Central Management 7.4.0
# Table of Contents

## About This Guide

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Quick Start with OPSWAT Central Management</td>
<td>8</td>
</tr>
<tr>
<td>1.1. Installation</td>
<td>8</td>
</tr>
<tr>
<td>Installation steps</td>
<td>8</td>
</tr>
<tr>
<td>1.2. Configuration wizard</td>
<td>9</td>
</tr>
<tr>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td>1.3. License Activation</td>
<td>12</td>
</tr>
<tr>
<td>2. Installing or Upgrading OPSWAT Central Management</td>
<td>13</td>
</tr>
<tr>
<td>2.1. Recommended System Requirements</td>
<td>13</td>
</tr>
<tr>
<td>Operating System</td>
<td>13</td>
</tr>
<tr>
<td>Minimum Hardware Requirement</td>
<td>14</td>
</tr>
<tr>
<td>Software Requirement</td>
<td>14</td>
</tr>
<tr>
<td>Hardware sizing</td>
<td>14</td>
</tr>
<tr>
<td>Directory</td>
<td>15</td>
</tr>
<tr>
<td>Ports used</td>
<td>15</td>
</tr>
<tr>
<td>Browser Requirement</td>
<td>16</td>
</tr>
<tr>
<td>2.2. Installing OPSWAT Central Management</td>
<td>16</td>
</tr>
<tr>
<td>Installation steps:</td>
<td>16</td>
</tr>
<tr>
<td>2.2.1 On Windows</td>
<td>17</td>
</tr>
<tr>
<td>2.2.2. On Red Hat Enterprise Linux</td>
<td>20</td>
</tr>
<tr>
<td>2.3. Upgrading OPSWAT Central Management</td>
<td>21</td>
</tr>
<tr>
<td>Upgrade OPSWAT Central Management</td>
<td>21</td>
</tr>
<tr>
<td>Update OPSWAT Clients</td>
<td>22</td>
</tr>
<tr>
<td>2.4. OPSWAT Central Management licensing</td>
<td>24</td>
</tr>
<tr>
<td>2.4.1. Activating license</td>
<td>24</td>
</tr>
<tr>
<td>2.4.2. Checking OPSWAT Central Management license</td>
<td>30</td>
</tr>
<tr>
<td>2.5. Uninstall OPSWAT Central Management</td>
<td>31</td>
</tr>
<tr>
<td>Windows:</td>
<td>31</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux:</td>
<td>32</td>
</tr>
</tbody>
</table>
3. Configure OPSWAT Products

3.1. Devices
   
   Overview
   Introduction
   3.1.1 Device Groups
   3.1.2. Device Policies
   3.1.3. Distribute OPSWAT Client to devices
   3.1.4. Devices Inventory
   3.1.5. Enable OPSWAT Client's auto-update feature

3.2. Managing MetaDefender Kiosk
   
   3.2.1. Adding an existing MetaDefender Kiosk instance
   3.2.2. Deleting/Remotely Restarting an existing MetaDefender Kiosk instance
   3.2.3. Managing MetaDefender Kiosk License
   3.2.4. Changing MetaDefender Kiosk Configuration

3.3. Managing MetaDefender Core
    
   3.3.1. Adding an existing MetaDefender Core instance
   3.3.2. Deleting an existing MetaDefender Core instance
   3.3.3. Managing MetaDefender Core License
   3.3.4. Changing MetaDefender Core Configuration
   3.3.5. Module Updater
   3.3.6 Processing History

3.4. Managing MetaDefender Vault
     
   3.4.1. Adding an existing MetaDefender Vault instance
   3.4.2. Deleting an existing MetaDefender Vault instance
   3.4.3. Managing MetaDefender Vault License
   3.4.4. Changing MetaDefender Vault Configuration

3.5. Import and Export data
    
   3.5.1. Importing from URL
   3.5.2. Exporting to file
   3.5.3. Importing from file

3.6. Remote Install OPSWAT Products
     
   System requirements on an OPSWAT Products' host machine:

3.7. Managing OPSWAT Product Sets and Groups
     
   3.7.1. Set Management
6. Troubleshooting

6.1. The management console hung at the loading step 176
6.2. Unable to connect to the target machine during remote installation 178
6.3. Failed to re-install OPSWAT Central Management 179
6.4. Failed to start OPSWAT Central Management service through the tray icon 182
6.5. Failed to remote install OPSWAT Products 183
6.6. OPSWAT Client failed to report to OPSWAT Central Management server 185
6.7. OPSWAT Central Management failed to start with memcached/mongod shells hanging in the foreground 187
6.8 Managed devices are unable to report to OPSWAT Central Management 191

7. Knowledge Base Articles

OPSWAT Client 193
   How do I know which version of OPSWAT Client is installed on a device? 193
   How do I retrieve the OPSWAT Client logs? 197
   What are the system requirements for OPSWAT Client? 200
   Which versions of OPSWAT Central Management v7 are compatible with OPSWAT Client? 201

User and Account Settings 202
   How can I provision users from our own single sign-on service to OPSWAT Central Management? 203
   How do I add additional users to manage my account? 204
   How do I add or change my PIN? 205
   Is there a way to change a User’s role? 208

Which versions of OPSWAT Products are compatible with OPSWAT Central Management v7? 208
   Metadefender Products 209

Notes: 210
8. Legal  

Copyright  
  DISCLAIMER OF WARRANTY  
  COPYRIGHT NOTICE  

MetaDefender Export Classification
About This Guide

Welcome to the OPSWAT Central Management v7.x guide. This guide is intended to provide the information you need to:

- Install, configure, and manage OPSWAT Central Management v7.x.
- Learn about new features, updated features, and bug fixes on each OPSWAT Central Management releases
- Learn about frequently asked questions and our library of knowledge base articles

While we offer the option to download this guide to a PDF file, it is optimized for online browser viewing. OPSWAT updates the online version of the guide regularly on an "as needed" basis. By viewing the document online, you are assured that you are always seeing the latest version of the guide.
1. Quick Start with OPSWAT Central Management

This section covers basic steps to install OPSWAT Central Management:

- Installation
- Configuration wizard
- License Activation

1.1. Installation

Before starting OPSWAT Central Management (OCM) installation, please make sure your server meets the minimum hardware and software requirements.

Installation steps

1. Download the **OPSWAT Central Management** package from the [OPSWAT Portal](#) to your server.

2. Install the product by executing the installer file downloaded from the [OPSWAT Portal](#).

3. After installation finished, you can access the OPSWAT Central Management console via the OPSWAT Central Management shortcut created during installation on the desktop or at the address `http://<your_server_address>:8018`

4. A configuration wizard will be prompted and walk you through the basic setup of OPSWAT Central Management.
For more information on the installation procedure, see Installing OPSWAT Central Management.

1.2. Configuration wizard

Introduction

On the first time, you access the OPSWAT Central Management Console, you are requested to complete a basic configuration wizard before using the product. The console will be available only after you have successfully finished this wizard.
To get-started, click on CONTINUE.

⚠️ **Sensitive information**

The wizard may transfer sensitive information over an unencrypted connection. Always use this wizard on a secure, closed network or localhost, and with care!

Basic configuration steps

**Admin User Setup**

The next step is to set up an administrator account. This account is the first one allowed to access the Web Management Console and is used to create accounts for other users. You have to fill all the fields in this step before continuing. When you are done, click NEXT to continue.

The following information is required for the administrator account:

| EMAIL | The unique email of the account used at the time of login and in log messages for accountability. |
### DISPLAY NAME

The name of the person bound to this account. This name (appended to the name of the account's user directory) is displayed in the top right corner of the Web Management Console.

### PASSWORD

The password of the user bound to this account, used at the time of login.

⚠️ Password is sent in plaintext.

---

**Admin User Setup**

- **Display Name**
  - Enter display name

- **Email**
  - Enter email

- **Password**
  - Enter password

- **Confirm Password**
  - Re-enter password

---

**Server Settings Setup**

For server settings setup, see 4.1 Setting up domain.

**Product Activation**

For product activation details, see 2.4.1. Activating licenses.

**Import Data**

For data import details, see 3.5.3 Importing from file.
Wizard Completed

After you have completed every step, click the **FINISH** button to complete the wizard. The product's services will be restarted and your browser will be redirected to the web management console. This can take several seconds. If the console doesn't show up, please check out our troubleshooting KB to check the issue.

You can log into the console with the administrator account that has just been created in the previous steps.

![Wizard Completed](image)

1.3. License Activation

To activate your instance, navigate to the **Settings -> License** in the Web Management Console. If you have no valid license, you will only see your installation's Deployment ID.

Click on the **ACTIVATE** button to bring up the **Activation** menu, where you should choose from the available options:

- **Online Activation**: The server will make a request to the OPSWAT license server for a license with your Activation key and Deployment ID.
- **Offline Activation**: You can upload a manually acquired license file from **OPSWAT Portal**.
- **Request Trial Key**: If you don't have any activation key and you would like to evaluate Device Management feature, you can request a trial key via email.
2. Installing or Upgrading OPSWAT Central Management

This section describes the installation and upgrade processes of OPSWAT Central Management in details.

- Recommended System Requirements
- Installing OPSWAT Central Management
- Upgrading OPSWAT Central Management
- OPSWAT Central Management licensing
- Uninstall OPSWAT Central Management

2.1. Recommended System Requirements

- Operating System
- Minimum Hardware Requirement
- Software Requirement
- Hardware sizing
- Directory
- Ports used
- Browser Requirement

Your server must meet the following requirements before installing OPSWAT Central Management.

**Operating System**

⚠️ Only support 64-bit platforms.

<table>
<thead>
<tr>
<th>OS family</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows</td>
<td>10</td>
</tr>
<tr>
<td>Microsoft Windows Server</td>
<td>2012+</td>
</tr>
<tr>
<td></td>
<td>• 2012 required Microsoft updates KB2999226</td>
</tr>
</tbody>
</table>

"Only support 64-bit platforms."
### Minimum Hardware Requirement

<table>
<thead>
<tr>
<th>RAM</th>
<th>16 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1 CPU (4 cores)</td>
</tr>
<tr>
<td>Hard disk</td>
<td>20 GB + ~500MB * [number of managed scan engines]</td>
</tr>
<tr>
<td>Available ports</td>
<td>9000, 9001, 9005, 9009, 27017</td>
</tr>
</tbody>
</table>

### Software Requirement

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Powershell (Windows only)</td>
<td>5.1+</td>
</tr>
<tr>
<td>Java Runtime Environment (JRE)</td>
<td>version 8 update 171, 64-bit</td>
</tr>
</tbody>
</table>

### Hardware sizing

The following table shows the configuration of the server that installs OPSWAT Central Management.

<table>
<thead>
<tr>
<th>Number of devices</th>
<th>Up to 5,000</th>
<th>5,000 to 20,000</th>
<th>20,000 to 40,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1 CPU (4 cores)</td>
<td>1 CPU (8 cores)</td>
<td>1 CPU (16 cores)</td>
</tr>
<tr>
<td>RAM</td>
<td>16 GB</td>
<td>16 GB</td>
<td>32 GB</td>
</tr>
<tr>
<td>Hard disk capacity</td>
<td>60 GB + ~500MB * [number of managed scan engines]</td>
<td>100 GB + ~500MB * [number of managed scan engines]</td>
<td>200 GB + ~500MB * [number of managed scan engines]</td>
</tr>
</tbody>
</table>
Directory
This section contains references to directories used by OPSWAT Central Management.

Windows:

<table>
<thead>
<tr>
<th>Directory/folder</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>C:\Program Files\OPSWAT\Central</td>
</tr>
<tr>
<td>Event log files</td>
<td>C:\Program Files\OPSWAT\Central \tomcat\logs</td>
</tr>
<tr>
<td>Data backup</td>
<td>C:\ProgramData\OPSWAT\Central</td>
</tr>
</tbody>
</table>

Red Hat Enterprise Linux:

<table>
<thead>
<tr>
<th>Directory/folder</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>/opt/ocm</td>
</tr>
<tr>
<td>Event log files</td>
<td>/var/log/ocm</td>
</tr>
<tr>
<td>Configuration</td>
<td>/etc/opt/ocm</td>
</tr>
<tr>
<td>Database</td>
<td>/var/lib/ocm</td>
</tr>
</tbody>
</table>

Ports used
The following table shows the port configuration of OPSWAT Central Management. The listed ports must be available to start OPSWAT Central Management.

<table>
<thead>
<tr>
<th>Component / Service</th>
<th>Port</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Management</td>
<td>Web Management Console and REST interface</td>
<td>9000, 9001</td>
</tr>
<tr>
<td></td>
<td>Customizable; adjust accordingly if modified.</td>
<td></td>
</tr>
<tr>
<td>MongoDB</td>
<td>Database of OPSWAT Central Management</td>
<td>27017</td>
</tr>
<tr>
<td>Memcached</td>
<td>Caching data</td>
<td>9005</td>
</tr>
</tbody>
</table>
### Browser Requirement

One of the following desktop browsers is required to use the web management console:

- Latest two Chrome versions
- Latest two Firefox versions
- Latest two Microsoft Edge versions

OPSWAT Central Management supports HTTPS configuration on all the aforementioned browsers. Please refer to [4.2. Enabling HTTPS](#) for more details.

Mobile layouts are not supported yet.

### 2.2. Installing OPSWAT Central Management

Before starting OPSWAT Central Management (OCM) installation, please make sure your server meets the [hardware and software system requirements](#).

**Installation steps:**

1. Download the **OPSWAT Central Management** package from the [OPSWAT Portal](#) to your server. Make sure that you download an applicable package for your server operating system (and distribution).

2. Install the package on your computer:
   
   a. **On Windows**
   
   b. **On Red Hat Enterprise Linux**

3. After installation finished, you can access the OPSWAT Central Management console via two methods.
   
   a. Use the OPSWAT Central Management shortcut that was created during installation on the desktop.
   
   b. Open a web browser and point to `<server name or IP>:<port>`, which is the address of your server:
      
      e.g., [http://localhost:9000](http://localhost:9000)

4. Complete the required steps of the **basic configuration wizard**,
5. You must activate this deployment to use its full features.

2.2.1 On Windows

- Installing OPSWAT Central Management using command line
- Installing OPSWAT Central Management using the installation wizard

2.2.1.1. Installing OPSWAT Central Management using command line

On Windows systems, it is possible to silently install the product by calling the corresponding .msi file from the command-line interface.

From the command-line interface, execute the command:

```msiexec /i <.msi file> /quiet```

For example:

```
msiexec /i C:\OPSWATCentralManagement.msi /quiet
```

Administrator permission is required for this command.

Alternatively, to start a GUI-assisted installation process - as in Installing OPSWAT Central Management using the installation wizard, execute the command:

```msiexec /i <.msi file>```

For example:

```
msiexec /i C:\OPSWATCentralManagement.msi
```

Windows Installer provides specific arguments for the installation/uninstallation process using a .msi file.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/i</td>
<td>Install</td>
</tr>
<tr>
<td>/x</td>
<td>Uninstall</td>
</tr>
<tr>
<td>/quiet</td>
<td>Quiet display option. The installer runs without displaying a user interface.</td>
</tr>
</tbody>
</table>
### Argument Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/l*v &lt;output file path&gt;</td>
<td>Log the install/uninstall process and output it to a specific filepath, for example, /l*v C:\log\log.txt</td>
</tr>
</tbody>
</table>

### 2.2.1.2. Installing OPSWAT Central Management using the installation wizard

The installation wizard is available for Windows installations only (.msi file).

Executing the following steps:

1. Accept the license agreement.
2. Installation in progress. The process may take some time.

3. Click **Finish** to complete installation. You can check **Launch OPSWAT Central Management** to launch the web management console immediately. If this is the first time you install OPSWAT Central Management, the **Configuration wizard** will walk you through the initial setup.
After a successful installation, OPSWAT Central Management tray icon shows status of the instance.

2.2.2. On Red Hat Enterprise Linux

On Red Hat Enterprise Linux system, please follow the below steps to install the OPSWAT Central Management package.

1. Open the terminal.
2. Setup a valid JRE_HOME or JAVA_HOME environment variable in the file /etc/bashrc.
3. Enter the command (requires sudo privilege):

```
sudo yum install <path to .rpm file>
```
For systems which enabled GPD check flag:

```
sudo yum install --nogpdcheck <path to .rpm file>
```

4. Start OPSWAT Central Central Management via the command (requires sudo privilege):

```
sudo systemctl start ocm
```

In case of startup problems, please refer to the startup log in /var/log/ocm or systemd log.

2.3. Upgrading OPSWAT Central Management

**Upgrade OPSWAT Central Management**

In order to perform an upgrade to a newer version of OPSWAT Central Management, please first uninstall the program via Windows’s Add or Remove Programs tool then follow the steps in [Installing OPSWAT Central Management using command line](#) or [Installing OPSWAT Central Management using the installation wizard](#) with a new installation package to upgrade the product.

All existing OPSWAT Central Management configuration and data will be kept during the upgrade.

Uninstalling OPSWAT Central Management will not cause any data or settings loss including files, configuration, and license. If you want to perform a clean uninstall and reinstall, please refer to [Clean uninstall of OPSWAT Central Management](#).
Update OPSWAT Clients

You can configure how OPSWAT Central Management should update OPSWAT Clients under Settings > Server Configuration > Update Settings.

OPSWAT Central Management supports 3 ways to upgrade OPSWAT Clients. Whenever you upgrade OPSWAT Client packages on OPSWAT Central Management, clients on endpoints will upgrade to the new version itself without extra action from administrators/end-users if Allow Client to automatically update to the latest version setting is enabled at Settings > Global Settings > Device Agent

- **Internet:** OPSWAT Central Management auto-looks for a new version of clients from OPSWAT Clients hosting server and upgrade OPSWAT Client packages to a new version if available
  - Requirement: OCM should have a connection to the below URLs. If OCM servers sit behind a firewall or a proxy, you need to whitelist domains.
    - http://agent-update.opswat.com
    - https://mem-onpremise.s3.amazonaws.com

- **Folder:** OPSWAT Central Management auto-looks for a new version of clients from a configured folder and upgrade OPSWAT Client packages to a new version if available. You can follow the below steps to perform an upgrade
  - Download desired OPSWAT Client packages from OPSWAT Portal > Products > Endpoint Clients manually. You need to download both the agent package and agent descriptor package
    - For example, you would like to upgrade Windows persistent client to version 7.6.248, you have to download both 7.6.248 (Persistent agent) and 7.6.248 (Persistent Agent Descriptor) packages
Copy them to the configured folder.

**Manually**: Administrators manually upload OPSWAT Client packages to OPSWAT Central Management. Here are steps you can follow:

- Download desired OPSWAT Client packages from **OPSWAT Portal > Products > Endpoint Clients** manually. You need to download both the agent package and agent descriptor package.
  - For example, you would like to upgrade Windows persistent client to version 7.6.248, you have to download both 7.6.248 (Persistent agent) and 7.6.248 (Persistent Agent Descriptor) packages.
Upload an OPSWAT Client package to OPSWAT Central Management console for an appropriated agent

2.4. OPSWAT Central Management licensing

By default, OPSWAT Central Management can manage up to 500 instances of each OPSWAT Products. To manage devices, OPSWAT Central Management requires users to acquire a valid license and activate it.

- Activating licenses
- Checking OPSWAT Central Management license

2.4.1. Activating license

This section covers how to activate your OPSWAT Central Management server.

- Initial Steps
- Offline Activation
Initial Steps

1. To activate your product, go to the **Settings > License** menu in the Web Management Console.

![License Console](image)

2. Click the **Activate** button to bring up the **Activation** dialog, where you can activate the product from available options and follow steps according an option you choose:

   - **Online Activation**: The product will contact the OPSWAT license portal to activate itself based on your **Activation key** and its **Deployment ID**.

   - **Offline Activation**: You can upload a license file generated from your **Activation key** and the product's **Deployment ID**, which can be downloaded from OPSWAT Portal.

![OPSWhatsApp Central Management Activation](image)
For a successful activation, a valid activation key is required regardless of what option is chosen.

Online Activation

To activate the product with this option, the below requirement must be met:

- The server has an Internet connection and can connect to OPSWAT License portal (https://activation.dl.opswat.com/)
- You have a valid activation key for OPSWAT Central Management

With a Internet connection, OPSWAT Central Management can be activated directly using the Activation key received upon purchasing the product or requested a trial key. Perform the following steps for an online activation:

1. In the Activation dialog, choose Online Activation.

2. Fill the Activation Key field with your key.

3. Fill the “Describe This Deployment” text box.

4. Click the ACTIVATE button to activate.

If your license is valid, the product shall be activated with number of device limit as you purchased. Otherwise, you will get an error message.
Offline Activation

You can activate the product with this option if you have a valid activation key. The Deployment ID of the OPSWAT Central Management instance and the Activation key received upon purchasing the product or a trial key.

Please follow the steps detailed below to acquire the activation file containing the unlock key required for offline activation.

2. Select OPSWAT Central Management for the field MetaDefender Package.
3. Fill in the requested information about your deployment.
4. Click the **Request Unlock Key** button. The **Download Unlock Key** link appears.
5. Click the **Download Unlock Key** link and save the activation file.
6. Go back to Offline Activation in OPSWAT Central Management console. Browse for the activation file and click the **ACTIVATE** button.

![Offline Activation](image)

If you have activated your installation, but your license then becomes invalid or expired, you will see an error message.

2.4.2. Checking OPSWAT Central Management license

**License information**

Basic license information is always visible in the lower left side of the console interface. The following information is available:

- Product version

**License menu**

For more license details on **activating** your installation, go to **Settings > License** menu on the Web Management Console.

The following information is available, listed according to the types of products that are being monitored:
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment ID</td>
<td>Identification of this installation</td>
</tr>
<tr>
<td>Monitored</td>
<td>The number of devices or OPSWAT Products managed by the current OPSWAT Central Management instance.</td>
</tr>
<tr>
<td>Limit</td>
<td>The maximum number of devices and OPSWAT Products allowed by the license registered to the current OPSWAT Central Management instance.</td>
</tr>
</tbody>
</table>

2.5. Uninstall OPSWAT Central Management

**Windows:**

On Windows, OPSWAT Central Management can be removed through the Add or Remove Programs tool or through the command prompt.

**Option 1: Use Add or Remove Programs tool**

1. Go to **Control Panel > Programs and Features** or **Add/Remove Programs** depending on your version of Windows.

2. Select **OPSWAT Central Management** and click Uninstall to start the uninstallation process.
Option 2: Use Command prompt

⚠️ While it is possible to uninstall the program from the same .msi package used for installation, please note that the procedure requires an elevated context (i.e. with administrative privilege), such as via an elevated command prompt.

1. Start command prompt **as administrator**.

2. From the command-line interface, execute the command:
   
   msiexec /x <msi file name>

   Or for silent uninstallation:
   
   msiexec /x <msi file name> /quiet

   Where <msi file name> should be the location of your msi package.

   For instance:

   ```
   msiexec /x C:\OPSWATCentralManagement.msi /quiet
   ```

**Red Hat Enterprise Linux:**

On Red Hat Enterprise Linux, OPSWAT Central Management can be removed through the terminal.

Enter the command (requires sudo privilege):

```sh
sudo yum remove ocm
```

**Clean Uninstallation:**

In case of a problem during the installation of a new version of OPSWAT Central Management, you can perform a clean uninstallation to completely remove all data related to OPSWAT Central Management and resolve any possible conflicts.

⚠️ Please note that clean uninstallation should only be performed at a last resort. The following instructions will result in the loss of all changes to your OPSWAT Central Management installation (persistent data from the current instance, stored files and custom configuration).
1. Uninstall OPSWAT Central Management via one of the methods described above.

2. Delete all OPSWAT Central Management directories (refer to 2.1. Recommended System Requirements for directories in use).
3. Configure OPSWAT Products

The following sections guide the OPSWAT Central Management's management features for OPSWAT products.

- Devices
- Managing MetaDefender Kiosk
- Managing MetaDefender Core
- Managing MetaDefender Vault
- Import
- Remote Install OPSWAT Products
- Managing OPSWAT Product Sets and Groups
- Managing Users and Active Directories
- Managing MetaDefender Email Gateway Security
- Managing MetaDefender ICAP Server
- Managing MetaDefender Drive

3.1. Devices

Overview

OPSWAT Central Management can manage devices that have installed the OPSWAT Client. OPSWAT Client is an endpoint client that leverages OPSWAT technologies to collect security & vulnerability information, detect threats, and protect endpoints from the threats that come from using removable media. It is lightweight and remains transparent to end-users while protecting and auditing any risky activities that could introduce threats to the organization. OPSWAT Client can be centrally managed by OPSWAT Central Management for policy control and reporting. For more information on OPSWAT Client, please refer to [OPSWAT Client](#).

Introduction

OPSWAT Central Management provides an extensive suite of features to manage your devices.

- Device Groups
- Device Policies
- Distribute OPSWAT Client to Devices
**Device Inventory**

### 3.1.1 Device Groups

OPSWAT Central Management allows administrators to manage devices by categorizing them into groups with different security levels. This will not only help administrators reduce the time spent in device management but also help ensure compliance by assigning different security requirements to a group.

#### Groups management page

The users can add new group via the **Add New Group** button, modify an existing group by clicking on the corresponding entry, or remove it via the corresponding delete icon.

#### Add new group

The users can add new device groups in the groups management page.

1. Click on **Add New Group**.

2. Fill out the required information and choose from the available customization options for the new device group. Click on **Assign Devices To Group** when ready.

- **Name, Description**: The group's name and description
- **Accessibility checkbox:** Choose if newly added devices should be assigned to this group automatically
- **Select existing policy:** Assign an existing policy to the group
- **Select existing package:** Assign an existing rebranding package to the group

3. Choose the devices that should be assigned under the new group. Click on **Create** when ready. Your new device group should now be displayed on the Groups management page.

### Update a group

1. From the Groups management page, click on the group you want to update.

2. You can choose to assign a new policy or rebranding package to the group in this page. Via the **Actions** drop-down menu, you can make changes to selected devices in the group.

   If you want to assign more devices to this group, click on **Add Devices To Group**.

3. Select the devices you wish to add and press **Add Devices To Group** to finalize your choice.
3.1.2. Device Policies

OPSWAT Central Management allows administrators to set different security requirements for different device groups.

To manage device policies, you can find all policies under your account by navigating to Device Policies.

Create a new policy

In case the administrators would like to create a new policy from an existing policy, they can clone an existing policy by clicking on the setting icon on the desired policy and Clone it. Otherwise, here are the steps to create a new policy with default settings.

1. Click on **Create New Policy**.
2. Fill out the required basic information for the new policy. Click on **Define Device Actions** when ready.

- **Name**: The new policy's name
- **Description**: The new policy's description
3. The **Define Device Actions** page allows administrators to customize the device’s security behaviors. Click on **Define Device Issues** when ready.

4. The **Define Device Issues** page specifies when a device should report a security issue for consideration. Click on **Define Device Status** when ready.
5. The **Define Device Status** page specifies the criteria to judge whether a device is compliant or non-compliant based on the security issues reported. Click on **Create** to finalize the new policy's creation, which will be displayed in the Policies management page.

3.1.3. **Distribute OPSWAT Client to devices**

OPSWAT Client can be deployed in many different ways. Here are the most common options.

**Install the agent manually on devices**

To install OPSWAT Client **directly** on a device:

1. Log into the management console
2. From **Dashboard > Overview** or **Inventory > Devices**, click **AddDevices**.
3. Click **Download OPSWAT Client for distribution**
4. **Download** either the installer or portable client as you wish and install or run the agent on devices.
The download link is shareable. You can send the download link to your users to download installers by themselves.

Distribute the agent through Active Directory:

1. Log into the management console
2. From Dashboard > Overview or Inventory > Devices, click AddDevices.
3. Click Download OPSWAT Client for distribution
4. Download the appropriate client (typically the MSI file).
5. Identify or create an accessible network share location.
6. Copy the MSI file to that location (do not change the file name).
7. Using Group Policy Manager, create a GPO with appropriate scope, and link it to an OU.
8. Create software installation for Computer Configuration and/or User Configuration. Provide the full UNC path to the .MSI file.
9. Enable and deploy the policy.

More information on how to use Active Directory to distribute OPSWAT Client: Can I use Active Directory to distribute, enforce or audit MetaAccess usage?
Other common techniques:

1. Add OPSWAT Client directly to your golden image for new systems.
2. Distribute OPSWAT Client with your software deployment or distribution tool.

More information on how to create a golden image containing OPSWAT Client: Can MetaAccess be distributed using a golden image, cloned VMs or AMIs?

If you have reached the limit of devices that can be monitored by your account (25 devices for free accounts), please contact sales to purchase additional devices.

3.1.4. Devices Inventory

OPSWAT Central Management offers visibility about endpoint security across the entire organization at **Inventory > Devices**.

The Device management page allows administrators to quickly apply actions to specific devices. Select devices you want to perform a specific action, then click **Action** to select an action.

- **Assign to Groups**: Assign the selected devices to an existing group. Please refer to **Device Groups** for more detail.
• **Scan Threats**: Perform a threat scan on the selected devices.

![Scan Threats interface]

• **Exempt/Unexempt**: Exempt for a specific amount of time or revoke an existing exemption for a device from the policy of the group they belong to (or the default policy for ungrouped devices). Please refer to **Device Policies** for more detail.

![Exempt/Unexempt interface]

• **Fetch log**: remotely fetch the OPSWAT Client's log. A fetch log command will be sent to an agent on selected devices to request the agent submit its log to the OCM when the devices connect to OCM. Administrators can download the log when the action is
• **Ignore**: This is applicable for unknown devices which has no OPSWAT Client installed. When an administrator reviews unknown devices, they can ignore an unknown device at their wish.

• **Undo Ignore**: This is applicable for ignored devices. When an administrator applies this action to ignored devices, those devices will be converted to Unknown status.

• **Re-identify**: Request users on selected devices to provide their information again. This is applicable if you enable Custom Information feature at **Settings > Global Settings > Advanced > Custom Information**.
• **Delete**: Remove devices from OPSWAT Central Management. By this action, the agent will be uninstalled on deleted devices when it connect to OPSWAT Central Management automatically.

3.1.5. **Enable OPSWAT Client's auto-update feature**

OPSWAT Client is capable of automatically updating to the latest version hosted on your OPSWAT Central Management server. To enable this feature, the administrator needs to enable the Client's auto-update feature in the OPSWAT Central Management console:

1. Log into OPSWAT Central Management console.
2. Navigate to **Settings > Global Settings**.
3. On the **Device Clients** tab, check on the **Allow Client to automatically update to the latest version** option as shown in the screenshot below.
4. Click the **Save** button.
3.2. Managing MetaDefender Kiosk

OPSWAT Central Management can not only manage MetaDefender Kiosk instance's setting but also install new MetaDefender Kiosk instances remotely.

- Adding an existing MetaDefender Kiosk instance
- Deleting/Remotely Restarting an existing MetaDefender Kiosk instance
- Managing MetaDefender Kiosk License
  - Online product activation
  - Offline product activation
- Changing MetaDefender Kiosk Configuration

3.2.1. Adding an existing MetaDefender Kiosk instance

The following guideline describes how to add an existing MetaDefender Kiosk instance to OPSWAT Central Management.

1. Go to the MetaDefender Kiosk management page under Inventory in the sidebar.
2. Click the **ADD KIOSK** button in the top right panel.

3. The dialog **Add Kiosk** will be opened. Select the **Add an existing Kiosk** button.

   **Add Kiosk**

   **Add an existing Kiosk**
   Import information about an existing kiosk to add it to your system

   **Remotely install a new Kiosk**
   Connect to a device and install your new Kiosk on it

4. Fill the proper inputs and click the **TEST CONNECTION** button to check the connection status.
3.2.2. Deleting/Remotely Restarting an existing MetaDefender Kiosk instance

The following guideline describes how to delete or remotely restart a MetaDefender Kiosk instance from the OPSWAT Central Management console. In the case of restarting, the machine running the Kiosk instance will be restarted.

1. Go to the MetaDefender Kiosk management page under Inventory in the sidebar.
2. Select the Kiosk instance that you want to delete or restart.

3. Click the ACTIONS drop-down menu and choose the Restart or Delete option. If Delete is chosen, your request is immediately processed.

4. If Restart is chosen, fill the proper inputs and click the RESTART button.
- **Username, Password:** The credential used to access the product, i.e. the account used to log into its host machine.

The dialog will be closed and the MetaDefender Kiosk management page will be reloaded automatically if the result is successful.

### 3.2.3. Managing MetaDefender Kiosk License

The following guideline describes how to activate or deactivate the license of a MetaDefender Kiosk instance remotely.

1. Go to the **MetaDefender Kiosk** management page under **Inventory** in the sidebar.

2. Select **License Information** for the Kiosk instance you wish to configure.
3. You can choose to remove or update the current license via the corresponding button. If **Remove License** is chosen, you are returned to the MetaDefender Kiosk management, which should update accordingly.
4. If **Update License** is chosen, the dialog **Kiosk Activation** will be opened. Please refer to the corresponding section for additional details.

- Online product activation
- Offline product activation

### 3.2.3.1. Online product activation

The following guideline describes how to activate the MetaDefender Kiosk license online.

1. Select the **Online Activation** option.
2. Enter the key.

3. The dialog will be closed and the Kiosk page will be reloaded automatically if the result is successful.

3.2.3.2. Offline product activation

The following guideline describes how to activate the MetaDefender Kiosk license offline.
1. Select the **Offline Activation** option.

2. The **Offline Activation** menu will be opened.
Offline Activation details

3. Fill in the requested information about your deployment.
MetaDefender Offline Activation

- **Activation Key**: The activation key of MetaDefender Kiosk that you have received.
- **Deployment ID**: The deployment ID shown in the previous section.
- **Optional description**: The description for this deployment.

4. Click the **Request Unlock Key** button. The **Download Unlock Key** link appears.
5. Click the **Download Unlock Key** link and save the activation file.

6. Go back to OPSWAT Central Management's Web Management Console. Browse for the activation file and click the **ACTIVATE** button.
7. The dialog will be closed and the Kiosk page will be reloaded automatically if the result is successful.

3.2.4. Changing MetaDefender Kiosk Configuration

The following guideline describes how to change the configuration of a MetaDefender Kiosk instance remotely.

1. Go to the **MetaDefender Kiosk** management page under **Inventory** in the sidebar.
2. Click the **Setting** button (from the gear icon) of the Kiosk instance you wish to configure.

3. **OPSWAT Central Management** will load the setting of the kiosk.

4. Change any settings and click **APPLY** button.
3.3. Managing MetaDefender Core

OPSWAT Central Management can not only manage MetaDefender Core instance's settings but also install MetaDefender Core instances remotely.

- Adding an existing MetaDefender Core instance
- Deleting an existing MetaDefender Core instance
- Managing MetaDefender Core License
  - Online product activation
  - Offline product activation
- Changing MetaDefender Core Configuration
  - Security zones
  - Workflow templates
  - Workflow rules
- Module Updater
  - Delivering module updates to MetaDefender Core instances
- Processing History

3.3.1. Adding an existing MetaDefender Core instance

The following guideline describes how to add an existing MetaDefender Core instance to OPSWAT Central Management.
1. Go to the MetaDefender Core management page under Inventory in the sidebar.

2. Click the ADD CORE button in the right top panel.

3. The dialog Add Core will be opened. Select the Add an existing Core button.

4. Fill the proper inputs. You can click the TEST CONNECTION button to check the connection status.
• **Name:** The name you want to assign to the new Core instance
• **API Key:** The API Key of the Core instance to authenticate the request
• **Server Address:** The address of the Core instance

5. The dialog will be closed and the Core page will be reloaded automatically if the result is successful.

The status of the Core is **Connected** after fetching the version of this Core successfully.

### 3.3.2. Deleting an existing MetaDefender Core instance

The following guideline describes how to delete a MetaDefender Core instance from OPSWAT Central Management.

1. Go to the **MetaDefender Core** management page under **Inventory** in the sidebar.
2. Select the Core instance that you want to delete.

3. Click the **ACTIONS** drop-down menu and choose the **Delete** option.

   ![ACTIONS menu]

   The dialog will be closed and the Core page will be reloaded automatically if the result is successful.

3.3.3. Managing MetaDefender Core License

The following guideline describes how to activate or deactivate the license of a MetaDefender Core instance remotely.

1. Go to the **MetaDefender Core** management page under **Inventory** in the sidebar.
2. Select License Information for the Core instance you wish to configure.

3. You can choose to remove or update the current license via the corresponding button. If Remove License is chosen, you are returned to the MetaDefender Core management page, which should update accordingly.
4. If **Update License** is chosen, the dialog **Core Activation** will be opened. Please refer to the corresponding section for additional details.

- Online product activation
- Offline product activation

### 3.3.3.1. Online product activation

The following guideline describes how to activate the MetaDefender Core license online.
1. Select the Online Activation option.

2. Enter the key.
3. The dialog will be closed and the Kiosk page will be reloaded automatically if the result is successful.

### 3.3.3.2. Offline product activation

The following guideline describes how to activate the MetaDefender Core license offline.

1. Select the **Offline Activation** option.

![Offline Activation Menu](image)

2. The **Offline Activation** menu will be opened.
 Offline Activation details

2. Select MetaDefender Core v4.x as MetaDefender Package.
3. Fill in the requested information about your deployment.
• **Activation Key**: The activation key of MetaDefender Core that you have received.

• **Requested Number of Nodes**: The number of MetaDefender Core nodes you wish to request.

• **Deployment ID**: The deployment ID shown in the previous section.

• **Optional description**: The description for this deployment.

4. Click the **Request Unlock Key** button. The **Download Unlock Key** link appears.
5. Click the **Download Unlock Key** link and save the activation file.

6. Go back to OPSWAT Central Management's Web Management Console. Browse for the activation file and click the **ACTIVATE** button.
7. The dialog will be closed and the Core page will be reloaded automatically if the result is success.

3.3.4. Changing MetaDefender Core Configuration

The following guideline describes how to change the configuration of a MetaDefender Core instance remotely.

1. Go to the MetaDefender Core management page under Inventory in the sidebar.
2. Click the **Setting** button (from the gear icon) of the Core instance you wish to configure.

3. OPSWAT Central Management will load the setting of the Core.

### 3.3.4.1. Security zones

The following guideline describes how to modify the Security Zone setting for MetaDefender Core.

- The **SECURITY ZONES** tab:

Add a new security zone

1. Click the **ADD NEW ZONE** button in the right top panel.
2. Fill the proper inputs and then click the SAVE button.

- **Zone Name**: The new zone's name.
- **Description**: The new zone's description
- **Networks**: The networks assigned to this security zone

3. The Security Zone management page will be reloaded automatically if the result is successful.

4. Click button **SAVE POLICY CHANGES**.

5. Show the message for saving the policy successfully.

**Modify the existing security zones**

1. Click each Security Zone record or the edit icon to modify zone and click **SAVE CHANGES** to save.
2. If you wish to delete a specific Security Zone, click the delete icon in the corresponding Security Zone record and click the **DELETE** button.

![Remove](image)

3. The Security Zone management page will be reloaded automatically if the result is successful.

![Security Zone Management](image)

### 3.3.4.2. Workflow templates

The following guideline describes how to modify the Workflow Templates setting for MetaDefender Core.

- The **WORKFLOW TEMPLATES** tab
Add a new workflow

1. Click **ADD NEW WORKFLOW** button in the right top panel.

2. Fill the proper inputs and then click the **SAVE** button.

   - **Workflow Name:** The new workflow's name
   - **Description:** The new workflow's description.

3. The Workflow Templates management page will be reloaded automatically if the result is successful.

4. Click button **SAVE POLICY CHANGES**.

5. A confirmation message is displayed.
Modify the existing workflow templates

1. Click each Workflow Templates record or the edit icon to modify the workflow and then click **SAVE CHANGES** to save.

2. If you wish to delete a specific workflow, click the delete icon in the corresponding Workflow Templates record and then click the **DELETE** button.

3. If you wish to clone a specific workflow, click the clone icon in the corresponding Workflow Templates record, give a new name to the new workflow and then click the **SAVE** button.
4. The Workflow Templates management page will be reloaded automatically if the result is successful.

![Workflow Templates Management](image)

3.3.4.3. Workflow rules

The following guideline describes how to modify the Workflow Rules setting for MetaDefender Core.

- The **WORKFLOW RULES** tab

![Workflow Rules Management](image)

Add a new rule

1. Click **ADD NEW RULE** button in the top right panel.
2. Fill the proper inputs and then click **SAVE** button.

   **Workflow Rules Management**

   **Add new Rule**

   - **Name**: The new rule's name
   - **Description**: The new rule's description
   - **Apply To Zone**: The zone that the new rule should apply to
   - **Use Workflow Template**: Make the new rule follow a preset template
   - **Use Certificate To Generate Batch Signature**: Choose if the new rule should be digitally signed
   - **Certificate Used For Batch Signing**: If the above option is selected, pick the certificate that should be used.

3. The Core page will be reloaded automatically if the result is successful.

4. Click the **SAVE POLICY CHANGES** button.

5. A confirmation message is displayed.
Modify the existing rules

1. Click each Workflow Rules record or the edit icon to modify zone and click SAVE CHANGES to save.

2. If you wish to delete a specific rule, click the delete icon in the corresponding Workflow Rules record and then click the DELETE button.

3. The Core page will be reloaded automatically if the result is successful.
3.3.5. Module Updater

Administrators can leverage OPSWAT Central Management to centralize management of modules for MetaDefender instances. OPSWAT Central Management downloads, stores, and distributes update packages to connected MetaDefender Core instances.

MetaDefender Core modules can be found at **Inventory > Modules.**

OPSWAT Central Management updates modules based on the modules available in all connected MetaDefender Core instances when the module update process happens.

During the update process, the module updater communicates with each MetaDefender Core instance to compile a complete list of modules. The updater then communicates with OPSWAT’s module update server to check if there are any updates available and downloads those updates to the OPSWAT Central Management. The updates are ready for distribution to the MetaDefender Core instances immediately. Please refer to **Delivering module updates to MetaDefender Core instances** to learn how to distribute updates to MetaDefender Core instances.

Administrators can determine what modules should be available in the update process by enabling modules from the Module inventory.
Administrators can update modules on-demand by clicking **UPDATE NOW** to trigger an update process and download module updates to OPSWAT Central Management. Beside that, administrator can schedule an update under **Settings > Server Configuration > Module Updater**

![Module Updater](image)

- To utilize the module updater, the MetaDefender Core instances must have their **Source** setting set to Internet in the **Update Settings** menu in the MetaDefender Core management console.

- Unused modules for more than 7 days (such as having been removed from the MetaDefender Core instances) will be removed from OPSWAT Central Management.

### 3.3.5.1. Delivering module updates to MetaDefender Core instances

The following guideline describes how to deliver module updates to MetaDefender Core instances.
1. In the MetaDefender Core management page, select the connected instances that need to be updated by ticking their checkboxes.

2. Select **Update Engine** from the **ACTIONS** drop-down menu.

3. In the **Update Engine** dialog, select the update method:

   - **Direct update from Central Management updater**: Update the MetaDefender Core instances with the module updates already downloaded to in OPSWAT Central Management. Please refer to [Module Updater](http://192.168.202.172:8000) for more details.

   - **Mediate update from MetaDefender Core server**: Manually upload the module updates that will be delivered to MetaDefender Core instances.

4. This step differs depending on the method chosen.
a. **Direct Update**: Enter the PIN and confirm the update process by selecting **UPDATE**.

![Direct Update](image)

The updating process will be triggered in background after pressing **UPDATE** button.

Enter your 4-digit PIN to update engine. If you have not yet set your PIN, please go to the account settings page to create your PIN.

b. **Mediate Update**:
i. Drag-and-drop or click on **Browse** to select the update files. Select **Next** to proceed to the next step.

**Mediate Update**

Confirm the instance(s) you want to update engine

- **Core172**

Drop here or **Browse** engine files and upload to MetaDefender Core server (zip or yml format)

**Mediate Update**

Confirm the instance(s) you want to update engine

- **Core172**

<table>
<thead>
<tr>
<th>ENGINE FILE</th>
<th>DESCRIPTOR</th>
<th>SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>7z_8_windows-d...</td>
<td>7z_8_windows-dat...</td>
<td>0.65 MB</td>
</tr>
</tbody>
</table>

Total size of engine files (0.65 MB) must be less than or equal 1536 MB

[BACK] [CANCEL] [BROWSE MORE FILE] [NEXT]
ii. Enter the PIN and confirm the update process by selecting UPDATE.

5. OPSWAT Central Management console will display a notification when the delivery process is complete.

For each updated module, the mediate update function requires both the actual update file (an archive file format such as .zip) and the update information file (.yml format).
The direct update function only works with MetaDefender Core instances from version 4.16.0.

For mediate update, there is a file size upload limit of 1536 MB and a timeout limit of 6 minutes.

3.3.6 Processing History

The Processing History page, located under the Events And History submenu, contains the scanning history of all MetaDefender Core instances under the management of OPSWAT Central Management.

Search criteria and filters can be applied to display only specific entries. The results can be exported to a .csv file via the EXPORT FILTERED RESULT button.
Administrators can also delete part or the entire history via the **CLEANUP** button.

**3.4. Managing MetaDefender Vault**

OPSWAT Central Management can not only manage MetaDefender Vault instance's setting but also install new MetaDefender Vault instances remotely.

- Adding an existing MetaDefender Vault
3.4.1. Adding an existing MetaDefender Vault instance

The following guideline describes how to add an existing MetaDefender Vault instance to OPSWAT Central Management.

1. Go to the **MetaDefender Vault** management page under **Inventory** in the sidebar.

![MetaDefender Vault management page](image)

2. Click the **ADD VAULT** button in the top right panel.

![ADD VAULT button](image)

3. The dialog **Add VAULT** will be opened and then select the **Add an existing Vault** button.
4. Fill the proper inputs and then click the **TEST CONNECTION** button to check the connection status.

- **Name**: The name you want to assign to the new Vault instance
- **API Key**: The API Key of the Vault instance to authenticate the request
- **Server Address**: The address of the Vault instance

5. The dialog will be closed and the Vault page will be reloaded automatically if the result is successful.
The status of the Vault is **Connected** after fetching the version of this Vault successfully.

### 3.4.2. Deleting an existing MetaDefender Vault instance

The following guideline describes how to delete a MetaDefender Vault instance from OPSWAT Central Management.

1. Go to the **MetaDefender Vault** management page under **Inventory** in the sidebar.

2. Select the Vault instance that you want to delete.

3. Click the **ACTION** drop-down menu and choose the **Delete** option.

The dialog will be closed and the Vault page will be reloaded automatically if the result is successful.

### 3.4.3. Managing MetaDefender Vault License

The following guideline describes how to activate or deactivate the license of a MetaDefender Vault instance remotely.
1. Go to the MetaDefender Vault management page under Inventory in the sidebar.

2. Select License Information for the vault you wish to configure.

3. If you want to activate a license, click the ADD LICENSE button and go the next step. If you want to deactivate a license, click the Activated switch to change it to Deactivated then close License Information dialog.
4. If **ADD LICENSE** is chosen, the dialog **Vault Activation** will be opened.

- Online product activation
- Offline product activation

### 3.4.3.1. Online product activation

The following guideline describes how to activate the MetaDefender Vault license online.
1. Select the **Online Activation** option.

2. Enter the key.

3. The dialog will be closed and the Vault page will be reloaded automatically if the result is successful.
3.4.3.2. Offline product activation

The following guideline describes how to activate the MetaDefender Vault license offline.

1. Select the **Offline Activation** option.

2. The **Offline Activation** menu will be opened.
Offline Activation details

2. Select MetaDefender Vault as MetaDefender Package.
3. Fill in the requested information about your deployment.
MetaDefender Offline Activation

- **Activation Key**: The activation key of MetaDefender Vault that you have received.
- **Deployment ID**: The deployment ID shown in the previous section.
- **Optional description**: The description for this deployment.

4. Click the **Request Unlock Key** button. The **Download Unlock Key** link appears.

5. Click the **Download Unlock Key** link and save the activation file.
6. Go back to OPSWAT Central Management's Web Management Console. Browse for the activation file and click the **ACTIVATE** button.

![Offline Activation](image-url)
7. The dialog will be closed and the Vault page will be reloaded automatically if the result is successful.

3.4.4. Changing MetaDefender Vault Configuration

The following guideline describes how to change the configuration of a MetaDefender Vault instance remotely.

1. Go to the MetaDefender Vault management page under Inventory in the sidebar.

   ![MetaDefender Vault Management Page](image)

2. Click the Setting button on the right.

   ![Setting Button](image)

3. OPSWAT Central Management will load the settings of the vault.

   ![Settings Page](image)

4. Change any settings and click the Submit button.
3.5. Import and Export data

OPSWAT Central Management supports data migration between OPSWAT Central Management instances via importing and exporting data in .json file format. The transferable data includes product instances, users and user directories. This feature is supported from OPSWAT Central Management version 7.2.0.

Additionally, all OPSWAT Central Management versions from 7.1.0 also support importing data from OPSWAT Central Management version 5.2.7+ via a given URL.

- Importing from URL
- Exporting to file
- Importing from file

3.5.1. Importing from URL

The following guideline describes how to import data from an older version of OPSWAT Central Management (from version 5.2.7) using its URL.

1. Navigate to the Import/Export page from the sidebar and select IMPORT FROM URL from the IMPORT/EXPORT drop-down menu.

2. Fill out the information and then click the IMPORT button.
2. Username, Password: The administrator credential used to access the older OPSWAT Central Management server

3. Central Management 5.x URL: The URL of the older OPSWAT Central Management server

3. The loading dialog will be opened.
4. The dialog will be closed and the Import/Export page will be reloaded automatically with updated Import History if the result is successful.

Multiple imports from the same server will only update new changes from the last import. If no change is detected for a specific section, the import history will display '0' in the corresponding column.

3.5.2. Exporting to file

The following guideline describes how to export OPSWAT Central Management's data to a .json file.

1. Navigate to the Import/Export page from the sidebar and select EXPORT TO FILE from the IMPORT/EXPORT drop-down menu.

2. Select EXPORT TO FILE in the next pop-up dialog.
3. Select which data to export by ticking their checkboxes. Select **NEXT** to confirm the selection.
4. Name the exported file, fill in the PIN and select **EXPORT** to start the export process.

5. The file will be downloaded by the browser.
Exporting user data requires also exporting the user directories data.

3.5.3. Importing from file

The following guideline describes how to import OPSWAT Central Management's data from a .json file.

1. Navigate to the Import/Export page from the sidebar and select IMPORT FROM FILE from the IMPORT/EXPORT drop-down menu.
2. Select the file to be imported via **Choose file**. Select **TEST** to check the validity of the chosen file and continue to the next step if the test is successful.

![Image of Import From File](image1.png)

3. Select the data that should be imported by ticking their checkboxes. Enter the PIN and select **IMPORT** to confirm the selection.

![Image of Import From File](image2.png)

- In the duplicated data warnings, the number in brackets is the number of duplicated instances.
4. The result dialog shows whether the data is imported successfully. Select **Finish** to complete the process.

**Import From File**

<table>
<thead>
<tr>
<th>SUCCESSFUL</th>
<th>FAILED</th>
</tr>
</thead>
<tbody>
<tr>
<td>METADEFENDER VAULT</td>
<td>1</td>
</tr>
<tr>
<td>METADEFENDER ICAP SERVER</td>
<td>1</td>
</tr>
<tr>
<td>USERS</td>
<td>9</td>
</tr>
<tr>
<td>USER DIRECTORIES</td>
<td>0</td>
</tr>
</tbody>
</table>

The web page will be refreshed after you click **Finish** and all data will be ready to use!

5. **Import History** will update with the result from the finished import process.

Import History only lists the data that was imported successfully in each import process.
Importing users data also requires importing user directories data.

3.6. Remote Install OPSWAT Products

Administrators can install OPSWAT products remotely through the OPSWAT Central Management console. The host machine for the OPSWAT Product must meet the system requirements and have OpenSSH Server enabled.

**System requirements on an OPSWAT Products’ host machine:**

- Powershell 5.1 or higher
- OpenSSH Server is enabled on the host machine

Administrators can follow the below steps to install an OPSWAT product on a remote machine through OPSWAT Central Management console. Note that while these steps are demonstrated with the MetaDefender Kiosk product, you can apply the same process for other OPSWAT Products such as MetaDefender Core and Vault.

1. Go to the **MetaDefender Kiosk** management page under **Inventory** in the sidebar.

2. Click the **ADD KIOSK** button in the top right panel.

3. The dialog **Add Kiosk** will be opened. Select the **Remotely install a new Kiosk** button.
4. Fill the proper inputs and click the TEST CONNECTION button to check the connection status.

- **Name**: The name of the new Kiosk instance.
- **Server Address**: The server address of the remoted device.
- **Username, Password**: The credentials used to access the remoted device.
- **Installer URL**: The URL to download MetaDefender Kiosk.

5. The dialog will be closed and the Kiosk management page will be reloaded automatically if the result is successful.

6. For MetaDefender Kiosk version 4.3.0 and above, a unique API Key is required to connect to OPSWAT Central Management. Log into the remoted device and retrieve the API Key from the User Management menu. Click **Generate** to get the API Key.

7. Click on the gear icon in the new kiosk's entry in the Kiosk Management page on your OPSWAT Central Management. Select **Edit**.

8. Enter the new API Key retrieved from step 6 into the API Key entry for MetaDefender Kiosk version 4.3.0 and above. For older versions, please enter "admin".
9. The status of the Kiosk is **Connected** after fetching the version of this Kiosk instance successfully.

### 3.7. Managing OPSWAT Product Sets and Groups

OPSWAT Central Management provides Set and Group Management to let users efficiently manage connected OPSWAT Products by organizing them into customizable collections.

Set is a collection of OPSWAT Products of the same type, e.g., only MetaDefender Core instances. Products within the same Set can be configured to a unified setting for their product type, which is specified in the Set settings.

Group is a collection of Sets, which can contain different OPSWAT Product types, e.g., a Group consists of a MetaDefender Core Set and a MetaDefender Kiosk Set.

- **Set Management**
  - Creating new Set
  - Configuring Set settings
- **Group Management**
  - Adding Product Group
3.7.1. Set Management

Set View

In order to access the Set Management feature for the OPSWAT Product type you wish to manage, navigate to its menu under **Inventory** and change the **View Mode** to **Set View**.

The **Default** Set is available by default, containing all unassigned instances of an OPSWAT Product type.
In Set View, users can delete one or multiple Sets by ticking their checkboxes, selecting **Delete** from the **ACTIONS** drop-down menu.

- Members of the deleted Sets will be reassigned to the Default Set of their product type.

Users can also assign individual Set to Group by clicking on the gear icon and selecting **Assign to Group**. In the pop-up dialog, select the Group where the Set should be added to and confirm the selection.

**Assign To Group**

Enter your 4-digit PIN to assign your set. If you have not yet set your PIN, please go to the account settings page to create your PIN

![Assign To Group](image)

**Edit individual Set and its member OPSWAT Product instances**

Users can modify the individual Set by clicking on the Set's entry.

![Edit Set](image)

To modify the Set's name, select the edit icon next to the Set's name. Similarly, to modify the Set's description, click on **Change** next to the Set's description.
The **Settings** option may not be available to some instances. To be able to access **Settings**, the instance must be connected, still possess a valid license, and must have a valid configuration.

Users can also edit the member OPSWAT Product instances from the Set menu. To change an instance's name, click on the edit icon on its entry. To modify an instance's settings, select **Settings** from its entry's gear icon's drop-down menu.

To assign additional OPSWAT Product instances to the Set, select **ADD <OPSWAT Product> TO SET**.

Select the additional instances by ticking their checkboxes. Finalize the selection by selecting **ADD**.

**3.7.1.1. Creating new Set**

The following guideline describes how to create a new Set in OPSWAT Central Management.

1. In **Set View**, select **CREATE NEW SET**.

2. In the **General information** page, fill out the required information for the new Set. Optionally, select an existing group where the new Set should be added to. Select **ASSIGN <OPSWAT Product> TO SET** when ready.
• **Name**: The name of the new Set, must be unique.

• **Description**: The description of the new Set.

3. In the **Assign instance to set** page, tick the checkboxes of the OPSWAT Product instances that should be added to the new Set. Select **CREATE** to finalize the new Set's creation.

4. The new Set is displayed in Set View.
Adding an OPSWAT Product belonging to another existing Set will remove it from that Set.

3.7.1.2. Configuring Set settings

Set settings allow users to unify all OPSWAT Product instances in the same Set under the same settings for their product type. The Set settings are derived from a specific instance’s settings.

The following guideline describes how to create Set settings and apply it to a Set of OPSWAT Product instances in OPSWAT Central Management.

1. In Set View, click on the Set that needs to be configured.

2. Choose the product instance that Set settings should be derived from by clicking on the gear icon and select Choose as Set settings from the drop-down menu.

3. Select VIEW SET SETTINGS to view and modify the current Set settings. In the newly opened page, select APPLY SET SETTINGS to apply it to all currently connected product instances in the Set.
Set settings will overwrite the individual settings of the OPSWAT Product instances in the set. Please ensure that the set only contains the instances that should have their settings unified.

Set settings are only applied to currently connected instances and are not applied retroactively to newly added instances. The users will need to reapply set settings for Set members that were disconnected when Set settings are applied or are newly added.

3.7.2. Group Management

Product Groups menu

The Group Management feature is located under Groups > Product Groups.

The Default Group is available by default, containing the Default Sets of each product type and all Sets which have not been assigned to a Group in OPSWAT Central Management. The content of the Sets is displayed in the Group entry.

Users can delete a Group by selecting the delete icon.

Members of the deleted Groups will be reassigned to the Default Group.

Group Detail

Select Group Detail to view the individual Group and its member Sets.
In Group Detail, the member Sets are categorized into tabs according to their product type. Users can change the Group's name by clicking on the edit icon next to its current name and the Group's description by clicking on Change next to its Description entry.

Users can also delete member Sets by ticking their checkboxes and select Delete from the ACTIONS drop-down menu.

Delete will delete the Set itself and reassign all member instances to their product type's Default Set, instead of just removing the set from its current Group.

To assign additional Sets to the Group, select ADD SET TO GROUP.

Select the additional Sets by ticking their checkboxes. Finalize the selection by selecting ADD.

3.7.2.1. Adding Product Group

The following guideline describes how to add a new Group to OPSWAT Central Management.

1. In Product Groups page, select ADD PRODUCT GROUP.
2. In the **General Information** page, fill out the required information of the new Group. Select **ASSIGN SET TO GROUP** to continue.

- **Name**: The name of the new Group, must be unique.
- **Description**: The description of the new Group.

3. In the **Assign Set to Group** page, select the Sets you wish to include in the new group by ticking their checkboxes. Select **ADD** to finalize the new Group's creation.

4. The new Group will be displayed in the Product Groups page.
3.8. Managing Users and Active Directories

Active Directory is a directory service developed to manage permissions and access to network resources. OPSWAT Central Management offers integration with Active Directory service along with a suite of accompanying user management features.

Administrators can manage access to the OPSWAT Central Management console for users registered in an existing Active Directory in the current network or create new access credentials in a locally-stored User Directory. Administrators can also define user roles to control the access level granted to different users and configure account security measures.

- Users and Groups
  - Adding a new user or group
- Roles
- User Directories
  - Adding User Directory

3.8.1. Users and Groups

In the Users and Groups menu, users can add or remove user and group (Active Directories only), reset PIN and password for individual users, and perform role reassignment.

To access the Users and Groups menu, navigate to User Management sidebar and select the corresponding tab.
There are 3 categories of user types:

- **Local**: Individual users originally created in the OPSWAT Central Management console. The administrator user created in the configuration wizard is designated the master account and cannot be modified (please refer to Configuration wizard for more information).

- **Active Directory User**: Individual users stored on an Active Directory server.

- **Active Directory Group**: Groups (as defined by the Active Directory service) of one or more users stored on an Active Directory server.

The **Actions** drop-down menu contain various user management features. Tick the checkboxes in the user entries that require modifications. Select **Reset Pin** or **Reset Password** and then select **Reset** in the pop-up dialog to reset the selected users' PIN or password to a randomly generated one. For password, the user will be prompted to change their password at their next login after using the temporary password.
The reset password function is disabled for active directory group.

Select **Update Role** to change the designated role of the selected users. In the pop-up dialog, select the new role from the drop-down menu and then click **Update** to confirm the selection.
For Active Directory Group, the role assigned to the group apply to all member users. If a user belongs to multiple groups with different roles (for example, both Administrator and Read-Only), the role with the higher privilege applies (Administrator in this case).

If a user with Administrator role demotes their roles to Read-Only, they will be immediately logged out of the session.

Select Delete to remove an existing users. In the pop-up dialog, select Delete again to confirm the selection.
The currently logged-in user cannot delete themselves, even if they have administrative access to user management.

An action performed against a user group applies to all member users.

3.8.1.1. Adding a new user or group

The following guideline describes how to add a new user or group in OPSWAT Central Management.

1. In the USERS AND GROUPS tab of the User Management menu, select ADD NEW USER/GROUP.

2. In the Add New User/Group page, select the user directory the new user or group should belong to.

The next steps differ depend on which directory type the selected user directory belongs to.

Local Directory:

1. If the selected user directory is of local type, fill in the required information and select the roles to be assigned to the new user. Select ADD to confirm.
1. **First Name, Last Name**: The user's identity
2. **Email**: The user's email, also used as part of their login credentials.
3. **Assign To Roles**: Assign user to either Administrator or Read-Only role.

   the new user will be assigned a temporary password and will be asked to change it at their first login.

**Temporary Password**

User three@opswat.com has been successfully added with the temporary password as below

HcYdMX3UFc0gGGZBb

COPY
Active Directory:

1. If the selected user directory is of active directory type, fill in the User Directory username and User Directory password in the User Directory Information section and select TEST CONNECTION to check the connection to the Active Directory and enable the Account Information section.

2. After a successful connection test, select the account type and either the user or user group to be added from the user directory in the Find Account Name field (type ** and click the magnifier icon to list all member users or groups). Select the role to assign to the new user or user group. Select ADD to confirm the selection.
If the selected user directory contains multiple active directories, the find function will return only results from the first active directory that the matches are found in. Similarly, "*" only returns results from the first active directory.

For both type of user directories, until the new user logs in, their status will be set as **Pending**.

User group can only be created in user directories of Active Directory type.

Added users that do not belong to the default LOCAL user directory have the login username format of <User Directory>/<Email>. For example, a user with email abc@email.com belonging to the NEWDIR user directory has the username NEWDIR/abc@email.com.
3.8.2. Roles

Roles define the level of access a given user or user group have in OPSWAT Central Management.

There are currently two roles available in OPSWAT Central Management:

- **Administrator**: Have full access to the management console. Can edit settings and perform all functions within OPSWAT Central Management.
- **Read-Only**: Only have viewing access. Cannot interact with settings nor perform any functions in OPSWAT Central Management.

The **Roles** tab is located in the **User Management** menu and shows the number of users assigned to each role.

3.8.3. User Directories

The User Directories menu allow users to add or remove user directories, change which user directories are currently enabled, and edit their settings.

The **User Directories** menu is a tab located in the **User Management** menu.

User Directories define the locations where user data is stored. There are two type of user directories.
- **Local**: User data is located locally within OPSWAT Central Management's database.
- **Active Directory**: User data is stored on an Active Directory service.

The **RELEASE LOCKOUT** button resets the lockout status of all users. Lockout refers to the security measure that prevents users from logging in after exceeding the maximum number of allowable failed login attempts.

To enable or disable user directories, click on the **ENABLE** slider.

To delete user directories, tick the checkboxes on their entries and select **Delete** in the **ACTIONS** drop-down menu.

⚠️ A user directory with at least one currently logged in user cannot be disabled or deleted.

To edit user directories, tick the checkboxes on their entries and select **Edit** from the gear icon. The edit interface is similar to the **ADD NEW USER DIRECTORY** menu. Please refer to Adding User Directory for more information. Modify the settings as needed and select **UPDATE** to confirm the changes.
3.8.3.1. Adding User Directory

The following guideline describes how to add a new user directory in OPSWAT Central Management.

1. In the User Directories menu, select **ADD NEW USER DIRECTORY**.
2. In the **General Information** step, fill in the required information and select **USER DIRECTORY SETTINGS** to continue to the next step.

- **Name:** The name of new user directory.
- **User Directory Type:** The type of user directory, either **Local** or **Active Directory**.
- **Enable this User directory:** Tick this checkbox to immediately enable this directory for use after creation.

3. The **USER DIRECTORY SETTINGS** step differs between user directory type.
   a. For **Local** type user directory, modify the default settings as required and select **ADD** to finalize the new directory's creation.

   - **Number of failed logins before lockout:** Number of allowed login attempts in 1 minute. Setting it to 0 allows unlimited failed logins.
- **Lockout time (minutes):** The length of the lockout period after a user reaches the maximum amount of failed logins. Setting it to 0 allows unlimited failed logins regardless of the number of failed logins specified.

b. **For Active Directory type** user directory, fill in the required information and select **TEST CONNECTION** to check connection to the Active Directory server. After the connection is verified, select **ADD** to finalize the new user directory's creation.

- **Server Host, Server Port:** The address of the Active Directory server.
- **Encryption:** The encryption type used by the Active Directory server (None, SSL, StartTLS)
- **User Base DN, Group Base DN:** The point where OPSWAT Central Management search for users and groups when adding new users and groups from Active Directories.
- **ADD NEW SERVER:** Add an additional Active Directory server entry.

⚠️ Adding multiple Active Directory servers under the same user directory requires that all these Active Directories share the same credentials.

⚠️ Adding an encrypted user directory may require importing its certificate to OPSWAT Central Management's Java Runtime Environment keystore. Please follow the instructions below to add the certificate:

1. Locate the root certificate file (.crt) for the user directory.
2. From an elevated command-line interface, enter the command:
2. Example:

```
"%JRE_HOME%\bin\keytool" -importcert -keystore "%JRE_HOME%\lib\security\cacerts" -storepass <password> -alias "<alias>" -file "<rootCA.crt path>"
```

The host machine should have the JRE_HOME environment variable already set so the command can work properly. Replace the following fields with the correct information.

- `<password>`: The keystore’s password
- `<alias>`: The certificate’s alias.
- `<rootCA.crt path>`: The path to the user directory’s root certificate file.

3. Restart OPSWAT Central Management for the changes to take effect.

3.9. Managing MetaDefender Email Gateway Security

OPSWAT Central Management can not only manage MetaDefender Email Gateway Security instance’s settings but also install MetaDefender Email Gateway Security instances remotely.

- Adding an existing MetaDefender Email Gateway Security instance
- Deleting an existing MetaDefender Email Gateway Security instance
- Managing MetaDefender Email Gateway Security License
  - Online product activation
  - Offline product activation
- Changing MetaDefender Email Gateway Security Configuration

3.9.1. Adding an existing MetaDefender Email Gateway Security instance

The following guideline describes how to add an existing MetaDefender Email Gateway Security instance to OPSWAT Central Management.
1. Go to the **MetaDefender Email Gateway Security** management page under **Inventory** in the sidebar.

   ![MetaDefender Email Gateway Security Management Page]

2. Click the **ADD NEW INSTANCE** button in the top right panel.

3. The dialog **Add Instance** will be opened. Select the **Add an existing Instance** button.
4. Fill the proper inputs and then click the **TEST CONNECTION** button to check the connection status.

![Add An Existing Instance](image)

- **Name**: The name you want to assign to the new Email Gateway Security instance.
- **API Key**: The API Key of the Email Gateway Security instance to authenticate the request
- **Server Address**: The address of the Email Gateway Security instance

5. The dialog will be closed and the management page will be reloaded automatically if the result is successful.

### 3.9.2. Deleting an existing MetaDefender Email Gateway Security instance

The following guideline describes how to delete a MetaDefender Email Gateway Security instance from OPSWAT Central Management.
1. Go to the **MetaDefender Email Gateway Security** management page under **Inventory** in the sidebar.

![Image of MetaDefender Email Gateway Security management page](image)

2. Select the Email Gateway Security instance that you want to delete.

![Image of selecting an instance](image)

3. Click the **ACTION** drop-down menu and choose the **Delete** option.

```
After PIN verification, the management page will reload if the result is successful.
```

3.9.3. Managing MetaDefender Email Gateway Security License

The following guideline describes how to activate or deactivate the license of a MetaDefender Email Gateway Security instance remotely.

1. Go to the **MetaDefender Email Gateway Security** management page under **Inventory** in the sidebar.
2. Select **License Information** for the Email Gateway Security instance you wish to configure.

3. If the current instance does not have an active license, select **ADD LICENSE** to activate one.

   ![License Information](image1)

   *No License found*

   ![Add License](image2)

   If it does have an active license, select **REMOVE LICENSE** to deactivate it or **UPDATE LICENSE** to switch to a different license.

   ![License Information](image3)

   ![Remove and Update Licenses](image4)

4. If either adding or updating is chosen in the previous step, please choose a license activation method in the newly opened dialog.
3.9.3.1. Online product activation

The following guideline describes how to activate the MetaDefender Email Gateway Security license online.

1. Select the **Online Activation** option.
2. Enter the key.

Starting with Online Activation:

**Activation Key**

Enter Activation Key

**Describe This Deployment**

This helps you to identify this host on OPSWAT License Portal

[BACK] [ACTIVATE]
3. The dialog will be closed and the management page will be reloaded automatically if the result is successful.

3.9.3.2. Offline product activation

The following guideline describes how to activate the MetaDefender Email Gateway Security license offline.

1. Select the **Offline Activation** option.
2. The **Offline Activation** menu will be opened.

**Offline Activation**

1. Log into [OPSWAT portal](https://portal.opswat.com/activation) > License Activation

2. Activate OPSWAT Central Management product and download an activation file. You will need

<table>
<thead>
<tr>
<th>ACTIVATION KEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have received an activation key from your purchase or from the trial email</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DEPLOYMENTID OF THIS INSTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDEMAIL2Bqnp6awujTn6uGEXDwv142AnTe1X0fB</td>
</tr>
</tbody>
</table>

3. Upload the activation file to here

   ![Choose file button](No file chosen.)

**Offline Activation details**


2. Select MetaDefender Email Security for **MetaDefender Package**.

3. Fill in the requested information about your deployment.
• **Activation Key**: The activation key of MetaDefender Email Gateway Security that you have received.

• **Deployment ID**: The deployment ID shown in the previous section.

• **Optional description**: The description for this deployment.

4. Click the **Request Unlock Key** button. The **Download Unlock Key** link will appear.
5. Click the **Download Unlock Key** link and save the activation file.
6. Go back to OPSWAT Central Management's Web Management Console. Browse for the activation file and click the **ACTIVATE** button.

7. The dialog will be closed and the management page will be reloaded automatically if the result is successful.

3.9.4. Changing MetaDefender Email Security Configuration

The following guideline describes how to change the configuration of a MetaDefender Email Security instance remotely.
1. Go to the MetaDefender Email Security management page under Inventory in the sidebar.

   ![MetaDefender Email Gateway Security Management](image)

2. Click the Settings button in the gear icon’s drop-down menu.

3. OPSWAT Central Management will load the settings of the instance. Change the settings as required.

   ![MetaDefender Email Gateway Security Settings](image)

   **Warning:** Settings cannot be changed if the instance is disconnected.

3.10. Managing MetaDefender ICAP Server

OPSWAT Central Management can not only manage MetaDefender ICAP Server instance’s settings but also install MetaDefender ICAP Server instances remotely.

- **Adding an existing MetaDefender ICAP Server instance**
• Deleting an existing MetaDefender ICAP Server instance
• Managing MetaDefender ICAP Server License
  • Online product activation
  • Offline product activation
• Changing MetaDefender ICAP Server Configuration

3.10.1. Adding an existing MetaDefender ICAP Server instance

The following guideline describes how to add an existing MetaDefender ICAP Server instance to OPSWAT Central Management.

1. Go to the MetaDefender ICAP Server management page under Inventory in the sidebar.

![MetaDefender ICAP Server management page](image)

2. Click the ADD NEW INSTANCE button in the top right panel.
3. The dialog **Add Instance** will be opened. Select the **Add an existing Instance** button.

**Add Instance**

- **Add an existing Instance**
  - Import information about an existing Metadefender ICAP Server to add it to your system

- **Remotely install a new Instance**
  - Connect to a device and install your new Metadefender ICAP Server on it

4. Fill the proper inputs and then click the **TEST CONNECTION** button to check the connection status.

**Add An Existing Instance**

- **Name**: The name you want to assign to the new ICAP Server instance.
- **API Key**: The API Key of the ICAP Server instance to authenticate the request
- **Server Address**: The address of the ICAP Server instance
5. The dialog will be closed and the management page will be reloaded automatically if the result is successful.

3.10.2. Deleting an existing MetaDefender ICAP Server instance

The following guideline describes how to delete a MetaDefender ICAP Server instance from OPSWAT Central Management.

1. Go to the MetaDefender ICAP Server management page under Inventory in the sidebar.

2. Select the ICAP Server instance that you want to delete.

3. Click the ACTION drop-down menu and choose the Delete option.

After PIN verification, the management page will reload if the result is successful.

3.10.3. Managing MetaDefender ICAP Server License

The following guideline describes how to activate or deactivate the license of a MetaDefender ICAP Server instance remotely.
1. Go to the MetaDefender ICAP Server management page under Inventory in the sidebar.

2. Select License Information for the ICAP Server instance you wish to configure.

3. If the current instance does not have an active license, select ADD LICENSE to activate one.

   License Information
   No License found
   ADD LICENSE

   If it does have an active license, select REMOVE LICENSE to deactivate it or UPDATE LICENSE to switch to a different license.
4. If either adding or updating is chosen in the previous step, please choose a license activation method in the newly opened dialog.

Metadefender ICAP Server Activation

Online Activation

Offline Activation

Cancel Activation

- Online product activation
- Offline product activation

3.10.3.1. Online product activation

The following guideline describes how to activate the MetaDefender ICAP Server license online.

1. Select the Online Activation option.
2. Enter the key.

**Online Activation**

*Activation Key*

Enter Activation Key

**Describe This Deployment**

This helps you to identify this host on OPSWAT License Portal

[BACK] [ACTIVATE]
3. The dialog will be closed and the management page will be reloaded automatically if the result is successful.

<table>
<thead>
<tr>
<th>STATUS</th>
<th>NAME</th>
<th>VERSION</th>
<th>SERVER ADDRESS</th>
<th>SET NAME</th>
<th>LICENSE</th>
<th>LAST SEEN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>igp711</td>
<td>4.7.0</td>
<td><a href="http://192.168.30.179:8090">http://192.168.30.179:8090</a></td>
<td>Default ICAP Server Set</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 3.10.3.2. Offline product activation

The following guideline describes how to activate the MetaDefender ICAP Server license offline.

1. Select the **Offline Activation** option.
2. The **Offline Activation** menu will be opened.

**Offline Activation**

1. Log into **OPSWAT portal** > License Activation
2. Activate OPSWAT Central Management product and download an activation file. You will need

<table>
<thead>
<tr>
<th>ACTIVATION KEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have received an activation key from your purchase or from the trial email</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DEPLOYMENTID OF THIS INSTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDEMAIL2BRqn6awujTn6uGEXDwv142ARTe1X0fB</td>
</tr>
</tbody>
</table>

3. Upload the activation file to here

[Choose file] No file chosen.

**BACK** **ACTIVATE**

---

**Offline Activation details**

2. Select MetaDefender ICAP Server for **MetaDefender Package**.
3. Fill in the requested information about your deployment.
- **Activation Key**: The activation key of MetaDefender ICAP Server that you have received.
- **Deployment ID**: The deployment ID shown in the previous section.
- **Optional description**: The description for this deployment.

4. Click the **Request Unlock Key** button. The **Download Unlock Key** link will appear.
5. Click the **Download Unlock Key** link and save the activation file.
6. Go back to OPSWAT Central Management's Web Management Console. Browse for the activation file and click the **ACTIVATE** button.

![Offline Activation](image)

7. The dialog will be closed and the management page will be reloaded automatically if the result is successful.

3.10.4. Changing MetaDefender ICAP Server Configuration

The following guideline describes how to change the configuration of a MetaDefender ICAP Server instance remotely.
1. Go to the MetaDefender ICAP Server management page under Inventory in the sidebar.

2. Click the Settings button in the gear icon’s drop-down menu.

3. OPSWAT Central Management will load the settings of the instance. Change the settings as required.

⚠️ Settings cannot be changed if the instance is disconnected.

3.11. Managing MetaDefender Drive

OPSWAT Central Management can manage MetaDefender Drive instance’s settings.

- Adding an existing MetaDefender Drive instance
- Deleting an existing MetaDefender Drive instance
- Changing MetaDefender Drive Configuration
- Downloading reports from an existing MetaDefender Drive instance
3.11.1. Adding an existing MetaDefender Drive instance

The following guideline describes how to add an existing MetaDefender Drive instance to OPSWAT Central Management.

Adding an existing MetaDefender Drive instance to OPSWAT Central Management can only be done from the MetaDefender Drive instance's interface.

1. From MetaDefender Drive's main page, select Central Management in the upper-right corner.

2. Enter the **IP Address** and **API Key** of the OPSWAT Central Management server.
   - **IP Address** can be found in Settings > Server Configuration > DEVICE API under **Server URL**.
   - **API Key** can be found in Settings > Global Settings > ACCOUNT under **Registration Code**.
3. Select **Connect**.

4. The **MetaDefender Drive** page will display the new instance if the process is successful.

### 3.11.2. Deleting an existing MetaDefender Drive instance

The following guideline describes how to delete a MetaDefender Drive instance from OPSWAT Central Management.

1. Go to the **MetaDefender Drive** management page under **Inventory** in the sidebar.
2. Select the Drive instance that you want to delete.

3. Click the ACTION drop-down menu and choose the **Delete** option.

- After PIN verification, the management page will reload if the result is successful.

- Deleting a MetaDefender Drive instance does not remove any reports that OPSWAT Central Management has collected from the instance. These reports will be accessible again if the instance is re-enrolled.

### 3.11.3. Changing MetaDefender Drive Configuration

The following guideline describes how to change the configuration of a MetaDefender Drive instance remotely.
1. Go to the MetaDefender Drive management page under Inventory in the sidebar.

```
<table>
<thead>
<tr>
<th>Settings</th>
<th>Management</th>
<th>License</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Type</td>
<td>OPSWAT Ltd</td>
<td>MetaDefender Drive 1 year</td>
<td>Unlimited usage per day</td>
</tr>
<tr>
<td>Expiry</td>
<td>05/01/2023</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deployment ID</td>
<td>MSC3dLDzLzFzFqslpCLHLtsc4pLzA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session Key</td>
<td>SessionKey123</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

2. Click the Settings button in the gear icon's drop-down menu.

3. OPSWAT Central Management will load the settings of the instance. Change the settings as required.

⚠️ Settings cannot be changed if the instance is disconnected or if the instance does not have a valid license (either expired or not available).

3.11.4. Downloading reports from an existing MetaDefender Drive instance

The following guideline describes how to download reports from an existing MetaDefender Drive instance.

Latest report:

1. Go to the MetaDefender Drive management page under Inventory in the sidebar.
2. Select the Drive instance that you want to download the report from.

3. Select either Download latest report (pdf) or Download latest report (txt).

Any past reports:

1. Go to the MetaDefender Drive management page under Inventory in the sidebar.
2. Click on an Drive instance's entry to go to its details page.

3. Select the report(s) to be downloaded by ticking their checkboxes. Select either Download report (pdf) or Download report (txt) from the drop-down action menu.
4. Configuring OPSWAT Central Management Server

This section explains how to configure an OPSWAT Central Management server.

- Setting up domain
- Enabling HTTPS

4.1. Setting up domain

If you have a domain name assigned to your OPSWAT Central Management server, you can configure it on the OPSWAT Central Management to embed that domain name into the OPSWAT Client installers and portable clients. OPSWAT Client will use that domain name to connect to the server. This change can be performed on the setup wizard or later in Setting → Server Configuration.

⚠️ Warning

Please be aware that changing domain name or IP address of the OPSWAT Central Management server can cause devices that have installed OPSWAT Client to be unable to connect to this server.

On the setup wizard

After a fresh installation, a setup wizard will be loaded to walk you through setting up your OPSWAT Central Management server. You can enter the domain name you assigned to your OPSWAT Central Management server in the Server Settings step.
From Server Configuration

You can modify the domain name of your OPSWAT Central Management server at any time in Settings > Server Configuration > Device API.
4.2. Enabling HTTPS

By default, the communication between a product and an OPSWAT Central Management server is not encrypted. If HTTPS is set, the server can enforce secure connections between clients and the server on SSL channels. This section describes how to enable SSL for OPSWAT Central Management.

⚠️ Warning

Please be aware that enabling HTTPS on the OPSWAT Central Management server can cause devices that have installed OPSWAT Client to be unable to connect to this server. These devices require reinstallation of OPSWAT Client.

Requirements

In order to enable HTTPS on OPSWAT Central Management server, a trusted certificate issued by a certificate authority provider or a self-signed certificate must be provided.

See the section below for information on how to install a self-signed server certificate if a trusted certificate is not provided.

Enabling HTTPS for OPSWAT Central Management

Requirement: You need to have a certificate and key file of your certificate on your server, for example, C:\OCM_Keys\your.crt and C:\OCM_Keys\your.key.

To enable HTTPS on OPSWAT Central Management server:

1. Go to nginx configuration folder under OPSWAT Central Management installation folder (e.g., C:\Program Files\OPSWAT\Central\nginx\conf).
2. The code block below should be available in the ssl.conf file. Note: You need to replace
a. `<PATH_TO_CERT_FILE>` with a path to your certificate file, for example: "C:\OCM_Keys\your.crt
C:\OCM_Keys\your.crt"

b. `<PATH_TO_KEY_FILE>` with a path to your key file, for example: "C:\OCM_Keys\your.key"

```nginx
ssl on;
ssl_certificate <PATH_TO_CERT_FILE>;
ssl_certificate_key <PATH_TO_KEY_FILE>;
ssl_protocols TLSv1.1 TLSv1.2;
ssl_ciphers HIGH:!aNULL:!MD5;
ssl_session_cache shared:SSL:10m;
ssl_session_timeout 10m;
error_page 497 https://$host:$server_port$request_uri;
```

⚠️ Using the standard Windows path separator backslash `\` may have unexpected results if the directory or file names start with `\n`. The reason is that the sequence `\n` is interpreted as a new line by nginx.

For example, the following directive:

```nginx
ssl_certificate "C:\Program Files\OPSWAT\Metadefender Centralmgmt\nginx\your.crt";
```

will be interpreted by nginx as:

```nginx
ssl_certificate "C:\Program Files\OPSWAT\Metadefender Centralmgmt\nginx\your.crt";
```

As a workaround, instead of backslash `\`, please use:

1. Forward slash `\` or
2. Double backslash `\\`.

Such as:

```nginx
ssl_certificate "C:\\Program Files\\OPSWAT\\Metadefender Centralmgmt\\nginx\\your.crt";
```
3. Restart the OPSWAT Central Management by clicking the **Restart** button on the OPSWAT Central Management tray icon.

4. After the service is restarted, open the OPSWAT Central Management console UI, for example **https://localhost:9000** , to check whether the console can be loaded successfully.

5. Update Device API setting to utilize HTTPS. Go to **Server Configuration > Device API** and change the **Server URL** from "http" to "https". Press **Save**.

OPSWAT Central Management below version 7.2.0 keeps the HTTPS configuration in nginx.conf. If you are upgrading from one such version to 7.2.0 or above, the setup should automatically generate ssl.conf from your modified nginx.conf file and reset nginx.conf to its default state. In case the generating process failed and the default ssl.conf is installed instead, please follow the instructions below to retrieve your HTTPS configuration.

1. Navigate to nginx.conf’s backup folder (located in C:\ProgramData\OPSWAT\Central\bak by default).
2. Locate the HTTPS configuration block as shown above.
3. Copy the configuration block to the active ssl.conf file (located in C:\Program Files\OPSWAT\Central\nginx\conf by default).
4. Restart OPSWAT Central Management for the new configuration to take effect.
Adding product instances with HTTPS configuration

Adding a product instance configured for HTTPS connection may require adding its root certificates to OPSWAT Central Management’s Java Runtime Environment keystore. Please follow the instructions below to add the certificate.

1. Locate the root certificate file (.crt) for the product instance.
2. From an elevated command-line interface, enter the command:

```
"%JRE_HOME%\bin\keytool" -importcert -keystore "%JRE_HOME%\lib\security\cacerts" -storepass <password> -alias "<alias> -file "<rootCA.crt path>"
```

Example:

```
"%JRE_HOME%\bin\keytool" -importcert -keystore "%JRE_HOME%\lib\security\cacerts" -storepass changeit -alias "ocmCA" -file "C:\Users\admin\Downloads\ocm.crt"
```

The host machine should have the JRE_HOME environment variable already set so the command can work properly. Replace the following fields with the correct information.

- `<password>`: The keystore’s password
- `<alias>`: The certificate’s alias.
- `<rootCA.crt path>`: The path to the product instance’s root certificate file.
3. Restart OPSWAT Central Management for the changes to take effect.

4.3 Interface Port Configuration

The port used to access the OPSWAT Central Management Console (9000 by default) can be changed on Windows systems by following the below steps:

1. Locate the file ProgramData/OPSWAT/Central/config.properties.
2. Change nginx_port to the desired value.

```
tomcat_port=9009
mongo_port=27017
memcached_port=9005
```
3. Locate the file Program Files/OPSWAT/Central/nginx/conf/serverSettings.conf
4. Change listen to the same value as nginx_port as above.

```
listen 9980;
```

5. Restart OPSWAT Central Management via the tray icon.

ℹ️ Port configuration is currently only available on the Windows version.
## 5. Release Notes

### 7.4.0 OPSWAT Central Management release

January 9, 2020

OPSWAT Central Management V7 (OCMv7), a newest version of the series, streamlines the product central configuration and added OPSWAT Client management to further enhance the security stance of organizations to protect against risky devices.

<table>
<thead>
<tr>
<th>Built-in OPSWAT Client version</th>
<th></th>
</tr>
</thead>
</table>
| Windows Persistent Agent 7.6.248.0 | • Supported MetaDefender Core Load-Balancer Layer 7  
• Built-in SDK 4.3.771.0 |
| Windows On-demand Agent 7.3.443.0 | • Built-in SDK 4.3.771.0 |
| macOS Persistent Agent 10.4.255.0 | • Supported MetaDefender Core Load-Balancer Layer 7  
• Built-in SDK 4.3.631.0 |
| macOS On-demand Agent 10.5.187.0 | • Built-in SDK 4.3.631.0 |

### New Features

| Red Hat Enterprise Linux 7.7’s support | OPSWAT Central Management now supports Red Hat Enterprise Linux 7.7 operating system. |
| MetaDefender Core Processing History | OPSWAT Central Management now allows users to view the combined processing history from all MetaDefender Core instances under its management. |
### Enhancements

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaDefender ICAP and MetaDefender Email Security offline configuration support</td>
<td>Settings changes can now be applied retroactively to instances that were offline at the time.</td>
</tr>
<tr>
<td>Import/Export improvement</td>
<td>Import/Export feature now include groups and sets.</td>
</tr>
<tr>
<td>SSO configuration without license</td>
<td>Administrators can now configure SSO option without activating a license.</td>
</tr>
<tr>
<td>Port configuration for the console interface</td>
<td>The default port for OPSWAT Central Management console can now be changed within the console.</td>
</tr>
<tr>
<td>Event log now displays all available data since initial installation</td>
<td>The 30-day retention limit for event logs is removed.</td>
</tr>
</tbody>
</table>

### Bugs Fixed

<table>
<thead>
<tr>
<th>Bug</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline activation of OPSWAT Central Management license failed in certain network configurations</td>
<td>OPSWAT Central Management now properly generates information used to generate an offline license file from the OPSWAT portal.</td>
</tr>
<tr>
<td></td>
<td>Fixed the verification of uploaded OPSWAT Client files.</td>
</tr>
</tbody>
</table>
OPSWAT Client could not be manually updated because of failed files verification

OPSWAT Central Management failed to start on certain Windows system's locale configurations

Changed the startup sequence to be locale-independent.

5.1. Changelog

Version 7.3.0
Release Date: November 22, 2019
New features:

- MetaDefender Drive management
- Single sign-on (SSO) support

Enhancements:

- Added password reset function for administrator account
- MetaDefender Core modules disabled during the update process now continue downloading instead of abort midway.
- Added log files containing the history of installed OPSWAT Central Management versions.
- Various UI enhancements to improve readability and usability.

Built-in OPSWAT Clients

| Windows Persistent Agent 7.6.248.0 | • Supported MetaDefender Core Load-Balancer Layer 7  
| | • Built-in SDK 4.3.771.0 |

| Built-in SDK 4.3.771.0 | • Built-in SDK 4.3.771.0 |
Built-in OPSWAT Clients

| Windows On-demand Agent 7.3.443.0 |  |
| macOS Persistent Agent 10.4.255.0 | • Supported MetaDefender Core Load-Balancer Layer 7  

• Built-in SDK 4.3.631.0 |
| macOS On-demand Agent 10.5.187.0 | • Built-in SDK 4.3.631.0 |

Version 7.2.0

Release Date: October 4, 2019

New features:
• Product Set and Group management
• User and User Group management
• Active Directory integration
• MetaDefender Core module updater
• Improved import/export function
• MetaDefender ICAP and Email Gateway Security management (Preview mode)

Enhancements:
• Added a mechanism to automatically detect system proxy
• Updated configuration wizard
• MetaDefender Core and Vault instances can now recognize being managed by OPSWAT Central Management.
• Separate HTTPS configuration from the main nginx's configuration file.
• Added a warning message when adding a disconnected product instance.
• Improved UI's consistency.

Built-in OPSWAT Clients

| Windows Persistent Agent 7.6.248.0 | • Supported MetaDefender Core Load-Balancer Layer 7  

• Built-in SDK 4.3.771.0 |
| Windows On-demand Agent 7.3.443.0 | • Built-in SDK 4.3.771.0 |
| macOS Persistent Agent 10.4.244.0 | • Supported MetaDefender Core Load-Balancer Layer 7  
• Built-in SDK 4.3.631.0 |
| macOS On-demand Agent 10.5.179.0 | • Built-in SDK 4.3.631.0 |

**Version 7.1.1**

Release Date: August 15, 2019

Enhancements:

- Added a mechanism to handle high load
- Updated the software requirements to JRE instead of JDK

### Built-in OPSWAT Clients

| Windows Persistent Agent 7.6.242.0 | • Supported MetaDefender Core Load-Balancer Layer 7  
• Built-in SDK 4.3.771.0 |
| Windows On-demand Agent 7.3.436.0 | • Built-in SDK 4.3.771.0 |
| macOS Persistent Agent 10.4.242.0 | • Supported MetaDefender Core Load-Balancer Layer 7  
• Built-in SDK 4.3.631.0 |
| macOS On-demand Agent 10.5.172.0 | • Built-in SDK 4.3.631.0 |

**Version 7.1.0**

Release Date: July 2, 2019

Built-in clients
Windows Persistent Agent 7.6.236.0
Windows On-demand Agent 7.3.436.0
macOS Persistent Agent 10.4.226.0
macOS On-demand Agent 10.5.172.0

New features:

- Inventory Management for OPSWAT Products (Kiosk, Core and Vault)
- Configuration Management for OPSWAT Products (Kiosk, Core and Vault)
- License Management for OPSWAT Products (Kiosk, Core and Vault)
- Policy Management for OPSWAT Products (Kiosk, Core and Vault)
- Health Check
- Import from URL
6. Troubleshooting

This is a general guideline to detect and correct problems in OPSWAT Central Management.

- The management console hung at the loading step
- Unable to connect to the target machine during remote installation
- Failed to re-install OPSWAT Central Management
- Failed to start OPSWAT Central Management service through the tray icon
- Failed to remote install OPSWAT Products
- OPSWAT Client failed to report to OPSWAT Central Management server
- OPSWAT Central Management failed to start with memcached/mongod shells hanging in the foreground
- Managed devices are unable to report to OPSWAT Central Management

6.1. The management console hung at the loading step

<table>
<thead>
<tr>
<th>Term</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>The management console hung at the loading step for more than 5 mins.</td>
</tr>
<tr>
<td>Cause</td>
<td>The loading page is not redirected properly.</td>
</tr>
<tr>
<td></td>
<td>Java environment variable is not defined correctly</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Refresh the page.</td>
</tr>
<tr>
<td></td>
<td>Check log in catalina_out.txt file. Look for the message &quot;The JRE_HOME environment variable is not defined correctly&quot;.</td>
</tr>
<tr>
<td>Solution</td>
<td>Install JRE 8 x64 (from update 171) and set the JRE_HOME environment variable to the JRE's installation path.</td>
</tr>
</tbody>
</table>

If the loading step hangs for more than 5 minutes, please first try refreshing the page.
If the problem persists, please check the logs in the log folder "C:\ProgramData\OPSWAT\Central\Logs".

Open the catalina_out.txt file, look for the error message "The JRE HOME environment variable is not defined correctly" as the below screenshot. This error message should occur when the OPSWAT Central Management starts.
In order to fix this error, please install JRE or JDK version 8, from update 171, and set either the JRE_HOME or JAVA_HOME environment variable paths to the correct installation path. Exit and reopen OPSWAT Central Management again for the changes to take effect.

6.2. Unable to connect to the target machine during remote installation

<table>
<thead>
<tr>
<th>Term</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>Unable to connect to the target machine during remote installation</td>
</tr>
<tr>
<td>Cause</td>
<td>The target machine has not enabled an OpenSSH server.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>The error message in the remote installation UI displays &quot;Connection cannot be established.&quot;</td>
</tr>
<tr>
<td>Solution</td>
<td>Refer to <a href="#">Remote Install OPSWAT Products</a> for how to enable OpenSSH server on the target machine.</td>
</tr>
</tbody>
</table>

If the UI displays the error message "Connection cannot be established" during the remote installation of an OPSWAT Product, it means that the target machine is not reachable.
A possible cause is that the target machine has not enabled an OpenSSH server to communicate with OPSWAT Central Management. Please refer to Remote Install OPSWAT Products on how to enable OpenSSH.

6.3. Failed to re-install OPSWAT Central Management

<table>
<thead>
<tr>
<th>Term</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>Failed to re-install OPSWAT Central Management</td>
</tr>
<tr>
<td>Cause</td>
<td>The installer could not copy some files to the system because they might still exist on the system from a previous version. The installer detected that the required ports for OPSWAT Central Management are unavailable.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>The installer stopped prematurely and showed the error message &quot;Installation ended prematurely because of an error.&quot;</td>
</tr>
</tbody>
</table>
Solution
Delete all leftover files and folders in the installation folder of OPSWAT Central Management. It may require a Windows restart in some cases.

Cause 1: The installer could not copy some files to the system because they might still exist on the system from a previous version.
The installation wizard failed with the error "OPSWAT Central Management <version> Setup Wizard ended prematurely" as in the below screenshot.

A possible cause is that a previous uninstallation process failed to remove all files from the installation folder because some of these files were locked by still-running processes.
The solution is to manually delete the installation folder (C:\Program Files\OPSWAT\Central by default) before reinstallation.

If Windows Explorer returns a "Folder in Use" or "Files in Use" error, this means that OPSWAT Central Management's services are still running in the background and locking these files. Please restart Windows and try again.
Cause 2: The installer detected that the required ports for OPSWAT Central Management are unavailable.

If prior to the error "OPSWAT Central Management <version> Setup Wizard ended prematurely" as shown above, the installer also display another error as shown below.
In this case, these ports are occupied by some background services. A possible cause is that these are OPSWAT Central Management's services which were not stopped correctly by the installer.

Please restart Windows and try again. If these ports are still unavailable, please check if there are other services unrelated to OPSWAT Central Management occupying these port.

### 6.4. Failed to start OPSWAT Central Management service through the tray icon

<table>
<thead>
<tr>
<th>Term</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>Failed to start OPSWAT Central Management service through the tray icon</td>
</tr>
<tr>
<td>Cause</td>
<td>OPSWAT Central Management services were not stopped correctly and are still running</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Failed to start OPSWAT Central Management through the tray icon with the error &quot;Failed to start OPSWAT Central Management due to the required port(s) &lt;ports&gt; being unavailable.&quot;</td>
</tr>
<tr>
<td>Solution</td>
<td>Restart the host machine</td>
</tr>
</tbody>
</table>

After stopping OPSWAT Central Management service through the tray icon, trying to start it again gives an error message such as in the image below. Similarly, restarting OPSWAT Central Management can produce the same message.

![Error Message](image.png)

A possible cause is that one or more support services for OPSWAT Central Management were not stopped properly and are still running, taking up the required port. Restarting Windows should clear all these running services.
OPSWAT Central Management is configured to start with Windows by default so it does not need to be manually started upon a Windows reboot.

6.5. Failed to remote install OPSWAT Products

<table>
<thead>
<tr>
<th>Term</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>Failed to remote install OPSWAT Products</td>
</tr>
<tr>
<td>Cause</td>
<td>OPSWAT Central Management was unable to open a SSH connection.</td>
</tr>
<tr>
<td></td>
<td>The target machine did not satisfy the system requirements of the</td>
</tr>
<tr>
<td></td>
<td>OPSWAT Product that was being installed.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Check log in gears_product_service.log file. Look for the newest version of the message &quot;Testing connection to &lt;target machine&gt;&quot;.</td>
</tr>
<tr>
<td>Solution</td>
<td>Ensure that the target machine has enabled OpenSSH server and can</td>
</tr>
<tr>
<td></td>
<td>satisfy the system requirements of the OPSWAT Product.</td>
</tr>
</tbody>
</table>

After starting the remote installation, the new OPSWAT Product's entry in the corresponding management page shows the **Disconnected** status.

Please check the file gears_product_service.log in the folder "C:\Program Files\OPSWAT\Central\tomcat\logs".
Look for the section that starts with "Testing connection to <target machine>" to find the remote installation's error message. If the log includes the line "Install failed", a possible cause is that the target machine did not satisfy the OPSWAT Product's system requirements. Please ensure that the target machine does meet the system requirements and try again.

If the log has one or more error messages "ExitStatus: 1" instead of "ExitStatus: 0", it is possible that OpenSSH server has not been enabled correctly on the target machine. Please refer to 3.6. Remote Install OPSWAT Products to correct its configuration.
6.6. OPSWAT Client failed to report to OPSWAT Central Management server

<table>
<thead>
<tr>
<th>Term</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>OPSWAT Client failed to report to OPSWAT Central Management server</td>
</tr>
<tr>
<td>Cause</td>
<td>OPSWAT Central Management's IP address has changed.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Go to Settings &gt; Server Configuration &gt; Device API and check if the Server URL field uses the new IP address.</td>
</tr>
<tr>
<td>Solution</td>
<td>Update Server URL and reinstall OPSWAT Client on the affected devices.</td>
</tr>
</tbody>
</table>

In the setup wizard, the user can choose to set Server URL to an IP address, which will be used by OPSWAT Client to report to OPSWAT Central Management. If the OPSWAT Central Management's server changes its IP address, OPSWAT Client instances still using the old address will be unable to connect.
Server Settings

These settings will be embedded to OPSWAT Agent installer/executable files to instruct the agent how to authenticate with this server.

You can update this setting later at Settings > Server Configuration.

Server URL *

Specify a valid URL which assigned to the OPSWAT Central Management server.

The URL format should be [http:\https://<server-domain-name OR server-IP-address>:port] and should NOT be localhost or a loopback address (127.x.x.x).


OPSWAT Agent Recovery Key *

The key below is uniquely generated for agent authentication. If you are recovering a server installation, please use the key you recorded from previous installation. Otherwise, please record this key for future recovery.

967a6f9077874a4b5adca54d38f4e9c
The solution is to update the Server URL field in **Settings > Server Configuration > Device API** and reinstall OPSWAT Client on the affected devices.

---

### 6.7. OPSWAT Central Management failed to start with memcached/mongod shells hanging in the foreground

<table>
<thead>
<tr>
<th>Term</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>OPSWAT Central Management failed to start with memcached/mongod shells hanging in the foreground</td>
</tr>
<tr>
<td>Cause</td>
<td>System variable Path is not set properly to Windows\System32 location.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Open OPSWAT Central Management's activity log in <strong>C:\ProgramData\OPSWAT\Central\Logs&lt;date&gt;.txt</strong> and check for the error &quot;The term &lt;&gt; is not recognized as the name of a cmdlet, function, script file, or operable program.&quot;</td>
</tr>
<tr>
<td>Solution</td>
<td>Add %SystemRoot%/system32 to system variable Path.</td>
</tr>
</tbody>
</table>
OPSWAT Central Management requires the use of command-line utilities such as netstat, which is located in the Windows\System32 folder. In order to access these commands, the system variable Path must include this folder.

Without access, the mongod and memcached services that OPSWAT Central Management depends on may hang in the foreground.

Navigating to OPSWAT Central Management’s activity log in **C:\ProgramData\OPSWAT\Central\Logs\<date>.txt**, the exact error is shown.
To solve this problem, navigate to the Environment Variables window from the Start menu.
Under **Path** (as highlighted), add "\%SystemRoot\%\system32" in a new line.
Restart the machine to ensure the change is propagated properly.

6.8 Managed devices are unable to report to OPSWAT Central Management

<table>
<thead>
<tr>
<th>Term</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td>Managed devices are unable to report to OPSWAT Central Management (Disconnected status)</td>
</tr>
<tr>
<td>Cause</td>
<td>OPSWAT Central Management has had its address changed and the server URL setting does not reflect the change.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Check if <strong>Server Configuration &gt; Device API &gt; Server URL</strong> is set correctly</td>
</tr>
<tr>
<td>Term</td>
<td>Detail</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Solution</td>
<td>Correct <strong>Server URL</strong> and reinstall OPSWAT Client on the affect devices.</td>
</tr>
</tbody>
</table>

If managed devices previously connected to OPSWAT Central Management now display as **Disconnected**, the OPSWAT Central Management console may have had its address changed since the last time OPSWAT Client were installed on the affected devices. This can be caused by a change in the IP address assigned to the system OPSWAT Central Management is running on.

To correct the server URL attached to OPSWAT Client by OPSWAT Central Management, navigate to **Server Configuration > Device API > Server URL**.

![Server Configuration](image)

Finally, reinstall OPSWAT Client on the affected devices according to **Distribute OPSWAT Client to devices**.
7. Knowledge Base Articles

- **OPSWAT Client**
  - What are the system requirements for OPSWAT Client?
  - How do I know which version of OPSWAT Client is installed on a device?
  - Which version of OCMv7 is compatible with OPSWAT Client?
  - How do I retrieve the OPSWAT Client logs?

- **User and Account Settings**
  - How can I provision users from our own single sign-on service to OPSWAT Central Management?
  - How do I change my PIN?
  - How do I add additional users to manage my account?
  - Is there a way to change a User’s role?

- Which versions of OPSWAT Products are compatible with OPSWAT Central Management v7?

---

**OPSWAT Client**

- What are the system requirements for OPSWAT Client?
- How do I know which version of OPSWAT Client is installed on a device?
- What OCMv7 version is OPSWAT Client compatible with?

**How do I know which version of OPSWAT Client is installed on a device?**

**From the OPSWAT Central Management console:**

The easiest way to find this information is to use **OPSWAT Central Management console**. Log into **OPSWAT Central Management console** and go to **Inventory > Devices:**

1. Search the device using its hostname/username/group name/…. 

---

7.4.0 193
2. The version of the Client installed on the device is shown on the **Client Version** column.

3. **Client Version** is also shown on the **System Information** box when we view device details. In this view, you are also able to check which SDK version the Client is running.

Unless **automatic updates are disabled**, the **persistent** OPSWAT Client will update automatically as new versions are released. If the device is offline for an extended period, the version will update the next time the device is online. An **on-demand** OPSWAT Client does not automatically update regardless of the account preference for automatic updates.

**From OPSWAT Client:**

The instructions for finding the version information from OPSWAT Client depend on the type of client, operating system, and UI settings.

**Windows/macOS Persistent Client with Tray Icon Enabled:**

1. Open Start menu, search for OPSWAT Client.
2. Click on OPSWAT Client.
3. Right-click the OPSWAT Client tray icon.
4. Choose About.

Information listed in the About dialog:

- Client version
- SDK Version (OESIS Framework version)
- Hostname
- Username
- OS information
- IP address
- MAC address
- The server the Client is talking to
- The account the device is associated to
- The last time the Client communicated with the OPSWAT Central Management cloud

Windows Persistent, Tray Icon Disabled:

- **OPSWAT Client Version**: check in registry at location
  - For Win 32bit: HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Gears Client\Config, key "MSIPackageVersion".
  - For Win 64bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\OPSWAT\Gears Client\Config, key "MSIPackageVersion".

- **SDK version (OESIS Framework version)**:
  - For Win 32bit: Go to folder C:\Program Files\OPSWAT\OnDemand\ondemands\oesis, check the product version/file version of any dll files.
  - For Win 64bit: Go to folder C:\Program Files (x86) \OPSWAT\OnDemand\ondemands\oesis, check the product version/file version of any dll files.

OSX Persistent, Tray Icon Disabled:

- **OPSWAT Client Version:**
• Go to /Application/OPSWAT GEARS Client.
• Click on OPSWAT Gears, you can see the version on the application info.

How do I retrieve the OPSWAT Client logs?
When troubleshooting an issue on devices, we will often ask you for the OPSWAT Client logs from your machine. There are 2 ways to retrieve the Client logs:

• OPTION 1: Collect the logs on a device directly.

• OPTION 2: Remotely retrieve the logs. This requires that you have administrator permission on your organization's OPSWAT Central Management account and the device is connecting to the OPSWAT Central Management servers.
OPTION 1: Collect the Client's logs on a device directly

Automatically:

This option is only available for Windows and macOS' persistent Client.

On Windows devices:
If you are using Windows installed client, the process is very simple. Just download this tool, run it, and the log files will automatically be placed in a zip file on your desktop. This zip file may be very large.

On macOS devices:
If you are using the macOS installed client, the process is very simple. Just download this tool, run it, and the log files will automatically be placed in a zip file on your desktop. This zip file may be very large.

Manually:
You can find your logs in the following locations:

Windows:
Installed client:
- Client logs: %ProgramData%\OPSWAT\Gears\logs\n- Crash dumps: %ProgramData%\OPSWAT\Gears\logs\reports\n- SDK logs: %ProgramData%\OPSWAT\Gears\sdk\n- OPG (verification file) logs: %HOMEPATH%\AppData\Local\OPSWAT\Gears\Logs

On-demand client:
- Client log: the file gears-ondemand.log should be located in the same folder of the executable file.
- Crash dumps: %HOMEPATH%\AppData\Local\CrashDump

Note: If the on-demand client is triggered by Pulse Secure Host Checker, you can find log files at %appdata%\Pulse Secure\Host Checker\policy_XXX (for example: C:\Users\bob\AppData\Roaming\Pulse Secure\Host Checker\policy_1)

macOS:
Installed client: ~/Library/Logs/Gears/logs and /Library/Logs/Gears/logs
On-demand client: On the desktop* as 'gears-ondemand.log'
Crash dump:~/Library/Logs/DiagnosticReports and /Library/Logs/DiagnosticReports
When running the Mac on-demand client as root, the logs will appear in `/var/root/Desktop/gears-on-demand.log` and additional malware logs will appear in `~/Library/Logs/Gears/logs/Metascan-Client-V2.log`.

**Android/iOS:**
Logs are only stored in memory, but can be sent via email from within the app by selecting the corresponding option on the feedback screen.

**OPTION 2: Remotely retrieve the Client's logs from the OPSWAT Central Management console**

**Note:** This option requires

- You have administrator permission on your organization's OPSWAT Central Management account.
- The device is connected to the OPSWAT Central Management servers.

As an administrator of the OPSWAT Central Management account, you can follow the below steps:

1. Log into OPSWAT Central Management console.
2. Go to **Inventory > Devices**.
3. Search for a device you would like to get logs of.
4. Select devices and choose the **Fetch log** action.
5. When a device is connecting to OPSWAT Central Management cloud, the device will collect log files and submit to OPSWAT Central Management cloud.
6. To download log file you fetched from OPSWAT Central Management console, go to **Device details** of the corresponding device and click on **Events > Actions**.
Sending the Logs to Support:
If you have been asked to share the files with support and they are too large to email or attach to the support ticket, please use the Large File submission feature on the OPSWAT support portal: https://portal.opswat.com/en/support/requests/large_file

What are the system requirements for OPSWAT Client?
Your devices must meet the following minimum system requirements to install OPSWAT Client.
### Operating System Family

<table>
<thead>
<tr>
<th>Operating System Family</th>
<th>Minimum OS Version</th>
<th>Minimum system requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows(1)</td>
<td>Windows 7</td>
<td>CPU: 1 GHz</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008</td>
<td>Hard disk space: 500MB</td>
</tr>
<tr>
<td>macOS</td>
<td>OSX 10.9</td>
<td>CPU: 1 GHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hard disk space: 500MB</td>
</tr>
<tr>
<td>iOS</td>
<td>iOS 8</td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td>Android 5.1</td>
<td>Memory: 1.5GB</td>
</tr>
</tbody>
</table>

Because of security issues, your device must support TLS 1.1, TLS 1.2. If it does not have these protocols enabled, please follow the instructions in the website below to enable them.


(1) On Windows system, you must install the following KBs to run OPSWAT Client.

- **Windows 10 and Windows Server 2012+**:


### Which versions of OPSWAT Central Management v7 are compatible with OPSWAT Client?

The below tables indicate the minimum OPSWAT Central Management v7 version each OPSWAT Client version supports.

- **Windows Persistent Client**
- **Windows On-demand Client**
- **macOS Persistent Client**
- **macOS On-demand Client**
OPSWAT Central Management v7.1.0 does not check the validity of OPSWAT Client's versions uploaded manually by the user to the server. If a Client's version incompatible with OPSWAT Central Management v7 is distributed to devices as update, the OPSWAT Clients on these devices will not be able to communicate with the server.

### Windows Persistent Client

<table>
<thead>
<tr>
<th>Client's version</th>
<th>Minimum OPSWAT Central Management v7's version</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.236.0</td>
<td>7.1.0</td>
</tr>
</tbody>
</table>

### Windows On-demand Client

<table>
<thead>
<tr>
<th>Client's version</th>
<th>Minimum OPSWAT Central Management v7's version</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.3.436.0</td>
<td>7.1.0</td>
</tr>
</tbody>
</table>

### macOS Persistent Client

<table>
<thead>
<tr>
<th>Client's version</th>
<th>Minimum OPSWAT Central Management v7's version</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.4.226.0</td>
<td>7.1.0</td>
</tr>
</tbody>
</table>

### macOS On-demand Client

<table>
<thead>
<tr>
<th>Client's version</th>
<th>Minimum OPSWAT Central Management v7's version</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5.172.0</td>
<td>7.1.0</td>
</tr>
</tbody>
</table>

### User and Account Settings

- How can I provision users from our own single sign-on service to OPSWAT Central Management?
- How do I change my PIN?
How do I add additional users to manage my account?

Is there a way to change a User's role?

How can I provision users from our own single sign-on service to OPSWAT Central Management?

OPSWAT Central Management offers integration with a 3rd-party Single Sign-on Service (SSO). This enables an account to provision new users to manage your account. When a user logs into the OPSWAT Central Management console through your own SSO service, OPSWAT Central Management will provision that user as a read-only user on your account. You can update the user’s role later.

OPSWAT Central Management uses the secure and widely adopted industry standard Security Assertion Markup Language 2.0 (SAML 2.0), so that you can integrate easily with any large identity provider that supports SAML 2.0.

To get started, go to your identity provider's website and follow the instructions to configure a SSO application for MetaAccess.

To integrate OPSWAT Central Management with your own SSO service:

1. Log into the OPSWAT Central Management console with admin permissions.
2. Navigate to **Settings > Integrations > Single sign-on**.
3. Select **Enable Single Sign On** checkbox.
4. Enter an IdP Name. This is for your reference.
5. Click the **Choose File** button to upload an IdP X.509 certificate .pem file that you received from the Identity Provider.
6. Enter the Issuer information you received earlier from the identity provider.
7. Enter the IdP SSO URL you received earlier from the identity provider.
8. Enter the IdP Log out URL and Error URL you received earlier from the identity provider if any.
9. Click the **Save** button.
10. After you save your changes successfully, OPSWAT Central Management will a OPSWAT Central Management Login URL You must copy this URL and update a postback SSO URL (also called the Assertion Consumer Service URL) of the SSO application for OPSWAT Central Management in your identity provider.

Note: You can import information from step #5 through #8 from the IdP metadata file that you received earlier from the identity provider if it is available.

You can find detailed setup guideline for some identity providers below:
**Okta**

**How do I add additional users to manage my account?**

In order to add an additional user to manage your account:

1. Log into OPSWAT Central Management console
2. Go to User Management.
3. Click on the **ADD NEW USER** button to add users to manage your account.

**Add New User**

**First Name**

Enter user's first name

**Last Name**

Enter user's last name

**Email**

Enter user's email

**User's Role**

Administrator

[ADD]
4. Enter the user’s email address and the role you wish them to have: **Administrator** or **Read Only** in the drop-down menu.

5. Click on the **ADD** button. You will then receive a temporary password for the new user. They can log into **OPSWAT Central Management** console with this password.

**Add New User**

User huyho89@opswat.com has been successfully added with the temporary password as below

![Temporary Password]

Once a user has been invited or added to your account, you will have the ability, through this console, to see:

- The **date** the user was invited
- The **status** of the invitation
- The **role** selected for the user

You are able to click **Update/Delete users** at any time.

Note that this feature is only available for paid accounts.

**How do I add or change my PIN?**

You can change your PIN to confirm your action when you make changes or push commands to devices on your User Information page as follows
1. Go to the User Information page by clicking your account name at the top-right corner.

2. Enter your current PIN and new PIN.

3. Click SAVE.

If you forget your PIN at any time, you can request a new temporary PIN which will be created and sent to you. To do this:

1. Go to the User Information page by clicking your account name at the top right corner.

2. Click Forgot your PIN? to reset your PIN.

3. Enter the correct set of question and answer and select RESET PIN.
4. Enter your new PIN and select CREATE PIN to confirm your choice.
Your new PIN will take effect immediately.

⚠️ Only new administrator accounts created from version 7.3.0+ can have their PIN reset.

Is there a way to change a User's role?

To update the role type of a User (i.e. from Administrator to Read Only), please follow the below steps:

1. Log into OPSWAT Central Management console.
2. Navigate to User Management.
3. Select the users that you wish to update.
4. Click on the Update button and select a role you would like to assign to them and then click Update.

Which versions of OPSWAT Products are compatible with OPSWAT Central Management v7?

- Metadefender Products

Notes:
OPSWAT Central Management v7.1.0 does not check the validity of OPSWAT Products' versions remote installed by the user. If an OPSWAT Product's version incompatible with OPSWAT Central Management v7 is distributed, that OPSWAT Product will not be able to communicate with the server.

Metadefender Products
Minimum supported Kiosk version is 4.3.0
Minimum supported Core version is 4.14.3
Minimum supported Vault version is 1.3.3
Minimum supported Email version is 4.7.2
Minimum supported ICAP version is 4.7.1
Minimum supported CM5 version is 5.2.7

<table>
<thead>
<tr>
<th>CM version</th>
<th>3 latest Kiosk versions tested</th>
<th>3 latest Core versions tested</th>
<th>3 latest Vault versions tested</th>
<th>3 latest Email versions tested</th>
<th>3 latest ICAP versions tested</th>
<th>3 latest CM5 versions tested</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1.0</td>
<td>4.3.0, 4.3.1, 4.3.2</td>
<td>4.14.3, 4.15.0, 4.15.1</td>
<td>1.3.3, 1.3.4, 1.3.5</td>
<td>Not supported</td>
<td></td>
<td>5.2.7</td>
<td></td>
</tr>
<tr>
<td>7.1.1</td>
<td>4.3.1, 4.3.2, 4.3.3</td>
<td>5.15.1, 4.15.2, 4.16.0</td>
<td>1.3.4, 1.3.5, 1.3.6</td>
<td>Not supported</td>
<td></td>
<td>5.2.7, 5.2.8, 5.2.9</td>
<td></td>
</tr>
<tr>
<td>7.2.0</td>
<td>4.3.3, 4.3.4, 4.3.5</td>
<td>4.16.0, 4.16.1, 4.16.2</td>
<td>1.3.6, 1.3.7, 1.3.8</td>
<td>4.7.2, 4.7.3</td>
<td></td>
<td>5.2.8, 5.2.9, 5.3.0</td>
<td>• For Email, just support online mode.</td>
</tr>
<tr>
<td>7.3.0</td>
<td>4.3.5, 4.3.6, 4.3.7</td>
<td>4.16.1, 4.16.2, 4.16.3</td>
<td>1.3.7, 1.3.8, 1.3.9</td>
<td>4.7.3, 4.7.4, 4.7.5</td>
<td></td>
<td>5.2.8, 5.2.9, 5.3.0</td>
<td></td>
</tr>
<tr>
<td>CM version</td>
<td>3 latest Kiosk versions tested</td>
<td>3 latest Core versions tested</td>
<td>3 latest Vault versions tested</td>
<td>3 latest Email versions tested</td>
<td>3 latest ICAP versions tested</td>
<td>3 latest CM5 versions tested</td>
<td>Notes</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------</td>
<td>------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>7.4.0</td>
<td>4.3.6, 4.3.7, 4.3.8</td>
<td>4.16.2, 4.16.3, 4.17.0.1</td>
<td>1.3.8, 1.3.9, 1.4.1</td>
<td>4.7.5, 4.7.6, 4.7.7</td>
<td>4.7.1, 4.7.2</td>
<td>5.2.8, 5.2.9, 5.3.0</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
- For Email, just support online mode.
- For Core, online module update is supported on Core version 4.16.0+
8. Legal

- Copyright
- MetaDefender Export Classification

Copyright

DISCLAIMER OF WARRANTY

OPSWAT Inc. makes no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages.

COPYRIGHT NOTICE

OPSWAT, OESIS, Metascan, Metadefender, AppRemover and the OPSWAT logo are trademarks and registered trademarks of OPSWAT, Inc. All other trademarks, trade names and images mentioned and/or used herein belong to their respective owners.

No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means (photocopying, recording or otherwise) without prior written consent of OPSWAT Inc. No patent liability is assumed with respect to the use of the information contained herein. While every precaution has been taken in the preparation of this publication, OPSWAT Inc. assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

MetaDefender Export Classification

MetaDefender United States Export Classification Number (ECCN) is 5D002, subparagraph c.1 Exports and re-exports of MetaDefender are subject to U.S. export controls and sanctions administered by the Commerce Department’s Bureau of Industry and Security (BIS) under the U.S. Export Administration Regulations (EAR).

This page provides export control information on MetaDefender. MetaDefender provides encryption features that are subject to the EAR and other U.S. laws. These features have been approved for export from the United States, subject to certain requirements and limitations. You may find the information on this page useful for determining exportability to particular countries or parties, and for completing export or shipping documentation, recordkeeping, or post-shipment reporting.
Although we provide the information on this page, you remain responsible for exporting or re-exporting MetaDefender in accordance with U.S. law. We encourage you to seek appropriate legal advice and/or consult the EAR and the BIS Information Technology Controls Division before exporting, re-exporting, or distributing MetaDefender. The information provided here is subject to change without notice.