

HIAB Maintenance Settings

Table of Contents

| | | |
|----------|--|----------|
| 1 | MAINTENANCE SETTINGS | 4 |
| 1.1 | UPDATE..... | 5 |
| 1.1.1 | <i>Update HIAB Without Internet Access</i> | 8 |
| 1.2 | BACKUP..... | 9 |
| 1.3 | PLANNING | 15 |

About This Guide

The purpose of this document is to provide users with a comprehensive overview of the Maintenance Settings for HIAB. This document has been elaborated under the assumption that the reader has access to the HIAB Account and Portal Interface.

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.

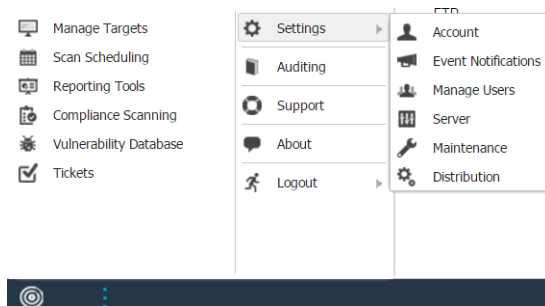
Trademark

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

1 Maintenance Settings

This feature enables you to manage updates, setup the HIAB backup correctly within your organization's environment and to plan automated removal of old vulnerability data.

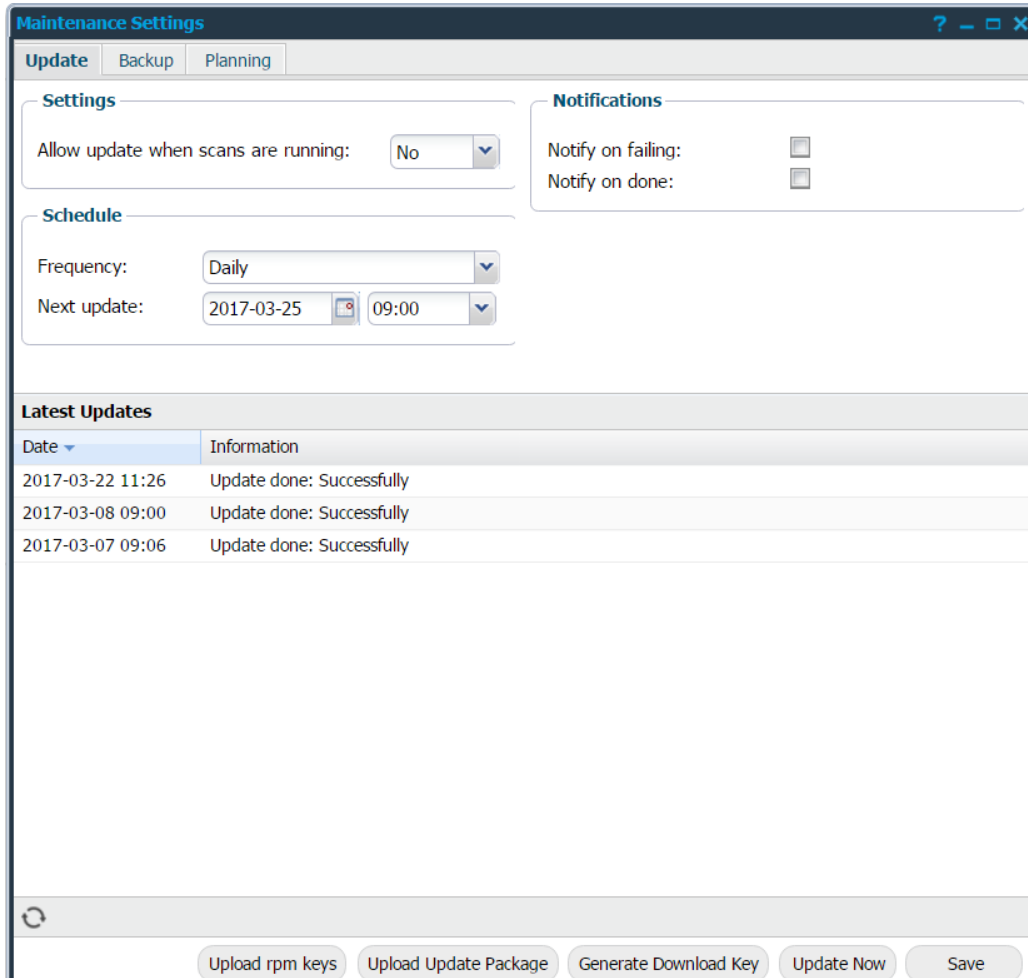
Once logged in, click the **Main Menu** button in the lower left corner and select **Maintenance**.



Note: Available in HIAB only.

1.1 Update

The **Update** tab allows you to schedule regular updates of the HIAB software and the vulnerability findings.



The screenshot shows the 'Update' tab in the Maintenance Settings window. It features three sub-sections: 'Settings', 'Schedule', and 'Notifications'. The 'Settings' section has a dropdown for 'Allow update when scans are running' set to 'No'. The 'Schedule' section has a dropdown for 'Frequency' set to 'Daily' and a date/time picker for 'Next update' set to '2017-03-25 09:00'. The 'Notifications' section has two checkboxes for 'Notify on failing' and 'Notify on done', both of which are unchecked. Below these sections is a 'Latest Updates' table with columns for 'Date' and 'Information'. The table contains three rows of update records, all showing 'Update done: Successfully'. At the bottom of the window, there are five buttons: 'Upload rpm keys', 'Upload Update Package', 'Generate Download Key', 'Update Now', and 'Save'.

| Date | Information |
|------------------|---------------------------|
| 2017-03-22 11:26 | Update done: Successfully |
| 2017-03-08 09:00 | Update done: Successfully |
| 2017-03-07 09:06 | Update done: Successfully |

The tab consists of four sections:

- ▶ Settings
- ▶ Schedule
- ▶ Notifications
- ▶ Latest Updates

Settings

Settings allows/prohibits updating when scans are running.

Schedule

Schedule allows you to schedule the updates on a regular basis. Here you can specify the frequency, date and time of the next update.

Notifications

The *Notifications* section allows you to define if you would like to be notified regarding update failures and/or success.

| Options | Description |
|--------------------------|---|
| Notify on failing | Enable/disable notifications on failed updates. |
| Notify on done | Enable/disable notifications on successful updates. |

Latest Updates

The *Latest Updates* grid displays the status of the latest updates performed. This grid is configurable, by clicking the arrow next to the name of any grid column allows you to customize which columns that will be shown out of the following:

| Option | Description |
|--------------------|------------------------------------|
| Date | Date when the update was performed |
| Information | Status of the update |

At the bottom of the window, five options are available:

- ▶ Upload rpm keys
- ▶ Upload Update Package
- ▶ Generate Download Key
- ▶ Update Now
- ▶ Save

| Option | Description |
|------------------------------|--|
| Upload rpm keys | This functionality is available only upon request. Please contact our support team in case of need. |
| Upload Update Package | Used together with Generate Download Key. It is used to upload an update package for HIAB when the HIAB does not have any internet access. |
| Generate Download Key | It is used to generate a download key. It is most commonly used together with Upload Update Package. |
| Update Now | Will initiate an update immediately. |
| Save | Saves the current settings in the system. |

Important Note: *The Update Package is bound to the generated key, in other words, it can only be uploaded on the specific HIAB on which the key was generated. Similarly, the key is bound to the HIAB on which it was generated.*

1.1.1 Update HIAB Without Internet Access

Follow the steps below to update your HIAB without internet access.

1. Click the **Generate Download Key** button. A key is displayed in a new window.

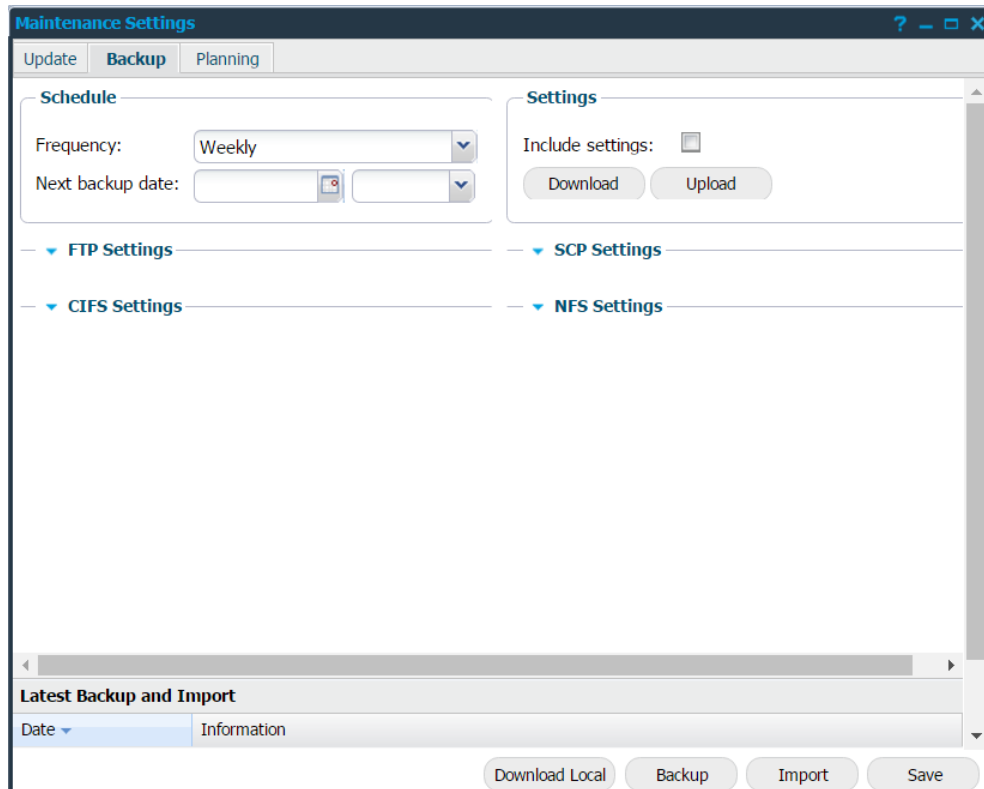


2. Copy the entire text into the **HIAB Update Package** tab under **OUTSCAN/Support**, and click on the **Download Update Package** button at the left bottom of the window.
3. This downloaded package can be uploaded using the above described **Upload Update Package** option.

1.2 Backup

Note: Only available on HIAB scheduler.

The **Backup** tab allows you to schedule regular backups of the HIAB data and upload them to defined servers.



The **Backup** tab consists of six sections.

- ▶ Schedule
- ▶ Settings
- ▶ FTP Settings
- ▶ SCP Settings
- ▶ CIFS Settings
- ▶ NFS Settings
- ▶ Latest Backup and Import

At the bottom of the window, four options are available:

- ▶ **Download Local:** You can download a backup file locally, which will be available once a backup has been performed.
- ▶ **Backup:** Force an instant backup of the HIAB data. The backup is uploaded to the configured file server. Priority for file servers is from high to low, i.e. FTP, SCP, CIFS, NFS.
- ▶ **Import:** Clicking on import opens a popup with list of files in the given setting of the first file server if configured any (FTP, SCP, CIFS, NFS). You can select a file and click on import button or click on upload local button which allows to import the local backup.

Note: The current data will be removed and replaced with the content from the imported file

- ▶ **Save:** Saves the current settings in the system.

Schedule

The *Schedule* section allows you to schedule your backup on a regular basis. You can specify the frequency, date, and time of the backup.

Settings

| Option | Description |
|-------------------------|--|
| Include Settings | Include Network and Host Settings in the backup. |
| Download | Download the Network and Host Settings. |
| Upload | Supply a configuration file, which will update the settings accordingly. |

FTP Settings

In the *FTP settings* section you can setup the FTP server credentials. In the Connect method drop down you can select if you would like to connect using regular FTP, FTPS, Implicit FTPS or SFTP (SSH FTP).

- ▲ **FTP Settings**

Host:

Port:

Username:

Password:

Connect Method: ▼

Passive Mode:

Directory:

Name Prefix:

| Option | Description |
|-----------------------|---|
| Host | Define the FTP host. |
| Port | Define the port in use. |
| Username | Define the username for authentication against the server. |
| Password | Define the password for authentication against the server. |
| Connect Method | Select if you would like to connect using regular FTP, FTPS, Implicit FTPS, or SFTP (SSH FTP). |
| Passive Mode | Enable/disable passive mode. When enabled, the FTP server should listen to another port than the standard FTP data port while transferring the files. |
| Directory | Used if you want to switch to another working directory after the authentication against the target. |
| Name Prefix | Given text string will be added as a prefix to the filename. |

SCP Settings

In the *SCP settings* section you can setup the SCP server credentials. The Private Key setting allows you to supply a private key to be used while authenticating.

— ▲ **SCP Settings** —

| | |
|--------------|--|
| Host: | <input type="text"/> |
| Port: | <input type="text" value="22"/> |
| Username: | <input type="text" value="hiab_backup"/> |
| Password: | <input type="password"/> |
| Private Key: | <input type="text"/> ▼ + |
| Directory: | <input type="text" value="/backup"/> |
| Name Prefix: | <input type="text" value="hiab"/> |

| Option | Description |
|--------------------|--|
| Host | Define the SCP host. |
| Port | Define the port in use. |
| Username | Define the username for authentication against the server. |
| Password | Define the password for authentication against the server. |
| Private Key | Supply a private key to be used while authenticating. |
| Directory | Used if you want to switch to another working directory after the authentication against the target. |
| Name Prefix | Given text string will be added as a prefix to the filename. |

CIFS Settings

In the *CIFS Settings* section you can set up the CIFS server credentials.

– ▲ **CIFS Settings**

| | |
|--------------|--|
| Host: | <input type="text"/> |
| Username: | <input type="text"/> |
| Password: | <input type="password"/> |
| Directory: | <input type="text" value="Ex. for Windows: /C\$/sharefolder"/> |
| Name Prefix: | <input type="text"/> |

| Option | Description |
|--------------------|--|
| Host | Define the CIFS host. |
| Username | Define the username for authentication against the server. |
| Password | Define the password for authentication against the server. |
| Directory | Used if you want to switch to another working directory after the authentication against the target. |
| Name Prefix | Given text string will be added as a prefix to the filename. |

NFS Settings

In the *NFS Settings* section you can set up the NFS server credentials.

▲ NFS Settings

Host:

Port:

Use Lock:

Directory:

Name Prefix:

| Option | Description |
|--------------------|--|
| Host | Define the NFS host. |
| Port | Define the port in use. |
| Use Lock | Disable/enable file locking. This setting is occasionally required when you are connecting to older NFS servers. |
| Directory | Used if you want to switch to another working directory after the authentication against the target. |
| Name Prefix | Given text string will be added as a prefix to the filename. |

Latest Backup and Import Grid

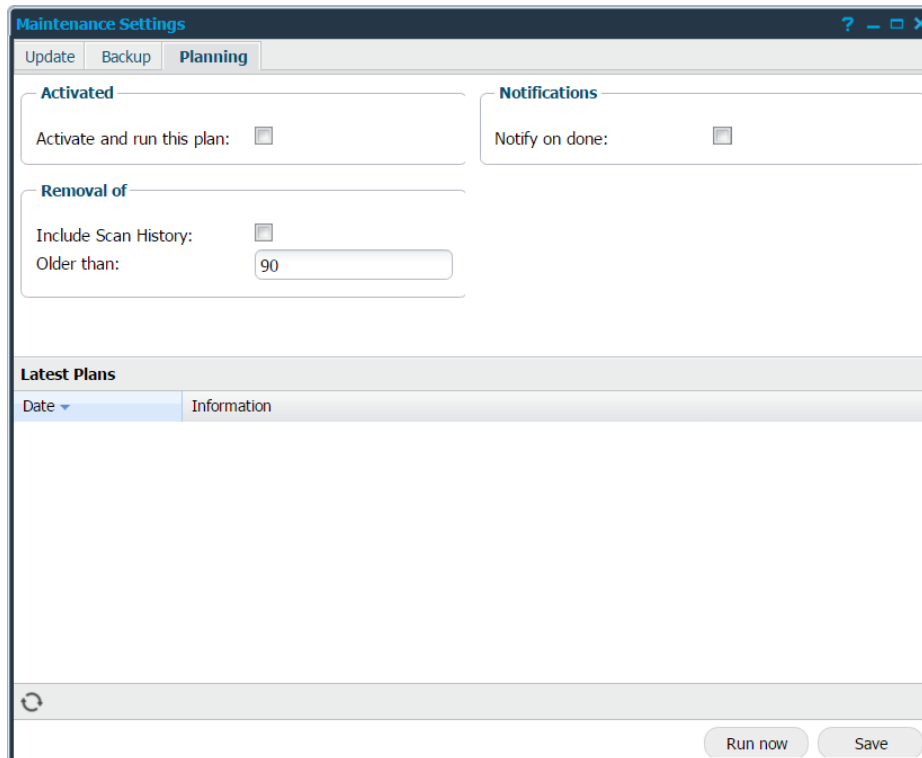
The *Latest Backup and Import* grid displays the backup history. This grid is configurable, by clicking the arrow next to the name of any grid column allows you to customize which columns that will be shown.

| Option | Description |
|--------------------|------------------------------------|
| Date | Date when the backup was performed |
| Information | Status of the backup or import |

1.3 Planning

Note: Only available on HIAB scheduler.

The **Planning** tab allows you to automatically remove any old vulnerability data that matches the given criteria daily.



There are four sections of the **Planning** tab:

- ▶ Activated
- ▶ Notifications
- ▶ Removal of
- ▶ Latest Plans

At the bottom of the window, two options are available:

Run now: Click on Run now to execute the plan immediately

Save: Saves the current settings in the system

Activated

The **Activated** section determines if removal of old data should be performed everyday.

Notifications

The **Notifications** section enable if you wish to receive an email once this has been performed.

Removal of

The **Removal of** section allows you to remove old scan data.

| Option | Description |
|-----------------------------|--|
| Include Scan History | Select to include removal of scan history details. This will remove all trace of the scan that took place. |
| Older than | Removes scan data which is older than the given number of days |

Latest Plans

The **Latest Plans** grid displays the latest plan executed. This grid is configurable, clicking the arrow next to the name of any grid allows you to customize which columns should be displayed.

| Option | Description |
|--------------------|---|
| Date | Date when the plan was executed |
| Information | Any additional information of the executed plan |