Operations by type** – Breaks down the number of alerts for each type of OT operation.
14. **Latest OT Operation** – Lists the top 10 most recent OT asset alerts.

5.4 Assets

You can manage your asset inventory from the **Assets** page.

To access the **Assets** page, click **Visibility > Assets** from the main menu.

This page enables monitoring of network and asset information, activities, and statuses. You can view operational statistics, baseline details, and your asset inventory. You can follow the asset's alerts, activities, and statuses.

Any filters that you set apply to each viewing mode:

Table 2 Asset Views

Icon	Name	Description
	Layered Topology View	The Layered Topology View divides all assets into Purdue model levels, showing the connections between assets. The lines that connect the assets represent the communication between them.
	List view	The List View displays a customizable table of all assets, divided into configurable fields.
	Network graph	The Network Topology View visualizes all assets that are currently filtered and positions them by the communication between them. Assets that communicate with each other are shown closer together.

5.4.1 Asset Classes

An asset class indicates whether the asset is essentially an (IT) device, an OT device such as those in an industrial network, or an Internet of Things (IoT) asset. This property can be used throughout the system to distinguish between various types of assets, e.g. to create asset inventory filters, widgets, reports, and exports. TIV derives the Class from the communications or protocols used.

To view the asset Class column:

- Go to Assets page (see Figure 23).

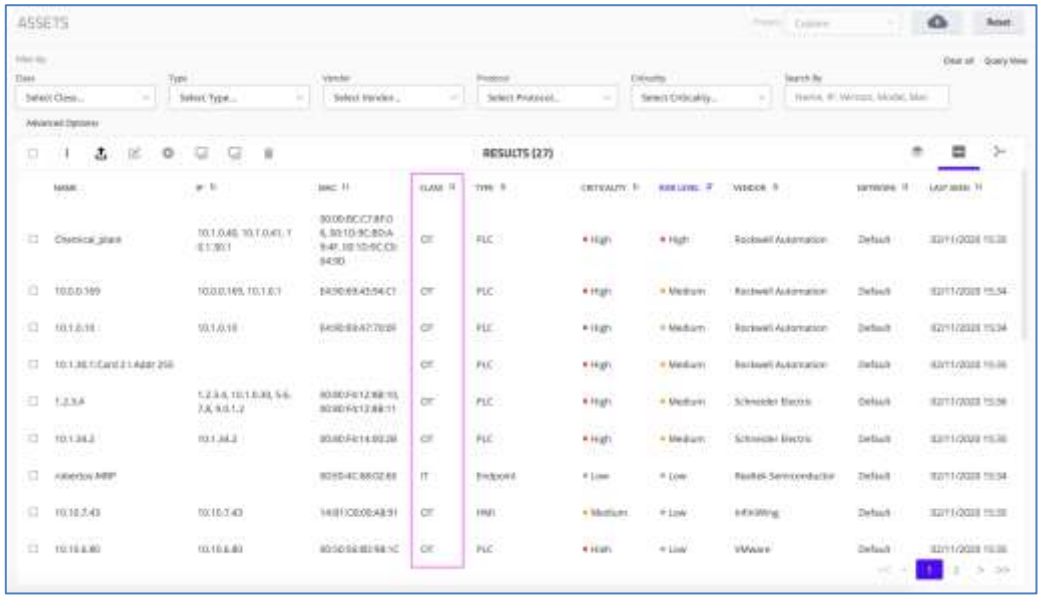


Figure 23 Asset Classes

5.4.2 Asset Types

TIV sniffs packets from the network, analyzes them, and extracts information using Deep Packet Inspection (DPI).

The following Device Types are identified from the traffic:

- PLCs
- HMIs
- Remote I/Os
- Engineering Stations
- OPC-Servers
- OTs
- Gateways

Some additional asset types TIV identifies include networking assets, printer assets, and endpoint assets. TIV determines an asset type to be a networking asset, extracted from the protocol dissectors, according to the asset's usage of the STP protocol. TIV determines the Printer asset type according to the specific SNMP queries performed on this asset. When no asset type can be readily identified, TIV classifies its asset type as an endpoint. TIV categorizes each asset as a specific type, which can be edited.

To see the asset types:

1. First go to the Assets View page.

2. Go to the Layered or Network graph views to see them listed in the Asset Type Legend  .

Table 3 Asset Types & Symbols

Access Control	Gateway	Printer
Access Point	GPS Device	Robot
Autonomous Vehicle	Historian	Router
Camera	HMI	RTU
Controller	IED	SCADA Client
Data Logger	Nested Devices/ Remote IO	SCADA Server
Domain Controller	Networking/Scan	Switch
Endpoint	OPC-Server	UPS
Engineering Station	OT	Video Recorder
File Server	PLC	VOIP Phone

Refer to the TIV Reference Guide for the full list of Supported Asset Types.

5.4.3 List View

To access the Assets List view:

- Navigate to **Visibility > Assets** in the Main Menu. The List view is displayed as follows:

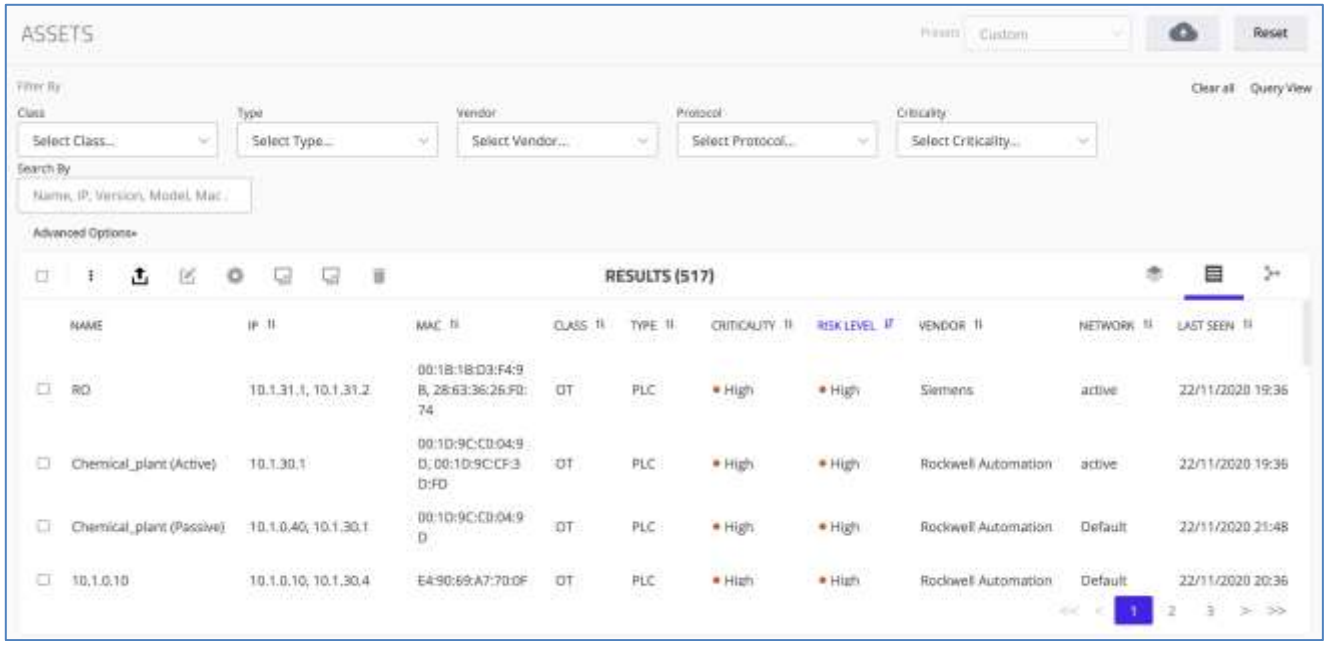


Figure 24 Assets - List View

The Assets table displays the following columns by default:

- **Name** – Asset name
- **IP –** IP address
- **MAC –** MAC address
- **Class** – IT, OT, or IoT
- **Type** – Endpoint, Broadcast, PLC, HMI, etc.
- **Criticality** – Low, Medium, or High. These values represent how critical the asset itself is to the operation. TIV assigns criticality automatically to certain types of assets but enables you to edit the value in the list and on the Asset Page.
- **Risk Level** – Calculated score of how much risk the asset poses to the system
- **Vendor –** Name of the equipment vendor
- **Network** – Network to which the asset belongs
- **Last Seen** – Date and time the asset was last detected

Additional columns, accessed through **More**  **> Select Columns**, include:

- **Active Queries** – Active Detection Queries associated with the asset
- **Discovered by** – Method used to discover the asset, such as Profinet scan, WMI ping
- Site – TIV site
- Address – Device address
- Hostname
- Purdue Level
- Operating System
- Firmware
- Model
- Virtual Zone
- Serial Number
- **Parsed Asset** – Indicates that the asset was imported by parsing configuration project files from App DB
- First Seen
- **Protocols** – Communication protocols used by the asset
- Vlan
- **Mode** – PLC operating mode

- **Tag** – Subnet tag associated with the asset
- **Subnet Type** – External, Internal, or Out of Scope
- **Custom Information** – Additional information about the asset
- **Display Name** – Alternate name given to asset after discovery

5.4.4 Layered Topology View

To access the assets' layered topology view:

- In List view, click the Layered Topology View button.

Figure 25 Asset View - Layered Topology

5.4.5 Network Topology View

The Network Topology View includes the connectivity between assets and communication directions.

To access the assets' network topology view:

- In List view, click the Layered Topology View button.

See below for an example of a filter applied in the **Network Topology**:

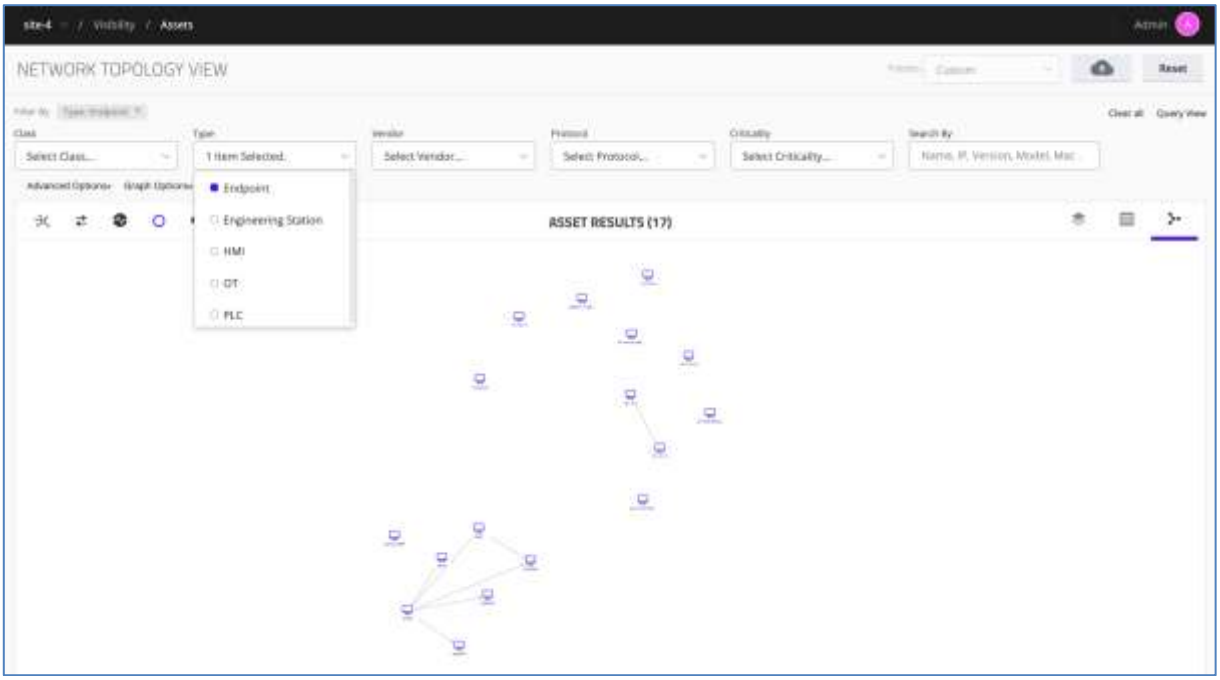


Figure 26 Asset View - Network Topology: Filtered for Endpoints

5.4.6 Asset Color By

The Asset Color By feature allows you to color the assets to see useful information at a glance. You can emphasize the most critical assets or highlight differences between subnets.

You can choose to color assets by: Type, Criticality, Risk level, New assets, Zone, VLAN, or Subnet.

To use Asset Color By:

1. In List view, click the Layered Topology or Network Topology button.
2. Click the **color assets by an attribute** icon and select the attribute from the dropdown menu.

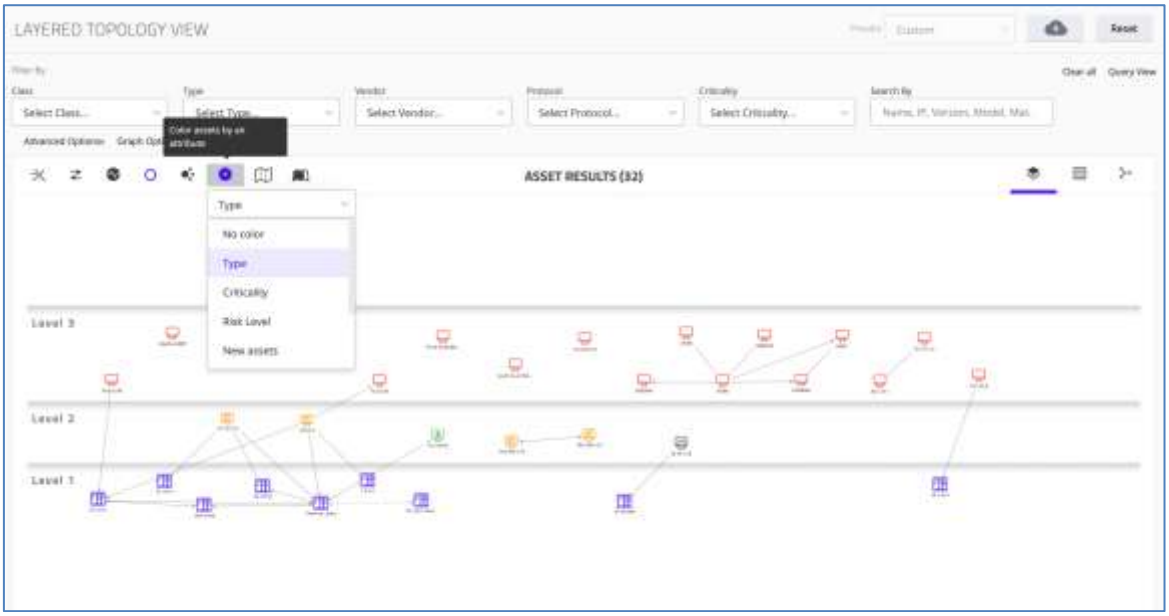


Figure 27: Asset Color by

5.4.7 Group By

All the assets are grouped by a selected attribute.

You can choose to group assets by:

- Type
- Criticality
- Risk level
- Vendor
- Tag
- Subnet
- VLAN
- Zone
- Discovered By

To use group by:

1. In List view, click the Layered Topology or Network Topology button.
2. Click the **group assets by an attribute** icon and select the attribute from the dropdown menu.

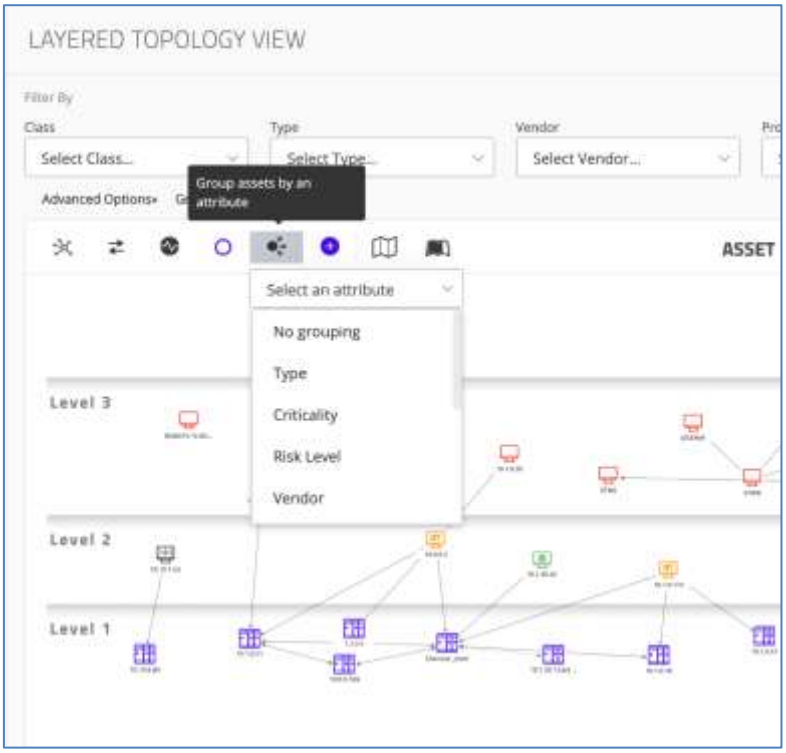


Figure 28: Group By

5.4.8 Showing Asset Neighbors

Asset Neighbors are two or more assets that communicate with one another.

You can use asset neighbors to understand communication patterns between groups of assets. For example, you might want to see with which assets HMIs are communicating or see the communication between assets with high criticality and their neighbors. You can even identify with which assets a specific asset is communicating by searching for it and viewing its neighbors.

To view Asset Neighbors:

1. In List view, click the Layered Topology or Network Topology button.
2. Apply filters as needed. For example, from the **Type** filter, select HMI.

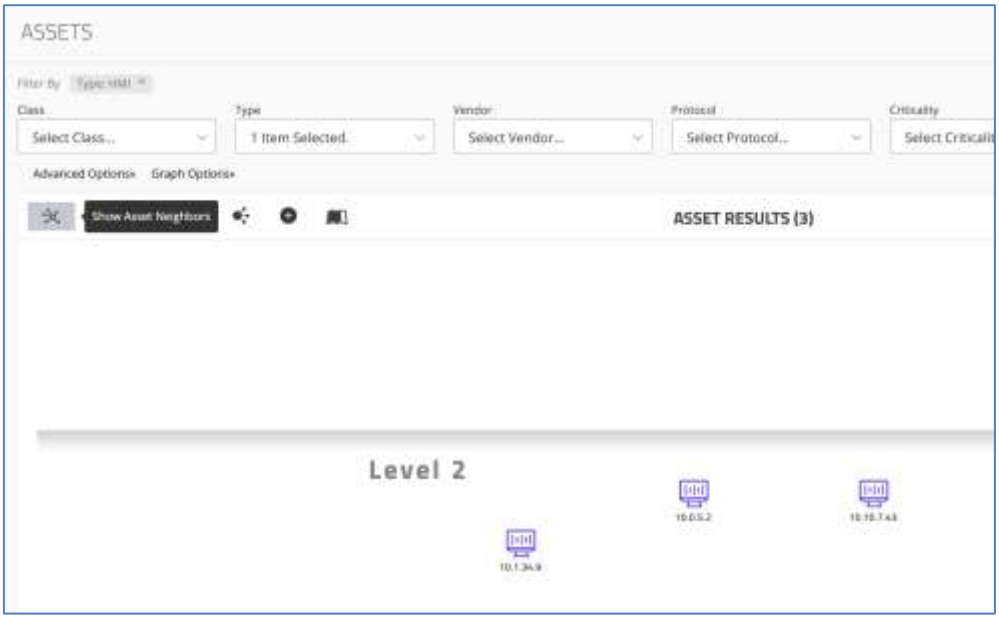


Figure 29: Assets - Layered Topology View, Filtered for Type HMI

3. In the toolbar, click **Show Asset Neighbors**  .

   The asset neighbors are shown.

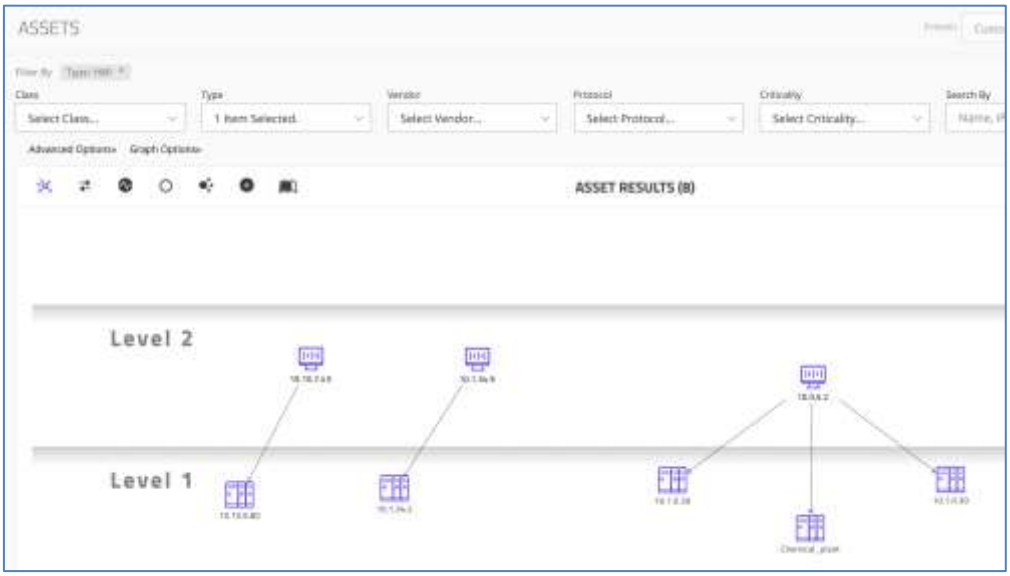


Figure 30: Assets - Layered Topology View, Showing All Neighbors of HMIs

5.5 Using Asset Filters

5.5.1 Using Basic Filters

To use basic filters:

1. First, go to the **Assets** page.
2. Use the following filters listed:
   - **Class** – Whether the asset is an OT, IT, or IoT device.
   - **Site** – (EMC only) The site to which the asset belongs.
   - **Type** – The asset type (Endpoint, Broadcast, PLC, HMI, etc.)
   - **Vendor** – The equipment vendor.
   - **Protocol** – The protocol in which the asset communicates.
   - **Criticality** – Low, Medium, or High. These values represent how critical the asset itself is to the operation. TIV assigns criticality automatically to certain types of assets but enables you to edit the value in the list and on the Asset Page.

Use the basic filters to manipulate the assets in the various viewing modes. You can search for a filter option in the dropdown lists:

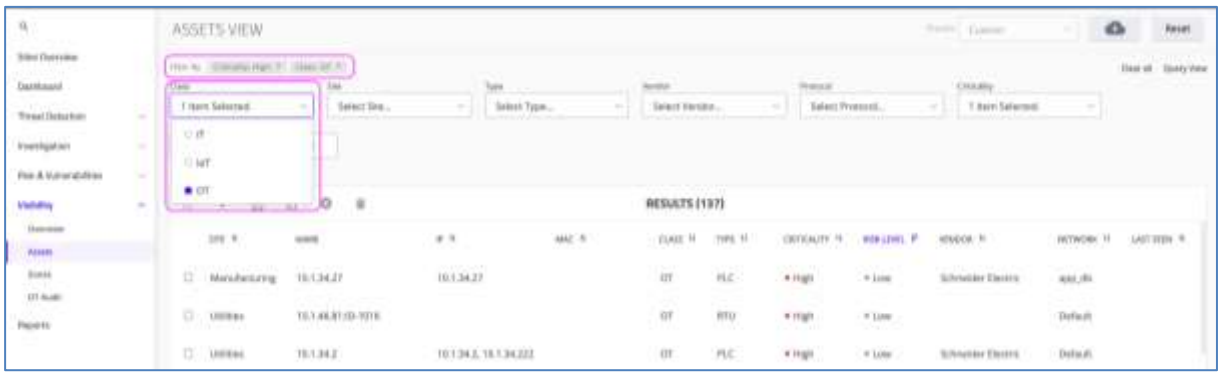


Figure 31 Basic Filters

- The OR filter contains either results.
- The AND filter must contain both results which is more restrictive.

5.5.2 Using Advanced Filters

To access advanced filters:

1. Go to the **Assets** page.
2. Click **Advanced Options** to access the Advanced Filters:

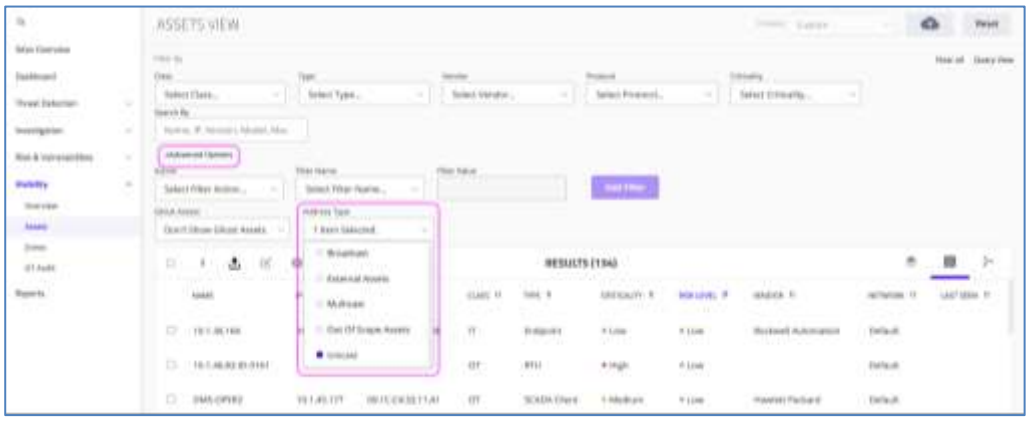


Figure 32 Advanced Filters

3. Select the required options from each of the dropdown lists.

   - Select the Search Attributes:

   - **Action** – The type of action (include or exclude).
   - **Filter Name/Filter Value** – The attribute by which you want to filter. For example, address, baseline, protocol, and so on.
     Some filters allow you to specify items in a free text field. This enables you to exclude a specific name, such as that of a certain vendor.
     Examples: Site, Virtual Zone, Primary Asset, Non-Primary Asset

   - Assets in TIV are classified into subnets of the following types:
     - **Address type** – Multi-select address filter; select from the following: Broadcast, External assets, Multicast, and/or Unicast.

Auto-Calculation of Subnets

TIV automatically calculates your subnets and classifies them as **Internal** or **External** as follows:

- **Internal** - Subnets that are in-scope for the system. This will automatically include all the subnets the system discovered using the TIV software. By default, every subnet that we see its Broadcast domain / Internal Subnets / OT traffic from or to it is classified as internal. In addition, you will be able to manually add new subnets and classify them as Internal.
- **External** – Subnets that are external to the customer sites. Usually internet subnets. Those subnets are not part of the client network and can be considered as external subnets. By default, any subnets that will not be classified as Internal subnets will be classified as External. You can manually add new subnets and classify them as External.

- **Out-of-Scope** –Subnets that are included in the environment but are not part of the Internal or External network. Classifying subnets as Out-Of-Scope can only be done manually as detailed in section 10.4.1.

While you are in Training mode you can choose to **Approve** these subnets so they will be validated after the system moves to Operational Mode.

> Note After you upgrade your system, all remote subnets will be classified as Internal

- **Ghost Assets** – Displays "ghost assets", i.e. assets that process assets attempted to communicate with, seen on the SPAN, but the target asset did not respond. These assets could be the result of a misconfiguration or indicate a security problem.
  - **Don't Show Ghost Assets** – This is the default
  - **Only Show Ghost Assets** – Display only ghost assets in the asset table
  - **Show Ghost Assets** – Include ghost assets in the asset table
- **ARP Baselines** – This attribute is only relevant for graph views:

Figure 33 Advanced Filters

4. Click **Add Filter** to apply each filter and repeat the process for as many filters as needed.

5.5.3 Advanced Graph Filter Options

The advanced **Graph Filter** options only appear when you are in **Layer** or **Network Graph** view mode. The graph filters apply to the asset communications while the other filters are on the nodes. Use these fields to create sophisticated queries by choosing various filter names and whether to include or exclude selected data. To access the advanced graph filter options, follow the steps below.

1. In the **Assets** page, click Layered Graph or Network Graph.
2. Click the **Graph Options** on the top right:
   - ♦ A new set of filters fields is added:
     - Action
     - Filter Name
     - Filter Value

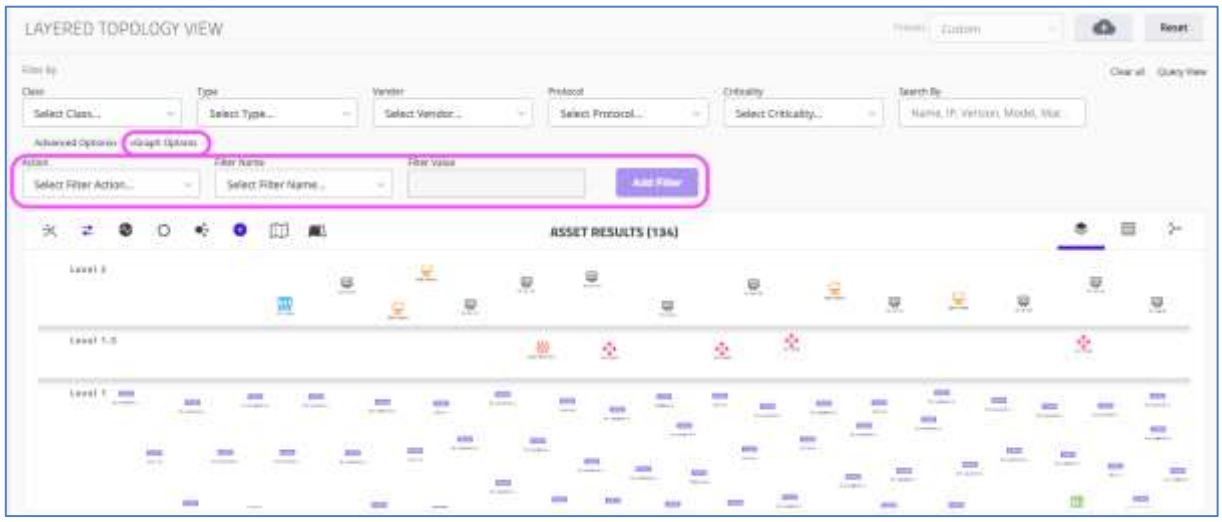


Figure 34 Layered Graph - Graph Options

3. Add multiple filters via 'AND' for a more complex query.
   - ♦ The graph will show assets that apply to all filters.

5.5.4 Searching for an Asset

- Search for a specific asset by name, IP, or MAC address in the **Search by** field.

> Note To search for a specific address, specify the address in quotation marks. Otherwise, the results will be any asset that **contains** the entered value.

5.5.5 Creating Predefined Filters (Presets)

You can save your preferred asset filters, search criteria, and selected advanced options as a **Preset** view that can be easily accessed later.

> Note Presets are deleted when a system reset is performed.

1. Set up your filters, search criteria and selected Advanced Options with the preferences that you use frequently and want to save between sessions.
2. Click the **Preset** button in upper right corner of the screen:

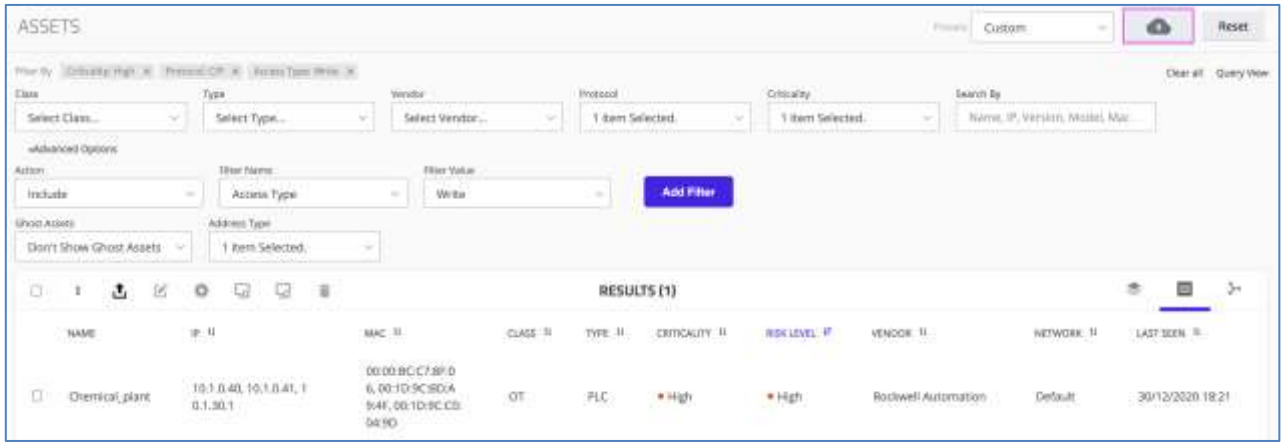


Figure 35 Filtering Presets

3. Name your Preset filter and click **Save**.

Figure 36 Save Preset

4. To change your Preset preferences, click **Reset**.
5. Select **<< Advanced Options** to revert to the basic Filter page.

5.5.5.1 Clearing Filters

- To clear all filtering, click **Clear All**.

Figure 37 Clearing filtering

5.6 Editing Assets

Assets can be edited individually and in bulk.

5.6.1 Editing Individual Assets

To edit individual assets:

1. Go to the **Assets** page.
2. Select the checkbox on the left side of the row of the asset:

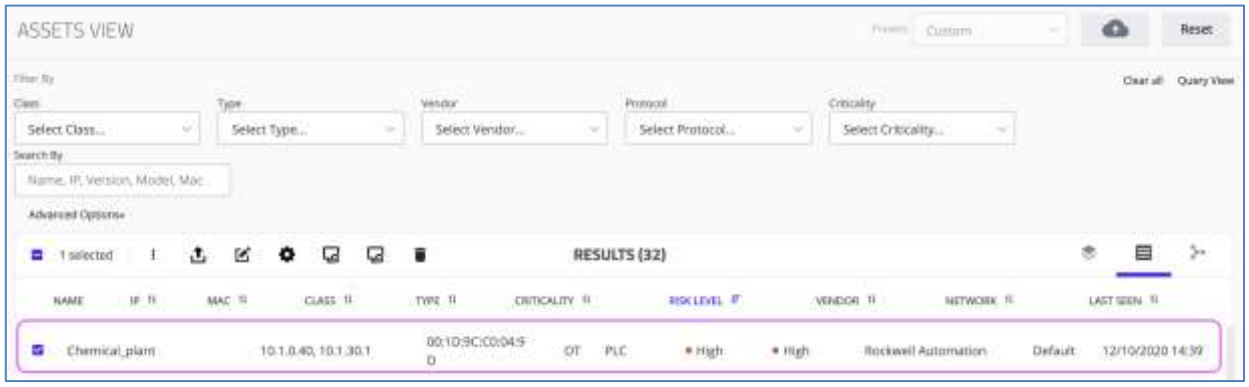


Figure 38 Selecting an Asset on the Asset Page

3. Click the **Edit Asset** button from the **toolbar**:

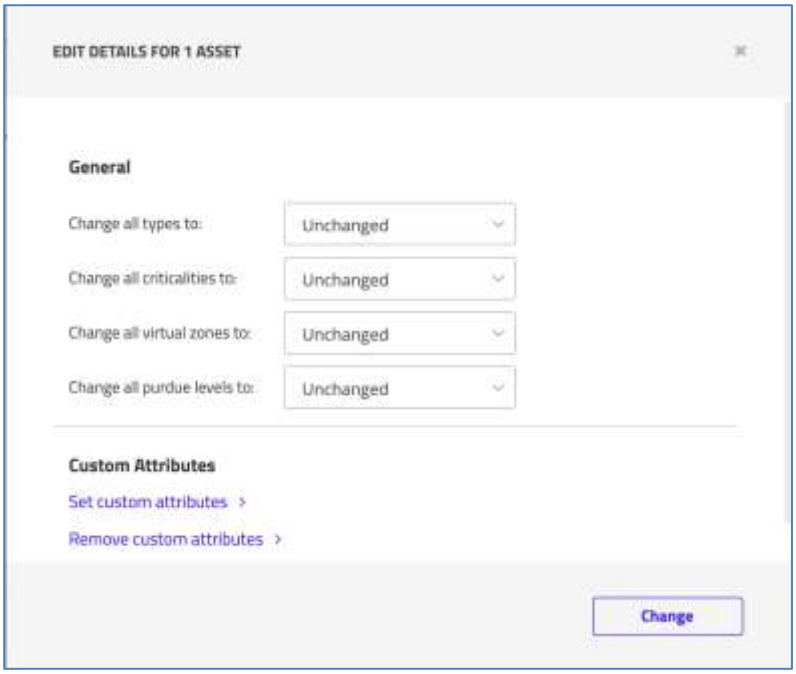


Figure 39 Edit Asset Details popup

5.6.2 Editing Assets in Bulk

1. Select multiple rows of assets of interest:

Figure 40 Bulk Asset Modification

2. After selecting numerous assets, select the **Edit** button  .
3. Choose the **Types**, **Criticalities**, **Virtual Zones** and/or **Purdue Levels** to modify for the selected assets, and click **Change**:

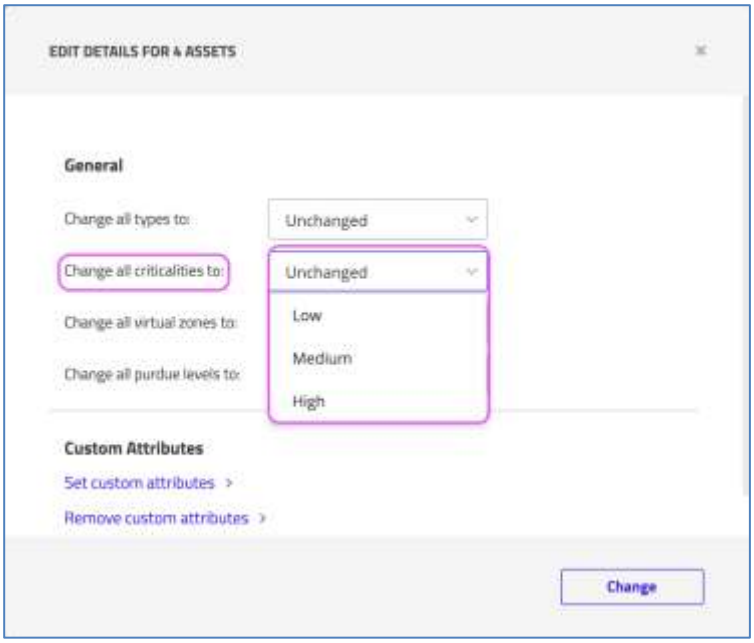


Figure 41 Edit Details - Bulk Change

> Note After changing the Criticality of all the assets through a bulk Criticality change, the system will no longer attempt to automatically assign a Criticality value to these assets.

5.7 Detailed Asset Page

To access the detailed asset page:

1. In the Main Menu, navigate to **Visibility > Assets.**
2. Click on the desired asset from the **Assets** table.

An example of a detailed asset page is shown below.

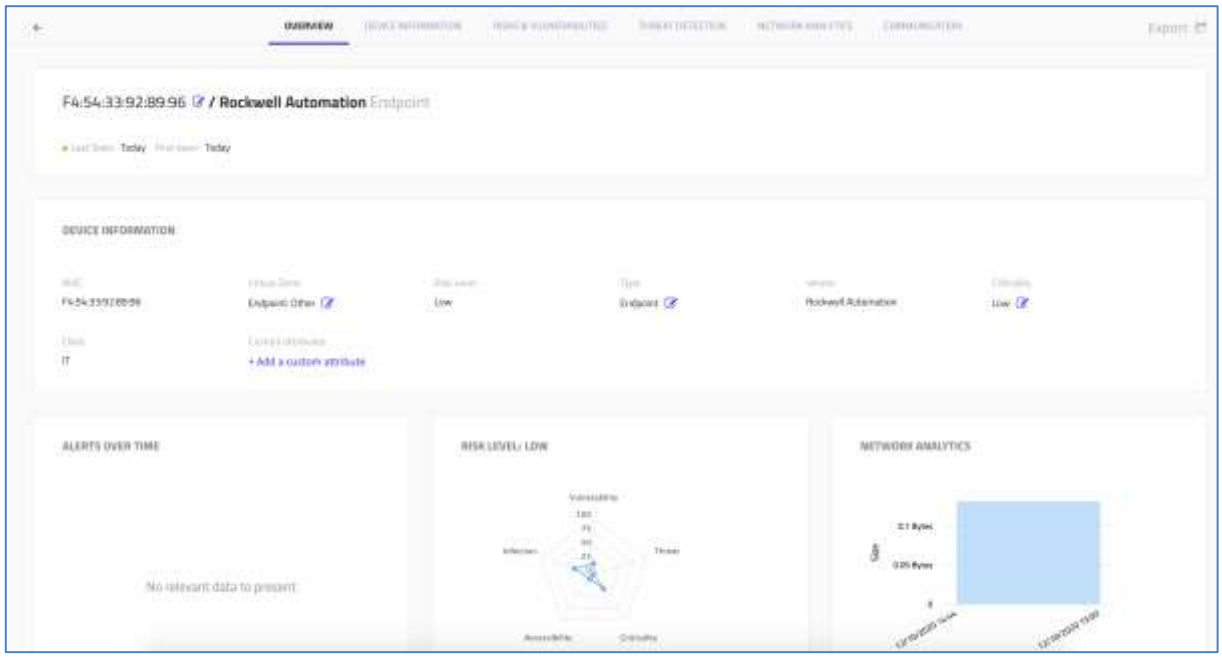


Figure 42 Detailed Asset Page - Overview

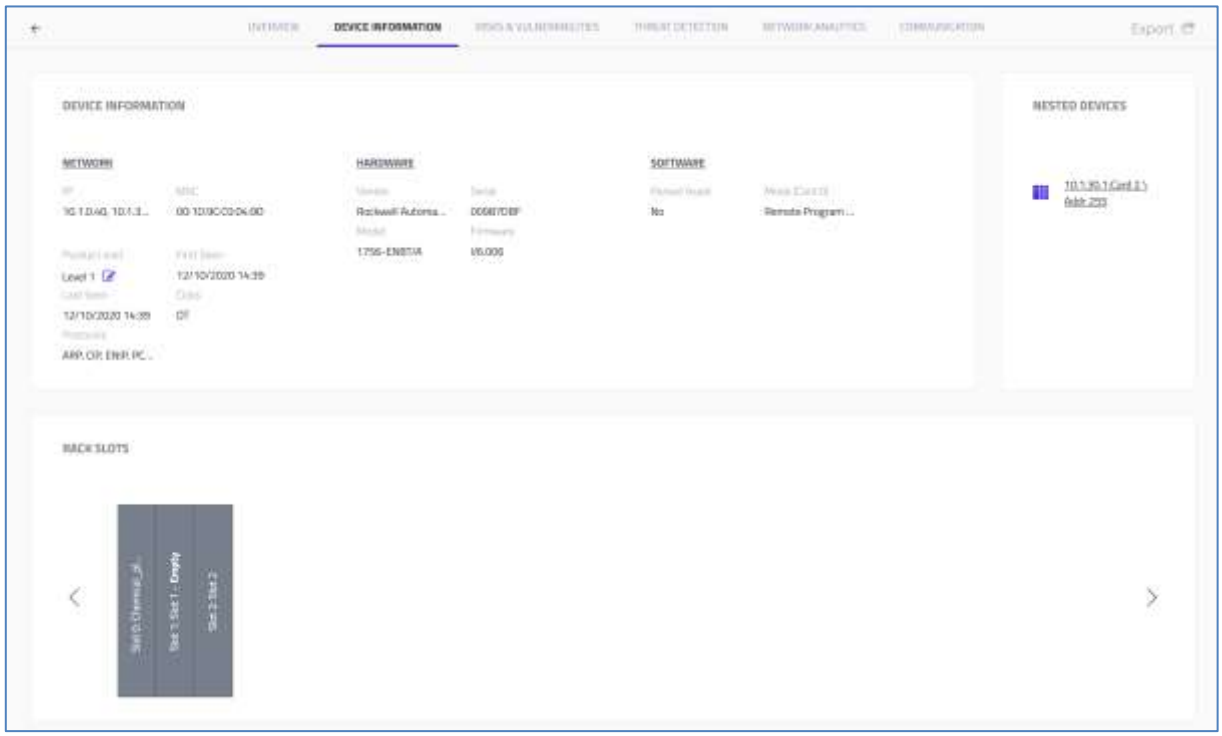


Figure 43 Detailed Asset Page - Device Information

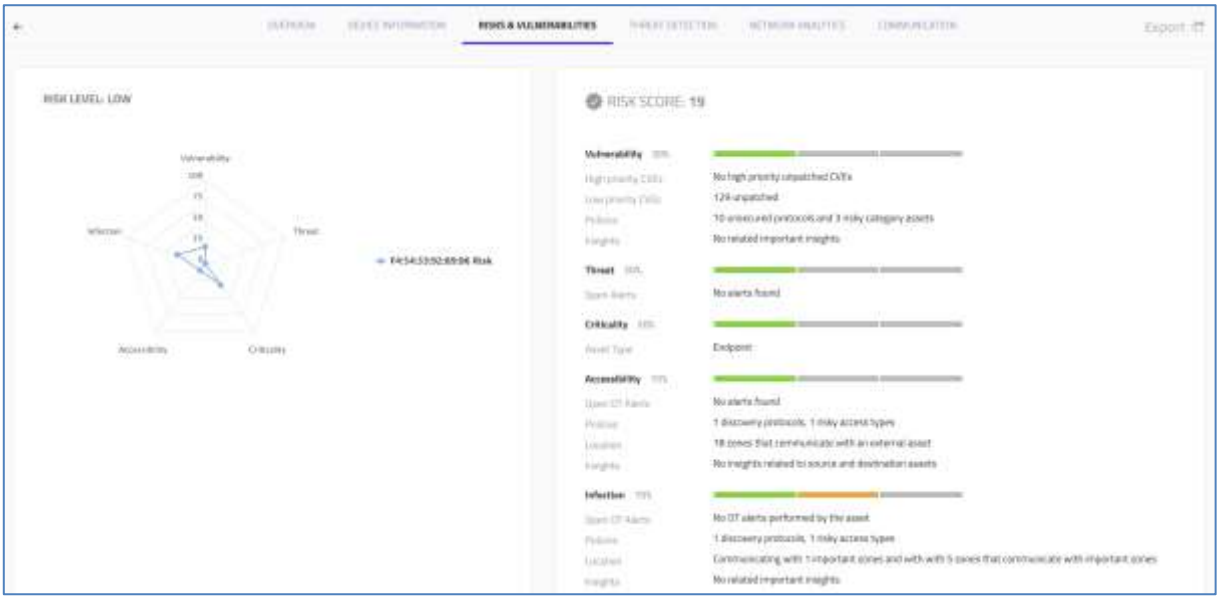


Figure 44 Detailed Asset Page - Risk & Vulnerabilities

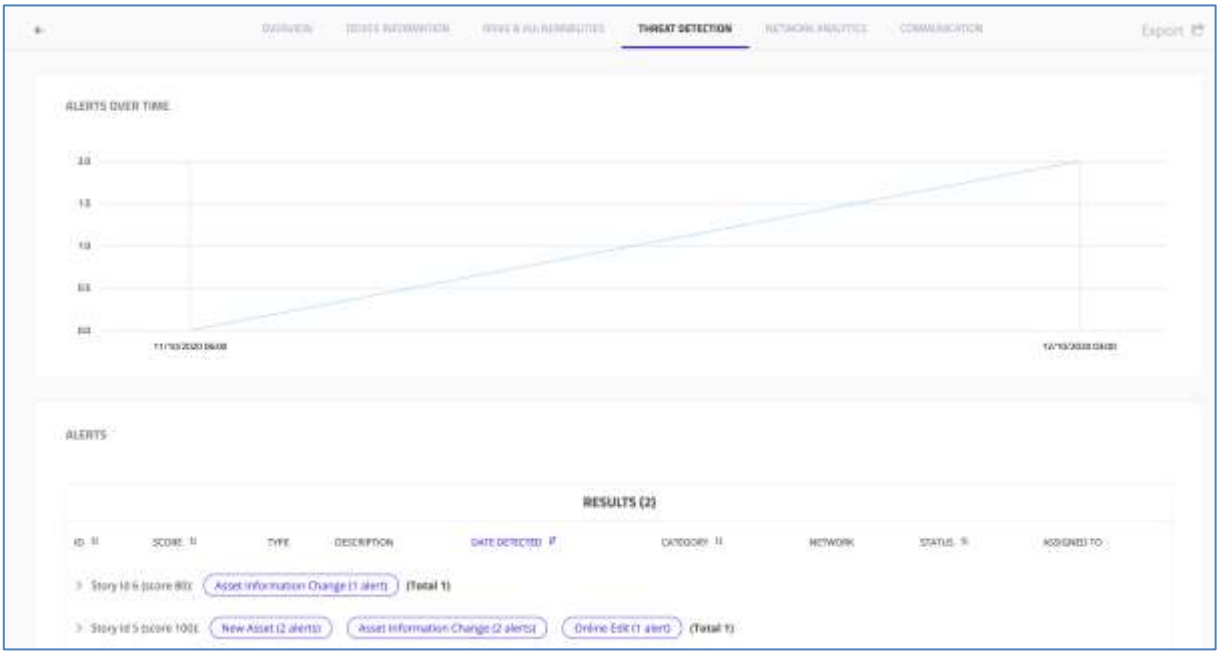


Figure 45 Detailed Asset Page - Threat Detection

Figure 46 Detailed Asset Page - Network Analytics

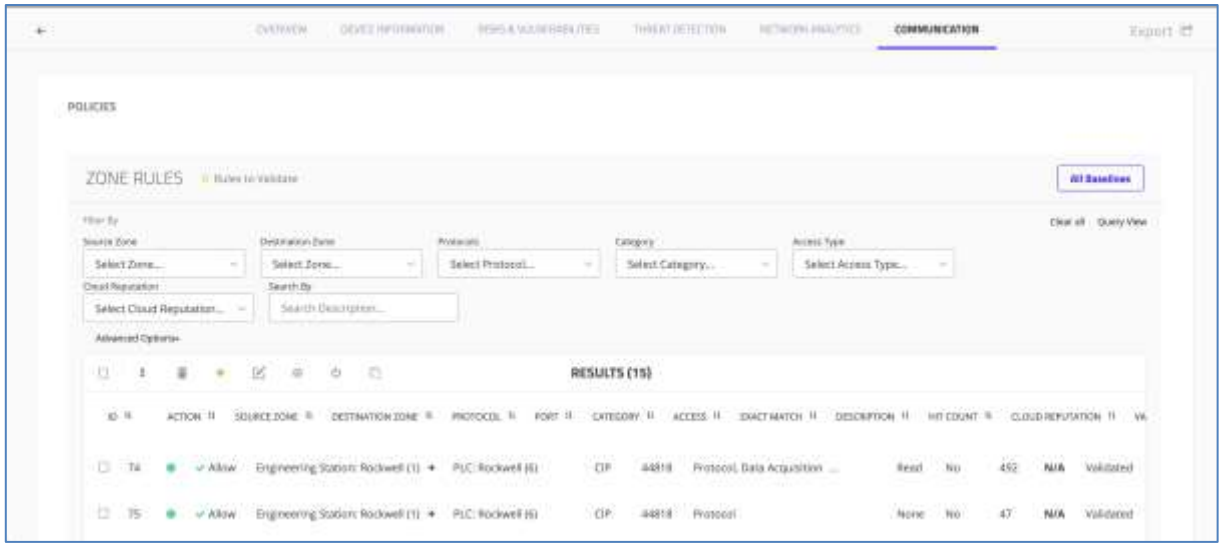


Figure 47 Detailed Asset Page - Communication

5.7.1 Physical Connections

The Detailed Asset Page provides information about physical connections between assets. A **Physical Connection** area in the Asset page displays any existing physical connection or switch. The switch is gathered via SNMP protocol.

To access the Physical Connection area:

1. In the **Assets** page, click the desired asset to open its detailed asset page.
2. Click the **Device Information** tab.

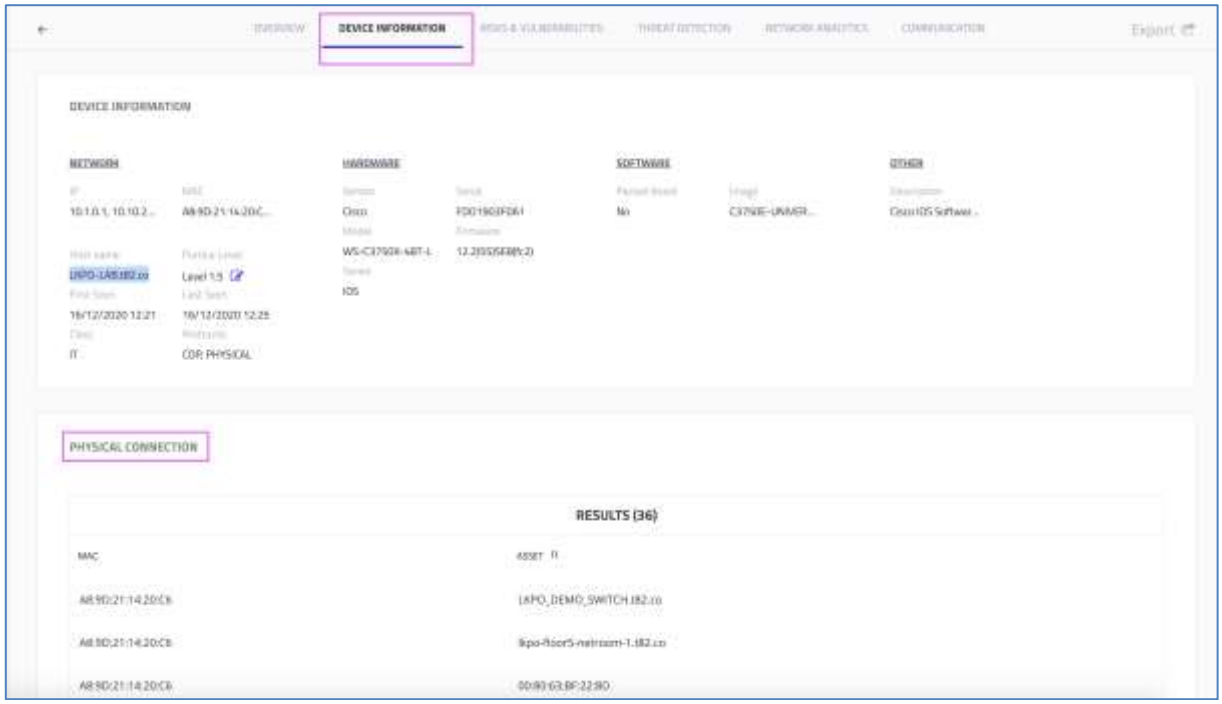


Figure 48 Asset Page: Physical Connection in the Device Information Tab

In this example, Asset *LKPO-LAB.t82.co* has Physical Connections. The table lists all the assets physically connected to the asset.

5.7.2 Changing Purdue Model Levels

The Layered Graph view features a Purdue model graph, displaying the assets according to their Purdue model layers. The changing of an asset Purdue level also is reflected in the Purdue Level of the Virtual Zone the assets exist in.

Users can change the Purdue model level defined for a specific asset manually. Generally, the Purdue model level for a specific asset is automatically determined based on the various characteristics of the asset and its purpose. Sometimes the automatically determined level needs to be adjusted to reflect the true asset behavior. This can be useful in cases where the system has placed the asset in a level that does not properly describe its criticality. Note that interim Purdue levels can also be applied, e.g. 1.5, 2.5, 3.5.

To change the Purdue model levels:

1. Navigate to the detailed asset page.
2. Click **Device Information**.
3. Click **Edit** for the Purdue Level and choose the desired level.
4. Click the check mark.

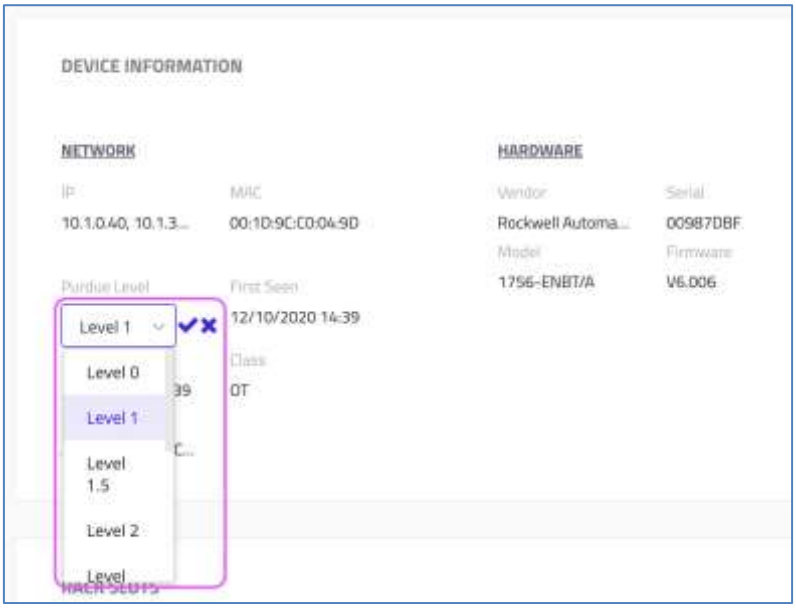


Figure 49 Changing an Asset's Purdue Level

5.7.3 Risk Score Widgets

The risk score widgets give a score on the risk level parameters. They provide a calculation showing the parameter's effect on the score. These widgets can help you to reduce risks on the asset/zone, by being aware of the vulnerabilities and resolving them.

To access the risk score widgets:

1. Navigate to **Visibility > Assets** in the Main Menu and click on an asset.
2. Click the **Risk & Vulnerabilities** tab.

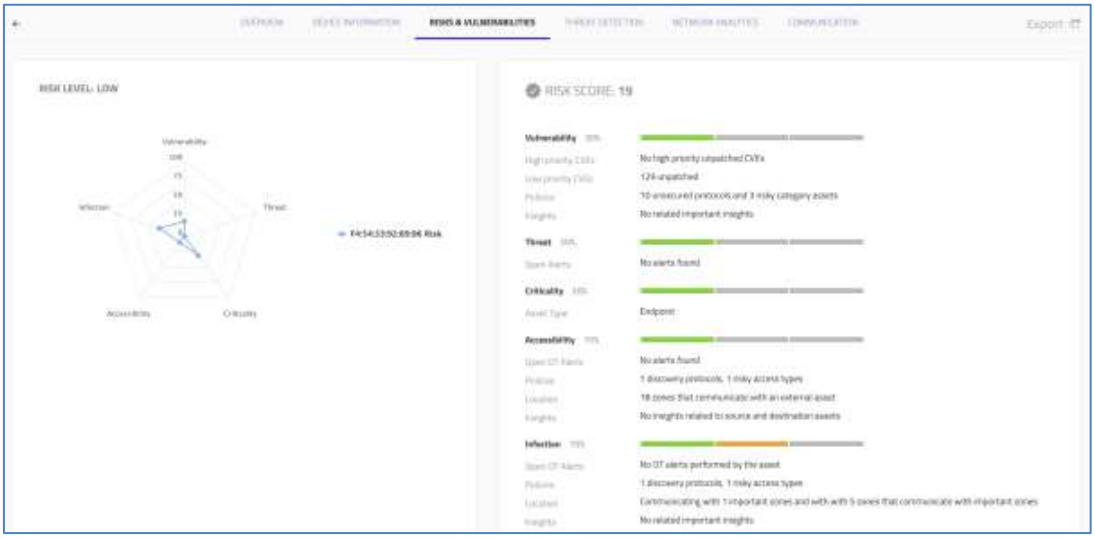


Figure 50: Risk Score Widgets

5.7.4 Network Communication Map

The network communication map shows the communication to and from the asset, the subnet, protocol, zone, and the asset it communicates with. The width of the lines represents the flow of the most bandwidth for a protocol.

To access the network communication map:

1. Navigate to **Visibility > Assets** in the Main Menu and click on an asset.
2. Navigate to **Network Analytics > Network Communication Map**.

Figure 51: Network Communication Map

The network communication map displays:

- Internal or external subnets
- Protocol
- Talking with destination assets

Effects of clicking on the network communication map:

- On hover – you see the bandwidth for each protocol.

The system shows up to 10 connected assets or protocols with an option to click load more. There is an option to filter the assets that communicate by clicking To or From. You can also filter by time frame.

5.7.5 Cross Site Correlations

When operating on a large-enterprise network, the EMC is required to act as a single point of truth where information from sites will be correlated and shown without duplications. Users handling asset inventory and alerts in the EMC need a coherent image of the entire network, regardless of how different sites capture their network behavior and inventory.

This Cross-Site Correlation behaves as follows:

- Only Internal assets are shown in the EMC

- For each asset, a user can see a list of “correlated assets” from different sites where the associated asset appears in subnets that are defined as "external" or "out of scope".

The table can be accessed through the **Device Information** tab of the **Asset View** page.

Figure 52 Correlated Assets

5.8 Custom Attributes

TIV offers the ability to add asset Custom Attributes for internal information that cannot be detected directly from the network traffic.

The attributes are available for use throughout the system in the same manner as the built-in fields, providing you with a tool for applying custom criteria to manage asset inventories more effectively.

Custom attributes can be shared on multiple sites and can be viewed from the EMC or the Site level.

The attributes are included in CSV import and export of assets.

The Admin sets up the Custom Attributes and can modify or remove them, as described in section 5.8.5.

5.8.1 Displaying Custom Attributes in the Assets Page

The Assets page enables you to apply custom attributes to both individual assets and groups of assets. In order for custom attributes to display in the Assets page along with the built-in data, you must add a column to the Assets page table for each custom attribute to be used.

- To display custom attributes in the Assets page:

1. In the Main Menu navigate to **Visibility > Assets**.
2. In the toolbar, click the **More**  icon and then click **Select Columns**.
3. In the Select Columns dialog, select the custom attributes to be displayed in the table.

Figure 53 Choosing Custom Attributes - Asset Page Column Selector

4. Click **Apply**.

   - The columns with the custom attributes you chose are added to the right side of the table.

Figure 54 Custom Attributes Added to Asset List

5.8.2 Applying Custom Attributes in the Detailed Asset Page

To apply a custom attribute to an asset directly in its Detailed Asset page:

1. Click the +Add a custom attribute link.
2. Select a custom attribute from the drop-down list and then add a value.

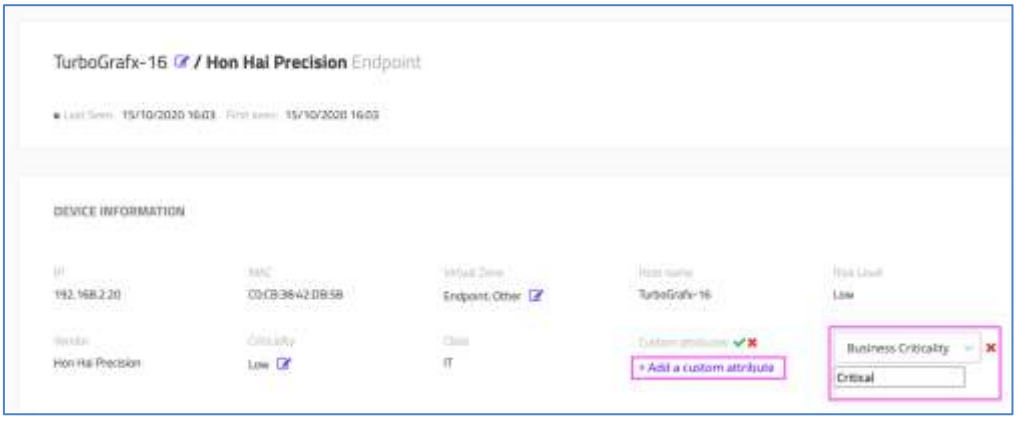


Figure 55 Choosing a Custom Attribute in the Asset Page

3. Click the checkmark next to the Custom Attributes heading to save your selection.

Figure 56 Saving a Custom Attribute in the Asset Page

5.8.3 Applying Custom Attributes to Multiple Assets

In the Assets page you can choose several assets and apply custom attributes as follows:

1. Select the relevant row/s of assets and click the **Edit Assets** icon in the toolbar.

Figure 57 Bulk Editing of Custom Attributes - Selecting Assets

- The **Edit details** dialog is displayed:

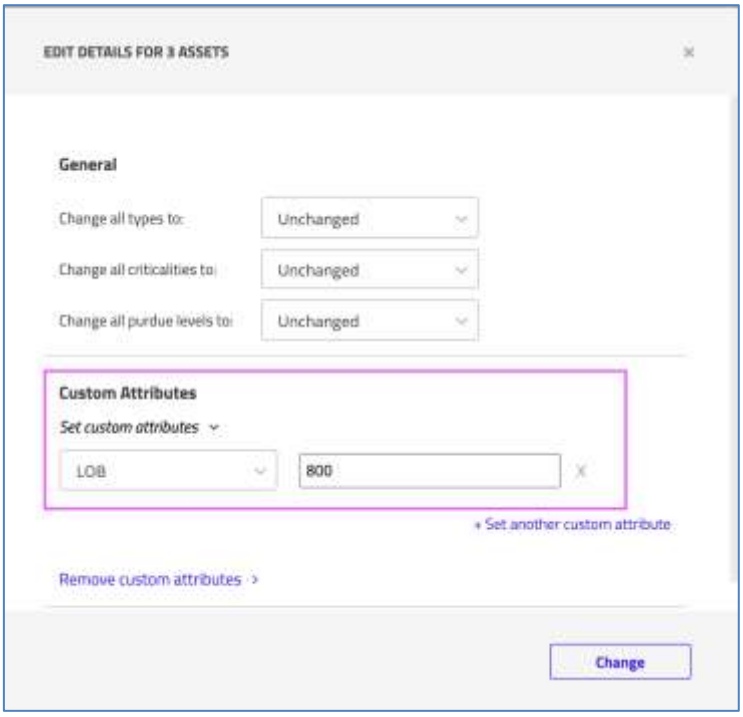


Figure 58 Dialog for Bulk Editing of Custom Attributes

2. In the **Custom Attributes** subsection of the dialog, click the **Set custom attributes** link Set custom attributes to open the custom attribute list.
3. Select a custom attribute from the drop-down list and enter a value for the custom attribute.
4. To apply another custom attribute to the selected asset(s), click **+Set another custom attribute** + Set another custom attribute and then set values.
5. To remove the custom attribute(s) just applied, click the X next to the attribute.
6. Click **Change**.

5.8.4 Removing Custom Attributes from Multiple Assets

Custom Attributes can be removed from one or more assets in the Assets list as follows:

1. Select the relevant row/s of assets from which you want to remove a custom attribute. Then click the **Edit Assets** icon in the toolbar.
2. In the Custom Attributes section of the dialog, click the **Remove custom attributes** link.

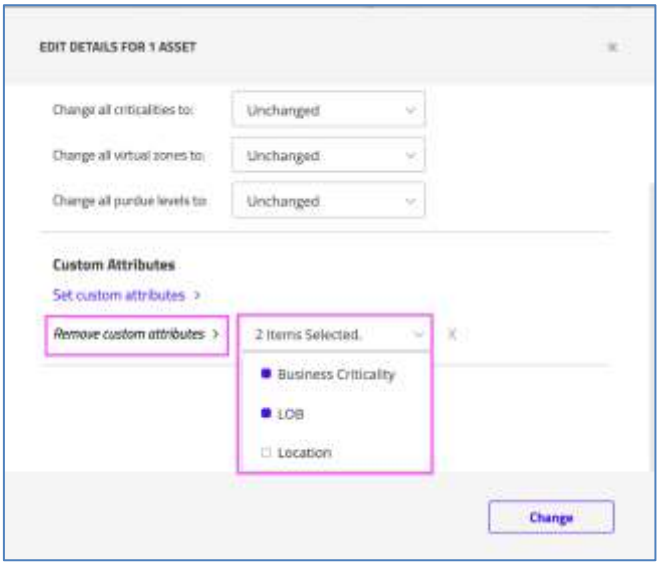


Figure 59 Remove Custom Attributes

3. Select the custom attributes to be removed from the assets.
4. Click **Change**.

5.8.5 Setting Up Custom Attributes

Custom Attributes can be created from either the Site or the EMC. Because all Custom Attributes created on a specific site also appear in the EMC, they can be easily shared with other sites as needed.

All Custom Attributes with the same name are assumed to be identical.

For information about applying custom attributes to assets, see Section 5.7.51

5.8.5.1 Adding Custom Attributes to a Site

To add a Custom Attributes to a site:

1. Navigate to **Settings** > **Management** > **General** and click the Custom Attributes tab:

Figure 60 Custom Attributes Tab

2. Click Create new .
3. Provide the following input in the **Add Custom Attribute** dialog:

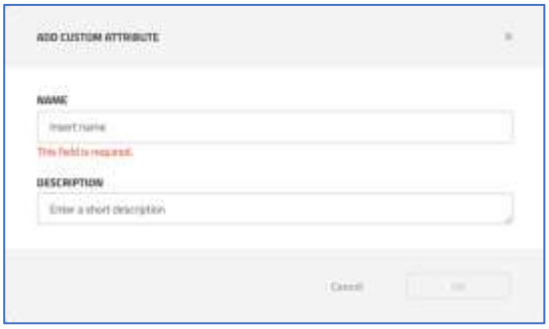


Figure 61 Custom Attributes Dialog

- **Name** — Enter the name of the attribute you are adding (this is a mandatory field).
- **Description** — Add a description for clarification. This description only appears the Custom Attributes tab.

4. Click **OK** to save the new attribute or **Cancel** to revert to the prior setup.
   - After the Attribute is added to the system, a new row appears on the tab with its Name, Description (if applied), and an Action column (see Figure 60).
5. Click **Edit** on the row of any Custom Attribute that you want to modify.

5.8.5.2 Adding Custom Attributes to Multiple Sites from the EMC

To add custom attributes to multiple sites from the EMC:

1. Navigate to **Settings** > **Management** > **General** and click the Custom Attributes tab:

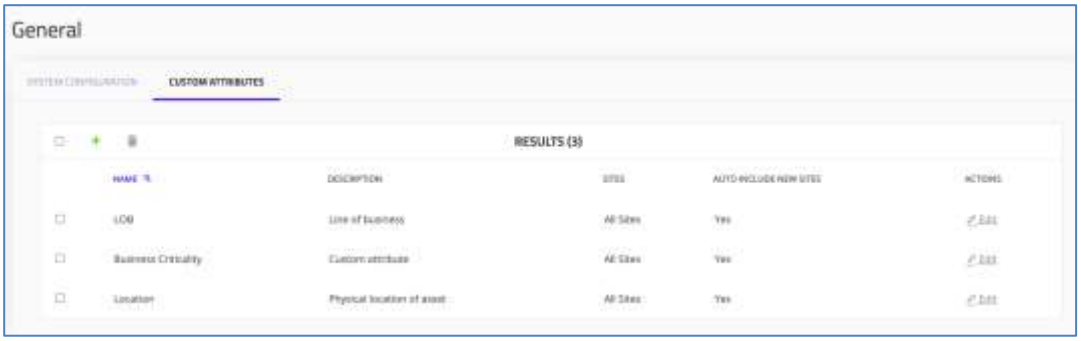


Figure 62 Custom Attributes Tab

2. Click Create new .
3. Provide the following input in the **Add Custom Attribute** dialog:

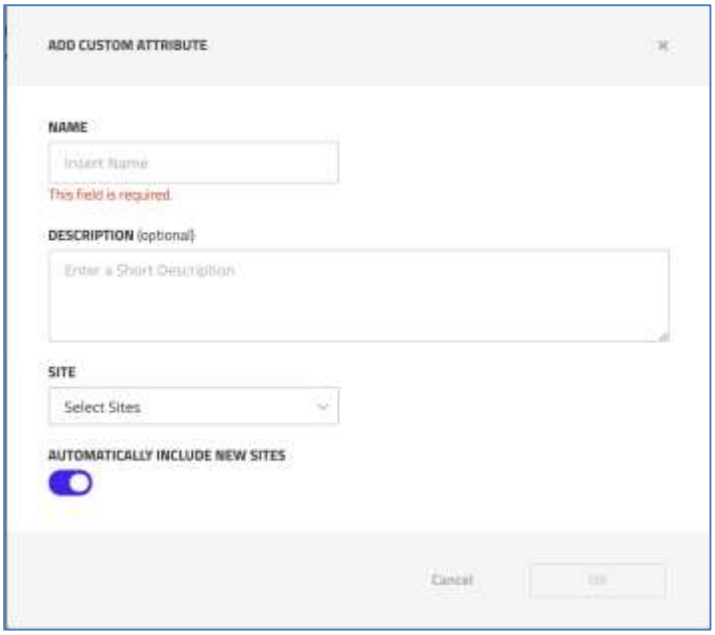


Figure 63 Add Custom Attribute Dialog - EMC

- **Name** — Enter the name of the attribute you are adding (this is a mandatory field).
- **Description** — Add a description for clarification that is useful across multiple sites. This description only appears in the Custom Attributes tab.
- **Site** – Select the sites to which the custom attribute should apply from the drop-down list.
- **Automatically Include New Sites** – Slide to the right to apply the custom attribute to new sites added to the enterprise.

4. Click **OK** to save the new attribute or **Cancel** to revert to the prior setup.

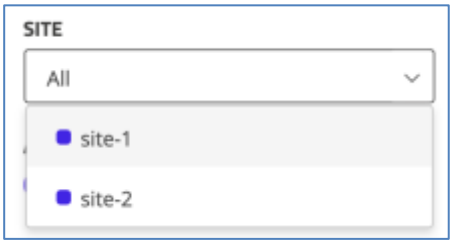
5.8.5.3 Applying a Custom Attribute Created on One Site to Another Site via the EMC

You might want to use a custom attribute created for one site on another site. For example, you might create a Warranty Expiration Date custom attribute for Site 1 and later decide to use it on Site 2 as well.

To apply a custom attribute created for one site to another site:

1. Click the **Edit** 

icon of the custom attribute you want to apply to another site.
2. In the **Site** drop-down list of the **Add Custom Attribute Dialog** (Figure 63), select the site to which you want to apply the custom attribute.



3. Click **OK**.

> **Note:** TIV recognizes that custom attributes with the same name from different sites are identical, so the name will only appear once in the Site drop-down list.

5.8.6 Exporting Assets with Custom Attributes

When exporting assets to a CSV file, any custom attributes that appear in the grid are automatically included in the export. When exporting to a PDF format, all custom attributes appear in a single cell separated by a column.

To export these assets, click the download icon in the toolbar.

5.8.7 CSV Imports with Custom Attributes

When importing assets from a CSV file, attributes not assigned should be left empty.

5.8.8 CSV Importing - Merging and Splitting Assets

Note that when two assets with the same custom attribute are automatically merged, the custom attributes are unified. If both have the same custom attribute

both values appear, separated by a comma. Similarly, when assets are split, each split asset obtains both values until revised by the user.

5.9 Import CSV (Optional) [Only Admins]

TIV provides an asset inventory capability that enables Administrators to manually onboard assets from a CSV file. This Import Assets feature is valuable for Administrators that want to perform bulk onboarding of assets manually or to perform bulk changes to their Asset Inventory, such as changing their asset names.

The process starts with an export of asset information with the relevant columns included. Then, select a CSV file that contains one or more assets. After the CSV is selected for import, the system parses it and starts analyzing all the information from the input file. The system notifies the Administrator of the summary results, reporting how effective the import was, while providing information on any rows of data that were not imported successfully.

Note that while an asset is being successfully onboarded, several seconds may elapse while the system is validating the data from the queue before the asset is accessible from the UI. The Importing Assets feature is available for users with Administrator privileges. For full detailed instructions refer to the **TIV Reference Guide: Importing Assets via CSV**.

For **IoT Matchers**, see section 11.5.

5.10 Zones

When in training mode, the system automatically allocates discovered assets into Zones, based on the assets' type and communication patterns. The communication links between zones are known as conduits. These zones and conduits are detailed in ISA/IEC-62443.

5.10.1 Zone Behavior

By default, Zones are groups of logically related assets. When in training mode (or when new assets are approved during operational mode), the system creates Zones according to the discovered asset types and their learned communication patterns.

Zones can also be edited, modified, or created manually to match a specific network segmentation defined by the end user.

By design, a Zone represents a group of assets that are similar or related in the type of function they serve within the OT network such as a PLC, HMI, or Engineering Station Endpoint, the other groups of assets they communicate with, and their profile of communication patterns.

As such, Zones serve as a segmentation and micro-segmentation design tool by providing users with a real view of how their network is logically segmented. They also offer a good base of understanding of what may be required to segment it properly and securely.

TIV's Zone Rules are based on Zone grouping and segmentation to define a security detection policy system. With its firewall-like management page, Zone Rules allow the user to review, modify, and validate system-generated policy rules. Zone Rules identify which traffic is allowed within and between Zones and should be alerted on.

This section focuses on the Zones and their management. Zone Rules are covered in section 5.10.77.5.

5.10.2 Creating Zones

Zones graphically display the communication between OT and IoT zones, and visualizations of inter-zone communications also known as conduits. These Zones are calculated automatically both in training and in operational mode. After a new asset is discovered or information is changed, the system calculates to which zone it should be assigned or creates a new virtual zone if a relevant one does not exist.

TIV's vast and growing range of firewall integrations enable users to enforce network segmentation policy violations by identifying and restricting anomalous or non-compliant communications across zones.

- The system calculates the optimal zones that will be used, and automatically creates them. Learned or approved assets are assigned to the most appropriate virtual zone.
- The system automatically creates rules that define the allowed or alerted communication within and between zones.
- You can modify the zone where the asset was assigned. Use the **Assets** page or use bulk editing (see section 5.6.2).

5.10.3 Zone Graph Views

There are two views to display the zones graphically: Layered Topology View  and Network Topology View  .

To view the zone graph views:

- Open the Zone list by clicking **Visibility > Zones** from the main menu. Then click on either layered or network graph.

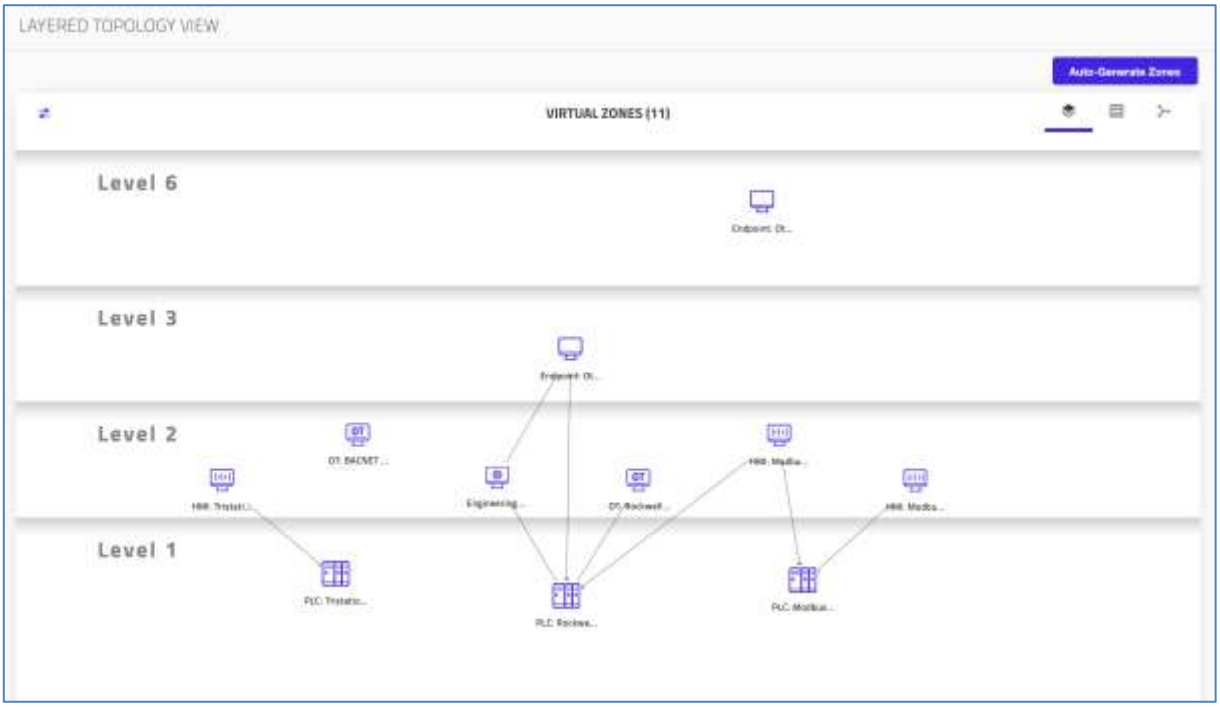


Figure 64 Layered Topology View of Zones

5.10.3.1 Zones - Network Topology View

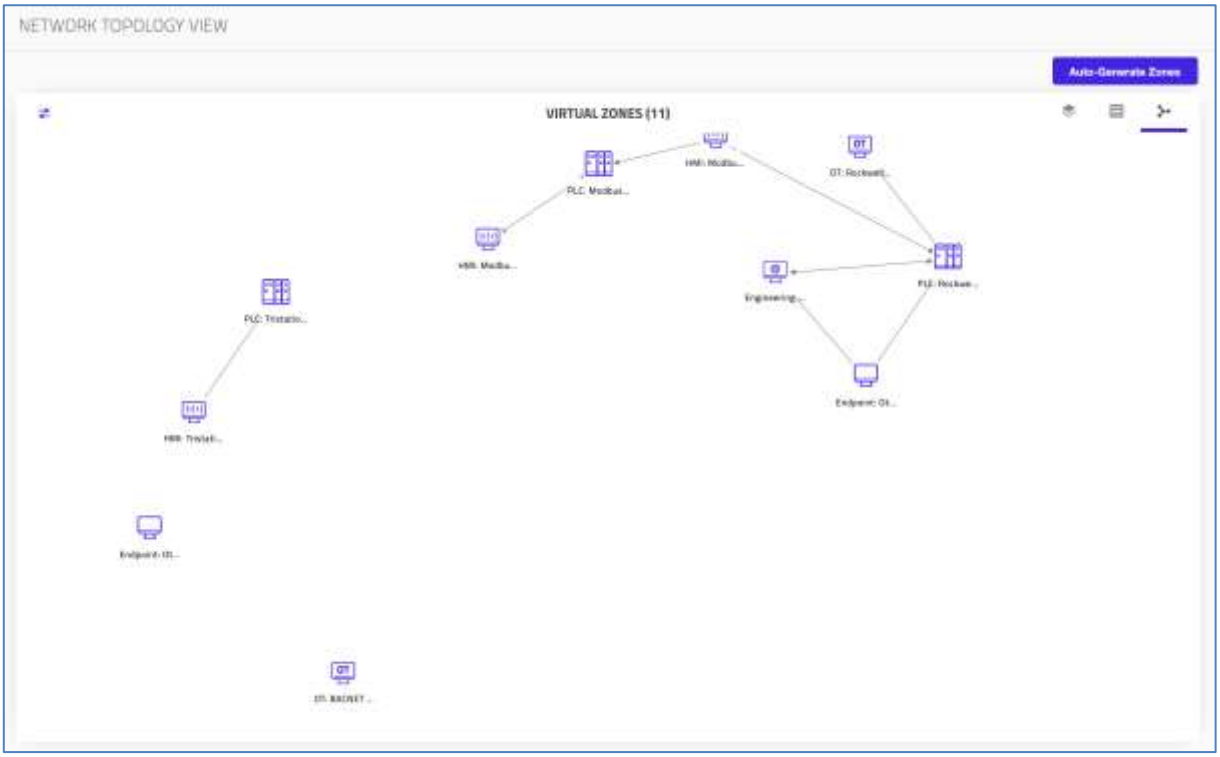


Figure 65 Virtual Zones - Network Topology View of Zones

5.10.3.2 Zones - Layered Topology View

The Layered Topology View features a Purdue model graph, displaying the zones in their relevant layers:

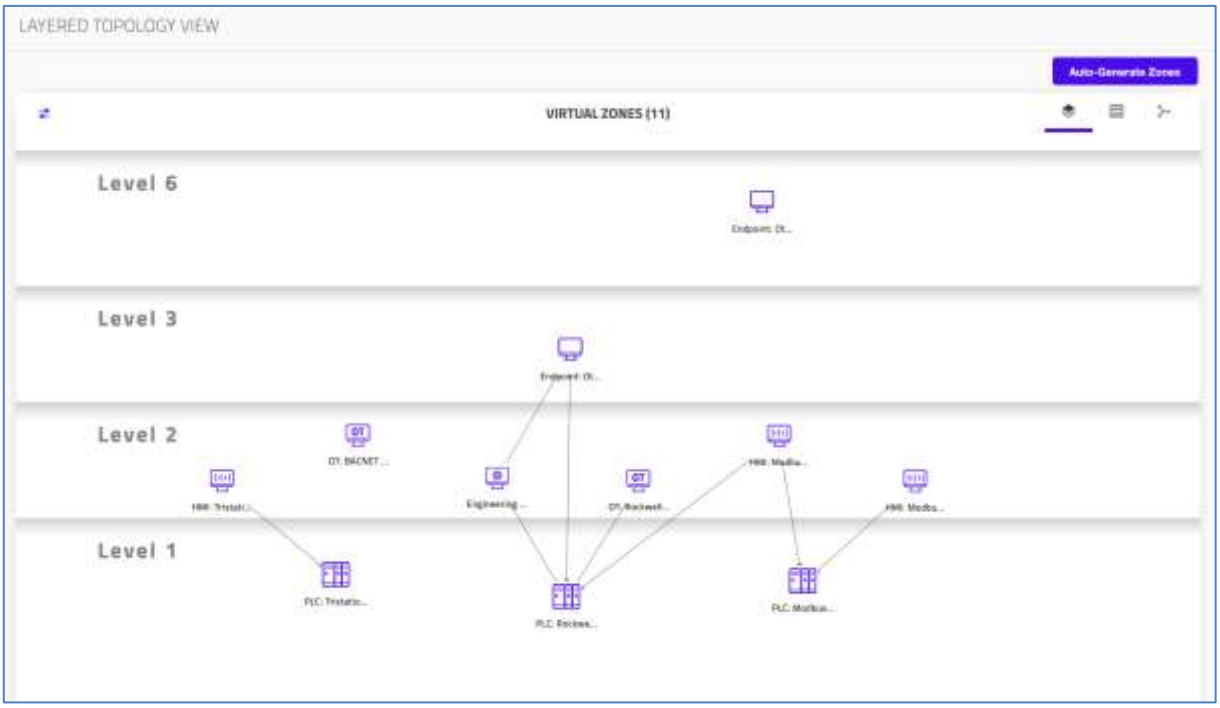


Figure 66 Zones - Layered Topology View

In both the Layered Topology and Network Topology views, you can use **Communication Direction**  to dynamically display the direction of the communication in the zones and view the dominant network communication at a glance:

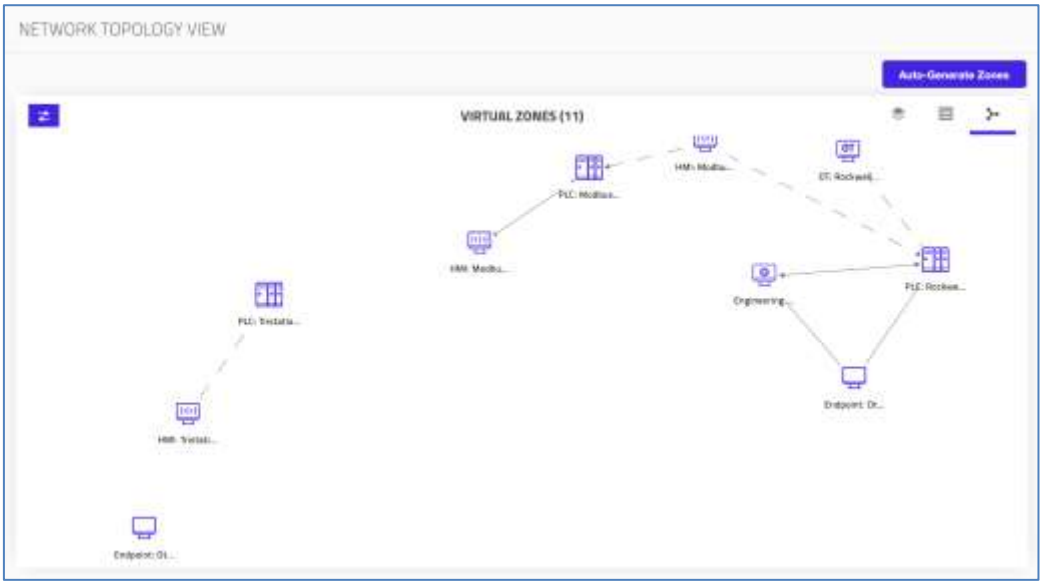


Figure 67 Zones - Communication Direction

You can pan to different areas and zoom in and out by hovering your mouse over the graphic and pressing the + or – keys on your keyboard.

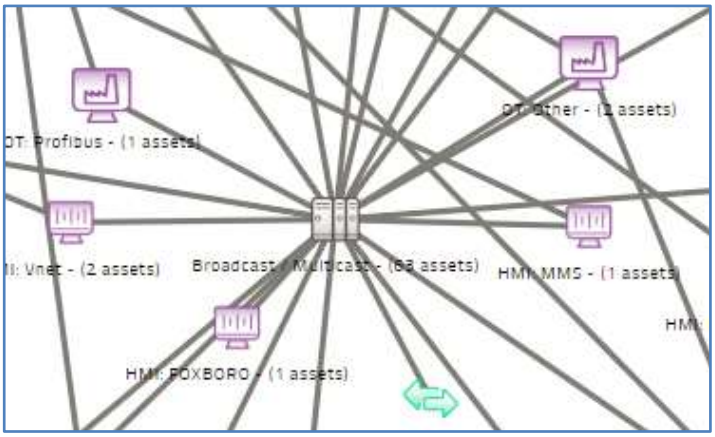


Figure 68 Policies & Zones - Zoom In

Communication between a pair of virtual zones (a conduit) is represented by a segment with the zone icon at each end.

5.10.4 Zone List

The **Zone List** displays all the zones in list form and is accessed by clicking **Visibility > Zones**.

Clicking on a zone leads you to more details. Each zone is assigned a zone **Risk Level** and a zone **Criticality**.

- Admins and Users with Write permissions can

- create zone/s
- generate automatic zones
- rename zones
- delete zones

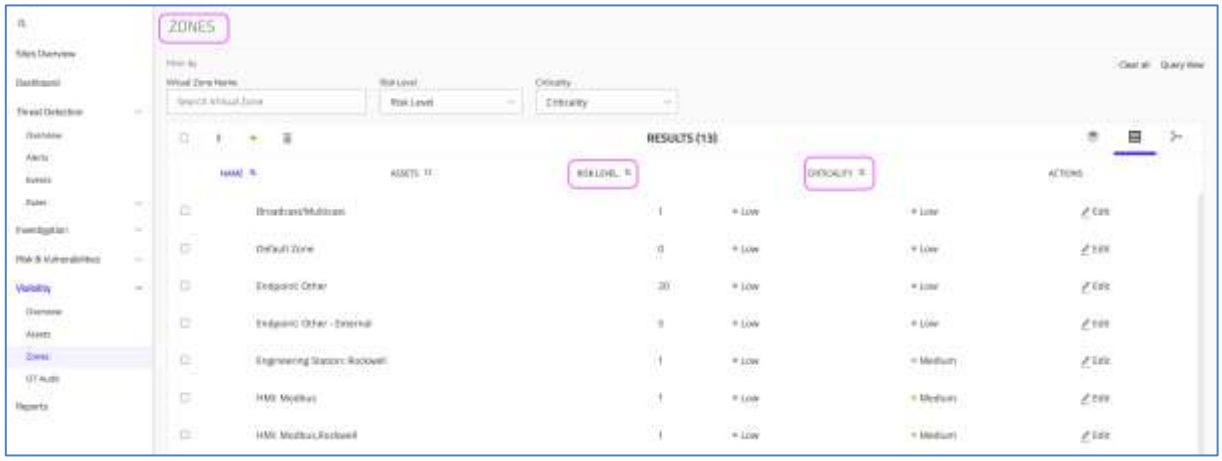


Figure 69: Zone List

5.10.5 Editing Zones

You can add, rename, and delete zones.

- All the columns are displayed by default: Name, Assets, Risk Level, Criticality, and Actions. To show or hide columns, click **More** > **Select Columns**.

5.10.5.1 Adding a Zone

- Click **Add** to create a new Zone.

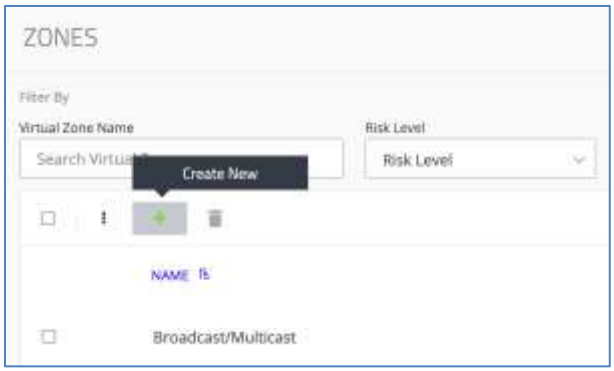


Figure 70 Adding a Zone

- After adding the new Zone, associate assets with it by editing the details on the **Assets** page.
- Select the relevant row and click **Edit** to rename it.

5.10.5.2 Renaming a Zone

1. To rename a Zone, click the row's **Edit** 

button.

2. Apply your change to the Zone name and click **Update**:

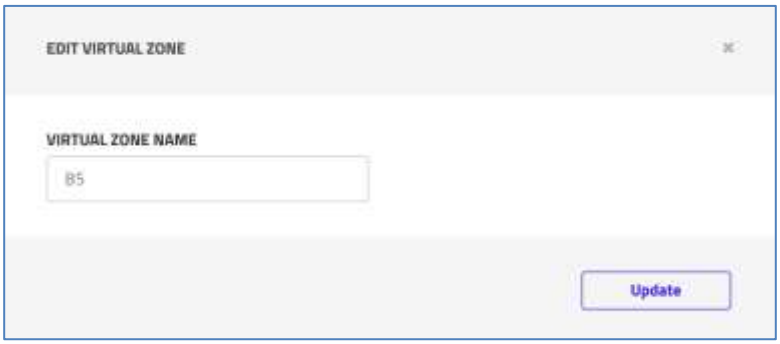


Figure 71 Updating a Virtual Zone

Deleting a Zone

- To remove a Zone, select the checkbox next to each row to be deleted and click **Delete**  .

5.10.6 Customized Auto-Grouping of Zones

The Zone feature helps to manage the assets and the Zone rules. When you have many assets with the same kind of attributes, you want to be able to see and manage them in an easy way and at a high-level. You can create rules according to those zones, manage the zone risk, and manage the asset inside the zone.

Customized Auto-Grouping allows you to choose which grouping method to group the zones by, which attribute; you can choose to group them by the default algorithm, subnets, or custom attributes.

- To modify the default Zone grouping:

1. Navigate to **Settings > Management > General > Virtual Zones** tab.

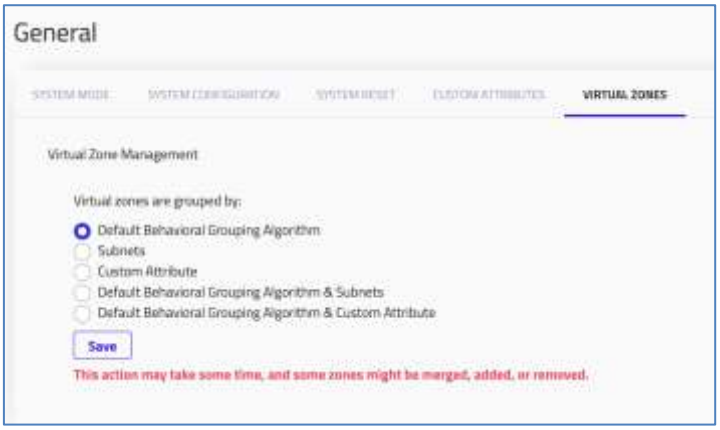


Figure 72 Virtual Zone Management

2. Choose the grouping method. Zones are grouped by:
   - Default Behavioral Grouping Algorithm - uses the asset type and protocol to group the zones (for example, PLC: Rockwell)
   - Subnets - groups the zones by the detected subnets in the network (each zone is another subnet)
   - Custom attribute - the user can define custom attributes for each asset, for example, the custom attribute that represents a process in the factory. By grouping assets by custom attribute, the user is able to create zones from these attributes.
   - Default behavior & subnets/custom attributes - are combining the default algorithm with subnets or custom attributes. It can be used if you want to create a zone of the default algorithm and consider the subnet or custom attribute in the zone calculation as well.
3. Click **Save**.

5.10.7 Zone View Page

Exploring a Virtual Zone is done with the Zone View Page, which enables users to investigate all the information in one place.

To access the Zone View page:

1. Navigate to **Visibility > Zones** in the main menu.
2. Click the name of the desired zone.

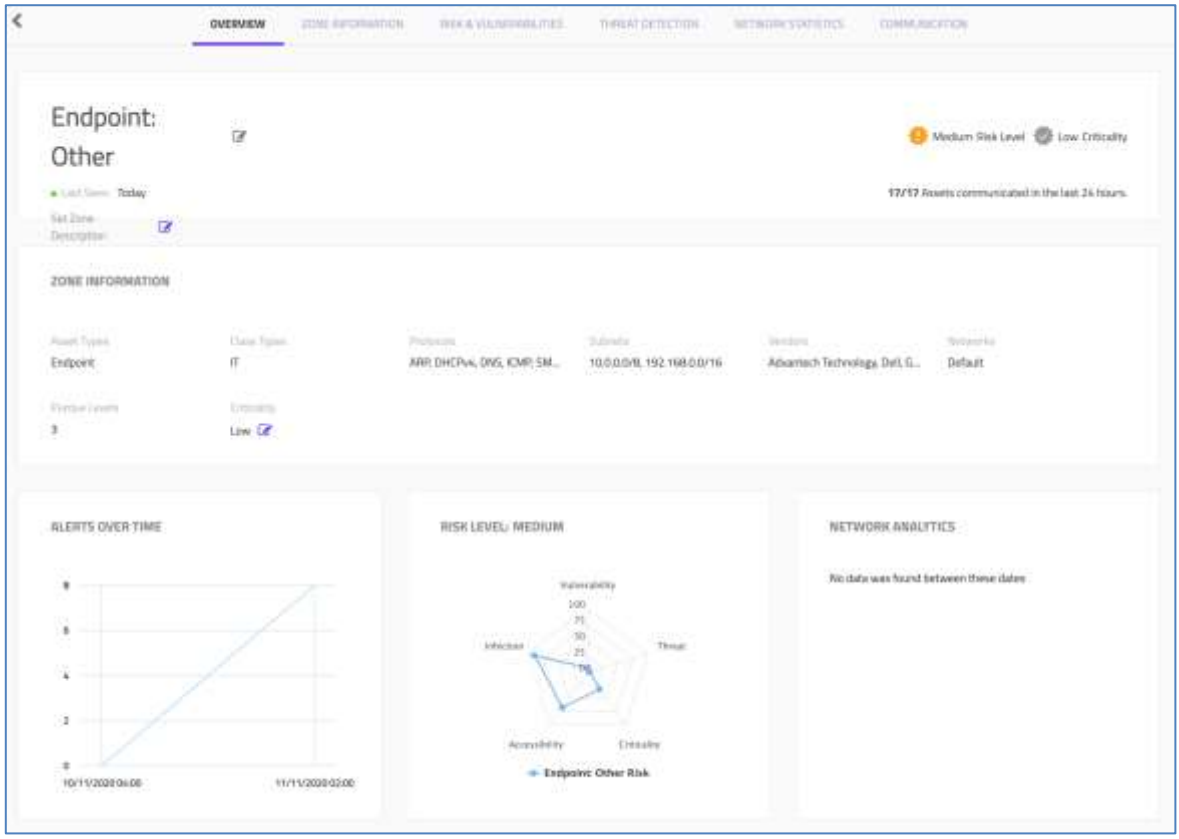


Figure 73 Zone View Page - Overview

The Zone View page features the following headers:

- Overview
- Zone Information
- Risk & Vulnerabilities
- Threat Detection
- Network Statistics
- Communication

6 Risk & Vulnerabilities

6.1 Overview

The Risk & Vulnerabilities Overview shows which aspects of the network can be fortified to achieve a more robust network architecture and enhance protection of the system. It highlights if the system is sufficiently patched by showing gaps in network security.

TIV generates Insights that reveal particular exposures and vulnerabilities, empowering users to investigate both operational (process) and security insights. This tool provides deep insights based on the analysis of your entire security posture, producing a holistic picture and risk assessment across your entire ICS network. These insights are collected from traffic by SPAN monitoring, ingesting PCAP, AppDB, or Active query.

This Overview provides a summary of the entire asset inventory and all communications discovered on the industrial network, pinpointing vulnerable assets and resolutions, while revealing network configuration and other "network hygiene" issues that can provide attackers with a means for interfering in critical processes.

TIV's key Insights show how to proactively enhance your ICS security posture, shedding light on mission critical assets and misconfigurations. Security and OT teams can easily use and act upon them. The system generates a summary score and detailed analysis of the weaknesses in your ICS environment. Some insights expose a list of protocols and the assets using these protocols. Others divulge assets that communicate with external assets, including assets that are performing data acquisition write actions on PLCs and thus have potential for impacting the process. Insights are calculated automatically and frequently. The Overview leads you to the full Insights page. A listing of potential Insights is provided in the *TIV Reference Guide*.

Users receive periodic packages for updating their Common Vulnerability and Exposure (CVE) databases to detect vulnerable models/firmware plus new threat signatures to detect attacks at the network level. TIV reports CVE matches for the devices in the network with a list of network hygiene and other configuration issues that can potentially open an attack path. TIV regularly adds Incident of Compromise (IOCs) that expand detection coverage even further to guard against CVEs that have yet to be addressed. By applying CVE updates, users can uncover compromised devices.

6.2 Risk & Vulnerabilities Overview

To access the Risk & Vulnerabilities Overview, click **Risk & Vulnerabilities > Overview** in the main menu.

The **Risk & Vulnerabilities Overview** appears as follows for a TIV Site (see section 6.2.1 for the EMC Overview):

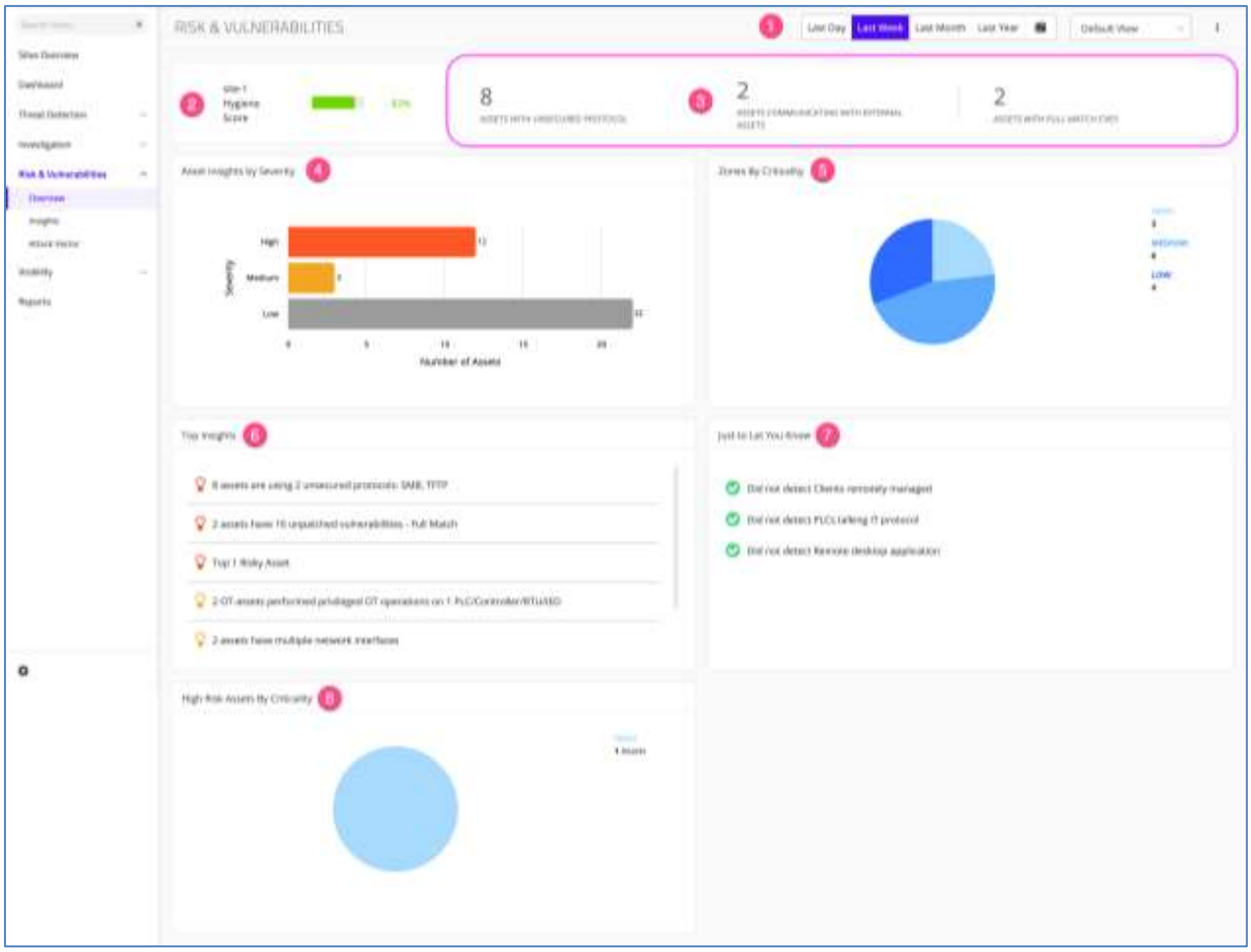


Figure 74 Risk & Vulnerabilities Overview

The Risk & Vulnerabilities Overview includes:

1. The **Time Frame Selector** to show information based on the time period of your choice (day/week/month/other). All widgets described below represent the results per the selected duration.
2. **Hygiene Score**
3. Asset Insight Numbers – Summarizes the prominent Insight findings:
   - **Assets with Unsecure Protocols** – Lists the total assets identified as having unsecure protocols.
   - **Assets Communicating with External Assets** – Lists the total assets communicating with External Assets.
   - **Assets with Full Match CVEs** – Lists the total vulnerabilities detected.

- For an EMC, an additional Top Info bar appears, displaying the Hygiene Score per site:
- When there are more sites than the amount shown on a single line, the Top Info bar is extended.

4. **Assets Vulnerabilities by Severity** – Lists the assets per name, sorted per severity level
5. **Zones by Criticality** – A pie chart widget of the distribution of the zones per Criticality.
   Clicking an area of the pie links to the associated Virtual Zones page with the relevant Criticality filter.
6. **Top Insights** – Shows the most significant insights. Slide the bar on the right side downward to see the lower part of the list. Click Show More to open the Insights page.
7. **Just to Let You Know** – List of Insights that highlight the potential issues that were investigated and do not exist in your system (e.g. Dangerous Protocols, Unpatched Vulnerabilities)
8. **High Risk Assets by Criticality**– Widget showing the distribution of high-risk assets per criticality.
   Click an area of interest in the pie chart to reach the detailed Asset list with the appropriate filters (by both Risk and Criticality). When no high-risk assets exist, the widget heading changes to '**No High-Risk Assets Found**'.

6.2.1 EMC Risk & Vulnerabilities Overview

The EMC Risk & Vulnerabilities Overview appears as follows:

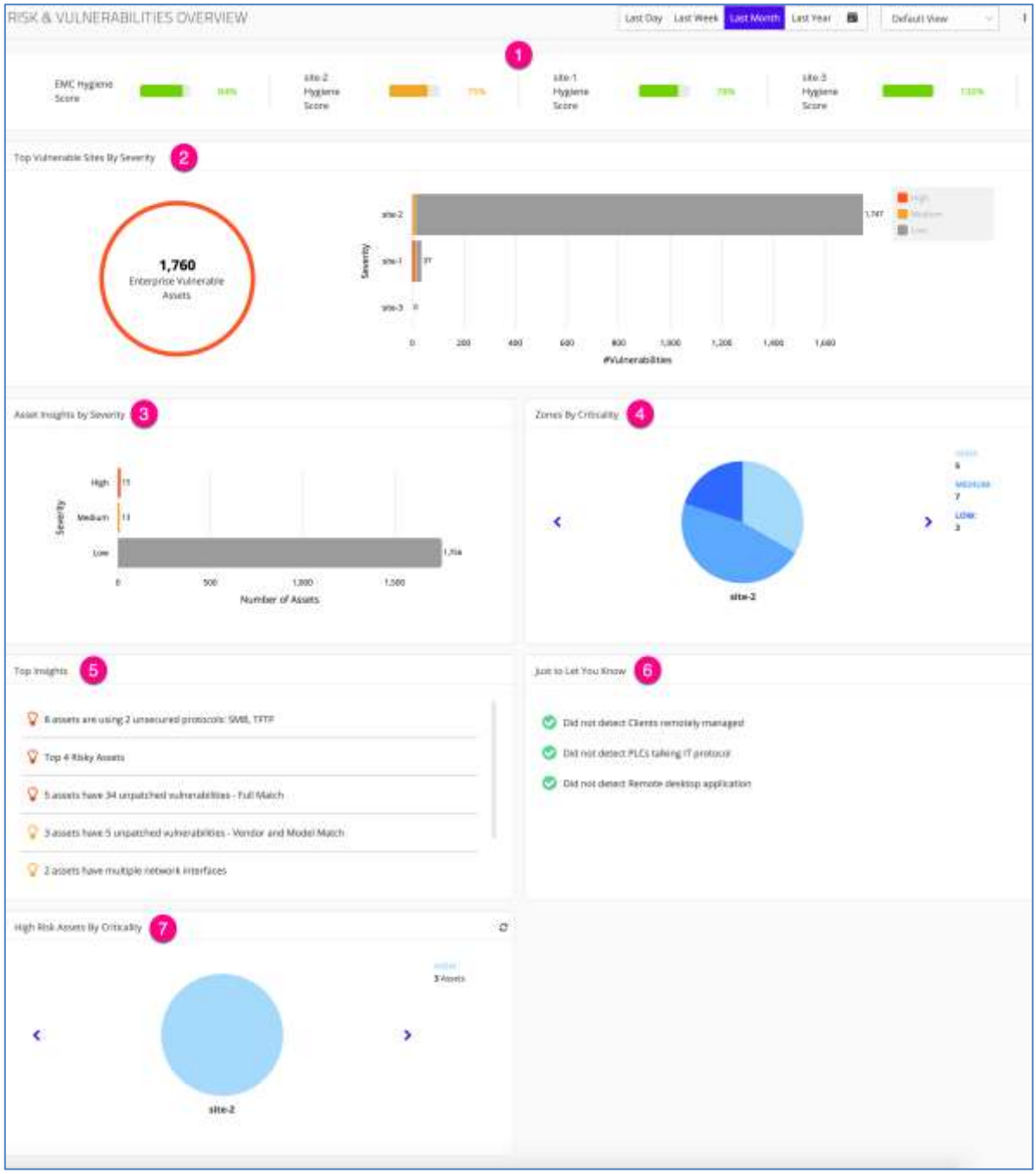


Figure 75 EMC Risk & Vulnerabilities Overview

1. **Hygiene Score** - This widget shows the Hygiene Score for each site.
2. **Top Vulnerable Sites by Severity** – Shows the volume of top enterprise vulnerable assets, sorted *per site* and per Severity level (High, Medium, and Low).
3. **Asset Vulnerabilities by Severity** – Shows the volume of top vulnerable assets *per site*, sorted per Severity level.

4. **Zones by Criticality** – A pie chart widget of the distribution of the zones per Criticality per site. Each pie chart represents a single site. Use the **< >** arrows to navigate to the **<** Previous or Next **>** site. Clicking an area of the pie links to the associated Virtual Zones page with the relevant risk filter. See Risk Calculation.
5. **Top Insights** – Shows the most significant insights, sorted by importance. Slide the bar on the right side downward to see the lower part of the list. Click **Show More** to open the Insights page.
6. **Just to Let You Know** – List of Insights that highlight the potential issues that that were investigated and do not exist in your system (e.g. Dangerous Protocols, Unpatched Vulnerabilities)
7. **High Risk Assets by Criticality** – Widget showing the distribution of high-risk assets per criticality per site. Each site is represented with its own pie chart. Click an area of interest in the pie chart to reach the Assets list with the appropriate filters (by both Risk and Criticality).

   Click the right arrow **>** to navigate to the next site.

6.3 Risk Calculation

TIV uses a granular risk mechanism for classifying assets and zones. It is a self-learning algorithm that enables users to detect risky areas and assets in the network. Then users will understand the nature of the risk in order to take the necessary steps to remediate it.

The Risk calculation impacts the assets, zones, and the Hygiene Score of the site, and its level is defined as High, Medium, or Low, based on the following parameters. Each parameter has its own score and impacts the asset risk level as follows:

- Risk Algorithm for Assets – The Asset Risk Score is based on the asset's Vulnerabilities, Insights, Alerts, Policies, Asset Criticality, and network locations.
- Risk Algorithm for Zones – The Zone Risk Score is based on an average of the asset parameters and the asset criticality of the zone; the number of zones communicating with this zone, and the number of zones that this zone is communicating with.
- Hygiene Score Algorithm – The Zone Risk has an impact on the Hygiene Score of all the sites. The Hygiene Score decreases when more zones are at high risk. When you want to improve the Hygiene Score, see section 6.3.1.

Note that Risk calculations occur continuously in the background; when you change the Criticality, the risk will be impacted directly, however the results are not shown in real time.

For more details refer to the *TIV Reference Guide*: Risk Score Specification.

6.3.1 Improving the Hygiene Score

1. Identify the assets with high risk scores by checking Insights of Top Risky Assets and checking their number of vulnerabilities.
2. Filter for high risk zones.
3. Resolve all the risk and vulnerabilities:
   - From the zones
   - From the assets
   - From the open alerts associated with those zones and assets.

> Note Completing Insight vulnerabilities will improve the overall network Hygiene Score. A "Hidden" or "Completed" Insight would not appear by default when showing the list of Insights and would not affect the network Hygiene Score.

For more information, see section 7.3.7.1 for resolving alerts and section 6.4.2 for approving and rejecting Insights.

6.4 Insights

Insights are derived from your entire security posture, producing a holistic picture and risk assessment. Both operational (process) and security insights are produced from a network switch. This page provides a detailed analysis of the assets and communications discovered on the industrial network. It pinpoints vulnerable assets and resolutions and uncovers network configuration that can provide attackers a pathway or impact critical processes.

TIV generates dozens of insights on how to enhance your ICS security posture, shedding light on critical assets and misconfigurations. Security and OT teams can easily use and act upon them. Some insights expose a list of protocols and the assets using these protocols. Other insights reveal assets that communicate with external assets, including assets performing data acquisition write actions on PLCs and have the potential to impact the process.

> Note Insight calculations are continuously calculated in the background, but the results are not shown in real time.

Insight operations are synchronized with the EMC, enabling users to view in the EMC relevant Insights from Sites. It also enables users to perform operations on the Insights from the EMC and vice versa.

The complete list of Insights is detailed in the *TIV Reference Guide*.

To access the Insights page:

- From the Main Menu, select Risk & Vulnerabilities > Insights.

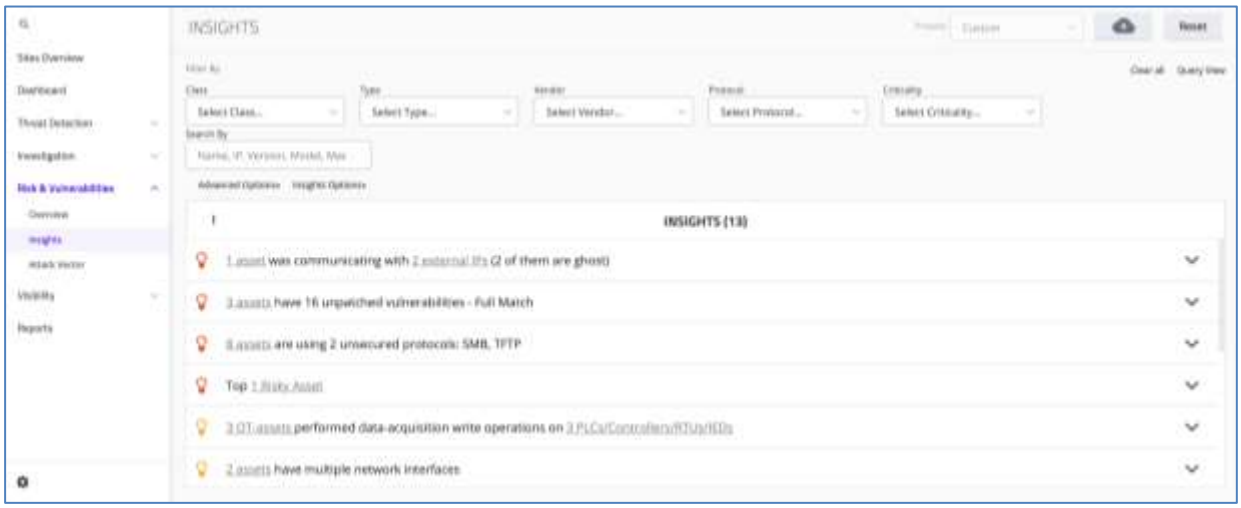


Figure 76 Insights Page

6.4.1 Insights for a Specific Asset

To view all Insights that effect a specific asset:

1. In the **Main Menu**, click **Visibility > Assets**. The Assets View page opens.
2. Click on a specific asset. The asset page opens.
3. Click the **Risk & Vulnerabilities** tab and then navigate to the **Insights** section of the asset page.

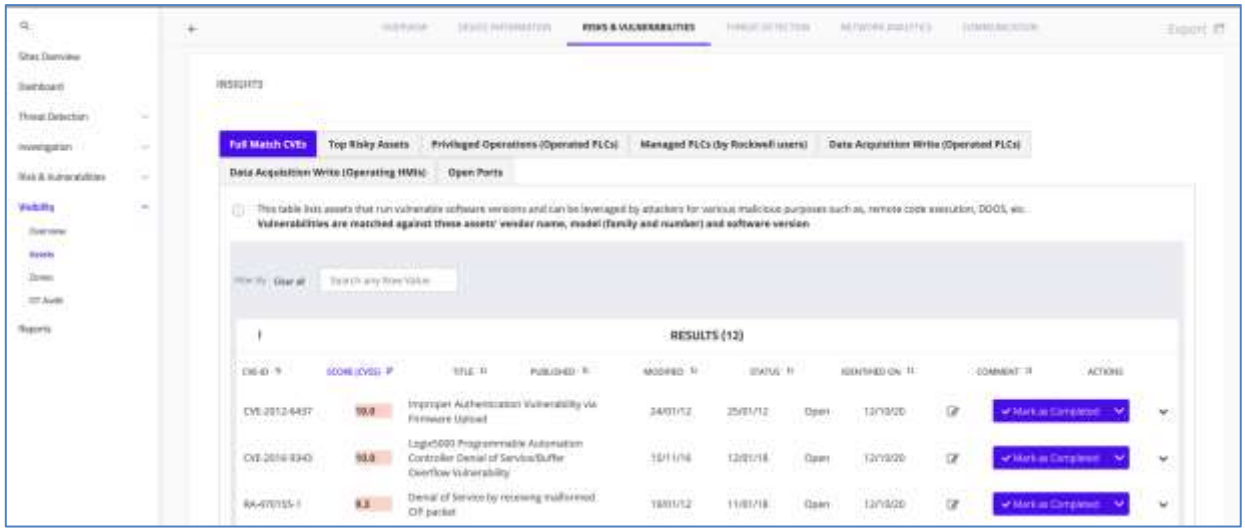


Figure 77 Insights under Risk & Vulnerabilities on the Asset page

6.4.2 Approving and Rejecting Insights

Users can update network insights with statuses. Supported statuses are "Completed", "Hidden", or "Open", where "Open" is the default status.

Comments can be applied to Insights, so the handling of the Insight could be managed per need. This allows the user to keep track of the vulnerabilities in their networks and statuses. This also ensures the Hygiene Score metrics are based only on relevant data.

To mark insights with statuses:

1. First go to the Insights section (see 6.4.1).
2. Mark status as completed, hidden, or open (see Figure 78).

Both Hidden and Completed act in the same manner. Both affect the hygiene score.

Figure 78 Marking Insights as Completed - Example

6.4.3 CVE Matching

With the Common Vulnerabilities and Exposures (CVE) discovery mechanism, asset vulnerabilities are differentiated between various types of matches: 'Full', 'Vendor', 'Model', and 'Windows'. Vulnerabilities are displayed according to their criticality level (High, Medium, and Low) as follows:

- A full match is displayed with Red (high criticality)
- The model and installed program matches are displayed with Yellow (medium criticality)

- Windows and vendor matches are displayed with Grey  (low criticality)

To view CVE matching, go to the Insights View page (see 6.4).

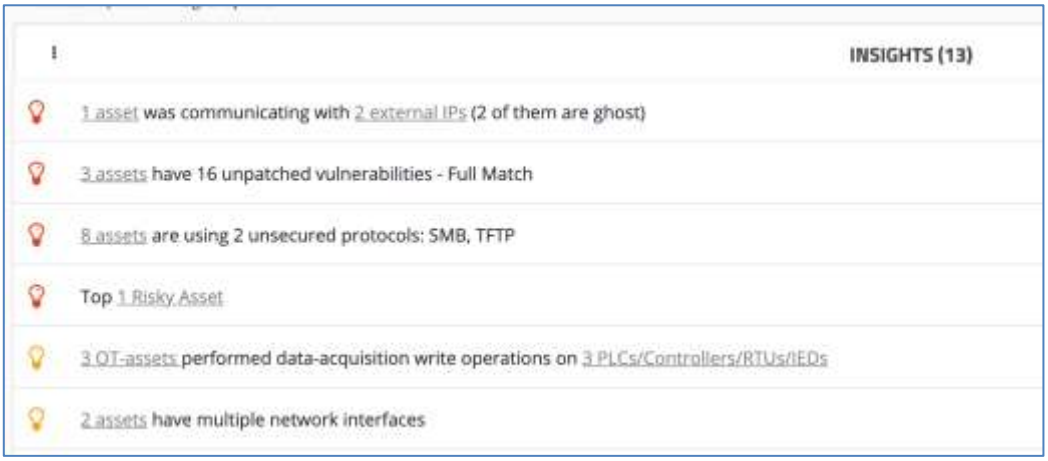


Figure 79 Insights Page - CVE Examples

TIV matches a CVE (vulnerability) to an asset based on gathered information. A match can be classified as a full match, vendor match, model match, or Windows match. For details, refer to the **TIV Reference Guide**.

6.4.3.1 Threat Definition Updates

Users receive regular update packages from Tripwire, providing the latest threat definitions discovered by TIV's Research team. These Threat Definition Updates include new CVEs as well as network traffic signatures and Yara signatures.

The update packages allow users to stay up to date with the latest threats without requiring a full upgrade of the entire TIV software. For more information, refer to the **TIV Reference Guide**.

6.4.4 Exporting Insights

For more information see section 9.6.9.3**, Insights Page**.

6.5 Attack Vectors

Attack Vectors are used to proactively mitigate risks in your ICS networks. By establishing a consolidated view of your security risks, this feature visualizes the impact of potential risks and other security gaps to your most vulnerable assets. Without impacting critical OT Infrastructure, Attack Vector simulation provides an attack analysis, which illustrates mitigation recommendations based on the most likely attack scenarios for your security teams.

The results display the scenarios that could potentially compromise your critical assets (especially OT assets), providing your security teams with the needed visibility to proactively mitigate risk and prioritize activities. TIV leverages proprietary analytics to reveal the most prominent attack scenarios an attacker could use to propagate between assets and zones in the network.

This empowers users to quickly visualize and simulate likely attack vectors based on risks and other security gaps. The system enables users to effectively mitigate and remediate against these critical potential paths an attacker would leverage to penetrate the environment.

> **Note** Due to the sensitivity of this capability, its access is limited to only those users with Administrator rights.
>
> Attack Vectors will not be calculated by default when using the Enterprise Management Console (EMC).

6.5.1 Using Attack Vectors

Select Risk & Vulnerabilities > Attack Vectors from the Main Menu.

- The default view represents the most threatened Attack Vector identified from all the potential possibilities calculated, which is in the riskiest zone.
- You can choose other target zone/s from which additional attack vectors can be calculated from the Target Zone dropdown.

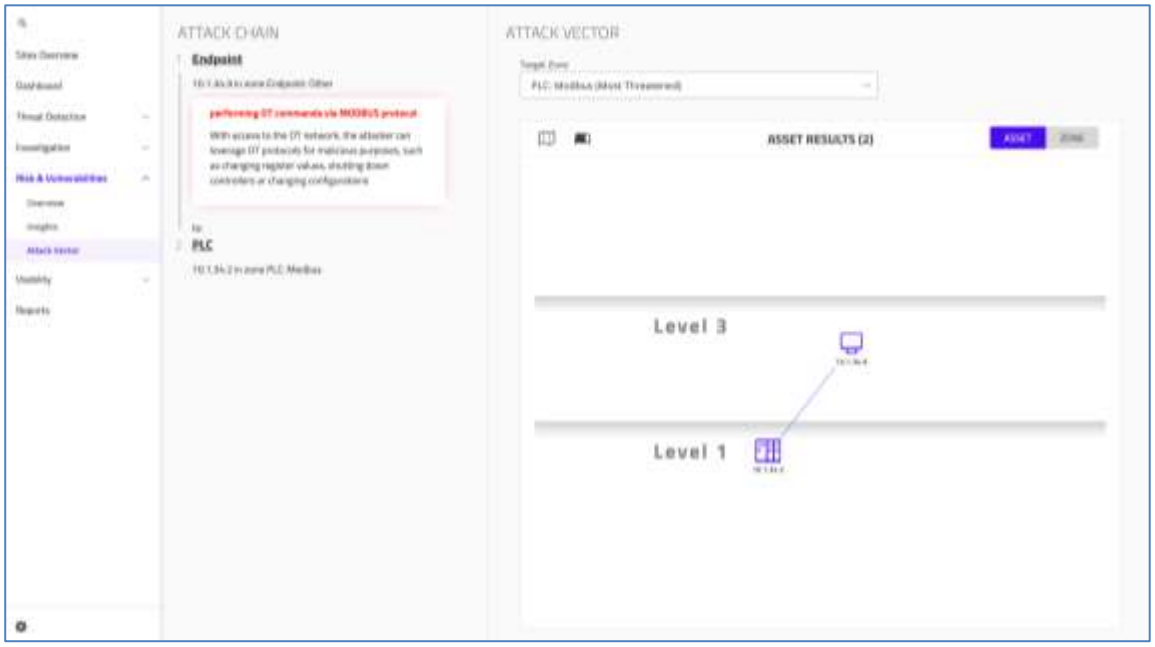


Figure 80 Attack Vector Simulation

The lateral movements that TIV considers an attack vector are:

- **Internal asset communicating with external assets** (except NTP, ghost assets)
- **Same subnets** - when an asset has a connection to an external network, the algorithm assumes that all assets in the network also have a connection to the external network
- **Remote connections** - if a remote communication between assets accrued (like RDP connection)
- **OT protocols** - running OT commands to change configurations
- **Domain controllers** – an attacker gaining control over a domain controller can execute commands

7 Threat Detection

7.1 Introduction

TIV is designed to identify threats early in their process. Relying on its in-depth knowledge of protocols, configuration, and communication flows, the system identifies known threat attacks and zero-day attacks as well as ones with sophisticated OT payloads.

The system uses deep packet inspection (DPI) analysis technology to

- protect critical infrastructures
- gain visibility into the network
- implement virtual network segmentation.

It continuously monitors for threats and policy violations.

TIV provides you with visibility to immediately focus on the network's vital signs to allow a quick response.

5 Detection Engines

TIV generates alerts based on anomalies, rules, signatures, and behaviors using the following engines:

- **Behavior Anomalies Detector –** This core engine alerts on baseline deviations. Baselines are generated from the protocols and communications the system has identified. Baseline deviations are behaviors that do not match the collection of traffic patterns that TIV has machine learned.

  This system translates this information into alerts to focus the operator's attention on

  - network changes
  - vulnerabilities
  - threats
  - zero-day exploits
  - malware
  - attacks in the ciphered traffic
  - resource misuse or misconfiguration.

- **Signature Based Detector** – This detector works on Yara and network traffic rules. TIV's known threat database also includes signatures provided by TIV's research team for zero-day vulnerabilities that are under formal disclosure. Network traffic rules allow users to create their own based on Snort rules and manually disable or enable existing signatures. Yara rules

provide pattern matching on data extracted from the network traffic, enabling extraction from TFTP, SMB, HTTP, and code sections. This provides more advanced signatures to target newer threats without requiring an overall system upgrade.
As with the Snort Engine, it is possible to develop customized rules using a Yara pattern language. This comprehensive set of tools identifies and alerts on threats and exploits such as DDoS.

- **Security Behavioral Pattern Detector** – This engine detects known security attacks such as man in the middle (MITM) and port and network scans. It also catches IT security patterns such as TAG/Address scans.
- **Operational Behavioral Pattern Detector** – This detector focuses on sensitive OT-related activity such as configuration downloads / uploads, mode changes on controllers, key state changes and firmware updates in addition to privileged commands to the controllers. This detector combats OT-targeted attacks and sophisticated payloads. It flags OT operations that occur within the network over any proprietary OT protocol. By identifying and reporting such activities, operators can make an informed decision and determine the next steps based on their Management of Change process.
- **Rule-Based Threat Detector** – This rule engine alerts on the customized rules that operators have configured to target specific events. For example, operators can employ rules to flag on values out of range or specific communication that is suspicious.

Correlation Engine

Based on alert indicators, the Correlation Engine compiles related, suspicious events into a Master Event. These events display as a chain with an alert score. All TIV alerts are correlated against the TIV indicator library. The alert score is made up of individual indicators, each contributing points (with a maximum of 100) to the overall alert score.

The alert score provides tools for

- identifying
- triaging
- investigating attacks.

This allows operators to prioritize which events need to be mitigated first.

Training vs. Operational Mode

Training mode builds initial baselines and policies by detecting and storing all network activity of all the assets which are being monitored. Training mode is essentially a listening and learning mode. When ready and enabled, the system identifies when no new activity is being recorded and automatically moves into Operational mode, without requiring operators to track and analyze the status of the training results manually.

After the network is in operational mode, deviation alerts will start flowing depending on new traffic being identified and compared to the stored baseline and policies. TIV alerts on any threat activity early in the kill chain.

For configuring auto-transitioning into Operational mode from Training mode, see section 10.1.1.5.

Approving Alerts

After analyzing an alert, Operators decide between several options:

- Approving the alert to add it to the TIV baseline
- Delegating the alert to another operator
- Archiving the alert to remove it from the screen unless it reoccurs.

7.2 Threat Detection Overview

To access the Threat Detection Overview, click **Threat Detection > Overview** in the menu.

The Threat Detection Overview appears as follows for a standalone TIV Server (see section 7.2.2 for the EMC Threat Detection Overview):

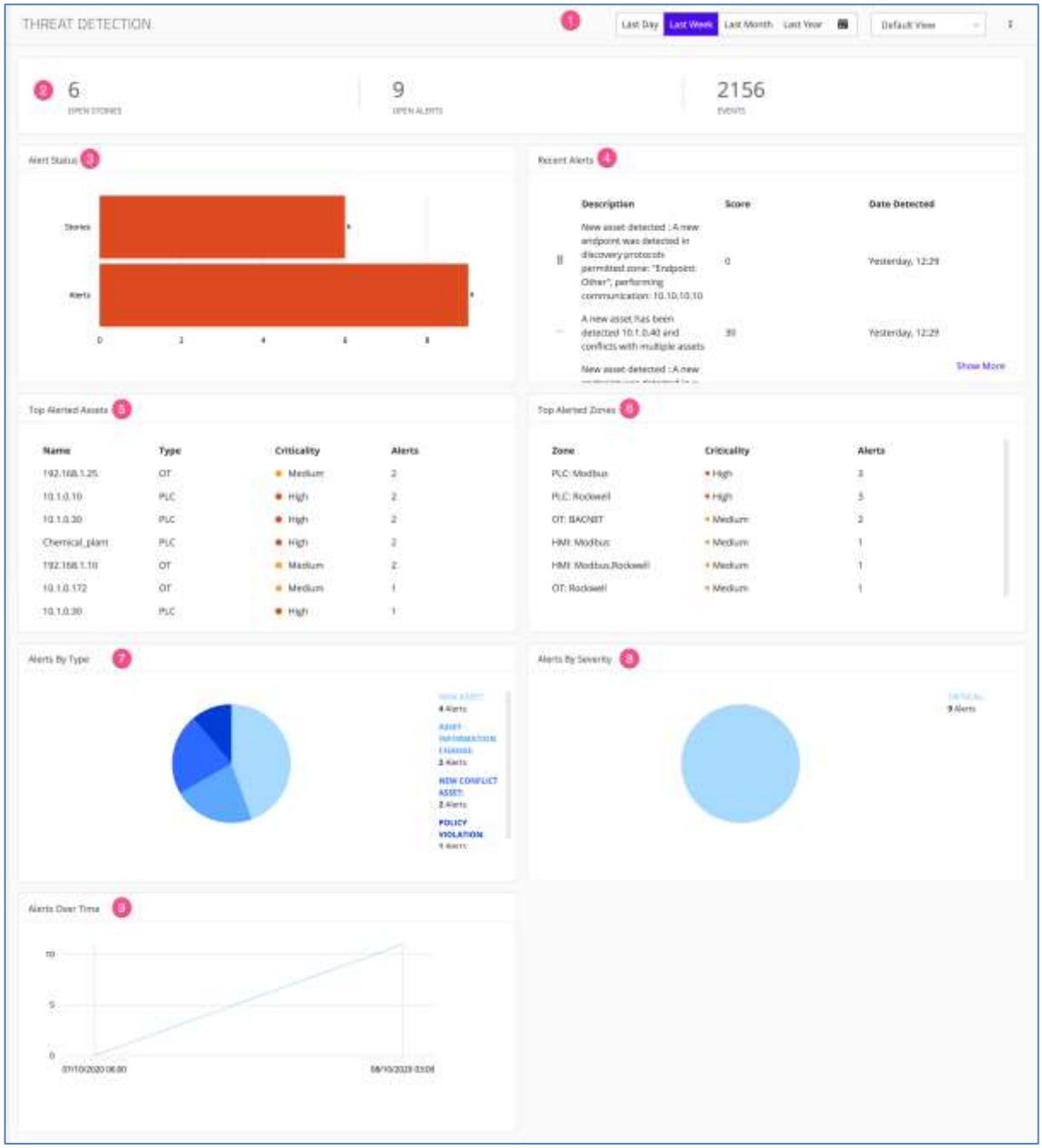


Figure 81 Threat Detection Overview

1. Use the **Time Frame Selector** to show information based on the time period of your preference (day/week/month/year). All widgets described below represent the results of the selected duration.

Threat Detection Widgets

2. **Threat Detection Bar** – Displays the total numbers of open alert stories, open alerts, and events for the selected time period. Click a number to display the full list of stories, alerts, or events.

3. **Alert Status** – Displays a bar graph of the open alert stories and open alerts for the selected time period. Click a bar in the graph to open a list.
4. **Recent Alerts** – A table highlighting the recent 10 alerts, displaying their **Description, Score,** and **Detection** date, with a colored dot to indicate the alert's severity level. Use the scroll bar on the right edge to view earlier alerts. Click an alert to navigate to the full details of its Alert page. Click **Show More** to display all alerts on the Alerts page.
5. **Top Alerted Assets** – Shows a table of the top 10 alerted assets, sorted by asset **Names**, its asset **Type**, each listing the alerted asset's **Criticality** level and the **number of alert instances** in the given timeframe. Assets with no alerts are not displayed. Click on an Alerted Asset to open its detailed Asset page.
6. **Top Alerted Zones** – This table shows virtual zones. Each virtual zone is grouped according to the type of alert associated with the asset. The virtual zones are displayed by criticality level. The top zones with open alerts are listed; zones that have no alerts are not listed. Click a virtual zone to reach its zone page (if there is one); otherwise, it leads to the Alerts page with the relevant zone filter. The zone page is a table of zones with each row displaying the zone name, its criticality, and the number of alerts in the given timeframe.
7. **Alerts by Type** – A pie chart widget showing the breakdown of alerts per type and the number of instances of each type. The top three types are shown. Click on an alert type to navigate to the Alert Page for detailed information.
8. **Alerts by Severity** – This widget displays a pie chart of the alert distribution for each severity category in the given timeframe. Click on a portion of the pie chart to reach the Alerts Page filtered by the specific severity and timeframe.
9. **Alerts over Time** – This time graph shows the distribution and total new alerts based on their alert types (with a line for each type) for the selected time period. Click on a line to navigate to the Alert page. The granularity of the alert groups displayed is relative to the selected time frame (for example, the alerts are grouped by hour when the timeframe selected is a day).

7.2.2 EMC Threat Detection Overview

The EMC Threat Detection Overview appears as follows:

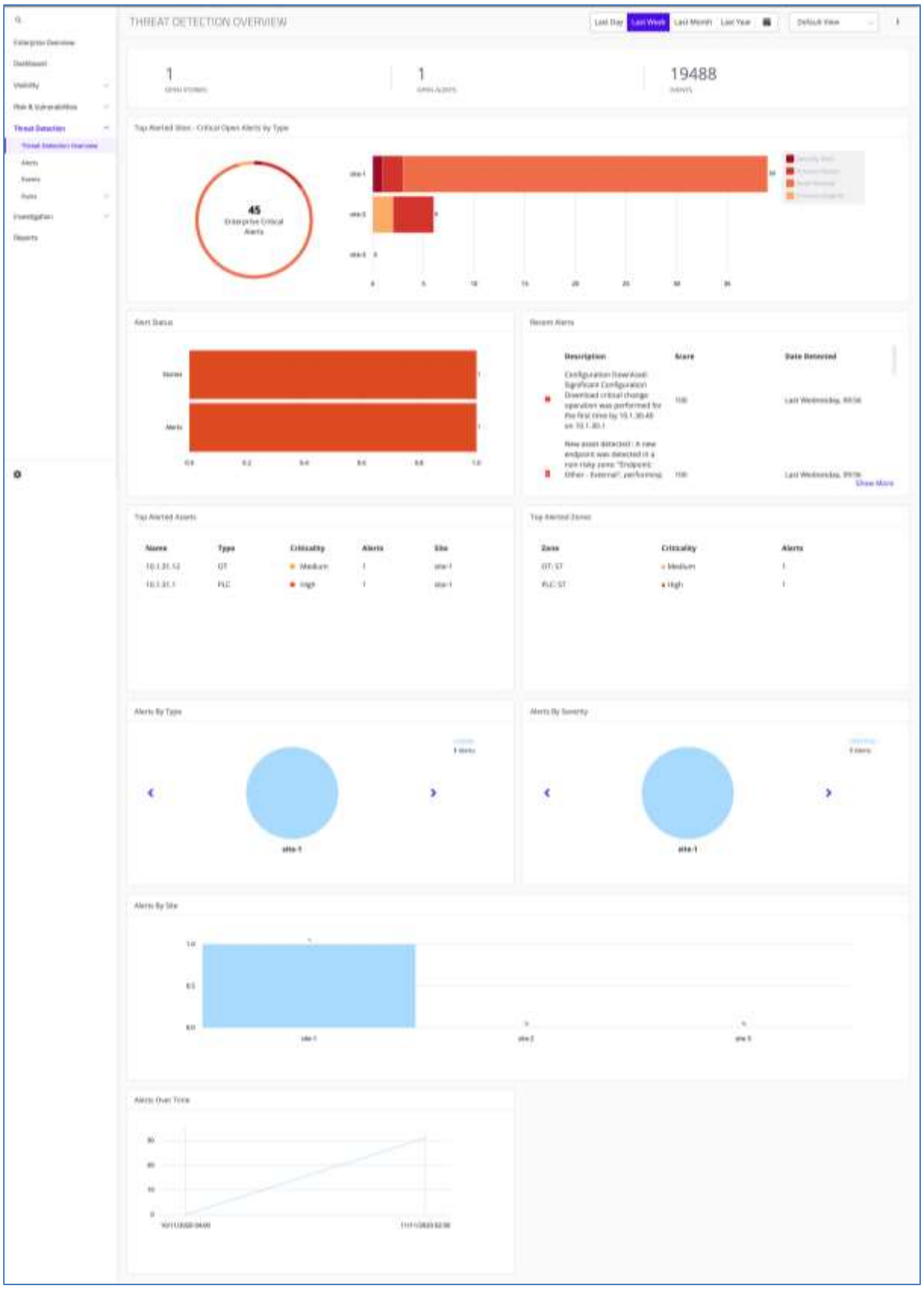

THREAT DETECTION OVERVIEW
Last Day
Last Week
Last Month
Last Year
Default View
1
1
19488
45
Enterprise Critical Alerts
Alert Status
Recent Alerts
Description
Score
Date Detected
Top Alerted Assets
Name
Type
Criticality
Alerts
Site
Top Alerted Zones
Zone
Criticality
Alerts
Alerts By Type
Alerts By Severity
Alerts By Site
Alerts Over Time

Figure 82 EMC Threat Detection Overview

Refer to the Threat Detection Overview in section 7.2 for descriptions of these widgets.

7.3 Alerts

Alerts appear in the Alerts page, which displays resolved and unresolved alerts and allows you to manage them.

To navigate to the Alerts Page, click **Threat Detection > Alerts**.

7.3.1 Alert Types

TIV differentiates Process Integrity Alerts from Security Events Alerts.

- **Process Integrity Alert** – Reflects a critical change to a process, such as configuration, download/upload, and mode change. These alerts are triggered by a network failure, operator error, or malicious attack.
- **Security Event Alert** – Raised when a well-defined cyber-attack vector occurs, such as a Man-in-the-Middle (MitM) attack, port or network scan attack.

7.3.1.1 Process Integrity Alerts

The Process Integrity Alerts generally appear while in Operational Mode as described below.

- **New Asset** — A new asset has been added into the environment (vendor laptops, virtual machines, physical servers, network switches, PLCs, etc.)
- **Policy Unmatched Violation** – This type of alert is triggered when the detected communication was not matched to any rule with an 'Allow' action, and as a result, the implicit "Alert on Anything" rule was hit. This means there was no pre-existing policy rule to allow such communication.
- **Policy Rule Match** – This occurs when the detected communication matches an explicit policy rule defined with an 'Alert' action.
- **Asset Information Change** — Occurs when information associated with an asset is changed (e.g. a new IP/MAC address).
- **Mode Change** — When a user changes the state of a PLC from an engineering workstation or other software application. Mode state examples: Run, Stop, Program.
- **Configuration Upload** — When a user uploads the configuration from a PLC to an engineering workstation or other software package. Commonly contains the following types of alert information: code segments being

uploaded; code differences; users performing code changes; project name/identifier.

- **Configuration Download** — When a user downloads the configuration from an engineering workstation or other software package to a PLC.
- **Monitor Debug** — When a user uses an engineering workstation or other software package to put a PLC into the monitor or debug mode (Note: This is typically a troubleshooting function built into some PLCs).
- **New Asset Conflict** — When new information occurs that conflicts with an existing assets information. Usually occurs when assets have the same IP/MAC addresses or other identical information.
- **Firmware Download** — When the firmware is changed for an asset. Generally performed by an engineering workstation or additional software on a PLC.
- **Online Edit** — When a user connects to the PLC from an engineering station and implements changes in the settings.
- **Suspicious Activity** — Suspicious behavior that generally indicates malware.

For more details, refer to Alert Guidelines in the **TIV Reference Guide**.

7.3.1.2 Security Event Alerts

Security Alerts represent malicious behavior and are not generally supposed to occur within the OT environment. Always evaluate them with the highest priority.

- **Failed Login**— This occurs with specific makes / models of PLCs that support authentication functions.
- **Man-in-the-Middle Attack** — When an attacker inserted a new machine into the communication pathway between two assets. This new machine will use this position to either monitor or alter the communication between these assets.
- **Network Scan** — When an attacker scans either the OT network, or assets within the OT network, looking for attack pathways. TIV shows the source of the network scan and the affected assets. Network scans can also be detected in training mode. The supported scans are as follows:
  - Single Port network scan in TCP and UDP
  - Multiport host scan in TCP and UDP
  - Ping Sweep scan
  - SYN flood Denial-of-Service.

  When approving such an alert, the system would allow this type of scan only from the originating host.

- **TCP Scan** – Suspicious activity of an asset that is performing port scanning in the network.
- **UDP Scan** – Suspicious activity of an asset that is performing port scanning in the network.
- **Known Threat Alerts** – TIV uses a sophisticated signatures-based database to enhance its capability for identifying known attacks.
- **Threats** – Collection of known malware commands and control servers.

For more details, refer to Alert Guidelines in the *TIV Reference Guide*.

7.3.2 Alert Story

An Alert Story is a set of alerts that TIV correlates after it has determined that the events are interrelated.

To navigate to an alert story:

- Click **Threat Detection > Alerts** in the main menu. The **Alerts** page appears.

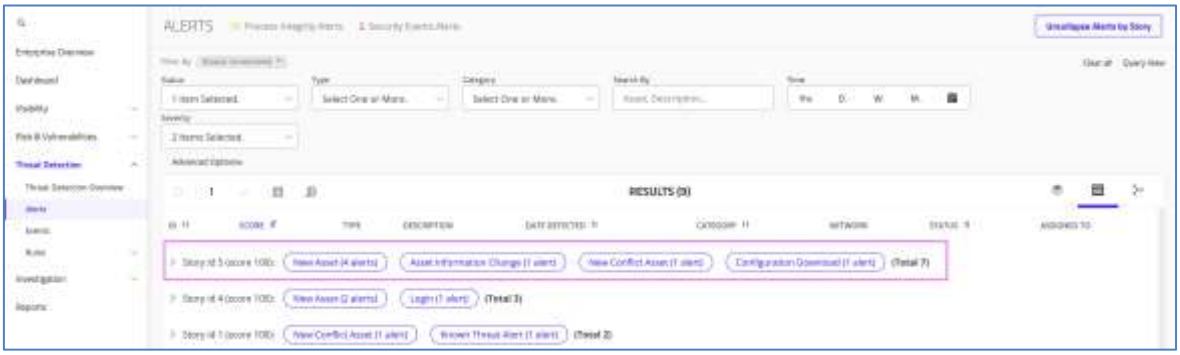


Figure 83 Alert Story Example: Story ID 5

The above Alert Story example contains several types of Alerts: New Assets, Asset Information Change, New Conflict Asset, Configuration Download.

7.3.2.1 Alerts vs. Stories

Alerts show a chain of events that provides a rationale behind the alert. The system employs alert mechanisms to interpret network and asset behavior into quantifiable risk factors.

The alert's chain of events indicates when the score has been impacted by network activity or other related behavior. The scoring mechanism runs on a range from 0 to 100, assigning each type of alert with a score indicating its relative significance.

Stories correlate the alerts and combine those alerts into one story. The Story graph of the alert is also displayed, showing when the score has been impacted by network activity or other related behavior.

7.3.3 Alert View Page

To navigate to the **Alert View** page:

1. Click on **Threat Detection > Alerts** in the main menu. The **Alerts** page appears.
2. Expand a **Story ID** and click on the desired alert. The **Alert View** page opens.

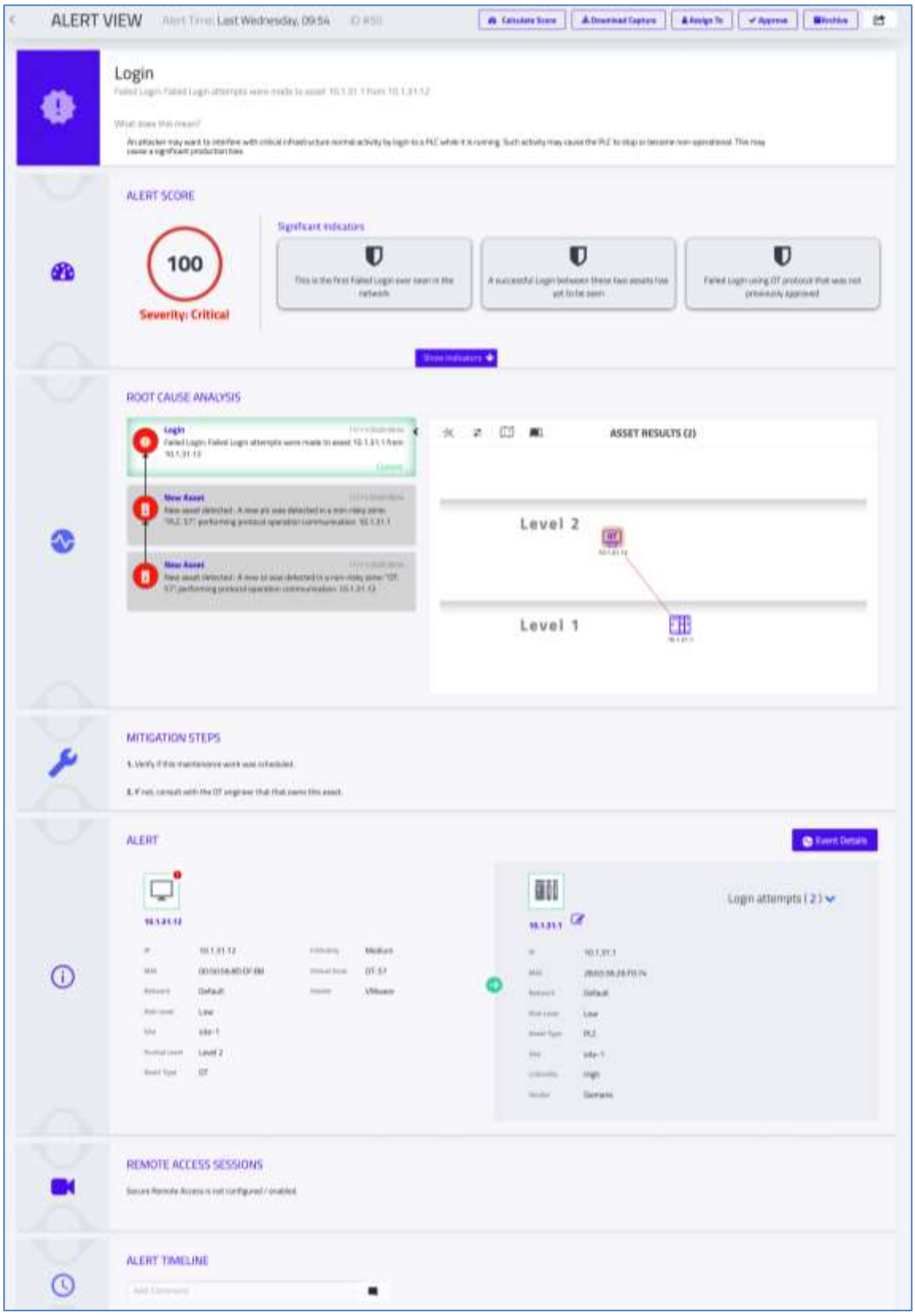


Figure 84 Alert View

7.3.4 Alert Scoring

TIV's Alert Scoring is a method for managing and controlling alerts. It enables different levels of sensitivities to enforce the strictness of the detection algorithm. The detection algorithm decides if an event is considered relevant enough to warrant investigation. Each individual alert receives a score ranging from 0 through 100.

Admins control the sensitivity value to suit their environment. After an alert passes the defined threshold, it is considered qualified. Until it has been approved or archived by the user, its score can only be increased by new indicators. The alerts are provided, with a chain of events that provide a rationale behind the alert mechanisms, to interpret network and asset behavior into quantifiable risk factors.

The scoring provides a detailed and transparent method for assessing the real risk involved with an alert. This enables TIV to significantly improve its ability to differentiate severe alerts from notifications. The alert score is shown with static indicators and each of their specific contributions to the overall alert score. An indicator is a result of a related network activity that can potentially affect the score of an alert and provides context.

7.3.4.1 Sensitivity

TIV's sensitivity value differentiates notifications from alerts. The possible sensitivity categories range between 0 and 100, as **Low, Medium, Normal,** or **High**.

7.3.4.2 Alert Scoring Formula

In the alert scoring, the indicators are evaluated against the asset information and communications. The alert score is then determined based on the matched indicators. The severity is hard coded based on the alert score:

- **Critical severity**
- **High severity**
- **Medium severity**
- **Low severity**

Alert Score Values

Each alert can receive a score of 0-100. The alert score is capped at 100, even if the sum of indicators exceeds 100.

7.3.5 Alert Title

The Alert Title section contains the alert name, the summary of the alert details and the meaning of the alert.

To navigate to an alert title:

1. Click on **Alerts** from the main menu. The **Alerts View** page appears.
2. Expand a **Story ID** and click on the desired alert. The **Alert View** page opens with the alert title, as shown in Figure 85.

Figure 85 Alert Title with Description

The TIV alert description describes the alert within the context of the process.

> Note When upgrading a multi-site configuration, until all sites are migrated, the Score will be equal to 88 for all stories of the old sites in EMC.

7.3.6 Alerts Page

Use the **Alerts** page for viewing and investigating your alerts.

To access the **Alerts** page:

- Navigate in the main menu to **Threat Detection > Alerts**.

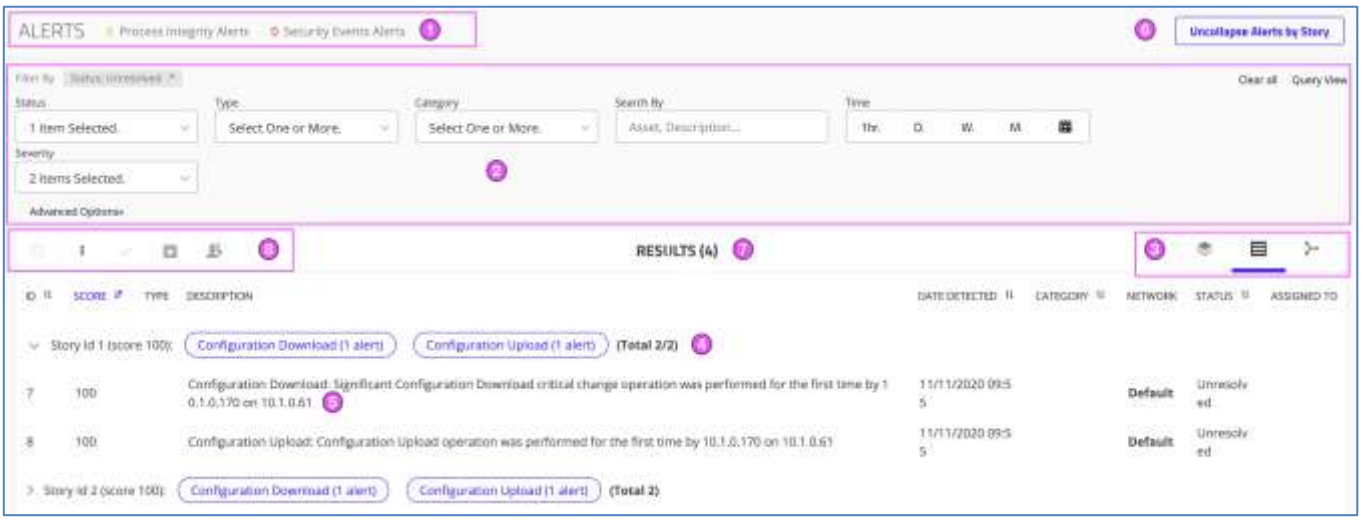


Figure 86 Alerts Page

1. The top bar gives the total Process Integrity Alerts vs. Security Event Alerts.
2. Filter the **Alerts** page to display the alerts according to the following.
   - Use the Alert **Status** to differentiate alerts with an Unresolved status (by default) vs. Resolved alerts.
   - Select specific Alert **Type**/s of interest. Choose to identify alerts of the **Category** Integrity and/or Security. Use the **Search by** window to find particular assets you suspect may be involved in this alert.
     Set the alert **Time** range of interest.
   - The Alert **Severity** level is based on the **Alert score**, which is determined based on the matched Indicators that are evaluated against the asset information and communication.
   - Click **Clear All** to clear all filters**.** Click **Query View** to show the filters in query view and edit as needed.
   - Click **Advanced Options** to show more filtering options.
3. The default **Alerts** page picture shown in Figure 86 is in **List View,** where the alerts are clustered into Alert Stories.
   - Alternatively, select a **Layered Graph** or **Network Graph** view:
   - Use the **Layered Graph** to view the assets impacted by the alerts in the context of the asset's Purdue model levels and the connections between the assets.
   - Use the **Network Graph** for visualizing all assets impacted by the currently filtered alerts. Assets that communicate with each other are shown closer together. The arrows indicate the direction of communication between related assets.
4. Rows of the **Alert Results table** are provided according to **Alert Stories.** They are listed by **Story ID** with the corresponding Alert Score in parentheses, as well as the total number of Alerts in each Story. Click the arrow to expand the Story and view its Alerts.
5. Click on an Alert name to open its Alert View page and examine its details.
6. Click **Uncollapse Alerts by Story** to view the alerts individually and perform actions on them. Sort order is by ID number. To regroup the alerts, click **Collapse Alerts by Story**.
7. The number of Alert Stories or individual Alerts is displayed at the top of the table according Uncollapse Alerts by Story selection.
8. Use the **Alert toolbar** to access all alert actions. You can Approve, Archive, and Assign alerts to other users. Click **More** for other actions: Selecting the columns shown in the table, creating a widget from the data, creating a scheduled report, and downloading a report.

7.3.6.1 Alert PCAP

TIV allows users to save the .pcap file of each alert raised for in depth analysis. This capability is configurable during setup in the **Store Raw Data (PCAP) option**. After the Save PCAP capability has been set up, users can selectively choose which alert PCAPs are of interest and then click on the **Download Capture** icon  .

- To download the packet, navigate to the alert's Alert View page and click **Download Capture**.

For more details, see section 7.3.7.6.

7.3.6.2 Alert Indicators

The **Alert Indicators** are shown in the **Alert Score** area of the **Alert View** page, as shown below:

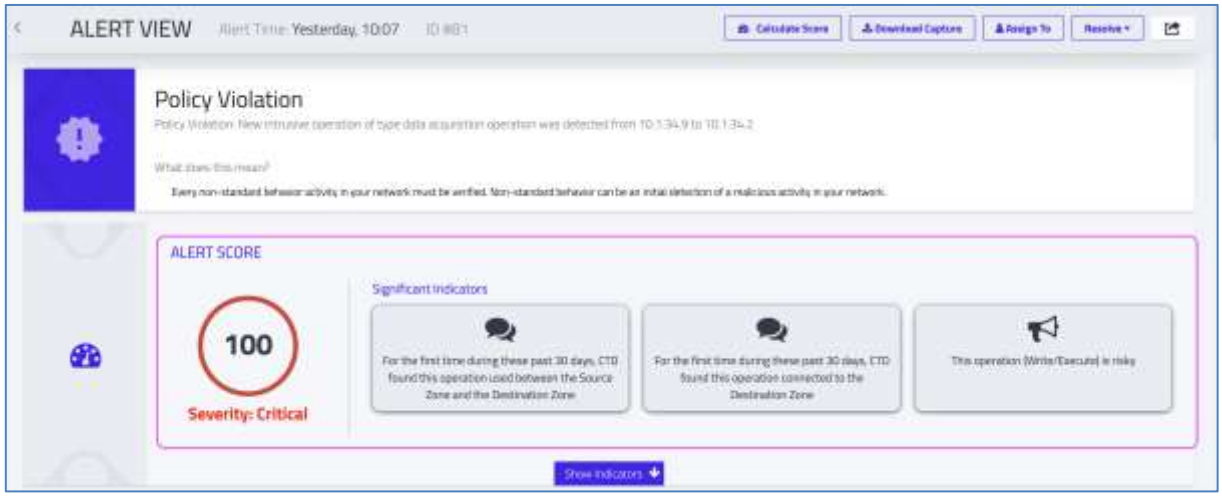


Figure 87 Indicator in the Alert Score Area

- The Significant Indicators are shown next to the alert score, with icons representing each of the alert indicator types:

Figure 88 Alert Score - Significant Indicators

- A maximum of three **Significant Indicators** are displayed. Out of all the evidence detected, these indicators are those most relevant for investigating the alert. Note these are not necessarily the ones with the highest score.
- Additional indicators are provided to show more details about this alert. Each indicator is assigned a different weight, representing its relative contribution to the total score points in the alert.
- Clicking **Show Indicators** Show Indicators displays the full set of indicators. After the alert is seen in context, it allows the user to view the alert score and severity level. This list of indicators includes two types of indicators: static and event indicators. Static indicators consist of static information that can potentially affect the score of an alert such as the asset type, subnet or virtual zone group. Event indicators consist of dynamic information, such as related network activity, that can potentially affect the score and provide context to the given alert.
- Toggle between **Show Indicators** Show Indicators and **Hide Indicators** Hide Indicators as needed.

Figure 89 Alert Score - List of Indicators

> Note: When the indicators reach a score over 100, the alert score is capped.

Other relevant information is provided by some of the indicators, even if they do not directly contribute to the score.

Alert Indicators for Repetitive Alerts in Training Mode

We auto-approve repetitive alerts when the system is in training mode (by using an indicator); this will decrease the number of duplicate alerts in the system.

Description: This alert has been repeated several times in the last 14 days with no rejection from the user while the system is in training mode.

To see the alert indicators:

1. Go to **Alerts** and click on an alert.
2. From the **Alert View** page, look under the **Alert Score** section.
3. Click on Show Indicators.

All the parameters in the alert indicator configuration:

- Enable/disable the feature
- number of days to check (days before)
- number of repetitive alerts

Figure 90 Repetitive Alerts

Supported alert types: Failed login, Configuration Download, Configuration Upload, Monitor Debug, Online Edit

Calculate Score

Users can prompt the system to calculate/recalculate using the **Calculate Score** button:

Figure 91 Alert Score - Calculate Score

By default, the alert score is automatically calculated. When needed, press **Calculate Score** to recalculate the alert score; this will also update the Indicators. A recalculated score affects the overall score of the alert and will take the context of the previous alerts. For example, an alert on a query to the PLC for the first time will appear as risky, but if it is supposed to repeat every day, then you can recalculate the score and it will appear as less risky.

7.3.6.3 Root Cause Analysis

The alerts are displayed with Root Cause Analysis, made of a chain of interrelated events. This timeline consists of a series of events that provide rationale behind the network and asset behavior. Admins can control the sensitivity level that differentiates alerts from notifications. The chain of events indicates when the score has been impacted by network activity or other related behavior.

Root cause analysis is found on the **Alert View** page in the area underneath the Alert Score. The following chain of events shows an example of a series of Known Threat Alerts:

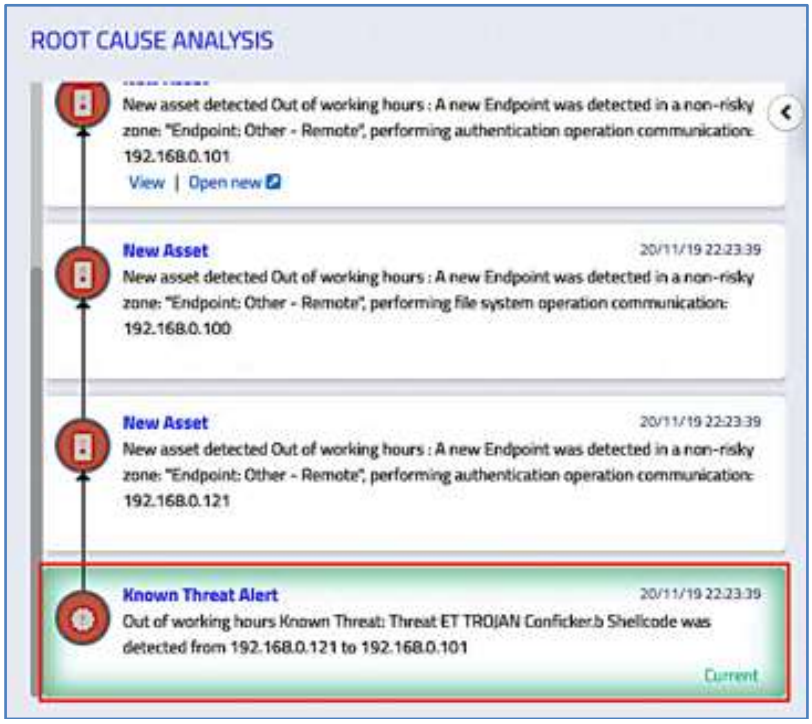


Figure 92 Root Cause Analysis: Known Threat Alerts

RCA gives users a picture of a suspected attack. This 'zoom out' perspective attempts to expose the overall attack path by highlighting related events that could enhance our understanding of the suspicious activity.

The alert's chain of events are those the system has identified, analyzed, and determined to have influenced the alert and its score. With this detailed information, users can investigate the attack, including actions that preceded the alert.

The timeline of the chain of events appears in descending order. An alert may include the chain of events, whether or not the score is qualified.

> Note An alert with no relevant events does not have a chain of events.

7.3.7 Alert Workflow

Critical and High alerts are the most crucial alerts to resolve. The other alerts are considered notifications and have a lower severity.

Most of the alerts will only be raised when the system is in Operational mode.

7.3.7.1 Resolving Alerts: Assign/Approve All/Approve Selected/Archive

Resolving Alerts in Bulk from the Alerts Page

1. List the alerts individually by clicking **Uncollapse Alerts by Story**.
2. Select the checkboxes of the alerts on which to perform a bulk change.

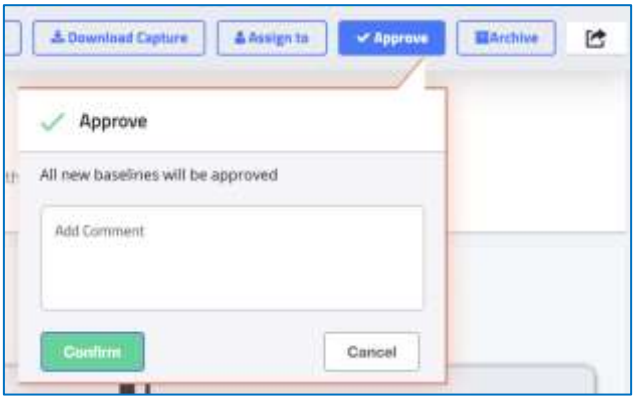
Resolving an Individual Alert from the Alert View Page

In the **Alert View Page**, the following options appear on the top right of the page for each alert:

Figure 93 Alert Options for an Individual Alert

Decide how to resolve the selected alert from the following options:

- **Assign to** – Click to delegate the alert to another user for investigation and resolution.
- **Approve** – Click when the activity that caused the alert is legal and valid communication, such as a newly-installed asset. Approving an alert as a valid change validates only the observed activity. In some cases, it is added to the baseline:



- **Archive** – Click to **Archive** the alert when the cause is *not* acceptable or is *not* a legitimate network communication. The information is archived; it is not added to the baseline.

Resolving Policy Unmatched Violation Alerts

In addition to **Assigning** a Policy Violation on the **Alert View** page, there are three options for resolving this type of alert:

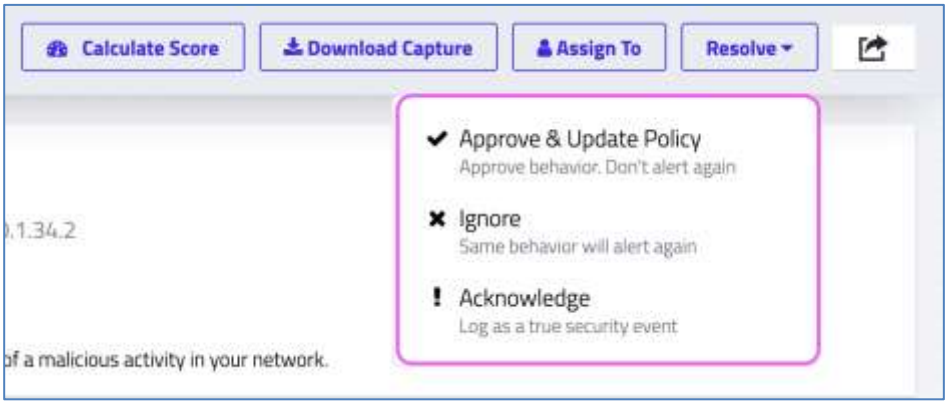


Figure 94 Resolution Options for Policy Unmatched Violation Alerts

- **Approve & Update Policy** - This means you are approving communication behavior. You are asked to approve the suggested rule(s) to be added to your policy (to prevent them from raising alerts) (See Figure 95).
- **Ignore** - Choose this when the event reported by the alert was expected or accepted as a one-time event that you are aware of. In this case, no change to the policy is required, and resolving the alert is logged as 'Alert Ignored'
- **Acknowledge** - This means the alert is signaling a real security event. You will want to continue being alerted on such events in the future, so no change to the policy is required. The result is the same as in the 'Ignore' case. However, in this case, the resolving of the alert is logged as a true security event for auditing purposes.

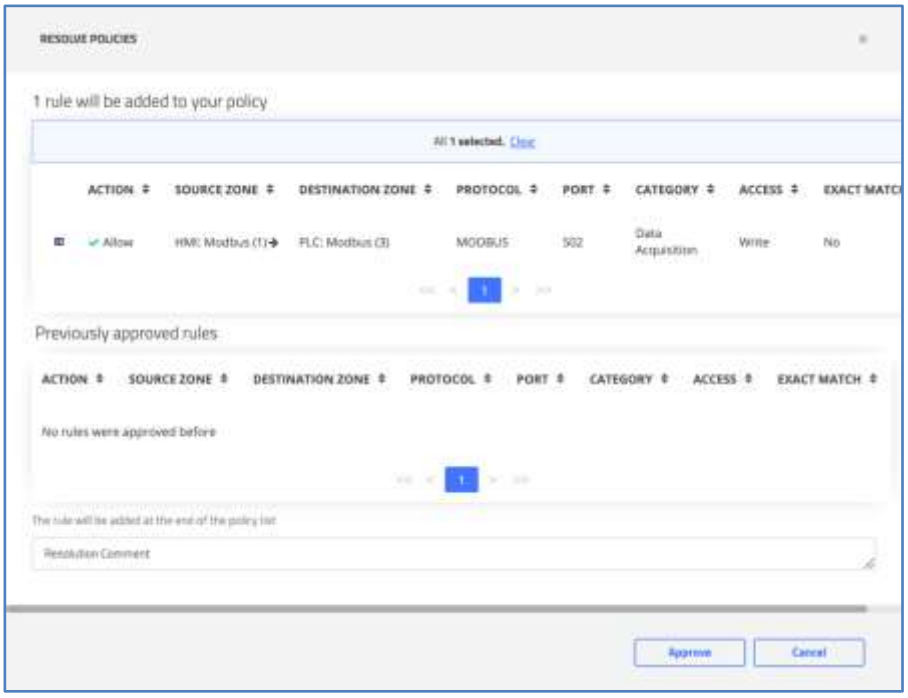


Figure 95 Approving & Updating a Policy

> **Note** In the case of approving a New Asset alert, you can uncheck all suggested rules, and still approve the alert. Doing so will result in the approval of the new asset itself, but without any change to your policy, which can result in a future Policy Unmatched Violation alert when the newly approved asset is communicating again.

7.3.7.2 Mitigating Alerts

Mitigation steps show how to respond to and resolve each alert. These mitigations guide SOC and OT engineers during investigation. The mitigations include instructions for avoiding future alerts of each type. For example, with a security alert, the mitigation steps may include how to secure the environment.

Refer to the **TIV Reference Guide: Alerts & Mitigation Table** for more information.

7.3.7.3 Viewing All Events in an Alert

Drill down to reveal all events collected that comprise the current alert.

- Click Event Details  from the Alert View page.

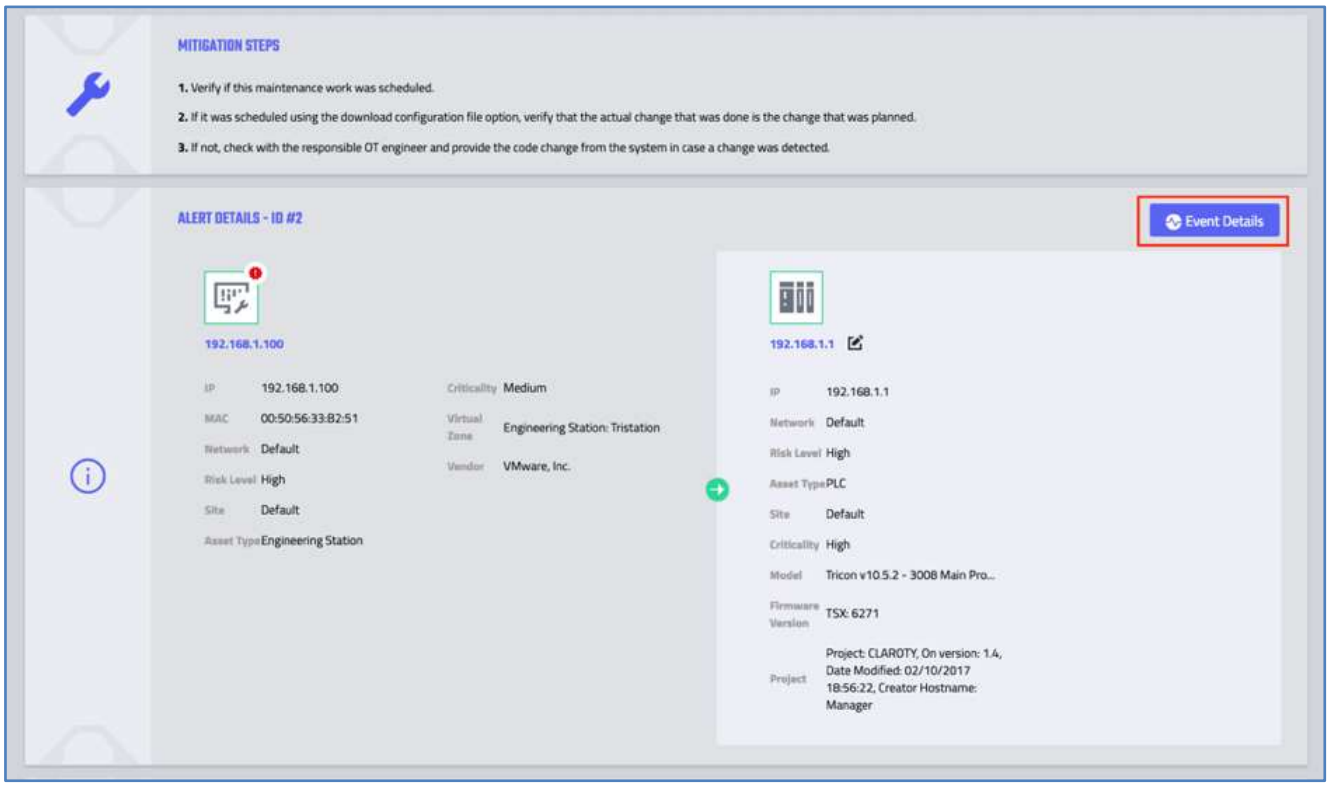


Figure 96 Event Details

- The **Event Details** pop up appears:

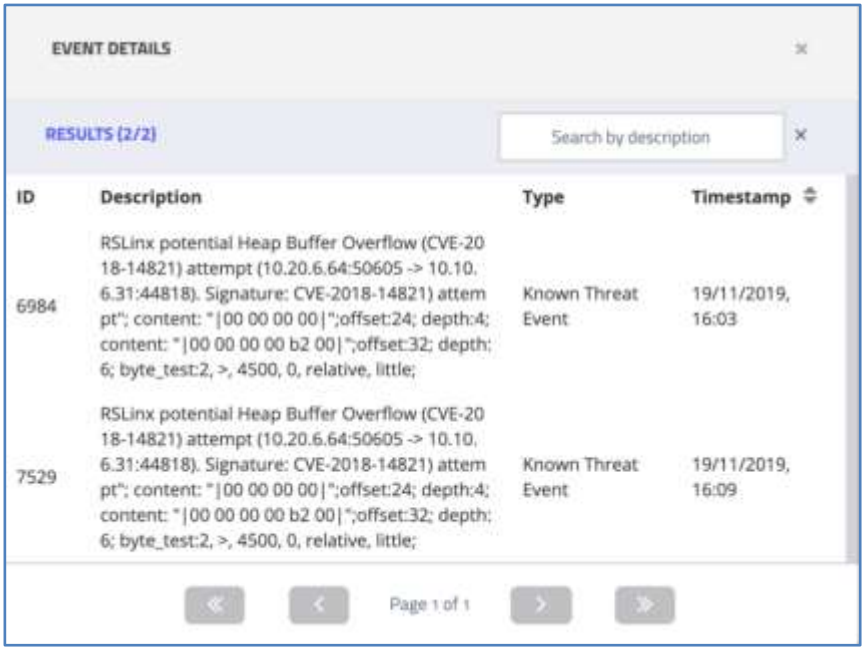


Figure 97 Event Details

7.3.7.4 Searching for an Event in the Event Details dialog

Use the **Search by Description** field  to search for an event (see Figure 97). This can be useful for forensic purposes.

7.3.7.5 Exporting Alerts

To export alerts:

1. Navigate to the top right corner of the Alert View page:

Figure 98 Alerts - Export Button

2. Click **Export**  to export this alert for investigation.
   - The **Download Report** popup appears:

3. Select the report format: **CSV** (default) or **PDF**.

Figure 99 Download Report

4. Select whether to include **Events** and/or **Activities** in the report.
5. Click Download.
   - The report is downloaded to your browser:

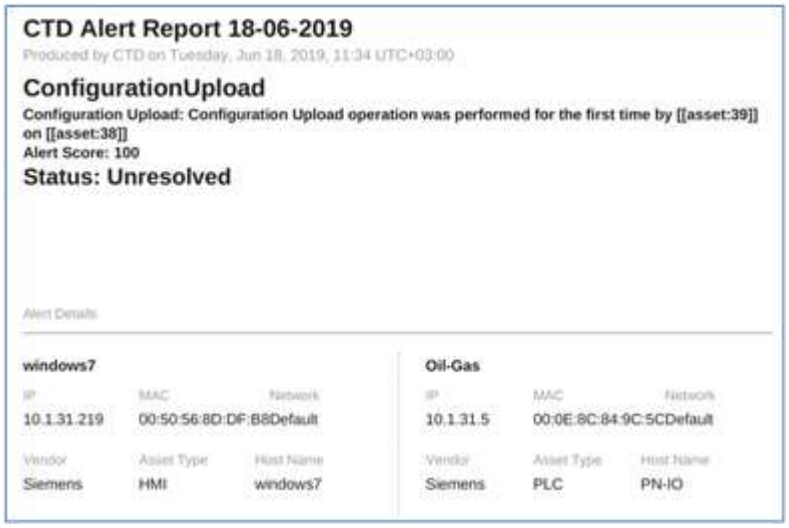


Figure 100 Cover Page of Alert Report in PDF Format

> Note: TIV supports the export of up to 1K alerts with the pdf format.

7.3.7.6 Downloading Capture - Raw Alert Data

When the packet capture file is preserved for an alert, it is available for download in PCAP format from the **Alert View** page.

Figure 101 PCAP download

- Click the **Download Capture** icon 

:

  This packet capture file includes raw information of the current alert for investigation. This icon only appears when there is an available PCAP file.

> Note Saving the PCAP file is configured by the Admin via the Save CAPs checkbox (refer to the *Admin Manual*).

- If the PCAP file was not saved, this icon is greyed out and appears with a tooltip: 'No capture file was recorded.'

7.3.8 Creating Your Own Alerts (Custom Alerts)

7.3.8.1 Admin Alert Rules

To view alert rules:

- Navigate to **Threat Detection > Rules**.

Note that Administrators can set various Alert Rules to approve or archive alerts without any user input automatically.

7.3.8.2 Baseline Rules

Admins can configure baseline rules from the Baseline Rules page. See configuration details in section 7.6.

7.3.8.3 Yara Signatures

Users can create their own custom network traffic monitoring rules based on Yara rules. These rules provide matching of patterns found on data blocks extracted from network traffic. The network traffic rules feature allows the user to manually disable or enable any existing network traffic signatures supplied by the system.

TIV extracts data from TFTP, SMB, HTTP, and code sections. This allows TIV to provide the user with more advanced signatures, targeting newer threats without the need for overall system upgrade. The user can create custom rules using a Yara pattern language.

7.3.8.4 Network Signatures

Network Signatures are another TIV capability. These network traffic rules allow users to disable or enable any existing network traffic signatures supplied manually.

Users can create their own custom network traffic monitoring rules based on Snort rules, similar to Yara rules, using a Snort pattern language.

See configuration details in section 7.6.

7.4 Events

A log of **all** the events logged by TIV's engines are displayed in the Events page, regardless of whether they are considered alerts that might impose a risk.

The Status of each event can be risky (an **Alert** or an **OT Alert**) or not (a **Non-Risky Change** or an **OT Operation**). Clicking a risky event opens an Alert View page, and clicking a non-risky event opens a Master Event View page, where groups of interrelated events are displayed.

7.4.1 Events Page

To access the Events page, navigate in the menu to **Threat Detection > Events**. The Events page appears as shown below.

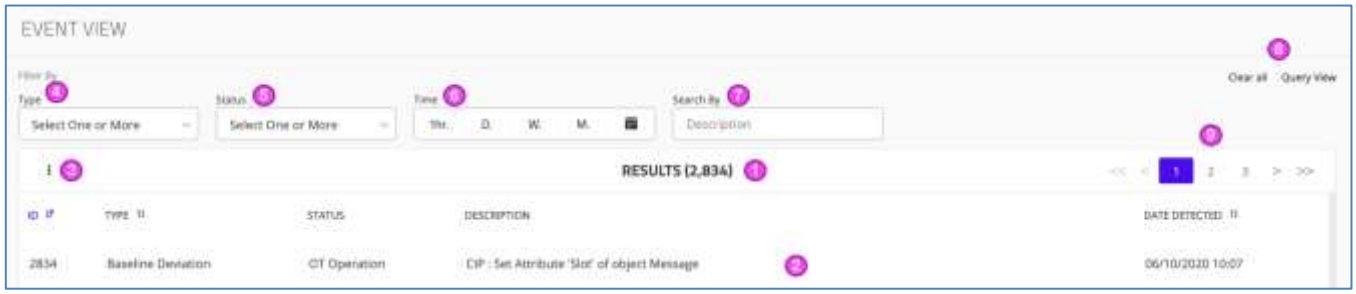


Figure 102 Events Page

1. The **Event Results** shows the total number of events logged. It dynamically displays a table of *all* events generated by TIV's engines, regardless of whether they are considered alerts that might impose a risk.
2. Each row of the table displays the event **ID**, the event **Type** detected (e.g. Configuration Download, Login, Known Threat Alert), its **Status**, a high-level **Description** and its detection **timestamp**.
3. To add the **Site** column to the table, click the **More**  icon, select **Selected Columns** from the menu, click Site and click **Apply**.
4. The **Type** filter allows multiple selections of the available Alert Types.
5. The **Status** filter lets you filter for **Alerts**, **Non-Risky Changes**, **OT Alerts** and **OT Operation** events or a combination of them:

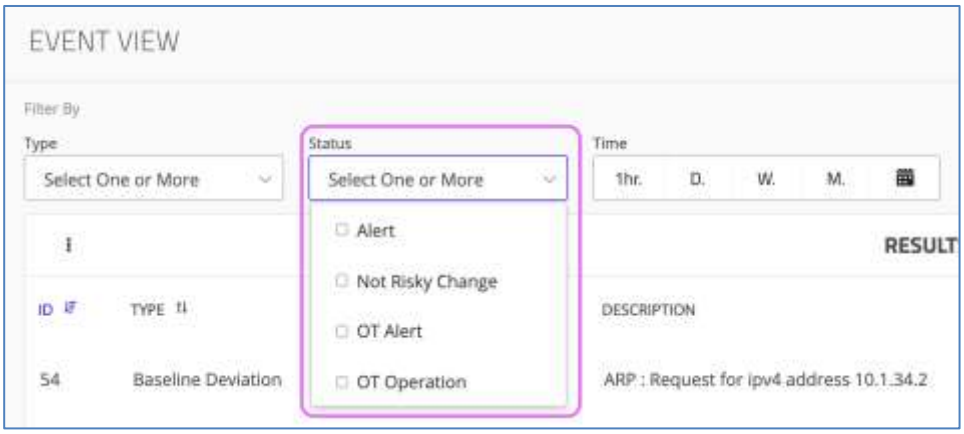


Figure 103 Event Status dropdown

- Clicking an event's **ID** leads to the Event view that displays information of any correlated events:

- In the case of a risky event (Events with **Alert** or an **OT Alert** statuses), selecting the event **ID** leads to the relevant Alert Page to access all the controls for managing and investigating the alert.
- For events classified as having no risk (i.e. events Status of **Not Risky Change** or **OT Operation**), selecting the event ID leads to the relevant Event for investigation.

6. Select a **Time** frame for the Event Results to display: During the past Hour/Day/Week/Month or any user-defined period.
7. Use the **Search by** field to search for an event by part of its **Description**.
8. Use the **Clear All** and **Query View** controls to adjust the display as needed.
9. Use the **Page Controls** to navigate through the pages of the Event table.

7.4.2 Master Event View

Related events are assembled into a Master Event. The Master Event View contains a chain of related events with an alert score.

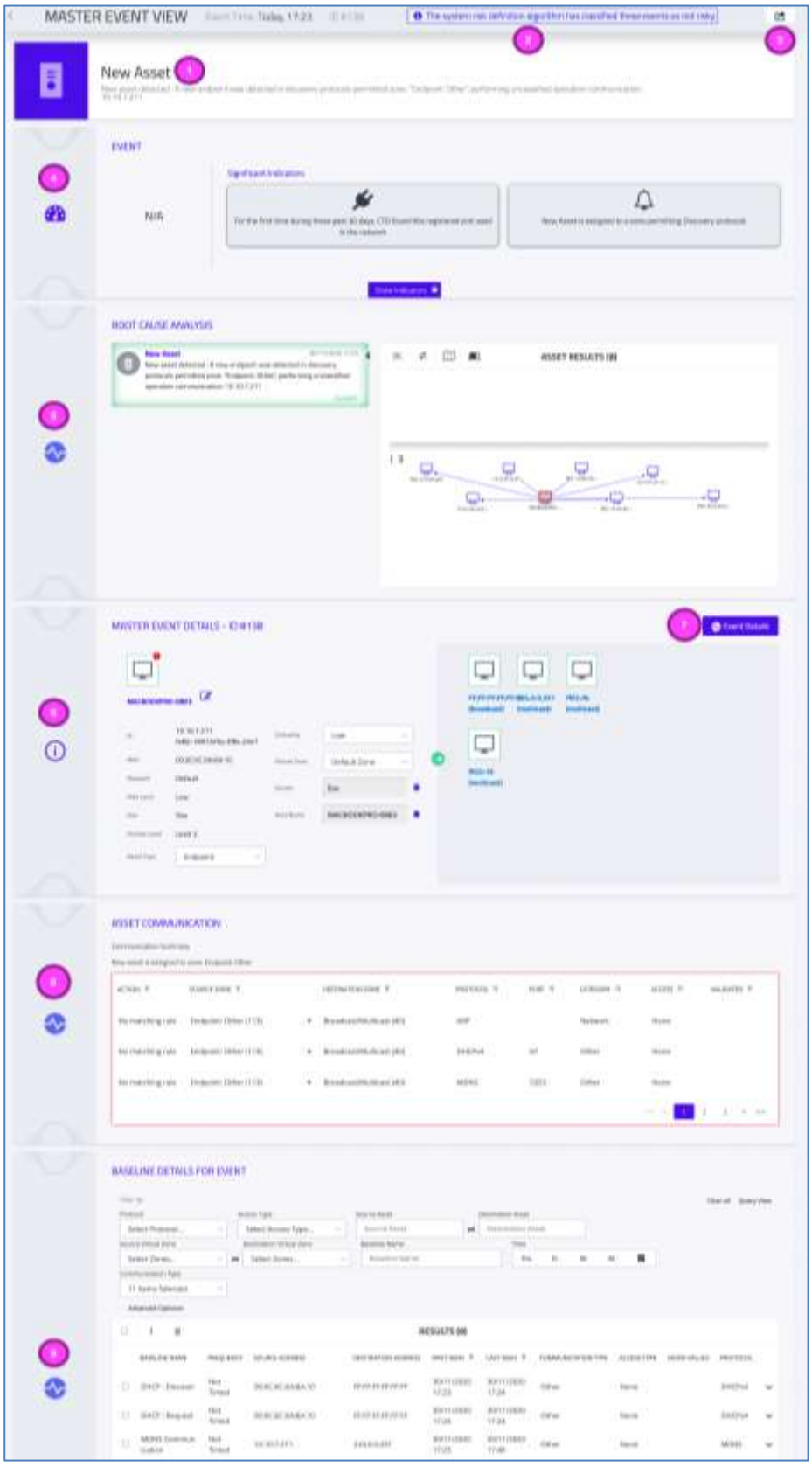


Figure 104 Master Event Details for a New Asset

1. Name of the event and its description. Above is the timestamp of the event.
2. The Master Event header displays the following:

   The system risk definition algorithm has classified these events as not risky

> Note This Event occurs when the sensitivity value that differentiates notifications from alerts determines that the current event is not interesting or relevant enough to be classified as an alert.

3. Click **Export** to generate a report for this event in PDF or CSV format, and choose to include **Events**, **Activities,** and/or **Baselines**:

Figure 105 Downloading a Report for a Master Event

4. The **Event** area provides metadata of the event:
   - The event is shown without a Score since this is a non-risky event.
   - The Significant Indicators are displayed.
   - Click **Show Indicators** to view additional event indicators. For further details see section 7.3.6.2.
5. The **Root Cause Analysis** shows the chain of events leading up to every single alert, which is essential for OT security alerts. It enables fast and easy triage of alerts, as well as proactive threat hunting. By providing the context surrounding the associated threat and risk, these details help users hunt for threats and resolve security events. For further details, see section 7.3.6.3.
6. The **Master Event Details** provide metadata of the event, such as the primary asset involved. The right side of the **Master Event Details** page shows the details of a secondary asset/s involved in this event.
7. Click **Event Details** to view details of the Master Event. Each row of the table displayed provides an **event description**, its **ID**, **type** and **timestamp**. A window is provided for text searches of the event descriptions instead of browsing through the Event Details results.
8. When applicable, the **Asset Communication** area appears for the event. This section provides a communication summary and details of any Virtual Zones impacted.

9. A section with all the **Baseline Details** for the event is populated when applicable. This table features filters for all aspects of the event and each communication type.

7.5 Zone Rules [Only Admins]

7.5.1 Overview to Zone Rules

This mechanism provides a high level of accuracy for fine-tuning the system's communication rules using a familiar, easy-to-use interface, similar to a firewall management interface.

When transitioning into operational mode, zone rules are applied to the network traffic. At this point, you can manage the rule list and customize it as needed. You can review, delete, validate, or modify the out-of-the-box zone rules or create new ones based on specific needs.

You can:

- Create and control zone rules with an intuitive interface
- Apply a rule validation process to allow Admins to review and validate newly created rules
- Investigate and resolve Policy Violation alerts, using the context provided by the matching of detected communication to existing rules, and quickly understand which rule was responsible for each generated alert or which rule is required to prevent an alert from being generated again in the future.
- Resolve an alert by updating its rule, based on new rule suggestions made by the system.

> Note: All the automatically created Zone Rules are zone-based and are mutually exclusive.

7.5.2 Zone Rules Page

The **Zone Rules** page displays a table similar to the one shown below, enabling you to see all rules in a firewall-type management interface. The view allows for creating, reviewing, validating, modifying, or deleting policy rules.

To view the Zone Rules page:

- Navigate to Threat Detection > **Rules > Zone Rules** in the main menu.

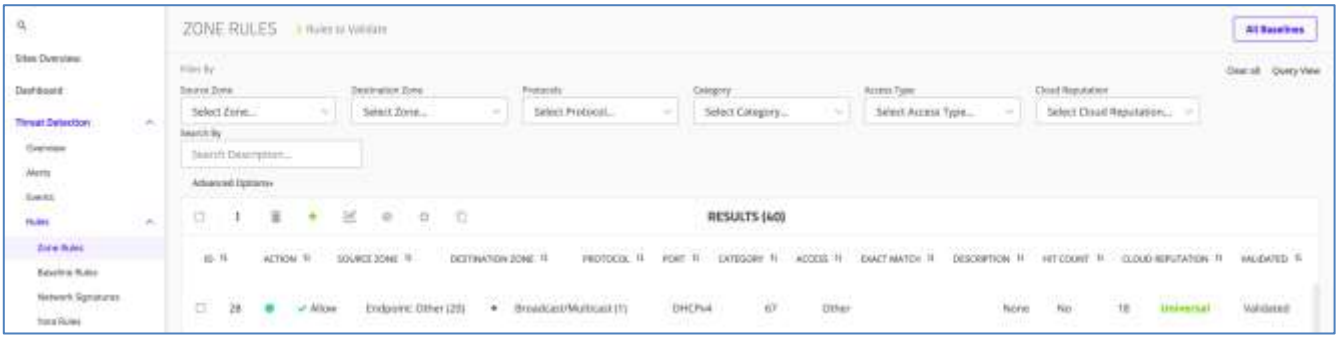


Figure 106 Zone Rules Page

See Table 4 Policies Grid: Default Columns for the Policy Rules parameters.

> Note: The **Baseline Deviation** alert has been deprecated and replaced with a **Policy Violation** alert.

7.5.3 Zone Rule Behavior

The Zone Rules behave as a set of logical conditions set upon the network traffic detected. When conditions are met, the system responds by taking one of the following actions:

- **Allow** – When the conditions of the zone rule are met and the action is set to "Allow", the system *does not* trigger an alert.
- **Alert** – When the conditions of the policy rule are met and the action is set to "Alert", the system triggers a **Policy Rule Match** alert.

The policy includes an implicit default "**Alert on anything**" rule (not visible in the Policy Rule list). In operational mode, if the detected communication did not match any of the existing rules, the system matches the **Alert on Anything** rule, which will trigger a **Policy Violation** alert.

A **Policy Violation** alert is triggered when none or only some of the conditions set in the Policy Rules do not match the parameters of the incoming network traffic.

> Note The action to be taken is configured by Administrators.

7.5.4 Policy Alert Types

The two types of Policy alerts are as follows:

- **Policy Rule Match** – This occurs when the detected communication matches an explicit policy rule defined with an 'Alert' action.
- **Policy Unmatched Violation** – This type of alert is triggered when the detected communication was not matched to any rule with an 'Allow' action,

and as a result, the implicit "Alert on Anything" rule was hit. This means there was no pre-existing policy rule for such communication.

In case the system detects a new asset, a **New Asset** alert will be triggered. If the new asset's communication is not already addressed in any existing policy rule, the system will suggest a rule to be added to approve the new asset's communication.

The system will suggest a zone for the new asset and a change in policy based on asset communication.

By definition, when a Policy rule is created, it is in an invalidated state. Only Admins can validate a rule.

For details on validating rules, see section *7.5.5*. For instructions on bulk editing see section *5.6.2*.

7.5.5 Zone Rules Columns

The table below describes the columns available in the Zone Rules grid. You can sort the results by clicking any column header.

Table 4 Policies Grid: Default Columns

Column Name	Description
ID *	Identifier of the Policy Rule. Each Policy Rule is automatically assigned with this unique number as it is created.
(Active)	Whether this Policy Rule has been enabled Green means the rule *has* been activated
Action *	Whether this Policy Rule allows or will trigger an alert
Source Zone *	The name of the source of this virtual zone
Destination Zone *	The name of the destination of this virtual zone
Protocol	The protocol/s used in the communication between the source and the destination zones (can accept multiple protocols)
Port	The port/s through which the communication flows for this rule (can accept multiple ports)
Category *	The categorization of this asset, such as Protocol, Programming, Network, Data Acquisition, etc.
Access *	The type of access this asset is allowed: Read, Write, Publish, Execute, None (uncategorized). This field can accept multiple access types.
Exact Match *	Whether the policy's communication should exactly match (Yes) or not (No), including the Baseline Description (which must be identical).
Description *	User-defined description of this policy rule
Hit Count *	The number of communications that matched (hit) this rule

Column Name	Description
Cloud Reputation *	Indicates the rule's prevalence among different sites. The Cloud Reputation classifications are as follows: • Rare - This policy was rarely seen in different site networks • Uncommon- This policy was seen in a small amount of our site networks • Common - This policy was seen in a large number of our site networks • Universal - This policy was seen in most of our site networks
Validated *	Whether the policy rule has already been validated or is not set to be validated Validate.

The table below describes the additional columns to display in the Zone Rules grid.

Table 5 Zone Rules Grid: Additional Columns

Column Name	Description
Created By	The username of the user that created this rule
Created On	The date and timestamp of the creation of this rule
Last Modified	The latest date and time that this rule was modified
Last Modified By	The username of the user that last modified this rule
Last Validated	The latest date and time that this rule was last validated
Validated By	The username of the user that last validated this rule

- To add additional columns to the Zone Rules table, click the **More** button in the toolbar and click **Select columns.**
- Choose additional columns to display from the Select Columns dialog and click **Apply**:

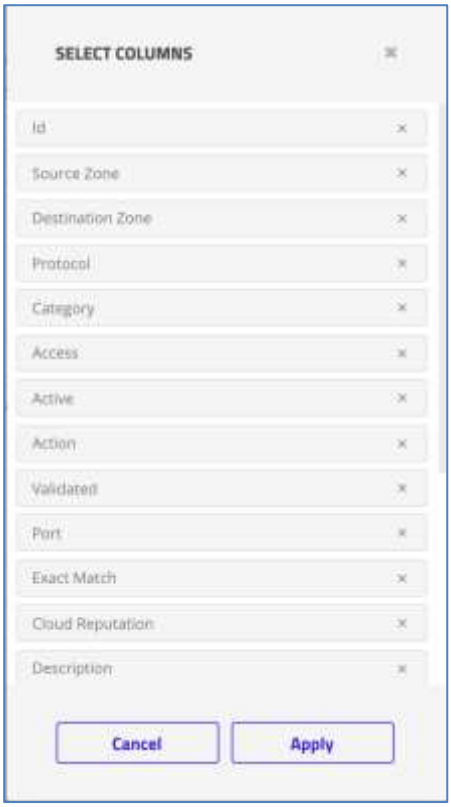


Figure 107 Select Columns Dialog

7.5.5.1 Creating a New Zone Rule

To manage your system effectively, you can create as many new zone rules as needed, or edit existing rules, as shown below. To create a new rule, select the **Create New** + button from the Zone Rules toolbar:

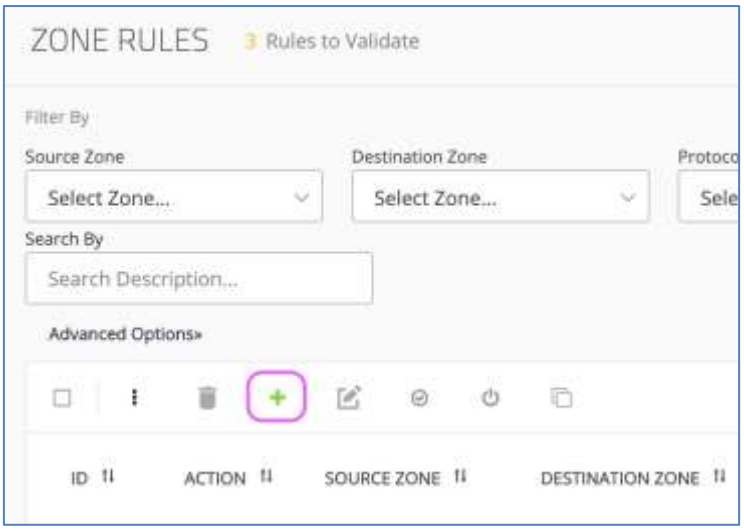


Figure 108 Create New button on the Policy Rules toolbar

The **Add New Alert Policy** dialog appears:

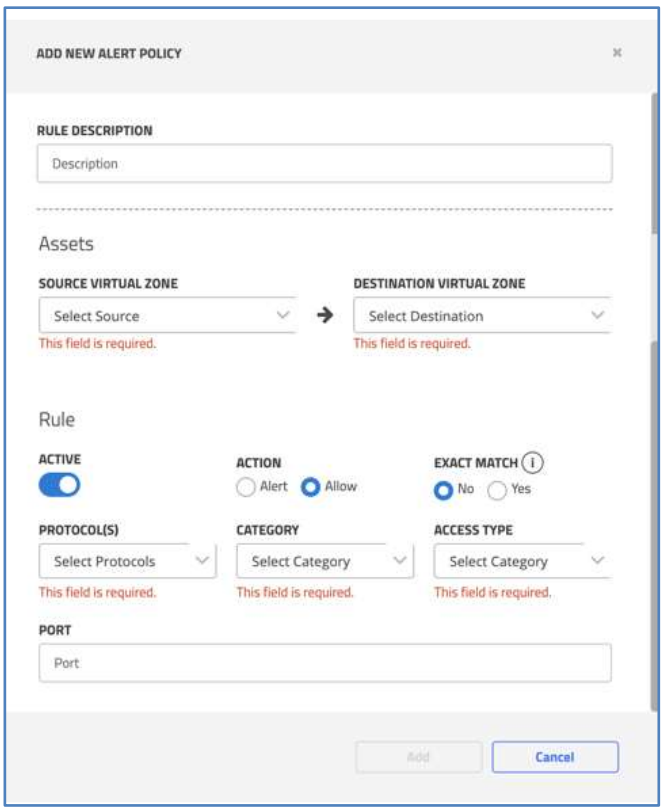


Figure 109 New Alert Policy dialog

To incorporate the new alert policy rule, define its characteristics:

- **Rule Description** – Provide an explanation of this rule to be easily identified in the future or by other users.
- **Source Virtual Zone** of the communication
- Destination Virtual Zone of the communication
- **Active** – By default, the rule will be activated. Slide this button to the left if you prefer to deactivate the rule.
- **Action** – By default, the rule is allowed. If otherwise, select the Alert button.
- **Exact Match** – By default, the rule does not require an exact match. If otherwise, select **Yes**.
- **Category** – A drop down list of communication categories. You can choose multiple categories, e.g. Diagnosis, Authentication, and Programming.
- **Access Type** – The type of access permitted for this communication. Select one of the following: Read, Write, None, Publish, Execute
- **Port** – The communication port(s) specified by the rule. You may specify multiple ports if required.

Click **Add** to commit the new policy rule.

7.5.5.2 Editing an Existing Rule

To edit an existing rule, select it from the list and click **Edit Rules**:

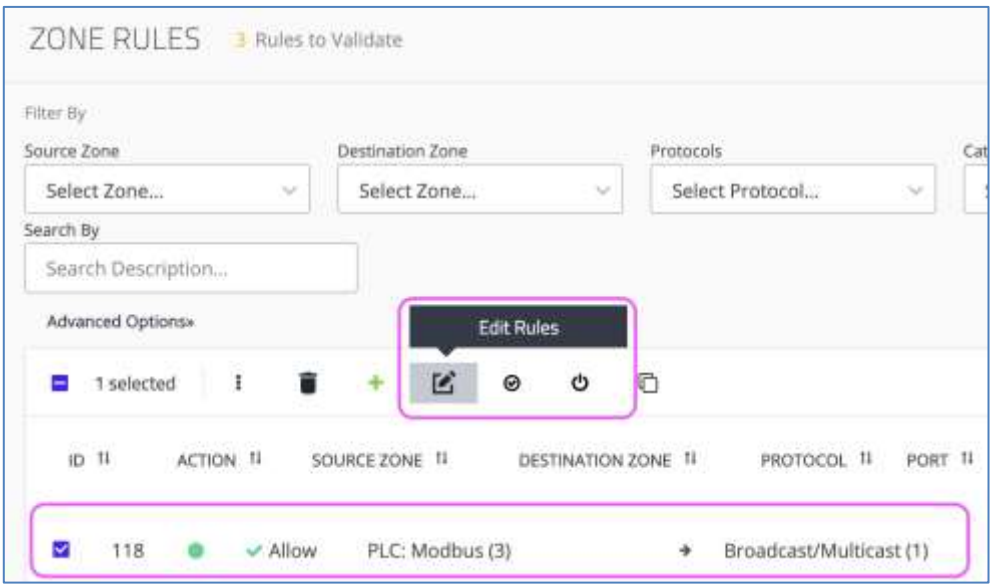


Figure 110 Edit Rules

The **Edit Alert Policy** popup appears, enabling editing of the rule parameters which are the same as the New Alert Policy dialog above (see Creating a New Zone Rule 7.5.5.1):

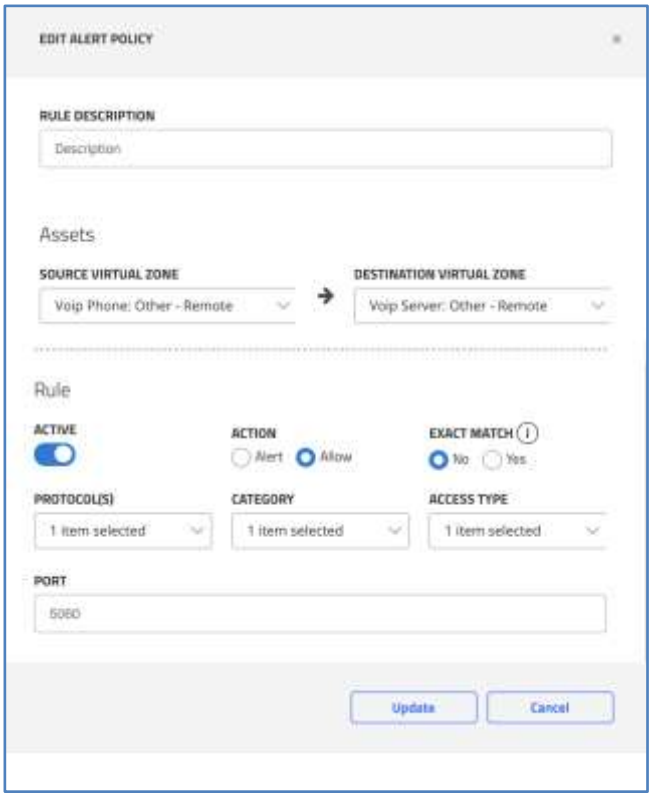


Figure 111 Edit Alert Policy dialog

7.5.5.3 Reviewing and Validating New Zone Rules

Policies are unvalidated by default until the admin validates them. After the system moves to operational mode, the admin can choose to validate a Zone Rule or leave it unvalidated. Zone Rules govern communication in the network that the system has learned while in training mode. The admin can validate all of them at once or manually validate them. If the behavior is learned, then you probably want to validate all rules. When a new policy is found in the system, a policy violation alert will show and need to be approved. Every new policy triggers a policy violation in operational mode.

If there is a policy violation and if not validated, there will be an alert. This represents a different communication that was not learned and an anomaly in the network. A new alert can be approved or not approved on the alert page and validated or invalidated on the policy page. Unvalidated rules are policy violations and will trigger an alert.

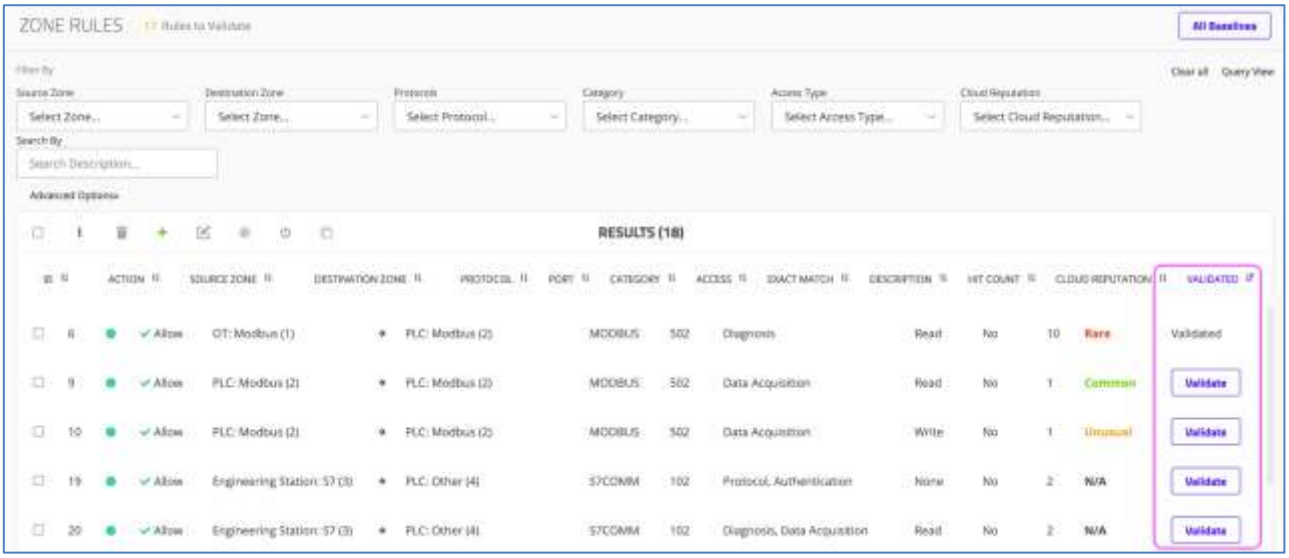


Figure 112 Zone Rules page with rules pending validation

7.6 Baseline Rules

Baseline Rules are a type of alert you can create based on changes to, or activities within, Baselines. For example, you might want to be alerted when the baseline "TCP from any port to port 5000" appears.

Baseline Rules can be viewed and edited from this page but are created in Baselines. See section 8.7.

7.6.1 Editing a Baseline Rule

To edit a baseline rule:

1. Navigate to **Threat Detection > Rules > Baseline Rules**. The Baseline Rules page appears:

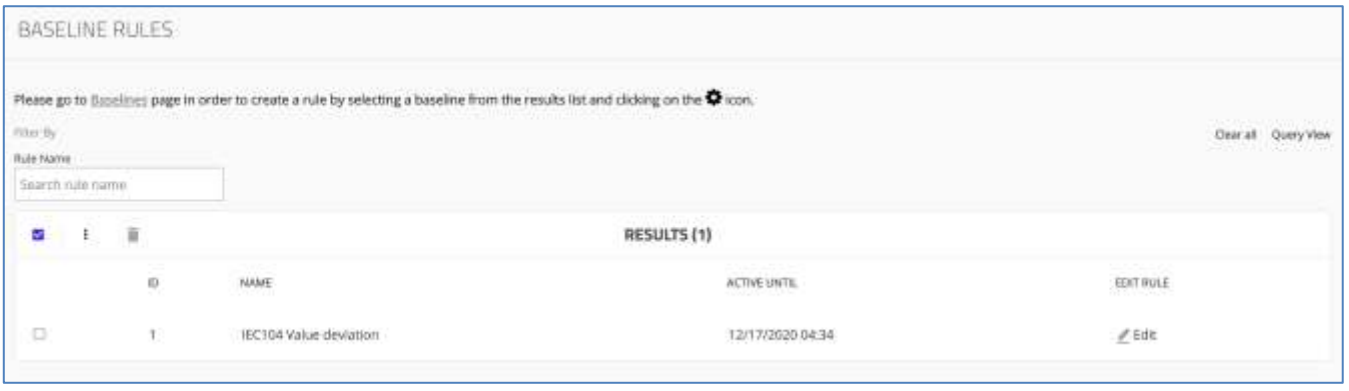


Figure 113 Baseline Rules Page

2. Select a rule and in the Edit Rule column, click **Edit**.

The Edit Baseline Rule dialog appears:

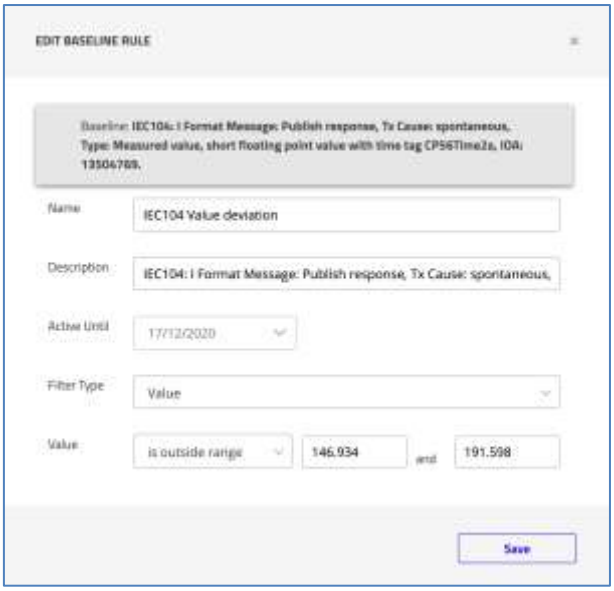


Figure 114 Edit Baseline Rule Dialog

3. Make changes as needed as described in section 7.6.2 - Creating a Baseline Rule.

7.6.2 Creating a Baseline Rule

Baseline Rules are created in the Baselines page.

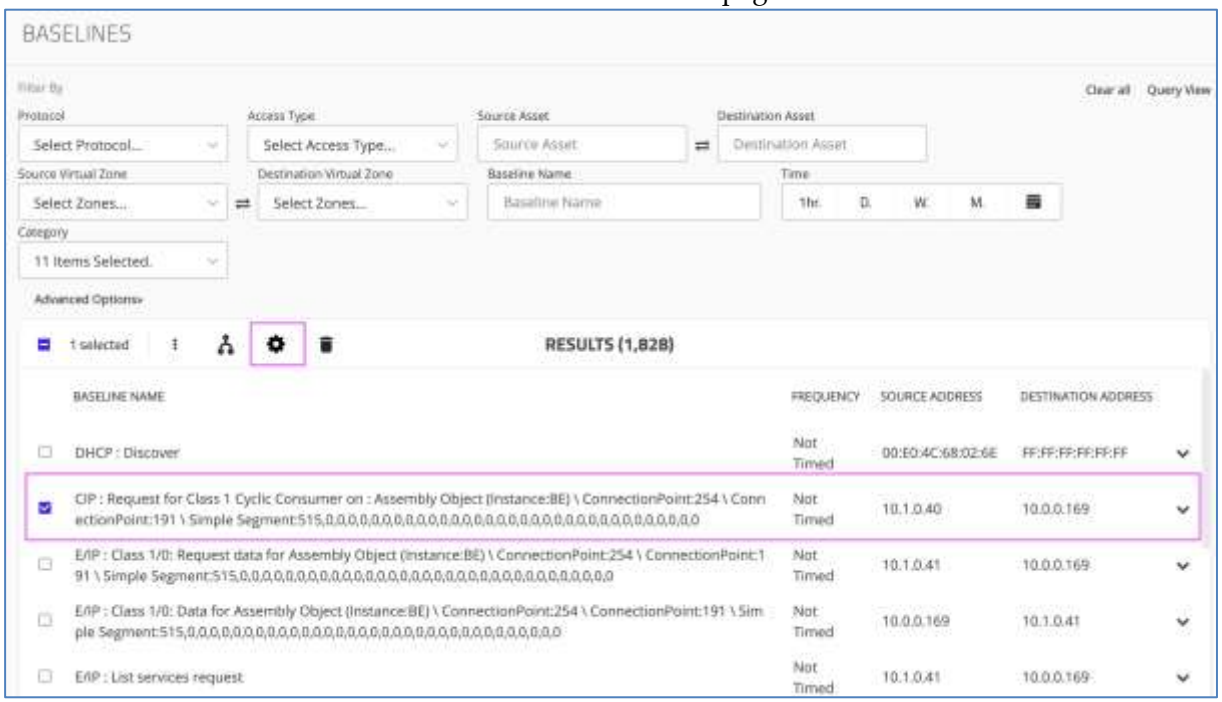


Figure 115 Selecting a Baseline from which to create the rule

To create a baseline rule:

1. Navigate to **Investigation > Baselines**
2. Select the relevant baseline from which you want to create the rule.
3. Click the **Create Rule** button.

   The Create Baseline Rule dialog appears:

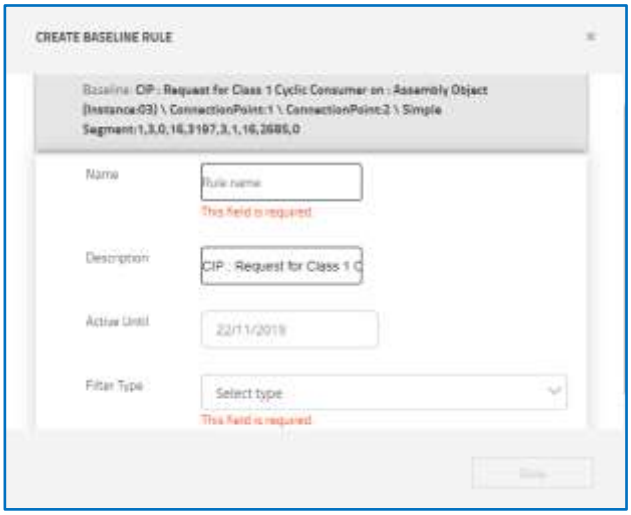


Figure 116 Create Baseline Rule popup

4. Provide the following details for your new baseline rule:
   - **Rule Name** – Provide a name for this rule
   - **Description** – This field is populated from the baseline name and can be changed as needed
   - **Active Until** – The duration (date and time limit) for this rule to apply
   - **Filter type** – Determine when the new alert will be triggered:
     - **Inactive for** – Select this type if you want to deactivate the period for this alert, and define its duration (the default is set for 1 minute):
     - **Upon appearance** – An alert will be raised when this baseline appears and meets the condition, whether or not there is a baseline deviation.
5. Click **Save**. The rule is added to the Baseline Rules page.

See section 7.6.3 for defining Baseline Rules using Baseline Values.

7.6.3 Baseline Rules using Baseline Values

Baseline values can be used to construct a rule to create an alert.

Preconditions

Before using this feature, make sure you have the following:

1. In the Advanced Network Settings in the **Settings** > **Data Sources** > **Interface Configuration,** the administrator has enabled Show Protocols by sliding the Show Protocol Configuration menu in the Interface Configuration Page button to the right (see Figure 261).

Warning: These settings can have a critical impact on the system and therefore should only be used by an Administrator in coordination with Tripwire Support.

2. The checkbox is selected for enabling IEC 101 in the **Settings** > **System Management** > **Deployment Configuration** > **Protocols** page (see Figure 262).
3. The Admin identified an existing baseline to use as the basis for defining the baseline rule which already includes relevant IEC 101 data with minimum and maximum values.

Steps

1. To define a baseline alert to be triggered on a certain value condition, follow the same baseline rule creation steps as in section 7.6.2.
2. Then in Filter Type select **Value** and enter the desired condition:

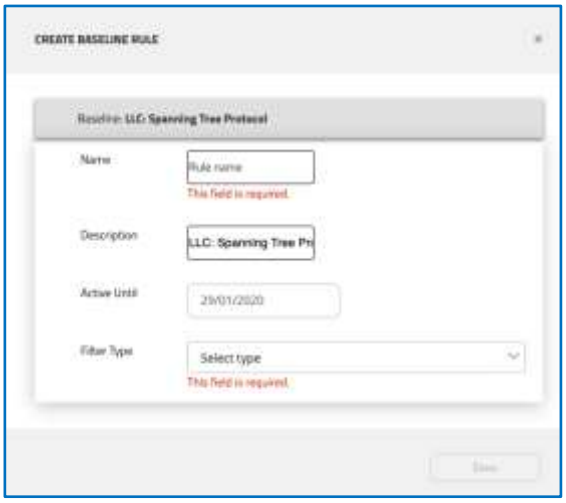


Figure 117 Setting a condition for a baseline rule

- **Filter Type** – Determines when the new alert will be triggered.
- **Value** – Sets the criteria for the deviation.

The condition is displayed in the Baseline view.

When a Baseline Alert occurs, it is displayed as follows:

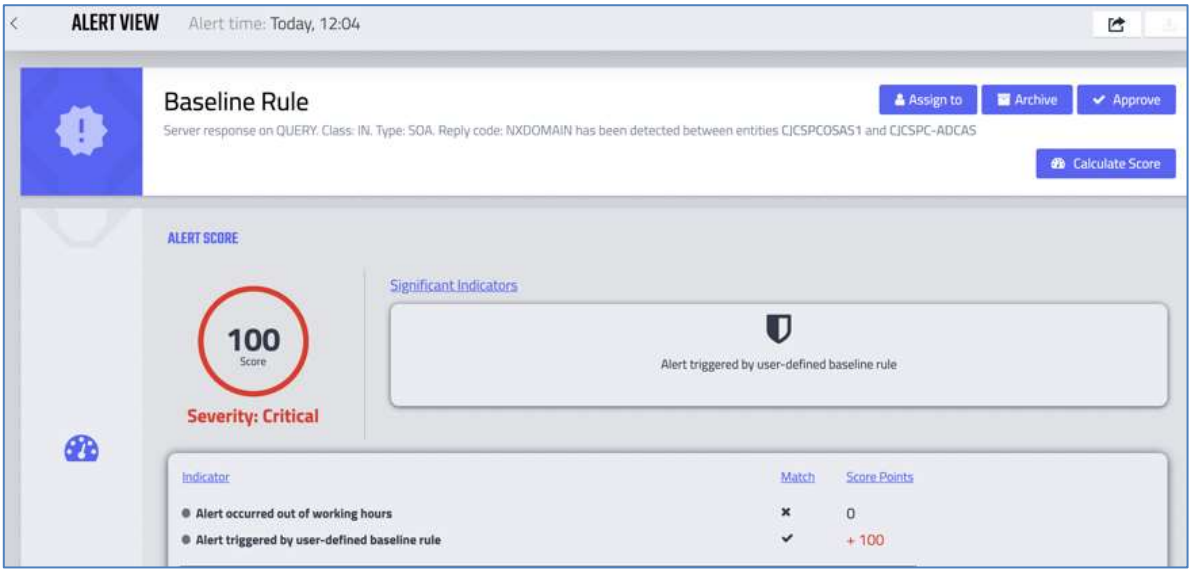


Figure 118 Baseline Rule Alert

7.7 Before Working with Network Signatures and Yara Rules

Before working with Yara or Network Signatures, ensure that your environment is set up for sniffing with 'Known Threat Detection' enabled on the specific network you are working on, as shown below.

To sniff 'Known Threat Detection':

1. Navigate to **Settings > Data Sources > Interface Configuration**.
2. Click **Advanced Network Settings** and turn on **Known Threat Alert Detection**.

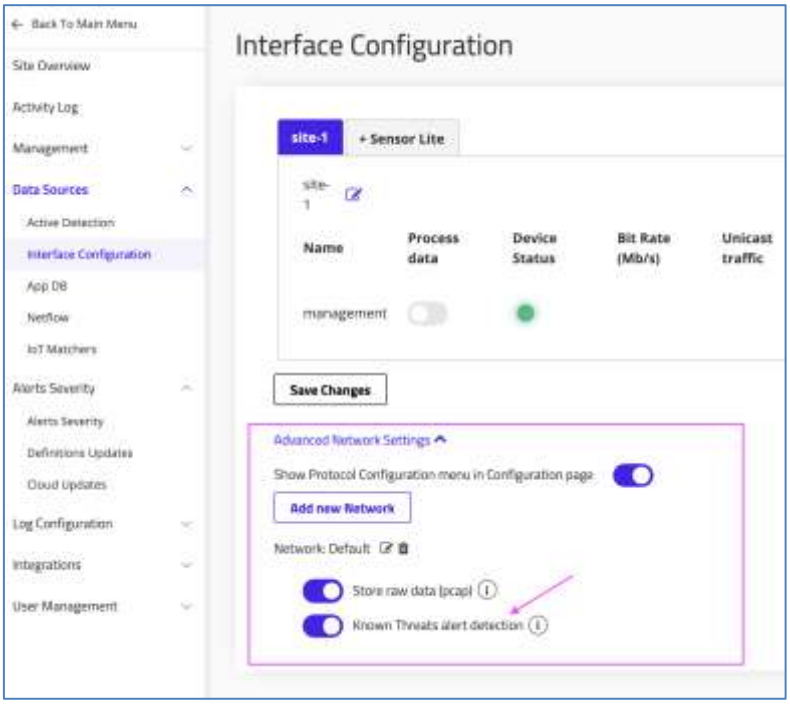


Figure 119 Configuring Known Threat Alert Detection

7.8 Network Signatures

To access network signatures:

- Navigate to **Threat Detection > Rules > Network Signatures**.

  The **Network Signatures** page appears as follows:

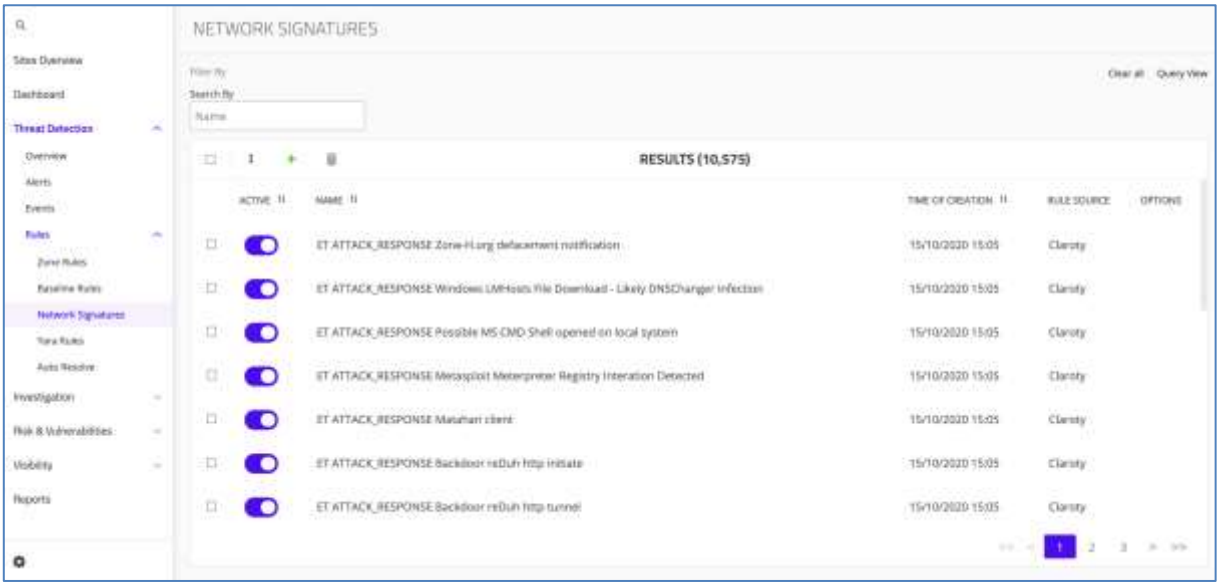


Figure 120 Network Signatures

7.8.1 Adding a new Network Signature Rule

1. Click **Create New**  in the toolbar to create a new Network Signature rule.

   The following dialog box appears:

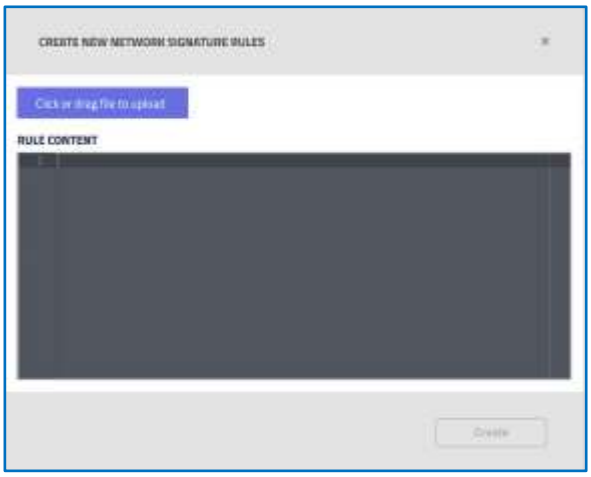


Figure 121 Network Signatures - Creating New Rules

The behavior of the Network Signatures form is the same as the Yara Signatures section.

You can edit any of the network signatures that you have provided under rule content.

7.9 Yara Rules

7.9.1 Working with Yara Rules

To work with Yara Rules:

- Navigate to **Threat Detection > Rules > Yara Rules**.
  - The list of installed Yara rules is displayed as shown below:

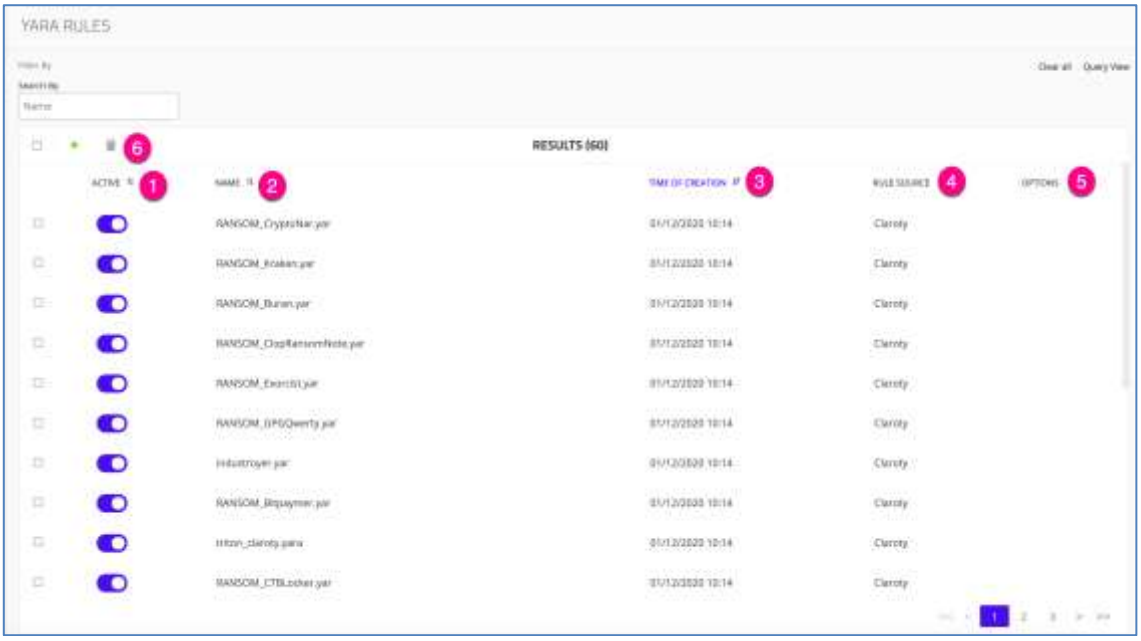


Figure 122 Yara Rules

The **Results** grid displays the Yara rules, listed with the following default sortable columns:

1. **Active** button – The default value is Active . Click this button to **Deactivate** an existing Yara rule.
2. **Name** – The name of this Yara rule
3. **Time of Creation** – The timestamp of when this rule originated
4. **Rule Source** – Whether the source of the rule is from the system (TIV) or is user created. System Rules can be disabled but you cannot edit or delete them.
5. **Options** – When a Yara rule is editable, the **Edit** icon appears in this column.

In addition:

6. The toolbar contains options for adding new Yara Rules and deleting selected ones. See sections 7.9.2 and 7.9.3 for details.

7.9.2 Adding a New Yara Rule

1. Click **Create New** in the toolbar.
   - The Create New Yara Signature Rule is displayed:

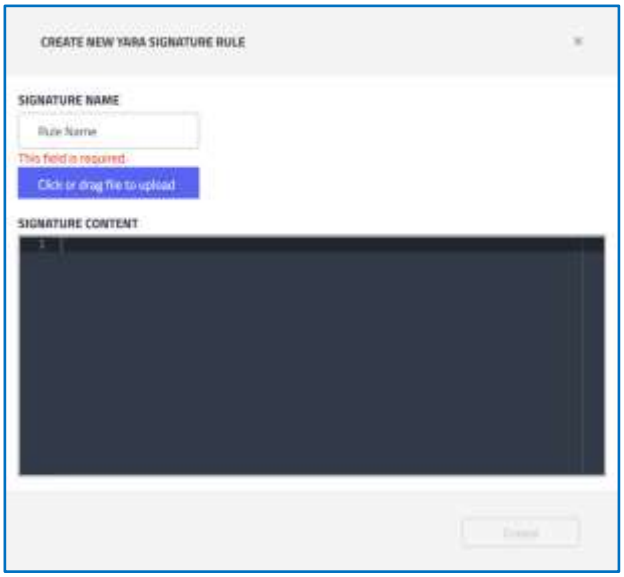


Figure 123 Creating a new Yara Signature dialog

- The dialog prompts you to:
  - Enter a **Signature Name** for your new Yara Rule
  - Click or drag the Yara signature file itself

  The content of the signature will be displayed in the main window.
  - Click **Create** to upload the Yara signature file

7.9.3 Deleting a Yara Rule

To delete a Yara rule:

1. Either select the row of the Yara Rule from the list of Results, or search for part of the string of the Yara Rule name in the **Search By** field.
2. Click **Delete** on the toolbar to remove the Yara Rule/s.
3. Before deleting any rules, the system requests confirmation of the deletion.

When a rule is modified, the system shows a message on the lower right corner of the screen indicating if it was deleted or not.

7.9.4 Yara Rule Example: Suspicious File Transfer Alert

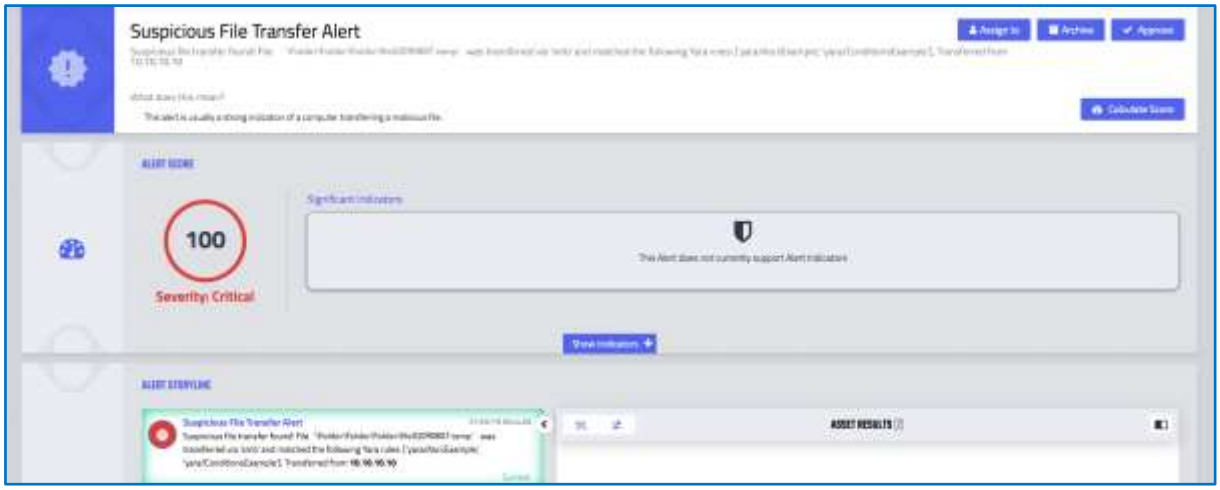


Figure 124 Yara Signature Example

7.10 Auto Resolve

To view the Auto Resolve tab:

- Navigate to **Threat Detection > Rules > Auto Resolve**.

  The **Auto Resolve** page appears as follows:

Figure 125 Auto Resolve Rules Tab

7.10.1 Creating Auto Resolve Rules

1. In the toolbar, click **Create New**  :

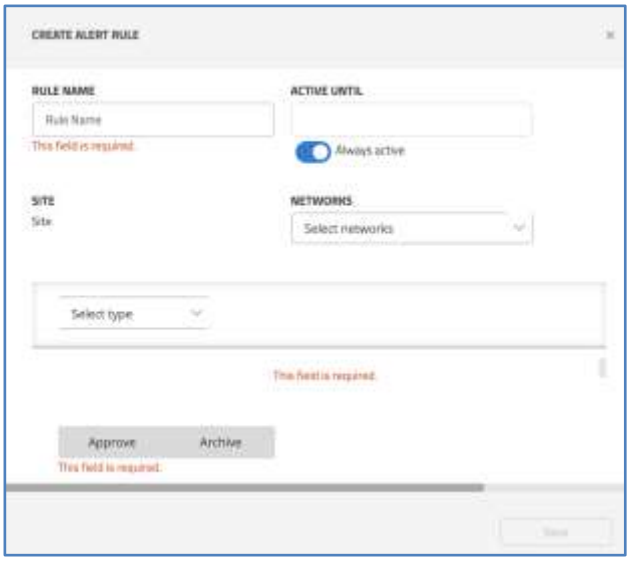


Figure 126 Create Alert Rule Dialog

2. Choose a name for your new rule in the **Rule Name**.
3. Specify the time limit for your rule in the **Active Until** box.
4. Select the site to which the rule applies from the **Site** dropdown list. Once you select a site, the **Networks** box opens.
5. Choose the applicable networks for your new rule.
6. Choose your required filters from the **Select Type** dropdown.
7. Provide criteria for defining the filter for your new rule:
8. Define the alerts/assets/baselines in which your rule applies, while selecting **Add** to provide multiple conditions.

> **Note** You can configure multiple conditions for the same rule. The rule is triggered only when all of the configured conditions apply (AND).

9. Set the required alert result: **Approve** or **Archive**.

   When all of the configured parameters apply, the system will automatically **Approve** your rule or **Archive** it.

10. Click **Save** to commit the new rule, which is listed in the Alert Rules table.
    - The row of each alert rule displays the following columns: **ID**, **Name**, **Active Until** date & time, **Action**, **Condition**, and **Edit Rule**.
    - Click **Edit** to modify a rule.
11. Repeat Steps 2 thru 11 for each rule.
12. To export the Auto Resolve rules and their conditions, select the relevant row/s. Then in the toolbar click **More** ⋮ > **Download**.

- The results are provided in a CSV file.

7.10.1.1 Auto Resolve Rules - Exception

In general, when Auto Resolve Rules are applied, they take effect on all future alerts as well as on the alerts that are already in the system, with the following exception: The Alert Types below are only supported for approving or archiving for future alerts (and not retroactively):

- Port Scan
- Network Scan
- Man-In-The-Middle (MITM)

8 Investigation

8.1 Overview

The Investigation functions of TIV are used investigate alerts or events in the network. They also give deeper visibility and tools for understanding the network and its behavior. For example, DNS Queries can be used to investigate if an external domain is being used, or to detect suspicious activities. They can also help to find configuration issues. The Network Sessions screen analyzes network traffic, giving you more insight into how your network traffic looks and your network health. Process Values enable you to investigate OT alerts and get visibility into OT asset behavior in the network.

Investigation functions are valuable not only for investigation purposes; they can help with threat hunting as well.

8.2 DNS

DNS allows you to do threat hunting to see if there is unexpected behavior on the network, to investigate previous issues in the network, or to investigate alerts.

To access **DNS** view:

- In the Main Menu, navigate to **Investigation** > **DNS.**

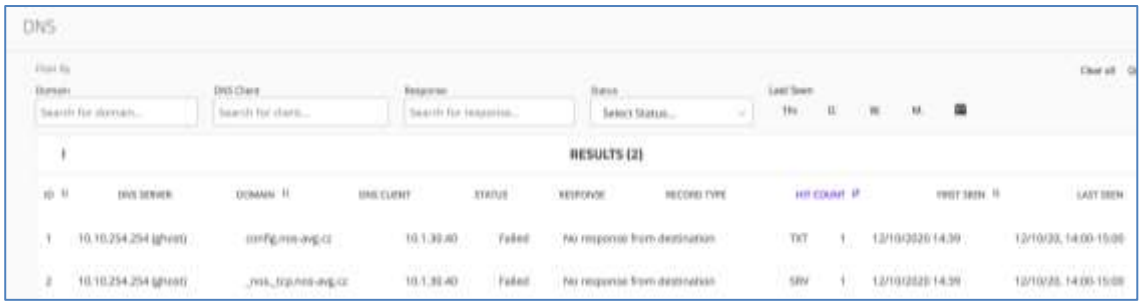


Figure 127: DNS Queries View

The DNS Queries page includes the following columns:

- ID
- DNS Server
- Domain
- DNS Client
- Status
- Response
- Record Type

- Hit Count
- First Seen
- Last Seen

8.2.1 DNS Widgets

The Visibility Overview and the Asset View page have DNS widgets that describe the DNS queries detected by the network. The widgets provide improved analyses of the network focusing on the DNS statistics:

- The number of DNS queries over time
- The names and volumes of the most frequent DNS queries
- The domains with the most assets.

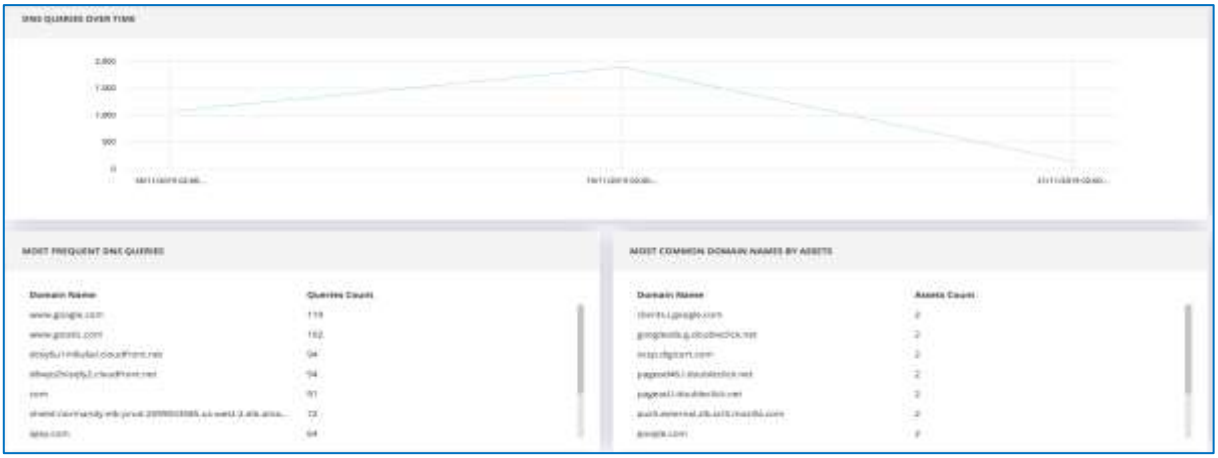


Figure 128: DNS Widgets

8.3 Process Values

TIV's Process Value tool enables sophisticated monitoring and investigation of OT processes. Based on its data and analytic algorithms, it provides visibility of the values that read, write or publish from an OT asset. For each asset you can see all the tags, their values, their access types and other vital statistics.

The Process Values can be used to combat unexpected changes that can indicate risks to process integrity and warn of an impending cyberattack.

This tool enables users to know the normal values and recognize when they are moving towards a critical state, when they are abnormal or unexpected. You might find behaviors related to a malware attack early in its kill chain or determine an operational reliability issue. One example of Process Values is temperature on a controller and observing normal behavior or any changes.

> **Note** This Process Values view is available by default, even before the user has selected any tag tracking at all.

Display according to Access Types

The order of the tags in the Process Values table is according to our recommendations for tracking tags. If a Write access type exists, it is of higher importance than the other types, and is therefore displayed at the top of the list. See below for further info on Access Types.

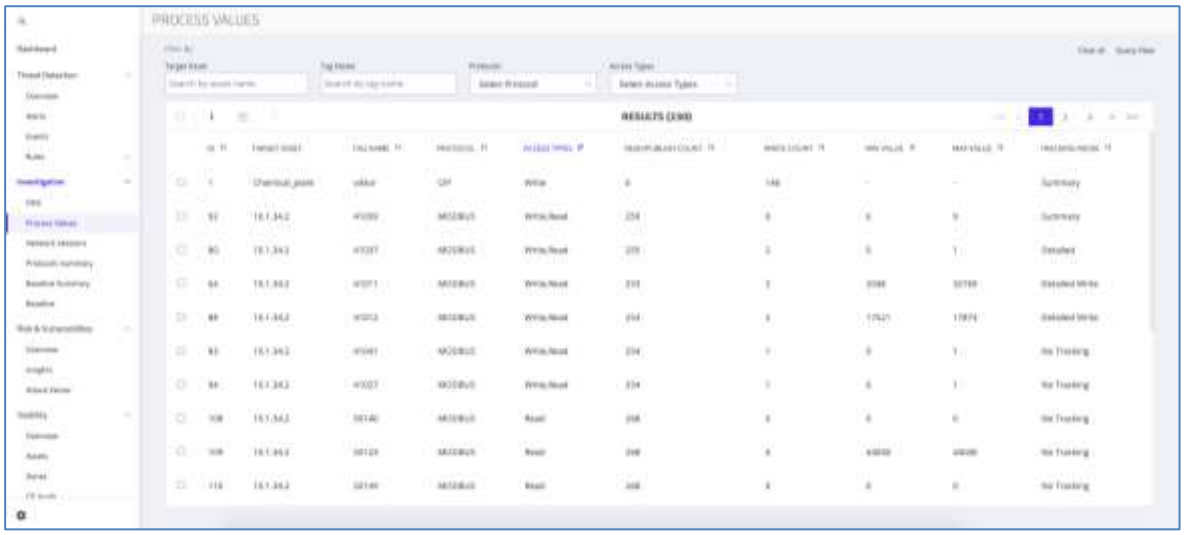


Figure 129: Investigation > Process Values

8.3.2 Viewing Process Values

1. From the Main Menu, click **Investigation > Process Values**.
2. By clicking a row, you can see a detailed screen with more info on the process value (see Figure 131).

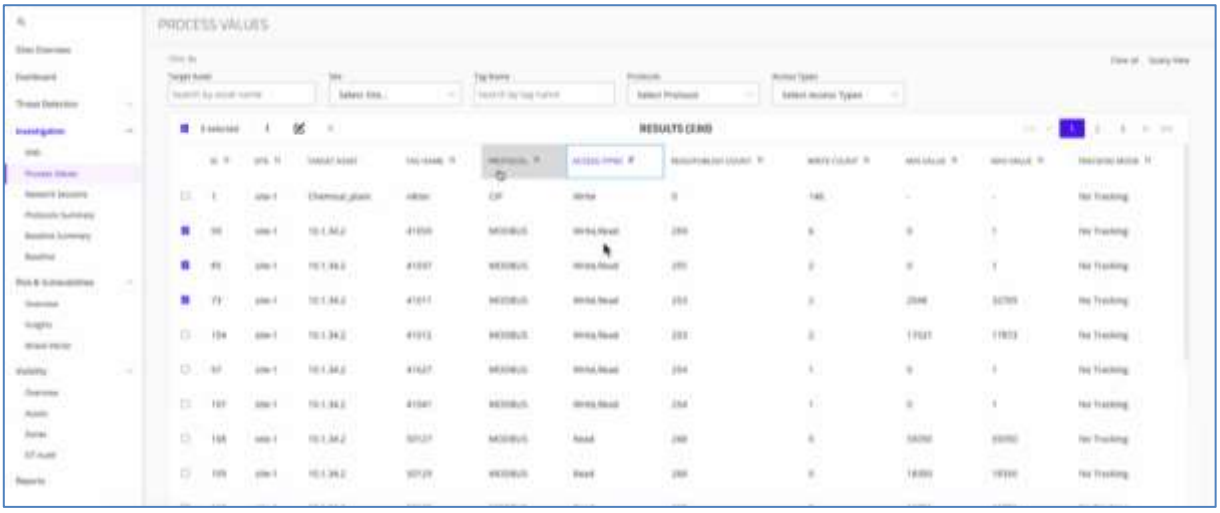


Figure 130: Process Values Table - No Tracking

The Process Value table displays the following columns by default:

- **ID** – The Process Value ID
- **Target Asset** – The target (affected) asset (e.g., a Controller)
- **Tag name** – The tag name that is related to the asset. This tag has a value.
- **Protocol** – The related protocol running on this asset
- **Access types** – The read or write to the asset
- **Read/Publish Count** – The sum of the Read/Publish requests for this tag
- **Write Count** – The sum of the Write requests for this tag
- **Last value** - The last tag value that was seen on this asset.

> Note When the following 3 fields are non-numeric, they will have no data:

  - **Min value** – The minimum tag value seen on this asset
  - **Max value** – The maximum tag value seen on this asset
  - **Average value** – The average tag value seen on this asset

Further info on tags that have no tracking

Figure 131: Detailed Process Values View: Collapsed

A screen will open on the right with a detailed page. Click the arrow on the top right corner to expand this view to the entire screen.

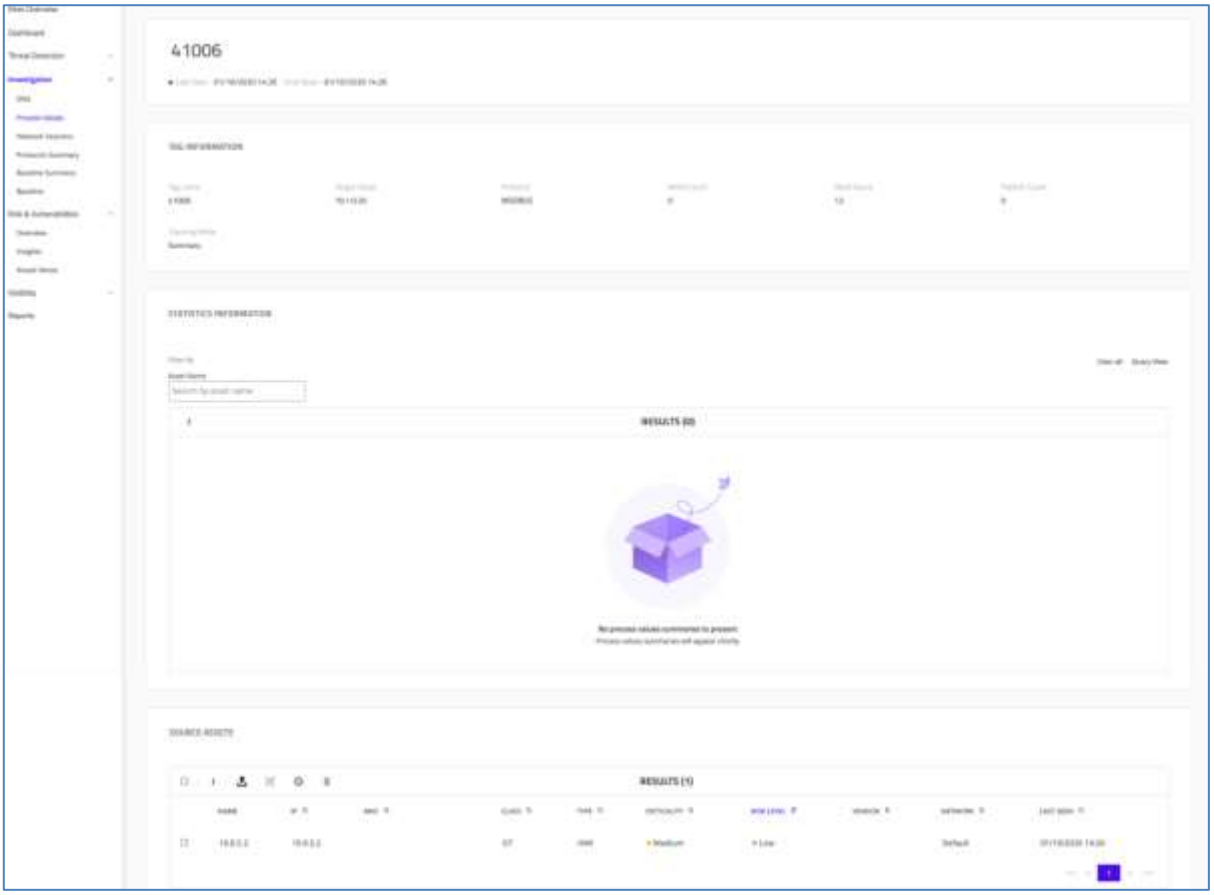


Figure 132: Process Values View: Expanded - (No Tracking mode)

The following fields appear, including:

- **Tag Information** – Includes the Tag name, the Target asset associated with this tag, Protocol, Write Count, Read Count, Publish Count and Tagging Mode as described above
- **Source assets** – The assets that communicated with the target asset and sent the read/write requests. The parameters includes the source asset **Name**, **IP** address, **MAC** address, **Class**, **Type**, **Criticality**, **Risk Level**, **Vendor**, **Network**, and **Last Seen** fields as described in Assets View, section 5.4. These assets are sorted by decreasing Risk Level.

8.3.3 Tracking Configuration

In the Tracking Configuration dialog, accessed by selecting assets and then clicking **Edit Tracking Configuration** in the toolbar, select the **Tracking mode** and **Access Type**.

Tracking Modes

Users are required to identify which tags are of interest in order for TIV to track them and collect information on them.

Figure 133: Tracking Mode dropdown

Choose from the following Process Value tracking modes:

- **No Tracking** – In this mode, there is no tracking whatsoever. The user obtains some data in the Process values table
- **Summary** – In this intermediate level of tracking, Process Values are tracked at a high level, including statistics and trends over time. If further information is needed, use Detailed tracking. The statistics are summarized on an hourly basis.
- **Detailed** – This is the most extensive type of tracking. Every detail of the process values is tracked and available for further investigation, yet it has less history than Summary tracking. This mode provides continuous tracking information in real time.

Access Types (relevant only for Detailed Tracking)

Users are required to identify and select tags that are of interest in order for TIV to track them and collect Process Value information on them.

- Select from the dropdown of trackable Access Type/s: **Write, Read/Publish**

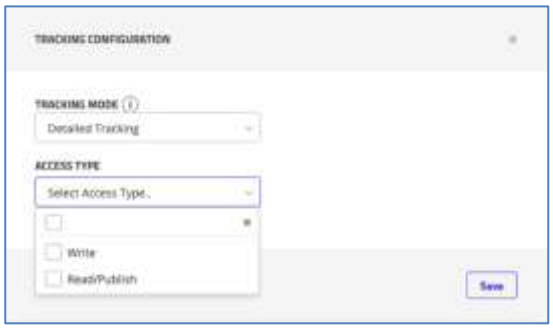


Figure 134: Access Type dropdown

> Note We highly recommend that users track **Write** access types.

8.3.4 Process Value Graph

This **Values Over Time** graph is featured in both the Detailed mode and Summary mode expanded views:

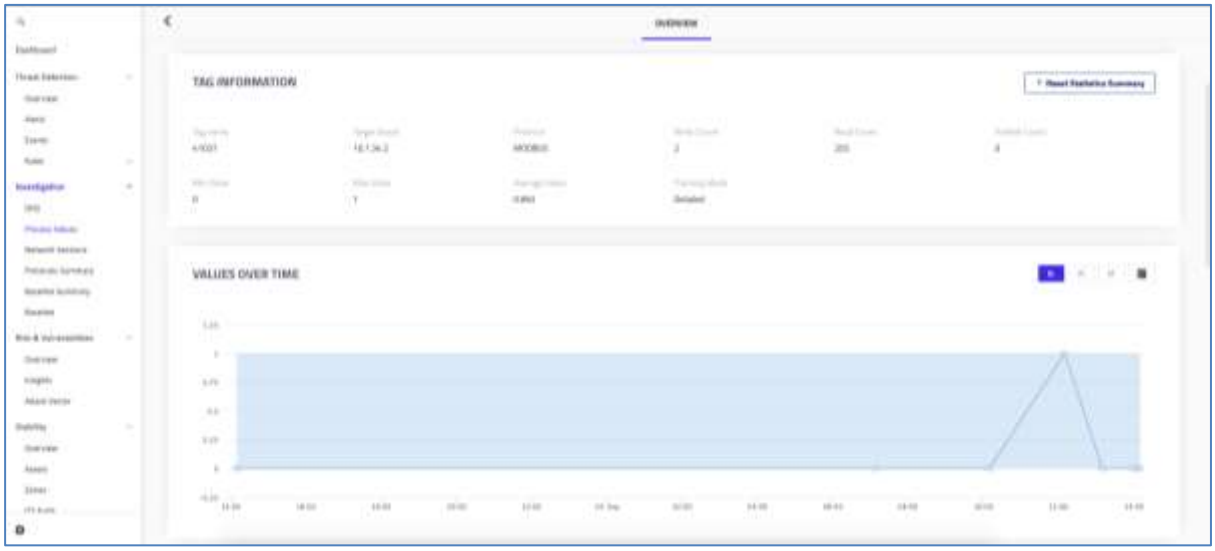


Figure 135: Timeline

This timeline graph shows two aspects: a light blue block that shows the range of values, plus an additional line graph superimposed above it:

- In Detailed mode, a timeline of the actual value in this range dynamically.
- In Summary mode, the average value is shown.

When hovering over the graph, further details are displayed, and the corresponding table is marked.

8.3.5 Summary Tracking Mode

In addition to the Values over Time graph, the Summary mode view highlights the tag information, the appropriate statistics as well as the source assets of the asset under investigation. **The statistics are summarized on an hourly basis**.

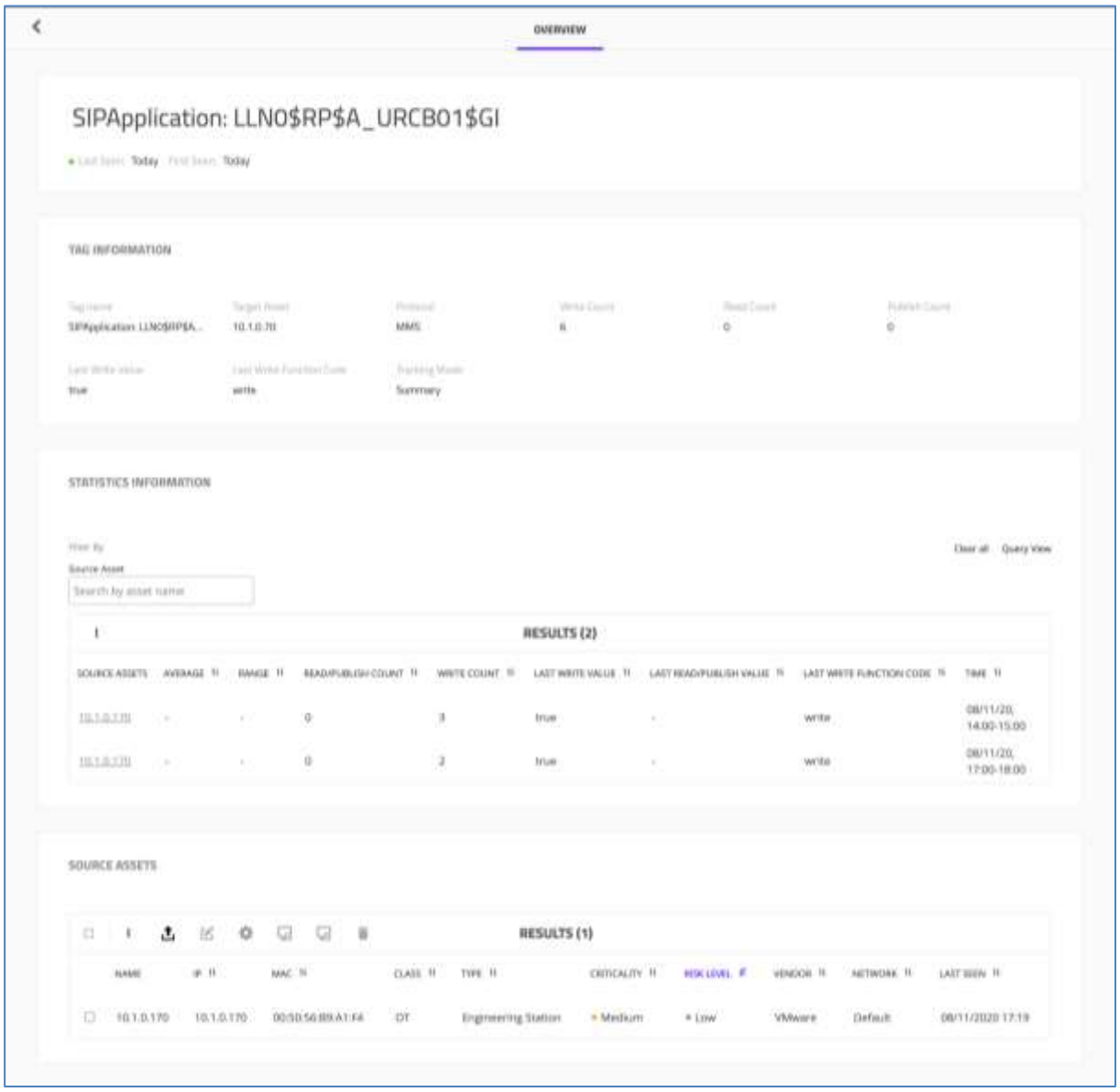


Figure 136: Summary View

The following fields are displayed in Overview page for the process values:

General Information

- **Process Values Title** – The name of the Process Value being tracked
- **First seen** – The first time there was a read/write/publish action on this tag
- **Last seen** – The last time there was a read/write/publish action on this tag

Tag Information

- **Tag Name** – The tag name that is related to the asset. This tag has a value
- **Target Asset** –The target (affected) asset (e.g., a Controller)

- **Protocol** –The related protocol running on this asset
- The Read/Write/Publish counts, the Last Read/Write/Publish value
- The **Last Function Code** – How the read/write action was done
- The **Tracking Mode** – No Tracking / Summary / Detailed

Statistics Information

- The **Site ID** – Identifies the site in which the process values are being tracked (only visible when investigating from the EMC)
- The **Source Asset/s** – The asset/s that communicated with the target asset and sent the read/write requests.
- **Min Value, Max Value, Average Value, Range:** These entities are measured from the time the system started to learn or after statistics reset.

> Note When a relevant value does not exist, the corresponding field is not displayed (for example, an average is not relevant for a Boolean or a string)

  - **Min Value** – The lower limit of a process value
  - **Max Value** – The upper limit of a process value
  - **Average Value** – The average of the Min Value and the Max Value
  - **Range** – The difference between the Min Value and the Max Value
- Write / Read / Publish count
- **Last access type** of the last action (e.g. read or write) to the asset
- **Last function code** – The last function code, how the read/write action was done.
- **Time** – The time period during which this value was tracked

Source Assets

- Clicking on the cell of a source asset opens the **Source Assets** dialog with a table listing each source asset and its corresponding request type
  - Clicking the asset name opens the full Asset View page
  - When there are multiple request types for a single asset source, the request types are separated by commas
  - The table can be sorted by the **Request Type** in the same manner as the main table

8.3.6 Detailed Tracking Mode

In addition to the Values over Time graph, the Detailed Mode table displays which **Source Asset** performed an operation, as well as the **Value** at each time interval, along with the **Access Type** (Read/Write/Publish) used and the **Function Code**.

The main areas of the Detailed page include:

General Information

Tag Information

Values over Time Graph

Value Information

Source Assets

8.3.6.2 Value Information

This view is similar to the Summary Mode view, with a **Value Information** area instead of the Summary Mode's **Statistical Information area**.

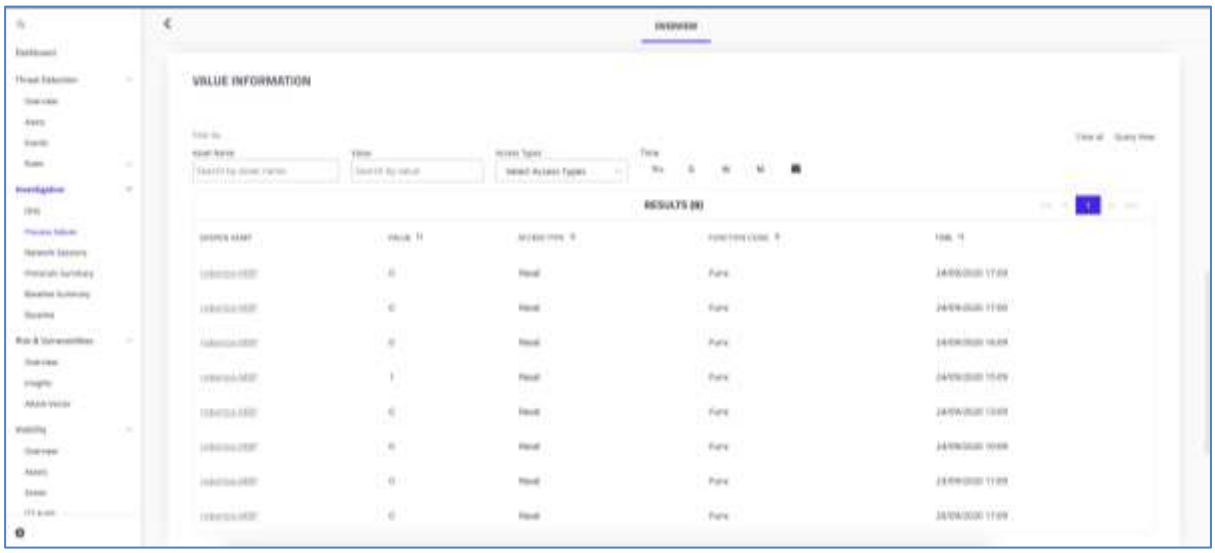


Figure 137: Detailed Mode - Value Information

Value Information Filters

The Detailed view presents the following filters for the Process Value results:

1. **Asset Name** for filtering the results asset name
2. **Value** for filtering the results by value

3. **Access Types** – Select **Write** / **Read** / **Publish** for filtering the results by access types
4. **Time** – Choose whether to filter the results per **Hour** / **Day** / **Week** / **Month**

These filters simplify search for something specific, such as Read Write access on a tag that uses the Modbus protocol.

Value Information Results Table

The Detailed **Results** table displays the following information. Click on any column name to sort the table by that parameter.

1. **Source Asset** – The name of the asset performed the operation with a link to its Detailed asset page
2. **Value** – The tag's value
3. **Access Type** – Write / Read / Publish
4. **Function Code** – The function code
5. **Time** – The timestamp of the tag

8.3.7 Resetting Statistics

When it is time to reset the statistics, select a row and then either open the Summary Side Bar and press the **Reset Statistics Summary** button as shown below; or press the **Reset** button  on the Process Values toolbar.

Figure 138: Resetting Statistics

Reset is used when the existing data is no longer relevant and there is a need to start over. Reset can be performed on a single Process Value or on several ones at once.

The values are Reset as follows:

- The Minimum and Maximum values that had previously been learned are now deleted
- The Counts are deleted

- The Averages are deleted

After Reset, new values are learned.

8.3.8 Protocol Details

> Notes: Process Values are currently supported for the following protocols: CIP, Goose (IEC-61850), IEC101, IEC104, MMS (IEC-61850/ICCP/TASE.2), Modbus, PCS7 WinCC (Historian), S7Comm, DPI (over PCCC).
>
> Prior to working with Process Values, make sure that the IEC-101 or IEC-104 protocol is enabled (in **Investigation > Protocols Summary**).
>
> Baselines values are still available from the baselines view and supported for DNP3, IEC101, IEC103, IEC104, VNET (VHF), DPI (over PCCC).

8.4 Network Sessions

Network Sessions analyzes network traffic. It gives you more insights into how your network traffic looks and your network health. It provides another dimension of visibility where traffic is based on the amount of data, validity of data, and number of errors.

The related Network Health graph shows retransmissions over time and the flow of data between assets. You can view a specific asset and determine if it has network issues.

To access Network Sessions view:

- In the Main Menu, navigate to Investigation > Network Sessions.

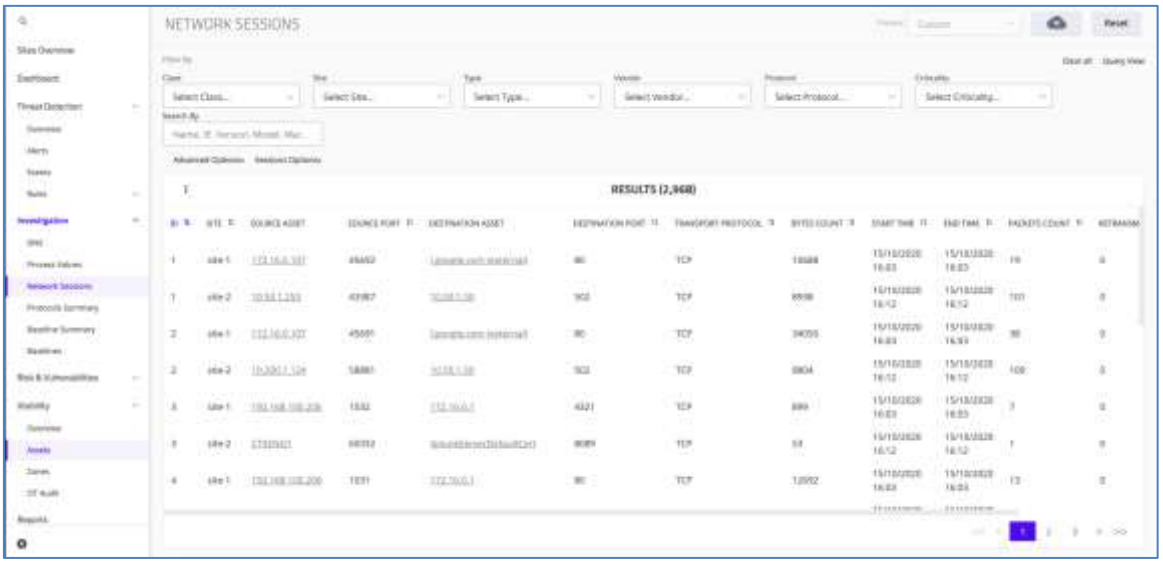


Figure 139: Network Sessions

To access the Network Health graph:

1. In **Investigation > Network Sessions** or **Visibility > Assets** in the Main Menu, click on an asset.
2. Go to the **Communication** tab and scroll down to the **Network Health** graph.

Figure 140: Network Health Graph

8.5 Protocol Summary

The Protocol Summary is an investigational tool that analyzes network communication by counting how many times each protocol in use appeared on a port. This helps engineers and analysts understand which protocols are the most commonly used.

To access Protocol Summary page:

- Navigate to **Investigation** > **Protocols Summary** in the main menu.

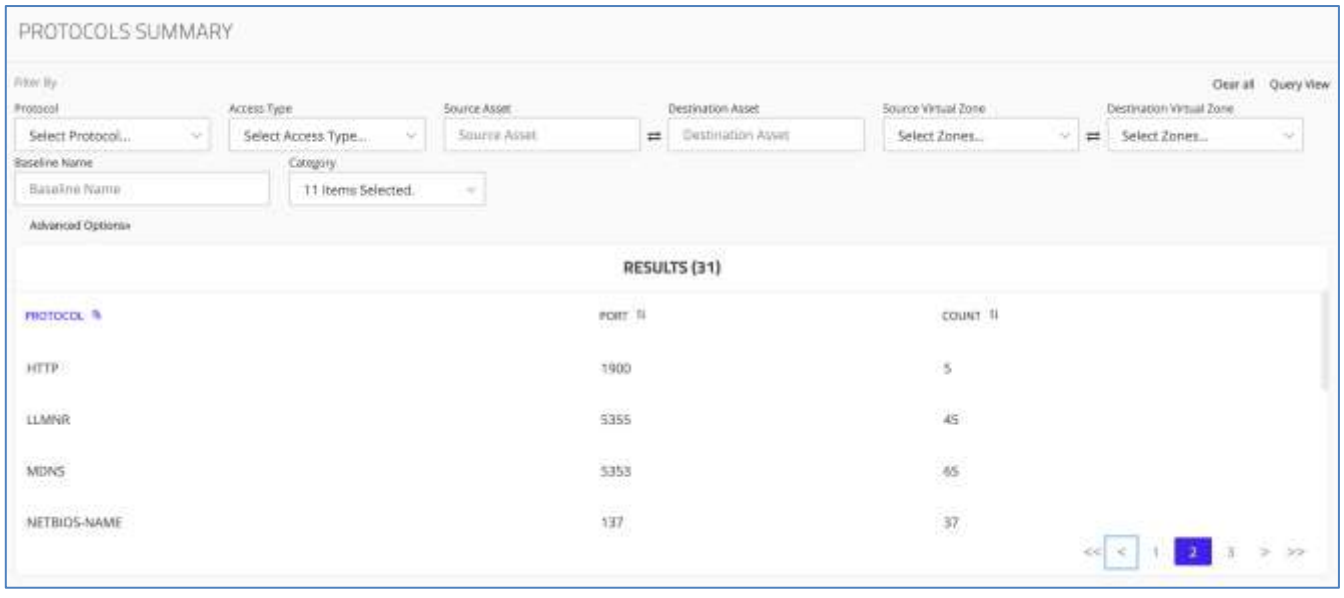


Figure 141: Protocol Summary

The filters in the Protocol Summary are identical to those in Baselines, minus the Time filter.

To use these filters, see section 8.7.1 – Baseline List Filters, and section 8.7.2 - Baseline List Filters in Advanced Options.

8.6 Baseline Summary

The Baseline Summary is an investigational tool that analyzes network communication. It enables engineers and analysts to understand, when investigating an alert, how many baselines from a specific port and it protocols were involved.

To use the Baseline Summary page:

- Navigate to **Investigation** > **Baseline Summary** in the main menu.

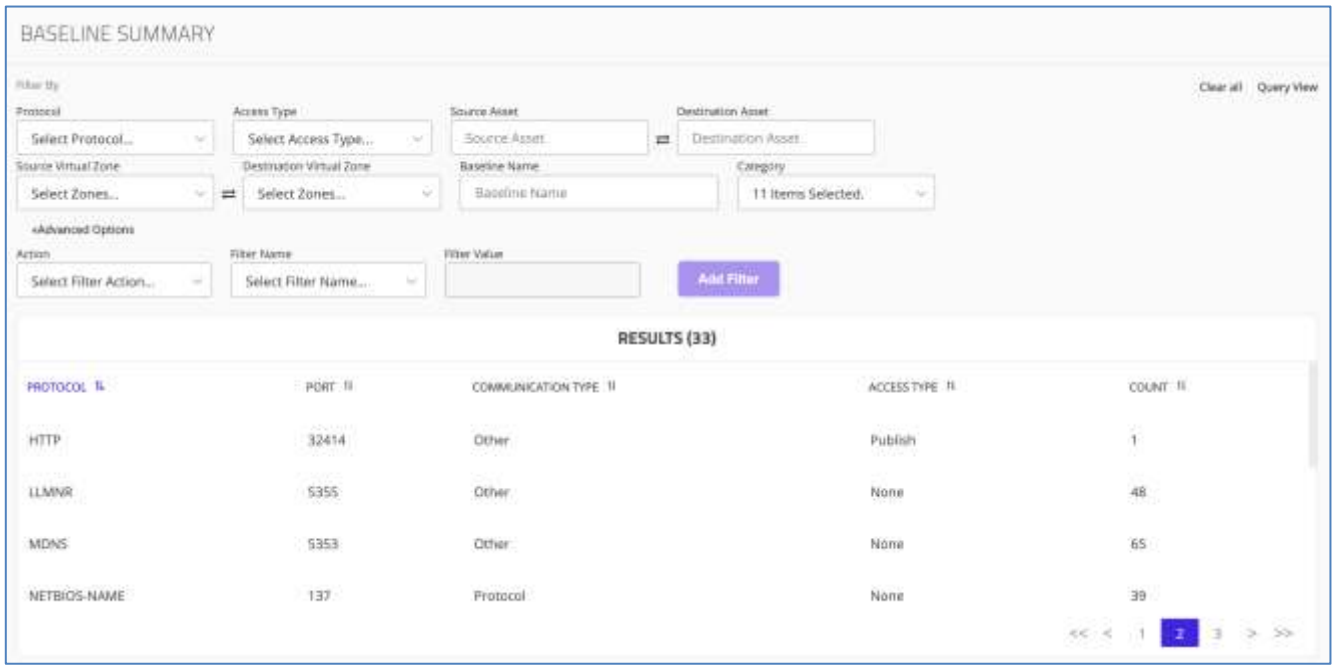


Figure 142: Baseline Summary

The filters in the Baseline Summary are identical to those in Baselines, minus the Time filter.

To use these filters, see section 8.7.1 – Baseline List Filters, and section 8.7.2 - Baseline List Filters in Advanced Options.

8.7 Baselines

Baselines displays all the baselines from all your assets, enabling filtering capabilities. These capabilities can be used during forensic processes done by Security Officers or operational investigations done by OT Engineers.

For example, OT Engineers could use this view to filter all write data acquisition operations performed in their environment. Security Officers or SOC operators could search for communications within a specific timeframe.

> Note: In the Enterprise Management Console (EMC), this page will include an additional Site filter to view baselines from some or all sites.
>
> Note 2: Baselines not active for more than a month in the system are removed automatically. This affects all the system components like insights, assets, etc.

8.7.1 Baseline List Filters

The Baselines List can be filtered in a variety of ways. The main columns are available in the normal view; additional columns are available in the **Advanced Options** filters as listed in section 8.7.2.

Figure 143 Baseline Filters

The following Baseline filters are supported:

1. **Protocol** – Dropdown list of all the supported protocols.
2. **Access Type** - Dropdown list of all the supported access types.
3. **Source Asset** – Filters by source of the identified asset.
4. **Destination Asset** –Filters by the destination of the identified asset.
5. **Source Virtual Zone** – Filters by the source of the virtual zone
6. **Destination Virtual Zone** – Filters by the destination of the virtual zone
7. **Baseline Name** – Filters by the name of the baseline
8. **Category** fields:
   - Alarm
   - Authentication
   - Data Acquisition
   - Diagnosis
   - File System
   - Firmware
   - Network
   - Operation
   - Other
   - Programming
   - Protocol
   - Remote Connection
9. **Time** – Filters the baselines by a set timeframe:
   - 1 hour/1 day/1 week/1 month

- By a range of your choice:

- **Source Address** – Address of the source of an identified asset. Note this field consists of the IP or MAC address.
- **Destination Address** – Address of the destination of an identified asset. Note this field consists of the IP or MAC address.

8.7.2 Baseline Filters in Advanced Options

The following baseline filters are also supported and accessed by clicking **Advanced Options**:

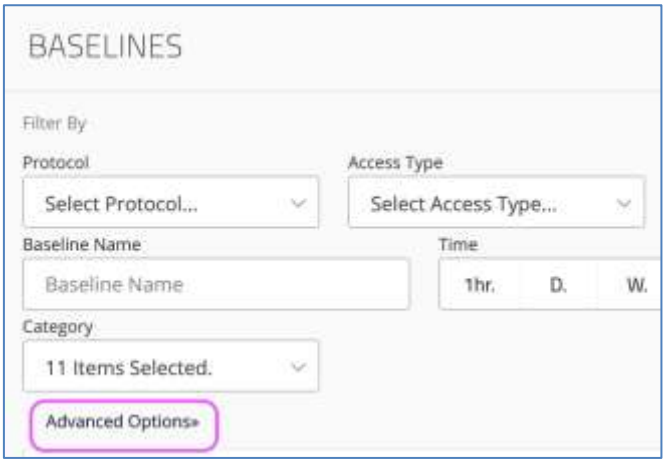


Figure 144 Selecting Advanced Options

Use the Baseline's **Advanced Options** as follows:

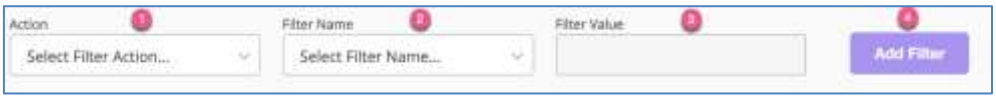


Figure 145 Baseline - Advanced Options

1. **Action** – Select an **Include** or **Exclude** action
2. **Filter Name** – Select a filter name from the following list:
   Baseline Name, Destination, Destination Port, First seen (days ago), Frequency, Last Seen (days ago), OT Protocols Only, Source, Source Port, Transmission
3. **Filter Value** – Enter the value for the filter you are creating
4. **Add Filter** button – Click this button to activate your filter.

8.7.2.1 Baseline Profiles of Virtual Zones

In the Baselines page, filter the results to source virtual zone and destination virtual zone. The baseline results are displayed as shown below:

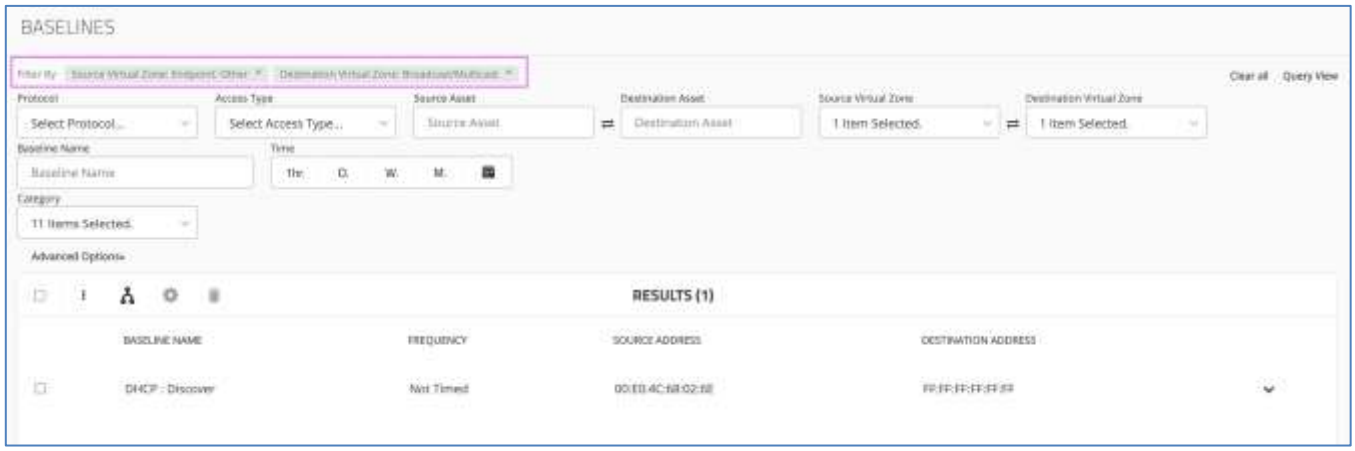


Figure 146 Baselines Results from Virtual Zones

8.7.3 Working with Baseline Values

Some communication protocols contain additional values representing various process-related information such as voltage, temperature, pressure, etc. For selected protocols, TIV can parse the numerical or textual value and incorporate it into the asset's baseline. These values can be viewed on the baselines page in a time-aggregated view, in a detailed view, or as a graph. Baseline values can also construct a baseline rule to create a baseline alert (refer to section 7.6.2 - Creating a Baseline Rule.)

> Note Baseline values are currently supported for the DNP3, IEC101, IEC103, IEC104, VNET (VHF), DPI (over PCCC).
> Prior to working with baseline values, make sure the IEC-101 and IEC-104 protocols are enabled (in the Protocols page, accessible from the Configuration Menu).

There are more protocols for the baseline values supported in the Process Values, see section 8.3.

8.7.3.1 Displaying Time-Aggregated Baseline Values

To view a time-aggregated display of IEC-101 baseline values:

1. Make sure that IEC-101 baselines are present in the table by using the **Protocol** filter, or by manually searching for them in the table.
2. Click the arrow at the end of a table row to display a sub-table with baseline values.

The sub-table shows the count and the size seen for the specific baseline in each given timeframe (between Start Time and End Time), as shown below:

Figure 147 Baseline Sub-Table

8.7.3.2 Displaying Detailed Baseline Values

To display detailed baseline values, do the following:

1. Add the Show Values column to the table by clicking **More**  **> Select columns,** choosing **Show Values**, and clicking **Apply**.

Figure 148 Selecting Show Values from the Select Columns popup

The Show Values column is added to the table.

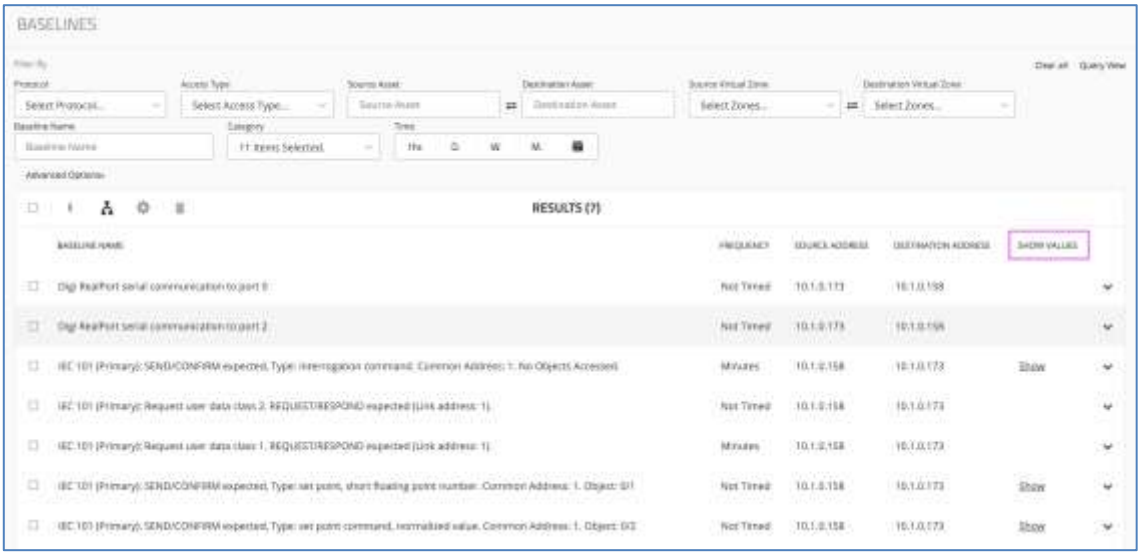


Figure 149 Show Values column

2. To display the values for a given baseline, click the arrow at the end of its table row.

   The row expands downwards to display a sub-table with the count and size seen for the specific baseline in each given timeframe (between Start Time and End Time).

   In this example, there are two baseline values and each one has a count of 1.

Figure 150 Baseline Sub-Table

3. To see a detailed view of the baseline values, click the baseline's **Show** link.

   A window displays the details of the baseline values.

Figure 151 Baseline Values window with baseline value details

The number of rows in the window reflect the counts of all the baseline values. In our example, there were two baseline values with a count of 1 each. Therefore, the Baseline Value window contains two rows.

8.8 OT Audit

The OT Audit page displays all the latest OT operations the system has detected. This page is essential for Management of Change (MOC) in OT operations.

To access the **OT Audit** page:

- In the Main Menu, navigate to **Investigation > OT Audit**.

Figure 152 OT Audit Page

OT Audit Results

Each row in the **OT Audit** table provides the following OT event information:

1. **ID** – The **OT event ID**; clicking it leads to the Event or Alert Page to access all the information for investigating, controlling, and managing the alert.
2. **Type** – The OT event/alert type.

3. **Description** – The description of the OT event/alert.
4. **Date Detected** – The timestamp of when this OT event/alert was detected.
5. **Network** – The network in which the OT event/alert occurred.

OT Audit Menu

6. Click the menu button  to hide duplicates (Distinct), download this OT audit as a .csv or .pdf file, or export/share/schedule this report.

Filter & Search

7. Use the **Type** field to select an OT event by its type.
8. Use the **Search by** field to search for text in the OT event description.
9. Use the **Clear All / Query View** tools to clear your filter/s or adapt the current query.

> Note: When the system transitions from Training mode to Operational mode, all OT alerts are auto approved. Any user that prefers that these OT alerts not be auto approved should archive them beforehand.

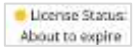
9 Management Tools

9.1 System Health Dashboard [Admins Only]

9.1.1 Overview

The System Health dashboard displays the status of the server itself, the license expiration date, the various sniffers in use, and any connected Sensors. It also displays status about the availability of the different traffic sources, including remote sensor status, and availability of SPAN traffic.

9.1.2 System Health Dashboard for a TIV Server

The statuses in the System Health Dashboard are colored with green  , yellow  , or red indicators . The Server status provides an overall **System Status** and the TIV **License Status** (hover over the **License** button to view its expiration date). The usage statistics are displayed in terms of percentages of available CPU, memory, and diskspace:

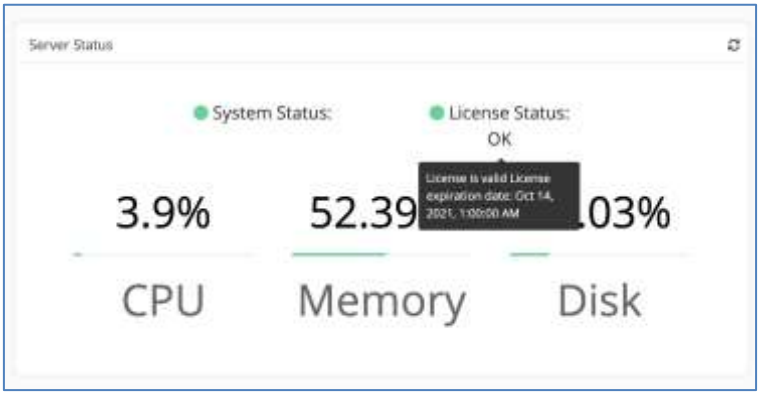


Figure 153 Server Status Example 1

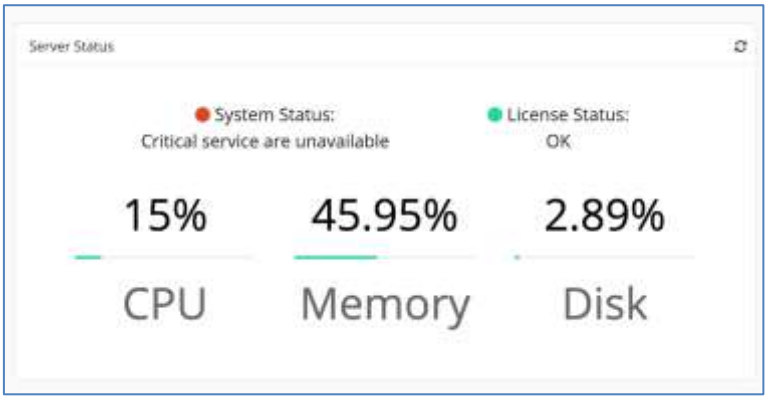


Figure 154 Server Status Example 2

The system displays the following status for each sniffer: Its OS name, its address, whether it is available, has traffic, and if the effectiveness of its SPAN port is sufficient:

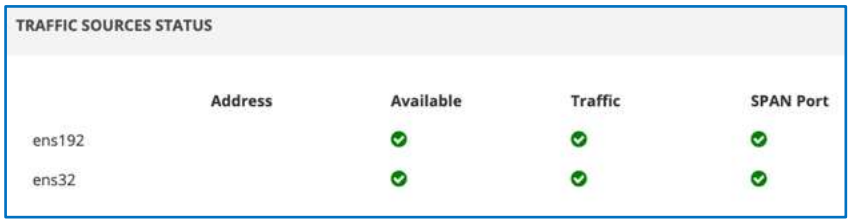


Figure 155 Traffic Sources Status Example

When the Span port is flagged with a red X , it means the system has not identified a sufficient amount of non-broadcast traffic, indicating it is not a monitoring port. For example, when more than 70% of the sniffing on the Span port is Unicast, consider reconfiguring this connection.

The Health Display will also show any associated TIV Sensors and TIV Sensor Lights, including the connection status, the device IP, Traffic, and sniffer port OS names and status.

9.1.3 System Health Dashboard for an EMC

The EMC System Health dashboard displays statuses of the Server on the left side and those of the Sites on the right side:

Figure 156 Sites Status Example

9.2 Maintenance & Upgrading (EMC/Sites/Sensor) [Admins Only]

You can select individual or multiple sites to upgrade directly from the EMC. After upgrading the EMC to the new version, you can navigate to the Site Maintenance page to select which sites to align with the same version as the EMC. The Download operation will download the newest version of the EMC to the site.

On the **Enterprise Overview** page, you can check all site versions at a glance before determining which ones require updates:

Figure 157 Enterprise Overview - Site Requires Update

Multiple site upgrades can be performed directly from the EMC via **Settings** > **Management > Site Management** as per section 10.2.3.

Figure 158 Navigating to Site Maintenance Page

9.3 Customizing Overviews

The Visibility, Risk & Vulnerabilities, and Threat Detection Overviews can be customized to show the information you need most. You can add and remove widgets and create your own.

Additionally, each default Overview can be used as a template to create personalized Overviews tailored to the needs of specific users.

Overviews can contain predefined widgets, as well as custom widgets with data important to specific users or roles.

9.3.1 Editing an Overview

A custom overview/widget can be edited only by the original owner but can be viewed by all users in the site/EMC in which the changes were made.

To edit the Overviews:

1. In the **View** dropdown list, choose the View to be edited.

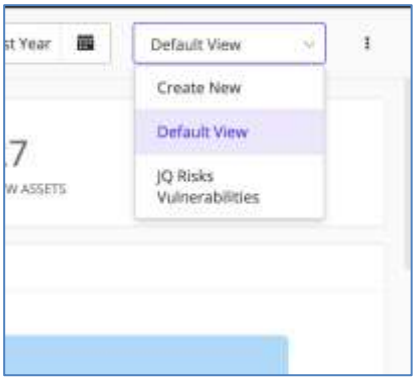


Figure 159 View Dropdown List

2. Click **More** ⋮ > **Edit**.
3. The following options are enabled:

Figure 160 Edit Overview Options

- **Add widgets** Add widgets – For adding new widgets. For more details see sections 9.3.4 and 9.3.5 below.
- **Save** Save – For saving the current overview as is presently set up, with the current name. When pressing **Save**:
  - If the "Default View" overview is currently displayed, only the **Save As** Save As option appears.
  - Otherwise all the **Save**, **Save As** and **Cancel** Cancel options appear.

> Note A customized Overview can only be revised by the user that created it.

- **Save As** Save As – For saving the existing overview with a new name. Use this option when cloning the current overview as a base template for creating a new overview.
- **Cancel** Cancel – To undo the changes initiated in Edit mode.
- **Delete** Delete – For deleting custom overviews/widgets. This option is only displayed for a custom-made overview.

9.3.2 Creating a Private Custom Overview

Custom Overviews can be viewed by all users in the site/EMC. However, in an organization with many Custom Overviews, the number of choices in the View list can become unwieldy.

To reduce the number of Overviews in the list, those that are of interest only to a specific user can be designated as Private and display only when that user is logged on.

To create a Private Custom Overview:

- When saving a new Custom Overview, select the **Private Dashboard** option in the Save Dashboard window.

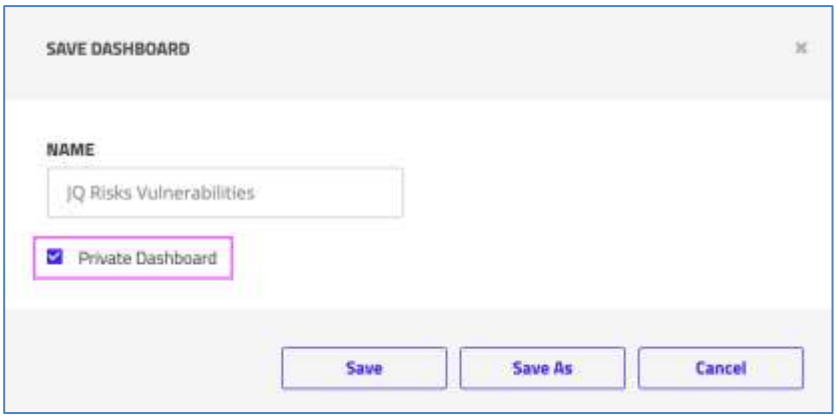


Figure 161 Making an Overview Private

9.3.3 Working with Widgets

The Overviews support creation and customization of widgets to effectively emphasize various aspects of the system as needed. By easily resetting the UI in this dynamic manner, you can display and highlight the critical data you prefer, and then visually analyze the results. The system also enables you to personalize Overviews to focus on these results regularly. You can create new widgets or customize the predefined ones.

You can create a customized Overview by reorganizing the placement of the widgets as follows:

- Click **More**  > **Edit** to start your customizations.
- The controls on the top right of each widget header are **Edit** mode controls  , enabling you to perform the following operations:
  - **Clone**  – To copy the selected widget.

- **Move** – To reposition the selected widget on the dashboard by dragging the widget with the mouse and releasing it at the target location.
- **Delete** – To delete the selected widget.

- To **Resize** the width of widget, click on the border and drag to the left or right.

9.3.4 Adding a Predefined Widget

To add a predefined widget, click **Add widgets** +Add widgets.

Predefined Widgets are available in the **Add Widgets** dialog by clicking the **Predefined Widgets** Predefined Widgets button on the left sidebar.

Use the **scroll bar** on the far right to scroll down to view the entire list of predefined widgets, select one or several widget/s to add, and choose **Done** to confirm your selection:

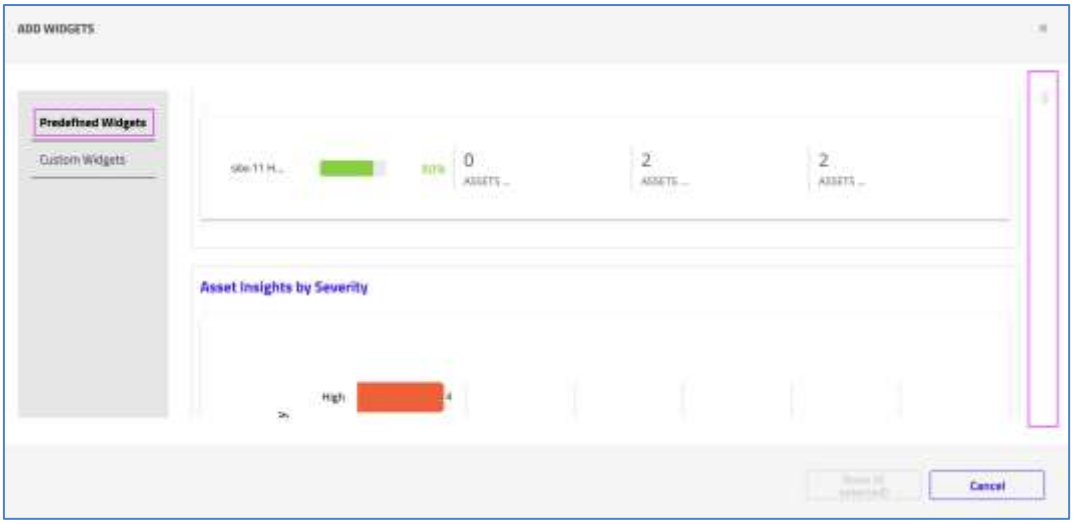


Figure 162 Add Widget - Predefined Widgets

9.3.5 Creating a Custom Widget

To create a custom widget, navigate to **Baselines**, **Assets**, or **Alerts**. Then, in the toolbar, click **More** > **Create a Widget**.

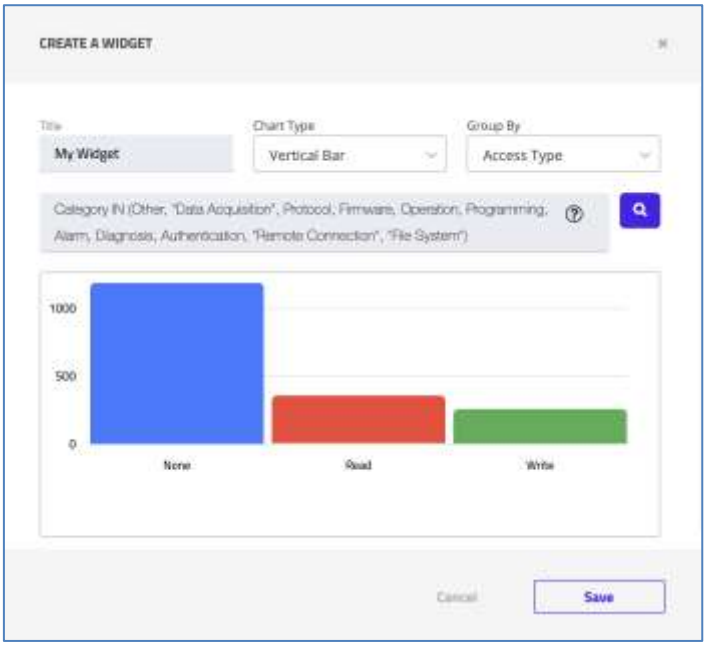


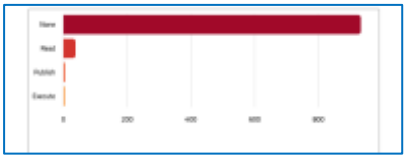
Figure 163 Create a Widget dialog

The elements of the Create a Widget dialog are as follows:

- **Title** – Provide a name for the new widget. This name will appear as the header in the top row of the new widget.
- **Chart Type** – Select the chart of your preference:

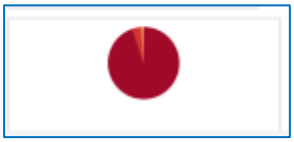
Select one of the following types of graphs to represent the data for your widget:

- **Horizontal Bar**

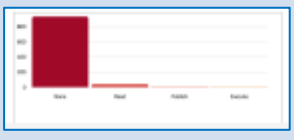


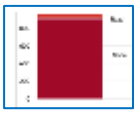
- **Line Chart**

- **Pie Chart**



- **Vertical Bar**



- **Vertical Bar Stacked** 

- **Group By** – Choose a category for how you want to group the results, if desired.
  You can group the results according to any of the following categories (listed alphabetically):
  - **In Assets** – Class, Criticality, Firmware, First Seen (days ago), Host Name, Last Seen (days ago), Mode, Model, Name, Network, OS, Parsed Asset, Purdue Level, Risk Level, Serial, Subnet, Type, Vendor, Virtual Zone
  - **In Alerts** – Category, Created (days ago), Severity, Site, Status, Type
  - **In Baselines** – Access Type, Baseline Name, Communication Type, Destination Port, First Seen (days ago), Protocol, Source Port, Transmission
- **Query Statement** – You can query by language only, or by a combination of filtering and TIV Query Language (TQL).

  Whatever filter is active in the viewed page is automatically translated into this query language. At that point you can modify the query statement or rewrite it to suit your requirements.

See 9.5.1 for full instructions for using TQL.

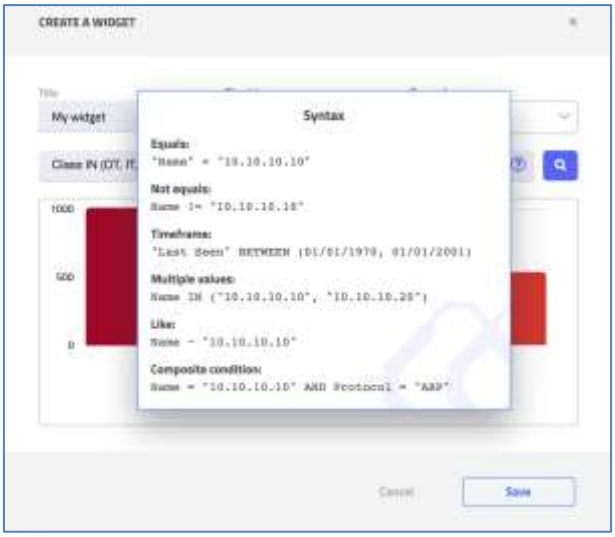


Figure 164 Filter/Query Statement

After your widget is created, it is added to the Custom Widgets section of the Add Widgets window and can be added to any Overview.

Figure 165 Custom Widget in Add Widgets Window

9.3.6 TQL Tooltips in Widgets

A tooltip hovers over every custom-made widget, revealing the underlying TQL query that produced the graph's results.

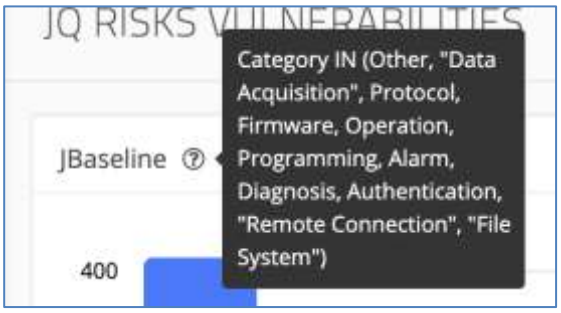


Figure 166 Query tooltip hovering over Widget

If the tooltip does not appear, move the mouse to an empty space on the graph until it appears.

9.3.7 Example - Creating an "OT Assets by Vendor" Widget and Adding it to an Overview

OT Engineers at a site want to be able to see all of the site's OT assets per vendor at the top of the Visibility Overview. This is accomplished in two steps:

1. Create an OT Assets by Vendor widget.
2. Add it to the Visibility Overview.

Create the Widget

1. Go to **Visibility > Assets**
2. Filter the list for OT Assets by selecting **OT** from the **Class** filter.

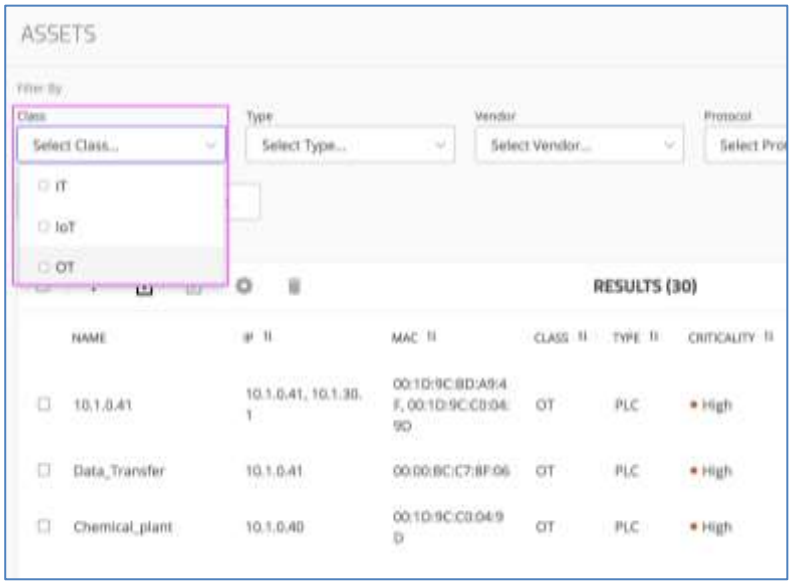


Figure 167 Filtering Asset List for OT Assets

3. Click **More** ⋮ > **Create a Widget**. The Create a Widget dialog opens with your filter:
   - Displayed as a graph with default settings
   - Transformed into query language (TQL):

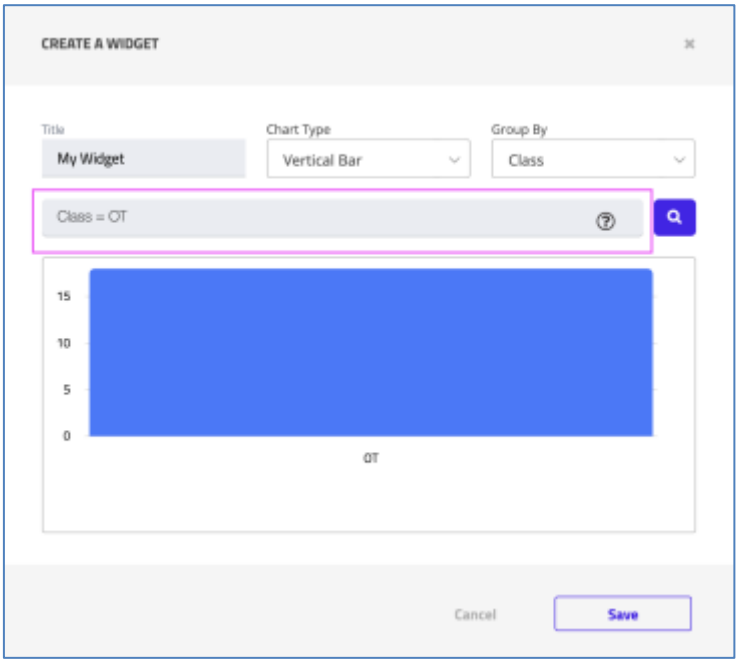


Figure 168 Create a Widget dialog

4. Create a horizontal bar chart of OT assets grouped by vendor:
   - In **Name**, type `OT Assets by Vendor`.
   - In **Chart Type,** select Horizonal Bar.
   - In **Group by,** select Vendor.

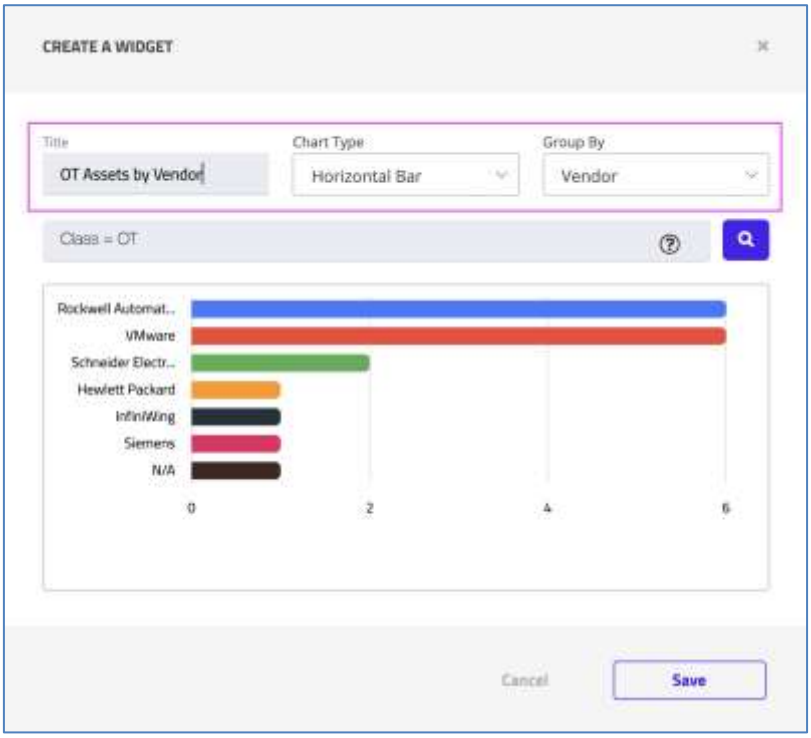


Figure 169 Adjusting the Title, Chart Type and Group By choices for a Widget

5. Click **Save**  .

Add the Widget to the Visibility Overview

1. Navigate to **Visibility > Overview**.
2. Because this widget should be available to anyone viewing the default Visibility Overview, leave **Default View** selected in the view selector.

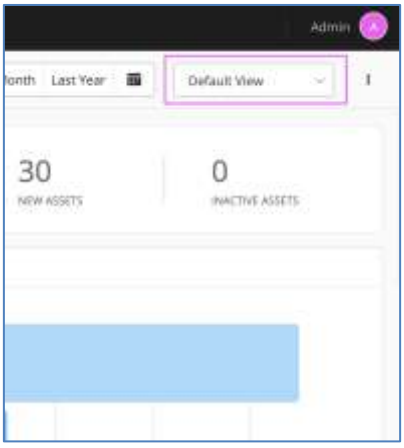


Figure 170 Default Visibility Overview

3. Click **More**  > **Edit**.

4. Click **Add Widgets** 

.

5. In the Add Widgets dialog, select **Custom Widgets,** choose the "OT Assets by Vendor" widget you created previously, and click **Done**.

Figure 171 Selecting the relevant widget to add to the Overview

The widget is added to the bottom of the Visibility Overview.

6. Drag the widget to the top right corner of the Overview.

7. Click **Save.**

9.4 Setting the Homepage

Depending on your role, you might want the Dashboard or one of the Overviews - Visibility, Risk & Vulnerabilities, Threat Detection - to display by default when you enter TIV.

The homepage is set per User.

To set the homepage:

1. Navigate to the desired Dashboard or Overview.

2. Click in the upper right corner of the content area, click **More**  **> Set as home page**.

9.5 Dynamic vs. Query Views

Basic filtering is available for each of the following TIV pages: Assets, Alerts, Events, Insights, Zones, and Activities. All data is presented in a **Dynamic View** by default. A **Query View** option is also provided, allowing users to use the TIV Query Language (TQL) to build swift SQL-like query statements for filtering data.

The Search field enables writing statements with auto-complete dropdowns.

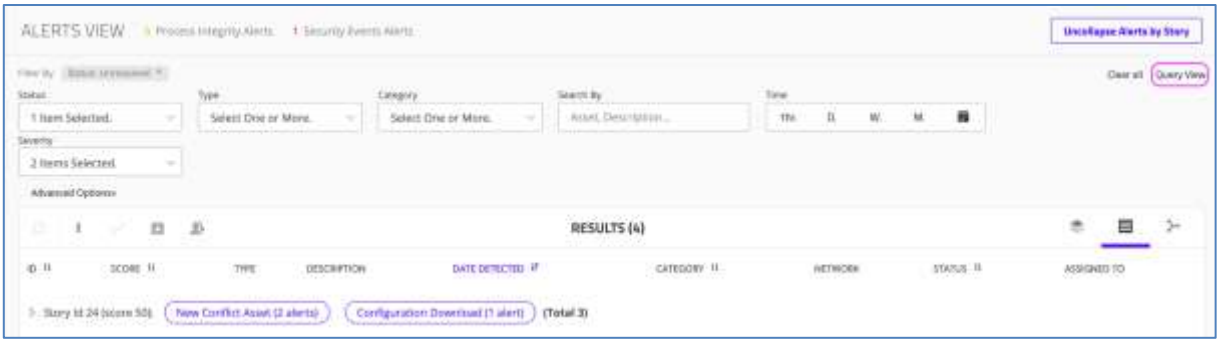


Figure 172 Alert Dynamic View (default) - with Query View button

To access **Query View**:

1. Click **Query View** to toggle to this option.

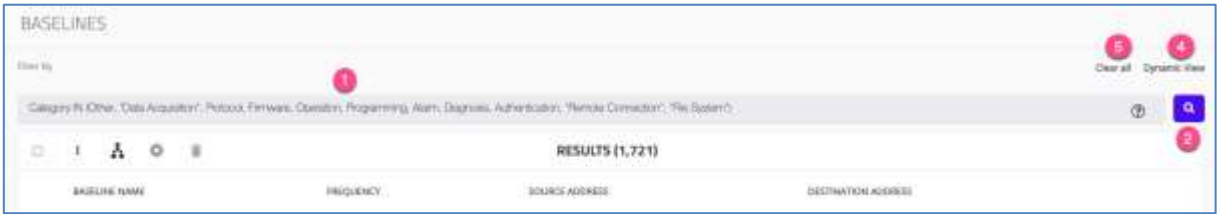


Figure 173 Baseline Query View

1. Enter your query statement into the **Search field**. Syntax options from the auto-complete feature pop up to continue your script. Type in the rest of the fields of interest or select from the dropdowns until your statement is finished.
2. Once your query statement is ready, press **Search** .
3. The query results are displayed.
4. To toggle back the Dynamic view, select **Dynamic View** on the upper right corner above the page results:
5. Select **Clear All** when needed.

9.5.1 TIV Query Language (TQL)

The intuitive and dynamic TIV Query Language is available throughout the interface, allowing advanced filtering and search in the Query View (see Figure 173).

9.5.1.1 Constructing TQL Queries

TQL, with an SQL-like syntax, supports both simple and complex queries.

- All built-in properties for every entity are supported

- Custom Attributes can be used for assets
- The operator 'AND' is supported between each phrase
- For IN or NOTIN, use brackets to group multiple values

Table 6 CQL Operators

TQL Operators	
=	For entities where the value matches exactly. This cannot be used with text fields; see the CONTAINS operator instead.
!=	For entities where the value **does not** match exactly. To find entities where the value of a specified field exactly matches multiple values, use multiple "=" statements with the 'AND' operator
IN	Contained in the list of values separated by commas and enclosed in brackets
NOTIN	Not contained in the list of values separated by commas and enclosed in brackets
~	Like
!~	Not like
~IN	Like in
~NOTIN	Not like in
AND	Displays the result if ALL the conditions separated by the 'AND' are met
OR	Displays the result if EITHER of the conditions separated by the 'OR' are met
BETWEEN	Selects values within a given range. The values can be numbers, text, or dates. It is inclusive; i.e. the begin and end values are included
NOT	Displays the result if the conditions separated by the 'AND' are not met

Table 7 CQL Syntax Examples

TQL Syntax Examples	
Equals	`"Name" = "10.10.10.10"`
Not Equals	`Name != "10.10.10.10"`
Time Frame	`"Last Seen" BETWEEN (01/01/1970,01/01/2019)`
Multiple Values	`Name IN ("10.10.10.10", "10.10.10.20")`
Like	`Name ~ "10.10"`
Composite Condition	`Name = "10.10.10.10" AND Protocol = "ARP"`

9.5.1.2 Entering TQL Queries

- Click on the Question button  to view TQL query examples:

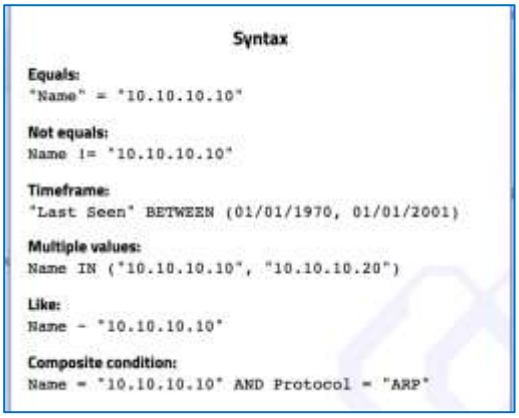


Figure 174 Popup with Syntax Rules and Examples

- As you type in the query statement, a drop down will appear, offering a list of auto-complete suggestions:

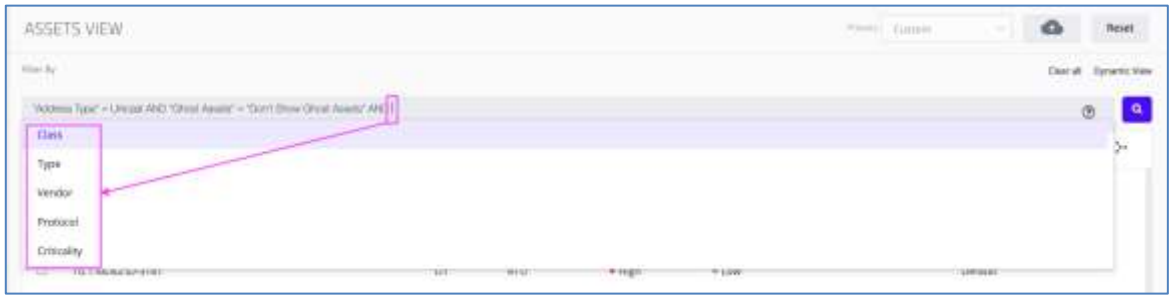


Figure 175 Creating Widget Popup

- In the relevant page, you can toggle between the Dynamic View and the Query View.
- Click **Search** to run the query
  - The results are displayed on the page in which the query is performed.

9.6 Reports

TIV enables you to produce a wide range of automatic reports, ranging from a detailed report on a single asset to a report on your asset inventory, to a comprehensive Risk Assessment Report that provides insights on the entire system. Reports can be scheduled to run periodically and configured to be sent automatically in an email notification as an attachment. Users have visibility of any reports they have produced in the past as well as those scheduled for the future.

9.6.1 Reports Page

To view the **Reports** page, navigate to **Reports** in the Main Menu.

- When reports have already been generated or scheduled, the **Reports** page displays the following:

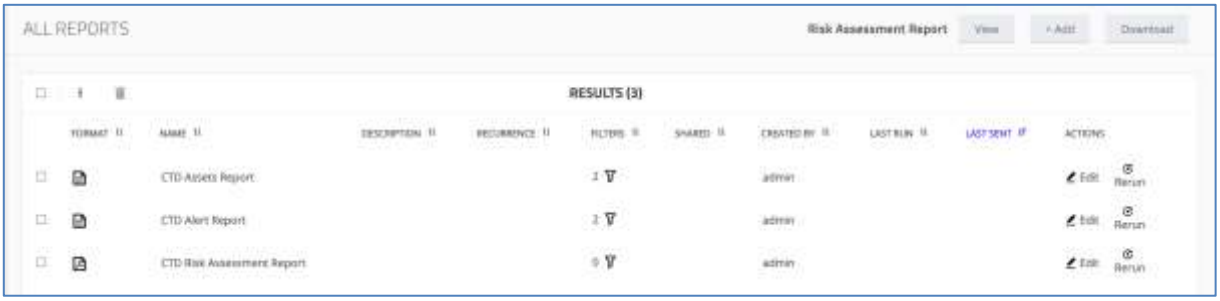


Figure 176 Reports Page with the listing of Reports

- The **Reports** page features a row for each existing or scheduled report:

Figure 177 An example of a report in the list

- Each row provides the following information:
  - **Format** – The format of the report: CSV or PDF

Name - The name of the report (e.g. TIV Inactive Assets from the last week) as provided by the user

  - **Description** – The boilerplate description of each report. Can be overridden by the user as needed.
  - **Recurrence** – If there is a scheduled recurring report, a clock icon appears. Hovering over it will show the scheduling information.
  - **Filters** – Indicates if any filters are applied to this report
  - **Shared** – Provides a Sharing icon indicating whether this report is configured to be shared via email. Hovering over this indication will show the list of emails.
  - **Created by** – The name of the user that created the report
  - **Last Run** – The timestamp of the last time that the report was run
  - **Last Sent** – The timestamp of the last time that the report was sent via email
  - **Actions** – Buttons for enabling editing, rerunning, and activating/deactivating existing reports

9.6.2 Risk Assessment Report

A summarized **Risk Assessment Report** can be generated by the system at any time. The report generation is automatic and faster than manually generated reports.

The Risk Assessment Report starts with an overall network summary then progresses to the details. These include the various control process devices, demonstrating how they communicate within and across the network. It provides specific visibility into your communication paths and associated devices.

This report provides a Network Hygiene score, which indicates the cumulative risk level that the alerts, insights, and assets pose to the system. A low value means that your system is more vulnerable to attacks. This score is calculated based on the critical security insights, CVEs, and anomalies detected, as well as how many critical assets were identified. When assets with severe vulnerabilities and alerts affecting them are used along with weak protocols, the score decreases.

The hygiene score appears together with a list of actionable insights that can help improve network hygiene, assets, and network statistics. This report can be used as a Key Process Indicator (KPI) to track progress as part of a security program, as an executive brief, and as a list of recommended changes.

Since the hygiene score is consolidated into a single score, it can be used to track progress in reducing the risk and attack surface.

When producing the report on the Enterprise Management Console (EMC) for all sites, be aware that the data being shown is an aggregation of the data from all the sites belonging to that EMC. As such, the Top Communicators and Protocol Distributions graphs will not be displayed in the report since this particular information does not apply when viewed from the EMC.

9.6.3 Creating a New Risk Assessment Report

1. Click **Reports** from the main menu
2. Next to Risk Assessment Report in the upper right corner, select **Add**

3. The **Create Report** dialog opens as follows:

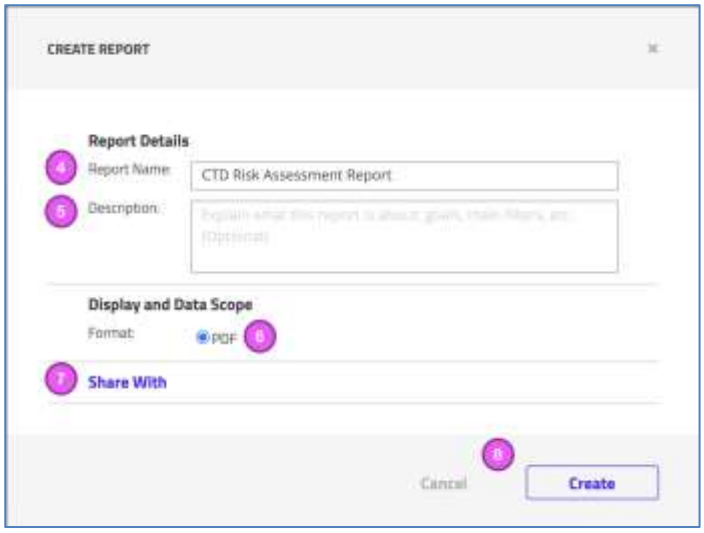


Figure 178 Create Risk Assessment Report - Report Details dialog

Enter the following **Report Details**:

4. **Report name** – Listed as TIV Risk Assessment Report by default. You can override or change the name as desired.
5. **Description** – Add a description (optional). This full description will be displayed on the All Reports page for your future reference. The properties of the Risk Assessment Report are pre-configured.
6. **PDF** is the default format.
7. **Share With** – If you want to send your report to others, select the **Share With** area of the dialog and follow the Sharing your Report instructions below.
8. **Create** – Press to produce the report or press **Cancel** to quit.
   - **Create** generates a Risk Assessment Report, automatically listed in the **All Reports** page. A toaster pops up on the top right area of the screen when the report is successfully generated.

9.6.3.1 Sharing your Report

To set up your report to be distributed to others, select **Share With**:

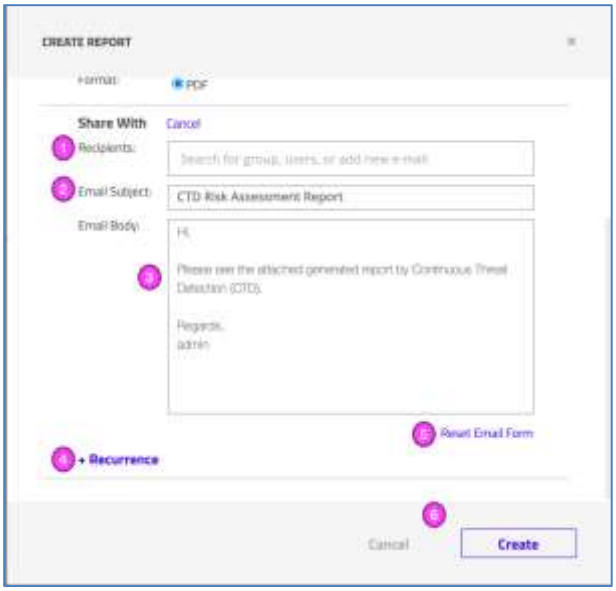


Figure 179 Button for Share With

The **Share With** features are as follows:

1. **Recipients** – Enter the recipient/s that you intend to share this report with.
2. **Email Subject** – By default, the Subject of the email will be 'TIV Risk Assessment Report'; append more information or adjust it if you prefer.
3. **Email Body** – Adjust the text to suit your needs.
4. **Recurrence** – If you intend to have this report generated on a regular basis, Follow the *Recurrence* steps:

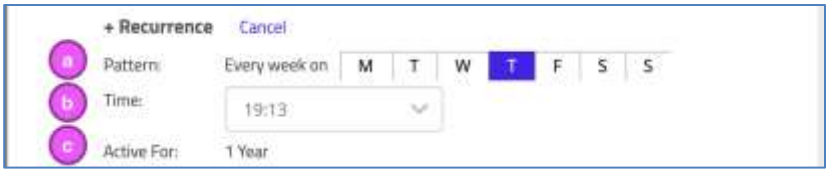


Figure 180 Recurrence settings

   a. **Pattern** – Choose the frequency of your report, clicking the relevant days of the week that you prefer. Select a daily, weekly (the default), or monthly recurrence. You can select one or multiple entries.

   b. **Time** – By default the system sets the default time to be the current hour. Adjust it to the hour of your choice.

   c. **Active for** – By default the duration is for 1 year. This field cannot be changed.

5. At any point you can reset these values by clicking **Reset Email Form.**
6. To produce this report for a one-time purpose only, click **Create**  .
7. The Scheduled Report appears in the Report list.

8. You can edit the report from the Reports List by clicking **Edit** from the Actions menu:

9. The **Edit Report** page is displayed.
10. Adjust the settings as needed, and then click **Update** to commit your selection.

9.6.4 Downloading a Risk Assessment Report

1. From the Reports page, select Download

.

The report is generated and automatically downloaded.

9.6.5 Viewing Existing Risk Assessment Reports

1. From the **Reports page**, select **View**

The report is generated and automatically displayed on your screen:

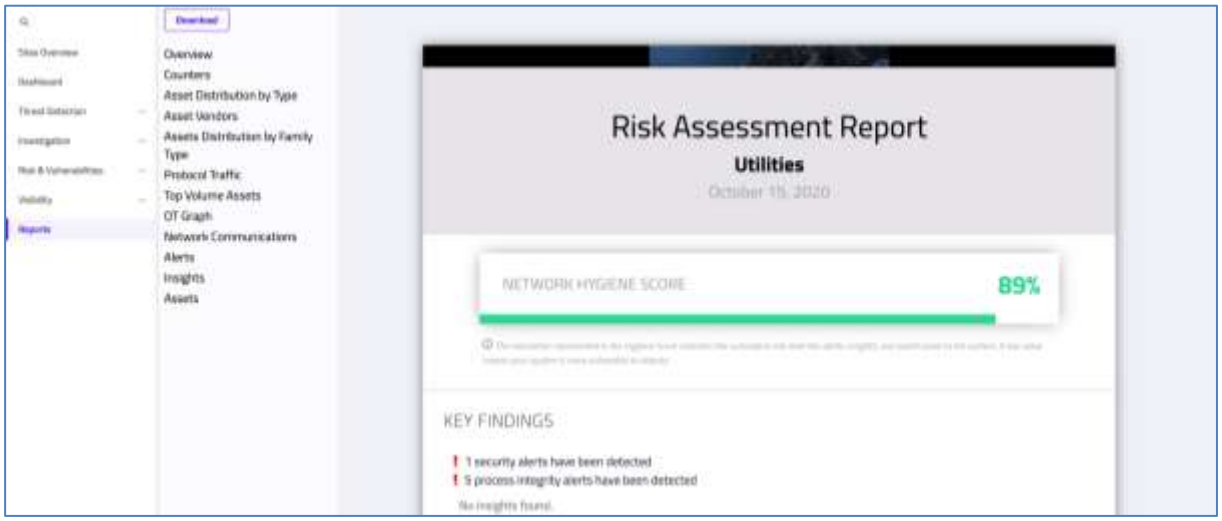


Figure 181 Viewing an Existing Risk Assessment Report

The menu on the left side highlights the topics covered in the report with a link.

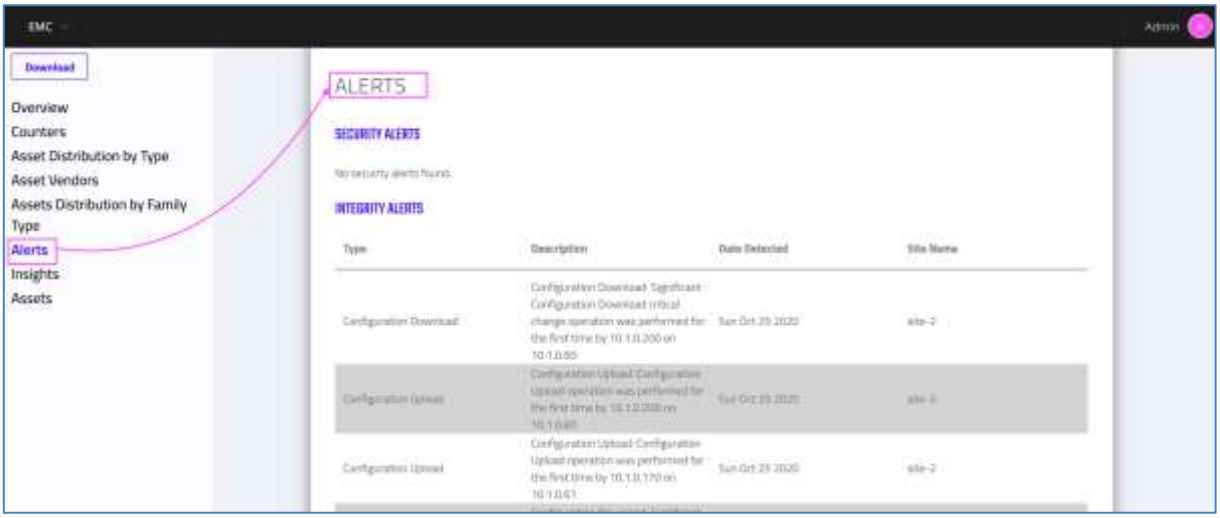


Figure 182 Selecting the Alerts page from the Report menu

9.6.6 Report Excerpt: USB Devices Connected to Assets

An excerpt of the USB devices Insight from the Risk Assessment Report:

Figure 183 Insight: USB Devices Connected to Assets

9.6.7 Report: Asset Distribution by USB devices

To obtain a report with the distribution by USB devices:

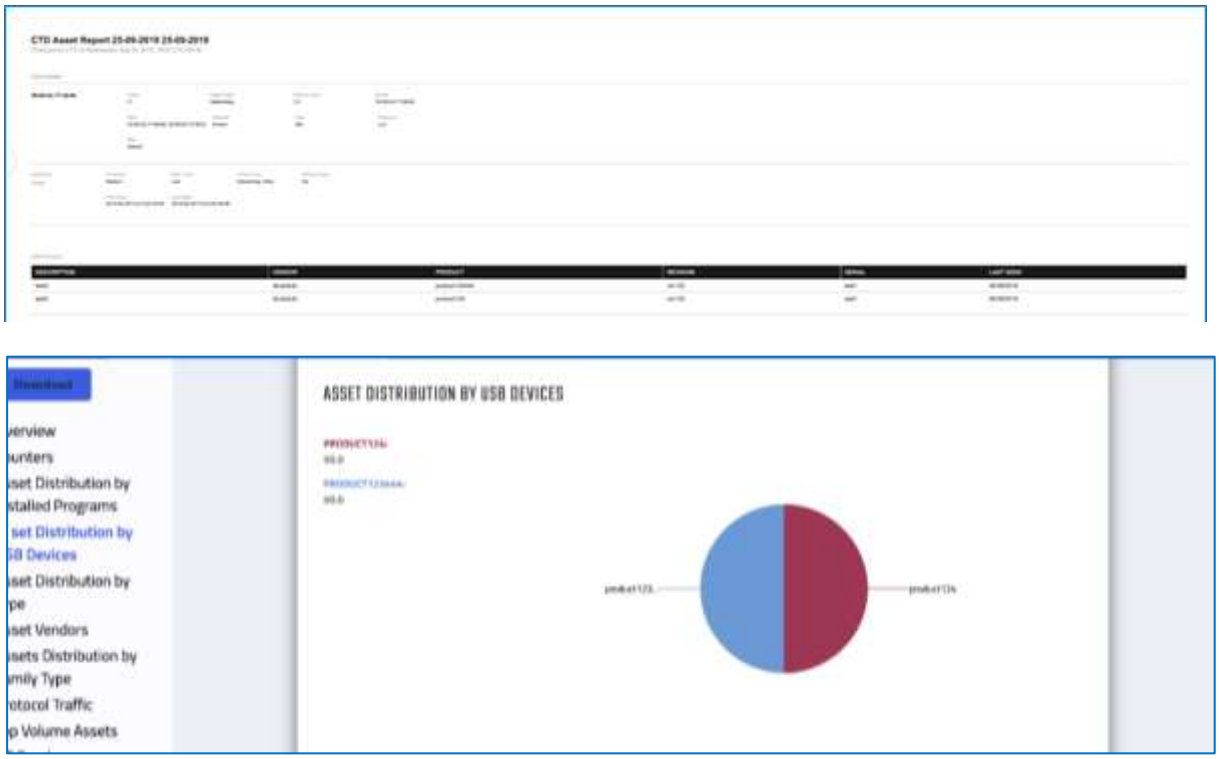


Figure 184 Report with the distribution by USB devices

> Note This report is only relevant for Active Detection - WMI Advanced Query.

9.6.8 Prerequisite for Sharing Reports

In order to share TIV Reports by email, the system requires prior configuration with an SMTP Server, which can be configured by Admins as described in section 13.1.1.

9.6.9 General Reports

Reports from each major page (Assets, Alerts, Baselines, Activities, Insights, etc.) can be exported in the same manner as the Asset Report.

9.6.9.1 Assets Page Reports

In the **Assets** page, click the **More** ⋮ button and then **Create Scheduled Report** or **Download**. Scheduled reports are similar to the general instructions provided for **Creating a New Risk Assessment Report**, as detailed in section 9.6.3.

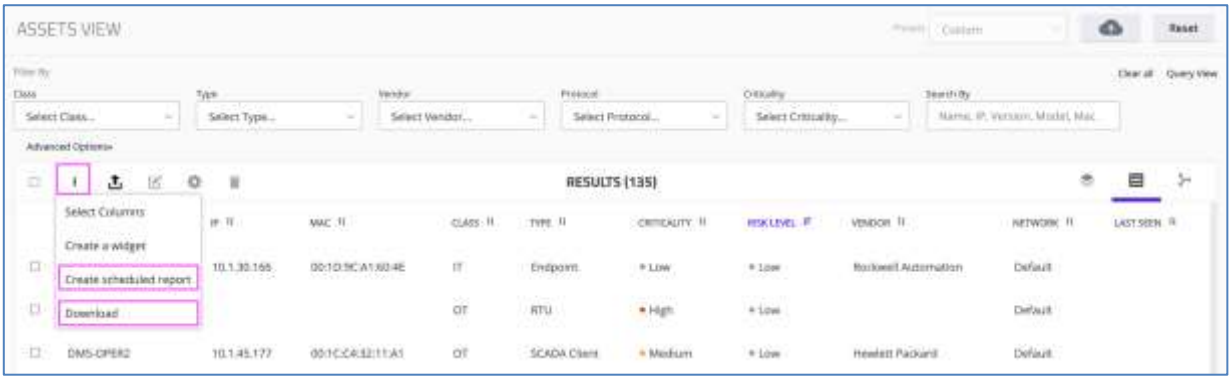


Figure 185 Reports from the Assets Page

9.6.9.2 Alerts Page Reports

In the **Alerts** page, click the **More** button and then **Create Scheduled Report** or **Download**. Scheduled reports are similar to the general instructions provided for **Creating a New Risk Assessment Report**, as detailed in section 9.6.3.

9.6.9.3 Insights Page Reports

In the **Insights** page, click the **More** button and then **Create Scheduled Report** or **Download**. Scheduled reports are similar to the general instructions provided for **Creating a New Risk Assessment Report**, as detailed in section 9.6.3.

9.6.9.4 Activity Log Reports

In the **Activity Log** page, click the **More** button and then **Create Scheduled Report** or **Download**. Scheduled reports are similar to the general instructions provided for **Creating a New Risk Assessment Report**, as detailed in section 9.6.3.

9.7 Activity Log

The **Activity Log** records all the activities performed in the system in the current period and the corresponding user activity or the system's response to alerts. It includes the information from all sites when selected from the EMC.

The activities are listed in chronological order with the newest items appearing at the top. This list provides the activities relevant to the site or EMC.

These activity logs also include data loaded into TIV from CSV import, App DB, and Active Queries.

- To view the **Activity Log**, open **Settings** from the Main Menu and then **Activity Log**.

- The **Type** column displays the name of the Activity that has been logged. Refer to the **TIV Reference Guide** for the full listing of **Activity Types**.

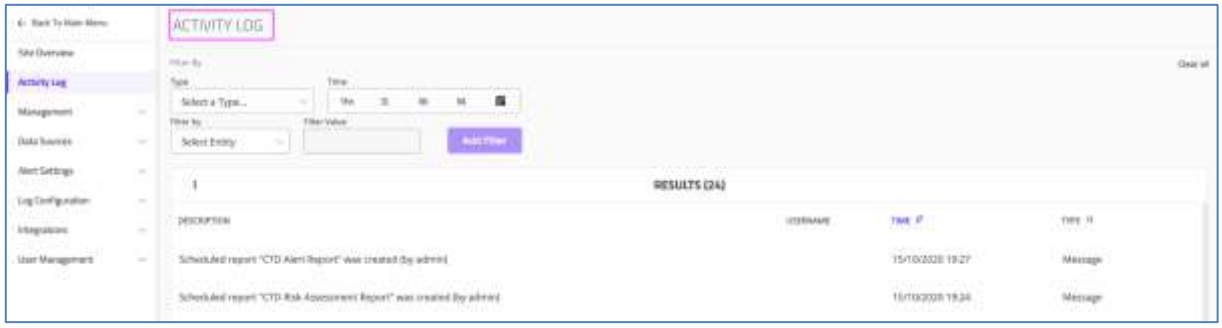


Figure 186 Activities Page

- For multiple site configurations (from the EMC) the **Activities** are listed with their site names:

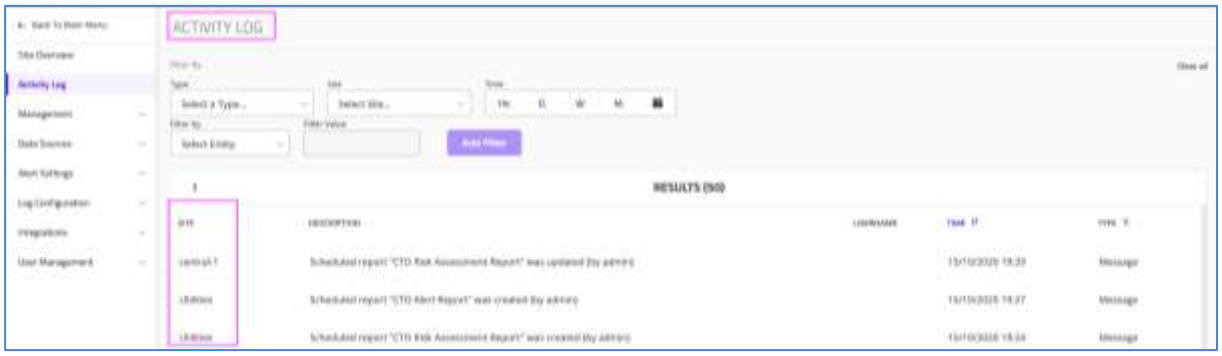


Figure 187 EMC Activity Log Page - Activities Displayed Per Site

- Use the **Activity Log** Page to take advantage of the system's filtering capabilities for investigating operations that occurred in your system.
- The following screen shows the Activities displayed after filtering for the Site Down type:

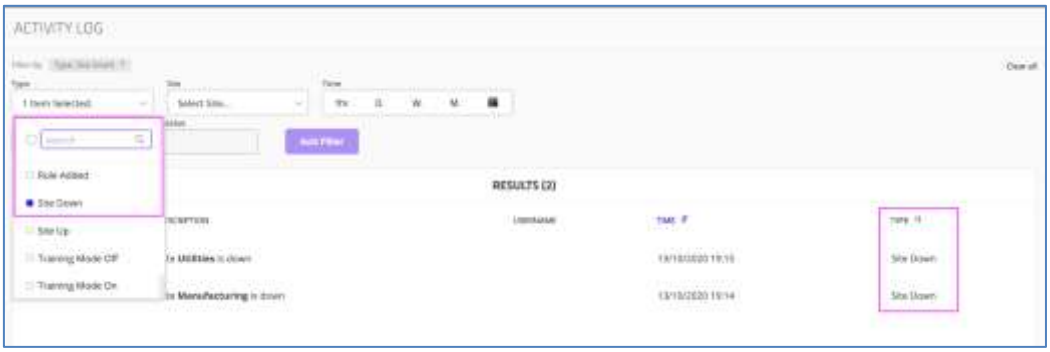


Figure 188 Activities Filtered by Site Down

9.7.1 Details of Activity Logging

The Custom Attributes listed in the Activity Log detail which user performed which action, with a timestamp and the relevant site, if it is a multiple site deployment.

The Activity Log logs configuration operations (Add/Delete/Update) for Custom Attributes as well as their usage. When a user changes the application or value of a Custom Attribute, the system logs the corresponding asset name and its value, including the site and the network in which the change occurred. When bulk actions are performed, they are listed per asset.

10 Configuring System Management [Only Admins]

To configure the full system, click **Settings** in the Main Menu.

All the Settings options are organized as follows:

Figure 189 Settings Options [Only Admins]

10.1 General

10.1.1 System Mode

To view the System Mode, select **Settings** > **Management** > **Gene**ral.

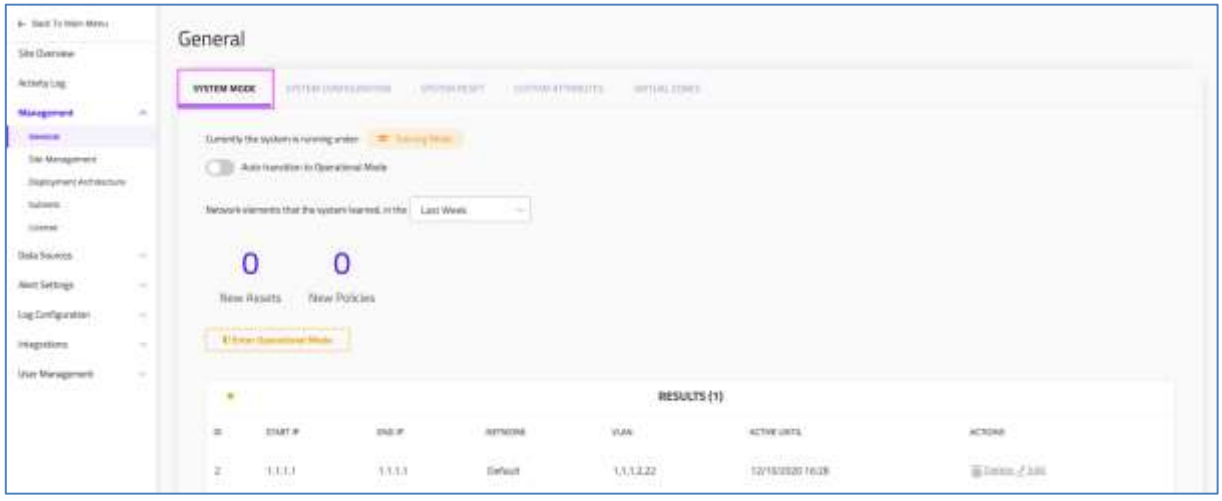


Figure 190 Management: System Mode tab in Training Mode

When the system is in Operational mode, the System Mode page appears as follows:

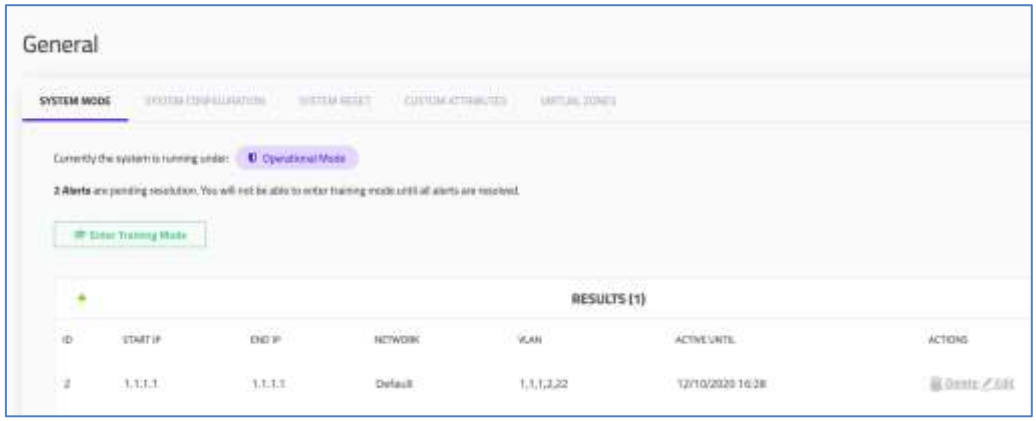


Figure 191 Management: System Mode tab in Operational Mode

10.1.1.1 Learning Policy Rules

When the system starts for the first time, it operates in Training Mode.

Training Mode

This mode automatically assembles policy rules based on the observed, valid network traffic until the number of newly discovered procedures per day is low. This process might take several days or weeks to complete.

In this mode, TIV triggers alerts for critical changes and security risks, while recording all newly discovered assets and communication patterns in its policy rules. The system displays the number of new assets and policy rules it has learned during the selected time period on the **System Management** page.

10.1.1.2 Auto-Transition to Operational Mode

By default, the system auto transitions from Training Mode to Operational mode:

Figure 192 Auto-transition to Operational Mode

10.1.1.3 Transitioning to Operational Mode Manually

You can change the default, so the system does not auto transition from Training mode into Operational Mode.

> **Note** When you perform the mode change manually, move the system to Operational Mode only after you are confident that you established your baseline.

To transition to operational mode manually:

1. In the site selector, choose the site and then select **Settings** > **Management > General**.
2. Click Enter Operational Mode:

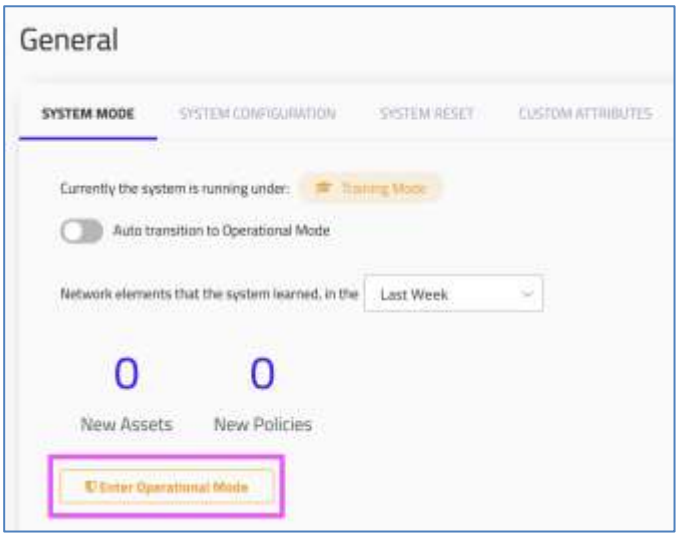


Figure 193 Enter Operational Mode

The **Set System Mode** dialog appears:

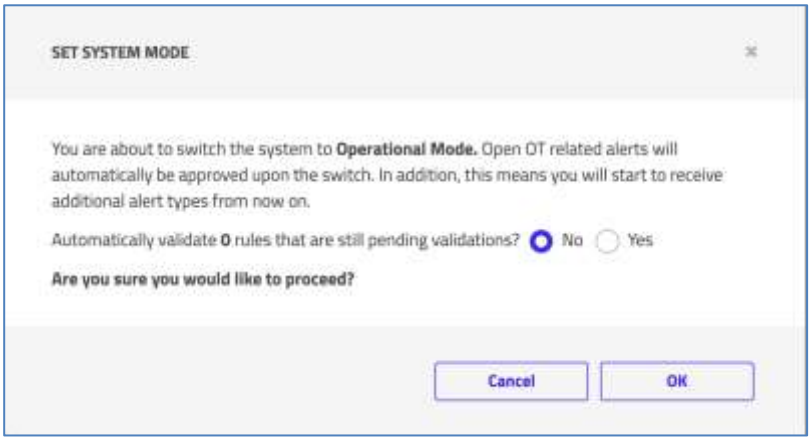
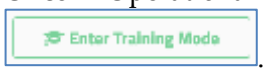


Figure 194 Set System Mode Clarification before Operation Mode

3. Choose whether or not to automatically validate the pending validation rules and click **OK**.

10.1.1.4 Transitioning back to Training Mode Manually

1. Once in Operational mode, to revert back to Training Mode click 

.

   The **Set System Mode** dialog appears, stating that after the system reverts to Training Mode, any existing alert types not visible in Training Mode will be auto approved:

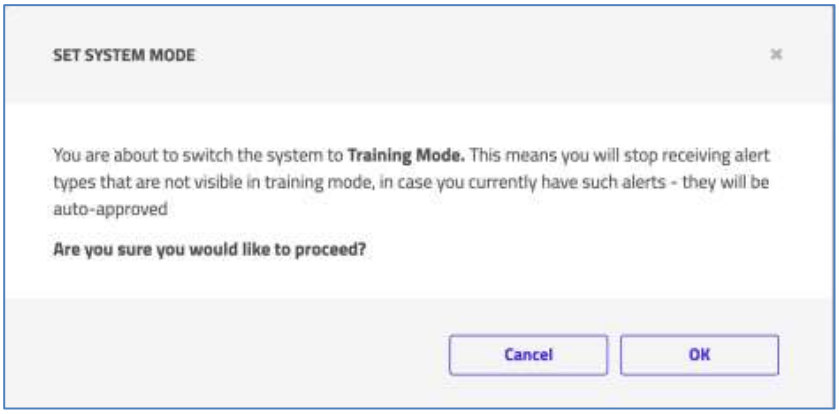


Figure 195 Set System Mode Clarification

2. Choose whether or not to automatically validate the pending validation rules.
3. Click **OK**.

10.1.1.5 Placing a Specific Network Segment into Training Mode

- **Adding A New Rule** – When a specific range on the network is still not ready for Operational mode, or if maintenance works are being performed in this range, you can configure this rule and then the system will not raise any non-security alerts in this range.

To place a specific network segment in Training Mode from Operational Mode:

1. Select Settings  > Management > General.
2. Click Create New 
.

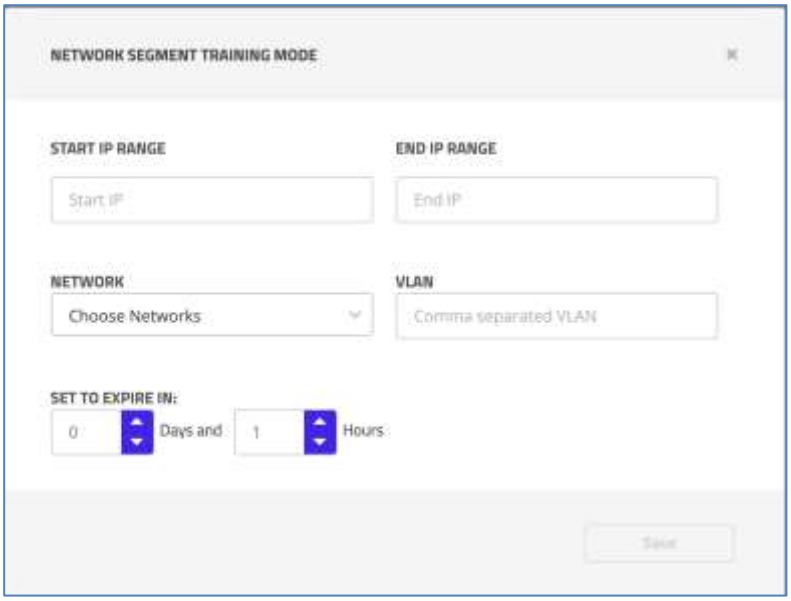


Figure 196 Network Segment Training Mode popup

In the Network Segment Training Mode popup:

3. Define the Start and End IP ranges, Networks, and VLAN that you want to move into Training Mode.
4. **Set to Expire In** – Specify the period of time during which you want to keep this segment in Training Mode.
5. Click **Save**.
6. Enter Operational Mode – The mode you are currently running in is presented in the System Mode tab. It displays the count of your New Assets and New Baselines according to the time duration that you select. When the number is less than 5, you can change the system mode to Operational Mode and then alert on any deviation discovered on the network.
7. When you switch from Operational to Training mode, you will be prompted to confirm the switch, and if you want, to resolve the alerts automatically:

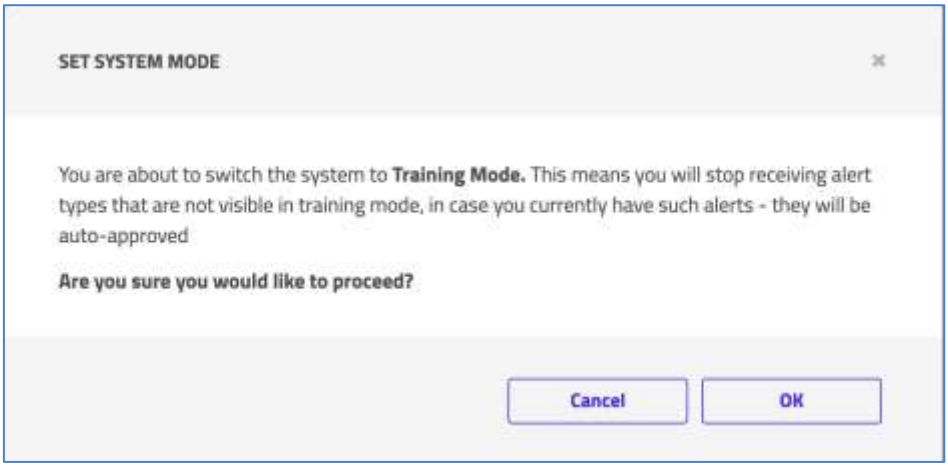


Figure 197 Set System Mode dialog

If you confirm **OK**, the system resolves the security alerts automatically and leaves the OT alerts untouched.

10.1.2 System Configuration

The **System Configuration** tab of the General page appears as follows:

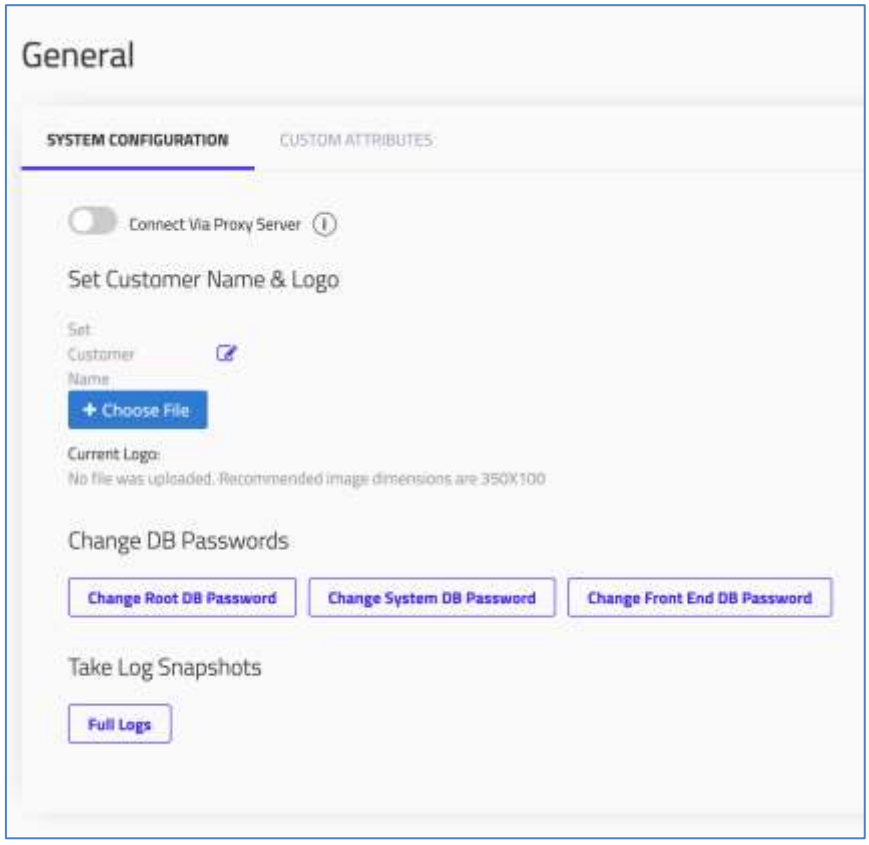


Figure 198 System Configuration Dialog

10.1.2.1 Proxy Server

You can enable TIV integrations and Cloud Services to connect to internet servers when there is a proxy in place.

There is an option to configure a proxy server via **System Management** which will enable a proxy client on the server and route outgoing (internet) traffic through it.

To connect via a proxy server:

1. Go to Settings > Management > General
2. Click on the System Configuration tab.
3. Click the toggle button **Connect Via Proxy Server** to On.
4. Type in the proxy address and port number.
5. Turn on the Proxy Authentication.
6. Type in the username and password.
7. Click **Connect**.

> Note: The proxy server is supported over https by default.

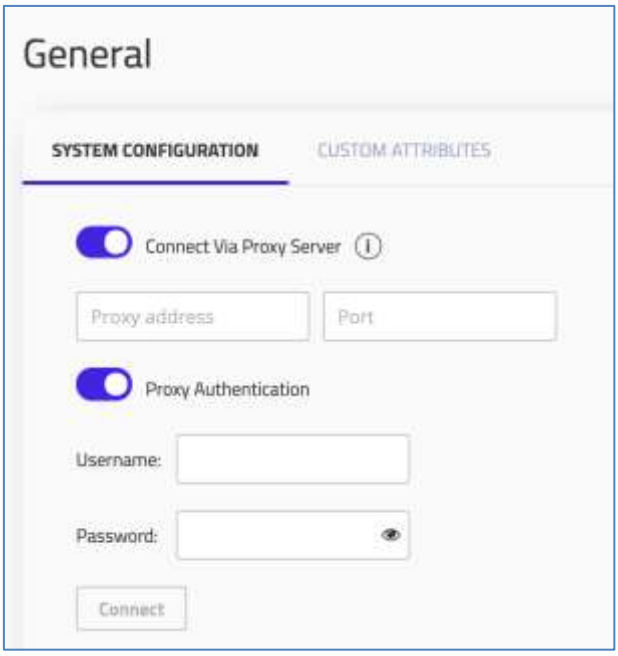


Figure 199: Proxy Server Configuration

10.1.2.2 Site Name & Description

The TIV Servers set up for your system by the Wizard are named by default.

To rename the sites and to provide descriptions for them:

- Navigate to **Settings** > **Management** > **General** and click the **System Configuration** tab. Set the site name & description (see Figure 198).
  - **Set site name** – Click Edit to enter or modify the site name (maximum of 24 characters).
  - **Site description** – provide essential information about your site (maximum of 150 characters). This description will appear in the All sites page and in the Site Dropdown selector.

See section 10.1.2.4 to set the Customer Name and Logo.

10.1.2.3 Set Folder Size for PCAP Alerts

The default limit on the PCAP Alert folder size is 5120 MB. When you are saving PCAPs of the alerts (i.e., the default setting), after this buffer is full, the oldest PCAPs are automatically deleted.

To change this setting:

1. Navigate to Settings > Management > General and click the System Configuration tab.
2. In **Set PCAP Alert Folder Size**, enter the desired size (in MB). (See Figure 198).

10.1.2.4 Set Customer Name and Logo

Customer Name and Logo settings can be set up to produce reports, such as the Risk Assessment Report (see section 9.6.2).

To set customer name and logo:

- **Settings** > **Management** > **General** and click the **System Configuration** tab. In **Set Customer Name & Logo** (see Figure 198):
  - **Set customer name** – Click Edit to enter the customer name (maximum of 30 characters).
  - **+ Choose File** – Browse to select the customer's logo image. The recommended dimensions of the logo image are 350x100 pixels. (If your logo has different dimensions, the system will transform it to this requirement).
  - **Current logo** – Displays the default logo in use (if any).

10.1.2.5 Changing DB Passwords

Use the **Change DB Passwords** dialog to reset various passwords in your system.

To change DB Passwords:

- Navigate to **Settings** > **Management** > **General** and click the **System Configuration** tab. In **Change DB Passwords**, click any of the following: (see Figure 198).
  - **Change Root DB Password** – Select this to change your user root system DB password
  - **Change System DB Password**– Select this to change your system database password. This is the user that the system uses to connect.
  - **Change Front End DB Password** – Select this to change your frontend (i.e. web HTTP) password

10.1.2.6 Taking Log Snapshots

Use this feature for capturing log snapshots.

To take log snapshots:

1. Navigate to **Settings** > **Management** > **General** and click the **System Configuration** tab. In **Take Log Snapshots**, click: (see Figure 198)

- **Full logs** – Enables you to take a snapshot of your logs (both machine and system logs) and all your databases.
- **Logs without DB** – Enables you to take a snapshot of your logs without DB

After the system is finished preparing the snapshot, you can download it by clicking the link of the Log file name  .

10.1.3 System Reset

Resetting the system means you will be losing some or all of your data. You have the option to retain some elements: Your system configuration and/or your users and groups.

To reset the system, navigate to **Settings** > **Management** > **General** and click the **System Reset** tab.

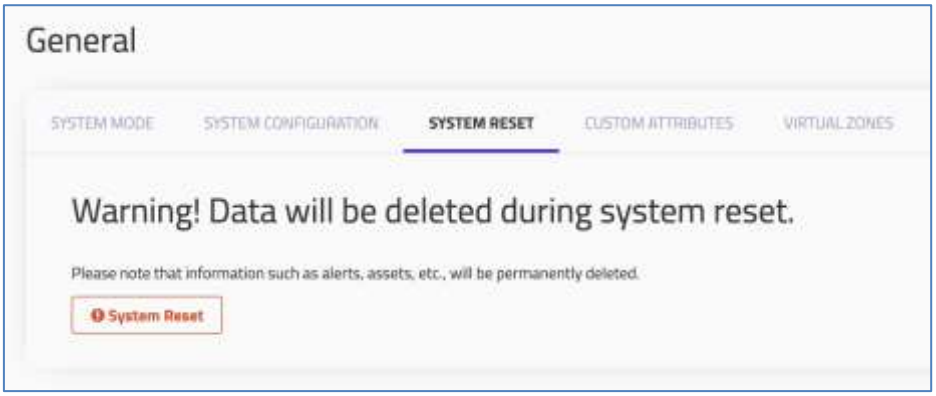


Figure 200 System Reset Tab

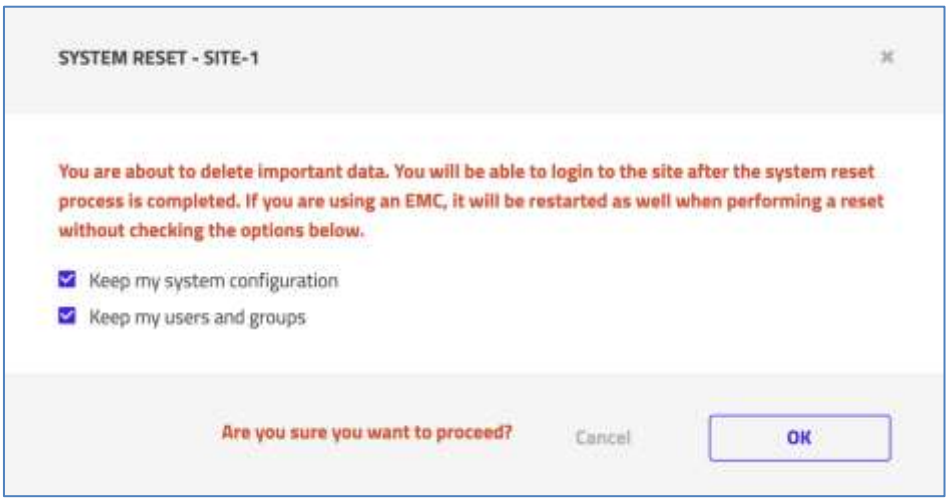


Figure 201 System Reset Dialog

- **Keep my system configuration** — Click this to retain the current configuration while deleting the database and logs.
- **Keep my users and groups** — Choose this type of reset when you want to retain users and groups.

> **Note** After you perform a System Reset, you will be required to login the next time.

10.1.4 Virtual Zone Management

To access Virtual Zone Management, click **Settings** > **Management** > **General** and click the **Virtual Zones** tab.

Use this **Virtual Zone Management** tab to set your preferred zone groupings. Assigning and reassigning assets to Virtual Zones is covered in section 5.10.

- The **Virtual Zone Management** tab appears as follows:

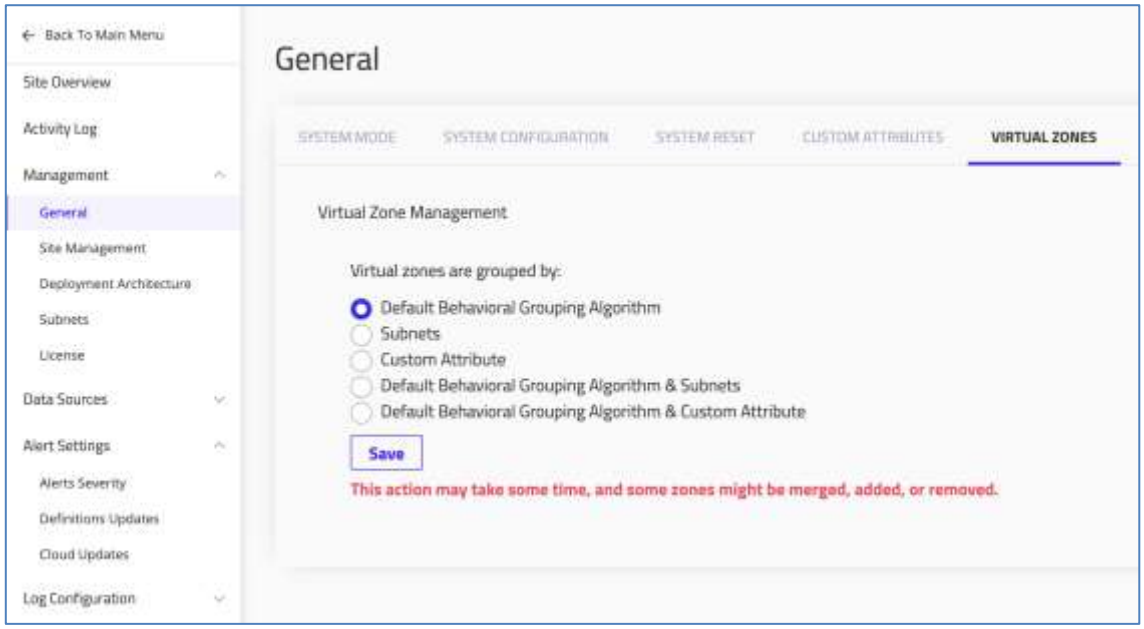


Figure 202 Changing the Virtual Zone groupings

The grouping options are as follows:

a. **Default Behavioral Grouping Algorithm** – The default virtual zone grouping is automatic. Admins can change the zones and the groupings in the Asset Page.

b. **Subnets** – Virtual Zones grouped by subnets

c. **Custom Attributes** – These user-defined fields can be used for defining and categorizing entities. This is not the default behavior.

d. **Default Behavioral Grouping Algorithm & Subnets** – Uses both sets of groupings to classify the zones. This is not the default behavior.

e. **Default Behavioral Grouping Algorithm & Custom Attribute** – Uses both sets of groupings to classify the zones. This is not the default behavior.

> Note For an overview and how to use Custom Attributes, see sections 5.8.55.7.5 and 5.8.1. For configuring Custom Attributes, see section 5.8.5.

10.1.4.1 Virtual Zone Grouped by Subnets

The current virtual zones in the system are created by an advanced algorithm that groups the assets by their device types and Purdue location. In addition, you can create virtual zones based on custom attributes, where you can configure them manually and classify them according to your preferences.

You can also choose to automatically create virtual zones by subnets. As a result, you can visualize your network and gain better understanding of the connections in aspects of virtual segmentation by subnets.

To group virtual zones by subnet:

1. Navigate to Settings > Management > General and click the Virtual Zones tab.
2. Choose Subnets (see Figure 202).
3. Click **Save.**

This feature can help your IT and OT teams to segment the network by subnets.

10.2 Site Maintenance

The **Site Maintenance** page enables you to select multiple sites to upgrade to the EMC version. This page is relevant for systems configured as an EMC; it is displayed only when the EMC is selected in the site dropdown.

10.2.1 Overview

You can select individual or multiple sites to upgrade directly from the EMC. You can use this page to enable **Automatic upgrading of sites** following the EMC upgrade.

From the **All Sites** page you can check the various site version numbers at a glance to see which ones require updates:

Figure 203 All Sites - Example

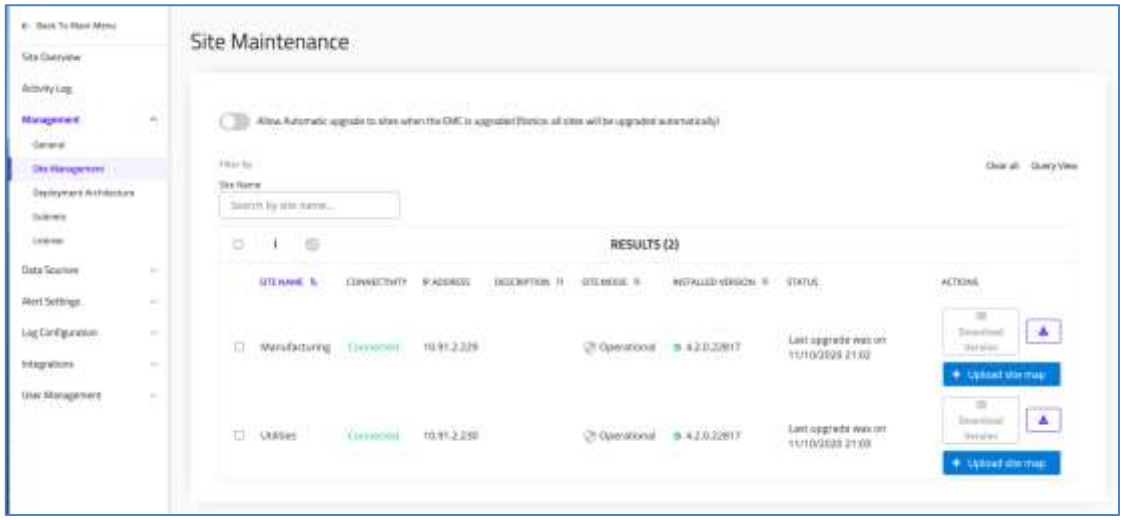


Figure 204 Navigating to the Site Maintenance Page

When upgrading sites manually, after upgrading the EMC to the new version, navigate to the **Site Management** page to select which sites to align with the same version as the EMC. The Download operation will download the newest version of the EMC to the site.

The manual upgrade process works in two phases: Downloading the upgrade package and then running it. You can select whether to automatically perform the two phases one after the other for all selected sites, or to perform one phase and then trigger the next phase manually.

First update the EMC to the new version, and then proceed to the **Site Management** page to download the new EMC version to the target site/s or Download and immediately install them.

10.2.2 Updating Sites

Navigate to **Settings** > **Management** > **Site Management**.

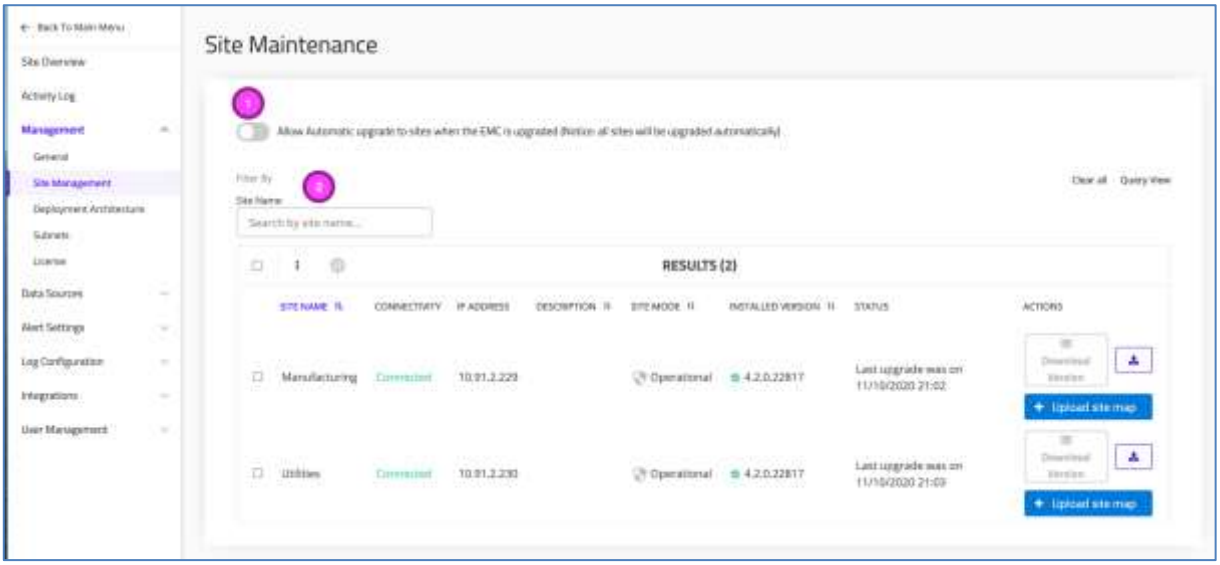


Figure 205 Site Maintenance

1. When **Automatic upgrading of sites** is enabled, all sites will be upgraded automatically following the EMC upgrade.
   The instructions below apply when the automatic upgrades are **not** enabled.
2. Use the **Site Name**  filter to find a specific site or a group of sites for performing Site Maintenance; you can filter by multiple criteria. Filtering is useful when you have many sites that span several pages.
3. View and modify your Site Maintenance information as shown below.
4. Use the **Page Selector**  to quickly jump between Site Management pages.

Figure 206 Site Maintenance - Results table & Toolbar

1. The **Results bar**  displays the total available sites.

   In the **Site Maintenance** toolbar:
2. Use the **checkboxes** to select individual or multiple sites to upgrade.

3. To choose which columns to display in the **Results** table, click **More** and then **Select Columns**.

4. **Upgrade multiple sites** button – Click this button to start the upgrade process for all the selected sites.

The default Columns for each site display the following information:

Figure 207 Site Maintenance Results table

a. **Site Name** – Name of the site

b. **Connectivity** – Whether or not this site is currently connected to the EMC

c. **IP Address** – The IP address of the site

d. Site **Description** – Optional description of the site, as configured in the **Settings > System Management > System Settings** menu.

e. **Site Mode** – Whether the site is in Training or Operational mode

f. **Installed Version** – The TIV version currently installed. It is listed with a green check when this is the latest available version. Otherwise a yellow icon appears:

g. **Status** – Details of the version status, such as timestamp of when the previous version was installed, and whether a version is pending installation

h. **Actions** – The following actions are available:

- **Download Version** – Choose whether to download the version and control the time of installation; or to download the version and install it immediately:

Prior to downloading, the system provides a confirmation screen with details of the name of the site/s selected for upgrading; the version number of the upgrade and a checkbox for saving the system backup (which includes databases, logs, users and groups).

> Note: During the upgrade process, the site interface will not be available, and you will not be able to do any modifications for the site via the EMC until the process is completed.

- Select **Download Log**  to download the log.
- Select **Upload Site Map**  to customize your system with an image of the site map to display in the **Enterprise Overview** page:

Figure 208 Site Map Image

10.2.3 Upgrading Multiple Sites

When upgrading multiple sites, perform the following steps:

1. First upgrade the EMC to the new version.
2. When the TIV Server checks in with the EMC, it is prompted with an option to update its software.
3. From the EMC page, navigate to **Settings** > **Management** > **Site Management**.
4. Select which sites to align with the same version as the EMC.
5. Decide whether you want to download the version and then continue the site upgrades manually, or to download and have the installation proceed automatically:
   - **Download version** – In this option, first you download, and then using this same page, proceed to select '**Install**' when you are ready.
   - Download & Install.

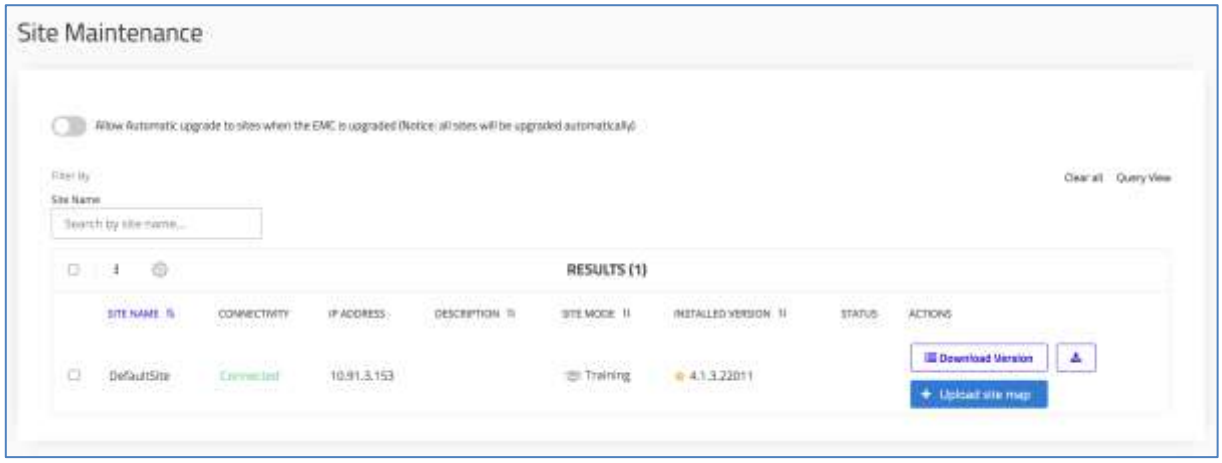


Figure 209 Site Maintenance - Download vs. Download & Install

6. Click **Upgrade multiple sites**  to apply your selection

   - The **Upgrade Sites** dialog is displayed:

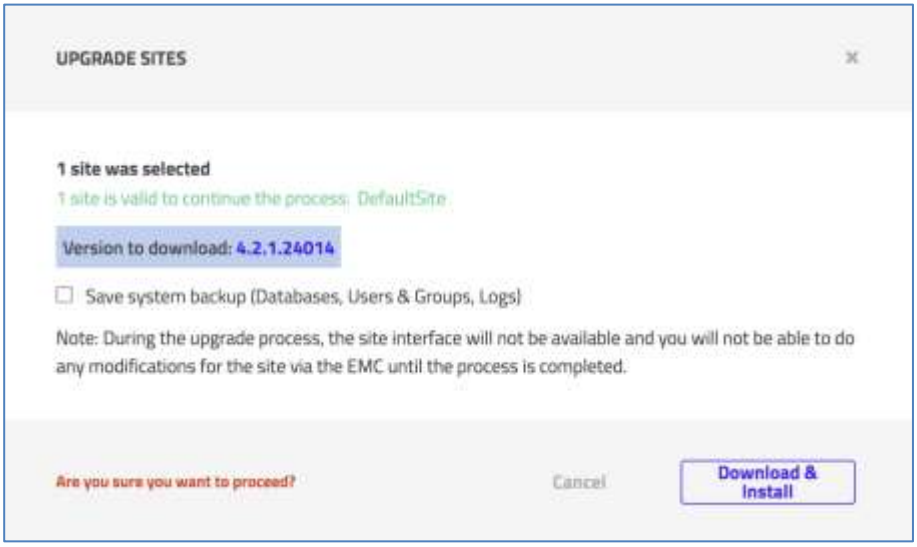


Figure 210 Site Maintenance - Upgrading Multiple Sites

Confirm the following information before pressing **Download & Install**:

- The **number of sites** selected for the download
- The **version** to download
- The **Save System backup** option is selected by default. Unselect this if you do not want the databases, users and groups, and logs backed up.

> **Note** During the upgrade process, the site interface will not be available, and you will not be able to perform any site modifications via the EMC until the download and installation process has completed.

- Be aware that although you have selected multiple site downloads with a single click, each installation process will be run individually in a serial manner.
- During the installation process, the installing icon is displayed on the row of the relevant site:

Figure 211 Site Maintenance - Installation in Progress

7. If you chose to install the version at a time under your control, click **Install Version** that appears after the download has completed.

> Note Refer to the *TIV Reference Manual* for information on upgrading via commands.

10.3 Deployment Architecture

10.3.1 EMC Deployment

To access Deployment Architecture:

1. Navigate to **Settings** > **Management** > **Deployment Architecture.**
2. Adjust your Deployment configuration settings as follows:

Figure 212 Deployment Architecture screen

Through this screen you can:

- Connect a standalone TIV to an EMC.
- Check all the sensors connected to the TIV to see whether they are activated.

In the Deployment Architecture screen apply the EMC parameters:

1. **EMC Address** - Apply a valid FQDN or IP
2. **EMC Access key** - Enter your EMC Access key
3. **Connect** to apply your settings.

10.3.2 Enabling SSL Connectivity for Site-EMC Communication

By default, SSH is used as the communication protocol between the Site and the EMC. But SSL can also be enabled (currently as a beta).

The ability to enable SSL exists both in the Wizard (during installation) as well as in the configuration setup.

In addition to changing the Site-EMC communication to the SSL protocol, this change also affects the communication between the sensor and TIV.

> Note No changes are required to the EMC, since the Site initiates the connection.

To enable SSL Connectivity:

1. Log directly into the Site

2. Navigate to **Setup > Management > Deployment Architecture** and click the Enable SSL checkbox as shown below:

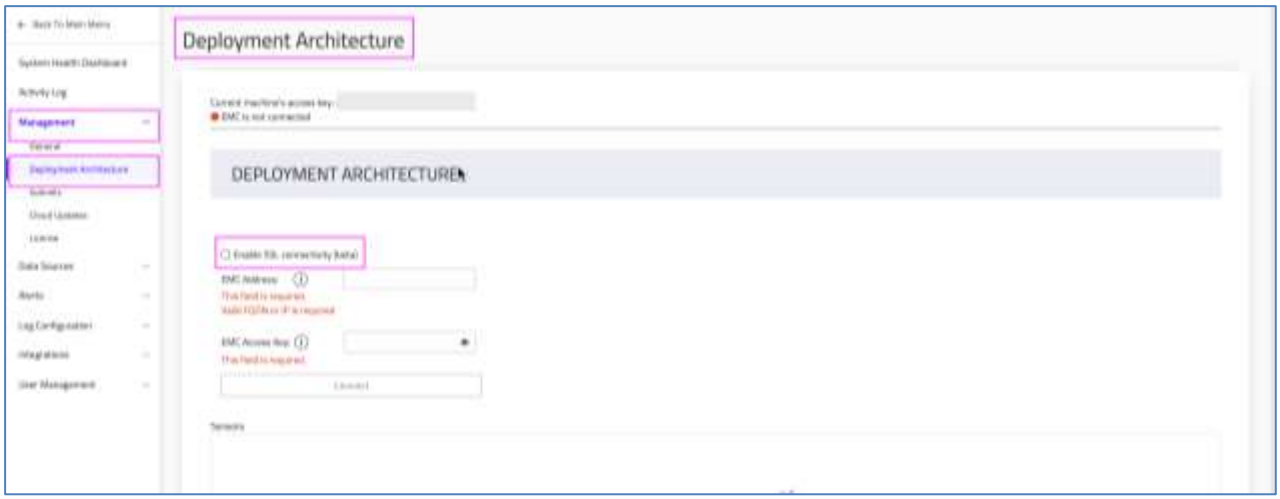


Figure 213 Checkbox for Enabling SSL Connectivity

You can log into the system only after it is fully configured.

For more information, refer to the *TIV Installation Guide*.

10.4 Subnets

Users can utilize Subnets to define and control their asset inventory and alerts in TIV. From the EMC, users can obtain a coherent understanding of the entire network, regardless of how differently sites capture their network behavior and inventory. Users can configure the subnets they have access to and choose how to view them.

In TIV, only Internal assets are shown. Based on extracted data from routers within the network, Subnets can be classified as Internal, External and Out-Of-Scope. For example, users that are focusing on OT areas may classify IT assets as Out-Of-Scope.

Admins can add, edit, or delete subnets for the various networks. The system enables approving them and tagging them as needed.

- The primary Subnet functionality includes:
- Classifying an asset type as “Out of Scope”, allowing marking subnets with lower impact on the organization and reducing the alert noise
- Bulk actions for efficiently editing multiple subnets at once
- Importing subnet lists, allowing them to override the existing subnets
- Exporting subnet lists, including tracked changes, to provide comprehensive reports to management

- Stopping to auto-calculate subnet knowledge in Training mode
- Restarting and reclassifying subnet knowledge
- Maximum visualization by calculating subnets automatically so the user does not need to manually configure the Subnets list

10.4.1 Configuration of Subnets

- To configure subnets, navigate to **Settings > Management > Subnets**:

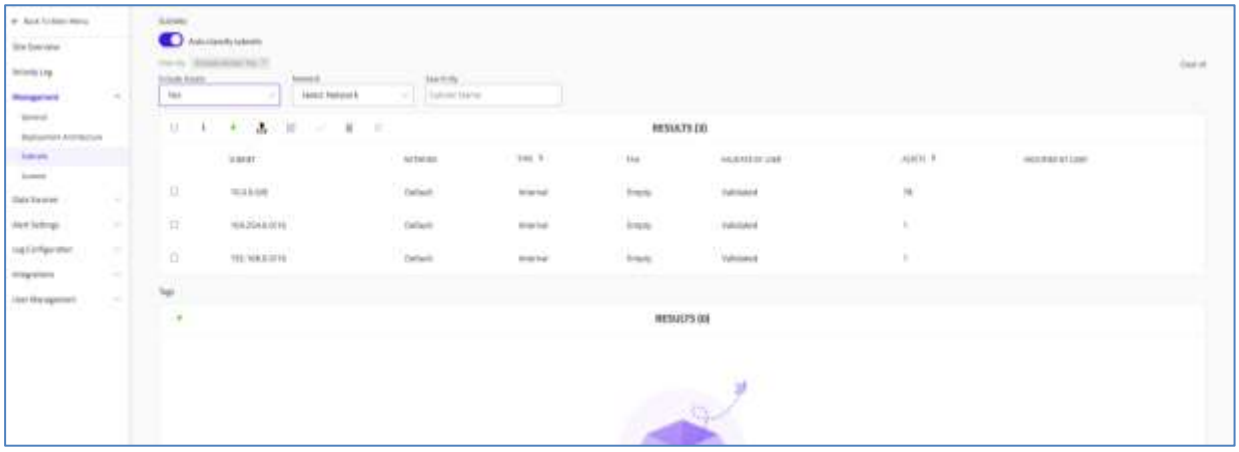


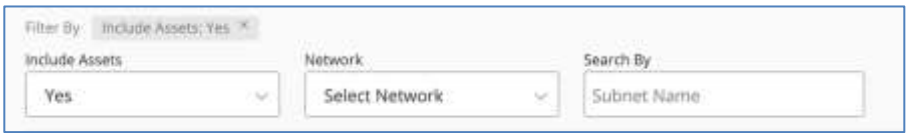
Figure 214: Subnets from TIV

All TIV subnets are presented from the EMC as well as in TIV Server. You can configure from the EMC the subnets of your connected sites or from the machine you have. The EMC has no auto-generated subnets.

- Subnets are set to  auto-classified by default

> Note: We do not recommend disabling this setting

- By default, the basic Subnet filters are **Include Assets** (set to Yes), **Network** (not selected) and a **Search By** button:



- The Subnets page includes the following default columns:

Figure 215: Subnets from the EMC

1. **Subnet** – the subnet ID, including the subnet mask
2. **Site** – the site in which this subnet exists.

> Note This field is only present when viewing Subnets from the EMC

3. **Network** – the network this subnet came from
4. **Type** – whether this asset is Internal / External / Out of Scope
   - **Internal**
   - **External**
   - **Out of Scope** – This asset type allows a reduction in the alert noise. Subnets marked in this manner have a lower impact on the environment/organization
5. **Tag** – for tagging your network. Default is Empty.
6. **Validated/Unvalidated** – if the user approved/hasn't approved this subnet
7. **Assets** – the total number of assets included in this subnet
8. **Edited by** – the system or the username of the user who last modified this subnet

10.4.1.1 Internal Subnets

- According to RFC1918, the following subnets are classified as **Internal** based on class C by default, including the subnets that are part of them:
  - 10.0.0.0/8
  - 192.168.0.0/16
  - 172.16.0.0/16
  - 169.254.0.0/16
  - 100.64.0.0/16
  - 192.0.0.0/24
  - 192.0.2.0/24
  - 198.18.0.0/15
  - 192.88.99.0/24
  - 240.0.0.0/4

- 224.0.0.0/24

- If assets in a subnet have any of the following broadcast domain protocols, they are classified as **Internal**:
  - DHCP
  - Cognex Discovery
  - IGMP
  - BROWSER
  - LLMNR
  - NET-BIOS
  - ARP
- All subnets that have assets with "Broadcast" as a special hint are **Internal**
- All multicast subnets are **Internal**

> Note The broadcast and multicast subnets will be added only if they have at least one Unicast address

> Note Routers do not transfer broadcast communication from LAN; the communication should be on the local network

> Note In training mode, in case one of the default subnets have been deleted, we will classify the subnets according to class C.

- For example, if the user deleted 10.0.0.0/8, we will add automatically the subnets that we are seen (10.2.5.0/24, etc.)

10.4.1.2 External Subnets

- All traffic that is not classified as **Internal** is considered to be **External** (unless explicitly defined by the user to be **Out-of-Scope**)
- **External** subnets are not presented via the UI unless the user manually changes the subnet type to External
- **Manually marking** External subnets – The user can manually add External subnets to the system. These manually marked External subnets will be displayed; the rest of the subnets that were classified automatically as External will not be displayed.

> Note The user won't be able to use tags on External subnets

10.4.1.3 Out of Scope Subnets

This status can be implemented only manually by the user for subnets that the user chooses not to consider as Internal. Although these subnets might be part of

the user networks, the user chooses not to consider them. By default, no subnet is classified as Out Of Scope.

This type of subnet enables decreasing the volume of alerts, thereby enabling users to focus on the subnets that matter. An example of an Out of Scope subnet is subnets that are part of the internal traffic of another plant.

This status can be implemented only manually by the user, for subnets that the user chooses not to monitor with TIV. Although these subnets might be part of the user networks, the user chooses not to consider them. By default, no subnet is classified as out of scope.

> Note In the snort engine, this subnet should be considered Internal.

10.4.2 Adding a Subnet

- In the Subnet table, click the green plus button to add a subnet
  - The **Add Subnet** popup appears:

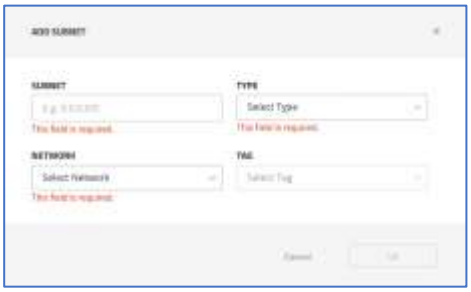


Figure 216 Adding a Subnet

1. **Subnet** – Enter the value of the subnet (in the format of x.x.x.x/y)
2. **Type** – Specify if the new subnet is External, Internal, or Out of Scope.

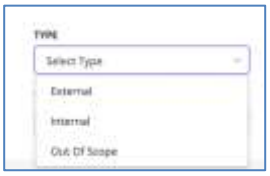


Figure 217 Adding a Subnet Type

3. **Network** – Enter the relevant network ID
4. **Tag** – Provide a tag if needed.
5. Click **OK**.

> Note: You should ensure that subnet addresses do not overlap.

10.4.3 Adding Subnet Tags

You can create custom tags and assign them to subnets. By doing so, all assets belonging to that subnet will be automatically tagged with the given tag. With subnet tags you can later view your assets grouped according to the subnets they belong to.

- To create a Subnet tag, click the **Add Tag** button:

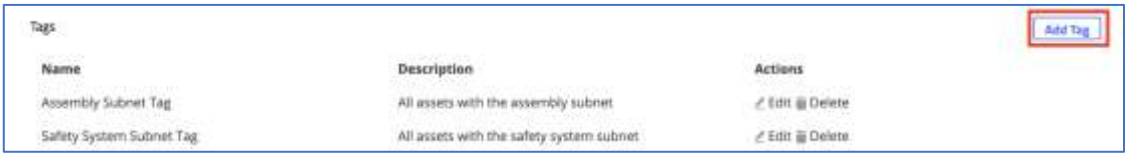


Figure 218 Adding a Tag

- Provide a name for the new tag and an optional description, and click **OK**:

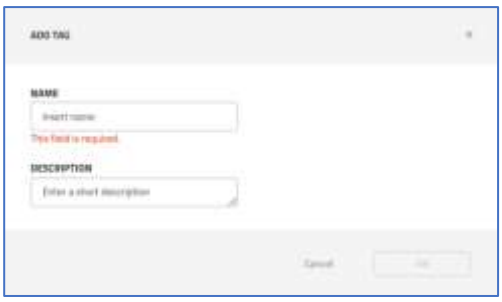


Figure 219 Providing Tag details

- To assign tags to subnets, either click the **Add Subnet** button, or edit an existing subnet to open the following pop-up, and select the tag you want to assign to that subnet:

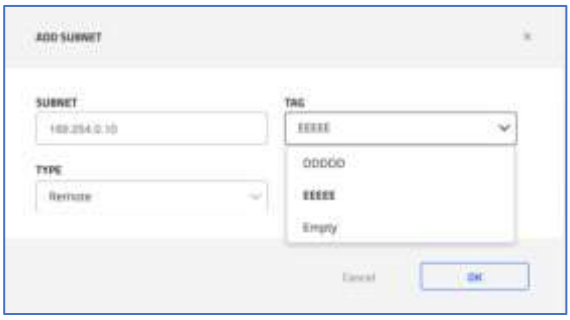


Figure 220 Assigning tags to subnets

- Click **OK** to confirm.

10.4.4 Editing a Subnet

You can use bulk actions to simultaneously and efficiently edit multiple subnets:

1. Click the checkbox ☑ of the rows of the Subnets to revise

Figure 221 Editing subnets

2. Click **Edit** button on the Subnets toolbar.
   - The **Edit Subnet** popup appears:

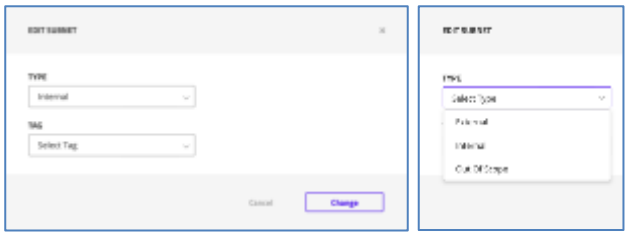


Figure 222 Editing subnets

3. Select a different **Type**
4. Open the **Tag** window to scroll down and apply one of the user defined tags

10.4.4.1 Exporting/Downloading Subnets

The Export (download) capability enables users to download an Excel report that contains all the subnets in the system. This export works in the same manner as exporting an asset. The exported information includes the subnets, types, tags, validation status, network name.

> Note The export will be supported from the EMC and TIV.

10.4.5 Exporting & Importing Subnets

This functionality is supported from both the EMC and a specific site.

Users can override existing subnets by:

1. Downloading the list as a CSV file:

Figure 223 Exporting subnets

2. Modifying the table outside of the system

3. **Importing** the subnets list back into TIV:

Figure 224 Importing subnets

- This data will overwrite the prior system values.
- An error message will appear to notify if there is a conflict

> Note: External subnets cannot be imported manually

10.4.6 Error Messages for Subnets

Table 8 System Messages

When…	Message/Present a popup
Deleting a subnet	"Are you sure you want to delete this subnet?" - already exist
Adding an Internal subnet that includes an existing Internal subnet	"This subnet has already existed as part of subnet_name"
Adding an Out-Of-Scope subnet that includes an existing Internal subnet	"This subnet is part of subnet_name, please delete it before committing any changes"

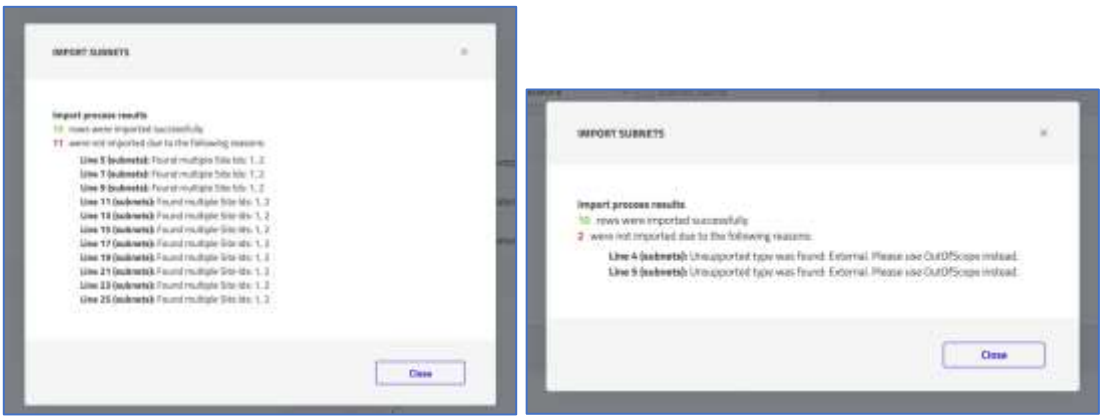


Figure 225 Subnet Error Message - Examples

10.4.7 Stopping/Restarting Subnet Knowledge

You can **stop** and **restart** calculating subnet knowledge as follows:

- Stopping calculation of subnet knowledge in training mode by setting the auto classify button to OFF
  - In the **Delete Subnet** window, press **Yes** to remove this capability:

Figure 226 Confirming Subnet deletion

- Restarting subnet knowledge by reclassifying them by resetting the Auto-classify button to ON

10.4.8 Deleting a Subnet

To delete a subnet:

- Identify the relevant subnet from the Subnet table.
- Click **Delete** from the Subnet **toolbar**.
  - In the **Delete Subnet** window, press **Yes** to remove this capability:

Figure 227 Confirming Subnet deletion

10.4.9 Subnets in Training vs. Operational Mode

Table 9 Training vs. Operational Mode

Term	Training Mode	Operational Mode
Deleting a subnet	If additional traffic is detected from this subnet again, we will re-add it	Will be considered as External

Term	Training Mode	Operational Mode
Auto classifying / calculating	Enabled by default: If users deleted the default subnets, the learned subnets will be presented based on Class C	Auto calculating does not work in Operational mode; only in Training
Adding subnets	Users can manually add subnets	Users can manually add subnets

10.4.10 Subnet Alert Behavior

- An alert is raised:
  - If there is communication between Internal subnets
  - If there is communication between External subnets
  - If there is communication between an Internal and an External subnet
  - If there is communication between an Internal and an Out of Scope subnet
- Communication between Out-of-Scope subnets or between an External and an Out of Scope subnet: An alert is auto-approved, with the exception of security alerts:
  - Known Threat alerts
  - Scanning alerts
  - MITM alerts
  - Baseline rule alerts
- New asset alerts will be approved automatically if they originated from a multicast message

10.5 License

To view the license:

- Navigate to **Settings** > **Management** > **License** to apply your license settings as follows:

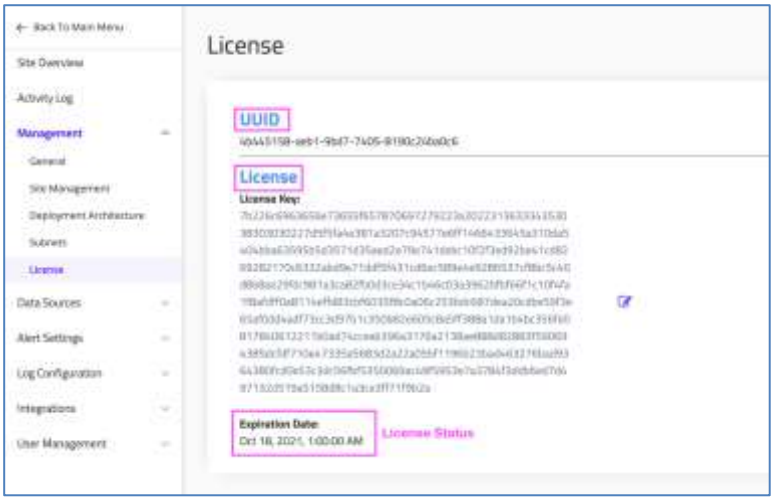


Figure 228 License screen

Through this screen you can enter your UUID and license key:

- **UUID** – Enter your unique customer identification number. Obtain this number from your Tripwire Customer Success Manager.
- License Key:
  - Contact your Tripwire Customer Success Manager with your UUID and they will supply you with the relevant **License Key**
  - Use the **Edit** button to apply it or change the existing license key
- View the License Status:
  - Valid – Lists the **Expiration Date** and time
  - About to Expire – Shows the **Expiration Date** and time when the expiration is imminent, warning that the system will stop digesting data
  - Expired – Shows the date that the system has already expired. In this case, the system is not ingesting any new data.

  These License Statuses are also shown in the System Health Dashboard.

10.6 Cloud

Cloud connectivity enables your EMC, on-premise and virtualized deployment options to further extend the cybersecurity of your OT networks by connecting to edge cloud-based technology.

Cloud connectivity is totally safe, and communication is secured over SSL. TIV customers share data for empowering their analytics and knowledge anonymously and privately, according to GDPR regulations.

Cloud services provide the following:

- **Threat Intelligence** - Automatically update threat and risk intelligence (CVEs/IoCs/signatures).
- **Data Analytics** - Trusted indications about data based on the wisdom of the crowd. TIV's data analytics is based on frequency of behaviors over big data shared by customers anonymously and privately. This helps you base your actions on the wisdom of the crowd.
- **Customer Experience Improvement Program (CEIP)** - Helpful tips and guidance about new functions.

10.6.1 Key Technical Points

To enable Cloud access, you must open a rule in your firewall policy to allow SSL connectivity (inbound and outbound) with
our cloud URL http://prod.cloud.claroty.com/.

The following table summarizes the technical key points to be familiar with when working with Cloud solution:

Table 10 Cloud Solution

Subject	Summary
Connectivity	■ The Data is sent to the cloud anonymously according to GDPR regulations over SSL ■ The Initiator of the SSL can only be a TIV/EMC machine ■ All cloud connectivity work is done with a new worker named "agent" ■ The Cloud is not connected directly to your TIV machines ○ Data Sent over API Tunnel
Working processes	■ TIV queries the cloud for new update tasks ■ Querying occurs every 10 min. by default ♦ This interval is configurable via the CLI. Contact Tripwire Support for further details. ■ If an update is available, it will be sent to TIV via API ■ Data is stored anonymously (customer UUID is attached to each record)
The Data	■ **Sent from the cloud** – TI updates, cloud reputation of zone rules ■ **Sent to the cloud** – TI bundle version, Firmware version, model version, serial number of assets without CVE's, Policy rules (SRC zones, DST zone, category, action, protocol) We do not send any sensitive information such as IP,MAC, PCAP's etc.
Security	■ Connectivity - The connection is only initiated from the EMC/TIV using a secure SSL tunnel.

Subject	Summary
	■ The data - Threat intelligence bundles, vendor & FW of asset, policy rules. No sensitive data such and IP, MAC is being sent. ■ Anonymous data - No possible correlation between the data to customer. The data is correlated using a customer UUID.

For further information about the Cloud solution, see the *TIV Reference Guide.*

10.6.2 Cloud Update Settings

To change Cloud Update settings:

- Navigate to **Settings** > **Management** > **Cloud Updates**.

Details for configuring Cloud updates are detailed in the *TIV Reference Guide* and covers the following Cloud parameters:

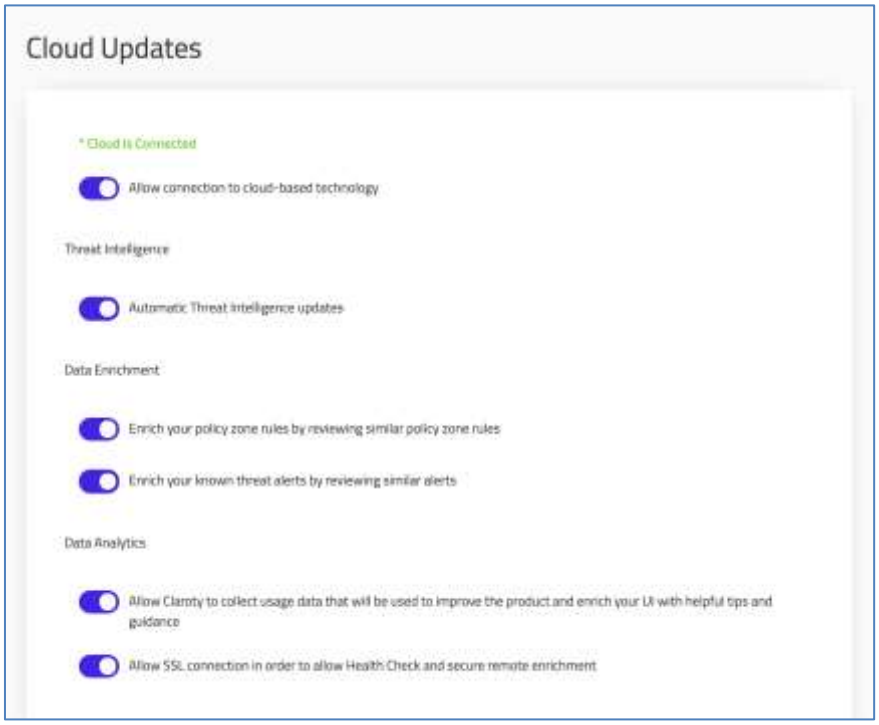


Figure 229 Configuration - Cloud Updates Menu

Connection

- Cloud is Connected/Not Connected indicator
- Allow Connection to Cloud based technology

Threat Intelligence

- Automatic Threat Intelligence Updates

Data Enrichment

- Enrich your policy zone rules by reviewing similar policy zone rules
- Enrich your known threat alerts by reviewing similar alerts

Data Analytics

- Allow TIV to collect usage data that will be used to improve the product and enrich your UI with helpful tips and guidance
- Allow SSL Connection in order to allow Health Check and secure remote enrichment

10.6.3 Cloud Reputation

This feature explains how common the signature discovered in your site is.

When the system raises a known threat alert in your environment, it will compare this signature among different sites with the same alert and signature. The system will send the signature ID from the cloud and receive information to the cloud. You will receive a cloud reputation response. This will give you a better understanding about this signature so you can solve the alert accordingly.

To access the cloud reputation column:

- In the Main Menu, navigate to **Threat Detection > Rules > Zone Rules**.

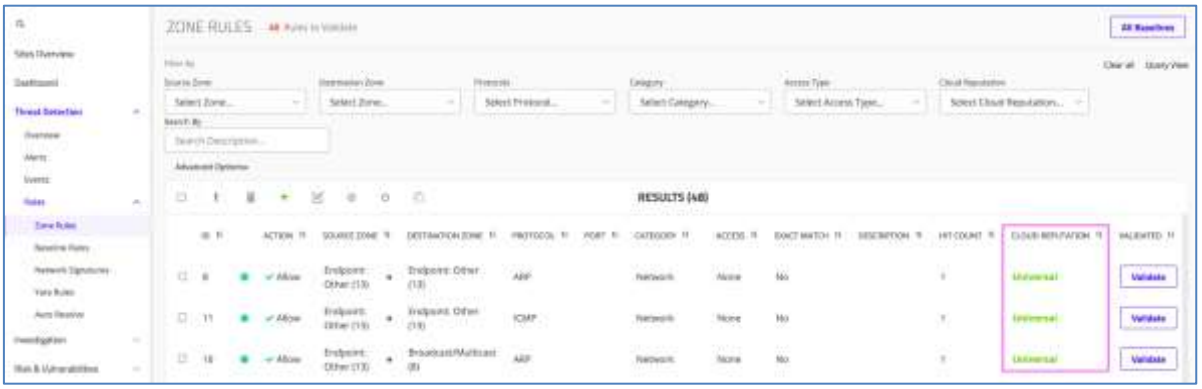


Figure 230: Cloud Reputation Column

The cloud reputation will explain how common the signature is using the response types below:

- **Universal** - This signature was seen in alerts in most of the other sites.
- **Common** - This signature was seen in alerts in a large number of different sites.
- **Uncommon** - This signature was seen in alerts in a small number of different sites.
- **Rare** - This signature was rarely seen in alerts in different sites.

10.7 ClarotyOS

ClarotyOS is an operating system based on CentOS. It enables you to use CentOS commands when you have a root shell. For more information on installation see the *TIV Reference Guide*.

11 Configuring Data Sources [Only Admins]

11.1 Active Detection

Tripwire Industrial Visibility (TIV) is for industrial environments and is designed to provide depth of threat detection and analysis. It offers passive anomaly detection and monitoring technology coupled with "safe-active" technology. To further enhance network visibility, TIV's safe-active technology adds active device integrity checks to enhance security.

TIV has a deep understanding of:

- ICS network assets
- Communications
- Protocols
- Communication patterns

The system discovers all assets and asset configuration details across the entire industrial network – both IP assigned assets and assets that communicate over serial connections. Active Detection further extends this asset visibility and coverage.

With periodic or on-demand inspection of ICS- network controllers (e.g. periodic verification of controller device firmware, control logic, and other settings), the system provides comprehensive visibility into the controller state. By validating the integrity of existing and new devices, TIV can make sure that no unauthorized changes were made without negatively impacting performance.

TIV's technology enables organizations to automatically maintain an up-to-date inventory throughout their IT/OT/IoT infrastructure from L5 to L0 devices. The inventory contains critical device and network information required by Security and SOC teams to proactively manage the security and productivity of the industrial network. Collected information is made available to third party external tools such as Security Information and Event Management (SIEM) solutions and Configuration Management Databases (CMDBs).

The pillars of TIV's Active Detection solution are Active Discovery Tasks, Asset Queries, and Active History. Both task and query functions can be scheduled to run on a periodic basis, providing continuous discovery and detection.

To use active monitoring and detection:

- Navigate to **Settings > Data Sources > Active Detection**.

11.1.1 Safe Active

TIV's "Safe-Active" technology means every network query is tightly controlled and monitored by the user. No action is taken within the network without the user explicitly triggering it.

The user controls the Task process:

- Stopping all Tasks and Queries with a single click using the "Red Button" .
- Controlling the time frame of tasks.
- Controlling the number of active Tasks and Queries that can run simultaneously (the default is 1).

TIV presents up to two variations for each Task and Query:

- **Basic** – With basic tasks and queries, input parameters are set to the optimal value by default, allowing users with little experience to safely perform Active queries.
- **Advanced** – While Advanced Active Detection requires more input data from the user (i.e. Port), it allows greater control over the Task or Query process.

TIV's Active solution uses vendor native protocols to perform tasks. This ensures only safe and native traffic within the network.

> We recommend performing Active Tasks and Queries during maintenance hours.

11.1.2 Prerequisites

- When configuring Active discovery tasks and asset queries, we recommend that users be familiar with the type of assets within the various network segments, in order to select the most appropriate type of tasks and queries.
- It is also advisable to identify specific network segments and/or assets that may be highly sensitive to out-of-band communication, such as third-party queries. When configuring tasks and queries, you should test and be sure to exclude these assets.
- TIV Active Monitoring and Detection uses Active network communications that utilize various protocols and ports to discover and query your assets. Before running it for the first time, make sure to allow the relevant protocols and ports in your firewalls and gateways. Refer to the *TIV Reference Guide: Query, Discovery, and Profile Types* for a full list of available tasks and queries as well as the protocols and ports they use.

Enable Active Query in the EMC as well as in all the Sites during Installation.

11.1.3 Working with Active Detection

With the goal of discovering all assets within the desired network locations, and learning all possible properties of these assets, take the following steps:

1. Configure your Asset Discovery Task to create a collection of scheduled discovery tasks. A Discovery task is defined by several parameters:
   - Setting the network segment or IP range in which to discover assets
   - Setting the type of the discovery task method to use
   - Choosing a set of queries (either created by the user or predefined out-of-the-box)
2. Configure your Asset Queries to create a collection of scheduled Tasks within the system to match the type of assets in your network and the way you would like them to be inspected by TIV.
3. Once all desired tasks are configured, enable them to run on schedule.
   - Alternatively, tasks can be triggered manually when needed.
4. As asset discovery tasks are run, followed by dedicated queries to gather more detailed information for the identified assets, the Assets Page is gradually populated with new assets and their detailed information.
   - Assets that are already in the system, and for which queries are assigned, will be queried again to detect any change in asset state or information. Any such change shall trigger an alert within TIV.
5. Review the assets found and their information:
   - Review the Assets Page to find assets with missing information and check your queries to understand if the correct query is being run on these assets.
   - Look for assets you expect find; if any are missing, check your tasks to understand if there are blind spots, or if there are any wrong types of task configurations.
6. Keep validating and updating the configured set of tasks on an ongoing basis:

- This ensures that all desired network segments are covered by at least one task, and that any sensitive asset for which an active approach is not desired is either not included or explicitly excluded.
- Similarly, keep your configured queries set updated with, for example, additional queries in case new types of assets are introduced in the network, or update queries schedule if needed.

7. To ensure safety across time zones: In cases where you are located in a different time zone from the target time zone in which you are performing Active tasks, change the Time Zone to represent the time zone of the site where the Active Tasks are will run.

11.1.4 Active Detection Flow

The base flow for working with Active Detection involves the following steps:

1. Setting up a Discovery Task
2. Configuring Queries to run on the Discovery Task
3. Running the Discovery Task
   - The Discovery Task assigns Queries to the assets automatically
4. Assigning a Get Info task to the assets for continual flow of asset information
5. Consider using a Discover Disconnected task to test connectivity

> Note: Smart Discovery functionality will be provided in a future release.

11.1.5 Active Tasks

To access the Active tasks, navigate to **Settings > Data Sources > Active Detection > Tasks**

The following Active tasks are available:

- Discovery
- Get Info
- Discover Disconnected

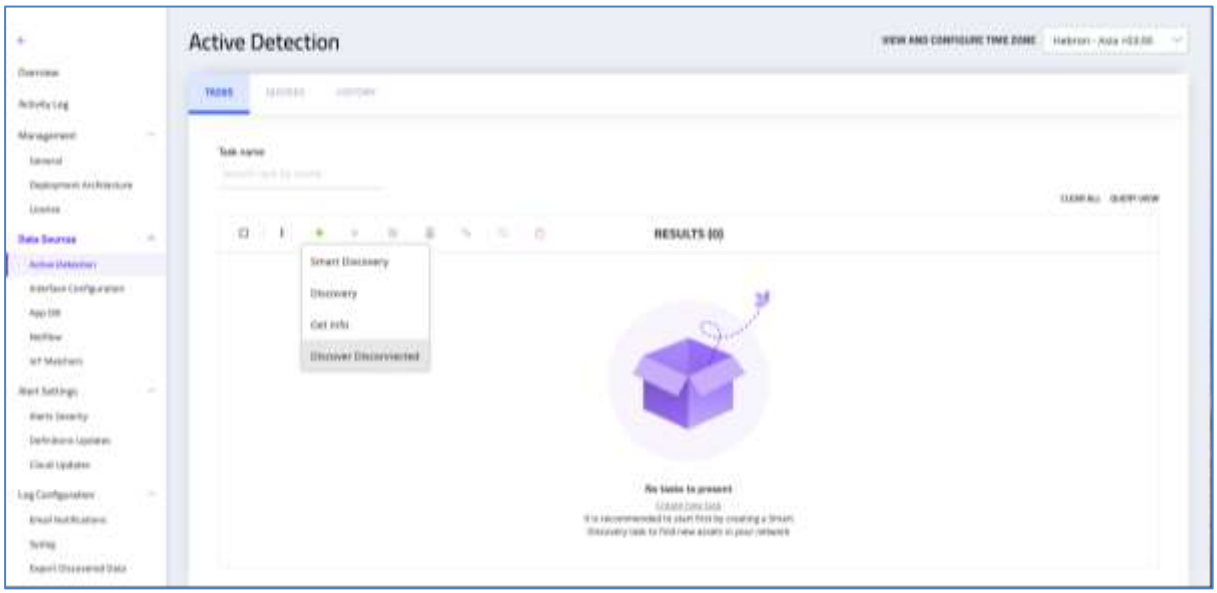


Figure 231: Active Detection Tasks

With Active Tasks, TIV employs several network asset discovery task techniques to find and learn about assets in the network:

- Ping Sweep
- ENIP broadcast transmission
- SNMP ARP cache reading and more.

Each technique is different in terms of:

- The type of assets it can discover
- The ability to discover across routing points
- The intrusiveness

Therefore, it is recommended to read through section **Query, Discovery, and Profile Types** in the *TIV Reference Guide* to learn about the various techniques and carefully select the right discovery technique to use for each scenario.

During the task process, newly found assets are populated into the system automatically, along with their IP address and their MAC address (if learned) and are visible on the Assets Page.

11.1.5.1 Configuring Asset Tasks

After setting up your queries, configure your discovery tasks. A Discovery task uses different techniques to find assets on the configured network segments, and then immediately follows with a set of queries to delve deeper to obtain more asset information and properties of the discovered assets.

To configure asset discovery tasks:

1. Navigate to **Settings > Data Sources > Active Detection > Tasks.**
2. Click the green plus button to add a new task:

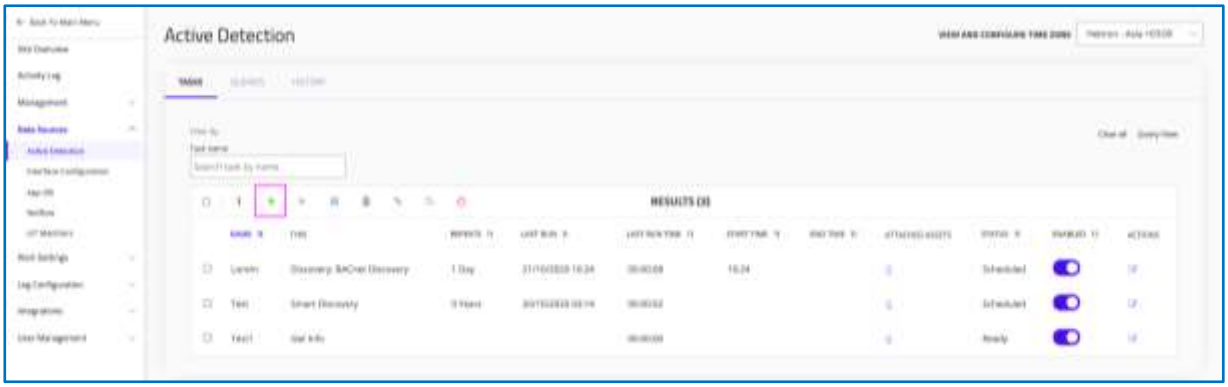


Figure 232: Adding a New Task

3. Select which type of Task to add:

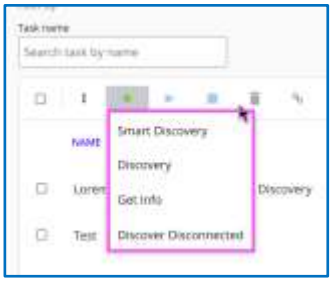


Figure 233: Selecting a New Task

11.1.5.2 Configuring Discovery Tasks

1. In the **New Discovery** configuration dialog, set the following parameters:

Figure 234: Adding a Discovery Task

> **Note** The displayed fields, and the ones explained below, change depending on the selected task Type and Sub-Type.

Input Validation: Depending on the context, limitations for the input fields will displayed, accompanied with violations (in red text) for warnings or when the input value does not comply with the expected value.

Figure 235: New Discovery Task - SNMP Example

a. **Name** – Provide a meaningful name for the task.
For instance, "Ping Discovery of Hirschmann Assets on 192.168.0.0/24"

b. **Type** – Select the type of Discovery Task. Refer to the *TIV Reference Guide: Summary Discoveries Table* for the list of available discoveries. Their descriptions and the relevant required parameters are available in the *Detailed Discovery Table* therein.

c. **Sub-Type** – Depending on the Discovery task selected, the form may display additional Sub-Types that need to be selected when applicable:

   - For example, selecting an SNMP ARP Table Discovery will require selecting a Sub-Type from either SNMPv1, SNMPv2c or SNMPv3

Note: The **Intrusive Level** appears, based on the Type/Subtype selected:

TIV immediately notifies the user in the configuration dialog of the intrusive level (**Low/Medium/High**) of the selection, including a short explanation, reflecting how much risk is being taken by this choice.

d. **Discovery Parameters** – Each task **Type** and **Sub-Type** requires a different set of parameters to be configured. Depending on the selection, the form will automatically update with the appropriate task parameters fields to be configured. Some fields are automatically filled with default values, such as port number.

e. **Interface Name** – Provide the name of the TIV machine interface name to be used to perform the Discovery task, such as `eth0` or `eth1` (relevant for some of the Task Types; not all)

f. **Custom Label** – Add a custom label if desired. The custom label will be attached to all assets discovered by the configured Discovery task.

- Use the following format to define custom labels:

```
name: value, name: value, name: value,…
```

- For example: `Location: South Building, Process: Bottle Labeling`

g. **IP Address** *(where available)* – Type the network segments on which you wish to perform the Task. The field can be filled with:

h. **Port** *(where available)* – Enter the Port value

i. **IP Range** *(where available)* – Enter the network segments on which you wish to perform the Task. The field can be filled with:

- CIDR Network segment.
  Multiple segments can be entered separated by a comma.
  Example: `192.168.0.0/24`
- IP Range, or multiple IP ranges separated by a comma
  Example: `192.168.1.1-192.168.1.254`
- Specific IP addresses, separated by a comma
- A combination of all the above, separated by commas

j. **IP Range Exclude** *(where available)* – Provide specific IP addresses, ranges or subnets to exclude from the current Discovery task

k. **Subnet** *(where available)* – The CIDR notation of the desired network segment to send the broadcast packet to

l. **Choose Network** – Select the TIV network to which the assets found during the task will be assigned

m. **Auto-Assign Queries** – Select one or more already configured queries to be automatically assigned to assets found during the Discovery Task:

- If one or more queries are selected, once a new asset is found during Discovery task, the system will attempt to query the asset using the selected queries, to obtain more asset information and properties.

- If one or more of the queries is successful, the query will automatically be assigned to that asset, so that when the next scheduled run of that query is triggered, it will query the asset

n. **Repeats** – The task shall run according to the interval defined:

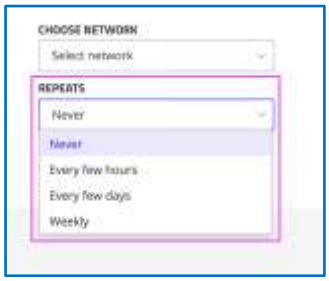


Figure 236: Setting Task Recurrence

- **Never** – Use this for a one-time task (this is the Default)
- **Every few hours/days** – Set the desired scheduling for the task to run on the configured network segments or IP ranges
- **Weekly**– Set the scheduling start and end times

> Note If the End Time is reached while a Task is already in progress, the Discovery task will be immediately stopped.

♦ Continue to set the recurrence details, including **Time Frame**, which can be set from a start time until the task is completed or until a set end time.

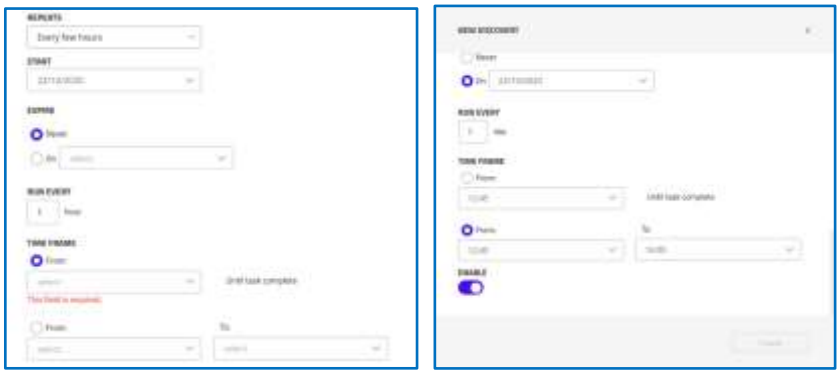


Figure 237: Setting Task Recurrence Details

See section 11.1.5.5 for further details on Recurring Tasks.

2. Keep the **Enable** button set to **ON**

♦ **Enable** – When ON, the query will be created and will immediately follow its scheduling setting and run accordingly.
When this is OFF (default), the task will be created but will be disabled, meaning it will not run despite its configured scheduling until it is enabled. However, even when disabled, it can be run manually.

3. Click **Create** to finish configuration of this Task.

> Note CrowdStrike Example: Refer to the *Tripwire Industrial Visibility - CrowdStrike Falcon Installation Guide* for detailed instructions on how to use Active Detection for asset discovery and enrichment with CrowdStrike.

11.1.5.3 Configuring Get Info Tasks

The **Get Info** task is used to update asset information. It works by querying discovered assets with the queries that have already been assigned to each asset. To use this capacity as effectively and safely as possible, the user updates info for specific assets by setting queries to run only on specific assets at precise times and on a predetermined controlled schedule.

1. From the Active **Task** tab, click the green plus button to add a new task
2. Choose the **Get Info** task
   - The **New Get Info** dialog appears:

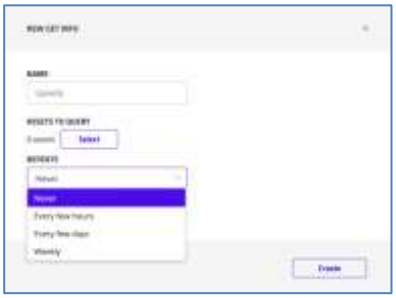


Figure 238: Get Info Task

3. **Name** – Provide a name for this Get Info task
4. **Assets to Query** – Select the Assets on which you want to run this query
   - Once selected, the total number of assets will appear
5. **Repeats** – Choose the recurrence pattern that is appropriate for this query. See recurrence details in section 11.1.5.5)
6. Press **Create**.

11.1.5.4 Reviewing Tasks

Pre-existing Tasks are displayed in tables located in the **Active Detection** pane within the **Settings** > **Data Sources** menu. Navigate to the **Tasks** tab to review them:

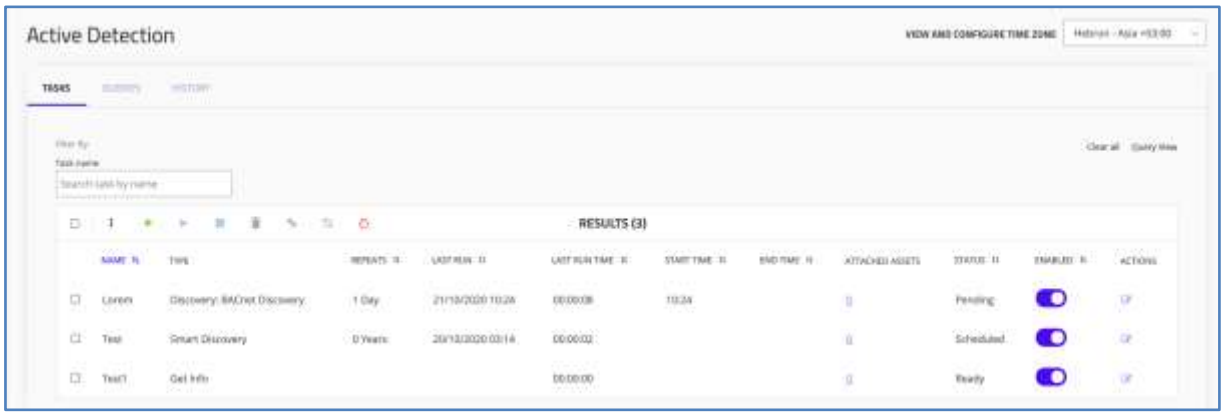


Figure 239: Active Detection - Tasks

The Active Detection Tasks table displays the columns as described below. Columns that are sortable are listed with arrows. When a sort is applied, the table is sorted according to a column title that is highlighted, which is accompanied with an icon (for an ascending sort) or a (for a descending sort).

- **Name** – The name of the task
- **Type** – The type of task configured
- **Repeats** – The configured scheduling interval, or 0 if no recurrence. For example: 3 Days – indicates that this task will run every 3 days within the configured time range
- **Last Run** – The timestamp of the last run
- **Last Run Time** – The duration of the last time the task was run
- **Start Time** and **End Time** – Within this time range, the task will run according to its defined interval
- **Attached Assets** – Shows the number of assets discovered by task (clickable). After you click on the number, you are directed to the filtered asset lists based on the number of discovered assets.
- **Status** – Provides indication on the current status of the task:
  - **Created** – A new task action has been created while another task is running (when the first task finished running, the status will change to **Scheduled**)
  - **Ready** – The task action is ready to run
  - **Pending** – The task action is pending other tasks to finish before it can run
  - **Scheduled** – A new task action has been created and will run according to its schedule
  - **Running** – The task action is currently running

- **Assigning (X/Y)** – Assets are discovered, and queries are assigned to the discovered assets
- **Completed** – The task action has finished running
- **Stopping** – The task action is being stopped after the user selected to stop it
- **Stopped** – The task action has been stopped by the user
- **Force Stopped** – The task action has been stopped by the user, but the system couldn't perform a clean stop and force stopped the task
- **Expired** – The task action has finished running

- **Enabled** – Indicates whether the task is enabled or not. When it is disabled, it will not be run again regardless of its defined scheduling
- **Actions** – Currently only **Edit** is available. Click to edit the discovery task.

11.1.5.5 Recurring Tasks

To set and control recurring tasks and queries:

1. Toggle on Recurring Task.

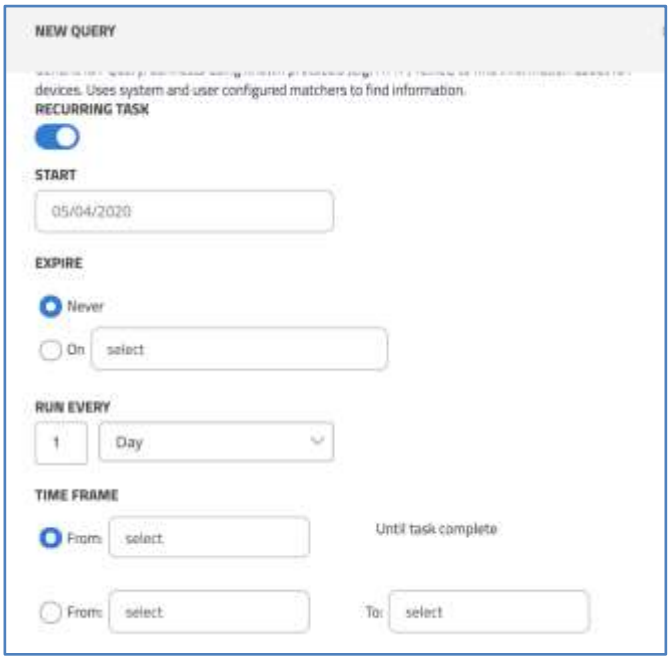


Figure 240: Recurring Task

2. Set the **Start** date.
3. Set **Expire** to Never or select a date.
4. Set **Run Every** for how often it reoccurs (hour, day, week).

5. Set the **Time Frame**. You can set **From** an hour (e.g. starting from 9 am) until the task completes or you can set the **From** and the **To** hour. For example, if you are running maintenance from 8 am to 10 am, set it from 8 am to 10 am.

> Note If you choose to run every [x] Weeks, set which days to repeat the task under **Repeat On.**

For example, you can configure the task to run every other week on Monday, Wednesday and Friday at a set time:

Figure 241: Weekly Run settings

11.1.5.6 Editing Tasks

To edit a task, select the row of the task and click the Edit button in the Actions column on the far right:

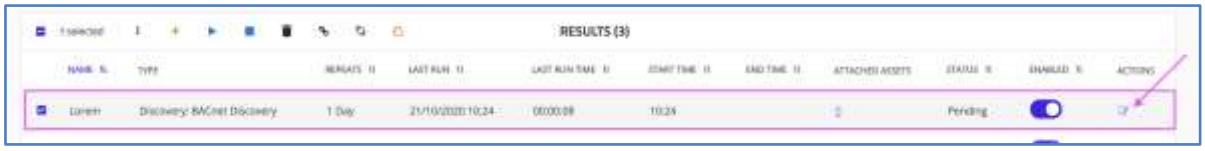


Figure 242: Editing a task

11.1.5.7 Filtering for a Task

Use the Filter capability to find specific Tasks by their names:

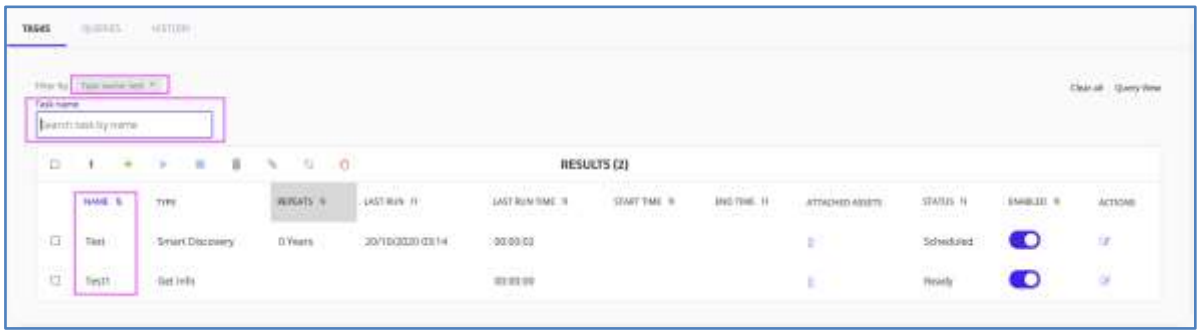


Figure 243: Task name filter

11.1.5.8 Assigning an Active Task/Query from the Asset Page

To add an Active task/query from the Asset Page:

1. Navigate to the Asset page from the Main Menu.
2. Select the relevant asset/s
3. Click the **Assign Task** or **Assign Query** button from the Asset toolbar
4. Continue to configure the details :
   - For a Task, in the same manner as described in section 11.1.5.111.1.6.1
   - For a Query, in the same manner as described in section 11.1.6.1

> Note Unassigning the Task or Query is performed in the same manner.

11.1.5.9 Stopping a Task

A Discovery Tasks, depending on its type and the number of assets it applies to, may take a long time to complete.

To stop a running task:

1. Navigate from **Settings > Data Sources > Active Detection** to either the Tasks table or the Queries table.
2. Select one or more Task/Query task by checking the task checkbox.

   On the top ribbon  :
3. To stop a single Task/Query task, click the Stop  button
4. To stop all current Task/Query tasks, click **Stop all tasks** 

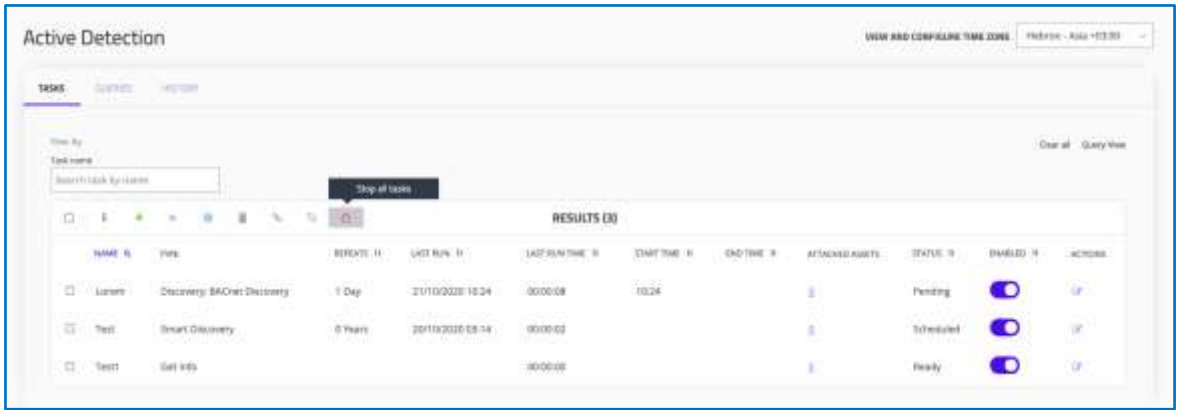


Figure 244: Stopping Tasks

11.1.5.10 Running a Task on Demand

While Tasks are usually configured to run on a scheduled basis, occasionally it is useful to run a specific one on the spot.

To trigger a Task to run immediately:

1. Navigate to either the Tasks table (under Settings > Data Sources > Active Detection).
2. Select one or more Tasks by checking their checkbox(es).
3. Click **Run Now** on the top ribbon:

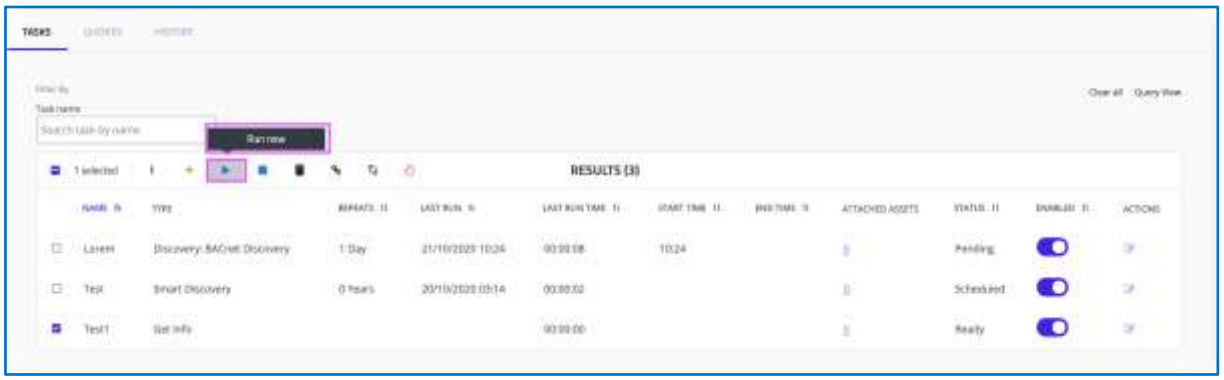


Figure 245: Selecting a Task/Query to run immediately

11.1.5.11 Enabling or Disabling a Task

New created Tasks are disabled by default, unless specifically enabled by the user during the creation time.

To enable or disable an existing Task:

1. Navigate to either the Tasks table (under Settings > Data Sources > Active Detection).
2. Select one or more Tasks by checking their checkbox(es).
3. Click the **Enable** or **Disable** button on the top ribbon:

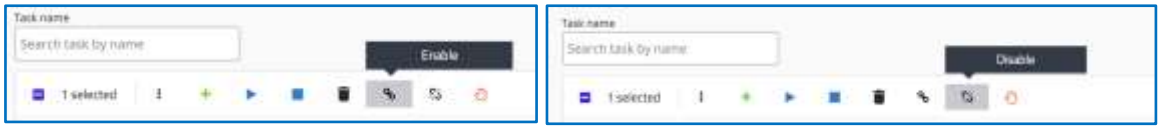


Figure 246: Enabling/Disabling a Query/Task

11.1.5.12 Configuring Discover Disconnected Tasks

Discover Disconnected is a lightweight task that runs a minimal query for each asset in order to determine if an asset is having communication issues.

This task checks whether assets that have already discovered in the past are still responsive. By performing this lightweight query, users can use its results to consider if/when to run it with a higher frequency compared to other heavier tasks. For example, a Get Info task may be scheduled to run weekly while its associated Discover Disconnected task may be scheduled to run daily.

Figure 247: Discover Disconnected Task

1. **Name** – Provide a name for this Discover Disconnected task
2. **Choose Network** – Select the network that will be inspected
3. **Assets to Query** – Select the Assets on which you want to run this query
   - Once selected, the total number of assets will appear
4. **Repeats** – Choose the recurrence pattern that is appropriate for this query. See recurrence details in section 11.1.5.5)
5. Set **Enable** when the task info is complete
6. Press **Create**.

11.1.5.13 Discovered By

The Discovered By capability enables each new asset that was discovered as a result of a task to indicate *which* active task identified it and its source. The system also tags nested devices with the task that discovered them.

Figure 248: Discover By Column

If multiple tasks discover the same assets, these assets should be counted in each one of the tasks and the asset will display the multiple tasks that discovered it.

11.1.6 Asset Queries

Following the discovery of an asset, the Active Asset Query can be initiated automatically or manually, to perform a deeper active inspection to retrieve additional information:

- Device type
- Vendor and model names
- Firmware version
- Asset vulnerabilities
- Operational status
- Configuration issues.

The system offers several types of Active Asset Queries including:

- SNMP
- CIP
- DNP3
- Other Native Vendor OT protocols.

Different query types have different properties, advantages, and disadvantages. Therefore, it is recommended to review the section **Query, Discovery, and Profile Types** in the *TIV Reference Guide* to learn more about each type and find the appropriate one.

11.1.6.1 Configuring Asset Queries

The first step of using TIV Active solution is to configure a set of queries. These queries can later be selected in a task to be run automatically when a new asset is found, or manually assigned to specific assets.

A query assignment to assets means that the query will be performed on the asset on the next iteration it is scheduled to run.

Make sure you configure the correct set of queries that correspond to the type of assets that exist in either of your network segments and your network constraints (such as bandwidth) and asset constraints (such as avoiding deep inspection of sensitive assets).

To configure asset queries:

1. Navigate to **Settings > Data Sources > Active Detection > Queries**:

Figure 249 Configuring Queries

2. Click the green plus button to add a new **Query**:

   The **New Query** dialog appears:

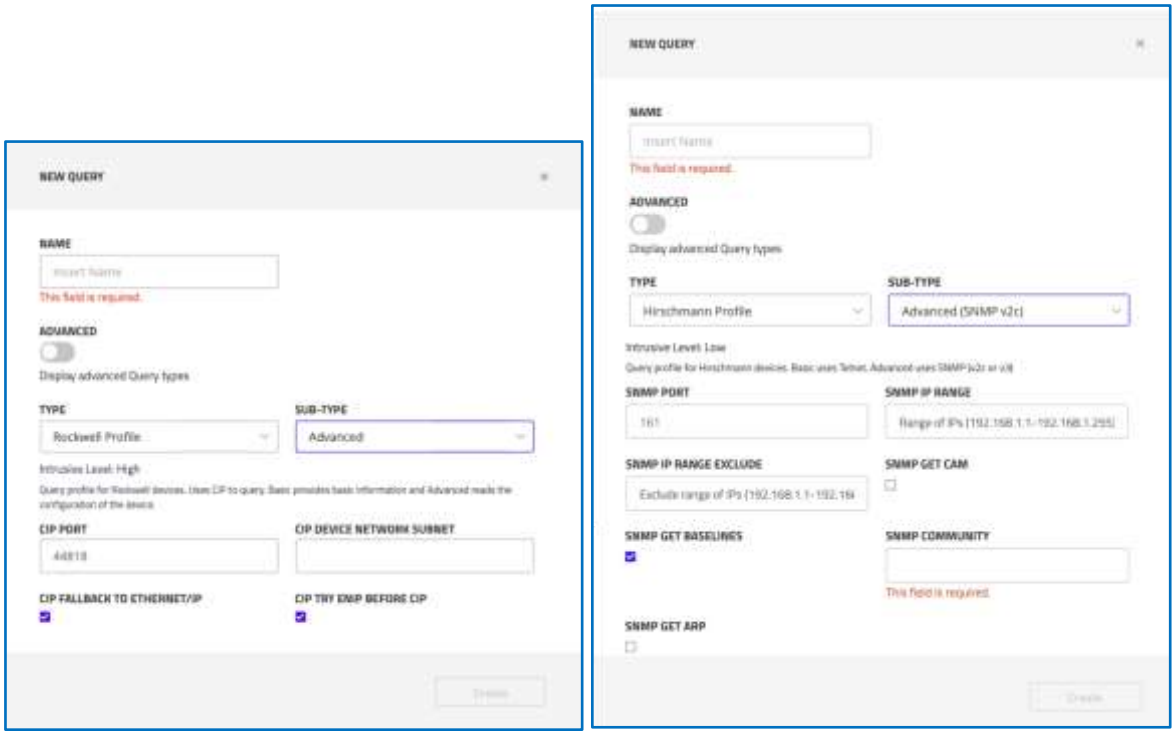


Figure 250 New Query Examples

In the **New Query** configuration dialog, set the following parameters:

a. **Name** – Provide a meaningful name for the query.
   For instance, "CIP query of Production Floor Rockwell devices"

b. **Advanced** – The basic dialog is displayed by default.
   Move this button to the right to access the Advanced dialog.

   i. **Basic** – When the **Advanced** toggle button is OFF, the form provides a simpler mode to configure the query, where the **Query Type** and **Sub-Query** dropdowns are populated with simple, predefined query profiles, that require less technical understanding from the

user. Scroll through these dropdown menus to see the available options.

ii. **Advanced** – When the **Advanced** toggle button is ON, the **Query Type** and **Sub-Type** dropdowns are populated with Advanced options that require better understanding of the various protocols

c. **Query Type** – Select the type of query. Refer to section *Summary Queries Table* in the *TIV Reference Guide* for the list of available queries. The detailed descriptions and the required parameters to provide are available in section *Detailed Queries Table* in the *TIV Reference Guide*.

d. **Sub-Type** – Depending on the Query selected, the form may display additional Sub-Types. Sub-Types need to be selected when a Query can have several sub types.

- For example, selecting an SNMP query will require selecting a Sub-Type out of SNMPv1, SNMPv2 or SNMPv3.

e. **Query Parameters** – Each query and sub-type requires a different set of parameters to be configured. When the Query and Sub-Type are selected, the form automatically updates with the appropriate query parameters fields to be filled in. Some fields are automatically filled with default values, such as port number.

3. Click **Create** to finish the query configuration.

♦ The new query is then displayed in the Active Queries table

Figure 251: Active Queries table

11.1.6.2 Reviewing Queries

Pre-existing Queries are displayed in tables located in the **Active Detection** pane within the **Settings** > **Data Sources** menu. Navigate to the Queries tab to review them.

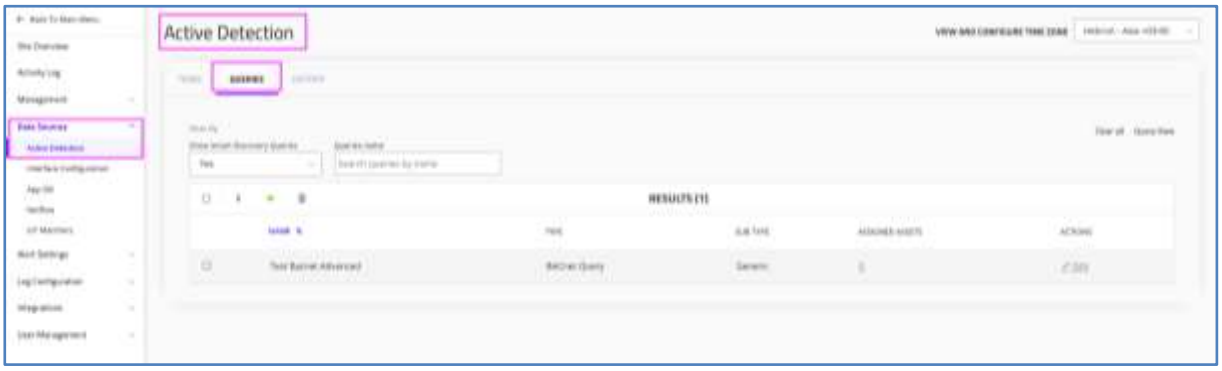


Figure 252: Queries Results

The Active Queries table shows the following columns:

- **Name** – The user-defined name of the Query
- **Type** – The type of query configured
- **Sub-Type** – Depending on the Query **Type** selected
- **Assigned Assets** – Shows the number of assets from this query (clickable). After you click on the number, you are directed to the filtered asset lists based on the number of discovered assets.
- **Actions** – Currently only **Edit** is available**.** Click to edit this active query.

11.1.6.3 Asset Inventory and Assigned Queries

When TIV discovers new assets, they are added to the system's asset inventory, available by navigating to the **Assets Page**. Furthermore, clicking on an asset on the **Assets Page** opens up the **Single Asset Page** where all the asset information and properties can be viewed, including the information retrieved by Active Queries. When a query retrieves new or updated information for an asset, the information on the **Assets Page** and in the **Single Asset Page** is updated with the new information.

Figure 253 Active Queries in Assets View

The Active Queries column shows the list of active queries assigned to the asset. Queries can be assigned to an asset in one of two ways:

- Automatically – During the Discovery Task phase, when a new asset is found, the system automatically attempts to query it using the configured auto-assign queries. For any successful query attempt, the query is automatically assigned to the asset.
- Manually – You can specifically select to assign or unassign queries to selected assets.

Assign/Unassign Queries to Assets

To assign/unassign queries to assets:

1. On the **Assets page**, select one or more assets.
2. Click the Assign/Unassign Queries button .
3. A pop-up window with a list of configured queries opens. Select one or more queries to assign to the selected asset(s) and click **Assign.**
4. To unassign queries from the selected assets, follow the same steps to select the relevant queries and click **Unassign.**

Asset Information Retrieved Actively

When an asset is queried, the system attempts to extract all available asset information such as model, firmware version, hardware revision and more. All available asset information is displayed on the Single Asset page, accessible by clicking an asset on the Assets Page.

For example:

Figure 254 Asset Information from an Active Query as displayed in the Single Asset page

- Refer to the Single Asset Page and its various components.
- See the tables in *Query, Discovery and Profile Types* in the *TIV Reference Guide* to learn about the various asset information types retrieved using the active queries.

Filtering Assets on the Assets Page

To filter the Assets Page according to actively retrieved asset information, use the **Advanced Options**, and select **Filter Name** to be **Custom Information**. Then enter the value on which you want to filter in the **Filter Value** field.

This filter shall also apply for the Custom Label field that can be added to assets as they are found during the Discovery Task process:

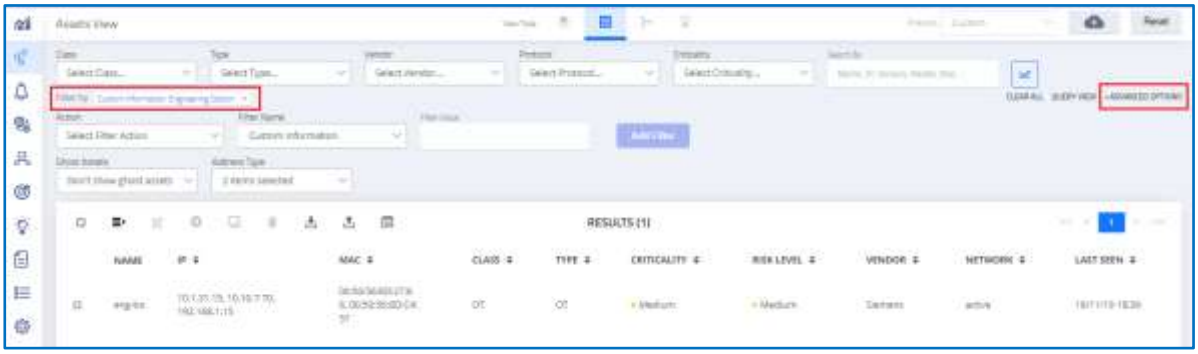


Figure 255 Advanced Filtering

11.1.7 Active History Summary

The Active History feature enables logging tasks and queries in a summary table. It does not require any configuration. Each time a task runs, it generates a new line in the table. Each line shows runtime information including: ID, start/end time, duration, end status, and status.

An Active History Side Panel is provided for further active history details and varies according to the task/queried being tracked. This detailed history of each task enables monitoring the tasks themselves, their results and facilitates further investigation when needed.

This powerful tool not only tracks active tasks in the network; it tracks disconnected assets, new ones as they are incorporated over time, and enables validating proper operation of the tasks (run times, errors, finish in time, etc.)

To access Active History:

1. Go to **Settings > Data Sources > Active Detection**.
2. Click the **History** tab.

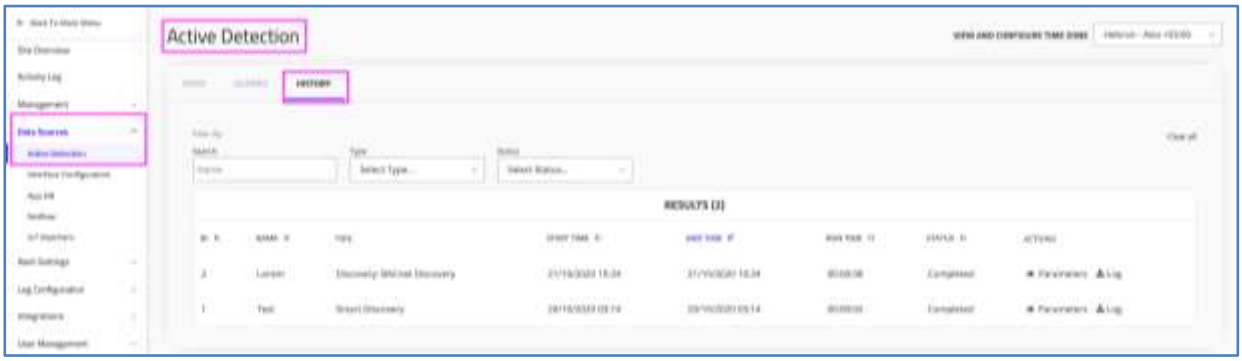


Figure 256: Active History

The Active History Page displays the following data:

- **ID** – The ID of the task that was run
- **Name** The name of the task that was run
- **Type** – The type of task used
- **Site ID** – The site on which this task was run
- **Start/end time**
- **Run time** – The duration of this task
- **Status** – Whether or not the task ran:
  - **Completed**
  - **Stopped** – Stopped automatically due to task timeframe
  - **Forced Stopped** – Stopped manually

- **Failed** – Technical issue prevented task from running

- **Last Run Results** – The outcome of the task.
- **Actions**:
  - A **parameters** button for displaying this task's parameters
  - A **log** button for downloading these results

Click the **Clear All** button when you want to restart this History table.

Summary side panel

When inspecting the Active History, clicking a row of a particular task or query, a Summary side panel with further details expands, as shown below:

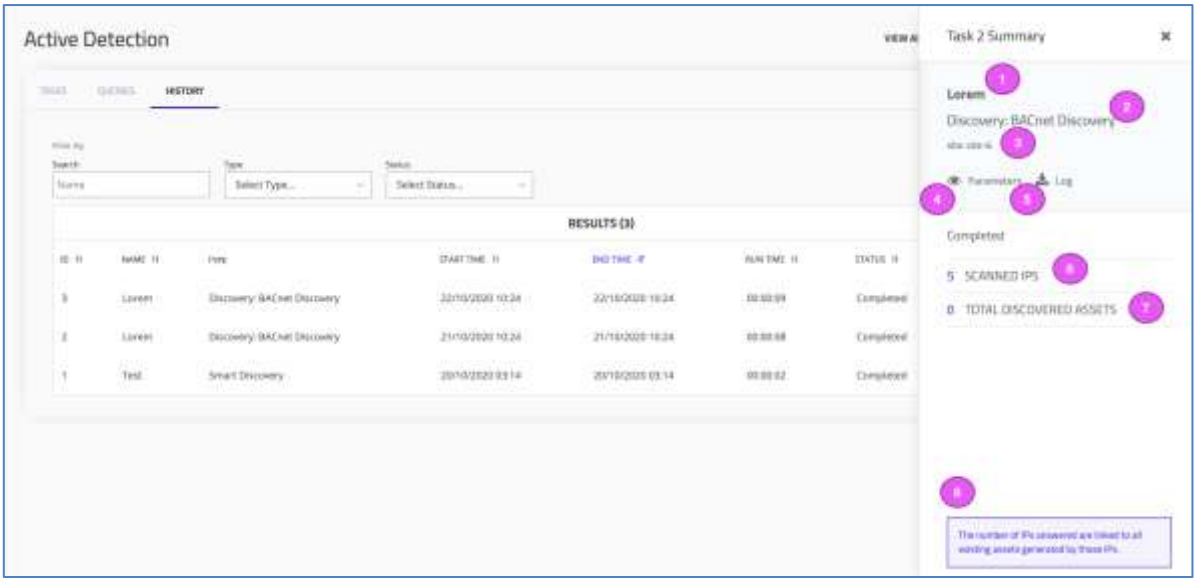


Figure 257: Summary Side Panel Examples in Active History

The summary side bar displays the following information:

1. The **Name** of the task
2. They **Type** of task used
3. The site ID
4. A **parameters** button for displaying this task's parameters
5. A **log** button for downloading these results
6. **Scanned IPs** – The number of IPs (assets) that were scanned in this manner. Clicking on this number opens the asset list popup that includes further details of these assets a link with the Asset Page displaying these filtered assets.
7. The number of IPs successfully queried

8. A summary message with further information.

When applicable, the summary info bar also includes the number of IPs whose query failed, including the reasons of failure, broken down per query.

11.2 Interface Configuration

Use the Interface Configuration screen to adjust your interface configurations as described below.

11.2.1 Default

To adjust the Default interface configuration settings:

- Navigate to **Settings** > **Data Sources** > **Interface Configuration** (see Figure 259).

Figure 258 Interface Configuration Site Tab

The interface configuration screen enables you to change the following:

1. **Site name** – The name of the site (*site1* in this example)
2. **Interface Name** – The OS name of the interface (*management* in this example)
3. **Process data** – You can enable it on order to get more information about your interface (by default "off")
4. **Device Status** – If the link is UP (connected) it is a Green dot; if it is DOWN (disconnected or unavailable) it is a Red dot.
   a. **Bit rate** (MB/s) – Describes the amount of traffic passing in this interface
   b. **Unicast Traffic** – Describes the quality of your traffic by counting unicast packets (Low, Medium, High)
   c. **OT Traffic** - Describes the amount of OT traffic on this interface (Low, Medium, High)

5. **Allocate to Network** – Displays the Network this interface is connected to. You can add a new network. Each interface can be connected to one network.
6. **Filters** – You can add filters to the traffic in the network, such as tcpdump capture filters.
7. **Dump Size** – Shows the size of the network traffic file that was recorded.
8. **Record** – Press this button when you want to record a PCAP file for the traffic on a network for investigating the PCAP file.
9. **Download** – Press this button to download the recorded PCAP file to your machine

See below for configuring **Advanced Network Settings**.

11.2.2 Advanced Network Settings

At the bottom of the **Interface Configuration** page you can configure **Advanced Network Settings**  as shown below:

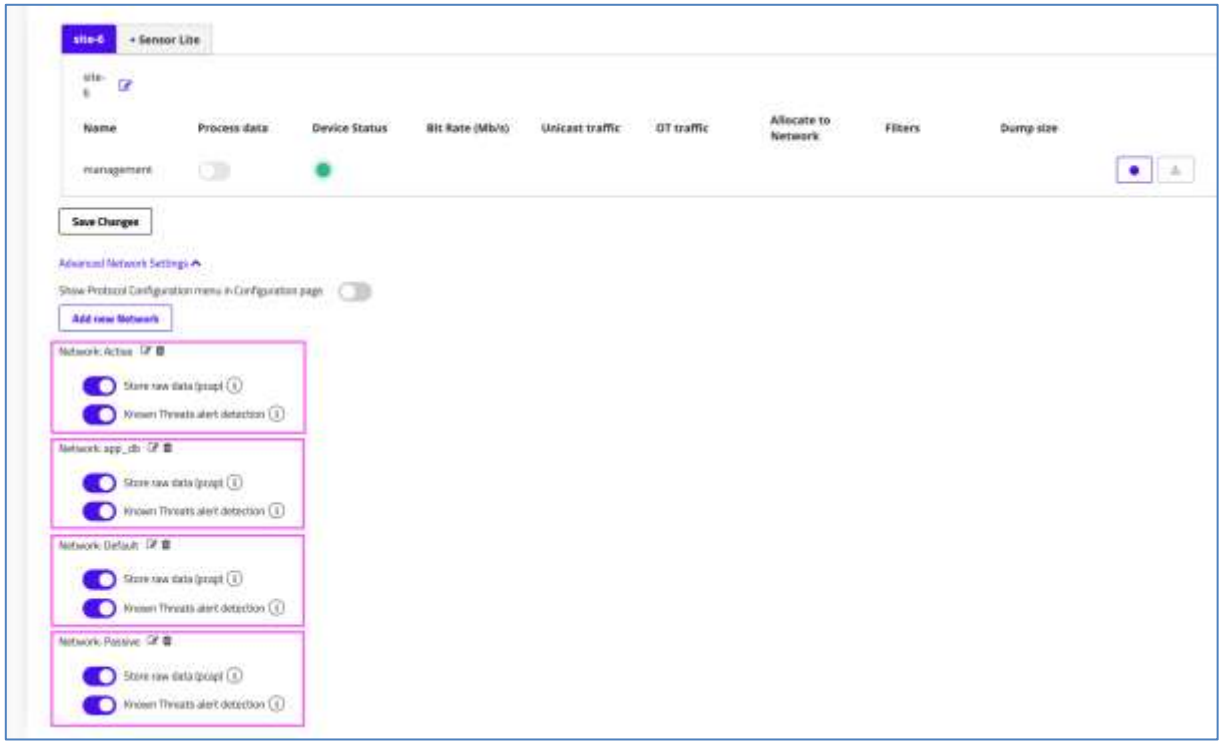


Figure 259 Advanced Network Settings

Configure your advanced network settings as follows:

- **Show Protocol Configuration Menu in Configuration Page** –Slide to the right to add a new Protocols option to the Main Menu. This page enables control of the protocols the system supports. (by default, it is OFF).

Warning: This option should only be enabled in coordination with Support, as the settings can have a critical impact on the system.

Both of the following settings can be configured per network:

- **Store raw data (PCAP)** – Slide to the right to enable downloading a PCAP file connected to the alert and store it in a specific directory on the server
- **Known Threats** alert detection – Enables TIV to use a sophisticated signatures-based database to enhance its capability for identifying known attacks.

- Select **Save Changes** to save your entries.

Note The example above shows a system running on the following networks in addition to the Default network: AppDB, Passive, Active.

11.2.3 Sensor Lite

To access Sensor Lite:

1. Navigate to Settings > Data Sources > Interface Configuration.
2. Select the **Sensor Lite** tab to adjust your Sensor Lite's interface configuration settings:

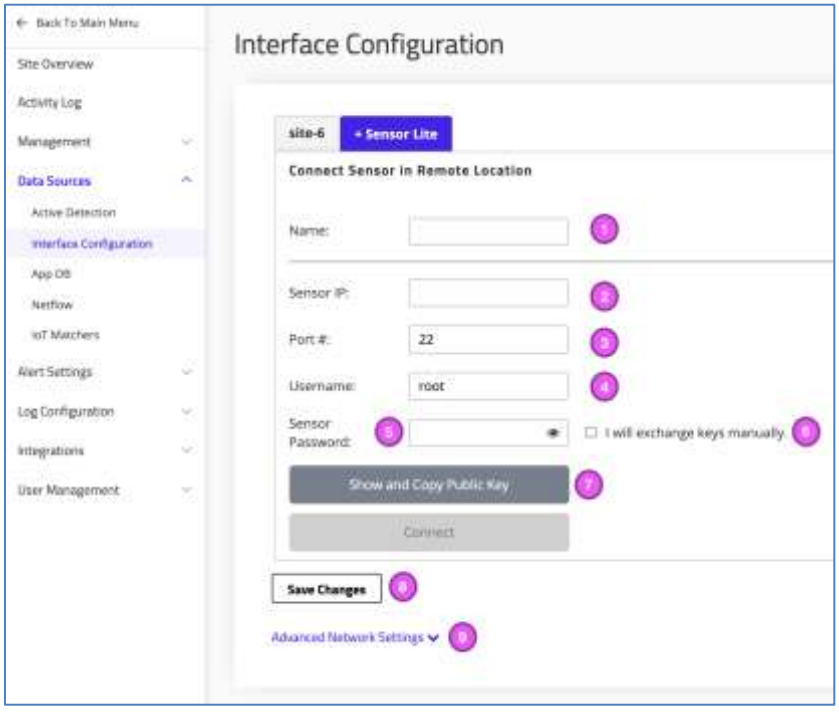


Figure 260 Interface Configuration for Sensor Lite

This screen enables you to reconfigure the following settings:

1. **Name** – The name of the Sensor Lite
2. **Sensor IP** – The IP Address for the Sensor Lite
3. **Port #** – The port number (by default, Port 22)
4. **Username** – The Username of this Sensor Lite
5. **Sensor Password** – The password of this user
6. **Sensor Password checkbox** – to select manually exchange of keys
7. **Show and Copy Public Key** – press to obtain the "Public Key". Copy it.
8. **Connect** – press to connect the Sensor Lite to your machine with the new configuration settings.
9. **Save Changes** – select to save your entries.
10. See Advanced Network Settings above.

11.2.4 Protocols

A predefined set of recommended passive protocols is built into the system. A Protocol Configuration mechanism enables Administrators to configure the passive protocols in a **Protocols** page. This configuration menu is not visible by default. These settings are controlled for each site individually.

To enable changing the passive protocols used:

1. Navigate to **Settings**  **> Data Sources > Interface Configuration**.
2. Click the **Advanced Network Settings** link:

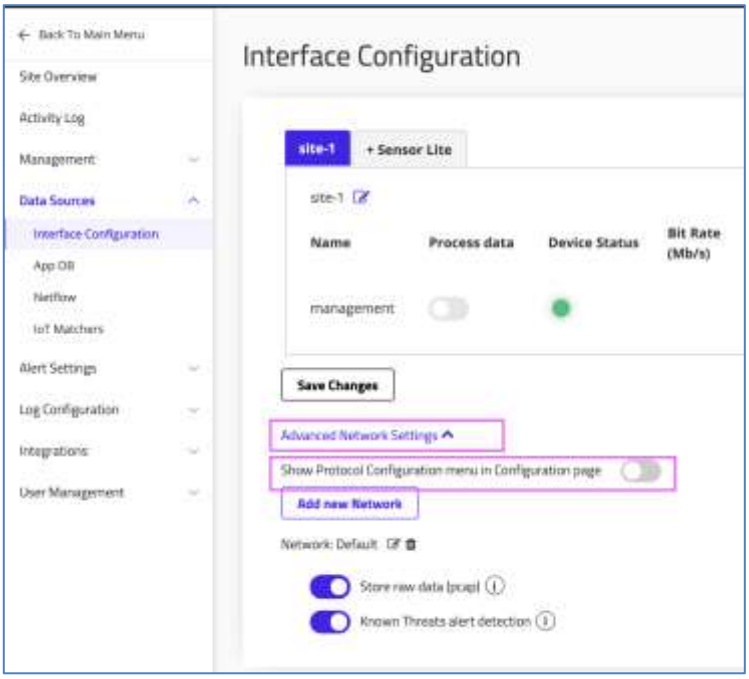


Figure 261 Enables Showing the Protocol Configuration menu

3. Slide the **Show Protocol Configuration menu in the Configuration page** button to the right.

   The list of protocols supported by the system appears.

> Warning Changing these settings could have a critical impact on the system and therefore should only be changed by an Administrator in coordination with Tripwire Support.

4. Keep the top checkbox selected and then revise the list, selecting any additional protocols:

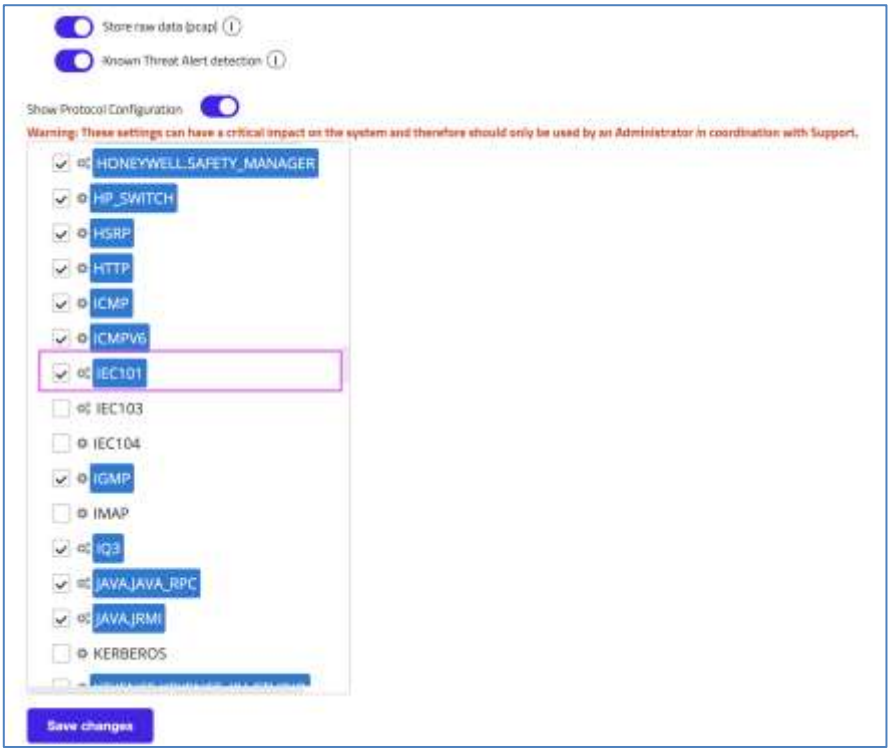


Figure 262 Selecting the IEC101 protocol from the Deployment Configuration Protocol List

5. Click Save Changes  .

   - When the changes take effect, a **Saved Successfully** message appears.

For the full list of passive protocols supported, refer to the *TIV Reference Guide*.

11.3 App DB (aka Configuration Projects)

Prerequisite: The App DB capability is set up in the Configuration wizard.

To view App DB page:

- Navigate to Settings > Data Sources > App DB:

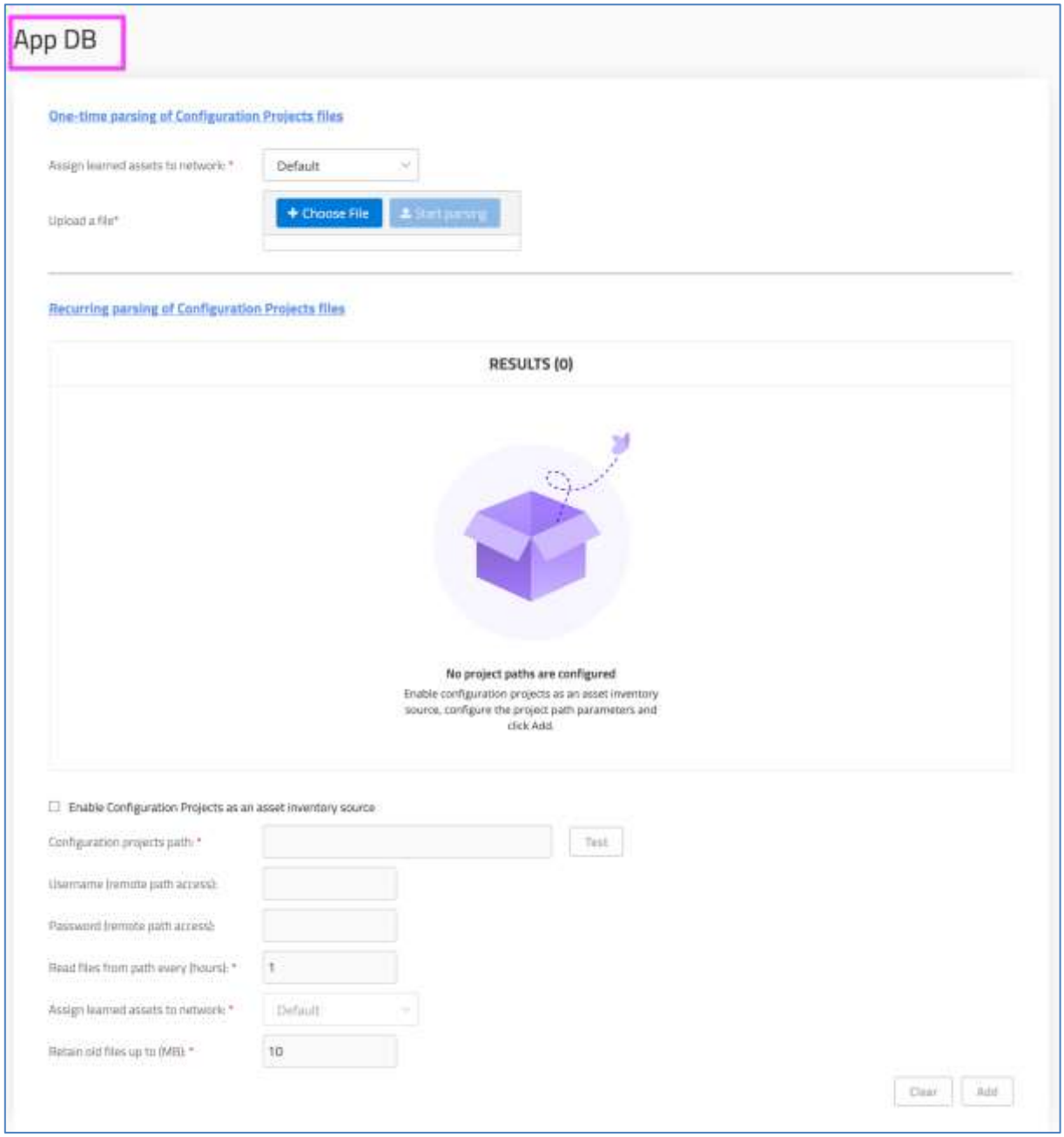


Figure 263 App DB page

The App DB page includes:

- One-time parsing of Configuration Projects files
- Recurring parsing of Configuration Projects files

Refer to the TIV Reference Guide: Configuring Application Database (App DB) Sources.

11.3.1 Enabling Protocols

A Protocol Configuration mechanism enables Administrators to configure the protocols in the Protocols page. This configuration menu is not visible by default.

See section 11.2.4 to enable configuration of the protocols.

11.3.2 Selecting Protocols and Further Configuration

Refer to the TIV Reference Guide: Configuring Application Database (App DB) Sources.

11.4 NetFlow

NetFlow is included in TIV as another source of asset data and network anomaly detection.

1. Navigate to **Settings > Data Sources > NetFlow**.

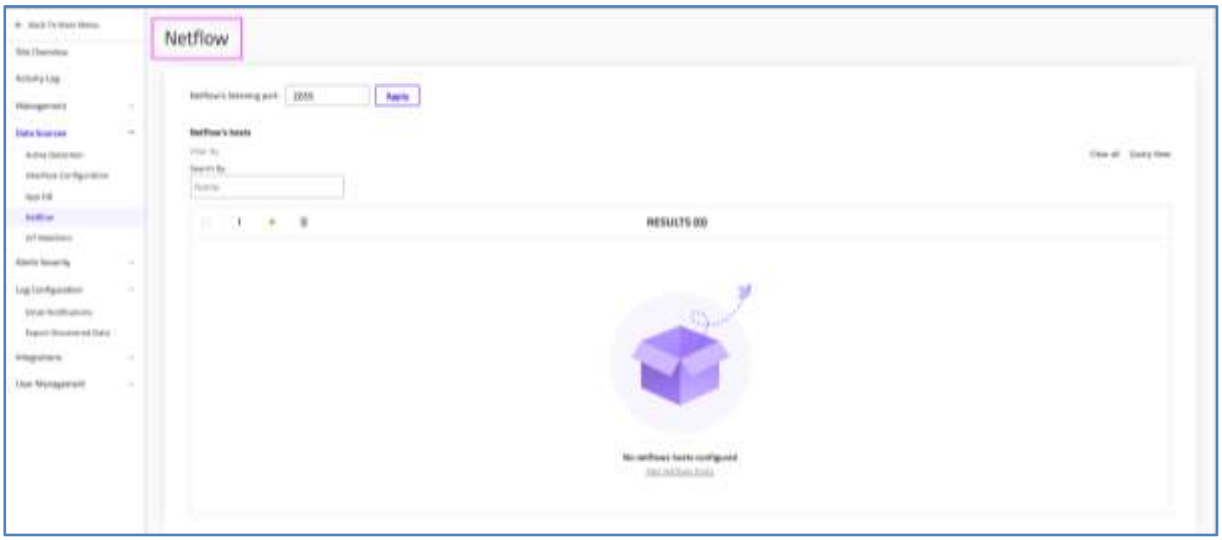


Figure 264 Navigating to NetFlow

2. Click the green plus button or **Add NetFlow Host** to add a new host:

Figure 265 Adding a NetFlow Host

- The **Create New Host** window appears:

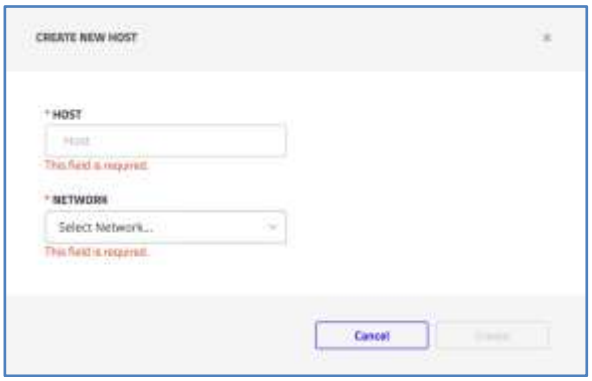


Figure 266 Adding a NetFlow Host

2. Host – Add the name of the host to add
3. Network – Select the Network for the new host
4. Click **Create**.

11.5 IoT Matchers

IoT Matchers is an optional tool that can be used to enrich your IoT Asset Inventory.

To view IoT Matchers:

- Navigate to **Settings > Data Sources > IoT Matchers**. The following screen appears.

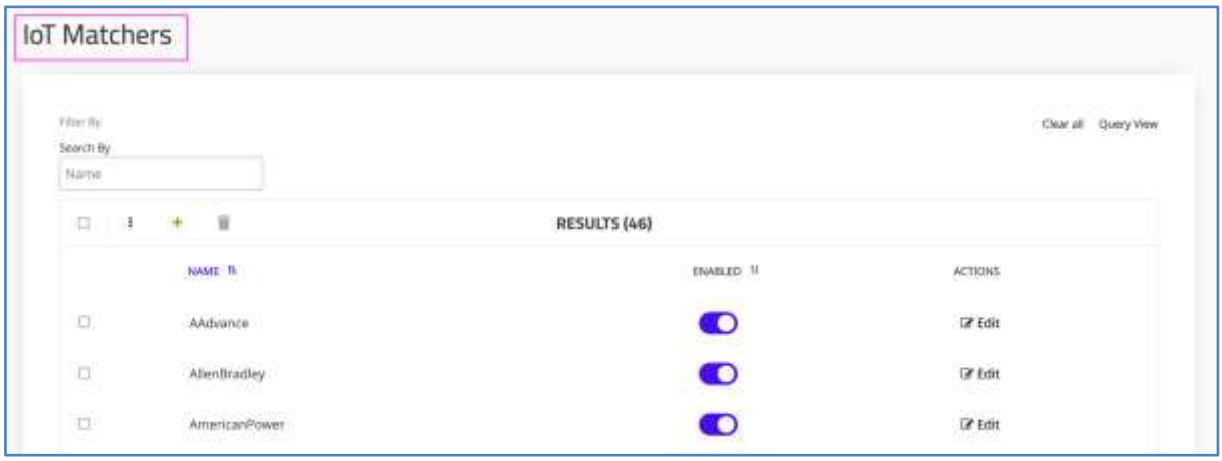


Figure 267 IoT Matchers Page

This advanced discovery tool extends TIV's visibility to IoT assets, providing micro segmentation of the network. IoT devices are dynamically supported by TIV. Users can filter for them and work with them using the full TIV suite of tools in the same manner as OT and IT assets.

11.5.1.1 IoT Matchers: General Structure

The general structure of the IoT matchers is:

- Matcher type - the protocol used (supported: SNMP, HTTP, banner, WSD)
- Verify - protocol dependent, but the idea is a field that allows the engine to identify the matcher is relevant for the current device/communication
- Information extraction regular expressions - the specific format is protocol dependent; we will usually run a regex on the response (HTTP Page, SNMP mib, Banner, etc.) to try and get the information from it - could be the standard information details (model, firmware, IP, etc.) or custom information that is specific to this matcher.

11.5.1.2 How to Write a Matcher

SNMP Matcher

1. Identify the product you are interested in
   a. Rockwell PLC (via ENBT Network card)
2. Verify the product has SNMP support
   a. Google it? "Rockwell ENBT SNMP"
   b. https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um051_-en-p.pdf
3. Determine the authentication method for the device
   a. Google "Rockwell default SNMP community string"

b. (BTW - "public" is a good guess even when we can find confirmation for that online)

4. Find a device you can work with to start learning the interesting stuff
   a. 10.1.30.1 - our lab PLC
5. Run a full SNMPWalk on the device - snmpwalk is a CLI utility that connects via SNMP to the desired IP and queries it for all supported OIDs, and prints the returned information (See a potential snmpwalk alternative for Windows in the links section)
   a. snmpwalk -On -c wheel -v 2c 10.1.30.1 1.3.6.1
      i. "snmpwalk" is the command
      ii. "-On" - tells snmpwalk to print out the full OID numbers so that we can later use them in our matcher
      iii. "-c wheel" - -c and then specify the community string you want to use
      iv. "-v 2c" - -v and then the protocol version you want to use (1/2c/3)
      v. "10.1.30.1" - the IP address of the device
      vi. "1.3.6.1" - The OID from which to start the "walk"
   b. The output is something like this:

```
(virtualenv3) ➜ ranger git:(master) ✗ snmpwalk -On -c wheel -v 2c  10.1.30.1 1.3.6.1
.1.3.6.1.2.1.1.1.0 = STRING: Rockwell Automation 1756-ENBT
.1.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.95.1.12
.1.3.6.1.2.1.1.3.0 = Timeticks: (71174074) 8 days, 5:42:20.74
.1.3.6.1.2.1.1.4.0 = STRING:
.1.3.6.1.2.1.1.5.0 = STRING:
.1.3.6.1.2.1.1.6.0 = STRING:
.1.3.6.1.2.1.1.7.0 = INTEGER: 79
.1.3.6.1.2.1.2.1.0 = INTEGER: 2
.1.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
.1.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
.1.3.6.1.2.1.2.2.1.2.1 = STRING: lo0
.1.3.6.1.2.1.2.2.1.2.2 = STRING: motfec0
.1.3.6.1.2.1.2.2.1.3.1 = INTEGER: softwareLoopback(24)
.1.3.6.1.2.1.2.2.1.3.2 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.4.1 = INTEGER: 32768
.1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500
.1.3.6.1.2.1.2.2.1.5.1 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.5.2 = Gauge32: 10000000
.1.3.6.1.2.1.2.2.1.6.1 = STRING:
.1.3.6.1.2.1.2.2.1.6.2 = STRING: 0:1d:9c:c0:4:9d
```

   c. Review the returned results and find the interesting OIDs
      i. .1.3.6.1.2.1.1.1.0 - we can see a lot of details here
      ii. .1.3.6.1.2.1.2.2.1.6.2 - looks like the device's MAC addresses
6. So, we know this is an interesting device to write a matcher to, as we saw it supports SNMP and retrieves interesting information
7. How we can fill in the "verify" field of the matcher

a. Regex on the description - generate a regex that will only match the description of the interesting device - would have to be specific to only match s7-300 PLCs but not too specific to match only our PLC

i. "Rockwell Automation 17" would make sense here

b. Using the vendor OID - the number in OID .1.3.6.1.2.1.1.2.0 - although not always reliable

i. The response was ".1.3.6.1.4.1.95.1.12" - We need to take the bold number - the one after the ".1.3.6.1.4.1" - 95

8. Create regexes on the description string to extract the relevant information

a. Model: "Rockwell Automation (?P<module>.*?)"

9. Create regexes on other interesting OIDs:

a. [False example but go with it] - hostname → .1.3.6.1.2.1.2.2.1.2.2

10. Determine your hardcoded information values

a. Type - PLC

b. Vendor - Rockwell

11. So, we have all the information - now write the matcher, based on the examples listed below

```
{
 "snmp": {
  "verify": {
   "oid": 95,
   "description": "Rockwell Automation 17"
  },
  "description_regexes": {
   "regexes": [
     "Rockwell Automation (?P<module>.*?),",
   ]
  },
  "info_oids": {
   "hostname": ".1.3.6.1.2.1.2.2.1.2.2",
   "vendor": {"default" : "Rockwell" },
   "type": {"default": "ePLC" }
  }
 }
}
```

12. Run the SNMP query on the device and review the information.

11.5.1.3 IoT Matchers: Discovery and Classification

IoT assets are discovered using Matchers, which are active HTTP and Telnet queries made to the assets for obtaining important device information such as vendor, model, type, OS version, role and more. A large number of IoT devices

are supported out-of-the-box, while additional device types can be readily added by the customer per their network and their needs, in an easy to use interface.

Tripwire releases update packages including IoT device matchers to further extend the library of known IoT devices. IoT Discovery can use both Active and Passive Detection capabilities. The same signatures can be used for both active and passive methods.

11.5.1.4 IoT Matchers: Workflow

To create your own IoT matchers to discover IoT devices:

1. Navigate to **Settings > Data Sources > IoT Matchers**.

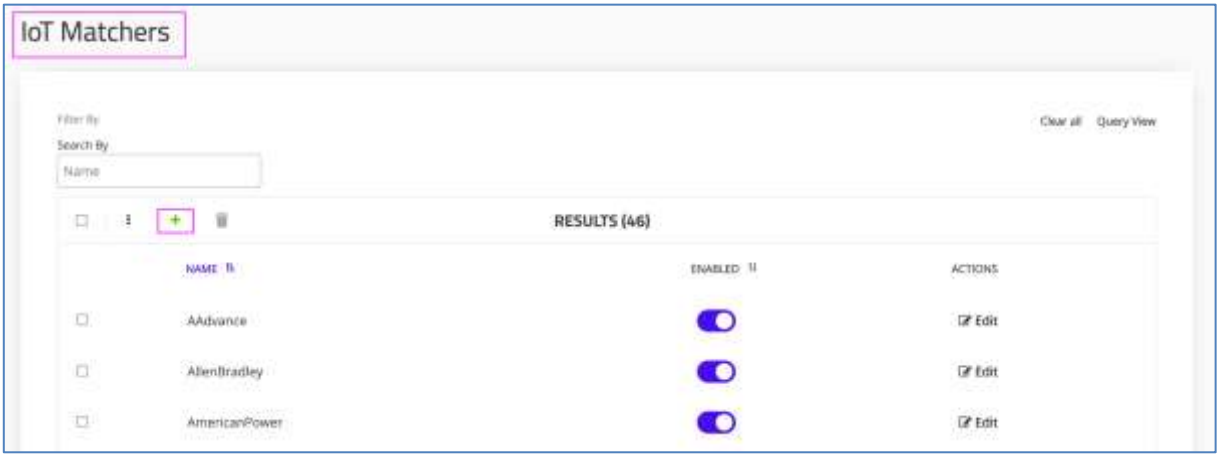


Figure 268 Adding a new IoT Matcher

2. In the toolbar, click **Add**  to open the **Create New Matcher** popup box:

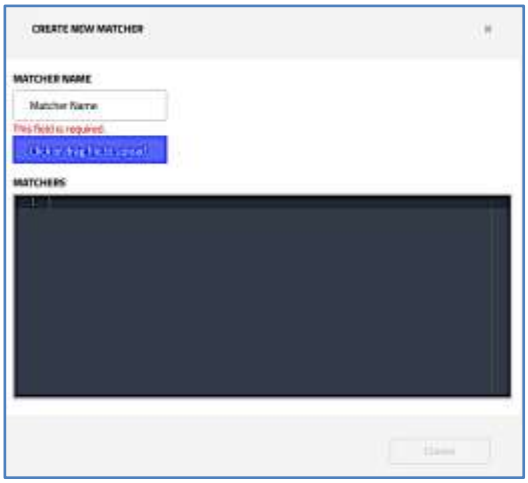


Figure 269 Adding a new IoT Matcher

3. Upload a Matcher file, which is a text file in a JSON format, by either selecting a file on your computer or by dragging the file directly into this popup box.
4. Edit the IoT matcher file.
5. Click **Create**.

> **Tip:** To obtain an example of the JSON format, open one of the matchers in the list.

For more information for working with IoT Matchers, refer to the **TIV Reference Guide: IoT Asset Management and Monitoring**.

11.6 Play PCAPs

Use the **Play PCAPs** feature to upload PCAP files for the system to dissect; the PCAPs are from actual traffic and enable simulating activity without connecting to live data. This is also useful when producing a Security Posture report.

> Note This feature is available only when you log directly into a TIV site.

To play PCAPs:

1. Navigate to **Settings > Data Sources > Play PCAPs**.

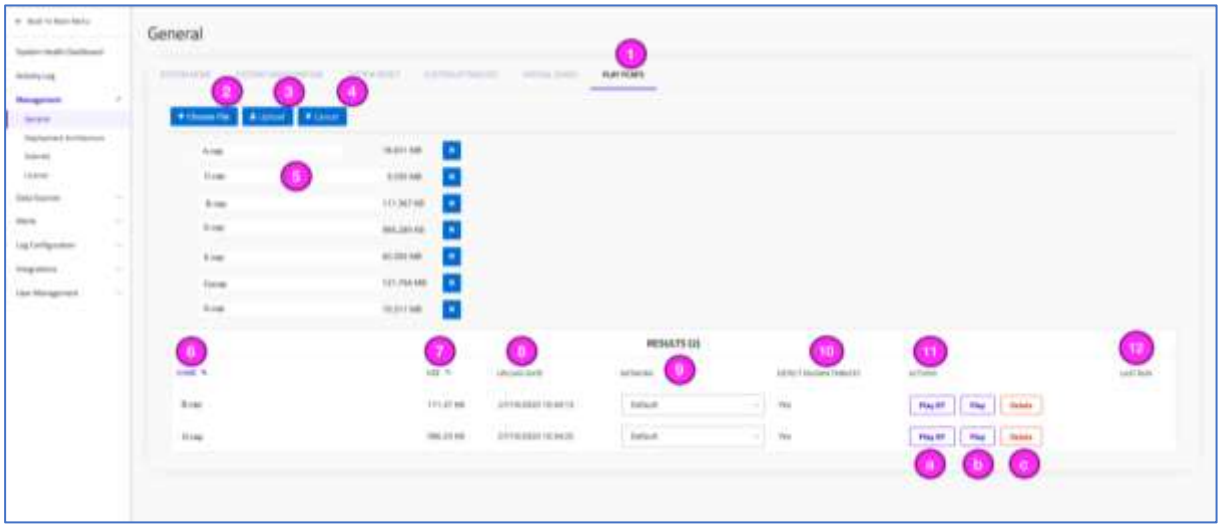


Figure 270 Play PCAPs tab

2. **Choose File** – Navigate to the file location.
   - Browse to select a single or multiple PCAP files to use.
3. Press **Upload**.
4. Click **Cancel** if needed.

5. The PCAP files start uploading and appear in the Results table below.

The following information for each uploaded PCAP file is displayed:

6. **Name** – The filename of the uploaded PCAP file
7. **Size** – The size of the PCAP file. This parameter enables uploading large PCAP files
8. **Upload Date** – The timestamp for when the PCAP file was uploaded.
9. **Network** – The name of network where this PCAP is used
10. **Detect Known Threats** –Whether to detect for known threats from the Known Threats database (default is YES).
11. Choose one of the Play PCAP **Actions**:
    a. **Play RT (Real Time)** – Click this button to play the PCAPs in real time. This option is recommended since it yields the full results.
    b. **Play** – This button plays the PCAPs but not in real time. This playback will not use algorithms that take the timing of the PCAPs into consideration. Use this option for demos or other cases where it is not critical to obtain the full results.
    c. **Delete** – This button deletes the PCAP files.
    d. **Stop** *(when a PCAP is currently running)* – Use this button when you want to stop a PCAP
12. The system tracks detailed behavior, providing activities with PCAP usage and progress, including the **Last Run** time of each PCAP file.

Figure 271 PCAP - Last Run time

13. Follow the **Activities** for the detailed log:

Figure 272 Activities log: PCAP actions

> Note: You can upload large PCAP files (up to 2G).

12 Configuring Alert Settings [Only Admins]

To configure alert settings:

- Navigate to Settings > Alerts.

The following options are available:

- Alert Severity
- Definition Updates
- Cloud Updates

12.1 Alert Severity

To set alert severity:

1. Navigate to **Settings** > **Alerts** > **Alert Severity**.
   - The **Alert Severity** page appears as follows:

Figure 273 Alert Severity Page

   - The sensitivity value is configurable: Slide the white segment of the bar to the left to decrease the sensitivity value (and increase the volume of alerts); slide it to the right to increase the sensitivity value (and decrease the volume of alerts).
2. Click **Save** Save.

12.2 Definition Updates

This section applies to configuring the system to manually upload TIV's Threat Detection bundle. This bundle includes CVEs, Insights, as well as Yara and Network Signatures and is issued periodically by Tripwire.

Threat Detection updates can be acquired automatically from the Cloud as detailed in the **TIV Reference Guide: Auto Pushing of Threat Intelligence Updates**.

When updating manually, the all sites are updated with the bundle, provided the supplied version is newer than the site's current version.

To access Threat Definitions Update:

- Navigate to Settings  > Alerts > Definition Updates.

To keep the system up to date with the latest threat data, upload the package received from Tripwire using the **Threat Definitions Updates** as shown below.

The benefit of updating with regular packages from Tripwire is that TIV is always up to date with the latest threats without requiring a full upgrade of the entire TIV software.

To update threat definitions:

1. Press Choose File  :
2. Browse your machine to select the Tripwire update bundle:
   - The filename appears with its size.
3. Select **Upload file**  to perform the upload or Click **X**  to cancel the process:

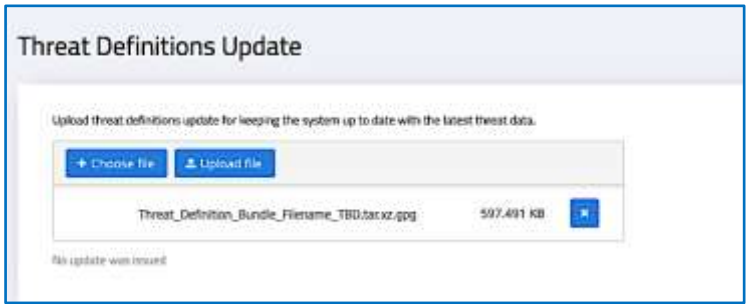


Figure 274 Uploading a Threat Definition update file

13 Log Configurations [Only Admins]

This menu includes two methods for exporting data: Email notifications and Exporting Discovered Data.

13.1 Configuring Email Notifications

TIV allows configuring the email notifications as needed.

13.1.1 Configuring the SMTP Server - Procedure

Prerequisite: For enabling email notifications, first set up an SMTP server account.

To set up an SMTP server account:

1. Select **Settings > Log Configuration > Email Notifications**.

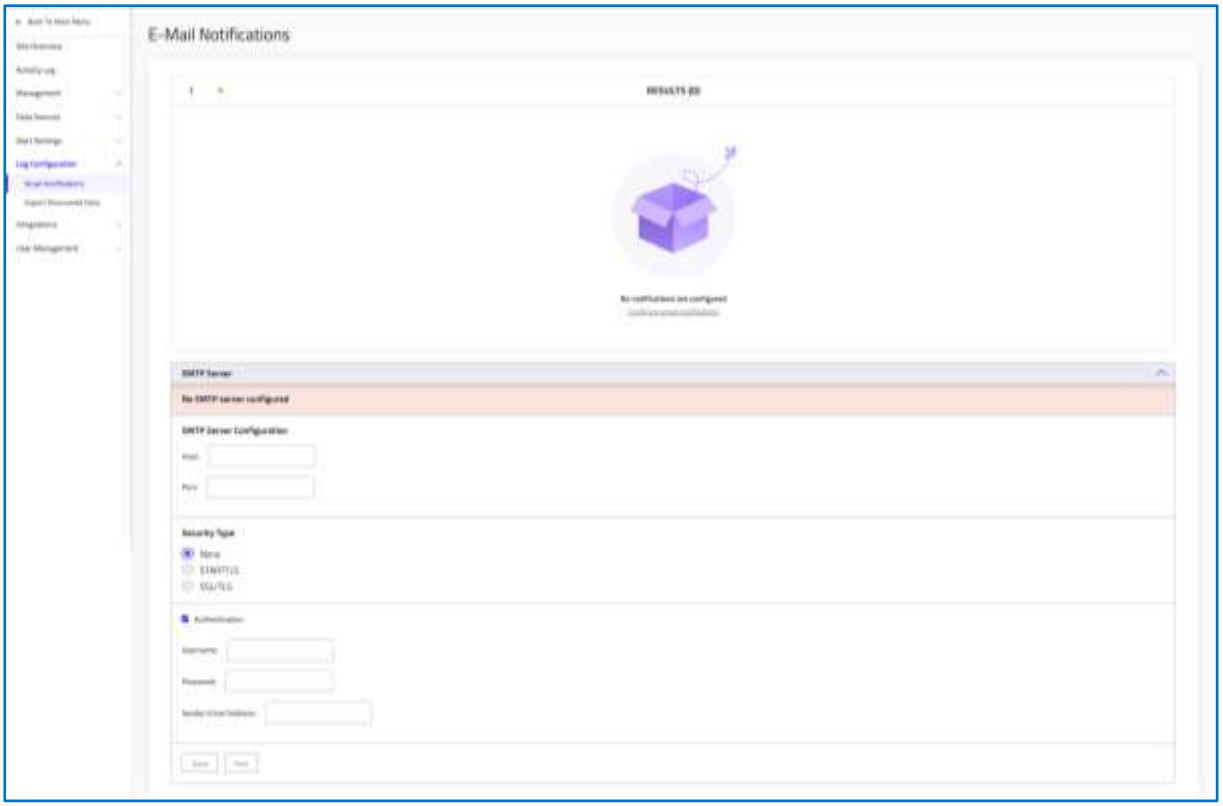


Figure 275 Email Notifications Dialog

2. Specify the SMTP hostname and port under **SMTP Server Configuration**.
3. Select the relevant security option under **Security Type**:
   - None / STARTLS / SSL/TLS.

4. Select **Authentication**, and then specify the username and password, if the mail server requires user authentication.
5. Specify the email address from which the email is to be sent.
6. Click **Save**.

13.1.1.1 Creating a New Email Notification Rule

Users can select from a range of options for granularity in email alerts. They can decide if they want email alerts to come for multiple sites or from a specific site.

To configure a rule that triggers an email notification:

1. Click the configure email notifications button:

Figure 276 Creating a New Email Notification Rule

- The **New Notification Rule** popup opens as follows:

Figure 277 E-Mail Notification Rule Dialog

2. **Rule Name** – In the New Notification Rule window, specify the name of the new rule in the Rule Name field.
3. **From Sites** – In the From Sites dropdown, select one or more of the available sites.

4. **Minimum Severity** – Under Minimum Severity, select the minimal severity level that will trigger an email notification for this rule:
    - Low (this is the default)
    - Medium
    - High
    - Critical
5. **Alert Types** or **Alert Categories** – when one is selected, the other is disabled:
    a. **Alert Type** – Select the relevant option/s of available Alert Types from the dropdown list below. (Note that this is only applicable when you are not using the Alert Category):
    b. **Alert Category** – Choose which alerts to notify for. (Note that this can only be selected if you are not using the Alert Type). The default is the entire list:
        - **Integrity** – Process Integrity alert.
        - **Security** – Security Event alert.
6. **Assign Emails** – under Assign Emails, search for the applicable group, users, or add a new email. Either specify an email address or search for an existing group or user to be notified by email when this rule applies.
7. **Email Data Level** section – select the Detailed checkbox for detailed email notifications (i.e., a description of the alert and the assets involved).
    - If this checkbox is clear, summary notifications are sent (and only include the alert time and the alert ID).
8. Click **Add**  to activate your new rule.

> Note The email is sent from the machine on which the configuration was performed.

13.1.1.2 Editing a Notification

1. Click the **Edit** icon of the relevant rule.
2. Edit the rule as per the parameters above, and then click **Update**.

13.1.1.3 Deleting a Notification

1. Click the **Edit** icon of the relevant rule.
2. Click **Delete**.

13.2 Configuring Export Discovered Data

Exporting Discovered Data functionality is covered in the TIV Reference Guide: Exporting Discovered Data.

To access Export Discovered Data:

Navigate to **Settings > Log Settings > Export Discovered Data**.

Figure 278 Exporting Discovered Data

14 Configuring SRA Integration [Only Admins]

SRA integrated with TIV enables context for alerts that have been detected on a remote connection and any related remote sessions that have occurred.

Alerts from the remote sessions are displayed in TIV with the details of the remote session, enabling:

- observing ongoing sessions (all users)
- disconnecting any live sessions that are suspicious (Admins)
- raising of alerts on remote sessions that have already completed

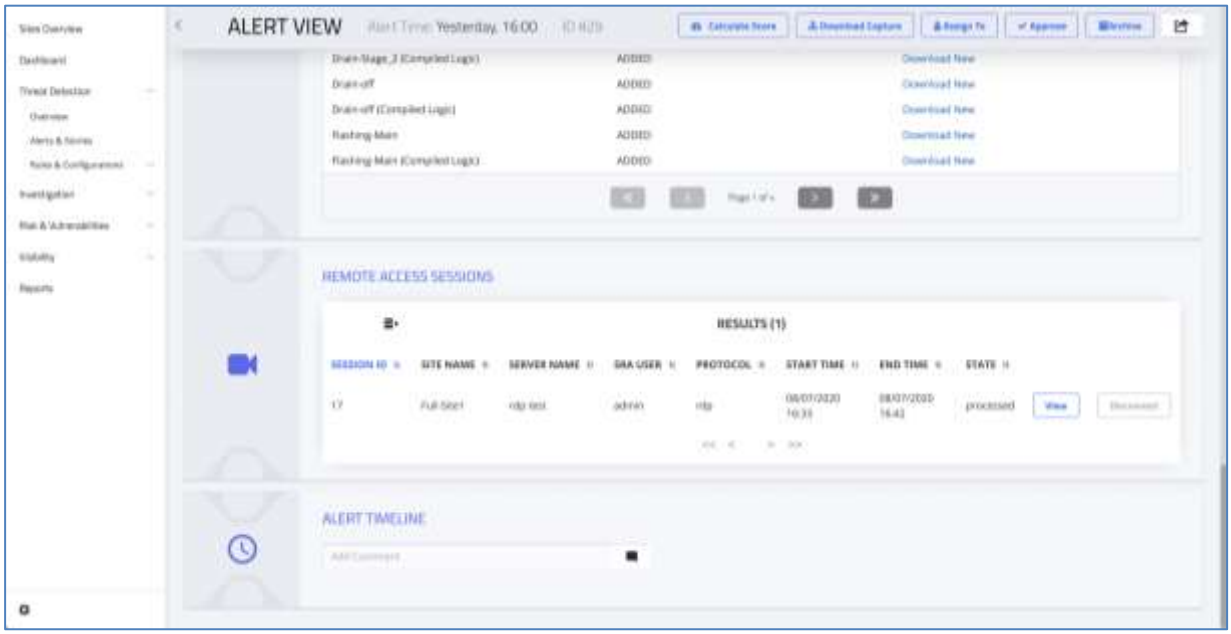


Figure 279: Alert View > Remote Access Sessions

14.1 Configuring TIV Integration with SRA

1. Navigate to **Settings > Integrations > Secure Remote Access** tab to establish communication from TIV to SRA.

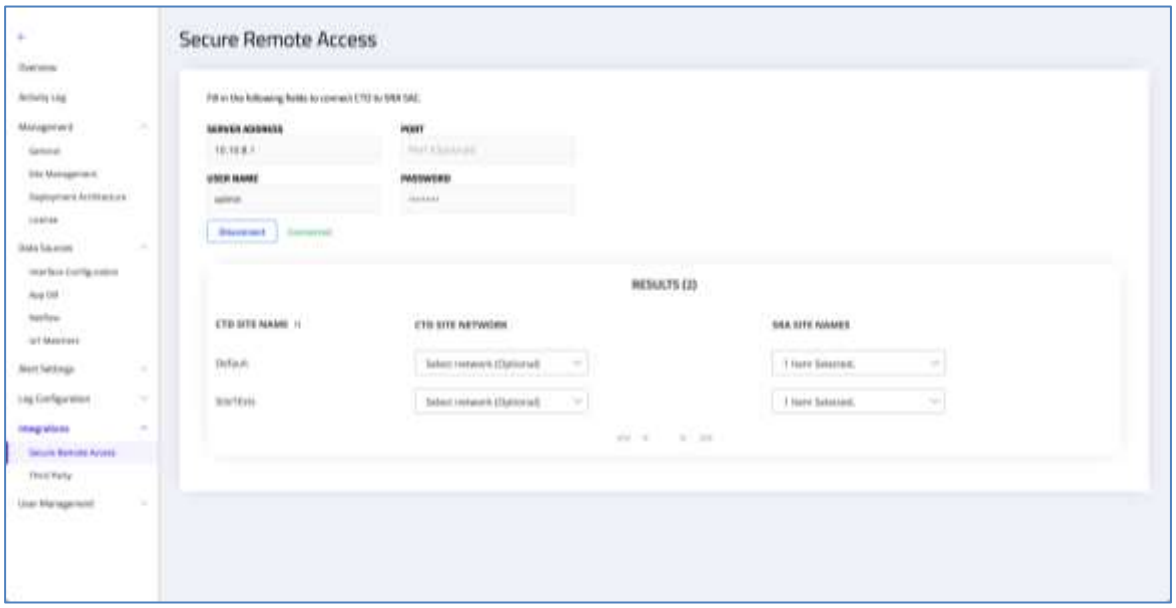


Figure 280: Settings > Integration > Secure Remote Access tab

2. Determine which Secure Remote Access (SRA) server is connected to each TIV Server.
3. Fill in the SRA configuration parameters for each relevant network:
   a. **Server Address –** The SRA server address
   b. **Port –** The SRA client port (usually 443)
   c. **Username –** The SRA username (as used to login to the web)
   d. **Password –** The SRA password (as used to login to the web)

> Note: The connection from TIV to SRA is only with the local SRA user.

4. Click **Connect**
5. Once the SRA integration is initiated,
   a. A green **Connected** message is displayed
   b. The **Results** table is populated with the details of each SRA – TIV connection
6. On the table, choose the SRA site that is related to the TIV site. The SRA session on that site will be raised on the chosen TIV site.

After finishing the configuration, TIV will raise an alert whenever a potentially hostile activity is performed (e.g. a configuration upload) from the remote machine. TIV will also associate the remote session and its details to the alert.

14.2 Viewing Remote Sessions & Disconnecting Remote Users

The TIV, SRA site and network connectivity statuses are displayed in the Alert view as shown below:

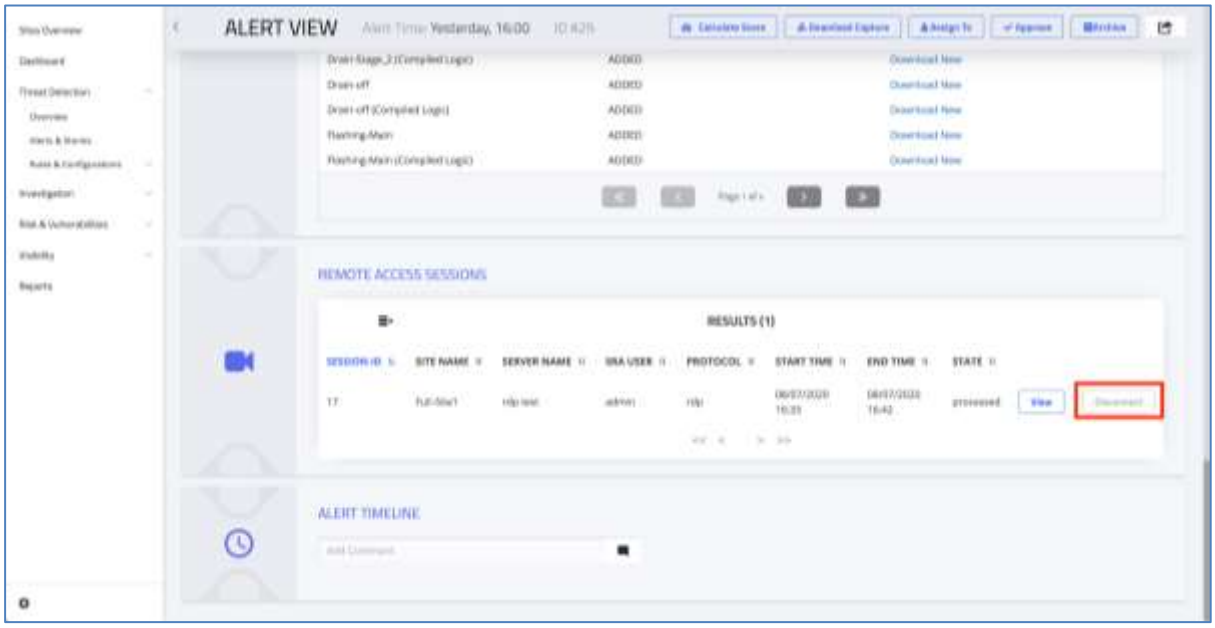


Figure 281: Alert View > Remote Access Sessions

- **View** – Enables users to view all aspects of a remote session: session details, video recordings, live viewing sessions (aka eye-over-the-shoulder).
- **Disconnect** – Admins can immediately click **Disconnect** to terminate any remote sessions when a suspicious activity or problem arises.

15 Configuring Third Party Integrations [Only Admins]

TIV can be configured to integrate with external systems, enterprise tools, and Partner solutions:

- Aruba ClearPass
- Palo Alto FW
- Cisco ISE
- Cisco FirePOWER
- FortiGate
- Check Point IoT
- ServiceNow
- CrowdStrike

To configure integrations:

- Navigate to **Settings > Integrations > Third Party**.

> Note These are one-way integrations that enable TIV to connect and send data to other systems and services.

Integration documentation is provided within the *TIV Reference Guide*.

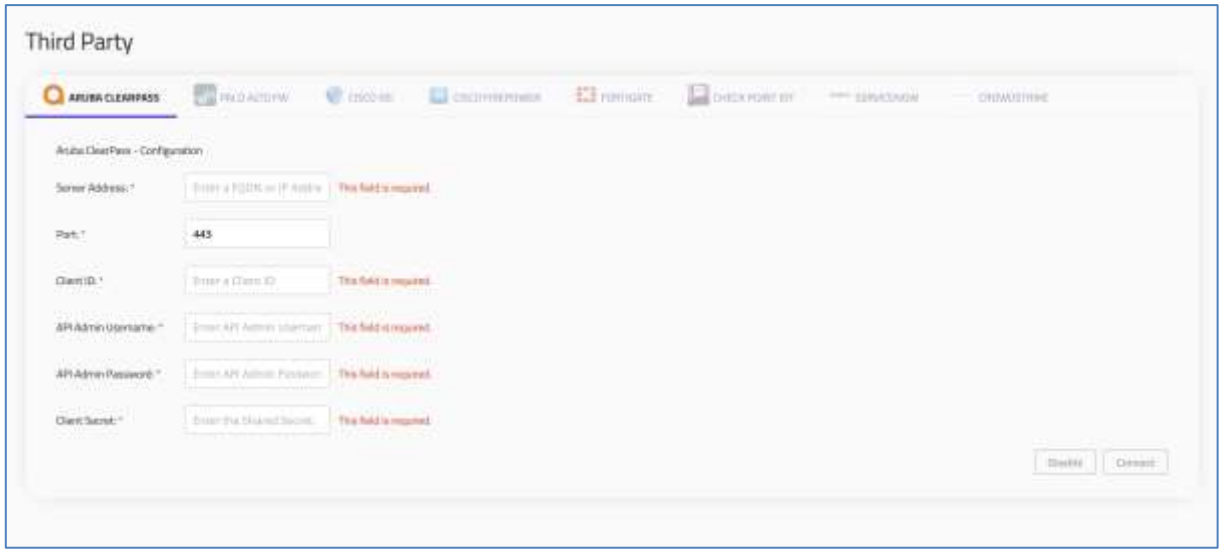


Figure 282 Third Party Integrations Menu

16 Configuring Syslog Integration

Use Syslog to export alert, baseline, event, or health monitoring data. The Syslog server sends information smoothly to third party vendors. Syslog enables choosing a SIEM vendor, whereby the related fields are auto-filled according to the vendor configuration. Syslog also sends the history of alert information.

To configure Syslog:

- Select **Settings > Integrations > SIEM Syslog**.

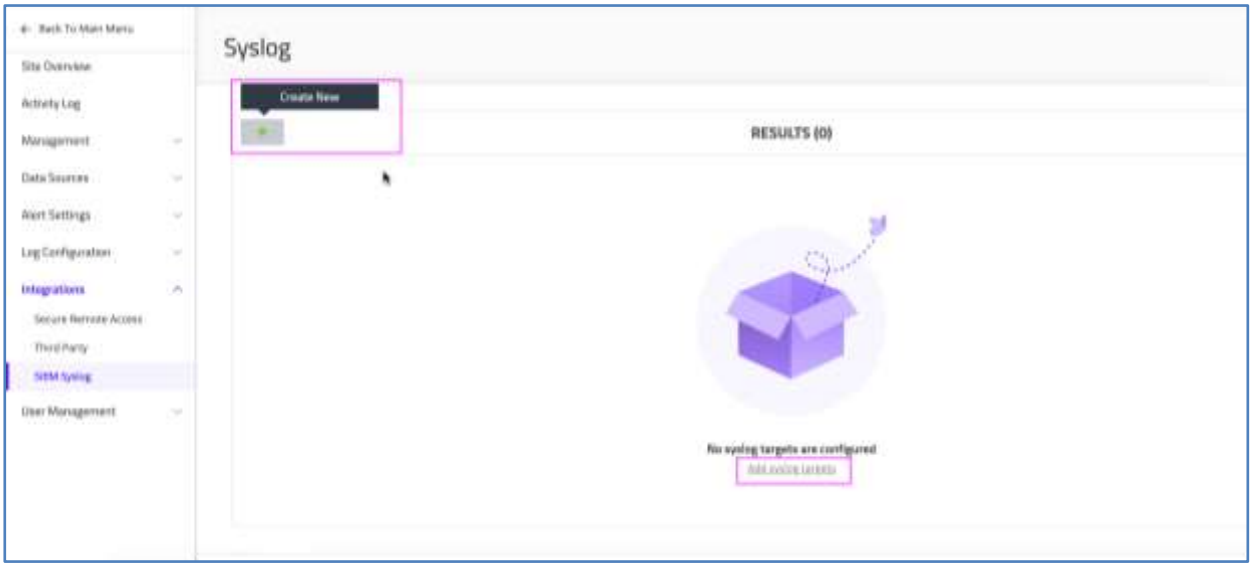


Figure 283 Configuring Syslog Messages

16.1 Add New Syslog Dialog

Click the green plus button + or click on the **Add syslog targets** button to open the **Add New Syslog** option:

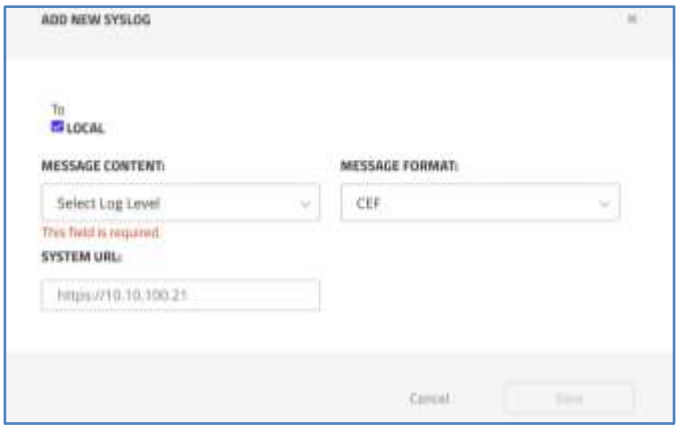


Figure 284 Configuring Syslog Messages

Use this dialog for configuring information such as:

- the server details
- the type of data (i.e., events, alerts, health monitoring)
- the format for the syslog messages
- the log protocol to be used (e.g. UDP, TCP or TLS)

You can also configure your system to:

- Send a message to syslog when a baseline appears.
- Send a syslog message when a Sniffer is down or is experiencing another problem.

An alert may consist of one or multiple events, depending on the type of alert. Every new alert (or the resolution of an alert) and the events associated with it will be sent through the configured syslog to an external SIEM to provide a unified view of the organization's security monitoring.

16.2 Common Elements of the Add New Syslog Dialog

The syslog/email is sent from the machine on which the configuration was performed.

- If the user is connected to the EMC and defines a new syslog/email notification, the message will be sent from the EMC (and not from the site/s).
- If the user is connected to a TIV Server and configures the syslog from within that site, the syslog message will be sent from that site (however there will not be an option from that site to select the other sites).
- **To** – Whether the target for the Syslog message is either the Local machine (which is the default, i.e. the **Local** checkbox is checked), or another server.

Syslog Target is Another Server

If the target is another server, the following destination information is required:

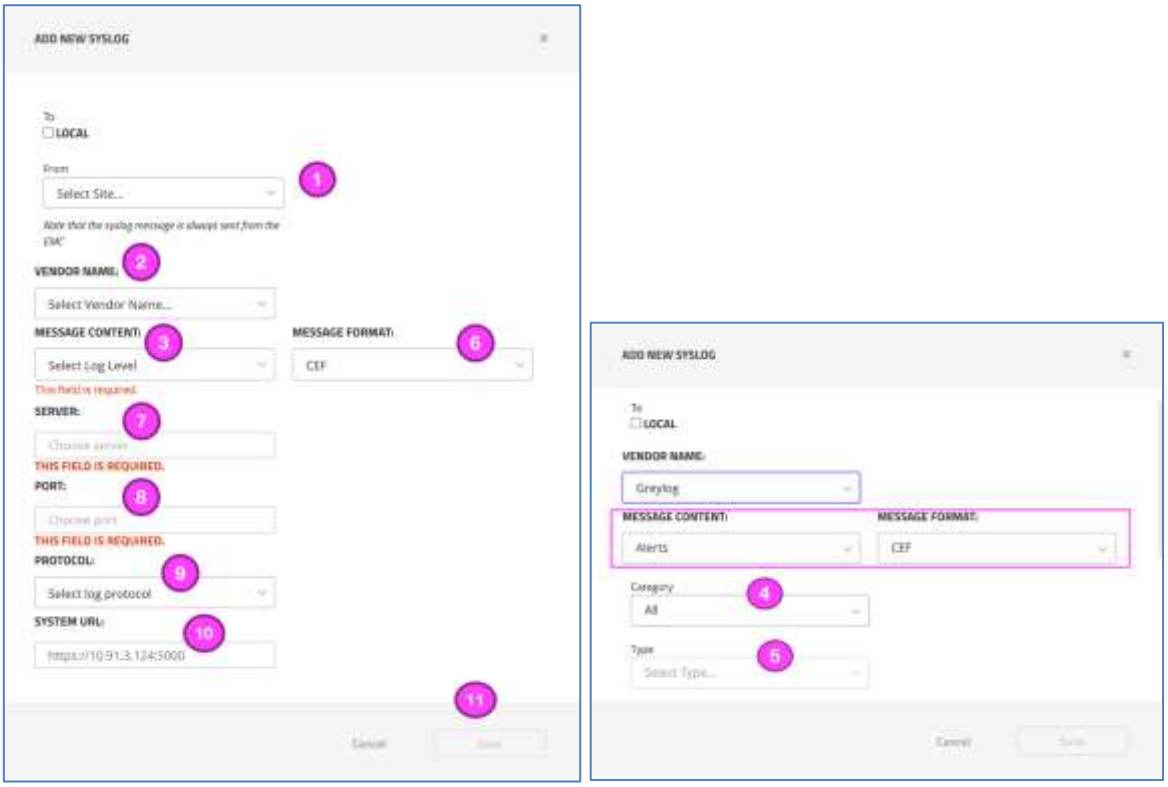


Figure 285 Syslog for a non-local machine (on the left) with an Alert example (on the right)

1. **From** (Site) – Select one or multiple sites (i.e. TIV Servers) from the dropdown, or select the EMC:

   - **EMC** – Select the EMC itself by checking the **Monitor EMC** checkbox (only for Health Monitoring) as shown below:

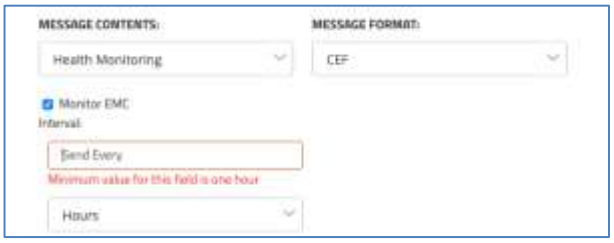


Figure 286 Selecting EMC & Log Level

2. **Vendor Name** – From this drop down, choose the desired SIEM vendor or **Other**:

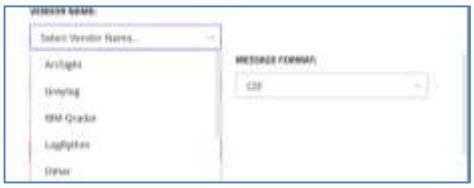


Figure 287 Vendor Name Selection

3. **Message Content** – When selecting which level to log, the enables choosing Alerts, Baselines, Events, or Health Monitoring. Default is Alerts.
4. **Category** – Select Integrity or Security or both (ALL). Default is ALL.
5. **Type** – This dropdown enables you to select one, several or all Alert Type/s
6. **Message Format** – Select a format from the Syslog message dropdown (CEF or RFC5424)
7. **Server** –The target server that will receive the syslog message. This field is mandatory.
8. **Port** – The port over which the syslog message will pass. This field is mandatory. Default is 514.
9. **Protocol** – Select the log protocol type from the dropdown list (TCP, TLS, or UDP). Default is UDP.

> Note When TLS is chosen, the Syslog message will be sent as an encrypted TCP message with RFC5424 or CEF format, with an option to add server authentication by uploading a server certificate.

10. **System URL** – Automatically shows the source URL; this field is not editable.
11. **Save** – Choose to commit your entries or **Cancel** to exit the **Add New Syslog** dialog.
    - The system assigns a Syslog ID to the new message and displays the new information as a new row in the full Syslog table.
      Select the relevant row to **Edit**, **Delete,** or **Send a Test Message**:

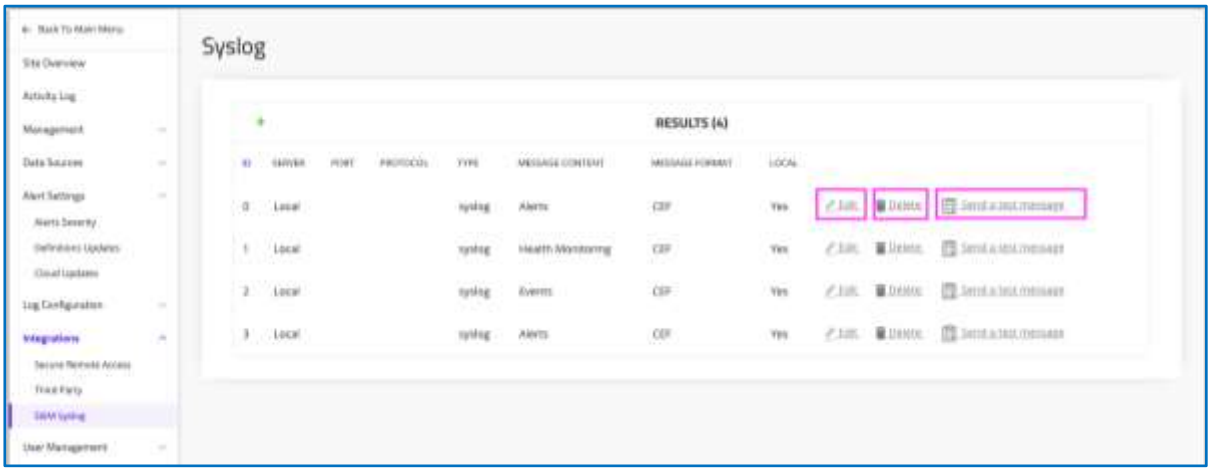


Figure 288 Syslog added as new row in Syslog Table

To test a Syslog message, see details in section 16.5.

16.3 Message Contents

The following Message Content options are available for logging Syslog messages (see Figure 284 Configuring Syslog Messages).

The parameters are detailed in section 16.4.

16.3.1 Alerts

When selecting **Alerts** to log, the following dialog is displayed (see Figure 285).

16.3.2 Baselines

When selecting the **Baselines** to log, the following dialog is displayed:

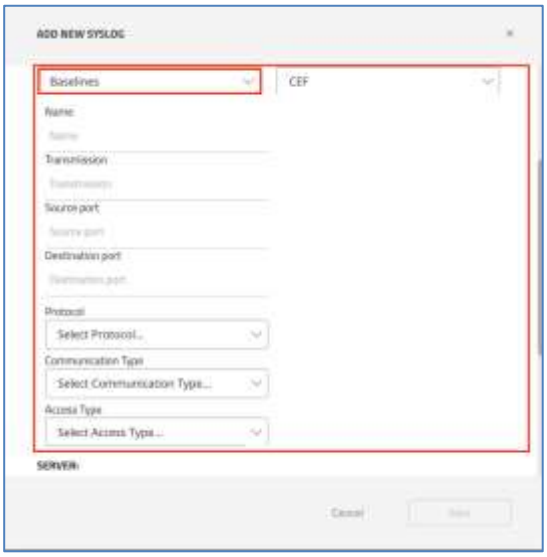


Figure 289 Syslog - Adding a New Baseline

16.3.3 Events

When selecting **Events** to log, the following dialog is displayed:

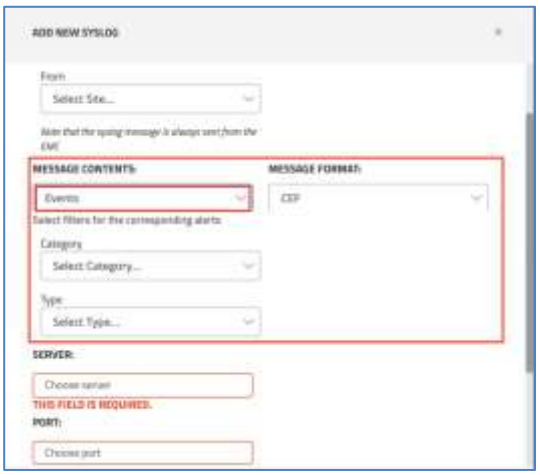


Figure 290 Syslog - Adding a New Event

16.3.4 Health Monitoring

When selecting Health Monitoring to log, the following dialog is displayed:

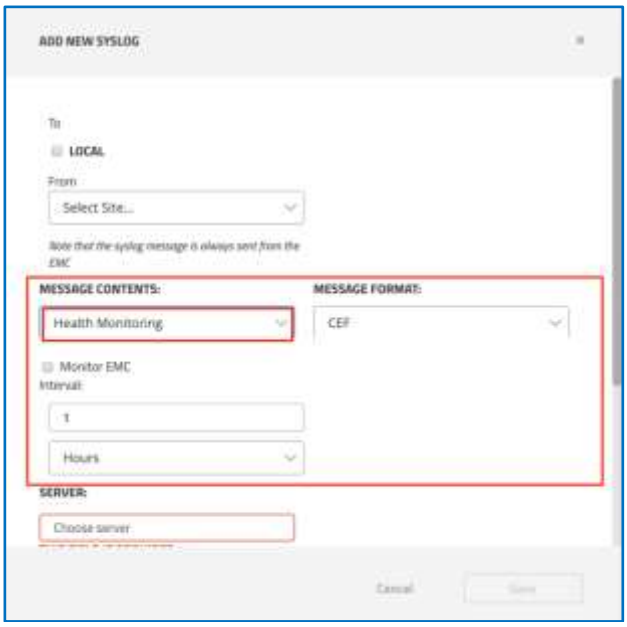


Figure 291 Syslog - Health Monitoring

This option enables sending scheduled periodic system Health Monitoring information via Syslog messages. This can be used for forwarding real time system health status information to external monitoring tools and for alert generation.

For example, the Health Monitoring script can run every hour in the backend, and the results can be sent via syslog.

The Health Monitoring message includes the following:

- CPU utilization
- Memory usage
- Disk utilization
- Network interface packets drop
- Service <service name> is running (for each critical service in the system)
- Queue <queue name> read count (for each critical queue in the system) – count should be greater than 1
- MySQL test query should take up to 10 seconds
- MySQL stuck queries – Expecting 0 queries running more than 10 sec
- Postgres test query should take up to 10 seconds
- Postgres stuck queries – Expecting 0 queries running more than 10 sec

16.4 Syslog Parameters for Message Log Levels

The following parameters are used for the various Syslog types.

16.4.1 Alert Categories

Select which specific **Alert Categories** (Integrity or Security Alerts, or both) should be sent.

> Note This capability can be useful for onboarding SOC teams when taking responsibility on the ICS environment. In the initial phase it is recommended to send the SOC team security alerts only. These are alerts that the SOC is already familiar with. In the next phase, add the integrity alerts gradually (since they are more OT-oriented).

16.4.2 Alert Types

Select which specific **Alert Types**, such as New Assets or Known Threats, should be sent. For common Alert Types, see section 7.3.1.

16.4.3 Protocol dropdown

Select the protocol/s you want to filter for. The drop down displays protocols that exist in the specific environment:

16.4.4 Communication Type dropdown

Search for the types of communication you require or scroll down to select from the list of communication types. Multiple selections are enabled.

- Examples: Alarm, Authentication, Data Acquisition, Diagnosis, File System, Firmware, Network, Operation, Other, Programming.

16.4.5 Access Type dropdown

Select from the following list of access types: **Read, Write, Execute, Publish, None**

16.5 Testing Syslog Servers

Use the **Send a Test Message** option to test the Syslog servers that were added (see Figure 288).

For further details on Syslog with examples, see the **Syslog Specification** in the *TIV Reference Guide.*

17 Configuring User Settings [Only Admins, EMC]

This section describes how to configure and manage security and authentication settings, users, domains, and user groups.

To access User Management:

- Navigate to Settings > User Management:

Figure 292 Settings > User Management Menus

17.1 Managing Security & Authentication Settings

17.1.1 Security Settings

To access security settings:

Navigate to Settings > User Management > Security & Authentication.

The security settings are as follows:

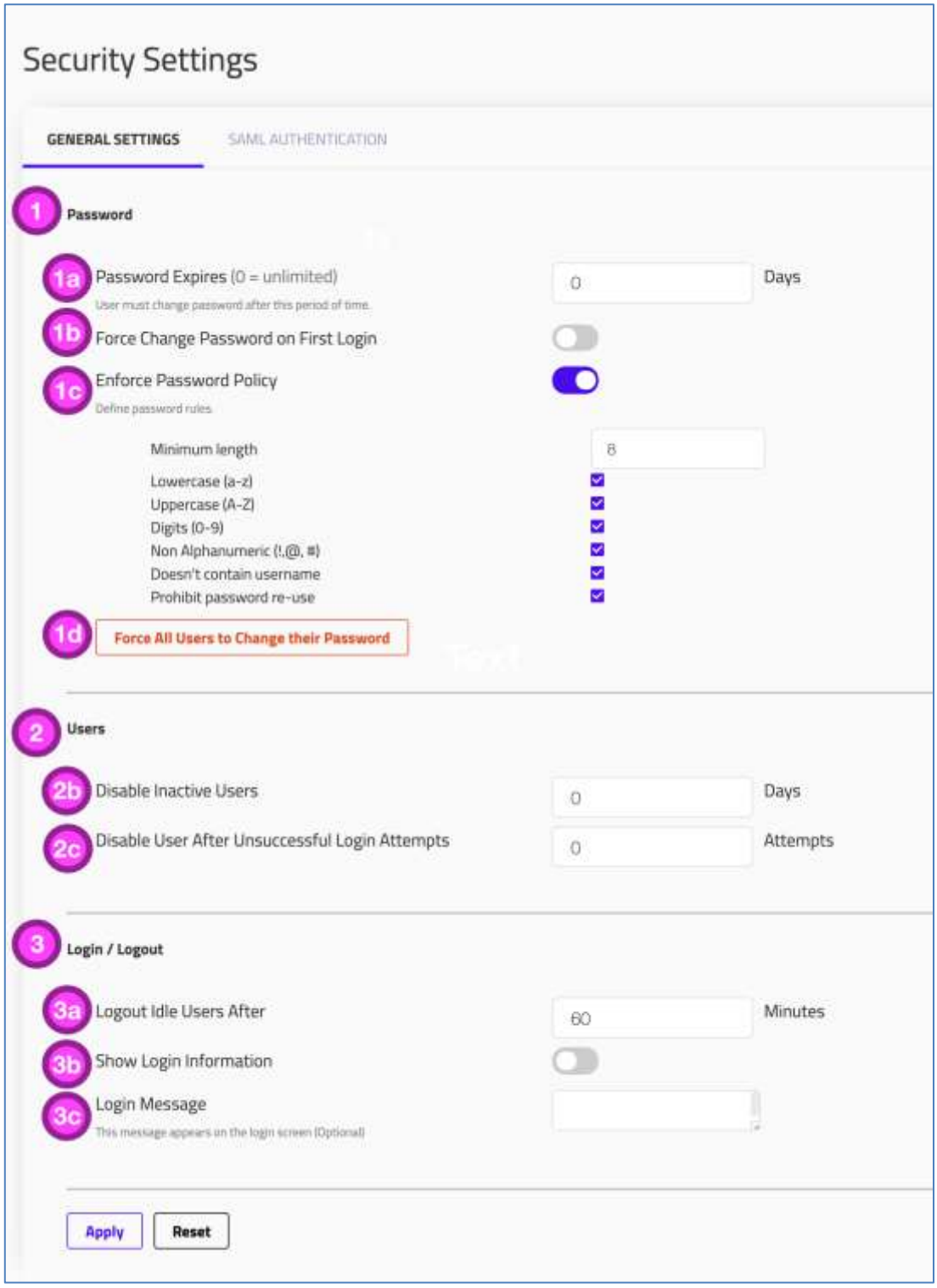


Figure 293 Managing Security Settings

1. Passwords

    a. **Password expire** – Time period, in days, after which users must change their passwords (default is zero, i.e. no expiration).

b. **Force change password on first login** – Slide to the right to require all users to change their passwords upon initial login (default is NO).

c. **Enforce password policy** – Slide to the right to enforce a password policy such as minimum length, number of lowercase characters (default is NO).

d. **Force all users to change their password** – Click this to require users to change their passwords immediately.

2. User Security Settings

a. **Disable inactive users** – Number of days after which a user's account will be disabled if not active (default is 0).

b. **Disable user after unsuccessful login attempts** – Limits users to this number of attempts to log in (default is 0).

3. Login/Logout Settings

a. **Logout idle users** – Auto logging out of idle users after a specified time period in minutes.

b. **Show login information** – Set to OFF by default.

c. **Login Message**– Option that enables Admins to configure a text logon message that pops up on the login screen

4. Click **Apply** to configure these Security settings.

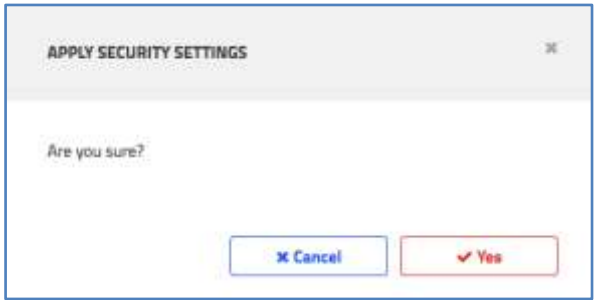


Figure 294 Confirmation of Changes to System Security Settings

17.1.2 SAML Authentication

Security Assertion Markup Language (SAML) is a standard single sign-on (SSO) format. Its authentication information is exchanged through digitally signed XML documents. It enables using SAML 2.0 to connect to third party authentication vendors such as Google and Okta. This complex SSO implementation enables seamless authentication, mostly between businesses and enterprises. With SAML, there is no need to type in authentication credentials or to remember or reset passwords.

To view SAML Authentication:

- Navigate to **Settings** > **User Management** > **Security & Authentication** > **SAML Authentication** tab.

The SAML-based federation involves two parties:

1. An Identity Provider (IdP) that authenticates users and provides an Authentication Assertion if successful;
2. A Service Provider (SP), which relies on the Identity Provider to authenticate users.

SAML Usage

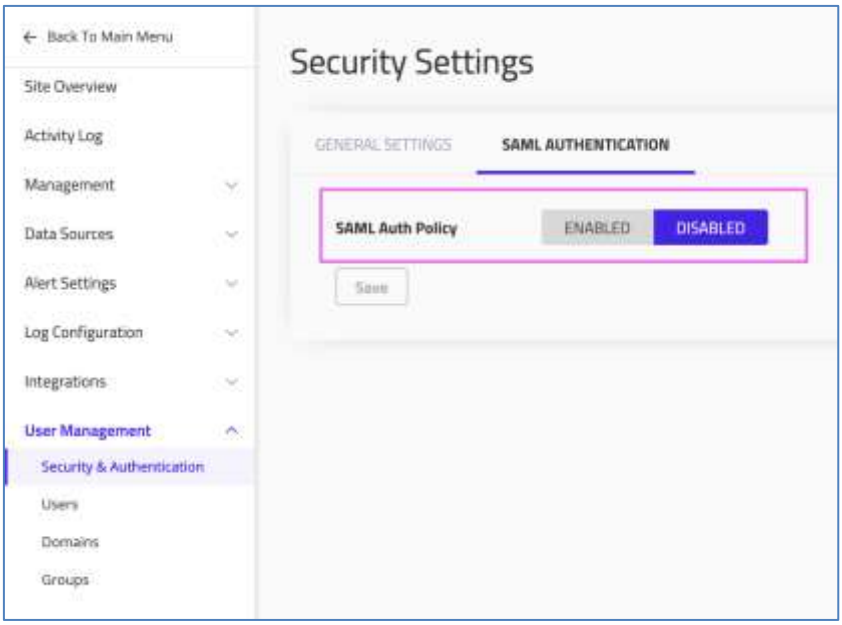


Figure 295 Security Settings - Enabling SAML Authentication Policy

The SAML authentication policy is disabled by default. It can be enabled for all web access users.

When configuring SAML authentication, set the **SAML Auth Policy** flag to **Enable** to reveal the SAML settings:

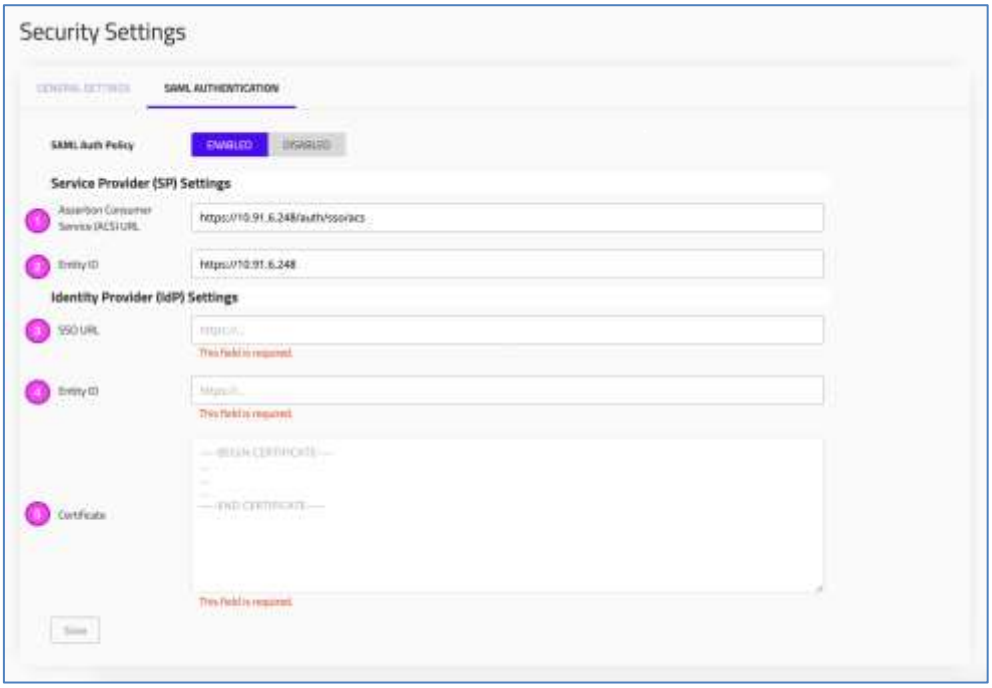


Figure 296 SAML Settings

SP Settings

1. **ACS URL** – An Assertion Consumer Service (ACS) is SAML terminology for the location at a Service Provider that accepts <samlp:Response> messages (or SAML artifacts) for the purpose of establishing a session based on an assertion.
   - (Just leave the default value and make sure it matches the configuration in the IdP)
2. **Entity ID** – The ID of the Service Provider
   (Just leave the default value and make sure it matches the configuration in the IdP. Default values are the IP of the TIV.)

IdP Settings

Configure the following parameters in accordance with the IdP you are working with (e.g. PingIdentity, Okta):

3. **SSO URL** - Single Sign-On URL (of your IdP)
4. **Entity ID** – The ID of your IdP
5. **Certificate** – The Certificate for your IdP
6. **Save** – Click to apply your SAML settings.

17.2 Managing Users

To view User Management:

- Navigate to Settings > User Management > Users.

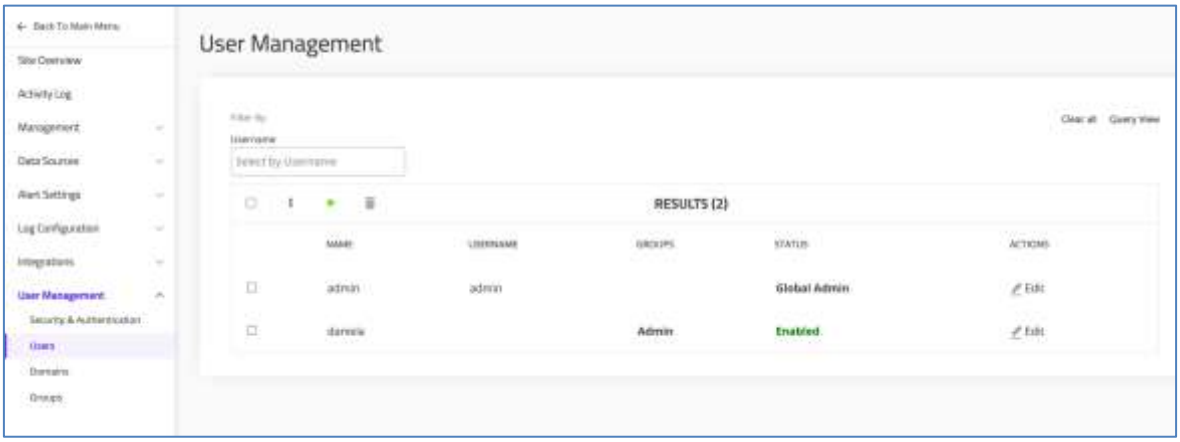


Figure 297 User Management Page

A user must be assigned to a group that has a permission associated with it before that user can log in. Users that have no permissions, or a user that is a member of a group without any permissions, will not be able to log in to the system.

17.2.1 Adding a User

To add a user:

1. In the Main Menu, select **Settings** > **User Management** > **Users**.
2. On the Users page, click **Create New**.
3. In the **New User** window, specify the following (all fields are mandatory):
   - **Username** – A username for the new user
   - **Full Name** – The user's full name
   - **Password** – Create a new password
   - **Repeat Password** – Repeat the password entered in the previous Password field.
4. Click **Add**.

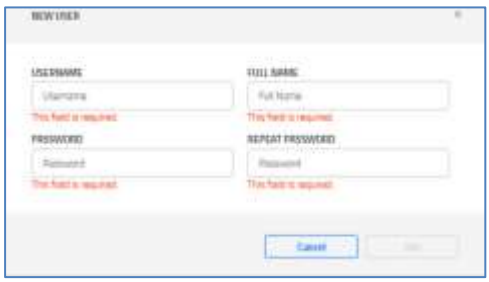


Figure 298 Add a User

17.2.2 Editing User Details

To edit user details:

1. Select **Settings** > **User Management** > **Users**.
2. On the **User Management** page, click the **Edit** icon in the row of the relevant user.
3. In the **Edit User** window, edit the user's information as needed.
4. Click **Save**.

> Note Users have the ability to change their own passwords (see below).

17.2.3 Overriding a User Password

Users have the ability to change their own passwords. Admins can override user passwords using one of the following options:

- Via the **Settings** > **User Management** > **Users** page, click **Edit** for a specific user, and reset the user's password:

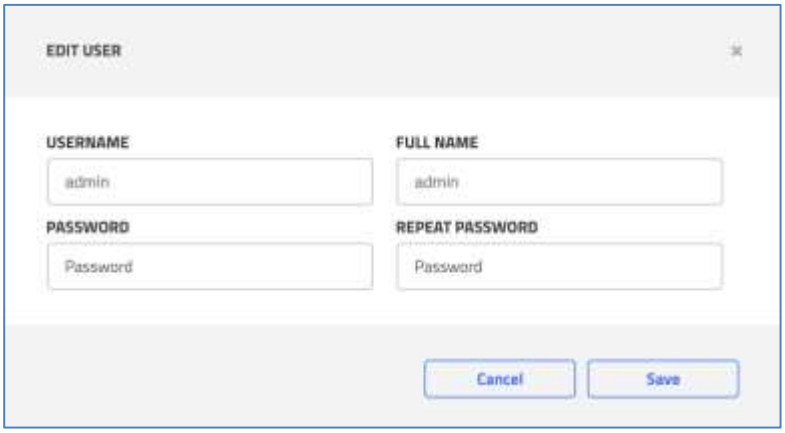


Figure 299 Resetting a User's Password

- Via the Settings > User Management > Security & Authentication page and click the Force all users to change their password button:

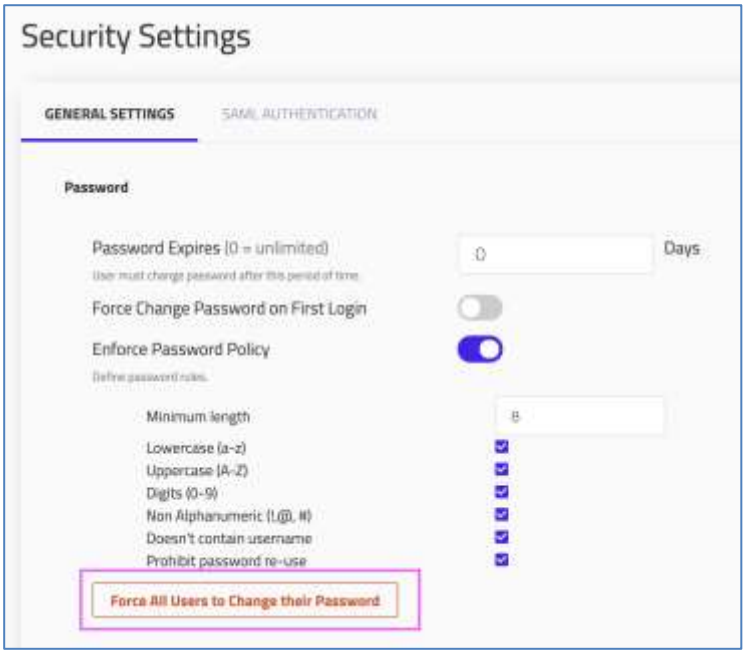


Figure 300 Forcing all users to change their passwords

17.2.4 Setting User Permissions

User permissions are set per groups of users. Therefore, a user must be a member of a group before you can set their permissions.

17.2.5 Adding a User to a Group

To add a user to a group:

1. Select **Settings** > **User Management** > **Groups**.
2. On the **Group Management** page, select the row of the relevant group and click on the **Edit** icon.
3. In the **Edit Group** window, in the Members area, select user/s in the Add User dropdown list.
4. Click **Save** to include the selected user/s to the designated group.

17.2.6 Searching for a User

On the **User Management** page, specify the user's credentials or ID in the **Search** field.

17.2.7 Deleting a User

To delete a user:

1. On the **User Management** page, select the user to be deleted and click **Delete** in the toolbar.

2. To delete the selected user, click **Yes**.

17.3 Managing Domains - Active Directory Configuration

There are two steps in this process:

1. Configuring the Active Directory server
2. Associating a TIV user group with one or more Active Directory user groups.

To manage domains:

- Navigate to Settings > User Management > Domains.

17.3.1 Server Configuration

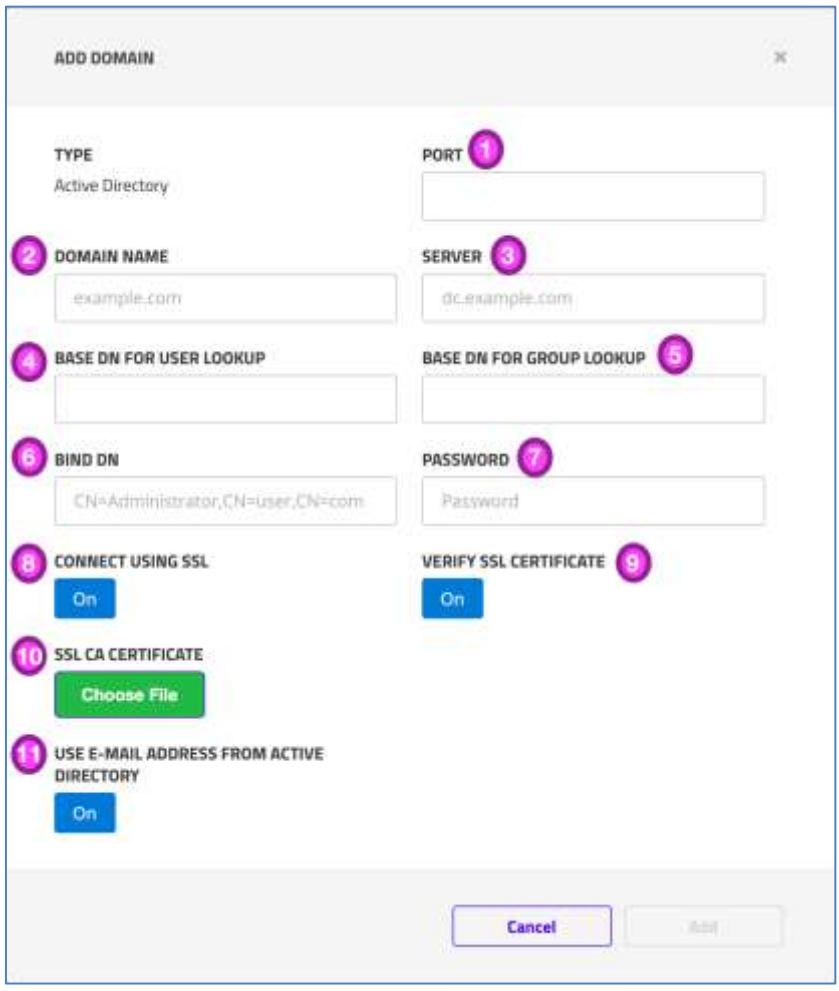


Figure 301 Add Domain - Active Directory

To add a new Active Directory domain, click the **Create New** button  and configure the server as follows:

1. **Port** – For LDAP, use 389. For LDAP over SSL (LDAPS), use 636.
2. **Domain name** – Fully Qualified Domain Name (FQDN).

   For example: "tripwire.com"
3. **Server** – Address of the domain controller. If you choose to verify SSL certificate, you should provider the DNS name of the server, as in the certificate file, and then if needed, add the DNS mapping to `/etc/hosts` of TIV's machine.
4. **Base DN for User Lookup** – Distinguished name (DN) string for the active directory node, in which to search for users.

   For example: "cn=Users,dc=tripwire,dc=com"
5. **Base DN for Group Lookup** – Distinguished name (DN) string for the active directory node, in which to search for groups.

   For example: "cn=Users,dc=tripwire,dc=com"
6. **Bind DN** – Address Distinguished name (DN) string for a user with active directory search privileges.

   For example: "cn=Administrator,cn=Users,dc=shlomi,dc=tripwire"
7. **Password** – Password for the user above.
8. **Connect Using SSL** – Whether the connection made with LDAPS or LDAP
9. **Verify SSL Certificate** – Whether we want to verify the server identity with the server's certificate.

> **Notes** **Microsoft Active Directory Systems**
>
> To receive the certificate file, log in to the domain controller that has the Active Directory Certificate Services role enabled, and perform the following:
>
> Run `certsrv.msc`
>
> On the right pane, right click the **CA** and press **Properties**
>
> View **Certificate -> Details -> Copy to file**
>
> Choose **Base 64**, and **export**

10. **SSL CA Certificate** – Browse for the server's certificate.
11. **Use Email address from active directory** – Whether TIV will use the Active Directory email of the logged in domain users (ON/OFF).
12. Press **Add**
    - The system performs a connection test to the Active Directory and provides an error message if any issue occurs.

After the process is completed, the server is displayed in the **Domain Management** table.

17.4 Managing Groups

17.4.1 Adding a Group

To add a group:

1. Select **Settings** > **User Management** > **Groups**. The Group Management page appears as follows:

Figure 302 Adding a New Group

2. Use the **Search** field to filter for existing associate external groups.
3. Click +Add Group.
   - **The New Group** window appears:

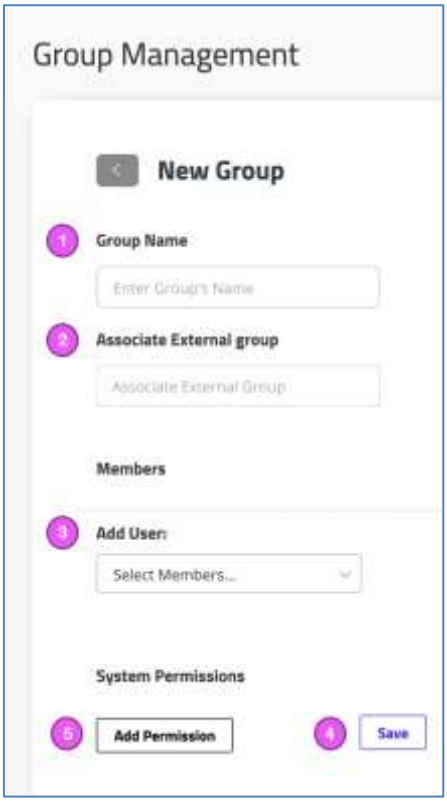


Figure 303 New Group Dialog

In the **New Group** window:

1. Provide a unique name in the **Group Name** field.
2. Enter a unique name in the **Associate External Group** field. Read section 17.4.5 to find out more information.
3. Select a user from the **Add User** dropdown list in the **Members** area.
4. Click **Save** in the **System Permissions** area. Repeat for as many users as needed.
5. Click **Add Permissions** to set the permissions per user group.

17.4.2 Managing Group Permissions

The specified permissions will apply to all members of this group. Note that groups without any permissions cannot be created.

To manage group permissions, click **Add Permission**.

Proceed to set the group's system permissions as follows:

Figure 304 Filters for System Permissions

1. Select specific sites to which the permission applies, or **All sites**.
2. From the **All/Asset** dropdown list, select the relevant option.
3. From the **Select attribute** dropdown list, select the relevant attribute.
4. In the **Filters** field, specify the filter.
5. Press **+And** to include any additional filters needed for this item.
6. Set the appropriate permission level: **Read** (default), **Write,** or **Admin**.
7. To reset system permissions prior to committing them, click **Delete** .
8. (Optional) Click **Add permission** Add permission to add attributes and filters to the user group. Repeat the procedure to add as many additional permissions as needed.
9. Click **Save**.

17.4.3 Editing Group Details

To edit group details:

1. Select Settings > User Management > Groups.
2. On the **Group Management** page, click on the **Edit** icon Edit in the row of the relevant group.
3. In the **Edit Group** window, edit the group member/s and permission/s as needed.
4. Click **Save**.

17.4.4 Deleting a Group

To delete a group:

1. On the **Group Management** page, select the row of the relevant group and click **Delete**:

Figure 305 Selecting Group to Delete

2. To confirm deletion of the group, click **Yes**.

After the group is deleted, the user exists without that group's permissions.

> Note: You have to associate a user with a group, with the exception of the default admin user that has automatic privileges. The admin user cannot be removed and doesn't need to be in a group.

17.4.5 Group Associations

To view group associations:

1. Navigate to **Settings** > **User Management** > **Groups** and edit an existing group or add a new Group as described above in section 17.4.1.
2. In the **Associate External Group** field, enter the Active Directory group you would like to associate with this TIV User Group.
3. After the External Group is selected, click **Save**.
   - Users with the Active Directory groups will now receive permissions in accordance with the associated TIV group.

   To manage permissions, see section 17.4.2.

18 Appendix A: Terminology

The table below defines the terms used throughout this document.

Table 11 Terms and Definitions

Term	Meaning
ACS	Assertion Consumer Service
AD	Active Directory
Alert	An event that may cause a threat or a risk to the security of the network and requires attention and investigation.
Alert Indicator	A predefined characteristic of an alert that affects the alert score.
Alert Score	A number representing the overall alert importance, resulting from the collection of observed indicators and network activities.
App DB	Application Database
ARP	Address Resolution Protocol. A communication protocol used for discovering the link layer address associated with a given IPv4 address, a critical function in the Internet protocol suite. Used for mapping a network address such as an IPv4 address, to a physical address, such as a MAC address.
Asset	Any distinguishable network entity.
Attack Vector	A path or means by which a hacker can gain access to a computer or network server to deliver a payload or a malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities.
Baseline	The TIV collection of valid network behaviors. An individual baseline represents a command or an instance of communication between two assets.
Baseline Deviation	During training mode, the system learns the existing asset communication and defines a baseline for how a normal asset (or group of assets) behaves on the network in terms of its communication patterns. A baseline deviation occurs when a communication occurs that has not been defined yet. During operational mode, baselines can be changed or further defined by auto-generated virtual zones and user approved alerts.
BPF	Berkeley Packet Filter. A mechanism to write/read packets to/from the network interface.
CSR	Certificate Signing Request
CAM	Content Addressable Memory table. **Used to record** a station's MAC address and its corresponding switch port location. Common in Layer 2 switching.
Cloud Reputation	Indications about the common rates of policy zone rules among different sites. This feature enables common rate of a specific rule among sites around the world.

Term	Meaning
CDP	Cisco Discovery Protocol. A proprietary Data Link Layer protocol developed by Cisco Systems. Used to share information about other directly connected Cisco equipment, such as the operating system version and IP address.
CEF	Common Event Format. A proprietary syslog-based event format that can be used by other vendors.
Chain of Events	A series of alerts/events that are correlated with each other and generated an alert and require investigation as group.
CIDR	Classless Inter-Domain Routing. IP Address syntax that uses IPv4 address space and prefix aggregation, known as route summarization or super-netting.
CIP	Common Industrial Protocol. Industrial protocol for industrial automation applications.
ClarotyOS	A hardened, purposely built Linux OS, ready for use for TIV out-of-the-box. Every TIV Appliance is delivered pre-installed with ClarotyOS for quick deployment.
CMDB	Configuration Management Database. A data repository that acts as a data warehouse or inventory for information technology (IT) installations. It holds data relating to a collection of IT assets, the relationships between assets and enables understanding the composition of critical assets such as information systems. Also help organizations track the configuration of components in the system.
Community	Group of TIV devices that are interconnected with the same EMC.
TQL	TIV Query Language. Provided for users to build swift SQL-like query statements for filtering data in the system.
CSV	Comma-separated values. A delimited text file that uses a comma to separate values. A CSV file stores tabular data (numbers and text) in plain text. Each line of the file is a data record. Each record consists of one or more fields, separated by commas. The use of the comma as a field separator is the source of the name for this file format.
TIV	Tripwire Industrial Visibility. The anomaly detection product within the Tripwire Platform for ICS networks, providing rapid and concrete situational awareness through real-time alerting. Constantly monitors ICS network traffic and generates alerts for anomalous network behavior that indicates a malicious presence and for changes that have the potential for disrupting the industrial processes.
CTI	Claroty Threat Intelligence. A highly curated, multi-source and tailored feed that enriches TIV's RCA with proprietary research and analysis of OT zero-day vulnerabilities and ICS-specific Indicators of compromise (IoC) linked to adversary tactics, techniques and procedures (TTP). CTI's YARA rules, for example, run on OT asset configuration changes and code sections, not just IT artifacts. CTI equips threat hunters and incident responders with the relevant context needed to detect and prevent targeted attacks early in the kill chain and mitigate the consequences of malware infections.

Term	Meaning
CVE	Common Vulnerabilities and Exposures. A catalog of known security threats. The threats are classified as vulnerabilities or exposures. The CVEs originate in software or firmware, and are identified, standardized and cataloged into a free “dictionary” for organizations to improve their security.
CVSS	Common Vulnerability Scoring System. A standardized method to indicate how critical a specific CVE is.
DCP	Discovery and Basic Configuration Protocol. A protocol definition within the PROFINET context. A link layer-based protocol to configure station names and IP addresses. It is restricted to one subnet and mainly used in small and medium applications without an installed DHCP server.
DDoS	Distributed Denial-of-Service. An attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. In this type of attack, multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource.
DHCP	Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.
DN	Distinguished Name. The fully qualified name of a domain or network device.
DNP	Distributed Network Protocol. A set of communication protocols used between components in process automation systems.
DNS	Domain Name System. A hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
DoS	Denial-of-Service (attack). Also known as DDoS (Distributed Denial of Service)
DPI	Deep Packet Inspection. A form of computer network packet filtering that examines the header and data part of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria. This method is used for identifying specific assets in the ICS network, lines of asset communication, communication timing, protocol communication between assets, types of commands and registers used, and the values of valid responses.
EMC	Enterprise Management Console, i.e. the Central Appliance at operation headquarters.
ENIP	Ethernet Industrial Protocol (Ethernet/IP)
Event	A single network event that TIV has collected using Deep Packet Inspection (DPI). Some of the events will be classified as alerts, e.g. when they pose a risk or threat to the network. See also Master Event.
Event Indicator	See Indicator

Term	Meaning
EWS	Engineering WorkStation. A high-end very reliable computing platform designed for configuration, maintenance and diagnostics of control system applications and other control system equipment.
FQDN	Fully Qualified Domain Name
FW	Firewall
GDPR	General Data Protection Regulation. A European Union regulation that specifies standards for data protection and electronic privacy in the European Economic Area, and the rights of European citizens to control the processing and distribution of personally identifiable information. Aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
HDD	Hard Disk Drive
HMI	Human-Machine Interface. A software application that presents information to an operator about the state of a process and accepts and implements the operator's control instructions.
HTTP	Hypertext Transfer Protocol. An application protocol for distributed, collaborative, and hypermedia information systems. HTTP is the foundation for data communication on the web.
Hygiene Score	TIV widget displaying the current cumulative risk level posed to the system by the insights. This score comprises the critical security insights, CVEs and anomalies that were detected, as well as how many critical assets were identified. A low hygiene score indicates that the system is highly vulnerable to attacks.
ICMP	Internet Control Message Protocol. A supporting protocol in the Internet protocol suite used by network devices.
ICS	Industrial Control Systems. Control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems.
IdP	Identity Provider. A system entity that creates, maintains, and manages identity information for principals while providing authentication services to relying applications within a federation or distributed network
IED	Intelligent Electronic Devices
IoC	Indicators of Compromise
Incident	An instance of invalid network activity (network failure, malicious attack, user error, etc.)

Term	Meaning
Indicator	■ **Static Indicator** – Static information that con potentially affect the score of an alert. For example: The asset type, subnet, and virtual zone group. ■ **Event Indicator** – An observed related network activity that can potentially affect the score of an alert and provides context to the given alert. For example: Whether an asset has performed write operations, or whether an asset has communicated using SMBv1.
Insight	Knowledge mined from TIV about the system or about one of the entities in the system.
IoT	Internet of Things. A system of interrelated computing devices, machines or objects that transfer data over a network. TIV's proprietary framework swiftly incorporates and processing these devices and provides micro-segmentation in the same manner as it does for IT and OT assets, with unified visibility, security monitoring and risk assessment. By automatically discovering and classifying IoT devices in the network, TIV correlates them with known vulnerabilities and continuously monitors them.
IoT Matcher	Simple code section in JSON format describing the retrieval of information from an IoT device. These Active HTTP and Telnet queries made to the assets obtain important device information (such as vendor, model, type, OS version, role).
IP	Internet Protocol. A numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It provides identification of the host or network interface and the device's location address.
IT	Information Technology
JSON	JavaScript Object Notation. A lightweight format for storing and transporting data, usually used when data is sent from a server to a web page. It is "self-describing" and easy to understand.
Known Threats	TIV uses a sophisticated signatures-based database to enhance its capability for identifying known attacks.
KPI	Key Process Indicator. A quantifiable measure used to evaluate the success of an organization, employee, etc., in meeting performance objectives.
MAC	Media Access Control address. This device address is a unique identifier assigned to a network interface for communication at the data link layer of a network segment.
Master Event	An event that occurs whose sensitivity value determines that it is not interesting or relevant enough to be classified as an alert.
MitM	Man-in-the-Middle. Type of attack in which the attacker secretly relays and possibly alters the communication between two parties who believe they are communicating with each other directly.
ML	Machine Learning. TIV's ML alert algorithm delivers fast response without the distracting noise of unnecessary alerts.
MLFB	Order Number

Term	Meaning
NetFlow	Source of asset data and network anomaly detection whose summarized data flows through the network. Enhances TIV's statistical data for network analytics.
NTP	Network Time Protocol
Operator	A person in charge of operating TIV.
Operational mode	System mode in which the system raises alerts about new assets, baselines, and abnormal communication, having already learned the necessary information about the network communications in the site from Training mode
OS	Operating System
OT	Operational Technology. Hardware and software that detect or cause a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.
PCAP	Packet Capture. By using PCAPs to records events, TIV can display which information was changed during a particular action/activity.
PCS 7	SIMATIC PCS 7 Process Control System.
Ping Sweep	AKA an Internet Control Message Protocol (ICMP) sweep. A supporting protocol in the Internet protocol suite used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached. Whereas a single ping will tell you whether one specified host computer exists on the network, a ping sweep consists of ICMP ECHO requests sent to multiple hosts; if a given address is live, it will return an ICMP ECHO reply.
PLC	Programmable Logic Controller. An industrial digital computer that has been ruggedized and adapted for the control of manufacturing processes.
Policy Rule	An expression that differentiates between communication that is considered a corporate policy violation and that which is allowed.
Policy Violation	Type of alert triggered when the detected communication did not match any explicit 'Allow' or 'Alert' policy rule
PsExec	A light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software.
RCA	Root Cause Analytics. This TIV feature provides visibility into the chain of events leading up to every single alert, which is particularly important for OT security alerts. RCA enables fast and easy triage of alerts, as well as proactive threat hunting. By providing the context surrounding the associated threat and risk, RCA helps users hunt for threats and resolve security events.
RTU	Remote Terminal Unit. A multipurpose device used for remote monitoring and control of various devices and systems for automation. It is typically deployed in an industrial environment and serves a similar purpose to PLCs but to a higher degree.

Term	Meaning
SAML	Security Assertion Markup Language. An open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider (IdP) and a service provider (SP). SAML is an XML-based markup language for security assertions (statements that service providers use to make access-control decisions).
S7Comm	Siemens proprietary protocol that runs between PLCs of the Siemens S7-300/400 family
SCADA	Supervisory Control And Data Acquisition
Sensitivity	Entity that controls the level to be used when correlating between associated alerts. For example, high sensitivity is in effect when the user trusts the communication between zones.
SIEM	Security Information and Event Management
SMB	Server Message Block. SMB operates as an application-layer network protocol mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network. It also provides an authenticated inter-process communication mechanism.
SMTP	Simple Mail Transfer Protocol. An Internet standard for electronic mail (email) transmission.
SNMP	Simple Network Management Protocol
SOC	Security Operations Center. A centralized unit dealing with security issues on an organizational and technical level.
SP	Service Provider. A system entity that receives and accepts authentication assertions
SPAN	Switched Port Analyzer. Used to monitor network traffic. With port mirroring enabled, the SPAN switch sends a copy of all network packets seen on one port (or an entire VLAN) to another port, where the packet can be analyzed.
SSH	Secure Shell. Cryptographic network protocol for operating network services securely over an unsecured network. Provides administrators with a secure way to access a remote computer. This encryption and protocol technology is used to connect two computers to lock out eavesdroppers by encrypting the connection and scrambling the transmitted data so it is meaningless to anyone outside of the two computers.
SSL	Secure Sockets Layer. Standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
Story	See Chain of events
Subnet	A group of IPs. Used to segregate the internet

Term	Meaning
SYN	A type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.
TCP	Transmission Control Protocol
Training mode	Learning mode in which TIV dynamically profiles the site's normal process behavior, assembling a baseline by observing all network traffic and registering it as valid. Alerts are triggered for critical changes and security risks, and newly discovered assets and communication patterns are recorded in the baseline as shown on the System Management page.
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface. A specification for a software program that connects a computer's firmware to its operating system (OS). UEFI is expected to eventually replace BIOS. Like BIOS, UEFI is installed at the time of manufacturing and is the first program that runs when a computer is turned on.
UI	User Interface
UPS	Uninterruptible Power Supply
User	A person using the TIV web interface.
UUID	Unique User Identification.
Virtual Zones	Capability for grouping related assets in a logical view. Virtual Zones allow definition of a Baseline Deviation alert policy for each Virtual Zone or communication between Virtual Zones.
VM	Virtual Machine
WMI	Windows Management Instrumentation. The infrastructure for management data and operations on Windows-based operating systems.
Zones	See Virtual Zones