# Table of Contents

## About this guide

1. *Quick Start with Central Management*  
   1.1. Product installation  
      - Operating system invariant initial steps  
      - Operating system variant installation steps  
      - Operating system invariant final steps  
      - Next steps  
      - 1.1.1. Basic configuration wizard  
   1.2. License activation  
   1.3. Start using Central Management

## 2. Installing or upgrading Central Management

2.1. System requirements  
   - Operating system  
   - Minimum hardware requirements  
   - Directories  
   - Ports that must be available  
   - Network throughput  
   - Browser requirements

2.2. Installing Central Management  
   - Installation steps:  
   - Installation  
   - Installation notes  
   - 2.2.1. Command line installation  
   - 2.2.2. Installing Central Management using the installation wizard
3.7. Hardening
   Changing the default password
   Running the service as an unprivileged account

4. Operating Central Management

4.1. Overview

4.2. Dashboard
   Overview page
   Update history
   Config history
   Processing history
   Unhealthy instances

4.3. Managing groups, products and instances
   4.3.1. Groups
   4.3.2. Products
   4.3.3. Instances

4.4. Inventory management
   Overview
   Functions

4.5. Product integration limitations
   General
   MetaDefender Core
   MetaDefender Email Security
   MetaDefender ICAP Server
   MetaDefender Kiosk

4.6. Regular maintenance
   Checking engines/databases health

4.7. Central license management
   High level architecture overview

4.8. High availability
   Cold swap example

5. Release notes
Previous releases

5.1. Changelog

Version 5.3.0
Version 5.2.9
Version 5.2.8
Version 5.2.7
Version 5.2.6
Version 5.2.5
Version 5.2.4
Version 5.2.3
Version 5.2.2
Version 5.2.1
Version 5.2.0
Version 5.1.2
Version 5.1.1
Version 5.1.0
Version 5.0.0RC
Version 4.2.0
Version 4.1.0
Version 4.0.1
Version 4.0.0

5.2. Archived release notes

5.2.1. Version 5.1.1
5.2.2. Version 5.1.2
5.2.3 Version 5.2.0
5.2.4 Version 5.2.1
5.2.5 Version 5.2.2
5.2.6 Version 5.2.3
5.2.7 Version 5.2.4
5.2.8 Version 5.2.5
5.2.9 Version 5.2.6
5.2.10 Version 5.2.7
5.2.11 Version 5.2.8
5.2.12 Version 5.2.9

6. Errata
8. Knowledge Base Articles

How long is the support life cycle for a specific version/release of MetaDefender Central Management v5? 204

How to create support package for Central Management? 205
   Linux 205
   Windows 206
   Content of the created package 206

How to read the Central Management log? 207
   Files 207
   Format 207
   Severity levels of log entries 207

Installing Central Management on Debian 9 208
   Symptom 208
   Reason 208
   Resolution 208

What you need to check if your Web Management Console is not responding after you installed the Central Management 211

What you need to do if you see too many TIME_WAIT sockets 212
   How to detect 212
   Solution 212
   Technical Insights 212
About this guide

This guide is intended to provide the information you need to:

- Install, configure, and manage Central Management v5.x;
- Learn about new and updated features, and bug fixes on each Central Management release (i.e. each product version's release notes);
- Learn about frequently asked questions and additional concepts through our library of knowledge base articles.

While we offer the option to download this guide as a PDF file, the contents are 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 most recent and most comprehensive version of the guide.
About Central Management

Central Management is the control room for the following OPSWAT products:

- MetaDefender Core v4 versions from v4.7.0,
- MetaDefender Email Security v4 versions from v4.1.3,
- MetaDefender ICAP Server v4 versions from v4.2.1,
- MetaDefender Kiosk v4 versions from v4.2.0,
- MetaDefender Client versions from v4.1.0,
- MetaDefender Core v3 and MetaDefender Core v4 versions before v4.7.0 with limited functionality.

The purpose of this guide is to introduce you to the flexible configuration options available in Central Management.
Feedback

For comments and questions regarding this document, please contact OPSWAT on the Support tab at https://portal.opswat.com/.
1. Quick Start with Central Management

This quick start guide describes the basic steps for installing Central Management. This guide assumes that the deployment machine has working Internet connection.

- 1.1. Product installation
- 1.2. License activation
- 1.3. Start using Central Management

1.1. Product installation

- Operating system invariant initial steps
- Operating system variant installation steps
  - Ubuntu or Debian
  - Red Hat Enterprise Linux or CentOS
  - Windows
- Operating system invariant final steps
- Next steps

Before starting the installation please make sure your server computer or virtual machine meets the minimum hardware and software requirements.

Operating system invariant initial steps

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

2. Upload the installation package to your server computer.

3. Follow the installation steps according to your operating system (and distribution).
Operating system variant installation steps

Ubuntu or Debian

1. Install the product with (filename is the package you downloaded from the OPSWAT Portal):

   ```bash
   $ sudo dpkg -i <filename>
   ```

2. If `dpkg` shows error messages about missing dependencies you should execute:

   ```bash
   $ sudo apt-get install -f
   ```

3. Finalize the installation following the final steps below.

Red Hat Enterprise Linux or CentOS

1. Install the product with (filename is the package you downloaded from the OPSWAT Portal):

   ```bash
   $ sudo yum install <filename>
   ```

2. Finalize the installation following the final steps below.

Windows

1. Install the product executing the MSI downloaded from the OPSWAT Portal.

2. Finalize the installation following the final steps below.

Operating system invariant final steps

1. Open a web browser and point to (\(<\text{server name or IP}>\) is the DNS name or IP address of your server):

   ```http://<server name or IP>:8018```
2. The **basic configuration wizard** will guide you through the rest of the basic setup.

Next steps

If license activation was skipped during the **basic configuration wizard**, then follow the license activation instructions on **1.2. License activation**

For more information on Installation procedures see **2.2. Installing Central Management**

1.1.1. **Basic configuration wizard**

- Introduction

- Basic configuration steps
  - End-User License Agreement
  - Admin User Setup
  - License activation
  - Wizard completion

- Transport Layer Security

- User directories
Introduction

When trying to access the Web Management Console for the first time, you are to complete a basic configuration wizard in order to be able to use the product. The Web Management Console will be available only after you have successfully finished this wizard.

To start the wizard click CONTINUE.

⚠️ Sensitive information

This 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

End-User License Agreement

In the first page you can find the End-User License Agreement. You have to accept the terms before moving on. Please read through the EULA carefully and if you agree with it, check I ACCEPT THE TERMS IN THE LICENSE AGREEMENT and click NEXT to continue.

Admin User Setup

The next step is to set up an administrator account. This account will be the first one being able to access the Web Management Console and to create accounts for other users. You have to fill all fields in this page to be able to move forward. When you are done, click NEXT to continue.

User directory

The administrator account, that is created via the basic configuration wizard, is always added to the LOCAL user directory as a member.

The following information is required for the administrator account:
<table>
<thead>
<tr>
<th>ACCOUNT NAME</th>
<th>The unique name of the account that is used at the time of login and in log messages for accountability.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCOUNT DISPLAY NAME</td>
<td>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.</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>Password of the user bound to this account that is used at the time of login.</td>
</tr>
</tbody>
</table>
| **⚠️ Passwords sent clear-text** | As long as TLS is not configured for the basic configuration wizard, passwords are sent clear-text over the network and may be disclosed to unauthorized parties. As a mitigation action:  
1. Either use the wizard on *localhost* or on a direct network connection, or  
2. Enable TLS as soon as possible and change the password immediately if it has already been set. |
| EMAIL | Email address of the person bound to this account. |
License activation

For license activation details see 2.4.1. Activating licenses.

Wizard completion

After you have completed every steps you are ready to finish the wizard and start using the product. Click the FINISH button to complete the wizard.

⚠️ The product's service will be restarted and the browser will be redirected to the Web Management Console. This could take several seconds.

You can login to the Web Management Console with the administrator user that have just been created in the previous steps.
Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol that provides communications security over a computer network. Websites, like the Web Management Console, are able to use TLS to secure all communications between their servers and web browsers.

The TLS protocol aims primarily to provide confidentiality (privacy) and data integrity between two communicating computer applications.

⚠️ No TLS for the wizard

By default, TLS is not enabled for the basic configuration wizard. As a consequence sessions between the wizard's backend and the browser may be insecure.

💡 Performing the same steps as for the Web Management Console, it is possible to set up TLS for the basic configuration wizard. Remember completing the TLS setup before launching the wizard.

For instructions to set up TLS see 3.5. Configuring TLS.

User directories

Users can be organized into separate user directories. User directories help to enforce certain login policies.

For further details about user directories see the User directories tab section in 3.2. User management.
1.2. License activation

To activate your installation go to the **Settings > License** menu in the Web Management Console. If you have no valid license, you will only see your installation's **Deployment ID**. You will also see a warning in the Web Management Console header.

Perform the following steps:

1. Press the ACTIVATE button to bring up the *Activation* dialog, where you should choose from the available modes:
   - **ONLINE**: The product will contact the OPSWAT license server online, and acquire its license based on your *Activation key* and *Deployment ID*,
   - **OFFLINE**: A manually acquired license file must be uploaded via the Web Management Console,

2. Select the desired option,
3. Follow the on-screen instructions,
4. Finally press the SEND button.
When the hardware information changes (for example the MAC address changes because the product runs in a virtual machine) the license get automatically reactivated on the first update attempt.

After successful activation, the product will start downloading the latest available scan engines and malware databases. You can follow the status of the scan engine installation on the **Inventory > Engines** page.

For detailed license activation instructions see **2.4. Central Management licensing**.

### 1.3. Start using Central Management

After installation and activation, instances can be started to be managed.

1. Go to **Groups** menu and click ADD NEW GROUP,
2. Specify the NAME for the group, an click CREATE GROUP,
3. The newly created group is opened automatically,
4. Click ADD INSTANCE to start adding instances.

For detailed instructions see **4.3. Managing groups, products and instances**.
2. Installing or upgrading Central Management

This part describes the installation and upgrade process of Central Management in details.

- 2.1. System requirements
- 2.2. Installing Central Management
- 2.3. Upgrading Central Management
- 2.4. Central Management licensing

2.1. System requirements

- Operating system
- Minimum hardware requirements
- Directories
  - Linux
  - Windows
  - Scan engine resources storage
- Ports that must be available
- Network throughput
- Browser requirements

⚠️ Confirm that your system meets the minimum requirements listed below before installing Central Management.

**Operating system**

⚠️ Only 64-bit platforms are supported.

The following operating systems are supported:

<table>
<thead>
<tr>
<th>OS family</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS</td>
<td>6.6 or newer, 7.0 or newer</td>
</tr>
</tbody>
</table>
## Minimum hardware requirements

Only 64-bit platforms are supported.

<table>
<thead>
<tr>
<th>RAM</th>
<th>2 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDD</td>
<td>2 GB + ~500MB * [number of managed scan engines]</td>
</tr>
</tbody>
</table>

## Directories

This section contains references to directories used by Central Management.

In further sections of this user guide the `directory reference` is used instead of the actual directory to refer to locations on the system disk.

### Linux

Depending on whether it is a program, a configuration or something else, files are installed to separate directories under Linux.

<table>
<thead>
<tr>
<th>Directory reference</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service control</td>
<td><code>/etc/init.d</code></td>
</tr>
<tr>
<td>Log rotation configuration</td>
<td><code>/etc/logrotate.d</code></td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Directory reference</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>/etc</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>/usr/bin</td>
</tr>
<tr>
<td>Libraries</td>
<td>/usr/lib</td>
</tr>
<tr>
<td>Utilities</td>
<td>/usr/sbin</td>
</tr>
<tr>
<td>Documentation</td>
<td>/usr/share/doc</td>
</tr>
<tr>
<td>Manual pages</td>
<td>/usr/share/man</td>
</tr>
<tr>
<td>Variable libraries</td>
<td>/var/lib</td>
</tr>
<tr>
<td>Log files</td>
<td>/var/log</td>
</tr>
<tr>
<td>System information</td>
<td>/var/run</td>
</tr>
</tbody>
</table>

**Windows**

Everything, except logs, is placed under the installation folder that can be customized during the installation.

<table>
<thead>
<tr>
<th>Directory reference</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation folder</td>
<td>C:\Program Files\OPSWAT\Metadefender Central Management</td>
</tr>
<tr>
<td>Event log files</td>
<td>C:\Windows\System32\WinEvt\Logs</td>
</tr>
<tr>
<td>Log file</td>
<td>Log file is not written by default. For details see the Windows section in 3.1.2. Central Management server configuration file.</td>
</tr>
</tbody>
</table>
Scan engine resources storage

Central Management uses a subdirectory under the following directory references for storing scan engine resources:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Variable libraries</td>
</tr>
<tr>
<td>Windows</td>
<td>Installation folder</td>
</tr>
</tbody>
</table>

⚠️ The partition holding these directories must have the appropriate free space. For further details see Minimum hardware requirements.

Ports that must be available

<table>
<thead>
<tr>
<th>Direction</th>
<th>Component / Service</th>
<th>Port</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Central Management Web Management Console and REST interface</td>
<td>8018</td>
<td>Customizable; adjust accordingly if modified.</td>
</tr>
</tbody>
</table>

Network throughput

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Management Console access</td>
<td>0.1 Mbps</td>
<td>5 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Management Console will work with any slow network but it is practically unusable under 1 Mbps.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Managed instance connection

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.1 Mbps</td>
<td>5 Mbps</td>
</tr>
</tbody>
</table>

Browser requirements

One of the following desktop browsers is required to use the Web Management Console:
1. Latest two Chrome versions
2. Latest two Firefox versions
3. Latest two Safari versions
4. Latest two Microsoft Edge versions
5. Internet Explorer 11

⚠️ Mobile layouts are not supported yet.

2.2. Installing Central Management

Installation steps:

1. Download the package of your choice from the **OPSWAT portal**,
2. Install the package on your computer via the **command line** or via the **installation wizard**,
3. Open a web browser and point to (<server name or IP> is the DNS name or IP address of the server; the port number may be customized during the installation):

   [http://<server name or IP>:8018](http://<server name or IP>:8018)

4. Complete the required steps of the **basic configuration wizard**,
5. **Activate** this deployment to use its features.

Installation

- 2.2.1. Command line installation
- 2.2.2. Installing Central Management using the installation wizard

Installation notes

- If the Central Management package dependencies are not installed on your system you may need to have a working Internet connection or you may have to provide the Installation media during the installation. Consult your operating system documentation on how to use installation media as a package repository.
- During installation the databases might need to be upgraded. This could take noticeable time.
2.2.1. Command line installation

Preliminary notes

- If Central Management package dependencies are not met on your system you may need to have a working Internet connection or you may have to provide the installation media during the installation. Consult your operating system documentation on how to use installation media as a package repository.

**Debian / Ubuntu package (.deb)**

```sh
sudo dpkg -i <file name> || sudo apt-get install -f
```

**Red Hat Enterprise Linux / CentOS package (.rpm)**

```sh
sudo yum install <file name>
```

**Windows package (.msi)**

On Windows systems it is possible to install the product by running the corresponding .msi file. From command line interface it is also possible to install the product by executing

```
msiexec /i <msi file name> <option key>=<option value>
```

where the possible *option keys* and their default *option values* are the following:

<table>
<thead>
<tr>
<th>Key</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESTADDRESS</td>
<td>0.0.0.0</td>
<td>REST interface binding address</td>
</tr>
<tr>
<td>RESTPORT</td>
<td>8018</td>
<td>REST interface binding port</td>
</tr>
</tbody>
</table>

For details on using msiexec please consult the Windows installer documentation.

2.2.2. Installing Central Management using the installation wizard
The installation wizard is available for Windows installations only (.msi file).

Perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Welcome message</td>
</tr>
<tr>
<td>2</td>
<td>Accept the license agreement</td>
</tr>
<tr>
<td>Step</td>
<td>Screenshot</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>3</td>
<td>Select setup type</td>
</tr>
</tbody>
</table>

```
3 Select setup type

Choose Setup Type
Choose the setup type that best suits your needs

Simple
Installs the most common program features. Recommended for most users.

Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><img src="image" alt="MetaDefender Central Management Setup" /></td>
</tr>
</tbody>
</table>

**Custom Setup**

To change default installation directory click on browse button below.

Location: C:\Program Files\OPSWAT\Metadefender Central Management\  
Browse...

| 5    | ![MetaDefender Central Management Setup](image) |

**MetaDefender Central Management server setup**

The setup wizard setup the MetaDefender Central Management server account.

Please enter MetaDefender Central Management web server and REST server IP address and port.

Users can access MetaDefender Central Management web server and REST services over this IP and port address. To make the service available on any IP of this computer set ‘*’, otherwise specify accordingly.

- Address: 
- Port: 3018
<table>
<thead>
<tr>
<th>Step</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><img src="image1.png" alt="Screenshot" /></td>
</tr>
</tbody>
</table>
| Commit installation | Ready to Install
The setup wizard is ready to begin the Custom installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard. |
| 7    | ![Screenshot](image2.png) |
| Installation in progress |  |
2.3. Upgrading Central Management

To upgrade from a former version of Central Management a simple installation of the latest version is enough.

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

**Clean re-installation**

To install the product from scratch instead of an upgrade, perform the following steps:

1. Uninstall previous version
2. Delete installation directories (see 2.1. System requirements for directories in use)
3. Clean-up Windows registry (applies for Windows installations only)
4. Install the current version
WARNING! Potential data loss
In case of a clean reinstall, data from the previous installation will be lost.

Legacy instances
Metadefender Core versions before v4.7.0 are considered as legacy instances.
On upgrade, all instances will be moved to group called Legacy regardless of version.

- From version v4.7.0, instances can be moved to other group by removing from Legacy group then adding to the desired one.
- Legacy instances (before v4.7.0) can be only added to Legacy group and cannot be moved to other group.
- Configuration of legacy instances cannot be updated from Central Management.

2.4. Central Management licensing
In order to use Central Management you need to activate the product.

- 2.4.1. Activating licenses
- 2.4.2. Checking Central Management license

2.4.1. Activating licenses

- Initial steps
- Online activation
- Offline activation
  - Offline activation details
- Notes

Drive administrator for activation
Unless the license of Central Management is activated, the Web Management Console will start with opening the Activation dialog at every administrator login:
Initial steps

1. To activate your installation go to the Settings > License menu in the Web Management Console. If you have no valid license, you will only see your installation's Deployment ID. You will also see a warning in the Web Management Console header.
2. Press the ACTIVATE button to bring up the Activation dialog, where you should choose from the available modes:

   - **ONLINE**: The product will contact the OPSWAT license server online, and acquire its license based on your Activation key and its Deployment ID.
   - **OFFLINE**: You can upload a manually acquired license file. Follow the instructions displayed.

   For successful activation a valid activation key is needed regardless of what mode is chosen.

**Online activation**

With internet connection on the server, Central Management may be activated directly using the Activation key received at the time of receiving the product. Perform the following steps for an online activation:

1. On the Activation page choose ONLINE as ACTIVATION MODE.
2. Fill the ACTIVATION KEY field with your key.

3. Specify the NUMBER OF MANAGED INSTANCES.

⚠️ License usage

Please note, you can use your license for multiple Central Management installations, provided that the sum of specified number of managed instances does not exceed the number that the license allows.

⚠️ Unlimited license

For unlimited license, when "as many as license allows" is chosen, CM will be activated with 999 instances.

4. Click the SEND button to activate.

ℹ️ If your license becomes invalid or expired, you will see a RE-ACTIVATE button. After clicking it, the product tries to activate the license with the formerly entered activation information.
**Offline activation**

With no internet connection on the server Central Management may be activated indirectly from a different machine, that has internet connection. The *Deployment ID* of Central Management and the *Activation key* received at the time of receiving the product will be required. Follow the steps on the screen to activate the product offline.

![Activation Screen](image)
### Offline activation details

1. Log on to [https://portal.opswat.com/activation](https://portal.opswat.com/activation)

2. Select *OPSWAT Central Management* as *MetaDefender Package*

3. Fill in the requested information about your deployment

   - **MetaDefender Package**
     - Select: *OPSWAT Central Management*
   
   - **Activation Key** *(must* be filled)*
     - Type your Activation Key
   
   - **Requested Number Of Agents**
     - Type: *100*
   
   - **Deployment ID** *(must* be filled)*
     - Type: *MCMSbBbY4ARJM02z1xTXBtEFAYpAtM8z41kn*

   - **Optional Description**
     - *This helps you to identify this deployment on OPSWAT License portal*

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

<table>
<thead>
<tr>
<th>MetaDefender Package</th>
<th>OPSWAT Central Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Key</td>
<td></td>
</tr>
<tr>
<td>Requested Number Of Agents</td>
<td>100</td>
</tr>
<tr>
<td>Deployment ID</td>
<td>MCMSbBbv4ARJMC2z1xTRBtEFAVpArM8z41kn</td>
</tr>
<tr>
<td>Optional Description</td>
<td>This helps you to identify this deployment on OPSWAT License portal</td>
</tr>
</tbody>
</table>

**Request Unlock Key**

**Please click this link to download license file.**

**Download Unlock Key**

5. Click the **Download Unlock Key** link and save the activation file.
Go back to Central Management’s Web Management Console. Browse for the activation file and click the SEND button.
Notes

⚠️ If you activated your installation, but your license becomes invalid or expired, you will see a RE-ACTIVATE button. After clicking it, the product tries to activate the license with the formerly entered activation information.

2.4.2. Checking Central Management license

User menu pane

Basic license information is always visible in the user menu pane on the lower left side of the screen. The following information is available

- Product version
- License expiration: last day of license validity
## License menu

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

The following information is available:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product ID</td>
<td>Product identification as on your order.</td>
</tr>
<tr>
<td>Product name</td>
<td>Product name as on your order.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Last day of license validity.</td>
</tr>
<tr>
<td>Max instances</td>
<td>Maximum number of MetaDefender Core, Email Security, ICAP Server and Kiosk instances that are allowed to be managed by this Central Management deployment.</td>
</tr>
<tr>
<td>Max client instances</td>
<td>Maximum number of MetaDefender Client instances that are allowed to be managed by this Central Management deployment.</td>
</tr>
<tr>
<td>Identification</td>
<td>Identification of this installation.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Deployment ID</td>
<td></td>
</tr>
<tr>
<td>Activation key</td>
<td>The activation key (only if activated online).</td>
</tr>
</tbody>
</table>
3. Configuring Central Management

- 3.1. Central Management configuration
- 3.2. User management
- 3.3. Update settings
- 3.4. Logging
- 3.5. Configuring TLS
- 3.6. Configuring proxy settings
- 3.7. Hardening

3.1. Central Management configuration

The Central Management configuration is separated into two parts. The basic server configurations are stored in the configuration files. Other configuration values can be set via the Web Management Console.

- 3.1.1. Web Management Console
- 3.1.2. Central Management server configuration file

3.1.1. Web Management Console

After installation and completion of the basic configuration wizard, the Web Management Console is available at:

http://<server name or IP>:<port>/

where <server name or IP> is the fully qualified domain name or IP address; and <port> is the port number of the system where the REST service is bound. Both the IP address and the port number may be customized during the installation.

Administrator account

After installing the product and completing the basic configuration wizard, the administrator account –created in the basic configuration wizard– is available for login.
As long as TLS is not configured for the Web Management Console, passwords are sent clear-text over the network. For details see Transport Layer Security.

Every change made in the product's configuration via the Web Management Console is applied when you select SAVE SETTINGS or OK, except if the change cannot be applied.

If not configured otherwise, the Central Management REST service is listening on port 8018.

Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol that provides communications security over a computer network. Websites, like the Web Management Console, are able to use TLS to secure all communications between their servers and web browsers.

The TLS protocol aims primarily to provide confidentiality (privacy) and data integrity between two communicating computer applications.

For instructions to set up TLS see 3.5. Configuring TLS.
3.1.2. Central Management server configuration file

Linux

The configuration file for the server is located in `/etc/mdcentralmgmt/mdcentralmgmt.conf`.

After modifying the server configuration file you must restart the Central Management service in order for the changes to take effect. You should use the distribution-standard way to restart the `mdcentralmgmt` service.

[global] section

<table>
<thead>
<tr>
<th>parameter</th>
<th>default value</th>
<th>required</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>restaddress</td>
<td>0.0.0.0</td>
<td>required</td>
<td>One of the IP addresses of the computer that runs the product to serve REST API and web user interface (0.0.0.0 means all interface)</td>
</tr>
<tr>
<td>restport</td>
<td>8018</td>
<td>required</td>
<td>Designated port number for the web and REST interface</td>
</tr>
</tbody>
</table>

[logger] section

<table>
<thead>
<tr>
<th>key</th>
<th>default value</th>
<th>required</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logfile</td>
<td>/var/log/mdcentralmgmt/mdcentralmgmt.log</td>
<td>optional</td>
<td>Full path of a logfile to write log messages to</td>
</tr>
<tr>
<td>loglevel</td>
<td>info</td>
<td>optional</td>
<td>Level of logging. Supported values are: debug, info, warning, error</td>
</tr>
<tr>
<td>syslog</td>
<td></td>
<td>optional</td>
<td>Switch on logging to a local ('local') or remote ('protocol://hostname:port') syslog server</td>
</tr>
<tr>
<td>syslog_level</td>
<td></td>
<td>optional</td>
<td>Level of logging. Supported values are: debug, info, warning, error</td>
</tr>
<tr>
<td>override</td>
<td></td>
<td>optional</td>
<td></td>
</tr>
</tbody>
</table>
You should set both of syslog and syslog_level or none of them and you should set both of logfile and loglevel or none of them.

For override a list of log message ids needed with optionally a level. If there is no level set for an id, it will be displayed on every occasion. e.g.: "1723,663:info" means id 1723 dump message will be displayed every time and id 663 warning message is reduced to info level.

**Windows**

The configuration for the server is located in **Windows Registry**

After modifying the server configuration file you must restart the Metadefender Central Management service in order for the changes to take effect.

Default logging target is Windows event log with default level of info (see below).

**HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Centralmgmt\global**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default value</th>
<th>type</th>
<th>required</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>restaddress</td>
<td>0.0.0.0</td>
<td>string</td>
<td>required</td>
<td>One of the IP addresses of the computer that runs the product to serve REST API and web user interface (0.0.0.0 means all interface)</td>
</tr>
<tr>
<td>restport</td>
<td>8018</td>
<td>string</td>
<td>required</td>
<td>Designated port number for the web and REST interface</td>
</tr>
</tbody>
</table>
### HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\CentralMgmt\logger

<table>
<thead>
<tr>
<th>key</th>
<th>default value</th>
<th>type</th>
<th>required</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logfile</td>
<td>string value</td>
<td>optional</td>
<td></td>
<td>Location of a logfile to write log messages to</td>
</tr>
<tr>
<td>loglevel</td>
<td>string value</td>
<td>optional</td>
<td></td>
<td>Level of logging. Supported values are: debug, info, warning, error</td>
</tr>
<tr>
<td>wineventlog_level</td>
<td>info</td>
<td>string value</td>
<td>optional</td>
<td>Level of logging. Supported values are: debug, info, warning, error</td>
</tr>
<tr>
<td>syslog</td>
<td>string value</td>
<td>optional</td>
<td></td>
<td>Value can only be in form of 'udp://&lt;hostname&gt;:&lt;port&gt;'</td>
</tr>
<tr>
<td>syslog_level</td>
<td>string value</td>
<td>optional</td>
<td></td>
<td>Level of logging. Supported values are: debug, info, warning, error</td>
</tr>
<tr>
<td>override</td>
<td>string value</td>
<td>optional</td>
<td></td>
<td>override specific log ids to display them on another level e.g.: &quot;1723:error,663:info&quot;</td>
</tr>
<tr>
<td>cef</td>
<td>false</td>
<td>string value</td>
<td>optional</td>
<td>If true, the log format is Common Event Format.</td>
</tr>
</tbody>
</table>

You should set both of syslog and syslog_level or none of them and you should set both of logfile and loglevel or none of them.

### 3.2. User management

- Users and groups tab
  - Legacy default user
  - Functions
    - Add new user from a Local type user directory
      - API keys
    - Add new users from an LDAP type or Active Directory type user directory
To manage the users of the product, go to the **Settings > User Management** menu in the Web Management Console.

**Users and groups tab**

The USERS AND GROUPS tab lists the existing users, LDAP groups and Active Directory groups in the system.
Legacy default user

Previous versions of the product created a default user during the installation with the following credentials and parameters. This default user may still exist if the product was upgraded from previous versions.

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Name</th>
<th>Email</th>
<th>Roles</th>
<th>User directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>admin</td>
<td>Administrator</td>
<td>admin@localhost</td>
<td>Administrators</td>
<td>LOCAL</td>
</tr>
</tbody>
</table>

Functions

Besides listing existing users, LDAP and AD groups, the USERS AND GROUPS tab provides the following functions:

- Add new user, LDAP or AD group
- Modify (and view) existing user’s, LDAP or AD group's properties
- Delete existing user, LDAP or AD group
Add new user from a Local type user directory

To add a new user from a Local type user directory click the ADD NEW USER button and select a Local type user directory in the USER DIRECTORY drop down list.

The field ASSIGN TO ROLES lists all the roles that are assigned to this user. See section Assign roles to a user, LDAP group or Active Directory group for details about role assignment.

⚠️ As long as TLS is not configured for the Web Management Console, passwords are sent clear-text over the network. For details see Transport Layer Security.

⚠️ If enhanced password policy is enabled for the user directory this user belongs to then the new password must fulfil the password complexity requirements listed at the Local type user directories section.

API keys

The APIKEY value provides access to the product's REST API for the user under editing with no authentication. If no such functionality is needed for the user then this field can be left blank.

There are two methods to create an APIKEY for a user:

1. Generate the APIKEY by using Generate link next to the APIKEY field,
2. Manually enter the APIKEY value; it must matches the following criteria:

### APIKEY validation criteria

- The length of the API key must be exactly 36 characters.
- It must contain numeric and lower case a, b, c, d, e and f letter characters only
  
  (e.g. "1x2y3z..." is invalid because of the x, y and z characters).
- It must contain at least 10 lower case a, b, c, d, e or f letter characters.
- It must contain at least 10 numeric characters.
- It is allowed to contain at most 3 consecutive lower case letter characters (e.g. "abcd1a2b3c..." is invalid because of the four consecutive letters).
- It is allowed to contain at most 3 consecutive numeric characters (e.g. "1234a1b2c3..." is invalid because of the four consecutive numeric characters).
Add new users from an LDAP type or Active Directory type user directory

To add a new user from an LDAP type or Active Directory type user directory click the ADD NEW USER button and select an LDAP type or Active Directory type user directory in the USER DIRECTORY drop down list. Select USER as the ACCOUNT TYPE.

Provide the name of the account in the ACCOUNT NAME field and click the FIND ACCOUNT button to look up the account in the LDAP or Active Directory. If the lookup succeeds then the ACCOUNT DISPLAY NAME and the DISTINGUISHED NAME fields are filled automatically.

⚠️ Do provide the account name precisely. There is no functionality to look up similar names or partial matches.

The field ASSIGN TO ROLES lists all the roles that are assigned to this user. See section Assign roles to a user, LDAP group or Active Directory group for details about role assignment.
Add new group from an LDAP type or Active Directory type user directory

The purpose of adding an LDAP or Active Directory group to the product is to assign role(s) to all the users in that LDAP or Active Directory group. The users of the LDAP or Active Directory group can authenticate with their LDAP or Active Directory credentials in the product’s Web Management Console and will be assigned with the roles assigned to the group.

To add a new group from an LDAP type or Active Directory type user directory click the ADD NEW USER button and select an LDAP type or Active Directory type user directory in the USER DIRECTORIES drop down list.

Select GROUP as the ACCOUNT TYPE.

Provide the name of the group in the ACCOUNT NAME field and click the FIND ACCOUNT button to look up the group in the LDAP or Active Directory. If the lookup succeeds then the ACCOUNT DISPLAY NAME and the DISTINGUISHED NAME fields are filled automatically.
Do provide the group name precisely. There is no functionality to look up similar names or partial matches.

The field ASSIGN TO ROLES lists all the roles that are assigned to all users of the selected group. See section Assign roles to a user, LDAP group or Active Directory group for details about role assignment.

Assign roles to a user, LDAP group or Active Directory group

Role(s) must be assigned to users, LDAP groups and Active Directory groups in order they can use the Web Management Console. The roles assigned to a certain user determine what pages that user can access in the Web Management Console and whether she can only read, or modify as well values on a page.

The field ASSIGN TO ROLES in the Add/assign new user(s) and Modify user dialogs lists all the roles that are assigned to the user.

The following is the role assignment policy:

1. At least one role must be assigned to a user, LDAP group or Active Directory group
2. Optionally multiple different roles can be assigned
   a. In this case the most permissive available right applies to each function.

   For details about the permissiveness of roles see the Roles tab section.

Example:

<table>
<thead>
<tr>
<th>Roles assigned</th>
<th>Effective permissions</th>
<th>No permission</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Read only permission</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security_auditor</td>
<td>Config history, Global settings</td>
<td></td>
</tr>
<tr>
<td>help_desk</td>
<td>Global settings</td>
<td>Config history</td>
</tr>
<tr>
<td>security_admin AND</td>
<td>Config history, Global settings</td>
<td></td>
</tr>
<tr>
<td>security_auditor</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Delete user

⚠️ Active sessions of the deleted user will be aborted at the time of the next interaction with the server.

Roles tab

Roles can be assigned to users. This simplifies controlling permissions. The Roles tab lists the existing roles in the system.

Default roles

After installation the following default roles are created with the following parameters:

<table>
<thead>
<tr>
<th>Rolename</th>
<th>Display name</th>
<th>Default member username</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Administrators</td>
<td>admin</td>
<td>FULL on all functions</td>
</tr>
<tr>
<td>Rolename</td>
<td>Display name</td>
<td>Default member username</td>
<td>Permissions</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>security_admin</td>
<td>Security administrators</td>
<td></td>
<td>FULL on Update history, Client history, Unhealthy instances, Group, Engines, Update settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>READ-ONLY on Global settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NONE on the rest</td>
</tr>
<tr>
<td>security_auditor</td>
<td>Security auditor</td>
<td></td>
<td>Read-only on all functions</td>
</tr>
<tr>
<td>help_desk</td>
<td>Help desk</td>
<td></td>
<td>READ-ONLY on Update history, Client history, Unhealthy instances, Group, Engines</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NONE on the rest</td>
</tr>
</tbody>
</table>

**Permissions**

Each role has a set of rights associated to it. Each of these rights represent the level of access to the appropriate function of the MetaDefender product's Web Management Console. A right can be set to one of three different values:

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONE</td>
<td>Users with this effective right have no right to access the given function of the MetaDefender product's Web Management Console. The menu belonging to the function is not displayed.</td>
</tr>
<tr>
<td>READ-ONLY</td>
<td>Users with this effective right are granted to access the given function for observation purposes only. Users of this role can, however, not effectuate any modifications or any change to the function.</td>
</tr>
<tr>
<td>FULL</td>
<td>Users with this effective right have full access to the given function, including viewing any data belonging to it and modifying its configuration.</td>
</tr>
</tbody>
</table>
Effective right

A single user may have multiple roles assigned to it. There may be cases, when one of the assigned roles of the user would prohibit, while the other assigned role of the user would permit a certain function. In this case the more permissive right will be effective.

<table>
<thead>
<tr>
<th>Right</th>
<th>More permissive</th>
<th>More restrictive</th>
</tr>
</thead>
<tbody>
<tr>
<td>FULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>READ-ONLY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NONE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See section Assign roles to a user, LDAP group or Active Directory group for details about assigning multiple roles to a single user.

Functions

Besides listing existing roles the Roles tab provides the following functions:

- Add new role
- Modify (and view) existing role
- Delete existing role

⚠️ The default role Administrators can not be deleted or modified.

Modify role

⚠️ The users' permissions won't be modified during the session, even if one of their roles are modified in the meantime.

For example:

1. A user is assigned to the role security_admin and has Full permissions on C onfig history
2. She can see Config history changes
3. During her session the Config history permissions are set to None for the security_admin role.
4. The logged in user can still select the Config history menu and can see the configuration changes there.

Then new permissions will be effective only after a logout and new login.

Delete role

⚠️ A role can not be deleted as long as it is assigned to any user.
As a consequence deleting a role can not affect active sessions of users.

User directories tab

Users can be organized into separate user directories. User directories help to enforce the following login policies:

1. Lockout after a number of consecutive failed login attempts
2. Disable logins for all users of the user directory

The Users tab lists the existing user directories in the system.
Default user directories

After installation two default user directories are created with the following parameters:

<table>
<thead>
<tr>
<th>User directory type</th>
<th>Name</th>
<th>Number of failed logins before lockout</th>
<th>Lockout time [minutes]</th>
<th>Enable enhanced password policy</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>LOCAL</td>
<td>3</td>
<td>5</td>
<td>False</td>
<td>This user directory can be used to add local user accounts to the system.</td>
</tr>
<tr>
<td>Local</td>
<td>SYSTEM</td>
<td>0</td>
<td>0</td>
<td>False</td>
<td>This user directory is used to add special, (e.g. machine-to-machine) user accounts to the system.</td>
</tr>
</tbody>
</table>

⚠️ This user directory is for system internal use, do not modify (delete, assign users, etc.) it manually.

Three types of user directories exist in MetaDefender products:
1. Local
2. LDAP
3. Active Directory

Local type user directories

Local type user directories allow creating users that locally exist on the MetaDefender product.

To protect user accounts of a local user directory against brute force password breaking attacks, the following policy settings may be applied to each local type user directory:

- **NUMBER OF FAILED LOGINS BEFORE LOCKOUT**: After this number of consecutive failed login attempts the account gets locked.
- **LOCKOUT TIME [MINUTES]**: The account remains locked for the given minutes.
When the lockout time elapses, the account lock gets released automatically.

Users with appropriate permission may release the account lock earlier using the RELEASE LOCKOUT button.

ENABLE ENHANCED PASSWORD POLICY: If enabled, then the following policy is enforced for new passwords:

**Enhanced password complexity policy**

- The password must be at least 8 characters long;
- The password must contain at least one of each
  - Upper case Latin letter character ([A-Z]),
  - Lower case Latin letter character ([a-z]),
  - Arabic numeral character ([0-9]);
- The password must not contain the user name.

**Active Directory type user directories**

Active Directory type user directories allow users defined in an Active Directory to access the MetaDefender product.

Active Directory type user directories do not provide the possibility to define login policies; these policies may be defined in the Active Directory directly.

**LDAP type user directories**

LDAP type user directories allow users defined in an LDAP directory to access the MetaDefender product.

LDAP type user directories do not provide the possibility to define login policies; these policies may be defined in the LDAP directory directly.

**Functions**

Besides listing existing user directories the USER DIRECTORIES tab provides the following functions:

- Add new user directory
- Modify (and view) existing user directory
- Delete existing user directory
- Enable or disable existing user directory
Unlock locked accounts

Add new Local type user directory

Click the ADD NEW USER DIRECTORY button and select Local in the USERDIRECTORY TYPE drop down list.

For explanation of the NUMBER OF FAILED LOGINS BEFORE LOCKOUT and LOCKOUT TIME [MINUTES] fields read the Local type user directories section.

Add new LDAP type or Active Directory type user directory

1. Click the ADD NEW USER DIRECTORY button and select LDAP or Active Directory in the USERDIRECTORY TYPE drop down list respectively. Learn more about the differences between LDAP and Active Directory type user directories.

2. Multiple LDAP or Active Directory servers can be configured to provide high availability of the directory services.
   a. Server preference:
      i. The configured servers are taken for a connection attempt in a top-bottom fashion.
b. Failover conditions

i. If the connection to a certain LDAP or AD server fails (for a reason other then authentication error) then

ii. The next server in the preference order is attempted.

![Diagram showing failover conditions]

C. Server properties

The following properties must be specified for each LDAP or AD server:

i. SERVER HOST: IP address or FQDN of the server

ii. SERVER PORT: The TCP port on which the directory service is listening
iii. ENCRYPTION: What kind of encryption to use when establishing the connection

1. None: No encryption, communication on a clear-text channel

   As long as ENCRYPTION field is set to None there is no encryption used between the MetaDefender product and the LDAP or Active Directory server. All passwords and other information are sent clear-text over the network.

   Use StartTLS or SSL as ENCRYPTION whenever possible.

2. StartTLS: The connection is established on a clear-text channel, then upgraded to TLS (TLS over LDAP)

3. SSL: The connection is established on a TLS encrypted channel (LDAP over TLS)

   For StartTLS and SSL type encrypted connections the LDAP or Active Directory server must authenticate itself with a certificate that's validity can be verified by the MetaDefender product. This can happen in basically two ways:

   a. Trusted certificate: the certificate's root certificate is issued by a trusted certificate authority (e.g. Comodo, Symantec, GoDaddy, GlobalSign, IdenTrust, DigiCert, StartCom, Entrust, Trustwave, Verizon, etc.) These root certificates are usually pre-installed in modern operating systems and as a result can be verified by the MetaDefender product.

   b. Self-signed certificate: the certificate (or it's root certificate) is added to the system as a trusted root certificate. For details about adding a certificate as a trusted root certificate, see the manuals of the operating system of your MetaDefender product. For your convenience here are the necessary commands for Windows and some Linux distributions (the path to the self signed certificate file is C: \Path\To\certificate.crt or /path/to /certificate.crt on Windows or Linux respectively):
3. Select whether to authenticate or not at the time of the bind request. Authentication at the time of the bind request is an additional security control for directory services like host based authentication at SSH. It may or may not be required by the server.

a. Selecting the ANONYMOUS BIND option will try to attempt to bind to the directory service with no username and password.

- If the ANONYMOUS BIND option is selected, then the values specified for BIND USERNAME and BIND PASSWORD are ignored, their text fields are disabled.

- Some LDAP and Active Directory servers may be configured to not permit anonymous bind requests.

b. Specify the BIND USERNAME and BIND PASSWORD values. These values must be the name as DN (distinguished name) and password of a user who has permissions to do searches in the directory.

- As long as TLS is not configured for the Web Management Console, passwords are sent clear-text over the network. For details see Transport Layer Security.

4. The USER BASE DN and the GROUP BASE DN values should provide the entries in the LDAP or Active Directory tree where user and group entity lookups should be started.

- For further LDAP specific property details see LDAP attributes.

- For further Active Directory specific property details see Active Directory attributes.

5. Click the TEST button to test the LDAP or Active Directory settings. If the test succeeds then the user directory can be added to the list with the ADD button.
Add user directory

USER DIRECTORY TYPE
Active Directory

NAME
NAME

ACTIVE DIRECTORY SETTINGS

SERVER HOST
PORT
ENCRIPTION

Add Server

ANONYMOUS BIND

BIND USERNAME
USERNAME

BIND PASSWORD
PASSWORD

USER BASE DN
USER BASE DN

GROUP BASE DN
GROUP BASE DN

ADD CANCEL TEST
### Add user directory

**USER DIRECTORY TYPE**

- **LDAP**

**NAME**

- **NAME**

**LDAP SETTINGS**

- **SERVER HOST**
- **SERVER PORT**
- **ENCRYPTION**

**Add Server**

- **ANONYMOUS BIND**

**BIND USERNAME**

- **USERNAME**

**BIND PASSWORD**

- **PASSWORD**

**USER BASE DN**

- **USER BASE DN**

**GROUP BASE DN**

- **GROUP BASE DN**

**LDAP USER SCHEMA SETTINGS**

- **USER OBJECT CLASS**
- **USER ACCOUNT ATTRIBUTE**
- **USER EMAIL ATTRIBUTE**
Differences between LDAP and Active Directory type user directories

From MetaDefender products' perspective LDAP directories are supersets of Active Directory directories. In other words, an Active Directory configuration can be specified using LDAP user directory type, setting certain properties to predefined values.

The following properties must be set to the following values to implement an Active Directory type user directory with LDAP type user directory.
<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER OBJECT CLASS</td>
<td>user</td>
</tr>
<tr>
<td>USER ACCOUNT ATTRIBUTE</td>
<td>samaccountname</td>
</tr>
<tr>
<td>USER EMAIL ATTRIBUTE</td>
<td>mail</td>
</tr>
<tr>
<td>USER DISPLAY NAME ATTRIBUTE</td>
<td>cn</td>
</tr>
<tr>
<td>GROUP OBJECT CLASS</td>
<td>group</td>
</tr>
<tr>
<td>GROUP ACCOUNT ATTRIBUTE</td>
<td>samaccountname</td>
</tr>
<tr>
<td>GROUP DISPLAY NAME ATTRIBUTE</td>
<td>cn</td>
</tr>
</tbody>
</table>

**Delete user directory**

⚠️ Users of the deleted user directory will be deleted as well. As a consequence: active sessions of the users of the deleted user directory will be aborted at the time of the next interaction with the server (for details see Delete user).

**Enable or disable user directory**

To disable a user directory hover over the user directory's entry in the list and click the Disable user directory icon.

When disabling a user directory, all users that are assigned to it will be blocked from logging in.

⚠️ Active sessions of users of the disabled user directory will not be aborted. The user will be blocked at the time of the next login.
When a user directory is disabled then the user directory's entry in the list displays the \textbf{x} mark. To enable the user directory click the \textit{Enable user directory} icon.

\begin{center}
\includegraphics[width=0.5\textwidth]{enable_user_directory.png}
\end{center}

\textbf{Unlock locked accounts}

All the locked user accounts that belong to a Local type user directory, can be released clicking the \textbf{RELEASE LOCKOUT} button.

\textbf{Transport Layer Security}

Transport Layer Security (TLS) is a cryptographic protocol that provides communications security over a computer network. Websites, like the Web Management Console, are able to use TLS to secure all communications between their servers and web browsers.

The TLS protocol aims primarily to provide confidentiality (privacy) and data integrity between two communicating computer applications.

For instructions to set up TLS see \textbf{3.5. Configuring TLS}.

\textbf{LDAP attributes}

For further details see \textbf{3.2.2. LDAP attributes}

\textbf{Active Directory attributes}

For further details see \textbf{3.2.3. Active Directory attributes}

\textbf{Notes}

The currently logged on user can not disable the user directory to which her account is assigned to. For example the \textit{admin} user can not disable the LOCAL user directory.

The currently logged on user can not delete the following:

- Her own user account. For example the \textit{admin} user can not delete the \textit{admin} user account.
- The user directory to which her account is assigned to. For example the \textit{admin} user can not delete the LOCAL user directory.

\textbf{3.2.1. Change user password}

The current user can change her password under \textbf{Settings > Password}. 

\vfill
\noindent v5.3.0

67
The password change option is only available for users of Local type user directories. Changing passwords in LDAP or Active Directory services is not supported.

Important notes

- As long as TLS is not configured for the Web Management Console, passwords are sent clear-text over the network. To set up TLS see 3.5. Configuring TLS.

### 3.2.2. LDAP attributes

- Bind username
• User base and group base DN
• LDAP user schema settings
  • Example
• LDAP group schema settings

This page contains tips on how to obtain the BIND USERNAME, the USER BASE DN and GROUP BASE DN attributes, the LDAP USER SCHEMA SETTINGS and the LDAP GROUP SCHEMA SETTINGS when creating an LDAP type user directory.

⚠️ Normally a domain administrator should provide these values.

✔️ The BIND USERNAME, the USER BASE DN and GROUP BASE DN attributes must be expressed using a valid LDAP syntax.
Bind username

Normally an LDAP administrator should provide these values, however there is a way to get the BIND USERNAME as an LDAP DN, that is needed for the product to do searches in the directory information tree. To get this information, there is, however, some information about the LDAP tree, that must be known in advance:

<table>
<thead>
<tr>
<th>LDAP property</th>
<th>Notes</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN of the LDAP tree node that has the bind user as a child.</td>
<td>This will be the base for the search. If selected improperly then the search may be very slow or won't find the appropriate user.</td>
<td>ou=users,dc=test</td>
</tr>
<tr>
<td>Attributes and their values that uniquely identify the bind user account.</td>
<td>These will be used as filter conditions to find the proper user.</td>
<td>uid=bind</td>
</tr>
</tbody>
</table>

To find the bind user, perform the following steps:

1. Log on to a Windows machine that has connectivity to the LDAP server
2. Choose a user that is intended for this purpose (ie: has rights to do searches in the tree)
3. Open the `LDP.exe` tool with elevated rights (Run as Administrator)
4. Assuming the example properties above are correct, do the following search:

![Search Dialog](image)

The search above will return the attributes for the user in question:

![Search Results](image)

The DN should look something like this:

```
cn=bind,ou=users,dc=test
```
Please note, the actual user DN will most probably look completely different than the above example, as it depends on the structure of the underlying directory information tree in the LDAP server.

On non-server Windows machines the `LDP.exe` tool can be obtained with installing the Remote Server Administration Tools (RSAT).

### User base and group base DN

Once the bind user DN is obtained, an easy way to get the DNs for the user and group searches is by taking all the DC parts of the user DN and leaving the rest out. Using the examples above the result DN will be the following:

```
dc=test
```

Please note that using only DC components for the user/group DNs may result in searches to be executed from the top of the directory information tree and potentially slow down the LDAP server responses a lot and thus have an impact on the MetaDefender product’s password validation. The rule of thumb here is that the more specific the user/group DN, the faster the server response is.

Please also note that users and groups may reside in different parts of the directory information tree, as a consequence applying the same, more specific DN both as USER BASE DN and GROUP BASE DN may cause the MetaDefender product to not find group accounts in the directory information tree. So these DNs should be chosen carefully.

### LDAP user schema settings

Similarly to the search in `Bind username`, we can search for users and determine the appropriate values.
Example

1. Let's assume the following search is executed:

   ![Search interface](image)

   That gives the following result:

   ![Search result](image)

2. That gives the following result:

   ![Ldp interface](image)

3. The LDAP USER SCHEMA SETTINGS may be the following:

<table>
<thead>
<tr>
<th>User schema setting</th>
<th>LDAP attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER OBJECT CLASS</td>
<td>user</td>
</tr>
<tr>
<td>User schema setting</td>
<td>LDAP attribute</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>USER ACCOUNT ATTRIBUTE</td>
<td>uid or samaccountname</td>
</tr>
<tr>
<td>USER EMAIL ATTRIBUTE</td>
<td>mail</td>
</tr>
<tr>
<td>USER DISPLAY NAME ATTRIBUTE</td>
<td>cn</td>
</tr>
</tbody>
</table>

**LDAP group schema settings**

Similarly to the search in LDAP user schema settings, we can search for users and determine the appropriate values.

### 3.2.3. Active Directory attributes

- **Bind username**
- **User base and group base DN**

This page contains tips on how to obtain the BIND USERNAME, the USER BASE DN and GROUP BASE DN attributes when creating an Active Directory type user directory.

⚠️ Normally a domain administrator should provide these values.

✅ All three attributes must be expressed using a valid LDAP syntax.
Bind username

Normally a domain administrator should provide these values, however there is a way to get the BIND USERNAME as an LDAP DN, that is needed for the product to do searches in the directory information tree, and it is as follows:
1. Log on to a Windows server machine that has connectivity to the Active Directory
2. Choose a user that is intended for this purpose (ie: has rights to do searches in the tree)
3. Open a Command window with elevated rights (Run as Administrator)
4. Assuming example.com as domain and John Smith with account name john.smith as the user, type the following:

   > dsquery user domainroot -samid john.smith

   or

   > dsquery user domainroot -name John Smith

   The commands above will return the correct DN for the user in question. The DN should look something like this:

   CN=John Smith,OU=People,OU=Engineering,DC=example,DC=com

   Please note, the actual user DN will not look exactly like the above example, but will depend on the structure of the underlying directory information tree in the Active Directory server.

   On non-server Windows machines the dsquery command can be obtained with installing the Remote Server Administration Tools (RSAT).

**User base and group base DN**

Once the bind user DN is obtained, an easy way to get the DNs for the user and group searches is by taking all the DC parts of the user DN and leaving the rest out, which results in the following DN:

DC=example,DC=com
Please note that using only DC components for the user/group DNs may result in searches to be executed from the top of the directory information tree and potentially slow down AD server responses a lot and thus have an impact on the MetaDefender product's password validation. The rule of thumb here is that the more specific the user/group DN the faster the server response.

Taking the above example into consideration: a user search DN of "OU=People,OU=Engineering,DC=example,DC=com" could potentially result in much faster server response than "DC=example,DC=com" and should be preferred assuming all users reside under "OU=People,OU=Engineering,DC=example,DC=com" in the directory information tree.

Please also note that users and groups may reside in different parts of the directory information tree, as a consequence applying the same, more specific DN both as USER BASE DN and GROUP BASE DN may cause the MetaDefender product to not find group accounts in the directory information tree. So these DNs should be chosen carefully.

3.3. Update settings

- Central Management updates in general
- Ad-hoc updates
- Updates from the internet
- Updates from a folder
- Manual update

Central Management updates in general

Central Management can keep the anti-virus engines, and other related technologies up-to-date on managed instances. All the engines and technologies managed by Central Management are listed under **Inventory > Engines**. It is basically two steps how Central Management keeps managed instances updated:

1. Central Management keeps its engine and technology repository up-to-date,
2. Distribute packages from Central Management repo to managed instances.

To configure how Central Management should keep its own engine and technology repository up-to-date, go to Settings > Update.

Three different sources are available for Central Management repository updates:

- INTERNET,
- FOLDER, or
- MANUAL

**Automatic update distribution**

Central Management will automatically distribute updated engine and technology packages to managed instances.

**Ad-hoc updates**

Irrelevant to the update source selected above, update packages can always be uploaded and installed clicking the Inventory > Engines / UPLOAD PACKAGE button:

![Upload update packages](image)

Where:

1. Packages: ZIP (.zip) files containing the package, while
2. Descriptor files: YAML (.yml) files containing metadata.
Updates from the internet
The INTERNET method will automatically download the updates from the OPSWAT update server. The following options are available:

1. Automatic database updates: The frequency of fetching updates from the update server.
   a. OFF: No scheduled update will be performed.

   ![Trigger updates from the internet](image)

   Updates can still be triggered manually clicking the **Inventory > Engines / UPDATE ALL** button.

2. Update pause: To protect the network from load caused by the updates, distribution of the updates to the instances will be paused during the configured time intervals.

**Updates from a folder**

![Update Settings](image)

Selecting the FOLDER method will cause the product to search for updates in a specific folder.

![Watching the update directory](image)
Central Management continuously watches the configured folder for modification. Whenever the contents of the directory are modified, it will try to pick up the new files as updates.

The following options are available:

1. Pick up updates from: The directory where Central Management will look for updates.
   a. DELETE FILES AFTER IMPORT: If selected, then update files are deleted from the folder set in Pick up updates from after successful processing.

   ![Not applied updates may be removed](image)
   Not applied updates may be removed
   Even if an update could not be applied, it will be removed because it was processed without an issue.

2. Update pause: To protect the network from load caused by the updates, distribution of the updates to the instances will be paused during the configured time intervals.

Manual update
Selecting the MANUAL option will turn off any automatic update mechanism.

⚠️ **No options for MANUAL method**
There are no specific options for the MANUAL option, the page is intentionally left blank.

⚠️ **Trigger updates from the internet**
Updates can still be triggered manually clicking the Inventory > Engines / UPDATE ALL button. In this case the updates will be downloaded from the OPSWAT update server.

### 3.3.1 Cleanup old packages in the update folder
All the packages of the anti-virus engines and other technologies will be stored and maintained under an update folder in Central Management.

By default this is `C:\Program Files\OPSWAT\Metadefender Central Management\data\update_packages`

In order to keep that directory tidy, Central Management provide a cleanup mechanism. This mechanism is triggered whenever the update process executes and finishes.

⚠️ **Cleanup interval time**
All updated Packages that are 24 hours or older than the current cleanup trigger time will be deleted.

### 3.4. Logging
Central Management has a wide variety of options to configure logging. Log settings are in the configuration files. For more details see:

- 3.4.1. Configuration
- 3.4.2. Debug logging

#### 3.4.1. Configuration
For details about configuring log outputs and levels, see 3.1.2. Central Management server configuration file.
Log rotation on Linux

The installer configures the `logrotate` service to rotate Central Management log files with the following settings:

<table>
<thead>
<tr>
<th>Configuration file</th>
<th>/etc/logrotate.d/mdcentralmgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotation period</td>
<td>daily</td>
</tr>
<tr>
<td>Retention time</td>
<td>30 days</td>
</tr>
</tbody>
</table>

⚠️ If the log file path is modified, the `logrotate` configuration should also be updated.

⚠️ Loading new settings

The new log settings can be loaded with

1. Restarting the `mdcentralmgmt` service, or by
2. Sending the HUP signal to the service process.

For example:

```
HUP signal
# kill -l <PID>
```

where `<PID>` is the process ID of the `mdcentralmgmt` process.

### 3.4.2. Debug logging

- Important notes
- Step-by-step guide
  - Windows
    - Enable debug logging
    - Disable debug logging
  - Linux
• Enable debug logging
• Disable debug logging

See also

Important notes

⚠️ Risks of debug logging

Debug logging is not designed to be constantly enabled. It should only be used for investigating issues for short periods of time.

Keeping it enabled permanently may impact performances. If running for too long, the log file can become huge and significantly reduce the available disk space.

⚠️ Required settings

In each case below, both of `logfile` and `loglevel` must be set or none of them.

Step-by-step guide

Windows

Enable debug logging

Perform the following steps to enable debug logging:

1. Make sure that Central Management service is stopped.

   > net stop mdcentralmgmt

2. Open the Windows Registry with `regedit`. Go to the `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Centralmgmt\logger` entry.

3. Add or modify the following entries with the following values:

   a. `loglevel`: debug,
   
   b. `logfile`: Path to the logfile, for example `C:\Program Files\OPSWAT\Metadefender Central Management\data\mdcentralmgmt.log`. 
Please note that the directory path must exist, logs are not written if the directory is not present.

4. Close the registry editor.

5. Start Central Management.

   > net start mdcentralmgmt

Disable debug logging

Perform the following steps to disable debug logging:

1. Make sure that Central Management is stopped.

   > net stop mdcentralmgmt

2. Open the Windows Registry with `regedit`. Go to the `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Centralmgmt\logger` entry.

3. Delete the following entries:
   a. `loglevel`,
   b. `logfile`.

4. Close the registry editor.

5. Start Central Management.

   > net start mdcentralmgmt

The log level `debug` can also be set for the `wineventlog_level` entry. Sending debug logs to the Windows Events would, however, flood the Event Viewer and as so it is not recommended.
Linux

Enable debug logging

Perform the following steps to enable debug logging:

1. Make sure that Central Management service is stopped.

   ```
   # service mdcentralmgmt stop
   ```

2. Open the configuration file: `/etc/mdcentralmgmt/mdcentralmgmt.conf`.

3. Add or modify the following entries with the following values under the `[logger]` section:
   
   a. loglevel: `debug`,
   
   b. logfile: `Path to the logfile, for example: /var/log/mdcentralmgmt` /mdcentralmgmt.log (default).

   Please note that the directory path must exist, logs are not written if the directory is not present.

4. Save the configuration file.

5. Start Central Management.

   ```
   # service mdcentralmgmt start
   ```

Disable debug logging

Perform the following steps to disable debug logging:

1. Make sure that Central Management service is stopped.

   ```
   # service mdcentralmgmt stop
   ```

2. Open the configuration file: `/etc/mdcentralmgmt/mdcentralmgmt.conf`.

3. Delete the following entries:
3.5. Configuring TLS

Central Management supports accessing Web UI and REST interface via HTTPS. This feature is not allowed by default, however. To allow the feature you should modify Central Management server configuration by following the next steps:

First create your certificate and key files in convenient directory. Let us take paths as an example /etc/mdcentralmgmt/nginx.d/your.crt and /etc/mdcentralmgmt/nginx.d/your.key for Linux and C:/Program Files/OPSWAT/Metadefender Centralmgmt/nginx/your.crt and C:/Program Files/OPSWAT/Metadefender Centralmgmt/nginx/your.key for Windows accordingly.

**On Linux**

1. Create file `ssl.conf` in the directory `/etc/mdcentralmgmt/nginx.d`

2. Enter SSL-configuration according to Nginx. To allow simple SSL one needs to add the following lines only:

```bash
ssl on;
ssl_certificate /etc/mdcentralmgmt/nginx.d/your.crt;
ssl_certificate_key /etc/mdcentralmgmt/nginx.d/your.key;
```
3. Service restart is required to take these changes into effect.

On Windows

1. Create file ssl.conf in the directory <Installation Directory>/nginx.

2. Enter SSL-configuration according to Nginx. To allow simple TLS one needs to add the following lines only

```nginx
ssl on;
ssl_certificate "C:/Program Files/OPSWAT/Metadefender Centralmgmt/nginx/your.crt";
ssl_certificate_key "C:/Program Files/OPSWAT/Metadefender Centralmgmt/nginx/your.key";
```

3. Service restart is required to take these changes into effect.

⚠️ ‘\n’ sequences in paths

Using the standard Windows path separator backslash '\' may give unexpected results if 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 appear at nginx as

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

As a workaround instead of backslash '\' use

1. Forward slash '/'
2. Double backslash '\\'.

Note that certificate and key files are to provided by the user who can store them whenever it is convenient. Please adjust the paths accordingly.
For more TLS options please consult Nginx documentation.

3.6. Configuring proxy settings

**How to set proxy for the product**

**Linux**

Under Linux modify CM configuration file in: /etc/default/mdcentralmgmt with the following format:

```
https_proxy="http://<hostname>:<port>"
http_proxy="http://<hostname>:<port>"
```

Depending on user’s proxy configuration, choose the appropriate protocol configuration (http or https proxy)

**Windows**

Under Windows use the `netsh` tool to set the proxy, *e.g.*:

```
netsh winhttp set proxy <ADDRESS>
```

In some cases setting the proxy with `netsh` is not sufficient. In that case set the proxy by starting Internet Explorer with SYSTEM rights and configure the proxy in the settings. To do this please follow this article.

You might need to configure Windows proxy to bypass local addresses (or instance addresses) if you can’t access Web Management Console from the host itself and/or if Central Management can access managed instances via your proxy. Consult `netsh` documentation for additional configuration options.

3.7. Hardening

- Changing the default password
- Running the service as an unprivileged account
  - Linux
  - Windows
Changing the default password

After installation of versions pre 5.2.0, a default user was created with a predefined password. This user may still exist in a post 5.2.0 version, if it was upgraded from an earlier version.

Change this predefined password as soon as possible, following these steps:

1. Log in using the default user account's name and password (admin / admin),
2. Go to Settings > Password and change the password here.

Running the service as an unprivileged account

Linux

By default the mdcentralmgmt service is running as the unprivileged centralmgmt account.

Windows

By default the mdcentralmgmt (OPSWAT Metadefender Central Management) service is running as the privileged Local System account.

To run the Windows service with another Windows account (we will use the Local Service account as an example below) follow these steps:

1. Grant read and write permissions to the target account for the installation folder and all other external files and folders that are configured to be read and written by the Central Management service (e.g.: logfile Windows Registry entry).
2. Stop the OPSWAT Metadefender Central Management service

   > net stop mdcentralmgmt

3. Open the Administrative Tools > Services window on your Windows server.
4. Right click the **OPSWAT Metadefender Central Management** entry and select the *Properties > Log On* dialog.

5. Change the service user account to the target user account.
6. Start the **OPSWAT Metadefender Central Management** service

```
> net start mdcentralmgmt
```
4. Operating Central Management

- 4.1. Overview
- 4.2. Dashboard
- 4.3. Managing groups, products and instances
- 4.4. Inventory management
- 4.5. Product integration limitations
- 4.6. Regular maintenance
- 4.7. Central license management
- 4.8. High availability

4.1. Overview

This page shows a comprehensive overview of
- The statistics on the processed files,
- The managed instances,
- Their connections to each other,
- The used processing options and
- Health issues of instances.

⚠️ Availability of statistics

Please note that MetaDefender Core versions before v4.9.1 cannot report statistics.
4.2. Dashboard

Central Management’s **Dashboard** gives a general overview of Central Management and its instances status.

**Auto screen refresh**

The default refresh rate of the information displayed is 30 seconds.

**Overview page**

The Overview page shows information about
- Proportion of the licensed to the total number of Core instances,
- Proportion of the Core instances that has engine update issues to the total number of Cores,
- What products and how many instances are connected to the Central Management,
- Aggregated number of objects processed by the managed instances.

**Update history**

The Update history shows information about every update-related event.

On the Update history page, you can also search for engine name, package type or message content. Also, you can filter the list for severity.

There is an option to export update history in CSV format. For the export, the filters will be applied, you can filter by date and type of Severity. After the filters are selected, you can download the history by click on "Export to CSV" button.

![Update History](image)

⚠️ **Export with Microsoft Edge**

If you use Microsoft Edge for downloading CSV file. The file may have some troubles with encoding. You can solve it in this way:

- Open Microsoft Excel as normal.
- On the main menu, select Data → From Text/CSV → Choose the CSV. A window will appear, on encode field, select "65001: Unicode (UTF-8)".
- Click "Load" button.
Config history

This page shows audit log that gives information about configuration changes such as user, group and instance management operations.
The events are ordered by the date field and searchable by any field.

The displayed fields are:

- **Date**: date and time of the event
- **User**: who has made the change (directory/username)
- **Type**: the type of object that has been changed
- **Change type**: the type of the change (for instance: create, edit, delete, etc.)
- **Parameter**: the name of the parameter
- **Old value**: the value of the changed parameter before modification
- **New value**: the value of the changed parameter after modification
Processing history
The Processing History page shows information on all scans made on the MetaDefender Core instances. The processing history is displayed associated with specific Core instance in a Group.

To fetch history from instance, select the group where the instance locates, then select the desire instance in the next drop down list.

The processing history page support following operations:

- Search for result, source, rule and for filenames and you can limit search result for a specific scan result.
- Clean up history that is older than a specific time range
- Export scan history in CSV. For the export, the scan history filters will be applied. After the desired time range selected, the download will be started by clicking on the OK button.
- Filter log by scan result, filter by action.

Unhealthy instances
Unhealthy instances shows the list of those engines of which health score is not 100 percent accompanying the following information:

- Satus
- Health status
- Score
- Address
- Product type
- Product version
- License
- Last seen

Score is an integer number between and including 0 and 100. The lower the value the more attention is needed from system administrators to take care of products having low score values. Calculation of the actual score uses the following factors:

- Whether the instance is reachable
- License issues such as fact of activation or expiration of the license and approaching expiry
- If product version is the latest available version
- If engine database is up-to-date

4.3. Managing groups, products and instances

Under Groups menu, groups of instances are listed and can be managed. Every instance can be member of one group exclusively.

⚠️ No instance managed

If there is no instance managed in any of the groups, then a notification appears at the top of the page:

Central Management can manage several instances. Instances are grouped and groups have subgroups called products. An instance is automatically added to the product of its type. If the product does not exist at the time of adding the instance, then the appropriate product is automatically added to the group.

ℹ️ Product example
For example, if a MetaDefender Core instance is added to a group that hasn't got a member of that type yet, then the Core product (subgroup) will be added to the group. If the instance is not the first of that type in the group, it will simply be added to the appropriate product.

⚠️ **Instance configuration stored with product**

Configuration of instances is stored on the product level. For example: configuration of all MetaDefender Core instances of a certain group is stored with the Core product. It means that if we want to get rid of the centrally stored configuration, then we first need to remove all instances from the Core product, then the Core product must also be removed.

- 4.3.1. Groups
- 4.3.2. Products
- 4.3.3. Instances

### 4.3.1. Groups

- Adding new group
- Group management
  - Functions
  - Chart

Every instance should be member of exclusively one group. In order to be able to add an instance to Central Management, a group must be created first.
Adding new group

1. Go to Groups menu and click on ADD NEW GROUP button.
2. Specify the properties of the group to be created and click CREATE GROUP.

The following properties are available:

a. NAME: Mandatory, unique name of this group,

b. DESCRIPTION: Optional, additional information about the group.

3. Clicking CREATE GROUP in the previous step automatically opens the Group Management page of that group.
4. Going to the **Groups** menu again will show the new group.
**Group management**

To manage a group, go to **Groups** menu and click on the box of the group. The Group Management page opens.

**Functions**

In Group Management the following functions are available:

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADD CLIENT PRODUCT</td>
<td>Enable MetaDefender Clients to be added to the group.</td>
<td>Connection between a MetaDefender Client and Central Management can only be initiated from the Client side.</td>
</tr>
<tr>
<td>ADD INSTANCE</td>
<td>Add a new MetaDefender (Core, Kiosk, Email Security or ICAP Server) instance.</td>
<td></td>
</tr>
<tr>
<td>EDIT GROUP</td>
<td>Change the name or description of the group.</td>
<td></td>
</tr>
<tr>
<td>DELETE GROUP</td>
<td>Delete this group.</td>
<td>Available for groups that have no instances and products (empty groups).</td>
</tr>
</tbody>
</table>

**Chart**

The chart in the Group Management page will show the aggregated number of objects processed by the managed instances within this group.
4.3.2. Products

- Managing MetaDefender (Core / ICAP Server / Email Security / Kiosk) products
- Managing MetaDefender Clients
- Deleting a product from a group
  - Policies

Every non-empty group has at least one subgroup called product. A product is created automatically when its first instance added to a group (see 4.3.3. Instances).
Managing MetaDefender (Core / ICAP Server / Email Security / Kiosk) products

The following functions are available for products:
1. **UPDATE NOW**: On the product page, you can force to update packages (for Core only), configuration and fetch information about scanned objects by clicking the **UPDATE NOW** button.

2. **COMMIT CONFIG CHANGES**: If the configuration has changed and you want it to be updated in the next automatic update period, use the **COMMIT CONFIG CHANGES** button. It activates the configuration but doesn’t update it right away.

![Deploy new configuration immediately](image)

To update the new configuration immediately, click on **UPDATE NOW** button after clicking the **COMMIT CONFIG CHANGES**.

On the Core product page the **OBJECTS PROCESSED** chart shows the aggregated number of processed object by all Core servers of this group.

---

**Managing MetaDefender Clients**

![Client initiates connection](image)

*Client initiates connection*
Connection between MetaDefender Client and Central Management can only be initiated from the Client side.

To enable Clients to connect to a group in the Central Management, Client product should be added to the group first. On the Group management page, press Add client product button. In the list of products, Client appears. From then on, Clients can be connect to this group of the Central Management.

Default for clients button also appears in place of Add client product button which is for setting the group as default for incoming client that has no designated group given in the registration request.

Deleting a product from a group

1. Under Groups menu choose the group where the product resides that is wanted to be deleted.

2. Choose the product you want to remove (the product is not highlighted in the list).

3. Click on DELETE PRODUCT.

Product deletion
Product deletion is only allowed if all of its instances has been removed already. See 4.3.3. Instances.

Policies
For details on workflows, zones, and rules, see the User Guide of the appropriate product.

4.3.3. Instances
- Adding instances
- Managing instances
  - Instance details

Every instance should be member of exclusively one group. In order to be able to add an instance to Central Management, a group must be created first.

Instances can be managed under the Groups menu. Clicking a group will show the products within that group in the left-side panel. Instances can be listed clicking the Instances entry within a certain product.

Adding instances

⚠️ Please note that Metadefender Core instances before v4.7.0 can only be managed by Metadefender Central Management that has been upgraded from version v4.2.0.
To manage different versions of Metadefender Core v4 under the same group, an instance of the oldest version of the prospective members should be added first.

To add an instance, perform the following steps:

1. Under **Groups** menu choose the group you intend to add the new instance to. The Group Management page is open. Click the **ADD INSTANCE** button.

2. Specify the properties of the instance to be added and click **ADD INSTANCE**.
Complete instance configuration first

The first instance of a certain product should be licensed and configured before adding to Central Management. Otherwise security rules may not work properly. To fix security rules, the product and its instances should be removed and added again after fixing the configuration of the instance.

The following properties are available:

a. NAME: Mandatory, unique name of this instance,

b. DESCRIPTION: Optional, additional description of this instance,

c. TAGS: Optional, tags of this instance

Tags defined elsewhere

Tags defined at an instance will automatically be offered at the edition of tags of an other instance.

d. REST ADDRESS: Mandatory, REST URI of the instance to be added,
REST URI syntax

The syntax of the REST URI must be:

**URI schema**

<scheme>://<host>:<port>[/function]

For example:

**URI with no function**

https://localhost:8008

**URI with function**

http://10.0.0.1:8009/metadefender_rest

e. CREDENTIALS: Mandatory to specify either the USERNAME / PASSWORD or the API KEY (or both),

i. Human user credentials

1. USERNAME: Username of a defined user in the instance,

2. PASSWORD: Password of the appropriate user in the instance.

ii. API KEY: API key of a defined user in the instance.

⚠️ Credential preference

If all the USERNAME / PASSWORD and API KEY properties are specified then the USERNAME / PASSWORD values will be used.

⚠️ User privileges

The user specified here by the USERNAME / PASSWORD or by the API KEY must have FULL privileges on the User Management on the instance to be added.
f. IMPORT CONFIGURATION: If the instance to be added is the first of its product in the group, its configuration should be imported by enabling this option. By default, it was enabled.

⚠️ **Configuration imported from the first instance of a product**

Enabling or disabling this option for other instances than the first one of a product in a group will make no difference.

3. Clicking on ADD INSTANCE button takes back to the Group Management page.
Under the PRODUCTS in the left panel, the product type of the added instance appears (if this is the first instance of a product within this group).

Managing instances

There are two ways to the Instances pages:

1. One is selecting the desired group and clicking the product on the Group Management page that has the instance you intend to manage.

2. The other one is selecting the desired group and choosing the Instances submenu of the product (for example: Groups > localhost > Core > Instances).

On the Instances page the list of instances displayed with details about each instance. You can search for a specific instance by "instance name", "address" or "version". The list of instances can also be export to CSV or PDF.
To see available functions, hover your cursor over an instance.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Image" alt="Info" /></td>
<td>Show details</td>
<td>View details about the instance</td>
</tr>
<tr>
<td><img src="Image" alt="Reconnect" /></td>
<td>Reconnect instance</td>
<td>Put instance back to under Central Management control.</td>
</tr>
<tr>
<td><img src="Image" alt="Edit" /></td>
<td>Edit instance</td>
<td>Modify information stored about this instance</td>
</tr>
<tr>
<td><img src="Image" alt="Remove" /></td>
<td>Remove instance</td>
<td>Remove this instance from under Central Management control.</td>
</tr>
</tbody>
</table>

This command is available for instances with *Not Managed* status only.
**Instance details**

Clicking on an instance, detailed information page appears. On the top of Instance details page, general information is displayed. There are 4 tabs in the lower half of the page.

- **Managed status**: It shows the status whether the instance is either "Managed", "Not managed" or "Unreachable" *(in unreachable state we can't detect the managed state of the instance)*

- **License details**: Except activation key it shows the same information as the License information page of the instance.

- **Engines (only for Core instances)**: All engines installed on the instance are listed with their details such as:
  - Name of engine
  - Type of engine
  - Platform the engine runs on
  - Engine version
  - Version of database the engine is currently using
  - Engine status (Active/Non-Active)

- **Objects processed (only for Core instances)**: This tab displays a graph of number of scanned objects in the last time period adjusted in the Show data for field.

**4.3.3.1. Adding MetaDefender Core**

1. Choose an already existing Group.
   If no group exists, create a new one and then click "ADD INSTANCE".
2. Specify the properties of the instance to be added.

⚠️ Complete instance configuration first
The first instance of a certain product should be licensed and configured before adding to Central Management. Otherwise, security rules may not work properly. To fix security rules, the product and its instances should be removed and added again after fixing the configuration of the instance.

The following properties are available:

a. NAME: mandatory, unique name of this instance.

b. DESCRIPTION: optional, additional description of this instance.

c. TAGS: optional, tags of this instance.

Tags defined elsewhere

Tags defined at an instance will automatically be offered at the edition of tags of the other instance.

d. REST ADDRESS: mandatory, REST URI or IP of the instance to be added.

REST URI syntax

The syntax of the REST URI must be:

URI schema

<scheme>://<host>:<port>

For example, HTTP:

Example with HTTP

http://localhost:8008

By default a MetaDefender Core configured to use HTTP. When Central Management wants to manage an instance with HTTPS. We need to add trusted root certificates to the machine that runs Central Management.

Add trusted root certificates

Please consult the Adding instance with HTTPS documentation for further details.
For example, HTTPS:

**Example with HTTPS**

https://localhost:8008

e. CREDENTIALS: mandatory to specify either the USERNAME/PASSWORD or the API KEY (or both).

f. Human user credentials
   i. USERNAME: Username of a defined user in the instance.
   ii. PASSWORD: Password of the appropriate user in the instance.

g. API KEY: API key of a defined user in the instance.

⚠️ **Credential preference**

If all the USERNAME / PASSWORD and API KEY properties are specified then the USERNAME / PASSWORD values will be used.

⚠️ **User privileges**

The user specified here by the USERNAME / PASSWORD or by the API KEY must have FULL privileges on the User Management on the instance to be added.
3. IMPORT CONFIGURATION: If the instance to be added is the first of its product in the group, its configuration can be imported by enabling this option.

⚠️ Configuration imported from the first instance of a product

Enabling or disabling this option for other instances than the first one of a product in a group will make no difference.

4. Click "ADD INSTANCE" button at the bottom of the page when done
5. MetaDefender Core will be added and displayed as below. However, STATUS is marked red.
6. Click on PRODUCT name

7. Click "COMMIT CONFIG CHANGES" then "UPDATE NOW"
8. Now STATUS is marked green. It means product is ready.

4.3.3.2. Adding MetaDefender Email Security

1. Choose an already existing Group.
   If no group exists, create a new one and then click "ADD INSTANCE".
## Group Mana...

<table>
<thead>
<tr>
<th>Products</th>
<th># of Instances</th>
<th>Last Update</th>
<th>Status</th>
</tr>
</thead>
</table>

There is no product in this group.

### OBJECTS PROCESSED

**Show data for**

- Last 24 hours

![Graph showing data processed over time]
2. Specify the properties of the instance to be added

Add new Instance

NAME

DESCRIPTION

TAGS
Add a tag

REST ADDRESS

CREDENTIALS

USERNAME

PASSWORD

ADD INSTANCE  CANCEL

⚠️ Complete instance configuration first
The first instance of a certain product should be licensed and configured before adding to Central Management. Otherwise, security rules may not work properly. To fix security rules, the product and its instances should be removed and added again after fixing the configuration of the instance.

The following properties are available:

a. NAME: mandatory, unique name of this instance.
b. DESCRIPTION: optional, additional description of this instance.
c. TAGS: optional, tags of this instance.

d. REST ADDRESS: Mandatory, REST URI or IP of the instance to be added.

Tags defined elsewhere

Tags defined at an instance will automatically be offered at the edition of tags of the other instance.

REST URI syntax

The syntax of the REST URI must be:

**URI schema**

<scheme>://<host>:<port>

For example, HTTP:

**Example with HTTP**

http://localhost:8058

By default a Email Security Server configured to use HTTP. When Central Management wants to manage an instance with HTTPS, we need to add trusted root certificates to the machine that runs Central Management.

Add trusted root certificates

Please consult the Adding instance with HTTPS documentation for further details.
For example, HTTPS:

**Example with HTTPS**

https://localhost:8058

e. CREDENTIALS: mandatory to specify either the USERNAME / PASSWORD or the API KEY (or both),

f. Human user credentials
   
   i. USERNAME: Username of a defined user in the instance.
   ii. PASSWORD: Password of the appropriate user in the instance.

g. API KEY: API key of a defined user in the instance.

⚠ **Credential preference**

If all the USERNAME / PASSWORD and API KEY properties are specified then the USERNAME / PASSWORD values will be used.

⚠ **User privileges**

The user specified here by the USERNAME / PASSWORD or by the API KEY must have FULL privileges on the User Management on the instance to be added.
3. IMPORT CONFIGURATION: If the instance to be added is the first of its product in the group, its configuration can be imported by enabling this option.

⚠️ Configuration imported from the first instance of a product

Enabling or disabling this option for other instances than the first one of a product in a group will make no difference.

4. Click "ADD INSTANCE" button at the bottom of the page when done.
5. MetaDefender Email Security will be added and displayed as below. However, STATUS is marked red.
6. Click on PRODUCT name.

7. Click "COMMIT CONFIG CHANGES" then "UPDATE NOW".
8. Now STATUS is marked green. It means product is ready.

4.3.3.3. Adding MetaDefender Kiosk

1. Choose an already existing Group.
   If no group exists, create a new one and then click "ADD INSTANCE".
2. Specify the properties of the instance to be added

Complete instance configuration first
The first instance of a certain product should be licensed and configured before adding to Central Management. Otherwise, security rules may not work properly. To fix security rules, the product and its instances should be removed and added again after fixing the configuration of the instance.

The following properties are available:

a. **NAME**: mandatory, unique name of this instance,

b. **DESCRIPTION**: optional, additional description of this instance,

c. **TAGS**: optional, tags of this instance

### Tags defined elsewhere

Tags defined at an instance will automatically be offered at the edition of tags of the other instance.

d. **REST ADDRESS**: Mandatory, REST URI or IP of the instance to be added

### REST URI syntax

The syntax of the REST URI must be:

```
URI schema
<scheme>://<host>:<port>/metadefender_rest
```

For example, HTTP:

```
Example with HTTP
http://localhost:8009/metadefender_rest
```

By default a MetaDefender Kiosk configured to use HTTP. When Central Management wants to manage an instance with HTTPS. We need to add trusted root certificates to the machine that runs Central Management.

### Add trusted root certificates

Please consult the [Adding instance with HTTPS](#) documentation for further details.
For example, HTTPS:

**Example with HTTPS**

https://localhost:8009/metadefender_rest

e. CREDENTIALS: Mandatory to specify either the USERNAME / PASSWORD or the API KEY (or both)

f. USERNAME/PASSWORD

⚠️ Kiosk already has username and password in the new version (v4.3.0), but currently, it supports only the API KEY method for authentication. Please use API KEY for CREDENTIALS

g. API KEY: API key of a defined user in the instance.

⚠️ **API KEY**

The value for the "API Key" field is the generated API key of an administrator user.
Refer to management console user information on how to generate it.

⚠️ **User privileges**

The user specified here by the USERNAME / PASSWORD or by the API KEY must have FULL privileges on the User Management on the instance to be added.
### Credential preference

If all the USERNAME / PASSWORD and API KEY properties are specified then the USERNAME / PASSWORD values will be used.

3. **IMPORT CONFIGURATION:** If the instance to be added is the first of its product in the group, its configuration can be imported by enabling this option.

⚠️ **Configuration imported from the first instance of a product**

Enabling or disabling this option for other instances than the first one of a product in a group will make no difference.
4. Click "ADD INSTANCE" button at the bottom of the page when done

5. MetaDefender Kiosk will be added and displayed as below. However, STATUS is marked red.
6. Click on PRODUCT name
7. Click "COMMIT CONFIG CHANGES" then "UPDATE NOW"

8. Now STATUS is marked green. It means product is ready.

4.3.3.3.1. UI Localization / Customization for MetaDefender Kiosk

You can change the language displayed in MetaDefender Kiosk from the 'CHOOSE LANGUAGE' drop-down menu.

The default languages included in the installation are English, Arabic, Hebrew, Korean, Vietnamese, German, and Japanese.
If you wish to edit the translations of any of the existing languages in the MetaDefender Kiosk UI, you can do so by clicking on 'VIEW AND EDIT LANGUAGES' at the bottom of the page, under 'USER INTERFACE' tab of Kiosk configuration.

After clicking 'VIEW AND EDIT LANGUAGES', you can choose which language to edit from the drop-down menu next to 'CHOOSE LANGUAGE TO UPDATE'.
You can edit the translations for any of the strings which appear in MetaDefender Kiosk. Once finished, click on ‘APPLY’ button.

### Future Support

Add and delete language currently not available.
4.3.3.4. Adding MetaDefender ICAP Server

1. Choose an already existing Group.
   If no group exists, create a new one and then click "ADD INSTANCE".
2. Specify the properties of the instance to be added

Add new Instance

NAME

DESCRIPTION

TAGS

Add a tag

REST ADDRESS

CREDENTIALS

USERNAME

PASSWORD

ADD INSTANCE CANCEL

⚠️ Complete instance configuration first
The first instance of a certain product should be licensed and configured before adding to Central Management. Otherwise, security rules may not work properly. To fix security rules, the product and its instances should be removed and added again after fixing the configuration of the instance.

The following properties are available:

a. NAME: Mandatory, unique name of this instance,
b. DESCRIPTION: Optional, additional description of this instance,
c. TAGS: Optional, tags of this instance

d. REST ADDRESS: Mandatory, REST URI or IP of the instance to be added

Tags defined elsewhere

Tags defined at an instance will automatically be offered at the edition of tags of the other instance.

REST URI syntax

The syntax of the REST URI must be:

```
URI schema
<scheme>://<host>:<port>
```

For example, HTTP:

```
Example with HTTP

http://localhost:8048
```

By default a MetaDefender ICAP Server configured to use HTTP. When Central Management wants to manage an instance with HTTPS. We need to add trusted root certificates to the machine that runs Central Management.

Add trusted root certificates
Please consult the Adding instance with HTTPS documentation for further details.

For example, HTTPS:

**Example with HTTPS**

https://localhost:8048

e. CREDENTIALS: Mandatory to specify either the USERNAME / PASSWORD or the API KEY (or both),

f. Human user credentials
   
i. USERNAME: Username of a defined user in the instance,
   
   ii. PASSWORD: Password of the appropriate user in the instance.

  g. API KEY: API key of a defined user in the instance.

⚠️ **Credential preference**

If all the USERNAME / PASSWORD and API KEY properties are specified then the USERNAME / PASSWORD values will be used.

⚠️ **User privileges**

The user specified here by the USERNAME / PASSWORD or by the API KEY must have FULL privileges on the User Management on the instance to be added.
3. IMPORT CONFIGURATION: If the instance to be added is the first of its product in the group, its configuration can be imported by enabling this option.

⚠️ Configuration imported from the first instance of a product

Enabling or disabling this option for other instances than the first one of a product in a group will make no difference.

4. Click "ADD INSTANCE" button at the bottom of the page when done
5. MetaDefender ICAP will be added and displayed as below. However, STATUS is marked red.
6. Click on PRODUCT name

7. Click "COMMIT CONFIG CHANGES" then "UPDATE NOW"
8. Now STATUS is marked green. It means product is ready

4.3.3.5. Adding instance with HTTPS

When Central Management wants to manage an instance with HTTPS. We need to add trusted root certificates to the machine that runs Central Management

Windows

1. Open Microsoft Management Control: on Start menu, type "mmc.exe"
2. File -> Add/Remove Snapp in..
3. Select Certificates → Add

4. In the left select Console Root > Certificates > Trusted Root Certification Authorities > Certificates
5. Right click -> All task -> Import -> Select your .crt file to import. Save config

6. Restart the Central Management and then adding an instance as normal

**Linux (CentOS 6)**

1. Install the ca-certificates package:
   
yum install ca-certificates

2. Enable the dynamic CA configuration feature:
   
update-ca-trust force-enable

3. Add your .crt file into /etc/pki/ca-trust/source/anchors/. Ex:
cp foo.crt /etc/pki/ca-trust/source/anchors/

4. Update CA

update-ca-trust extract

5. Restart the Central Management and then adding an instance as normal

4.4. Inventory management

- Overview
- Functions

Overview

Under the **Inventory > Engines** menu Central Management displays detailed information about scan engines and technologies including anti-malware engines, archive engines, utilities, etc.

On the Engines page all the licensed engines are listed with their details:

- **ENGINE**: The name of the engine,
- **TYPE**: the Type of the engine. The possible types are:
  - Archive engine,
  - Anti-malware engine,
  - Data sanitization engine,
  - Filetype detection engine,
  - Utility engine,
  - Vulnerability detection engine,
- **PLATFORM**: Operating system platform the engine runs on,
- **VERSION**: Engine version,
- **DATABASE**: Database version the engine is using,
- **ENABLED**: Enabled/disabled status of the engine.

Functions

The following functions are available:

1. **UPDATE ALL**: To manually trigger update of engine and database packages, click on the **UPDATE ALL** button.

2. **UPLOAD PACKAGE**: To install engine or database packages of your own, select the **UPLOAD PACKAGE** option.
3. Enable / Disable: Engines can be disabled (and re-enabled afterwards) by clicking on the ✔️ (Enable) or ✗ (Disable) button.

**How to find the Enable / Disable button**

To make the Enable or Disable button visible, hover over the line of the engine. The button will appear at the end of the line:

![Enable/Disable button](image)

**Disabled status**

When an engine is disabled neither the engine nor the corresponding database package is updated. Enabled status of the engine is marked by ✔️, while disabled status is marked by ✗.

![Disabled status](image)

In case of having a MetaDefender Core v3 database update for which remote engine update is not supported, engine version information is not shown.

4.5. Product integration limitations

- General
  - Central license management
- MetaDefender Core
  - Engines
    - Enable or disable engines
    - Advanced engine configuration
  - Whitelist
- MetaDefender Email Security
  - Server Profiles
  - Global Settings
• MetaDefender ICAP Server
  • Server Profiles
• MetaDefender Kiosk
  • Custom workflows

This page lists the most important limitations or missing features of product integrations.
The list on this page is not complete, it only wants to grab the most important cases that were already requested by customers.

General

Central license management

As of version 5.2.0, central management of licenses of the managed instances is supported by Central Management.
For details see 4.7. Central license management

MetaDefender Core
For MetaDefender Core instances, Central Management supports the following only to be configured centrally:

1. Policy > Workflow rules
2. Policy > Workflow templates
3. Policy > Security zones

No other configuration is supported by Central Management.

Engines

Enable or disable engines
It is not supported to enable or disable engines of managed Core instances from Central Management.

Enable or disable engine updates
Under **Inventory > Engines** Central Management has the list of engines. The *Disable* and *Enable* functions on this page can, however, enable and disable the updates of these engines only.

**Advanced engine configuration**

It is not supported to set the advanced engine configuration for managed Core instances in Central Management.
Advanced engine configuration can be set under Inventory > Engines clicking the (Edit) icon at the end of the row of the engine.

**Whitelist**

It is not supported to set the **Inventory > Whitelist** for managed Core instances in Central Management.

**MetaDefender Email Security**

For MetaDefender Email Security instances, Central Management supports the following only to be configured centrally:

1. **Policy > Security Rules**

No other configuration is supported by Central Management.

**Server Profiles**

Since version 5.1.1 Central Management already has the support built-in for Email Security server profiles.

On the other hand this Central Management feature is not supported by Email Security yet.
Global Settings
It is not supported to set the Settings > Global Settings for managed Email Security instances in Central Management.

MetaDefender ICAP Server
For MetaDefender ICAP Server instances, Central Management supports the following only to be configured centrally:

1. Policy > Security Rules

No other configuration is supported by Central Management.

Server Profiles
Since version 5.1.1 Central Management already has the support built-in for ICAP Server server profiles.
On the other hand this Central Management feature is not supported by ICAP Server yet.

MetaDefender Kiosk
For MetaDefender Kiosk instances, Central Management supports the following only to be configured centrally:

1. Configuration
2. Workflows

Custom workflows
There are limitations on certain Kiosk workflow configurations in Central Management.
For details see 364249535.

No other configuration is supported by Central Management.

Custom workflows
Central Management is not yet capable to assign member users to custom Kiosk workflows.
As a workaround custom Kiosk workflows (Workflows / CREATE NEW PROFILE) are removed from under Central Management control with Kiosk version 4.2.2.
Membership

Workflow membership can be set for custom workflows in Kiosk:

4.6. Regular maintenance

Checking for upgrades

Central Management checks for available database updates and scan engine updates for the installed anti-malware engines on a regular basis. To manually update a scan engine or its database, click on the UPDATE NOW button or the UPLOAD PACKAGE button on the Inventory > Engines page.

Checking engines/databases health

Central Management regularly checks for available database updates and scan engine updates for the installed anti-malware engines. Both database and engine upgrades are based on a mechanism that checks for authenticity of the origin of the upgrade package. If the authenticity is confirmed, the upgrade package is downloaded. As an extra stability measure each downloaded upgrade package is tested locally to ensure that it is functioning properly. Only after successful testing will the upgrade package be distributed among Central Management agents.
4.7. Central license management

As of version 5.2.0, centralized management of licenses of the managed instances is supported by Central Management.

It means that the licenses of managed instances are not needed to be maintained manually on the instances themselves.

The centralized license management does not require any operator interaction, it is performed in an automated way by the system.

High level architecture overview

1. The centralized license management uses OPSWAT's update infrastructure and Activation Server to keep managed instances' licenses up-to-date.

2. When a managed instance asks Central Management for updates, Central Management contacts the update infrastructure for new packages. The update infrastructure prepares the new packages, and –in parallel– checks the Activation Server for license updates.

3. The new license and the updates are served to the managed instance in a single batch at the end.

4.8. High availability

- Cold swap example
  - Infrastructure
    - Shared storage
    - Active Central Management node
    - Spare Central Management node
    - Network address translator
  - Switch-over

No HA out of the box
Central Management does not support high availability out-of-the-box. This example shows, however, how to set Central Management up for high availability using 3rd party tools.

**Cold swap example**

In this example we will use four servers installed with CentOS-7-x86_64-Minimal-1804.iso as OS and a managed instance to demonstrate a cold swap high availability setup. The network setup will be the following:

Use `nmtui` to configure static IP addresses and static routes if needed.

**Infrastructure**

To build the infrastructure, perform the following steps:

1. Install CentOS on all the four machines (shared storage, Central Management A (active), Central Management B (spare), network address translator)
2. Enable networking on each

```bash
# nmtui
```
Shared storage

The shared storage will use Network File System (NFS) to share a directory where the data files will be stored for both the active and the spare Central Management servers.

Perform the following steps on the shared storage server:

1. Install NFS utils

```bash
# yum install nfs-utils
```
2. Enable services

```bash
# systemctl enable rpcbind
# systemctl enable nfs-server
# systemctl enable nfs-lock
# systemctl enable nfs-idmap
# systemctl start rpcbind
# systemctl start nfs-server
# systemctl start nfs-lock
# systemctl start nfs-idmap
```

3. Create the directory to be shared

```bash
# mkdir /var/nfsshare
# chmod -R 755 /var/nfsshare
# chown nfsnobody:nfsnobody /var/nfsshare
```

4. Share the directory

```bash
# vi /etc/exports
/var/nfsshare *(rw,sync,no_acl,no_root_squash,no_all_squash)
```

5. Restart NFS server

```bash
# systemctl restart nfs-server
```

6. Enable NFS on the firewall

```bash
# firewall-cmd --permanent --zone=public --add-service=nfs
# firewall-cmd --permanent --zone=public --add-service=mountd
# firewall-cmd --permanent --zone=public --add-service=rpc-bind
# firewall-cmd --reload
```

**Active Central Management node**

The active Central Management server will use Network File System (NFS) to access the shared directory where the data files will be stored.
Perform the following steps on the active Central Management server:

1. Install NFS utils

   ```
   # yum install nfs-utils
   ```

2. Install Central Management

   ```
   # yum install mdcentralmgmt-5.2.0-1.x86_64.rpm
   ```

3. Stop the service

   ```
   # service mdcentralmgmt stop
   ```

4. Bind the data directory to the share
   a. Back up the contents of the installation data directory

      ```
      # cp -R /var/lib/mdcentralmgmt /root/backup
      ```

   b. Clear the contents of the installation data directory

      ```
      # rm -rf /var/lib/mdcentralmgmt/*
      ```

c. Mount the shared directory on the data directory

   ```
   # vi /etc/fstab
   10.0.2.10:/var/nfsshare  /var/lib/mdcentralmgmt  nfs
defaults 0 0
   # mount -a
   ```

d. Restore the contents of the data directory

   ```
   cp -R /root/backup/mdcentralmgmt/* /var/lib/mdcentralmgmt
   ```
5. Restart the service

```
# service mdcentralmgmt start
```

6. Record the UID and GID of the *centralmgmt* user and group (see Sync the UID and GID of the centralmgmt user and group with the active node)

```
# id -u centralmgmt
998
#id -g centralmgmt
996
```

**Spare Central Management node**

The spare Central Management server will use Network File System (NFS) to access the shared directory where the data files will be stored.

Perform the following steps on the active Central Management server:

1. Install NFS utils

```
# yum install nfs-utils
```

2. Install Central Management

```
# yum install mdcentralmgmt-5.2.0-1.x86_64.rpm
```

3. Stop the service

```
# service mdcentralmgmt stop
```

4. Bind the data directory to the share
   a. Clear the contents of the installation data directory

```
# rm -rf /var/lib/mdcentralmgmt/*
```

   b. Mount the shared directory on the data directory
5. Sync the UID and GID of the centralmgmt user and group with the active node (see Record the UID and GID of the centralmgmt user and group)
   
a. Record the current UID and GID values

   ```
   # id -u centralmgmt
   1001
   # id -g centralmgmt
   1002
   ```

   b. Set the UID and GID values to the same as on the active node

   ```
   # usermod -u 998 centralmgmt
   # groupmod -g 996 centralmgmt
   ```

   c. Set the new UID and GID values for all files and directories that must be owned by the centralmgmt user or group

   ```
   # find / -user 1001 -exec chown -h centralmgmt {} \;
   # find / -group 1002 -exec chgrp -h centralmgmt {} \;
   ```

6. Remember to not (re)start the mdcentralmgmt service on the spare Central Management node as it may cause data inconsistency.

**Network address translator**

The network address translator server will provide the shared IP address for both the active and the spare Central Management nodes. This will ensure that the managed instances will always see the same IP address for the Central Management server either it is the active or the spare server that is doing the actual management.

Perform the following steps on the network address translator server:

```
1. Enable packet forwarding

   # sysctl -w net.ipv4.ip_forward=1

   a. Persist packet forwarding

      # vi /etc/sysctl.conf
      net.ipv4.ip_forward = 1

2. Assign the network interfaces to the firewall zones accordingly

   # firewall-cmd --zone=external --add-interface=eth0 --permanent
   # firewall-cmd --zone=internal --add-interface=eth1 --permanent

3. Configure masquerading on the externally facing interface

   # firewall-cmd --zone=external --add-masquerade --permanent

4. Add the NAT rule

   # firewall-cmd --permanent --direct --passthrough ipv4 -t nat
   -I POSTROUTING -o eth0 -j MASQUERADE -s 10.0.2.0/24

5. Enable instance REST ports (e.g. 8008) so that the managed instances' REST interfaces can be accessible

   # firewall-cmd --permanent --zone=internal --add-port=8008/tcp

6. Reload and verify the firewall configuration

   # firewall-cmd --complete-reload
   # firewall-cmd --list-all-zones
Switch-over

1. Stop the active Central Management on the active Central Management server

   # service mdcentralmgmt stop

2. On the spare Central Management server
   a. Start the spare Central Management service

      # service mdcentralmgmt start

   b. Activate the license and check if managed instances appear right.
5. Release notes

<table>
<thead>
<tr>
<th>5.3.0 Central Management release</th>
<th>Central Management 5.3.0 provides enhancement to the UI experience, improve CM Engine Updater's functionality on low bandwidth network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 Aug , 2019</td>
<td></td>
</tr>
</tbody>
</table>

**Enhancement**

<table>
<thead>
<tr>
<th>Improve CM Engine Updater's functionality on low bandwidth network</th>
<th>When updating engine packages to Metadefender Core, If the bandwidth is consistently slow, the updating process will be aborted. The enhancement is to decrease the abort update threshold.</th>
</tr>
</thead>
</table>

**Enhancement to the UI experience**

<table>
<thead>
<tr>
<th>Enhancement to user experience in UI.</th>
</tr>
</thead>
</table>

**Previous releases**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>— 12 Aug 2019</td>
</tr>
<tr>
<td>5.2.0</td>
<td>— 29 Jun 2018</td>
</tr>
<tr>
<td>5.2.1</td>
<td>— 13 Jul 2018</td>
</tr>
<tr>
<td>5.2.2</td>
<td>— 15 Oct 2018</td>
</tr>
<tr>
<td>5.2.3</td>
<td>— 26 Nov 2018</td>
</tr>
<tr>
<td>5.2.4</td>
<td>— 04 Jan 2019</td>
</tr>
<tr>
<td>5.2.5</td>
<td>— 01 Mar 2019</td>
</tr>
<tr>
<td>5.2.6</td>
<td>— 12 Apr 2019</td>
</tr>
<tr>
<td>5.2.7</td>
<td>— 17 May 2019</td>
</tr>
<tr>
<td>5.2.8</td>
<td>— 1 July 2019</td>
</tr>
<tr>
<td>5.2.9</td>
<td>— 1 July 2019</td>
</tr>
</tbody>
</table>
5.1. Changelog

Version 5.3.0

Issues fixed:
- Improve CM Engine Updater's functionality for low bandwidth network
- Enhancement to the UI experience

Version 5.2.9

Issues fixed:
- Change all product names with "Metadefender" prefix at the Overview page
- Change all product names with "Metadefender" prefix at the Dashboard page
- Update document for adding Metadefender Kiosk
- Update Metadefender Core's health score calculation

Version 5.2.8

Issues fixed:
- Enhance engine configuration detection logic
- Reset page when changing group in processing history page
- Change message warning when authentication failed

Version 5.2.7

New features:
- Processing a history page with filtering, searching and exporting options
- Import configuration is made by default
- Adding an API to support CM migration to OPSWAT Central Management in future
Issues fixed:
- Set number of agents for unlimited license activation
- Auto detect CDR configuration

Version 5.2.6
New features:
- Detect and display Managed Status of MetaDefender Client instances
- Engine status in health score
- Search for instances by either instance name, address or version
- Export a list of instances to CSV and PDF
Issues fixed:
- "Managed Status" column width is a little smaller than "Address" one
- Password support in API key section

Version 5.2.5
New features:
- Ability to export Update History to Excel
- Improve Management of Client Instances
- Enhanced Logging for MetaDefender Central Management
- Edit the language setting of MetaDefender Kiosk from Central Management
- Update User Guide: Adding MetaDefender Kiosk
- Update User Guide: UI Localization / Customization for MetaDefender Kiosk
Issues fixed:
- Active Directory binds password is in clear text

Version 5.2.4
New features:
- Update user guide: how to add products into CM
- Update user guide: how to configure CM for manage an instance with HTTPS
- Add configuration workflow rule for DLP engine in Core 4.12
Issues fixed:
- The update folder is not cleared up after new engines are updated.
**Version 5.2.3**

Issues fixed:
- Long group name overflows to next section.
- UI text overlapping on small screen device, or shrink down browser.

**Version 5.2.2**

New features:
- Added support for anonymous LDAP and Active Directory bind

Issues fixed:
- Engines not updating over slow or limited network connections
- Added more details in case of the *UNKNOWN* error message
- License and engine status values were wrong on the Dashboard

**Version 5.2.1**

Issues fixed:
- Schema upgrades may break config update

**Version 5.2.0**

New features:
- Support for centralized license management
- Welcome wizard for administrator onboarding
- Drive admin in case of non-activated instance

**Version 5.1.2**

Issues fixed:
- Failed to upgrade schema version warnings in Update History
- Configuration update fails on managed instances

**Version 5.1.1**

New features:
- Reconnect Not Managed instances
- LDAP user directory type
• Multiple LDAP and AD servers support
• Capability to manually specify API keys
• Configurable number of parallel instances

Issues fixed:
• Periodically upgrade schema version of instances
• Central Management failed to deploy updates
• Server profiles were not centrally manageable
• Rights were not configurable for Unhealthy Instances
• Clients were reported as Not Activated

Version 5.1.0
New features:
• MetaDefender Central Management now has the ability to connect to:
  • MetaDefender ICAP Server from version v4.2.1
  • MetaDefender Email Security from version v4.1.3
  • MetaDefender Client from version v4.1.0
  • MetaDefender Kiosk from version v4.2.0
• Centralized policy management for MetaDefender v4 product family
• New-looking user interface
• More informative Overview and Dashboard pages

Issues fixed:
• MetaDefender v4.9.0 cannot be managed by Central Management

Version 5.0.0RC
New features:
• Centralized policy/configuration management for Metadefender Core v4 instances
• New looking, rearranged user interface
• New instance grouping principles
• Statistics on all grouping levels
• Individual log message level override
• Self-lockout protection, admins can not delete themselves
• Active Directory integration
• Role (user group) based rule availability configuration
• Multiple user roles introduced with different access rights
• Timezone changed to local in log messages
• Instance tagging

Issues fixed:
• Fixed unavailable instance handling

**Version 4.2.0**

New features:
• Full audit log about any configuration changes via Web user interface or REST API
• Able to disable applying update in user configurable time periods
• Central Management can act as an update source for OESIS product line
• Able to set up apikey for every user for easier REST API integration
• Improved hardware detection in license component
• Modified update distribution to support engine update delivery for Windows emulated engines
• Improved activation process feedback on web user interface

Issues fixed:
• Improved reliability of file detection of update pickup from folder feature
• Fixed unstable update deployment process in certain cases
• Fixed detection of failed updates on Core instances
• Fixed message content format in Windows Event log
• Fixed system wide proxy usage on Windows
• Improved browser cache handling in case of product upgrades
• Patched internal nginx web server to fix CVE-2016-4450
• Improved logging of proxy usage
• Improved handling of slow offline update package uploads
• Detailed logging in case of SSL connection issues
Version 4.1.0

- Added offline update picker feature to make it easy to apply offline updates without user interaction or scripting
- Improved update deployment process
- Improved speed of initial package generation
- Decrease REST API calls to Metadefender Core v3.x instances
- Improved reporting of unsuccessful update delivery
- Show update in progress status on Web Management Console
- Support package generation on Microsoft Windows
- Added hardware related info into generated support package
- Option added to log to a remote syslog server
- Improved system issue notification on Web Management Console
- Removed unmeaningful database age display of non-anti-malware engines

Version 4.0.1

- Rebranded to Metadefender Central Management
- Update deployment fixes
- Added support for platform based licenses

Version 4.0.0

- Initial release

5.2. Archived release notes

- 5.2.1. Version 5.1.1
- 5.2.2. Version 5.1.2
- 5.2.3 Version 5.2.0
- 5.2.4 Version 5.2.1
- 5.2.5 Version 5.2.2
- 5.2.6 Version 5.2.3
- 5.2.7 Version 5.2.4
• 5.2.8 Version 5.2.5
• 5.2.9 Version 5.2.6
• 5.2.10 Version 5.2.7
• 5.2.11 Version 5.2.8
• 5.2.12 Version 5.2.9
5.2.1. Version 5.1.1

5.1.1 Central Management release
18 May, 2018

Central Management 5.1.1 is intended to be a maintenance release. It tries to address issues arose in the previous version that—to some extent—was a completely new product (previously Central Management was capable to manage MetaDefender Core only; now Kiosk, Client, Email Security and ICAP server are supported as well).

New & improved

Reconnect Not Managed instance

Previously it was not supported out of the box to take an instance back under it has been disconnected.

We have a function now to reconnect an unmanaged instance:

<table>
<thead>
<tr>
<th>INSTANCE NAME</th>
<th>MANAGED STATUS</th>
<th>SCORE</th>
<th>ADDRESS</th>
<th>PRODUCT VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>icap</td>
<td>Not Managed</td>
<td>0 / 100</td>
<td><a href="http://localhost:8048/">http://localhost:8048/</a></td>
<td>4.2.3</td>
</tr>
</tbody>
</table>

LDAP user directory type

Besides Local and Active Directory type user directories, from release 5.1.1 (new, LDAP type user directories. This new feature will help organizations that integrate their directory service based user management to Central Management.

To add users from your LDAP directory service to Central Management's Web Management Console, go to Settings > User Management / USER DIRECTORIES and click ADD NEW USER DIRECTORY TYPE.

Multiple LDAP and AD servers support

To support redundant (load balancing or high availability) directory service sy specify multiple LDAP and Active Directory servers for LDAP and Active Directory respectively.
Central Management will try all the servers to establish a successful connection when authenticating users.

The only way to create an API key was previously to generate it using the Generate link. Now it is possible to enter API keys manually. It is useful when the same API key needs to be used for a certain account on all instances of a product so that this API key can be configured in Central Management.

Please note that validation rules apply.

- Pagination is now supported for the Unhealthy Instances page. Previously instances could slow down or even crash certain browsers.
- When the Settings or the Policy of an instance have just changed, Central Management now displays a message to warn the user to remember committing the changes:

  ![Configuration saved. Press the COMMIT CONFIG CHANGES button on product](image)

Previously Central Management queried the configuration descriptor (schema) of the addition of the first product instance. Later this schema was no updated automatically. As a result, the configuration capabilities did not improve on Central Management side even if a newer version of the product has already been taken under management.

Now Central Management periodically queries the schema version of each connected instance of a product and updates its own configuration capabilities to the newest possible version instances.

Under special circumstances Central Management failed to deploy huge anti-virus database updates. It was a timeout issue.
<table>
<thead>
<tr>
<th>Central Management failed to deploy updates</th>
<th>Server profiles were not centrally manageable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server profiles are an integral part of the security rules of ICAP Server and Email Security. The Email Security and ICAP Server security rules were previously supported by Central Management, but server profiles were not.</td>
<td>Server profiles were not centrally manageable</td>
</tr>
<tr>
<td>With version 5.1.1 Central Management supports centralized configuration of server profiles of ICAP Server and Email Security type instances.</td>
<td></td>
</tr>
<tr>
<td>! This centralized configuration is, however, not supported by the latest Email Security (version 4.2.0) and ICAP Server (version 4.2.3) yet.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rights were not configurable for Unhealthy Instances</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>It was not possible to restrict access rights to the Unhealthy instances page. Setting &gt; User Management / ROLES.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clients were reported as Not Activated</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaDefender Client instances' license status was reported in Central Management, however, be not activated at all. From now on license status for Clients will not be configurable.</td>
<td></td>
</tr>
<tr>
<td>(Similarly for health status: it is not applicable for Clients. It will be N/A.)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Some labels were not completely clear</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Some lables of the Central Management UI were not expressive enough or d</td>
<td></td>
</tr>
</tbody>
</table>

| Changed |
| **Maximum parallel update settings were not used** | Under **Settings > Global** there was the *Maximum number of parallel update* implemented at all (it did not do anything).

It was renamed to *Maximum number of instances managed in parallel* and it controls the maximum number of instances that are managed in parallel, in the same time. The goal is to provide option for administrators to restrict Central Management's footprint in the network traffic. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Known issues</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Assign users to custom Kiosk workflows</strong></td>
<td>Central Management is not yet capable to assign member users to custom Kiosk workflows. As a workaround, custom Kiosk workflows are removed from under Central Management control with Kiosk version 4.2.2. For details see <strong>Kiosk section in 4.5. Product integration limitations</strong>.</td>
</tr>
</tbody>
</table>
## 5.2.2. Version 5.1.2

### 5.1.2 Central Management release
04 June, 2018

Central Management 5.1.2 is a maintenance release. Most importantly it fixes a critical issue found in the previous version: Central Management could not update the configuration (except on one specific MetaDefender (Core) and on specific Email Security versions) of instances.

### Fixed

**Configuration update fails on managed instances**

Caused by a configuration descriptor (schema) related mistake, Central Management could update the configuration of MetaDefender (Core) version 4.10.1 (or newer) and Email Security version 4.2.1 (or newer) instances only.

For any other product instances and versions, the update failed.

**Failed to upgrade schema version warnings in Update History**

Central Management 5.1.1 introduced support for automated periodic schema upgrades. Central Management tries to upgrade the schema version even if it is not supported by the instance yet. In this case Central Management erroneously added the Failed to upgrade schema version warning message to the Update History.
## 5.2.3 Version 5.2.0

| **5.2.0 Central Management release** | Central Management 5.2.0 is a major feature release primarily providing central license management capabilities. |
| **29 June, 2018** | |

### New & improved

| **Support for centralized license management** | Central Management—and related products— are now capable to distribute and handle product licenses centrally, by Central Management. It means, for example, that when the licensed engines change for managed MetaDefender (Core) products, then there is no need for re-activating each and every instance manually: the license upgrade is performed by Central Management automatically. |
| **Central license management does not require administrator involvement, it is performed automatically by the system.** |

For further details see 4.7. Central license management.

| **Welcome wizard for administrator onboarding** | After a successful installation and before the Web Management Console can be put into practice, a basic configuration wizard is available on the port of the product. This wizard will guide the administrator through the most important configuration steps of the product. |
| **For further details see 1.1.1. Basic configuration wizard or watch the video clip.** |

| **Drive admin in case of non-activated instance** | Unless the license of Central Management is activated, the Web Management Console will start with opening the Activation dialog at every administrator login. This will give the hint to the administrator that the license must be activated first, before the product can be used. |
| **For further details see 2.4.1. Activating licenses or watch the video clip.** |
## Known issues

| Assign users to custom Kiosk workflows | Central Management is not yet capable to assign member users to custom Kiosk workflows.  
As a workaround, custom Kiosk workflows were removed from under Central Management control with Kiosk version 4.2.2.  
For details see [Kiosk section in 4.5. Product integration limitations](#). |

## 5.2.4 Version 5.2.1

| 5.2.1 Central Management release | Central Management 5.2.0 is a maintenance release most importantly to fix the configuration update issue of instances not supporting schema upgrades. |

## Fixed

| Configuration update –of instances not supporting schema upgrades–may break | Central Management 5.1.1 introduced to [periodically upgrade schema version of instances](#): with this feature it was no more necessary to re-connect instances to Central Management after the change of configuration capabilities. This feature kept the configuration descriptor (schema) on the latest possible version allowed by all of the instances of a certain product.  
Given by a bug introduced in 5.1.2, instances that do not support the schema upgrade were not taken into consideration when this latest possible schema version was selected. As a consequence, configuration possibility of instances not supporting the schema upgrade may have been broken as the configuration descriptor enforced by Central Management could be on a version, that was not understood by the instance. |
### 5.2.5 Version 5.2.2

**5.2.2 Central Management release**  
10 August, 2018

Central Management 5.2.2 is a maintenance release most importantly to fix the update issues over slow or limited network connections.

## New & improved

### Support anonymous LDAP and Active Directory bind

From now it is possible to send anonymous bind requests to LDAP and Active services. At the time of LDAP or AD bind it is possible to perform some kind of machine authentication providing a user name and a password. Performing an bind, however, this authentication is skipped.

For some further details read the instructions how to connect to an LDAP or AD server.

### Fixed

### Engines not updating over slow or limited

Some engines did not update on managed MetaDefender (Core) instances that connected to Central Management over limited network connections.

The limits have been raised, now Central Management and instance communication even over very slow connections.
### network connections

#### UNKNOWN error message

When an instance’s REST service was listening on HTTPS but the REST ADDRESS was specified as *http://...* during the creation of the instance, then Central Man displayed an error message simply saying *UNKNOWN*.

The error message have been modified to be much more specific to its cause.

#### License and engine status calculations were wrong on the Dashboard

On the **Dashboard > Overview** page, the LICENSE STATUS and the ENGINE STATUS always displayed 100%. It is fixed now to give the correct values.
### 5.2.6 Version 5.2.3

<table>
<thead>
<tr>
<th><strong>5.2.3 Central Management release</strong></th>
<th>Central Management 5.2.3 is a maintenance release to fix a few UI issues.</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 October, 2018</td>
<td></td>
</tr>
</tbody>
</table>

| **Fixed** |

<table>
<thead>
<tr>
<th><strong>Long group names overflowed into the next group</strong></th>
<th>Fix is applied and long group names will wrap into it's own group section.</th>
</tr>
</thead>
</table>

| **UI text overlapped on small screen devices and shrinked browsers** | When you downsized the browser or visited the management console on a mobile device, the text labels overlapped each other. The issue is fixed to properly display labels. |
### 5.2.7 Version 5.2.4

<table>
<thead>
<tr>
<th><strong>5.2.4 Central Management release</strong></th>
<th>Central Management 5.2.4 is a maintenance release to fix a few UI issues.</th>
</tr>
</thead>
<tbody>
<tr>
<td>26 November, 2018</td>
<td></td>
</tr>
</tbody>
</table>

#### New features

<table>
<thead>
<tr>
<th><strong>Add configuration workflow rule for DLP engine in Core 4.12</strong></th>
<th>Core 4.12 has new DLP engine integrated. CM 5.2.4 now supports configuration for DLP engine</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Updated user guide: How to configure CM to manage an instance with HTTPS</strong></td>
<td>Added topic &quot;Adding an instance with HTTPS&quot; under Instances section</td>
</tr>
<tr>
<td><strong>Update user guide: How to add products to CM</strong></td>
<td>Added the following pages to the user guide, under the Instances section:</td>
</tr>
<tr>
<td></td>
<td>- Adding Kiosk into Central Management,</td>
</tr>
<tr>
<td></td>
<td>- Adding Email Security into Central Management,</td>
</tr>
<tr>
<td></td>
<td>- Adding ICAP into Central Management,</td>
</tr>
<tr>
<td></td>
<td>- Adding Core into Central Management,</td>
</tr>
</tbody>
</table>

#### Fixed

<table>
<thead>
<tr>
<th><strong>Update Folder creating space issues</strong></th>
<th>The update folder is not cleared up after new engines are updated.</th>
</tr>
</thead>
</table>
5.2.8 Version 5.2.5

Central Management 5.2.5 is a feature release to providing language editing f

New features

Ability to export Update History to Excel

User can export Update History to CSV file format.

<table>
<thead>
<tr>
<th>SEVERITY</th>
<th>DATE</th>
<th>INSTANCE</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>info</td>
<td>2018-12-06 14:17:33 GMT+7</td>
<td>Kiosk &gt; Kiosk</td>
<td>configuration</td>
</tr>
<tr>
<td>info</td>
<td>2018-12-06 14:12:33 GMT+7</td>
<td>Kiosk &gt; Kiosk</td>
<td>configuration</td>
</tr>
<tr>
<td>info</td>
<td>2018-12-06 14:07:33 GMT+7</td>
<td>Kiosk &gt; Kiosk</td>
<td>configuration</td>
</tr>
<tr>
<td>info</td>
<td>2018-12-06 14:02:33 GMT+7</td>
<td>Kiosk &gt; Kiosk</td>
<td>configuration</td>
</tr>
<tr>
<td>info</td>
<td>2018-12-06 13:57:33 GMT+7</td>
<td>Kiosk &gt; Kiosk</td>
<td>configuration</td>
</tr>
</tbody>
</table>

Improve Management of Client Instances

Provide sorting functionality for the following columns:

- Instance Name
- Product Version
- Last Seen
Enhanced Logging for Central Management

Add more log messages and show more detailed information.

Edit the language setting of MetaDefender Kiosk from Central Management

Add a feature to edit language settings of MetaDefender Kiosk

Update User Guide: Adding MetaDefender Kiosk

MetaDefender Kiosk does not have username/password, so we must fill 'API Key' field instead.

Update User Guide: UI Localization / Customization for MetaDefender Kiosk

Describe how to edit language of MetaDefender Kiosk from Central Management.
Fixed

Active Directory binds password is in clear text

Fixed password in clear text, and thus it is now hidden.

**PASSWORD**

```
.............
```

**HOST**

```
127.0.0.1
```

**PORT**

```
25
```
5.2.9 Version 5.2.6

Central Management 5.2.6 is a feature release to providing a mechanism to detect status of MetaDefender Client instances and export them to either CSV or PDF.

### New features

<table>
<thead>
<tr>
<th>Detect and display Managed Status of MetaDefender Client instances</th>
<th>Now Central Management can analyse the Managed Status of MetaDefender Client instances. There are two kinds of Managed Status of MetaDefender Client instances: &quot;Managed&quot; and &quot;Not Managed&quot;.</th>
</tr>
</thead>
</table>

#### Instances

<table>
<thead>
<tr>
<th>INSTANCE NAME</th>
<th>MANAGED STATUS</th>
<th>HEALTH</th>
<th>ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP10-02943</td>
<td>Managed</td>
<td>100%</td>
<td>192.11</td>
</tr>
<tr>
<td>Q8TJIINRAM</td>
<td>Not Managed</td>
<td>0%</td>
<td>98.03</td>
</tr>
<tr>
<td>Q3XOEWPZZ</td>
<td>Not Managed</td>
<td>0%</td>
<td>110.2</td>
</tr>
</tbody>
</table>

| Engine status in health score | Make the engines' status more reflected in the health score |
Providing a search feature in the Instances menu.
User now can search for a specific instance by either "instance name", "addre

User now can export a list of instances to CSV or PDF
### Fixed

<table>
<thead>
<tr>
<th>&quot;Managed Status&quot; column width is a little smaller than &quot;Address&quot; one</th>
<th>Make the width of &quot;Managed Status&quot; and &quot;Address&quot; columns more relevant</th>
</tr>
</thead>
</table>

API key is now hidden.
### Password support in API key section

<table>
<thead>
<tr>
<th>REST ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://localhost:8009/metadefender_rest/">http://localhost:8009/metadefender_rest/</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CREDENTIALS</th>
</tr>
</thead>
<tbody>
<tr>
<td>USERNAME</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>API KEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>*****</td>
</tr>
</tbody>
</table>
## 5.2.10 Version 5.2.7

### 5.2.7 Central Management release
11 Apr, 2019

Central Management 5.2.7 is a feature release to providing a processing history page to collect all scan logs from MetaDefender Core instances. In addition, this release introduces features for searching, filtering and exporting scan logs to CSV.

Other enhancements include features such as, importing configurations selected as default when adding an instance and license setting enhancements.

### New features

#### Processing a history page with filtering, searching and exporting options

Central Management can now display scan history from all MetaDefender Core instances.

![Processing History](image)

**Processing History**

- **Fetch history from instance:**
  - 1

- **Filter by result:**
  - All

**RESULT**

<table>
<thead>
<tr>
<th>No Threat Detected</th>
<th>processinghistory-csv</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Threat Detected</td>
<td>c++_book 1.pdf</td>
</tr>
</tbody>
</table>

#### Import configuration is made by default

When adding a new instance to a group. Option import configuration is ticked by default.

![Import Configuration](image)

**API KEY**

**CONFIGURATION**

- IMPORT CONFIGURATION (NOTE THIS IS ONLY USED IF THIS IS THE FIRST INSTANCE FOR THE GIVEN PRODUCT!)

#### Adding an API to support CM

Developing an User info API to support migrating user data from Central Management.
<table>
<thead>
<tr>
<th>migration to OPSWAT Central Management in future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed</td>
</tr>
<tr>
<td><strong>Set number of agents for unlimited license activation</strong></td>
</tr>
<tr>
<td><strong>Auto-detect CDR configuration</strong></td>
</tr>
</tbody>
</table>
5.2.11 Version 5.2.8

5.2.8 Central Management release
23 May, 2019

Central Management 5.2.8 provides enhanced features for processing history, error messages, and engine configuration detection.
<table>
<thead>
<tr>
<th>Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enhance engine configuration detection logic</strong></td>
</tr>
<tr>
<td><strong>Reset page number when changing group in processing history page</strong></td>
</tr>
<tr>
<td><strong>Change message warning when authentication failed</strong></td>
</tr>
</tbody>
</table>
### 5.2.12 Version 5.2.9

**5.2.9 Central Management release**

5 July, 2019

Central Management 5.2.9 provides the correction of product names, MetaDefender.

### Enhancement

**Change all product names with MetaDefender prefix at the Overview page**
<table>
<thead>
<tr>
<th>Change all product names with MetaDefender prefix at the Dashboard page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dashboard: Central Management</strong></td>
</tr>
<tr>
<td><strong>METADEFENDER CORE INSTANCES</strong></td>
</tr>
<tr>
<td>- 1</td>
</tr>
<tr>
<td>- LICENSE STATUS 1/1</td>
</tr>
<tr>
<td>- 100%</td>
</tr>
<tr>
<td><strong>Total Objects Processed</strong> Last 30 days</td>
</tr>
<tr>
<td><strong>Update help document for adding MetaDefender Kiosk</strong></td>
</tr>
<tr>
<td>From MetaDefender Kiosk 4.3.0, username/password authentication will be used</td>
</tr>
<tr>
<td><strong>Update Metadefender Core's health score calculation</strong></td>
</tr>
<tr>
<td>Update Metadefender Core's health score calculation to check only enabled engines</td>
</tr>
</tbody>
</table>
6. Errata

| Central Management errata | This errata document contains late-breaking news about the latest Central Management release. Before installing this version, it is important to consult this document to learn about any post-release discoveries or problems that may already have been found and fixed. |

⚠️ Updated on-line only

This errata document is updated in the on-line documentation only. The on-line errata is available at [https://onlinehelp.opswat.com/centralmgmt/6._Errata.html](https://onlinehelp.opswat.com/centralmgmt/6._Errata.html).
7. Legal

- Copyright
- Export Classification EAR99

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.

Export Classification EAR99

EAR99 (Export Administration Regulation 99) is an export classification category regulated by the U.S. Department of Commerce that covers most commercial items exported out of the U.S.

OPSWAT’s software is designated as EAR99, and there are no export restrictions other than embargoed countries and persons.
8. Knowledge Base Articles

How long is the support life cycle for a specific version/release of MetaDefender Central Management v5?

OPSWAT provides support on each release of MetaDefender Central Management for 12 months after the publication of the next release of the product (i.e. once a new release is published, you have 12 more months of support on the previous release). However, bug fixes and enhancements are applied only to the next release of a product, not to the current release or historical releases, even when those releases are still under support. In some cases, hotfixes can be provided for the current release of the product and then incorporated as a regular fix in the next release.

OPSWAT strongly encourages customers to upgrade to the latest release on a regular basis and not to wait until the end of a release supported life-cycle.

Please note: MetaDefender Central Management will reach the end of support on 30 Sep 2019. Every version that is released after 30 Sep 2018 (5.2.3) will not follow the regular 12 months support life cycle and have an end of support date on 30 Sep 2019.

<table>
<thead>
<tr>
<th>Release number</th>
<th>Release date</th>
<th>End-of-life date</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.9</td>
<td>05 Jul 2019</td>
<td>30 Sep 2019</td>
</tr>
<tr>
<td>5.2.8</td>
<td>23 May 2019</td>
<td>30 Sep 2019</td>
</tr>
<tr>
<td>5.2.7</td>
<td>11 Apr 2019</td>
<td>30 Sep 2019</td>
</tr>
<tr>
<td>5.2.6</td>
<td>27 Feb 2019</td>
<td>30 Sep 2019</td>
</tr>
<tr>
<td>5.2.5</td>
<td>04 Jan 2019</td>
<td>30 Sep 2019</td>
</tr>
<tr>
<td>5.2.4</td>
<td>27 Nov 2018</td>
<td>30 Sep 2019</td>
</tr>
<tr>
<td>5.2.3</td>
<td>24 Oct 2018</td>
<td>30 Sep 2019</td>
</tr>
<tr>
<td>5.2.2</td>
<td>10 Aug 2018</td>
<td>30 Sep 2019</td>
</tr>
<tr>
<td>5.2.1</td>
<td>13 Jul 2018</td>
<td>10 Aug 2019</td>
</tr>
</tbody>
</table>
How to create support package for Central Management?

To ensure the best help from OPSWAT support, you can create a support package with a tool that comes with Central Management. The support package contains essential information regarding the operating system and OPSWAT software found on the machine.

**Linux**

To create a package you must start the script found under `/usr/bin/mdcentralmgmt-collect-support-data.sh`.

As the script processes the necessary information, the script generates the support package output.

The package is a tar.gz archive with the following name:

```
mdcentralmgmt-support--<TIMESTAMP>.tar.gz
```

The timestamp is the package generation date.

Example:
The generated package will be placed in the same location where the script was ran.

**Windows**

To create a package you must start the script found under the installation directory of the product. By default this is `C:\Program Files\MetaDefender Central Management\mdcentralmgmt-collect-support-data.bat`.

As the script processes the necessary information, the script generates the support package output.

The package is a zip archive with the following name:

```
mdcentralmgmt-support-<TIMESTAMP>.zip
```

The timestamp is the date when the package was generated.

Example:

```
mdcentralmgmt-support-1439983514.zip
```

The generated package will be placed in the same location where the script was ran.

**Content of the created package**

The support package contains the following elements:

- **configuration**: the configuration files of OPSWAT software found on machine
- **log**: the log files of OPSWAT software found on machine
- **system information**: system information stored in file named `os.info`
- **hardware information**: hardware information stored in file named `hw.info`
- **network information**: network information stored in file named `network.info`
- **directory information**: OPSWAT software directory information stored in file named `files.info`
- **copy of config database**: configuration database **WITHOUT** user data

You can check the content of the generated package to make sure it does not contain any confidential information.
How to read the Central Management log?

MetaDefender Central Management generates log files under `/var/log/mdcentralmgmt`. The log files are plain text files that can be opened with any text editor.

**Files**

The Central Manager generates a log file under `/var/log/mdcentralmgmt` named `mdcentralmgmt.log`.

**Format**

In the log, each line represents a log message sent by the server or agent. Depending on the log file, the format of the line is as follows:

```
[LEVEL] TIMESTAMP (COMPONENT) MESSAGE [msgid: MESSAGE ID]
```

Example:

```
[INFO   ] 2015.11.18 15:46:06.026: (mgmt.instance) Instance status gathered, 'MetaDefender Core v4', version='4.1.0' [msgid: 786]
```

The different values are:

- **LEVEL**: the severity of the message
- **TIMESTAMP**: The date value when the log entry was sent
- **COMPONENT**: which component sent the entry
- **MESSAGE**: the verbose string of the entry's message
- **MESSAGE ID**: the unique ID of this log entry

**Severity levels of log entries**

Depending on the reason for the log entry, there are different types of severity levels.

Based on the configuration, the following levels are possible:
Installing Central Management on Debian 9

Symptom
When you install Central Management on Debian 9 you may get the following error message:

```
dpkg: dependency problems prevent configuration of mdcentralmgmt:
  mdcentralmgmt depends on libssl1.0.0 (>= 1.0.0); however:
    Package libssl1.0.0 is not installed.
```

Reason
By default, Debian 9 is installed with libssl1.0.2. For compatibility reasons OPSWAT products require libssl1.0.0. libssl1.0.0 is, however, only available in Debian 8 repositories, and is not available for Debian 9.

Resolution
To install libssl1.0.0 on Debian 9 from a Debian 8 repository perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot / Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Screenshot / Example</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>1</td>
<td>Open <a href="https://packages.debian.org/jessie/libssl1.0.0">https://packages.debian.org/jessie/libssl1.0.0</a> in your browser</td>
<td><img src="image-url" alt="Screenshot" /></td>
</tr>
<tr>
<td></td>
<td><strong>Package: libssl1.0.0 (1.0.1t-1+deb7u1) Secure Sockets Layer toolkit - shared libraries</strong></td>
<td><img src="image-url" alt="Package Details" /></td>
</tr>
<tr>
<td></td>
<td>This package is part of the OpenSSL project's implemen of the SSL and TLS cryptographic protocols for secure communication over the Internet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>It provides the libssl and libcrypto shared libraries.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Tags:</strong> Implemented in: C  <strong>Role:</strong> Shared Library</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>In the <strong>Downloads</strong> section at the bottom of the page select your server's architecture</td>
<td></td>
</tr>
</tbody>
</table>
### Step 3: Download libssl1.0.0

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Package Size</th>
<th>Installed Size</th>
<th>Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>amd64</td>
<td>1,021.8 kB</td>
<td>3,075.0 kB</td>
<td>list of files</td>
</tr>
<tr>
<td>arm64</td>
<td>844.5 kB</td>
<td>2,572.0 kB</td>
<td>list of files</td>
</tr>
<tr>
<td>armel</td>
<td>831.2 kB</td>
<td>2,283.0 kB</td>
<td>list of files</td>
</tr>
<tr>
<td>armhf</td>
<td>846.9 kB</td>
<td>1,863.0 kB</td>
<td>list of files</td>
</tr>
<tr>
<td>i386</td>
<td>2,001.2 kB</td>
<td>7,465.0 kB</td>
<td>list of files</td>
</tr>
<tr>
<td>mips</td>
<td>865.9 kB</td>
<td>2,759.0 kB</td>
<td>list of files</td>
</tr>
<tr>
<td>mipsel</td>
<td>874.7 kB</td>
<td>2,759.0 kB</td>
<td>list of files</td>
</tr>
<tr>
<td>powerpc</td>
<td>881.6 kB</td>
<td>2,849.0 kB</td>
<td>list of files</td>
</tr>
<tr>
<td>ppc64el</td>
<td>901.7 kB</td>
<td>3,106.0 kB</td>
<td>list of files</td>
</tr>
<tr>
<td>s386x</td>
<td>844.6 kB</td>
<td>3,174.0 kB</td>
<td>list of files</td>
</tr>
</tbody>
</table>

This page is also available in the following languages (How to set up de have de Wood, de Russian, de English)

To report a problem with the website, e-mail debian-lists@debian.org.

Content Copyright © 1997 - 2018 SPI Inc.; See license terms. Debian is sponsored by 1&1 Internet AG.

---


```
# wget http://ftp.cz.debian.org/debian/pool/main/o/openssl/libssl1.0.0_1.0.1t-1+deb8u7_amd64.deb
```

4. Install the downloaded package

```
# dpkg -i libssl1.0.0_1.0.1t-1+deb8u7_amd64.deb
```
### What you need to check if your Web Management Console is not responding after you installed the Central Management

If you cannot access the Web Management Console from your browser and you get an error message (connection refused) or your browser is waiting for reply after you installed the Central Management on your machine, please check the following instructions:

1. Please make sure your computer can access the Central Management IP address.
2. Please make sure you entered the correct URL into your browser.
3. Please make sure you opened the firewall port on the Central Management server for the Web Management Console. Consult your Linux Distribution manual on how to configure a firewall in your distribution.

If you have done all this and you are still receiving the error, please submit a support ticket via the OPSWAT Portal.

---

This article pertains to MetaDefender Central Management

This article was last updated on 2018-03-28

CN
What you need to do if you see too many TIME_WAIT sockets

If TCP connections are in use the port limit can be reached. In this case, no new connection can be created. This can happen on the Agent or Server side.

**How to detect**

Kernel message:

```
```

Check the TIME_WAIT sockets count:

```
watch -n 1 "netstat -nt | grep TIME_WAIT | wc -l"
```

If it is close to the available port range then your system is affected by this issue:

```
cat /proc/sys/net/ipv4/ip_local_port_range
```

**Solution**

You should enable socket reuse.

By default Linux selects a port from an ephemeral port range, which by default is within the range of 32768 to 61000.

A TCP local socket address that has been bound is unavailable for some time after closing, unless the `SO_REUSEADDR` flag has been set. Please use caution when using this flag as it makes TCP less reliable.

To avoid waiting on closed sockets and enable their reuse, please set `tcp_twReuse` sysctl to enable reuse of TIME_WAIT sockets by appending the following line to file `/etc/sysctl.conf`:

```
net.ipv4.tcp_tw_reuse = 1
```

Afterwards, sockets in state TIME_WAIT will be reused when necessary.

**Technical Insights**

Connect function error value in these cases is `EADDRNOTAVAIL`. 