tripwire®

TRIPWIRE®
INDUSTRIAL
VISIBILITY

TRIPWIRE INDUSTRIAL VISIBILITY 4.2.4
INSTALLATION GUIDE

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Tripwire Industrial Visibility Installation Guide Revisions

Revision	Date	Owner	Author	Revisions
Rev 1	April 2021	Moshe Alvoer	Beth Stolper	Initial release

Contents

1 Introduction

This document provides the installation procedure for , version 4.2.4.

> Note TIV supports RHEL/CentOS up to version 7.9 minimal.

2 Network Preparation for Tripwire TIV Installation

TIV has three different options for collecting data from your system. The main setup is a passive monitoring on a SPAN/Mirror port on a central switch. All traffic routed to the SPAN port will be analyzed and presented in the Tripwire user interface. To be able to get more details on each asset, you can use the AppDB option or the Active Query option.

If you have traffic in your system that does not pass the SPAN port, for example a local RTU on a remote location, then you can use a sensor installation. The sensor will operate similar to the TIV, by setting up a baseline and alerting if you have deviations from the baseline. The data is compressed and encrypted and sent to the central TIV.

To be able to see all assets in your system, you need to evaluate the topology to find the most appropriate placement, and then reconfigure some of the switches to span the traffic to the point where the TIV is placed.

2.1 Network Setup Procedure

1. Decide which assets you want to monitor. Typically, you will take your topology drawings of the control system and mark the systems you want to include. If possible, set up a list of all assets you expect to see. Then you will be able to evaluate the hit-rate of the asset discovery in Tripwire.
2. The best placement is often close to the SCADA and Engineering stations. This is centralized positions where data from a lot of assets are passing by. Choose a switch in this position.
3. Analyze the traffic flow in your system. If the system is segmented with a VLAN structure, you can SPAN one or more VLANs to the selected SPAN port.
   BE CAREFUL! Check the load of the switch and evaluate the amount of data before you do the SPAN.
4. You can also SPAN physical ports on the switch, like the ports connected to the SCADA server, Engineering stations, historian servers, and asset management systems.
5. After the TIV has been running in learning mode for a while, you can start to enrich the assets data by importing the PLC/RTU program files by using the AppDB import. This will give you a more detailed picture of the assets with vulnerabilities, and it will also show the nested devices in the back of a PLC.
6. Next step will be to do dedicated active queries to assets like servers. This will give you more detailed information about programs installed, patches, and versions. A more detailed list of vulnerabilities will show up.
7. Compare your asset list with the discovered assets in Tripwire. If some assets are missing, check the communication paths. Maybe you need to install a sensor or SPAN more VLANs/ports into the TIV monitoring port.

3 ClarotyOS Wizard [Only Admins]

3.1 Quick Installation via ISO

. Insert the installation file to your server.

- Either install directly with ClarotyOS' ISO or with a bootable media file containing the ISO.

2. Open the Server Console and select Install ClarotyOS:

Figure Error! No sequence specified. **Installing ClarotyOS**

3. Wait until the installation is finished; the following screen appears:

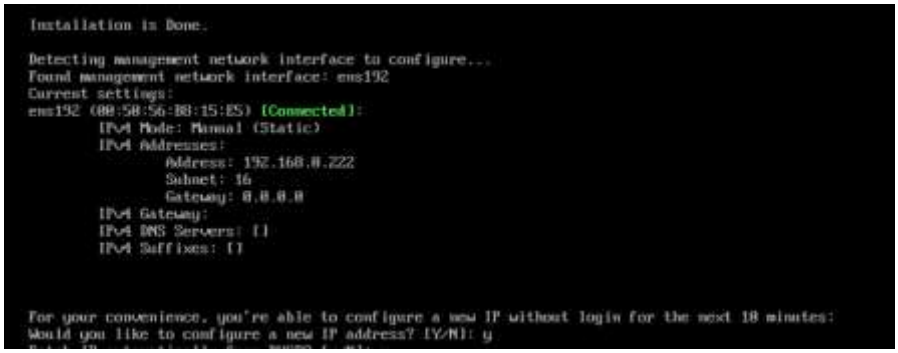


Figure Error! No sequence specified. **ClarotyOS installation complete**

> Note In the first installation, you can opt to change the IP address once.

4. You can reconfigure your network settings by entering the Admin password and then **Run**.

- Wait until the machine IP is presented.

5. Choose whether you prefer to configure your IP via a console using CLI or via the TIV UI; then continue to the TIV Wizard.

3.2 Deploying via OVA

In order to deploy ClarotyOS as a ready-to-go VM, make sure you have:

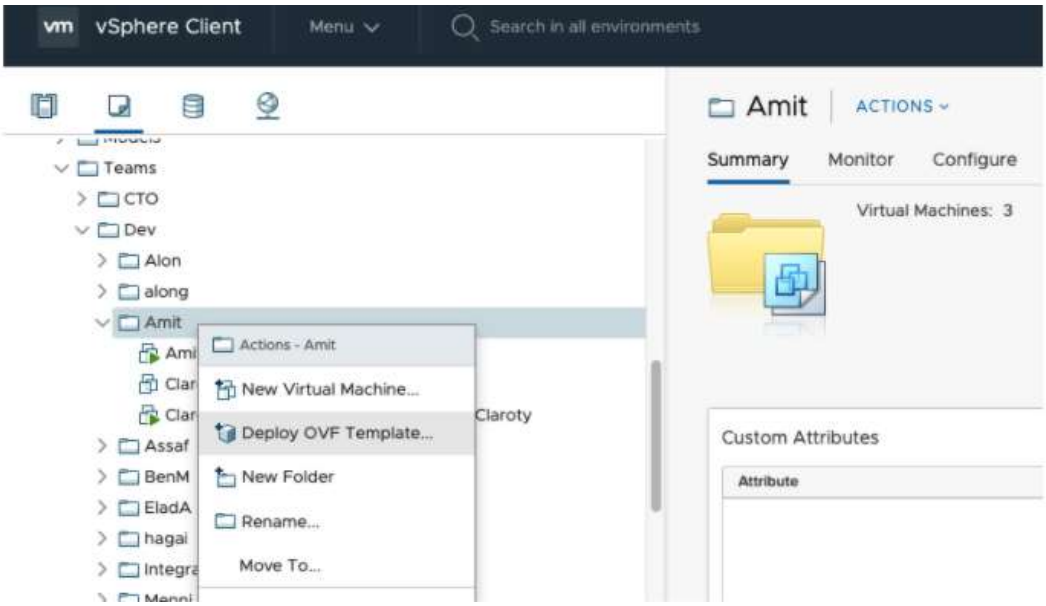
1. The .ova file of ClarotyOS

2. Optional: a settings.iso file with your deployment settings. This file will be generated by the Tripwire team.
3. Choose how you want to deploy your OVA: via VMware (continue the steps below) or a using a Cloud platform, such as AWS as described in section 3.5).

3.2.1 Deployment on VMware vCenter

- Log into your vCenter UI, and go to the folder you want to deploy the VM in.

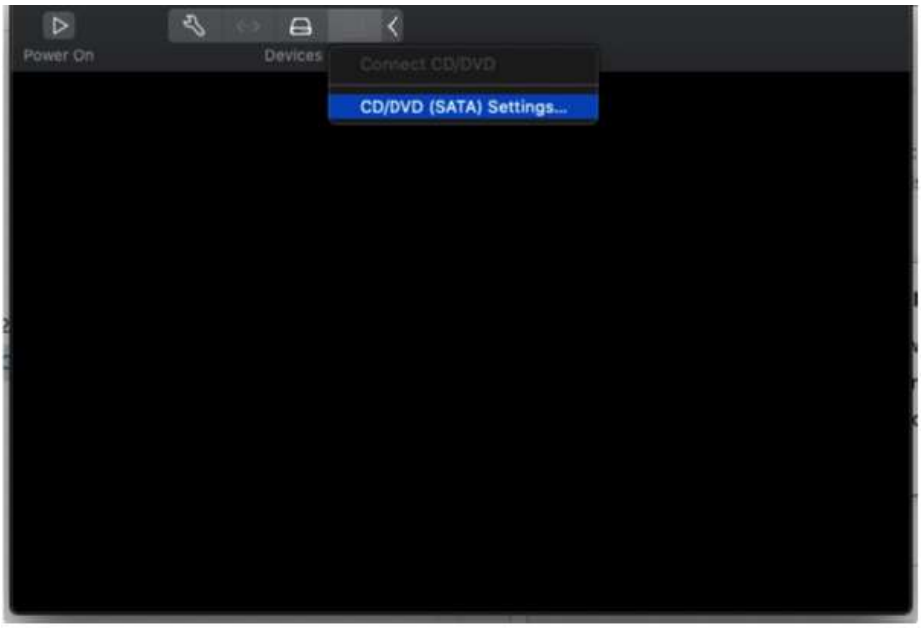
  Right-click on the folder and select "Deploy OVF Template"



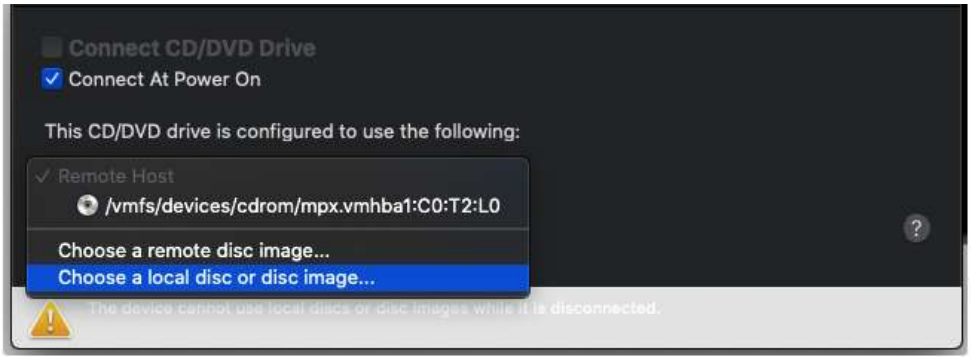
- Select the OVA file and click Next:

- Continue the wizard and select the name of the VM, the folder, the ESX, and the storage.
- When the wizard is done, you will have the machine powered off in your folder. DON'T TURN ON THE MACHINE YET!
- Right-click on the machine, choose "edit settings", and configure the VM CPU and Memory allocation to your needs. You may also increase the size of the Hard Disk, but you will have to do a manual command later in the admin shell in order to make the VM see the change admin@localhost# storage extend-device.
- If you don't have a settings file, you may turn on the machine and configure it through the ClarotyOS Wizard.
- If you have a settings.iso file, before turning the machine on, open the machine console through "Remote Console". You may get the installation of "VMware remote console" from their website if you need it.

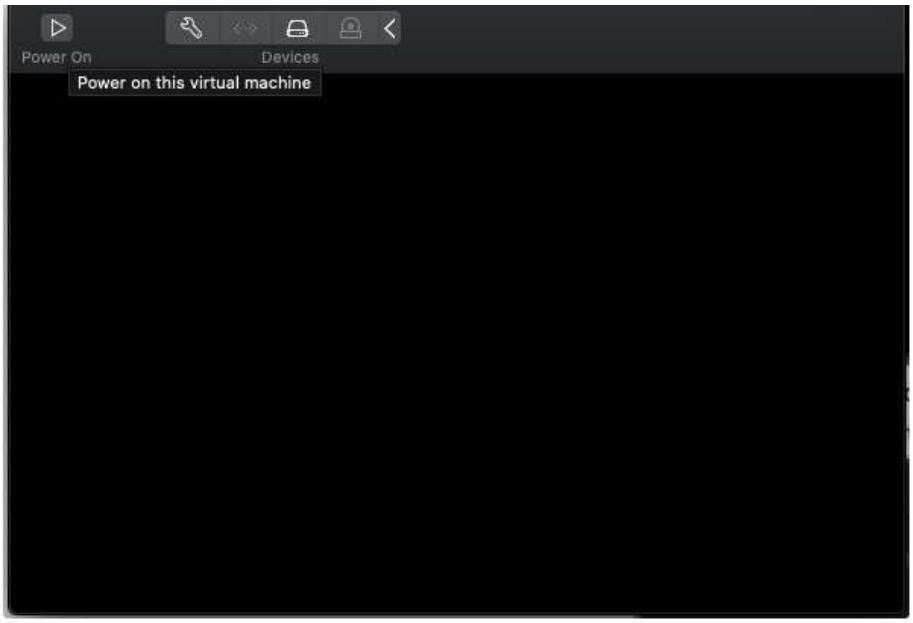
- On VMware Remote Console, click the disc icon and select “CD/DVD Settings”



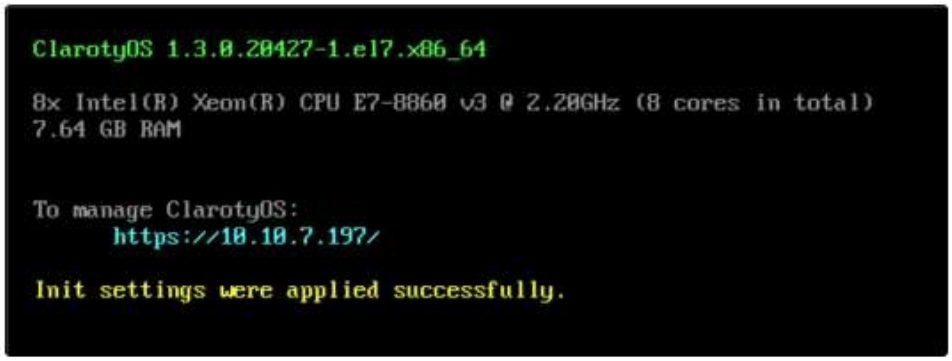
- Check the “Connect At Power On” checkbox. Then click on “Choose a local disc or disc image” and choose the provided “settings.iso” file. After, you can close this window.



- Now, turn on the machine using the “Power On” button on the top of the screen:



- A minute or two after the machine will finish the boot, it will read the settings from the iso file and apply them. Once the process is done, you will see a message is the machine console:



3.2.2 Applying settings from a settings.iso after first boot is already done

If you forgot to connect the ISO file before the first boot, don't worry.

You can apply the settings with a simple solution:

. Connect the "settings.iso" file to the machine's CD-ROM.

2. Login to the admin shell, and run the command "apply_settings_from_cd"

```
[admin@localhost]#
[admin@localhost]# apply_settings_from_cd
Warning: this command will override current system settings
Please make sure the settings iso is connected to the machine cd-rom
Are you ready to start? [y/N]: y
Reloading and applying settings from cd...
All settings were applied successfully.
[admin@localhost]# _
```

> Note To add the new hard disk via the command line run this command:

```
storage add-device
```

3.2.3 Add a new hard disk or extend an existing one

This command allows you to add or expand hard drives in your ClarotyOS and add the extra space to the filesystem.

3.2.3.1 Option1: Adding a New HD

This command adds a new partition, creates PV, extends VG size, extends LV size, and resizes the XFS filesystem's size for you.

In order to add your new HD to the current filesystem, login to admin's shell and run:

```
storage add-device
```

- Choose wanted device from list:

```
[admin@localhost]# storage add-device
New Devices found:
/dev/sdb          5G
/dev/sdc          5G
Please choose the wanted device [Default: /dev/sdb]:
```

- Approve:

```
[admin@localhost]# storage add-device
New Devices found:
/dev/sdb          5G
/dev/sdc          5G
Please choose the wanted device [Default: /dev/sdb]:
Are you sure you want to add new device '/dev/sdb' [y/N]: y
```

- Approval message:

Creating partition, adding new "Physical Volume"

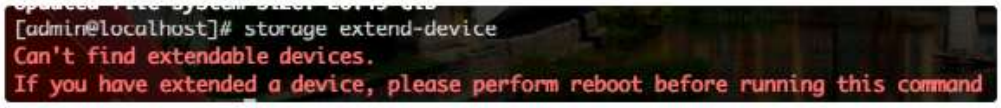
3.2.3.2 Option2: Extending an Exiting HD

This command resizes the partition size, resizes PV size, extends LV size, and resizes the XFS filesystem's size for you.

- In order to extend your HD and resize current filesystem size, login to admin's shell and run:

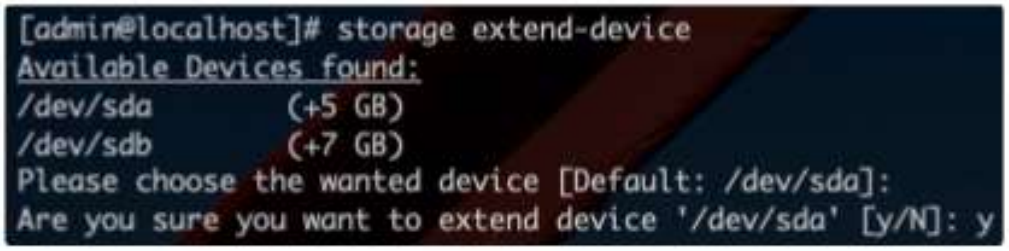
```
storage extend-device
```

> **Note** If you can't find the device you have extended in the list please perform a reboot and try this command again:



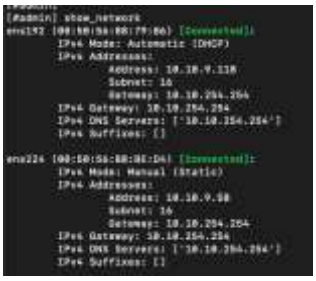
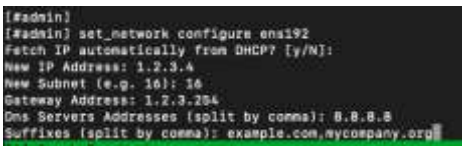
- Choose the wanted device from the list:

- Approve:



- Approval message:

3.3 Configuring your IP via a Console using CLI

1.	Open your server's console and press any key	
2.	Connect with Admin User	
	Default password: ■ For White Label - "Password1!"	
	■ Change the Default password	
3.	Change your IP Address:	
	a. Use "network show" to see your current configuration	
	b. Use "network interface configure <interface-name>" to Change IP Address, Subnet, Gateway, DNS, and suffix or choose to get IP from your DHCP.	
4.	Open a browser session	
5.	Go to https://<Your New IP Address>/	
6.	Continue to the TIV Wizard	

3.4 Configuring your IP via the TIV UI

- Wait until the machine IP is presented.
- Go to https://192.168.0.222/; this is TIV's default IP.
  - Ensure that you are in the same network and subnet (192.168.0.0/24)
- If you cannot connect in this manner, follow the CLI instructions.
- Proceed with the Installation of the Wizard Procedure in section 4, *TIV Wizard.*

3.5 Installing on AWS

Amazon Web Services (AWS) is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.

This section describes how to login and create a Tripwire TIV machine until the installation phase on the Amazon Web Services cloud.

Prerequisites

- A valid username and password.
- Approval to use the platform, due to company costs.

3.5.1 Deployment from Scratch

. Browse to the AWS console:

- https://eu-central-1.console.aws.amazon.com/ec2/v2/home?region=eu-central-1#Instances:search=running;sort=desc:launchTime

2. Enter your given credentials to login into the web interface
3. Navigate to **Instances > Launch Instance**:

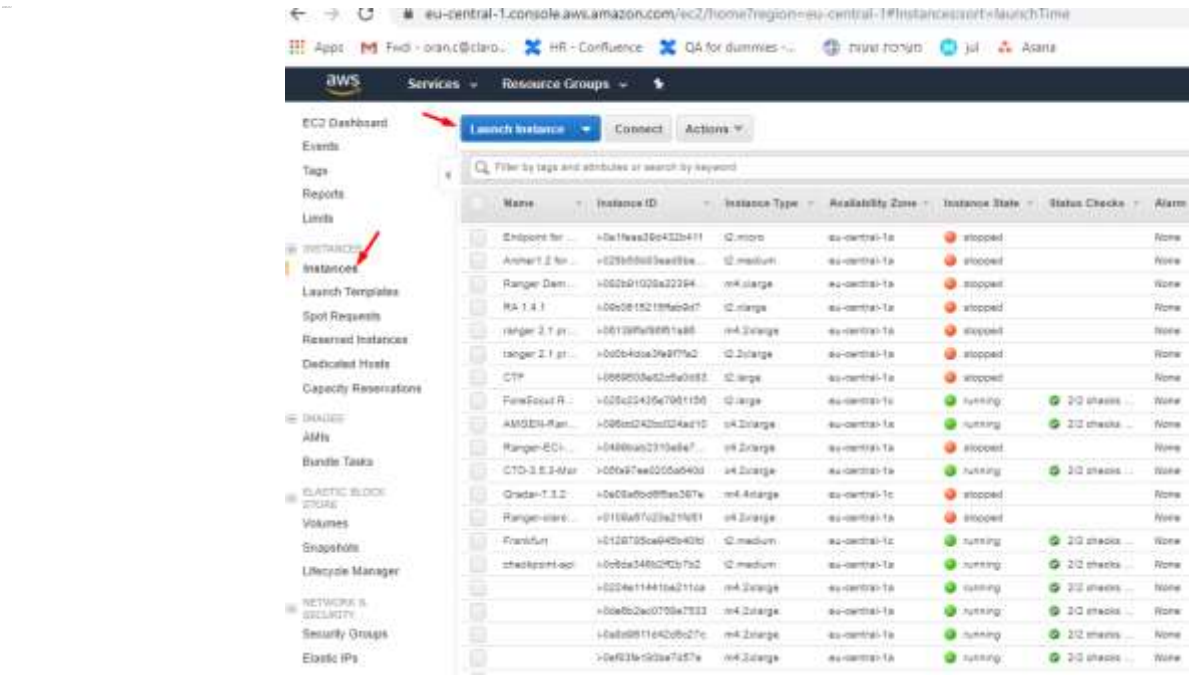


Figure Error! No sequence specified. **Launch Instance**

4. Choose the correct OS for deployment.

   In this example, we use the free CentOS to deploy TIV:

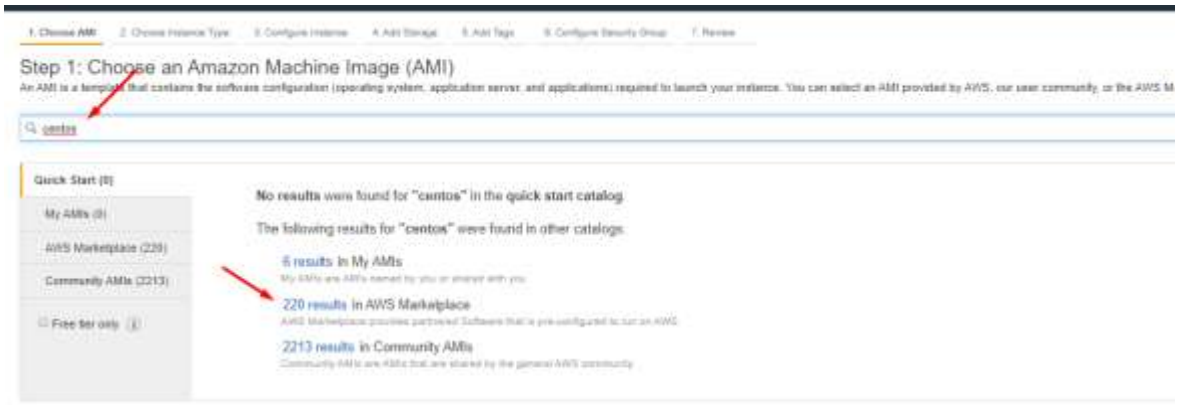


Figure Error! No sequence specified. **Search for CentOS**

Figure Error! No sequence specified. **Choose an Amazon Machine Image (AMI)**

5. Select the size model for your system.

   Keep in mind that every resource is billable.

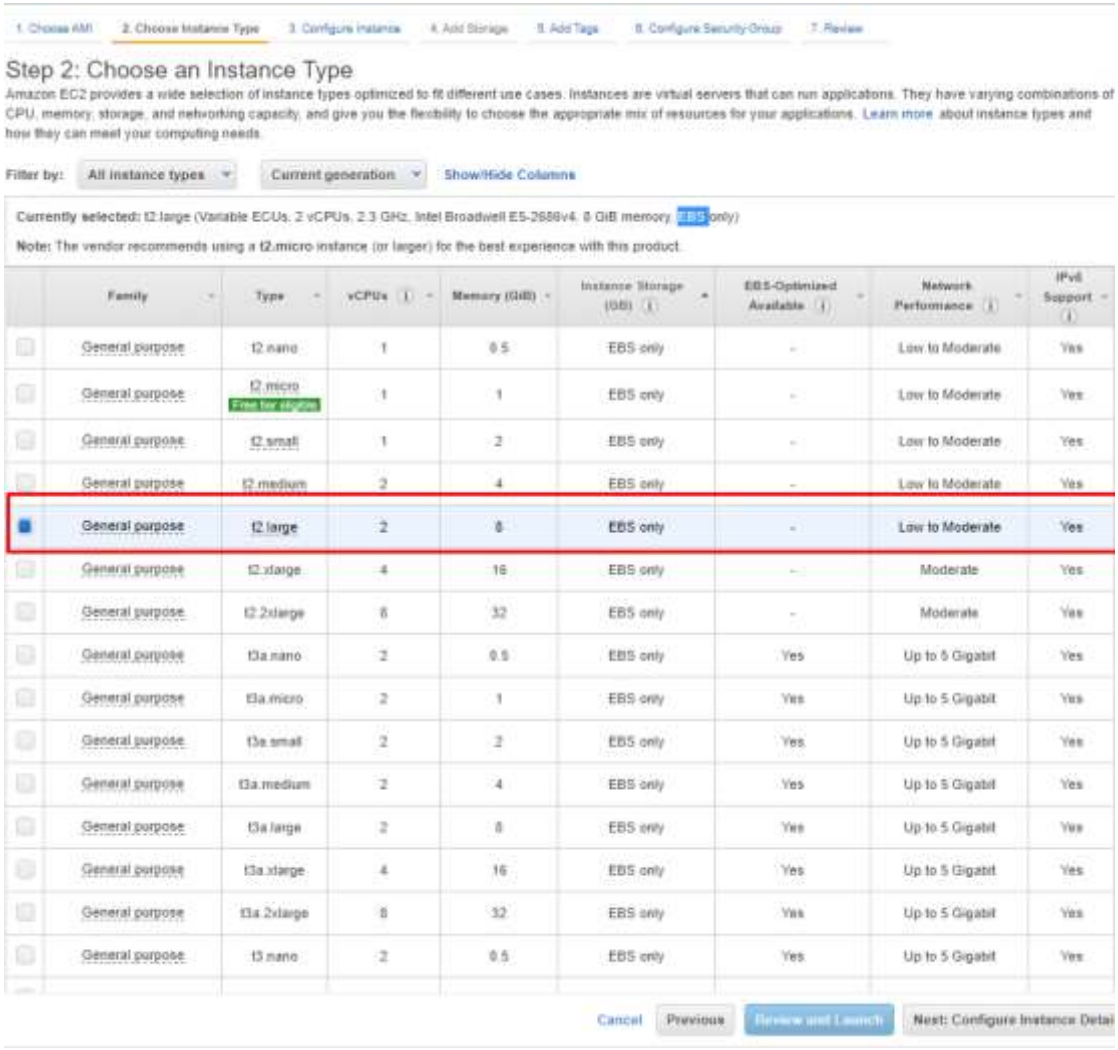


Figure Error! No sequence specified. **Choose an Instance Type**

6. Configure additional instance parameters such as:

   - IP Range
   - Number of instances to create

- Network interfaces, etc.

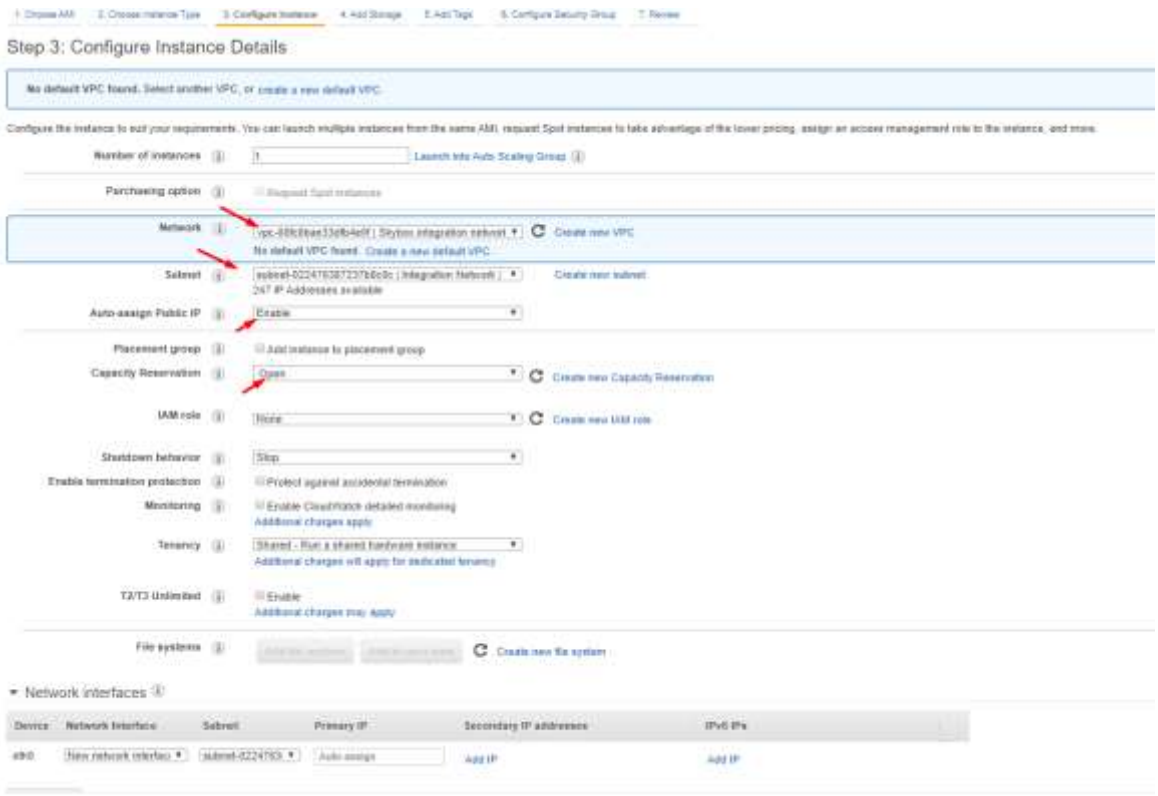


Figure Error! No sequence specified. **Configure Instance Details**

7. Configure the quality and amount of storage you require for your instance.

Figure Error! No sequence specified. **Add Storage**

8. Configure the security group policy you require for your instance.

   You may use a default security policy created to allow access to your instance, and drop any other traffic, as shown below:

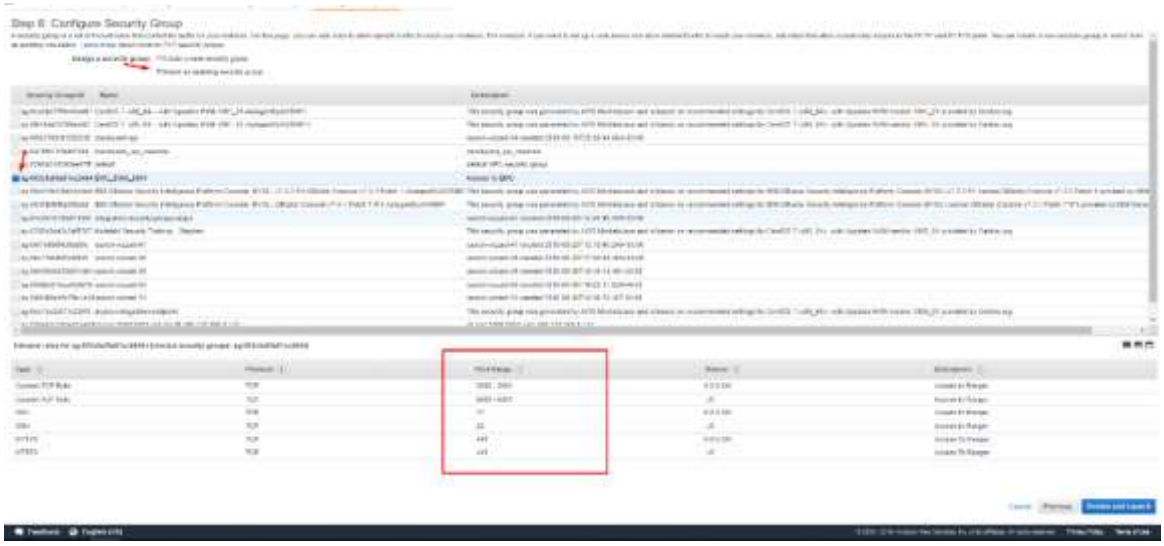


Figure Error! No sequence specified. **Configure Security Group**

9. You will now be prompted to download your private key; it is necessary you save it to access your server post-installation.
10. Launch your instance creation and wait until deployment is finished.
11. Return to section 3.3, *Configuring your IP via a Console using CLI*.
12. Then proceed with the Wizard installation.

4 TIV Wizard [Only Admins]

4.1 Configuring your Network Settings

- Enter the IP address of the machine in the Web Browser.
  - The Welcome screen of the TIV Wizard appears.

. Click **Start**

2. Read and confirm the End User License Agreement (EULA).
3. Configure your server's network.

> Alternatively, you can get the IP automatically from your DHCP.

Figure Error! No sequence specified. **Network Configuration Example**

4. Configure your server's time. You can set your time by NTP server or sync with your local time:

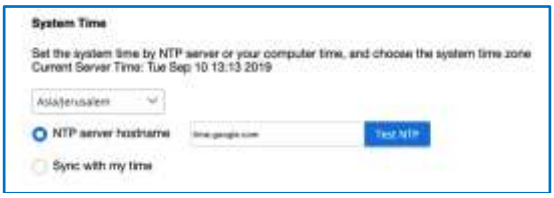


Figure Error! No sequence specified. **Configuring the Server Time**

5. Press **Next**.
6. Make sure your network settings are defined correctly before committing them:

Figure Error! No sequence specified. **Setting the Configuration**

7. Press **Set Configuration**.

   ♦ During the configuration process the following screen appears:

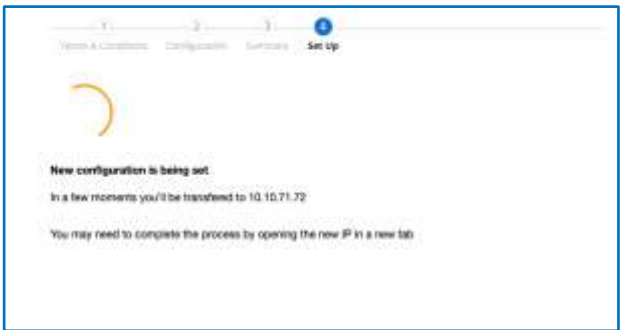


Figure Error! No sequence specified. **New Configuration set up**

■ The system redirects you to the TIV Wizard's platform settings.

4.2 Step 1: Choose Product to Install

Choose which Tripwire product to install:

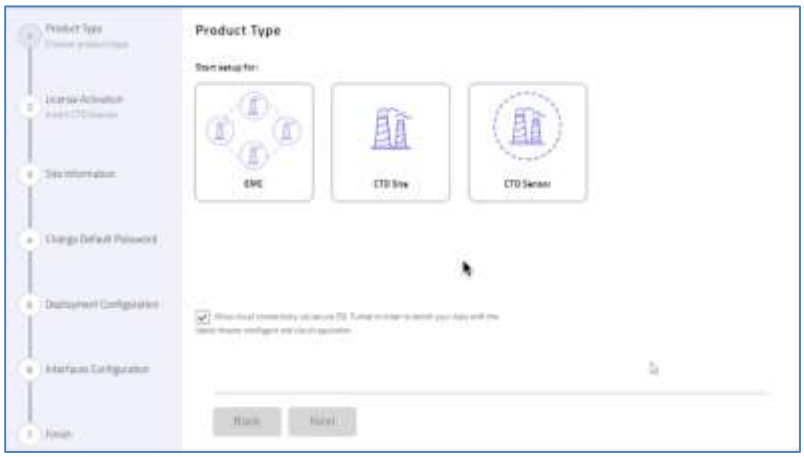


Figure Error! No sequence specified. **Product Type selection**

■ If you choose to install an **EMC** or a **TIV Site,** the additional configuration options are as follows:

Figure Error! No sequence specified. **Configuring Additional Options for TIV Site**

- **Active Query** – When selected, TIV's Active Query data collection enables active discovery of assets by scanning and then performing precise queries tailored to the network typography. Active Query is disabled by default. For more information refer to the *TIV User Manual: Active Queries.*
- **App DB** – When selected, TIV's Application Database (App DB) mechanism onboards assets from PLC configuration files or projects to enhance asset coverage. It is enabled by default as shown above. App DB extends the system's asset inventory by including assets that are not available directly through the network. For more information refer to the *TIV User Manual: AppDB.*
- **Cloud** – When checked, Cloud updates are configured as described in the *TIV Reference Guide*.

- As described above, choose to activate Active Query, App DB and/or Cloud detection, and press **Next**.

Note that the steps below have variations depending on which product is being installed.

4.3 Step 2: Activate the License

You can start with the production license or opt to use a temporary license for the initial 14 days.

Contact Tripwire to get a Tripwire **License Key**.

- Approve the **License Agreement** and set the TIV network configuration.
- Wait until the **License Activation** screen shows up.
- Obtain a License Key from Tripwire using the UUID that you see on the screen, enter it into the system and press **Activate**; or click the **Skip** option to use a temporary license (which is valid for 14 days).

Figure Error! No sequence specified. **License Activation screen**

- To apply for the license for your production server, please contact Tripwire Support or your direct partner.

4.4 Step 3: Site Information

The EMC is TIV's central appliance, usually located at the Security Operations Center (SOC) or at the corporate site, and you can name it as you wish.

Enter an appropriate name and an optional description for the machine you are configuring and then press **Next**.

Figure Error! No sequence specified. **Site Info for an EMC**

Figure Error! No sequence specified. **Site Info for a TIV Site**

4.5 Step 4: Change Password (for EMC or TIV Site)

In order to increase security, you can change your default password:

Figure Error! No sequence specified. **Change Default Password**

This is the last step for the EMC setup.

4.6 Step 5: Deployment Configuration

The next step is to set the Deployment Configuration, which differs for each product type.

4.6.1 TIV Site: Site Information and Deployment Configuration

The TIV Server performs DPI processing and will process the data from desired network.

Figure Error! No sequence specified. **EMC Information for connecting to TIV Site**

- Check the SSL checkbox ☐ Enable SSL connectivity (beta) if you prefer to use SSL (beta) instead of the default SSH communication.
- To connect the TIV Site to the EMC:
  - Enter the EMC IP address and the **Access Key** or choose **Skip** if the EMC is not configured.

- **EMC Access Key** – The access key is a password from the EMC. It lets the TIV Site authenticate with the EMC or the Sensor authenticate with TIV Site. The EMC's access key is accessible in **Settings > Management > Deployment Architecture > Deployment Configuration**:

Figure Error! No sequence specified. **EMC Access Key**

4.6.1.1 Step 6: Interface Connectivity for TIV

Select to process data to the desired interface from which the system will collect data:

Figure Error! No sequence specified. **Interfaces Configuration**

. **Process Data** – Button for obtaining more information about the interface. OFF by default.

2. **Device Status** – If the interface link is UP (connected) it is a Green dot; if it is DOWN (disconnected or unavailable) it is a Red dot.

   a. **Bit rate** (MB/s) – Describes the amount of traffic passing in this interface

   b. **Unicast Traffic** – Describes the quality of your traffic by counting unicast packets (Low, Medium, High)

   c. **OT Traffic** - Describes the amount of OT traffic on this interface (Low, Medium, High)

3. **Allocate to Network** – Displays the Network this interface is connected to. You can add new network. Each interface can be connected to one network.

4. **Filters** – Use this button to add filters to the traffic in the network, such as tcpdump capture filters.

5. **Record** – Press this button when you want to record a PCAP file for the traffic on a network for investigating the PCAP file.
6. **Download** – Press this button to download the recorded PCAP file to your machine
7. **Dump Size** – Shows the size of the network traffic file that was recorded.
8. **Save Changes** – Press when done to commit your settings.

4.6.1.2 Advanced Network Settings

Open this area to configure the following advanced network settings:

. **Network** – Set to Default. Use the Edit button to modify your network settings.

2. **Store Raw Data (PCAP)** – When selected, this button lets you to save a .pcap file for each alert that raised in the system.
3. **Known Threat Alert detection**– TIV uses a sophisticated signatures-based database in order to identify known attacks. We recommend setting this button to ON.

You have successfully finished installing the system.

Refer to the *TIV User Guide: Interface Configuration* and *Configuring Log Settings* for configuration details.

4.6.2 TIV Sensor: Deployment Configuration

Set the details for your TIV Sensor as follows:

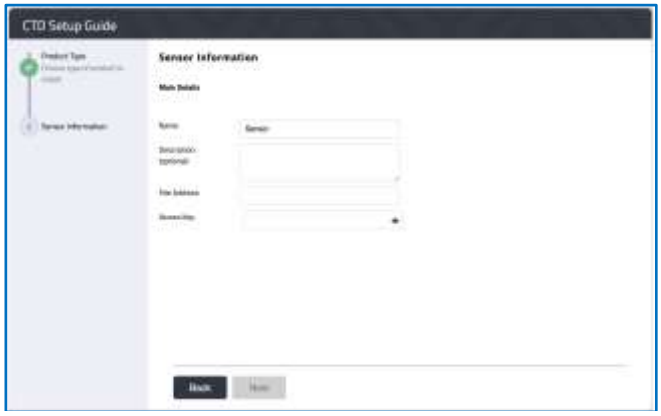


Figure Error! No sequence specified. **TIV Sensor Configuration**

- Enter the Sensor **Name*** (mandatory)
- Provide an informative **Description** (optional)
- Set the **Site address** and **Access key**:
  - **Access Key for the Sensor** – The access key for the Sensor is a password from the Site. It lets the Sensor authenticate with TIV Site. You can find

the access key in **Settings > Management> Deployment Configuration > Deployment Architecture**.

You have successfully finished installing the TIV Sensor.

Figure Error! No sequence specified. **Sensor setup complete**

4.6.2.1 TIV Sensor Info in TIV

Enter the TIV Site UI, and navigate to **Settings > Management > Deployment Architecture > Deployment Configuration**:

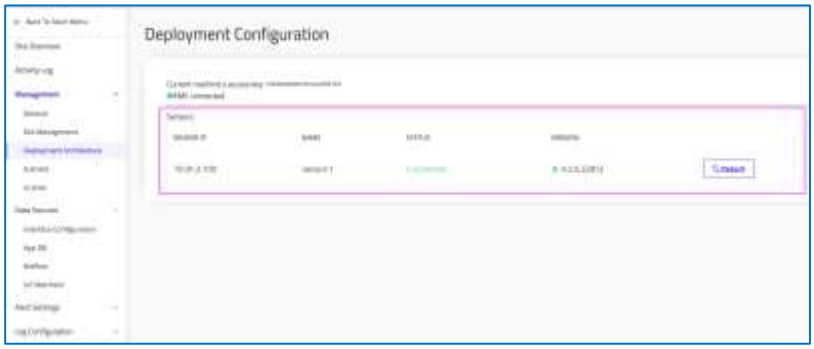


Figure Error! No sequence specified. **Sensor Info screen in Settings > Management > Deployment Architecture > Deployment Configuration**

The Sensor tab will now appear in the Interface Configuration page with the relevant properties:

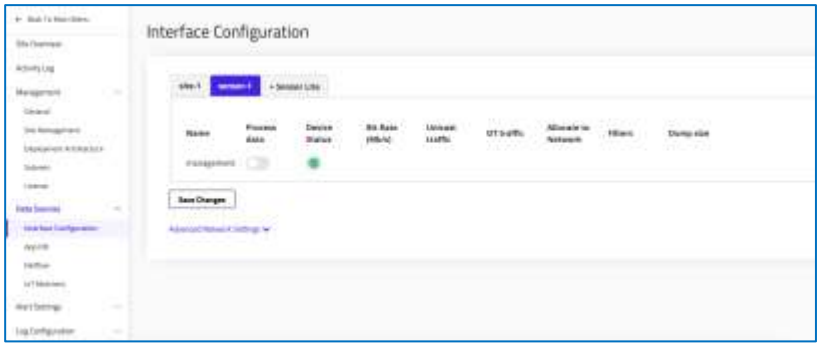


Figure Error! No sequence specified. **Sensor Tab in Settings > Data Sources > Interface Configuration**

4.6.3 TIV Sensor Lite: Deployment Configuration

The TIV Sensor is designed for setups in which the bandwidth between the TIV Sensor and the TIV Server is very limited and should be limited to a bare minimum. It will connect to the TIV site and send data.

4.6.3.1 Step 6: Interface Connectivity for TIV Sensor Lite

From TIV, connect to the Sensor as follows.

. Navigate to **Settings > Data Sources > Interface Configuration**.

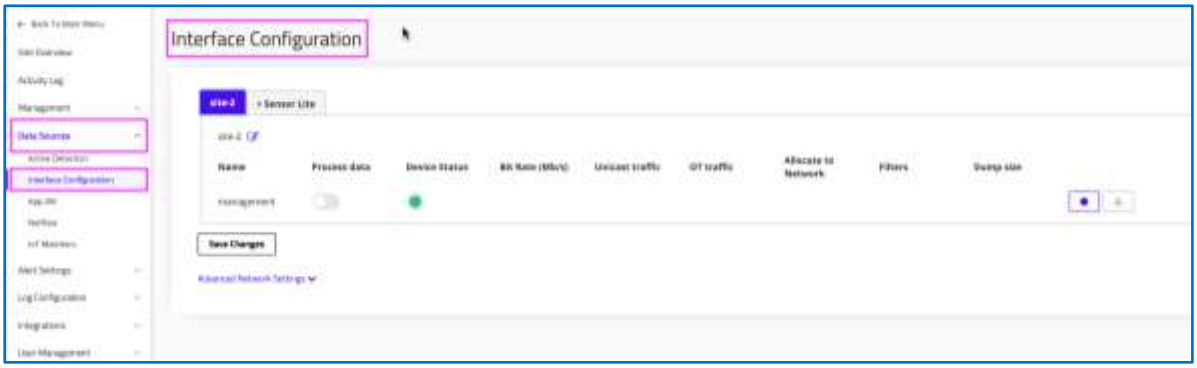


Figure Error! No sequence specified. **Interfaces Connectivity**

2. Select the **Sensor Lite** tab and enter the following information:

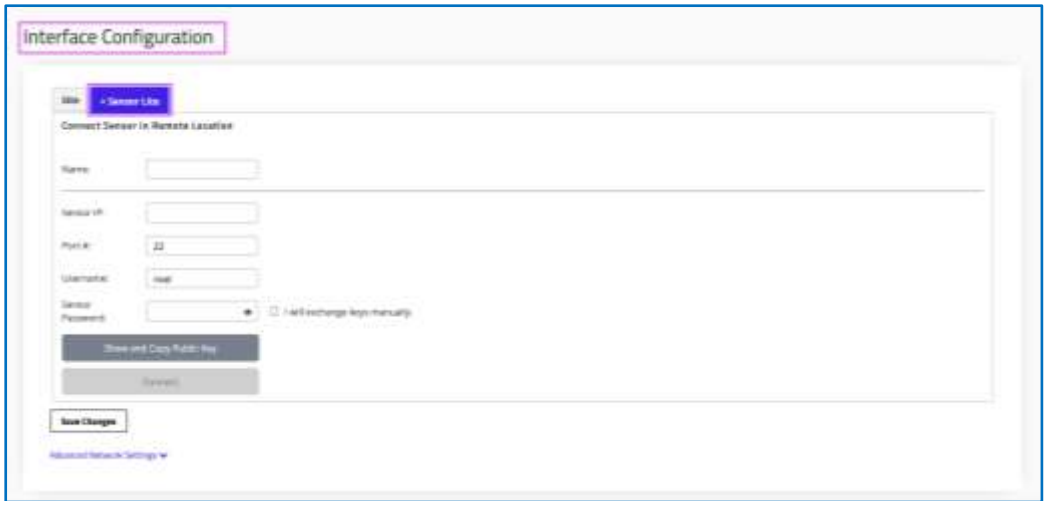


Figure Error! No sequence specified. **Sensor Lite tab**

a. **Name** – The name of the sensor

b. **Sensor IP** – The IP address of the sensor

c. **Port#** – Enter the desired port. The default port is 22

d. **Username** – Enter the username for the sensor

e. **Sensor Password** – The sensor's password

f. **Save Changes** – When all the information is correct, press **Save Changes**.

For **Advanced Network Settings**, see section 4.6.1.2 above for modifying the network, storing raw data and using Known Threat alerts for the sensor.

You have successfully finished installing the sensor. The Sensor Lite tab now appears in the **Interface Configuration** page with the relevant properties:

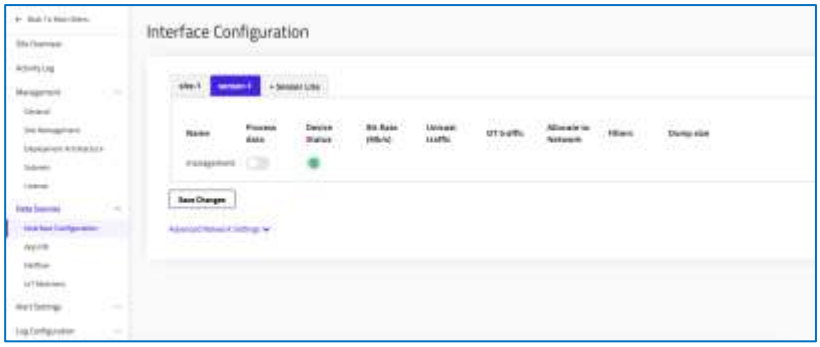


Figure Error! No sequence specified. **Sensor Lite Tab in Settings >Data Sources > Interface Configuration**

5 Upgrade Procedure for ClarotyOS

Prerequisite: First, upgrade the EMC with the following instructions. After the EMC finishes upgrading, you can upgrade the connected sites automatically through the EMC.

> Note When upgrading the EMC, the EMC Insight operation statuses are deleted, assuming that the Site statuses are more significant. If otherwise, contact Tripwire Support to retain the EMC Insight actions.

To upgrade the EMC/TIV manually:

- Go to the **ClarotyOS Configuration** page (through TIV) and navigate to the **Upgrade** tab.
- In the Upload Bundle area, upload your upgrade bundle and click Upload File.

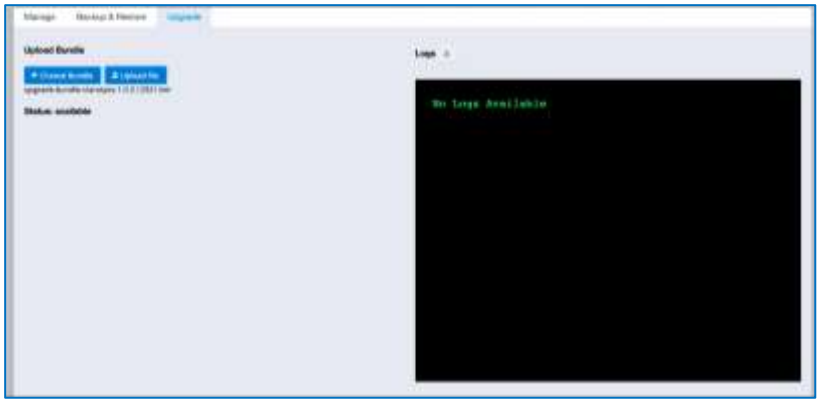


Figure Error! No sequence specified. **Upload the bundle**

- Wait until upload is finished.
  - Follow the green progress bar on top

Upgrade your machine from by clicking on the Upgrade tab:

- **Choose Bundle** – Choose a file from TIV in order to get specific fixes or upgrades
- **Upload File** – Upload to TIV in order to upgrade your machine to a higher version or to allow specific fixes.

> Note Watch the logs to ensure your upgrade was successful. If it failed, please consult Tripwire Support and send the presented logs.

- Read the Bundle Information and click **Upgrade**:

Figure Error! No sequence specified. **Bundle Information**

- Wait
  - Follow the upgrade's logs on the right side of the screen:

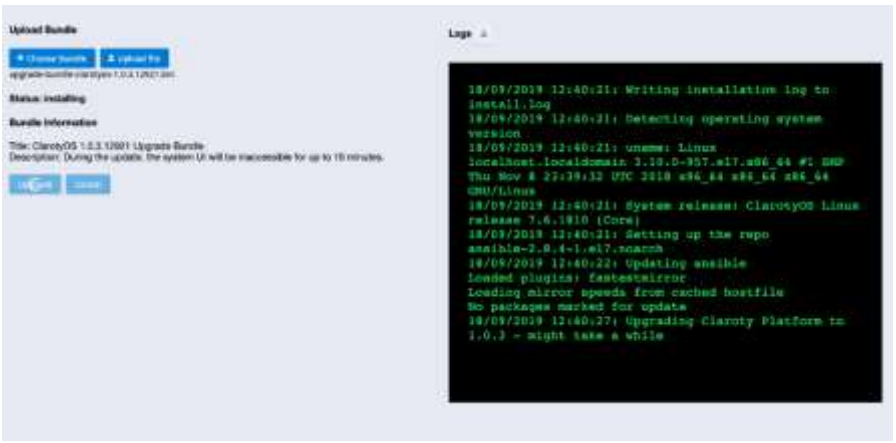


Figure Error! No sequence specified. **Read the Logs**

> Note If the service will be restarted during the upgrade, your connection will be lost for a few minutes.

- When the upgrade is finished, the Status will change to "Success" or "Failed".

Figure Error! No sequence specified. **Upload bundle**

- You can download the logs file (on the top-right download button).

After the EMC upgraded successfully, you can login to the site maintenance window and upgrade your connected TIV site.

> Note: The connected sensors will be upgraded by default after the TIV is upgraded.

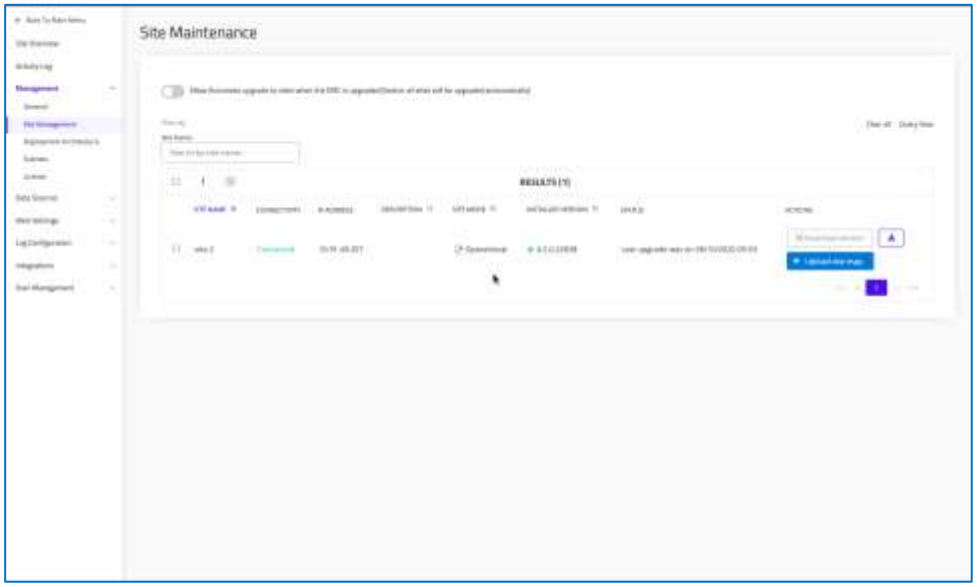


Figure Error! No sequence specified. **Site Maintenance**

6 Upgrade Procedure for CentOS and RHEL via Commands

To upgrade the system via bash commands:

. Copy the `tar` file to your machine.

2. Extract the tar file:

```
tar -xvf <tar_file_name>
```

   - The system prints installation extraction DIRs

3. Enter the TIV directory.
4. Choose whether you want to run the TIV installation script with default options or specify your preferences for optional flags.
5. To install TIV with default options, run:

```
./install.sh
```

6. The system will ask if you want an upgrade or a clean installation. Choose if you want to back up the old configuration:

```
Do you want to upgrade to <new_version #>? [U] or perform a
clean install [C]? : u
```

7. Choose if you want a backup.

```
Do you want to backup previous configuration? [Y/N]: y
```

8. When you respond 'yes', you are prompted to choose a backup directory and path:

```
Please choose backup directory: [root]
```

9. The system asks you to confirm if you are upgrading from a previous version to the current one, and the backup directory and path:

```
Upgrading TIV from <current_version #> to <new_version #>,
performing backup in /root. Are you sure? [Y/N]:
```

10. When you respond 'Yes', TIV performs the backup and the upgrade.
11. After installation is successfully completed, the following output appears:

```
Done – TIV successfully installed
```

12. If the installation failed, see the `install.log` file for details.

7 Backing up and Restoring for ClarotyOS

7.1 Backup

In this screen you can easily Backup your system in two ways:

- **Local** – Backup the data on your local machine
- **Remote** – Backup your data on a remote machine via the SMB protocol.

Navigate to the **Configuration > ClarotyOS > Backup & Restore** tab.

Specify the following fields:

- **Type** – for example SMB
- **Path** – the path the file will be saved in
- **Username** – the username of the remote machine
- **Password** – the password of the username you entered

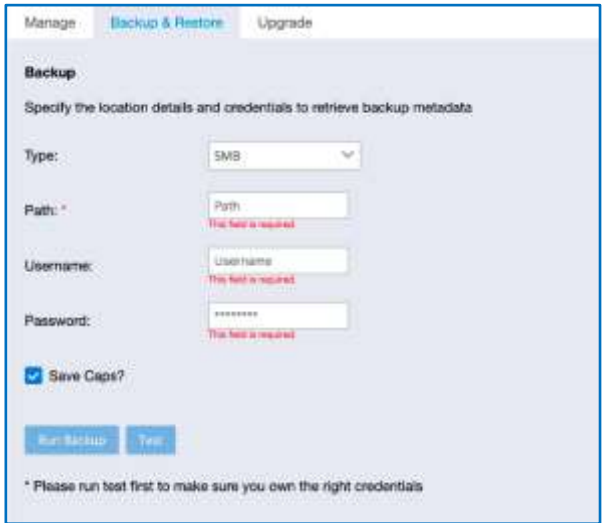


Figure Error! No sequence specified. **ClarotyOS - Backup and Restore - for Upgrade**

7.2 Restore

7.2.1 Restore Latest

To restore the latest backup you created in this ClarotyOS server:

. You can see the time of the latest backup under **Restore**

2. Click Restore Latest:

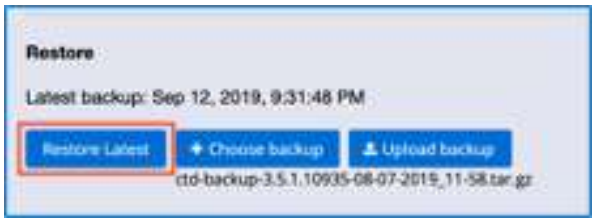


Figure Error! No sequence specified. **ClarotyOS - Restore Latest**

7.2.2 Upload Backup and Restore

. Under Restore, click Choose Backup:

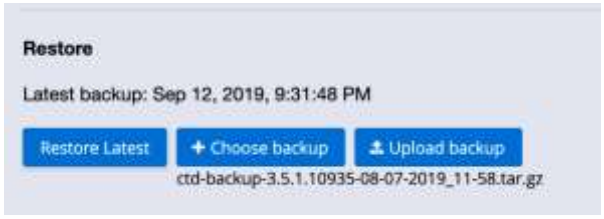


Figure Error! No sequence specified. **ClarotyOS -Choose Backup**

2. Click Upload Backup:

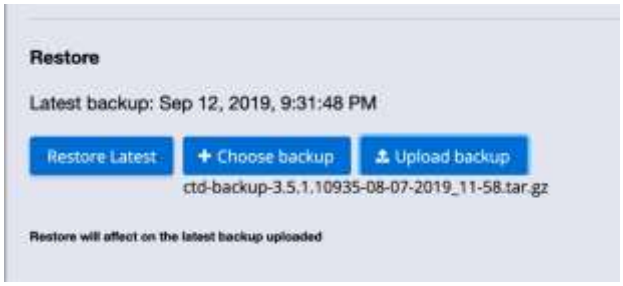


Figure Error! No sequence specified. **ClarotyOS - Upload Backup**

- Press **Restore Latest** and wait for the restore to end.

8 Backup and Restore Procedure for CentOS and RHEL via Commands

The installation process enables restoration when an upgrade fails. The Backup and Restore processes enable creating a full backup of the system, including all relevant system information and databases. A complete backup can be performed in a single file. This enables TIV to be restored on your machine or moved to another one. When the version of the backup file is lower than the installed TIV version, the script suggests migrating the data to the installed version.

8.1 Backing up TIV

To backup TIV:

. Go into the `/opt/icsranger` directory via the terminal.

2. Activate the `backup_ranger.sh` script. The script is stored in the `/opt/icsranger` directory with the time and date:

Example

```
[root@localhost - ] #cd /opt/icsranger/
[root@localhost icsranger] # ./backup_ranger.sh
Backup target is /opt/icsranger
Done - Backup successfully created
Backup tar: /opt/icsranger/ranger-backup-xxx.xxxxx.tar.gz
```

3. Provide a location for the backup file.

4. The backup file is named `ranger-backup-[version number].tar.gz`.

8.2 Restoring TIV

To restore TIV:

. Navigate to the `/opt/icsranger` directory via CLI.

2. Activate the `restore_ranger.sh` script with the filename.

3. In case the backup `.tar` version was taken by an old version of TIV, the script will suggest running migrations for you.

4. The restoration script restores TIV as backed up and starts automatically. You can run the script with `"--migration"` and skip the question.

> Note Migration is limited to cases in which there were no major changes between the versions. In case of a major change between versions, first install the backup's TIV version, restore TIV, and then upgrade.

Backup and Restore Example

```
[root@localhost icsranger]# ./restore_ranger.sh ranger-backup-
x.x.x.xxxxx-DD-MM-YYYY_hh-mm.tar.gz
```

```
DD-MM-YYYY hh:mm:ss: Done - /opt/icsranger/ranger-backup-
x.x.x.xxxxx-DD-MM-YYYY_hh-mm.tar.gz successfully restored
Ranger will start automatically in a few seconds
```

9 Installation Reference

9.1 Package Contents

- `ctd_deps/` – Contains the various dependencies required by TIV.
- `ctd/` – Contains TIV RPMs.
- `install.sh` – Installation bash script for TIV.
- `install.log` – Log of the installation process as it is run using the installation script.
- `Readme.txt` – Includes installation instructions and release notes.
- `Harden-*.tar.gz` – Extract this file and run `apply.sh`.

> Note The hardening runs automatically from the appliance image.

9.2 Installation Optional Flags

You can run the TIV installation script using the installation options as provided. If a command is not selected, a corresponding question will be presented.

```
./install.sh [options]
```

Command	Outcome
-b [PATH_TO_DIR] ***or*** **--backup-dir [PATH_TO_DIR]**	Choose a backup directory and perform backup
-- no-backup	Do not back up previous configuration
-u ***or*** **-- upgrade**	Upgrade current TIV installation (if exists)
-y ***or*** **auto-run**	Answer yes to Validate question (auto run)

Command	Outcome
`--online`	Use online repositories during installation This option should be used when the server packages were updated prior to the installation of TIV. For example, if a “yum update” was previously run on the machine. Note: This flag is only relevant for machines that have internet access.

`-h`
or
`-- help`
	Print this help

The options can be used either by the flags above within the `install.sh` command, or by answering the questions.

> Note The questions appear when the flags are not used.

Example

```
./install.sh -no-backup -no-upgrade
```

9.3 Additional Components

The following optional components are also supported:

- Active Directory
- SIEM

9.4 NTP Usage

- TIV Servers can use NTP from any source that provides NTP.
- EMCs can use NTP from any source that provides NTP.
- Sensors do not require NTP.

9.5 Sensor Setup via CLI Commands

9.5.1 Adding a Sensor to a Standalone Site

In order to connect a Sensor with a Standalone TIV Server via CLI, log into each system via SSH or the local console.

Step 1: Bootstrap the Standalone TIV Server

Bootstrap the standalone site by executing the following commands from CLI:

```
lkpocli manager api configurator bootstrap site_name='site name'
lkpocli community init --name 'site name' --bootstrap_password
1234
```

Step 2: Bootstrap the Sensor

Execute the following command:

```
lkpocli manager api configurator bootstrap_sensor ‘sensor name’
‘site IP address’
```

e.g.

```
lkpocli manager api configurator bootstrap_sensor Sensor
10.10.10.1
```

> Note The default password of the community is 1234.

In case the password has been changed, there is a need to add the new password along with the command.

For example, if the password is 123456, the command should be as follows:

```
lkpocli manager api configurator bootstrap_sensor Sensor1
10.10.10.1 bootstrap_password=123456
```

Step 3: Verify that the Sensor has been added to the TIV Server

. Run the following command:

```
lkpocli community friends
```

Step 4: Verify the Output

The output should display:

- The name of the site
- The IP address of the site
- The ports that are communicating

9.5.2 Bootstrap & Connect Sensor to TIV Server Connected to EMC

This section describes how to connect a Sensor to a TIV Server that is already connected to an EMC.

Step 1: Bootstrap the EMC (Central)

. In order to connect a Sensor with a standalone TIV Server, connect into both machines from CLI:

```
lkpocli manager api configurator bootstrap_central

lkpocli community init
```

2. Provide the name of the EMC machine
3. Provide the bootstrap password.

Step 2: Bootstrap the TIV Server to Join the EMC

. Proceed to the Configurator and bootstrap the standalone site.

2. Join the site to the EMC (as described in Step 1)

3. Verify that the site has been added to the EMC by running:

```
lkpocli community friends
```

Step 3: Add the Sensor

. From the TIV Server: Perform the following command:

```
lkpocli manager api community init_server 1234
```

> Note The default password of the community is 1234 as previously shown; you can modify it accordingly.

2. From the Sensor: Perform the following command:

```
lkpocli manager api configurator bootstrap_sensor ‘sensor name’
‘site IP address’
```

- In case the password has been changed, there is a need to add the new password along with the command.
- For example, if the password is 123456, the site IP address is 10.10.10.1 and the name is Sensor, then the command should be as follows:

```
lkpocli manager api configurator bootstrap_sensor Sensor
10.10.10.1 bootstrap_password=123456
```

9.6 NAT/PAT Mappings

TIV supports the mapping of internal and external addresses in a NAT/PAT environment. It was built so several address spaces from several internal networks may overlap.

In this case, a network would automatically be generated for each internal network, holding all internal assets.

Internal networks are generated with the name `autogen-nat-translated-router-network:ROUTER_IP`

Configuration of NAT/PAT Settings

NAT/PAT settings are configured from the command line using an input tab-separated file with each line having the following format:

```
"ROUTER_NAME"  EXTERNAL_ADDRESS    EXTERNAL_PORT   INTERNAL_ADDRESS
  INTERNAL_PORT   TCP|UDP
```

For example:

```
"TB ROC"   10.185.51.41    4002    192.168.1.2 4002    TCP
```

Files can be loaded from the command line as follows:

```
lm nat_translator load_csv PATH_TO_CSV_FILE
```

Errors in this process will be reported via the console screen and TIV activities.

The system is able to generate the following errors:

- `CSV file not found`
- `Not enough columns`

- `Failed to generate JSON PAT configuration, too many routers`
- `Invalid router IP`
- `Invalid PAT IP`
- `Invalid router port`
- `Invalid PAT port`
- `Invalid routing! Double translation`
- `Received empty file`

> Note If a problem occurs with loading a specific record, the system will make the best effort in parsing the rest of the file.

> Note Data is built on a per-site basis, where sensors get their data from their respective site.

9.6.2 Extracting PAT data from Ubiquiti Network Management Server integration

TIV is able to pull data automatically from the Ubiquiti NMS server in order to feed its NAT/PAT configuration.

NMS Server Configuration

. In order to allow automatic extraction of NAT/PAT data from NMS server, create an API key in the NMS server configuration.

2. Server configuration can be done by executing from the command line:

```
lm nat_translator set_unms_server_information API_KEY SERVER_URL \
OUTPUT_FILE PERIODIC_DOWNLOAD_INTERVAL_SECONDS
```

3. After configuration, download from the server can be initiated by using the following command:

```
lm nat_translator download_from_server
```

4. Output would be a CSV file adapted for TIV as input for NAT/PAT mapping.

5. Another option would be to periodically download data from the NMS server. This can be started and stopped by using the following commands:

```
lm nat_translator start_periodic_download
lm nat_translator stop_periodic_download
```

9.7 Advanced Configuration

9.7.1 Importing non-standard port allocations from Kepware KEPServerEX

Kepware's KEPServerEX is a software suite for handling automation data. TIV uses the data from Kepware KEPServerEX for defining non-standard port allocations.

Since some devices are listening on non-standard ports (such as, MODBUS on 4004), Tripwire is able to use Kepware's JSON configuration files for translating the end port received (such as, 4004) to the actual protocol (for example, Modbus).

9.7.1.1 Configuration

To configure a Kepware-based port allocation:

. Download the JSON configuration files to a persistent path on the machine

2. Run from the command line:

```
lkpocli manager api manager set_config kepware_path \
PATH_TO_KEPWARE_FILE_OR_DIRECTORY_OF_FILES
```

3. Restart TIV for the changes to take effect.

> Note Configuration is done on a single site basis - meaning that sensors would automatically be configured by their respective site.

> Note After the configuration has been set, it will be loaded for the specified file on every startup of TIV.

To de-configure the Kepware-based port allocation:

- Execute the following CLI command:

```
lkpocli manager api manager set_config kepware_path
```

9.8 Support for Bridge Network Interfaces

Bridges are a way to forward network traffic between two or more network interfaces.

You can use the admin shell to support the bridge network interfaces. In the admin shell the command `network` is used to view and manage network-related settings.

Here's a list of the bridge commands:

```
[admin@localhost]# network bridge
Usage: network bridge [OPTIONS] COMMAND [ARGS]...

  Manage bridges

Options:
  --help  Show this message and exit.

Commands:
  add_interface     Adds a network interface to a bridge
  configure         Configure a network bridge
  create            Creates a new network bridge
  delete            Deletes an existing network bridge
  remove_interface  Removes a network interface from a bridge
```

To use bridges, you'll first need to create one using `network bridge create`. Then, you're able to configure, and add network interfaces to the newly created bridge:

```
[admin@localhost]# network bridge create
Bridge 'bridge0' created
[admin@localhost]# network bridge add_interface bridge0 enp0s9
[admin@localhost]# network bridge add_interface bridge0 enp0s8
[admin@localhost]# network bridge configure bridge0
Fetch IP automatically from DHCP? [y/N]: y
Detecting available IP from DHCP...
Detected offer: 192.168.0.6
Detected offer: 192.168.0.5
Do you want to proceed? [Y/n]: Y
[admin@localhost]# network show
Bridge 'bridge0' (08:00:27:30:AE:B1): [Activating]
        Interfaces:
                enp0s8 (08:00:27:E9:AA:10)
                enp0s9 (08:00:27:30:AE:B1)
```

Bridges might take up to a minute until they're fully initialized, so please be patient.

Bridge support in the UI

To attach a network interface to a bridge, you'll need first to press "Create Bridge" under the "Bridges" tab:

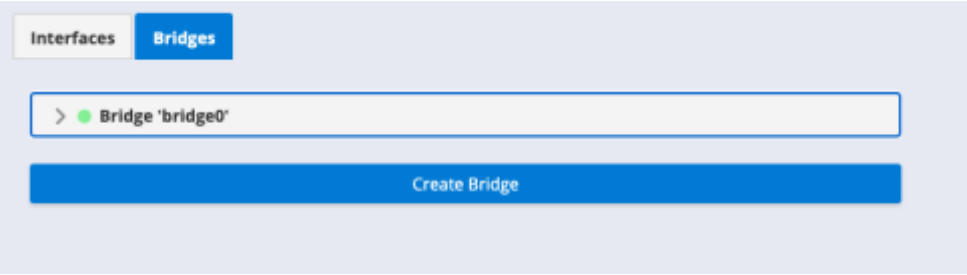


Figure 1: Create Bridge

After you generate a bridge, a new bridge instance will be generated without any interfaces. You can Attach an interface to a bridge by pressing the "Attach to Bridge" button on the desired interface. (Make sure to press the Update button first if you changed some settings on that network interface).

You'll be prompted to choose a bridge to be attached to:

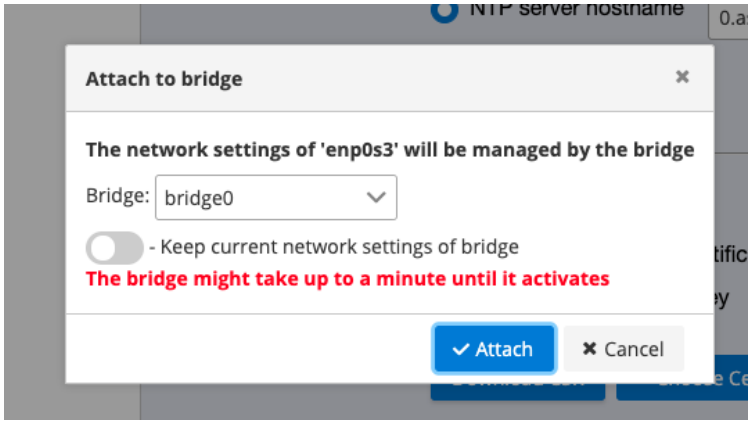


Figure 2: Attach to Bridge

You also have an option to migrate this interface's network configurations to the chosen bridge. This will override the bridge's current network settings (disabled by default as you can see on the image above). You'll want to use this only if you'll lose connection to the server by attaching that network interface.

After attaching a network interface to a bridge, the interface cannot be managed individually as you can see on the image below:

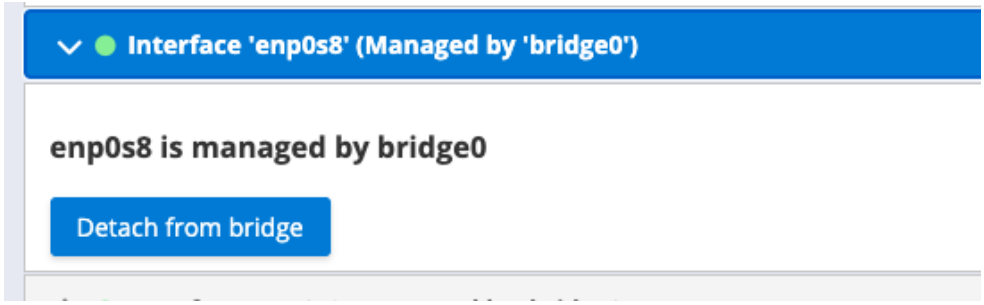


Figure 3: Detach from Bridge

The network interface will have bridge0's network configurations. You can detach the network interface either by pressing the "Detach from bridge" button, or from the bridge0's "detach" link of the desired interface:

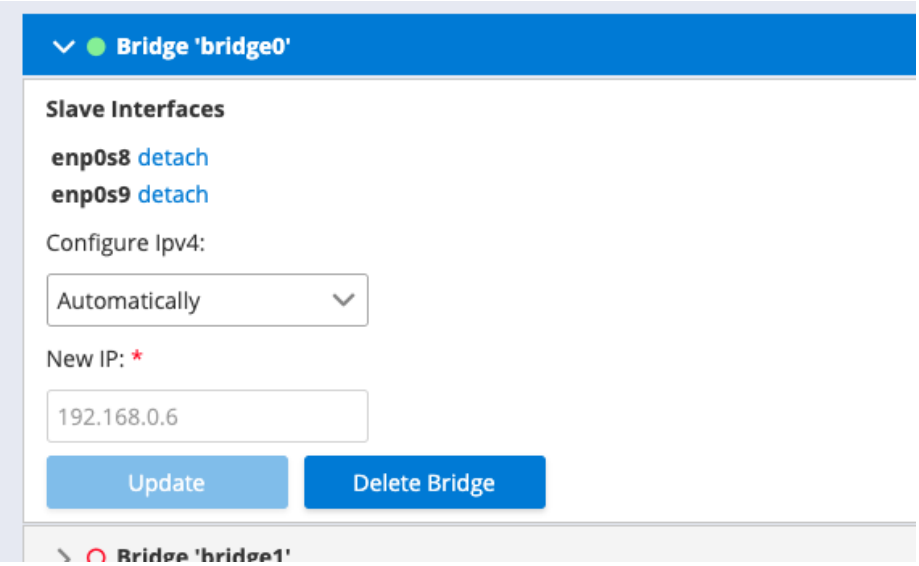


Figure 4: Detach Link

You'll be prompted once again with an option to migrate the bridge's network settings into the network interface. This action will erase the bridge's network settings so there won't be a conflict.

9.9 Support for Tripwire Hardware Plugin

We added support for Tripwire Hardware Plugin for better integration with their dedicated hardware. This plugin is dedicated to ClarotyOS instances with Tripwire's hardware specifications - The LAN Bypass. It installs the SDK required to manage the hardware and web interface.

To Install:

. Go to the upgrade page

2. Upload Tripwire Hardware BNI

3. Run upgrade

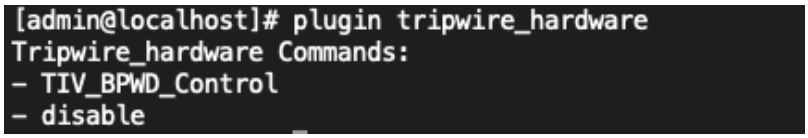
4. Reload web page

Web Management

The switches control LAN Bypass and its Watchdog process.

Figure 5: LAN Bypass and Watchdog Process

Shell Commands



- Enabling/Disabling Lan Bypass:

```
plugin tripwire_hardware TIV_BPWD_Control TIV_BPWD_Control -lbp_rescue <on|off>
```

- Enabling/Disabling Watchdog:

```
plugin tripwire_hardware TIV_BPWD_Control TIV_BPWD_Control -wdt_s_alone <on|off>
```

- To check the status:

```
plugin tripwire_hardware TIV_BPWD_Control TIV_BPWD_Control -qry_state all
```

10 Exporting Data

10.1 Overview

The system exports assets to an external database, the External Data Component. After it is configured, the Export Data Server (EDS) is the TIV component responsible for exporting the assets.

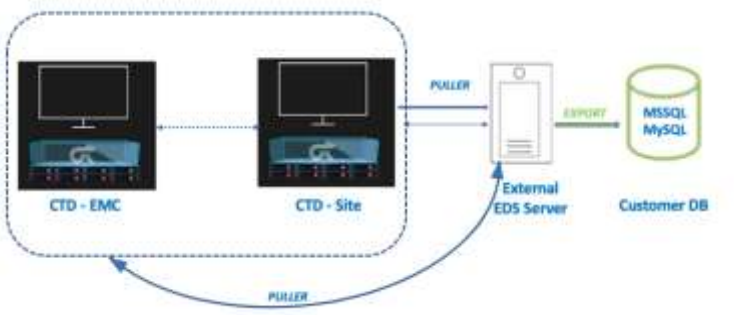


Figure Error! No sequence specified. **Flow - External Data**

10.2 Prerequisites

After the Export Data Server is configured, the DB of the supported platforms should comply with the following requirements.

The Export Data Server is supported on RHEL or CentOS v7.6 (Minimal) or higher with MySQL database. Alternatively, the Export Data service can be installed on the Linux machines and the database can be separated into a different machine on Windows Server 2008 and MSSQL 2012 and higher.

Table 1 Supported Platforms

OS	OS Version	Database	Agent
Linux RHEL	7.6 (Minimal) or higher	√ MySQL	√
Linux CentOS	7.6 (Minimal) or higher	√ MySQL	√
Windows	Windows Server 2008	√ MSSQL 2012 and above	X

The machine specifications are according to the following table:

Table 2 Export Data Specification

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

Capacity - Export Data for up to:	#CPU Cores	RAM	Required Free Disk Space (not including OS)	Disk Type
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

> Note The agent can be installed only on RHEL or CentOS.
> The database can either MySQL or MSSQL, and the MSSQL will be installed on Windows.

10.3 Database Schema

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

10.3.1 Database Assets Table

Table 3 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 assigned 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

Field Name	Key	Type	Comment
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
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	The 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.

10.3.2 Database Stats Table

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

Table 4 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

10.3.3 Database Slots Table

The Slots table stores the PLC slots per combination of central, site, and asset:

Table 5 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

Field Name	Key	Type	Comment
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 PLC slot

10.3.4 Database Protocols Table

The Protocols table stores the protocol names per asset:

Table 6 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

10.4 Installation and Configuration

10.4.1 Installing the Export Data Server Component

. On an RHEL or CentOS 7.6 (Minimal) 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
```

In the database create user with full permissions. The username and password should be provided to the Export Data server.

Type in the command:

```
passwd bootstrap.
```

Set the password for the user “bootstrap”.

> Note: The password you set for the user bootstrap and the actual bootstrap password of your EDS must match exactly.

Bootstrap the server as the Export Data component:

```
lkpocli manager api --worker export_data_puller api bootstrap
username=<DB USERNAME> password=<DB PASSWORD>
db_type=<mssql/mysql> hostname=<IP/hostname> db_name=assets_db
```

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>
```

10.4.2 Registering TIV or EMC for Exporting Data

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

. Connect to the TIV server with SSH.

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 **Log Configuration > Export Discovered Data**, select the **Export Data** page:

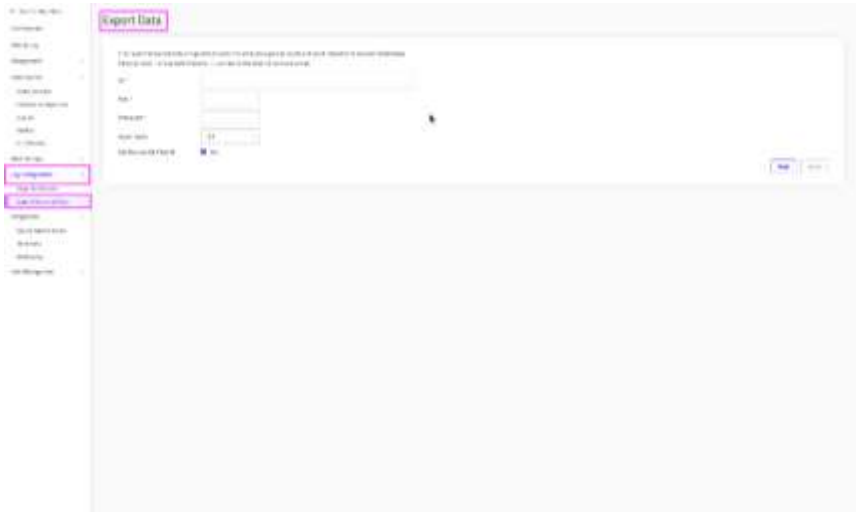


Figure Error! No sequence specified. **Registering TIV - Export Data**

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

   c. **Password*** – The password 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)

10.4.3 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:

. 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 10.4.1).

> Limitations:
>
> Manual edits on assets are not pushed via the export data feature.
>
> Assets can only be sent with IPv4.

10.4.4 Maintenance of the Export Data Server

- 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.

10.4.5 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`.

10.4.6 Open Ports

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

- 9300

10.5 Export Data Troubleshooting

Use the following commands for basic troubleshooting:

- On the Server – to view the log file:

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

- On the TIV site to view any issues or errors

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