tripwire®

TRIPWIRE®
INDUSTRIAL
VISIBILITY

TRIPWIRE INDUSTRIAL VISIBILITY 4.2.4
REFERENCE GUIDE

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Reference Guide Revisions

Rev	Date	Owner	Author	Revisions
Rev 1	February 2021	Moshe Alvoer	Beth Stolper	Initial Version

Table of Contents

List of Tables

List of Figures

1 Introduction

This document provides reference material for Tripwire Industrial Visibility (TIV) Version 4.2.4 and supplements the *TIV User Guide*.

2 Reference

2.1 Alerts

2.1.1 Alert Guidelines

2.1.1.1 Common Alert Types

Integrity Alerts

- Asset Down
- Asset Information Change — Occurs when information associated with an asset is changed (new IP/MAC address)
- Auto Resolved
- Baseline Down
- Baseline Deviation — New traffic occurs between devices that has never occurred before within the baseline. The baselines are categorized by communication type, access type, and frequency
- Baseline Rule
- Configuration Download— When a user downloads the configuration from an engineering workstation or other software package to a PLC.
- Configuration Upload — When a user uploads the configuration from a PLC to an engineering workstation or other software package. Commonly contains the following: code segments being uploaded, code differences, users performing code changes, project name/identifier
- DCS Configuration Change Event
- Firmware Download — When firmware is changed for an asset. Generally performed by an engineering workstation or other software on a PLC
- FS Change
- Generic
- Mode Change — When a user changes the state of a PLC from an engineering workstation or other software application. Mode state examples: Run, Stop, Program
- Monitor Debug — When a user uses an engineering workstation or other software package to put a PLC into monitor or debug mode.

> Note: This is typically a troubleshooting function built into some PLCs

- New Asset — A new asset has been added into the environment (vendor laptops, virtual machines, physical servers, network switches, and PLCs)
- New Conflict Asset — When new information occurs that conflicts with existing asset information. Typically occurs when assets have the same IP/MAC addresses or other identical information
- No Conclusion
- Online Edit — When a user connects to the PLC from an engineering station and performs changes in the settings
- Policy Rule Match
- Policy Violation
- Program Operation
- Protocol
- Specific
- Suspicious Activity — Suspicious behavior generally indicative of malware
- Suspicious File Transfer Alert — Suspicious behavior generally indicative of malware

Security Alerts

Security alerts represent malicious behavior and are not generally supposed to occur within the OT environment and should always be evaluated at the highest priority.

- Login — Occurs with certain makes/models of PLCs that support authentication functions
- Man-in-the-Middle Attack — When an attacker inserted a new machine into the communication pathway between two assets. This new machine will use

this position to either monitor or alter the communication between these assets.

- Network Scan — When an attacker scans either the OT network, or assets within it, looking for attack pathways. Shows the source of the network scan and the affected assets
- TCP Scan – Suspicious activity of an asset performing port scanning in the network
- UDP Scan – Suspicious activity of an asset performing port scanning in the network
- Known Threat Alerts – TIV uses a sophisticated signatures-based database to identify known attacks
- Threat – Collection of known malware commands and control servers

2.1.1.2 Process Integrity Alert Details

A process integrity alert is not necessarily malicious but has an impact on the control of the process and should be investigated. These are events that regularly happen as a part of approved engineering and maintenance tasks, but if they happen outside of this, require attention. The following section outlines the different process integrity alerts, explains what they mean, and defines their severity.

New Asset Alert

A new asset is learned by detecting its communication. Although the asset is new, its communication could be familiar because it was seen within the same Virtual Zone. It is possible the policy already contains rules that address this communication.

A new asset alert occurs when a new asset is added. Examples of new assets are:

- Vendor laptops
- Virtual Machines
- Physical servers
- Network switches
- PLCs
- I/O cards
- Media converters

A new asset alert can be approved or archived. When a new asset alert is approved, all of its associated baseline information is added as valid. If the alert is archived, it will be rejected, and the asset and baselines will not be added.

The **Asset Communication** section of the **New Asset** alert shows if the communication is addressed by existing policy rules. The following cases can be found:

- When the asset communication is covered by existing rules:

Figure 1 Asset communication already covered by rules

- Some of the asset's observed communication is addressed by existing rules (either 'Allow' or 'Alert'):

Figure 2 Some asset communication already covered by Alert or Allow rules

- The asset communication does not have any matching existing rules:

Figure 3 Asset communication does not match any existing rules

Policy Unmatched Violation Alert

The Policy mechanism automatically generates rules that control alert strategies. These rules differentiate between allowable versus suspicious communication.

The rules are presented by zones, assets, or groups of assets, depending on how the assets are assigned during the discovery process.

The **Policy Unmatched Violation** alert is triggered when the communication detected between assets did not match any explicit 'Allow' or 'Alert' rules. The implicit "Alert on Anything" rule is matched by default.

When investigating such alerts, the alert page "**Policy Unmatched Violation**" assists with:

- Understanding the detected communication
- Finding the closest existing policy rules and seeing how the detected communication differs from them
- Understanding which rules should be created and added to the policy in order to approve the detected communication so it does not trigger an alert if seen again

In the following example, the closest policy rule is only allowed for 'Read' access, while the violating communication is using 'Write' access with an action of 'no matching rule':

Figure 4 Policy Violation Alert Page - Example

Policy Rule Match Alert

This policy alert occurs when communication matches an existing rule with an action of 'Alert'. The alert page displays the only matched rule:

Figure 5 Policy Rule Match Alert

Asset Information Change

An information change alert occurs when information associated with an asset is changed.

Every asset information change must be verified and approved. When a software version changes, the system reports the change.

Examples of the types of information changes are:

- A new IP address
- A new MAC address
- A new firmware version
- New card information

You can approve or archive an asset information change alert. Archiving an alert rejects it.

Online Edit

An online edit alert raises when you connect to the PLC from an engineering station and perform changes in the settings.

Mode Change

A mode change alert occurs when a user changes the mode of a PLC from an engineering workstation, or other software application. The modes of the PLC are:

- Run
- Stop
- Program

Depending on the make and model of the PLC, there may be more or less modes. The alert always indicates which mode the PLC was changed to and which mode it was changed from.

When you resolve a mode change alert, the system captures this change.

Configuration Upload

A configuration upload alert occurs when you upload the configuration from a PLC to an engineering workstation or other software package.

This alert commonly contains the following:

- Code segments being uploaded
- Code differences
- Users performing code changes
- Project name/identifier

When you resolve a configuration upload alert, the system captures this change.

Configuration Download

A configuration download alert occurs when you download the configuration from an engineering workstation or other software package to a PLC. This alert commonly contains the following:

- Code segments being uploaded
- Code differences
- Users performing code changes
- Project name/identifier

When you resolve a download configuration alert, the system captures this change.

Monitor/Debug

A monitor/debug alert occurs if a user uses an engineering workstation or other software package to put a PLC into monitor or debug mode. This is typically a troubleshooting function built into some PLCs. This alert does not occur for every make and model of PLC and should rarely occur during normal operation.

When you resolve a monitor/debug alert, the system records this change.

New Conflict Asset

A new asset conflict alert occurs when new information conflicts with an existing asset's information. This could occur because an asset with an identical IP address, MAC address, or other information is present.

Choose from the following to resolve the conflict:

- Merge the old and the new data
- Remove the old asset data, and insert the new asset data
- Remove the new asset data, and keep the old asset data

Firmware Upgrade

A firmware upgrade alert occurs when the firmware is changed for an asset. An engineering workstation or other software on a PLC typically performs this upgrade. When this alert occurs, the system captures both the new and old version of firmware.

When you resolve a firmware upgrade alert, the system records this change.

Suspicious Activity

Suspicious behavior is generally indicative of malware. This uncommon network activity has been seen before in malware attacks and should be checked.

An example is accessing uncommon variables and executing commands with suspicious arguments.

2.1.1.3 Security Event Alert Details

Security event alerts are not generally supposed to occur within the OT environment. These events should always be evaluated at the highest priority because of immediate security concerns.

TIV identifies both known and unknown threats. The known threats are identified based on the signature database. Unknown threats are identified based on our anomaly detection system.

Login

A failed login to a PLC occurs when a user attempts to login multiple times in a row and fails each time. It occurs with certain makes/models of PLCs that support authentication. This alert could represent an attacker attempting to gain access into a PLC through a brute force attack.

When this alert occurs, evaluate the details of the failed login attempts to determine if it is a user inputting incorrect credentials, or if it is a malicious attempt.

This can normally be determined by the source and frequency of the authentication attempts. If the source of the authentication attempts is not a normal access point for a PLC (for example, an engineering workstation or HMI), this may indicate malicious traffic. If the frequency of failed login attempts is significantly faster than a normal user would attempt, this would also indicate malicious behavior.

Man in the Middle Attack

A Man In The Middle (MITM) attack indicates an attacker inserted a new machine into the communication pathway between two assets. This new machine will use this position to either monitor or alter the communication between these assets.

Whenever a man in the middle attack alert is generated, it will capture both the new machine inserted into the communication pathway, and both of the assets affected by the attack. The new asset added should be identified and removed or remediated to prevent it from being used in an attack again. The pathway the attacker used should be evaluated as well. All the actions taken during the man in the middle attack will be captured. This information should be used to reverse any changes made to the affected assets.

Host/Port - TCP/UDP Scan

A Host or Port Scan alert is raised when one of the assets is scanning the ports. The port scan occurs on either TCP or UDP protocols. Attackers can use this activity to identify which ports are open and determine which OS is running on a given asset.

Network Scan

A network scan alert occurs when an attacker scans either the OT network, or assets within the OT network, looking for attack pathways. This alert shows the source of the network scan, and the affected assets.

When a network scan occurs within the network, evaluate the machine that performed this scan, the pathway the attacker used, and the affected machine to ensure they are not vulnerable to remote network attacks.

Network scans can also be detected in training mode.

Threats

TIV uses a signature-based database to identify known attacks, such as Conficker and Havex.

2.1.2 Alerts & Mitigation Table

The following table lists the names of the alerts in the system, their descriptions, their corresponding mitigation steps, as well as their significance.

The various alert tables differentiate between Integrity or Security Alerts. They are broken down into the alert types displayed in the Open Alert widget in the dashboard.

Table 1: Process Integrity Alerts & Mitigations

Alert Type	Alert Classification	Description	Meaning	Mitigation Steps
Asset Information Change	Asset Related	Occurs when information associated with an asset is changed (e.g. rack slot, model, hostname, etc.)	Every asset information change in your network must be verified and approved. When a software version changes, for instance, the system will report a software version change.	1) Understand the purpose of the change (e.g. hostname change), and determine if anyone has been notified about an upcoming IP modification 2) Update an OT Engineer or an IT Admin if necessary.
Baseline Rule	User Specific			

Alert Type	Alert Classification	Description	Meaning	Mitigation Steps
Baseline Deviation	Policy Deviation	During training mode, the system learns the existing asset communication and defines a baseline for how a normal asset (or group of assets) behaves on the network in terms of its communication patterns. During operational mode, baselines can be changed or further defined by (a) Auto-generated virtual zones and (b) user approving alerts. Example: A baseline deviation has been detected from AssetID1 to ZoneXX	Every non-standard behavior activity in your network must be verified. Non-standard behavior can be an initial detection of malicious activity in your network.	1) Open the asset details and try to determine whether the communication is expected. 2) In case this behavior is unexpected, update the IT admin or a network owner for further investigation.
Baseline Volume Deviation	Policy Deviation			
Configuration Download	Process Impact	When a user downloads the configuration from an engineering workstation or other software package to a PLC. Commonly contains the following types of alert information: code segments being downloaded; code differences; users performing code changes; project name/identifier.	An attacker may want to interfere with normal critical infrastructure activity by changing a PLC code. If the PLC is running and as a result stops functioning, it may cause a significant production loss.	1) Verify if this maintenance work was scheduled. 2) If it was scheduled using the download configuration file option, verify that the actual change that was done is the change that was planned. 3) If not, check with the responsible OT engineer and provide the code change from the system in case a change was detected.

Alert Type	Alert Classification	Description	Meaning	Mitigation Steps
Configuration Upload	Process Integrity	When a user uploads the configuration from a PLC to an engineering workstation or other software package. Commonly contains the following types of alert information: code segments being uploaded; code differences; users performing code changes; project name/identifier.	An attacker may want to interfere with normal critical infrastructure activity by changing a PLC code. If the PLC is running and as a result stops functioning, it may cause a significant production loss.	1) Verify if this maintenance work was scheduled. 2) If it was scheduled using the download configuration file option, verify that the actual change that was done is the change that was planned. 3) If not, check with the OT engineer, the owner of this answer, and provide the code change from the system in case a change was detected.
DCS Configuration Change Event	Process Impact			
File System (FS) Change	Process Impact			
Firmware Download	Process Impact	When firmware is changed for an asset. Firmware upgrades are generally performed by an engineering workstation of other software on a PLC. Example: Out of working hours a Firmware Download operation was performed for the first time by <Asset ID1> on <Asset ID2>	A firmware upgrade may introduce new vulnerabilities that have not previously existed. This action should be examined and carefully considered before it is done. If an attacker is aware of this vulnerability, they may make a firmware change in order to be able to perform more destructive actions. Since critical infrastructure is involved, such activity is severe and must trigger an alarm.	1) Verify if this maintenance work was scheduled. 2) If not, check it with the OT engineer that owns this asset.
Memory Reset	Process Impact			
Mode Change	Process Impact	When a user changes the state of a PLC from an engineering workstation or other software application. Mode state examples: Run, Stop, Program. Example: PLC-X mode changed to Run Mode by Engineering Station-Y, by User-Z	An attacker may want to interfere with normal critical infrastructure activity by changing a PLC mode. If the PLC is running, and the attacker stops it, this may cause a significant production loss. For example, a command such as a 'stop' to a PLC can cause a DoS (Denial-of-Service) attack.	1) Check if the reason for the mode change is familiar. 2) Check with the OT Engineer that owns this asset to ensure that this change is allowed and reasonable.

Alert Type	Alert Classification	Description	Meaning	Mitigation Steps
Monitor Debug	Process Impact	When a user utilizes an engineering workstation or other software package to put a PLC into monitor or debug mode (Note: This is typically a troubleshooting function built into some PLCs).	An attacker may want to interfere with normal critical infrastructure normal activity by changing a PLC mode to debug mode. If the PLC is running and the attacker stops it, or slows it down, this may cause a significant production loss. For example, a command such as a 'stop' to a PLC can cause a DoS.	1) Verify if this maintenance work was scheduled. 2) If not, check with the OT engineer that owns this asset if this was the planned change.
New Asset	Asset Related	A new asset (e.g. vendor laptop, virtual machine, physical server, network switch, PLC, etc.) has been added into the environment.	Every new asset that was added to your network should be examined and approved to determine the purpose of its network activity and whether it is legitimate.	1) Check with an OT Engineer or an IT Admin if this is a known asset. 2) View the asset details to get more information about the new asset, such as the vendor, the nature of the communication, who is talking to who, and the baselines. 3) Try to connect to the asset to get more details.
New Conflict Asset	Asset Related	When new asset information conflicts with existing asset information. This typically occurs when assets have the same IP/MAC addresses or other identical information. Example: A new asset has been detected AssetID1 and is conflicting with AssetID2.	Every new asset change in your network must be verified. A change in your asset details may be done by attackers to perform authentication based on an IP address. For example, a common attack is to impersonate a high privileged IP address, such as an engineering station, and use it to run changes on a critical equipment.	1) Verify whether this information change was expected and if anyone provided notification of an upcoming IP modification. A MAC modification is uncommon and might be suspicious, further investigation is needed. 2) Update the IT admin.

Alert Type	Alert Classification	Description	Meaning	Mitigation Steps
Online Edit	Process Impact	When a user connects to a PLC from an engineering station and performs changes in the settings. Example: Online edit was performed on PLC-X by Engineering Station-Y	An attacker may want to interfere with normal critical infrastructure activity by changing a PLC mode. If the PLC is running and the attacker stops it, this may cause a significant production loss. For example, a command such as a 'stop' to a PLC can cause a DoS.	1) Verify if this maintenance work was scheduled. 2) If not, check it with the OT engineer who is the owner of this asset.
Policy Rule Match	Policy Deviation	Communication matching Policy Rule ID NNN was detected from AssetID1 to AssetID2	Occurs when a communication instance matches an existing rule with an Action of 'Alert'.	The user requested to be notified when incoming traffic hits this rule.
Policy Unmatched Violation	Policy Deviation	Out of working hours Policy Violation: New intrusive operation of type data acquisition operation was detected from AssetID1 to AssetID2	Every non-standard behavior activity in your network must be verified. Non-standard behavior can be an initial detection of malicious activity in your network.	

Table 2: Security Events Alerts & Mitigations

Alert Name	Alert Classification	Description	Meaning ("What does this mean")	Mitigation Steps
Invalid Session	Security Alert			
Known Threat Alert	Security Alert	TIV uses a sophisticated signature-based database in order to enhance the capability of identifying known attacks. Example: AssetID1 request buffer overflow attempt from AssetID2.	This alert is usually a strong indication of a computer performing a malicious action.	Attack alarm! Report this activity to your Security Risk Officer as soon as possible.
Login	Process Integrity	Example: Out of working hours Failed Login: Failed Login attempts were made to asset to <AssetID1> from <AssetID2>	An attacker may want to interfere with normal critical infrastructure activity by logging into a PLC while it is running. Such activity may cause the PLC to stop or become non-operational. This may cause a significant production loss.	1) Verify if this maintenance work was scheduled. 2) If not, consult with the OT engineer that owns this asset.
Malformed Packet/s	Security Alert			
Suspicious Activity	Security Alert	Suspicious behavior generally related to malware.	Suspicious activities are recognized behavior of malware based on a known collection of common behavior and signatures.	1) Understand who initiated the activity, who was affected by it, and attempt to clear any suspicion of the initiating computer in order to understand the nature of the traffic. 2) Inform your Security Risk Officer.

Alert Name	Alert Classification	Description	Meaning ("What does this mean")	Mitigation Steps
Suspicious File Transfer Alert	Security Alert	Suspicious file transfer found. Example: File-X was transferred via Protocol-Y and matched the following Yara rules: ZZZ, transferred from AssetID1.	This alert is usually a strong indication of a computer transferring a malicious file	1) Understand who initiated the activity, who was affected by it, and attempt to clear any suspicion of the initiating computer in order to understand the nature of the traffic. 2) Inform your Security Risk Officer.
Threat	**Security Alert**	**Collection of known malware commands and control servers.**	**This alert can usually identify a computer infected by a specific malware trying to communicate with its command and control server.**	**Attack alarm! Report this activity to your Security Risk Officer as soon as possible. Infected by a specific malware trying to communicate with its command and control**

Threat Name	Description	Meaning	Description
Man-in-the-Middle Attack (MitM)	Occurs when an attacker inserts a new machine into the communication pathway between two assets in the network. This new machine will use this position to either monitor the communication between these assets or to alter the communication between them.	A man-in-the-middle attack (MitM) indicates that an attacker inserted a new machine into the communication pathway between two assets within the network. This new machine will use this position to either monitor the communication between these assets, or to alter the communication between these assets. Whenever a MITM attack is generated, it will capture both the new machine inserted into the communication pathway, and both of the assets affected by the attack. The new asset added should be identified and removed or remediated to prevent it from being used in an attack again in the future. The pathway the attacker utilized to compromise the attacking machine should be evaluated as well. Additionally, all the actions taken during the MitM attack will be captured and should be used to reverse any changes made to the affected assets.	Attack alarm! Report this activity to your Security Risk Officer as soon as possible.

Threat Name	Description	Meaning	Description
Network Scan	When an attacker scans either the OT network, or assets within the OT network, looking for attack pathways. Shows the source of the network scan and the affected assets.	Network scanning refers to the use of a computer network to gather information regarding computing systems. Network scanning is mainly used for performing attacks by hackers and also used for security assessment or system maintenance. Example: AssetID1 has performed a network scan, attempting to scan IT sensitive communication ports.	1) Understand which asset triggered the scan and which assets were affected by it. Also understand attempts to clear any suspicion of the initiating asset in order to understand the nature of the traffic. 2) Report this activity to your Security Risk Officer.
TCP Scan	Suspicious activity of an asset scanning ports in the network.	A port scan attack occurs when an attacker sends packets to your machine, varying the destination port. The attacker can use this method to determine the services you are running and obtain a strong indication of the operating system you are using.	Attack alarm! Report this activity to your Security Risk Officer as soon as possible.
UDP Scan	Suspicious activity of an asset scanning ports in the network.	A port scan attack occurs when an attacker sends packets to your machine, varying the destination port. The attacker can use this method to determine the services you are running and obtain a strong indication of the operating system you are using.	Attack alarm! Report this activity to your Security Risk Officer as soon as possible.

2.2 Insights

Insights are categorized according to levels of importance: red is high, yellow is intermediate, and grey is low importance.

The following asset types are not considered in Insight calculations:

- External
- Out of scope
- Ghost
- Multicast
- Broadcast

> **Note:** Note all of the following insights are written in plural; they may also appear in singular.

2.2.1 Insights with High Importance

2.2.1.1 Top Risky Assets

Top X Risky Assets

Assets with the highest risk score.

> **Note:** The Risk Score indicates the risk level of an asset. The higher the score, the riskier the asset.
>
> The system will take up to 10 assets with the highest risk score.

2.2.1.2 Talking with External IPs

X assets were communicating with X external IPs (X of them are ghost)

External Ips, with respect to network interfaces, expose the asset to users outside of the company's perimeter, enabling attackers to enter the OT network.

> Note: Popular talking with - limited to 50 assets

2.2.1.3 Unsecured Protocols

X assets are using X unsecured protocols: List of Protocol Names

Protocols containing security weaknesses that attackers can leverage to compromise the network's security.

> The TFTP protocol has no authentication and transfers data in plain-text.

The protocols the system considers as unsecured are: FTP, SMB (v1), SMTP, SNMP (v1/v2), SSH (v1), SSL (all versions), TELNET, TFTP, TLS (1.0 – 1.1) and VNC.

To understand why a particular protocol is considered unsecured, see the details provided in the column 'Reason Protocol is Unsecured':

Figure 6 Reason Protocol is Unsecured

2.2.1.4 Full Match CVEs

X assets have X unpatched vulnerabilities - Full Match

This table lists assets that run vulnerable software versions and can be leveraged by attackers for various malicious purposes such as remote code execution, DDoS, etc..

Vulnerabilities are matched against these assets' vendor name, model family and number, and software version.

2.2.1.5 Windows Full Match

X assets have X unpatched vulnerabilities - Windows Full Match

This table lists assets, running a Windows operating system version, matched against known vulnerabilities published by Microsoft.

> Note Vulnerabilities are matched against these Windows assets' version, build number and list of installed security patches.

2.2.2 Insights with Medium Importance

2.2.2.1 Data Acquisition Write (Operated PLCs)

X assets performed data-acquisition write operations on X assets

This insight includes all the assets that performed data acquisition write actions. These assets should be considered as potential assets that can change the process by changing values.

2.2.2.2 Assets using SMBv1 Protocol Only for Negotiate

Assets using SMBv1 Protocol Only for Negotiate

SMBv1 negotiation has been detected. SMBv1 has published vulnerabilities most commonly used by WannaCry malware.

It is recommended to disable the use of the SMBv1 protocol extension on all Windows boxes.

2.2.2.3 Managed PLCs (by Rockwell users)

X users using X Rockwell engineering stations managed X PLCs

This insight contains information regarding a user that performed a connection to the PLC using a Rockwell engineering station. The users listed are those that logged into the Windows machine running the engineering software.

2.2.2.4 Multiple Interfaces

X assets have multiple network interfaces

Every network interface enables independent communication. This may compromise the efficiency of firewall segmentation, which may not take into consideration all the interfaces when defining the asset's policy.

2.2.2.5 Privileged Operations (Operated PLCs)

X engineering stations performed privileged OT operations on X PLCs

Privileged commands are not part of the standard data acquisition commands. These commands are often used as part of engineering work such as configuration download/upload or changing settings and modes.

2.2.2.6 Clients Remotely Managed

X assets managed X assets remotely using: List of Protocols

Assets feature a connection with remote users (3rd parties or employees) for various maintenance purposes.

2.2.2.7 Model Match CVEs

X assets have X unpatched vulnerabilities - Vendor and Model Match

This table lists assets with vulnerable software versions that can be leveraged by attackers for various malicious purposes such as remote code execution and DDoS.

Vulnerabilities are matched against these assets' vendor name and model family and number.

2.2.2.8 Program Match CVEs

This table lists assets with installed program versions and can be leveraged by attackers for various malicious purposes such as remote code execution and DDoS.

> Note Vulnerabilities are matched against these assets' installed program versions.

2.2.2.9 Using Default Passwords

Assets use default passwords that can be easily guessed by unauthorized users.

2.2.2.10 Using Unencrypted & Weak Passwords

Weak passwords from unencrypted or default passwords make those assets exploitable. To reduce the risk of those assets, use passwords with encrypted protocols and change the default password.

2.2.2.11 Assets with partial connection to the internet

Assets seem to be intended to be isolated, yet these assets can still access external resources via DNS requests.

When there are assets that seem to be intended to be isolated, they can still access external resources via DNS requests. This Partial External Access Insight addresses the issue by identifying any potentially exploitable assets, enabling users to change the policies in the network accordingly. It works by locating the assets that are requested to reach an external address, getting a response from the DNS server, and are not allowed to have an external connection.

2.2.2.12 PLCs Talking IT Protocol

X assets using IT protocols

Asset is communicating using IT protocol. This could be the result of misconfiguration or malicious activity.

2.2.2.13 Triconex in Program mode

X Triconex safety systems are in remote programmable mode

Setting the device in a remote program mode enables a malicious user to alter the configuration on the remote device. The same methodology was leveraged by the Triton malware to exploit a remote device.

It is considered best practice to avoid setting the device in remote programmable mode.

2.2.2.14 PLCs not in Run mode

X PLCs are exposed to remote program changes or have stopped

The ability to set a PLC key mode enables the lockdown and hardening of the device in order to block any remote code changes. This can be a virtual or a physical key state. Setting the device in run mode (disabling the remote program capability) will reduce the risk of unauthorized logic/program modifications. Devices that have stopped can indicate that something went wrong.

2.2.2.15 OT connection to a Triconex device in Program mode

Performing OT commands via {protocol} protocol on a Triconex safety system in Program mode

The risk of having a device in Program mode is unauthorized change of logic. An attacker can leverage Triconex protocols to enter new programs to the controller or modify the existing program on the device and cause unexpected behaviour. The same methodology was used by the triton malware in order to exploit a remote device.

2.2.2.16 OT connection to a PLC in Program mode (not Triconex)

Performing OT commands via {protocol} protocol on a controller in Program state

The risk of having a device in Program mode is unauthorized change of logic. An attacker can leverage OT protocols to enter new programs to the controller or modify the existing program on the device and cause unexpected behaviour.

2.2.2.17 OT connection to a PLC in Remote mode

Performing OT commands via {protocol} protocol on a controller in Remote state

The risk of having a device in Remote mode is unauthorized change of logic by a remote endpoint. An attacker can leverage OT protocols to enter new programs to the controller or modify the existing program on the device and cause unexpected behavior.

2.2.3 Insights with Low Importance

2.2.3.1 Communicating with many assets

X assets are communicating with many assets

These assets are highly ranked in terms of the amount of network connections they initiate. In some cases, this indicates key elements in the network such as,

data collection services, monitor servers, or possibly an adversary performing broad reconnaissance.

2.2.3.2 DHCP servers

X assets are acting as DHCP servers

A DHCP server enables clients to request IP addresses and networking parameters automatically. It is important to monitor the DHCP servers in the network because an attacker can pretend to be the server and use it to perform various attacks.

2.2.3.3 DNS servers and queries

X assets performed DNS queries on X servers

Examination of DNS queries can reveal if an asset features any anomalous outbound communication that may indicate malicious presence.

2.2.3.4 Files Downloaded (clients)

X assets downloaded files from X file servers using protocols: List of Protocols

A prominent OT attack method is to maliciously modify a configuration file and download it to the controller. Any asset involved with downloading files should be closely monitored.

2.2.3.5 Open Ports

X assets have open ports

Open ports are the doorways to your secure perimeter. Behind open ports, there are applications and services listening for inbound packets, waiting for connections from the outside in order to perform their jobs. Security best practices imply the use of a firewall system that controls which ports are opened or closed on Internet-facing servers.

Additionally, security best practices advise that ports should be opened only on an "as-needed" basis, dictated by the Internet communication needs of applications and services that run on the servers.

> Note: Shows open ports for the top 50 ports of the asset. If the port is above 30,000 it will not be displayed.

2.2.3.6 Assets that Highly Connected Assets Talked to

X assets are highly connected assets

These assets are highly ranked in terms of the amount of network connections they initiate. In some cases, this indicates key elements in the network such as, data collection services, monitor servers, or possibly an adversary performing broad reconnaissance.

2.2.3.7 Assets Accessed SMB Shares

X assets had open SMB shares; X assets accessed them

SMB file shares accessed by assets in the network. Based on this insight, one can find critical shares that hold operational information or unauthorized access.

2.2.3.8 Assets Accessing SMB Pipes

X assets had open named pipes of SMB; X assets accessed them

Accessing a named pipe can give an indication of remote management and can be used for monitoring remotely, reading event-log records, modifying registry keys, and executing code (e.g. PsExec).

2.2.3.9 Talking with Ghost Assets

X ghost assets were identified in the network; X assets were communicating with them

Ghost assets are network entities that never replied. These assets could be the result of a misconfiguration and can be used as an attack surface into the network. Attackers can hijack such communication by impersonating as a ghost asset, compromising the talking asset.

2.2.3.10 Web Servers

X assets accessed X Web Servers

Assets that function as web servers.

2.2.3.11 SNMP Querying Assets

X assets had SNMP queries issued by X servers

SNMP is a legitimate tool to gather information from Windows machines. However, it is also in common use with attackers attempting to expand their knowledge on the network following an initial compromise.

A high volume of SNMP queries relative to other machines may indicate malicious presence.

2.2.3.12 Windows CVEs

X assets have X unpatched vulnerabilities - Windows Match

This table lists assets, running a Windows operating system version, matched against known vulnerabilities published by Microsoft.

> Note that Vulnerabilities are only matched against Windows OS version, regardless of Service Pack version or Security Updates.

2.2.3.13 Vendor Match CVEs

X assets have X unpatched vulnerabilities - Vendor Match

This table lists assets that run vulnerable software versions and can be leveraged by attackers for various malicious purposes such as remote code execution and DDOS.

> Vulnerabilities are matched against these assets' vendor name.

2.2.3.14 USB Devices Connected to Assets

X USB Devices connected to X assets

This table shows the USB devices in the network and which assets these devices connect to.

2.2.3.15 Remote Desktop Application

X assets have remote desktop application

This table lists assets indicating the existence of remote desktop applications that can be leveraged by attackers for various malicious activities.

2.2.4 CVE Matching

With the system's Common Vulnerabilities and Exposures (CVE) discovery mechanism, asset vulnerabilities differ between various types of matches: 'full', 'vendor', 'model', and 'Windows'. The solution matches a CVE (vulnerability) to an asset based on the information gathered:

- **Full match** – This category covers vulnerabilities for assets where their vendor, model, firmware version, and software version match those specified in the CVE. This is the most accurate level of CVE matching that results in a very high probability of exposure to the identified CVE.

  This table lists assets with vulnerable software versions that can be leveraged by attackers for remote code execution and DDoS.

- **Vendor match** – This category includes vulnerabilities for assets whose vendor matches the vendor specified in the CVE.

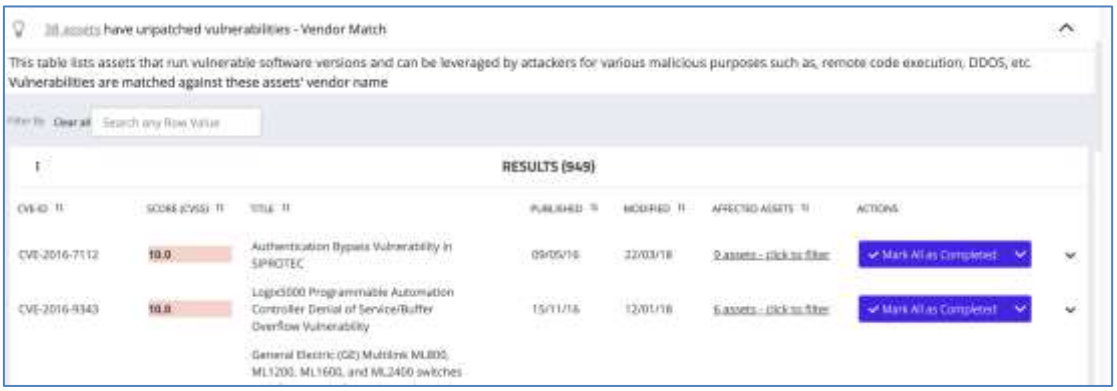


Figure 7 Vendor Match CVE table

- **Model match** – This table lists assets with vulnerable software versions that can be leveraged by attackers for remote code execution and DDoS. Vulnerabilities are matched against these assets' vendor name and model (family and number).
- **Installed Program match** – This table lists assets with installed program versions that are vulnerable and can be leveraged by attackers for remote code execution and DDoS.
  Vulnerabilities are matched against these assets' installed program version.

Figure 8 Installed Program Match CVE table

- **Windows** – This category includes vulnerabilities for assets that matched only the OS version (without considering service packs).

These vulnerabilities are displayed according to their criticality level (High, Medium, and Low) as follows:

- A full match is displayed with red (high criticality).
- The model and installed program matches are displayed with yellow (medium criticality).
- Windows and vendor matches are displayed with grey (low criticality).

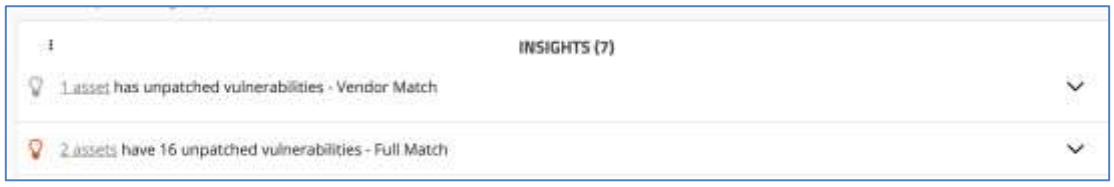


Figure 9 Insights Page - CVE Examples

> Note Users can receive regular update packages from Tripwire with the latest threat definitions as discovered by Tripwire's Research team. These Threat Definition Updates include new CVEs as well as network traffic signatures and Yara signatures.
> The update packages allow users to stay up-to-date without a full upgrade of the entire TIV software. For more information, see the **TIV User Guide**.

2.2.4.1 Supported Vendor List for CVE Matching

Vendors
Siemens
Rockwell Automation (including Rockwell software)
Yokogawa
Omron
Mitsubishi
Hirschmann
Beckhoff
Cisco
Schneider Electric
ABB
Emerson
Google (partial support for Chromecast)

Vendors
GE
Hikvision
Microsoft (for Windows CVEs)
VNC

2.2.5 Approving and Rejecting Insights

Users can update network insights with statuses. Supported statuses are “completed”, “hidden” or “open”, where “open” is the default status. Completing insight vulnerabilities will improve the overall network Hygiene Score. A “hidden” or “completed” insight would not appear by default when showing the list of insights.

> Note When the insight is marked as ‘hidden’ it **does not** affect the asset’s risk score and will not change the hygiene score.

Comments can be applied to Insights. This allows better manageability, allowing the user to keep track of the vulnerabilities and their statuses, while ensuring the Hygiene Score metrics are based only on relevant data.

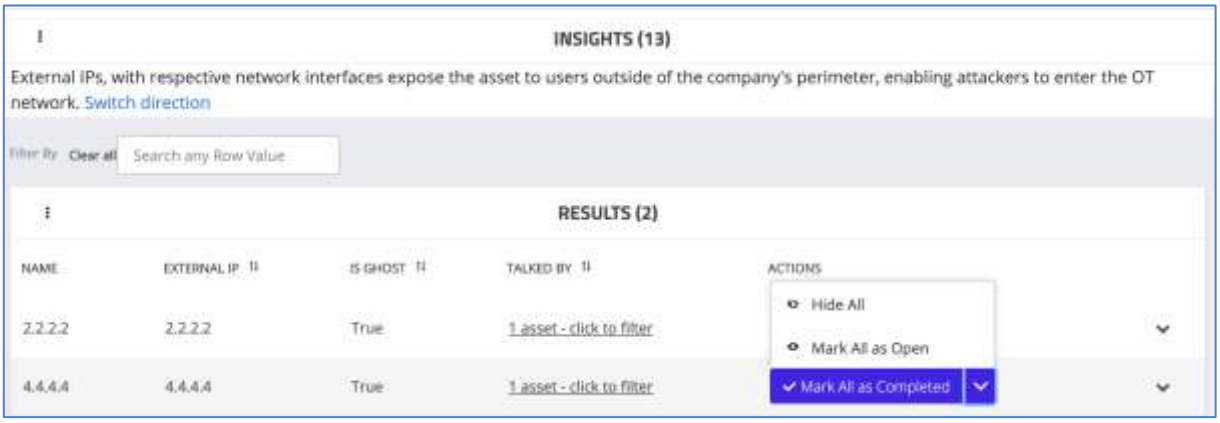


Figure 10 Marking Insights as Completed - Example

2.2.6 DHCP Servers

Insights include an indication of assets providing DHCP services to clients. The DHCP Server Insight includes the DHCP server and the full list of client assets that received the DHCP service from that server:

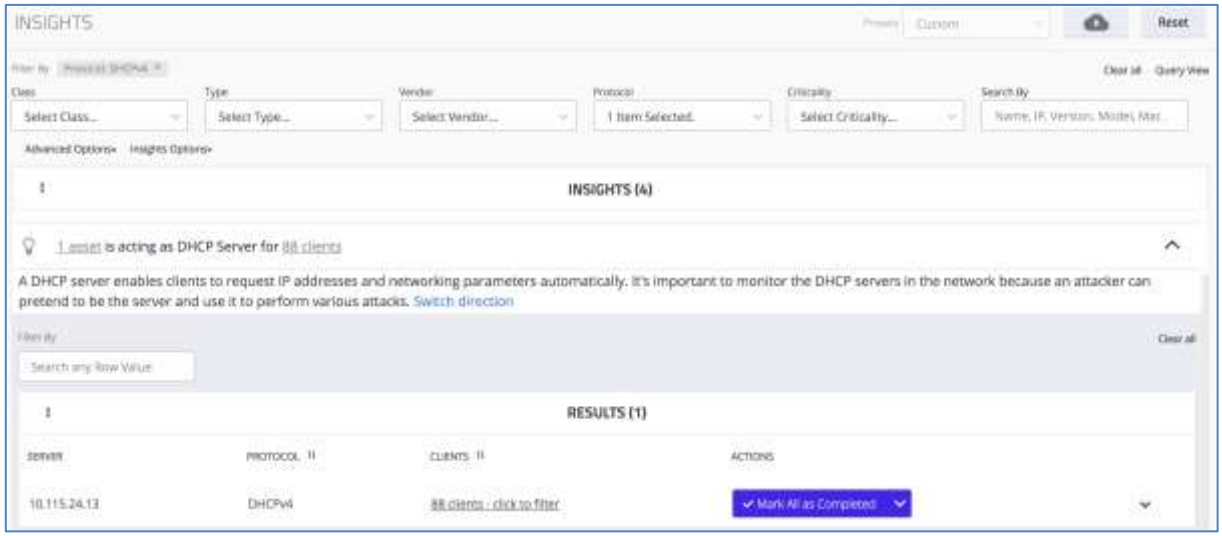


Figure 11 DHCP Servers

2.3 Risk Score Calculation

2.3.1 Overview

TIV's risk score calculation is based on three layers as shown in the following figure:

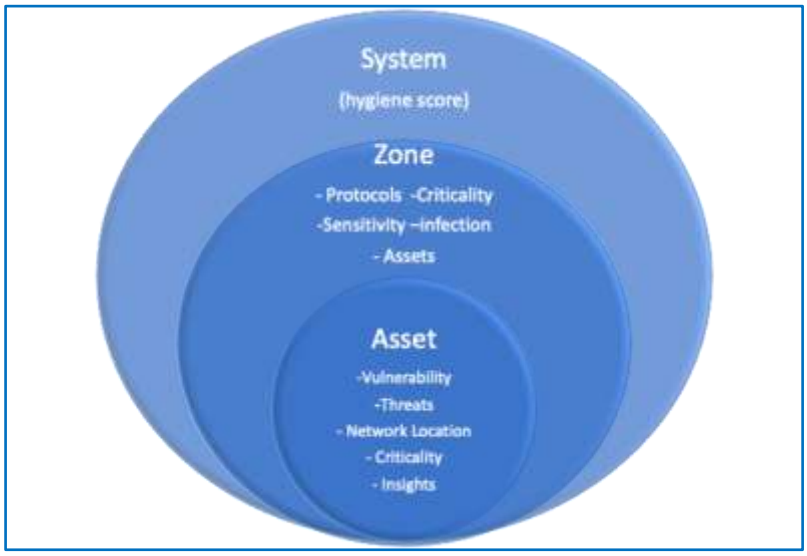


Figure 12 Risk Score Calculation

These three layers (System, Zone, and Asset) are interdependent and are calculated dynamically to ensure the risk score is always correct. Every layer of the risk score is influenced by its asset parameters and the overall risk score of the layers below. The risk for an EMC is calculated on the basis of the risks of all of the sites within the system.

2.3.2 Asset Risk Score

The following five vectors determine the risk score of an asset:

- Vulnerability – The more CVEs an asset has, the more vulnerable it is to attack. The TIV algorithm matches between every asset and its unpatched CVEs and determines a vulnerability score according to the number of CVEs and their corresponding severities. There are additional qualities that deter vulnerability, such as the protocols the asset is using.
- Criticality – This vector is based on how important the asset is in the network and how much damage it could inflict. It is based on the asset's qualities and its privileges (for example, Write HMI PLC, Privileged operations).
- Accessibility – The accessibility score of an asset depends on the asset's network location (its subnet), its communication with dangerous assets and zones (which depends on its baselines and zone policies), and the asset's network behavior (for example, open ports, multiple interfaces, talking with IT).
- Infection – Indicates the extent of the asset's ability to spread malicious content to other assets. This vector is based on the asset's policies, baselines, privileges, insights, and protocols.
- Threat – This vector indicates whether the asset is already considered a threat. This vector is based on open alerts. When there are a lot of open alerts, the asset behavior is suspicious, and likely exposed to threats or is going to be a threat in the network. This parameter is also based on Insights that express a suspicious behavior (for example, talking with external assets and ghost assets, downloaded files).

2.3.3 Zone Risk Score

Five parameters contribute to the calculation of the Risk score of a specific zone:

- Vulnerability – The vulnerability rate of a zone is impacted by its assets vulnerabilities. This value is the average (or the maximum) of all the asset vulnerability vector scores in the zone.
- Criticality – Every zone has its own criticality values that determine its importance.
- Accessibility – Represents to what extent the zone is exposed to risks by its communication to other zones. This rate is influenced by the average

accessibility vector score of the zone's assets, and by the number of zones that communicate with this zone.

- Infection – Indicates the extent of the zone's ability to spread malicious content. It is determined by the average infection rate of the zone's assets and by the number of zones that communicate with this zone.
- Threat – The threat vector indicates whether the asset is already a threat. This vector is the average (or the maximum) of all the asset threat scores in the zone.

2.3.4 Hygiene Score Calculation

The Hygiene Score is the health barometer for the sites and the EMCs. It indicates whether the site is healthy (with few risks) or if it is exposed to many risks. Its scale ranges between 0 and 100, where 100 is the healthiest.

2.4 Cloud

Cloud connectivity enables your existing EMC, on-premise and virtualized deployment options to connect to edge cloud-based technology to further extend cybersecurity of OT networks. This feature is enabled by default using an "Agent" dissector to connect to cloud-based technology via a secure SSL Tunnel.

2.4.1 Overview

The Cloud is a Cloud Update Center to which you can connect any EMC/TIV machine that runs with version 4.0 via a secure SSL Tunnel. The EMC/TIV deployment (whether it is on a VM or on-premise) is irrelevant. Any machine running the TIV/EMC and internet connectivity can connect to the Cloud.

The Cloud Update Server is a database located in the cloud and available via the secure SSL Tunnel to enrich your information, such as Zone Rules. Zone Rules feature a common rate among various sites around the world that obtain ongoing Threat Intelligence updates, thereby enabling users to always be updated with the latest signatures and vulnerabilities. In addition, the Health Check statuses of your machines are sent to the cloud in order to analyze your machine state. This data is sent anonymously according to GDPR regulations.

The primary cloud-based feature is an update to Claroty Threat Intelligence (CTI). The value of threat intelligence decreases with every passing second. Version 4.0 and above equips TIV users with real-time situational awareness of CVEs, Yara Rules, Snort Rules, and other proprietary intelligence sourced from Team82. Instead of waiting for the next version upgrade for an update, TIV's Update Center in the Cloud continuously pushes this information to Enterprise Management Consoles (EMCs) and TIV via a secure tunnel.

Another cloud-based feature is to provide even more context using the "wisdom of the crowd". It starts with an update to our Zones feature, which automatically tags assets with similar attributes and behaviors into logical zones, allowing TIV users to set and enforce policies governing communication between zones.

A worker named “Agent” runs on the TIV/EMC and manages communication with the Cloud. When the agent is off, connection to the Cloud is not possible. After the agent is On, Cloud features are fully accessible for information enrichment and support if needed.

This Cloud data is sent anonymously with the customer UUID, compliant with GDPR regulations.

2.4.2 Cloud Features

The Cloud Features impact several functions:

- Wizard
- Configuration Screen
- Zone Rule Enrichment
- Threat Intelligence Update.

2.4.2.1 Wizard

When installing the system, the cloud checkbox shows at the end of the page. It is enabled by default in order to allow cloud connectivity:

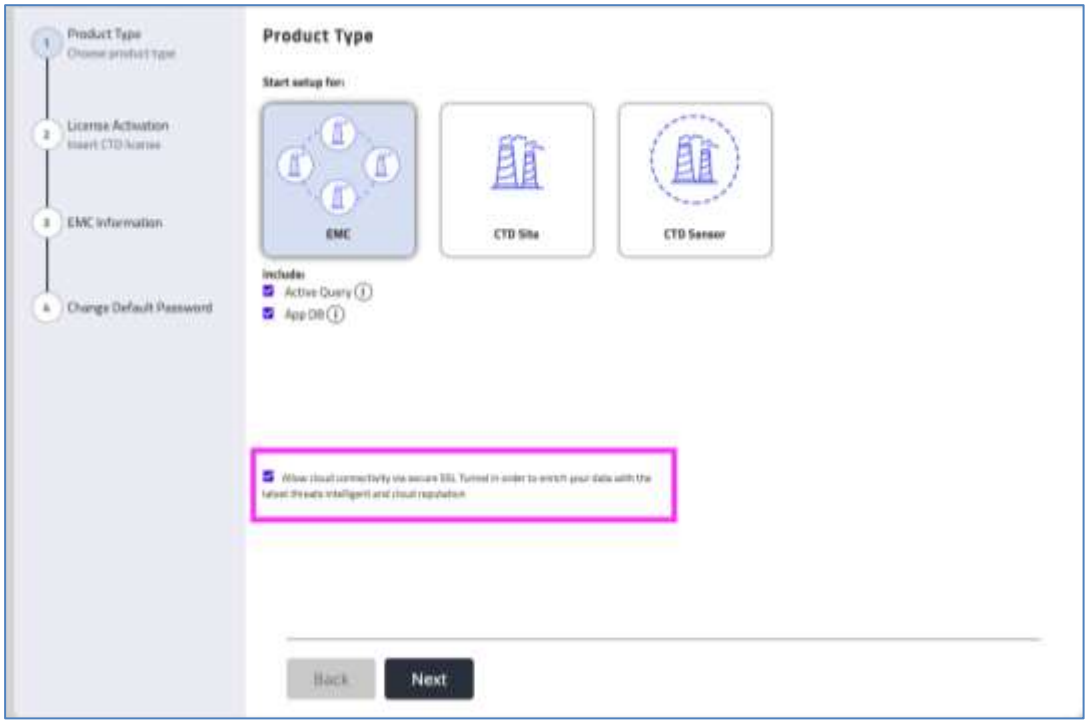


Figure 13 Cloud Connectivity Checkbox

2.4.2.2 Configuration Screen

After installing your EMC with Cloud Connectivity via the first-time-Wizard, you will be able to review the Cloud configuration from your EMC machine.

The “Cloud Update” presents all the cloud related features. From this screen you can control each Cloud feature:

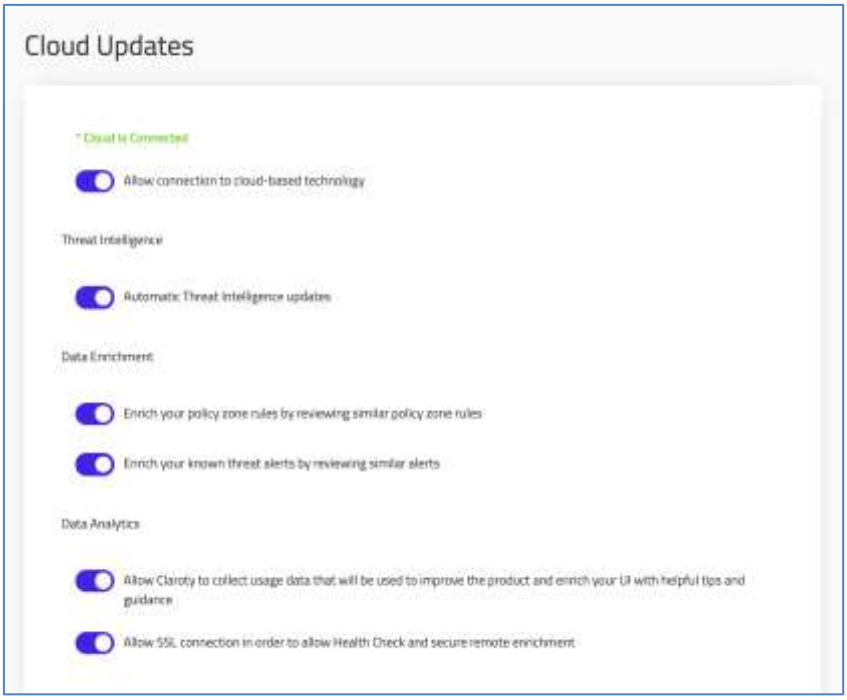


Figure 14 Settings > Management > Cloud Updates

Allow connection to cloud based technology – Enables the Agent worker on the machine and allows your TIV/EMC machine to connect with the Cloud.

Allow SSL connection in order to get Health Check and secure remote enrichment – Allows you to open an SSL tunnel to allow the Tripwire Support team to connect to your environment and handle issues over a secure remote connection.

Automatic Threat Intelligence (TI) Updates – Automatically updates your machine with the latest published vulnerabilities and signatures.

Enrich your policy zone rules by reviewing similar policy zone rules – Enriches the cloud reputation to provide indication of the common rates of your policy zone rules among different sites. It enables the common rate of a specific rule among sites around the world.

Enrich your known threat alerts by reviewing similar alerts – Enriches the cloud to provide indication of the common rates of your known threats among different sites. It enables the common rate of a specific alerts among sites around the world.

Allow TIV to collect usage data that will be used to improve the product and enrich your UI with helpful tips and guidance – Turns on TIV in-product guidance and collects data to be used in the development of new features.

Allow SSL connection in order to allow Health Check and secure remote enrichment – Sends System Health data to the cloud for health monitoring.

2.4.2.3 Zone Rule Enrichment

Zones leverage TIV's deep packet inspection to transform complex OT communications into an intuitive, user-friendly view. Version 4.0 and above takes this visualization to a new level by incorporating data from our sites.

The Cloud enables you to benchmark asset communications and the policies governing them against those of TIV's other sites with cloud-based deployments. Instead of combing through hundreds of communication patterns to look for misconfigurations or to assign permission levels, TIV customers can confidently focus their endeavors based on the "wisdom of the crowd". If a particular baseline or policy is common or universal across sites that TIV is monitoring, TIV customers will be aware of it. Likewise, the same is true for behaviors that are rare or unusual.

Cloud connectivity enriches your Zone rules with a “Cloud Reputation” common rate. This column is displayed in the Zone Rules page and explains about the common rate of a specific rule among sites around the world by indicating the rule’s prevalence among different sites.

The Cloud Reputation classifications are as follows:

- Universal – This policy was seen in most of our site networks
- Common – This policy was seen in a large number of our site networks
- Unusual – This policy was seen in a small number of our site networks
- Rare – This policy was rarely seen in other site networks

The statuses are displayed with different colors to indicate if they require investigation:

- Green – This rule is acceptable in comparison to other sites
- Orange – Probably worthwhile to investigate this rule since it was observed on other sites
- Red – Investigate: This feature is Rare; you need to check it and approve it

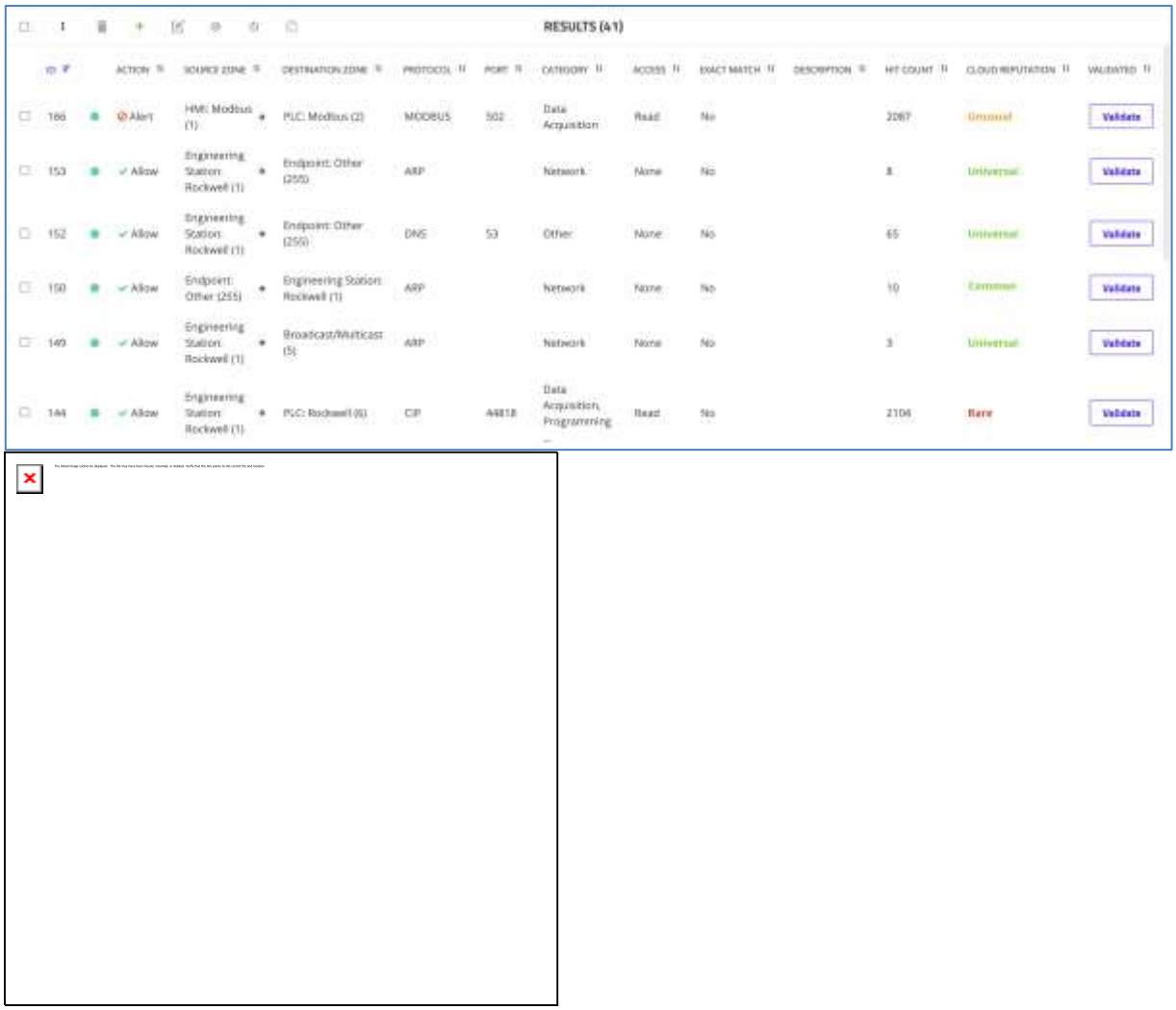


Figure 15 Zone Rules Page - Cloud Reputation Column

2.4.2.4 Auto Pushing of Threat Intelligence Updates

TIV supports auto pushing of Automatic Threat Intelligence updates via the Cloud from the EMC when a new updated Threat Intelligence bundle is recognized. The last date the files were updated is displayed in the Threat Definition Updates screen.

This update can either be acquired automatically from the Cloud or manually uploaded into the EMC, streamlining the entire threat definition update process in a way that keeps all sites up to date with the most recent CVE's, network, and Yara signatures, without the need for a complex update of all sites individually.

When updating manually, you can choose which sites get the update by selecting specific sites from a list. Sites do not get an update when their current version is newer than the one supplied. For more details, see the TIV User Guide: Configuring Threat Detection Updates.

When the system recognizes that an asset has no CVEs, its machine information (including FM version and Model version) is sent to the Cloud and checked by Tripwire's team of analysts.

2.5 Data Sources

2.5.1 Active Detection

2.5.1.1 Changes in Alerting from Passive Behavior

The following information changes generate an alert even in Training mode.

- Firmware
- Mode
- Last Program Installed Date

- Configuration Upload will only be triggered in case of changes (and not for same sections or first time).
- Information change alerts will be generated in Operational mode for changes in non-custom information.

All other information changes will not trigger any alerts in either Training or Operational Mode.

2.5.1.2 Baselines Generated from Active Detection

Typically, in active detection, you don't see baselines because it is not listening to the communication like in passive communication. In active detection, TIV communicates directly to the device. However, if the cases fit one of the following scenarios, then active detection logs baselines:

1. SNMP Queries
   a. TCP connections (current)
   b. ARP connections (historical)
   c. CDP connections (historical)
2. TCP Queries
   a. UDP/TCP

2.5.1.3 Discovery Task, Query and Profile Types

The following tables provide the Discovery Tasks, Queries, and Profiles.

Summary Discovery Tasks Table

Table 3: Summary Table of Discovery Tasks

Task Name	Description
BACnet Discovery	Finds BACnet Devices using a broadcast request
CrowdStrike Discovery	Discovers devices running CrowdStrike Sensors using CrowdStrike's remote API
ENIP Scan	Uses EtherNet/IP broadcast List Identity message to identify PLCs in the network
Hirschmann Discovery Scan	Queries Hirschmann switches using the HiDiscovery protocol. Transmits broadcast level 2 messages
Ping Sweep	Performs a ping sweep across all IPs specified to detect existing assets
Profinet-DCP Scan	Uses the Profinet-DCP broadcast message to detect devices
TCP Port Discovery	IPs based on the specific ports. Will detect all IPs where the specified ports are open
VMware ESX Discovery	Using VMWare Public API to discover VMs running on the specified ESX
SNMP Scan	Uses SNMP to read the ARP cache of devices to generate new assets
WSD Discovery	Uses WSD and ONVIF to find network devices, based on the WSD IoT Matchers

Summary Queries Table

Table 4: Summary Table of Queries

Task Name	Description
B&R Query	Uses proprietary B&R SNMP OIDs to collect information on B&R PLCs
BACnet Query	Query a device using the BACnet protocol
Beckhoff Query	Query using the Beckhoff AMS protocol
CIP Query	Uses CIP to query PLCs for information and scan for nested devices
Cognex Query	Uses Cognex Discovery protocol to find basic information about Cognex devices (usually cameras)
CrowdStrike Query	Retrieves data about a device running CrowdStrike Sensor and uses AppDB to parse OT projects existing on it
CTI Query	Uses the CTI Proprietary protocol to query CTI2500 PLCs
DNP3	Reads the Identity object from the RTU using DNP3 protocol
ENIP Query	Uses EtherNet/IP List Identity message to identify PLCs in the network

Task Name	Description
Hirschmann Discovery Query	Queries Hirschmann switches using the HiDiscovery protocol
HTTP Query	Uses HTTP to get the home page of a device and extract information
Mitsubishi Melsoft Query	Using proprietary Mitsubishi Melsoft protocol to connect to Mitsubishi PLCs
Modbus Information Object	Uses the Modbus protocol Get Information command to query PLCs
MS SQL	Uses TDS and SQL browser protocols to find MS SQL installations
Net Bios	Uses the Windows NetBIOS service to learn the hostname and OS version. Also uses SMBv1
Opto22 Query	Uses the Opto22 protocol to query Opto PAC PLCs
Profinet-DCP Query	Uses the Profinet-DCP broadcast message to detect devices
S7Comm Query	Uses the Siemens S7Comm to query PLCs for information and nested devices
S7CommPlus Query	S7CommPlus is a Siemens proprietary protocol that runs between programmable logic controllers of the Siemens S7-1200/1500 family.
Schneider TSX Query	Uses the PL7 software proprietary protocol to query Schneider TSX devices
Schneider Unity Query	Uses the Schneider Unity Modbus function code 90 to query PLCs
Siprotec Query	Uses the Siprotec protocol to query RTUs
SNMP Query	Uses the SNMP Protocol to query devices for information
SNMP Siprotec 5	Uses SNMP to query the Siprotec5 proprietary OIDs via SNMP
SSH Discovery	Uses SSH to remotely connect and collect data from SSH supporting servers
TBox Query	Ovarro TBox General Info Query
TCP Port Scan	TCP Port scanning
Telnet	Performs a telnet banner grabbing. Extracts info from Scalance, Hirschmann switches
Unitronics Query	Uses the PCOM-TCP protocol to query Unitronics PLCs
WMI Query	Uses WMI to query Windows hosts for information
WSD Query	Uses WSD and ONVIF to find network devices, based on the WSD IoT Matchers

Summary Profiles Table

Table 5: Summary Table of Profiles

Task Name	Description
B&R Profile	Uses proprietary B&R SNMP OIDs to collect information on B&R PLCs

Task Name	Description
Cisco Profile	Uses SNMP
Hirschmann Profile	Basic: Telnet Advanced: Telnet + SNMP
Mitsubishi Profile	Simple: See Mitsubishi Melsoft Query Advanced: See Mitsubishi Melsoft Query
Rockwell Profile	Basic: EtherNet/IP Advanced: CIP Configuration read
Siemens Profile	Basic: S7 Basic Advanced: S7 Configuration read
Siprotec 5 Profile	Basic HTTPS: Uses the Digsi5 HTTPS Protocol Advanced HTTPS: Uses the Digsi5 HTTPS protocol to collect advanced information
Windows Profile	Basic: NetBios Medium: WMI Basic query Advanced: WMI Advanced query

2.5.1.4 Detailed Tables

Detailed Discovery Task Tables

Table 6: BACnet Discovery

Task Name	BACnet Discovery	Task ID: 27
TIV Task Name	BACnet Discovery	
Description	Finds BACnet Devices using a broadcast request	
Port	47808	
Target Devices	Mainly BMS controllers	
Intrusive Level	Low	
Custom Info Fields	■ Object Name ■ Application Software Version ■ Location ■ Description ■ Object Identifier ■ Custom Label	
Sub Query	Generic	
Sub Query Description	Uses BACnet broadcast requests to collect information about devices	

Task Name	BACnet Discovery	Task ID: 27
Potential Information Collected	Firmware, model, application version, object Name, hostname, location, object ID, vendor, IP, description	
Parameters		
Interface name		
Meaning	Network interface on the machine from which the packets are sent	
Format	string	
Default	-	
Example	en192	
Subnet		
Meaning	Subnet on which to broadcast	
Format	CIDR subnet	
Default	-	
Example	192.168.1.0/24	
Use Object ID as Hostname		
Meaning	Should use the BACnet Object ID as the hostname of the target	
Format	Checkbox	
Default	TRUE	
Example	FALSE	
Query Discovered Devices		
Meaning	Should query the discovered devices for more details	
Format	Checkbox	
Default	TRUE	
Example	FALSE	

Table 7: CrowdStrike Discovery

Task Name	CrowdStrike Discovery	Task ID: 53
TIV Task Name	CrowdStrike Discovery	
Description	Retrieves data about a device running CrowdStrike Sensor and uses AppDB to parse OT projects existing on it.	
Port	443 (TCP) - Internet Access	
Target Devices	Windows Hosts	
Intrusive Level	Low	
Custom Info Fields	-	
Sub Queries		
Sub Query	**Generic**	
Sub Query Description	Retrieves data about a device running CrowdStrike Sensor and uses AppDB to parse OT projects existing on it.	
Potential Information Collected	IP, Mac, OS, Hostname, Vendor, Model	
Parameters		
Client ID		
Meaning	CrowdStrike Client ID	
Format	numbers and letters a-f	
Default	-	
Example	f3bac176a05c544492e83aba9cba08fe	
Client Secret		
Meaning	CrowdStrike Client Secret of Client ID	
Format	Numbers and letters	
Default	-	
Example	F5sd3J8f3wer67Plk	
Cloud		
Meaning	CrowdStrike Cloud	
Format	dropdown	
Default	US	
Example	US-2	
IP Range		
Meaning	IP ranges to retrieve from CrowdStrike	

Task Name	CrowdStrike Discovery	Task ID: 53
Format	IP range	
Default	- (not required)	
Example	192.168.1.0/24	
IP Range Exclude		
Meaning	IP ranges not to retrieve from CrowdStrike	
Format	IP range	
Default	- (not required)	
Example	192.168.1.13	
Sensor Tags		
Meaning	CrowdStrike Sensor tags to filter in	
Format	Comma separated words	
Default	- (not required)	
Example	Claroty,SensorGroupingTags/Siemens	

Table 8: ENIP Scan

Task Name	ENIP Scan	Task ID: 12
TIV Task Name	ENIP BroadcastScan	
Description	Uses EtherNet/IP broadcast List Identity message to identify PLCs in the network	
Port	44818	
Target Devices	Rockwell Devices	
Intrusive Level	Low	
Custom Info Fields	Custom Label	
Sub Query	UDP Broadcast	
Sub Query Description	Use the ENIP Identity Request command to collect basic information on ENIP compatible devices	
Potential Information Collected	IP, model, vendor, serial	
Parameters		
Interface Name		
Meaning	Network interface on the machine from which the packets are sent	
Format	string	
Default	-	
Example	en192	
Subnet		
Meaning	Subnet on which to broadcast	
Format	CIDR subnet	
Default	-	
Example	192.168.1.0/24	
Custom Label		
Meaning	Custom Label to add to all assets discovered	
Format	string	
Default	-	
Example	Location:aaa, Process: bbb	

Table 9: Hirschmann Discovery Scan

Task Name	Hirschmann Discovery Scan	Task ID: 9
TIV Task Name	HiDiscoveryScan	
Description	Queries Hirschmann switches using the HiDiscovery protocol. Transmits broadcast level 2 messages	
Port	-	
Target Devices	Hirschmann devices	
Intrusive Level	Low	
Custom Info Fields	Custom Label	
Sub Query	LLC Broadcast	
Sub Query Description	Use the Hirschmann HiDiscovery protocol to query Hirschmann devices (2nd layer)	
Potential Information Collected	model, vendor, IP, MAC, hostname	
Parameters		
Interface name		
Meaning	Network interface on the machine from which the packets are sent	
Format	string	
Default	-	
Example	en192	
Custom label		
Meaning	Custom Label to add to all assets discovered	
Format	string	
Default	-	
Example	Assembly Line 2	

Table 10: Ping Sweep

Task Name	Ping Sweep	Task ID: 7
TIV Task Name	PingSweep	
Description	Performs a ping sweep across all IPs specified to detect existing assets	
Port	-	
Target Devices	All devices that respond to ping (endpoints, PLCs, networking)	
Intrusive Level	High	
Custom Info Fields	Custom Labels	
Sub Query	**Generic**	
Sub Query Description	Send Ping requests to all listed IPs, and determine their existence in the network based on the response	
Potential Information Collected	IPs	
Parameters		
IP Range		
Meaning	Range of IPs to ping	
Format	IP, CIDR or IP range comma separated	
Default	-	
Example	work,192.168.1.0/24	
IP Range exclude		
Meaning	Range of IPs to not ping	
Format	IP, CIDR or IP range comma separated	
Default	-	
Example	10.0.0.1-10.0.0.10, 192.168.1.0/24	
Concurrent scans		
Meaning	Number of packets to send concurrently	
Format	number	
Default	50	
Example	50	
Retransmissions		

Task Name	Ping Sweep	Task ID: 7
Meaning	Number of times to ping an IP if no response was received	
Format	number	
Default	2	
Example	2	
Custom Label		
Meaning	Custom Label to add to all assets discovered	
Format	key:value, key:value...	
Default	-	
Example	Location:aaa, Process: bbb	
Sub Query	Host Name Resolving	
Sub Query Description	Performs a ping as well as a reverse DNS query on the found IPs, to collect hostnames as well	
Potential Information Collected	IP, hostname	
Parameters		
DNS Server		
Meaning	The IP of the DNS Server to query. If empty will use the default server configured to TIV	
Format	IP address	
Default	-	
Example	8.8.8.8	
Domain Name		
Meaning	The Domain name, to strip from the returning names	
Format	string	
Default	-	
Example	company.co	

Table 11: Profinet-DCP Scan

Task Name	Profinet-DCP Scan	Task ID: 14
TIV Task Name	ProfinetScan	
Description	Uses the Profinet-DCP broadcast message to detect devices	
Port	-	
Target Devices	Siemens devices	
Intrusive Level	Low	
Custom Info Fields	Custom Labels	
Sub Query	DCP Broadcast	
Sub Query Description	Use the Profinet-DCP information collection broadcast packet to discover (layer 2) relevant network devices	
Potential Information Collected	IP, model, hostname, vendor, mac	
Parameters		
Interface name		
Meaning	Network interface on the machine from which the packets are sent	
Format	string	
Default	-	
Example	en192	
Custom Label		
Meaning	Custom Label to add to all assets discovered	
Format	string	
Default	-	
Example	Assembly Line 2	
VLAN		
Meaning	VLAN tag number	
Format	300,599,601	
Default	-	
Example	Applicable only via trunk port with native VLAN	

Table 12: TCP Port Discovery

Task Name	TCP Port Discovery	Task ID: 41
TIV Task Name	PortScanDiscovery	
Description	Scans IPs based on the specified ports. Will detect all IPs where the specified ports are open	
Port	22,23,80,102,139,445,502,2222,44818	
Target Devices	All	
Intrusive Level	High	
Custom Info Fields	N/A	
Sub Query	Generic	
Sub Query Description	Discovers assets in the network using the Port Knocking technique on the specified ports	
Potential Information Collected	IPs, open ports (as baselines)	
Parameters		
IP range		
Meaning	IP range to scan	
Format	IP range	
Default	-	
Example	192.168.1.0/24	
ip_range_exclude		
Meaning	IPs not to scan	
Format	IPs	
Default	- (not required)	
Example	192.168.1.13	
tcp_ports		
Meaning	TCP ports to check	
Format	List of numbers	
Default	22,23,80,102,139,445,502,2222,44818	
Example	1234	
concurrent_ports		
Meaning	Maximum number of ports to concurrently scan in a single IP	
Format	number	

Task Name	TCP Port Discovery	Task ID: 41
Default	1	
Example	10	
concurrent_ips		
Meaning	Maximum number of IPs to concurrently scan	
Format	number	
Default	50	
Example	3	

Table 13: VMware ESX Discovery

Task Name	VMware ESX Discovery	Task ID: 42
TIV Task Name	esxScan	
Description	Using VMWare Public API to discover VMs running on the specified ESX	
Port	443	
Target Devices	VMware ESX	
Intrusive Level	Low/Medium	
Custom Info Fields	■ Machine UUID ■ ESX IP	
Sub Query	Generic	
Sub Query Description	Uses the VMWare API protocol to identify the ESX/VSphere server as well as all VMs running on top of it	
Potential Information Collected	For Host: IP, OS For Guests: OS, UUID, hostname, vendor	
Parameters		
IP range		
Meaning	IP range to scan	
Format	IP range	
Default	-	
Example	192.168.1.0/24	
port		
Meaning	port	
Format	number	
Default	443	
Example	443	
username		
Meaning	username	
Format	text	
Default	-	
Example	root	
password		
Meaning	password	

Task Name	VMware ESX Discovery	Task ID: 42
Format	text(number)	
Default	-	
Example	toor	

Table 14: SNMP Scan

Task Name	SNMP Scan	Task ID: 16
TIV Task Name	SNMPArpCacheScan	
Description	Uses SNMP to read the ARP cache of devices to generate new assets	
Port	161	
Target Devices	All devices implementing SNMP (Networking, PLCs)	
Intrusive Level	Medium	
Custom Info Fields	Custom Label	
Sub Queries	**See SNMP Sub queries**	
Sub Query Description	Uses SNMP to collect the ARP table from a network device, to discover all devices connected to it	
Potential Information Collected	Matcher dependent, connected devices	
Parameters	**See SNMP Parameters**	
Custom Label		
Meaning	Custom Label to add to all assets discovered	
Format	key:value, key:value...	
Default	-	
Example	Location:aaa, Process: bbb	

Table 15: WSD Discovery

Task Name	WSD Discovery	Task ID: 37
TIV Task Name	WSD Discovery	
Description	Uses WSD and ONVIF to find network devices, based on the WSD IoT Matchers	
Port	3702	
Target Devices	Network devices	
Intrusive Level	Low	
Custom Info Fields	location	
Sub Query	Generic	
Sub Query Description	Uses the Web Services for Devices (WSD) generic discovery protocol to identify IoT devices	
Potential Information Collected	Matcher Dependent	
Parameters		
Meaning	Port to access	
Format	number	
Default	3702	
Example	1234	

Detailed Query Tables

Table 16: B&R Query

Task Name	B&R Query	Task ID: 30
TIV Task Name	B&R Automation SNMP Query	
Description	Uses proprietary B&R SNMP OIDs to collect information on B&R PLCs	
Ports	-	
Target Devices	B&R PLCs	
Intrusive Level	Low	
Custom Info Fields	■ CF Serial Number ■ Family	
Sub Query	V3	
Sub Query Description	Uses SNMP v3 with proprietary B&R properties	

Task Name	B&R Query	Task ID: 30
Parameters		
Port		
Meaning	Port to access	
Format	number	
Default	161	
Example	1234	

Table 17: BACnet Query

Task Name	BACnet Query	Task ID: 28
TIV Task Name	BACnet Query	
Description	Query a device using the BACnet protocol	
Port	47808	
Target Devices	Mainly BMS controllers	
Intrusive Level	Low	
Custom Info Fields	■ Object Name ■ Application Software Version ■ Location ■ Description ■ Object Identifier	
Sub Query	Generic	
Sub Query Description	Uses BACnet requests to collect information about devices	
Potential Information Collected	Firmware, Model, Application version, Object Name, hostname, Location, Object ID, Vendor, IP, Description	
Parameters		
IP		
Meaning	IP of the target	
Format	IP	
Default	-	
Example	10.0.0.1	
Use Object ID as Hostname		
Meaning	Should use the BACnet Object ID as the hostname of the target	
Format	Checkbox	
Default	TRUE	
Example	FALSE	

Table 18: Beckhoff Query

Task Name	Beckhoff Query	Task ID: 26
TIV Task Name	Beckhoff Query	
Description	Query using the Beckhoff AMS protocol	
Ports	48898, 48899	
Target Devices	Beckhoff Devices	
Intrusive Level	Low	
Custom Info Fields	N/A	
Sub Query	Generic	
Sub Query Description	Uses the Beckhoff AMS protocol to collect information on Beckhoff devices	
Potential Information Collected	IP, hostname, OS, firmware, model, vendor, serial, installed programs, patches	
Parameters		
IP		
Meaning	IP of the target	
Format	IP	
Default	-	
Example	10.0.0.1	

Table 19: CIP Query

Task Name	CIP Query	Task ID: 10
TIV Task Name	CIPQuery	
Description	Uses CIP to query PLCs for information and scan for nested devices	
Port	44818	
Target Devices	Rockwell Devices	
Intrusive Level	Potentially High	
Custom Info Fields	N/A	
Sub Queries: TCP CIP DEEP, TCP CIP CONFIGURATION, TCP CIP HYBRID		
Sub Query	**TCP CIP**	
Sub Query Description	Queries the controller for basic information using the CIP Identity request	
Potential Information Collected	IP, Model, Vendor, Serial, Firmware	
Sub Query	**TCP CIP DEEP**	
Sub Query Description	Queries the controller for information. Also scans for nested devices	
Potential Information Collected	IP, model, vendor, serial, slots, Mac, code sections, nested devices, firmware	
Sub Query	**TCP CIP CONFIGURATION**	
Sub Query Description	Performs Configuration Upload from the controller. Allows gathering information, nested devices, and code sections.	
Potential Information Collected	IP, model, vendor, serial, slots, Mac, code sections, nested devices, firmware	
Sub Query	**TCP CIP HYBRID**	
Sub Query Description	Combines both CIP Configuration upload and CIP Deep sub queries methodology. The sub query first retrieves the queried device configuration and extract all of the slots and nested devices. After retrieval it will initiate a scan of only these devices and get the current information from the devices. This methodology reduces the need to scan wide address ranges to detect slots and nested devices.	
Potential Information Collected	IP, model, vendor, serial, slots, Mac, code sections, nested devices, firmware	
Parameters		
IP		
Meaning	IP of the target	

Task Name	CIP Query	Task ID: 10
Format	IP	
Default	-	
Example	10.0.0.1	
Port		
Meaning	Port to access	
Format	Number	
Default	44818	
Example	1234	
Max inner depth		
Meaning	How deep the nested hierarchy should go	
Format	Number	
Default	1	
Example	3	
Scanning timeout		
Meaning	Timeout for scan responses	
Format	Number (seconds)	
Default	5	
Example	10	
Specific Address		
Meaning	Query specific CIP address	
Format	Card X \ Addr Y	
Default	-	
Example	Card 2 \ Addr 53	
Scanning try best effort		
Meaning	Should try best effort for nested scans	
Format	Bool	
Default	TRUE	
Example	FALSE	
Device network subnet		
Meaning	External subnet of the Rockwell device	

Task Name	CIP Query	Task ID: 10
Format	CIDR subnet	
Default	***If not given, the default is Class C of the **GIVEN IP**	
Example	10.0.0.0/24	

Table 20: Cognex Query

Task Name	Cognex Query	Task ID: 38
TIV Task Name	Cognex Query	
Description	Uses Cognex Discovery protocol to find basic information about Cognex devices (usually cameras)	
Port	1069	
Target Devices	Cameras and related devices	
Intrusive Level	Low	
Custom Info Fields	Description	
Sub Queries		
Sub Query	**Generic**	
Sub Query Description	Uses the Cognex Discovery protocol to identify and collect information from Cognex devices	
Potential Information Collected	IP, hostname, Mac, serial, model, firmware, description	
Parameters		
Port		
Meaning	Port to access	
Format	number	
Default	1069	
Example	51069	

Table 21: CrowdStrike Query

Task Name	CrowdStrike Query	Task ID: 54
TIV Task Name	CrowdStrike Query	
Description	Retrieves data about a device running CrowdStrike Sensor and uses AppDB to parse OT projects existing on it.	
Port	443 (TCP) - Internet Access	
Target Devices	Windows Hosts	
Intrusive Level	Potentially High	
Custom Info Fields	■ -	
Sub Queries		
Sub Query	**Basic**	
Sub Query Description	Retrieves data about a device running CrowdStrike Sensor	
Potential Information Collected	Installed Programs	
Parameters		
Client ID		
Meaning	CrowdStrike Client ID	
Format	numbers and letters a-f	
Default	-	
Example	f3bac176a05c544492e83aba9cba08fe	
Client Secret		
Meaning	CrowdStrike Client Secret of Client ID	
Format	Numbers and letters	
Default	-	
Example	F5sd3J8f3wer67Plk	
Cloud		
Meaning	CrowdStrike Cloud	
Format	dropdown	
Default	US	
Example	US-2	
Sub Query	**Advanced**	
Sub Query Description	Retrieves data about a device running CrowdStrike Sensor and uses AppDB to parse OT projects existing on it.	

Task Name	CrowdStrike Query	Task ID: 54
Potential Information Collected	On CrowdStrike Sensor: Installed Programs On Devices from AppDB Files: IP, Mac, Hostname, Model, Firmware, Slots	
Parameters		
Client ID		
Meaning	CrowdStrike Client ID	
Format	numbers and letters a-f	
Default	-	
Example	f3bac176a05c544492e83aba9cba08fe	
Client Secret		
Meaning	CrowdStrike Client Secret of Client ID	
Format	Numbers and letters	
Default	-	
Example	F5sd3J8f3wer67Plk	
Cloud		
Meaning	CrowdStrike Cloud	
Format	dropdown	
Default	US	
Example	US-2	
Max Recent Files		
Meaning	Max number of AppDB files to retrieve from Recent Files	
Format	number (1-50)	
Default	20	
Example	15	
Should Use Windows Recently Opened Files		
Meaning	Should Use Windows Recently Opened Files (or only from AppDB locations)	
Format	checkbox	
Default	FALSE	
Example	TRUE	
Should Get Project Files From Remote Paths		

Task Name	CrowdStrike Query	Task ID: 54
Meaning	Should Get Project Files From Remote Paths like \\server-pc\files\my_file.acd	
Format	checkbox	
Default	FALSE	
Example	TRUE	

Table 22: CTI Query

Task Name	CTI Query	Task ID: 46
TIV Task Name	CTI Query	
Description	Uses the CTI Proprietary protocol to query CTI2500 PLCs	
Port	1069	
Target Devices	CTI2500 PLCs	
Intrusive Level	Low	
Custom Info Fields	Rack Firmware	
Sub Query	**Generic**	
Sub Query Description	Uses the CTI Proprietary protocol to query CTI2500 PLCs	
Potential Information Collected	IP, Vendor, Family, Model, Firmware, Rack Firmware	
Parameters		
Port		
Meaning	Port to access	
Format	number	
Default	1505	
Example	1000	

Table 23: DNP3 Query

Task Name	DNP3 Query	Task ID: 5
TIV Task Name	DNP3 Query	
Description	Reads the Identity object from the RTU using DNP3 protocol	
Port	20000	
Target Devices	Devices that implement the Identity object within DNP (PLCs, RTUs, IEDs)	
Intrusive Level	Low	
Custom Info Fields	User Assigned Location Device Manufacturer HW version Device Manufacturer SW Version	
Sub Query	Generic	
Sub Query Description	Use the DNP3 Information Object to query devices with this function implemented	
Potential Information Collected	Serial, hostname, model, vendor, HW version, SW version, location	
Parameters		
IP		
Meaning	IP of the target	
Format	IP address	
Default	-	
Example	10.0.0.1	
Port		
Meaning	Port to access	
Format	Number	
Default	20000	
Example	20000	
Protocol		
Meaning	Transmission protocol to use	
Format	TCP or UDP	
Default	TCP	
Example	UDP	
Unit ID		
Meaning	DNP3 unit ID	

Task Name	DNP3 Query	Task ID: 5
Format	Number	
Default	0	
Example	1	

Table 24: EtherNet/IP Query

Task Name	EtherNet/IP Query	Task ID: 11
TIV Task Name	EtherNet/IP Query	
Description	Uses EtherNet/IP List Identity message to identify PLCs in the network	
Port	44818	
Target Devices	Rockwell Devices	
Intrusive Level	Low	
Custom Info Fields	N/A	
Sub Query	UDP Unicast	
Sub Query Description	Use the EtherNet/IP Identity Request command to collect basic information on EtherNet/IP compatible devices	
Potential Information Collected	IP, model, vendor, serial, firmware	
Parameters		
IP		
Meaning	IP of the target	
Format	IP	
Default	-	
Example	10.0.0.1	

Table 25: Hirschmann Discovery Query

Task Name	Hirschmann Discovery Query	Task ID: 8
TIV Task Name	HiDiscoveryQuery	
Description	Queries Hirschmann switches using the HiDiscovery protocol	
Port	-	
Target Devices	Hirschmann devices	
Intrusive Level	Low	
Custom Info Fields	N/A	
Sub Query	Single Device	
Sub Query Description	Use the Hirschmann HiDiscovery protocol to query Hirschmann devices (2nd layer)	
Potential Information Collected	Model, vendor, IP, mac, hostname	
Parameters		
Interface name		
Meaning	Network interface on the machine from which the packets are sent	
Format	String	
Default	-	
Example	en192	
MAC address		
Meaning	MAC address of the target device	
Format	MAC address string	
Default	-	
Example	112233445566	

Table 26: HTTP Query

Task Name	HTTP Query	Task ID: 34
TIV Task Name	HTTP Query	
Description	Uses HTTP to get the home page of a device and extract information	
Port	Depending on registered IoT matchers - 80, 443	
Target Devices	Devices with HTTP Access	
Intrusive Level	Low	
Custom Info Fields	Device dependent	
Sub Queries		
Sub Query	**HTTP**	
Sub Query Description	Uses HTTP to access devices	
Potential Information Collected	Matcher Dependent	
Sub Query	**HTTPS**	
Sub Query Description	Uses HTTPS to access devices	
Potential Information Collected	Matcher Dependent	
Parameters		
Port		
Meaning	Port to access	
Format	number	
Default	161	
Example	1234	

Table 27: Mitsubishi Melsoft Querty

Task Name	Mitsubishi Melsoft Query Task ID: 44
TIV Task Name	Melsoft Query
Description	Using proprietary Mitsubishi Melsoft protocol to connect to Mitsubishi PLCs
Port	5002 (TCP), 5007 (TCP)
Target Devices	Mitsubishi PLCs
Intrusive Level	Low
Sub Query	Simple
Sub Query Description	Requires only parameters and only detects whether the PLC is a Mitsubishi PLC
Potential Information Collected	IP, vendor
Sub Query	Medium
Sub Query Description	Requires most parameters and should extract most relevant data.
Potential Information Collected	IP, vendor, firmware, model, slots
Sub Query	Advanced
Sub Query Description	Adds target system as well, which is relevant for multi-CPU PLCs.
Potential Information Collected	IP, vendor, firmware, model, slots
Parameters	
IP	
Meaning	IP
Format	ips
Default	-
Example	10.1.39.1
plc_side	
Meaning	type of connection in the side of the PLC (ethernet module/cpu/auto select)
Format	dropdown
Default	Ethernet Module
Example	PLC Module
network and station numbers setting method	

Task Name	Mitsubishi Melsoft Query Task ID: 44
Meaning	manually choose values, or automatically choose according to IP (e.g. if ip is 10.1.39.5, network number will be 39, plc station number will be 5)
Format	dropdown
Default	Not Use IP Address
Example	Use IP Address
network number	
Meaning	network number we connect to- this is internal Mitsubishi parameter
Format	number
Default	1
Example	4
pc station number	
Meaning	station number representing the engineering station - this is an internal Mitsubishi parameter
Format	number
Default	1
Example	3
plc station number	
Meaning	station number representing the PLC - this is an internal Mitsubishi parameter
Format	number
Default	1
Example	2
target system	
Meaning	target CPU number, in case of multi-CPU PLC
Format	number
Default	0
Example	1

Table 28: Modbus Information Object

Task Name	Modbus Information Object	Task ID: 15
TIV Task Name	Modbus Query	
Description	Uses the Modbus protocol Get Information command to query PLCs	
Port	502	
Target Devices	Modbus masters - PLCs	
Intrusive Level	Low	
Custom Info Fields	Product Code	
Sub Query	Generic	
Sub Query Description	Use the Modbus Information Object to query devices with this function implemented	
Potential Information Collected	Vendor, product code, model, project name	
Parameters		
IP		
Meaning	IP of the target	
Format	IP address	
Default	-	
Example	10.0.0.1	
Port		
Meaning	Port to access	
Format	Number	
Default	502	
Example	1234	
Unit ID		
Meaning	Modbus Unit ID	
Format	Number list	
Default	0	
Example	0-10,15	
Is a gateway		
Meaning	Determine whether querying a gateway and the PLCs are nested	
Format	Boolean	

Task Name	Modbus Information Object	Task ID: 15
Default	FALSE	
Example	TRUE	

Table 29: MS SQL Query

Task Name	MS SQL Query	Task ID: 52
TIV Task Name	MS SQL Query	
Description	Uses TDS and SQL browser protocols to find MS SQL installations	
Port	1433 (TCP), 1434 (UDP)	
Target Devices	Windows Hosts	
Intrusive Level	Low	
Custom Info Fields		
Sub Query	Generic	
Sub Query Description	Uses TDS and SQL browser protocols to find MS SQL installations	
Potential Information Collected	Installed Programs	

Table 30: Net Bios

Task Name	Net Bios	Task ID: 4
TIV Task Name	NetBiosQuery	
Description	Uses the Windows NetBIOS service to learn the hostname and OS version. Also uses SMBv1	
Ports	137, 138, 445	
Target Devices	Windows devices	
Intrusive Level	Low	
Custom Info Fields	N/A	
Sub Query	Generic	
Sub Query Description	Use the NetBios Protocol to interrogate Windows devices using this basic discovery protocol	
Potential Information Collected	OS, hostname, SMB server version, Mac, IP	
Parameters		
IP		
Meaning	IP of the target	
Format	IP address	
Default	-	
Example	10.0.0.1	
Port		
Meaning	Port to use for SMBv1	
Format	Number	
Default	139	
Example	445	

Table 31: Opto22 Query

Task Name	Opto22 Query	Task ID: 48
TIV Task Name	Opto22 Query	
Description	Uses the Opto22 protocol to query Opto PAC PLCs	
Port	22001 (TCP)	
Target Devices	Opto PAC PLCs	
Intrusive Level	Low	
Custom Info Fields	Device dependent	
Sub Queries		
Sub Query	Basic	
Sub Query Description	Uses the protocol to collect basic information	
Potential Information Collected	Model, Firmware, Loader Revision, Project Information	
Sub Query	Advanced	
Sub Query Description	Uses the protocol to also upload the strategy archive from the device, if exists	
Potential Information Collected	Model, Firmware, Loader Revision, Project Information	
Parameters		
Port		
Meaning	Port to access	
Format	number	
Default	22001	
Example	1234	

Table 32: Profinet-DCP Query

Task Name	Profinet-DCP Query	Task ID: 13
TIV Task Name	ProfinetQuery	
Description	Uses the Profinet-DCP broadcast message to detect devices	
Port	-	
Target Devices	Siemens devices	
Intrusive Level	Low	
Custom Info Fields	N/A	
Sub Query	UDP Unicast	
Sub Query Description	Use the Profinet-DCP information collection packet to discover (layer 2) relevant network devices	
Potential Information Collected	IP, model, hostname, vendor, mac	
Parameters		
Interface name		
Meaning	Network interface on the machine from the packets are sent	
Format	String	
Default	-	
Example	en192	
MAC address		
Meaning	MAC address of the target device	
Format	MAC address string	
Default	-	
Example	112233445566	
VLAN		
Meaning	VLAN tag number	
Format	300,599,601	
Default	-	
Example	Applicable only via trunk port with native VLAN	

Task Name	Profinet-DCP Scan	Task ID: 14
TIV Task Name	ProfinetScan	
Description	Uses the Profinet-DCP broadcast message to detect devices	
Port	-	
Target Devices	Siemens devices	
Intrusive Level	Low	
Custom Info Fields	Custom Labels	
Sub Query	DCP Broadcast	
Sub Query Description	Use the Profinet-DCP information collection broadcast packet to discover (layer 2) relevant network devices	
Potential Information Collected	IP, model, hostname, vendor, mac	
Parameters		
Interface name		
Meaning	Network interface on the machine from which the packets are sent	
Format	string	
Default	-	
Example	en192	
Custom Label		
Meaning	Custom Label to add to all assets discovered	
Format	string	
Default	-	
Example	Assembly Line 2	
VLAN		
Meaning	VLAN tag number	
Format	300,599,601	
Default	-	
Example	Applicable only via trunk port with native VLAN	

Table 33: S7Comm Query

Task Name	S7Comm Query	Task ID: 17
TIV Task Name	S7CommQuery	
Description	Uses the Siemens S7comm to query PLCs for information and nested devices	
Port	102	
Target Devices	Siemens PLCs (S7-300, S7-400 families)	
Intrusive Level	Low	
Custom Info Fields	Order Number (MLFB)	
Sub Queries		
Sub Query	**Basic**	
Sub Query Description	S7Comm reads device information from the controller	
Potential Information Collected	Hostname, vendor, model, firmware, IP, serial, MLFB, mode, slots	
Sub Query	**Advanced**	
Sub Query Description	S7Comm reads configuration from the controller - extracts nested devices and code sections	
Potential Information Collected	Hostname, vendor, model, firmware, IP, serial, MLFB, mode, slots, code sections, nested devices	
Parameters		
IP		
Meaning	IP of the target	
Format	IP	
Default	-	
Example	10.0.0.1	
Password		
Meaning	Login password to the PLC	
Format	String (8 characters or less)	
Default	-	
Example	Password	
CPU slot		
Meaning	Slot in which the CPU is on the rack	
Format	Number	
Default	0	

Task Name	S7Comm Query	Task ID: 17
Example	2	

Table 34: S7CommPlus Query

Task Name	S7CommPlus Query	Task ID: 51
TIV Task Name	S7CommPlus Query	
Description	S7CommPlus is a Siemens proprietary protocol that runs between programmable logic controllers of the Siemens S7-1200/1500 family.	
Port	102 (TCP)	
Target Devices	Siemens S71500 Siemens S71200 Siemens ET-200	
Intrusive Level	Low	
Custom Info Fields	MLFB Variables	
Sub Query	Identify s71200 s71500	
Sub Query Description	Identify - try to identify if 1500/1200	
Potential Information Collected	Model, Firmware, MLFB, Mac, IP, Project Information, Slots	
Parameters		
Password		
Meaning	-	
Format	text	
Default	-	
Example	-	

Table 35: Schneider TSX Query

Task Name	Schneider TSX Query	Task ID: 47
TIV Task Name	Schneider TSX Query	
Description	Uses the PL7 software proprietary protocol to query Schneider TSX devices	
Ports	502 (TCP)	
Target Devices	Schneider TSX	
Intrusive Level	Low	
Custom Info Fields	■ Node Number	
Sub Query	**Generic**	
Sub Query Description	Uses the PL7 software proprietary protocol to query Schneider TSX devices	
Potential Information Collected	IP, Vendor, Family, Model, Firmware, Project name	
Parameters		
Port		
Meaning	The port on which the PLC listens on Modbus connections	
Format	number	
Default	502	
Example	2000	
Network ID		
Meaning	XWay Network ID	
Format	number	
Default	0	
Example	1	
Station IDs		
Meaning	XWay Station IDs to try to communicate with	
Format	List of numbers	
Default	-	
Example	0-1	

Table 36: Schneider Unity Query

Task Name	Schneider Unity Query	Task ID: 29
TIV Task Name	Schneider Unity Query	
Description	Uses the Schneider Unity Modbus function code 90 to query PLCs	
Ports	502 (TCP), 21 (TCP)	
Target Devices	Schneider PLCs	
Intrusive Level	Low	
Custom Info Fields	■ Mode ■ Hardware ID ■ Rack Model	
Sub Queries	Unity Basic, Unity Basic FTP, Unity Advanced	
Sub Query	**Unity Basic**	
Sub Query Description	Uses basic Unity functions to learn information about the PLC	
Potential Information Collected	Model, Family, Firmware, Hardware ID, vendor, Project, Mode, Project path, Last Stop Time (M221)	
Sub Query	**Unity Basic FTP**	
Sub Query Description	Uses basic Unity functions as well as default FTP credentials to learn information about the PLC	
Potential Information Collected	Model, Family, Firmware, Hardware ID, Vendor, Project, Mode, Mac, Project path, Last Stop Time (M221)	
Sub Query	**Unity Advanced**	
Sub Query Description	Uses advanced Unity functions to learn information and configuration about the PLC	
Potential Information Collected	Model, Family, Firmware, Hardware ID, Vendor, Project, Mode, Mac, Code sections, Project path, Last Stop Time (M221)	
Parameters		
Modbus Port		
Meaning	The port on which the PLC listens on Modbus connections	
Format	Number	
Default	502	
Example	502	
FTP Port		
Meaning	The port on which the PLC listens on FTP connections	
Format	number	

Task Name	Schneider Unity Query	Task ID: 29
Default	21	
Example	21	
Unit ID		
Meaning	Modbus Unit ID	
Format	number	
Default	0	
Example	0	

Table 37: Siprotec Query

Task Name	Siprotec Query	Task ID: 6
TIV Task Name	SiprotecQuery	
Description	Uses the Siprotec protocol to query RTUs	
Port	443	
Target Devices	Siprotec 5 relays	
Intrusive Level	Low	
Custom Info Fields	■ Order Number (MLFB) ■ FPGA Version ■ Configuration Version	
Sub Queries	Basic, Advanced	
Sub Query	**Basic**	
Sub Query Description	Uses the DIGSI protocol version 5 to query the controller for basic information	
Potential Information Collected	IP, serial	
Sub Query	**Advanced**	
Sub Query Description	Uses the DIGSI protocol version 5 to query the controller for advanced information	
Potential Information Collected	IP, serial, slots, firmware, configuration version, mac, code sections	
Parameters		
IP		
Meaning	IP of the target	
Format	IP	
Default	-	
Example	10.0.0.1	

Table 38: SNMP Network Layout Query

Task Name	SNMP Network Layout Query	Task ID: 40
TIV Task Name	SNMP Network Layout Query	
Description	Using SNMP and a starting IP, the query recursively gets information about network switches and devices, and gets the entities connected to their interfaces	
Port	161	
Target Devices	Network devices (especially switches)	
Intrusive Level	High	
Custom Info Fields	location	
Sub Queries		
Sub Query	See SNMP Query	
Sub Query Description	See SNMP Query	
Parameters		
SNMP Parameters		
Meaning	See SNMP Query Parameters	
Format	See SNMP Query Parameters	
Default	See SNMP Query Parameters	
Example	See SNMP Query Parameters	
Max Recursion Depth		
Meaning	Maximum recursion depth to reach while querying switches and their neighbors.	
Format	number	
Default	2	
Example	3	
Max Number of Switches		
Meaning	Maximum Number of switches to get their CAM tables and neighbors.	
Format	number	
Default	15	
Example	10	

Table 39: SNMP Query

Task Name	SNMP Query	Task ID: 1
TIV Task Name	SNMPQuery	
Description	Uses the SNMP Protocol to query devices for information	
Port	161	
Target Devices	All devices implementing SNMP (Networking, PLCs, etc.)	
Intrusive Level	Medium	
Custom Info Fields	■ Image ■ Series ■ Hardware Revision ■ Order Number ■ Location ■ Short Module Name	
Sub Queries		
Sub Query	**V1**	
Sub Query Description	Uses SNMP Version 1 to query devices based on the configured SNMP Matchers	
Potential Information Collected	Matcher dependent, connected devices	
Sub Query	**V2c**	
Sub Query Description	Uses SNMP Version 2 to query devices based on the configured SNMP Matchers	
Potential Information Collected	Matcher dependent, connected devices	
Sub Query	**V3**	
Sub Query Description	Uses SNMP Version 3 to query devices based on the configured SNMP Matchers	
Potential Information Collected	Matcher dependent, connected devices	
Parameters		
Sub query		
Meaning	SNMP version	
Format	Dropdown list	
Default	-	
Example	v1, v2, v3...	
IP		

Task Name	SNMP Query	Task ID: 1
Meaning	IP of the target	
Format	IP	
Default	-	
Example	10.0.0.1	
Community (for v1, v2)		
Meaning	Community string for connection	
Format	string	
Default	-	
Example	public	
username (for v3)		
Meaning	Username for login	
Format	string	
Default	-	
Example	administrator	
auth proto		
Meaning	Authentication protocol	
Format	Dropdown list	
Default	Md5	
Example	sha224	
priv_proto		
Meaning	Encryption method	
Format	Dropdown list	
Default	des	
Example	aes128	
auth_key		
Meaning	Authentication key	
Format	String	
Default	-	
Example	password	
priv_key		

Task Name	SNMP Query	Task ID: 1
Meaning	Private key for authentication	
Format	Private key	
Default	-	
Example		
get_arp		
Meaning	Should read ARP table to learn net assets	
Format	Bool	
Default	FALSE	
Example	TRUE	
get_cam		
Meaning	Should read CAM table to learn net assets	
Format	Bool	
Default	FALSE	
Example	TRUE	
get_comms		
Meaning	Should generate baselines in the system for CDP, TCP connections	
Format	Bool	
Default	TRUE	
Example	FALSE	

Table 40: SNMP Siprotec 5 Query

Task Name	SNMP Siprotec 5 Query	Task ID: 32
TIV Task Name	Siemens Siprotec5 SNMP Query	
Description	Uses SNMP to query the Siprotec5 proprietary OIDs via SNMP	
Port	See SNMP	
Target Devices	Siprotec 5 relays	
Intrusive Level	Low	
Custom Info Fields	N/A	
Sub Query	**V3**	
Sub Query Description	Uses SNMP v3 with built-in credentials in Siprotec 5	
Parameters		
Port		
Meaning	Port to access	
Format	number	
Default	161	
Example	1234	
get_arp		
Meaning	Should read ARP table to learn net assets	
Format	Boolean	
Default	FALSE	
Example	TRUE	
get_cam		
Meaning	Should read CAM table to learn net assets	
Format	Boolean	
Default	FALSE	
Example	TRUE	

Table 41: SSH Discovery

Task Name	SSH Discovery	Task ID: 43
TIV Task Name	SSHQuery	
Description	Uses SSH to remotely connect and collect data from SSH supporting servers.	
Port	22	
Target Devices	SSH Servers	
Intrusive Level	Low	
Custom Info Fields	Kemel SSH Server Daemon	
Sub Query	Generic	
Sub Query Description	Uses the SSH protocol to connect to relevant hosts and run several commands to attempt to collect information	
Potential Information Collected	OS, kernel version, hostname, vendor, serial model	
Parameters		
username		
Meaning	username	
Format	text	
Default	-	
Example	myuser	
password		
Meaning	password	
Format	text	
Default	-	
Example	mypassword	
port		
Meaning	port	
Format	number	
Default	22	
Example	22	

Table 42: TBox Query

Task Name	TBox Query	Task ID: 50
TIV Task Name	TBox Query	
Description	Ovarro TBox General Info Query	
Port	502 (TCP)	
Target Devices	Ovarro TBox	
Intrusive Level	Low	
Custom Info Fields	-	
Sub Query	Generic	
Sub Query Description	Login with default credentials to provide basic info	
Potential Information Collected	Hostname, Firmware, IP, Module, Project Information	
Parameters		
Port		
Meaning	Port to access	
Format	number	
Default	502	
Example	501	

Table 43: TCP Port Scan

Task Name	TCP Port Scan	Task ID: 20
TIV Task Name	PortScanQuery	
Description	TCP Port Scanning	
Port	-	
Target Devices	All	
Intrusive Level	Medium	
Custom Info Fields	N/A	
Sub Query	Generic	
Sub Query Description	Uses TCP to attempt connection to all specified ports to detect whether those ports are in "listen" mode	
Potential Information Collected	Open ports (as baselines), IPs	
Parameters		
IP		
Meaning	IP of the target	
Format	IP address	
Default	-	
Example	10.0.0.1	
Tcp_ports		
Meaning	Ports to scan	
Format	Comma separated ports	
Default	22,23,80,102,139,445,502,2222,44818	
Example	123456678	

Table 44: Telnet

Task Name	Telnet	Task ID: 3
TIV Task Name	Telnet	
Description	Performs a telnet banner grabbing. Extracts info from Scalance, Hirschmann switches	
Port	23	
Target Devices	Scalance switches, Hirschmann switches	
Intrusive Level	Low	
Custom Info Fields	N/A	
Sub Query	Generic	
Sub Query Description	Use the Telnet protocol to perform "banner grabbing" by connecting to the Telnet service and identifying the returned banner	
Potential Information Collected	Matcher dependent	
Parameters		
IP		
Meaning	IP of the target	
Format	IP	
Default	-	
Example	10.0.0.1	

Table 45: Unitronix Query

Task Name	Unitronix Query	Task ID: 49
TIV Task Name	Unitronix Query	
Description	Uses the PCOM-TCP protocol to query Unitronics PLCs	
Port	20256 (TCP)	
Target Devices	Unitronix PLCs	
Intrusive Level	Low	
Custom Info Fields	Hardware Revision	
Sub Query	Generic	
Sub Query Description	Uses the PCOM protocol to query Unitronics devices	
Potential Information Collected	IP, Vendor, Model, Firmware, Hostname	
Parameters		
Port		
Meaning	Port to access	
Format	number	
Default	20256	
Example	2000	

Table 46: WinRM Query

Task Name	WinRM Query	Task ID: 39
TIV Task Name	WinRM Query	
Description	Uses WinRM protocol to query information about Windows computers, using WMI and registry. Uses SOAP over HTTP and must be configured	
Port	5985(HTTP)/5986(HTTPS)	
Target Devices	Windows machines	
Intrusive Level	High	
Custom Info Fields	Description	
Sub Queries		
Sub Query	Basic	
Sub Query Description	Uses WinRM to collect basic information about the host	
Potential Information Collected	IP, hostname, OS, Windows serial, Windows edition, model, serial, Mac, installed programs	
Sub Query	Advanced	
Sub Query Description	Uses WMI to collect information about the host, including installed software and security patches	
Potential Information Collected	IP, hostname, OS, Windows serial, Windows edition, model, serial, Mac, installed programs, patches, USB connected devices	
Parameters		
Username		
Meaning	username	
Format	string	
Default	-	
Example	myuser	
Password		
Meaning	password	
Format	string	
Default	-	
Example	mypassword	
Domain		
Meaning	domain (if in a domain)	

Task Name	WinRM Query	Task ID: 39
Format	string	
Default	- (not required)	
Example	mydomain	
Service		
Meaning	service - HTTP or HTTPS	
Format	string out of enum	
Default	HTTP	
Example	HTTP	

Table 47: WMI Query

Task Name	WMI Query	Task ID: 19
TIV Task Name	WMIQuery	
Description	Uses WMI to query Windows hosts for information	
Port	135	
Target Devices	Windows Hosts	
Intrusive Level	Medium	
Custom Info Fields	■ Windows Serial Number ■ Windows Edition ■ Windows Domain ■ Logged On User ■ Last Program Installed Date	
Sub Queries		
Sub Query	**Basic**	
Sub Query Description	Use WMI to collect basic information about the host	
Potential Information Collected	IP, hostname, OS, Windows serial, Windows edition, model, serial, Mac, installed programs	
Sub Query	**Advanced**	
Sub Query Description	Uses WMI to collect information about the host, including installed software and security patches	
Potential Information Collected	IP, hostname, OS, Windows serial, Windows edition, model, serial, Mac, installed programs, patches, USB connected devices	
Parameters		
IP		
Meaning	IP of the target	
Format	IP	
Default	-	
Example	10.0.0.1	
Username		
Meaning	Username for the Windows login	
Format	String	
Default	-	
Example	Administrator	

Task Name	WMI Query	Task ID: 19
Password		
Meaning	Password for the username	
Format	String	
Default	-	
Example	Password1	
Domain		
Meaning	Domain for the login	
Format	String	
Default	-	
Example	domain01	

Table 48: WSD Query

Task Name	WSD Query	Task ID: 35
TIV Task Name	WSD Query	
Description	Uses WSD and ONVIF to query network devices, based on the WSD IoT Matchers	
Port	3702	
Target Devices	Network devices	
Intrusive Level	Low	
Custom Info Fields	location	
Sub Queries		
Sub Query	**Generic**	
Sub Query Description	Uses the Web Services for Devices (WSD) generic discovery protocol to identify IoT devices	
Potential Information Collected	Matcher Dependent	
Parameters		
Port		
Meaning	Port to access	
Format	number	
Default	3702	
Example	1234	

Detailed Profile Tables

Table 49: B&R Profile

Task Name	B&R Profile	Task ID: 31
TIV Task Name	B&R Profile	
Description	Uses proprietary B&R SNMP OIDs to collect information on B&R PLCs	
Port	-	
Target Devices	B&R PLCs	
Intrusive Level	Low	
Custom Info Fields	■ CF Serial Number ■ Family	
Sub Query	V3	

Task Name	B&R Profile	Task ID: 31
Sub Query Description	Uses SNMP v3 with proprietary B&R properties	
Parameters		
Port		
Meaning	Port to access	
Format	number	
Default	161	
Example	1234	

Table 50: Cisco Profile

Task Name	Cisco Profile	Task ID: 25
TIV Task Name	Cisco Profile	
Description	Uses SNMP	
Port	See SNMP	
Target Devices	Cisco Devices	
Intrusive Level	Low	
Custom Info Fields	See *SNMP*	
Sub Query	**SNMP versions**	
Sub Query Description	Use the *SNMP* protocol to query Cisco devices	
Parameters		
See SNMP		

Table 51: IoT Query

Task Name	IoT Query	Task ID: 36
TIV Task Name	IoT Query	
Description	Uses the IoT matchers configured in the system to discover IoT devices	
Port	Depending on matchers	
Target Devices	IoT	
Intrusive Level	Medium	
Custom Info Fields	Device dependent	
Sub Query	Generic	
Sub Query Description	Uses all IoT directed queries - banner, WSD, HTTP, HTTPS, SNMP	

Table 52: Hirschmann Profile

Task Name	Hirschmann Profile	Task ID: 21
TIV Task Name	Hirschmann Profile	
Description	Basic: Telnet Advanced: Telnet + SNMP	
Port	See Telnet, SNMP	
Target Devices	Hirschmann	
Intrusive Level	Low	
Custom Info Fields	*See SNMP, Telnet*	
Sub Queries		
Sub Query	**Basic**	
Sub Query Description	Uses the Telnet query to collect information	
Parameters		
See SNMP, Telnet		
Sub Query	**Advanced**	
Sub Query Description	Uses Telnet and SNMP to collect information	
Parameters		
See SNMP, Telnet		

Table 53: Mitsubishi Profile

Task Name	Mitsubishi Profile	Task ID: 45
TIV Task Name	Mitsubishi Profile	
Description	See Mitsubishi Melsoft Query	
Port	5002, 5007	
Target Devices	Mitsubishi PLCs	
Intrusive Level	Low	
Sub Query	Simple	
Sub Query Description	See Mitsubishi Melsoft Query	
Sub Query	Advanced	
Sub Query Description	See Mitsubishi Melsoft Query	
Parameters		
IP		
Meaning	IP	
Format	ips	
Default	-	
Example	10.1.39.1	
Ports		
Meaning	ports	
Format	list of numbers	
Default	5002, 5007	
Example	5005	
plc_side		
Meaning	type of connection in the side of the PLC (ethernet module/cpu)	
Format	dropdown	
Default	Ethernet Module	
Example	PLC Module	

Task Name	Mitsubishi Profile	Task ID: 45
network number		
Meaning	network number we connect to - this is internal Mitsubishi parameter	
Format	number	
Default	1	
Example	4	
pc station number		
Meaning	station number representing the engineering station - this is an internal Mitsubishi parameter	
Format	number	
Default	1	
Example	3	
plc station number		
Meaning	station number representing the PLC - this is an internal Mitsubishi parameter	
Format	number	
Default	0	
Example	1	
target system		
Meaning	target CPU number, in case of multi-CPU PLC	
Format	number	
Default	0	
Example	1	

Table 54: Rockwell Profile

Task Name	Rockwell Profile	Task ID: 24
TIV Task Name	Rockwell Profile	
Description	Basic: *EtherNet/IP* Advanced: CIP Configuration read	
Port	See ENIP, CIP	
Target Devices	Rockwell Devices	
Intrusive Level	Potentially High	
Custom Info Fields	*See EtherNet/IP, CIP*	
Sub Queries		
Sub Query	**Basic**	
Sub Query Description	Uses the IP Query	
Sub Query	**Advanced**	
Sub Query Description	Uses the *TCP CIP HYBRID* Query	
Parameters		
See EtherNet/IP, CIP		

Table 55: Siemens Profile

Task Name	Siemens Profile	Task ID: 23
TIV Task Name	Siemens Profile	
Description	Basic: S7 Basic Advanced: S7 Configuration read	
Port	See S7	
Target Devices	Siemens Devices	
Intrusive Level	Low	
Custom Info Fields	See *S7Comm Query*	
Sub Queries		
Sub Query	**Basic**	
Sub Query Description	Uses the S7Comm Basic Query	
Sub Query	**Advanced**	
Sub Query Description	Uses the S7Comm Advanced Query	
Sub Query	**Advanced + SNMP**	
Sub Query Description	Uses the S7Comm Advanced Query as well as SNMP (to also collect communication information)	
Parameters		
See S7Comm Query		

Table 56: Siprotec 5 Profile

Task Name	Siprotec 5 Profile	Task ID: 33
TIV Task Name	Siemens Siprotec 5 Profile	
Description	■ SNMP: Uses the Siprotec 5 SNMP Query ■ Basic HTTPS: Uses the Digsi5 HTTPS Protocol ■ Advanced HTTPS: Uses the Digsi5 HTTPS protocol to collect advanced information	
Port	See SNMP	
Target Devices	Siprotec 5 relays	
Intrusive Level	Low	
Custom Info Fields	See relevant queries	
Sub Queries	SNMP, Basic HTTPS, Advanced HTTPS	
Sub Query	**SNMP**	
Sub Query Description	Uses the Siprotec 5 SNMP Query	
Sub Query	**Basic HTTPS**	
Sub Query Description	Uses the basic HTTPS Digsi5 (i.e. Siprotec5) Query	
Sub Query	**Advanced HTTPS**	
Sub Query Description	Uses the advanced HTTPS Digsi5 (i.e. Siprotec5) Query	
Parameters		
See Siprotec 5 SNMP Query		

Table 57: Windows Profile

Task Name	Windows Profile	Task ID: 22
TIV Task Name	Windows Profile	
Description	Basic: NetBios	
Port	See NetBios, WMI	
Target Devices	Windows Hosts	
Intrusive Level	Medium	
Custom Info Fields	*See NetBios, WMI*	
Sub Queries		
Sub Query	**Basic**	
Sub Query Description	Uses the *NetBios Query*	
Sub Query	**Medium**	
Sub Query Description	Uses the *WMI Basic Query*	
Sub Query	**Advanced**	
Sub Query Description	Uses the WMI Advanced Query	
Sub Query	Advanced WinRM	
Sub Query Description	Uses the WinRM Advanced Query	
Parameters		
See NetBios, WMI		

2.5.2 IoT Asset Management and Monitoring

2.5.2.1 IoT Matchers Configuration

TIV provides out-of-the-box predefined IoT matchers able to detect various types of IoT devices, such as IP phones, printers, and cameras.

IoT matchers are code sections, written in JSON format, that describe how to address IoT devices using HTTP or Telnet communication protocols. They also describe how the response received from the device should be interpreted to understand what the device is and what its attributes are. These IoT matchers work with passive collection as well.

These predefined matchers unlike user defined custom matchers, cannot be edited or deleted. They can only be disabled. Custom matcher's rules can also be disabled to stop their activity and enabled later if needed.

To create your own custom IoT matchers, follow these steps:

1. Navigate to the IoT Matchers configuration tab under **Configuration** > **Data Sources** > **IoT Matchers.**

2. Click **Add** to open the Create New Matcher popup:

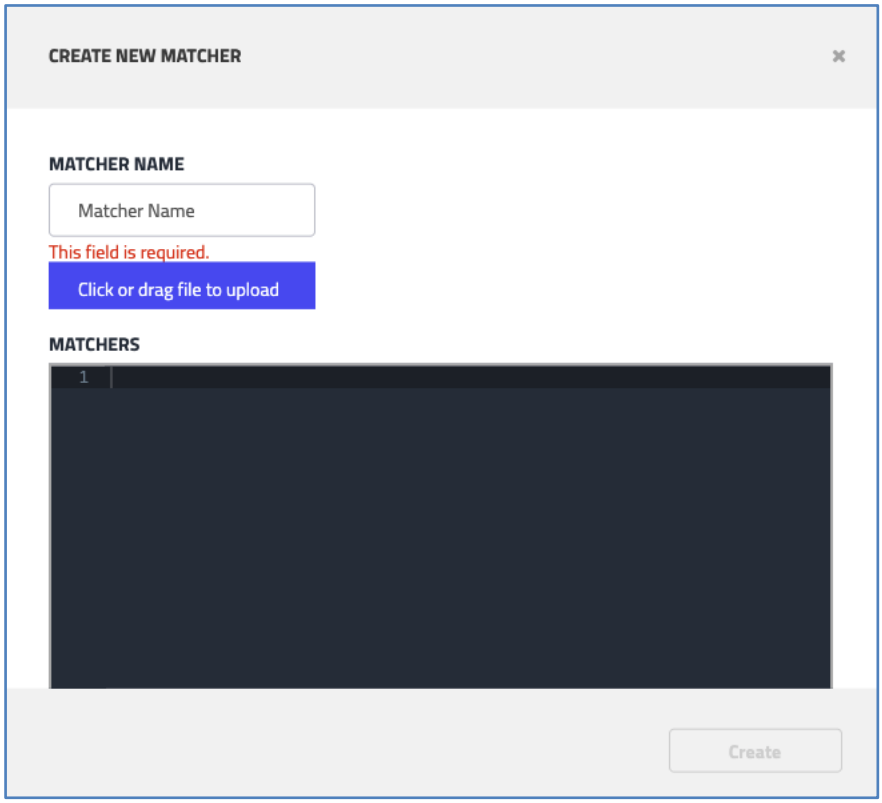


Figure 16 IoT - Create New Matcher popup

3. Type in a name for the matcher

4. Upload a matcher file (any text file in a JSON format) either by selecting a file on your computer or by dragging it directly into the box.

5. Edit the file as needed and click **Create**.

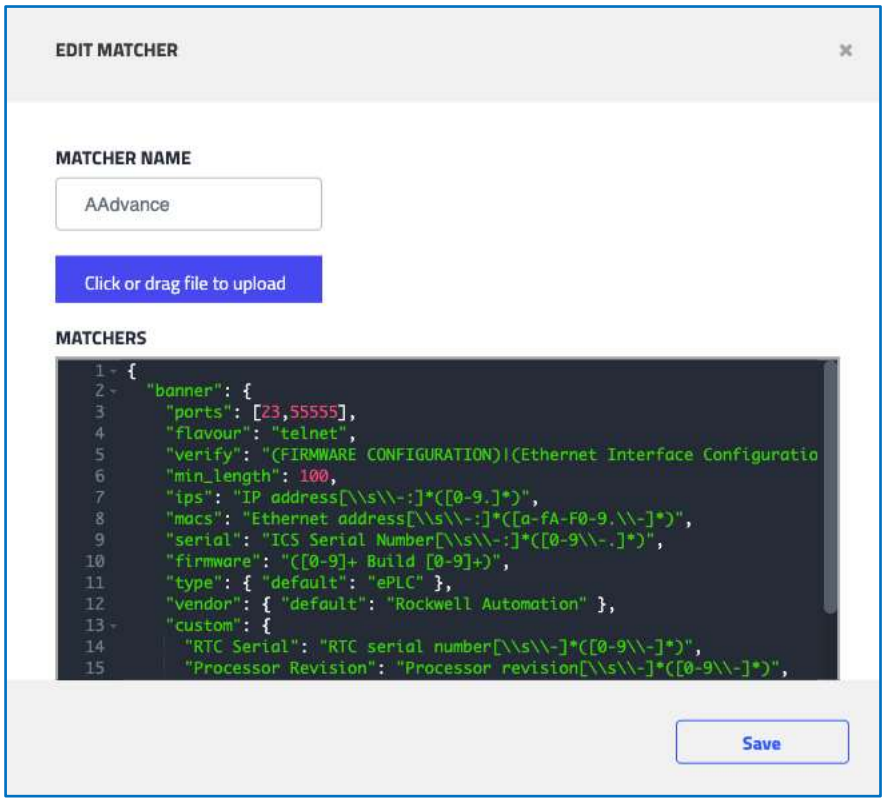


Figure 17 Edit Matcher dialog

The file, which can be uploaded to TIV or edited within the console, contains parameters used for the collection of information, such as:

- The ports, if they differ from the default (such as http:80)
- A "verify" statement, to make sure the accessed page is the one requested, and for which the parsers can actually work, for example, looking for a vendor's name like "Rockwell Automation" in the HTTP page header.

A set of parsers are used to grab asset information from the device to be able to classify the IoT device, such as:

```
"vendor": { "default": "Rockwell Automation" },
"model": "<td>Device Name</td>\\s+<td>(\\S+)</td>\\s+",
"serial": "<td>Serial Number</td>\\s+<td>(\\S+)</td>\\s+",
"firmware": "<td>Product Revision</td>\\s+<td>([\\S ]+)</td>\\s+",
```

Tripwire recommends that Admins review the existing, predefined system IoT matchers to understand how the parsers are defined, before trying to create your own.

List of available information keywords

{KEYWORD} → Information type (Case sensitive!)

- module/model → Model
- firmware → Firmware version
- hostname → Hostname
- serial → Serial number
- vendor → Vendor
- type → Asset type (needs to be the asset type as appears in TIV, with “e” before - “ePLC”, “eCamera”, “eEngineeringStation” etc.)
- family → Family
- description → Description

Links

- Vendor OIDs list:

https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

- SNMP Walk for Windows (Not tested):

https://www.softpedia.com/get/Network-Tools/Misc-Networking-Tools/SnmpWalk.shtml

IoT Matcher Examples

The following is an example of an IoT Matcher in JSON format. You can modify the relevant fields from the example in order to obtain the expected results.

```
{
  "banner": { // Matcher type – could be “http”, “banner”, etc.
  "ports": 23, // Matcher ports – has a default value (80 for HTTP etc.)
  "flavour": "telnet", // Flavour – to specify sub type of the matcher (“telnet” for banner, “http”/”https” for http)
  "verify": "Copyright \\(c\\) [0-9\\-]* Hirschmann Automation and Control", // this field is a regex that must appear in the response, to make sure we have the correct device
  "hostname": "System Name[ ]*:[ ]*(.*?)[\\n\\r]", // Now follows a list of available information values – the name and then the regex to exract it from the response
  "macs": "Base-MAC[ ]*:[ ]*([a-fA-F0-9\\:]*)", // “macs” is for MAC address extraction
  "ips": "Mgmt-IP[ ]*:[ ]*([0-9\\.]*)", // “ips” is for IP address extraction
  "firmware": "Railswitch Rugged Release[ ]*L2P\\-(.*?)\n", // “firmware” is for the Firmware Version
  "vendor": { "default": "Hirschmann" } // “vendor” is to get the vendor. The use of “default” here means there is no regex – that’s a hardcoded vendor, regardless of the contents of the response
  }
```

SNMP

```
{
 "snmp": {                                          # Matcher Type
  "verify": {                                       # How we can identify that the matcher is relevant
   "oid": 1234,                                     # By vendor specific OID
   "description": "^Integrated PrintNet Enterprise" # By RegEx on the description string
  },
  "description_regexes": {                          # Details we can extract from the description string
   "regexes": [
    "Version (?P<firmware>[0-9.]*)"                 # For example - RegEx getting the firmware
   ]
  },
  "info_oids": {                                    # More OIDs that contain interesting information
   "model": ".1.3.6.1.2.1.25.3.2.1.3.1",            # The model lies in the OID
   "vendor": {"default" : "Printronix" },           # Default hardcoded value - in this case, vendor
   "type": {"default": "ePrinter" }                 # Default hardcoded value - in this case, asset type
  }
 }
}
```

HTTP

```
{
 "http": {                                          # Matcher Type
  "verify": "<(?:TITLE)>Rockwell</(?:TITLE)>",      # RegEx on the "/" page - identify matcher is relevant
  "min_length": 100,                                # Minimum length of the "/" page
  "pages": {                                        # List of pages to check
   "home.asp": {                                    # Page URL
    "verify": "\\<(?:TITLE|title)\\>Rockwell Automation\\</(?:TITLE|title)\\>.*<(?:TD|td)>Device
Name</(?:TD|td)>",                                  # RegEx on the page - identify matcher is relevant
    "vendor": { "default": "Rockwell Automation" }, # Default hardcoded value - in this case, vendor
    "model": "<(?:TD|td)>Device Name</(?:TD|td)>\\s+<(?:TD|td)>(\\S+)</(?:TD|td)>\\s+",
                                                    # RegEx to run on the page to get the Model
    "serial": "<(?:TD|td)>Serial Number</(?:TD|td)>\\s+<(?:TD|td)>(\\S+)</(?:TD|td)>\\s+",
                                                    # RegEx to run on the page to get the Serial
    "firmware": "<(?:TD|td)>Product Revision</(?:TD|td)>\\s+<(?:TD|td)>([\\S ]+?)</(?:TD|td)>\\s+",
                                                    # RegEx to run on the page to get the Firmwae
    "ips": "<(?:TD|td)>IP Address</(?:TD|td)>\\s+<(?:TD|td)>(\\S+)</(?:TD|td)>\\s+",
                                                    # RegEx to run on the page to get the IP list
    "macs": "<(?:TD|td)>Ethernet Address \\(MAC\\)</(?:TD|td)>\\s+<(?:TD|td)>(\\S+)</(?:TD|td)>\\s+",
                                                    # RegEx to run on the page to get the Mac list
    "type": { "default": "eOT" }                    # Default hardcoded value - in this case, asset type
   }
```

Banner

```
{
 "banner": {                                        # Matcher Type
  "ports": 23,                                      # Port on which the banner is accessible
  "flavour": "telnet",                              # Type of protocol - telnet
  "verify": "Omni Flow Computers       Modbus Mux", # RegEx the banner to assure relvevance
  "min_length": 100,                                # Min length of banner to assure relevance
  "macs": "MAC:[ \t]*([0-9a-zA-Z\\-]*)",            # RegEx on the banner to get macs
  "firmware": "Omni Firmware Vers:  ([a-z0-9\\.]*)",# RegEx on the banner to get firmware
  "vendor": {"default": "Omniflow"},                # Hardcoded value for this banner - vendor
  "model": {"default": "OmniFlow computer"},        # Hardcoded value for this banner - Model
  "type": {"default": "ePLC"},                      # Hardcoded value for this banner - type
  "custom": {
   "SWVersion": "Modbus Mux[ \t]*?v([0-9\\.]*) \\|" # Regex for custom information - SWVersion
  }
 }
}
```

WSD

```
{
  "wsd": {                                                    # Matcher Type
   "verify": "http://www[.]onvif[.]org.*\"http://schemas[.]xmlsoap[.]org/ws/[0-9]{4}/[0-9]{2}/discovery\"",
                                                              # Regex in the response to verify relevance
   "is_onvif": { "default": "True" },                         # Type of WSD request - ONVIF
   "onvif_types": "onvif://www[.]onvif[.]org/type/([^ <]+)",  # RegEx to extract ONVIF types
   "model": ["onvif://www[.]onvif[.]org/model/([^ <]+)", "onvif://www[.]onvif[.]org/hardware/([^ <]+)"],
                                                              # RegEx to extract Model
   "hostname": "onvif://www[.]onvif[.]org/name/([^ <]+)",     # RegEx to extract hostname
   "firmware": "onvif://www[.]onvif[.]org/firmware/([^ <]+)", # RegEx to extract firmware
   "custom": {
     "Location": "onvif://www[.]onvif[.]org/location/([^ <]+)"  # Regex for custom information - Location
    }
  }
}
```

IoT Active Query Configuration

For the IoT matchers to work using TIV active detection, you should first define the required active query for IoT matching.

To configure an IoT active query:

1. Navigate to the Active Detection query configuration tab under **Configuration** > **Data Sources** > **Active Detection** > **Queries tab.**
2. Click **Create New** to open the **New Query** popup:

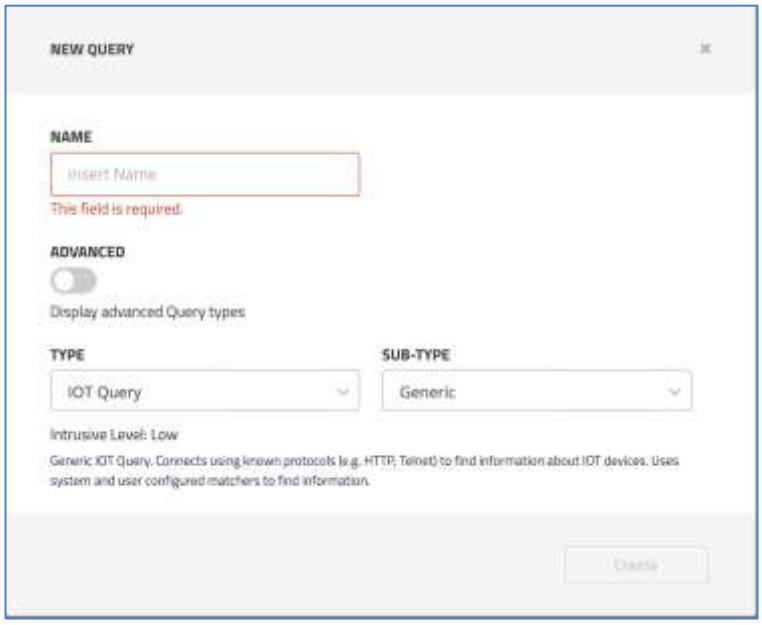


Figure 18 IoT - New Query popup

3. Provide a name for the query, and in **Query Type** dropdown menu, select "**IoT Query**"
4. Choose a Sub-Type

5. Enable the Recurring Task toggle button.
6. Choose the start and expire date.
7. Choose Run Every (hour, day, or week).
8. Choose the Time Frame (From and the To time).
9. Click **Create**.

IoT Active Task Configuration

After defining the IoT query, continue to create the active task to define the IP addresses or segments to apply the query to.

To configure active tasks:

1. Navigate to the Active Detection query configuration tab under **Settings > Extended Discovery** > **Active Detection** > **Tasks**
2. Click Add New Task to open the New Task popup:

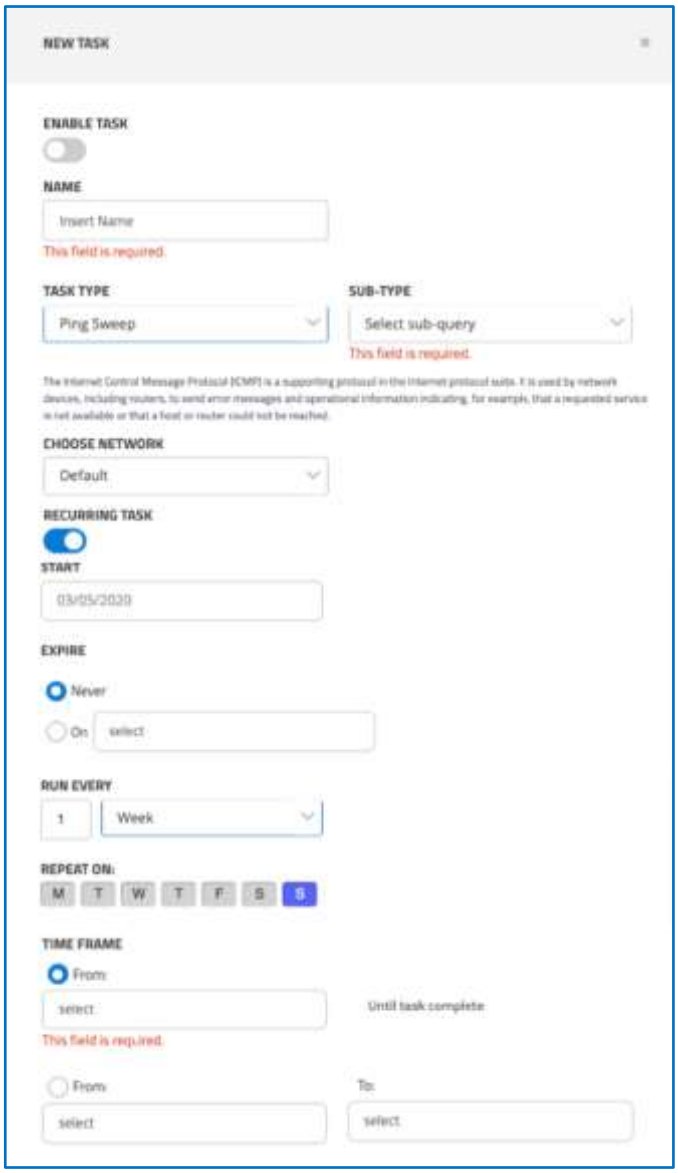


Figure 19 IoT - New Task popup

3. Provide a name for the task and select your desired Task **Type in the** dropdown menu.
4. Choose the network from the dropdown menu.
5. Enable the Recurring Task toggle button.
6. Choose the start and expire date.
7. Choose Run Every (hour, day, or week).
8. Choose the Time Frame (From and the To time).
9. Click **Create**.

IoT Discovery Task and Classification

IoT Matchers can be treated as signatures matched against the information obtained from the IoT asset. They can detect the device type, the OS, and the version. The information can be obtained using Active Task and Query, or passively by listening to traffic sent from/to the IoT asset that discloses the required asset information.

To configure IoT Matchers using Active Task and Query, follow these steps:

1. Configure IoT Active Query
2. Configure Active task(s)
3. Configure IoT Matchers
4. For more information about Active Detection capabilities and configuration, refer to the **TIV User Guide**.

2.5.2.2 IoT Assets Information

For IoT Assets, the type of information and level of detail depend on several factors:

- The techniques used to obtain the information – Passive or Active
  - With Passive, the amount and type of traffic transmitted on the network determines what information is available for TIV to process
  - With Active, the availability of the relevant HTTP pages and their information
- The quality and level of detail of the IoT matchers

In the following example, a Vending Machine was classified, and its Virtual Zone, Risk Level, Type, Criticality, and Class were obtained:

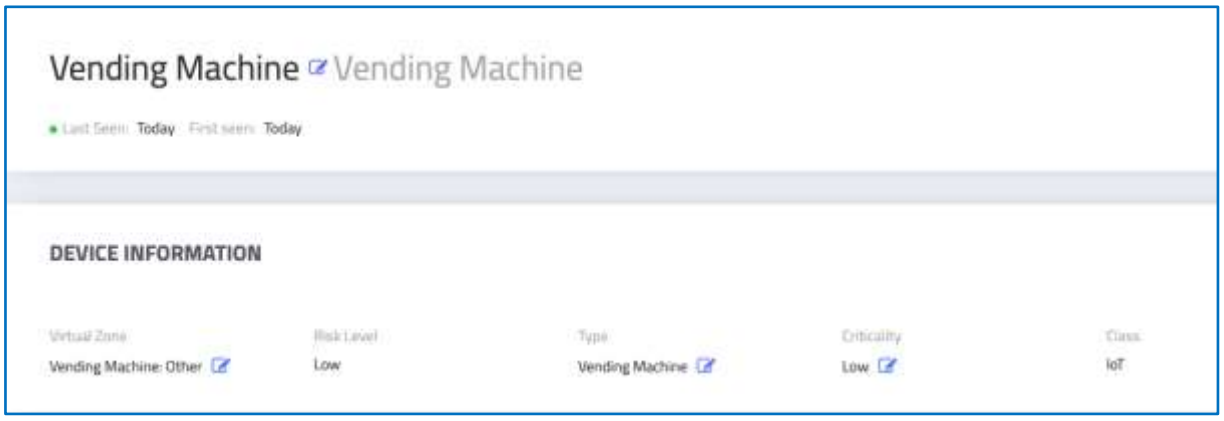


Figure 20 Asset View - IoT Example

2.5.3 Configuring Application Database (App DB) Sources

2.5.3.1 Setting up the Application Database

Follow the procedure of one-time parsing or recurring parsing of configuration projects files to set up the Application Database. There is an option to manually select a file and parse it immediately.

To set up the Application Database:

1. Click **Settings**  **> Data Sources > App DB**:

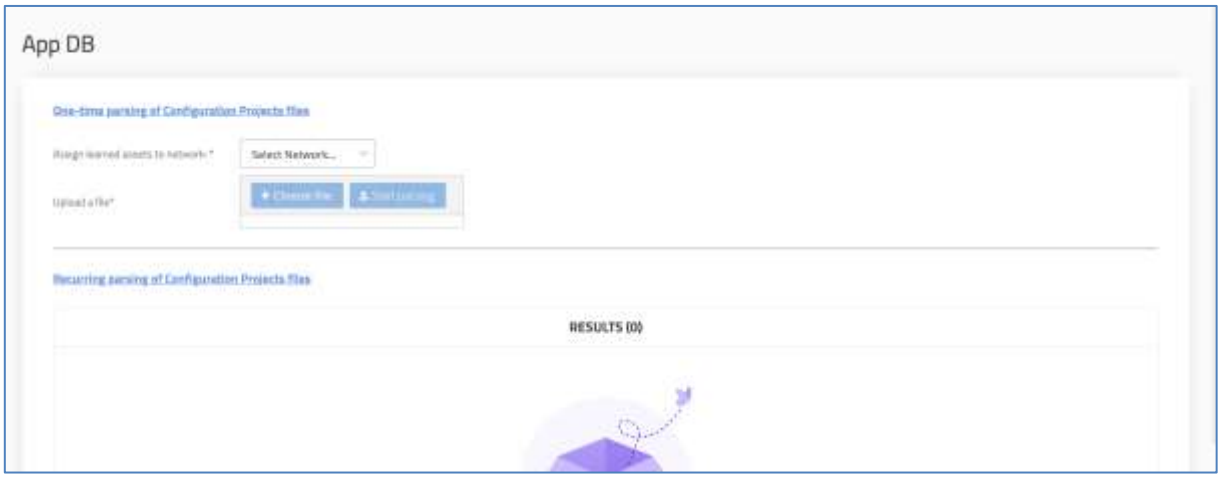


Figure 21 App DB - Configuring Asset Sources

App DB: One Time Parsing

To configure one-time parsing:

1. Navigate to the One-time parsing area:

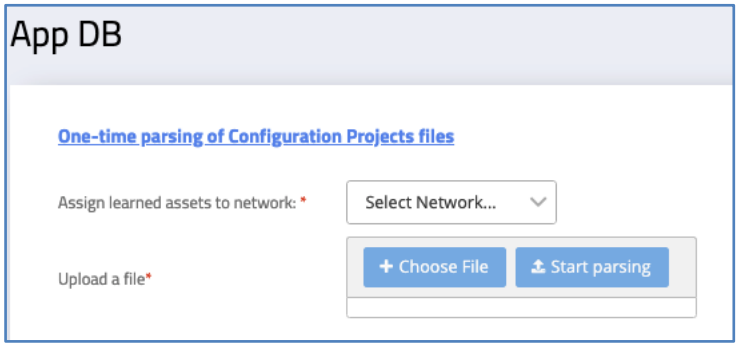


Figure 22 App DB One Time Parsing - Select Network

2. From the dropdown, 'Assign learned assets to network', select the network:

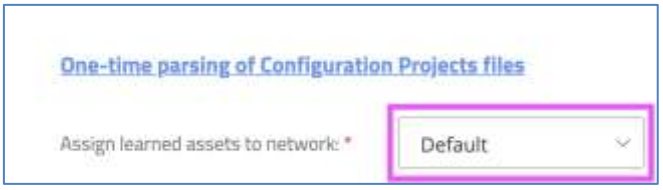


Figure 23 Choose the Network

3. Click **Choose file** to browse the relevant files;repeat this step as needed:

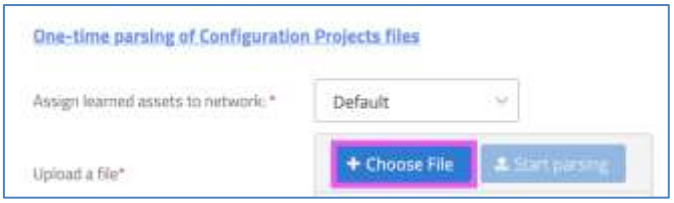


Figure 24 Choose the file/s to parse

- The system displays the filename/s of the uploaded files, including their sizes.

4. Click Start Parsing.

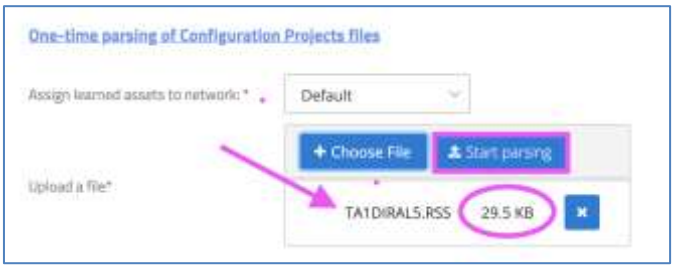


Figure 25 Start Parsing

- The system displays the status of the files on the bottom of the **One-time parsing** area:

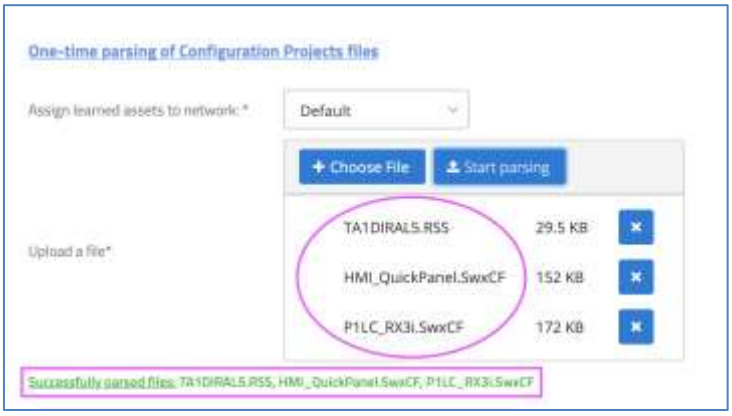


Figure 26 System displays the status of file parsing process

5. Navigate to the **Visibility** > **Assets.** Then show the Parsed Assets column in the table by clicking the **More** ⋮ menu in the tool bar, selecting **Select Columns**, and selecting the **Parsed Asset** item from the Select Columns list.

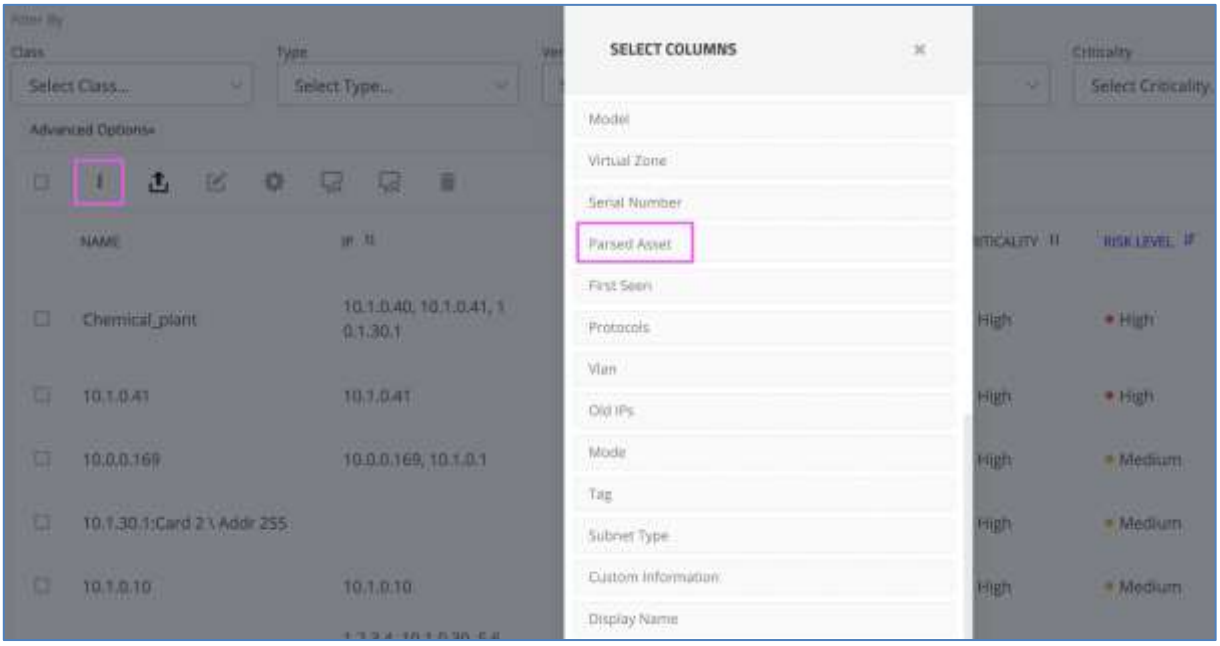


Figure 27 Selecting the Parsed Assets column for the Assets View

App DB: Recurring Parsing

To configure recurring parsing:

1. Navigate to the Recurring Parsing area of **Settings** ⚙ > **Data Sources** > **App DB.**

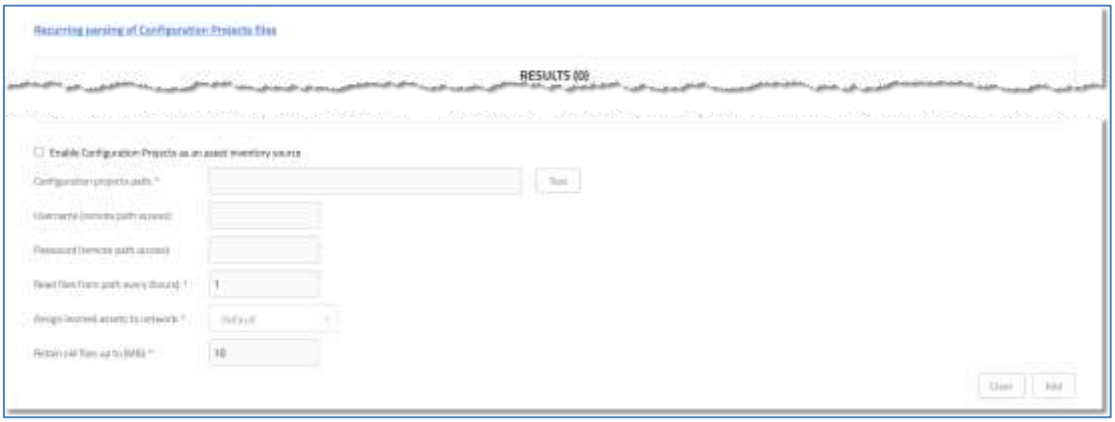


Figure 28 Recurring Parsing

2. Provide the **Configuration Projects path.** After you type a valid path, the **Test** Test button becomes enabled.

This input is mandatory. This can be either a local path on the TIV Server or a Share on a remote Windows machine. Use the Fully Qualified Domain Name (FQDN) format to specify the share (for example \\1.1.1.1\share).

For the local path:

- You must provide permissions for the lkpo user for this path/folder.
- The folder should be above and outside of the "root" folder, and the folder's ownership should be given to user 'lkpo'.
- The set of commands needed to run a viable folder is as follows:

```
cd /
mkdir <local folder name>
sudo chown -R lkpo /<local folder name>/
```

3. **Username** – If the share is protected with an account, enter the username.
4. **Password** – If the share is protected with an account, enter the password.
5. Provide the **Interval** (in hours). The **Read files from path every (hours)** determines how often the system checks for new configuration projects. This input is mandatory. The default is 1 hour.
   - The set interval enables users to control the overhead on the system and balance it with the speed at which it parses the configuration projects. As soon as these assets are parsed, the system onboards the assets and logs the activity.
6. Select the **Network** from **Assign learned assets to network** in which the onboarded assets will be assigned. This input is mandatory. It defaults to the default network.
7. **Retain Old Files** (in MB). Set the limit in MB for the maximum space for retaining old files.
   After the parsing process is done and all relevant data has been extracted from the configuration file, the file is moved automatically to an Old folder.
8. Click the **Test** button Test to test if the **Configuration Projects path** you provided to the configuration projects (in Step 2) is to a valid folder on the machine and that both read and write permissions were given.
   - If the path test passes successfully, a check appears as shown:

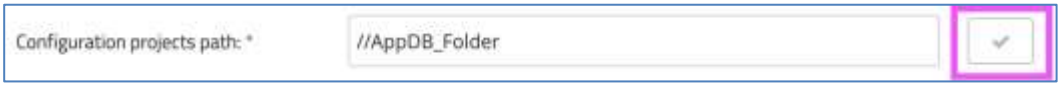


Figure 29 Configuration Path - Test Passed

2.5.3.2 Supported App DB Tools

Currently the following tools are supported by the App DB, listed alphabetically. Tripwire will provide instructions for the exact file type and process used in order to obtain the file. This information is available upon request.

Table 58: App DB Tools Supported

Vendor	Family	Tool
ABB		Composer
ABB	Advant	
ABB	Totalflow	PCCU
B&R	-	Automation Studio v3 /v4
Emerson	DeltaV	Exploring DeltaV
GE	Bently Nevada	3500 System Configuration
GE	MarkVI	ToolBoxST
GE	rx3i,9030	PacsAnalyzer
GE	rx3i,9030	Proficy Machine Edition
Generic	-	-
Generic	-	SCL=Substation Configuration File
Honeywell	EHPM	
Honeywell	Experion	Ctools
Honeywell	Experion	SIT
Mitsubishi	Melsoft (R)	GX Works3
Mitsubishi Hitachi Power Systems (MHPS)	DIASYS Netmation	DIASYS Netmation
Motorola	ACE, MOSCAD	ACE3600 System Suite Tools 17.50
Omron	Generic	CX-One
Red Lion	Redlion HMIs	Crimson 3.0/3.1
Rockwell	*	ISaGRAF (multiple)
Rockwell	*	RSLinx
Rockwell	AAdvance	AADvance Log Collection Tool
Rockwell	FactoryTalkView / RSView	FactoryTalkSE/FactoryTalk ME

Vendor	Family	Tool
Rockwell	ICSTriplex	ICSTriplex Log Collection Tool
Rockwell	MicroLogix	Factory View
Rockwell	MicroLogix	RS System Ferret
Rockwell	MicroLogix	RSLogix 5
Rockwell	MicroLogix	RSLogix 500
Rockwell	MicroLogix	RSLogix 5000
Schneider	Concept	Concept
Schneider	GP-3000 GP-4000 SP-5000 LT-3000 LT-4000 ST3000 IPC (PC/AT)	GP-Pro EX
Schneider	M221	SoMachine
Schneider	Modicon, Quantum	Unity L/XL
Schneider	SCADAPack 32	Telepace Studio
Schneider	TSX Micro, Premium	PL7
Schneider	Twido	TwidoSuite
SEL	SEL	AcSELerator
Siemens	-	Proneta
Siemens	LOGO!Soft	LOGO!Soft Comfort
Siemens	PCS7	PCS7
Siemens	S7	TiaPortal (v13, 14,15,16)
Siemens	S7/T3000	Step7
Siemens	Simatic	Softshop 505
Siemens	Siprotec	Digsi4
Siemens	Siprotec	Digsi5
Triconex	Tricon/Trident/TriGP	TriStation 1131
Xinje	Xinje PLCs	XDPPro
Yokogawa	CentumVP/CS3000	
Yokogawa	CentumVP/CS3000	CentumVP

Vendor	Family	Tool
Yokogawa	Prosafe	ProsafeRS

2.5.4 Importing Assets via CSV

2.5.4.1 Prerequisites

- Only users with admin rights working on a Site can use the Import Asset feature.
- Select a site. If you are working in the EMC, select a target site before proceeding:

Figure 30 Selecting a site

Recommendations

- Tripwire recommends the following when importing assets via CSV:
  - Asset properties not compliant with section 2.5.4.4 are skipped. These assets will appear in a pop-up that will present the assets and the reasons why they failed.
  - For example: For an IP or MAC value, when the entry is not a valid address with the required format, it is ignored.
    - IP address format – `nnn.nnn.nnn.nnn` (such as, 91.6.191.10)
    - MAC address format – `xx:xx:xx:xx:xx:xx` (such as, 00:50:56:A0:E7:64)
- Instead of building the CSV file from scratch, download your existing asset list, from the Assets Page, to minimize input errors. Then, modify the CSV file.

Figure 31 Default Columns on the Assets page

Asset Id	Site Id	Is Ghost	Name	IP	Mac	Class	Type	Criticality	Risk Level	Vendor	Network
4	1	FALSE	00:D7:8F:A7:	-	00:D7:8F:A7:	IT	Networking	Medium	Low	Cisco	Default
5	1	FALSE	00:50:56:8D:	-	00:50:56:8D:	IT	Endpoint	Low	Low	VMware	Default
6	1	FALSE	Windows7	-	00:50:56:B8:(	IT	Endpoint	Low	Low	VMware	Default
9	1	FALSE	10.10.9.185	10.10.9.185	00:50:56:B8:(	IT	Endpoint	Low	Low	VMware	Default
11	1	FALSE	10.10.7.20	10.10.7.20	40:8D:5C:D5:	IT	Endpoint	Low	Low	Giga Byte Tec	Default
13	1	FALSE	10.10.7.65	10.10.7.65	00:50:56:B8:(	IT	Endpoint	Low	Low	VMware	Default
18	1	FALSE	10.10.254.25	10.10.254.25	64:D1:54:37:	IT	Endpoint	Low	Low	Routerboard	Default
20	1	FALSE	LAPTOP-T5O(	10.10.7.30	3C:E1:A1:4E:(	IT	Endpoint	Low	Low	Universa	Default

Figure 32 CSV File with Default Columns highlighted in Red; system added columns 'Asset ID', 'Site ID', 'Is Ghost' in Blue

2.5.4.2 Exporting Assets to CSV

1. Before performing the **Download** assets operation, set up the **Assets View** with the relevant columns and display them in the desired order.

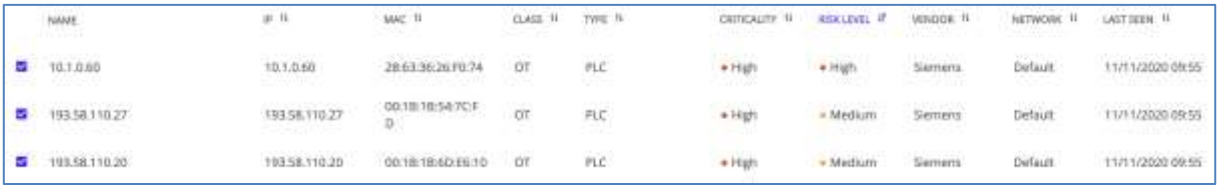


Figure 33 Setting up the Assets View Page with the Relevant Parameters

2. Press **More** ⋮ > **Download** to export your existing assets from the **Assets Page.**

   - Choose the CSV format.
   - Only choose the Rack Slots and/or **Nested Devices** options when you intend to modify them.

> **Note** If you choose Nested Devices, ensure you include the Address parameter in the Assets Page display before downloading (it is not a default parameter).

   - The resulting file will contain your current assets inside a file with the valid CSV structure.
   - Pressing **Download** will download selected assets or filtered assets. If you select assets, it shows only the selection from the partial filtered list. If you don't select assets, it downloads all the assets in the specific applied filter.

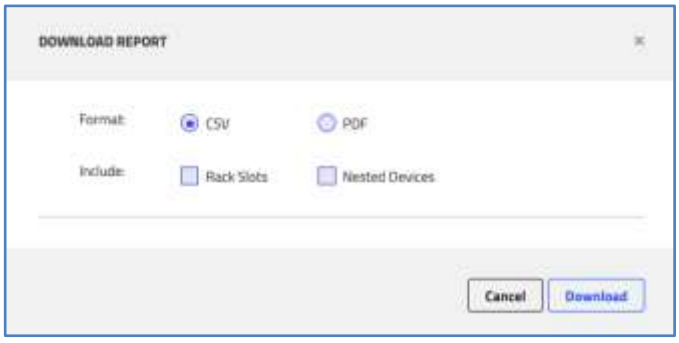
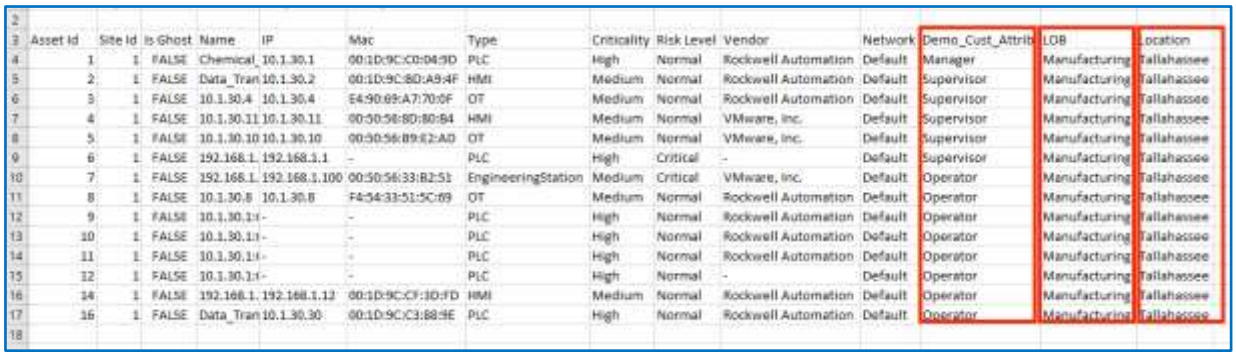


Figure 34 Download Report window



Asset Id	Site Id	Is Ghost	Name	IP	Mac	Type	Criticality	Risk Level	Vendor	Network	Demo_Cust_Attrib	LOB	Location
1	1	FALSE	Chemical_	10.1.30.1	00:1D:9C:C0:D4:9D	PLC	High	Normal	Rockwell Automation	Default	Manager	Manufacturing	Tallahassee
2	1	FALSE	Data_Tran	10.1.30.2	00:1D:9C:8D:A9:4F	HMI	Medium	Normal	Rockwell Automation	Default	Supervisor	Manufacturing	Tallahassee
3	1	FALSE	10.1.30.4	10.1.30.4	E4:90:69:A7:70:0F	OT	Medium	Normal	Rockwell Automation	Default	Supervisor	Manufacturing	Tallahassee
4	1	FALSE	10.1.30.11	10.1.30.11	00:50:56:8D:80:B4	HMI	Medium	Normal	VMware, Inc.	Default	Supervisor	Manufacturing	Tallahassee
5	1	FALSE	10.1.30.10	10.1.30.10	00:50:56:89:E2:AD	OT	Medium	Normal	VMware, Inc.	Default	Supervisor	Manufacturing	Tallahassee
6	1	FALSE	192.168.1.	192.168.1.1	-	PLC	High	Critical	-	Default	Supervisor	Manufacturing	Tallahassee
7	1	FALSE	192.168.1.	192.168.1.100	00:50:56:33:B2:51	EngineeringStation	Medium	Critical	VMware, Inc.	Default	Operator	Manufacturing	Tallahassee
8	1	FALSE	10.1.30.8	10.1.30.8	F4:54:33:51:5C:69	OT	Medium	Normal	Rockwell Automation	Default	Operator	Manufacturing	Tallahassee
9	1	FALSE	10.1.30.1:(	-	-	PLC	High	Normal	Rockwell Automation	Default	Operator	Manufacturing	Tallahassee
10	1	FALSE	10.1.30.1:(	-	-	PLC	High	Normal	Rockwell Automation	Default	Operator	Manufacturing	Tallahassee
11	1	FALSE	10.1.30.1:(	-	-	PLC	High	Normal	Rockwell Automation	Default	Operator	Manufacturing	Tallahassee
12	1	FALSE	10.1.30.1:(	-	-	PLC	High	Normal	-	Default	Operator	Manufacturing	Tallahassee
14	1	FALSE	192.168.1.	192.168.1.12	00:1D:9C:CF:3D:FD	HMI	Medium	Normal	Rockwell Automation	Default	Operator	Manufacturing	Tallahassee
16	1	FALSE	Data_Tran	10.1.30.30	00:1D:9C:C3:88:9E	PLC	High	Normal	Rockwell Automation	Default	Operator	Manufacturing	Tallahassee

Figure 35 Example of Exported Assets with Custom Attributes

3. Open and modify the exported CSV file while retaining the existing structure.
   - Be careful to only modify the parameters that you need to change
   - Beware that a change you make in the CSV file will only be applied if the input conditions are met as per **Parameter Details**.

2.5.4.3 Importing Assets

To import assets:

1. Press the **Import Assets** button.
2. Press **Choose File** to browse and select the modified CSV file:

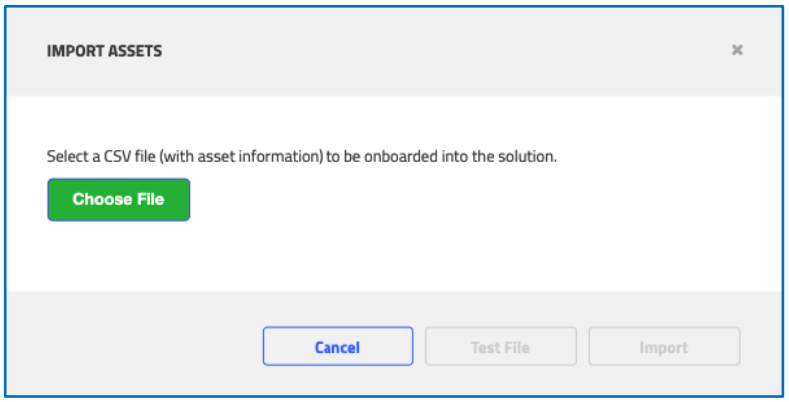


Figure 36 Selecting CSV file to import

3. Choose the **Test File** button to check the validity of your CSV file.
4. Check the Test Summary output to determine the success of the **Import Assets** operation.

- This response tells you how many assets will be imported successfully; how many are expected to fail; and the reasons for any failures.

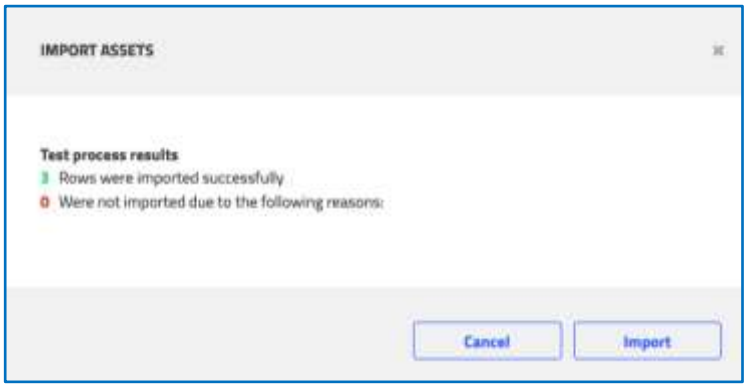


Figure 37 Sample of Successful Test Summary Results

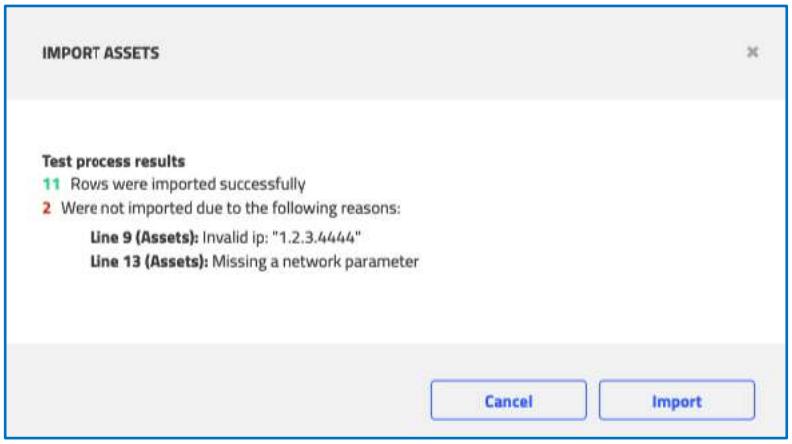


Figure 38 Samples of Test Summary Results with Errors

> Note: Tripwire recommends that users use the Test feature to determine the success of your CSV file.
> The Import operation displays the results in the same manner as with the 'Test' feature.

5. If necessary, modify your CSV input file according to the Summary output and repeat the Test step.
6. After you are satisfied with the test summary results, press the **Import** button to implement your changes.

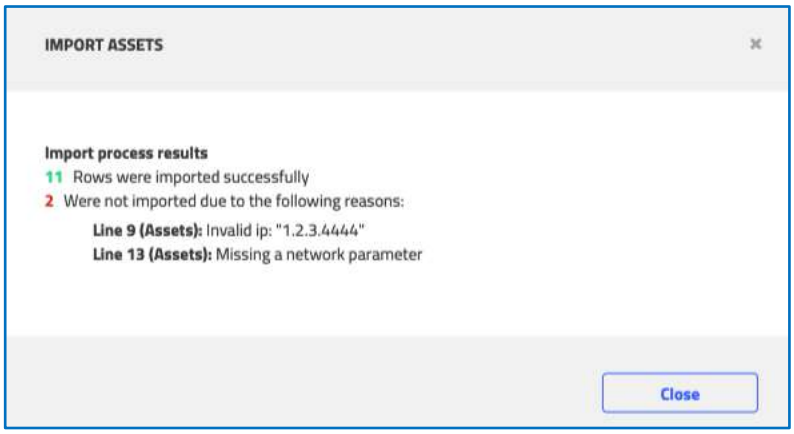


Figure 39 Sample Import Summary Result

For more details on the Summary Results, see section 2.5.4.6.

> **Note** If the system is in Operational mode when the CSV file is imported, it is possible that New Asset alerts or Information Change alerts will be displayed.
> The alerts raised will need to be approved; until these approvals are done, the system will not honor the new values.

2.5.4.4 Table & Guidelines for Structuring the CSV Import File

Table 59: CSV Import Table: Parameter Details

Parameter Name	Parameter Description	Type	Parameter Details	Example/*Notes*
PARAMETERS WHOSE VALUES CAN BE MODIFIED				
Name	The asset name	Text		10.91.6.91 *See notes:* *Name/Display Name*
Display Name	The display name for the asset	Text		10.91.6.91 *See notes:* *Name/Display Name*
Criticality	A value representing the relative criticality of this asset to the overall operation	List	Low Medium High	Low *See notes:* *Type/Criticality*
Type	The asset type	List	*See Appendix C*	Endpoint *See notes:* *Type/Criticality*
Custom Attributes	Any user defined custom attributes	List	As configured by Admin and defined by user	LOB *See notes:* *Custom Attributes*
OS	The Operating System for this asset	List		*See section 3.3*
Virtual Zone	The name of the assigned virtual zone	Text		PLC: Rockwell *See notes:* *Custom Attributes*
Network	The network assigned to this asset The name of a network in the system (or Default).	Text	Default or named network	Default *See notes:* *Network*
Vendor	The equipment vendor of the asset	Text		Rockwell Automation
PARAMETERS WHOSE VALUES SHOULD NOT BE CHANGED				

Parameter Name	Parameter Description	Type	Parameter Details	Example/*Notes*
Asset ID	The internal ID assigned to the asset by the system	Numeric		28 *See notes:* *Asset ID*
Site ID	The ID of the current site	Numeric		1 *See notes:* *Site ID*
NETWORK PROPERTIES WHOSE VALUES SHOULD NOT BE CHANGED: Additional values can be added for these properties (except for VLAN)				
IP	The asset's IP address	Text		91.6.91.10 *See notes:* *IP/MAC addresses*
MAC	The asset's MAC address	Text		00:50:56:A0:E7:64 *See notes:* *IP/MAC addresses*
Address	The asset's gateway address	Text		001B8EE0049F:Card 1 \ Addr 727
VLAN*	The number for the VLAN	Numeric		N/A * NOTE: No additional values for VLAN are possible.
DEFAULT PARAMETERS These parameters can be modified, but preference is given to the information obtained from sniffing/active query/etc.				
Firmware	The firmware version for this asset	Text		Chemical_plant *See notes:* *Firmware*
Model	The hardware model	Text		1756-ENBT/A *See notes:* *Model*

PARAMETERS THAT CANNOT BE CHANGED VIA CSV IMPORT Any changes to these parameters will be ignored		
Active Queries	Queries used to actively monitor the system and discover assets	Not supported
Class	Whether the asset is a security (IT) or an ICS (IOT) type device or an Internet of Things (IoT) device	Not supported

PARAMETERS THAT CANNOT BE CHANGED VIA CSV IMPORT Any changes to these parameters will be ignored		
Custom Information	Custom information for this asset	Not supported
First Seen	The first date and time this asset was seen in the communication in the network	Not supported
Host Name	The name of the host	Not supported
Last Seen	The last date and time this asset was seen in the communication in the network	Not supported
Mode	Whether this asset is in training mode or not	Not supported
Old IPs	List of previous identified IPs for this asset	Not supported
Parsed Asset	Whether this asset was identified by sniffing the network or from parsing a configuration file (Yes/No)	Not supported
Protocols	The list of protocols that the asset uses for communication	Not supported
Purdue Level	The level in the Purdue model.	Not supported
Risk Level	The risk level assigned to this asset; How often the asset generates alerts, and the severity of these alerts	Not supported
Serial Number	The serial number of this asset	Not supported
Site	The name of the TIV Site	Not supported

> Note The asset can only be overridden by the Admin.

2.5.4.5 CSV Import Guidelines

The system enables input of CSV files that comply with the following conventions.

- The values in the table are not case sensitive.
  - However, on free text fields, the UI will display the exact parameter names and capitalization.
- Empty fields will be ignored by the system, whether they are any of the following:
  - Blank
  - A dash (-)
  - 'N/A'
- Max Length of text fields – 256 characters

Name/Display Name

- These fields are interdependent:
  - Name – The asset name, which may contain additional information such as "ghost" or "external". The names are case sensitive.
  - Display **Name** – Tripwire recommends changing this parameter instead of changing the **Name** parameter. When you change the **Display Name**, it changes the **Name** automatically without effecting any additional attributes (like ghost, external). The **Display Name** is case sensitive.

Type and Criticality

- Changing these values in the imported CSV file will have the same effect as changing these fields from the UI. The new value will be kept unless you change it again.
  - **Type** – The specific type of asset; includes IoT types in addition to IT and OT ones. The system derives the **Class** based on the Asset Type.

Default Parameters (for example, Firmware version):

- The system gives preference to the information it can obtain from the sniffing or from an active query. The system will only take the information from the

imported CSV file for these default values when it cannot get the information from any other source.

- If an asset's **Firmware** is changed through the Import CSV, when the system sniffs this asset again in Operational mode, if it conflicts with the data supplied via the CSV, it will raise an **Asset Information Change** alert.

Mandatory Parameters

- Network
  - **Network** is always a mandatory **column**
    - Note there may be only one network.
  - When only the Default network exists, the network column should be present, and labelled 'Default'.
    - An entry without a network value will result in an error.
  - When a new network is added, the Administrator must associate assets to it.
  - When parsing an asset from one network to another, the system will duplicate it and not move it between the networks.
- Key Parameters - **Asset ID** and **Site ID**:
  - Asset ID and Site ID are used to uniquely identify the asset for the CSV.
  - Rack **Slots** and **Nested Devices** use these keys to correlate information.

Multiple IP/MAC addresses

- Multiple IP **and** multiple MAC addresses are supported in a limited manner:

> Note The tool is not intended for editing multiple IPs and MACs simultaneously. A common consequence of this is merging assets unintentionally.

- Adding new assets with multiple IP and MAC addresses simultaneously is supported as follows:
  - Multiple IPs work with a single MAC
  - A single IP with Multiple MACs works
  - A combination of a new asset with both. It will only consider the newly added IPs
  - Editing assets with multiple IP and MAC addresses simultaneously is supported as follows:
    - All the information should be added **only** to the first IP address
    - The first MAC address is taken when no IP address previously exists
    - When there is no MAC address, it gets added to the asset by its Asset ID
  - If a user makes a mistake in the Import CSV, delete the specific asset/s via the UI and import it/them again.

Operating System

You can choose from the list of supported Operating Systems.

Custom Attributes

Custom Attributes are supported (refer to the **TIV User Guide** for details)

Virtual Zones

- If a virtual zone already exists for an asset being imported via CSV, the zone is editable.
  - New assets can be added to the existing zones.
  - Assets can be moved between zones.
- You cannot **create** a virtual zone via the CSV.
- There should not be a Virtual Zone column in the CSV when importing assets for a new site or when you want to import new assets without assigning them to a pre-existing zones.

Model

If an asset's **Model** number is changed through the Import CSV, when the system sniffs this asset again in Operational mode, if it conflicts with the data from the CSV, it will raise an **Asset Information Change** alert.

Hostname

The **Hostname** is not editable, even if it is from a new asset.

Ghost Assets

Ghost Assets cannot be imported via CSV.

2.5.4.6 Summary Results

The CSV Asset Import is successful when the system correctly updates existing assets and/or imports new assets. See the following for several common error messages.

> Note: 'Success' means the system added these assets to the queue for processing.

The Summary Results pop-up displays the amount of assets successfully onboarded and the amount of assets that failed, with the relevant failure message.

> Note: TIV can import an asset that has no data other than its network. In this case, it is imported as '**Asset#** '.

Table 60: Common Error Messages for CSV Import

Message	Meaning/Resolution/Notes
Network <network name> does not exist	The network name in the CSV file is not configured in the TIV as a valid network and cannot be used.
Network <network name> does not exist	The selected CSV file is empty
Invalid CSV structure	Please use the same structure of the asset CSV report; See section 2.5.4.4, *Guidelines for Structuring the CSV Import File*
Internal errors while processing asset details	Check that the CSV file meets the guidelines for structuring the file.

3 Specifications

3.1 System Boundaries

3.1.1 Data Collection Boundaries Status (only Admin)

The data collection boundaries status shows the boundaries of collecting assets and baselines in the following colors:

- Green – system is collecting assets/baselines.
- Red – system stopped collecting assets/baselines.

To see the data collection boundaries status:

- Click **Settings**  **> System Health Dashboard.**

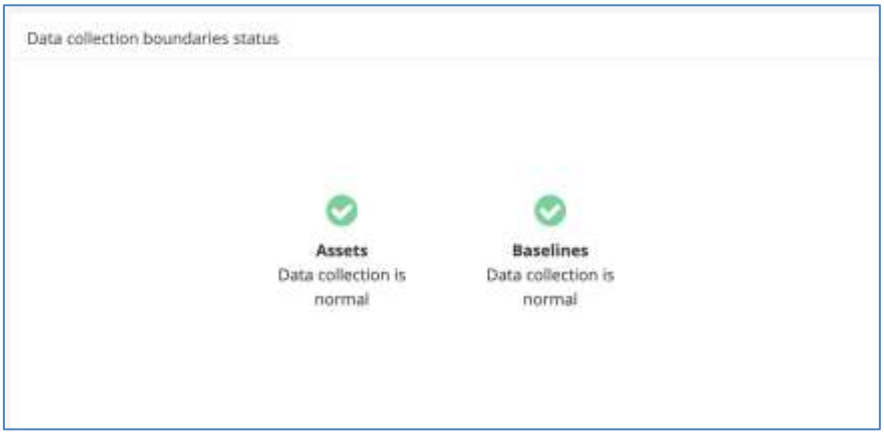


Figure 40 Data Collection Boundaries Status

> Note: The red status occurs only in uncommon situations.

Table 61: Data Collection Boundaries

Assets Limit	Baselines Limit
30K internal	1,000,000 baselines per protocol
20K external	More than 50K baselines per protocol in 5 minutes

> Note: The limits are configurable via the CLI.

3.1.1.1 Steps to take when Assets reach boundary

See section 4.8.9 in the Troubleshooting Guide section.

3.1.1.2 Steps to take when Baselines reach boundary

See section 4.8.10 in the Troubleshooting Guide section.

3.1.2 Baselines Retention

Baselines not active for more than a month in the system are removed automatically. This affects all the system components like insights and assets.

If you want to save inactive baselines for more than a month, it is configurable with assistance from Tripwire Support via the CLI.

3.1.3 Number of Sensors - Limitation

The maximum number of sensors attached to a single site varies and is determined by the number depicted in the specific license attached to the TIV site. For the current maximum limit, a boundary of 50 sensors per site should be in place.

> Note This limit does not cover Sensor Lite integrations, which are limited by the accumulated bandwidth aggregated by all Sensor Lites.

3.2 Open Ports

The required ports for TIV are as follows:

Table 62: Required Open Ports

Port Number	Usage	Comment
22	SSH	Open Port 22. TIV establishes the community connection over this standard SSH port (TCP port 22).
443	HTTPS (UI)	

3.3 Supported Operating Systems - Passive

The Operating Systems that TIV passively detects are as follows:

Table 63: Operating Systems Supported

Operating Systems
Android
Linux
MACOS X

Operating Systems
UNIX
Windows 10
Windows 10 Beta
Windows 2000
Windows 7.1
Windows 7/ Server 2008 R2
Windows 8.1/Server 2012 R2
Windows 8/Server 2012
Windows 95
Windows 98
Windows ME
Windows NT 4.0
Windows Server 2003
Windows Vista
Windows XP
Windows 2016
Windows 2019
Xbox360

3.4 Supported Passive Protocols

The following passive protocols are supported by TIV. Not all of them are configured by default. For information on configuring the protocols, refer to the **User Guide: Configuring Passive Protocols**.

> Note: In most cases, when TIV intercepts OS from passive protocols, the information in the packet will just be the version number (5.0, 6.1, etc.). TIV then translates it to the OS name (6.1 --> Windows 7/Server 2008 R2). You can see the mapping of the version number and OS name in the following link:
>
> https://docs.microsoft.com/en-us/windows/win32/sysinfo/operating-system-version

Table 64: Passive Protocols Supported

Protocol	Vendor
ABB DMS system	ABB

Protocol	Vendor
ABB HC800 (Infinet)	ABB
Alspa (Multicast messages)	Alstom
Altus ALnet	Altus
AMS	Beckhoff
B&R INA2000	B&R
BACNET	-
Bailey	ABB
BSAP	Bristol
CAPWAP	-
Caterpillar AHS	Caterpillar
CC Link IE - Field	CC Link IE
CIP	Rockwell
Cisco Discovery Protocol (CDP)	Cisco
Citect HMI	-
Cognex Discovery	Cognex
Comtrol NS Link	Comtrol
Control Technologies Inc. (CTI)	CTI
CPHA (Checkpoint High Availability)	Checkpoint
Cygnet SCADA	Cygnet
DACP	Willowglen
DeltaV	Emerson
DHCP	-
Digsi4	Siemens
Digsi5	Siemens
DNP3	-
Dropbox LAN-sync	Dropbox
E-Terra	Alstom
Enhanced Modbus	Themis
ENIP	Rockwell
EPM - Endpoint Mapper	-
ETHERNET/IP	-

Protocol	Vendor
FINS	Omron
Foundation Fieldbus (FF)	-
Foxboro LLC	Foxboro
Foxboro RTV	Foxboro
FTP - SEL	Schweitzer
GE Bentley Nevada (BNC3500)	GE
GE PAC8000 (AXE)	GE
GE QuickPanel (TRAPI+HTTP)	GE
GE SDI (MarkVie)	GE
GE SDI Classic (MarkVie)	GE
GE SRTP	GE
GE-ALM	GE
GE-EGD	GE
GE-EGD-CMP	GE
Goose (IEC-61850)	IEC
HART-IP	-
HiDiscovery	Hirschmann
Hikvision Discovery Protocols	Hikvision
Honeywell C200 - Ftebcip	Honeywell
Honeywell EpicMo (C300 management)	Honeywell
Honeywell Experion - CeeNTComm (C300,EHPM)	Honeywell
Honeywell Firewall CF9	Honeywell
Hot Standby Router Protocol (HSRP)	-
HP Switch	HP
HTTP	-
HTTP-XML (specific schemes)	-
IEC101	-
IEC103	-
IEC104	-
IQ3	Trend
Keyence Host-Link Communication	Keyence

Protocol	Vendor
Keyence KV Studio	Keyence
Keyence Logger	Keyence
Knapp	Knapp
Kongsberg	Kongsberg
Lantronix Serial GW	Lantronix
Linux High Availability	Linux
LLDP	-
MasterBus 300	ABB
MDLC	Motorola
Melsec	Mitsubishi
Melsoft	Mitsubishi
Microsoft CIFS (SMB)	-
Microsoft DCE RPC	-
Microsoft DCE RPC - ABB DCS Service Manager	-
Microsoft NTLMSSP (Auth protocol)	-
Microsoft RDP	
Microsoft SAMR	-
MMS (IEC-61850/ICCP/TASE.2)	-
MNDP	Mikrotik
Modbus	-
Modbus Modsoft	Schneider
Modbus Concept	Schneider
Modbus Eltec	Eltec
Modbus Execload	
Modbus GE Enervista	GE
Modbus ScadaPack	ScadaPack
Modbus Schneider	Schneider
MQTT	-
NASNavigator	Buffalo
NDP	Nortel
NetBIOS Browser (UDP 138)	-

Protocol	Vendor
NetBios Datagram Service	-
NMEA-0183	NMEA
odeq	Yokogawa
Omniflow Flow computer	Omniflow
OPTO	OPTO
OPTO MMP	OPTO
Opto SoftPAC Agent	Opto
Ovation	Emerson
P2	Siemens
PCCC	Rockwell
PI	OSISoft
POP3	-
Portwell	Portwell
ProConoS (TCP 20547)	Phoenix Contact
Profinet DCP	-
Profinet I/O	-
Profinet Real-Time	-
PTP	
Radius	
RCDP	Ruggedcomm
Redlion Crimson	Redlion
Redlion NView-2 Discovery	Redlion
RNRP	ABB
ROC Plus	Emerson
RTCP	-
S7Comm	Siemens
S7Comm Plus	Siemens
Schneider NetManage	Schneider
Siemens FWL LOAD (firmware upload)	Siemens
SIP	-
Skinny (SCCP)	Cisco

Protocol	Vendor
SLMP (CC Link IE Field Basic)	CC Link
SNMP	-
Spirit	ABB
Spotify P2P	Spotify
SSH	-
Symphony Plus	ABB
Synchrophasor	-
TDS	Microsoft
Telnet - Hirschmann	Hirschmann
Telnet - DeltaV	Emerson
Telnet - Moxa	Moxa
Telnet - Omniflow	Omniflow
Telnet - SEL	Schweitzer
TFTP	-
Totalflow	ABB
Triconex Tristation	Schneider
Triconex TSAA	Schneider
Tridium	Niagara
UDLD	Cisco
Valmet DNA	Valmet
VNET (VHF)	Yokogawa
Windows Update Delivery Optimization	Microsoft
WonderWare Suitelink IOTalk	WonderWare

3.5 TIV Appliance

TIV Appliances are provided in various sizes to fit different deployment requirements. Customers can benefit from a quick and easy deployment process, with significant reduction in setup, maintenance, monitoring time and effort.

Each TIV Appliance is delivered pre-installed with ClarotyOS – a hardened, built Linux OS – and ready for use out-of-the-box. Simply plug the appliance into the designated network interfaces and after the configuration wizard is completed, TIV begins its network learning. TIV establishes deep asset inventory and

communications profiling to provide instantaneous visibility and threat protection.

By choosing an appliance-based deployment rather than deploying TIV on virtual servers, users can:

- Deploy in a Plug & Play manner
- Follow straightforward monitoring and maintenance hardware procedures, including qualified updates for OS and the TIV Application
- Obtain full compatibility between the TIV software and its underlying hardware
- Backup & restore the entire system in a built-in manner: application and configuration, operating system and settings, as well as customer data. This can be done locally or to a remote location.

3.6 Hardening

Hardening is the process of securing a system by reducing its surface of vulnerability.

Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary services.

The following sections describe the hardening procedure for the Red Hat Enterprise Linux 7 / CentOS 7 operating systems that run the TIV and SRA applications.

TIV is approved to run on Red Hat Enterprise Linux 7 and the derived versions of CentOS 7.
ClarotyOS is based on CentOS and applies to the hardening procedure out of the box.

The hardening procedure is based on the CIS Red Hat 7 benchmark 2.1.1.

3.6.1 Applying Hardening Scripts

3.6.1.1 Run hardening for TIV

```
# Open the TIV tar
tar -xzvf TIV-4.1.2.20740-Installer-CentOS7.7.tar.gz
```

```
# Go to the extracted directory
cd TIV-4.1.2.20740/

# Recommended: Install TIV before hardening

# Open the hardening tar
tar -xzvf harden-prod.tar.gz

# Run the hardening script
harden-prod/apply.sh
```

3.6.1.2 Run hardening for SRA

```
# Open the SRA tar
tar -xzvf SRA-3.0.2.20635-Installer-CentOS7.7.tar.gz

# Go to the extracted directory
cd sra-3.0.2.20635/

# Recommended: Install SRA before hardening

# Open the hardening tar
tar -xzvf harden-prod.tar.gz

# Run the hardening script
harden-prod/apply.sh
```

3.6.2 Exceptions

3.6.2.1 Not included

Not relevant with the TIV configuration:

Section	Subject	Reason
1.1.6-20	Disable unused filesystems	The customer should decide if they want separate partitions for system directories
1.3.1-2	Ensure AIDE is installed	AIDE is irrelevant for a static server
1.7.1-2, 5.2.16	Warning Banners	Tripwire does not configure login prompts for the customer
3.4.2-5	Ensure /etc/hosts.allow is configured Ensure /etc/hosts.deny is configured	In another section, we removed the packages these files apply to
4.2.1.4	Ensure rsyslog is configured to send logs to a remote log host	Tripwire does not automatically configure remote logging, the customer is responsible for this configuration.

5.2.15, 5.4.1.4, 5.5, 6.1.10	Ensure SSH access is limited Ensure inactive password lock is 30 days or less Ensure root login is restricted to system console Ensure no world writable files exist	Our server has only one user and it needs SSH access
6.1.11-12	Ensure no unowned/ungrouped files or directories exist	The Tripwire software is not an NFS server

Not relevant since the application should not be connected to the Internet

Section	Subject	Reason
1.2.1-4	Configure Software Updates	Relevant for Internet repositories
1.8	Ensure updates, patches, and additional security software are installed	Tripwire does not recommend upgrading packages automatically

These are set automatically by the OS if supported by the hardware:

Section	Subject	Reason
1.5.2	Ensure XD/NX support is enabled	NX bit, turned on by the kernel if supported, otherwise irrelevant

3.6.2.2 Changed

Section	Subject	Change
5.3.1	Ensure password creation requirements are configured.	Changed minimum length to 8 (instead of 14).
5.3.2	Ensure lockout for failed password attempts is configured	allow 10 login attempts before lockout (instead of 3) and show message when locked out.

3.7 TIV Services and Dependencies

TIV has several services and dependencies running on the machine.

3.7.1 TIV Running Services

- icsranger
- icsranger-watchdog

3.7.2 Dependent Services

- mariadb
- rabbitmq-server
- redis
- postgressql-11.2

3.8 Supported Asset Types

Table 65: List of Asset Types

Asset Types		
AAA Server	Access Control	Access Point
AD Server	Autonomous Vehicle	AV Server
Barcode Scanner	Bluetooth Device	Broadcast
Camera	Cleaning Device	Controller
DB Server	Data Logger	Domain Controller
Endpoint	Engineering Station	File Server
Firewall	Front End Processor	Gateway
GPS Clock	GPS Device	Historian
HMI	Home Assistant	IED
Infusion Pump	Media Server	Medical Device
Microscope	Modem	Network Access Storage
Networking	NTP Server	OPC Server
OT	PLC	Printer
Proxy Server	Remote IO	Reverse Proxy Server
Robot	Router	RTU
SCADA Client	SCADA Master	SCADA Server
Smart Light	Smart Phone	Smart Watch
Storage Array	Streamer	Switch
Syslog Server	Terminal Server	TV Screen

Asset Types		
UPS	User Console	User Workstation
Vending Machine	Video Recorder	Virtualization Server
VOIP Phone	VOIP Server	Web Server
Wireless LAN Controller		

3.8.1 Purdue Level Classifications of Asset Types

Table 66: Purdue Levels

Asset Type	Purdue Level
Autonomous Vehicle	0
Remote IO	0
Robot	0
UPS	0
Access Control	1
Controller	1
GPS Device	1
IED	1
Infusion Pump	1
Medical Device	1
Microscope	1
PLC	1
RTU	1
Smart Light	1
Access Point	1.5
Firewall	1.5
Gateway	1.5
Networking	1.5
Router	1.5
Switch	1.5
Engineering Station	2
Front End Processor	2
HMI	2

Asset Type	Purdue Level
OPC Server	2
OT	2
SCADA Client	2
SCADA Master	2
SCADA Server	2
Broadcast	2.5
Cleaning Device	3
Data Logger	3
Endpoint	3
Home Assistant	3
Media Server	3
NTP Server	3
Proxy Server	3
Reverse Proxy Server	3
Streamer	3
Syslog Server	3
User Console	3
User Workstation	3
Video Recorder	3
AAA Server	4
AD Server	4
AV Server	4
Barcode Scanner	4
Bluetooth Device	4
Camera	4
DB Server	4
Domain Controller	4
File Server	4
GPS Clock	4
Historian	4
Modem	4

Asset Type	Purdue Level
Network Access Storage	4
Printer	4
Smart Phone	4
Smart Watch	4
Storage Array	4
Terminal Server	4
TV Screen	4
Vending Machine	4
Virtualization Server	4
VOIP Phone	4
VOIP Server	4
Web Server	4
Wireless LAN Controller	4

3.8.2 Asset Classes

Table 67: Asset Class

Asset Type	Asset Class
AAA Server	IT
Access Control	
Access Point	IT
AD Server	
Autonomous Vehicle	
AV Server	
Barcode Scanner	IoT
Bluetooth Device	IoT
Broadcast	
Camera	IoT
Cleaning Device	
Controller	OT
Data Logger	
DB Server	

Asset Type	Asset Class
Domain Controller	IT
Endpoint	IT
Engineering Station	OT
File Server	
Firewall	
Front End Processor	
Gateway	OT
GPS Clock	
GPS Device	
Historian	
HMI	OT
Home Assistant	
IED	
Infusion Pump	IoT
Media Server	
Medical Device	
Microscope	IoT
Modem	
Network Access Storage	IT
Networking	IT
NTP Server	
OPC Server	
OT	OT
PLC	OT
Printer	IT
Proxy Server	
Remote IO	OT
Reverse Proxy Server	
Robot	
Router	IoT
RTU	OT

Asset Type	Asset Class
SCADA Client	OT
SCADA Master	
SCADA Server	OT
Smart Light	IoT
Smart Phone	IoT
Smart Watch	IoT
Storage Array	
Streamer	IoT
Switch	IoT
Syslog Server	
Terminal Server	
TV Screen	IoT
UPS	IoT
User Console	
User Workstation	
Vending Machine	IoT
Video Recorder	IoT
Virtualization Server	
VOIP Phone	IoT
VOIP Server	
Web Server	
Wireless LAN Controller	

3.9 Supported Activity Types

Table 68: Activity Types

Activity Types
Active Baseline
Alert Acknowledged
Alert Assign
Alert Auto Resolved
Alert Enrichment

Activity Types
Alert Ignored
Alert New
Alert Non-Relevant
Alert Resolved
Alert Resolved By Rule
Alerts Resolved
Asset Changed IP
Asset User Changed Info
Comment Add
Communication Down
Communication Up
Message
Policy Invalidated
Policy Updated
Policy Validated
Rule Added
Site Down
Site Up
Training Mode Off
Training Mode On

3.10 Supported Reports

The following report types are generated by the system.

Table 69: Report Types

Report Name	Report Contents
TIV Inactive assets from the last week	Report with unicast assets that didn't communicate in the last week.
TIV Completed Insights	All marked as completed insights, include vulnerabilities.
TIV Resolved alerts from the last week	Activities report for alerts that resolved in the last week.
TIV Site connectivity from the last week	Site connectivity status from the last week (site up or down).

Report Name	Report Contents
TIV New Alerts from the last week	Critical and High alerts that created in the last week and their status.
TIV Alerts Ignored/Acknowledged from the last week	Activities of alerts that marked as ignored or acknowledge from the last week.
TIV Top Risky Assets	This is a report for the top risky assets.
TIV Insights with High Criticality	Insights with high criticality.
TIV Assets that talk with external IP	Unicast and remote assets that are talking with external assets. External IPs coupled with respective network interfaces expose the asset to users outside of the company's perimeter, enabling attackers to enter the OT network.
TIV Assets discovered in the last week	All assets discovered in the last week.
TIV Assets with unsecured protocols	All assets that are using unsecured protocols. Assets with unsecured protocols contain security weaknesses that attackers can leverage to compromise the network's security.
TIV Assets from the Industrial Security Zone	Assets in the industrial security zone (level 3).
TIV Assets with unpatched CVEs	All assets with unpatched vulnerabilities that have Full Match CVEs. Assets that run software versions that are vulnerable and can be leveraged by attackers for various malicious purposes such as remote code execution, DDoS, etc.
TIV Assets performed Data Acquisition Write (Operated PLCs)	All assets that performed data acquisition write. These assets should be considered as potential assets that can change the process by changing values.
TIV Assets using remote connections	All assets using remote connections.
TIV Assets from the Enterprise Security Zone	TIV assets from the Enterprise Security Zone and assets from the enterprise network (level 4 and level 5).
TIV Assets Changed IP in the last month	Activities about assets that changed their IP in the last month.
TIV Parsed Assets	All assets discovered as parsed assets via App DB.
TIV Insights Report	All open Insights (severity: High, Medium, Low)

3.11 Reverse Proxy Server

In some cases, it might be required to enable access to multiple sites through a single reverse proxy host. In this case, the host is required to have connectivity to all sites it is supposed to allow access to. It is required to set up and Apache HTTP server as the reverse proxy host. Below is a sample configuration for setting Apache as a reverse proxy server for TIV.

```
Listen 443 https
SSLPassPhraseDialog exec:/usr/libexec/httpd-ssl-pass-dialog
SSLSessionCache shmcb:/run/httpd/sslcache(512000)
SSLSessionCacheTimeout 300
SSLRandomSeed startup file:/dev/urandom 256
SSLRandomSeed connect builtin
SSLCryptoDevice builtin

<VirtualHost _default_:443>
   SSLEngine on
   SSLCertificateFile /etc/pki/tls/certs/ca.crt
   SSLCertificateKeyFile /etc/pki/tls/private/ca.key
   SSLProtocol all -SSLv2 -SSLv3
   SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA

   ProxyPreserveHost On
   SSLProxyVerify none
   SSLProxyEngine on
   SSLProxyCheckPeerCN off
   SSLProxyCheckPeerName off
   SSLProxyCheckPeerExpire off
   ProxyRequests off
   RewriteEngine on

   #EMC
   RewriteCond %{HTTP:Connection} "upgrade" [NC]
   RewriteCond %{HTTP:Upgrade} "websocket" [NC]
   RewriteRule "/secure/emc/(.*)" "wss://<TIV-IP>/$1" [P,L]
   RewriteRule "/secure/emc/(.*)" "https://<TIV-IP>/$1" [P,L]
   ProxyPassReverse "/secure/emc/" "https://<TIV-IP>/"
   <Location "/secure/emc/">
       AddOutputFilterByType SUBSTITUTE text/html
       Substitute "s|<base href=\"/\">|<base href=\"/secure\/emc\/\">|i"
   </Location>

   #site1
   RewriteCond %{HTTP:Connection} "upgrade" [NC]
   RewriteCond %{HTTP:Upgrade} "websocket" [NC]
   RewriteRule "/secure/site1-name/(.*)" "wss://<TIV-IP>/$1" [P,L]
   RewriteRule "/secure/site1-name/(.*)" "https://<TIV-IP>/$1" [P,L]
   ProxyPassReverse "/secure/site1-name/" "https://<TIV-IP>/"
   <Location "/secure/site1-name/">
       AddOutputFilterByType SUBSTITUTE text/html
       Substitute "s|<base href=\"/\">|<base href=\"/secure\/site1-name\/\">|i"
   </Location>
</VirtualHost>
```

In this example, have created entries for a site an EMC.

When creating such entries, remember to change **site1-name** and **<TIV-IP>** with the site's name and IP address respectively.

4 Admin Tools

4.1 Health Check Monitoring Script

A health check script is available for monitoring the state of the system.

4.1.1 Scheduled Health Monitoring Syslog

- For automatic running of the script through Syslog, see section 4.4.
- For more information, refer to the Syslog messaging instructions.

4.1.2 Script

The script is in `/opt/icsranger` and is named `health_check.sh`.

4.2 TIV Integration Instructions

- Navigate to **Settings > Integrations** > **Third Party** to set up the system for integrations with external systems, enterprise tools, and Tripwire Partner solutions.

> Note These are one-way integrations that enable TIV to connect and send data to other systems and services.

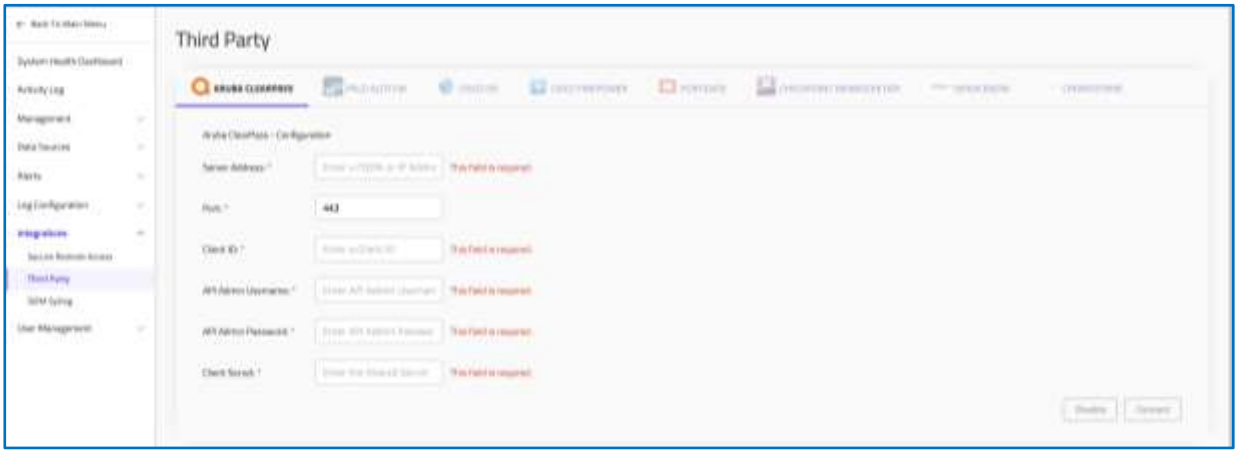


Figure 41 Configuration - Integrations > Third Party Menus

4.2.1 Aruba ClearPass Integration

Tripwire Industrial Visibility integrates with Aruba ClearPass. The TIV asset inventory, including all discovered assets and their attributes, can be sent to ClearPass to enrich ClearPass' visibility into the previously-hidden OT network.

The extreme visibility provided by TIV's DPI and OT protocol analysis allows customers to use ClearPass authentication, authorization, and enforcement policies to achieve high level access control in their ICS environments.

Figure 42 Aruba ClearPass Integration tab

Enter the following information, all of which are mandatory other than the Port:

- **Server Address** – Enter a valid server address
- **Port** – Enter the port used for the Aruba integration
- **Client ID** – Enter the Client ID
- **API Admin Username** – Enter the API Admin's username
- **API Admin Password** – Enter the API Admin's password
- **Client Secret** – Browse to select the shared secret for this integration.

- When you finish setting up the integration details, press the **Connect** button to implement your choices, or press **Disconnect** to undo the connection and revert to the prior setup.

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

4.2.2 Palo Alto FW Integration

This integration enables you to connect with the Palo Alto FireWall (FW) system. It provides extreme visibility into the lowest levels of their industrial networks and enables dynamic, automated, and active threat protection. The integration also improves threat hunting via real time alerting with implications on process integrity and cyber resilience.

With this integration, existing customers can integrate NGFW with TIV to decide which events will be reported back to the Palo Alto Network Security Operating Platform and trigger the creation of a new firewall rule, that will block or limit the source of the threat.

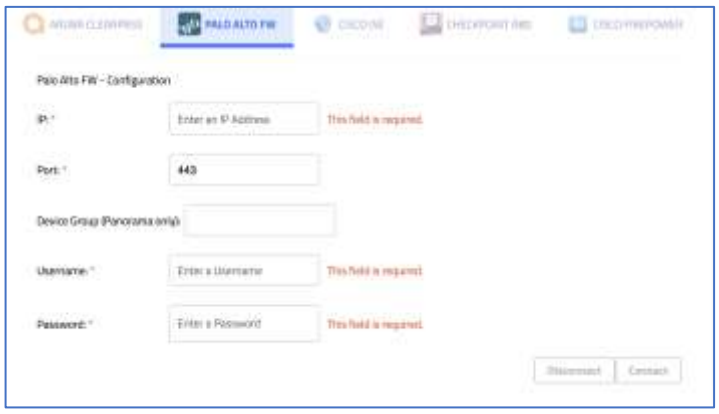


Figure 43 Configuration - Palo Alto FW Tab

- **IP** – Enter a valid IP address for the target machine (mandatory field)
- **Port** – The port to be used for the Palo Alto FW integration (mandatory field). The default value is **443**.
- **Username** – Enter the relevant password for connecting to the port (mandatory field)
- **Certificate Password** – Enter the password of your choice (mandatory field)
- Choose Connect or Disconnect .

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

4.2.3 Cisco ISE Integration

This integration enables you to connect with the Cisco ISE system for managing system-wide OT, IT, and IoT assets/endpoints.

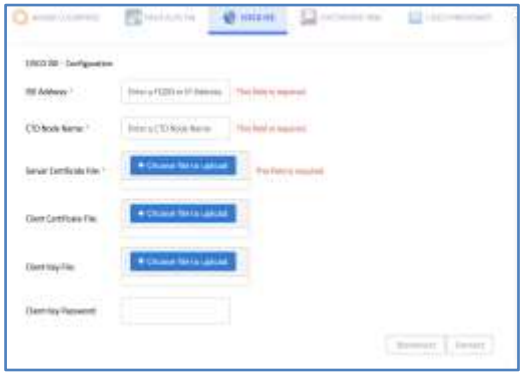


Figure 44 Cisco ISE Integration parameters

1. If you are using a credential-based approach, provide the following integration information.

- **ISE Address** – Enter a valid address for the target machine (mandatory field). This could be an FQDN or an IP address (preferably FQDN).
- **TIV Node Name** – Enter the name this device will be displayed with on the **pxGrid Management Screen** (mandatory field).
- **Server Certificate File** – Select your Cisco ISE certificate file from your browser if you already have it in your system (mandatory field).
  Click the **Choose file to upload** button if this is the first instance.

> Note: All of these certificates originate in the file that you downloaded from Cisco ISE or an external Certification Server.

- **Client Certificate File** – Input your Cisco client certificate file from your browser if you already have it in your system (optional field).
  Click the **Choose file to upload** button if this is the first instance.
- **Client Key File** – Select your key certificate file from your browser if you already have it in your system (optional field).
  Click the **Choose file to upload** button if this is the first instance.
- **Client Key Password** –This is optional. It is the password for the client certificate (if one exists).
- Skip to Step 3 to continue

2. If you are using a password-based approach, provide the following integration information:
   - **ISE Address** – Enter the valid address for the target machine (mandatory field)
   - **TIV Node Name** – Enter the name that this device will be displayed with on the pxGrid Management Screen (mandatory field).
   - Server Certificate File – Not relevant for this option.
   - Client Certificate File – Not relevant for this option.
   - Client Key File – Not relevant for this option.
   - Client Key Password – Not relevant for this option.
3. After the previous integration details have been applied:
   - Press **Connect**  in the lower right corner of the dialog to implement your choices,

     or
   - Press **Disconnect**  to undo the connection and revert to the prior setup.
4. After you have connected to Cisco ISE:

- The Connect button changes to an Update button
- A popup notification appears when a new integration is added:

5. Otherwise, a red popup box appears to indicate the integration did not connect successfully.
6. The relevant logs are stored in the Export Data TIV logs:

```
/opt/icsranger/workdir/logs/export_data.log
/opt/icsranger/workdir/logs/export_data.stderr.log
/opt/icsranger/workdir/logs/export_data.stdout.log
```

4.2.4 Cisco FirePOWER Integration

This integration enables you to connect with Cisco FirePOWER. Cisco Firepower is a threat-focused firewall with unified management.

TIV's integration with Firepower transfers the following information from TIV:

- Assets in TIV, including: IP addresses, MAC addresses, Names, and attributes.
- CVEs for each asset, if applicable.

Information is updated every 5 minutes.

4.2.4.1 Step 1: Configuring Cisco Firepower

Configure Cisco Firepower before connecting it to TIV:

1. Log into the Cisco Firepower Web UI.
2. Navigate to System > Integration > Host Input Client and click on Create Client:

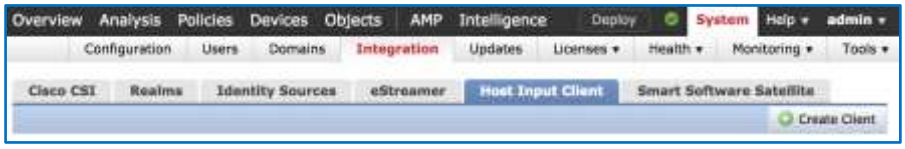


Figure 45 Cisco Firepower Integration tabs

3. To add the client, enter the TIV IP address and press **Save**. Using a password is optional.

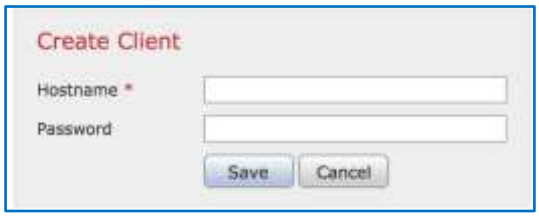


Figure 46 Cisco Firepower Integration - Create Client menu

4. After adding the Client, download its certificate using the download button on the right side:

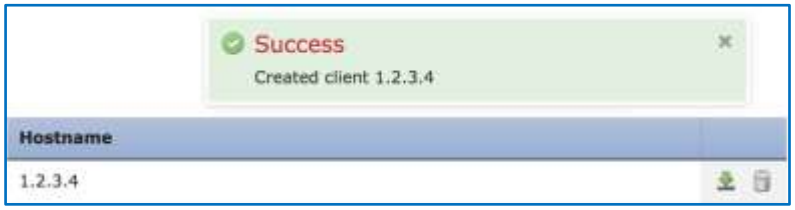


Figure 47 Cisco Firepower Integration - Create Client menu

5. Continue to the next step to configure TIV to connect with Cisco Firepower.

4.2.4.2 Step 2: Connecting to Cisco Firepower from TIV

To connect TIV to Cisco Firepower:

1. Navigate to the Settings > Integrations > Third Party > Cisco Firepower tab:

Figure 48 Configuration - Cisco Firepower Tab

2. Enter the following information:
   - IP – Enter a valid IP address (mandatory field)
   - Certificate Password – Enter the password of your choice
   - Certificate File – Browse to select the relevant certificate file downloaded in Step 4 (mandatory field).

- When you finish setting up the integration details, press **Connect** or press **Disconnect** .

For more information, refer to the *Tripwire Industrial Visibility Cisco Firepower Installation Guide*.

4.2.5 Integration with Fortinet's FortiGate and FortiSIEM

The integration of Tripwire Industrial Visibility with FortiGate, Fortinet's Next Generation Firewall, provides a seamless transformation of TIV's Virtual Zones and alerting policies, into enforceable firewall policies.

TIV's Virtual Zones are sent to FortiGate and automatically create Address Groups. These Address Groups can then be used by FortiGate users to create Firewall policies, which are no longer based on minimal information such as an asset's IP or MAC address but can now be managed as an asset type (such as PLC, HMI, or RTU), model, and firmware version.

TIV's alerting policies automatically create FortiGate firewall rules to provide the needed enforcement of policies to stop malicious communications and to serve as a complete segmentation tool.

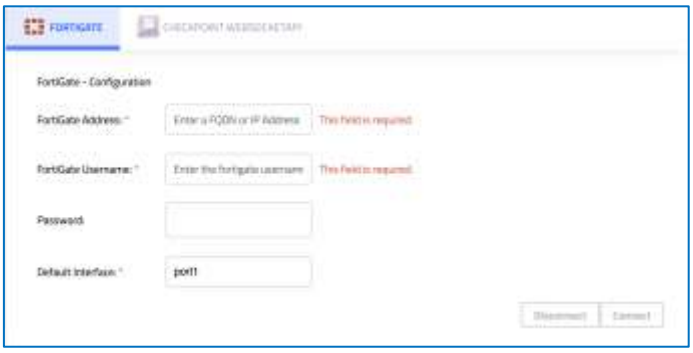


Figure 49 Configuration - Fortigate Tab

The extended visibility into OT asset attributes, Virtual Zones, and security policies provided by TIV allows FortiGate users context into the OT networks and the required control to protect them.

- OT network assets learned by TIV are sent to FortiGate along with their device type (such as PLC, HMI, and Endpoint) and the Virtual Zone
- TIV Virtual Zones are sent to FortiGate to define Address Groups
- These Address Groups are then automatically used to create firewall policies within FortiGate. While these Address Groups are created in a disabled state, they can be easily enabled to provide out-of-the-box firewall enforcement policies for the OT network
- With TIV's asset and Address Groups information, users can also modify policies or create their own to achieve tailored firewall policies for their OT networks

For more information, refer to the *Tripwire Industrial Visibility Installation Guide for Fortinet.*

4.2.5.1 Configuring FortiGate Integration

To configure and use the FortiGate integration:

1. Navigate to the FortiGate integration configuration page: **Settings > Integrations** > **FortiGate** tab.
2. Enter the required details of your FortiGate instance:
   a. **FortiGate Address** – The IP or FQDN. This is a mandatory field.
   b. **FortiGate Username** – The username that will be used to establish the connection between TIV and FortiGate. This is a mandatory field.
   c. **Password** – The FortiGate password corresponding to the provided FortiGate username.
   d. **Default Interface** – The interface to be used for creating FortiGate's IPv4 policies.
3. Click Connect  .
4. Verify the connection was successful by looking for the status line to show **Online.**
   - From this point, TIV will send or update asset and virtual zone information and create FortiGate policies every 5 minutes.
5. Log into your FortiGate to review the assets (referred to as "Addresses" within FortiGate), the Address Groups, and the IPv4 Policies created by TIV in FortiGate. You can then make changes and enable the policies created.

4.2.5.2 FortiSIEM Integration

FortiSIEM, Fortinet's SIEM tool, is now fully compatible with TIV's asset inventory and alerts sent via Syslog. With FortiSIEM, customers can leverage their existing SIEM-based workflows and monitor processes to perform security operations.

- FortiSIEM integration is a Syslog integration. Refer to section 4.4.

4.2.6 Checkpoint IoT Integration

- Follow these steps to perform the Checkpoint IoT integration:

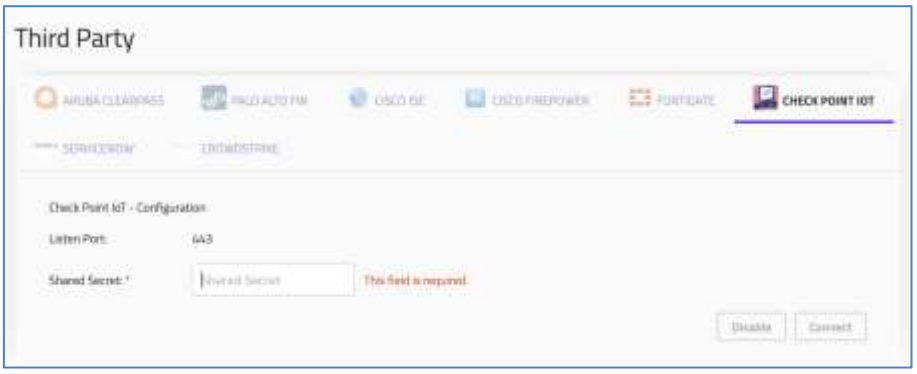


Figure 50 Configuration - Checkpoint IoT Tab

1. Navigate to the Checkpoint IoT configuration page, located in the **Settings > Integrations > Checkpoint IoT** tab.
2. Enter a value for the **Shared Secret**.
3. Click **Connect** Connect .

For more information, refer to the *Tripwire Industrial Visibility Installation Guide for Check Point*.

4.2.7 ServiceNow Integration

Tripwire has partnered with ServiceNow to leverage TIV's ability to detect, discover and classify OT/ICS assets and share this classification directly with ServiceNow CMDB. TIV will automatically updates the ServiceNow CMDB with asset classification data and custom security attributes.

This ServiceNow - TIV integration provides centralized visibility of network assets across IT and OT infrastructure in which a centralized asset and edge security policy is defined and managed.

- From TIV, navigate to the bottom left menu to the cog wheel ⚙ to access the **Integrations > Third Party > ServiceNow** page

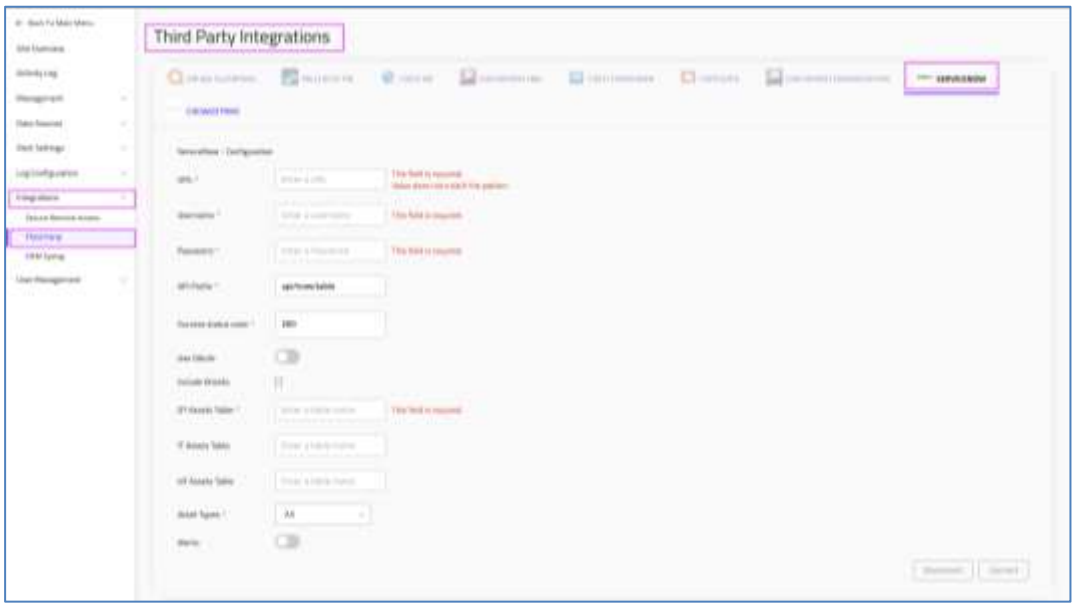


Figure 51 Accessing ServiceNow from the Settings > Integrations > Third Party > menu

Figure 52 Fields in the ServiceNow tab - when not using OAuth

> Note: This is the recommended use.
> However, instead of using the UI, you can opt to use the CLI command - in the *ServiceNow Integration Guide*

- The ServiceNow tab includes the configuration fields listed below. Use the values collected during ServiceNow configuration.

> Note: Mandatory fields are marked with a red asterisk*.

Table 70: ServiceNow Integration Parameters

Field	Meaning	Notes
URL*	The URL of the ServiceNow instance	
Username*	The Administrator's username for the ServiceNow system as set up in the previous section	
Password*	The Administrator's password for the ServiceNow system as set up in the previous section	
API Prefix*	A configurable endpoint, adding automatically from TIV code (api/now/table/) By default	
Success Status code*	200 by default	The HTTP 200 OK Success Status response code indicates that the request has succeeded
Use OAuth	By default, OAuthentication is set to OFF. When turned ON, the following fields are required:	For more information, see section *TIV ServiceNow Integration Guide, Using OAuthentication* Use this option when using the OAuth authentication is provided by ServiceNow
Client ID	The ID of the Client	
Client Secret	The Client's secret	
Use external OAuth Provider	By default, using an external OAuthentication Provider is set to OFF. When turned ON, the following field is required:	Use this option when using OAuth authentication defined in an external provider
OAuth Provider URL	The URL of the external OAuthentication Provider	
Include Ghosts	Whether or not to include ghost assets	Ghost assets are excluded by default
OT Assets Table*	The target Table of **OT Assets** located in the ServiceNow system	
IT Assets Table	The target Table of **IT Assets** located in the ServiceNow system	
IoT Assets Table	The target Table of **IoT Assets** located in the ServiceNow system	
Include Ghosts	Check this box to filter for any ghost assets	

Field	Meaning	Notes
Asset Types*	All by default. Otherwise, use this filter to obtain only the specific asset types intended for exporting to ServiceNow.	For more information, see *TIV ServiceNow Integration Guide*, *Filtering Fields*
Alerts	By default, Alerts are set to OFF. When turned ON, the following fields are required:	For more information, see *TIV ServiceNow Integration Guide*, *Alerts for ServiceNow*
	Client Secret	The Client's secret

- Once all the fields are entered, click **Connect**  .
  - When successful, a message is displayed at the bottom right of the screen in a green box indicating "Added Integration Configuration".
- The button for **Connect** changes to **Update**, which indicates that the configuration has been saved.
- You can put the same table name for each type of assets if you prefer. However, TIV will send an API call for each asset type. In this case an empty list of objects will be returned if you have no assets of a particular type.

For more information, refer to the *TIV ServiceNow Integration Guide*.

4.2.8 CrowdStrike Integration

- From TIV, navigate to **Settings > Integrations > Third Party > CrowdStrike**.

Figure 53 TIV Configuration for CrowdStrike

- In the CrowdStrike tab, the following configuration fields are required. Use the values collected during CrowdStrike Falcon configuration.

Field	Meaning
Client ID	The OAuth2 Client ID for the CrowdStrike server from the CrowdStrike platform
Client Secret	The OAuth2 Client Secret for the CrowdStrike server from the CrowdStrike platform
Cloud URL	Select the relevant server to connect to by choosing from the dropdown of CrowdStrike Cloud URLs
Get Snort Signatures	Choose whether to pull the Snort signatures from CrowdStrike (Default is Yes)
Get YARA Signatures	Choose whether to pull the YARA signatures from CrowdStrike (Default is Yes)
For **Active Detection** asset information, navigate to **Settings > Data Sources > Active Detection** and follow the instructions in the *TIV - CrowdStrike Falcon Installation Guide*	

- Once all the fields are entered, click **Connect**  .
  - When successful, a message is displayed at the bottom right of the screen indicating "Added Integration Configuration".

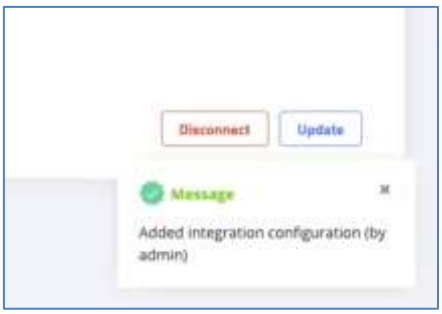


Figure 54 Activity notification when integration is configured successfully

  - The button for **Connect** changes to **Update**, indicating that the configuration has been saved.

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

4.3 API Explorer

These instructions cover the API Explorer for version 4.2.4 of Tripwire Industrial Visibility (TIV).

This web API reference provides all the information needed for application developers to implement calls for TIV's endpoints. Use these RESTful APIs to access TIV routes for enhancing your system.

4.3.1 Accessing the API Explorer

Log in to TIV with your username and password.

> Note that the functionality is relevant for only for Admins.

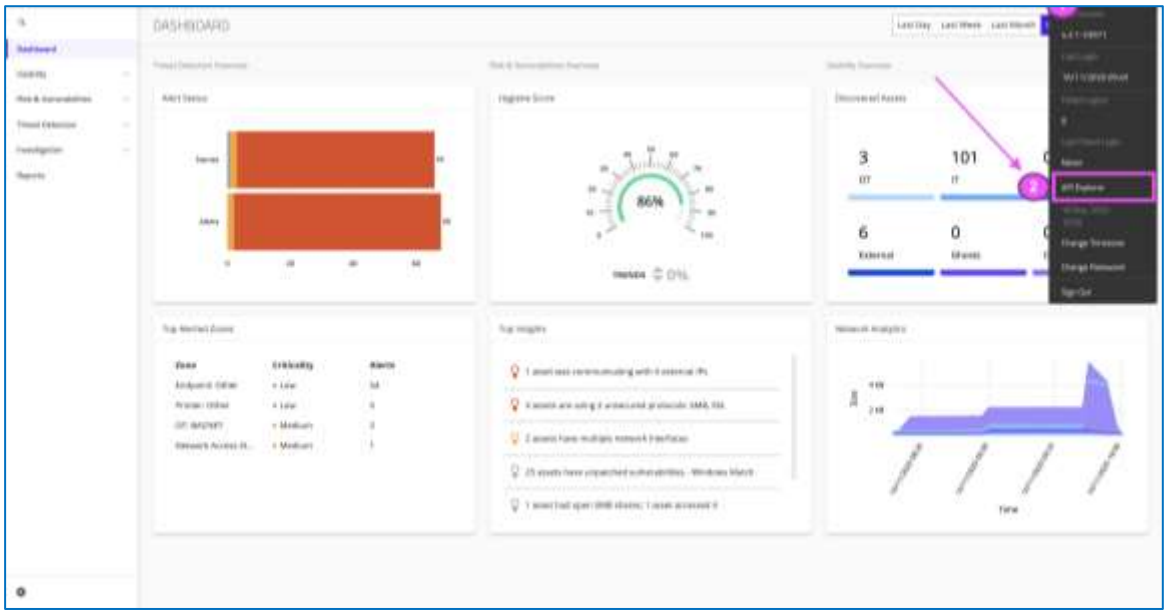


Figure 55 API Explorer

1. On the far right edge of the Activity bar at the top of the screen, click on your username to open the user dialog
2. Select the **API Explorer** button.
3. The API Explorer opens in *Swagger* as shown in the figure below.

4.3.2 Using the API Explorer

The API Explorer opens in a separate tab as follows:

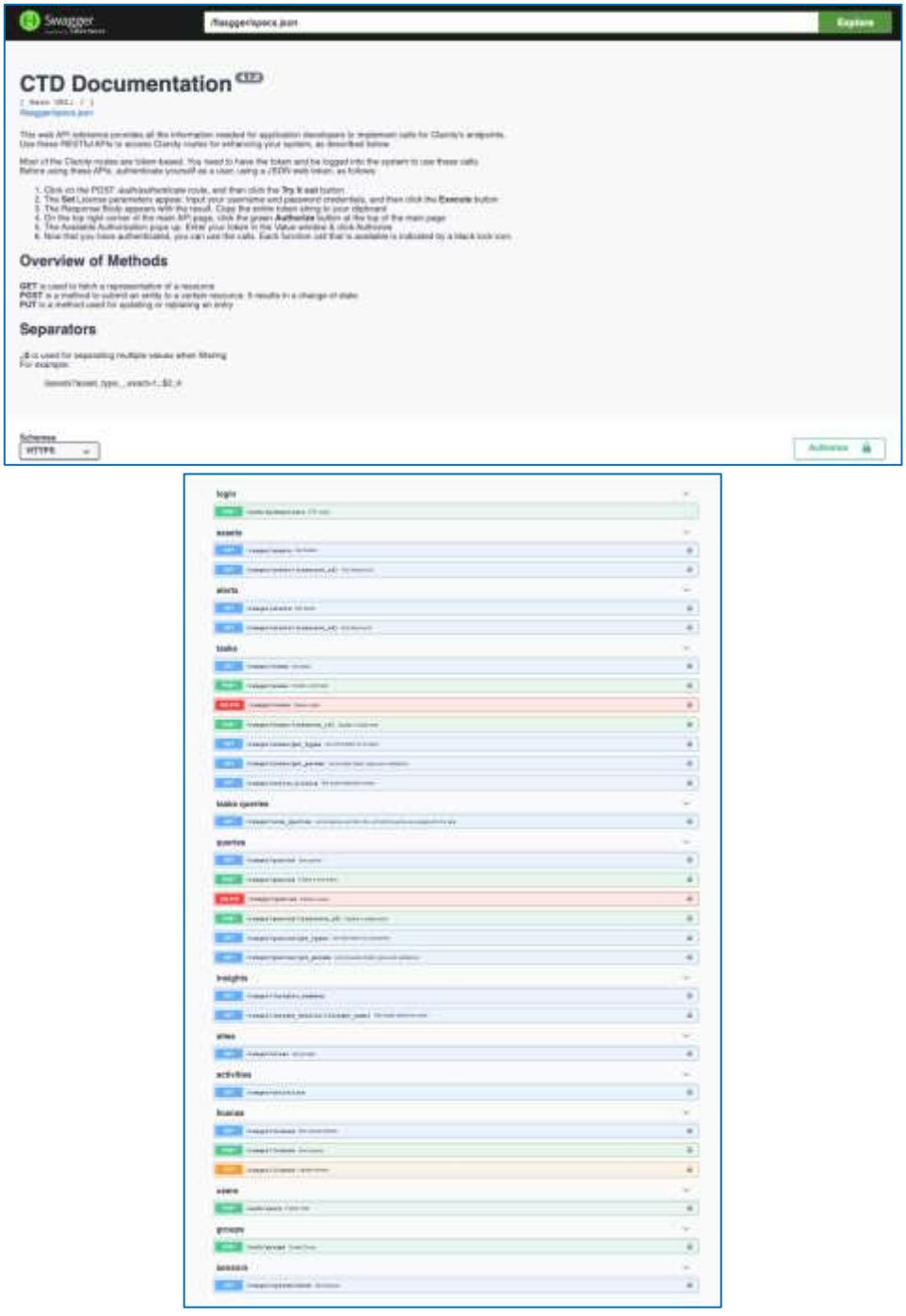


Figure 56 API Explorer – Main Screen

Figure 57 API Models

4.3.3 Authentication

Most of the TIV routes are token-based. You need to have the token and be logged into the system to use these calls.

Before using these APIs, authenticate yourself as a user using a JSON web token, as described below.

4.3.3.1 Authentication steps

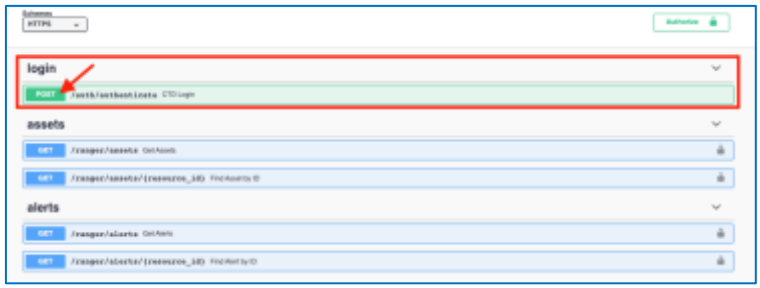


Figure 58 Authentication

1. Click on the `POST /auth/authenticate` route, and then click the **Try it out** button
2. The **Set License** parameters appear. Input your username and password credentials, and then click the **Execute** button
3. The **Response Body** appears with the result. Select and copy to your clipboard the entire token string (between the quote marks), as shown in the example below:

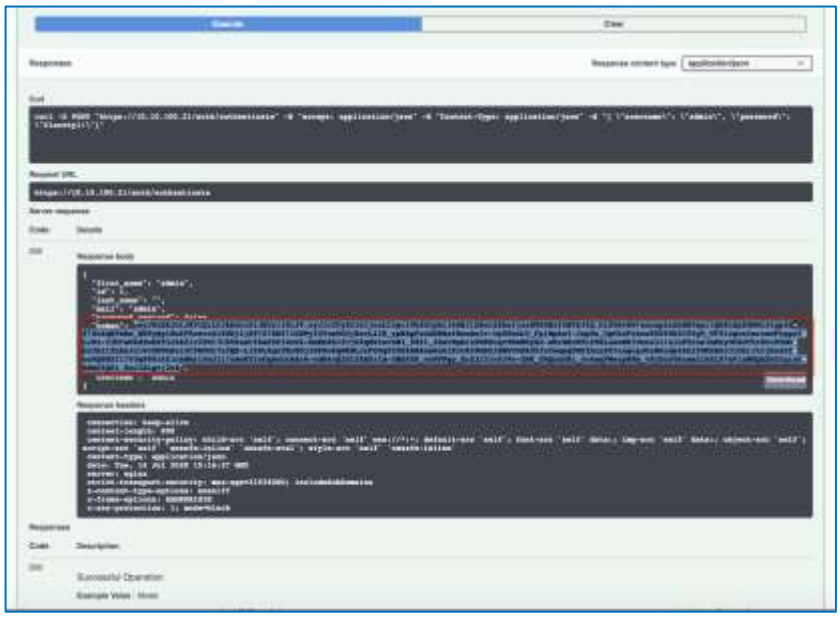


Figure 59 Copying the token from the response body

4. On the top right corner of the main API page, click the green Authorize button
5. The Available Authorization pops up.

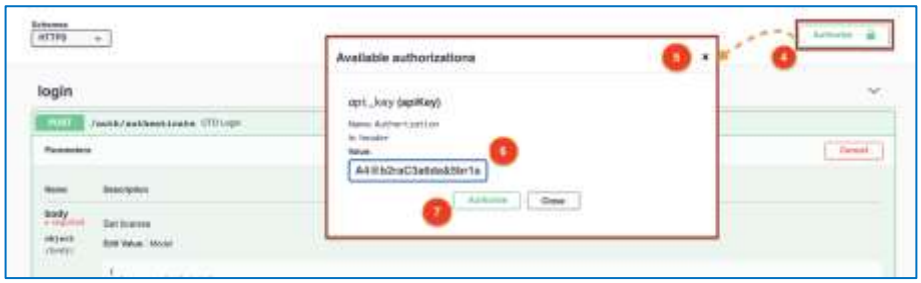


Figure 60 Authorization popup

6. Enter your token in the **Value** window
7. Click Authorize
8. Now that you have authenticated, you can use the calls.

Each function call that is available is indicated by a black lock icon.

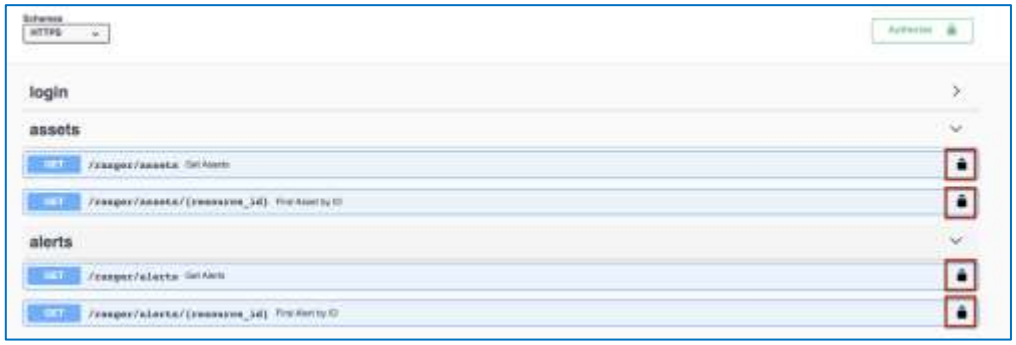


Figure 61 Black lock icons appear once the User is authenticated

4.3.4 Overview

4.3.4.1 Permissions

Admins can access all the routes. Other users can obtain all the information they can access in the TIV UI.

4.3.4.2 Separators

`,;$` is used for separating multiple values when filtering.

For example:

```
/assets?asset_type__exact=1,;$2,;$4
```

Will search for all assets but return just the assets of type 1, 2, 4.

```
/ranger/assets?fields=vendor,;$id
```

Will search for all assets but return just the vendor and ID fields

4.3.4.3 Models

The Response Body is usually a JSON document, and the structure of that JSON document is defined in the **Models** provided in the API Explorer, immediately below the area of the function calls:

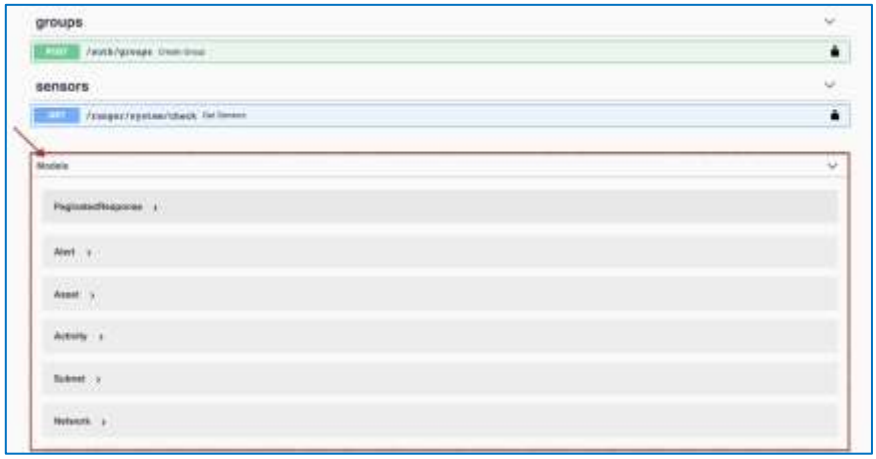


Figure 62 Models

4.3.5 Example of Get Asset Type - Exact Match

The following example shows how to retrieve an exact match:

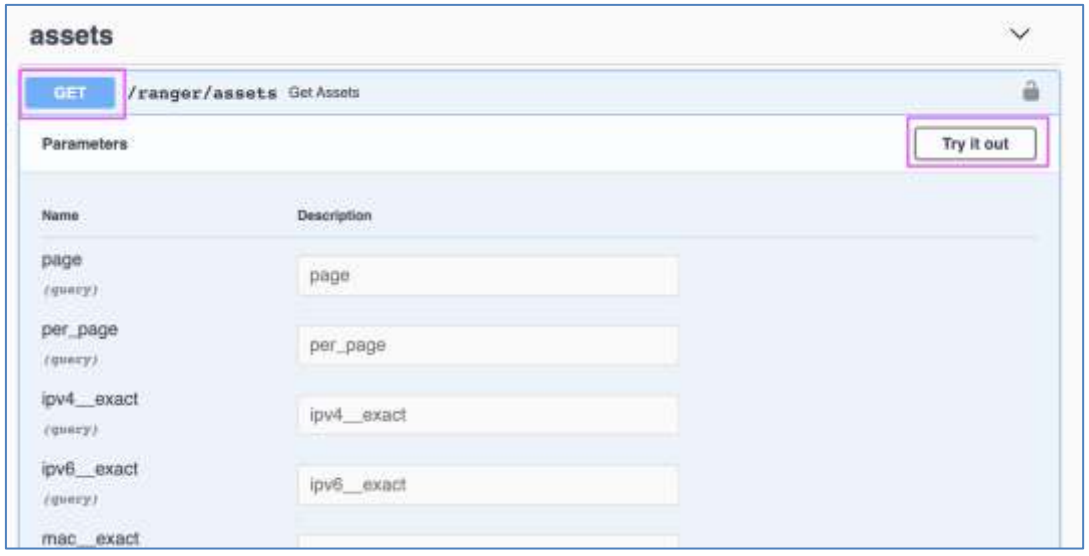


Figure 63 Get Assets method

1. Select the method to use (e.g. **Get Assets**)
2. Click **Try it Out** to make the method available
3. Select the filter you want. You can search for the filter, e.g:
   - `asset_type_exact`
4. Enter the filter you want using the separator, e.g.
   - `1,;$2,;$4,;$5`

Figure 64 Specifying an Asset Type - Exact Match

5. Press **Execute**
6. The system responds with:
   - the resulting CURL statement
   - the Request URL
   - the Server Response Body, which you can copy or download as a json file or copy

4.3.6 Example of Get Alerts

The following example shows how to retrieve all assets:

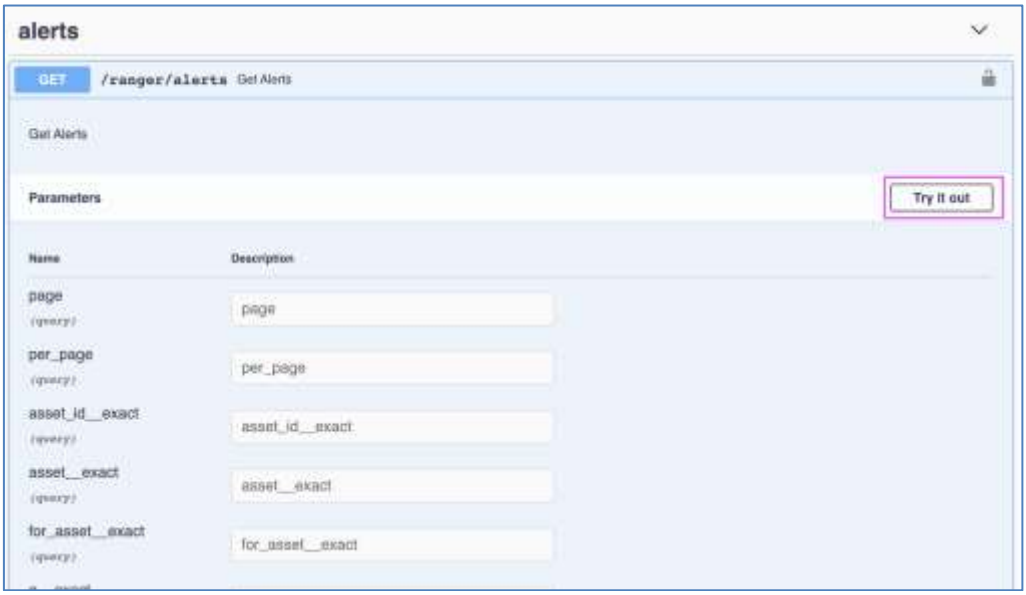


Figure 65 Get Alerts method

1. Open the **Get Alerts** method

2. Click **Try it Out**
3. Enter the filter/s you want, using the separators where needed, e.g.:

For Site ID = 1

For Severity Levels of 2 and 3

With Exact Resolved = false

With Qualified Alert = true

4. This selection runs the following command:

```
ranger/alerts?fields=
&format=alert_list
&sort=-score
&page=1
&per_page=20
&resolved__exact=false
&is_qualified__exact=true
&severity__exact=2,;$3
&site_id__exact=1
```

5. Press the **Execute** button at the bottom of the method
6. The system responds with:

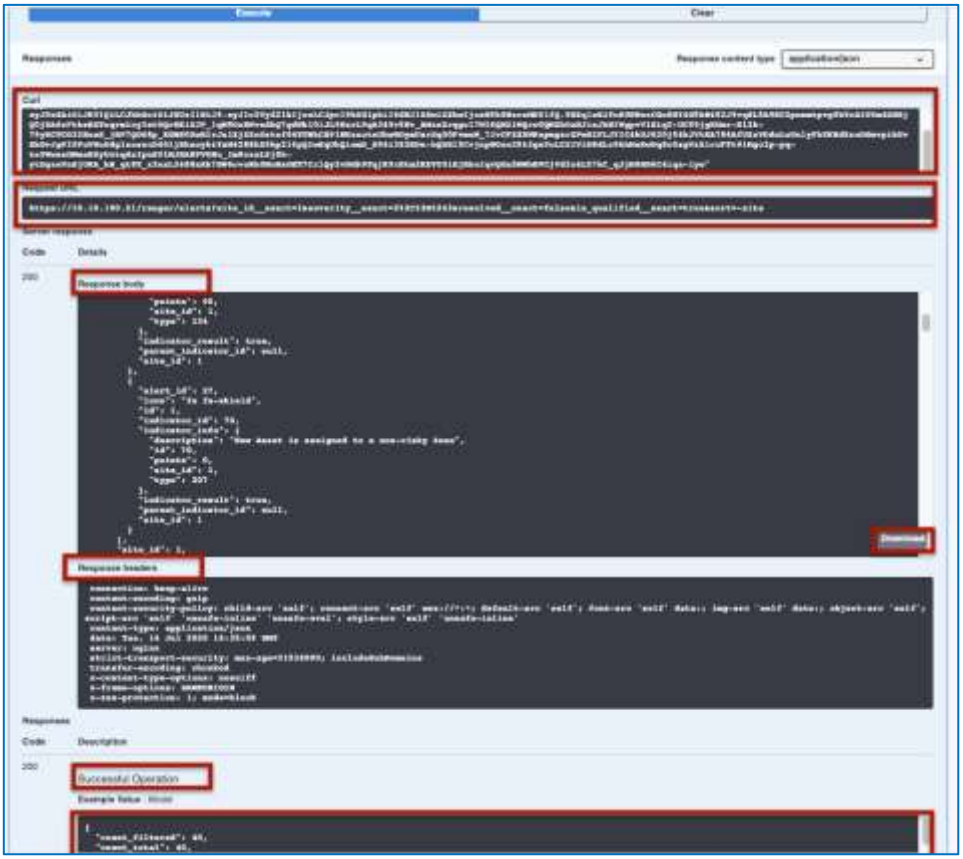


Figure 66 Get Alerts - Response

- The resulting CURL statement
- The Request URL
- The Server Response Body, which you can copy or download as a JSON file
- The Server Response Header
- The Code and Description, e.g. 200 Successful Operation
- The Example Value / Model

4.3.7 Example: Retrieve the Assets of an Insight

The following example shows how use the following sequence of functions to retrieve all the assets associated with a specific Insight, using the following sequence of methods:

- **GET /ranger/insights_summary**
- **GET /ranger/insight_details-{insight_name}**
- **GET /ranger/assets**

4.3.7.1 GET /ranger/insights_summary

1. Open the **GET /ranger/insights_summary** method
2. Click **Try it Out**
3. Apply the relevant site number in the field site_id__exact
4. Click **Execute**
5. From the Response body, select the insight of interest
   - e.g. `Assets Accessed SMB shares`
   - Copy the string of the insight name

4.3.7.2 GET /ranger/insight_details-{insight_name}

1. Open the **GET /ranger/insight_details-{insight_name}** method
2. Click **Try it Out**
3. Enter (paste) the insight name from above into the insight name field
4. Apply the relevant site number in the site_id__exact field
5. Click **Execute**
6. From the Response Body, select the filter_key
7. Copy the string of the filter_key

4.3.7.3 GET /ranger/assets

1. Open the **GET /ranger/assets** method
2. Click **Try it Out**
3. Enter (paste) the **filter_key** from above into the **INSIGHT_ROW_KEY_EXACT** field
4. Apply the relevant site number in the **site_id__exact** field
5. Enter **VALID_TRUE** to the **valid_exact** field in order to filter the assets accordingly
6. Enter **APPROVED_TRUE** to the **approved_exact** field in order to filter the assets accordingly
7. Enter other relevant filters as needed
8. Click **Execute**
   - The requested assets for this Insight appear in the Response Body

Figure 67 Get Assets for an Insight - Response

- The resulting CURL statement
- The Request URL
- The Server Response Body, which you can copy or download as a JSON file
- The Server Response Header
- The Code and Description, e.g. 200 Successful Operation
- The Example Value / Model

4.4 Syslog Specification

TIV can be configured to send syslog messages to external tools such as SIEM solutions, analytics tools, and log collectors. Syslog messages can be configured to be sent automatically for:

- Alerts and alert resolutions
- Events (of which an alert is composed)
- Baselines
- System status checks
- System health monitoring information.

The system sends raw information to syslog, allowing users to monitor the values and create alarms, analytics, and dashboards in other systems.

> Note Currently TLS 1.2 is supported through Syslog

4.4.1 Syslog Configuration

For information on Syslog configuration, see the *TIV User Guide: Configuring Syslog*.

4.4.2 Syslog Alert Examples

4.4.2.1 Known Threat Alert (CEF Format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Alert|Known Threat Alert|5| cn1Label=SiteId
cn1=1 cs1Label=Site cs1=Default cs2Label=Network cs2=Default
cs3Label=ResolvedAs cs3=Unresolved cs5Label=Src Zone cs5=Default Zone
cs6Label=Dst Zone cs6=Default Zone cs7Label=Category cs7=Security
cs8Label=AlertUrl cs8=https://<IP.Address>/detection/alert/1-1
outcome=Unresolved request= https://<IP.Address>/detection/alert/1-1
cn2Label=Alert Score cn2=100 cs10Label=PrimaryAssetIP cs10=10.5.22.101
cs11Label=PrimaryAssetType cs11=Endpoint
cs12Label=PrimaryAssetHostname cs12=N/A cs13Label=PrimaryAssetMAC
cs13=00:08:02:1c:47:ae cs14Label=PrimaryAssetOS cs14=Windows 7/Server
2008 R2 cs15Label=PrimaryAssetVendor cs15=Hewlett Packard
cs16Label=NonPrimaryAssetIP cs16=185.52.2.154
cs17Label=NonPrimaryAssetType cs17=Endpoint
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=20:e5:2a:b6:93:f1
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Netgear cn3Label=StoryId cn3=1  src=10.5.22.101
smac=00:08:02:1c:47:ae shost=N/A dst=185.52.2.154
dmac=20:e5:2a:b6:93:f1 dhost=N/A externalId=1 cat=Create rt=Nov 17
10:18:55 start=Oct 12 2020 17:28:33 msg=Out of working hours Known
Threat: Threat Claroty Rule: GranCrab Ransomware - C2 Certificate was
detected from 10.5.22.101 to 185.52.2.154
```

Table 71: Known Threat Alert

Name	Description	Value in Example
`Protocol`	The name of the syslog message format in use	`CEF:0`
`Vendor`	The name of the vendor of the product	`Claroty`
`Product`	The name of the product in use	`CTD`
`Product version`	The version number of the product in use	`4.2.3`
`Signature`	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	`Alert`
`Name`	The type of event.	`Known Threat Alert`
Severity	The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	`5` An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
`SiteID`	The ID of the site	`1`
Parameters	The format of the list of parameters is `csNLabel=<parameter name> csN=<value>` *where:* N is incremental according to the number of parameters	
`Site`	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	`Default`

Name	Description	Value in Example
Network	The network of the primary asset involved in the alert	Default
ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or Unresolved	Unresolved
Src Zone	The source zone	Default Zone
Dst Zone	The destination zone	Default Zone
Category	The type of event: Integrity or Security	Security
AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/1-1 outcome=Unresolved request= https://<IP.Address>/detection/alert/1-1
Alert Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**		
PrimaryAssetIP	The IP address of the primary asset	10.5.22.101
PrimaryAssetType	The asset type of the primary asset	Endpoint
PrimaryAssetHostname	The host name of the primary asset	N/A
PrimaryAssetMAC	The MAC address of the primary asset	cs13=00:08:02:1c:47:ae
PrimaryAssetOS	The OS of the primary asset	Windows 7/Server 2008 R2
PrimaryAssetVendor	The vendor of the primary asset	Hewlett Packard
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**		
NonPrimaryAssetIP	The IP address/es of the non-primary asset	185.52.2.154
NonPrimaryAssetType	The asset type/s of the non-primary asset	Endpoint
NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
NonPrimaryAssetMAC	The MAC address of the non-primary asset	20:e5:2a:b6:93:f1
NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Netgear
storyID	The ID of the story for this event	1
src	The IP address of the primary asset involved in the event	10.5.22.101
smac	The MAC address of the primary asset involved in the event	00:08:02:1c:47:ae
shost	The host name of the primary asset involved in the event	N/A
dst	The IP address of the secondary asset involved in the event	185.52.2.154
dmac	The MAC address of the secondary asset involved in the event	20:e5:2a:b6:93:f1
dhost	The host address of the secondary asset involved in the event	N/A
externalId	The ID of the alert which this event is part of.	1
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Update
rt	The timestamp of the current time (not of the alert)	Nov 17 10:18:55
start	The alert creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	Out of working hours Known Threat: Threat Claroty Rule: GranCrab Ransomware - C2 Certificate was detected from 10.5.22.101 to 185.52.2.154

4.4.2.2 Login Alert (CEF Format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Alert|Login|5| cn1Label=SiteId cn1=1
cs1Label=Site cs1=site-1 cs2Label=Network cs2=Default
cs3Label=ResolvedAs cs3=Unresolved cs5Label=Src Zone cs5=Endpoint:
Other cs6Label=Dst Zone cs6=Endpoint: Other cs7Label=Category
cs7=Security cs8Label=AlertUrl cs8=
https://<IP.Address>/detection/alert/14-1 outcome=Unresolved request=
https://<IP.Address>/detection/alert/14-1 cn2Label=Alert Score cn2=100
cs10Label=PrimaryAssetIP cs10=10.1.31.12 cs11Label=PrimaryAssetType
cs11=Endpoint cs12Label=PrimaryAssetHostname cs12=N/A
cs13Label=PrimaryAssetMAC cs13=00:50:56:8d:df:b8
cs14Label=PrimaryAssetOS cs14=N/A cs15Label=PrimaryAssetVendor
cs15=VMware cs16Label=NonPrimaryAssetIP cs16=10.1.31.1
cs17Label=NonPrimaryAssetType cs17=Endpoint
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=28:63:36:26:f0:74
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Siemens cn3Label=StoryId cn3=1 duser=N/A
destinationServiceName=S7COMM  src=10.1.31.12 smac=00:50:56:8d:df:b8
shost=N/A dst=10.1.31.1 dmac=28:63:36:26:f0:74 dhost=N/A externalId=14
cat=Security rt=Nov 17 10:18:55 start=Oct 12 2020 17:28:33 msg=Failed
Login: Failed Login attempts were made to asset 10.1.31.1 from
10.1.31.12
```

Table 72: Login Alert

Name		Description	Value in Example
Protocol		The name of the syslog message format in use	CEF:0
Vendor		The name of the vendor of the product	Claroty
Product		The name of the product in use	CTD
Product version		The version number of the product in use	4.2.3
Signature		The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name		The type of event.	Login
Severity		The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID		The ID of the site	1
Parameters		The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
	Site	The name of the site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	site-1
	Network	The network of the primary asset involved in the alert	Default
	ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or Unresolved	Unresolved

Name	Description	Value in Example
Src Zone	The source zone	Endpoint: Other
Dst Zone	The destination zone	Endpoint: Other
Category	The type of event: Integrity or Security	Security
AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/14-1 outcome=Unresolved request= https://<IP.Address>/detection/alert/14-1
Alert Score	The score for this alert	100

NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as:

ip1, ip2, ip3 …

PrimaryAssetIP	The IP address of the primary asset	10.1.31.12
PrimaryAssetType	The asset type of the primary asset	Endpoint
PrimaryAssetHostname	The host name of the primary asset	N/A
PrimaryAssetMAC	The MAC address of the primary asset	00:50:56:8d:df:b8
PrimaryAssetOS	The OS of the primary asset	N/A
PrimaryAssetVendor	The vendor of the primary asset	VMware

NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as:

asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;

NonPrimaryAssetIP	The IP address/es of the non-primary asset	10.1.31.1
NonPrimaryAssetType	The asset type/s of the non-primary asset	Endpoint
NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
NonPrimaryAssetMAC	The MAC address of the non-primary asset	28:63:36:26:f0:74
NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Siemens
storyID	The ID of the story for this event	1
duser	The username of this attempted login	N/A
destinationServiceName	The name of the destination service	S7COMM
src	The IP address of the primary asset involved in the event	10.1.31.12
smac	The MAC address of the primary asset involved in the event	00:50:56:8d:df:b8
shost	The host name of the primary asset involved in the event	N/A
dst	The IP address of the secondary asset involved in the event	10.1.31.1
dmac	The MAC address of the secondary asset involved in the event	28:63:36:26:f0:74
dhost	The host address of the secondary asset involved in the event	N/A
externalId	The ID of the alert which this event is part of.	14
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Security
rt	The timestamp of the current time (not of the alert)	Nov 17 10:18:55
start	The alert creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	Failed Login: Failed Login attempts were made to asset 10.1.31.1 from 10.1.31.12

4.4.2.3 Configuration Download Alert (CEF Format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Alert|Configuration Download|5|rt=Nov 01 2020
11:04:44 cn1Label=SiteId cn1=1 cs1Label=Site cs1=site-1
cs2Label=Network cs2=Default cs3Label=ResolvedAs cs3=Unresolved
cs5Label=Src Zone cs5=Engineering Station: Rockwell cs6Label=Dst Zone
cs6=PLC: Rockwell cs7Label=Category cs7=Integrity cs8Label=AlertUrl
cs8= https://<IP.Address>/detection/alert/40-1 outcome=Unresolved
request= https://<IP.Address>/detection/alert/40-1 cn2Label=Alert
Score cn2=100 cs10Label=PrimaryAssetIP cs10=10.1.30.40
cs11Label=PrimaryAssetType cs11=Engineering Station
cs12Label=PrimaryAssetHostname cs12=N/A cs13Label=PrimaryAssetMAC
cs13=00:50:56:b9:e2:ad cs14Label=PrimaryAssetOS cs14=N/A
cs15Label=PrimaryAssetVendor cs15=VMware cs16Label=NonPrimaryAssetIP
cs16=10.1.0.40,10.1.30.1 cs17Label=NonPrimaryAssetType cs17=PLC
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=00:1d:9c:c0:04:9d
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Rockwell Automation cn3Label=StoryId cn3=2  src=10.1.30.40
smac=00:50:56:b9:e2:ad shost=N/A dst=10.1.0.40 dmac=00:1d:9c:c0:04:9d
dhost=N/A externalId=40 cat=Integrity rt=Nov 17 10:18:55 start=Oct 12
2020 17:28:33 msg=Configuration Download: Configuration Download
critical change operation was performed for the first time by
10.1.30.40 on 10.1.30.1
```

Table 73: Configuration Download Alert

Name	Description	Value in Example
Protocol	The name of the syslog message format in use	CEF:0
Vendor	The name of the vendor of the product	Claroty
Product	The name of the product in use	CTD
Product version	The version number of the product in use	4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name	The type of event.	Login
Severity	The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
Timestamp	Timestamp of the alert	rt=Nov 01 2020 11:04:44
SiteID	The ID of the site	1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
Site	The name of the site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	site-1

Name	Description	Value in Example
Network	The network of the primary asset involved in the alert	Default
ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or Unresolved	Unresolved
Src Zone	The source zone	Engineering Station: Rockwell
Dst Zone	The destination zone	Rockwell
Category	The type of event: Integrity or Security	Integrity
AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/40-1 outcome=Unresolved request= https://<IP.Address>/detection/alert/40-1
Alert Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**		
PrimaryAssetIP	The IP address of the primary asset	10.1.30.40
PrimaryAssetType	The asset type of the primary asset	Engineering Station
PrimaryAssetHostname	The host name of the primary asset	N/A
PrimaryAssetMAC	The MAC address of the primary asset	cs13=00:50:56:b9:e2:ad
PrimaryAssetOS	The OS of the primary asset	N/A
PrimaryAssetVendor	The vendor of the primary asset	VMware
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**		
NonPrimaryAssetIP	The IP address/es of the non-primary asset	10.1.0.40,10.1.30.1
NonPrimaryAssetType	The asset type/s of the non-primary asset	PLC
NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
NonPrimaryAssetMAC	The MAC address of the non-primary asset	00:1d:9c:c0:04:9d
NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Rockwell Automation
storyID	The ID of the story for this event	2
src	The IP address of the primary asset involved in the event	10.1.30.40
smac	The MAC address of the primary asset involved in the event	00:50:56:b9:e2:ad
shost	The host name of the primary asset involved in the event	N/A
dst	The IP address of the secondary asset involved in the event	10.1.0.40
dmac	The MAC address of the secondary asset involved in the event	00:1d:9c:c0:04:9d
dhost	The host address of the secondary asset involved in the event	N/A
externalId	The ID of the alert which this event is part of.	40
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Integrity
rt	The timestamp of the current time (not of the alert)	Nov 17 10:18:55
start	The alert creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	Configuration Download: Configuration Download critical change operation was performed for the first time by 10.1.30.40 on 10.1.30.1

4.4.2.4 Host Scan Alert (CEF Format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Alert|Host Scan|5|cn1Label=SiteId cn1=7
cs1Label=Site cs1=ZZZ cs2Label=Network cs2=Default cs3Label=ResolvedAs
cs3=Unresolved cs5Label=Src Zone cs5=10.77.109.0/24 - Endpoint: Other
cs6Label=Dst Zone cs6=10.77.119.0/24 - Endpoint: Other
cs7Label=Category cs7=Security cs8Label=AlertUrl cs8=
https://<IP.Address>/detection/alert/286659-71 outcome=Unresolved
request= https://<IP.Address>/detection/alert/286659-71 cn2Label=Alert
Score cn2=100 cs10Label=PrimaryAssetIP cs10=10.77.109.112,10.77.109.9
cs11Label=PrimaryAssetType cs11=Endpoint
cs12Label=PrimaryAssetHostname cs12=Host-abc cs13Label=PrimaryAssetMAC
cs13=84:a9:3e:8c:57:d7,84:a9:3e:8c:6d:86,c8:d3:ff:bc:46:0c
cs14Label=PrimaryAssetOS cs14=Windows 10/Server 2016
cs15Label=PrimaryAssetVendor cs15=Hewlett Packard
cs16Label=NonPrimaryAssetIP cs16=Multiple Assets
cs17Label=NonPrimaryAssetType cs17=Multiple Assets
cs18Label=NonPrimaryAssetHostname cs18=Multiple Assets
cs19Label=NonPrimaryAssetMAC cs19=Multiple Assets
cs20Label=NonPrimaryAssetOS cs20=Multiple Assets
cs21Label=NonPrimaryAssetVendor cs21=Multiple Assets cn3Label=StoryId
cn3=58 {}src=10.77.109.112 smac=84:a9:3e:8c:57:d7 shost= ABC-DEF
dst=Multiple Assets dmac=c4:34:6b:62:60:b7 dhost= GHI-JKL
externalId=999999 cat=Create rt=Nov 17 10:18:55 start=Oct 12 2020
17:28:33 msg=TCP Host scan: Asset 10.77.109.9 sent packets to
different IP destinations on the same port: 7680
```

Table 74: Host Scan Alert

Name		Description	Value in Example
Protocol		The name of the syslog message format in use	CEF:0
Vendor		The name of the vendor of the product	Claroty
Product		The name of the product in use	CTD
Product version		The version number of the product in use	4.2.3
Signature		The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name		The type of event.	Host Scan
Severity		The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID		The ID of the site	7
Parameters		The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
	Site	The name of the site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	ZZZ
	Network	The network of the primary asset involved in the alert	Default

Name	Description	Value in Example
ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or Unresolved	Unresolved
Src Zone	The source zone	10.77.109.0/24 - Endpoint: Other
Dst Zone	The destination zone	10.77.119.0/24 - Endpoint: Other
Category	The type of event: Integrity or Security	Security
AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/286659-71 outcome=Unresolved request= https://<IP.Address>/detection/alert/
Alert Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**		
PrimaryAssetIP	The IP address of the primary asset	10.77.109.112, 10.77.109.9
PrimaryAssetType	The asset type of the primary asset	Endpoint
PrimaryAssetHostname	The host name of the primary asset	Host-abc
PrimaryAssetMAC	The MAC address of the primary asset	84:a9:3e:8c:57:d7, 84:a9:3e:8c:6d:86, c8:d3:ff:bc:46:0c
PrimaryAssetOS	The OS of the primary asset	Windows 10/Server 2016
PrimaryAssetVendor	The vendor of the primary asset	Hewlett Packard
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**		
NonPrimaryAssetIP	The IP address/es of the non-primary asset	Multiple Assets
NonPrimaryAssetType	The asset type/s of the non-primary asset	Multiple Assets
NonPrimaryAssetHostname	The host name/s of the non-primary asset	Multiple Assets
NonPrimaryAssetMAC	The MAC address of the non-primary asset	Multiple Assets
NonPrimaryAssetOS	The OS/es of the non-primary asset	Multiple Assets
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Multiple Assets
storyID	The ID of the story for this event	58 {}
src	The IP address of the primary asset involved in the event	10.77.109.112
smac	The MAC address of the primary asset involved in the event	84:a9:3e:8c:57:d7
shost	The host name of the primary asset involved in the event	ABC-DEF
dst	The IP address of the secondary asset involved in the event *NOTE:* In scan alert types, the dst asset data is "multiple assets" to avoid spam and to comply with the CEF format	Multiple Assets
dmac	The MAC address of the secondary asset involved in the event	c4:34:6b:62:60:b7
dhost	The host address of the secondary asset involved in the event	GHI-JKL
externalId	The ID of the alert which this event is part of.	999999
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Create
rt	The timestamp of the current time (not of the alert)	Nov 17 10:18:55
start	The alert creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	TCP Host scan: Asset 10.77.109.9 sent packets to different IP destinations on the same port: 7680

4.4.2.5 Suspicious File Transfer Alert (CEF Format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Alert|Suspicious File Transfer|5|rt=Nov 01
2020 11:04:44 cn1Label=SiteId cn1=1 cs1Label=Site cs1=Default
cs2Label=Network cs2=Default cs3Label=ResolvedAs cs3=Unresolved
cs5Label=Src Zone cs5=Endpoint: Other cs6Label=Dst Zone cs6=Endpoint:
Other cs7Label=Category cs7=Security cs8Label=AlertUrl cs8=
https://<IP.Address>/detection/alert/60-1 outcome=Unresolved request=
https://<IP.Address>/detection/alert/60-1 cn2Label=Alert Score cn2=100
cs10Label=PrimaryAssetIP cs10=10.20.6.205 cs11Label=PrimaryAssetType
cs11=Endpoint cs12Label=PrimaryAssetHostname cs12=N/A
cs13Label=PrimaryAssetMAC cs13=f0:18:98:66:5a:0c
cs14Label=PrimaryAssetOS cs14=N/A cs15Label=PrimaryAssetVendor
cs15=Apple cs16Label=NonPrimaryAssetIP cs16=10.10.10.10
cs17Label=NonPrimaryAssetType cs17=Endpoint
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=N/A cs20Label=NonPrimaryAssetOS
cs20=N/A cs21Label=NonPrimaryAssetVendor cs21=N/A cn3Label=StoryId
cn3=4
filePath=/private/var/lib/icsranger/master/workers/known_threats/yara_
exported_files/matched_yara_files/1/smb/1597600276270606_0.bin
src=10.20.6.205 smac=f0:18:98:66:5a:0c shost=N/A dst=10.10.10.10
dmac=N/A dhost=N/A externalId=60 cat=Create rt=Nov 17 10:18:55
start=Oct 12 2020 17:28:33 msg=Suspicious file transfer found! File
'/Teams/QA/all/imain.bin' was transferred via 'smb' and matched the
following Yara rules: ['ics_cert_hatman.yara/hatman_payload',
'ics_cert_hatman.yara/hatman'], Transferred from 10.20.6.205
```

Table 75: Suspicious File Transfer Alert

Name		Description	Value in Example
Protocol		The name of the syslog message format in use	CEF:0
Vendor		The name of the vendor of the product	Claroty
Product		The name of the product in use	CTD
Product version		The version number of the product in use	4.2.3
Signature		The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name		The type of event.	Suspicious File Transfer
Severity		The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
	SiteID	The ID of the site	1
Parameters		The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
	Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	Default

Name	Description		Value in Example
	Network	The network of the primary asset involved in the alert	Default
	ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or Unresolved	Unresolved
	Src Zone	The source zone	Endpoint: Other
	Dst Zone	The destination zone	Endpoint: Other
	Category	The type of event: Integrity or Security	Security
	AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/60-1 outcome=Unresolved request= https://<IP.Address>/detection/alert/60-1
	Alert Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**			
	PrimaryAssetIP	The IP address of the primary asset	10.20.6.205
	PrimaryAssetType	The asset type of the primary asset	Endpoint
	PrimaryAssetHostname	The host name of the primary asset	N/A
	PrimaryAssetMAC	The MAC address of the primary asset	f0:18:98:66:5a:0c
	PrimaryAssetOS	The OS of the primary asset	N/A
	PrimaryAssetVendor	The vendor of the primary asset	Apple
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**			
	NonPrimaryAssetIP	The IP address/es of the non-primary asset	10.10.10.10
	NonPrimaryAssetType	The asset type/s of the non-primary asset	Endpoint
	NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
	NonPrimaryAssetMAC	The MAC address of the non-primary asset	N/A
	NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
	NonPrimaryAssetVendor	The vendor/s of the non-primary asset	N/A
storyID	The ID of the story for this event		4
filepath	The filepath for the suspicious file transfer		/private/var/lib/icsranger/master/workers/known_threats/yara_exported_files/matched_yara_files/1/smb/1597600276270606_0.bin
src	The IP address of the primary asset involved in the event		10.20.6.205
smac	The MAC address of the primary asset involved in the event		f0:18:98:66:5a:0c
shost	The host name of the primary asset involved in the event		N/A
dst	The IP address of the secondary asset involved in the event		10.10.10.10
dmac	The MAC address of the secondary asset involved in the event		N/A
dhost	The host address of the secondary asset involved in the event		N/A
externalId	The ID of the alert which this event is part of.		60
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)		Create
rt	The timestamp of the current time (not of the alert)		Nov 17 10:18:55
start	The alert creation timestamp		Oct 12 2020 17:28:33
msg	The message containing the description of the event		Suspicious file transfer found! File '/Teams/QA/all/imain.bin' was transferred via 'smb' and matched the following Yara rules: ['ics_cert_hatman.yara/hatman_payload', 'ics_cert_hatman.yara/hatman'], Transferred from 10.20.6.205

4.4.2.6 New Asset Alert (CEF format)

Syslog Message String

```
CEF:0|Test_Brand|CTD|4.2.3|Alert|New Asset|5| cn1Label=SiteId cn1=1
cs1Label=Site cs1=Default cs2Label=Network cs2=Default
cs3Label=ResolvedAs cs3=Unresolved cs4Label=SiteId cs4=1
cs5Label=SrcZone cs5=Endpoint: Other cs6Label=DstZone cs6=Endpoint:
Other cs7Label=Category cs7=Integrity cs8Label=AlertUrl cs8=
https://<IP.Address>/detection/alert/105-1 cs9Label=Score cs9=80
cs10Label=PrimaryAssetIP cs10=10.10.6.121 cs11Label=PrimaryAssetType
cs11=Endpoint cs12Label=PrimaryAssetHostname cs12=N/A
cs13Label=PrimaryAssetMAC cs13=N/A cs14Label=PrimaryAssetOS cs14=N/A
cs15Label=PrimaryAssetVendor cs15=N/A cs16Label=NonPrimaryAssetIP
cs16=10.20.10.166 cs17Label=NonPrimaryAssetType cs17=Endpoint
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=ac:bc:32:d1:40:b7
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=N/A cs22Label=StoryId cs22=2 src=10.10.6.121 smac=N/A shost=N/A
dst=10.20.10.166 dmac=ac:bc:32:d1:40:b7 dhost=N/A externalId=105
cat=Create rt=Nov 17 10:18:55 start=Oct 12 2020 17:28:33 msg=A new
asset has been detected: 10.10.6.121.
```

Table 76: New Asset Alert

Name	Description	Value in Example
Protocol	The name of the syslog message format in use	CEF:0
Vendor	The name of the vendor of the product	Test_Brand
Product	The name of the product in use	CTD
Product version	The version number of the product in use	4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Alert
Name	The type of alert. There are several types of alerts (e.g. 'baseline deviation', 'new asset', 'configuration downloaded to PLC', 'known attack signature detected', etc. See Appendix A for common alerts.	New Asset
Severity	The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID	The ID of the site	1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters.	
Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	Default
Network	The network of the primary asset involved in the alert	Default
ResolvedAs	How the alert was treated; whether or not the alert was resolved: (Resolved or UnResolved)	UnResolved
SiteID	The ID of the site	1
SrcZone	The source zone	Endpoint: Other
DstZone	The destination zone	Endpoint: Other

Name	Description		Value in Example
	Category	The type of event: Integrity or Security	Integrity
	AlertUrl	The URL for this alert	https://<IP.Address>/detection/alert/105-1
	Score	The alert score for this alert	80
	NOTE: **The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as:** `ip1, ip2, ip3 ...`		
	PrimaryAssetIP	The IP address of the primary asset	10.10.6.121
	PrimaryAssetType	The asset type of the primary asset	Endpoint
	PrimaryAssetHostname	The host name of the primary asset	N/A
	PrimaryAssetMAC	The MAC address of the primary asset	N/A
	PrimaryAssetOS	The OS of the primary asset	N/A
	PrimaryAssetVendor	The vendor of the primary asset	N/A
	NOTE: **The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as:** `asset1_ip1, asset1_ip2, asset1_ip3, ...; asset2_ip1, asset2_ip2, asset2_ip3, ...;`		
	NonPrimaryAssetIP	The IP address of the non-primary asset	10.20.10.166
	NonPrimaryAssetType	The asset type of the non-primary asset	Endpoint
	NonPrimaryAssetHostname	The host name of the non-primary asset	N/A
	NonPrimaryAssetMAC	The MAC address of the non-primary asset	ac:bc:32:d1:40:b7
	NonPrimaryAssetOS	The OS of the non-primary asset	N/A
	NonPrimaryAssetVendor	The vendor of the non-primary asset	N/A
StoryID	The ID of the story (i.e. the chain of events that provide the context for this alert)		2
src	A randomly selected IP address of the primary asset involved in the alert *		10.10.6.121
smac	A randomly selected MAC address of the primary asset involved in the alert *	*	N/A
shost	A randomly selected host name (if known) of the primary asset involved in the alert*	Note that the asset may have additional addresses	N/A
dst	A randomly selected IP address of the secondary asset involved in the alert *		10.20.10.166
dmac	A randomly selected MAC address of the secondary asset involved in the alert *		ac:bc:32:d1:40:b7
dhost	A randomly selected host name (if known) of the secondary asset involved in the alert *		N/A
externalId	The ID of the corresponding alert. For example: An event with externalId 7 is associated with an alert with externalId 7		105
cat	The type of notification, depending on whether this event: • Is a new event in the system (Create) *or* • Is an existing event being updated (Update)		Create
rt	The timestamp of the current time (not of the alert)		Nov 17 10:18:55
start	The alert creation timestamp		Oct 12 2020 17:28:33
msg	The message containing the description of the alert		A new asset has been detected: 10.10.6.121

4.4.3 Syslog Event Examples

4.4.3.1 Known Threat Event (CEF format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Event|Known Threat Event|5|rt=Nov 01 2020
11:04:44 cn1Label=SiteId cn1=1 cs1Label=Site cs1=Default
cs2Label=Network cs2=Default cs3Label=ResolvedAs cs3=Unresolved
cs5Label=Src Zone cs5=Default Zone cs6Label=Dst Zone cs6=Default Zone
cs7Label=Category cs7=Security cs8Label=AlertUrl
cs8=http://localhost:4200/alert/1-1 outcome=Unresolved
request=http://localhost:4200/alert/1-1 cn2Label=Alert Score cn2=100
cs10Label=PrimaryAssetIP cs10=10.5.22.101 cs11Label=PrimaryAssetType
cs11=Endpoint cs12Label=PrimaryAssetHostname cs12=N/A
cs13Label=PrimaryAssetMAC cs13=00:08:02:1c:47:ae
cs14Label=PrimaryAssetOS cs14=Windows 7/Server 2008 R2
cs15Label=PrimaryAssetVendor cs15=Hewlett Packard
cs16Label=NonPrimaryAssetIP cs16=185.52.2.154
cs17Label=NonPrimaryAssetType cs17=Endpoint
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=20:e5:2a:b6:93:f1
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Netgear cn3Label=StoryId cn3=1  src=10.5.22.101
smac=00:08:02:1c:47:ae shost=N/A dst=185.52.2.154
dmac=20:e5:2a:b6:93:f1 dhost=N/A externalId=1 cat=Update rt=Nov 17
10:18:55 start=Oct 12 2020 17:28:33 msg=Claroty Rule: GranCrab
Ransomware - C2 Certificate (10.5.22.101:49201 -> 185.52.2.154:443).
Signature:  content:"www|2e|kakaocorp|2e|link"; depth:200;
```

Table 77: Known Threat Event

Name	Description	Value in Example
`Protocol`	The name of the syslog message format in use	`CEF:0`
`Vendor`	The name of the vendor of the product	`Claroty`
`Product`	The name of the product in use	`CTD`
`Product version`	The version number of the product in use	`4.2.3`
`Signature`	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	`Event`
`Name`	The type of event.	`Known Threat Event`
Severity	The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	`5` An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
`SiteID`	The ID of the site	`1`
Parameters	The format of the list of parameters is `csNLabel=<parameter name> csN=<value>` *where:* N is incremental according to the number of parameters	

Name	Description		Value in Example
	SiteID	The ID of the site	1
	Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	Default
	Network	The network of the primary asset involved in the alert	Default
	ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or Unresolved	Unresolved
	SrcZone	The source zone	Default Zone
	DstZone	The destination zone	Default Zone
	Category	The type of event: Integrity or Security	Security
	AlertUrl	The URL for this alert	http://localhost:4200/alert/1-1 outcome=Unresolved request=http://localhost:4200/alert/1-1
	Alert Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**			
	PrimaryAssetIP	The IP address of the primary asset	10.5.22.101
	PrimaryAssetType	The asset type of the primary asset	Endpoint
	PrimaryAssetHostname	The host name of the primary asset	N/A
	PrimaryAssetMAC	The MAC address of the primary asset	cs13=00:08:02:1c:47:ae
	PrimaryAssetOS	The OS of the primary asset	Windows 7/Server 2008 R2
	PrimaryAssetVendor	The vendor of the primary asset	Hewlett Packard
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**			
	NonPrimaryAssetIP	The IP address/es of the non-primary asset	185.52.2.154
	NonPrimaryAssetType	The asset type/s of the non-primary asset	Endpoint
	NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
	NonPrimaryAssetMAC	The MAC address of the non-primary asset	20:e5:2a:b6:93:f1
	NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
	NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Netgear
storyID	The ID of the story for this event		1
src	The IP address of the primary asset involved in the event		10.5.22.101
smac	The MAC address of the primary asset involved in the event		00:08:02:1c:47:ae
shost	The host name of the primary asset involved in the event		N/A
dst	The IP address of the secondary asset involved in the event		185.52.2.154
dmac	The MAC address of the secondary asset involved in the event		20:e5:2a:b6:93:f1
dhost	The host address of the secondary asset involved in the event		N/A
externalId	The ID of the alert which this event is part of.		1
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)		Update
rt	The timestamp of the current time (not of the alert)		Nov 17 10:18:55
start	The alert creation timestamp		Oct 12 2020 17:28:33
msg	The message containing the description of the event		Claroty Rule: GranCrab Ransomware - C2 Certificate (10.5.22.101:49201 -> 185.52.2.154:443). Signature: content:"www|2e|kakaocorp|2e|link"; depth:200;

4.4.3.2 Baseline Deviation Event (CEF format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Event|Baseline Deviation|5|rt=Nov 01 2020
11:04:44 cn1Label=SiteId cn1=1 cs1Label=Site cs1=site-2
cs2Label=Network cs2=Default cs3Label=ResolvedAs cs3=Unresolved
cs4Label=SiteId cs4=2 cs5Label=SrcZone cs5=Engineering Station:
Rockwell cs6Label=DstZone cs6=PLC: Rockwell cs7Label=Category
cs7=Integrity cs8Label=AlertUrl cs8=https://10.91.1.186:5000/alert/25-
2 cs9Label=Score cs9=100 cs10Label=PrimaryAssetIP cs10=10.1.30.40
cs11Label=PrimaryAssetType cs11=Engineering Station
cs12Label=PrimaryAssetHostname cs12=N/A cs13Label=PrimaryAssetMAC
cs13=00:50:56:b9:e2:ad cs14Label=PrimaryAssetOS cs14=N/A
cs15Label=PrimaryAssetVendor cs15=VMware cs16Label=NonPrimaryAssetIP
cs16=10.1.0.40,10.1.30.1 cs17Label=NonPrimaryAssetType cs17=PLC
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=00:1d:9c:c0:04:9d
cs20Label=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Rockwell Automation cs22Label=StoryId cs22=3 src=10.1.30.40
smac=00:50:56:b9:e2:ad shost=N/A dst=10.1.0.40 dmac=00:1d:9c:c0:04:9d
dhost=N/A externalId=25 cat=Update rt=Nov 17 10:18:55 start=Oct 12
2020 17:28:33 msg=CIP : Service Get Attribute All called on
ExtendedDevice
```

Table 78: Baseline Deviation Event

Name		Description	Value in Example
Protocol		The name of the syslog message format in use	CEF:0
Vendor		The name of the vendor of the product	Claroty
Product		The name of the product in use	CTD
Product version		The version number of the product in use	4.2.3
Signature		The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Event
Name		The type of event.	Baseline Deviation
Severity		The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID		The ID of the site	1
Parameters		The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where*: N is incremental according to the number of parameters	
	Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	site-2
	Network	The network of the primary asset involved in the alert	Default
	ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or UnResolved	UnResolved
	SiteID	The ID of the site	2

Name	Description	Value in Example
SrcZone	The source zone	Engineering Station: Rockwell
DstZone	The destination zone	PLC: Rockwell
Category	The type of event: Integrity or Security	Integrity
AlertUrl	The URL for this alert	https://10.91.1.186:5000/alert/25-2
Score	The score for this alert	100
NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **ip1, ip2, ip3 …**		
PrimaryAssetIP	The IP address of the primary asset	10.1.30.40
PrimaryAssetType	The asset type of the primary asset	Engineering Station
PrimaryAssetHostname	The host name of the primary asset	N/A
PrimaryAssetMAC	The MAC address of the primary asset	00:50:56:b9:e2:ad
PrimaryAssetOS	The OS of the primary asset	N/A
PrimaryAssetVendor	The vendor of the primary asset	VMware
NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: **asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;**		
NonPrimaryAssetIP	The IP address/es of the non-primary asset	10.1.0.40,10.1.30.1
NonPrimaryAssetType	The asset type/s of the non-primary asset	PLC
NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
NonPrimaryAssetMAC	The MAC address of the non-primary asset	00:1d:9c:c0:04:9d
NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Rockwell Automation
storyID	The ID of the story for this alert	3
src	The IP address of the primary asset involved in the event	10.1.30.40
smac	The MAC address of the primary asset involved in the event	00:50:56:b9:e2:ad
shost	The host name of the primary asset involved in the event	N/A
dst	The IP address of the secondary asset involved in the event	10.1.0.40
dmac	The MAC address of the secondary asset involved in the event	00:1d:9c:c0:04:9d
dhost	The host address of the secondary asset involved in the event	N/A
externalId	The ID of the alert which this event is part of.	25
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)	Update
rt	The timestamp of the current time (not of the baseline)	Nov 17 10:18:55
start	The baseline creation timestamp	Oct 12 2020 17:28:33
msg	The message containing the description of the event	CIP : Service Get Attribute All called on ExtendedDevice

4.4.3.3 Protocol Specific OT Alert (CEF format)

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|Event|Protocol|5|rt=Nov 01 2020 11:04:44
cn1Label=SiteId cn1=1 cs1Label=Site cs1=site-2 cs2Label=Network
cs2=Default cs3Label=Resolved
As cs3=Unresolved cs4Label=SiteId cs4=2 cs5Label=SrcZone
cs5=Engineering Station: Rockwell cs6Label=DstZone cs6=PLC: Rockwell
cs7Label=Category cs7=Integrity cs8Label=AlertUrl
cs8=https://10.91.1.186:5000/alert/25-2 cs9Label=Score cs9=100
cs10Label=PrimaryAssetIP cs10=10.1.30.40 cs11Label=PrimaryAssetType
cs11=Engineering Station cs12Label=Prim
aryAssetHostname cs12=N/A cs13Label=PrimaryAssetMAC
cs13=00:50:56:b9:e2:ad cs14Label=PrimaryAssetOS cs14=N/A
cs15Label=PrimaryAssetVendor cs15=VMware cs16Label=NonPrimaryAss
etIP cs16=10.1.0.40,10.1.30.1 cs17Label=NonPrimaryAssetType cs17=PLC
cs18Label=NonPrimaryAssetHostname cs18=N/A
cs19Label=NonPrimaryAssetMAC cs19=00:1d:9c:c0:04:9d cs20Label
=NonPrimaryAssetOS cs20=N/A cs21Label=NonPrimaryAssetVendor
cs21=Rockwell Automation cs22Label=StoryId cs22=3 src=10.1.30.40
smac=00:50:56:b9:e2:ad shost=N/A dst=10.1.0.40 d
mac=00:1d:9c:c0:04:9d dhost=N/A externalId=25 cat=Update rt=Nov 17
10:18:55 start=Oct 12 2020 17:28:33 msg=Editing was done on DataTable
object (Operation: Create Instance).format(ctd_version, site_name,
alertURL)
```

Table 79: Protocol Specific OT Alert

Name	Description	Value in Example
Protocol	The name **of the syslog** message format in use	CEF:0
Vendor	The name of the vendor of the product	Claroty
Product	The name of the product in use	CTD
Product version	The version number of the product in use	4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	Event
Name	The type of event.	Protocol
Severity	The degree of impact of the alert, represented as an integer ranging from 2 to 5 where the Severity scale is as follows: ▪ 2 = Low severity ▪ 3 = Medium severity ▪ 4 = High severity ▪ 5 = Critical severity	5 An alert is considered critical if its calculated score is in the highest 20% of the section above the threshold.
SiteID	The ID of the site	1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters	
Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	site-2
Network	The network of the primary asset involved in the alert	Default
ResolvedAs	How the event was treated; whether or not the event was resolved: ▪ Resolved or UnResolved	UnResolved
SiteID	The ID of the site	2
SrcZone	The source zone	Engineering Station: Rockwell

Name	Description		Value in Example
	DstZone	The destination zone	PLC: Rockwell
	Category	The type of event: ▪ Integrity or Security	Integrity
	AlertUrl	The URL for this alert	https://10.91.1.186:5000/alert/25-2
	Score	The score of this event	100
	NOTE: The Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: ip1, ip2, ip3 …		
	PrimaryAssetIP	The IP address of the primary asset	10.1.30.40
	PrimaryAssetType	The asset type of the primary asset	Engineering Station
	PrimaryAssetHostname	The host name of the primary asset	N/A
	PrimaryAssetMAC	The MAC address of the primary asset	00:50:56:b9:e2:ad
	PrimaryAssetOS	The OS of the primary asset	N/A
	PrimaryAssetVendor	The vendor of the primary asset	VMware
	NOTE: The Non-Primary IP, hostname and MAC parameters support multiple values, with the full list of asset addresses output as: asset1_ip1, asset1_ip2, asset1_ip3, …; asset2_ip1, asset2_ip2, asset2_ip3, …;		
	NonPrimaryAssetIP	The IP address/es of the non-primary asset	10.1.0.40,10.1.30.1
	NonPrimaryAssetType	The asset type/s of the non-primary asset	PLC
	NonPrimaryAssetHostname	The host name/s of the non-primary asset	N/A
	NonPrimaryAssetMAC	The MAC address/es of the non-primary asset	00:1d:9c:c0:04:9d
	NonPrimaryAssetOS	The OS/es of the non-primary asset	N/A
	NonPrimaryAssetVendor	The vendor/s of the non-primary asset	Rockwell Automation
StoryId			3
src	The ID of the story (i.e. the chain of events that provide the context for this event)		10.1.30.40
smac	The MAC address of the primary asset involved in the event		00:50:56:b9:e2:ad
shost	The host name of the primary asset involved in the event		N/A
dst	The IP address of the secondary asset involved in the event		10.1.0.40
dmac	The MAC address of the secondary asset involved in the event		00:1d:9c:c0:04:9d
dhost	The host address of the secondary asset involved in the event		N/A
externalId	The ID of the alert which this event is part of.		25
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)		Update
rt	The timestamp of the current time (not of the alert)		Nov 17 10:18:55
start	The alert creation timestamp		Oct 12 2020 17:28:33
msg	The message containing the description of the event		Editing was done on DataTable object (Operation: Create Instance).format(ctd_version, site_name, alertURL)

4.4.4 Syslog New Baseline Examples

Syslog Message String (CEF format)

```
CEF:0|Claroty|CTD|4.2.3|Baseline|None|1|rt=Nov 01 2020 11:04:44
cn1Label=SiteId cn1=1 cs1Label=Site cs1=Default cs2Label=Network
cs2=Default cs3Label=Transmission cs3=None cs5Label=Src Zone cs5=Default
Zone cs6Label=Dst Zone cs6=Default Zone cs7Label=Category cs7=Network
cs8Label=CategoryAccess cs8=None cs9Label=Frequency cs9=NotTimed
cs10Label=FirstSeen cs10=Aug 16 2020 17:50:52 src=N/A
smac=00:80:f4:12:8b:10 shost=N/A dst=N/A dmac=ff:ff:ff:ff:ff:ff dhost=N/A
externalId=41 cat=Create rt=Aug 16 2020 17:50:52 msg=ARP : Gratuitous ARP
for ipv4 address 84.18.139.16 with mac address 00:80:f4:12:8b:10
```

Table 80: Baseline Example

Name	Description		Value in Example
Protocol	The name of the syslog message format in use		CEF
Vendor	The name of the vendor of the product		Claroty
Product	The name of the product in use		CTD
Product version	The version number of the product in use		4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck		Baseline
Name	The type of baseline		None
Approved	Whether this baseline is approved or not, represented as an integer of 0 or 1 where: ▪ 0 = Baseline Approved ▪ 1 = Baseline Unapproved		1
SiteID	The ID of the site		1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value> *where:* N is incremental according to the number of parameters		
	SiteID	The ID of the site	1
	Site	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	Default
	Network	The network involved	Default
	Transmission	The type of transmission protocol in use	None
	Src Zone	The source Virtual Zone	Default Zone
	Dst Zone	The destination Virtual Zone	Default Zone
	Category	The type of alert: ▪ Integrity/Security/Network/Other For baseline the category shall be Network	Network
	CategoryAccess	Access type: None, Read, Write, Execute, Publish	None
	Frequency	Frequency of recurrence if timed. Otherwise: NotTimed	NotTimed
	FirstSeen	Timestamp of when the baseline was first detected	Aug 16 2020 17:50:52
src	The IP address of the primary asset involved in the event		N/A
smac	The MAC address of the primary asset involved in the event		00:80:f4:12:8b:10
shost	The host name of the primary asset involved in the event		N/A
dst	The IP address of the secondary asset involved in the event		N/A
dmac	The MAC address of the secondary asset involved in the event		ff:ff:ff:ff:ff:ff
dhost	The host address of the secondary asset involved in the event		N/A
externalId	The ID of the alert which this event is part of.		41
cat	The type of notification, depending on whether this event is a new event in the system (Create) or an existing event being updated (Update)		Create
rt	The timestamp of the current time (not of the alert)		Nov 17 10:18:55
msg	The message containing the description of the status check		msg=ARP : Gratuitous ARP for ipv4 address 84.18.139.16 with mac address 00:80:f4:12:8b:10

4.4.5 Syslog Sniffer Status Check Example

This is a type of system event.

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|SnifferStatus|SnifferStatus|3|rt=Nov 01 2020
11:04:44 cn1Label=SiteId cn1=1 cs1Label=SiteName cs1=site-1
cs2Label=SiteId cs2=1 cs3Label=InterfaceName cs3=ens224
cs4Label=Network cs4=Default cs5Label=IPaddress cs5=10.10.6.207
cs6Label=SnifferStatus cs6=down rt=Jul 15 2020 09:04:53 msg=interface
ens224 is currently not receiving any packets
```

Table 81: Sniffer Status Alert

Name	Description	Value in Example
Protocol	The name of the syslog message format in use	CEF:0
Vendor	The name of the vendor of the product	Claroty
Product	The name of the product in use	CTD
Product version	The version number of the product in use	4.2.3
Signature	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/Health Check	SnifferStatus
Name	The name of the message	Sniffer Status
Severity	The severity of the status message For a Sniffer Status alert, the Severity is always 3. For a Site Status alert: • Site Down = 8 • Site Up = 0	
SiteID	The ID of the site	1
Parameters	The format of the list of parameters is csNLabel=<parameter name> csN=<value>, *where:* N is incremental according to the number of parameters.	
Site Name	The site from which the message is being sent. When an alert/event involves more than one asset this parameter will hold the site name of the primary asset involved in the alert/event.	site-1
Site ID	The ID of the site	1
Interface Name	The name of the interface in use	Ens224
Network	The network involved	Default
IPaddress	The IP address involved	10.10.6.207
Sniffer Status	Whether the sniffer is currently active: ▪ Up or Down	down
rt	The timestamp of the status check	Jul 15 2020 09:04:53
msg	The message containing the description of the status check	interface ens224 is currently not receiving any packets

4.4.6 Syslog Health Check Monitoring Example

Below is an example of a Syslog message for Health Check monitoring. Note that this message structure is dependent on your environment and on your TIV

configuration. For example, Site output will differ from Central output; as there are no dissectors in the EMC.

> **Note** The labelling in the values in this example changes according to the user's running environment.

Syslog Message String

```
CEF:0|Claroty|CTD|4.2.3|HealthCheck| cn1Label=SiteId cn1=1
cs1Label=Site cs1=Default cs2Label=cpu cs2=0.19 cs3Label=mem cs3=54.3
cs4Label=used__opt_icsranger cs4=9.23 cs5Label=used__var cs5=9.23
cs6Label=used__tmp cs6=9.23 cs7Label=used__etc cs7=9.23
cs8Label=busy_sda cs8=0.84 cs9Label=busy_sda1 cs9=0.0
cs10Label=busy_sda2 cs10=0.84 cs11Label=busy_sr0 cs11=0.0
cs12Label=busy_dm-0 cs12=0.93 cs13Label=busy_sdb cs13=0.19
cs14Label=busy_sdb1 cs14=0.19 cs15Label=drop_ens192 cs15=0
cs16Label=drop_lo cs16=0 cs17Label=service_mariadb cs17=Up
cs18Label=service_postgres cs18=Up cs19Label=service_redis cs19=Up
cs20Label=service_rabbitmq cs20=Up cs21Label=service_icsranger cs21=Up
cs22Label=service_watchdog cs22=Up cs23Label=q_baseline_tracker cs23=0
cs24Label=q_bridge cs24=0 cs25Label=q_central_bridge cs25=0
cs26Label=q_concluding cs26=0 cs27Label=q_diode_feeder cs27=0
cs28Label=q_dissector-0 cs28=0 cs29Label=q_dissector-1 cs29=0
cs30Label=q_dissector-2 cs30=0 cs31Label=q_dissector_ng cs31=0
cs32Label=q_enricher cs32=0 cs33Label=q_leecher cs33=0
cs34Label=q_monitor cs34=0 cs35Label=q_packets cs35=0
cs36Label=q_packets_errors cs36=0 cs37Label=q_preprocessing cs37=0
cs38Label=q_processing cs38=0 cs39Label=q_processing_errors cs39=0
cs40Label=q_processing_high cs40=0 cs41Label=q_zordon_updates cs41=0
cs42Label=queue_purge cs42=0 cs43Label=rd_bridge cs43=11
cs44Label=rd_dissector-0 cs44=0 cs45Label=rd_dissector-1 cs45=0
cs46Label=rd_dissector-2 cs46=0 cs47Label=rd_dissector_ng cs47=0
cs48Label=rd_preprocessing cs48=0 cs49Label=unhandled_events cs49=0
cs50Label=conclude_time cs50=0 cs51Label=exceptions cs51=0
cs52Label=mysql_query cs52=0.02 cs53Label=postgres_query cs53=0.0
cs54Label=dropped_entities cs54=0 cs55Label=workers cs55=26
cs56Label=workers_stop cs56=0 cs57Label=workers_restart cs57=0
msg=Successfully ran health monitoring
```

Table 82: Health Check Monitoring Example

Name	Description	Value in Example
`Protocol`	The name of the syslog message format in use	`CEF:0`
`Vendor`	The name of the vendor of the product	`Claroty`
`Product`	The name of the product in use	`CTD`
`Product version`	The version number of the product in use	`4.2.3`
`Signature`	The category of the underlying object that the syslog refers to: Alert/Event/Baseline/Status Check/HealthCheck	`Healthcheck`
`SiteID`	The ID of the site	`1`
Parameters	The format of the list of parameters is `csNLabel=<parameter name> csN=<value>` *where:* N is incremental according to the number of parameters.	
`Site`	The site from which the information contained in the message is being sent.	`Default`

Name	Description		Value in Example
	cpu	CPU Utilization: CPU load average as a percentage of the total available CPU capacity (including all available cores)	0.19
	mem	Memory Usage: The percent of current memory consumption. The value is a number between 0 and 100	54.3
	Disk Utilization The percent of disk space currently used in this particular directory		
	used__opt_icsranger		9.23
	used__var		9.23
	used__tmp		9.23
	used__etc		9.23
	Disk Busy Percent How frequently the particular disk partition is in use (as a percentage between 0 and 1)		
	busy_sda		0.84
	busy_sda1		0.0
	busy_sda2		0.84
	busy_sr0		0.0
	busy_dm-0		0.93
	busy_sdb		0.19
	busy_sdb1		0.19
	Network Interface Packet Drops The number of packets that are dropped when using this network interface		
	drop_ens192		0
	drop_lo		0
	Services Running Whether the service is running (Up or Down)		
	service_mariadb		Up
	service_postgres		Up
	service_redis		Up
	service_rabbitmq		Up
	service_icsranger		Up
	service_watchdog		Up

Name	Description	Value in Example
	Queue Message Counts Each worker has its own read queue	
	q_baseline_tracker	0
	q_bridge	0
	q_central_bridge	0
	q_concluding	0
	q_diode_feeder	0
	q_dissector-0 . . n	0 . . .
	q_dissector_ng	0
	q_enricher	0
	q_leecher	0
	q_monitor	0
	q_packets	0
	q_packets_errors	0
	q_preprocessing	0
	q_processing	0
	q_processing_errors	0
	q_processing_high	0
	q_zordon_updates	0
	Queue Purges Queue purges counted in the last 24 hours	
	queue_purge	0
	Queue Read Count The queue read count for each component	
	rd_bridge	11
	rd_dissector-0	0
	rd_dissector-1	0
	rd_dissector-2	0
	rd_dissector_ng	0
	rd_preprocessing	0
	Event Handling The number of events that have not been handled by the system	
	unhandled_events	0
	Conclusion Time	
	conclude_time	0
	Logs Exceptions The number of new logged exceptions	
	exceptions	0
	MySQL Query time, in seconds	
	mysql_query	0.02
	PostgreSQL Query time, in seconds	
	postgres_query	0.0
	Dropped entities Number of entities dropped by the system due to reaching the limit of number of entities	
	dropped_entities	0
	Workers Stopped/Restarted	
	workers — The total number of workers (processes) in the system	26
	workers_stop — The number of stopped workers	0
	workers_restart — Total number of workers restarted	0
msg	The message containing the description of the health check monitoring test	Successfully ran health monitoring

4.5 White-labeling Reference

- When connecting with an Admin User, use the following Default password:
  - For White Label - "Password1!"

For more details, see the *ClarotyOS Guide – Configuring your IP via Console.*

4.6 Default Credentials

The default credentials to log into the console of the system. These credentials are:

- Username: admin
- Password: `Password1!`

Then you are required to set a strong password (14 characters, Uppercase, Lowercase, Number, Symbol).

4.7 Export Data Component

The Tripwire Industrial Visibility (TIV) Export Data component provides the ability to export all the assets into an external database.

TIV's Export Data component creates an external independent database repository with asset information from all TIV sites and Enterprise Management Console (EMC) installations.

A typical Export Data use case is an organization that requires maintenance of an enterprise central asset management repository whose assets span across the entire organization (IT networks, OT networks and so on). Typically, in such case an enterprise Configuration Management Database (CMDB) will be used to hold all assets across the organization. The TIV Export Data component can be used in order to integrate with this CMDB by exporting all assets from all TIV servers to a single database and having the CMDB read the information from this database.

4.7.1 Solution Overview

The ability to export asset information from all TIV instances requires the use of an Export Data component that can be installed on the same server as the TIV server, or in a central location in case of a distributed environment.

Deployment with hundreds of TIV sites and multiple Enterprise Management Consoles (EMCs) can use a single instance of the Export Data component, located in a central location.

The Export Data component connects to each one of the site's or EMC instances, pulls the selected asset information from each one, and stores all the information in a local database.

The following diagram illustrates the Export Data architecture:

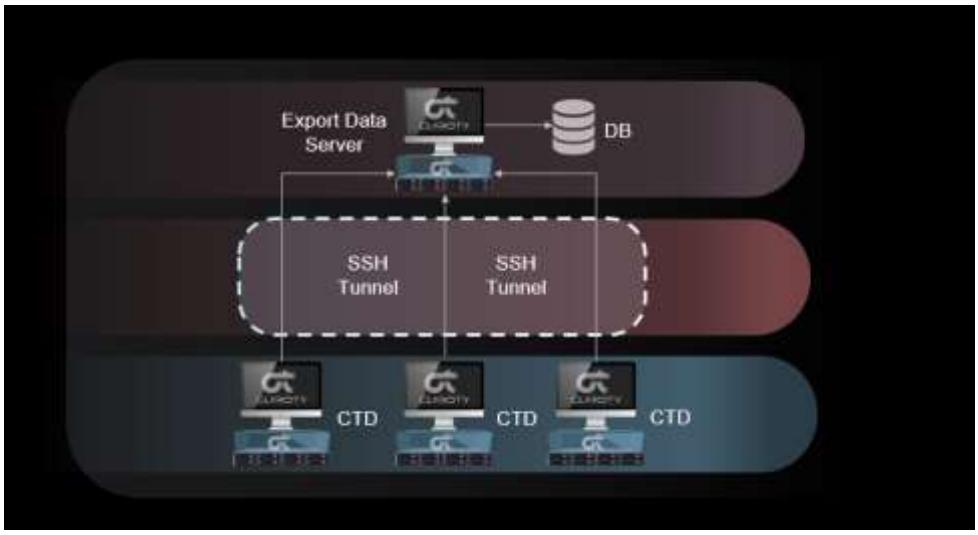


Figure 68 Export Data Architecture

Every TIV Server instance or EMC instance registers itself to the Export Data component. During the registration phase, SSH keys are created and exchanged between each pair. Once registration is complete, a secure SSH reverse tunnel is established between the pair and is initiated from the TIV/EMC to the Export Data machine.

The Export Data machine contains a MySQL database and a service called `export_data_puller`.

Export Data operates at configurable intervals. At each interval, Export Data checks if any new assets have been identified or if there are assets that have been updated that should be added/updated in the MySQL database. For optimization purposes and to preserve network bandwidth, only assets that have been changed or added will be synchronized by Export Data.

The polling is currently done serially. If a TIV/EMC does not respond or has network issues, the system will attempt to continue fetching from the subsequent TIV/EMC instances and return to this TIV/EMC in the next interval.

4.7.2 Specification

The Export Data Server is supported with TIV version 2.7.2 and higher. Currently the Export Data Server is supported only on RHEL or CentOS v7.4 or higher machines according to the following specifications:

Table 83: Export Data Specification

Capacity - Export Data for up to:	#CPU Cores	RAM	Req Free Disk Space (not including OS)	Disk Type
1 million assets	8 Cores	8 Gb	60 Gb free space	Standard HDD
2 million assets	8 Cores	8 Gb	120 Gb free space	Standard HDD
7 million assets	8 Cores	8 Gb	500 Gb free space	Standard HDD

4.7.2.1 Database Schema

There are several tables in the database used by the Export Data component: Assets, Stats, Slots and Protocols.

Table 84: Database Assets Table

Field Name	Key	Type	Comment
central_id	Primary key	Int	The ID of the EMC component
site_id	Primary key	Int	The ID of the TIV Site
id	Primary key	Int	The internal ID assigned to the asset by the system
central_name		Text	The name of the EMC component
site_name		Text	The name of the TIV Site
network		Text	The network assigned to this asset
name		Text	The asset name
ip		Text	The asset IP
state		Text	Whether this asset is in training mode or not
parsed		String	Whether this asset was identified by sniffing the network or from parsing a configuration file (Yes/No)
Mac		Text	The asset Mac address
criticality		Text	The criticality assign to this asset
vendor		Text	The vendor identified by the solution
address		Text	Gateway address
Firmware		Text	The firmware version identified by the solution
Serial		Text	The serial number identified by the solution
vlan		Int	VLAN number: 0-1024
asset_type		Text	The type of the asset (PLC, HMI, Endpoint, etc.)
risk_level		Text	The risk level assigned to this asset
model		Text	The hardware model

Field Name	Key	Type	Comment
OS		Text	The OS
first_seen		datetime	The first date and time this asset was seen in the communication in the network
last_seen		datetime	The last date and time this asset was seen in the communication in the network
virtual_zone		text	The name of the assigned virtual zone
Approved		int	Whether or not there is a “New Asset” alert
Hostname		text	The name of the host
old_ips		text	List of previous identified IPs for this asset
Parent_ID		int	The parent Asset ID of this asset

The combination of `Central_id`, `site_id` and `id` creates a UUID that can be used to uniquely identify an asset.

The Stats table stores the details of the last successful synch of a site:

Table 85: Database Stats Table

Field Name	Key	Type	Comment
central_id	Primary key	int	The ID of the EMC component
Central_name		text	The name of the EMC component
Last_sync		datetime	The date and time of the last synchronization

The Slots table stores the PLC slots per asset – Central – site combination:

Table 86: Database Slots Table

Field Name	Key	Type	Comment
Central_id	Primary key	int	The ID of the EMC component
Site_id	Primary key	int	The ID of the site
Asset_id	Primary key	int	The ID of the asset
ID		int	The ID of the PLC slot
Name		string	The name of the PLC slot
Model		string	The model of the PLC slot
Serial		string	The serial number of the PLC slot
Firmware		string	The firmware of the PLC slot
Address		string	The address of the database slot

The Protocols table stores the protocol names per asset – Central – site combination:

Table 87: Database Protocols Table

Field Name	Key	Type	Comment
Central_id	Primary key	int	The ID of the EMC component
Site_id	Primary key	int	The ID of the site
Asset_id	Primary key	int	The ID of the asset
protocol	Primary key	string	A single protocol per column

4.7.2.2 Installation and Configuration

Installing the Export Data Server Component

1. On an RHEL or CentOS 7.4 or higher machine, run the regular TIV installation.
2. Following the installation, run the following commands from the terminal:
   a. Add the Export Data component capability:
   ```
   lkpocli manager api export_data add_export_data_puller_worker
   ```
   b. Bootstrap the server as the Export Data component:
   ```
   lkpocli manager api --worker export_data_puller api bootstrap
   username=<USERNAME> password=<PASSWORD> db_type=<mssql/mysql>
   hostname=<IP/hostname> db_name=assets_db
   ```
   c. Create a community that will be used for the TIV/EMC to establish a connection:
   ```
   lkpocli community init --name Asset_DB --bootstrap_password
   <password. Default is 1234>
   ```

Registering TIV or EMC for Exporting Data

This solution requires setting up an Export Data Server for streaming the asset data.

1. Connect to the TIV server with SSH.

> **Note:** This capability is supported from TIV version 2.7.1 and above.

2. From the TIV/EMC SSH terminal, run the following command to enable the Export Data capability:
   ```
   lm set_config web.load_sections.configuration.export_data True
   ```
3. Login to TIV and browse to the **Configuration** menu.
4. In **Settings**, select the **Export Data** page:

Figure 69 Registering TIV - Export Data

5. Provide the following information (* fields are mandatory), and click **Apply**:

   a. **IP*** – the address of the Export Data Server

   b. **Port*** – the port to use in order to open the SSH reverse tunnel (the default is 9301)

   c. **Password*** – the password that was used to establish the community during the Export Data installation (the default is 1234)

   d. **Assets Field** – select the information that will be replicated to the database. Multi-selection is supported.

> **Note:** The columns are configured on the TIV/EMC side, not on the Export Data side. This allows specific data from specific sites to flow to Export Data Server.

   e. **Use reverse SSH tunnel** – the default is Yes (uncheck the checkbox if not relevant)

   f. Once the servers are joined, the following screen changes as shown below:

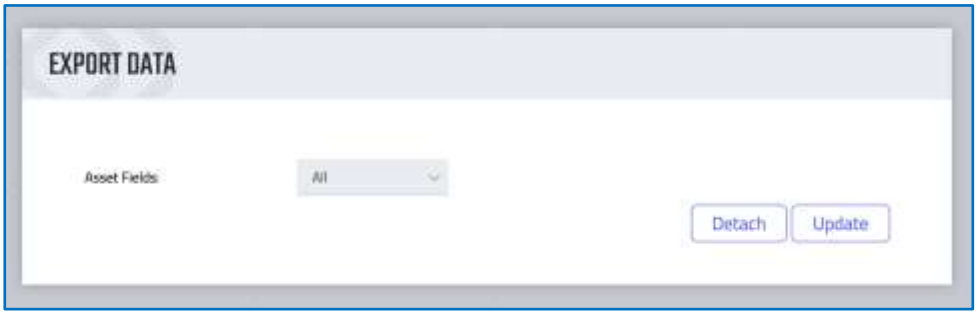


Figure 70 Configuring the Export Data Server

Configuring the Export Data Server

The server pulls data from the sites at a configured interval. On the Export Data Server there is a service, `export_data_puller`, that can be configured as follows:

1. Configure and override the interval configuration, using the following command (by default, the interval is 300 seconds).:

```
lkpocli manager api export_data set_export_data_pull_interval
<seconds>
```

2. Changing the username or password requires bootstrap according to the installation command (see section a.b).

Maintenance

- On the Export Data Server, rather than waiting for the next sync iteration you can sync all the TIV/EMC sites immediately, using the following command:

```
lkpocli manager api --worker export_data_puller api sync_all
```

- To bootstrap the Export Data Server:

```
lkpocli manager api --worker export_data_puller api bootstrap
```

> NOTE: We recommend not deleting the database manually. However, if you choose to do so, remember to re-bootstrap the server by running this command again.

Connecting to the Export Data database

Connecting to the MS SQL database / MySQL database is done by using a client of your choice. The database name is assets_db.

Open Ports

The open ports used by the Export Data Server are as follows:

- 9300
- 9301

4.7.2.3 Troubleshooting

Use the following commands for basic troubleshooting:

- On the Export Data Server – to view the log file:

```
/var/lib/icsranger/master/logs/export_data_puller.log
```

- On the TIV site – to view any issues or errors:

```
/var/lib/icsranger/master/logs/export_data.log
```

4.8 Troubleshooting Guide

This section provides information on how to collect TIV logs for troubleshooting, where to find the TIV logs, and detailed troubleshooting use cases.

See the following instructions. If your issue is not resolved, open a ticket with Tripwire Support with the relevant logs.

4.8.1 Collecting TIV Logs and Database

To collect TIV logs and database:

1. Navigate to **Settings > Management > General > System Configuration ta**b. Then in the Take Log Snapshots area:

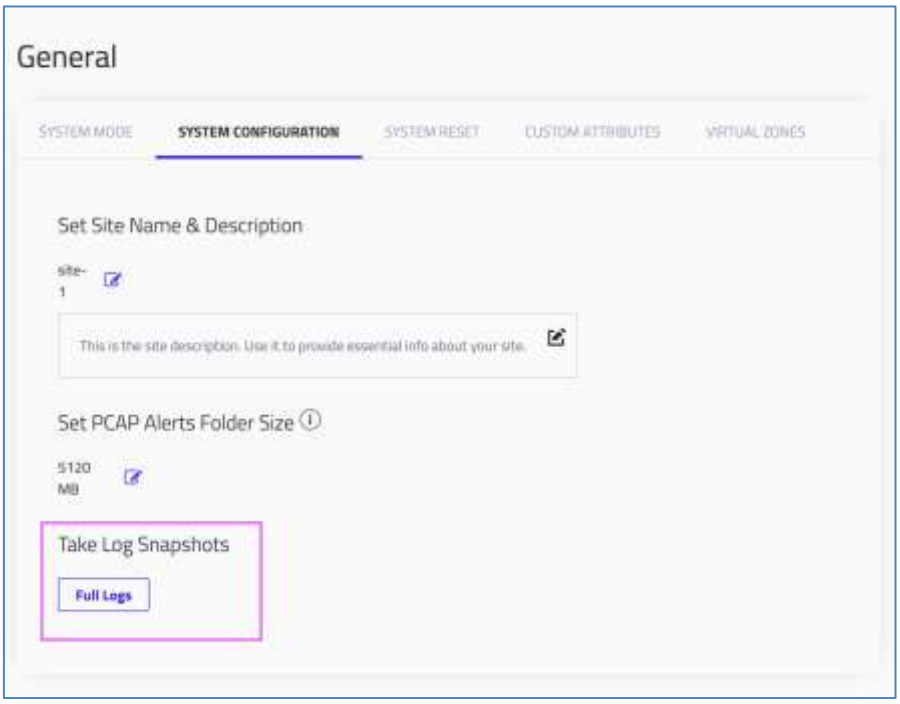


Figure 71 Log Snapshots

2. Click the **Full Logs** button.

After the system is finished preparing the snapshot, you can download it by clicking on the download link.

4.8.2 Location of TIV Log Files

TIV worker logs:

```
/opt/icsranger/workdir/logs/
```

TIV manager and watchdog logs:

- `journalctl -u icsranger`
- `journalctl -u icsranger-watchdog`

4.8.3 User cannot log into the site

To login to the site:

1. Make sure you are using a Google Chrome browser, and your login credentials are correct.
2. Press **F5** (for Windows) or **cmd+ shift + F5** (for Mac) to refresh the browser screen without using cache.

3. Check that there is a route from the workstation running the web UI to the TIV appliance machine (using ping or checking the routing table).
4. If it is an Active Directory user, make sure the AD server is up and running.
5. Make sure you have enough disk space on the appliance machine by running the following command:

```
df -h
```

```
[root@Central ~]# df -h
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/cl-root   72G   26G   47G  35% /
devtmpfs              16G     0   16G   0% /dev
tmpfs                 16G  4.0K   16G   1% /dev/shm
tmpfs                 16G   17M   16G   1% /run
tmpfs                 16G     0   16G   0% /sys/fs/cgroup
/dev/sda1           1014M  186M  829M  19% /boot
tmpfs                3.2G     0  3.2G   0% /run/user/0
```

6. Check that the TIV Service is running:

```
systemctl status icsranger
```

7. Check that Ports 5001 and 5000 are listening:

```
netstat -nltp | grep 500*
```

8. Check for a `journalctl` error:

```
journalctl -u icsranger | grep err*
```

4.8.4 Unable to Start the TIV Service

To start the TIV Service:

1. Verify that all dependent services are running.
   - `systemctl status rabbitmq-server`
   - `systemctl status redis`
   - `systemctl status mariadb`
   - `systemctl status postgresql-11.2`
2. Check the `icsranger journalctl` log file:

```
journalctl -u icsranger
```

3. Check the disk space and verify there is available free space for the application.

```
df -h
```

```
[root@localhost ~]# df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/mapper/centos-root  12G  3.3G  8.3G  29% /
devtmpfs                1.9G     0  1.9G   0% /dev
tmpfs                   1.9G     0  1.9G   0% /dev/shm
tmpfs                   1.9G  183M  1.7G  10% /run
tmpfs                   1.9G     0  1.9G   0% /sys/fs/cgroup
/dev/sda1               497M  120M  378M  24% /boot
[root@localhost ~]#
```

4.8.5 Upgrading Multiple Sites

Users can choose to set the system to automatically upgrade TIV across all sites. The EMC can be configured to automatically update the site versions to the latest EMC version. After this functionality is enabled, the system continuously attempts to perform the version update. In this procedure, each site update is performed individually in sequence.

Configuration details for automatically and manually upgrading are provided in the *TIV User Manual*.

If a particular site fails to upgrade successfully, an error message is displayed in the Activities page, stating the cause of the failure. Backups are available in site `/temp` directory (no automatic Rollback). The log files stored in the `/var/claroty/installers/ctd-version/` Directory.

4.8.6 Upgrading Sensors

Sensors are automatically updated to the current version of the site component. This process is enabled by default. The sensors are upgraded one by one. If one of the upgrades fails, an error message with the cause of failure is logged in the **Activities** screen.

The logs are saved at the following location:

```
/var/claroty/installers/ctd-version/
```

A sensor failure occurs when the sensor version is not aligned with the site version. To disable this behavior, run the following command:

```
lkpocli manager api manager set_config site.upgrade_children.auto False
```

4.8.7 EMC/TIV Replication Issues

In order to check that the Site replicates to the EMC, check that the “bundle id” between the site leecher and the EMC site-bridge are equal.

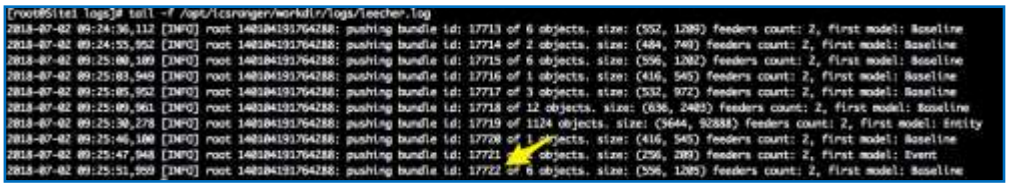
Run the following commands:

4.8.7.1 On the EMC CLI

```
tail -f /opt/icsranger/workdir/logs/bridge-<site_name>.log
```

4.8.7.2 On the Site CLI

```
tail -f /opt/icsranger/workdir/logs/leecher.log
```



4.8.7.3 Resolution

If you encounter any issues in the replication process, follow the next steps:

1. On the EMC, check if there are any error messages in the last 100 bridge and error logs:

   ```
   tail -n 100 /opt/icsranger/workdir/logs/bridge-<Site_name>.log

   tail -n 100 /opt/icsranger/workdir/logs/bridge-
   <Site_name>.error.log
   ```

   where the `Site_name` is the name of the TIV Server the data is **not** replicating from.

2. If you could not find any errors, open an SSH console to the site and check for errors in the last 100 logs of the leecher:

   ```
   tail -n 100 /opt/icsranger/workdir/logs/leecher.log
   tail -n 100 /opt/icsranger/workdir/logs/leecher.error.log
   ```

3. If you encounter any relevant errors, contact Tripwire Support and attach the logs with all the necessary information.

4.8.8 Confirming the system is online and sniffing

To confirm the system is online and sniffing:

1. Make sure that the sniffing interface is checked in the **Settings > System Management > Site Maintenance** page.
2. Check if the traffic rate is changing.
3. Check in the RabbitMQ list if there is any traffic in the dissector queues:

   ```
   watch -n 0.5 rabbitmqctl list_queues
   ```

```
Every 0.5s: rabbitmqctl list_queues

Listing queues ...
Central-Golda   1
baseline_tracker        0
bridge  0
central_bridge  0
concluding      1
diode_feeder    0
dissector-0     0
dissector-1     0
dissector-2     0
enricher        0
leecher 0
monitor 0
packets 0
packets_errors  0
preprocessing   0
processing      7
processing_errors       0
processing_high 0
zordon_updates  0
...done.
```

4. Run the following CLI command to determine if the name of the interface you are sniffing from is correct:

```
ps -ef | grep net-sniff | grep tcpdump
```

5. Run an open `tcpdump` on the interface you should sniff from to check if any traffic is coming into this interface:

```
tcpdump -i <interface_name> -nnvv
```

6. In the Assets page, ensure that the **Last Seen** and **First Seen** columns are displayed:

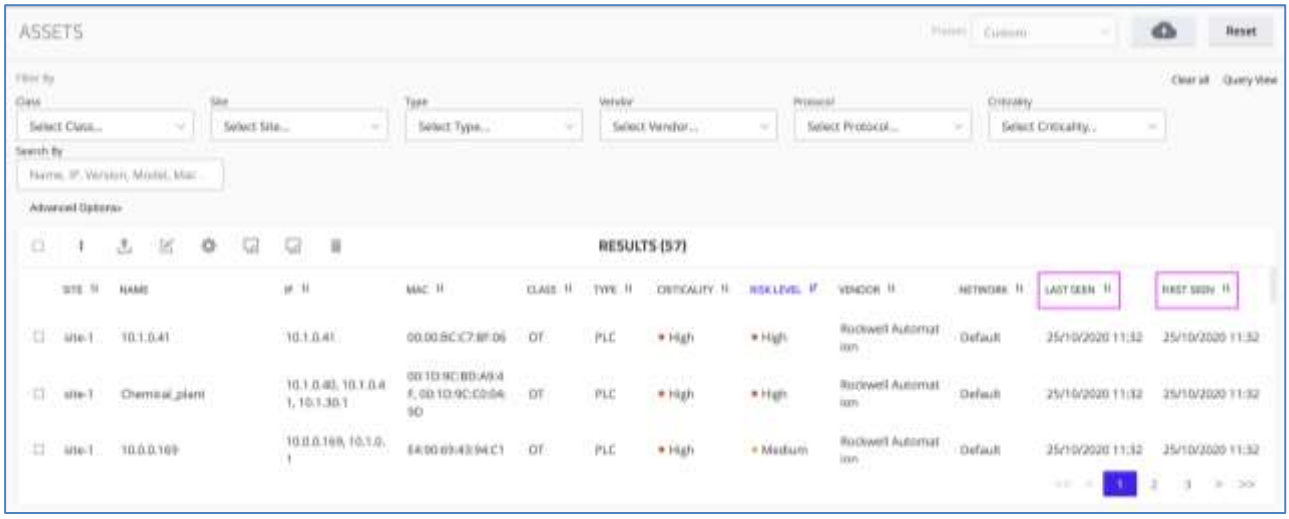


Figure 72 Assets Page with First Seen and Last Seen columns

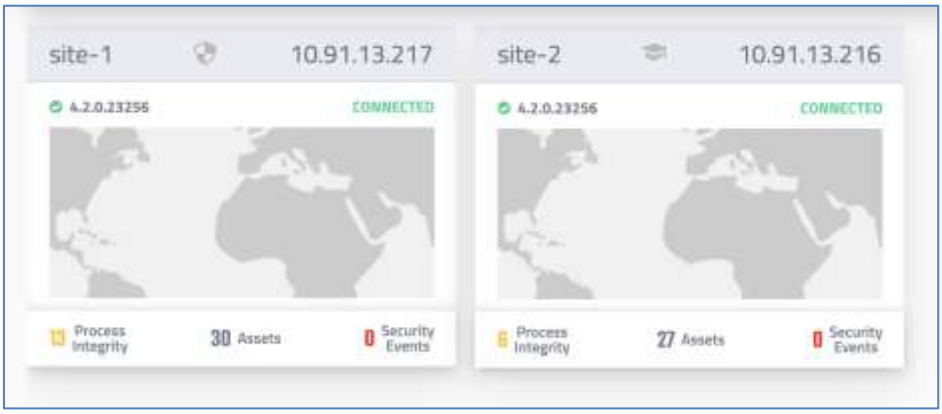
7. If any of the previous steps did not help to solve the issue, collect a Full dump, traffic capture and open a case in Salesforce (SF) for Tripwire Support assistance.

8. You can use the following `tcpdump` command for collecting the traffic capture:

```
tcpdump -i <interface_name> -nnvv -c 1000 -w
<output_file_name.pcap>
```

4.8.8.1 From the EMC

1. On the **Enterprise Overview** page, check the connected sites are marked as "CONNECTED":



2. Check in **Settings > Activity Log** that the site is not down (Communication Up/Down or Site Up/Down):

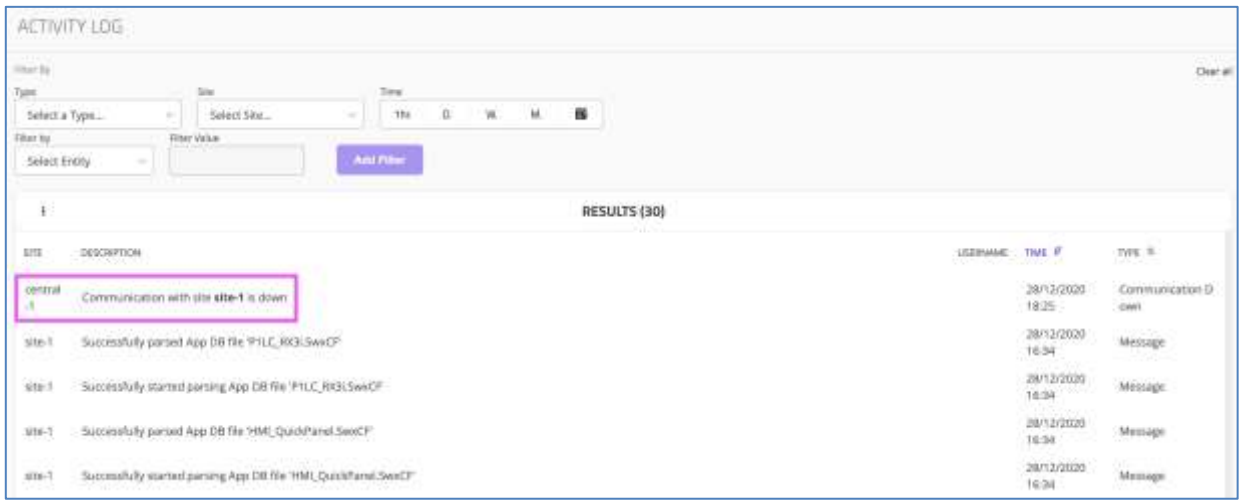


Figure 73 Activity Log updated

4.8.9 Steps to take when Assets reach boundary

To check the assets:

1. Navigate to **Visibility > Assets**. Then click Advanced Options and set the following filters:
   - **Ghost Assets**: Show ghost assets
   - **Address Type:** Unicast, Multicast, and Broadcast (see Figure 74).
2. Check results with the same filter as Step 1, but with only **External Assets** selected in the **Address Type** filter.

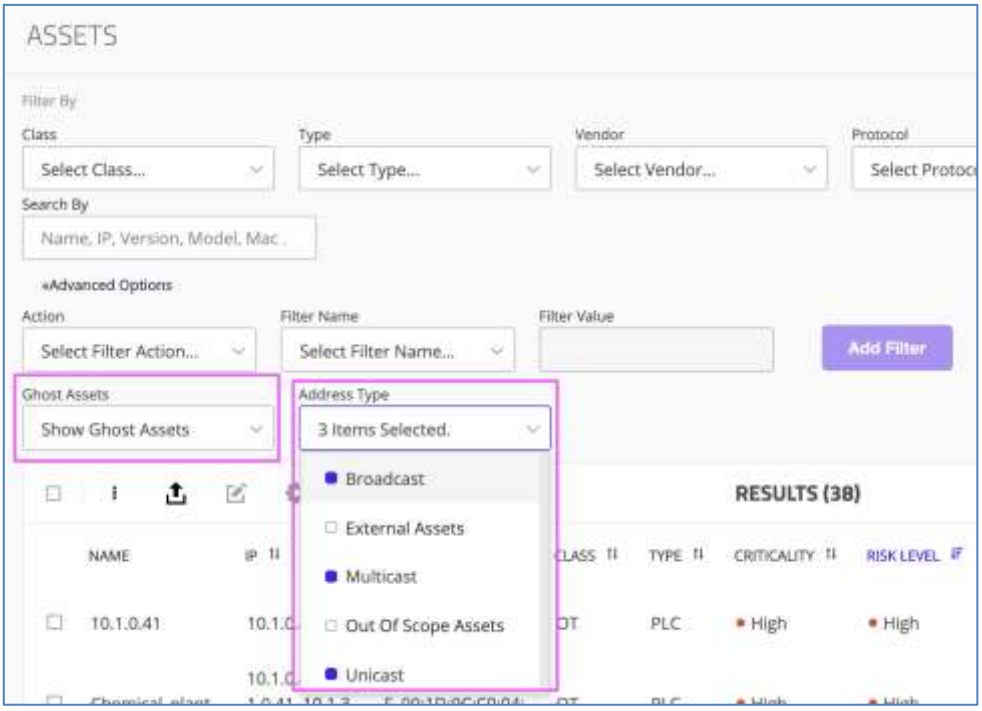


Figure 74 Check Assets

If you reach the external assets limit but did not reach the internal assets limit, you can keep working.

3. Ensure the network is configured correctly.

   - If internal assets reach the limit, act on one of the following scenarios:

4.8.9.1 Scenario 1: Are you connected to the correct network?

If network is configured incorrectly, then define another interface to sniff.

To sniff another interface:

1. **Go to Settings > Data Sources > Interface Configuration**.
2. Disable the incorrect network
3. Remove the learned assets.

- Go to **Visibility > Assets**, mark the ones that you want to remove, and click **Delete**. (Recommended)

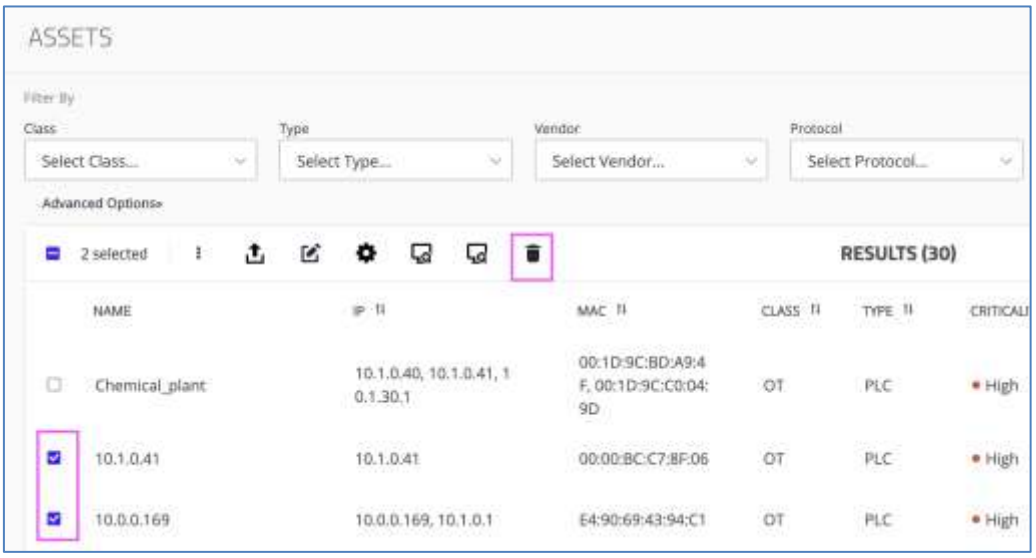


Figure 75 Removing Assets from the Assets page

OR

- Go to **Configuration** > **Management** > **General** and click the **System Reset** tab (see Figure 77).

Warning:	If you do System Reset, you will lose all of your data.

4. Enable the correct interface to process data.
5. Check if assets learned is correct.

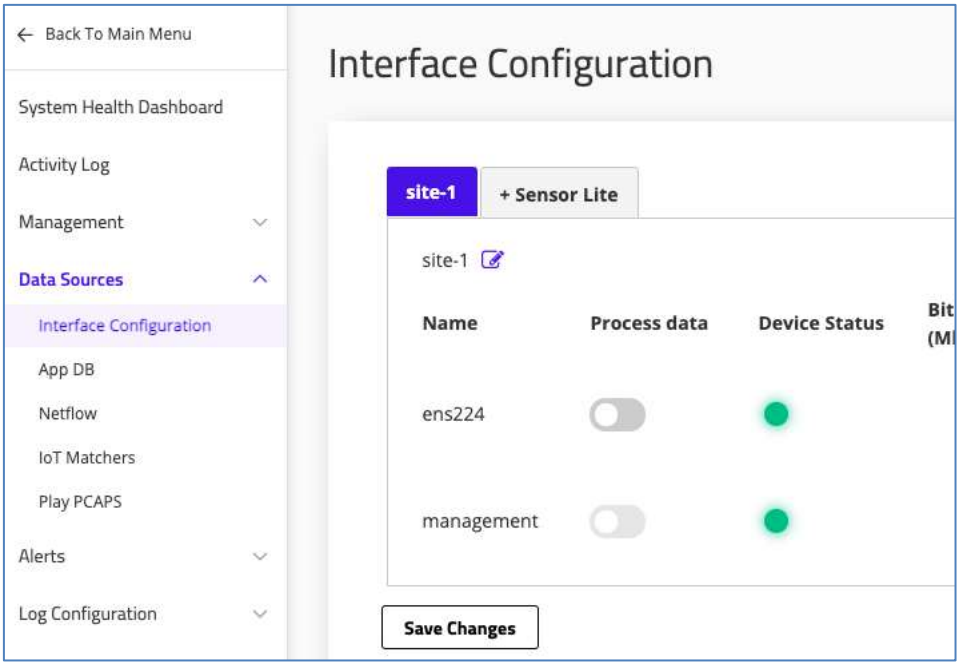


Figure 76 Sniff Another Interface

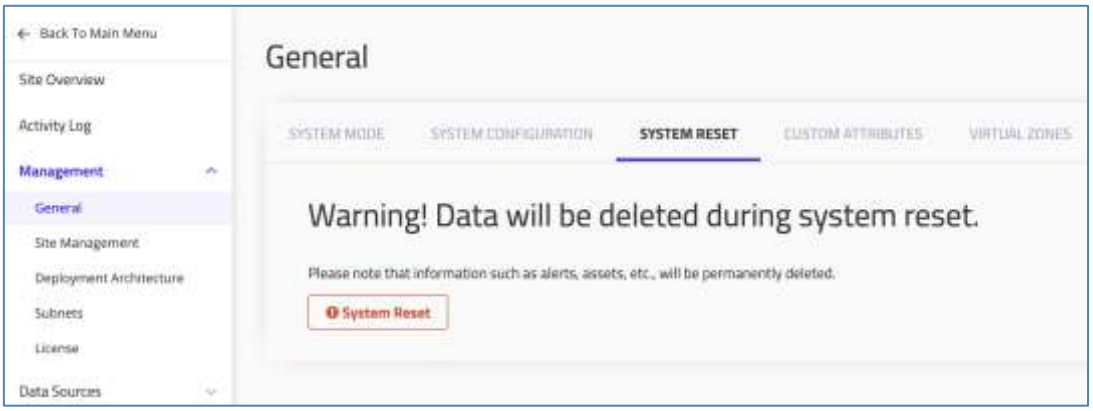


Figure 77 Remove the Learned Assets with System Reset

4.8.9.2 Scenario 2: You listen to the correct interface and see unexpected assets.

Your network configuration is incorrect. In this case, contact your Network Administrator.

4.8.9.3 Scenario 3: You are using the correct interface and configuration, but data collection has stopped.

In this case, contact Tripwire Support if you don't see any problem with your configuration.

4.8.10 Steps to take when Baselines reach boundary

1. Check in Zone Rules to filter by this protocol and check which rule has the highest hit count.
   - Go to **Visibility > Rules > Zone Rules.**
2. Sort by hit count.
3. Look at related protocol.
4. Check if communication is as expected.
5. Click on rule and look at the baselines.
6. If the protocol is important to keep, then contact Tripwire Support. If the protocol is not important, then you can disable it.

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

To disable the protocol:

a. Go to **Settings > Data Sources > Interface Configuration.** Then click **Advanced Network Settings** and enable **Show Protocol Configuration menu in Configuration page**. The **Protocols** list appears.

b. Uncheck the incorrect protocol.

c. Follow same scenarios as assets listed in section 4.8.9 Steps to take when Assets reach boundary section.

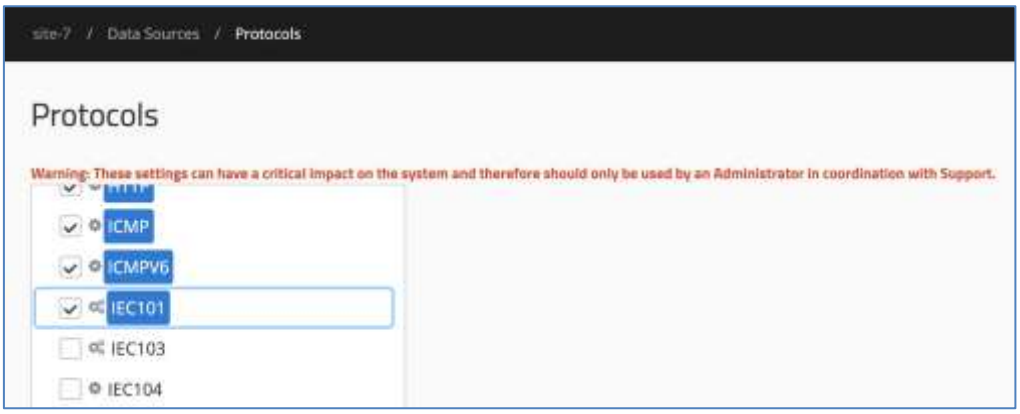


Figure 78 Disable the Protocol

5 Appendix A: Terminology

Refer to the *TIV User Guide.*