

HIAB Setup Guide

64-Bit

Table of Contents

1	GETTING STARTED	4
1.1	CHECKLIST.....	4
2	CONNECT THE APPLIANCE AND BOOT	5
2.1	THE MINI HIAB.....	5
2.2	1U RACK MOUNTABLE SERVER.....	5
2.3	A VIRTUAL IMAGE	5
3	SET UP THE IP ASSIGNMENT IN THE CONSOLE	6
3.1	STATIC IP.....	7
3.2	DHCP ASSIGNED IP FOR IPV4/IPV6.....	8
4	VERIFY THE REQUIRED COMMUNICATION SETTINGS	9
5	ENROLL THE SERVER	10
6	LOG ON TO THE PORTAL INTERFACE	11
7	CONFIGURE ADDITIONAL NETWORK SETTINGS	12
7.1	NTP SETTINGS.....	13
8	VERIFY TIME ZONE	14
9	SET UP AUTOMATIC UPDATES	15
10	CONFIGURE BACKUP	16
11	SET UP EVENTS AND NOTIFICATIONS	17

About This Guide

The main purpose of this document is to help you install and configure your HIAB appliance when setting it up for the first time in your organization's environment. This document has been elaborated under the assumption that the reader has access to the OUTSCAN account and HIAB license.

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

Copyright

© 2018 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®, OUTSCAN™, and HIAB™ are trademarks of Outpost24® in Sweden and other countries.

1 Getting Started

This guide will help you (the appliance administrator/network technician) to set up the HIAB appliance in your data center. Once the appliance is enrolled and configured to send out the alerts through the proper channels, then the vulnerability program should be implemented (not covered in this document).

1.1 Checklist

The below table displays the checklist for HIAB installation.

Number	Action
1	Connect the appliance and boot
2	Set up the IP assignment in the console
3	Verify the required communication settings
4	Enroll the server
5	Log on to the portal interface
6	Configure additional network settings
7	Verify time zone
8	Set up automatic updates
9	Configure backup
10	Set up events and notification

2 Connect the Appliance and Boot

The HIAB appliance is available as a mini HIAB, a 1U rack mountable server, or as a virtual image. During the installation, the HIAB requires a keyboard and screen to enable set up and registered to the correct account.

2.1 The Mini HIAB

1. Insert the batteries in the keyboard and remove the remote wireless receiver from underneath the keyboard and plug it into the appliance in a preferred USB port.
2. The mini HIAB has a DVI output and a converter to VGA should be included.
3. Connect the preferred cable type to a monitor. Insert a network cable and finally plug in the power adapter.
4. Once the HIAB displays a menu, proceed to the next step.

2.2 1U Rack Mountable Server

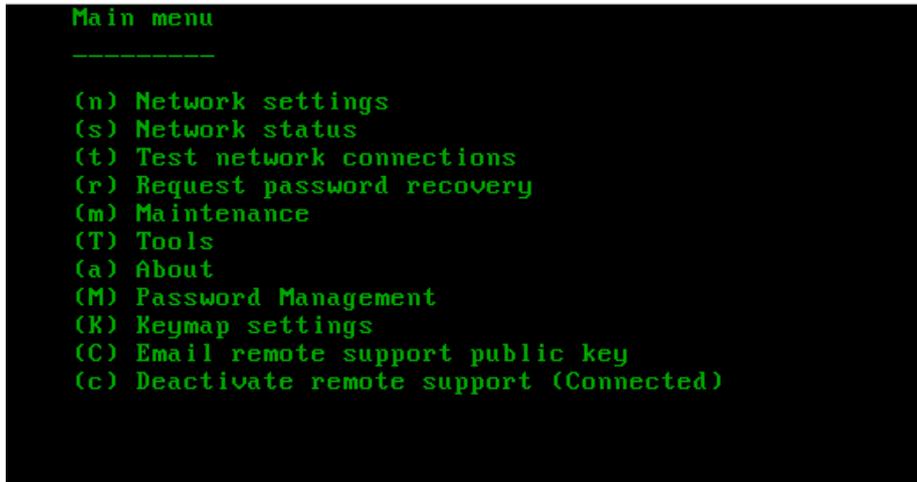
1. Insert the keyboard, VGA, network and power cable to the appliance and boot it.
2. Once the HIAB displays a menu, proceed to the next step.

2.3 A Virtual Image

1. Log in to **OUTSCAN** with the main user credentials.
2. Go to Menu → Support. → Virtual HIAB Appliance.
3. Once you click on **Download HIAB Virtual Image**, you will be presented with available options. Select an option that is most suitable for your virtual environment.
4. Select a location to store the downloaded **OVA file or Hyper-V image**.
5. Open your **administration tool** for the virtual environment.
6. Select the option to deploy a OVF, OVA or Hyper-V image file.
7. Follow the instructions in the application.
8. Start the virtual machine.

3 Set up the IP Assignment in the Console

Once the HIAB has booted (or if you connect to the appliance via SSH), you will see the following screen on your monitor.

A screenshot of a terminal window showing a green text menu on a black background. The menu is titled "Main menu" and lists several options with their corresponding first letters in parentheses: (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, and (c) Deactivate remote support (Connected).

```
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) Deactivate remote support (Connected)
```

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.

If you want to restrict the access, define a password.

1. Select option **M** in the above menu and provide a password.

Important Note

Do not forget this password or you may be locked out of the console and require remote access to reset the password.

3.1 Static IP

To set up the HIAB to use a static IP, you need to perform the following steps from the **main menu**:

1. Select option **n** to configure network settings

Network settings:

2. Select option **d (Devices)** to see to the available devices
 - a. Use the arrow keys to select the right device
 - b. Select the option **c** to connect the selected device
 - c. Select option **q** to go back to the network settings menu
3. Select option **c (Connections)** to go the connections window
 - a. Use the arrow keys to select the right connection
 - b. Select option **a** to activate the selected connection

Modify selected connection:

- c. Select option **m** to modify the selected connection
 - Select option **a (Addresses)** to go to the addresses window
 - Select either option **4** or **6** depending on which IP version you are utilizing
 - Type **manual** and press Enter
 - Select option **a** to **Add IP**
 - Enter the wanted IP address, for example 192.168.2.3/24 and press Enter.
Note: Specified in CIDR
- d. Select option **q** twice to go back to **Connections**
- e. Select option **d** and thereafter **a** to reactivate the interface

3.2 DHCP Assigned IP for IPv4/IPv6

To enable the server to be granted an IP address via DHCP, please perform the following steps from the **main menu**.

1. Select option **n** to configure network settings.
2. Select option **c (Connections)** from the network settings menu.
3. Use the arrow keys to select an interface which you wish to change.
4. Select option **m** to modify the selected connection.
5. Select option **a** to modify the addresses for the interface.
6. Select option **4 or 6** to set DHCP for an IPv4 or IPv6 address.
7. Type **auto** and press **Enter**.
8. Select option **q** twice to go back to **Connections**.
9. Select option **d** and thereafter **a** to reactivate the interface.

4 Verify the Required Communication Settings

During the installation, it is required that the HIAB is able to communicate with the following locations:

- ▶ Outbound to 91.216.32.141 over TCP port 443 (Enrollment server)
- ▶ Outbound to 91.216.32.142 over TCP port 443 and TCP port 5000 (Update server)

To verify if the HIAB is able to communicate with the above locations, please perform the following steps from the **main menu**.

1. Select option **t** to test network connections
2. Select option **r** to run network tests
3. Select option **q** to go back

Please refer to *HIAB 64-Bit Console Manual* for information regarding additional ports required for full functionality.

5 Enroll the Server

The HIAB needs to be registered to the correct account to be able to perform any scanning. Therefore, you need to pair it with the Main Account, this is done through an enrollment process.

You can enroll the appliance through console or portal interface.

If you are enrolling using console, you need to perform the following steps:

1. Select option **m** (Maintenance), from the main menu.
2. Select option **u** (Update).
3. Select option **e** to enroll.
4. Insert the user name for the HIAB license, which you have received in an email from Outpost24 and press **Enter**.
5. Type the password given in the email and press **Enter**.
6. Now the HIAB will connect to the update server and perform registration of the appliance.

If you are enrolling through portal interface, you need to perform the following steps:

1. Navigate to **https://<hiab-ip>**
2. Provide your details and click **Enroll**



You can also configure your **Network** settings and **Activate Remote Support**.

Note: It is the main account on the OUTSCAN system that should be used, so if you have downloaded the virtual appliance then it's the same details that should be used. Alternatively, any account with the "Allow enroll HIAB" option checked can be used to enroll the appliance.

6 Log on to the Portal Interface

Once you enroll the server, you should be able to see the below screen available at <https://<hiab-ip>>.

Example: If your assigned IP is 192.168.0.2, navigate to <https://192.168.0.2>

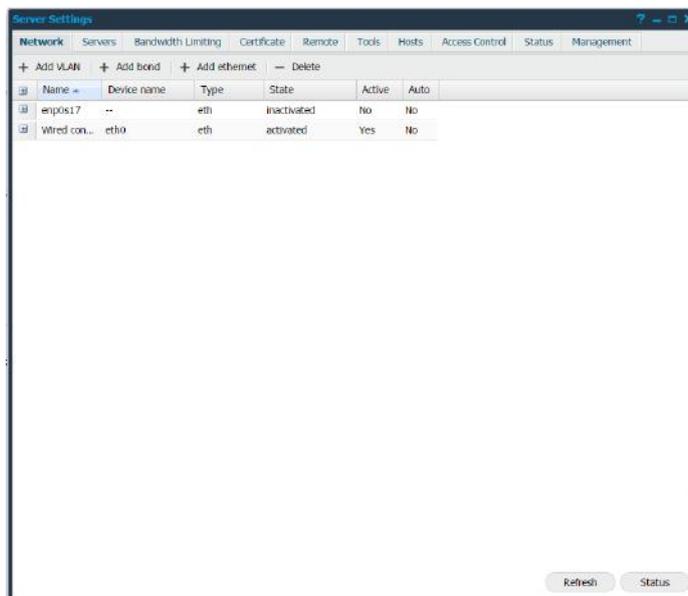


Log in using your credentials.

7 Configure Additional Network Settings

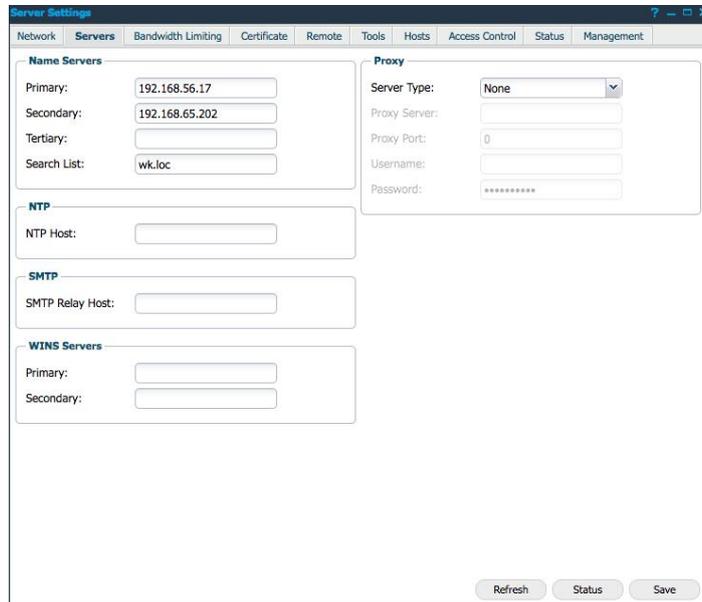
Once logged in, you will be able to set up any additional network interfaces and define any additional routes if required. This is much simpler from the portal interface than the console.

The network settings are available in the **Main Menu** → **Settings** → **Server**, under the **Network** tab.



7.1 NTP Settings

NTP settings can be configured in: **Main Menu → Settings → Server → Servers**



The screenshot displays the 'Server Settings' web interface. The 'Servers' tab is active, showing configuration options for Name Servers, NTP, SMTP, and WINS Servers. The 'Proxy' section is also visible on the right side of the interface.

Section	Field	Value
Name Servers	Primary:	192.168.56.17
	Secondary:	192.168.65.202
	Tertiary:	
	Search List:	wk.loc
NTP	NTP Host:	
SMTP	SMTP Relay Host:	
WINS Servers	Primary:	
	Secondary:	
Proxy	Server Type:	None
	Proxy Server:	
	Proxy Port:	0
	Password:	*****

Buttons at the bottom: Refresh, Status, Save

8 Verify Time Zone

All references to time can be modified to reflect the time in the current time zone. Click on the time section of the window (highlighted in the below figure) to modify the time zone offset from GMT.



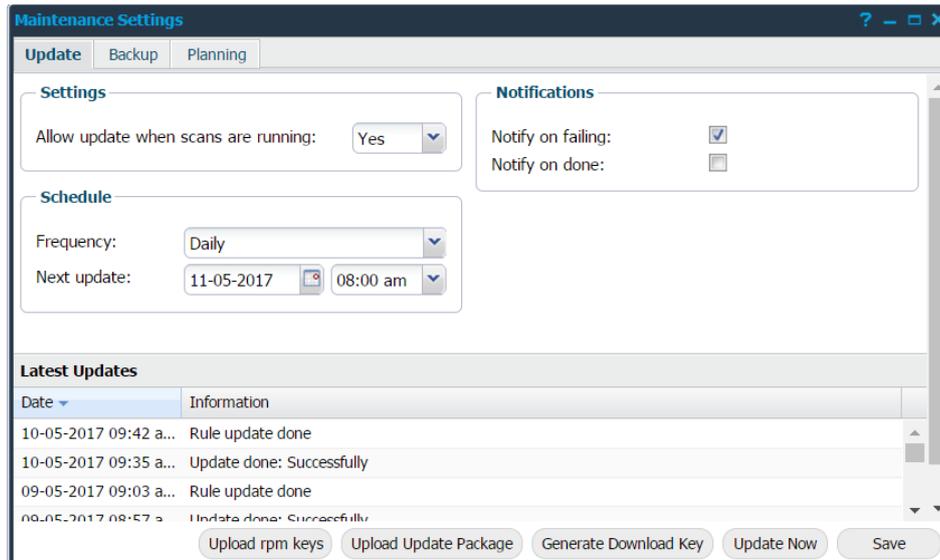
You can also change the date and time format and what is considered the first day of the week.



9 Set up Automatic Updates

Before you start using your appliance, it is a good idea to set up automatic updates. This will enable you to always receive the latest vulnerability tests and provide you with new features as they become available.

To schedule your updates, go to **Main Menu → Settings → Maintenance**, select the **Update** tab.

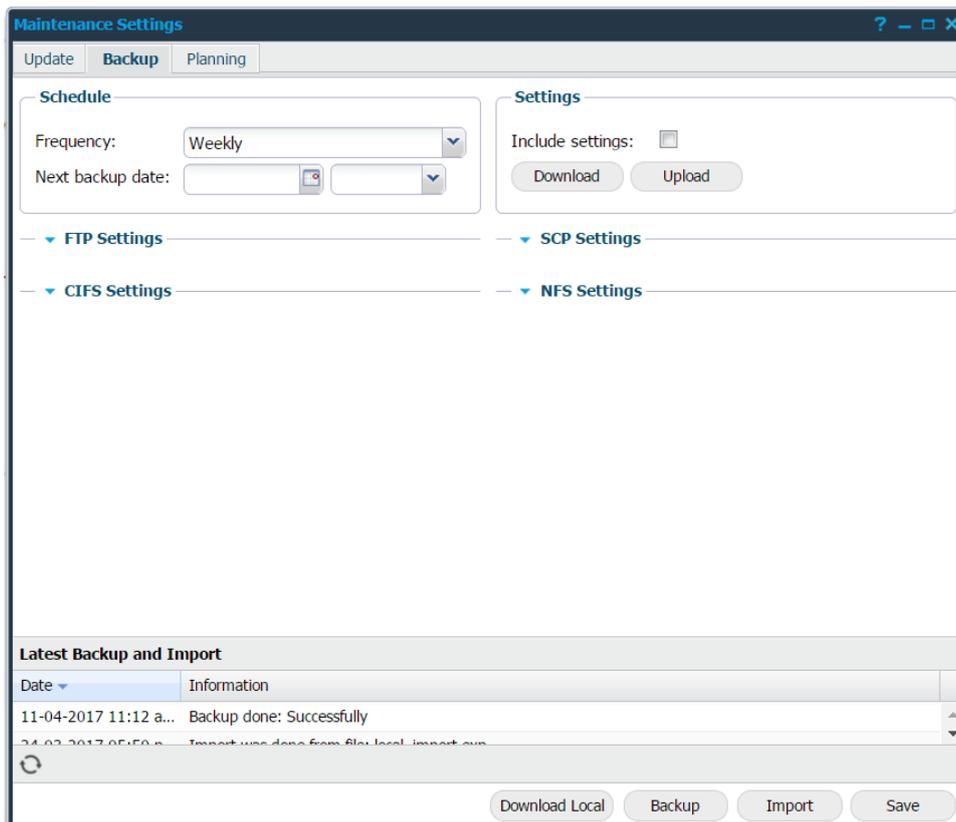


Here you can define if the updates are allowed to terminate any running scans (they will be resumed afterwards if they are still within their scanning window).

Select the frequency for the update and provide a start time, then click **Save** to save the current settings.

10 Configure Backup

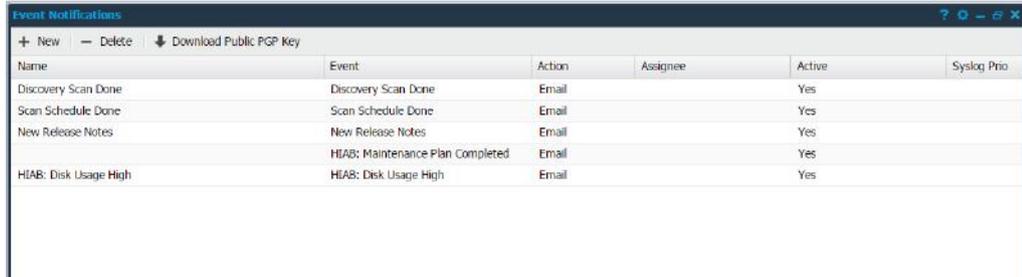
The HIAB can be set up to perform regular backups and transfer them over various protocols to a remote location for safekeeping. To configure these settings, go to **Main Menu → Settings → Maintenance**, select the **Backup** tab.



Please refer to *HIAB Maintenance Settings* guide for detailed information about Update and Backup.

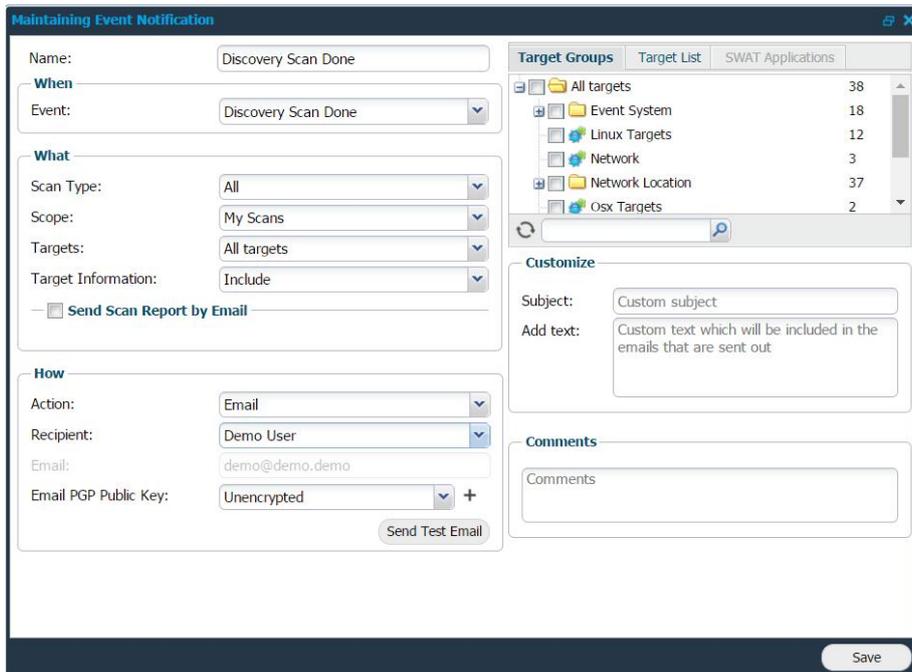
11 Set up Events and Notifications

The HIAB can send you the notifications either through email, Syslog or SNMP traps. The supported events that can be defined are located under **Main Menu → Settings → Event notifications**.



Name	Event	Action	Assignee	Active	Syslog Prio
Discovery Scan Done	Discovery Scan Done	Email		Yes	
Scan Schedule Done	Scan Schedule Done	Email		Yes	
New Release Notes	New Release Notes	Email		Yes	
HIAB: Maintenance Plan Completed	HIAB: Maintenance Plan Completed	Email		Yes	
HIAB: Disk Usage High	HIAB: Disk Usage High	Email		Yes	

Click on **+ New** button, to add a new event to the system. Right click on any event and select **edit** to set the event notification.



Maintaining Event Notification

Name:

When

Event:

What

Scan Type:

Scope:

Targets:

Target Information:

Send Scan Report by Email

How

Action:

Recipient:

Email:

Email PGP Public Key:

Target Groups | Target List | SWAT Applications

- All targets: 38
- Event System: 18
- Linux Targets: 12
- Network: 3
- Network Location: 37
- Osx Targets: 2

Customize

Subject:

Add text:

Comments

Please click on ? (help button) on the top right corner of the window to know more details about the available options.