OPSWAT.

MetaDefender™ Update Downloader

MetaDefender Update Downloader

v3.5.0

Contents

Before Installation

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

> **Info**
> MetaDefender Update Downloader only supports for MetaDefender Core and MetaDefender Aether

System Requirements

> **Plan for legacy OS support**
> OPSWAT will discontinue support for the following OS in MetaDefender Update Downloader:
>
> - Windows 10 after **October 2025**.
> - Windows Server 2016 after **October 2025**.
>
> You can stay with these OS and would not see negative impacts during your operation and usage. However, we suggest you move on to newer OS for good measure.

Only 64-bit platforms are supported.

- Operating System:
  - Rocky Linux 9.4
  - Debian 12
  - Ubuntu 22.04
  - Windows 11
  - Windows Server 2019, 2022
- Hardware requirements
  - RAM: min. 2 GB
  - HDD: 2 GB + ~500MB * [number of managed scan engines]
    - Note: some engines might have a bigger file size than others, for example: SBOM, Adaptive Sandbox engine will take more than 1GB.
- Third party dependency:
  - Microsoft Visual C++ Redistributable for Visual Studio 2015-2022; x64 version.

- Internet connection required to be able to connect to OPSWAT update servers.

Allowlisting URLs

If you have installed or plan to use the MetaDefender Update Downloader in a restricted environment, you must allow access to the following hosts for engine and database downloads:

- https://update.dl.opswat.com

Note: *IP address-based allowlisting on your firewall may fail over time because OPSWAT uses CDN (AWS Cloudfront) to accelerate global update delivery, and the IP address of edge servers may change periodically.*

Depending on your location, connections to OPSWAT's cloud-based servers may be forwarded to specific AWS Cloudfront edge locations, each assigned its own unique IP address ranges. You may also need to allow the corresponding AWS Cloudfront IP address ranges by referring to https://ip-ranges.amazonaws.com/ip-ranges.json

Warning

Although OPSWAT update servers host updates for all supported engines, some custom engines may attempt to connect to their own cloud for updates. However, this can be blocked at the firewall, ensuring that updates are retrieved exclusively from OPSWAT.

Browser Requirements for the Update Downloader Management Console

One of the following browsers is suggested to view the Update Downloader Management Console:

- Microsoft Edge
- Chrome
- Firefox
- Safari

Chrome, Firefox, Safari and Edge browsers are tested with the latest available version at the time of release.

Installing Update Downloader

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. Visit the My OPSWAT. Search for MetaDefender Core, navigate to section "Modules & Utilities", then you can find the product at "Update Downloader for Offline Environment".
2. Make sure that you download the applicable package for Debian 12 / Ubuntu 22.04.

3. Upload the installation package to your test computers.
4. Install the product with sudo dpkg -i <filename>, where filename is the Update Downloader package you downloaded from our portal.
5. If dpkg shows error messages about missing dependencies you should execute sudo apt-get install -f
6. Open a web browser and point to http://<server name or IP>:8028
7. Follow welcome wizard to create local admin user account and start working on Update Downloader

Installing Update Downloader on Red Hat Enterprise or Rocky Linux computers

1. Visit the My OPSWAT. Search for MetaDefender Core, navigate to section "Modules & Utilities", then you can find the product at "Update Downloader for Offline Environment".
2. Make sure that you download the applicable package for Red Hat Enterprise Linux or Rocky Linux.
3. Upload the installation package to your test computers
4. Install the product with sudo yum install <filename>, where filename is the Update Downloader package you downloaded from our portal
5. Open a web browser and point to http://<server name or IP>:8028
6. Follow welcome wizard to create local admin user account and start working on Update Downloader

Installing Update Downloader on Windows

1. Visit the My OPSWAT. Search for MetaDefender Core, navigate to section "Modules & Utilities", then you can find the product at "Update Downloader for Offline Environment".
2. Make sure that you download the applicable package for Windows Server 2022.
3. Upload the installation package to your test computers
4. Install the product with executing the installer
5. Open a web browser and point to http://<server name or IP>:8028
6. Follow welcome wizard to create local admin user account and start working on Update Downloader

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

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)

install cmd · bash

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

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

install cmd · bash

```
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

install cmd · bash

```
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
INSTALLFOLDER	C:\Program Files\OPSWAT\Metadefender Update Downloader\	Custom installation folder path

For details on using msiexec please consult Windows installer documentation.

Automation deployment via ignition file

From version 3.3.0, users can setup automation deployment via ignition file

Overview

The ignition file is a configuration file that enables automated deployment and configuration of the Update Downloader system. It allows you to pre-configure settings, create admin users, add products, and set up post-

installation actions without manual intervention through the web interface.

Location

- Windows: `C:\opswat\ometadownloader.conf`
- Linux: `/etc/opswat/ometadownloader.conf`

File Format

The ignition file uses INI format with sections and key-value pairs. The file should be named appropriately and placed in the correct location where the system can detect it during startup.

Complete Example

ometadownloader.conf · bash

```
eula=true

[user]
name=admin
password=admin
email=admin@local
apikey=user_apikey_36_characters

[update_settings]
interval=15
packagelocation=C:/Program Files/OPSWAT/Metadefender Update Downloader/data/update_packages
cleanup=4
exclude=Monday-Friday 08:15-16:15
exclude_1=Saturday 13:00-23:59
exclude_2=Sunday 00:00-11:00

[post_action]
name=ps_python
command=D:/post action/post.py

[post_action_1]
name=ps_binary
command=D:/post action/post.exe
product_name=MetaDefender Core A
product_name_1=MetaDefender Core B


[product]
name=MetaDefender Core A
license=E:/opswat/Core_licenses/md_core_a_license_file.yml

[product_1]
name=MetaDefender Core B
license=E:/opswat/Core_licenses/md_core_b_license_file.yml
```

Details Configuration

EULA Acceptance - Required

The EULA (End User License Agreement) must be accepted for the ignition file to be processed:

Code · bash

```
eula=true
```

Note: This is a required field. The ignition file will not be processed if this is not set to `true`.

User Configuration - Optional

You can automatically create an admin user during deployment:

Code · bash

```
[user]
name=admin
password=admin
email=admin@local
apikey=user_apikey_36_characters
```

User Fields:

- `name`: Username for the admin account
- `password`: Password for the admin account
- `email`: Email address for the admin account
- `apikey`: (Optional) API key for the user

Note: If you provide user information, all fields except `apikey` are required.

Update Settings Configuration - Optional

Configure automatic update settings for the Update Downloader:

Code · bash

```
[update_settings]
interval=15
packagelocation=C:/Program Files/OPSWAT/Metadefender Update Downloader/data/update_packages
cleanup=4
exclude=Monday-Friday 08:15-16:15
exclude_1=Saturday 13:00-23:59
```

```
exclude_2=Sunday 00:00-11:00
```

Update Settings Fields - Optional

interval

Auto-update interval in minutes. Valid values:

- `0` - Disabled
- `15` - 15 minutes
- `30` - 30 minutes
- `60` - 1 hour
- `120` - 2 hours
- `240` - 4 hours (default)
- `360` - 6 hours
- `720` - 12 hours
- `1440` - 24 hours

cleanup

Cleanup interval in hours. Valid values:

- `0` - Disabled
- `1` - 1 hour
- `4` - 4 hours
- `12` - 12 hours
- `24` - 24 hours (default)
- `168` - 1 week
- `672` - 4 weeks

packagelocation

Directory path where update packages will be stored. The system will create this directory if it doesn't exist and verify write permissions.

exclude

Time periods when updates should be disabled. Format options:

- Single day: `Monday 08:00-17:00`
- Day range: `Monday-Friday 08:00-17:00`

Valid day ranges:

- `Monday-Friday`
- `Friday-Sunday`
- `Sunday-Thursday`

You can specify multiple exclude periods using numbered suffixes (`exclude_1`, `exclude_2`, etc.). Maximum 100 excludes

Post-Action Configuration - Optional

Configure commands to run after product installation:

Users can add maximum 100 items for Post-Action, the first one should be `post_action`

If user want to add more Post-Action, using this pattern: "post_action_1" , "post_action _2", etc

Code · bash

```
[post_action]
name=ps_python
command=D:/post action/post.py

[post_action_1]
name=ps_binary
command=D:/post action/post.exe
product_name=MetaDefender Core A
product_name_1=MetaDefender Core B
```

Post-Action Fields:

- `name`: Action name (maximum 16 characters, must be unique)
- `command`: Command to execute
- `product_name`: Product name that triggers this action (can have multiple using numbered suffixes)
- We can add multiple products to a Post-Action: product_name_1, product_name_2, etc. Maximum 100 products

Note: Actions are triggered when the associated products are installed.

Product Configuration - Optional

Add products with their licenses during deployment:

Code · bash

```
[product]
name=MetaDefender Core A
license=E:/opswat/Core_licenses/md_core_a_license_file.yml
```

```
[product_1]
name=MetaDefender Core B
license=E:/opswat/Core_licenses/md_core_b_license_file.yml
```

Product Fields:

- `name`: Product name - **must be unique** between product fields
- `license`: The absolute path to the license file

Note: Both fields are required for each product section.

Limitations

- Maximum 100 items for repeated sections (product, product_name, post-action, exclude)
- Post-action names limited to 16 characters
- Package location must be writable by the system
- License files must be accessible during processing
- Time exclusions must follow exact format specifications

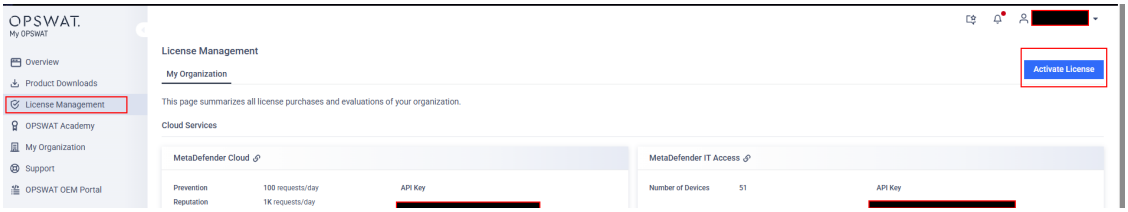
License activation

> **Note**
>
> Since MetaDefender Update Downloader 2.4.0, the licensing mechanism has been changed.
>
> - No longer need to activate license of Update Downloader itself to make it operational.
> - Instead required to add license file (.yml) of offline MetaDefender products
>
> Check 1.2. License activation to learn more how to add

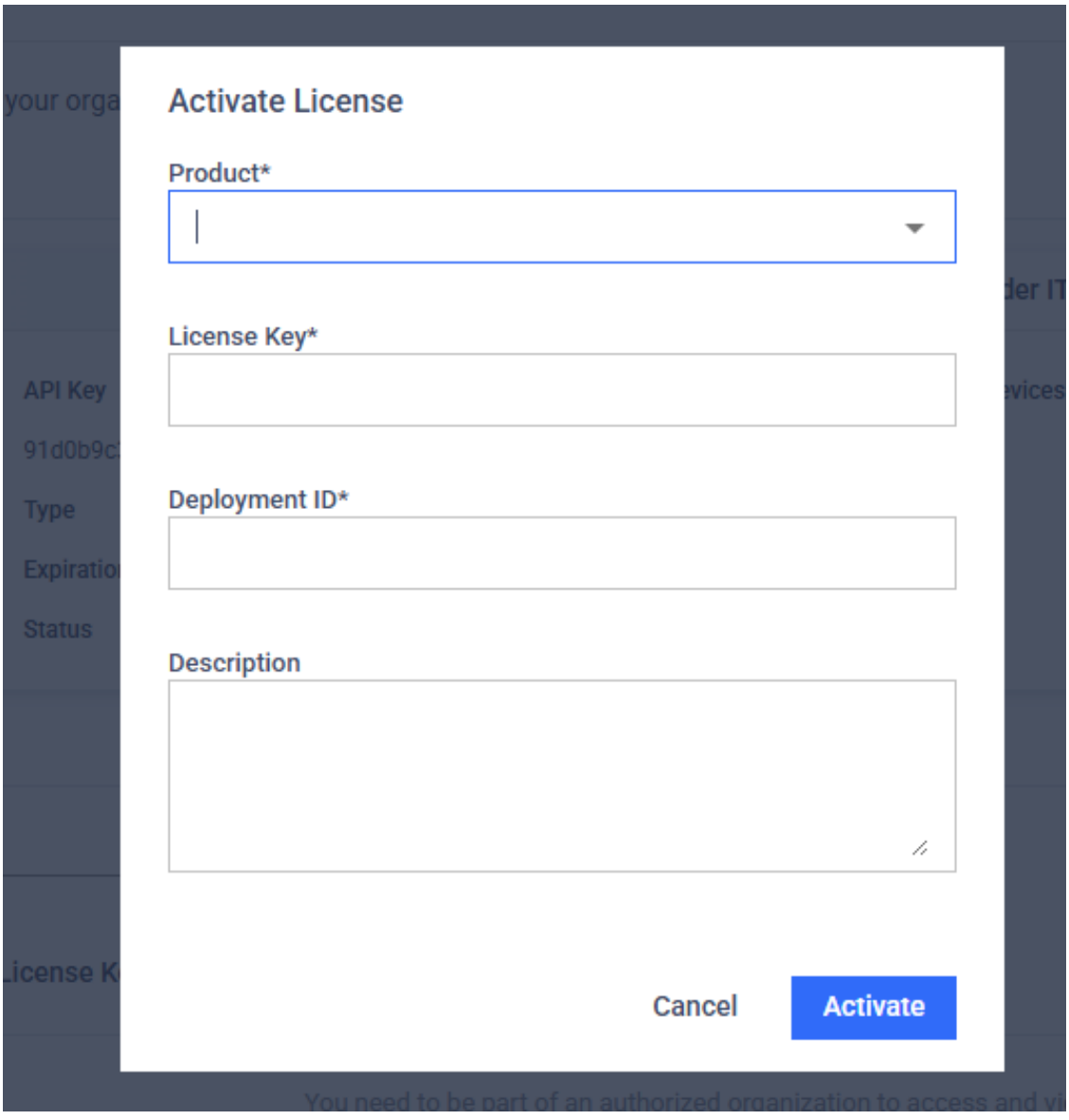
Clean installation with Update Downloader 2.4.x

Generate a license file (.yml)

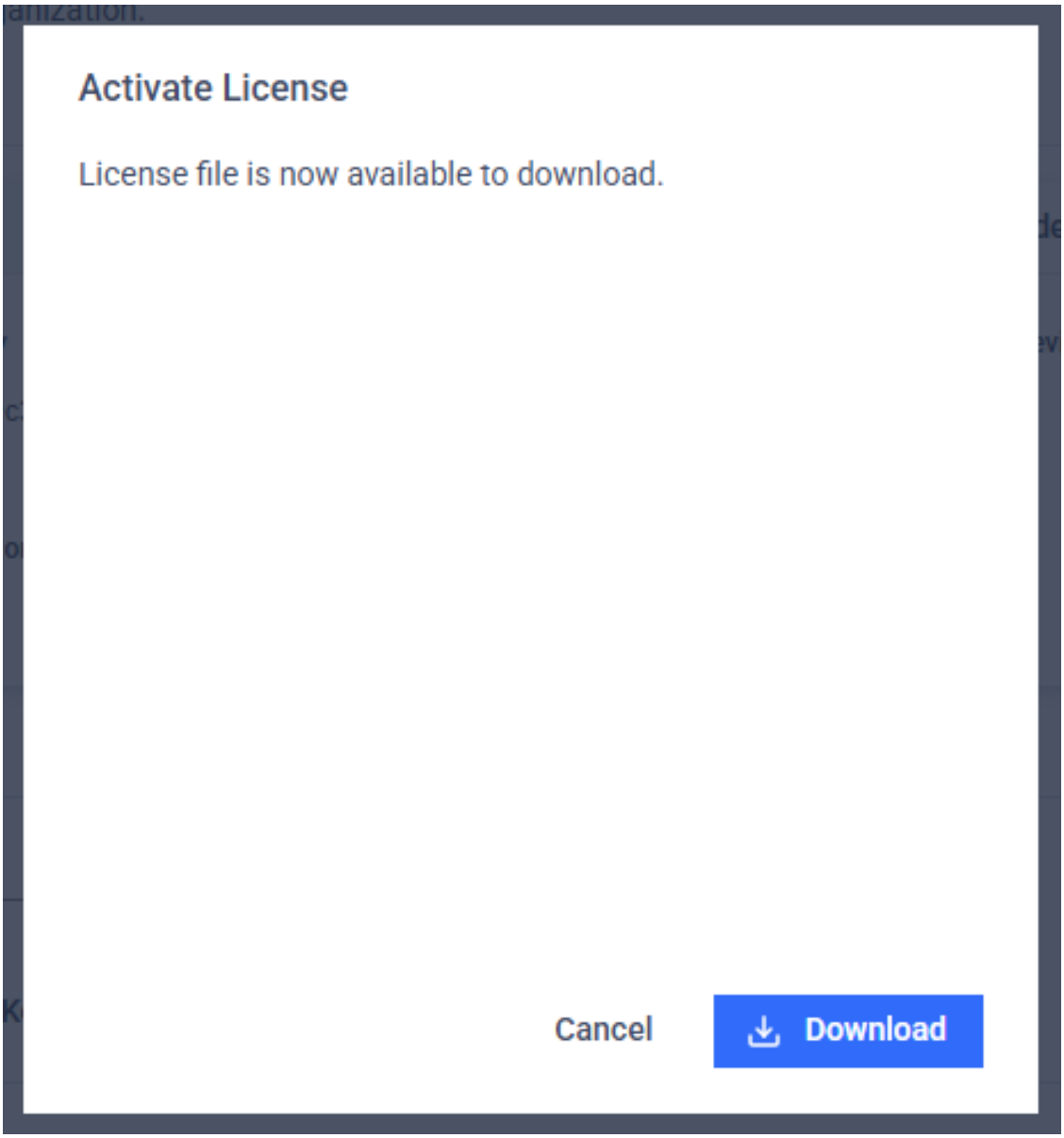
- Navigate to My OPSWAT Central Management - https://my.opswat.com (login required)
- Navigate to “License Management” → Click “Activate License”



- Product: MetaDefender Core
- Type or paste your associated MetaDefender product's license activation key.
  - Double check to ensure no redudant space unintentionally attached into the head or tail of license string
- Type or paste your associated MetaDefender product's deployment ID.
  - Double check to ensure no redudant space unintentionally attached into the head or tail of license string
- (Optional) Write a description to keep track of this particular activation on our system for "Optional Description"
- Hit **Activate** button to generate the license file (<deployment ID>.yml)

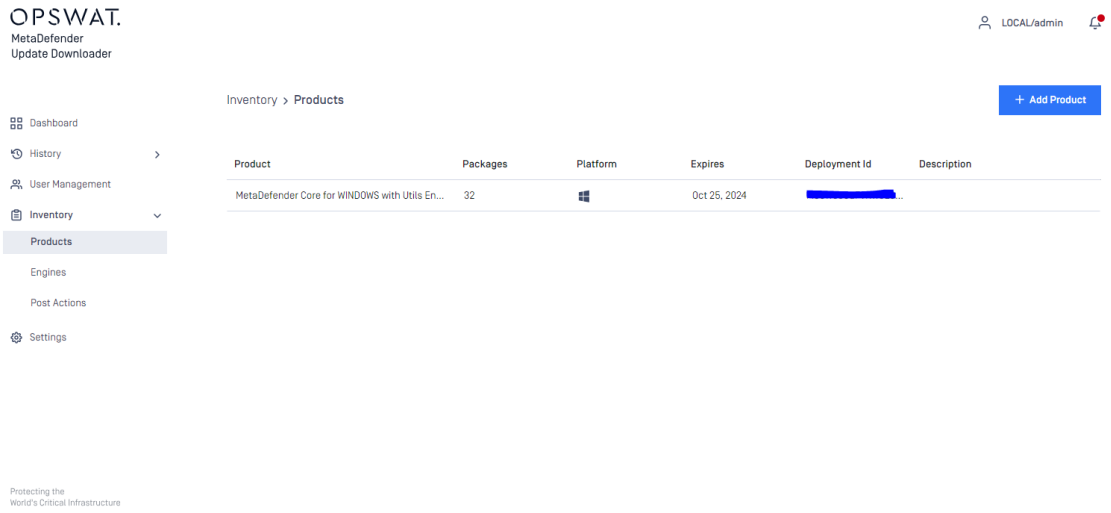


- After that, click `Download` to download the yml file

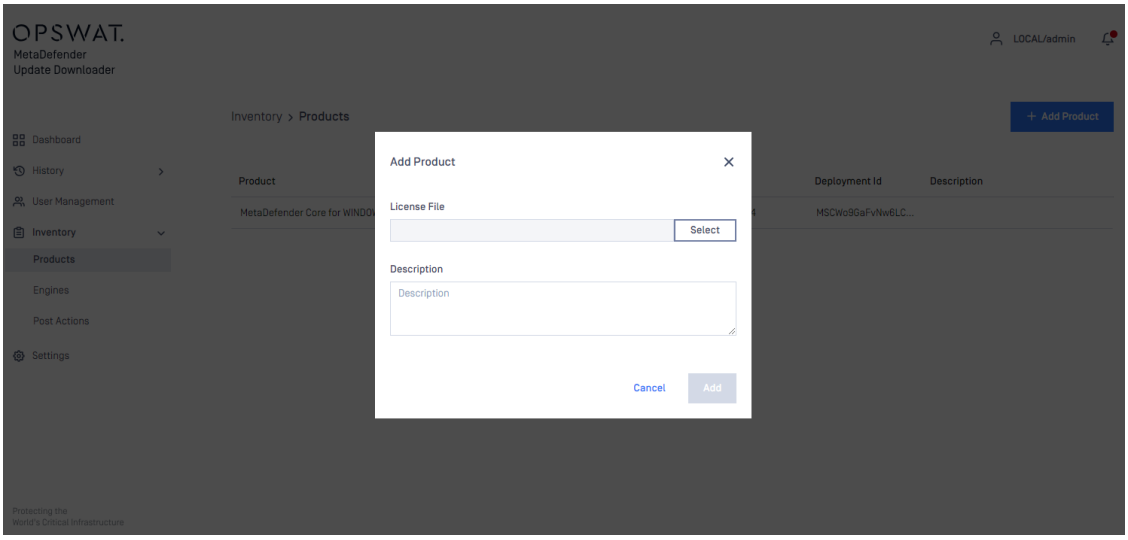


Add a new product on Update Downloader

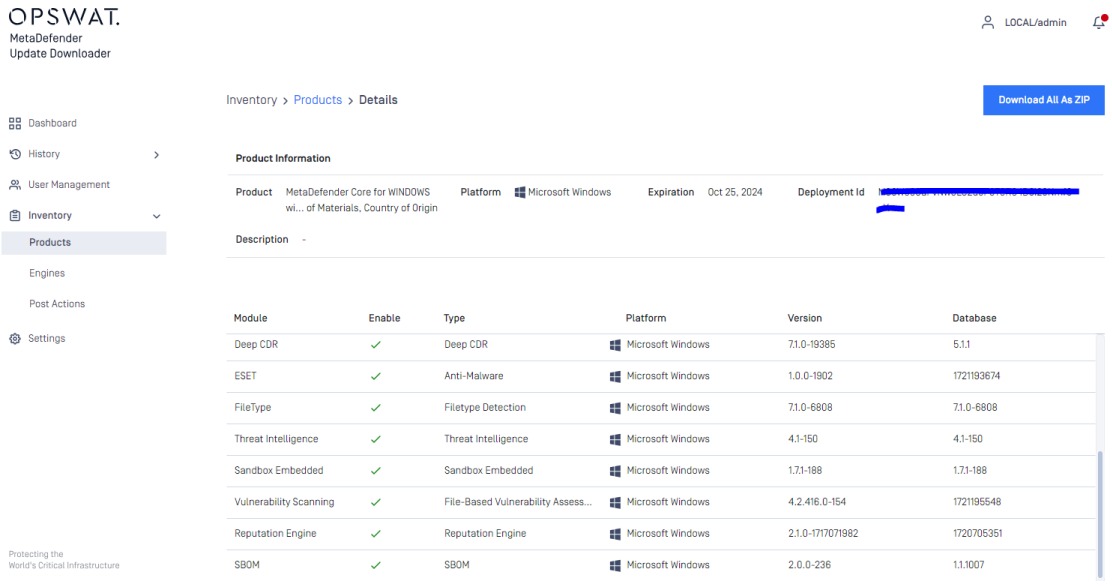
- Ensure you already installed Update Downloader, and setup a local admin user through its wizard
- Navigate to Inventory Products page under left menu - http://localhost:8028/#/user/inventory/products
- Hit **ADD NEW PRODUCT** button to add new product on Update Downloader



- Select the license file (.yml) which was obtained in steps above



- Hit **ADD** button to start downloading offline update packages for associated licensed product

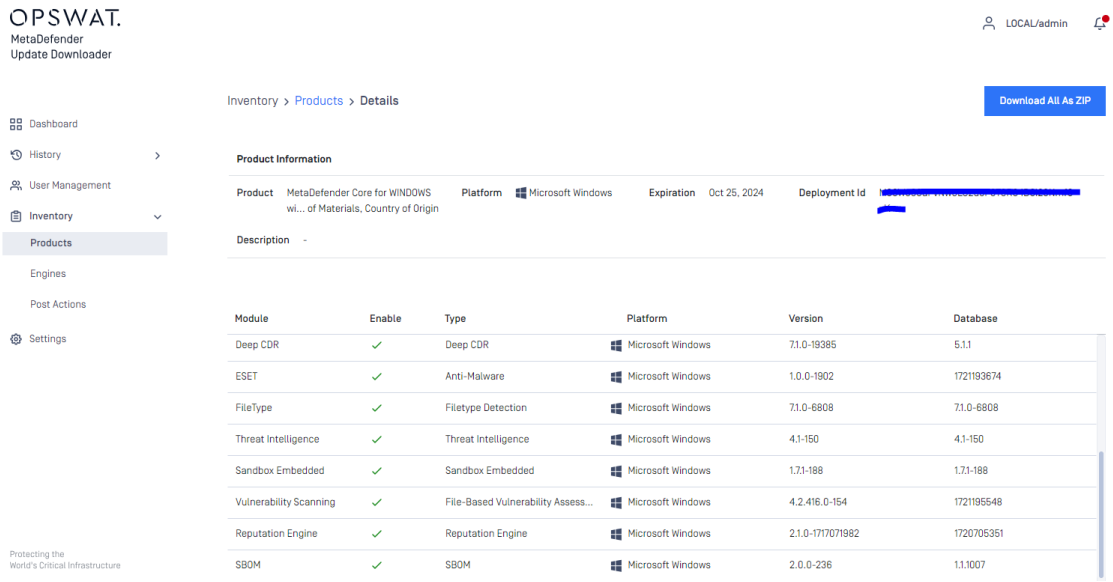


Upgrading Update Downloader to version 2.4.x or newer

Update Downloader will auto create an entry the product will support to automatically migrate the configurations, and keep all licensed engine packages remained. See screenshot below as an example of upgrading from Update Downloader older version to version 2.4.0 and above.

Start using Update Downloader

After installation and having product imported, updates will download automatically under that product section.



Please find details under Operating Update Downloader.

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.

> **Info**
>
> For customers who already activated and used Update Downloader older version, and now upgrading to version 2.4.0, Update Downloader will auto create an entry the product will support to automatically migrate the configurations, and keep all licensed engine packages remained. See screenshot below as an example of upgrading from Update Downloader older version to version 2.4.0 and above.

Update Downloader configuration

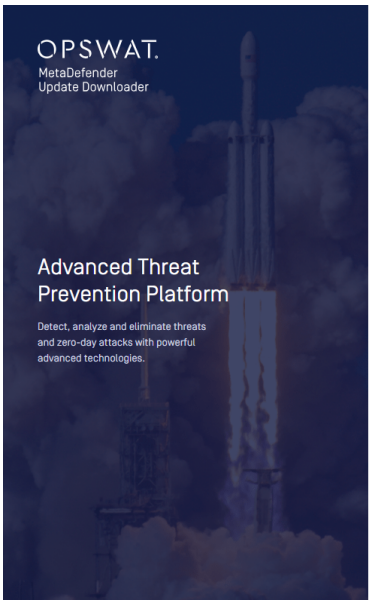
The Update Downloader configuration is separated into two parts. The basic server configurations are stored in the configuration files. Other configuration values can be set via the Web Management Console.

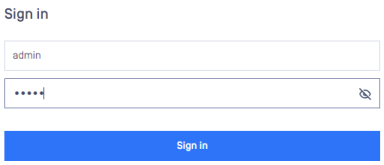
Management Console

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

Linux

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

parameter	default value	required	description
			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
override		optional	override specific log ids to display them on another level e.g.: "1723:error,663:info"
cef	false	optional	If true, the log format is Common Event Format.

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.

Windows

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

After modifying the server configuration file you must restart the OPSWAT Metadefender Update Downloader 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\Metadownloader\global

parameter	default value	type	required	description
restaddress	0.0.0.0	string value	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	string value	required	Designated port number for the web and REST interface

HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadownloader\logger

key	default value	type	required	description
logfile		string value	optional	Location of a logfile to write log messages to
loglevel		string value	optional	Level of logging. Supported values are: debug, info, warning, error
wineventlog_level	info	string value	optional	Level of logging. Supported values

key	default value	type	required	description
				are: debug, info, warning, error
syslog		string value	optional	Value can only by in form of `udp://<hostname>:<port>`
syslog_level		string value	optional	Level of logging. Supported values are: debug, info, warning, error
override		string value	optional	override specific log ids to display them on another level e.g.: "1723:error,663:info"
cef	false	string value	optional	If true, the log format is Common Event Format.

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.

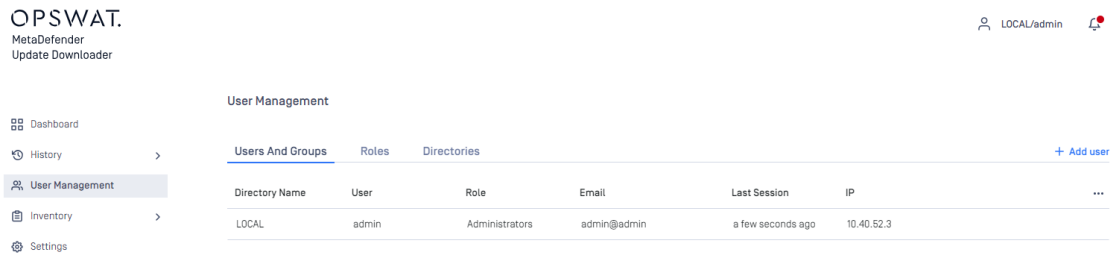
For override a list of log message ids needed with optionally a level. If there is no level set for an id, it will be displayed on every occasion. e.g.: "1723,663:info" means id 1723 dump message will be displayed every time and id 663 warning message is reduced to info level.

User management

To manage the users of the Metadefender Update Downloader go to the **Settings > User Management** menu in the Web Management Console.

Users and groups

The Users and groups tab lists the existing users and **Active Directory groups** in the system.



Default user

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

Username	Password	Name	Email	Roles	User directory
admin	admin	Administrator	admin@localhost	Administrators	LOCAL

Functions

Besides listing existing users and AD groups the **Users** tab provides the following functions:

- Add new user or AD group
- Modify (and view) existing user's or AD group's properties
- Delete existing user 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 or an Active Directory group for details about role assignment.

> **Warning**
>
> 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 Configuring TLS.

The APIKEY value provides access to the Metadefender Update Downloader REST API for this user with no authentication. If no such functionality is needed for the user then this field can be left blank.

Add new users from an Active Directory type user directory

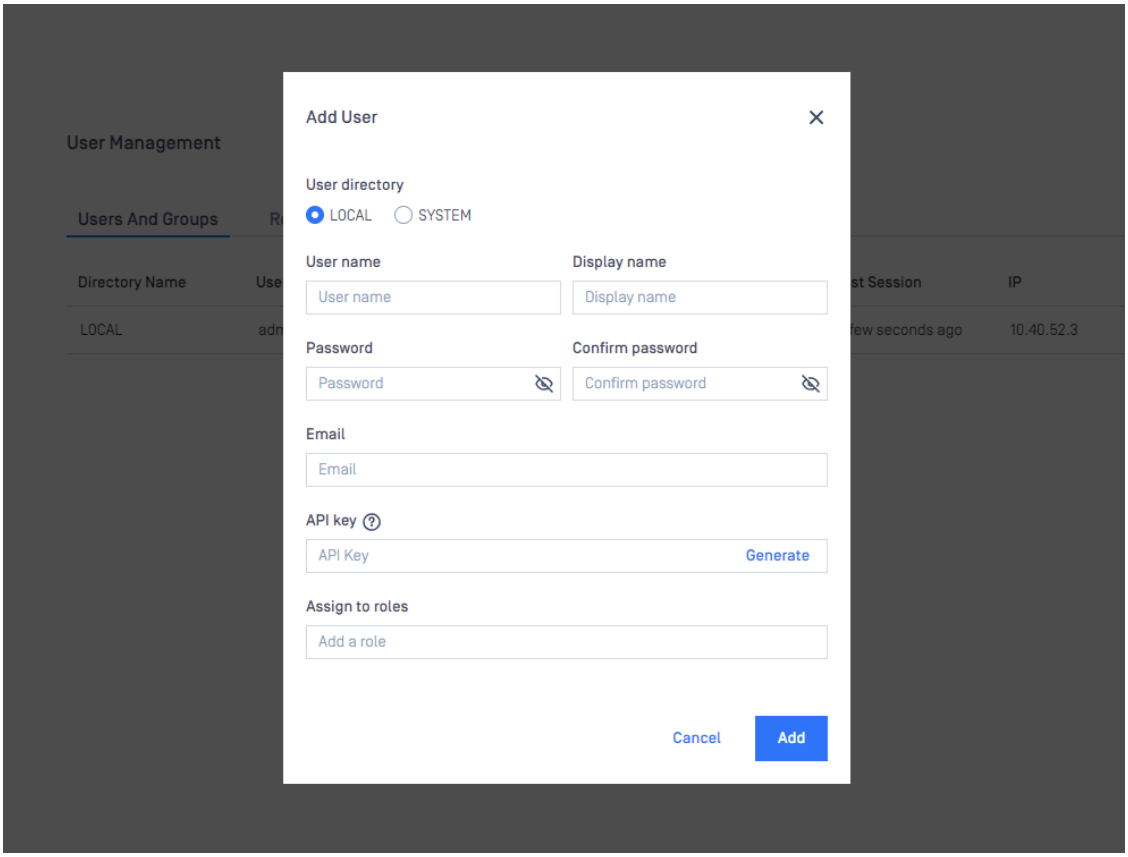
To add a new user from an Active Directory type user directory click the ADD NEW USER button and select an Active Directory type user directory in the USER DIRECTORY drop down list. Select USER as the ACCOUNT TYPE.

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

Note

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 or an Active Directory group for details about role assignment.



Add new group from an Active Directory type user directory

Info

The purpose of adding an Active Directory group to the Metadefender Update Downloader is to assign Update Downloader role(s) to all the users in that Active Directory group.

The users of the Active Directory group can authenticate with their Active Directory credentials in Metadefender Update Downloader Web Management Console and will be assigned with the roles of the group.

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

> **Note**
>
> Select GROUP as the ACCOUNT TYPE.

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

> **Note**
>
> 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 all users of this group. See section **Assign roles to a user or an Active Directory group** for details about role assignment.

Assign roles to a user or an Active Directory group

Role(s) must be assigned to users and Active Directory groups in order they can use the Web Management Console.

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 or Active Directory group
2. Optionally multiple different roles can be assigned
    1. In this case the highest available permission applies to each function. Example:

Roles assigned	Effective permissions	
	Full permission	Read only permission
security_admin	Update history, Engines, Update settings	
security_auditor		All permission
security_admin AND security_auditor	Update history, Engines, Update settings	Config history, License, User management

Delete user

Note

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

Roles

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:

Rolename	Display name	Default member username	Permissions
admin	Administrators	admin	Full on all functions
security_admin	Security administrators		Full on Update history, Engines, Update settings functions
security_auditor	Security auditor		Read-only on all functions
help_desk	Help desk		Read-only on Update history and Engines functions

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 Metadefender Update Downloader Web Management Console.A right can be set to one of three different states:

- **None:** users of this role have no right to access the given function of Metadefender Update Downloader Web Management Console. The menu belonging to the function is not displayed for the users of this role.
- **Read-only:** users of this role have right 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.
- **Full:** users of this role have full access to the given function, including viewing any data belonging to it and modifying its configuration.

Functions

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

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

> **Note**
> The default role **Administrators** can not be deleted or modified.

Modify role

> **Warning**
> 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

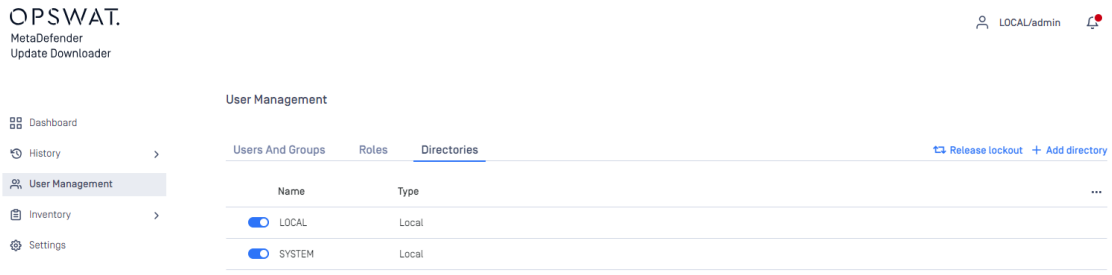
> **Note**
> A role can not be deleted as long as it is assigned to any user.
>
> As a consequence deleting a role can not affect active sessions of users.

User directories

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 directory

After installation a default user directory is created with the following parameters:

User directory type	Name	Number of failed logins before lockout	Lockout time [minutes]
Local	LOCAL	3	5
Local	SYSTEM	0	0

Two types of user directories exist in Metadefender Update Downloader:

1. Local
2. Active Directory

Local type user directories

Local type user directories allow creating users that locally exist on the Metadefender Update Downloader.

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

Active Directory type user directories

Active Directory type user directories allow users defined in an Active Directory to access Metadefender Update

Downloader.

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

Functions

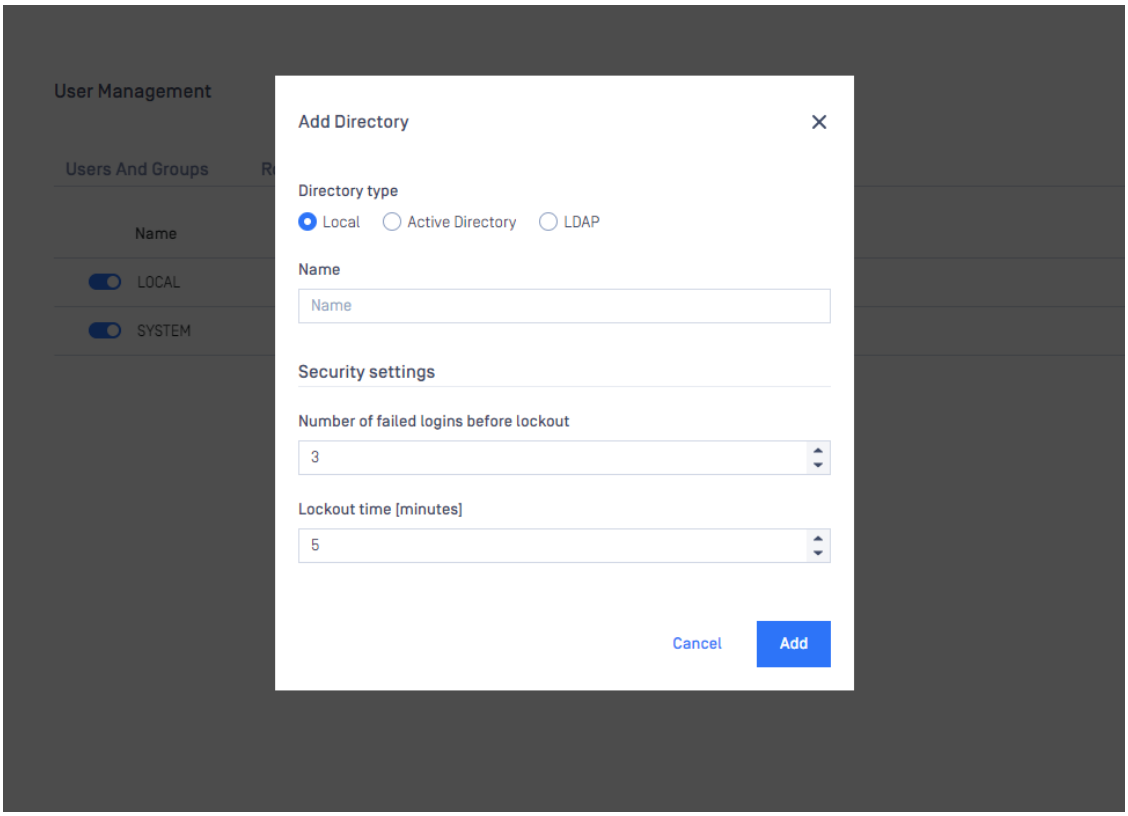
Besides listing existing user directories the **User directories** tab provides the following functions:

- 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 148078792 section.



Add new Active Directory type user directory

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

The USERNAME and PASSWORD values should be the name as DN (distinguished name) and password of a user who has permissions to do searches in the directory.

Warning

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 Configuring TLS.

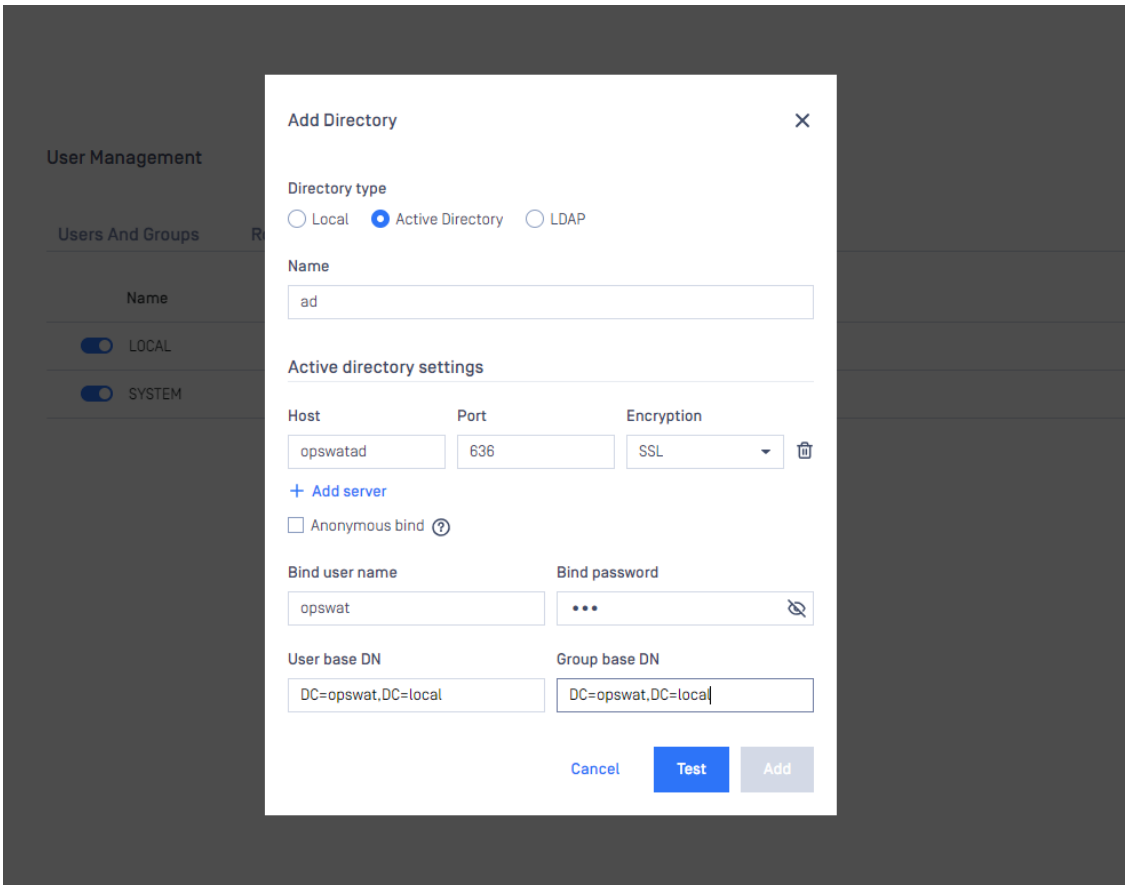
Warning

As long as ENCRYPTION field is set to *None* there is no encryption used between the Metadefender Update Downloader and the Active Directory server. All passwords and other information are sent clear-text over the network.

Use *StartTLS* or *SSL* as ENCRYPTION whenever possible.

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

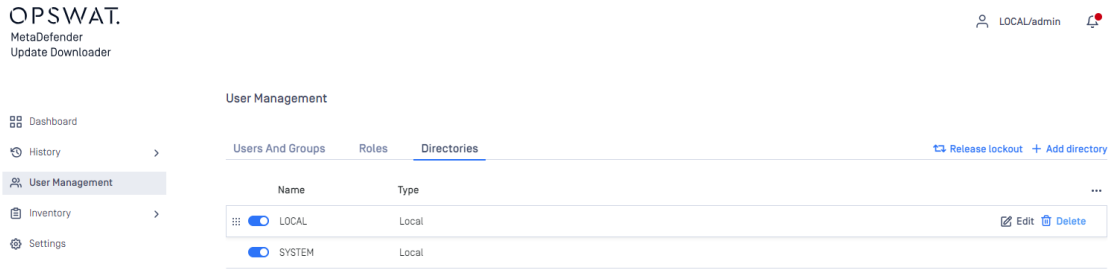
Click the *TEST* button to test the Active Directory settings. If the test succeeds then the user directory can be added to the list with the *ADD* button.



Delete user directory

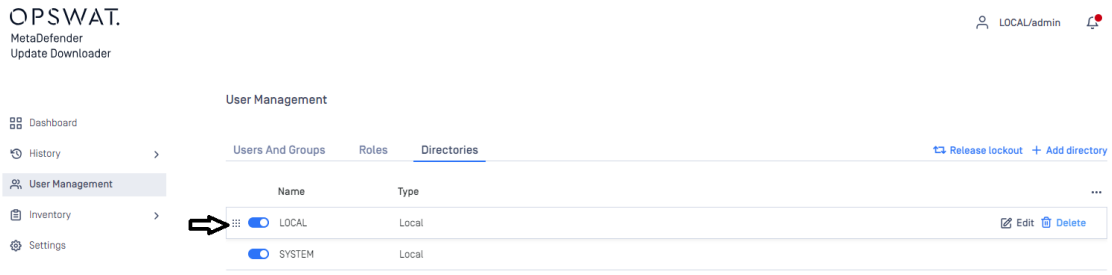
> **Note**
>
> Users of the deleted user directory will be deleted as well. As a consequence active sessions of the users of the deleted user directory will be aborted at the time of the next interaction with the server (see the Delete user section).

To remove a user directory, hover the mouse pointer over the user directory's entry in the list and click **Remove user directory** icon.



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.

> **Note**
>
> 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 **x** mark. To enable the user directory click the **Enable user directory** icon.

Unlock locked accounts

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

Notes

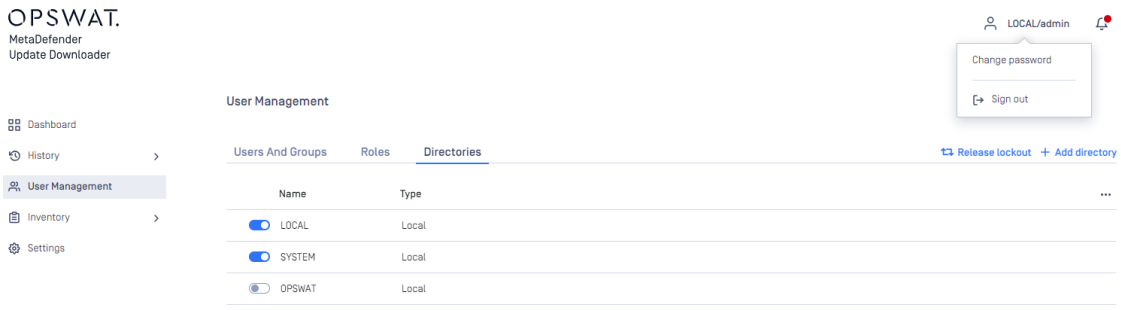
The currently logged on user can not disable the user directory to which her account is assigned to. For example the admin user can not disable the LOCAL user directory.

The currently logged on user can not delete the following:

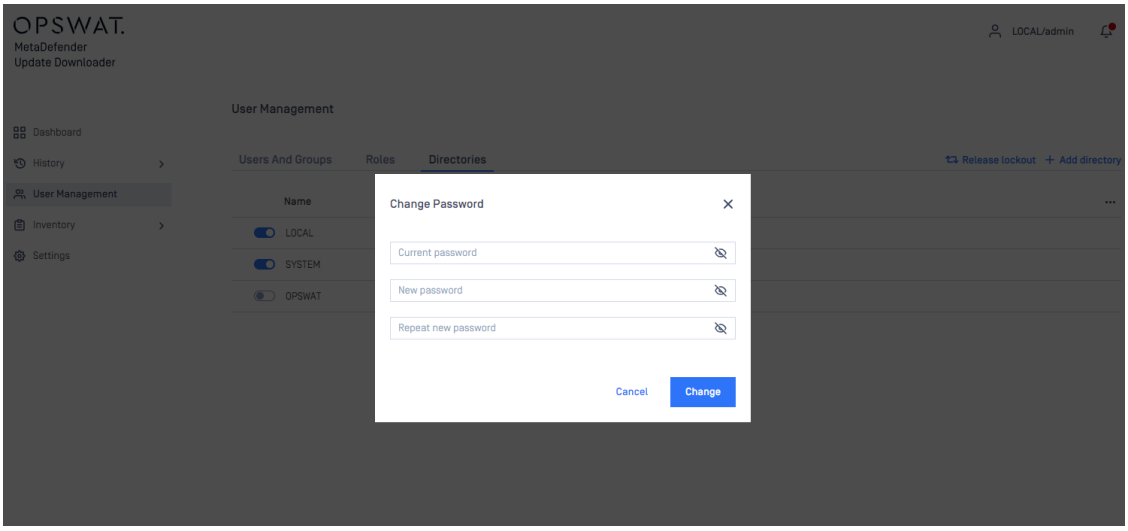
- Her own user account. For example the admin user can not delete the admin user account.
- The user directory to which her account is assigned to. For example the admin user can not delete the LOCAL user directory.

Change user password

The current user can change the password by hovering on the right corner, User icon



Changing password



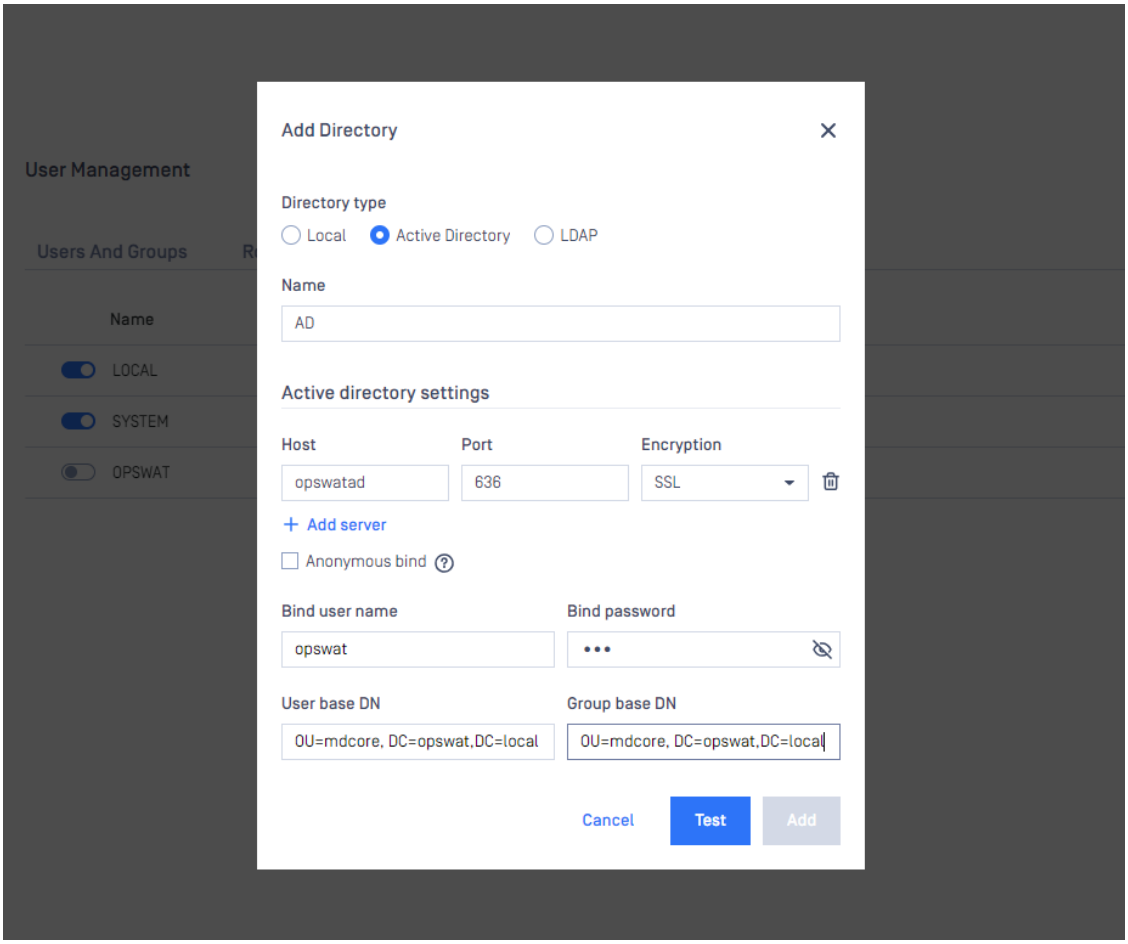
Important notes

Warning

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 Configuring TLS.

Active Directory attributes

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



Username

All three attributes should be expressed with a valid LDAP syntax.

Normally a domain administrator should provide these values, however there is a way to get the USERNAME as a LDAP DN, that is needed for the Metadefender Update Downloader to do searches in the directory information tree, and it is as follows:

Log on to a Windows server machine that has connectivity to the Active Directory

1. Choose a user that is intended for this purpose (ie: has rights to do searches in the tree)

2. Open a Command window with elevated rights (Run as Administrator)

3. Assuming example.com as domain and John Smith with account name john.smith as the user, type the following:

cmd · bash

```
> dsquery user domainroot -samid john.smith
```

or

```
cmd · bash

> dsquery user domainroot -name John Smith
```

Info

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.

User base and group base DN

Once the 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:

```
Code

DC=example,DC=com
```

Note

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 Metadefender Update Downloader password validation. The rule of thumb here is that the more specific the user/group DN the faster the server response.

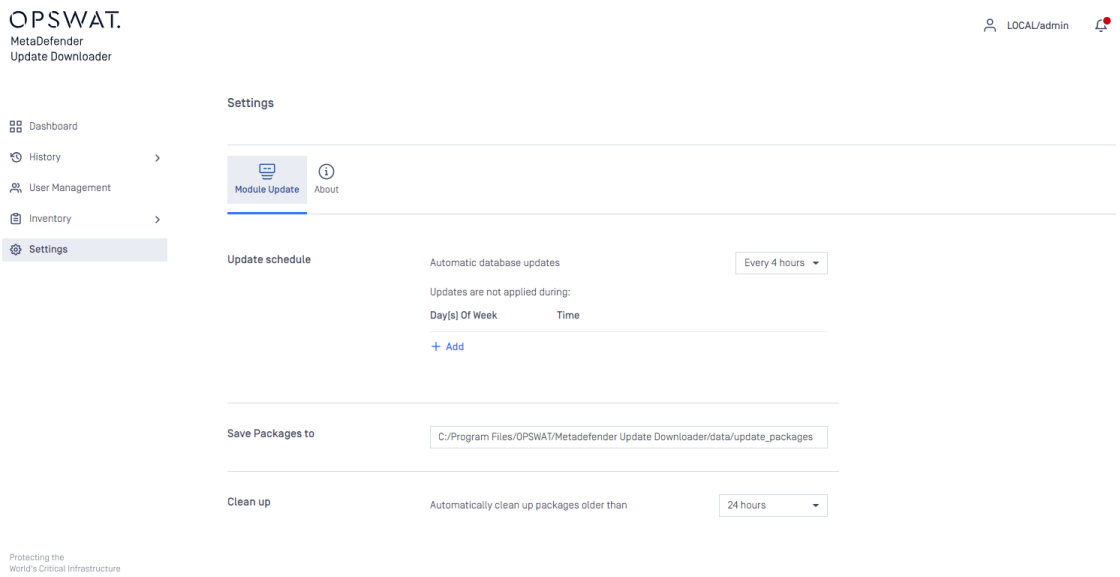
Taking the above example into consideration: a user search DN of "OU=People,OU=Engineering,DC=example,DC=com" could potentially result in much faster server response than "DC=example,DC=com" and should be preferred assuming all users reside under "OU=People,OU=Engineering,DC=example,DC=com" in the directory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

Note

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 Metadefender Update Downloader not to find group accounts in the directory information tree. So these DNs should be chosen carefully.

Automatic update

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



Update settings

- **Automatic database updates**: Update Downloader will check for new updates according to this schedule.

If you have installed or if you wish to use the MetaDefender Update Downloader in a restricted environment, you will have to allow access to the following hosts' for engines / databases download:

- https://update.dl.opswat.com

Note:

IP address-based whitelisting on your firewall might probably fail after some time since OPSWAT uses CDN (Content Delivery Network) to faster delivery updates over the world, and IP address of edge servers might change over time.

Even the OPSWAT update servers host updates for all of the available engines we support, sometimes the custom engines might try to connect to their own cloud for updates, but this can be disabled in firewall and they will be updated just from OPSWAT.

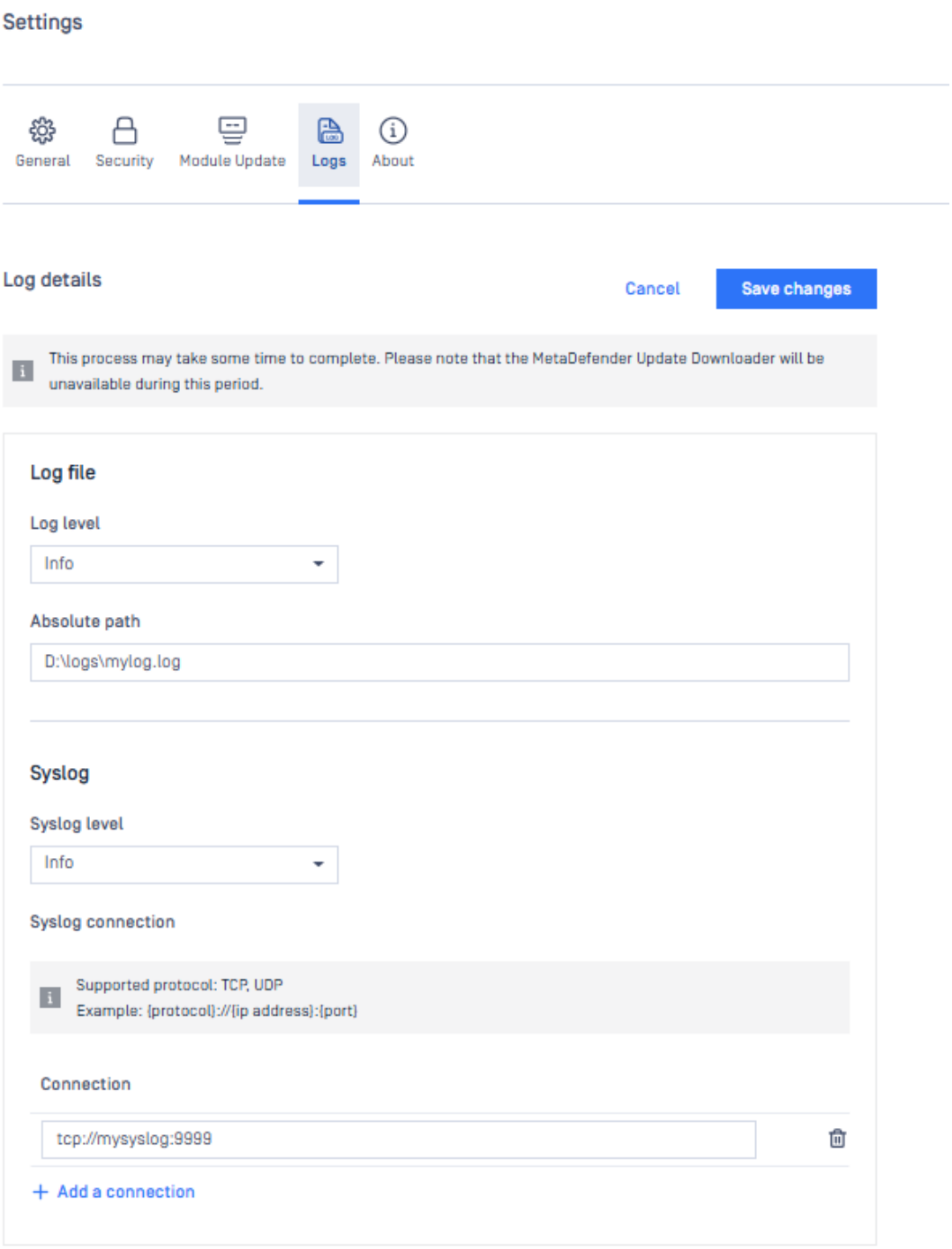
- **Save packages to**: You can find exported update packages in this directory. For Metascan v4.x/Central Management you can find updates in the root of this directory. For Metascan v3.x updates are generated into a subdirectory called MetascanV3
- **Automatically clean up packages older than**: Product 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.

- **Update time**: configure when NOT to export packages.

Logging

MetaDefender Update Downloader has wide variety of options to configure logging. Log settings are in the configuration files or web console

Configure via web console



Web console support:

- Log file path
- Log file path level
- Syslog connection
- Syslog level

For more configuration, please use the configuration file.

> **Warning**
>
> Please note that when changing logging configuration, Update Downloader will automatically reload it service, during this time, the service is unavailable
>
> **Limitation:** On Rocky/RHEL 9, in certain situations, the service may not automatically reload as expected. In such cases, users are required to manually reload the service.

Configure via the configuration file

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

- Update Downloader server configuration file

In case of using linux operating system 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?

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:

> **Warning**
>
> MetaDefender Update Downloader only **accepts** the file named **ssl.conf.mddownloader** for HTTPS **enable only**
>
> The user **needs** to take care of the permissions of the file **ssl.conf.mddownloader**.
>
> For other configuration related to SSL like TLS version, ciphers, etc. Please use an other configuration file for example ssl.conf

HTTPS enable via ssl.conf.mddownloader

1.Create file **ssl.conf.mddownloader** in the directory

- Linux /etc/ometadownloader/nginx.d
- Windows: in the directory <Installation Directory>\nginx.

2.Enter SSL-configuration according to Nginx. In order for the encrypted HTTPS connection to work, the certificate-key pair is required. This pair contains a certificate.crt file and a certificate_key.key file.

To allow simple SSL one needs to add the following lines only:

Linux:

ssl.conf.mddownloader · bash

```
ssl on;
ssl_certificate /etc/ometadownloader/nginx.d/your.crt;
ssl_certificate_key /etc/ometadownloader/nginx.d/your.key;
```

Windows:

ssl.conf.mddownloader · bash

```
ssl on;
ssl_certificate C:\Program Files\OPSWAT\Metadefender Update Downloader\nginx\your.crt;
ssl_certificate_key C:\Program Files\OPSWAT\Metadefender Update Downloader\nginx\your.key;
```

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

Note that certificate and key files **are provided** by the user who can store them **wherever** it is convenient. Please adjust the paths accordingly.

Note: When **choosing the location** for **.crt** and .key files, make sure they are readable by the service user as well as

the directory **they are executed from.**

Other SSL configurations

The file ssl.conf.mddownloader is only for enable HTTPS, for other configurations like TLS version, cipher, please create another conf file, for example ssl.conf

ssl.conf · bash

```
ssl_protocols TLSv1.3;
```

> **Info**
>
> OPSWAT has **fully deprecated support for TLS 1.0 and TLS 1.1** across its product line

For more SSL-options please consult Nginx documentation.

Password Policy

Password Policy settings are accessible under **Settings > Security** tab .

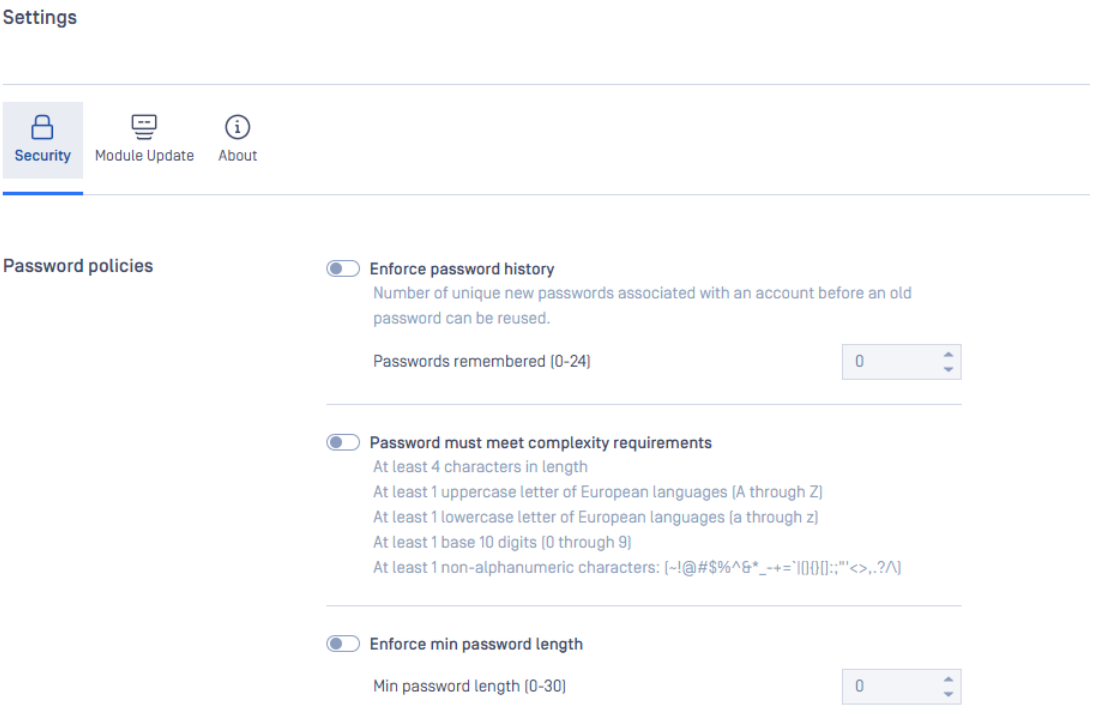
Local users' password can be enforced to meet requirements set by administrators, which includes following constraints:

- **Enforce password policy:**
  - Determines the number of unique new passwords that must be associated with a user account before an old password can be reused
  - Range: [0-24]
  - Default: 0 (to disable enforcement)
- **Minimum password length:**
  - The least number of characters that can make up a password for a user account
  - Range: [0-8]
  - Default: 0 (to disable enforcement)
- **Password must meet complexity requirements:**
  - Determines whether passwords must meet a series of guidelines that are considered important for a strong password:
  - Default: unchecked

> **Info**
>
> At least 1 uppercase letter of European languages (A through Z) At least 1 lowercase letter of European

languages (a through z).

At least 1 base 10 digits (0 through 9) At least 1 non-alphanumeric characters (special characters): (~!@#$ %^&*_-+=`|(){}[]:;'"<>,.?/)



Info

Only the user that has an admin role can modify this setting

User Guide

Note

Since MetaDefender Update Downloader 2.4.0, the licensing mechanism has been changed.

- No longer need to activate license of Update Downloader itself to make it operational.
- Instead required to add license file (.yml) of offline MetaDefender products

Check out 1.2. License activation to learn more.

About this guide

The Update Downloader product is designed to download updates to an internet connected computer and save it to

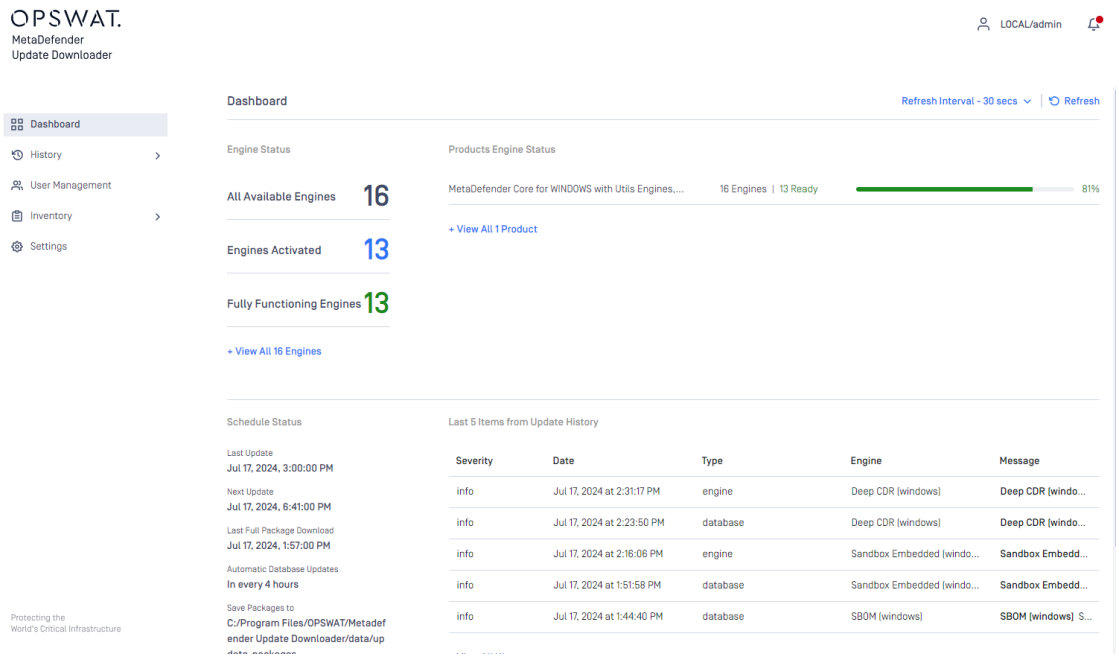
a specified folder to make it possible to upload to a non-internet connected Metascan v3, v4 or Central Management product.

Feedback

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

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.



Dashboard overview

Overview page

The Overview page shows information on

- Number of engines
- Number of selected engines
- Update status
- Licence information
- Active engines with platform, version and database information
- Recent records from update history

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

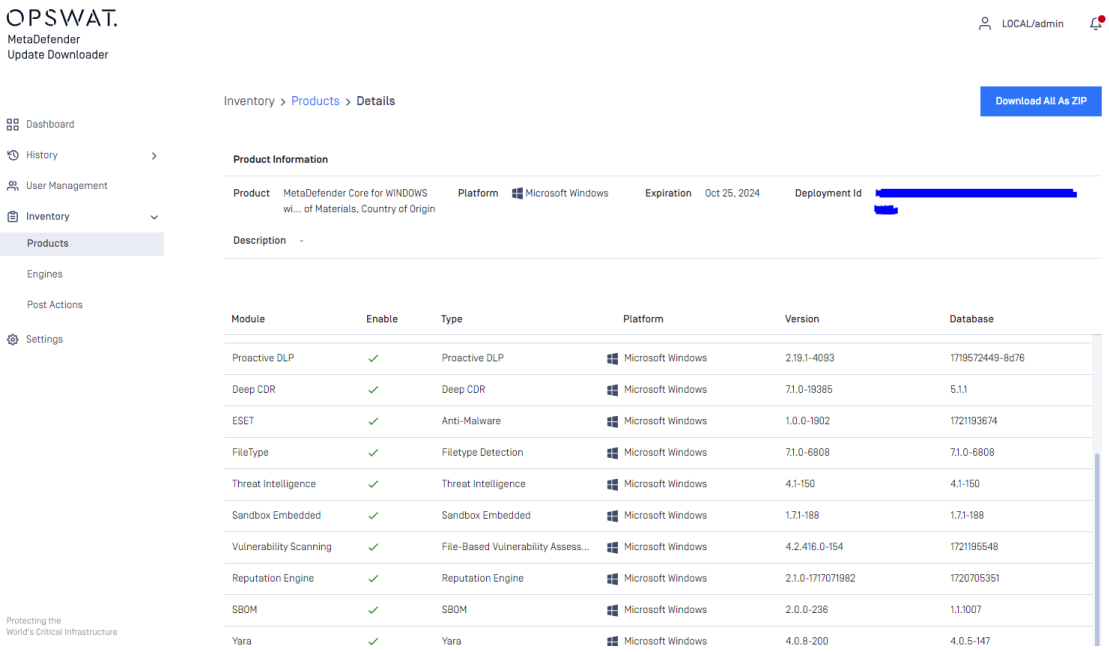
Update history

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.

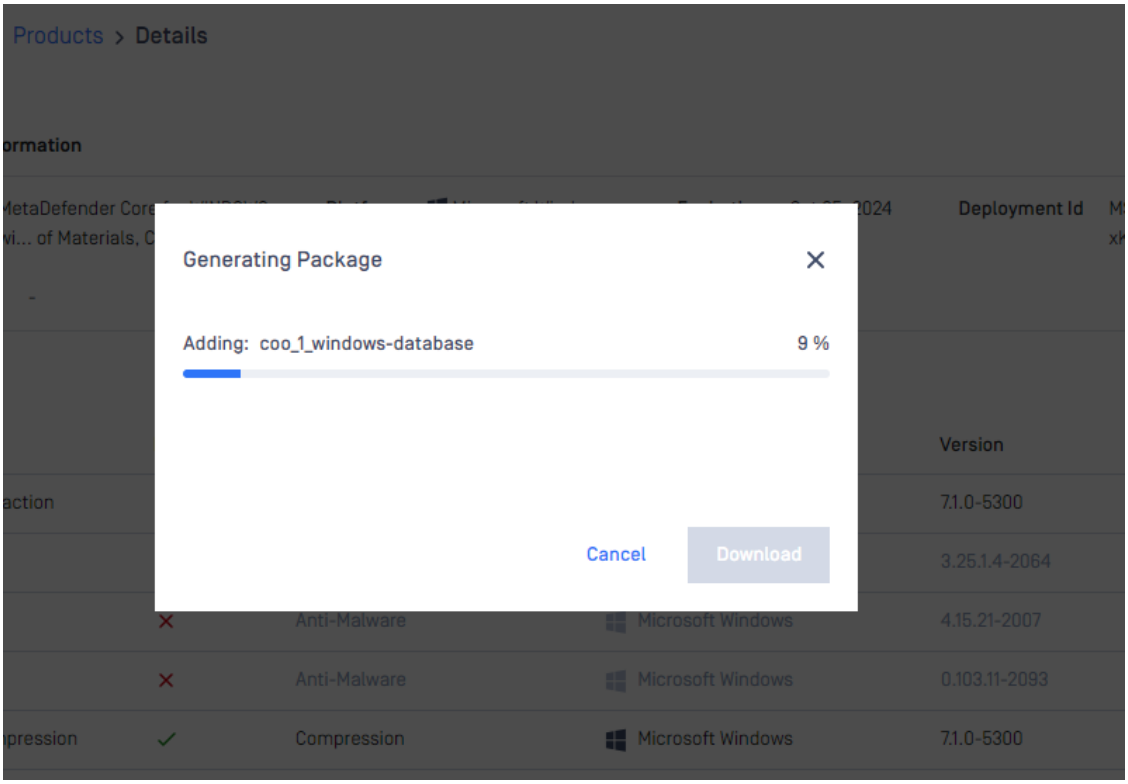
Download all update packages

Goto Inventory > Products > Select the product you want to download

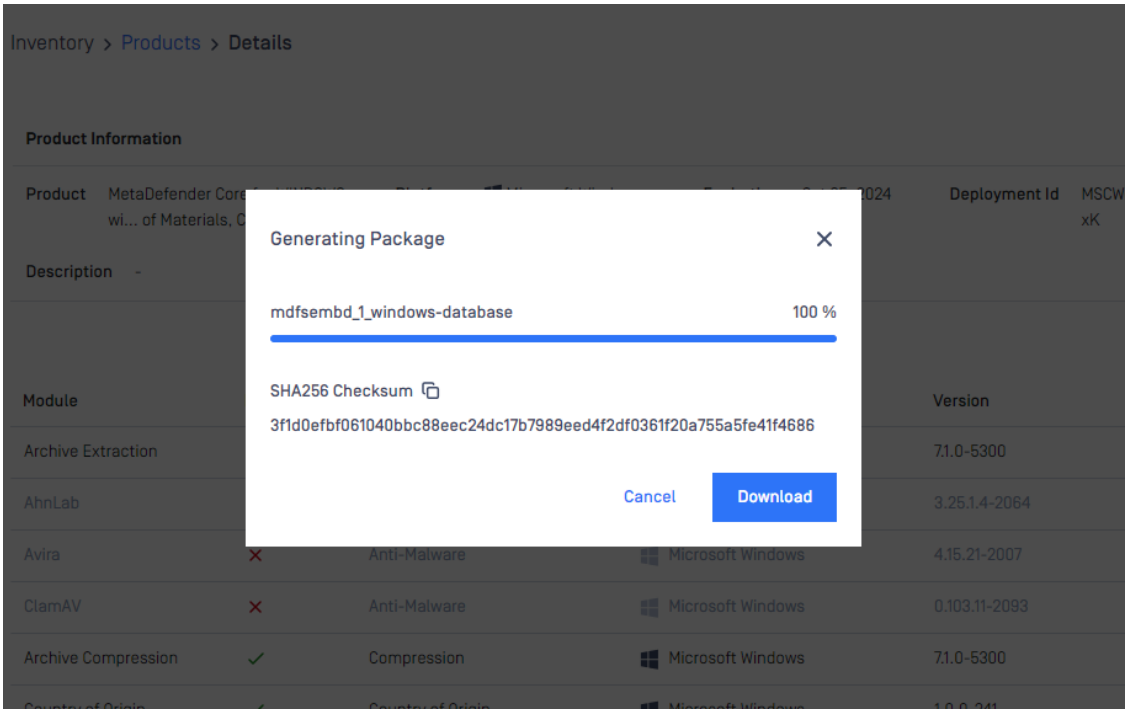


Hitting **Download All As Zip** button at the top right to download all engines' update packages as single archive .zip file

Confirm the package generation and wait for the package to be built.



When package generation is done the modal looks as below. For security reasons the modal also shows the SHA256 checksum of the generated package file so it can be validated.



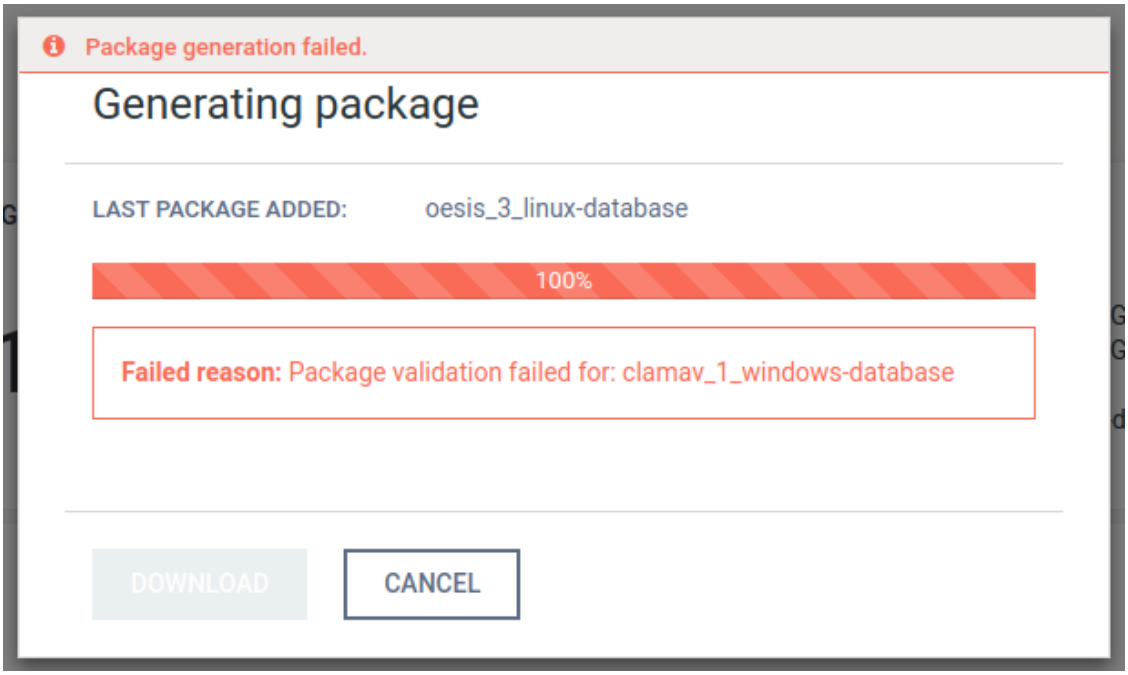
The resulting zip file among the update packages (**.yml and .zip files**) will contain a file called **report.txt** that holds information on the package generation and looks like the following.

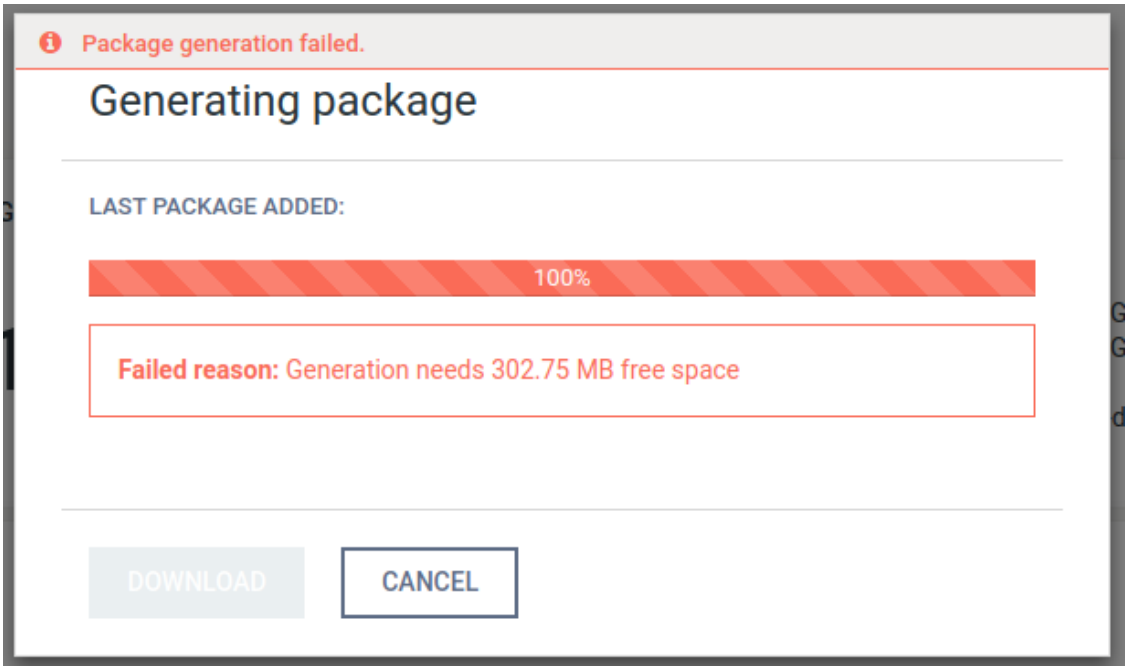
report.txt · bash

```
===== Update package report =====
```

```
Created at 2018-06-07T07:06:01.879Z

There are 20 update packages in this archive

== clamav_1_windows-engine ==

    clamav_1_windows-engine-1486651156-1528354018032.yml
        Package version: 0.99.2-24
        Filesize: 5565 bytes
        SHA256: 4091a5d032c8f2996a362fa266f56a4cf9fd949acb15d33ce4edfc9caa6b72d0
        OPSWAT digital signature.......... VALIDATED
        Checksum.......................... VALIDATED
    clamav_1_windows-engine-1486651156.zip
        Filesize: 4134048 bytes
        SHA256: fcaaf883823dec041c540236d0a4b76496e4a088e0a21ebbefe12bf0fdfe432c
        Extraction........................ VALIDATED
        Checksum of the extracted files... VALIDATED

== 7z_4_linux-database ==

    7z_4_linux-database-1507797673-1528354018032.yml
        Package version: 16.02-242
        Filesize: 1578 bytes
        SHA256: 29acddc32b8b3656df89466bf46c6770b1dfe881d5982b007f8c8c97805515e4
        OPSWAT digital signature.......... VALIDATED
        Checksum.......................... VALIDATED
    7z_4_linux-database-1507797673.zip
        Filesize: 929419 bytes
        SHA256: e3b7f772d99837c8fdd19e619013af7f5d60bc7c4accf982afa1a90a06f1fe8b
        Extraction........................ VALIDATED
        Checksum of the extracted files... VALIDATED

== eset_1_windows_engine ==
...
```

If something goes wrong during the package generation the zip won't be available and an error message will be displayed.





Info

Note:

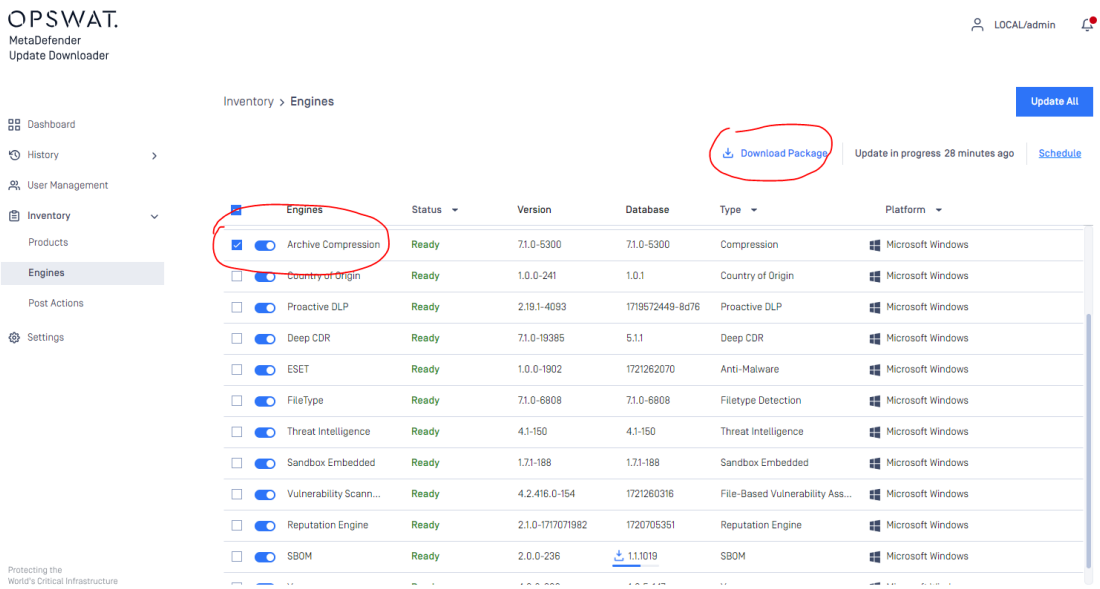
- Generated package contains all those update packages which states are "ready". The "exporting" state means that the update package export is still in progress and it will not be contained by the generated package.
- Depending on the number of update packages, the generated package can be a huge zip file.
- Before the package generation, the product checks if there is enough free disk space and in case of insufficient space, it informs you on the needed amount.
- After a successful download the generated package will be removed to free up disk space.

- When a new package is generated all previous ones that are not currently being downloaded will be removed automatically.

Download individual package

Starting from version 3.1.0 we now can download an individual package

Goto Inventory > Engines > Select the engine that you want to download > Click Download Package



Inventory management

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

Engines

Products

Post Actions

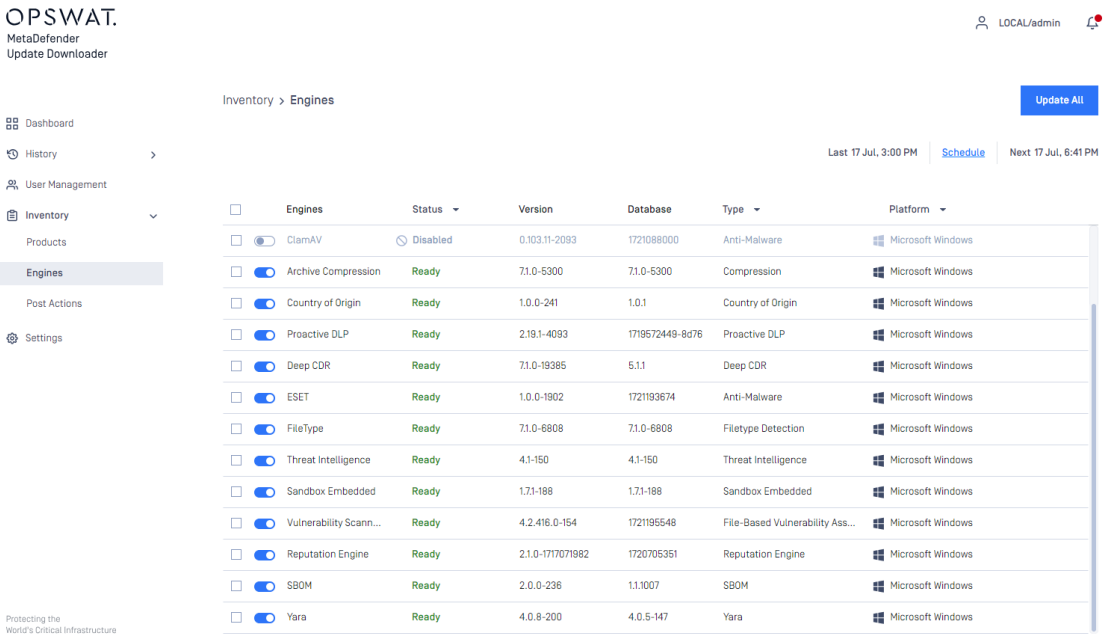
Engines

Under the **Inventory > 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
  - Data sanitization engine

- Filetype detection engine
- Utility engine
- Vulnerability detection engine

- Platform the engine runs on
- Engine version
- Database version the engine is using
- Engine status (Enabled / Disabled)



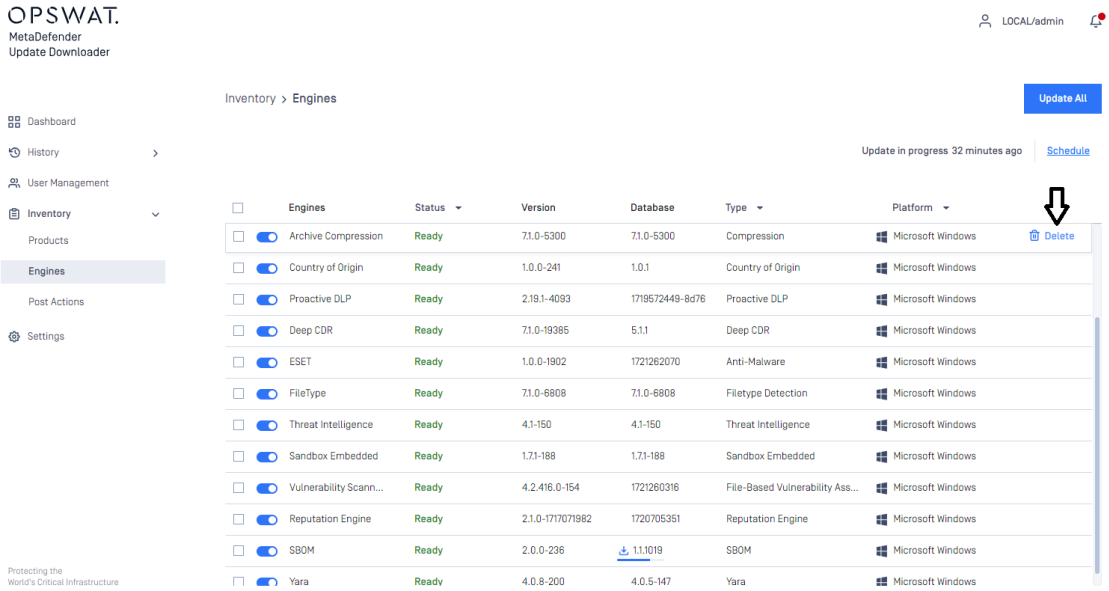
Engines

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

Remove engine

To manually remove engine you can hover on each engine, click on Delete button



Products

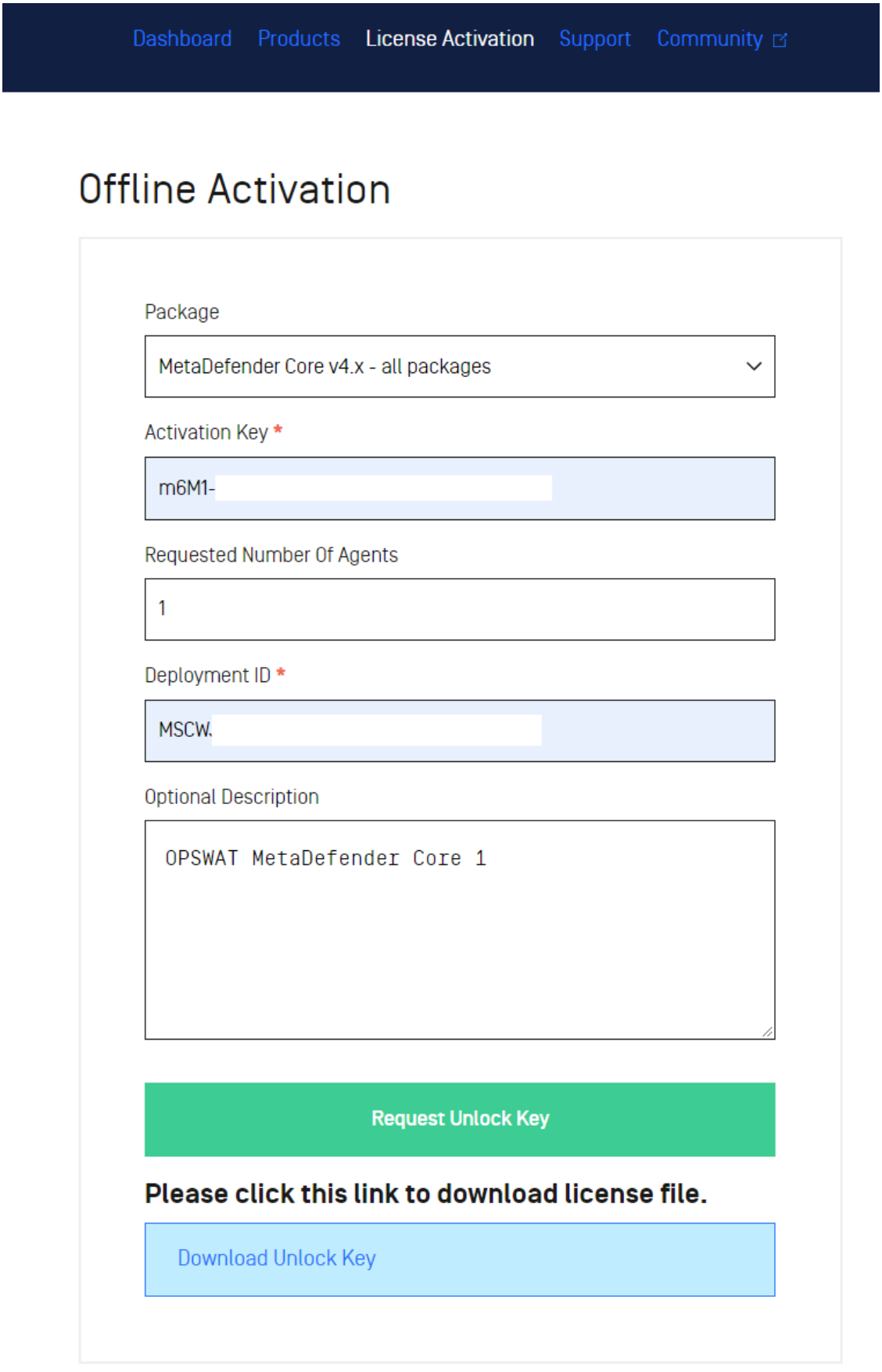
> **Note**
>
> Since MetaDefender Update Downloader 2.4.0, the licensing mechanism has been changed.
>
> - No longer need to activate license of Update Downloader itself to make it operational.
> - Instead required to add license file (.yml) of offline MetaDefender products
>
> Check 4.2.2 Products to learn more how to add

> **Info**
>
> MetaDefender Update Downloader only support for MetaDefender Core

Generate a license file (.yml)

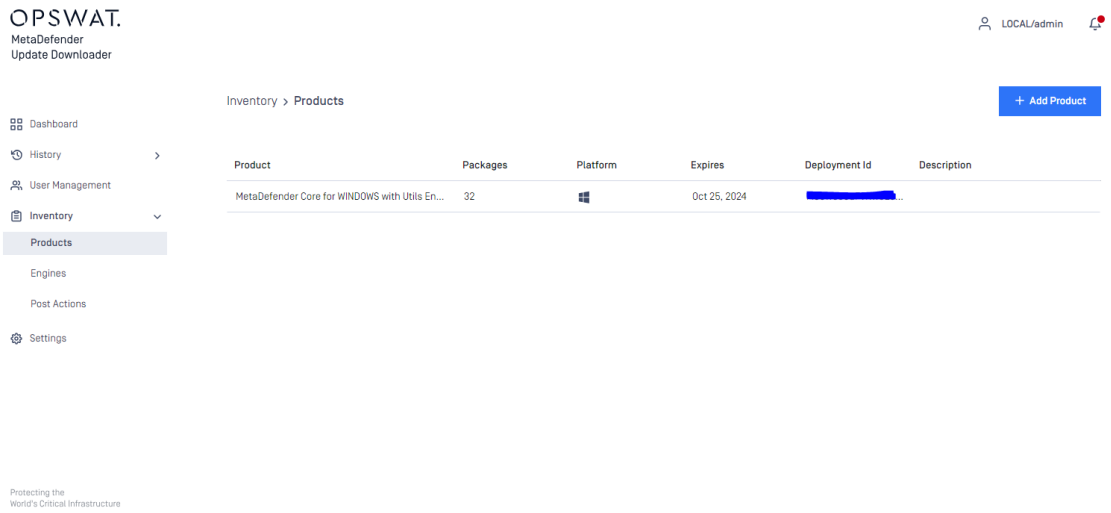
- Navigate to OPSWAT Activation portal page - https://portal.opswat.com/licenses/activate (login required)
- Choose right **Package** option assiociated to your MetaDefender product (e.g. MetaDefender Core, MetaDefender Drive)
- Type or paste your associated MetaDefender product's license activation key.
  - Double check to ensure no redudant space unintentionally attached into the head or tail of license string
- Keep default value for **Requested Number of Agents**
- Type or paste your associated MetaDefender product's deployment ID.
  - Double check to ensure no redudant space unintentionally attached into the head or tail of license string

- (Optional) Write a description to keep track of this particular activation on our system for **Optional Description**
- Hit **Request Unlock Key** button to generate the license file (<deployment ID>.yml)
- Hit the hyperlink **Download Unlock Key** to download the license file and save it locally on server where you pre-installed Update Downloader

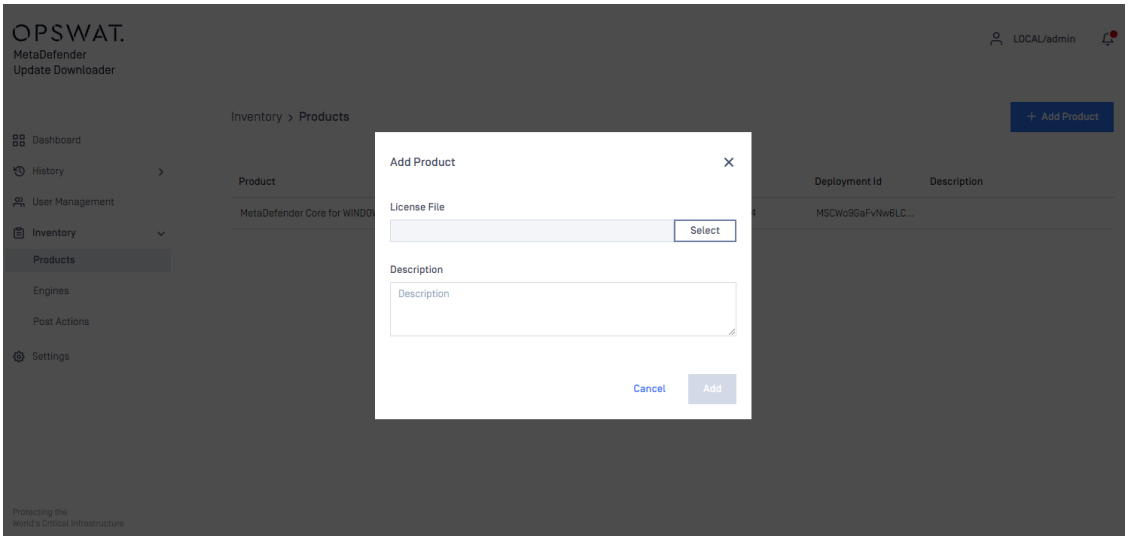


Add a new product on Update Downloader

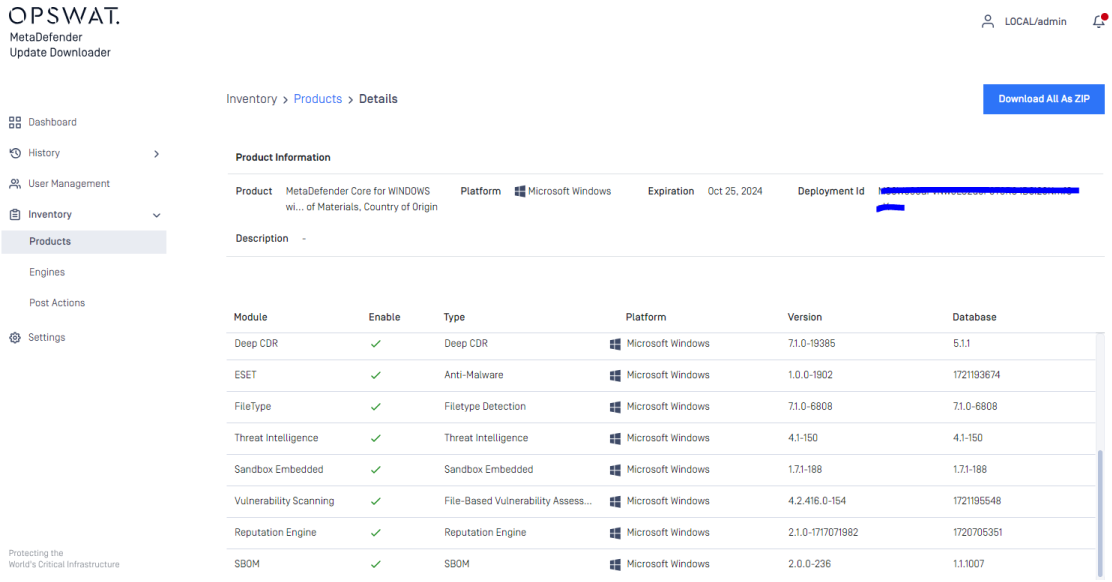
- Ensure you already installed Update Downloader, and setup a local admin user through its wizard
- Navigate to **Inventory** → **Products** page under left menu - http://localhost:8028/#/user/inventory/products
- Hit **ADD NEW PRODUCT** button to add new product on Update Downloader



- Select the license file (.yml) which was obtained in steps above



- Hit **ADD** button to start downloading offline update packages for associated licensed product



- Hitting **Download All As Zip** button at the top right to download all engines' update packages as single archive .zip file, see more at Download all update packages
- You can add and manage offline update packages for multiple licensed MetaDefender products

Post Actions

> **Info**
>
> This feature is only available since Update Downloader 2.5.0
>
> We do not recommend to create post action and assign it to a product when:
>
> - Update Downloader shares an export folder with any MetaDefender Core, and
> - In Update Settings of that MetaDefender Core, the setting DELETE FILES AFTER IMPORT is enabled.
>
> Reason: the packages in shared folder might be removed by MetaDefender Core first before the post action takes action on those packages.

Pre-defined post actions to be auto triggered whenever a downloaded engine, or its database, turns to ready state to deliver to your all associated offline MetaDefender product(s).

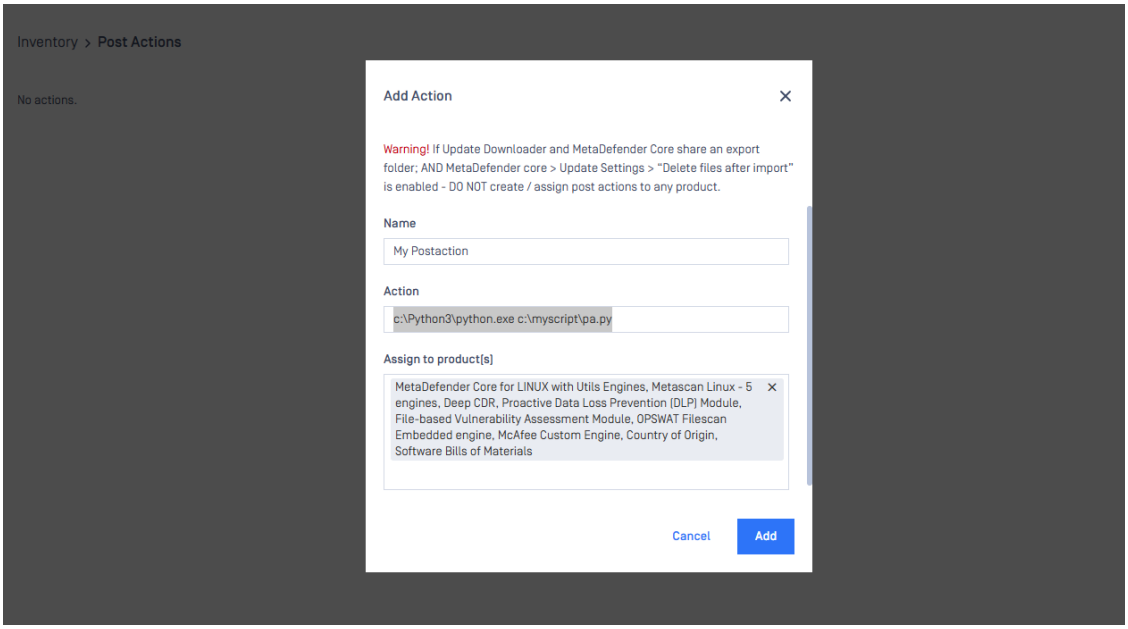
This feature setting can be found under **Inventory menu Post Actions**

- Hit **ADD NEW POST ACTION** to add a new one

> **Info**
>
> - One post action could be assigned to one or multiple created product(s) - Check 4.2.2 Products to learn how to create a product on Update Downloader
> - One created product can have one or multiple post action(s) assigned to run

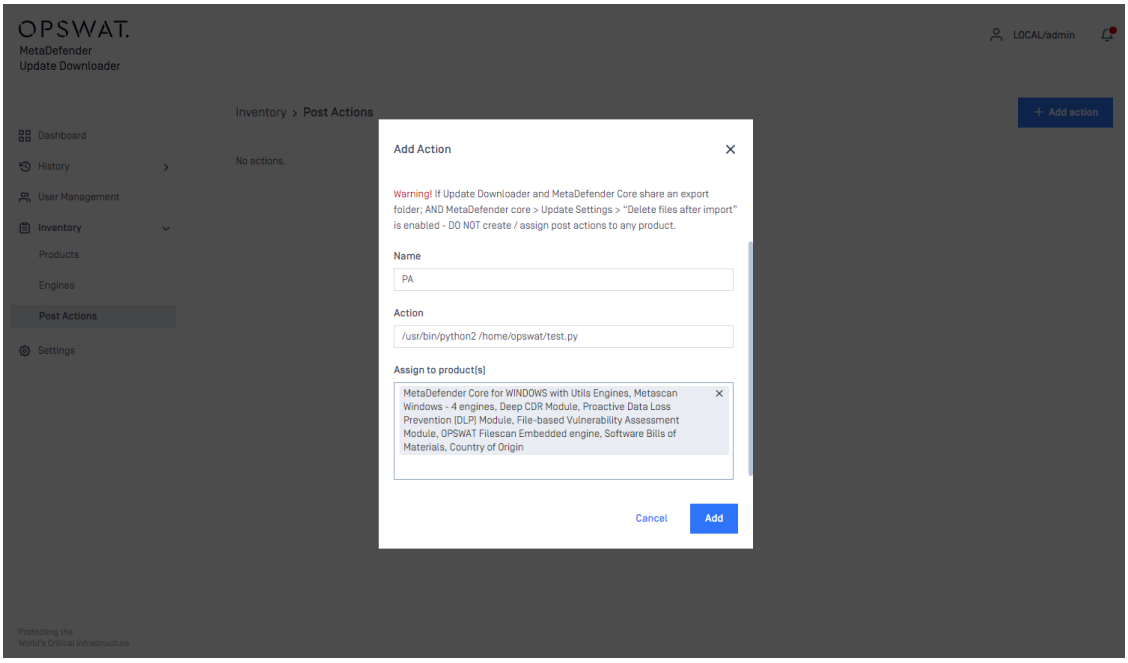
Windows

Example action: `c:\Python3\python.exe c:\myscript\pa.py`



Linux

Example action: `/usr/bin/python2 /home/opswat/test.py



- Hit **ADD** button to finish.

Integration instruction

STD input for your integrated script to consume and process:

Code · json

```
{
  "content_type": "[string] <engine / database>",
  "location": "[string] full folder path where .zip and .yml created",
  "generated_end_time": "[string] EPOCH datetime when both .zip and .yml are built done 100%",
  "package": {
    "display_name": "[string] file name of .zip",
    "file_size": "[integer] ORIGINAL file size of .zip",
    "file_hash": "[string] ORIGINAL SHA256 hash of .zip"
  },
  "package_metadescriptor": {
    "display_name": "[string] file name of associated .yml",
    "file_size": "[integer] ACTUAL file size of associated .yml",
    "file_hash": "[string] ACTUAL SHA256 hash of associated .yml",
    "content": "[string] full content of .yml file which must be converted to JSON format"
  }
}
```

ORIGINAL file size and hash of .zip file are defined in the master .yml file "\data\updates\metadescriptor".

For example:

```
{
    "content_type" : "database",
    "location" : "C:\\Program Files\\OPSWAT\\Metadefender Update Downloader\\data\\update_packages",
    "generated_end_time" : "1592212251",
    "package" : {
        "display_name" : "clamav_1_windows-database-1592179220.zip",
        "file_size" : 188403712,
        "file_hash" : "9888259784F7ACE37E0585BCFCED92EA6B7DCFE884F25F408FAC260F04F5EA7A"
    },
    "package_metadescriptor" : {
        "display_name" : "clamav_1_windows-database-1592179220-1592187038805.yml",
        "file_size" : 2006,
        "file_hash" : "4EFA879EB28471FB1A48269F81C9FD29B5A6D6FF72FEFFB54B27DA82CF62366D",
        "content" : {
            "archive" : { ... },
            "content_type" : "database",
            "db_api" : 1,
            "database_dir" : "db",
            "update_method" : "file",
            "engine" : {
                "id" : "clamav_1_windows",
                "name" : "Clamav",
                "type" : "av"
            },
            "files" : [ ... ],
            "package_version" : 1592179200
        }
    }
}
```


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.

Monitoring

Overview

The `/readyz` API provides a simple way to monitor the health and status of your MetaDefender Downloader instance. This endpoint is particularly valuable for air-gapped environments where active monitoring of engine updates and system health is required.

API Endpoint

GET /readyz

Query Parameters

The API accepts an optional `info` query parameter with the following possible values:

Parameter Value	Description
version	Returns the MetaDefender Downloader version
updater_server_connection	Checks connectivity to the updater server
diskspace	Reports free and total disk space for the data directory (in bytes)
engine	Returns status of all engine and database packages
update	Provides update-related information including timestamps and status
all	Returns all information listed above. Note: when using `all`, if other options also included -> it will be considered as invalid option

Multiple values can be requested by separating them with commas (e.g., info=diskspace,version).

Default Response

When called without the `info` parameter, the API returns:

- Downloader version
- Connection status to updater server

Example Requests

Basic Health Check

GET /readyz

Response:

Code · javascript

```
{
    "updater_server": "connected",
    "version": "3.2.3"
}
```

Request Specific Information

GET /readyz?info=diskspace,updater_server_connection

Response:

Code · javascript

```
{
    "free_disk_space": 22213443584,
    "total_disk_space": 247882248192,
    "updater_server": "connected"
}
```

Request All Available Information

GET /readyz?info=all

Response:

Code · javascript

```
{
    "updater_server": "connected",
    "version": "3.2.3",
    "free_disk_space": 37685030912,
    "total_disk_space": 247882248192,
    "update_info": {
        "export_running": true,
        "last_update": 1746761060690,
        "last_update_was_successful": true,
        "next_update": 1746772282162,
        "update_running": true
    },
    "engines": [
        {
            "abandoned": false,
            "download_progress": 100,
            "download_time": "2025-05-09T03:24:20.750Z",
            "eng_id": "7z_17_windows",
```

```
            "eng_name": "Archive Extraction",
            "eng_type": "Bundled engine",
            "eng_ver": "6.4.0-3939",
            "engine_type": "archive",
            "pinned": false,
            "state": "validating",
            "type": "engine"
        },
        {
            "abandoned": false,
            "download_progress": 100,
            "download_time": "2025-05-09T03:24:20.762Z",
            "eng_id": "ahnlab_1_windows",
            "eng_name": "AhnLab",
            "eng_type": "Bundled engine",
            "eng_ver": "3.23.3.2-1947",
            "engine_type": "av",
            "pinned": false,
            "state": "ready",
            "type": "engine"
        },
        {
            "abandoned": false,
            "download_progress": 42,
            "download_time": "2025-05-09T03:24:20.805Z",
            "eng_id": "dlp_13_windows",
            "eng_name": "Proactive DLP",
            "eng_type": "Bundled engine",
            "eng_ver": "2.10.0-1639650749",
            "engine_type": "dlp",
            "pinned": false,
            "state": "downloading",
            "type": "engine"
        }
    ]
}
```


Response Codes

Status Code	Description
200	Request successful
400	Invalid parameter(s) provided

Error Handling

If an invalid `info` parameter is supplied, the API returns:

GET /readyz?info=invalid

Response:

Code · javascript

```
{
    "err": "Invalid param info"
}
```

Monitoring Best Practices

1. **Regular Polling**: Set up automated checks every 5-15 minutes
2. **Alert on Failures**: Configure alerts for:
   - Disconnected updater server
   - Low disk space (below 10% free)
   - Failed update status

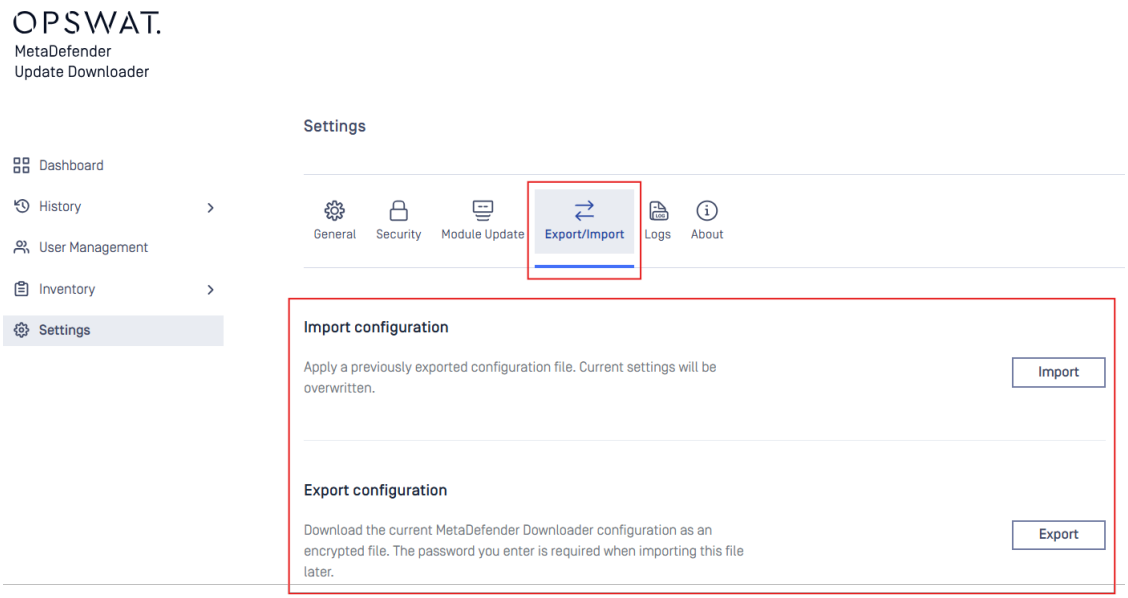
Implementation Notes

- Disk space is reported in bytes
- If engines are actively downloading, the updater server connection is automatically considered "connected"

Export/Import Configuration

Starting from v3.5.0 - MetaDefender Update Downloader has been supported for export/import configuration.

User can find it in: Setting -> Export/Import



The exported configurations will have

- Base configs:
  - General, Module update, Security settings.
  - Post action.
- User management: Users, Roles, Directories.
- Products.
  - Automatically download engines if `Automatic database updates` option is **ON**.

> **Warning**
>
> Logger setting does not supported in Export/Import feature of MetaDefender Update Downloader

How long is the support lifecycle for a specific version of MetaDefender Update Downloader?

OPSWAT provides support on each release of MetaDefender Update Downloader for 18 months after the publication of the **following** release of the product. So, once a new release is published, you have 18 more months of support on the previous release.

Keep in mind, however, that 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, hot-fixes can be provided for the current release of the product, and then incorporated as regular fixes in the next release.

Lifecycles:

Release number	Release date	End-of-life date
3.3.0	July 17, 2025	January 17, 2027
3.2.3	May 20, 2025	November 20, 2026
3.2.2	April 10, 2025	October 10, 2026
3.2.1	February 06, 2025	August 06, 2026
3.2.0	November 19, 2024	May 19, 2026
3.1.0	July 18, 2024	January 18, 2026

Attention:

The versions not mentioned on this page are no longer supported.

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.

- MetaDefender Core v5
- Central Management v7

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.

Info

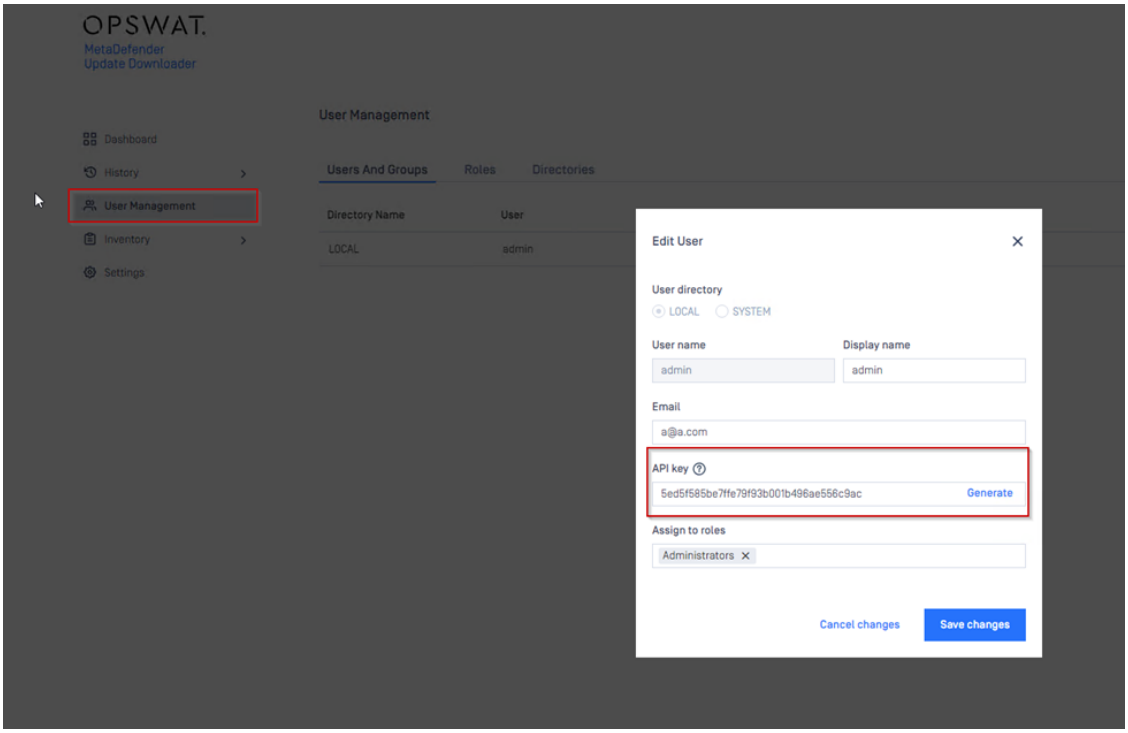
You might need to configure Windows proxy to bypass local addresses if you can't access Web Management

Console from the host itself. Consult netsh documentation for additional configuration options.

How to increase session timeout in MetaDefender Update Downloader via API?

To increase the session timeout on the Update Downloader console via API call you will need the following resources from the Update Downloader instance:

- An API key generated from the Update Downloader console.

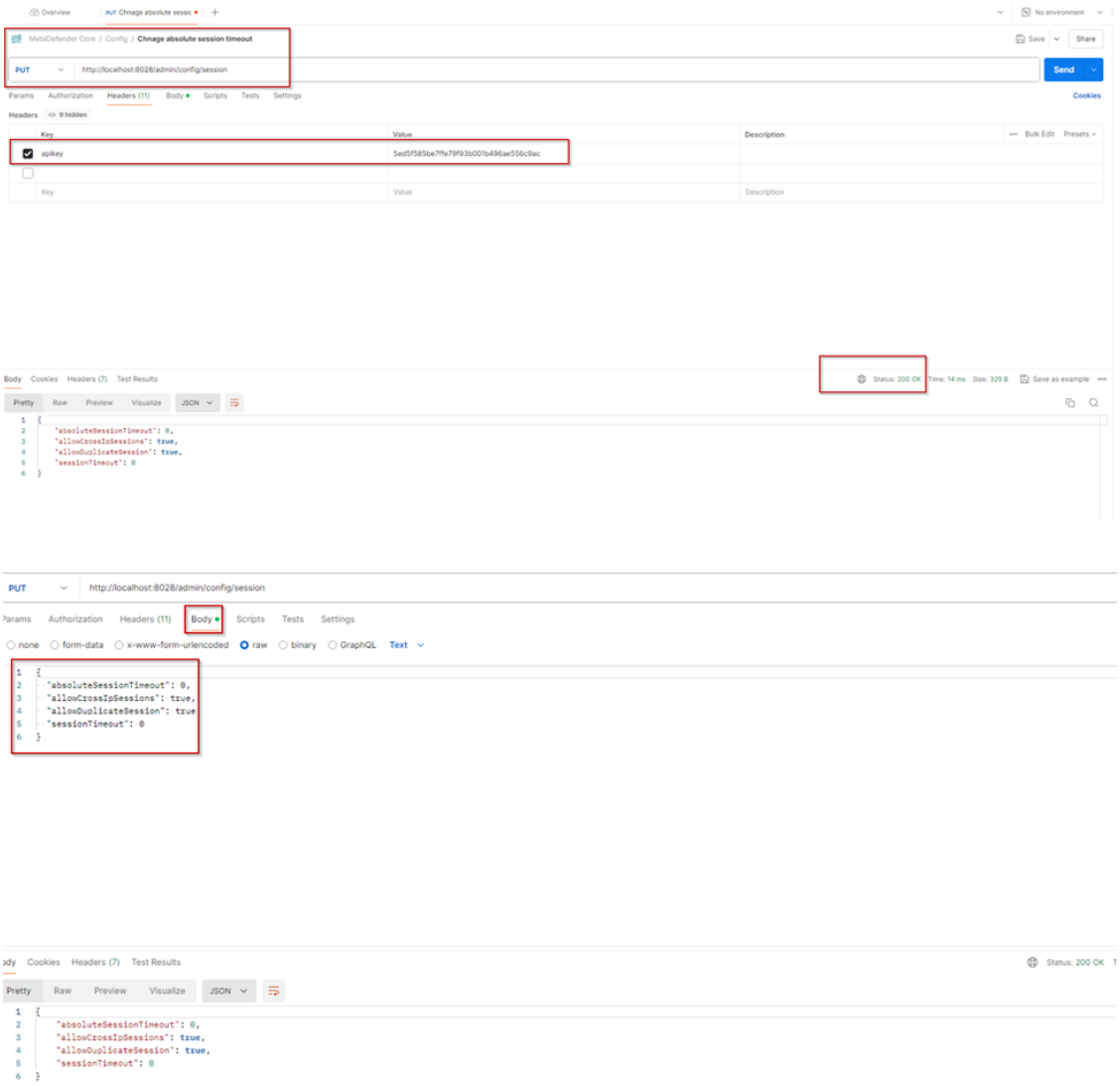


- A valid URL from the Update Downloader instance we are trying to make this change.

Once we have the two items mentioned above we will need to use the following API call to make the change to the session timeout value:

Code · bash

```
curl --request PUT \ --url 'http://localhost:8028/admin/config/session' \ --header 'Content-Type: application/json' \ --header 'apikey: {apikey}' \ --data '{ "absoluteSessionTimeout": 0, "allowCrossIpSessions": true, "allowDuplicateSession": true, "sessionTimeout": 300000 }'
```



The value for the highlighted images from above is set to milliseconds.

Having the “0” value as can be seen in the image above will result in the timeout setting to be disabled.

Support:

If **Further Assistance** is required, please proceed to create a support case or chat with our support engineer.

Can MetaDefender Update Downloader Be Set Up to Transfer Updates to OPSWAT Central Management via FTP?

Yes, MetaDefender Update Downloader can support FTP transfer to OPSWAT Central Management Server, but it is not recommended due to security purposes.

Security Considerations

FTP (File Transfer Protocol) is an outdated and insecure method for transferring files due to several vulnerabilities, including:

1. Lack of Encryption: FTP transfers data, including credentials, in plain text, making it susceptible to interception and unauthorized access.
2. Passive and Active Mode Risks: FTP operates in both passive and active modes, both of which can introduce security risks such as port exposure and susceptibility to man-in-the-middle attacks.
3. No Integrity Verification: FTP does not provide built-in mechanisms for verifying data integrity, increasing the risk of tampered updates being transferred.
4. Limited Access Control: FTP does not support modern authentication mechanisms, making it harder to enforce strict security policies.

To ensure secure and reliable communication, OPSWAT Central Management requires the use of secure protocols such as HTTPS or SFTP for transferring updates. These protocols provide encryption, authentication, and data integrity verification, aligning with modern security best practices.

Support:

If Further Assistance is required, please proceed to create a support case or chat with our support engineer.

How to remove an engine that is stuck on an old database or engine version for MetaDefender Update Downloader?

Please following the steps below:

1. Navigate to Update Downloader located at http://localhost:8028
2. Navigate to “Inventory” > “Engines” > click the trash can to the right of the engine [if able]
3. Stop the Update Downloader Service under “Services” of the OS
4. Open up the File explorer and remove the specific engine[s] package[s] from the following locations `C:\Program Files\OPSWAT\Metadefender Update Downloader\data\updates\av` `C:\Program Files\OPSWAT\Metadefender Update Downloader\data\updates\db`
5. Remove the specific engine[s] package[s] from `C:\Program Files\OPSWAT\Metadefender Update Downloader\data\update_packages`
6. Start the Update Downloader service and navigate to “Inventory” > “Engines” to hit “Update All”
7. If the engine still does not download the latest, you can rename the folder [update_packages] `C:\Program Files\OPSWAT\Metadefender Update Downloader\data\update_packages` then when getting new updates, a new folder will be created [update_packages], redownloading all the engines from our update server.

Support:

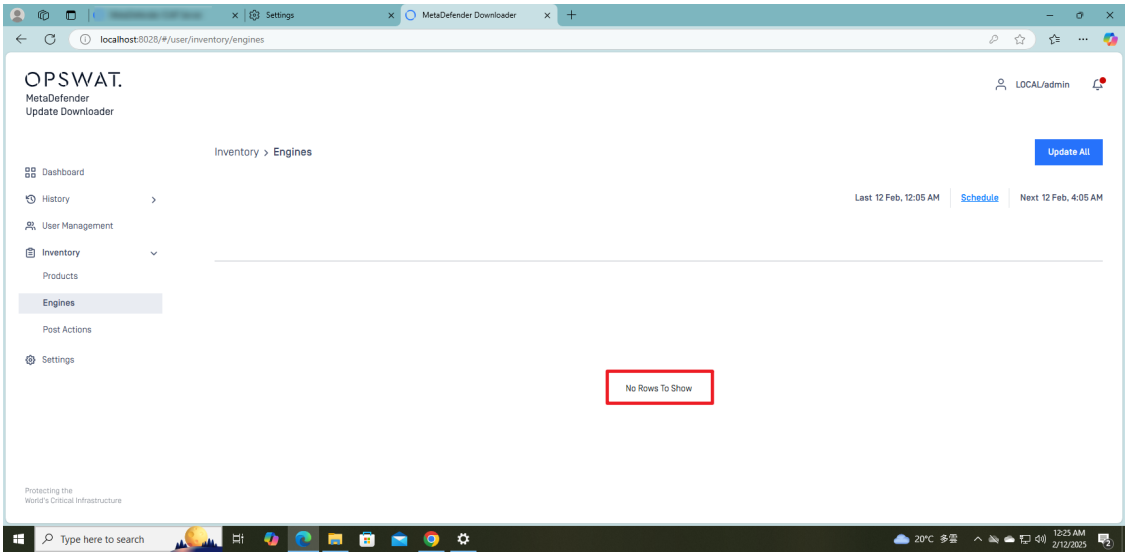
If Further Assistance is required, please proceed to create a support case or chat with our support engineer.

Why Am I Getting "No Rows to Show" When Using a Proxy Without Authentication in Browser Settings?

Problem

When you set the proxy without authentication in Edge or Chrome, it typically applies to the system proxy settings. However, the MetaDefender Update Downloader relies on WinHTTP instead of WinINet, meaning it does not inherit the browser's proxy settings.

As a result, you may encounter the error: "No rows to show."



Solution

Since the MetaDefender Update Downloader currently does not provide a UI option to configure proxy settings, you need to set the WinHTTP proxy manually using the `netsh` command:

1. Open Command Prompt as Administrator:

- Press `Win + R`, type `cmd`, and press `Ctrl + Shift + Enter`.

2. Set the WinHTTP Proxy:

- Run the following command, replacing `<proxy_ip>:<port>` with your actual proxy details:

Code · html

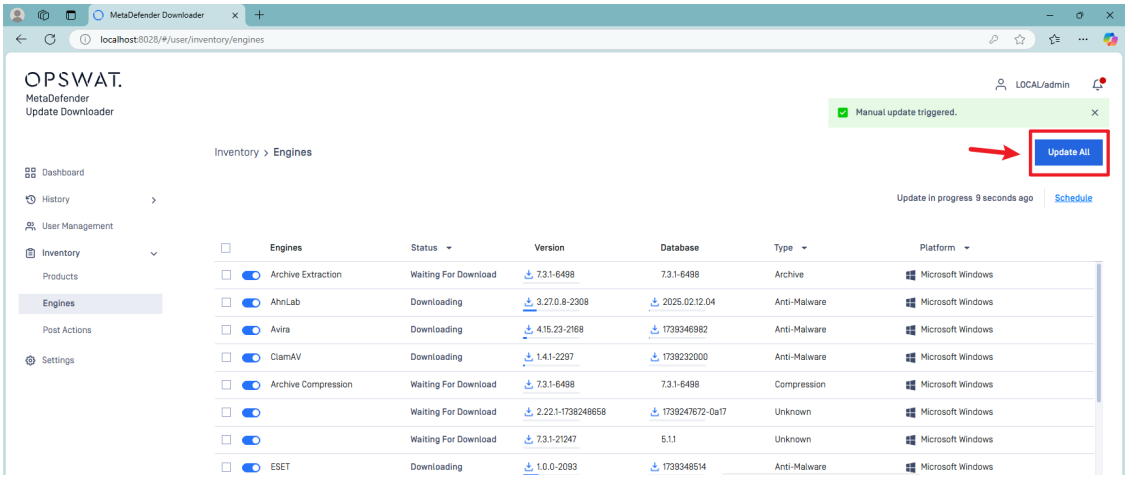
```
netsh winhttp set proxy <proxy_ip>:<port>
```

Example:

Code · html

```
netsh winhttp set proxy 192.168.1.100:8080
```

1. Refresh the Update Downloader web console and click "Update All."



1. Check if the page now displays correctly.

> **Support:**
>
> If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**

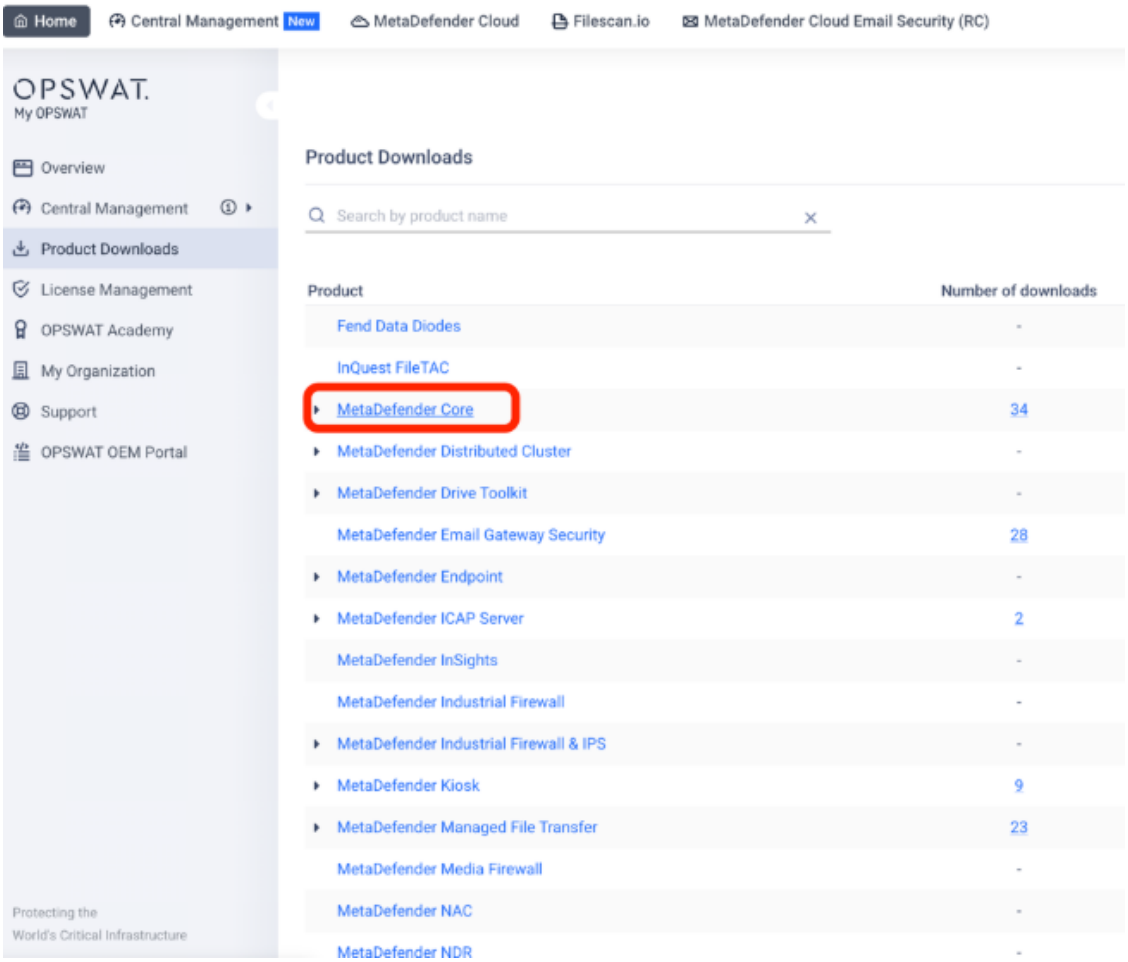
What is the latest MetaDefender Update Downloader version

> **Check Your Version:**
>
> This article applies to all MetaDefender Update Downloader releases deployed on Windows, MacOS and Linux systems.

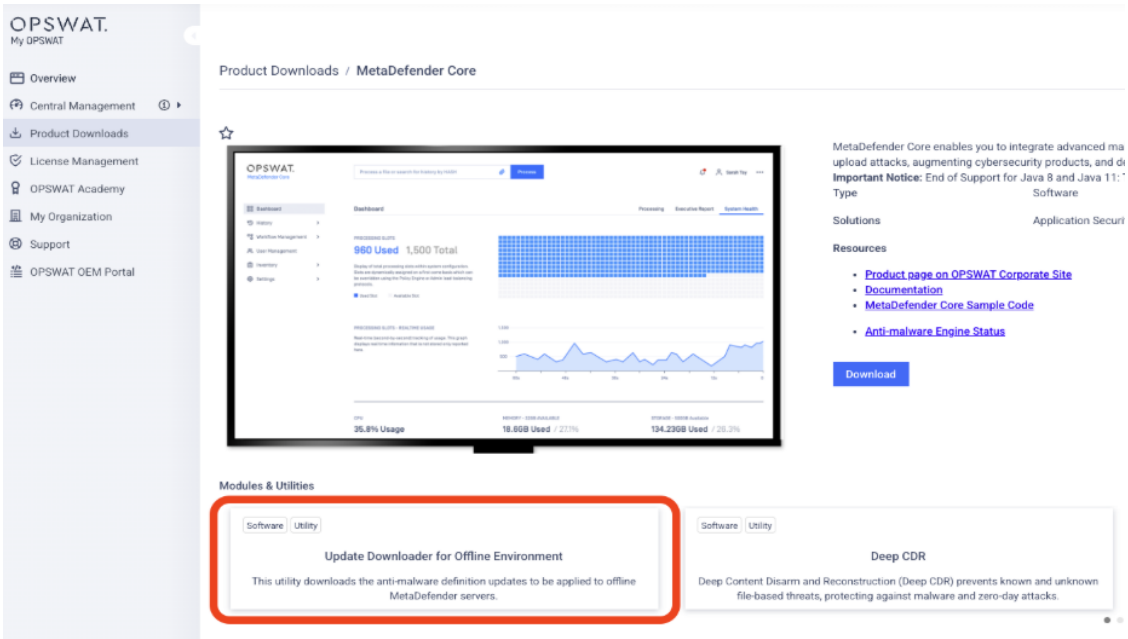
Browse MetaDefender Update Downloader Release Notes for details on the latest version, version history, version comparisons and release notes.

Alternatively, go directly through the My OPSWAT for a list of available downloads.:

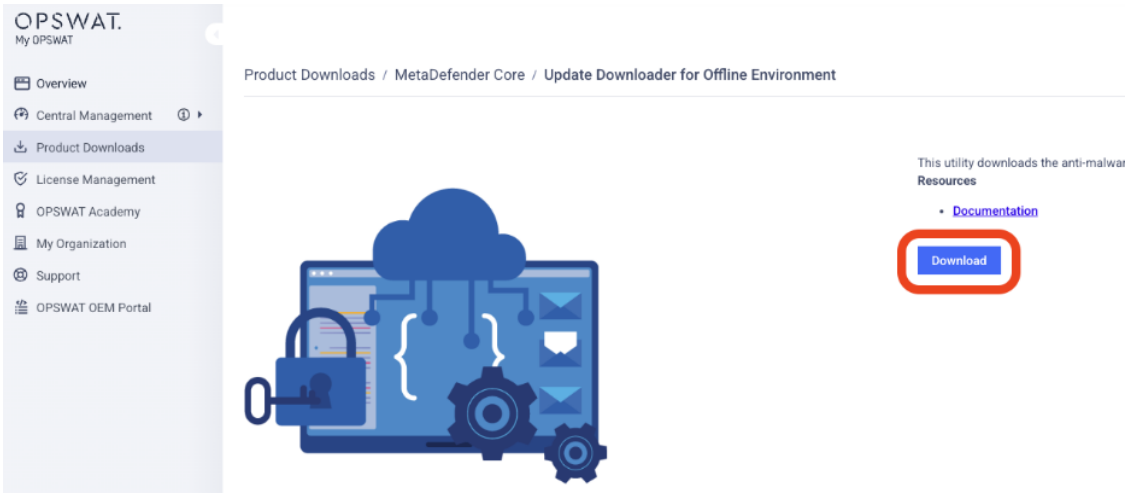
1. Login to My OPSWAT portal
2. Click on “MetaDefender Core”



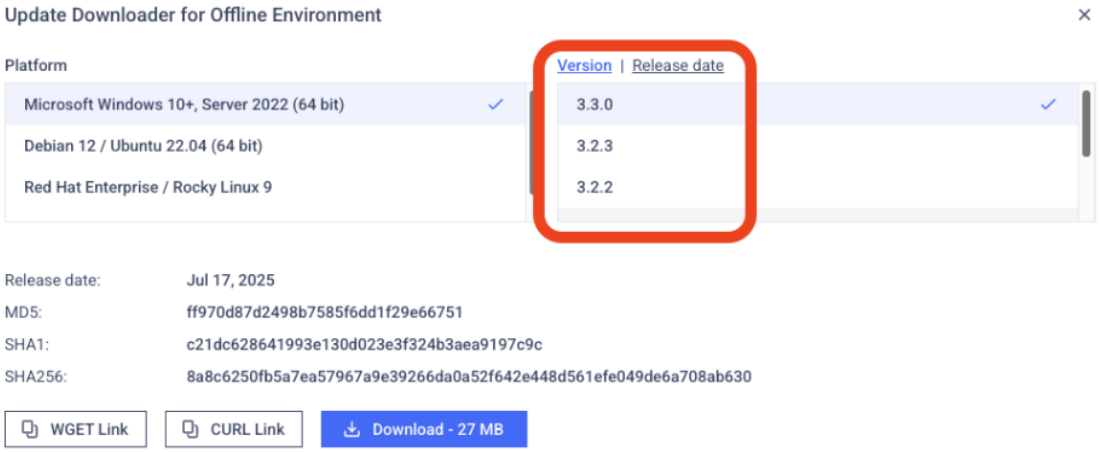
1. Click on section “Update Downloader for Offline Environment”



1. Click on “Download” button



1. In the new window opened, always the version from the top is the latest version



Pro Tip:

OPSWAT highly recommends that users upgrade to the latest version of MetaDefender Update Downloader. Current versions incorporate state-of-the-art features and necessary bug fixes, and are freely available for all license holders to download.

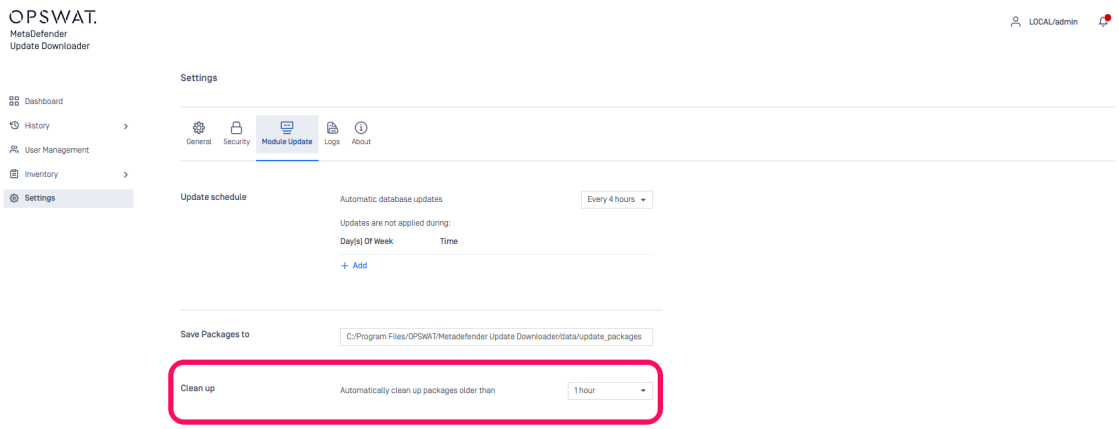
Support:

Feel free to contact OPSWAT support for further guidance through your Upgrade process. Please follow these instructions on How To Create a Support Package, before logging a Support Ticket with the OPSWAT team.

Does the “Clean Up” Function Remove Only Definition Files in the Module Update Folder?

Overview

This article explains how the **Clean up** function in **Settings > Module Update** behaves and whether it affects non-definition files stored in the same directory.



How the Clean Up Function Works

Cleanup applies **only** to official OPSWAT update packages downloaded by the Update Downloader.

Each update package includes a YML file with a timestamp embedded in its filename, for example:

`ds_3_windows-database-1553828845-1555551582691.yml`

The cleanup logic evaluates this timestamp. If the timestamp is older than the configured cleanup interval, the Update Downloader removes:

- The YML file
- The corresponding ZIP file for the same package

The process does **not** rely on Windows “Date Modified” or file creation dates, only the timestamp inside the filename.

Which Files Are Affected?

Files that may be deleted

Only **valid OPSWAT update packages** that follow the expected filename pattern containing a timestamp.

Files that will NOT be deleted

Any file that does **not** match the update package naming format, such as:

- `readme.txt`
- `custom_config.yml`
- `manual_backup.zip`
- `notes.docx`

Even if the file extension is `.yml` or `.zip`, it is ignored unless the filename resembles an OPSWAT update package

with an embedded timestamp.

Support:

If Further Assistance is required, please proceed to **create a support case or chat with our support engineer**.

Can I delete/modify the source engine folder of MetaDefender Update Downloader?

Check Your Version:

This article applies to **MetaDefender Update Downloader** deployment on **Windows** and **Linux** environment.

With Post Actions, this feature is only available since **Update Downloader version 2.5.0**.

Overview

This article addresses whether it is acceptable to configure an external transfer agent (such as a Data Diode) to delete files from the MetaDefender Update Downloader source directory immediately after transferring them to a secure zone.

Recommended Configuration

The recommended way is to **not remove files from the source folder.**

The MetaDefender Update Downloader relies on the presence of existing files to track for incremental updates. If these files are deleted externally:

- The Update Downloader cannot track the deletion, leading to potential conflicts.
- The system will be forced to perform a **full re-download** of the entire database during every cycle, causing significant bandwidth usage and operational delays.

Workaround

If your architecture requires the transfer agent to delete files after ingestion (common with **Data Diodes**), you should decouple the download process from the transfer process using **Post Actions**.

Instead of the Data Diode picking up files directly from the Download folder, configure the Update Downloader to copy the files to a secondary "Staging Folder" automatically.

Steps:

1. **Create a Seperated Folder:** Create a separate directory for the Data Diode to monitor.
2. **Configure Post Actions:** Use the MetaDefender Update Downloader **Post Actions** feature to trigger a script that copies the content from the Download folder to the Staging Folder.

3. **Configure Data Diode:** Point the Data Diode to the **Seperated Folder**. It can now safely ingest and delete files from this location without affecting the Update Downloader.

For detailed instructions on configuring this feature, please refer to our documentation:

- **Post Actions - MetaDefender Update Downloader**

Support:

If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

What are the installation directories for MetaDefender Update Downloader?

Check Your Version:

This article applies to all MetaDefender Update Downloader releases deployed on Windows and Linux systems.

Below lists the default installation directories for Windows and Linux

Windows

Location	Path
Registry	1. Computer\HKEY_LOCAL_MACH 2. Computer\HKEY_LOCAL_MACH 3. Computer\HKEY_LOCAL_MACH
File Explorer	1. C:\Program Files\OPSWAT\Met 2. C:\Program Files\OPSWAT\Met 3. C:\Program Files\OPSWAT\Met 4. C:\Program Files\OPSWAT\Met 5. C:\Program Files\OPSWAT\Met

Linux

Directory Path	Description
/etc/default/ometadownloader	Environment variables for proxy
/etc/init.d/ometadownloader	Script for ometadownloader service start
/etc/logrotate.d/ometadownloader	How often logs rotate for ometadownloader.log and nginx-ometadownloader.log
/etc/ometadownloader/ometadownloader.conf	Configuration file for rest port, and log directories
/usr/bin	Script for collecting support package: ometadownloader-collect-support-data.sh Script for watchdog: ometadownloader-watchdog.sh
/usr/lib/ometadownloader	Library files Directories: lib, resources, plugins [SQL database, drivers, TLS]
/usr/lib/systemd/system	Ometadownloader.service
/usr/sbin	Directories: ometadownloader, ometadownloader-strip-configdb, ometadownloader-upgrade-db
/usr/share/doc/ometadownloader/copyright	Copyright file
/usr/share/man/man1	Ometadownloader.1.gz
/usr/share/ometadownloader	Ometadownloader.conf - Global configuration for rest port and rest address. Log configuration on where to store log files
/var/lib/ometadownloader	Auditlog.sqlite, config.db.sqlite Directories: html, update_packages, updates. Where core engine update database and engine packages store locally.
/var/lib/ometadownloader/html	HTML, CSS for website funtionality
/var/log/ometadownloader	ometadownloader.log

Directory Path	Description
	Log file for troubleshooting

Support:

If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

MetaDefender Downloader Uninstallation Guide for Windows and Linux

Check Your Version:

This article applies to All version of Metadefender Downloader Windows and Linux version

Issue:

This article provides the commands and directory locations required to fully uninstall MetaDefender Downloader from Windows and Linux environments, including the removal of application files, configuration files, services, and residual data.

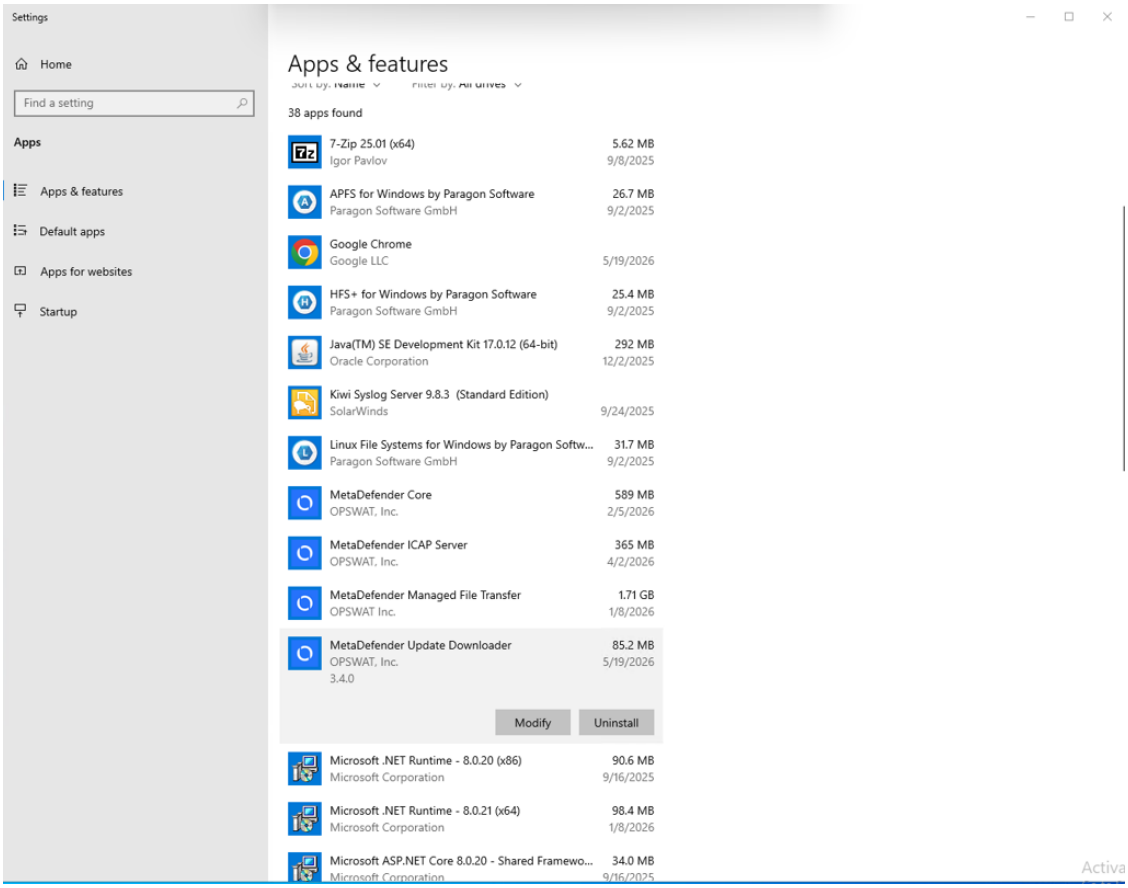
Solution:

To completely uninstall MetaDefender Downloader and ensure a clean removal of all application components by follow the instructions below:

Uninstall on a Window's Deployment:

1. Go to **Add or Remove Program** under the search menu

Find the **MetaDefender Update Downloader** and Press the Uninstall button to uninstall application.



1. Click the Uninstall button to uninstall the MetaDefender Downloader application.
2. To completely remove all MetaDefender Downloader related data, logs and configuration files, please deleted all the directories reference in this article: What are the installation directories for MetaDefender Update Downloader?

Uninstall Linux Environment:

The command line to uninstall the downloader is as follows:

1. Stop and Disabled MetaDefender Downloader Core services.

Code

```
sudo systemctl stop ometadownloader
sudo systemctl disable ometadownloader
```

1. For Debian-based Systems (Ubuntu, Debian):

Code

```
sudo apt-get remove --purge ometadownloader
```

For RPM-Based Systems (Rocky Linux, CentOS, RHEL):

Code

```
sudo dnf remove ometadownloader
```

1. To completely remove all MetaDefender Downloader related data, logs and configuration files, please deleted all the directories reference in this article: What are the installation directories for MetaDefender Update Downloader?

Support:

If **Further Assistance** is required, please proceed to log a support case or chatting with our support engineer.

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:

package · bash

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

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

Example:

package · bash

```
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:

```
package · bash

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

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

Example:

```
package · bash

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:

log format · bash

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

Example:

log example · bash

```
[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.

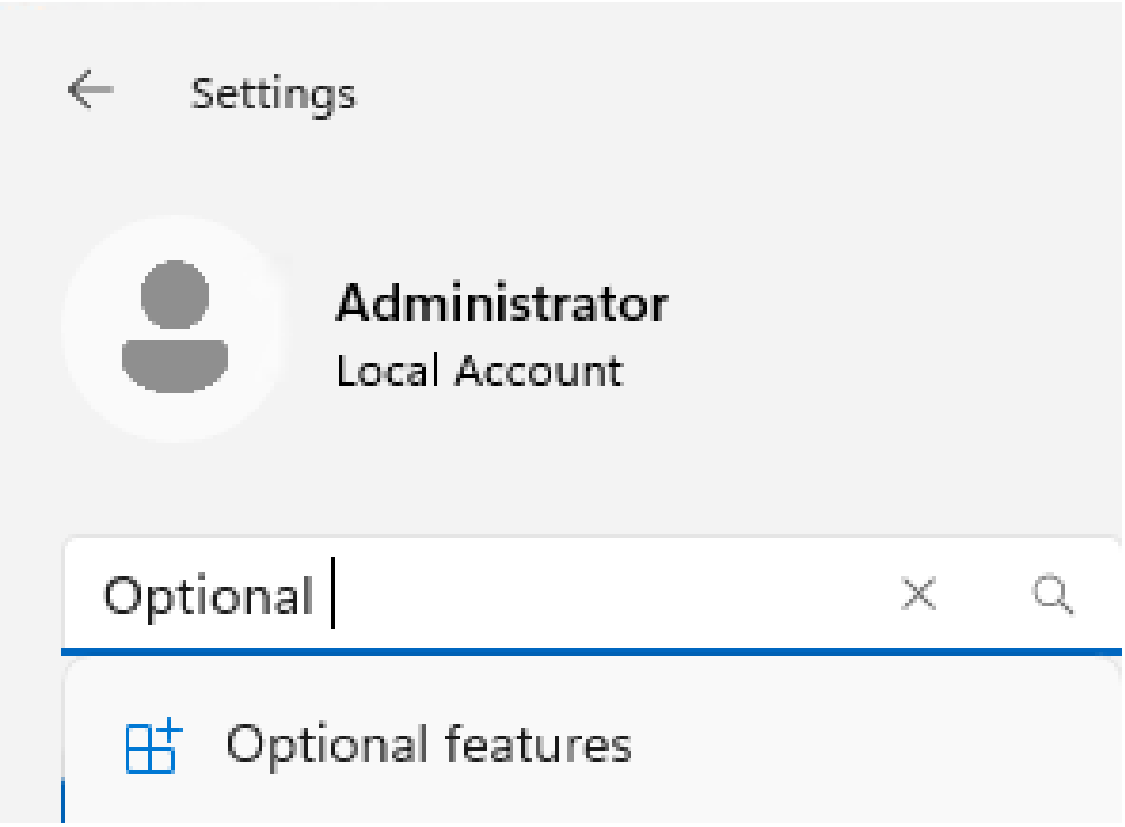
Solution

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.

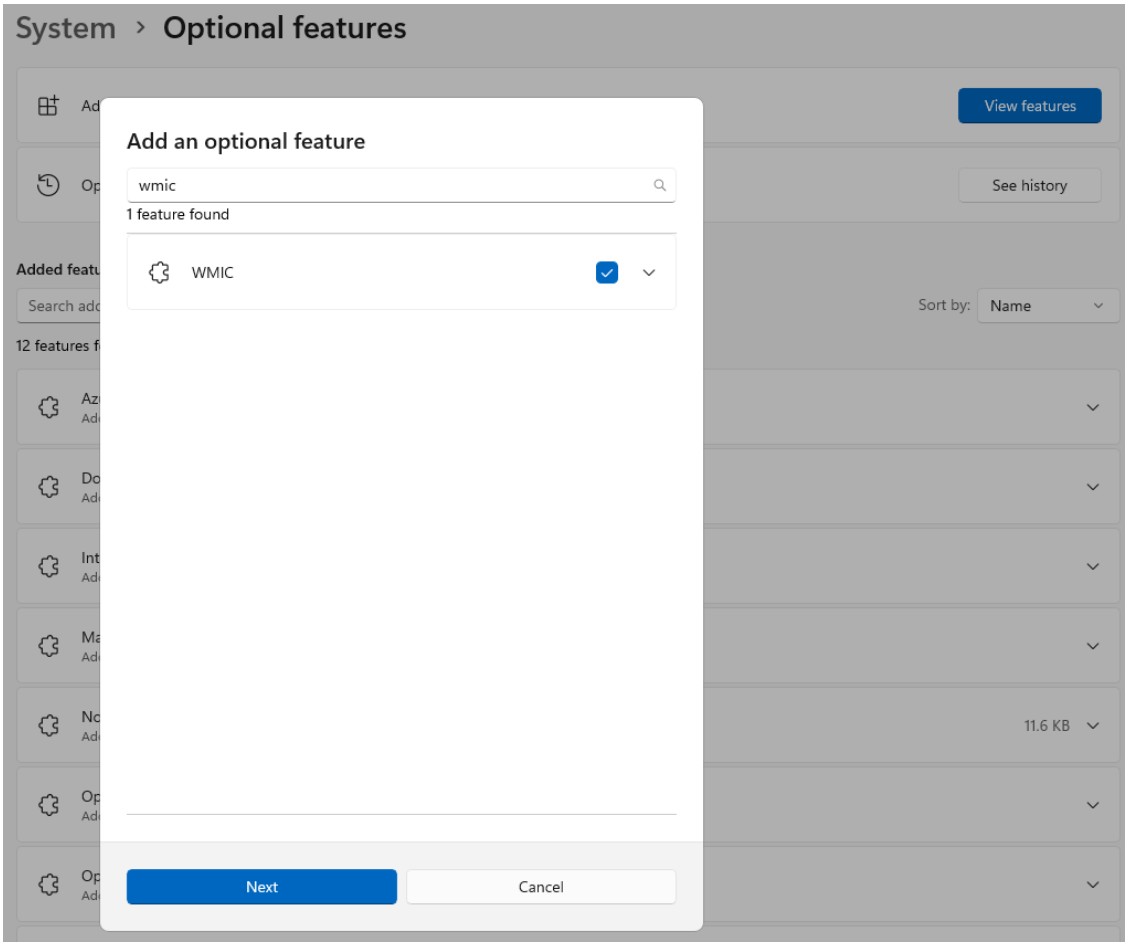
Install wmic in Windows Server 2025

In Windows, the tool for collecting the support package is rely on wmic, if you cannot run on Windows Server 2025 because of wmic, please install it following this steps

Go to Settings and search Optional features



In Optional features, search for WMIC and install it



Wait for the installation to be successful

Release Notes

Version 3.5.0

Release date: June 17, 2026

New features:

- Support for Export/Import configuration. Details: Export/Import Configuration
- Support for custom installation path, details: Installing Update Downloader using the Command Line

- Support Ubuntu 24.04 with CIS level 1 and level 2

Enhancements:

- Upgraded NGINX to v1.30.2
- Upgraded zlib to v1.3.2
- Upgraded OpenSSL to v3.5.6

Version 3.4.0

Release date: Mar 04, 2026

New features:

- New OS support: Ubuntu 24.04
- API key protection:
  - Strengthening security by protecting users' API key (if created) in the database using SHA256 hashing. Then actual API key value could not be retrieved back for good.
  - By default, this feature is not enabled for backward compatibility. Administrators need to opt-in by enabling that. Expecting to see the following UI notification poped up upon signed in:
  - ***Warning:*** *Once enabled, administrators cannot turn back the feature for security enforcement. Before switching on this feature, it's strongly recommended to backup your users' API key in a secured vault / secrets manager.*
  - When this feature is enabled, API key will be hashed out in the database, and no one, including administrators, will be able to see actual API key value anywhere in the product.
  - In case API key is lost or not remembered, then administrators must re-create a new one. The new one will be displayed for only one time on the UI.
- Unified User Interface and Experience of Login and Guest Scan Screens
- Support add license for new OPSWAT product: Standalone SANDBOX

Enhancements:

- Upgrade encryption from DES to AES-256-GCM
- Upgraded Qt to 6.8.1
- Upgraded OpenSSL to 3.5.5
- Upgraded 7zip to 26.0
- Upgraded NGINX to 1.29.5
- Upgraded Angular to 19.2.17
- Updated Terms of Service

Bug fix:

- Fix bug when session token show in the URL

- Some minor UI bugs.

Version 3.3.1

Release date: Nov 12, 2025

Enhancements:

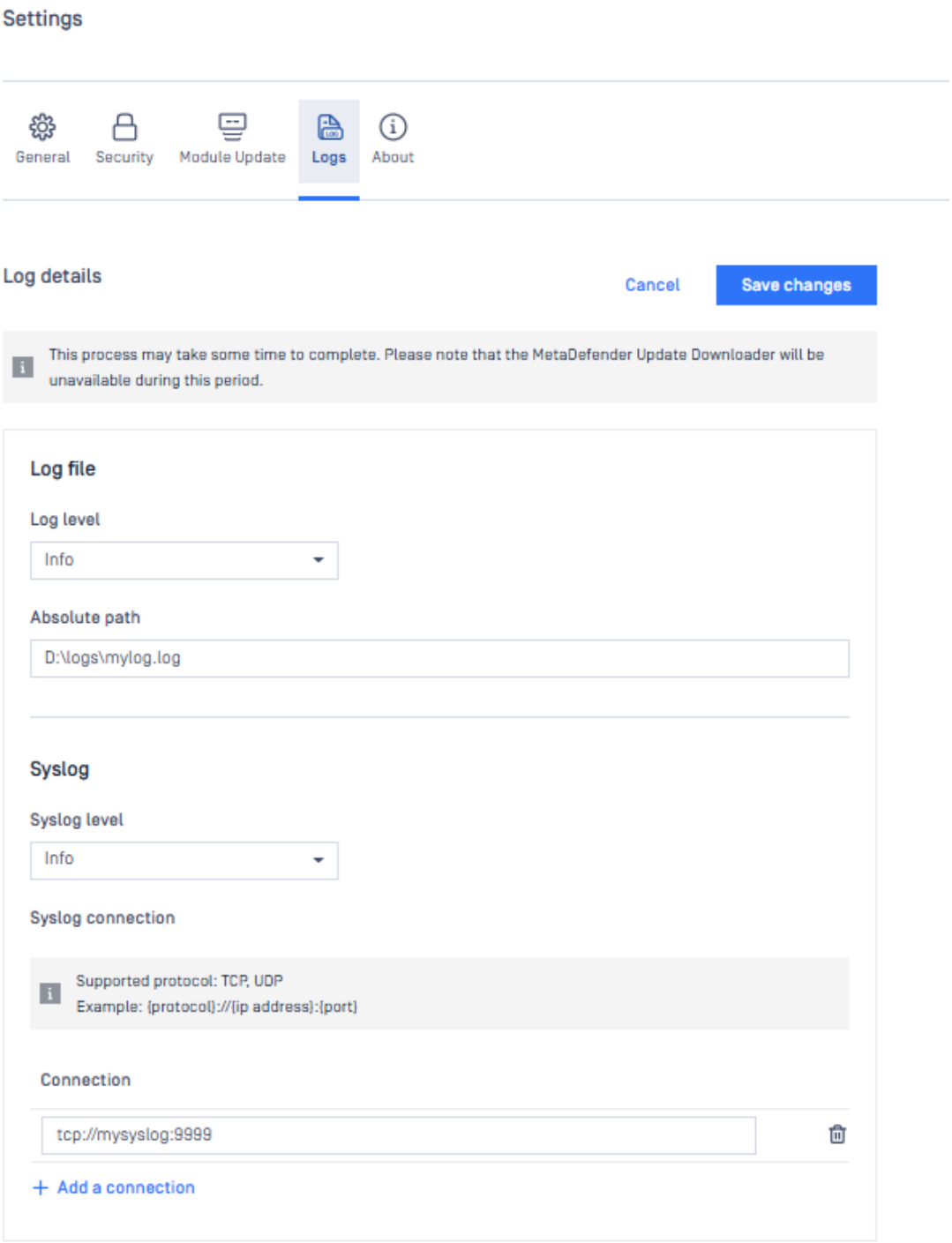
- Upgraded OpenSSL to 3.5.4
- Upgraded Protobuf to 32.1
- Upgraded NGINX to 1.28.0
- Upgraded Yaml-Cpp to 0.8.0
- Upgraded OpenLDAP to 2.6.10
- Upgraded 7zip to 25.01

Version 3.3.0

Release date: July 17, 2025

New features:

- New OS support: Windows Server 2025
- Support automation deployment via ignition file. More details at Automation Deployment.
- Support configure logging via web console.



Version 3.2.3

Release date: May 20, 2025

Enhancements:

- New API endpoint for health check which provides server disk space, updater connection status, product version. Document: Monitoring
- Introduce configurable settings for idle timeout and absolute session timeout.
- Unlicensed engines now can be removed on Engines screen.

- Updated EULA.

Version 3.2.2

Release date: April 10, 2025

Enhancements:

- Support offline licensing with On-prem License Management Server (OLMS).
- Introduce an ability to display a custom notice on signin screen.
- For vulnerability fixes:
  - Upgraded zlib to v1.3
  - Upgraded quazip to v1.4
  - Upgraded protobuf to v3.21.12
  - Upgraded openssl to v3.4.1

Version 3.2.1

Release date: February 06, 2025

Enhancements:

- Upgraded NGINX to v1.26.2 for vulnerability fixes.
- Upgraded OpenSSL to v3.4.0 for vulnerability fixes.
- Upgraded 7z to v24.09 for vulnerability fixes.

Bug fix:

- Addressed an issues that caused intermittent operation of Post Action.

Version 3.2.0

Release date: November 19, 2024

New features:

- Password policy enforcement
- New OS support: Rocky Linux 9

Bug fix:

- Addressed an issue that made the feature "Download All as ZIP" not work when engine version of embedded Sandbox engine was not visible yet.

Version 3.1.0

Release date: July 18, 2024

New features:

- New OS support:
  - Debian 12
  - Ubuntu 22.04
  - Windows 11
  - Windows Server 2022
- OS support retirement: Debian 9.x, Ubuntu 16.04, Microsoft Windows Server 2008 R2 or newer (64 bit)
- Updated Terms of Service.
- Introduce the ability to remove specific engines from the user interface.
- Supported new engine types: Adaptive Sandbox, Reputation, COO (Country of Origin), and SBOM (Software Bill of Materials).
- Introduced the ability to download individual packages. Users can now selectively download specific packages, allowing for a more targeted and efficient approach to package management.
- Users can now add descriptions to products, providing valuable context and information facilitating better organization and tracking of updates.

Bug fixes:

- Addressed the issue that only the engine part was disabled, while the database part remained enabled.
- Resolved an issue that installation folder was not removed entirely after uninstalling the product.

Version 3.0.0

Release date: February 17, 2023

New features:

- A brand-new user interface for the management console

Version 2.5.0

New features:

- Support post actions (to auto trigger script whenever engines and databases are ready)

Bug fixes:

- Fixed unable to download all as .zip big package
- Fixed issue when engine can't reach ready state for MetaDefender Core v3
- UI minor fixes

Version 2.4.1

Bug fixes:

- Fixed issues on update time rules
- Refined user guide

Version 2.4.0

New features:

- Support multiple OPSWAT MetaDefender products
- Enhance engine package verification before allowing download all as .zip

Version 2.3.0

New features:

- The available packages can be downloaded via web interface as one big ZIP file
- More informative dashboard

Version 2.2.1

New features:

- New-looking user interface

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

OPSWAT.