tripwire®

TRIPWIRE®
INDUSTRIAL
VISIBILITY

TRIPWIRE INDUSTRIAL VISIBILITY 4.2.4

ClarityOS GUIDE

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Tripwire Industrial Visibility - ClarotyOS Guide Revisions

Doc Rev	TIV Version	Date	Owner	Author	Revisions
Rev 1	v4.2.1	November 2020	Daniel Ashual	Beth Stolper	Added OID Table
Rev 2	v4.1.3	September 2020	Daniel Ashual	Beth Stolper	Included Restore instructions
Rev 1	v4.1.3	August 2020	Daniel Ashual	Beth Stolper	No changes
Rev 1	v4.1.2	June 2020	Daniel Ashual	Nina Mazel	Updated
Rev 2	v4.1	April 2020	Daniel Ashual	Nina Mazel	Updated
Rev 1	v4.1	March 2020	Daniel Ashual	Beth Stolper	Updated
Rev 1	v4.0.4	February 2020	Benny Porat	Beth Stolper	No changes
Rev 1	v4.0.3	January 2020	Benny Porat	Beth Stolper	No changes
Rev 1	v4.0.1	December 2019	Benny Porat	Beth Stolper	Updated
Rev 1	v3.5.7	November 2019	Benny Porat	Beth Stolper	Initial Version

Contents

1 About ClarotyOS

ClarotyOS is the operating system based on CentOS. It enables you to use CentOS commands when you have a root shell.

Tripwire-Platform is the service running the UI.

ClarotyOS provides network and time configuration, TIV backups and restores, and an upgrade manager. You can access it through TIV's UI or with CLI commands using the Admin shell.

In the Admin shell, you can:

- Change the network & time configuration
- Get system information
- Change ClarotyOS/TIV's branding
- Run lm/lkpocli (TIV commands)
- Get a root shell.

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

2 Getting Started

2.1 Installation

2.1.1 Quick Installation via ClarotyOS

1. Insert the installation file into 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 1 Installing ClarotyOS

3. Wait until the installation is finished:

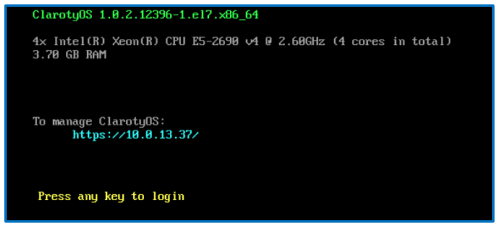


Figure 2 ClarotyOS installation complete

4. You can reconfigure your network settings by entering the Admin password and then **Run**.
5. Wait until the machine IP is presented.
6. Choose whether you prefer to configure your IP via a console using CLI or via the TIV UI.
7. Continue to the TIV Wizard.

2.1.2 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.

2.1.2.1 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:

- Approve:

- Approval message:

Creating partition, adding new "Physical Volume"

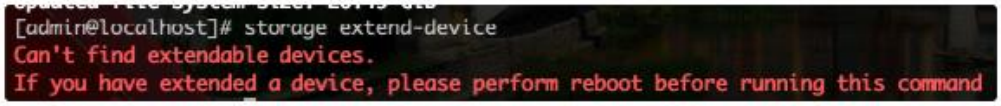
2.1.2.2 Option2: Extending an Exiting HD

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:

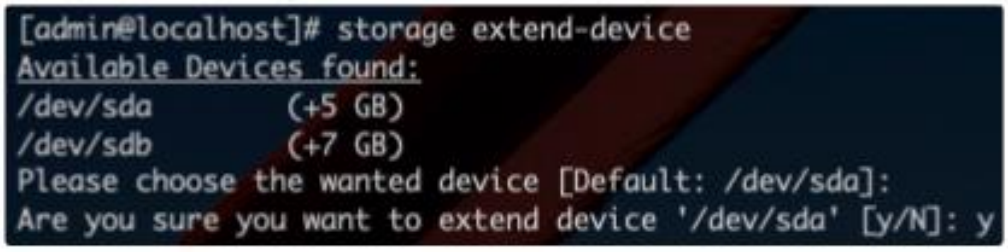
```
storage extend-device
```

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



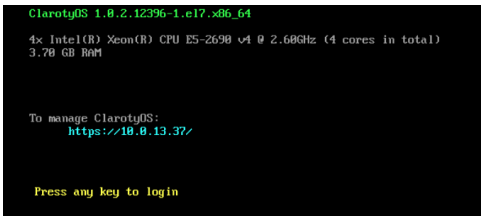
- Choose the wanted device from the list:

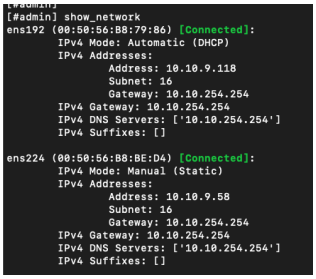
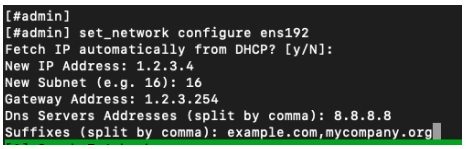
- Approve:



- Approval message:

2.1.3 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: ■ "Password1!"	
	■ Change the Default password	
	Password Handling ■ The current minimum password for the Admin shell is 8 characters. You will need to change the default password on the first login.	

	■ The password expires after 90 days. ■ After 10 failed attempts to login with the password, the user is locked out	
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	

2.1.4 Configuring your IP via the TIV UI

1. Wait until the machine IP is presented.
2. Go to https://192.168.0.222/; this is Tripwire’s default IP.
   - Ensure you are in the same network and subnet (192.168.0.0/24)
   - If you cannot connect in this manner, follow the CLI instructions.
3. Continue to the TIV Wizard.

2.1.5 Configuring your Network Settings

1. Enter the IP address of the machine in the Web Browser. The Welcome screen of the TIV Wizard appears.
2. Read and confirm the End User License Agreement (EULA).
3. Configure your server’s network.

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

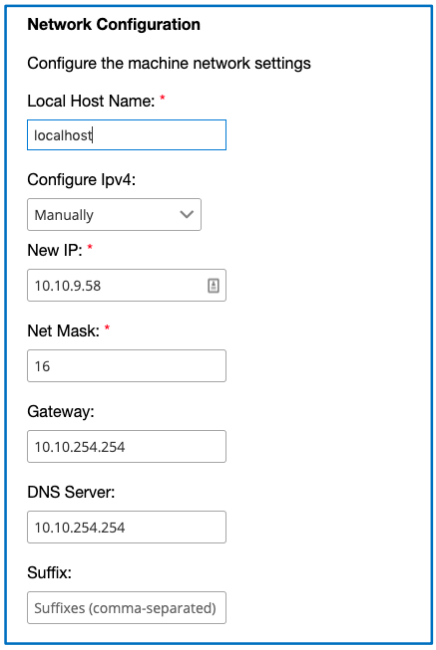


Figure 3 Network Configuration Example

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

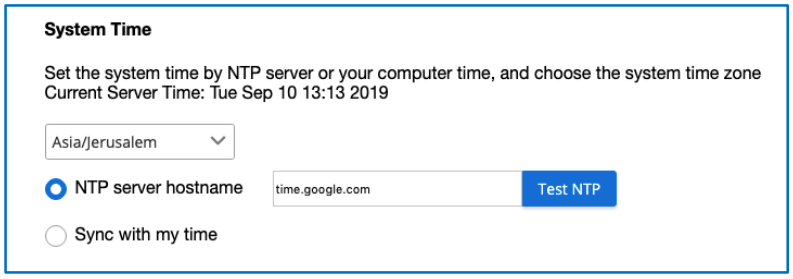


Figure 4 Configuring the Server Time

5. Press **Next**.

6. Make sure your network settings are defined correctly:

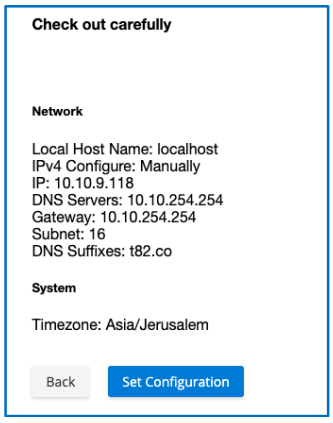


Figure 5 Setting the Configuration

7. Press Set Configuration.
   - During the configuration process the following screen appears:

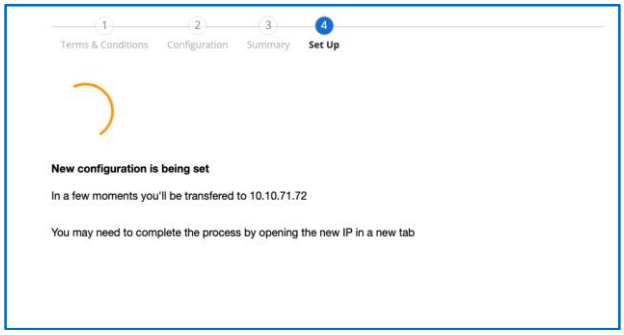


Figure 6 New Configuration Setup

8. The system redirects you to the TIV Wizard. Refer to the **TIV User Guide** for details.

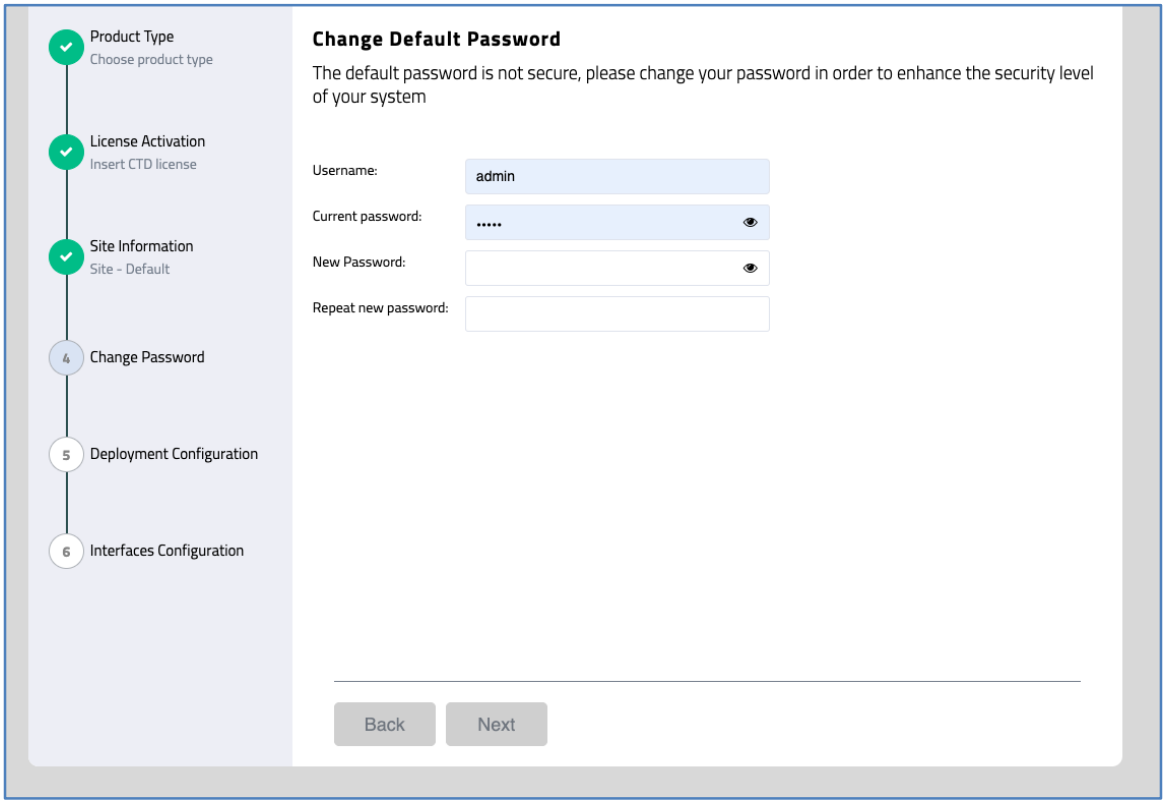


Figure 7 TIV Wizard

3 ClarotyOS General Usage

3.1 ClarotyOS IP Address

- The installation IP is 192.168.0.222
- Ability to choose the IP address during the installation process (automatically/manually, including DHCP support)

After the installation is finished, the default IP the system is uploading with is 192.168.0.222. Below this IP address the user will be asked:

- "Would you like to configure a new IP address? Y/N".

If the user chose to configure a new IP address, the user will be asked if they would like to use DHCP:

- "Fetch IP automatically from DHCP"? Y/N".

3.2 Getting ClarotyOS Configuration through TIV

1. Open a browser session for TIV.
2. Go to https://<Your TIV IP Address>/ and log in with your username and password.
3. Navigate from the **Main Menu** to **Configuration**:

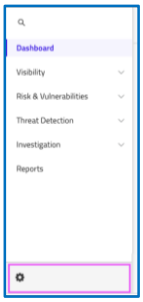


Figure 8 TIV Main Menu: Configuration

4. Navigate to **System Management** > **OS Configuration** to access the ClarotyOS Configuration and use it as described in section 4.1.

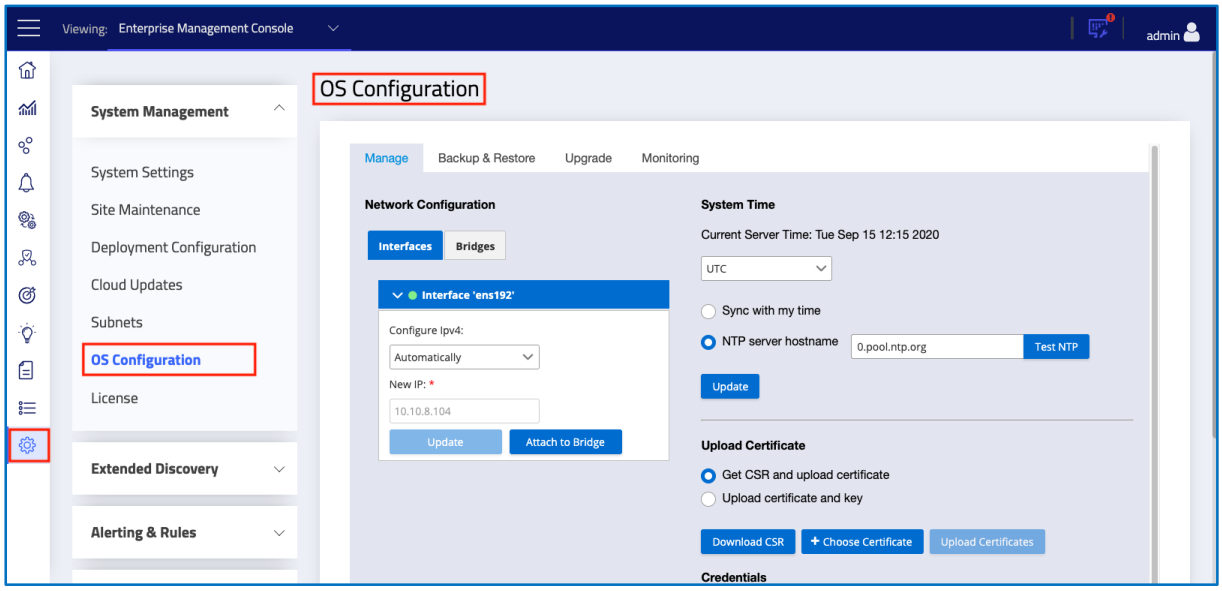


Figure 9 System Management: OS Configuration page

3.3 Admin Shell

1. Login to the ClarotyOS shell with an Admin user. You can log in through SSH or the console.
2. The Admin's default password is "`Password1!`"

> **Note** You will need to change the default password on the first login.

3. Run "`?`" or "`help`" to see the Admin commands:

```
[#admin] help

Commands (Type help <command>):
==========================
arp          exit      ip        ping       reboot       set_time
ctd          get_time  lkpocli   platform   reset_shell  show_network
date         help      lm        poweroff   set_brand    support
disk_status  htop      passwd    processes  set_network  tcpdump
```

Figure 10 Run "?" or "Help" to view the Admin Commands

4. Help is available for every command using "`--help`". For example:

```
[#admin] set_network --help
Usage: set_network [configure|disable] <interface>
```

Figure 11 Admin Shell - Help for a Command

3.4 Reset Admin's Password

3.4.1 Resetting the Admin password through the TIV UI

1. In TIV, navigate to the **Configuration > System Management > OS Configuration > Manage** tab.
2. Under Credentials, click the **Change OS Password** button (see Figure number 4).

3.4.2 Resetting the Admin password through the Single-User mode

In case you do not have access to TIV's UI, you can reset it by rebooting into "single-user mode" as follows:

1. To boot your system into single-user mode:

> Note Do not run the Reboot command

   https://www.tecmint.com/boot-into-single-user-mode-in-centos-7/

2. Before running the last command in the guide which performs the reboot, run:

```
passwd admin
```

   This will let you choose a new password for the Admin.

3. Run the Reboot command and enjoy your ClarotyOS.

3.5 Check TIV/ClarotyOS version

- In the Admin shell, run "`platform version`" or "`ctd version`":

3.6 Change Brand

- Log in to the Admin shell and type:

```
set_brand <brand>
```

  - If you get a connection error, it means that the Tripwire-platform is down, and you must start it first.
  - You can use `platform pervice start`

3.7 Copy files to your ClarotyOS Server via SFTP

1. Starting from version 1.0.3, ClarotyOS supports connecting via SFTP using the Admin credentials.

2. On Windows platforms, you can use tools such as WinSCP (which by default uses SFTP) to transfer files.
3. On any other platform, you can simply use the SFTP command such as:

```
sftp admin@<clarotyos_ip>
```

4. Although it may seem like you can access any file on ClarotyOS, you are limited to a different root folder. Instead of /, you will see all the files under `/opt/claroty-platform/sftp`. Therefore, if you are using a root shell later on and you are searching for some files that you uploaded, look for them on `/opt/claroty-platform/sftp/home`.

4 System Configuration of ClarotyOS

You can change your system configuration through the TIV UI or through CLI.

4.1 Configuring your System via the TIV UI

In TIV, navigate to the **Configuration > System Management > OS Configuration > Manage** tab as shown below:

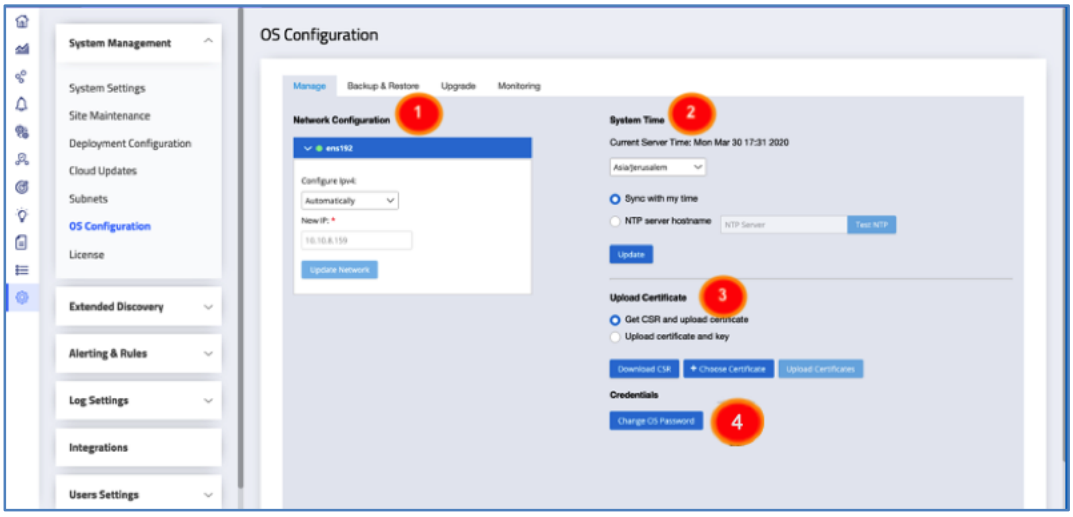


Figure 12 OS Configuration > Manage tab

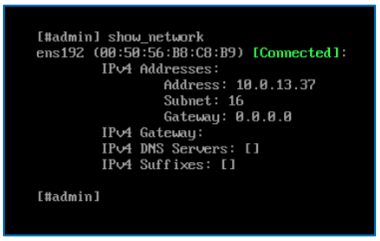
1. To change the network configuration for the desired interface, select a different IPV4 option (automatic is the default) or provide a new IP address, and then click Update Network.
2. To change the Time Configuration:
   - Use the System Time dropdown to change your time zone if needed.
   - You can sync ClarotyOS with your client time (this is the default)
   - You can change your system time to that of the NTP server by changing the NTP server hostname
   - Click **Test NTP** to make sure your ClarotyOS has a connection with this NTP server before continuing.
   - Click **Update**.
3. To upload a Certificate, choose one of the following options:
   - **Option 1:** Download CSR (Certificate Signing Request), sign on the CSR with your CA and choose the certificate. This is the default option.
   - **Option 2**: Choose a certificate file (`cert.pem` / `ssl.crt`) and a key file (`privkey.pem` / `ssl.key`)
   - Click Upload Certificates.
4. To change the OS password, click the **Change OS Password** button.

4.2 Configuring your System via a Console using CLI

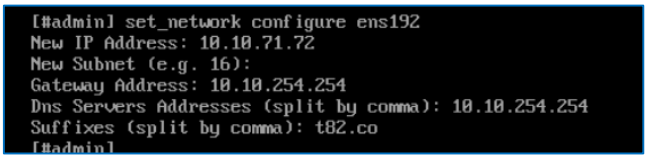
Connect to the Admin's shell.

4.2.1 Network Configuration

1. Use "`show_network`" to see your current configuration:

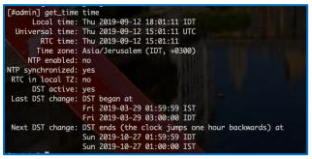


2. Use "`set_network configure <interface>`" to Change IP Address, Subnet, Gateway, DNS, and suffix:



4.2.2 Time Configuration

- Use "`get_time time`" to see current time configuration:



  - Current time, if NTP is enabled & synchronized, and time zone.

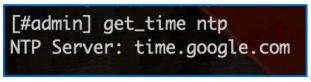
4.2.3 Time Zone Change

1. Use "`get_time timezones`" to see all time zones

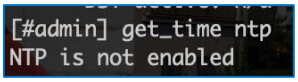
2. "`set_time timezone <Timezone>`"

4.2.4 Set NTP Server

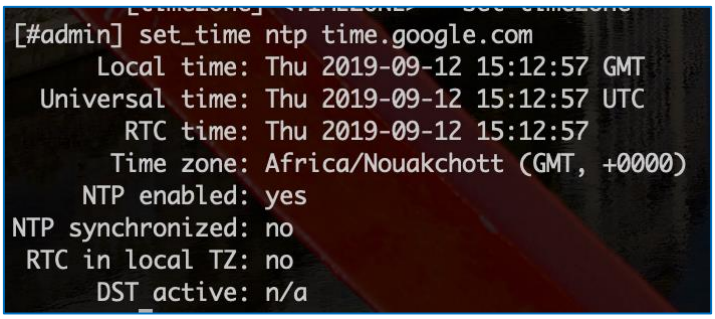
1. Use "`get_time ntp`" to get the current NTP server:



- Will return only if NTP is enabled:

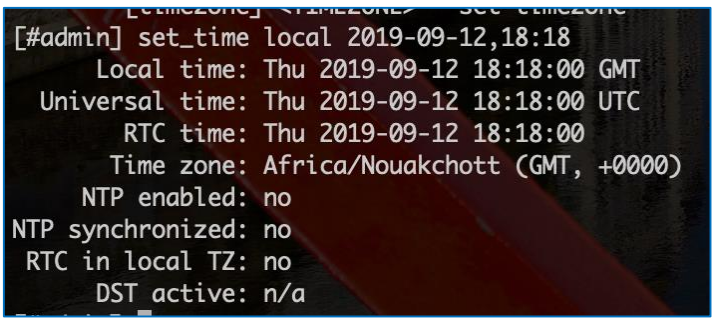


2. "`set_time ntp <NTP server>`"



4.2.5 Change Local Time

- "`set_time local <YYYY-MM-DD,HH:MM>`"



5 Backing up and Restoring

5.1 Backing up

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 as shown below:

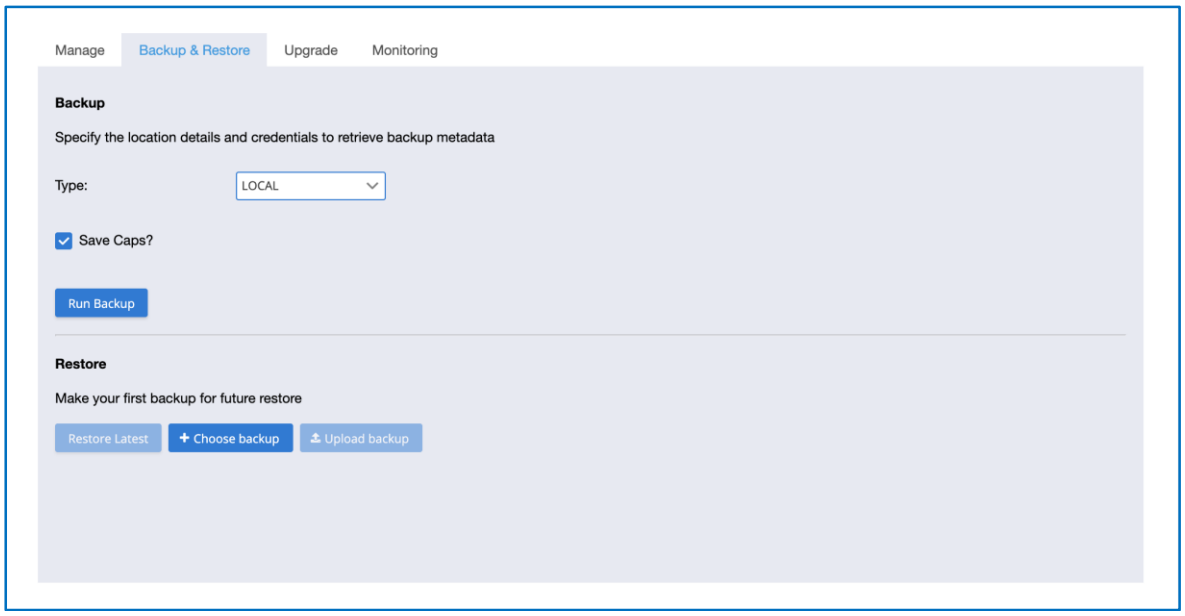


Figure 13 ClarotyOS - Backup & Restore tab

Specify the following fields:

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

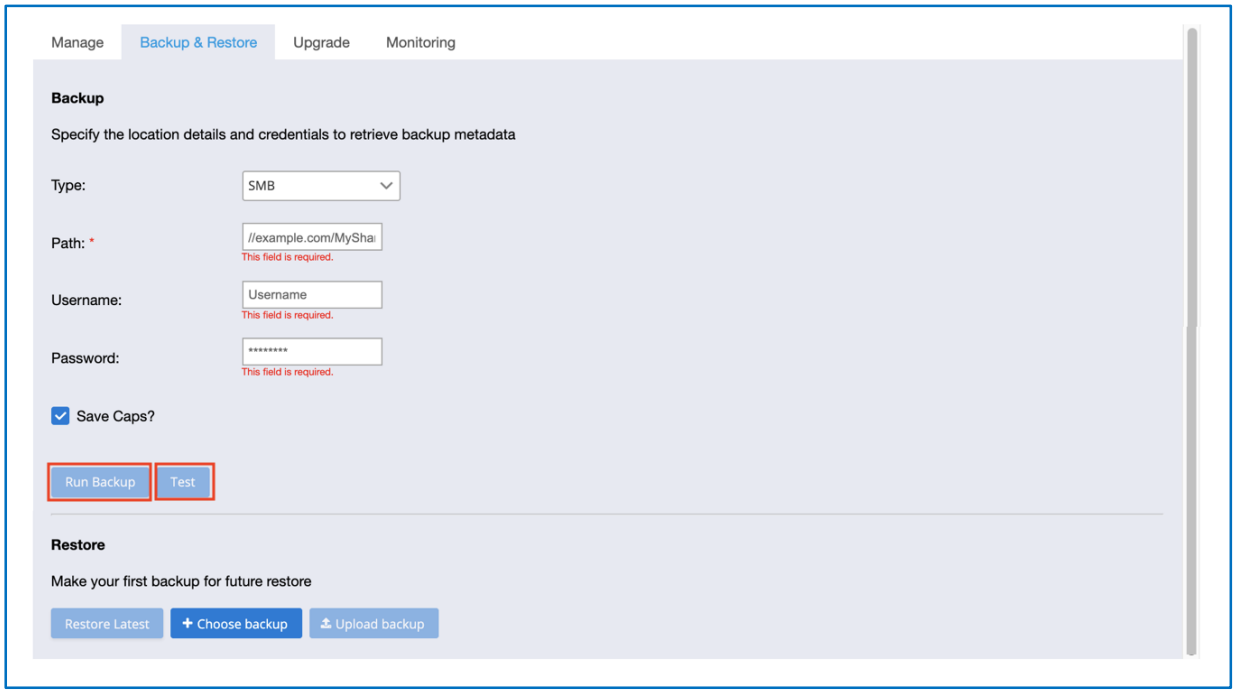


Figure 14 ClarotyOS - Backup and Restore - for Remote Upgrade

- Run **Test** to test your ClarotyOS connection to the SMB
- Click **Run Backup**

5.2 Restore

5.2.1 Restore Latest

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

1. You can see the time of the latest backup under **Restore**
2. Click **Restore Latest**:

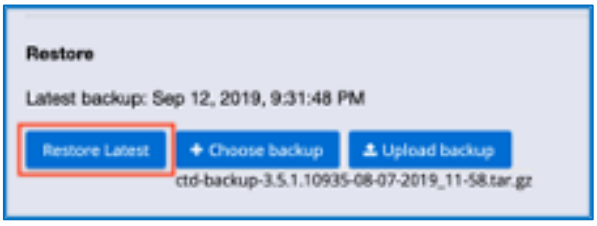


Figure 15 ClarotyOS - Restore Latest

5.2.2 Upload Backup and Restore

1. Under **Restore**, click **Choose Backup**:

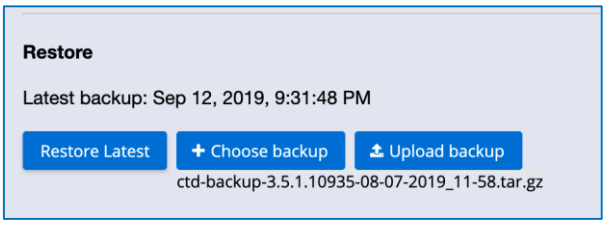


Figure 16 ClarotyOS -Choose Backup

2. Click **Upload Backup**:

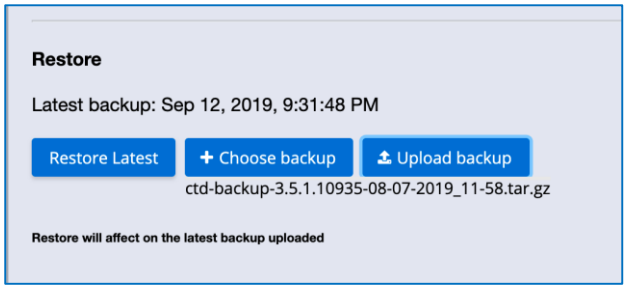


Figure 17 ClarotyOS - Upload Backup

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

6 Upgrading your System

- Navigate to the **Configuration > ClarotyOS > Upgrade** tab:

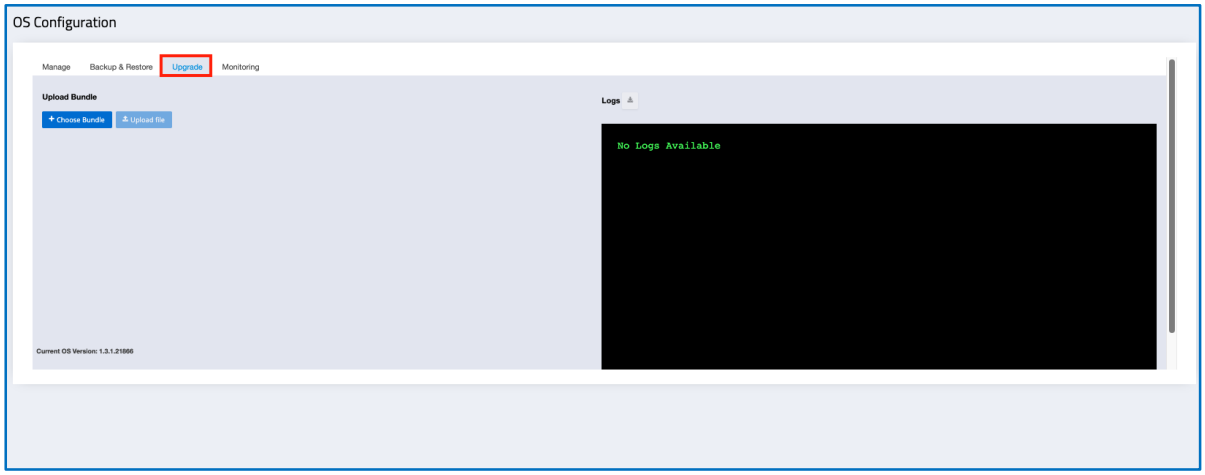


Figure 18 ClarotyOS - Upgrade tab

Upgrade from this screen as follows:

- **Choose Bundle** – Choose a file from TIV
- **Upload File** – Upload to TIV

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

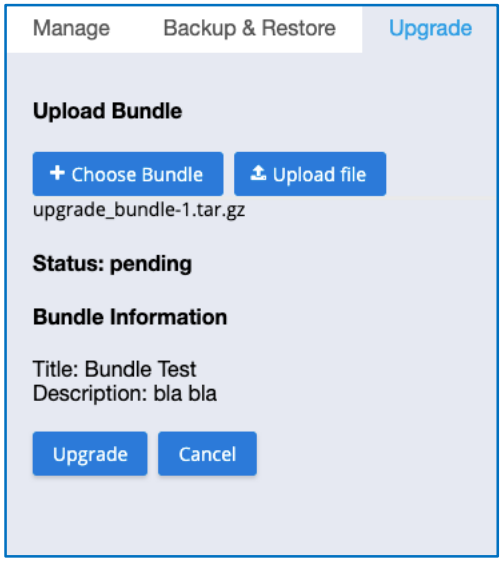


Figure 3 ClarotyOS - Upgrade details

7 ClarotyOS Features

7.1 SNMP Traps

SNMP traps are notifications, initiated by the monitored devices, and sent to one manager or more over the network.

On ClarotyOS, you use an agent of SNMP called net-SNMP and expose the SNMP traps feature as a way to monitor some of the server's components.

You can configure SNMP Traps from the TIV interface or from CLI via the Admin shell.

From the TIV interface

Navigate to **Configuration > System Management > OS Configuration > Monitoring** tab.

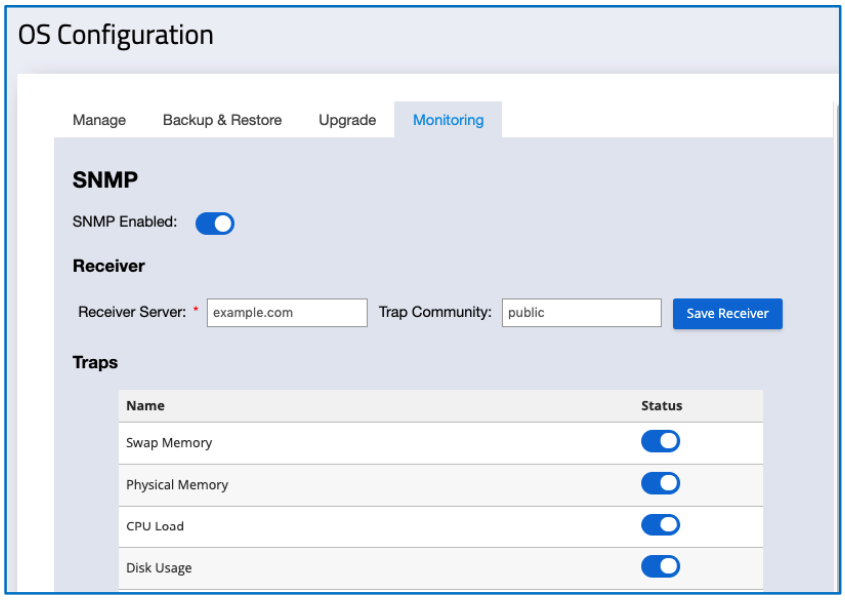


Figure 20 SNMP Traps

From the Admin shell

In order to use this feature, you'll need to do the next steps:

1. Login to the Admin shell via SSH
2. After you login to the system activate the "SNMP" by running the below command:

```
SNMP state enable
```

3. You can make sure SNMP is activated by running:

```
SNMP state status
```

4. You can review the SNMP list by running:

```
SNMP traps list
```

a. swap - alert when there is less then 10% free space

b. memory - alert when there is less then 10% free space

c. cpu_load - alert when the average load for 1 min is on 100% or 5min is on 90% or 15min is on 80%

d. disk - alert when / or any other partition on the server has less then 10% available space

e. ntpd - alert when ntpd process is down

f. sshd - alert when sshd process is down

g. crond - alert when crond process is down

h. zombies - alert when a zombie process spotted

i. network_interfaces - alert when a network_interface has gone up / down or an error spotted

5. You can enable/disable each one of the traps separately

```
SNMP traps enable <name>
SNMP traps disable <name>
```

6. You'll be able to configure SNMP manager (trap receiver), by running the following command:

```
SNMP manager add -h <hostname/ip>
```

7. If you wish to remove or list existing managers, run:

```
SNMP manager remove -h <hostname/ip>
SNMP manager list
```

7.2 SolarWinds Agent

This feature allows you to upload SolarWinds agent using BNI file. Then you will be able to install it and run it on your machine. With this feature you will be able to integrate TIV with your SolarWinds system and manage your machines remotely.

To upload a BNI file:

1. Enter Configuration > OS configuration > Upgrade & Restore.

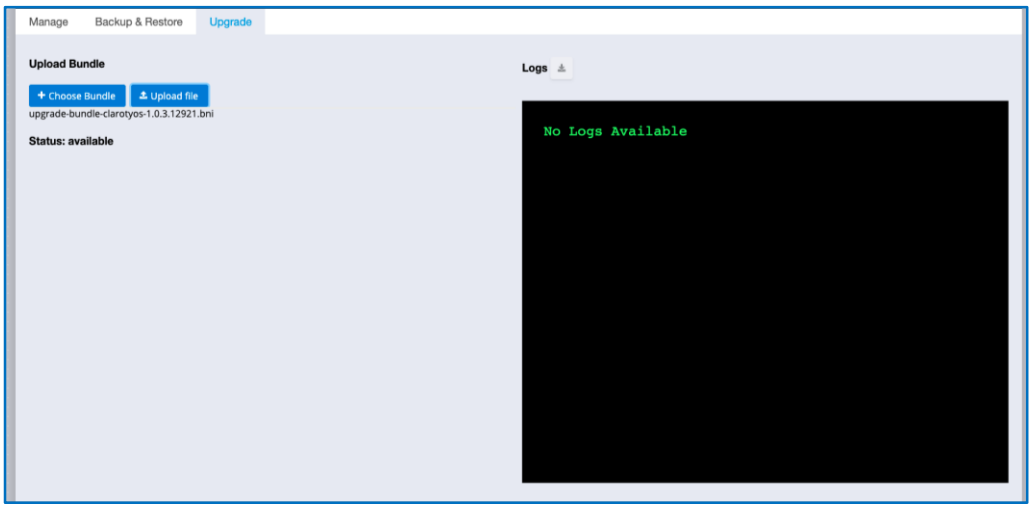
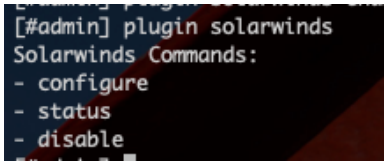


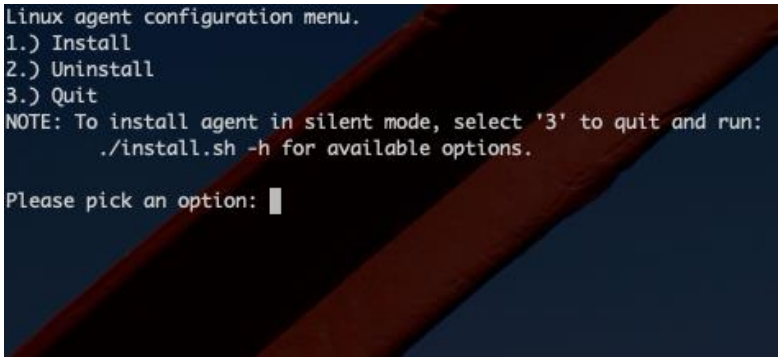
Figure 41 Upgrade & Restore

To use the plugin:

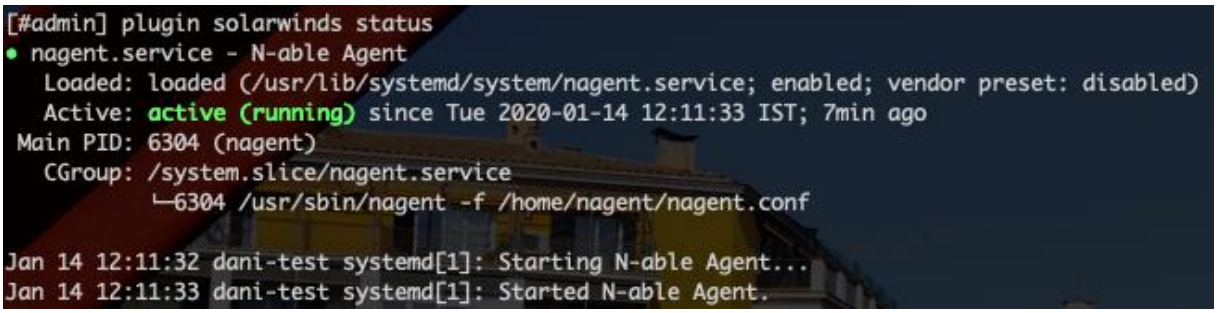
2. After you finish uploading and installing the SolarWinds agent via our UI, login to the admin shell and use the `plugin` command.
3. Get SolarWinds' plugin available commands `plugin solarwinds`.



4. Configure SolarWinds, run SolarWinds' install script `plugin solarwinds configure`



5. Configure SolarWinds' service status (nagent service status) `plugin solarwinds status`



- Disable SolarWinds - stop service and disable shell command `plugin solarwinds disable`
- Enable SolarWinds - start service and enable shell commands `plugin solarwinds enable`

7.3 Open VM-tools

You can open VM-tools in order to allow a quick and easy installation. They are supported by xen, hyperV, and KVM.

7.4 Login page for Tripwire Platform - Sensor UI

As part of Claroty OS, you'll be able to enter directly to Tripwire portal from Sensors, TIV, and EMC.

Only "OS admin" will be able to connect to this screen.

Connect to the following URL.
https://192.168.0.220/osconfiguration

Enter admin password.

You'll be able to view all the OS configuration screens:

- Network Configuration
- Backup & Restore
- Monitor SNMP Traps
- Upgrade

7.5 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.

7.5.1 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:

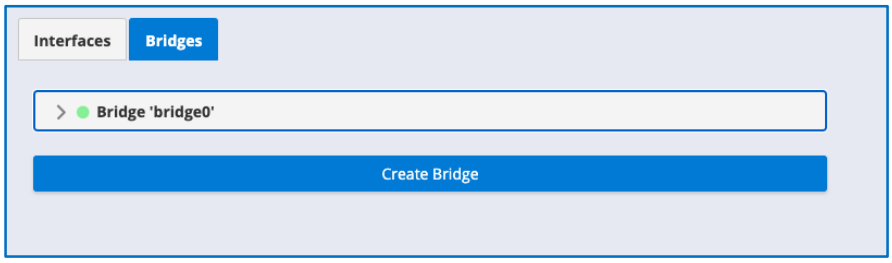


Figure 21: Create Bridge

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:

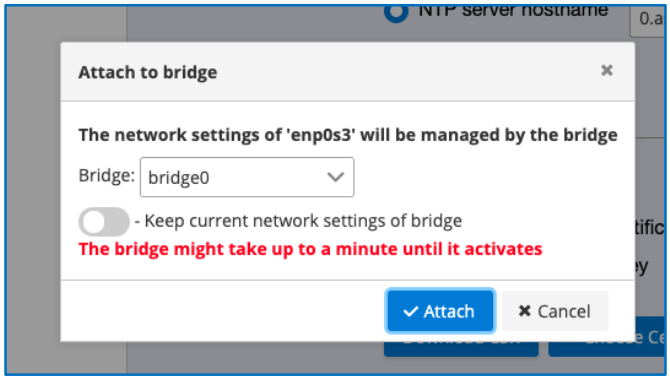


Figure 23: Attach to Bridge

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:

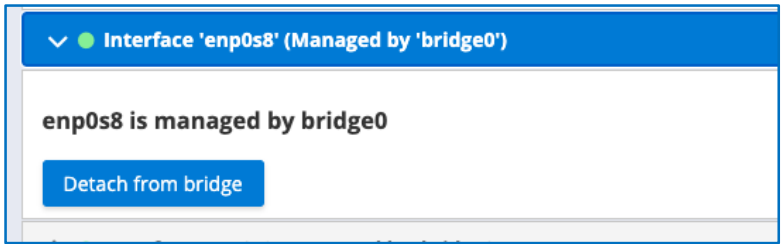


Figure 24: Detach from Bridge

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:

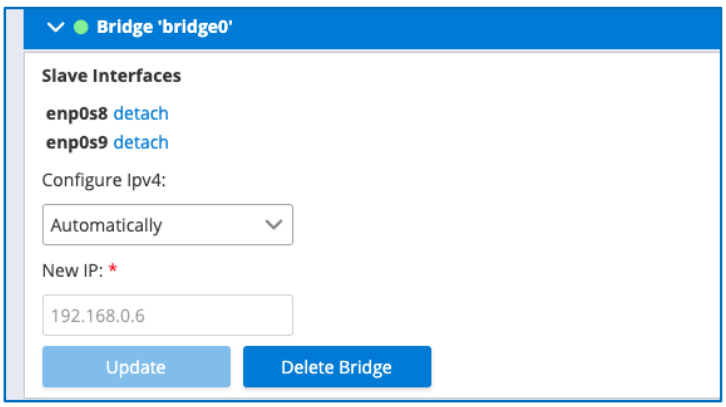


Figure 25: Detach Link

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.

7.6 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.

7.6.1 To Install

1. Go to the **Upgrade** page
2. Upload Tripwire Hardware BNI
3. Run upgrade
4. Reload web page

7.6.2 Web Management

The switches control the LAN Bypass and its Watchdog process:

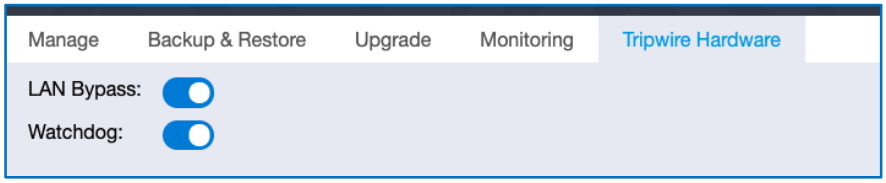


Figure 26: LAN Bypass and Watchdog Process

7.6.3 Shell Commands

```
[admin@localhost]# plugin tripwire_hardware
Tripwire_hardware Commands:
- TIV_BPWD_Control
- disable
```

- Enabling/Disabling the LAN Bypass:

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

- Enabling/Disabling the 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
```

8 Debugging

8.1 Logs

Log in to the ClarotyOS server with an admin user. Get the root shell.

Run the following commands:

Platform Service Logs

```
journalctl -x claroty-platform -f
```

TIV Service Logs

```
journalctl -x icsranger -f
```

Platform Logs

```
tail -f /opt/claroty-platform/workdir/logs
```

TIV Logs

```
tail -f /opt/icsranger/workdir/log
```

8.2 Debugging Screen

The following screen is displayed for debugging of the ClarotyOS procedure:

Figure 27: Debug CLI screen

9 ClarotyOS Support User Access

ClarotyOS has a special user for support purposes, called “support”. It is enabled by default and allows the support team to connect to the machine in case the customer needs help in maintaining its system.

The “support” user is protected with Multi-Factor Authentication, allowing high support capabilities with low risk to the system.

In case a customer is not willing Tripwire to have the ability to use the support user on their system, they may control it using the following admin-shell commands:

```
[admin@localhost]# support --show-access
Support User Access: ON
[admin@localhost]# support --disable-access
[admin@localhost]# support --show-access
Support User Access: OFF
[admin@localhost]# support --enable-access
[admin@localhost]# support --show-access
Support User Access: ON
```

We highly recommend keeping the Support User Access ON, in order to allow our support team to give the best treatment they can.

10 OID Table

The following list describes the OIDs responsible for each Trap Name on the ClarotyOS platform website. See section 10.1 below for the links to download the required MIBs for these traps.

Table 1: OIDs

Trap Name	Table Name	MIB	Type	OID
Swap Memory		UCD-SNMP-MIB	memErrorName.0 = STRING	.1.3.6.1.4.1.2021.4.2
			memSwapErrorMsg.	.1.3.6.1.4.1.2021.4.101
Physical Memory		UCD-SNMP-MIB	memAvailReal.0 = INTEGER	.1.3.6.1.4.1.2021.4.6
			memTotalReal.0 = INTEGER	.1.3.6.1.4.1.2021.4.5
CPU Load	laTable	UCD-SNMP-MIB	laNames.X = STRING	.1.3.6.1.4.1.2021.10.1.2
			laErrMessage.X = STRING	.1.3.6.1.4.1.2021.10.1.101
Disk Usage	dskTable	UCD-SNMP-MIB	dskPath.X = STRING	.1.3.6.1.4.1.2021.9.1.2
			dskErrorMsg.X = STRING	.1.3.6.1.4.1.2021.9.1.101
NTPD Service	prTable	UCD-SNMP-MIB	prNames.X = STRING	.1.3.6.1.4.1.2021.2.1.2
			prErrMessage.X = STRING	.1.3.6.1.4.1.2021.2.1.101
SSHD Service	prTable	UCD-SNMP-MIB	prNames.X = STRING	.1.3.6.1.4.1.2021.2.1.2
			prErrMessage.X = STRING	.1.3.6.1.4.1.2021.2.1.101
CronD Service	prTable	UCD-SNMP-MIB	prNames.X = STRING	.1.3.6.1.4.1.2021.2.1.2
			prErrMessage.X = STRING	.1.3.6.1.4.1.2021.2.1.101
Zombie Processes	hrSWRunTable	HOST-RESOURCES-MIB	hrSWRunName.X = STRING	.1.3.6.1.2.1.25.4.2.1.2
			hrSWRunIndex.X = INTEGER	.1.3.6.1.2.1.25.4.2.1.1
Network Interfaces	ifXTable	IF-MIB	ifName.X = STRING	.1.3.6.1.2.1.31.1.1.1
	ifTable		ifInOctets.X = Counter32	.1.3.6.1.2.1.2.2.1.10

Trap Name	Table Name	MIB	Type	OID
			ifOutOctets.X = Counter32	.1.3.6.1.2.1.2.2.1.16
Kernel Errors	logMatchTable	UCD-SNMP-MIB	logMatchName.X = STRING	.1.3.6.1.4.1.2021.16.2.1.2
Login Failures	logMatchTable	UCD-SNMP-MIB	logMatchName.X = STRING	.1.3.6.1.4.1.2021.16.2.1.2
Boot Errors	logMatchTable	UCD-SNMP-MIB	logMatchName.X = STRING	.1.3.6.1.4.1.2021.16.2.1.2

10.1 MIBs to Download

Use the following links to obtain the MIB files that you will need to upload to the client's monitoring system so it can process the traps in Table 1 above:

- http://www.circitor.fr/Mibs/Mib/U/UCD-SNMP-MIB.mib
- http://www.circitor.fr/Mibs/Mib/H/HOST-RESOURCES-MIB.mib
- http://www.circitor.fr/Mibs/Mib/I/IF-MIB.mib

Use "Save As" to download those files to your computer and then upload them to the client monitoring system.

> Note Some of these files may already be supported by the client