



SUPERVISOR

Profitap Centralized Management

USER MANUAL

Supervisor software version: v0.7.0

If you have any questions, you can contact us through our website:

www.profitap.com

or by email:

support@profitap.com

For the latest documentation and software, visit our Resource Center:

<https://resources.profitap.com/>

TABLE OF CONTENTS

1. Supervisor Overview	4
2. Supervisor Deployment and Update	5
2.1 Profitap Supervisor Installation	5
2.1.1 Prerequisites	5
2.1.2 Installation	5
2.2 Update From a Previous Version of Supervisor	6
2.2.1 Prerequisites	6
2.2.2 Update	6
2.3 Profitap Supervisor Access	7
3. Supervisor Configuration	8
3.1 Login	8
3.2 Device Monitoring	9
3.2.1 Registered Devices	9
3.2.2 Event Monitoring	11
3.3 Traffic Statistics	11
3.4 Traffic Management	11
3.4.1 Port Groups	11
3.4.2 Packet Broker Uplinks	13
3.4.3 External Devices	15
3.4.4 Virtual Stack Broker	16
3.4.5 Rule Sets	17
3.4.6 Traffic Rules	18
3.5 Firmware Update	19
3.6 Authentication	20
3.6.1 Users	20
3.6.2 TACACS+	20
3.6.3 RADIUS	21
3.6.4 Custom Authentication Configuration	21
3.6.5 Centralized Authentication	21
3.7 Administration	22
3.7.1 License Information	22
3.7.2 Configuration Backup and Restore	22
3.7.3 Syslog	22
Legal	23
Disclaimer	23
Copyright	23
Trademarks	23

1. Supervisor Overview

Profitap Supervisor is a centralized management system that allows you to organize and control all XX-Series and X2-Series Network Packet Brokers deployed inside your network architecture. It provides a comprehensive overview of the connected monitoring fabric and brings this together into a single interface. Instead of maintaining each device separately, Supervisor helps orchestrate clusters of devices all at once.

By automating update and maintenance processes, Profitap Supervisor simplifies the workflow of managing your network monitoring infrastructure, saving you valuable time and money.

2. Supervisor Deployment and Update

2.1 Profitap Supervisor Installation

2.1.1 Prerequisites

In order to perform the application deployment, the following elements are necessary:

- *docker* installed and running;
- Profitap Supervisor *docker* image (provided);
- Profitap Supervisor license file (provided).

2.1.2 Installation

The installation can be performed using the following commands in order:

1. Create a directory to be used to store the supervisor configuration and license:

```
mkdir -p /home/user/supervisor-data/
```

This is only a reference path used for this documentation. If a different path is used, edit the following commands accordingly.

2. Copy the provided license file in the data directory:

```
cp SFM-010010-10.lic /home/user/supervisor-data/license.lic
```

Replace the name of the file in this command with the actual license file provided.

3. Load the provided *docker* container (replace 'X.Y.Z' with the appropriate version number):

```
docker load -i profitap-supervisor-vX.Y.Z.tar
```

4. Run the *docker* container, specifying the correct data directory (replace 'X.Y.Z' with the appropriate version number):

```
docker run -v /home/user/supervisor-data:/data:Z --network host --rm --name supervisor -d profitap-supervisor:vX.Y.Z
```

At this point, the Supervisor application should be running. If you wish to verify that deployment has proceeded correctly, you can check the running containers using the following command:

```
docker ps
```

The Profitap Supervisor container should appear.

2.2 Update From a Previous Version of Supervisor

When using the Supervisor *docker* container, the update process simply consists of shutting down the currently-running *docker* container, and starting the new updated *docker* container using the same data folder. The new instance will perform all of the necessary data migration. It is good practice to perform a backup of the Supervisor configuration before proceeding with the update (see [Configuration Backup and Restore](#)).

2.2.1 Prerequisites

In order to perform the update, the following elements are necessary:

- Currently installed Supervisor *docker* container;
- Data folder (we are using `/home/user/supervisor-data` for this example);
- Supervisor license file.

2.2.2 Update

The steps for updating Supervisor are as follows:

1. (Optional) Backup the current Supervisor configuration (see [Configuration Backup and Restore](#)).
2. Load the new *docker* container in your local registry (replace 'X.Y.Z' with the appropriate version number):

```
docker load -i profitap-supervisor-vX.Y.Z.tar
```

3. Stop previous instance using the following command:

```
docker stop supervisor
```

4. Start a new *docker* container instance (replace 'X.Y.Z' with the appropriate version number):

```
docker run -v /home/user/supervisor-data:/data:Z --network host --rm --name supervisor -d profitap-supervisor:vX.Y.Z
```

2.3 Profitap Supervisor Access

When deployed, Supervisor is accessible through the following ports:

- **443**: HTTPS GUI and API access;
- **80**: HTTP redirection to HTTPS GUI;
- **8080**: HTTP API access (docker container only).

The first access is possible using the following default credentials:

- **username**: admin
- **password**: admin

It is strongly advised to change these credentials on first access.

3. Supervisor Configuration

3.1 Login

Open a web browser and enter the Supervisor address in the address bar:

https://<ip_addr>

<ip_addr> being the IP address of the machine running the docker container.

Login, using the appropriate account credentials.

The initial credentials are as follows:

Default username: admin

Default password: admin

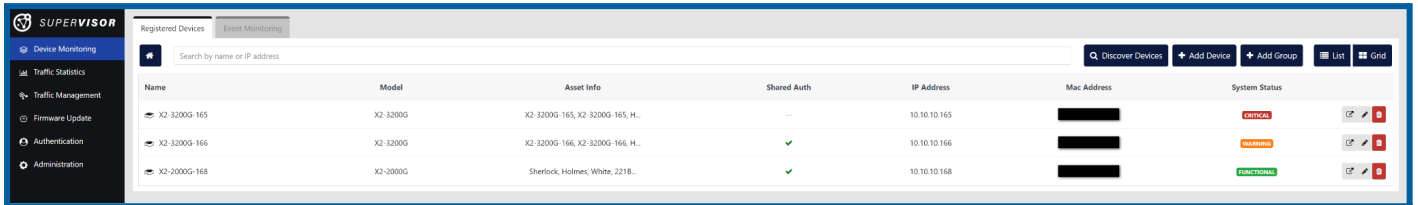
Note: It is strongly recommended to change the default administrator password when first accessing Supervisor.

To change the default password, click the *Default Admin* link at the bottom left of the screen and enter a new password in the *Edit User* window.

3.2 Device Monitoring

3.2.1 Registered Devices

The **Registered Devices** tab of the **Device Monitoring** page provides an overview of the devices managed by the Supervisor, and general information about them, such as their name, model, asset information, shared authentication status, IP address, MAC address, and system status.

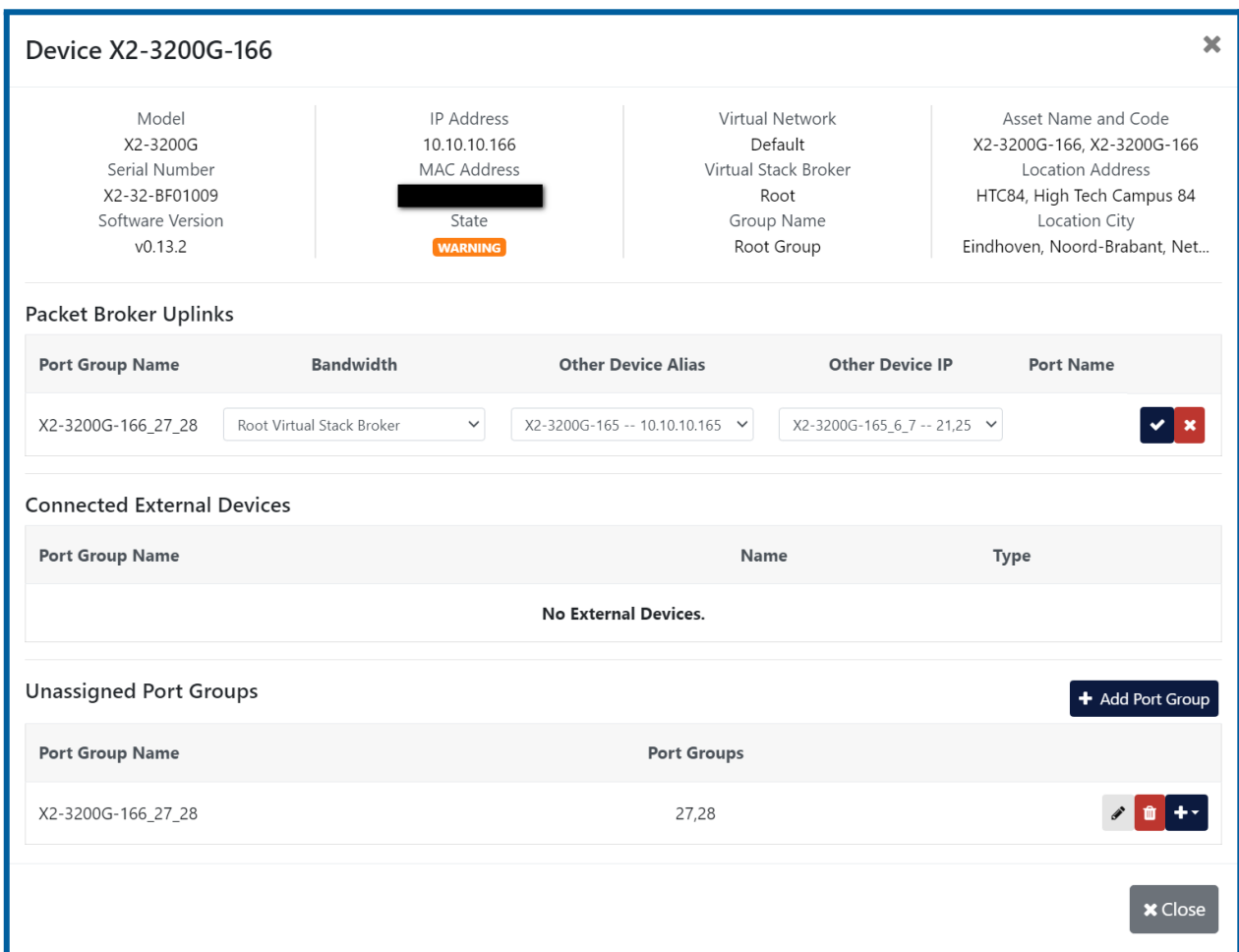


Name	Model	Asset Info	Shared Auth	IP Address	Mac Address	System Status	
X2-3200G-165	X2-3200G	X2-3200G-165, X2-3200G-165, H...	---	10.10.10.165	[REDACTED]	CRITICAL	[Edit] [Delete]
X2-3200G-166	X2-3200G	X2-3200G-166, X2-3200G-166, H...	✓	10.10.10.166	[REDACTED]	WARNING	[Edit] [Delete]
X2-2000G-168	X2-2000G	Sherlock, Holmes, White, 221B...	✓	10.10.10.168	[REDACTED]	FUNCTIONAL	[Edit] [Delete]

List of registered devices

The view can be changed by clicking either *List* or *Grid* in the top right corner of the interface. The search bar (case-sensitive) can be used to filter the current view to display specific devices or groups.

Clicking on a device provides additional information about this device, and the ability to prepare port groups, packet broker uplinks and external devices prior to [Traffic Management](#).



Device X2-3200G-166

Model X2-3200G Serial Number X2-32-BF01009 Software Version v0.13.2	IP Address 10.10.10.166 MAC Address [REDACTED] State WARNING	Virtual Network Default Virtual Stack Broker Root Group Name Root Group	Asset Name and Code X2-3200G-166, X2-3200G-166 Location Address HTC84, High Tech Campus 84 Location City Eindhoven, Noord-Brabant, Net...
------------------------------------------------------------------------------------	------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------

Packet Broker Uplinks

Port Group Name	Bandwidth	Other Device Alias	Other Device IP	Port Name
X2-3200G-166_27_28	Root Virtual Stack Broker	X2-3200G-165 -- 10.10.10.165	X2-3200G-165_6_7 -- 21,25	[Check] [X]

Connected External Devices

Port Group Name	Name	Type
No External Devices.		

Unassigned Port Groups

Port Group Name	Port Groups	
X2-3200G-166_27_28	27,28	[Edit] [Delete] [Add]

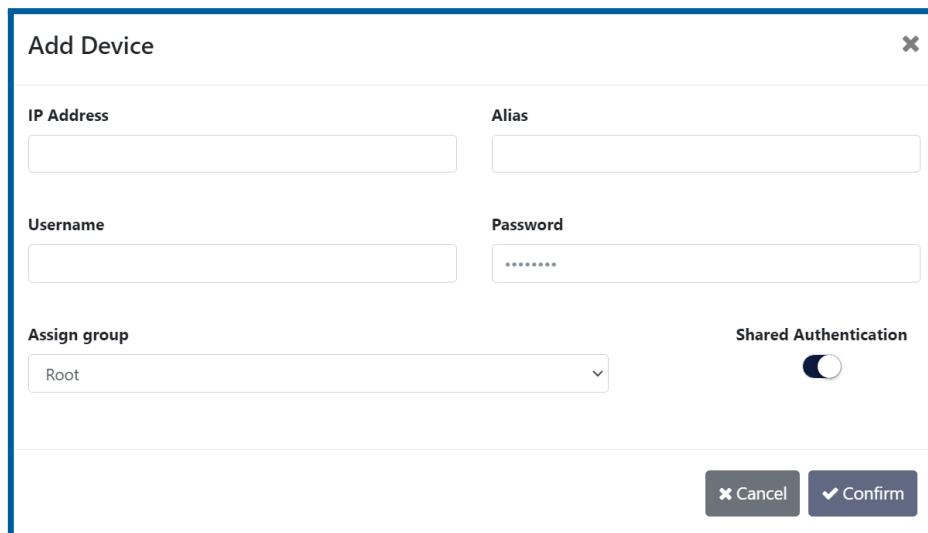
[Close]

Device Details window

Clicking on a group navigates to this group, listing the devices it contains. Clicking the *Home* button navigates back to the root. Clicking the *Manage* button of a device opens this device's XX-Manager or X2-Manager GUI in a new tab.

From this dashboard, devices and groups can be added, modified, or removed.


To add a new device, click the *Add Device* button in the top right corner of the interface, and enter the device's information in the *Add Device* window. Select a group in this window to add the device to this group. Enable *Shared Authentication* to enable Supervisor's centralized authentication function on this device (see [Centralized Authentication](#)). The device's information and the group to which it belongs can be changed at a later time by clicking the device's *Edit* button.



Add Device window

You can also add new devices via the *Discover Devices* button. The *Discover Devices* window lists devices found on the Supervisor's local network, and allows you to add them to the Supervisor.

To create a group, click the *Add Group* button, and enter the group name and description in the *Add Group* window. The group's name and description can be changed at a later time by clicking the group's *Edit* button.



Add Group window

To remove a device or group, click its *Delete* button. If a group contains one or more devices, you will be asked whether these devices should be moved to another group, or removed along with the group.

3.2.2 Event Monitoring

The **Event Monitoring** tab of the **Device Monitoring** page displays all of the events detected by the Supervisor. The events can be filtered using the *Open* button and selecting the filtering options. It is also possible to navigate to the device and rule set involved in the event by clicking the event description.

3.3 Traffic Statistics

The **Traffic Statistics** page provides an overview of the traffic statistics of the devices managed by the Supervisor.

The view can be changed by clicking either *List* or *Grid* in the top right corner of the interface. The search bar (case-sensitive) can be used to filter the current view to display specific devices or groups.

Clicking on a device adds it to, or removes it from, the statistics view in the bottom half of the page. Clicking on a group navigates to this group, listing the devices it contains, and allowing these devices to be added to, or removed from, the statistics view. Clicking the *Home* button navigates back to the root. Right-clicking a group allows a statistics column for this group to be added to, or removed from, the statistics view. Statistics columns can also be removed from the statistics view by clicking the *Clear statistics* button next to the column's name.

3.4 Traffic Management

The **Traffic Management** page allows users to define traffic rules operating on an interconnected fleet of Profitap XX-Series and X2-Series packet brokers. The traffic rules can be used to forward, aggregate and replicate traffic from different devices. Profitap Supervisor will automatically generate and deploy the necessary device configuration to achieve the desired result.

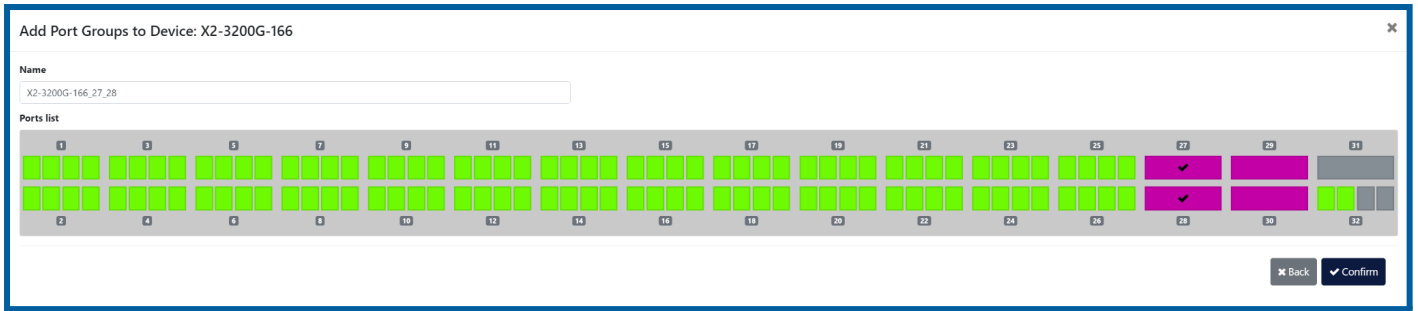
Port groups, packet broker uplinks and external devices can be prepared from the **Device Monitoring > Registered Devices** page prior to creating traffic rules.

The **Help** window (accessed from the sidebar) can assist you in setting up the different traffic management components.

3.4.1 Port Groups

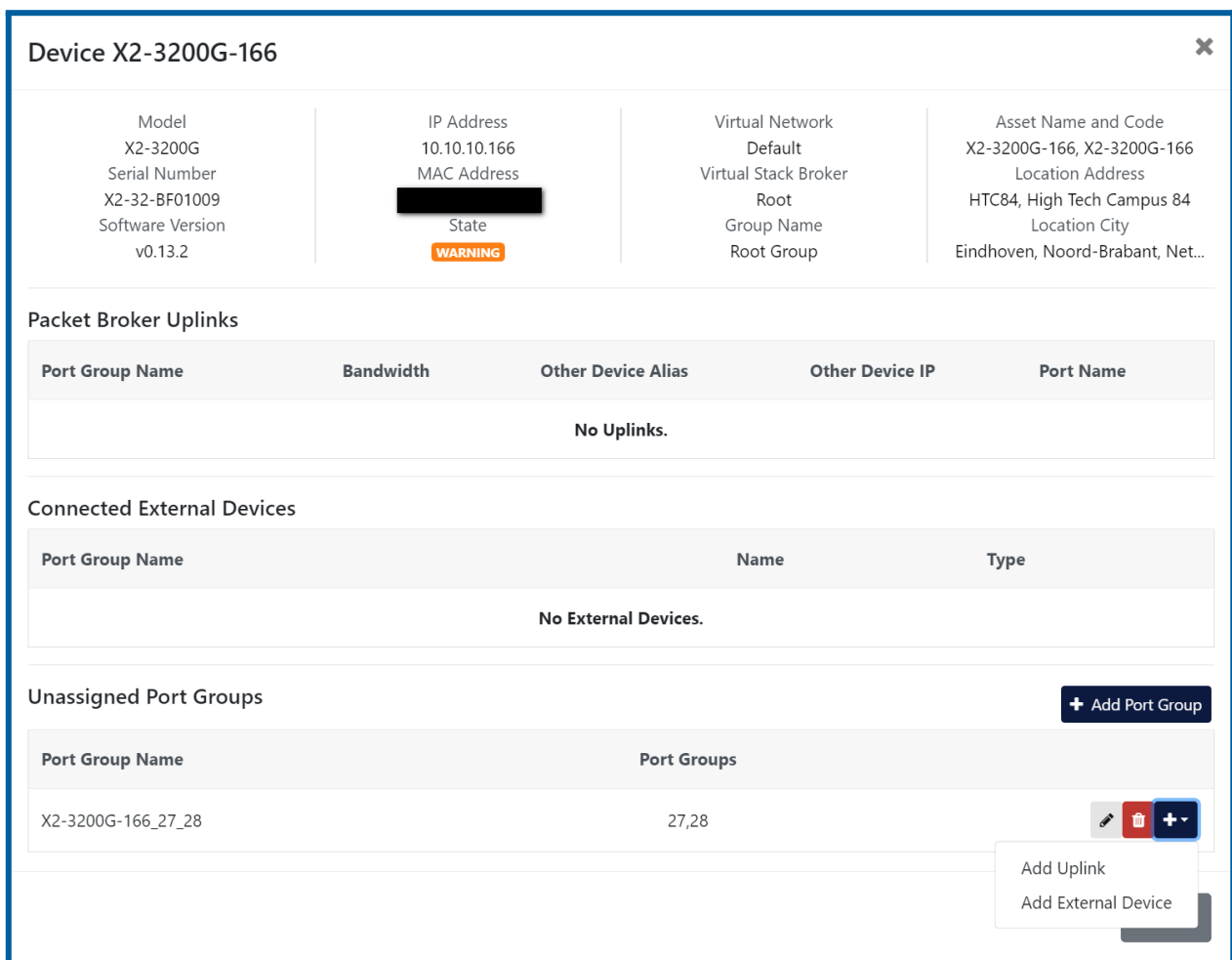
Profitap XX-Series and X2-Series packet brokers interfaces can be organized in port groups in order to be used together. A port group is used to aggregate incoming traffic and/or to distribute (load balance) the outgoing packets. Note that each physical port can only be used within a single port group.

To create a port group, navigate to the **Device Monitoring > Registered Devices** page, click the device for which to create a port group to open its device details window, and click the *Add Port Group* button to open the *Add Port Groups* window. In this window, give a name to the port group, select one or more ports, and click the *Confirm* button.



Add Port Group window

Port groups that are not currently used in a packet broker uplink or connected to an external device are listed in the *Unassigned Port Groups* section of the device details window. From this listing, port groups can be edited or deleted, or they can be added to a packet broker uplink or connected to an external device.



Device Details window showing the newly created port group

3.4.2 Packet Broker Uplinks

Profitap Supervisor can help you monitor and control how the packet brokers hierarchy is interconnected. The physical connections between the packet brokers are called **uplink**, and are used to distribute the traffic across the XX-Series or X2-Series fleet.

To add an uplink, navigate to the **Device Monitoring > Registered Devices** page, click one of the devices for which to create an uplink to open its device details window, click the **[+]** button next to an unassigned port group and select **Add Uplink**.

Device X2-3200G-166

Model X2-3200G Serial Number X2-32-BF01009 Software Version v0.13.2	IP Address 10.10.10.166 MAC Address [REDACTED] State WARNING	Virtual Network Default Virtual Stack Broker Root Group Name Root Group	Asset Name and Code X2-3200G-166, X2-3200G-166 Location Address HTC84, High Tech Campus 84 Location City Eindhoven, Noord-Brabant, Net..
------------------------------------------------------------------------------------	------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------

Packet Broker Uplinks

Port Group Name	Bandwidth	Other Device Alias	Other Device IP	Port Name
No Uplinks.				

Connected External Devices

Port Group Name	Name	Type
No External Devices.		

Unassigned Port Groups + Add Port Group

Port Group Name	Port Groups	
X2-3200G-166_27_28	27,28	[Edit] [Delete] [Add]

Dropdown menu options:
Add Uplink
Add External Device

Click the **[+]** button next to an unassigned port group and select **Add Uplink** to create an uplink using this port group

Select the Virtual Stack Broker, and the packet broker device and port group to which to connect the uplink, then click the confirm button.

Device X2-3200G-166 ✕

Model X2-3200G Serial Number X2-32-BF01009 Software Version v0.13.2	IP Address 10.10.10.166 MAC Address [REDACTED] State WARNING	Virtual Network Default Virtual Stack Broker Root Group Name Root Group	Asset Name and Code X2-3200G-166, X2-3200G-166 Location Address HTC84, High Tech Campus 84 Location City Eindhoven, Noord-Brabant, Net...
------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------

Packet Broker Uplinks

Port Group Name	Bandwidth	Other Device Alias	Other Device IP	Port Name
X2-3200G-166_27_28	Root Virtual Stack Broker	X2-3200G-165 -- 10.10.10.165	X2-3200G-165_6_7 -- 21,25	✓ ✕

Connected External Devices

Port Group Name	Name	Type
No External Devices.		

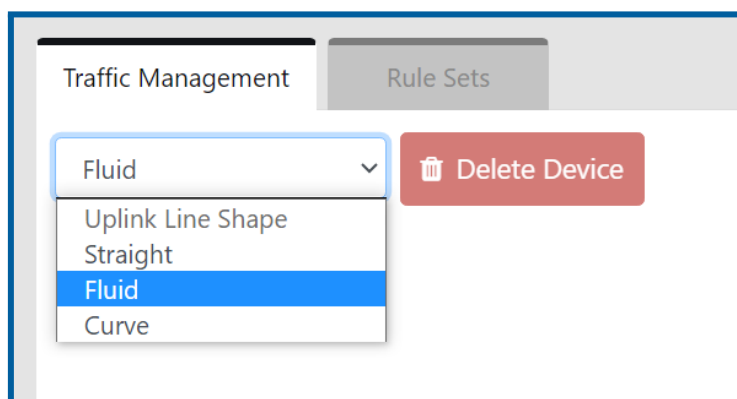
Unassigned Port Groups + Add Port Group

Port Group Name	Port Groups	
X2-3200G-166_27_28	27,28	✎ ✕ +

✕ Close

Uplinks are created between port groups of separate devices, and thus an unassigned port group must exist on each of the devices you wish to link.

Once an uplink has been created, both devices will appear in the graphical view on the **Traffic Management** page. They can be arranged by clicking and dragging them, and the uplink line shape can be changed via the *Uplink Line Shape* drop-down menu at the top left of the page.



Uplink Line Shape drop-down menu

Clicking on a device in the graphical view opens its *Device Details* window.

Right-clicking a device in the graphical view provides the option to open the *Device Details* window, create an uplink, or add an external device.



Packet broker device options menu

3.4.3 External Devices

Since Profitap packet brokers are likely not the only components of your visibility infrastructure, Profitap Supervisor allows you to map external devices connected to your XX-Series and X2-Series devices in the visibility network topology. These can be used as source or destination for your traffic rules.

To add an external device, navigate to the **Device Monitoring > Registered Devices** page, click one of the devices to which to connect an external device to open its device details window, click the **[+]** button next to an unassigned port group and select *Add External Device*. Give the external device a name and select its type, then click the confirm button.

Device X2-3200G-166
✕

Model
X2-3200G

Serial Number
X2-32-BF01009

Software Version
v0.13.2

IP Address
10.10.10.166

MAC Address
[REDACTED]

State
WARNING

Virtual Network
Default

Virtual Stack Broker
Root

Group Name
Root Group

Asset Name and Code
X2-3200G-166, X2-3200G-166

Location Address
HTC84, High Tech Campus 84

Location City
Eindhoven, Noord-Brabant, Net...

Packet Broker Uplinks

Port Group Name	Bandwidth	Other Device Alias	Other Device IP	Port Name
No Uplinks.				

Connected External Devices

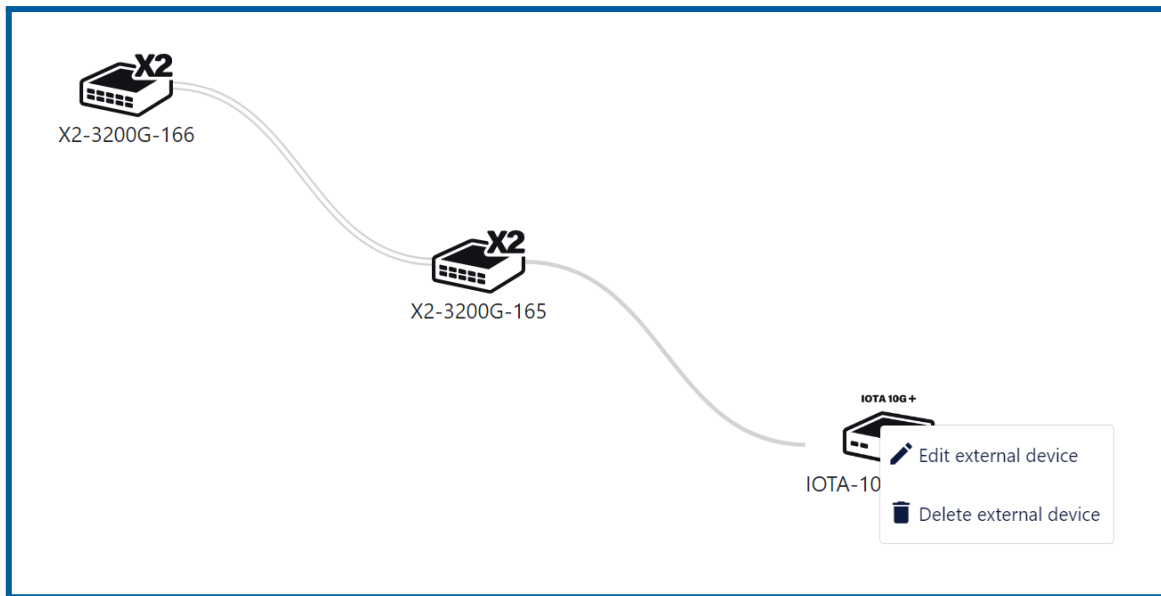
Port Group Name	Name	Other Device Alias	Type
X2-3200G-166_27_28	<input type="text" value="IOTA-10G-PLUS-1"/>	<input type="text" value="IOTA_10G_PLUS"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>

Unassigned Port Groups + Add Port Group

Port Group Name	Port Groups	
X2-3200G-166_27_28	27,28	<input type="text"/> <input type="checkbox"/> <input checked="" type="checkbox"/>

✕ Close

External devices can also be added by right-clicking a device in the graphical view and selecting *Add external device*. Clicking an external device in the graphical view will open the *Edit external device* window, and right-clicking it provides the option to edit or delete it.



3.4.4 Virtual Stack Broker

As your NPB hierarchy grows, it will be helpful to group your devices in order to reduce your topology complexity. Profitap Supervisor allows you to create Virtual Stack Brokers to organize multiple packet brokers together, linked with each other. This new entity can be used as a logical device, which can be connected to external devices or other uplinks. Note that VSBs are empty at their creation. To use them, you will need to define an uplink between a device already existing in your topology and a new one to add to the empty VSB.

To create a VSB, click the *Add Virtual Stack Broker* button, name it, and click *Confirm*.







Devices can now be added to the VSB by selecting it in the *Add Uplink* window (see [3.4.2](#)).

The screenshot shows the 'Add Uplink' dialog box. It has a title bar 'Add Uplink' with a close button. The dialog is divided into two sections: 'First Port Group' and 'Second Port Group'. Each section contains three dropdown menus. The 'First Port Group' dropdowns are: 'Root Virtual Stack Broker', '2000G-1', and '2000G-1_39_40_41_42 -- 39,40,41,42'. The 'Second Port Group' dropdowns are: 'VSB1', '720G-1', and '720G-1_9 -- [9]nine'. At the bottom right, there are 'Confirm' and 'Cancel' buttons.

3.4.5 Rule Sets

Profitap Supervisor uses the registered topology of Devices, External Devices and VSBs to allow you to perform advanced cross-device traffic management. The configuration of all these elements is covered by the Supervisor Rule Sets. These are traffic management profiles that can be created, cloned, swapped and modified. Any time a new Rule Set is applied, the Supervisor system will make sure that the configuration is automatically deployed on the targeted devices.

The **Rule Sets** tab displays the list of existing sets of rules, allowing users to:

-  Create a rule set
-  Clone a rule set
-  Configure a rule set
-  Apply a rule set
-  Rename a rule set
-  Delete a rule set

Multiple Rule Sets can be deleted by selecting one or more Rule Sets and pressing the *Delete Rule Sets* button.

Note: In order to apply changes to the active rule set, it is necessary to apply the rule set again.

If a Rule Set is currently active, it is displayed at the bottom of the **Traffic Management** tab. It can be deactivated via the *Deactivate Rule Set* button.

3.4.6 Traffic Rules

Traffic Rules are at the core definition of the Supervisor traffic management. Each rule allows the definition of the source and destination of the network traffic. The Rules can cover devices distributed across different Virtual Stack Brokers, and will use the physical Uplinks to make sure that the packets reach the intended target.

The first step in creating a rule is defining the traffic sources. Add one or more sources by clicking the *Add* button, selecting either *Add Port Group Source* or *Add External Device Source*, selecting the port group or external device you wish to add, and clicking the *checkmark* button. Click the *Next* button, and repeat the process for traffic destinations. Click *Next* for an overview of the rule, then click *Confirm*.

Add Rule ✕

Traffic Sources Traffic Destinations Filters Rule Overview

Rule name

Source Devices and Port Groups + Add

External Device	Virtual Stack Broker	Device	Port Group	
--	<input type="text" value="Root Virtual Stack Broker"/>	<input type="text" value="X2-3200G-166 -- 10.10.10.166"/>	<input type="text" value="X2-3200G-166_29 -- 29"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>

Next ✕ Cancel ✓ Confirm

3.5 Firmware Update

The **Firmware Update** page allows firmware updates to be pushed to multiple devices at once.

Select the devices you would like to update from the list. The list can be filtered by device family, and by group. To filter by device family, use the *Device family* drop-down menu at the top left of the page. To filter by group, click the *filter by group* button next to the name of the group on the right-hand side of the list. To remove the group filter, click the *clear group filter* button at the top right of the list. To select or unselect all devices in the current view, click the checkbox at the top left of the list.

After having selected the appropriate devices, click the *Firmware update* button to select the firmware file. After confirming the update, the file will be uploaded to the Supervisor, after which the Supervisor will push the update to each of the selected devices. The update status can be followed on this page. Note that the current batch must be completed before a new batch can be started. Also note that, if attempting to update an XX-Series device using an X2-Series firmware file (or vice versa), the update will fail for that particular device.

3.6 Authentication

3.6.1 Users

The **Users** tab allows users logged in as administrators to add new users or edit existing users and their privilege levels. Depending on the selected role, the user has the following rights:

- **administrator**: full control, limitless administration and system update;
- **user**: create and set rules, aggregate and filter traffic, and port configuration;
- **viewer**: view only: settings, statistics, active rules.

The minimum requirements for the passwords are as follows:

- 8 characters;
- one letter uppercase;
- one letter lowercase;
- one digit.

The *Allow External Authentication* option allows the user's credentials to be used to log into devices on which *Shared Authentication* was enabled (see [Centralized Authentication](#)).

3.6.2 TACACS+



The **TACACS+** tab allows adding one or more TACACS+ servers, and configuring the following details:

- priority (sets the order in which the servers will be taken into account, if more are added, with a lower number corresponding to a higher priority);
- login type (chap, login, pap);
- server hostname;
- port;
- secret key;
- timeout (waiting time for response from the TACACS+ server, can be set between 1 and 15 seconds);
- privilege mapping (translates the 15 privilege levels from TACACS+ into those of the viewers, users and admins; can be configured).

The *Allow External Authentication* option allows the user credentials defined on the TACACS+ server to be used to log into devices on which *Shared Authentication* was enabled (see [Centralized Authentication](#)).

3.6.3 RADIUS

The **RADIUS** tab allows adding one or more RADIUS servers, and configuring the following details:

- priority (sets the order in which the servers will be taken into account, if more are added, with a lower number corresponding to a higher priority);
 - server hostname;
 - port;
 - secret key;
 - timeout (waiting time for response from the RADIUS server, can be set between 1 and 15 seconds);
 - privilege level mappings (allows adding one or more rules for users. These rules are integer or string **type** attributes, requiring a **name** and a **value**. During authentication, the system checks if a user matches the rules. If there is a match between a user and a rule, then a **role** is applied for the user);
- Note:** To add a new rule, click the  button. To apply the rule, click the  button.
- fallback role (comes into place when there isn't a match between a user and a rule, with the 'none' option denying authentication access to *any* user).

The *Allow External Authentication* option allows the user credentials defined on the RADIUS server to be used to log into devices on which *Shared Authentication* was enabled (see [Centralized Authentication](#)).

3.6.4 Custom Authentication Configuration

Supervisor allows users to not only define multiple authentication methods, but also to configure how the different methods are used by the system. Clicking the *Configure Authentication* button on either the *Users*, *TACACS+*, or *RADIUS* page allows users to see the list of available authentication methods and change their priority and activation strategy.

For each method, one of the following strategies can be selected:

- **Enable:** The method is activated and will be used to authenticate users;
- **Disable:** The method is not active and its configuration will be ignored;
- **Restrict:** A restricted authentication method is activated only if all higher priority methods are failing access. In the case of RADIUS or TACACS+ methods, this means that no server is responding (or no server is programmed). If only one of the registered RADIUS/TACACS+ servers replies with a rejection, the following restricted methods will be skipped. Note that "Local Users" are always available, meaning that any "restrict" method after that will never be activated.

3.6.5 Centralized Authentication

Supervisor provides the ability to use credentials defined in the Supervisor itself in order to log into devices it manages. Devices on which *Shared Authentication* was enabled (see [3.2.1](#)) will be able to use Supervisor credentials, be they Local Users, or users defined on TACACS+ or RADIUS servers, on which *Allow External Authentication* was enabled. The Centralized Authentication follows the Supervisor's [Custom Authentication Configuration](#).

3.7 Administration

3.7.1 License Information

The **License information** section of the **Setup** tab displays information about the current Supervisor license, including the maintenance period and the maximum number of devices that can be controlled.

3.7.2 Configuration Backup and Restore

The **Configuration Backup and Restore** section of the **Setup** tab allows the exporting and importing of the Supervisor instance configuration. The data can be exported by inserting a passphrase, selecting the parts to be exported, and pressing the *Export* button. The system will generate an encrypted archive that can be safely stored as backup. This package can be imported back to the Supervisor instance via a similar process: insert the passphrase, select the parts of the configuration you wish to import, press the *Import* button, and select the archived configuration file.

Note: The same passphrase as the one used for exporting the configuration file is required for importing it.

Note: The export functionality will not backup the Supervisor license.

3.7.3 Syslog

The **Syslog** tab displays the logs of the Supervisor system. On this page, the system logs can be refreshed, downloaded, or reset.

Legal

Disclaimer

The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranty of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes in the content thereof without obligation of the manufacturer to notify any person of such revision or changes.

Copyright

This publication, including all photographs and illustrations, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Trademarks

The trademarks mentioned in this manual are the sole property of their owners.

Profitap HQ B.V.
High Tech Campus 84
5656 AG Eindhoven
The Netherlands
sales@profitap.com
www.profitap.com

© 2023 Profitap — v1.8