

HIAB 64-Bit Migration

A Quick Start Guide

Table of Contents

1	OVERVIEW OF HIAB MIGRATION PROCESS	4
2	BACKUP HIAB	5
3	RECORD IP & MAC INFORMATION	7
3.1	MAC ADDRESS	8
3.2	IP ADDRESS	8
4	START NEW HIAB	9
5	CONTACT SUPPORT	12
6	CONFIGURE NETWORK SETTINGS	13
6.1	CONFIGURE ACTIVE INTERFACE	14
6.2	CONFIGURE INTERFACE CONNECTIONS	15
6.3	CONFIGURE DEFAULT GATEWAY	17
6.4	CONFIGURE DNS SERVERS	18
6.5	TOGGLE INTERFACE	19
6.6	TEST NETWORK CONNECTIONS	20
7	ENROLL 64-BIT HIAB	22
8	RESTORE BACKUP	24
9	UPDATE DISTRIBUTION SETTINGS	26
9.1	CONFIRM DISTRIBUTED CONFIGURATIONS	26
9.2	CONNECTING SCANNERS TO SCHEDULERS	27
9.3	GROUPING SCANNERS	28
10	DECOMMISSION 32-BIT HIAB	29

About This Guide

The purpose of this document is to aid the HIAB Migration process. This document will refer to the different stages of the migration process from 32-bit to 64-bit. 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

© 2020 Outpost24®. All rights reserved.

This document may only be redistributed unedited and unaltered. This document may be cited and referenced only if clearly crediting Outpost24® and this document as the source. Any other reproduction and redistribution in print or electronically is strictly prohibited without explicit permission.

Trademark

Outpost24® and OUTSCAN™ are trademarks of Outpost24® in Sweden and other countries.

1 Overview of HIAB Migration Process

The migration process follows a simple timeline, which is as shown below:



Step 1: Backup HIAB

Step 2: Record IP & MAC Information

Step 3: Start New HIAB

Step 4: Contact Support

Step 5: Configure Network Settings

Step 6: Enroll 64-Bit HIAB

Step 7: Restore Backup

Step 8: Update Distribution Settings (only applicable to Distributed HIAB scenario)

Step 9: Decommission 32-Bit HIAB

Important Note

Updating distribution settings is only applicable to those environments where distributed deployments are in place.

2 Backup HIAB

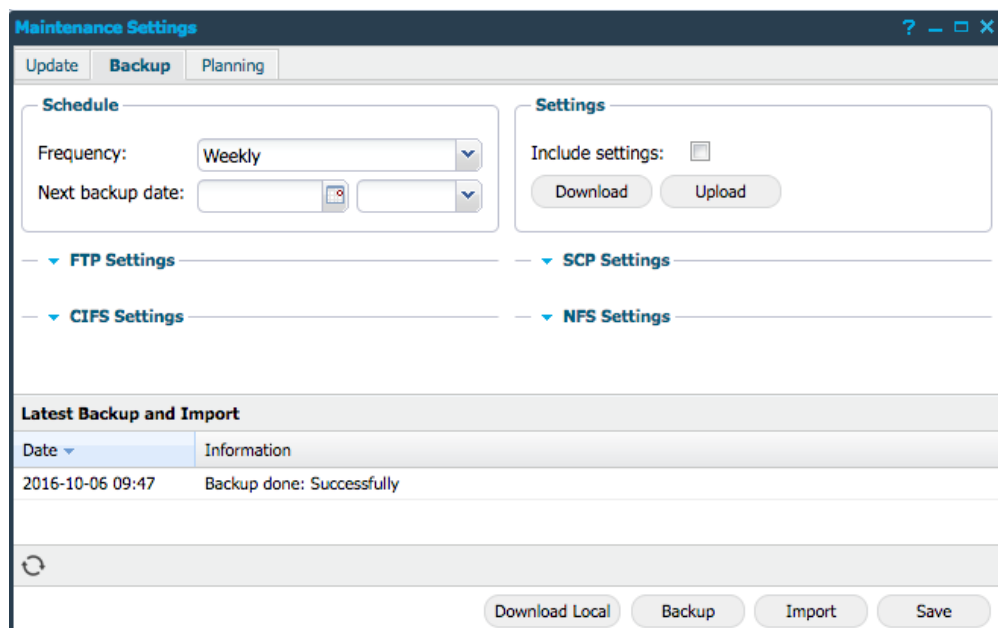
HIABs can be backed up to FTP, SCP, CIFS, or NFS servers. Alternatively, a local backup can be downloaded to your own machine.

To back up the existing HIAB scheduler, follow the below procedure.

1. Go to the **Main Menu → Settings → Account** window, select the **License** tab and review the number of IPs and scans of your license.
2. Go to the **Main Menu → Settings → Maintenance** window, select the **Backup** tab.
3. To include the server settings to Backup file, select the checkbox beside **Include settings**. To download the settings as a separate file, click on **Download**.

Note: The network settings will not be migrated.

4. To enable to the **Download Local** option, you must first backup the system to the HIAB locally, this will then allow you to download the HIAB to your local machine. Click on the **Backup** button.



5. Once complete, select the refresh icon (bottom left) to view the **Backup done: Successfully** message.

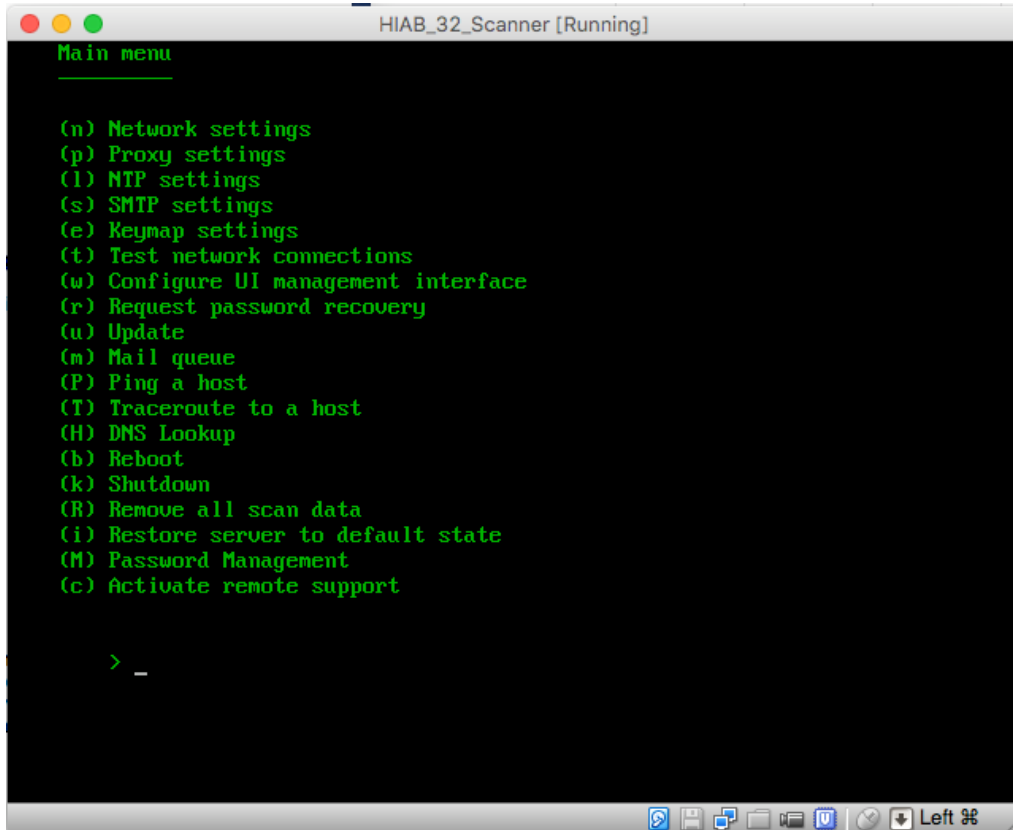
Note: The HIAB will not notify you that the backup is complete.

- ◆ Using FTP creates a file on the FTP server called:
`hiabdumpData_THE_IP_ADDRESS_YYYY-MM-DD.exp`, it holds all information such as scan schedules, users, roles, results and so on. Take a note of the file name.
- ◆ Using the **Download local** option creates a file on your device named `localbackup.exp`.

3 Record IP & MAC Information

The network information is obtainable from the HIAB Console by selecting option **(n)** Network Settings.

Make a note of the network settings.

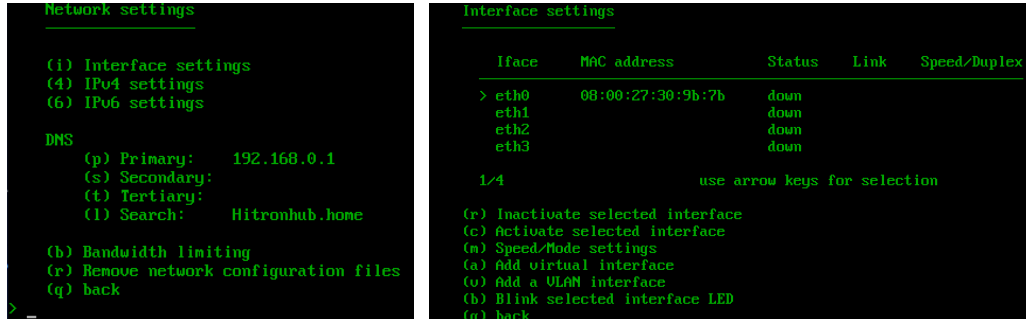


```
HIAB_32_Scanner [Running]
Main menu
-----
(n) Network settings
(p) Proxy settings
(l) NTP settings
(s) SMTP settings
(e) Keymap settings
(t) Test network connections
(w) Configure UI management interface
(r) Request password recovery
(u) Update
(m) Mail queue
(P) Ping a host
(T) Traceroute to a host
(H) DNS Lookup
(b) Reboot
(k) Shutdown
(R) Remove all scan data
(i) Restore server to default state
(M) Password Management
(c) Activate remote support

> _
```

3.1 MAC Address

- To find the MAC address for the HIAB interface, choose option **i** (Interface Settings) to view the MAC address of the active interface.



```

Network settings
(i) Interface settings
(4) IPv4 settings
(6) IPv6 settings

DNS
  (p) Primary:    192.168.0.1
  (s) Secondary:
  (t) Tertiary:
  (l) Search:    Hitronhub.home

(b) Bandwidth limiting
(r) Remove network configuration files
(q) back
> _

Interface settings
  Iface  MAC address  Status  Link  Speed/Duplex
  > eth0  08:00:27:30:9b:7b  down
  eth1  down
  eth2  down
  eth3  down

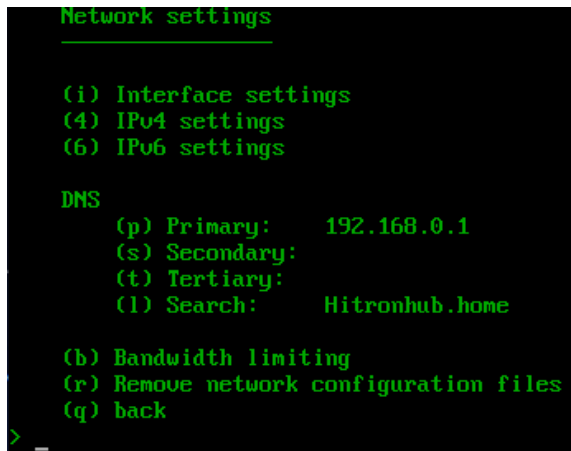
  1/4 use arrow keys for selection

(r) Inactivate selected interface
(c) Activate selected interface
(m) Speed/Mode settings
(a) Add virtual interface
(o) Add a VLAN interface
(b) Blink selected interface LED
(q) back
  
```

- Note the MAC address.
- Select option **q** (back).

3.2 IP Address

- To check the IP address of the interface, select option **4** (IPv4 settings) or **6** (IPv6 settings) from the network settings.



```

Network settings
(i) Interface settings
(4) IPv4 settings
(6) IPv6 settings

DNS
  (p) Primary:    192.168.0.1
  (s) Secondary:
  (t) Tertiary:
  (l) Search:    Hitronhub.home

(b) Bandwidth limiting
(r) Remove network configuration files
(q) back
> _
  
```

- Note the IP address.
- Select option **q** (back) until you return to the main HIAB menu.

4 Start New HIAB

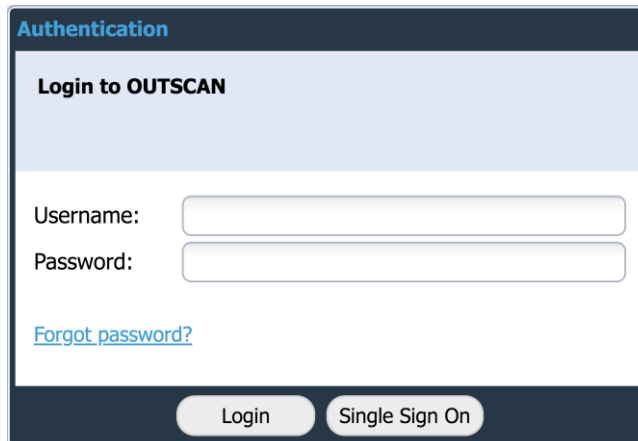
Disable the updates on the 32-bit HIAB by navigating to **Main Menu → Settings → Maintenance** removing any scheduled updates in the **Update** tab.

Select a time frame where no scans are scheduled, and no users will access the system. Follow the below procedure to start a new HIAB.

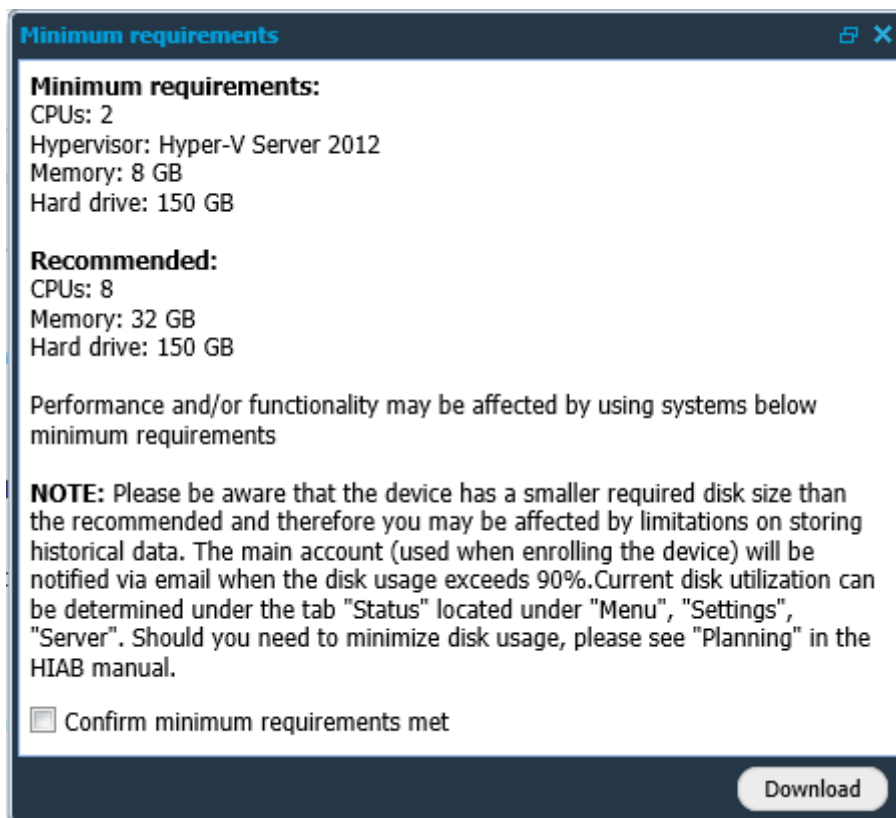
Note: *Do not proceed with enrolment until you have received confirmation of the HIAB license amendment from Support.*

Virtual HIAB Appliance

1. Visit <https://outscan.outpost24.com>.
2. Log in to **OUTSCAN** with the main user credentials.



3. Go to **Menu → Support** to open the *Support System* window.
4. In the Support System window select the **Virtual HIAB Appliance** tab. Six download options are displayed, four VMware and two Hyper-V.
5. Select the option that is most suitable for your virtual environment, see *Download Option* table for more information and click on the **Download** button located to the right.
6. In the Minimum Requirements pop-up window, select the **Confirm minimum requirements met** and click on the **Download** button.



7. Select a location to store the downloaded **OVA file**.
8. Open your **administration tool** for the virtual environment.
9. Select the option to **deploy an OVF or OVA file**.
10. Follow the instructions in the application.
11. Start the virtual machine.

Download Options

Title	Attributes	Recommended	Minimum
VMware			
HIAB VMware Virtual Image (150 GB)	Size: ~1.1GB	CPUs: 8 Memory: 32 GB Hard drive: 150 GB	CPUs: 2 Hypervisor: ESXi 5.5, Fusion 6.x, Workstation 10.x or Player 6.x Memory: 8 GB Hard drive: 150 GB
HIAB VMware Virtual Image (150 GB)*	Size: ~1.1GB	CPUs: 8 Memory: 32 GB Hard drive: 150 GB	CPUs: 8 Hypervisor: ESXi 5.5, Fusion 6.x, Workstation 10.x or Player 6.x Memory: 32 GB Hard drive: 150 GB

HIAB VMware Virtual Image (1 TB)	Size: ~1.1GB	CPUs: 8 Memory: 32 GB Hard drive: 1 TB	CPUs: 2 Hypervisor: ESXi 5.5, Fusion 6.x, Workstation 10.x or Player 6.x Memory: 8 GB Hard drive: 500 GB
HIAB VMware Virtual Image (1 TB)*	Size: ~1.1GB	CPUs: 8 Memory: 32 GB Hard drive: 1 TB	CPUs: 8 Hypervisor: ESXi 5.5, Fusion 6.x, Workstation 10.x or Player 6.x Memory: 32 GB Hard drive: 500 GB
Hyper-V			
HIAB Hyper-V Virtual Image (150 GB)	Size: ~1.1GB	CPUs: 8 Memory: 32 GB Hard drive: 150 GB	CPUs: 2 Hypervisor: Hyper-V Server 2012 Memory: 8 GB Hard drive: 150 GB
HIAB Hyper-V Virtual Image (1 TB)	Size: ~1.1GB	CPUs: 8 Memory: 32 GB Hard drive: 1 TB	CPUs: 2 Hypervisor: Hyper-V Server 2012 Memory: 8 GB Hard drive: 500 GB

Physical HIAB Appliance

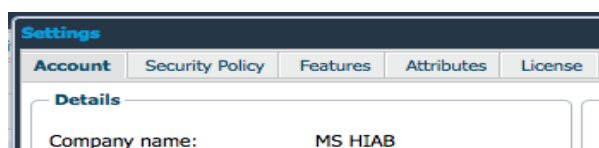
1. Make sure that the new HIAB is connected to a monitor and has access to internet.
2. Download the latest Remote installation disk image and burn it to a disk (contact support@outpost24.com for the latest version).
3. Power on the new HIAB and insert the **Remote Installation Disk**.
4. Follow the onscreen instructions.
5. Enter a static IP address when prompted.

Note: If you do not disable the updates on 32-bit HIAB before starting up the 64-bit HIAB, it might interfere and grab the license. Then the 64-bit cannot be enrolled.

5 Contact Support

Contact Outpost24's Support team and notify that you are migrating to a 64-bit HIAB. You are required to provide the following information to our support team.

1. **MAC Address** of the old HIAB.
2. Your Account Name.
To check this, log in to HIAB.
Go to **Menu** → **Settings** → **Account** → **Company Name**.



Outpost24 Support will prepare the HIAB licenses ready for migration to the 64-bit HIAB. In the meantime, you can proceed with configuring the 64-bit HIAB network settings.

6 Configure Network Settings

You need to configure the network settings of the new HIAB and test the network connections to ensure that all works as expected, prior to enrollment.

It is key to ensure the HIAB IP address remains the same; this makes it simpler for distributed setups to restore from the previous backup and ensure settings and firewall rules remain the same.

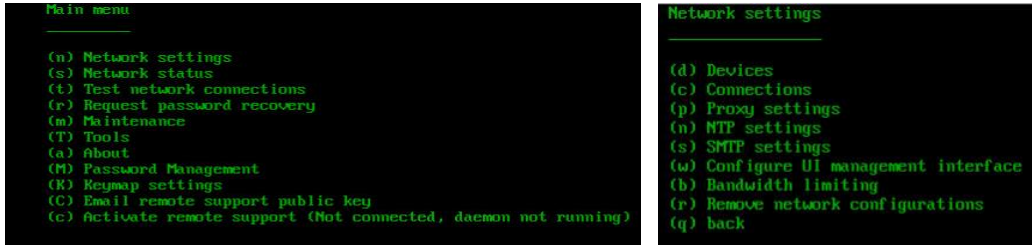
HIAB Firewall Rules

The HIAB Requires several firewall rules to allow smooth functionality regarding updates and enrolment. Below is a list of rules that are possible, however *Enrollment* and *Update* rules are necessary.

Service	Destination	Port	Protocol	Direction	Description
NTP	91.216.32.135	123	UDP	Outbound	Time Protocol
Remote Support	91.216.32.136	22	TCP	Outbound	Remote Assistance
Update	91.216.32.142	443 and/or 5000	TCP	Outbound	HIAB Updates
Enrolment	91.216.32.141	443	TCP	Outbound	Registering HIAB
External	outscan.outpost24.com	443	TCP	Outbound	External Scanning from HIAB
WEB	<HIAB IP>	443	TCP	Inbound	WEB GUI
Scanner	<HIAB IP>	443	TCP	Outbound	Communication to scanner, depends on Polling enabled or not
SMTP	<SMTP Server>	25	TCP	Outbound	For the HIAB to send emails
DNS	<DNS Server>	53	TCP/UDP	Outbound	To resolve host names
SSH	<HIAB IP>	22	TCP	Inbound	To allow remote access to the console
Proxy	<Proxy IP>	<Proxy port>	TCP	Outbound	To allow communications using a proxy server
FTP	<FTP IP>	<FTP Port>	TCP	Outbound	To perform backup and imports

6.1 Configure Active Interface

The console for the 64-bit HIAB is slightly different to the 32-bit appliance.



1. Select option **n** (Network Settings) to configure the network.



Device	Type	State	Connection	MAC
> eth0	ethernet	connected	Wired connection 1	00:0C:29:46:72:EB
1/1				

2. Select option **d** (Devices) to go to network interface.
3. The interface may already be up. If it does not show up, select option **c** (Connect selected device).
4. Select option **q** (back) and proceed further.

6.2 Configure Interface Connections

Next, you must configure the IP address and other network information to ensure the HIAB can communicate with your network.



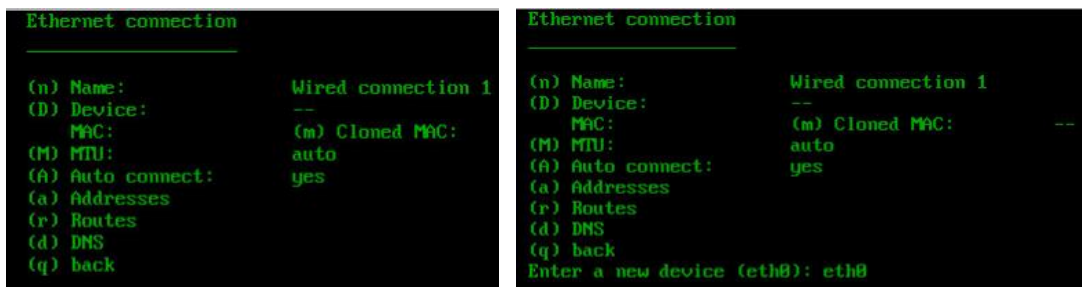
```

Network settings
-----
(d) Devices
(c) Connections
(p) Proxy settings
(n) NTP settings
(s) SMTP settings
(w) Configure UI management interface
(b) Bandwidth limiting
(r) Remove network configurations
(q) back

Connections
-----
Name                Device Type Auto Active State
-----
> Wired connection 1 eth0  eth  yes  yes  activated
  eth0                --  eth  yes  no  inactivated
1/2
      use arrow keys for selection

(a) Activate selected connection
(d) Deactivate selected connection
(m) Modify selected connection
(D) Delete selected connection
(e) Add ethernet
(o) Add VLAN
(b) Add Bond
(t) Add Team
(q) back
  
```

1. Navigate to option **c** (Connections), you will see a list of available interfaces. If there are two but previously you saw only one, disregard the second interface and only work on the first connection. You may see the state of the first connection as already active, if it is not, do not worry - we will do this later.



```

Ethernet connection
-----
(n) Name:                Wired connection 1
(D) Device:              --
   MAC:                  (m) Cloned MAC:      --
(M) MTU:                 auto
(A) Auto connect:       yes
(a) Addresses
(r) Routes
(d) DNS
(q) back

Ethernet connection
-----
(n) Name:                Wired connection 1
(D) Device:              --
   MAC:                  (m) Cloned MAC:      --
(M) MTU:                 auto
(A) Auto connect:       yes
(a) Addresses
(r) Routes
(d) DNS
(q) back
Enter a new device (eth0): eth0
  
```

2. Select option **m** (Modify selected connection). You will need to assign a device to the connection beforehand.
3. Option **D** (Device) allows you to define the interface to use for this connection – typically eth0, if you are unsure, go back to section 6.1 *Configure Active Interface* and check your interface name.
4. Configure the addresses for the connection, select option **a** (Addresses).
5. By default, the IPv4/6 addresses will be set to auto. Ideally, we would define a manual IP address.

- Select option **a** (Add IP) to add the IP address you wish to set for this HIAB. You must also add the CIDR subnet range.

```

Addresses
-----
CIDR
0/0          use arrow keys for selection
IPv4 Dynamic: 192.168.0.54
IPv6 Link:    fe80::28c:29ff:fe46:72eb/64
IPv6 Dynamic:
(a) Add IP
(d) Remove selected IP
(4) IPv4 Method: auto
(6) IPv6 Method: auto
(q) back
  
```

```

Addresses
-----
CIDR
> 192.168.0.230/24
L/1          use arrow keys for selection
IPv4 Dynamic: 192.168.0.54
IPv6 Link:    fe80::28c:29ff:fe46:72eb/64
IPv6 Dynamic:
(a) Add IP
(d) Remove selected IP
(4) IPv4 Method: manual
(6) IPv6 Method: ignore
(q) back
  
```

- Select option **4** (IPv4 method) and set this to manual, then select option **6** (IPv6 Method) and set this to ignore.
Note: If you do not wish to use IPv6, select option q (back) twice to continue with next steps.
- Activate the connection by selecting option **a** (activate selected connection) from the connection screen.
- Select option **q** (back) and proceed further.

6.3 Configure Default Gateway

The next step is to configure the default gateway.

1. From the Ethernet connection screen, select option **r** (routes).

```

Ethernet connection
-----
(n) Name:          Wired connection 1
(D) Device:       eth0
    MAC:          00:0C:29:46:72:EB
(m) Cloned MAC:   --
(M) MTU:          auto
(A) Auto connect: yes
(a) Addresses
(r) Routes
(d) DNS
(q) back
  
```

```

Routes
-----
Destination  Next hop  Metric
-----
0/0
           use arrow keys for selection

(a) Add route
(d) Remove selected route
(r) Default IPv4 gateway: --
(R) Default IPv6 gateway: --
(4) IPv4 Never use this connection for default route: no
(6) IPv6 Never use this connection for default route: no
(q) back
  
```

2. Select option **r** (Default IPv4 gateway) and enter your default gateway address (No subnet mask or CIDR needed).

Note: *The connection must be active before you do this (refer to step 6 in Configure Interface Connections).*

3. Select option **q** (back) and proceed further.

6.4 Configure DNS Servers

You must configure DNS to ensure that HIAB can communicate with our servers and resolve any host names (OUTSCAN for HIAB external).

1. From the Ethernet connection screen, select option **d** (DNS)

```
Ethernet connection
-----
(n) Name:          Wired connection 1
(D) Device:       eth0
    MAC:          00:0C:29:46:72:EB
(m) Cloned MAC:   --
(M) MTU:         auto
(A) Auto connect: yes
(a) Addresses
(r) Routes
(d) DNS
(q) back
```

```
DNS
-----
DNS server
-----
0/0 use arrow keys for selection

(a) Add DNS server
(d) Remove selected DNS server
(4) IPv4 Search domain:
(6) IPv6 Search domain:
(q) back
```

2. Select option **a** (Add DNS Server) and enter your DNS server.
3. Repeat the previous step if there are more than one DNS server (secondary and tertiary).

6.5 Toggle Interface

All necessary networking configurations are now complete. You should toggle the network interface for the changes to take effect.



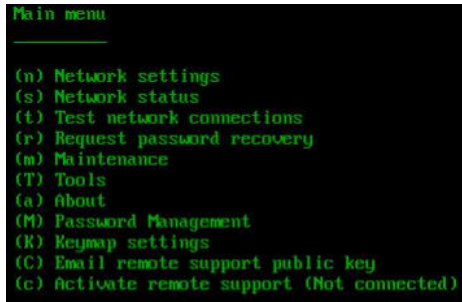
```

Network settings
-----
(d) Devices
(c) Connections
(p) Proxy settings
(n) NTP settings
(s) SMTP settings
(w) Configure UI management interface
(b) Bandwidth limiting
(r) Remove network configurations
(q) back

Devices
-----
Device  Type      State      Connection      MAC
-----  -
> eth0   ethernet  connected  Wired connection 1  00:0C:29:
1/1
      use arrow keys for selection

(c) Connect selected device
(d) Disconnect selected device
(b) Blink selected device LED
(q) back
  
```

1. Return to the main HIAB Network Settings menu.



```

Main menu
-----
(n) Network settings
(s) Network status
(t) Test network connections
(r) Request password recovery
(m) Maintenance
(T) Tools
(a) About
(M) Password Management
(R) Keymap settings
(C) Email remote support public key
(c) activate remote support (Not connected)
  
```

2. Select option **d** (Devices).
3. Select option **d** (Disconnect selected device).
4. Select option **c** (Connect selected device).
5. Select option **q** (back) twice to return to the main HIAB menu.
6. Proceed further.

6.6 Test Network Connections

Next, you must ensure that all network configurations are working as expected and pass the network tests.

```
Main menu
-----
(n) Network settings
(s) Network status
(t) Test network connections
(r) Request password recovery
(m) Maintenance
(T) Tools
(a) About
(M) Password Management
(K) Keymap settings
(C) Email remote support public key
(c) Activate remote support (Not connected)
```

```
Network tests
-----
(r) Run network tests
(d) Debug information
(q) back
```

From the main menu, you need to do the following:

1. Select option t (Test network connections).
2. Select option r (Run network tests).
3. Your network test should look like the below figure:

```
Run network tests
-----
Testing...

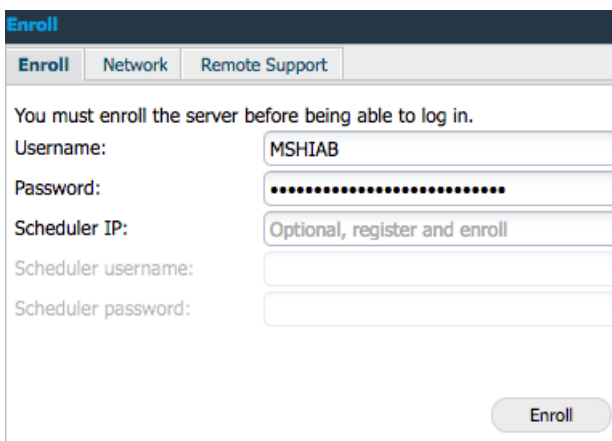
SUCCESS!DNS lookup (looking up www.outpost24.com)
SUCCESS!Update repositories
NO CONF!SMTP Relay server
INFORM.!NTP Reach: 16/16 Fail: 0 False-tick: 0 Variable: 0
FAILURE!Remote support (91.216.32.136:22 - SBC client failed to start)
SUCCESS!Outscan
[press any key to continue]
```

Troubleshooting

- ▶ If you see **Remote Support Failure**, you may need to reboot the machine for the client to initiate properly.
- ▶ If there are other **Failures**, review the configurations to ensure they are correctly setup as previously described.
- ▶ It is recommended to review your firewall rules to ensure they match the ones previously mentioned.
- ▶ If all else fails, ask **Support** to investigate the setup for you.

7 Enroll 64-Bit HIAB

1. To **Enroll**, navigate to the IP address of the HIAB you have just configured (**https://<HIAB IP>**).
2. Enter the main account credentials for the account you are registering the HIAB against.

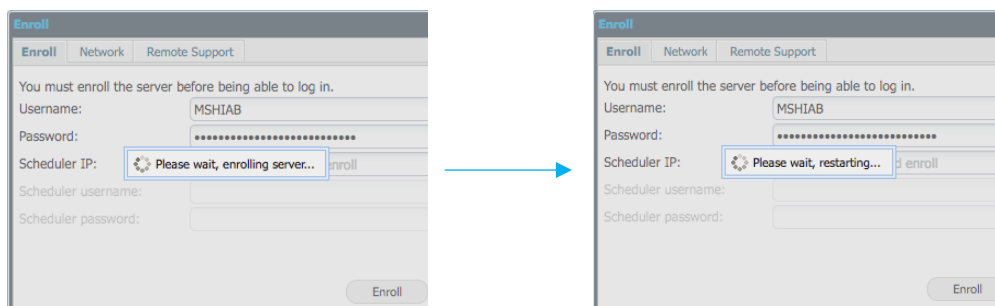


The screenshot shows the 'Enroll' form with the following fields and values:

- Username:** MSHIAB
- Password:** [Redacted]
- Scheduler IP:** Optional, register and enroll
- Scheduler username:** [Empty]
- Scheduler password:** [Empty]

An 'Enroll' button is located at the bottom right of the form.

3. Click **Enroll**. The HIAB will go through two stages within the enrolment process.



It can as well display another stage **Please wait, checking license...** depending on how long the enrollment procedure takes.

4. If any issues arise, please contact Outpost24 Support and enable remote support on the management console whilst providing them with the remote SSH key.
5. Once restarted, you can log in to the HIAB with the main account credentials you previously enrolled the appliance with.
6. Go to **Menu → Settings → Account → License** and confirm if you have the same number of IPs and scans as in your old HIAB.

Important Note

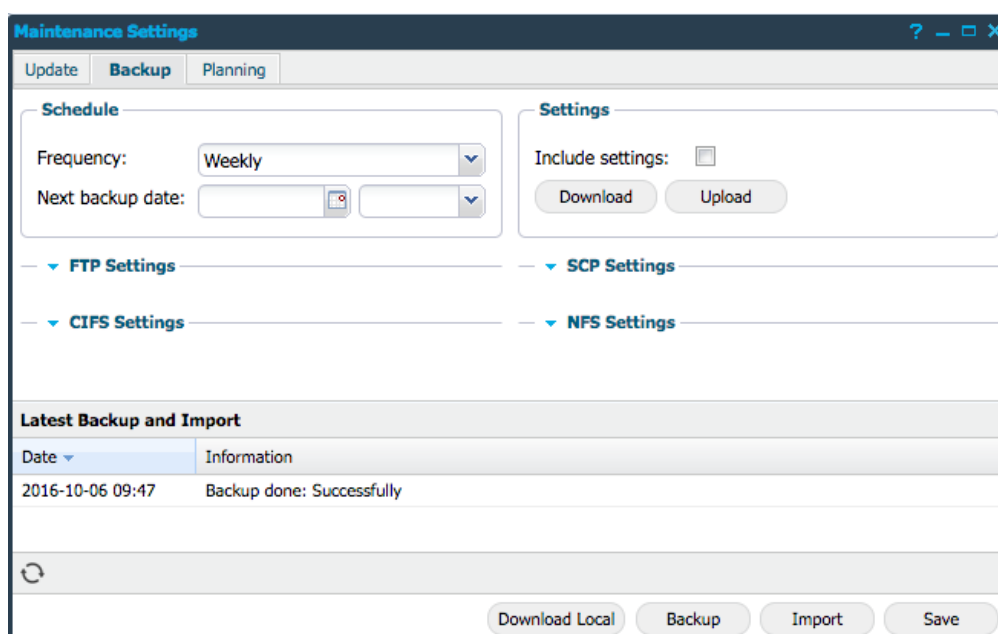
Prior to enrolment, ensure there is nothing in your network that will modify the packets being sent to the external enrolment and update servers (Deep packet inspection and SSL inspection). If so, please ensure these are bypassed to prevent enrolment errors.

8 Restore Backup

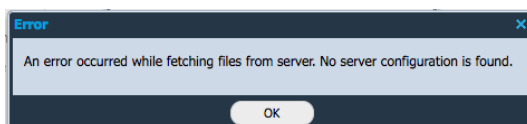
To restore the HIAB appliance from a backup, navigate to the following location in HIAB. Go to **Menu → Settings → Maintenance → Backup**

Note: *The maintenance portal is where you manage updates and backups for the HIAB itself.*

HIABs can be restored from FTP, SCP, CIFS, or NFS servers. You will need to reconfigure these settings if you wish to use this method. Alternatively, you can upload a local backup from your local machine.



1. Click on **Import**. If you receive the below error, do not worry. You have simply not configured your server information to restore the backup from. If you are restoring from a local file, select **OK** and move on to the next step.



2. For network-based backups, select your backup file and click **Import**.
3. For local based backups, choose **Upload local** select the file you wish to restore from and click **Upload**.



4. Select **Yes** on any pop-up stating all data will be replaced after the restore.

You can refresh the **Latest Backup and Import** section to see when your backup has completed.

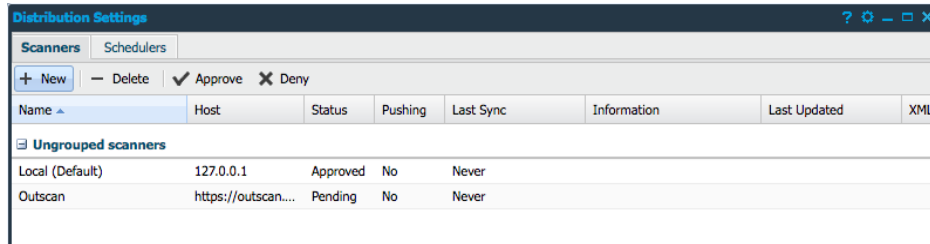
Note: *If you refresh and see Server not responding, then the backup will be completed, and you can refresh the entire page.*

9 Update Distribution Settings

Updating distribution settings is only applicable to those environments where distributed deployments are in place.

9.1 Confirm Distributed Configurations

1. Once the **Backup** has completed, navigate to **Menu** → **Settings** → **Distribution** to see the distribution settings.
2. If any devices other than OUTSCAN and Local are already present, then please remove these and re-create the connections using the **+ New** button.



The screenshot shows the 'Distribution Settings' window with the 'Scanners' tab selected. The table below lists the current scanners.

Name	Host	Status	Pushing	Last Sync	Information	Last Updated	XML
Ungrouped scanners							
Local (Default)	127.0.0.1	Approved	No	Never			
Outscan	https://outscan...	Pending	No	Never			

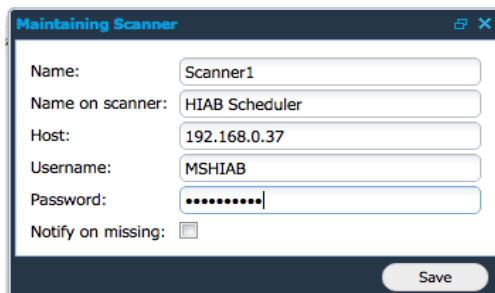
3. Later, re-add the scanner to the HIAB and make sure the targets are re-assigned to the correct scanner by following the same procedure. Additionally, verify that discovery scans are associated with correct scanner.

9.2 Connecting Scanners to Schedulers

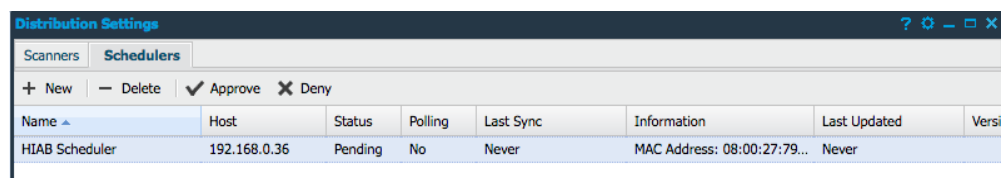
It is mandatory to ensure that firewall rules are in place to allow communication between the appliances, as defined previously. This includes preventing any form of Deep Packet Inspection, which can interfere with the SSL connection between the Schedulers and Scanners.

To begin the process, access to both appliances via the web browser is required.

1. Enter the HIAB Scanner Name, then the name of the HIAB Scheduler, the IP address of the scanner, and the main account credentials. Click **Save**.



2. Scheduler Approval:
 - a. Log into the Scanner you have just added to the scheduler. Navigate to the Distribution settings of the scanner.
 - b. Select **Schedulers** and approve the pending connection request from the HIAB Scheduler. Select and click **Approve**.



Name	Host	Status	Polling	Last Sync	Information	Last Updated	Version
HIAB Scheduler	192.168.0.36	Pending	No	Never	MAC Address: 08:00:27:79...	Never	

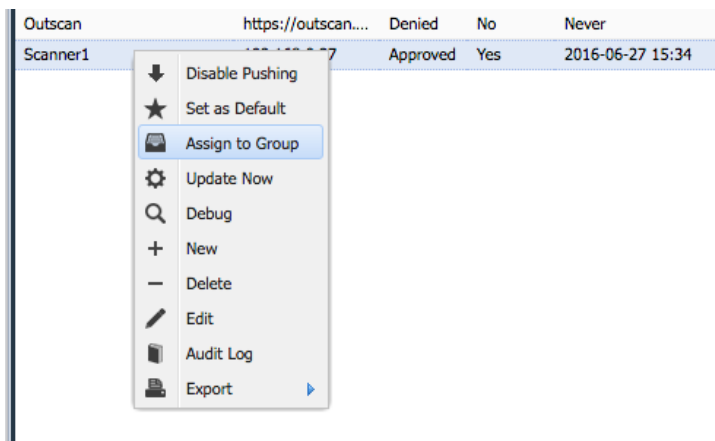
- c. This update the HIAB scheduler showing an approved connection on the HIAB.
3. You may need to refresh the distribution screen on the scheduler (or close and open the distribution screen). This updates the status to **Approved**.

Note: *The communication from the scheduler to the scanner may take some time.*

9.3 Grouping Scanners

Achievable within the **HIAB Scheduler** → **Distribution Settings**.

In the distribution settings, you can group scanners as a single entity for scanning purposes. This will enable the HIAB to distribute the scanning process evenly across several scanning appliances. This is beneficial for a more efficient scan and in some instances, reduces the overall scan window. To enable this feature, right click on a scanner and select **Assign to Group**.



Applying to scan schedule:

Within the **Scan schedule settings**, you can assign a scanner group within the *Discovery settings* tab.

10 Decommission 32-Bit HIAB

Do not delete or destroy data on the old HIABs until the new ones are up and running correctly.

1. Select a timeframe where no scans are scheduled, and no users will access the system.
2. Take the Scheduler offline.
3. Disconnect the HIAB devices from the network and turn off the HIABs.

Note: *Bootup the old HIAB if necessary.*