Radiflow

iSID 6.0
USER MANUAL

Copyright

Statement of Liability

This publication has been compiled with care. The information contained herein is provided solely as a user guide for the Radiflow iSID. Radiflow Ltd and its distributors are not liable, nor do they assume any responsibility, for any errors, accidents, personal injuries, consequential or incidental damages, loss of profits, loss of use, or any other damages that may result from the misuse or misrepresentation of any information contained in this publication.

iSID - Controlled release 6.0

www.radiflow.com

INDUSTRIAL THREAT DETECTION

- ✓ Automatic learning of topology and operational behavior
- ✓ Network traffic analysis based on DPI protocols for SCADA
- ✓ Supervision over configuration changes in PLCs
- ✓ Model-based anomaly detection analytics
- ✓ Signature-based detection of known vulnerabilities learning
- ✓ Non-intrusive network operation
- ✓ Central or distributed deployment
- ✓ Low false alarm rate
- ✓ Integration with third-party security systems (e.g. SIEM)
- ✓ NERC CIP-compatible reports

Contents

Introduction

Radiflow iSID Industrial Threat Detection System for SCADA networks is a server-based software that analyzes the operational technology (OT) network traffic in order to protect against cyber threats.
It is a low-maintenance and low-false alarm solution, designed specifically for the needs of ICS/SCADA network security.

Radiflow iSID includes six security packages to protect the OT network. Each package has a unique capability to detect suspicious traffic within the network in order to protect the process.

The Radiflow iSID system also combines the following two distinct capabilities:

- SCADA/ICS modeling
- Anomaly detection

SCADA/ICS Modeling

Radiflow iSID receives a parallel (mirrored) stream of all network traffic (directly or through remote RF-2120 /80 smart probes) and analyzes it to both generate and display a network topology model; and to maintain the model and serve as a baseline for detecting exceptions indicating unauthorized traffic.

Anomaly Detection

Deploying the iSID system in ICS/SCADA networks enables securing operational technology networks through the monitoring of distributed networks and detection of topology changes, SCADA information integrity breaches, known threats, and anomalous behavior in operational networks.

Web Based Solution

Radiflow iSID simplifies the management of detected network threat events. Its web-based solution is designed to display the most critical information as an overlay over familiar network topology.

The web-based solution includes two distinct views:

- Dashboard view - displays a security event summary as well as a set of aggregating statistics, including the number of detected security breaches
- Network map view - provides real-time visibility of the network topology, with indications for detected risks on the ICS/SCADA networks

The web-based application provides alerts on detected security events and alert management tools, in addition to easy access to data, configuration tools, and overall functionality information.

Functional Description

Network Visibility

Radiflow iSID is able to automatically learn the traffic within the OT network by means of passive network scanning. To do this, the iSID receives data from all devices across the entire network (using port mirroring.)

During the learning stage the data is used to construct a network model for all devices, protocols and sessions, which is displayed on a GUI at the end of the learning stage.

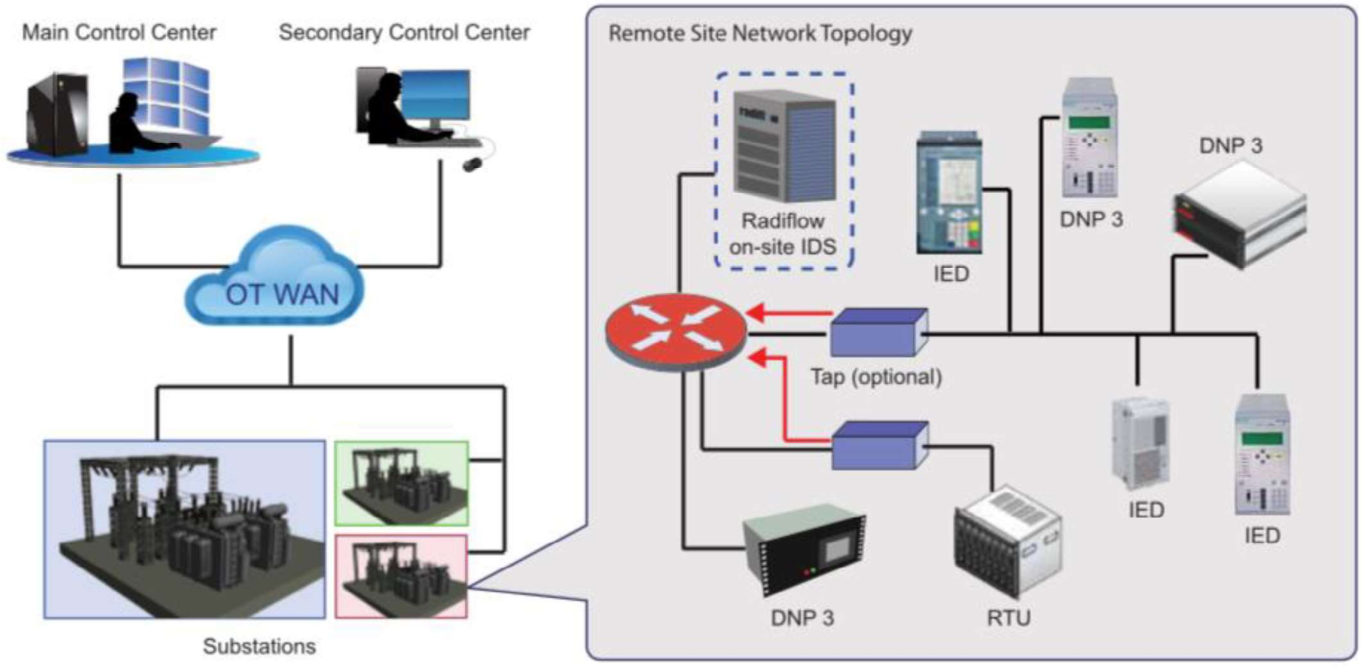
The visual network model helps to understand the processes that take place across the OT network, including security events. The visual network model map is also used to manually edit the network model itself, e.g. to add a client PC at one of the remote sites that was not detected during the learning stage.

Following the learning stage, any detected change in the network topology, such as new devices or new sessions, will trigger an alert, compelling the user to evaluate the underlying event.

CYBER ATTACK

The Cyber Attack package handles known threats designed to exploit vulnerabilities in the SCADA network, including threats to PLCs, RTUs and industrial protocols.

The vulnerability signatures used by the Cyber Attack package are based on public data sources (research labs) as well as Radiflow Labs' own research. The signature database is continuously updated and made available to respond to emerging threats.



Radiflow iSID installed at a remote site

Policy Monitoring

The Policy Monitoring package allows defining policies for each link on the SCADA network. These rules, based on Deep Packet Inspection (DPI) for SCADA protocols, allow the validation of specific commands (e.g. “write to controller”) and operational parameter ranges (e.g. the technician should not change the RPM parameter of a turbine outside the 600-800 rpm range.) If a violation occurs, these rules will generate an alert at the control center.

The Policy Monitor also allows editing firewall rules suggested by the iSID following the learning period, and/or easily creating rules manually.

Maintenance Management

Maintenance operations pose innate complexity and risk, since the user is required to grant network access to the maintenance technician, thus exposing the network during maintenance. The current situation in most SCADA-based systems is that once the technician is granted access, there is no way for the user to know what’s happening on the network, unless a problem arises.

Radiflow iSID offers a dedicated Maintenance Package to handle maintenance processes. The Maintenance Package provides the option to easily create work orders for specific devices at set time windows through a centralized tool. During maintenance, the iSID offers two monitoring modes: pause monitoring for the maintained zone during the defined time period, to prevent many false alarms; or close monitoring of the maintenance process, and generating an alert for each unauthorized command executed outside the defined work order. For example, a maintenance work order can be defined to allow access to a specific device, and only between 8:00AM and 10:00AM on a certain day. Outside of this time period, any command would be unauthorized. At the end of the maintenance period, a log report of all activities during the maintenance session is issued by the iSID.

Implementation Overview

While the implementation of devices—especially security devices--on SCADA networks is typically far from simple, installing Radiflow iSID is very easy and quick, and does not require making changes to the operational technology network traffic.

Modes of Operation

Radiflow iSID can operate in three modes:

- Idle - iSID security packages remain passive, allowing the user to define configuration parameters and review existing data.
- Learning - iSID collects network information, which is used to build a complete network and industrial communication model. The network topology is presented as a graphical map allowing the investigation of processes and gaining an understanding of the network's inner workings.
- Detection - at the conclusion of the learning stage you can transition the iSID to Detection mode. In this mode, the iSID provides constant network monitoring based on the data gathered and analyzed during the Learning mode. In Detection mode iSID uses analytical engines to detect unauthorized traffic or cyber threats on the SCADA network.

Learning Stage

Upon installation, the iSID enters the Learning Stage in which it collects information about the network.

Radiflow iSID begins to passively collect information about the network. During this stage, a copy of the network traffic is streamed to the iSID with no network intervention, i.e. – passive learning of the network.

Radiflow iSID's DPI (deep packet inspection) capability is used to extract valuable data such as MAC addresses (L2), IP Addresses (L3), transport protocol (L4), industrial protocol specific information (L5-7) - all of which are necessary to learn the overall behavior of the network.

All of iSID's six security packages take part in the Learning Stage, as it is imperative for each package to define the predictable behavior of the network.

The collected data is used to build a complete network model, which in effect assigns a virtual fingerprint to each session between any two devices on the OT network.

The network model is then translated into a privileges list, which triggers an alert on every non-baseline activity. Besides assigning a unique identifier for each session, Radiflow iSID graphically lays out the network topology on its GUI, allowing the investigation of processes and providing insight into the network's inner workings.

Depending on the configurable storage size, Radiflow iSID traffic capture feature saves traffic permanently in PCAP file format, which can be easily downloaded and analyzed for further inspection.

Network Learning

Network Learning consists of several stages that are performed in the background:

1. Identify network devices by: MAC address, IP Address, Unit ID / ASDU, Router's Vendor, device type.
2. Learn the protocol used by the device, and its role in this protocol (Master/Slave).
3. Identify network connections by: source device and destination device, protocol used, function codes on the link, exception responses and errors in parsing.
4. Logical graphical map is created including a table with all the types of connection.
5. Creation of rules. The information learned is generated and presented in the suggested rules, including auto generated rules based on the learned network that will later allow you to better control the network behavior.
6. Concluding the Learning stage. Learning is concluded when requested from the user.

Detection Stage

At the end of the Learning Stage iSID transitions to the Detection Stage. In this stage iSID performs real time monitoring of the traffic based on network topology created in the Learning Stage.

In Detection Stage, iSID provides continuous network monitoring and uses its six security packages to detect various cyber threats on the SCADA network.

During this stage iSID raises an alert for every possible attack, anomaly, or change in network behavior. The iSID's dashboard displays a dynamic security event log, as well as a set of aggregate statistics including the number of security breaches detected by each engine and the cyber-health of each sub-network. Alongside the statistics, by drilling down to specific devices the user is able to edit each device's policy monitor rules. This provides users with great flexibility in managing individual devices.

Once iSID detects an unauthorized activity in the network it issues an alert on the IDS (or sends Syslog messages to the Syslog server). The user assigned to investigate the alert can extract the PCAP file from the iSID to expedite the response to the incident. In addition, the various reports generated by the iSID help improve compliance with regulatory requirements such as NERC CIP.

Smart Probe

Typically, IDS systems are implemented as local systems, usually at large sites.

Radiflow Smart Probe enables implementing an IDS at a central location, for the purpose of monitoring multiple small remote sites.

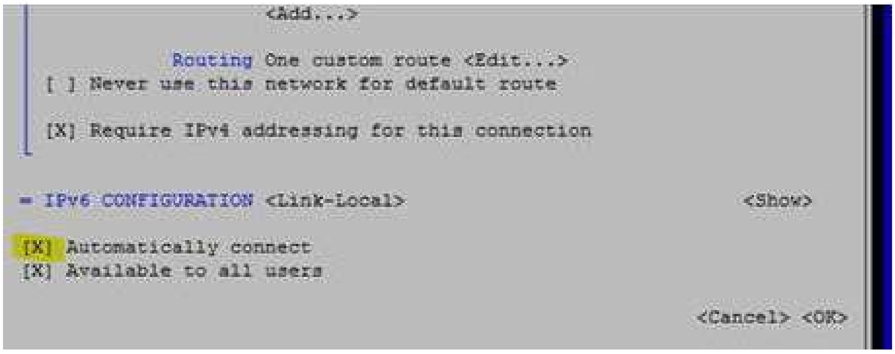
This type of implementation would typically create a network overload problem, caused by the collection and sending of large volumes of data to the Central IDS. Radiflow's complimentary Smart Probe solves this problem: installed at each site, receives all LAN traffic from the local switch, using port mirroring. It then filters out much of the general traffic data, leaving intact the SCADA traffic (e.g. ModBus data). To further prevent network overload, the Smart Probe compresses the data, and the compressed, filtered traffic is sent to the central iSID over VPN tunnels.

Install

Installing Radiflow iSID is a simple process that does not require making changes to the OT network traffic.

Minimum Hardware Requirements:

- CPU: Intel i5 Quad-Core
- RAM: 16GB DDR4
- HDD: 1TB HDD RAID 0,1 (additional storage may be required based on retention needs)
- Network: 3 x Network Interface Cards (NIC)
- Operating System: CentOS distribution 8.2 (will be provided by Radiflow)
  Note: Make sure the server's interfaces are enabled and 'auto connect' configuration is enabled (using 'nmtui' utility)



```
                          <Add...>

                  Routing One custom route <Edit...>
  [ ] Never use this network for default route

  [X] Require IPv4 addressing for this connection

═ IPv6 CONFIGURATION <Link-Local>                          <Show>

[X] Automatically connect
[X] Available to all users

                                                    <Cancel> <OK>
```

Install iSID via a CLI

1. Enter the following commands to install Radiflow iSID
   # cd ~
   # tar -xvf isid-<x.x.x.x>.tar (where <x.x.x.x> is the iSID version number)
   # cd isid-<X.X.X.X> (where <x.x.x.x> is the iSID version number)
   # sudo ./start.sh
2. When the menu appears, select 1 to begin the installation process.
3. When the installation is complete, select 2 to configure the IP address.
4. Enter the IP address for the management interface, subnet mask, name of the NIC that will serve as the management interface and the default gateway (same as set during the CentOS installation procedure)
5. Select 0 to exit.
6. Enter the command: # reboot
7. Log in again. Wait for one minute, and check all relevant processes are running by entering # sseq
8. On your PC, do the following:
   - Open Google Chrome
   - Browse to the following address:
     https://<IP address> (iSID server address as set during the installation)
9. Send the displayed code to your system integrator or Radiflow in order to receive the activation key.
10. Upon receiving the activation key, enter it as required.

After installing Radiflow iSID, by default the SCADA servers are disabled.

Enable the interface

1. Choose either DNP3 (Distributed Network Protocol) or Modbus RTU.
2. Enable the interface as follows:

```
sudo rfids stop
sudo isid-components --activate-components dnp3-interface
sudo isid-components --activate-components modbus-interface
sudo rfids start
```

Install iSID via RIM

Overview

As an alternative to the command line, Radiflow provide an intuitive, web-based installation manager, called RIM (Radiflow Installation Manager).

Install RIM

In order to make use of RIM, you first need to install it on the target server (the server on which you intend to install iSID or iCEN).

To install RIM:

1. Copy the tar file provided to the target server.
2. Run the following from a command line on the target server:

```
tar -xvf rim-<x.x.x.x>.tar (where <x.x.x.x> is the RIM version number)
cd rim-<x.x.x.x> (where <x.x.x.x> is the RIM version number)
sudo ./start.sh
```

Access RIM

To access RIM, open a Chrome web browser and navigate to:

https://<Server IP>/rim

Note:

- Server IP is the IP of the target server (the server on which you intend to install iSID or iCEN)
- Currently, Google Chrome is the only officially supported browser.

The RIM workflow

Installing an image via RIM involves 3 steps:

1. Upload an image to the target server.
2. Install the uploaded image.

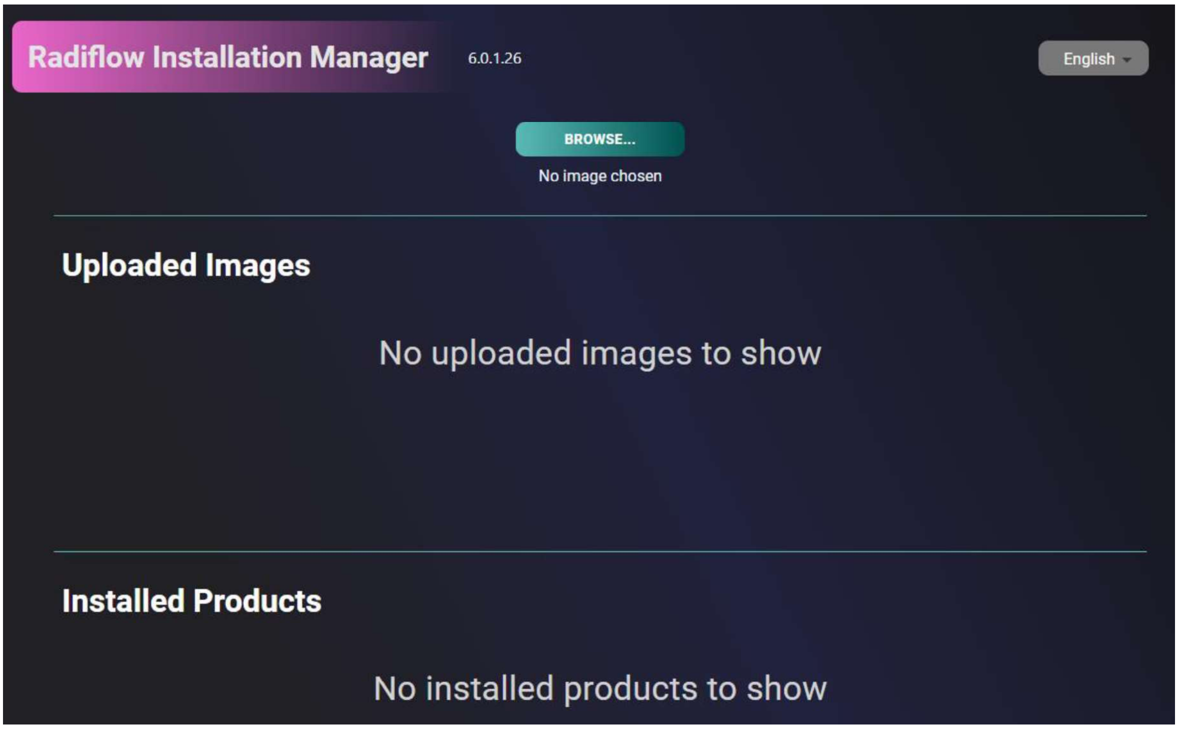
3. Run the installed image.

Each of these steps is preformed independently. You can upload an image, and decide to install it later. You can install an uploaded image and decide to run it later.

Get familiar with the UI

The RIM page is divided into 3 sections:

1. Upload - you can upload new images here
2. Uploaded Images - images that have been uploaded to the server (but might not be installed)
3. Installed Products - images that have been installed on the server (but might not be running)


Radiflow Installation Manager
6.0.1.26
English
BROWSE...
No image chosen
Uploaded Images
No uploaded images to show
Installed Products
No installed products to show

Change the UI language

You can change the RIM UI and input language:

1. Access the RIM UI.
2. Select the desired language on top, right.

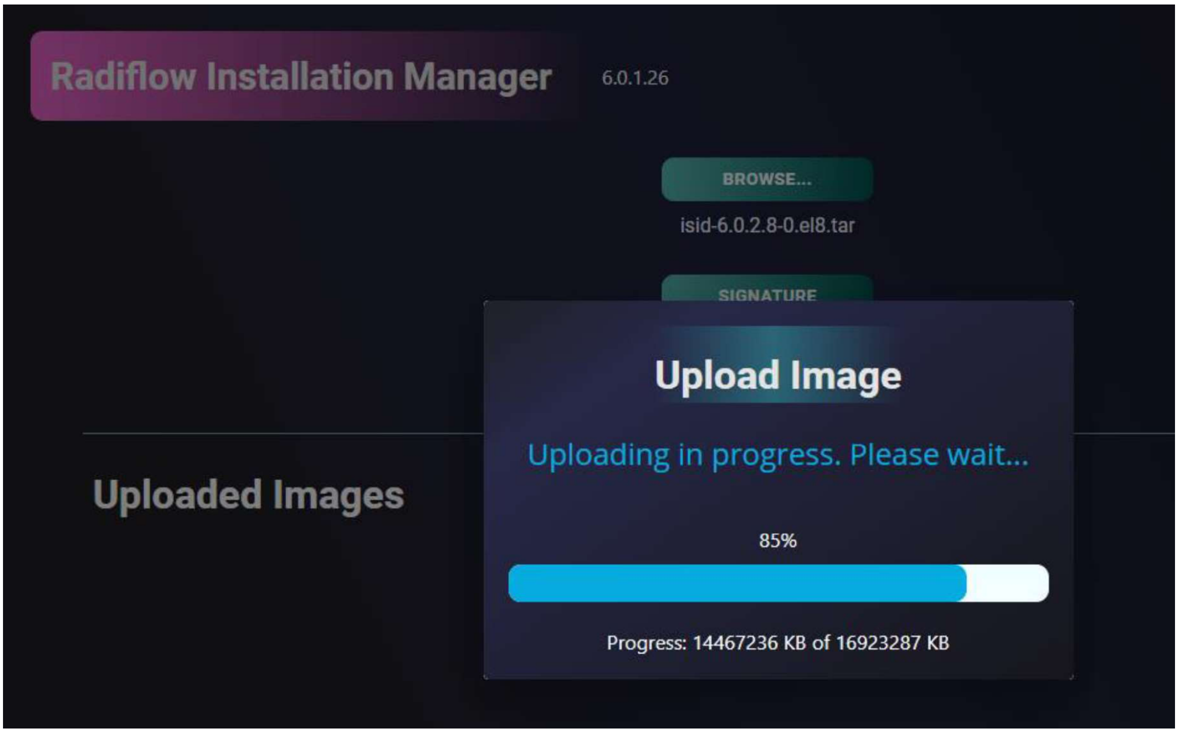
Note: currently, the following 2 languages are supported:

- English (default)
- German

Upload an image

1. Access the RIM UI.
2. Click on Browse (top) and select the relevant image file.

   Note: Initially, only the Browse button is visible. Each time you complete a step, the subsequent button will display.
3. Click on Add Signature and select the relevant signature file.
4. Click on the Upload icon and confirm.
5. A progress bar shows the upload progress:



isid-6.0.2.8-0.el8.tar

Upload Image

Uploading in progress. Please wait...

85%

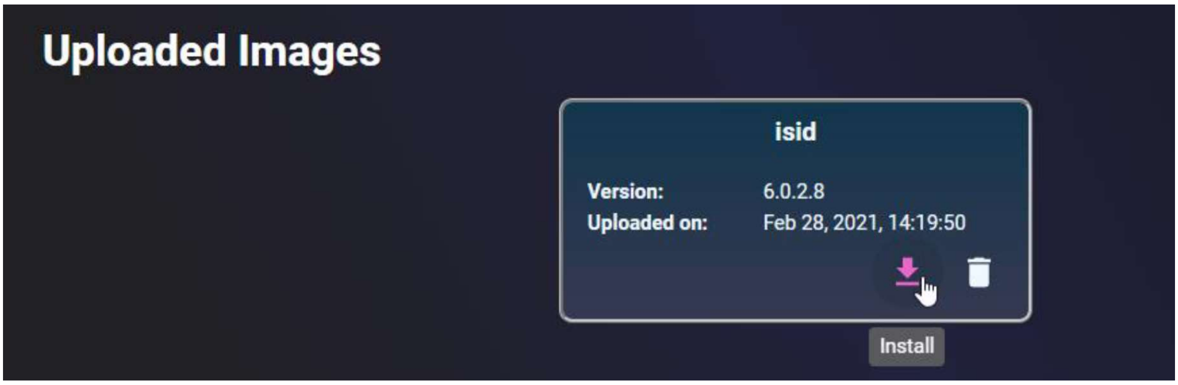
Progress: 14467236 KB of 16923287 KB

6. Once uploaded, the image can be found under Uploaded Images (middle section of the RIM page).
7. You are now ready to install the uploaded image.

Install an uploaded image

To install an uploaded image:

1. Access the RIM UI.
2. Locate the image under Uploaded Images (middle section of the RIM page):



Uploaded Images

isid

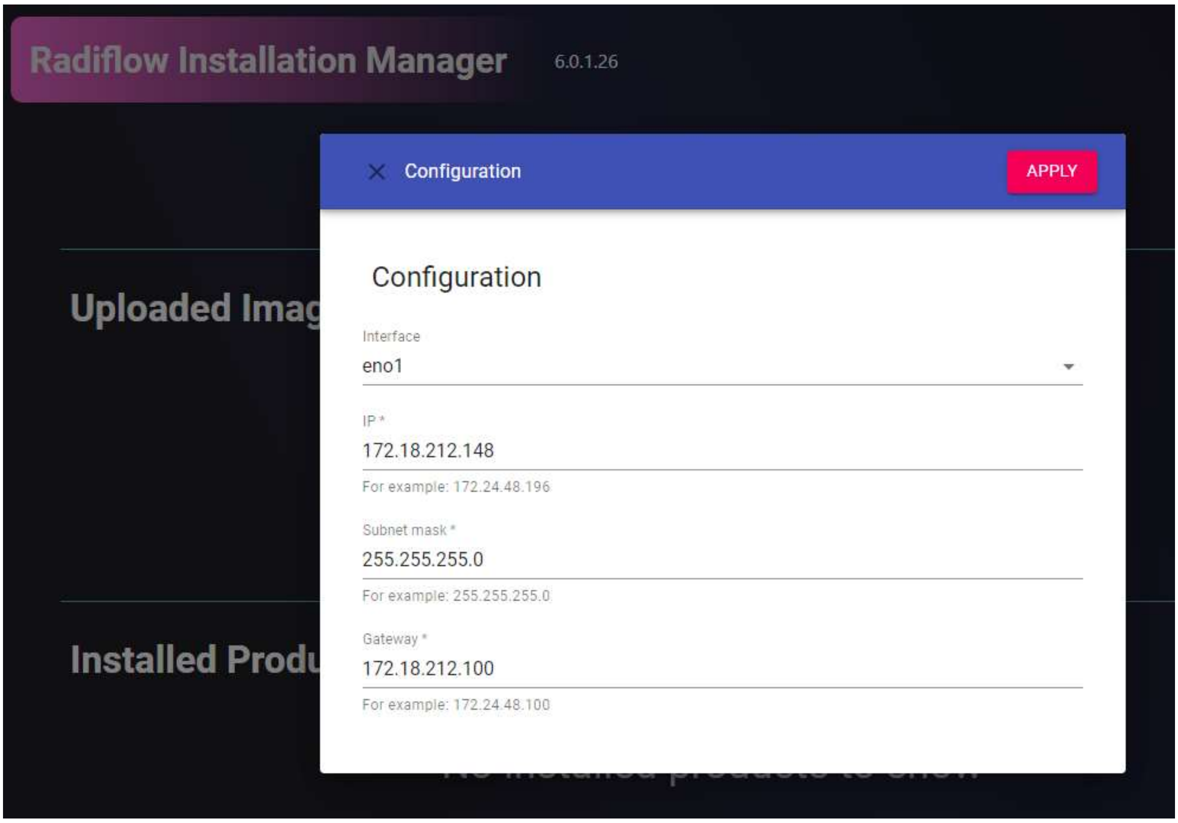
Version: 6.0.2.8
Uploaded on: Feb 28, 2021, 14:19:50

3. Click on the install icon (bottom, right) and confirm.

Note: if the image has already been installed, the install icon will be disabled.

4. In the Configuration pop-up, fill in the physical interface details for the server:

1. Name (e.g. eth0)
2. IP address
3. Subnet mask
4. Default gateway



Configuration

Interface
eno1

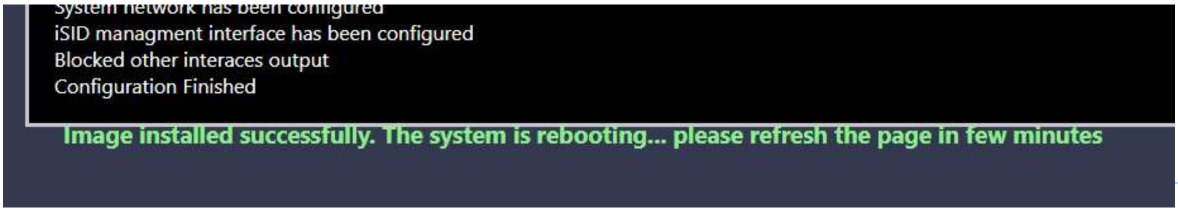
IP *
172.18.212.148
For example: 172.24.48.196

Subnet mask *
255.255.255.0
For example: 255.255.255.0

Gateway *
172.18.212.100
For example: 172.24.48.100

5. Click Apply (top, right) and confirm.

6. A Product Installation window displays, with line-by-line console output for the installation:



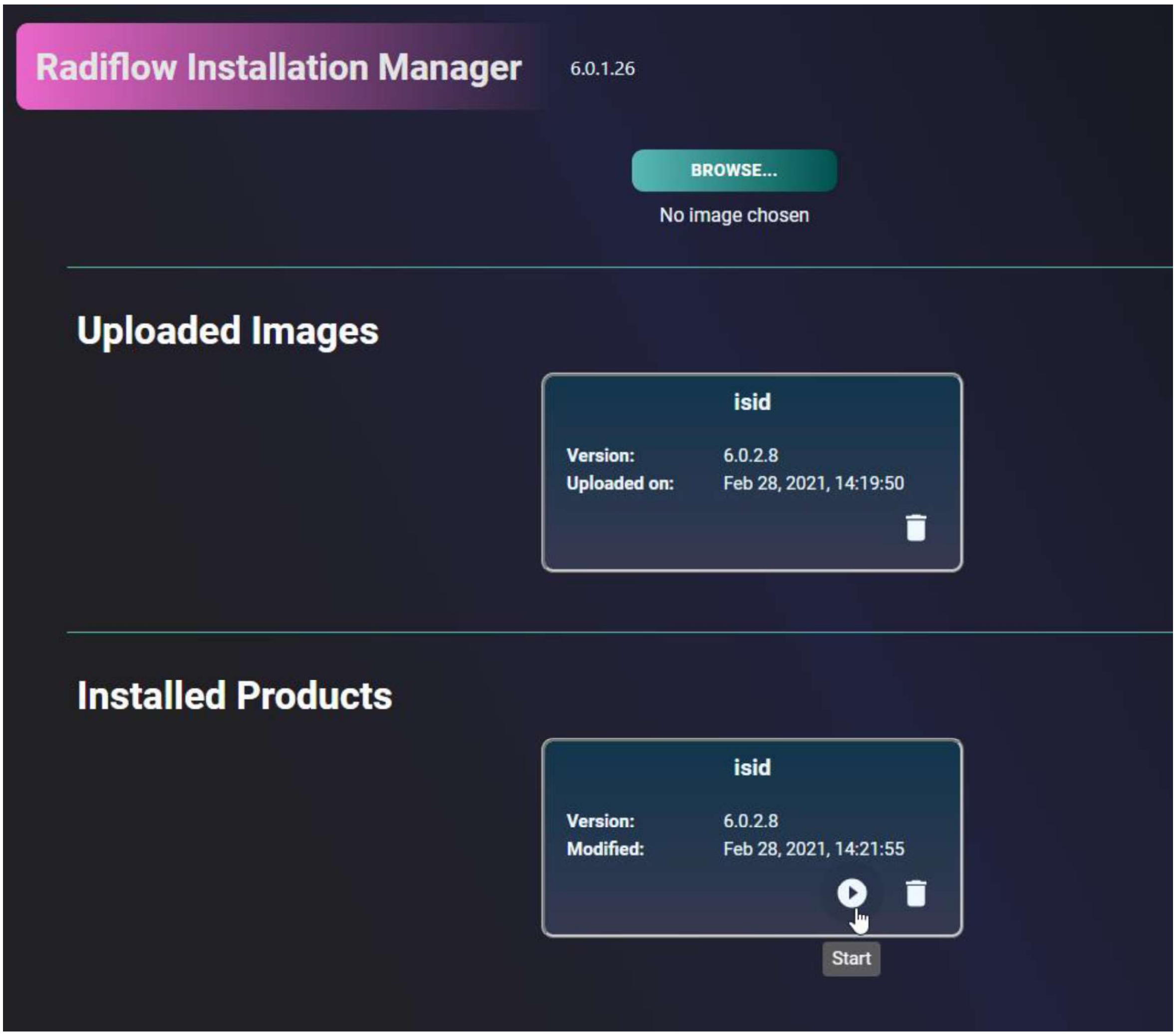
```
System network has been configured
iSID managment interface has been configured
Blocked other interaces output
Configuration Finished
Image installed successfully. The system is rebooting... please refresh the page in few minutes
```

8. The installed image now displays under Installed Products (bottom section of the RIM page).
9. You are now ready to run your installed image.

Run an installed image

1. Access the RIM UI.
2. Locate the relevant image under Installed Products (bottom section of the RIM page).
3. Click the Start icon ▶ (bottom, right) to start the installed product:

Note: if the image is already running, the Start icon ▶ will be disabled.



Radiflow Installation Manager 6.0.1.26

No image chosen

Uploaded Images

isid

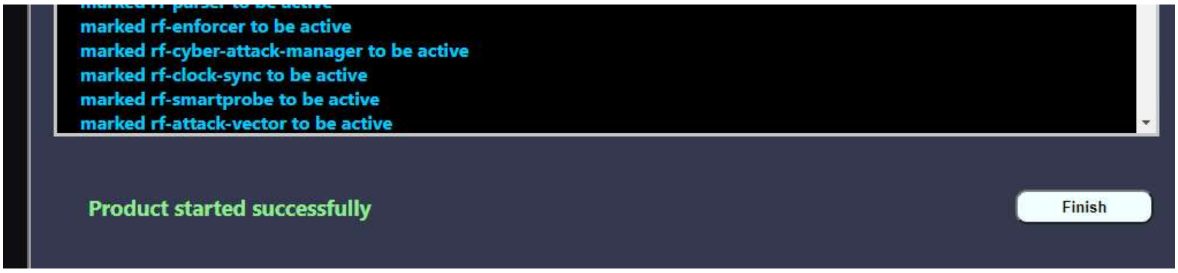
Version: 6.0.2.8
Uploaded on: Feb 28, 2021, 14:19:50

Installed Products

isid

Version: 6.0.2.8
Modified: Feb 28, 2021, 14:21:55

4. A Product Startup window displays, with line-by-line console output for the startup:



```
marked rf-parser to be active
marked rf-enforcer to be active
marked rf-cyber-attack-manager to be active
marked rf-clock-sync to be active
marked rf-smartprobe to be active
marked rf-attack-vector to be active
```

Product started successfully

5. Once the startup completes, click Finish (bottom, right).

Note: the Finish button will only display once the startup is complete.

6. Your image is now installed and running! Test the installation by opening a Chrome browser and navigating to:

https://<Server IP>/isid

Or (if the installed product was iCEN):

https://<Server IP>/icen

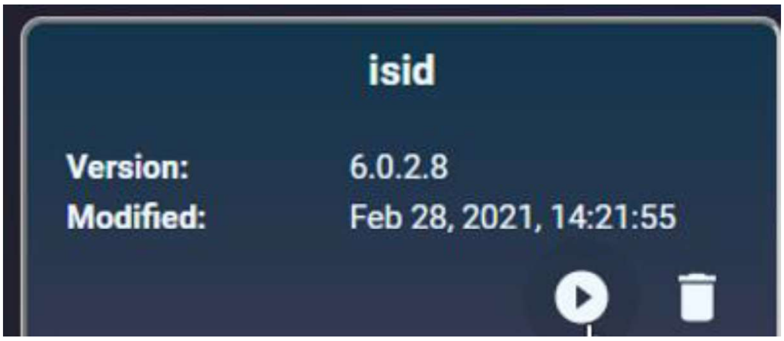
Remove an uploaded image

1. Access the RIM UI.
2. Locate the relevant image under Uploaded Images (middle section of the page).
3. Click the Remove 🗑 icon (bottom, right) to remove the uploaded image:

Uninstall an installed image

Warning: before uninstalling an image, make sure that everyone in the team is aware of the pending downtime, etc.

1. Access the RIM UI.
2. Locate the relevant image under Installed Products (bottom section of the page).
3. Click the Uninstall 🗑 icon (bottom, right) and confirm:



isid

Version: 6.0.2.8
Modified: Feb 28, 2021, 14:21:55

Access

Radiflow iSID is operated and managed via a web browser-based application.

Requirements:

- Google Chrome browser
- Computer with at least one active network interface, with an assigned IP address

Log in

1. Open Google Chrome and navigate to: https://A.B.C.D/

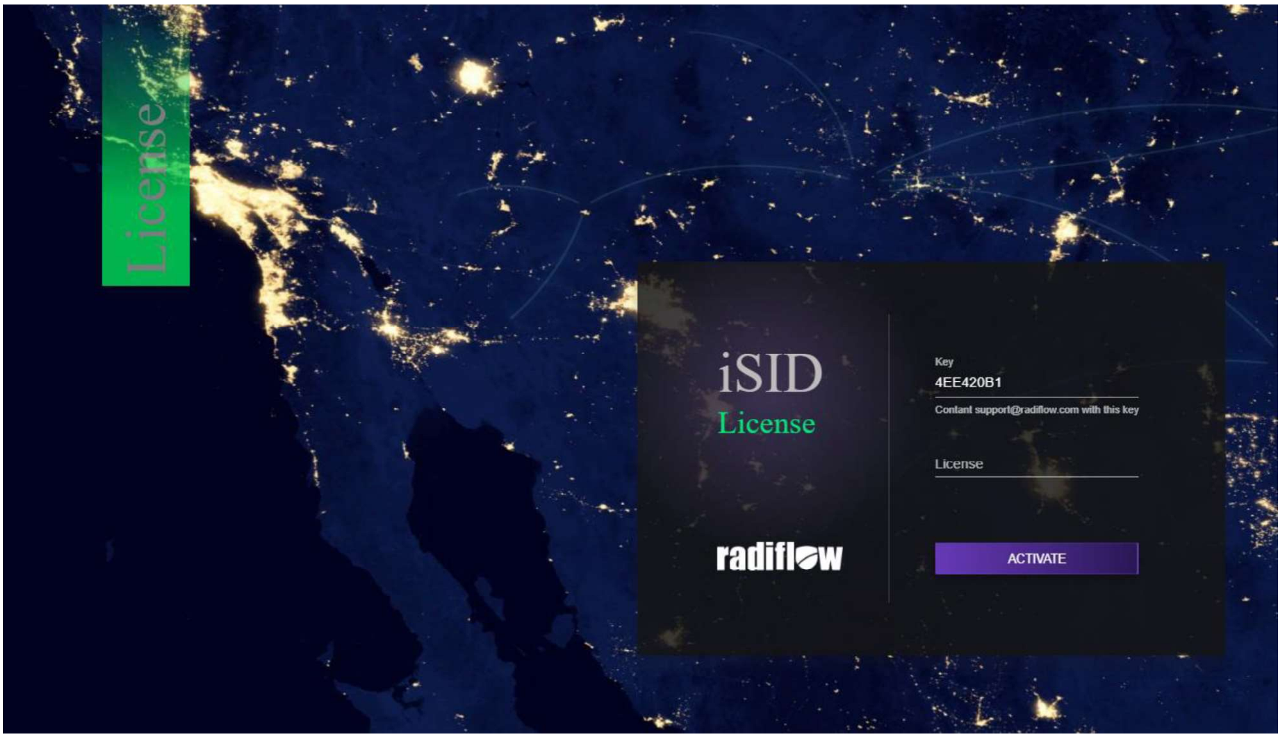
(where A.B.C.D represents the Management IPv4 Address defined during the server installation).

Note: You can change the management IP address in Configuration.

The login dialog box opens.

2. Enter your login credentials:

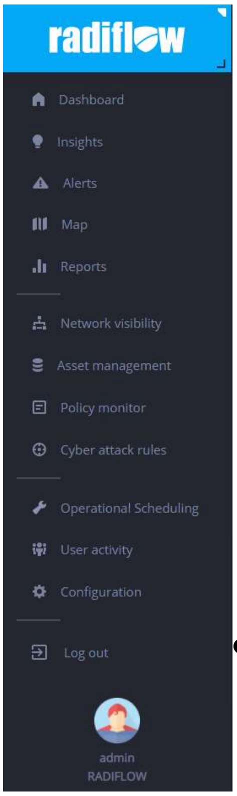
   - User name: Radiflow
   - Password: ******* (please contact Radiflow)



Key
4EE420B1
Contant support@radiflow.com with this key

Log out

In the sidebar, click Log out.



Click Log out to exit Radiflow iSID web application

Configure

There are a few basic configuration steps that are required before running Radiflow iSID.
Go to Configuration and define the following:

- Syslog server
- Timeout interval
- Protocols
- Interfaces
- Cyber attack rules

When all the physical connections are set and the basic configurations have been defined, Radiflow iSID is ready to start learning the network behavior.

Set system to Learning mode

In the Dashboard, set the system Learning mode (see Change the mode of operation).
After a few moments of processing, iSID starts displaying the learned network behavior:

- Dashboard offers a quick visual and graphical indication representing the learned network.
- Map dynamically updates and shows a visual indication of the devices and the logical connections between them
- Textual and visual indications of the learned data collected from the various security packages is displayed in the corresponding security package windows of the web application.

The extent of the network Learning Stage will provide a good and comprehensive knowledge which will lead for better results and analysis of the network.

Radiflow recommends allocating one full week for Learning mode.
Once you are confident that all entities have been learned by the system, it is recommended to transition iSID to Detection mode to start looking for suspicious behaviors.

The Basics

Learn about the icons and how to perform basic tasks in Radiflow iSID web application.

Change the View

Expand or collapse the sidebar, and choose how many items to view per a page.

Expand and collapse the sidebar

In the sidebar, click the Radiflow logo to expand or collapse the sidebar.

Choose how many items to view per page

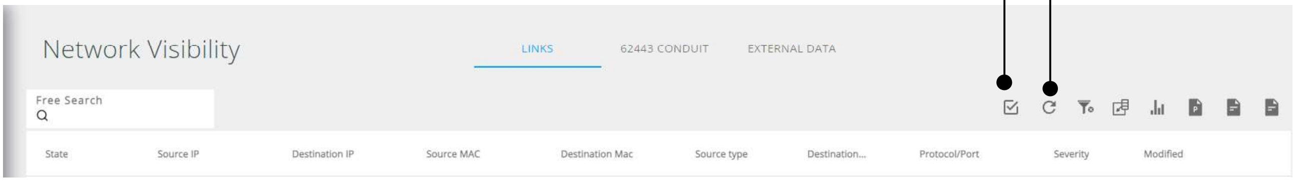
In many windows and panes, there is an option to change the number of items that can be viewed per page.

Manage Items

Select all items in a list and refresh the list.

Click Refresh icon to update items in list

Click Select All to select all items



Select/Deselect all items

To select or deselect all items in a list, do one of the following:

- Click Select All/Clear Filter

Refresh items in a list

Click the Refresh icon.

Change the Column Appearance

In most panes and windows in the Radiflow iSID web application, you can change the order items are displayed in each column, from ascending to descending, and vice-versa. In addition, it is possible to show/hide specific columns.

Change the column order

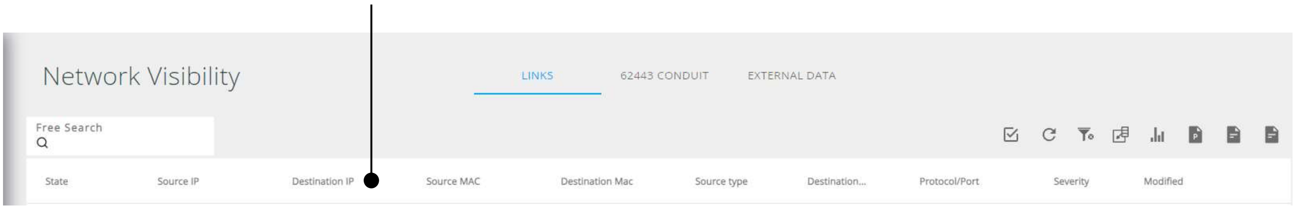
1. Click the title name of a column. An arrow and a number appear next to the title.

When you click an additional column, the numbers of the column change incrementally.

2. Click the arrow to reverse the order the items are displayed (from ascending to descending).

Click the arrow again to display the items in their previous order.

Click arrow to change list order from ascending to descending, and vice-versa

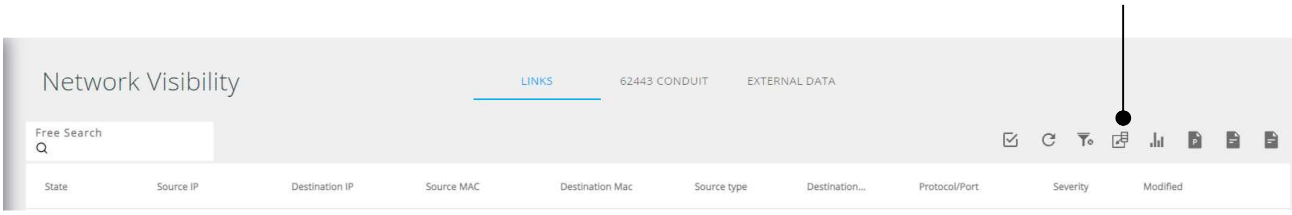


Show or hide a column

In most panes and windows, you can show or hide specific columns.

1. Click the "Column Visibility" button. The Columns to Display pop-up window opens.
2. In the Columns to Display pop-up window do the following:
   - Select the columns you wish to display
   - Unselect the columns you wish to hide

Column Visibility



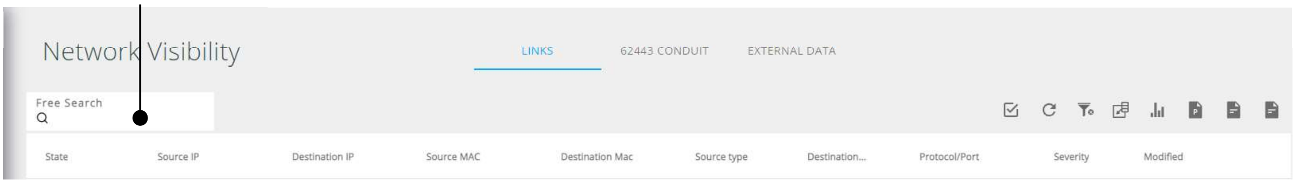
Search Tools

Use the search tools and custom-built filter lists to quickly locate items in Radiflow iSID web application.

Search for specific items

1. Use the Search Field to specify search parameters and strings.

Search box



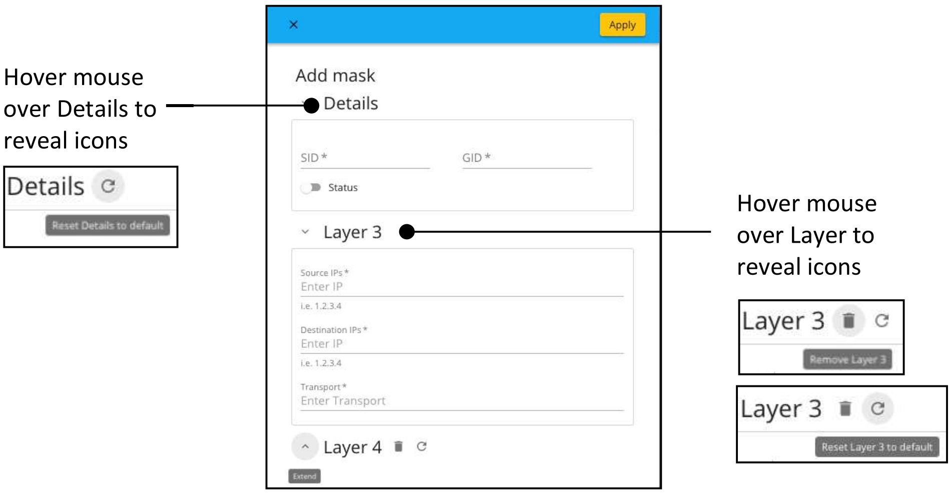
Edit Items

When editing items in Radiflow iSID web application, you can quickly reset edited details or layers to their default settings and remove layers entirely.

Reset details to their default settings

When editing details, undo the edits and restore the default settings.

1. In an edit window, hover the mouse over the word “Details”. The Reset Details to default icon appears.
2. Click the icon to reset the default settings.


Hover mouse over Details to reveal icons

Hover mouse over Layer to reveal icons

Reset layers to their default settings

When editing layers, undo the edits and restore the layer’s default settings.

1. In the edit window/pane, hover the mouse over the word “Layer”. The Reset Layer to default icon appears.
2. Click the icon to reset the layer to its default settings.

Remove a layer

When editing layers, you can remove a layer entirely. The layer will no longer show up in searches or lists.

1. In the edit window/pane, hover the mouse over the word “Layer”. The Remove Layer icon appears.

Click the icon to remove the layer.

Dashboard

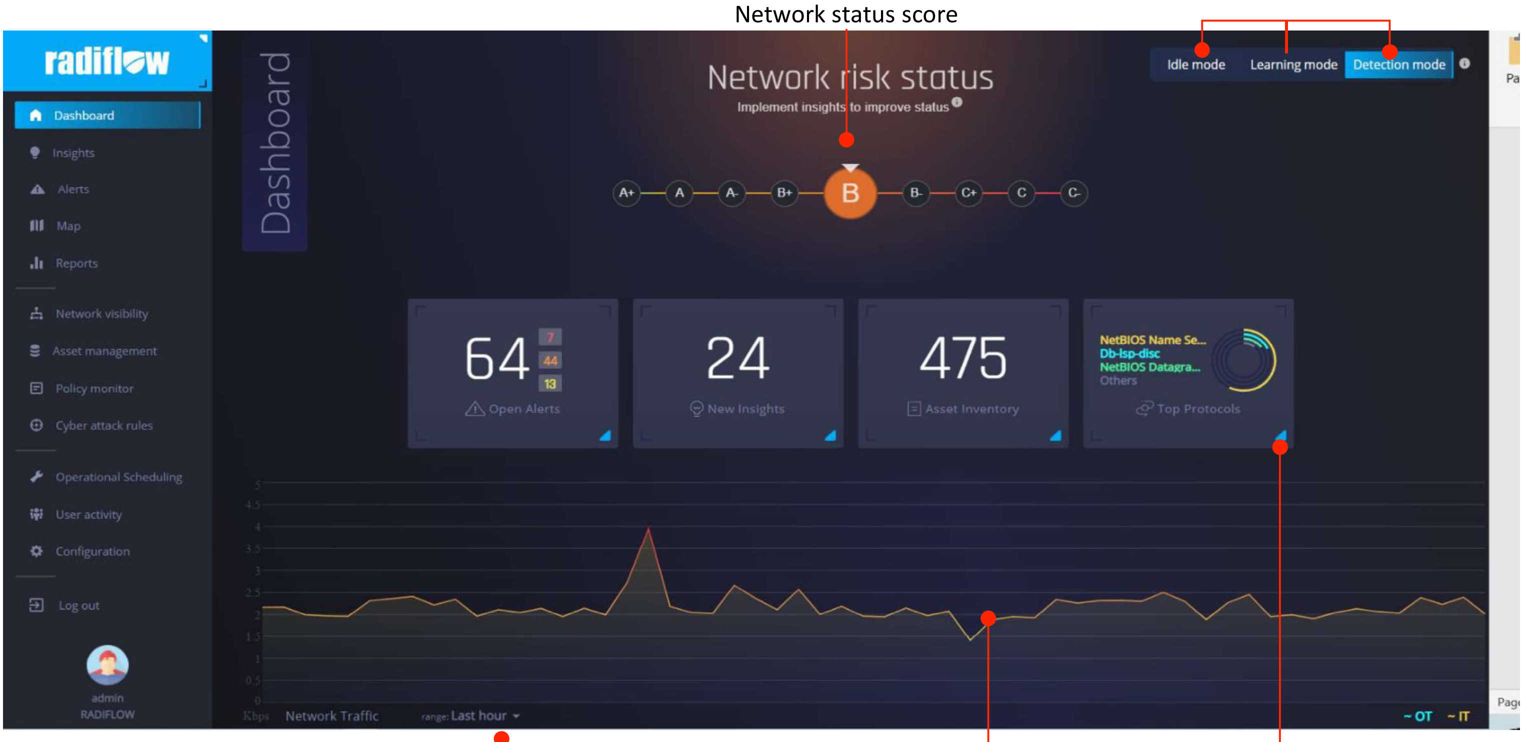
When you access the Radiflow iSID web application, the dashboard opens by default, displaying a status snapshot of the network.

View network information at a glance

1. In the sidebar, click Dashboard.

View and select

Network status score



Select network traffic timeframe

Expand dashboard widget

Link to network details

2. View the following information at a glance:

- Network status The network status is prominently displayed as a letter in the top center of the dashboard
- Network status View the network traffic during a specific timeframe (previous hour, previous day, previous month)
- Open alerts
  - View the number of open alerts during a specific timeframe
  - Expand the widget to view a list of all the open alerts
  - Click View all to leave the Dashboard and view all open alerts
- New Insights
  - View the number of new insights
  - Expand the New insights widget to view a list of all the new insights
- Inventory Assets
  - View the number of inventory assets
  - Expand the widget to view a list of all the devices types
  - Click View to view more information about the devices on the network
- Links
  - View information about the network links
  - Expand the widget to view more information about the links
  - Click View to view more detailed information about the links on the network

Change the mode of operation

The Radiflow iSID can operate in three different modes. The modes can be changed at any time.

1. In the sidebar, click Dashboard.
2. Select one of the following modes:

- Idle mode:

  Radiflow iSID remain passive, allowing the user to define configuration parameters and review existing data

- Learning mode:

  Radiflow iSID collects network information, which is used to build a complete network and industrial communication model. The network topology is presented as a graphical map allowing the investigation of processes and gaining an understanding of the network’s inner workings (see Map).

- Detection mode:

  At the conclusion of the learning stage, moves Radiflow iSID into Detection mode. In this mode, Radiflow iSID provides constant network monitoring based on the data gathered and analyzed during the Learning mode. In Detection mode Radiflow iSID uses analytical engines to detect unauthorized traffic or cyber threats on the SCADA network.

3. Click OK to confirm the mode change.

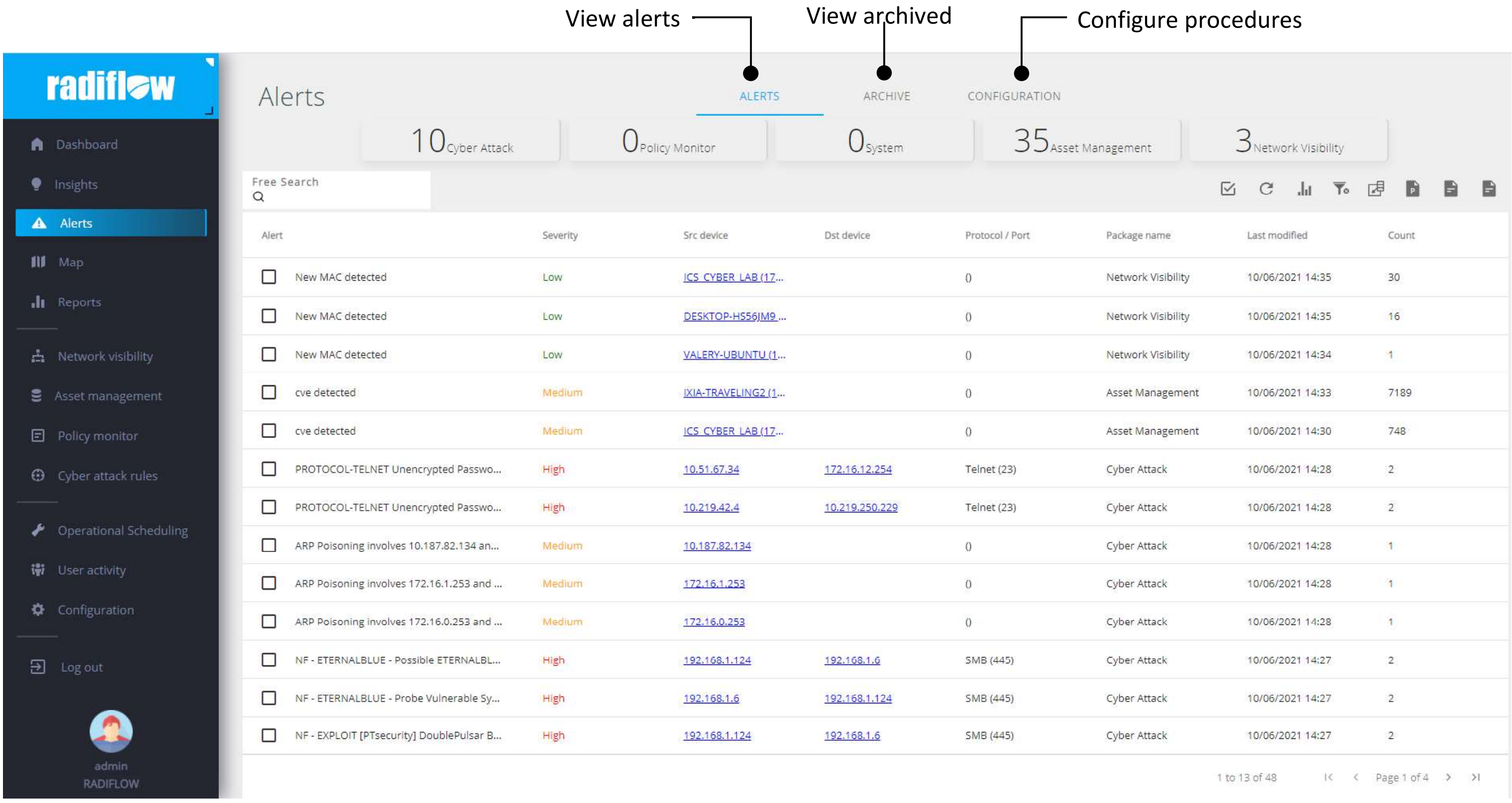
Alerts

In Detection mode, whenever Radiflow iSID identifies a threat or a risk, it will be registered as an alert in Alerts.

Each alert is accompanied by an indicative message with a description of the violation, arranged in a dynamic table. When configured, Radiflow iSID also sends Syslog messages with the same data to a predefined Syslog server.

Access Alerts to do the following:

- View current alerts and archived alerts
- Manage alerts
- Configure procedures



Alerts

10 Cyber Attack | 0 Policy Monitor | 0 System | 35 Asset Management | 3 Network Visibility

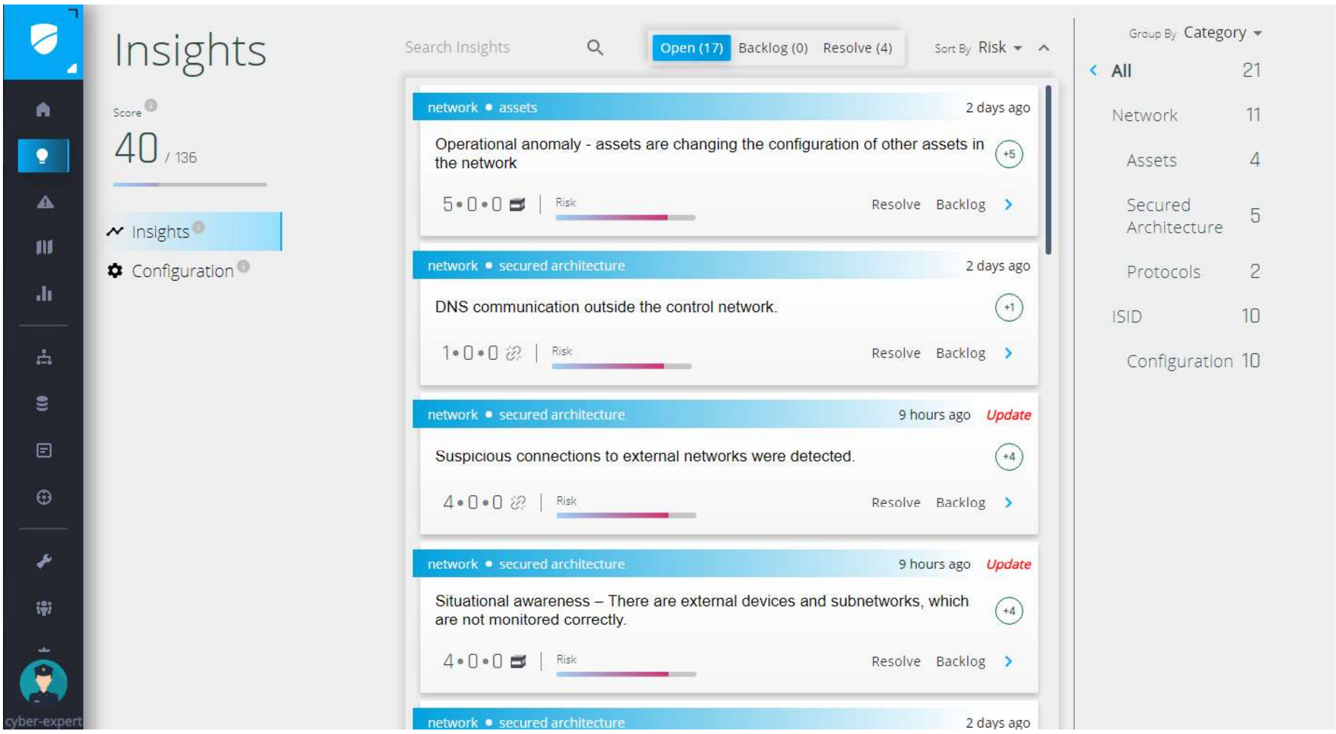
	Alert	Severity	Src device	Dst device	Protocol / Port	Package name	Last modified	Count
☐	New MAC detected	Low	ICS_CYBER_LAB (17...		()	Network Visibility	10/06/2021 14:35	30
☐	New MAC detected	Low	DESKTOP-HS56JM9 ...		()	Network Visibility	10/06/2021 14:35	16
☐	New MAC detected	Low	VALERY-UBUNTU (1...		()	Network Visibility	10/06/2021 14:34	1
☐	cve detected	Medium	IXIA-TRAVELING2 (1...		()	Asset Management	10/06/2021 14:33	7189
☐	cve detected	Medium	ICS_CYBER_LAB (17...		()	Asset Management	10/06/2021 14:30	748
☐	PROTOCOL-TELNET Unencrypted Passwo...	High	10.51.67.34	172.16.12.254	Telnet (23)	Cyber Attack	10/06/2021 14:28	2
☐	PROTOCOL-TELNET Unencrypted Passwo...	High	10.219.42.4	10.219.250.229	Telnet (23)	Cyber Attack	10/06/2021 14:28	2
☐	ARP Poisoning involves 10.187.82.134 an...	Medium	10.187.82.134		()	Cyber Attack	10/06/2021 14:28	1
☐	ARP Poisoning involves 172.16.1.253 and ...	Medium	172.16.1.253		()	Cyber Attack	10/06/2021 14:28	1
☐	ARP Poisoning involves 172.16.0.253 and ...	Medium	172.16.0.253		()	Cyber Attack	10/06/2021 14:28	1
☐	NF - ETERNALBLUE - Possible ETERNALBL...	High	192.168.1.124	192.168.1.6	SMB (445)	Cyber Attack	10/06/2021 14:27	2
☐	NF - ETERNALBLUE - Probe Vulnerable Sy...	High	192.168.1.6	192.168.1.124	SMB (445)	Cyber Attack	10/06/2021 14:27	2
☐	NF - EXPLOIT [PTsecurity] DoublePulsar B...	High	192.168.1.124	192.168.1.6	SMB (445)	Cyber Attack	10/06/2021 14:27	2

1 to 13 of 48 |< < Page 1 of 4 > >|

Insights

Overview

The Insights module provides a dynamic list of actionable insights to help tighten your OT security. Once you address a specific insight (as per the guidelines on the card), you can return and mark the card as resolved. If iSID is capable of detecting a successful resolution, it will mark the card as resolved without user interaction; in that case, the 'Resolve' option will not be display for that card:



Operational anomaly - assets are changing the configuration of other assets in the network

DNS communication outside the control network.

Suspicious connections to external networks were detected.

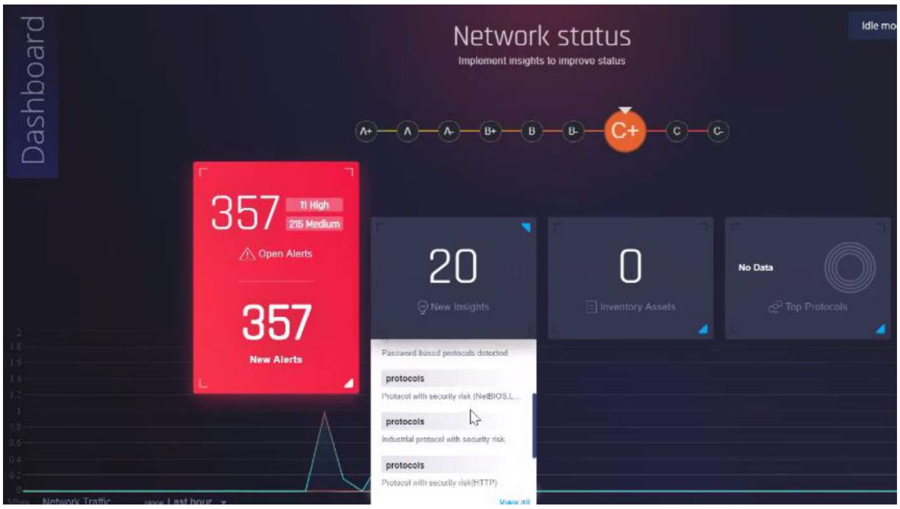
Situational awareness – There are external devices and subnetworks, which are not monitored correctly.

Access

You can access the Insights module via the following locations:

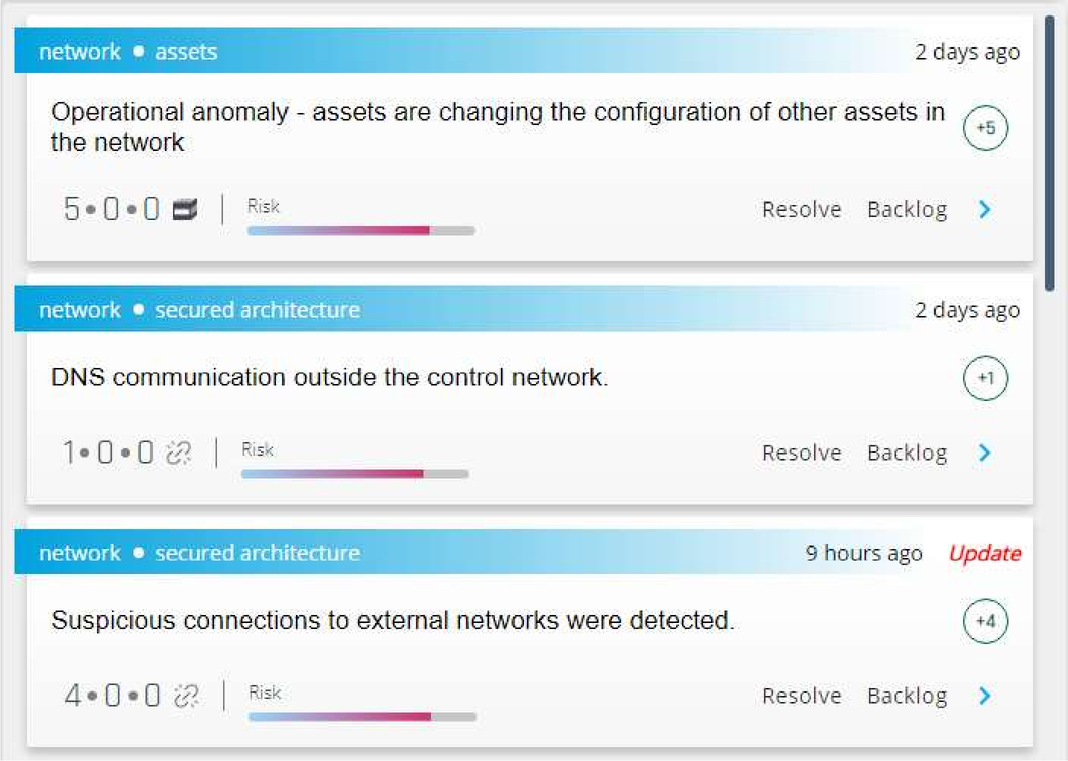
a) The Insights 💡 icon (top, left) on the vertical toolbar (left).

b) The summary box (center, left) in the Dashboard view:



List view

Insights are displayed as a list of cards:



network • assets 2 days ago

Operational anomaly - assets are changing the configuration of other assets in the network

+5

5•0•0 | Risk Resolve Backlog

network • secured architecture 2 days ago

DNS communication outside the control network.

+1

1•0•0 | Risk Resolve Backlog

network • secured architecture 9 hours ago *Update*

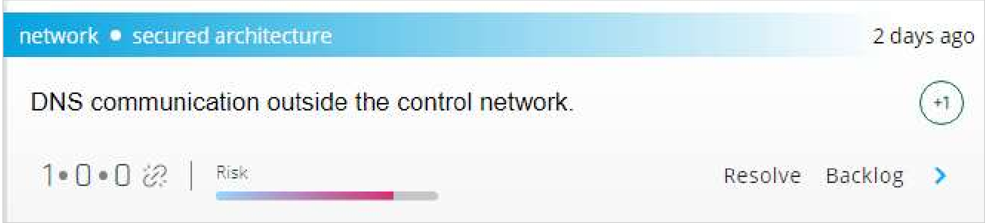
Suspicious connections to external networks were detected.

+4

4•0•0 | Risk Resolve Backlog

Card layout

Each card the in the list view has the following layout:

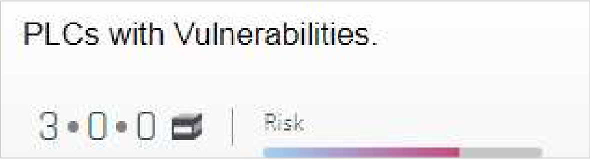


network • secured architecture 2 days ago

DNS communication outside the control network.

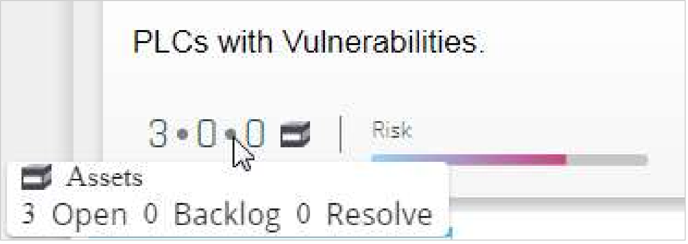
On the left (moving from top to bottom):

- Header - the insight type (e.g. ‘network’ or ‘configuration’) and sub-type (e.g. ‘assets’.)
- Summary - a short summary of the issue - e.g. “Assets with high exploitability.”
- Element's count - the number of elements (network devices or network links) that triggered this insight. (Each time a network element triggers the insight, it is added to the card.) The count stats are grouped according to status:



PLCs with Vulnerabilities.

For a more verbose display, mouse over the count stats:



PLCs with Vulnerabilities.

Assets
3 Open 0 Backlog 0 Resolve

- Risk level - the calculated risk for this incident.

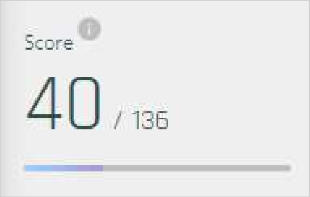
On the right (moving from top to bottom):

- Date-time stamp - the date-time that the card was created.

Note: Cards that were created with the last 24 hours show a New label. Cards that were updated (after creation) show an Updated label.

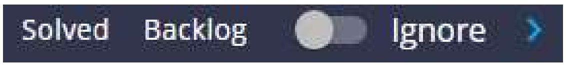
- Insight weight +7 - the overall weight assigned to the insight, based on the number of affected network elements and the insight type.

Note: the score counter (top, left) updates according to the insight weight (see previous section):


Score

40 / 136

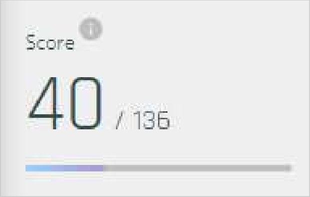
- Action bar - Resolve (or re-open) a card, Move card to backlog, etc.:



Score counter

Each card is assigned a certain weight or score. As you resolve insights, your score increases accordingly.

Use the Score counter (top, left) to track your score progress. In the example below, 10 points have been awarded thus far - but a total of 154 can be earned.


Score

40 / 136

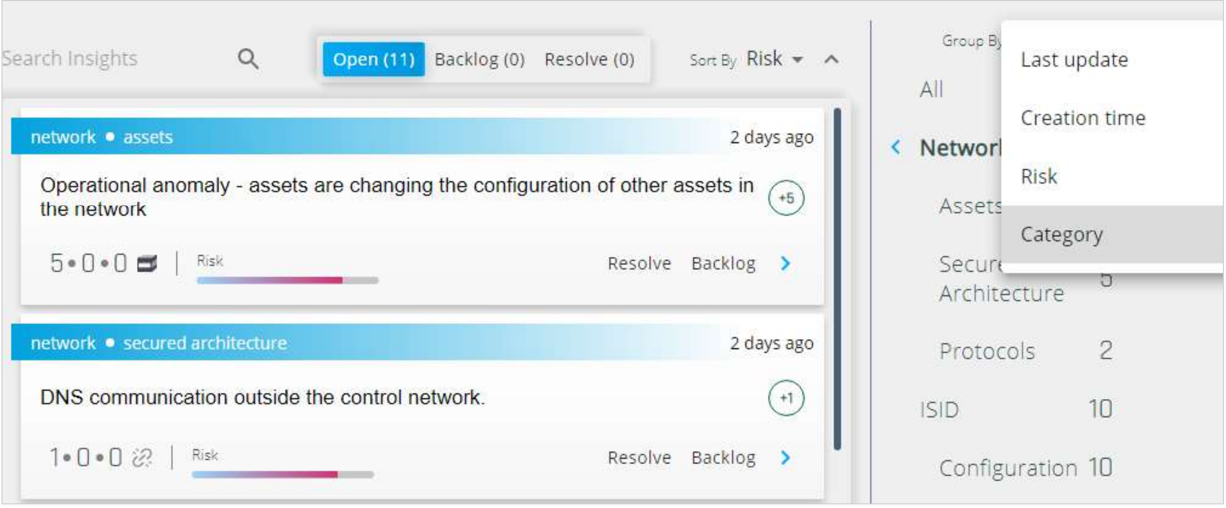
A high score ratio indicates that you are taking action on insights in a timely manner - and that your overall, insight-based security is healthy.

Change the view

Group by

To view the Insights by group, in the right side of the pane, select the parameter to group by.

You can then select a specific group to view.



network • assets 2 days ago

Operational anomaly - assets are changing the configuration of other assets in the network

5•0•0 | Risk Resolve Backlog

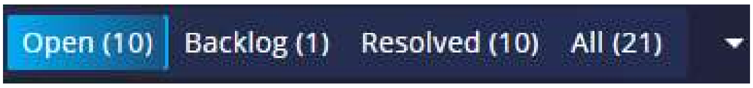
network • secured architecture 2 days ago

DNS communication outside the control network.

1•0•0 | Risk Resolve Backlog

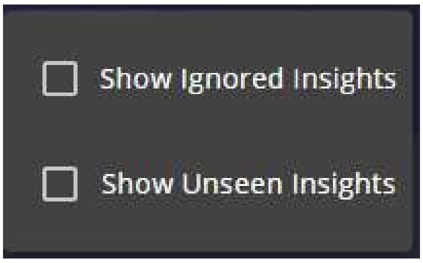
Status filters

To view a subset of insights, use the status filters (top, left):



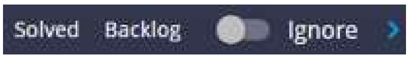
Additional status filters

Use the More ▾ icon to show/hide additional status filters: Ignored and Unseen:



Ignored insights

You can instruct the system to ignore a given insight, using the Ignore toggle switch (bottom, right of card):



Ignored insights are hidden by default, but can be viewed under the Ignored Insights tab.

Note: if you toggle off the ignored status, the insight will show again.

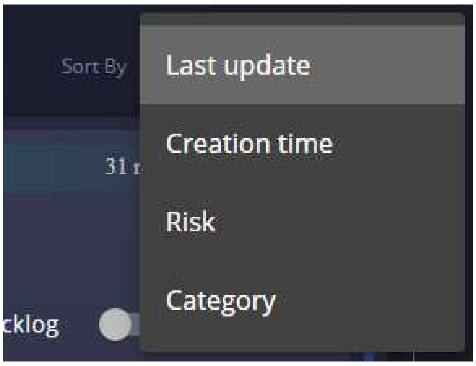
Unseen insights

An unseen insight is an insight that has not been triggered yet by any network element.

Unseen insights are hidden by default, but can be viewed under the Unseen Insights tab.

Sort by column

1. To sort on a given column, use the Sort by dropdown (top, right):



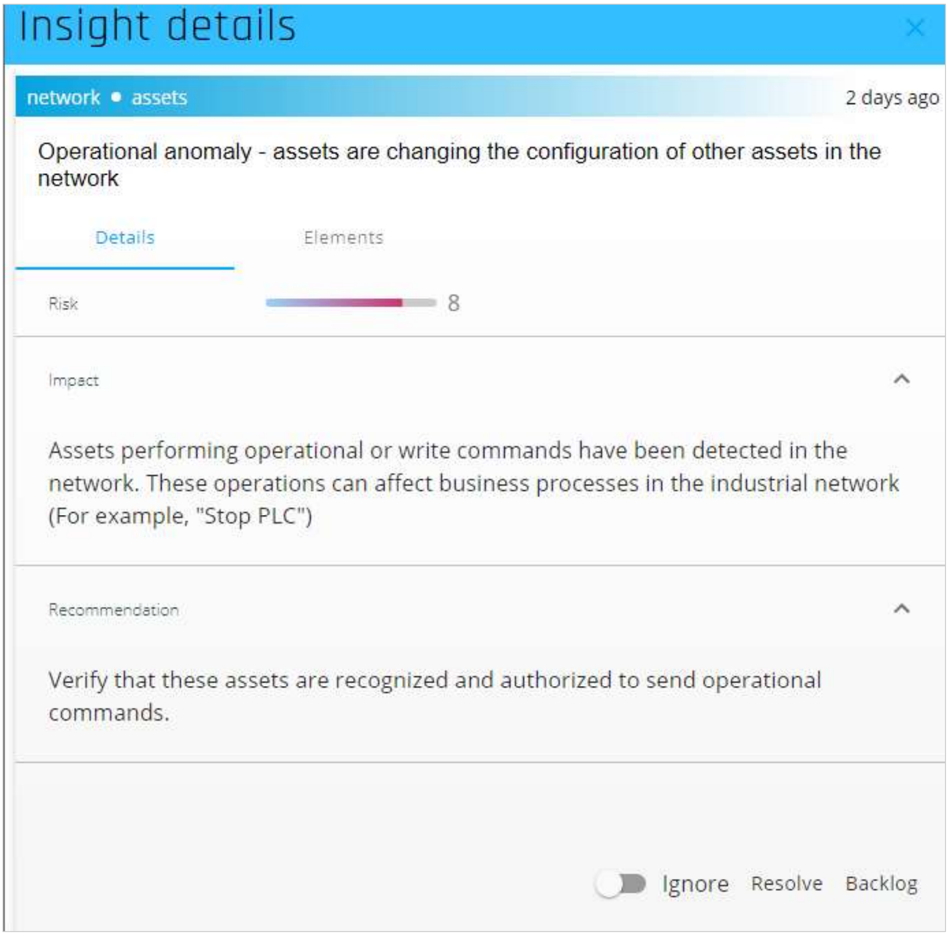
2. To toggle the sort order (ascending or descending), click the arrow ▾ icon (far right):

View card details

To view card details, do either 1 of the following:

1. Click on the card summary line (e.g. “Assets with high exploitability.”)
2. Or - click the View more › icon (bottom, right).

Tab 1: Details



Insight details

network • assets 2 days ago

Operational anomaly - assets are changing the configuration of other assets in the network

Details Elements

Risk 8

Impact

Assets performing operational or write commands have been detected in the network. These operations can affect business processes in the industrial network (For example, "Stop PLC")

Recommendation

Verify that these assets are recognized and authorized to send operational commands.

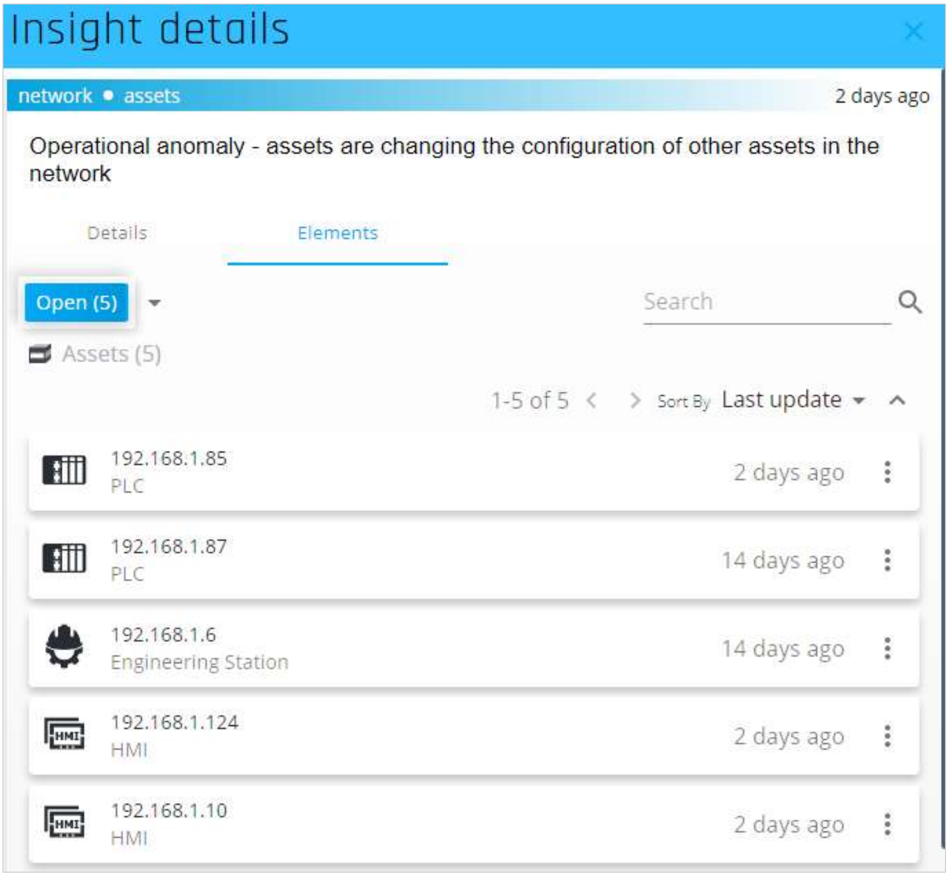
The Details tab provides the following sections:

- Risk level - the estimated risk for this incident.
- Impact - a general description of the security guideline and the motivation behind it
- Recommendation - the recommended action to take
- Authority - the authority that issued the guideline e.g. Nist. This heading is followed by 2 sub-sections:
- Quote - a snippet from the relevant specification document

- Link - a hyperlink to the above document (if available)
- Actions – you can ignore, resolve, or pass the insight to backlog

Tab 2: Elements

The Elements tab displays a list of all network elements that are affected by this actionable insight:



Insight details

network • assets 2 days ago

Operational anomaly - assets are changing the configuration of other assets in the network

192.168.1.85 PLC	2 days ago
192.168.1.87 PLC	14 days ago
192.168.1.6 Engineering Station	14 days ago
192.168.1.124 HMI	2 days ago
192.168.1.10 HMI	2 days ago

Note: the term element refers to a network device or network link

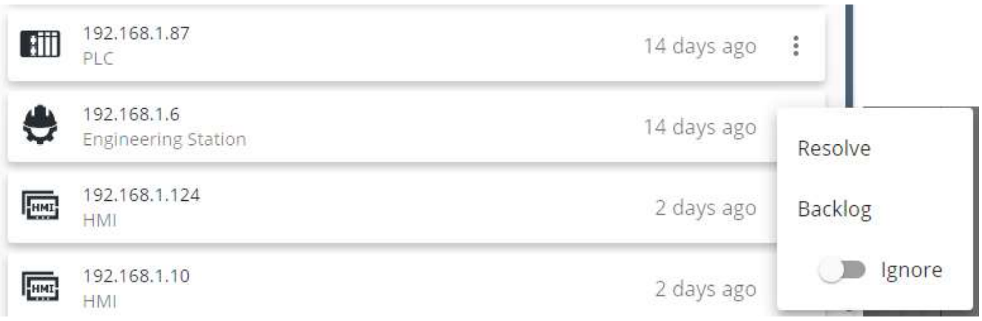
Change the view

To search for specific network elements, use the status filters (top, left), or the search box (top, right). (Note: additional status filters can be accessed via the arrow ▾ icon.)

To sort the list, use the Sort by dropdown (right) and Sort order ▴ icon (far right).

Action bar

To mark an individual network element as resolved (or move it to the backlog), click the menu button in the desired row. An action pop up displays:



192.168.1.87 PLC 14 days ago

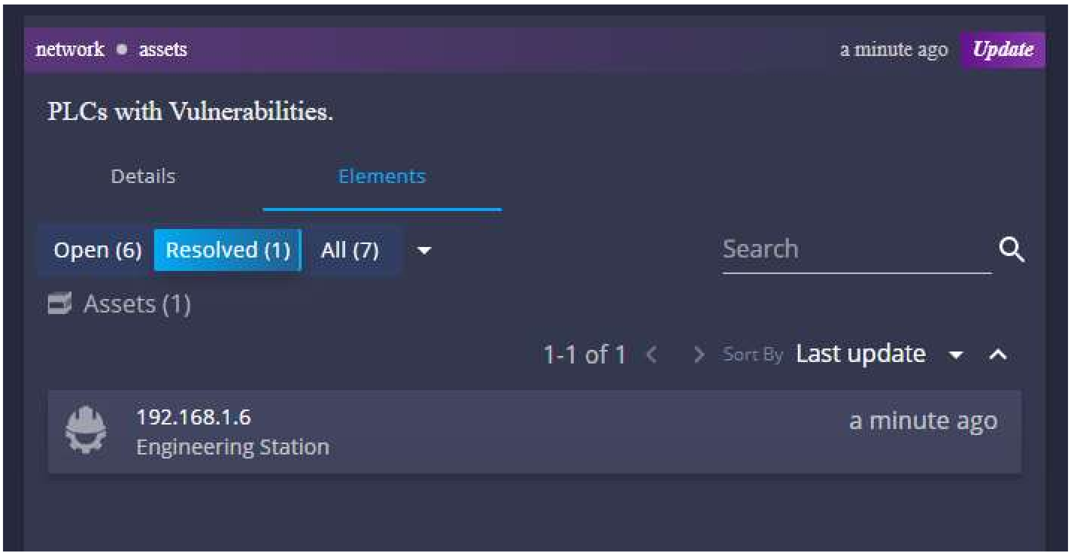
192.168.1.6 Engineering Station 14 days ago

192.168.1.124 HMI 2 days ago

192.168.1.10 HMI 2 days ago

Note:

Once you mark a network element within a card as resolved, it will display under the ‘Resolved’ category within that card (under the Elements tab):



network • assets a minute ago

PLCs with Vulnerabilities.

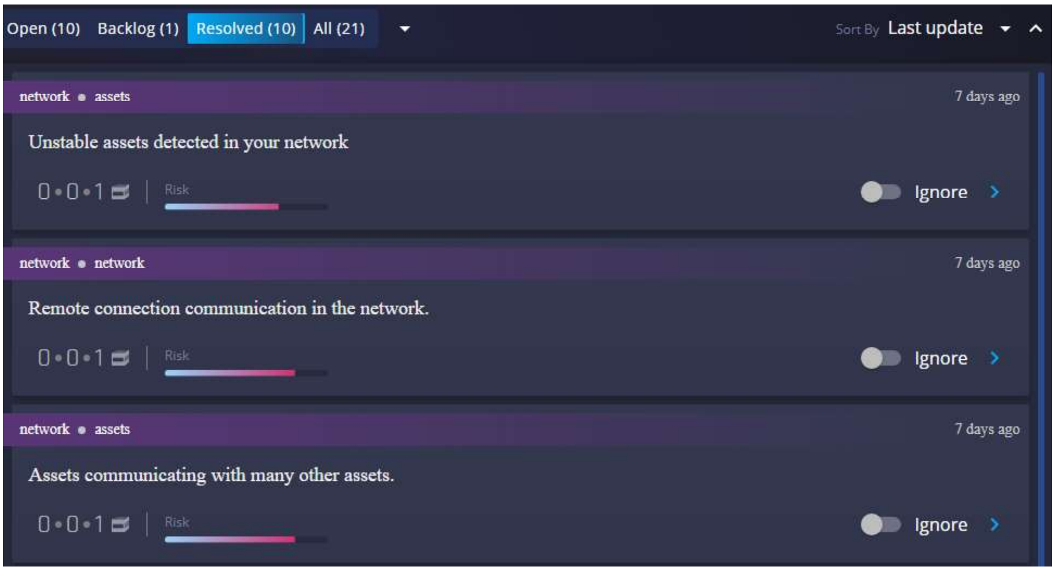
Open (6) Resolved (1) All (7)

Assets (1)

1-1 of 1 Sort By Last update

192.168.1.6 Engineering Station a minute ago

If all elements in the card have been marked as resolved, the card itself will be marked as resolved (and will appear under the ‘Resolved’ category in the card list view):



Open (10) Backlog (1) Resolved (10) All (21) Sort By Last update

network • assets 7 days ago

Unstable assets detected in your network

0 • 0 • 1 Risk Ignore

network • network 7 days ago

Remote connection communication in the network.

0 • 0 • 1 Risk Ignore

network • assets 7 days ago

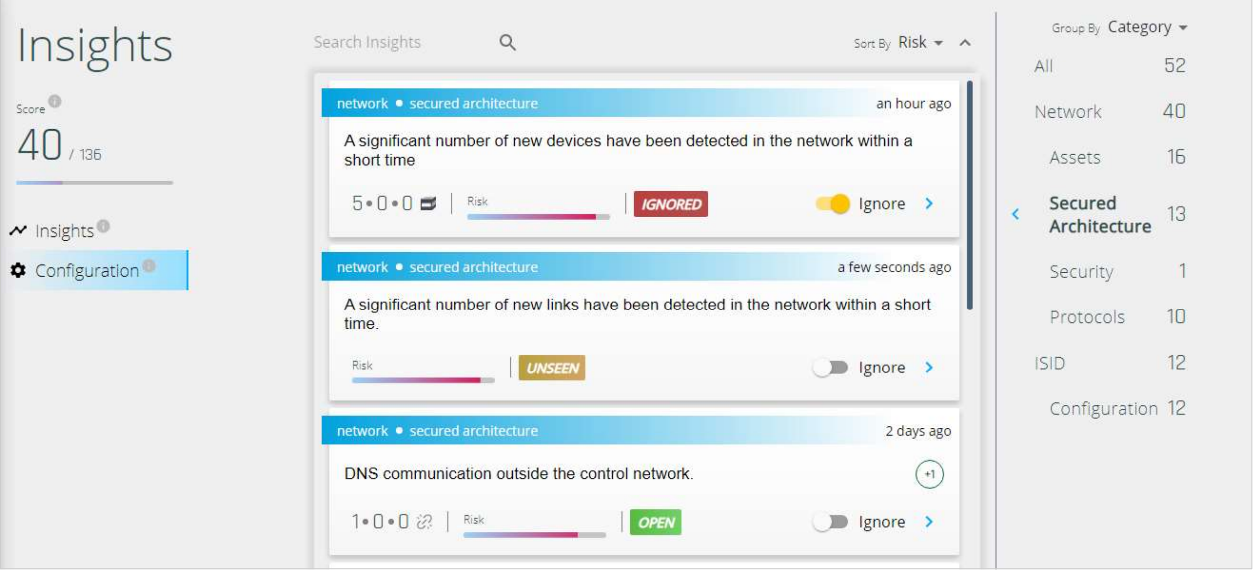
Assets communicating with many other assets.

0 • 0 • 1 Risk Ignore

Note: The same flow applies when moving network elements to the backlog.

Configuration

The Configuration tab lets you easily select the insights that should be ignored by iSID. It lists all defined insights, regardless of whether they are currently seen or not. It functions exactly the same as the Insights tab; you can search, sort, display in groups, and view details the same as in the Insights tab.



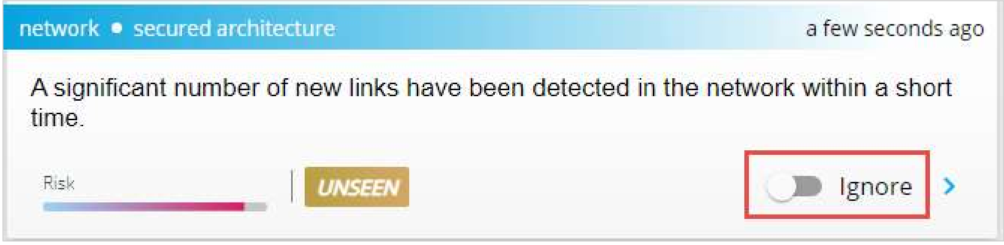
A significant number of new devices have been detected in the network within a short time

A significant number of new links have been detected in the network within a short time.

DNS communication outside the control network.

Ignore an insight

In the Configuration tab (Insights > Configuration) set the Ignore toggle button in the insight card to Ignore. This insight will no longer appear in the Insights tab.



A significant number of new links have been detected in the network within a short time.

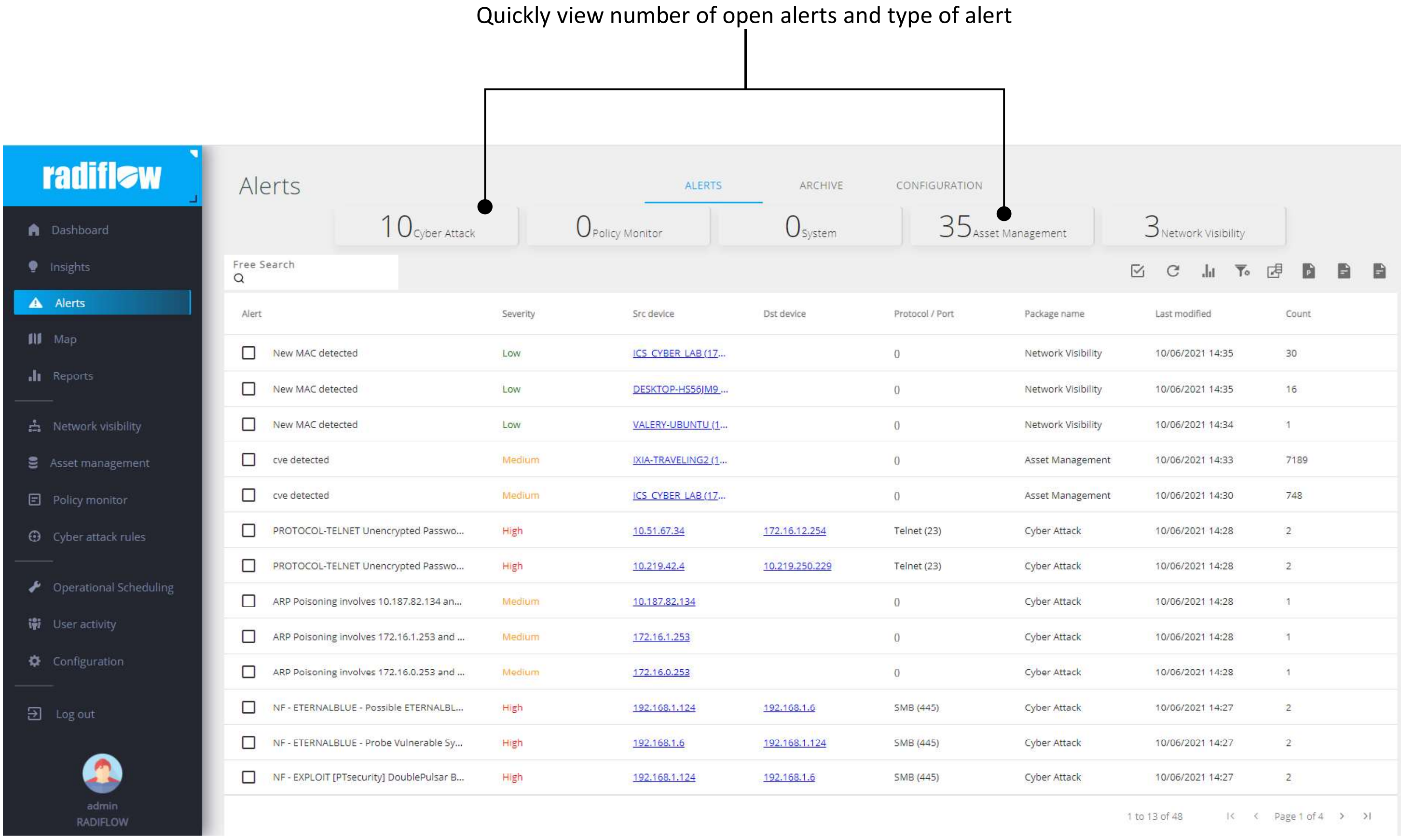
Alerts

View Alert Details

You can view general information or in-depth details about alerts and their root causes.

View general alert information

Select Alerts in the sidebar.
By default, the Alerts pane opens displaying general alert information, such as number of alerts, type of alert, severity, device IP address etc.



Quickly view number of open alerts and type of alert

	Alert	Severity	Src device	Dst device	Protocol / Port	Package name	Last modified	Count
☐	New MAC detected	Low	ICS_CYBER_LAB (17...		()	Network Visibility	10/06/2021 14:35	30
☐	New MAC detected	Low	DESKTOP-HS56JM9 ...		()	Network Visibility	10/06/2021 14:35	16
☐	New MAC detected	Low	VALERY-UBUNTU (1...		()	Network Visibility	10/06/2021 14:34	1
☐	cve detected	Medium	IXIA-TRAVELING2 (1...		()	Asset Management	10/06/2021 14:33	7189
☐	cve detected	Medium	ICS_CYBER_LAB (17...		()	Asset Management	10/06/2021 14:30	748
☐	PROTOCOL-TELNET Unencrypted Passwo...	High	10.51.67.34	172.16.12.254	Telnet (23)	Cyber Attack	10/06/2021 14:28	2
☐	PROTOCOL-TELNET Unencrypted Passwo...	High	10.219.42.4	10.219.250.229	Telnet (23)	Cyber Attack	10/06/2021 14:28	2
☐	ARP Poisoning involves 10.187.82.134 an...	Medium	10.187.82.134		()	Cyber Attack	10/06/2021 14:28	1
☐	ARP Poisoning involves 172.16.1.253 and ...	Medium	172.16.1.253		()	Cyber Attack	10/06/2021 14:28	1
☐	ARP Poisoning involves 172.16.0.253 and ...	Medium	172.16.0.253		()	Cyber Attack	10/06/2021 14:28	1
☐	NF - ETERNALBLUE - Possible ETERNALBL...	High	192.168.1.124	192.168.1.6	SMB (445)	Cyber Attack	10/06/2021 14:27	2
☐	NF - ETERNALBLUE - Probe Vulnerable Sy...	High	192.168.1.6	192.168.1.124	SMB (445)	Cyber Attack	10/06/2021 14:27	2
☐	NF - EXPLOIT [PTsecurity] DoublePulsar B...	High	192.168.1.124	192.168.1.6	SMB (445)	Cyber Attack	10/06/2021 14:27	2

In the Alerts pane you can do the following

- Choose to view alert details
- Choose to view the root cause of an alert
- Move an alert to archives
- Add an alert to baseline
- Search for alerts based on specific criteria
- Attach a procedure to an alert
- Display an alerts timestamp
- Download a traffic PCAP file

- Adjust the order the alerts are displayed
- Show and hide columns
- Choose how many alerts to view per page

View details about an alert

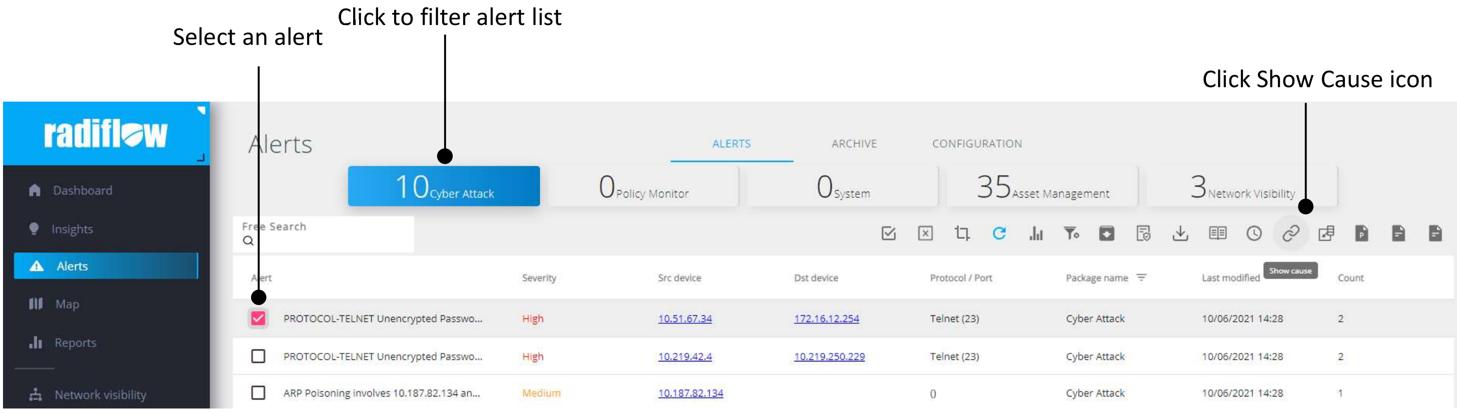
1. Go to Alerts or Archive (Alerts > Alerts/Archive).
2. Select the checkbox of the alert you wish to view details about. It is possible to select multiple alerts.

The View Details icon appears in the top right corner of the pane.

3. Click the View Details icon.

A pop-up window opens displaying detailed information about the selected alert(s).

If required, add a comment to an alert.



	Alert	Severity	Src device	Dst device	Protocol / Port	Package name	Last modified	Count
☑	PROTOCOL-TELNET Unencrypted Passwo...	High	10.51.67.34	172.16.12.254	Telnet (23)	Cyber Attack	10/06/2021 14:28	2
□	PROTOCOL-TELNET Unencrypted Passwo...	High	10.219.42.4	10.219.250.229	Telnet (23)	Cyber Attack	10/06/2021 14:28	2
□	ARP Poisoning involves 10.187.82.134 an...	Medium	10.187.82.134		()	Cyber Attack	10/06/2021 14:28	1

Click to filter alert list

Select an alert

Click Show Cause icon

View the root cause of an alert

In many instances you may wish to learn about the root cause of an alert.

1. Go to Alerts or Archive (Alerts > Alerts/Archive).
2. Make sure the Cause column is visible.

Note: If the Cause column is not visible, open the Select Columns to display pop-up window and select Cause.

3. In the Cause column, click the icon corresponding to the alert you wish to view.

A window opens displaying the root cause of the alert.

Manage Alerts

In Alerts, you can manage alerts as follows:

- Download a PCAP of an alert
- View a timestamp of a suspicious packet
- Add an alert to baseline
- Archive an alert
- Delete an archived alert
- Attach a procedure to an alert

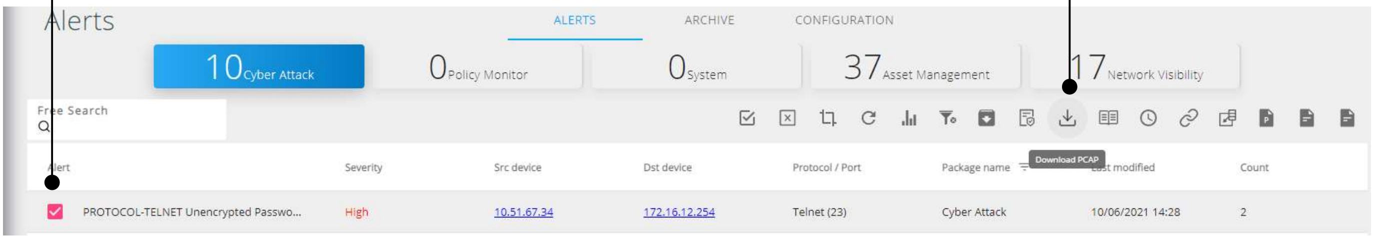
Download a traffic PCAP file

For investigative purposes, you may wish to download a PCAP file of the traffic ‘before’ and ‘after’, surrounding the root cause packet.

1. Go to Alerts.
2. Select the relevant alert, suing the checkbox provided.
3. Click the Download PCAP icon. The PCAP will be downloaded to your default download folder.

Select an alert

Click Download button



Alert	Severity	Src device	Dst device	Protocol / Port	Package name	Last modified	Count
☑ PROTOCOL-TELNET Unencrypted Passwo...	High	10.51.67.34	172.16.12.254	Telnet (23)	Cyber Attack	10/06/2021 14:28	2

View the timestamp of a suspicious packet

1. Go to Alerts.
2. See the Last modified column.
3. Within the downloaded PCAP file, there will be also a text file contains the exact timestamp (In Epoch Format) of the suspicious packet.

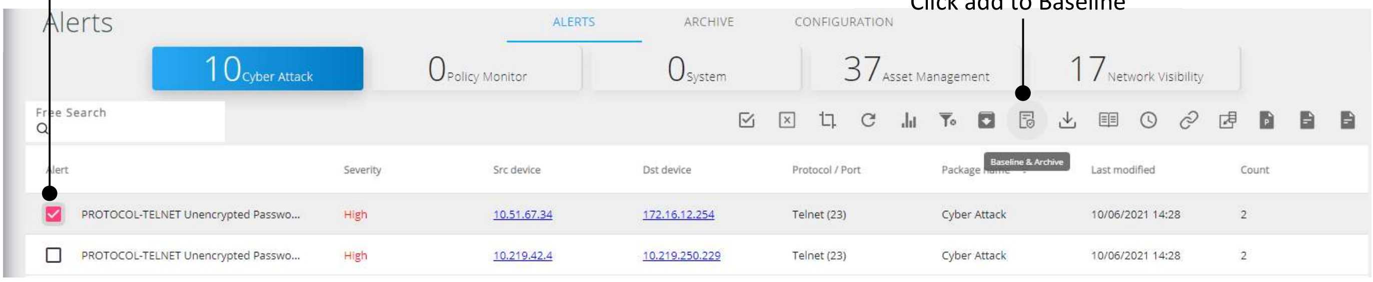
Add an alert to baseline

You can add an alert to the baseline. By doing so, iSID learns that the threat is normal behavior and does not issue future notifications as if it were detected during the learning phase.

1. Go to the Alerts pane (Alerts > Alerts).

Select an alert

Click add to Baseline



Alert	Severity	Src device	Dst device	Protocol / Port	Package name	Last modified	Count
☑ PROTOCOL-TELNET Unencrypted Passwo...	High	10.51.67.34	172.16.12.254	Telnet (23)	Cyber Attack	10/06/2021 14:28	2
□ PROTOCOL-TELNET Unencrypted Passwo...	High	10.219.42.4	10.219.250.229	Telnet (23)	Cyber Attack	10/06/2021 14:28	2

2. Select the checkbox of the alert you want to add to baseline.
3. Click the Add to Baseline & Archive icon. The alert is added to the baseline.

Archive an alert

Whenever a threat is repeated, Radiflow iSID will pop up the same alert and increase the count of same detected alert in the Count column. To acknowledge the threat, you may wish to remove the newly-learned threat from Radiflow iSID's understanding of the network together with any dependent entity.

For example, when a new device is detected, normally it starts communicating with some other device; therefore, a new Link is also detected. The new Device and new Link appear on the Map in red, indicating that a new alert was issued for each.

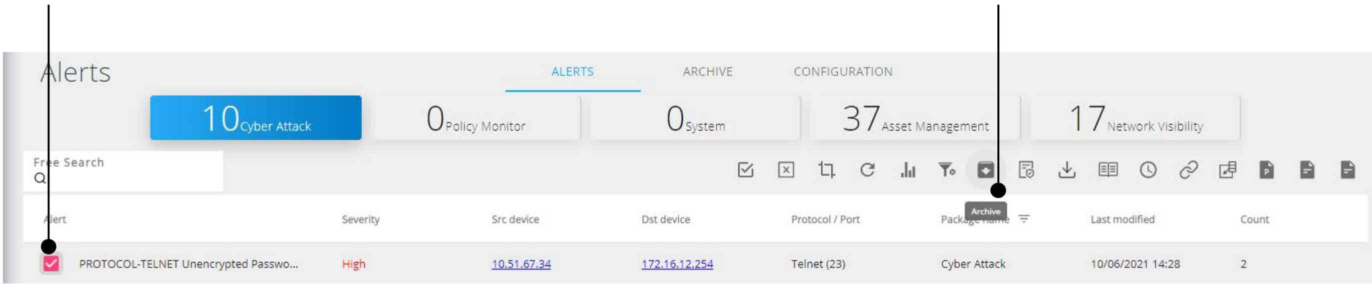
Since the newly-connected device was not a user-approved device, you can identify the device, disconnect it physically from the network and archive the "New Device Detected" alert.

The new device is then removed from the Map together with any link it may have. In addition, every new alert on this device or any of its links will be moved automatically to Archive.

1. Go to the Alerts pane (Alerts > Alerts).

Select an alert

Click Move to Archive



Alert	Severity	Src device	Dst device	Protocol / Port	Package name	Last modified	Count
☑ PROTOCOL-TELNET Unencrypted Passwo...	High	10.51.67.34	172.16.12.254	Telnet (23)	Cyber Attack	10/06/2021 14:28	2

2. Select the checkbox of the alert you want to archive.
3. Click the Move to Archive icon. The alert is removed from the open alerts list and added to the archived alerts.

Archive Alerts

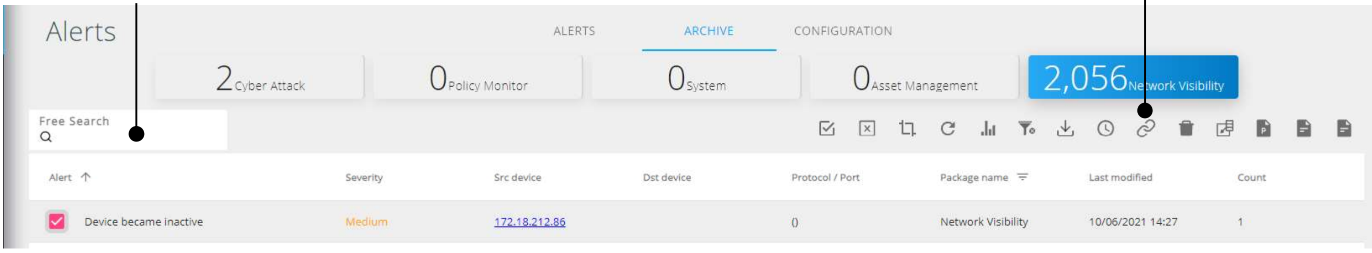
When an alert has been acknowledged, you may want to archive it.

View archived alerts

You can view general information or in-depth details about archived alerts and their root causes.
 Go to Archive (Alerts > Archive).

Click to filter archive alerts by type

Click to view archive alert cause



Alert	Severity	Src device	Dst device	Protocol / Port	Package name	Last modified	Count
☑ Device became inactive	Medium	172.18.212.86		0	Network Visibility	10/06/2021 14:27	1

In Archive you can do the following:

- Quickly view the number of archived alerts and the type of archived alert
- Click each alert type to filter the archived alert list according to type of alert
- View details about an archived alert
- View the root cause of an archived alert
- Delete an archived alert
- Search for archived alerts based on specific criteria
- Adjust the order the archived alerts are displayed
- Show and hide columns
- Choose how many archived alerts to view per page

Delete an archived alert

1. Go to Archive (Alerts > Archive).
2. Select the checkbox of the archived alert you want to delete.
3. Click the Delete icon. In the confirmation pop-up window, click OK.

The archived alert is deleted and no longer appears in the archive alert list.

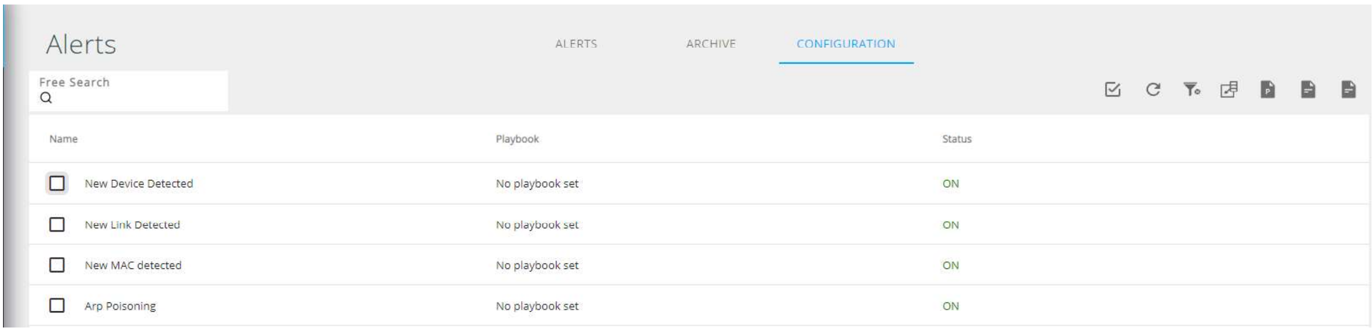
Alert Configuration

Under Alerts > Configuration, you can:

- View and edit alerts
- Enable and disable specific alerts

View configured alerts

1. Click Alerts in the sidebar.
2. Click Configuration. The Configuration pane opens.



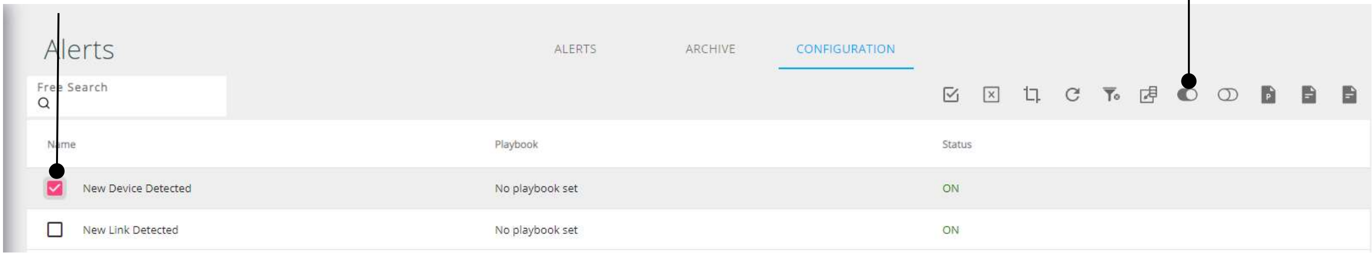
	Name	Playbook	Status
□	New Device Detected	No playbook set	ON
□	New Link Detected	No playbook set	ON
□	New MAC detected	No playbook set	ON
□	Arp Poisoning	No playbook set	ON

3. In the Configuration pane, do the following:

- View alert name
- Enable and disable the selected alert
- Search for specific alert
- Show and hide columns
- Choose how many items to view per page

Enable and Disable alerts

1. Go to Configuration (Alerts > Configuration).
2. Select the checkbox of the alert you wish to enable or disable.
3. Move Status to on to enable the alert
4. Move Status to off to disable the alert
5. Edit the procedure's free text (limit to 2,000 characters).



Click to disable / enable the alert

Click to filter archive alerts by type

	Name	Playbook	Status
☑	New Device Detected	No playbook set	ON
□	New Link Detected	No playbook set	ON

Map

Radiflow iSID Map is a graphical representation of the network map. It is dynamically updated as additional entities (devices, links) are detected.

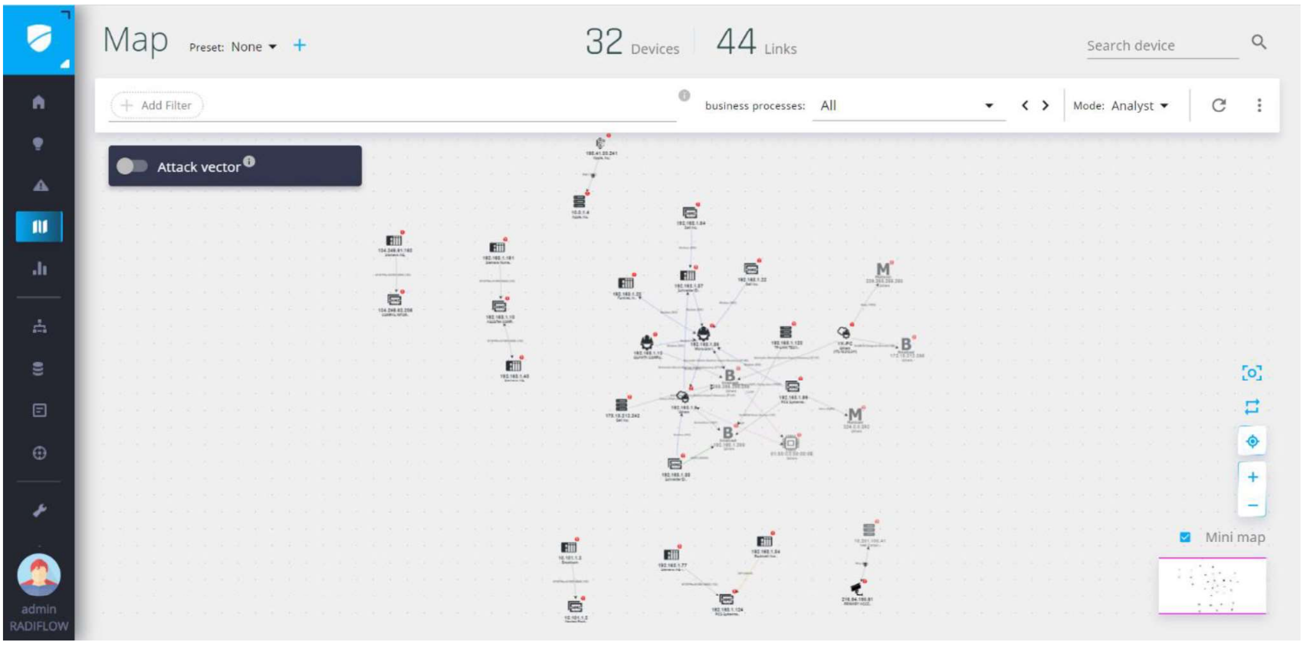
The network topology map allows you to understand the inner workings of the network.

Go to Maps to do the following:

- Quickly view how many devices and links there are on the network
- View a graphical representation of the network
- View the relationship between various devices and various subnets

View Maps

In the sidebar click Map to view the map.



The Map is built according to several rules:

- Structural view of the network – iSID passively detects all network devices
- Logical connections view of the network which does not include passive networking devices such as switches, routers, etc.
- Inactive devices are displayed as well as devices that never transmitted (shown with transparency)

The Map is a powerful tool, enabling you to do the following:

- View a summary of each device
- Search for a device
- Re-arrange the map with different layouts
- Filter by device, vendor, link etc.

- Take a screen shot of the map
- Rearrange the map
- Create a new map layout

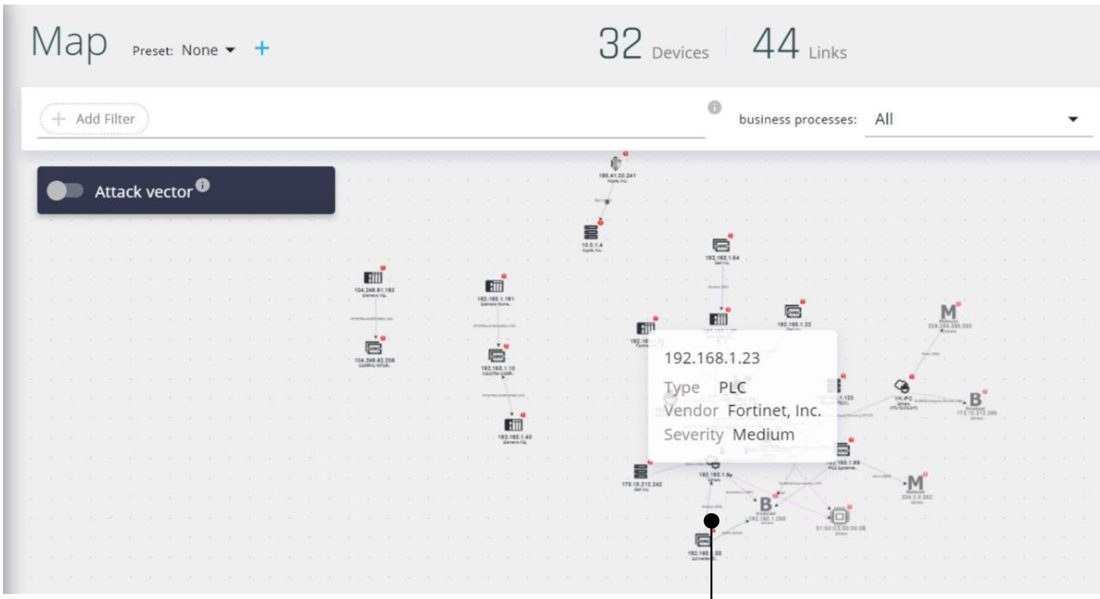
View Device Information

In Maps, view a summary of each device or in-depth details about each device.

View a summary of each device

1. Open the Map view.
2. Hover the mouse over an entity on the map. A summary of each device appears, including the type of device, vendor, and severity value.

The severity value represents the risk amongst all new events related to that device or its links. If the device has no new/or open alerts, the severity value will revert to normal state (value = 1).



Map Preset: None 32 Devices 44 Links

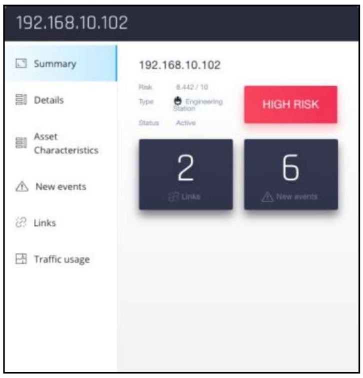
business processes: All

192.168.1.23
Type PLC
Vendor Fortinet, Inc.
Severity Medium

Move mouse over a device to reveal the summary window

View details about each device

1. Open the Map view.
2. Double-click a device. A pop-up window opens displaying a summary and details about the device. Click through the pop-up window to view and edit individual device details.



192.168.10.102

192.168.10.102

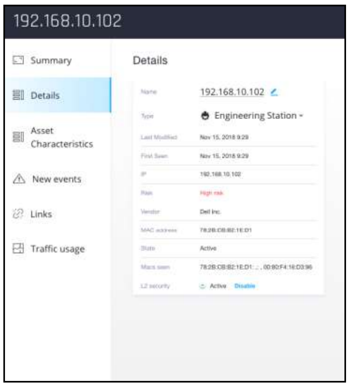
Risk	8.442 / 10
Type	Engineering Station
Status	Active

2 Links

6 New events

View the IP address, risk, device type, status, and number of links and events associated to the device

- Click Links to view link details
- Click New events to view

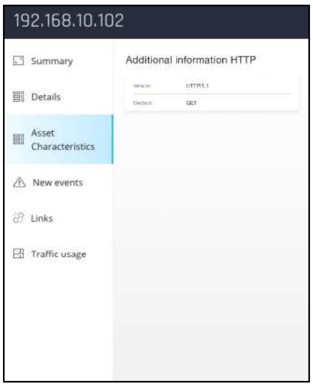


192.168.10.102

Details

Name	192.168.10.102
Type	Engineering Station
Last Modified	Nov 15, 2018 9:29
First Seen	Nov 15, 2018 9:29
IP	192.168.10.102
Risk	High risk
Vendor	Dell Inc.
MAC address	78:2B:CB:B2:1E:D1
State	Active
Macs seen	78:2B:CB:B2:1E:D1 : , 00:80:F4:16:D3:96
L2 security	Active Disable

- View the device details
- Edit a device name
- Edit a device type
- Update the BPs for the device
- Edit the L2 security

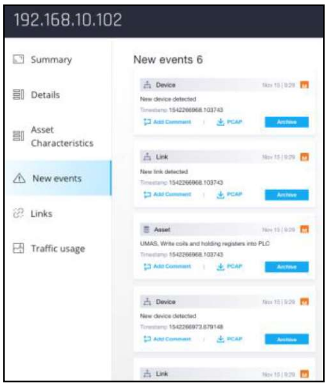


192.168.10.102

Additional information HTTP

Version	HTTP/1.1
Method	GET

- View the asset characteristics



192.168.10.102

New events 6

Device Nov 15 | 9:29
New device detected
Timestamp 1542266968.103743

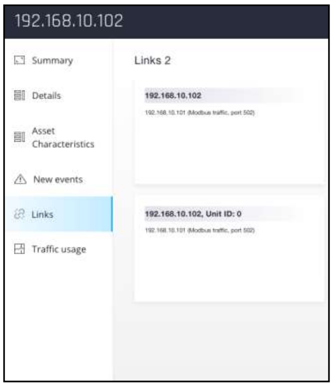
Link Nov 15 | 9:29
New link detected
Timestamp 1542266968.103743

Asset Nov 15 | 9:29
UMAS, Write coils and holding registers into PLC
Timestamp 1542266968.103743

Device Nov 15 | 9:29
New device detected
Timestamp 1542266973.679148

Link Nov 15 | 9:29

- View new events associated with this device
- Add a comment, download, or archive an



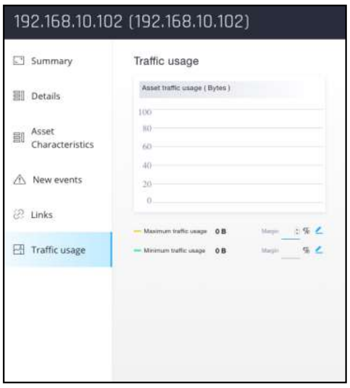
192.168.10.102

Links 2

192.168.10.102
192.168.10.101 (Modbus traffic, port 502)

192.168.10.102, Unit ID: 0
192.168.10.101 (Modbus traffic, port 502)

- View links to other IP addresses



192.168.10.102 (192.168.10.102)

Traffic usage

Maximum traffic usage 0 B

Minimum traffic usage 0 B

- View the current minimum and maximum traffic thresholds
- Edit the traffic usage thresholds for this device

Search for a device

There are two methods for searching for a device in Maps

- Use the search filters to perform a search
- Search for a device without using search filters

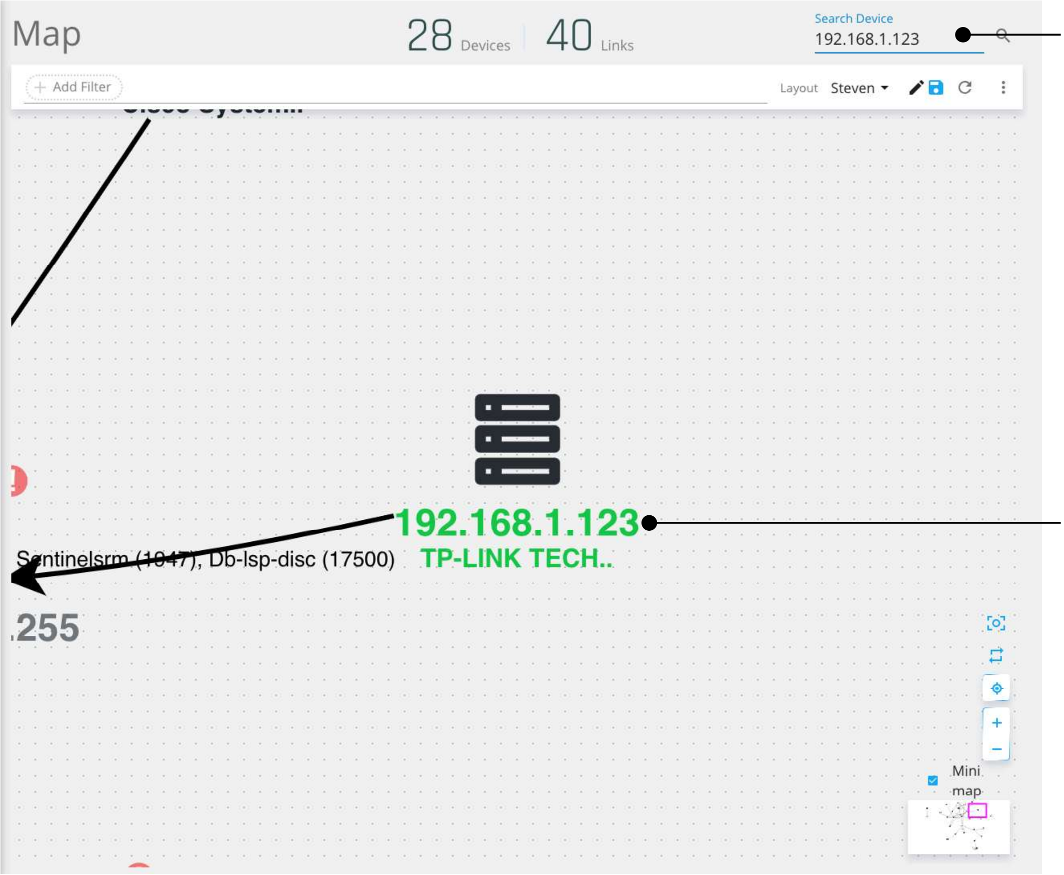
Search for a device using search filters

1. Open the Map view.
2. Click Add Filter, and use the search tools and filters to search for a device
3. Click the Filter icon.

If there is a positive match to the search, Maps automatically refreshes and zooms in on the device you searched for.

Search for a device without using search filters

1. Open the Map view.
2. In the Search Device field, enter the name of the device you are looking for, and click the magnifying glass icon. If there is a positive match to the search, Maps automatically refreshes and zooms in on the device you searched for.



Use the Search Device field to search for a device

Maps zooms into device matching search parameters

Remove a device

If a device is no longer active, you might prefer to remove it from the map. To remove an inactive device:

1. Open the Map view.
2. Locate the device on the Map. (Zoom in with the mouse wheel. Click and drag to move the map.)
3. Right-click on the device and select Delete from the context menu.
   Note: the Delete option is present only if all of the following conditions are met:

1. The device status is inactive.
2. All device links are inactive.
3. The device type is destination-only.
4. The device type is not Broadcast or Multicast.

Map Mode

In the Map view, you can select a different map layout by selecting your desired map mode:

- Custom
- Analyst
- Flow
- Purdue

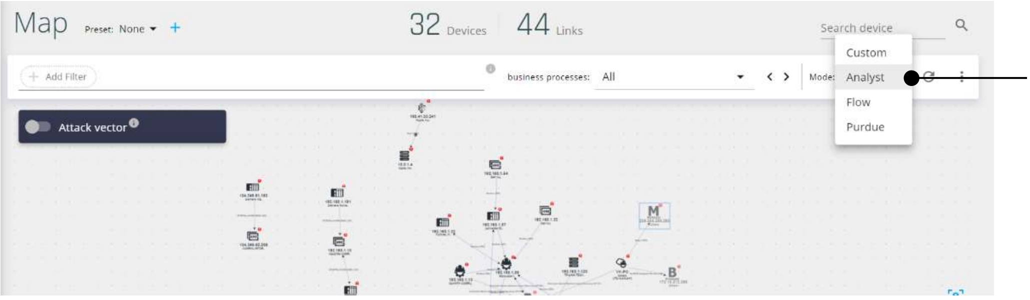
1.

Change the map mode

You can select which layout to view.

1. Open the Map view.
2. Select a layout from the Mode list.

Map refreshes displaying the selected layout.

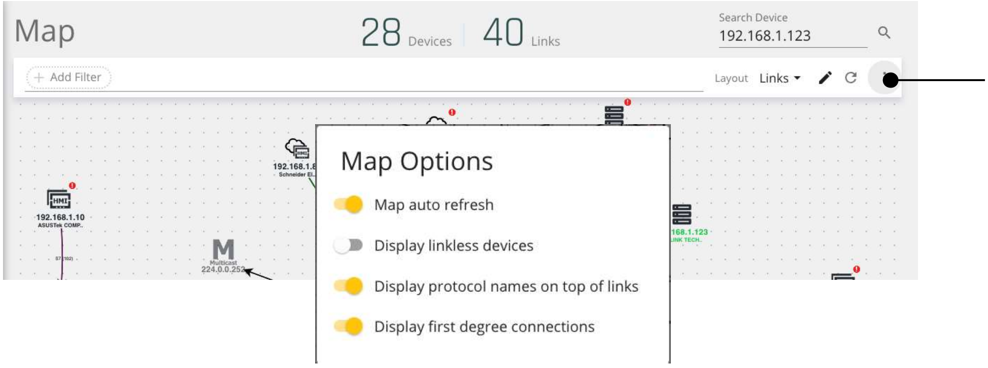


Select a mode

If you make any manual change to the map layout (for example, by dragging and dropping an asset to a different place in the map) the Map Mode will automatically switch to Custom mode. Specify the map options

Specify how you want to display the map

1. Open the Map view.
2. Click the Map options icon. The Map options pop-up window opens.



Map Options

- ● Map auto refresh
- ○ Display linkless devices
- ● Display protocol names on top of links
- ● Display first degree connections

Map options icon

3. Toggle the options to on or off as required. The map refreshes to reflect the selected options.

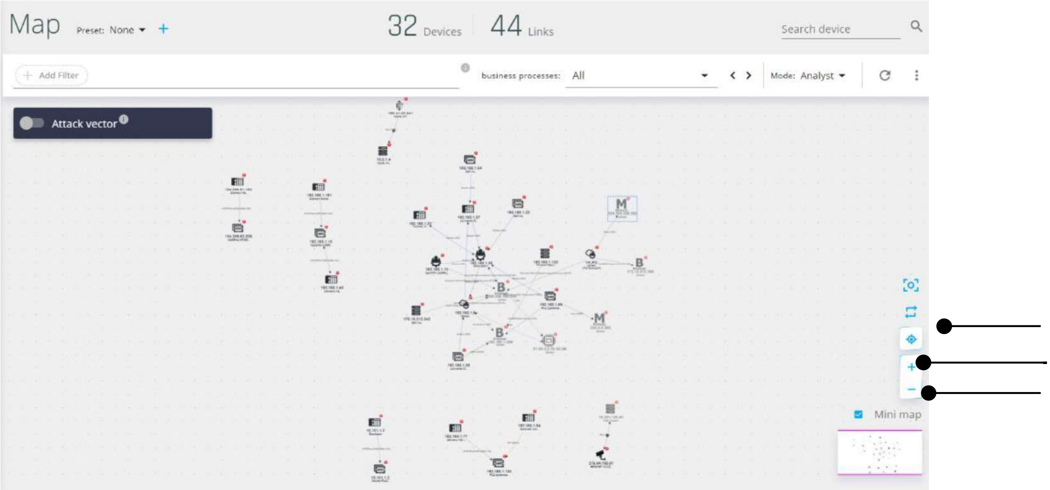
Take a screenshot of the map

1. Open the Map view.
2. Click Screen Shot.

A screenshot of the map is downloaded to the local PC in PNG format.

Change the map view

1. Open the Map view.
2. Use the Zoom in/out, and Zoom to fit tools to view the map according to your requirements.



Click Screen Shot icon

Zoom to fit

Zoom in/out

Business Processes (BPs)

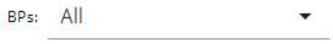
Overview

It is often useful to view a subset of assets within the OT network, based on a specific business process. For example, you might want to view all devices required for a specific output e.g. the generation of electricity. The BP (Business Process) feature allows you to filter the Map view according to 1 or more business processes.

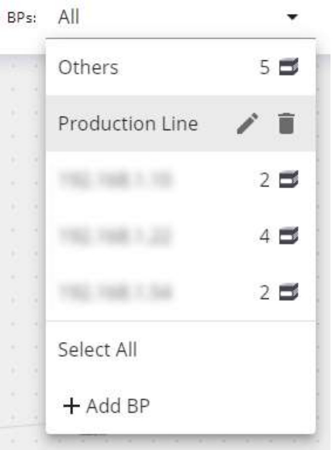
The BP list

The iSID solution automatically identifies business processes and groups network devices accordingly. To view the known list of BPs (business processes):

1. Open the Map view.
2. Click on BPs field (top, right):



3. The BPs drop-down displays:



4. Each BP (business process) identified by the system is automatically assigned a name. This name reflects the IP of the top-level HMI device within that group.
5. Each BP also displays a counter (on the right). This indicates the number of devices within that group.
6. While viewing the list of BPs, you can rename a BP, remove a BP - or add or your own, user-defined BP.

Rename a BP

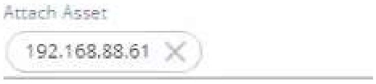
1. Open the Map view.
2. Click on BPs drop-down list (top, right).
3. Click on Edit ✎ and type in your own, user-defined name.

Remove a BP

1. Open the Map view.
2. Click on BPs drop-down list (top, right).
3. Click on the Delete 🗑 icon provided.

Add a BP

1. Open the Map view.
2. Click on BPs drop-down list (top, right).
3. Click on Add BP + (at the bottom of the drop-down list).
4. In the pop-up provided:
1. Enter the name of the user-defined BP.
2. In the Attach Asset field, start typing the IP of the desired asset. As you type, the autocomplete field displays a list of matching IPs. Select the desired IP from the list:


Attach Asset
192.168.88.61 ✕

3. Repeat the previous step multiple times, adding as many assets as desired.
4. Indicate if you also want to add any assets linked to the asset(s) that you chose above:

● Attach linked assets

5. Click Apply.

Filter by Business Process (BP)

You can filter the map view to show only those assets that belong to 1 or more BPs (business processes):

1. Open the Map view.
2. Click on the BPs drop-down list (top, right).
3. Select 1 or more BPs in the list. As you select a BP in the drop-down list, the map view updates to show only those assets that belong to the selected BP(s).

Multi-selection

1. When you filter by BP, you can select more than 1 BP (business process) in the BP list. As you do so, the map view updates to show devices across all selected BPs.
2. To remove a single selection in the BP list, click a second time on that BP.
3. To remove all selections in the BP list, click on Select all (bottom of the list).
4. To show all devices not within the selected BP(s), click on Others (top of the list).

BP counters

1. Each BP (business process) in the BP list displays a counter (on the right). This indicates the number of devices within that BP.
2. BPs often ‘overlap’. As you apply BP filters, the counters in the BP list update to show how many devices are displaying for each BP.
3. For example, let’s say that:
1. BP 10.0.0.1 contains 140 devices
2. BP 10.0.0.2 contains 70 of those devices.

4. When you select BP 10.0.0.2, the counter for BP 10.0.0.1 updates to show 70/140. In other words, 70 of the 140 devices in BP 10.0.0.1 are showing within the current filter.

View/update BPs for a given device

To view the BPs (business processes) to which a given device belongs:

1. Open the Map view.
2. Double-click on a device to open the device details pop-up.
3. Select the Details tab. The Business Processes section lists the BPs (business processes) to which the device belongs.
4. To remove the device from a BP, click on the Delete 🗑 icon for that BP.
5. To add the device to an additional BP, click on Add + (at the bottom of the list).

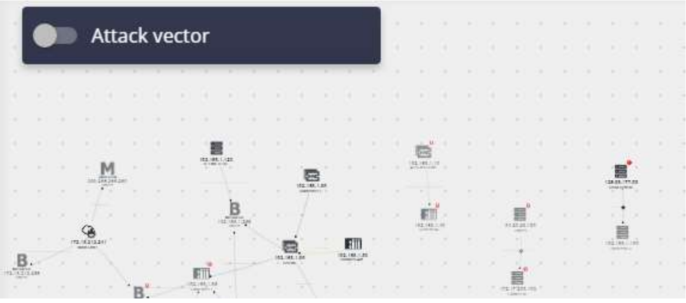
Attack vector

Overview

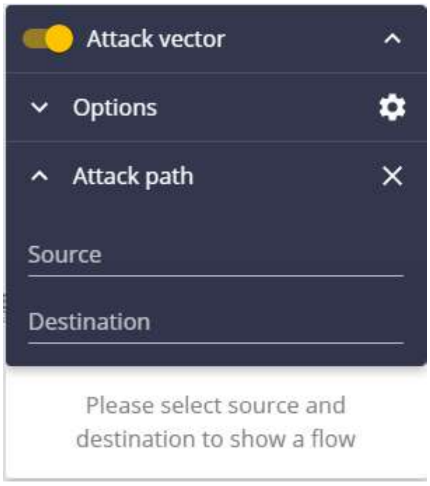
Sometimes, it is useful to analyze the potential risk of a given attack vector - i.e. a potential attack path between 2 specific network assets. The Attack vector feature allows you to view this analysis upon request.

View an attack vector

1. Open the Map view.
2. Toggle on Attack vector (top, left):



3. The Attack vector slide-out displays:



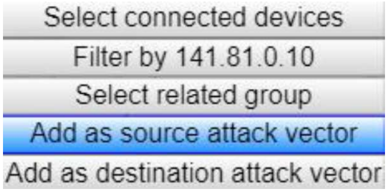
Please select source and destination to show a flow

4. Under Attack path, fill in a Source and Destination. You can use either of the following methods:

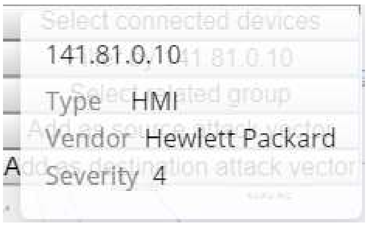
1. Fill in each IP address manually.

   Or

2. Locate the relevant device on the Map (zoom in with the mouse wheel - then click and drag). Right-click on the device and select Add as source or Add as destination from the context menu:



Note: If the context menu is obscured by the mouse-over tool-tip, move your mouse over the visible edge of the menu (on the left):

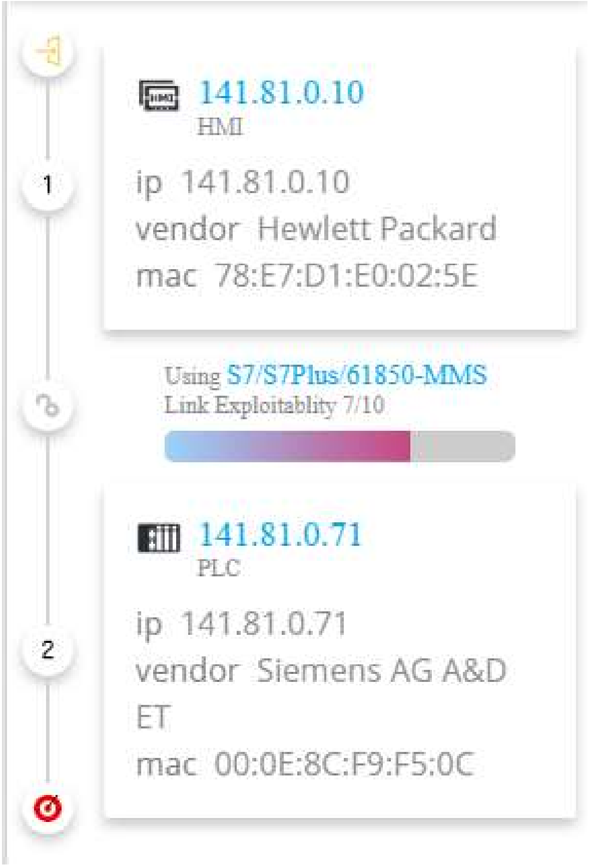


141.81.0.10
Type HMI
Vendor Hewlett Packard
Severity 4

5. Expand the Options section (using the arrow ⌄) and select the attacker model (sophistication level) of concern:

- Low
- Medium
- High

6. Once you have specified both the attack path and attacker model, the slide-out expands downward to display the attack vector analysis:



141.81.0.10
HMI

ip 141.81.0.10
vendor Hewlett Packard
mac 78:E7:D1:E0:02:5E

Using S7/S7Plus/61850-MMS
Link Exploitablity 7/10

141.81.0.71
PLC

ip 141.81.0.71
vendor Siemens AG A&D ET
mac 00:0E:8C:F9:F5:0C

Note:
The system will notify you if no attack vector exists for the specified path and model. In that case, consider trying an alternative model (e.g. Medium or High).

Clear the query

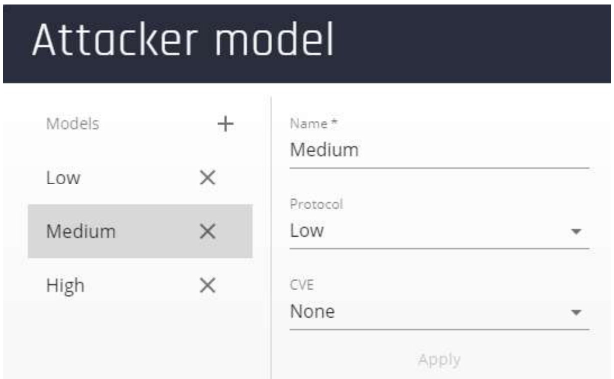
After viewing an attack vector analysis, you may wish to clear your input and start afresh. To do so:

1. Click on the Clear query ☒ icon.
2. Enter new parameters (see previous section).

Edit an attacker model

To tweak the definition of a given attacker model:

1. Click on the Attacker model settings ⚙ icon (top, right).
2. The attacker model dialogue box displays:



Name * Medium

Protocol Low

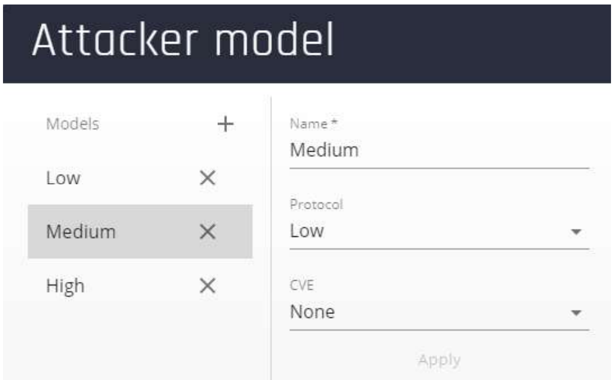
CVE None

3. Select the desired model on the left (Low, Medium or High).
4. Adjust the Protocol and CVE fields as desired, and Apply (bottom, right).
   Note: the Apply button will be enabled once you make a change.
5. The system confirms that the change has been applied (bottom, right).

Add an attacker model

To add a custom attacker model:

1. Click on the Attacker model settings ⚙ icon (top, right).
2. The attacker model dialogue box displays:



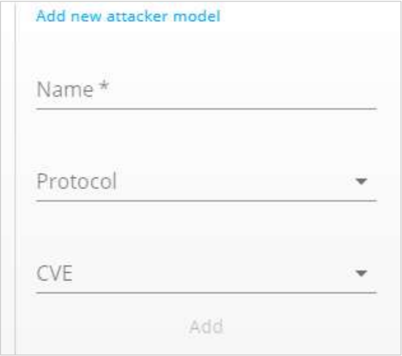
Name * Medium

Protocol Low

CVE None

3. Click on the Add model + icon (top, left).

   In the section on the right, fill in a name for the new model, and select a value for Protocol and CVE:



4. Click Apply (bottom, right) to save.
   Note: the Apply button will be enabled once you fill in Protocol and CVE.

Reports

Key activities

Using the Reports nodule, you can do the following:

Queries (right):

- Create a new query (mini-report) or tweak an existing one.
- Download a query as PDF or CSV.
- Save a query.
- Group saved queries under a report.
- Remove queries from a report/re-order queries within a report.

General (left):

- Prepare and download security reports.
- Prepare and download event PCAPS.
- Create custom reports.

Queries

Overview

A query is a mini-report for a single, chosen entity - e.g. Devices. You can group multiple queries under 1 report. In this way, the report acts as a 'container' for several queries. If you download the report as a PDF document, each query displays sequentially. (You can re-order the queries as desired.)

iSID comes with some basic queries built in to the system. You can simply run these queries as-is or you can customize them as described below in Create a query and then save it as a new query. You can also join built-in queries to a report (see Join queries to a report).

You can customize a query, according to your needs and preferences:

- Apply filters
- Choose columns
- Sort by 1 or more columns
- Group by

You can download your query as CSV or PDF. You can also save your query and run it again later.

Once you have saved 1 or more queries, you can join them to an existing report - or group them under a new report that you create 'on the fly'.

Create a query

1. Under Reports, select the Queries tab (top, right):

2. Click on the Add query ⊕ icon (left pane).
3. Select an entity - e.g. Devices. This will determine the available columns and data.
4. Provide a Title and Description (top, left)
5. Customize the query, according to your needs and preferences:

1. Add 1 or more filters (top, left): + Add Filter
2. Choose desired columns and column aliases (top, right):
3. Sort by 1 or more columns (top, right):
4. Group by a column (top, right):
1. Choose an output display: Bar, Line, Pie and/or Table

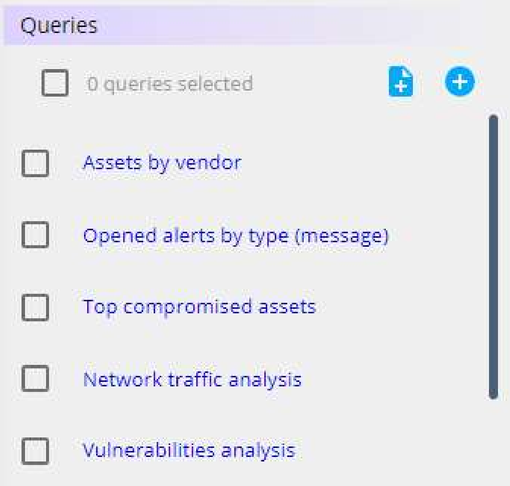
    Note: if desired, you can select more than 1 display

6. Download the query as PDF or CSV (far right):
7. Save the query, so that you can easily run it again (far top, right):

Join queries to a report

1. Under Reports, select the Queries tab (top, right):

2. A list of saved queries displays in the left pane, under Queries (top). Select 1 or more queries, using the checkboxes provided:


Queries

□ 0 queries selected

□ Assets by vendor

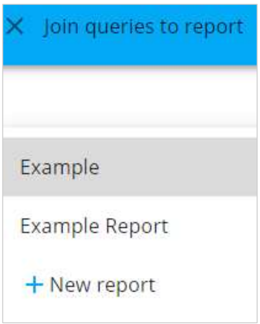
□ Opened alerts by type (message)

□ Top compromised assets

□ Network traffic analysis

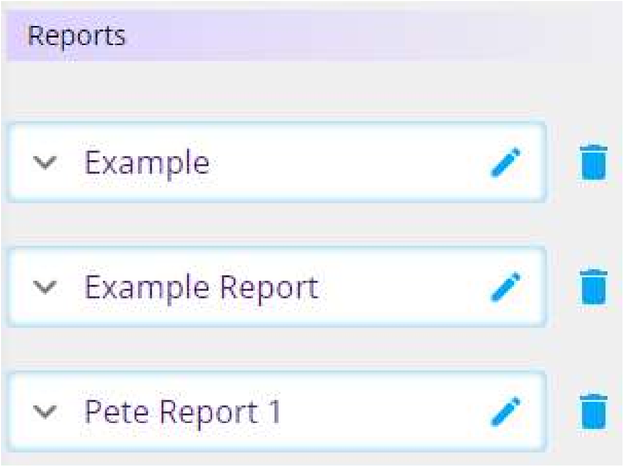
□ Vulnerabilities analysis

3. Click on the join queries to report icon (top right).
4. Select an existing report - or create a new one:

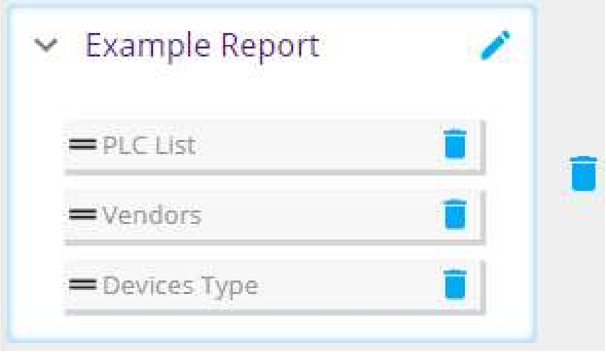


Customize a report

1. Under Reports, select the Queries tab (top, right).
2. A list of saved reports displays in the left pane, under Reports (bottom):



3. To rename a report, click on the Edit icon ✎ (right).
4. To customize the queries within the report:
   1. Expand the report, using the arrow ⌄ icon (left). The list of queries display.
   2. Drag queries to re-order them, or click remove 🗑 to remove a given query.



Note:

1. Changes made will be auto-saved in real time.

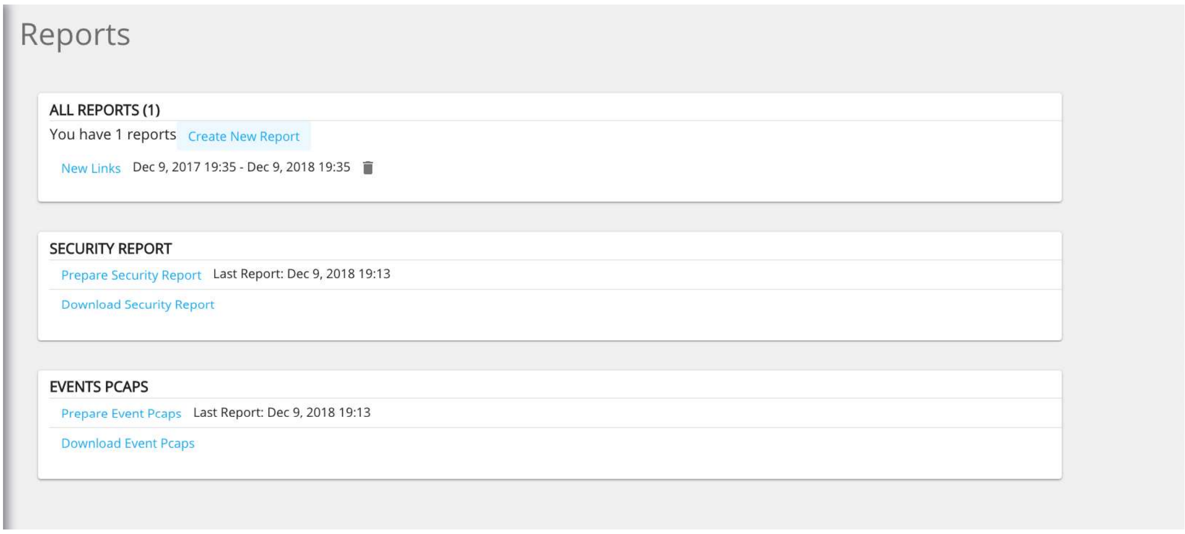
2. You can also delete 🗑 the entire report (far right). When removing a query, take care not to mistakenly delete the entire report!

View Report Information

You can view high-level report information or in-depth details about each report.

View general report information

Select Reports in the sidebar.
By default, the Reports pane opens displaying general report information, such as name of report, date report was created, number of reports.



Reports

ALL REPORTS (1)

You have 1 reports Create New Report

New Links Dec 9, 2017 19:35 - Dec 9, 2018 19:35 🗑

SECURITY REPORT

Prepare Security Report Last Report: Dec 9, 2018 19:13

Download Security Report

EVENTS PCAPS

Prepare Event Pcaps Last Report: Dec 9, 2018 19:13

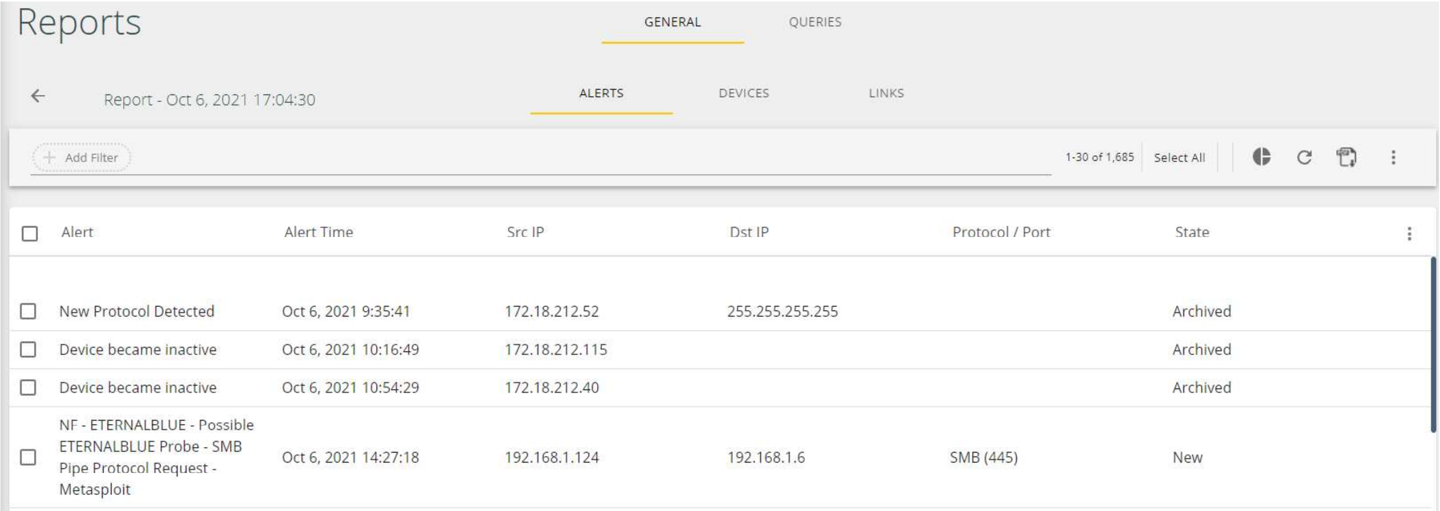
Download Event Pcaps

View details about a report

1. Go to Reports.
2. In the All Reports section, click the name of the report you wish to view.

A reports pane opens with three links: Alerts, Devices, and Links.

3. Click the three links to view details about each alerts, devices on the network, and network links.



□	Alert	Alert Time	Src IP	Dst IP	Protocol / Port	State
□	New Protocol Detected	Oct 6, 2021 9:35:41	172.18.212.52	255.255.255.255		Archived
□	Device became inactive	Oct 6, 2021 10:16:49	172.18.212.115			Archived
□	Device became inactive	Oct 6, 2021 10:54:29	172.18.212.40			Archived
□	NF - ETERNALBLUE - Possible ETERNALBLUE Probe - SMB Pipe Protocol Request - Metasploit	Oct 6, 2021 14:27:18	192.168.1.124	192.168.1.6	SMB (445)	New

In the reports pane, you can do the following:

- Click into Alerts, Devices, and Links to view detailed reports
- Search for reports based on specific criteria
- Adjust the report order
- Show and hide columns
- Choose how many items to view per page

4. To return to the main reports window, click the report name (located in the top left corner of the pane).

Manage Reports

Radiflow iSID enables you to create and prepare three kinds of report:

- User-defined reports - create a report with specified information
- Security reports - summarizes the findings of Radiflow iSID
- Events PCAPS - prepare and download an events packet capture file

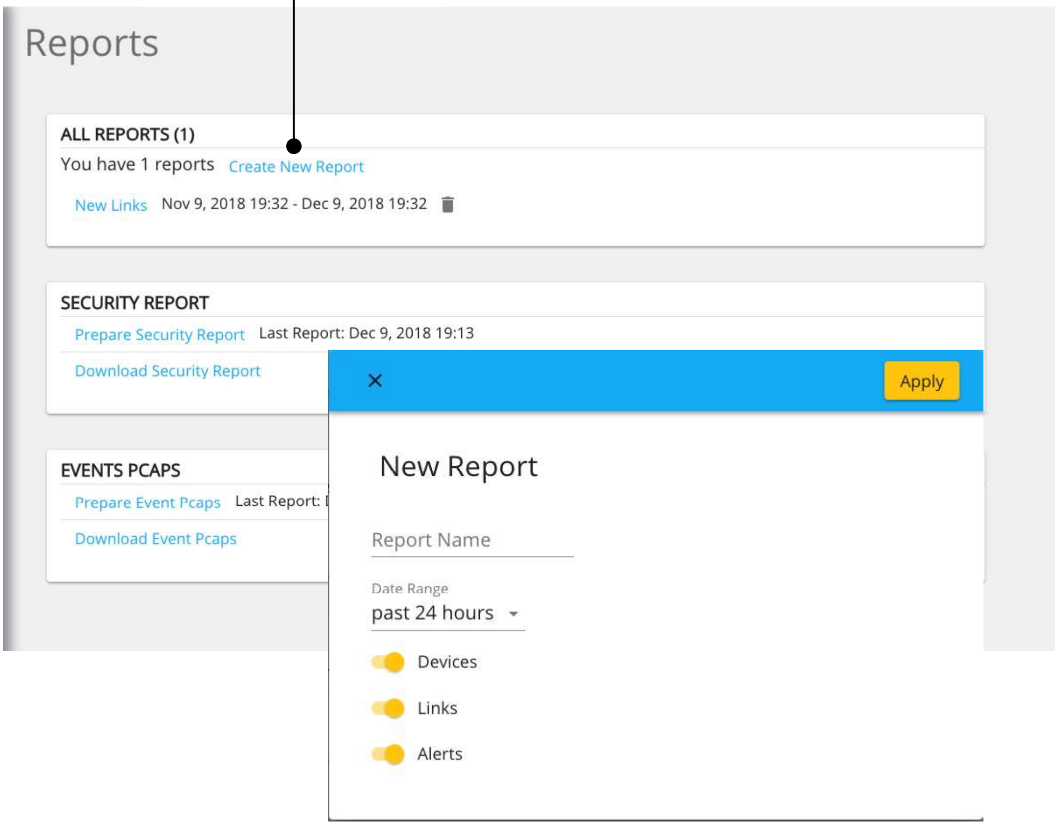
Create a report

Manually create a report with specified information. The report is created on-the-fly and can be saved for future retrieval. Go to Reports.

1. In the All Reports section, click Create New Report.

The New Report pop-up window opens.

Click Create New Report



You have 1 reports

New Links Nov 9, 2018 19:32 - Dec 9, 2018 19:32

Last Report: Dec 9, 2018 19:13

Date Range: past 24 hours

2. In the New Report pop-up window, do the following:
   - Enter a report name
   - Specify the date range of the report
   - Toggle Devices, Links, and Alerts to either include or exclude these three entities from the report
3. Click Apply.
   - A message confirms the report has been successfully created

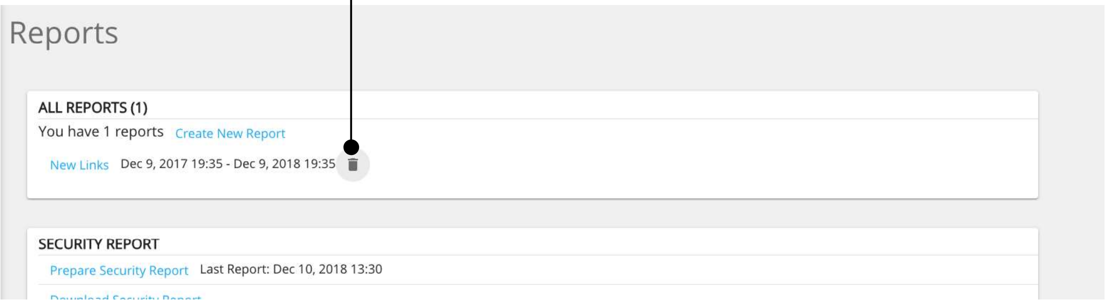
- The newly created report appears in the All Reports section of the Reports

4. Click the report to view its contents.

Delete a user defined report

User defined reports can be deleted, however once a user-defined report is deleted, it is not possible to retrieve the report again for future reference.

1. Go to Reports.
2. In the All Reports section, click the Delete icon associated with the report you wish to delete.



Reports

ALL REPORTS (1)

You have 1 reports Create New Report

New Links Dec 9, 2017 19:35 - Dec 9, 2018 19:35

SECURITY REPORT

Prepare Security Report Last Report: Dec 10, 2018 13:30

Download Security Report

Click Delete icon to delete report

3. Click OK when prompted. A message confirms the report was successfully deleted.

Prepare a security report

Security reports summarize the findings of the network visibility, asset management, cyber attack signature, and policy monitor packages. Reports also contains information about the system (devices, links, protocols, IPs, alerts, etc.).

Security reports are compiled on-the-fly and can be downloaded as Microsoft Excel files.

1. Go to Reports.
2. In the Security Report section, click Prepare Security Report.

A message confirms the report is ready for downloading.

3. Click Download Security Report. The report is downloaded to the local PC.
4. Navigate to the ‘downloads’ folder to view the report.

Prepare an events PCAP

Prepare and download the packet capture files for events over a specified time range.

Events PCAPS reports are compiled on-the-fly and can be downloaded as a compressed file.

1. Go to Reports.
2. In the Events PCAPS section, click Prepare Event PCAPS.

A message confirms the report is ready for downloading.

3. Click Download Events PCAPS. A compressed file is downloaded to the local PC.
4. Navigate to the ‘downloads’ folder to view the PCAP file.

Network Visibility

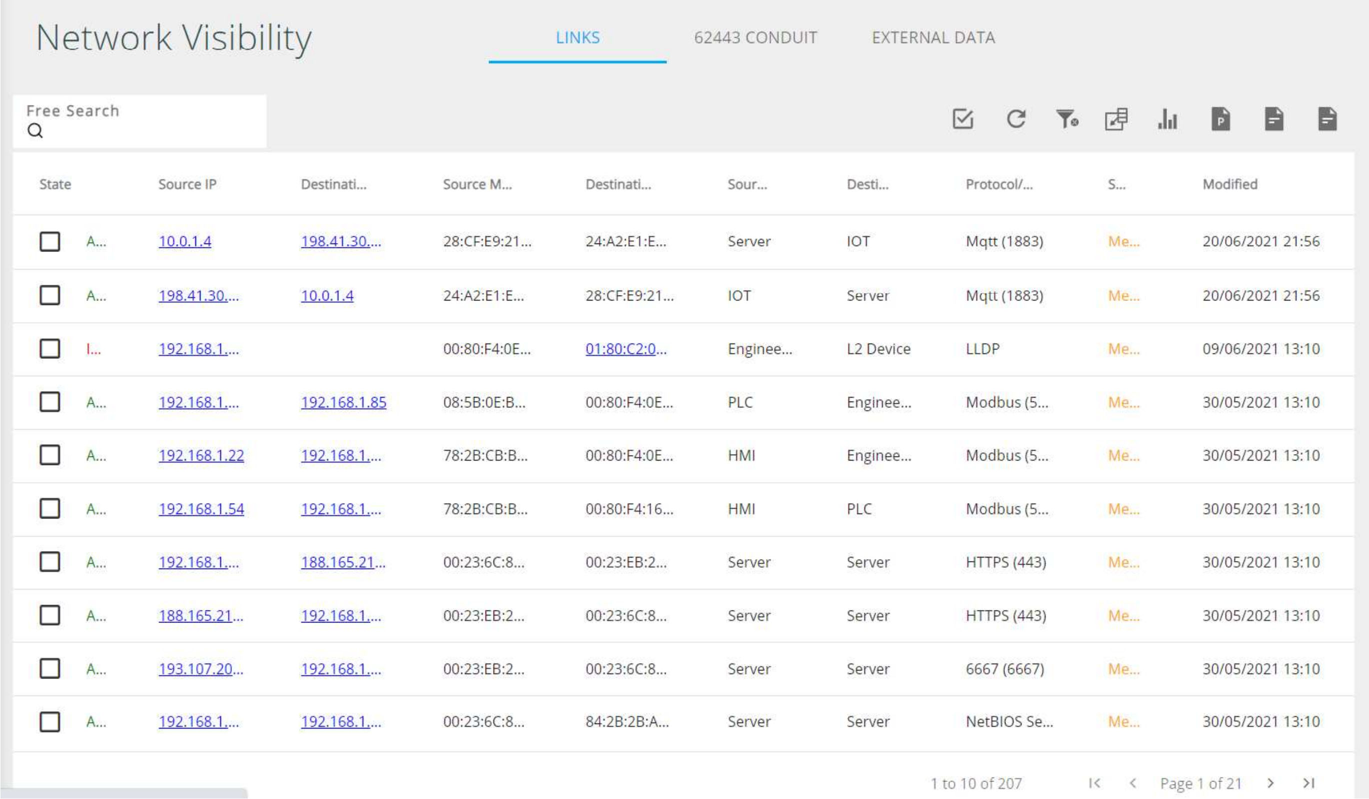
The iSID Network Visibility is a passive, self-learning SCADA network utility used to automatically construct the Operational Technology (OT) network topology model during the learning stage.

The iSID system automatically learns about the traffic within the Operational Technology (OT) network by using network Passive Learning.

Access Network Visibility to view and manage the following network elements:

- Links
- 62443 Conduit
- External Data

You can also change the network's global notification settings from any of the Network Visibility's 3 panes.



State	Source IP	Destinati...	Source M...	Destinati...	Sour...	Desti...	Protocol/...	S...	Modified
☐ A...	10.0.1.4	198.41.30....	28:CF:E9:21...	24:A2:E1:E...	Server	IOT	Mqtt (1883)	Me...	20/06/2021 21:56
☐ A...	198.41.30....	10.0.1.4	24:A2:E1:E...	28:CF:E9:21...	IOT	Server	Mqtt (1883)	Me...	20/06/2021 21:56
☐ I...	192.168.1....		00:80:F4:0E...	01:80:C2:0...	Enginee...	L2 Device	LLDP	Me...	09/06/2021 13:10
☐ A...	192.168.1....	192.168.1.85	08:5B:0E:B...	00:80:F4:0E...	PLC	Enginee...	Modbus (5...	Me...	30/05/2021 13:10
☐ A...	192.168.1.22	192.168.1....	78:2B:CB:B...	00:80:F4:0E...	HMI	Enginee...	Modbus (5...	Me...	30/05/2021 13:10
☐ A...	192.168.1.54	192.168.1....	78:2B:CB:B...	00:80:F4:16...	HMI	PLC	Modbus (5...	Me...	30/05/2021 13:10
☐ A...	192.168.1....	188.165.21...	00:23:6C:8...	00:23:EB:2...	Server	Server	HTTPS (443)	Me...	30/05/2021 13:10
☐ A...	188.165.21...	192.168.1....	00:23:EB:2...	00:23:6C:8...	Server	Server	HTTPS (443)	Me...	30/05/2021 13:10
☐ A...	193.107.20...	192.168.1....	00:23:EB:2...	00:23:6C:8...	Server	Server	6667 (6667)	Me...	30/05/2021 13:10
☐ A...	192.168.1....	192.168.1....	00:23:6C:8...	84:2B:2B:A...	Server	Server	NetBIOS Se...	Me...	30/05/2021 13:10

Notification Settings

There are two global notification settings that are accessible from all Network Visibility panes:

- Device inactivity notifications
- Layer 2 security notifications

By default both settings are selected, meaning notifications are sent when specific actions occur.

Define device inactivity notification settings

By default, iSID detects silent entities - links/devices that were once active and became silent or inactive – meaning they stopped transmitting any traffic. Once the entity is active again, iSID will re-detect it and send a notification.

1. Go to Network Visibility window, and from any pane do the following:
   - Clear the Device inactivity checkbox to turn off notifications
   - Select the Device inactivity checkbox to turn on notifications
2. In the confirmation pop-up, click OK. A message confirms iSID has been successfully updated.

Define layer 2 security notification settings

By default, iSID sends a notification if a change between the IP address and the corresponding MAC address of a network entity is detected (as a sign for ARP Positioning Attack).

1. Go to Network Visibility window, and from any pane do the following:

- Clear the Layer 2 security checkbox to turn off notifications
- Select the Layer 2 security checkbox to turn on notifications

2. In the confirmation pop-up, click OK. A message confirms iSID has been successfully updated.

Links

In Network Visibility Links you can do the following:

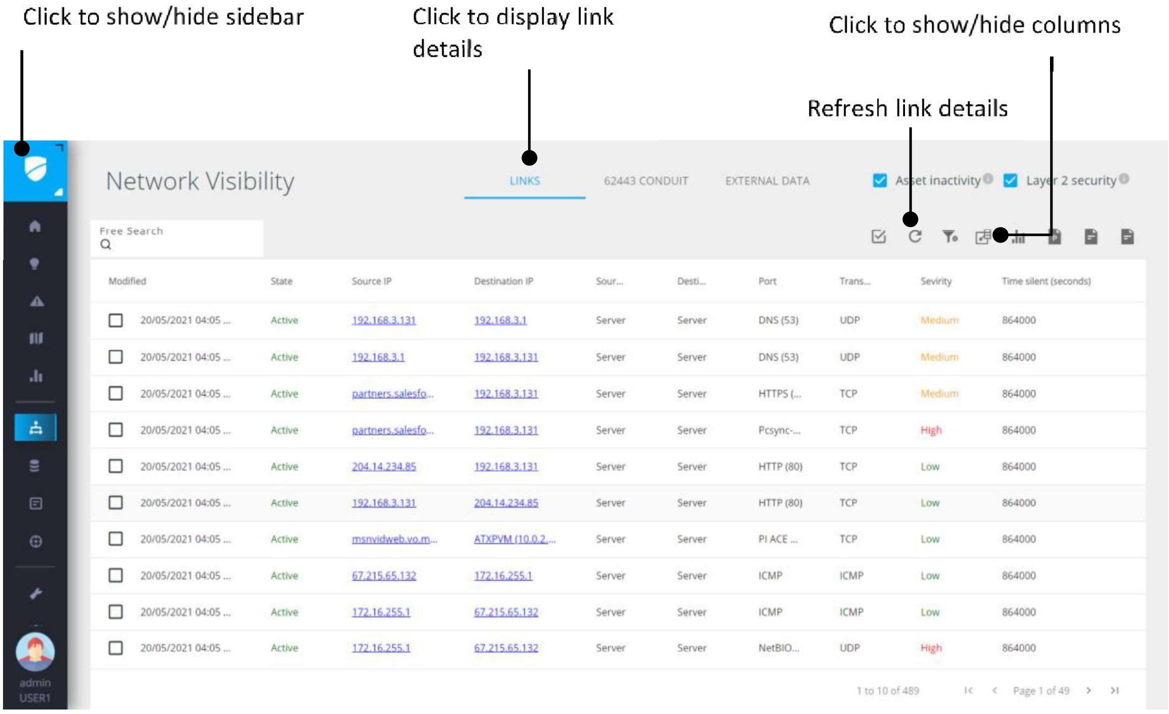
- View link details
- Search for links
- Configure the inactive times for links

View Link Details

You can view either general information or in-depth details about each link on the network.

View general information about a link

Select Network visibility in the sidebar.
By default, the Links pane opens displaying general information about a linked device, such as state, device type, port, transport, severity etc.



Click to show/hide sidebar

Click to display link details

Click to show/hide columns

Refresh link details

Network Visibility

☑ Asset inactivity ☑ Layer 2 security

Free Search

	Modified	State	Source IP	Destination IP	Sour...	Desti...	Port	Trans...	Sevirity	Time silent (seconds)
□	20/05/2021 04:05 ...	Active	192.168.3.131	192.168.3.1	Server	Server	DNS (53)	UDP	Medium	864000
□	20/05/2021 04:05 ...	Active	192.168.3.1	192.168.3.131	Server	Server	DNS (53)	UDP	Medium	864000
□	20/05/2021 04:05 ...	Active	partners.salesfo...	192.168.3.131	Server	Server	HTTPS (...	TCP	Medium	864000
□	20/05/2021 04:05 ...	Active	partners.salesfo...	192.168.3.131	Server	Server	Pcsync-...	TCP	High	864000
□	20/05/2021 04:05 ...	Active	204.14.234.85	192.168.3.131	Server	Server	HTTP (80)	TCP	Low	864000
□	20/05/2021 04:05 ...	Active	192.168.3.131	204.14.234.85	Server	Server	HTTP (80)	TCP	Low	864000
□	20/05/2021 04:05 ...	Active	msnvidweb.vo.m...	ATXPVM (10.0.2....	Server	Server	PI ACE ...	TCP	Low	864000
□	20/05/2021 04:05 ...	Active	67.215.65.132	172.16.255.1	Server	Server	ICMP	ICMP	Low	864000
□	20/05/2021 04:05 ...	Active	172.16.255.1	67.215.65.132	Server	Server	ICMP	ICMP	Low	864000
□	20/05/2021 04:05 ...	Active	172.16.255.1	67.215.65.132	Server	Server	NetBIO...	UDP	High	864000

1 to 10 of 489 |< < Page 1 of 49 > >|

- Search for items based on specific criteria
- Adjust the item order
- Show and hide columns
- Choose how many items to view per page

View details about a link

1. Go to the Links pane (Network visibility > Links).
2. Select the checkbox of the device you wish to view details about.

The View details icon appears in the top right corner of the pane.

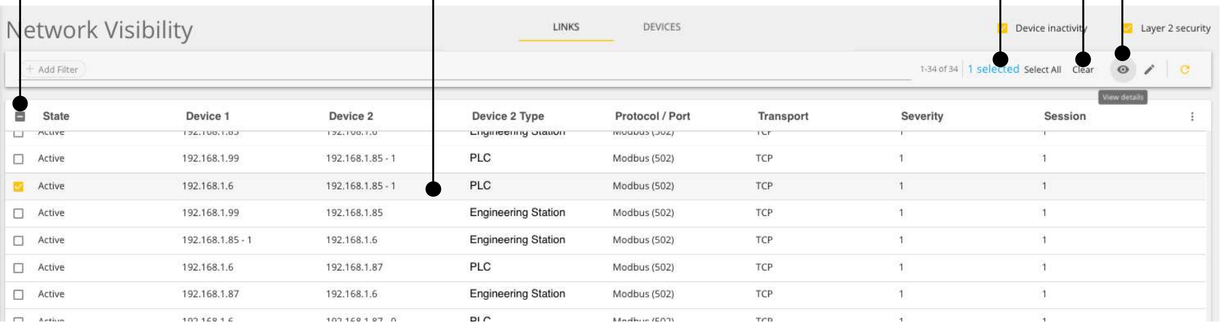
Click View details icon to display details about selected link

Select all/Clear all links

Select all/Clear all links

Selected link

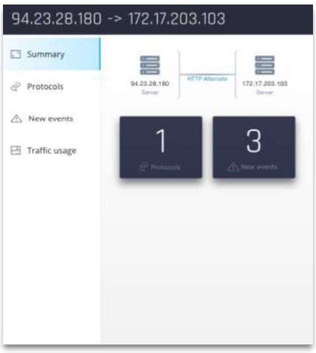
Number of links selected

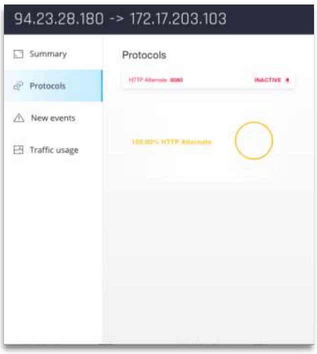


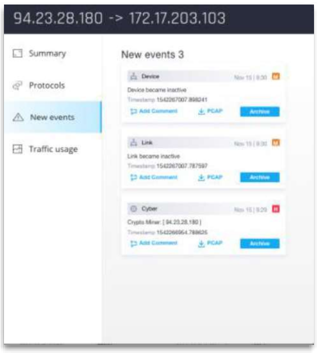
	State	Device 1	Device 2	Device 2 Type	Protocol / Port	Transport	Severity	Session
□	Active	192.168.1.99	192.168.1.85 - 1	PLC	Modbus (502)	TCP	1	1
☑	Active	192.168.1.6	192.168.1.85 - 1	PLC	Modbus (502)	TCP	1	1
□	Active	192.168.1.99	192.168.1.85	Engineering Station	Modbus (502)	TCP	1	1
□	Active	192.168.1.85 - 1	192.168.1.6	Engineering Station	Modbus (502)	TCP	1	1
□	Active	192.168.1.6	192.168.1.87	PLC	Modbus (502)	TCP	1	1
□	Active	192.168.1.87	192.168.1.6	Engineering Station	Modbus (502)	TCP	1	1

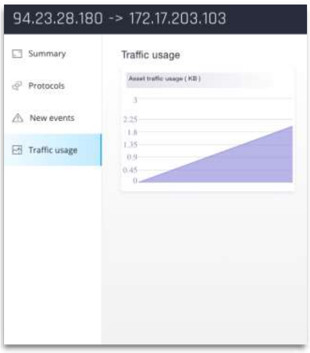
3. Click the View details icon.

A pop-up window opens displaying detailed information about the selected link.









Summary of device: Name, type, IP, state and MAC address, number of protocols and new events associated with the device.

- Click Protocols to display protocol details
- Click New events to display new event details

Status of each protocol

New events associated with the device. Add a comment, download, or archive an event

Asset traffic usage of each device

Search for links

1. Go to the Links pane (Network visibility > Links).
2. Use the search tools and Links Filter Lists to search for items
3. Click the Filter icon.

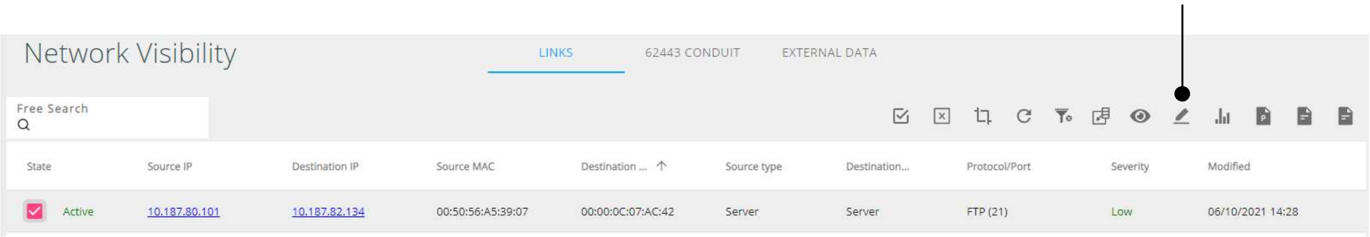
The item list automatically refreshes and displays only those items matching the search filters.

Links Filter Lists

First Level Search Filter	Second Level Search Filter	Third Level Search Filter
First seen	Equal to • Not equal to • Greater than • Less than	Click cursor in search field. Specify date in the pop-up calendar.
Last seen		
Severity		Use arrows to specify required value
Session		
Silence Time (s)		
Port		
ID		
State	Like • Not Like	Active Inactive
Device 1		Enter free text in search field
Device 2		
Protocol		
Transport	Equal to Not equal to	UDP TCP ICMP
Device 1 Type	Equal to Not equal to	PLC Server HMI Engineering Station Broadcast Multicast Router Historian OPC Server
Device 2 Type		

Link Inactivity

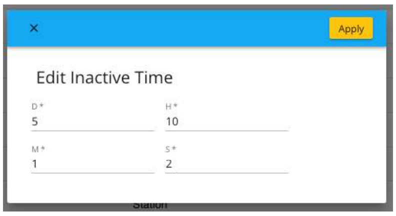
In the Links pane, you can edit the inactive times assigned to links. Any edits override the global notification settings for the links, meaning the device/link inactivity time will be changed by the edits.



State	Source IP	Destination IP	Source MAC	Destination ...	Source type	Destination...	Protocol/Port	Severity	Modified
☑ Active	10.187.80.101	10.187.82.134	00:50:56:A5:39:07	00:00:0C:07:AC:42	Server	Server	FTP (21)	Low	06/10/2021 14:28

Edit the inactive time assigned to links

1. Go to the Links pane (Network visibility > Links).
2. Select the checkbox of the device/link you wish to edit.
3. Click the Edit inactive time icon. The Edit Inactive Time pop-up window opens.



Edit Inactive Time

D * 5
H * 10
M * 1
S * 2

4. Specify the inactive time (days, hours, minutes, seconds) for the individual device/link
5. Click Apply. A message confirms the changes have been successfully implemented.

IEC 62443 Conduit

Assets are automatically classified to the relevant zone according to IEC 62443 standards.

In 62443 Conduit you can do the following:

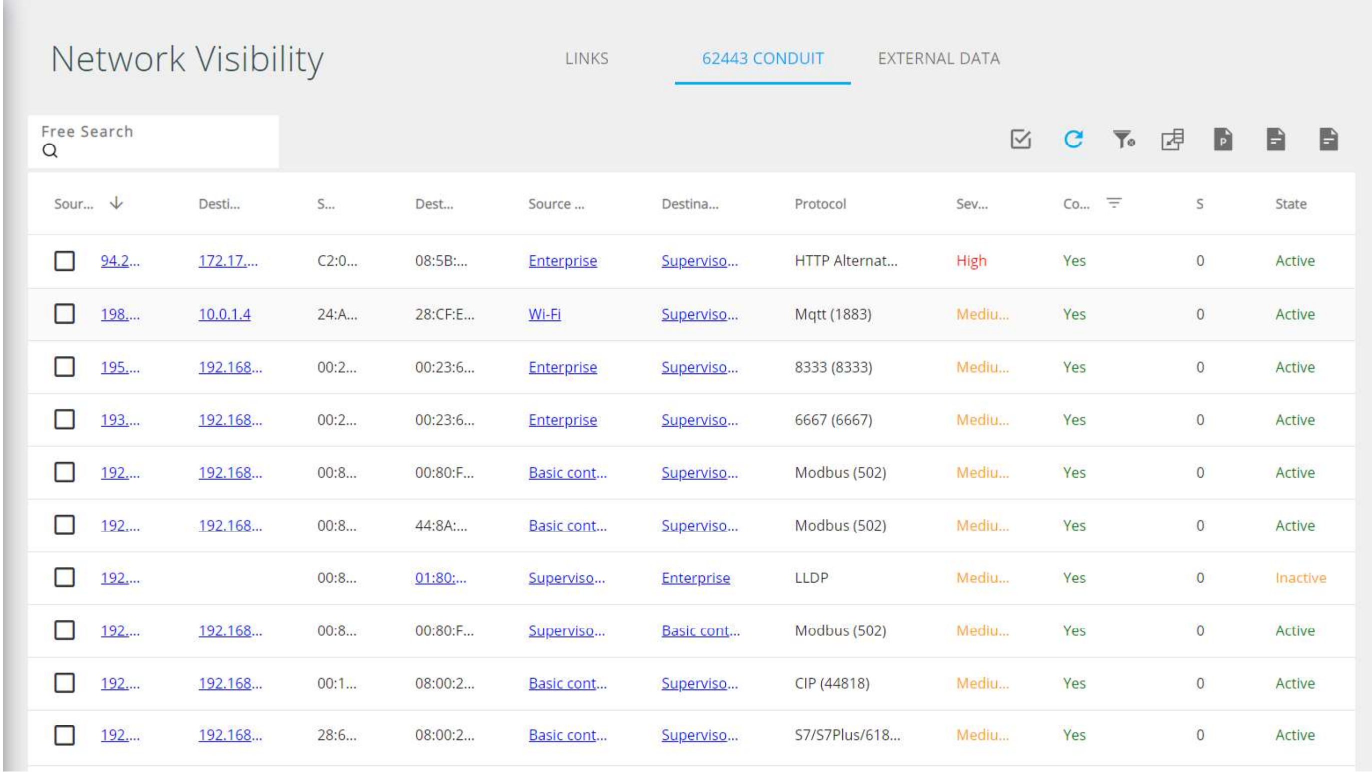
- View 62443 Conduit details
- Search for conduits

View 62443Conduit Details

In the 62443 Conduit pane, quickly glance at general information or view more details about each conduit on the network.

View general information about a conduit

Go to the 62443 Conduit pane (Network visibility > 62443 Conduit).
The 62443 Conduit pane opens displaying the general information about each conduit on the network.



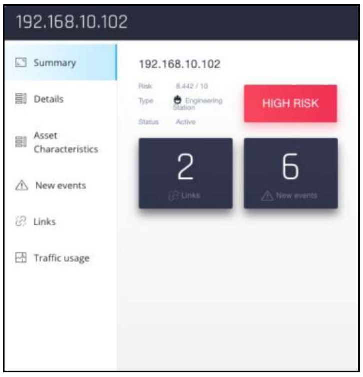
	Sour... ↓	Desti...	S...	Dest...	Source ...	Destina...	Protocol	Sev...	Co...	S	State
☐	94.2...	172.17....	C2:0...	08:5B:...	Enterprise	Superviso...	HTTP Alternat...	High	Yes	0	Active
☐	198....	10.0.1.4	24:A...	28:CF:E...	Wi-Fi	Superviso...	Mqtt (1883)	Mediu...	Yes	0	Active
☐	195....	192.168...	00:2...	00:23:6...	Enterprise	Superviso...	8333 (8333)	Mediu...	Yes	0	Active
☐	193....	192.168...	00:2...	00:23:6...	Enterprise	Superviso...	6667 (6667)	Mediu...	Yes	0	Active
☐	192....	192.168...	00:8...	00:80:F...	Basic cont...	Superviso...	Modbus (502)	Mediu...	Yes	0	Active
☐	192....	192.168...	00:8...	44:8A:...	Basic cont...	Superviso...	Modbus (502)	Mediu...	Yes	0	Active
☐	192....		00:8...	01:80:...	Superviso...	Enterprise	LLDP	Mediu...	Yes	0	Inactive
☐	192....	192.168...	00:8...	00:80:F...	Superviso...	Basic cont...	Modbus (502)	Mediu...	Yes	0	Active
☐	192....	192.168...	00:1...	08:00:2...	Basic cont...	Superviso...	CIP (44818)	Mediu...	Yes	0	Active
☐	192....	192.168...	28:6...	08:00:2...	Basic cont...	Superviso...	S7/S7Plus/618...	Mediu...	Yes	0	Active

- Search for items based on specific criteria
- Change the item order
- Show and hide columns
- Choose how many items to view per page

View details about a conduit

1. Go to the 62443 Conduit pane (Network visibility > 62443 Conduit).
2. Click the Source IP, Destination IP, Source Zone or Destination Zone to open an info card on the selected column.

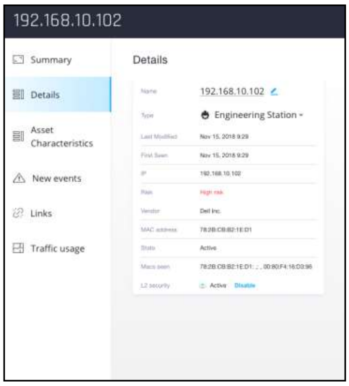
Click through each tab in the pop-up window to view and edit details:



192.168.10.102
Risk 8.442 / 10
Type Engineering Station
Status Active
2 Links
6 New events

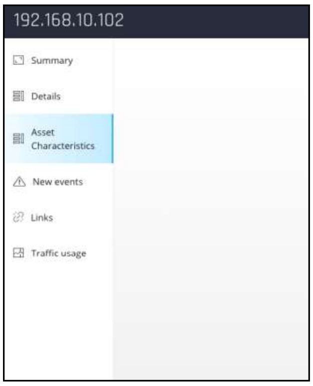
View the IP address, risk, device type, status, and number of links and events associated to the device

- Click Links to view link details
- Click New events to view event details
- (Optional) Add a **comment**

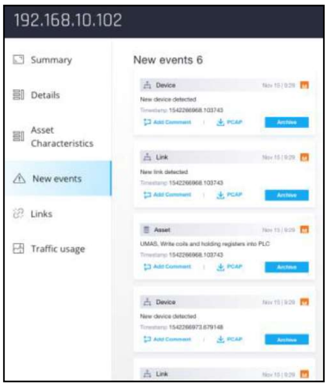


Name 192.168.10.102
Type Engineering Station
Last Modified Nov 15, 2018 9:29
First Seen Nov 15, 2018 9:29
IP 192.168.10.102
Risk High risk
Vendor Dell Inc.
MAC address 78:2B:CB:B2:1E:D1
State Active
Macs seen 78:2B:CB:B2:1E:D1: ; , 00:80:F4:18:D3:96
L2 security Active

- View the device details
- Edit a device name
- Edit a device type
- Edit the L2 security settings



- View the device operating system



Device Nov 15 | 9:29
New device detected
Timestamp 1542266968.103743

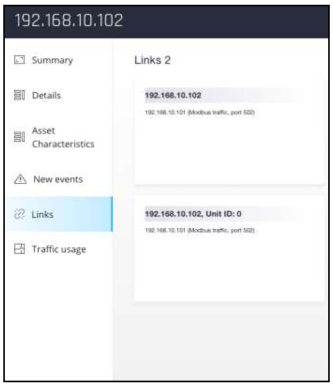
Link Nov 15 | 9:29
New link detected
Timestamp 1542266968.103743

Asset Nov 15 | 9:29
UMAS. Write coils and holding registers into PLC
Timestamp 1542266968.103743

Device Nov 15 | 9:29
New device detected
Timestamp 1542266973.679148

Link Nov 15 | 9:29

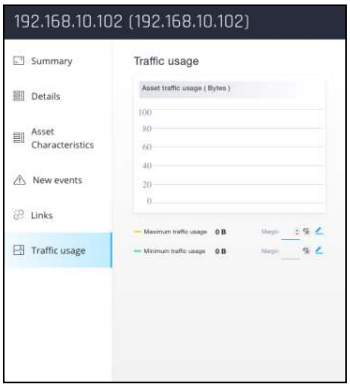
- View new events associated with this device
- Add a comment, download, or archive an



192.168.10.102
192.168.10.101 (Modbus traffic, port 502)

192.168.10.102, Unit ID: 0
192.168.10.101 (Modbus traffic, port 502)

- View links to other IP addresses



- View the current minimum and maximum traffic thresholds
- Edit the traffic usage thresholds for this device

62443 Zones

Zone

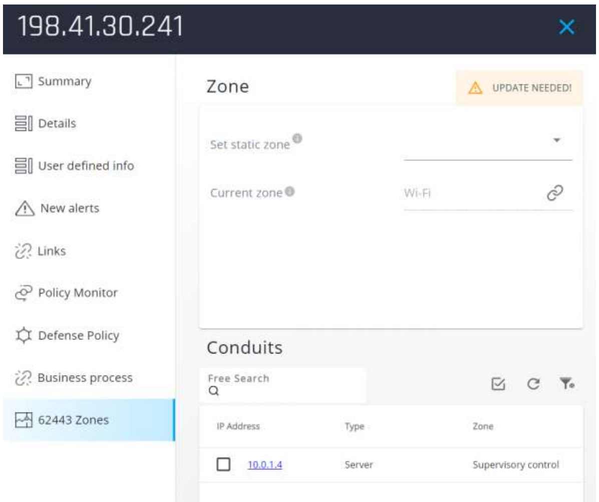
In the 62443 Zone tab you can set any zone to static

- Once the static zone is set, system detection is not taken into consideration
- To revert to default detection, click **Cancel**

The current zone displays the zone that the asset is classified to. This takes into consideration the asset's characteristics and the IEC 62443 standard. The current zone is set either automatically, according to the iSID algorithm, or manually according to user preference.

Conduits

You can search for relevant conduits according to IP, Type and Zone.x



Zone

Set static zone

Current zone: Wi-Fi

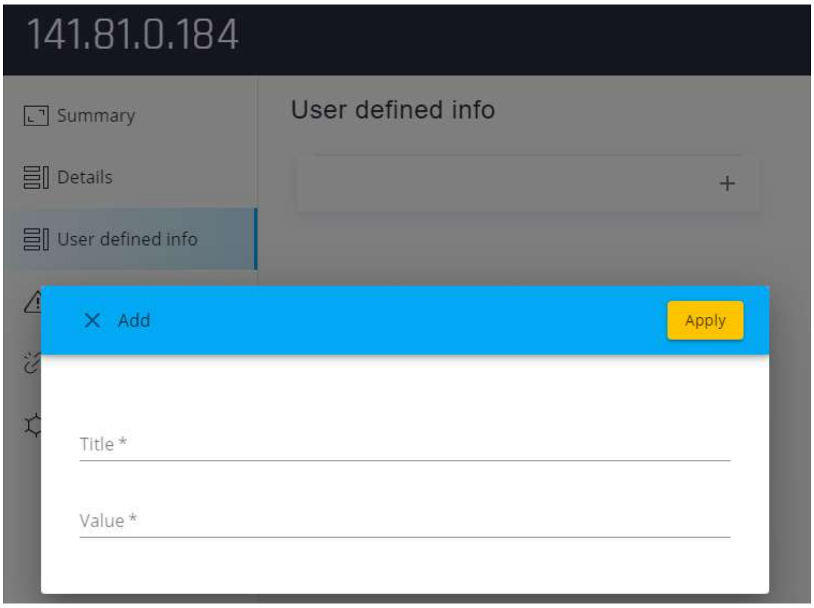
Conduits

	IP Address	Type	Zone
□	10.0.1.4	Server	Supervisory control

User defined info

To add your own, custom fields to the selected device:

1. Select the User defined info tab and click on the Add + icon (top, right).
2. Fill in a field title and value and Apply:



User defined info

Title *

Value *

Search for 62443 Conduits

Use the search tools to search for specific devices

Filter the list

- Use the search tools and 62443 Conduit Filter Lists to search for a specific item

1. Click the Filter icon.

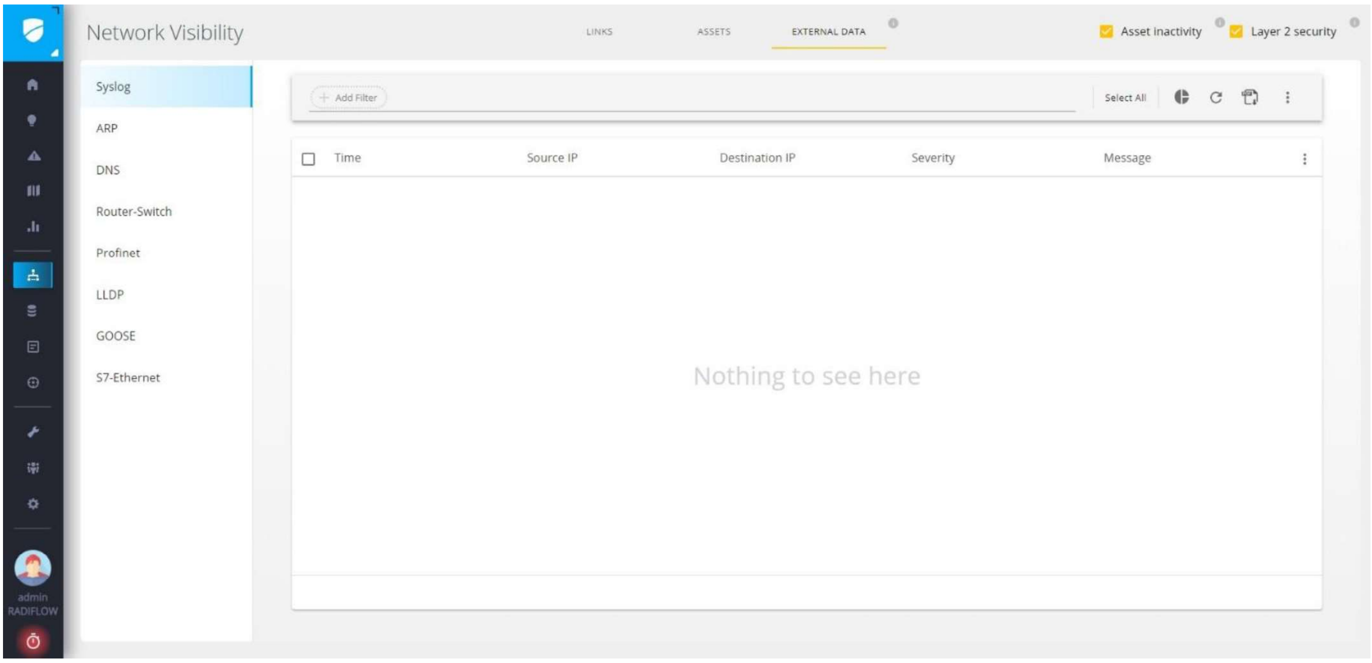
The item list automatically refreshes and displays only those items matching the search filters.

62443 Conduit Filter Lists

First Level Search Filter	Second Level Search Filter	Third Level Search Filter
First seen	Equal to • Not equal to • Greater than • Less than	Click cursor in search field. Specify date in the pop-up calendar.
Last seen		
State	Like • Not Like	Inactive • Active
Device Name		Enter free text in search field
IP		
MAC		
Vendor Name		
Behind Router	Equal to • Not equal to • Greater than • Less than	Yes • No
ID		Use arrows to specify required value
Type	Equal to Not equal to	PLC Server HMI Engineering Station Broadcast Multicast Router Historian OPC Server User-defined types

External Data

In addition to the data described above, iSID also collects external network information - i.e. information that is not necessarily related to a specific iSID asset, or to layer 2 data. This data is provided to the user for enriched visibility, under the External Data tab:



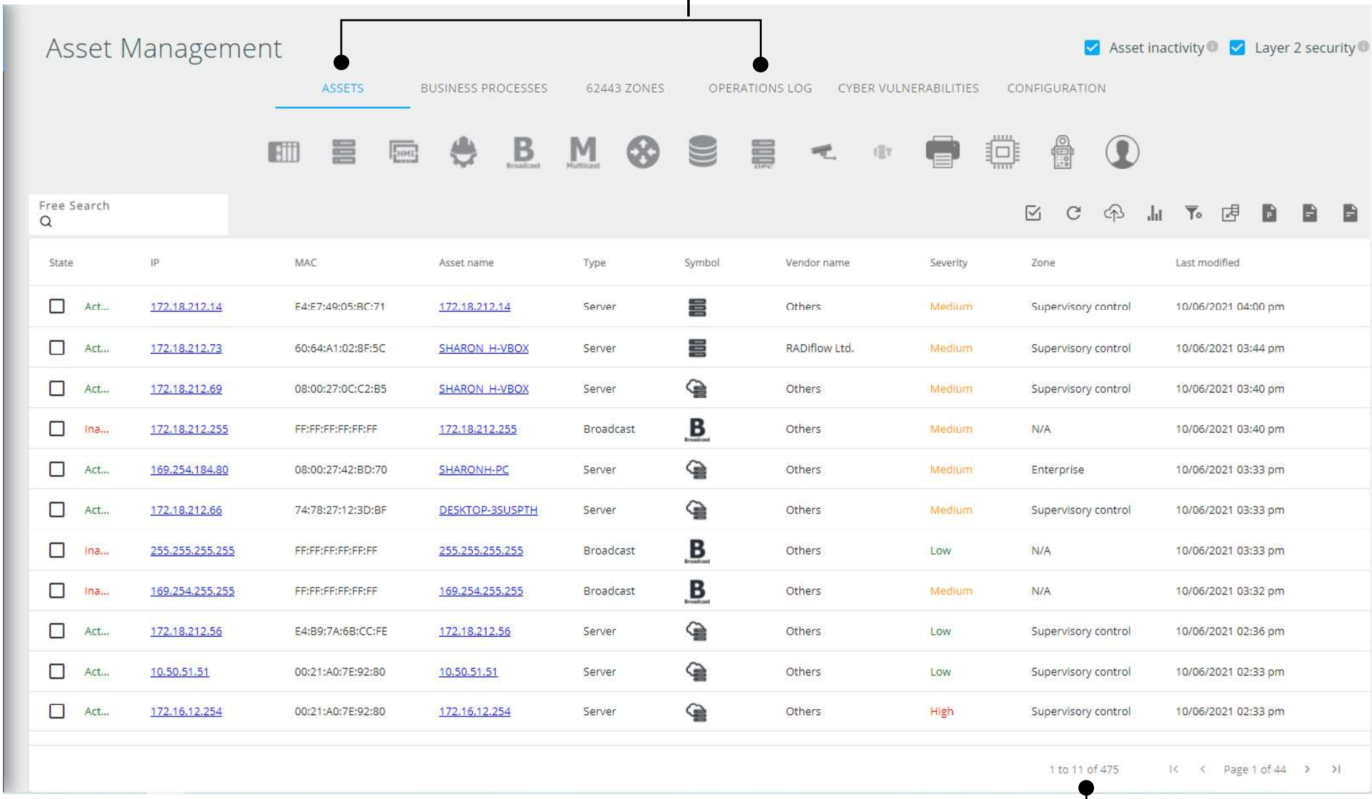
Asset Management

The iSID Asset Management monitors dedicated SCADA device operations such as read/write, download, and CPU start/stop.

Go to the Asset Management pane to view and manage the following:

- Assets - view device details, events, links, and traffic usage configuration
- Business Processes -
- Operations Log - view the operational actions between the configured SCADA devices on the network
- Cyber Vulnerabilities - common vulnerabilities and exposure details
- Configuration - configure what action is triggered in response to a specific operation

Click to view and manage the operations of all devices in the monitored network



	State	IP	MAC	Asset name	Type	Symbol	Vendor name	Severity	Zone	Last modified
□	Act...	172.18.212.14	E4:E7:49:05:BC:71	172.18.212.14	Server	☰	Others	Medium	Supervisory control	10/06/2021 04:00 pm
□	Act...	172.18.212.73	60:64:A1:02:8F:5C	SHARON_H-VBOX	Server	☰	RADiflow Ltd.	Medium	Supervisory control	10/06/2021 03:44 pm
□	Act...	172.18.212.69	08:00:27:0C:C2:B5	SHARON_H-VBOX	Server	☁	Others	Medium	Supervisory control	10/06/2021 03:40 pm
□	Ina...	172.18.212.255	FF:FF:FF:FF:FF:FF	172.18.212.255	Broadcast	B	Others	Medium	N/A	10/06/2021 03:40 pm
□	Act...	169.254.184.80	08:00:27:42:BD:70	SHARONH-PC	Server	☁	Others	Medium	Enterprise	10/06/2021 03:33 pm
□	Act...	172.18.212.66	74:78:27:12:3D:BF	DESKTOP-3SUSPTH	Server	☁	Others	Medium	Supervisory control	10/06/2021 03:33 pm
□	Ina...	255.255.255.255	FF:FF:FF:FF:FF:FF	255.255.255.255	Broadcast	B	Others	Low	N/A	10/06/2021 03:33 pm
□	Ina...	169.254.255.255	FF:FF:FF:FF:FF:FF	169.254.255.255	Broadcast	B	Others	Medium	N/A	10/06/2021 03:32 pm
□	Act...	172.18.212.56	E4:B9:7A:6B:CC:FE	172.18.212.56	Server	☁	Others	Low	Supervisory control	10/06/2021 02:36 pm
□	Act...	10.50.51.51	00:21:A0:7E:92:80	10.50.51.51	Server	☁	Others	Low	Supervisory control	10/06/2021 02:33 pm
□	Act...	172.16.12.254	00:21:A0:7E:92:80	172.16.12.254	Server	☁	Others	High	Supervisory control	10/06/2021 02:33 pm

1 to 11 of 475 |< < Page 1 of 44 > >|

Number of Assets

Assets

Go to Asset Management Devices pane to do the following:

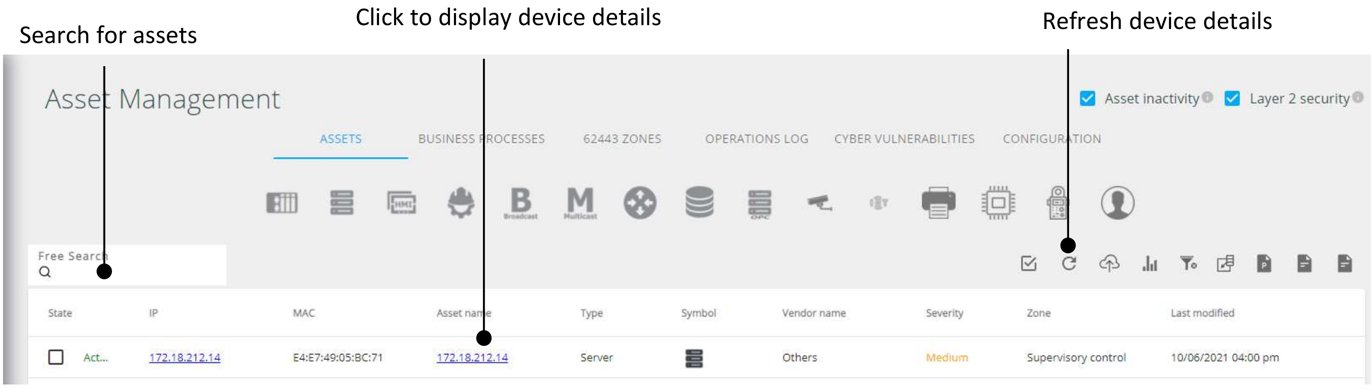
- View device details, events, links, and traffic usage configuration
- Edit device names and types
- Edit the traffic usage thresholds per each device

View Asset Information

In the Assets pane, quickly glance at general device information or view more details about each device on the network.

View general asset information

Go to the Assets pane (Asset management > Assets).
The Assets pane opens displaying the general information about each device on the network.



Search for assets

Click to display device details

Refresh device details

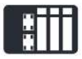
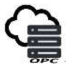
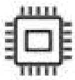
	State	IP	MAC	Asset name	Type	Symbol	Vendor name	Severity	Zone	Last modified
□	Act...	172.18.212.14	E4:E7:49:05:BC:71	172.18.212.14	Server	☰	Others	Medium	Supervisory control	10/06/2021 04:00 pm

View the date and time a device was last modified, the device state, name, IP address, type, MAC address, vendor name, router details, and ID number.
Note: Device types and specific details associated to individual devices are represented by icons, see Device Type Icons.

- Search for items based on specific criteria
- Change the item order
- Show and hide columns
- Choose how many items to view per page

In the Assets pane, the device types are represented by the following icons:

Device Type Icons

	PLC		Router
	Server		Historian
	HMI		OPC Server
	Engineering Station		Camera
	Broadcast		IOT
	Multicast		Printer
	User-defined type		A cloud alongside an icon of a device denotes that the device is behind a router
	Layer 2 device		

Upload asset information

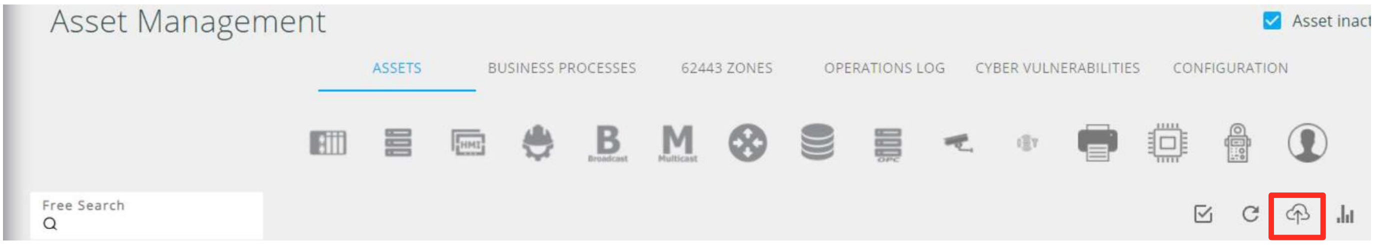
You can update asset information by uploading that information from an excel or csv file.

The columns in the file must be as follows:

1. IP_address
2. device_name
3. device_type
4. device_mac
5. vendor

Although all columns are required, it is not required to fill all cells in every row. If specific information does not need to be updated you can leave the relevant cell empty.

1. Go to the Assets pane (Asset Management > Assets).
2. Click on Upload.

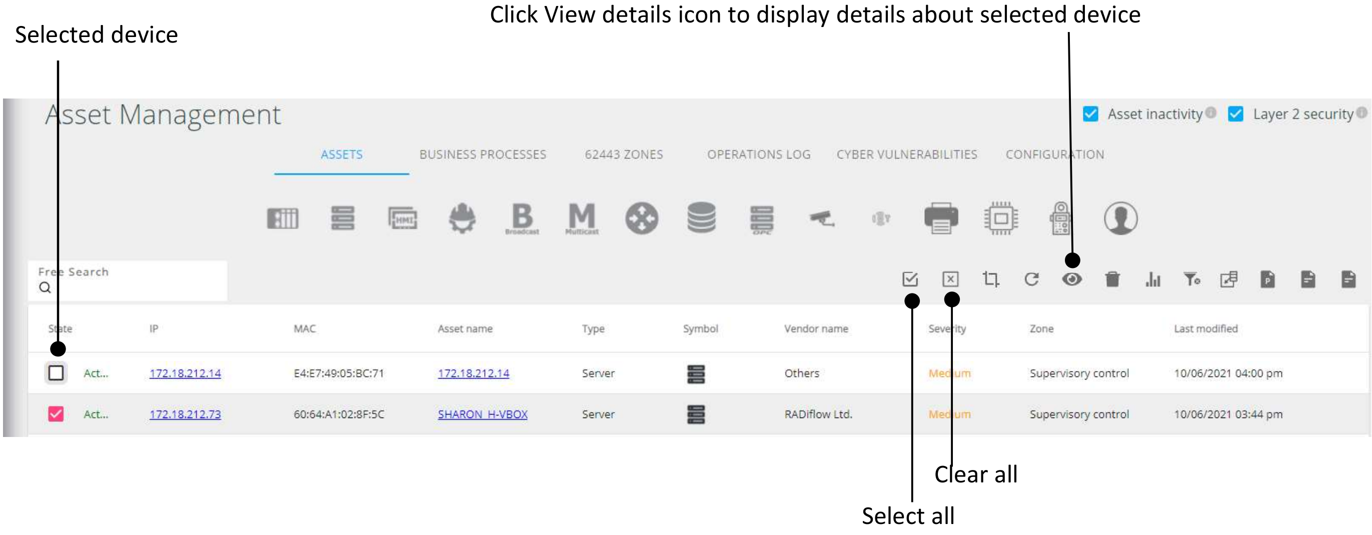


3. In the Update devices information pop up window, click OK.
4. In the Update devices pop up window, click Choose file to browse to the file.
5. Click Apply.

View in-depth details about an asset

1. Go to the Assets pane (Asset Management > Assets).
2. Select the checkbox of the device you wish to view in-depth details about.

The View details icon appears in the top right corner of the pane.



Selected device

Click View details icon to display details about selected device

State	IP	MAC	Asset name	Type	Symbol	Vendor name	Severity	Zone	Last modified
□ Act...	172.18.212.14	E4:E7:49:05:BC:71	172.18.212.14	Server		Others	Medium	Supervisory control	10/06/2021 04:00 pm
☑ Act...	172.18.212.73	60:64:A1:02:8F:5C	SHARON_H-VBOX	Server		RADiflow Ltd.	Medium	Supervisory control	10/06/2021 03:44 pm

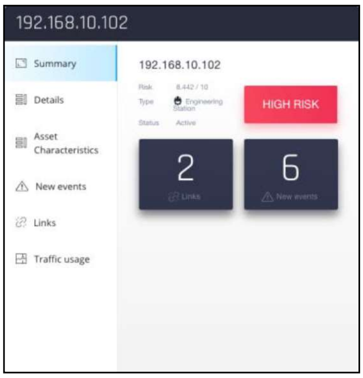
Clear all

Select all

3. Click the View details icon.

A pop-up window opens displaying a summary of the device.

Click through the pop-up window to view and edit individual device details.



192.168.10.102

Risk 8.442 / 10

Type Engineering Station

Status Active

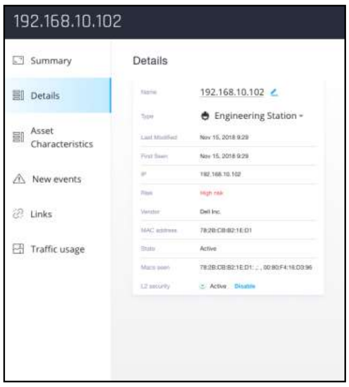
HIGH RISK

2 Links

6 New events

View the IP address, risk, device type, status, and number of links and events associated to the device

- Click Links to view link details
- Click New events to view



Details

Name 192.168.10.102

Type Engineering Station

Last Modified Nov 15, 2018 9:29

First Seen Nov 15, 2018 9:29

IP 192.168.10.102

Risk High risk

Vendor Dell Inc.

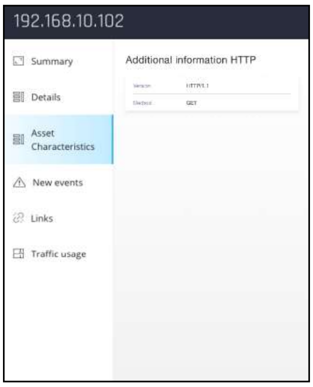
MAC address 78:2B:CB:B2:1E:D1

State Active

Macs seen 78:2B:CB:B2:1E:D1: , , 00:80:F4:16:D3:96

L2 security Active Disable

- View the device details
- Edit a device name
- Edit a device type
- Edit the L2 security

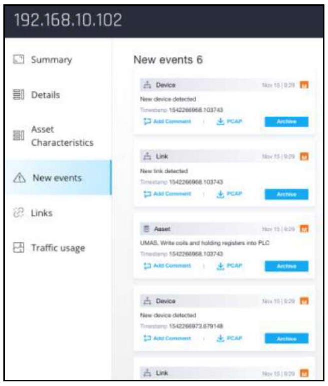


Additional information HTTP

Version HTTP/1.1

Method GET

- View the asset characteristics



New events 6

Device Nov 15 | 9:29

New device detected

Timestamp 1542266968.103743

Add Comment | PCAP Archive

Link Nov 15 | 9:29

New link detected

Timestamp 1542266968.103743

Add Comment | PCAP Archive

Asset Nov 15 | 9:29

UMAS. Write coils and holding registers into PLC

Timestamp 1542266968.103743

Add Comment | PCAP Archive

Device Nov 15 | 9:29

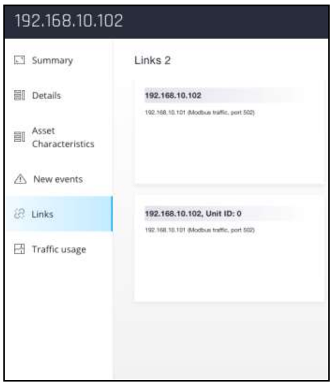
New device detected

Timestamp 1542266973.679148

Add Comment | PCAP Archive

Link Nov 15 | 9:29

- View new events associated with this device
- Add a comment, download, or archive an



Links 2

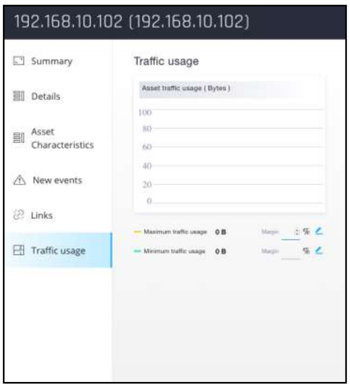
192.168.10.102

192.168.10.101 (Modbus traffic, port 502)

192.168.10.102, Unit ID: 0

192.168.10.101 (Modbus traffic, port 502)

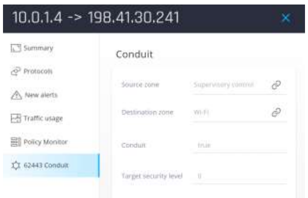
- View links to other IP addresses



Maximum traffic usage 0 B Margin %

Minimum traffic usage 0 B Margin %

- View the current minimum and maximum traffic thresholds
- Edit the traffic usage thresholds for this device



10.0.1.4 -> 198.41.30.241

Conduit

Source zone: Supervisory control

Destination zone: Wi-Fi

Conduit: true

Target security level: 0

- View the Conduit Source and Destination Zones

Search for specific assets

1. Go to the Assets pane (Asset management > Assets).
2. Use the search tools and Devices Filter Lists to search for a specific item.
3. Click the Filter icon.

The item list automatically refreshes and displays only those items matching the search filters.

Devices Filter Lists

First Level Search Filter	Second Level Search Filter	Third Level Search Filter
First seen	• **Equal to** • Not equal to • Greater than • Less than	**Click cursor in search field.** **Specify date in the pop-up calendar.**
Last seen		
State	• **Like** • Not Like	• **Inactive** • Active
Device Name		**Enter free text in search field**
IP		
MAC		
Vendor Name		
Behind Router	• **Equal to** • Not equal to • Greater than • Less than	• **Yes** • No
ID		**Use arrows to specify required value**
Type	• **Equal to** • **Not equal to**	• **PLC** • **Server** • **HMI** • **Engineering Station** • **Broadcast** • **Multicast** • **Router** • **Historian** • **OPC Server**

Change asset details

In the Assets pane, change the following device details:

- Name and type
- L2 security settings

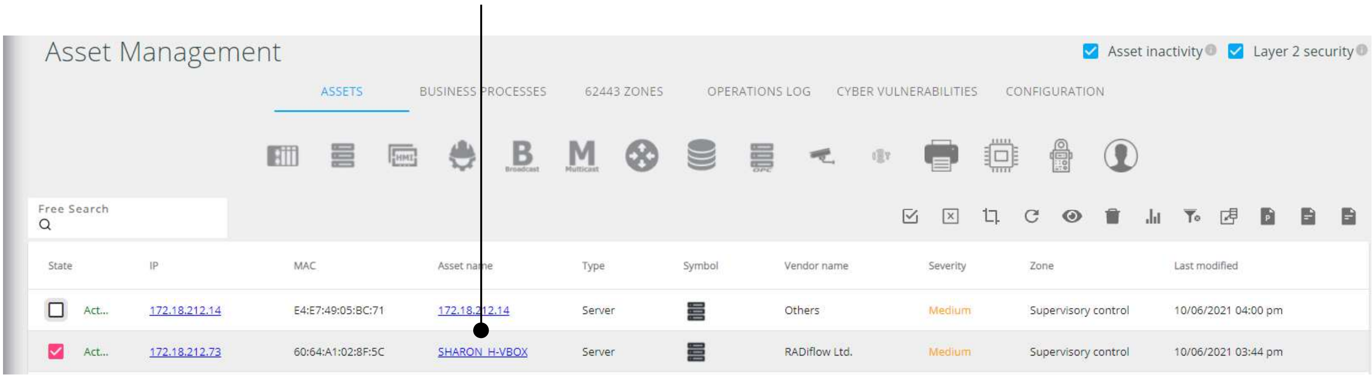
Change the name and type of device

The device name and type can be changed either via the Edit icon or the View details icon.

This procedure describes how to change the name and type of the device via the Edit Detail icon.

1. Go to the Assets pane (Asset management > Assets).
2. Select the checkbox of the device you wish to edit.

Click on the device name



Asset Management

☑ Asset inactivity ☑ Layer 2 security

State		IP	MAC	Asset name	Type	Symbol	Vendor name	Severity	Zone	Last modified
□	Act...	172.18.212.14	E4:E7:49:05:BC:71	172.18.212.14	Server		Others	Medium	Supervisory control	10/06/2021 04:00 pm
☑	Act...	172.18.212.73	60:64:A1:02:8F:5C	SHARON_H-VBOX	Server		RADiflow Ltd.	Medium	Supervisory control	10/06/2021 03:44 pm

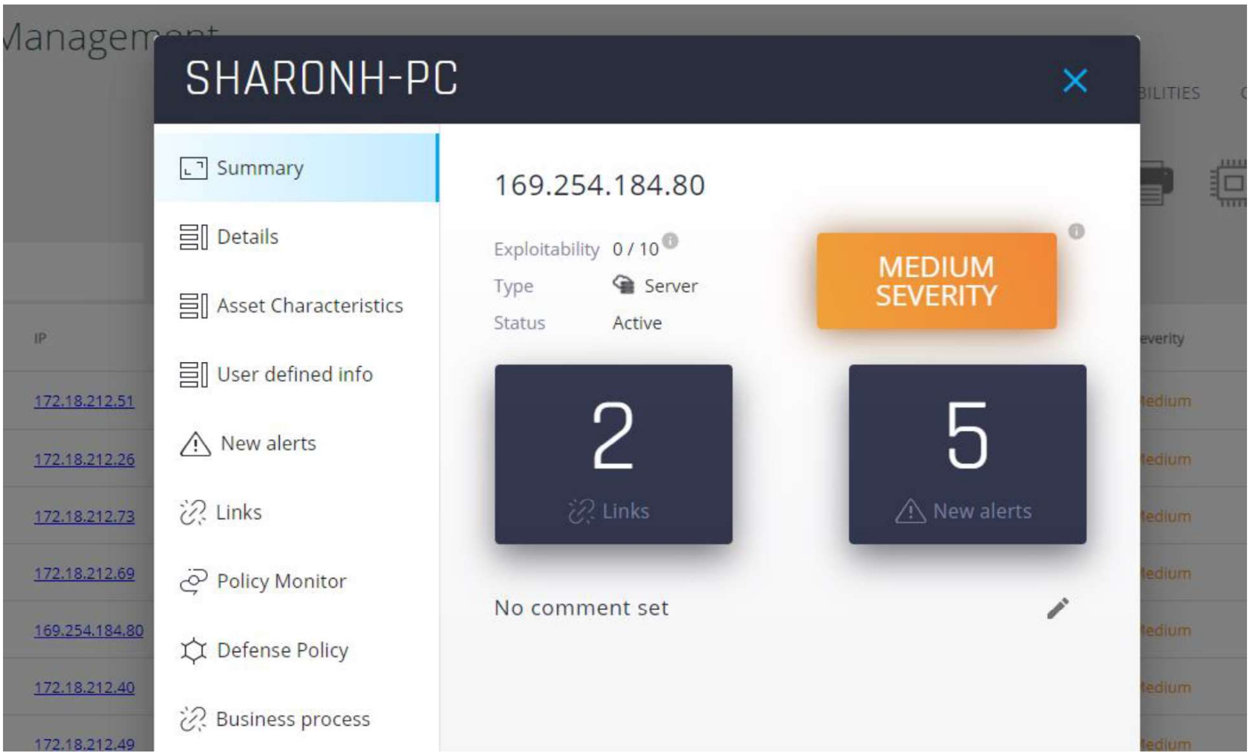
Change the name and type of device

The device name and type can be changed either via the View details icon or the Edit icon.

This procedure describes how to change the name and type of the device via the View details icon.

1. Go to the Assets pane (Asset management > Assets).

2. Click the device name or IP. A pop-up window opens displaying a summary of the device.



169.254.184.80

Exploitability 0 / 10

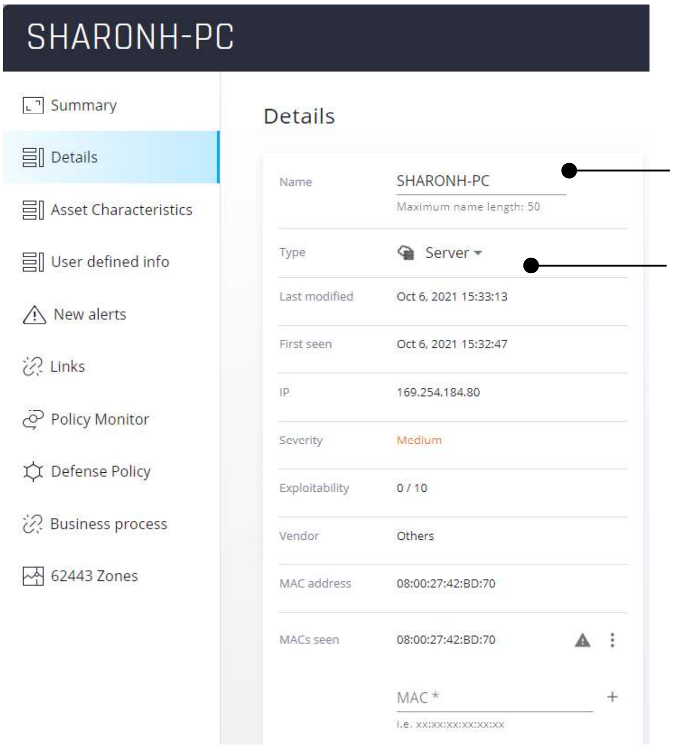
Type Server

Status Active

No comment set

3. Click the Details tab.

- Change the name of the device. The new name will appear in parentheses after the original name
- Select a new device type
- When the window closes, a message confirms the changes have been successfully implemented



Name	SHARONH-PC Maximum name length: 50
Type	Server
Last modified	Oct 6, 2021 15:33:13
First seen	Oct 6, 2021 15:32:47
IP	169.254.184.80
Severity	Medium
Exploitability	0 / 10
Vendor	Others
MAC address	08:00:27:42:BD:70
MACs seen	08:00:27:42:BD:70

MAC *

i.e. xx:xx:xx:xx:xx:xx

Change the name of the device

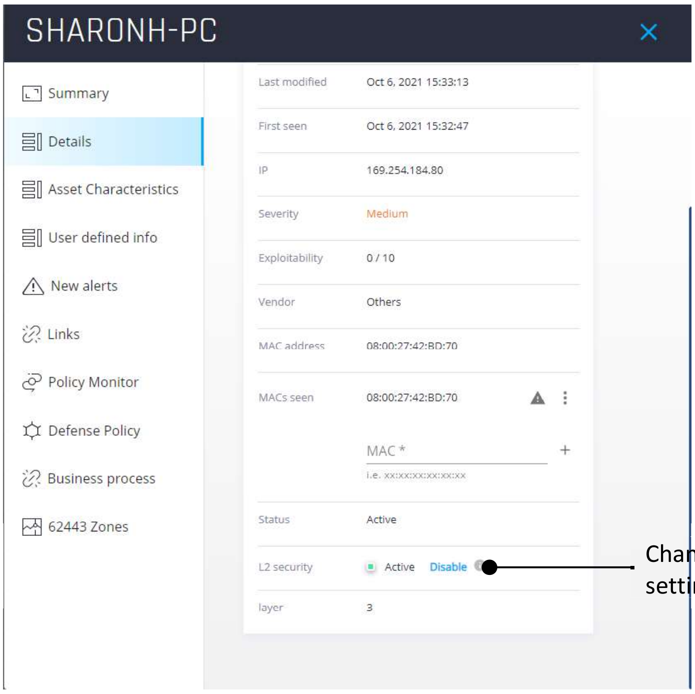
Change the type of device

Change the L2 security settings for a specific device

1. Go to the Assets pane (Asset management > Assets).
2. Select the checkbox of the device you wish to change.
3. Click the View details icon. A pop-up window opens displaying a summary of the device.
4. Click the Details tab.

- Select Active to trigger a notification when a change between the IP address and the corresponding MAC address of a network entity is detected
- Select Disable to stop triggering a notification when a change between the IP address and the corresponding MAC address of a network entity is detected

Important: Any changes override the global L2 Security settings for this specific device.



Last modified Oct 6, 2021 15:33:13

First seen Oct 6, 2021 15:32:47

IP 169.254.184.80

Severity Medium

Exploitability 0 / 10

Vendor Others

MAC address 08:00:27:42:BD:70

MACs seen 08:00:27:42:BD:70

MAC *
i.e. xx:xx:xx:xx:xx:xx

Status Active

L2 security ● Active Disable

layer 3

Change the L2 security settings for a specific device

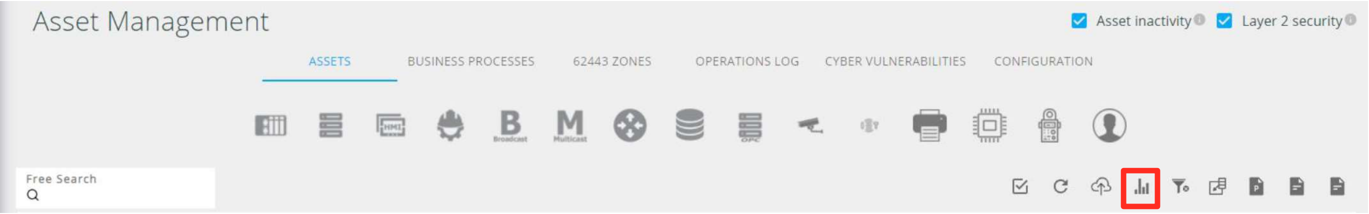
Export asset information

There are 2 ways you can export the information in the Assets pane to other formats:

- Create an iSID report
- Download to a PDF, CSV, or JSON file

Create a report

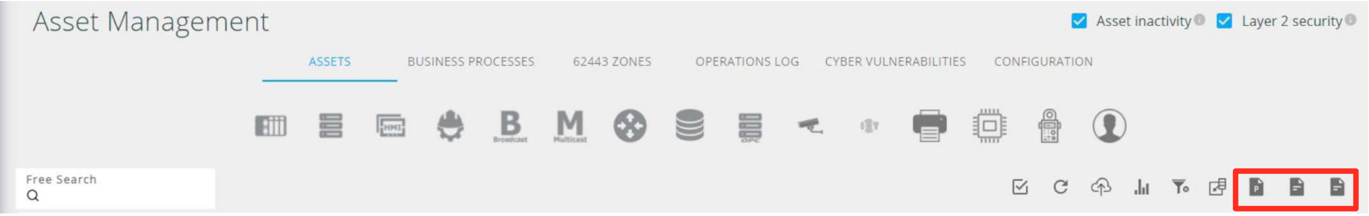
1. Go to the Assets pane (Asset Management > Assets).
2. Click on Create report.



The iSID Reports pane opens with the assets information displayed as a report that you can customize (see Create a query).

Download to a file

1. Go to the Assets pane (Asset Management > Assets).
2. Click on the menu button.
3. Select the file format.

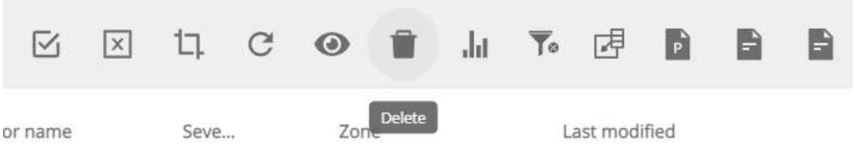


4. In the Select columns to display pop up window, select the columns to include in the file and click Apply.
5. Give the file a name, browse to the desired location and click Save.

Delete Asset

Assets can be deleted directly from the UI

1. Go to the Assets pane (Asset Management > Assets).
2. Select the checkbox of the device you wish to delete.
3. Click the Delete icon and confirm that you want to delete the selected asset(s).



It is recommended to back up your data before deleting assets from the system.

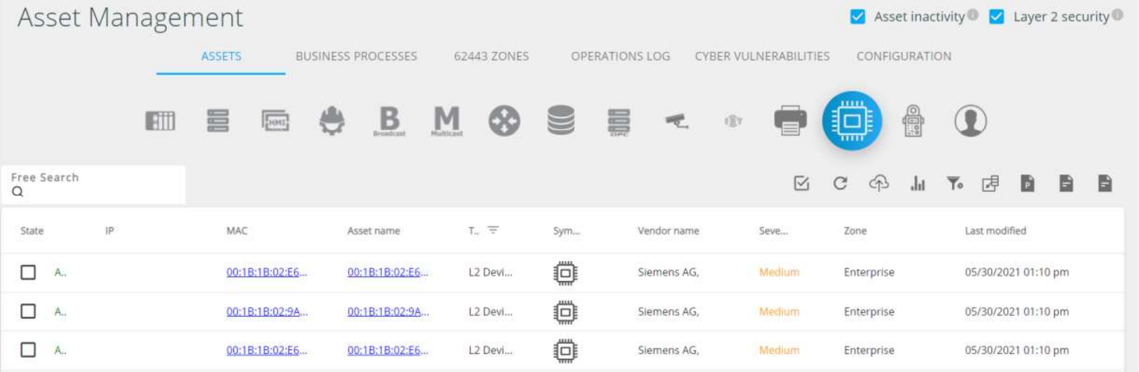
Note: During assets deletion process, the system is in ‘Idle’ mode, and a system reset is performed.

Layer 2 Asset Detection

iSiD provides system-wide support for Layer2 asset detection. It detects and analyzes Layer 2 (non-IP) assets, as well as the Layer 2 asset types.

To view Layer 2 assets:

1. Go to Asset Management. Make sure that the **Layer 2 security** checkbox is selected.
2. Click on the **L2 Device** icon



State	IP	MAC	Asset name	T..	Sym...	Vendor name	Seve...	Zone	Last modified
□ A..		00:1B:1B:02:E6...	00:1B:1B:02:E6...	L2 Devi...		Siemens AG,	Medium	Enterprise	05/30/2021 01:10 pm
□ A..		00:1B:1B:02:9A...	00:1B:1B:02:9A...	L2 Devi...		Siemens AG,	Medium	Enterprise	05/30/2021 01:10 pm
□ A..		00:1B:1B:02:E6...	00:1B:1B:02:E6...	L2 Devi...		Siemens AG,	Medium	Enterprise	05/30/2021 01:10 pm

3. Select a device and click **View**

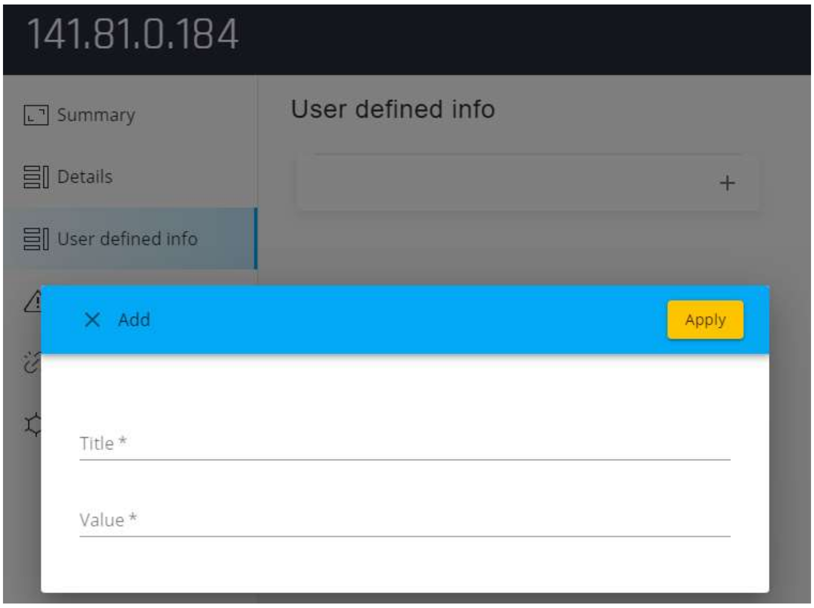
A pop-up window opens displaying a summary of the device.

Click through the pop-up window to view and edit individual device details. For more information on the L2 device details, see View in-depth details about an asset

User defined info

You can add your own custom fields to the selected L2 device:

1. Select the User defined info tab and click Add + icon (top, right).
2. Fill in the Key and Value, and click Apply:

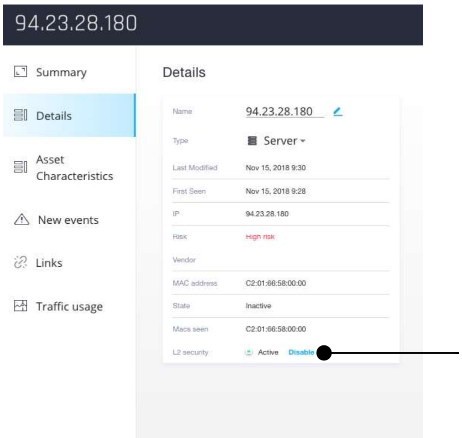


Change the L2 security settings for a specific device

1. Go to the Devices pane (Network visibility > Devices).
2. Select the checkbox of the device you wish to change.
3. Click the View details icon. A pop-up window opens displaying a summary of the device.
4. Click the Details tab.

- Select Active to trigger a notification when a change between the IP address and the corresponding MAC address of a network entity is detected
- Select Disable to stop triggering a notification when a change between the IP address and the corresponding MAC address of a network entity is detected

Important: Any changes override the global L2 Security settings for this specific device.



Name	94.23.28.180
Type	Server
Last Modified	Nov 15, 2018 9:30
First Seen	Nov 15, 2018 9:28
IP	94.23.28.180
Risk	High risk
Vendor	
MAC address	C2:01:66:58:00:00
State	Inactive
Macs seen	C2:01:66:58:00:00
L2 security	● Active Disable

Change the L2 security settings for a specific

Business Processes

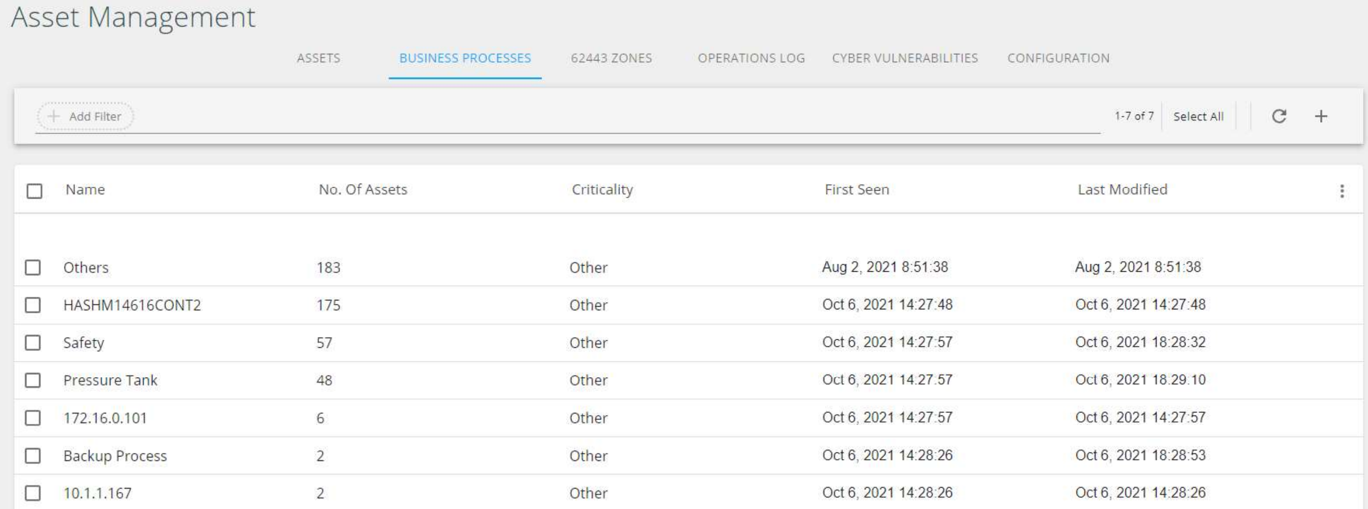
In the Asset Management Business Processes pane, you can do the following:

- Get an overview of the assets grouped by business process (see Business Processes (BPs)for more information).
- See detailed information about a selected business process.
- Attach or detach assets to/from the business process.
- Change the criticality of a business process.

View general business process information

Go to Business Processes (Asset management > Business Processes).

The Business Processes pane opens displaying business process details.



□ Name	No. Of Assets	Criticality	First Seen	Last Modified
□ Others	183	Other	Aug 2, 2021 8:51:38	Aug 2, 2021 8:51:38
□ HASHM14616CONT2	175	Other	Oct 6, 2021 14:27:48	Oct 6, 2021 14:27:48
□ Safety	57	Other	Oct 6, 2021 14:27:57	Oct 6, 2021 18:28:32
□ Pressure Tank	48	Other	Oct 6, 2021 14:27:57	Oct 6, 2021 18:29:10
□ 172.16.0.101	6	Other	Oct 6, 2021 14:27:57	Oct 6, 2021 14:27:57
□ Backup Process	2	Other	Oct 6, 2021 14:28:26	Oct 6, 2021 18:28:53
□ 10.1.1.167	2	Other	Oct 6, 2021 14:28:26	Oct 6, 2021 14:28:26

- View the number of assets, the business process ID, criticality, and when it was first seen and last modified
- Search for a business process based on specific criteria
- Change the item order
- Show and hide columns

Search for specific business processes

1. Go to Business Processes (Asset management > Business Processes).
2. Use the search tools and Business Process Filter Lists to search for a specific business process.
3. Click the Filter icon.

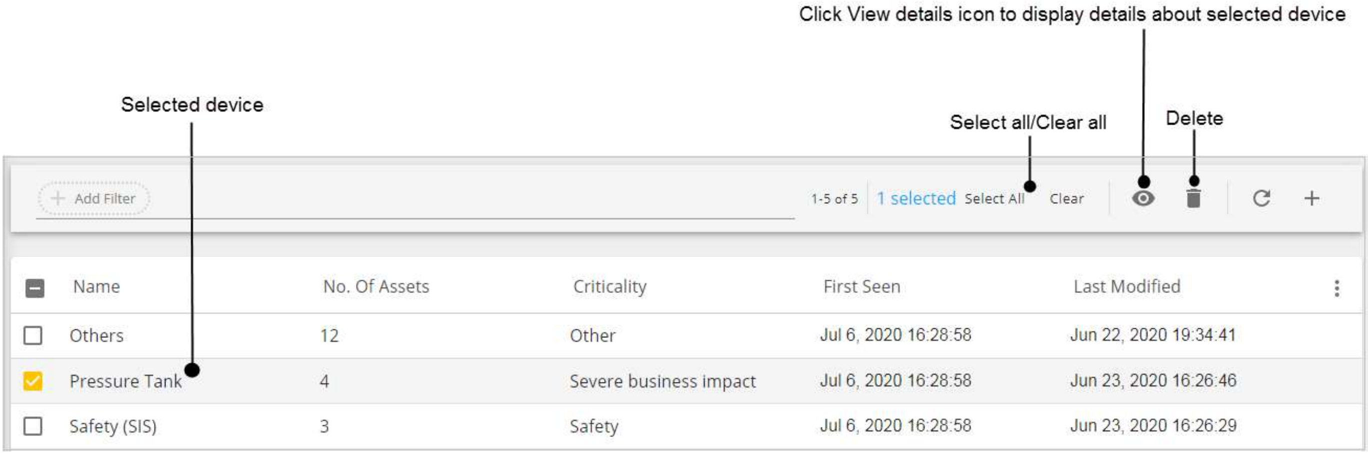
   The item list automatically refreshes and displays only those items matching the search filters.

Business Process Filter Lists

First Level Search Filter	Second Level Search Filter	Third Level Search Filter
Criticality	• Like • Not Like	Select from drop down list
First seen	• Equal to • Less than	Click cursor in search field. Specify date in the pop-up calendar.
Last modified		
Description	• Like • Not Like	Enter free text in search field
ID		
Name		
No. of Assets	• Equal to • Not equal to • Greater than • Less than	Use arrows to specify required value

View in-depth details about a specific business process

1. Go to Business Processes (Asset management > Business Processes).
   Select the checkbox of the process for which you want to view in-depth details.
   The View details icon (and the Delete icon) appear in the top right corner of the pane .



Click View details icon to display details about selected device

Selected device

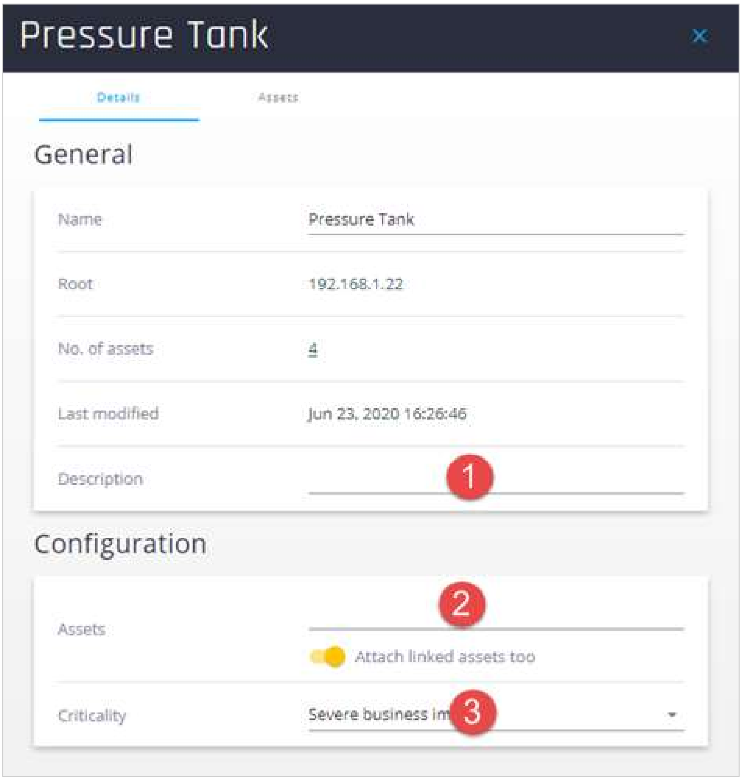
Select all/Clear all

Delete

☐	Name	No. Of Assets	Criticality	First Seen	Last Modified
☐	Others	12	Other	Jul 6, 2020 16:28:58	Jun 22, 2020 19:34:41
☑	Pressure Tank	4	Severe business impact	Jul 6, 2020 16:28:58	Jun 23, 2020 16:26:46
☐	Safety (SIS)	3	Safety	Jul 6, 2020 16:28:58	Jun 23, 2020 16:26:29

2. Click the View details icon.

A pop-up window opens displaying the process details.



Pressure Tank

General

Name Pressure Tank

Root 192.168.1.22

No. of assets 4

Last modified Jun 23, 2020 16:26:46

Description

Configuration

Assets

Attach linked assets too

Criticality Severe business im

Add or edit a business process description

In the business process details pop up (Asset management > Business Processes>View details), in the General section, add or edit the description of the process (#1 above).

Edit the business process criticality

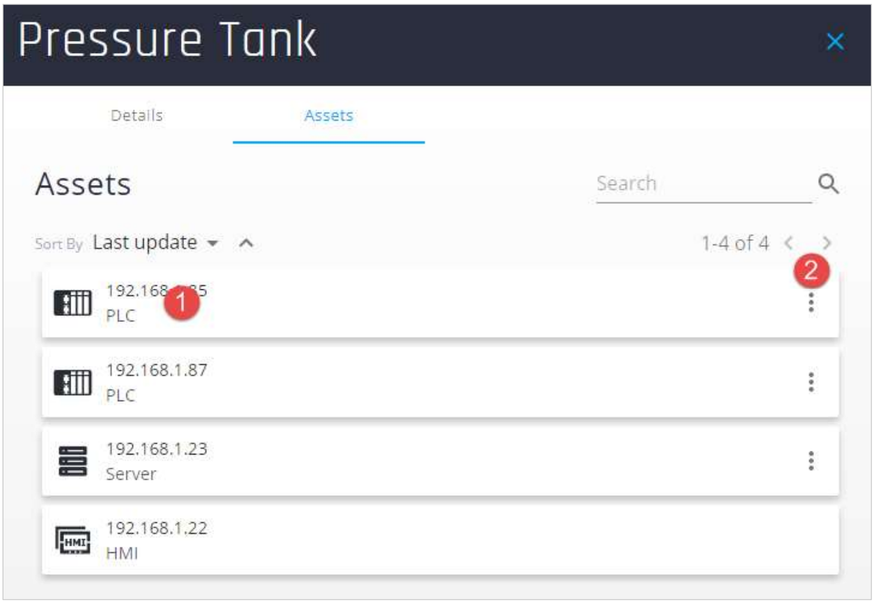
In the business process details pop up (Asset management > Business Processes>View details), in the Configuration section, select the criticality from the drop-down list (#3 above).

Attach assets

In the business process details pop up (Asset management > Business Processes>View details), in the Configuration section, click in the Assets field to display a listing of the available assets (#2 above). Use the toggle button to enable or disable attaching linked assets, also.

View the assets attached to the selected process

In the business process details pop up (Asset management > Business Processes>View details), click Assets.


Pressure Tank

Assets

192.168.1.85 PLC
192.168.1.87 PLC
192.168.1.23 Server
192.168.1.22 HMI

Detach assets

In the business process details pop up (Asset management > Business Processes>View details), click Assets to display the Assets listing. Click the menu button (#2) and select Detach asset.

View asset details

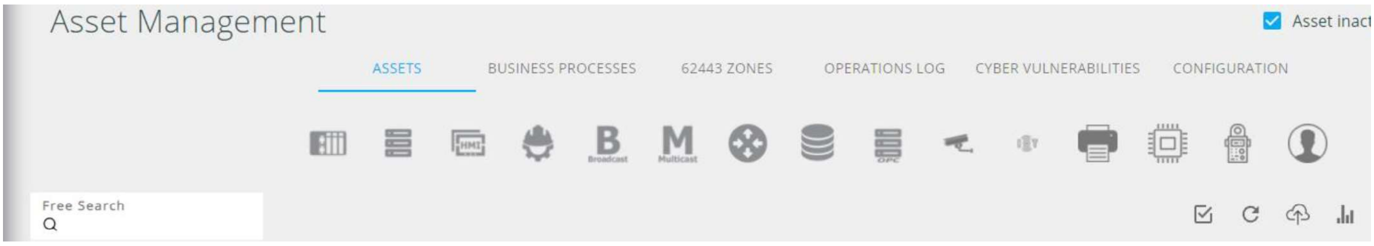
In the business process details pop up (Asset management > Business Processes>View details), click Assets to display the Assets listing. Double-click on an asset (#1) to display the asset details (see under Upload asset information

You can update asset information by uploading that information from an excel or csv file.
The columns in the file must be as follows:

6. IP_address
7. device_name
8. device_type
9. device_mac
10. vendor

Although all columns are required, it is not required to fill all cells in every row. If specific information does not need to be updated you can leave the relevant cell empty.

6. Go to the Assets pane (Asset Management > Assets).
7. Click on Upload.


Asset Management

In the Update devices information pop up window, click OK.

8. In the Update devices pop up window, click Choose file to browse to the file.
9. Click Apply.
10.

View in-depth details about an asset for information regarding asset details).

Operations Log

In the Asset Management Operations Log you can view all the operational actions between the configured SCADA Devices on the network (see Asset Management > Configuration for a list of supported devices).

View Operation Log Details

In Operations Log, quickly glance at general operation log information or view in-depth details of all the operational actions relating to network assets.

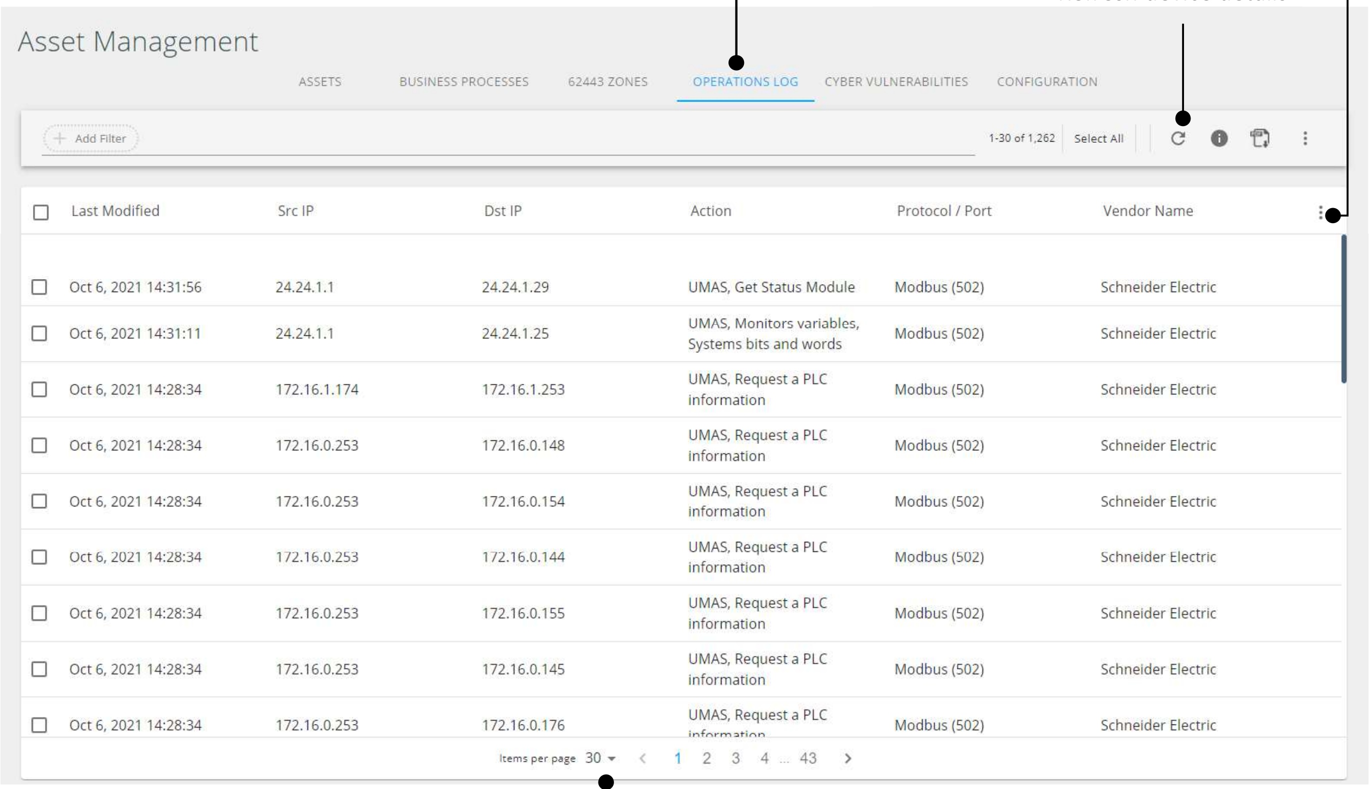
View general log information

Go to Operations Log (Asset management > Operations Log).
The Operations Log opens displaying general asset log details.

Click to show/hide columns

Click to display operation log details

Refresh device details



□	Last Modified	Src IP	Dst IP	Action	Protocol / Port	Vendor Name
□	Oct 6, 2021 14:31:56	24.24.1.1	24.24.1.29	UMAS, Get Status Module	Modbus (502)	Schneider Electric
□	Oct 6, 2021 14:31:11	24.24.1.1	24.24.1.25	UMAS, Monitors variables, Systems bits and words	Modbus (502)	Schneider Electric
□	Oct 6, 2021 14:28:34	172.16.1.174	172.16.1.253	UMAS, Request a PLC information	Modbus (502)	Schneider Electric
□	Oct 6, 2021 14:28:34	172.16.0.253	172.16.0.148	UMAS, Request a PLC information	Modbus (502)	Schneider Electric
□	Oct 6, 2021 14:28:34	172.16.0.253	172.16.0.154	UMAS, Request a PLC information	Modbus (502)	Schneider Electric
□	Oct 6, 2021 14:28:34	172.16.0.253	172.16.0.144	UMAS, Request a PLC information	Modbus (502)	Schneider Electric
□	Oct 6, 2021 14:28:34	172.16.0.253	172.16.0.155	UMAS, Request a PLC information	Modbus (502)	Schneider Electric
□	Oct 6, 2021 14:28:34	172.16.0.253	172.16.0.145	UMAS, Request a PLC information	Modbus (502)	Schneider Electric
□	Oct 6, 2021 14:28:34	172.16.0.253	172.16.0.176	UMAS, Request a PLC information	Modbus (502)	Schneider Electric

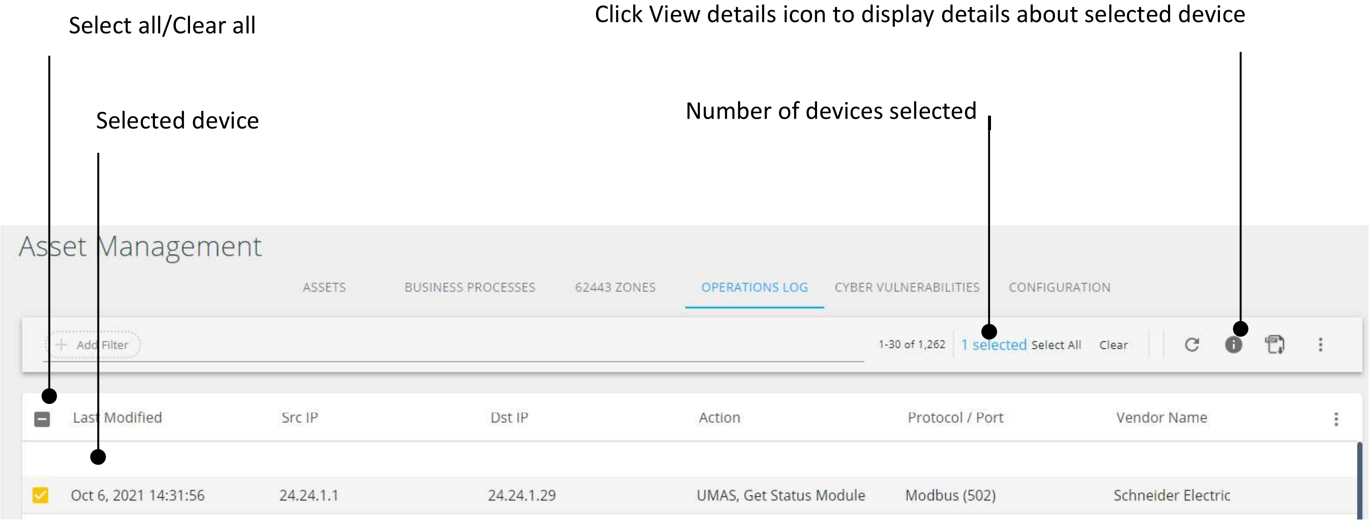
Choose how many logs to view per page

- View the date and time an asset was first/last seen, the source/destination IP, action, protocol, port, vendor name, and count
- Search for asset logs based on specific criteria
- Change the item order
- Show and hide columns
- Choose how many items to view per page

View in-depth log details about a specific asset

1. Go to Operations Log (Asset management > Operations Log).
2. Select the checkbox of the asset you wish to view in-depth details about.

The View details icon appears in the top right corner of the pane.

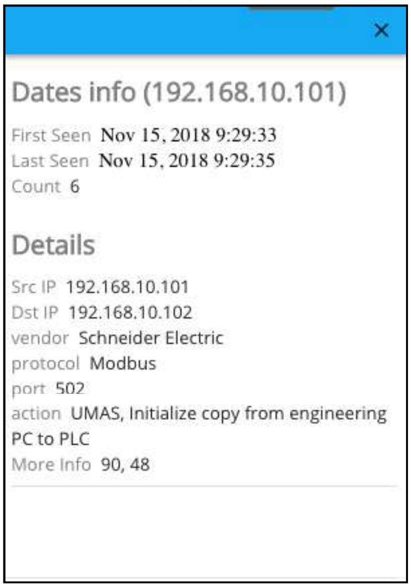


	Last Modified	Src IP	Dst IP	Action	Protocol / Port	Vendor Name
☑	Oct 6, 2021 14:31:56	24.24.1.1	24.24.1.29	UMAS, Get Status Module	Modbus (502)	Schneider Electric

3. Click the View details icon.

A pop-up window opens displaying the following details about an asset.

Date and time an asset was first/least seen, the count, the source/destination IP, vendor, protocol, port, action, and any other additional details that may be available regarding the asset.



Dates info (192.168.10.101)

First Seen Nov 15, 2018 9:29:33
Last Seen Nov 15, 2018 9:29:35
Count 6

Details

Src IP 192.168.10.101
Dst IP 192.168.10.102
vendor Schneider Electric
protocol Modbus
port 502
action UMAS, Initialize copy from engineering PC to PLC
More Info 90, 48

Search for specific asset operation logs

1. Go to Operations Log (Asset management > Operations Log).
2. Use the search tools and Operations Log Filter Lists to search for a specific asset operation log.
3. Click the Filter icon.

The item list automatically refreshes and displays only those items matching the search filters.

Operations Log Filter Lists

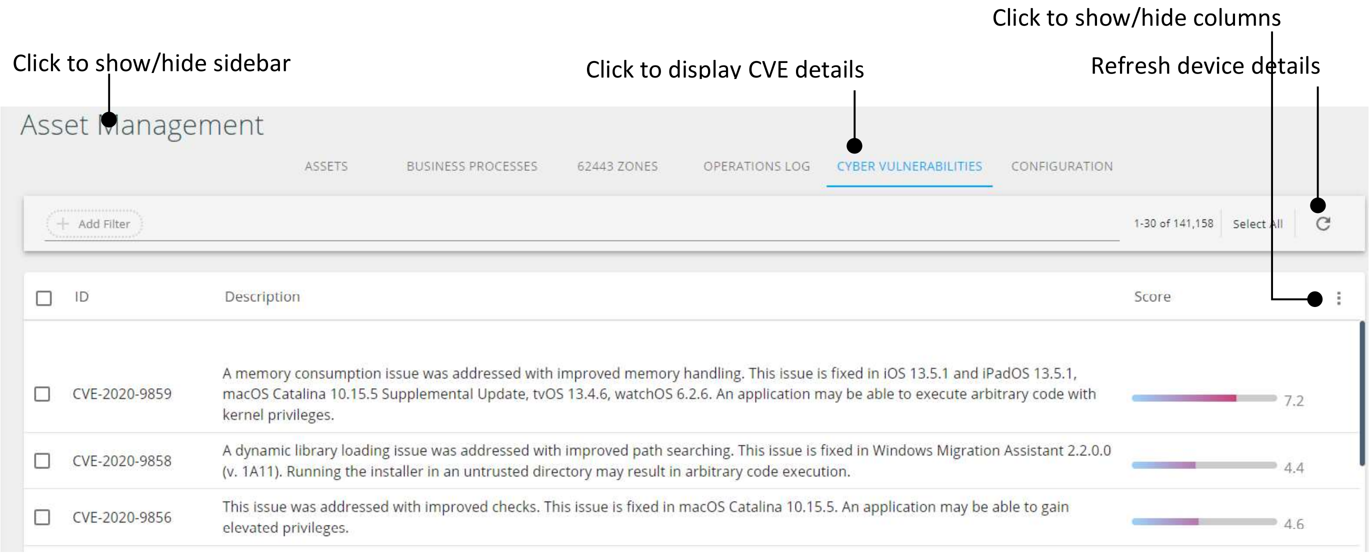
First Level Search Filter	Second Level Search Filter	Third Level Search Filter
First seen	• **Equal to** • Not equal to • Greater than • Less than	**Click cursor in search field.** **Specify date in the pop-up calendar.**
Last seen		
Src IP	• **Like** • Not Like	Enter free text in search field
Dst IP		
Action		
Protocol		
Vendor Name		
Port	• **Equal to** • Not equal to • Greater than • Less than	Use arrows to specify required value
Count		

Cyber Vulnerabilities

In Asset Management Cyber Vulnerabilities pane, you can view common vulnerabilities and exposure details.

View common vulnerabilities and exposure details

Go to Cyber Vulnerabilities (Asset management > Cyber Vulnerabilities).
The Cyber Vulnerabilities pane opens displaying common vulnerabilities and exposure details.



Click to show/hide columns

Click to show/hide sidebar

Click to display CVE details

Refresh device details

□	ID	Description	Score
□	CVE-2020-9859	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6. An application may be able to execute arbitrary code with kernel privileges.	7.2
□	CVE-2020-9858	A dynamic library loading issue was addressed with improved path searching. This issue is fixed in Windows Migration Assistant 2.2.0.0 (v. 1A11). Running the installer in an untrusted directory may result in arbitrary code execution.	4.4
□	CVE-2020-9856	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15.5. An application may be able to gain elevated privileges.	4.6

- View the unique CVE ID number, vendor, product and versions, description, score details, score
- Use the search tools and search filters to search for specific details
- Hide or show individual columns
- Change the number of items viewed per page

Search for a specific CVE

1. Go to Cyber Vulnerabilities (Asset management > Cyber Vulnerabilities).
2. Use the search tools and CVE Filter Lists to search for a specific item.
3. Click the Filter icon.

The item list automatically refreshes and displays only those items matching the search filters.

CVE Filter Lists

First Level Search Filter	Second Level Search Filter	Third Level Search Filter
ID	• **Like** • Not Like	**Enter free text in search field**
Vendor		
Description		
Attack Complexity		
Attack Vector		
Availability Impact		
Base Severity		
User Interaction		
Privileges Required		
Confidentiality Impact		
Integrity Impact		
Scope		
Version	• **Equal to** • **Not equal to**	
Product Names		
Base Score		
Labels		
Score	• **Equal to** • **Not Equal to** • **Greater than** • **Less than**	**Use arrows to specify required value**

Configuration

Go to Asset Management Configuration to do the following:

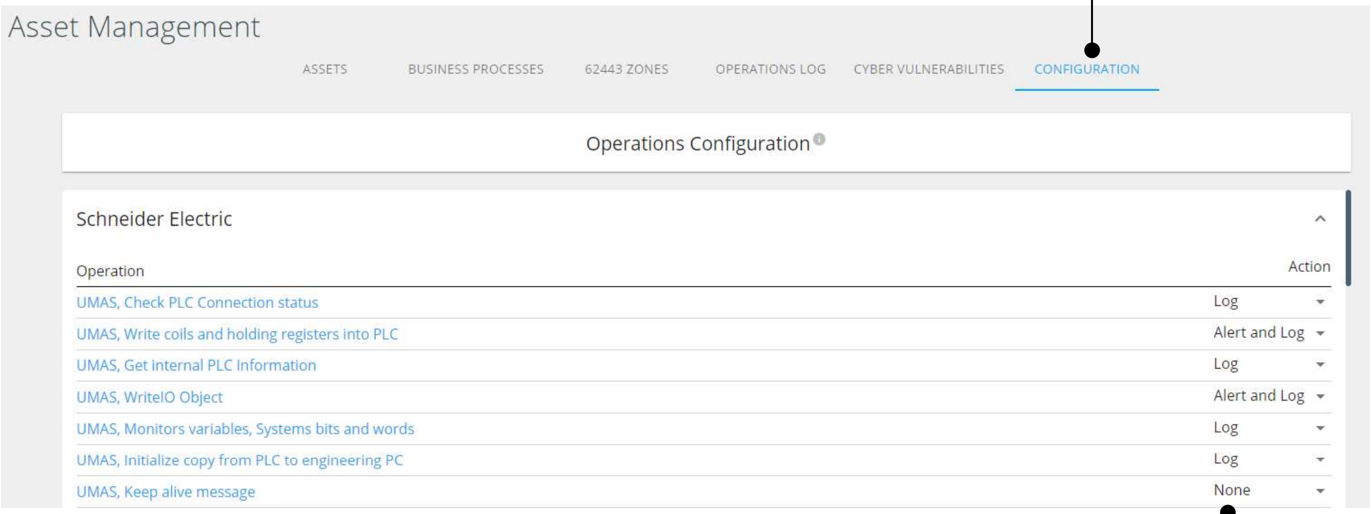
- Configure how iSID reacts when a specific management operation is identified
- View a list of vendors and their operation configurations

When all the physical connections are set and the basic configurations have been defined, Radiflow iSID is ready to start learning the network behavior (see Set system to Learning mode).

Configure how iSID reacts when a management operation is identified

1. Go to the Configuration pane (Asset management > Configuration).
2. If required expand the vendor lists to view all the management operations for the selected vendor.
3. In the Action column, specify how iSID reacts when a specific management operation is identified:
   - None - No action will be triggered by iSID
   - Log - Send a syslog message in CEF format, but do not trigger a notification
   - Alert and Log - Send a syslog message in CEF format and trigger a notification in the system

Click to display operation configuration details



Schneider Electric

Operation	Action
UMAS, Check PLC Connection status	Log
UMAS, Write coils and holding registers into PLC	Alert and Log
UMAS, Get internal PLC Information	Log
UMAS, WriteIO Object	Alert and Log
UMAS, Monitors variables, Systems bits and words	Log
UMAS, Initialize copy from PLC to engineering PC	Log
UMAS, Keep alive message	None

Actions taken when a specific operation is identified

View a list of vendors

1. Go to the Configuration pane (Asset management > Configuration).
2. View a list of vendors (Schneider Electric, Siemens Allen-Bradley) and view all the possible operations for each vendor.

Cyber Attack Rules

The iSID Cyber Attack Rules monitors for known threats designed to exploit vulnerabilities in the SCADA network, including threats to PLCs, RTUs, and industrial protocols.

The Cyber Attack Rules database is a comprehensive collection of the most up-to-date publicly available cyber-attack rules, as well as rules developed by Radiflow specifically for SCADA networks. The database is updated periodically to respond to emerging threats.

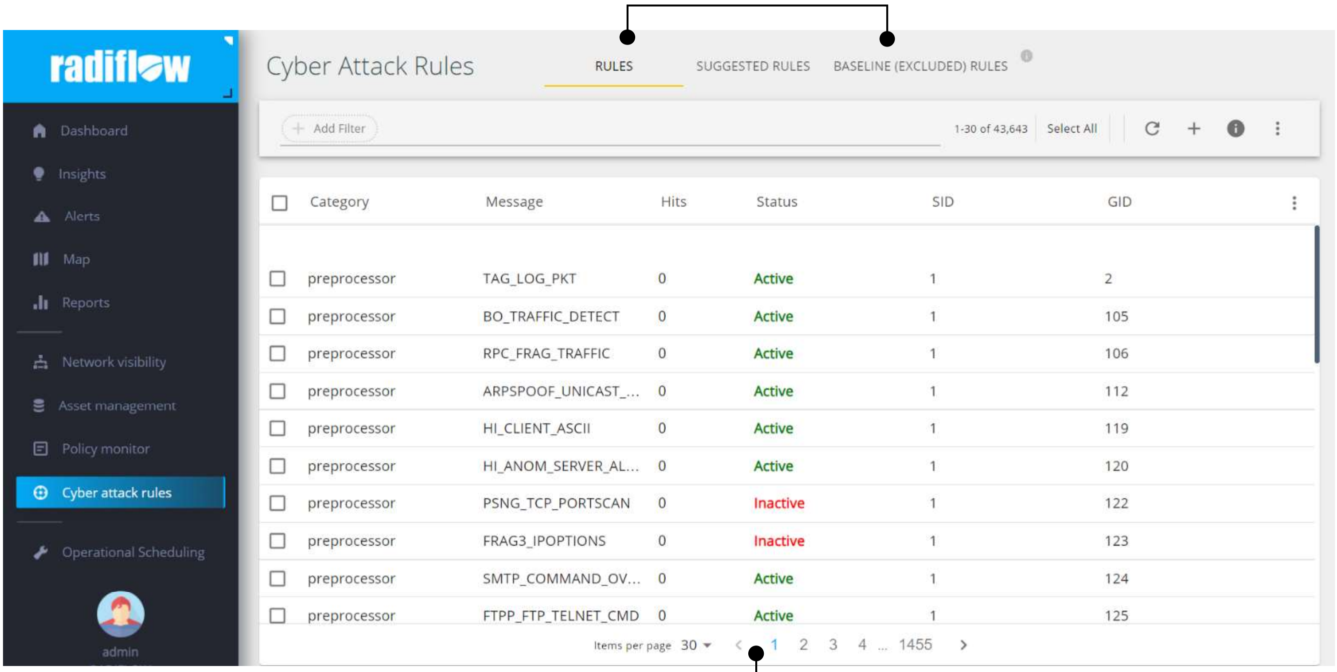
By default, when in learning mode, the Cyber Attack Rules is not active; but it is activated during the detection phase.

Note: Rules can be created using the rule syntax.

In the iSID Cyber Attack Rules panes you can view and manage the following cyber attack rules:

- Rules
- Suggested rules
- Baseline rules

Click to view and manage the cyber attack rules



Category	Message	Hits	Status	SID	GID
preprocessor	TAG_LOG_PKT	0	Active	1	2
preprocessor	BO_TRAFFIC_DETECT	0	Active	1	105
preprocessor	RPC_FRAG_TRAFFIC	0	Active	1	106
preprocessor	ARPSPOOF_UNICAST_...	0	Active	1	112
preprocessor	HI_CLIENT_ASCII	0	Active	1	119
preprocessor	HI_ANOM_SERVER_AL...	0	Active	1	120
preprocessor	PSNG_TCP_PORTSCAN	0	Inactive	1	122
preprocessor	FRAG3_IPOPTIONS	0	Inactive	1	123
preprocessor	SMTP_COMMAND_OV...	0	Active	1	124
preprocessor	FTPP_FTP_TELNET_CMD	0	Active	1	125

Choose how many items to view per page

Rules

rules use a different methodology for performing detection. Unlike signatures, rules are based on detecting the actual vulnerability, not an exploit or a unique piece of data. Developing a rule requires an acute understanding of how the vulnerability actually works.

View Rules

You can view either general rule information or in-depth details about each snort rule.

View general information about a rule

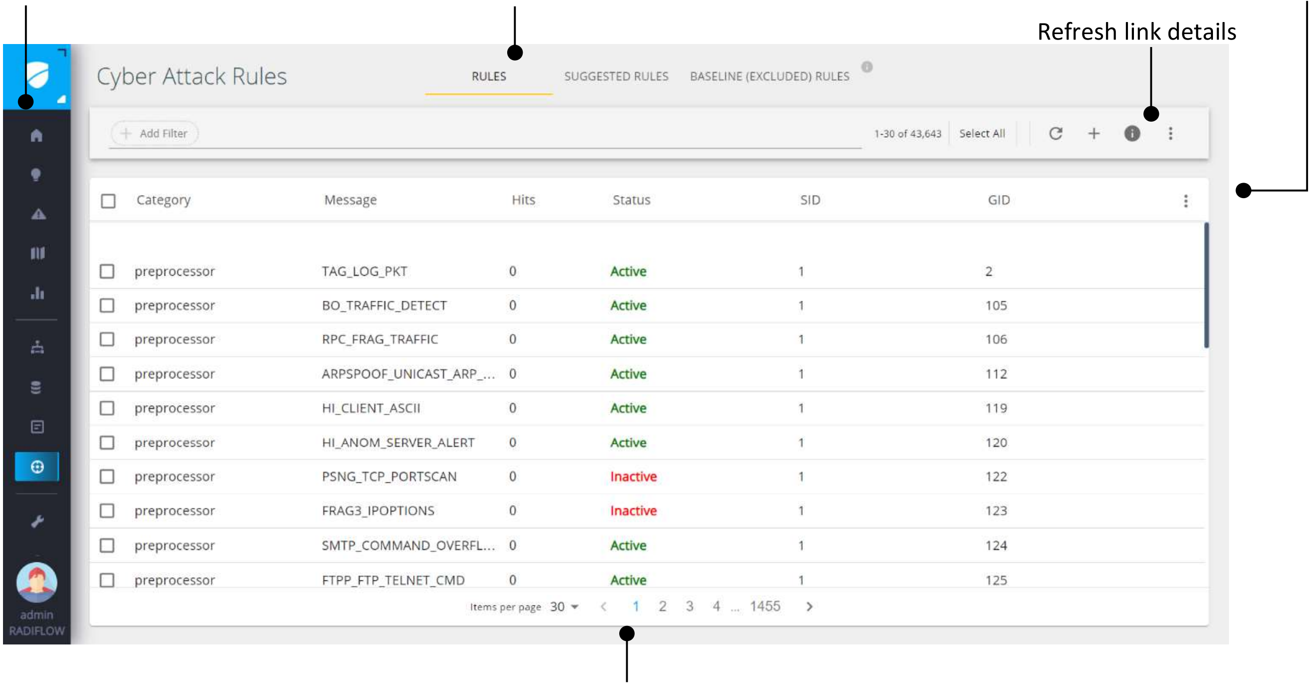
Select Cyber attack rules in the sidebar.
By default, the Rules pane opens displaying general information about the rules, such as their SID, GID, message, hits, status etc.

Click to show/hide sidebar

Click to view rules

Click to show/hide columns

Refresh link details



Cyber Attack Rules

□ Category	Message	Hits	Status	SID	GID
□ preprocessor	TAG_LOG_PKT	0	Active	1	2
□ preprocessor	BO_TRAFFIC_DETECT	0	Active	1	105
□ preprocessor	RPC_FRAG_TRAFFIC	0	Active	1	106
□ preprocessor	ARPSPOOF_UNICAST_ARP_...	0	Active	1	112
□ preprocessor	HI_CLIENT_ASCII	0	Active	1	119
□ preprocessor	HI_ANOM_SERVER_ALERT	0	Active	1	120
□ preprocessor	PSNG_TCP_PORTSCAN	0	Inactive	1	122
□ preprocessor	FRAG3_IPOPTIONS	0	Inactive	1	123
□ preprocessor	SMTP_COMMAND_OVERFL...	0	Active	1	124
□ preprocessor	FTPP_FTP_TELNET_CMD	0	Active	1	125

Items per page 30 ‹ 1 2 3 4 ... 1455 ›

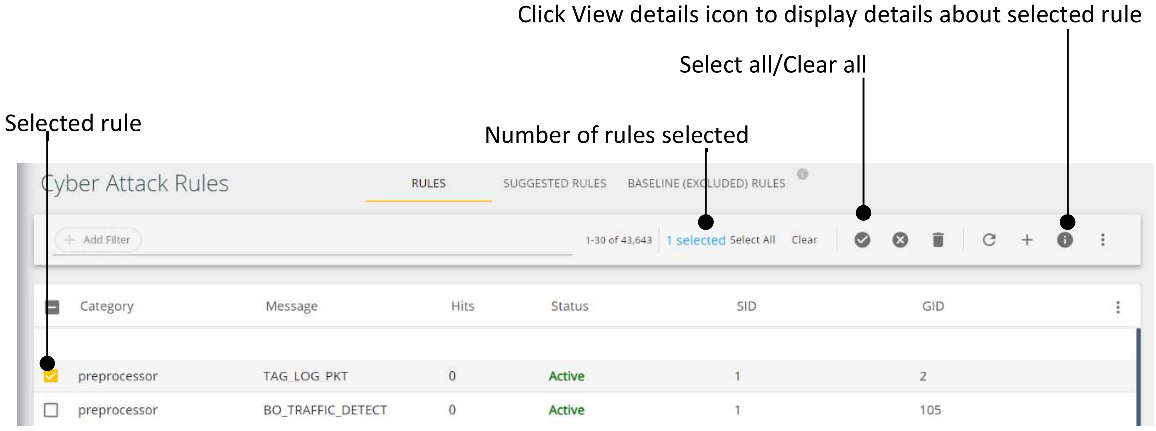
Choose how many items to view per page

- Use the search tools and search filters to search for specific rules
- Change the status of a rule
- Add a mask to a rule
- Enable/Disable rules
- Delete rules
- Hide or show individual columns
- Change the order the rules are displayed in each column
- Change the number of rules viewed per page

View in-depth details about a rule

1. Go to Snort Rules (Cyber attack rules > Rules).
2. Select the checkbox of the rule you wish to view in-depth details about.

The View details icon appears in the top right corner of the pane.



Click View details icon to display details about selected rule

Select all/Clear all

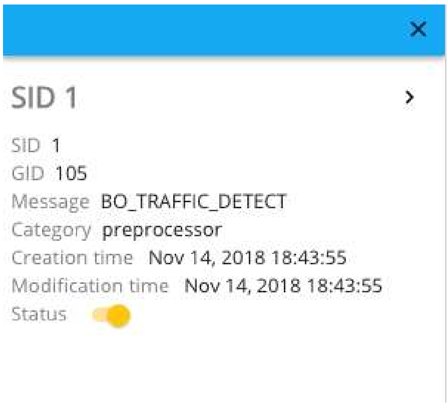
Selected rule

Number of rules selected

	Category	Message	Hits	Status	SID	GID
☑	preprocessor	TAG_LOG_PKT	0	Active	1	2
☐	preprocessor	BO_TRAFFIC_DETECT	0	Active	1	105

3. Click the View details icon.

A pop-up window opens displaying the following details about the rule:
Security identifier (SID), group identification (GID), message, category, creation date, modification date, and status.



SID 1

SID 1
GID 105
Message BO_TRAFFIC_DETECT
Category preprocessor
Creation time Nov 14, 2018 18:43:55
Modification time Nov 14, 2018 18:43:55
Status

Search for specific rules

1. Go to Rules (Cyber attack rules > Rules).
2. Use the search tools and Rules Filter List to search for a specific item.
3. Click the Filter icon.

The item list automatically refreshes and displays only those items matching the search filters.

Rules Filter Lists

First Level Search Filter	Second Level Search Filter	Third Level Search Filter
SID	• **Equal to** • Not equal to • Greater than • Less than	**Use arrows to specify required value**
GID		
Hits		
Creation time		**Enter date in pop-up calendar**
Modification time		
Category	• **Equal to** • **Not equal to**	**Select filter from category list**
Status		• **True** • **False**
Messages	• **Like** • Not Like	**Enter free text in search field**
Rule		

Manage Rules

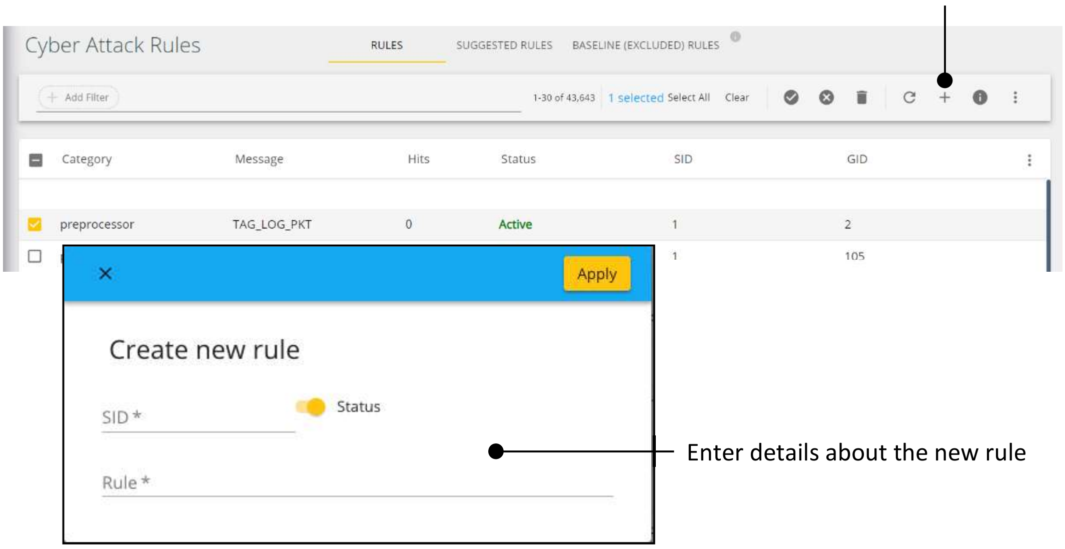
In the Snorts Rules pane, manage rules as follows:

- Create a new rule
- Change the status of a rule
- Add a mask to a rule
- Delete a rule

Create a new rule

1. Go to Rules (Cyber attack rules > Rules).
2. Click the Add rule icon. The Create new rule pop-up window opens.

Click the Add rule icon



☐	Category	Message	Hits	Status	SID	GID
☑	preprocessor	TAG_LOG_PKT	0	Active	1	2
☐					1	105

Create new rule

SID *

Status

Rule *

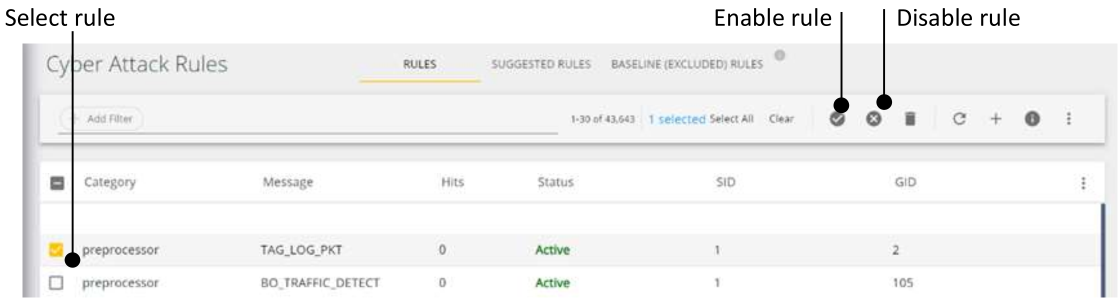
Enter details about the new rule

3. In the Create new rule pop-up window do the following:
   - Enter a unique SID number for the rule
   - Create a name for the rule using the rule syntax
   - Enable/Disable the rule
4. Click Apply. A message confirms the rule has been created.

Change the status of a rule

1. Go to Rules (Cyber attack signature > Rules).
2. Select the checkbox of the rule you wish to change.

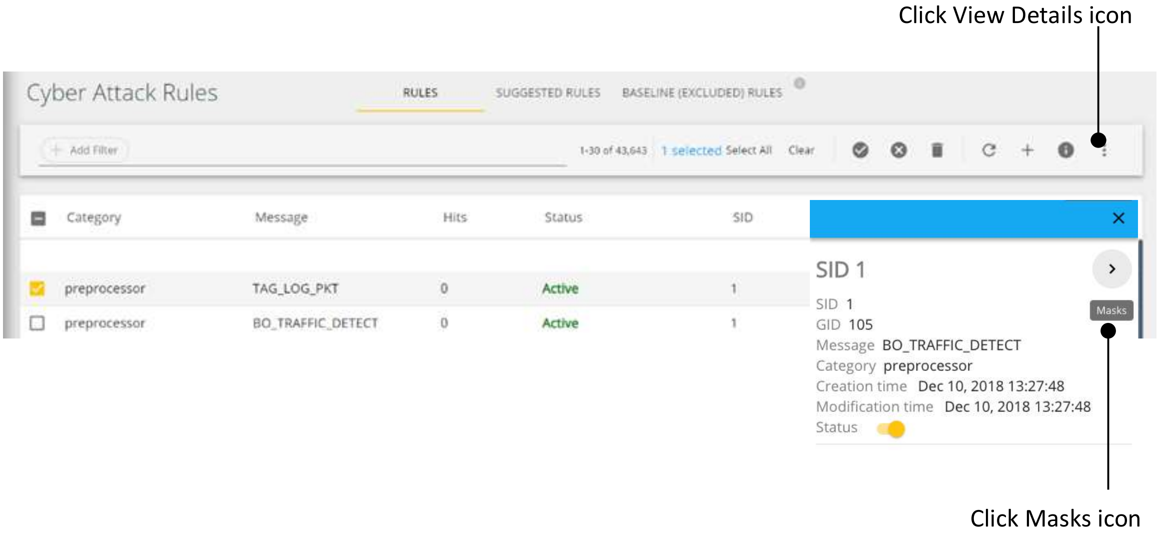
- Click the Enable rule icon to activate a deactivated rule
- Click the Disable rule icon to deactivate an active rule.
  The status of the rule changes and a message confirms the rule has been enabled/disabled.



☐	Category	Message	Hits	Status	SID	GID
☑	preprocessor	TAG_LOG_PKT	0	Active	1	2
☐	preprocessor	BO_TRAFFIC_DETECT	0	Active	1	105

Add a mask to a rule

1. Go to Rules (Cyber attack signature > Rules).
2. Select the checkbox of the rule you wish to add a mask.
3. Click the View details icon. A pop-up window opens

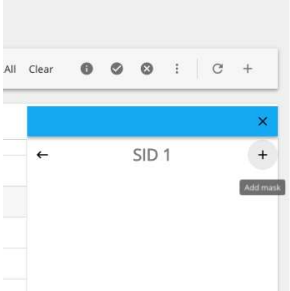


☐	Category	Message	Hits	Status	SID
☑	preprocessor	TAG_LOG_PKT	0	Active	1
☐	preprocessor	BO_TRAFFIC_DETECT	0	Active	1

SID 1

SID 1
GID 105
Message BO_TRAFFIC_DETECT
Category preprocessor
Creation time Dec 10, 2018 13:27:48
Modification time Dec 10, 2018 13:27:48
Status

4. In the pop-up window, click the Masks icon. The pop-up window transitions to the next window.
5. Click the Add mask icon. The Add mask pop-up window opens.



6. From the Add mask pop-up window, you can do the following:

- Enter an SID and GID number
- If required, toggle the Status button to activate the mask (by default new masks are deactivated)
- Reset the mask to its default details settings

Layer 3 section

- Enter the source and destination IP addresses
- Enter a Transport mode (TCP, UDP, ICMP)
- Remove Layer 3
- Reset Layer 3 to its default settings

Layer 4 section

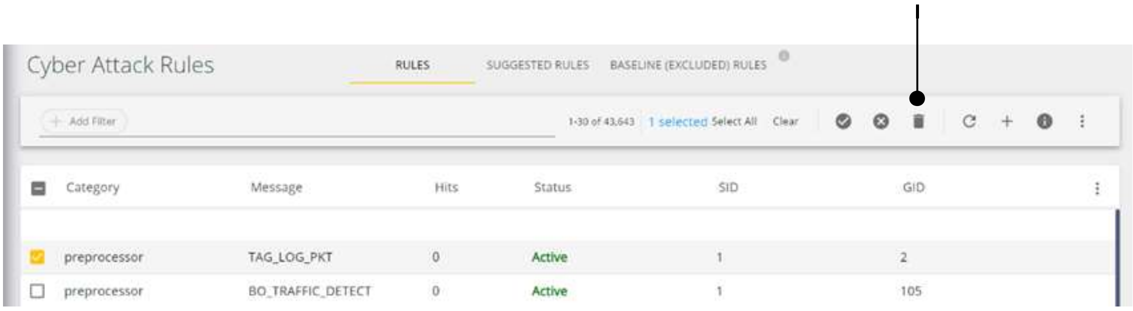
- Select a protocols port from the list
- Remove Layer 3
- Reset Layer 3 to its default setting

7. Click Apply. The window closes and a message confirms the mask has been added.

Delete a new rule

1. Go to Rules (Cyber attack rules > Rules).
2. Select the checkbox of the rule you wish to delete.
3. Click the Delete rule icon.
4. At the prompt, click OK to delete the rule. A message confirms the rule was successfully deleted.

Click the Delete rule icon



	Category	Message	Hits	Status	SID	GID
☑	preprocessor	TAG_LOG_PKT	0	Active	1	2
□	preprocessor	BO_TRAFFIC_DETECT	0	Active	1	105

Suggested Rules

Suggested rules, which are automatically created with traffic flow, are available for improving existing cyber attack management strategies.

View Suggested Rules

View either general suggested rule details or in-depth details about each suggested rule.

View general information about a suggested rule

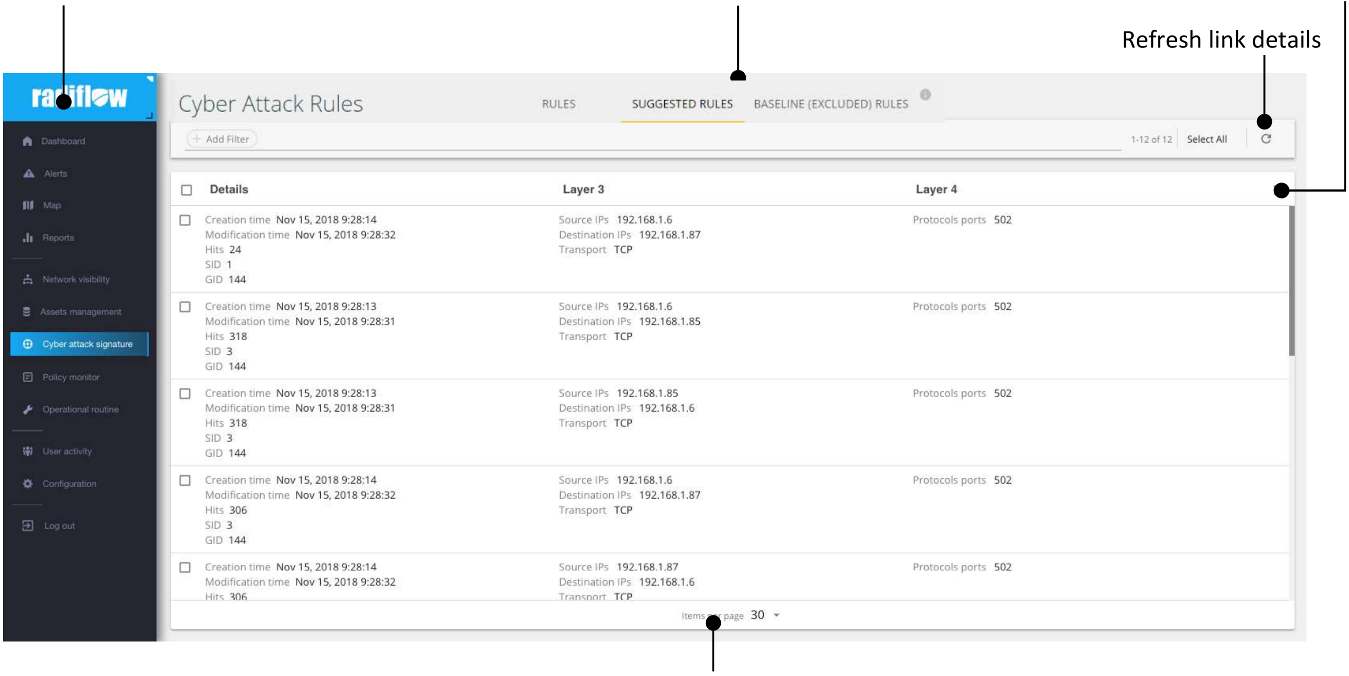
Go to Suggested Rules (Cyber attack rules > Suggested Rules).
The Suggested Rules pane displays general information about each suggested rule, such as SID, GID, hits, layer 3 and layer 4 details.

Click to show/hide sidebar

Click to view suggested rules

Click to show/hide columns

Refresh link details



□ Details	Layer 3	Layer 4
□ Creation time Nov 15, 2018 9:28:14 Modification time Nov 15, 2018 9:28:32 Hits 24 SID 1 GID 144	Source IPs 192.168.1.6 Destination IPs 192.168.1.87 Transport TCP	Protocols ports 502
□ Creation time Nov 15, 2018 9:28:13 Modification time Nov 15, 2018 9:28:31 Hits 318 SID 3 GID 144	Source IPs 192.168.1.6 Destination IPs 192.168.1.85 Transport TCP	Protocols ports 502
□ Creation time Nov 15, 2018 9:28:13 Modification time Nov 15, 2018 9:28:31 Hits 318 SID 3 GID 144	Source IPs 192.168.1.85 Destination IPs 192.168.1.6 Transport TCP	Protocols ports 502
□ Creation time Nov 15, 2018 9:28:14 Modification time Nov 15, 2018 9:28:32 Hits 306 SID 3 GID 144	Source IPs 192.168.1.6 Destination IPs 192.168.1.87 Transport TCP	Protocols ports 502
□ Creation time Nov 15, 2018 9:28:14 Modification time Nov 15, 2018 9:28:32 Hits 306	Source IPs 192.168.1.87 Destination IPs 192.168.1.6 Transport TCP	Protocols ports 502

Items per page 30

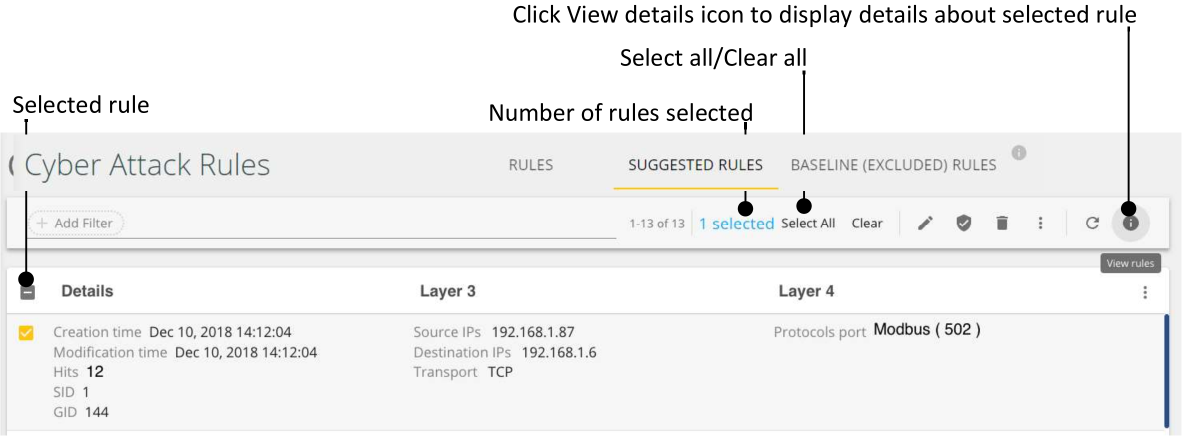
Choose how many items to view per page

- Use the search tools and search filters to search for specific rules
- Edit and approve a rule
- Delete a rule
- Download a PCAP (packet capture)
- Hide or show individual columns
- Change the order the rules are displayed in each column
- Change the number of rules viewed per page

View in-depth details about a suggested rule

1. Go to Suggested Rules (Cyber attack rules > Suggested Rules).
2. Select the checkbox of the rule you wish to view in-depth details about.

The View details icon appears in the top right corner of the pane.



Click View details icon to display details about selected rule

Select all/Clear all

Number of rules selected

Selected rule

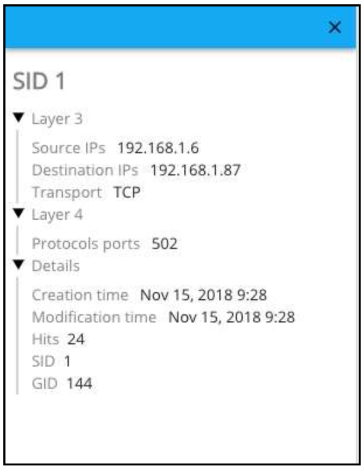
Cyber Attack Rules

Details	Layer 3	Layer 4
☑ Creation time Dec 10, 2018 14:12:04 Modification time Dec 10, 2018 14:12:04 Hits 12 SID 1 GID 144	Source IPs 192.168.1.87 Destination IPs 192.168.1.6 Transport TCP	Protocols port Modbus (502)

3. Click the View details icon.

A pop-up window opens displaying the following details about the rules.

SID, GID, Hits, creation and modification dates, layer 3 details such as source and destination IP addresses, and layer 4 protocol ports.



SID 1

▼ Layer 3

Source IPs 192.168.1.6

Destination IPs 192.168.1.87

Transport TCP

▼ Layer 4

Protocols ports 502

▼ Details

Creation time Nov 15, 2018 9:28

Modification time Nov 15, 2018 9:28

Hits 24

SID 1

GID 144

Search for specific suggested rules

1. Go to Suggested Rules (Cyber attack rules > Suggested Rules).
2. Use the search tools and Suggested Rules Filter Lists to search for a specific item.
3. Click the Filter icon.

The item list automatically refreshes and displays only those items matching the search filters.

Suggested Rules Filter Lists

First Level Search Filter	Second Level Search Filter	Third Level Search Filter
SID	• **Equal to** • Not equal to • Greater than • Less than	**Use arrows to specify required value**
GID		
Hits		
Creation time		**Enter date in pop-up calendar**
Modification time		
Source IPs	• **Equal to** • **Not equal to**	**Use arrows to specify required value**
Destination IPs		
Transport	• **Equal to** • **Not equal to**	• **TCP** • **UDP** • **ICMP**
Protocol Ports	• **Equal to** • **Not equal to**	**Enter free text in search field**

Manage Suggested Rules

In the Suggested Rules pane, manage suggested rules as follows:

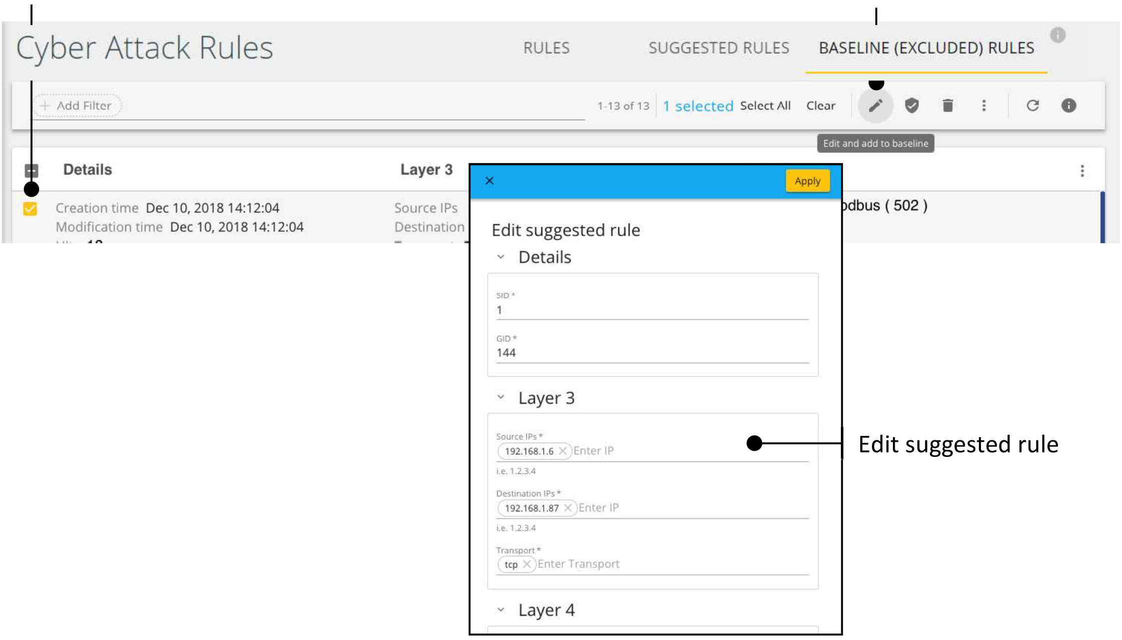
- Edit a suggested rule
- Add a suggested rule to the baseline rules
- Delete a suggested rule
- Download a PCAP (packet capture)

Edit a suggested rule and add it to the baseline rules

1. Go to Suggested Rules (Cyber attack rules > Suggested Rules).
2. Select the checkbox of the suggested rule you want to edit and add to the baseline rules.
3. Click the Edit and add to baseline icon. The Edit suggested rule pop-up window opens.

Select rule to edit

Click Edit and add to baseline icon



Cyber Attack Rules

Creation time Dec 10, 2018 14:12:04
Modification time Dec 10, 2018 14:12:04

Source IPs
Destination

odbus (502)

Edit suggested rule

Details

SID * 1

GID * 144

Layer 3

Source IPs * 192.168.1.6 Enter IP
i.e. 1.2.3.4

Destination IPs * 192.168.1.87 Enter IP
i.e. 1.2.3.4

Transport * tcp Enter Transport

Layer 4

Edit suggested rule

4. In the Edit suggested rule pop-up window, you can do the following:

Details section

- Enter an SID and GID number
- Reset the details to its default settings

Layer 3 section

- Enter the source and destination IP addresses
- Enter a Transport mode (TCP, UDP, ICMP)
- Reset the layer to its default settings

Layer 4 section

- Select a protocols port from the list
- Reset the layer to its default settings

5. Click Apply to apply the edits and add the rule to the baseline rules.

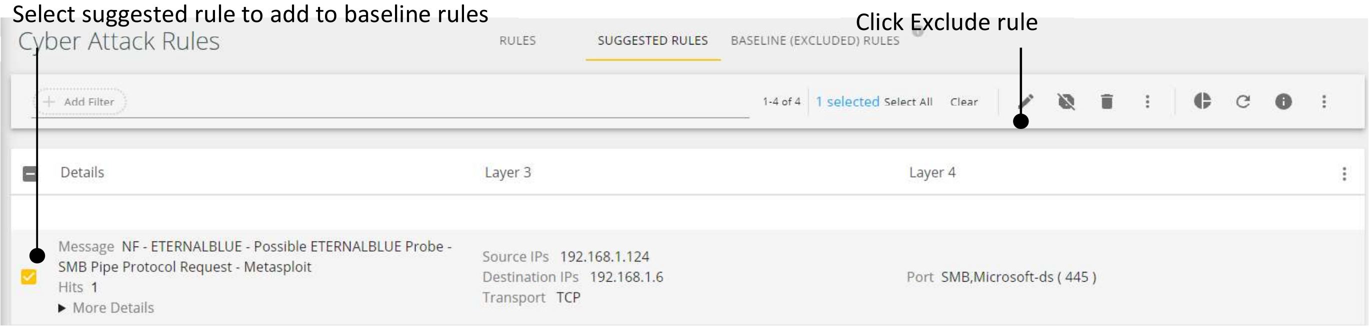
A message confirms the edits have been applied.

Add a suggested rule to the baseline rules

1. Go to Suggested Rules (Cyber attack rules > Suggested Rules).
2. Select the checkbox of the suggested rule you want to add to the baseline rules.
3. Click the Add rule to Baseline icon. A message confirms the rule has been added to the baseline rules.

Select suggested rule to add to baseline rules

Click Exclude rule



Details	Layer 3	Layer 4
Message NF - ETERNALBLUE - Possible ETERNALBLUE Probe - SMB Pipe Protocol Request - Metasploit Hits 1 ▸ More Details	Source IPs 192.168.1.124 Destination IPs 192.168.1.6 Transport TCP	Port SMB,Microsoft-ds (445)

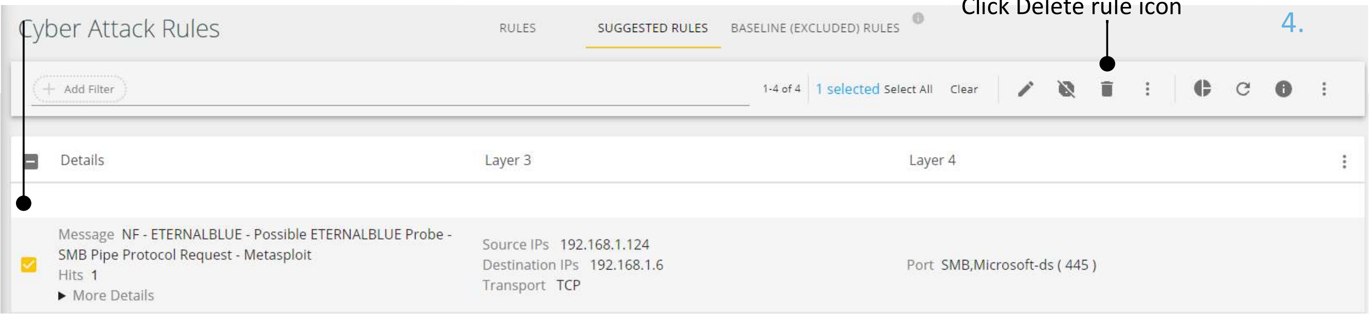
Delete a suggested rule

1. Go to Suggested Rules (Cyber attack rules > Suggested Rules).
2. Select the checkbox of the suggested rule you want to delete.
3. Click the Delete rule icon. At the prompt, click OK to delete the rule.

Select rule to delete

Click Delete rule icon

4.



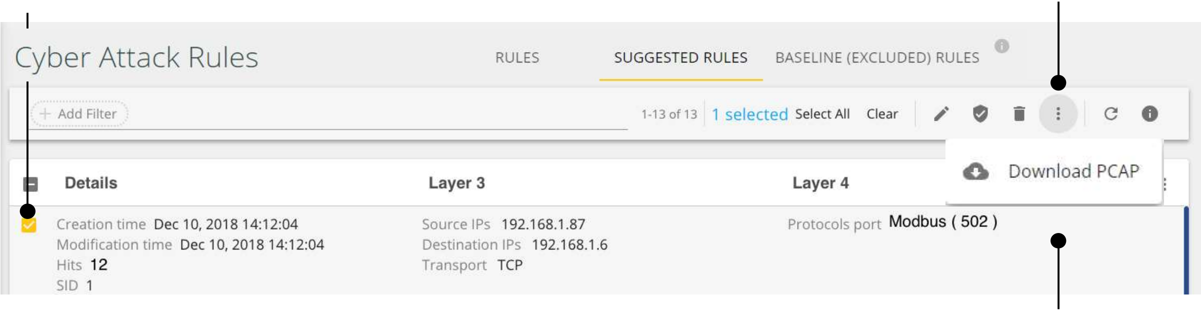
Details	Layer 3	Layer 4
Message NF - ETERNALBLUE - Possible ETERNALBLUE Probe - SMB Pipe Protocol Request - Metasploit Hits 1 ▸ More Details	Source IPs 192.168.1.124 Destination IPs 192.168.1.6 Transport TCP	Port SMB,Microsoft-ds (445)

Download a PCAP (packet capture)

1. Go to Suggested Rules (Cyber attack rules > Suggested Rules).
2. Select the relevant suggested rule, using the checkbox provided.

Select suggested rule

Click More



Details	Layer 3	Layer 4
Creation time Dec 10, 2018 14:12:04 Modification time Dec 10, 2018 14:12:04 Hits 12 SID 1	Source IPs 192.168.1.87 Destination IPs 192.168.1.6 Transport TCP	Protocols port Modbus (502)

Click Download PCAP

3. Click the More icon and then select Download PCAP rule. The PCAP downloads to the local PC.

Baseline Rules

The baseline rules are the minimum level of security the system, network, and device must adhere to.

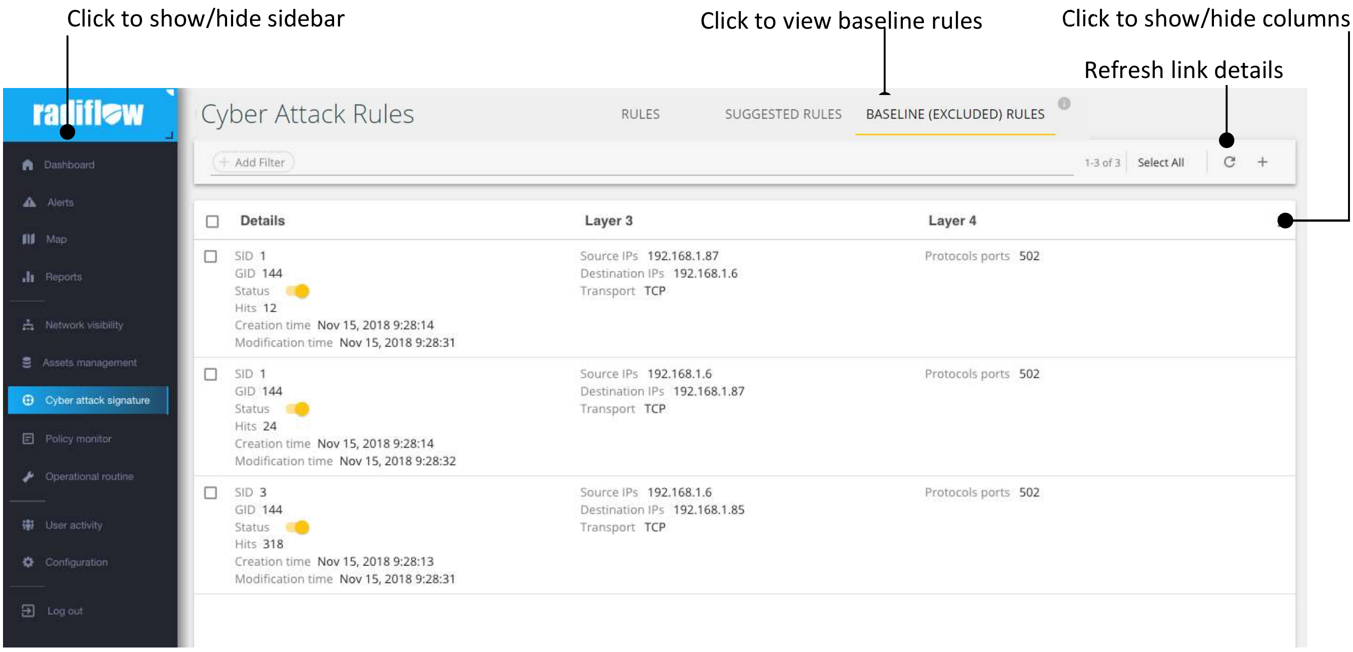
View Masks

The Baseline Rules panel displays details about subnet masks associated to internal networks.

View details about each mask

Go to Baseline Rules (Cyber attack signature > Baseline Rules).

The Baseline Rules pane displays details about each mask, such as its SID, GID, status, creation and modification dates, and layer details.


Click to show/hide sidebar

Click to view baseline rules

Click to show/hide columns

Refresh link details

□	Details	Layer 3	Layer 4
□	SID 1 GID 144 Status Hits 12 Creation time Nov 15, 2018 9:28:14 Modification time Nov 15, 2018 9:28:31	Source IPs 192.168.1.87 Destination IPs 192.168.1.6 Transport TCP	Protocols ports 502
□	SID 1 GID 144 Status Hits 24 Creation time Nov 15, 2018 9:28:14 Modification time Nov 15, 2018 9:28:32	Source IPs 192.168.1.6 Destination IPs 192.168.1.87 Transport TCP	Protocols ports 502
□	SID 3 GID 144 Status Hits 318 Creation time Nov 15, 2018 9:28:13 Modification time Nov 15, 2018 9:28:31	Source IPs 192.168.1.6 Destination IPs 192.168.1.85 Transport TCP	Protocols ports 502

- Manage masks
- Search for items based on specific criteria
- Show and hide columns
- Choose how many items to view per page

Search for specific baseline rules

1. Go to Baseline Rules (Cyber attack rules > Baseline Rules).
2. Use the search tools and Baseline Rules Filter Lists to search for a specific item.
3. Click the Filter icon.

The item list automatically refreshes and displays only those items matching the search filters.

Baseline Rules Filter Lists

First Level Search Filter	Second Level Search Filter	Third Level Search Filter
SID	• **Equal to** • Not equal to • Greater than • Less than	**Use arrows to specify required value**
GID		
Hits		
Creation time		**Enter date in pop-up calendar**
Modification time		
Source IPs	• **Equal to** • **Not equal to**	**Use arrows to specify required value**
Destination IPs		
Transport	• **Equal to** • **Not equal to**	• **TCP** • **UDP** • **ICMP**
Protocol Ports	• **Equal to** • **Not equal to**	**Enter free text in search field**

Manage Masks

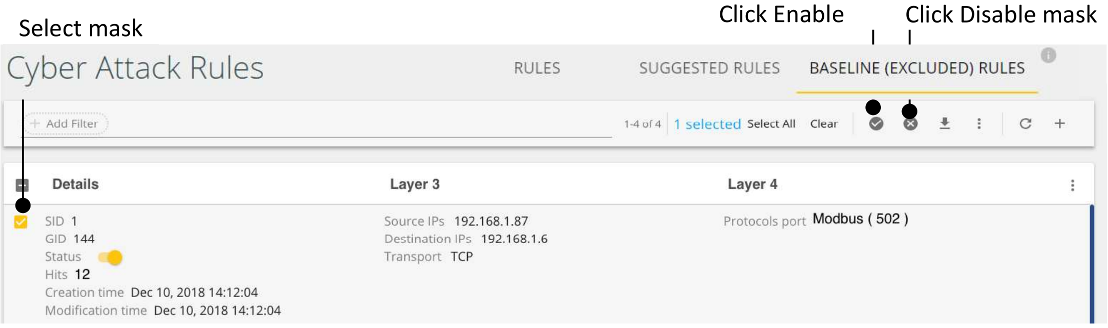
In Baseline Rules, you can apply appropriate subnet masks to internal networks, i.e., masks that are sufficiently long to identify only that fragment of the IP network number that you are using.

In the Baseline Rules pane, manage masks as follows:

- Enable a mask
- Disable a mask
- Delete a mask
- Add a mask
- Download a mask PCAP

Enable or disable mask

1. Go to Baseline Rules (Cyber attack rules > Baseline Rules).
2. Select the checkbox of the mask you want to enable or disable.
3. Enable or disable the mask as follows:
   - To enable a mask, click the Enable mask icon. A message confirms the mask has been enabled.
   - To disable a mask, click the Disable mask icon. A message confirms the mask has been disabled.



Select mask

Click Enable

Click Disable mask

Cyber Attack Rules

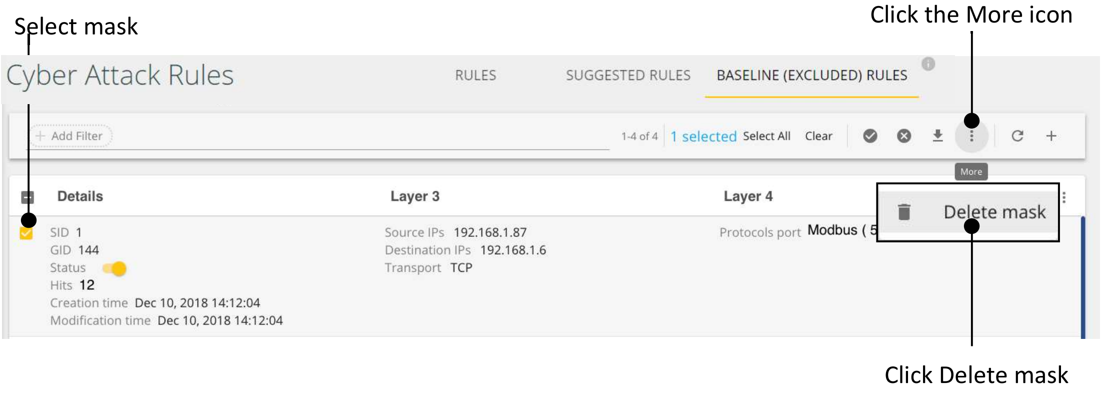
SID 1
GID 144
Status
Hits 12
Creation time Dec 10, 2018 14:12:04
Modification time Dec 10, 2018 14:12:04

Source IPs 192.168.1.87
Destination IPs 192.168.1.6
Transport TCP

Protocols port Modbus (502)

Delete a mask

1. Go to Baseline Rules (Cyber attack rules > Baseline Rules).
2. Select the checkbox of the mask you want to delete.
3. Click the More icon and then click Delete mask. A message confirms the mask has been deleted.



Select mask

Click the More icon

Click Delete mask

Cyber Attack Rules

SID 1
GID 144
Status
Hits 12
Creation time Dec 10, 2018 14:12:04
Modification time Dec 10, 2018 14:12:04

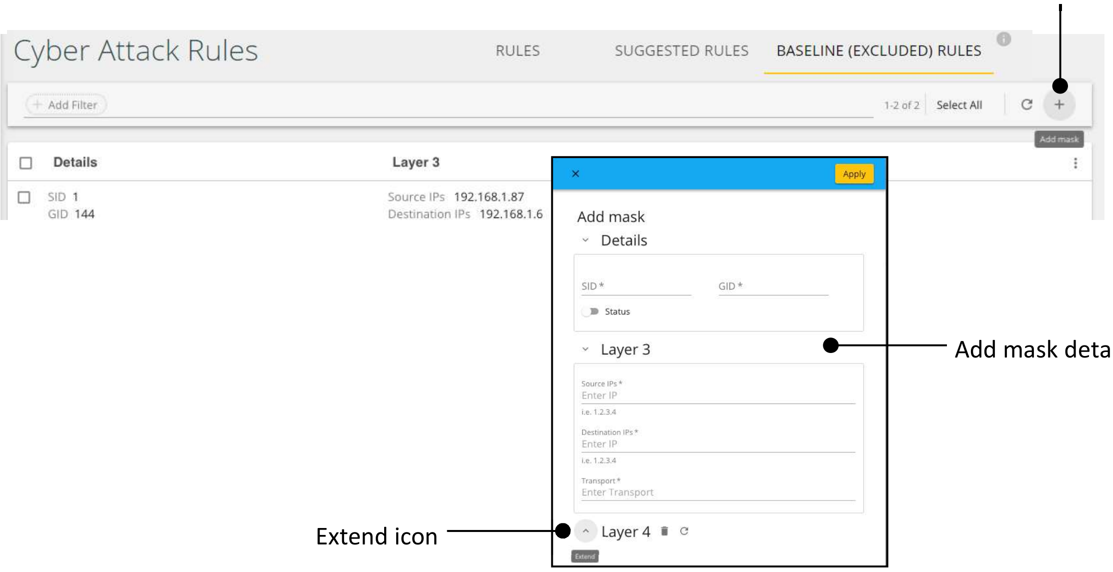
Source IPs 192.168.1.87
Destination IPs 192.168.1.6
Transport TCP

Protocols port Modbus (5

Add a mask

1. Go to Baseline Rules (Cyber attack rules > Baseline Rules).
2. Click the Add mask icon. The Add mask pop-up window opens.

Click Add mask



SID 1
GID 144
Source IPs 192.168.1.87
Destination IPs 192.168.1.6

Add mask details

Extend icon

3. In the Add mask pop-up window, do the following:

Details section

- Enter an SID and GID number
- Reset the mask details to its default settings.

Layer 3 section

- Enter the source and destination IP addresses
- Enter a Transport mode (TCP, UDP, ICMP)
- Remove Layer 3 details
- Reset Layer 3 to its default settings

Layer 4 section

- Select a protocols port from the list
- Remove Layer 4 details
- Reset Layer 4 to its default settings

4. Click Apply to add the mask. A message confirms the mask has been added.

Policy Monitor

The iSID Policy Monitor enables you to create rules for a variety of behaviors. A rule may combine a variety of parameters from various Ethernet L2-L7 fields. Rules can then be enforced and set to trigger a number of possible actions.

In addition to manually creating rules, Policy Monitor generates rules automatically from the incoming traffic. These suggested rules can also be edited and adjusted, so they too can be enforced.

By utilizing the capabilities of Deep Packet Inspection (DPI), iSID is able to generate an alert when a match between a defined rule and the inspected traffic accrues.

How it works

During the learning stage, Policy Monitor analyzes the traffic within the OT network and creates suggested rule policies based on the network behavior on each link.
These polices can be separated into black/white list like behavior, where a user defines what kind of network activity triggers an alert.
Note: The iSID Policy Monitor package is passive. It provides alerts for violated rules but does not block or actively prevent actions. The barrier between the trusted, secure SCADA network and other outside networks, therefore, is merely virtual. Policy enforcement is possible through integration with Radiflow's Secure Gateway (iSEG).

Advantages and Features

- Define policies on each link
- Upon violation, an alert is generated, however the iSID Policy Monitor packages do not block the network traffic
- Edit policies suggested by the iSID Policy Monitor.
- Ability to create labels makes it to easier to manage enforced rules.
- Suggested rules are automatically created with traffic flow.
- Option to create scheduled Policy Monitor rules for specific time periods.

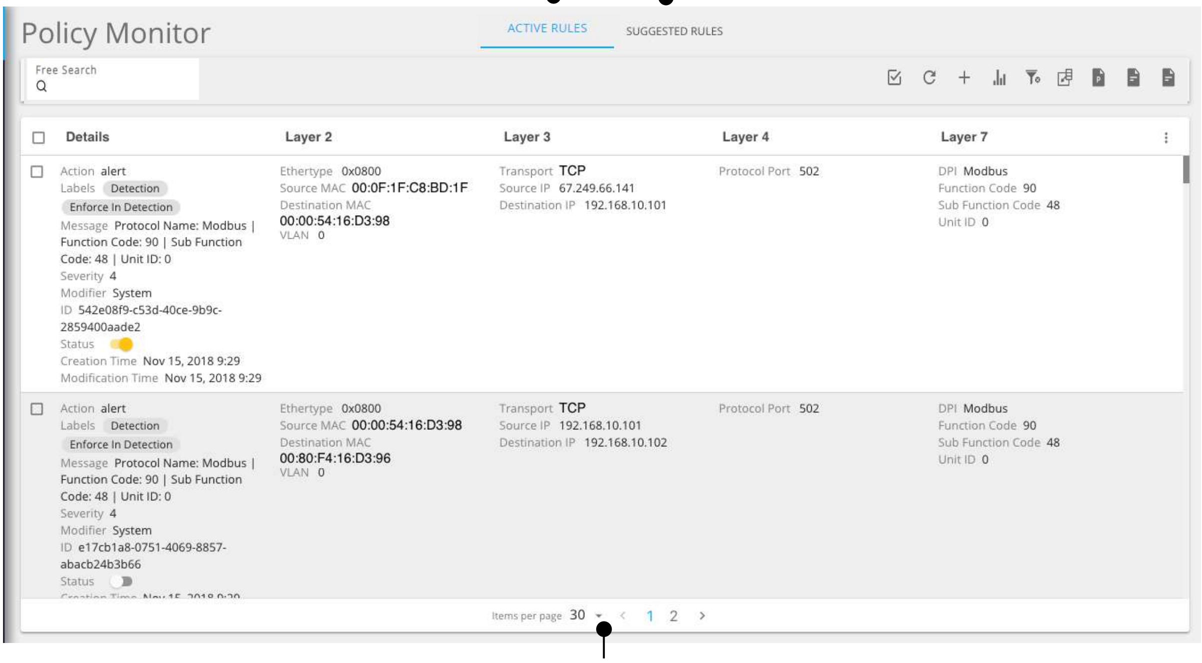
(e.g. 08:00, November 3rd to 10:00, November 3rd)

- Optional policy enforcement via integration with Radiflow's Secure Gateway (iSEG).

Go to iSID Policy Monitor panes to view and manage the following:

- Policy rules
- Suggested rules

Click to view and manage rules



Policy Monitor

□ Details	Layer 2	Layer 3	Layer 4	Layer 7
□ Action alert Labels Detection Enforce In Detection Message Protocol Name: Modbus | Function Code: 90 | Sub Function Code: 48 | Unit ID: 0 Severity 4 Modifier System ID 542e08f9-c53d-40ce-9b9c-2859400aade2 Status Creation Time Nov 15, 2018 9:29 Modification Time Nov 15, 2018 9:29	Ethertype 0x0800 Source MAC 00:0F:1F:C8:BD:1F Destination MAC 00:00:54:16:D3:98 VLAN 0	Transport TCP Source IP 67.249.66.141 Destination IP 192.168.10.101	Protocol Port 502	DPI Modbus Function Code 90 Sub Function Code 48 Unit ID 0
□ Action alert Labels Detection Enforce In Detection Message Protocol Name: Modbus | Function Code: 90 | Sub Function Code: 48 | Unit ID: 0 Severity 4 Modifier System ID e17cb1a8-0751-4069-8857-abacb24b3b66 Status Creation Time Nov 15, 2018 9:29	Ethertype 0x0800 Source MAC 00:00:54:16:D3:98 Destination MAC 00:80:F4:16:D3:96 VLAN 0	Transport TCP Source IP 192.168.10.101 Destination IP 192.168.10.102	Protocol Port 502	DPI Modbus Function Code 90 Sub Function Code 48 Unit ID 0

Choose how many items to view per page

Policy Rules

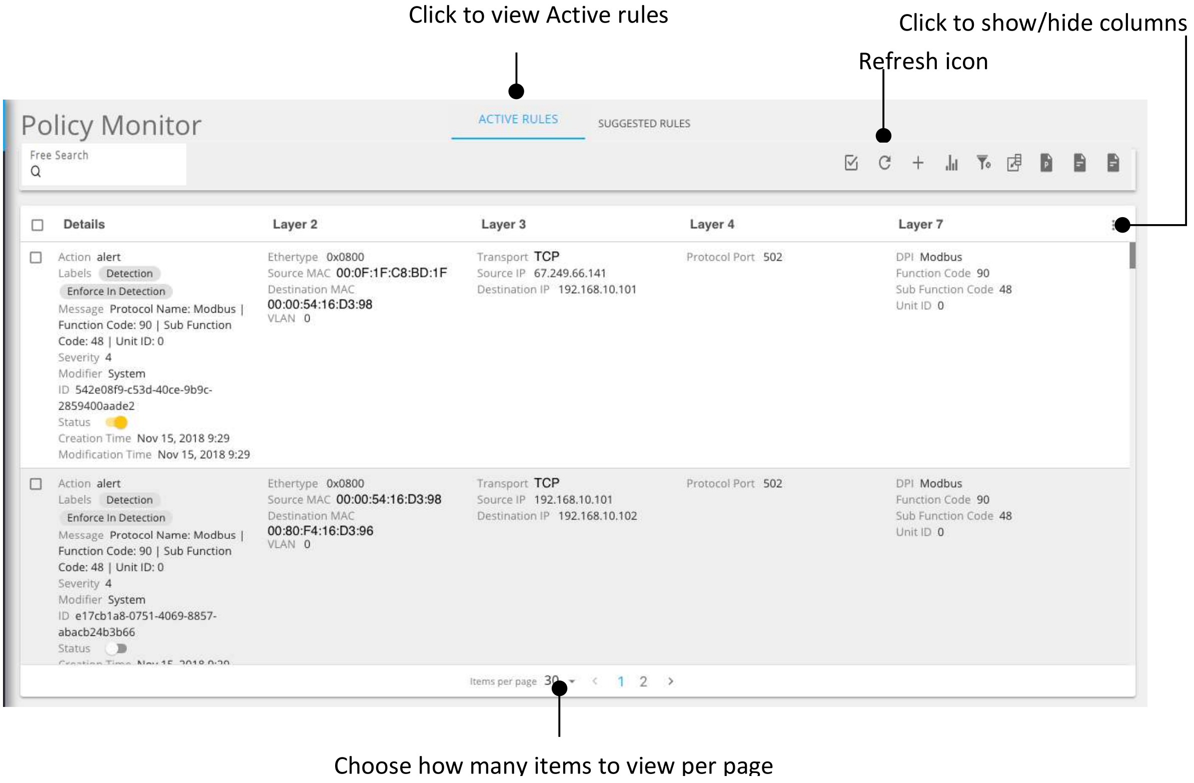
Policy rules are created and managed in the Policy Rule pane.

View Active Rules

The Policy Rules panel displays details about manually created policy rules. Access the Policy Rules panel to view the complete rule definition including metadata as well as all layer configurations.

View Active Rule Details

Go to Policy Rules (Policy monitor > Active Rules).
The Active Rules pane displays details about each policy rule, such as its action trigger, messages associated with the rule, ID, status, creation dates, and Layer 2-Layer 7 details etc.


Click to view Active rules

Click to show/hide columns

Refresh icon

Policy Monitor

☐	Details	Layer 2	Layer 3	Layer 4	Layer 7
☐	Action alert Labels Detection Enforce In Detection Message Protocol Name: Modbus | Function Code: 90 | Sub Function Code: 48 | Unit ID: 0 Severity 4 Modifier System ID 542e08f9-c53d-40ce-9b9c-2859400aade2 Status Creation Time Nov 15, 2018 9:29 Modification Time Nov 15, 2018 9:29	Ethertype 0x0800 Source MAC 00:0F:1F:C8:BD:1F Destination MAC 00:00:54:16:D3:98 VLAN 0	Transport TCP Source IP 67.249.66.141 Destination IP 192.168.10.101	Protocol Port 502	DPI Modbus Function Code 90 Sub Function Code 48 Unit ID 0
☐	Action alert Labels Detection Enforce In Detection Message Protocol Name: Modbus | Function Code: 90 | Sub Function Code: 48 | Unit ID: 0 Severity 4 Modifier System ID e17cb1a8-0751-4069-8857-abacb24b3b66 Status Creation Time Nov 15, 2018 9:29	Ethertype 0x0800 Source MAC 00:00:54:16:D3:98 Destination MAC 00:80:F4:16:D3:96 VLAN 0	Transport TCP Source IP 192.168.10.101 Destination IP 192.168.10.102	Protocol Port 502	DPI Modbus Function Code 90 Sub Function Code 48 Unit ID 0

Items per page 30

Choose how many items to view per page

- Use the search tools and search filters to search for specific policy rules
- Manage rules
- Hide or show individual columns
- Change the number of items viewed per page

Search for specific policy rules

1. Go to Policy Rules (Policy monitor > Active Rules).
2. Use the search box to search for a specific item.

The item list automatically refreshes and displays only those items matching the search filters.

Policy Rules Filter Lists

First Level Search Filter	Second Level Search Filter	Third Level Search Filter
Labels	- **Equal to** - **Not equal to**	**Enter free text in search field**
Src Vendors		
VLAN		
EtherType		
Transport		
Protocol Port		
Severity		**1-5**
Action		- **Log** - **Alert** - **Pass**
ID	- **Like** - Not Like	**Enter free text in search field**
Message		
Procedure		
Source MAC		
Destination MAC		
Source IP		
Destination IP		
Creation Time		**Enter date in pop-up calendar**
Modification Time		

First Level Search Filter	Second Level Search Filter	Third Level Search Filter
MMS Service	• **Equal to** • **Not equal to** • **Greater than** • **Less than**	**Use arrows to specify a value**
MMS Sub Service		
Unit ID		
Destination Address		
Source Address		
APDU		
Backnet Service		
ACPI Type		
ASDU Type		
COT		
ASDU Address		

Manage Policy Rules

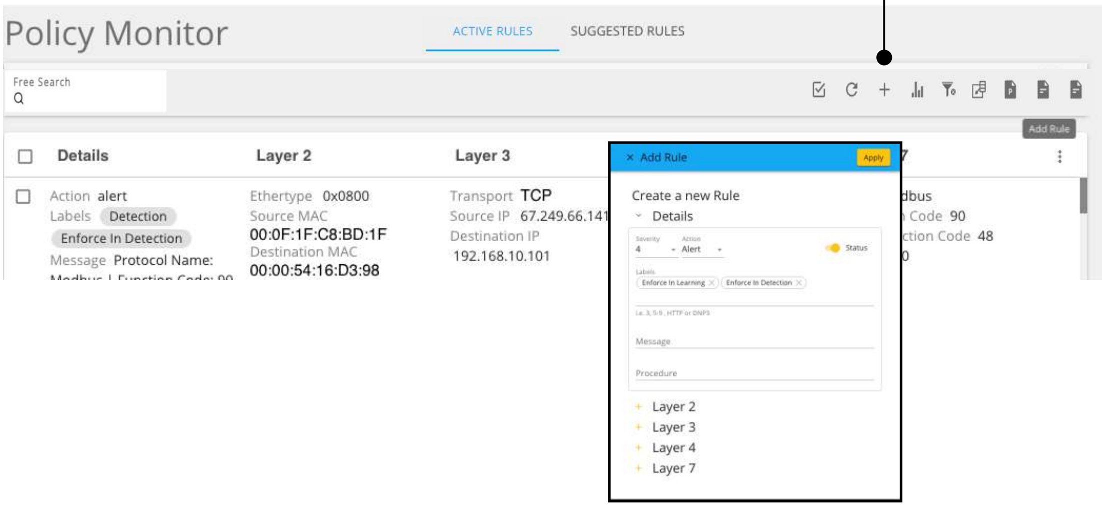
In the Policy Rules pane, manage policy rules as follows:

- Create a policy rule
- Edit a policy rule
- Delete a policy rule
- Clone a policy rule
- Enable and disable a policy rule

Create a new policy rule

1. Go to Active Rules (Policy monitor > Active Rules).
2. Click the Add Rule icon. The Add Rule pop-up window opens.

Click Add Rule icon



Action alert
Labels Detection
Enforce In Detection
Message Protocol Name:

Ethertype 0x0800
Source MAC 00:0F:1F:C8:BD:1F
Destination MAC 00:00:54:16:D3:98

Transport TCP
Source IP 67.249.66.141
Destination IP 192.168.10.101

dbus
Code 90
ction Code 48

Severity 4
Action Alert
Status
Labels Enforce In Learning × Enforce In Detection ×
i.e. 3, 5-9 , HTTP or DNP3
Message
Procedure

3. In the Add Rule pop-up window, you can do the following:

- Reset the Details to their default settings
- Create a new layer
- Remove a layer
- Reset a layer to its default settings
- Create a new policy rule as described in the table below:

Rule Fields

Policy Rule Fields	Description
DETAILS SECTION	
Severity	Severity level of the event created when rule is violated (1-5) (See Manage Events).
Action	Select the desired action when rule conditions are detected: Ignore: System does not take any action and ignores the packet Alert: Add a new event to the Event listing. Log: Sends a Syslog message to a pre-defined syslog server. (See Configuration Syslog)
Status	Toggle to enable or disable the policy rule
Labels	Select the labels that apply to the rule
Message	Define the message that will be displayed in case of an event
Procedure	Define the procedure to be followed in case of an event
LAYER 2	
VLAN	Enter the VLAN ID number in the Range of 1-4096
EtherType	Select the EtherType: • 0x0800 • 0x8100 • 0x0806 • 0x86DD
Source MAC	Enter MAC address of the source device (AA:BB:CC:DD:EE:FF)
Destination MAC	Enter MAC address of the destination device. (AA:BB:CC:DD:EE:FF)
LAYER 3	
Transport	Select transport type: • TCP • UDP • ICMP

Policy Rule Fields	Description
Source IP	Enter the source IP (A.B.C.D)
Destination IP	Enter the destination IP (A.B.C.D)
LAYER 4	
Protocol Ports	Enter the protocol ports either by port number or protocol
LAYER 7	
DPI	Select the DPI type matching the unique industrial protocol.
Function code	Select the function code.
DPI dependent parameters	Other parameters may appear, depending on the DPI type selected.

4. Click Apply to create the policy rule. A message confirms the policy rule has been created.

Labels

In iSID Policy Monitor you can add labels to policy rules. This feature provides a convenient method for delineating categories of policies.
A label can be used as a keyword for filtering and tagging policies and profiles.
Radiflow iSID comes with four predefined system labels:

- Learning – represent the suggested rules created in the learning phase
- Detection – represent the suggested rules created in the detection phase
- Enforce in Learning - rules tagged with this label will be enforced in the learning phase
- Enforce in Detection – rules tagged with this label will be enforced in the detection phase

Create Labels

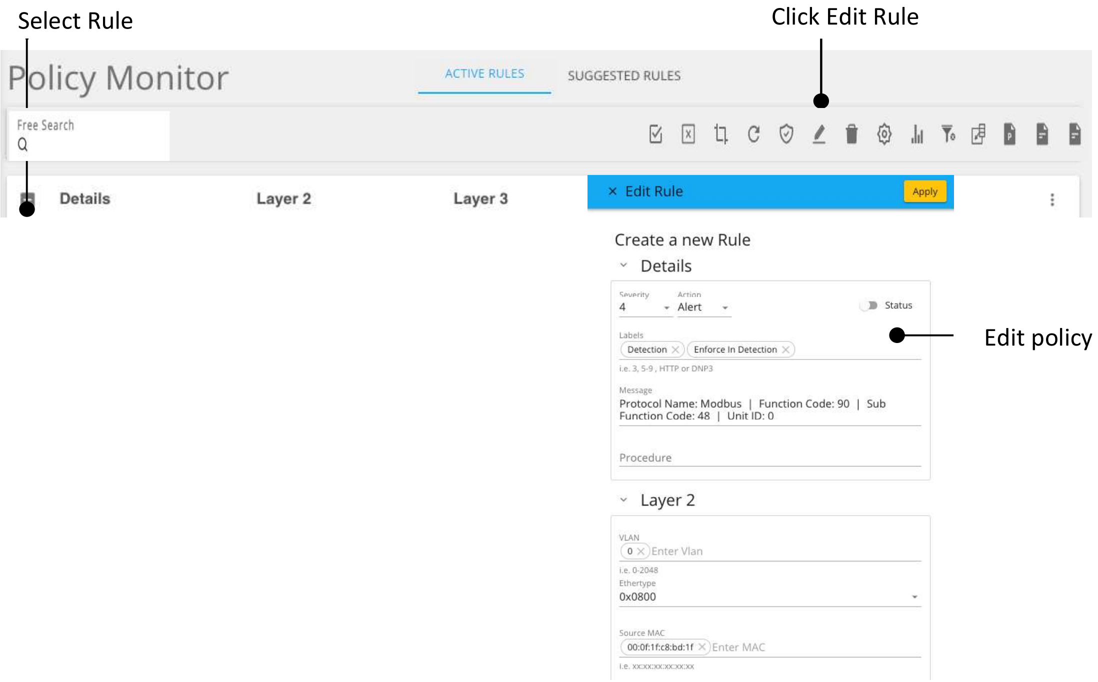
You create labels to categorize policy rules. These labels can be filtered and associated with user defined profiles to easily manage system policies.

Create a user-defined label

When you create a new policy rule, you can enter a new label name. The label will be saved and assigned to the policy.

Edit a Policy rule

1. Go to Active Rules (Policy monitor > Active Rules).
2. Select the checkbox of the policy rule you want to edit.
3. Click the Edit Rule icon. The Edit Rule pop-up window opens.



Select Rule

Click Edit Rule

Edit policy

Severity: 4

Action: Alert

Status

Labels: Detection, Enforce In Detection

i.e. 3, 5-9 , HTTP or DNP3

Message: Protocol Name: Modbus | Function Code: 90 | Sub Function Code: 48 | Unit ID: 0

Procedure

VLAN: 0 Enter Vlan

i.e. 0-2048

Ethertype: 0x0800

Source MAC: 00:0f:1f:c8:bd:1f Enter MAC

i.e. xx:xx:xx:xx:xx:xx

In the Edit Rule pop-up window, you can do the following:

- Expand each relevant section and edit the fields as required (see Policy Rule Fields)
- Reset the Details to their default settings
- Remove a Layer
- Reset a Layer to its default settings

4. Click Apply to apply the change. A message confirms the changes has been applied.

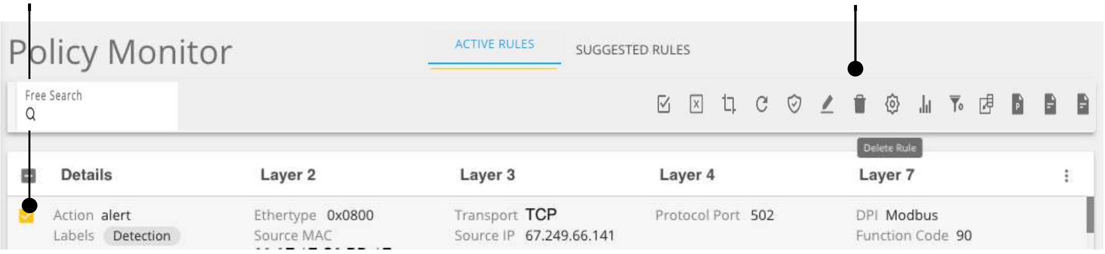
Delete a policy rule

1. Go to Policy Rules (Policy monitor > Active Rules).
2. Select the checkbox of the policy rule you want to delete.
3. Click the Delete icon, and when prompted click OK to delete the rule.

A message confirms the policy rule has been deleted.

Select rule

Click Delete Rule



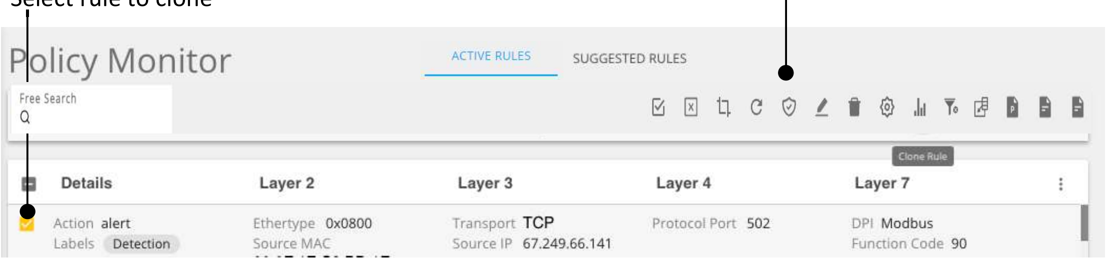
Details	Layer 2	Layer 3	Layer 4	Layer 7
Action alert Labels Detection	Ethertype 0x0800 Source MAC	Transport TCP Source IP 67.249.66.141	Protocol Port 502	DPI Modbus Function Code 90

Duplicate a policy rule

1. Go to Policy Rules (Policy monitor > Active Rules).
2. Select the checkbox of the policy rule you want to clone.
3. Click the Duplicate Rule icon. A message confirms the policy rule was successfully cloned.

Select rule to clone

Click Duplicate Rule



Details	Layer 2	Layer 3	Layer 4	Layer 7
Action alert Labels Detection	Ethertype 0x0800 Source MAC	Transport TCP Source IP 67.249.66.141	Protocol Port 502	DPI Modbus Function Code 90

Suggested Rules

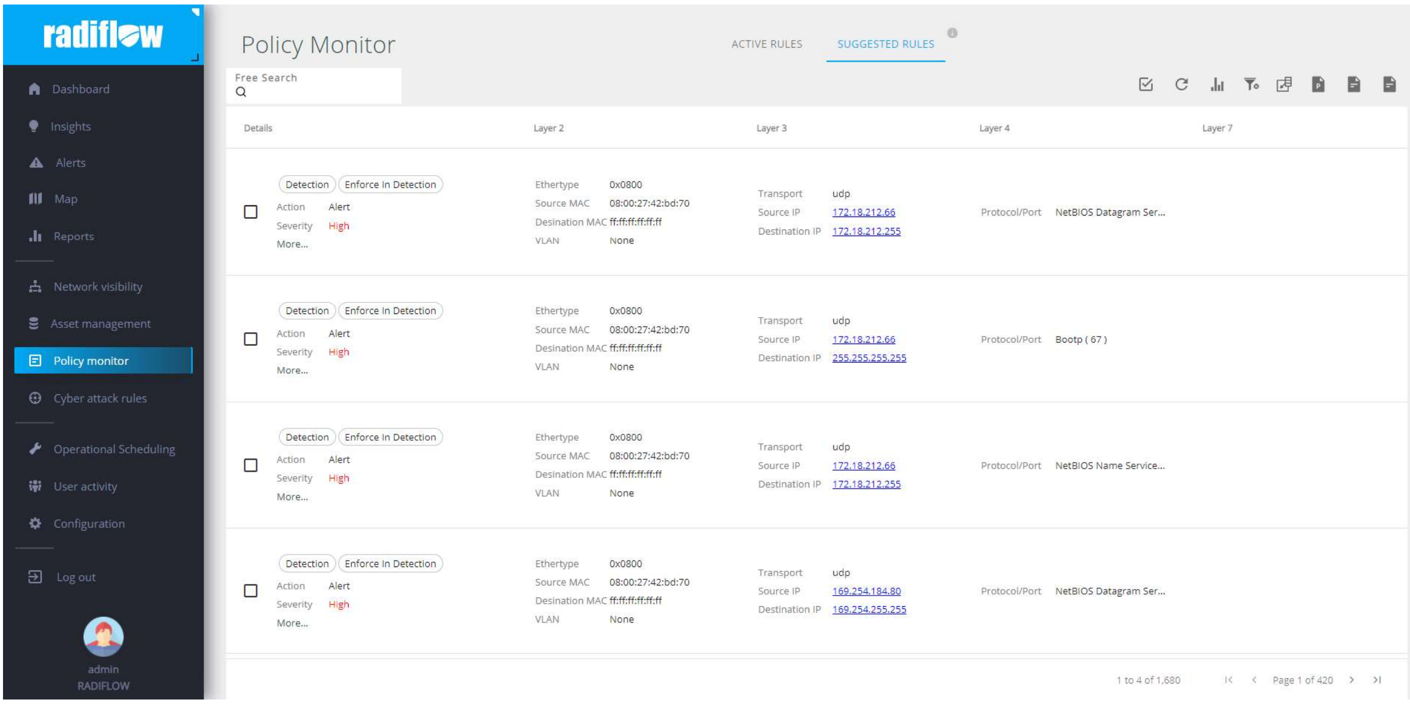
In the course of the learning stage, iSID creates policies based on the learned traffic. These policies can be based on regular IT protocols as well as industrial protocols such as Modbus, CIP, DNP3 and IEC 104. Policies created and suggested by iSID are not enabled until they are approved. As with manually created policy rules, suggested rules can be viewed, deleted, cloned, edited, and approved. When a suggested rule is approved, it is removed from the Suggested Rules list and added to the Policy Rules listing.

View Suggested Rules

The Suggested Rules panel displays details about automatically created policy rules. Access the Suggested Rules panel to view the complete rule definition including metadata as well as all layer configuration.

View Suggested Rule Details

Go to Suggested Rules (Policy monitor > Suggested Rules).
The Suggested Rules pane displays details about each suggested policy rule, such as its action trigger, severity, ID, status, creation dates, and Layer 2-Layer 7 details etc.



	Details	Layer 2	Layer 3	Layer 4	Layer 7
☐	Detection Enforce In Detection Action Alert Severity High More...	Ethertype 0x0800 Source MAC 08:00:27:42:bd:70 Desination MAC ff:ff:ff:ff:ff:ff VLAN None	Transport udp Source IP 172.18.212.66 Destination IP 172.18.212.255	Protocol/Port NetBIOS Datagram Ser...	
☐	Detection Enforce In Detection Action Alert Severity High More...	Ethertype 0x0800 Source MAC 08:00:27:42:bd:70 Desination MAC ff:ff:ff:ff:ff:ff VLAN None	Transport udp Source IP 172.18.212.66 Destination IP 255.255.255.255	Protocol/Port Bootp (67)	
☐	Detection Enforce In Detection Action Alert Severity High More...	Ethertype 0x0800 Source MAC 08:00:27:42:bd:70 Desination MAC ff:ff:ff:ff:ff:ff VLAN None	Transport udp Source IP 172.18.212.66 Destination IP 172.18.212.255	Protocol/Port NetBIOS Name Service...	
☐	Detection Enforce In Detection Action Alert Severity High More...	Ethertype 0x0800 Source MAC 08:00:27:42:bd:70 Desination MAC ff:ff:ff:ff:ff:ff VLAN None	Transport udp Source IP 169.254.184.80 Destination IP 169.254.255.255	Protocol/Port NetBIOS Datagram Ser...	

1 to 4 of 1,680 |< < Page 1 of 420 > >|

- Use the search tools and search filters to search for specific policy rules
- Enable and disable rules
- Edit and approve a rule
- Delete a rule
- Approve a rule
- Hide or show individual columns
- Change the number of items viewed per page

Search for specific suggested rules

1. Go to Suggested Rules (Policy monitor > Suggested Rules).
2. Use the search box to search for a specific item.

Manage Suggested Rules

In the Suggested Rules pane, manage suggested rules as follows:

- Edit and approve a suggested rule
- Delete a suggested rule
- Approve a suggested rule
- Edit rule labels
- Edit rule actions

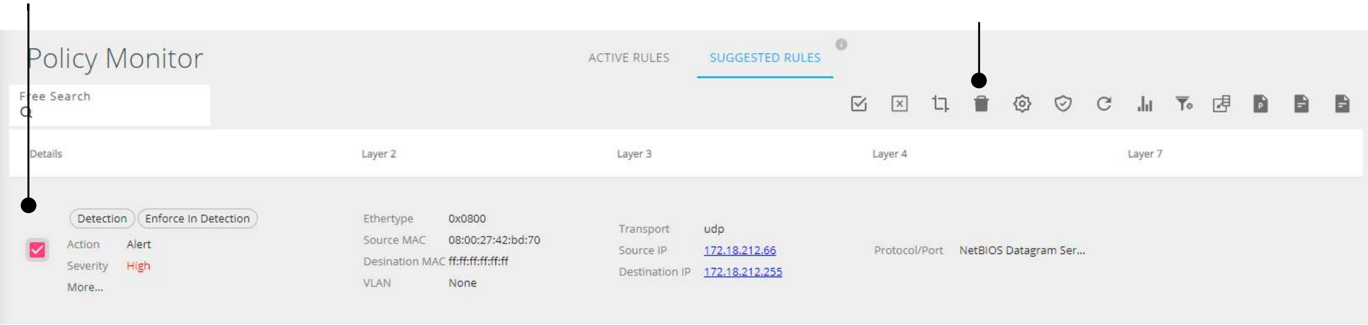
Delete a suggested rule

1. Go to Suggested Rules (Policy monitor > Suggested Rules).
2. Select the checkbox of the suggested rule you want to delete.
3. Click the Delete icon. At the prompt click OK to delete the rule.

A message confirms the suggested rule has been deleted.

Select rule

Click Delete Rule



Policy Monitor

ACTIVE RULES | SUGGESTED RULES

Free Search

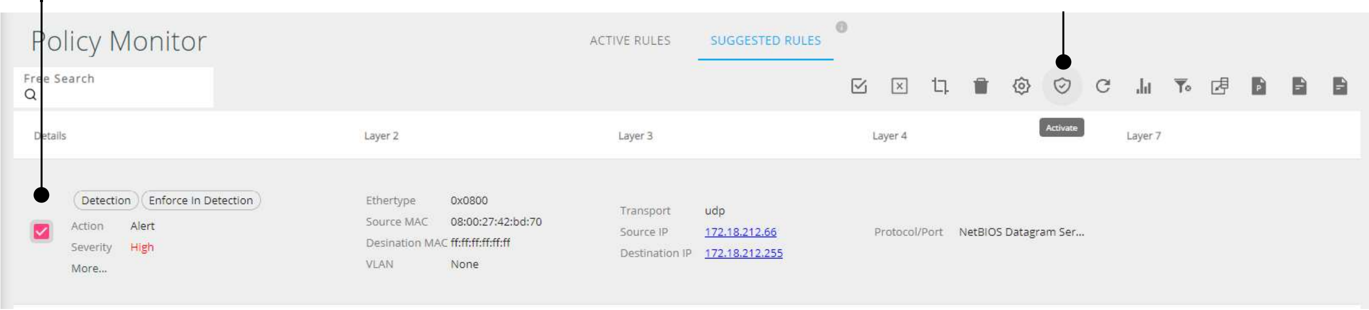
Details	Layer 2	Layer 3	Layer 4	Layer 7
☑ Detection, Enforce In Detection Action: Alert Severity: High More...	Ethertype: 0x0800 Source MAC: 08:00:27:42:bd:70 Desination MAC: ff:ff:ff:ff:ff:ff VLAN: None	Transport: udp Source IP: 172.18.212.66 Destination IP: 172.18.212.255	Protocol/Port: NetBIOS Datagram Ser...	

Approve a suggested rule

1. Go to Suggested Rules (Policy monitor > Suggested Rules).
2. Select the checkbox of the suggested rule you want to approve.
3. Click the Activate icon, and when prompted click OK to approve the rule.
    - A message confirms the suggested rule has been approved
    - The rule is moved from the Suggested Rules listing to the Policy Rules listing

Select suggested

Click Activate icon



Policy Monitor

ACTIVE RULES | SUGGESTED RULES

Free Search

Activate

Details	Layer 2	Layer 3	Layer 4	Layer 7
☑ Detection, Enforce In Detection Action: Alert Severity: High More...	Ethertype: 0x0800 Source MAC: 08:00:27:42:bd:70 Desination MAC: ff:ff:ff:ff:ff:ff VLAN: None	Transport: udp Source IP: 172.18.212.66 Destination IP: 172.18.212.255	Protocol/Port: NetBIOS Datagram Ser...	

Operational Scheduling

Overview

Occasionally, your team may need to perform operational activities on the network. Such activities typically generate a slew of false alerts for an intrusion detection system. To address this problem, iSID allows you to schedule operational changes.

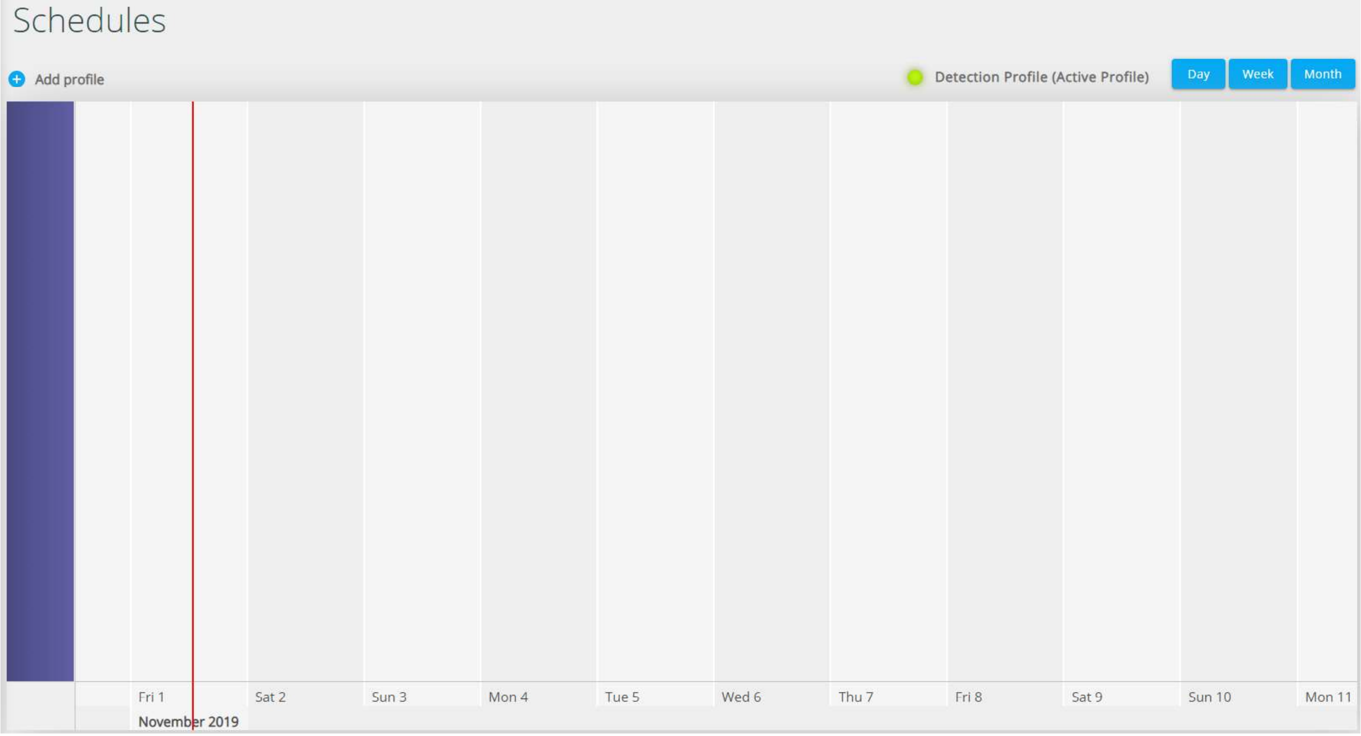
Scheduling operational changes is a 2-step process:

1. Add user-defined profiles. For each user-defined profile, specify which actions, alerts and settings are enabled.

2. Add a scheduled time - and assign a user-defined profile to that time slot.

Note: you can also add and manage user-defined profile under Configuration > Profiles.

Get familiar with the UI



1. Open Operational Scheduling.
2. On the top, left, you can add a user-defined profile:

   ⊕ Add profile

3. Any existing user-defined profiles display below that, on the left (and are read-only).

   Note: you can edit and manage user-defined profile under Configuration > Profiles.

4. A calendar view displays to the right of the profile names. You can double-click on a given day to add a schedule.

5. The system mode that is currently active displays in the top, right corner of the Operational Scheduling page. You can change the active mode from the Dashboard.

Add a user-defined profile

1. Open Operational Scheduling.
2. Click Add profile ⊕ (top, left).
3. Provide a profile name.
4. Click Expand + to define which actions, alerts and settings are enabled for each section under this profile. (See ‘Edit a profile’ for more detail.)
5. Click Apply to save.

Note: you can also add and manage user-defined profile under Configuration > Profiles.

Add a schedule

1. Open Operational Scheduling.
2. Double-click on the calendar view (right).
3. Fill in a name for the scheduled time.
4. Under When, fill in the following details:
1. The system mode for which this profile applies. For example, if you want this profile to take effect only if iSID is in learning mode, then select Learning.

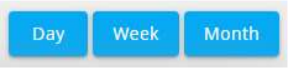
   Note: the system mode that is currently active displays in the top, right corner of the Operational Scheduling page. You can change the active mode from the Dashboard.

2. Frequency - choose once off or select a fixed period.
3. From and To dates.
5. Under Action, fill in the user-defined profile that will apply for this time slot. (See Add a user-defined profile.) This will determine which actions and alerts are enabled for that time period.
6. Click Apply to save.

Adjust the calendar view

You can adjust the calendar view to display your desired segment of time:

1. Open Operational Scheduling.
2. Click on Day/Week/Month (top, right), to display your desired segment of time:



3. Click and drag the calendar view to the right to view additional dates.

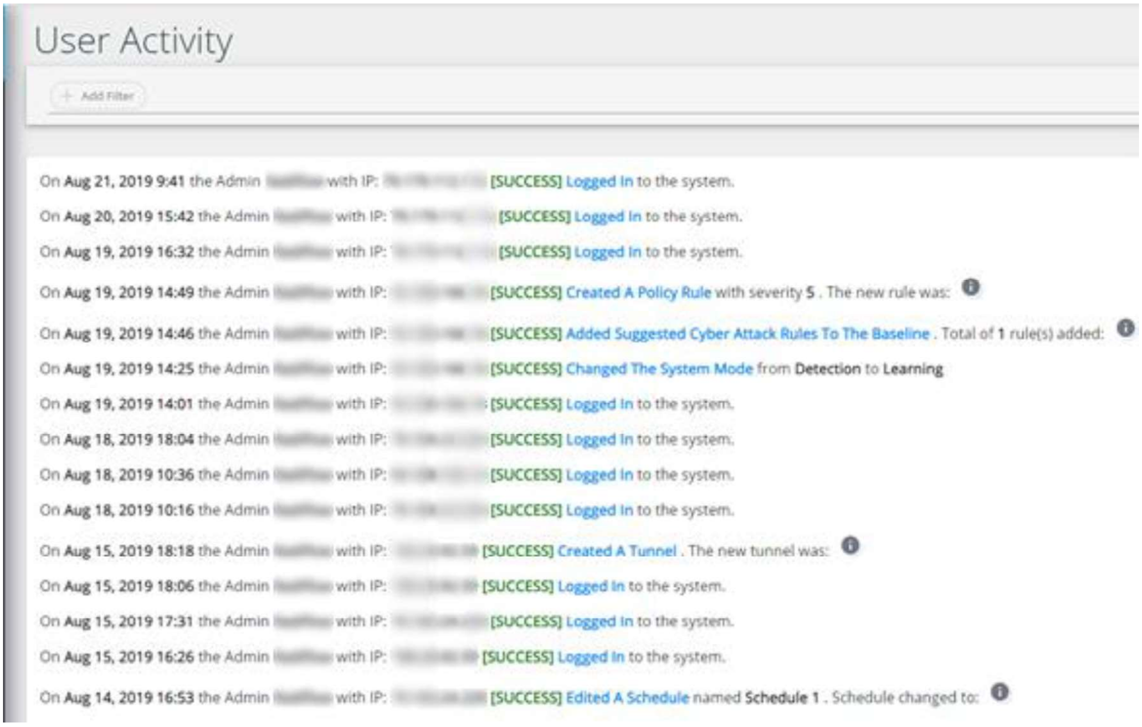
User Activity

User actions performed via the iSID web interface are logged and recorded in an internal database. This is useful for tracking when configuration changes were made - and by whom.

This activity log can be viewed in the User Activity screen.

View the user activity log

Open the User Activity pane to view the user activity log:



User Activity

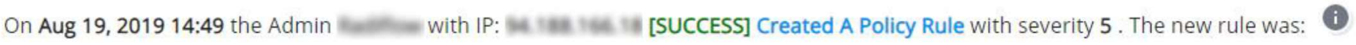
```
On Aug 21, 2019 9:41 the Admin [redacted] with IP: [redacted] [SUCCESS] Logged In to the system.
On Aug 20, 2019 15:42 the Admin [redacted] with IP: [redacted] [SUCCESS] Logged In to the system.
On Aug 19, 2019 16:32 the Admin [redacted] with IP: [redacted] [SUCCESS] Logged In to the system.
On Aug 19, 2019 14:49 the Admin [redacted] with IP: [redacted] [SUCCESS] Created A Policy Rule with severity 5 . The new rule was: 
On Aug 19, 2019 14:46 the Admin [redacted] with IP: [redacted] [SUCCESS] Added Suggested Cyber Attack Rules To The Baseline . Total of 1 rule(s) added: 
On Aug 19, 2019 14:25 the Admin [redacted] with IP: [redacted] [SUCCESS] Changed The System Mode from Detection to Learning
On Aug 19, 2019 14:01 the Admin [redacted] with IP: [redacted] [SUCCESS] Logged In to the system.
On Aug 18, 2019 18:04 the Admin [redacted] with IP: [redacted] [SUCCESS] Logged In to the system.
On Aug 18, 2019 10:36 the Admin [redacted] with IP: [redacted] [SUCCESS] Logged In to the system.
On Aug 18, 2019 10:16 the Admin [redacted] with IP: [redacted] [SUCCESS] Logged In to the system.
On Aug 15, 2019 18:18 the Admin [redacted] with IP: [redacted] [SUCCESS] Created A Tunnel . The new tunnel was: 
On Aug 15, 2019 18:06 the Admin [redacted] with IP: [redacted] [SUCCESS] Logged In to the system.
On Aug 15, 2019 17:31 the Admin [redacted] with IP: [redacted] [SUCCESS] Logged In to the system.
On Aug 15, 2019 16:26 the Admin [redacted] with IP: [redacted] [SUCCESS] Logged In to the system.
On Aug 14, 2019 16:53 the Admin [redacted] with IP: [redacted] [SUCCESS] Edited A Schedule named Schedule 1 . Schedule changed to: 
```

Each log entry displays the following color-coded information:

- Date
- Username and IP of user
- Success/Failure
- Action description

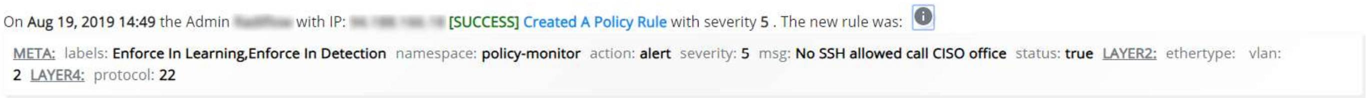
Expand the action description

1. Open the User Activity pane.
2. Identify a log entry of interest:



```
On Aug 19, 2019 14:49 the Admin [redacted] with IP: [redacted] [SUCCESS] Created A Policy Rule with severity 5 . The new rule was: 
```

3. Click on the more info icon (far right) to show more information about the action:



```
On Aug 19, 2019 14:49 the Admin [redacted] with IP: [redacted] [SUCCESS] Created A Policy Rule with severity 5 . The new rule was: 
META: labels: Enforce In Learning,Enforce In Detection namespace: policy-monitor action: alert severity: 5 msg: No SSH allowed call CISO office status: true LAYER2: ethertype: vlan:
2 LAYER4: protocol: 22
```

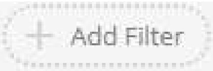
Note:

- The more info ⓘ icon is shown for relevant log entries only.
- Where relevant, multiple more info ⓘ icons are provided for different segments of the action description.
- The more info ⓘ icon is sensitive to the context of the action. The information displayed will depend on the type of action taken. Some examples include:
  - The set of values that previously existed for an entity - prior to the Edit action
  - The set of values that exist for a newly added entity - after the Create action
  - Etc.

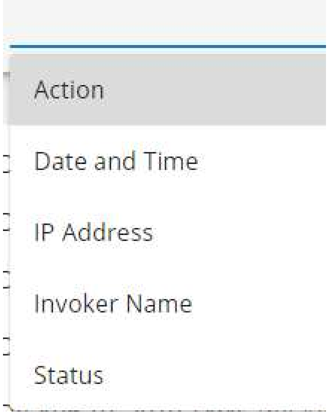
Apply a filter

To filter the log of user actions:

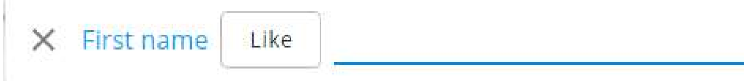
1. Open the User Activity pane.
2. Click on the Add filter button (top, left):



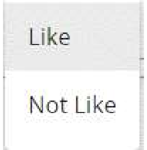
3. Choose a column:



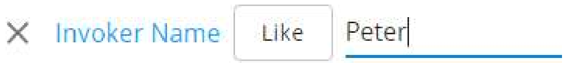
4. To filter for rows that do match, select Like (or Equal to - depending on the column):



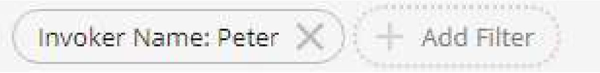
5. To filter for rows that do not match, select Not Like (or Not equal to - depending on the column):



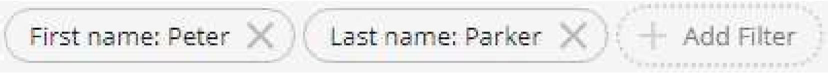
6. Type a value:


✕ Invoker Name | Like | Peter

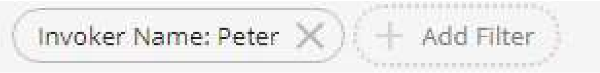
7. Click on Search 🔍 (far right) or tap the Enter key. The applied filter displays at the top of the page - and the rows are filtered accordingly:


Invoker Name: Peter ✕ | + Add Filter

8. You can easily combine multiple filters:


First name: Peter ✕ | Last name: Parker ✕ | + Add Filter

9. To remove a filter, click the Remove ✕ icon:


Invoker Name: Peter ✕ | + Add Filter

Download the log

It is often useful to download the user activity log in CSV or JSON format. You can then import the downloaded file into your own spreadsheet, database or third-party application - and consume/massage the data as needed.

To download the user activity log:

1. Open the User Activity pane.

2. Click on Export as CSV (top, right) or Export as JSON (top, far right).

Configuration

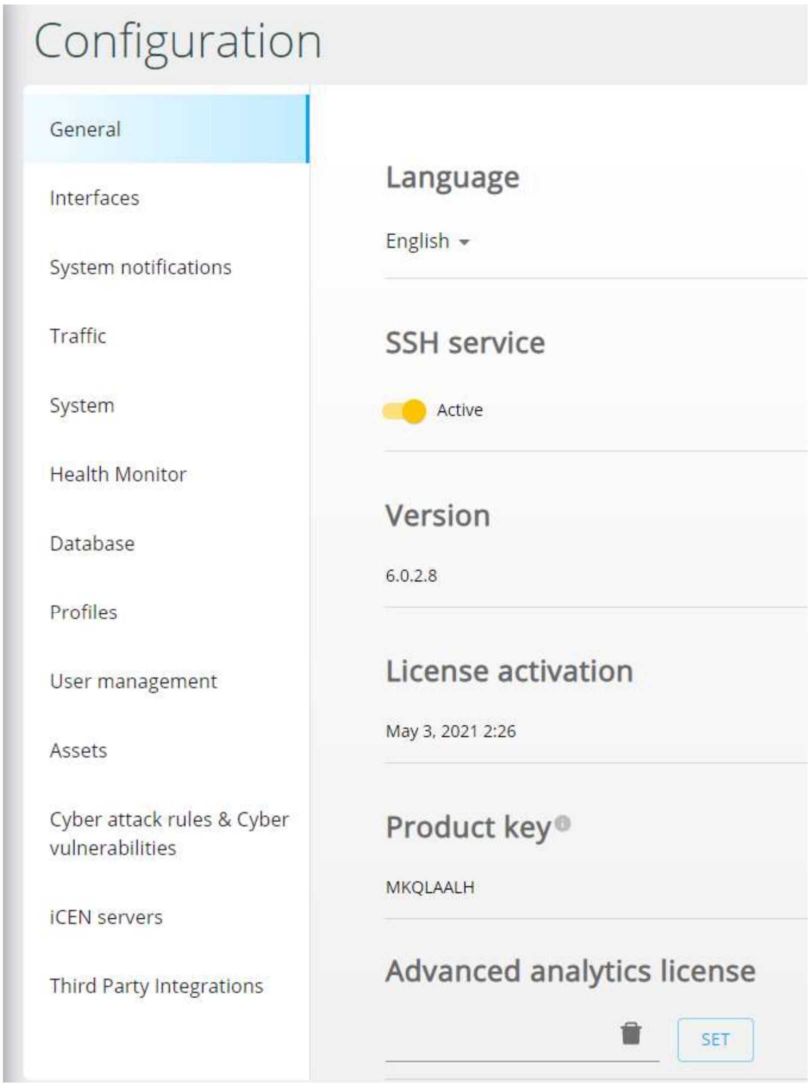
There are a few basic configuration steps that are required before working with Radiflow iSID

- General configuration - check parameters such as the syslog server configuration, timeout interval, and SSH mode.
- Defining procedures - define the procedure to be followed when a specified event occurs.
- Defining interfaces - iSID system must have a minimum of one defined management interface and one other interface for listening to network traffic.

General

Use the General configuration tab to do the following:

- Choose the UI and input language
- Activate/turn off SSH (secure shell)
- View the iSID version, license start date and product key



Language

English

SSH service

Active

Version

6.0.2.8

License activation

May 3, 2021 2:26

Product key

MKQLAALH

Advanced analytics license

Language

You can change the display and input language for ISID under the General configuration tab (top).

Note: currently, the following 2 languages are supported:

- English (default)
- German

Activate/turn off SSH

1. Go to General (Configuration > General).
2. Toggle the SSH service on or off.
   - To activate SSH service and provide a secure channel over the network, toggle SSH service to Active.
   - To deactivate SSH service and stop providing a secure channel over the network, toggle SSH service to Inactive.

Product key

Radiflow iCEN is a separate solution that monitors your iSID instances.

When you configure iCEN, you will need to add configuration details for each iSID instance - including the product key. You can copy the iSID product key from the General configuration tab (bottom). For further information, refer to the iCEN User Guide.

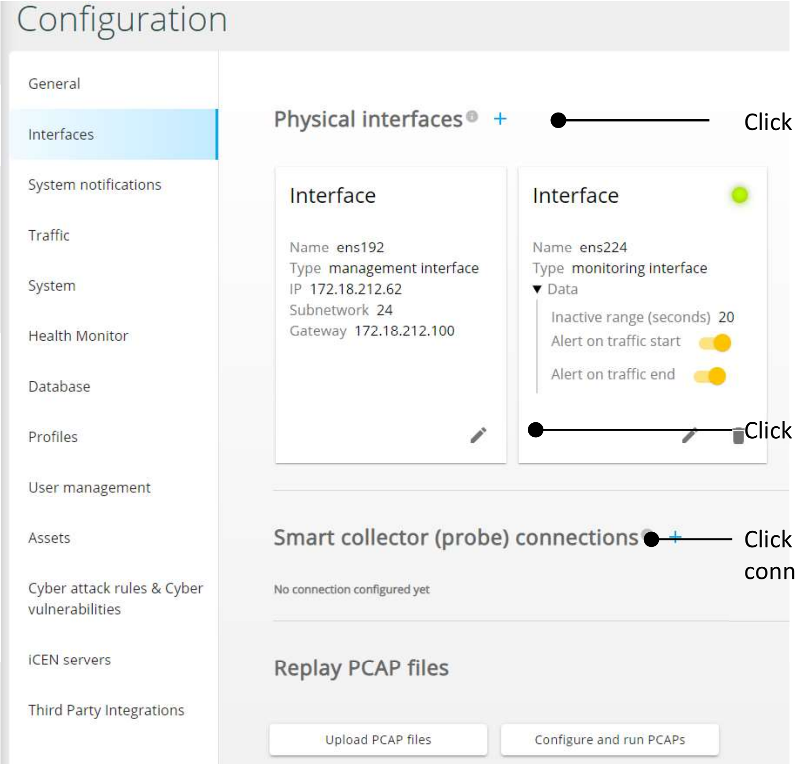
Note: Your iCEN configuration also needs to be added within iSID. See Configuration > ICEN Servers in this guide.

Interfaces

Radiflow iSID requires a physical interface.

In addition, to the mandatory physical interface, you can also create a smart probe connection.

Each network interface must have a unique identifier name.



Interface

Name ens192
Type management interface
IP 172.18.212.62
Subnetwork 24
Gateway 172.18.212.100

Interface

Name ens224
Type monitoring interface
▼ Data
Inactive range (seconds) 20
Alert on traffic start ●
Alert on traffic end ●

No connection configured yet

Click to create a new interface

Click Edit icon to edit an interface

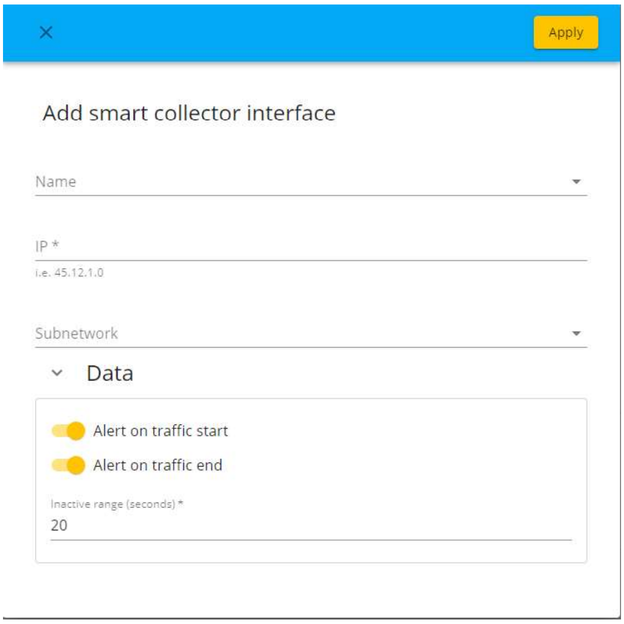
Click to create a new smart probe connection

Configure a physical interface

1. Go to Interfaces (Configuration > Interfaces).
2. Click + to create a new physical interface.
3. Select New monitoring interface or New smart probe interface

- A monitored interface passively listens to network traffic. This port does not transmit any packets, only receives traffic and does not have an IP address
- A smart probe interface listens to multiple remote networks using Radiflow iSAP devices

4. The Add New Interface pop-up window opens.



Add smart collector interface

Name

IP *

i.e. 45.12.1.0

Subnetwork

Data

Alert on traffic start

Alert on traffic end

Inactive range (seconds) *

20

5. In the Name field, select the physical interface name from the list of interfaces.

If you created a smart probe interface proceed to the next step; if you created a monitored interface continue to step 8.

6. In the IP field, enter the IP address of the smart probe interface.
7. Select the subnetwork number from the list (1-31).
8. In the Data section, do the following:
   - If Event on traffic start is toggled to on, an event is raised when traffic starts
   - If Event on traffic ends is toggled to on, an event is raised when traffic ends
   - In the Inactive range (seconds) field, use the arrows to specify the inactive range interval of traffic absence for the device to be recognized as inactive.
9. Click Apply. A message confirms a new physical interface has been added.

Edit a physical interface

1. Go to Interfaces (Configuration > Interfaces).
2. Click the edit icon of the physical interface you want to edit. The Edit interface pop-up window opens.
3. In the Edit interface pop-up window, do the following:
   - Edit the name of the physical interface
   - Edit the IP address
     Important: Before changing the management IP address, verify network connectivity to the new IP address. Once an IP address has been entered, you will be requested to Apply and Reload; the web page will reload using the newly-configured IP address.

- Edit the subnetwork number
- Edit the Gateway IP address

4. Click Apply. A message confirms the interface changed.

View existing physical interfaces

1. Go to Interfaces (Configuration > Interfaces).
2. View the name, type, IP address, subnetwork, and gateway details of an existing physical interface.

Configure a smart probe connection

In addition to analysis of the traffic received from the physical monitored network interface, Radiflow iSID can also receive and analyze traffic coming from multiple remote sites and network segments.

To do this, an RF-2180 iSAP is installed at each remote site as the destination of a port mirroring. The iSAP compresses the received traffic and transfers it to the iSID using a GRE tunnel.

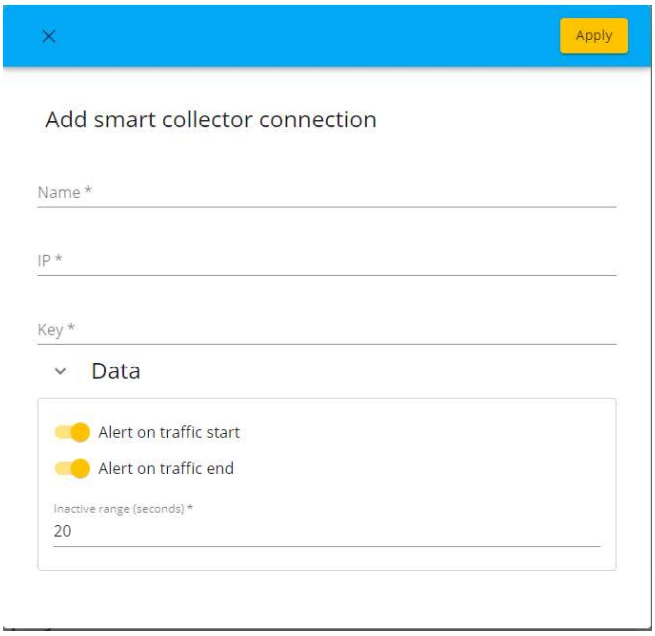
In order for the iSID to communicate with the smart probe, the following must be defined

- Smart probe physical interface
- Remote iSAP properties (user defined name, GRE key and iSAP IP address) for each remote site

1. Go to Interfaces (Configuration > Interfaces).
2. Click + to create a new smart probe connections.

The Add smart probe connection pop-up window opens.

Note: Connections will not be activated without a smart probe interface.



Add smart collector connection

Name *

IP *

Key *

Data

Alert on traffic start

Alert on traffic end

Inactive range (seconds) *
20

In the Add smart probe connection pop-up window, enter the smart probe details as follows:

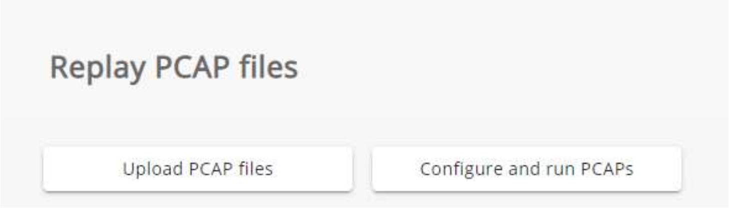
- Name - a user-defined name to identify the connection
- IP - remote IP address of the iSAP device
- Key - GRE key to be used by the iSAP device

3. In the Data section, do the following:

- If Event on traffic start is toggled to on, an event is raised when traffic starts
- If Event on traffic ends is toggled to on, an event is raised when traffic ends
- In the Inactive range (seconds) field, use the arrows to specify the time interval for receiving traffic, meaning: after X time the device will be recognized as inactive.

4. Click Apply. A message confirms the smart probe connection has been added.

Replay a PCAP file



Replay PCAP files

Overview

You can upload and replay 1 or more PCAP files, causing iSID to process and analyze the recorded traffic. iSID will process the recorded traffic as if it were live - e.g. add newly discovered devices, generate security alerts, etc.

Note: Traffic recorded by iSID can also be downloaded as a PCAP file - e.g. for further inspection and analysis.

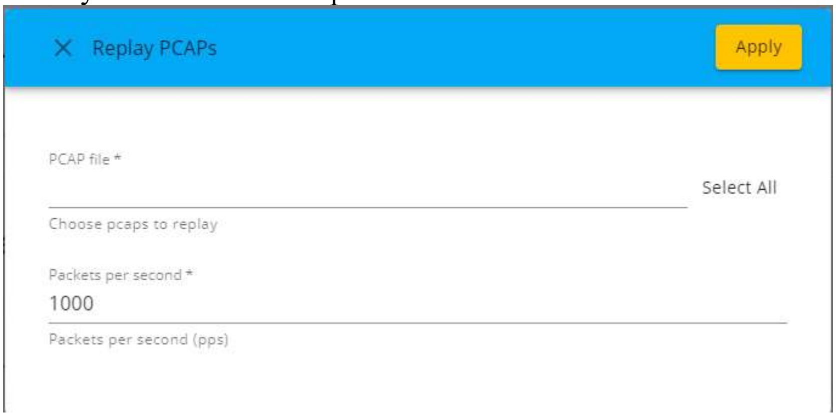
Upload PCAP files

1. Go to Configuration > Interfaces > Replay PCAP Files.
2. Click on the Upload PCAP Files button (left).
3. In the Upload PCAP window, click Choose PCAP files, browse for the relevant file(s), and click Upload (top, right).
4. A pinwheel animation displays while the files upload. Once complete, a message displays on the bottom, right.

Replay PCAP files

1. Go to Configuration > Interfaces > Replay PCAP files.
2. Click on the Configure and run PCAPs button (right):
3. In the Replay PCAP window:
1. Select the desired PCAP file(s) from the dropdown list.

Note: you can select multiple files in succession:



PCAP file *

Choose pcaps to replay

Packets per second *
1000

Packets per second (pps)

2. Select the number of times to loop (replay).
3. Enter the desired packets per second (or leave the default value).
4. Click Apply.

Delete all PCAP files

Occasionally, the system will prompt you delete all existing PCAP files, before allowing you to upload a new one.
Note:

- This function deletes all uploaded PCAP files.
- This function is located under Configuration > System.

1. Go to Configuration > System > User PCAP files.
2. Click on Delete all uploaded PCAPs and confirm.

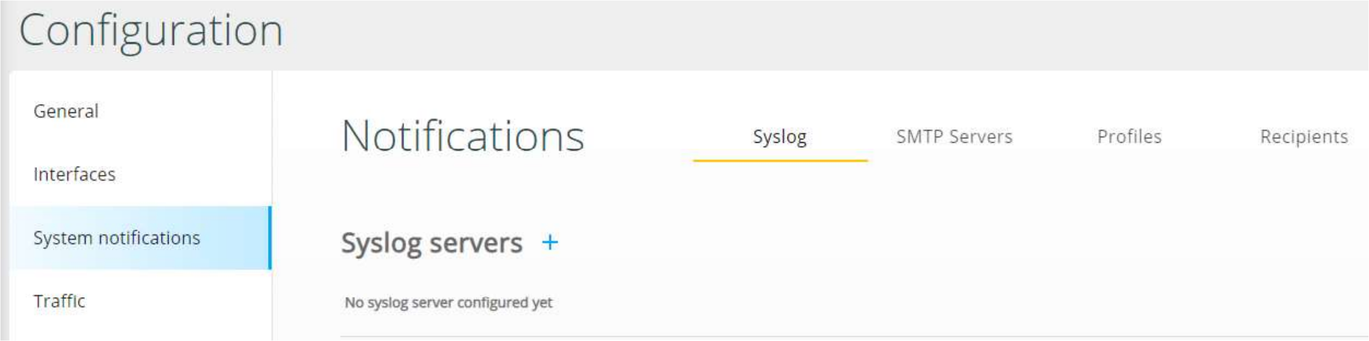
System Notifications

You can configure iSID to send syslog notifications to a syslog server (for example: SIEM) and email notifications by defining syslog and SMTP servers.

The syslog and SMTP profiles let you define different parameters for different servers, such as what type of notifications should be sent, which recipients the notifications should be sent to, and how often to send them.

Use the System Notifications configuration tab to do the following:

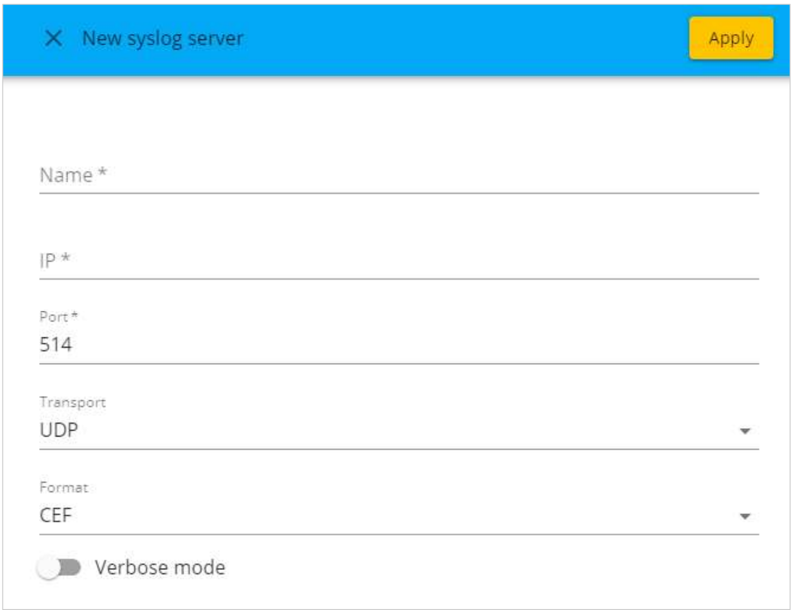
- Define syslog servers
- Define SMTP servers
- Manage the notification recipients
- Configure syslog and SMTP profiles



No syslog server configured yet

Define a syslog server

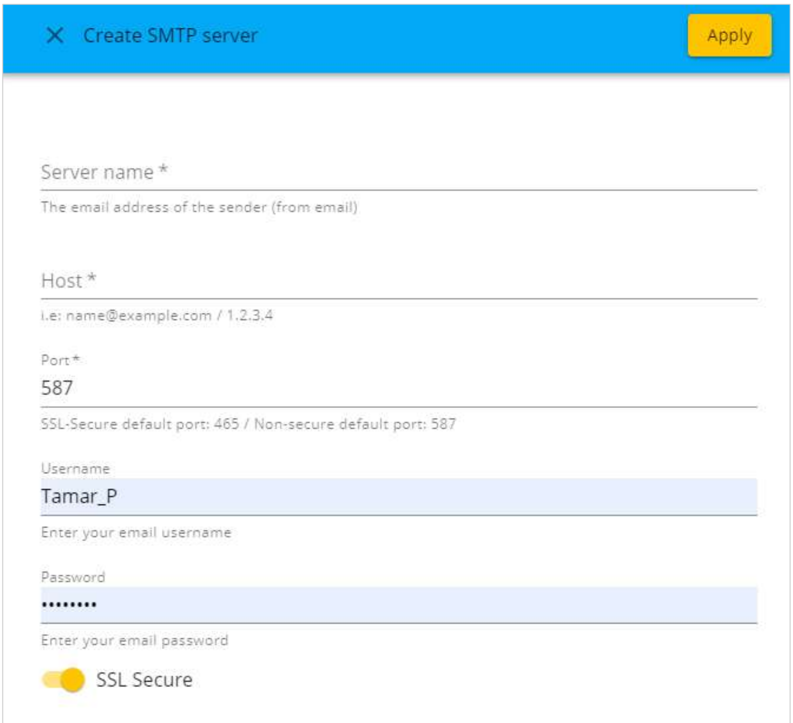
1. Open Configuration > System Notifications > Syslog.
2. In the Syslog Servers section, click on Add +.
3. The New syslog server pop-up window opens.



4. In the New syslog server pop-up window, enter the syslog server details as follows:
   - Name - enter the name of the syslog server
   - IP - syslog server IP address
   - Port - syslog server port number
   - Transport - select either UDP or TCP
   - Format - select either CEF or LEEF
   - Verbose mode – set the toggle button to enable or disable verbose mode
     - If verbose mode is on, iSID will send a syslog message for each instance a repeating abnormal behavior is detected
     - If verbose mode is off, iSID will send a syslog message only once per abnormal behavior
5. Click Apply. A message confirms the syslog server has been added.

Define an SMTP server

1. Go to Configuration > System Notifications > SMTP Servers.
2. In the SMTP Servers section, click on Add +.
3. The Create SMTP server pop-up window opens.



Create SMTP server

Server name *

The email address of the sender (from email)

Host *

i.e: name@example.com / 1.2.3.4

Port *

587

SSL-Secure default port: 465 / Non-secure default port: 587

Username

Tamar_P

Enter your email username

Password

••••••••

Enter your email password

SSL Secure

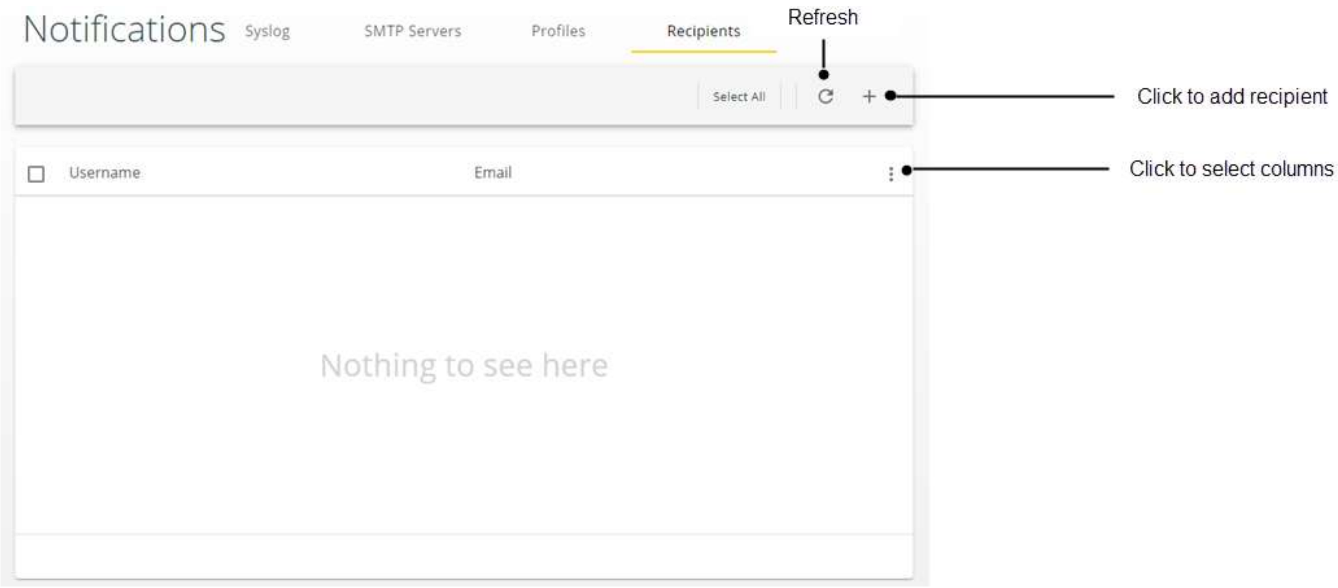
4. In the Create SMTP server pop-up window, enter the SMTP server details as follows:
   - Server name - enter the email address of the sender
   - Host - SMTP server hostname or IP address
   - Port - SMTP server port number
   - Username – the email server username
   - Password - the email server password
   - SSL Secure - set the toggle button to enable or disable SSL secure mode
5. Click Apply. A message confirms the SMTP server has been added.

Manage recipients

To manage the recipients, open Configuration > System Notifications > Recipients.

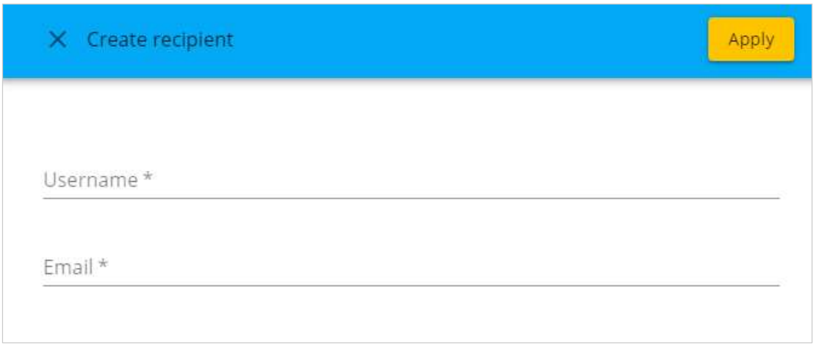
In the Recipient listing, you can:

- Add a recipient
- Refresh the listing
- Choose the columns to be displayed
- Edit recipients (use Select All or individual check boxes)



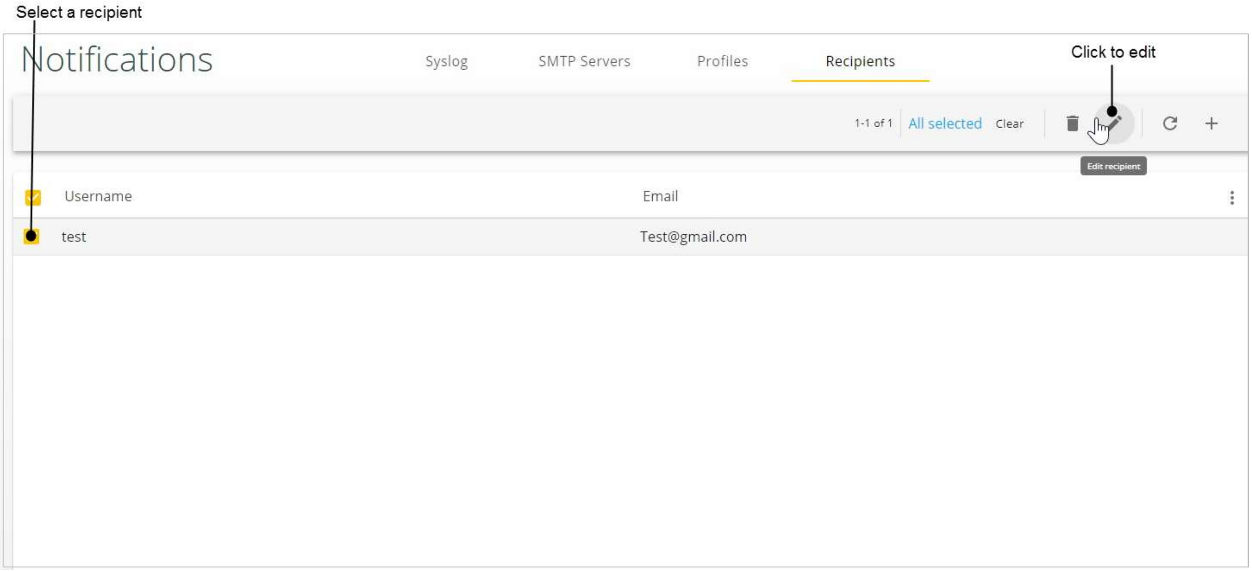
Add a recipient

1. Open Configuration > System Notifications > Recipients.
2. Click on Add +.
3. The Create recipient pop-up window opens.



4. Type in the username and email address of the recipient.
5. Click Apply. The new recipient appears in the listing.

Edit a recipient

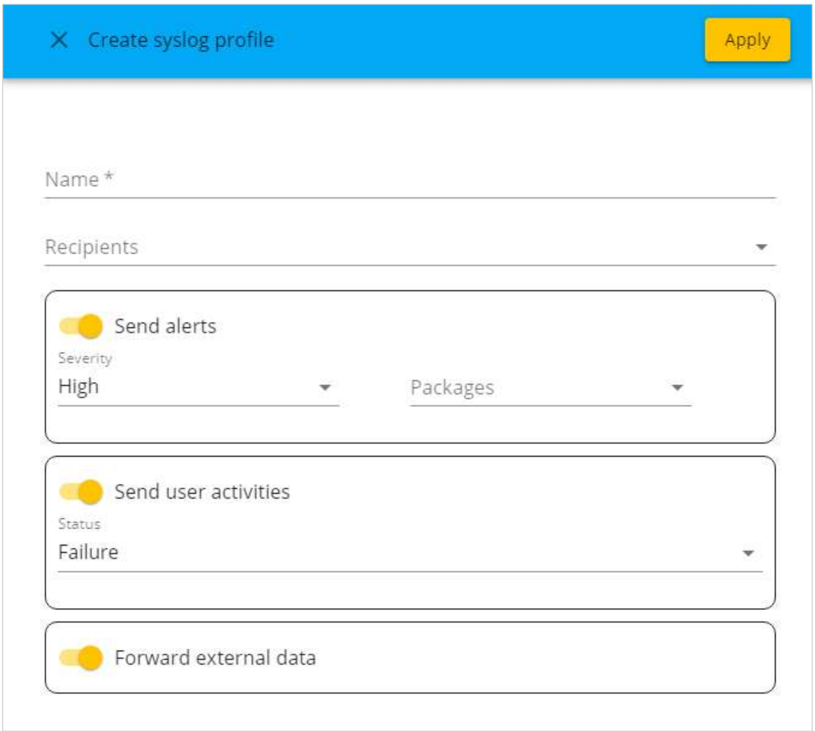


Username	Email
test	Test@gmail.com

1. Open Configuration > System Notifications > Recipients.
2. Select the checkbox of the profile you want to edit.
3. Click the Edit icon. The Edit Recipient pop-up window opens.
4. Edit the username and/or email as needed.
5. Click Apply. A message confirms the recipient was successfully updated.

Define a syslog profile

1. Open Configuration > System Notifications > Profiles.
2. In the Profiles section, click on Add +.
3. Select New Syslog profile.
4. The Create syslog profile pop-up window opens.



Send alerts

Severity
High

Send user activities

Status
Failure

Forward external data

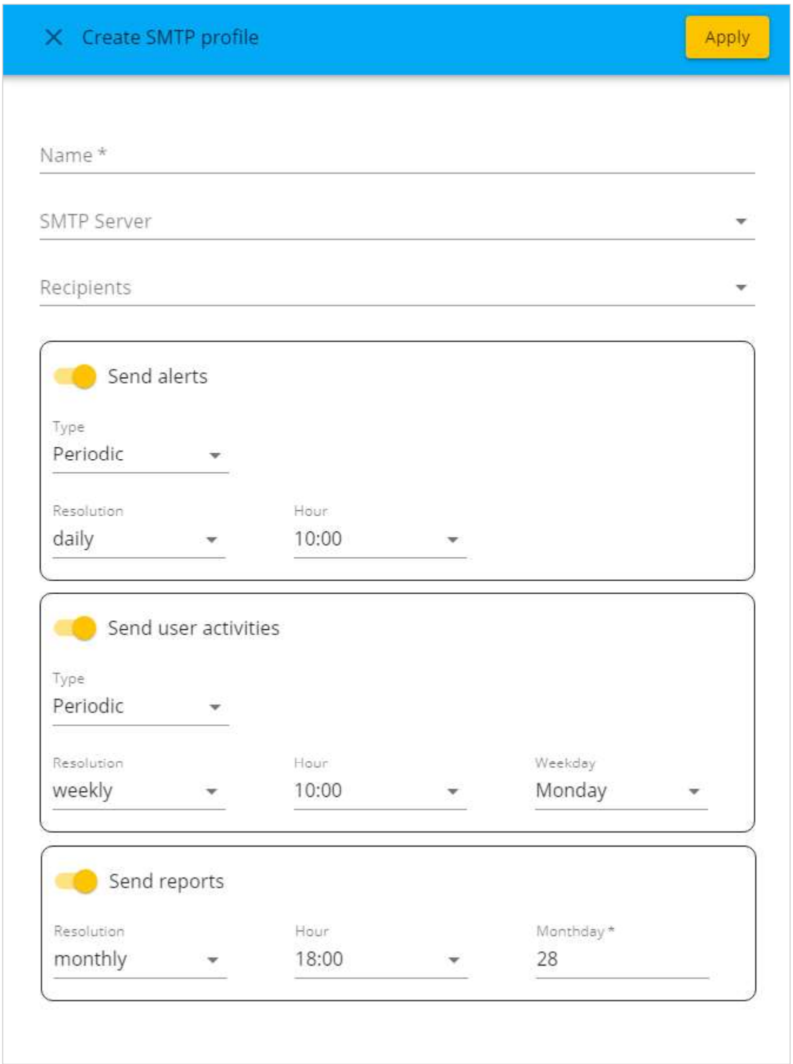
5. In the Create syslog profile pop-up window, enter the syslog profile details as follows:

- Name – give the profile a meaningful name
- Recipients – select all the recipients (syslog servers) for this profile
- Send alerts – toggle to enable sending alerts to display options:
  - Severity – select the all the severity levels of alerts that should be sent
  - Packages – select all the packages for which alerts should be sent

  Note: You must define both the severity **AND** packages
- Send user activities – toggle to enable sending notifications related to user activities to display options:
  - Status – should notifications be sent upon failure or upon success of user activities?
- Forward external data - toggle to enable or disable forwarding syslog events collected by iSID from external sources (see External Data)

Define an SMTP profile

1. Open Configuration > System Notifications > Profiles.
2. In the Profiles section, click on Add +.
3. Select New SMTP profile.
4. The Create SMTP profile pop-up window opens.



Name *

SMTP Server

Recipients

Send alerts

Type: Periodic

Resolution: daily | Hour: 10:00

Send user activities

Type: Periodic

Resolution: weekly | Hour: 10:00 | Weekday: Monday

Send reports

Resolution: monthly | Hour: 18:00 | Monthday *: 28

5. In the Create SMTP profile pop-up window, enter the SMTP profile details as follows:

- Name – give the profile a meaningful name
- SMTP Server - select the SMTP server for this profile
- Recipients – select all the recipients for this profile
- Send alerts – toggle to enable sending alerts to display options (see table of options below)
- Send user activities – toggle to enable sending notifications related to user activities to display options (see table of options below)
- Send reports – toggle to enable sending reports to display options (see table of options below)

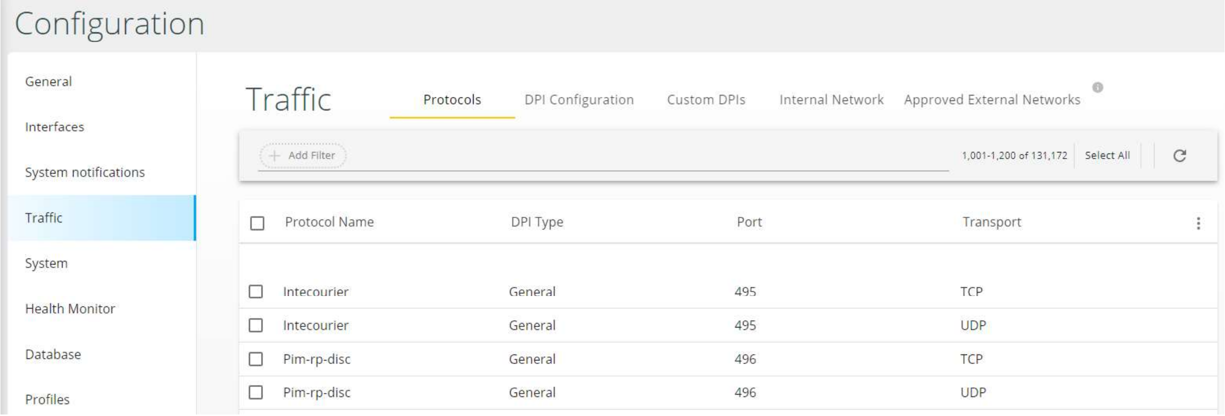
SMTP Profile Options

Option	Description
Type	• Periodic: send notifications at the specified frequency (resolution) and at the specified time of day (hour) • Real time: send notifications as they occur for the specified severity and packages
Resolution (periodic notifications)	How often to send notifications: • Daily • Weekly • Monthly
Hour (periodic notifications)	Select the time of day to send the notifications
Weekday (weekly notifications)	Select the day of the week on which to send notifications
Monthday (monthly notifications)	Select the date of the month on which to send notifications
Severity (real time alerts)	Select all the severity levels for which alerts should be sent
Packages (real time alerts)	Select all the packages for which alerts should be sent

Traffic

The Traffic pane lets you configure 3 aspects of your network:

- Protocol definitions
- Internal network
- Approved external networks



□	Protocol Name	DPI Type	Port	Transport
□	Intecourier	General	495	TCP
□	Intecourier	General	495	UDP
□	Pim-rp-disc	General	496	TCP
□	Pim-rp-disc	General	496	UDP

Defining your internal and approved external networks is important so that iSID can recognize which IPs are part of the monitored network and which are not and, therefore, should be alerted.

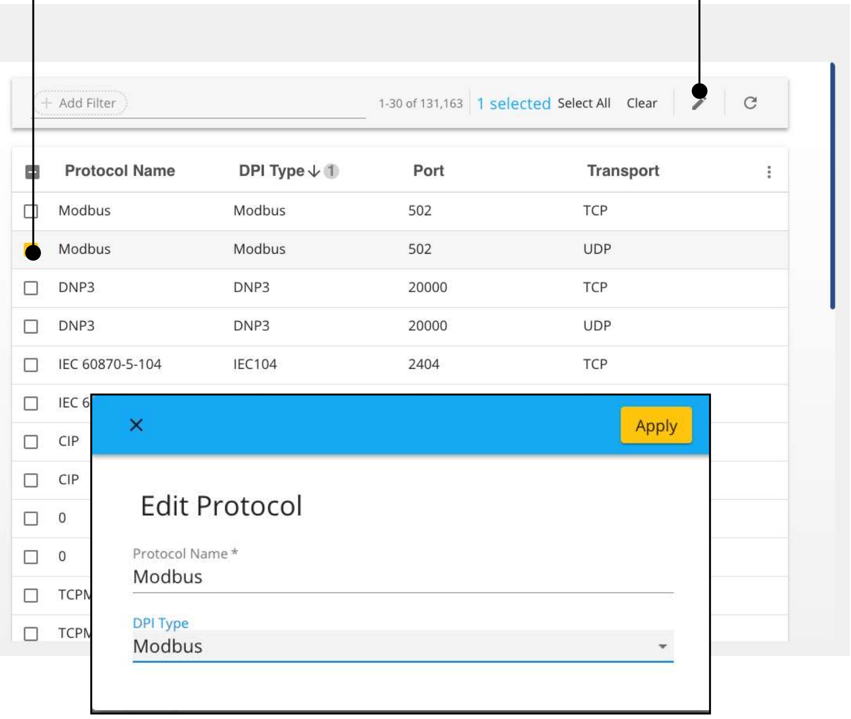
Protocols

Radiflow iSID enables users to configure protocol definitions of the 65K TCP and 65K UDP port, as follows:

- Protocol name - how the protocol is presented throughout the iSID screens
- DPI type - the method/structure iSID inspect packets

Edit protocol definitions

1. Go to Protocols (Configuration > Traffic > Protocols).
2. Select the checkbox of the protocol you want to edit.
3. Click the Edit icon. The Edit Protocol pop-up window opens.



Select a protocol

Edit icon

☐	Protocol Name	DPI Type ↓ 1	Port	Transport
☐	Modbus	Modbus	502	TCP
☑	Modbus	Modbus	502	UDP
☐	DNP3	DNP3	20000	TCP
☐	DNP3	DNP3	20000	UDP
☐	IEC 60870-5-104	IEC104	2404	TCP
☐	IEC 6			
☐	CIP			
☐	CIP			
☐	0			
☐	0			
☐	TCPM			
☐	TCPM			

Edit Protocol

Protocol Name *
Modbus

DPI Type
Modbus

4. In the Edit Protocol pop-up window, edit the protocol details as follows:
   - Protocol Name - edit the protocol name
   - DPI Type - select the type of deep packet inspection from the list of DPIs
5. Click Apply. A message confirms the protocol was successfully updated.

View protocols

Go to Protocols (Configuration > Traffic > Protocols).

- Use the search tools and search filters to search for specific protocols
- Hide or show individual columns
- Change the order the protocols appear
- Change the number of items viewed per page

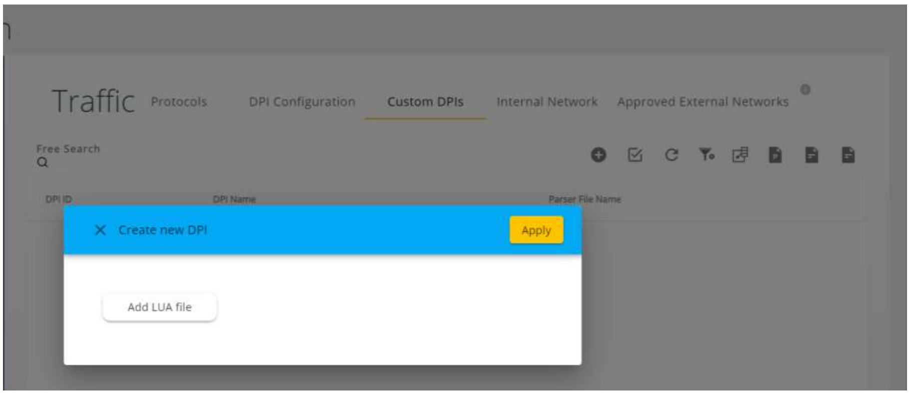
Custom parser

Radiflow iSID custom DPI function enables users to define and build a custom protocol dissector (parser). This gives more flexibility and control over the system protocols.

Parsers are created using Lua code. For full instructions on the custom parser, see the ***Setting up an iSID Custom Parser*** Technical Document

To add a custom parser:

1. Open the Custom DPI tab, or navigate to Custom DPI (Configuration > Traffic > Custom DPI)
2. Click the **Create** button ⊕ to open the Create new DPI dialogue



3. Click **Add LUA file**
4. Select the LUA file to upload.

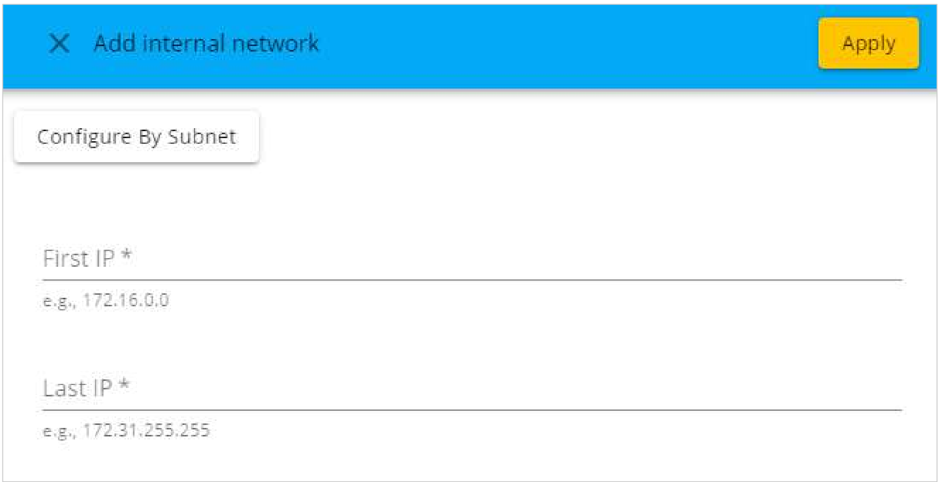
The Custom Parser is uploaded to the system.

Internal Network

You can define your internal network using either an IP range or by subnet.

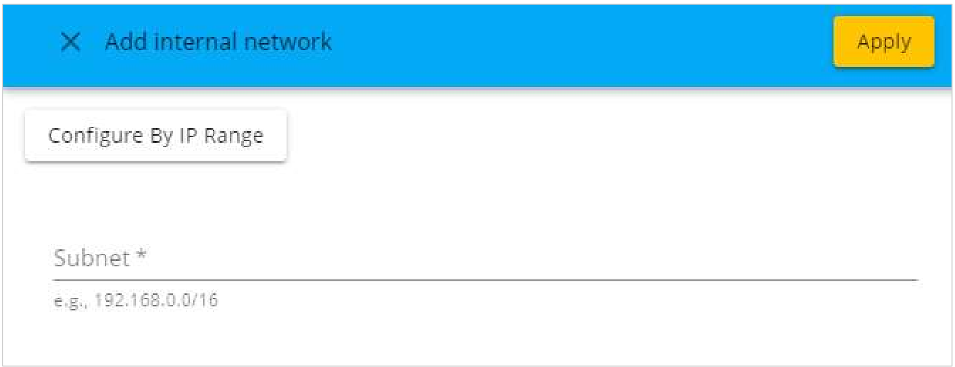
Add an internal network

1. Go to Internal Network (Configuration > Traffic > Internal Network).
2. Click on Add + .
3. The Add internal network pop-up window opens.



4. In the Add internal network pop-up window, enter first and last IP addresses of the network.

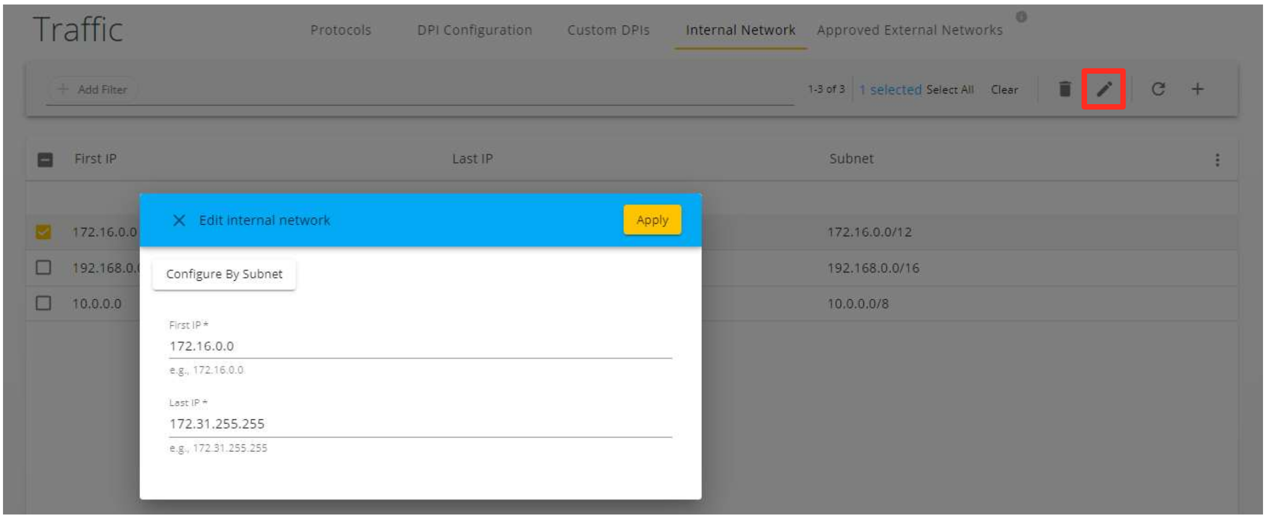
- To define the network by the subnet, click Configure By Subnet and enter the subnet



5. Click Apply. The network appears in the Internal Network listing.

Edit internal network definitions

1. Go to Internal Network (Configuration > Traffic > Internal Network).
2. Select the checkbox of the network you want to edit.
3. Click the Edit icon. The Edit internal network pop-up window opens.



	First IP	Last IP	Subnet
☑	172.16.0.0		172.16.0.0/12
□	192.168.0.		192.168.0.0/16
□	10.0.0.0		10.0.0.0/8

First IP *
172.16.0.0
e.g., 172.16.0.0

Last IP *
172.31.255.255
e.g., 172.31.255.255

4. In the Edit Protocol pop-up window, edit the internal network details as explained above in Add an internal network.
5. Click Apply. A message confirms the network was successfully updated.

View internal network

Go to Internal Network (Configuration > Traffic > Internal Network).

- Use the search tools and search filters to search for specific networks
- Hide or show individual columns
- Change the order the networks appear
- Change the number of items viewed per page

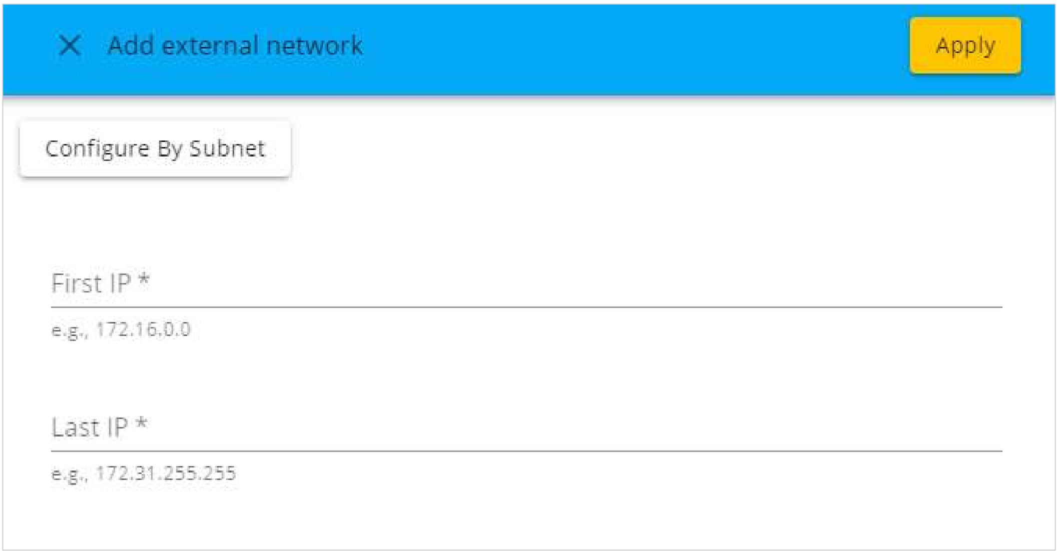
Approved External Networks

Define here all network segments for which connections from the internal network to these segments are approved network traffic. You can define them using either an IP range or by subnet.

Note that when the alert ‘IP address in your network is suspected to be on the internet’ appears in the Alerts pane and that IP address/network is added to the baseline (see Add an alert to baseline), it will also appear in this listing and can be edited.

Add an external network

1. Go to Approved External Networks (Configuration > Traffic > Approved External Networks).
2. Click on Add +.
3. The Add external network pop-up window opens.

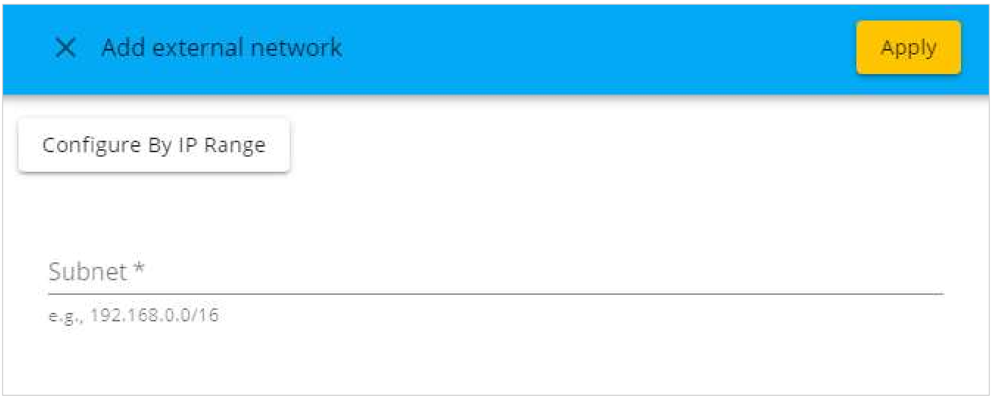


First IP *
e.g., 172.16.0.0

Last IP *
e.g., 172.31.255.255

4. In the Add external network pop-up window, enter first and last IP addresses of the network.

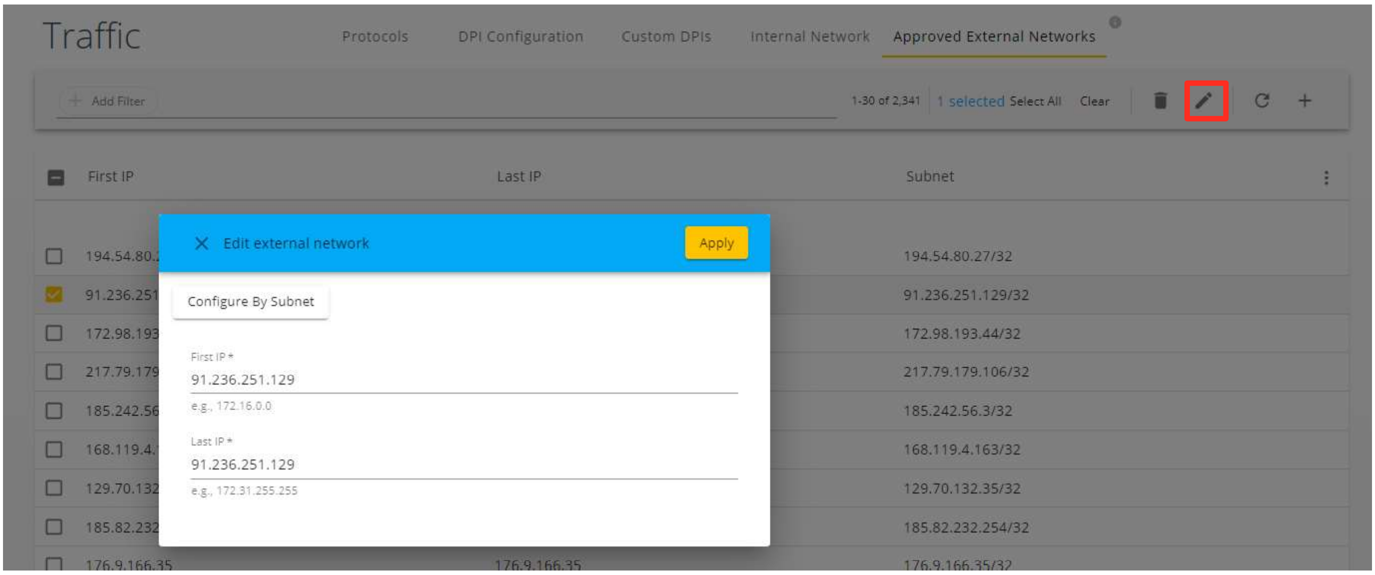
- To define the network by the subnet, click Configure By Subnet and enter the subnet



5. Click Apply. The network appears in the Approved External Networks listing.

Edit external network definitions

1. Go to Approved External Networks (Configuration > Traffic > Approved External Networks).
2. Select the checkbox of the network you want to edit.
3. Click the Edit icon. The Edit external network pop-up window opens.



First IP *: 91.236.251.129

Last IP *: 91.236.251.129

	First IP	Last IP	Subnet
☐	194.54.80.		194.54.80.27/32
☑	91.236.251		91.236.251.129/32
☐	172.98.193		172.98.193.44/32
☐	217.79.179		217.79.179.106/32
☐	185.242.56		185.242.56.3/32
☐	168.119.4.		168.119.4.163/32
☐	129.70.132		129.70.132.35/32
☐	185.82.232		185.82.232.254/32
☐	176.9.166.35	176.9.166.35	176.9.166.35/32

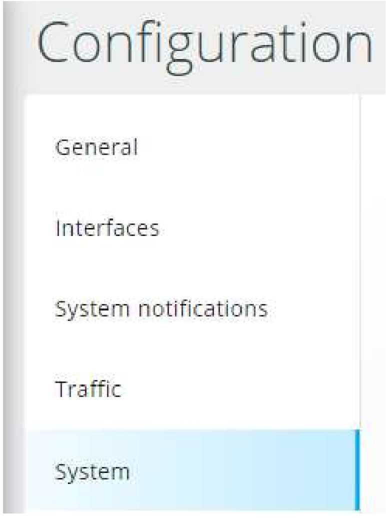
4. In the Edit Protocol pop-up window, edit the external network details as explained above in Add an external network.
5. Click Apply. A message confirms the network was successfully updated.

View external networks

Go to Approved External Networks (Configuration > Traffic > Approved External Networks).

- Use the search tools and search filters to search for specific networks
- Hide or show individual columns
- Change the order the networks appear
- Change the number of items viewed per page

System



Under Configuration > System, you can do the following:

- Clear data (data only or full factory reset)
- Restart the iSID application
- Delete all uploaded PCAPs

Clear data

1. Go to Configuration > System > Data Operations.
2. To delete data only - and preserve the current configuration - click Clear Data.
3. To delete data and configuration (i.e. restore the application to its initial defaults), click Factory Reset.

Restart the application

1. Go to Configuration > System > System Operations.
2. Click on System reboot.

Note: this restarts the iSID application - not the server itself.

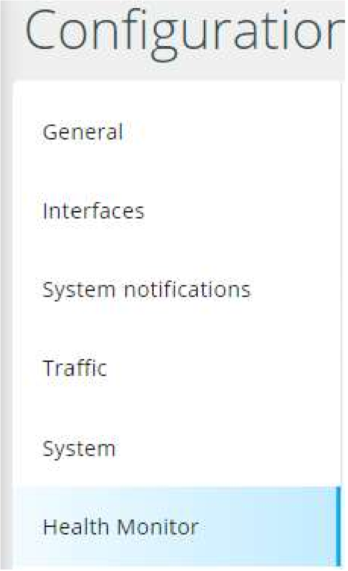
Delete all PCAP files

Occasionally, the system will prompt you delete all existing PCAP files, before allowing you to upload a new one (see Replay a PCAP file).

Note: This function deletes all uploaded PCAP files.

1. Go to Configuration > System > User PCAP files.
2. Click on Delete all uploaded PCAPs and confirm.

Health Monitor



Configuration

General

Interfaces

System notifications

Traffic

System

Health Monitor

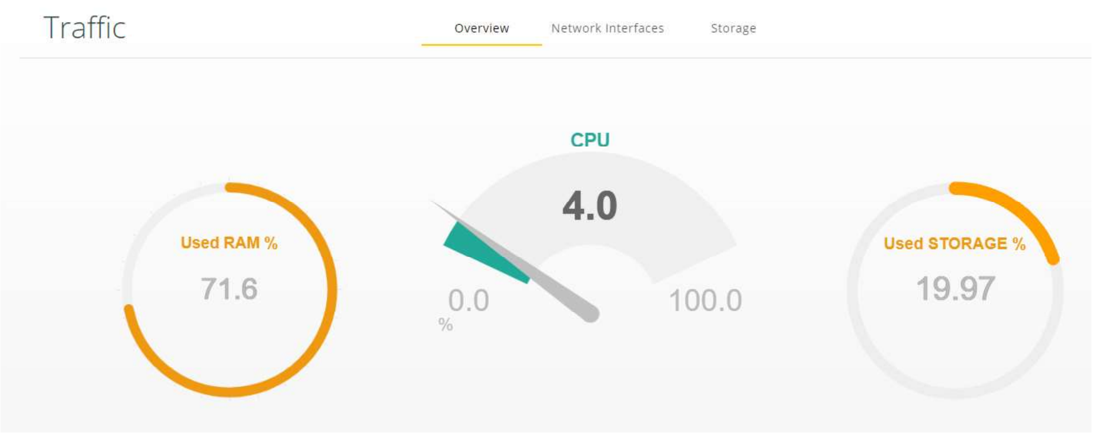
The Health Monitor shows key performance metrics for your iSID Server. The screen is divided into 3 tabs:

1. Overview
2. Network interfaces
3. Storage

Overview

The Overview tab shows performance stats for:

- RAM
- CPU
- Used Storage



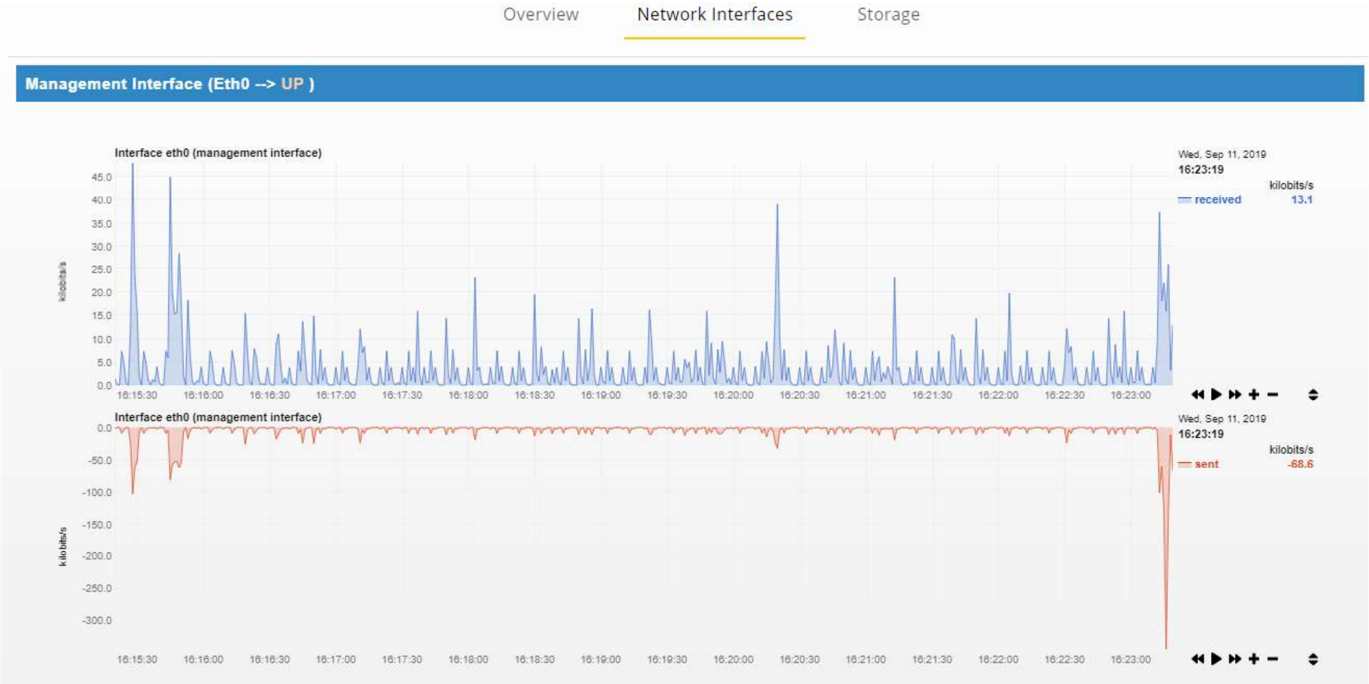
Traffic

Overview Network Interfaces Storage

Network Interfaces

The Network interfaces tab shows usage stats for each interface defined under Configuration > Interfaces. The following stats are displayed for each interface:

- Is the interface UP or DOWN? (shown in title bar)
- Traffic received (live graph)
- Traffic sent (live graph)



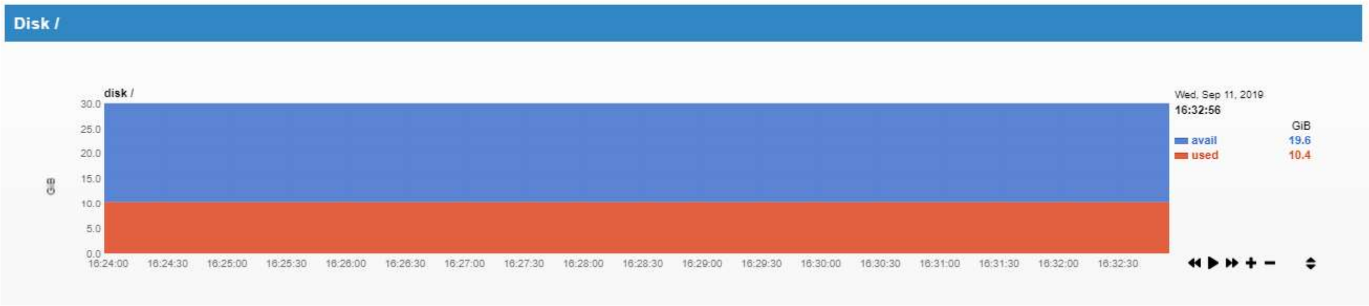
Note: Traffic sent is shown as an inverted graph (bottom).

Storage

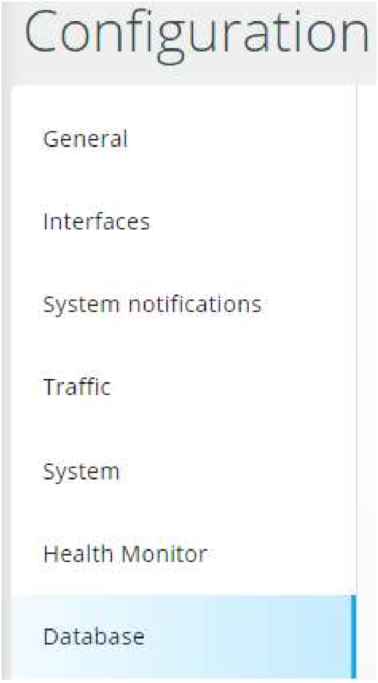
The Storage tab shows how much disk space is being used on the iSID Server.

For each partition on the disk, the system shows:

- Avail (color-coded in blue) - i.e. available storage
- Used (color-coded in red) - i.e. used storage



Database



Overview

In this module, you configure the databases used with iSID.

As part of the initial installation, the system is configured with 1 MySQL database and 1 MongoDB database. You can edit the configuration of each one.

You can choose to store data locally - or connect to a remote server. You can also specify if you want to clear any existing data (start ‘from scratch’) - or keep existing data ‘as is’.

Edit a database server

To edit the configuration of a database server:

1. Go to Configuration > Database.
2. Click the Edit ✎ icon (bottom, right corner) for the relevant database.
3. Choose what action you want to take with existing data (keep data ‘as is’ - or start a clean database ‘from scratch’)
4. Choose a database location - local or remote.
5. If remote, fill in the database server and user account details.
6. Click Apply to save.

Profiles

Profiles enable you to define how the Radiflow iSID reacts in non-regular occurrences, such as holidays or system maintenance.

Radiflow iSID comes with three default profiles, one for each system mode:

- Learning Profile
- Idle Profile
- Detection Profile

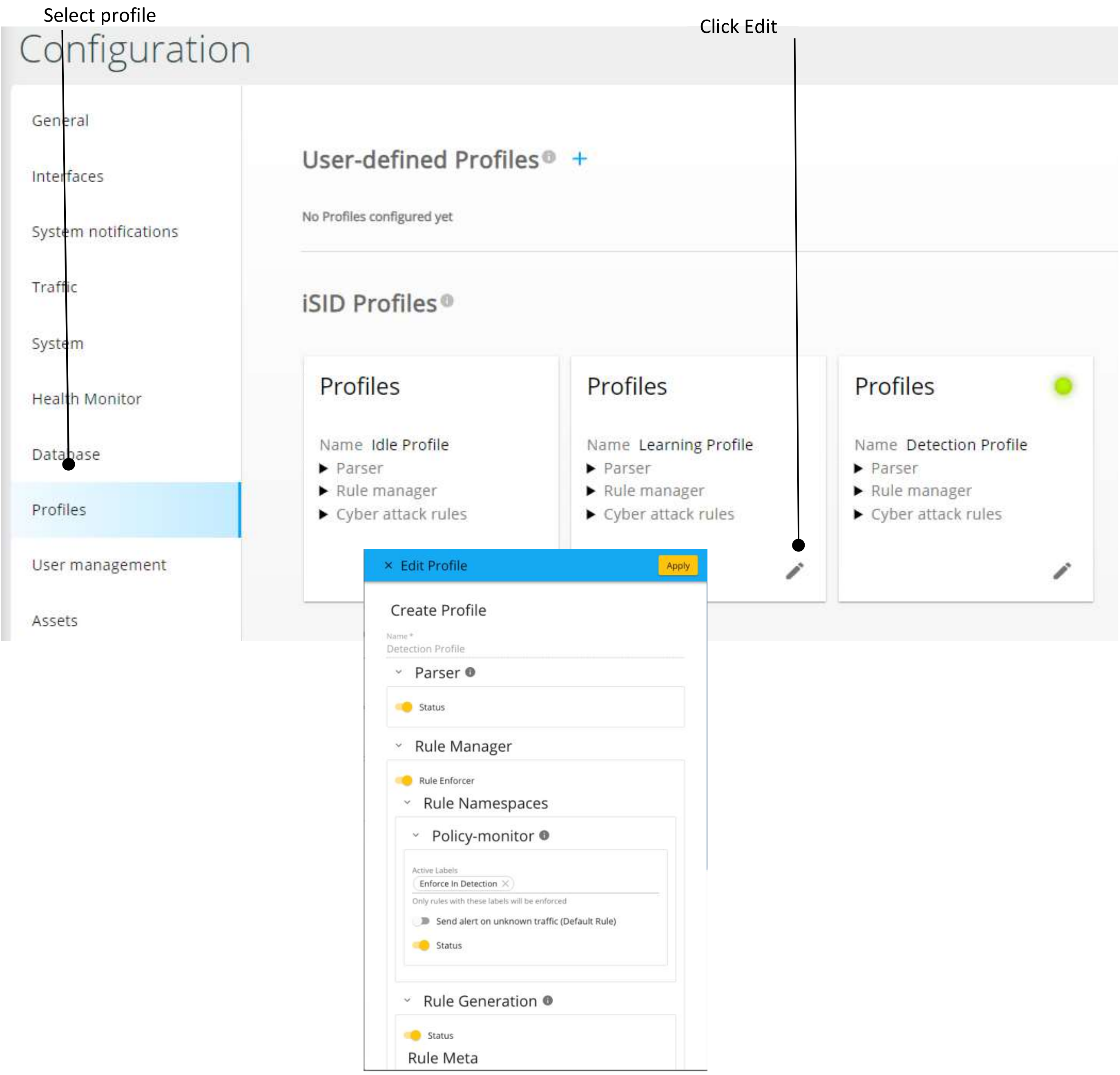
The default profiles can be edited but not deleted.

Note: the system will indicate which mode is currently active. The active mode can be changed from the Dashboard.

Edit a profile

IMPORTANT: Profiles should be edited by advanced users only.

1. Open Configuration > Profiles.
2. Select the checkbox of the profile you want to edit.
3. Click the Edit icon. The Edit Profile pop-up window opens.



User-defined Profiles +

No Profiles configured yet

iSID Profiles

Profiles	Profiles	Profiles
Name Idle Profile	Name Learning Profile	Name Detection Profile
▶ Parser	▶ Parser	▶ Parser
▶ Rule manager	▶ Rule manager	▶ Rule manager
▶ Cyber attack rules	▶ Cyber attack rules	▶ Cyber attack rules

Create Profile

Name *
Detection Profile

Parser
- Status

Rule Manager
- Rule Enforcer

Rule Namespaces

Policy-monitor

Active Labels
Enforce In Detection
Only rules with these labels will be enforced
- Send alert on unknown traffic (Default Rule)
- Status

Rule Generation
- Status

Rule Meta

4. In the Edit Profile pop-up window, edit the profile as follows:

Parser

- Toggle the Status slider to enable or disable the parsing of network traffic

Rule Manager

- Toggle the Rules Enforcer slider to enforce/not enforce rules

  Rule Namespaces

  Policy-monitor

  - Select the Active Labels that the profile applies to (see Labels).

    - Specify if an alert should be sent on unknown traffic (only applies to rules containing the selected active labels)
    - Toggle the Status slider to enable/disable policy monitor enforcement of user rules

Rule Generation

Rule Meta

- Toggle the Status slider to enable/disable Rule Generation
- Select the action to take (Log, Alert or Pass).
- Enter a message to appear in log
- Toggle the Rule Status slider to enable/disable rules
- Select a label or enter new label name

Cyber Attack rules

- Toggle the Events Reporter slider to enable/disable event reporting
- Toggle the Suggested slider to enable/disable suggested cyber attack rules
- Toggle the Pack Processing enable/disable packet processing

5. Click Apply. A message confirms the profiles were edited.

View a profile

1. Go to Profiles (Configuration > Profiles).
2. View the rule name, parser details, rule manager and cyber attack rule details.

User-defined profiles

Overview

In addition to the system profiles that are included by default, you can add your own, user-defined profiles.

Note: user-defined profiles are useful for operational scheduling.

Add a user-defined profile

1. Open Configuration > Profiles.
2. Click Add Profile + (top of page).
3. Provide a profile name.
4. Click Expand + to define which actions, alerts and settings to enable for each section under this profile. (See ‘Edit a profile’ for more detail.)
5. Click Apply to save.

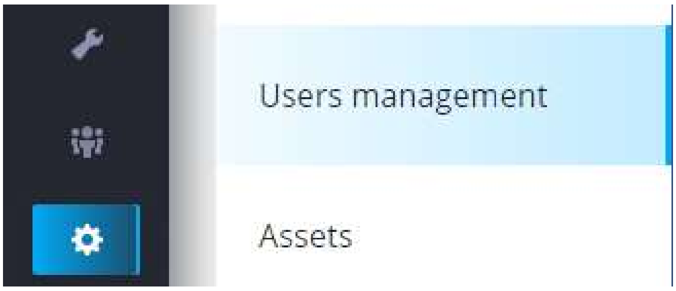
Remove a user-defined profile

1. Open Configuration > Profiles.
2. Locate the user-define profile that you wish to remove and click Delete 🗑.

Edit a user-defined profile

1. Open Configuration > Profiles.
2. Locate the user-define profile that you wish to edit and click Edit ✎.
3. Click Expand + to define which actions, alerts and settings are enabled for each section under this profile. (See ‘Edit a profile’ for more detail.)
4. Click Apply to save.

User management



Overview

You can use the User Management module to define if user authentication is local (authenticated by iSID) or remote (authenticated by Active Directory).

Note: iSID does not support a ‘mixed’ authentication mode - you must choose 1.

If you choose local authentication, you can create local user accounts and assign each one a role.

If you choose remote authentication, you can configure the Active Directory connection - and specify how Active Directory groups map to iSID roles.

Roles

Each user account must be assigned 1 of the following roles:

1. **Admin** - user has full control over the iSID system, including administrative functions (e.g. user management, iCEN configuration, storage configuration, etc.)
2. **Cyber expert** - user can perform all cyber-related tasks (e.g. take action on security alerts, take action on security insights, etc.)
3. **Cyber analyst** - user can access the same modules as Cyber expert - but with read-only permissions.

The configuration tab

The Configuration tab allows you to manage the following global settings for user management:

- Authentication mode
- Superuser password
- Define auto-logout times

Authentication mode

Before you can enable either remote or RSA SecurID authentication mode, you must configure the relevant remote server (see Remote authentication).

- local - all logins are authenticated by iSID
- remote - all logins are authenticated by Active Directory.
  Requires an existing Active Directory server defined in iSID.
- RSA SecurID – all logins are authenticated using 2 factor authentication by RSA SecurID.
  Requires both an Active Directory server as well as an RSA SecurID server already defined in iSID.

Note: iSID does not support a 'mixed' authentication mode. If you enable remote authentication (Active Directory or RSA SecurID), all login attempts will be authenticated remotely. Any existing local accounts will be ignored (with the exception of the superuser account).

Superuser password

To update the password for the superuser account (the admin account that comes bundled with iSID):

1. Click on 'Edit Superuser Password'.
2. Enter the old superuser password, and the new password twice - and Update.

Define the auto-logout times

1. Under Auto logout, select the length of inactive time that should elapse before iSID automatically logs out a user.

Authentication mode

Before creating user accounts, decide if your organization will manage user accounts within iSID (local authentication) - or make use of existing accounts in Active Directory or RSA SecurID (remote authentication).

This setting is managed under the configuration tab.

Local authentication

If your organization has chosen local authentication (see above), select the Local Users tab (top, left) to manage your local user accounts.

Add a user

1. Select Configuration > User Management > Local Users.
2. Click on Add + (top, right).
3. Fill in the user details and Apply.

Edit a user

1. Select Configuration > User Management > Local Users.
2. Select a user, using the checkbox □ provided.
3. Click on Edit user in the action bar (top, right).
4. Make changes and Apply.

Reset user password

1. Select Configuration > User Management > Local Users.
2. Select a user, using the checkbox □ provided.
3. Click on Reset password 🔒 in the action bar (top, right).
4. Make changes and Apply.

Delete a user

1. Select a user, using the checkbox □ provided.
2. Click on Delete user 🗑 in the action bar (top, right).
3. Click OK to confirm.

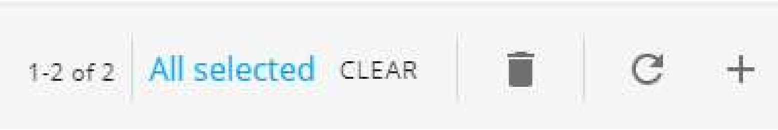
Delete multiple users

1. Select Configuration > User Management > Local Users.
2. Select the relevant users, using the checkboxes □ provided.

   Note:

   To select all (or clear all), use 1 of the following methods:

   1. Click SELECT ALL (or CLEAR) in the action bar (top, right):



Or

2. Check or uncheck the checkbox □ above the checkbox column:

Change the view

Sort by column

1. Select Configuration > User Management > Local Users.

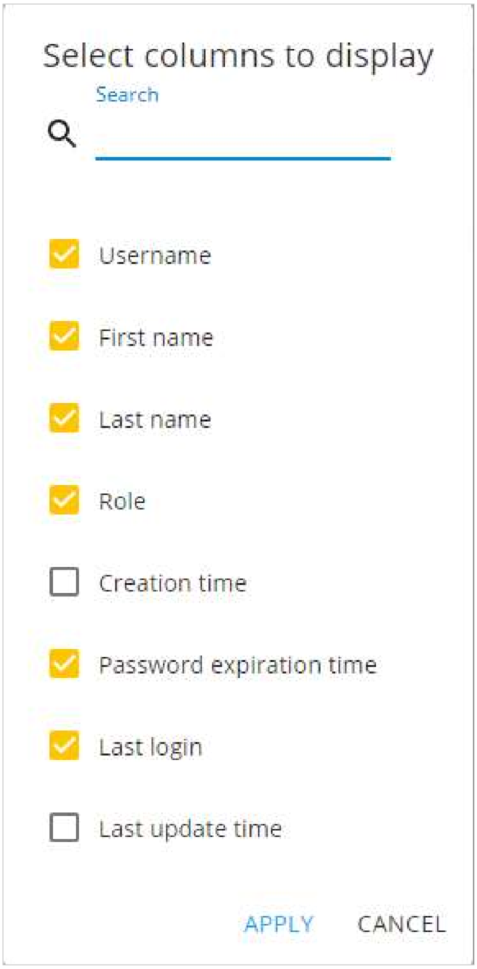
2. Click on the desired column header. An arrow ↓ indicates the sort direction. Click again to reverse the sort order.

3. To sort on multiple columns, click successively on several column headings. A number displays in each column heading, indicating if a given column is the primary sort ①, secondary sort ②, etc. In the example below, users are sorted by Last Name (desc) and then by first name (desc).

First Name ↓ 2
Last Name ↓ 1

Choose columns

To choose which columns display in the local users list, click on the More options ⋮ icon (top, right):



Select columns to display

Search

☑ Username

☑ First name

☑ Last name

☑ Role

□ Creation time

☑ Password expiration time

☑ Last login

□ Last update time

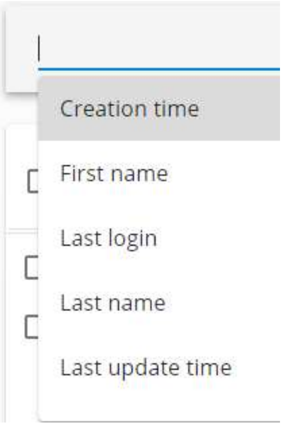
APPLY CANCEL

Apply a filter

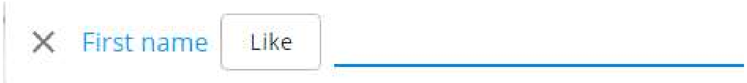
To filter the local users list:

1. Click on the Add filter button (top, left):

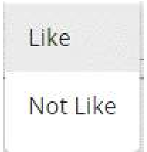
2. Choose a column:



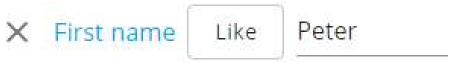
3. To filter for rows that do match, select Like:



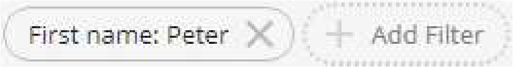
4. To filter for rows that do not match, select Not Like:



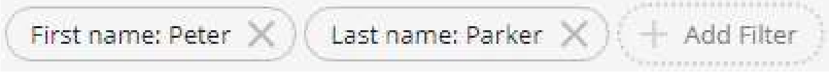
5. Type a value:



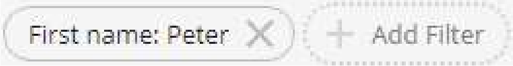
6. Click on Search 🔍 (far right) or tap the Enter key. The applied filter displays at the top of the page - and the rows are filtered accordingly:



7. You can easily combine multiple filters:



8. To remove a filter, click the Remove ✕ icon:



Remote authentication

Overview

If your organization prefers a single, centralized repository of credentials (rather than separate credentials for each application), you can configure iSID to use remote authentication - and hand off authentication to Active Directory or RSA SecurID.

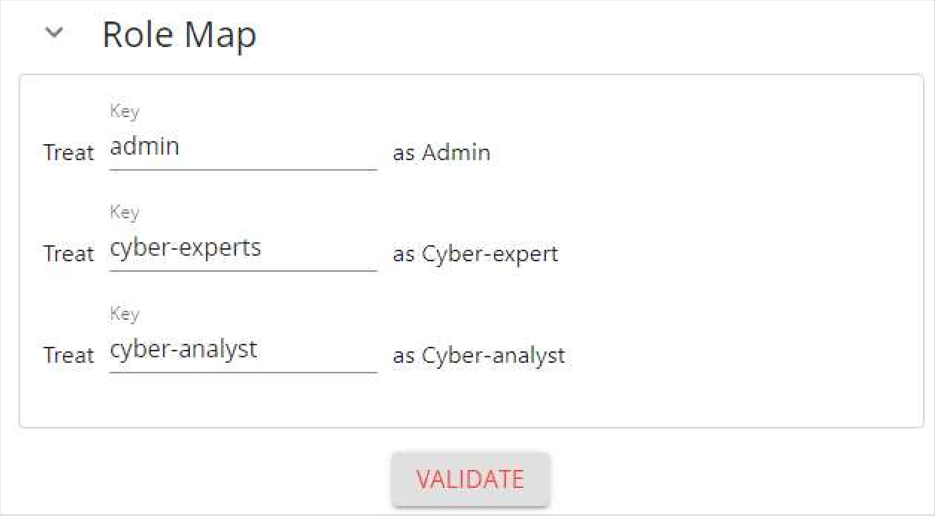
Note: iSID does not support a ‘mixed’ authentication mode. If you enable remote authentication, all login attempts will be authenticated remotely. Any existing, local accounts will be ignored (with the exception of the superuser account).

To configure remote authentication:

1. Select Configuration > User Management.
2. Select the Remote Users tab and add an Active Directory and/or RSA SecurID server (see next section - Add a remote server).
    - Remote authentication mode requires only an Active Directory server.
    - RSA SecurID authentication mode requires both an Active Directory server and an RSA SecurID server.
3. Select the Configuration tab and enable remote or RSA SecurID authentication.

Add an Active Directory server

1. In the Local Users tab (Configuration > User Management > Local Users) click on Active Directory Add +.
2. Fill in the user account for accessing the Active Directory server, as well as the Active Directory server details.
3. Under Role Map, enter the Active Directory group in the Key field, next to the corresponding iSID role.
4. As an example, you could perform the following steps for the Cyber expert role:
    a. In Active Directory, create a group called cyber-experts and assign the relevant accounts to the new group.
    b. In iSID, fill in the newly created group name in the Key field, next to the Cyber expert role:



Treat Key: admin as Admin

Treat Key: cyber-experts as Cyber-expert

Treat Key: cyber-analyst as Cyber-analyst

c. Click Validate to confirm that the Active Directory group name does exist.

5. Once you have mapped your Active Directory groups to iSID roles, you are ready to test! Active Directory user accounts in those groups should now be able to log into iSID - with the relevant iSID role.

Note: if an Active Directory user account belongs to multiple groups - and these groups map to multiple iSID roles - iSID will apply the user role with the highest permissions.

Add an RSA SecurID server

1. In the Remote Users tab (Configuration > User Management > Local Users) click on RSA SecurID Add + .

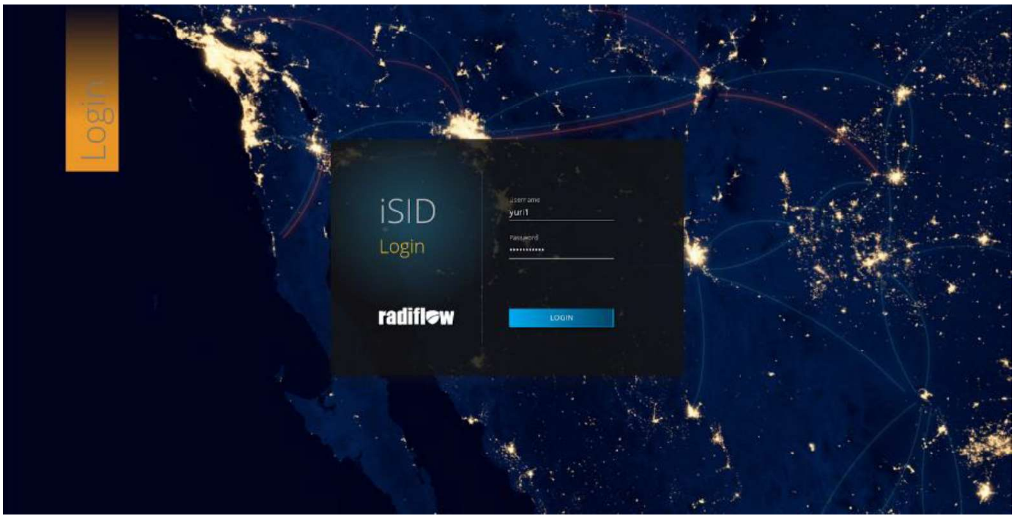
2. Fill in the following details for the RSA SecurID server:

- Domain
- Port
- Client key

3. Click Validate.

Authentication via RSA SecurID

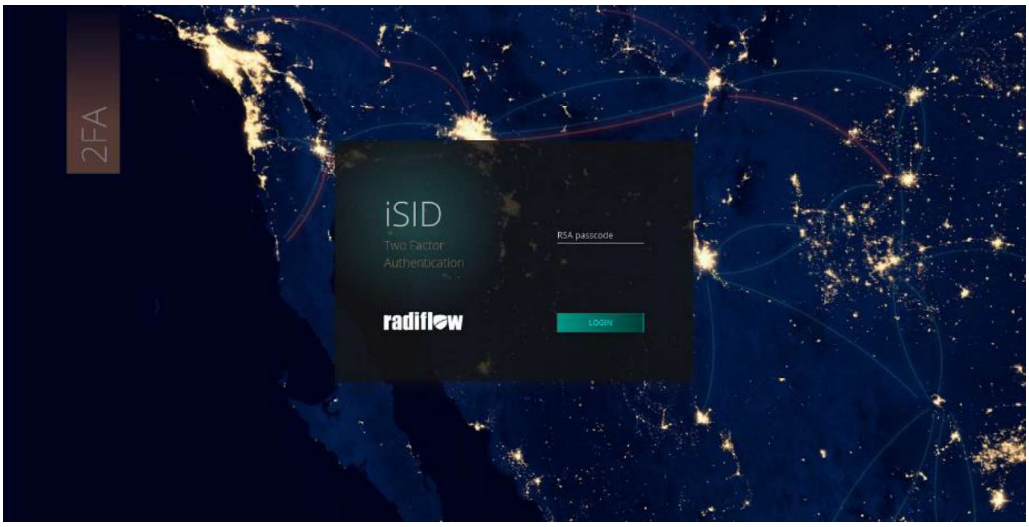
1. Configure the RSA SecurID server.
2. In the Configuration tab, select RSA SecurID as the authentication method
3. When you login, enter your username and password as usual.



Username: yuri1

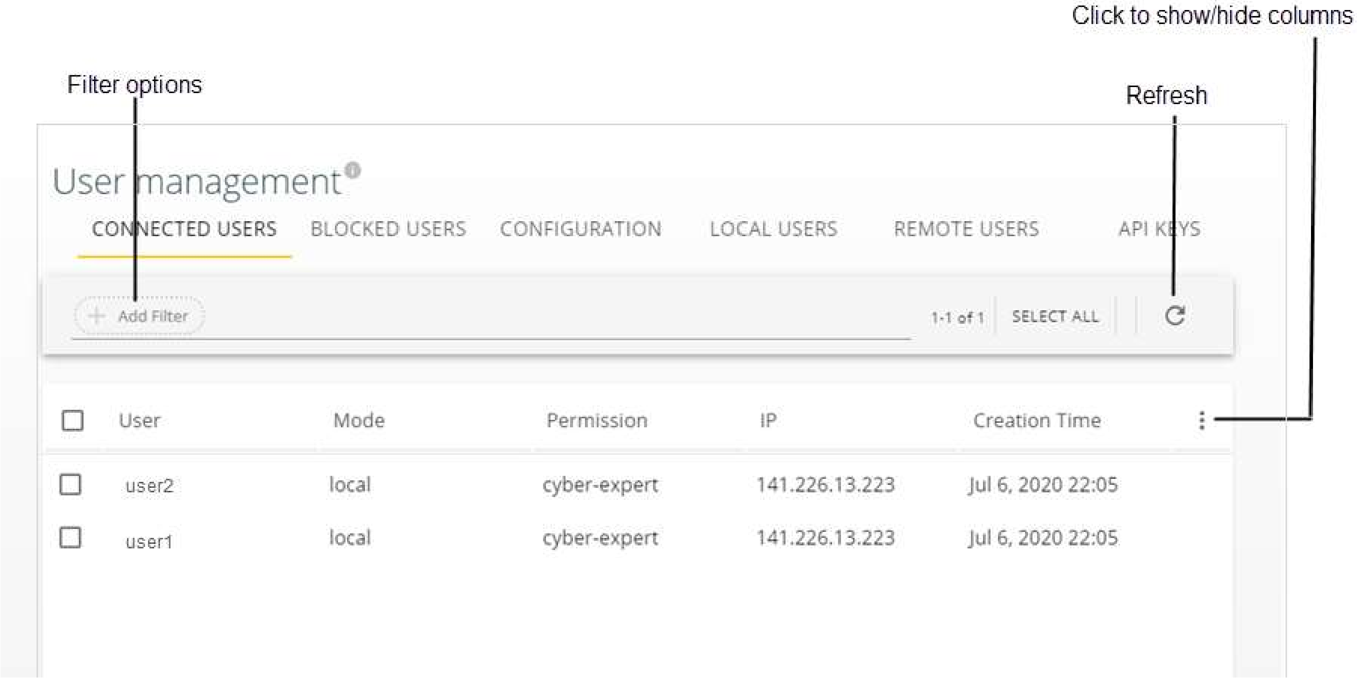
Password: ••••••••••••

4. In the next screen, enter the code generated by the SecurID application.



Connected users

The Connected users tab displays a listing of all users currently connect to iSID.


Click to show/hide columns

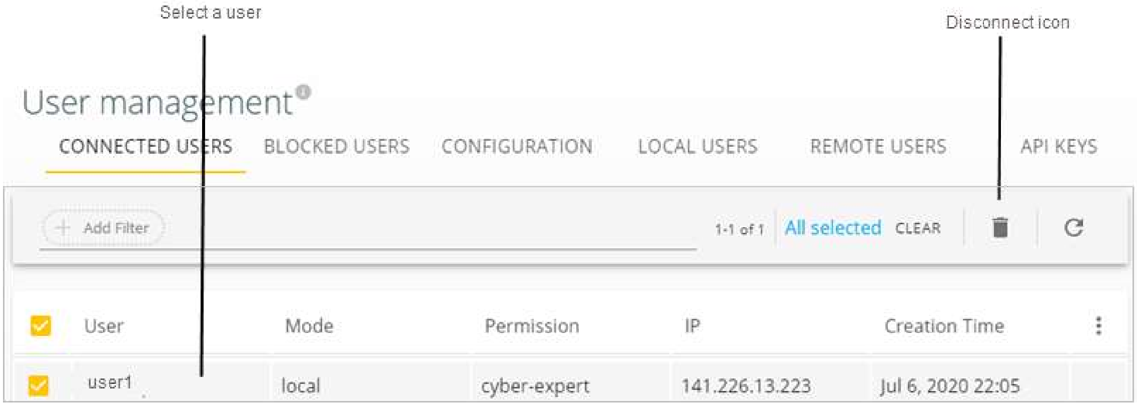
Filter options

Refresh

□	User	Mode	Permission	IP	Creation Time
□	user2	local	cyber-expert	141.226.13.223	Jul 6, 2020 22:05
□	user1	local	cyber-expert	141.226.13.223	Jul 6, 2020 22:05

Disconnect a user

1. Go to Connected Users (Configuration > User management > Connected Users).
2. Select the checkbox of the user you want to disconnect. The disconnect button appears.


Select a user

Disconnect icon

☑	User	Mode	Permission	IP	Creation Time
☑	user1	local	cyber-expert	141.226.13.223	Jul 6, 2020 22:05

3. Click the disconnect button.
4. Confirm the disconnect request.

Change the view

As explained under Local authentication (above), you can change the view in the following ways:

- Sort by column
- Choose columns

- Apply a filter

Blocked users

Overview

After 5 unsuccessful login attempts, the system blocks the user from any further logins. To review a list of blocked users, select Configuration > User Management > Blocked Users.

Unblock a user

1. Select Configuration > User Management > Blocked Users (far right).
2. Select 1 or more accounts, using the checkboxes □ provided.
3. Click on the Release icon (top, right).

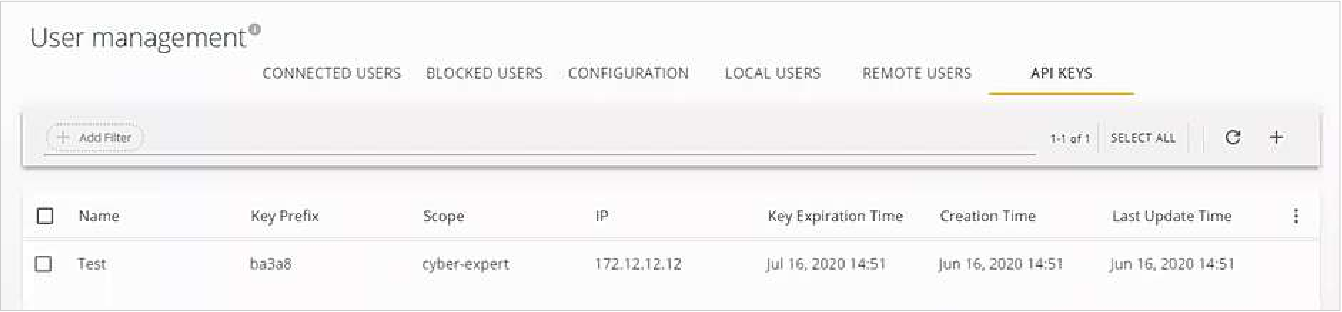
Change the view

As explained under Local authentication (above), you can change the view in the following ways:

- Sort by column
- Choose columns
- Apply a filter

API keys

API keys provide an authentication method for 3rd party users who are connecting to iSID via API rather than via the browser. iSID generates a key, which is then provided to the API user.

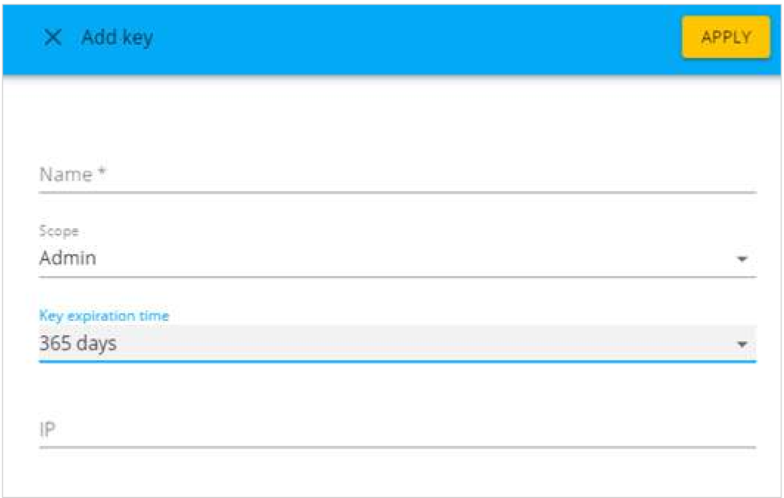


□	Name	Key Prefix	Scope	IP	Key Expiration Time	Creation Time	Last Update Time
□	Test	ba3a8	cyber-expert	172.12.12.12	Jul 16, 2020 14:51	Jun 16, 2020 14:51	Jun 16, 2020 14:51

Add an API key

1. Go to Configuration > User Management > API Keys.
2. Click on Add +.

3. The Add key pop-up window opens.



Name *

Scope: Admin

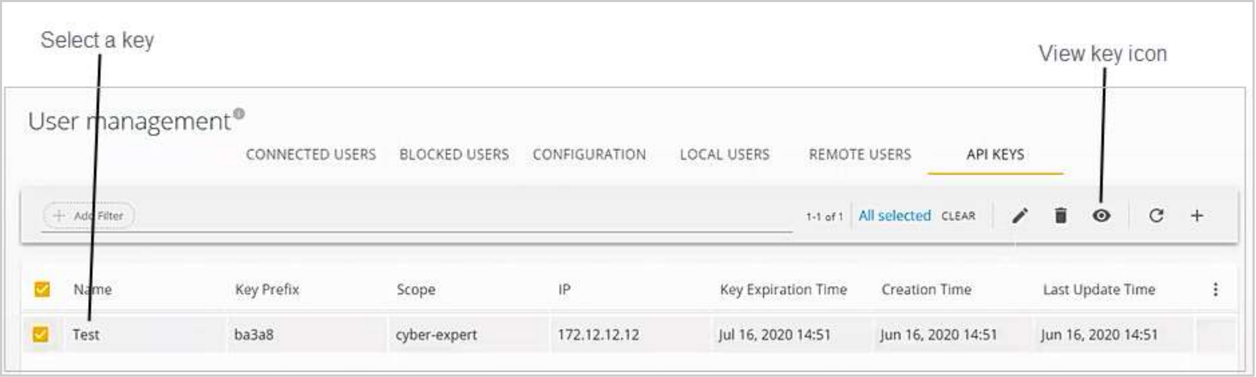
Key expiration time: 365 days

IP

4. In the Add key pop-up window, enter the details as follows:
   - Name - enter a name to identify the key and who should get it
   - Scope – select the role that this key provides access to (Admin, Cyber expert, or Cyber analyst)
   - Key expiration time – select the number of days for which the key is valid. After that the key will expire.
   - IP – enter the IP address for which the key is valid. Access from any other IP will not be allowed.
5. Click Apply. The new key information appears in the API keys listing.

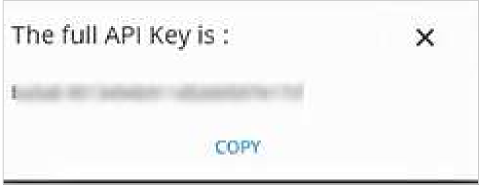
View a full API key

1. Go to Configuration > User Management > API Keys.
2. Select the checkbox of the key you want to display. The View key icon appears.



☑	Name	Key Prefix	Scope	IP	Key Expiration Time	Creation Time	Last Update Time
☑	Test	ba3a8	cyber-expert	172.12.12.12	Jul 16, 2020 14:51	Jun 16, 2020 14:51	Jun 16, 2020 14:51

3. Click the View key button.

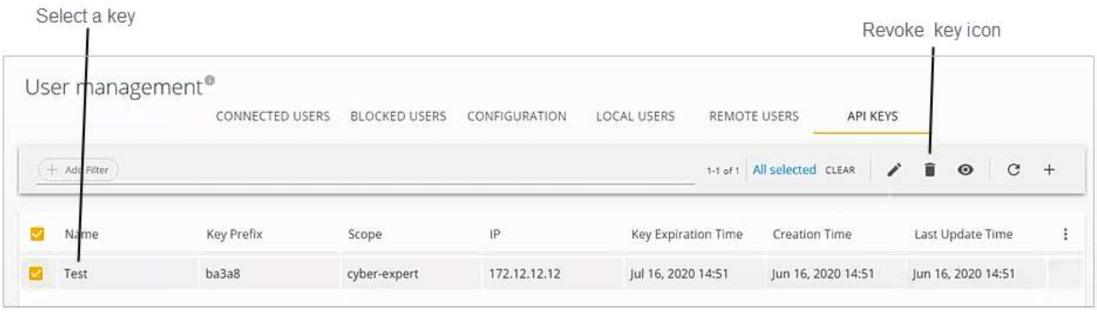


The full API Key is :

[redacted]

Revoke an API key

1. Go to Configuration > User Management > API Keys.
2. Select the checkbox of the key you want to revoke. The Revoke key icon appears.



Select a key

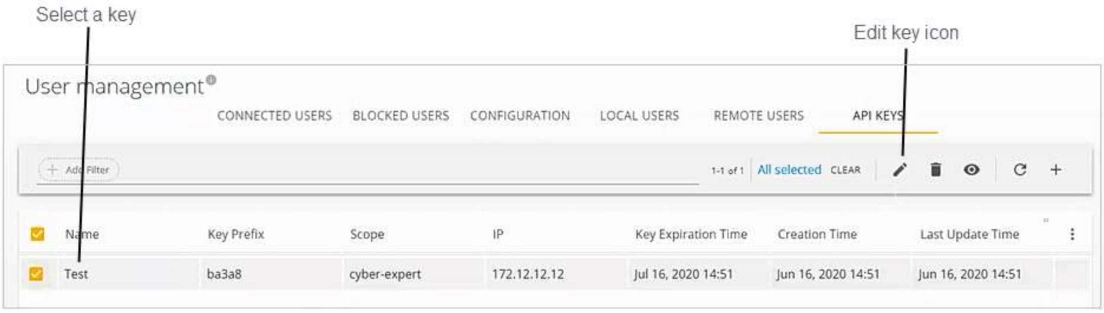
Revoke key icon

☑ Name	Key Prefix	Scope	IP	Key Expiration Time	Creation Time	Last Update Time
☑ Test	ba3a8	cyber-expert	172.12.12.12	Jul 16, 2020 14:51	Jun 16, 2020 14:51	Jun 16, 2020 14:51

3. Click the Revoke key button and confirm.

Edit API key parameters

1. Go to Configuration > User Management > API Keys.
2. Select the checkbox of the key you want to edit. The Edit key icon appears.



Select a key

Edit key icon

☑ Name	Key Prefix	Scope	IP	Key Expiration Time	Creation Time	Last Update Time
☑ Test	ba3a8	cyber-expert	172.12.12.12	Jul 16, 2020 14:51	Jun 16, 2020 14:51	Jun 16, 2020 14:51

3. Click the Edit key button and edit the key parameters (see Add an API key).

Change the view

As explained under Local authentication (above), you can change the view in the following ways:

- Sort by column
- Choose columns
- Apply a filter

Assets

Inactive time

Overview

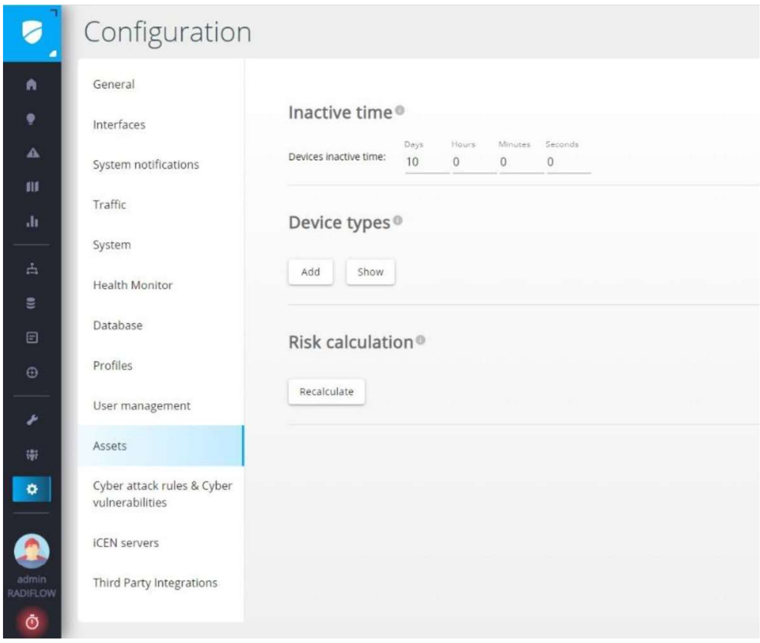
By default, Radiflow iSID detects silent entities (devices/links) that were once active and became silent – meaning they stopped transmitting any traffic. If an entity becomes active again, iSID re-detects the entity and sends a notification.

Configure inactive time

To configure the amount of time that must elapse before an entity is considered inactive:

Note: You can override these global inactive times and configure specific inactivity intervals for specific links (see Link Inactivity).

1. Go to Server actions (Configuration > Server actions).

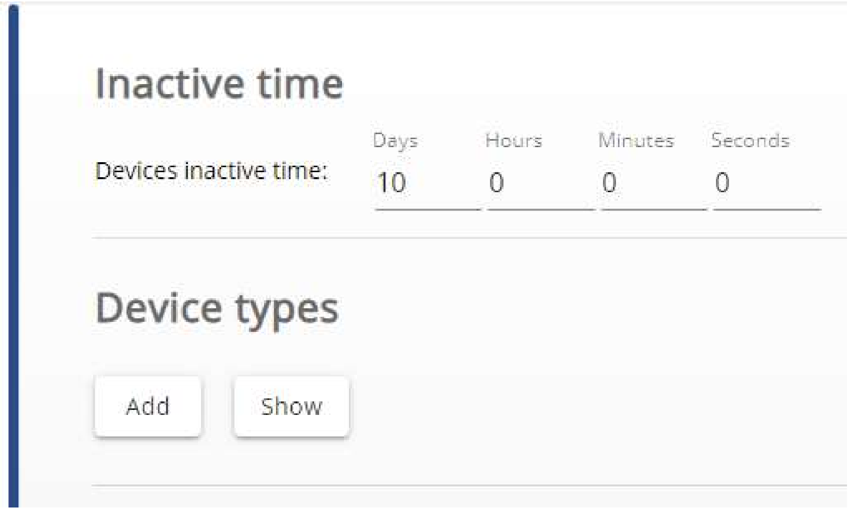


Devices inactive time: Days 10 Hours 0 Minutes 0 Seconds 0

2. In the Inactive time section, specify the amount of silent time (in days, hours, minutes, and seconds) should elapse until an entity is inactive.

Device types

When iSID discovers a device on the network, it is not always able to categorize that device at a fine-grained level. At some point, you may wish to assign your own, user-defined type to a given network asset. The list of available, user-defined types is managed here.



Inactive time

Devices inactive time: Days 10, Hours 0, Minutes 0, Seconds 0

Device types

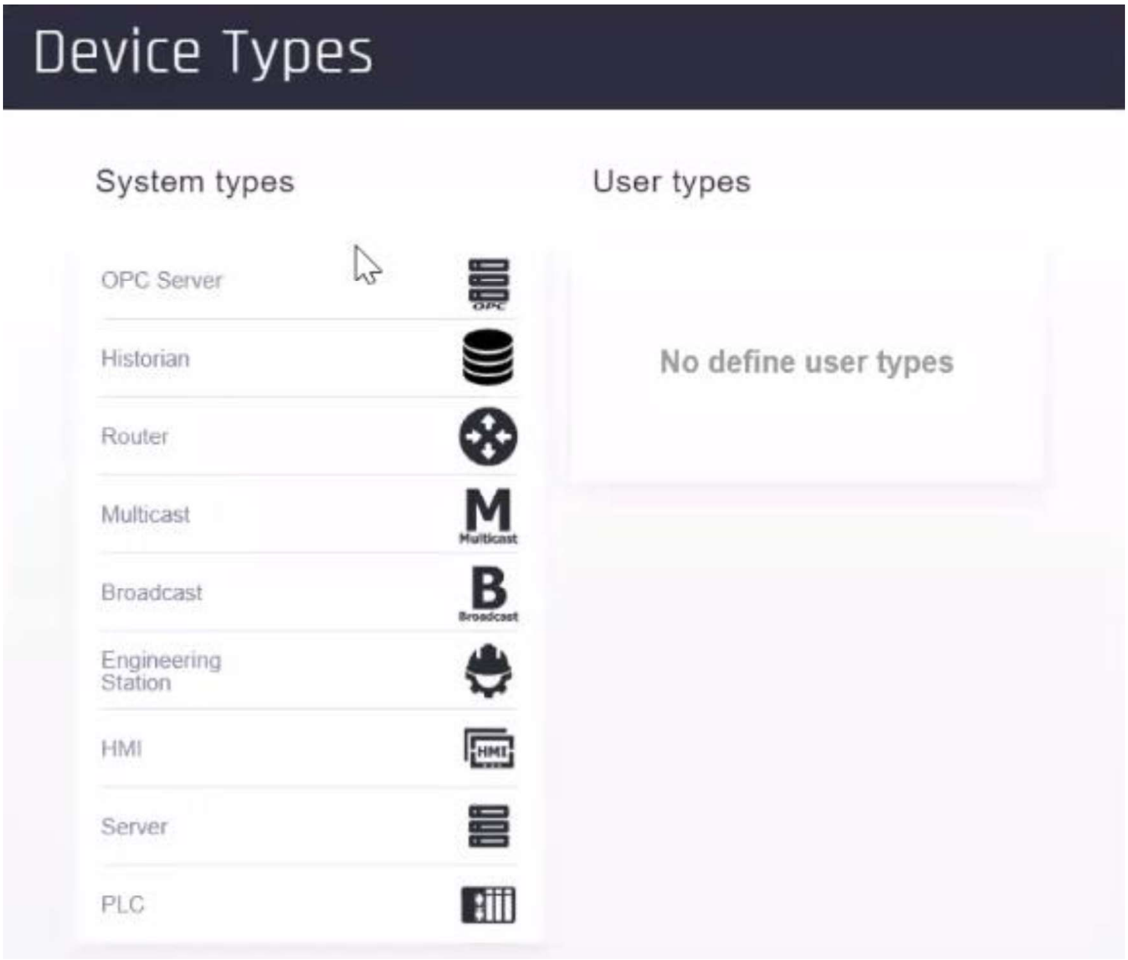
Note: User-defined types are available across the solution, just like system-defined types. For example, when filtering the Map View on device type, you can filter on a user-defined type.

Device type list

To see a list of all device types:

4. Select Configuration > Assets
5. Click Show (top, right)

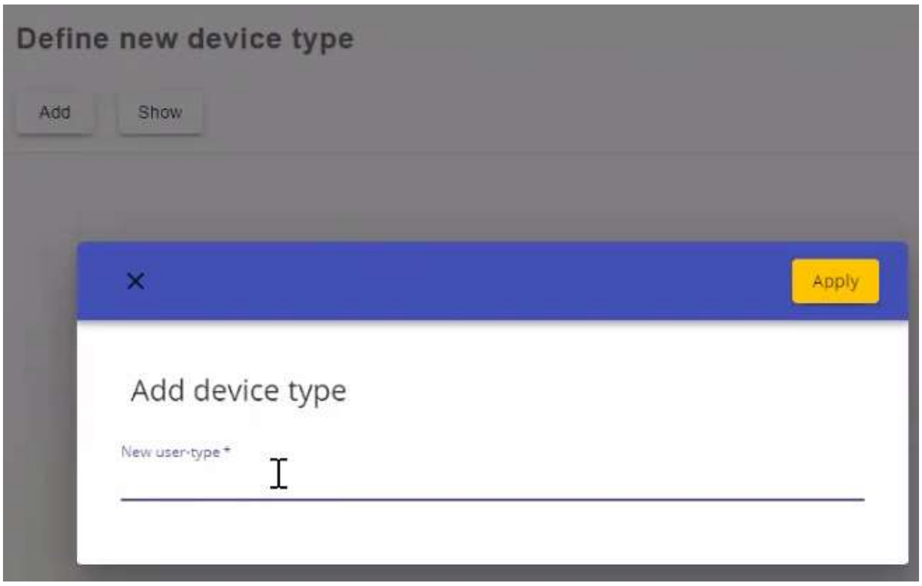
If any user-defined types exist, they will display in the User Types section on the right:



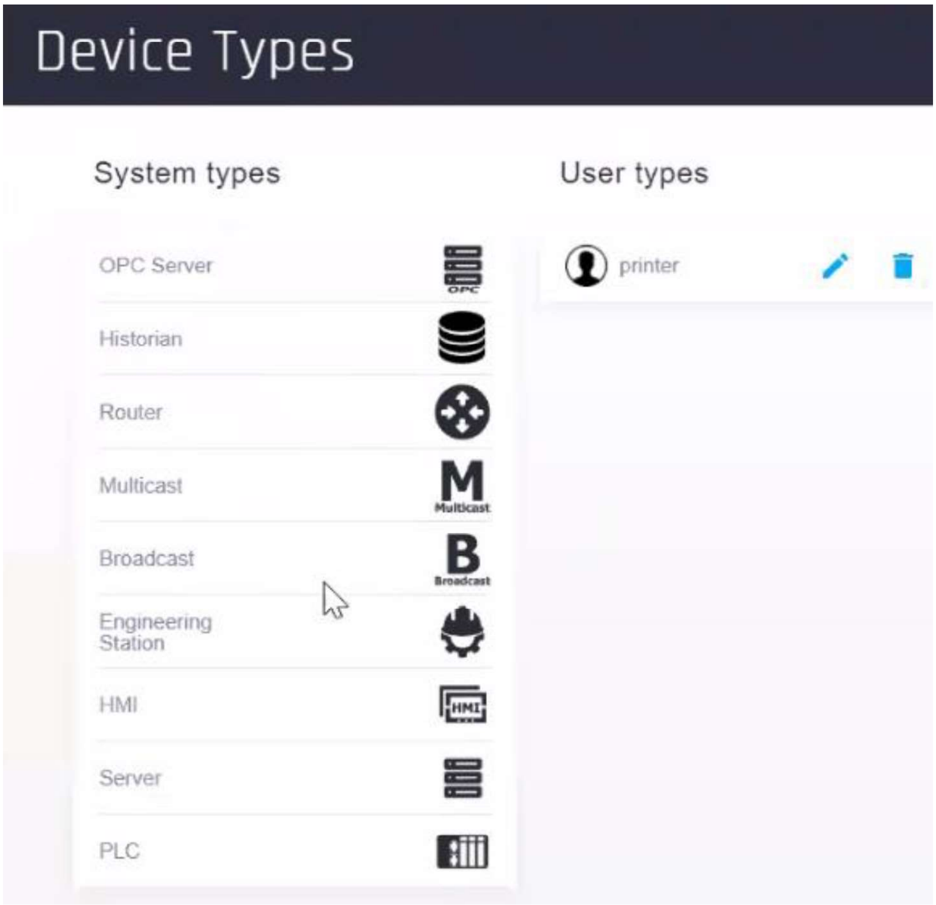
Add a user type

To add a new, user-defined type:

1. Select Configuration > Assets
2. Click Add (top, middle)
3. Type in a name and click Apply:



4. Return to the initial Assets screen and click Show (top, right). The device type is now listed in the User Types section on the right:



Note: User-defined types are available across the solution, just like system-defined types. For example, when filtering the Map View on device type, you can filter on a user-defined type.

Edit a user type

To edit the name of a user type, click on the Edit icon.

Note: All user-defined device types share the same device icon:

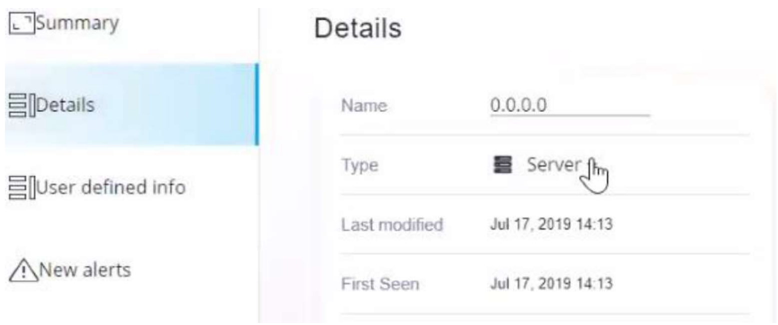
Delete a user type

To delete a user type, click on the Delete icon.

Assign the new type to a device

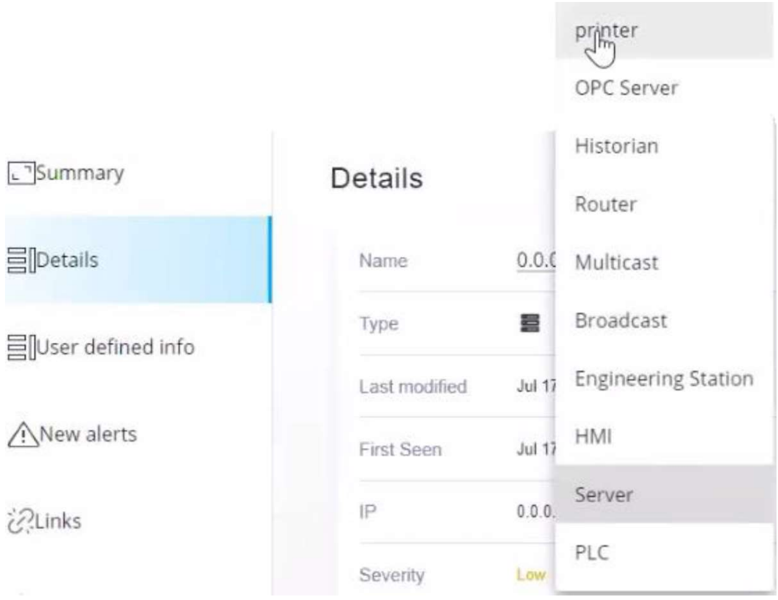
To update an existing device with your new user type:

1. Locate the desired device. (Use the Map module or Asset Management module - see vertical toolbar on left).
2. Bring up the device details pop-up, and select the Details tab.
3. Click on the existing type to select a new type:



Details

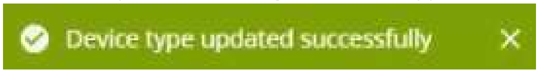
Name	0.0.0.0
Type	Server
Last modified	Jul 17, 2019 14:13
First Seen	Jul 17, 2019 14:13



Details

Name	0.0.(
Type	
Last modified	Jul 17
First Seen	Jul 17
IP	0.0.0.
Severity	Low

4. Upon selecting the new type, an onscreen message (bottom, right) confirms the change:



Device type updated successfully

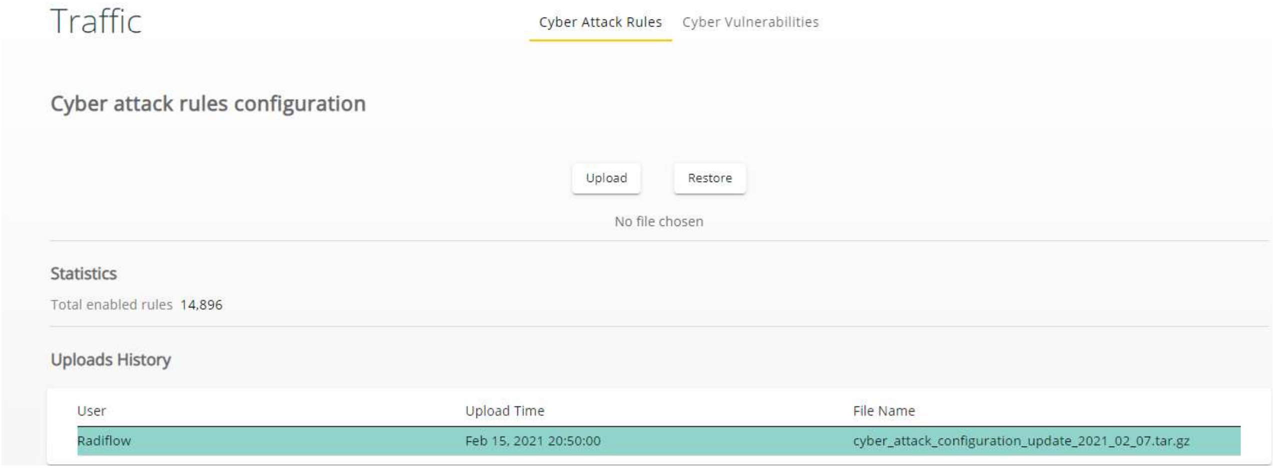
Cyber attack rules & Cyber vulnerabilities

Use Cyber attack rules & Cyber vulnerabilities to do the following:

- View stats for enabled/disabled rules
- Update Rules configuration
- Update CVE configuration

View stats

1. Open Configuration > Cyber attack rules & Cyber vulnerabilities.
2. View the Statistics section (middle):



Cyber attack rules configuration

No file chosen

Statistics

Total enabled rules 14,896

Uploads History

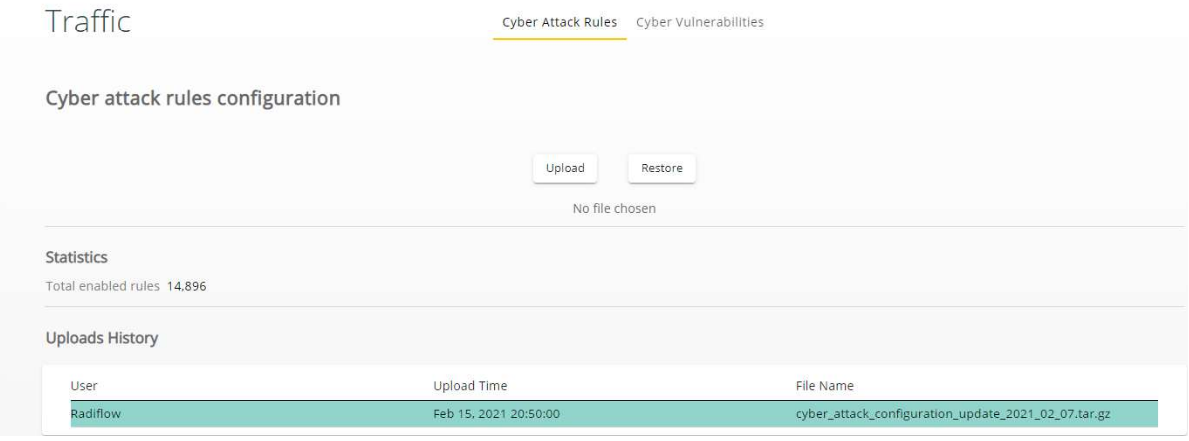
User	Upload Time	File Name
Radiflow	Feb 15, 2021 20:50:00	cyber_attack_configuration_update_2021_02_07.tar.gz

Upload cyber-attacker rules

From time to time, Radiflow provides a file with an updated set of cyber-attack rules. Once uploaded, iSID updates with the latest set of cyber-attack rules.

Note: Any rule that was previously edited is preserved ‘as is’. In all other cases, the new set of rules overrides the old set.

1. Open Configuration > Cyber attack rules & Cyber vulnerabilities.



Cyber attack rules configuration

No file chosen

Statistics

Total enabled rules 14,896

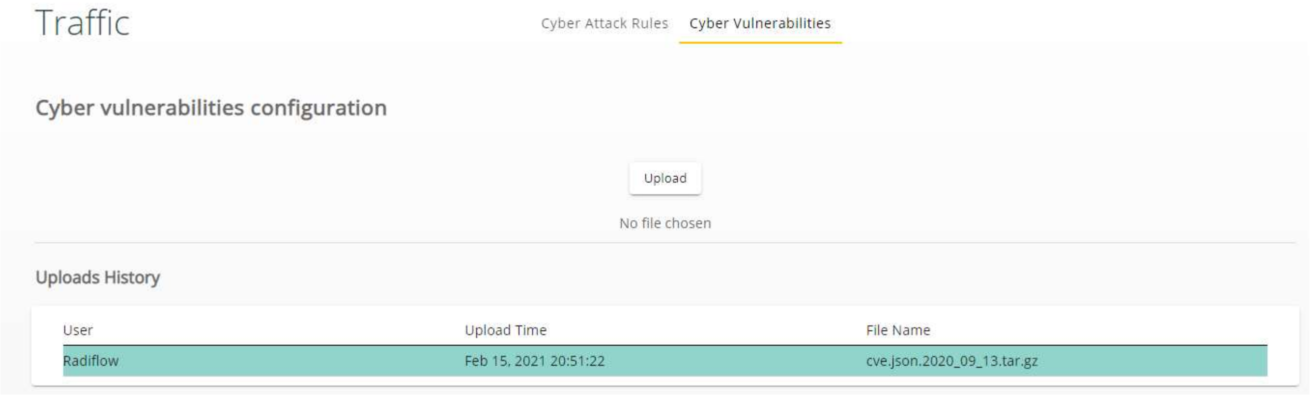
Uploads History

User	Upload Time	File Name
Radiflow	Feb 15, 2021 20:50:00	cyber_attack_configuration_update_2021_02_07.tar.gz

2. Under Rules configuration (middle), click Upload.
3. The Upload pop-up displays:
1. Browse for the rules file.
2. Click Add signature and browse for the corresponding signature file.
3. Click Apply (top, right) to initiate the update process.

Upload CVEs

From time to time, Radiflow provides a file with an updated set of CVEs. Once uploaded, iSID updates with the latest set of CVEs.



Cyber vulnerabilities configuration

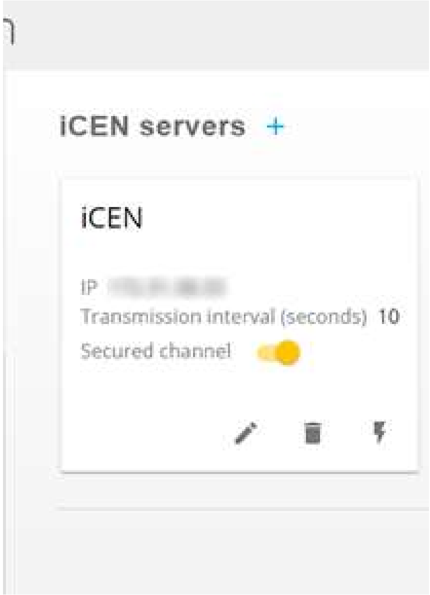
No file chosen

Uploads History

User	Upload Time	File Name
Radiflow	Feb 15, 2021 20:51:22	cve.json.2020_09_13.tar.gz

1. Open Configuration > Cyber attack rules & Cyber vulnerabilities.
2. Under CVE configuration (bottom), click Update.
3. The Update pop-up displays:
1. Click Choose file and browse for the CVE file.
2. Click Add signature and browse for the corresponding signature file.
3. Click Apply (top, right) to initiate the update process.

iCEN Servers



iCEN servers +

iCEN

IP [redacted]

Transmission interval (seconds) 10

Secured channel

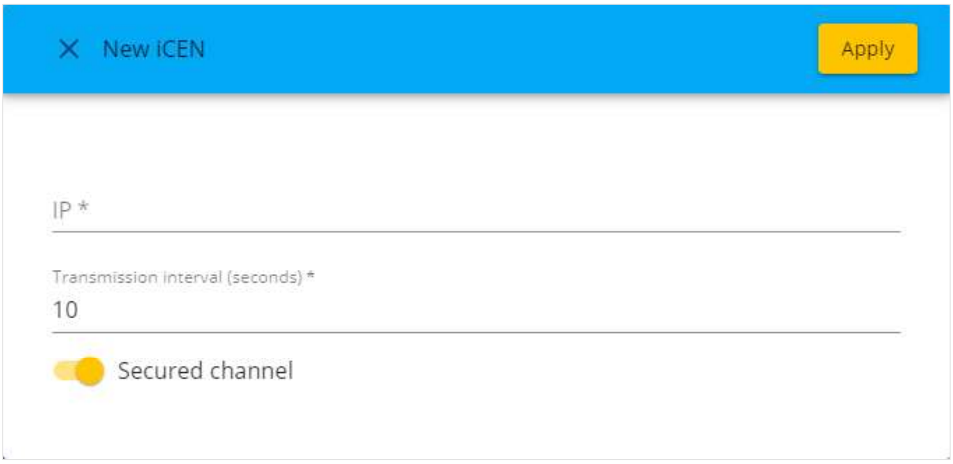
Overview

If your organization is running iCEN Server, you will need to point each instance of iSID to 1 or more iCEN Servers. There are 3 bits of information to fill in:

- IP
- Transmission interval (how often iSID should send updated stats to iCEN)
- Secured channel
- Note: If you also send information from iCEN to iSID, you can enable TLS via this toggle switch.

Actions

- To edit an existing iCEN Server configuration, click on the Edit ✎ icon.
- To delete an existing iCEN Server configuration, click on the Delete 🗑 icon. (Note: this does not delete the actual iCEN implementation - it just removes the reference from iSID.)
- To test the connection with the iCEN Server, click on the Check connection ⚡ icon.
- To add a new iCEN configuration, click on the Add + icon (next to the section heading, at the top).



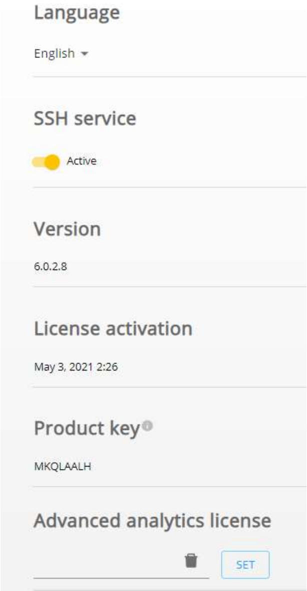
IP *

Transmission interval (seconds) *
10

Secured channel

Product key

Before iCEN can monitor your iSID instance, you will need to add an iSID instance configuration there - and enter your iCEN Product Key:
The Product Key can be found under Configuration > General:



Language
English

SSH service
Active

Version
6.0.2.8

License activation
May 3, 2021 2:26

Product key
MKQLAALH

Advanced analytics license

Note: The License field displays the start date for the ISID Server license.
For more information about iCEN, refer to the iCEN User Guide.

Third Party Integrations

Overview

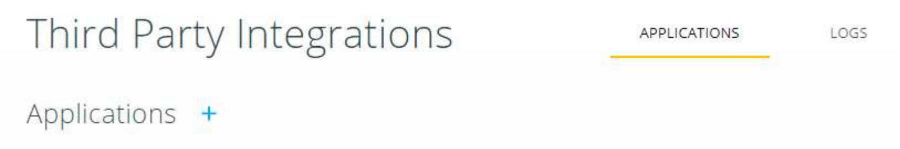
For a more holistic solution, iSID provides integration with certain third-party cyber solutions. For example, you can configure iSID to report newly discovered assets to the Palo Alto Firewall.

The following applications are supported:

1. Palo Alto Firewall
2. Fortinet Firewall
3. ServiceNow Workflows

Add an application

1. Open Configuration > Third Party Integrations:

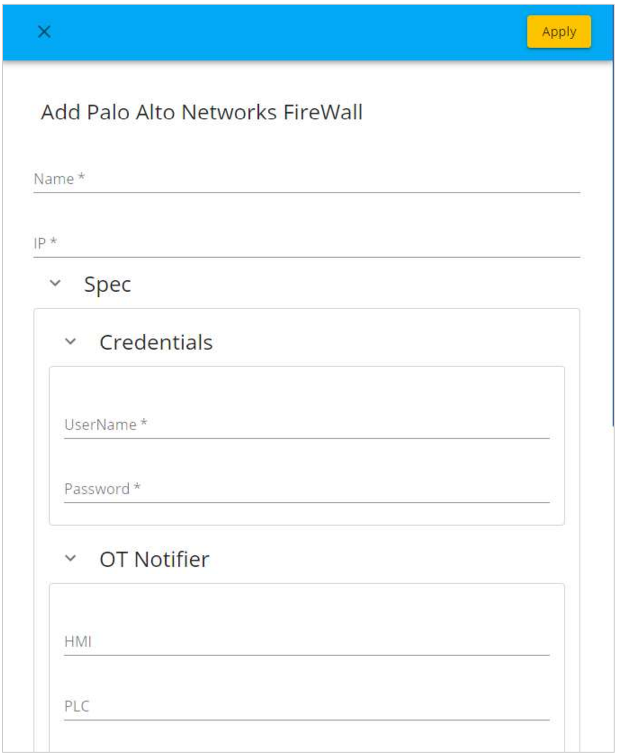


Third Party Integrations

2. Click Add + and select an application e.g. Palo Alto Firewall.

Palo Alto Networks Firewall

1. The Add Palo Alto Networks Firewall dialogue box displays:

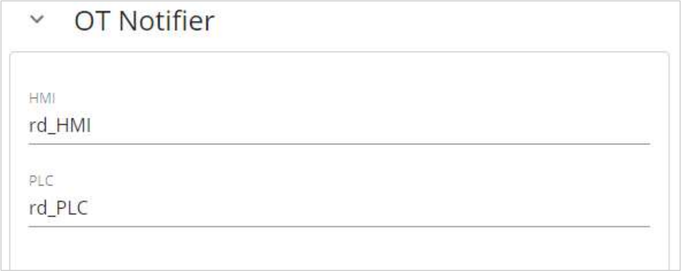


Add Palo Alto Networks FireWall

2. Fill in all the necessary configuration details:

- A Name for the integration profile.
- The IP of the Palo Alto server.
- Credentials for connecting to the Palo Alto server.

- A set of OT Notifier tags for reporting new assets to the Palo Alto server. For example (see screenshot below):
  - If a new HMI device was discovered, send the tag “rd_HMI” to the Palo Alto server.
  - If a new PLC device was discovered, send the tag “rd_PLC” to the Palo Alto server.
  - Etc.



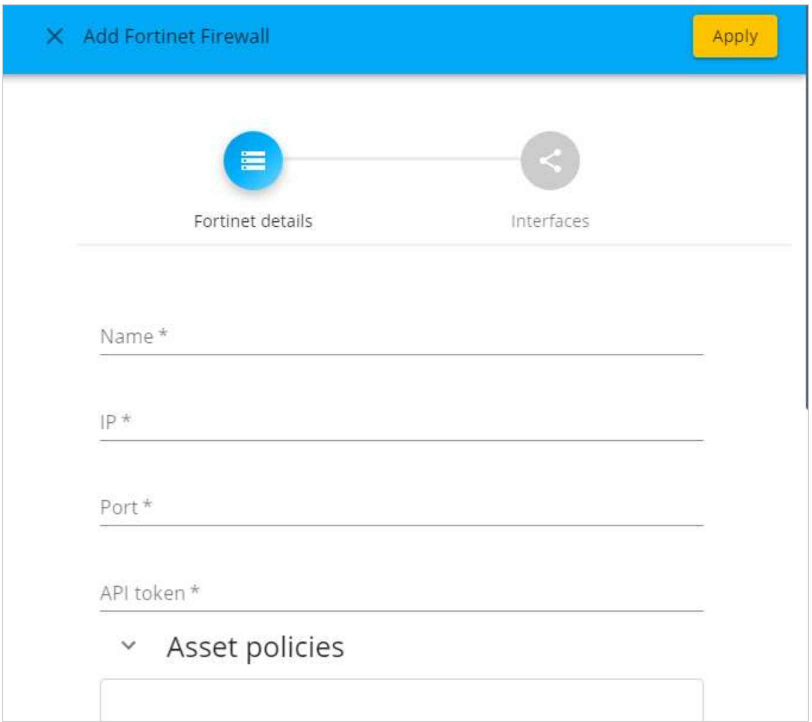
HMI
rd_HMI

PLC
rd_PLC

3. Once all configuration details have been filled, click on Apply (top, right).

Fortinet Firewall

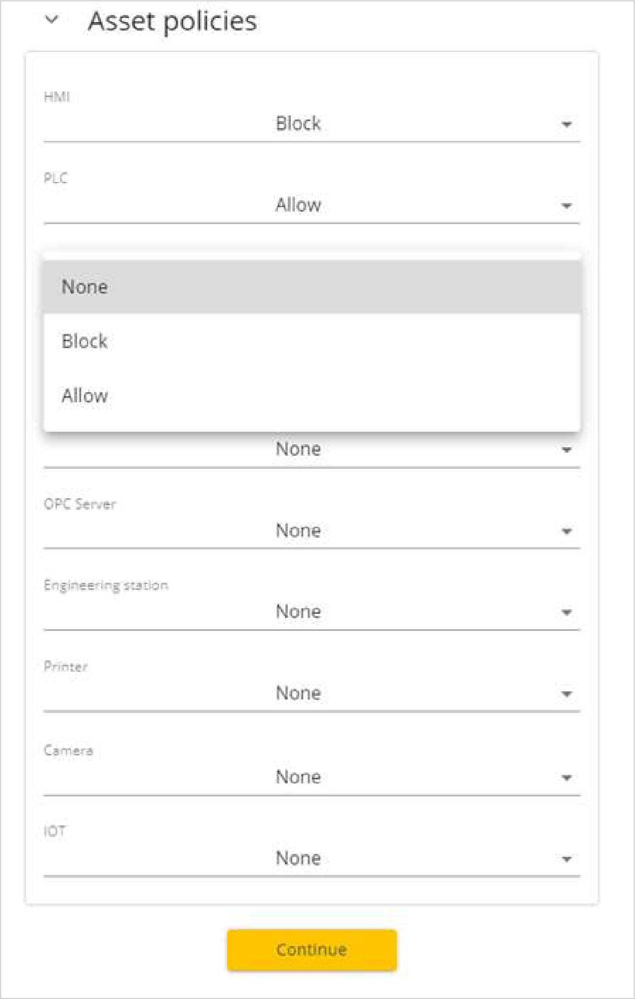
1. The Add Fortinet Firewall dialogue box opens:



2. Fill in all the necessary configuration details:

- A Name for the application profile.
- The IP of the Fortinet server.
- The port number of the Fortinet server.
- Connection credentials (API token)

- A set of policies for automatic response when detecting a new connected asset (see screenshot below):
  For example:
  - New HMI devices - block.
  - New PLC devices - allow.
  - Etc.



Asset policies

HMI
Block

PLC
Allow

None

OPC Server
None

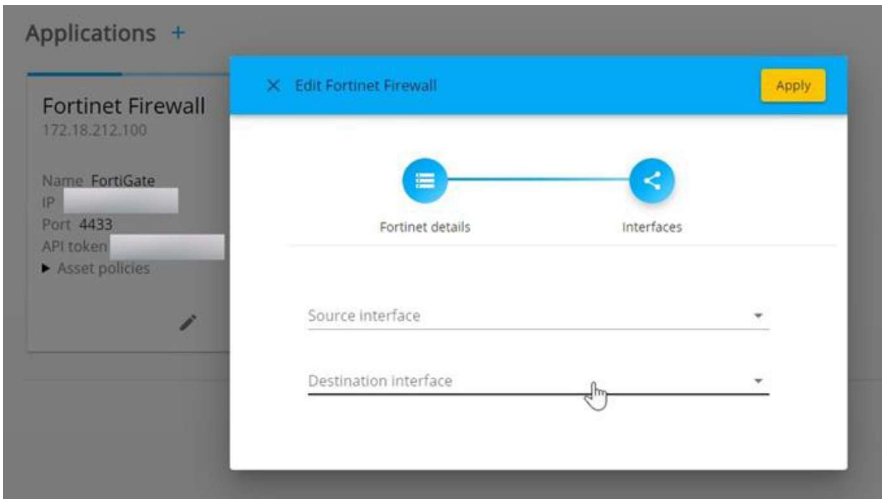
Engineering station
None

Printer
None

Camera
None

IOT
None

3. Click Continue.
4. Select the source and destination interfaces in the firewall.



Fortinet Firewall
172.18.212.100

Name FortiGate
IP [redacted]
Port 4433
API token [redacted]
▸ Asset policies

Source interface
Destination interface

5. Click Apply.

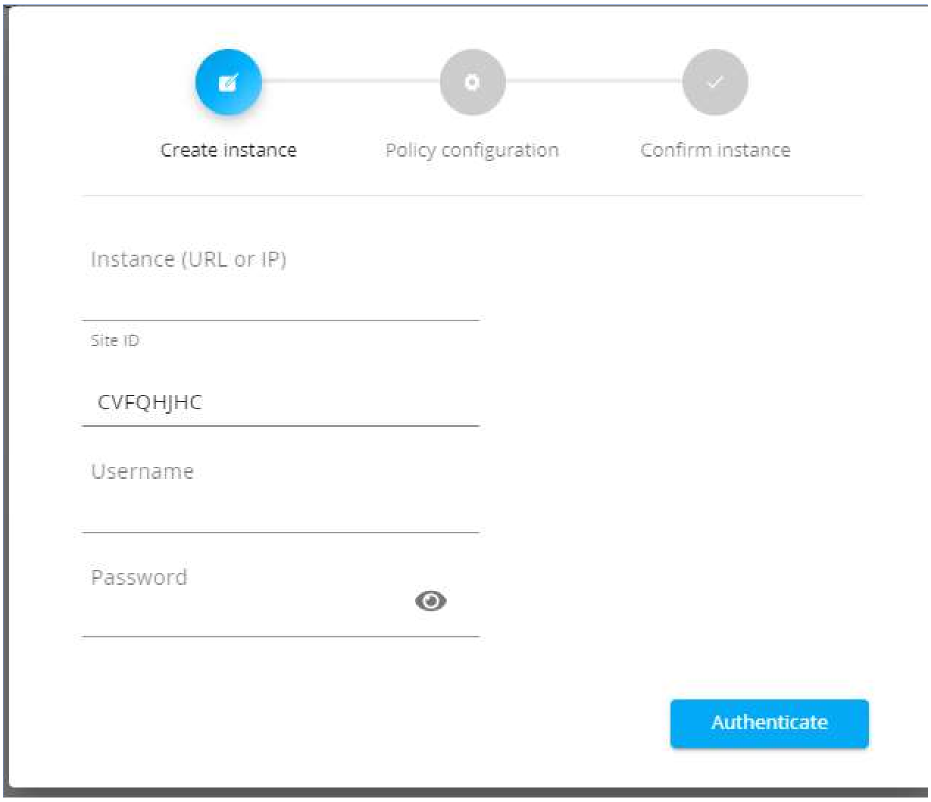
ServiceNow

When configuring iSID to connect to ServiceNow, make sure to receive relevant ServiceNow information:

- Instance link: https://f*************demo1.service-now.com/ - Where to send the traffic
- Site ID: MySite_AB_iSID1 -iSID name in ServiceNow
- Username: b*********r@servicenow.com
- Password: *********

Note: Site ID is unique per iSID and will be provided by Radiflow. It is used to identify where site the assets are located within ServiceNow.

1) The Add ServiceNow dialogue box opens:



2) Create an Instance:

a) Instance: Only part of the text of the provided link should be inserted.

For example:

- If the provided link is as following: https://f************demo1.service-now.com/
- Text for Side ID is: f*************demo1

b) Site ID: as provided
For example

- MySite_AB_iSID1

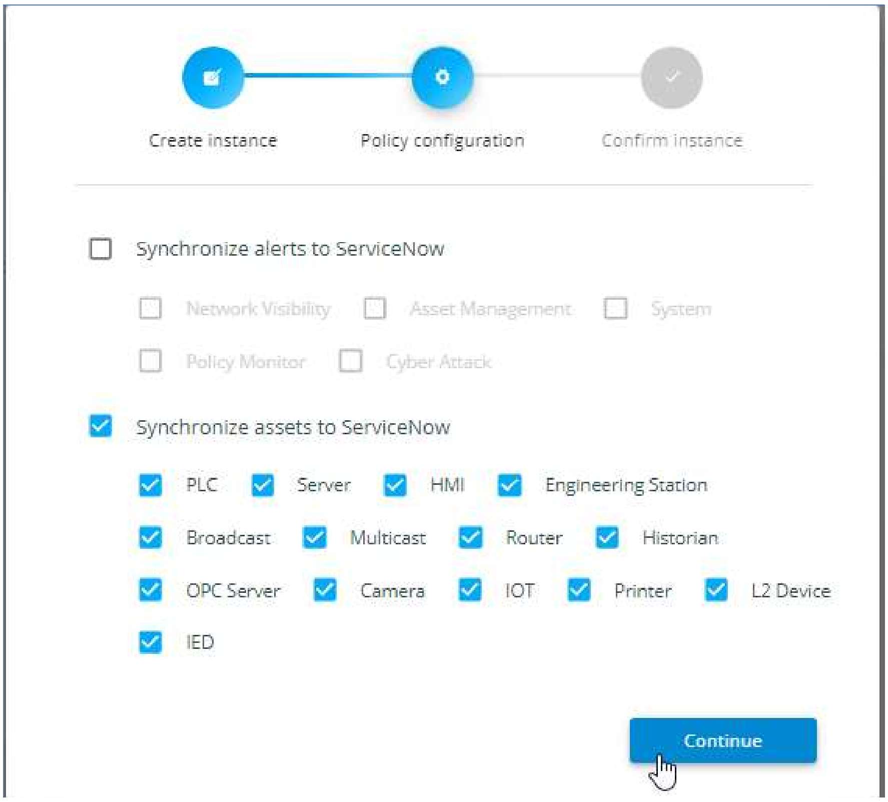
c) Username: as provided
For example:

- b************r@servicenow.com

d) Password: as provided

Once completed, press **Authenticate**

3) In **Policy configuration**, check the **Synchronize assets to ServiceNow** checkbox and all the assets’ checkboxes listed. Press **Continue**



□ Synchronize alerts to ServiceNow

□ Network Visibility □ Asset Management □ System

□ Policy Monitor □ Cyber Attack

☑ Synchronize assets to ServiceNow

☑ PLC ☑ Server ☑ HMI ☑ Engineering Station

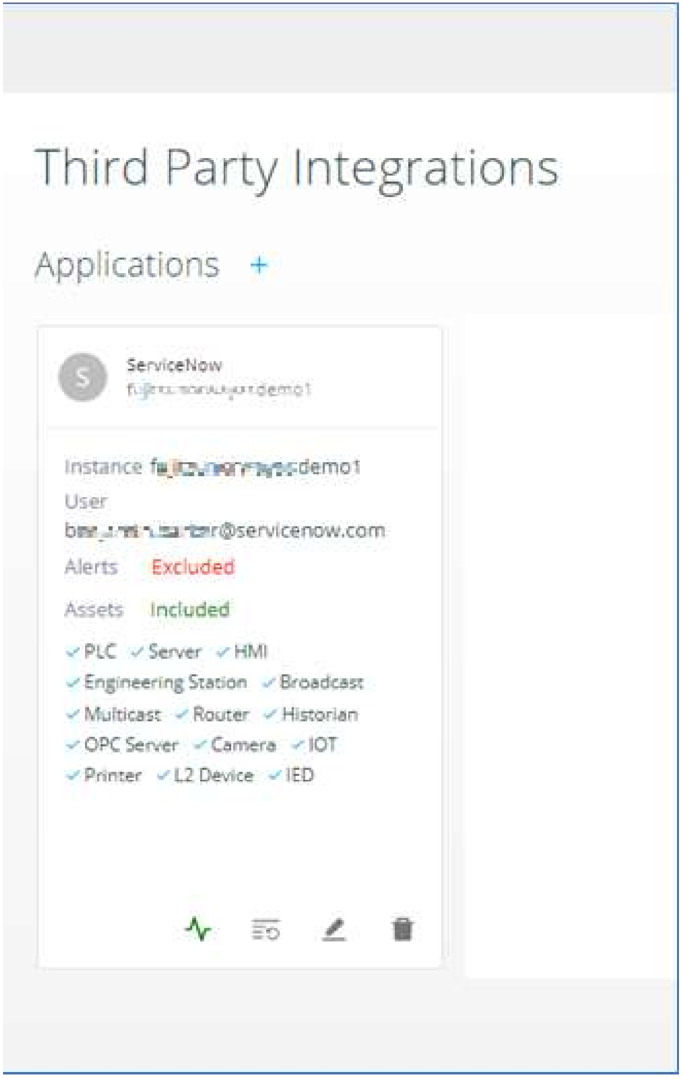
☑ Broadcast ☑ Multicast ☑ Router ☑ Historian

☑ OPC Server ☑ Camera ☑ IOT ☑ Printer ☑ L2 Device

☑ IED

4) Confirm the configuration

5) The integration configuration is presented



Third Party Integrations

Applications +

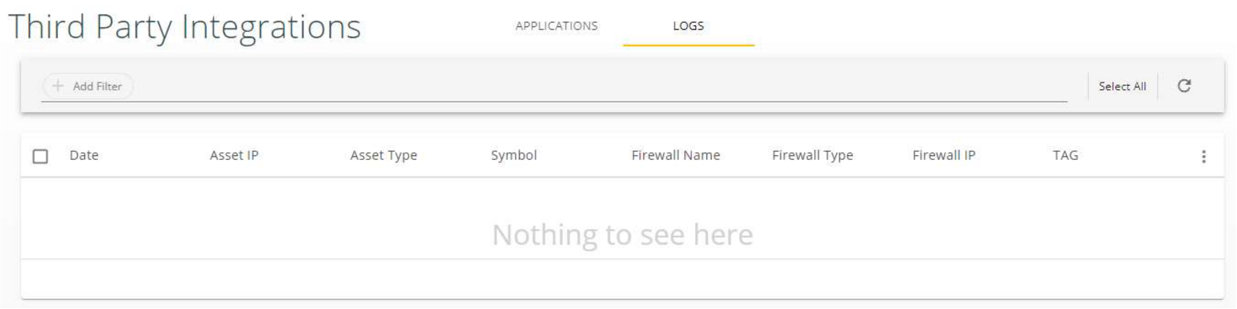
ServiceNow
f[redacted]demo1

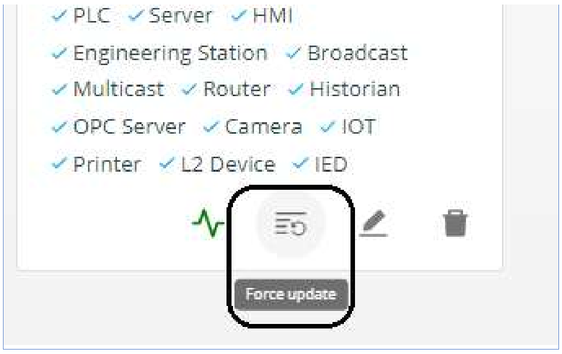
Instance f[redacted]demo1
User
b[redacted]r@servicenow.com
Alerts Excluded
Assets Included

✓ PLC ✓ Server ✓ HMI
✓ Engineering Station ✓ Broadcast
✓ Multicast ✓ Router ✓ Historian
✓ OPC Server ✓ Camera ✓ IOT
✓ Printer ✓ L2 Device ✓ IED

View application logs

1. Open Configuration > Third Party Integrations.
2. Click on the Application logs tab (top, right):




✓ PLC ✓ Server ✓ HMI
✓ Engineering Station ✓ Broadcast
✓ Multicast ✓ Router ✓ Historian
✓ OPC Server ✓ Camera ✓ IOT
✓ Printer ✓ L2 Device ✓ IED
Force update