OPSWAT Metadefender™

© 2016 OPSWAT, Inc. All rights reserved. OPSWAT®, MetadefenderTM and the OPSWAT logo are trademarks of OPSWAT, Inc.All other trademarks, trade names, service marks, service names, and images mentioned and/or used herein belong to their respective owners.

Table of Contents

About this guide

The Update Downloader product is designed to download updates to an internet connected computer and save it to a specified folder to make it possible to upload to a non-internet connected Metascan v3, v4 or Central Management product.

Feedback

For comments and questions regarding this document, please contact OPSWAT on the Support tab at https://portal.opswat.com/.

1. Quick Start with Update Downloader

This guide describes the basic steps for installing and using Update Downloader:

1. Installation
2. License activation
3. Start using Update Downloader

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 Update Downloader on Ubuntu or Debian computers

1. Download ometadownloader 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 Update Downloader 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>:8028`
6. Enter default login credentials, username: **admin**, password: **admin**

Installing Update Downloader on Red Hat Enterprise Linux or CentOS computers

1. Download ometadownloader 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 Update Downloader package you downloaded from our portal
4. Open a web browser and point to `http://<server name or IP>:8028`
5. Enter default login credentials, username: **admin**, password: **admin**

Installing Update Downloader on Windows

1. Download ometadownloader Windows installer from the OPSWAT Portal
2. Upload the installation package to your test computers
3. Install the product with executing the installer
4. Open a web browser and point to `http://<server name or IP>:8028`
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 Update Downloader

1.2. License activation

In order to use the product you need an activation key. Offline activation is not available since Update Downloader can't operate without Internet connection.

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.

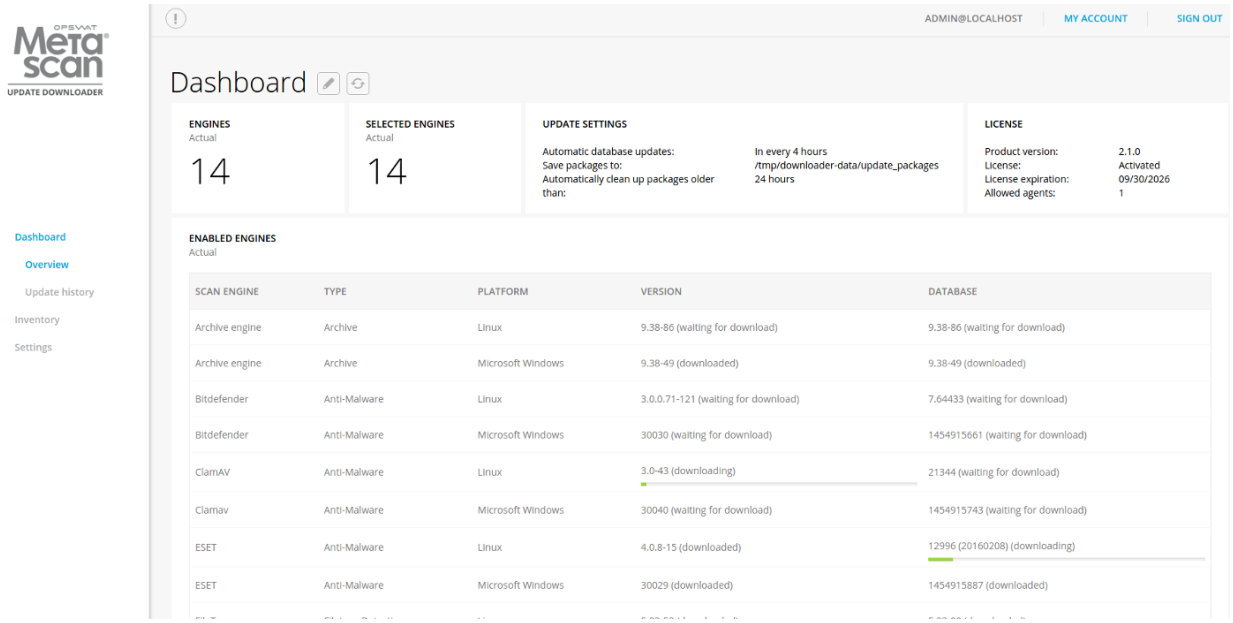
1. Press the *ACTIVATE* button to bring up the Activation menu
2. Type in your activation key
3. Press the *SEND* button

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 Update Downloader

After installation and activation updates will download automatically.



Downloading updates after activation

Please find details under Operating Update Downloader.

2. Installing or Upgrading Update Downloader

This part of the guide describes in detail the installation and upgrade process of Update Downloader

2.1. Before Installation

Before installing Update Downloader make sure the target computer meets the hardware and software requirements.

2.1.1. System Requirements

Please confirm that your system meets the minimum requirements listed below before installing Update Downloader.

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, 16.04
  - 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]

2.1.2. Browser Requirements for the Update Downloader Management Console

One of the following browsers is required to view the Update Downloader 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 Update Downloader

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>:8028`
4. Login with the default credentials, username: **admin**, password: **admin**
5. You must Activate this deployment to use its features

Installation

Installing Update Downloader using the Command Line

Installation notes

- If the Update Downloader 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.

Installing Update Downloader using the Command Line

Preliminary notes

- If the Update Downloader 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.

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	8028	REST interface binding port

For details on using msiexec please consult Windows installer documentation.

2.3. Upgrading Update Downloader

To upgrade from a former version of Update Downloader a simple installation of the latest version is enough.

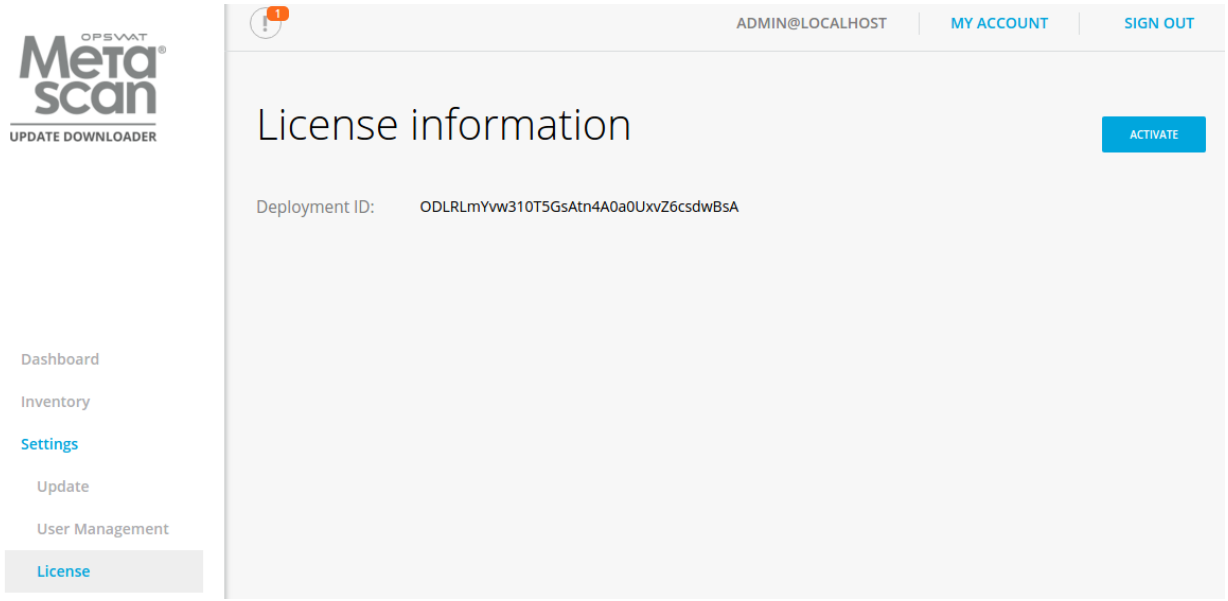
All existing Update Downloader configuration and data will be kept during the upgrade.

2.4. Update Downloader Licensing

In order to use Update Downloader you need to activate the product. If you are a Metascan v4 or Central Management customer please use your existing activation key you got for Metascan or Central Management. If you are a Metascan v3 customer please contact OPSWAT support for your activation key.

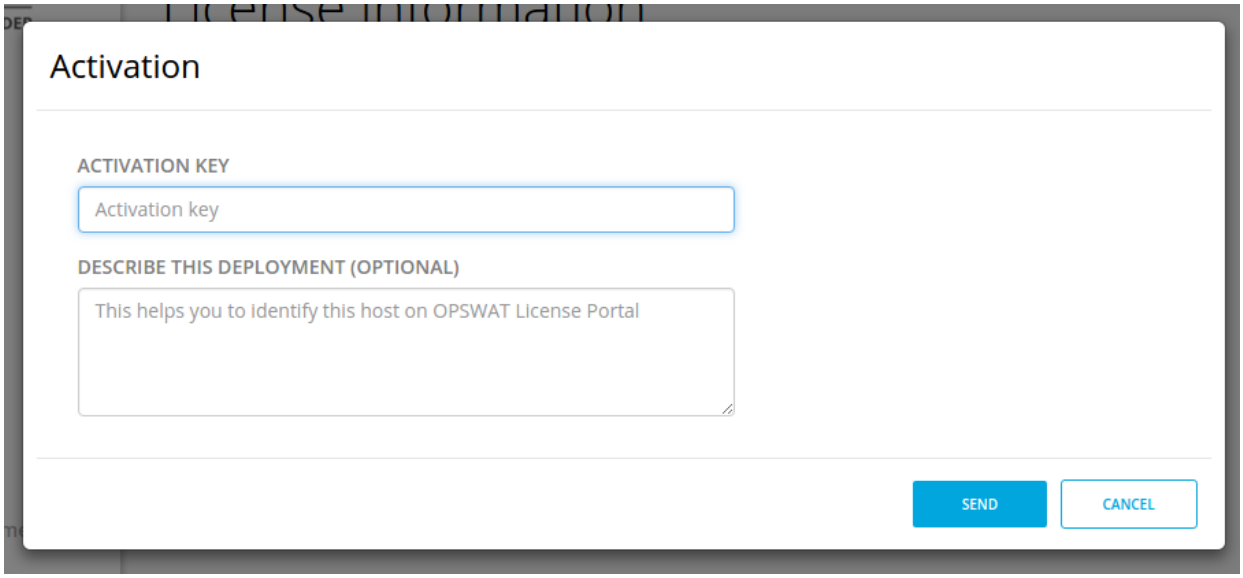
Activating Update Downloader Licenses

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



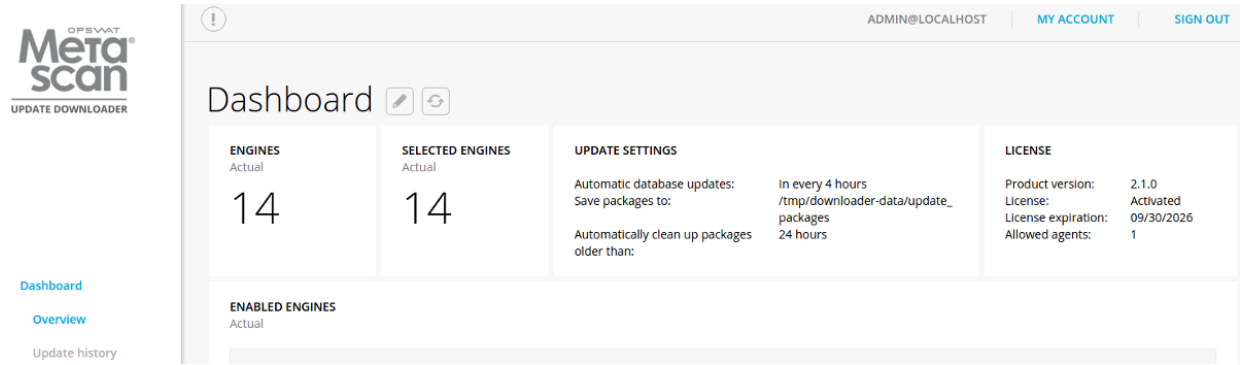
Settings/License/ACTIVATE page

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.

Checking Your Update Downloader 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 agents: maximum number of agents that can connect simultaneously

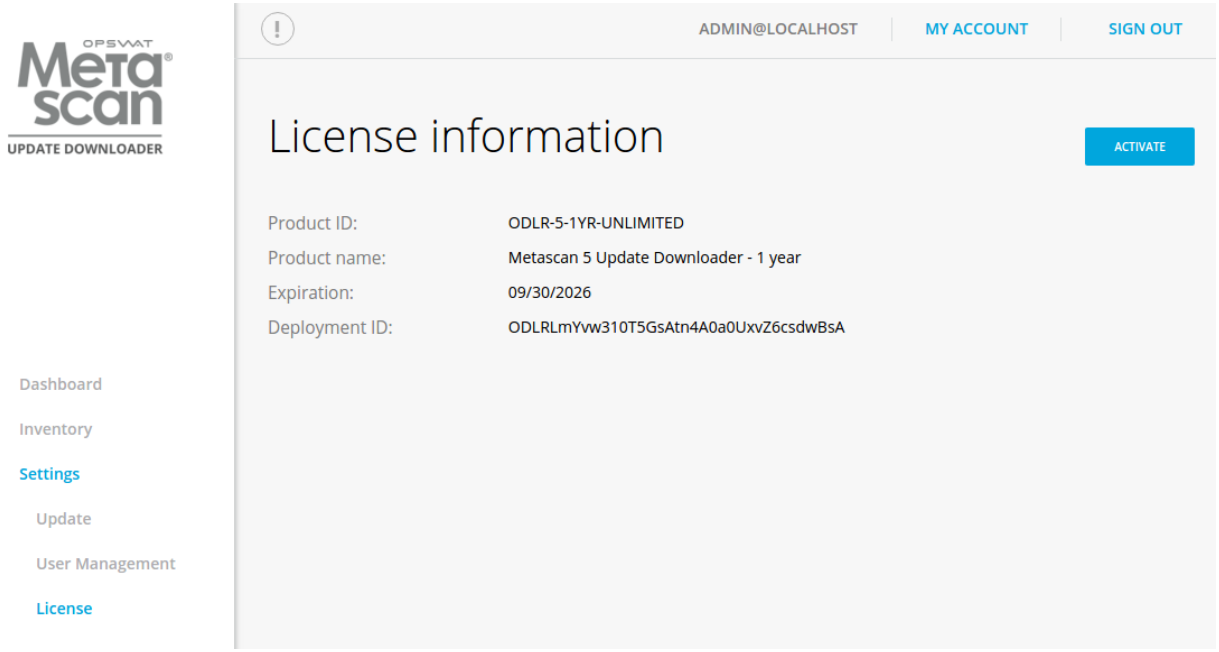


Dashboard/Overview page

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
- Deployment ID: identification of this installation



Settings/License page

3. Configuring Update Downloader

3.1. Update Downloader configuration

The Update Downloader 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.

Management Console

The management console is available at: `http://<Metadefender Update Downloader Server>:8028/`
where <Metadefender Update Downloader Server> is the name or IP address of the system where Update Downloader is installed.

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

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

Login screen

Typical issues related to the Web Management Console:

- Inaccessible Management Console

Update Downloader server configuration file

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

After modifying the server configuration file you must restart the Metascan service in order for the changes to take effect. You should use the distribution-standard way to restart the ometadownloader 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	8028	required	Designated port number for the web and REST interface

[logger] section

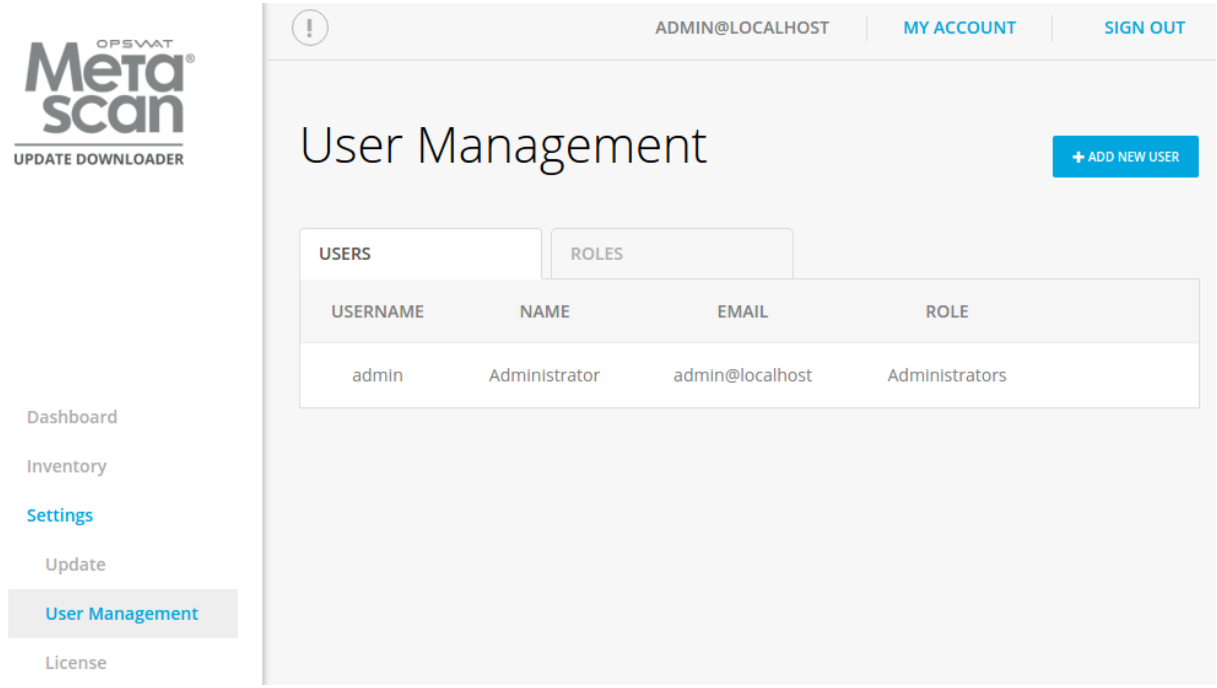
key	default value	required	description
logfile	/var/log /ometadownloader /ometadownloader.log	optional	Full path of a logfile to write log messages to
loglevel	info	optional	Level of logging. Supported values are: debug, info, warning, error
syslog		optional	Switch on logging to a local ('local') or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

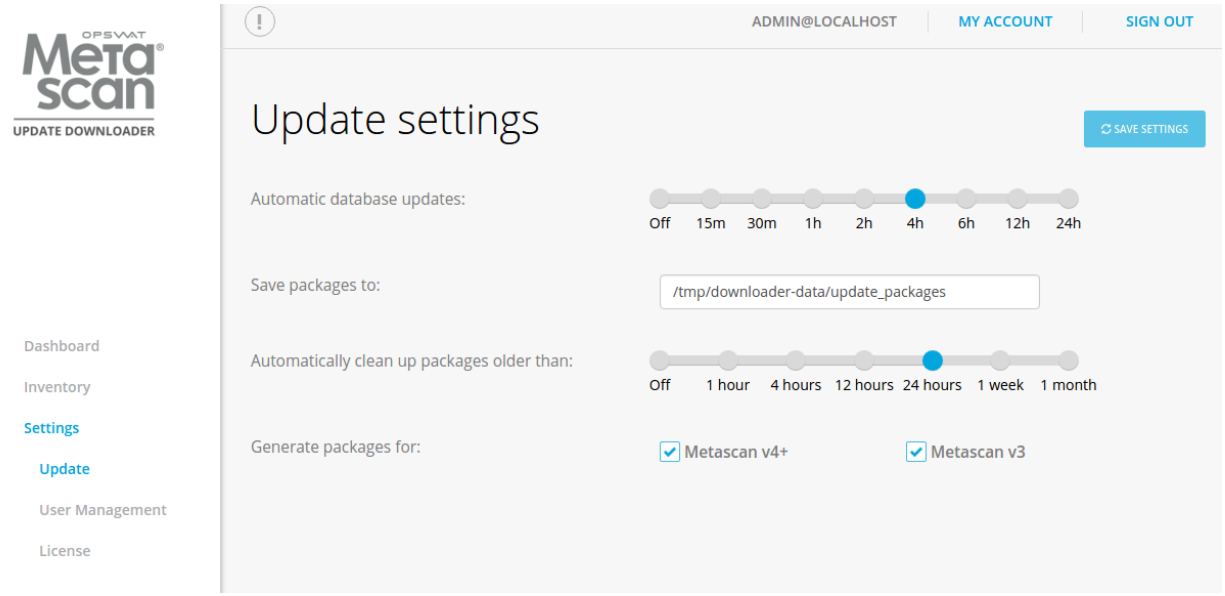
- existing roles can be viewed

Each role has a set of rights. Each of these rights represent access to a specific part of Metascan.
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

Automatic update

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



Update settings

- **Automatic database updates**: Update Downloader will check for new updates according to this schedule.
- **Save packages to**: You can find exported update packages in this directory. For Metascan v4.x/Central Management you can find updates in the root of this directory. For Metascan v3.x updates are generated into a subdirectory called MetascanV3
- **Automatically clean up packages older than**: Product will clean up target directory regularly and delete packages older than the specified age.
- **Generate packages for**: Metascan v3 and v4 use different format of update packages. To save your system resources you can control what packages need to be generated. Central Management uses Metascan v4+ packages even the managed products under Central Management are v3.
- **Updates are not applied during**: configure when NOT to export packages.

3.4. Logging

Metadefender Update Downloader 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

Configuration

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

- Update Downloader server configuration file

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

Configuration file is located:

- /etc/logrotate.d/ometadownloader

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.

Debug logging

To provide debug logs for the OPSWAT support team, the level of the logfile for the given service (ometadownloader) 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 How to create support package?

For information on how to interpret the log files consult: How to read the Update Downloader log?

3.5. Configuring SSL

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

1. Create file `ssl.conf` in the directory `/etc/ometadownloader/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/ometadownloader/nginx.d/your.crt;
ssl_certificate_key /etc/ometadownloader/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.

Note: When choosing location for cert and key files, make sure they are readable by the service user as well as the directory is executable by it.

For more SSL-options please consult Nginx documentation.

3.6. Configuring proxy settings

How can I set proxy server for the product

Linux

Set variables `https_proxy` in file `/etc/default/ometadownloader`.

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.

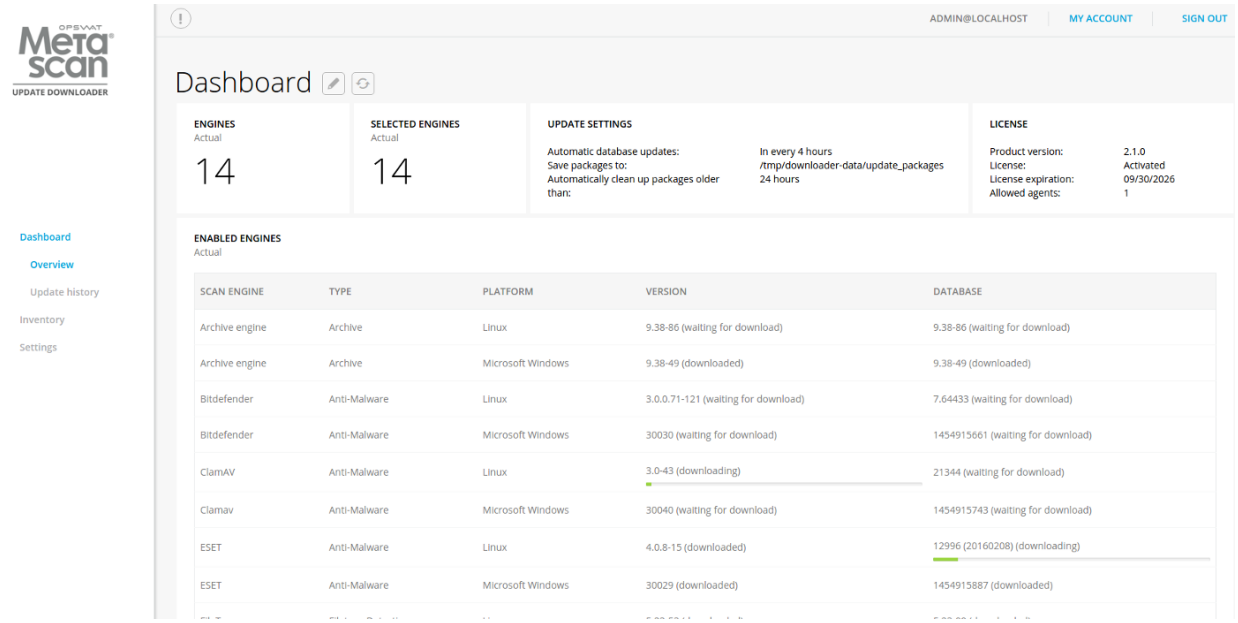
> You might need to configure Windows proxy to bypass local addresses if you can't access Web Management Console from the host itself. Consult netsh documentation for additional configuration options.

4. Operating Update Downloader

4.1. Dashboard

Metadefender Update Downloader provides a Web-based user interface (default port is 8028) that gives a general overview of Update Downloader status and allows you to configure its options.

Note that the default refresh rate of displayed information is 1 minute.



Dashboard overview

Overview page

The Overview page shows information on

- Number of engines
- Number of selected engines
- Update settings

- Licence information
- Active engines with platform, version and database information

Both the default refresh rate (1 minute) and the span of time displayed (24 hours) can be changed.

Update history

The Update history shows information on every update package 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.

4.2. Inventory management

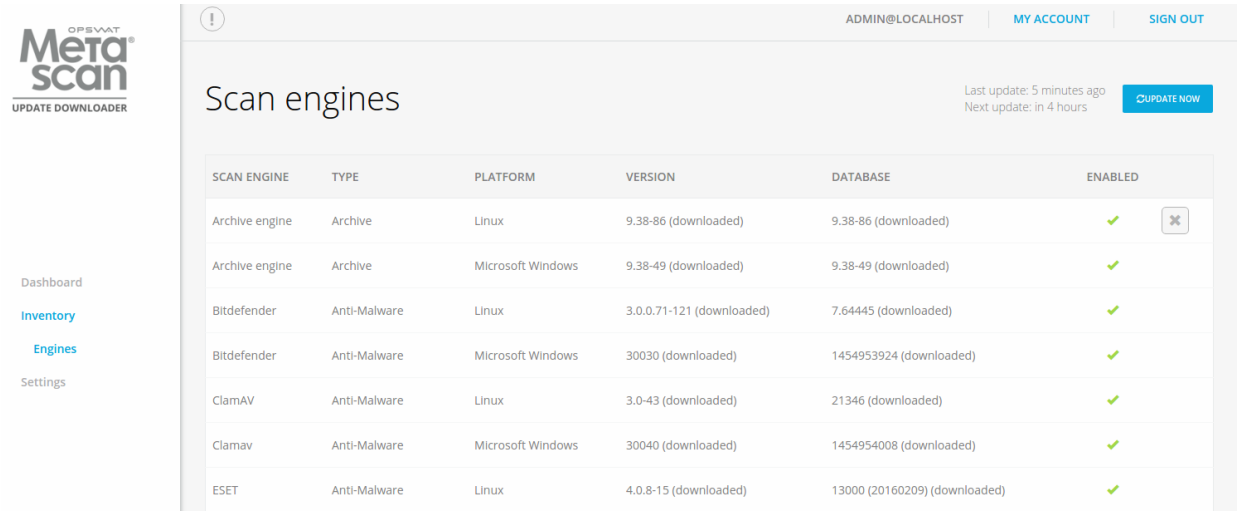
Metadefender Update Downloader displays detailed information on scan engines including anti-malware engines, archive engines, etc.

Engines

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
- Engine status (Enabled / Disabled)



Engines

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

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. Status of the engine is displayed by green mark sign, red cross sign or grey cross sign meaning the engine is active, not active or disabled accordingly.

4.3. Regular Maintenance

Checking engines/databases health

Metadefender Update Downloader 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.

Checking for upgrades

Metadefender Update Downloader 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.

5. Troubleshooting Update Downloader

In this section you can find solutions for generic issues with Update Downloader

Installation issues

- Inaccessible Management Console

Where are the Update Downloader logs located?

Metadefender Update Downloader Linux generates log files under **/var/log/ometadownloader**.

The server and agent logs are collected separately and are
plain text files. For more information on how to read the logs, go to

- How to read the Update Downloader log?

How can I create a support package?

To ensure the best help from OPSWAT support, you can create a support package with a tool that comes with Update Downloader.

For more information on how to create a support package, go to

- How to create support package?

How to create support package

A 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/ometadownloader-collect-support-data.sh**.

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

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

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

Where the timestamp is the date when the package was generated.

Example:

```
ometadownloader-support-1439983514.tar.gz
```

The generated package will be placed in the same location as the script that was called.

Windows

To create a package you must start the script found under the installation directory of the product, default this is **C:\Program Files\Metadefender Update Downloader\ometadownloader-collect-support-data.bat**.

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

The package files is a zip archive with the following name:

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

Where the timestamp is the date when the package was generated.

Example:

```
ometadownloader-support-1439983514.zip
```

The generated package will be placed in the same location as the script that was called.

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** : config 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 Update Downloader log

The log files are plain text files that can be opened with any text editor.

Files

The Update Downloader generates a log file under **/var/log/ometadownloader** named ometadownloader.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   ] 2016.02.09 08:41:37.099: (common.update) Package
successfully downloaded, packageDir='/tmp/downloader-data/updates
/db/clamav_1_linux_2OMCap' [msgid: 671
```

Where 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:

- **DUMP** : The most verbose severity level, these entries are for debuggers only.
- **DEBUG** : Debuggers severity level, mostly used by support issues.
- **INFO** : Information from the software, such as scan results.
- **WARNING** : A problem occurred needs investigation and OPSWAT support must be contacted, however the product is supposed to be operational.
- **ERROR** : Software error happened, please contact support if the issue is persist. Software functionality may be downgraded in these cases.

Inaccessible Management Console

Problem: You cannot access the Web Management Console from your browser.

How to detect

After you enter the Update Downloader Web Management Console address you get an error message (connection refused) or your browser is waiting for reply.

Solution

1. Please make sure your computer can access the Update Downloader 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 Update Downloader server for the Web Management Console. Consult your Linux Distribution manual on how to configure a firewall in your distribution.

6. Release Notes

Version 2.2.0

New features:

- Full audit log about any configuration changes via Web user interface or REST API
- Able to disable exporting update in user configurable time periods
- Support to download OESIS updates
- Able to set up apikey for every user for easier REST API integration
- Improved hardware detection in license component
- Improved activation process feedback on web user interface

Issues fixed:

- 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
- Detailed logging in case of SSL connection issues

Version 2.1.2

- 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 2.1.1

- Rebranded to Metadefender Update Downloader
- Download stability fixes

Version 2.1.0

- Initial release

7. How to upload packages to offline products

Please read the appropriate documentation for your product to learn how to use the update packages downloaded by the Update Downloader.

- **Metascan v3.x**: https://onlinehelp.opswat.com/corev3/Applying_Offline_Updates.html
- **Metascan v4.x**: https://onlinehelp.opswat.com/corev4/Engines.html
- **Central Management**: http://software.opswat.com/metascan/Documentation/CentralMgmt/documentation/user_guide_operating_centralmgmt_inventory_management_engines.html

8. 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

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.