Outpost24

Vulnerability Management made easy

HIAB Server Settings

Version: 2.4

2018-11-21

Table of Contents

About This Document

This document provides users with a comprehensive overview of the server settings for HIAB. This document has been elaborated under the assumption the reader has access to the HIAB Account and Graphical User Interface.

For support information, visit https://www.outpost24.com/support.

Copyright

Trademark

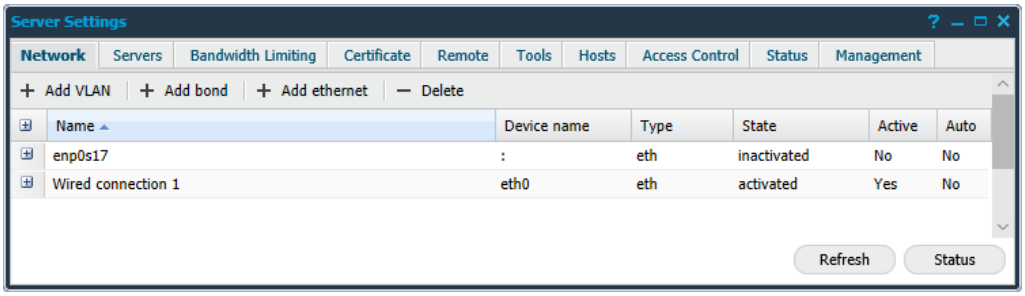
1 Server Settings

The HIAB comes with a variety of settings which are available under **Main Menu → Settings → Server**. In *Server Settings* it is possible to change:

- Network specific settings
- Information of different servers
- Connections to a LDAP/AD server

1.1 Network Tab

In the **Network** tab, the network specific settings for the HIAB can be changed.



Right clicking a network interface will presents the following options:

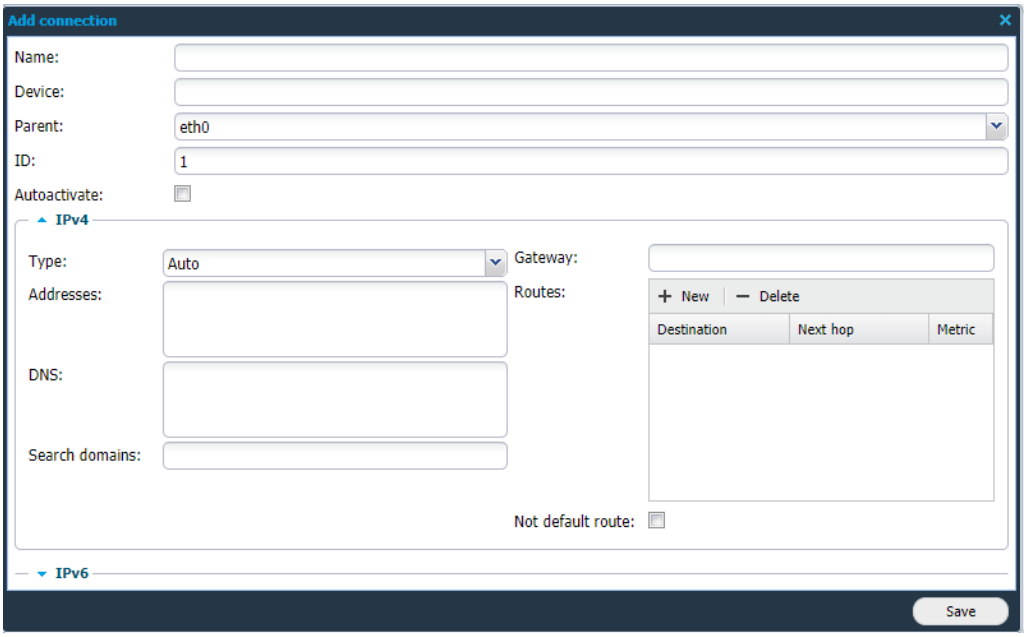
- Activate/Deactivate
- Add VLAN
- Add bond
- Add Ethernet
- Delete
- Edit

Activate/Deactivate

Right click a network device to **Activate** or **Deactivate** it. Shows different option depending on the state.

Add VLAN

Same as using **Add VLAN** in the top of the window. Displays the *Add connection* window.

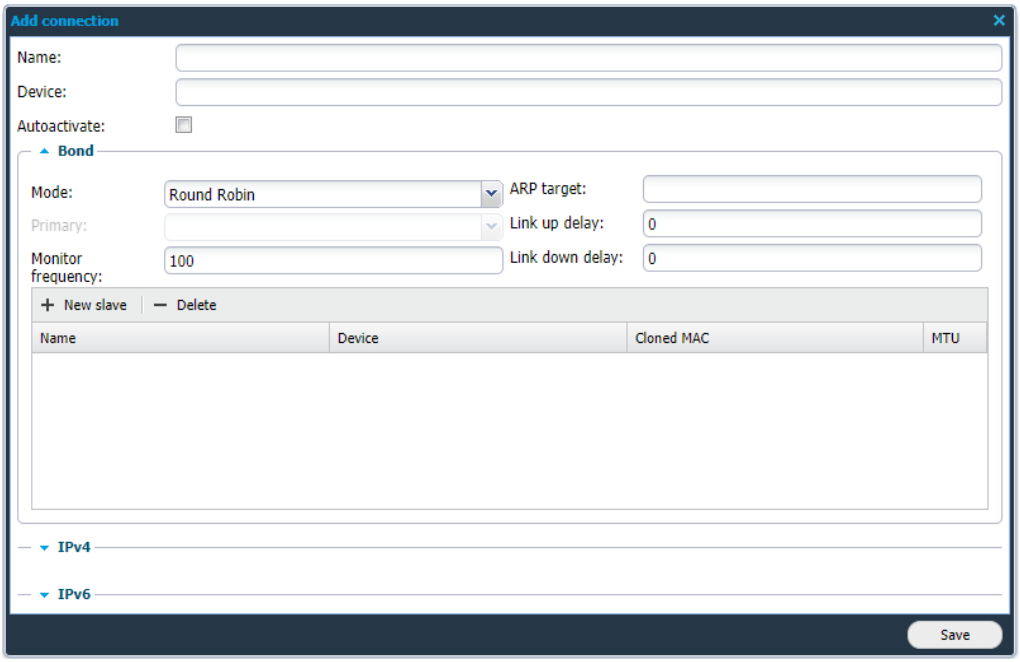


Options	Description
Name	Name of the VLAN.
Device	Device name of the VLAN.
Parent	Define the parent for the VLAN (Drop down menu where you can choose between already created interfaces).
ID	ID for the VLAN.
Autoactivate	Define if this interface should be automatically activated.
IPv4	Define IPv4 options such as ▶ **Type**: Auto, Manual, Link-Local, Shared, Disabled ▶ Addresses ▶ DNS ▶ Search Domain ▶ Default Gateway ▶ Routes ▶ Not default route ***Note**: Multiple DNS servers must be added comma separated.*
IPv6	Define IPv6 options such as ▶ **Type**: Auto, Manual, Link-Local, Shared, Disabled ▶ Addresses ▶ DNS ▶ Search Domain ▶ Default Gateway ▶ Routes

Options	Description
	► Not default route ***Note**: Multiple DNS servers must be added comma separated*.

Add bond

Same as using **Add bond** in the top of the window. Displays the *Add connection* window.



Options	Description
Name	Name of the bond.
Device	Device name of the bond.
Autoactivate	Define if this interface should be automatically activated.
Mode	Choose how the network packages should be sent out to the slave devices. ▶ Round Robin ▶ Active Backup ▶ XOR ▶ Broadcast ▶ 802.3ad ▶ Adaptive Transmit Load Balancing ▶ Adaptive Load Balancing
Primary	Only configurable for *Active Backup* mode. Choose which interface to be the primary device.
Monitor frequency	Enter how often monitoring should occur, in milliseconds, to verify if the interface is active.
ARP target	Define the target IP address of ARP requests.
Link up delay	Specify how long to wait before enabling the link in milliseconds.
Link down delay	Specify how long to wait after link failure before disabling the link in milliseconds.

Options	Description
Slave	Define the slave devices for the bond.
IPv4	Define IPv4 options such as ► **Type**: Auto, Manual, Link-Local, Shared, Disabled ► Addresses ► DNS ► Search Domain ► Default Gateway ► Routes ► Not default route ***Note**: Multiple DNS servers must be added comma separated*.
IPv6	Define IPv6 options such as ► **Type**: Auto, Manual, Link-Local, Shared, Disabled ► Addresses ► DNS ► Search Domain ► Default Gateway ► Routes ► Not default route ***Note**: Multiple DNS servers must be added comma separated*.

Add Ethernet

Same as using **Add ethernet** in the top of the window. Displays the *Add connection* window.

Options	Description
Name	Name of the Ethernet interface.
Device	Choose which device to enable.
Cloned MAC	Enter the MAC address of the interface.
MTU	Specify the Maximum Transfer Unit of the interface.
Autoactive	Define if this interface should be automatically activated.
IPv4	Define IPv4 options such as: ▶ **Type**: Auto, Manual, Link-Local, Shared, Disabled ▶ Addresses ▶ DNS ▶ Search Domain ▶ Default Gateway ▶ Routes ▶ Not default route ***Note**: Multiple DNS servers must be added comma separated.*
IPv6	Define IPv6 options such as: ▶ **Type**: Auto, Manual, Link-Local, Shared, Disabled ▶ Addresses ▶ DNS ▶ Search Domain ▶ Default Gateway ▶ Routes ▶ Not default route ***Note**: Multiple DNS servers must be added comma separated.*

Delete

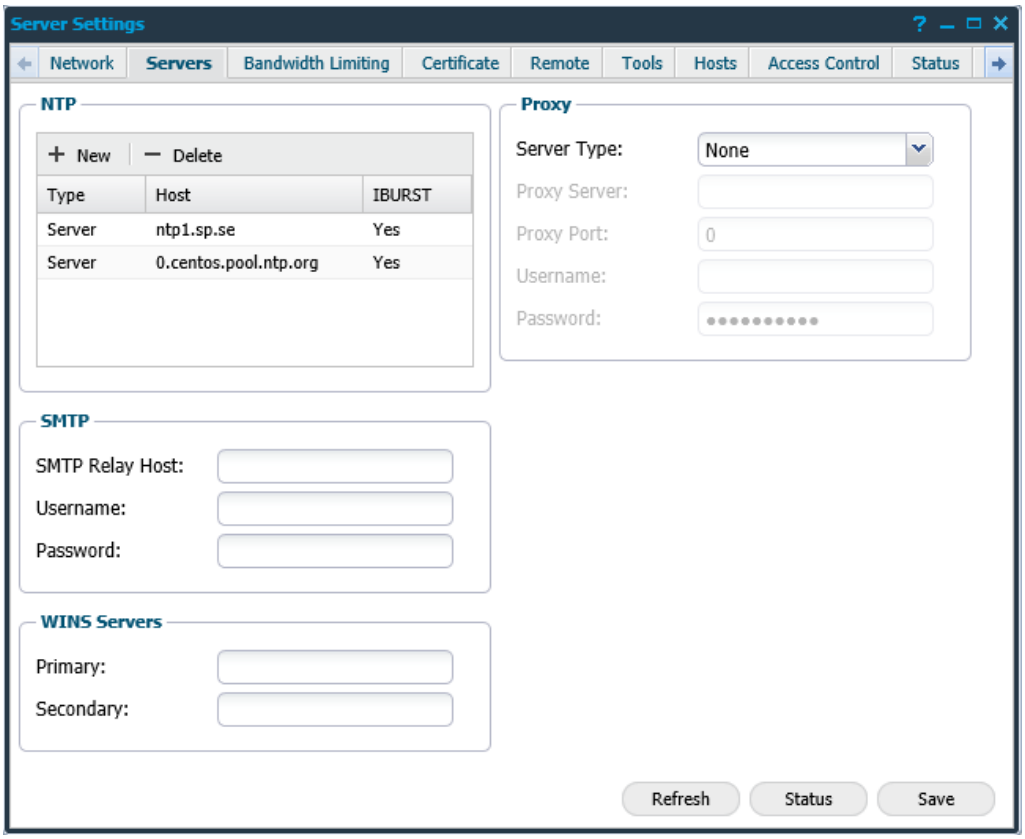
Removes the selected entry.

Edit

Edit the selected entry.

1.2 Servers Tab

In the **Servers** tab, the information related to different servers can be configured and changed.



1.2.1 NTP

In the NTP field, click **New** to add NTP hosts.
The following options are configurable for **NTP**:

Options	Description
Type	Choose between: ► Server ► Pool
NTP host	The host of the NTP server.
Iburst	► Enable (Checked) ► Disable (Unchecked)

1.2.2 SMTP

The following options are configurable for **SMTP**:

Options	Description
SMTP Relay Host	The hosts which the SMTP relay resides on. The relay host can be configured with its port. Example: mail.host.tld:587
Username	Define the username which is in use for authentication against the SMTP server.
Password	Define the password which is in use for authentication against the SMTP server.

1.2.3 WINS Servers

The following options are configurable for **WINS Servers**:

Options	Description
Primary	The primary host of the WINS server.
Secondary	The secondary host of the WINS server.

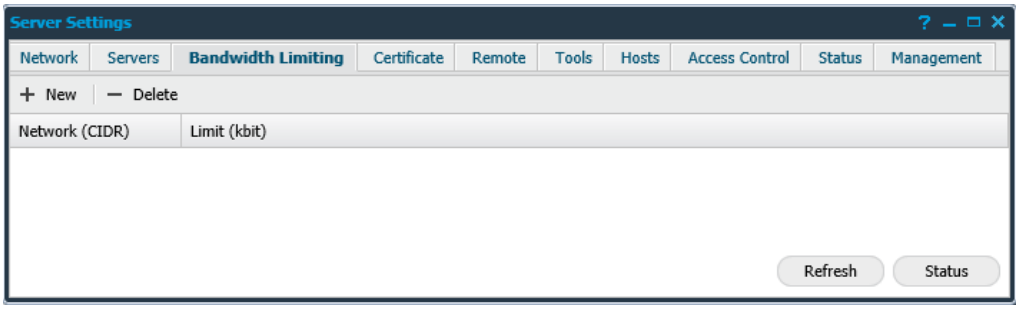
1.2.4 Proxy

The following options are configurable for **Proxy**:

Options	Description
Server Type	Define the server type of the proxy, choose between: ► None ► HTTP/HTTPS ► Socks4 ► Socks4a ► Socks5
Proxy Server	Define the proxy server.
Proxy Port	Define the port for which you connect to the proxy server.
Username	Define the username which is in use for authentication against the proxy server.
Password	Define the password which is in use for authentication against the proxy server.

1.3 Bandwidth Limiting

The **Bandwidth Limiting** grid is used to limit the bandwidth used to different networks.
***Note**: Bandwidth limit settings must be set on the HIAB performing the scanning in a Distributed environment.*



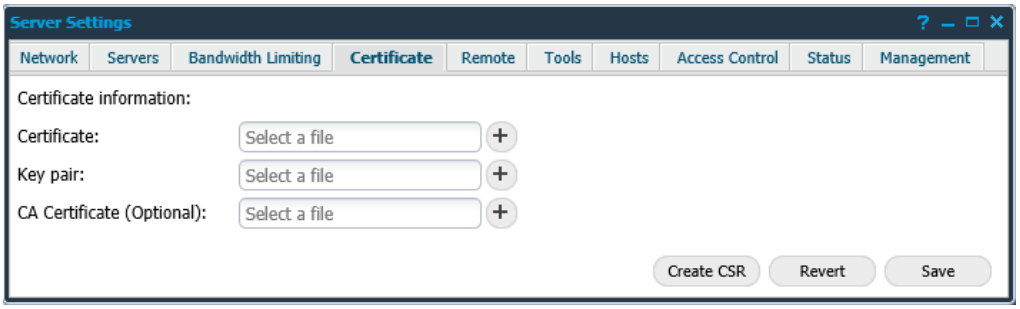
New opens the *Maintaining Bandwidth Limit* window where the bandwidth limit can be configured with the following options:

Options	Description
Network (CIDR)	Define the network range for the bandwidth limit.
Limit (kbit)	The limit on how much bandwidth the HIAB can use in kbit.

Delete removes the selected entry in the **Bandwidth Limiting Grid**.

1.4 Certificate Tab

In the **Certificate** tab the SSL certificates can be maintained, allowing secure communication with the HIAB over the HTTPS protocol.
The needed files can be uploaded for setting up the HIAB to authenticate itself correctly, with proper validation.

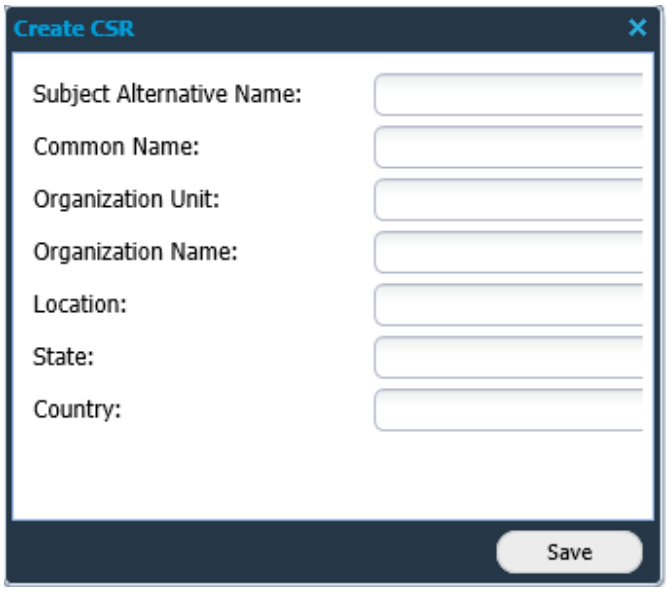


Options	Description
Certificate	Upload the certificate which you have received from your CA. Note that the certificate should start with a ----BEGIN CERTIFICATE---- marker.
Key	Upload the private key associated with the public key present in the certificate above. Note that this should not be password protected.
CA Certificate	Upload the certificate authorities' file containing the whole certificate chain to validate the certificate.

In the lower right corner, there are three buttons:

- **Create CSR** – Creates new certificate
- **Revert** – Reverts to the default certificate
- **Save** – Saves the new certificate

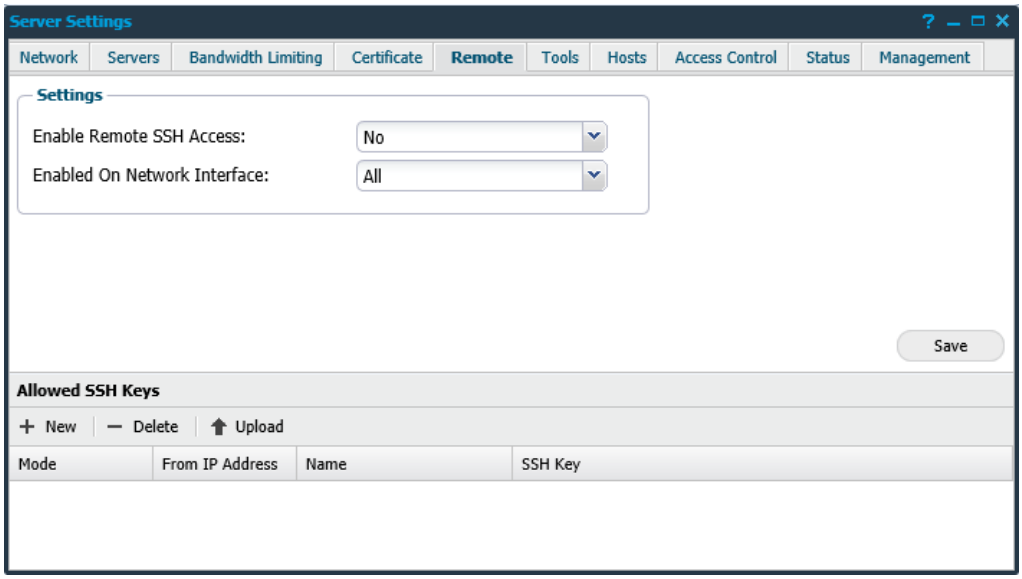
By clicking the **Create CSR** button, the *Create CSR* window is displayed, allowing you to create a private key file and a Certificate Signing Request (CSR) file using 4096-bit RSA encryption. The following options are configurable when creating the CSR:



Options	Description
Subject Alternative Name	The additional host names (sites, IP addresses, common names, etc.) to be protected by a single SSL Certificate.
Common Name	Define the domain name.
Organization Unit	The division of the organization handling the certificate.
Organization Name	The legal name of the organization.
Location	The city where the organization is located.
State	The state/region where the organization is located.
Country	The two-letter ISO code for the country where the organization is located.

1.5 Remote Tab

In the **Remote Tab** the remote SSH access to the HIAB console can be maintained.

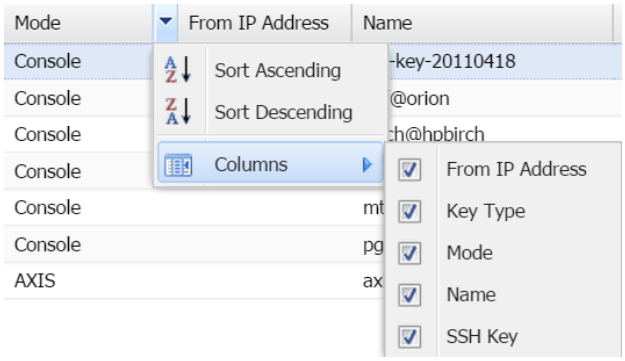


1.5.1 Settings Grid

In the settings grid, you can choose if whether to allow remote SSH connections to the HIAB console, and if the SSH daemon should be limited only to listen to a specific interface.

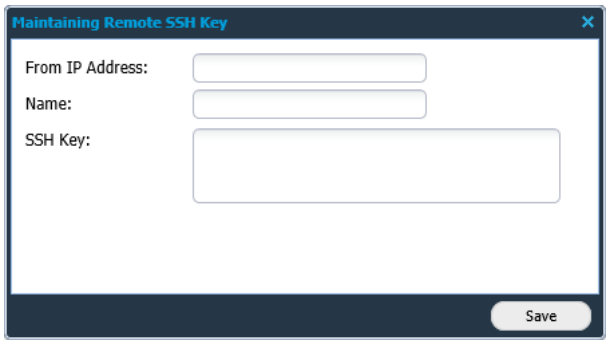
1.5.2 Allowed SSH Key Grid

The remote SSH access to the HIAB console requires valid SSH keys for authentication. The keys listed in the SSH Key Grid are valid for authentication.
Note that if **HIAB pingable** is set to OFF in the console, remote SSH access to the HIAB console is not possible. To enable the SSH access, open the HIAB console and press **w** *Configure UI management interface* followed by **p** *Toggle pingable* for the desired interface.
It is possible to disable or enable columns in the SSH Key Grid.



Options	Description
IP address	Displays if the key is limited to an IP address.
Key Type	The format of the SSH Key (RSA, DSA).
Mode	Displays mode (Console).
Name	Custom name.
SSH Key	SSH Key data.

New opens the *Maintaining Remote SSH Key* window where a new key can be created:

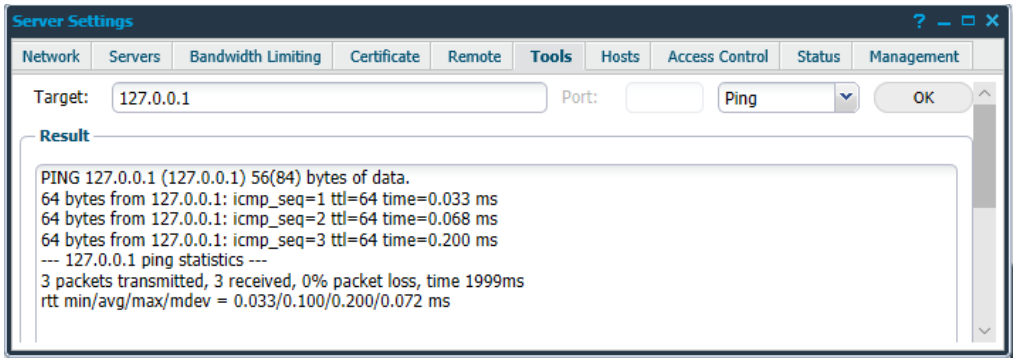


Options	Description
From IP address	Limit from what IP address a key can be used for authentication.
Name	Give the Key a custom name.
SSH Key	SSH Key data.

Upload displays a new window where an existing key be uploaded.

1.6 Tools Tab

The **Tools** tab gives you the opportunity to perform network commands while troubleshooting network issues.



Options	Description
Target	The target host that you wish to test with the selected tool.
Ping	Send PING requests to the defined target.
Traceroute	Perform UDP traceroute to the defined target.
TCP traceroute	Perform TCP traceroute to the defined target.
Port	Port number for the TCP traceroute. Not available for Ping and UDP traceroute.

Examples:

```
Ping
/usr/bin/ping -c3 <hostname>
/usr/bin/ping6 -c3 <hostname>

Traceroute
/usr/bin/traceroute [-T -p <port>] <hostname>
/usr/bin/traceroute6 [-T -p <port>] <hostname>
```

All results from the various troubleshooting tools is displayed in the Results field.

1.7 Hosts Tab

The **Hosts** tab gives you the opportunity to add host names which resolves the defined IP address when performing scans.
***Note**: Click **Save** in the lower right corner to update the list permanently.*

New opens the *Add Host* window where following options can be defined:

Options	Description
IP Address	Define the IP address.
Host Name	Define the host name.

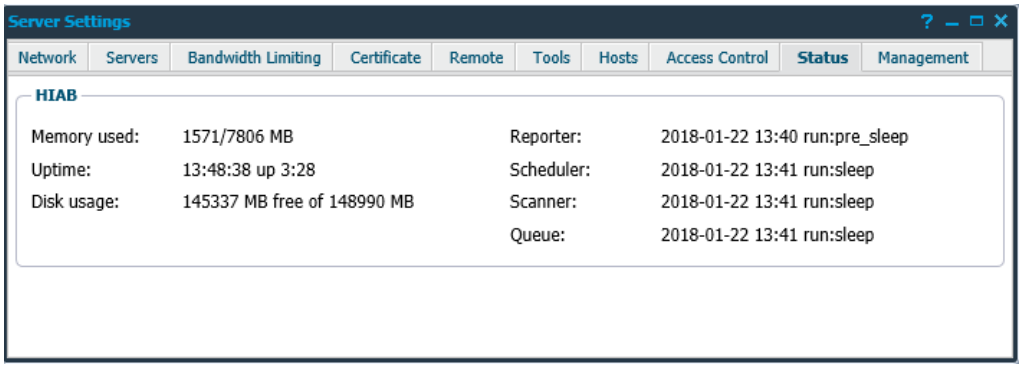
Delete removes the selected entry from the list.

1.8 Access Control Tab

The **Access Control** tab is used to limit the IP addresses that can access the Graphical User Interface.
To restrict the use, enter the IP address range which have access to the HIAB Graphical User Interface, make sure that the machine from which the Administrator is entering the IP range is a part of the allowed IP range.
Correct IP ranges is a requirement to prevent any unwarranted denial of access.

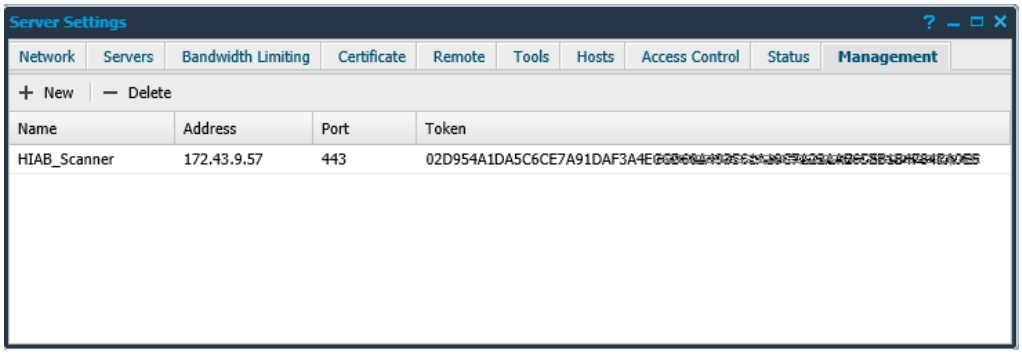
1.9 Status Tab

The **Status** tab shows status for the Scheduler and distributed scanners.



1.10 Management Tab

The **Management** tab allows you to remotely access the Graphical User Interface of another HIAB, if the two HIAB can communicate.



New opens the *Edit Hiab Management* window where the options for the remote HIAB can be configured:

Options	Description
Name	Name of the remote HIAB.
Address	IP address of the remote HIAB.
Port	Port the communication will talk over.
Token	App Token generated within the remote HIAB.

Delete removes the selected entry.