

OPSWAT.

MetaDefender

MetaDefender Core v4.13.2

Table of Contents

About This Guide	13
Key Features of Metadefender Core	14
1. Quick Start with Metadefender Core	15
1.1. Installation	15
Operating system invariant initial steps	15
Basic setup	16
1.1.1. Configuration wizard	16
1.2. License Activation	21
1.3. Scan Files with Metadefender Core	21
2. Installing or Upgrading Metadefender Core	22
2.1. Recommended System Requirements	22
System Requirements For Server	22
Browser Requirements for the Metadefender Core Management Console	24
2.2. Installing Metadefender	25
Installation	25
Installation notes	25
2.2.1. Installing Metadefender Core using command line	26
2.2.2. Installing Metadefender Core using the Install Wizard	27
2.3. Upgrading MetaDefender Core	27
Upgrading from MetaDefender Core 3.x	27
Upgrading from MetaDefender Core 4.x	28
2.4. Metadefender Core Licensing	28
2.4.1. Activating Metadefender Licenses	28
2.4.2. Checking Your Metadefender Core License	35
2.5. Performance and Load Estimation	36
What to know before reading the results: Some factors that affect performance	36
How test results are calculated	37

Test Reports	37
Performance Report - Multi-Scanning On Linux	37
Performance Report - Multi-Scanning On Windows	41
2.6. Special installation options	46
Use RAMDISK for the tempdirectory	46
3. Configuring Metadefender Core	50
3.1. Management Console	50
3.2. Metadefender Configuration	51
3.2.1. Startup Core Configuration	51
3.2.2. Startup Node Configuration	55
3.2.3 Nginx related configuration	58
3.3. User management	58
3.3.1. Users and groups	59
3.3.2. Roles	64
3.3.3. User directories	66
3.3.4. Active Directory attributes	74
3.3.5. Change user password	77
3.4. Update settings	78
Internet	79
Folder	80
Manual	80
3.5. Clean up scan database	81
Technology Note:	81
3.6. Policies configuration	81
3.6.1. How MetaDefender Core policies work	82
3.6.2. Workflow template configuration	82
3.6.3. Security zone configuration	95
3.6.4. Workflow rule configuration	95
3.6.5. Quarantine	100
3.7. Logging	100
3.7.1. Configuration	101
3.7.2. Debug logging	101
3.8 Security settings on web console	102
3.8.1 Enabling HTTPS	102

3.8.2 Session timeout	106
3.9. Configuring proxy settings	107
How can I set proxy server for the product	107
3.10. External Scanners And Post Actions	108
External Scanners	108
Post Actions	111
3.11. Yara rule sources	113
4. Scan files with Metadefender Core	115
Scan Files via REST API	115
Scan Files via Web Interface	116
Choose what to scan and how	116
Start scanning	116
Progress of scanning	116
5. Data Sanitization	118
6. Operating Metadefender Core	119
6.1. Dashboard	119
Overview page	119
Scan history	120
Quarantine	120
Update history	120
6.2. Inventory Management	121
Certificates	121
Nodes	124
Skip by hash	126
Technologies	128
6.3. Regular Maintenance	136
Checking for Upgrades	136
Checking Engines / Databases Health	136
6.4 Import/Export configuration	136
Export	137

Import	137
Note	137
7. Metadefender Core Developer Guide	138
How to Interact with Metadefender Core using REST	138
File scan process	138
7.1. MetaDefender API Code Samples	138
Activate License Online	139
Successful response	139
Error response	140
Cancel Batch	140
Cancel Scan Batch	140
Cancel File Scan	142
Cancel Scan File	142
Close Batch	143
Close Scan Batch	143
Download Batch Signed Result	144
Download Batch Signed Result	144
Download Sanitized Files	147
Download Sanitized Files Using Data Id	147
Error response	147
Fetching Available Scan Rules	148
Successful response	149
Error response	150
Fetching Engine/Database Versions	150
Successful response	150
Error response	151
Fetch Scan Result	152
Retrieving Scan Reports Using Data ID	152
Successful response	152
Successful response with archive detection	158
Response (not existing data_id)	160
Error response	160

Fetch Scan Result by File Hash	161
Retrieve Scan Results Using Hash	161
Request http header parameters	161
The retrieved result is always the most recent for the processed item, if rule is set then it will be the most recent - if exists - under the given rule.	161
Successful response	161
Successful response with archive detection	165
Response (not existing hash)	167
Error response	167
Get Current License Information	168
Successful response	168
Error response	169
Get Product Version	169
Successful response	170
Error response	170
Initiate Batch	171
Initiate Scan Batch	171
Login / Create a Session	172
Successful response	172
Error response	173
Logout / Destroy a Session	173
Successful response	174
Error response	174
Scan A File	174
Successful response	175
Error response	175
Scan file in batch	176
Scan file in batch	176
Status of Batch	177
Status of Scan Batch	177
Uploading License Key File	178
Successful response	179
Error response	179
Vulnerability Info In Scan Result	180
Example	180

8. Advanced Metadefender Deployment	184
8.1. Scripted license management	184
Requirements	184
Activation steps	184
Deactivation steps	186
Important notes	187
8.2. Multi-node deployment	187
Setting up several Metadefender Core nodes	187
8.3. Using external load-balancer	190
8.3.1. HTTP(S) - Layer 7 load balancing	191
8.3.2. DNS load balancing	193
8.4. Cloud Deployment	196
8.4.1. AWS Deployment	196
9. Troubleshooting Metadefender Core	217
Installation issues	217
Issues with nodes	217
Where are the Metadefender Core logs located?	217
How can I create a support package?	217
Issues under high load	217
How to Create Support Package?	218
Creating the package on Linux	218
Creating the package on Windows	218
Content of the created package	219
How to Read the Metadefender Core Log?	219
Files	219
Format	219
Severity levels of log entries	220
Inaccessible Management Console	220
How to detect	220
Solution	220

Possible Issues on Nodes	221
Q. Node detected 3rd party product on system	221
Q. There is no scan node connected	221
Too Many Sockets or Files Open	222
How to detect	222
Solution	222
Too Many TIME_WAIT Socket	223
How to detect	223
Solution	223
Technical Insights	224
10. Release notes	225
Version v4.13.2	225
Version v4.13.1	225
Version v4.13.0	225
Version v4.12.2	226
Version v4.12.1	226
Version v4.12.0	226
Version v4.11.3	227
Version v4.11.2	227
Version v4.11.1	228
Version v4.11.0	228
Version v4.10.2	228
Version v4.10.1	229
Version v4.10.0	229
Version 4.9.1	230
Version 4.9.0	230
Version 4.8.2	231
Version 4.8.1	231

Version 4.7.2	233
Version 4.7.1	233
Version 4.6.3	234
Version 4.6.2	234
Version 4.6.1	234
Version 4.6.0	235
Version 4.5.1	236
Version 4.5.0	236
Version 4.4.1	237
Version 4.3.0	237
Version 4.2.0	238
Version 4.1.0	239
Version 4.0.1	239
Version 4.0.0	240

11. Metadefender / Client	241
About This Guide	241
Key Features of MetaDefender Client	241
Supported Operating Systems	241
1. MetaDefender Client Packages	242
MetaDefender Free Client	242
MetaDefender Premium Client	242
2. MetaDefender Premium Client	243
2.1 Install using the Install Wizard	243
2.2 Install using the Command Line	245
2.3 Using the MetaDefender Premium Client	246
2.4 Configuring through the config file	261
2.5 Configuring through Central Management	268
3. MetaDefender Free Client	273

4. Command Line Interface	273
Example:	273
Command Line Options	273
4.1 Generating and using the Administrator Password	277
5. MetaDefender Client Release Notes	279
Tips and Known Issues	279
5.1. Archived MetaDefender Client Release Notes	281
12. Legal	294
Copyright	294
DISCLAIMER OF WARRANTY	294
COPYRIGHT NOTICE	294
Export Classification EAR99	294
13. Knowledge Base Articles	295
Are MetaDefender Core v4 upgrades free?	296
Are there any dependencies that need to be fulfilled for MetaDefender Core v4 engines ?	296
Does Metadefender Core v4 offer real-time antivirus protection on the system where it is installed?	297
Does MetaDefender Core v4 Detect the NotPetya Ransomware?	297
Does the fixing updates for Meltdown and Spectre vulnerabilities affect any engines in MetaDefender Core v4?	300
External scanners in MetaDefender core v4.8.0 and above	301
How can I configure the maximum queue size in MetaDefender Core v4 ?	303
How can I find a sanitized file scanned with MetaDefender Core v4?	304
How can I increase the scaling up performance?	305
How can I upgrade from Core v4.7.0/v4.7.1 to a newer Core v4.7 release	307
How can the TEMP folder be changed?	308
How do I collect verbose debug packages on MetaDefender Core v4 for Linux?	309
How do I deploy MetaDefender Core v4 to an offline Linux environment?	310

Installing MetaDefender Core	310
Activate your license	311
Installing the MetaDefender Update Downloader utility	312
Applying offline updates	314
Contacting OPSWAT Support	315
How do I deploy MetaDefender Core v4 to an offline Windows environment?	315
Installing MetaDefender Core	316
Activate your license	316
Installing the MetaDefender Update Downloader utility	317
Applying offline updates	319
Contacting OPSWAT Support	320
How do I disable real-time protection of my anti-malware software if it is not allowed by corporate policy for use with MetaDefender Core v4?	320
How do I remove an engine from my MetaDefender v4 instance?	322
How do I use MetaDefender Core v4 Workflows ?	322
Defining and administering Workflow Templates in MetaDefender Core v4	323
How long is the support life cycle for a specific version/release of MetaDefender Core v4?	324
Is action needed because Metadefender v4's AVG license is expiring on 2018-06-15?	326
What do I need to do?	326
What if I don't take action by June 15, 2018?	327
Why is the license for AVG expiring?	327
What if I need more assistance from OPSWAT on this topic?	327
Is there a virus test I could use to test MetaDefender Core v4?	327
MetaDefender Core v4 shows a large number of files that failed to scan. What can I do?	328
Post actions in MetaDefender core V4.8.0 and above	329
Using MetaDefender core V4 BLACKLIST/WHITELIST feature	331
Using filetype groups VS. MIME-types VS file extensions	331
Using Regular Expressions	331
Advanced usage	331
What are Security Policies and how do I use them?	332
Understanding Security Policies	332
What features of MetaDefender Core version 3 are available in version 4 ?	334
What file types are supported by DLP engine?	337
What is Data Loss Prevention (DLP)?	337

Meta Data Check (Only):	338
File Conversion and Parse:	338
What file types can be verified by MetaDefender v4?	340
What links, target-services or target host-IP's need to be allowed for MetaDefender Core v4? 588	
What operating system patches should be applied to the system hosting MetaDefender Core? 588	
What should I do if an engine is in "failed" or "permanently_failed" status?	589
Where can I submit false positives detected by MetaDefender Core v4?	589
Which are the supported archive formats for MetaDefender Core v4?	592
Why don't I see the Data Sanitization engine in MetaDefender Core v4?	593
Why should I upgrade my MetaDefender Core v4?	594

About This Guide

Welcome to the Metadefender v4 guide. This guide is intended to provide the information you need to:

- Install, configure, and manage Metadefender Core v4.x. If you are using Metadefender Core v3.x, refer to [Metadefender Core v3.x user guide](#).
- Learn about new features, updated features, and bug fixes on each Metadefender Release (i.e. each product version's release notes)
- Learn about frequently asked questions and additional concepts through our library of knowledge base articles

While we offer the option to download this guide to a PDF file, it is optimized for online browser viewing. OPSWAT updates the online version of the guide regularly on an "as needed" basis. By viewing the document online, you are assured that you are always seeing the most recent and most comprehensive version of the guide.

Key Features of Metadefender Core

- File sanitization (aka Content Disarm and Reconstruction) using [90 data sanitization engines](#)
- Multi-scanning for malware with more than [30 leading anti-malware engines](#)
- [Heuristic](#) analysis to detect more unknown and targeted attacks
- Vulnerability Engines
- File Type Verification
- Archive Extraction
- Workflow Engine (simple or advanced)
- High performance processing

1. Quick Start with Metadefender Core

This guide describes the basic steps for installing and scanning files with Metadefender Core:

- [1.1. Installation](#)
- [1.2. License Activation](#)
- [1.3. Scan Files with Metadefender Core](#)

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

1.1. Installation

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

Operating system invariant initial steps

1. Download the *OPSWAT Central Management* package from the [OPSWAT Portal](#). Make sure that you download the applicable package for your operating system (and distribution).
2. Upload the installation package to your server computer.
3. Follow the installation steps according to your operating system (and distribution).

Installing Metadefender on Ubuntu or Debian computers

1. Download ometascan package from the OPSWAT Portal. Make sure that you download the applicable package for your distribution.
2. Upload the installation package to your test computers
3. Install the product with `sudo dpkg -i <filename>`, where filename is the Metadefender Core package you downloaded from our portal
4. If dpkg shows error messages about missing dependencies you should execute `sudo apt-get install -f`

Installing Metadefender on Red Hat Enterprise Linux or CentOS computers

1. Download ometascan package from the OPSWAT Portal. Make sure that you download the applicable package for your distribution.
2. Upload the installation package to your test computers

3. Install the product with `sudo yum install <filename>`, where filename is the Metadefender Core package you downloaded from our portal

Installing Metadefender on Windows computers

1. Download ometascan installer from the OPSWAT Portal. Make sure that you download the applicable package for your distribution.
2. Upload the installation package to your test computers
3. Install the product with running the downloaded `<filename>.msi`, where filename is the Metadefender Core installer you downloaded from our portal

Basic setup

1. Open a web browser and point to `http://<server name or IP>:<port>`
 - Default port is **8008**
 - In case of problem check [Inaccessible Management Console](#) page
2. The [basic configuration wizard](#) will guide you through the rest of the basic setup.

For more information on Installation procedures see [Installing Metadefender](#)

1.1.1. Configuration wizard

- [Introduction](#)
- [Basic configuration steps](#)
 - [End-User License Agreement](#)
 - [Admin User Setup](#)
 - [License activation](#)
 - [Wizard completion](#)
- [Transport Layer Security](#)
- [User directories](#)

Introduction

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

WARNING!

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

To start the wizard click CONTINUE.

⚠ Sensitive information

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

Basic configuration steps

End-User License Agreement

End-User License Agreement

venue in, and the exclusive jurisdiction of, the federal and state courts, as applicable, located in San Francisco, California (except that a party may enforce a judgment in any court of competent jurisdiction).

Attribution and Additional Rights
The Server You licensed may include files or data from OPSWAT's suppliers which grant You additional rights specific to the files suppliers provide OPSWAT, when used separately from the Server. Attribution of such suppliers and material terms of additional rights available to You may be found at https://onlinehelp.opswat.com/eula/3rd_Party_EULA.html.
OPSWAT, the OPSWAT logo, Metadefender and Metascan are trademarks or registered trademarks of OPSWAT, Inc. Trademarks not owned by OPSWAT are owned by their respective owners.
(C) 2002-2018 OPSWAT Inc. All rights reserved

I ACCEPT THE TERMS IN THE LICENSE AGREEMENT

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


Admin User Setup

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

User directory

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

The following information is required for the administrator account:

ACCOUNT NAME	The unique name of the account that is used at the time of login and in log messages for accountability.
ACCOUNT DISPLAY NAME	Name of the person bound to this account. This name (appended to the name of the account's user directory) is displayed in the top right corner of the Web Management Console.
PASSWORD	Password of the user bound to this account that is used at the time of login. <div data-bbox="408 1189 1428 1749" style="border: 1px solid red; padding: 10px;"><p> Passwords sent clear-text</p><p>As long as TLS is not configured for the basic configuration wizard, passwords are sent clear-text over the network and may be disclosed to unauthorized parties.</p><p>As a mitigation action:</p><ol style="list-style-type: none">1. Either use the wizard on <i>localhost</i> or on a direct network connection, or2. Enable TLS as soon as possible and change the password immediately if it has already been set.</div>
EMAIL	Email address of the person bound to this account.

Admin User Setup

ACCOUNT NAME

ACCOUNT DISPLAY NAME

PASSWORD

RETYPE PASSWORD

EMAIL

License activation

For license activation details see [2.4.1. Activating MetaDefender licenses](#).

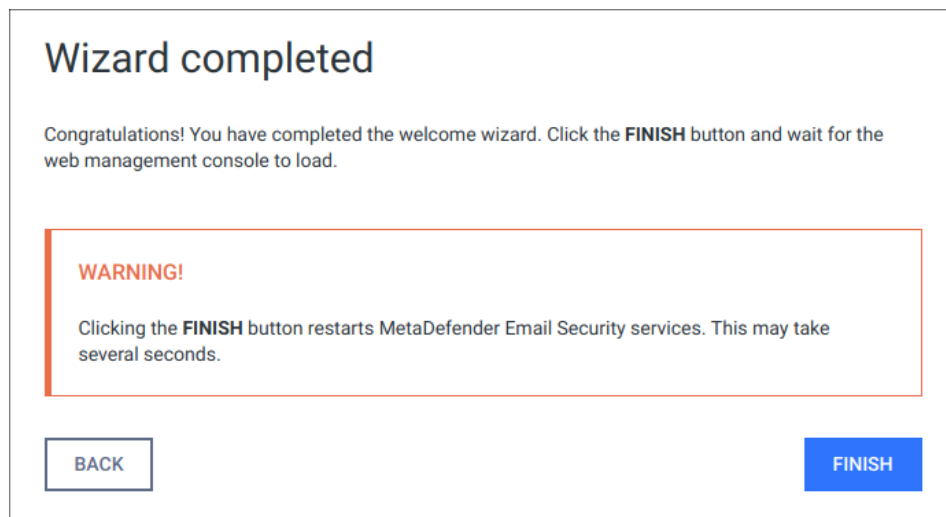
Wizard completion

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



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

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




Transport Layer Security

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

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

No TLS for the wizard

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

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

For instructions to set up TLS see [3.8.1 Enabling HTTPS](#).

User directories

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

For further details about user directories see [3.3.3. User directories](#).

1.2. License Activation

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

Press the *ACTIVATE* button to bring up the Activation menu, where you should choose from the available modes:

- Online: the product will contact the OPSWAT license server online, and acquire its license based on your Activation key and Deployment ID.
- Offline: you can upload a manually acquired license file.
- Request trial key online: if you want to try out the product first, you can receive a trial Activation key via email.

If you selected the `Request trial key online` option then follow the on-screen instructions.

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

When scan engines are installed you can start using the installed Metadefender Core to scan files with multiple anti-malware engines.

For more information on how to scan files with Metadefender Core see [Scan Files with Metadefender Core](#)

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

1.3. Scan Files with Metadefender Core

There are several ways to scan files with Metadefender Core:

- [Scan Files via Web Interface](#)
- [Scan Files via REST API](#)

2. Installing or Upgrading Metadefender Core

This part of the guide describes in detail the installation and upgrade process of Metadefender Core

- [2.1. Recommended System Requirements](#)
- [2.2. Installing Metadefender](#)
- [2.3. Upgrading MetaDefender Core](#)
- [2.4. Metadefender Core Licensing](#)
- [2.5. Performance and Load Estimation](#)
- [2.6. Special installation options](#)

2.1. Recommended System Requirements

Before installing Metadefender Core v4, please refer to recommended system requirements listed below.

System Requirements For Server

- Operating System (Only 64-bit platforms are supported):
 - CentOS 6.6+, 7.0+
 - Red Hat Enterprise Linux 6.6+, 7.0+
 - Debian 7.0+,
 - Ubuntu 14.04, 16.04
 - Windows 7, 8, 8.1, 10
 - Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016



Please note that there are custom engines that might have different needs. Please refer to knowledge base!

The following amount of resources (CPU, RAM, disk space) are recommended for Metadefender Core v4 on **Linux**:

Package	CPU cores	Free System RAM	Free Hard Drive Space
Metadefender Core 1	2	2 GB	2 GB + 1.5 GB / one million of scan data
Metadefender Core 5	4	4 GB	10 GB + 1.5 GB / one million of scan data
Metadefender Core 10	8	8 GB	20 GB + 1.5 GB / one million of scan data

The following amount of resources (CPU, RAM, disk space) are recommended for Metadefender Core v4 on **Windows**:

Package	CPU cores	Free System RAM	Free Hard Drive Space
Metadefender Core 1	2	4 GB	2 GB + 1.5 GB / one million of scan data
Metadefender Core 4	4	8 GB	8 GB + 1.5 GB / one million of scan data
Metadefender Core 8	8	8 GB	16 GB + 1.5 GB / one million of scan data
Metadefender Core 12	16	16 GB	24 GB + 1.5 GB / one million of scan data
Metadefender Core 16	16	16 GB	32 GB + 1.5 GB / one million of scan data
Metadefender Core 20	32	16 GB	40 GB + 1.5 GB / one million of scan data

For Metadefender Core Node, the following resources are recommended on **Linux**:

Package	CPU cores	Free System RAM	Free Hard Drive Space
Metadefender Core 1	2	2 GB	2 GB
Metadefender Core 5	4	4 GB	10 GB
Metadefender Core 10	8	8 GB	20 GB

For Metadefender Core Node, the following resources are recommended on **Windows**:

Package	CPU cores	Free System RAM	Free Hard Drive Space
Metadefender Core 1	2	4 GB	2 GB
Metadefender Core 4	4	8 GB	8 GB
Metadefender Core 8	8	8 GB	16 GB
Metadefender Core 12	16	16 GB	24 GB
Metadefender Core 16	16	16 GB	32 GB
Metadefender Core 20	32	16 GB	40 GB

Metadefender Core on Linux uses /var folder for storing resources.

Metadefender Core on Windows uses C:\Program Files\OPSWAT folder for storing resources or the installation directory.

It is suggested to use SSD for the Core and Node products.

Browser Requirements for the Metadefender Core Management Console

One of the following browsers is suggested to view the Metadefender Core Management Console:

- Internet Explorer 11
- Microsoft Edge
- Chrome
- Firefox
- Safari

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

2.2. Installing Metadefender

Installation

1. Download the package of your choice from the [OPSWAT portal](#)
2. Install the package on your computer via the [Command Line](#) or via the [Install Wizard](#)
3. Open a web browser and point to `http://<server name or IP>:<port>`
 - Default port is **8008**
 - In case of problem check [Inaccessible Management Console](#) page
4. Complete the required steps of the [basic configuration wizard](#)
5. You must [activate](#) this deployment to use its features

Installation notes

- If the Metadefender 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.
- Metadefender installer already contains the Node part of the system. In a single computer deployment you don't need to separately install the Metadefender Node on your computer. To install additional instances, please see [Multi-node deployment](#) page.
- During installation the databases might need to be upgraded. This could take noticeable time depending on database size (eg.: length of scan history).
- If Metadefender Kiosk is installed on the host where Metadefender v4 is to be installed on, then be aware the default port (8009) used by Metadefender Kiosk and Metadefender (before version v4.9.0) for accepting external node connections is the same.

2.2.1. Installing Metadefender Core using command line

Preliminary notes

- If the Metadefender Core package dependencies are not installed on your system you may need to have a working Internet connection or you may have to provide the Installation media during the installation. Consult your Operating System documentation on how to use Installation media as a package repository.

Debian package (.deb)

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

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

```
sudo yum install <filename>
```

Windows package (.msi)

On Windows systems it is possible to install the product by running the corresponding .msi file.

From command line interface it is also possible to install the product by executing

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

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

Key	Default Value	Description
RESTADDRESS	*	REST interface binding IPv4 or IPv6 address ('*' means that service listens on all IPv4 and IPv6 interfaces)
RESTPORT	8008	REST interface binding port
ADDRESS	-	

Key	Default Value	Description
		Address of the computer to accept external scan node connections
PORT	-	Designated port number to accept external scan node connections
REPORT_ENGINE_ISSUE	true	Enable reporting of engine issue count. (possible values: "true" or "false").

Reporting of engine issue count

If reporting of engine issue count is enabled, Metadefender Core v4 server will send only the **number** of initialization errors and **number** of unexpected stops for the specific db /engine version. This information is sent over a HTTPS channel when the product downloads the latest package descriptors. This information is used for early detection of any specific 3rd party engine quality issues.

For details on using msiexec please consult [Windows installer documentation](#).

2.2.2. Installing Metadefender Core using the Install Wizard

The Install Wizard is only for the Windows installer (.msi file).

To install Metadefender Core run the installer and follow the instructions.

2.3. Upgrading MetaDefender Core

Upgrading from MetaDefender Core 3.x

To upgrade from MetaDefender Core 3.x a separate license is necessary.

Your configuration cannot be migrated to the new version. Read through the [configuration](#) section for your possibilities.

The two versions have different feature sets. It is advisable to check the differences and your requirements before upgrading.

If you decide to upgrade to MetaDefender Core 4.x, you will need a separate [installation](#). Note that no database migration tool exists yet.

Upgrading from MetaDefender Core 4.x

To upgrade from a former version of MetaDefender Core 4.x a simple [installation](#) of the latest version is enough.

All existing MetaDefender Core configuration and data will be kept during the upgrade.

Downgrading your MetaDefender Core 4.x is not supported.



Please note that only those default [workflow templates](#) will be upgraded on MetaDefender Core v4 upgrade that have been not edited via workflow editor.

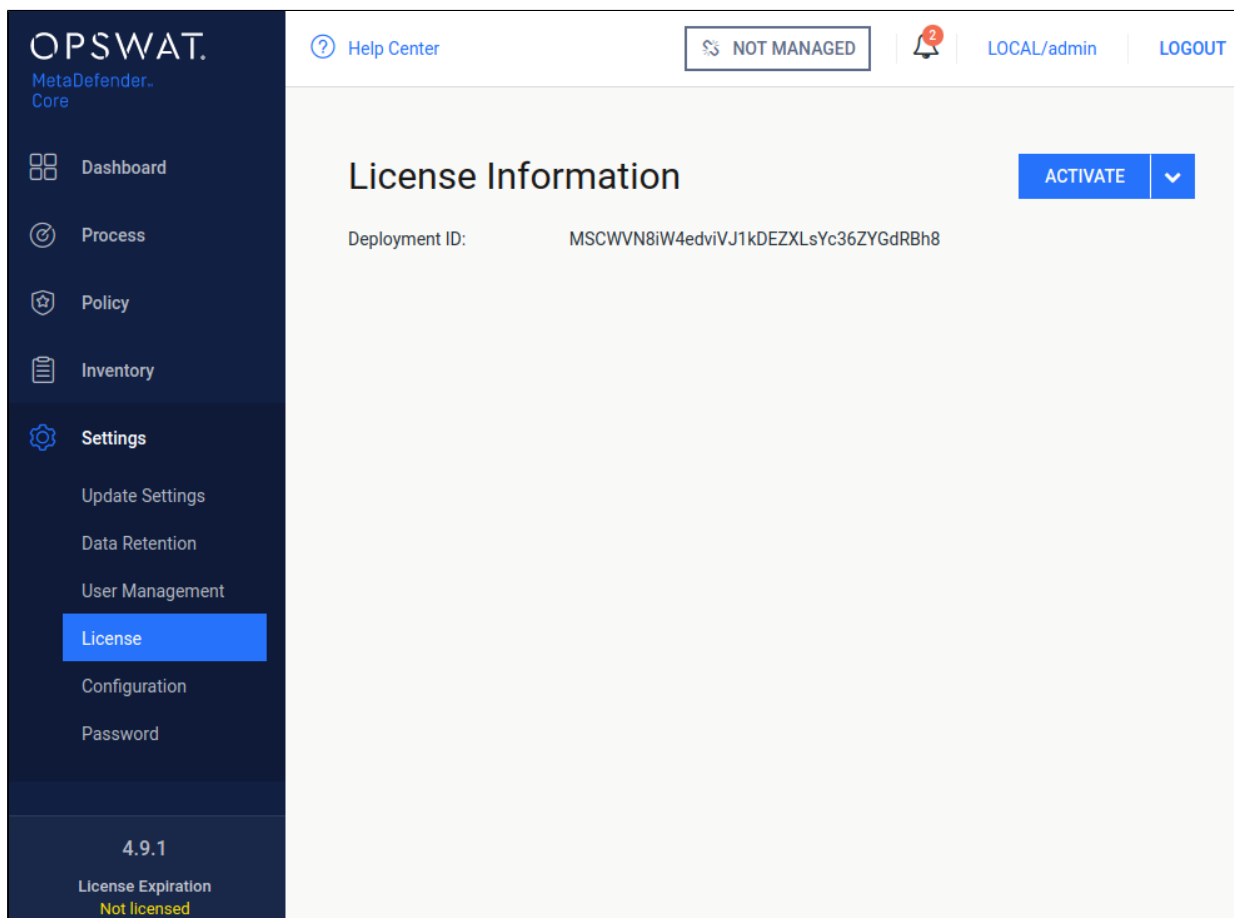
2.4. Metadefender Core Licensing

In order to use Metadefender Core you need to activate the product. If you don't have an activation key you can request a 14 day evaluation key during the activation process.

- [2.4.1. Activating Metadefender Licenses](#)
- [2.4.2. Checking Your Metadefender Core License](#)

2.4.1. Activating Metadefender Licenses

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



Settings/License page, when no valid license exists

Press the *ACTIVATE* button to bring up the Activation menu, where you should choose from the available modes:

- Online: the product will contact the OPSWAT license server online, and acquire its license based on your Activation key and its Deployment ID.
- Offline: you can upload a manually acquired license file. Follow the displayed instructions.
- Request trial key online: if you want to try out the product first, you can receive an trial Activation key via email. Follow the displayed instructions.

Activation

ACTIVATION MODE

ONLINE OFFLINE REQUEST TRIAL KEY ONLINE

ACTIVATION KEY

Activation key

REQUESTED NUMBER OF SCAN NODES

SINGLE-NODE DEPLOYMENT

MULTI-NODE DEPLOYMENT (SPECIFY COUNT OF NODE INSTANCES BEHIND THIS CORE SERVER)

Max node

DESCRIBE THIS DEPLOYMENT (OPTIONAL)

This helps you to identify this host on OPSWAT License Portal

SEND CANCEL

Not licensed

Settings/License/ACTIVATE page

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

Offline activation

With no internet connection on the server the Metadefender v4 instance may be activated indirectly from a different machine, that has internet connection. The Deployment ID of the Metadefender v4 instance and the the Activation key received at the time of purchasing the

product will be required. Follow the steps on the screen to activate the product offline.

Activation

ACTIVATION MODE

ONLINE OFFLINE REQUEST TRIAL KEY ONLINE

Offline activation steps:

1. Copy down your Deployment ID: **MSCWVN8iW4edviVJ1kDEZXLsYc36ZYGdRBh8**
2. Go to OPSWAT portal: <https://portal.opswat.com/activation>
3. Activate and download your license file (you will need your Activation key and the Deployment ID of this instance)
4. Upload the license file here
5. Check license details in the license menu
6. Tell your friends, enemies and competitors how much you enjoy using MetaDefender Core

ACTIVATION FILE

Offline activation details

1. Log on to <https://portal.opswat.com/activation>

Fill in the requested information about your deployment

Metadefender Offline Activation

Metadefender Package

Metadefender Core v4.x - all packages ▼

Activation Key *

879c 7a08 e6b5 6c2b 4285 c285 4287 889a

Requested Number of Nodes *

1

Deployment ID *

MSCWVN8iW4edviVJ1kDEZXLsYc36ZYGdRBh8

Optional Description

This helps you to identify this deployment on OPSWAT License portal

Request Unlock Key

Activation page on OPSWAT portal

1. Click the *Request unlock key* button. The download section appears. Click the *Download* button and save the activation file.
2. Go back to Metadefender Web Management Console. Browse for the activation file and click the *SEND* button.

Activation

ACTIVATION MODE

ONLINE OFFLINE REQUEST TRIAL KEY ONLINE

Offline activation steps:

1. Copy down your Deployment ID: **MSCWVN8iW4edviVJ1kDEZXLsYc36ZYGdRBh8**
2. Go to OPSWAT portal: <https://portal.opswat.com/activation>
3. Activate and download your license file (you will need your Activation key and the Deployment ID of this instance)
4. Upload the license file here
5. Check license details in the license menu
6. Tell your friends, enemies and competitors how much you enjoy using MetaDefender Core

ACTIVATION FILE

MSCWVN8iW4edviVJ1kDEZXLsYc36ZYGdRBh8.yml SELECT A FILE

SEND CANCEL

Request trial key online

An evaluation license may be acquired for 14 days. To obtain a trial key register on the OPSWAT Portal first.

Activation

ACTIVATION MODE

ONLINE OFFLINE REQUEST TRIAL KEY ONLINE

Activation key required to use this installation. You can receive a trial key valid for 14 days via email.

Please provide the email address you registered with on OPSWAT Portal.

Trial key is valid for up to 3 scan nodes. If you would like to test our product with more than 3 scan nodes please contact our sales via opswat.com

EMAIL ADDRESS

REQUESTED NUMBER OF SCAN NODES

Trial key request details

1. Provide your e-mail address (that was registered on the OPSWAT portal) in the *EMAIL ADDRESS* field and click the *SEND* button.

2. An e-mail response will arrive from sales@opswat.com containing your trial activation key and activation instructions.

[OPSWAT] Metadefender Core v4 Evaluation Key



sales@opswat.com

Today, 11:03 AM

Avatar Opswat

Thank you for requesting evaluation key for a Metadefender product!

We registered a trial key request from your email address: willis.gilman@opswat.com

Your activation key is `72M9-CAS-5m5n-G4p-L7Cp-PT1s-8uCu-1E9W`

This key is valid for the following products:

- Metadefender Update Downloader - 5 Linux engine package - Evaluation
- Metadefender Core for Linux - 5 engine package - Evaluation

To activate your Metadefender product installation, please follow the following steps:

1. Access the web management console from a web browser.
2. Login with your credentials. (default user: 'admin', default password: 'admin')
3. Go to the Settings menu, License submenu.
4. Click on the ACTIVATE button.
5. Select Online mode. (should be selected by default)
6. Copy and paste your activation key: `72M9-CAS-5m5n-G4p-L7Cp-PT1s-8uCu-1E9W` to the 'Activation key' field
7. Type in the selected maximum agent count up to 3 (If you enter more than three, you will receive an activation error.)
8. Add a comment describing this installation if you wish.

3. Using the received activation key continue with an [online](#) or [offline](#) activation.

Notes



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

2.4.2. Checking Your Metadefender Core License

The license expiration date (last day of license validity) can be seen in the lower left corner of the Web Management Console.

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

- Product ID: product identification as on your order
- Product name: product name as on your order
- Expiration: last day of license validity

- Max nodes: maximum number of nodes that can connect simultaneously
- Deployment ID: identification of this installation
- Activation key: key used for activating product


The screenshot displays the 'License Information' page in the OPSWAT MetaDefender Core interface. The page title is 'License Information' with an 'ACTIVATE' button and a dropdown arrow. The license details are as follows:

Product ID:	MSCW-8b-EVAL-UNLIMITED
Product name:	Metadefender Core for Windows - 8 engine package (Rev.B) - Evaluation
Expiration:	12/31/2026
Max nodes:	1
Deployment ID:	MSCWVN8iW4edviVJ1kDEZXLsYc36ZYGdRBh8
Activation key:	[Blurred]

The sidebar on the left includes the following menu items: Dashboard, Process, Policy, Inventory, Settings (with sub-items: Update Settings, Data Retention, User Management, License, Configuration, Password), and a version indicator '4.9.1' with a 'License Expiration' of '12/31/2026'. The top right of the page shows a 'NOT MANAGED' status, a notification bell, and user information 'LOCAL/admin' with a 'LOGOUT' link.

Settings/License page

2.5. Performance and Load Estimation

 Disclaimer: These results should be viewed as guidelines and not performance guarantees, since there are many variables that affect performance (file set, network configurations, hardware characteristics, etc.). If throughput is important to your implementation, OPSWAT recommends site-specific benchmarking before implementing a production solution.

What to know before reading the results: Some factors that affect performance

- Metadefender product version
- Metadefender package and configuration
 - set of engines (which and how many)
 - product configuration (e.g., thread pool size)
- system environment

- server profile (CPU, RAM, hard disk)
- client application location - remote or local
- system caching and engine level caching
- dataset
 - encrypted or decrypted
 - file types
 - different file types (e.g., document, image, executable)
 - archive file or compound document format files
 - file size
 - bad or unknown (assume to be clean)
- performance tool itself

How test results are calculated


Performance (mainly scanning speed) is measured by throughput rather than unit speed. For example, if it takes 10 seconds to process 1 file, and it also takes 10 seconds to process 10 files, then performance is quantified as 1 second per file, rather than 10 seconds.

- total time / total number of files processed: 10 seconds / 10 files = 1 second / file.

Test Reports

- [Performance Report - Multi-Scanning On Linux](#)
- [Performance Report - Multi-Scanning On Windows](#)

Performance Report - Multi-Scanning On Linux

 Disclaimer: These results should be viewed as guidelines and not performance guarantees, since there are many variables that affect performance (file set, network configurations, hardware characteristics, etc.). If throughput is important to your implementation, OPSWAT recommends site-specific benchmarking before implementing a production solution.

Setup / Configuration

Metadefender version	v4.9.0 Linux
System environment	<ul style="list-style-type: none"> • OS: Centos 6.8 • CPU: 2.10GHz 4 core vCPUs • RAM: 8GB • Hard disk: HDD
Product configuration	<ul style="list-style-type: none"> • No. of threads: 20 • Archive library: disabled • Workflow: File scan
Dataset	<ul style="list-style-type: none"> • All decrypted • Mixed 4% infected
Method	<ul style="list-style-type: none"> • REST
Others	<ul style="list-style-type: none"> • System caching and engine-level caching is ignored • Auto update disabled • Caching disabled

Test results

		Number of Files	Total Size (MB)	Average File Size (MB)	M5 (sec /file)	M10 (sec /file)	DS Overhead
DOC (4992)	<500KB	4645	533	0.12	0.06	0.08	0.01
	500kb~1m	153	101	0.66	0.08	0.12	0.36
	1m~5m	180	382	2.12	0.37	0.22	0.34
	5m~10m	14	101	7.21	0.64	0.71	3.56

		Number of Files	Total Size (MB)	Average File Size (MB)	M5 (sec /file)	M10 (sec /file)	DS Overhead
DOCX (5134)	<500KB	4737	384	0.08	0.05	0.06	0.05
	500kb~1m	130	89.2	0.69	0.07	0.17	1.51
	1m~5m	198	431	2.18	0.28	0.23	0.94
	5m~10m	69	522	7.57	0.35	0.55	4.14
PPT (1925)	<500KB	568	142	0.25	0.06	0.07	n/a
	500kb~1m	430	323	0.75	0.09	0.10	
	1m~5m	912	2027.52	2.22	0.26	0.20	
	5m~10m	15	101	6.73	0.73	0.60	
PPTX (1355)	<500KB	670	100	0.15	0.06	0.06	0.12
	500kb~1m	243	173	0.71	0.07	0.14	0.31
	1m~5m	404	846	2.09	0.12	0.22	0.89
	5m~10m	38	341	8.97	0.50	0.58	1.82
XLS (2939)	<500KB	2354	240	0.1	0.06	0.06	n/a
	500kb~1m	198	144	0.73	0.14	0.12	
	1m~5m	357	657	1.84	0.28	0.24	
	5m~10m	30	237	7.9	1.00	0.83	
XLSX (2153)	<500KB	1881	133	0.07	0.06	0.06	0.08
	500kb~1m	203	133	0.66	0.06	0.17	1.21

		Number of Files	Total Size (MB)	Average File Size (MB)	M5 (sec /file)	M10 (sec /file)	DS Overhead
	1m~5m	49	122	2.49	0.16	0.33	5.98
	5m~10m	20	140	7	0.45	0.70	14.64
RTF (2513)	<500KB	2391	91	0.04	0.06	0.07	n/a
	500kb~1m	55	41	0.75	0.16	0.46	
	1m~5m	39	76	1.95	0.23	0.87	
	5m~10m	28	228	8.14	0.68	2.18	
Executables (1249 files)	<500KB	483	87.3	0.18	0.08	0.26	
	500kb~1m	129	90.2	0.7	0.19	1.16	
	1m~5m	368	886	2.41	0.40	1.53	
	5m~10m	239	1689.6	7.07	0.73	1.52	
Graphic Images (20936 files)	<500KB	17607	1157.12	0.07	0.06	0.06	0.03
	500kb~1m	1049	751	0.72	0.08	0.12	0.15
	1m~5m	1638	3614.72	2.21	0.18	0.17	0.36
	5m~110m	642	8427.52	13.13	0.70	0.61	0.39
Media (1249 files)	<500KB	499	89.3	0.18	0.06	0.06	n/a
	500kb~1m	141	93	0.66	0.09	0.14	
	1m~5m	368	935	2.54	0.17	0.18	
	5m~10m	241	1689.6	7.01	0.34	0.30	

		Number of Files	Total Size (MB)	Average File Size (MB)	M5 (sec /file)	M10 (sec /file)	DS Overhead
Other Misc (1031 files)	<500KB	477	82.8	0.17	0.07	0.08	
	500kb~1m	124	89.1	0.72	0.12	0.19	
	1m~5m	260	604	2.32	0.62	0.69	
	5m~10m	169	1259.52	7.45	0.49	0.85	
PDF (5990 files)	<500KB	4864	431	0.09	0.20	0.16	0.34
	500kb~1m	349	247	0.71	0.16	0.24	0.79
	1m~5m	542	1239.04	2.29	0.38	0.41	1.73
	5m~10m	232	1669.12	7.19	0.61	0.67	4.14
Text (1248 files)	<500KB	500	92.3	0.19	0.19	0.16	n/a
	500kb~1m	134	94.5	0.71	0.27	0.23	
	1m~5m	378	906	2.4	0.33	0.37	
	5m~10m	236	1628.16	6.9	0.64	0.69	
Average scan time					0.27	0.40	

Performance Report - Multi-Scanning On Windows



Disclaimer: These results should be viewed as guidelines and not performance guarantees, since there are many variables that affect performance (file set, network configurations, hardware characteristics, etc.). If throughput is important to your implementation, OPSWAT recommends site-specific benchmarking before implementing a production solution.

Setup / Configuration

Metadefender Core version	4.9.0
System environment	<ul style="list-style-type: none"> • OS: Windows 2008 R2 64 bit • CPU: 2.10GHz 4 core vCPUs • RAM: <ul style="list-style-type: none"> • 16 GB RAM (for 12, 20 engine packages) • 8 GB RAM (for 1, 4, 8 engine packages) • Hard disk: 100 GB HDD
Product configuration	<ul style="list-style-type: none"> • No. of threads: 20 • Archive library: disabled • Workflow: File scan (default)
Dataset	<ul style="list-style-type: none"> • All decrypted • Mixed, 4% infected
Method	<ul style="list-style-type: none"> • REST
Others	<ul style="list-style-type: none"> • System caching and engine-level caching is ignored • Disabled Vulnerability engine • Engine packages used for testing: Rev. A

Test results

		Number of Files	Total Size (MB)	Average File Size (MB)	M4 (sec /file)	M8 (sec /file)	M12 (sec /file)	M16 (sec /file)	M20 (sec /file)
DOC (4992)	<500KB	4645	533	0.12	0.05	0.05	0.09	0.14	0.21
	500kb~1m	153	101	0.66	0.10	0.11	0.21	0.19	0.45
	1m~5m	180	382	2.12	0.34	0.33	0.64	0.59	0.77

		Number of Files	Total Size (MB)	Average File Size (MB)	M4 (sec /file)	M8 (sec /file)	M12 (sec /file)	M16 (sec /file)	M20 (sec /file)
	5m~10m	14	101	7.21	0.68	0.67	0.60	0.99	0.54
DOCX (5134)	<500KB	4737	384	0.08	0.06	0.04	0.07	0.14	0.22
	500kb~1m	130	89.2	0.69	0.08	0.07	0.15	0.20	0.30
	1m~5m	198	431	2.18	0.17	0.13	0.30	0.34	0.47
	5m~10m	69	522	7.57	0.85	0.64	1.21	1.21	1.40
PPT (1925)	<500KB	568	142	0.25	0.10	0.08	0.16	0.16	0.19
	500kb~1m	430	323	0.75	0.15	0.11	0.26	0.22	0.27
	1m~5m	912	2027.52	2.22	0.30	0.21	0.33	0.46	0.57
	5m~10m	15	101	6.73	0.49	0.63	0.93	1.35	0.88
PPTX (1355)	<500KB	670	100	0.15	0.05	0.04	0.08	0.18	0.21
	500kb~1m	243	173	0.71	0.07	0.07	0.14	0.24	0.35
	1m~5m	404	846	2.09	0.20	0.16	0.31	0.35	0.47
	5m~10m	38	341	8.97	0.79	0.58	1.11	1.09	1.14
XLS (2939)	<500KB	2354	240	0.1	0.06	0.05	0.13	0.13	0.18
	500kb~1m	198	144	0.73	0.15	0.11	0.30	0.24	0.26
	1m~5m	357	657	1.84	0.29	0.22	0.41	0.51	0.68
	5m~10m	30	237	7.9	0.89	0.57	1.74	1.19	1.36

		Number of Files	Total Size (MB)	Average File Size (MB)	M4 (sec /file)	M8 (sec /file)	M12 (sec /file)	M16 (sec /file)	M20 (sec /file)
XLSX (2153)	<500KB	1881	133	0.07	0.06	0.04	0.07	0.12	0.15
	500kb~1m	203	133	0.66	0.13	0.10	0.18	0.33	0.43
	1m~5m	49	122	2.49	0.15	0.15	0.44	0.52	0.78
	5m~10m	20	140	7	1.27	0.94	1.47	1.43	1.86
RTF (2513)	<500KB	2391	91	0.04	0.05	0.05	0.07	0.11	0.13
	500kb~1m	55	41	0.75	0.11	0.14	0.53	1.04	1.02
	1m~5m	39	76	1.95	0.18	0.25	1.14	1.57	1.60
	5m~10m	28	228	8.14	0.50	0.63	2.75	3.56	3.13
Executables (1249 files)	<500KB	483	87.3	0.18	0.09	0.09	0.23	0.48	0.41
	500kb~1m	129	90.2	0.7	0.27	0.33	0.49	0.91	0.95
	1m~5m	368	886	2.41	0.69	0.55	0.94	1.47	1.43
	5m~10m	239	1689.6	7.07	1.27	1.15	1.73	1.88	2.42
Graphic Images (20936 files)	<500KB	17607	1157.12	0.07	0.06	0.04	0.09	0.08	0.10
	500kb~1m	1049	751	0.72	0.11	0.08	0.11	0.14	0.17
	1m~5m	1638	3614.72	2.21	0.22	0.16	0.24	0.30	0.28
	5m~110m	642	8427.52	13.13	0.99	0.77	1.17	1.13	1.38
Media (1249 files)	<500KB	499	89.3	0.18	0.07	0.05	0.07	0.09	0.11

		Number of Files	Total Size (MB)	Average File Size (MB)	M4 (sec /file)	M8 (sec /file)	M12 (sec /file)	M16 (sec /file)	M20 (sec /file)
	500kb~1m	141	93	0.66	0.12	0.08	0.11	0.13	0.16
	1m~5m	368	935	2.54	0.23	0.16	0.24	0.29	0.31
	5m~10m	241	1689.6	7.01	0.51	0.36	0.53	0.55	0.58
Other Misc (1031 files)	<500KB	477	82.8	0.17	0.09	0.07	0.21	0.21	0.24
	500kb~1m	124	89.1	0.72	0.14	0.11	0.27	0.34	0.35
	1m~5m	260	604	2.32	0.36	0.26	0.52	0.57	0.66
	5m~10m	169	1259.52	7.45	0.65	0.49	0.85	1.45	1.36
PDF (5990 files)	<500KB	4864	431	0.09	0.08	0.16	0.20	0.30	0.44
	500kb~1m	349	247	0.71	0.21	0.14	0.25	0.34	0.63
	1m~5m	542	1239.04	2.29	0.34	0.31	0.54	0.67	0.92
	5m~10m	232	1669.12	7.19	0.81	0.80	1.15	1.31	1.60
Text (1248 files)	<500kb	500	92.3	0.19	0.07	0.20	0.26	0.41	0.56
	500kb~1m	134	94.5	0.71	0.13	0.17	0.41	0.41	0.79
	1m~5m	378	906	2.4	0.25	0.43	0.60	0.70	1.08
	5m~10m	236	1628.16	6.9	0.62	0.85	1.23	1.41	2.31
Average scan time					0.32	0.29	0.54	0.66	0.76

2.6. Special installation options

Use RAMDISK for the tempdirectory

In order to improve the file scan speed, a custom *tempdirectory* can be set for Metadefender Core.

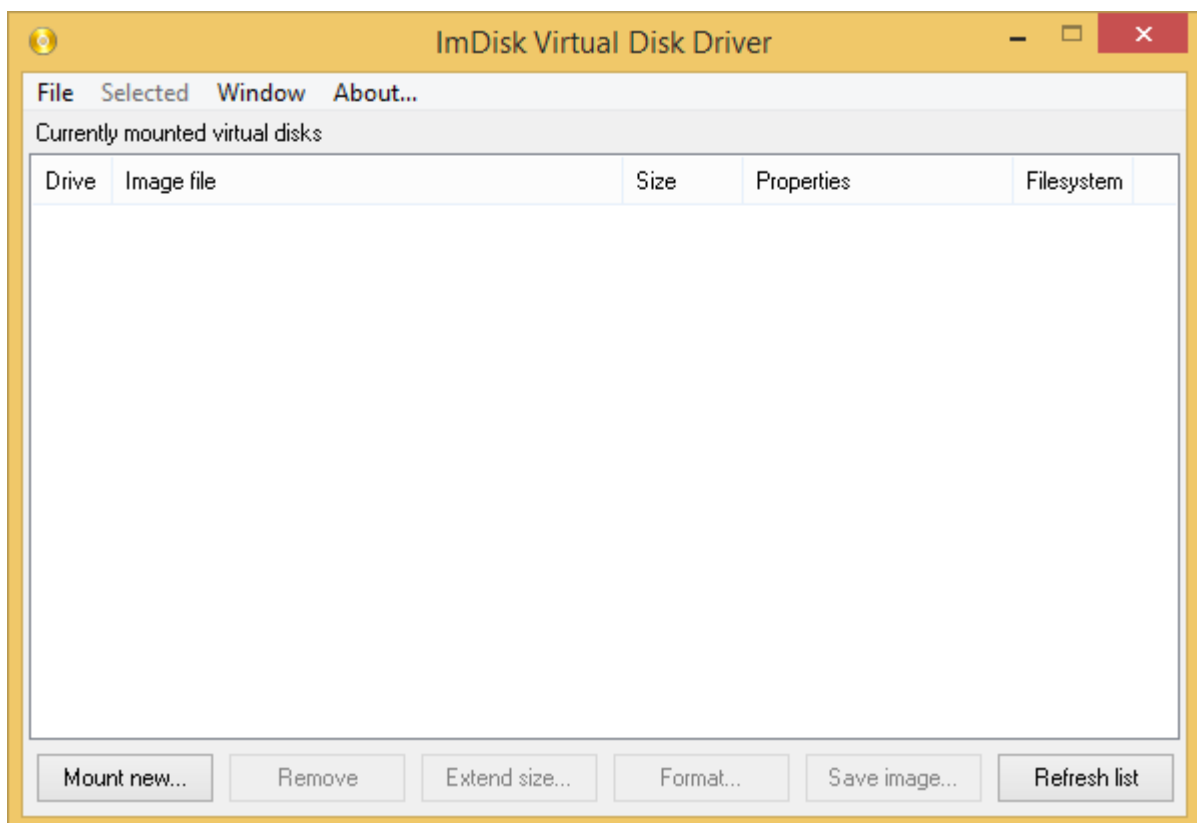
Instructions for windows

Step 1:

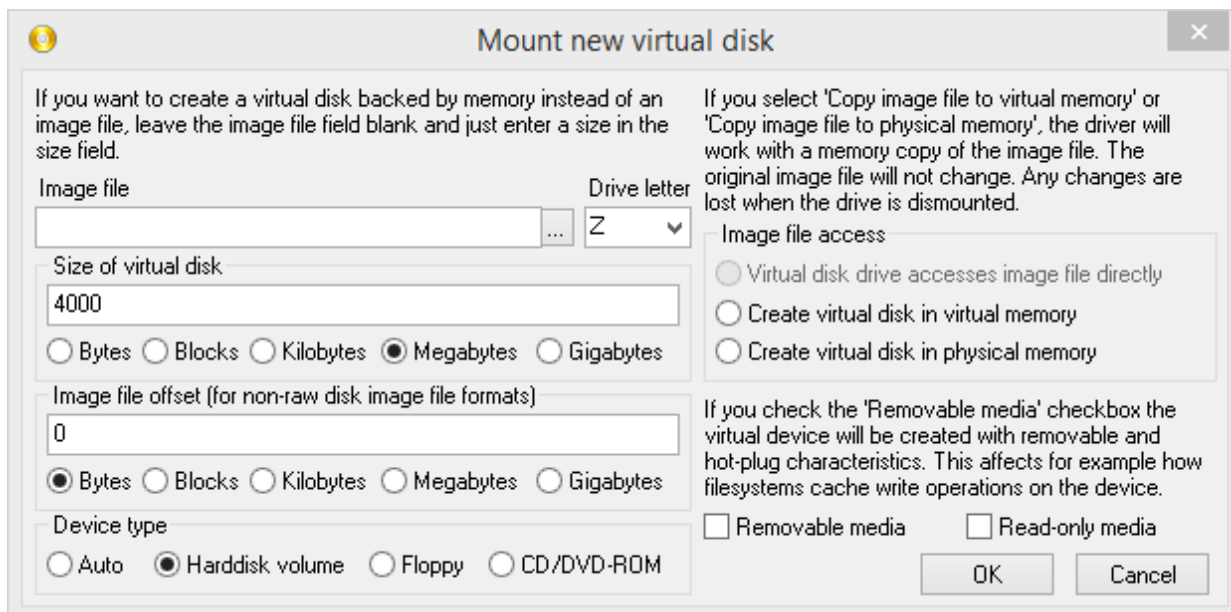
Create a RAMDISK on your system.

We recommend the following tool for this: <http://www.ltr-data.se/opencode.html/#ImDisk>

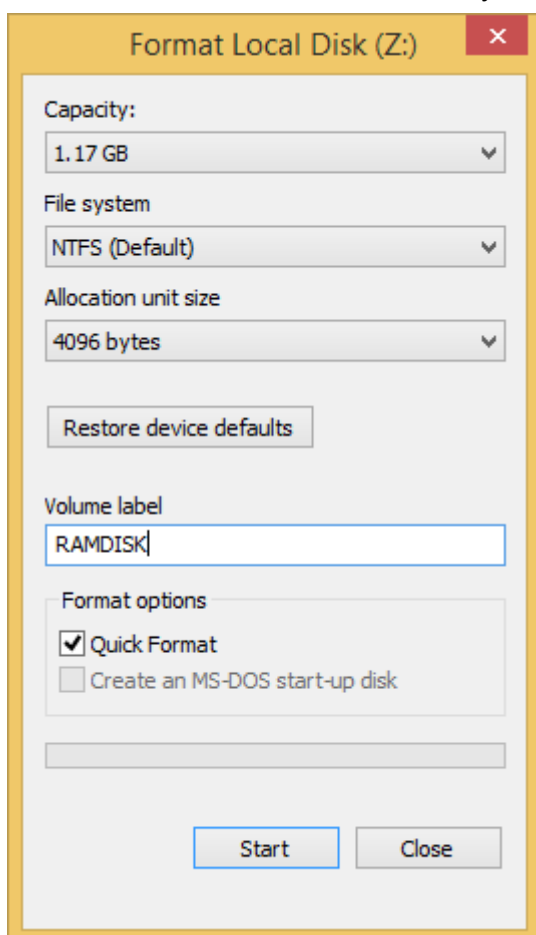
After installation, use the **ImDisk Virtual Disk Driver** application, to create a new RAMDISK.



Mount new virtual disk:



After disk creation, windows will ask you to format the new disk.



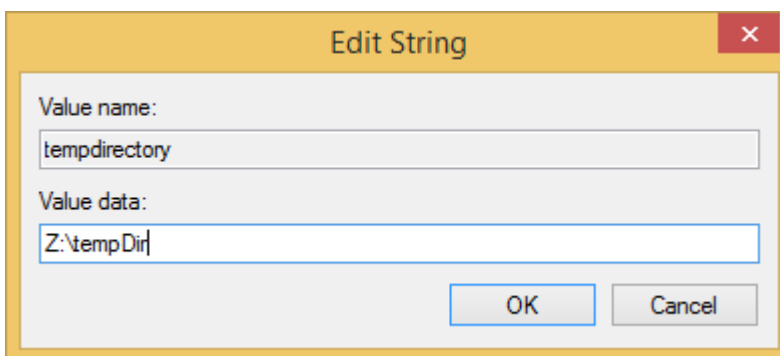
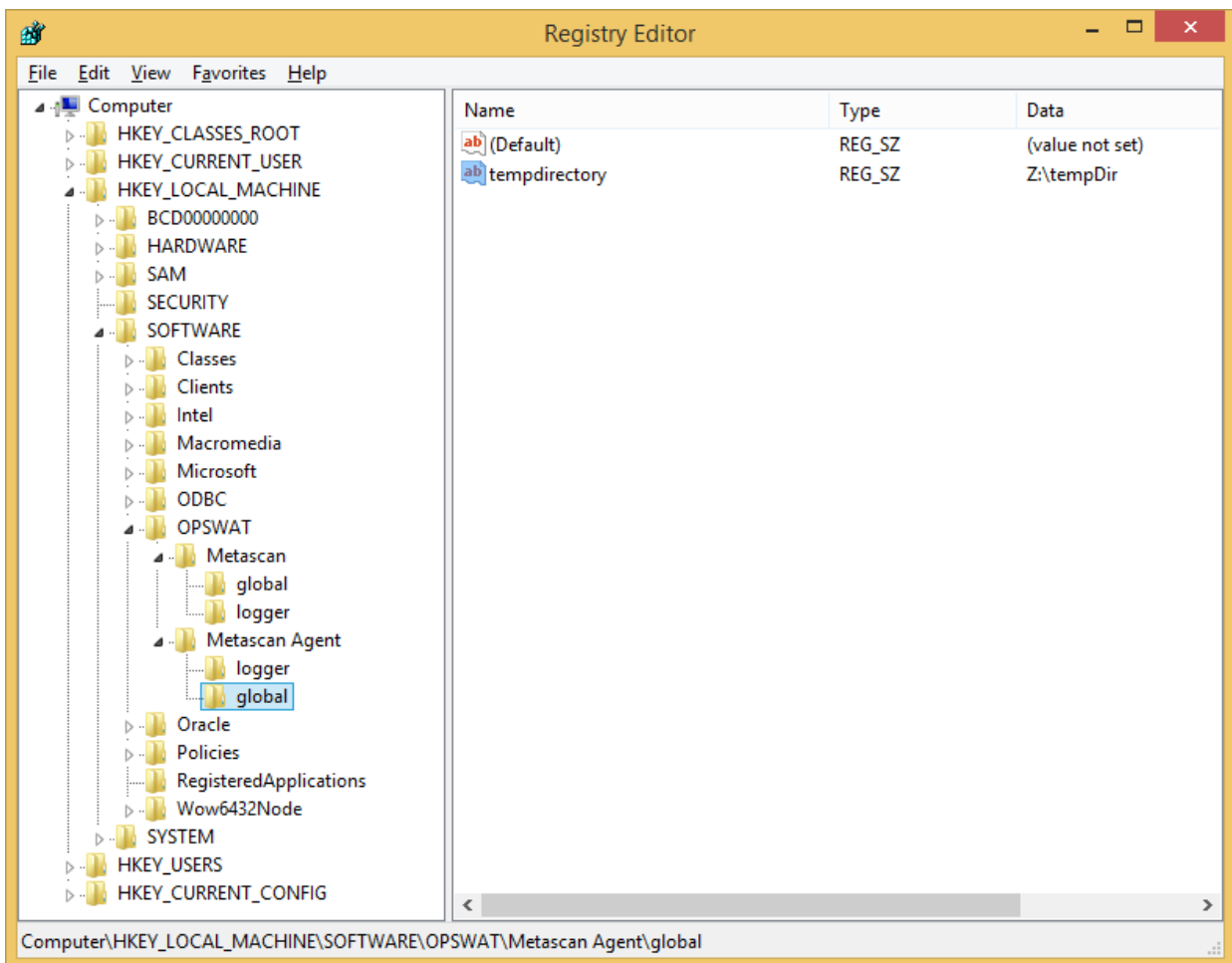
Step 2:

Create, or edit the following registry entry:

HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan Node\global\tempdirectory

i In versions older than v4.6.0 the location of the configuration option is
HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan
Agent\global\tempdirectory

where *tempdirectory* should be a string value with a desired location, for example: *Z:\tempDir*



The Recommended minimum size for the *tempdirectory* is:

- For non archive files: the average file size * 40, at least 10GB
- For archive files: the average archive size * 200

Step 3:

The changes to take effect restart the OPSWAT Metadefender Code Node service.

After the service restart, your custom directory will be used for temporary file storage during file scan.

3. Configuring Metadefender Core

- 3.1. Management Console
- 3.2. Metadefender Configuration
- 3.3. User management
- 3.4. Update settings
- 3.5. Clean up scan database
- 3.6. Policies configuration
- 3.7. Logging
- 3.8 Security settings on web console
- 3.9. Configuring proxy settings
- 3.10. External Scanners And Post Actions
- 3.11. Yara rule sources

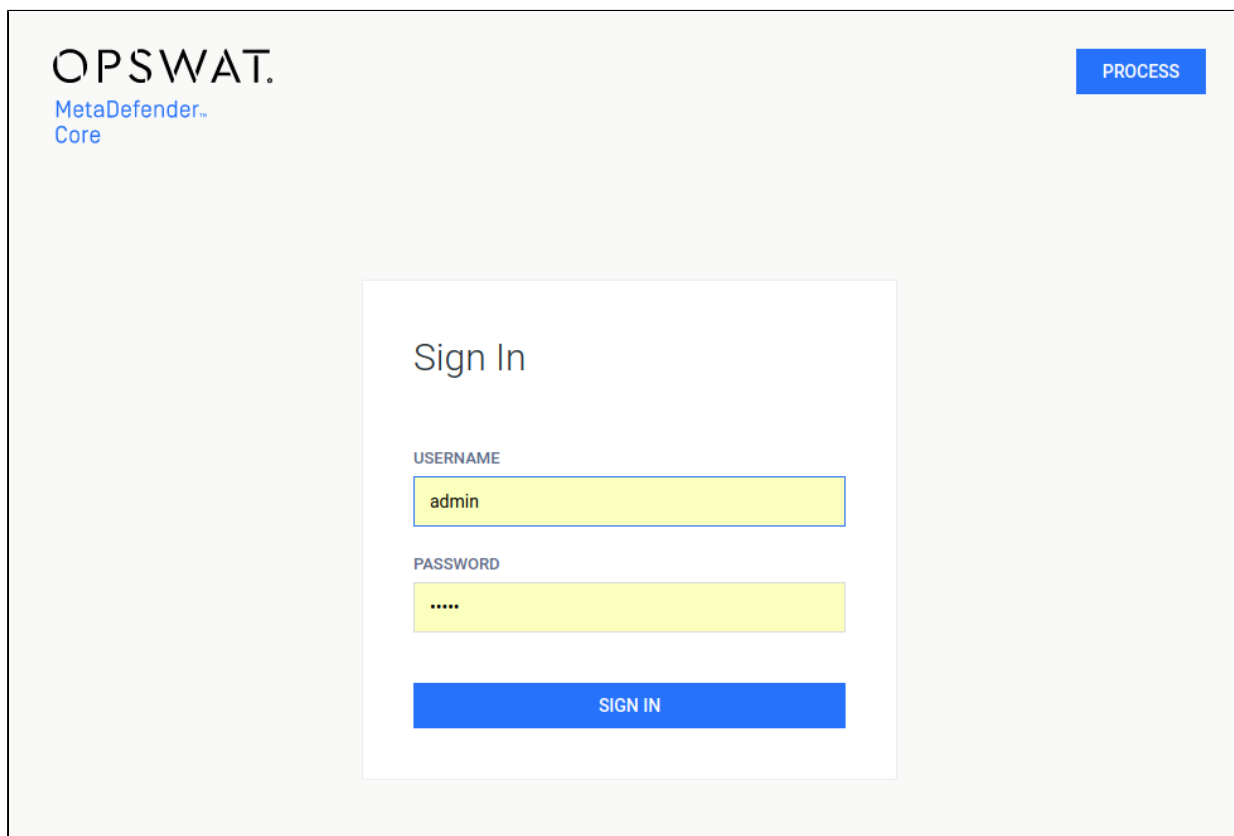
3.1. Management Console

The management console is available at: `http://<MetaDefender Core Server>:<port>/`

where `<MetaDefender Core Server>` is the name or IP address of the system where MetaDefender Core is installed.

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

Every change made in the MetaDefender Core 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](#)

3.2. Metadefender Configuration

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

- [3.2.1. Startup Core Configuration](#)
- [3.2.2. Startup Node Configuration](#)
- [3.2.3 Nginx related configuration](#)

3.2.1. Startup Core Configuration

Linux

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

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

[global] section

parameter	default value	required	description
restaddress	0.0.0.0	required	One of the IP addresses of the computer that runs the product to serve REST API and web user interface (0.0.0.0 means all interface)
restport	8008	required	Designated port number for the web and REST interface
address		optional	Address of the computer to accept external scan node connections
port		optional	Designated port number to accept external scan node connections

[logger] section

key	default value	required	description
logfile	/var/log/ometascan /ometascan.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 (Multiple server can be specified separated with comma)
syslog_level		optional	Level of logging. Supported values are: debug, info, warning, error

key	default value	required	description
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.

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

Windows

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

After modifying the server configuration file you must restart the Metadefender Core 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\Metascan\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	8008	string value	required	Designated port number for the web and REST interface
address		string value	optional	Address of the computer to accept external scan node connections
port		string value	optional	Designated port number to accept external scan node connections

parameter	default value	type	required	description
report_engine_issue	true	string value	optional	Enable reporting of engine issue count. (possible values: "true" or "false").

Reporting of engine issue count

If reporting of engine issue count is enabled, Metadefender Core v4 server will send only the **number** of initialization errors and **number** of unexpected stops for the specific db /engine version. This information is sent over a HTTPS channel when the product downloads the latest package descriptors. This information is used for early detection of any specific 3rd party engine quality issues.

HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan\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 are: debug, info, warning, error
syslog		string value	optional	Value can only be in form of 'udp://<hostname>:<port>' (Multiple server can be specified separated with comma)
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"

key	default value	type	required	description
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.

Please note, if a data entry to be used does not exist, it should be created first.

3.2.2. Startup Node Configuration

Linux

The configuration file for the node is located in `/etc/ometascan-node/ometascan-node.conf`

After modifying the node configuration file you must restart the Metadefender Core Node service in order for the changes to take effect. You should use the distribution-standard way to restart the service.

[global] section

parameter	default value	required	description
serveraddress		optional	Address of the computer to accept external scan node connections
serverport		optional	Designated port number to accept external scan node connections
tempdirectory		optional	Full path of a directory to use for storing temporary files (Node creates a subfolder called resources in this folder)

In case the `serveraddress` and `serverport` are not provided, the scan node will try to connect the Metadefender Core server on the local machine. You should set both or none of them.

[logger] section

key	default value	required	description
logfile	/var/log/ometascan /ometascan-node. 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 (Multiple server can be specified separated with comma)
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.

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

Windows

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

After modifying the node configuration file you must restart the Metadefender Core Node service in order for the changes to take effect. You should use the distribution-standard way to restart the service.

HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan Node\global

parameter	default value	type	required	description
serveraddress		string value	optional	Address of the computer to accept external scan node connections
serverport		string value	optional	Designated port number to accept external scan node connections

In case the *serveraddress* and *serverport* are not provided, the scan node will try to connect the Metadefender Core server on the local machine.

HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan Node\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 are: debug, info, warning, error
syslog		string value	optional	Value can only be in form of 'udp://<hostname>:<port>' (Multiple server can be specified separated with comma)
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"

key	default value	type	required	description
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.

Please note, if a data entry to be used does not exist, it should be created first.



In versions older than v4.6.0 the location of the configuration option is HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan Agent\...

3.2.3 Nginx related configuration

The web console user interface of MetaDefender Core is provided by a web server called Nginx. Some but not all of the Nginx directives can be overridden using additional configuration files.

- On **linux**: All files with .conf extension under */etc/ometascan/nginx.d* directory,
- on **Windows**: All files with .conf extension under *<Installation Directory>\nginx* directory

are included into the Nginx configuration.

For details on how to use Nginx directives, please refer to Nginx documentation.



The configuration files should be readable for the user that runs MetaDefender Core service (On linux: metascan, on Windows: service user).

3.3. User management

To manage the users of the Metadefender Core v4 go to the **Settings > User Management** menu in the Web Management Console.

- [3.3.1. Users and groups](#)
- [3.3.2. Roles](#)
- [3.3.3. User directories](#)
- [3.3.4. Active Directory attributes](#)

- [3.3.5. Change user password](#)

3.3.1. 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

Special user accounts

Some user accounts are reserved in the product for system internal usage. These accounts are documented in this section.



The special accounts documented in this section are for internal usage. Do not directly modify these accounts through the user management functions cause it may give unexpected results.

SYSTEM/management account

The SYSTEM/management account is reserved for [Central Management](#).

When the product is connected to *Central Management* as a managed instance, then this account is automatically created by *Central Management* at the first successful connection with the following parameters:

Username	Password	Name	Email	Roles	User directory
management	N/A	Metadefender Central Management	management@localhost	Administrators	SYSTEM

All consecutive connection attempts are performed by *Central Management* using the SYSTEM/management account.

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.



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 Core v4 REST API for this user with no authentication. If no such functionality is needed for the user then this field can be left blank.

There are two ways to have an APIKEY for a user.

- generating by using *Generate* button next to APIKEY field,
- typing one that matches the following criterias:
 - The length of the API key must be exactly 36 characters.
 - It must contain numeric and lower case letter characters only
[0-9a-z].
 - It must contain at least 10 lower case letter characters.
 - It must contain at least 10 numeric characters.
 - It is allowed to contain at most 3 consecutive lower case letter characters (e.g. "abcd1a2b3c..." is invalid).
 - It is allowed to contain at most 3 consecutive numeric characters (e.g. "1234a1b2c3..." is invalid).

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.



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/assign new user(s)

USER DIRECTORY

AD

ACCOUNT TYPE



USER



GROUP

ACCOUNT NAME

Account name

ACCOUNT DISPLAY NAME

Display name

ASSIGN TO ROLES

▼ ✕

[Add new role](#)

DISTINGUISHED NAME

DISTINGUISHED NAME

ADD

CANCEL

FIND ACCOUNT


Add new group from an Active Directory type user directory




The purpose of adding an Active Directory group to the Metadefender Core v4 is to assign Core v4 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 Core v4 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.

 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.

 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
 - a. In this case the highest available permission applies to each function. Example:

Roles assigned	Effective permissions	
	Full permission	Read only permission
security_admin	Scan history, Update history, Security rules, Security zones, Analysis workflows, Scan nodes, Engines, Update settings, Scan settings	

Roles assigned	Effective permissions	
security_auditor		All except External settings
security_admin AND security_auditor	Scan history, Update history, Security rules, Security zones, Analysis workflows, Scan nodes, Engines, Update settings, Scan settings	Config history, Data retention, User management, License

Delete user



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

3.3.2. Roles

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

The screenshot shows the OPSWAT User Management interface. The left sidebar contains navigation options: Dashboard, Process, Policy, Inventory, Settings (with sub-options: Update Settings, Data Retention, User Management, License, Configuration, Password), and version information (4.9.1, License Expiration 12/31/2026). The main content area is titled 'User Management' and includes a 'Help Center' link, a 'NOT MANAGED' status indicator, and user information (LOCAL/admin, LOGOUT). A blue 'ADD NEW ROLE' button is visible in the top right. Below the title, there are three tabs: 'USERS AND GROUPS', 'ROLES' (selected), and 'USER DIRECTORIES'. A table lists the roles:

ROLENAME	DISPLAY NAME	NUMBER OF USERS	RIGHTS
admin	Administrators	1	Full
security_admin	Security administrators	0	Full: Processing history, Quarantine, Update history, Security rules, S...
security_auditor	Security auditor	0	Read-only
help_desk	Help desk	0	Read-only: Processing history, Update history, Security rules, Security zone...

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 Scan history, Update history, Security rules, Security zones, Analysis workflows, Scan nodes, Engines, Update settings, Scan settings functions
security_auditor	Security auditor		Read-only on a ll except External settings functions
help_desk	Help desk		Read-only on Scan history, Update history, Security rules, Security zones, Analysis workflows, Scan nodes, Engines, Scan settings 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 Core v4 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 Core v4 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 modification 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



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

Modify role



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

For example:

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

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

Delete role



A role can not be deleted as long as it is assigned to any user.

As a consequence deleting a role can not affect active sessions of users.

3.3.3. 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 Core v4:

1. Local
2. Active Directory

Local type user directories

Local type user directories allow creating users that locally exist on the Metadefender Core v4.

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

- **Number of failed logins before lockout:** After this number of consecutive failed login attempts the account gets locked.
- **Lockout time [minutes]:** The account remains locked for the given minutes.
 - When the lockout time elapses, the account lock gets released automatically.
 - Users with appropriate permission may release the account lock earlier using the [RELEASE LOCKOUT button](#).

LDAP and Active Directory type user directories

LDAP and Active Directory type user directories allow users defined in an LDAP or Active Directory to access Metadefender Core v4.

These types of user directories do not provide the possibility to define login policies; these policies may be defined in the LDAP or 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 [Local type user directories](#) section.

Add user directory

USERDIRECTORY TYPE

Local ▼

NAME

NAME

SECURITY SETTINGS

NUMBER OF FAILED LOGINS BEFORE LOCKOUT ⓘ

3

LOCKOUT TIME [MINUTES] ⓘ

5

ADD CANCEL

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.

ⓘ 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 [Enabling HTTPS](#).





As long as ENCRYPTION field is set to *None* there is no encryption used between the Metadefender Core v4 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 and don't forget to install the certificate of the issuer of the AD server's certificate on the server that runs Metadefender Core v4.

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. For tips about finding the proper values for these fields see [3.3.4. Active Directory attributes](#).

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.

Add new Active Directory type user directory

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

The following information should be given to configure an LDAP user directory:

- **bind username:** The name as DN of a user who has permissions to do searches in the LDAP directory.
- **user base DN:** The DN from where all users can be reached.
- **group base DN:** The DN from where all groups can be reached.
- **user object class:** The name of the object class (objectClass) that is for user objects. (e.g. posixAccount or person)
- **user account attribute:** The name of the LDAP attribute that contains the login name of the users.
- **group object class:** The name of the object class (objectClass) that is for group objects. (e.g. posixGroup or group)
- **group account attribute:** The name of the attribute that contains the name of the group of the users.

Add user directory

<input type="text" value="172.16.172.16"/>	<input type="text" value="636"/>	SSL ▼	Delete
--	----------------------------------	-------	------------------------

SERVER HOST	SERVER PORT	ENCRYPTION	
<input type="text" value="172.16.172.17"/>	<input type="text" value="389"/>	None ▼	Delete

[Add Server](#)

BIND USERNAME

BIND PASSWORD

USER BASE DN

GROUP BASE DN

LDAP USER SCHEMA SETTINGS

USER OBJECT CLASS

USER ACCOUNT ATTRIBUTE

USER EMAIL ATTRIBUTE


USER DISPLAY NAME ATTRIBUTE


LDAP GROUP SCHEMA SETTINGS


GROUP OBJECT CLASS

GROUP ACCOUNT ATTRIBUTE


GROUP DISPLAY NAME ATTRIBUTE

 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 LDAP server responses a lot and thus have an impact on Metadefender Core v4 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,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,DC=example,DC=com" in the directory information tree.

 Please also note that users and groups may reside in different parts of the directory information tree, as a consequence applying the same, more specific DN both as USER BASE DN and GROUP BASE DN may cause Metadefender Core v4 not to find group accounts in the directory information tree. So these DNs should be chosen carefully.

Delete user directory

 Users of the deleted user directory will be deleted as well. As a consequence active sessions of the users of the deleted user directory will be aborted at the time of the next interaction with the server.

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

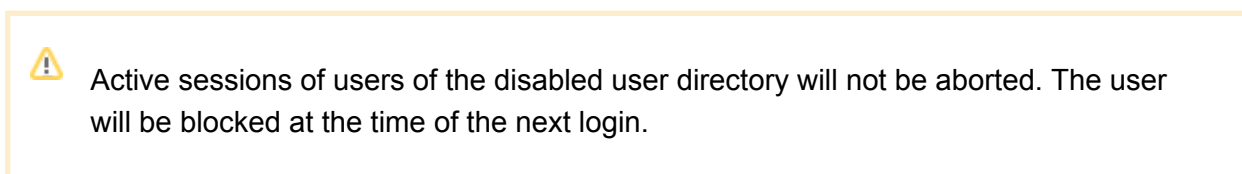


Enable or disable user directory

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.



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.

3.3.4. 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](#).

Add user directory

USER DIRECTORY TYPE

Active Directory

NAME

AD-1

ACTIVE DIRECTORY SETTINGS

SERVER HOST

172.16.172.16

SERVER PORT

636

ENCRYPTION

SSL

[Delete](#)

SERVER HOST

172.16.172.17

SERVER PORT

389

ENCRYPTION

None

[Delete](#)

[Add Server](#)

BIND USERNAME

binduser

BIND PASSWORD

.....

USER BASE DN

OU=OrgUnit1,DC=DomComp1,DC=DomComp2

GROUP BASE DN

OU=OrgUnit2,DC=DomComp1,DC=DomComp2

ADD

CANCEL

TEST

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 Core v4 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:

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

or

```
> dsquery user domainroot -name John Smith
```

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

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



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

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:

DC=example,DC=com



Please note that using only DC components for the user/group DNs may result in searches to be executed from the top of the directory information tree and potentially slow down AD server responses a lot and thus have an impact on Metadefender Core v4 password validation. The rule of thumb here is that the more specific the user /group DN the faster the server response.



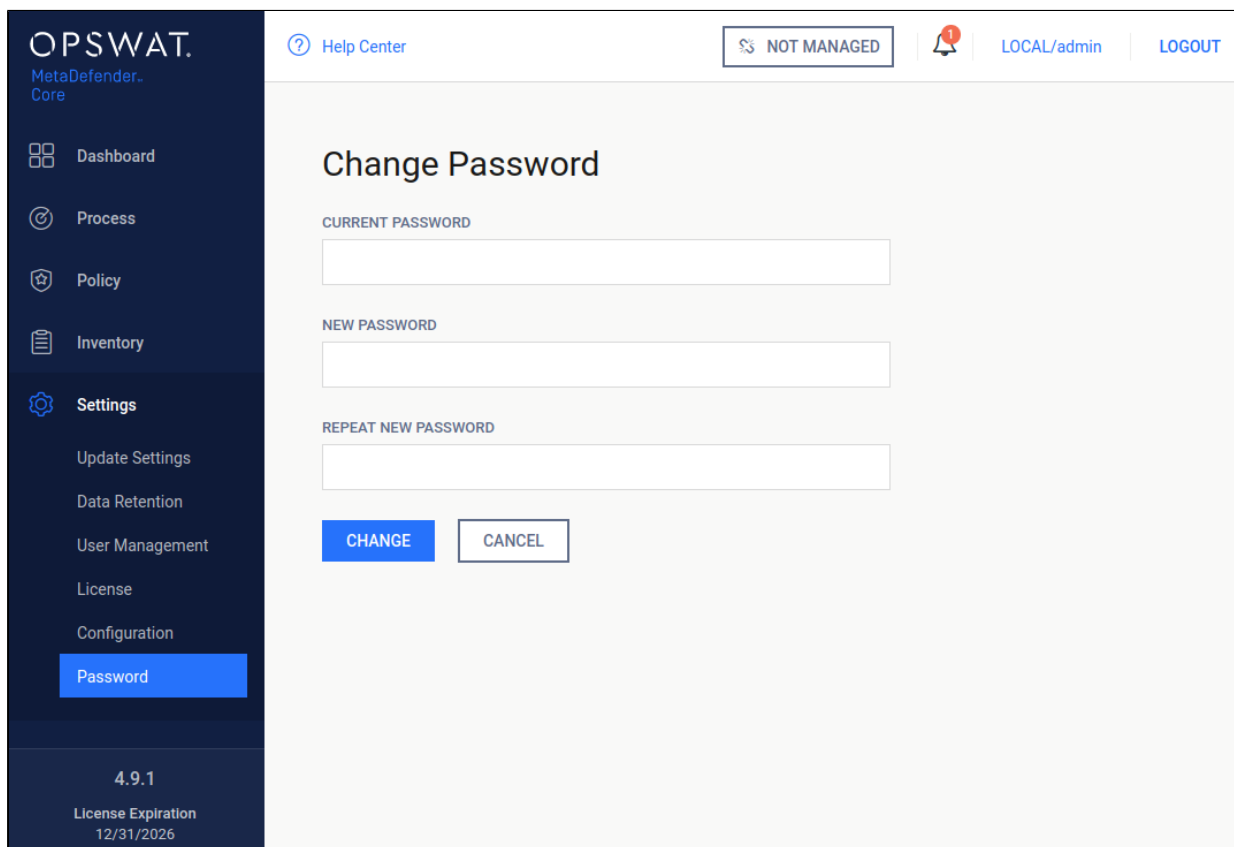
Taking the above example into consideration: a user search DN of "OU=People,OU=Engineering,DC=example,DC=com" could potentially result in much faster server response than "DC=example,DC=com" and should be preferred assuming all users reside under "OU=People,OU=Engineering,DC=example,DC=com" in the directory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



Please also note that users and groups may reside in different parts of the directory information tree, as a consequence applying the same, more specific DN both as USER BASE DN and GROUP BASE DN may cause Metadefender Core v4 not to find group accounts in the directory information tree. So these DNs should be chosen carefully.


3.3.5. Change user password

The current user can change her password in **Settings > Password**.



Changing password

Important notes

 As long as TLS is not configured for the Web Management Console, passwords are sent clear-text over the network. To set up TLS see [Enabling HTTPS](#).

3.4. Update settings

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

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

- Internet: automatic update downloading from the internet.
- Folder: searching for updates in a specific folder.
- Manual: disable automatic updates.

Internet

The screenshot displays the 'Update Settings' interface in the OPSWAT MetaDefender Core. The left sidebar is dark blue with the OPSWAT logo and navigation menu items: Dashboard, Process, Policy, Inventory, and Settings. Under Settings, 'Update Settings' is highlighted. At the bottom of the sidebar, the version '4.9.1' and 'License Expiration 12/31/2026' are shown. The main content area has a light gray background. At the top, there's a 'Help Center' link, a 'NOT MANAGED' status box, a notification bell, and user info 'LOCAL/admin' with a 'LOGOUT' link. The 'Update Settings' title is at the top left of the main area, with a 'SAVE SETTINGS' button to its right. Below the title, the 'Source' section has three radio buttons: 'INTERNET' (selected), 'FOLDER', and 'MANUAL'. The 'Automatic database updates' section features a horizontal scrollbar with options: Off, 15m, 30m, 1h, 2h, 4h (selected), 6h, 12h, and 24h. The 'Update Time' section includes the text 'Updates are not applied during:' followed by 'DAY OF WEEK' (a dropdown menu with 'Choose day of week') and 'TIME PERIOD' (a time range selector showing '08 : 00 TO 16 : 00' with a 'Delete' link). An 'Add rule' link is located below the time period.

Internet update method

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

To set the frequency of these updates choose the corresponding value presented on the **Automatic database updates** scrollbar.

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

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

Folder

The screenshot displays the 'Update Settings' interface in the OPSWAT MetaDefender Core. The left sidebar contains navigation options: Dashboard, Process, Policy, Inventory, and Settings. Under Settings, 'Update Settings' is highlighted. The main content area shows the 'Source' set to 'FOLDER'. The 'Pick up updates from' field contains the path 'C:/Program Files/OPSWAT/Metadefender Core/data/update_autoadd'. The 'DELETE FILES AFTER IMPORT' checkbox is checked. The 'Update Time' section indicates that updates are not applied during a specific time period, with a 'DAY OF WEEK' dropdown set to 'Choose day of week' and a 'TIME PERIOD' set to '08 : 00 TO 16 : 00'. A 'Delete' link is visible next to the time period. A 'SAVE SETTINGS' button is located in the top right corner. The top navigation bar includes 'Help Center', 'NOT MANAGED', 'LOCAL/admin', and 'LOGOUT'. The bottom of the sidebar shows the version '4.9.1' and 'License Expiration 12/31/2026'.

Folder update method

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

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

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

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

Manual

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

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

3.5. Clean up scan database

Clean up settings are accessible under **Settings > Data retention** after successful login.

The screenshot shows the OPSWAT MetaDefender Core interface. The left sidebar contains navigation options: Dashboard, Process, Policy, Inventory, Settings (highlighted), Update Settings, Data Retention (highlighted), User Management, License, Configuration, and Password. The main content area is titled "Data Retention" and includes a "SAVE SETTINGS" button. It features four sections for cleaning up records older than a specified duration:

- Processing history clean up**: Options include Off, 1 Hour, 1 Day, 1 Week, 4 Weeks (selected), 3 Months, 6 Months, and 12 Months.
- Quarantine clean up**: Options include Off, 1 Hour, 1 Day, 1 Week, 4 Weeks (selected), 3 Months, 6 Months, and 12 Months.
- Audit records (update history) clean up**: Options include Off, 1 Hour, 1 Day, 1 Week, 4 Weeks (selected), 3 Months, 6 Months, and 12 Months.
- Sanitized file clean up**: Options include Off, 15m, 30m, 1h, 2h, 4h (selected), 6h, 12h, and 24h.

The bottom of the sidebar shows the version "4.9.1" and the license expiration date "12/31/2026".

Data retention

Stored scan results, quarantined files, audit log records and sanitized files that are older than the value set on this page, are permanently deleted from the server. In case you do not want to enable automatic clean up, set the value to off. This will prevent automatic removal of the scan history.

Technology Note:

Setting the clean up value to off can have performance penalty.

3.6. Policies configuration

The policy settings determine how MetaDefender Core scans files.

- [3.6.1. How MetaDefender Core policies work](#)
- [3.6.2. Workflow template configuration](#)

- [3.6.3. Security zone configuration](#)
- [3.6.4. Workflow rule configuration](#)
- [3.6.5. Quarantine](#)

3.6.1. How MetaDefender Core policies work

The MetaDefender Core server can be configured to use different scanning profiles for different clients. The selection is based on the client's source IP address.

In case multiple scanning profiles are configured for the given client, the client can choose which one to use. If a client does not have a scanning profile specified, MetaDefender Core uses the first matching profile from the Workflow rules.

All configuration options related to the policies are found under the **Policy** menu.

How policies work

A policy is pairing a *user* with a *workflow template* based on a *workflow rule*.

Users can be grouped into *zones* based on their network address.

Workflow templates can be created/modified to change how file scanning is carried out.

Creating a policy means creating a rule, where a source zone will be paired with a workflow template.

How a file scan is processed via the REST API

When MetaDefender Core receives a scan request through the REST API it will match the source address through the zones in the list of rules and apply the first matching rule's workflow. The processing request then will then be processed based on this specific workflow.

If a workflow is provided by the REST request it still should be one which has a matching rule. Otherwise the scan request will fail.

How a file scan is processed on the web UI

When MetaDefender Core receives a scan request through the web UI it will match the source address through the list of rules. The user will be able to select only those workflows with a matching rule. This scan request then will then be processed based on the workflow selected by the user.

3.6.2. Workflow template configuration

- [Archive](#)
- [Blacklist/Whitelist](#)

- Scan
- MetaDefender Cloud
- Data Sanitization (CDR)
- Data Loss Prevention (DLP)
 - DLP configuration options
- Advanced

The Workflow templates page is found under **Policy > Workflow templates** after successful login.

These workflow templates define the scanning methods that can be used by the rules.

MetaDefender Core comes with predefined workflow templates that can not be modified, however they can be copied and the created workflow templates are fully customizable.

NOTE: These predefined workflow templates cannot be modified or removed.



It is highly recommended to use less workflow template and rather more rules based on the workflow templates.

NAME	DESCRIPTION
Default	Selecting this template all files will be processed without any filtering.
Skip images	Selecting this template all files but certain commonly used image files, such as gif, jpg, png, psd, bmp and tif...
Executables only	Selecting this template only executable files will be processed. All skipped files will be shown as 'not scanned'.

Workflow templates When clicking on a workflow template a window pops up showing different tabs related to the workflow templates different kind of properties.

Archive

On the Archive tab the archive handling can be enabled or disabled as well as other parameters can be set.

The max recursion level defines how deep extraction should go into the archive, the number of maximum extracted files also can be set as well as the overall maximum size of these files.

It is also possible to disable scanning the archive itself, and a timeout for the whole process can be set as well.

Modify Workflow

WORKFLOW NAME

DESCRIPTION

< **ARCHIVE** BLACKLIST WHITELIST SCAN METADEFENDER CLOUD DATA SANITIZATION AD >

ENABLE ARCHIVE HANDLING ⓘ

MAX RECURSION LEVEL ⓘ

MAX NUMBER OF FILES EXTRACTED ⓘ

MAX TOTAL SIZE OF EXTRACTED FILES [IN MEGABYTES] ⓘ

ENABLE SCAN OF ORIGINAL UNEXTRACTED ARCHIVE ⓘ

ENABLE EXTRACTION OF OFFICE DOCUMENTS ⓘ

TIMEOUT FOR HANDLING THE ARCHIVE [IN MINUTES]

SAVE CHANGES **CANCEL**

Archive

Blacklist/Whitelist

During scan it is possible to create blacklists/whitelists where files depending on their checksum or MIME-TYPE and extensions can be skipped. All of these can be stored in the fields on the Blacklist/Whitelist tab. Also it is available to blacklist/whitelist all the files coming from the same group, such as executables, Microsoft Office files and others. When filtering by mime-type or filename, the filter is handled as a regular expression.

Exceptions can be defined in **Exceptions (by mime-type)** section using regular exceptions. For instance, if all office files have to be blocked except docx files, then **Office documents** group should be chosen and `^application\/vnd\.openxmlformats-officedocument\.wordprocessingml\.document$` expression should be given as exception.

- [Using MetaDefender core V4 BLACKLIST/WHITELIST feature](#)

ENABLE PROCESSING OF BLACKLISTED FILES ⓘ

BLACKLIST BY FILETYPE [REVERT TO DEFAULT](#)

ADOBE FILES

ARCHIVE FILES [REVERT TO DEFAULT](#)

BLACKLIST FILETYPES [REVERT TO DEFAULT](#)

TYPE

IF BIGGER THAN

7Z ▾	0	MB	✕
ALL			
7Z			
CPIO			
EXE_SFX			
GZ			
ISO			
JAR			
RAR			

MEDIA FILES

OFFICE DOCUMENTS

TEXT FILES

OTHER

BLACKLIST BY MIME-TYPE

FILETYPE FILTERS

NO FILTER HAS BEEN CREATED YET.

[ADD ROW](#)

BLACKLIST BY FILENAME

FILENAME FILTERS

NO FILTER HAS BEEN CREATED YET.

[ADD ROW](#)

EXCEPTIONS (BY MIME-TYPE)

FILETYPE FILTERS

NO FILTER HAS BEEN CREATED YET.

[ADD ROW](#)



Blacklist

Files can also be whitelisted by their checksums. For more information please see [Skip by hash](#) page.

Scan

File type mismatch feature can be enabled on the tab. With this feature on, when the extension of the file does not match with the available extensions for the actual file type, the scan result will be Filetype Mismatch.

You can specify the number of active anti-malware engines required for performing a processing. When disabled, no active anti-malware engine is needed to be up to start a processing.

Anti-malware engines not to be used in this workflow also can be listed here.

The timeout for the different engines and the whole scanning process also can be set. The maximum allowed size of scanned objects can be set also on this tab as well.

It is possible to enable and set a threshold value for the failed engine results. If the number of failed engine results for the currently scanned object reaches this value, then the overall result will also be failed. This threshold value does not have an effect on suspicious or infected results.

The threat detected threshold has two value infected limit and the suspicious limit if the number of infected engine results is between these values the overall result will be suspicious. If the infected limit is reached the overall result will be always infected. If none of them is reached the overall result will be the highest priority engine result (infected results are ignored).

If the provided workflows do not meet your requirements, please contact our support team via the [OPSWAT Portal](#).

ARCHIVE **SCAN** DATA SANITIZATION METADEFENDER CLOUD MORE ▾

ENABLE MALWARE SCAN ⓘ

DO NOT SCAN UNLESS NUMBER OF ANTI-MALWARE ENGINES ARE UP ⓘ

NUMBER OF ACTIVE ANTI-MALWARE ENGINES ⓘ

1

EXCLUDE ENGINES ⓘ

▾ × +

DETECT FILE TYPE MISMATCH ⓘ

PER ENGINE SCAN TIMEOUT [IN MINUTES]

1

EXTERNAL SCANNER TIMEOUT [IN MINUTES]

1

GLOBAL SCAN TIMEOUT [IN MINUTES]

10

MAXIMUM FILE SIZE FOR FILES SCANNED [IN MEGABYTES]

200

SCAN FAILURE THRESHOLD ⓘ

THRESHOLD VALUE ⓘ

1

THREAT DETECTED THRESHOLD ⓘ

THRESHOLD VALUE ⓘ

1

SAVE CHANGES **CANCEL**

Scan

MetaDefender Cloud

When MetaDefender Cloud workflow element is enabled, online database of MetaDefender Cloud will be used as source for hash lookups.

Available options:

1. **Use results:** INFECTED or ALL RESULTS
If INFECTED is chosen, then only that result will be accepted as result, otherwise all type of results will be taken into account.
2. **MetaDefender Cloud API key:** An API key is necessary to have access to the MetaDefender Cloud database. API Key Information can be found on <http://metadefender.com>, under **Account Information** page.
3. **Maximum age of scan results:** Only results that are not older than what is set here will be considered as a valid result.
4. **Excluded engines' name:** Name of the engines whose results are not to be taken into account.
5. **Minimum hit count:** To consider a verdict as a valid one, there should be at least as many result for a hash as it has been set here. (If **Use result** is set to INFECTED, then only infected results will be counted in.)
6. **Time out:** The time interval within which the response should be received from MetaDefender Cloud.

Modify Workflow

WORKFLOW NAME

WorkFlow-1

DESCRIPTION

Selecting this template all files will be processed without any filtering.

- ARCHIVE
- BLACKLIST
- WHITELIST
- SCAN
- METADEFENDER CLOUD**
- DATA SANITIZATION
- AD

CHECK FILE HASHES FOR EXISTING SCAN RESULTS BEFORE SCANNING

USE RESULTS

INFECTED

METADEFENDER CLOUD API KEY

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

MAXIMUM AGE OF SCAN RESULTS [IN HOURS] ⓘ

240

EXCLUDED ENGINE NAMES

✕ Add

MINIMUM HIT COUNT

1

TIMEOUT [IN SECONDS]

120

SAVE CHANGES CANCEL

MetaDefender Cloud

Data Sanitization (CDR)

By enabling data sanitization one can convert from a set of supported filetypes into another (or the same). By doing so lot of vulnerabilities can be got rid out of rendering the resulting file be more safe. Both the types to be sanitized and the target filetype can be set. File name fro sanitized files can be defined by using "Output filename format" field. For usage and meanings of variables, please refer to [Setup output file name](#) page.

The maximum allowed time for data sanitization to be made can be configured through the "Conversion timeout" and "Try count" options, where first one means that data sanitization should finish within the configured timeframe, otherwise abort the conversion and latter means the number of times product should retry in case of a failed conversion.

Beware, however, that possible data loss or change may occur during conversion, thus this feature is disabled by default.

Note that data sanitization engine is currently available only for Windows nodes.

Result of sanitization can be either downloaded on the scan page or retrieved the data ID via REST. See [Fetch Scan Result](#). Note that /hash API does not provide such information.

Length of time the system stores sanitized files can be set in **Settings > Data retention**.

Modify Workflow

WORKFLOW NAME

WorkFlow-1

DESCRIPTION

Selecting this template all files will be processed without any filtering.

[←](#)
[ARCHIVE](#)
[BLACKLIST](#)
[WHITELIST](#)
[SCAN](#)
[METADEFENDER CLOUD](#)
[DATA SANITIZATION](#)
[→](#)

CONVERSION TIMEOUT [IN MINUTES] ⓘ

5

TRY COUNT ⓘ

3

OUTPUT FILENAME FORMAT

`$(original.basenamelong)_sanitized_by_OPSSWAT_MetaDefender_$(dataid).$(converted.extension)`

OFFICE DOCUMENTS

<input type="checkbox"/>	MICROSOFT WORD DOCUMENT (.DOC)	doc
<input type="checkbox"/>	WORD MICROSOFT OFFICE OPEN XML FORMAT DOCUMENT (.DOCX)	docx
<input type="checkbox"/>	OPENDOCUMENT TEXT (.ODT)	odt
<input type="checkbox"/>	POWERPOINT MICROSOFT OFFICE OPEN XML FORMAT DOCUMENT (.PPTX)	pptx

Data sanitization

Data Loss Prevention (DLP)

Using this feature, sensitive data can be prevented acquiring them by an unauthorized party. There are two special type of data that the DLP engine can identify automatically:

- Social Security Number
- Credit Card Number.

Using regular expressions, custom texts can be searched for.

With the context option, the number of words to show before and after a hit can be given.

Data Loss Prevention

DLP configuration options

On the Technologies page, clicking on the line of the DLP engine then on the Settings text on the top right corner of the popup window, the configuration options for the DLP engine appear.

DLP engine configuration

Options:

- "Mask numbers in CCN/SSN hits": On the result page, the found CCN/SSN numbers will be masked with "X"s.
- "Mask regex matches": On the result page, texts matching regex will be masked with "X"s.
- "Parse binary files": Choosing this option, sensitive data will be searched for in files that cannot be converted to text.

Advanced

By enabling 'Quarantine blocked files' all of the files which are blocked are automatically copied to the quarantine. For detailed description of the quarantine please see the [Quarantine page](#).

By enabling 'Fallback filetype detection to current extension if needed' (default enabled), file type detection can use the extension of the currently processed file as a helping hand. For example this could be useful, when analyzing CSV files.

By enabling 'OVERRIDE SCAN RESULTS CLASSIFIED AS ALLOWED' it is possible to overwrite the default behaviour of MetaDefender and determine which scan verdicts should result as allowed.

Scan results checked are marked as allowed.

By default only 'No Threat Detected' and 'Skipped Clean' verdicts result in allowed status.

Modify Workflow

WORKFLOW NAME

WorkFlow-1

DESCRIPTION

Selecting this template all files will be processed without any filtering.

[BLACKLIST](#) [WHITELIST](#) [SCAN](#) [METADEFENDER CLOUD](#) [DATA SANITIZATION](#) **[ADVANCED](#)**

- QUARANTINE BLOCKED FILES ⓘ
- FALLBACK FILETYPE DETECTION TO CURRENT EXTENSION IF NEEDED ⓘ
- OVERRIDE SCAN RESULTS CLASSIFIED AS ALLOWED ⓘ
 - NO THREAT FOUND
 - THREAT FOUND
 - SUSPICIOUS
 - FAILED TO SCAN
 - WHITELISTED
 - BLACKLISTED
 - NOT SCANNED
 - ENCRYPTED ARCHIVE
 - EXCEEDED ARCHIVE DEPTH
 - EXCEEDED ARCHIVE SIZE
 - EXCEEDED ARCHIVE FILE NUMBER
 - EXCEEDED ARCHIVE TIMEOUT
 - FILETYPE MISMATCH
 - PASSWORD PROTECTED DOCUMENT
 - POTENTIALLY VULNERABLE FILE

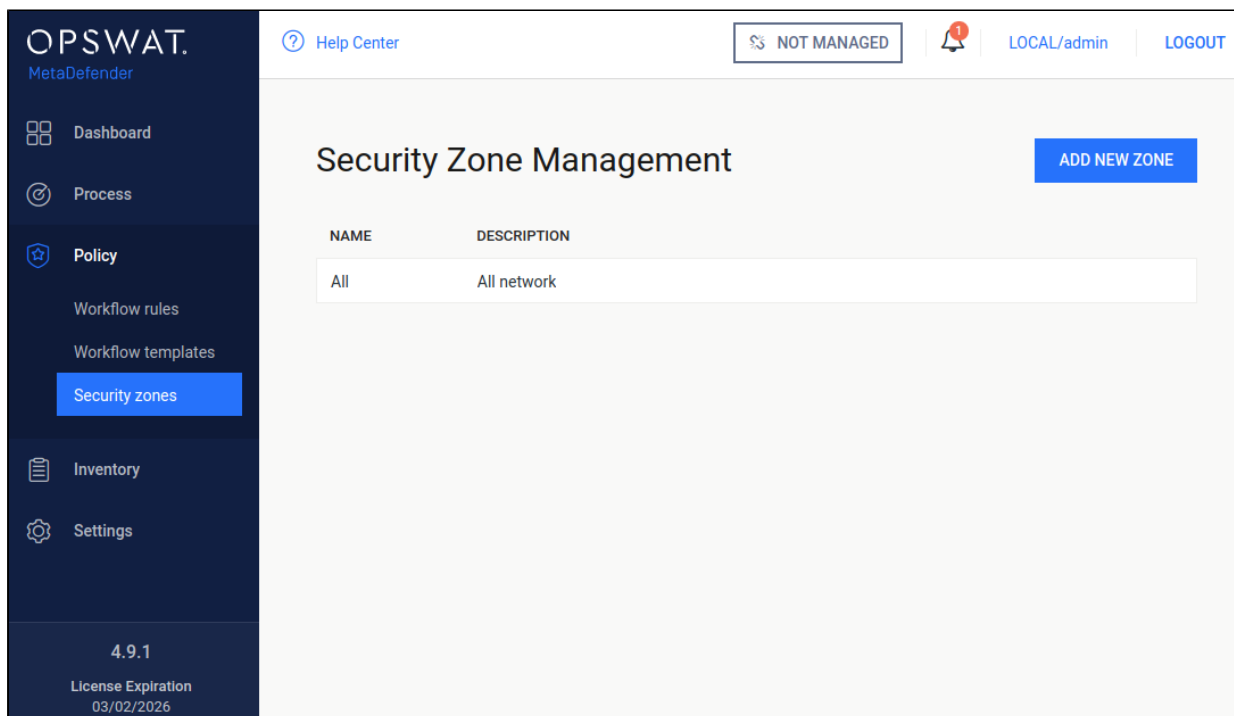
SAVE CHANGES

CANCEL

Advanced

3.6.3. Security zone configuration

The Security zone page is found under **Policy > Security zones** after successful login.



The screenshot shows the OPSWAT MetaDefender interface. The left sidebar contains navigation options: Dashboard, Process, Policy (selected), Workflow rules, Workflow templates, Security zones (highlighted), Inventory, and Settings. The main content area is titled "Security Zone Management" and features an "ADD NEW ZONE" button. Below the title is a table with columns "NAME" and "DESCRIPTION". The table contains one entry: "All" with the description "All network". The top right of the interface shows a "NOT MANAGED" status, a notification bell, the user "LOCAL/admin", and a "LOGOUT" link. The bottom left of the sidebar displays the version "4.9.1" and the license expiration date "03/02/2026".

Security zone

The following actions are available:

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

Each zone contains a name, description and multiple network masks. Both IPv4 and IPv6 network zones are supported.

3.6.4. Workflow rule configuration

The Workflow rule page is found under **Policy > Workflow rules** after successful login.

The rules represent different processing profiles.

OPSWAT
MetaDefender

Help Center

NOT MANAGED LOCAL/admin LOGOUT

Workflow Rules Management

ADD NEW RULE

NAME	DESCRIPTION
Kiosk	File process with Kiosk
MetaDefender Vault	File process with MetaDefender Vault
File process	File process
File process witho...	File process without archive

4.9.1
License Expiration
03/02/2026

Workflow rules

The following actions are available:

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

Rules combine workflow templates and security zones and describe which workflows are available in a specified security zone. Multiple rules can be added for the same security zone.

Configuration

Once clicking on a rule, a window pops up where beside the rule properties all the chosen rule's options are shown on the different tabs.

The screenshot shows the OPSWAT MetaDefender interface. On the left is a dark blue sidebar with navigation options: Dashboard, Process, Policy (selected), Workflow rules (highlighted), Workflow templates, Security zones, Inventory, and Settings. At the bottom of the sidebar, it shows version 4.9.1 and a license expiration date of 03/02/2026. The main content area is titled 'Workflow Rule...' and contains a list of rules: 'Kiosk', 'MetaDefender Vault', 'File process', and 'File process without archive'. The 'Kiosk' rule is selected. To the right is a 'Modify Rule' form with the following fields: 'NAME' (Kiosk), 'DESCRIPTION' (File process with Kiosk), 'APPLY TO ZONE' (All), 'USE WORKFLOW TEMPLATE' (Default), 'USE CERTIFICATE TO GENERATE BATCH SIGNATURE' (unchecked), 'CERTIFICATE USED FOR BATCH SIGNING' (None), and 'CERTIFICATE VALIDITY [IN HOURS]' (24). At the bottom of the form are 'SAVE CHANGES' and 'CANCEL' buttons. The top right of the interface shows 'NOT MANAGED', a notification bell, 'LOCAL/admin', and 'LOGOUT'.

Modifying workflow rules

On this page it is possible to enable local file scanning by checking the **ALLOW SCAN FILES ON SERVER** checkbox. By enabling this feature a local scan node is able to scan the files at their original place if the files' location is allowed in the list below the checkbox. For example if this list has *C:\data* in it, then all files under that folder (e.g.: *C:\data\not_scanned\JPG_213134.jpg*) are allowed to be scanned locally if it is chosen. For UNC file paths you have to check the permissions because if the service does not have the correct rights it cannot access network folders or network shared files.

Various accessibility options can be set on this page. You can define one of three visibility levels for the scan results for each role in the **VISIBILITY OF SCAN RESULT** field:

VISIBILITY OF SCAN RESULT

ROLE VISIBILITY [Delete](#)

RESTRICT ACCESS TO FOLLOWING ROLES

[Add](#)

- Full details: all information for a scan is displayed

file.txt [PROCESS NEW FILE](#)

NO THREAT DETECTED
0 / 1

None of the engines found a threat

UPLOADED 2018-08-31 15:56:35 GMT+2	SCANNED 2018-08-31 15:56:35 GMT+2
FILE TYPE UTF-8 Unicode text	FILE SIZE 311 B

VULNERABILITY LEVEL ⓘ
|||||

DATA LOSS PREVENTION ⓘ
NOT DETECTED ✓

MULTISCANNING

ENGINE	SCAN TIME	DEFINITION DATE	RESULT
✓ ClamAV	1 ms	2018-01-26(7 months ago)	No Threat Detected

MD5 3d833e2ef9b62e5c164e7d86906c9c7	<input type="button" value="COPY"/>
SHA1 834481369b71807c368e78c9c6d87b217fc59e81	<input type="button" value="COPY"/>
SHA256 ca56191836c07680922ccad1c6665d88e125ff51f69a187b6e81494d5021d72c	<input type="button" value="COPY"/>

- Per engine result: Scan details are displayed except per engine scan time and definition date.

file.txt PROCESS NEW FILE

NO THREAT DETECTED
0 / 1

None of the engines found a threat

UPLOADED 2018-08-31 15:56:35 GMT+2	SCANNED 2018-08-31 15:56:35 GMT+2
FILE TYPE UTF-8 Unicode text	FILE SIZE 311 B

VULNERABILITY LEVEL ⓘ UNKNOWN |||||

DATA LOSS PREVENTION ⓘ NOT DETECTED ✔

MD5 3d833e2fef9b62e5c164e7d86906c9c7	COPY
SHA1 834481369b71807c368e78c9c6d87b217fc59e81	COPY
SHA256 ca56191836c07680922ccad1c6665d88e125ff51f69a187b6e81494d5021d72c	COPY

MULTISCANNING

ENGINE	SCAN TIME	DEFINITION DATE	RESULT
✔ ClamAV	-	-	No Threat Detected

- Overall result only: Only the overall verdict is displayed.

file.txt PROCESS NEW FILE

/

UPLOADED 2018-08-31 15:56:35 GMT+2	SCANNED N/A
FILE TYPE UTF-8 Unicode text	FILE SIZE 311 B

VULNERABILITY LEVEL ⓘ UNKNOWN |||||

DATA LOSS PREVENTION ⓘ NOT DETECTED ✔

MD5 3d833e2fef9b62e5c164e7d86906c9c7	COPY
SHA1 834481369b71807c368e78c9c6d87b217fc59e81	COPY
SHA256 ca56191836c07680922ccad1c6665d88e125ff51f69a187b6e81494d5021d72c	COPY

MULTISCANNING

ENGINE	SCAN TIME	DEFINITION DATE	RESULT
Unauthorized to view detailed scan result.			

There are also two special roles - **Every authenticated** refers to any logged in user, while **Everybody** refers to any user. Without belonging to any role specified within the rule, the user has no access to view the scan results. The usage of the rule to given roles can also be restricted with the **RESTRICT ACCESS TO FOLLOWING ROLES** field.

Clicking on a tab it is possible to overwrite a property that was previously defined inside the workflow template.

An option if changed will only overwrite the specific property for the underlying rule and makes no modification on the original workflow template that was chosen by the rule.

This means that several rules can be created using the same workflow template overwriting different options while the untouched properties will remain as they were set in the workflow template.

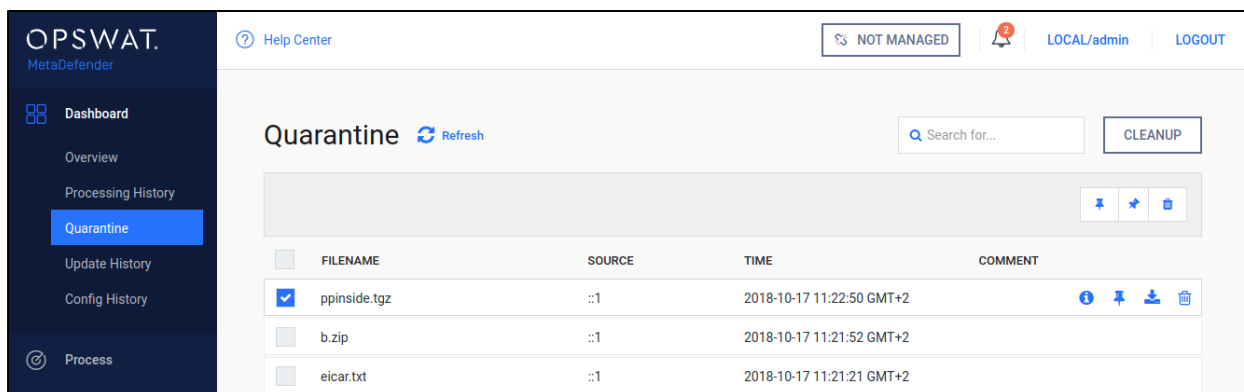
Rules are processed in order, the first matching rule will be used for the request. You can change order of rules via drag&drop in the Web Management Console. If there is no rule that matches for the client (source IP address), then the scan request will be denied.


3.6.5. Quarantine

Options

The quarantine is for keeping blocked files in a separated place. It can be used by configuring workflows (see [Advanced section on Workflow template configuration page](#)).

On the **Quarantine** page (**Dashboard** → **Quarantine**), the following operations can be performed on the files:



1. By clicking on the  , item details appear
2. Pinned files won't be removed on clean-ups. Use the pin icon to do so.
3. For removing the files from the list, please use the bin icon.
4. Files can be downloaded by clicking the download icon.

The first three operations can also be performed in bulk using the check-boxes before the filenames and clicking the action icons above the file list.

3.7. Logging

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

- [3.7.1. Configuration](#)

- [3.7.2. Debug logging](#)

3.7.1. Configuration

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

- [Startup Core Configuration](#)
- [Startup Node Configuration](#)

For Linux systems the installer configures the **logrotate** service to handle the Metadefender Core log files.

Configuration files are located:

- `/etc/logrotate.d/ometascan`
- `/etc/logrotate.d/ometascan-node`

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.



Permissions to set:

- The directory that contains the logs: read, write and execute permissions for ometascan user or at least for ometascan group
- The other directories on the path to the logs: at least read and execute permissions for ometascan user and/or ometascan group

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

3.7.2. Debug logging

To provide debug logs for the OPSWAT support team, the level of the logfile for the given service (ometascan or ometascan-node) 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 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 Metadefender Core Log?](#)

3.8 Security settings on web console

- [3.8.1 Enabling HTTPS](#)
- [3.8.2 Session timeout](#)

3.8.1 Enabling HTTPS

MetaDefender Core supports accessing Web UI and REST interface via HTTPS. This feature is not enabled by default. There are two ways to enable the feature:

- via Management Console or
- modifying MetaDefender Core server configuration via configuration files.



If HTTPS is configured via both ways, only the settings made on Management Console will take effect. It is highly recommended not to use both configuration files and user interface for HTTPS settings at the same time.

Enabling HTTPS via Management Console

1. Go to **Settings**→**Security** page

OPSWAT.
MetaDefender

Help Center NOT MANAGED LOCAL/admin LOGOUT

Dashboard
Process
Policy
Inventory
Settings
Update Settings
Data Retention
Security
User Management
License
Configuration
Password

4.12.0
License Expiration
03/02/2026

Security

SAVE SETTINGS

HTTPS Configuration

ENABLE HTTPS CONNECTION

CERTIFICATE
There are no available certifications.
Please go to [Inventory / Certificates](#).

Session Configuration

ABSOLUTE SESSION TIMEOUT
User session length in minutes: Sessions will be invalid after the given time regardless of the user activity (0 = no limit)

10

- If there's no certificate-key pair added to the inventory, [please go to Inventory](#)→[Certificates page](#) and add one that is desired to use for securing HTTP connections.

OPSWAT.
MetaDefender

Help Center NOT MANAGED LOCAL/admin LOGOUT

Dashboard
Process
Policy
Inventory
Settings
Update Settings
Data Retention
Security
User Management
License
Configuration
Password

4.12.0
License Expiration
12/31/2019

Security

SAVE SETTINGS

HTTPS Configuration

ENABLE HTTPS CONNECTION

CERTIFICATE
[Empty dropdown menu]

Session Configuration

ABSOLUTE SESSION TIMEOUT
User session length in minutes: Sessions will be invalid after the given time regardless of the user activity (0 = no limit)

0

3. Tick *Enable HTTPS connection* checkbox and choose a certificate-key pair.

The screenshot shows the OPSWAT MetaDefender interface. On the left is a dark blue sidebar with navigation options: Dashboard, Process, Policy, Inventory, Settings (highlighted), Update Settings, Data Retention, User Management, License, Configuration, and Password. At the bottom of the sidebar, it displays version 4.12.0 and license expiration 12/31/2019. The main content area is titled 'Security' and contains two sections: 'HTTPS Configuration' and 'Session Configuration'. In the 'HTTPS Configuration' section, the 'ENABLE HTTPS CONNECTION' checkbox is checked, and a dropdown menu for 'CERTIFICATE' is open, showing 'CertForHTTPS' selected. The 'Session Configuration' section has an 'ABSOLUTE SESSION TIMEOUT' field with the value '0'. A 'SAVE SETTINGS' button is located in the top right corner of the main content area.

4. As clicking on *Save settings*, you will be warned that Management Console is going to be restarted and this will take some time.

The screenshot shows a modal dialog box titled 'Save security settings'. The text inside the dialog asks: 'Are you sure you want to save Security Configuration? Please note that by submitting changes, the management console will be restarted and will not be accessible for about 30 seconds.' There are two buttons: 'SAVE' (highlighted in blue) and 'CANCEL'. In the background, the 'Session Configuration' section of the main page is visible but dimmed, showing the 'ABSOLUTE SESSION TIMEOUT' field with the value '0' and a 'SAVE SETTINGS' button in the top right corner.

5. Approximately 30 seconds after confirming saving of configuration the Management Console will be reloaded via HTTPS.

Enabling HTTPS via configuration files

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

On Linux

1. Create file `ssl.conf` in the directory `/etc/ometascan/nginx.d`
2. Enter SSL-configuration according to Nginx. To allow simple SSL one needs to add the following lines only:

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

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

On Windows

1. Create file `ssl.conf` in the directory `<Installation Directory>\nginx`.
2. Enter SSL-configuration according to Nginx. To allow simple SSL one needs to add the following lines only (note the forward "/" slashes)

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

3. A restart of the "OPSWAT Metadefender Core" service is required.

ⓘ '\n' sequences in paths

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

For example the following directive

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

will appear at nginx as

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

As a workaround instead of backslash '\' use

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

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

Note: When choosing location for cert and key files, make sure the files are in a location which is readable to the service user.

For more SSL-options please consult [Nginx documentation](#).

3.8.2 Session timeout

User sessions can be terminated regardless of user activity. Under the **Settings** menu, on the **Security** page, a timeout value can be given in minutes, in order to limit the length of a user session. After the given time elapsed, the user session will be terminated even if it is during an operation.

The screenshot shows the OPSWAT MetaDefender web management console. The left sidebar contains navigation options: Dashboard, Process, Policy, Inventory, Settings (highlighted), Update Settings, Data Retention, Security, User Management, License, Configuration, and Password. The main content area is titled 'Security' and includes a 'SAVE SETTINGS' button. Under 'HTTPS Configuration', the 'ENABLE HTTPS CONNECTION' checkbox is checked. Below it, the 'CERTIFICATE' section states 'There are no available certifications. Please go to [Inventory / Certificates](#).' Under 'Session Configuration', the 'ABSOLUTE SESSION TIMEOUT' is set to 10 minutes. The top right of the page shows 'NOT MANAGED', a notification bell with '2', and user information 'LOCAL/admin' with a 'LOGOUT' link. The bottom left of the sidebar shows the version '4.12.0' and 'License Expiration 03/02/2026'.

3.9. Configuring proxy settings

How can I set proxy server for the product

Linux

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

Windows

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

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



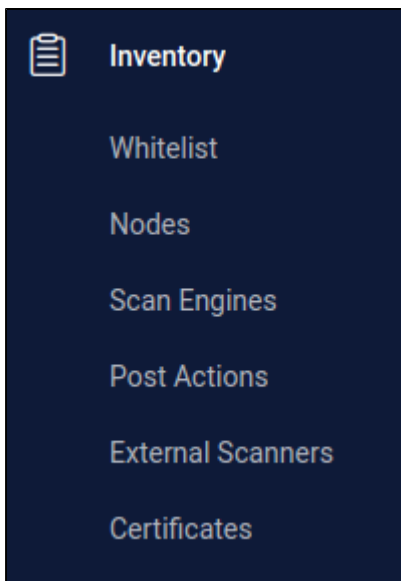
You might need to configure Windows proxy to bypass local addresses if you can't access Web Management Console from the host itself. Consult netsh documentation for additional configuration options.

3.10. External Scanners And Post Actions

Under **Inventory** menu it is possible to configure custom **External Scanners** and custom **Post Actions**.

For both these options we must enter two fields:

- a unique name (maximum 16 character ASCII only text)
- a full path to your executable/interpreter, that will be called by the scan node



External Scanners

External Scanners are handled as scan engines from product side but are not updatable through the product.

Specification for external scanner process

- **INPUT**
 - on standard input it gets the currently available scan result JSON without the `extracted_files` field
 - as last argument on the command line it gets the absolute path for the file to scan
- **OUTPUT**
 - if everything goes well return value must be 0, non-zero return value indicates this scanner **Failed**.
 - scan result must be put on standard output in JSON format with the following fields

- **def_time**: the definition time of this scanner in milliseconds since epoch that will be displayed by Metadefender Core V4
- **scan_result_i**: the scan verdict for the file, see https://onlinehelp.opswat.com/corev3/Description_of_Scan_Results.html
- **threat_found**: the found threat's description if any
- If any of the above fields is missing or invalid, the result will automatically be **Failed** for this scanner

i Number of External Scanners is a separately licensed feature. If you plan to use this feature please contact your OPSWAT reseller.

Example for a Custom Scanner

NAME

ExtScn_01

SCANNER

/usr/bin/custom_engine --log-level debug

Example input for a Custom Scanner

```
{
  "data_id": "091c07fe6203479983682f3b4a491ee6",
  "file_info": {
    "display_name": "archive.zip",
    "file_size": 2123967,
    "file_type": "application\zip",
    "file_type_description": "ZIP compressed archive",
    "md5": "ec8fa3c2897c0956f0e9ed5c092310b9",
    "sha1": "0027fc18ed97063387bca9c518a02a6faba85c38",
    "sha256": "4fb0083cd3cd966817c1ee4fa3f02519d05eca0b57c2bf71109d3bd69acebd41",
    "upload_timestamp": "2017-04-27T13:05:20.435Z"
  },
  "process_info": {
    "blocked_reason": "Infected",
    "file_type_skipped_scan": false,
    "post_processing": {
```

```

    "actions_failed": "",
    "actions_ran": "",
    "converted_destination": "",
    "converted_to": "",
    "copy_move_destination": ""
  },
  "profile": "File scan",
  "progress_percentage": 100,
  "result": "Blocked",
  "user_agent": "webscan"
},
"scan_results": {
  "data_id": "091c07fe6203479983682f3b4a491ee6",
  "progress_percentage": 100,
  "scan_all_result_a": "Infected",
  "scan_all_result_i": 1,
  "scan_details": {
    "ClamAV": {
      "def_time": "2017-04-27T06:59:21.000Z",
      "location": "local",
      "scan_result_i": 1,
      "scan_time": 51,
      "threat_found": "Win.Trojan.Trojan-1082 FOUND"
    }
  },
  "start_time": "2017-04-27T13:05:20.471Z",
  "total_avs": 1,
  "total_time": 1444
},
"vulnerability_info": {}
}

```

Example valid output of a Custom Scanner

```

{
  "def_time": 1491288912392,
  "scan_result_i": 0,
  "threat_found": ""
}

```

Example scan result where External Scanner found the file to be clean

```

...
"scan_results": {
  "data_id": "091c07fe6203479983682f3b4a491ee6",

```

```

"progress_percentage": 100,
"scan_all_result_a": "Infected",
"scan_all_result_i": 1,
"scan_details": {
  "ClamAV": {
    "def_time": "2017-04-27T06:59:21.000Z",
    "location": "local",
    "scan_result_i": 1,
    "scan_time": 51,
    "threat_found": "Win.Trojan.Trojan-1082 FOUND"
  },
  "ExtScn_01": {
    "def_time": "2017-02-27T05:19:11.000Z",
    "location": "local",
    "scan_result_i": 0,
    "scan_time": 10,
    "threat_found": ""
  }
},
"start_time": "2017-04-27T13:05:20.471Z",
"total_avs": 1,
"total_time": 1444
...

```

Post Actions

Post Actions run after the scan of the file for any post functionality such as copying the file etc...

Specification for post action process

- **INPUT**
 - on standard input it gets the currently available scan result JSON without the `extracted_files` field
 - as last argument on the command line it gets the absolute path for the file
- **OUTPUT**
 - if everything goes well return value must be 0, non-zero return value indicates this action **Failed**.

Adding a Post Action is the same as in case of an External Scanner. The only difference is in the result handling.

All executed Post Action's result will be on the `process_info.post_processing` object of the scan result JSON. If the return value of an action is zero it will be shown in the `actions_ran` field, if the return value of the action is non-zero then it will be listed in the `actions_failed` field.

Example of a Post Action

Add new post action

NAME

Pst_Act_01

ACTION

/home/admin/scripts/copy_if_infected --log-level WARNING

The scan result JSON if the Post Action returns 0

```
...
  "process_info": {
    "blocked_reason": "Infected",
    "file_type_skipped_scan": false,
    "post_processing": {
      "actions_failed": "",
      "actions_ran": "Pst_Act_01",
      "converted_destination": "",
      "converted_to": "",
      "copy_move_destination": ""
    },
    "profile": "File scan",
    "progress_percentage": 100,
    "result": "Blocked",
    "user_agent": "webscan"
  },
  ...
```

The scan result JSON if the Post Action returns non-zero

```
...
  "process_info": {
    "blocked_reason": "Infected",
    "file_type_skipped_scan": false,
    "post_processing": {
      "actions_failed": "Pst_Act_01 failed",
      "actions_ran": "",
    },
  },
  ...
```



```

    "converted_destination": "",
    "converted_to": "",
    "copy_move_destination": ""
  },
  "profile": "File scan",
  "progress_percentage": 100,
  "result": "Blocked",
  "user_agent": "webscan"
},
...

```

3.11. Yara rule sources

Under **Inventory/Technologies** menu it is possible to configure custom **Yara sources**.

Technologies						UPLOAD PACKAGE	UPDATE ALL	
						Last update: 3 minutes ago Next update: in 4 hours Edit Update Settings		
TECHNOLOGY	LAST UPDATE	ACTIVITY	ENGINE	DATABASE	ENABLED			
Anti-malware engines	No available engine				<input type="checkbox"/>			
Data Sanitization (CDR)	No available engine				<input type="checkbox"/>			
Data Loss Prevention	No available engine				<input type="checkbox"/>			
Yara	Never	No node connected		1539256809627 (downloaded)	<input type="checkbox"/>			
SOURCE	SOURCE TYPE	LAST UPDATE					Add source	Generate package
No sources added.								

To add new source, click on **Add new source** button. You can specify the type of the source, and the URL itself. The product supports 2 type of Yara sources: network source (HTTP /HTTPS) and local directory. A network source must be a zip file. The content of the zip file will be used by the Yara engine. As a local directory, you can set a local path on the computer. This path must point to a directory. A copy of this directory will be used by the Yara engine.

Add new source

SOURCE TYPE

Local directory ▼

SOURCE

Source

To generate a package, click on the **Generate package** button. This will start the process, and the start time will be shown next to the buttons. Next to the sources, you can enable or disable the sources. Disabled sources will not be used when generating the next package.

Sources can be modified by clicking the row, and removed by clicking the trash icon on the right side of the rows.

4. Scan files with Metadefender Core

There are several ways to scan files with Metadefender Core:

- [Scan Files via REST API](#)
- [Scan Files via Web Interface](#)

Scan Files via REST API

The Metadefender Core server also provides a REST API to interface with the application. To scan a file even the user interface uses this API.

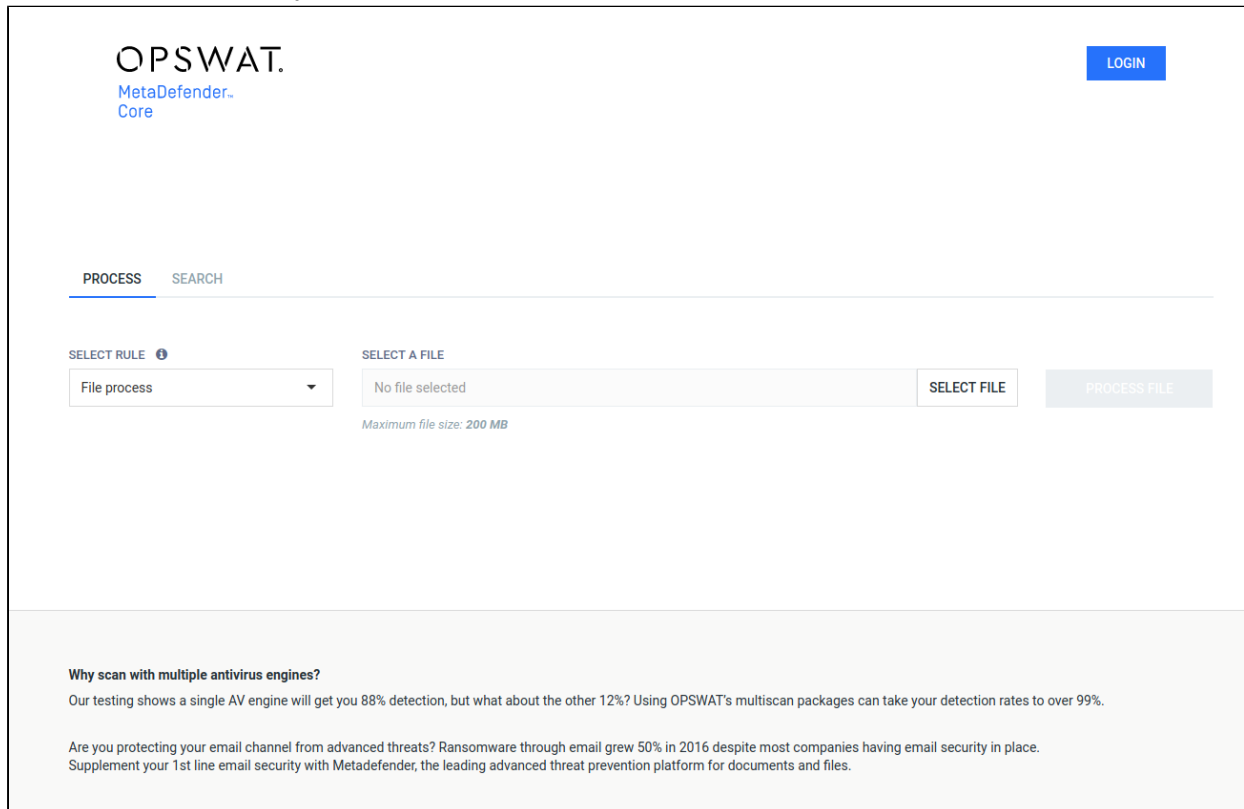
Chunked transfer encoding is not supported to upload files for scanning.

All the responses from the server are in JSON format for easy parsing.

For more information on how to use the REST API please check our [developer guide](#).

Scan Files via Web Interface

Once you open your browser and go to the Metadefender Core server's URL the public file scan interface will be displayed.



The screenshot shows the OPSWAT MetaDefender Core web interface. At the top left, the logo "OPSWAT. MetaDefender. Core" is displayed. In the top right corner, there is a blue "LOGIN" button. Below the logo, there are two tabs: "PROCESS" (which is active and underlined) and "SEARCH". The main content area features a "SELECT RULE" dropdown menu with "File process" selected, and a "SELECT A FILE" section with a "No file selected" message and a "SELECT FILE" button. To the right of the "SELECT FILE" button is a "PROCESS FILE" button. Below these controls, there is a note: "Maximum file size: 200 MB". At the bottom of the interface, there is a section titled "Why scan with multiple antivirus engines?" with text explaining that using OPSWAT's multiscan packages can increase detection rates to over 99% compared to a single AV engine's 88%. Another line of text asks if the user is protecting their email channel from advanced threats like ransomware, noting a 50% increase in 2016 and recommending Metadefender as a supplement to email security.

Scan

Choose what to scan and how

There are two option fields in the middle of the page. Next to them there is the **SCAN** button. With the leftmost option you can select between the available workflows for the public file scanning.

These workflows are determined by the Metadefender Core administrators, so it is possible that only one workflow will be available for public scanning, or even none.

The next option is where you choose the file to scan. Click on the **SELECT A FILE** button and browse to the file to be scanned.

Start scanning

When ready click on the **SCAN** button. A progress bar will appear.

Progress of scanning

Once the file is uploaded the file will be scanned.

On the left you will see a circle with text in it. The outer circle will start filling up, indicating that scanning is in progress. Once the circle is full, the scan is complete.

The color of the circle and the text inside refer to possible threats found in the file.

The numbers in the circle represent how many of the active AV engines found a threat inside the object, A/B where A is the number of engines which found the file harmful and B is the number of all active engines.

To the right to the circle you will find some details of the uploaded file generated by Metadefender Core.

At the bottom of the page a list of the active AV engines will be displayed along with the details of each related to the object scanned.

5. Data Sanitization

Please check the latest Data Sanitization document [here](#).

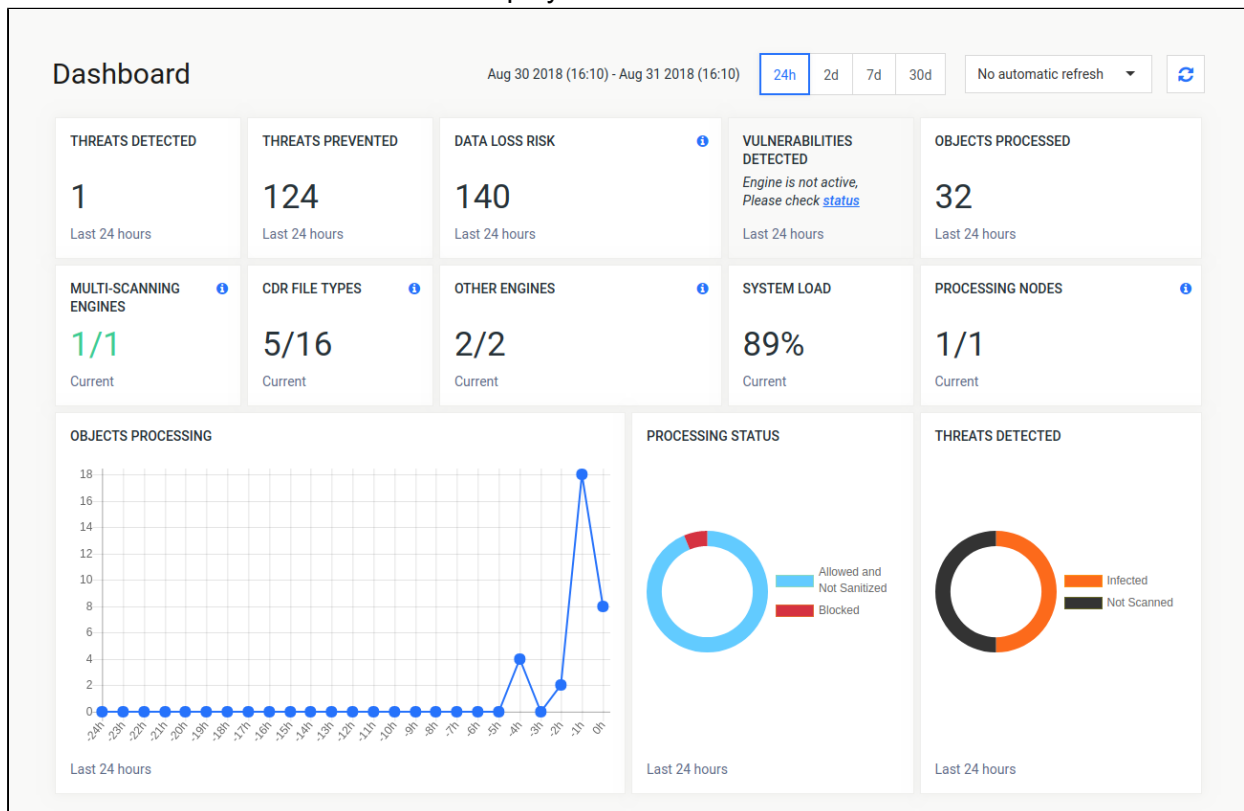
6. Operating Metadefender Core

- 6.1. Dashboard
- 6.2. Inventory Management
- 6.3. Regular Maintenance
- 6.4 Import/Export configuration

6.1. Dashboard

MetaDefender Core provides a Web-based user interface (default port is 8008) that gives a general overview of MetaDefender Core status and allows you to configure its options.

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



Dashboard overview

Overview page

The Overview page shows information on

- Number of threats detected

- Number of files sanitized
- Number of detected vulnerabilities
- Total number of files processed
- Average load of all nodes
- Number of active anti-virus engines against total number of AV engines
- The proportion of used and usable Data Sanitization file types
- Number of known CVEs and file hashes in the vulnerability database
- The proportion of used and usable non-AV engines (external scanners, filetype and archive engines)
- Number of connected nodes
- Number of scanned objects in the last 30 days
- Statistics on number of processed files in time (line chart)
- Statistics on processing results (two doughnut charts)

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

Scan history

The Scan History page shows information on all scans made on the MetaDefender Core.

If an archive was scanned, its details popup will include tabs for the original files scan details and also a list with the results of the contained files.

On the Scan history page you can also search for MD5, SHA1, SHA256 hashes and for filenames and you can limit search result for a specific scan result.

There is an option to export scan history in CSV or STIX format. For the export, the scan history filters will be applied. The user can export STIX file by clicking on STIX export button. In addition to set scan history filters, STIX file will contain only blocked scans. After the desired time range selected, the download will be started by clicking on the OK button. CSV file is accessible by clicking on the CSV export button, and pressing OK after the desired time range selected.

Quarantine

The Quarantine page shows all scanned files which are copied to the quarantine. Each of them can be pinned to avoid removal on cleaning up. Also comments can be written to each quarantined file. Quarantine log can be searched for comment, file name and source of the scan request.

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.

6.2. Inventory Management

Metadefender Core displays detailed information on scan nodes and the status of engine updates including anti-malware engines, archive engines, etc.

- [Certificates](#)
- [Nodes](#)
- [Skip by hash](#)
- [Technologies](#)

Certificates

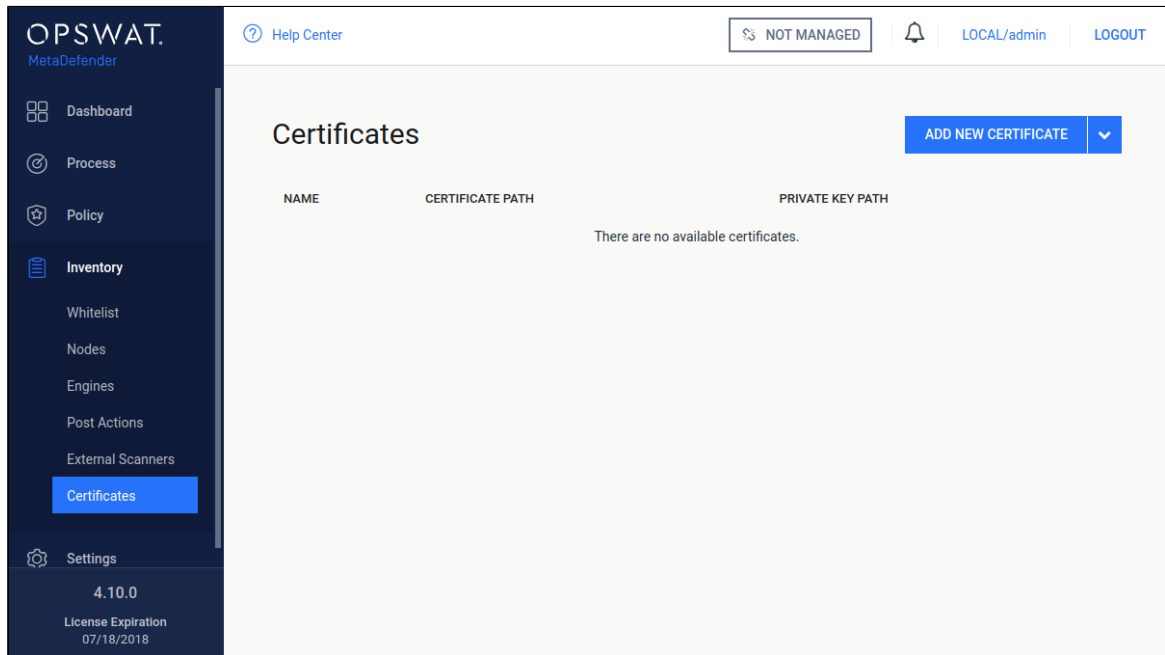
On this page, path to certificates and private keys for signing scan batches or HTTPS configuration can be given.



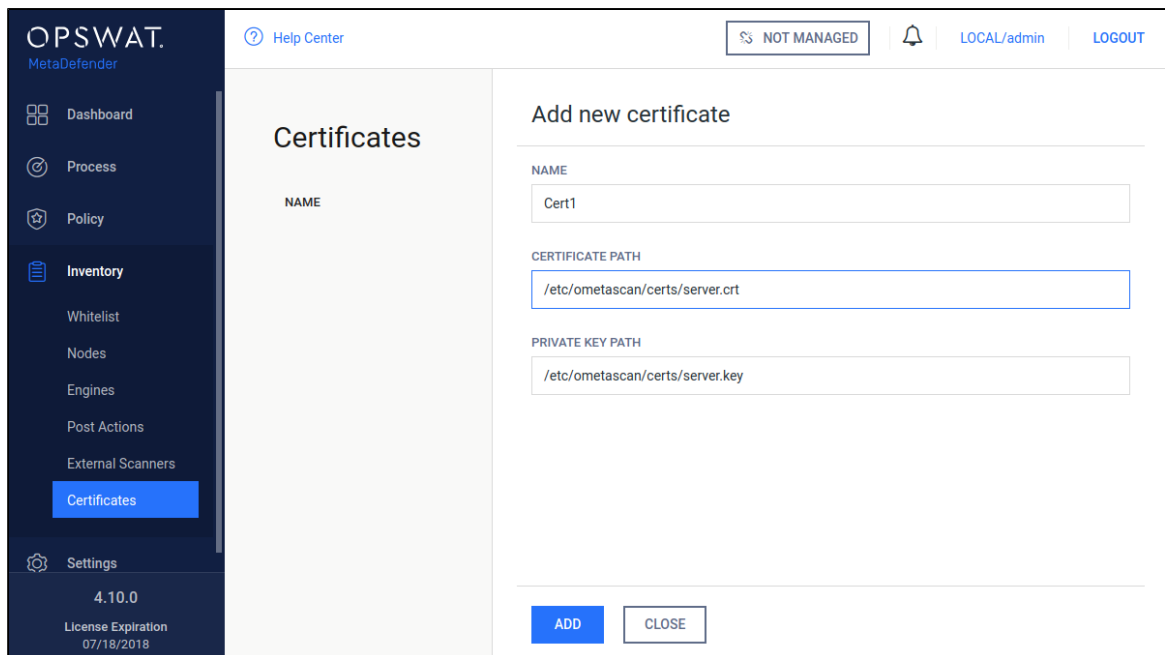
- Certificate should be in a Base64-encoded X.509 certificate file (.crt, .cer) format.
- Private key should be a privacy-enhanced electronic mail file (.pem) format and it should not be locked by password.

Adding certificate-key pair to the inventory

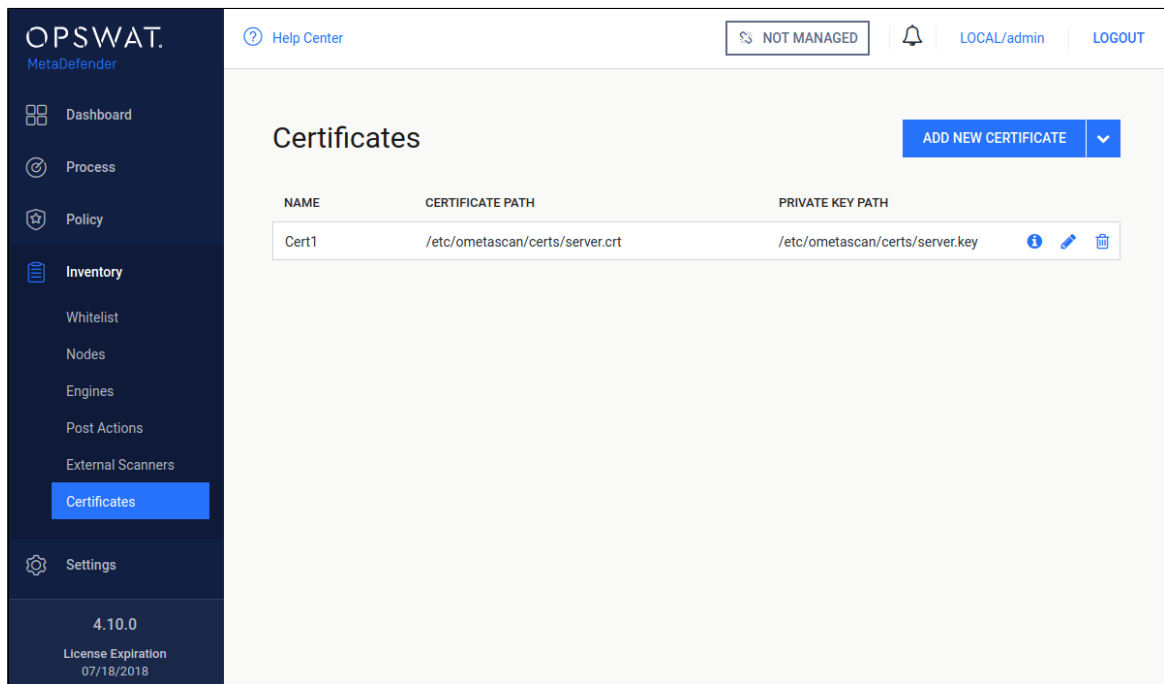
1. Go to **Inventory**→**Certificates** page
2. Click on **Add new certificate** button



3. Fill the **Add new certificate** form by giving a name, a path to certificate file and a path to the corresponding key file

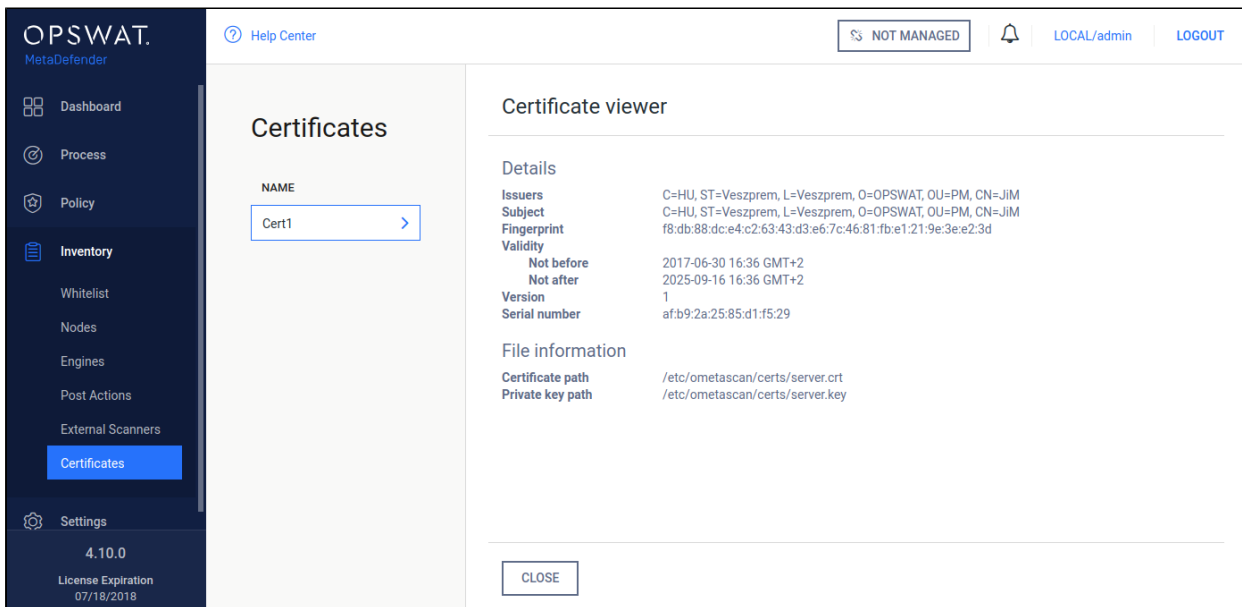


4. Click **Add** button




Checking the details of a certificate

By clicking the line of the certificate, the "Certificate viewer" pops up and shows the details of the certificate.



Modifying the name or the paths of a certification

Hover the mouse cursor over the line that is to be modified and click on the pen picto. The **Modify certificate** modal pops up and the fields can be edited.

 The certificate file and the key file should be readable by the user who owns the ometascan process.

Nodes

Under the **Nodes** menu the connected nodes are listed with the following information:

- Address of the node
- Actual load of the node
- Number of CPU cores of the node
- Free disk space on the node
- Total memory of the node
- Version of installed Metadefender Core
- Operating system with version (and distribution) information
- Number of active engines / number of installed engines on the node (including archive and filetype engines)
- Status of the node

OPSWAT.
MetaDefender

Help Center

NOT MANAGED

LOCAL/admin

LOGOUT

Process Nodes

ADDRESS	ACTUAL LOAD	CPU CORES	FREE DISK SPACE	TOTAL MEMORY	NODE VERSION	OS	INSTALLED ENGINES	STATUS
localhost	35%	4	568.94 GB	5.67 GB	4.11.0.265	CentOS Linux 7 (Core)	8/8	✓

4.11.3
License Expiration
09/30/2027

Nodes

Information

When clicking on an node a window pops up showing different tabs corresponding to different properties.

On top left corner of this window the status, address, operating system and version information can be seen.

On top right corner a visual confirmation about engines with a pie chart is shown.

The screenshot displays the OPSWAT MetaDefender interface. On the left is a dark sidebar with navigation items: Dashboard, Process, Policy, Inventory (with sub-items: Technologies, Whitelist, Nodes, Post Actions, External Scanners, Certificates), and Settings. The main content area is titled 'Process Nodes' and features a table with the following data:

ADDRESS	ACTUAL LOAD	INSTALLED ENGINES
localhost	30%	8/8

To the right of the table is the 'Node details' section, which includes a 'CLOSE' button at the bottom. The details are as follows:

- STATUS: The node is operational
- ADDRESS: localhost
- OS: CentOS Linux 7 (Core)
- VERSION: 4.11.0.265

A circular gauge on the right side of the 'Node details' section shows 'ENGINES 8/8'. Below the details are three tabs: 'ISSUES', 'ENGINES', and 'HARDWARE INFO'. The top right of the interface shows a 'NOT MANAGED' status, a notification bell, the user 'LOCAL/admin', and a 'LOGOUT' button. The bottom left corner of the sidebar indicates the version '4.11.3' and 'License Expiration 09/30/2027'.

Information pop-up

Issues

On the Issues tab the issues of node and engines are shown.

To solve typical issues related to node issues visit page [Possible Issues on Nodes](#).

Engines

On the Engines tab information of engines such as name, type and version of engine is shown.

Hardware info

The last tab shows hardware information such as number of used cores, total memory and free disk space.

Skip by hash

This page contains three lists which belong to similar but different features. Note that rules listed in these there features are globally applied, not per workflow.

- [Skip engines](#)
 - [Adding a hash to the Skip engines list](#)
- [Whitelist](#)

- [Blacklist](#)

Skip by hash

Skip engines

On this page, users can define rules on what files should be skipped by what engines. That is, a file with the given hash will not be processed by the listed engines.

The screenshot shows the 'Skip by Hash' page in the OPSWAT MetaDefender interface. The page includes a search bar, a table of skip engines, and filters for Skip Engines, Whitelist, and Blacklist.

HASH	ENGINES	COMMENT
69630e4574ec6798239b091cda43dca0	ClamAV	pseudo virus
d3a0d8a53b6b2a241c141a8405ca767c0100dcdd	ESET, Bitdefender	a file

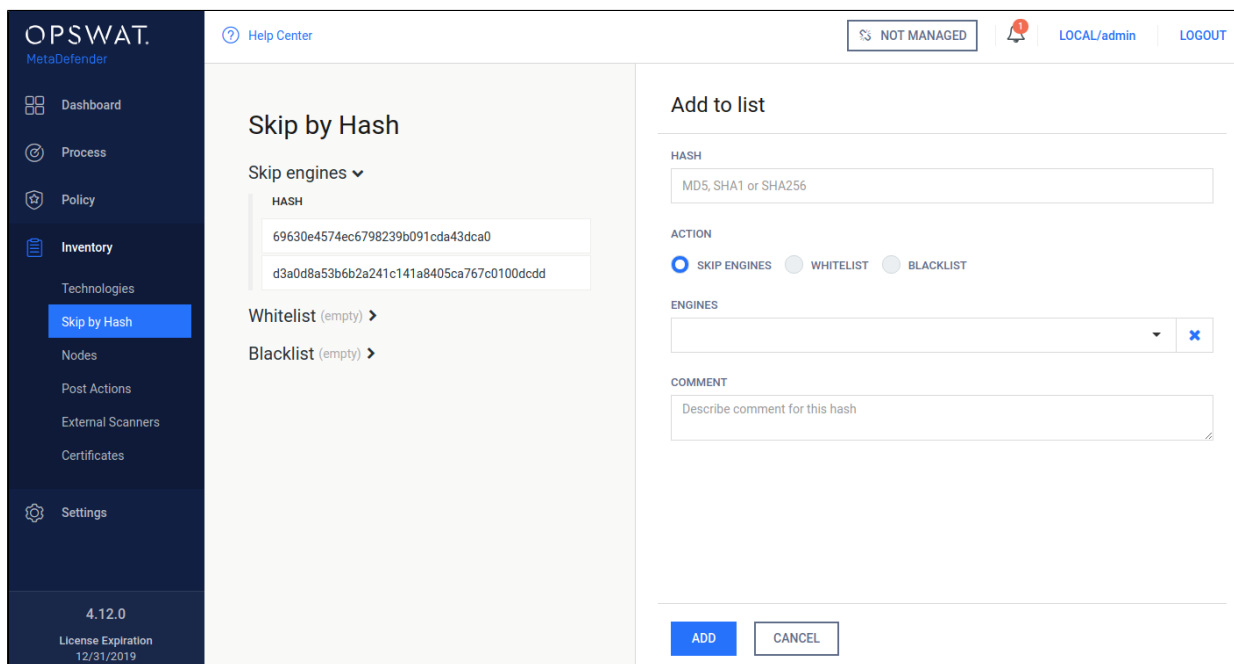
Whitelist (empty) >

Blacklist (empty) >

Skip engines

Adding a hash to the Skip engines list

On the **Skip by Hash** page click the "Add to list" button on the top right. "Add to list" page appears. Hash and at least one engine are mandatory to give, comment is optional. Hash can be either MD5, SHA1 or SHA256. After giving the necessary information and choosing the "Skip engines" action, click on the **Add** button.



Adding a hash to the Skip engines list

Whitelist

Files whose hashes listed here will be globally whitelisted, so they won't be processed in any workflow and will be allowed.

Blacklist

Files whose hashes listed here will be globally blacklisted, so they won't be processed in any workflow and will be blocked.

Technologies

Engine type details

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

- Type of engine. Possible types are
 - Anti-malware engine
 - Archive engine
 - Data Loss Prevention engine
 - Data sanitization engine
 - Filetype detection engine
 - Utility engine

- Vulnerability detection engine
- Elapsed time since last update
- Proportion of active and non-active engines of a particular type
- Engine version
- Version of database the engine is currently using
- Engine status (Active/Non-Active)

The screenshot displays the 'Technologies' management interface in OPSWAT MetaDefender. The left sidebar contains navigation options like Dashboard, Process, Policy, Inventory, and Settings. The main content area features a table of installed technologies. At the top right, there are 'UPLOAD PACKAGE' and 'UPDATE ALL' buttons. A status bar indicates 'Auto update turned off' with a link to 'Edit Update Settings'.

TECHNOLOGY	LAST UPDATE	ACTIVITY	ENGINE	DATABASE	ENABLED
Anti-malware engines	19 hours ago	4/11 processing engines are active			<input type="checkbox"/>
Data Sanitization	18 hours ago	Active on 1/1 node	5.2.3-669-283	5.1.1	<input checked="" type="checkbox"/>
Data Loss Prevention	No available engine				<input type="checkbox"/>
Vulnerability	19 hours ago	Active on 1/1 node	4.57-168	1535550645	<input checked="" type="checkbox"/>
Utilities	No available engine				<input type="checkbox"/>
Filetype Detection	14 days ago	Active on 1/1 node	5.1.11-292	5.1.11-292	<input checked="" type="checkbox"/>
Archive	a month ago	Active on 1/1 node	16.02-269	16.02-269	<input checked="" type="checkbox"/>

Technologies

Engines can be disabled (and re-enabled afterwards) by clicking on the switch at the end of the line that belongs to that particular engine. When an engine is disabled neither the engine nor the corresponding database package is updated and it will be removed from every node.

Manual updates

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

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


Upload update packages

Please select packages and corresponding descriptor files downloaded by the Offline Downloader Utility then press START UPLOAD to initiate upload and update process

ARCHIVE PACKAGE	DESCRIPTOR
<input type="button" value="CANCEL"/>	<input type="button" value="SELECT FILES"/> <input type="button" value="START UPLOAD"/>

Upload packages

The package should be a ZIP and the descriptor YML file, which can be downloaded with the Update Downloader. Multiple files can be selected.

 Engine or database versions that have ever been used on a system won't be accepted as updates.

Configuring engines

Some engines can be configured by using **Advanced Engine Configuration**. Hover mouse pointer over the line related to the engine to be configured, to let the **Edit** button to appear (pencil at the end of line) and click on it. The edit page is displayed.

Edit Configuration

ADVANCED ENGINE CONFIGURATION

Configuration

OK
CANCEL

Put the desired configuration into the text box and click **OK**.

Available options

Scan engine	Configuration	Note
ClamAV	<pre>[engine] heuristic_scan=1 extract_archive=0 max_file_size=0 max_scan_size=0 enable_pup_scan=0 deep_scan=0</pre>	<p>max_file_size: Setting it too high may result in severe damage to the system. Make sure you have enough free memory. Setting to 0 to disable this limit. Default value is 524288000 bytes.</p> <p>max_scan_size: The maximum amount of data to scan for each container file. Certain files (e. g. documents, archives, etc.) may in turn contain other files inside. This options ensure safe processing of this kind of data..Setting it too high may result in severe damage to the system. Make sure you have enough free memory. Setting to 0 to disable this limit. Default value is 524288000 bytes.</p> <p>deep_scan:</p>

Scan engine	Configuration	Note
		<p>0 - Do not scan the whole file if it is a big file</p> <p>1 - Scan full file, it may take significantly higher time</p>
Avira	<pre>[engine] heuristic_scan=1 extract_archive=0 detect_all_types=1</pre>	<p>heuristic_scan:</p> <p>0 - Disable heuristic detection.</p> <p>1 - Lazy heuristic detection. This is the lowest possible mode, detection is not very good, but the false positives number will be low.</p> <p>2 - Normal heuristic detection.</p> <p>3 - High heuristic detection. This is the highest possible mode, but the false positives number will be high.</p>
ESET	<pre>[engine] heuristic_scan=1 extract_archive=0 enable_pup_scan=1</pre>	
Ahnlab	<pre>[engine] extract_archive=0 enable_cloud_scan=0 enable_pup_scan=0</pre>	
BitDefender	<pre>[engine] extract_archive=0</pre>	
CYREN	<pre>[engine] extract_archive=0 enable_pup_scan=0</pre>	
QuickHeal	<pre>[engine] heuristic_scan=0 extract_archive=0 mail_heuristic=0 enable_pup_scan=0</pre>	<p>mail_heuristic: set 1 to enable scan mail files</p>

Scan engine	Configuration	Note
Vir.IT eXplorer	[engine] extract_archive=0 enable_pup_scan=1	
TotalDefense	[engine] heuristic_scan=1 extract_archive=0 enable_cloud_scan=0	
F-Prot	[engine] heuristic_scan=3 extract_archive=0	heuristic_scan: 0 - No heuristics. 1 - Minimal heuristics - almost no FP chance. 2 - Standard setting. 3 - Higher detection and more FP. 4 - Even higher detection and even more FP.
Ikarus	[engine] extract_archive=0	
K7	[engine] heuristic_scan=0 extract_archive=0	
TACHYON	[engine] heuristic_scan=1 extract_archive=0	
Emsisoft	[engine] heuristic_scan=1 extract_archive=0 max_file_size=104857600 enable_bd_module=1	extract_archive will not work if enable_bd_module is disabled
Kaspersky	[engine] heuristic_scan=1 extract_archive=0	heuristic_scan:

Scan engine	Configuration	Note
		0 - Disable heuristic analysis. 1 - Enable light heuristic analysis. 2 - Enable medium heuristic analysis. 3 - Enable deep heuristic analysis.
VirusBlokAda	No configuration	
Zillya	[engine] heuristic_scan=0 extract_archive=0 load_extended_database=1	load_extended_daabase: engine will load a larger database 0 - faster initialization, but lower detection rate 1 - higher detection rate, but initialization takes longer (default)
Antiy	[engine] extract_archive=0 heuristic_scan=0 enable_high_scan=1	enable_high_scan: 0 - lower memory usage 1 - default; high detection rate, but a bit slower and more resources usage
McAfee	[engine] heuristic_scan=1 extract_archive=0	
NanoAV	[engine] extract_archive=0 heuristic_scan=1	
NETGATE	No configuration	
Sophos	[engine] heuristic_scan=1 extract_archive=0 enable_pup_scan=1	
Aegislab	[engine] extract_archive=0 enable_cloud_scan=0	

Scan engine	Configuration	Note
ByteHero	[engine] extract_archive=0	
Filseclab	[engine] heuristic_scan=1 extract_archive=0	heuristic_scan: 0 - Disable heuristic analysis. 1 - basic mode (default). 2 - static mode (MVM). 3 - dynamic mode (MVM). 4 - full mode (MVM). 5 - use advanced heuristic.
Lavasoft	[engine] extract_archive=0	
MSE	[engine] extract_archive=0	
STOPzilla	[engine] extract_archive=0	
Symantec	[engine] server=127.0.0.1:1344 heuristic_scan=1 enable_pup_scan=0	should not change server value, it's the ip and host where Symantec service is running.
Systweak	[engine] extract_archive=0	
Huorong	[engine] extract_archive=0	
Trend Micro and Trend Micro House Call	No configuration	
Xvirus	No configuration	



- Values in the table are default values
- If there is no special note, available values are 0 and 1
- After applying new configuration, need to wait for 30s-60s for engine reloading
- nProtect was renamed to TACHYON from 6/20/2018

6.3. Regular Maintenance

Checking for Upgrades

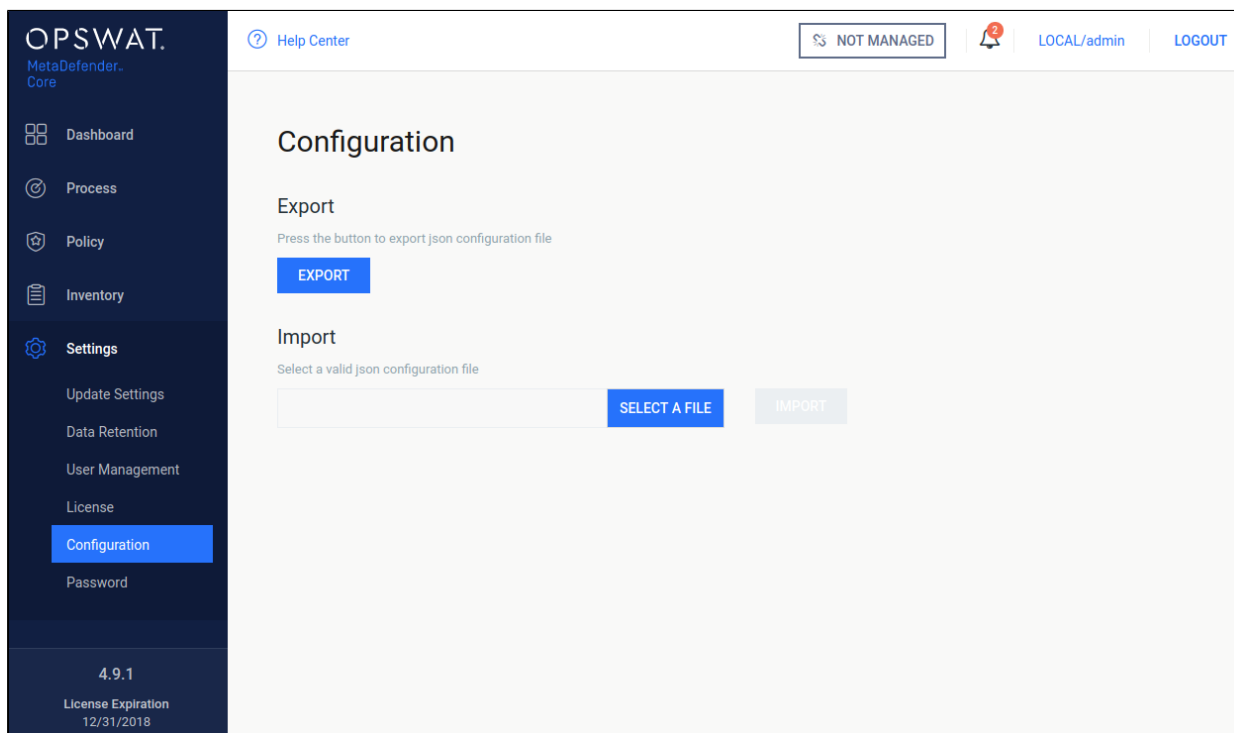
Metadefender Core checks for available database updates and scan engine updates for the installed anti-malware engines on a regular basis. To manually update a scan engine or its database, click on the update now button or the upload package link on the **Inventory > Engines** page.

Checking Engines / Databases Health

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

6.4 Import/Export configuration

MetaDefender Core current configuration can be exported or a new one can be imported under the **Settings > Configuration** page.



Configuration import/export

Export

Click the export button to download the JSON file containing the current configuration. This JSON file will contain the whole configuration about security zones, analysis workflows, security rules.

Import

The importable file must be a valid JSON file and it should contain all the necessary fields, otherwise the MetaDefender Core will reject it.

After the successful import, the new configuration will replace the old one. You can check it under the policy page.

Note

If the imported configuration is the same as the active configuration, the MetaDefender Core will reject it. This is the expected behavior.

7. Metadefender Core Developer Guide

How to Interact with Metadefender Core using REST

Beginning with Metadefender Core 4.x, OPSWAT recommends using the JSON-based REST API.

The available methods are documented [below](#).

File scan process

1. Upload a file to scan (POST to /file resource), then receive data_id from response: ([Scan File](#))

Note: The performance depends on:

- number of nodes (scaling)
- number of engines per node
- type of file to be scanned
- Metadefender Core and nodes' hardware

2. Fetch the result with previously received data_id (GET from /file/{data_id resource) until scan result belonging to data_id doesn't reach the 100 percent progress_percentage: ([Fetch Scan Result](#))

Note: Too many data_id requests can reduce performance. It is enough to just check every few hundred milliseconds.

3. Retrieve the scan results anytime after the scan is completed with hash for files (md5, sha1, sha256). (The hash can be found in the scan results) ([Fetch Scan Result by File Hash](#))



OPSWAT provides some sample codes on [GitHub](#) to make it easier to understand how the MetaDefender REST API works.

7.1. MetaDefender API Code Samples

OPSWAT provides some sample codes on [GitHub](#) to make it easier to understand how the MetaDefender REST API works.

- <https://github.com/OPSWAT>

Activate License Online

This API initiates an online activation of the deployment.

Request	Value
Method	POST
URL	/admin/license/activation

Request HTTP header parameters:

name	type	required	value
apikey	string	true	Session id, can be acquired by Login / Create a Session

Request body:

JSON path	Type	Required	Value
activationKey	string	true	activation key
quantity	number	true	maximum node count this instance allows to connect
comment	string	false	description to help identify this deployment later

Example:

```
{
  "activationKey": "xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx",
  "quantity": "1",
  "comment": "Core server 001 for Kiosks"
}
```

Successful response

HTTP status code: 200

Response contains

```
{
  "success": true
}
```

Error response

Invalid user information

HTTP status code: **403**

```
{
  "err": "Access denied"
}
```

HTTP status code: **400**

```
{
  "error": "<error message>"
}
```

Unexpected event on server

HTTP status code: **500**

```
{
  "err": "<error message>"
}
```

Note: Check Metadefender Core server logs for more information.

Cancel Batch

Cancel Scan Batch

Url	/file/batch/<batch_id>/cancel
Method	POST

When cancelling a batch, the connected scans that are still in progress will be cancelled also. The cancelled batch will be closed.

Header	Description
apikey (OPTIONAL)	User's session id, if it was set for creation it is required

Result Code	Description
200	Batch cancelled successfully
400	Bad request, (e.g.: wrong header values)
403	Access denied
404	Batch not found
500	Internal server error

HTTP status code: 200

```
{
  [batch_id]: "cancelled"
}
```

HTTP status code: 500, 403, 400

```
{
  "err": <error message>
}
```

Cancel File Scan

Cancel Scan File

Url	/file/<data_id>/cancel
Method	POST

When cancelling a file scan, the connected scans that are still in progress will be cancelled also. The cancelled scan will be closed.

Header	Description
apikey (OPTIONAL)	User's session id, if it was set for creation it is required

Result Code	Description
200	File scan cancelled successfully
400	Bad request, (e.g.: scan already finished)
404	Scan not found
405	Access denied
500	Internal server error

HTTP status code: 200

```
{
  [data_id]: "cancelled"
}
```

HTTP status code: 500, 405, 404, 400

```
{
  "err": <error message>
}
```

```
}
```

Close Batch

Close Scan Batch

Url	/file/batch/<batch_id>/close
Method	POST

Header	Description
apikey (OPTIONAL)	User's session id, if it was set for creation it is required

Result Code	Description
200	Batch closed successfully
400	Bad request, (e.g.: wrong header values)
403	Access denied
404	Batch not found
500	Internal server error

HTTP status code: 200

```
{
  "batch_id": "092876200fb54cfb80b6e3332c410ae9",
  "is_closed": true,
  "batch_files": {
    "batch_count": 1
  },
  "process_info": {
    "blocked_reason": "",
    "file_type_skipped_scan": false,
    "profile": "File scan",
  }
}
```

```

    "result": "Processing",
    "user_agent": "webscan"
  },
  "scan_results": {
    "batch_id": "092876200fb54cfb80b6e3332c410ae9",
    "scan_all_result_a": "In Progress",
    "scan_all_result_i": 255,
    "scan_details": {},
    "start_time": "2017-05-23T11:22:03.010Z",
    "total_avs": 14,
    "total_time": 995
  }
}

```

HTTP status code: 500, 403, 400

```

{
  "err": <error message>
}

```

Download Batch Signed Result

Download Batch Signed Result

Url	/file/batch/<batch_id>/certificate
Method	GET

Header	Description
apikey (OPTIONAL)	User's session id, if batch was created with apikey it is required

Result Code	Description
200	Signed batch result and certificate are sent back in response body (YAML format)
400	Bad request, (e.g.: wrong header values)

Result Code	Description
403	Access denied
500	Internal server error

HTTP status code: 200

```

---
batch_id: 092876200fb54cfb80b6e3332c410ae9
user_data: the user data from the header from batch creation
cert_sha1_fingerprint: <some cert serial value>
batch_files:
  batch_count: 1
  files_in_batch:
    - data_id: 9112b225f0634f189a2bb46ec1a7826f
      display_name: New%20Text%20Document.txt
      file_size: 5
      scan_all_result_i: 0
      process_info:
        blocked_reason:
          result: Allowed
        sha256:
f4191b3ec6ce93aaf712919a38e52815c5da9c91d2b141df920bc8bcb5cbb8e3
      process_info:
        blocked_reason:
          file_type_skipped_scan: false
        profile: File scan
        result: Allowed
        user_agent: webscan
      scan_results:
        scan_all_result_a: No Threat Detected
        scan_all_result_i: 0
        start_time: 2017-05-23T11:22:03.010Z
        total_avs: 14
        total_time: 995
    ...
---
signature:
881d22220c4ca0557d7c7d5c5794d53a8a2780997cd65b27b6e7f1c099a15de03d
bcb5edbeaea7aafa6099fab37be07017b39e3e3a7d66c550f44eb59a096c54d5b9
555cb28198546fbec57c33b717751d333a09733d95dd876e2798d044c8caef828f
4352b91f9a6d057253bb1a9461e0e0e0bf4313a80895998d645bebc81841ff3499
589c80ffc4e8a190d1ec9b3e4126d86659d303b0e1f22d9289c9c4671d35532b55
ad4620e048a78bb405b573897da63efdd5f036692c934a82d9bdc9b9862e7fea5e

```

8abeeb1444be0689d50373c5c0632484950c0fe0337ed5f91bdf26986f7cff8aa3
431bf4bc948fc127c16ba13ec679fe9f67e7586075c1f467454fa8cf40e9cd5012
91c95d862eb16f4477c17d1711294f0ff2b3a1140bd53dbd1fbb0846af6062e9e4
e2e1a09af3448503ed11e342164e535fc268bf7d8fbc28ed946cd2bb8ea075f229
5d2fa8392076d41608c3b5decf8fab3a5ec7de190f07583331e0517e5f361735cd
59326622dc8b07b10a464028de781a063e408f918c1d5534329140f4e4dc1a717d
808d6784410410b00d36cb9a345f5bbc11fa1c58ee28f8e7b863f3ea2c923ec5fb
2ac29eaa4ddc0d6d9dfd3f16a97f207dc2858410a577c7f4a92ff01bad3229f5fc
db08e21df9869a113272aa9d96bfdfe8bfb3a50414c174e16a3504e5780c271877
9b0757298546f287ef7ea86e67510d48a8

certificate: |

-----BEGIN CERTIFICATE-----

```
MIIGJzCCBA+gAwIBAgIBATANBgkqhkiG9w0BAQUFADCBSjELMAkGA1UEBhMCRLIx
DzANBgNVBAGMBkFsc2FjZTETMBEgA1UEBwwKU3RyYXNib3VyZzEYMBYGA1UECgwP
d3d3LmZyZWVsYW4ub3JnMRAwDgYDVQQLDAdmcmVlbGFuMS0wKwYDVQQDDCRGcmVl
bGFuIFNhbXBsZSBDZXJ0aWZpY2F0ZSBBDXR0b3JpdHkxIjAgBgkqhkiG9w0BCQEW
E2NvbnRhY3RAZnJlZWxhbi5vcmcwHhcNMTIwNDI3MTAzMTE4WWhcNMjIwNDI3MTAz
MTE4WjB+MQswCQYDVQQGEWJGUjEPMjE0MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1
MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1
MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1MDE1
MSIWIAYJKoZIhvcNAQkBFhNjb250YWN0QGZyZWVsYW4ub3JnMIIICjANBgkqhkiG
9w0BAQEFAAOCAg8AMIICCgKCAgEA3W29+ID6194bH6eJLrIC4hb2Ugo8v6ZC+Mrc
k2dNYMNPjcOKABvxxEtBamnSaeU/IY7FC/giN622LEtV/3oDcrua0+yWuVafyxmZ
yTKUb4/GUgafRQPf/eix9urWurtIK7XgNGFNUjYPq4dSJQPPhwCHE/LKAykWnZBX
RrX0Dq4XyApNku0IpjIjEXH+8ixE12wH8wt7DEvd07T3N3CfUbaITl1qBX+Nm2Z6
q4Ag/u5r18NJfXg71ZmXA3XOj7zFvpyapRIZcPmkvZYn7SMCP8dXyXHPdpSiIWL2
uB3Ki04JrUYvt2GzLBUThp+lNSzaZ/Q3yOaAAUkOx+1h08285Pi+P810+H2Xic4S
vMq1xtLg2bNoPC5KnBRfuFPuUD2/3dSiiragJ6uYDLOyWJDIVKgt/720VTEPAL9o
6T2pGZrwbQuiFGrGTMZOvWMSpQtNl+tCCXlT4mWqJDRwuMGrI4DnnGzt3IKqNwS4
Qyo9KqjMIPwnXZAmWpM3FOke4sFwc5fpawKO01JZewDsYTDxVj+cwXwFxbE2yBiF
z2FAHwfopwaH35p3C61kcgP2k/zgAlnBluzACUI+MKJ/G0gv/uAhj1OHJQ3L6kn1
SpvQ41/ueBj1unExqQSYD7GtZ1Kq8uOcq2r+WISE3Qc9MpQFFkUVllmgWGwYDuN3
Zsez95kCAwEAAa7MHkwCQYDVR0TBAIwADAsBg1ghkgBhvhCAQ0EHEXydt3BlblNT
TCBHZW51cmF0ZWQgQ2VydG1maWNhdGUwHQYDVR0OBBYEFFlfyRO6G8y5qEFKik15
ajb2ft7XMB8GA1UdIwQYMBaAFCNsLT0+KV14uGw+quK7Lh5sh/JTMA0GCSqGSIB3
DQEBBQUAA4ICAQAT5wJFPqervbja5+90iKxild0QVtVGB+z6aoAMuWK+qgi0vgvr
mu9ot2lvTSCSnRhjeiP0SIdqFMORMbtOCfk/kYDp9M/91b+vS+S9eAlxrNCB5Vof
PqxEPp/wv1rBcE4GBO/c6HcFon3F+oBYCsUQbZDKSSZxhDm3mj7pb67FNbZbJIzJ
70HDSre2004oiTx+h6g6pW3cOQMgIAvFgKN5Ex727K4230B0NidGkzuj4KSML0NM
s1SAcXZ410oSKNjy44BVEZv0ZdxTDrRM4EwJtNygFzmtTuV02nkUj1bYYC5f0L
ADr6s0XMyaNk8twlWY1YDZ5uKDPVRVbfIGcQ0uJIZIvemhuTrofh8pBQQNkPRDFT
RqliTo1Ihh13/F11kXk1WR3jTjNb4jHX71IoXwpwp767HAPKGhjQ9cFbnHMETkro
RlJYdtRq5mccDtwT0GFyoJLLBZdHHMHJz0F9H7FNk2tTQQMhK5MVYwg+LIaee586
CQVqfbscp7evlgjLW98H+5zylRHAgOH2G79aHljNKMp9BOuq6SnEgLEsiWGVtu21
hnx8SB3sVJZHeer8f/UQQwqbAO+Kdy70NmbSaqAVtp8jOxLiidWkwSyRTsuU6D8i
DiH5uEqBXExjrj0FslxcVKdVj5glVcSmkLwZKbEU1OKwleT/iXFhvoowhQ==
```

-----END CERTIFICATE-----

...

HTTP status code: 500, 403, 400

```
{
  "err": <error message>
}
```

Download Sanitized Files

Download Sanitized Files Using Data Id

Request	Value
Method	GET
URL	/file/converted/{data_id}

The data_id comes from the result of [Scan A File](#). In case of sanitizing the content of an archive, the data_id of contained file can be found in [Fetch Scan Result](#).

Request HTTP header parameters:

name	type	required	value
apikey	string	false	Session id, can be acquired by Login / Create a Session

When a user's apikey was used for scanning a file, it is necessary to set an apikey which belongs to the same user to access the sanitized files.

Successful response

HTTP status code: 200

Raw file data

Error response

Invalid data id

HTTP status code: 404

```
{
  "err": "File could not be found"
}
```

```
}
```

Internal error

HTTP status code: **404**

```
{  
  "err": "<error message>"  
}
```

Invalid api key or rights

HTTP status code: **405**

```
{  
  "err": "Access denied"  
}
```

Unexpected event on server

HTTP status code: **500**

```
{  
  "err": "<error message>"  
}
```

Note: Check Metadefender Core server logs for more information.

Fetching Available Scan Rules

The response is an array of available rules

Request	Value	Note
Method	GET	
URL	/file/rules	

Request	Value	Note
URL	/file/workflows	Same as /file/rules, deprecated

Request HTTP header parameters:

name	type	required	value	notes
user_agent	string	optional	The user agent string value sent in the header (specified by the client).	<p>Only those rules are returned, that:</p> <ol style="list-style-type: none"> 1. Match the client's user agent sent using the <i>user_agent</i> header, or 2. Are not restricted to a specific user agent. <p>For details see KB article What are Security Policies and how do I use them?.</p>

Successful response

HTTP status code: **200**

The response contains the available rules:

```
[
  {
    "max_file_size": 200000000,
    "name": "File scan"
  },
  {
    "max_file_size": 200000000,
    "name": "File scan w/o archive"
  }
]
```

Response description:

- max_file_size: Maximum file size for files scanned in bytes.
- name: A unique identifier for identify in the used rule for a scan.

Error response

Unexpected event on server

HTTP status code: **500**

```
{
  "err": "<error message>"
}
```

Note: Check Metadefender Core server logs for more information.

Fetching Engine/Database Versions

The response is an array of engines with database information.

Request	Value
Method	GET
URL	/stat/engines

Successful response

HTTP status code: **200**

```
[
  {
    "active": true,
    "def_time": "",
    "download_progress": 100,
    "download_time": "2015-08-14T15:57:46.898Z",
    "eng_id": "7z_1_linux",
    "eng_name": "Archive engine",
    "eng_type": "Bundled engine",
    "eng_ver": "9.38-57",
    "engine_type": "archive",
    "state": "production",
    "type": "engine"
  },
  {
    "active": true,
    "def_time": "2015-08-17T02:37:05.000Z",
```

```
    "download_progress": 100,
    "download_time": "2015-08-17T08:17:22.810Z",
    "eng_id": "clamav_1_linux",
    "eng_name": "ClamAV",
    "eng_type": "Bundled engine",
    "eng_ver": "3.0-43",
    "engine_type": "av",
    "state": "production",
    "type": "engine"
  }
]
```

Response description:

- active: if used by at least one engine
- def_time: the database definition time for this engine
- download_progress: percentage progress of download
- download_time: when this engine downloaded from the update server
- eng_id: engine internal ID
- eng_name: engine name
- eng_type: engine type in human readable form
- eng_ver: engine's version
- engine_type: engine's type (av, archive or filetype)
- state: status of the engine (downloading, downloaded, staging, production, removed, temporary failed, permanently failed, content invalid or download failed)

Error response

Internal error

HTTP status code: 500

```
{
  "err": "Error querying engine list"
}
```

Unexpected event on server

HTTP status code: 500

```
{
  "err": "<error message>"
}
```

Fetch Scan Result

Retrieving Scan Reports Using Data ID

Retrieve scan results.

Scan is done asynchronously and each scan request is tracked by a data ID. Initiating file scans and retrieving the results need to be done using two separate API calls. This request needs to be made multiple times until the scan is complete. Scan completion can be traced using "scan_results.progress_percentage" value from the response.

Request	Value
Method	GET
URL	/file/{data_id} or /process/{data_id}

Successful response

HTTP status code: **200**

```
{
  "data_id": "61dfffeaa728844adbf49eb090e4ece0e",
  "dlp_info": {
    "hits": {
      "ccn": {
        "display_name": "Credit Card Number",
        "hits": [
          {
            "after": "Duo case nulla dicunt eu\n",
            "before": "velit..\nEos nostro recteque te. ",
            "hit": "XXXXXXXXXXXX1113",
            "severity": "0"
          }
        ]
      }
    },
    "regex_0": {
      "display_name": "RegEx rule",
      "hits": [
        {
```



```

        "after": "Text after the searched data \n",
        "before": "animal voluptua.\nText matched data. ",
        "hit": "sXXXXXXXXXXXXXXXXXXXXn",
        "severity": "0"
    }
  ]
},
"ssn": {
  "display_name": "Social Security Number",
  "hits": [
    {
      "after": "Eam ad verear animal voluptua.\n",
      "before": "doctus eligendi an vim.\nSSN: ",
      "hit": "XXXXXXX7777",
      "severity": "0"
    }
  ]
}
},
"verdict": 1
},
"file_info": {
  "display_name": "samplefile.txt",
  "file_size": 81035,
  "file_type": "text/plain",
  "file_type_description": "ASCII text",
  "md5": "c05017f68343a5257fc3c0db72aa58dc",
  "sha1": "ba46b945f408cc729458380350b4e78f61741c81",
  "sha256": "8805777d2d561255edcb499f7445ef0216b75737bacb6bc
6665dbf9830272f53",
  "upload_timestamp": "2015-08-14T12:46:59.360Z"
},
"scan_results": {
  "data_id": "61dffeaa728844adbf49eb090e4ece0e",
  "progress_percentage": 100,
  "scan_all_result_a": "No Threat Detected",
  "scan_all_result_i": 0,
  "scan_details": {
    "Engine1": {
      "def_time": "2015-08-13T09:32:48.000Z",
      "location": "local",
      "scan_result_i": 0,
      "scan_time": 1,
      "wait_time": 1,
      "threat_found": ""
    },
    "Engine2": {
      "def_time": "2015-08-10T00:00:00.000Z",
      "location": "local",
      "scan_result_i": 0,
      "scan_time": 3,

```

```

        "wait_time": 2,
        "threat_found": ""
    },
    },
    "start_time": "2015-08-14T12:46:59.363Z",
    "total_avs": 2,
    "total_time": 389
},
"process_info": {
    "post_processing": {
        "actions_ran": "Sanitize",
        "actions_failed": "",
        "converted_to": "png",
        "copy_move_destination": "",
        "converted_destination": ""
    },
    "outdated_data": [
        "sanitization",
        "configuration"
    ]
    "processing_time": 400,
    "progress_percentage": 100,
    "user_agent": "webscan",
    "profile": "File scan",
    "queue_time": 10,
    "result": "Allowed",
    "blocked_reason": "",
    "file_type_skipped_scan": false,
    "issues": [
        {
            description: "Probably blocked by a 3rd party
software",
            severity: "fatal"
        }
    ]
},
"vulnerability_info": {...}
}

```

Response description:

- data_id: data ID of the requested file
- file_info: basic information of the scanned file
- scan_results: results of the scan
 - data_id: data ID of the requested file
 - progress_percentage: percentage of progress, if it is 100, then the scan is completed

- scan_all_result_a: the overall scan result in string
- scan_all_result_i: the overall scan result in number code
- individual scan engine results will be consolidated according to the following priority:
 1. Threat found
 2. Object is suspicious
 3. Object is encrypted / too deep (archive only) / too big (archive only) / containing too many files (archive only) / extraction timeout exceeded (archive only)
 4. Filetype mismatch
 5. No threat detected
 6. Object was not scanned
 7. Failed to scan the object
- scan_details: scan results for each antivirus engine. The key is the name of the antivirus engine and the value is the result of the antivirus engine
 - def_time: the database definition time for this engine
 - location: place of scan engine
 - scan_result_i: numeric code of engine scan result
 - scan_time: time elapsed during scan with the engine in milliseconds
 - wait_time: time elapsed between sending file to node and receiving the result from the engine in milliseconds
 - threat_found: name of the scan result
- start_time: start time of scan
- total_avs: number of used antivirus engines
- total_time: total time elapsed during scan in milliseconds
- process_info: process information
 - post_processing: Contains information about result of data sanitization
 - "actions_ran": "Sanitized" or "" and the names of Post Actions that were also run.
The separator is "|" (pipe). (e.g.: actions_ran: "PAscript" or actions_ran: "Sanitized | PAscript")

- "actions_failed": "Sanitization Failed" or "" and the names of failed Post Actions.
The separator is "|" (pipe). (e.g.: actions_failed: "PAscript failed" or actions_failed: "Sanitization Failed | PAscript failed")
- "converted_to": contains target type name of sanitization
- "copy_move_destination": ""
- "converted_destination": contains the name of the sanitized file
- processing_time: total time elapsed during processing file on the node in milliseconds
- progress_percentage: percentage of processing completed
- queue_time: total time elapsed during file waits in the queue in milliseconds
- user_agent: who called this API
- profile: the name of the rule used
- result: the final result of processing the file (Allowed / Blocked / Processing)
- blocked_reason: gives the reason if the file is blocked
- file_type_skipped_scan: indicates if the input file's detected type was configured to skip scanning
- issues: task related issues (e.g.: blocked by 3rd party software, can not access file for scanning)
- outdated_data: array of flags - if occur - describing outdated data in the result, these can be
 - enginedefinitions: at least one of the AV engines the item was scanned with has a newer definition database
 - configuration: the process' rule - or any item used by the rule - was modified since the item was processed
 - sanitization: if item was sanitized this flag notifies that the sanitization information regarding this result is outdated, meaning the sanitized item is no longer available
- vulnerability_info: see [Vulnerability Info In Scan Result](#)
- dlp_info: information on matched sensitive data
 - hits: detailed results that contains
 - type of matched rule: ccn (credit card number), ssn (social security number), regex_<number> (regular expression with a number in order to differentiate the RegEx rules if there are more.)

- display_name: Credit Card Number, Social Security Number, or in case of RegEx, the name of the rule that has been given by the user
- hits: the hits for that type
 - before: the context before the matched data
 - after: the context after the matched data
 - hit: the matched data
 - severity: can be 0 (detected) or 1 (suspicious)
- verdict: the overall result for the scanned file. It can be
 - 0 - clean
 - 1 - found matched data
 - 2 - suspicious
 - 3 - failed
 - 4 - not scanned (e.g. not supported file type)

Possible overall and per engine scan results

scan_result_a	scan_result_i
No Threat Detected	0
Infected	1
Suspicious	2
Failed	3
Cleaned / Deleted	4
Scan Skipped - Whitelisted	7
Scan Skipped - Blacklisted	8
Exceeded Archive Depth	9
Not Scanned	10
Encrypted Archive	12

scan_result_a	scan_result_i
Exceeded Archive Size	13
Exceeded Archive File Number	14
Password Protected Document	15
Exceeded Archive Timeout	16
Filetype Mismatch	17
Potentially Vulnerable File	18
Canceled	19
Sensitive data found	20
In Progress	255

Successful response with archive detection

HTTP status code: **200**

```
{
  "data_id": "d7016058f0874d12b98a8c1ece9d3ea9",
  "extracted_files": {
    "files_in_archive": [
      {
        "data_id": "21d48f2c463c4ca89b7544c2c127e945",
        "detected_by": 0,
        "display_name": "samplezip.tar.gz/[Content]
/samplezip/sampleimg.jpg",
        "file_size": 215684,
        "file_type": "image/jpeg",
        "file_type_description": "JPEG image data",
        "progress_percentage": 100,
        "scan_all_result_i": 0,
        "scanned_with": 10
      },
      {
        "data_id": "7cb298eb42614ca9bc87a4de4acad436",
        "detected_by": 9,
```

```

        "display_name": "samplezip.tar.gz/[Content]
/samplezip/eicar",
        "file_size": 69,
        "file_type": "text/plain",
        "file_type_description": "EICAR virus test files",
        "progress_percentage": 100,
        "scan_all_result_i": 1,
        "scanned_with": 10
    },
    ]
},
"file_info": {
    "display_name": "samplezip.tar.gz",
    "file_size": 1486610,
    "file_type": "application/x-gzip",
    "file_type_description": "gzip compressed data",
    "md5": "60d5fc5b07ecd1dc8c781bfa94ec8619",
    "sha1": "992e40a2a6906c6d21f92034dfba779aae6d9ee7",
    "sha256": "6ec5e258141528f004a43f7d25163alc7486df76fde7976
a793b140b1leda95d",
    "upload_timestamp": "2015-08-14T12:46:59.360Z"
},
"scan_results": {
    "last_file_scanned": "example.pdf",
    "data_id": "d7016058f0874d12b98a8clece9d3ea9",
    "progress_percentage": 100,
    "scan_all_result_a": "Infected",
    "scan_all_result_i": 1,
    "scan_details": {
        "Engine1": {
            "def_time": "2015-08-13T09:32:48.000Z",
            "location": "local",
            "scan_result_i": 0,
            "scan_time": 1,
            "wait_time": 3,
            "threat_found": ""
        },
        "Engine2": {
            "def_time": "2015-08-10T00:00:00.000Z",
            "location": "local",
            "scan_result_i": 0,
            "scan_time": 3,
            "wait_time": 1,
            "threat_found": ""
        }
    },
    "start_time": "2015-08-14T12:46:59.363Z",
    "total_avs": 10,
    "total_time": 389
}
"process_info": {

```

```

    "post_processing": {
      "actions_ran": "",
      "actions_failed": "",
      "converted_to": "",
      "copy_move_destination": "",
      "converted_destination": ""
    },
    "processing_time": 400,
    "progress_percentage": 100,
    "user_agent": "webscan",
    "profile": "File scan",
    "queue_time": 20,
    "result": "Blocked",
    "blocked_reason": "Scan result: Infected",
    "file_type_skipped_scan": false
  },
  "vulnerability_info": {...}
}

```

Completed response description with archive detection:

- extracted_files: extracted files
 - files_in_archive: array of files in archive
 - detected_by: number of threat reporting engines
 - scanned_with: number of engines used for scanning the file
- scan_results
 - last_file_scanned: If available, the name of the most recent processed file

Response (not existing data_id)

HTTP status code: **200**

```

{
  "61dfffeaa728844adbf49eb090e4ece0e": "Not Found"
}

```

Error response

Unexpected event on server

HTTP status code: **500**


```
{
  "err": "<error message>"
}
```

Note: Check Metadefender Core server logs for more information.

Fetch Scan Result by File Hash

Retrieve Scan Results Using Hash

Request	Value
Method	GET
URL	/hash/{md5 sha1 sha256 hash}

Request http header parameters

name	type	required	value
rule	string	false	the name is the desired rule to query for (see Fetching Available Scan Rules)

The retrieved result is always the most recent for the processed item, if rule is set then it will be the most recent - if exists - under the given rule.

Successful response

HTTP status code: 200

```
{
  "data_id": "61dfffeaa728844adbf49eb090e4ece0e",
  "file_info": {
    "display_name": "samplefile.txt",
    "file_size": 81035,
    "file_type": "text/plain",
    "file_type_description": "ASCII text",
    "md5": "c05017f68343a5257fc3c0db72aa58dc",
    "sha1": "ba46b945f408cc729458380350b4e78f61741c81",
    "sha256": "8805777d2d561255edcb499f7445ef0216b75737bacb6bc6665dbf9830272f53",
  }
}
```

```

    "upload_timestamp": "2015-08-14T12:46:59.360Z"
  },
  "scan_results": {
    "data_id": "61dffeaa728844adbf49eb090e4ece0e",
    "progress_percentage": 100,
    "scan_all_result_a": "No Threat Detected",
    "scan_all_result_i": 0,
    "scan_details": {
      "Engine1": {
        "def_time": "2015-08-13T09:32:48.000Z",
        "location": "local",
        "scan_result_i": 0,
        "scan_time": 1,
        "wait_time": 3,
        "threat_found": ""
      },
      "Engine2": {
        "def_time": "2015-08-10T00:00:00.000Z",
        "location": "local",
        "scan_result_i": 0,
        "scan_time": 3,
        "wait_time": 1,
        "threat_found": ""
      }
    },
    "start_time": "2015-08-14T12:46:59.363Z",
    "total_avs": 2,
    "total_time": 389
  }
}
"process_info": {
  "processing_time": 400,
  "progress_percentage": 100,
  "user_agent": "webscan",
  "profile": "File scan",
  "queue_time": 24,
  "result": "Allowed",
  "blocked_reason": "",
  "file_type_skipped_scan": false,
  "outdated_data": [
    "enginedefinitions"
  ]
},
"vulnerability_info": {...}
}

```

Response description:

- data_id: data ID of the requested file
- file_info: basic information of the scanned file

- scan_results: results of the scan
 - data_id: data ID of the requested file
 - progress_percentage: percentage of progress, if it is 100, then the scan is completed
 - scan_all_result_a: the overall scan result in string
 - scan_all_result_i: the overall scan result in number code
 - individual scan engine results will be consolidated according to the following priority:
 1. Threat found
 2. Object is suspicious
 3. Potentially Vulnerable File
 4. Filetype mismatch
 5. Archive is encrypted / too deep (archive only) / too big (archive only) / containing too many files (archive only) / extraction timeout exceeded (archive only)
 6. Encrypted Document
 7. No threat detected
 8. Object was not scanned / Whitelisted / Blacklisted
 9. Failed to scan the object
 - scan_details: scan results for each antivirus engine. The key is the name of the antivirus engine and the value is the result of the antivirus engine
 - def_time: the database definition time for this engine
 - location: place of scan engine
 - scan_result_i: numeric code of engine scan result
 - scan_time: time elapsed during scan with the engine in milliseconds
 - wait_time: time elapsed between sending file to node and receiving the result from the engine in milliseconds
 - threat_found: name of the scan result
 - start_time: start time of scan
 - total_avs: number of used antivirus engines
 - total_time: total time elapsed during scan in milliseconds
- process_info: process information

- `processing_time`: total time elapsed during processing file on the node in milliseconds
- `progress_percentage`: percentage of processing completed
- `user_agent`: who called this API
- `profile`: the name of the rule used
- `queue_time`: total time elapsed during file waits in the queue in milliseconds
- `result`: the final result of processing the file (Allowed / Blocked / Processing)
- `blocked_reason`: gives the reason if the file is blocked
- `file_type_skipped_scan`: indicates if the input file's detected type was configured to skip scanning
- `outdated_data`: array of flags - if occur - describing outdated data in the result, these can be
 - `enginedefinitions`: at least one of the AV engines the item was scanned with has a newer definition database
 - `configuration`: the process' rule - or any item used by the rule - was modified since the item was processed
 - `sanitization`: if item was sanitized this flag notifies that the sanitization information regarding this result is outdated, meaning the sanitized item is no longer available
- `vulnerability_info`: see [Vulnerability Info In Scan Result](#)

Possible overall and per engine scan results

<code>scan_result_a</code>	<code>scan_result_i</code>
No Threat Detected	0
Infected	1
Suspicious	2
Failed	3
Scan Skipped - Whitelisted	7
Scan Skipped - Blacklisted	8

scan_result_a	scan_result_i
Not Scanned	10
Exceeded Archive Depth	9
Encrypted Archive	12
Exceeded Archive Size	13
Exceeded Archive File Number	14
Exceeded Archive Timeout	16
Filetype Mismatch	17
Potentially Vulnerable File	18
In Progress	255

Successful response with archive detection

HTTP status code: **200**

```
{
  "data_id": "d7016058f0874d12b98a8c1ece9d3ea9",
  "extracted_files": {
    "files_in_archive": [
      {
        "data_id": "21d48f2c463c4ca89b7544c2c127e945",
        "detected_by": 0,
        "display_name": "samplezip.tar.gz/[Content]
/samplezip/sampleimg.jpg",
        "file_size": 215684,
        "file_type": "image/jpeg",
        "file_type_description": "JPEG image data",
        "progress_percentage": 100,
        "scan_all_result_i": 0
      },
      {
        "data_id": "7cb298eb42614ca9bc87a4de4acad436",
        "detected_by": 9,

```

```

        "display_name": "samplezip.tar.gz/[Content]
/samplezip/eicar",
        "file_size": 69,
        "file_type": "text/plain",
        "file_type_description": "EICAR virus test files",
        "progress_percentage": 100,
        "scan_all_result_i": 1
    },
    ]
},
"file_info": {
    "display_name": "samplezip.tar.gz",
    "file_size": 1486610,
    "file_type": "application/x-gzip",
    "file_type_description": "gzip compressed data",
    "md5": "60d5fc5b07ecd1dc8c781bfa94ec8619",
    "sha1": "992e40a2a6906c6d21f92034dfba779aae6d9ee7",
    "sha256": "6ec5e258141528f004a43f7d25163alc7486df76fde7976
a793b140b11eda95d",
    "upload_timestamp": "2015-08-14T12:46:59.360Z"
},
"scan_results": {
    "last_file_scanned": "example.jim",
    "data_id": "d7016058f0874d12b98a8clece9d3ea9",
    "progress_percentage": 100,
    "scan_all_result_a": "Infected",
    "scan_all_result_i": 1,
    "scan_details": {
        "Engine1": {
            "def_time": "2015-08-13T09:32:48.000Z",
            "location": "local",
            "scan_result_i": 0,
            "scan_time": 1,
            "wait_time": 3,
            "threat_found": ""
        },
        "Engine2": {
            "def_time": "2015-08-10T00:00:00.000Z",
            "location": "local",
            "scan_result_i": 0,
            "scan_time": 3,
            "wait_time": 1,
            "threat_found": ""
        }
    },
    "start_time": "2015-08-14T12:46:59.363Z",
    "total_avs": 2,
    "total_time": 389
}
"process_info": {
    "processing_time": 400,

```

```
    "progress_percentage": 100,  
    "user_agent": "webscan",  
    "profile": "File scan",  
    "queue_time": 24,  
    "result": "Blocked",  
    "blocked_reason": "Scan result: Infected",  
    "file_type_skipped_scan": false  
  },  
  "vulnerability_info": {...}  
}
```

Completed response description with archive detection:

- extracted_files: extracted files
 - files_in_archive: array of files in archive
 - detected_by: number of threat reporting engines
- scan_results
 - last_file_scanned: If available, the name of the most recent processed file

Response (not existing hash)

HTTP status code: **200**

```
{  
  "61dffeaa728844adbf49eb090e4ece0e": "Not Found"  
}
```

Error response

Unexpected event on server

HTTP status code: **500**

```
{  
  "err": "<error message>"  
}
```

Note: Check Metadefender Core server logs for more information.

Get Current License Information

Fetch all details about the licensing status of the product.

Request	Value
Method	GET
URL	/admin/license

Request HTTP header parameters:

name	type	required	value
apikey	string	true	Session id, can be acquired by Login / Create a Session

Successful response

HTTP status code: **200**

If a valid license found:

```
{
  "days_left": 3731,
  "deployment": "MSCL00000000000000000000000000000000",
  "expiration": "09/30/2026",
  "licensed_engines": "*",
  "licensed_to": "OPSWAT, Inc.",
  "max_node_count": "10",
  "online_activated": true,
  "product_id": "MSCL-4-unlimited",
  "product_name": "Metadefender Core 5 Linux"
}
```

If **no** valid license found:

```
{
  "deployment_id": "MSCL00000000000000000000000000000000"
}
```

If **no** valid license, but activation key found:


```
{
  "deployment_id": "MSCL00000000000000000000000000000000",
  "reactivate": true
}
```

Error response

Invalid user information

HTTP status code: **403**

```
{
  "err": "Access denied"
}
```

Unexpected event on server

HTTP status code: **500**

```
{
  "err": "<error message>"
}
```

Note: Check Metadefender Core server logs for more information.

Get Product Version

Fetch details about the product version.

Request	Value
Method	GET
URL	/version

Request HTTP header parameters:

name	type	required	value
apikey	string	true	Session id, can be acquired by Login / Create a Session

Successful response

HTTP status code: **200**

```
{
  "product_id": "MSCL",
  "version": "4.3.0.311"
}
```

Error response

Invalid user information

HTTP status code: **403**

```
{
  "err": "Access denied"
}
```

Unexpected event on server

HTTP status code: **500**

```
{
  "err": "<error message>"
}
```

Note: Check Metadefender Core server logs for more information.

Initiate Batch

Initiate Scan Batch

Url	/file/batch
Method	POST

Header	Description
user-data (OPTIONAL)	Additional custom information (max 1024 bytes, URL encoded UTF-8 string)
rule (OPTIONAL)	Select rule for the batch, if no header given the default rule will be selected (URL encoded string of rule name)
user-agent (OPTIONAL)	User-Agent header for helping Rule selection
apikey (OPTIONAL)	User's session id, for e.g.: if rule is role dependent

Result Code	Description
200	Batch id generated in response body
400	Bad request, (e.g.: wrong header values)
403	Access denied
500	Internal server error

HTTP status code: 200

```
{
  "batch_id": "74c85f475147439bac4d33b181853923"
```

```
}
```

HTTP status code: 500, 403, 400

```
{  
  "err": <error message>  
}
```

Login / Create a Session

Initiate a new session for using protected REST APIs.

Request	Value
Method	POST
URL	/login

Request body:

JSON path	Type	Required	Value
user	string	true	user name
password	string	true	user password

Example:

```
{  
  "password": "admin",  
  "user": "admin"  
}
```

Successful response

HTTP status code: 200

Response contains the session_id

```
{
  "session_id": "a5dd6114dbd14a3b8f4577b7b54e6b0a"
}
```

Error response

Invalid user information

HTTP status code: **403**

```
{
  "err": "Failed to login"
}
```

Unexpected event on server

HTTP status code: **500**

```
{
  "err": "<error message>"
}
```

Note: Check Metadefender Core server logs for more information.

Logout / Destroy a Session

Destroy session for not using protected REST APIs.

Request	Value
Method	POST
URL	/logout

Request HTTP header parameters:

name	type	required	value
apikey	string	true	Session id, can be acquired by Login / Create a Session

Successful response

HTTP status code: **200**

```
{
  "response": "Logout success"
}
```

Error response

Invalid user information

HTTP status code: **403**

```
{
  "err": "Access denied"
}
```

HTTP status code: **400**

```
{
  "err": "Logout error"
}
```

Unexpected event on server

HTTP status code: **500**

```
{
  "err": "<error message>"
}
```

Note: Check Metadefender Core server logs for more information.

Scan A File

Scanning a file using a specified workflow.

Scan is done asynchronously and each scan request is tracked by data id of which result can be retrieved by API [Fetch Scan Result](#).

Chunked transfer encoding (applying header *Transfer-Encoding: Chunked*) is not supported on /file API.

Request	Value
Method	POST
URL	/file

Request HTTP header parameters:

name	type	required	value
filename	string	false	name of file
filepath	string	false	if local file scan is enabled the path to the file (see Security rule configuration)
user_agent	string	false	client identification string
rule	string	false	name of the selected rule (see Fetching Available Scan Rules)
workflow	string	false	name of the selected workflow, deprecated
archivepwd	string	false	password for archive

Request body should contain the the content to be scanned.

Successful response

HTTP status code: 200

```
{
  "data_id": "61dffeaa728844adbf49eb090e4ece0e"
}
```

Error response

Internal error

HTTP status code: **500**

```
{
  "err": "Failed to request scan. Try again later."
}
```

Scan queue is full

HTTP status code: **503**

```
{
  "err": "Server is too busy. Try again later."
}
```

Unexpected event on server

HTTP status code: **500**

```
{
  "err": "<error message>"
}
```

Note: Check Metadefender Core server logs for more information.

Scan file in batch

Scan file in batch

Using /file API

For scanning file we are using the traditional /file API. These are just additions to [Scan A File](#):

Header	Description
batch (OPTIONAL)	Batch id to scan with, coming from Initiate Batch (If it is not given, it will be a single file scan.)

Header	Description
rule (OPTIONAL)	If rule header is set, then it MUST match the one configured for the chosen batch otherwise the request will result in error
user-agent (OPTIONAL)	If batch is set, this won't be used (provide compatibility for user_agent also, user-agent is the higher priority if both present)

Status of Batch

Status of Scan Batch

Url	/file/batch/<batch_id>
Method	GET

Header	Description
apikey (OPTIONAL)	User's session id

Result Code	Description
200	Batch status given successfully
400	Bad request, (e.g.: wrong header values)
403	Access denied
404	Batch not found
500	Internal server error

HTTP status code: 200

```

{
  "batch_id": "092876200fb54cfb80b6e3332c410ae9",
  "user_data": "the user data from the header from batch creation"
,
  "is_closed": true,
  "batch_files": {
    "batch_count": 1
  },
  "process_info": {
    "blocked_reason": "",
    "file_type_skipped_scan": false,
    "profile": "File scan",
    "result": "Processing",
    "user_agent": "webscan"
  },
  "scan_results": {
    "batch_id": "092876200fb54cfb80b6e3332c410ae9",
    "scan_all_result_a": "In Progress",
    "scan_all_result_i": 255,
    "scan_details": {},
    "start_time": "2017-05-23T11:22:03.010Z",
    "total_avs": 14,
    "total_time": 995
  }
}

```

HTTP status code: 500, 403, 400

```

{
  "err": <error message>
}

```

Uploading License Key File

Uploading a license file to the Metadefender Core.

There are two ways to obtain a license key file:

- via <https://portal.opswat.com/activation> portal
- via activation server REST API: <https://activation.dl.opswat.com/activation?key=<activation key>&deployment=<deployment unique ID>&quantity=<quantity>>
Deployment unique ID can be fetched via [Get Current License Information API](#).

Request	Value
Method	POST
URL	/admin/license

Request HTTP header parameters:

name	type	required	value
apikey	string	true	Session id, can be acquired by Login / Create a Session

Request body contains a license file

Successful response

HTTP status code: **200**

Response contains

```
{
  "success": true
}
```

Error response

Invalid user information

HTTP status code: **403**

```
{
  "err": "Access denied"
}
```

HTTP status code: **400**

```
{
  "err": "Invalid license"
}
```

Unexpected event on server

HTTP status code: **500**

```
{
  "err": "<error message>"
}
```

Note: Check Metadefender Core server logs for more information.

Vulnerability Info In Scan Result

Vulnerability info can be generated into scan result if the vulnerability engine is enabled on the scanning node and the file uploaded contains known vulnerability. This detection is done by the Vulnerability detection engine.

Example

```
"vulnerability_info": {
  "result": {
    "code": 0,
    "hash": "B428501D1FAD1BA14AA2FC3F9B5F051EC8721EA2",
    "method": 50700,
    "timestamp": "1493020752",
    "timing": 48,
    "detected_product": {
      "has_vulnerability": true,
      "is_current": false,
      "product": {
        "id": 104,
        "name": "Adobe Flash Player"
      }
    },
    "remediation_link": "http://get.adobe.com/flashplayer/",
    "severity": "CRITICAL",
    "sig_name": "Adobe Flash Player",
    "signature": 107,
    "vendor": {
      "id": 91,
      "name": "Adobe Systems Inc."
    }
  },
  "version": "20.0.0.235",
  "version_data": {
    "count_behind": 65,
  }
}
```

```

    "feed_id": 200005,
    "version": "25.0.0.149"
  },
  "vulnerabilities": [
    {
      "description": "Adobe Flash Player before 18.0.0.324 and
19.x and 20.x before 20.0.0.267 on Windows and OS X and before
11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK
before 20.0.0.233, and Adobe AIR SDK & Compiler before
20.0.0.233 allow attackers to execute arbitrary code or cause a
denial of service (memory corruption) via unspecified vectors, a
different vulnerability than CVE-2015-8460, CVE-2015-8636, and
CVE-2015-8645.",
      "details": {
        "cpe": "cpe:/a:adobe:flash player",
        "cve": "CVE-2015-8459",
        "cvss": {
          "access-complexity": "LOW",
          "access-vector": "NETWORK",
          "authentication": "NONE",
          "availability-impact": "",
          "confidentiality-impact": "COMPLETE",
          "generated-on-epoch": "1451411824",
          "integrity-impact": "COMPLETE",
          "score": "10.0",
          "source": "http://nvd.nist.gov"
        },
        "cwe": "CWE-119",
        "last-modified-epoch": "1487300348",
        "published-epoch": "1451347140",
        "references": [
          "http://lists.opensuse.org/opensuse-security-
announce/2015-12/msg00045.html",
          ...
        ]
      },
      "severity": "CRITICAL",
      "severity_index": 5,
      "static_id": 20158459
    },
    {...}
  ]
}
}

```

Response description:

- **vulnerability_info**: Contains all vulnerability related information of the scan result
 - **result**: The result information from the OESIS Framework

Result description (vulnerability_info.result)

- **code**: The result code for vulnerability check, 0 means a successful check
- **hash**: The file's SHA1 hash value
- **method**: The method used by OESIS Framework, it should be 50700 every time
- **timestamp**: Timestamp of the request issued
- **timing**: The vulnerability check's duration in milliseconds
- **detected_product**: Detected products object is present if input hash has been found to correspond to verified product
 - **has_vulnerability**: Indicates whether any vulnerabilities have been associated with the particular product
 - **is_current**: True if this product's patch level is current, defaults to true
 - **product**: Product data object
 - **id**: The OPSWAT product id
 - **name**: The product name
 - **remediation_link**: A link where product updates or patches can be obtained
 - **severity**: String description of Severity level: 'low', 'moderate', 'important', 'critical', 'not_available', 'unknown'
 - **sig_name**: Product signature descriptor
 - **signature**: OPSWAT signature id
 - **vendor**: Vendor data object
 - **id**: The OPSWAT vendor id
 - **name**: The vendor name
 - **version**: The installed product version
 - **version_data**: Object containing detailed patch information
 - **count_behind**: The number of patches behind of the installed product
 - **feed_id**: The remote feed ID used to determine patch level
 - **version**: The current version of the product in the remote feed
 - **vulnerabilites**: A list of specific vulnerabilities
 - **description**: A text description of the specific vulnerability
 - **details**: A set of optional vulnerability details
 - **cpe**: A CPE product reference

- **cve**: A CVE identification string
- **cvss**: A set of cvss severity information
 - **access-complexity**: A CVSS access-complexity descriptor
 - **access-vector**: A CVSS access-vector descriptor
 - **authentication**: A CVSS authentication descriptor
 - **availability-impact**: A CVSS availability impact descriptor
 - **confidentiality-impact**: A CVSS confidentiality impact descriptor
 - **generated-on-epoch**: An epoch timestamp indicating CVSS generation time
 - **integrity-impact**: A CVSS integrity impact descriptor
 - **score**: A CVSS 10-point severity score
 - **source**: A CVSS source descriptor
- **cwe**: A CWE group identification string
- **last_modified_epoch**: An epoch timestamp indicating source last update time
- **published-epoch**: An epoch timestamp indicating source publishing time
- **references**: An array of external reference links
- **severity**: String description of Severity level: 'low', 'moderate', 'important', 'critical', 'not_available', 'unknown'
- **severity_index**: A 5 point scale numerical description of Severity level with 5 being greatest and 0 being unknown
- **static_id**: An OPSWAT identifier for the vulnerability

8. Advanced Metadefender Deployment

- [8.1. Scripted license management](#)
- [8.2. Multi-node deployment](#)
- [8.3. Using external load-balancer](#)
- [8.4. Cloud Deployment](#)

8.1. Scripted license management

Using REST API calls there is an option for scripted activation and deactivation for Metadefender Core servers with **no Internet connection or if your infrastructure is using automation to create/destroy Metadefender Core instances**. In this chapter the steps of these two scenarios are described.

Requirements

- an installed Metadefender Core instance without Internet connection
- another computer that has Internet connection and can run your activation scripts
- a manual or automated way to transfer data between the two computers

Activation steps

1. For activating Metadefender Core v4, deployment ID and activation key are needed to generate the license file.
 - a. Activation key should be purchased from OPSWAT.
 - b. Metadefender Core v4 deployment ID can be queried by using REST API (for details see [Get Current License Information](#) page)



Save this deployment ID in your system, you might need this ID when the instance is unavailable at the time of deactivation.

2. Activate license and get the license file using the following URL:
`https://activation.dl.opswat.com/activation?key=<activation key>&deployment=<deployment unique ID>&quantity=<quantity>`
Where *<quantity>* is the number of scan nodes to be connected to this Core instance (most cases it's 1, please refer [8.2. Multi-node deployment](#) for multi-node deployment)

scenarios)

If the activation is successfully, a license file is downloaded. Save this file.

HTTP status codes can be:

HTTP Response	Body	Comment
200 Ok	license file	Activation was successfully.
200 Activation failed	error: '<user conform error message>'	Failed activation
200 Invalid parameter	error: 'Could not activate your product because the Activation Key you provided is invalid. Check if you typed it correctly or open a support ticket if problem persist.'	Invalid key format
200 Invalid parameter	error: 'Could not activate your product because the Deployment ID you provided is invalid. Check if you typed it correctly or open a support ticket if problem persist.'	Invalid deployment format
200 Invalid parameter	error: 'Could not activate your product because the quantity you provided is invalid. Check if you typed it correctly or open a support ticket if problem persist.'	Invalid deployment format
400 Bad request		Missing key, quantity or deployment
500 Internal server error	error: 'Internal server error (<error ID>). Please contact support'	



In case of any activation issue, contact OPSWAT support for help

3. Upload license file to Metadefender Core v4:

The license file should be uploaded to the Metadefender Core v4 to activate the product.

For details see page: [Uploading License Key File](#)

Deactivation steps

1. For deactivation of a deployment ID an activation key is necessary:

- a. Activation key should be purchased from OPSWAT.
- b. Metadefender Core v4 deployment ID can be queried by using REST API (for details see [Get Current License Information](#) page)

2. Deactivate license using the following URL:

<https://activation.dl.opswat.com/deactivation?key=<activation key>&deployment=<deployment unique ID>>

HTTP status codes can be:

HTTP Response	Body	Comment
200 Ok	result: ok	Successful deactivation
200 No active license found	error: 'Could not found any active license with the given parameters'	The license has not been activated yet or it has been deactivated already.
200 Invalid parameter	error: 'Could not deactivate your product because the Activation Key you provided is invalid. Check if you typed it correctly or open a support ticket if problem persist.'	Invalid key format
200 Invalid parameter	error: 'Could not deactivate your product because the Deployment ID you provided is invalid. Check if you typed it correctly or open a support ticket if problem persist.'	Invalid deployment format
400 Bad request		Missing key or deployment

HTTP Response	Body	Comment
500 Internal server error	error: 'Internal server error (<error ID>). Please contact support'	

Important notes



Product activation is tight to several hardware, operating system and software parameters. In case of one or more major hardware or software parameter change the product might turn into deactivated status. Operating system updates, other software updates should not affecting the activation status.

If the product is online activated and has live Internet connection then in case of deployment ID change the product reactivates itself. If the product doesn't have Internet connection then the administrator is responsible to reactivate the product.

Because of the above administrator should consider licensing restrictions of the offline deployments if using any virtualization and/or containerization technologies.

8.2. Multi-node deployment

Metadefender Core is designed to support scaling of the scanning infrastructure by distributing scan requests among several scan nodes. The benefit of having such a distributed infrastructure is that based on node loads, Metadefender Core server can always choose the most appropriate node to assign a new scan task to. In case of high scan load, node tasks are well-balanced to provide robust load balancing.

Metadefender Core servers allow connections from several nodes. The server-node communication is unsecured. Therefore it is advisable to configure a dedicated virtual LAN and open only the respective ports. Alternatively you can set up an ssl-tunnel to encrypt data-flow.

Setting up several Metadefender Core nodes

After activation of the product it is possible to connect as many nodes to your server is allowed by the purchased license. Please note that there is a node running on the Metadefender Core server itself.

The Metadefender Core server needs to be installed on a dedicated server, and the nodes on other machines, using the installation packages applicable to your distribution. To set up multiple nodes both the configuration of the server and the nodes are to be changed according to the following paragraphs.

Installing additional Metadefender Core Node instances

Windows

There are two options to install a node on Windows systems:


- With Install Wizard:
Run the installer (.msi file) and follow the instructions.
- Using command line interface:

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

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

Key	Default Value	Description
SERVERPORT	8007 (in versions before v4.9.0: 8009)	The value should match to the port value defined on the Metadefender Core server.
SERVERADDRESS	-	The value should be the IP address that the Metadefender Core server listens on for accepting external node connections.

Linux

 If the Metadefender Core Node package dependencies are not installed on your system you may need to have a working Internet connection or you may have to provide the Installation media during the installation. Consult your Operating System documentation on how to use Installation media as a package repository.

Debian package (.deb)

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

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

```
sudo yum install <filename>
```

Setup on the server machine on Linux

1. Open the configuration file `/etc/ometascan/ometascan.conf`
2. Within `[global]` section create a new entry called *address*. The value should be the IP address of network interface you want the server be accepting nodes on. If you want to allow all interfaces for this purpose you can either skip this step or define value `0.0.0.0` to this field.
3. Within `[global]` section create a new entry called *port* on with the server accepts connections. The suggested value is `8007`.
4. Restart ometascan service using your distribution service manager utility.

```
[global]
...
address=0.0.0.0
port=8007
...
```

Setup on the node machine(s) on Linux

1. Open the configuration file `/etc/ometascan-node/ometascan-node.conf` on the node machine
2. Within `[global]` section create an new entry called *serveraddress*. The value should be the IP address of the server. If defined at server side these addresses should match.
3. Within `[global]` section create an new entry called *serverport* of which the value should match to the port value defined at server side.
4. Restart ometascan-node service using your distribution service manager utility

```
[global]
...
serveraddress=<server IP>
serverport=8007
...
```

Setup on the server machine on Windows

1. Open the key `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan\global` in Windows Registry
2. Within `global` key create a new string value called **address**. The value should be the IP address of network interface you want the server be accepting nodes on. If you want to allow all interfaces for this purpose you can either skip this step or define value `0.0.0.0` to this field.
3. Within `global` key create a new string value called **port** on with the server accepts connections. The suggested value is `8007`.
4. Restart OPSWAT Metadefender Core service.

Setup on the node machine(s) on Windows

1. Open the key `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan Node\global` in Windows Registry
2. Within `global` key create an new string value called **serveraddress**. The value should be the IP address of the server. If defined at server side these addresses should match.
3. Within `global` key create an new string value called **serverport** of which the value should match to the port value defined at server side.
4. Restart OPSWAT Metadefender Node for Core service.

Note that after specifying the port value in the server configuration, you should set the configuration file of the node which is installed on the server machine.

After these steps Metadefender Core server starts deploying scan engines and malware databases onto the connected nodes, which will be shown on the Metadefender Core web interface in the Inventory Scan nodes menu.

8.3. Using external load-balancer

- [8.3.1. HTTP\(S\) - Layer 7 load balancing](#)

- [8.3.2. DNS load balancing](#)

8.3.1. HTTP(S) - Layer 7 load balancing

This page provides information about recommended ways to use sessions with a Layer 7 load-balancer.

Most load-balancers have the ability to provide cookies for pinning subsequent traffic from a client to the appropriate server. This method is called sticky session, session persistence or session affinity. Using cookies efficiently requires the client to know when a cookie should be sent, should not be sent or should be deleted.

Sticky session load balancing

Each Metadefender Core v4 instance has its own databases and application sessions that cannot be seen by other instances. Therefore, in order to get the related data/response to our queries we should ask the appropriate Metadefender Core v4 server. On the other hand, to keep the advantages of the used load balancing method, cookies should not be sent if it is not necessary.

Single file scanning

Steps

No.	Stage	Task	Cookie usage
1.	Sending file	Initiate processing a file on the client side. Send file through the load-balancer. (See REST API: Scan A File)	Cookie should not be sent.
2.		Save the cookie and the data_id you got from the load-balancer	Save cookie
3.	Getting result	Request result related to data_id saved in step 2. (See REST API: Fetch Scan Result)	Send cookie saved in step 2.
4.		If processing is in progress (See REST API: Fetch Scan Result), wait a little while and repeat step 3.	Send cookie saved in step 2.

Batch scanning

Steps

No.	Stage	Task	Cookie usage
1.	Open batch	Initiate processing file(s) in batch. Request a batch ID through the load-balancer. (See REST API: Initiate Batch)	Cookie should not be sent.
2.		Save the cookie and the batch_id you got from a Core server through the load-balancer.	Save cookie
3.	Sending files	Send file through the load-balancer. (See REST API: Scan file in batch)	Send cookie saved in step 2.
4.		Save the data_id you got from the load-balancer.	-
		Status/result of scanning of sent files can be queried: (See REST API: Fetch Scan Result)	Send cookie saved in step 2.
5.		Repeat step 3-4. with files wanted to be in the same batch.	-
6.	Getting batch status	See REST API: Status of Batch	Send cookie saved in step 2.
7.	Close batch	Tell the server that no more files will be sent to this batch. (See REST API: Close Batch). (This will only be successful if all the files sent to the batch have been processed already. Repeat this step until batch is closed.)	Send cookie saved in step 2.
8.	Getting results	Request results related to batch ID saved in step 2. (See REST API: Download Batch Signed Result).	Send cookie saved in step 2.

If it does not matter which upstream server responds, then query should be sent without cookie.



It is recommended not to send cookies when it's not necessary to allow load-balancer to use its own method to share the load between Metadefender Core v4 servers.

Limitations, additional notes

Using load-balancing between Metadefender Core servers does not support:

- Global scan history
- Core server administration through load-balancer

OPSWAT products that support HTTP load balanced Metadefender Cores

Product name	Minimum version	Further information
MetaDefender Kiosk	does not support yet	-
MetaDefender Client	does not support yet	-
MetaDefender Email Security	4.3.0	-
MetaDefender ICAP Server	4.3.0	-
MetaDefender Vault	does not support yet	-

8.3.2. DNS load balancing

Using this method is logically similar to Layer 7 load-balancing.

Briefly how it works

Client uses a domain name to send a query to a server. Client's DNS server has more "A" records for that name with different IPs. When a client resolves the server's domain name DNS server randomly chooses an IP for that name to send back. When a session is used on the application layer, client should know the IP address of the Core server that handles that specific session. In every other case, client should resolve the domain name with DNS query to let requests to be balanced between Metadefender Core servers.

Single file scanning

Steps

No.	Stage	Task	Addressing
1.	Choose a Core server by using DNS load balancing	Resolve the Core servers' common domain name.	Use domain name
2.		Save the IP gotten from the DNS server.	Save the IP
3.	Sending file	Initiate processing a file on the client side. (See REST API: Scan A File)	Use IP saved in step 2.
4.		Save the data_id got from the Core server	-
5.	Getting result	Request result related to data_id saved in step 2. (See REST API: Fetch Scan Result)	Use IP saved in step 2.
6.		If processing is in progress (See REST API: Fetch Scan Result), wait a little while and repeat step 3.	Use IP saved in step 2.

Batch scanning

Steps

No.	Stage	Task	Addressing
1.	Choose a Core server by using DNS load balancing	Resolve the Core servers' common domain name.	Use domain name
2.		Save the IP gotten from the DNS server.	Save the IP
3.	Open batch	Initiate processing file(s) in batch. Request a batch ID. (See REST API: Initiate Batch)	Use IP saved in step 2.

No.	Stage	Task	Addressing
4.	Sending files	Send file to the specific Core server with the batch ID saved in step 3. (See REST API: Scan file in batch)	Use IP saved in step 2.
5.		Save the data_id you got from the Core server.	-
6.		Status/result of scanning of sent files can be queried: (See REST API: Fetch Scan Result)	Use IP saved in step 2.
7.		Repeat step 3-4. with files wanted to be in the same batch.	-
8.	Getting batch status	See REST API: Status of Batch	Use IP saved in step 2.
9.	Close batch	Tell the server that no more files will be sent to this batch. (See REST API: Close Batch). (This will only be successful if all the files sent to the batch have been processed already. Repeat this step until batch is closed.)	Use IP saved in step 2.
10.	Getting results	Request results related to batch ID saved in step 2. (See REST API: Download Batch Signed Result).	Use IP saved in step 2.

Limitations, additional notes

Using load-balancing between Metadefender Core servers does not support:

- Global scan history
- Core server administration via DNS load-balancing

OPSWAT products that support DNS load balanced Metadefender Cores

Product name	Minimum version	Further information
MetaDefender Kiosk	does not support yet	-

Product name	Minimum version	Further information
MetaDefender Client	does not support yet	-
MetaDefender Email Security	does not support yet	-
MetaDefender ICAP Server	does not support yet	-
MetaDefender Vault	does not support yet	-

8.4. Cloud Deployment

- [8.4.1. AWS Deployment](#)

8.4.1. AWS Deployment

Baseline Requirements: User Deployment Guides

- [Introductory Material](#)
 - [Introduction](#)
 - [Architecture diagrams](#)
- [Planning guidance](#)
 - [Security](#)
 - [Costs](#)
 - [Sizing](#)
- [Deployment guidance](#)
 - [Deployment Assets](#)
- [Operate guidance](#)
 - [Health Check](#)
 - [Backup and Recovery](#)
 - [Routine Maintenance](#)
 - [Emergency Maintenance](#)
 - [Support](#)

- [Accessibility](#)
 - [Reference Materials](#)
 - [Localization](#)

Introductory Material

Introduction

This Deployment Guide provides step-by-step instructions for deploying MetaDefender version 4.9.0 on Amazon Web Services infrastructure.

Organizations interested in protecting their solutions deployed in AWS can leverage MetaDefender to analyze and sanitize files residing, or transitioning, their AWS deployment. MetaDefender can scan and either sanitize or check for known vulnerabilities, depending on the type of traffic it's seeing. The ideal use case would be an organization that allows files to be uploaded to AWS through an external facing web portal. Analyzing files before they are made accessible to the end-users is critical to ensure that no malicious content is allowed and distributed through the web application.

Advanced attacks are concealing the malicious payload and are relying on productivity files (documents, pdfs, images) as a distribution mechanism. Productivity files allow active content to be leveraged, but these features are frequently exploited to execute the malicious behavior.

This guide is for IT infrastructure architects, administrators and DevOps professionals who are seeking to prevent potential malicious traffic being allowed in their AWS Cloud deployment. Threat Prevention is ensured for both productivity files that might be uploaded and for known vulnerabilities that can be identified for all running services/applications deployed in AWS. The vulnerability scanning is checking known vulnerabilities for unpatched OS and running applications.

MetaDefender is provided as an AMI through the AWS Marketplace ([MetaDefender Windows](#) and [MetaDefender Linux](#) offerings) or as a packaged installer available for download through the [OPSWAT Portal](#).

For installing our solution and deploy it without taking leverage of the predefined AMIs and CloudFormation scripts, please review the guideline listed below:

- [8.4.1.1. Install MetaDefender in AWS EC2](#)
- [8.4.1.2. AMI - Single MetaDefender Deployment](#)
- [8.4.1.3. AMI - Distributed MetaDefender Deployment](#)

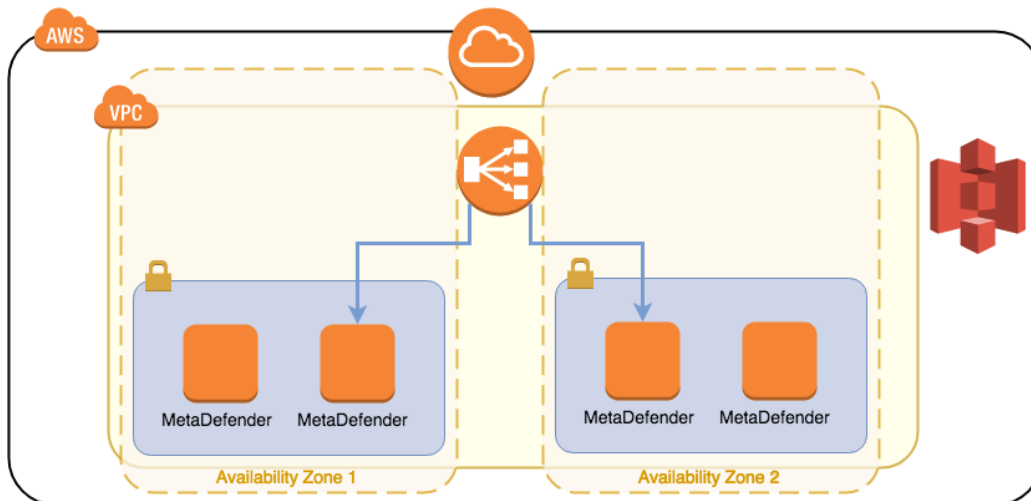
For deploying the available AMIs, we provide the following deployment guidelines and as an example CloudFormation scripts:

- Single deployment of MetaDefender in a public subnet

- Distributed deployment - load balanced MetaDefender instances in 2 private subnets, maintained by OPSWAT Central Management deployed in a public subnet

By using predefined CloudFormation scripts the deployment time will be roughly 3 minutes (for single MetaDefender deployment) or 12 minutes (for distributed deployment)

Architecture diagrams



MetaDefender AWS (2).xml

Planning guidance

Security

Depending on the selected deployment model, we provide guidance on which are the IAM roles and services that MetaDefender needs to interact with.

All the details for each service and their role in the deployment architecture are detailed in the guidelines below:

- [8.4.1.1. Install MetaDefender in AWS EC2](#)
- [8.4.1.2. AMI - Single MetaDefender Deployment](#)
- [8.4.1.3. AMI - Distributed MetaDefender Deployment](#)

Costs

MetaDefender is made available as an annual subscription. Contact our sales team via our Contact form, available here: <https://www.opswat.com/contact>

Considering that there are over 60 different options to license MetaDefender, it is highly coupled to the use case and the advanced features that you are considering deploying. Note that the more functionality you are adding to MetaDefender, the more need will be of CPU from the EC2 instance.

Our recommendation would be a minimum 8 vCPU for our lower tiers. The list of recommended EC2 instances are below:

- m5.xlarge
- m5.2xlarge
- m5.4xlarge
- c5.2xlarge
- c5.4xlarge
- c5.8xlarge

We recommend to go with Reserved Instances, considering that you are committing to an annual subscription for MetaDefender.

For pricing per instance, please refer to the official AWS pricelist: <https://aws.amazon.com/ec2/pricing/>

Sizing

MetaDefender needs an EC2 instance with minimum 8 vCPU, in order to have an optimal response rate to submitted files for analysis. However, depending on the use case and expected throughput (analysis SLA), higher tier instances are recommended.

The system requirements (hardware and supported operating system) are defined here: https://onlinehelp.opswat.com/corev4/2.1._Recommended_System_Requirements.html

Deployment guidance

Deployment Assets

An ideal deployment in AWS will follow this process:

- Store the files in an S3 bucket before they are submitted to MetaDefender
 - In order to avoid any AZ or Region failure, would be recommended to use S3's Cross-Region Replication
- Define a pool of jobs for your webapp, which are in a pending state while MetaDefender analyses the files
 - Best option would be to use the SQS service and your application to send the files from the SQS to MetaDefender

- Every time the files are being uploaded to a temporary S3 bucket, there is a new job added to the SQS
- If MetaDefender fails, the job is still defined in SQS
- If AZ or even the region fails, if the S3 bucket is synced in multiple regions, the SQS queue should be easily able to be reconstructed for the remaining files in the bucket
 - On initializing stage, check the files in the S3 bucket and if there is any file left, add them to the SQS
- Based on the result from MetaDefender, the file should be moved to the final location or its sanitized copy should. Either way, the original file should be deleted from the temporary S3 bucket
- When the job is being removed from SQS, remove also the file from the S3 bucket

Regarding MetaDefender deployment in AWS and its needed assets/services, we provide 3 deployment guides:

- [8.4.1.1. Install MetaDefender in AWS EC2](#)
- [8.4.1.2. AMI - Single MetaDefender Deployment](#)
- [8.4.1.3. AMI - Distributed MetaDefender Deployment](#)

Operate guidance

Health Check

It is important to set a health check of the MetaDefender instance. There are multiple factors that can result in failure of the system, some of them are AWS related (AZ fault, hardware fault) or application fault. Depending on the use case, each customer defines differently what application failed is.

For generic hardware or AZ fault, we recommend always a distributed environment as defined in [8.4.1.3. AMI - Distributed MetaDefender Deployment](#). By deploying MetaDefender in different Availability Zones with a load balancer in front of them, you will always be sure that no hardware fault will result in service interruption.

1. If you have an ELB in front of MetaDefender instances, configure it to do the health checks using the engines status.
 - How to setup ELB to do health checks: <https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>
 - Use Engines status as API endpoint for health check: https://onlinehelp.opswat.com/corev4/Fetching_Engine_Database_Versions.html

2. In case you are not using an ELB or you would like to have a more advanced health check, our recommendation would be to setup a Lambda function to check on each MetaDefender instance. In case of the health check monitored via Lambda, you will have the flexibility to actually adapt based on the REST API response provided by MetaDefender. One of the following should apply:
 - If all engines are healthy, the instance is considered healthy
 - If some of the engines are not up to date or failing, based on the internal policy you might invalidate this MetaDefender instance.
 - Recovery of MetaDefender will be detailed in the next section
 - If the REST API response is an error, the instance should be considered down
3. An even more advanced check can be considered actually submitting a file to be analyzed using a Lambda function. Note that depending on the file size and complexity, workflow configurations and the number of files in the queue, it might result in timing out the Lambda execution.
 - Submit always the same file to MetaDefender through the REST API
 - Compare the response with a baseline

Backup and Recovery

MetaDefender service in general is not storing any data that needs to be recovered or backed-up. Regardless if it's an hardware or service failure, MetaDefender will not recover the files submitted in the queue. In order to have a sustainable service, not affected by any hardware or software failures, the recommendation would be to:

- Store the files in an S3 bucket before they are submitted to MetaDefender
 - In order to avoid any AZ or Region failure, would be recommended to use S3's Cross-Region Replication
- Define a pool of jobs for your webapp, which are in a pending state while MetaDefender analyses the files
 - Best option would be to use the SQS service and your application to send the files from the SQS to MetaDefender
 - Every time the files are being uploaded to a temporary S3 bucket, there is a new job added to the SQS
 - If MetaDefender fails, the job is still defined in SQS
 - If AZ or even the region fails, if the S3 bucket is synced in multiple regions, the SQS queue should be easily be able to be reconstructed for the remaining files in the bucket

- On initializing stage, check the files in the S3 bucket and if there is any file left, add them to the SQS
- Based on the result from MetaDefender, the file should be moved to the final location or it's sanitized copy should. Either way, the original file should be deleted from the temporary S3 bucket
- When the job is being removed from SQS, remove also the file from the S3 bucket

In case of failure of MetaDefender service, follow the instructions defined in the Troubleshooting section: https://onlinehelp.opswat.com/corev4/9._Troubleshooting_Metadefender_Core.html

Routine Maintenance

Always update the MetaDefender deployment with the new versions published either on:

- portal.opswat.com > Products section
- AWS Marketplace

Release Notes are available [here](#).

In general MetaDefender instance has Internet connection. If an offline deployment is considered, make sure you are using either the Central Management or the Update Downloader and that you are uploading the engine updates minimum once a day.

Emergency Maintenance

In case of any availability failures of an AWS Service, recommended actions would be to pass the load to another MetaDefender instances, preferably deployed in a different AZ than the one affected. Any analysis in progress submitted to MetaDefender will be considered lost. However, is highly recommended to build a resilient system that won't rely on MetaDefender to recover the pending jobs, but to be managed by a queuing mechanism (e.g. [AWS SQS](#)). See Backup and Recovery suggested deployment scenarios.

Support

Support policies, costs, levels and SLA's are described on our website, at the Support section: <https://www.opswat.com/support>

Accessibility

Reference Materials

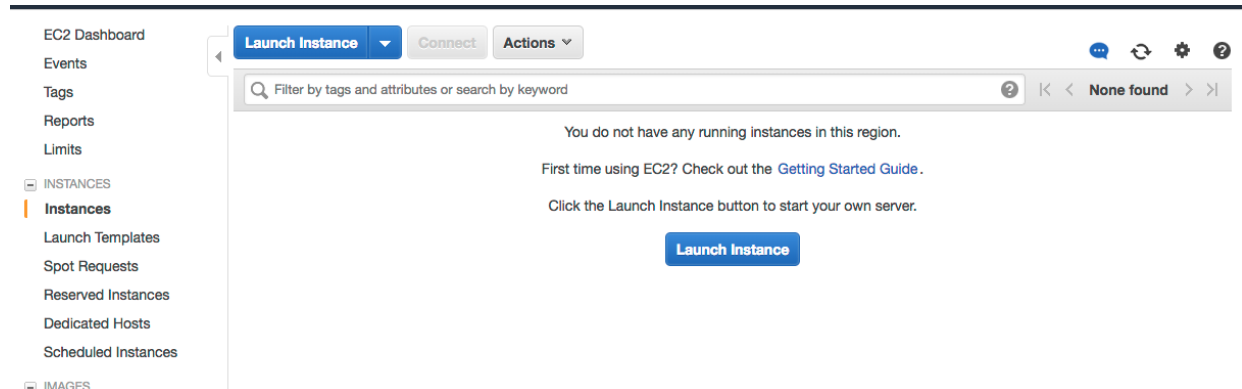
All MetaDefender documentation is available on onlinehelp.opswat.com

Localization

MetaDefender products and documentation are available exclusively in English for now.

8.4.1.1. Install MetaDefender in AWS EC2

1. Go to the EC2 Management Console in AWS and select Launch Instance:



2. Select the desired Operating System you want to run for MetaDefender instance. And then select the instance type.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit 64-bit

OS	AMI ID	Architecture	Root Device Type	Virtualization Type	ENA Enabled	Action
Windows	Microsoft Windows Server 2012 R2 Base - ami-10375468	64-bit	ebs	hvm	Yes	Select
Windows	Microsoft Windows 2012 R2 Standard edition with 64-bit architecture, [English]	64-bit	ebs	hvm	Yes	Select
Windows	Microsoft Windows Server 2012 Base - ami-a20063da	64-bit	ebs	hvm	Yes	Select
Windows	Microsoft Windows 2012 Standard edition with 64-bit architecture, [English]	64-bit	ebs	hvm	Yes	Select
Windows	Microsoft Windows Server 2008 R2 Base - ami-e432519c	64-bit	ebs	hvm	Yes	Select
Windows	Microsoft Windows 2008 R2 SP1 Datacenter edition, 64-bit architecture, [English]	64-bit	ebs	hvm	Yes	Select
Windows	Microsoft Windows Server 2008 SP2 Base - ami-205f3f58 (64-bit) / ami-6cd2b214 (32-bit)	64-bit / 32-bit	ebs	hvm	No	Select
Windows	Microsoft Windows 2008 SP2 Datacenter edition, [English]	64-bit / 32-bit	ebs	hvm	No	Select
SUSE Linux	SUSE Linux Enterprise Server 11 SP4 (PV), SSD Volume Type - ami-7eb31906	64-bit	ebs	hvm	No	Select
SUSE Linux	SUSE Linux Enterprise Server 11 Service Pack 4 (PV), EBS General Purpose (SSD) Volume Type, Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.	64-bit	ebs	hvm	No	Select

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Instance Type	General Purpose	Memory	Storage	EBS Only	Yes	Up to 10 Gigabit	Yes	
<input type="checkbox"/>	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input checked="" type="checkbox"/>	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.24xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
<input type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
<input type="checkbox"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
<input type="checkbox"/>	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes
<input type="checkbox"/>	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m4.16xlarge	64	256	EBS only	Yes	25 Gigabit	Yes
<input type="checkbox"/>	Compute optimized	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

Please review MetaDefender's system requirements (OS and hardware requirements) before choosing the desired AMI and instance type.

3. Select the desired VPC and subnet you would like to have MetaDefender deployed.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: Request Spot Instances

Network: vpc-81fc98e8 | myVPC (default) Create new VPC

Subnet: No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: Add instance to placement group.

Domain join directory: None Create new directory

IAM role: None Create new IAM role

Shutdown behavior: Stop

Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring Additional charges apply.

EBS-optimized instance: Launch as EBS-optimized instance

Tenancy: Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

Elastic GPU: Add GPU Additional charges apply.

Advanced Details

User data: As text As file Input is already base64 encoded

(Optional)

Cancel Previous **Review and Launch** Next: Add Storage

Depending on the deployment model, the recommendation would be to deploy MetaDefender in a private subnet, with no Internet Connection. And to separately deploy an instance of OPSWAT Central Management in a different EC2 instance as part of a public subnet. The 2 subnets need to be able to connect to each other, in order for Central Management to manage and deploy new engine versions to MetaDefender.

From security perspective, no IAM role is needed as of right now for MetaDefender. However, depending on the deployment model, it might be needed in order to have access to different internal resources

- Lambda functions:
 - if Lambda functions are used for product activation/deactivation or to process uploaded files to S3, define an IAM role that grants access to those resources and attach it to the instance
- Advanced Details:
 - Recommended would be to add an User Data script to do the following:
 - Change default credentials from admin/admin to admin/instance-id
 - Activate the product

See [OPSWAT's Github account](#) for scripts references.

4. Storage step can be skipped

In general there's no need for additional storage by MetaDefender. However, there are 2 situations where additional local storage might be required:

- MetaDefender will process large files or a high volume of files which submitted in MetaDefender's queue will need over 10GB files storage
- MetaDefender is configured to store files in the Quarantine section which will eventually fill the entire root volume.

In case quarantining the files in the MetaDefender instance or analyzing high volumes of files is a requirement, please consider adding an EBS volume.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MiB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-00b4d9274c2016b0cc	30	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	xvdb	Search (aws-learn:st)	8	General Purpose SSD (GP2)	100 / 3000	N/A	<input type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

5. Security Groups

There are 2 rules that are needed to be opened during the installation phase, after which only one rule should remain:

- Custom TCP: 8008
 - MetaDefender exposes it's REST API by default to port 8008. However this port can be changed during the installation phase or updated during it's lifetime.
- RDP / SSH
 - In order to install MetaDefender on Windows add access for RDP and for Linux add support for SSH
 - Highly recommended would be not to allow traffic to RDP or SSH from anywhere, but to limit to your IP address

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

Security group name: launch-wizard-12
 Description: launch-wizard-12 created 2018-04-25T15:17:16.925-07:00

Type	Protocol	Port Range	Source	Description
Custom TCP	TCP	8080	Custom 0.0.0.0/0	MetaDefender REST API
RDP	TCP	3389	Custom CIDR, IP or Security Group	RDP

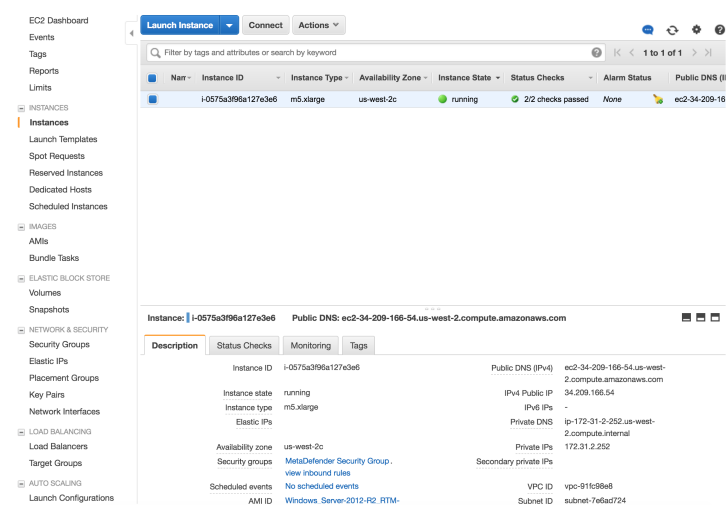
Add Rule

Warning
 Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

After the installation remove RDP or SSH from this Security Group!

6. Launch the instance

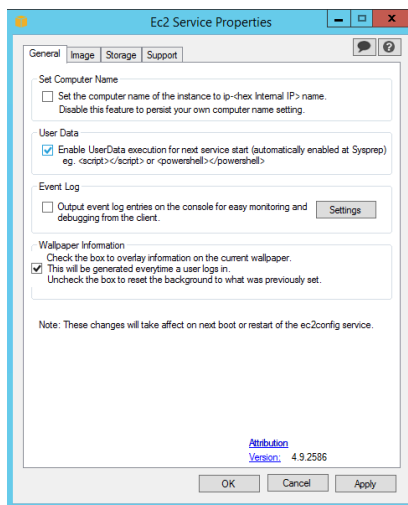
After you review the settings, hit Launch. In a few minutes the instance should become available



7. Additional steps

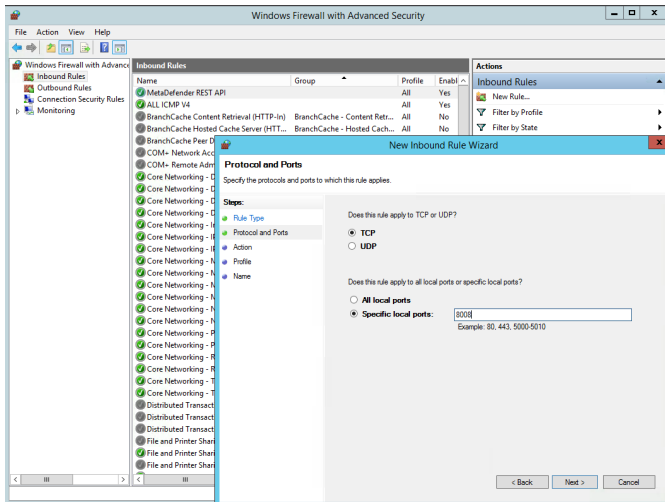
1. User Data

- In case you've added a User Data script, make sure that running User Data is enabled on the new instance



For instances running Windows OS versions, make sure that Windows Firewall will allow traffic to 8008.

In order to do that, RDP into the instance, open Windows Firewall and Advanced Security and create a New Rule for Inbound. Select Ports and choose the port you'll going to use for MetaDefender API (default is 8008).



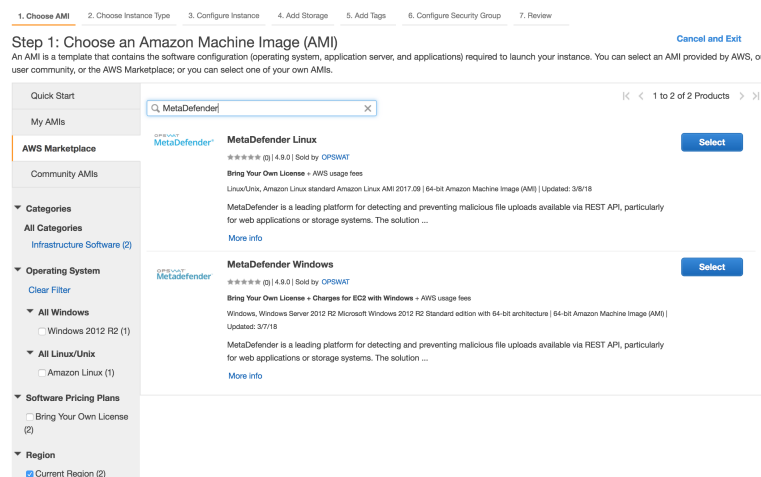
8.4.1.2. AMI - Single MetaDefender Deployment

For a single deployment of MetaDefender in a public subnet, refer to the CloudFormation script provided as example.

In this example, besides the MetaDefender EC2 instance, additional resources are being generated and set up.

Deployment flow:

Select the desired MetaDefender, based on the OS support:



Go through the steps to launch an instance (steps defined here: [8.4.1.1. Install MetaDefender in AWS EC2](#))

Or, use the CloudFormation template available on [OPSWAT's Github account](#). Feel free to review it and modify it accordingly.

To launch the CloudFormation script, follow these steps:

1. Go to CloudFormation > Create Stack and select the template (or import it):
2. Fill the needed details:
 - Stack name : Identifier for this entire MetaDefender stack
 - Activation Key: MetaDefender license key
 - AMI: grab the AMI id from the AWS Marketplace or from your own built MetaDefender AMI
 - KeyName: the keypair you would like to use in order to manage this instance
 - Note that it's very important to provide a valid key, especially if you plan to connect to this machine for different investigations
 - VPC and Subnet: Select from the dropdown which is the VPC and the subnet used for this instance.
 - a. Note that it's very important that the selected subnet will provide MetaDefender Internet access, in order to get all the needed updates.

The screenshot shows the 'Specify Details' step of the AWS CloudFormation 'Create Stack' wizard. The breadcrumb navigation at the top reads 'CloudFormation > Stacks > Create Stack'. On the left, there are navigation links: 'Select Template', 'Specify Details' (which is active), 'Options', and 'Review'. The main content area is titled 'Specify Details' and contains a sub-header: 'Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.' Below this, there are several input fields:

- Stack name:** A text input field with a copy icon.
- Parameters:** A section containing several fields:
 - ActivationKey:** A text input field with a tooltip: 'MetaDefender Windows License key - please note that same key might have multiple activations.'
 - AMI:** A text input field with a tooltip: 'Specify the MetaDefender AMI.'
 - InstanceType:** A dropdown menu currently showing 'm4.xlarge' with a tooltip: 'Select desired instance type'.
 - KeyName:** A dropdown menu with a search icon and a tooltip: 'Specify key pair name used to connect to this instance'.
 - Subnet:** A dropdown menu with a search icon and a tooltip: 'Specify the subnet'.
 - VPC:** A dropdown menu with a search icon and a tooltip: 'Specify the desired Virtual Private Cloud.'

 At the bottom right of the form, there are three buttons: 'Cancel', 'Previous', and 'Next'.

3. Finish the wizard, acknowledge that IAM roles are being generated and hit Create

The CloudFormation script will generate the needed resources to provide the following flow:

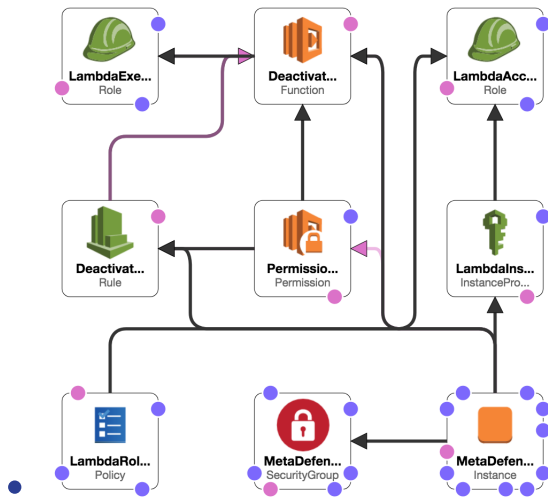
- Instance initialize phase
 - User Data script (Powershell for Windows and shell for Linux) will be called which will:
 - change the credentials from the default admin/admin to admin/instance-id
 - updates the CloudWatch Event Rule to be dispatched only for the instances running MetaDefender (adds the new instance-id to the existing list)

- updates the Deactivate Lambda function by mapping the instance-id to the MetaDefender's unique deploymentId
 - activate the product based on the provided activation key
- Instance shutting-down / terminate
 - Deactivate Lambda function will call the OPSWAT Activation Server to deregister the existing MetaDefender deployment
 - Results are logged in CloudWatch
- Instance rebooted
 - Respects same flow as Initialize phase

Resources:

- MetaDefender Windows EC2
 - The VM running the MetaDefender instance
- MetaDefenderSecurityGroup
 - Only the TCP port 8008 is opened, being the only port needed to communicate with MetaDefender
- LambdaAccessRole
 - IAM Role created for to the EC2 instance, to allow it to update the DeactivateLambda function and the DeactivateEventRule
- LambdaRolePolicies
 - The IAM Policy which grants access to update the defined lambda function and CloudWatch event rule
- LambdaInstanceProfile
 - IAM InstanceProfile that is attached to the EC2 instance
- DeactivateLambda
 - Calls the OPSWAT's Activation Server to deregister the MetaDefender instance on termination.
- LambdaExecutionRole
 - IAM Role to allow running the lambda function and publishing the results in logs
- DeactivateEventRule
 - CloudWatch EventRule which allows to monitor the EC2 instance and calls DeactivateLambda on shutting-down or stopping.
- PermissionForEventsToInvokeLambda

- Lambda Permission needed to invoke the DeactivateLambda function
- Resources and relationships:

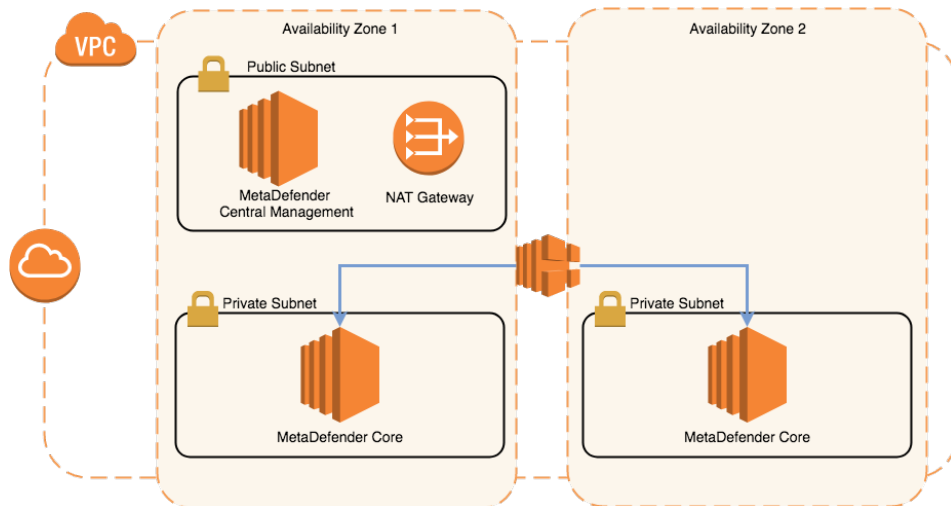


8.4.1.3. AMI - Distributed MetaDefender Deployment

For a distributed environment, we would recommend to use MetaDefender Central Management deployed in a public subnet and MetaDefender Core instances deployed in private subnets, in separate Availability Zones.

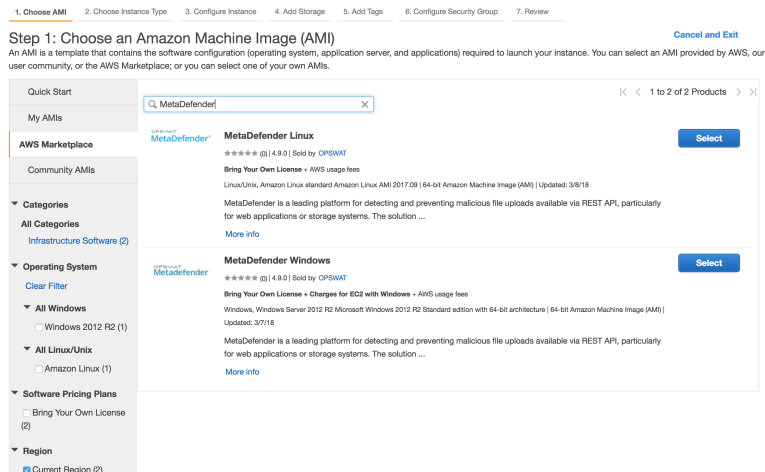
OPSWAT provides a CloudFormation template as an example of the deployment seen in the diagram below.

Deployment Diagram:



Deployment flow:

Select the desired MetaDefender, based on the OS support:



Go through the steps to launch an instance (steps defined here: [8.4.1.1. Install MetaDefender in AWS EC2](#))

Or, in order to use the CloudFormation template provided, please see [OPSWAT's Github account](#). Our recommendation would be to use this template as an example and modify it accordingly to your business requirements.

To launch the CloudFormation script, follow these steps:

1. Go to CloudFormation > Create Stack and select the template (or import it):
2. Fill the needed details:
 - Stack name : Identifier for this entire MetaDefender stack
 - Availability Zones
 - Select at least 2 availability zones in the selected region
 - Network Configuration
 - Distribution of the CIDR blocks
 - Configure the needed IP allocation per subnets
 - If needed, create additional private subnets with dedicated ACL, not default ones.
 - EC2 Configuration
 - KeyName: the keypair you would like to use in order to manage this instance
 - Note that it's very important to provide a valid key, especially if you plan to connect to this machine for different investigations
 - NAT instance type

- This is important for regions where NAT Gateway are not yet available (e.g. GovCloud)
- MetaDefender Configuration
- Activation Key: MetaDefender license key
- AMI:
 - Both for Central Management and Core
 - Grab the AMI id from the AWS Marketplace or from your own built MetaDefender AMI

The screenshot shows the 'Specify Details' step of the AWS CloudFormation 'Create stack' wizard. The form includes the following sections and parameters:

- Specify Details:** Stack name (text input).
- Parameters:** A section for defining stack parameters.
- Availability Zone Configuration:**
 - Availability Zones: Search field.
 - Number of Availability Zones: 2. Note: Number of Availability Zones to use in the VPC. This must match your selections in the list of Availability Zones parameter.
- Network Configuration:**
 - VPC CIDR: 10.0.0.0/16. Note: CIDR block for the VPC.
 - Public subnet 1 CIDR: 10.0.128.0/20. Note: CIDR block for the public (DMZ) subnet 1, located in Availability Zone 1.
 - Create private subnets: 3/4. Note: Set to false to create only public subnets. If false, the CIDR parameters for ALL private subnets will be ignored.
 - Private subnet 1A CIDR: 10.0.0.0/19. Note: CIDR block for private subnet 1A, located in Availability Zone 1.
 - Private subnet 2A CIDR: 10.0.32.0/19. Note: CIDR block for private subnet 2A, located in Availability Zone 2.
 - Create additional private subnets with dedicated network ACLs: false. Note: Set to true to create a network ACL, protected subnet in each Availability Zone. If false, the CIDR parameters for those subnets will be ignored. If true, it also requires that the 'Create private subnets' parameter is also true to have any effect.
 - Private subnet 1B with dedicated network ACL CIDR: 10.0.192.0/21. Note: CIDR block for private subnet 1B with dedicated network ACL, located in Availability Zone 1.
 - Private subnet 2B with dedicated network ACL CIDR: 10.0.200.0/21. Note: CIDR block for private subnet 2B with dedicated network ACL, located in Availability Zone 2.
 - VPC tenancy: default. Note: The allowed tenancy of instances launched into the VPC.
- Amazon EC2 Configuration:**
 - Key pair name: Search field. Note: Public/private key pairs allow you to securely connect to your EC2 instances after it launches. This is used only if the region does not support NAT gateways.
 - NAT instance type: t1.small. Note: Amazon EC2 instance type for the NAT instances. This is used only if the region does not support NAT gateways.
- Other parameters:**
 - ActivationKey: MetaDefender Windows License key - please note that same key might have multiple activations.
 - CentralMgmtAMI: Specify the MetaDefender Central Management AMI.
 - CoreAMI: Specify the MetaDefender Core AMI.
 - InstanceType: t1.micro. Note: Select desired instance type.

3. Finish the wizard, acknowledge that IAM roles are being generated and hit Create

The CloudFormation script will generate the needed resources to provide the following flow:

- Instance initialize phase
 - Central Management
 - User Data script (Powershell for Windows and shell for Linux) will be called which will:
 - change the credentials from the default admin/admin to admin /instance-id

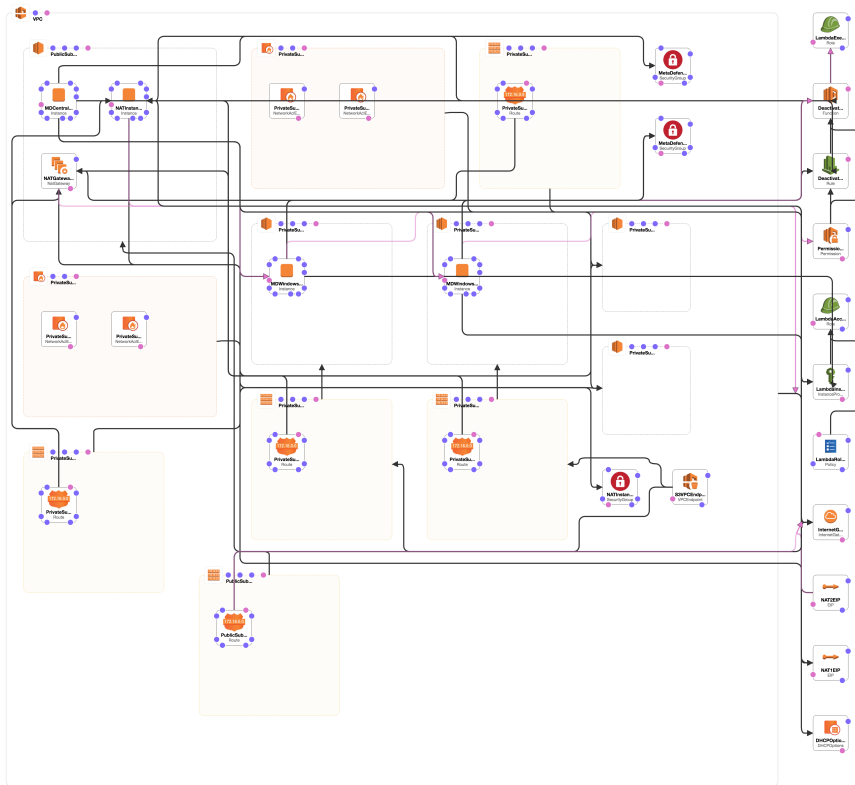
- updates the CloudWatch Event Rule to be dispatched only for the instances running MetaDefender (adds the new instance-id to the existing list)
- updates the Deactivate Lambda function by mapping the instance-id to the MetaDefender's unique deploymentId
- activate the product based on the provided activation key
- attach the running MetaDefender instances
- activate MetaDefender instances and push the activation file to MetaDefender instances
- MetaDefender Core
 - User Data script (Powershell for Windows and shell for Linux) will be called which will:
 - change the credentials from the default admin/admin to admin /instance-id
- Instance shutting-down / terminate
 - Deactivate Lambda function will call the OPSWAT Activation Server to deregister the existing MetaDefender deployment
 - Results are logged in CloudWatch
- Instance rebooted
 - Respects same flow as Initialize phase

Resources:

- MetaDefender Windows MDWindowsEC2AZ1
 - The VM running the MetaDefender instance in Availability Zone 1
- MetaDefender Windows MDWindowsEC2AZ2
 - The VM running the MetaDefender instance in Availability Zone 2
- MetaDefenderSecurityGroup
 - Only the TCP port 8008 is opened, being the only port needed to communicate with MetaDefender
- CentralManagementSecurityGroup
 - Only the TCP port 8018 is opened, being the only port needed to communicate with MetaDefender Central Management
- LambdaAccessRole

- IAM Role created for to the EC2 instance, to allow it to update the DeactivateLambda function and the DeactivateEventRule
- LambdaRolePolicies
 - The IAM Policy which grants access to update the defined lambda function and CloudWatch event rule
- LambdaInstanceProfile
 - IAM InstanceProfile that is attached to the EC2 instance
- DeactivateLambda
 - Calls the OPSWAT's Activation Server to deregister the MetaDefender instance on termination.
- LambdaExecutionRole
 - IAM Role to allow running the lambda function and publishing the results in logs
- DeactivateEventRule
 - CloudWatch EventRule which allows to monitor the EC2 instance and calls DeactivateLambda on shutting-down or stopping.
- PermissionForEventsToInvokeLambda
 - Lambda Permission needed to invoke the DeactivateLambda function

Resources and relationships:



9. Troubleshooting Metadefender Core

In this section you can find solutions for generic issues with Metadefender Core

Installation issues

- [Inaccessible Management Console](#)

Issues with nodes

Metadefender Core should log and display any issue related to scan nodes. For more information about these kind of issues, go to

- [Possible Issues on Nodes](#)

Where are the Metadefender Core logs located?

Metadefender Core generates log files to **/var/log/ometascan** under Linux and to Windows Event Log under Windows.

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

- [How to Read the Metadefender Core Log?](#)

How can I create a support package?

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

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

- [How to Create Support Package?](#)

Issues under high load

- [Too Many Sockets or Files Open](#)
- [Too Many TIME_WAIT Socket](#)

How to Create Support Package?

A support package contains essential information regarding the operating system and OPSWAT software found on the machine.

Creating the package on Linux

To create a package you have to start the `/usr/bin/ometascan-collect-support-data.sh` for Core and `/usr/bin/ometascan-node-collect-support-data.sh` for Node.

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

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

```
ometascan-support-<TIMESTAMP>.tar.gz  
ometascan-node-support-<TIMESTAMP>.tar.gz
```

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

Example:

```
ometascan-support-1439983514.tar.gz  
ometascan-node-support-1506936465.tar.gz
```

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

Creating the package on Windows

To create a package you have to start the script found under the installation directory of the product, default is `C:\Program Files\OPSWAT\Metadefender Core\ometascan-collect-support-data.bat` for Core and `C:\Program Files\OPSWAT\Metadefender Core Node\ometascan-node-collect-support-data.bat` for Node.

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:

```
ometascan-support-<TIMESTAMP>.zip  
ometascan-node-support-<TIMESTAMP>.zip
```

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

Example:

```
ometascan-support-1439983514.zip  
ometascan-node-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 Metadefender Core Log?

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

Files

Under Linux the server and nodes generate separate log files under `/var/log/ometascan`.

The **ometascan.log** file (if present) belongs to the server and the **ometascan-node.log** file (if present) belongs to the installed scan node.

Under Windows there is no default logging into file unless otherwise specified. For details see [Startup Core Configuration](#) and [Startup Node Configuration](#) accordingly.

Format

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

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

Example:

```
[INFO ] 2015.08.19 09:40:27.941: (core.workflow) Scan finished,  
dataId='c35a190681944380a52efb9ef32ef509', overallResult='No  
Threat Detected', totalResultCount='5', infectedResultCount='0'  
[msgid: 82]
```

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 Metadefender 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 Metadefender 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 Metadefender server for the Web Management Console. Consult your Distribution manual on how to configure a firewall in your distribution.

Possible Issues on Nodes

Q. Node detected 3rd party product on system

Scan node detected that a 3rd party protection product is installed on the same system where the node is. This product blocks the scan node from proper functioning.

Issue:

A 3rd party product blocks our operation. The node or some of the engines can not access the file that are currently under processing.

Solution:

The blocking product should be uninstalled or disabled for the resource directory of node to work properly.

Other solution might be to exclude the specific directory mentioned in the description from the real-time scanning.

How to recover node:

After doing the necessary steps the node should work correctly, no further steps needed. The notification about the issue will disappear within a few minutes, when the node detects the blocking was eliminated.

Q. There is no scan node connected

To ensure that Metadefender nodes can connect Metadefender Core check the following:

1. Check if your license allows connecting as many nodes as you need.
2. Check if node service is running properly both on Core Server side and on remote machines, if any. Start/restart them, if necessary. For details visit windows or packages.

3. Check if your node configuration is valid. For more information see [Startup Node Configuration](#).
4. In case of having running nodes on remote machines check firewall settings to have necessary ports open. For port settings see [Startup Core Configuration](#).
5. Check node log for further details.

If none of the above solves connecting issues then create a support package for submitting OPSWAT. For details on doing so see [How to Create Support Package?](#).

Too Many Sockets or Files Open

Only on Linux systems: if too many sockets or files are open by the process this can cause problems.

How to detect

Check the file descriptor limit:

```
ulimit -n
```

Check the used file descriptor count on a running process:

```
watch -n 1 "ls /proc/\`ps -eo comm,pid | awk '\$1 == \"ometascan-node\" { print \$2 }'\`/fd | wc -l"
```

Replace the ometascan-node to ometascan if needed.

If the count is close to the limit this will cause problems.

Rule of thumb: 1 scan workflow requires 2-3 file descriptors.

Solution

Increasing the number of file descriptors

The command **ulimit -n** displays the current set number of maximum file descriptors. In order to increase this number follow the next steps:

Append this line to **/etc/sysctl.conf**

```
fs.file-max = 65535
```

Add the following lines to `/etc/security/limits.conf`

```
* soft proc 65535
* hard nproc 65535
* soft nofile 65535
* hard nofile 65535
```

Restart the system to apply the new configuration. After restart you can check the changed limit by issuing `ulimit -n`.

```
> ulimit -n
> 65535
```

Starting from Metadefender Core v4.0.1 product set up sets a higher limit during the installation and service start.

Too Many TIME_WAIT Socket

This trouble is only on Linux systems.

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

How to detect

Kernel message:

```
kernel: TCP: request_sock_TCP: Possible SYN flooding on port 8009.
Sending cookies. Check SNMP counters.
```

Check the TIME_WAIT sockets count:

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

If it is close to the available port range then your system is suffers from this issue:

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

Solution

You should enable socket reusing

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

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

To avoid waiting on closed sockets and enable reusing them set `tcp_tw_reuse` sysctl to enable reusing of `TIME_WAIT` sockets by appending the following line to file `/etc/sysctl.conf`:

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

After this, sockets in state `TIME_WAIT` will be reused when necessary.

Technical Insights

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

10. Release notes

Version v4.13.2

Release date: 21 Nov, 2018

New features:

- Tiles on Dashboard are linked to the corresponding pages
- More options to filter Processing History (Post Actions and CDR)

Fixed issues:

- In case of an engine hangs, the communication channel is blocked between the Node and the Core, so more engines can time out
- Clean-up mechanism removes files still in use
- Various engine handling issues

Version v4.13.1

Release date: 31 Oct, 2018

Fixed issues:

- Yara and DLP tasks are not stopped on cancelling a processing
- Batch processings cannot be cancelled via web management console
- "Can't process shared resource file" error message did not contain the file name

Version v4.13.0

Release date: 16 Oct, 2018

Important:

- Yara engine integration

New features:

- Processing history entries can be colorized
- Files can be marked as suspicious if less than a given number of engine mark it as infected
- Processings can be cancelled via web management console

- Default rules are added for MetaDefender Email Security
- Bulk operations in quarantine

Fixed issues:

- Extracted files are left behind
- On Debian based systems, on upgrades, engines are deleted and disabled engines are re-enabled

Version v4.12.2

Release date: 3 Oct, 2018

Fixed issues:

- In case of archive processing, sometimes clean-up mechanism removes some extracted files before processing is finished

Version v4.12.1

Release date: 26 Sept, 2018

New features:

- Files can be whitelisted/blacklisted by their checksums
- More specific log entries for CDR

Fixed issues:

- Details of scan result for nested archives (for the file itself not for the content) is not propagated to the top level
- The value, set in "MAX TOTAL SIZE OF EXTRACTED FILES" is handled incorrectly
- Older configs cannot be imported into v4.12.0

Version v4.12.0

Release date: 15 Sept, 2018

Important:

- Data Loss Prevention functionality

New features:

- Possibility to set the number of engines that required to start file processings (per workflow)

- Possibility to exclude engines from processings (per workflow)
- Improved user interface performance
- Possibility to blacklist/whitelist files by file types besides file type groups
- Re-designed workflow tab list appearance
- Possibility to set timeout for sessions regardless of user activity

Fixed issues:

- On Node details page, every issue appears multiple times
- Despite not detecting any vulnerabilities, the vulnerability tab appears
- On hash lookup page, empty hash can be searched
- Sanitized output file name validation can cause user interface stalled

Version v4.11.3

Release date: 30 Aug, 2018

Fixed issues:

- Whitelist page under Inventory menu does not exist (only UI issue)

Version v4.11.2

Release date: 29 Aug, 2018

New features:

- The access_log Nginx directive now can be overridden
- The parallel count parameter now can be set per engine
- Minor changes on user interface for better user experience

Fixed issues:

- A critical CSV injection vulnerability in the CSV export functionality (issue reported by Wojciech Reguła, SecuRing)
- Archives can be sanitized even in case of partial processing (e.g. exceeded archive size, exceeded archive file number)
- In some cases, blocked results can be overwritten by an allowed result with higher priority
- Inconsistent operation of MetaDefender Cloud integration

- Typos on the user interface
- Abandoned files left behind after processings

Version v4.11.1

Release date: 8 Aug, 2018

Fixed issues:

- Unexpected Core and Node service restart in some corner cases
- Using remote syslog server slows down the product in case of missing PTR record in DNS
- Empty files are skipped in archives
- Incomplete archive extraction issue happened on heavily overloaded systems

Version v4.11.0

Release date: 11 July, 2018

New Features:

- Exceptions (by mime-type) from whitelist/blacklist
- New engine page called Technologies
- Support for user-friendly engine configuration (depends on the engine version)
- Welcome wizard

Fixed issues:

- Slow clean-up mechanism
- Abandoned files after uninstall in Windows
- Temporary files are left behind after processings
- Wrong sanitized output file name in some cases
- Default workflows can be overridden on config import
- Core crashes

Version v4.10.2

Release Date: 27 June, 2018

Fixed issues:

- Uninstall not properly cleans the system
- The "whitelisted" and "blacklisted" results are overridden by "infected" result
- Node crashes
- Inconsistent results in case of archive processing: In case of processing an archive more times, the result may be different by cases (infected/exceeded archive file number /exceeded archive size)

Version v4.10.1

Release Date: 23 May, 2018

New features:

- Data Sanitization engine [time-out and retry count](#) is now configurable
- REST API: process info contains the name of the last scanned file when scanning archive file types
- REST API: Configurations that may change the final scan result since the time of processing will be included in the [process info response](#) (i.e., outdated definitions)
- Hash based result lookups can be filtered by rule name

Fixed issues:

- Sanitized DB integrity issue
- On the dashboard, category names of doughnut charts were truncated
- In case of archive processing, the "Not scanned" result to a file is not propagated to a higher level (overall verdict)

Version v4.10.0

Release Date: 2 May, 2018

Important:

- Added support for the LDAP directory type
- Syslog messages can now be sent to multiple log aggregators
- MetaDefender installers no longer use eicar test files

New features:

- AD and LDAP directories can now be configured with multiple servers
- Sanitization failures are marked with a badge in the scan session summary

- Admin's will be notified if a third party solution is blocking MetaDefender from working as expected
- Users can now be granted API keys manually
- Paginated archive results
- HTTPS can now be enabled from web management console

Fixed issues:

- Improved license status info
- In some cases, sanitized files had faulty names
- Suspicious scan results were not always at the top of the list in archive file types
- Inappropriate handling of user rights in the Whitelist page
- AD group members did not have user profiles
- Misleading license information

Version 4.9.1

Release Date: 28 February, 2018

New features:

- New-looking user interface
- Workflows based on the default one (not edited by workflow editor) will be kept and upgraded on version upgrade in the future
- It is allowed blacklisted/whitelisted files to be processed

Fixed issues:

- Security zone: IP address validation
- Cancelled batches are displayed as in-progress
- Removing certificates from the inventory caused policies to disappear
- Memory leak in Node
- Access via Active Directory is not logged
- Sluggish pages under Policy menu

Version 4.9.0

Release Date: 13 December, 2017

New features:

- IPv6 support
- Global whitelist by hash
- Whitelist by file type group
- Display more security related information on dashboard
- Changed default port for external nodes to 8007
- New default security rule for Metadefender Secure File Transfer (SFT)
- Performance tuning of processing history
- Improved resource handling on Node
- On Linux, multiple nginx worker processes for better scaling

Fixed issues:

- Upgrades overwrite existing configuration (IP, port, etc.)
- Resource folder clean up after data sanitization
- Update timing settings affect manual updates
- Poorly handled invalid update files
- Poorly handled UTF-8 characters in output file name for sanitized files
- /hash API can give "in progress" result

Version 4.8.2

Fixed issues:

- Fixed a memory leak caused by failed update download
- Fixed a possible crash issue at Scan history manual cleanup in case of high load
- Fixed a memory leak in case of recurring failed database deployment on Node

Version 4.8.1

Release Date: 5 October, 2017

New features:

- Improved engine/database update distribution to nodes
- Improved archive extraction limit handling
- Improved engine monitoring

- More precise time duration measurement for requests
- API for canceling scans (file/batch scans)
- Option to disable archive extraction of office documents
- For batch scans, certificate validity interval can be set
- Improved scan result badge

Fixed issues:

- Fixed issue of scans stuck in "in progress" state
- Fixed possible product crash during archive scanning
- Fixed update bug where incorrect packages left behind
- Fixed failed quarantine handling
- Fixed handling unavailable engine during scans
- Scan result JSON now contains file name in UTF-8 format
- Limited number of parallel Post Action and External Scanner scripts
- Archive handling parameters now have upper bound
- Improved archive handling
- Archive related failure handling

Version 4.8.0

New features:

- Quarantine for blocked files
- Scanning files in batch (REST API)
- Certificate and key handling for scan batch signing
- Configurable sanitized file name
- Post action commands gets the result JSON with final verdict included
- Increased scan history export interval
- Improved archive bomb handling
- Added eng_id to scan_results.scan_details (REST API)
- Showing in-progress files in "extracted files" list of archives
- Added "scan_all_result_a" into "extracted_files" (REST API)

Fixed issues:

- Fixed case insensitive username comparison in Active Directory integration
- Process workflow revamped (post actions run every time)

- Fixed non-updated policy user interface after added new user roles
- Fixed handling of database upgrade errors in linux package installers
- Fixed error handling when scan target was sent in the body and via filepath (/file REST API)
- Fixed disconnected ghost node issue displayed on user interface

Version 4.7.2

Issues fixed:

- Fixed bug that could cause policies to not contain any elements and forbid user to create new items
- Fixed bug where Core could download older version of engines where newer one was already downloaded

Version 4.7.1

Issues fixed:

- Fixed upgrade of scan configuration
- Fixed ghost nodes appeared on Inventory→ Nodes page

Version 4.7.0

New features:

- Active Directory integration
- Custom post actions
- Redesigned user interface
- External (customer developed) scanner integrations
- Policies export/import
- Archive sanitization
- Individual log message level override
- Aggregated archive scan result in Scan History
- Self-lockout protection, admins can not delete themselves
- gzip and base64 encoding now supported on /file REST API
- Able to navigate through archive hierarchy
- Timezone changed to local in log messages

- Metadefender Cloud integration hostname changed to api.metadefender.com

Issues fixed:

- Fixed scanning of .lnk files on Windows
- Fixed blacklisting of Unicode filenames
- Automatically downloads packages again if the previous download failed
- Fixed order of extracted files on scan details view
- Fixed rare temporary file leak during archive scan

Version 4.6.3

Issues fixed:

- Improved scan result fetching performance for big archives

Version 4.6.2

Issues fixed:

- Improved archive extraction performance
- Fixed a race condition in /file/<data id> REST API that could provide access error in some cases
- Fixed advanced engine config reload for Data sanitization engine
- Fixed login issue which happened when many login request was initiated concurrently
- Fixed calculation of extracted file count

Version 4.6.1

New features:

- List of path for local files can be blacklist / whitelist with specific error message on REST

Issues fixed:

- Invalid external Node listening IP/port config stops product startup
- Connection to remote syslog is reactivated on network error
- If user has no right to use a rule, following rules in order will still be checked
- sending HEAD request where GET should have been sent will not lead to product crash

- Ensure resource file deletion on Microsoft Windows when a scan engine locks file further than expected
- Scan history CSV export uses comma as separator
- Fixed potential Node service crash when stopping during scanning
- More specific error message when uploaded file size limit exceeded
- Fixed a rare race condition in update downloader component
- Fixed login issue when Core v3 like URL is used by the admin (/management)

Version 4.6.0

New features:

- Multiple user roles introduced with different access rights
- Scan Agent has been renamed to Scan Node
- Role (user group) based rule availability configuration
- Role based scan result visibility with different level of details exposed
- Ability to export part of scan history into STIX/Cybox format
- Ability to export part of scan history into CSV format
- Filter on rule and source added into Scan history
- Configurable lockout feature against brute force login attack
- Official support introduced for Ubuntu 16.04
- Detection threshold (suppress threat detection if less than X engines detected a threat)
- Custom engine configuration via user interface
- Free text search functionality in user guide
- Suspend engine testing/deployment to Node when 3rd party security software blocks access to malware files
- Successful login / unsuccessful login / lockout events are logged
- Option to send engine issue count info during update
- [REST API] /file/{data_id} response for scan results now contain process info block for extracted files
- Initiating local scan is faster as no wait for hashing is required

Issues fixed:

- [REST API] /file/{data_id} blocked reason change to mirror V3 API

- Fixed handling of archive extraction depth
- More flexible and stable internal database upgrade when upgrading product
- Custom engine update timeout increased to one hour to deal with slow engine updates
- Archive engine fixes (non-ASCII filenames in archive)
- Engine handling fixes, improved handling of engine deinitialization
- More precise engine cleanup when removing engines
- Fixed bug where random connections were rejected every 2 min
- Fixed bug regarding updates handling (conflicting names)
- Filesize is now correctly displayed on scan result user interface
- Support package generator now includes auditlog db

Version 4.5.1

Issues fixed:

- Fixed possible crash of Agent when there is database which is handled by engine
- Fixed possible crash of Core that could occur when updating a package

Version 4.5.0

New features:

- Data Sanitization of files to protect against unknown threats
- Filetype mismatch detection
- Improved user interface responsiveness for small screens
- Real filetype based blacklist option in rules/workflows
- Improved licensing for offline deployments
- Added product specific proxy settings in the Linux version
- Advanced configuration for allowed/blocked file scan result types

Issues fixed:

- Fixed local scan option user interface for new rules
- Fixed Scan History auto cleanup collision with manual cleanup
- Potential issue fixed for update file upload
- /apiversion interface is added to easily determine REST API compatibility level

Version 4.4.1

New features:

- Added several features/improvement for better Metadefender Kiosk integration
- Full audit log about any configuration changes via Web user interface or REST API
- Able to disable applying update in user configurable time periods
- Core can act as an update source for OESIS product line
- Detect if the analyzed binary is a part of any vulnerability detection
- Improved scan engine status monitoring and auto recovery
- Custom directory can be set for storing temporary files
- Able to set up apikey for every user for easier REST API integration
- Improved hardware detection in license component

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
- Fixed a path specification issue in local file scanning feature on Windows
- Fixed engine counting on Agent details page (do not count utility type engines)
- Fixed lost agent connection handling
- Fixed handling of unsupported Transfer-Encoding on REST API
- Patched internal nginx web server to fix CVE-2016-4450
- Fixed archive timeout handling and user interface
- Fixed scan results in case of archive related findings
- Improved logging of proxy usage
- Improved handling of slow file uploads
- Detailed logging in case of SSL connection issues
- Improved auto-recovery of engines running under Emulated Windows

Version 4.3.0

New features:

- Introduced official support for Microsoft Windows 7 or newer and Microsoft Windows Server 2008 R2 or newer
- Added offline update picker feature to make it easy to apply offline updates without user interaction or scripting
- Able to scan local files stored on server without transferring the content via REST API
- Added hardware related info into generated support package
- Created a framework in Linux version to be able to run Windows scan engines on Linux server
- Option added to log to a remote syslog server
- Inventory / Scan Agents page extended with more detailed agent information
- Parameter workflow renamed to rule in some REST APIs
- Improved system issue notification on Web Management Console
- Added detection of 3rd party anti-malware products that break operation of Metadefender Core
- Improved scan performance of various engine integrations

Issues fixed:

- Improved documentation of multiple REST APIs
- Fixed failed scans during some engine or database update
- Removed unmeaningful database age display of non-anti-malware engines

Version 4.2.0

New features:

- product name has changed to Metadefender Core
- able to use scan results from metadefender.com
- workflow options can be configured from Web Management Console
- workflow options can be overridden from rule editor window
- support for system wide HTTPS proxy
- it is possible to configure maximum file size of scanned files
- filtering security rule by user agent is now possible
- eliminate limitations on the size of scanned files
- improved scan related log messages

- deployment can now be deactivated on the License page
- automatic deployment reactivation of online installations if license becomes invalid
- Metascan v3 URLs (/management and /metascan_rest) are now redirected to the proper v4 URLs
- check disk space before/during scan requests

Issues fixed:

- fixed encrypted communication error with activation server on Ubuntu 12.04
- fixed temporary folder cleanup
- fixed support data collector scripts
- do not download database without the corresponding engine package
- number of engines and maximum file size is now reflect the current status

Version 4.1.0

New features:

- https support for REST API and for Web Management Console
- update history to track every database/engine change
- new option to globally disable or enable specific scan engine
- reworked result page for archive files
- user guide is available within the product
- no scan downtime while updating engine/database (if engine supports)

Issues fixed:

- more descriptive communication error messages instead of error codes in logs
- proper handling of update download issues
- fixed handling of scan engine crashes
- fixed manual update package upload
- fixed unwanted warning message after successful activation

Version 4.0.1

New features:

- new script to help log collection for support

- inform the user if browser is not HTML5 compatible
- show a spinner if loading a page takes too much time
- support lower screen resolution for web interface
- support for non-ascii character filenames in archives

Issues fixed:

- fix stability issue in update downloader
- optimize database queries
- do not check for updates at product startup if auto update is off
- fixed a page auto refresh issue with Internet Explorer

Version 4.0.0

New features:

- Able to to monitor Metascan v4 for Linux instances
- Able to to monitor Metascan v3 for Windows instances
- Collect Files scanned and Infections found stats from managed instances
- Deploy scan engine database updates to Metascan v3 for Windows instances
- Deploy scan engine and scan engine database updates to Metascan v4 for Linux instances

11. Metadefender / Client

About This Guide

Welcome to the MetaDefender Client user guide. This guide is intended to provide the information you need to:

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

While we offer the option to download this guide as a PDF file, it is optimized for online browser viewing. OPSWAT updates the online version of the guide regularly on an "as needed" basis. By viewing the document online, you are assured that you are always seeing the most recent and most comprehensive version of the guide.

Key Features of MetaDefender Client

- File scanning and processing with MetaDefender Core workflows, including:
 - Multi-scanning for malware with more than [30 leading anti-malware engines](#)
 - [Heuristic](#) analysis to detect more unknown and targeted attacks
 - Vulnerability Engine
 - File Type Verification
 - Archive Extraction
- Enumeration and scanning of running processes and loaded libraries
- Blocking of USB & CD/DVD media until they have been scanned by MetaDefender and found clean

Supported Operating Systems

MetaDefender Client is only supported on the following operating systems. Both 32 and 64 bit operating systems are supported.

- Windows 7
 - Requires Service Pack 1 and Microsoft updates KB2533623 and KB3033929

- Windows 8
- Windows 8.1
- Windows 10
- Windows Server Small Business Server standard FE (version: 2011 Standard)
 - Requires KB2533623 installed <http://go.microsoft.com/fwlink/p/?linkid=217865>
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

1. MetaDefender Client Packages

MetaDefender Free Client

MetaDefender Client can be run as a single executable for scanning files on demand without the need for installation.

The following can be scanned by the MetaDefender Free Client:

- Running processes and associated libraries
- Up to 100 local files
- Boot Records
- System Drives

MetaDefender Premium Client

The MetaDefender Client can be installed on endpoints and run in the background, monitoring for any USB storage devices or discs that are inserted into the system. When a USB storage device is detected MetaDefender Client will block access to that device and prompt the user to initiate a scan.

The following can be scanned by the MetaDefender Premium Client:

- Running processes and associated libraries
- Boot Records
- System Drives
- USB
- CD/DVD

For more information see section: [2. MetaDefender Premium Client](#)

2. MetaDefender Premium Client

The MetaDefender Premium Client is a single executable that launches the MetaDefender Client application and allows the following to be scanned.

- Running processes and associated libraries
- Boot Records
- System Drives

In addition, the MetaDefender Premium Client can be installed on endpoints and run in the background, monitoring for any USB storage devices or discs that are inserted into the system. When a device is detected, MetaDefender Premium Client will block access to that device and prompt the user to initiate a scan. The user can select three options for handling the device:

Copy files from drive - Allows users to specify files, which if found clean will be copied to the "MetaDefender" folder on the desktop. If the file is suspicious, it will not be copied.

Unlock drive - Scans the entire drive, if the drive is found clean then it unlocks the drive. Once unlocked, the drive should work as normal, it is fully accessible from Windows Explorer.

Copy files to drive - Allows users to copy files to a drive without scanning it with MetaDefender. This enables users to skip the scanning process if read access to the USB is not required.

2.1 Install using the Install Wizard

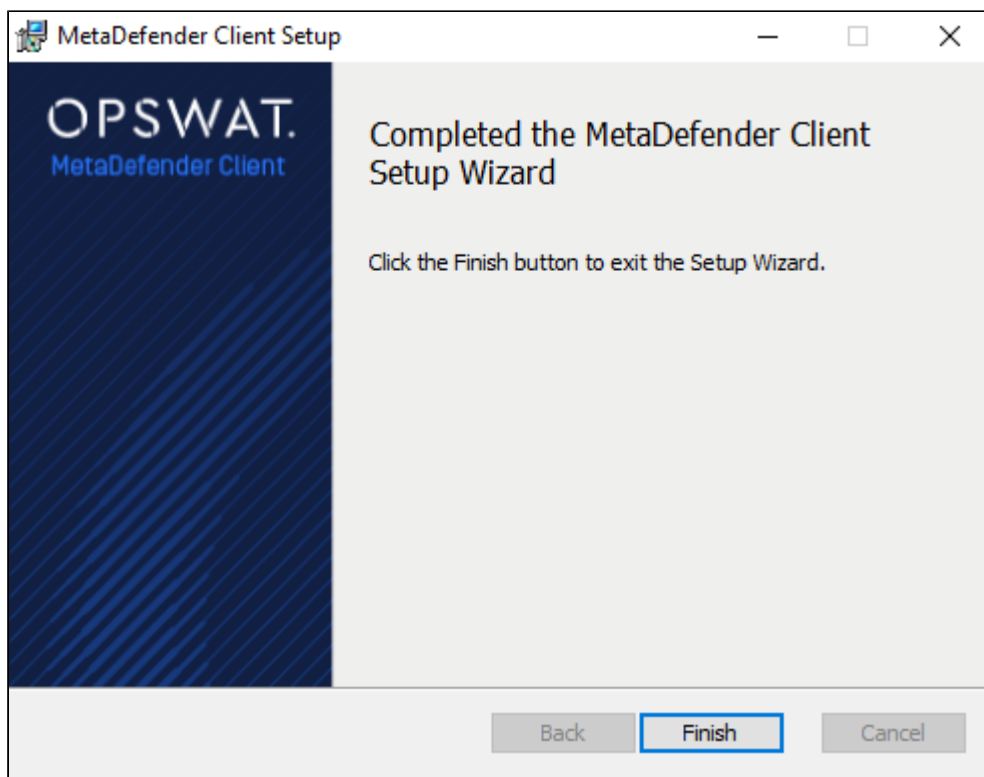
1. Launch the installer by double-clicking on the MSI file



2. Accept the End User License Agreement



3. After the installation has completed, click the 'Finish' button



- Confirm that the MetaDefender Premium Client is running by looking for the icon in the system tray.



2.2 Install using the Command Line

The following command line options are available with the MetaDefender Premium Client installation package.

Command	Description	Example Usage
/i	Install the MetaDefender Premium Client	<code>msiexec /i MetaDefender-Client.msi</code>
/x	Uninstall the MetaDefender Premium Client	<code>msiexec /x MetaDefender-Client.msi</code>
/q	Run the MetaDefender Premium Client installation silently	<code>msiexec /i MetaDefender-Client.msi /q</code>
/L	Create an installation log file	<code>msiexec /i MetaDefender-Client.msi /q /L c:\clientinstall.log</code>
URL=<CM url>	Central Management address	<code>msiexec /i MetaDefender-Client.msi /q URL=127.0.0.1:8018</code>
GROUP=<CM group>	Group from Central Management (optional)	<code>msiexec /i MetaDefender-Client.msi /q URL=127.0.0.1:8018 GROUP=clients</code>

Client Distribution

To distribute & manage Clients among multiple endpoints with Central Management, we recommend using Active Directory to push out the Clients and install using URL and GROUP keys.

2.3 Using the MetaDefender Premium Client

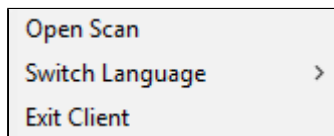
Launching MetaDefender Premium Client

When installed, the Client will run as a persistent service.

Access to the Client is available via the system tray.

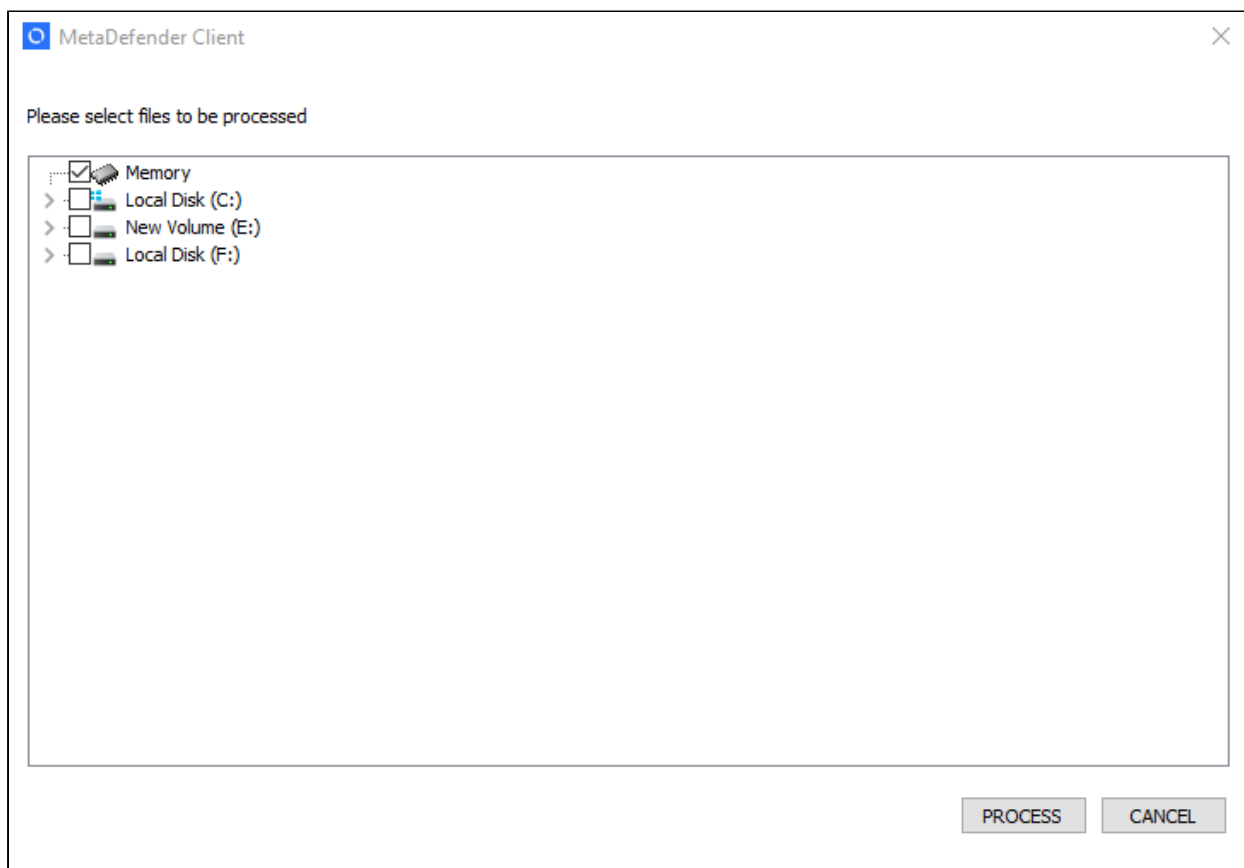
Left-clicking the system tray icon will bring up the Client UI.

Right-clicking the system tray icon provides multiple options:



Open Scan

Opens a browse window to quickly select files from the system to be processed.



Switch Language

Provides the ability to switch the language of the text displayed on the Client UI.

Restarting the "MDCClient" service or exiting the Client will allow for the switch to take effect.

If a desired language is not supported, please contact OPSWAT to request support.

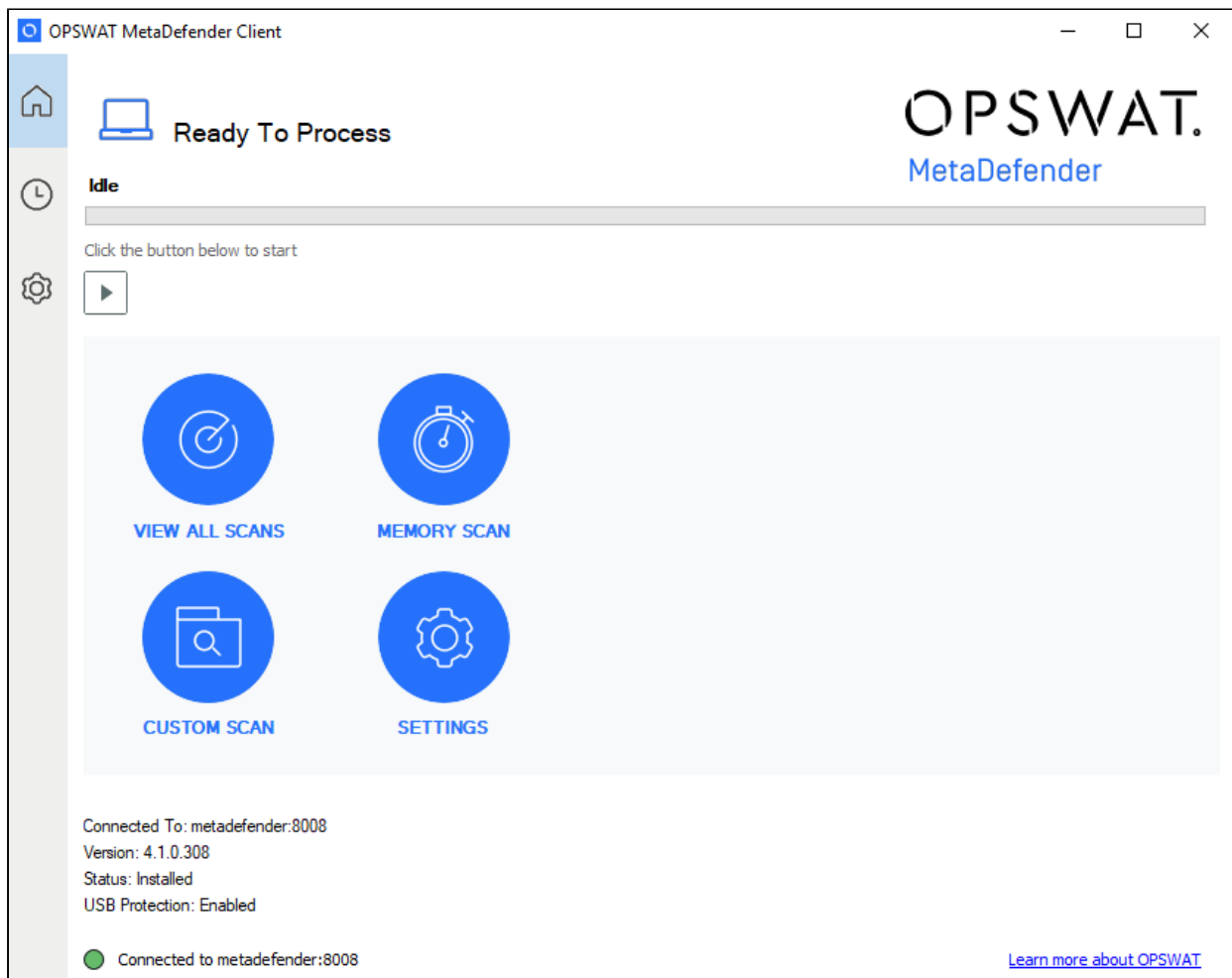
Exit Client

Allows the ability to restart the Client UI.

The following sections give an overview of the end user experience in using the MetaDefender Premium Client UI.

2.3.1 Home Page

The home page provides quick access options and high level information of the Client status.

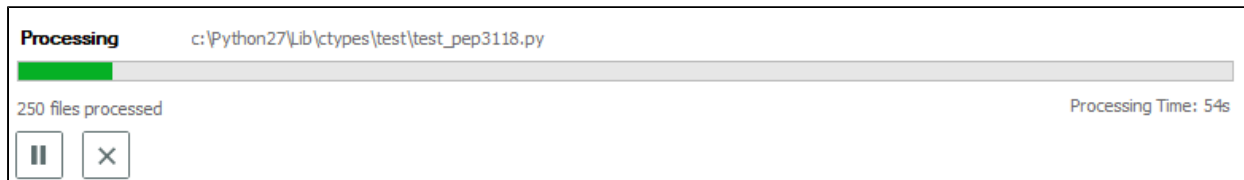


Progress Bar

The top of the home screen shows the progress of a current running task, "Idle" if no task is running.

The play icon allows to start a new task to process selected files from the system.

If a current task is running, it can be paused or canceled.



Left Panel

The left panel allows for quick navigation among sections of the Client UI:

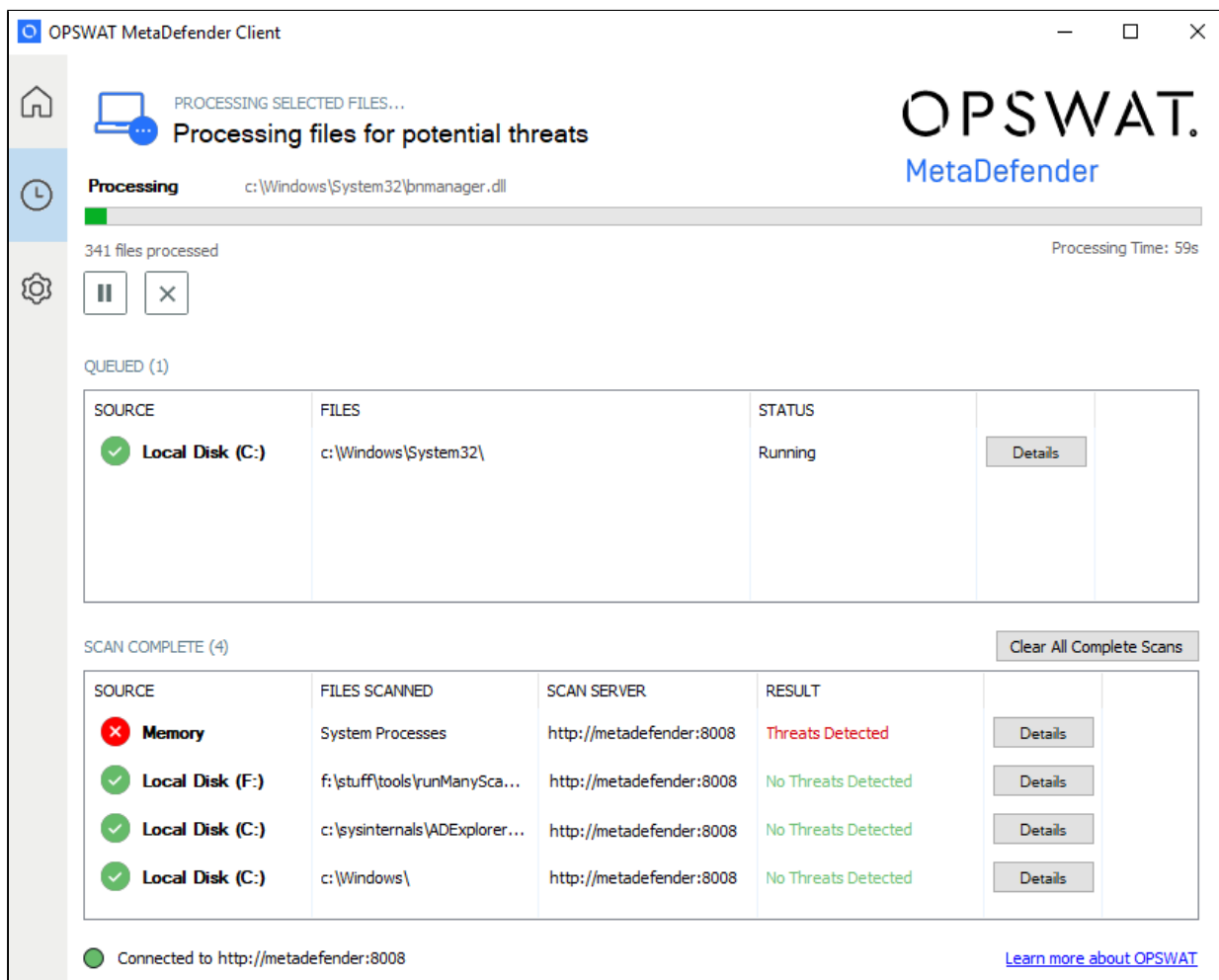
- Home
- Tasks
- Settings

Quick Access Options

- View All Scans - navigates to the Tasks page to view all Queued and Completed scan tasks
- Memory Scan - launches a new scan task for all running system processes
- Custom Scan - launches the browse window to start a new task to process selected files from the system
- Settings - navigates to the Settings page to configure the Client

2.3.2 Tasks Page

The tasks page provides visibility of queued and completed scan tasks with the ability to view the details of a specific task.



Details

The summary of a currently running or completed task or can be viewed by clicking 'Details' for the specific task.

If a Memory scan task was chosen, an App Memory tab will list the current running processes. Each process can be expanded to show the associated loaded libraries and their scan results as well.

OPSWAT MetaDefender Client

PROCESSING SELECTED FILES...
Processing files for potential threats

OPSWAT.
MetaDefender

Processing c:\windows\system32\maxxaudioaposhell64.dll

476 files processed Processing Time: 1m:24s

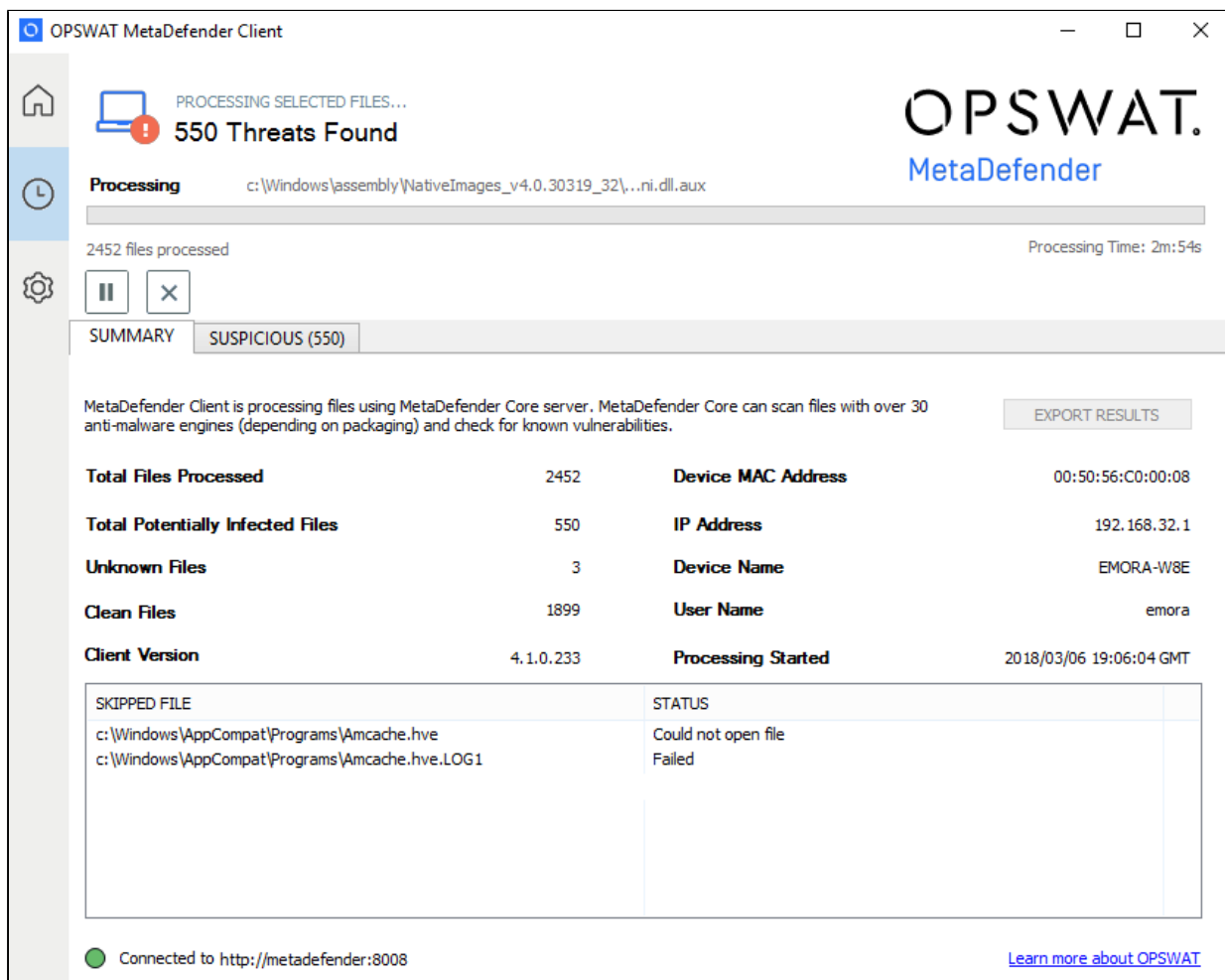
SUMMARY SUSPICIOUS APP MEMORY

NAME	PATH	SCAN RESULTS	SHA256	SCAN TIME
> chrome.exe	c:\program files (x86)\google\chr...	clean	fccf1b67404134894...	2018-03-06T 18:34:...
> mousewithoutbordershelper.e	c:\program files (x86)\microsoft g...	clean	fce27df82f950b424...	2018-03-06T 18:34:...
> onenotem.exe	c:\program files (x86)\microsoft o...	clean	2a6bce65e5dafbc0...	2018-03-06T 18:34:...
> notepad++.exe	c:\program files (x86)\notepad+...	clean	44e3b542da9d6684...	2018-03-06T 18:34:...
> wa_3rd_party_host_32.exe	c:\program files (x86)\opswat\pn...	clean	4fee2e04ebacfe26...	2018-03-06T 18:34:...
▼ egui.exe	c:\program files\eset\eset securit...	clean	62c91cdb22072ac4...	2018-03-06T 18:34:...
ntdll.dll	c:\windows\system32\ntdll.dll	clean	f5fe851a614d0c4c8...	2018-03-06T 18:33:...
kernel32.dll	c:\windows\system32\kernel32.dll	clean	7c76bb7aec3c5116...	2018-03-06T 18:34:...
kernelbase.dll	c:\windows\system32\kernelbase...	clean	e926769d1d2b0b49...	2018-03-06T 18:34:...
user32.dll	c:\windows\system32\user32.dll	clean	6f0ff65c9fb132fbc9...	2018-03-06T 18:34:...
win32u.dll	c:\windows\system32\win32u.dll	clean	89bda3318e23ee3d...	2018-03-06T 18:34:...
gdi32.dll	c:\windows\system32\gdi32.dll	clean	b76f8a431c641589...	2018-03-06T 18:34:...
ndi32f.dll	c:\windows\system32\ndi32f.dll	clean	5f97027117657daf...	2018-03-06T 18:34:...

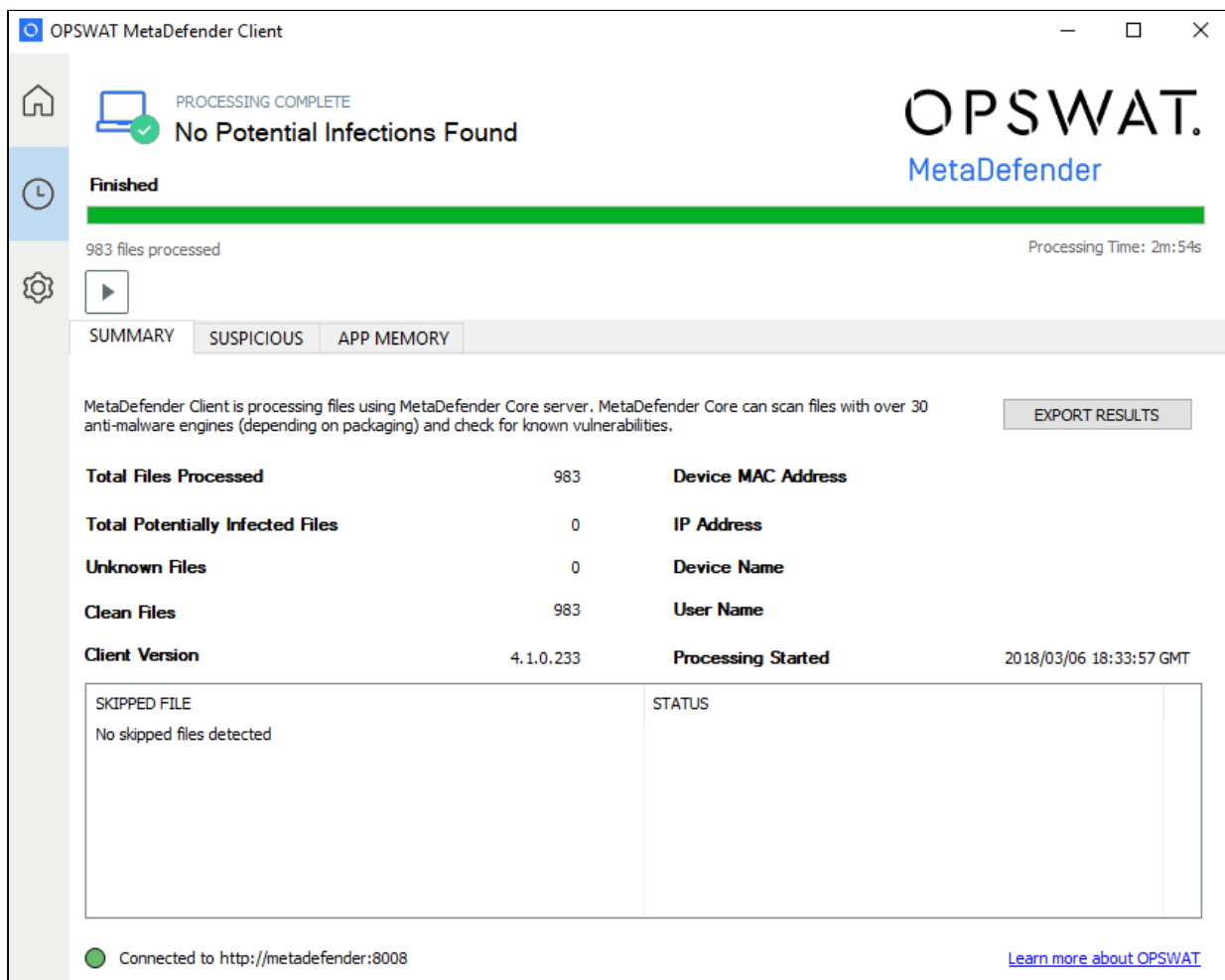
ENGINE	THREAT_NAME	LAST ENGINE UPDATE
● Ahnlab	No Threat Detected	2018-03-06T 18:01:00.000Z
● Avira	No Threat Detected	2018-03-05T00:00:00.000Z
● ClamAV	No Threat Detected	2018-03-06T09:14:00.000Z
● ESET	No Threat Detected	2018-03-06T00:00:00.000Z

● Connected to http://metadefender:8008 [Learn more about OPSWAT](#)

Any issues with files will be listed in the Summary tab within the Skipped File window.



When the scan has finished the overall result will be shown at the top of the Client UI.

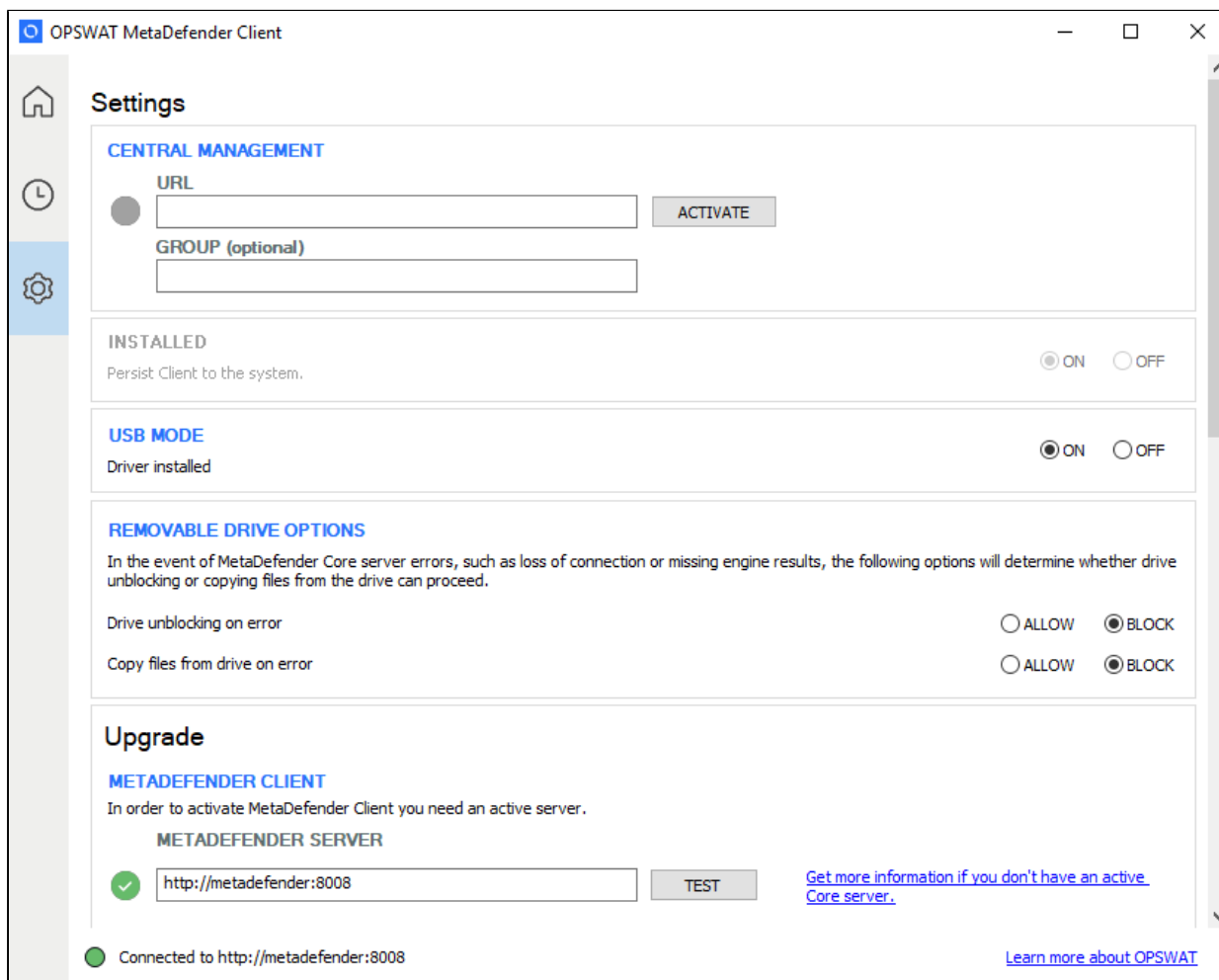


Exporting Scan Report

Scan reports can be saved in either text, PDF, or CSV format by clicking on the 'Export Results' button on the top right of the Summary tab.

2.3.3 Settings Page

The settings page allows the ability to configure the Client.



Settings	Description
Central Management URL	URL of the Central Management
Central Management Group	Specific group in Central Management that the Client should be included in
Installed	Ensures the Client will be installed on the system and running as a service
USB Mode	Enables blocking of inserted USB and CD/DVD devices when Client is installed
Drive unblocking on error	

Settings	Description
	If USB Mode is enabled, this specifies whether Client allows or blocks a drive when a MetaDefender error occurs
Copy files from drive on error	If USB Mode is enabled, this specifies whether Client allows or blocks copying files from a drive when a MetaDefender error occurs
MetaDefender Server	URL of the MetaDefender used to process files
User Agent	The user agent Client provides to MetaDefender for rule/workflow security restrictions
Rule	Specifies the security rule Client should use for MetaDefender v4
Workflow	Specifies the workflow profile Client should use for MetaDefender v3
API Key	API Key used for processing files with MetaDefender v3 (if one is set)
Disable Hash Checking	Disables attempting to check for file's hash result before processing
MetaDefender.com API Key	API Key used for processing files with MetaDefender Cloud
Upload allowed/blocked files to MetaDefender Vault	Enables uploading allowed or blocked files to MetaDefender Vault after processing

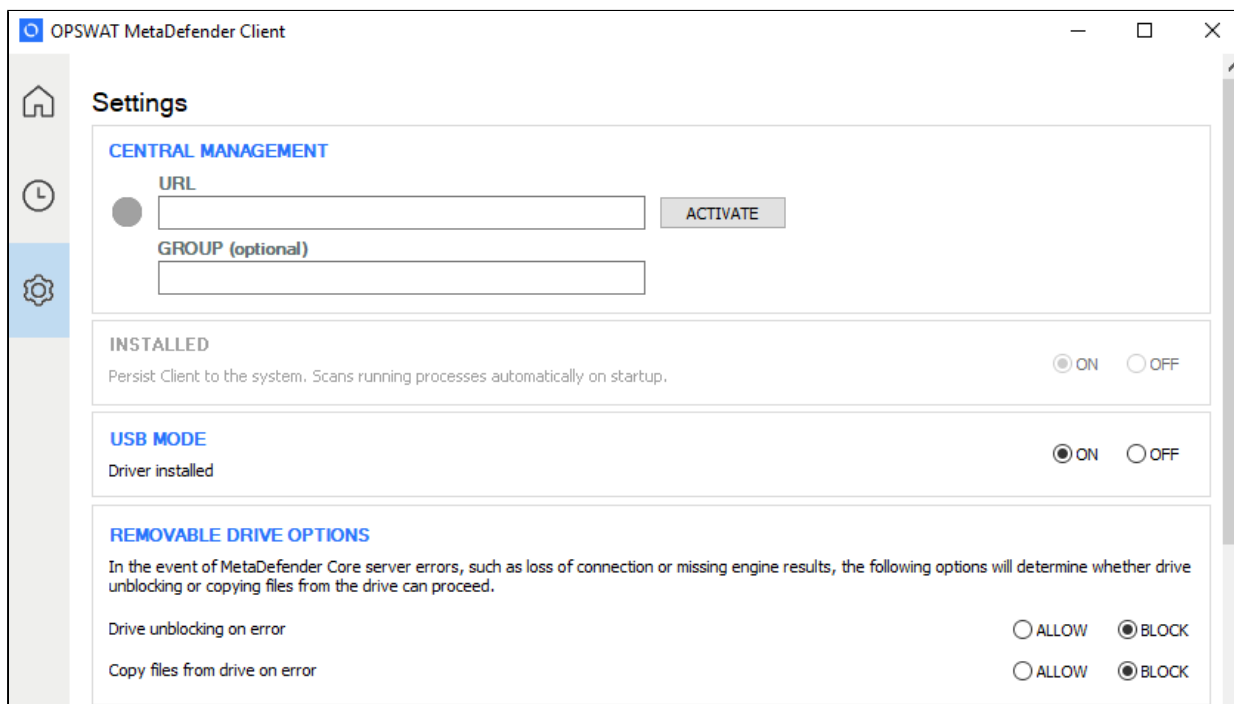
Settings	Description
	Note: files will be uploaded within a zip named with the upload timestamp
MetaDefender Vault URL	URL to the MetaDefender Vault to upload files
MetaDefender Vault Authentication Token	MetaDefender Vault administrator token used to allow files to be uploaded
Always upload to a Vault guest account	<p>If enabled, a guest user id will be generated to retrieve files with</p> <p>If disabled, files will be uploaded as the logged in user</p> <p>Note: if any upload fails, files will be uploaded as a guest user</p>
Use File Sanitization	With data sanitization enabled in MetaDefender, this will provide the option to download available sanitized versions of files
Copy only sanitized file, do not copy original	When copying files to the system, only the available sanitized version will be copied over
Copy from media location	Specifies the location where clean files will be copied

2.3.4 Device Protection

Enable Device Protection

The MetaDefender Client device protection can be enabled by going to Settings → USB Mode → Driver installed → On.

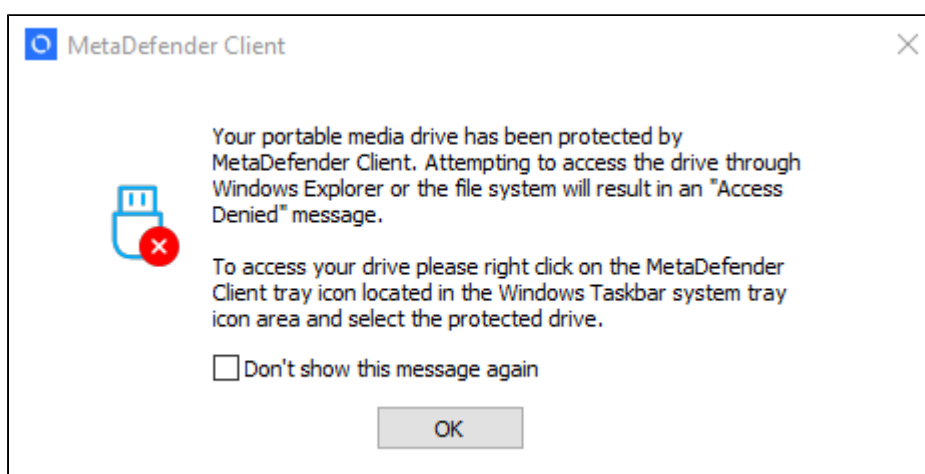
This can only be enabled after the Client is installed.

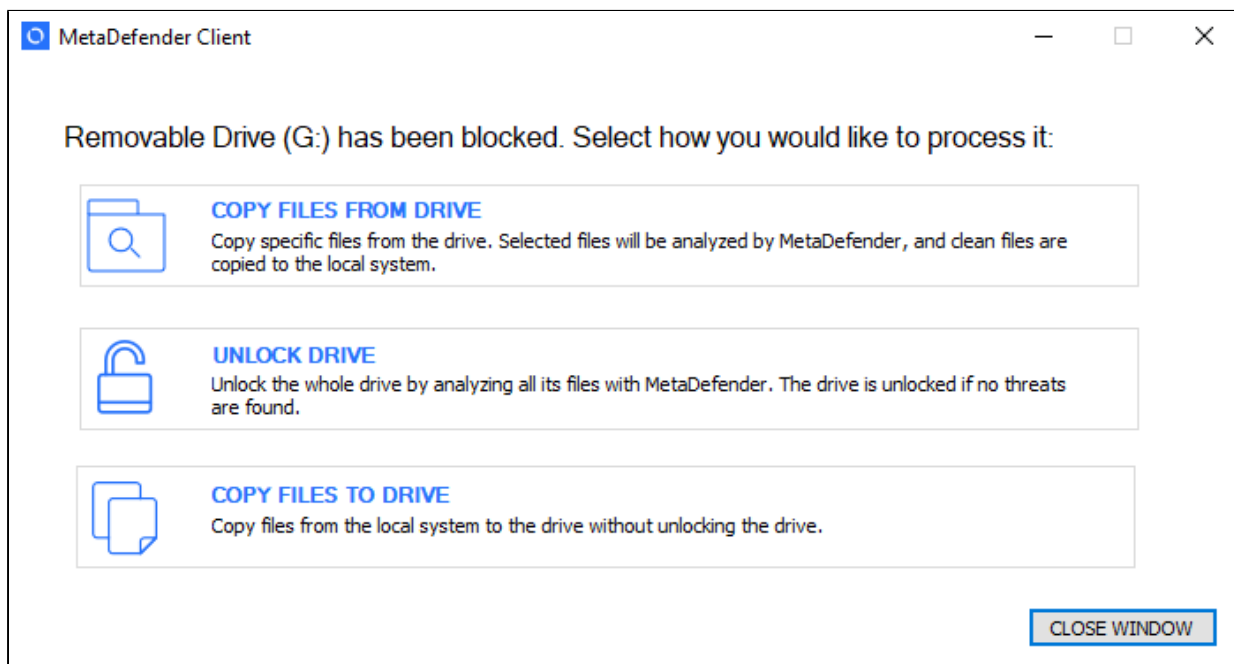


Using Device Protection

Once installed, the MetaDefender Premium Client will run as a Windows service, and will monitor the endpoint for any insertion of USB media or CD/DVD discs. Access to inserted devices will be blocked until they have been scanned by MetaDefender. The only way the device can be used without going through the MetaDefender Client is by uninstalling the MetaDefender Premium Client.

When a USB or disc is inserted, MetaDefender Client will prompt the user to decide how to handle the device.

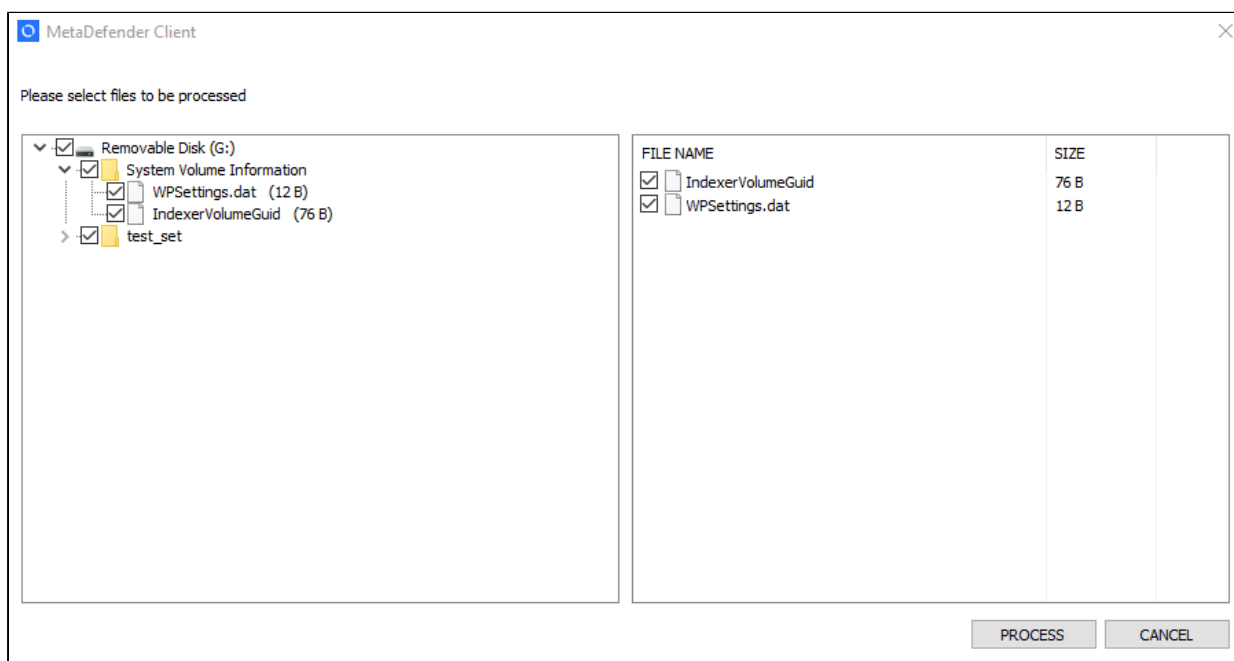




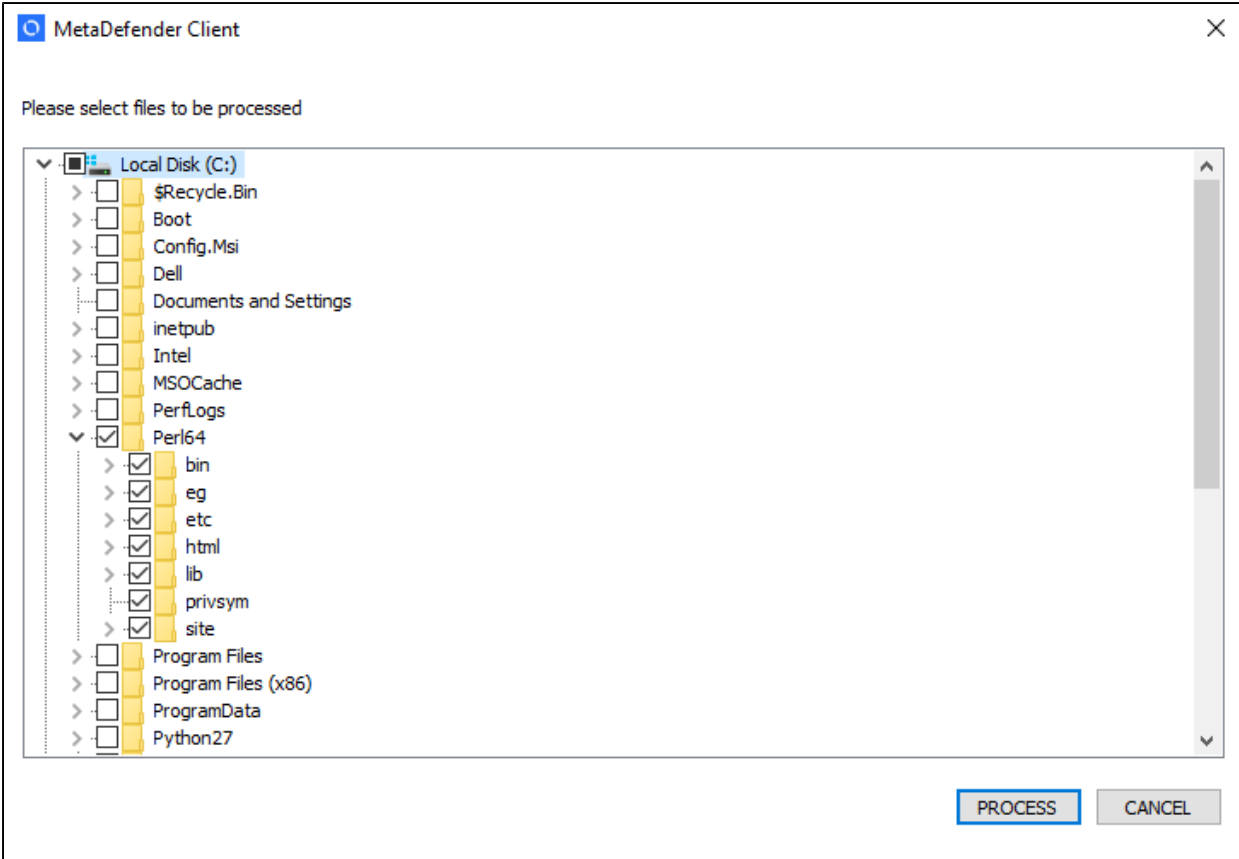
The user can select one of three options

1. Copy files from drive - The user can select which files on the drive they would like to scan
2. Unlock drive - The entire drive will be scanned
3. Copy files to drive - The user can select which files to copy to the USB drive without scanning

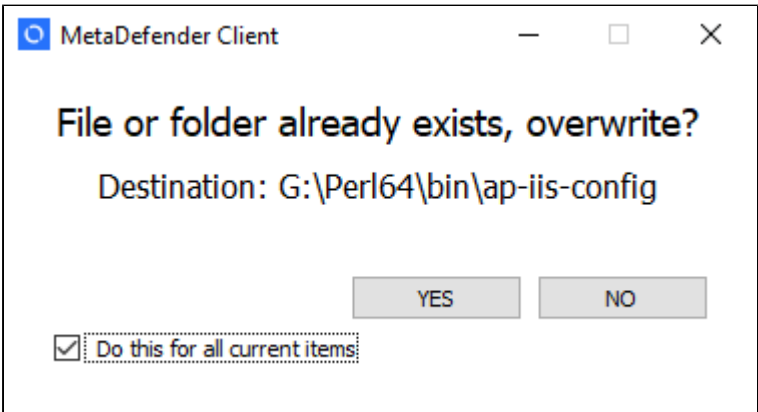
If the user chooses the 'Copy files from drive' option, they will be able to select which files on the media are to be scanned.



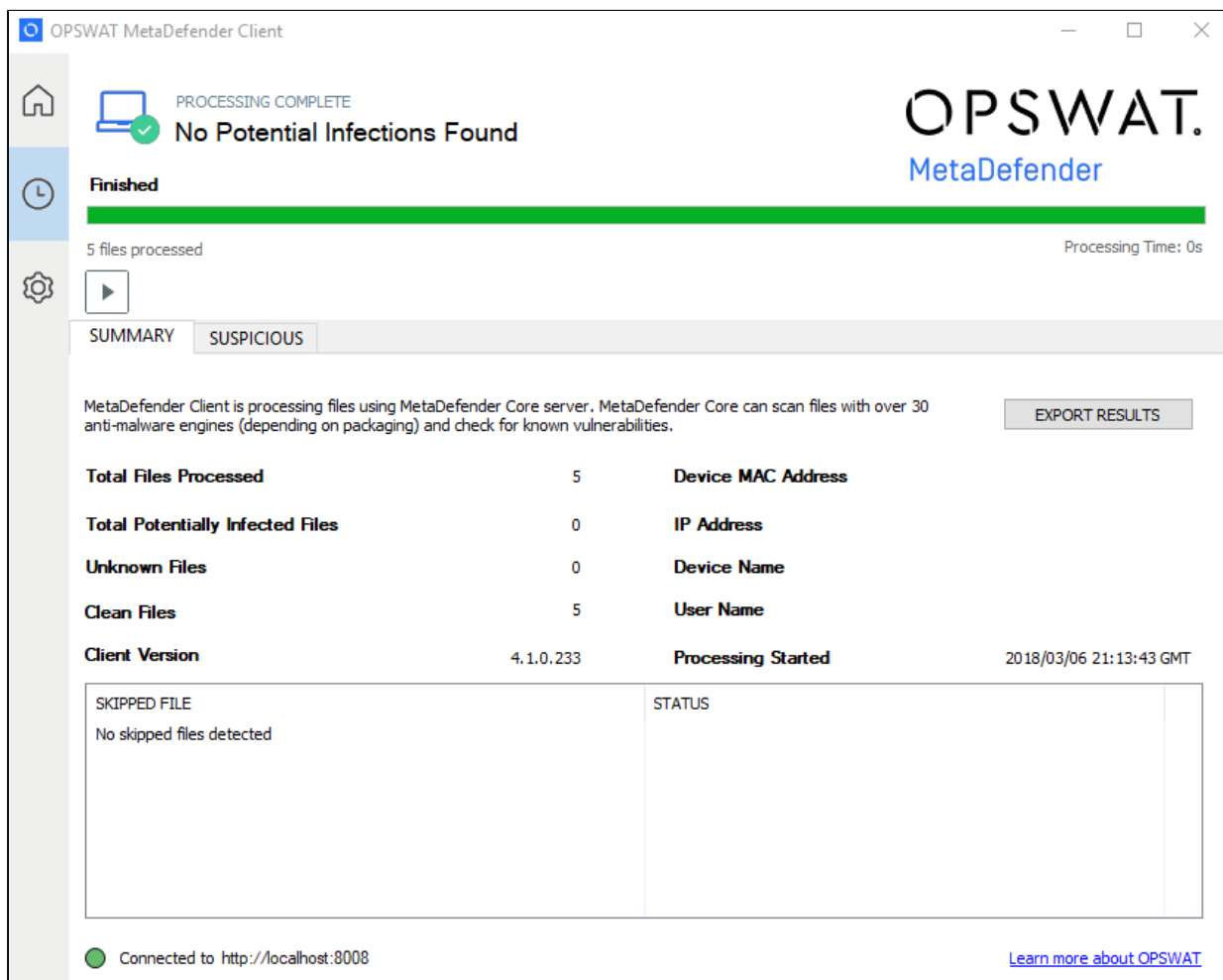
If the user chooses the 'Copy files to drive' option, they will be able to select which files on their system should be copied to the device. If this option is selected, the drive will not be scanned and the user will not have read access to the drive.



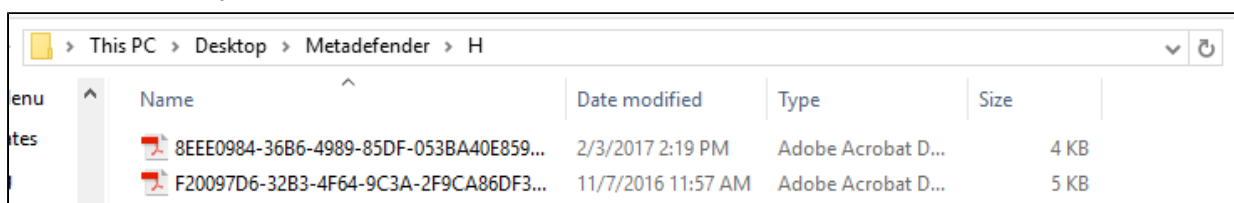
If a file already exists on the USB, the user will be prompted to choose whether or not they want to overwrite the file.



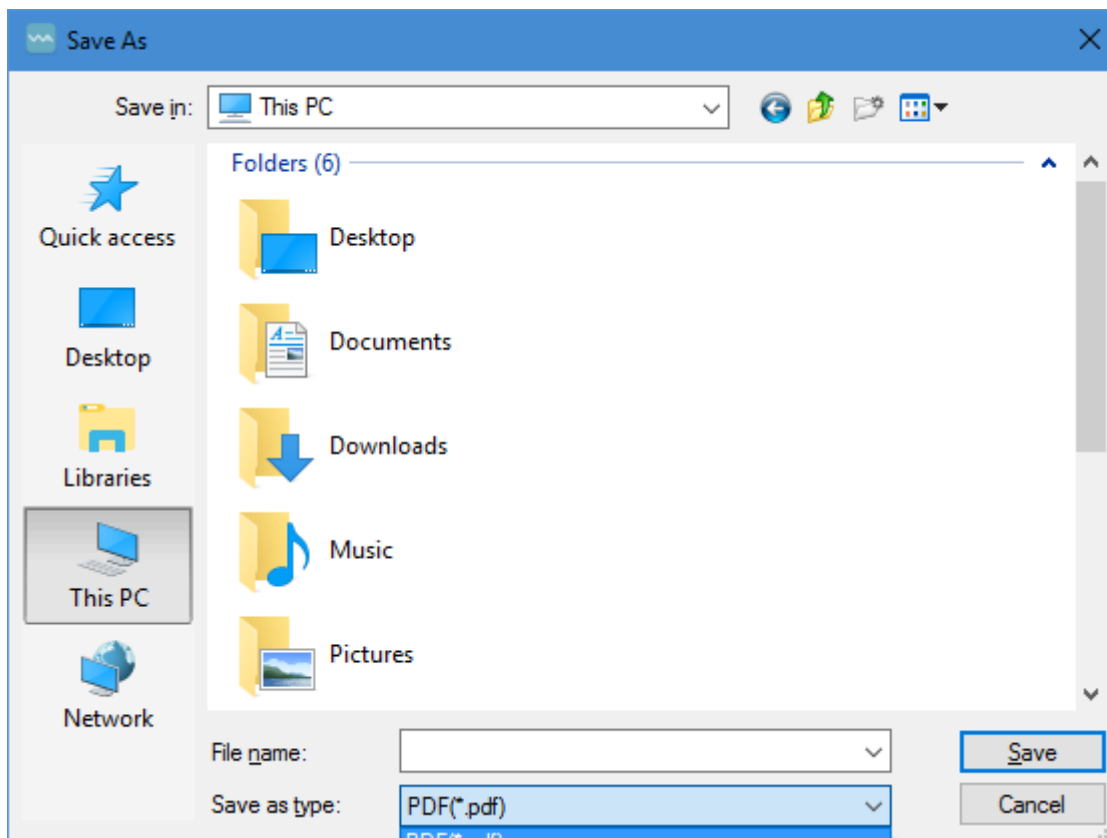
After all of the files have been processed a summary will be displayed to the user. If the 'Unlock drive' option was chosen and no threats were found, the drive will become accessible to the user.



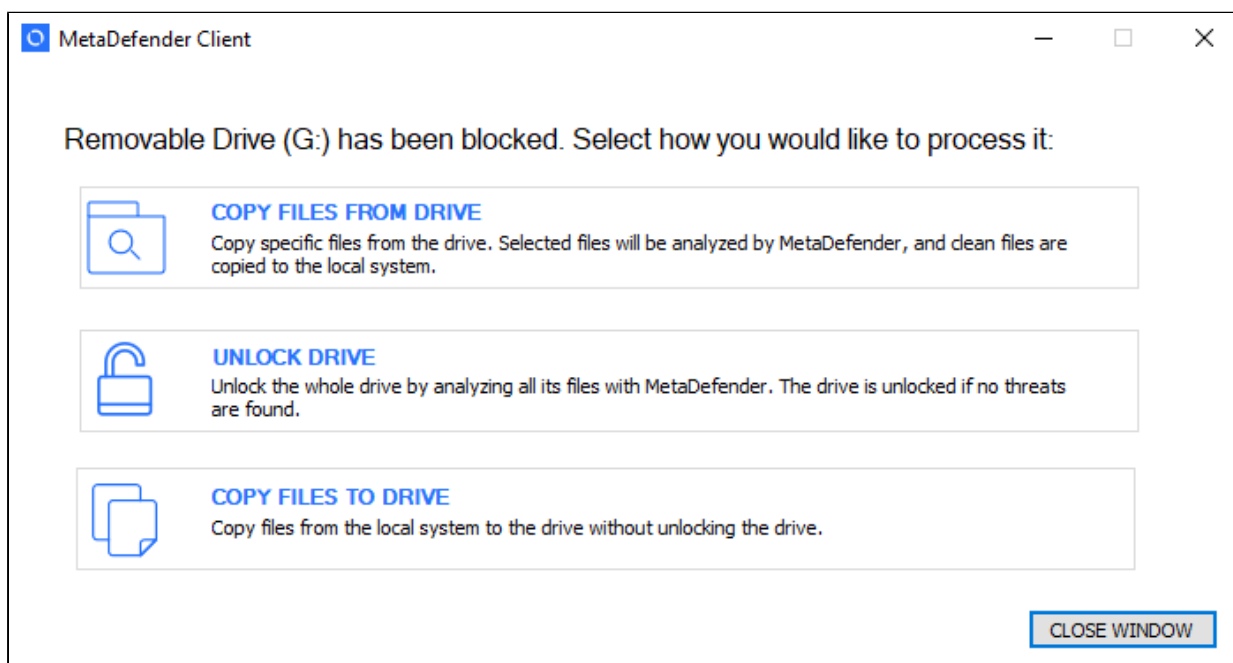
The user can choose to go to the directory of files that were scanned. If they chose the 'Unlock drive' option this will be the drive itself, but if they chose the 'Copy files from drive' option this will be a directory on their desktop where files were copied.



They can also choose to save a report of the scan session in PDF, text, or CSV format.



2.3.5 Media Manifest



To utilize the Media Manifest feature the user should select the "Unlock drive" option. Once the client begins scanning the removable media, it performs the following steps:

1. Looks for an OPSWAT Media Manifest file on the removable media
2. Checks to make sure the Certificate that is signing the Media Manifest is trusted by the client
3. Checks each file on the removable media against the Media Manifest to make sure it has not been modified
 - a. If a file has not been modified and the Media Manifest states it is allowed, then the file is not uploaded for scanning, and is considered clean
 - b. If a file has not been modified and the Media Manifest states it is blocked, then the file is uploaded for scanning
4. Any files found that have been added to the removable media since the generation of the Media Manifest are scanned against the configured server

Note: The client must be provided with the certificates it should consider trusted. The client will look in the following folders to locate all trusted certificates.

1. %ALLUSERSPROFILE%\OPSWAT\.ssh\
2. %USERPROFILE%\\.ssh\
3. %APPDATA%\\.ssh\
4. %APPDATA%\OPSWAT\.ssh\

If the trusted certificate is not in any of the directories above, the client can also verify certificate trust if the root Certificate Authority certificate is installed. OPSWAT recommends automating the deployment and installation of trusted certificates to the client using an AD Push or similar technique. A Certificate Authority certificate can also be installed for an individual client by copying the .crt file over, right clicking on it, and selecting "Install Certificate."

2.4 Configuring through the config file

The MetaDefender Premium Client can be configured by updating the %appdata%\MetaDefenderApp\client_config.json file after MetaDefender Premium Client installation. Changes will be applied the next time the MetaDefender Premium Client is started.

Note: Take care in modifying the client_config.json file. If there are errors in the file, the MetaDefender Premium Client may not start.

Key	Value Type	JSON Key Pair Example	Default Value
servers	JSON array		

Key	Value Type	JSON Key Pair Example	Default Value
		<pre>"servers": [{ "url": "http://<ip or dns>:8008", "apikey": "1234" }]</pre>	<pre>"server": [{ "url": "http://me: 8008", "apikey": "" }]</pre>
user_agent	string	"user_agent":"md_client"	"MDClient"
rule	string	"rule":"client"	" "
workflow	string	"workflow":"client"	" "
disable_hash_check	boolean	"disable_hash_check":false	false

Key	Value Type	JSON Key Pair Example	Default Value
allow_exit	boolean	"allow_exit":true	true
allow_user_selection	boolean	"allow_user_selection":true	false
scan_type	string array	"scan_type":["physical", "process"]	["removable", "
log_file	file path	"log_file": ""	"%AppData% \\MetaDefende

Key	Value Type	JSON Key Pair Example	Default Value
force_usb	boolean	"force_usb":true	false
copy_clean_location	file path	"copy_clean_location":""	"%USERPROF \\Desktop\\Metz
copy_to_maintain_dir_structure	boolean	"copy_to_maintain_dir_structure": false	false
hide_usb_warning	boolean	"hide_usb_warning":false	false
unblock_on_error	boolean	"unblock_on_error":false	false
copy_on_error	boolean	"copy_on_error":false	false

Key	Value Type	JSON Key Pair Example	Default Value
hide_drive_unlock	boolean	"hide_drive_unlock":false	false
hide_drive_browse	boolean	"hide_drive_browse":false	false
hide_drive_copy	boolean	"hide_drive_copy":false	false
max_file_size	integer	"max_file_size":52428800	1000000 MB
media_manifest. trust_only_manifest	boolean	"media_manifest": { "trust_only_manifest":false }	false

Key	Value Type	JSON Key Pair Example	Default Value
media_manifest.days_trusted	integer	"media_manifest": { "days_trusted":30 }	30
pdf_report_dir	string	"pdf_report_dir":"D:\\"	" "
use_file_sanitization	boolean	"use_file_sanitization":true	false
delete_original_sanitized_file	boolean	"delete_original_sanitized_file": true	false

Key	Value Type	JSON Key Pair Example	Default Value
default_language	integer	"default_language":13	9
exclude_engines	string array	"exclude_engines":["engine1", "engine2"]	[]
vault	JSON object	"vault": { "allowed": { "enabled":true, "auth_token":"1234", "copy_to_url":"http://VaultServer: 8000/vault_rest", "guest_only" false }, 	"vault": { "allowed": { "enabled":false "auth_token":"" "copy_to_url":"" "guest_only" fa }, "blocked" {

Key	Value Type	JSON Key Pair Example	Default Value
		<pre>"blocked" { "enabled":false, "auth_token":""," "copy_to_url":""," "guest_only":false } }</pre>	<pre>"enabled":false "auth_token": "" "copy_to_url": "" "guest_only":fa } }</pre>

2.5 Configuring through Central Management

Multiple MetaDefender Clients can be configured from a Central Management. Some changes will take effect at the next restart of Client.

To point MetaDefender Client to Central Management either the Client is installed with the Central Management parameters or the settings are set on the Client settings page. Refer to the Central Management documentation for further details on how to setup managing MetaDefender Clients.

When a Client is centrally managed, the settings will no longer be allowed to be changed on the Client itself, only through Central Management.

The screenshot displays the 'Configuration' page for 'Endpoints'. The left sidebar shows a navigation menu with 'Configuration' selected under 'Settings'. The main content area contains the following configuration fields:

- METADEFENDER LOCAL URL**:
- METADEFENDER LOCAL APIKEY**:
- USER AGENT**:
- RULE**:
- WORKFLOW**:
- METADEFENDER CLOUD API KEY**:
- ALLOW USER TO EXIT**
- ALLOW USER SELECTION**
- SCAN TYPE**: [Add](#)
- MAX FILE SIZE TO SCAN**:

Settings	Description
MetaDefender Local URL	URL of the MetaDefender used to process files
MetaDefender Local API Key	API Key used for processing files with MetaDefender v3 (if one is set)
User Agent	The user agent Client provides to MetaDefender for rule/workflow security restrictions
Rule	

Settings	Description
	Specifies the security rule Client should use for MetaDefender v4
Workflow	Specifies the workflow profile Client should use for MetaDefender v3
MetaDefender Cloud API Key	API Key used for processing files with MetaDefender Cloud
Allow User to Exit	Allow the user to exit through the UI
Allow User Selection	Allow the user to select scan type through the UI
Scan type	The type of scan that is performed if "Allow User Selection" is not checked
Max File Size to Scan	The maximum size of the file to process with MetaDefender (in Bytes)
Disable Checking Hash	Never perform hash lookups, always upload files to MetaDefender for processing
Engines to Exclude from Results	Engine(s) to not be included in the final MetaDefender result output This will modify the final allowed/blocked result of a processed file
Log File Location	Path to store the location for an auto-generated log
Enable Media Drive Protection	All USB/CD/DVD media inserted into the endpoint will be blocked and require processing by MetaDefender before use

Settings	Description
Hide Locked Drive Warning	Disable displaying the warning message of a blocked drive upon insertion
Hide Drive Unlock Option	Disallow a user from unlocking a blocked drive
Hide Drive Browse Option	Disallow a user from copying files from a blocked drive to the system
Hide Drive Copy Option	Disallow a user from copying files from the system to a blocked drive
Drive Unblocking on Error	Drive unblocking can proceed in the event of MetaDefender server errors
Copy Files from Drive on Error	Copying files from the drive can proceed in the event of MetaDefender server errors
Copy Clean File Location	The folder to copy clean files to, from the removable media in Browse File mode
Maintain Directory Structure for Copy	Maintain the directory structure of files on the media in the copy to destination
Use File Sanitization	Check for a sanitized copy of the file generated by MetaDefender
Copy Only Sanitized File, Do Not Copy Original	Dictates if the original file will be removed, or keep it alongside the sanitized copy
UI Display Language	Language the UI will be displayed in

Settings	Description
Upload Allowed/Blocked Files to MetaDefender Vault	Allowed/Blocked files will be uploaded to MetaDefender Vault
URL	URL of the MetaDefender Vault server to upload files to
Authentication Token	Vault admin authentication token used for uploading files
Always Upload to a Vault Guest Account	Uploads will be sent to a newly created guest account
Media Manifest	Client will utilize a Media Manifest existing on the media inserted
Block All Files Not Found on Manifest	Any file not found in the Media Manifest will be immediately blocked and Client will not attempt to process the file with MetaDefender
Days to Trust Manifest	The maximum days to use a Media Manifest result
Client Admin Password Hash	Hashed administrative password. This will be used to uninstall the Client or disable USB blocking. The input to this field MUST be in the format <salt>:<iterations>:<password hash>. Use the "–hash_password" command line option for Metadefender.exe to generate a password hash. See section 4.1 Generating and using the Administrator Password for more information
Allow Disabling of USB Blocking	Allow the user to use the Admin Password to disable USB blocking until next restart

3. MetaDefender Free Client

The MetaDefender Free Client is a free tool that scans files with the engines available in MetaDefender Cloud (metadefender.opswat.com).

The MetaDefender Free Client can be downloaded from the [Free Tools page](#) on OPSWAT.com.

The following functionality is available in the MetaDefender Free Client.

- Running processes and associated libraries
- Up to 100 local files
- Boot Records
- System Drives

4. Command Line Interface

The MetaDefender Client CLI can be run from the command line with the options as described in the table below.

The CLI executable is MetaDefender.exe found at the root of your installation directory.

Example:

```
C:\Program Files (x86)\MetaDefender Client\MetaDefender.exe <option>=<value> ...
```

Command Line Options

A list of available command line options is also available by running the MetaDefender Client executable from the command line without any options

Option	Value Types	Example(s)	Comment
server	<standard url>	-server=http://127.0.0.1:8008/	Specifies URL of the MetaDefender server to
rule	String	-rule=Client	Specifies MetaDefender security rule process f

Option	Value Types	Example(s)	Comment
			Note: Or applicab MetaDef
apikey	String	-apikey=13e5f8h4r3s	Specifies MetaDef apikey Note: Or applicab MetaDef
workflow	String	-workflow=Client	Specifies MetaDef workflow process f Note: Or applicab MetaDef
verbose	n/a	-verbose	Enables logging o
user_agent	<val>	-user_agent=MDClient	Specifies value of user_age will be pr MetaDef
cloud_api_key	String	-cloud_api_key=13e5f8h4r3s	Specifies to use wi MetaDef Cloud
scan_type	A list of one or more of the following strings <ul style="list-style-type: none"> physical 	-scan_type="system process physical removable remote" -scan_type="process physical removable" -scan_type=process	Indicates type of sc MetaDef Client sh

Option	Value Types	Example(s)	Comments
	<ul style="list-style-type: none"> • system • removable • process • remote 		<ul style="list-style-type: none"> • pr all dri (e: re • sy on sy dri • re - a re me • pr on sy pr • re ne dri <p>Note: An invalid parameter will be ignored and a warning will be displayed.</p>
scan_location	"C:\somedir\C:\somefile"	-scan_location="c:\somedir with space\c:\somefile"	<p>Specifies location of files and/or directories scanned.</p> <p>Note: A path is needed for directories.</p>

Option	Value Types	Example(s)	Comment
			Note: Invalid paths will be ignored
exclude_drive	E: F:	-exclude_drive=E: F:	Excludes scan *Only drives supported currently
report_dir	Directory Path	-report_dir="%AppData%\logs\"	Specifies location where scan logs will be saved option is specified file will be generated
report_type	One or more of the following strings <ul style="list-style-type: none"> • pdf • txt • csv 	-report_type=csv	Specifies type of log to write out at end of scan Note: Default is txt if option is unavailable
max_file_size	<val> [GB G MB M KB K]	-max_file_size=512KB	Specifies maximum file size for which MetaDefender Client will scan with MetaDefender

Option	Value Types	Example(s)	Comments
			Note: An greater t max file display "Exceed Size"
hash_password	String	--hash_password 123qwe	Generate password for use in Manager See 4.1 Generati using the Administ Passwor more info

4.1 Generating and using the Administrator Password

The Metadefender Client CLI can also be used to generate the administrator password hash. This password is used to uninstall the Client or allow the user to disable USB blocking until next restart.

To generate the password hash, use the "--hash_password" command followed by your desired password.

Usage:

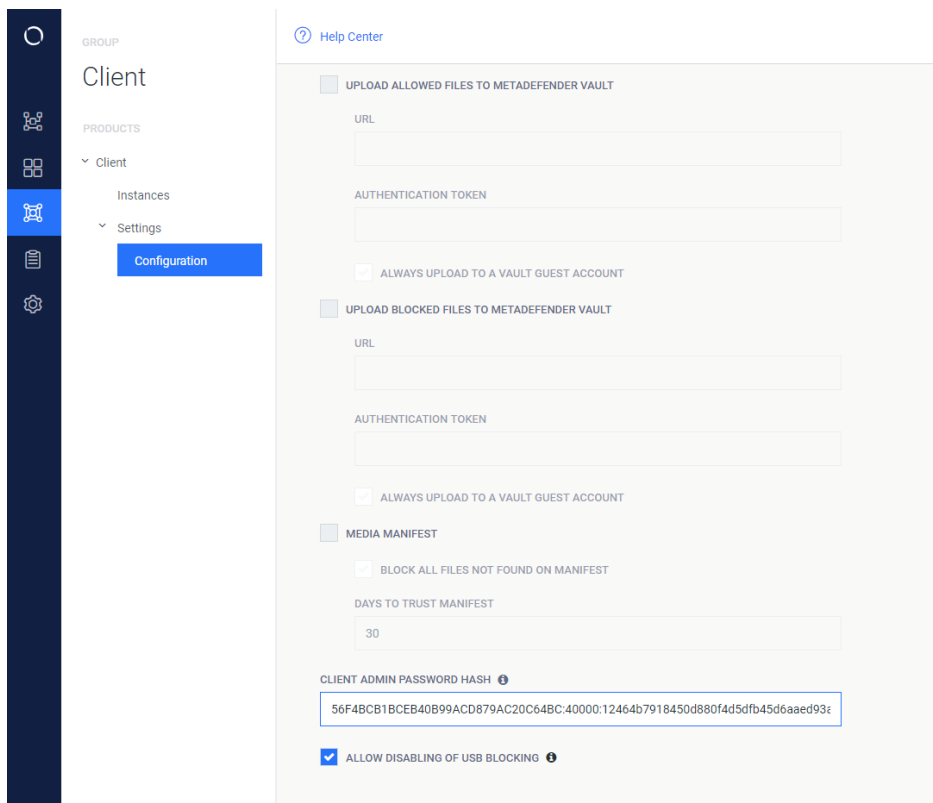
For example, if your desired password is "testpassword", you would use the following command:

```
C:\Program Files (x86)\MetaDefender Client\MetaDefender.exe --hash_password testpassword
```

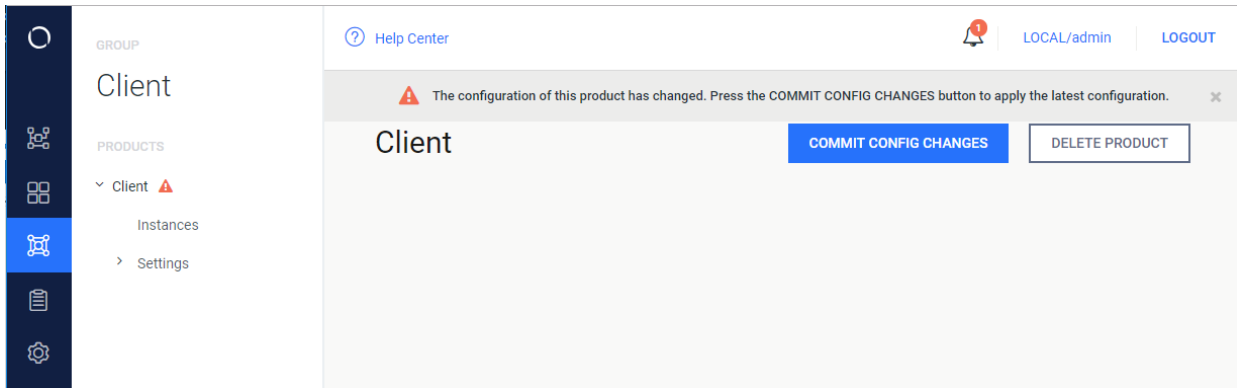
The output will look like the following:

```
Administrator: Command Prompt
c:\Program Files (x86)\OPSWAT\MetaDefender Client>Metadefender.exe --hash_password testpassword
56F4BCB1BCEB40B99ACD879AC20C64BC:40000:12464b7918450d880f4d5dfb45d6aaed93adadf3d191f41b87ddd8861188010a30836de88a4548c2fc2eadb55d8d42
c:\Program Files (x86)\OPSWAT\MetaDefender Client>
```

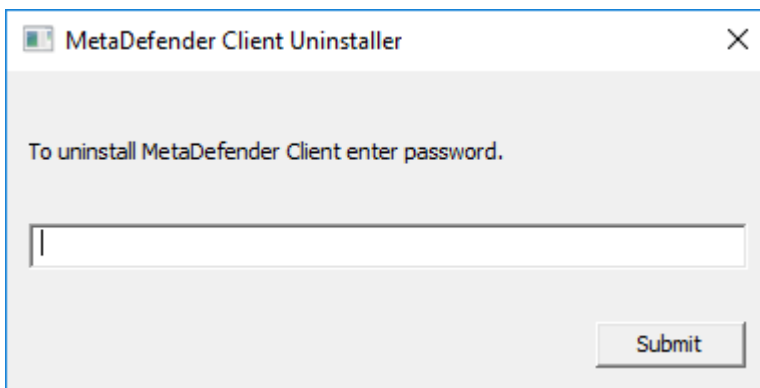
Copy this hashed password to your Central Management settings in the "CLIENT ADMIN PASSWORD HASH" field:



Next, click "SAVE SETTINGS", then open up your Metadefender Client group and click "COMMIT CONFIG CHANGES" to apply this password to all Client instances managed by Central Management.



Now when users attempt to uninstall the Client they will be prompted to enter this password before they are able to uninstall:



5. MetaDefender Client Release Notes

Tips and Known Issues

- If MetaDefender Client is reporting an error in scanning a file, the file should first be scanned through the MetaDefender Core's web interface to determine the cause of the error.

<p>4.1.10 MetaDefender Client release</p> <p>06 November, 2018</p>	<p>MetaDefender Client 4.1.10 is a maintenance release</p>
<p>Distributions included</p>	

- MetaDefender Premium Client

Improvements & Maintenance

Added a new section into scan reports/summary, Potential Vulnerable Files

MetaDefender Client lists potential vulnerable files which have no threats detected under a new section in reports/summary, Potential Vulnerable Files, instead of the Potential Infected Files section.

Fixed

client's IP address was shown as 0.0.0.0 on Central Management

MetaDefender Client only reports connected network adapters

scanning process was hang until a user clicked Details to see the scan's result.

A scan was hang during copying files to destination location or Vault until a user clicks Details to view the scan's result.

Client UI loaded the default language, English, instead of a configured language on Central Management when a user first logs in

An administrator changes client language on Central Management and it's applied to the current user after restarting the client, but the client still loads the default language when a new user first logs in

Allow users to unblocked CD /DVD if scanning

A user has no way to unblock CD/DVD if a scan was failed. MetaDefender Client will now allow to unblock CD/DVD if the setting "Drive unblocking on error" is set to "Allowed"

gets error when the setting "Drive unblocking on error" is set to "Allowed"	
sanitized files were not copied to defined location if enabled	MetaDefender Client didn't copy sanitized files if the setting "Copy only sanitized file, do not copy original" is enabled.

[Previous Releases](#)

5.1. Archived MetaDefender Client Release Notes

Tips and Known Issues

- If MetaDefender Client is reporting an error in scanning a file, the file should first be scanned through the MetaDefender Core's web interface to determine the cause of the error.

4.1.10 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Added a new section into scan reports/summary, Potential Vulnerable Files, to list potentially vulnerable files which have no threat detected.
- Fixed: client's IP address was shown as 0.0.0.0 on Central Management.
- Fixed: scanning process was hang until a user clicked Details to see the scan's result.
- Fixed: Client UI loaded the default language, English, instead of a configured language on Central Management when a user first logs in.
- Fixed: Allow users to unblocked CD/DVD if scanning gets error when the setting "Drive unblocking on error" is set to "Allowed"
- Fixed: sanitized files were not copied to defined location if enabled

4.1.9 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Added a new key into configuration file to define a location to generate a scan report automatically after finishing a scan
- Fixed: a scan report couldn't open in Adobe Acrobat
- Fixed: empty folders don't get copied
- Fixed: missing File Scan Path in the pdf scan report
- Fixed: .csv scan result format file is broken

4.1.8 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Fixed critical bug causing core scans to hang
- Fixed bug where Central Management settings were not populated to all users on a machine
- Fixed MetaDefender Core V3 support
- Corrected minor bug where connection status displayed inaccurate information

4.1.7 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Improvements & Maintenance

- Full visibility to scan network drives
- General bug fixes

4.1.6 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Significant improvement to scan time
- Added File Vulnerability information for executables scanned
- Fixed problem where service would stop with non-admin users
- General bug fixes

4.1.5 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Added [optional uninstall password](#) to further lockdown the system
- Added the ability to temporarily disable the client using the uninstall password
- Added warning to settings page if you move away and haven't saved changes
- Fixed bug that would not allow you to sanitize a file and save the results with the same name
- Added sorting to suspicious file tab
- Better retry logic when server is too busy or unavailable
- Added link to OPSWAT Privacy Policy

4.1.4 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Fixed high priority bug where MetaDefender Client would not onboard or heartbeat with Central Management

4.1.3 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Over all stability fixes
- Fixed crash bug with removable media
- Fixed bug dealing with copying from root of a blocked media
- Refined CLI, added verbose flag
- Enabled MetaDefender Cloud as backup server
- Fixed system resource leak
- Fixed bug where systray would not appear on slower systems

4.1.2 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Fixed Sanitization with Post Actions

- Fixed GDI Leak
- Fixed Play Button behavior when previous scan was against removable media
- Better Hebrew Localization
- Handle File Size of 0
- Fixed CURL Timeout
- Rebooting will lock removable media
- Fixed scanning against MetaDefender V3
- Better CLI support

4.1.1 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- General bug fixes
- Fixed memory leak
- Corrected Data Sanitization behavior with Vault

4.1.0 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- New UI and unified functionality
- Multiple historic scans
- MetaDefender Vault integration

4.0.18 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

Other Changes

- Rebranding
- General bug fixes

4.0.17 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

Other Changes

- Added additional requirement in file to enable data sanitization
- General bug fixes

4.0.16 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- Localization of strings supported (English, Japanese, and Hebrew included by default)

Other Changes

- The 'View Processed Files' button has been removed from the MetaDefender Local Client

4.0.15 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- None

Other Changes

- Option to maintain directory structure when MetaDefender USB Client copies to the local system
- Fixed bug where inserting multiple USB drives and then removing one would exit MetaDefender USB Client for other drives

4.0.14 Release

Distributions included in release

- MetaDefender Cloud Client

New Features

- None

Other Changes

- Update to use new MetaDefender Cloud URL

4.0.13 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- None

Other Changes

- 4.0.12 regression fix

4.0.12 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- MetaDefender USB Client can run under non-admin accounts after being installed with admin privileges

Other Changes

- MetaDefender Client does not need a connection to a MetaDefender Core server to be installed
- Reprocess option to start new scan session on MetaDefender Client without physically ejecting drive

4.0.11 Release

Distributions included in release

- MetaDefender Local Client

- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- Data Sanitization Support
- Files can be deleted from browse dialog

Other Changes

- Additional options for handling contents of media manifest file
- MetaDefender Client will not require access to a MetaDefender Core server if all files are present in the media manifest
- The dialog displayed to the user when a USB is inserted has been updated
- MetaDefender Client can run on systems with lower screen resolutions
- The MetaDefender Cloud Client now excludes results from Filseclab, STOPzilla, ByteHero, and Xvirus

4.0.10 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- Media manifest validation done for Browse option in MetaDefender USB Client

Other Changes

- Drives are not displayed in Windows Explorer until they have been unlocked
- File sizes are displayed in Browse window
- Certificates for Media Manifest validation can be stored in the Windows certificate store
- Minor bug fixes

4.0.9 Release

Distributions included in release

- MetaDefender USB Client

New Features

- Validation of MetaDefender Kiosk media scan manifests

Other Changes

- Minor bug fixes

4.0.8 Release

Distributions included in release

- MetaDefender Cloud Client

New Features

- Application CleanUp Tab

Other Changes

- User interface improvements
- Minor bug fixes

4.0.7 Release

Distributions included in release

- MetaDefender Cloud Client

New Features

- None

Other Changes

- Vulnerability detection improvements

4.0.6 Release

Distributions included in release

- MetaDefender Cloud Client

New Features

- Detection for operating system vulnerability MS17-010, which is the vulnerability exploited by the WannaCry virus

Other Changes

- None

4.0.5 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client

New Features

- Compliance Tab (only applies to MetaDefender Cloud Client)
- Vulnerabilities Tab (only applies to MetaDefender Cloud Client)
- Option to automatically run MetaDefender Client when logging in to Windows

Other Changes

- IP Scan tab has been removed (only applies to MetaDefender Cloud Client)
- The mdproxy.exe included in the MetaDefender Client package is now digitally signed by OPSWAT
- Usability improvements

4.0.4 Release (Internal Only)

4.0.3 Release

Distributions included in release

- MetaDefender Local Client

- MetaDefender USB Client

New Features

- Option to copy files to USB drive without scanning

Other Changes

- Minor UI changes

4.0.2 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender USB Client

New Features

- First Release of MetaDefender USB Client

Other Changes

- Support HTTPS on MetaDefender Core server
- Better handling of non-English file names

4.0.1 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client

New Features

- Release of MetaDefender Cloud Client

Other Changes

- The CLI report_type option 'text' has been changed to 'txt'
- Changed the CLI option -save to -persist_config
- Fixed issue where logging to a long file path caused MetaDefender Client to crash

4.0.0 Release

Distributions included in release

- Metadefender Local Client

New Features

- Support for HTTPS
- Command Line Interface

Other Changes

- Better handling of locked and temp files
- Removed limit on maximum file size to upload against MetaDefender Core V4
- Added CLI generation of CSV and PDF report types
- Better handling of additional scan return types

Changes in 3.12.5

- Better handling of Malformed URLs that are inputted in the MetaDefender Core Server URL dialog
- Resolved an issue where the splash screen did not close under older operating systems (e.g. Windows 7 64bit)
- Removed files from the MetaDefender Client package which caused the package to be detected as encrypted archive
- Improved performance by adding a hash lookup for existing scan results before uploading a file for scanning
- Added support for network mapped drives
- Improved the reporting of processes with infected DLLs in the exported report
- Added support for files that have been whitelisted or blacklisted on the Metadefender Core Server

12. Legal

- [Copyright](#)
- [Export Classification EAR99](#)

Copyright

DISCLAIMER OF WARRANTY

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

COPYRIGHT NOTICE

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

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

Export Classification EAR99

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

OPSWAT's software is designated as EAR99, and there are no export restrictions other than embargoed countries and persons.

13. Knowledge Base Articles

- [Page:External scanners in MetaDefender core v4.8.0 and above](#)
- [Page:Does the fixing updates for Meltdown and Spectre vulnerabilities affect any engines in MetaDefender Core v4?](#)
- [Page:Does MetaDefender Core v4 Detect the NotPetya Ransomware?](#)
- [Page:Are there any dependencies that need to be fulfilled for MetaDefender Core v4 engines ?](#)
- [Page:How can I configure the maximum queue size in MetaDefender Core v4 ?](#)
- [Page:Using MetaDefender core V4 BLACKLIST/WHITELIST feature](#)
- [Page:What are Security Policies and how do I use them?](#)
- [Page:What file types are supported by DLP engine?](#)
- [Page:What file types can be verified by MetaDefender v4?](#)
- [Page:Where can I submit false positives detected by MetaDefender Core v4?](#)
- [Page:What links, target-services or target host-IP's need to be allowed for MetaDefender Core v4?](#)
- [Page:What operating system patches should be applied to the system hosting MetaDefender Core?](#)
- [Page:What should I do if an engine is in "failed" or "permanently_failed" status?](#)
- [Page:Which are the supported archive formats for MetaDefender Core v4?](#)
- [Page:Why don't I see the Data Sanitization engine in MetaDefender Core v4?](#)
- [Page:Why should I upgrade my MetaDefender Core v4?](#)
- [Page:How do I deploy MetaDefender Core v4 to an offline Windows environment?](#)
- [Page:How can the TEMP folder be changed?](#)
- [Page:How can I upgrade from Core v4.7.0/v4.7.1 to a newer Core v4.7 release](#)
- [Page:Does Metadefender Core v4 offer real-time antivirus protection on the system where it is installed?](#)
- [Page:Are MetaDefender Core v4 upgrades free?](#)
- [Page:How can I find a sanitized file scanned with MetaDefender Core v4?](#)
- [Page:How do I remove an engine from my MetaDefender v4 instance?](#)
- [Page:How do I disable real-time protection of my anti-malware software if it is not allowed by corporate policy for use with MetaDefender Core v4?](#)

- [Page:Is there a virus test I could use to test MetaDefender Core v4?](#)
- [Page:How long is the support life cycle for a specific version/release of MetaDefender Core v4?](#)
- [Page:What features of MetaDefender Core version 3 are available in version 4 ?](#)
- [Page:How do I collect verbose debug packages on MetaDefender Core v4 for Linux?](#)
- [Page:How can I increase the scaling up performance?](#)
- [Page:How do I deploy MetaDefender Core v4 to an offline Linux environment?](#)
- [Page:How do I use MetaDefender Core v4 Workflows ?](#)
- [Page:MetaDefender Core v4 shows a large number of files that failed to scan. What can I do?](#)
- [Page:Post actions in MetaDefender core V4.8.0 and above](#)

Are MetaDefender Core v4 upgrades free?

Yes. Your MetaDefender Core license lets you run the latest version of the product during your licensed period. In fact, OPSWAT recommends that you upgrade to the latest release as soon as possible so that you can benefit from new AV engine versions, new features, and bug fixes.

If you are interested in upgrading, please check our Release Notes and our Installation and Upgrade Guide, which can be found [here](#).

If you are a MetaDefender Core Custom customer, OPSWAT recommends that you contact OPSWAT Support and let us guide you through the upgrade process. You can contact OPSWAT Support by [logging a support ticket with us](#).

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-09

CN

Are there any dependencies that need to be fulfilled for MetaDefender Core v4 engines ?

Yes, there are some dependencies for the engines, as described in the table below :

Vir.IT	Microsoft Visual C++ 2010 Redistributable Package Net framework 4
--------	--

ESET	MetaDefender Core v4 temporary directory should have more than 200MB free disk space
Microsoft Security Essentials	Net framework 4.5 Installed on a Windows Server Edition
Symantec	Installed on a Windows Server Edition One NIC with static IP address running TCP/IP
Systweak	Net framework 3.5

Most of the times MetaDefender Core v4 can detect a missing dependency and display it on the Inventory → Nodes → Node details page.

This article applies to MetaDefender Core v4

This article was last updated on 2018-08-22

IB

Does Metadefender Core v4 offer real-time antivirus protection on the system where it is installed?

Although MetaDefender Core uses a number of antivirus engines that are typically found in anti-malware products, it does not offer real-time protection for the system it is installed on.

MetaDefender Core only scans files that are submitted to it on demand. We recommend installing an anti-malware product that provides real time protection on the MetaDefender Core server if such protection is needed.

If a real-time protection agent is installed on the MetaDefender Core server, the MetaDefender Core installation directory and the temporary directory used for scanning need to be excluded from this protection.

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-22

CN

Does MetaDefender Core v4 Detect the NotPetya Ransomware?

A new ransomware attack that was allegedly first detected in Ukraine is spreading across Europe and the world. Does OPSWAT technology currently detect this new attack?

At the heart of the solution, the base MetaDefender Core multi-scanning engine uses up to 20 anti-malware engines to scan files for threats. Our detection rate is dependent on the number of enabled engines, with a higher number of engines increasing malware detection rates.

Currently, most of the engines used in our MetaDefender Core base packages have acknowledged the Petya ransomware threat. Below is a package breakdown with the available information provided from each of the engine vendors.

Please note:

1. Lower packages of MetaDefender Core are a subset of higher packages. For example, MetaDefender Core 4 uses the engine in MetaDefender Core 1 alongside Ahnlab, Avira, and ESET for a total of 4 engines.
2. Some of our vendors may already be detecting this threat but do not have any official post about it. These vendors are not listed below but will be included as more information becomes available.
3. Specific engine detection is based on the most up to date engine definitions. Some latency may occur due to update frequency, update methods, or network speeds.

Windows:

MetaDefender Core 4:

Ahnlab: <https://company.ahnlab.com/company/site/pr/comSecuNews/comSecuNewsView.do?seq=25748>

Avira: <https://blog.avira.com/petya-strikes-back/>

ESET: <https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now-3/>

MetaDefender Core 8:

Bitdefender: <https://labs.bitdefender.com/2017/06/massive-goldeneye-ransomware-campaign-slams-worldwide-users/>

<https://labs.bitdefender.com/2016/04/low-level-petya-ransomware-gets-bitdefender-vaccine/>

Quick Heal: <http://blogs.quickheal.com/petya-ransomware-affecting-users-globally-things-can/>

Total Defense: <https://www.totaldefense.com/security-blog/total-defense-products-detect-the-known-variations-of-the-goldeneye-petya-ransomware>

Zillya!: <https://ru.tsn.ua/ukrayina/v-antivirusnoy-kompanii-rasskazali-kto-mozhet-stoyat-za-hakerskoy-atakoy-petya-a-i-chem-eto-grozit-885812.html>

MetaDefender Core 12:

AVG: <https://support.avg.com/answers?id=906b0000000DrE1AAK>

Ikarus: <https://www.ikarussecurity.com/about-ikarus/security-blog/new-ransomware-petya-hides-in-application-files/>

MetaDefender Core 16:

CYREN: <https://blog.cyren.com/articles/petya-ransomware-spreading-fast-using-same-wannacry-exploit>

Emsisoft: <http://blog.emsisoft.com/2017/06/27/petya-petna-ransomware/>

Kaspersky: <https://blog.kaspersky.com/new-ransomware-epidemics/17314/>

<https://blog.kaspersky.com/petya-ransomware/11715/>

<https://blog.kaspersky.com/petya-decryptor/11819/>

<https://blog.kaspersky.com/tag/petya/>

VirusBlokAda: <https://blog.fortinet.com/2017/06/27/new-ransomware-follows-wannacry-exploits>

MetaDefender Core 20:

McAfee: <https://kc.mcafee.com/corporate/index?page=content&id=KB89540>

<https://securingtomorrow.mcafee.com/mcafee-labs/new-variant-petya-ransomware-spreading-like-wildfire/>

Sophos: <https://nakedsecurity.sophos.com/2017/06/27/breaking-news-what-we-know-about-the-global-ransomware-outbreak/>

<https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Petya-AQ.aspx>

<https://community.sophos.com/kb/en-us/127027>

<https://community.sophos.com/products/b/sophos-community-blog/posts/new-disk-encrypting-ransomware>

VirITeXplorer: http://www.tgsoft.it/italy/news_archivio.asp?id=843

Linux:

MetaDefender Core 5:

Bitdefender: <https://labs.bitdefender.com/2017/06/massive-goldeneye-ransomware-campaign-slams-worldwide-users/>

<https://labs.bitdefender.com/2016/04/low-level-petya-ransomware-gets-bitdefender-vaccine/>

ESET: <https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now-3/>

Total Defense: <https://www.totaldefense.com/security-blog/total-defense-products-detect-the-known-variations-of-the-goldeneye-petya-ransomware>

MetaDefender Core 10:

Avira: <https://blog.avira.com/petya-strikes-back/>

CYREN: <https://blog.cyren.com/articles/petya-ransomware-spreading-fast-using-same-wannacry-exploit>

Ikarus: <https://www.ikarussecurity.com/about-ikarus/security-blog/new-ransomware-petya-hides-in-application-files/>

Quick Heal: <http://blogs.quickheal.com/petya-ransomware-affecting-users-globally-things-can/>

VirusBlokAda: <https://blog.fortinet.com/2017/06/27/new-ransomware-follows-wannacry-exploits>

This article applies to MetaDefender Core v3 and MetaDefender Core v4

This article was last updated on 2018-03-22

CN

Does the fixing updates for Meltdown and Spectre vulnerabilities affect any engines in MetaDefender Core v4?

On January 3, 2018 Microsoft has identified a compatibility issue with a small number of antivirus software products.

The compatibility issue arises when antivirus applications make unsupported calls into Windows kernel memory. These calls may cause stop errors (also known as blue screen errors) that make the device unable to boot.

From the tests we conducted on all Windows operating systems we support, we noticed that the only engine affected by Windows updates is F-secure, on the following operating systems :

1. Windows Server 2012 R2
2. Windows Server 2016
3. Windows 10
4. Windows 8.1

Microsoft has released some patches which fix the issue, and they can be found below :

For Windows Server 2016 and Windows 10: <https://www.catalog.update.microsoft.com/Search.aspx?q=kb4088787>

For Windows server 2012 R2 and Windows 8.1: <https://www.catalog.update.microsoft.com/Search.aspx?q=KB4088879>

References:

- <https://support.microsoft.com/en-ca/help/4088787/windows-10-update-kb4088787>
- <https://support.microsoft.com/en-us/help/4088879/windows-81-update-kb4088879>

*This article applies to MetaDefender Core v4
This article was last updated on 2018-06-21*

CN

External scanners in MetaDefender core v4.8.0 and above

Disclaimer

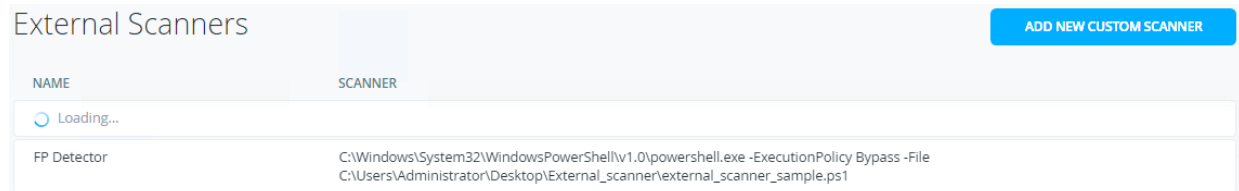
This sample script is provided for illustrative purpose only and is not guaranteed to be functional in a production environment.

MetaDefender Core V4.8.0 has a new feature "External scanners".

You can define an "External scanner" which can be invoked through a command line executable or script. This executable/script will be called for each scanned file, after all other engines but before final verdict is decided.

The documentation of this feature can be found here: https://onlinehelp.opswat.com/corev4/3.10._External_Scanners_And_Post_Actions.html

The script in this sample is a Powershell script, for this script to work properly, we need to call the Powershell executable in the External Scanners screen of MetaDefender Core:



NAME	SCANNER
FP Detector	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Users\Administrator\Desktop\External_scanner\external_scanner_sample.ps1

You will need to specify the location from where Powershell is running in your system, followed by:

- ExecutionPolicy Bypass
- -File TheNameAndPathOfYourScriptFile.ps1

We created a sample Powershell script that attempts to flag files suspicious as False Positive.

The script checks the scan results of the current file, if the file is flagged as infected by only one engine, the file's hash is then sent to MetaDefender cloud.

MetaDefender cloud's results are then analysed :

In case the file is flagged as infected in MetaDefender Cloud by ONLY the same one engine which flagged the file in MetaDefender Core

OR if the file is found to be clean by MetaDefender Cloud, the file will be copied to a

`$false_positive` folder for later investigation,

and verdict will be "Suspicious" (2). and `threat_found` will be 'Suspected False Positive'.

If the file is flagged by any other engine on MetaDefender Cloud then the verdict will be

"Infected" (1) and `threat_found` will be "Infected - Probably NOT False Positive ".

If the file is not flagged by any local engine the script returns the verdict " No Threat Detected" (0).

It accepts as its input:

1. It is your responsibility to create and populate the system context variable `%false_positive%` with a valid folder name before running the script
2. It is your responsibility to create and populate the system context variable `%apikey%` with your valid MetaDefender cloud license key.
3. The script accepts the currently scanned file location as its last command line argument, and stores it in the variable `$current_file_path`
4. The script expects to find the scan results json on STDIN. it is read into the variable `$scan_results`

output:

1. The script will add its verdict (based on results from MetaDefender Cloud) to the result JSON and write it to the STDOUT
2. if only the same engine (or no engine at all) flag the file as malicious the script will copy the file to the folder `$false_positive` for later investigation
3. The script has 6 possible return values:
 - "0" - Success
 - "1" - Input Json Parse error
 - "2" - Copy error
 - "3" - file path of currently scanned file is invalid
 - "4" - the destination path of "false positive" is invalid.
 - "5" - call to MetaDefender hash lookup failed
 - "6" - hash not found on MetaDefender Cloud

The script itself can be found and downloaded from the following link:

external_scanner_sample.ps1

This article applies to MetaDefender Core v4 Windows

This article was last updated on 2018-03-22

CN

How can I configure the maximum queue size in MetaDefender Core v4 ?

The maximum queue size can be configured in MetaDefender Core v4 via REST API, as follows :

Set scan config {#rest_setscanconfig}

Request	Value
Method	PUT
URL	/admin/config/scan

Request HTTP header parameters:

Name	Type	Required	Value
apikey	string	true	Session id, can be acquired by Login / Create a Session

Request body:

JSON path	Type	Required	Value
max_queue_per_agent	int	true	Max queue size allowed per agent

Example:



An example of a successful response can be found below :

HTTP status code: **200**

Response contains information about the modified scan configuration



In case the configuration change was not correct, an error response like the one below will be returned :

Internal error

HTTP status code: **500**



This article applies to MetaDefender Core v4

This article was last updated on 2018-03-22

CN

How can I find a sanitized file scanned with MetaDefender Core v4?

Once a file is scanned by MetaDefender Core and then sanitized, it can be downloaded from the following link:

```
http://<MetaDefender>:8008/file/converted/<dataid>?apikey=<apikeyset>
```

- <MetaDefender> needs to be set to your MetaDefender I.P. location or name
- <dataid> needs to be inserted as per data id of the file
- <apikey> Only required if REST API keys have been defined

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-22

CN

How can I increase the scaling up performance?

The only reason to increase the scaling up performance is when you have 32-48 CPU cores and you wish for your file to be processed very fast . In order to increase the scaling up performance, there are 2 approaches as follows:

Approach A

If you have a Scan Node (formerly known as Agent) connected to Core and the queue is full of incoming scan requests, they will be denied until there is a free slot.

To change the queue size, you can use the following API call:

PUT on `http://<serveraddress>:8008/admin/config/scan`

With the following body:

```
{  
    "max_queue_per_agent": 500  
}
```

Note that to use this API you need an apikey,

apikey can be obtained from the management console->Settings->User Management->Admin user

use the apikey in the apikey header.

This works for both Linux and Windows.

Approach B

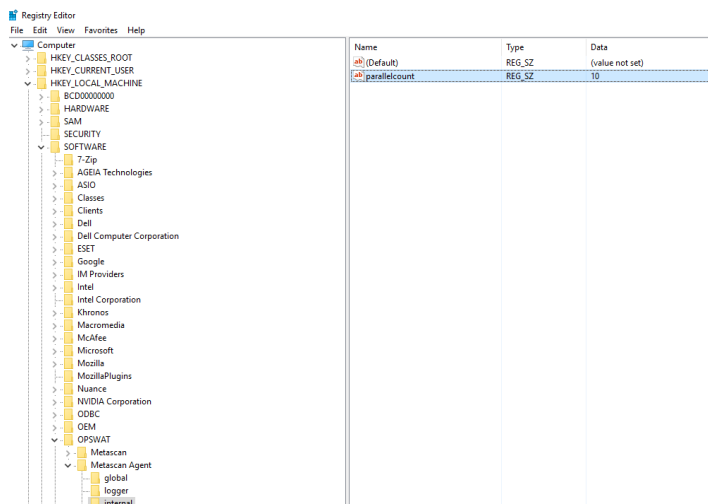
Other way to better utilize your CPU, if you have 16-32+ cores, is to increase the parallel number of scans running per engine. This way you can tell the Node how many scans should run simultaneously per engine. This applies to engines supporting multi-threaded scan.

To change this you have to write in the node's config in the registry:

HKLM/Software/OPSWAT/Metascan Node/internal/parallelcount (or **HKLM/Software/OPSWAT/Metascan Agent/internal/parallelcount** in case of versions <= 4.5.1)

If internal key is not present just create it and then create the new config value. The default value is 20.

Example:



After you modified the value, please note that you have to restart the MetaDefender Core services for the changes to take effect. To restart the services, please open an elevated command prompt and type the following commands:

- net stop ometascan
- net stop ometascan-node
- net start ometascan
- net start ometascan-node

(use service name ometascan-agent instead of ometascan-node for versions <= 4.5.1)

On Linux you have to modify Node's startup configuration (add internal/parallelcount) file and restart the service.

```
[logger]
...

[global]
...

[internal]
parallelcount=20
```

This article applies to MetaDefender Core v4 Windows and Linux

This article was last updated on 2018-03-22

CN

How can I upgrade from Core v4.7.0/v4.7.1 to a newer Core v4.7 release

MetaDefender Core v4.7.0 and v4.7.1 releases contains an issue which can cause configuration data loss during upgrade.

To upgrade from v4.7.0/v4.7.1, please do the following

1. Stop the Core services using the following commands

```
net stop ometascan  
net stop ometascan-node
```

2. Check the data folder under MetaDefender Core installation folder (<INSTALLATION DIRECTORY>\data, usually C:\Program Files\OPSWAT\MetaDefender Core\data). If there is any *.war or *.shm files that exists in this folder, this means that the services are still running. Please be sure to stop the services correctly (no running ometascan.exe and ometascan-node.exe processes are running)
3. **Copy** the content of your <INSTALLATION DIRECTORY>\data folder from the installation folder to a safe place
4. Uninstall MetaDefender Core v4.7.0/v4.7.1
5. Remove content of <INSTALLATION DIRECTORY>\data folder
6. Install the latest version of the MetaDefender Core
7. Stop the Core services again using the following commands

```
net stop ometascan  
net stop ometascan-node
```

8. **Replace** the data folder with the files from **Step 3** to <INSTALLATION DIRECTORY>\data (keeping your data backup untouched)
9. Run the following command: <INSTALLATION DIRECTORY>\ometascan-upgrade-db.exe
10. Restart the Core services using the following commands

```
net start ometascan  
net start ometascan-node
```

11. Login to the web management interface and check if your configuration and scan history is untouched



if you need further help to upgrade from these version contact OPSWAT's support for assistance

This article pertains to MetaDefender Core v4

This article was last updated on 2018-03-23

CN

How can the TEMP folder be changed?

The "**temp** folder", or the "**resources** folder" is where the scanned files are getting written down for the Nodes (Agents) to scan.

The temporary folder is used to store the following files:

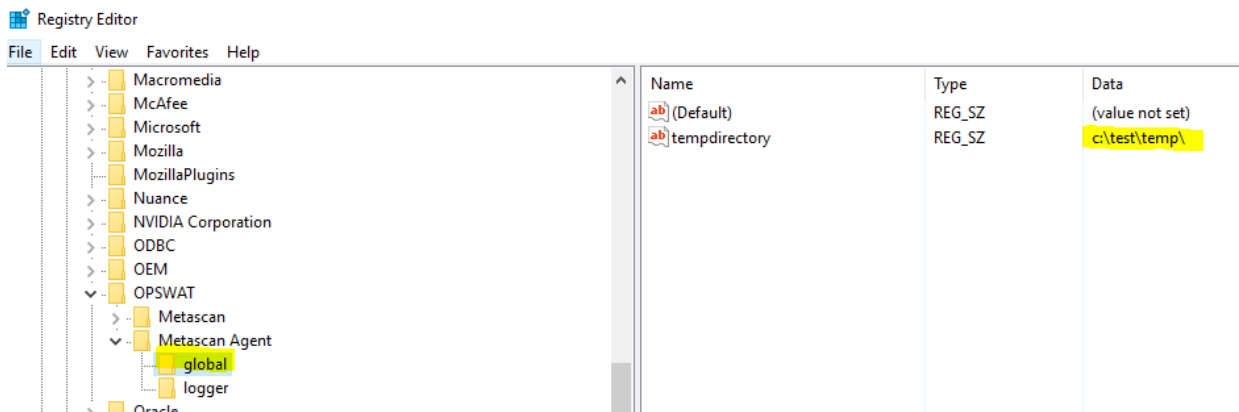
- *EICAR Standard Anti-Virus Test File* for engine testing (see <http://www.eicar.org/86-0-Intended-use.html>)
- all the uploaded files to scan/process
- all the extracted files during archive handling while scanning/processing a file
- file generated with sanitization before sent back to Core
- all the update package files sent by Core before processing them (engine and database updates)

It can be changed by configuring a new registry key as follows in v4.6 or higher:

1. Under HKLM/Software/OPSWAT/Metascan Node/ create a new key named "global",
2. Under HKLM/Software/OPSWAT/Metascan Node/global/ create a new string value with name "tempdirectory" and insert in the value data the desired path (ex c:\temp),
3. Restart Metascan Node service,

It can be changed by configuring a new registry key as follows in versions before v4.6:

1. Under HKLM/Software/OPSWAT/Metascan Agent/ create a new key named "global",
2. Under HKLM/Software/OPSWAT/Metascan Agent/global/ create a new string value with name "tempdirectory" and insert in the value data the desired path (ex c:\temp),
3. Restart Metascan Agent service,



This article applies to MetaDefender Core v4

This article was last updated on 2018-03-23

CN

How do I collect verbose debug packages on MetaDefender Core v4 for Linux?

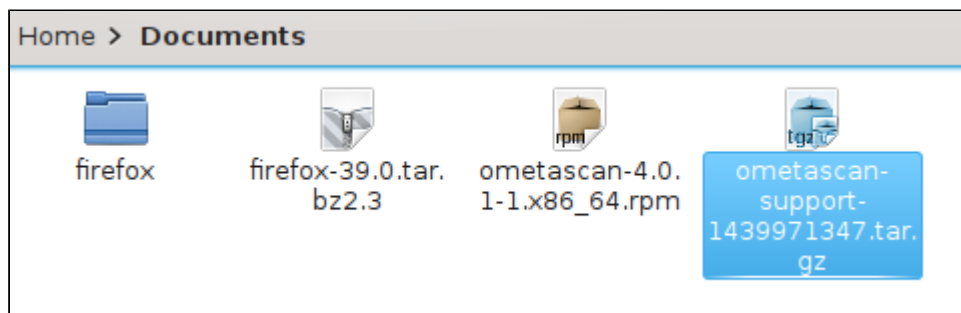
In order to collect verbose debug packages on MetaDefender Core v4 for Linux, please follow the instructions below:

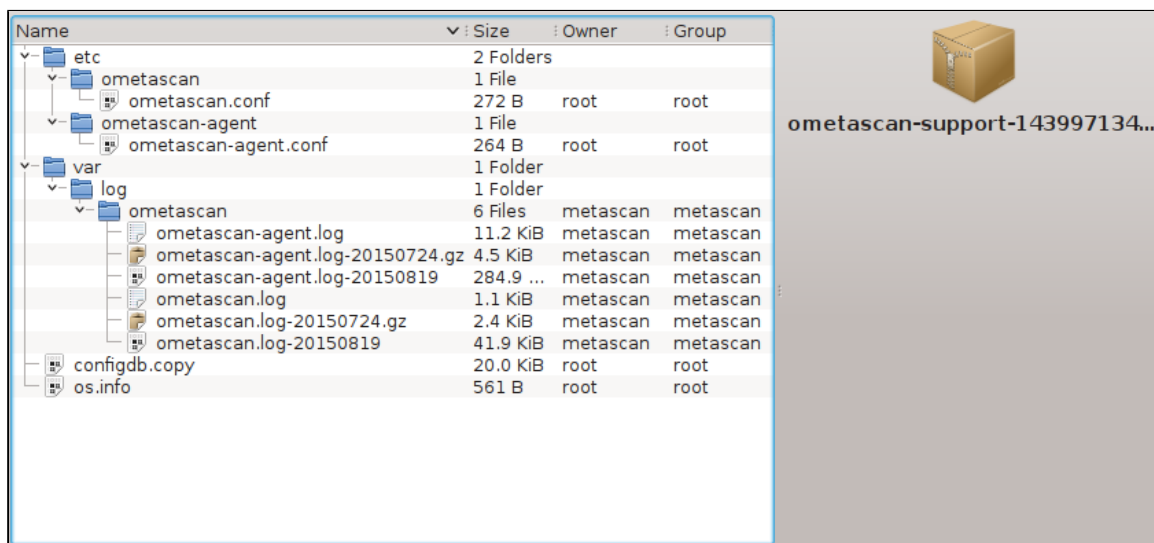
1. Run `/usr/bin/ometascan-collect-support-data.sh` script under root privileges (e.g., `sudo sh /usr/bin/ometascan-collect-support-data.sh`):

```
[root@localhost Documents]# sudo sh /usr/bin/ometascan-collect-support-data.sh
/usr/bin/ometascan-collect-support-data.sh: line 5: lsb_release: command not found
/usr/bin/ometascan-collect-support-data.sh: line 7: lsb_release: command not found
tar: Removing leading `/' from member names
Support file created: ometascan-support-1439971347.tar.gz
```

2. A file is created by the script in the actual directory you are currently on (e.g., "Support file created: ometascan-support-1438969411.tar.gz").

Note: The timestamp in the filename changes every run.





This article applies to MetaDefender Core v4 Linux

This article was last updated on 2018-03-26

CN

How do I deploy MetaDefender Core v4 to an offline Linux environment?

MetaDefender Core v4 supports deployment in either online or offline environments.

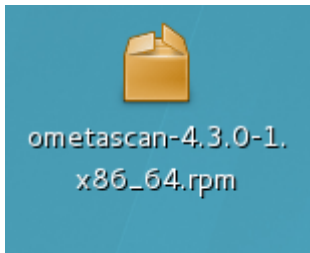
There are four steps to getting the product up and running in an offline environment:

1. Install MetaDefender Core on the offline server.
2. Activate your license.
3. Install and configure the MetaDefender Update Downloader utility.
4. Apply the offline updates that are downloaded by the update utility to the offline MetaDefender Core server.

Installing MetaDefender Core

The MetaDefender Core installation packages can be downloaded from the [OPSWAT Portal](#). After logging into the portal, go to the Downloads page where you can select the MetaDefender Core package you wish to download. The supported platforms include Red Hat Enterprise, CentOS, Debian, and Ubuntu.

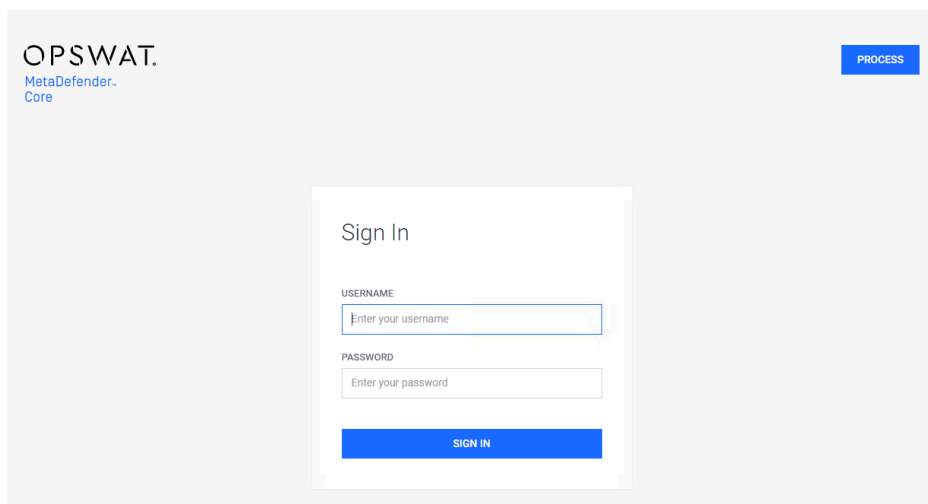
Download the appropriate installer for your distribution:



Activate your license

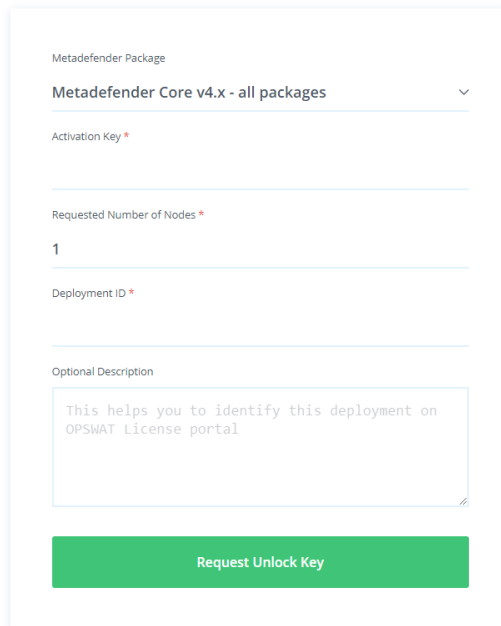
After MetaDefender Core is installed, you will need to activate your MetaDefender Core installation.

1. Log into your MetaDefender Core Management Console at <http://localhost:8008/>. The default user ID and password for a new installation are admin/admin.



2. Go to **Settings > License**.
3. Log into the OPSWAT Portal and navigate to the MetaDefender Offline Activation page.
4. Enter your license key and the activation code that you obtained from the MetaDefender Core Management Console.

Metadefender Offline Activation



The form is titled "Metadefender Offline Activation" and is contained within a light gray border. It features several input fields and a button. At the top, there is a dropdown menu labeled "Metadefender Package" with the selected option "Metadefender Core v4.x - all packages". Below this is a text input field for "Activation Key *". The next field is "Requested Number of Nodes *", which contains the number "1". This is followed by a text input field for "Deployment ID *". Below these fields is a text area for "Optional Description" with the placeholder text "This helps you to identify this deployment on OPSWAT License portal". At the bottom of the form is a green button labeled "Request Unlock Key".

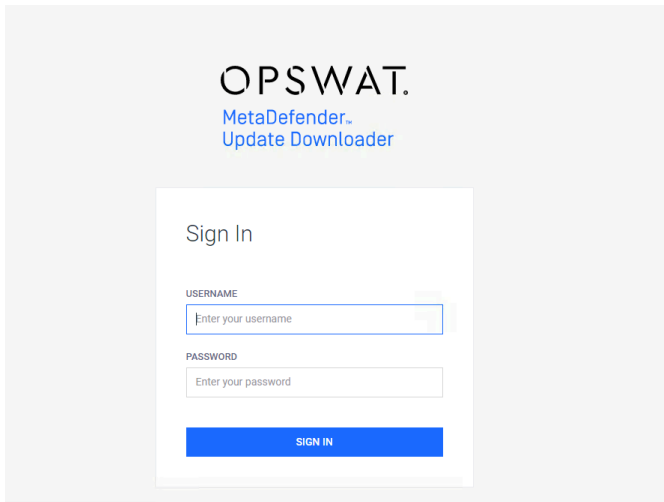
5. Apply that key to your MetaDefender Core server via the Management Console.

Installing the MetaDefender Update Downloader utility

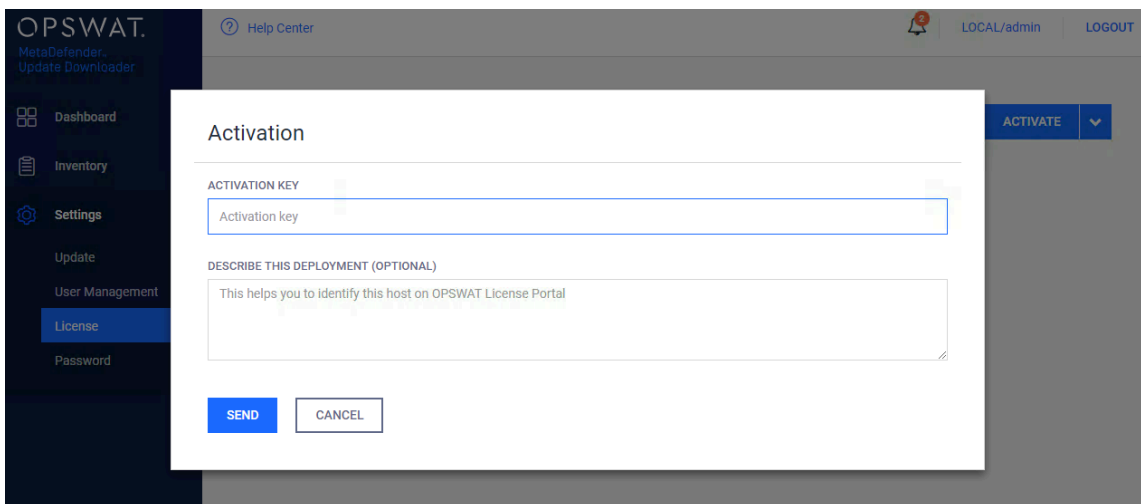
If your MetaDefender Core server is deployed offline, you will need to use the Update Downloader utility to download the anti-malware definition updates to be applied to the server. You can download the Update Downloader utility from the [OPSWAT Portal](#).

Once you have installed the Update Downloader, apply your license key to activate the product:

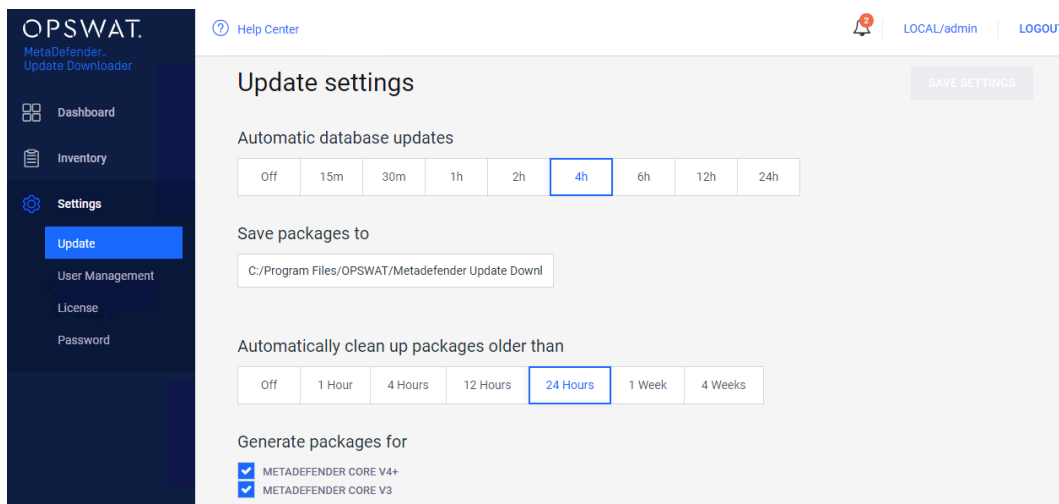
1. Log into the Update Downloader Management Console at `http://<server>:8028/`. The default user ID and password are admin/admin.



2. Apply your license key under **Settings > License**. This automatically configures the Update Downloader to download the anti-malware engine updates that are included with your license.



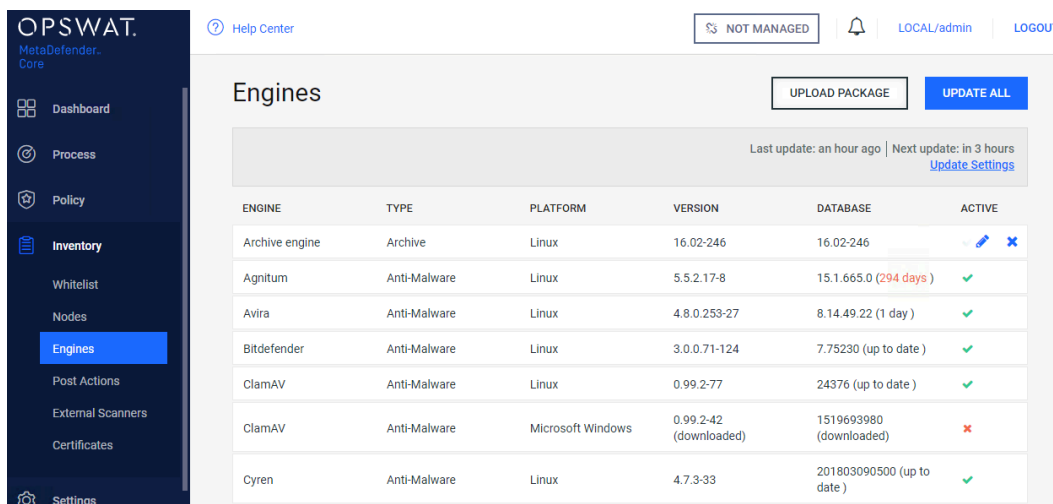
3. Update the configuration for update download and package generation on the Settings page of the Management Console.



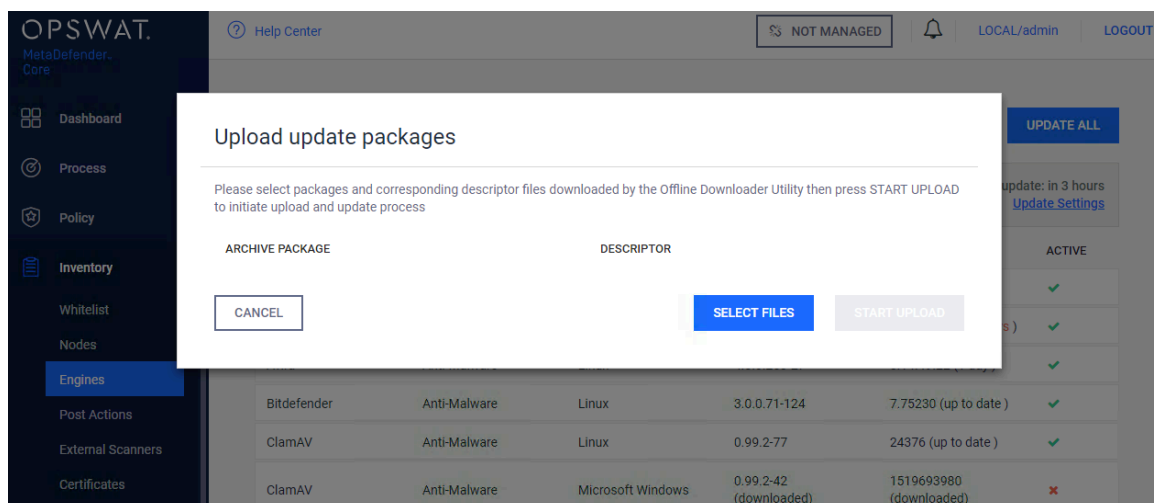
Applying offline updates

Once the update packages have been downloaded, you can apply them to the offline MetaDefender Core server through the MetaDefender Core Management Console.

1. Copy all of the update packages from the directory where the Update Downloader saves the updates to the offline MetaDefender Core system.
2. Upload the update packages through the MetaDefender Core Management Console.



3. Select the engine update packages from the directory where the Update Downloader is configured to save the update packages.



Contacting OPSWAT Support

If you have any questions or run into any difficulties in setting up your offline deployment of MetaDefender Core v4, please contact the [OPSWAT Support team](#).

This article applies to MetaDefender Core v4 Linux

This article was last updated on 2018-03-26

CN

How do I deploy MetaDefender Core v4 to an offline Windows environment?

Just like MetaDefender Core v3 (formerly Metascan), MetaDefender Core v4 supports deployment in either online or offline environments, although there are some differences between the two versions. Since the process has changed, we would like to provide an update to our users that will be upgrading to MetaDefender Core v4 in an offline environment.

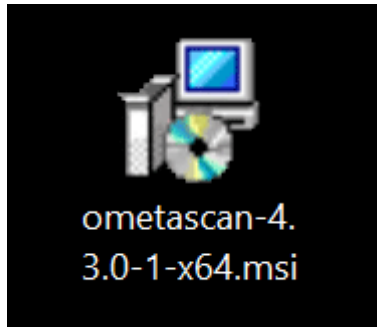
There are four steps to getting the product up and running in an offline environment:

1. Install MetaDefender Core on the offline server.
2. Activate your license.
3. Install and configure the MetaDefender Update Downloader utility.
4. Apply the offline updates that are downloaded by the update utility to the offline MetaDefender Core server.

Installing MetaDefender Core

You can download the MetaDefender Core installation packages from the [OPSWAT Portal](#). After logging into the Portal, navigate to the Downloads page, where you can select the MetaDefender Core package you wish to download. The supported operating systems include Windows 7 and later.

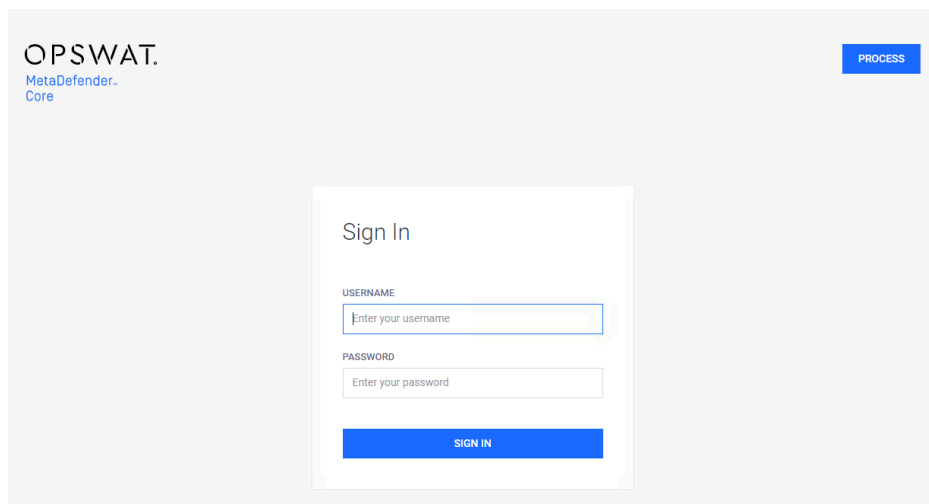
Download the installer and run it on the Windows system.



Activate your license

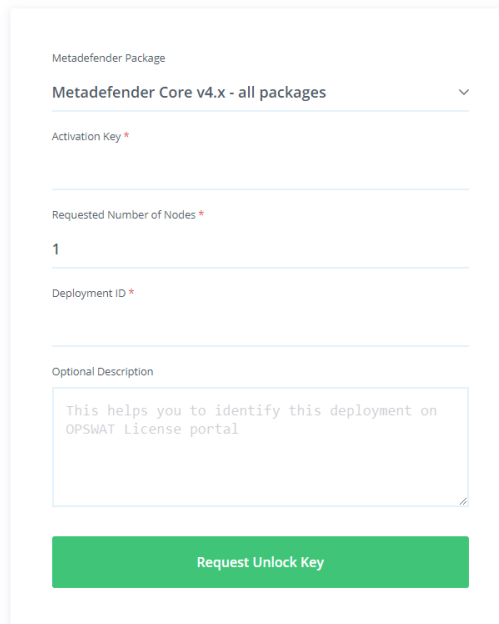
After MetaDefender Core is installed, you will need to activate your MetaDefender Core installation.

1. Log into your MetaDefender Core Management Console at <http://localhost:8008/>. The default user ID and password for a new installation are admin/admin.



2. Go to **Settings > License**.
3. Log into the OPSWAT Portal and navigate to the MetaDefender Offline Activation page.
4. Enter your license key and the activation code that you obtained from the MetaDefender Core Management Console.

Metadefender Offline Activation



The form is titled "Metadefender Offline Activation" and is contained within a light gray border. It features several input fields and a submit button. At the top, there is a dropdown menu labeled "Metadefender Package" with the selected option "Metadefender Core v4.x - all packages". Below this is a text input field for "Activation Key *". The next field is "Requested Number of Nodes *", which contains the number "1". This is followed by a "Deployment ID *" field. Below these is a text area for "Optional Description" with the placeholder text "This helps you to identify this deployment on OPSWAT License portal". At the bottom of the form is a prominent green button labeled "Request Unlock Key".

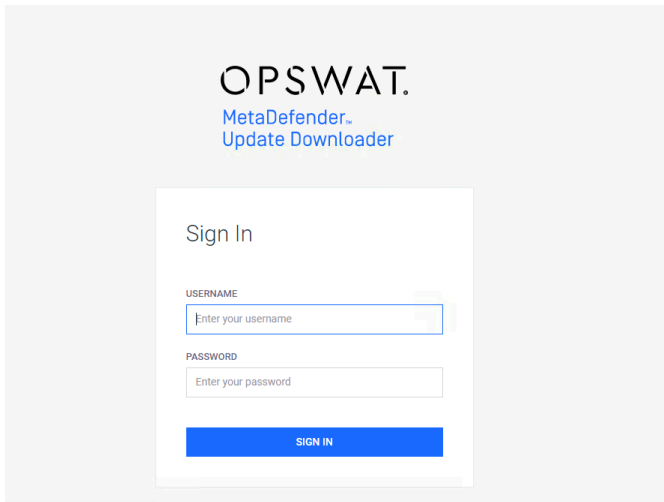
5. Apply that key to your MetaDefender Core server through the Management Console.

Installing the MetaDefender Update Downloader utility

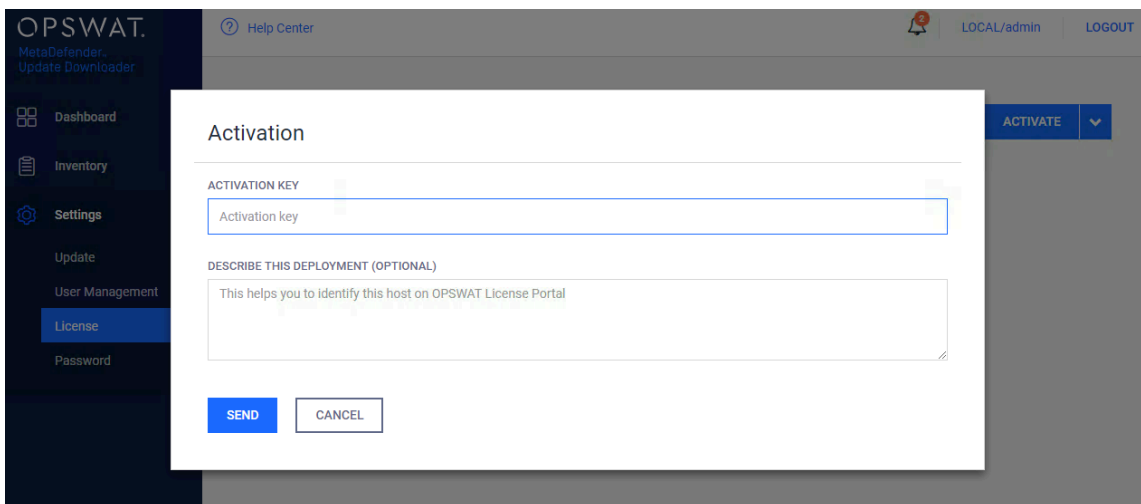
If your MetaDefender Core server is deployed offline, you will need to use the Update Downloader utility to download the anti-malware definition updates to be applied to the server. You can download the Update Downloader utility from the [OPSWAT Portal](#).

Once you have installed Update Downloader, apply your license key to activate the product.

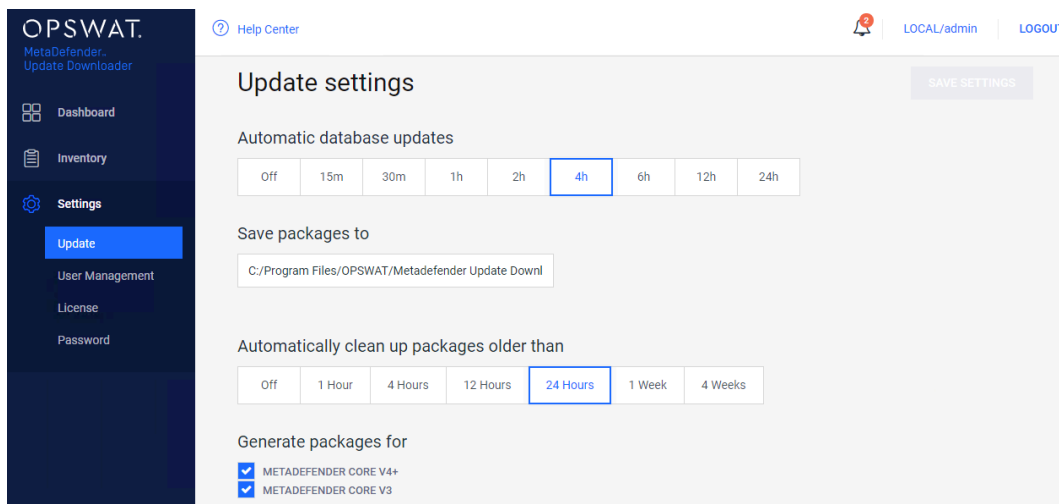
1. Log into the Update Downloader Management Console at `http://<server>:8028/`. The default user ID and password are admin/admin.



2. Apply your license key under **Settings > License**. This automatically configures the Update Downloader to download the anti-malware engine updates that are included with your license.



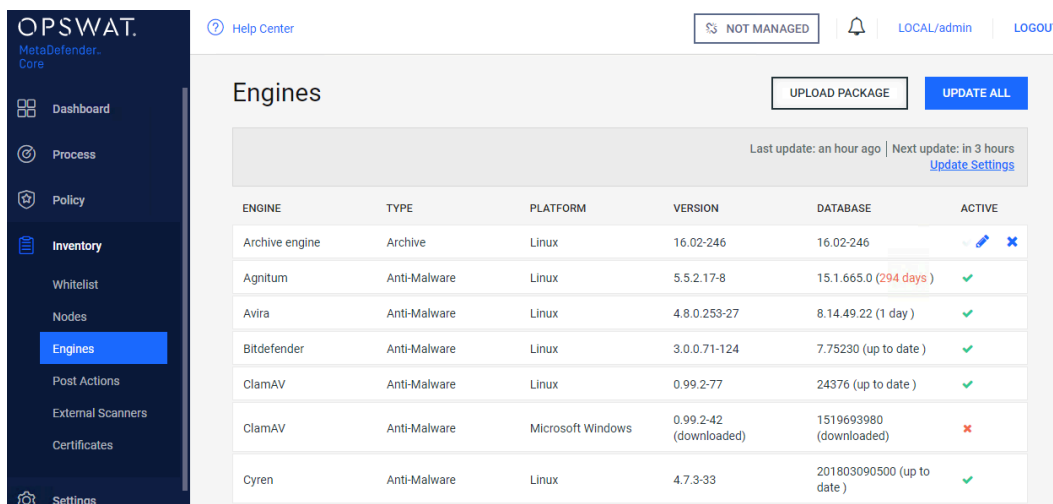
3. Update the configuration for update download and package generation on the Settings page of the Management Console.



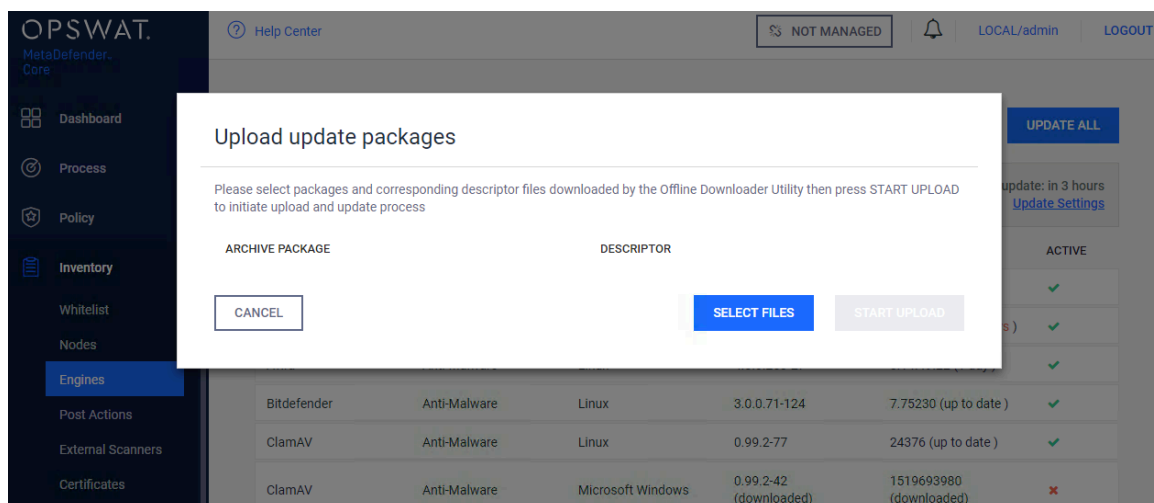
Applying offline updates

Once the update packages have been downloaded, you can apply them to the offline MetaDefender Core server through the MetaDefender Core Management Console.

1. Copy all of the update packages from the directory where the Update Downloader saves the updates to the offline MetaDefender Core system.
2. Upload the update packages through the MetaDefender Core Management Console.



3. Select the engine update packages from the directory where the Update Downloader is configured to save the update packages.



Contacting OPSWAT Support

If you have any questions or run into any difficulties in setting up your offline deployment of MetaDefender Core v4, please contact the [OPSWAT Support team](#).

This article applies to MetaDefender Core v4 Windows

This article was last updated on 2018-03-26

CN

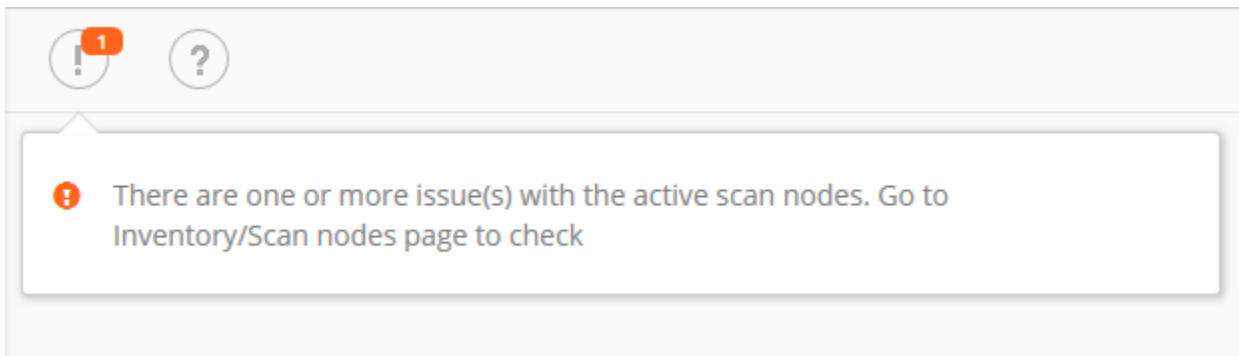
How do I disable real-time protection of my anti-malware software if it is not allowed by corporate policy for use with MetaDefender Core v4?

Anti-malware engines included in MetaDefender Core v4 do not install real-time protection agents. If you already have an anti-malware product installed on your system which may also be one of the anti-malware engines in your version of MetaDefender Core v4, it will interfere with the scanning process performed by MetaDefender Core v4. For this reason, it is recommended that you disable the real-time protection of your anti-malware product.

If your corporate policy does not allow you to disable your real-time anti-virus product, you will need to add some exception rules. As part of your exception rule, you need to exclude the OPSWAT installation folder which by default also includes the folder where MetaDefender Core is creating its temporary files.

Metadefender will not deploy engines if it detects an active on-access scanner. It does the detection using an eicar file put into the product's temp folder.

Please monitor the notification you see on the exclamation mark



Troubleshooting should start by checking the Scan Nodes tab under Inventory:

Node details

Status: A 3rd party product blocks our operation. Can't access our files in C:/Program Files/OPSWAT/Metadefender Core/data/resources.
6 engines are not deployed to this node
[See documentation for details.](#)

Address: localhost
OS: Microsoft Windows 10 Enterprise Edition
Version: 4.6.1

ENGINES
0/6

ISSUES ENGINES HARDWARE INFO

ISSUE	SEVERITY
A 3rd party product blocks our operation. Can't access our files in C:/Program Files/OPSWAT/Metadefender Core/data/resources.	⚠
6 engines are not deployed to this node	⚠

[CLOSE](#)

If you do not add this exception or if you do not disable real-time protection, results returned by MetaDefender Core v4 for scanning will not be consistent.

1. If no engines will be deployed :

- The following result will be returned: Not Scanned
- An error will be displayed

2. If the engines get deployed and you turn Real Time protection on, the return value of the scans would be one of the following:

- **Clean:** If your existing anti-malware product was able to clean the threat

- **Failed** (or other errors): If your existing anti-malware product removed the file before MetaDefender Core could scan it

If you need help on how to add an exception rule to exclude a given folder from scanning for a anti-malware product, please [tell us](#) what product you are using and we may be able to help you. Be sure to include the product version.

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-26

CN

How do I remove an engine from my MetaDefender v4 instance?

MetaDefender v4 downloads engines based on the license key activated on the system. If an engine is manually removed, MetaDefender Core v4 will automatically download the engine again the next time it updates.

In order to completely remove an engine so it will disappear from the engine list and no engine files are left on the system or downloaded again, you will need to get a new license key that does not include the engine. Please contact OPSWAT support.

To create a support ticket, please follow the steps below :

1. Navigate to <https://my.opswat.com/hc/en-us/requests/new>.
2. From the dropdown select MetaDefender Core v4 for Linux/Windows.
3. Fill in the required fields.
4. Fill in the section labeled "OPSWAT License Information".
5. Click Submit.

A support engineer should get back to you with a new license or a request for more information shortly after you've created this ticket.

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-26

CN

How do I use MetaDefender Core v4 Workflows ?

In MetaDefender Core v4, Workflows are called Workflow Templates and are just one integrated component of Security Policies. Thus it is typically not sufficient to understand just how to use Workflows; you need to understand how [Security Policies work and all of the components within these policies](#).

For readers familiar with MetaDefender v3 Workflows, be aware that the design, the attributes, and the overall architecture of Workflows has changed in MetaDefender Core v4, so be careful not to confuse the concepts you know from v3 with the behavior and setup in v4.

Defining and administering Workflow Templates in MetaDefender Core v4

As an administrator, you define Workflows and apply them to the security policies that will determine how files get processed. MetaDefender Core v4 provides three predefined Workflows out-of-the-box: "Default", "Skip Images", and "Executables only".

The screenshot shows the 'Workflow Templates Management' page in the OPSWAT MetaDefender Core v4 interface. The left sidebar contains navigation options: Dashboard, Process, Policy (selected), Workflow rules, Workflow templates (highlighted), Security zones, Inventory, and Settings. The main content area features a table with the following data:

NAME	DESCRIPTION
Default	Selecting this template all files will be processed without any filtering.
Skip images	Selecting this template all files but certain commonly used image files, such as gif, jpg, png, psd, bmp and tiff files will be p...
Executables only	Selecting this template only executable files will be processed. All skipped files will be shown as 'not scanned' in the report.

At the top right of the main content area, there is a blue button labeled 'ADD NEW WORKFLOW'. The top navigation bar includes 'Help Center', 'NOT MANAGED', a notification bell, 'LOCAL/admin', and 'LOGOUT'.

You cannot edit or remove these predefined Workflows, but you can define additional Workflows. You can do this by pressing the "ADD NEW WORKFLOW" button on the top right side of the screen to create a new Workflow. The pop-up lets you name the Workflow and provide a description that will help you track the purpose of the Workflow.

The screenshot shows the 'Add new Workflow' pop-up form. The left sidebar is partially visible, showing the 'Policy' section with 'Workflow templates' selected. The main content area is titled 'Add new Workflow' and contains two input fields: 'WORKFLOW NAME' and 'DESCRIPTION'. Below the input fields are 'SAVE' and 'CANCEL' buttons. The top navigation bar is identical to the previous screenshot, showing 'Help Center', 'NOT MANAGED', a notification bell, 'LOCAL/admin', and 'LOGOUT'. The bottom of the sidebar shows the version '4.9.0.680' and the license expiration date '03/02/2026'.

To edit a Workflow click on the Workflow in the list to pop up the "Modify workflow" window. The configuration options are categorized into a set of tabs. These tabs are explained in more detail in the MetaDefender Core v4 user guide. Make sure to review the tab definitions in the [MetaDefender Core v4 user guide's workflow section](#).

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-26

CN

How long is the support life cycle for a specific version/release of MetaDefender Core v4?

OPSWAT provides support on each release of MetaDefender Core for **18 months** after the publication of the next release of the product (i.e. once a new release is published, you have 18 more months of support on the previous release). However, bug fixes and enhancements are applied only to the next release of a product, not to the current release or historical releases, even when those releases are still under support. In some cases hot-fixes can be provided for the current release of the product, and then incorporated as a regular fix in the next release.

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

Release number	Release date	End-of-life date
4.13.1	01 Nov 2018	01 May 2020
4.12.2	04 Oct 2018	04 Apr 2020
4.12.1	27 Sep 2018	27 Mar 2020
4.12.0	17 Sep 2018	17 Mar 2020
4.11.3	30 Aug 2018	02 Mar 2020
4.11.2	29 Aug 2018	01 Mar 2020
4.11.1	08 Aug 2018	08 Feb 2020
4.10.1	23 May 2018	23 Nov 2019

Release number	Release date	End-of-life date
4.10.0	02 May 2018	02 Nov 2019
4.9.1	08 Mar 2018	09 Sep 2019
4.9.0	11 Dec 2017	08 Jun 2019
4.8.2	11 Oct 2017	11 Jun 2019
4.8.1	05 Oct 2017	29 Mar 2019
4.8.0	07 Jul 2017	06 Jan 2019
4.7.2	31 May 2017	30 Nov 2018
4.7.1	16 May 2017	15 Nov 2018
4.6.3	04 Apr 2017	03 Oct 2018
4.6.2	15 Mar 2017	14 Sep 2018
4.6.1	03 Feb 2017	03 Aug 2018
4.6.0	07 Jan 2017	07 Jul 2018
4.5.1	12 Oct 2016	11 Apr 2018
4.5.0	30 Sep 2016	29 Mar 2018
4.4.1	10 Aug 2016	09 Feb 2018
4.3.0	12 May 2016	11 Nov 2017
4.2.0	19 Feb 2016	18 Aug 2017
4.1.0	30 Sep 2015	29 Mar 2017
4.0.1	10 Aug 2015	09 Feb 2017

4.0.0	16 Jul 2015	15 Jan 2017
-------	-------------	-------------

This article pertains to all supported releases of MetaDefender Core v4

This article was last updated on 2018-11-01

SS

Is action needed because Metadefender v4's AVG license is expiring on 2018-06-15?

Effective June 15, 2018, the AVG license used by MetaDefender will expire, and that engine will no longer work properly within MetaDefender.

What do I need to do?

If you purchased the product after August, 2017 then you do not have any further task.

License owners purchased the license before this date should check the following:

- If you are using a MetaDefender 12 package on v4 you need to ensure that your MetaDefender Management Console lists Cyren as one of the active engines. If it does not, you should deactivate and then re-activate the MetaDefender license, after which you should see on the management console that the Cyren engine has replace the AVG engine.
- If you are using a MetaDefender 16 package on v4 you need to ensure that your MetaDefender Management Console lists VirIT Explorer as one of the active engines. If it does not, you should deactivate and then re-activate the MetaDefender license, after which you should see on the management console that the VitIT Explorer engine has replace the AVG engine.
- If you are using a MetaDefender 20 package on v4 you need to ensure that your MetaDefender Management Console lists Antiy as one of the active engines. If it does not, you should deactivate and then re-activate the MetaDefender license, after which you should see on the management console that the Antiy engine has replace the AVG engine.

All other supported MetaDefender packages (MetaDefender 4, MetaDefender 8, MetaDefender for Linux, MetaDefender ISV) are not affected by the AVG license and thus require no action on your part.

What if I don't take action by June 15, 2018?

AVG will stop working properly once the license terminates. If you are using a MetaDefender package that has AVG, you will notice that that engine fails to scan any incoming files. Other AVs and other elements of MetaDefender should not be affected by this.

Why is the license for AVG expiring?

Avast announced AVG's acquisition in mid 2016 and then ended the AVG OEM business of AVG in August, 2017. However, the last AVG OEM license purchased by OPSWAT was set to terminate on June 15, 2018.

What if I need more assistance from OPSWAT on this topic?

If you need more assistance, please contact OPSWAT Support by logging a ticket through your OPSWAT Portal Account at portal.opswat.com

This article applies to any MetaDefender Core v4 installation that has not had a license reactivation since end-of-August, 2017

This article was last updated on 2018-06-14

AA

Is there a virus test I could use to test MetaDefender Core v4?

Tests to determine an engine's operation are rarely run with live malware. The suggested approach to test is to use an industry-standard test file called an EICAR Test File, which most antivirus engines detect as positive even though no threat exists.

The EICAR Test File can be found at the following path from MetaDefender Core directory if the product is up and running: **MetaDefender Core\data\resources**. You can also create your own version of the file by copying the following string into a file and renaming it to "eicar.com".

`X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`

For more information about the EICAR Test File, please visit the European Expert Group for IT-Security's [website](http://www.eug-security.org).

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-26

CN

MetaDefender Core v4 shows a large number of files that failed to scan. What can I do?

MetaDefender Core v4 introduces an option that modifies the behavior of MetaDefender Core when a specific engine fails to scan.

Under normal circumstances, all active engines scan every file. Occasionally, an engine will encounter a file that causes it to crash. When this happens, MetaDefender Core will wait some time for the engine to recover, after which, it will restart the engine. During this time, the engine's results will be logged as "Failed to scan".

However, MetaDefender Core can be configured to fail the scan if any of the engines report problems. In other words, it can toss out all partially incomplete scans. This can give the illusion that MetaDefender core is failing to scan large amounts of files.

Disabling this option can be done by:

1. In your web browser, navigate to the MetaDefender Core Management Console at: <http://localhost:8008/> (you may need to login under admin privilege)
2. On the left menu, navigate to Policy -> Workflow Rules to list all available rules
3. Click on a rule you are using for the current scan, a window pops up where beside the rule properties all the chosen workflow's options are shown on the different tabs.
4. Click on Scan tab
5. Uncheck the option "Scan failure threshold" shown below:

Modify rule

GENERAL
ARCHIVE
BLACKLIST
SCAN
METADEFENDER.COM
DATA SANITIZATION

SKIP SCAN BY FILENAME

FILENAME	IF SIZE IS BIGGER [IN MEGABYTES]
No filter has been created yet.	
<input style="border: none; background: none; cursor: pointer;" type="button" value="+"/>	

PER ENGINE SCAN TIMEOUT [IN MINUTES]

GLOBAL SCAN TIMEOUT [IN MINUTES]

MAXIMUM FILE SIZE FOR FILES SCANNED [IN MEGABYTES]

SCAN FAILURE THRESHOLD ⓘ

THRESHOLD VALUE ⓘ

This article applies to MetaDefender Core v4 Windows and Linux

This article was last updated on 2018-03-26

CN

Post actions in MetaDefender core V4.8.0 and above

ⓘ Disclaimer

This sample script is provided for illustrative purpose only and is not guaranteed to be functional in a production environment.

MetaDefender core V4.8.0 has a new feature "Post Actions".

You can define a "Post Action" which is a command line executable or script that will be called after each scan is finished.

The documentation of this feature can be found here: https://onlinehelp.opswat.com/corev4/3.10._External_Scanners_And_Post_Actions.html

For this script to work properly, we need to call Powershell in the Post Actions screen of MetaDefender core:

NAME	POST ACTION
Loading...	
Sorter	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Users\Administrator\Desktop\Post_actions\post_action_sample.ps1

You will need to specify the location from where Powershell is running in your system followed by:

- ExecutionPolicy Bypass
- -File TheNameAndPathOfYourScriptFile.ps1

We created a sample Powershell script that sorts the files according to their result. (Allowed /Blocked)

The script is called after the scan is finished.

It accepts as its input:

1. The current scan results JSON from STDIN.
2. The full path to the currently scanned file as the last argument on the command line.

And returns the following return values:

0 - Success

1 - Json Parse error - The script was unable to parse the expected JSON from STDIN

2 - Copy error - file copy to failed

3 - file path of currently scanned file is invalid

4 - the destination path of either allowed/blocked or both is invalid.

The script itself can be found and downloaded from the following link:

post_action_sample.ps1

This article applies to MetaDefender Core v4 Windows

This article was last updated on 2018-03-26

CN

Using MetaDefender core V4 BLACKLIST/WHITELIST feature

MetaDefender core V4.x includes the option to block or allow files by creating a BLACKLIST or WHITELIST.

The user can select files to be blocked or allowed based on:

- File type group
- MIME-type
- File name

The documentation is here https://onlinehelp.opswat.com/corev4/3.6.2._Analysis_workflow_configuration.html

The conventional usage of this feature would be, to create a list of files to be blocked or allowed, by any of the three selectors mentioned above (filetype groups, mime-types, file names) or a combination of them.

Using filetype groups VS. MIME-types VS file extensions

When possible, It is better to use Filetype groups over MIME types, and MIME types over File names.

It is shorter to define, leaves less space for human error and can also leverage OPSWAT's file detection mechanism, so that even if an imposter file has the extension .doc but in reality it is a .exe it will be treated as .exe

Using Regular Expressions

The rules we create can consist of literal strings but can also include wild cards in the form of Regular Expressions.

For example if we use the string : `^.*\.docx$` in the "Blacklist by file names", it will test as True for all files who's name is terminating with docx.

Each file processed by MetaDefender core will be tested against the rules defined in the blacklist.

As soon as any of the rules tests as True the file will be blocked.

Advanced usage

Sometimes the business rule is something like "Block all files except...".

Such a scenario is accommodated in the system by the usage of Regular Expressions.

In Regular Expression we can create an expression that will test as True when a certain string is NOT found (known as Negative Look Ahead)

For example if we use the string: `^.*\.(?!docx$).*` in the "Blacklist by file names", it will test as True for files who's names do NOT terminate with docx.

* To make the above Regular Expression case insensitive we can use: `^.*\.(?![dD][oO][cC][xX]$).*`

In many cases we will need to allow more than one file type.

For example if we use the string: `^.*\.(?!docx$)(?!xls$).*` in the "Blacklist by file names", it will test as True for files who's names do NOT terminate with either docx or xls.

The Negative Look Ahead block `(?!XYZ$)` can be repeated as many times as required.

In the example given above "Block all files except docx" there is a hidden problem.

.docx files are actually archive files, containing other files (such as xml, gif, jpeg etc...)

This means that if the business rule is **block everything except docx** it most likely means **block everything except docx and all the files it contains**.

Note: You can use a tool such as <https://regex101.com/> to create and test your regular expressions.

This article applies to MetaDefender Core v4 Windows

This article was last updated on 2018-04-11

OL

What are Security Policies and how do I use them?

Understanding Security Policies

The term Security Policies describes three objects and their relationship to each other:

- Workflow Rules
- Workflow Templates
- Security Zones

Workflow Rules

Workflow Rules is the object that each file interacts with directly when being processed by MetaDefender. i.e. Each file is processed through one (and only one) of the defined Workflow Rules.

The workflow rule is identified by its name. It defines eligibility parameters to use it (i.e. whether a client is in the proper Security Zone and/or the actual logged in user is in the specified Role and/or the client has provided the required user_agent). It inherits processing characteristics (i.e. whether to scan files with the malware engines, if and how to use data sanitization, if and how to extract archives, etc.) from a Workflow that gets assigned to it. It also allows direct assignment of processing characteristics that over-ride the characteristics of the workflow.

You create a workflow rule by giving it a name and assigning a Security Zone and a Workflow template to it. You can also assign specific processing characteristics to it. A file's eligibility to be processed by the Workflow Rule is determined by the filtering parameters in the General tab. If all the required parameters are matching, the processing actions performed on that file are determined by the specific processing characteristics set on the Workflow Rule in case the Workflow Rule does not override the underlying Workflow, then the Workflow's scanning characteristics will be used. i.e. the workflow determines each processing setting that is not explicitly set at the Workflow Rule. Workflow Rules can be reordered using drag&drop.

A file that is eligible to be processed by more than one Workflow Rule will still only get assigned to one Workflow Rule (the assignment logic is described below). A file that is not eligible for any Workflow Rule will not be processed.

Security Zones

Security Zones is the object that defines a network or set of networks (as defined by IP masks). Only files whose source location is in that network are eligible to be routed to a Workflow Rule that is assigned that Security Zone

Workflow Templates

Workflow Templates is the object where you define a set of process actions (and associated action properties) such as malware scanning, sanitization, archive handling, etc. The Workflow Rule does not get applied directly to the file; the Workflow Rule is associated with a Workflow Templates, and it is the Workflow Rule that gets applied to the file. The Workflow Template can be thought of as a template of process settings - by assigning the Workflow Rule to a Workflow Template, the Workflow Rule inherits the Workflow Template settings for each field that has not been directly populated on the Workflow Rule.

Workflow Templates that are included out-of-the-box with each MetaDefender Core v4 installation are: "Default", "Skip Images", and "Executables only". These workflows cannot be altered or deleted, but they can be copied to custom workflows that can then be edited.

Note: Only the three Workflows mentioned above will be migrated when you upgrade MetaDefender core.

Assigning a Workflow Rule to process a file

Workflow Rules are evaluated one by one according to the order they appear in the UI. The first Workflow Rule that satisfies the request will be selected for processing.

When submitting a file via the [REST API](#) you can use a specific Rule or specific set of Rules.

- the User Agent that represents your client application (user_agent header) and/or
- the name of a specific Workflow Rule you want to use (rule header)

Please keep in mind that even if you specified a specific Workflow Rule to use, It still needs to satisfy the eligibility (Security Zone and/or logged in user is in the specified Role and/or the client has provided the required user_agent) in order to be used.

You can use [this REST API](#) to fetch the names of the available rules that match all the criteria (you have to specify the same user_agent header as you want to use for the file scan request).

When submitting a file via one of the OPSWAT client applications (e.g. MetaDefender Client, MetaDefender Kiosk) and you want to use a specific Rule for the application please make sure you have set up a proper rule with the proper User Agent filter.

When submitting a file via the browser (web scan), MetaDefender will use the Workflow Rule you selected via the UI. Only the rules that match with all the eligibility parameters are shown on the UI.

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-26

CN

What features of MetaDefender Core version 3 are available in version 4 ?

MetaDefender Core v4 is a completely redesigned and re-architected product, built with the latest generation tools to provide more flexibility, security and scalability for our customers.

OPSWAT continuously introduces new features and functionality on MetaDefender v4 that are not available on MetaDefender v3. OPSWAT is also working aggressively to add most of the MetaDefender v3 features and functions into v4 - i.e. for v4 to have feature parity with v3. The table below provides a quick overview of the feature parity status.

If there are any key features missing from v4 that you use in your v3 deployment, please contact OPSWAT Support and let us know.

	Included in MetaDefender Core v3?	Included in MetaDefender Core v4?
Engines and updates		
4, 8,12,16 and 20 engine packages	YES	YES
Custom engines	YES	YES
Support for HTTP proxy authentication	YES	NOT YET
Engine auto update (Other than signature)	NO	YES
RAM drive for scanning	YES	YES See this how-to
Workflow functionality	YES	YES
File type detection		
File type grouping	YES	YES
Detection overwrite	YES	NOT PLANNED Report any misdetection to OPSWAT support
Data sanitization	YES	YES

	Included in MetaDefender Core v3?	Included in MetaDefender Core v4?
Sanitize clean and blocked files (Windows)	YES	YES
Sanitize clean and blocked files (Linux)	N/A	BETA
API		
REST v1	END-OF-LIFE	NOT PLANNED
REST v2	YES	YES
COM	YES	NOT PLANNED
Sample code for existing APIs		
Java	YES	YES https://github.com/OPSWAT/MetaDefender-Core-Client
C#	YES	YES https://github.com/OPSWAT/metadefender-core-client-csharp
Upload files using chunked encoding	YES	NOT YET
Support for other MetaDefender products		

	Included in MetaDefender Core v3?	Included in MetaDefender Core v4?
Secure File Transfer	YES	YES
Email Security	YES	YES
ICAP Server	YES	YES
Kiosk	YES	YES
New generation MetaDefender Client	YES as of v3.12.2	YES



Note: Customers with an active license for MetaDefender Core v3 can upgrade to v4 for free. Contact OPSWAT Support to get a replacement MetaDefender Core v4 license as well as guidance on your upgrade / migration plan.

Although there is no date yet announced for end-of-life / end-of-support for v3, customers are encouraged to move to v4 as soon as possible to get all the benefits of our flagship product version.

This article applies to MetaDefender Core v3 and v4

This article was last updated on 2018-03-26

CN

What file types are supported by DLP engine?

What is Data Loss Prevention (DLP)?

The purpose of Data Loss Prevention (DLP) is to detect potential data breaches or the theft of data by detecting and blocking sensitive data. The data can be at rest (on a device) or in motion (a file being sent somewhere). Usually sensitive data are data items like social security numbers or credit card numbers, but also might be company confidential or sensitive documents.

What is the strength of OPSWAT's DLP Solution?

Where OPSWAT shines is in its ability to handle a huge number of file types. DLP is also a great add-on technology if you are already using OPSWAT's MetaDefender solutions. If you are already doing multi-scanning or vulnerability assessment you can easily add data loss prevention to your pre-existing MetaDefender deployments.

Meta Data Check (Only):

For the following file types OPSWAT only checks the metadata in the file. Most of these file types in this category are media or image files, where the meta data is embedded in the file property, and might be for example the time when the image was taken, the model of the camera used to create the image, the location where the photo was taken, etc.. One example of this type of meta data is EXIF data. Sensitive information cannot be detected if it is part of the image, for example if a photograph of a whiteboard was taken that has writing on it that was sensitive.

- Adobe Photoshop images (*.psd)
- ASF media files (*.asf)
- JPEG (*.jpg)
- MP3 (*.mp3)
- TIFF (*.tif)
- WMA media files (*.wma)
- WMV video files (*.wmv)

File Conversion and Parse:

With these types of files OPSWAT can detect any type of confidential information in the text portion of the file to include meta data areas of the file. Conceptually, think of the file as being converted into a text file and all of the text in the file being parsed and searched for sensitive data items. So for example, all the text elements of an Excel file would be converted into text and then the text would be searched.

- Adobe Framemaker MIF (*.mif)
- Ansi Text (*.txt)
- Apple iWork KeyNote 2009 (*.key)
- Apple iWork Numbers 2009 (*.numbers)
- Apple iWork Pages 2009 (*.pages)
- ASCII Text

- CSV (Comma-separated values) (*.csv)
- DBF (*.dbf)
- EML (emails saved by Outlook Express) (*.eml)
- Eudora MBX message files (*.mbx)
- HTML (*.htm, *.html)
- iCalendar (*.ics)
- MSG (emails saved by Outlook), including attachments (*.msg)
- Microsoft Access 95, 97, 2000, 2003, 2007, 2010, 2013, and 2016 MDB (*.mdb, *.accdb)
- Microsoft Excel for Mac 2.2, 3, 4, 5, 98, 2001, X, 2004, 2008, 2011
- Microsoft Excel for Windows 2, 3, 4, 5
- Microsoft Excel 95, 97, 2000, XP, 2003, 2007, 2010, 2013, 2016 (*.xls)
- Microsoft Excel 2003 XML (*.xml)
- Microsoft Excel Office Open XML 2007, 2010, 2013, and 2016 (*.xlsx)
- Microsoft OneNote 2007, 2010, 2013, and 2016 (*.one)
- Microsoft Outlook 97, 2000, 2003, 2007, 2010, 2013, and 2016 data files, including attachments (*.PST, *.OST)
- Microsoft Outlook/Exchange Messages, Notes, Contacts, Appointments, and Tasks
- Microsoft Outlook Express 5 and 6 (*.dbx) message stores
- Microsoft PowerPoint 3, 4, 95, 97, 98, 2000, 2001, 2002, 2003, 2004, 2007, 2008, 2010, 2011, 2013, 2016 (*.ppt)
- Microsoft PowerPoint Office Open XML 2007, 2010, 2013, and 2016 (*.pptx)
- Microsoft Rich Text Format (*.rtf)
- Microsoft Searchable Tiff (*.tiff)
- Microsoft Word for DOS 1, 2, 3, 4, 5, 6 (*.doc)
- Microsoft Word for Mac 1, 3, 4, 5, 6, 98, 2001, X, 2004, 2008, 2011
- Microsoft Word for Windows 1, 2, 6 (*.doc)
- Microsoft Word 95, 97, 98, 2000, 2002, 2003, 2007, 2010, 2013, 2016 (*.doc)
- Microsoft Word 2003 XML (*.xml)
- Microsoft Word Office Open XML 2007, 2010, 2013, 2016 (*.docx)
- Microsoft Works WP (*.wks)

- OpenOffice/LibreOffice versions 1, 2, 3, 4, and 5 documents, spreadsheets, and presentations (*.sxc, *.sxd, *.sxi, *.sxw, *.sxc, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (includes OASIS Open Document Format for Office Applications)
- PDF files (*.pdf), note: Encrypted PDF files cannot be indexed, unless the PDF file can be opened without a password and the PDF file permissions allow for text extraction.
- PDF Portfolio files (*.pdf), including embedded non-PDF documents.
- Unicode (UCS16, Mac or Windows byte order, or UTF-8)
- Visio XML files (*.vdx)
- WordPerfect 4.2 (*.wpd, *.wpf)
- WordPerfect (5.0 and later) (*.wpd, *.wpf)
- WordStar version 1, 2, 3 (*.ws)
- WordStar 2000
- XML (*.xml)

This article applies to MetaDefender Core v4

This article was last updated on 2018-09-24

AA

What file types can be verified by MetaDefender v4?

What is file type verification?

File type is usually represented by its file extension and associated application(s). Each file type has one or more corresponding file extensions. The file extension is appended to the end of each file name which provides a simple way for both the operating system and users to identify the file type of each file. However, file extension can be changed easily to spoof the operating system and users without modifying the content or changing the capability of the file to bypass certain security or filtering prevention systems. Our file type verification function offers an advanced mechanism to validate a given file type by analyzing the file's structure and content. With this technology, users can verify the true file type for given files and minimize the risk of file type spoofing.

What is the difference between file type and file format?

File type and file format are, in most of the cases, used interchangeably. But from a strict definition stand point, file format describes how the file structures and organizes the content. It specifies how bits are used to encode information in a digital storage medium. And it is

considered as a standard way that information is encoded for storage in a computer file. For example, the file type of an image file saved using JPEG compression may be defined as a "JPEG image file." The file format may be described as a binary file that contains a file header, metadata, and compressed bitmap image data.

What does MetaDefender offer for file type verification?

With MetaDefender's file type verification technology, users can process files based on their true file types, so the system can take more precautions with risky file types like EXEs, perhaps setting different policies or rules based on file type. Spoofed file types indicate potentially malicious intent, so to mitigate this risk, MetaDefender offers functionality to block files with incorrect extensions, for example prevents an instance of EXE file which is posed as TXT file from entering the organization. Also, more strict rules, like remediation steps can be applied. For example, Data Sanitization is triggered as a post action for the file type verification. This is highly configurable so that Data Sanitization or any other secure processes can happen based on the target file name, file format and any other recognized file property data as well.

What is the limitation of file type verification?

File type verification is not the ultimate security protection for all use cases: our engineers analyze the file format identifier (magic signature), pattern and structure of the file content . This approach is not guaranteed to work for all file types. B oth false positive and false negative incidences may potentially apply

- File type verification is a validation method so it does not mean all file types that are covered for verification are supported by Multi-Scanning or Data Sanitization
- You should understand your use case and the potential impact on productivity before leveraging file type verification as a secure mechanism to stop files or allow files

MetaDefender version 4 can verify **more than 4,500 different file types** as of writing this article. See below for a complete list of all the supported file types:

Supported file type	Description
BAM	Infinity Engine Animation (v1)
0	Hacha multipart archive (block 0)
1	CP Backup saved data (v7.x)
545	AIMutation skin
669	Composer 669 module

Supported file type	Description
777	777 compressed archive
??_	Microsoft KWAJ compressed (Phil Katz's 'deflate')
@@@	DOS 2.0-3.2 Backup control info
_01	Compaq QRST disk image
{SA}PROJ	{smartassembly} project
~I	AZZ Cardfile index
000/001/999	Sage Backup
0SC/0FN	Jazz Jackrabbit font/cutscene
1SC	Bio-Rad Scan file
1TM	1tracker Module
2BIT	2BIT DNA sequences (LE)
2D	VersaCAD 2D drawing (MS-DOS)
2DA	Infinity Engine 2-Dimensional Array (v1.0)
2DC	Cadwork 2D Catalog
2DL	VersaCAD 2D Library (MS-DOS)
2MG/2IMG	2IMG Universal Format disk image (Apple II)
2SFLIB	2SF Nintendo DS Sound Format rip
3D	CAD-3D object

Supported file type	Description
3D2	Cyber Studio CAD-3D v2 object
3DB	3DMark database
3DM	Cadent 3D Model
3DMF	QuickDraw 3D Metafile (binary)
3DP	3Digi Parameters
3DR	3DMark2003 Results
3DS	3D Studio mesh
3DSX	Nintendo 3DS Homebrew relocatable and eXecutable binary
3DXML	3D XML files (unzipped)
3FR	Hasselblad 3F RAW image
3G2/3GPP2	3GPP2 multimedia audio/video
3GA	Mobile phone audio
3GP/3GPP	3GPP multimedia audio/video
3MF	3D Manufacturing Format model
3MM/3TH/CHK	3D Movie Maker (generic)
4PK	Perfect Keyboard macro set
4PP/PHP	Photoparade Slideshow
5VW	5View capture

Supported file type	Description
64C	C64 8x8 font bitmap
64S	Hoxs64 state snapshot
7Z	7-Zip compressed archive (gen)
8*	PhotoShop plug-in (generic)
8BF	Photoshop filter plug-in
8SVX/IFF	Amiga IFF 8SVX audio
8XK	Texas Instruments TI-8x series Calculators Program
8XU	Texas Instruments TI-8x series Calculators OS Upgrade
92I	TI bitmap
A	Binding of Isaac Rebirth packed Archive
A1WISH	Audials One Wishlist
A2D	Agros2D document
A2M	AdLib Tracker II Module
A2MENU	Aston 2 Menu
A2THEME	Aston 2 Theme
A3D/X	Amapi 3D model
A3P	Alice 3 Project
A3W	Unpackaged Authorware 3 for Windows file

Supported file type	Description
A3X	Autolt v3 compiled script
A4P/A5P	Authorware Packaged file (w/o runtime)
A4R/A5R	Authorware Packaged file (with runtime)
A4W	Apple II Oasis for Windows savestate
A5WCMP	Alpha Five Web Components
A78	Atari 7800 ROM
A8K	Atari800Win Plus Keyboard
A8S	Atari800Win Plus Snapshot (un-gzipped)
A8T	Atari800Win Plus Trainer
AA	Audible Audio
AA3	ATRAC3 encoded audio
AAC	Astrid/Quartex AAC encoded audio
AAE	Apple Sidecar data
AAM	Art And Magic module
AAS	Advanced Authoring System adventure
AAS/AOS	Archos signed / encrypted data
AAUI	Acrobat User Interface data
AAX	Audible Enhanced Audio
AB	Android adb backup (unencrypted)

Supported file type	Description
AB1/FSA	ABIF - Applied Biosystems Inc. Format
ABA	Palm Address Book
ABC	ABC FlowCharter document
ABCDP	Address Book CoreData Person
ABD	The Bat! Address Book
ABF	Altair Binary Format
ABR	Adobe PhotoShop Brush
ABS	AMOS Banks group
ABW	AbiWord document
ABY	AOL Address Book
AC	AC3D geometry/model
AC_	CaseWare 2005 Compressed file
AC1D	AC1D-DC1A Packer
AC2	Banana accounting data
AC3	Dolby Digital audio
AC3D	AC3D model
ACB	Adobe Photoshop Color Book
ACCDB	Microsoft Access 2007 Database
ACCDW	Microsoft Access Database Link

Supported file type	Description
ACD	ALAN game
ACDB	Audio Calibration DataBase
ACE	ACE compressed archive
ACF	DB/TextWorks Database Access Control
ACI	ACI development appraisal data
ACM	Infinity Engine Music
ACP	ArCon project
ACR	American College of Radiology file
ACS	Microsoft Agent Character
ACS2	AIMP Skin (v2)
ACS3	AIMP Skin (v3)
ACSM	Adobe Digital Editions Adobe Content Server Message
ACT	ADPCM (?) compressed file recorded by some MP3 Players/Voice recorders
AD	Anno Designer layout
AD_ASM	Alibre Design Assembly
AD_DRW	Alibre Design Drawing
AD_PRT	Alibre Design Part
AD1/E01/S01	AD Encrypted disk image

Supported file type	Description
ADA	Advanced Digital Audio compressed audio
ADB/NDB/GDB/PDB	HP Phone/Database/Note database
ADC	XemiComputers Active Desktop Calendar
ADCP	Adobe Device Central Project
ADF	ARIS Document File
ADF/ADFS/ADL	ADFS disk image
ADI/ADIF	Amateur Data Interchange Format
ADL	openEHR Archetype Definition Language
ADM	Addict compiled dictionary
ADML	Group Policy Language-Specific Administrative Template
ADMX	Group Policy Administrative Template
ADR	Opera Hotlist (v2.0) / bookmark
ADT	Advantage Data Server table
ADV	Advantage spreadsheet
ADX	ADX lossy compressed audio
AEF	CA Visual Object Application Export File
AEH	iPer Advanced Embedded Hypertext
AEM	STK Azimuth-Elevation Mask format

Supported file type	Description
AEP	After Effects Project
AERO	Aero Studio song
AES	AES Crypt encrypted
AF3	ABC FlowCharter chart
AFA	Astrotite compressed archive
AFB	AYFX Editor Bank
AFDESIGN	Affinity Design document
AFI	Advanced Floppy Image
AFL	X-Plane Airfoils
AFM	Outline Font Metric
AFP	ABC FlowCharter shapes Palette
AFT	ABC FlowCharter Template
AFW	ABC FlowCharter Workspace
AG	Applixware Graphic
AGR	Grace project file
AGTEMPLATE	Adobe Photoshop Lightroom template
AGX	Adventure Game eXecutable
AHX	Abyss' Highest eXperience module (v1)
AI	Adobe Illustrator graphics

Supported file type	Description
AIA	Adobe Illustrator Action
AIC	Advanced Image Coding bitmap
AIF	EPOC/Symbian Application Info
AIF/AIFF	AIFF Audio Interchange File Format
AIFC	AIFF-C (Audio Interchange File Format Compressed)
AIML	Artificial Intelligence Markup Language
AIMPPL	AIMP PlayList
AIN	AIN compressed archive
AIP	Actual Installer Project
AIR	Adobe Apollo Rich Internet Application (obsolete)
AIU	Advanced Installer Updates configuration
AJP	Anfy Applet Generator Saved file
AKM	Aksharamala Keymap Binary
AKP	Akai AKP format
AKS	AkAbak Script
AKT	AKT compressed archive
ALB	Seattle FilmWorks / PhotoWorks photo album
ALBM	HP Photosmart Photo Printing Album

Supported file type	Description
ALC/VLC	AcuCorp AcuCOBOL license
ALE	Avid Log Exchange
ALIAS	Find and Run Robot (FARR) alias
ALM	Aley's Module v1.0
ALN	Clustal Alignment format
ALP	AnyLogic Project
ALS	MPEG-4 ALS (Audio Lossless coding Standard)
ALTSTATE	Altirra save state
ALX	BlackBerry Application Loader
ALZ	ALZip compressed archive
AM	AmiraMesh (ASCII)
AMAD	AY Amadeus chiptune
AMB	Modular V preset
AMC	A.M.Composer 1.2 music
AMD	Amusic tracker (packed) song/module
AMF	Additive Manufacturing Format
AMG	AMGC compressed archive
AML	Abstract Markup Language

Supported file type	Description
AMOS	AMOS Pro source
AMR	AMR (Adaptive Multi Rate) encoded audio
AMS	Extreme's Tracker module
AMT	ABBYY Finereader language data
AMV	MTV Movie
AMW	Anark Media Workspace
AMXD	Ableton Max Patch
AMXX	AMX Mod X plugin
AN2	AceNotes PIM data
AN8	Anim8or project
ANA	Analysis for Windows structure
ANB	Project Dogwaffle Animated Brush
ANBM	IFF ANimated BitMap
ANC	Motion Analysis Corp. ANC format
ANE	Adobe AIR Native Extension
ANI	Atari NEOchrome animation
ANIM	ClariSSA Super Smooth Animation
ANIM/ANM	IFF ANIM (Amiga delta/RLE encoded bitmap animation)

Supported file type	Description
ANJUTA	Anjuta IDE project
ANK	Children of the Nile city
ANL	SimLife Animal
ANM	DeluxePaint Animation
ANM2	The Binding of Isaac: Rebirth animation
ANS	ANSYS model data
ANS/ASC	ANSI escape sequence text
ANTMPL	Adobe Edge Animate Template
ANY	AnyRail model railroad layout
AOF	Artlantis Object File
AOI	Art Of Illusion 3D scene
AOM	Adobe Download Manager
AON	Art Of Noise 4-channel module
AOS	AOS File Format
AP	ALICE: The Personal Pascal Program
APALBUM	Aperture Album
APC	Cryo Interactive APC audio
APCDOC	Ashampoo Photo Commander Document
APDISK	OS X system data

Supported file type	Description
APE	Monkey's Audio
APEX	AVM APEX sample studio sound bank
APF	MightyFax
API	Adobe Acrobat Reader Plugin
APJ	ARM Project Manager Project
APK	Android Package
APKG	Exported Anki Flashcard Deck
APL	ACDSee plugin
APL/APP	Team Developer / SQLWindows application (binary)
APN	APN Wallpaper
APNX	Amazon Kindle Page Number index
APP	APP raster bitmap
APP/DL	oZone GUI executable code
APP/IMG	PSION Application/Image executable
APPLICATION	ClickOnce Deployment Manifest
APPUP	Erlang Application Upgrade
APPX	Windows 8 App package
APPXBUNDLE	Windows 8.1 App Bundle

Supported file type	Description
APPXMANIFEST	Windows 8 Appx Package Manifest
APR	Apadana Project
APS	AProSys module
APT	Adaptive Prediction Tree (APT) encoded bitmap
APV	API Viewer Database
APXL	Apple Keynote Presentation data
AQM	AlpineQuest Map
AR	ACCReader document
AR/A/LBR	ar archive
ARC	EZBIND archive
ARC/SZS/YAZ0	Nintendo Yaz0 compressed data
ARCH00	F.E.A.R. game archive
ARDUBOY	Arduboy game package
ARE	Infinity Engine Area (v9.1)
AREN	Advanced Renamer method
ARF	Active Tutor data
ARFF	Attribute-Relation File Format
ARGO	ArgoUML project

Supported file type	Description
ARH	Squash compressed archive
ARI	ARRIRAW image
ARJ	ARJ compressed archive
ARK	DS Squeeze archive
ARL	Aureal Aspen sound bank
ARMODEL	Kudan AR Model
ARP	Audition Play Data
ARPBANK	ARP2600V preset
ARQ	ARQ archive
ARS	Carmageddon Saved Game
ARSC	Android Package Resource
ART	AOL ART (Johnson-Grace compressed) bitmap
ARTASK	Remedy User Tool shortcut
ARTBORDER	ArtBorder data
ARW/SR2	Sony digital camera RAW image
ARX	ARX compressed archive
AS	Applix spreadsheet
AS2PROJ	FlashDevelop ActionScript 2 Project

Supported file type	Description
AS3PROJ	FlashDevelop ActionScript 3 Project
ASAR	asar Electron Archive
ASC	ASCII Encoded HP 48 Object
ASC/AEXPK/PGP/PUB/TXT	PGP public key block
ASC/PGP/TXT	PGP message
ASC/TXT	PGP clear text signed message
ASCX	Microsoft ASP.NET Web User Control
ASD	ASD Archiver compressed archive
ASDATABSE	Microsoft SQL Server Analysis Services project
ASE	3D Studio Max ASCII Export file
ASE/ASEF	Adobe Swatch Exchange File
ASF	Acclaim Skeleton File
ASF/STR	Electronic Arts ASF video (generic)
ASH	ASH compressed data
ASHPRJ	Ashampoo Burning Studio project
ASK	askSam Windows database
ASLX	Quest Adventure Script
ASM	Solid Edge Assembly Document
ASN	Atlantis Word Processor Sound Scheme

Supported file type	Description
ASPX	Microsoft ASP.NET Web Form
ASS	SubStation Alpha Subtitle (Unicode)
ASS/SSA	SubStation Alpha Subtitle
ASSET	Unity YAML Scene
AST	'Need for Speed: Underground' soundtrack
ASVF	Asphyre Sphinx Archive File
ASX	Advanced Stream Redirector
ASY	LTSpice Symbol
ATA	Antenna project
ATDF	ASCII Test Data Format
ATF	ATF Texture
ATH	Alienware AlienFX Theme
ATHTUNE	athtune script
ATL	Artlantis 3D scene (gen)
ATM	TerraGen Light and Atmosphere
ATN	Photoshop Action
ATP	ATRAC encoded audio
ATR	Atari ATR disk image
ATT	Calamus ASCII Translation Table

Supported file type	Description
ATTR	iPhoto image data
ATX	VAPI/ATX Atari 8-bit disk image
AU	Audacity audio block
AUD	INRS-Telecom audio (10KHz)
AUM	Adobe Update Manager data
AUP	Audacity project
AUR	AutoREALM Map
AUS	AutoREALM Symbols
AUTOMATICDESTINATIONS-MS	Windows 7 Jump List
AUTOPLAY	AutoPlay Media Studio Project
AVASTSOUNDS	Avast! Soundpack
AVB	Avid Editor Bin
AVC	Kaspersky Anti-virus data base
AVF	AVF video
AVI	AVI Audio Video Interleaved
AVJ	AntiVir Job
AVL	Avira AntiVir Log status report
AVP	AntiVir Profile
AVRO	Avro serialized data

Supported file type	Description
AVS	Winamp Advanced Visualization Studio File
AW	Microsoft Answer Wizard
AWD	Artweaver Document
AWL	AWL programming language (Var. 1)
AWLIVE	Active WebCam live capture
AWM	AllWebMenus project (v2.xx)
AWS	Ability Office Spreadsheet
AWSES	Active WebCam Settings
AX	DirectShow filter
AXE	AutoRoute Export file
AXF/BIN/GXB	GP32 eXecutable Binary
AXP	Avid / Pinnacle Studio Project
AXS	AXS module
AXT	ZenWorks snAPPshot ASCII Application Object Template
AXX	AxCrypt encrypted
AY/EMUL	AY chiptune
AYL	Ay Emul play List
AYM	Z80 music code with AY music

Supported file type	Description
AYS	Ay Emul Skin (v2.0)
AZA	QazaR compressed file
AZF	AirZip FileSECURE format (print quality)
AZW	Amazon Kindle eBook
AZW1/TPZ	Kindle Topaz eBook
AZW3	Amazon Kindle KF8 eBook
AZZ	AZZ Cardfile card
BAK	Microsoft SQL Server backup
BAL	B4A Layout
BALZ	BALZ compressed data
BANK	FMOD 5 Sound Bank
BAR	Total Commander button Bar config
BAS	BAS VBDOS Pro 1.0 Source
BASIN	HEC-HMS Basin model settings
BATTLE	Robocode Battle
BAV	The Bat! Antivirus plugin
BAW	BrainLED AlfaWave session
BB	Artlantis Billboard
BB/BIGBED	bigBed Track Format

Supported file type	Description
BBL	BibTeX Generated Bibliography
BBSONG	Beepola chiptune
BBX	BrainBox neural net
BC	Big Crunch compressed file
BCIF	BCIF bitmap
BCK	BackupExpress Pro
BCO	Bitstream Compressed Outline font
BCKPKG	Beyond Compare Settings Package
BCS	BCS Video
BCT	Adobe Bridge cache
BCW	BusinessCards MX project
BD	Benn Daglish chiptune
BDC	Babylon Dictionary
BDF	Brother Embroidery File
BDL	Grid 2 Bundle
BDOC/ASICE	Binary Document container
BDR	Microsoft Border art
BDS	Benn Daglish SID chiptune
BDSPROJ	Borland Developer Studio Project

Supported file type	Description
BEAM	Compiled Erlang code
BED	UCSC BED Annotation Track
BEE	The Bee Archiver compressed archive
BFA	Blowfish Advanced CS encrypted
BFA/TMP	BigFix File Archive
BFF	AIX Backup File Format
BFI	Brute Force and Ignorance video
BFLI	Big Flexible Line Interpretation bitmap
BFX	Bitware BitFax page(s)
BGA	OS/2 Bitmap Graphics Array (generic)
BGDB	Global Virtual Accademy e-learning file
BGI	Borland Graphics Interface driver (v2.x)
BGL	Babylon Glossary
BH	BlackHole compressed archive
BHF	PCAnywhere32 Data
BHL	BlockHashLoc recovery info
BHO	Behold Organize data
BHW	Blophome published project
BIB/BIBTEX/TXT	BibTeX references

Supported file type	Description
BIDULE	Bidule layout
BIF	BIF bitmap ASCII info
BIG	SGA archive - Home World 2 game data
BIG/VIV	VIV/BIGF Electronic Arts Game Archive
BIK	Bink video
BIK/BIK2/BK2	Bink2 video
BIN	AVG update package
BIN/BLI	Thomson Speedtouch serie WLAN router firmware
BINDS	Elite: Dangerous controls bindings
BINVOX	BINVOX voxel file format
BIO	BioArk compressed archive
BIP	KeyShot 3D scene
BIX	BIX Archiver compressed archive
BIZ	Division dVS 3d model
BK2	BizHawk movie capture
BKF	Windows NTBackup archive
BKG/GUL	Samsung document
BKI	IBM Softcopy Reader (Bookmanager) Bookshelf (and Book) index file

Supported file type	Description
BKM	BizHawk movie capture (obsolete)
BKR	ReplaceEm fileset
BKRIFF	Brass preset
BKS	IBM Softcopy Reader (Bookmanager) book file
BLB/BLORB/GBLORB/GLB/ZBLORB/ZLB	Blorb interactive fiction package
BLD	3D Home Design Suite model
BLEND	Blender 3D data
BLI	BLINK compressed archive
BLIF	Berkeley Logic Interchange Format
BLOB	Cosmic Blobs model
BLP	Blizzard Picture (type 1)
BLSC	Blue Scan drawing
BLT	Saved AIM Buddy List
BLU	Apple Binary 2 Library Utility archive
BLUE	EVE Online data (generic)
BLUEJ	BlueJ Package
BLZ	BriefLZ compressed data
BMA	BMA Archiver compressed archive
BMD	Nintendo GameCube/Wii 3D Model

Supported file type	Description
BMF	BMF v1.x bitmap
BMFC	AngelCode Bitmap Font Generator Configuration
BMG	Message string storage
BMM	Beeper Music Maker music
BMML	Balsamiq Mockups prototype
BMP	Alpha Microsystems Bitmap
BMP/EPA	Award BIOS logo bitmap (v2)
BMS	QuickBMS script (with XML header)
BMSK	STK Body Mask format
BMU	Aurora Engine BioWare Music Unit (v1.0)
BMX/BMW	Buzz song
BND	DB2 Bind File
BNDL	Need For Speed Bundle
BNK	Adlib instruments/sound bank
BNR	BannerMania banner
BNZ	bonZai3d project
BOA/B**	BOA Constrictor Archiver compressed archive
BOM	Bill Of Materials

Supported file type	Description
BONK	Bonk compressed audio
BOOK	FrameMaker book
BOOTSKIN	BootSkin Vista theme
BOT	Soldat Bot Information
BP	BP SoundMon 2 module
BP3	BP SoundMon 3 module
BPD	Buero Plus NexT FlashFiler database file
BPF	Binary Point File 3
BPG	Better Portable Graphics bitmap
BPL	Borland Package Library
BPM	Bizagi Process Modeler document
BPP	BPP bitmap
BPR	C++ Builder XML Project
BQY	BrioQuery
BR6	Bryce 6 Scene
BRAINZIP	PersonalBrain document
BRC	BlueCielo Meridian BriefCase - File Archive Library (v1.00)
BRD	BorderMaker project

Supported file type	Description
BREP	Open Cascade Technology 3D model
BRN	Gabriel Knight 3 barn game data
BRP	BRender BRP
BRRES	Mario Kart Wii BRRES model data
BRSTM	BRST Audio Stream
BRT	BeRoTracker module
BS	Infinity Engine compiled character Script
BS/BIN	PrintFox (C64) bitmap (RLE encoded)
BS4	Mikogo session video recording
BSB	MapInfo Sea Chart
BSC	BinSCII encoded file
BSDIFF	bsdiff patch
BSDL	Boundary Scan Description Language
BSG	Besiege machine
BSI	Future Composer (BSI) module
BSN	BSA Packing program compressed archive
BSS	Beethoven Synthesizer module
BSX	BrickStore XML data
BT	BluffTitler Show

Supported file type	Description
BTAPP	uTorrent Application
BTD	Power To-Do List Data
BTG	Binary TerraGear - FlightGear scenary data
BTPC	BTPC encoded bitmap
BTR	FrontPage Binary-tree index
BTSEARCH	BitTorrent Search engine specification
BTW	BarTender label format
BTX	DB/TextWorks Database Term and Word Index
BUNDLE	Krita resource Bundle
BUZ	Buzzic 1.x module
BUZ2	Buzzic 2 module
BVH	Motion Capture File
BVY	Breevy text snippet
BW	Silicon Graphics B/W bitmap
BWE	Black and White 2 Environment data
BWG	BrainWave Generator
BWS	Photo Enote (Enot) external photo viewer settings
BWW	Bagpipe notation

Supported file type	Description
BX	BX Embrilliance font
BXB	BasicX compiled bytecode
BXL	Accelerated Designs PCB Library
BXU	PictureGear Studio file
BXY	NuFX archive (with Binary II header)
BZ	BZIP compressed archive
BZ2/BZIP2	bzip2 compressed archive
BZA	BZA compressed archive
C10	Virtual MC-10 tape image
C3	3D model
C32	Syslinux COM32 module (generic)
C3D	Chem3D Format
C3XML	Chem3D XML format
C4*	Clonk game data
C4D	CINEMA 4D model (generic)
C4M	Clonk Material definition
C64	CCS64 Freeze saved state
CA1	Crack Art bitmap (low-res)
CA3	Crack Art bitmap (hi-res)

Supported file type	Description
CAB	InstallShield compressed Archive
CAD	CadStd drawing
CAF	Cal3D Animation File
CAG	Capella gallery data file
CAI	SeeYou flight data
CAJ	CAJ database
CAKEWALKSTUDIOWARE	Cakewalk Studio Ware panel
CAL	Microsoft Project 4.0 for DOS Calendar
CAL/CALS	CALS raster bitmap
CAMM	Crystal Alien Map Maker project (INI)
CAMPROJ	Camtasia Studio Project
CAMREC	Camtasia Studio Screen Recording
CAP	Capella sheet data file
CAPROJ	Construct 2 Project
CAPX	Construct compressed game project
CAPX/CAPXML	Capella CapXML music notation
CAQ	Aquarius Cassette tape image
CAR	Atari Cartridge
CAS	Atari Cassette tape image

Supported file type	Description
CAT	Elcomsoft ADC Advanced Disc Catalog
CATALOG	Amiga Catalog translation format
CATDRAWING	CATIA Drawing (generic)
CATPART	CATIA Part Description (generic)
CATPRODUCT	CATIA Assembly (v5 r16)
CAZ	CAZIP compressed file
CBA	Chuck Biscuits/Black Artist module
CBC	Clam Antivirus ByteCode signatures
CBCX	Comic Book Creator document
CBDS	Comic Book DS
CBF	CoffeeCup Button Factory button
CBMPRJ	CBM prg Studio Project
CBOARD	Final Cut Pro X Color Board preset
CBP	Code::Blocks Project
CBPROJ	Borland C++ Builder project
CBS	Codebreaker save
CBV	ChessBase Archive file
CBXML	CodeBox snippet library
CC3D	CompuCell3D project

Supported file type	Description
CCA	Multimedia Fusion - Click'n'Create file
CCB	CocosBuilder info
CCBI	CocosBuilder exported info
CCC	TeslaCrypt/Cryptowall encrypted
CCD	Elaborate Bytes/SlySoft CloneCD CDImage (description)
CCF	Component Configuration File (generic)
CCM	Creative Commons Module music
CCPROJ	Visual Studio Cloud service project
CCRF	Saba Centra Recording Studio recording
CCS	CableNut Custom Settings
CCT	Calamus Codepage Table
CCVF	CompuColor Virtual Floppy disk image
CD	Class Diagram (UTF-8)
CD5	Chasys Draw IES drawing
CDA	CD Audio track shortcut
CDB	CodeSuite DataBase - BitMatch
CDCOM	Circuit Diagram Component (compiled)
CDD	Cadifra Diagram

Supported file type	Description
CDDS	Midtown Madness 3 data
CDE	MicroHof Code
CDF	Affymetrix Chip Definition File (Text)
CDF/NC	NetCDF Network Common Data Form
CDF-MS	ClickOnce Compiled Manifest
CDK	Calamus Document
CDM	NTI CD Maker image file
CDO	Crescendo Music Notation score
CDPZ	ConceptDraw Project document (Zipped)
CDR	CorelDRAW drawing (zipped)
CDRZIP	DICOM Images zipped archive
CDS	Borland Client Dataset data
CDV	Javelin Country Driver
CDW	CeledyDraw drawing
CDX	CDX Internet Archive index
CDXL	Amiga CDXL video (Std, HAM, bit planar)
CDXML	ChemDraw XML
CDZ	pSX compressed CD image
CE1	

Supported file type	Description
	ComputerEyes Raw Data Format low-res bitmap
CE2	ComputerEyes Raw Data Format hi-res bitmap
CEB	Apabi eBook
CED	EEGLAB Channel Data
CEG	Continuous Edge Graphic bitmap
CEL	Affymetrix Probe Results (Bin)
CER	Internet Security Certificate
CER/MSI	MSI/Accelrys Cerius II
CF1	Common Loudspeaker Format binary (v1, Type 1)
CF2	Common Loudspeaker Format binary (v1, Type 2)
CFDG	Context Free design grammar
CFF	BoomTracker 4.0 module
CFG	Ableton project configuration
CFL	Compressed File Library 3 compressed data
CFM	ColdFusion Template
CFML	ColdFusion Markup Language
CFN	Calamus Font Data

Supported file type	Description
CFOSSPEED	cFosSpeed registration key
CFP	CoverFactory Project
CFT	CFast Animation
CGC	Colour Genie high level tape image
CGM	Computer Graphics Metafile (Clear Text)
CGP	DVDFab Change Graphic Picture
CGR	Quest3D data
CGT	GOLD Parser Tables
CGX	CommonGraph format
CH3	Harvard Graphics Chart (v3.x)
CHAIN	Chain format
CHART	MacStitch/WinStitch design
CHESSTITANSSAVE-MS	Microsoft Chess Titans Saved game
CHI	ChiWriter document (v3.x or older)
CHK	PolySpace check results
CHL	Black and White 2 game data script
CHM	Windows HELP File
CHN	ApBasic Chain file/module
CHORDS	SuperJAM! Chords

Supported file type	Description
CHR	BGI (Borland Graphics Interface) font
CHT	Harvard Graphics Chart (v2.x)
CHT/SCT	SPSS template
CHZ	ChArc compressed archive
CI	CyberTracker Instrument
CIF	BoomTracker 4.0 instrument
CIL	Clip Gallery Download Package
CINE	Phantom Cine video
CINEMA4D	Cinema 4D project
CIP	Cisco IP Phone Image bitmap
CIRC	Logisim Circuit
CIRCUIT	KTechlab circuit design
CISO/CSO/WBI	CISO Compressed ISO CD image
CIV5MAP	Civilization 5 Map
CIV5PROJ	Civilization 5 Project
CIV5SAVE	Civilization V saved game
CIV5SLN	Visual Studio Civilization 5 Solution
CKBX	Cricket Audio XML Bank Description
CKD	Cadkey Design file

Supported file type	Description
CKF	Casio Keyboard File
CKT	CircuitMaker schematic
CL2	Hy-Tek Meet Results
CL2ARC	Comic Life 2 Archive
CL4	Easy CD Creator 4 Layout
CL5	Easy CD Creator 5 Layout
CLA	CLASS336 Markup Language
CLASS	Java bytecode
CLB	COM+ catalog file
CLBX	MP3 Automagic CD Cover Creator label
CLF	ListPro data
CLG	Collage Maker document
CLIPS	Programmer's Notepad text Clips
CLK	ClickFORMS data
CLKX	Crick Software Clicker File
CLMOV	Clan Lord movie - Visiostone
CLO	SPSS Chart Look
CLP	DeskMate clipart
CLPI	Blu-ray Clip AV stream

Supported file type	Description
CLR	3ds UI colors
CLS	Visual Basic class definition
CMA	OCaml bytecode (library)
CMAP/PAL/IFF	IFF Color Map
CMATE	ControllerMate programming
CMB	Reason Combinator Instrument Patch
CMBL	Vernier Logger Pro data
CMC	Comic Collector Collection data
CMD5	CrystalMaker Data format (v5-6)
CMD5/CMD5/CMMF	CrystalMaker Data format (generic)
CMD5	CrystalMaker Data format (v2-4)
CML	Chemical Markup Language
CMML	Continuous Media Markup Language
CMP	AUKTOOLS 2000 compressed archive
CMPROJ	Channel Master Project
CMR	SeeYou Raster Map
CMS	Creative Music System music
CMU	CMU Window Manager bitmap
CMV	Corel Movie animation

Supported file type	Description
CMX	Corel Metafile Exchange Image (Legacy)
CMZ	Compressed archive
CN	Copy Numbers format
CNC3REPLAY	Command and Conquer 3 replay
CNDF	Compressed Channel Data File
CNF	Lotus 123 configuration (V1)
CNT	Help File Contents
CNV	DB2 Conversion File
CO	Cult3D object
COB	Caligari TrueSpace Object
COD	Atlantis Word Processor encrypted document
COD/LOD	Microsoft p-code (Multiplan)
COK	Cookeo recipe
COL	Grand Theft Auto 3 collision data
COM	16bit COM executable BAT2EXEC v1.3
COMFYCAKESAVE-MS	Comfy Cakes saved game
COMICDOC	Comic Life Document
COMICLIFE	Comic Life Document
COMPANYLOGO	CompanyLogoDesigner project file

Supported file type	Description
COMPILED	Flare3D Shader Language Compiled
COMPOSITEFONT	Windows Composite Font
COMX	COMX-35 program
CONF	fswebcam configuration
CONTACT	Windows Contact
CONTROL	HEC-HMS Control specifications data
COOKIE/TXT	libwww-perl cookie_jar
COP/ET/ETC/T	E-Tracker chiptune
COR	WinArcadia Recording/macro
CORE	Core Design module
COS	WinArcadia Saved State
COW	Copy On Write disk image
CP2	PSFTools CodePage map
CPC/CPI	Cartesian Perceptual Compression Image bitmap
CPE	Windows FAX cover
CPF	Canon EOS Custom Picture Profile
CPG	Cool Page Project
CPH	Corel PrintHouse image

Supported file type	Description
CPI	AVCHD Clip Information
CPIO	CPIO archive (binary)
CPJ	WinOnCD Project
CPK/CAK/FILM	Sega CPK video
CPL	Corel Color Palette
CPR	CPC Plus Cartridge image
CPS	Corel PhotoHouse image
CPT	Corel Photo Paint bitmap (new)
CPX	Atari Control Panel applet
CPX/FLT	ImgStar bitmap
CR2	Poser character rigging
CRAFT	Kerbal Space Program (KSP) spacecraft
CRASH	Mac OS X crash log
CRD	PPC Organiser Card
CRE	Infinity Engine Creature (generic)
CRF/CCRF/PRN	Calcomp raster bitmap
CRG	Calamus Raster Graphic bitmap
CRI	Calamus Raster Information
CRP	Colossal Raw asset Package

Supported file type	Description
CRPLUGIN	ComicRack plugin
CRS	StepMania Course
CRT	C64 Cartridge image
CRU	Crush compressed archive
CRV	Corel PhotoPaint Tone Curve
CRV3D	Vectric Aspire 3D drawing
CRW	Canon RAW format
CRX	Google Chrome Extension
CRYPT7	WhatsApp encrypted database
CRYPTOMITE	CryptoMite encrypted
CRYSISJMSF	Crysis saved game
CRYSISPSF	Crysis Warhead saved game
CS	ColorSchemer Studio Color Scheme
CS0	Callus savestate
CSAPLAN	SPSS Analysis Plan
CSCFG	Azure Service Configuration Schema
CSCHEME	Caffeine Scheme
CSD	Cabbage script
CSDEF	Azure Service Definition schema

Supported file type	Description
CSDL	ADO.NET Conceptual Schema Definition Language
CSF	Cal3D Skeleton File
CSH	Adobe Photoshop Custom Shape
CSM	CASL compiled PalmPilot program
CSO	DirectX Compiled Shader Object
CSP	AudioZip encoded audio
CSPLAN	SPSS Sampling Plan
CSPROJ	Visual Studio C# Project
CSS	Cartoon Studio Script
CSV	Weather Analytics data
CSW	Compressed Square Wave (v1.1)
CT	Cheat Engine Cheat Table
CTB	AutoCAD Color-Based Plot Style
CTD	CherryTree note (XML)
CTF	WhereIsIt? catalog file
CTG	Canon Photo Info file
CTI	Bitz and Pixels XML (ASCII)Report Template Info for collectorz.com products
CTL	Phoenix Visual Designer third party control

Supported file type	Description
CTM	OpenCTM 3D mesh
CTP	CrazyTalk Project
CTS	TreeSheets project
CTT	MSN Messenger Saved Contact List
CTW	Context tree weighing (CTW) compressed file
CTX	Gasteiger group CTX
CTXT	BlueJ Class Context
CUB	Isis Cube data
CUBE	Gaussian Cube data
CUE	ISO CDImage cue/description - Data
CUEPROFILE	Corsair Utility Engine Profile (v2)
CUI	AutoCAD Custom User Interface
CUR	Windows Cursor shape
CURSORFX	CursorFX theme
CURXPTHEME	CursorXP theme
CUS	Delitracker Customplay module
CVA	Compaq Diagnostics
CVC	Cybiko Video Container video
CVD	Calamus Vector Document

Supported file type	Description
CVF	Jet-VoiceMail audio data
CVG	Calamus Vector Graphic
CVP	WinFax Cover Page
CVS	Satori Paint Canvas
CVT	GEOS ConVerT container format
CVX	Covox ADPCM encoded audio
CWD	Cardwar Cards deck
CWK	Claris Works document
CWP	Cakewalk SONAR project
CWR	WrapCandy template
CWS	Combustion v2 Workspace project
CWW	Crossword Weaver puzzle
CWY	SongTrix Style
CXF	CTXf compressed archive
CXI	Coherent X-ray Imaging format
CXT	Adobe Director Protected Cast
CYG	CryoGen ECC data
CYP	Crocodile Physics Simulation
CZD	Crash Zone Drawing

Supported file type	Description
CZIP	ZipGenius encrypted compressed archive
DAT/FH11	Freehand 11 Project
DAT/LOG	LabVIEW binary Datalog
DAT1	NeoRAGEx savestate
DATA	RHVoice data
DATABASE	SQL Server Data Tools Database info
DATATYPE	Amiga Datatype
DAV	Dahua DVR video
DAX	DAKX compressed audio
DAZIP	Dragon Age: Origins game data
DB	Everything index
DB/DIGI	DIGIBooster module
DB_INFO	Quartus DataBase Info
DB3	SeqBox SBxScan recovery info
DBA	DateBook Archive
DBB	Skype user data
DBD	Dan Bricklin's Demo 2 demo
DBF	Psion serie 3 Database
DBG	ASIC compiler debug info

Supported file type	Description
DBH	PC-File database header
DBI	Isearch Database Info
DBK	Orcad Schematic Capture Backup
DBK/XML	DocBook document
DBM	DigiBoosterPro module
DBO	DB/TextWorks Database Directory
DBR	DB/TextWorks Database
DBS	DB/TextWorks Database Textbase Structure file
DBX	Outlook Express Database
DC	DeltaCad drawing
DC3	Diamond Caves 3 levels group
DC42/IMAGE	DiskCopy 4.2 1440k MFM disk image
DC5	DataCAD Drawing
DCA/RFT	IBM Document Content Architecture / Revisable Form Text
DCD	DCD binary trajectory format
DCE	DriveCam video
DCF	D-LIB bytecode (generic)
DCH	DipTrace Schematic

Supported file type	Description
DCM	KiCad Documentation
DCM/DIC/DICOM	DICOM medical imaging bitmap
DCOL/IFF	IFF Direct Color bitmap
DCR	Director - Shockwave movie
DCU	Borland Delphi 6 Library
DCUPDATE	DcUpdater local configuration
DCX	Graphics Multipage PCX bitmap
DD2	Dave 2 Huffman compressed game data
DDD	ColdFusion Verity engine fields definition
DDF	GEM Driver Definition
DDOC	DigiDoc digital signature
DDP	Delphi Diagram Portfolio
DDS	DirectX DirectDraw Surface
DDT	Diagram Designer Template
DDY	ASHRAE Design Conditions Design Day data
DEB	Debian Linux Package
DEEP	IFF DEEP animation/bitmap
DEH	DeHackEd patch
DEM	Half-Life 2 Demo

Supported file type	Description
DEPEND	Code::Blocks Dependencies
DEPLOYPROJ	Deployment Manager configuration
DEPOT	HP-UX Software Distributor catalog depot
DER	DER encoded X509 Certificate
DES	GRAFIT layout
DESC	Battlefield 2 map Description
DESKTHEMEPACK	Windows 8-10 Desktop Theme Package
DESKTHEMEPACK/THEMEPACK	Windows Desktop Theme Package
DESKTOP	KDE/GNOME desktop entry
DESKTOP/DXTHEME	DesktopX Theme
DEV	Bloodshed Dev-C++ project
DEVELOPERPROFILE	Xcode Developer Profile
DEVELVE	Develve data
DEX	Dalvik Dex class
DF1	Omnis Studio database
DFA	DreamForge video
DFD	ATK Data Flow Diagram
DFF	DSD Interchange File Format audio
DFM	Borland Delphi - C++ Builder Form (var.1)

Supported file type	Description
DFONT	Macintosh OS X Data Fork Font
DFT	Solid Edge Draft Document
DFU	Device Firmware Upgrade format (generic)
DFW	Derive for Windows (generic)
DFXML/XML	Digital Forensics XML
DFXP	Distribution Format Exchange Profile
DGC	DGCA Digital G Codec Archiver
DGML	Directed Graph XML document
DGN	Bentley MicroStation CAD drawing
DGR	PhoneTools Internal Graphic Format
DGS	Dagesh document
DH	David Hanney chiptune
DI	XL/ST link / XLDJ Disk Image
DIA	Dia drawing (uncompressed)
DIAGCAB	Diagnostic Cabinet
DIC	Kingsoft PowerWord Dictionary
DIG	Sound Designer I (Mac) audio
DII	Summation Document Image Information Load File

Supported file type	Description
DIN/BIN	DESI-III drawing
DIP	DipTrace PCB
DIS	DRI Display Manager Display
DIT	Studio Printer Dither method
DITA	DITA document
DITAMAP	DITA map
DJR	Macromedia Director Java Resource - Video
DJVU/DJV	DjVu (gen)
DJX	Fluid Entertainment Dundjinni - included Art
DL	Dave Lowe module
DLC	DLC - DIGILINEAR compressed archive
DLDI	Dynamically Linked Device Interface
DLG	Infinity Engine Dialogue (v1.0)
DLIS	Digital Log Interchange Standard well format
DLL	ATI The Compressorator plugin
DLS	Downloadable Sound bank
DLT	DELTA binary dataset
DM	Delta Music module
DMB	BYOND game byte-code executable

Supported file type	Description
DMD	Oracle SQL Developer Data Model
DMF	D-Lusion Music Format module
DMG	Macintosh Disk image (BZ2 compressed)
DMI	DMIS input data
DMK	TRS-80 DMK 5"1/4 DD disk image
DMM	DropMind Mind Map
DMP	DC2N DMP format (v0)
DMP/MDMP	Windows Minidump
DMSD	VideoWave DVD Project
DMT	DeLorme Street Atlas Map Transfer
DMU	Digital Mugician module
DMX	Data Model eXchange encoding format
DMZ	DMesh 3d model
DNH	Touhou Danmakufu script
DNL	DNL eBook / eCatalog / eCard / eBrochure
DNM	YS FLIGHT Dynamic 3d model
DNP	Eudemons Online game data
DOC	Better Working Eight-In-One Document
DOC/DCX	Microsoft Word for DOS Document

Supported file type	Description
DOC/ST	1ST Word Plus Document
DOC/WS	WordStar document (gen)
DOC/WS2	WordStar 2000 document
DOC/WS5	WordStar 5 document
DOC/WS7	WordStar 7 document
DOCKERFILE	Dockerfile
DOCM	Word Microsoft Office Open XML Format document (with Macro)
DOCX	Word Microsoft Office Open XML Format document
DOCZIP	dockzip format
DOF	Delphi Options File
DOTFUPROJ	Visual Studio Dotfuscator Project
DPAL	Dragon UnPACKer color Palette
DPD	Ovation Pro document
DPK	Delphi Package
DPL	Borland component
DPLSAVE	Driver: Parallel Lines savegame
DPR	Delphi Project source
DPROJ	Delphi Project

Supported file type	Description
DPS	DivX Skin
DPT	Kingsoft Presentation template
DPW	Decision Pad Worksheet (v2.x)
DPX	Digital Moving Picture Exchange bitmap (big endian)
DR	Open Digital Rights Language
DR2D/IFF	IFF 2-D Object standard format
DRC	Dirac video
DREAM	Stardock's DeskScapes animated wallpaper
DRF	Dynojet Run File
DRG	AllyCAD Drawing
DRL/DLP	Drazlace bitmap
DRN	DRAKON Editor diagram
DRO	D-Robots robot
DROID	Droid profile
DRPM	Delta RPM Package
DRR	Altium Designer Drill Report
DRU	EAGLE Design Rules
DRV	Javelin screen Driver

Supported file type	Description
DRW	CADS Planner drawing
DRW/DSF	Micrografx Designer Drawing (v3.1)
DRX	DaVinci Resolve eXchange data
DRY	PPC Organiser Diary
DRZ	Drazpaint (C64) bitmap
DS	Furcadia DragonSpeak Script
DS_STORE	Mac OS X folder information
DS1/DS4	DeSmuME savestate (gen)
DS2	Dream Station 2.0 module
DS4	Micrografx Designer Graphics (ver 4)
DSA	DAZ Studio script
DSE	Dyalog APL Session
DSF	DSD Storage Facility audio
DSF/MINIDSF/DSFLIB	Dreamcast Sound Format
DSG	Doom SaveGame
DSK/CPY/CQM	CopyQM disk image
DSK/DTK	TI-99 PC99 Track Dump Format
DSK/IMG	CP Backup disk image
DSK/TIDISK	TI-99 V9T9 Sector Dump Format

Supported file type	Description
DSM	DeSmuME Movie capture
DSN	ISIS Schematic file
DSP	MS Developer Studio Project
DSPACKAGE	Desktop Sidebar skin
DSR	Visual Basic Active Designer file
DSS	Digital Sound Studio module
DST	AutoCAD Sheet Set
DSW	Microsoft Developer Studio Workspace
DSX	Vivid DiffSet
DSYM	Digital Symphony relocatable module
DTB/DTBO	Device Tree Blob/Overlay
DTC	Weresc CADE drawing
DTD	TechSoft 2D Design drawing
DTF	Symantec QandA Database File
DTG	Desktop Guitarist music score
DTM	Digital Tracker 1.9 module
DTM/MBM	Digitrax module
DTP	PDP-8 DECTape tape image
DTPROJ	SQL Server Data Tools Project (ASCII)

Supported file type	Description
DTQ	Visual Database Tools Query
DTS	DTS encoded audio
DTSCONFIG	SQL Server Integration Services Configuration
DTSX	SQL Server Integration Services package
DTYP	dtread Type Descriptor
DUC	Action Replay Saved gamestate
DUMP	SVN dump format (generic)
DUR	DURILCA compressed file
DV	Digital Video
DVB	AutoCAD VBA macro
DVDS	DVDStyler Project
DVF/MSV	Sony Compressed Voice File
DVG	GraphicWorks Vector Drawing
DVI	Device Independent Document (TeX/LaTeX compiled)
DVMS/VMS	Variable Slope Delta Modulation audio
DVR	DVR-Studio stream
DVR-MS	Microsoft Digital Video Recording
DVTCOLORTHEME	Xcode Color Theme

Supported file type	Description
DWA	Project Dogwaffle animation (generic)
DWD	DiamondWare Digitized audio
DWF	Autodesk Design Web Format
DWFX	Design Web Format XPS
DWG	AutoCAD 2000-2002 Drawing
DWG/PCB/SCH	CIRCAD data (v3.x)
DWI	Dance With Intensity song
DWL2	AutoCAD drawing lock
DWP	DarkWave Studio module
DWS	Dyalog APL WorkSpace
DWZ	Ulead DVD MovieFactory project
DXA	DXA video
DXE	AutoCAD Data Extraction template
DXF	AutoCAD Drawing eXchange Format (binary)
DXG/CFG	Doxygen configuration settings
DXLS	DashXL Dashboard
DXM	DXM music
DXP	CDBurnerXP Data compilation
DXR	Macromedia Director Protected Movie (MAC)

Supported file type	Description
DXS	DeleD scene
DYF	Audio DiffMaker file set
DYL	Psion Library
DYN	Dynamo program
DZ	Darius Zendeh module
DZPRJ	Deep Zoom Composer Project
E	STK Ephemeris format
E00	ArcInfo interchange format
E01	Expert Witness compression Format disk image
E24	Bitmapped Signum!2 printer font (screen)
E2P	PonyProg device file
E3	Emulator 3000 snapshot (binary)
E4XMI	Eclipse 4 Application Model Info
E57	LIDAR Point Cloud data
EAR	Java Enterprise Archive
EASM/EPRT	eDrawings part (v 2008)
EBC	Compiled MediaBasic Project
EBF	Efficient and Easy to use Binary Format

Supported file type	Description
EBK/SAL/SCL/SLS/SME/SMEA/SPB/SPBA /SSC/SSM/SSN/SWI/SWP	Samsung Kies backup
EBO	Microsoft Reader eBook annotations
EBS2	E-Run 2.0 Script
EBUILD	Gentoo Linux ebuild package
EBX	Electronic Book Exchange
ECF	Embird Cross stitch Format
ECLIPSEPRODUCT	Eclipse product marker
ECP	EasyC Project
ECW	EclipseCrossword CrossWord
ED2K	eDonkey network download link
EDAT2	E-DataAid 2.0 data
EDB	ETABS model
EDB/SDB/STM	Extensible Storage Engine DataBase format
EDG	EDGE Diagrammer diagram
EDGE	Adobe Edge Project
EDI	UN/EDIFACT
EDMX	Entity Data Model
EDN	EDIF Netlist

Supported file type	Description
EDOC	Electronically certified Document
EDX	EDraw Max drawing
EED	EEDraw Drawing
EFE	Ensoniq EPS family instrument
EFF	Infinity Engine Effect (v2.0)
EFG	Gambit Extensive Game File Format
EFP	SilkRoad effect
EFT	ChiWriter high resolution screen font
EFX	j2 Global Communications eFax
EGG	EGG compressed archive
EGISENC	egis encrypted data
EGLIB	Adobe Edge Animate Library
EGON	Egon animation
EGR	EGrid32 Form
EGRP/EOBJ/ECHR	Explorations RPG Game Engine resource
EIO	Evermore Software EIOffice document binder
EIP	Capture One Enhanced Image Package
EIT	Encharta database update
EJP	Elite Japan Crossword Puzzle

Supported file type	Description
EJPG	Encrypted JPEG bitmap
EKB	ZMC VisualTablet data
ELC	Combustion 2 Particle Library
ELD	EasyLanguage Document
ELF	EurekaLog log file
ELI	DipTrace Component
ELM	FrontPage Theme-Pack
ELS/ELA	EasyLanguage Storage / Archive
EMA	EPLAN Macro
EMB	EMB Wilcom Design embroidery file
EMBL/EMB	EMBL sequence data
EMD	DATACOMP 1.0 compressed archive
EMDL	Softimage Exported 3D Model
EMF	HyperVision EMF ASCII Format
EMG	Delsys EMG format
EMI	Pocket Tanks emitter
EML	E-Mail message (Var. 1)
EMM	MindMaple document
EMOD	Quadra Composer module

Supported file type	Description
EMS	Electronic Music System v6 module
EMULECOLLECTION	eMule Collection file
EMW	Resident Evil player model data
EMX	Rational Software Architect Model
EMY	Ericsson eMelody Ringtone
ENC	ENhanced Compressor compressed archive
ENC1	Kaspersky encrypted trace
ENCRYPTED	EasyCrypto encrypted
ENEX	Evernote Exported XML
ENF	EndNote Filter
ENG	Live For Speed Engine sound
ENL	EndNote Library
ENS	EndNote Style
ENW	Endnote Export Format
ENZ	EndNote Connection
EOC	EncryptOnClick encrypted
EOP	EveryonePiano music score
EOPM	EOP Music Master music score
EOT	ExamView Online Test

Supported file type	Description
EOT/FNTDATA	Embedded OpenType font
EP	Pencil sketch
EP/EPW/EZP/TXT	EasyPlot save file
EPA	Award BIOS logo bitmap (136x126) (v1)
EPITASK	Telestream Episode Task
EPM	Electric Pipes Music
EPP	EasyPrint Preview
EPS	Adobe Encapsulated PostScript
EPS/PS	Encapsulated PostScript (with DOS style preview)
EPUB	Open Publication Structure eBook
EPV	IPLAY Enterprise Video
EPW	EnergyPlus Weather data
EPX	Rational Software Architect Profile
EQCONFIG	EQATEC Profiler configuration
EQF/Q1	Winamp EQ Settings File
EQG/PAK/PFS/S3D	EverQuest Game data
ER1/ERX	AllFusion ERwin data
ERD	Entity Relation Diagram

Supported file type	Description
ERF	BioWare Entity Resource File
ERS	Earth Resource Mapping Raster
ERV	Earth Resource Mapper Vector
ERWIN	ERwin model
ES	E-Studio 1.x experiment
ES2	E-Studio 2.x experiment
ES3	e-Szigno signed document
ESB/WBD	eBeam Whiteboard
ESP	ESP - Extension Sort Packer compressed archive
ESQ/FIL	Yamaha e-SEQ music
ESS	Ekahau Site Survey File
EST	Microsoft Streets and Trips map
ESU	ESU electronic sounds
ESY	EmEditor Syntax file
ET	Easiteach lesson
ETA	Keyhole - Google Earth Overlay
ETD	Acrobat eBook Reader EBX Transfer Data
ETHERPAD	Etherpad document

Supported file type	Description
ETL	Window tracing/diagnostic binary log
EU4	Europa Universalis IV saved game
EV2	Emblaze Video 2 video
EV3	LEGO Mindstorms EV3 project
EV3P	LEGO Mindstorms EV3 Program
EVO	Enhanced Video Object
EVT	Windows Event Viewer Log
EVTX	Vista Event Log
EVY	Envoy document
EWB	EasyWorship Bible text
EWNET	Ultiboard netlist data
EWPRJ	Compressed Electronics Workbench project
EX	Fashion Tracker module
EX_	Microsoft SZDD compressed (Haruhiko Okumura's LZSS)
EX4	MetaQuotes Language 4 compiled program
EXAM	ProfExam Exam
EXB	CAXA drawing
EXE	16bit DOS EXE ApBasic

Supported file type	Description
EXE/COM	SymbOS Executable
EXE/OBJ	QDOS executable
EXM	HP Palmtop 95/100/200LX Sys.Manager compliant Executable
EXR	OpenEXR High Dynamic-Range bitmap
EXSD	Eclipse Extension Point Schema
EYB	Encarta Encyclopedia Yearbook and Web Links update
EYETVP	EyeTV scheduling metadata
EYETVR	EyeTV Recording metadata
EYW	EyesWeb patch
EYWX	EyesWeb patch (XML)
EZLOG	Skype Extras Manager log
EZP	GoLabel document
EZPX	GoLabel document (XML)
F01/F02/F99	HEC-RAS Flow file
F3D	Flare3D binary model
FA/FZA/MZA	Novastorm Media video
FABBPROJECT	netfabb Project
FACE	Facer watch Face

Supported file type	Description
FACE/FAC	FaceSaver bitmap
FACET	Facet file
FACT	ElectricImage 3D file
FACTORY	Simplify3D Factory session data
FAMILYX	My Family Tree Family
FAR	Farandole Composer module
FARCONFIG	Far settings
FAS	AutoCAD Fast-load AutoLISP (FAS4)
FASTA	FASTA DNA sequence
FASTQ/FQ	FASTQ format
FAV	Outlook Shortcuts
FAXX/FAX/IFF	IFF Facsimile image
FB	Slim! compressed archive
FB2	FictionBook 2.0 eBook
FB2K-COMPONENT	foobar2000 component
FBC	FamilyTree Maker compressed backup
FBF	Free Backup Fix backup
FBI	Spring Engine unit Info
FBK	FamilyTree Backup File

Supported file type	Description
FBL	iGO map
FBM/CBM	Fuzzy Bitmap
FBP7	FinalBuilder 7 Project
FBS	FBIde session
FBX	Autodesk - Kaydara FBX 3D format (Binary)
FC	Future Composer v1.4 module
FC0	FCE Ultra FC0 savestate
FC3MAP	Far Cry 3 map
FC7	FastCAD for Windows drawing (V7)
FCA	Omnis Web Client Form Cache
FCD	FidoCAD drawing
FCF	Thrustmaster TARGET profile
FCLR	Flowgorithm Color scheme
FCO	FIASCO image/video
FCP	Final Cut project
FCPXML	Final Cut Pro X XML project
FCS	Flow Cytometry Standard format
FCSTD	FreeCAD Standard document
FCV	ColecoVision Font

Supported file type	Description
FCW	FastCAD for Windows drawing (generic)
FD2	EasyPrint PictureMate borders
FDAT	Fiasco Database: data file
FDB	FT/Pro Form
FDD	FlexiDATA Database
FDF	Acrobat Forms Data Format
FDI	Formatted Disk Image (gen)
FDM	Floppy Disk Manager disk image
FDNEUT	FIDAP Neutral format
FDP	FMOD Designer Project
FDR	Final Draft document
FDS	FireDAC database
FDT	FormDocs template
FDX	Final Draft Script
FE_LAUNCH	FCS Express Layout Link
FEA	PLS-CADD Feature code
FEATURE	Gherkin Feature
FED	FORMIK form
FEM	Algor FEMPRO model

Supported file type	Description
FET	FET Timetable
FF	Call of Duty game data
FFDATA	ABBYY eForm Filler data
FFE	Microsoft DirectInput Force Feedback Effect
FFL	Fast Find document List
FFN	FIFA game serie Font
FFP	FLAC Fingerprint
FFS_GUI	FreeFileSync configuration
FFT	IBM Final-Form Text document
FFX	Microsoft Fast Find Index v1.x
FFXML	Filter Forge filter
FG	Fred Gray module
FH*	Freehand (MX) Project (generic)
FH10	Freehand 10(MX) Project
FH3	Freehand drawing (v3)
FIB/FID/FIH/FIP/FIV	File Investigator data (generic)
FIC	Hyper File database
FID	Felix format spectra
FID/SPC/2D/001/002/003	NUTS format

Supported file type	Description
FIDX	Fiasco Database: index File
FIF	Fractal Image Format bitmap
FIG	Cabri figure
FIL	AVG Antivirus Vault file
FILM	Amiga Murder video
FILTERS	Visual Studio C++ project Filters
FIM	Paul van Keep's Icon Heaven icons package
FIN	Corel saved find/search
FIT	Mechwarrior FIT data
FITS/FIT/FTS/FZ	Flexible Image Transport System bitmap (gen)
FLA	Flash Authoring / source material
FLAC/FLA	FLAC lossless compressed audio
FLAME	Fractal Flame Parameters
FLC	FIGfont control file
FLD	AVS Field data
FLF	FIGfont
FLI	Autodesk Animator
FLIPCHART	ActivInspire Flipchart
FLL	TextPipe Filter List

Supported file type	Description
FLM	Adobe FilmStrip
FLOW	Expression SketchFlow data
FLP	Activstudio Flipchart
FLSX/FLWX	FileLocator Pro workspace/search (v8.0)
FLV	Flash Video
FM	Art Of Noise MF instrument (v1.x)
FM2	FCEUX movie capture
FM3	Formatting Data for Lotus 1-2-3 worksheet (V3)
FMB	Oracle Binary Form
FMD	Cumulate Draw's editable FMD format
FMK	FM-Kingtracker module
FML	FCEditor XML project
FMP	The Fractal Mapper map
FMP12	FileMaker Pro database (v12)
FMT/FJ3	Formatting data for Lotus 1-2-3 worksheet (V2)
FMX	FileMaker Pro 32-bit plug-in
FMZ	Form*Z Project
FN	STK Facility Network
FN3	Harvard Graphics Font (v3.x)

Supported file type	Description
FNC	Vue D'Esprit 4 function definition
FNF	PTC FEM Neutral Format model
FNK	FunkTracker module
FNS	Free Notes document
FNT	BMFont Font control data (text)
FODP	OpenDocument Flat XML Presentation
FODS	OpenDocument Flat XML Spreadsheet
FODT	OpenDocument Flat XML Document
FON	Beyond Words Composer Font
FONT	Amiga bitmap Font
FORM	Gambas form (v2)
FOS	Fallout 3 save game
FOT	Win 3.x Installed TrueType Font
FOUNTAIN	Fountain Script
FOX	Furcadia Art
FP	FinePrint saved - output file
FP2/FUN	Funpaint 2 bitmap
FP3	FileMaker Pro 3 database
FP5	FileMaker Pro database (v5)

Supported file type	Description
FP7	FileMaker Pro database (v7-11)
FPAGE	XPS FixedPage object
FPF	IKEA Kitchen Planner Document
FPG	DIV Games Studio Graphics Library
FPK	PerFORM Communicator File Packet
FPL	foobar2000 playlist
FPPX	Fresh Paint Painting
FPRG	Flowgorithm Program
FPT	Farandole Composer pattern
FPX	Kodak FlashPix bitmap
FR3	FastReport 3 report
FREC	Fiasco Database: frequencies files
FRED	Fred Editor module
FREF	Freenet node Reference
FRESHROUTE	Navigon Fresh route data
FRF/FRL/FRP	PerFORM compressed database
FRG	Sound Forge project
FRL	FormFlow 1.x form
FRL/FRP/FRZ	FormFlow 2.x form

Supported file type	Description
FRO	A-Robots Fighting Robot Object
FRX	Microsoft Visual Basic Form
FS	Final Burn savestate
FSB	FMOD Sample Bank Format
FSC	SimCity 3000 Freshness Score
FSD	COCO/COFE Flowsheet Document
FSF	Quartus Software Build Settings File
FSH	Electronic Arts graphics
FSM	Farandole Composer sample
FSN	Greeting Card Factory
FSP	Flash Slideshow Builder project
FSPROJ	Visual Studio F# Project
FST	FAST input
FSTF	Flexible Stream Transport Format
FSY	FileSync profile
FTC	FluxTime Clip
FTF	Sony FlashTool Firmware
FTI	FamiTracker Instrument
FTL	Family Tree Legends data

Supported file type	Description
FTM	Face The Music module
FTR	File-Type Rule
FTS	Windows Help Full-Text Search index file
FTW	Family Tree Maker Family Tree
FUCHS/FT	Fuchs Tracker module
FUN	Cubify Invent model
FUZ	Bethesda Softworks FUZE voice
FVF	Fluke View data
FW	Forgotten Worlds custom music format
FW2	Framework II file
FW3	Framework III file
FX	Age of Wonders: Shadow Magic Effects
FXB	HALion Sampler patch - bank
FXCOP	FxCop project
FXCPROJ	FX Composer Project
FXE	GP32 Free eXecutable Encrypted
FXG	Flash XML Graphics
FXM	Fuxoft AY Language module
FXP	Steinberg Plug-in

Supported file type	Description
FXR	WinFax Sent / Received document
FZ	Flexible Image Transport System bitmap (compressed)
FZB	Fritzing Bin module
FZBZ	Fritzing Bundled Bin
FZIP	Foxit Reader Add-on
FZP	Fritzing Part
FZPZ	Fritzing Bundled Part
FZZ	Fritzing shareable project
G	MicroPlanet Gravity news database
G01/G02/G99	HEC-RAS Geometry file
G2W	GeoplanW data
G3	raw Group 3 FAX bitmap
G3A	Casio Prizm add-in
G3W	GeospaceW data
G64	G64 1541 raw disk image
G8	Cubicomp PictureMaker green channel image data
G9B	G9B graphics format bitmap
GA/PG	STK Great Arc Propagator format

Supported file type	Description
GA3	Graphical Analysis 3 document
GAB	WinDev Controls' Styles description
GADGET	Microsoft Vista Sidebar Gadget (CAB - Obsolete)
GAI	Adobe SING Glyphlet
GAL	GenePix Array List
GAM	Cyberboard Game
GAM/VEC	Vectrex game ROM
GAMBAS	Gambas application (v2)
GAN	GanttProject project
GAU	MS Flight Simulator Gauge
GAX	MS Age of Empires II: The Conquerors Expansion v1.0 Saved Game
GB/GENBANK/GP/GBK	GenBank sequence record
GBA	Game Boy Advance ROM
GBAP	GLBasic Project (XML)
GBC	GameBoy Color ROM File
GBD	Graphtec Binary Data
GBI	gBurner Image
GBP	gBurner Project

Supported file type	Description
GBR	GameBoy Sound System GBR dump
GBS	GameBoy Sound System dump
GBT	GFI Backup Task
GBX	Cyberboard Gamebox
GCA	G Compression Archiver
GCAT	GUI Design Studio Catalogue
GCD	Garmin firmware update
GCF	ArcSoft Greeting Card Creator project
GCG	GCG Sequence Chemical file
GCL	DISGCL script
GCT	GenePattern GCT format
GCW	Microsoft Math worksheet
GCZ	GameCubeZip image
GD	STK database update information
GDB	GVA/GVA2000 Author lecture
GDF	General Data Format for biosignals
GDFMAKERPROJECT	Game Definition File Editor project
GDG	GDevelop Game project
GDL	Game Description Language

Supported file type	Description
GDM	General DigiMusic module
GDOC	Google Drive Document link
GDP	GUI Design Studio Project
GDS	GDSII stream format layout (binary)
GDTB	gretl Binary Data
GEANY	Geany project
GED	Arts and Letters Graphics file
GEM	GEM metafile
GEMSPEC	Ruby Gem::Specification
GENERICTEST	Visual Studio Generic Test
GEO	GeoWorks GEOS FAX driver
GEO/3D	Videoscape GEO mesh
GEOJSON	GeoJSON format
GETVIEWPORTINFO	Google Maps API data
GEXF	Graph Exchange XML Format
GFA	GFA-BASIC Amiga tokenized source
GFAR	Greenfoot Archive
GFF3	Generic Feature Format Version 3
GFI/GFIE	Greenfish Icon Editor Pro

Supported file type	Description
GFS	GGFileSPlit File Fragment
GFT	GSP Family Tree
GFX	Explorations RPG Game Engine resource - Bitmap
GG	Google Gadget
GGP	GemCom Graphic bitmap
GGR	GIMP Gradient
GGZ	Garmin Zipped geocache
GHLAYOUT	Grasshopper custom Layout
GHO	Norton older Ghost image (first file)
GHS/001/002/003/999	Norton older Ghost image (split file)
GHX	Grasshopper program (XML)
GID	GID Help index
GIF	GIF animated bitmap
GIG	GigaSampler Sound bank
GIM	Playstation 3 icon
GIR	GObject Introspection information
GISE	ISE Project generated data
GITMODULE	git submodule properties definition

Supported file type	Description
GLA	Sothink SWF Easy Project
GLADE	Glade UI design
GLIF	Glyph Interchange Format
GLL	EASE GLL loudspeaker format
GLOX	Microsoft Office SmartArt Graphics Layout
GLUE	GlueMon module
GLY/GLX	Microsoft Word for DOS Glossary
GM	Game Music
GM/GM2/GM4	Autologic bitmap
GM6	Game Maker 6 project
GMANIFEST	Google Desktop Gadget manifest
GMBL	Logger Lite data
GMC	Game Music Creator Music
GME	DexDrive memory card save game
GMI	GPS Tuner map calibration data
GML	Graphlet File Format
GMO/MO	GNU Gettext Machine Object file
GMP	GUEmap document
GNUMERIC/XML	GNUMERIC spreadsheet (XML, unzipped)

Supported file type	Description
GO/PRB	Ishi Format Go game
GOB	Dark Forces Game data archive
GOCAD	GOCAD ascii data format
GOE	GOES Satellite bitmap
GOOMOD	World of Good addin
GOZ	ZBrush GoZ export template
GP3	Guitar Pro v3 tablature
GP4	Guitar Pro v4 tablature
GP5	Guitar Pro v5 tablature
GPD	Generic Printer Description - Unidrv minidriver
GPG	GNU Privacy Guard public keyring
GPI	Garmin Point of Interest
GPJ	jGRASP Project
GPL	GIMP Palette
GPM	Crossword Puzzle
GPOL	Bruker binary pole figure format
GPR	GenePix Results
GPX	GPS eXchange format
GQ	QLFC compressed archive

Supported file type	Description
GRA	Chasys Draw IES Gradient
GRAFFLE	OmniGraffle Drawing
GRAMMAR	Synalyze It! Grammar
GRAMPS	GRAMPS XML
GRAPHML	GraphML graph
GRB/GRIB/GRIB1	Gridded Binary data
GRB/GRIB/GRIB2	Gridded Binary data 2
GRD	Adobe Photoshop gradient
GREENFOOT	Greenfoot Project
GREENSHOT	Greenshot screenshot bitmap
GRF	ExpressGraph Graph
GRID	GridMove grid template
GRINDX	Juice Grinder recipe
GRLE	Farming Simulator terrain data
GRO	Allegro MIDI music
GROUPPROJ	Borland Group Project
GRS	GetRight Skin
GRX	GetRight File List
GRXML	XML Grammar

Supported file type	Description
GRZ	GRZip compressed archive
GSC	GS-Calc workbook
GSF	Grand Smeta data
GSF/GSFLIB/MINIGSF	Gameboy Sound Format
GSHEET	Google Drive Spreadsheet link
GSI	GPS Tuner map slices calibration data
GSLIDES	Google Drive Presentation link
GSM	ArchiCAD Library Object
GSN	Cyberboard Scenario
GSO	GoldenSection Organizer database
GSP	Geometer's Sketchpad Document
GSS	Geometer's Sketchpad Script
GT2	Graoumf Tracker 2 module
GTK	Beaver Sweeper module
GTKW	GTKWave Saved session
GTM	GPS TrackMaker map
GTP	Guitar Pro Tablature (v1.x)
GTR	Spectrum Global Tracker chiptune
GTX	Genetica 1.0 Texture

Supported file type	Description
GUI	GUI Design Studio design
GUIDE	Amigaguide hypertext document
GUIKIT	Shapeshifter theme
GVI	Google Video
GVP	Google Video pointer
GW1/GW2/GW3	HomeBrew File Folder game data archive
GWB	InterWrite Reader document
GWI	Novell Groupwise File link
GWP	GoodWay Flight Planner flight plan
GWS	GateWay Settings
GX1	GX1 bitmap
GXD	General CADD Pro (generic)
GXF	General eXchange Format video
GYM	Sega Genesis/Mega Drive sound/music data
GZA	GZA compressed archive
H/HRP	Hrip compressed
H17	HDOS H-17 portable dump disk image
H264	Raw H.264/MPEG-4 AVC Video
H2P	Zebra2 Preset

Supported file type	Description
H2PATTERN	Hydrogen Pattern
H2SONG	Hydrogen song
H5	HDF5 data file
H8T	H8 Tape image
HA	HA compressed archive
HAR	HTTP Archive format
HASH	EnCase forensics Hash
HCC	HydroCAD Data for prefabricated storage Chambers
HCD	HCD format firmware
HCG	HCLab document
HCOM	Huffman Compressed audio
HCP	HydroCAD Project
HCX/HQX	BinHex encoded
HDB	PC-File data (gen)
HDP	MAGIX Hard Disk Project Audio
HDP/JXR/WDP/WMP	JPEG XR bitmap
HDR	InstallShield setup header
HDR/PIC/RGBE/XYZE	Radiance High Dynamic Range bitmap

Supported file type	Description
HDZ	KeyShot environment
HE5	Hierarchical Data Format Release 5
HEAD	HEAD AFNI medical metadata
HEARTSSAVE-MS	Microsoft Hearts Saved game
HEIC	HIEF bitmap (heic)
HEIF	HIEF bitmap (mif1)
HES	Hudson Entertainment System Sound Format dump
HEXDWC	Free Hex Editor Neo layout
HF2	L3DT compressed Heightfield Format
HFA	ERDAS Imagine Hierarchical File Architecture
HFE	HxC Floppy Emulator disk image
HFF	L3DT HeightField File
HFZ	HollywoodFX Plug-In
HG1	Hellgate London save game
HHB	LigPlot Hydrogen-Bonds data
HHP	Microsoft HTML Help Project
HIN	HyperChem molecule format
HIPC	Hippel COmpressed SOng module

Supported file type	Description
HIR	C64 Hires bitmap
HIV/DAT	Windows NT Registry Hive (generic)
HJT	TreePAD document
HL7	Health Level-7 data (pipe delimited)
HLE	HomeBrew Level
HLF	FAR help
HLP	C-Worthy Help Librarian Data (v1.x)
HLX	Help Magician text file
HMK	Hallmark Card Studio file
HMP	Frontier 2 First Encounters Music
HMT	HighMAT file
HND	HNSKY Deep Sky Database
HNM	CRYO HNM4 video
HNM/HNS	CRYO HNM6 video
HNT	Magnetic Hint
HONMOD	HoN Modification Manager package
HOT	Anders Oland music
HPD	HP Document
HPGL/HPG	Hewlett-Packard Graphics Language

Supported file type	Description
HPI	Hemera Photo-Object Image
HPK	HPACK compressed archive
HPKG	Haiku Delta Package
HPR	RoboHelp data
HPROJ	HOBOWare Project
HPT	RoboHelp Topic Export
HPUB	HPub HTML Publication
HRF	Hitachi Raster Format bitmap
HRM	Polar Heart Rate Monitor format
HRU	HRU bitmap
HSB	HandStory eBook
HSC	HYSYS Simulation Case
HSF	HOOPS 3D Stream Format
HSI/JPG	HSI JPEG bitmap
HSM	HelpSmith Project
HT	HyperTerminal data file
HTC	HTML Component (ASCII)
HTM/HTML	HyperText Markup Language with DOCTYPE
HTML	HyperText Markup Language

Supported file type	Description
HTR/HAPTAR	Hapttek Compressed file
HUD	HUD Maker
HUH	HydroCAD Unit Hydrograph definitions
HUS	Husqvarna Designer I Embroidery Machine Format
HV	Amiga HAM Video
HVL	Hively Tracker module
HVS	High Voltage SID Collection update info
HWP	HWP document
HWT	Huawei EMUI Theme
HXN	Hexagon model
HXS	Microsoft compiled help format 2.0
HXT	Help Table of Contents
HYP	Acrobat spelling dictionary
HZF	neosat fixes
HZP	CrossStudio project
I3D	Instant3D document
I3F	I3 Fax file
IAF	Outlook 97 and 2000 E-mail Account Settings

Supported file type	Description
IB3	ICDRAW group icon bitmap
IBCC	Apple Application Information Table
IBG	NASA PDS labeled bitmap
IBI	ICDRAW single icon bitmap
ICA	Citrix Independent Computer Architecture
ICC	Art Icons Pro - IconCollection
ICC/ICM/CC	ICC Color profile (generic)
ICL	Icons Library
ICN	DEGAS Elite Icon Definition
ICN/XBG	HP Palmtop 100/200LX Icon
ICNS	Mac OS X icon
ICO	OS/2 Icon
ICPR	Art Icons Pro - IconProject
ICR	NCSA Telnet Interactive Color Raster bitmap
ICS/VCS	iCalendar - vCalendar
ICSPKG	Intellitools Classroom Suite Package
IDF	Microsoft Instrument Definition File
IDML	Adobe InDesign Markup Language
IDN	Alpha Four Index Definition

Supported file type	Description
IDW	AutoDesk Inventor drawing
IDX	Java Applet cache index
IES	IESNA Photometric data
IFF	"The Sims" object
IFIXION	iFiction Metadata
IFL	IncrediFlash animation
IFO	DVD Info file
IFS	DIV Games Studio Font Source
IFX	Imagine Effect
IGC	IGC Flight Track
IGM	Indigo Renderer Material
IGR	Intergraph SmartSketch Drawing
IGS/IGES	Initial Graphics Exchange Specification (IGES) data
IGTX/ITX/TXT/TEXT	IGOR Pro Text document
IGX	iGrafx document
IIF	QuickBooks Import/Export Interchange File
IIM	InShape IIM bitmap
IIQ	Intelligent Image Quality - Phase One RAW image

Supported file type	Description
IKMP	IK Multimedia Preset
IL3	particleIllusion library
ILBM	IFF ILBM bitmap (variant)
ILBM/LBM/IFF	IFF InterLeaved BitMap
ILD/ILDA	ILDA image data transfer format
ILK	Microsoft Incremental Linker data
ILM	Opus Creator multimedia file
ILV	ILOG View
ILX	Interlex vocabulary
IMA	IncrediMail animation
IMA/IMG	Old DOS disk image
IMB	IncrediMail Address Book
IMD	ImageDisk disk image
IME	IncrediMail emoticon
IMF	Imago Orpheus module
IMG/DMF	Distribution Media Format disk image
IMG/RLE	ADEX bitmap
IMG/XDF	eXtended Density Format disk image
IMI	IncrediMail image

Supported file type	Description
IMN	IncrediMail notifier
IMO	iMON Setting file
IMOVIEPROJ	iMovie project
IMQ	NASA Planetary Data System image
IMR	Impromptu report
IMS	IMS Content Package
IMW	IncrediMail sound (MIDI music)
IMX	iMindMap Map
IMY	iMELODY sound/music
IMZ	Compressed Disk Image (password protected)
IND	AOL thumbnails index
INDD	InDesign Document
INF	Adobe Type Manager Font Information
INFO	Amiga icon file (NewIcons type)
INI	Generic INI configuration
INP	InPage document
INS	InstallShield Script
INSTRUMENT	SuperJAM! Instrument
INT	Borland Interface unit

Supported file type	Description
INX	Inkscape extension descriptor
IOBJ	Visual Studio Intermediate Object
IOC	Indicator Of Compromise
IOM	ZEMU IO Map
IP	IconPackager theme
IP2	Interpress format
IPA	iOS Application
IPD	BlackBerry Backup
IPDB	Visual Studio Internal Program Data Base
IPE	Microth Stroke Set
IPF	Interchangeable Preservation Format floppy disk image
IPJ	Autodesk Inventor project
IPR	InstallShield Project
IPS	Image Analyst MKII Pipeline
IPT	Inventor Part
IPUZ	ipuz puzzle open format
IPX	lpix Spherical Panorama
IPYNB	IPython notebook

Supported file type	Description
IQY	Microsoft Web query
IRCP	IRIDAS Composite playlist
IRP	InfraRecorder Project
IRR	Irrlicht 3D scene
IRRMESH	Irrlicht static Mesh
IS	Sound Invasion Music System module
IS20	Sound Invasion Music System 2.0 module
ISF	Inspiration Software data
ISM	ISAM table handler data
ISO	Apple ISO9660/HFS hybrid CD image
ISPRO	InstallSimple Project
ISS	Inno Setup Script
ISS/XARC	FunCom ISS audio
IST	Adobe Image Styler file
ISTG	Imagine Staging File
ISU	InstallShield Uninstall Script
ISZ	ISO Zipped format
ITA	IconTweaker theme
ITC	iTunes CoverFlow data

Supported file type	Description
ITC2	iTunes Cover Flow Data (v2)
ITL	iTunes Music Library
ITM	Diablo 1 Item save file format
ITMX	XMILE XML Model Interchange Language
ITR	Icy Tower Replay
ITW	BMW TIS grayscale bitmap
ITX	Imagine Texture
IUM	infoUSA Network Meter file
IV	SGI Open Inventor Scene Graph (ASCII)
IVE	OpenSceneGraph native binary format
IVF	Intel Indeo Video File
IVML	INDENICA Variability Modelling Language
IVR	RealNetworks Internet Video Recording
IVU	ImmerVision XML user interface
IVY	Ivy module descriptor
IW2	Information Workshop 2000 data file
IW5DLC	Call of Duty Modern Warfare 3 DLC
IWC	WaveL bitmap
IWD	Call Of Duty map - game data archive

Supported file type	Description
IWI	Infinity Ward Image bitmap
IXL	DB/TextWorks Database Indexed List
IXS	Ixalance module
J	JAR Compressed Archive
JACKSUM	Jacksum fingerprints
JAD	Java Application Descriptor
JAM	JAM Archive
JAP	Nonogram puzzle
JAR	JARCS compressed archive
JAS	Cheetah3D format
JBA	Jabaco project
JBEAM	BeamNG vehicle definition format
JBF	PaintShop Pro Browser cache
JBG/JBIG/BIE	JBIG raster bitmap
JB1	Motoman Relative Job
JCE	JWPce document
JCEKS	Java SunJCE KeyStore
JCF	JTAG Chain File
JCI	JTAG Chain Information

Supported file type	Description
JCLIC	JClc project
JCP	JCreator Project
JDF	Job Definition Format Job File
JDP	BlackBerry JDE Application Project
JDT	Capture Classic Filler - Accelio JetForm
JDX/DX	JCAMP-DX format
JED	CUPL format
JEF	Janome NH10000 Sewing Machine Stitch
JG6	BigJig Jigsaw
JGCSCS	EditPad Pro Custom Syntax Coloring Scheme (ASCII)
JHM	JavaHelp map
JIF	Jeff's Image Format bitmap
JIG	GameHouse Jigsaw Game
JKS/KEYSTORE	Java KeyStore
JLS	JPEG-LS bitmap
JMF	Janko Mrsic-Flogel module
JMX	Hot Potatoes JMix project
JNB	Sigma Plot Workbook

Supported file type	Description
JNG	JPEG Network Graphics bitmap
JNILIB	JNI Library
JNLP	Java Web Start application descriptor
JNT	Windows Journal
JO	FlowJo Mac Workspace
JOB	Compass and Ruler Job
JOBOPTIONS	Acrobat Distiller Job Options
JP2	JPEG 2000 bitmap
JPC/J2C/J2K	JPEG-2000 Code Stream bitmap
JPF/JPX	JPEG 2000 eXtended bitmap
JPM	JPEG 2000 Multi-layer bitmap
JPO	Jason Page audio format (old)
JPS	JPEG Stereoscopic bitmap
JPX	JBuilder Project
JQZ	JQuiz quiz
JR2	Fishing Simulator 2 addon
JRC	JRchive compressed archive
JRPRINT	JasperReports Print
JRSR	JPC-RR rerecording

Supported file type	Description
JRXML	JasperReports JRXML report definition
JSB	JavaScript Bean file
JSD	eFAX Jet Suite Document
JSF	Jahshaka Scene File
JSON	Coriolis.io ship loadout
JSONLZ4	Mozilla JSON compressed bookmark
JSPF	JSON Playlist File
JSPROJ	Visual Studio JavaScript Project
JSRC	Jabaco Source
JST	Jnes save state
JSXBIN	Binary ExtendScript Script
JT	JT 3D visualization format
JTD	Ichitaro document
JUCER	JUCE project
JUI	Qt Jambi User Interface
JVEROM	ParaJVE ROM
JVX	JavaView JVX geometry
JWC	JewelCase Maker project
JWL	Easy CD Creator's media label

Supported file type	Description
JWR	LegaSuite GUI Runtime
JZLIB	Lemur Module
JZML	Lemur Layout
K64	Kernal64 save state
K7	DCMO5 emulator tape image
KA	Karma Asset
KAL	Hondata K-Manager Calibration data
KAP	MapInfo Sea Chart
KAR/MID	Karaoke MIDI
KAW	Karma Workspace
KBDX	3DS MAX keyboard shortcuts (XML)
KCH	KChess saved match
KCM	KonyvCalc file
KCX	Kea Coloring Book page
KD1	ProHance Mouse Keys Definition table
KDB/KDBX	KeePass Password Safe database
KDC	Kaspersky Anti-Virus signature bases
KDELNK	KDE desktop Link
KDH	KDH document

Supported file type	Description
KDS	KD Player Skin
KDX	Google Earth import definition
KDZ	LG smartphone firmware archive
KES	Kurzweil 3000 document
KEXI	Kexi database
KEY	H-BEDV - AVIRA product key
KEYBOARD	SuperJAM! Keyboard
KEYSTORE	Gnome Keyring Store
KFA	Voxlap Frame Animation
KFG	Indiana Jones and the Infernal Machine keys configuration
KFM	Gamebyro KFM data
KFN	KaraFun Karaoke Song
KFR	Kalles Fraktaler parameters
KGB	KGB Archiver compressed archive
KI	Klystrack Instrument
KICAD_PCB	KiCad PCB
KID	Kidspiration file
KIF/KIFF	Kt Interchange File Format compressed bitmap

Supported file type	Description
KIN	Kinemage protein language
KK3	Kaleidoscope Kreator 3 workspace
KLA	KLARFF map-data
KLC	Microsoft Keyboard Layout Creator source (UTF-16-BE)
KLIP	KlipFolio Klip
KLQ	Kaspersky Anti-Virus quarantined
KMAP	BeebEm Keymap
KML	Emu48 keyboard configuration
KMN	Keyman keyboard source
KMP	IBM i (Client) Access Keyboard Map
KMY	KMyMoney XML data (decompressed)
KMZ	Google Earth saved working session
KOA	Koala Paint (C64) bitmap
KODU	Kodu game world
KP	KeyKit Page
KPJ	Keyman Project
KPL	Kazaa Playlist
KPP	Kid Pix Presentation

Supported file type	Description
KPR	KOffice KPresenter Presentation
KPX	Kid Pix project
KR1/KRZ	Kurzweil K2-serie sample
KRA	Krita document
KRC	Chinese KuGou ResourCe (KuGou Music lyric)
KSF	Korg Trinity/Triton sample
KSP	KeyShot Package
KSV	Kheops Studio Video
KSY	Kaitai Struct language
KT	Klystrack chiptune
KT3	Battery 3 Drum Kit
KTN	KToon project
KTS	KT-Tech compressed audio
KTZ	Kahootz Project
KV	Kv design language
KV6	Voxlap voxel sprite
KVA	KVirc Addon
KVK	Keyman Virtual Keyboard
KVT	KVirc Theme

Supported file type	Description
KVTML	KWordQuiz learning file
KW3	KanjiWORD document
KWD	KWord document
KWO	KeyWallet Object - encrypted data
KWS	KeyWallet Skin
KX	KiXtart tokenized script
KXF	Koda Form Designer Form
KZ	Chinese kuaiya kzip compressed archive
L01	Encase Logical Evidence
L2R	Lineage II Replay
L30	Bitmapped Signum!2 printer font (Laser/Inkjet)
L64	64LAN container
L6T	Line 6 Tone
L86	CP/M-86 library
LA	La Lossless Audio compressed (generic)
LAB	Bar-One Lite label
LAN/GIS	ERDAS Image bitmap (v7.x)
LAS	CWLS Log ASCII Standard
LAUNCH	Eclipse Launch configuration

Supported file type	Description
LAV	DNA Sequence Alignment
LAY	Sprint Layout Printed Circuit Design (v6.0)
LAYOUT	Code::Blocks Workspace Layout
LAZ	LASzip compressed LAS LiDAR data
LB	Low Bitrate Packer compressed audio
LB6/LBX	CODESYS Library
LBL	Planetary Data System info (v3)
LBS	Omnis Studio Library
LCD	Lucid 3-D spreadsheet (v2.x)
LD	Polycom SoundPoint IP firmware
LDF	LuraDocument Format bitmap
LDIF	LDAP Data Interchange Format
LDP	Altium Designer Layer Pairs export data
LDR	GoDot C64 Image Processing - Loader
LDW	Little Draw Drawing
LDX	Lingoes Dictionary
LEF	LEN Exchange Format
LEX	Polar SpellChecker dictionary
LFD	LucasFilm Data - LucasArts game resource

Supported file type	Description
LFM	Lazarus Form
LFP	Lytro Light Field Picture web format
LG	ARHANGEL compressed archive
LG32	GFA-BASIC 32 library
LGO	Modern ListGeo Output
LGX	Logistix spreadsheet
LHA	Amiga WHDLoad package (lha compressed)
LIB	CIRCAD source library (v4.x)
LIB4D	Cinema 4D Preset Library
LIBR	Music-X patch Library
LIBRARY-MS	Microsoft Windows library description
LIBZIP	Camtasia Studio Zipped Library
LIC	ESET NOD32 Antivirus License data
LID	Lextek Language Identification Module
LIF	Life cellular automata format
LIFT	Lexicon Interchange Format
LIGHTHOUSE-PROJECT	Lighthouse Project
LIGT	Caligari TrueSpace Light (v2.x)
LIM	Limit compressed archive

Supported file type	Description
LIN	X-Plane Painted Line
LIQ	Liquid Tracker module
LIST	JAR Index
LIT	Microsoft Reader eBook
LITEMOD	Minecraft LiteLoader Mod
LIVECODE	LiveCode stack
LKD	Pioneer OEL screensaver
LL	Combit List and Label printer setup file
LLSD	Linden Lab Structured Data
LMA	Learning Mobile Author (LMA) Project
LME	Leggless Music Editor module
LMF	Quartus Library Mapping File
LMK	Sothink Logo Maker logo
LMU	RPG Maker 2000/2003 Map
LMX	Route 66 Landmarks
LNG	SourceEdit Language Definition
LNK	Windows Shortcut
LNX	Atari Lynx ROM
LOADTEST	Visual Studio LoadTest project

Supported file type	Description
LOC	Topografix's EasyGPS/TerraByte Location file
LOG	Cabrillo Log (v2.0)
LOG/LOG1/LOG2	Windows NT Registry Hive (transaction 1)
LOGICX	Logic Pro X project
LOGONVISTA	LogonStudio Vista logon image
LOGONXP	LogonStudio theme
LOOK	SpeedGrade Look
LP	LaTeX-CAD drawing
LPAQ	lpaq compressed data (generic)
LPD	Lecturnity Player file
LPI	Lazarus Project Information
LPK	Lazarus Package
LPMD	LPMD Molecular Data
LPS	Lazarus Project Session
LPU	Passolo Localization Project
LQM/JLQM	LG QuickMemo note
LQT	Liquid Audio
LRC	Lyric file (with ID tags)
LRF	Unencrypted BBeB - BroadBand eBook

Supported file type	Description
LRPREV	Lightroom preview data
LRTEMPLATE	Adobe Photoshop Lightroom Template
LS3PROJ	Visual Studio LightSwitch (V3) Project
LSA	Domino Designer Agent
LSC	LOGO!Soft Comfort Circuit
LSD	ABBYY Lingvo dictionary
LSIM	LogicSim circuit (Java ver.)
LSL	SuperMap World GIS Line Style Library
LSM	Linux Software Map entry (gen)
LSMV	Lsnes movie capture
LSPROJ	Visual Studio LightSwitch Project
LSS/16	LSS16 SYSLINUX Splash image
LST	CUPL error Listing
LSXPROJ	Visual Studio LightSwitch Project
LSXTPROJ	Visual Studio LightSwitch project
LSZ	Litestep theme
LTF	Frogans Short-cut
LTN	LinkTreeNote document
LUACODEC	Reason Remote Lua Codec

Supported file type	Description
LVA	Logitech Video Effects Avatar
LVF	Lightweight Video Format video
LVLX	PGE Extendable Level
LVM	LabVIEW Measurement
LVW	Livewire Document
LW	LiteWave compressed audio
LWF	LuraWave Format bitmap
LWO/LW	LightWave 3D Object
LWS	LightWave 3D Scene
LWTP	LimeWire theme
LXF	LEGO Exchange Format - Digital Designer
LXFML	LEGO Digital Designer XML data
LXO	Luxology 3D scene
LXXPLOT	LXBeams Light Plot
LY/ILY	LilyPond music score
LYR	Project Dogwaffle layered bitmap
LYT	PCB Layout
LYX	LyX document
LZ	LZIP compressed archive

Supported file type	Description
LZC	Need for Speed game data
LZH/LHA	LHARC/LZARK compressed archive (generic)
LZMA	LZMA compressed archive
LZO	Izop compressed
LZS	LARC compressed archive
LZT	LzTurbo compressed
LZX	LZX Amiga compressed archive
M	Maple Common Binary file (generic)
M01/P01/R01/S01	MicroStation Modification resource file
M15	thinEdge model
M2	Mesa 2 spreadsheet
M2I	MMC2IEC mapping/container format
M2S	Maxthon skin (MX2)
M2TS/MTS	MPEG-2 Transport Stream video
M3G	Mobile 3D Graphics
M3U	Extended M3U playlist
M3U8/M3U	Extended M3U playlist (UTF-8)
M4	m4 preprocessor / macro source
M4A	Apple Lossless Audio Codec

Supported file type	Description
M4A/MP4	AAC Audio in MP4 container
M4B	iTunes Audio Book
M4P	Protected iTunes Music Store audio track
M4V	iTunes Apple TV Video
M5P	Motus MachFive Preset
M8M	8mam8 model
M99	M99 compressed data
MA	Maya ASCII Scene
MAB	Mozilla Address Book
MAC	MegaCAD Macro
MAE	Maestro molecular model
MAF	Multiple Alignment Format
MAFF	Mozilla Archive Format (gen)
MAFF/ZIP	Mozilla Archive Format (Firefox)
MAG	MAG v2 bitmap
MAKI	Compiled Winamp Maki script
MAL	MadAppLauncher configuration
MAN	Man page
MANI	Mine-imator Project

Supported file type	Description
MANIFEST	Windows Manifest - Visual Stylesheet XML file
MAP	3by5 Index
MAP/CSF	PCRaster map
MAR	MAR compressed archive
MASSEFFECTSAVE	Mass Effect save game
MAT	3D Studio Max Material Library
MATERIAL	OGRE Material
MATHML	Mathematical Markup Language
MAUD/IFF	IFF MacroSystem Audio
MAX	3D Studio Max Scene
MAXC	MaxCrypt encrypted
MAXPAT	Max Patch
MAZ	Hover! maze data
MB	Maya Binary Scene (32bit)
MB1/MBD	BS-DOS MB1 disk image
MB2/MBD	BS-DOS MB2 disk image
MBC	ModBus Configuration
MBD	Multimedia Builder Data
MBF	Microsoft Money Backup file

Supported file type	Description
MBI	MBasic source
MBM	EPOC/Symbian MultiBitMap
MBOX	Standard Unix Mailbox
MBP	Mobipocket eBook Auxiliary data
MBPV2	Amazon Kindle ebook metadata
MBSA	Microsoft Baseline Security Analyser report
MBX	MapInfo MapBasic application eXtension (generic)
MBZ	Moodle Backup
MC	Macrocell format
MC4D/C4D	Maxon Cinema 4D v4.x object
MC9	Mastercam 9 geometry
MCADDON	Minecraft Add-on
MCD	Mathcad document
MCD/MCR	Playstation Memory Card savestate
MCDX	Mathcad Prime Document
MCL	MCell Cellular Automata format
MCLIB	MaxonCAD Library
MCMD	MCMD module

Supported file type	Description
MCML	Media Center Markup Language
MCO	MSN Messenger Wink
MCP	CodeWarrior Project (Big Endian)
MCPACK	Minecraft resources Package
MCR	Compass and Ruler Macro
MCW	MPLAB IDE Workspace
MCW/DOC	Word for the Macintosh/Write for Atari ST document (v1.0)
MCWORLD	Minecraft World
MD	MDCD compressed archive
MD2	Quake 2 model
MD3	Quake III Arena model
MD5ANIM	Doom 3 MD5 Animation
MD5MESH	Doom 3 MD5 Mesh
MD8	Mediator Project
MDA	MicroDesign Area bitmap (AREA2)
MDAT	The Final Musicsystem eXtended module (pattern)
MDB	Microsoft Jet DB
MDC	Merkaartor Document

Supported file type	Description
MDD	MDict resource
MDF	Microsoft SQL Server database (generic)
MDI	Microsoft Document Imaging format
MDJ	StarUML Model
MDL	CA-Compete! Model (v4.0)
MDR	MagicDraw UML project
MDS	Media Descriptor
MDSX	MonoDevelop Solution
MDU	D-Flow FM Model Data
MDV	QLAY MDV image
MDW	Microsoft Jet DB Workgroup Information
MDXML	Magic Draw UML model
ME	TROFF markup
ME/MEW	Multi Edit configuration
ME1	MagicEngine savestate
ME3	Arcsoft MultiMedia Email 3.0 message
MEB	Open eBook
MED	Music Editor module
MED/MMD0/MMD1/MMD2/MMD3/MMDC	MED/OctaMED Amiga module

Supported file type	Description
MEG	MEGA data format
MEI	Music Encoding Initiative format
MELLEL/MELL	Mellel document
MEM	Mnemosyne database
MER	Entity-Relationship (ER) Diagram
MERLIN2	Merlin Project
MET	HEC-HMS Metereologic model configuration
META	Unity asset Meta data
METALINK	Metalink file
MEX	Macro Express Macro
MEXW32	MATLAB Windows 32bit compiled function
MEXW64	MATLAB Windows 64bit compiled function
MF	Java Manifest
MFA	MultiMedia Fusion 2 Application
MFCRIBBON-MS	MFC Ribbon definition
MFIL	Blizzard Manifest
MFL	Mozilla XUL FastLoad File
MFT	Battlefield Bad Company package manifest
MG1/MG2/MG4/MG8	MultiArtist bitmap

Supported file type	Description
MGB	Paragon 5 Gameboy Tracker module
MGF	L3DT Map Group File
MGOURMET3	MacGourmet 3 document
MGR	MGR bitmap (modern, 8bit aligned)
MGS	MSX Gigamix MGSDRV3 music
MGT	Megatracker module
MHD	MetaImage MetaHeader
MHT	MIME HTML archive format
MHT/MHTML	MIME HTML archive format (var 2)
MID	MIDI Music
MIDNAM	MIDI patch name
MIF	Maker Interchange Format
MIF/MIFF	ImageMagick Machine independent File Format bitmap
MIG	Mighty Draw drawing
MINI2SF	2SF Nintendo DS Sound Format rip (Mini)
MINIBANK	Mini V preset
MININCSF	NCSF Nitro Composer Sound Format rip (Mini)
MINIPSF	PSF1 Playstation Sound Format rip (Mini)

Supported file type	Description
MINIPSF2	PSF2 Playstation 2 Sound Format rip (Mini)
MINIQSF	QSF Capcom QSound Format rip (Mini)
MINISNSF	SNSF Super Nintendo Sound Format rip (mini)
MINISSF	SSF Saturn Sound Format rip (mini)
MINIUSF	USF Ultra64 Sound Format rip (mini)
MIO	MIO compressed audio
MIS	McGrath Information Solution metadata
MITSU	Mitsubishi S340-10 bitmap
MIX	Atari Digi-Mix module
MIZ	DCS Mission
MJ2/MJP2	Motion JPEG 2000 video
MJP	J.River Media Center plugin
MK2/MKII	Mark II Sound-System module
MKA	Matroska Audio stream
MKD	CAD6 Drawing
MKF	KaraBox Karaoke song
MKL	CAD6 Library
MKV	Matroska Video stream
MKW	mkwACT lossless compressed audio

Supported file type	Description
ML	Musicline module
MLAPPINSTALL	MATLAB app installer
MLB	MyLittleBase database
MLL	Maya plug-in (generic)
MLM	MolMeccano molecule
MLP	Meridian Lossless Packing audio
MLPKGINSTALL	MATLAB support package
MLR	MK Jogo Replay
MLS	Skype localization data
MLV	Magic Lantern raw Video format v2.0
MLX	MeshLab filter script
MM	FreeMind mind map
MM8	MusicMaker v8 module
MMAP	MindManager Brainstorm and Process Control Map
MMD	Cumulate Draw's editable MMD format
MMDB	GeoLite2 IP geolocation database
MMF	MathMagic equation File
MML	Aleph One Marathon Markup Language

Supported file type	Description
MMM	Adobe Type Manager Multiple Master Metrics
MMMS	MetaMind Machine Sequence
MMO	Hyper File memo
MMP	LMMS Project
MMPZ	LMMS Project Zipped
MMW	AceMoney data
MMZ	MiraMon compressed data
MN	MuPAD Notebook
MNC	MINC1 Medical Imaging format
MND	Fractal Forge 2.x fractal parameters
MNG	Multiple-image Network Graphics bitmap/anim
MNU/IN1/MB0/MB1/PB0/PB1	UltraEdit Menu
MO3	MO3 module
MOBI/PRC	Mobipocket - PRC Palm e-Book
MOD	Digital Tracker 4-channel module
MOD/TEXT/TOOL	Oberon System 3 text document
MODD	Picture Motion Browser data
MODE1V3	Xcode project data
MODE2V3	Xcode project data

Supported file type	Description
MODEL	CATIA model
MODFEM	Femap Model
MOFLEX	Mobiclip for Nintendo CTR
MOGG	Rock Band multi track music
MOGRT	Adobe Motion Graphics Template
MOL2	Tripos Mol2
MOLDEN	Molden Format
MON	M.O.N New module
MOP	MOP report
MOS	Infinity Engine compressed graphic (v1)
MOTIF	MacStitch/WinStitch Motif
MOU	WinMount archive
MOV	Knowledge Adventure MoVie video
MOV/QT	QuickTime Movie
MP2S	Max Payne 2 saved game
MP4	ISO base media container
MP4/STEM	Native Instruments Stems audio
MPB	MyPhoneExplorer Backup
MPC	Electronic Arts MPC video

Supported file type	Description
MPCPL	MediaPlayer Classic Playlist
MPD	DASH Media Presentation Description
MPEX/TXT	Mass Properties Exchange data
MPF	MainActor project
MPG	MPEG2 Video File recorded by ProgDVB
MPG/MPEG	MPEG video
MPHBIN	COMSOL Multiphysics mesh (bin)
MPHTXT	COMSOL Multiphysics mesh (txt)
MPI	InstallJammer Project
MPK	Project64 Memory Pack
MPL	AVCHD Playlist
MPO	Multi-Picture Object bitmap
MPP	Microsoft Project
MPPZ	MagicPlot Project
MPS	Garmin MapSource data
MPW	WordPerfect Executive Spreadsheet
MPX	Microsoft Project exported data
MQ4	MetaQuote / MetaTrader indicator
MQL	MetaTrader indicator

Supported file type	Description
MQO	Metasequoia 3D scene
MQV	Sony / Mobile Quicktime Video
MRB	Multiple Resolution Bitmap
MRF	Meta Raster Format XML metadata
MRP	China Mobile application
MRT	Stimulsoft Reports report
MRW	Minolta Dimage RAW image
MRX	DCMOTO save state
MS1	VirtualBus Map
MS3D	MilkShape 3D model
MS8/MS9/MS10	MultiSim Design (generic)
MSA	Atari MSA Disk Image
MSC	Microsoft Management Console Snap-in control file
MSCX	MuseScore music score
MSCZ	MuseScore compressed music score
MSDVD	Windows DVD Maker project
MSE-INSTALLER	Magic Set Editor Installer
MSE-SET	Magic Set Editor Set

Supported file type	Description
MSF	Mozilla Mail Summary file
MSH	Fluent mesh
MSI	Microsoft Windows Installer
MSKIN	Maxthon skin (MX1)
MSL	Mapping Specification Language (ASCII)
MSM	Windows Installer Merge Module
MSO	ActiveMime object
MSQ	Mario Sequencer song
MSRCINCIDENT	Remote Assistance Request
MSS	Advanced Mario Sequencer Song
MST	Room Arranger design
MSU	Windows Update Package
MSWMM	Windows Movie Maker project
MT2	MadTracker 2 module
MT5	Poser Material (V5)
MTC	MTC chiptune
MTE	TargetExpress target
MTF	Mediatek Font
MTL	Alias Wavefront material

Supported file type	Description
MTM	MultiTracker module
MTP	EasyBuilder8000 project
MTS	AVCHD video clips - MPEG Transport Stream
MTV	MTV video
MTW	Minitab Worksheet
MTX	Matrix spreadsheet
MTZ	MIUI Theme
MUG	Digital Mugician 2 module
MULIB	Muse Library
MULTISAMPLE	Bitwig Studio multisample
MUM	Windows Update Package
MUP	MindMup Mindmap
MUS	Doom/Heretic music
MUS/ETF	Finale ETF Enigma Tansportable File
MUS/MYR	Myriad Harmony / Melody assistant music
MUSE	Emacs Muse project
MUSIC	SuperTux Music
MUSINK	Musink music score
MUX	MUX video

Supported file type	Description
MV	Miva Script
MV/MOVIE	SGI movie format
MV3	AUPEC encoded audio
MVA	Setup Program Archive
MVB	Multimedia Viewer Book
MVC	Collectorz.com Movie Collector data
MVDX	MindView Windows Document
MVE	Interplay MVE video
MVEX	Muvee autoProducer 6 project
MVG	Magick Vector Graphics
MVM	MVX Module
MVPL	Microsoft Visual Programming Language project
MVS	MusicMatch JukeBox Visualization (v1.0)
MW	Maple XML Worksheet
MW2	MicroWorlds LOGO Activity
MW4	MechWarrior 4 game data
MWB	MySQL Workbench model archive
MWD	Mariner Write Document

Supported file type	Description
MWDECK	Magic Workstation Deck
MWM	Space Engineers Model
MWP	STEP7-Micro WIN PLC Program
MWS	Maple worksheet
MWZ	Maple compressed Worksheet
MXD	ArcMap GIS project
MXF	Material Exchange Format
MXMF/XMF	eXtensible Music File Format
MXP	Macromedia Extension Package
MXR	MatrixREDUCE 2.0 PSAM XML format
MXS	Maxwell Render Scene
MXTX	MaxTrax module
MYAPP	VisualStudio MyApp
MYI	MySQL MyISAM tables index
MYO	MYOB data
MYS	Mystic BBS install package
MZ	MOZART Music Document
MZF	MediaZip compressed archive
MZML	MzML

Supported file type	Description
MZP	MOZART Percussion map
MZTAB	mzTab format
MZX	MegaZeux game
MZXML	mzXML format
N2P/N2V	Nebula Program / Vector
N3M	Nokia 3D Map
NAB	Novell Groupwise Address Book
NAP	NAPLPS graphics
NAS	Nastran input data
NATVIS	Visual Studio Natvis visualization
NB	Mathematica Notebook (headerless)
NB/NBP	Mathematica Notebook
NBF	NVIDIA Scene Graph binary
NBI	Ahead Nero BackItUp file (v1.x)
NBKT	Native Instruments BATTERY kit
NBM	NetBeans Module
NBU	Nokia phone BackUp
NBZ	C64 NBZ disk image
NC	mcrypt encrypted

Supported file type	Description
NCB	Microsoft C/C++ program database
NCC	NI Controller Configuration
NCD	Nero CoverDesigner
NCER	Nintendo Cell Resource
NCM	NI MASCHINE template
NCM2	NI MASCHINE MK2 template
NCMM	NI MASCHINE MIKRO template
NCMM2	NI MASCHINE MIKRO MK2 template
NCP	Nikon Custom Picture Control
NCS	KOTOR (Knight Of The Old Republic) compiled script
NCSFLIB	NCSF Nitro Composer Sound Format rip
NCT	Ahead Nero CoverDesigner Template
NCX	Navigation Control file for XML
NDB	SeeYou Waypoint
NDF	Channel Data File
NDM	Enemy Territory: Quake Wars demo
NDPA	NanoZoomer Annotation
NDPI	Hamamatsu NanoZoomer Digital Pathology Image

Supported file type	Description
NDX	WinDev Index
NED	Nerdtracker II module
NEF	Nikon raw image
NEO	Atari NeoChrome bitmap
NEPPRJ	NEPLAN Project
NES	Nintendo Entertainment System ROM
NET	Epanet data file
NEU	Gambit Neutral file
NEX/NXS	NEXUS format
NEXE	Google NaCl Executable (x86)
NF	Faase Paint-by-Numbers puzzle format
NFC	Nokia PC Suite Content Copier file
NFF	Haines NFF scene
NFG	Gambit strategic N-player Game File Format
NFM8	Native Instruments FM8 patch
NFO	Folio Views Infobase
NFZ	JB BAHN vehicle
NG	Norton Guide
N-GAGE	N-Gage 2.0 on-device installation

Supported file type	Description
NGB	NonoPocket nonogram
NGC/NGD/NGM	Xilinx Netlist
NGC/NGP/NPC	NeoGeo game cartridge (var 1)
NGG	Nokia Group Graphics bitmap
NGRR	Native Instruments Guitar Rig 5 preset
NGS	NGPocket savestate
NIB	Apple Interface Builder NIB archive (XML)
NIC	NeoDesk icon (compressed)
NII	NIfTI-1 data format (big endian)
NITF/NTF	NITF National Imagery Transmission Format image (generic)
NJA	Seifert ASCII pole figure format
NK	Nuke script
NK2	Outlook Nickfile
NKPLE	Nuke script (encrypted)
NKTRL_SET	KORG Kontrol Editor Settings
NKTRL2_DATA	KORG nanoKONTROL2 Editor data
NL2PARK	NoLimits 2 Park
NL2PKG	NoLimits 2 Package

Supported file type	Description
NLM	Netware Loadable Module
NLTRACK	NoLimits Track
NM2	Navitel 3.1 Map
NMEA/NMA	NMEA GPS log data
NMF	Nikon Movie File
NML	Traktor collection
NMSV	Native Instruments Massive Sound
NMV	Nintendulator movie capture
NNB	LigPlot Non-Bonded contacts data
NOA	Nancy Codec video
NOL	Nokia Operator Logo bitmap
NOTEBOOK	SMART Notebook
NOV	Battery 3 quick load sample data
NPK	MikroTik RouterOS Upgrade Package
NPL	Xilinx Integrated Software Environment Project
NPM	Corel Custom Natural Media Stroke
NPP	Art Explosion Publisher Pro document
NPS	Natron Node Preset
NPW	nPassword DataBank (w/o password)

Supported file type	Description
NPY	NumPy data
NQI	ESET Smart Security Quarantined file Information
NR3	Nero MP3 ISO Compilation
NRA	Nero Audio-CD Compilation
NRG	Nero BurningROM CDImage
NRI	Nero ISO Compilation
NRKT	Native Instruments Reaktor sample
NRRD	Nearly Raw Raster Data
NRV	Nero Video-CD compilation
NS1	NetStumbler NS1 log
NS2P	Nord Stage 2 Program
NS2PB	Nord Stage 2 Program Bundle
NSF	Lotus Notes database
NSFE	Extended Nintendo Sound Format chiptune
NSI	NSIS script (with rem)
NSL	Nokia Startup Logo Editor bitmap
NSLA	Nero Scalable Audio
NSMP	Nord User Sample

Supported file type	Description
NSP	Computerized Speech Lab NSP audio
NSPG	Nord Stage Classic/EX Program
NST	Nestopia savestate
NSV	Nullsoft Streaming Video
NSX	Index Apollo Database Engine
NT	Startrekker 1.x module info
NT3	JB BAHN layout
NTF	Font descriptor
NTH	Nokia theme
NTM	Navitel 2.0 Map
NTP	NovoTrade Packer module
NTT	Neato MediaFACE label template
NTW	Lode Data Network
NUMBERS	Numbers spreadsheet
NUNIT	NUnit project
NUP	NOD32 Antivirus Update file
NUPKG	NuGet Package
NUSPEC	NuGet Specification
NUT/SAN	Smush Animation format (old)

Supported file type	Description
NUV	NuppelVideo (MythTV) video
NV	Juno address book
NVB	NVIDIA Scene
NVDL	NVDL script
NVF	Creative Nomad II series MP3 players Voice File audio
NVRAM	VMware BIOS state
NWC	NoteWorthy Composer song
NWD	NavisWorks Document
NWP	Neo Content file
NX1	NexusDB database
NXV	NXV video
NY	Audacity Nyquits plug-in
NYF	myBase database
NZ	NanoZip compressed archive
NZB	Newzbin Usenet Index
O	ELF Executable and Linkable format (generic)
O/OBJ	Intel 80386 Common Object File Format (COFF) object
O2C	Objects to See 3D object

Supported file type	Description
OAD	Notaro document
OB3	ORTIM Zeit data
OBD	Office Binder Document
OBJ	Blender 3D object
OBJ/A	Common Object File Format (COFF) Library
OBML	Opera Binary Markup Language
OBML16	Opera Mini saved page
OBO	PSI MI format
OBP	Bryce Object Presets
OBPACK	ObjectBar theme
OBSP	Oberheim SEM V preset
OCC	DB/TextWorks Database Terms and Words
OCD	OCAD map
OCF	Oberon/F Code File
OCI	OpenCanvas Image
OCT	Radiance Octree
OCX	Windows ActiveX control
ODB	OpenDocument DataBase (generic)
ODC	Oberon/F Document

Supported file type	Description
ODCL	Open Dialog Control Language for AutoCAD
ODEX	Optimized Dalvik Executable
ODF	OpenDocument Formula
ODG	OpenDocument Graphics document
ODM	OpenDocument Master Text document
ODP	OpenDocument Presentation
ODS	OpenDocument Spreadsheet document
ODT	MindRender VREK Object File Format
ODTTF	Obfuscated subsetted Font
ODV	Ocean Data View data (TXT)
OEMODEL	Seene 3d model (v2)
OFC	Open Financial Connectivity
OFF	OFF geometry definition
OFM	OmniForm Form
OFNT	IFF Outline Font
OFP	Origin Function Plot
OFR/OFS	OptimFROG encoded audio
OFT	Outlook Form Template
OFW	TopLevel Forms Form

Supported file type	Description
OGG	OGG Vorbis audio
OGM	OGG Media stream
OGP	PlayStation RSD Object Group (gen)
OGV	Ogg Vorbis Video
OGV/OGG	Ogg Theora video
OHT	Oracle Help for Java mapping
OIV	OpenIV mod package
OKT/OKTA	Oktalyzer module
OLB	OrCAD PSpice Capture Symbols Models
OLEO	Oleo spreadsheet
OLRW/OLR	Openlab Raw Format
OMA	Sony OpenMG Audio (SonicStage)
OMF	Onyx Music File module
OMF/OMFI	Open Media Framework Interchange
OMOD	OpenMRS Module
OMP	OpenMusic Patch
OMR	openMSX replay (ungzipped)
OMX	OMAX Make tool path data
ONB	OpenModelica NoteBook

Supported file type	Description
OND	Lotus Notes Encapsulated Memo
ONE	Microsoft OneNote note
ONEPKG	Microsoft OneNote Package
ONETOC2	OneNote table of contents
OOM	PowerDesigner Model
OOP	OOP compressed archive
OPA/OPO/APP	Psion Object/OPL Output
OPAM	OPAM package info
OPC	Office Upgrade Control file
OPD	Durango Interferometry data
OPF	Obsidium Project File
OPJ	OrCAD Project
OPK	Origin Pack file
OPL/OPH/OXH	EPOC OPL source
OPML/XML	Outline Processor Markup Language
OPO	EPOC OPL Object module
OPPC/OPPS3	Darksiders game data package
OPS	Office Profile-Settings (v1.1)
OPUS	Opus compressed audio

Supported file type	Description
OPX	EPOC OPL eXtension
OPY	OptiY Model
ORA	OpenRaster bitmap
ORC	Csound Orchestra
ORF	Olympus digital camera RAW image (IIRO)
ORG	Creative Music System Intelligent Organ music
OSF	Oberon/F Symbol File
OSG	Open Scenegraph scene
OSM	OpenStreetMap XML Data
OSP	OpenShot Project
OSQ	Original Sound Quality audio
OST	Outlook Exchange Offline Storage
OSU	Osu! script
OTF	OpenType Font
OTP	OpenDocument Presentation Template
OTRKEY	OnlineTVRecorder (OTR) Keyfile
OTS	OpenDocument Spreadsheet template
OTT	OpenDocument Text Document template
OTZ	OpenLP Theme

Supported file type	Description
OUT	Lua 4.0 bytecode
OUT/TXT	Wireshark traffic log
OUTJOB	Altium Designer Output Job
OVA	Open Virtualization Format package
OVD	ObjectVision Datafile
OVE	Cakewalk Overture Score
OVF	OOMMF Vector Field 1.0 format
OVL	C-Worthy Machine Dependant Overlay (v1.x)
OVPN	OpenVPN profile (var.1)
OVR	Borland Overlay
OVX	Psion OVAL Control
OXP	OmniRush eXtended Package
OXPS/XPS	Open XML Paper Specification
OXT	OpenOffice Extension
OXYGENE	Oxygene Project
OZF	Mozart functor
OZF2	OziExplorer Map
OZV	ORTIM Zeit project
P	MATLAB p-code

Supported file type	Description
P00/S00/R00/U00	PC64 flexible container format
P24	Bitmapped Signum!2 printer font (24 Pins)
P2F	Eclipse Plugin list
P2G	Power2Go project
P2I	Power2Go Image
P3T	PlayStation 3 Theme
P40	The Player 4.0a module
P41	The Player 4.1a module
P4X	The Player 4.x Music
P5D	Planner 5D Project
P5M	Image Packaging System Manifest
P5P	Solaris Image Packaging System
P60	The Player 6.0a module
P65	Adobe PageMaker document (v6.5)
P7	Xv's Visual Schnauzer bitmap
P7S	PKCS #7 Signature
P8	PICO-8 cartridge
P9	Bitmapped Signum!2 printer font (9 Pins)
PA	PrintArtist project

Supported file type	Description
PACK	Git pack format
PACKAGE	Maxis package/archive
PAD	Boeing Calc WorkPad (v3.x)
PAE	PowerArchiver Rijndael Encrypted file
PAG	RealTick page
PAGES	Pages document
PAK/ARC	PAK/ARC Compressed archive
PAL	DIV Games Studio Palette
PAL/PSPPALETTE	JASC format Palette
PAM	Portable Arbitrary Map bitmap
PAN	Panorama database
PANDO	Pando Package
PAP	Fractal Design Painter Paper texture
PAQ8F	PAQ8F compressed archive
PAQ8JC	PAQ8JC compressed archive
PAQ8O	PAQ8O compressed archive
PAR	Aerofly model parameters
PAR2	Parity Archive Volume Set (Par2)
PAT	Adobe Photoshop Pattern

Supported file type	Description
PATCH	RCS/CVS diff output
PAX	PAX password protected bitmap
PBC	Parrot ByteCode
PBD	PowerBASIC debugger symbols
PBF	Paragon Backup Format image
PBI	PC-BSD Installer Package
PBIX	Power BI report
PBJ	Pixel Bender bytecode
PBK	Microsoft PhoneBook
PBLIB/SLL	PowerBASIC Static Link Library
PBN	Portable Bridge Notation (gen)
PBP	Phoenix Visual Designer project
PBR	PowerBASIC resource
PBT	PocketBook Theme
PBTX	PowerBuilder .NET Target
PBU	PowerBASIC/DOS Compiled Unit
PBW	Pebble Watchface
PBXPROJ	Apple Project Builder Xcode Project
PBXUSER	Apple Xcode User data

Supported file type	Description
PBZ	Pebble firmware
PC1	DEGAS low-res compressed bitmap
PC3	AutoCAD Plotter Configuration
PCB	ACCEL Printed Circuit Board (ASCII)
PCBDOC	Altium Designer PCB Document
PCBLIB	Protel PCB 3.0 Binary Library
PCD	Kodak PhotoCD bitmap
PCF	Cisco VPN Profile Configuration File
PCG	Korg Trinity/Triton instruments bank (generic)
PCH	IFF binary Patch
PCH2	Nord Modular G2 Patch
PCL	Pencil project
PCL/PRN	HP Printer Command Language (ESC+E)
PCM/PCS	Pfaff Compatible design card
PCO	PC-Outline outline
PCP	AutoCAD Plotter Configuration
PCS	Microsoft PowerPoint Picture Storage
PCSAV	Mass Effect 2 save game
PCT/PICT/PIC	QuickDraw/PICT bitmap (v1)

Supported file type	Description
PCU	XProfan Compiled Unit
PCV	MozBackup backup file
PD	PipeDream document
PD3	Denso BHT PD3 Image File / Program
PDB	BGBlitz position database
PDC	Pebble Draw Command image
PDD	PhotoDeluxe image
PDE	Prescription Drug Event format
PDF	Adobe Portable Document Format
PDFXML	Adobe PDFXML document
PDG	Chaoxing SSReader Digital Library e-Book
PDM	PowerDesigner Model
PDM/ACC	DeskMate Program/Accessory executable (v3.x)
PDN	Paint.NET Image (v3)
PDO	Pepakura Designer work
PDS	PALASM Design Description
PDSPRJ	Proteus Project
PDT	PDT structure definition

Supported file type	Description
PDU	Protocol Data Unit message data
PDX	Adobe Portable Document Catalog Index 2.0
PE	PETSCII Editor screen
PE4	Ulead thumbnail
PEC	Brother/Babylock/Bernina Home Embroidery format
PECOM	Pecom 64 program
PEF	Pentax raw image
PEG	Peggle replay
PEGN	Peggle Nights replay
PEK	Adobe Premiere Peak Waveform
PERLAPP	PerlApp settings
PERSPECTIVE	Xcode perspective
PERSPECTIVEV3	Xcode perspective (V3)
PES	Brother/Babylock/Bernina Home Embroidery Format
PEZ	Prezi Desktop presentation
PF	Microsoft Windows 8 Prefetch data
PF2	GRUB2 font
PFA	Postscript Type 1 Font

Supported file type	Description
PFB	Adobe PostScript Type 1 Font
PFD	Playstation 3 savegame control data
PFF	Formatta Portable Form File
PFG	jEEPers Program Configuration file (with rem)
PFL	PhotoFilter plugin
PFM	Adobe Printer Font Metrics
PFT	ChiWriter Printer Font
PFV	PhotoFiltre path
PGC	PGN (Portable Gaming Notation) Compressed format
PGM	Opentech Digital STB main software
PGML	Precision Graphics Markup Language
PGMX	ProbModelXML model
PGN	Portable Gaming Notation
PGO	Papagayo lipsync info
PGS	PageStream document
PGX	PGX JPEG 2000 bitmap
PHB	CMN Phonebook
PHC	Home Embroidery Format

Supported file type	Description
PHF	Photo Font
PHJ	PhCNC project
PHN	Phun scene
PHO	Gerber Photoplot
PHP	PHP source
PHPPROJ	Visual Studio PHP Project
PHPRJ	RadPHP Project
PHR	iGO Phoneme data
PHX	Advanced Gravis Phoenix configuration
PI	Pi bitmap
PIB	PIM Backup
PIC	Bio-Rad Image(s) bitmap
PIC/CLP	PC Paint/Pictor bitmap
PICT	Macintosh Quickdraw/PICT Drawing
PIF	Program Information File (Windows)
PIGM	Packaged Indigo Renderer Material
PIKA	Pika Software Builder Project
PIM	PIM compressed archive
PIS	Beni Tracker module

Supported file type	Description
PISKEL	Piskel sprite
PIT	Odin Partition Information Table
PIXEXP	PIX Experiment
PIXICODE	Pixilang compiled byte-code
PJG	packJPG compressed JPEG bitmap
PJM	PSXjin movie capture
PK3	Quake 3 game data
PKE/PKN	Extron IP Link driver
PKG	BeOS installation package
PKINFO	ArcGIS Package Info
PKM	GrafX2 bitmap
PKPASS	iOS Passbook Pass
PKPROJ	Visual CScript Project
PKR	Pretty Good Privacy (PGP) Public Keyring
PL	PROGRESS Procedure Library (v11)
PLAN	Chief Architect plan
PLANNER	Planner project
PLAYER	2D Fighter Maker 2nd player data
PLB	PhotoLine browse index

Supported file type	Description
PLBM	IFF Planar Bitmap
PLD	CUPL PLD Program format
PLE	Messenger Plus! Encrypted chat log
PLG	Aston Shell plugin
PLIST	XML Property List
PLM	Disorder Tracker 2 module
PLN	Microsoft Flight Simulator Flight Plan
PLP	Messenger Plus! Sound Pack
PLS	PenCell Spreadsheet
PLSC	Messenger Script Pack
PLSK	Messenger Plus! Skin Pack
PLT	Gerber Scientific plot
PM0	DeLorme map data
PM3	Crouzet Logic Software M3 project
PM4	Aldus PageMaker document (v4)
PM5	Aldus PageMaker document (v5)
PM6	Adobe PageMaker document (v6)
PMA	PMarc compressed archive
PMB	Print Magic Banner

Supported file type	Description
PMC	Print Magic Card
PMD	PMDraw drawing/presentation
PME	Pixela Digital Picture
PMF	Print Magic Font
PMG	Photomerge Composition
PML	Palm Markup Language
PMP	AutoCAD Plotter-Modell Parameter
PMR	PhotoModeler project
PMS	AliceSoft PMS bitmap
PN	PokeyNoise chiptune
PNA	TomTom PNA map info
PNACH	PCSX2 Patch
PNC	Panasonic Network Camera compressed images
PNF	Windows precompiled INF
PNML	Workflow Petri Net Designer project
PNPROJ	Programmer's Notepad Project
PNPS	Programmer's Notepad State
PNT	DeskMate Paint image

Supported file type	Description
POD	Plain Old Documentation format
PODSPEC	Pod Specification
POF	Programming Object File
POL	InnovMetric Software Polygon Model
POLY	Caligari TrueSpace Polyline (v2.x)
POM	Maven Project Object Model
PONT	Protege classes
POR	SPSS Portable ASCII Data
POSTBUILD	Xenocode Postbuild settings
POT	Fractint Continuous Potential Image
POV-STATE	Persistence of Vision state
PP1/PP2/PP3	Picture Packer bitmap
PP2	Ping Plotter Sample file
PP3	RawTherapee Postprocessing Profile
PPAM	PowerPoint Macro-enabled Open XML add-in
PPD	PostScript Printer Description
PPENC	Ashampoo Magical Security encrypted
PPF	Micrografx Picture Publisher document
PPG	Programmer's Notepad Project Group

Supported file type	Description
PPJ	Premiere project
PPK	PuTTY Private Key
PPM	Portable PixMap bitmap (ASCII)
PPN	packPNM compressed BMP bitmap
PPP	CyberLink PowerProducer Project
PPR	Photodex ProShow Workspace
PPRJ	Protege Project
PPS/PPT	Microsoft PowerPoint document
PPT	Microsoft PowerPoint (v2.0)
PPTM	PowerPoint Microsoft Office Open XML Format document (with Macro)
PPTX	PowerPoint Microsoft Office Open XML Format document
PPV	Pocket PowerPoint
PPX	PingPlotter script
PPZ	PowerPoint Presentation
PQF	Corel Presentations file
PR	Javelin Printer driver
PR0	DCS device Profile
PR2	Aldus Persuasion Presentation (v2)

Supported file type	Description
PR4	Harvard Graphics Presentation
PRC	PMD 85 emulator recording
PRD	Microsoft Printer Definition
PREFS	Amiga Preferences
PREXPORT	Premiere Export preset
PRF2	Nord Modular G2 Performance
PRFPSET	Adobe Premiere Effect Preset
PRJ	3D Project file (generic)
PRJPCB	Altium Designer project
PRM	The Print Shop Deluxe graphic
PRO	APE ProSystem Atari 8-bit disk image
PROCSPEC	SpectraSuite data
PROJ	BeOS CodeWarrior Project
PROJECT	Gambas Project
PROJECTMGR	ISE Project configuration
PROPERTIES	HSQLDB configuration
PROVBANK	Prophet V preset
PRPRESET	Adobe Premiere Preset
PRPROJ	Premiere Project

Supported file type	Description
PRS	SNS-HDR Preset
PRT	MegaCAD Project
PRTL	Adobe Premiere Title
PRU2	Prorunner 2.0 Music
PRX/WME	Windows Media stream profile
PRZ	Lotus Freelance Graphics
PS	Postscript document
PS1XML	Windows PowerShell formatting
PSC	Spectrum Pro Sound Creator chiptune
PSCI	PETSCII character graphics
PSD	Adobe Photoshop image
PSEG/PSE	IBM Printer Page Segment
PSESS	Visual Studio Performance Session
PSF/PSFLIB	PSF Playstation Sound Format rip
PSF2/PSF2LIB	PSF2 Playstation 2 Sound Format rip
PSH	Photodex ProShow Show file
PSI	PCE Sector Image disk image
PSID/SID	SID tune
PSK	Unreal Engine character

Supported file type	Description
PSL	Pattern Space Layout format
PSM	Epic Megagames MASI module (new format)
PSMDCP	NuGet Package Service MetaData Core Properties
PSO	Particle Systems 3D Object
PSO/VSO	Direct3DX9 Shader (4.09.00.1126)
PSP/PSPIMAGE	Paint Shop Pro Image
PSR	PowerSoft DataWindow - DataStore
PSSG	EGO Engine Textures
PST	LightWave 3D Preset
PSU	PSU Designer 2 project
PSV	Playstation 2-3 Save game
PSWX	Portable Password Depot XML data
PSX	Playstation single game save
PSY	Psycle module
PSYEXP	PsychoPy 2 Experiment
PT	Kodak Precision Transform
PT2	Picatune 2 soundtrack
PT3	Spectrum Pro Tracker 3 chiptune

Supported file type	Description
PT36	ProTracker 3.6x module
PTB	Power Tab Guitar and Bass Tablature Editor
PTCOP	PxTone Collage module
PTF	LiveNote Portable legal Transcript File
PTG	Ambient Design ArtRage project
PTK	Pro Trekkrr 2.0 module
PTL	Premiere title
PTM	Microsoft MapPoint map
PTN	TrendMicro HouseCall Cleaner database
PTO	Hugin Project
PTP	PMD 85 emulator tape image
PTS	PTgui project
PTTUNE	PxTone Collage module (protected)
PTX	RealLegal E-Transcript
PUB	ClickArt Personal Publisher document
PUBLISHPROJ	MSBuild website Project
PUBXML	Visual Studio Publish profile
PUD	WarCraft map (v2)
PUMPKIN	Pumpkin Shop stencil

Supported file type	Description
PUP	Puppy Linux DotPup installer package
PURBLEPAIRSSAVE-MS	Microsoft Purble Pairs Saved game
PURBLESHOPSAVE-MS	Microsoft Purble Shop Saved game
PUT/INS	Microfox Company PUT compressed archive
PUZ	Across crossword puzzle
PVC	Panasonic Voice Container
PVD	PV3D scene description data
PVE	GoBe Productive Document (gen)
PVM	OSTA.org MusicPhotoVideo
PVN	Design and Print Business Edition document
PVR	Dreamcast PVR texture format
PVR/SPR	Dreamcast VR texture
PVSM	ParaView state
PVT	PlayStation RSD Pivot (gen)
PW	Pathetic Writer document
PWB	Password Boss data
PWC	Piecewise-Constant Image Model bitmap
PWD	Password Commander Pro database (v2.x)
PWF	PageWunder document

Supported file type	Description
PWI	Pocket Word document
PWL	Windows 95 passwords
PWM	Seattle FilmWorks / PhotoWorks photo Meta file
PWP	Seattle FilmWorks / PhotoWorks photos
PX	PC-Axis data (var 1)
PXD	Pxlab experiment Design
PXE	Preboot Execution Environment
PXF	Phoenix RC simulator flying site
PXI	Pixie drawing / paint
PXL	Pocket Excel sheet
PXM	PCSX movie capture
PYA	PlayReady audio
PYC	CPython 1.x bytecode
PYD	Python Dynamic module
PYO	Python optimized code
PYV	PlayReady video
PZ	pzip compressed
PZ2	Poser pose

Supported file type	Description
PZ3	Poser scene
PZA	Roxio/MGI PhotoSuite Album
PZF	GraphPad Prism project
PZFX	GraphPad Prism XML document
PZP	Roxio/MGI PhotoSuite Project
PZX	Perfect ZX Tape image
Q/PAK	Quantum compressed archive
Q3C	Quick 3D Cover project
Q3O	Quick3D Model
Q4	XLD4 bitmap
QAT	Office Quick Access Toolbar info
QBB	Intuit QuickBooks Backup
QBW	Intuit QuickBooks for Windows
QCF	Q-emulator Configuration
QCOW/IMG	QCOW disk image (gen)
QCOW2/IMG	QCOW2 disk image
QCP	QualComm PureVoice
QDA	Quadruple D Archiver compressed archive
QF	Ovi Maps info

Supported file type	Description
QFILTER	Apple Quartz Filter
QIC	Windows 98 MSBackup backup set
QIF	Quality Information Framework document
QIP	Altera Quartus IP
QLB	Microsoft Basic 7.x Quick library
QLI	Statler Stitcher
QLPAK	Q-emuLator Package
QM	Qt Message
QMBL	LabQuest results
QMG	Qmage encoded data
QOP	3ds Quad colors
QP03	qpress compressed archive
QPU	Microsoft QuickPascal Unit
QPW	Quattro Pro for Windows spreadsheet
QR2	Delphi QuickReport
QRC	Qt Resource Collection
QRM	Allen Communications Quest Released Module (v5)
QRP	QuickReport Report

Supported file type	Description
QRS	SlickRun MagicWord Pack
QSD	Quicken Win Data
QSF	Quintessential Player Family Skin
QSFLIB	QSF Capcom QSound Format rip
QSK	Quintessential Player Kid Skin
QST	HeroQuest Quest
QSYS	Qsys System
QTCH	Quicktime Cached data
QTIF/QIF	QuickTime Image Format bitmap
QTL	QuickTime Media Link
QTP	QuickTime Preferences
QTT	Qtracker Theme
QTZ	Quartz Composer data
QUERY	Microsoft PCHealth query
QUEST	Quest adventure
QVW	QlikView document
QW	QandA Write for Windows document (v3.0)
QWC	QuickBooks Web Connector configuration
QWK	QWK offline mail packet (ZIP compressed)

Supported file type	Description
QWS	Quartus Workspace
QX	Quexal sourcecode
QXD	Quark XPress document
QXM	Quexal macro
QZD/QZE/QZS	QuizPro quiz data
R	Twist 2 Report
R2D	Reflex 2 Database
R2R	Reflex 2 Report
R2SKIN	Rainlendar 2 Skin
R3D	R3D data stream
R8	Cubicomp PictureMaker red channel image data
RA	RealAudio audio
RA3REPLAY	Red Alert 3 replay
RAC/RAW	Rdos Raw OPL Capture music
RAD	Reality ADLib tracker module/song
RAF	Fujifilm Raw image
RAM	RealMedia meta file
RAP	Raptor flowchart

Supported file type	Description
RAR	RAR compressed archive (gen)
RAS	Max Payne data file
RAS/IM1/IM24/IM32/IM8/RAST/RS/SR/SUN	Sun Raster bitmap
RAT	PICS Rating System
RATDVD	ratDVD DVD image
RAV	Rave Reports Project
RAW	CT Raw disk image
RB	RocketBook eBook
RBC	Easy Resume Creator Pro resume
RBF	Raw Bitmap Font
RBFRM	REALbasic Form/Window
RBJ	Redcode Object XRA PC (v1.x)
RBN	Richard's Bridge Notation
RBP	REALbasic/Xojo Project
RBS	Propellerhead Software ReBirth Song
RBT	LEGO NXT Brick
RBVCP	REALbasic Project
RBX	Richard's Bridge Notation (inline)

Supported file type	Description
RBXL	Roblox Location
RBXM/RBXMV	Roblox Model
RCAD	RealCADD drawing
RCD	Oloneo HDR preset
RCL	Easy CD Creator Layout
RCM	LigPlot Residue Centres-of-Mass data
RCS	RadDeveloper color scheme
RD	R documentation
RDATA	R saved work space
RDC	IDRISI Raster image Documentation
RDF	Friend of a Friend (FOAF) Resource Description Framework
RDG	RDCMan config
RDI	RIFF Device Independent Bitmap
RDL/RDLC	SQL Server Reporting Services Report Definition Language
RDOC_OPTIONS	Ruby RDoc Options
RDP	Remote Desktop Connection Settings
RDS	Ray Dream Studio
RDW	Real-DRAW Project

Supported file type	Description
REAPEAKS	REAPER media peak information (v1.0)
REASON	Reason song
RED	REDway DER (Dynamic Elements Resource)
REDIF/RDF	ReDIF template
REF	Atari ST Guide ref links
REG	Windows Registry Data
REKO	REKO cardset
RELS	Open Office XML Relationships
REMOTEMAP	Reason Remote Mapping
REP	Business Objects Report
REPORT/TXT	GENSCAN output results
REPX	DevExpress Report layout (v1)
RESX	Microsoft .NET XML Resource template
REV	Revolution MetaCard stack
REX	ReCycled Audio Loop Export
REZ	LinTech resource
RFA	Revit Family Architecture project
RFL	Propellerhead Software Reason SoundBank
RFLW	Edge Reflow data

Supported file type	Description
RFN/RFP/RFX	RoboForm saved data
RFX/G3X	RealFlight data
RGE	R.A.G.E. Driver
RGFX/RGX	IFF Retargetable Graphics bitmap
RGO	RepliGo virtual print
RGP	RealArcade Game Package
RGS	InstallShield Script for Windows Registry
RH	Rob Hubbard chiptune
RHL	Rathole compressed data
RIB	Renderman RIB
RIDL	RAD Studio Active X RIDL data
RIFF	Riff Raff module
RIP	Rocky Interlace Picture bitmap
RIR	Satori RIR scaled raster
RIX/SCX/SCI	ColorIX bitmap
RJS	RealSystem Skin
RK	RK compressed archive
RKA	RK Audio lossless compressed audio
RLA	Alias Wavefront Raster bitmap

Supported file type	Description
RLC	Radiant LoopCAD Project
RLE	Autodesk Screencast video (intermediate format)
RLF	ArtCAM 3D Relief model
RLG	RegCleaner v4.3 Language File
RLI	RealWorld Layered Image bitmap
RLL	Microsoft Resource Library
RLN	Alpha Four field rules
RM	Real Media stream
RM/RA	Real Audio
RMF	Rich Map Format
RMI	RMI RIFF MIDI Music
RMP	Magellan Raster Map
RMT	RASTER Music Tracker module
RMTL	Rhino 3D Material
RMVB	RealVideo Variable Bit Rate
RMX	RealMedia Secure clip
RND	AutoCAD Autoshade rendering slide
RNG	RELAX NG

Supported file type	Description
RNQS	Pokemon Randomization Quick Settings
ROC	SpaceCAD rocket model
RODL	RemObjects Definition Language
ROL	AdLib Visual Composer music
ROM	Cloanto Amiga OS encrypted ROM
ROM/BIN	BIOS ROM Extension (IA-32)
ROQ	Id Software RoQ video
ROR	ROR Structured Feed
ROSE	Rosegarden musical notation (RV21)
ROT	Home World 2 - ROT graphics
ROTACTION	ROT Object 3D Action
ROTOBJ	ROT Object 3D
RP2	RetroPlatform Player archive (old)
RP9	RetroPlatform Player archive
RPL	ARMovie video
RPM	RPM Package (generic)
RPMSG	Restricted-Permission Message
RPP	REAPER Project
RPROJ	RStudio Project

Supported file type	Description
RPS	Propellerhead Software Reason Song
RPT	Crystal Reports output file (Report)
RPX	ActiveReports Report
RRA	Windows Installer temp data
RRD	RRD4J Round Robin Database
RRH	BlackBerry resource
RSDOC	DesignSpark Mechanical 3D Document
RSG	Drakan: Order Of The Flame Saved Game
RSH	Warhammer 40K textures
RSM	Resume
RSN	RAR packaged SPC soundtrack
RSND/IFF	IFF RSND audio
RSO	LEGO NXT brick audio
RSRC	BeOS Resource data
RSY	FLEXIT Multishot Survey Raw Data file
RT	RealTime subtitles
RTAB	RandyTab guitar tablature
RTBW	Syzygy tablebase win/draw/loss
RTBZ	Syzygy tablebase distance-to-zero

Supported file type	Description
RTC	Office Live Meeting Connection
RTD	RagTime document
RTE	Autodesk Revit Template
RTF	Rich Text Format
RTI	Okino plugin Run Time Information
RTL	HP Raster Transfer Language
RTP	GROMACS Residue Topology
RTS	Roytal TS remote connection
RTST_PAK	Recursion Real-Time Stat Tracker Package
RTTEX	Robinson Technologies Textures
RTZ	RedTitan Zip
RULE	Golly Rule
RUN	ApplImage Portable Linux App
RUS	Navitel 1.1 Map
RVD	Raster-Vector Hybrid Drawing
RVF	RichView Format (Unicode)
RVIZ	RViz workspace
RVL	Muvee project
RVPROJ	RPG Maker VX Project

Supported file type	Description
RVPROJ2	RPG Maker VX Ace Project
RVT	Autodesk Revit Project
RW2/RAW	Panasonic RAW image
RW3	Regressi Win data
RWL	Leica RAW image
RWT	ReadWriteThink data
RWX	RenderWare 3d model
RWZ	Rawzor compressed raw image
RX2/REX	REX2 audio sample loop
RXDATA/RVDATA2	RPG Maker data
RXF	Recipe Exchange Format
RXM	GisRX GPS Navigator map
RXN	MDL Reaction format
RXO	Receiver Independent Exchange Format
RXT	X-Stitch Designer Gold Template
RZX	File Crypt encrypted
S	Digital Micrograph Script
S00	MEKA savestate
S01	

Supported file type	Description
	Expert Witness compression Format SMART disk image
S10W	S10 WebAlbums project
S2	Stranded II Mapfile
S2A	SEAL 2 Application
S2K	Sasami Script subtitles
S2M	The Settlers 2 Map
S2MA	StarCraft 2 Map data
S2MH	StarCraft 2 Map Header
S2ML	StarCraft 2 Map Localization
S2QH	StarCraft 2 Localization Header
S2QL	StarCraft 2 Unit Localization
S3D	SEAM 3D Project
S3I/SMP	Scream Tracker/Digiplayer sample
S3M	Scream Tracker 3 module
S3O	Spring Engine 3D model
S4MI	skinner4moto module
S8THEME	Start8 menu Theme
S98	PC88/PC9801 sound logs rip

Supported file type	Description
SA	Sonic Arranger module
SA2	Surprise! AdLib Tracker 2.0 module
SAC	Adobe Shared Asset Catalog
SAD	Black and White sounds data
SAF	Helix Stronghold Encrypted file
SAM	AMI Pro / Word Pro document
SAMI/SMI	SAMI captions
SAR	SAPCAR CAR compressed archive
SAS7BDAT	SAS v8+ data
SAT	ACIS Solid Model
SAV	Anacreon savegame
SAV/POW	Windows NT Registry Hive (SAV/POW)
SAV/SPV	American's McGee's Alice Saved Game File
SAVE	Doom 3 Savegame
SAZ	Fiddler Session Archive Zip
SB	Frostbite SuperBundle
SB2	Scratch 2.0 project
SBC	SBC compressed archive
SBGF	Grapher Graph

Supported file type	Description
SBJ	Superbase Project
SBK	Emu Sound Font v1.0
SBL	Limbo Symbol table
SBMI	Space Engineers ModInfo
SBPF	Small Business Publisher document
SBQ	Superbase Query definition
SBT	Duxbury Scrub Table
SBV	Superbase form
SBW	Savings Bonds Wizard data
SBX	SeqBox container (gen)
SBZ	ShowBiZ project
SC	IRIS Showcase drawing / presentation
SC2	SimCity 2000 save game
SC2REPLAY	StarCraft 2 game replay
SC6	RollerCoaster Tycoon 2 scenario
SC68	sc68 soundchip music
SCC	Scenarist Closed Caption data
SCD	Agfa/Matrix SCODL bitmap
SCDOC	SpaceClaim Document

Supported file type	Description
SCEN	Caligari TrueSpace Scene (v2.x)
SCENE	3D Master Scene
SCF	ChemWindow Standard Chemistry File
SCH	DProtel for Windows schematic
SCHDOC	Protel for Windows schematic capture (binary)
SCHEME	Programmer's Notepad Scheme
SCHLIB	Protel Schematic Library editor binary v1.2-2.0
SCHREPX	DevExpress Scheduler Report layout
SCL	FrontDesigner Scale setting
SCM	GIMP Script-Fu Script
SCM/SCX	StarCraft Map
SCN	Children of the Nile Scenario
SCNTOC	Softimage Scene TOC
SCO	Csound Score
SCP	Alpha Four Script
SCPT	Compiled AppleScript script
SCR	CA-Compete! Script
SCREEM	SCREEM project
SCRIPT	Aegis Animator Script

Supported file type	Description
SCRIPTTERMINOLOGY	AppleScript Terminology
SCRIVX	Scrivener XML document
SCRPT	Genesis - The Third Day Script
SCT	Form Memo MS Visual FoxPro 7
SCUT	Easy Cut Studio project
SCW	Movie Magic Screenwriter document
SCX	Form MS Visual FoxPro 7
SCZ	Wingz script
SDA	Self-Dissolving compressed Archive
SDAT	Nintendo DS Sound Data
SDATA	MusicMaker Song Data
SDB	Pegasus SPS encoded audio
SDC	ArcGIS geospatial and attribute data
SDD	CBM .prg Studio Screen Designer Data
SDEF	Scripting Definition
SDF	Kawai music score
SDF/SDO	IEEE DASC Standard Delay Format
SDI	ArcGIS spatial and attribute indexes
SDINSTALL	Speckie Dictionary Installation

Supported file type	Description
SDLPPX	SDL Trados Studio Project Package
SDLPROJ	SDL Trados Studio Project
SDLXLIFF	SDL Trados XLIFF Localization data
SDO	DB/TextWorks Database Deferred Update Directory
SDP	Session Description Protocol
SDR	Dell System Information
SDT	Siemens mobile theme
SdTID	SecurID Soft Token
SDW	StarOffice StarWriter document
SDX	CaptiveWorks satellite channel database
SDXML	SimpleDiagrams diagram
SDZ	Spring Engine Zipped mod
SE1	Swiss Ephemeris data
SEA	Mac Stuffit Self-Extracting Archive
SEARCHCONNECTOR-MS	Windows Search Connector
SEARCH-MS	Microsoft Vista Saved Search
SEEXPL	Spec Explorer results
SEG	SEG-2 data

Supported file type	Description
SEP	ChemSep project
SEQ	Cyber Paint Sequence
SER	SER format video
SES	Cool Edit / Audition Session
SESSION	Session Manager Firefox Backup
SESX	Adobe Audition Session
SET	Alpha Four record Set
SEW	Janome (New Home) Sewing Machine stitch
SEX	SExtractor configuration
SF2	Standard SoundFont
SFARK	sfArk compressed SoundFont
SFB	PlayStation 3 Disc data
SFC	GEMPACK data management info
SFD	Mozilla Spam Filter Definition
SFF	Elecbyte M.U.G.E.N. sprites
SFL/SFP/SFT	LaserJet Soft Font
SFPACK	SFPack compressed SoundFont
SFS	sfxr Sample
SFT	ChiWriter Screen Font

Supported file type	Description
SFVIDCAP	Sony Foundry Video Capture project
SFW	Seattle FilmWorks / PhotoWorks photo (SFW93)
SFX	Self-Extracting LHA Archive
SFX2	SoundFX 2 module
SFZ	SFZ Sample definition
SGA	SGA archive - game data
SGF	Smart Game Format
SGI	Silicon Graphics 24bit compressed bitmap
SGM/SGML	EAD - Encoded Archival Description
SGPBPRJ	SGP Baltie Project
SGPG	SGP Model Group
SGRIDDLER	SGriddler Paint-by-Number puzzle
SGT	Microsoft DirectMusic Segments Type
SH	Linux/UNIX shell script
SH3	Harvard Graphics presentation (v3.x)
SHAPE	Dia shape
SHEET	Dia sheet
SHFB	Sandcastle Help File Builder project

Supported file type	Description
SHFBPROJ	Sandcastle Help File Builder Project
SHG	Segmented Hypergraphics bitmap
SHIPSECTION	Swords of the Stars Ship
SHK	NuFX archive
SHN	Shorten lossless compressed audio
SHO	ShroomPlayer module
SHP	ArcView Shape
SHPROJ	Visual Studio Shared Code project
SHPRST	LuSH-101 global Preset
SHR/SHAR/SHA	shar SHell self-extracting aRchive
SHS	Shell Scrap object
SHTMBR	LuSH-101 Timbre preset
SHV	Viking Designer 1 embroidery file
SHX	ArcView DataBase Index
SIA	Silo 3D model (ascii)
SIAG	Siag spreadsheet
SIARD	SIARD format
SIB	ShipInBottle compressed file
SID	LizardTech MrSID photo

Supported file type	Description
SID2	Sidmon II module
SIF	SkyOS Installation File
SIG	IDA Signatures
SIM	ITI-SIM Model
SIMP	Software Ideas Modeler Project
SIMS2PACK	The Sims Compacted Resource file
SIMS3PACK	The Sims 3 game package
SIMSS	Software Ideas Modeler Style Set
SIMT	Software Ideas Modeler Template
SIS	EPOC Installation package (rel. 2,3,5)
SISX	Symbian Series 3 Installation file
SIT	Stuffit compressed archive
SITE	GoLive Website project
SITX	Stuffit X compressed archive
SIX	DEC SIXEL Graphic bitmap
SJAM	SuperJAM! song
SK	Skencil drawing
SK1	sK1 vector graphic
SKC	ISIS sketch

Supported file type	Description
SKCHR	SketchChair document
SKD	AutoSketch Drawing
SKEIN	Skein replay data
SKF	skincrafter skin
SKI	Motorola phone skin info
SKL	Hondata S-Manager calibration
SKM	STarKos tune
SKN	Blaze Media Pro Skin
SKN/FHS	RoboHelp / FlashHelp skin
SKP	SketchUp model
SKR/GPG/PGP	Pretty Good Privacy (PGP) Private/Secret Keyring
SKS	Creature House Expression Skeletal Stroke
SKYT	SKYT/Drifters Packer song
SLA	Scribus document
SLDASM	SolidWorks Assembly
SLDDRW	SolidWorks Drawing
SLDPRT	SolidWorks (generic)
SLE	Surfplan kite project

Supported file type	Description
SLK	SYLK - SYmbolic LinK data
SLOGO	StarLogo project
SLTNG	StarLogo TNG Project
SLTX	MATLAB Simulink model Template
SLX	MATLAB Simulink model
SM	SMath Studio worksheet
SMALI	Smali assembly source
SMC	Super Nintendo game - ROM Image
SMD	MicroMap map data
SMDLPROJ	SQL Server Report Model Project
SME	Samsung Kies Messages backup
SMENT	StarMade Entity
SMF	3D World Studio mesh
SMI	Lotus Smart Icon
SMI/SMO	Siemens archived SMS messages
SMK	Smacker movie/video
SMM	Smart Install Maker project
SMOD	Future Composer v1.0-v1.3 module
SMOL	Spartan molecule data

Supported file type	Description
SMT	Memo File Apollo Database Engine
SMUFI	Picatune soundtrack
SMUS/SONG	SMUS IFF Simple Musical Score
SMV	Snes9x movie capture
SMW	SIMPL Windows source
SMX	SysMetrix skin
SMZIP	StepMania music package
SN	Sound Club module
SN2	Sound Club 2 module
SNAG	SnagIt capture
SNAGPROF	Snagit Profile
SNAPPY	Szip compressed (comment-43 format)
SNB	S-Note document
SNC	Sonarc compressed RAW PCM audio
SND	Dalet Sound format audio (old)
SNDT	SndTool sound/audio
SNF	Starry Night Document
SNF/TRC	Sniffer capture
SNG	DeskMate song

Supported file type	Description
SNK	Strong Name Key
SNM	Netscape Mail Message
SNOOP	snoop verbose trace
SNS	SNS-HDR project
SNSF/SNSFLIB	SNSF Super Nintendo Sound Format rip
SNSX	SNS-HDR 2.x project
SNT	Amnesia: T.D.D. sound entity
SNZ	Snzip compressed (snzip format)
SOBJ	Caligari TrueSpace 3D object (v2.x)
SOF	Quartus II Project
SOFT	Simple Omnibus in Text Format
SOL	Flash Shared Object file
SOLITAIRESAVE-MS	Microsoft Solitaire Saved game
SONG	AudioSauna Song
SOS	Adventure SOS compiled walkthrough
SOU	SBStudio II sounds
SOUND	The Music Studio Sound (Amiga)
SPA	Spectral Data file
SPARC	Skype Extra

Supported file type	Description
SPC	Crimson Editor language specification file
SPC/SPS	Spectrum 512 compressed/smooshed bitmap
SPD	Bitstream Speedo font
SPE	Princeton Instruments WinView CCD image format
SPECCY	Speccy snapshot
SPFX	Squeeze Presets
SPH/NIST	NIST Sphere waveform audio
SPIDERSOLITAIRESAVE-MS	Microsoft Spider Solitaire Saved game
SPIF	Streaming Progressive Image Format bitmap
SPIFF/SPF	SPIFF Still Picture Interchange File Format bitmap
SPINPUT	Spartan spinput format
SPK	KiXtart SPK notation format
SPK/ARC	Acorn Spark Archive
SPL7	sPlan 7.0 schematic
SPM	Spektrum DX serie transmitter settings
SPMO	SpeedView Meta Objects
SPO	SPSS Output Document
SPP	Serif PhotoPlus Picture

Supported file type	Description
SPR	Brother PowerNote spreadsheet
SPRITE	SuperTux Sprite
SPS	SharkPort file
SPT	SpeedTree format
SPU	SPU Playstation log rip
SPVCHAIN	Multibit Bitcoin blockchain
SQF	FreeMotion Flash movie
SQL	phpMyAdmin SQL dump
SQLITE/SQLITE2	SQLite 2.x database
SQLITE/SQLITE3	SQLite 3.x database
SQLITE-WAL	SQLite Write-Ahead Log (little endian)
SQLPLAN	Microsoft SQL Server execution Plan
SQLPROJ	Visual Studio SQL Server Project
SQM	Operation Flashpoint mission
SQR	SQR script
SQX	SQX compressed archive
SR2	sr2 compressed data
SRF	FileLocator Pro Search Criteria (gen)
SRL	Strelok Scope Reticle

Supported file type	Description
SRR	ReScene Release data
SRS	Outlook Send-Receive Settings
SRT	SubRip subtitles
SRW	Samsung Raw image
SS	First Choice SpreadSheet
SS1	Mini Office II SpreadSheet
SSA	Children of the Nile campaign
SSC	StepMania Song
SSDL	ADO.NET Store Schema Definition Language
SSF	Enable SpreadSheet
SSF/SSFLIB	SSF Saturn Sound Format rip
SSML	Speech Synthesis Markup Language
SSMSASPROJ	Microsoft SQL Server Analysis Services Project
SSMSMOBILEPROJ	SQL server Management Studio Mobile Project
SSS	Coda Style Sheet
SST	AVHRR satellite bitmap
SSTS	Stream SubText Script subtitles
SSW/CRY	SETool encrypted firmware

Supported file type	Description
ST*	GetDataBack Scan trace
ST0	VirtuaNES savestate
ST11	Spectrum Sound Tracker 1.1 chiptune
ST1H/MEM	Fanuc parameters file
ST2	RCA Studio 2 binary dump cartridge
ST3	Star 3 MIDI Karaoke file
STAGE	2D Fighter Maker 2nd stage data
STAPL	Standard Test and Programming Language
STAT	Weather data summary report
STATE	atari++ state
STB	AutoCAD Plot Style Table (name based)
STD/SUM/TXT	wi-scan log
STENCYL	Stencyl game data
STF	3D World Studio material
STG	STG SNMP Traffic Grapher settings
STH	Sisthema Personal System
STK/TIF/TIFF	MetaMorph Stack
STL	ATF STereoLithography (binary)
STM	GNU TeXmacs Scheme

Supported file type	Description
STM/STX	Scream Tracker module
STMX	XMILE Model
STO	Infinity Engine Store (v1.0)
STORMREPLAY	Heroes of the Storm replay
STORYBOARD	Interface Builder Storyboard document
STP	SignalTap II capture
STP/STEP	ISO-10303 STEP model data
STPROJ	Sapphire Project
STRC	AY STRC chiptune
STREAM	Shockwave Stream
STRM	Nintendo DS audio Stream
STS	Atari Works Spreadsheet
STSG	SuperTux Saved Game
STU	Pinnacle Studio Video Project
STWM	SuperTux World Map
STX	EditPlus Syntax file
STY	Beyond Words Composer Style
STY/STX	Microsoft Word for DOS Style sheet
STYLE	SuperJAM! Style

Supported file type	Description
STZ	stz compressed data
SUA	Tim Newport-Peace's Special Use Airspace Format
SUB	DVDSubtitle subtitles
SUBLIME-MOUSEMAP	Sublime Text Mouse settings
SUBLIME-PROJECT	Sublime Text Project
SUBLIME-SNIPPET	Sublime Text Snippets
SUBLIME-WORKSPACE	Sublime Text Workspace
SUI	Mac font
SUITE	Theme Manager / WinStyles theme
SUN	SUNTronic module
SUNSYNTH	SunVox Synthesizer
SUNVOX	SunVox module
SUO	Microsoft VisualStudio Solution User Options
SV2I	Symantec LiveState recovery image
SV4	RollerCoaster Tycoon Saved game
SV6	RollerCoaster Tycoon 2 Saved game
SVC	SupervisionCam Camera Settings
SVCINFO	Saved WCF Configuration Information

Supported file type	Description
SVF	Simple Vector Format (generic)
SVG	Scalable Vector Graphics (var.1)
SVM	StarView Metafile
SVN	Solace Virtual Northstar disk image
SVQ	Roland MC-80 music sequence
SVR	GoDot C64 Image Processing - Saver
SVT	Solace Virtual Tape format 1
SW2	SoftWrap license data
SWA	ShockWave Audio
SWAV	Nintendo DS Sound Wave
SWC	Flash Component distribution archive
SWD	Flash file with debug info
SWD/WLD	Settlers II map
SWF	Macromedia Flash Player Compressed Movie
SWG	Swag Reader Packet
SWI	HP Switch firmware
SWIDTAG	SWID Tag
SWISH	Swish-e index
SWM	SMIRT file

Supported file type	Description
SWS	PowerDesigner Workspace
SX2	Propellerhead Reason NN-XT Patch
SXC	OpenOffice Calc spreadsheet
SXD	StarOffice Drawing
SXE	ProfiCAD drawing
SXI	OpenOffice Impress presentation
SXM	StarOffice Math document
SXW	OpenOffice Writer document
SYF	Artline Symbol File
SYM	CADVANCE 2D symbol
SYMCACHE	Windows Symbol Cache
SYMMOD	Symphonie Module
SYN	Synthesis module
SYNMOD	SynTracker module
SYNW-PROJ	SynWrite Project
SYNW-SNIPPET	SynWrite Snippet
SYS	FreeDOS KEYBoard layout collection
SZ	Szip compressed (framing format)
SZX	zx-state snapshot

Supported file type	Description
T@0	Timeline schedule (v2.0)
T0*	TaxCut Tax Return file
T0AST	The 0ok Amazing Synth Tracker module
T2FLOW	Taverna Workbench workflow definition
T2K	Teach2000 document
T3	TADS 3 Game
T3D	Swift 3D 3D Graphic
T64	Commodore 64 Tape container
T65	Adobe PageMaker Template (v6.5)
T81	T81 EightyOne tape image
T8C	SDLTRS Configuration
TAB	MapInfo MapBasic initial data Table
TABLECONTENT	SMART Table Activity Pack
TAF	ADRIFT Text Adventure File
TAK	TAK lossless compressed audio
TAP/DAT	Oric Tape image
TAR	TAR - Tape ARchive
TBA	DB/TextWorks Database Primary Textbase Definition

Supported file type	Description
TBASICCX	thinBasic Console scripts (obfuscated)
TBASICX	thinBasic GUI scripts (obfuscated)
TBB	The Bat! Message Base
TBK	Asymetrix ToolBook (generic)
TBL	Binary Unicode conversion Table
TBP	The Bat! plugin
TBR	Mesa 2 ToolBar
TBS	Chess Tablebase
TBX	TermBase eXchange Format
TC	TransCopy disk image
TCAX	TestComplete Project events
TCB	TCB Tracker module
TCC	TCruise codes and parameters
TCD	TCruise Document
TCN	Techne Model
TCP	TeXnicCenter Project
TCW	TurboCAD drawing
TCX	Garmin Training Center Database XML (V2)
TD	TheDraw design (gen)

Supported file type	Description
TD0	Teledisk Disk compressed image (advanced mode)
TDD/OBJ	3D Data Description object
TDF	Binary Tiled Data File
TDMS	TDM Streaming format
TDT	CodeWarrior Target Data (Big Endian)
TDUMP	Java HotSpot Thread Dump
TE1	UltraEdit Template
TEC	TECkit compiled mapping
TER	Black and White 2 Terrain data
TEX	Corel 10 Texture
TEXI/TEXINFO	Texinfo source
TF	Follin Player II module
TFC	TurboFM Compiler chiptune
TFE	TFM Music Maker music (V2)
TFI/TIFILE/TIFILES	TI-99 TIFILES file image
TFM	FormTool Gold form
TFW	ArcView World File
TG	TuxGuitar Tablature

Supported file type	Description
TGC	Terragen Clip
TGD	Terragen project
TGF	MDL Transportable Graphics Format
TGO	Terragen Object geometry
TGQ	Electronic Arts TGQ video
TGW	Terragen World
THEME	Windows 8-10 Desktop Theme
THEME/THE	Windows 98-7 Desktop Theme
THING	MakerBot Thing
THM	Sony Ericsson Theme (for mobile phones)
THMX	Microsoft PowerPoint 2007 theme / template
THN	Graphics Workshop for Windows Thumbnail
THP	GameCube THP video
THR	THOR compressed data
TIB	Acronis True Image
TIBKP	Titanium Backup Easy Backup saved data
TICART	Win994a cartdrige image
TICR	Kindle app book info
TID	AVCHD Thumbnail Index

Supported file type	Description
TIF/TIFF	BigTIFF bitmap
TII	TI Interactive Workbook
TIL	IDA Type Information List
TIM	PSX TIM 16bpp bitmap
TIP	Taquart Interlace Picture bitmap
TITAPE	Win994a tape image
TIZ	Infinity Engine compressed Tileset
TJA	Taikojiro Song Map
TJN	Taijin Media Net karaoke song
TK3	Tk3 eBook
TKC	tKC Cracking Tutorial File
TKN	Libery BASIC tokenized source
TKU	TKUY map format
TL5	TimeLiner 5.x data
TLA	TuneUp Styler Logo Animation
TLB	SPSS Type Library
TLD	Tag Library Descriptor
TLG	KiriKiri TLG bitmap
TLO	SPSS Table Look

Supported file type	Description
TLP	Tulip graph format
TLX	Wintertree dictionary
TM	GNU TeXmacs document
TM2	TIM2 PlayStation2 bitmap
TMC	Thrustmaster TARGET script
TMCOMMAND	TextMate Command
TMD	PSX TMD 3d Model
TML	Apache Tapestry Markup Language document
TMLANGUAGE	TextMate Language grammar
TMOD	Terraria Mod
TMPL	eMule Web Interface template
TMPREFERENCES	TextMate Preferences
TMPROJ	TextMate Project
TMSNIPPET	TextMate Snippet
TMT	TimeCult workspace
TMTHEME	TextMate Theme
TMU	Trilo Tracker chiptune
TMX	Tile Map XML
TNC	SuperJPG ThumbNail Cache

Supported file type	Description
TNEF/DAT	Transport Neutral Encapsulation Format
TNFO	Spybot Search'n'Destroy process data
TNGZ	Immaginaria TNG 3D scene
TNO	TI-Nspire OS image
TNS	TI-Nspire document
TNSP	TI-Nspire PublishView document
TNY/TN1	Tiny Stuff format bitmap (low-res)
TO4/T4	Top 4 compressed data
TOC	LaTeX table of contents
TOOT	SuperJAM! Toot
TOP	Waltop digital ink-pad graphic
TOPOJSON	TopoJSON format
TOPPRJ	TopSolid Project
TORRENT	Torrent
TOS	Atari ST TOS executable
TOX	Typed Voxel format
TP	Pokemon Online team
TP3	Trackerpacker 3 Music
TP4	Kaleidescape Touch Panel Variations

Supported file type	Description
TPA	TwinCAT Addresses data
TPF	HiJaak PCL soft font
TPG	Tektronix Pattern
TPH	Turbo Pascal Help
TPP	Teleport Pro (generic) Project
TPS	Clarion Topspeed Data file
TPU	Borland Turbo Pascal 5.5 compiled Unit
TPX	Photo Express Template
TPY	TwinCAT Project
TQ	STK Torque format
TQ5	TQSLCert request
TR	TomeRaider e-book/document
TR3	TomeRaider 3 eBook
TRC	Track Row Column markers data format
TREEDB	TreeDBNotes document
TRELBY	Trelby document
TRF	LFToolkit Transformation Rules File
TRIG	TriG RDF serialization format
TRK	DCS Track

Supported file type	Description
TRK/WPT	Magellan MapSend
TRM	Injector Trim data
TRP	EggPaint bitmap
TRS	TrIDNet serialized definitions package
TRV	Track Record Viewer TRV/TRVX definition
TRX	Track Record Viewer TRV/TRVX Index
TS	MPEG-2 Transport Stream
TS3_ADDON	TeamSpeak 3 Addon
TS3_PLUGIN	TeamSpeak 3 Plugin
TS3_SOUNDPACK	TeamSpeak 3 Soundpack
TS3_STYLE	TeamSpeak 3 Style
TSC/SCH	TINA Schematic
TSI	Traktor Settings
TSK	Skin / Theme for Pocket PC PDAs
TSS	T'SoundSystem Source
TST	ExamView Test
TSV	Time Shift Video
TSX	MSX Tape image
TTA	TTA/True Audio lossless compressed audio

Supported file type	Description
TTC	TrueType Font Collection (v1)
TTC/OTC	OpenType Font Collection (v2)
TTF	TrueType Font (true var.)
TTF/TTE	TrueType Font
TTKGP	TatukGIS Project
TTML	Timed Text Markup Language
TTS	7DTD prefabs
TTX	TRADOSTag XML
TUN	Enterprise Music Box tune
TUP	Tupi project
TV1	trsvid TV1 video
TV3	trsvid TV3 video
TV6	trsvid TV6 video
TVC	NK - BMP/TV lossless compressed bitmap
TW	That's Write document
TWB	Tableau Workbook
TWBX	Tableau Packaged Workbook
TWD	MindMapper Map
TWF	PCsync for Windows

Supported file type	Description
TWL	GPS track
TWR	Timing Wizard Report
TWW	Tagwrite Template
TWX	Timing Wizard report (XML)
TXM	TrakAx Mixer Configuration data
TXT	Adobe InDesign printing instructions report
TXVACTIVITYDIAGRAM20	Together Activity Diagram (UML 2.0)
TXVCLASSDIAGRAM20	Together Class Diagram (UML 2.0)
TXVPCK	Together Class Diagram (UML 1.4)
TY	TiVo video
TYPE/LIB	Intellifont font
TZ	TimeZone data
TZX	ZX Spectrum Tape image
U3P	U3 application Package
UAE	UAE - WinUAE Configuration
UAEM	FS-UAE file metadata
UASSET	Unreal Package
UBOX	Universe Sandbox simulation
UBZ	Open-Sankore document

Supported file type	Description
UC2	UltraCompressor 2 Archive
UCCAPILOG	Microsoft UCC API Log
UCE	UniCode Extensions
UCF	Universal Communications Format
UCI	Samsung YP-P2 theme
UCLS	ObjectAid UML Explorer Class diagram
UCM	Crazy Machines model
UCS	Universal Classification Standard Database
UCT	UC Browser Theme
UDB	VBA32 Antivirus Signature
UDD	OllyDbg Module Info
UDF	Universal Data Format
UDN	Alpha Four User Definition
UDS	NHTSA UDS-1992 crash test results
UEF	Unified Emulator Format
UEW	UltraEdit Wordfile
UEZ	Ulead COOL 3D (generic)
UFA	UFA compressed archive
UFI	UFOCaptureV2 Preset settings

Supported file type	Description
UFO	Ellisys Visual USB Data
UGI	Universal Go Format
UHS	Universal Hint System
UI	Qt User Interface
UIFILE	Windows Explorer UIFILE
UIR	LabWindows User Interface Resource
ULP	EAGLE script
ULT	Ultra Tracker module
ULX	Glulx Game
UMAP	Unreal Engine Map
UMD	UMD Photobook
UMLCLASS_DIAGRAM	UML2Tools UML Class Diagram
UMP	UModel Project
UMX	Unreal Music
UNF	Ulysses Native Format
UNI	MikMod module
UNITY3D	Unity Web Player scene
UNITYPROJ	Unity 3D Project
UNR	Unreal Map

Supported file type	Description
UOF	Uniform Office Format (generic)
UOP	Uniform Office Format Presentation
UOS	Uniform Office Format Spreadsheet
UOT	Uniform Office Format Text document
UP3	UP! 3D model
UPC	Ultimate Paint Graphics Editor plugin/effect
UPD	McAfee AV Pattern update
UPLUGIN	Unreal Engine Plugin
UPP	Unified Printer Parameter
UPROJECT	Unreal Engine Project
UPS	VisualBoyAdvance UPS patch
URF	AppFace skin
URL	Windows URL shortcut
USB	Ulysses Speaker Database
USD	UML Sequence Diagram
USEQ	USeq genome data
USER	Visual Studio Project User Options
USF	EVGA Precision X skin
USF/USFLIB	USF Ultra64 Sound Format rip

Supported file type	Description
USKN	KSDev ThemeEngine theme/skin
USR	COREL Photo Paint User Defined Filter
USS	UAE Saved State
UST	UTAU vocal track
USX	Unified Scripture Format XML
UTI	SafeGuard PrivateCrypto Encrypted
UTK	Maxis UTalk audio
UTX	Unreal Texture
UUE/UU/XXE	UUencoded/XXencoded text
UV2	uVision v2 Project
UVO	Sanyo Katana DLX call/voice memo
UVOPT	uVision v4 Project Options
UVOPTX	uVision v5 Project Options
UVOX	Universal Voxel format
UVPROJ	uVision v4 Project
UVPROJX	uVision v5 Project
UWF	UltraTracker Wave File audio
UXDC	Office Data Retrieval Service Connection
UXF	UMLet diagram

Supported file type	Description
UZ1	JB BAHN scenery
UZ2	JB BAHN scenery (Zoom2)
UZ4	JB BAHN scenery (Zoom4)
V00	Krez 3D ultrasound image
V3D	Vectric Cut3D model
V3M	Vector Art 3D Machinist model
V3O	Emergency 3D model
V4P	VVVV Patchlet
VAL	PV3D Value data
VAP	Annotated Speech audio
VAULT	mSIGNA Vault
VB	Beam Software SIFF video
VBE	VBScript Encoded script
VBF	Var Bitmap Font (generic)
VBL	Virtual CD v4 log
VBM	Veeam Backup Metadata
VBO	VBOX data
VBOX/VBOX-PREV	VirtualBox machine definition
VBP	VisualBasic Project (ActiveX DLL)

Supported file type	Description
VBPROJ	Visual Studio Visual Basic Project
VBR	MSHeli Vbar data
VC	Sonarc compressed VOC audio
VC4	Virtual CD v4 and older
VC6	Ashlar-Vellum Part
VCD	Value Change Dump
VCDIFF	VCDIFF format
VCE	Visual CertExam Suite Exam file
VCF	Variant Call Format (txt)
VCF/VCARD	vCard - Business Card
VCG	VCG graph
VCM	Interwise Participant Recorded WebCast
VCPROJ	Visual Studio .NET Visual C Project
VCXPROJ	Visual Studio Visual C++ Project
VD	PLC Data
VDATA	Vaulty obscured
VDB	Dr.Web Anti-Virus Database
VDF	Avira AntiVir Virus Database
VDI	VirtualBox Disk Image (Innotek)

Supported file type	Description
VDJSAMPLE	VirtualDJ audio Sample
VDM	Microsoft Windows Defender Virus Definition Module
VDPROJ	Visual Studio Setup and Deployment Project
VDX	Visio Drawing XML
VEG	Sony Vegas video project
VEM	MM Video E-Mail
VEP	AVS Video Editor Project
VEX	VLBI Experiment
VF	Vegas Movie Studio Project
VFF	V9990 font format
VFT	VisiForm form
VFZ	Webcam Video Effects pack
VGE	VGM Music Maker module
VGM	Video Game Music format
VGS	Virtual Game Station memory card save game
VGZ	VGZ video
VHD	Virtual PC Virtual HD image
VHDL/VHD	VHSIC Hardware Description Language (with rem)

Supported file type	Description
VHO	Xilinx instantiation template
VI	ArcSoft VideoImpression project
VIC	Yamaha PSR-9000 custom voice (v1.0)
VIC/IMG	PDS image bitmap
VIC/VICAR/IMG	VICAR JPL image bitmap
VID	Bethesda Softworks video
VIF/VIFF/XV	Khoros Visualization Image File Format bitmap (v1.0)
VIIVO	Viivo encrypted
VIP	Husqvarna Viking/Pfaff Home Embroidery Format
VIS	Visionaire project
VIX	Acu4GL/AcuCOBOL Index
VIZ	Division dVS geometry
VJP	Visual J++ Project
VJSPROJ	Visual Studio J# Project (v7)
VK	VisKit 3d model
VLA	Digistar II VLA geometry
VLAB	VisionLab Studio Project
VLCL	VMware Localization

Supported file type	Description
VLM	Ashlar-Vellum Drawing
VLW	Processing Font
VLX	Visual LISP Application
VM1	Panasonic SD Voice
VMC	Virtual PC virtual machine configuration
VMCX	Virtual Machine Shell Information
VMD	Optical Simulation Rendering VMD format
VMDK	(part of a) VMware 3 Virtual Disk
VMF	Valve Map Format
VMG	Nokia Saved SMS
VMLF	Sony Picture Motion Browser Film roll
VMLT	Sony Picture Motion Browser video data
VMO	Emergency people animation data
VMS	Hamamatsu Virtual Microscope Specimen
VMT	Valve Material Type
VMX	VMware configuration
VMXF	VMware supplemental team member configuration
VNT	Sony Ericsson Mobile Phone Note

Supported file type	Description
VOB	VOB video files
VOC	Creative Voice audio
VOICES	Music-X Voices
VOR	StarOffice template (generic)
VOT	VOTable
VOX	Dialogic VOX (telephony) encoded audio
VP	VOCPACK lossless compressed audio
VP3	VP3 sewing machine file
VP5	On2 TrueMotion VP5 video
VP6	VP6 encoded video
VPDB	VIP Organizer DB
VPJ	SlickEdit project
VPK	Valve Package (v1)
VPM	Garmin Voice Processing Module
VPN	Shrew VPN configuration
VPP	Visual Paradigm Project
VPT	Visual Pinball Table
VPU	Avast setup-update package
VQA	Westwood VQA multimedia format

Supported file type	Description
VQF	TwinVQF audio
VRF	Ventrilo audio recording
VRO	DVD Video Recording format
VRS	VICE Rom Set
VRT	GDAL Virtual Format
VSCT	Visual Studio Command Table configuration (XML)
VSD	Microsoft Visio Drawing
VSDISCO	DISCO Dynamic Discovery file
VSDX	Visio 2013 drawing
VSF	ViPlay Subtitle Format
VSGLOG	Visual Studio Graphics Analyzer Log
VSIX	Visual Studio Extension
VSIXMANIFEST	VSIX Manifest
VSPS	Visual Studio analyzed Performance report
VSPX	Visual Studio Performance report data
VSQ	Vocaloid Sequence
VSQX	Vocaloid 3D Project
VSS	Microsoft Visio Stencil

Supported file type	Description
VSSETTINGS	Visual Studio Settings
VST	Microsoft Visio Template
VSTEMPLATE	Microsoft Visual Studio project template
VSTO	Visual Studio Tools for Office add-in
VSTPRESET	VST Preset
VSZ	Visual Studio wizard
VT	Vic-Tracker module
VT2	Vortex Tracker 2 chiptune
VTF	Valve Texture Format
VTHOUGHT	Visual Thought diagram
VTI	ParaView VTK Image data
VTK	Visualization Toolkit format
VTP	VisionTools Pro-e source
VTR	ParaView VTK Rectilinear grid
VTS	ParaView VTK Structured grid
VTT	Web Video Text Tracks
VTU	ParaView VTK Unstructured grid
VTX	Vortex Tracker (AY) chiptune
VUE	Vue D'Esprit 4 Scene File

Supported file type	Description
VUZE	Vuze link
VV	virt-viewer configuration
VVD	Valve Studio Model Vertex Data
VVP	Icarus Verilog VVP format
VVVVV	VVVVV map
VW2	Lotus Magellan Viewer (v2.x)
VWF	Quartus Waveform simulation
VWL	Vuforia Word List
VWR	Lotus Magellan Viewer (v1.x)
VXD	VXD Driver
VXL	Voxel Animation
VXM	vTask Studio script
VXP	Maui Runtime Environment application (Zlib packed)
VYM	VYM Mind Map
VZ	VZ200/300 image (type F0)
VZT	Verilog/VHDL Zipped Trace
W2M	Solo Explorer Transcription
W3D	Shockwave 3D Scene Export

Supported file type	Description
W3M	WarCraft III map
W3Z	WarCraft III saved game
W64	Sonic Foundry Wave-64 audio
WAB	Outlook Express addressbook
WACOMXS	Wacom eXpert Settings
WAD	DoomRL WAD resource
WAL	Black and White 2 Wall data
WALLET	Multibit Bitcoin wallet
WAR	Java Web Archive
WARC	Web ARChive File Format
WATCH	WatchMaker Watch face
WAV	ECHOSPEECH encoded audio
WAV/BWF	Broadcast Wave File audio
WB1	Webshots Image
WB1/WB2	Quattro Pro spreadsheet
WB3	Quattro Pro 7 spreadsheet
WBA	WindowBlinds Progress Anim theme
WBD	Softlink Whiteboard data
WBDP	Workbench DesignPoint Data

Supported file type	Description
WBEX	ANSYS Workbench Binary Extension
WBK	Writer's Block document
WBM	Webmin Module
WBS	Winbot Script
WBZ	WebShots Image
WCM	Corel WordPerfect Macro
WCP_SETTINGS	Alpha Five Web Project Settings
WCST	Wirecast Setup
WCX	FAR TC.Packer PlugIn
WCZ	Chamaleon Clock wallpaper clock skin
WDB	Microsoft Works Database
WDE	WinDev Report
WDI	WinDev Component description
WDK	WinDev Component
WDL	DynaDoc Electric Exchange Document
WDP	WinDev Project
WDPROJ	Visual Studio Web Deployment Project
WDR	Psion Serie 3/3a printer driver
WDW	WinDev Window

Supported file type	Description
WDX	Total Commander Content plugin
WDY	WinDev Run-Time Template
WDZ	WINDEV compressed archive
WEA	WeatherTool weather data
WEB	BlackWidow Website Description
WEBARCHIVE	Apple Safari WebArchive
WEBARCHIVEXML	Android browser XML webarchive
WEBHISTORY	Safari Web History
WEBLOC	Apple Finder Internet Location
WEBM	WebM video
WEBP	WebP bitmap
WEBPART	SharePoint Web Part
WEBTEST	Fiddler saved WebTest
WED	Infinity Engine region/map (v1.x)
WER	Windows Error Report
WF1	EViews Workfile
WFM	Rigol waveform
WFN	Wordup Graphics Toolkit Font
WFX	AIM Extended Wavefunction

Supported file type	Description
WGEO	League of Legends World Geometry
WGP	WingMan profile
WGS	Thief: Deadly Shadows save game
WGZ	Nokia S60 Web Runtime Widget Package
WHL	Wheel package
WHX	WinHex backup
WIC	J Wavelet Image Codec bitmap
WIDGET	Konfabulator widget
WIF	CoffeCup Web Image Studio
WIM/SWM	Windows Imaging Format
WINDSPROSKIN	WinDS Pro Skin
WINGS	Wings 3D mesh
WIQ	Visual Studio Work Item Query
WIRE	Autodesk Alias 2017 Model
WIX	Xara graphics
WIXLIB	WiX Library
WIXOBJ	WiX Object
WIXPROJ	WiX Project
WJ3	Lotus 123 Worksheet (V2J)

Supported file type	Description
WJF	WinZip Job File
WK	Khoros Visual Programming Workspace
WK1/WR1	Lotus 123/Symphony Worksheet (V2)
WK3	Lotus 123 Worksheet (V3)
WK3/Wk4/WT4/FM3/123	Lotus 123 Worksheet/format (V3-)
WK4/WT4	Lotus 123 Worksheet (V4)
WKF	VISI-serie CAD/CAM work file
WKQ	Quattro for DOS spreadsheet (v1.0)
WKS	DeskMate worksheet
WKSP	Khoros/Cantata Workspace
WKZ	DOS Navigator spreadsheet
WL1/VS1/BS1	GameMaps format
WLD	Morfit WorldBuilder document
WLF	WLF WolfMAME recording info
WLM	CompW bitmap
WLMP	Windows Live Movie Maker Project
WLS	602Tab Workbook
WLX	Garmin MapSource Web Link
WM/WM2D	Working Model 2D data

Supported file type	Description
WM3	MSC.visualNastran Desktop Document
WMD	Windows Media Download package
WMF	L3DT Water Map File
WMV/WMA	Windows Media (generic)
WMZ	Windows Media Player skin
WOF	Hercules WriteOn Font
WOFF	Web Open Font Format
WOFF2	Web Open Font Format 2
WOL	WOLF eBook
WOR	MapInfo Workspace
WOTREPLAY	World of Tanks battle recording
WOWPROJ	AddOn Studio for Word of Warcraft Project
WOWSL	WOW Slider settings
WOWSREPLAY	World of Warships Replay
WP	WordPerfect 4.2 document
WP/DOC	Enterprise 128 Word Processor document
WP2	WinPlot data (v2)
WP3	WinPlot data (v3)
WPA	ACT! word processor document

Supported file type	Description
WPD	602Text Document
WPF	Enable document
WPG	WordPerfect Graphics bitmap
WPI	WarpIN Installer
WPJ	Microsoft Works wizard
WPL	Windows Media Player playlist
WPM	WordPerfect Macro
WPROJ	Wwise Project
WPS	KingSoft WPS2000 document
WPT	602PC Suite Template Document
WQ1	Quattro Pro for DOS spreadsheet (v2.x-4.x)
WQ2	Quattro Pro for DOS spreadsheet (v5.x)
WR1	Lotus Symphony Worksheet (V1)
WR3/WRA	WRaptor compressed
WRD	EPOC Word document
WRF/WOT	WebEx Recording
WRI	Windows Write Document
WRK	Cakewalk Music project
WRL	Virtual Reality Modeling Language

Supported file type	Description
WRPL	War Thunder replay
WS	IBM iSeries Client Access WorkStation profile
WSC	Windows Script Component
WSD	WordStar for Windows document
WSDL	Web Services Description Language
WSE	Wise script
WSF	Windows Script File
WSI	Lenovo OneKey Recovery info
WSKN	Wise Care 365 Skin
WSP	FlowJo PC Workspace
WSQ	Wavelet Scalar Quantization bitmap
WSSTYLES	Windows Sidebar Style
WST	WebMSX Save State
WSZ	WinAmp 2.x Skin
WTF/HGM	Hourglass movie capture
WTL	Windows Test Technologies (WTT) logger results
WTML	WorldWide Telescope collection
WTT	WorldWide Telescope Tour

Supported file type	Description
WTV	Windows Media Center recorded Television Video
WUP	WhatsUp Gold network map
WV	Sonarc compressed WAV audio
WVC	WavPack compressed audio correction data
WVD	Wang Virtual Disk image
WVE	Cyberlink WaVeEditor project
WVF	Yokogawa waveform data
WVX	Windows Media redirector / shortcut
WVZ	MUST music / song
WWD	Claw custome level
WWP	WWarp disk image
WWU	Wwise Work Unit
WXL	WiX Localization (ASCII)
WXN	Waixing Famicom Game ROM
WXP	EXP document
WXS	WiX Source
WYG	WYSIWYG project data
WZ	MapleStory game data

Supported file type	Description
WZD	Sharp Wizard data (generic)
X	Aurora Editor compiled macro
X_B/X_T	Parasolid model
X2D	XML 2D graphics
X3D	Extensible 3D vector graphics (XML)
X3DB	Extensible 3D vector graphics (binary)
X3DV	Extensible 3D vector graphics (VRML)
X3F	Sigma - Foveon X3 raw picture
X3G	MakerBot 3D print format
X83	GAEB-Format X83
XA	Maxis XA Audio (generic)
XAB/XDB/XGR/XPF/XSS/XTX	Ability document
XADML	XML-based Application Description information
XAF	3ds Max XML Animation File
XAIML	eXtended Artificial Intelligence Markup Language
XAML	Microsoft Extensible Application Markup Language
XAMLX	Visual Studio Workflow service data
XANIM	FSX Aircraft Animation

Supported file type	Description
XAP	Silverlight Application Package
XAPK	Android Package with OBB data
XAR	XAR archive
XB	XBIN image/palette/font data
XBAP	XAML Browser Applications
XBCD	Xilinx internal data
XBDR	Darkroom Booth template
XBE	XBOX executable
XBEL	XML Bookmark Exchange Language
XBF	XAML Binary Format
XBK	SMART Board Slide Collection
XBM	X Bitmap
XBRL	eXtensible Business Reporting Language
XBS	XnConvert configuration
XCCOLORTHEME	Xcode Color Theme (old)
XCF	The GIMP image format
XCLF	Source Insight Custom Language File (XML)
XCScheme	Xcode Scheme
XCWORKSPACEDATA	Xcode Workspace Data

Supported file type	Description
XDD	XFIT XDD format data file
XDF	TunerPro Definition
XDI	WinArchiver Extended Disc Image
XDP	XML Data Package
XDR	X-CAD Drawing
XDS	LCDStudio Design
XDT	Termbase definition
XDV	X86 Delta Compiler Video
XDW	DocuWorks File
XDXF	XML Dictionary eXchange Format
XEP	XenoDream Graphics Data
XEX	Xbox 360 Executable
XEX/EXE	Atari XE Executable
XFB	Binary Device Interface File Format
XFD	Acu4GL/AcuCOBOL Extended File Descriptor
XFDF	XML Forms Data Format
XFDL	XFDL form
XFM	MNI Transform File
XFR	Xfrog organic 3D model

Supported file type	Description
XGMML	eXtensible Graph Markup and Modeling Language
XGR	GraphEdit Filter Graph Markup Language
XGS	XACT Global Settings
XHN	EASE ASCII-format speaker
XI	eXtended Instrument (generic)
XIF	Text Device Interface File Format
XIMG/IMG	Extended GEM bitmap
XIP	Hotbar skin
XISE	Xilinx ISE Project
XKS	IBM Softcopy Reader PDF Extended bookshelf file
XLAM	Excel Macro-enabled Open XML add-in
XLF	XLIFF - XML Localization Interchange File Format (Unicode)
XLF/XLIFF	XLIFF - XML Localization Interchange File Format
XLO	Autodesk Inventor Export Journal
XLR	Microsoft Works Spreadsheet
XLS/XML	Microsoft Excel XML spreadsheet
XLSM	

Supported file type	Description
	Excel Microsoft Office Open XML Format document (with Macro)
XLSX	Excel Microsoft Office Open XML Format document
XLT	Biew Xlat Table
XM	FastTracker 2 eXtended Module
XMBL	Logger Pro data
XMCD	Mathcad XML based worksheet
XMCT	Mathcad XML Worksheet Template
XMD	BitDefender plug-in
XMF	Cal3D Xml Mesh File
XMFG	MediaForge Runtime Player Distribution Project
XMI	Extended MIDI
XMIND	XMind Workbook
XMIX	eXtensible Music and Instruments Xml
XML	7DTD prefabs properties
XML/ADF	Auto-lead Data Format
XML/ATOM	Atom web feed
XML/RSS	RSS web feed

Supported file type	Description
XMLTV	XMLTV format
XMOD	Monarch Pro model
XMOVE/XML	XMOVE 3D trajectories format
XMP	Adobe Extensible Metadata Platform
XMS	XMS-Tracker module
XMU	SmartUML UML diagram
XMV	Xbox Video
XNB	XNA Framework Content Pipeline Binary
XNK	Microsoft Exchange Server Shortcut
XOJO_CODE	Xojo build
XP0	Secret Photos puzzle
XP2	XPilot NG map
XP3	KiriKiri Adventure Game System package
XPA	Xpack compressed archive
XPADDERCONTROLLER	Xpadder Controller layout
XPDL	XML Process Definition Language format
XPF	LMMS Preset
XPI	Mozilla Firefox browser extension
XPJ	RoboHelp XML Project

Supported file type	Description
XPL	LCDStudio configuration Playlist
XPM	X PixMap bitmap
XPR	Creature House Expression3 drawing
XPT	SAS Transport (XPORT) format
XQL/XQM/XQY	XML Query Language
XRC	wxWindows - wxPython Resource
XRDML	XRDML data
XREPORT	ISE XReport
XRF	Cal3D Xml material File
XRM-MS	Microsoft security certificate
XRNI	Renoise Instrument
XRNS	Renoise module (w/o samples)
XRNT	Renoise effects chain
XRP	RationalPlan project
XRPT	ISE Report
XS3/XS4/XS5	XESS worksheet (generic)
XSB	XACT Sound Bank
XSD	DFDL schema
XSH	Amapi Shader

Supported file type	Description
XSI	SoftImage XSI 3D image
XSIADDON	XSI Addon
XSIG	XML Signature
XSN	InfoPath Dynamic Form - Template
XSP	XBMC Smart Playlist
XSPF	XML Shareable Playlist Format
XSVF	Xilinx Serial Vector Format
XTC	XTrkCAD project
XTG	QuarkXPress Tags
XTODVD	ConvertXtoDVD project
XTP	InfoPath Template Part
XTR	XTrkCAD demo
XTRACHART	DevExpress Chart
XTREME	Winstep Xtreme Theme Pack
XUI	Xbox 360 User Interface
XUL	Mozilla XML User interface Language
XUS	UpdateStar info
XVC	MuPAD Uncompressed VCam Graphics
XWD	X Windows Dump bitmap

Supported file type	Description
XWF	Declan Software word file
XWP	XWinPlot layout
XWRL	XML Virtual Reality Modeling Language
XWS	Xara WebStyle file
XXX	Compucon/Singer PSW Embroidery Design File
XZ	xz compressed container
Y4M	YUV4MPEG2 video
YAL	Arts and Letters clip art library
YAML	YAML serialized data
YANG	YANG data model
YBK	YanCEyWare Reader eBook
YES	Quick Bible document
YKA	Yenka model
YM	ST-Sound YM chiptune
YM/YMST	YM2149 song
YMV	Yabause movie capture
YPR	BYOB project
YRP	YGOPRO replay

Supported file type	Description
YSP	BYOB sprite
YTD	Grand Theft Auto 5 Texture Dictionary
YTF	Picasa font cache
YTR	IRIS OCR data
YY	GNU Bison grammar
YYY	CrLZH compressed
YZ1	Yamazaki Zipper compressed archive
Z	InstallShield archive
Z/GZ/GZIP	GZipped data
Z2S	Zoo Tycoon 2 Saved game
Z3D	ZModeler 3D Model
Z5	Z-Code V5 adventure for Infocom Z-Machine
Z8	Z-Code V8 adventure for Infocom Z-Machine
Z88	OZvm snapshot
ZAB	Zipped Audio Book
ZAM	ZBrush Array Mesh
ZAN	BlueEyes Animation
ZAP	ZoneLabs Zone Alarm data
ZARGO	ArgoUML Zipped package

Supported file type	Description
ZBP	ZBrush Preset
ZBR	ZBrush Document
ZDB	ZenPhoto Database Backup
ZDP	Avery DesignPro Label design
ZDS	ZDoom savegame
ZED	ZX-Edit document
ZEG	ZeroG subtitles
ZEL	Zelio Soft project
ZET	ZET compressed archive
ZEXP	Zope binary export file
ZF3D	Flare3D model
ZFP	ZBrush Fiber Preset
ZFX	ZipForm data
ZGEPROJ	ZGameEditor project
ZGR	ZBrush Grid
ZIM	ZIM format
ZING	Zing! directory info
ZIP	Archive file format that supports lossless data compression

Supported file type	Description
ZIR	Compass and Ruler geometry
ZL	Easy CD Creator Drag to Disk File
ZLIC	ZBrush License
ZMA	ZMA impedance response data
ZMI	ZAP Meta Image
ZMT	ZBrush Material
ZMX	ZEMAX lens data
ZNM	ZBrush Noise Maker
ZNO	Zinio Reader Magazine
ZOO	Microsoft Zoo Tycoon saved game
ZOT	Zoot information processor database
ZPAQ	zpaq compressed archive
ZPJ	Zephyr Eclipse server Project
ZPL	Zune PlayList
ZPP	ZPanel Package
ZPR	ZBrush Project
ZSC	ZBrush Script
ZSG	Zillions of Games Solution - Saved Game
ZST	ZSNES Save State

Supported file type	Description
ZSYNC	zsync meta data
ZTH	DivX Connected Theme
ZTL	ZBrush ZTool native format
ZTQ	z-Tree Questionnaire
ZTT	z-Tree Treatment
ZUML	Poseidon for UML project file
ZVD/ZYX	ZyXEL Voice Format audio
ZVPL	Visual Paradigm License Key
ZVR	Recorded voice audio
ZW	Zooper Widget template
ZX82	Speculator '97 snapshot
ZXS	zx32's ZXS snapshot format
ZZ	Zzip compressed archive
ZZT	ZZT Game Creation System data format

This article applies to MetaDefender Core v3 and v4


This article was last updated on 2018-03-19.


EF

What links, target-services or target host-IP's need to be allowed for MetaDefender Core v4?

If you have installed or if you wish to use the MetaDefender Core in a restricted environment, you will have to allow access to the following hosts' for an accurate functioning of MetaDefender Core:

- <https://activation.dl.opswat.com> - this is for product activation/licensing
- <https://update.dl.opswat.com> - this is for fetching engine/database updates

 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.

 Note: IP address based whitelisting might fail after some time as OPSWAT uses CDN (Content Delivery Network) to faster delivery updates over the world and IP address of edge servers might change over time.

This article applies to the MetaDefender Core v4

This article was last updated on 2018-03-26

CN

What operating system patches should be applied to the system hosting MetaDefender Core?

We recommend that you keep the operating system hosting MetaDefender Core completely updated with the latest operating system updates.

The systems in OPSWAT's labs are updated with the latest patches and thus MetaDefender Core is tested and optimized for that condition.

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-26

CN

What should I do if an engine is in "failed" or "permanently_failed" status?

Sometimes after activating MetaDefender Core v4, during the engines downloading, some of the engines may be in "failed" or "permanently failed" status.

In this case, you can do the following :

- Make sure your system adheres to our [system requirements](#).
- Go to Inventory → Scan Nodes page and check the Nodes one by one and see if there is any issue displayed on the Issues tab. Resolve the issues displayed. Example of issues:
 - If Data Sanitization is the single engine which is not active, you may have to install .NET framework 4.6 and restart the MetaDefender core services.
 - If you have a local antivirus product installed, you have to add both the OPSWAT and the resources folders to the exclusions list of that antivirus product and then follow the above steps again.
- Disable and enable each failed engine, one after another on the Inventory → Engines page.

If you have followed all of these steps and your engines are still unusable, please see [how to create support package](#), login into [OPSWAT Portal](#) and open a ticket with us with the support package attached.

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-26

CN

Where can I submit false positives detected by MetaDefender Core v4?

Below is a list of where you can send false positives detected by MetaDefender Core V4 to:

AhnLab

Email 1: v3sos@ahnlab.com

Email 2: e-support@ahnlab.com

Avira AntiVir

Submission: <http://analysis.avira.com/samples/>

AVG

Email: virus@avg.com

Info: <https://support.avg.com/SupportArticleView?urlname=How-to-report-a-false-incorrect-detection>

Submission: <https://secure.avg.com/submit-sample>

BitDefender

Submission: <http://www.bitdefender.com/submit>

Email: oemsamples@bitdefender.com

ClamAV

Submission: <https://www.clamav.net/reports/fp>

Emsisoft

Submission: <https://www.emsisoft.com/en/support/submit/>

ESET / Nod32

Email: samples@eset.com

Info: <http://kb.eset.com/esetkb/index?page=content&id=SOLN141>

Filseclab

Email: fp@filseclab.com

F-PROT / Cyren

Info: http://www.f-prot.com/virusinfo/false_positive_form.html

Submission: <https://kb.cyren.com/av-support/?/Tickets/Submit/RenderForm/7>

F-Secure

Submission: https://www.f-secure.com/en/web/labs_global/submit-a-sample

Ikarus

Email 1: false-positive@ikarus.at

Email 2: samples@ikarus.at

K7

Email 1: support@k7computing.com

Email 2: reportfp@labs.k7computing.com

Info: <https://support.k7computing.com/index.php?/Knowledgebase/Article/View/3/0/how-to-report-a-false-detection>

Kaspersky

Email: newvirus@kaspersky.com

Submission: <https://newvirus.kaspersky.com/>

Info: <http://forum.kaspersky.com/index.php?showtopic=13881> - Here you will have to scan again the file and if you don't agree with the scan result, you will be able to send the sample to Kaspersky for deep investigation.

Lavasoft

Submission: http://www.lavasoft.com/support/securitycenter/report_false_positives.php

McAfee

Info: <https://kc.mcafee.com/corporate/index?page=content&id=KB85567>

Email: virus_research@avertlabs.com

Contact: <https://kc.mcafee.com/corporate/index?page=content&id=KB67411>

Microsoft Security Essentials and Windows Defender

Email: windefend@submit.microsoft.com

Submission: <https://www.microsoft.com/security/portal/submit/submit.aspx>

nProtect

Email: support@nprotect.com

Quick Heal

Submission: <http://support.quickheal.com/v4/index.php?/Tickets/Submit/RenderForm>

Sophos

Submission: <https://secure2.sophos.com/support/contact-support.aspx>

Info: <http://www.sophos.com/support/knowledgebase/article/35504.html>

STOPzilla

Submission: <http://www.stopzilla.com/support/false-positive/>

Symantec / Norton

Submission: https://submit.symantec.com/dispute/false_positive/

Systweak

Submission: <http://support.systweak.com/kayako/index.php?/Tickets/Submit>

Trend Micro

Email: trendlabs@av-emea.com

Submission: <https://success.trendmicro.com/sign-in?startURL=/new-request?issue=analyze>

Info: <https://esupport.trendmicro.com/en-us/home/pages/technical-support/1031392.aspx>

VirIT/TGSoft

Submission: http://www.tgsoft.it/italy/file_sospetti.asp

VirusBlokAda

Email: newvirus@anti-virus.by

Submission: <http://www.anti-virus.by/check/>

Xvirus

Email: samples@mysecuritywin.com

Submission: <https://xvirus.net/submit>

Zillya

Email: virus@zillya.com

Submission: <https://zillya.com/support>

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-26

CN

Which are the supported archive formats for MetaDefender Core v4?

The Archive configuration determines how archives are handled within MetaDefender Core. If archive handling is enabled, MetaDefender Core extracts archives and scans the individual files within the archive.

- The supported archive formats are the following: Zip, 7z, Jar, rar, rar5, tar, ISO, Gzip, CAB, ARJ, LZH, RPM, DEB, LZMA, WIM, SFX, XZ, VDI, VHD, MBR, CPIO, HFS, .apk, .gz, .msi, .tgz, .tbz, bz2. Metadefender Core can also extract self-extracting archives created by both 7zip and WinRAR
- Microsoft Office Documents (e.g., DOCX files) are detected as archive files by default
- For more information, please see the screenshot below:

Enable archive handling ⓘ

Max recursion level ⓘ

Max number of files extracted ⓘ

Max total size of extracted files [in megabytes] ⓘ

Enable scan original unextracted archive ⓘ

Timeout for handling the archive [in minutes]

Note: We do not maintain a list of supported non-archive files. All file types are supported for scanning.

This article applies to MetaDefender Core v4

This article was last updated on 2018-10-23

TV

Why don't I see the Data Sanitization engine in MetaDefender Core v4?

The Data Sanitization engine was introduced in MetaDefender Core v4 in release v4.5.1. You should see it as an engine listed in your engine inventory in the management console (From the sidebar menu, go to Inventory → Engines)

If you have upgraded to v4.5.1 or newer from an older release and the Data Sanitization engine is missing, you will need to deactivate and then reactivate MetaDefender. You do this by following these steps:

- Access the MetaDefender Core Management Console by typing the following link into a browser: <http://localhost:8008/> or <http://:8008/> depending on your setup (this could be https://your_host_name:8008/).
- From the left panel, click on Settings -> License

- In the upper right corner, click on Activate (or click on the drop-down list if you can't see the Activate option)
- Introduce your license key and how many nodes you want to use with this Core instance (specified number should be less than or equal with your free license slots for this product)

To check the status of the Data Sanitization engine, you can go to Inventory → Engines.

If after following these steps Data Sanitization is not available, please feel free to log a ticket with us on the [OPSWAT Portal](#).

This article pertains to MetaDefender Core v4.5.1 and above

This article was last updated on 2018-03-26

CN

Why should I upgrade my MetaDefender Core v4?

Upgrading to the latest releases of OPSWAT products allows you to take advantage of new features, added functionality, bug fixes and performance improvements. It also ensures the best path to timely support.

OPSWAT typically has a new release of the MetaDefender Core once a month. We recommend that you uptake each new release as it comes out. For organizations that have more restrictive upgrade policies, we recommend that you plan out regularly scheduled upgrades as part of your application management procedures.

Customers with active licenses are entitled to upgrade for free. The upgrade can be done self-service by downloading the latest installer from our [portal](#) in the [Products section](#) and following the guidelines in our [documentation](#).

Note that Metascan was renamed MetaDefender Core, but the license is interchangeable. i.e. a license for Metascan is the same as a license for MetaDefender Core. Customers with active licenses can download the latest MetaDefender Core releases.

This article applies to MetaDefender Core v4

This article was last updated on 2018-03-26

CN