Outpost24

Vulnerability Management made easy

HIAB 64-Bit Console Manual

Version: 1.3

2018-03-28

Table of Contents

About this Guide

The main purpose of this document is to provide users a comprehensive overview of how to navigate in the 64-bit HIAB console. This document has been elaborated under the assumption that the reader has access to the HIAB appliance and its console.

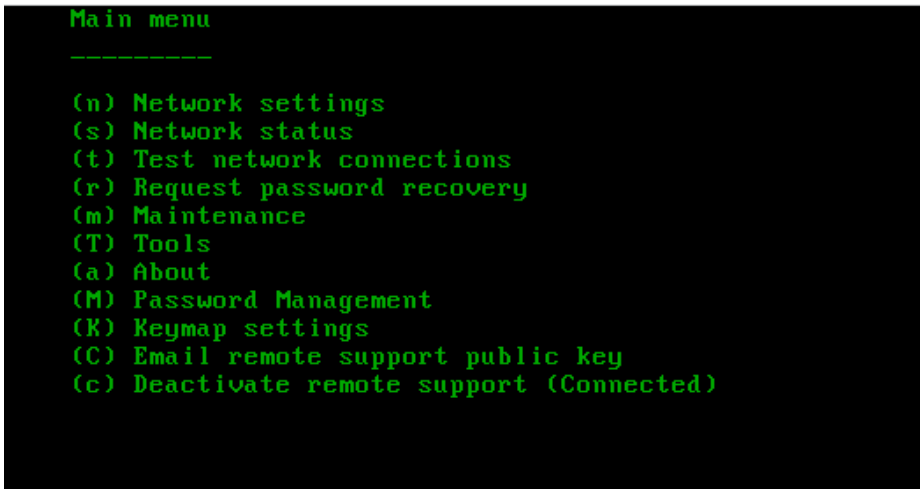
For support information, visit https://www.outpost24.com/support.

Copyright

Trademark

1 Getting Started

This guide will help you in setting up the HIAB appliance using terminal console. Once the HIAB is booted (or if you connect to the appliance via SSH), you will see the following screen on your monitor.



The main menu is a multi-choice menu that allows you to access different sections of the configuration of the appliance. From this menu, you can configure, update and harden your appliance.

The below table displays the available options and their functionalities.

Option	Description	Function
n	Network settings	Configure network settings like virtual hosts, static and dynamic interfaces, gateways, name servers and interface speed.
s	Network status	See the status for your current network settings.
t	Test network connections	Test all your network connections required to run Outpost services.
r	Request password recovery	Recover passwords for HIAB user.
m	Maintenance	Perform various maintenance actions such as updates, reboots and removals.
T	Tools	This section gives you access to system commands like ping, trace route and DNS lookup.
a	About	Displays your HIAB's current versions, uptime, memory and disk usage.
M	Password management	Set a password for your appliance so that future users need to present a set password to access the HIAB console.
K	Keymap settings	Choose your key map settings so that it corresponds to the keyboard you are using.
C	Email remote support public key	Email the public remote support key to Outpost24. This is required for remote support connection to succeed.
c	Remote support	Activating Remote Support will allow the support staff of Outpost24 to access the backend of your appliance. This is used for troubleshooting purposes.

***Note**: The options are case sensitive.*

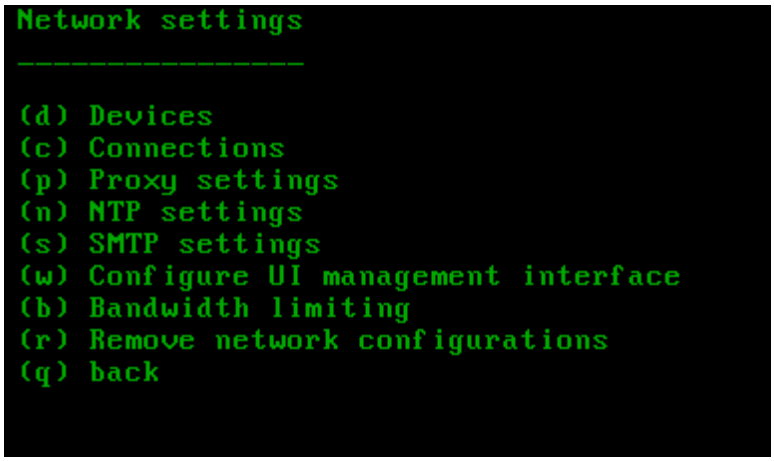
Most of the options in the Main Menu have one or multiple submenus. The submenus are not listed in the above table.

2 Configuring HIAB

Please check the below sections to configure HIAB as per your requirement.

2.1 Configure Network Settings

Press **n** in the main menu to access the Network Settings. In this section, you will be provided with an additional menu, each option will give you access to different sections in order to configure your network settings.

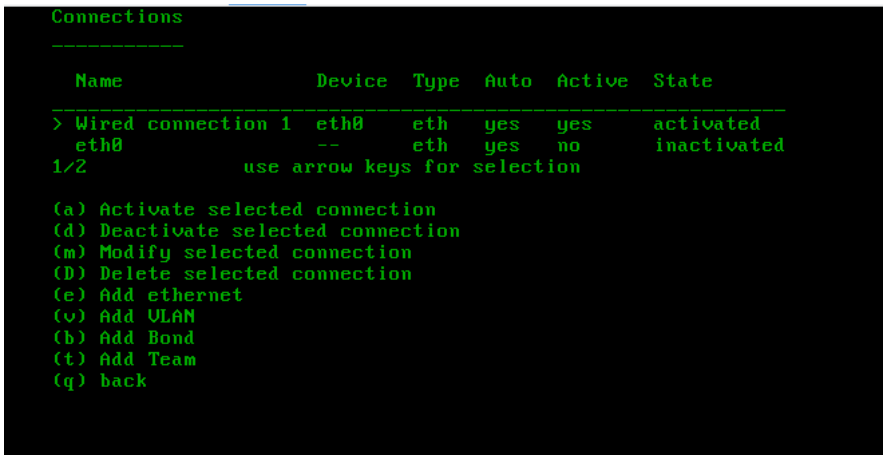


The below table displays the available options and their functionalities.

Option	Description	Function
d	Devices	This section allows you to see what devices your HIAB is connected to
c	Connections	In this section, you will be able to configure all the connections for your HIAB
p	Proxy settings	This section allows you to connect your HIAB to a proxy server through communication with updater, OUTSCAN & remote support. Scans does not happen through the proxy
n	NTP settings	This section allows you to connect your HIAB to a NTP server
s	SMTP settings	This section allows you to connect your HIAB to a SMTP server
w	Configure UI management interface	This section will let you set up to which active interfaces the HIAB should listen. Additional actions possible in this section are configuring pingable for interfaces and restarting the HIAB's HTTP server. For yes it will respond with ICMP rejects to TCP connects on closed ports and respond to ICMP requests while set to no it will simply drop such requests.
b	Bandwidth limiting	Set a bandwidth limit for your HIAB
r	Remove network configurations	This option removes all existing network settings from your HIAB
q	Back	Go back to previous menu

2.1.1 Connections

Press **c** in the Network settings menu to access **Connections**. The following window is displayed:



In the Connections menu, you will find all available interfaces. You can activate, deactivate and/or delete existing interfaces. By using the arrows on your keyboard, you may navigate to an entry and then use one of the set hotkeys to perform the intended action.
You can also add **Ethernet, VLAN** and **Bond** by performing the following actions:
***Note**: All guides below start from the Connections menu*

2.1.1.1 Adding Ethernet

1. Select option **e**
2. Enter the connection name, e.g. **MyEth**
3. Enter one device from all listed interfaces in the parentheses, e.g. **eth0**

2.1.1.2 Adding VLAN

1. Select option **v**
2. Enter the connection name, e.g. **MyVLAN**
3. Enter the device name, e.g. **Vlan**
4. Enter one parent device from all listed interfaces in the parentheses, e.g. **eth0**
5. Enter the VLAN id, e.g. **123**

2.1.1.3 Adding a Bond

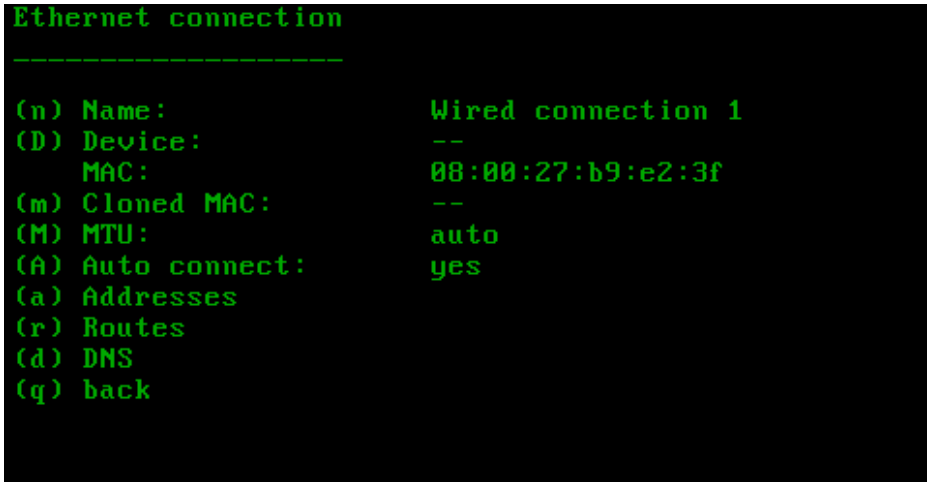
1. Select option **b**
2. Enter the connection name, e.g. **MyBond**
3. Enter the device name, e.g. **Bond1**
4. The bond will then be added to the list of connections. Use the arrows and the action **Modify selected connection** to configure it further.

2.1.1.4 Adding a Team

1. Select option **t**
2. Enter the connection name, e.g. **MyTeam**
3. Enter the device name, e.g. **Team1**
4. The team will then be added to the list of connections. Use the arrows and the action **Modify selected connection** to configure it further.

To modify your connections and assign IP's to them, you need to perform the following steps:

1. Select option **m**
   The following window is displayed:



1. Select option **a** to modify the addresses for the interface**.**
   The following window is displayed:

When an interface is activated, the IPv4 and IPv6 method is set to **auto** which states that DHCP is used by the HIAB to obtain the IP. You can also add static addresses under **auto**, but it will not be successful without a DHCP lease.

For more information on this, please refer to pg.27 of the following pdf:
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Networking_Guide/Red_Hat_Enterprise_Linux-7-Networking_Guide-en-US.pdf
To add a static IP, you need to perform following steps:

1. Select either **4** or **6**, depending on which IP version you are using
2. Enter **manual** and press enter
3. Press **a** to Add IP
4. Enter the desired IP address, for e.g. 192.168.2.3/24 and press enter.
   Note*: Specified in CIDR*

Note*: Once a change is made, you must deactivate and reactivate the interface for the changes to be active.*

You should now be back in the Ethernet connection window. In this menu, you are also able to add custom **Routes** and **DNS**.

2.1.1.5 To add custom Routes (optional)

1. Select option **r**
    2. Select option **a**
    3. Enter the destination, for e.g. 192.168.1.2/24.
       ***Note**: Specified in CIDR*
    4. Enter next hop (optional)
    5. Enter Metric for the route
    6. Press **q** to go back to **Ethernet connection** menu

2.1.1.6 Set Domain Name Servers (optional):

1. Select option **d**
    2. Select option **a**
    3. Enter the IP of the DNS server, for e.g. 192.168.1.3.
    4. Select **q** to go back to the **Ethernet connection** menu

2.1.2 Configure Proxy Settings

The HIAB may be configured to use a proxy when communicating with other devices. The use of a proxy is setup by performing the following steps (starting from the **Network Settings** menu):

1. Select option **p**
    2. Select option **t** to choose which type of proxy you wish to connect to
    3. Select type:
       0 disables the use of proxy
       4 socks version 4
       a socks version 4a
       5 socks version 5
       h HTTP/HTTPS proxy
    4. Select option **h**, enter the proxy address, e.g. 192.168.100.2
    5. Select option **p**, enter the proxy port, e.g. 8080

If you want to add a password, follow the below steps:

1. Select option **u**
    2. Enter the user name for the proxy service, e.g. “myusername”
    3. Select option **a**
    4. Enter the password for the above username, e.g. “mypassword”
    5. Select option **d** to update the proxy settings

2.1.3 Configure NTP Settings

The HIAB can be configured to use a time service in order to keep the clock accurate. To define the usage of NTP server, you need to perform the following steps (starting from the **Network Settings** menu):

1. Select option **n**
    2. Select option **s**
    3. Enter the IP address or hostname of the NTP server. You can also add an NTP ppol instead of a specific server.

2.1.4 Configure SMTP Settings

The HIAB can be configured to use a SMTP relay server if the network does not allow communication out using port 25. You can also configure **sasl** authentication for SMTP. Performing the following steps will set up the use of a SMTP relay (Starting from **Network Settings** menu):

1. Select option **s**
2. Select option **a**
3. Enter the SMTP relay server, e.g. **smtp.mycompany.com**

2.1.5 Configure UI Management Interface

The HIAB can be configured to show only the user interface on a specific interface instead of allowing it on all available interfaces (which it does by default). In order to change this, you need to perform the following steps (Starting from the **Network Settings** menu):

1. Select option **w**
2. Use the arrow keys to select on which interface you wish to change the settings.
3. Use options **p** and **t** to toggle (enable/disable) the different functions per interface. If **pingable** results in any change, disable the response on ping. You are not allowed to have the HTTP server listen to all interfaces.
4. If you make any changes to the HTTP server, you should restart that service before the changes takes effect. Select the option **r** to restart.

2.1.6 Bandwidth Limiting

You can limit the amount of outbound traffic from the HIAB which is configured in this section. Define the network for which you would like to set a limit and then define the maximum amount of data sent to that network. To configure the bandwidth limitation, perform the following steps (Starting from the Network Settings menu):

1. Select option **b**
2. Select option **a**
3. Enter network, e.g. 192.168.1.1/24.
   ***Note**: Defined in CIDR*
4. Enter the bandwidth limit in Kbit/s, e.g. 400

2.2 Network Status

Press **s** in the main menu to access the Network Status.

2.3 Test Network Connections

Press **t** in the main menu to access Test Network Connections. In this section, you can test your network connections. Option **t** in the main menu will confirm whether the appliance can connect to outside services or not. Select option **r** to start the network test.
For more information, choose option **d** and you will be presented with a tcpdump from the last performed network test, that information may be useful when troubleshooting.

The result of test is determined by **INFORM**. Following ramifications will occur if the test results in a **FAILURE**:

DNS lookup: Lacks the possibility to look up host names based on IP addresses and lacks support for sending emails directly.

Update repositories: No updates will be possible. Out of band updates may be an option if preferred.
***Note**: Before enrollment is conducted, the key isn't available and it will produce a failure until enrolled.*

SMTP Relay Server: If the HIAB is not allowed to send emails directly, it will use the SMTP relay host for sending emails. If this is not defined, there will not be any email notifications sent.

NTP server: The INFORM. presented by NTP will reflect values retrieved from the **chronyc sources** command. The reach expresses how many of the last 8 polls for the different servers have succeeded.
Ex: 16/16 means all the latest 8 polls from both servers have succeeded. Fail indicates the count of servers to which connectivity has been lost or whose packets do not pass all tests. It is also shown at start-up, until at least 3 samples have been gathered from it. False-tick indicates the count of servers which **chronyc** thinks is a false-ticker (i.e. its time is inconsistent with a majority of other sources). Variable indicates the count of servers whose time appears to have too much variability. There is no simple way to boil this down to a binary **SUCCESS** or **FAILURE**.

Remote support: No remote assistance will be available.

Outscan: No scans can be executed using the HIAB EXTERNAL service even if a license is available.
***Note**: HIAB (effective since the 64-bit version) cannot be enrolled if this fails.*

2.4 Request Password Recovery

Press **r** in the main menu to access Request Password Recovery. If the main account's password is lost, you can request for a recovery link to be sent from the console.
For recovery link email to be delivered, the HIAB needs to be able to send emails. This means, it is required to configure the email feature correctly.
The password link will also be available on the screen, even if the HIAB is not properly configured to send out emails.
To request a new password, perform the following steps:

1. Select option **e**. Insert a recipient email address for the recovery link, different to the one registered to the main account; e.g. myemail@mycompany.com.
2. Select option **r**.
   The recovery link is sent from HIAB to the provided email address. It is also displayed on screen.

Or

1. Select option **r**.
   The recovery link will appear on screen.

2.5 Maintenance

Press **m** in the main menu to access the Maintenance. In this section, you will find all the actions necessary for maintaining your HIAB:

2.5.1 Update

The HIAB can perform updates for its installed software and scripts directly from the console.
If the HIAB has not yet been enrolled, the update option will not be available.
It is instead replaced by an enroll option. Perform the following steps (starting from the **Maintenance** menu):

If the HIAB is not yet enrolled:

1. Select option **e**
2. Enter the credentials for your Main user

If the HIAB is enrolled:

1. Select option **u**
2. Select option **d** to start the update process

2.5.2 Reboot

To reboot the HIAB appliance, select option **b** in the **Maintenance** menu and enter **yes** to

confirm

***Note**: The HIAB will reboot immediately without any additional confirmation being required.*

2.5.3 Shutdown

To shut down the HIAB appliance, select option **s** in the **Maintenance** menu and enter yes to confirm.

***Note**: If you wish to abort, press Ctrl+C. This will restart the console menu application and bring you back to the main menu.*

2.5.4 Remove all scan data

This option can be used for deleting all scan data from the appliance when necessary. For e.g. an exchange of the appliance or upon returning the device to service.

The following steps are required to remove all scan data (starting from the **Maintenance** menu):

1. Select option **r**. Read the information that is displayed on the screen until you fully understand what will happen once you proceed with this action.
2. Type **yes** if you are certain, and press Enter

The HIAB will remove all scan data and return to the main menu.

2.5.5 Restore Server to default state

This option allows you to restore the HIAB appliance to default state from the console.

The following steps are required to perform a restore (starting from the **Maintenance** menu):

1. Select option **d**. Read the information that is displayed on the screen until you fully understand what will happen once you proceed with this action.
2. Type **yes** if when certain, and press **Enter**.

The HIAB will restore itself to default state and reboot.

2.6 Tools

Press **T** in the main menu to go to Tools. In this section, you can perform various tasks to determine if HIAB is working properly.

2.6.1 Mail Queue

The HIAB has its own SMTP server, which it uses to send out emails. For e.g. reports or event notifications.

To see the mail queue, do the following step (starting from the **Tools** menu):

1. Select option **m**

2.6.2 Ping to a Host

The HIAB can PING other hosts for the administrator to determine if the network configuration allows it to connect to other networks properly.

To PING a host, do the following steps (starting from the **Tools** menu):

1. Select option **p**
2. Enter the host name or IP, e.g. 192.168.100.1
3. Press Enter to return to the tools menu

2.6.3 Traceroute to a host:

The HIAB can perform a trace route to other hosts for the administrator to determine if the network configuration allows it to connect to other networks correctly.

To trace route to a host, do the following steps (starting from the **Tools** menu):

1. Select option **t**
2. Enter the host name or IP, e.g. 192.168.100.1
3. Press Enter to return to the tools menu

2.6.4 DNS Lookup:

The HIAB can perform a DNS lookup of a host for the administrator to determine if the DNS service works correctly.

To do a DNS lookup, do the following steps (starting from the **Tools** menu):

1. Select option **d**
2. Enter the host name or IP, e.g. 192.168.100.1

2.7 About

Press **a** in the main menu to access the About. This section displays the details of your 64-bit HIAB's version, memory used, disk space and copyrights.

2.8 Password Management

Press **M** in the main menu to access *Password Management*. The HIAB appliance can be set up to demand a password to gain access to the console when you have physical access to the appliance.

To set this up, do the following steps:

1. Select option **s**
2. Enter a password like "mysecretpassword", confirm the password.

Once a password is set, an extra option is added in the main menu **Logout**, using the hotkey **L**. This allows you to lock the appliance.
To unlock the appliance, enter the set password.

***Note**: No password recovery is available for this feature.*

2.9 Keymap Settings

Press **K** in the main menu to access the Keymap Settings. By default, the standard key map is **us**. However, if you are using another keyboard you can configure the key map in this section.
Choose between 500+ key maps to find the one that matches your setup.

To change the key map, you need to perform the following steps:

1. Browse through all the available key maps by using the up and down arrows. For quicker browsing through the entries, use ENTER and BACKSPACE to move eight entries up or down the list.
2. Select option **c**, when the arrow is pointing at the desired keymap.
3. Select option **r** to restore to the default keymap.

2.10 Email remote support public key

Press **C** in the main menu to go to Email remote support public key. Sending the public SSH key of the HIAB will allow the support team at Outpost24 to access the backend of your HIAB, once remote support has been activated.

To send the email, please perform the following steps:

1. Select option **e** to enter the recipient email address (support@outpost24.com is default).
2. Select option **r** to send the public key to entered email address.

2.11 Activate remote support

Press **c** in the main menu to access the Activate remote support. By activating Remote Support, you allow the support team at Outpost24 to access the backend of your HIAB. This is mainly used for troubleshooting if any issues occur during the operational use of your HIAB.

If a successful connection is to be made between your HIAB and Outpost24's remote support server, the following criteria must be fulfilled:

The HIAB must be able to communicate outwards on port 22 to the IP 91.216.32.136, through any firewall/IDS/IPS.
Deep package inspection must be turned off for the communication between the HIAB and the remote support server.

Use the Test Network Connections to determine if the communication to our remote support server is successful.