OPSWAT Metadefender™

Table of Contents

About this guide

Metadefender Central Management provides a comprehensive framework for systems administrators to manage Metadefender Core installations. The purpose of this guide is to introduce you to the flexible configuration options available in Metadefender 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 Metadefender Central Management

This guide describes the basic steps for installing Metadefender Central Management:

1. Step 1. Installation
2. Step 2. License activation
3. Step 3. Start using Metadefender Central Management

This Quick Guide assumes that the test machine has working Internet connection.

1.1. Installation

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

Installing Metadefender Central Management on Ubuntu or Debian computers

1. Download mdcentralmgmt package from the OPSWAT Portal. Make sure that you download the applicable package for your distribution.
2. Upload the installation package to your test computers
3. Install the product with `sudo dpkg -i <filename>`, where filename is the package you downloaded from our portal
4. If dpkg shows error messages about missing dependencies you should execute `sudo apt-get install -f`
5. Open a web browser and point to `http://<server name or IP>:8018`
6. Enter default login credentials, username: admin, password: admin

Installing Metadefender Central Management on Red Hat Enterprise Linux or CentOS computers

1. Download mdcentralmgmt package from the OPSWAT Portal. Make sure that you download the applicable package for your distribution.
2. Upload the installation package to your test computers
3. Install the product with `sudo yum install <filename>`, where filename is the package you downloaded from our portal
4. Open a web browser and point to `http://<server name or IP>:8018`

5. Enter default login credentials, username: admin, password: admin

To continue the basic setup, follow the license activation instructions on Step 2. License activation

For more information on Installation procedures see Installing Metadefender Central 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.

1. Press the *ACTIVATE* button to bring up the Activation menu, 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: you can upload a manually acquired license file.
    - Request trial key online: if you want to try out the product first, you can receive a trial Activation key via email.
2. Select the `Request trial key online` option
3. Follow the on-screen instructions

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.

When your hardware information changes, for example your mac address changes because the product runs in a virtual machine, the license get automatically reactivated on the first update attempt.

1.3. Start using Metadefender Central Management

After installation and activation only adding instances are left.

Please find details in chapter Instances.

2. Installing or Upgrading Metadefender Central Management

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

2.1. Before Installation

Before installing Metadefender Central Management make sure the target computer meets the hardware and software requirements of Metadefender Central Management.

2.1.1. System Requirements

Please confirm that your system meets the minimum requirements listed below before installing Metadefender Central Management.

Only 64-bit platforms are supported.

- Operating System:
  - CentOS 6.6, 7.0+
  - Red Hat Enterprise Linux 6.6, 7.0+
  - Debian 7.0,
  - Ubuntu 12.04, 14.04
  - Windows 7+ (64 bit)
  - Microsoft Windows Server 2008 R2 or newer (64 bit)
- Hardware requirements
  - RAM: min. 2 GB
  - HDD: 2 GB + ~500MB * [number of managed scan engines]

Metadefender Central Management uses these folders for storing scan engine resources:

- On Linux: /var/
- On Windows: <INSTALL FOLDER>

2.1.2. Browser Requirements for the Metadefender Central Management Console

One of the following browsers is required to view the Metadefender Central Management Console:

- Internet Explorer 10 or later
- Chrome
- Firefox
- Safari 7 or later

Chrome and Firefox are tested with the latest available version at the time of release.

2.2. Installing Metadefender 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
3. Open a web browser and point to `http://<server name or IP>:8018`
4. Login with the default credentials, username: **admin**, password: **admin**
5. You must Activate this deployment to use its features

Installation

Installing Metadefender Central Management using Command Line

Installation notes

- If the Metadefender 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. Installing Metadefender Central Management using Command Line

Preliminary notes

- If the Metadefender 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 package (.deb)

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

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

```
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 keys and their default values are the following:

Key	Default Value	Description
RESTADDRESS	0.0.0.0	REST interface binding address
RESTPORT	8018	REST interface binding port

For details on using msiexec please consult Windows installer documentation.

2.3. Upgrading Metadefender Central Management

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

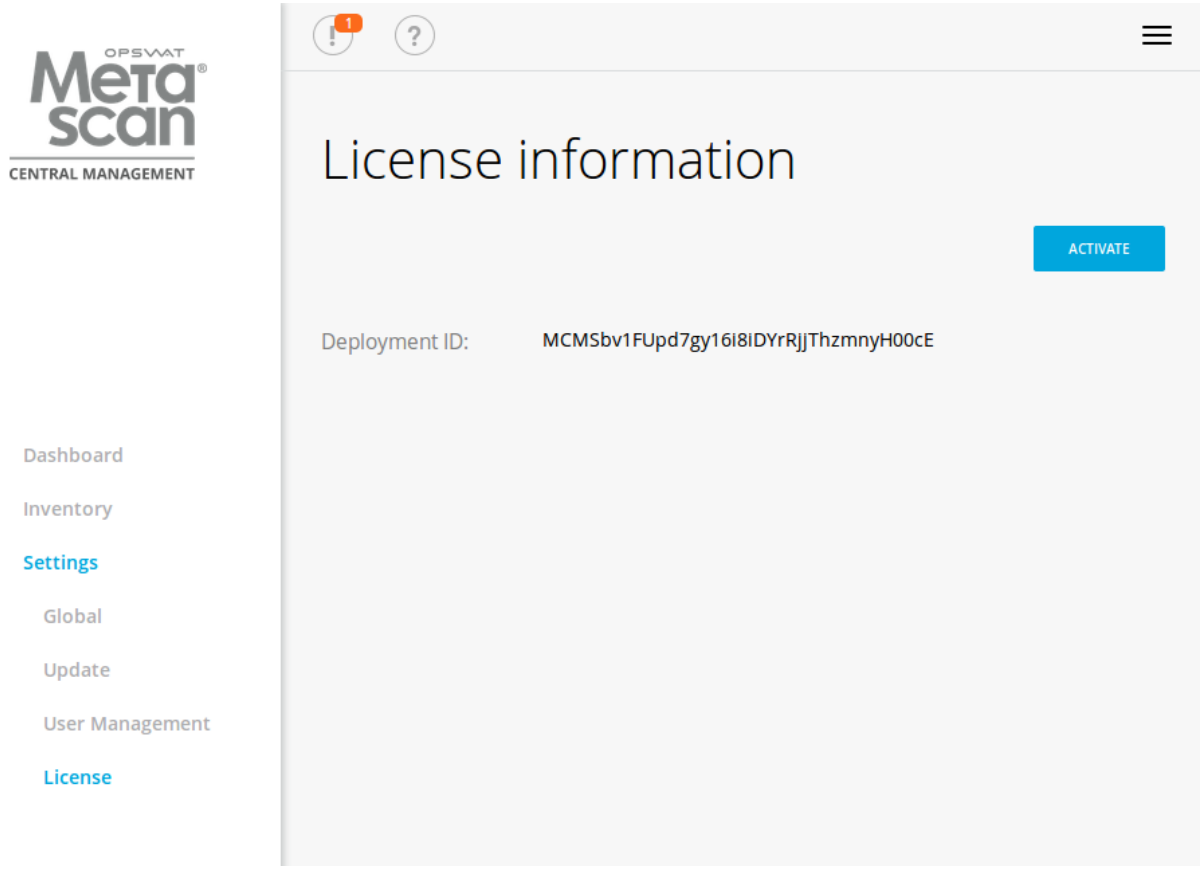
All existing Metadefender Central Management configuration and data will be kept during the upgrade.

2.4. Metadefender Central Management Licensing

In order to use Metadefender Central Management you need to activate the product. If you do not have an activation key you can request a 14 day evaluation key during the activation process.

2.4.1. Activating Metadefender Central Management Licenses

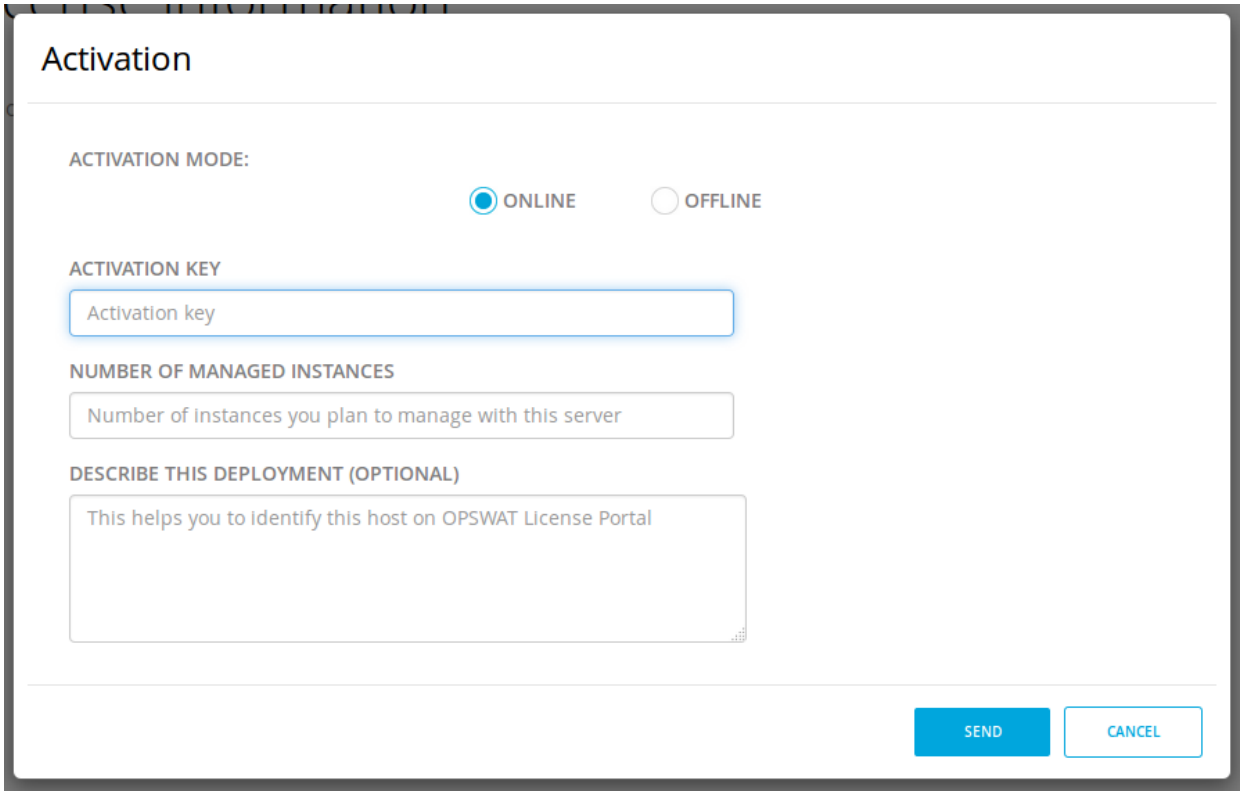
To activate your installation go to the Settings > License menu in the Web Management Console. If you have no valid license, you will only see your installation's Deployment ID. You will also see a warning in the Web Management Console header.



Settings/License page, when no valid license exists

Press the *ACTIVATE* button to bring up the Activation menu, 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 displayed instructions.



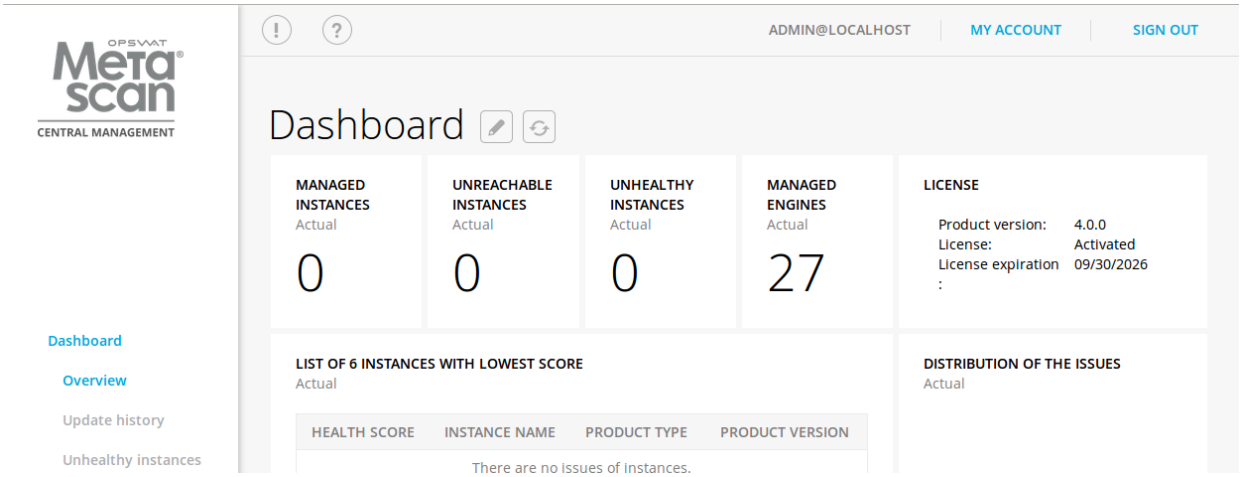
Settings/License/ACTIVATE page

If you activated your installation online, 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 Your Metadefender Central Management License

Go to the Dashboard > Overview menu in the Web Management Console, in the License dashboard widget you will see the following information:

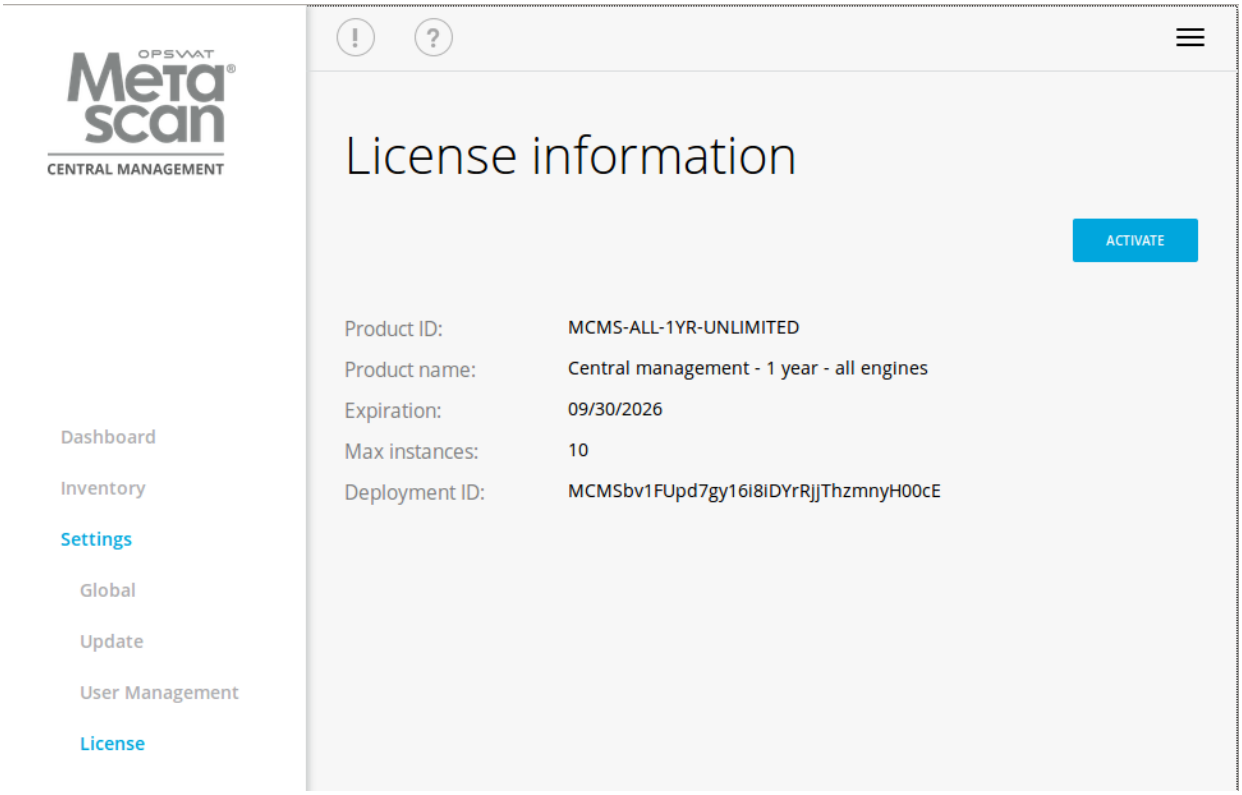
- License: activation state of the license
- License expiration: last day of license validity
- Allowed instances: maximum number of instances that are manageable



Dashboard/Overview page

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

- Product ID: product identification as on your order
- Product name: product name as on your order
- Expiration: last day of license validity
- Max instances: maximum number of instances that can are manageable
- Deployment ID: identification of this installation



Settings/License page

3. Configuring Metadefender Central Management

3.1. Metadefender Central Management configuration

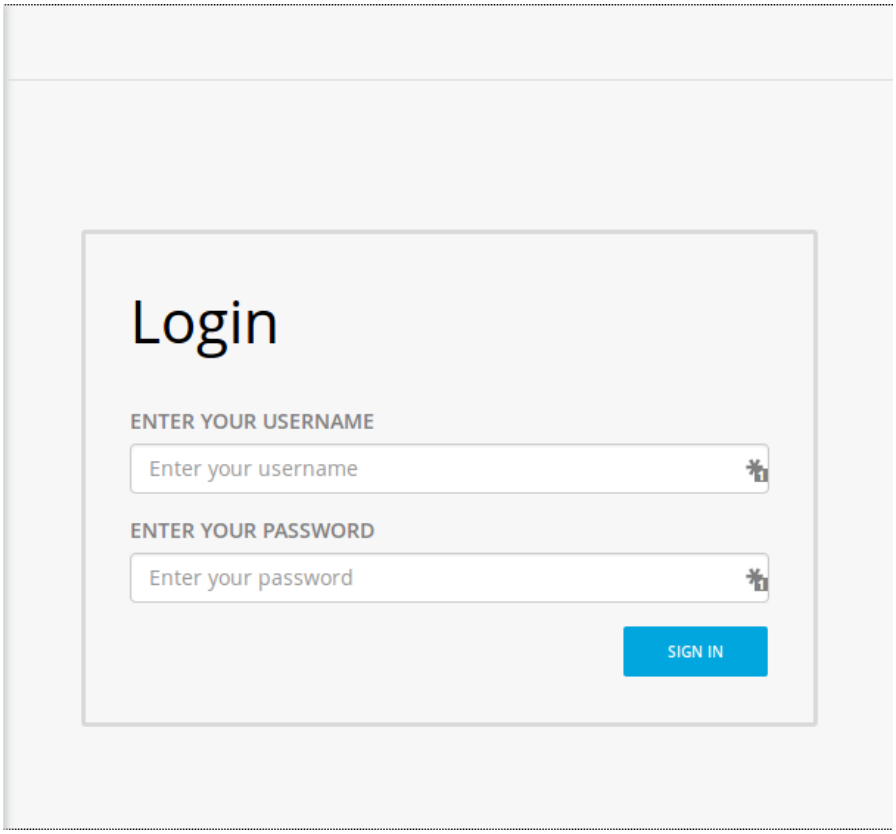
The Metadefender Central Management configuration is separated into two parts. The basic server configurations are stored in the configuration files. Other configuration values can be set via the Web Management Console.

3.1.1. Management Console

The management console is available at: `http://<Metadefender Central Management Server>:8018/`
where <Metadefender Central Management Server> is the name or IP address of the system where Metadefender Central Management is installed.

After installing the product the default password for the **admin** user is **admin**.

Every change made in the Metadefender Central Management configuration via the Management console is applied when you select **Save settings** or **OK**, except if the change cannot be applied.



Login screen

3.1.2. Metadefender Central Management server configuration file

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

After modifying the server configuration file you must restart the Metadefender 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

parameter	default value	required	description
restaddress	0.0.0.0	required	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)
restport	8018	required	Designated port number for the web and REST interface

[logger] section

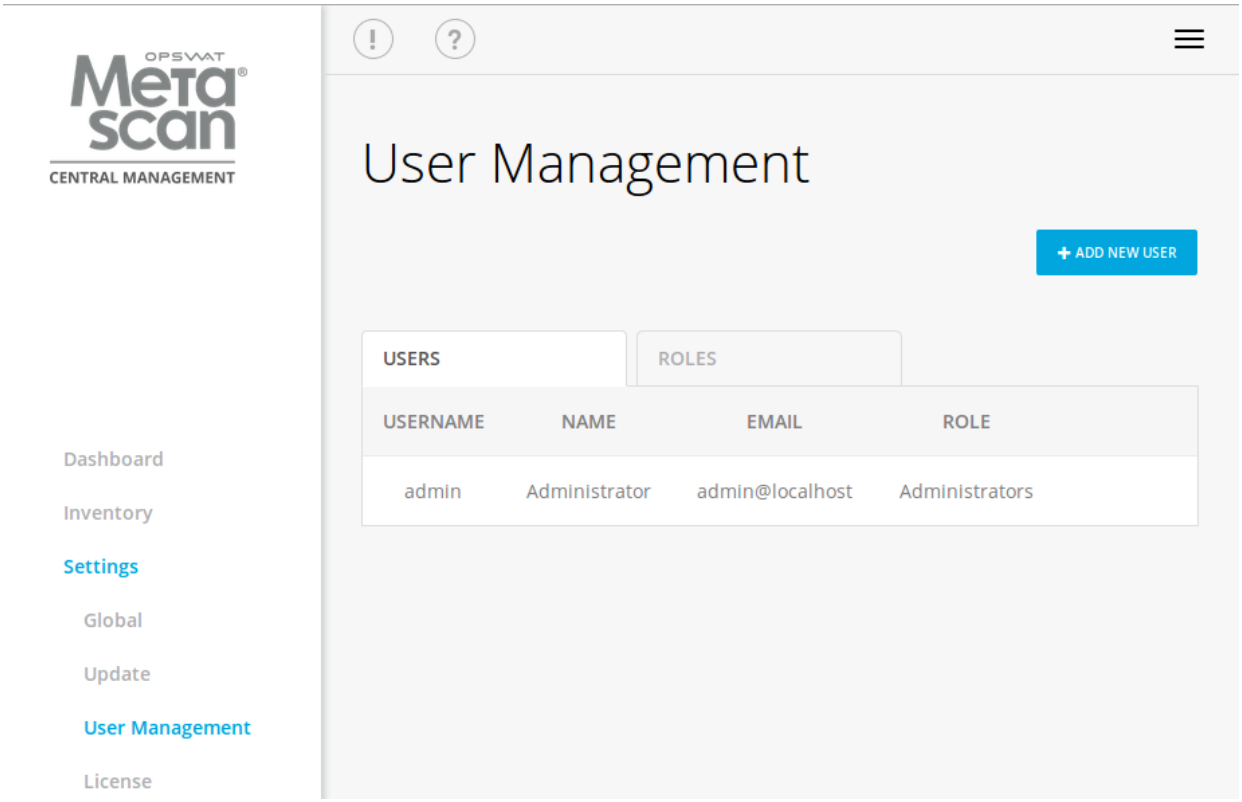
key	default value	required	description
logfile	/var/log /mdcentralmgmt /mdcentralmgmt.log	optional	Full path of a logfile to write log messages to
loglevel	info	optional	Level of logging. Supported values are: debug, info, warning, error
syslog		optional	Switch on logging to a local ('local') or remote ('protocol://hostname:port') syslog server
syslog_level		optional	Level of logging. Supported values are: debug, info, warning , error

3.2. User management

After installation a default user is created with the following credentials:

- username: admin
- password: admin

User management is accessible from **Settings > User Management** after successful login.



User management

Under the **Users** tab:

- new users can be added
- existing users can be viewed
- existing users can be modified
- existing users can be deleted

Under the **Roles** tab:

- existing roles can be viewed

Each role has a set of rights. Each of these rights represent access to a specific part of Metadefender Central Management.
A user has all of the rights of it's rules. Currently only the **admin** right exists which give the user full access.

3.3. Update settings

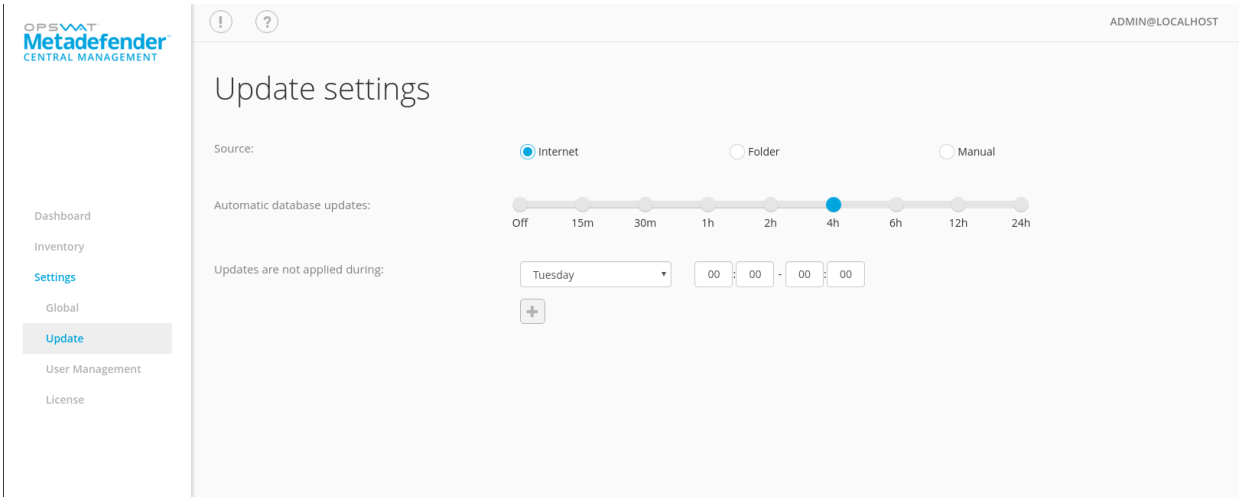
Update settings are accessible under **Settings > Update** after successful login.

On this page the update mechanism can be choosen between three different methods

- Internet

- Folder
- Manual

Internet



Internet update method

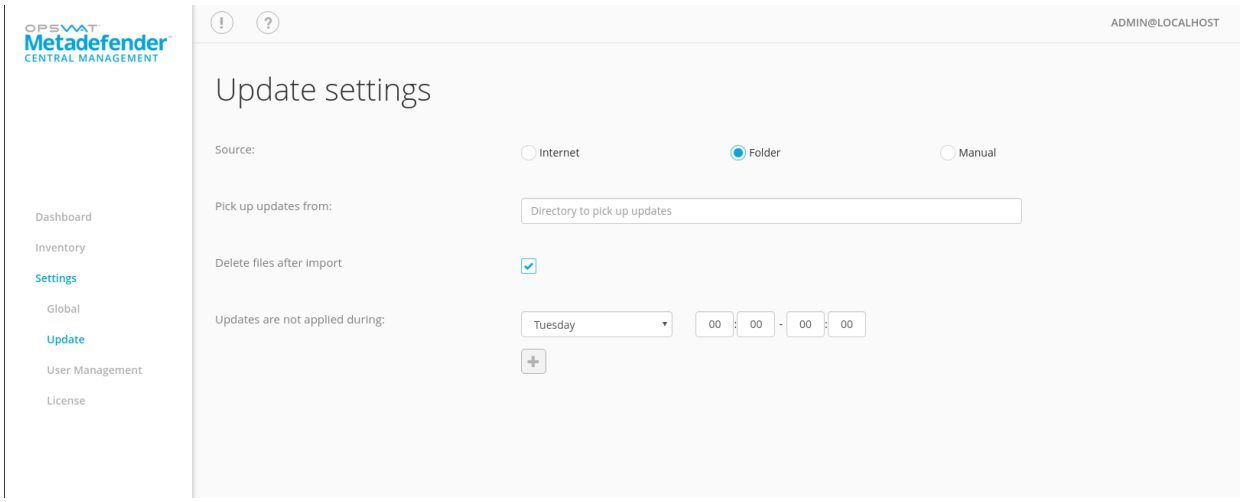
Choosing the **Internet** method means the product will do automatic update downloading from the internet.

To set the frequency of these updates choose the corresponding value presented on the **Update interval** scrollbar.

Setting off the interval means the update will only occur, when the **Update Now** button is clicked on the engines page under **Inventory > Engines**.

With the **Updates are not applied during** field it is configurable when NOT to distribute update packages to managed instances.

Folder



Folder update method

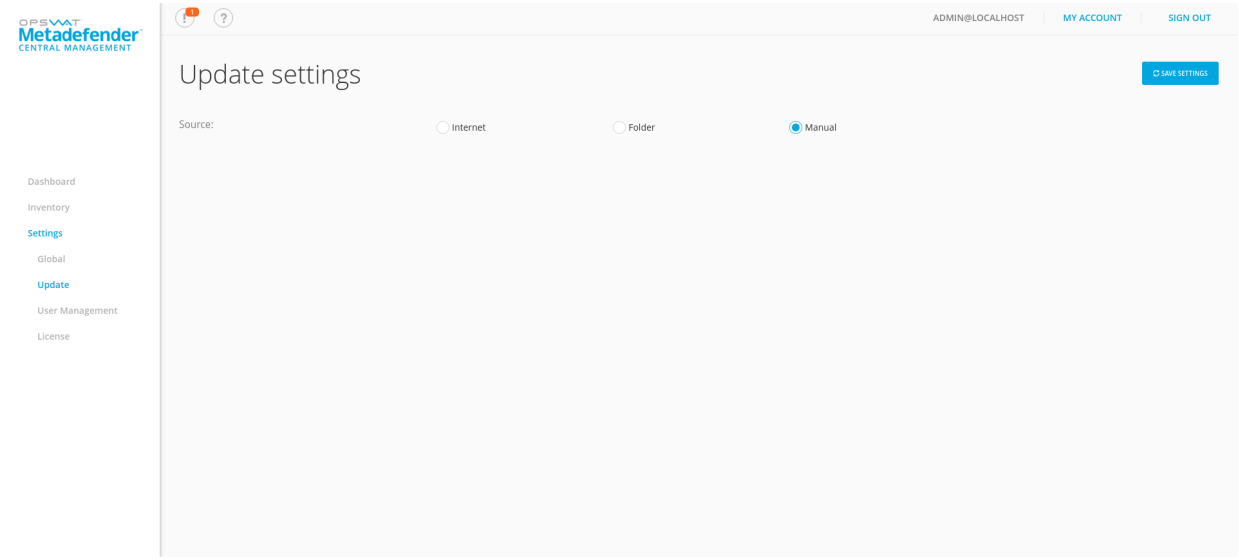
Choosing the **Folder** method will make the product searching for updates in a specific folder set in the **Pick up updates from** option.

The product watches the folder for modification, whenever the content is modified it will try to pick
up the files placed under the folder.

Another option of this method is **Delete files after import**, which means product will delete files after they were processed successfully. This means even if an update could not be applied, it will be
removed because it was processed without any issue.

With the **Updates are not applied during** field it is configurable when NOT to distribute update packages to managed instances.

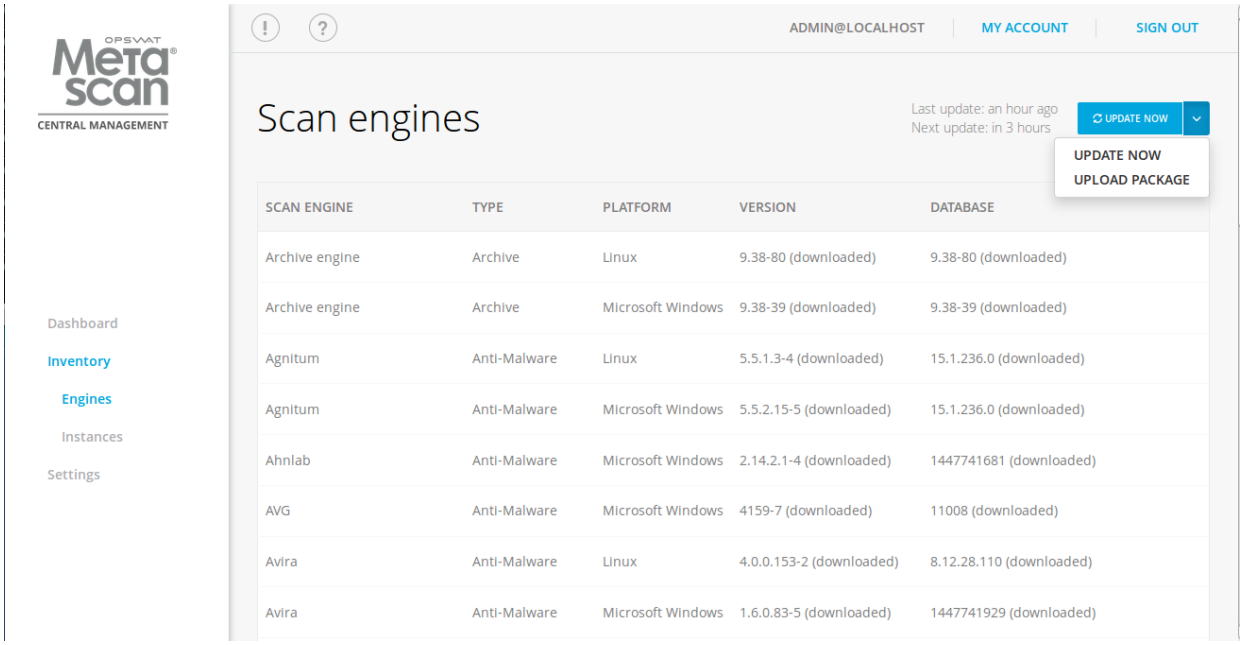
Manual



Manual update method

Choosing the **Manual** option will turn off any automatic udpate mechanism stated above and only accepts
updates uploaded directly on the engines page under **Inventory > Engines**.

Choosing this method will set the default operation to **Upload Package** on the engines page instead of **Update Now**.



Manual upload

With the **Upload Package** option, engine/database updates can be installed.

3.4. Logging

Metadefender Central Management has wide variety of options to configure logging. Log settings are in the configuration files. To see more details about log configuration see the following pages:

Configuration
Debug logging

3.4.1. Configuration

To configure the log outputs and levels, consult the following paragraph:

- Metadefender Central Management server configuration file

The installer configures the **logrotate** service to handle the centralmgmt log files.

Configuration file is located:

- /etc/logrotate.d/mdcentralmgmt

The default configuration will rotate daily and store the last 30 days.

If the log file path is modified, the logrotate config file should be updated as well.

The new log settings will be used after a service restart or a HUP signal.

3.4.2. Debug logging

To provide debug logs for the OPSWAT support team, the level of the logfile for the given service (mdcentralmgmt) must be set to 'debug'.

Next, execute the scenarios requested by the support team, and collect the generated log files from the configured location.

After that the log level should be set back to 'info'. In debug level the size of the logfile size will increase significantly.

For information on how to modify the logging settings of the product consult the paragraph: Configuration

For information on other data that OPSWAT support might require go to Knowledge Base/How to create support package?

For information on how to interpret the log files consult: Knowledge Base/How to read the centralmgmt log?

3.5. Configuring SSL

Metadefender 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 Metadefender Central Management server configuration by following the next steps:

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:

```
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.

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 SSL-options please consult Nginx documentation.

3.6. Configuring proxy settings

How can I set proxy server for the product

Linux

Under Linux set the environment variable `http_proxy` or `https_proxy` for the system.

Windows

Under Windows use the netsh tool to set the proxy, e.g.: `netsh winhttp set proxy <ADDRESS>`

In same 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.

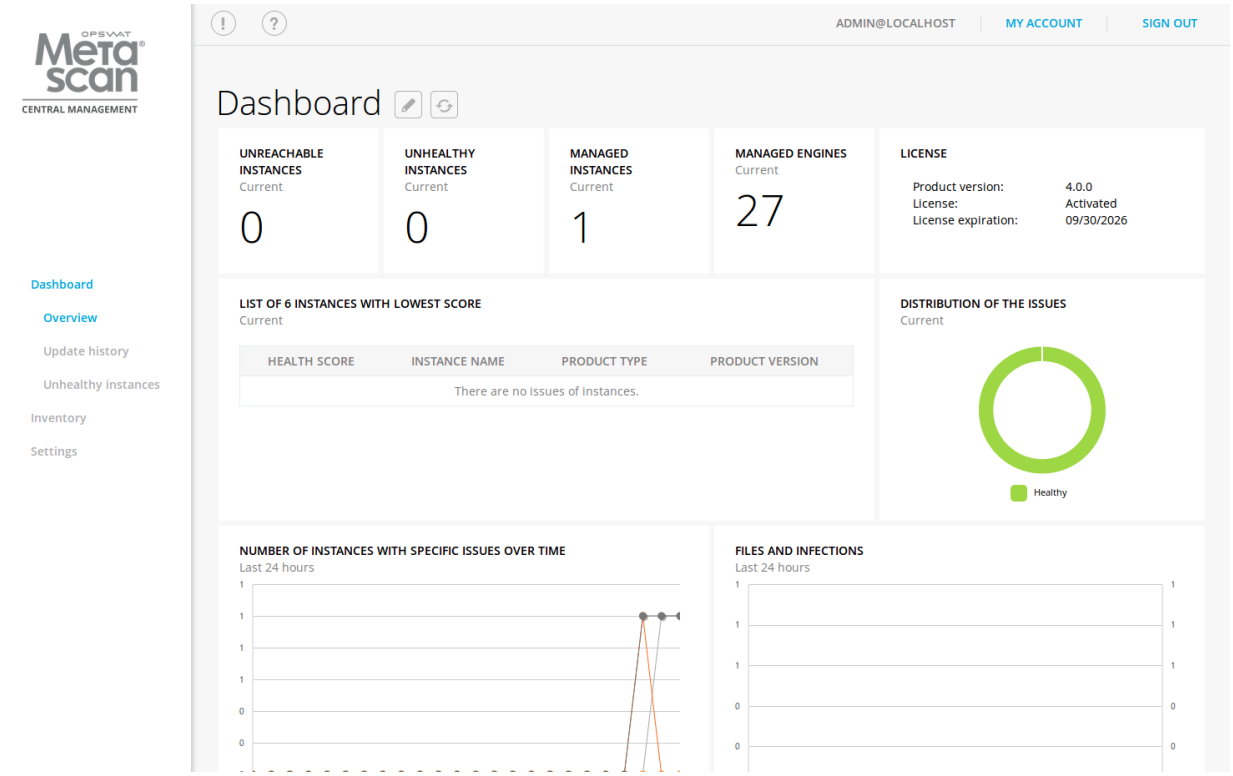
You might need to configure Windows proxy to bypass local addresses (or instance addresses) if you can't access Web Management Console from the host itself and/or if Central Management can access managed instances via your proxy. Consult netsh documentation for additional configuration options.

4. Operating Metadefender Central Management

4.1. Dashboard

Metadefender Central Management provides a Web-based user interface (default port is 8018) that gives a general overview of Metadefender Central Management status and allows you to configure its options.

Note that the default refresh rate of displayed information is 30 seconds.



Dashboard overview

Overview page

The Overview page shows information on

- Number of unreachable instances
- Number of unhealthy instances

- Number of managed instances
- Number of managed engines
- Licence information
- List of 6 instances with lowest score
- Distribution of the issues
- Number of instances with specific issues over time
- Files and infections

Both the default refresh rate (default is 30 seconds) and the span of time displayed (30 days) can be changed.

Update history

The Update history shows information on 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.

Unhealthy instances

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

- Satus
- Health score
- Instance name
- Product type
- Product version
- License status
- Date and time the instance was last available

Health 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 sore values. Calculation of the actual score uses the following factors:

- if 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

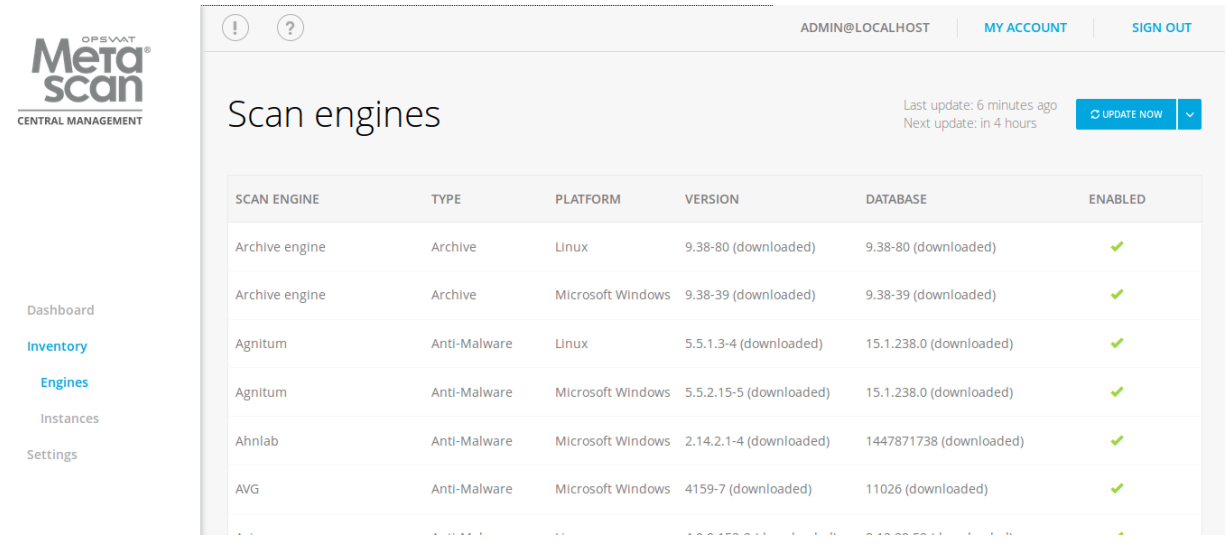
4.2. Inventory management

Metadefender Central Management displays detailed information on scan engines including anti-malware engines, archive engines, etc. and and status of managed instances too.

4.2.1. Engines

Under the **Engines** menu all the installed engines are listed with their details such as

- Name of engine
- Type of engine. Possible types are
  - Archive engine
  - Anti-malware engine
  - Filetype detection engine
  - Utility engine
- Platform the engine runs on
- Engine version
- Database version the engine is using



Engines

To manually trigger update of scan engine and database packages, click on the **Update now** button.

To provide engine or database packages on your own, select the **Upload package** option.

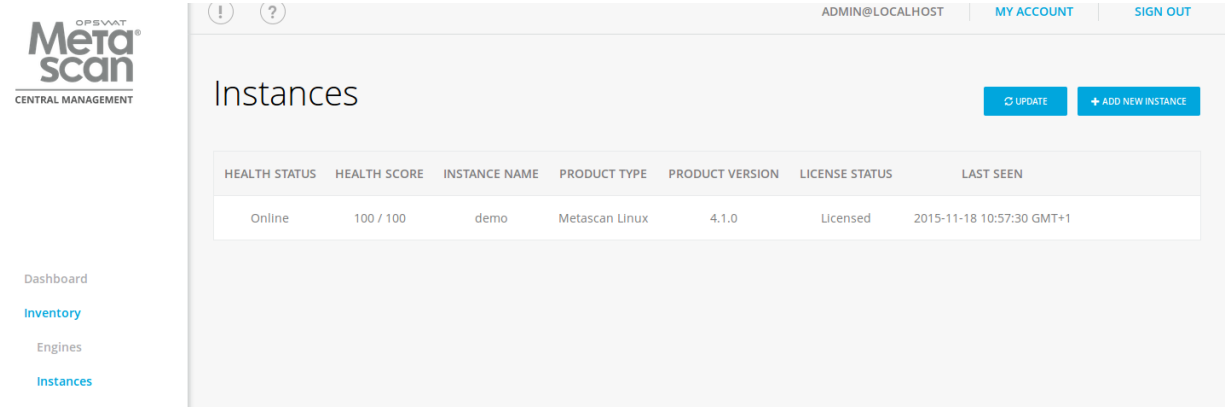
Engines can be disabled (and re-enabled afterwards) by clicking on the cross button. When an engine is disabled neither the engine nor the corresponding database package is updated and it will be removed from every agent. Status of the engine is displayed by green mark sign, grey cross sign meaning the enabled or disabled accordingly.

Note that in case of having a Metadefender Core v3 database update for which remote engine update is not supported, engine version information is not shown.

4.2.2. Instances

Under the **Instances** menu the manged instances are listed with the following information:

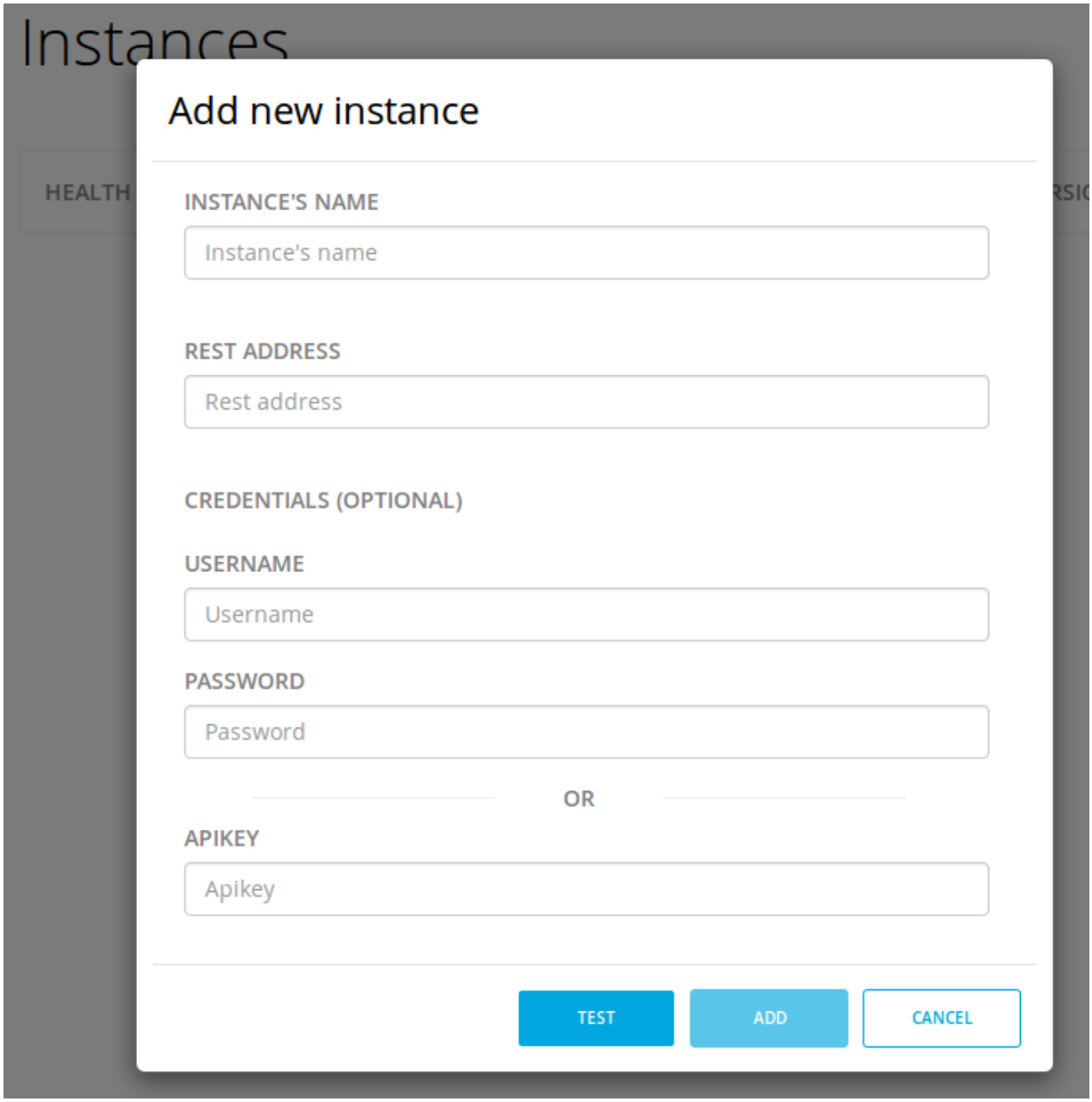
- Health status
- Health score
- Instance name
- Product type
- Product version
- License status
- Instance last seen



Instances

Add instances

Pressing the button **Add New Instance** one can manage Metadefender Core instances. Both version 3 and 4 are supported.



Add instance

Add v3 Instance

You should add a name for the instance and the REST address of the Metadefender Core server. URL needs to be fully qualified with scheme provided: `http(s)://<server_address>:<port>/metascan_rest` where the `port`, if not defined otherwise on Metadefender Core server side, usually is 8008. Note also that if password is set for administrator user on Metadefender Core server, the password has to be provided in the **APIKEY** field. Once the credentials are provided, after successfully testing by pressing button **TEST** you can add the instance by pressing the button **ADD**.

Add v4 Instance

You should add a name for the instance and the REST address of the Metadefender Core server. URL needs to be fully qualified with scheme provided: `http(s)://<server_address>:<port>` where the `port`, if not defined otherwise on Metadefender Core server side, usually is 8008. The API-key or Metadefender Core administrator user and the corresponding password have to be provided in the **APIKEY** or **USERNAME** and **PASSWORD** field accordingly. Once the credentials are provided, after successfully testing by pressing button **TEST** you can add the instance by pressing the button **ADD**.

4.3. Regular maintenance

4.3.1. Checking for upgrades

Metadefender 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 link on the Inventory > Engines page.

4.3.2. Checking engines/databases health

Metadefender Central Management Linux 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 Mangement agents.

5. Release Notes

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 unsuccesful 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

6. Legal

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

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.