

OPSWAT.

MetaDefender

MetaDefender Core v4.19.0

Table of Contents

About This Guide	14
Key Features of MetaDefender Core	15
1. Quick Start with MetaDefender Core	16
1.1. Installation	16
Basic setup	16
1.1.1. Configuration wizard	16
1.2. License Activation	22
1.3. Process Files with MetaDefender Core	22
2. Installing or Upgrading MetaDefender Core	23
2.1. Recommended System Configuration	23
Microsoft Windows Deployments	24
Unix Based Deployments	26
Data Retention	28
Custom Engines	28
Browser Requirements for the Metadefender Core Management Console	28
2.2. Installing MetaDefender	29
Installation	29
Installation notes	29
2.2.1. MetaDefender Core 4.18.0 or older	30
2.2.2. MetaDefender Core 4.19.0 or newer	33
2.3. Upgrading MetaDefender Core	38
Upgrading from MetaDefender Core 3.x to 4.x	38
Upgrading from MetaDefender Core older version to 4.18.0 (SQLite)	38
Upgrading from MetaDefender Core 4.18.0 or older (SQLite) to 4.19.0 or newer (PostgreSQL):	39
Upgrading from MetaDefender Core 4.19.0 to newer (PostgreSQL):	40
2.4. MetaDefender Core Licensing	41

2.4.1. Activating Metadefender Licenses	41
2.4.2. Checking Your Metadefender Core License	46
2.5. Performance and Load Estimation	47
What to know before reading the results: Some factors that affect performance	47
How test results are calculated	48
Test Reports	48
2.5.1. MetaDefender Core 4.19.0 or newer (PostgreSQL)	48
2.5.2. MetaDefender Core 4.18.0 or older (SQLite)	54
2.6. Special installation options	60
Use RAMDISK for the tempdirectory	60
3. Configuring MetaDefender Core	64
3.1. Management Console	64
3.1.1. Password Recovery	65
3.2. MetaDefender Configuration	72
3.2.1. Startup Core Configuration	73
3.2.2. Startup Node Configuration	82
3.2.3 Nginx related configuration	89
3.3. User management	98
3.3.1. Users and groups	99
3.3.2. Roles	104
3.3.3. User directories	109
3.3.4. Active Directory attributes	116
3.3.5. Change user password	119
3.3.6. Single Sign-On (SSO)	120
3.4. Update settings	143
Internet	144
Folder	145
Manual	145
3.5. Clean up scan database	146
Technology Note:	146
3.6. Policy configuration	146
3.6.1. How MetaDefender Core policies work	147
3.6.2. Workflow template configuration	147
3.6.3. Security zone configuration	161

3.6.4. Workflow rule configuration	162
3.6.5. Quarantine	167
3.7. Logging	175
3.7.1. Configuration	175
3.7.2 Log message format	176
3.7.3 Syslog message format	177
3.7.4 Error Message Description Table	181
3.8 Security settings on web console	222
3.8.1 Enabling HTTPS	222
3.8.2 Session timeout	227
3.8.3 Password Policy	227
3.9. Configuring proxy settings	229
How can I set proxy server for the product	229
3.10. External Scanners And Post Actions	230
External Scanners	230
Post Actions	233
3.11. Yara rule sources	235
3.12 Server Configurations	238
3.12.1 Email Configuration	238
3.12.2 Proxy Configuration	239
4. Process files with MetaDefender Core	241
Process Files via REST API	241
Process Files via Web Interface	241
Choose what to process and how	242
5. Deep CDR (Data Sanitization)	243
6. Proactive DLP	245
7. Operating MetaDefender Core	246
7.1. Dashboard	246

Overview page	247
Processing history	247
Quarantine	248
Update history	248
7.2. Inventory Management	249
7.2.1. Certificates	249
7.2.2. Modules	252
7.2.3. Nodes	262
7.2.4. Skip by hash	264
7.3. Regular Maintenance	266
Checking for Upgrades	266
Checking Engines / Databases Health	266
7.4 Import/Export configuration	267
Export	267
Import	267
Note	268
7.5. Database Defragmentation and Optimization	268
7.6. Reporting	271
7.7. Statistics	273
8. MetaDefender Core Developer Guide	274
How to Interact with MetaDefender Core using REST	274
File scan process	274
8.1. MetaDefender API	274
8.1.1. Sessions	275
8.1.2. Licensing	278
8.1.3. Processing files	283
8.1.4. Processing files in batch	312
8.1.5. Download Sanitized Files	324
8.1.6. Vulnerability Info In Processing Result	326
8.1.7. Skip by hash	329
8.1.8. Get version of components	335
8.1.9. Configuration related APIs	337
8.1.10. Yara	474
8.1.11. Webhooks	481

8.2. MetaDefender API Code Samples	486
9. (NEW) MetaDefender Core Developer Guide	488
10. Advanced MetaDefender Deployment	489
10.1. Scripted license management	489
Requirements	489
Activation steps	489
Deactivation steps	491
Important notes	492
10.2. Deployment automation support	492
Installation	493
Initialization	494
Configuration	498
10.3. Cloud Deployment	498
10.3.1. AWS Deployment	498
10.4. Multi-node deployment	518
Setting up several Metadefender Core nodes	518
10.5. Using external load-balancer	522
10.5.1. HTTP(S) - Layer 7 load balancing	522
10.5.2. DNS load balancing	525
11. Troubleshooting MetaDefender Core	528
Installation issues	528
Issues with nodes	528
Where are the Metadefender Core logs located?	528
How can I create a support package?	528
Issues under high load	528
Debug logging	529
Engine Clean-up Tool	529
MetaDefender Core 4.19.0 database information to connect	530

Example usages	530
How to Create Support Package?	534
Creating the package on Linux	534
Creating the package on Windows	534
Content of the created package	535
How to Read the Metadefender Core Log?	535
Files	535
Format	535
Severity levels of log entries	536
Inaccessible Management Console	536
How to detect	536
Solution	537
Possible Issues on Nodes	537
Q. Node detected 3rd party product on system	537
Q. There is no scan node connected	537
Too Many Sockets or Files Open	538
How to detect	538
Solution	538
Too Many TIME_WAIT Socket	539
How to detect	539
Solution	540
Technical Insights	540
12. Release notes	542
12.2 Proactive DLP Release Notes	544
v2.4.1	544
v2.4	545
v2.3.2	545
v2.3.1	545
v2.3.0	545
v2.2.1	546
v2.2	546
v2.1.2	546
v2.1.1	546
v2.1	546
v2.0.1	547

v2.0	547
v1.0.3	547
12.3 File Type module Release Notes	547
v5.2.26	547
v5.2.25	547
v5.2.24	547
v5.2.23	548
12.4 Archive module Release Notes	548
v5.3.5	548
v5.3.4	548
v5.3.3	548
v5.3.2	548
12.4 MetaDefender Core archived release notes	548
Version v4.18.0	548
Version v4.17.3	551
Version v4.17.2	553
Version v4.17.1	556
Version v4.17.0.1	557
Version v4.17.0	557
Version v4.16.3	559
Version v4.16.2	559
Version v4.16.1	560
Version v4.16.0	560
Version v4.15.2	561
Version v4.15.1	561
Version v4.15.0	562
Version v4.14.3	563
Version v4.14.2	564
Version v4.14.1	564
Version v4.14.0	565
Version v4.13.2	565
Version v4.13.1	565
Version v4.13.0	565
Version v4.12.2	566
Version v4.12.1	566
Version v4.12.0	566
Version v4.11.3	567
Version v4.11.2	567
Version v4.11.1	568

Version v4.11.0	568
Version v4.10.2	568
Version v4.10.1	569
Version v4.10.0	569
Version 4.9.1	570
Version 4.9.0	570
Version 4.8.2	571
Version 4.8.1	571
Version 4.7.2	573
Version 4.7.1	573
Version 4.6.3	574
Version 4.6.2	574
Version 4.6.1	574
Version 4.6.0	575
Version 4.5.1	576
Version 4.5.0	576
Version 4.4.1	576
Version 4.3.0	577
Version 4.2.0	578
Version 4.1.0	579
Version 4.0.1	579
Version 4.0.0	579
13. Legal	581
Copyright	581
DISCLAIMER OF WARRANTY	581
COPYRIGHT NOTICE	581
MetaDefender Export Classification	581
14. Knowledge Base Articles	583
Are MetaDefender Core v4 upgrades free?	584
Are there any limitations regarding the MetaDefender Core v4 scan engines?	585
Can I control access to the RAM disk in MetaDefender Core v4?	586
Does Metadefender Core v4 offer real-time antivirus protection on the system where it is installed?	586

Does MetaDefender Core v4 Detect the NotPetya Ransomware?	586
Does the fixing updates for Meltdown and Spectre vulnerabilities affect any engines in MetaDefender Core v4?	588
Engine clean-up instructions	589
External scanners in MetaDefender core v4.8.0 and above	592
How can I configure the maximum queue size in Metadefender Core v4 ?	595
How can I find a sanitized file scanned with MetaDefender Core v4?	596
How can I increase the scaling up performance?	596
How can I run tests to see the different scan results on MetaDefender Core v4?	599
How can I upgrade from Core v4.7.0/v4.7.1 to a newer Core v4.7 release	600
How can the TEMP folder be changed?	602
How do I check if "noexec" flag exists on a Linux OS?	603
How do I collect verbose debug packages on MetaDefender Core v4 for Linux?	604
How do I deploy MetaDefender Core v4 to an offline Linux environment?	605
Installing MetaDefender Core	606
Activate your license	606
Installing the MetaDefender Update Downloader utility	608
Applying offline updates	610
Contacting OPSWAT Support	610
How do I deploy MetaDefender Core v4 to an offline Windows environment?	611
Installing MetaDefender Core	611
Activate your license	612
Installing the MetaDefender Update Downloader utility	614
Applying offline updates	616
Contacting OPSWAT Support	617
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?	617
How do I remove an engine from my MetaDefender v4 instance?	618
How do I use MetaDefender Core v4 Workflows ?	619
Defining and administering Workflow Templates in MetaDefender Core v4	619
How long is the support life cycle for a specific version/release of MetaDefender Core v4?	620

How to install MSE on Windows Server 2012 R2 and Windows Server 2016	623
MSE on Windows Server 2012 R2	623
MSE on Windows Server 2016	627
How to transfer your Metadefender Core v4 scan history database	633
Installing .NET Core runtime 3.1 on Linux for Proactive DLP 2.4.0+	633
Is Metadefender Core compromised while scanning files?	637
Is there a virus test I could use to test MetaDefender Core v4?	637
MetaDefender Core v4 shows a large number of files that failed to scan. What can I do?	638
Microsoft Visual C++ 2017 Redistributable requirement for Deep CDR 5.8 or newer	640
How to install Microsoft Visual C++ 2017 Redistributable?	640
What happens if you haven't installed Visual C++ 2017?	640
What should you do if you can't install Visual C++ 2017?	642
What should you do if Deep CDR 5.8+ becomes "permanently failed"?	642
Post actions in MetaDefender Core V4.8.0 and above	643
Queue mechanism on Metadefender Core v4	645
Queue mechanism in general	645
Queue size for requests	645
Limit of concurrent connections	645
Max file size allowed	645
Setting up Windows Defender as a custom engine in MetaDefender Core	646
Symantec Endpoint Protection settings	648
Using MetaDefender Core V4 BLACKLIST/WHITELIST feature	651
Using filetype groups VS. MIME-types VS file extensions	651
Using Regular Expressions	651
Advanced usage	651
What are Security Policies and how do I use them?	652
Understanding Security Policies	652
What are the differences between TrendMicro and TrendMicro HouseCall anti-malware engines?	654
What does "Potentially Vulnerable File" result mean?	655
What features of MetaDefender Core version 3 are available in version 4 ?	655
What file types are supported by DLP engine?	658

What is Data Loss Prevention (DLP)?	658
Meta Data Check (Only):	658
File Conversion and Parse:	659
What file types can be verified by MetaDefender v4?	660
What is the frequency of signature/definition updates?	907
What links, target-services or target host-IP's need to be allowed for MetaDefender Core v4?	908
What operating system patches should be applied to the system hosting MetaDefender Core?	909
What should I do if an engine is in "failed" or "permanently failed" status?	909
What temporary folder do Custom Engines use ?	910
Where can I submit false positives detected by MetaDefender Core v4?	911
Which are the supported archive formats for MetaDefender Core v4?	913
Why does the deployment ID appear NULL In MetaDefender Core v4?	914
Why don't I see the Data Sanitization engine in MetaDefender Core v4?	915
Why is the scan stuck in "processing" state on WebScan UI, when the Core Processing History shows that it is already finished?	916
Why should I upgrade my MetaDefender Core v4?	916

Highlights On New MetaDefender Core Release (4.19.0)

- New DBMS for Core - PostgreSQL (to replace SQLite) + DB migration supported
- Native proxy management with authentication support
- Harden Nginx web server settings for security
- Nginx web server statistics queried via REST API query
- Origin client source address retrieval when running via load balancer
- Blacklist overridden on nested files within archive
- Processing history searching with new mechanism
- Enhanced calculation mechanism on statistics page
- Pre-check mode for file submission
- Sanitized file information appended into JSON scan result
- New engine sweeper tool bundled into the product
- Logic improvement to handle better sanitization timed out

Check out more at [12. Release notes](#)

About This Guide

Welcome to the MetaDefender Core 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 Core 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 [OPSWAT Deep CDR technology](#) with over 100 file types supported
- Data leak prevention with redaction and watermarking using [OPSWAT Proactive DLP technology](#)
- Multi-scanning for malware with more than [30 leading anti-malware engines](#)
- [Heuristic](#) analysis to detect more unknown and targeted attacks
- [OPSWAT file-based vulnerability assessment](#)
- 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. Process 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](#).



Please follow all required steps described at [2.2. Installing MetaDefender](#)

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](#)

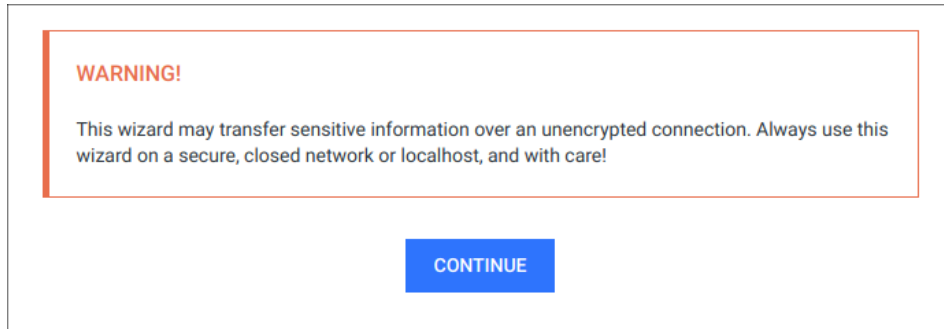
1.1.1. Configuration wizard

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

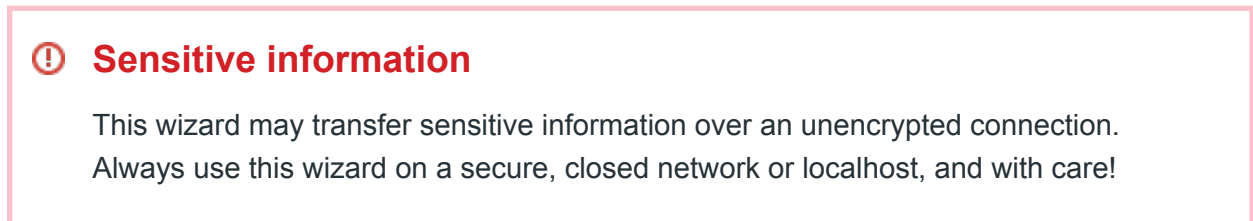
- [User directories](#)

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.



To start the wizard click CONTINUE.



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.

i 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	<p>Password of the user bound to this account that is used at the time of login.</p> <div style="border: 1px solid red; padding: 10px; margin-top: 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, or 2. 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](#).

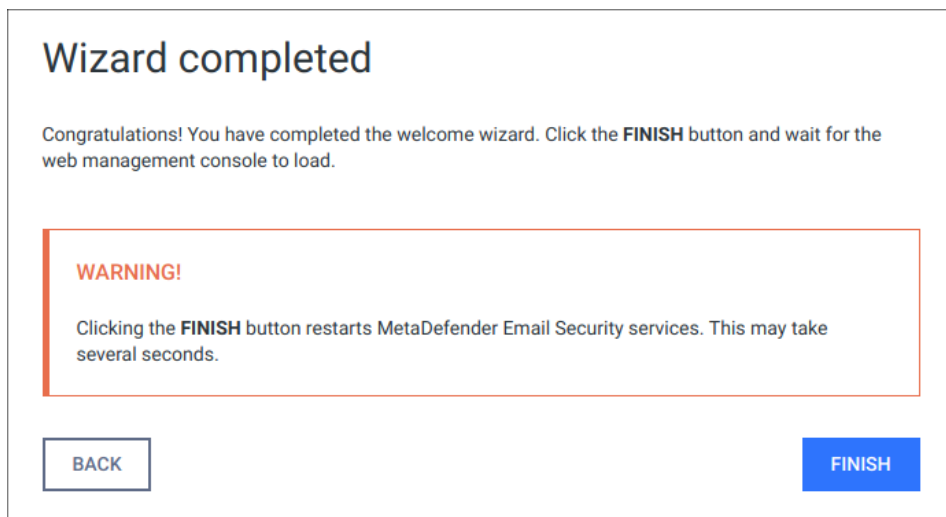
Wizard completion

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. Process Files with MetaDefender Core

There are several ways to scan files with MetaDefender Core:

- [Process Files via Web Interface](#)
- [Process 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 Configuration](#)
- [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 Configuration

Before installing Metadefender Core v4, please refer to the **recommended system configuration** listed below. Please note that the server specifications are built to allow a high volume daily processing.

For certain use cases these might be adjusted and customized on their specific needs. We highly recommend to engage our ProServ team to assist in fine tuning MetaDefender and get the maximum performance out of your systems.



We will deprecate to drop product environment support on following OS versions soon, thus we highly recommended you to upgrade OS on your MetaDefender Core server soon when applicable.

- Windows 7, 8, 8.1
- CentOS 6.x



The recommendations below are for MetaDefender Core, API usage only.

For any other use cases, please consult the user guide of the licensed products for accurate recommendations.

Microsoft Windows Deployments

Supported Operating Systems

- Windows 7 (deprectated soon ⚠), 8 (deprectated soon ⚠), 8.1 (deprectated soon ⚠), 10
- Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019



Disclaimer: End-customer is responsible of verifying the OS license agreement and choose the right OS based on their planned usage of MetaDefender.

Recommended System Configuration

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

Package	CPU cores	Free System RAM	Free Disk Space
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 MAX	32	32 GB	120 GB

In case Metadefender Core Node runs on a separate instance, the following resources are recommended:

Package	CPU cores	Free System RAM	Free Disk Space
MetaDefender Core 8	8	8 GB	16 GB
MetaDefender Core 12	16	16 GB	24 GB

Package	CPU cores	Free System RAM	Free Disk Space
MetaDefender Core 16	16	16 GB	32 GB
MetaDefender Core 20	32	16 GB	40 GB
MetaDefender Core 32	32	32 GB	120 GB

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

Third Party Dependencies

- Microsoft Visual C++ Redistributable for Visual Studio 2010
- Microsoft Visual C++ Redistributable for Visual Studio 2013
- Microsoft Visual C++ Redistributable for Visual Studio 2017

Some engines also have dependencies as described 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
CrowdStrike Falcon ML	Microsoft Visual C++ 2015 Redistributable Package
RocketCyber	Microsoft Visual C++ 2015 Redistributable Package
Microsoft Security Essentials	.NET framework 4.5 Only available on Windows Server edition
Symantec	Only available on Windows Server edition Needs at least one NIC with static IP address running TCP/IP
Systweak	.NET framework 3.5

Proactive DLP	Windows engine build: <ul style="list-style-type: none"> • Microsoft Visual C++ 2017 Redistributable Package (Only applicable to engine version 2.0 or above) • .NET framework 4.5 or newer Linux engine build (only applicable to engine version 2.4.0 or above) <ul style="list-style-type: none"> • .NET Core runtime 3.1
Deep CDR	Microsoft Visual C++ 2017 Redistributable Package (Only applicable to engine version 5.8.0 or above) .NET framework 4.5 or newer


Installation Details

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

MetaDefender will use its resources folder to store temp files as part of the analysis. It's recommended to exclude this folder from real-time protection monitoring.

Unix Based Deployments

Supported Operating Systems

- CentOS 6.6+ (**deprecated soon** ) , 7.0+
- Red Hat Enterprise Linux 6.6+, 7.0+
- Debian 9.0+ ,
- Ubuntu 16.04, 18.04



Disclaimer: End-customer is responsible of verifying the OS license agreement and choose the right OS based on their planned usage of MetaDefender.

Recommended System Configuration

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

Package	CPU cores	Free System RAM	Free Disk Space
Metadefender Core 5	4	4 GB	10 GB
Metadefender Core 10	8	8 GB	20 GB

In case Metadefender Core Node runs on a separate instance, the following resources are recommended:

Package	CPU cores	Free System RAM	Free Disk Space
Metadefender Core 5	4	4 GB	10 GB
Metadefender Core 10	8	8 GB	20 GB

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

Third Party Dependencies

- **Dependencies list:**
 - openssl
 - grep
 - lib32stdc++6 (>= 4.5)
 - libc6-i386 (>= 2.10)
 - procps
 - zlib1g
 - libcurl3 (>= 7.19.7)
 - libcurl4
 - ncurses-compat-libs

Not all above dependencies will need to be installed, it is depending on different Unix distro & version

Installation details

Metadefender Core default installation path is using /var folder for storing resources:

- /var/lib/ometascan(-node): installation folder with all its resources

- /var/log/ometascan(-node): application logs
- /etc/lib/ometascan(node): application config files

Data Retention

Based on the configuration, MetaDefender Core could need additional disk space to store analysis data:

- Analysis Reports: full analysis report is stored in the database and can be retrieved any time (within the defined data retention policy)
 - Approximate **1.5GB for each 1M analysis reports** is required
- Quarantine: blocked files can be stored in the dedicated Quarantine section to allow further analysis (within the defined data retention policy)
 - Depends on the customers' dataset
- Sanitized files: Files that were cleansed using Deep CDR will be stored and made available within the defined data retention policy
 - Depends on customers' dataset

Custom Engines

The recommendations above are specific for MetaDefender pre-packaged bundles.

However for additional Custom Engines, please review the Knowledge base to review additional requirements (if any) for the selected engine.

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>`
 - The 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. MetaDefender Core 4.18.0 or older

2.2.1.1. Installing Metadefender Core (4.18.0 or older) 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>
```

For systems which enabled GPD check flag:

```
sudo yum install --nogpdcheck <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
INSTALLFOLDER		

Key	Default Value	Description
	\Program Files\OPSWAT\MetaDefender Core	Customize installation folder for product Example: INSTALLFOLDER="D:\Products"
RESTADDRESS	*	REST interface binding IPv4 or IPv6 address ('*' means that service listens on all IPv4 and IPv6 interfaces)
RESTPORT	8008	REST interface binding port
EXTERNALNODE		Whether to enable external processing nodes or not. <div data-bbox="1018 992 1428 1205" style="border: 1px solid #add8e6; padding: 5px;">  To enable external processing nodes, set EXTERNALNODE=1. </div> <div data-bbox="1018 1229 1428 1532" style="border: 1px solid #ffcc00; padding: 5px;">  ADDRESS and PORT values below are admitted only if EXTERNALNODE=1 is set. </div>
ADDRESS		Address of the computer to accept external scan node connections <div data-bbox="1018 1731 1428 1989" style="border: 1px solid #ffcc00; padding: 5px;">  ADDRESS value is only admitted if EXTERNALNODE=1 is set. </div>

Key	Default Value	Description
		<p>If EXTERNALNODE=1 is set but ADDRESS is not, then ADDRESS defaults to * (all IPv4 and IPv6 interfaces)</p>
PORT		<p>Designated port number to accept external scan node connections</p> <p> PORT value is only admitted if EXTERNALNODE=1 is set.</p> <p> If EXTERNALNODE=1 is set but PORT is not, then PORT defaults to 8007.</p>
REPORT_ENGINE_ISSUE	true	<p>Enable reporting of engine issue count. (possible values: "true" or "false").</p>

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 msixexec please consult [Windows installer documentation](#).

2.2.1.2 Installing Metadefender Core (4.18.0 or older) 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.

2.2.2. MetaDefender Core 4.19.0 or newer

2.2.2.1. Installing Metadefender Core (4.19.0 or newer) using command line



For command line fashion install on both Linux and Windows, it is **mandatory** to use [MetaDefender Core ignition file](#) to pre-define PostgreSQL server information **BEFORE** installing MetaDefender Core 4.19.0 or newer. Making sure to create the ignition file if not existed before you go ahead to install MetaDefender Core via command line.

- **Windows:** C:\OPSWAT\ometascan.conf
- **Linux:** /etc/opswat/ometascan.conf

MetaDefender Core supports two modes to setup PostgreSQL server:

- **Create new local PostgreSQL server:** MetaDefender Core will install a new PostgreSQL server locally in the same box with the product.

A sample ignition file for PostgreSQL server information (Only non-Unicode characters supported for "user"):



```
[dbserver]
type=local
host=localhost
port=5432
user=postgres
password=whatever_you_decide
```

- **Use your existing PostgreSQL server:** MetaDefender Core will connect to setup its database on a pre-installed PostgreSQL server running remotely. "Test Connection" button needs to be hit to make sure the PostgreSQL is connected and authenticated successfully.

A sample ignition file for PostgreSQL server information:



```
[dbserver]
type=remote
```

```
host=192.168.86.32
port=5432
user=existing_server_admin_user
password=existing_server_pass
```

⚠ After installing MetaDefender Core successfully, you may want to remove all credentials info created for [dbsever] section in ignition file for security reason.

i 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>
```

For systems which enabled GPD check flag:

```
sudo yum install --nogpdcheck <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
INSTALLFOLDER	\Program Files\OPSWAT\MetaDefender Core	Customize installation folder for product Example: INSTALLFOLDER="D:\Products"
RESTADDRESS	*	REST interface binding IPv4 or IPv6 address ('*' means that service listens on all IPv4 and IPv6 interfaces)
RESTPORT	8008	REST interface binding port
EXTERNALNODE		Whether to enable external processing nodes or not. <div data-bbox="1018 1016 1428 1232" style="border: 1px solid #add8e6; padding: 5px;">  To enable external processing nodes, set EXTERNALNODE=1. </div> <div data-bbox="1018 1256 1428 1559" style="border: 1px solid #ffd700; padding: 5px;">  ADDRESS and PORT values below are admitted only if EXTERNALNODE=1 is set. </div>
ADDRESS		Address of the computer to accept external scan node connections <div data-bbox="1018 1760 1428 1975" style="border: 1px solid #ffd700; padding: 5px;">  ADDRESS value is only admitted if EXTERNALNODE=1 is set. </div>

Key	Default Value	Description
		<p> If EXTERNALNODE=1 is set but ADDRESS is not, then ADDRESS defaults to * (all IPv4 and IPv6 interfaces)</p>
PORT		<p>Designated port number to accept external scan node connections</p> <p> PORT value is only admitted if EXTERNALNODE=1 is set.</p> <p> If EXTERNALNODE=1 is set but PORT is not, then PORT defaults to 8007.</p>
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](#).

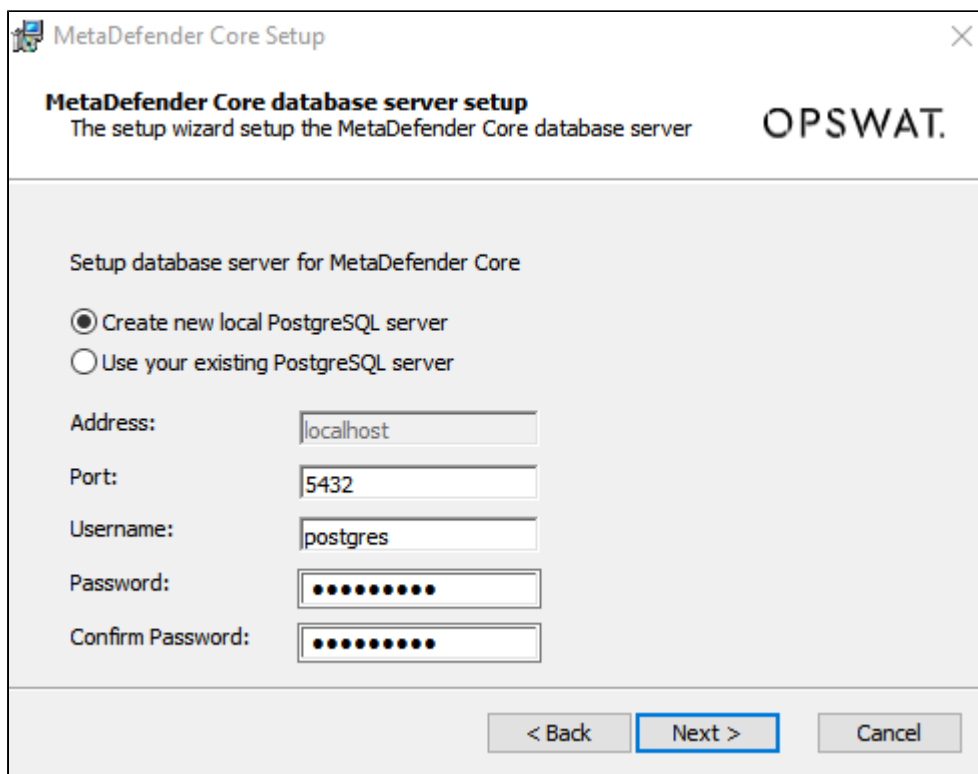
2.2.2.2. Installing Metadefender Core (4.19.0 or newer) using the Install Wizard

The Install Wizard is only for the Windows installer (.msi file). **For Linux installation, please refer to [2.2.2.1. Installing Metadefender Core \(4.19.0 or newer\) using command line](#).**

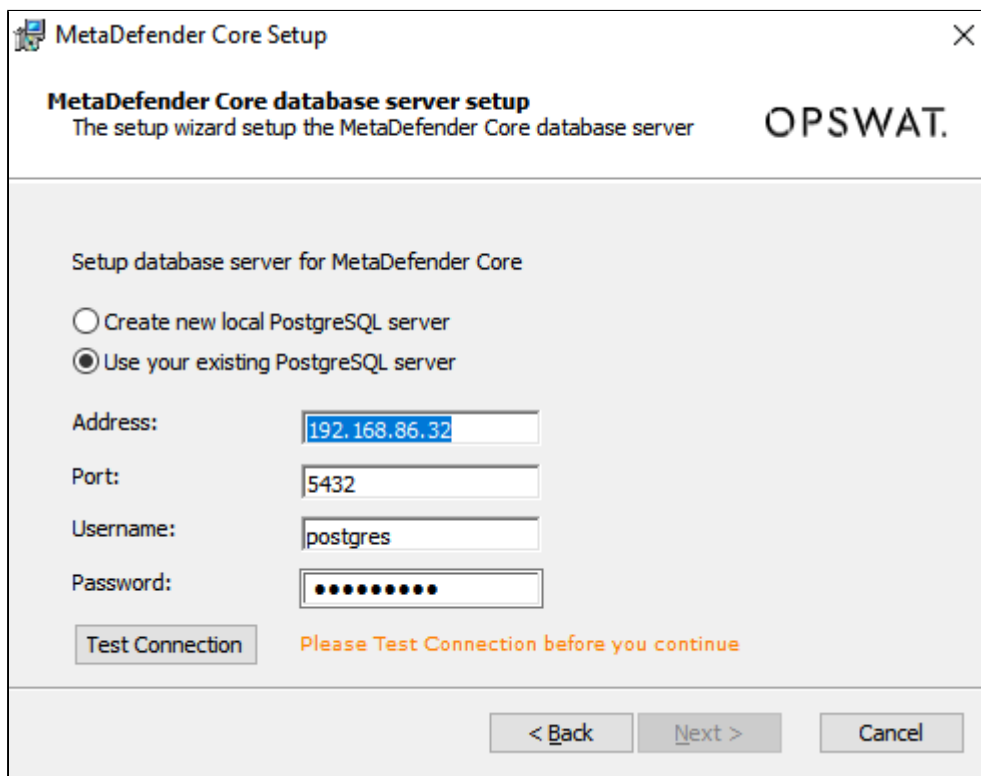
Since MetaDefender Core 4.19.0, we have switched to using PostgreSQL DBMS which needs a dedicated database server. MetaDefender Core supports two modes to setup PostgreSQL server:

- **Create new local PostgreSQL server:** MetaDefender Core will install a new PostgreSQL server locally in the same box with the product.

 Only non-Unicode characters supported for "Username"



- **Use your existing PostgreSQL server:** MetaDefender Core will connect to remote pre-installed PostgreSQL running remotely. "Test Connection" button needs to be hit to make sure the PostgreSQL is connected and authenticated successfully.



2.3. Upgrading MetaDefender Core

Upgrading from MetaDefender Core 3.x to 4.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.

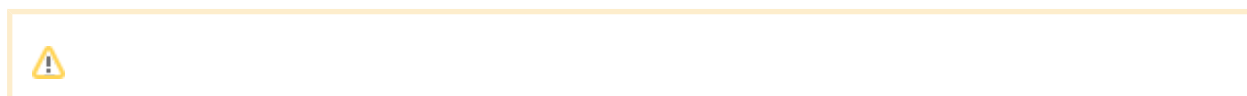
If you decide to upgrade to MetaDefender Core 4.x, you will need a separate [installation](#). Note that no database migration tool exists yet.

Upgrading from MetaDefender Core older version to 4.18.0 (SQLite)

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.

Upgrading from MetaDefender Core 4.18.0 or older (SQLite) to 4.19.0 or newer (PostgreSQL):

To upgrade from a former version to 4.19.0 or newer, running installer of the latest version is enough.



Since we have changed the DBMS (SQLite to PostgreSQL) between 2 versions, thus expecting to give/decide all database information for PostgreSQL server to the new MetaDefender Core.

Please refer to [2.2.2. MetaDefender Core 4.19.0 or newer](#) for detailed instructions.

ⓘ Database migration

Upon finished the product installation step, MetaDefender Core will automatically trigger to run database migration in the background.

While it is still running, if browsing to MetaDefender Core home page (e.g. <http://localhost:8008>), MetaDefender Core will redirect user to database migration UI screen for the migration percentage progress and final outcome.

OPSWAT.

MetaDefender Core

Data Migration



Final result: FINISHED

Elapsed time: 1 second

Data migration log location: C:/Program Files/OPSWAT/Metadefender Core/data/logs/migration_log.log

Old Data location: C:/Program Files/OPSWAT/Metadefender Core/data/old_db

IMPORTANT!

Please do not turn off your server, or stop MetaDefender Core service while migrating your database.
Your SQLite database file will be retained upon migrated regardless for your manual posture check, or rollback if required

FINISH



Just in case the migration failed at any step, you should collect and submit the migration log with your SQLite database files as instructed on the UI screen to OPSWAT support for troubleshooting.

Upgrading from MetaDefender Core 4.19.0 to newer (PostgreSQL):

To upgrade from a former version to 4.19.0 or newer, running installer of the latest version is enough.

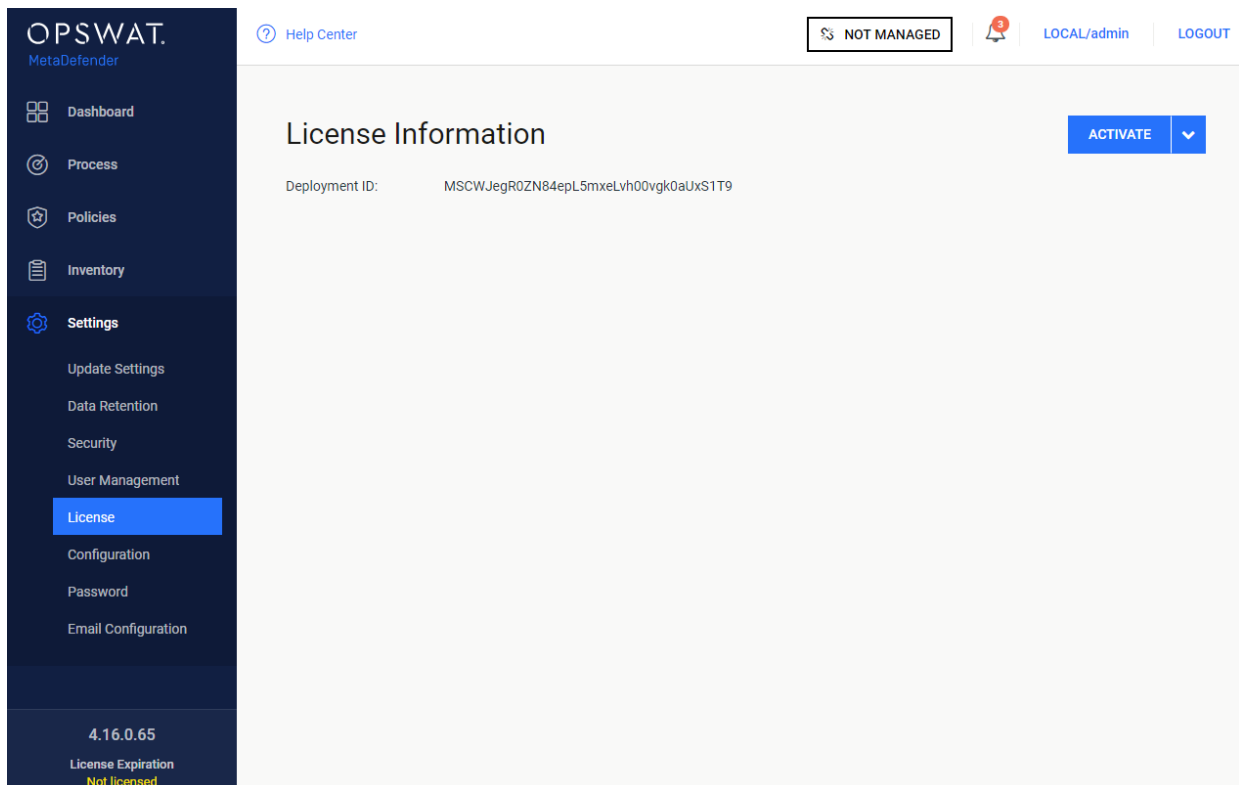
2.4. MetaDefender Core Licensing

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

SELECT A FILE

SEND CANCEL

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

Request trial key online

An evaluation license could be acquired by contacting our sales team.

Activation

ACTIVATION MODE

ONLINE OFFLINE REQUEST TRIAL KEY ONLINE

To request a quote or trial license key for OPSWAT MetaDefender Core, please contact our sales team at <https://www.opswat.com/contact>

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

OPSWAT.
MetaDefender

Help Center

NOT MANAGED LOCAL/admin LOGOUT

License Information

ACTIVATE

Product ID: MSCW-4c-EVAL-UNLIMITED
 Product name: MetaDefender Core for Windows - 4 engine package (Rev.C) - Evaluation
 Expiration: 2026-12-31
 Max nodes: 1
 Deployment ID: MSCWJegR0ZN84epL5mxelVh00vgk0aUxS1T9
 Activation key:

4.16.0
License Expiration 2026-12-31

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

- [2.5.1. MetaDefender Core 4.19.0 or newer \(PostgreSQL\)](#)
- [2.5.2. MetaDefender Core 4.18.0 or older \(SQLite\)](#)

2.5.1. MetaDefender Core 4.19.0 or newer (PostgreSQL)

Updated: 27 Aug 2020

The current performance report is in BETA version.

OPSWAT continuously updates our performance report on regular basis.



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.

System Specs

CPU	3.2GHz Core i7-8700 6 physical cores 12 logical cores
RAM	32 GB
HDD	SSD 150GB available disk

Deployment Setups

	Deployment A	Deployment B	Deployment C
Deployment fashion	On-premise (Physical server)	On-premise (Physical server)	On-premise (Physical server)
MetaDefender Core version	4.18.0 (SQLite)	4.19.0 (PostgreSQL)	4.19.0 (PostgreSQL)
Database location	Local	Local	Remote
Platform	Windows	Windows	Windows
Licensing	8 AV engines Deep CDR engine	8 AV engines Deep CDR engine	8 AV engines Deep CDR engine

- Local: Database files managed in the same machine with MetaDefender Core
- Remote: Database files managed in a different machine from MetaDefender Core, in local area network (LAN)

Data Set

- Total data set size: 12.1 GB
- Number of files: 2,000
 - File Category: Documents (MS Office, PDF)

- Average file size: 6.2 MB
- Total number of extracted files: 155,137
 - Average number of extracted files per one original file: 77.57

Test Scenarios

- Number of simultaneous threads (for scan submission): 50
 - Always have 50 original document files active being processed on MetaDefender Core at any given time
- Polling mode used for scan result retrieval
 - Interval time between every 2 polling requests: 200 ms

MetaDefender Core configurations:

- Node queue size: 500
- Archive handling settings:
 - Max allowed extracted files: 20000
 - Max allowed extracted size (GB): 2
 - Max allowed recursive level: 5
 - Enabled to extract document files
- Deep CDR settings: Enabled for all file types
- AV scanning setting:
 - Engine timeout (minute): 1
 - Global scan timeout (minute): 10

Test Results

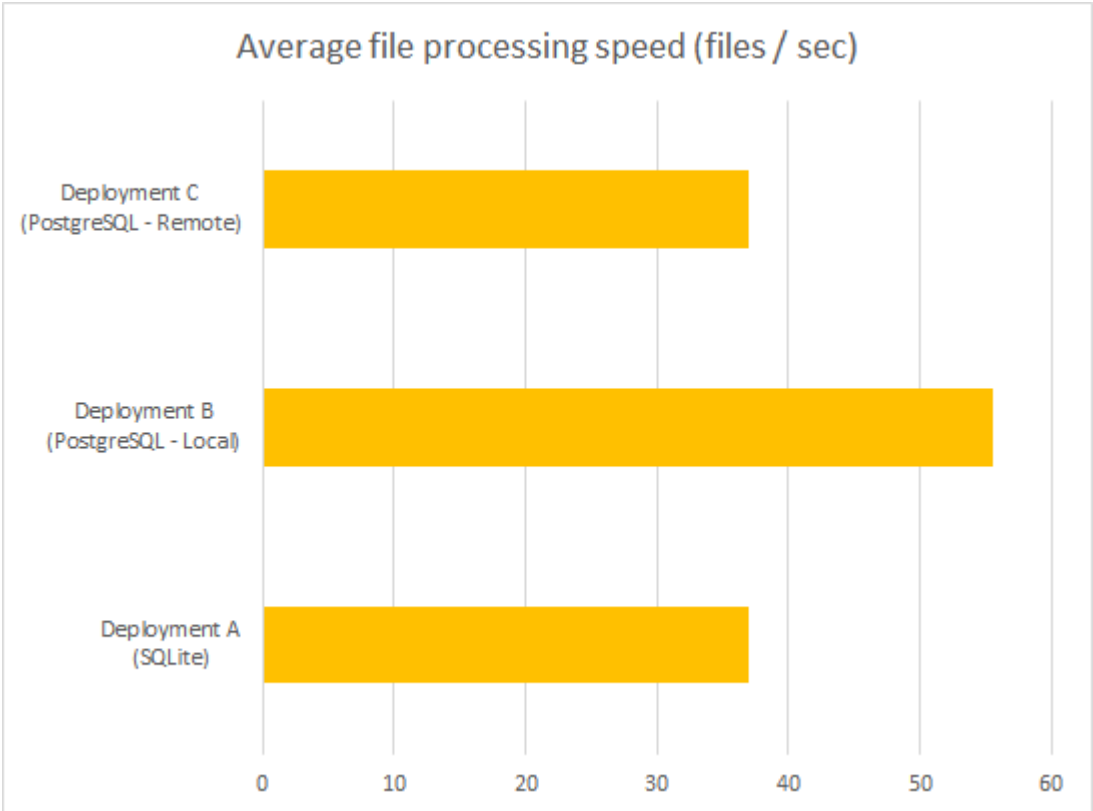
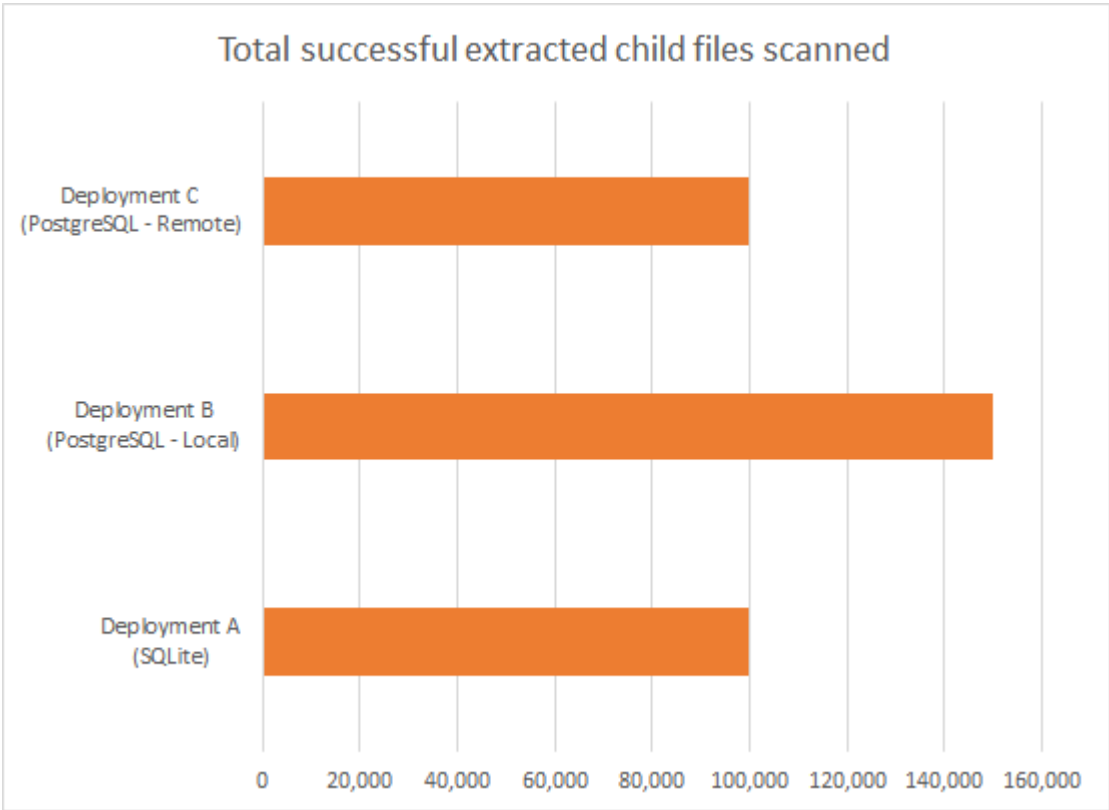
Run time: 45 minutes (2700 seconds)

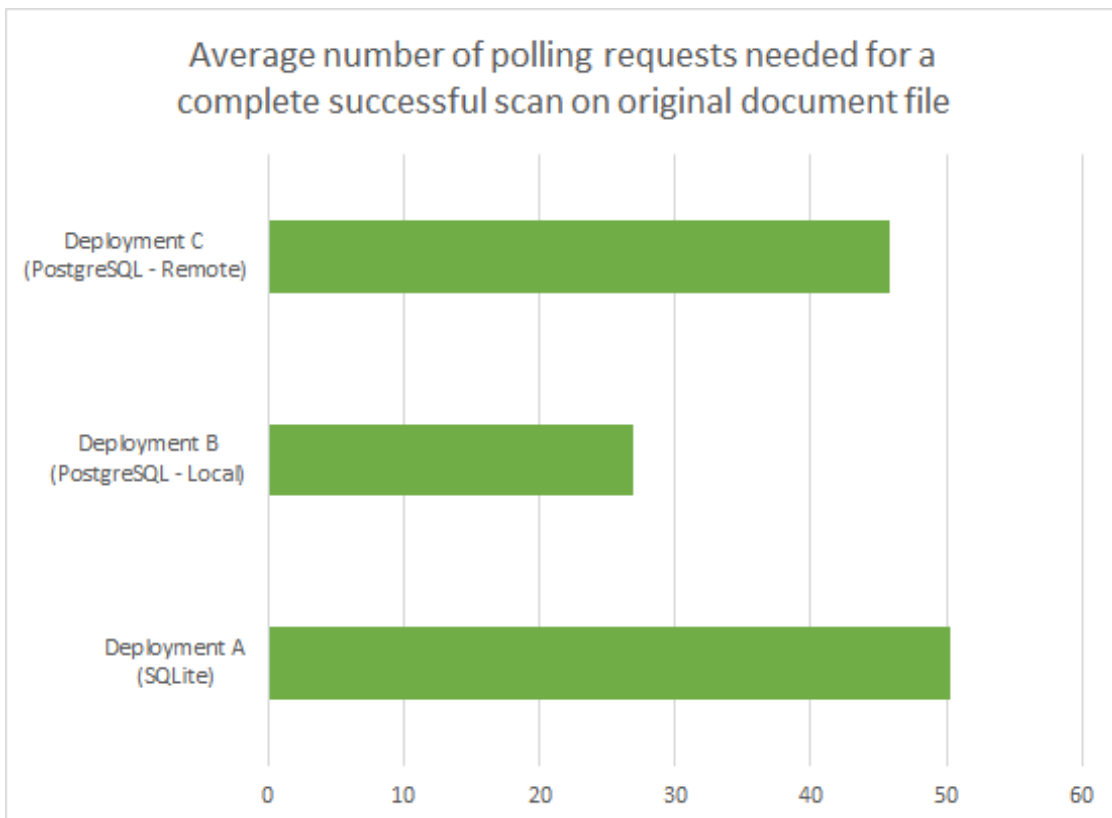
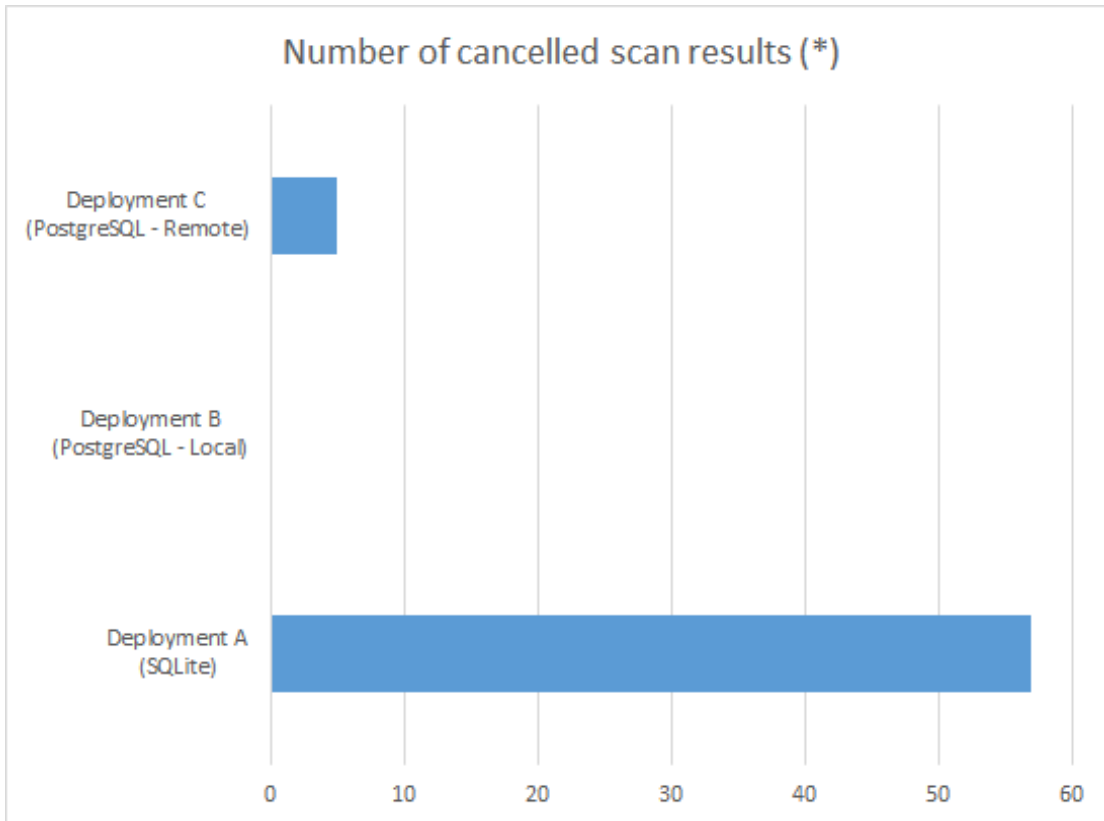
	Deployment A (SQLite)	Deployment B (PostgreSQL - Local)	Deployment C (PostgreSQL - Remote)
Total successful extracted child files (objects) scanned	99,753	149,785	99,860
Total successful original document files scanned	1,266	1,928	1,304

	Deployment A (SQLite)	Deployment B (PostgreSQL - Local)	Deployment C (PostgreSQL - Remote)
Average processing speed (objects / sec)	36.94	55.48	36.99
Number of cancelled scan results (*)	57	0	5
Average number of polling requests needed for a complete successful scan on original document file (interval polling = 200 ms)	50.24	26.89	45.89

Notes:

(): Cancelled result happens when after 5 minutes timeout passed without a complete final result, then client stopped polling and canceled the scan*





2.5.2. MetaDefender Core 4.18.0 or older (SQLite)

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
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

		Number of Files	Total Size (MB)	Average File Size (MB)	M5 (sec /file)	M10 (sec /file)	DS Overhead
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
	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

		Number of Files	Total Size (MB)	Average File Size (MB)	M5 (sec /file)	M10 (sec /file)	DS Overhead
	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	
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	

		Number of Files	Total Size (MB)	Average File Size (MB)	M5 (sec /file)	M10 (sec /file)	DS Overhead
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 Product + Version	4.13.2
System Environment	<p>OS: Windows Server 2016</p> <p>CPU:</p> <p>2.10GHz 8 core vCPUs (for 8 engine package)</p> <p>2.10GHz 16 core vCPUs (for 12, 16 engine packages)</p> <p>2.10GHz 32 core vCPUs (for 20 engine package)</p> <p>RAM:</p> <ul style="list-style-type: none"> • 16 GB RAM (for 12,16, 20 engine packages) • 8 GB RAM (for 8 engine package) <p>HD: 99.5 GB</p>
Product Configuration	<p>Performance tool setting:</p> <ol style="list-style-type: none"> 1. No. of threads: 20 2. Workflow: File Process

	<p>Core setting:</p> <ol style="list-style-type: none"> 1. Archive: <ul style="list-style-type: none"> • max size:20000 • max number:20000 • max level:50000 2. Scan: <ul style="list-style-type: none"> • max file size for files scanned: 2000 MB 3. Data sanitization: All enabled except Text 4. Data retention policy: All Default except: <ul style="list-style-type: none"> • Sanitized file clean up : 1h
Exclusions/Other	No sanitization for text file types

Test Results

File Category	Number of Files (777,531 Files)	Weight of File Type by Category (%)	CDR + 8 Anti-malware engines (sec/file)	CDR + 12 Anti-malware engines (sec/file)	CDR + 16 Anti-malware engines (sec/file)	CDR + 20 Anti-malware engines (sec/file)
Documents	565,606	72.7%	0.825	0.927	1.113	1.504
Archive	82,156	10.56%	0.053	0.096	0.112	0.142
Graphic	54,537	7.01%	0.354	0.277	0.279	0.762
PDF	53,915	6.93%	1.184	0.982	1.030	1.196
Text*	21,317	2.74%	0.058	0.055	0.056	0.074
Average Scan Time (sec)			0.495	0.467	0.516	0.735
Total Scan Time (sec)			34,340	35,633	42,062	57,011

File Category	Number of Files (777,531 Files)	Weight of File Type by Category (%)	CDR + 8 Anti-malware engines (sec/file)	CDR + 12 Anti-malware engines (sec/file)	CDR + 16 Anti-malware engines (sec/file)	CDR + 20 Anti-malware engines (sec/file)
Throughput/day			1,956,280 files/day	1,885,259 files/day	1,597,104 files/day	1,178, 329 files/day
Average Memory Usage (GB)			3.92 GB out of 8GB	7.29 GB out of 16 GB	8.61 GB out of 16 GB	7.40 GB out of 16 GB
Average CPU Usage (%)			77.03% out of 8 CPU Cores	53.088% out of 16 CPU Cores	53.368% out of 16 CPU Cores	31.982% out of 32 CPU Cores

*Note**

no data sanitization for text file

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.

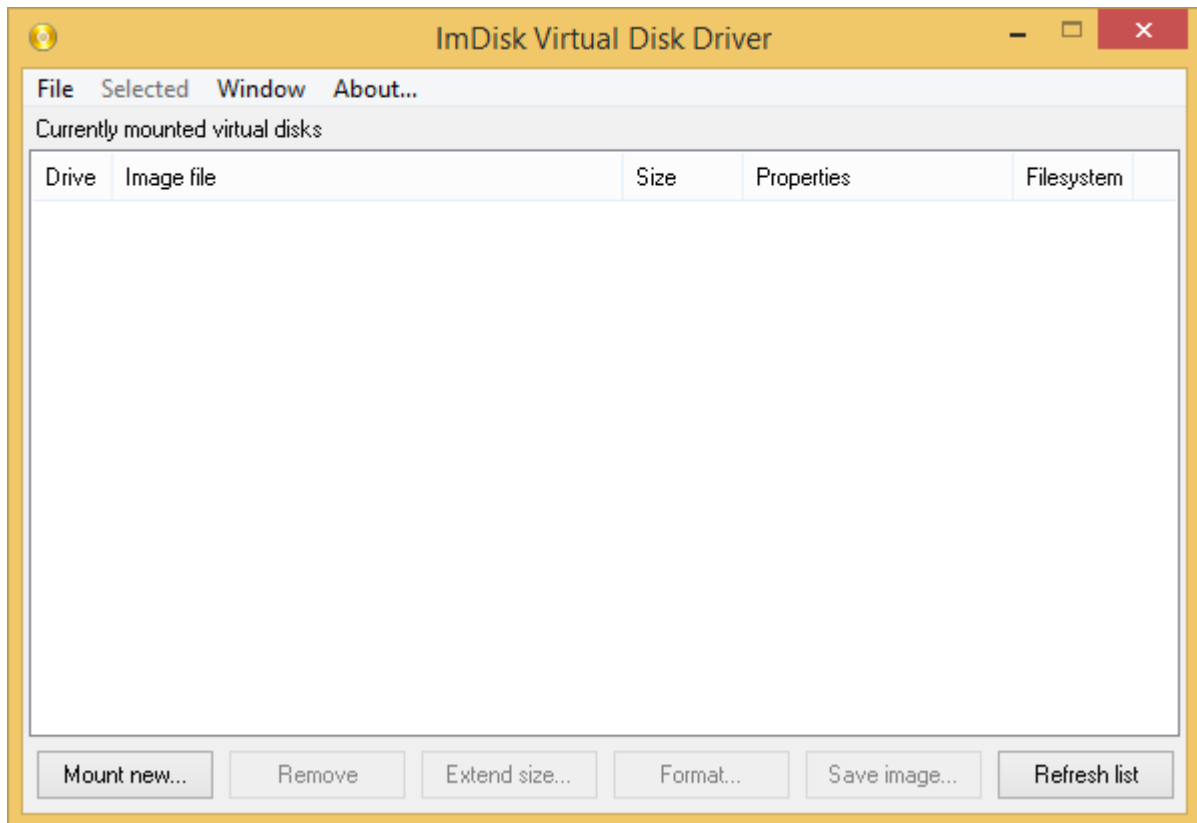
Instructions for windows

Step 1:

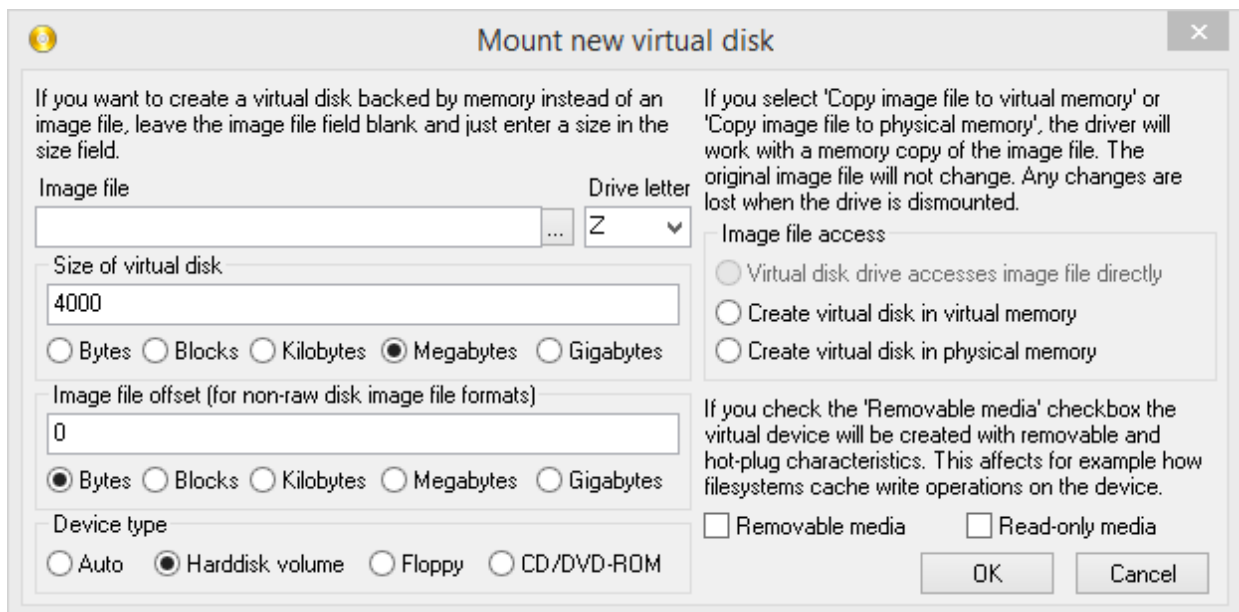
Create a RAMDISK on your system.

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

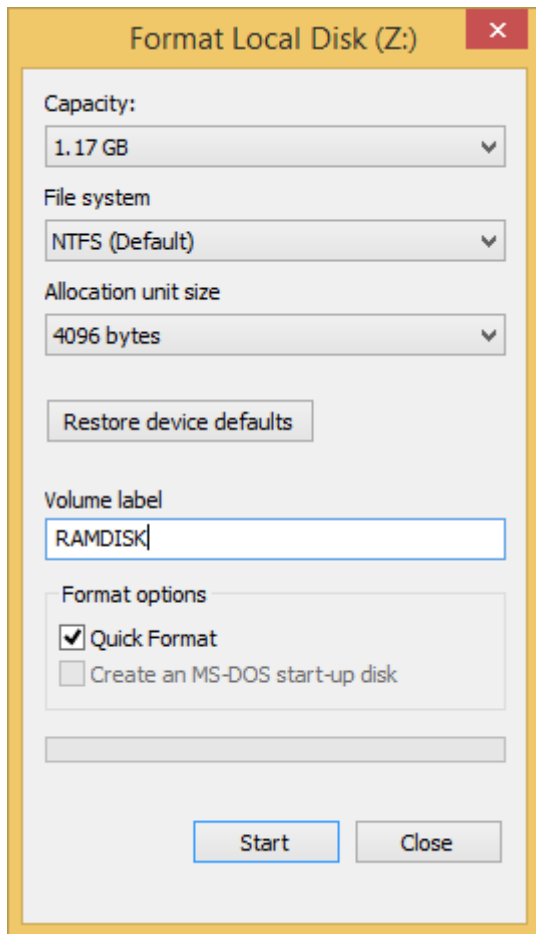
After installation, use the **ImDisk Virtual Disk Driver** application, to create a new RAMDISK.



Mount new virtual disk:



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

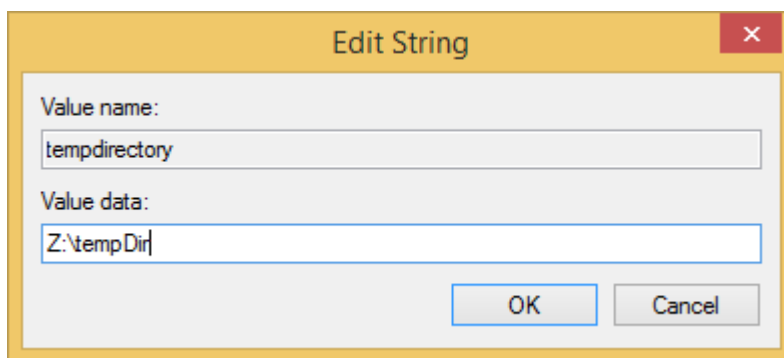
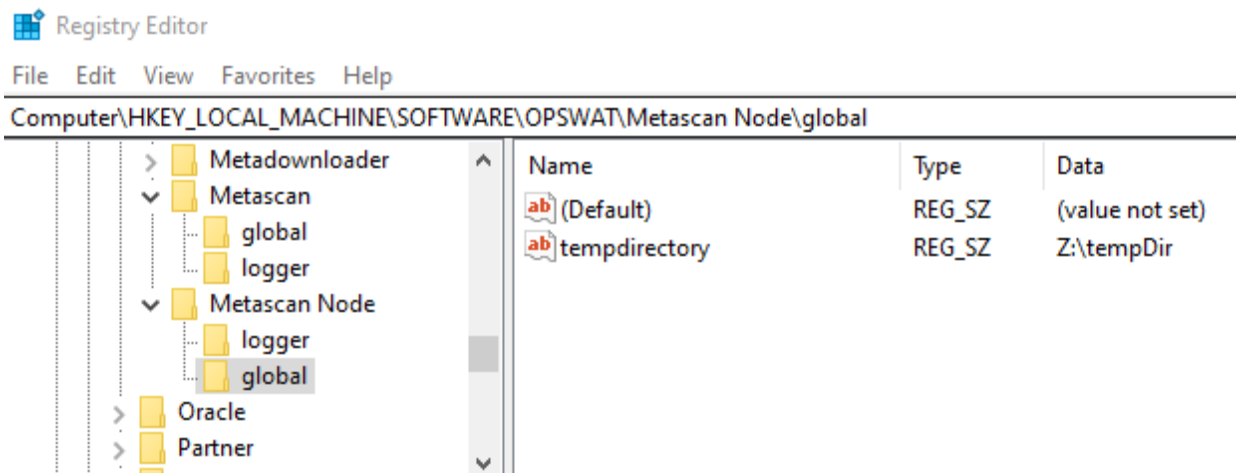


Step 2:

Create, or edit the following registry entry:

i HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan
Node\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 at least 10GB, and also:

- For non archive files: the average file size * 40
- 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. Policy 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
- 3.12 Server Configurations

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.

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.

Sign In

USERNAME

PASSWORD

[Forgot password?](#)

SIGN IN

© 2002-2019 OPSWAT, Inc. All rights reserved.

[Documentation](#) • [Privacy Policy](#)

Login screen

Typical issues related to the Web Management Console:

- [Inaccessible Management Console](#)

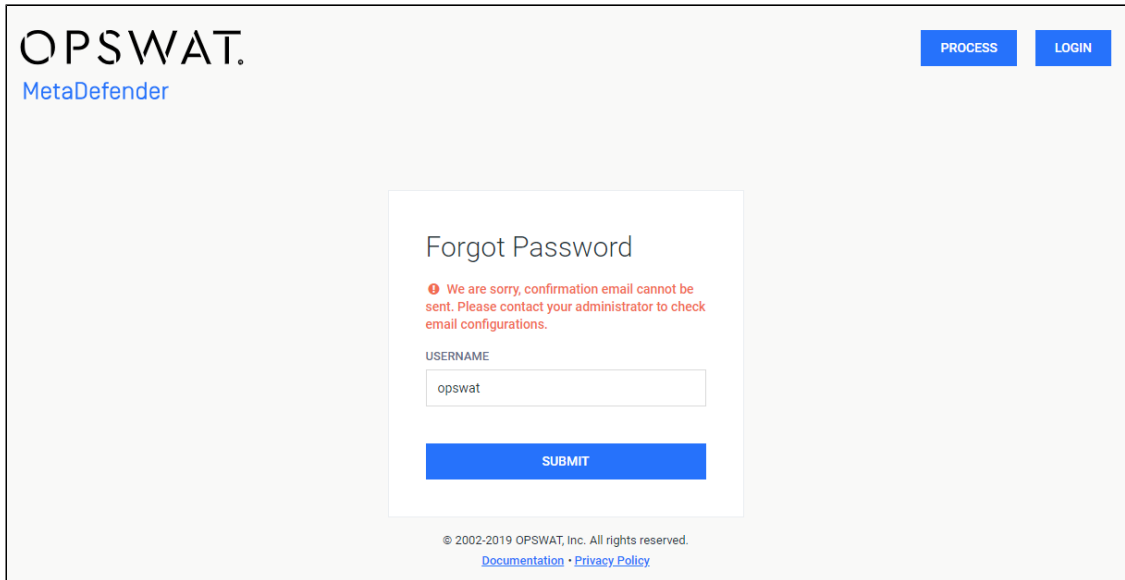
3.1.1. Password Recovery



Prerequisites:

- Only supports local users, not applicable to Active Directory / LDAP users where all their credential settings should be managed on Domain controller / LDAP server.
- The feature authenticates local users via email to reset their own password (assuming user was registered with a valid email on MetaDefender Core, if not then user should update their email properly on User Management page), and

therefore it is mandatory for MetaDefender Core's administrators to follow steps at [3.12.1 Email Configuration](#) and ensure all SMTP configurations set properly beforehand. Otherwise, expecting users to hit following warning message when trying to reset their password:



The screenshot shows the OPSWAT MetaDefender interface. At the top left is the OPSWAT logo and 'MetaDefender' text. At the top right are 'PROCESS' and 'LOGIN' buttons. The main content area is titled 'Forgot Password'. Below the title is a red error message: 'We are sorry, confirmation email cannot be sent. Please contact your administrator to check email configurations.' Underneath is a 'USERNAME' label and a text input field containing 'opswat'. A blue 'SUBMIT' button is positioned below the input field. At the bottom of the page, there is a copyright notice: '© 2002-2019 OPSWAT, Inc. All rights reserved.' and links for 'Documentation' and 'Privacy Policy'.

How This Feature Works

Just in case MetaDefender Core user credentials are lost or forgotten, basically any local user (not AD / LDAP) will be supported to reset their password by either one of two methods:

- **Forgot password (active):** Any local user can choose to reset their own password.
- **Reset password by administrators (passive):** Any local user's password can be reset by administrators.

Both methods requires authentication via email, and force the affected user to change their password at the first login time for security reason.

Forgot Password

Any local user registered with email on MetaDefender Core should be able to reset their own password by clicking on **Forgot password?** link on login page.

Sign In

USERNAME

PASSWORD

[Forgot password?](#)

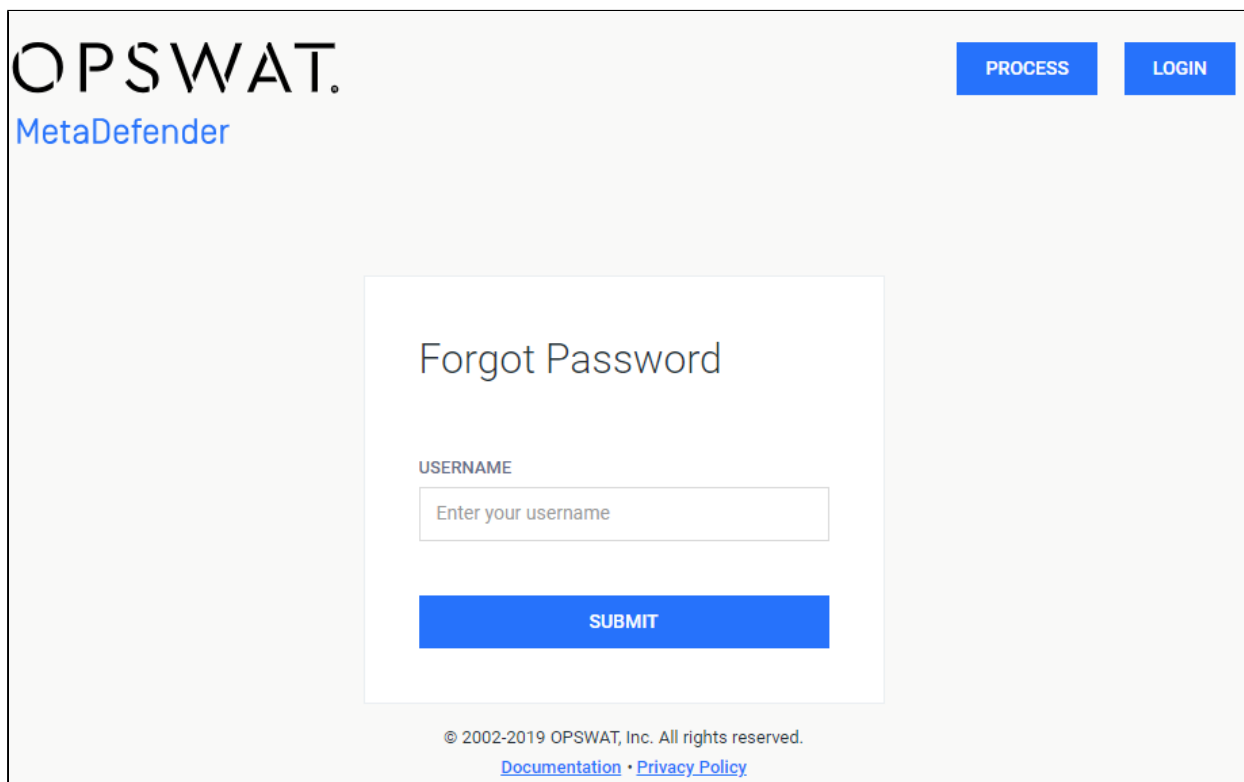
SIGN IN

© 2002-2019 OPSWAT, Inc. All rights reserved.

[Documentation](#) • [Privacy Policy](#)

Login page

You will be redirected to Recover Password page.



Forgot Password page

An email with password reset link will be sent to user's registered email entitled "MetaDefender Core Password Reset".

Hi,
You're receiving this email because you requested a password reset for your MetaDefender Core's user account: **test-user**
If you did not request this change, you can safely ignore this email, your password will not be changed.

To choose a new password and complete your request, please follow the link below:
<http://localhost:8008/#/rspw?u=5&t=a45b4f2c32a64905993f5f127c1e5a6b>
If it is not clickable, please copy and paste the URL into your browser's address bar.

For any questions or concerns, please contact your MetaDefender Core's local administrator.
The MetaDefender Core Team.

Email with link to reset password

If that user don't take any action, the link on email will be expired in 3 days, and since then if that user uses that expired link will result in following message on MetaDefender Core management console:

Reset Password

ⓘ We are sorry, the password reset link seems expired or invalid.

© 2002-2019 OPSWAT, Inc. All rights reserved.

[Documentation](#) • [Privacy Policy](#)

While the link is still valid, clicking on link will redirected to MetaDefender Core management console where user will be forced to create a new password:

Reset Password

NEW PASSWORD

CONFIRM NEW PASSWORD

RESET

© 2002-2019 OPSWAT, Inc. All rights reserved.

[Documentation](#) • [Privacy Policy](#)

Reset Password page

You will be automatically redirected to MetaDefender Core dashboard after resetting password successfully.

Reset Password By Administrators

As an administrator, you are now supported to reset password of any local user on MetaDefender Core, it could be either other local user (admin / non-admin) or even oneself.

Go to User Management → under USER AND GROUPS, choose which user to reset password → click RESET PASSWORD button

The screenshot displays the OPSWAT MetaDefender User Management interface. On the left is a dark sidebar with navigation options: Dashboard, Process, Policies, Inventory, Settings (with sub-options: Update Settings, Data Retention, Security, User Management, License, Configuration, Password, Email Configuration), and License. The main content area is titled 'User Management' and contains a table of 'USERS AND GROUPS' with columns for 'USERS AND GROUPS' and 'NAME'. The table lists four users: LOCAL/admin (admin), SUPPORTLAB/Administrator (Administrator), LOCAL/test-user (test-user), and LOCAL/trivu (trivu 2). The 'LOCAL/test-user' row is selected. To the right is the 'Modify user' form, which includes fields for USER DIRECTORY (LOCAL), ACCOUNT NAME (test-user), ACCOUNT DISPLAY NAME (test-user), and ASSIGN TO ROLES (Security auditor). There is also an 'APIKEY' field with a 'Generate' link. At the bottom of the form, there are 'OK', 'CANCEL', and 'RESET PASSWORD' buttons. The 'RESET PASSWORD' button is highlighted with a red box.


Admin to RESET PASSWORD

Then administrator must create a new password by clicking **Generate** link or typing any text in the text-box.

Click RESET PASSWORD button once done.

Reset Password

NEW PASSWORD

 [Generate](#)

[RESET PASSWORD](#) [CANCEL](#)

Admin to generate a new password

An email titled "MetaDefender Core Password Reset" will be sent to user's email. Please check the inbox to collect a temporary password.

Hi,
You're receiving this email because your administrator just reset password on your MetaDefender Core's user account: **test-user**.

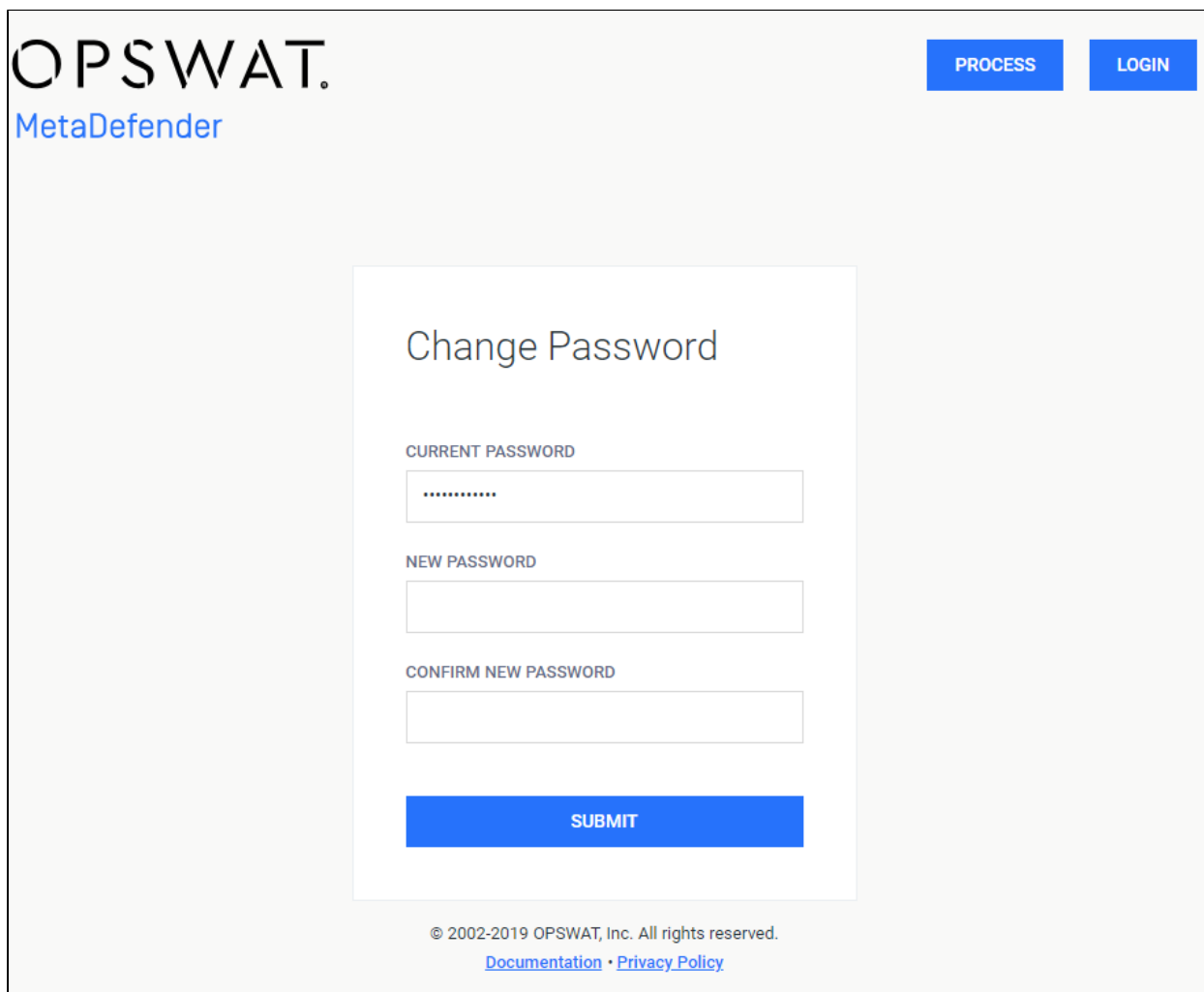
Here is your temporary password: **xtpOm7UJ67A8**

At the first time you log in back with this temporary password under your account, you will be asked to change this password for security reasons.

For any questions or concerns, please contact your MetaDefender Core's local administrator.
The MetaDefender Core Team.

Email with temporary password

When the impacted user tries to log into MetaDefender management console afterwards with the provided temporary password in the email at the first time, that user will be redirected to page where they are required to change their password.



Change Password page

Once successfully changed the password, the user will be automatically redirected to the MetaDefender dashboard.

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
report_engine issue	true	optional	Enable reporting of engine issue count. (possible values: "true" or "false").
quarantinepath	[Core data directory] /quarantine	optional	Directory for quarantine database and quarantined items
sanitizepath	[Core data directory] /sanitized	optional	Directory for sanitized database and sanitized items

[logger] section

key	default value	required	description
logfile	<code>/var/log</code> <code>/ometascan</code> <code>/ometascan.</code> <code>log</code>	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
local_timezone	false	optional	Set local timezone for events sending to local syslog server
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.
nginx_logfile	<code>/var/log</code> <code>/ometascan</code> <code>/nginx-</code> <code>ometascan.log</code>	optional	File name and path to store the NGINX logs. If this value is changed, the <code>/etc/logrotate.d/ometascan</code> should be changed accordingly.

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.

[internal] section

key	default value	required	description
data_directory	/var/lib /ometascan	optional	Full path for MD Core's data (data etc.) E.g. /var/lib/ometascan/test
db_optimization	0	optional	<p>This setting is only applicable Meta Core version 4.17.3 or above.</p> <p>Database optimization has been introduced since Core 4.17.0 to help run data tasks faster on MetaDefender Core. The task could be, while this task is running (seconds), further data queries need to be performed and possibly causing timeout on client.</p> <p>If this parameter is enabled (set to 1), MetaDefender Core performs a database optimization task.</p> <p>Supported values:</p> <ul style="list-style-type: none"> • 0 (default mode, same behavior as Core 4.16.3 or older): scheduled_db_optimization setting will be ignored. • 1 (enabled to run optimize): <ul style="list-style-type: none"> • If scheduled_db_optimization setting is not set: MD Core performs database optimization on 10,000 records, not time specified time. • Otherwise if scheduled_db_optimization is set to X (from 0:00

key	default value	required	description
			Core performs the op (e.g. 3:00 am) each d run optimization every records.
scheduled_db_optimization_time	<hh> : <mm> (24 hour format)	optional	<p>This setting is only applicable Meta Core version 4.17.3 or above.</p> <p>This setting is only applicable when when db_optimization setting is s (enabled). When being set, then M Core performs a database optimiza time configured.</p> <p>E.g.: Configure MetaDefender Core the optimization at 10:35 PM every</p> <ul style="list-style-type: none"> • scheduled_db_optimizatio = 22 : 35

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

parameter	default value	type	required	description
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
report_engine_issue	true	string value	optional	Enable reporting of engine issue count. (possible values: "true" or "false").
quarantinepath	[installdir] \data\quarantine	string value	optional	Directory for quarantine database and quarantined items
sanitizepath	[installdir] \data\sanitized	string value	optional	Directory for sanitized database and sanitized items

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. Must set value on this key when logfile key is also set accordingly.

key	default value	type	required	description
log_rotation	0	string value	optional	<p>This setting is only applicable MetaDefender Core version 4.17.3 or above, Windows OS only (on Linux, we use already-supported OS log rotation).</p> <p>Should only set this key when logfile key is also set accordingly.</p> <p>Supported values:</p> <ul style="list-style-type: none"> • 0 (default mode, same behavior like MetaDefender Core 4.17.2 or older): Core logs are not rotated. • 1 (enable to rotate log): <ul style="list-style-type: none"> • Rotation process will be performed every day, regardless of file size. • Limit rotated log to be stored is 30 files, the oldest log will be deleted if file number reaches the limit. • Rotated log name format: <logname>-<yyyyMMdd>.gz (e.g.: core.log-20200330.gz), all saved in same location with what you set in logfile. • All generated log packages included in MetaDefender Core support package.
wineventlog_level	info		optional	

key	default value	type	required	description
		string value		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. Must set value on this key when syslog key is also set accordingly.
local_timezone	false	string value	optional	Set local timezone for events sending to local syslog server.
override		string value	optional	Override specific log ids to display them on another level e.g.: "1723: error,663:info".
cef	false	string value	optional	If true, the log format is Common Event Format.
nginx_logfile	[installdir] \nginx\nginx. log	string value	optional	File name and path to store the NGINX logs.
nginx_log_rotation	0	string value	optional	This setting is only applicable MetaDefender Core version 4.17.3 or above, Windows OS only (on Linux, we use already-supported OS log rotation). Should only set this key when nginx_logfile key is also set accordingly. Supported values:

key	default value	type	required	description
				<ul style="list-style-type: none"> • 0 (default mode, same behavior like Core 4.17.2 or older): Nginx logs are not rotated. • 1 (enable to rotate log): <ul style="list-style-type: none"> • Rotation process will be performed every day, regardless of file size. • Limit rotated log to be stored is 30 files, the oldest log will be deleted if file number reaches the limit. • Rotated log name format: <logname>-<yyyyMMdd>.gz (e.g.: nginxlog.log-20200330.gz), all saved in same location with what you set in nginx_logfile. • All generated log packages included in MetaDefender Core support package

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

HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan\internal

key	default value	type	required	description
data_directory	<MD Core installation folder>\data	string value	optional	Full path for MD Core's data (etc.) E.g. D:\custom_path

key	default value	type	required	description
db_optimization	0	string value	optional	<p>This setting is only applicable Core version 4.17.3 or above. Database optimization has been added since Core 4.17.0 to help reduce the time taken for the task to complete faster on MetaDefender Core (the task could be, while this task is running, further data queries and possibly causing timeouts).</p> <p>If this parameter is enabled, MetaDefender Core performs an optimization task.</p> <p>Supported values:</p> <ul style="list-style-type: none"> • 0 (default mode, same as Core 4.16.3 or older): scheduled_db_optimization setting will be ignored. • 1 (enabled to run optimization task) <ul style="list-style-type: none"> • If scheduled_db_optimization_time setting is not set, MetaDefender Core runs data optimization every 10,000 records or any specified interval. • Otherwise if scheduled_db_optimization_time is set to X (from Core 4.17.0), MetaDefender Core performs optimization (e.g. 3:00 am) and records optimization records.
scheduled_db_optimization_time	<hh> : <mm> (24 hour format)	string value	optional	This setting is only applicable Core version 4.17.3 or above.

key	default value	type	required	description
				<p>This setting is only applical when db_optimization set being set, then MD Core p optimization at the time cor</p> <p>E.g.: Configure MetaDefen the optimization at 10:35 P</p> <ul style="list-style-type: none"> • scheduled_db_opt = 22:35

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)
tempdirectory_create_timeout		optional	

parameter	default value	required	description
			If node cannot create the resources folder, it will retry for the specified amount of milliseconds

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
local_timezone	false	optional	Set local timezone for events sending to local syslog server
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.

key	default value	required	description
archive_debug	0	optional	When enabled (set to 1), verbose debug info will be written into the Core log file

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.

[internal] section

key	default value	required	description
data_directory	/var/lib/ometascan-node	optional	Full path for Node's data (engines, resources etc.) E.g. /var/lib/ometascan-node/test
parallelcount	20	optional	Set maximum number of threads (files) sending to engine at the same time, applicable to all engines except Archi engine (extraction, default = -1 unlimited) and Proactive DLP engine (default = 5)
parallelcount_<enginename>		optional	<enginename> is the first part of engine which all can be found in <MD Core folder>\data\updates\metadescriptor <u>For example:</u> engine id: symantec_1_windows → <enginename> = symantec Some common use-cases: <ul style="list-style-type: none"> • ds (parallelcount_ds): Deep C engine. By default, parallelcount = 20

key	default value	required	description
			<ul style="list-style-type: none"> • 7z (parallelcount_7z): Archive engine, applicable to archive extraction only. By default, parallelcount_7z = -1 (unlimited threads) <ul style="list-style-type: none"> • 7z_extract (parallelcount_7z_extra) Archive engine, extraction only. By default, parallelcount_7z_extract (unlimited threads) • 7z_compress (parallelcount_7z_compress) : Archive engine, compression only for archive sanitization. By default, parallelcount_7z_compress = 20

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. Must set value on this key when logfile key is also set accordingly.
log_rotation	0	string value	optional	This setting is only applicable MD Core version 4.17.3 or above, Windows OS only (on Linux, we use already-supported OS log rotation) Should only set this key when logfile key is also set accordingly. Supported values: <ul style="list-style-type: none"> • 0 (default mode, same behavior like Core 4.17.2 or older): Core logs are not rotated. • 1 (enable to rotate log): <ul style="list-style-type: none"> • Rotation process will be performed every day, regardless of file size. • Limit rotated log to be stored is 30 files, the oldest log will be deleted if file number reaches the limit.

key	default value	type	required	description
				<ul style="list-style-type: none"> Rotated log name format: <logname>-<yyyyMMdd>.gz (e.g.: core.log-20200330.gz), all saved in same location with what you set in logfile All generated log packages included in Core support package,
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. Only set this key when syslog key is also set accordingly.
override		string value	optional	override specific log ids to display them on another level e.g.: "1723:error,663:info".
cef	false	string value	optional	If true, the log format is Common Event Format.
archive_debug	0	string value	optional	When enabled (set to 1), verbose debug info will be written into the Core log file.

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\...

HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metascan Node\internal

key	default value	type	required	description
data_directory	<MD Core installation folder>\data	string value	optional	Full path for MD Core's data (updates etc.) E.g. D:\custom_path
parallelcount	20	string value	optional	Set maximum number of threads sending to engine at the same time, applicable to all engines except engine (extraction, default = unlimited) and Proactive DLI (default = 3)
parallelcount_<enginename>		string value	optional	<enginename> is the first part of the engine id which all can be found in <MD Core installation folder>\data\updates\metascan\engines\<enginename>. For example: engine id: symantec_1_windows_64bit_10.0.0.0_10.0.0.0 <enginename> = symantec Some common use-cases: <ul style="list-style-type: none"> • ds (parallelcount_ds): CDR engine. By default parallelcount_ds = 20 • 7z (parallelcount_7z): 7z engine, applicable to archive extraction only. By default parallelcount_7z = -1 (unlimited threads) <ul style="list-style-type: none"> • 7z_extract (parallelcount_7z_extract): Archive engine,

key	default value	type	required	description
				<p>only. By default, parallelcount_7z_ -1 (unlimited three</p> <ul style="list-style-type: none"> • 7z_compress (parallelcount_7 : Archive engine, compression only archive sanitization default, parallelcount_7z_ = 20

3.2.3 Nginx related configuration

The MetaDefender Core supports REST interface powered by Nginx's web server.

Here are Nginx configuration guidelines:

- [3.2.3.1 API Rate Limiting](#)
- [3.2.3.2 SSL Configurations](#)
- [3.2.3.3 Hardening](#)
- [3.2.3.4 Origin Client Source Identification](#)
- [3.2.3.5 Web Server Processing Statistics Query](#)

3.2.3.1 API Rate Limiting

By default MetaDefender Core does not have any hard limit on the number of API requests coming to Nginx web server. However, in order to secure more your MetaDefender Core server, users are supported to limit the number of API requests to better control their server load and prevent potential DOS (Deny of service) attack (this feature has been introduced since MetaDefender Core version 4.15.0).

This configuration support is applicable to two REST requests on MetaDefender Core:

- [Login \(POST /login\)](#)
- [Process a file \(POST /file\)](#)

On Linux

1. Create file `nginx_rate_limit.ini` in the directory `/etc/ometascan/nginx.d`



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

2. Enter the following settings into the file:

```
max_scan_request = X;  
max_login_request = Y;
```

Whereas $X, Y > 0$ (If X or Y is not valid then MetaDefener Core will ignore and remain unlimited as default behavior).

When these configurations are set, MetaDefender Core will allow users to send maximum X "/login" REST request per minute, and maximum Y "/file" REST request per minute.

3. Restart MetaDefender Core service (ometascan).

On Windows

1. Create file `nginx_rate_limit.ini` in the directory `<Installation Directory>\nginx`



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

2. Enter the following settings into the file:

```
max_scan_request = X;  
max_login_request = Y;
```

Whereas $X, Y > 0$ (If X or Y is not valid then MetaDefener Core will ignore and remain unlimited as default behavior).

When these configurations are set, MetaDefender Core will allow users to send maximum X "/login" REST request per minute, and maximum Y "/file" REST request per minute.

3. Restart MetaDefender Core service (ometascan).

How this feature actually works:

This feature fundamentally respects Nginx web server's rate limiting, learn it more: <https://www.nginx.com/blog/rate-limiting-nginx/>

For instance, users can set a limit for [Process a file \(POST /file\)](#) by setting "max_scan_request" = 600, that means MetaDefender Core only allows serving maximum 600 file process requests per minute. However due to the fact that NGINX mechanism tracks request at millisecond granularity, this limit means 1 request per 100 milliseconds, and thus users should not be able to send all 600 process requests at once (In this particular circumstance, every request coming after the allowed one will be rejected, and result in HTTP 503 response error code)

3.2.3.2 SSL Configurations

- 1.) Create a "ssl.conf" file

- On Windows, under **<Installation Directory>\nginx**

```
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";
```

- On Linux, under **/etc/ometascan/nginx.d/**

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

- 2.) A restart of the "OPSWAT Metadefender Core" service is required.

Advanced SSL configurations

- 1.) Explicitly allow specific TLS versions, optionally with preferred ciphers. For example:

```
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";

ssl_protocols tlsv1.1 tlsv1.2
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256
```

2.) Use SSL private key and(or) certificate which is encrypted with a passphrase. Strongly recommended to put the passphrase file(s) into a secured vault where only MetaDefender Core can access.

A reference for typical practice: <https://www.nginx.com/blog/protecting-ssl-private-keys-nginx-hashicorp-vault/>

```
ssl on;

ssl_certificate "C:/Program Files/OPSWAT/Metadefender Core/nginx
/cert.pem";
ssl_certificate_key "/etc/keys/secretkey.pass";

ssl_certificate_key "C:/Program Files/OPSWAT/Metadefender Core
/nginx/your_encrypted.key";
ssl_password_file "/etc/keys/private.pass";

ssl_protocols tlsv1.1 tlsv1.2
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256
```

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

3.2.3.3 Hardening

 Only applicable to MetaDefender Core version 4.19.0 or above.

- [3.2.3.3.1 Restriction](#)
- [3.2.3.3.2 OSCP Stapling and Session Cache](#)
- [3.2.3.3.3 SELinux Secured Policy](#)

3.2.3.3.1 Restriction

 Only applicable to MetaDefender Core version 4.19.0 or above.

Only allow access to our domain only

```
if ( $host !~ ^(metadefendercore.in|www.metadefendercore.in|images.
metadefendercore.in)$ ) {
    return 444;
}
```

Deny certain user-agents

Blocking user-agents i.e. scanners, bots, and spammers who may be abusing your server.

```
## Block download agents ##
if ( $http_user_agent ~* LWP::Simple|BBBike|wget ) {
    return 403;
}
##

## Block robots ##
if ( $http_user_agent ~* msnbot|scrapbot ) {
    return 403;
}
##
```

Block referral spam

Only direct access is allowed

```
## Deny certain Referers ###
if ( $http_referer ~*
(babes|forsale|girl|jewelry|love|nudit|organic|poker|porn|sex|teen
) ) {
    return 403;
}
##
```

How to configure

1.) Create a .conf file (create “built-in” folder if not existed)

- On Windows, under **<Installation Directory>\nginx\built-in**

- On Linux, under **/etc/ometascan/nginx.d/built-in/**

Here is sample .conf file. Choose what meets to your scenario and update .conf file

```

if ($host !~ ^(metadefendercore.in|www.metadefendercore.in|images.
metadefendercore.in)$ ) {
    return 444;
}

if ($http_user_agent ~* LWP::Simple|BBBike|wget) {
    return 403;
}

if ($http_user_agent ~* msnbot|scrapbot) {
    return 403;
}

if ( $http_referer ~*
(babes|forsale|girl|jewelry|love|nudit|organic|poker|porn|sex|teen
) ) {
    return 403;
}

```

2.) A restart of the “OPSWAT Metadefender Core” service is required.

3.2.3.3.2 OSCP Stapling and Session Cache

 Only applicable to MetaDefender Core version 4.19.0 or above.

1.) Modify “ssl.conf” file (create new if not existed)

- On Windows, under **<Installation Directory>\nginx**
- On Linux, under **/etc/ometascan/nginx.d/**

Modify ssl.conf file with following recommended settings

```

# Enable OSCP stapling, Optimize session cache
ssl_ecdh_curve secp384r1;
ssl_session_timeout 1d;
ssl_session_cache shared:SSL:10m;
ssl_session_tickets off;
ssl_stapling on;
ssl_stapling_verify on;

```

```
# verify chain of trust of OCSP response using Root CA and
Intermediate certs
ssl_trusted_certificate /path/to/root_CA_cert_plus_intermediates;

# replace with the IP address of your resolver
resolver 127.0.0.1;
```

2.) A restart of the “OPSWAT Metadefender Core” service is required.

3.2.3.3 SELinux Secured Policy

 Only applicable to MetaDefender Core version 4.19.0 or above.

By default, SELinux (Linux security system based on role access, available on RedHat and CentOS) does not protect the Nginx web server. The following instruction will help you setup and turn on the protection.

1.) First, install required SELinux compile-time support:

```
yum -y install selinux-policy-targeted selinux-policy-devel
```

2.) The download targeted SELinux policies to harden the Nginx web server on Linux servers from the

[selinuxnginx project](#) page:

```
cd /opt
wget 'http://downloads.sourceforge.net/project/selinuxnginx/se-
nginx_1_0_10.tar.gz?use_mirror=nchc'
```

3.) Untar the same:

```
tar -zxvf se-nginx_1_0_10.tar.gz
```

4.) Compile the same

```
cd se-nginx_1_0_10/nginx
make
```

Sample output:

```
Compiling targeted nginx module
/usr/bin/checkmodule: loading policy configuration from tmp
/nginx.tmp
/usr/bin/checkmodule: policy configuration loaded
/usr/bin/checkmodule: writing binary representation (version 6)
to tmp/nginx.mod
Creating targeted nginx.pp policy package
rm tmp/nginx.mod.fc tmp/nginx.mod
```

5.) Install the resulting nginx.pp SELinux module:

```
/usr/sbin/semodule -i nginx.pp
```

3.2.3.4 Origin Client Source Identification

 Only applicable to MetaDefender Core version 4.19.0 or above.

By default, when triggering scan from client through a load balancer or proxy server, MetaDefender Core's Nginx web server will not identify the original client source (but the load balancer or proxy server's address instead).

In order to force Nginx web server to trace back the origin client source:

1.) Create a "extra.conf" file

- On Windows, under **<Installation Directory>\nginx**
- On Linux, under **/etc/ometascan/nginx.d/**

```
set_real_ip_from 192.168.1.1;
real_ip_header X-Forwarded-For;
real_ip_recursive on;
```

Make sure to change "192.168.1.1" to your actual load balancer or proxy server address.

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

3.2.3.5 Web Server Processing Statistics Query

 Only applicable to MetaDefender Core version 4.19.0 or above.

Configure Nginx web server

1.) Create a “status.conf” file

- On Windows, under **<Installation Directory>\nginx**
- On Linux, under **/etc/ometascan/nginx.d/**

```
server {  
    listen 8088 ; listen [::]:8088 ;  
    location = /nginx_status {  
        stub_status;  
    }  
}
```

2.) A restart of the “OPSWAT Metadefender Core” service is required.

Query Nginx processing stats information

Property	Value
DESCRIPTION	Query Nginx processing stats information
URL	http://<server>:<port>/nginx_status
HTTP METHOD	GET

Response

Result code	Value	Description
200	<pre>Active connections: <n> server accepts handled requests <a1> <a2> <a3> Reading: <b1> Writing: <b2> Waiting: <b3></pre>	<p>Request processed successfully.</p> <ul style="list-style-type: none">• Active connections <n> <p>The current number of active client connections including waiting <b3> connections.</p> <ul style="list-style-type: none">• accepts <a1>

Result code	Value	Description
	<p>For example:</p> <pre> Active connections: 1 server accepts handled requests 144 144 358 Reading: 0 Writing: 1 Waiting: 0 </pre>	<p>The total number of accepted client connections.</p> <ul style="list-style-type: none"> • handled <a2> <p>The total number of handled connections. Generally, the parameter value is the same as accepts <a1> unless some resource limits have been reached (for example, the worker_connections limit).</p> <ul style="list-style-type: none"> • requests <a3> <p>The total number of client requests.</p> <ul style="list-style-type: none"> • Reading <b1> <p>The current number of connections where nginx is reading the request header.</p> <ul style="list-style-type: none"> • Writing <b2> <p>The current number of connections where nginx is writing the response back to the client.</p> <ul style="list-style-type: none"> • Waiting <b3> <p>The current number of idle client connections waiting for a request.</p>

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](#)
- [3.3.6. Single Sign-On \(SSO\)](#)

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 local admin user needs to be created under LOCAL user directory following the welcome wizard

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](#).

⚠ If enhanced password policy is enabled for the user directory this user belongs to, then the new password must fulfil the password complexity requirements listed on the [3.3.3. User directories](#) page.

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 [148068294](#) 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 [148068294](#) 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 'ROLES' tab is selected, displaying a table with the following data:

ROLENAME	DISPLAY NAME	NUMBER OF USERS	RIGHTS
admin	Administrators	1	Functionality: Full API: Anyone
security_admin	Security administrators	0	Functionality: Full: Processing history, Quarantine, Update history, Workflow rules, Workflow templates, Security zones, Nodes, Engines, External settings, Skip by hash settings, Certificates, Update settings, Scan settings API: Anyone
security_auditor	Security auditor	0	Functionality: Read-only API: Anyone
help_desk	Help desk	0	Functionality: Read-only: Processing history, Update history, Workflow rules, Workflow templates, Security zones, Nodes, Engines, External settings, Skip by hash settings, Scan settings API: Anyone

Default roles

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

Rolename	Display name	Default member username	Permissions on functionality	Permissions on API level
admin	Administrators	admin	Full on all functions	Be able to fetch scan result submitted by anyone Be able to download processed file where original file was submitted by anyone
security_admin	Security administrators		Full on Scan history, Update history, Security rules, Security zones, Analysis workflows, Scan nodes, Engines, Update settings, Scan settings functions	Be able to fetch scan result submitted by anyone Be able to download processed file where original file was submitted by anyone
security_auditor	Security auditor		Read-only on a ll except External settings functions	Be able to fetch scan result submitted by anyone Be able to download processed file where original file was submitted by anyone
help_desk	Help desk		Read-only on Scan history, Update history, Security rules, Security zones, Analysis workflows, Scan nodes, Engines, Scan settings functions	Be able to fetch scan result submitted by anyone Be able to download processed file where original file was submitted by anyone

Permissions on functionality

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.

Permissions on API level

Each role has a set of rights pertaining to REST API access level, including following REST endpoints:

Processing result fetching:

- GET /hash/<md5, sha1, sha256> ([Fetch processing result](#))
- GET /file/<data_id> ([Fetch processing result](#))
- GET /file/batch/<batch_id> ([Status of Batch](#))
- GET /stat/log/scan (Leveraged by Core management console)
- GET /stat/log/scan/export (Leveraged by Core management console)

Download processed file:

- GET /file/converted/<data_id> ([Download Sanitized Files](#))
- GET /file/processed/<data_id> (Leveraged by Core 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 REST APIs (return "Access denied" error) and relevant functionalities on Metadefender Core v4 Web Management Console

- **Note:** When "NONE" is selected for "Processing result fetching", "Processing history" menu item under Dashboard will automatically switch to "READ-ONLY" right, and "FULL" right will instead be disabled for selection ("FULL" right can be only enabled for selection back when this option is switched to "ANYONE")

Modify role

Dashboard	
Processing history	<input type="radio"/> NONE <input checked="" type="radio"/> READ-ONLY <input type="radio"/> FULL
Quarantine	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Update history	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Config history	<input checked="" type="radio"/> NONE <input type="radio"/> READ-ONLY <input type="radio"/> FULL
Policies	
Workflow rules	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Workflow templates	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Security zones	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Inventory	
Nodes	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Engines	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
External settings	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Skip by hash settings	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Certificates	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Settings	
Data retention	<input checked="" type="radio"/> NONE <input type="radio"/> READ-ONLY <input type="radio"/> FULL
User management	<input checked="" type="radio"/> NONE <input type="radio"/> READ-ONLY <input type="radio"/> FULL
License	<input checked="" type="radio"/> NONE <input type="radio"/> READ-ONLY <input type="radio"/> FULL
Update settings	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Scan settings	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
API access	
Processing result fetching	<input checked="" type="radio"/> NONE <input type="radio"/> SELF-ONLY <input type="radio"/> ANYONE
Download processed file	<input type="radio"/> NONE <input type="radio"/> SELF-ONLY <input checked="" type="radio"/> ANYONE

- **Self-only:**
 - Users of this role only have right to access the given REST APIs and relevant functionalities on Metadefender Core v4 Web Management Console where the scan requests were submitted by themselves only
 - Users of this role have no right to access the given REST APIs (return "Access denied" error) where scan requests were submitted by anyone else
 - **Note:** When "SELF-ONLY" is selected for "Processing result fetching", "Processing history" menu item under Dashboard will automatically switch to "READ-ONLY" right, and "FULL" right will instead be disabled for selection ("FULL" right can be only enabled for selection back when this option is switched to "ANYONE")

Modify role

Dashboard	
Processing history	<input type="radio"/> NONE <input checked="" type="radio"/> READ-ONLY <input type="radio"/> FULL
Quarantine	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Update history	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Config history	<input checked="" type="radio"/> NONE <input type="radio"/> READ-ONLY <input type="radio"/> FULL
Policies	
Workflow rules	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Workflow templates	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Security zones	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Inventory	
Nodes	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Engines	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
External settings	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Skip by hash settings	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Certificates	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Settings	
Data retention	<input checked="" type="radio"/> NONE <input type="radio"/> READ-ONLY <input type="radio"/> FULL
User management	<input checked="" type="radio"/> NONE <input type="radio"/> READ-ONLY <input type="radio"/> FULL
License	<input checked="" type="radio"/> NONE <input type="radio"/> READ-ONLY <input type="radio"/> FULL
Update settings	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
Scan settings	<input type="radio"/> NONE <input type="radio"/> READ-ONLY <input checked="" type="radio"/> FULL
API access	
Processing result fetching	<input type="radio"/> NONE <input checked="" type="radio"/> SELF-ONLY <input type="radio"/> ANYONE
Download processed file	<input type="radio"/> NONE <input type="radio"/> SELF-ONLY <input checked="" type="radio"/> ANYONE

- **Anyone:** Users of this role have full access to the given REST APIs and relevant functionalities on Metadefender Core v4 Web Management Console where the scan requests were submitted by anyone

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, policy settings may be applied:

- **Number of failed logins before lockout:** After this number of consecutive failed login attempts the account gets locked.
- **Lockout time [minutes]:** The account remains locked for the given minutes.
 - When the lockout time elapses, the account lock gets released automatically.
 - Users with appropriate permission may release the account lock earlier using the [RELEASE LOCKOUT button](#).
- **Enable enhanced password policy:** Check out more at [3.8.3 Password Policy](#)

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 [148068766](#) 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.

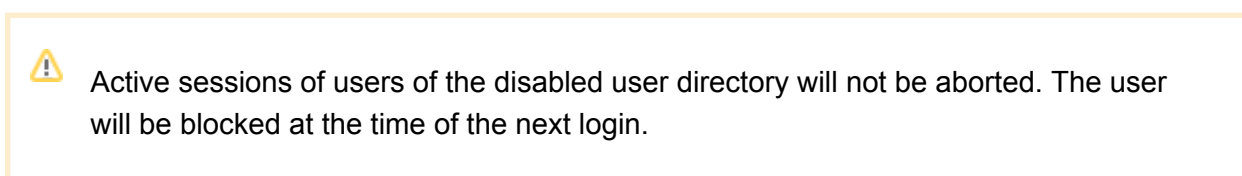


Enable or disable user directory

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.



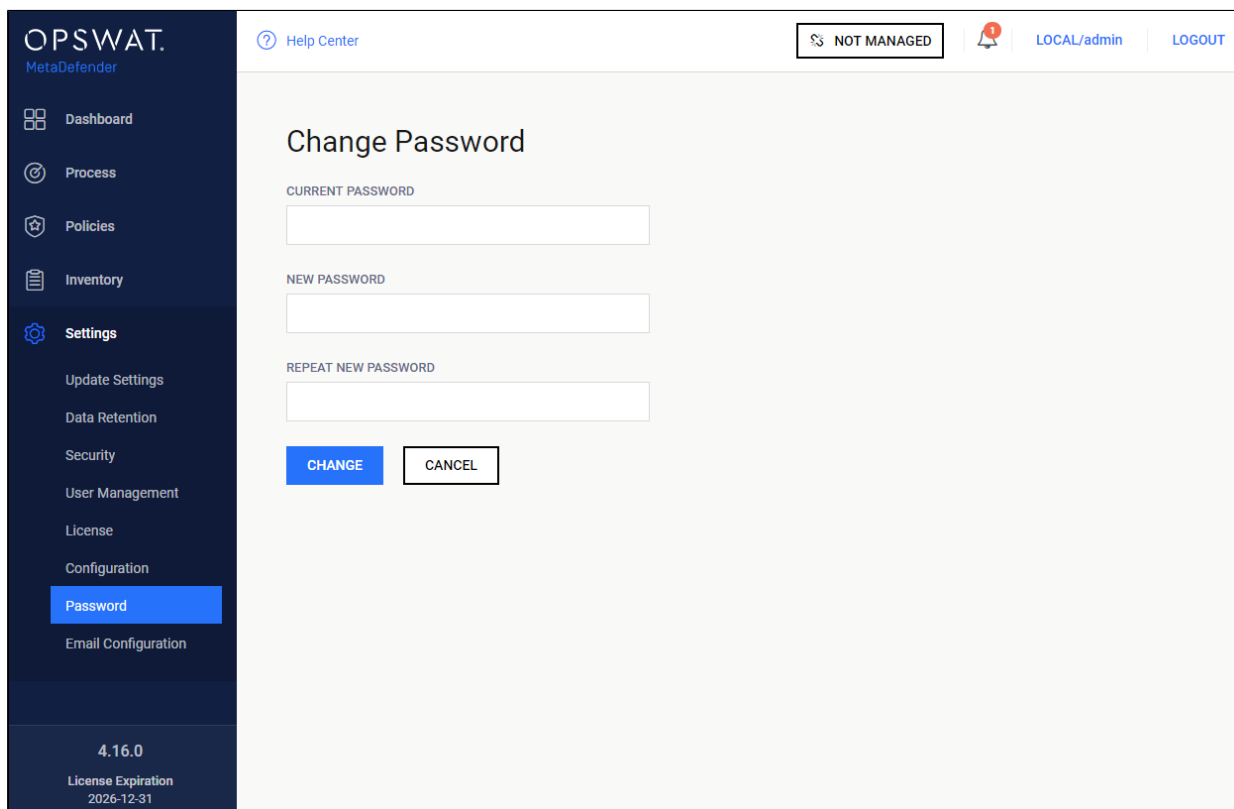
Taking the above example into consideration: a user search DN of "OU=People,OU=Engineering,DC=example,DC=com" could potentially result in much faster server response than "DC=example,DC=com" and should be preferred assuming all users reside under "OU=People,OU=Engineering,DC=example,DC=com" in the directory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

⚠ If enhanced password policy is enabled for the user directory this user belongs to, then the new password must fulfil the password complexity requirements listed on the [3.3.3. User directories](#) page.

3.3.6. Single Sign-On (SSO)

Since MetaDefender Core 4.18.0, Single Sign-On (SSO) authentication is supported to integrate with most of Identifier Providers (IDP) thanks to its various authentication protocols support:

- OpenID Connect (OIDC) 1.x
- Security Assertion Markup Language (SAML) 2.x

- ... And more coming soon (i.e. Kerberos)

Check out all integration guidelines:

- [3.3.6.1. OpenID Connect \(OIDC\) Integration](#)
- [3.3.6.2. SAML Integration](#)
- [3.3.6.3. Backup Login](#)

3.3.6.1. OpenID Connect (OIDC) Integration

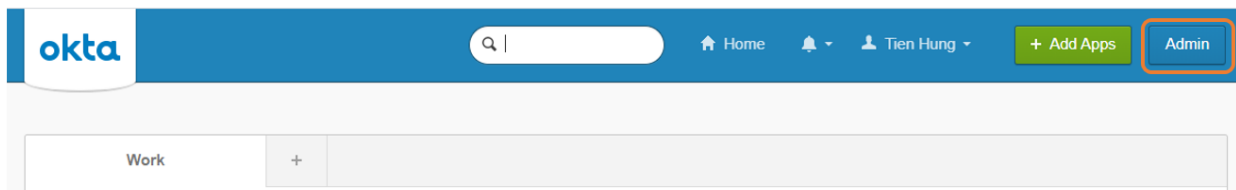
In order to integrate MetaDefender Core with OIDC:

- [Create new application on IDP site for MetaDefender Core](#)
- [On MetaDefender Core management console, create a new user directory for SSO](#)
- [Sign on using IDP authentication](#)

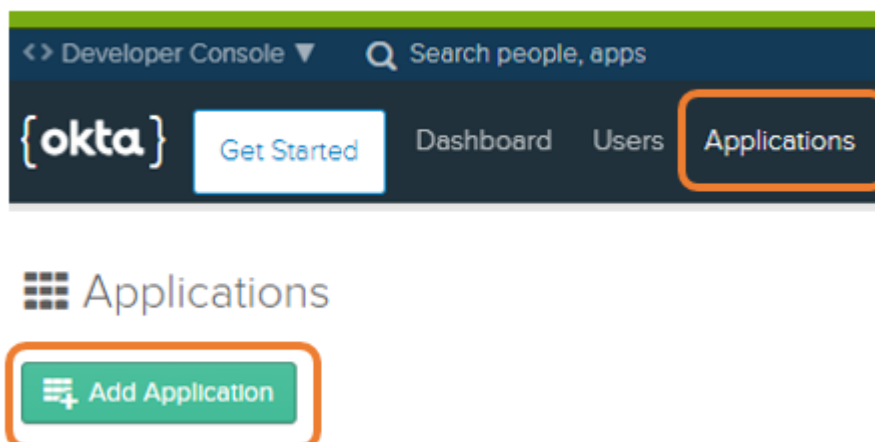
Create new application on IDP site for MetaDefender Core

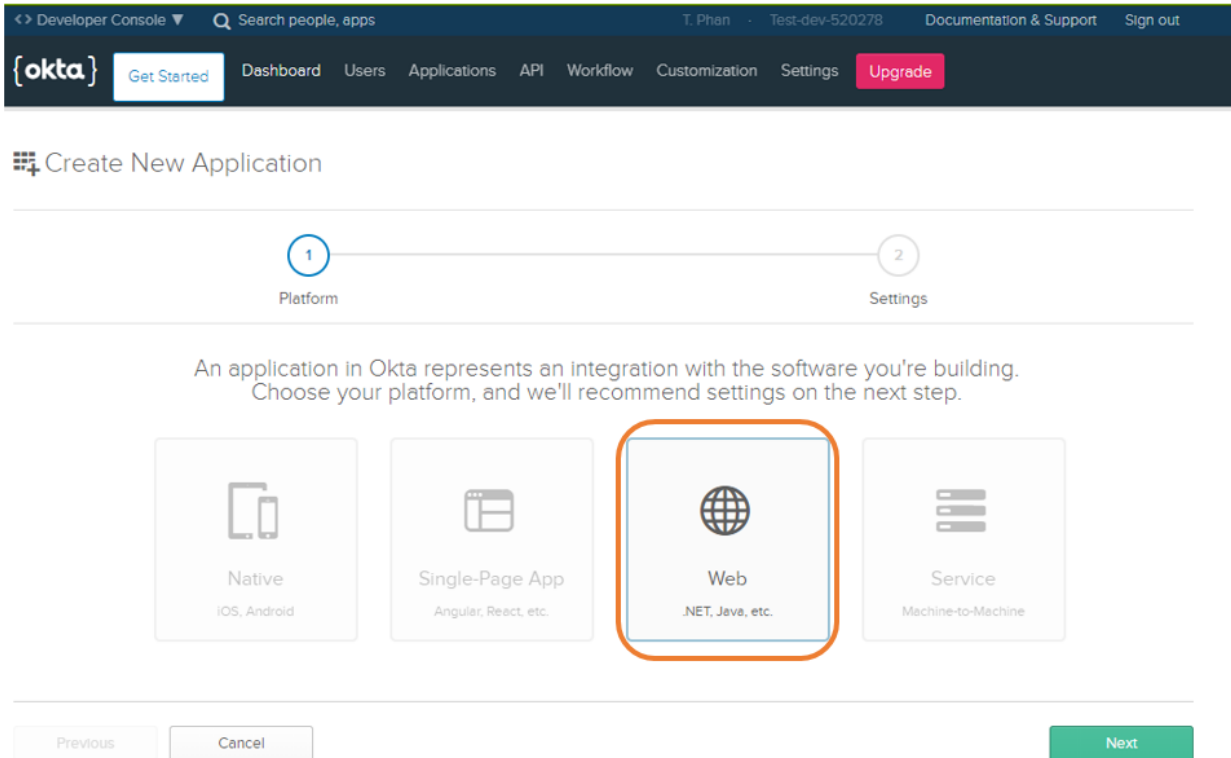
We selected Okta IDP (<https://www.okta.com/>) as a supported IDP to demonstrate OIDC integration with MetaDefender Core.

1.) Sign in Okta site, and navigate to admin dashboard

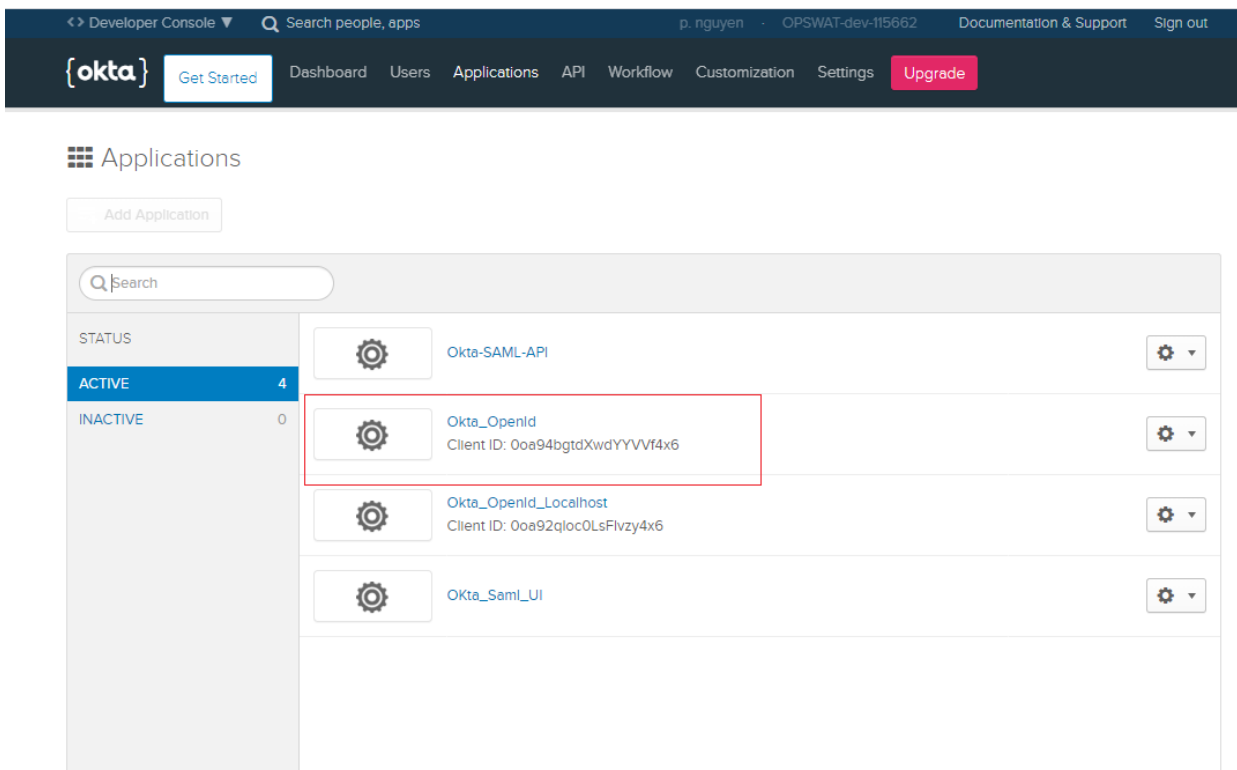


2.) Add an application, select “Web” application type, and **choose “OpenID Connect” for Sign on method**





Making sure the new created application in ACTIVE list (e.g. Okta_OpenId)



Access to the new created application (e.g. Okta_OpenId), navigate to “General” tab, create a new secret if not existed:

Client acting on behalf of a user

- Authorization Code
- Refresh Token
- Implicit (Hybrid)

LOGIN

Login redirect URIs ? <http://192.168.200.141:8008/ssologin/oidc/dWto>

Logout redirect URIs ?

Login initiated by [?](#) App Only

Initiate login URI <http://192.168.200.141:8008/#/public/login>

Client Credentials Cancel

Client ID [?](#) 00a94bgtdXwdYYVvF4x6
Public Identifier for the client that is required for all OAuth flows.

Client secret [?](#)

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

[Generate New Client Secret](#)

Once done, expecting to have ClientID and Client secret created:

Client Credentials
Edit

Client ID 📄

Public Identifier for the client that is required for all OAuth flows.

Client secret 👁️ 📄

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

On MetaDefender Core management console, create a new user directory for SSO

- Navigate to Settings > User Management
- On “USER DIRECTORIES” tab, hit “ADD NEW USER DIRECTORY” button
- Choose “OpenID Connect (OIDC)” option for “USER DIRECTORY TYPE”
- Type directory name at your choice
- In “IDENTIFY PROVIDER” section, hit “FETCH” button to input IDP’s designated metadata API URL (e.g. Okta could be found at <https://developer.okta.com/docs/reference/api/oidc/#well-known-oauth-authorization-server>)

IDENTITY PROVIDER

ISSUER

FETCH
SUBMIT

OK

CANCEL

CLIENT SECRET

Add user directory

USER DIRECTORY TYPE

NAME

IDENTITY PROVIDER

ISSUER

- In “IDENTIFY PROVIDER” section:

+ Fill up “Client ID” and “Client Secret” matched to what generated in IDP console:

MetaDefender Core

SERVICE PROVIDER

CLIENT ID

CLIENT SECRET

Okta console

Client Credentials

Client ID

Public identifier for the client that is required for all OAuth flows.

Client secret

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

+ On MetaDefender Console current display, type your MetaDefender Core address in “HOST OR IP” field

HOST OR IP

and a login redirect URL will be auto generated by MetaDefender Core, you will want to copy the full link to proceed:

LOGIN URL

http://192.168.200.143:8008/ssologin/oidc/LiZO



+ Switching to Okta IDP console, paste the login redirect URL and also input the Initiate login URI

General Settings

Cancel

APPLICATION

Application label: Okta_OpenId

Application type: Web

Allowed grant types:

- Client acting on behalf of itself
 - Client Credentials
- Client acting on behalf of a user
 - Authorization Code
 - Refresh Token
 - Implicit (Hybrid)

LOGIN

Login redirect URIs: ×
+ Add URI

Logout redirect URIs: + Add URI

Login initiated by:

Initiate login URI:

Save Cancel

“USER IDENTIFIED BY” field:

1. Username can be constructed by *claims* under *profile* scope
2. Claim variable is specified by syntax `${<claim-name>}`

Notes: Supported claims under *profile* scope are IDP specified. Please review IDP document for more details. For example, for Okta: <https://developer.okta.com/blog/2017/07/25/oidc-primer-part-1>

LOGIN URL

`http://192.168.200.141:8008/ssologin/oidc/BNJE`



USER IDENTIFIED BY

`${given_name}_${family_name}`

- In “USER ROLE” section, you are supported to choose default role to map an existing MetaDefender Core local role:

USER ROLE

ROLE MATCHING OPTION

Default role



USER ROLE

Administrators



Or create a custom role mapping based on RegEx:

USER ROLE

ROLE MATCHING OPTION

Role mapping

ROLE MATCHING RULES

RULE 1 

SCOPE

profile

KEY

email

VALUE 1 

MATCHING TYPE

Regular expression

CONDITION

admin@company.com

ASSIGN TO ROLES

Security administrators

[Add new role](#)

[Add new value](#)

[Add new rule](#)

- Hit “ADD” button to finish creating new SSO user directory, by default the new created user directory is disabled:

OPSWAT.
MetaDefender Core

Help Center NOT MANAGED LOCAL/admin LOGOUT

User Management

RELEASE LOCKOUT ADD NEW USER DIRECTORY

USERS AND GROUPS ROLES USER DIRECTORIES

USER DIRECTORY	ACTIVE
LOCAL	✓
SYSTEM	✓
OIDC OKTA	✗

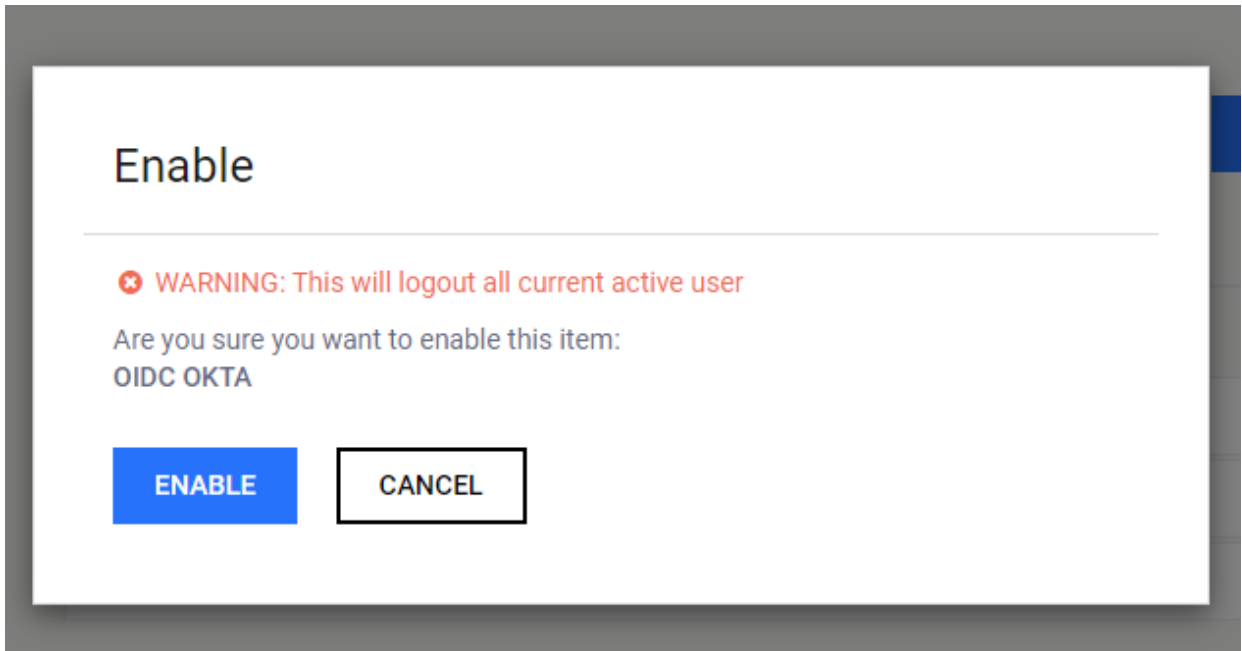
4.18.0
License Expiration 2026-12-31

You may want to enable it for SSO login fashion

Warning: This action will auto forcefully logout all current active users

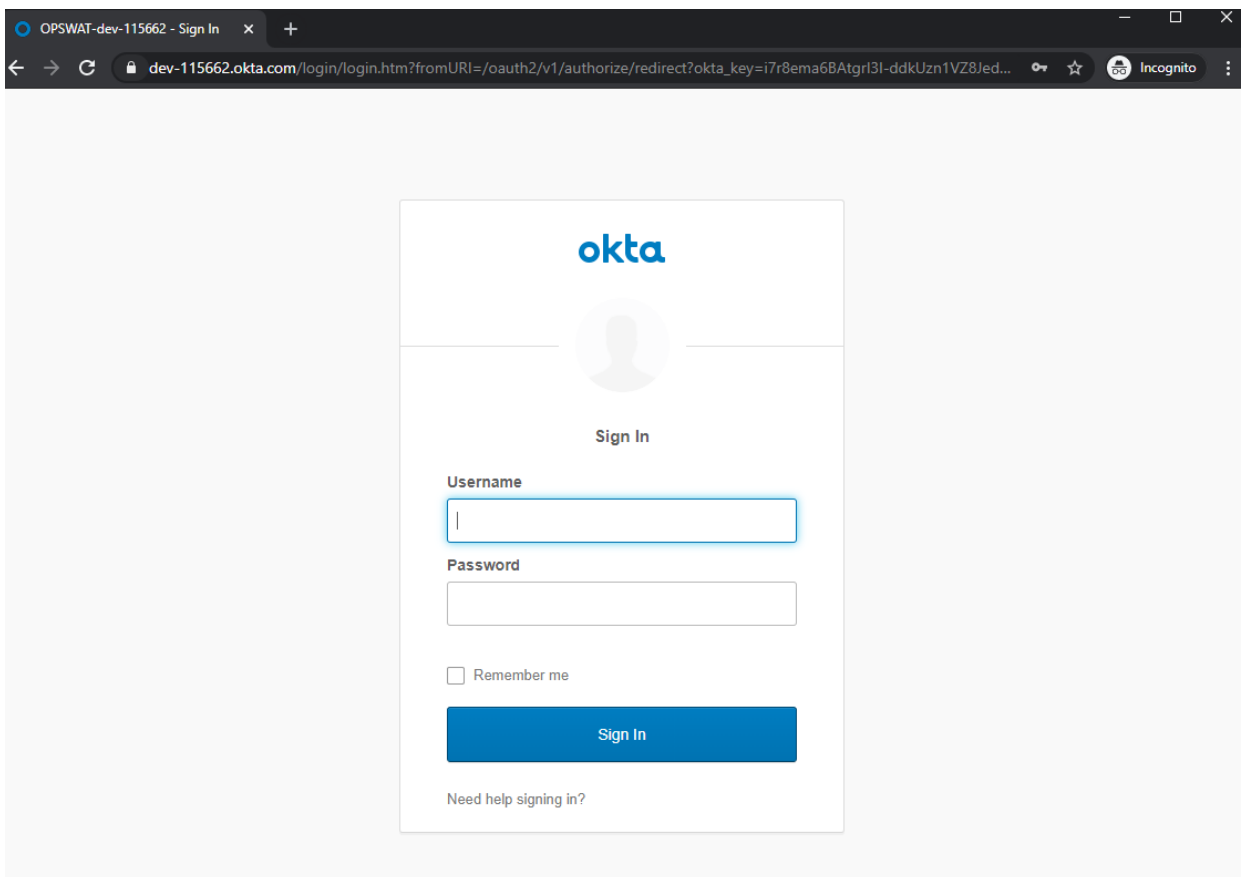
USERS AND GROUPS ROLES USER DIRECTORIES

USER DIRECTORY	ACTIVE	
LOCAL	✓	
SYSTEM	✓	
OIDC OKTA	✗	✎ ✓ 🗑️

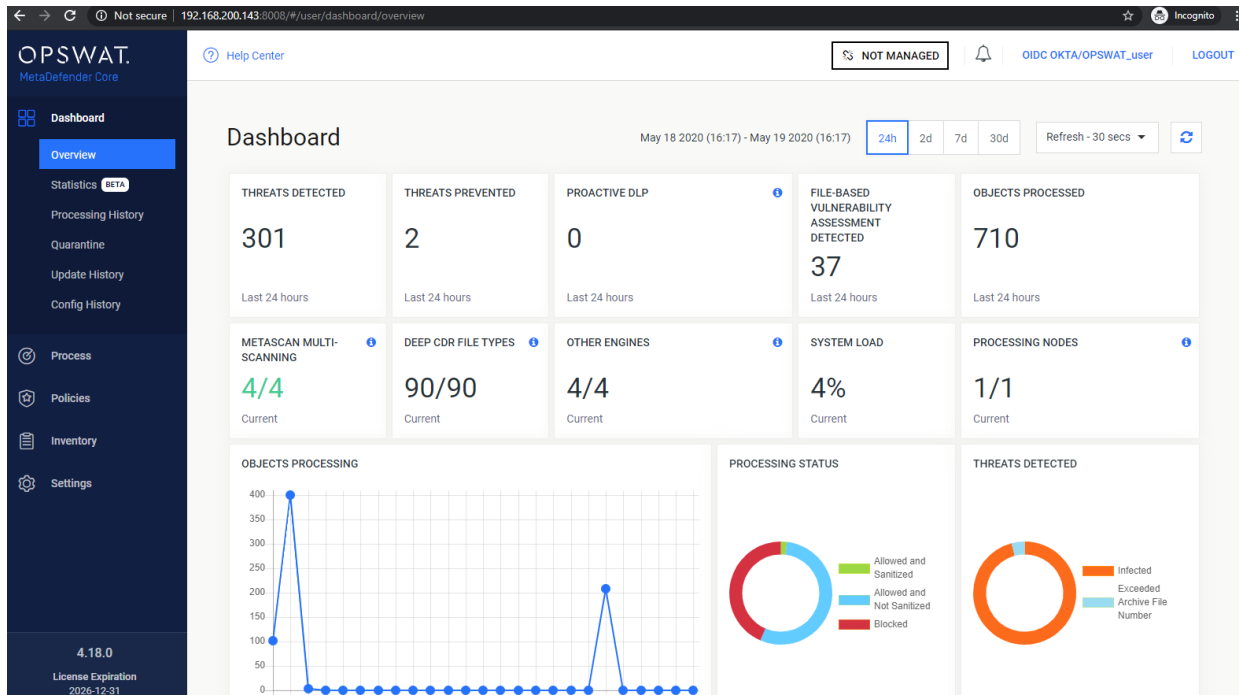


Sign on using IDP authentication

Now hitting "LOGIN" button on MetaDefender Core management console upon created SSO user directory, it will auto redirect you to Okta IDP login page as expected:



- Logged in successfully will help you are redirected back to MetaDefender Core management console:



3.3.6.2. SAML Integration

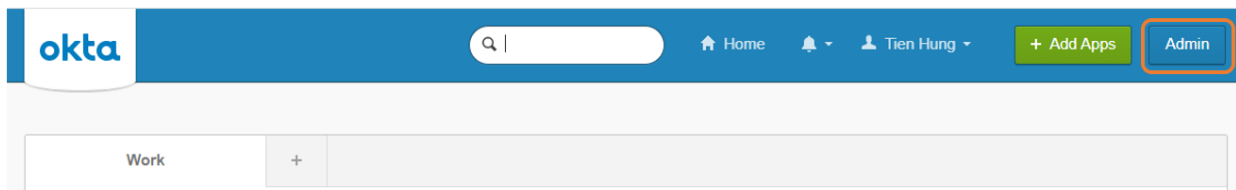
In order to integrate MetaDefender Core with SAML 2.x:

- [Create new application on IDP site for MetaDefender Core](#)
- [On MetaDefender Core management console, create a new user directory for SSO](#)
- [Sign on using IDP authentication](#)

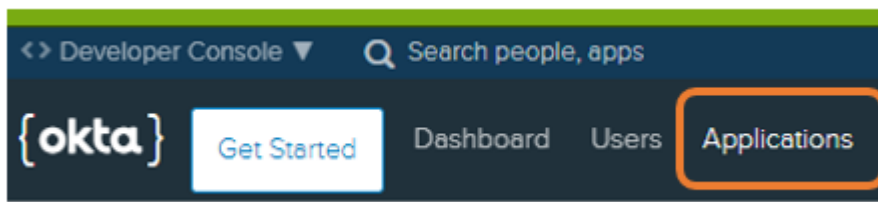
Create new application on IDP site for MetaDefender Core

We selected Okta IDP (<https://www.okta.com/>) as a supported IDP to demonstrate SAML integration with MetaDefender Core.

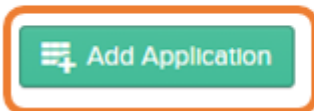
1.) Sign in Okta site, and navigate to admin dashboard



2.) Add an application, select “Web” application type, and **choose “SAML 2.0” for Sign on method**



Applications



Create a New Application Integration ✕

Platform

Sign on method SAML 2.0
Uses the SAML protocol to log users into the app.

OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

Proceeding to “Configure SAML” step on SAML integration configuration, and keep this page on-hold, we need to generate some data from MetaDefender Core management console before getting back to this page later.

Edit SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

A SAML Settings

GENERAL

Single sign on URL

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Recipient URL

Destination URL

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Application username

Show Advanced Settings

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

On MetaDefender Core management console, create a new user directory for SSO

- Navigate to Settings > User Management
- On "USER DIRECTORIES" tab, hit "ADD NEW USER DIRECTORY" button
- Choose "Security Assertion Markup Language (SAML)" option for "USER DIRECTORY TYPE"
- Type directory name at your choice
- In "IDENTIFY PROVIDER" section, hit "FETCH" button to input IDP's SAML designated metadata API URL (e.g. Okta could be found at <https://developer.okta.com/docs/guides/add-an-external-idp/saml2/configure-idp-in-okta/>)

← Back to Applications

Okta-SAML-API
Active View Logs

Once you have a working SAML integration, submit it for Okta review to publish in the OAN. Submit your app for review

General Sign On Mobile Import Assignments

Settings Edit

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.
Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.
[View Setup Instructions](#)
Identity Provider metadata is available if this application supports dynamic configuration.

About
SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username
Choose a format to use as the default username value when assigning the application to users.
If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Add user directory

USER DIRECTORY TYPE

Security Assertion Markup Language (SAML) ▼

NAME

SAML OKTA

IDENTITY PROVIDER

ISSUER

Issuer

FETCH

SUBMIT

<https://dev-115662.okta.com/app/exk947p00JeXUMGTd4x6/sso/saml/metadata>

OK

CANCEL

<https://192.168.200.143:8008>

LOGIN URL

<https://192.168.200.143:8008/ssologin/saml/UUAr>

Add user directory

USER DIRECTORY TYPE

Security Assertion Markup Language (SAML) ▼

NAME

SAML OKTA

IDENTITY PROVIDER

ISSUER

<http://www.okta.com/exk947p00JeXUMGTd4x6>

FETCH

SUBMIT

- In “SERVICE PROVIDER” section:

+ On MetaDefender Console current display, type your MetaDefender Core address in “HOST OR IP” field

HOST OR IP

<http://192.168.200.143:8008>

and a login redirect URL will be auto generated by MetaDefender Core, you will want to copy the full link to proceed:

LOGIN URL

<https://192.168.200.143:8008/ssologin/saml/UUAr>



+ Switching to Okta IDP console, paste the single sign on URL and also input Audience URI, check “Use this for Recipient URL and Destination URL” option

Edit SAML Integration

1 General Settings 2 Configure SAML

A SAML Settings

GENERAL

Single sign on URL
 Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState
If no value is set, a blank RelayState is sent

Name ID format

Application username

Show Advanced Settings

“USER IDENTIFIED BY” field:

1. Username can be constructed by attributes set by IDP, or
2. Defined by customer on IDP site

Please review IDP document for more details. For example, for Okta: https://help.okta.com/en/prod/Content/Topics/Apps/Apps_App_Integration_Wizard_SAML.htm

LOGIN URL

https://192.168.200.143:8008/ssologin/saml/UUAr



USER IDENTIFIED BY

\$(first_name)_\$(last_name)

- In “USER ROLE” section, you are supported to choose default role to map an existing MetaDefender Core local role:

USER ROLE

ROLE MATCHING OPTION

Default role



USER ROLE

Administrators



Or create a custom role mapping based on RegEx:

USER ROLE

ROLE MATCHING OPTION

Role mapping

ROLE MATCHING RULES

RULE 1 

SCOPE

profile

KEY

email

VALUE 1 

MATCHING TYPE

Regular expression

CONDITION

admin@company.com

ASSIGN TO ROLES

Security administrators

[Add new role](#)

[Add new value](#)

[Add new rule](#)

- Hit “ADD” button to finish creating new SSO user directory, by default the new created user directory is disabled:

OPSWAT.
MetaDefender Core

Help Center NOT MANAGED OIDC OKTA/OPSWAT_user LOGOUT

User directory added successfully.

User Management

RELEASE LOCKOUT ADD NEW USER DIRECTORY

USERS AND GROUPS ROLES USER DIRECTORIES

USER DIRECTORY	ACTIVE
LOCAL	✓
SYSTEM	✓
OIDC OKTA	✓
SAML OKTA	✗

4.18.0
License Expiration 2026-12-31

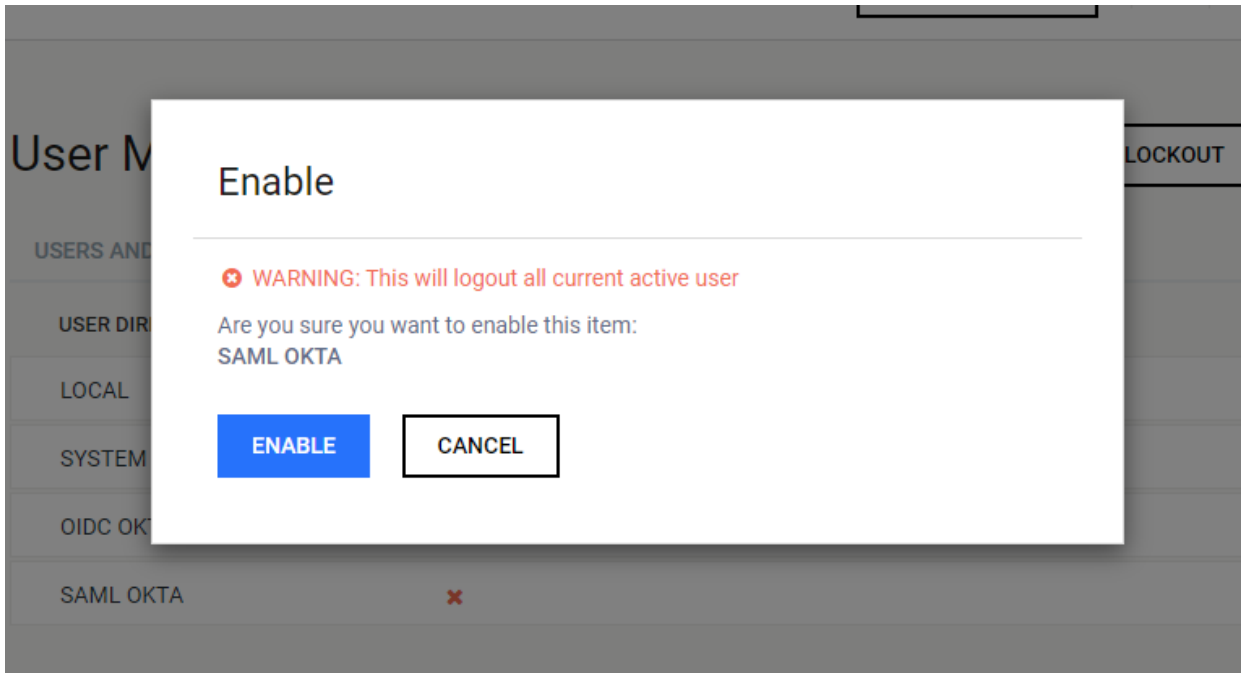
You may want to enable it for SSO login fashion

Warning: This action will auto forcefully logout all current active users

USERS AND GROUPS ROLES USER DIRECTORIES

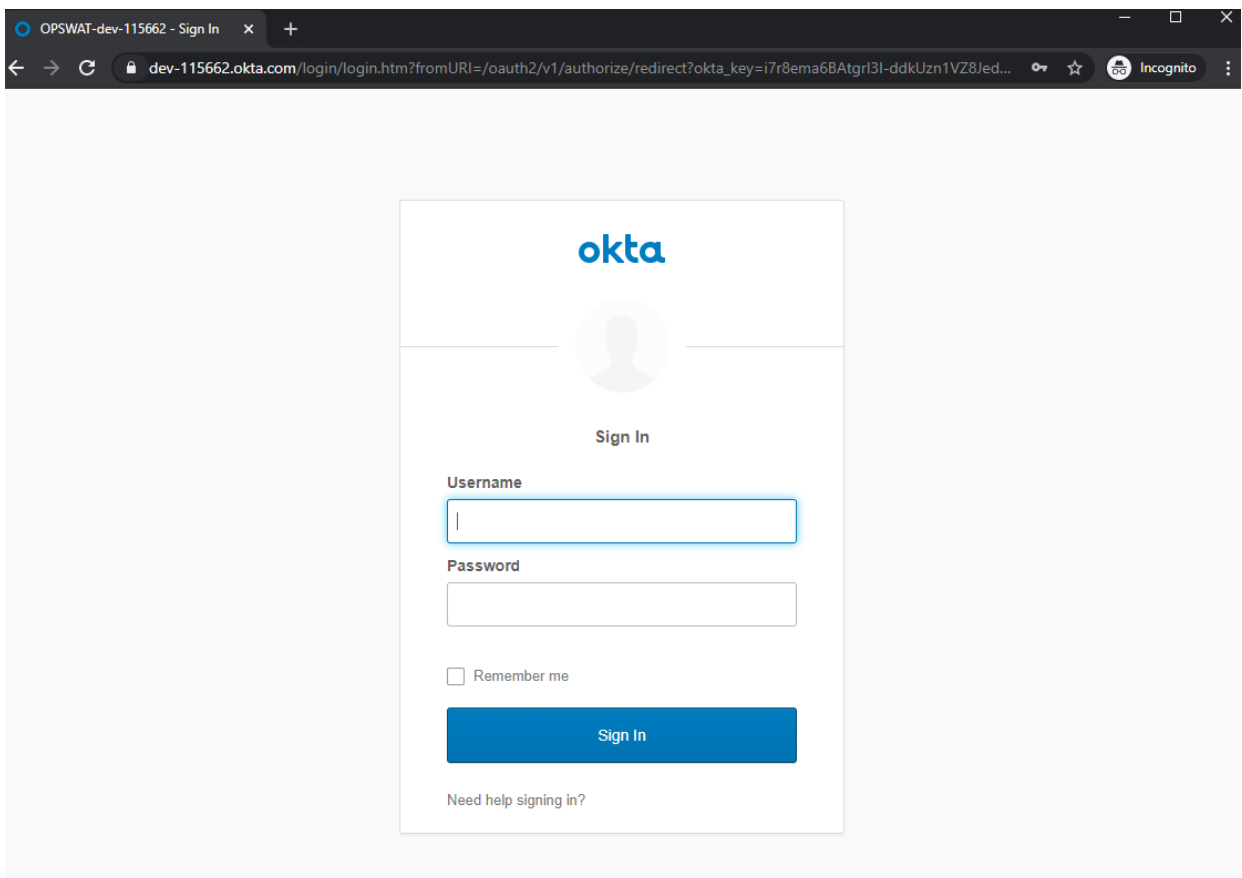
USER DIRECTORY	ACTIVE
LOCAL	✓
SYSTEM	✓
OIDC OKTA	✓
! SAML OKTA	✗

✎ ✓ 🗑️

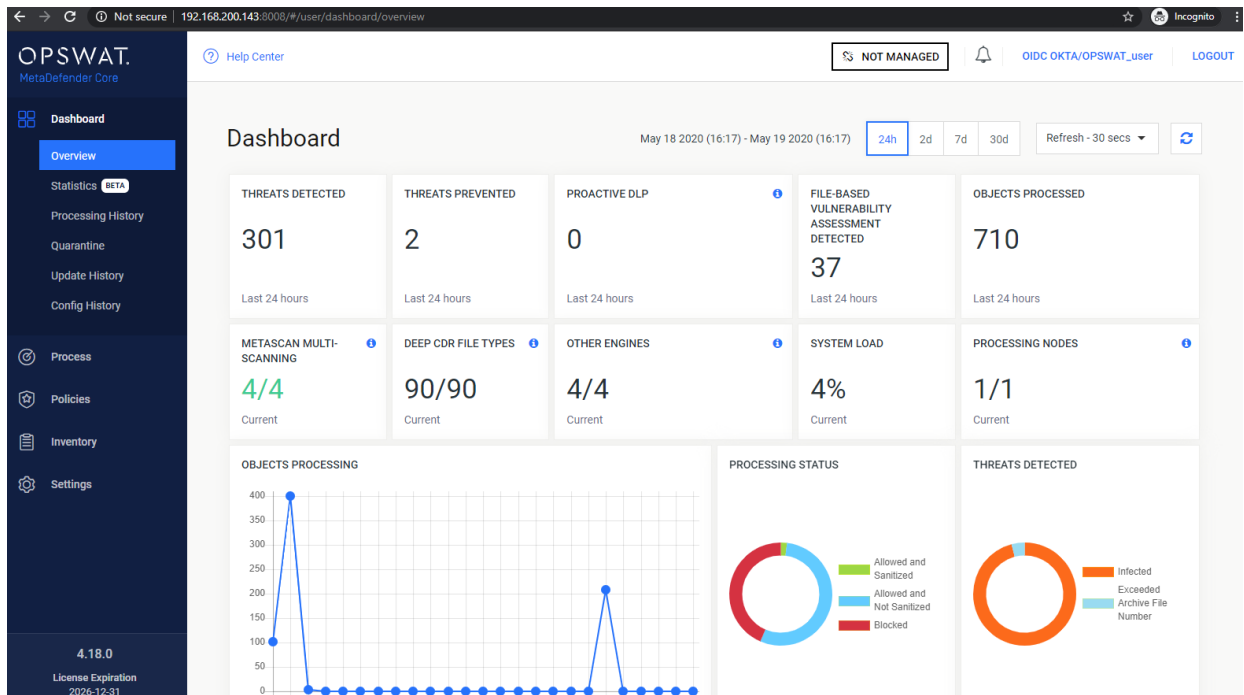


Sign on using IDP authentication

Now hitting “LOGIN” button on MetaDefender Core management console upon created SSO user directory, it will auto redirect you to SAML IDP login page as expected:



- Logged in successfully will help you are redirected back to MetaDefender Core management console:



3.3.6.3. Backup Login

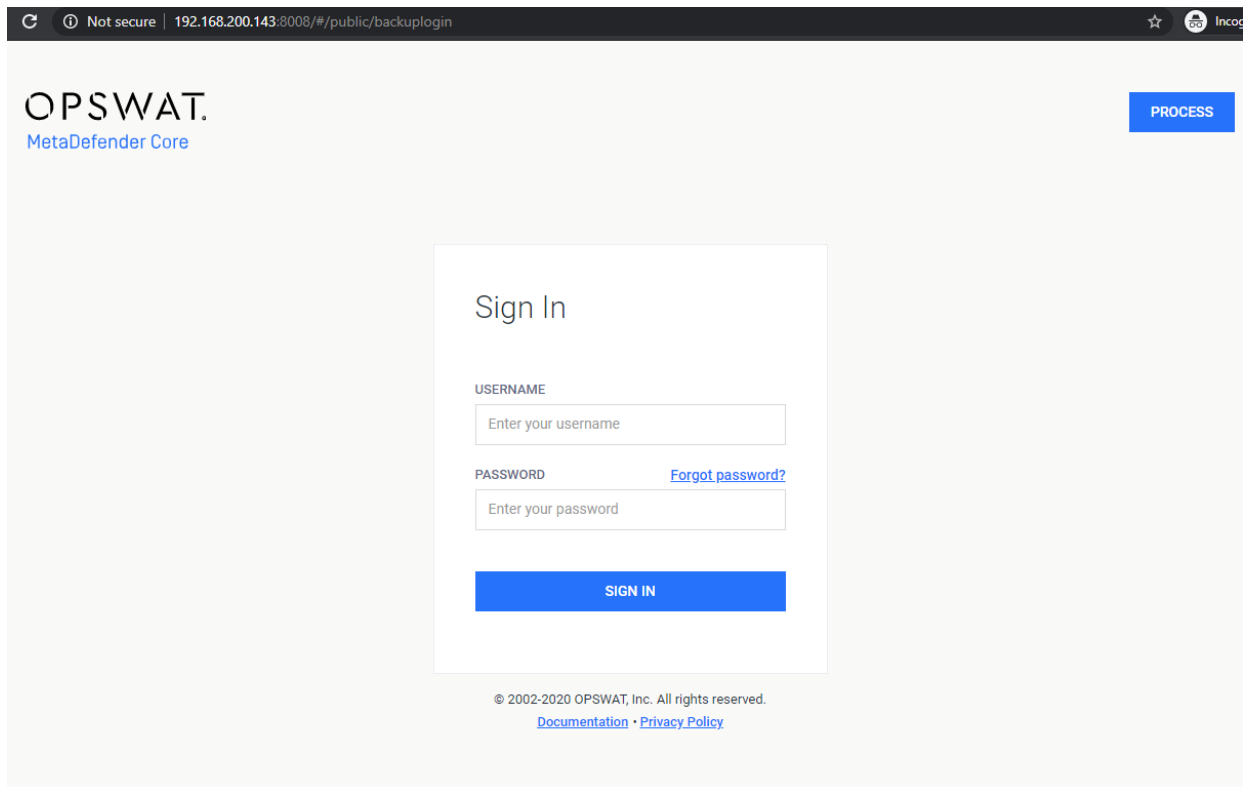
MetaDefender Core provides a backup login page to cover following circumstances:

- Mis-configured with SSO user directory, and now it locks everyone (including local admins themselves) out of MetaDefender Core management console access
- Provide local admin users an method to disable SSO authentication

URL: `<MetaDefender Core server address>:<port>/#/public/backuplogin`

For example: <http://192.168.200.143:8008/#/public/backuplogin>

Note: This URL is only available and accessible only when at least one SSO user directory enabled.



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 web console. The left sidebar contains navigation options: Dashboard, Process, Policies, Inventory, and Settings. Under 'Settings', 'Update Settings' is selected. The main content area includes a 'Source' section with radio buttons for 'INTERNET' (selected), 'FOLDER', and 'MANUAL'. Below this is the 'Automatic database updates' section with a horizontal scrollbar containing options from 15m to Off, with '4h' selected. The 'Update Pause' section is titled 'Updates are not applied during:' and includes a 'DAY OF WEEK' dropdown set to 'Monday - Friday' and a 'TIME PERIOD' field set to '08 : 00 TO 16 : 00'. A 'Delete' link is next to the time period. An 'Add rule' link is located below the time period. A 'SAVE SETTINGS' button is positioned in the top right corner of the settings area. The top navigation bar shows 'Help Center', 'NOT MANAGED', 'LOCAL/admin', and 'LOGOUT'. The bottom left of the sidebar shows the version '4.16.0' and 'License Expiration 2026-12-31'.

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 > Technologies**.

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 web console. On the left is a dark blue sidebar with navigation options: Dashboard, Process, Policies, Inventory, and Settings. The 'Settings' menu is expanded, showing 'Update Settings' as the active option, along with Data Retention, Security, User Management, License, Configuration, Password, and Email Configuration. At the bottom of the sidebar, the version '4.16.0' and 'License Expiration 2026-12-31' are shown. The main content area has a top navigation bar with 'Help Center', 'NOT MANAGED', a notification bell, 'LOCAL/admin', and 'LOGOUT'. The 'Update Settings' page features three radio buttons for 'Source': 'INTERNET', 'FOLDER' (selected), and 'MANUAL'. Below this is a text input field for 'Pick up updates from' containing the path 'C:/Program Files/OPSWAT/Metadefender Core/data/update_autoadd'. A checked checkbox labeled 'DELETE FILES AFTER IMPORT' is present. The 'Update Pause' section includes a dropdown for 'DAY OF WEEK' set to 'Monday - Friday' and a 'TIME PERIOD' field showing '08 : 00 TO 16 : 00' with a 'Delete' link. An 'Add rule' link is also visible. A blue 'SAVE SETTINGS' button is located in the top right corner of the main content area.

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 > Technologies**.

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 displays the 'Data Retention' settings page in the OPSWAT MetaDefender interface. The left sidebar shows the navigation menu with 'Settings' expanded and 'Data Retention' selected. The main content area is titled 'Data Retention' and includes a 'SAVE SETTINGS' button. Below the title, there are five sections, each with a sub-header and a dropdown menu for selecting a retention period:

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

The bottom of the sidebar shows the version '4.16.0' and the license expiration date '2026-12-31'.

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. Policy 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
- Deep CDR
 - Deep CDR configuration options
- Block files if sanitization fails
- Proactive Data Loss Prevention (Proactive DLP)
 - Proactive 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.

OPSWAT.
MetaDefender Core

Help Center

NOT MANAGED

LOCAL/admin

LOGOUT

Workflow Templates Management

ADD NEW WORKFLOW

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 wi...
Executables only	Selecting this template only executable files will be processed. All skipped files will be shown as 'not scanned' in the ...

4.18.0
License Expiration
2026-12-31

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.

ARCHIVE SCAN DEEP CDR PROACTIVE DLP MORE ▾

ENABLE ARCHIVE HANDLING ⓘ

MAX RECURSION LEVEL ⓘ

5

MAX NUMBER OF FILES EXTRACTED ⓘ

200

MAX TOTAL SIZE OF EXTRACTED FILES [IN MEGABYTES] ⓘ

200

HANDLE ARCHIVE EXTRACTION TASK AS FAILED ⓘ [REVERT TO DEFAULT](#)

INVALID FILE STRUCTURE

EXTRACTED PARTIALLY [REVERT TO DEFAULT](#)

OTHERS (DISK SPACE ISSUE, SYSTEM ERRORS, ETC.)

ENABLE SCAN OF ORIGINAL UNEXTRACTED ARCHIVE ⓘ

ENABLE EXTRACTION OF OFFICE DOCUMENTS ⓘ

TIMEOUT FOR ARCHIVE ANALYSIS [IN MINUTES]

3

SAVE CHANGES CANCEL

Archive

Blacklist/Whitelist

ⓘ Since MetaDefender Core 4.19.0, user is allowed to configure to exclude child extracted files from archive file type for being blacklisted.

Modify Rule

ARCHIVE SCAN DEEP CDR PROACTIVE DLP **BLACKLIST** ▾

ENABLE PROCESSING OF BLACKLISTED FILES ⓘ

BLACKLIST BY HASH

HASHES

[x] [+]

BLACKLIST BY FILETYPE [REVERT TO DEFAULT](#)

ADOBE FILES

ARCHIVE FILES

DISK IMAGE FILES

ENCRYPTED DOCUMENTS

EMAIL FILES

EXECUTABLE FILES

IMAGE FILES [REVERT TO DEFAULT](#)

BLACKLIST FILETYPES [REVERT TO DEFAULT](#)

TYPE IF BIGGER THAN

JPG 0 MB ALLOW IN ARCHIVE [x]

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.

Files can also be whitelisted by their checksums. For more information please see [7.2.4. Skip by hash](#) page.

Scan

NUMBER OF ACTIVE ANTI-MALWARE ENGINES: 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.

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

DETECT FILE TYPE MISMATCH: 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.

PER ENGINE TIMEOUT / EXTERNAL SCANNER TIMEOUT / GLOBAL SCAN TIMEOUT: 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.

SCAN FAILURE THRESHOLD: 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.

SUSPICIOUS DETECTED HANDLED AS: By enabled, you are able to decide if Suspicious result on any particular engine is considered as Infected or No Threat Found result, and it will take consideration into overall process result which also is constraint by threat detected threshold setting.

THREAT DETECTED THRESHOLD: When checked, this setting supports two configuration options **INFECTED LIMIT** and the **SUSPICIOUS LIMIT** when **SUSPICIOUS DETECTED HANDLED AS** is disabled, and its handling logic will be described as following:

- 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).

Nevertheless, if **SUSPICIOUS DETECTED HANDLED AS** is also enabled, regardless of handling as Infected or No Threat Found, **SUSPICIOUS LIMIT** setting are no longer taken into account. The following is the handling logic:

- If the **INFECTED LIMIT** is reached, the overall result will be always infected.
- Otherwise, the overall result will be the highest priority engine result (infected results are ignored).

ARCHIVE **SCAN** DEEP CDR PROACTIVE DLP 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

SUSPICIOUS DETECTED HANDLED AS Infected ▾

THREAT DETECTED THRESHOLD ⓘ

INFECTED LIMIT ⓘ

1

SUSPICIOUS LIMIT ⓘ

1

SAVE CHANGES **CANCEL**

Scan

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

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 <https://metadefender.opswat.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.

By default, MetaDefender Core allows files, where sanitization fails. This behavior can be overridden enabling "BLOCK FILES IF SANITIZATION FAILS OR TIMES OUT".

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 time frame, otherwise abort the conversion and latter means the number of times product should retry in case of a failed conversion.

When "DISTINGUISH PARTIAL ARCHIVE SANITIZATION RESULT" checked, MetaDefender Core will return "Partial Sanitization" processing result for Deep CDR when only some of child files in original archive files are sanitized successfully.

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

Result of sanitization can be either downloaded on the scan page or retrieved the data ID via REST. See [8.1.3.2. Fetch processing 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**.

ARCHIVE
SCAN
DEEP CDR
PROACTIVE DLP
MORE ▾

BLOCK FILES IF SANITIZATION FAILS OR TIMES OUT ⓘ

BLACKLIST UNSUPPORTED FILE TYPES ⓘ

ENABLE FOR ALL FILE TYPES ⓘ

DISTINGUISH PARTIAL ARCHIVE SANITIZATION RESULT ⓘ

RETAIN PASSWORD PROTECTION ON SUPPORTED ARCHIVE AND DOCUMENT FILES ⓘ

DOCUMENT FILES

 ADOBE PORTABLE DOCUMENT FORMAT (.PDF)

 MICROSOFT EXCEL 97-2003 WORKBOOK (.XLS)

 MICROSOFT EXCEL WORKBOOK (.XLSX)

 MICROSOFT POWERPOINT 97-2003 PRESENTATION(.PPT)

 MICROSOFT POWERPOINT PRESENTATION(.PPTX)

 MICROSOFT WORD 97-2003 DOCUMENT (.DOC)

 MICROSOFT WORD DOCUMENT (.DOCX)

ARCHIVE FILES

 ZIP ARCHIVE (.ZIP)

 7-ZIP COMPRESSED ARCHIVE (.7Z)

CONVERSION TIMEOUT [IN MINUTES] ⓘ

TIMEOUT FOR ARCHIVE SANITIZATION [IN MINUTES] ⓘ

Deep CDR

Deep CDR configuration options

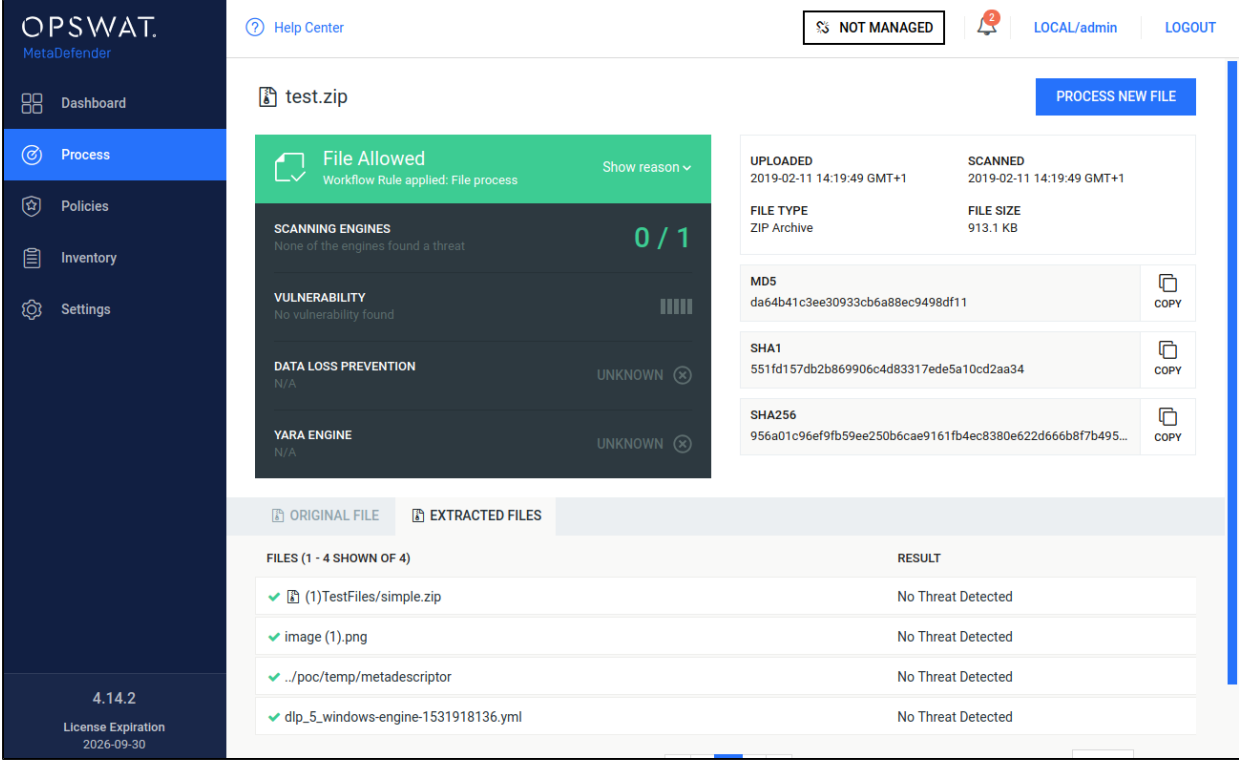
On the Technologies page, clicking on the line of the Proactive DLP engine then on the Settings text on the top right corner of the popup window, the configuration options for the Proactive DLP engine appear.

Deep CDR engine configuration

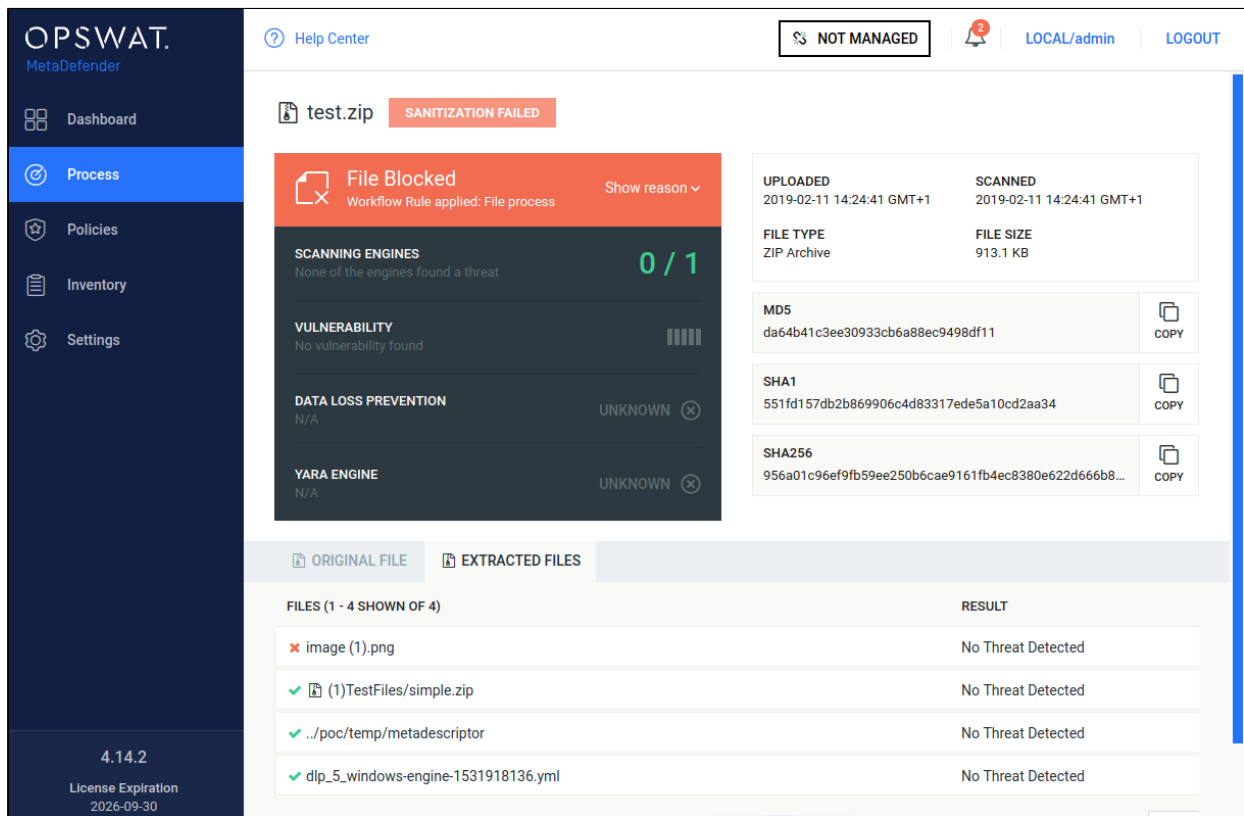
Block files if sanitization fails

By default, MetaDefender allows files, where sanitization fails.

For example: even if sanitization of an underlying element in a .zip file fails (sanitization is enabled for .png files in the examples below), the overall result (and the result of the .png file as well) is allowed by default:



Once "BLOCK FILES IF SANITIZATION FAILS OR TIMES OUT" is enabled, the overall and the individual result are blocked in case of a sanitization failure:



The sanitization failure of the zipped file is propagated to the .zip file level:

Proactive Data Loss Prevention (Proactive DLP)

For all information about features powered by Proactive DLP, please learn more at [Proactive DLP](#)

Proactive DLP

Proactive DLP configuration options

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

Proactive DLP engine configuration

Options:

- "Parse binary files": Choosing this option, sensitive data will be searched for in files that cannot be converted to text.

- "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.
- "Mask context": Mask sensitive information in context

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 following verdicts result in allowed status:

- No Threat Detected
- Skipped Clean
- Potentially Vulnerable File
- Yara Rule Matched

ARCHIVE
SCAN
DEEP CDR
PROACTIVE DLP
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

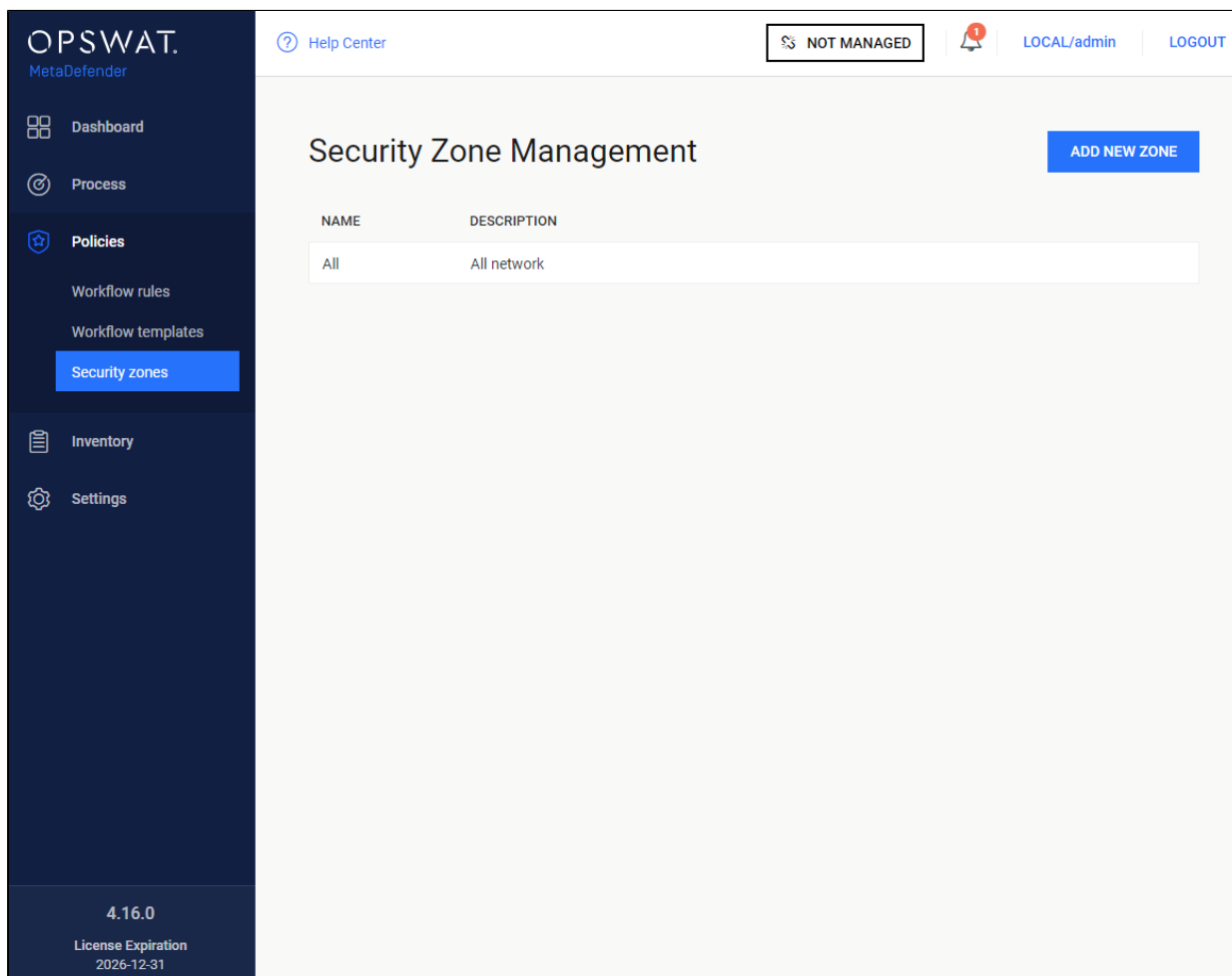
SAVE CHANGES

CANCEL

Advanced

3.6.3. Security zone configuration

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



Security zone

The following actions are available:

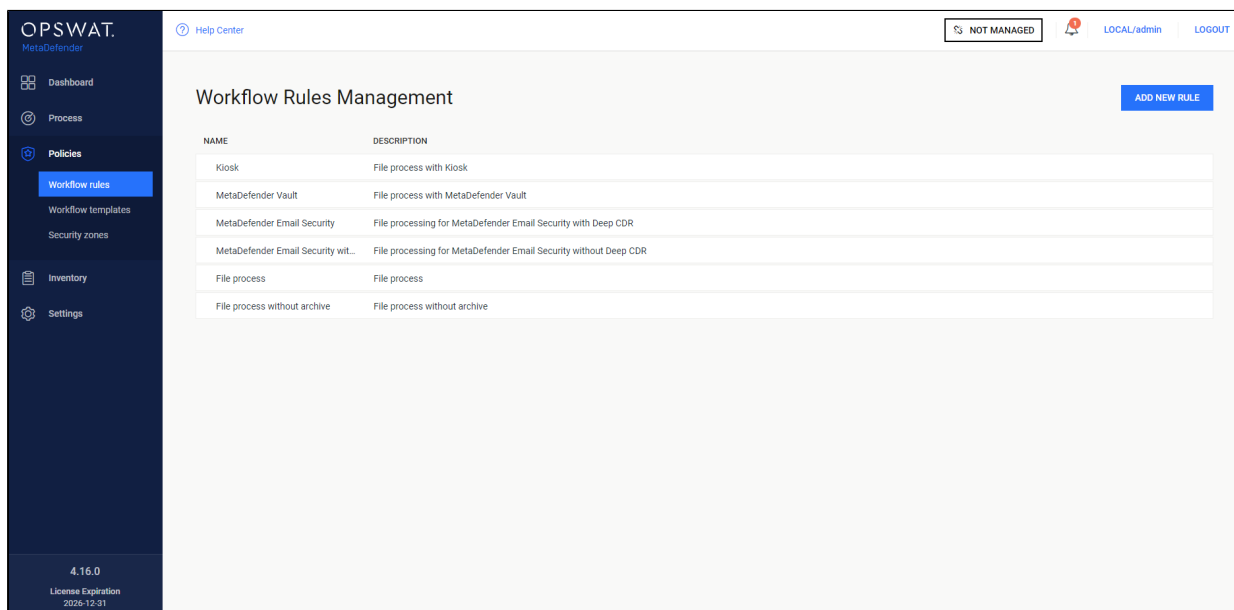
- new zones can be added
- existing zones can be viewed
- existing zones can be modified
- existing zones can be deleted

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.



Workflow rules

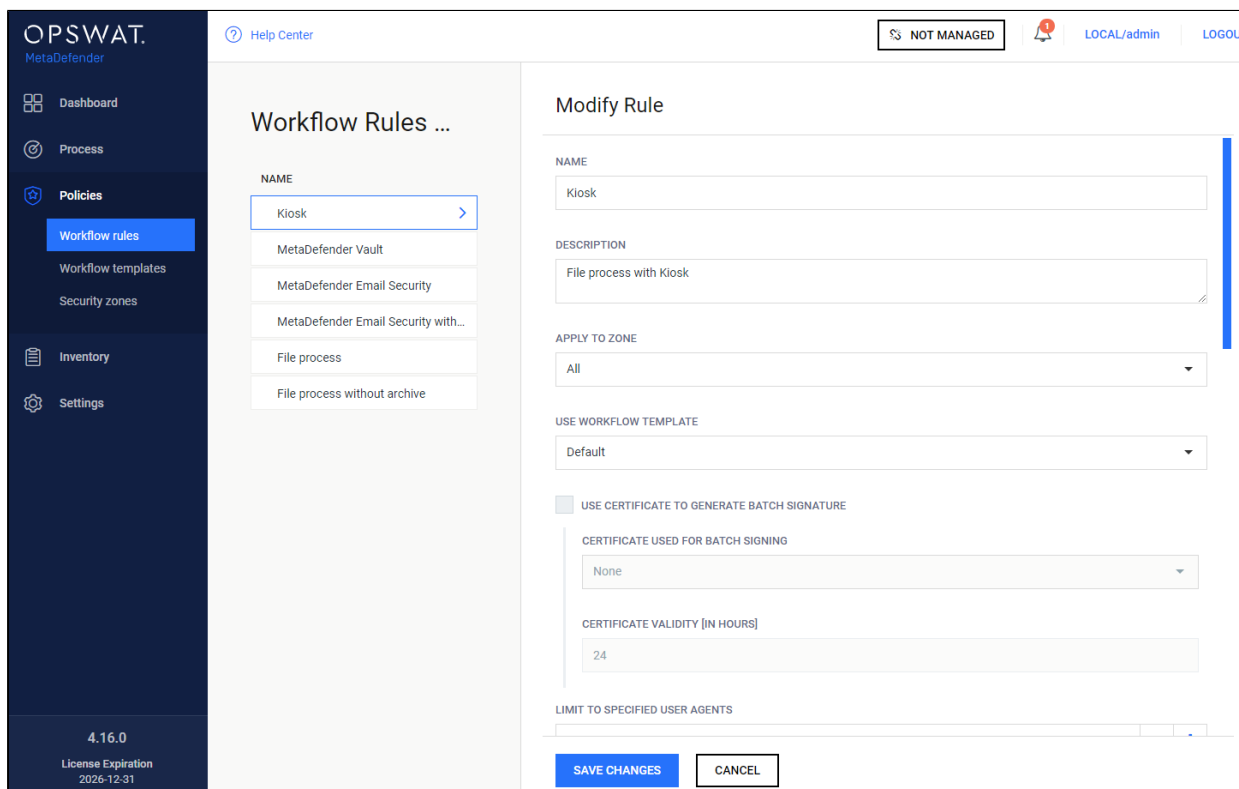
The following actions are available:

- 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.



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 testing this local scan feature, please note:

- Need to use "filepath" header while submitting a file via REST, see more at [Process a file](#)
- Core's web scan (localhost:8008) is not applicable tool to test because it does not allow you to customize the scan request's header

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](#)

File Allowed
Workflow Rule applied: File process
Show reason ▾

SCANNING ENGINES
None of the engines found a threat. 0 / 1

VULNERABILITY
No vulnerability found. ||||

DATA LOSS PREVENTION
N/A. UNKNOWN ⊗

YARA ENGINE
N/A. UNKNOWN ⊗

UPLOADED
2019-02-11 14:09:08 GMT+1

SCANNED
2019-02-11 14:09:08 GMT+1

FILE TYPE
UTF-8 Unicode text

FILE SIZE
32 B

MD5
be598f583c8b6d445188a47733de18d4 COPY

SHA1
d6b7c0551e0962a36fdd34e3baccf2bdacaf9ff7 COPY

SHA256
c232ca46e316ac097611e6d0b634141f3cfa41e2acc5d87793e76043e3fc1ec7 COPY

MULTISCANNING

ENGINE	SCAN TIME	DEFINITION DATE	RESULT
✓ ClamAV	3 ms	2019-02-10(a day ago)	No Threat Detected

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

file.txt PROCESS NEW FILE

File Allowed
Workflow Rule applied: File process
Show reason ▾

SCANNING ENGINES 0 / 1
None of the engines found a threat

VULNERABILITY UNKNOWN ||||
Unauthorized to view detailed scan result

DATA LOSS PREVENTION UNKNOWN ⊗
Unauthorized to view detailed scan result

YARA ENGINE UNKNOWN ⊗
Unauthorized to view detailed scan result

UPLOADED 2019-02-11 14:11:37 GMT+1	SCANNED 2019-02-11 14:11:37 GMT+1
FILE TYPE UTF-8 Unicode text	FILE SIZE 32 B

MD5 be598f583c8b6d445188a47733de18d4	COPY
SHA1 d6b7c0551e0962a36fdd34e3baccf2bdacaf9ff7	COPY
SHA256 c232ca46e316ac097611e6d0b634141f3cfa41e2acc5d87793e76043e3fc1ec7	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

File Allowed
Workflow Rule applied: File process
Show reason ▾

SCANNING ENGINES UNKNOWN
Unauthorized to view detailed scan result

VULNERABILITY UNKNOWN ||||
Unauthorized to view detailed scan result

DATA LOSS PREVENTION UNKNOWN ⊗
Unauthorized to view detailed scan result

YARA ENGINE UNKNOWN ⊗
Unauthorized to view detailed scan result

UPLOADED 2019-02-11 14:12:43 GMT+1	SCANNED N/A
FILE TYPE UTF-8 Unicode text	FILE SIZE 32 B

MD5 be598f583c8b6d445188a47733de18d4	COPY
SHA1 d6b7c0551e0962a36fdd34e3baccf2bdacaf9ff7	COPY
SHA256 c232ca46e316ac097611e6d0b634141f3cfa41e2acc5d87793e76043e3fc1ec7	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](#)
- [Send to MetaDefender Cloud](#)
 - [Quarantine settings](#)
 - [Operating MetaDefender Cloud integration](#)
 - [Threat intelligence details](#)
 - [Enabling MetaDefender Cloud integration](#)
 - [Troubleshooting](#)

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 quarantined files:

The screenshot displays the OPSWAT MetaDefender Quarantine interface. On the left is a dark sidebar with navigation links: Dashboard, Overview, Processing History, Quarantine (highlighted), Update History, and Config History. Below these are sections for Process, Policies, Inventory, and Settings. At the bottom of the sidebar, it shows version 4.14.0 and a license expiration date of 2026-12-31. The main content area has a top navigation bar with 'Help Center', 'NOT MANAGED', a notification bell, 'LOCAL/admin', and 'LOGOUT'. The 'Quarantine' section includes a 'Refresh' button, a search bar, and 'CLEANUP' and 'SETTINGS' buttons. Below this is a table with the following data:

<input checked="" type="checkbox"/>	FILENAME	SOURCE	TIME (GMT+1)	THREAT INTELLIGENCE	COMMENT
<input checked="" type="checkbox"/>	elf.zip	::1	2018-12-13 12:28:06		

At the bottom of the table, it indicates '1 - 1 SHOWN OF 1' and 'SHOW 20 per pages'.

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.
5.  Send to MetaDefender Cloud for threat intel. For details see the next section.

The *Send to MetaDefender Cloud*, the *Pin*, *Unpin* and *Delete* operations can also be performed in bulk using the check-boxes before the filenames and clicking the action icons above the file list.


Send to MetaDefender Cloud

Since MetaDefender version 4.14.0 MetaDefender Cloud integration is available.

Files in the quarantine can be uploaded to MetaDefender Cloud to get threat intelligence on them.

This feature requires the [Threat Intelligence technology to be licensed, and enabled](#).

Quarantine items may be sent to MetaDefender Cloud:

1. Manually using the  [Send to MetaDefender Cloud function](#), or
2. Automatically, driven by the configuration under [Quarantine settings](#).

Quarantine settings

To edit quarantine settings, click SETTINGS in **Dashboard > Quarantine**. The following options are available:

1. AUTOMATICALLY SEND ITEMS TO METADEFENDER CLOUD: If enabled, all new quarantine items will be uploaded to MetaDefender Cloud for threat intelligence information.
 - a. CHECK QUARANTINE FOR NEW ITEMS TO SEND: The frequency (in seconds) to check for new quarantine items to upload to MetaDefender Cloud.
2. RESULT POLLING: Once a quarantine item is uploaded to MetaDefender Cloud, MetaDefender must poll the Cloud for results. The polling frequency (in seconds) can be set here.

Quarantine settings

AUTOMATICALLY SEND ITEMS TO METADEFENDER CLOUD

CHECK QUARANTINE FOR NEW ITEMS TO SEND

Frequency in seconds

60

RESULT POLLING

Frequency in seconds

5

SAVE
CANCEL

Operating MetaDefender Cloud integration

While a quarantine item is uploading to MetaDefender Cloud (either manually, or automatically), the THREAT INTELLIGENCE status is set Uploading:

<input checked="" type="checkbox"/>	FILENAME	SOURCE	TIME (GMT+1)	THREAT INTELLIGENCE	COMMENT
<input checked="" type="checkbox"/>	elf.zip	::1	2018-12-13 12:28:06	Uploading	


When the upload is complete and MetaDefender waits for the results (and does the polling), the THREAT INTELLIGENCE field shows the processing progress:

<input type="checkbox"/>	FILENAME	SOURCE	TIME (GMT+1)	THREAT INTELLIGENCE	COMMENT
<input checked="" type="checkbox"/>	elf.zip	::1	2018-12-13 12:28:06	60%	

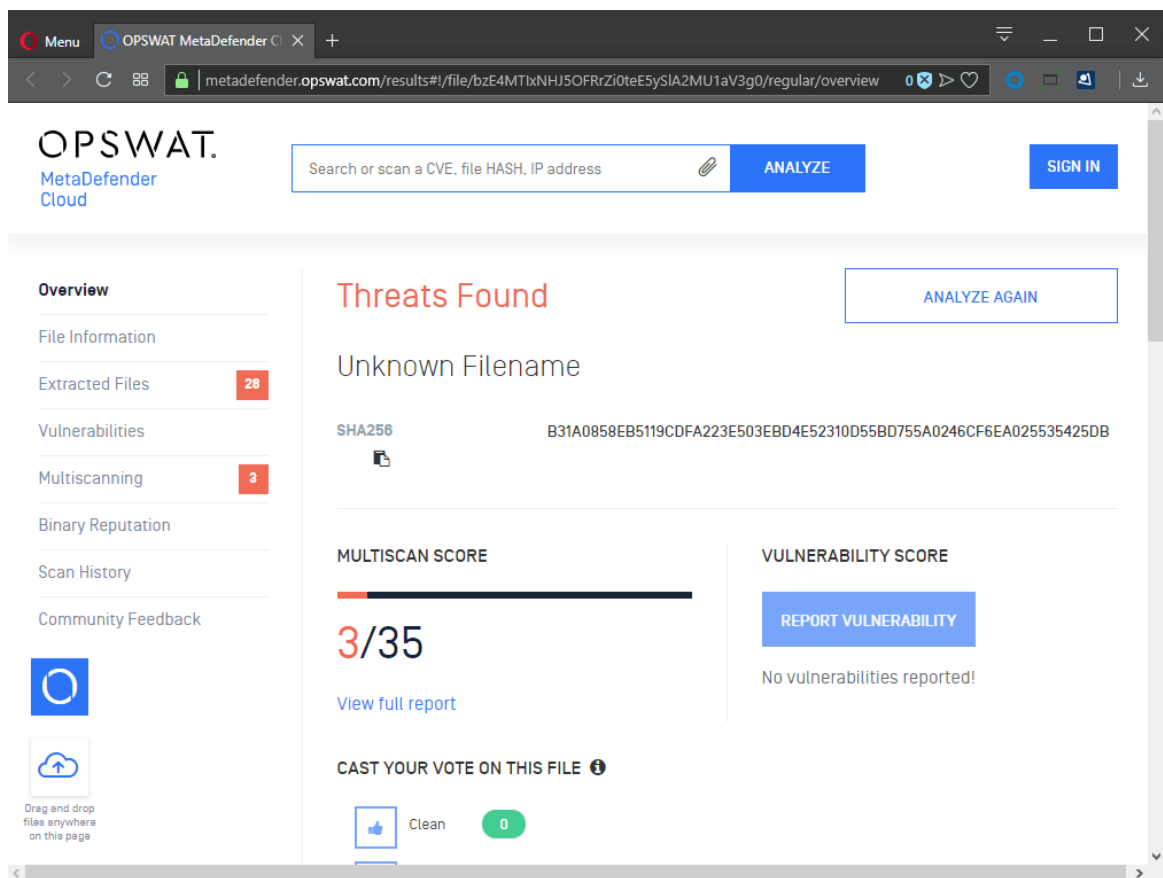
When the scan is complete on the Cloud side and MetaDefender got them, the results will be shown in the THREAT INTELLIGENCE field:

<input type="checkbox"/>	FILENAME	SOURCE	TIME (GMT+1)	THREAT INTELLIGENCE	COMMENT
<input checked="" type="checkbox"/>	elf.zip	::1	2018-12-13 12:28:06	Infected	

Threat intelligence details

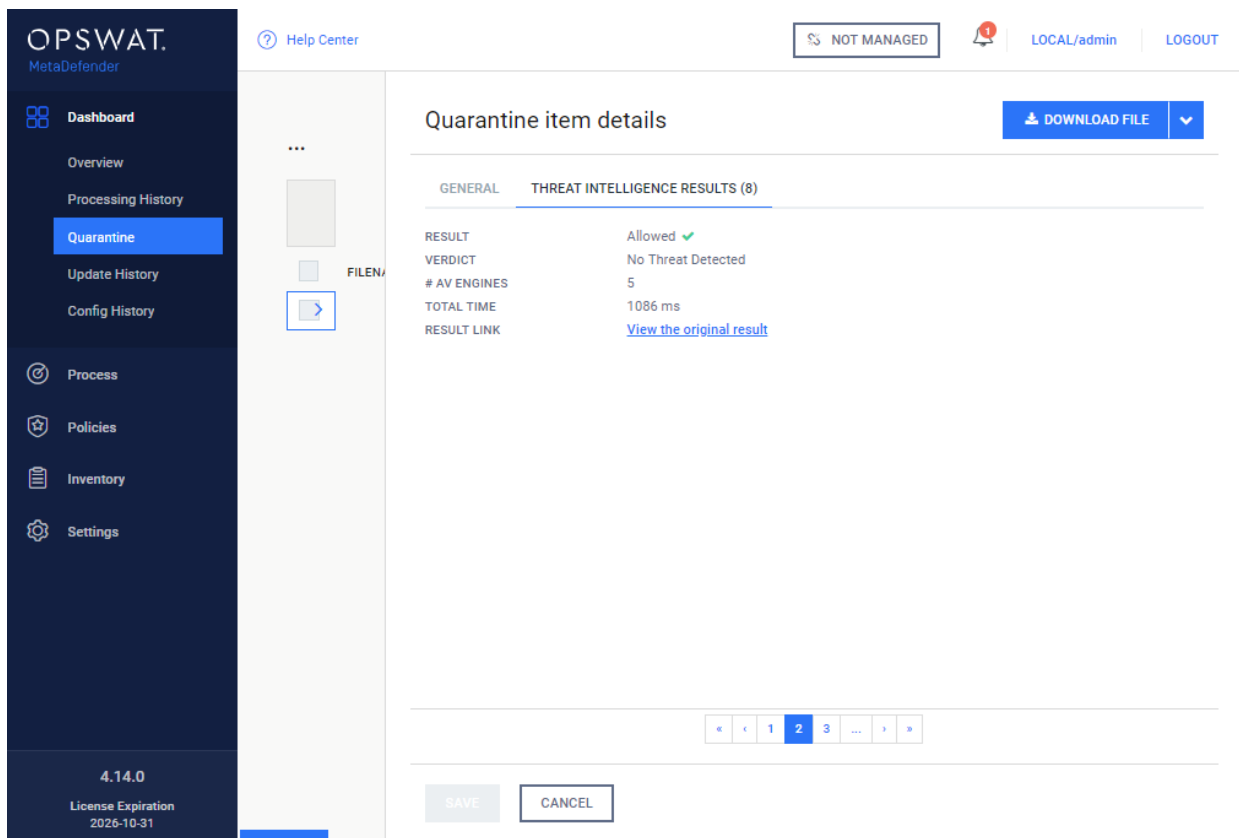
Clicking the  *Show details* function, the *Quarantine item details* view is shown. Clicking the THREAT INTELLIGENCE RESULTS tab, further details from MetaDefender Cloud are shown:

1. RESULT: Processing summary if the entry was blocked or allowed.
2. VERDICT: A more verbose details about the processing results.
3. AV ENGINES: Number of anti-virus engines that were used for scanning this item.
4. TOTAL TIME: Total processing time of this item for this scan.
5. RESULT LINK: Link to the processing results on MetaDefender Cloud.



The screenshot displays the OPSWAT MetaDefender Cloud interface. At the top, there is a search bar with the text "Search or scan a CVE, file HASH, IP address" and an "ANALYZE" button. A "SIGN IN" button is located in the top right corner. The main content area is divided into a left sidebar and a main panel. The sidebar includes sections for "Overview", "File Information", "Extracted Files" (with a red badge showing "28"), "Vulnerabilities", "Multiscanning" (with a red badge showing "3"), "Binary Reputation", "Scan History", and "Community Feedback". The main panel features a "Threats Found" section with a red heading and an "ANALYZE AGAIN" button. Below this, the file name "Unknown Filename" is displayed, along with its SHA256 hash: "B31A0858EB5119CDA223E503EBD4E52310D55BD755A0246CF6EA025535425DB". A "MULTISCAN SCORE" section shows a progress bar and the score "3/35", with a "View full report" link. A "VULNERABILITY SCORE" section includes a "REPORT VULNERABILITY" button and the text "No vulnerabilities reported!". At the bottom, there is a "CAST YOUR VOTE ON THIS FILE" section with a thumbs-up icon, the word "Clean", and a green badge showing "0".

If this quarantine item was uploaded to the Cloud multiple times, then there will be multiple THREAT INTELLIGENCE RESULTS pages in the tab.



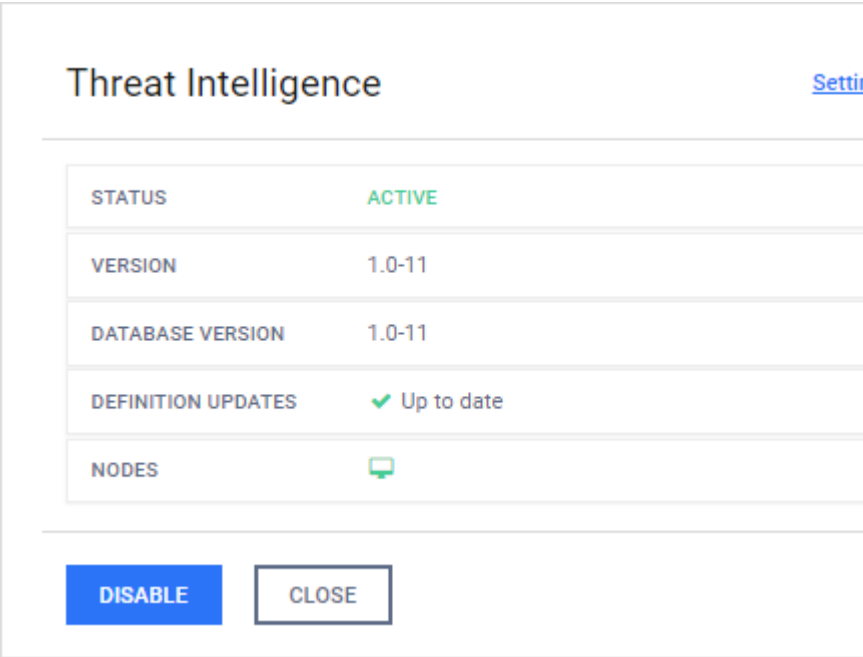
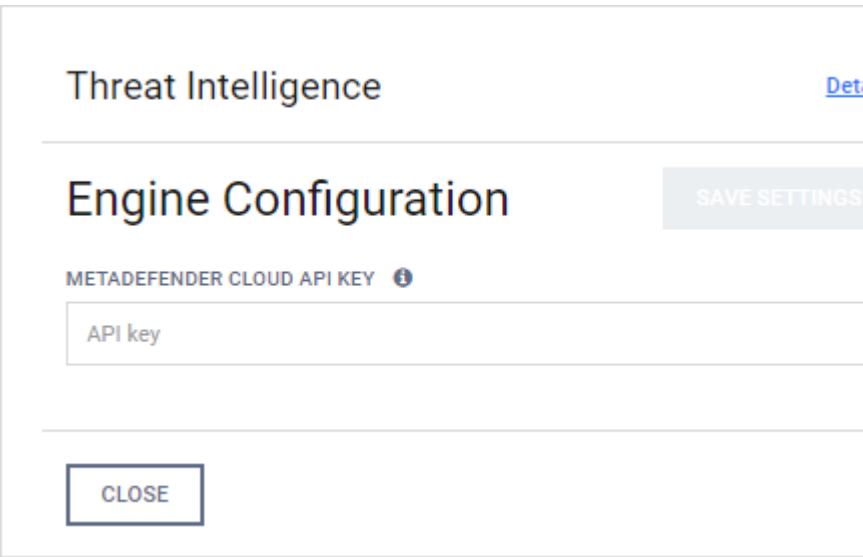
Enabling MetaDefender Cloud integration

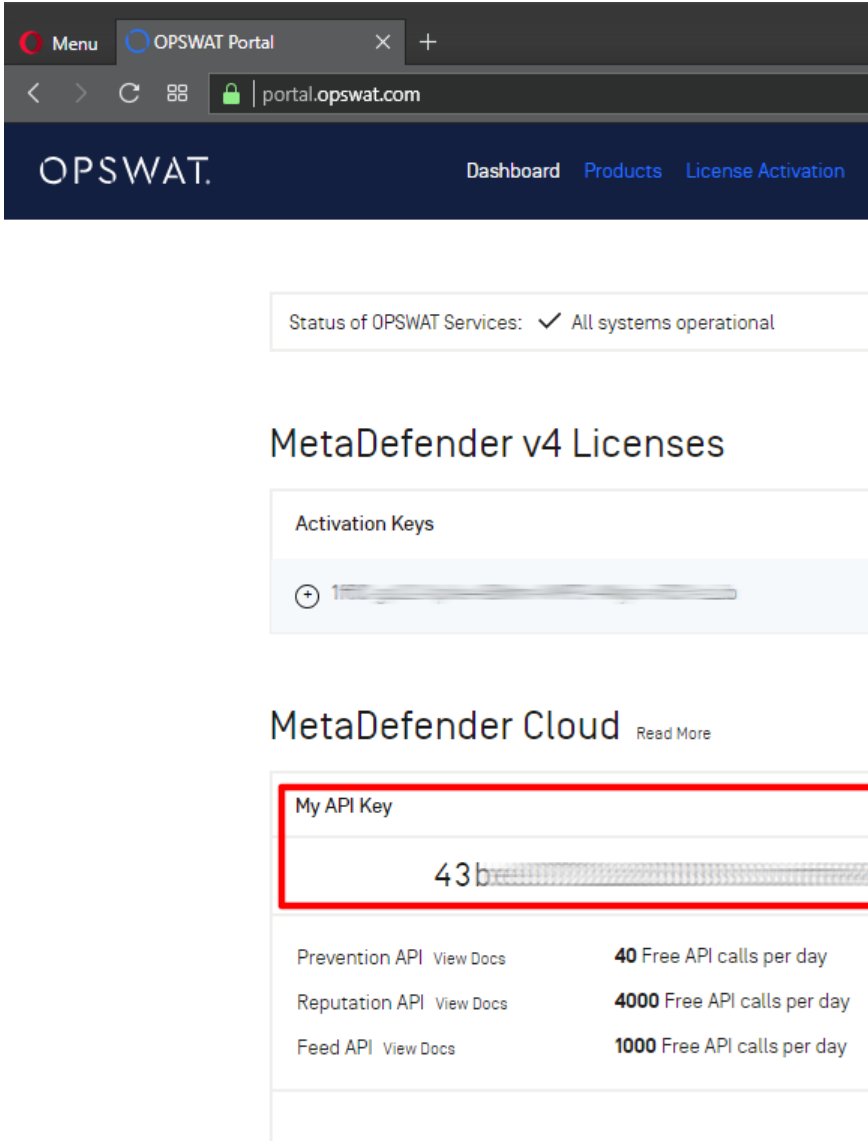
MetaDefender Cloud integration requires the *Threat Intelligence* technology to be licensed, and enabled under **Inventory > Technologies**:

Unless the *Threat Intelligence* technology is enabled, Cloud upload attempts will give *Unavailable* result:

<input type="checkbox"/>	FILENAME	SOURCE	TIME (GMT+1)	THREAT INTELLIGENCE	COMMENT
<input type="checkbox"/>	karoly.arnhoffer@opswat.com-Enhanc...	::1	2018-12-13 12:48:52	Unavailable	

Step	Description	Screenshot
1	1. Click on the <i>Threat Intelligence</i> entry in the <i>Technologies</i> list, the <i>Threat</i>	

Step	Description	Screenshot
	<p><i>Intelligence</i> dialog opens.</p>	
2	<p>Click on the <i>Settings</i> link, the <i>Engine Configuration</i> dialog opens</p>	
3	<p>Provide the METADEFENDER CLOUD API KEY value. The API key may be obtained from the OPSWAT portal.</p>	

Step	Description	Screenshot								
		 <p>The screenshot shows the OPSWAT Portal dashboard. At the top, there is a navigation bar with the OPSWAT logo and links for Dashboard, Products, and License Activation. Below the navigation bar, a status box indicates "Status of OPSWAT Services: ✓ All systems operational". The main content area features a section for "MetaDefender v4 Licenses" with a sub-section for "Activation Keys" showing one key. Below this is a section for "MetaDefender Cloud" with a "Read More" link. A red box highlights the "My API Key" field, which contains the value "43b...". Below the API key, there is a table listing API endpoints and their free call limits:</p> <table border="1"> <thead> <tr> <th>API Endpoint</th> <th>Free API calls per day</th> </tr> </thead> <tbody> <tr> <td>Prevention API View Docs</td> <td>40</td> </tr> <tr> <td>Reputation API View Docs</td> <td>4000</td> </tr> <tr> <td>Feed API View Docs</td> <td>1000</td> </tr> </tbody> </table>	API Endpoint	Free API calls per day	Prevention API View Docs	40	Reputation API View Docs	4000	Feed API View Docs	1000
API Endpoint	Free API calls per day									
Prevention API View Docs	40									
Reputation API View Docs	4000									
Feed API View Docs	1000									
4	Click SAVE SETTINGS to save the engine configuration.									

Step	Description	Screenshot

Troubleshooting

Symptom

MetaDefender Cloud upload attempts give *Unavailable* result.

<input checked="" type="checkbox"/>	FILENAME	SOURCE	TIME (GMT+1)	THREAT INTELLIGENCE
<input checked="" type="checkbox"/>	elf.zip	::1	2018-12-14 11:11:44	Unavailable

Symptom

MetaDefender Cloud upload attempts give *Add the API key for cloud analysis* result.

<input type="checkbox"/>	FILENAME	SOURCE	TIME (GMT+1)	THREAT INTELLIGENCE
<input checked="" type="checkbox"/>	elf.zip	::1	2018-12-13 12:28:06	✘ Add the API key for

MetaDefender Cloud upload attempts give *API calls per day limit reached* result.

<input type="checkbox"/>	FILENAME	SOURCE	TIME (GMT+1)	THREAT INTELLIGENCE
<input checked="" type="checkbox"/>	elf.zip	::1	2018-12-13 12:28:06	✘ AFI calls per day

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 Log message format](#)
- [3.7.3 Syslog message format](#)
- [3.7.4 Error Message Description Table](#)

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 Log message format

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] 2019.07.02 05:25:27.115: (core.workflow) Processing finished, node=':1076', user='LOCAL/admin', workflow_id='lms::workflow::WorkflowExecutor(0x214b02a8f60)', dataId='702a2230dd0d44de9bd773bccfe472a9', fileName='TermUtil.class', sha256sum='07aca175cc8a9f40819a47f6b5f809404bae8d31cf16e70d0a182c413ab39c98', blocked='false', blocked_reason='', overallResult='No Threat Detected', threatFoundCount='0', embeddedObjectsWithThreat='0', totalResultCount='3', threatDetectedBy='', threatName='', ruleName='File process', source='::1' [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 - Learn more at [3.7.4 Error Message Description Table](#)

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.

3.7.3 Syslog message format

MetaDefender Core supports to send CEF (Common Event Format) syslog message style

Remote Syslog

```
[Local Timestamp] [Source IP Address] [UTC Timestamp] [Hostname]
[CEF:Version|Device Vendor|Device Product|Device Version|Signature
ID|Name|Severity|Extension]
```

For example:

```
Jun 24 14:33:18 192.168.200.223 2019-06-24T14:33:19+07:00
OPSWATPC CEF:0|OPSWAT|MSCL|4.16.0|core.network|MSCL[7548] New
maximum agent count is set|2|maxAgentCount='1' msgid=665
```

Prefix field	Sample value	Description
Local timestamp	Jun 24 14:33:18	
IP address	192.168.200.223	Source IP address ver. 4
UTC timestamp	2019-06-24T14:33:19+07:00	
Hostname	OPSWATPC	
CEF: Version	CEF:0	Version 0
Device Vendor	OPSWAT	
Device Product	MSCL	MSCL = MetaDefender Core on Linux MSCW = MetaDefender Core on Windows
Device Version	4.16.0	MetaDefender Core version
Signature ID	core.network	For example: <ul style="list-style-type: none"> • core.network: Component "network" on "Core" module • agent.engines: Component "engines" on "Node" • common.update: Component "update" on common module shared by all modules
Name	MSCL[7548] New maximum agent count is set	Subject of log message <ul style="list-style-type: none"> • MSCL[7548] = MetaDefender Core on Linux ["ometascan" process id = 7548] • ometascan-node[455] = MetaDefender Core Node ["ometascan-node" process id = 455]

Prefix field	Sample value	Description
Severity	2	Log level <ul style="list-style-type: none"> • DUMP (0): The most verbose severity level, these entries are for debuggers only. • DEBUG (1): Debuggers severity level, mostly used by support issues. • INFO (2): Information from the software, such as scan results. • WARNING (3): A problem occurred needs investigation and OPSWAT support must be contacted, however the product is supposed to be operational. • ERROR (4): Software error happened, please contact support if the issue is persist. Software functionality may be downgraded in these cases.
Extension	maxAgentCount='1' msgid=665	To learn more about msgid (message ID): 3.7.4 Error Message Description Table

Local Syslog

```
[Local Timestamp] [Hostname] [CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension]
```

For example:

```
Jun 24 14:33:18 OPSWATPC CEF:0|OPSWAT|MSCL|4.16.0|core.network|MSCL[7548] New maximum agent count is set|2|maxAgentCount='1' msgid=665
```

Prefix field	Sample value	Description
Timestamp	Jun 24 14:33:18	

Prefix field	Sample value	Description
Hostname	OPSWATPC	
CEF: Version	CEF:0	Version 0
Device Vendor	OPSWAT	
Device Product	MSCL	MSCL = MetaDefender Core on Linux MSCW = MetaDefender Core on Windows
Device Version	4.16.0	MetaDefender Core version
Signature ID	core.network	For example: <ul style="list-style-type: none"> • core.network: Component "network" on "Core" module • agent.engines: Component "engines" on "Node" • common.update: Component "update" on common module shared by all modules
Name	MSCL[7548] New maximum agent count is set	Subject of log message <ul style="list-style-type: none"> • MSCL[7548] = MetaDefender Core on Linux ["ometascan" process id = 7548] • ometascan-node[455] = MetaDefender Core Node ["ometascan-node" process id = 455]
Severity	2	Log level <ul style="list-style-type: none"> • DUMP (0): The most verbose severity level, these entries are for debuggers only. • DEBUG (1): Debuggers severity level, mostly used by support issues. • INFO (2): Information from the software, such as scan results.

Prefix field	Sample value	Description
		<ul style="list-style-type: none"> • WARNING (3): A problem occurred needs investigation and OPSWAT support must be contacted, however the product is supposed to be operational. • ERROR (4): Software error happened, please contact support if the issue is persist. Software functionality may be downgraded in these cases.
Extension	maxAgentCount='1' msgid=665	To learn more about msgid (message ID): 3.7.4 Error Message Description Table

3.7.4 Error Message Description Table

Every log entry on MetaDefender Core always comes with a message ID number which is an unique identifier for that log entry ([3.7.2 Log message format](#))

For example:

```
[WARNING] 2019.07.02 05:25:27.749: (core.workflow) Can not send
extract task, id='lms::workflow::WorkflowExecutor(0x214af499d00)',
node=':1076', block='ExtractBlock' [msgid: 3059]
```

Then message ID associated to that message would be 3059.

For warning/error message type, besides the message itself (e.g. *Can not send extract task, id='lms::workflow::WorkflowExecutor(0x214af499d00)', node=':1076', block='ExtractBlock'*), using message ID (e.g. 3059) can help reveal more information about that warning/error.

Following is the list of error message description (only applicable to warning/error message type).



Disclaim:

- This list is auto generated and should be updated accordingly with MetaDefender Core upgrade.
- Should be used as reference only, for a complete issue troubleshooting guidance, please reach out to OPSWAT Support.

Error message ID	Error description
8	Unknown error occurred in the daemon/service.
16	Error happened in the communication
21	Can't connect to the server
26	Can't send a message to the target, it's probably disconnected
28	The connection is timed out
73	Error happened in the communication
101	Error happened in the communication
113	Invalid file deletion
130	Unknown error occurred in the daemon/service.
149	Unable to gather OS information
162	Sending scan requests failed
166	File given can not be opened
169	REST frontend timeout.
176	Agent status is not available
179	Agent status is unavailable
181	REST response format is invalid
217	Engine name unreachable
218	Engine definition unreachable

Error message ID	Error description
219	Engine leak
220	Engine leak
221	Engine leak
222	Engine leak
231	Engine error
246	Can't transfer file, data channel is not open
248	File transfer response error
250	Error transferring file
252	Error in package staging process
253	Error in package staging process
254	Error in package staging process
255	Error in package staging process
256	Error in package staging process
275	Email sending error
277	Email sending error
282	Invalid main update descriptor
283	Invalid package descriptor
285	Invalid file downloaded

Error message ID	Error description
297	Invalid state option given in GetEngineInfoBlock
303	Downloaded package is not complete
304	Downloaded package is invalid
305	Downloaded package is invalid
306	Downloaded package is invalid
307	Downloaded package is invalid
308	Downloaded package is invalid
314	Agent with identifier is unavailable
319	Can not open downloaded package
320	Downloaded package is invalid
321	No respond from agent
325	No respond from agent
326	Error loading database
330	Error in uploaded descriptor
338	No respond from agent
341	Error in getting update package
342	Error in getting update package
343	Error in package staging process

Error message ID	Error description
355	Invalid reference to user data
379	Database error: user query
382	Database error: user query
383	Database error: users query
385	Database error: role query
386	Database error: roles query
425	Invalid state option given in GetDatabaseInfoBlock
428	Error in checking package updatable
431	Error validating engine
439	Agent status is not available
453	Agent with identifier is unavailable
459	No respond from agent
465	Database error: getting scan request
473	Agent does not have specific engine
474	Downloaded packagedescriptor is invalid
485	Error while downloading files from update server
486	Invalid certificate found while downloading files from update server
495	File missing during validation

Error message ID	Error description
496	File size mismatch during validation
497	SSL errors for https://update.dl.opswat.com
506	File type checking timed out
520	Could not trigger update
523	Invalid file reference
541	Invalid type reference for entry
542	Invalid type reference for entry
543	Invalid type reference for entry
545	Invalid type reference for entry
547	Invalid type reference for entry
551	Internal error occurred during the program run
552	System error occurred during the program run
553	Unknown error occurred during the program run
554	Can't create resource file
556	HTTP redirection count exceeded limit
563	Database error: get linked extracts
598	Invalid file reference
599	Engine type unreachable

Error message ID	Error description
602	Download timed out.
611	Can't remove the downloaded zip archive
613	File extraction failed while updating
620	Invalid content received for update
621	Can't download file for update
624	File open file for update
628	Can't read file to validate it's content
639	No respond from agent
641	Error in getting package state information
642	Error in checking package updatable
652	License is invalid or not containing licensed_engines
657	No activation_key is received
658	Invalid activation option value
659	Activation error
662	Connected agent count reached the license limit
663	License is invalid or not containing max_agent_count
670	Package download failed
678	Could not upload file

Error message ID	Error description
679	Update could not be applied
686	Trying to load engine which is not installed to the agent
687	Trying to load engine which is corrupt
708	Engine load failed
711	Updated engine can't find eicar file as threat
716	Installing engine resulted in error
718	Installing database resulted in error
721	Error in install database
722	Installing database resulted in error
723	File is missing for update in agent
727	Error loading engine
732	Error installing engine, unable to copy descriptor file
734	After updating the database the package descriptor is invalid
736	Error in prepare database
737	Error installing engine, unable to copy descriptor file
749	Engine process crashed
802	Could not create path to save updates
808	Could not save package, skipping

Error message ID	Error description
809	Could not save package, skipping
812	Could not save package, skipping
813	Could not save package, skipping
814	Error creating database package
816	Error creating database package
819	Error creating database package
820	Error creating database package
827	Database error: retrieving audit log
828	Database error: inserting audit log
829	Database error: retrieving audit log count
833	Exception during operation
835	Could not trigger update
837	Could not trigger update
838	Update package download failed
842	Error adding license information to engine descriptor
843	Could not copy legacy package, skipping
844	Could not save legacy package, skipping
846	Packagedescriptor could not be read

Error message ID	Error description
847	Could not read descriptor file
848	Could not write descriptor file
852	Error opening CERT file
854	No legacy database wrapper package present
855	Could not write licenses to database descriptor
858	Metadescriptor could contains tampered information, abort processing
861	Can't process new licence information
862	Error in package staging process
863	Can't initialize source instance
864	Can't create resource file
865	Can't send data to agent
866	Can't transfer file, can't open resource file
868	Can't get temporary file name
869	Can not find data channel
870	Can not load engine shared library
871	Cannot create temporary directory for engine files
892	Could not export legacy package, skipping

Error message ID	Error description
931	Unexpected network reply arrived
945	Error in getting update package by state
947	Error receiving data, request log from customer
948	Not enough disk space to export package(s)
949	Not enough disk space to export package(s)
950	Not enough disk space to export package(s)
951	Error sending data to agent, request log from customer
952	Not enough disk space to apply update package on agent
953	Not enough free disk space for agent to handle updates
955	Error sending data to agent, request log from customer
969	Creating of symbolic link has failed
970	Error in prepare database
978	Could not establish remote communication
979	Could not establish local communication
981	Deactivation error
995	Activation key not found in license
996	Stored license is invalid
997	Invalid activation option value

Error message ID	Error description
998	Automatic reactivation error
999	Error saving license information
1002	License activation error
1003	Error during license activation
1009	Network error occurred while trying to lookup hash
1010	Invalid response retrieved from server
1017	Due to errors in previous requests, disabling hash lookup for a given interval
1019	Too many timeout error occurred in a short period of time
1025	Error occurred in engine process
1027	Issue occurred while transferring file to agent
1030	Invalid update folder found
1031	Error Sending hashes message, request log from customer
1037	Engine capabilities unreachable
1042	Engine's descriptor is invalid
1043	Could not open update archive
1046	Custom engine task starting timed out
1047	Custom engine task finishing timed out

Error message ID	Error description
1050	Issue with agent, see troubleshooting guide
1051	Engine issue on agent
1052	Error in installing custom engine, engine with id not found
1053	Issue happened with engine
1055	Agent with identifier is unavailable
1057	No respond from agent for custom engine installation
1058	Error validating engine, no engine descriptor found
1059	Error validating engine, invalid engine descriptor found
1064	Not handling file as local, not must be an issue
1068	Could not apply updates from pickup folder
1081	Could not create folder for pickup
1095	Testing engine failed
1096	File transfer response error
1100	Error in package staging process
1126	Could not create quarantine database
1134	Error in quarantine database
1135	Error in quarantine database
1136	No such file to remove

Error message ID	Error description
1141	Error in quarantine database
1142	Error in quarantine database
1144	Error in quarantine database
1147	Error reading quarantine file
1148	Download aborted
1151	Error adding file to quarantine
1152	Error adding data chunk to quarantine file
1153	Error receiving file data, removing file from sanitized storage
1154	Given path is not absolute
1155	Could not create storage folder
1156	File storage path is not writable
1157	No owner given
1158	Id is not specified
1159	Id is too short
1160	Could not create directory
1161	Could not create directory
1163	Error opening file
1164	Could not write file

Error message ID	Error description
1165	File id is not specified
1166	No such file found
1167	Could not remove file
1168	File id or owner is not specified
1169	No such file to finalize
1170	Error sending file data to core
1171	Can't request file, data channel is not open
1173	Could not request file from agent
1174	Can't request file from agent
1176	Processing file from agent encountered an error
1177	Could not read salt value
1178	Could not read salt value
1179	Error creating salt file
1180	Error generating salt value for quarantine
1182	Error occurred quarantining file
1183	File not found in quarantine
1184	Same owner was already reading another file
1185	Error reading file in quarantine

Error message ID	Error description
1186	Error writing data to quarantined file
1188	Could not finalize quarantined file
1190	No file with given id is present for removal
1191	Could not remove file from quarantine
1192	Could not remove file from quarantine
1193	Could not gather quarantine information
1196	Database error: user query
1198	Error parsing disabled times information
1201	See reason for more information about the reason
1204	Can't open metadescriptor file for writing
1220	The certificate chain maybe invalid
1221	Info about the certificates in the chain
1226	Vulnerability lookup timed out
1227	Error in checking package updatable
1229	Error receiving file data, removing file from quarantine
1230	Engine capabilities unreachable
1231	Engine leak
1232	Engine capabilities unreachable

Error message ID	Error description
1233	Engine leak
1235	Could not create sanitized database
1252	Error in sanitize database
1253	Error in sanitize database
1254	Error getting sanitized files
1258	Error querying sanitized files
1266	Error occurred adding file to sanitized storage
1267	File not found in sanitized storage
1268	Same owner was already reading another file
1269	Error reading file in sanitized storage
1270	Error writing data to sanitized file
1272	Could not finalize sanitized file
1277	Could not gather sanitized files information
1280	Error reading quarantine file
1281	Download aborted
1284	Wrong enabled template in sanitize block
1285	Wrong convert template in sanitize block
1287	Error in sanitization, retries emptied

Error message ID	Error description
1290	Error adding file to sanitized storage
1291	Error adding data chunk to sanitized file
1295	Error saving sanitized file
1305	Database's descriptor is invalid
1603	Error in package staging process
1604	Filestore unreachable
1605	Could not upload file
1606	Could not upload file
1607	File not exist to load schema from
1608	Schema is not a proper JSON
1609	Schema format is invalid
1670	Error while checking if package is md.com only
1677	File not exist to load default value from
1678	Default value file is not a proper JSON
1679	Default value file format is invalid
1693	Database error occurred
1695	Database error occurred
1696	Database error occurred

Error message ID	Error description
1697	Database error occurred
1699	Unable to apply patch to revert configuration
1700	Reverted configuration is invalid, hash not matching
1701	Database error occurred
1702	Unable to load configuration from default values
1703	Unable to save configuration from default values
1704	Default value file is not a proper JSON
1705	Default value file format is invalid
1706	Unable to load configuration
1711	Error when sending bytes through socket
1712	Default value file is not a proper JSON
1740	Error reserving data id
1741	Process local file encountered an error
1742	No data id was set in HandleLocalFileBlock
1777	Unable to save new configuration
1781	Database error: requesting export on empty processing history
1782	Removing engine folder failed
1783	Removing engine folder failed

Error message ID	Error description
1784	Removing engine folder failed
1785	Removing folder failed
1787	Removing invalid update folder failed
1790	Removing folder failed
1791	Removing folder failed
1792	Removing package folder failed
1793	Removing database folder failed
1794	Removing folder failed
1795	Removing folder failed
1798	Removing downloading packages failed
1801	Error when selecting from downloaded
1803	Error when deleting from downloaded
1804	No result when selecting from downloaded
1805	Removing engine folder failed
1825	Database error: role query
1828	Invalid username or password
1830	Error in writing configuration file
1833	User has been suspended

Error message ID	Error description
1835	Database error: users query
1836	Error in updating engine configuration
1850	Database error: could not create default local directory
1855	Database error: userdirectory query failed
1859	User validation error
1861	User validation error: missing password or salt
1862	Database error: user query
1869	Error in workflow manager
1870	Error in workflow manager
1871	Error in workflow manager
1877	Failed to remove stuck file after multiple attempts
1883	Database error: users of user directory could not be deleted
1911	No root CA certificates found for LDAP SSL/TLS connections on windows platform
1994	Content length header does not match with downloaded content
2031	Timed out adding file to sanitized archive
2035	Invalid sanitization configuration found for archive
2049	Engine compression capabilities unreachable

Error message ID	Error description
2050	Engine leak
2051	Next file extraction resulted in fail
2090	Database error: user query
2091	Database error: user query
2095	Sending scan requests failed
2102	Sending external action requests failed
2107	Block missing option 'origin'
2123	No respond from agent
2124	Not enough information for whitelisting
2194	Input folder got corrupted, removing it
2333	File transfer response error
2337	Local file path and body both set, ambiguous request
2352	Error adding file to quarantine
2354	Error in quarantine database
2357	Error in quarantine database
2360	Could not update quarantined file
2361	Could not gather quarantine information
2382	Selected rule not matches batch's rule

Error message ID	Error description
2384	Error storing scan batch
2388	Database error: error querying batch
2390	Database error: get batched requests
2394	Error in writing license file
2395	Error in writing license file
2424	Could not create job object
2425	Could not set information on job object
2426	Could not assign process to job
2484	Cert or key file is not readable
2485	Configured certificate cannot be used
2486	Configured certificate cannot be used
2487	Configured certificate cannot be used
2532	Found unregistered file inside sanitized storage
2547	Stopped extracting archive file due to reaching a limit
2548	Archive engine gave invalid response
2555	Unable to save updated configuration
2637	Invalid node id while trying to load engine
2640	Invalid node id while trying to query node status

Error message ID	Error description
2646	Database error: error querying what to delete
2651	Cannot find file in FinalizeScanResultBlock
2652	Given dataid can not be cancelled
2653	Given dataid can not be cancelled
2654	Database error: users query
2737	Database error: userdirectory query failed
2748	Database error: finalizing statistics
2888	Something is wrong when opening file
2892	Possible Insufficient memory to operate, system throw bad_alloc
2895	LDAP error: DN of group has changed in remote directory service. Group can not be considered valid any more
2897	Database error: Can not cache user. Already exists as non-cached
2898	Database error: Can not cache user. Already cached in DB with different DN attribute
2905	File can not be opened for writing
2906	Unable to write to file
2910	Certificate name is invalid, not using HTTPS
2973	Invalid INIT state setting for megapackage
2974	Invalid same state setting for megapackage

Error message ID	Error description
2983	No megapackage to delete with id
2988	Error removing package
2996	Package sent for validation is invalid
2997	Error validating checksum of package
2998	Invalid path to generate megapackage
2999	Not enough free space to generate megapackage
3000	Error creating package
3001	Invalid package found during megapackage generation, aborting
3002	Error adding file to megapackage
3003	Error adding file to megapackage
3004	Error adding report to megapackage
3005	Error generating sha256 checksum for megapackage
3006	Could not open file for reading
3007	Error creating database package
3008	Error creating database package
3009	Error creating database package
3013	Megapackage could not be locked for download
3014	Error opening megapackage for reading

Error message ID	Error description
3015	Megapackage file is missing from disk
3016	Could not initiate download
3040	An engine failed to initialize properly
3042	Node could not create new folder for engine
3043	Node could not create new folder for engine
3044	Error in updating engine schema
3045	Error in package storing process
3048	Invalid engine configuration
3049	Schema based configuration received for non schema based engine
3050	Schema based engine received legacy configuration
3051	Legacy configuration received is invalid
3052	Invalid configuration received for engine
3053	Schema based engine config is invalid
3059	Failed to send extract task to Agent
3060	Failed to extract
3061	Extraction timeout reached
3109	Database installation failed
3110	Engine installation failed

Error message ID	Error description
3111	Engine installation failed
3112	Engine installation failed
3113	Custom Engine installation failed
3114	Engine installation failed
3115	Communication possible disconnected
3116	Communication possible disconnected
3118	No valid node status found
3120	No result for DLP lookup
3121	Engine capabilities unreachable
3122	Engine leak
3123	Engine leak
3126	Invalid DLP engine preferences found
3127	Invalid DLP engine preferences defaults found
3128	Invalid DLP engine preferences schema found
3133	No valid node status found
3136	Database error: finalizing statistics
3140	Can't process shared resource file
3141	Can't transfer file, data channel is not open

Error message ID	Error description
3142	Can't transfer file, no result from node
3143	Resource file sharing response error
3185	Error reading quarantine file
3186	Error sending data to agent, request log from customer
3188	Error transferring file
3195	Sandbox scheduling error
3197	Error in quarantine database
3198	Invalid result from sandbox engine
3199	Invalid result from sandbox engine
3201	Invalid result from sandbox engine
3205	Sending scan requests failed
3206	Sending scan requests failed
3207	Sending scan requests failed
3208	Invalid sandbox result
3209	Invalid sandbox result
3210	Invalid result from sandbox engine
3211	Sending scan requests failed
3214	Invalid sandbox result

Error message ID	Error description
3215	Invalid sandbox result
3216	Invalid result from sandbox engine
3241	Extraction open task timed out
3242	Extraction next task timed out
3257	An error occurred while generating package
3259	Package generation is already in progress
3260	Package generation is already in progress
3261	Error while generating package
3264	Source type is unknown
3267	Can't extract zip source
3268	Http source is not a zip
3269	Can't open package descriptor for writing
3273	No status for node found
3274	No Yara engine found on node
3275	No result received
3276	Database error: sources query.
3277	Database error: issues query
3288	Expiration field is not a proper date

Error message ID	Error description
3289	License is expired
3291	Expiration field is present but it is not a timestamp
3303	EngineManager: RPC message received, but has no sender
3305	EngineManager: RPC executor not found, sending back to caller
3307	EngineManager: RPC caller not found, result orphaned
3311	Engine failed to call remote procedure call
3313	Remote procedure call timed out
3315	Engine called RPC, but an error happened
3317	Engine: There is no active engine to send RPC message to
3326	Cloud scheduling error
3331	Error in quarantine database
3338	Database error: cloud
3340	Database error: cloud
3346	Database error: cloud
3347	Database error: cloud
3349	Database error: cloud
3350	Database error: cloud
3352	Database error: cloud

Error message ID	Error description
3354	Database error: cloud
3357	Sending scan requests failed
3358	Sending scan requests failed
3359	Sending scan requests failed
3360	Invalid result from cloud engine
3363	Sending scan requests failed
3365	No cloud engine can be found in Core's engine set
3367	No cloud engine is running on the node
3368	Invalid result from cloud engine
3373	Ignition file processing failed
3378	Failed to finish welcome wizard
3379	Welcome wizard user not found
3380	Failed to remove welcome wizard user
3414	Probably incorrect db state
3415	Probably incorrect db state
3454	An error occurred after data was transferred to node
3461	Engine compression capabilities unreachable
3467	Database error: product query failed

Error message ID	Error description
3473	No respond from agent
3474	Installing database resulted in error
3475	Engine: There is no passive engine
3476	Engine: There is no active engine to deactivate
3477	Engine: Engine is already deactivated
3479	Error in updating custom engine, engine with id not found
3480	Error in updating custom engine, engine with id not found
3481	Error in updating custom engine, engine with id is active
3482	Installing database resulted in error
3483	Removing custom engine db folder failed
3484	Error installing database
3485	Error installing database, preupdate custom engine failed
3486	Error installing database, unable to copy descriptor file
3487	Error installing database, unable to copy database files
3488	Error installing database, postupdate custom engine failed
3490	Error in updating custom engine, engine with id not found
3494	Node couldn't create resources folder in given timeout
3500	Error validating user. Current server time is wrong.

Error message ID	Error description
3501	User validation error: Missing token data
3502	User validation error: Token data has expired
3503	Failed to remove reset password token from database
3506	Failed to validate user belonging to a disabled directory
3507	Non-local users are not allowed to login by token
3508	User validation error
3510	Error updating password
3515	Email sending error
3517	Email sending error
3519	Invalid login token
3523	Can't login mail server with the configuration
3524	Can't connect to mail server with the configuration
3525	Exception during closing connection to mail server
3532	Engine process is killed when timed out
3534	Can't find watermarked file
3535	File was still open when started reading from another
3536	Can't open watermarked file
3537	Error adding data to dlp file

Error message ID	Error description
3539	Error finalizing file
3541	Error occurred adding file to dlp storage
3544	Error reading watermarked file content
3545	Downloading watermarked file aborted
3546	Could not create dlp database
3553	Error in dlp database
3554	Error in dlp database
3555	No such file to remove
3559	Warning, could not remove file
3561	Error in dlp database
3567	Error querying watermarked files
3571	Error adding file to dlp storage
3572	Error adding data chunk to dlp file
3573	Error receiving file data, removing file from dlp storage
3575	Engine capabilities unreachable
3576	Engine leak
3580	Error adding new watermarked file to dlp storage
3644	

Error message ID	Error description
	Trying to send a compress task not exist in running compression tasks
3645	Trying to send an extract task not exist in running extraction tasks
3661	Error occurred while accessing scan details to add quarantine action
3664	Trying to load un-existed engineprocess*.exe
3666	Error when creating symlink of engineprocess*.exe
3677	Found unregistered file inside dlp storage
3678	Null metadata
3679	Invalid format metadata
3680	Error at parsing metadata
3681	Invalid format metadata
3687	Extraction size limit reached
3688	Cannot remove session id
3692	Extraction timeout reached
3693	Engine extraction capabilities unreachable
3694	Engine leak
3736	Failed to get version of preference schema
3738	Failed to get converted preference schema

Error message ID	Error description
3746	Failed to receive result after sending task to handle scan preferences
3747	Failed to convert scan preferences
3753	Error in creating result container.
3754	Archive engine return a not empty folder
3756	Error in response while hash lookup such as invalid apikey
3758	Failed to hash
3762	Timeout when loading engine
3763	Timeout when testing engine
3774	Client disconnected, the data has not been transferred successfully
3775	Client disconnected, the data has not been transferred successfully
3780	Found unregistered file inside quarantine storage
3807	Error in setting update url
3809	Re-generate download ID
3811	Clean up outdated download IDs
3827	User roles validation error
3828	User roles validation error
3832	The file is not an archive or corrupted

Error message ID	Error description
3833	The file is not an archive or corrupted
3835	Error in getting package
3845	Failed to rotate nginx log, cannot rename log file
3847	Failed to rotate nginx log, cannot rename log file
3850	Failed to rotate nginx log, failed to reopen log
3854	Rotate nginx log successfully but cannot compress
3863	Could not remove file
3870	Could not remove file from sanitized storage
3871	Could not remove file from sanitized storage
3872	Could not request file from agent
3873	Processing file from agent encountered an error
3876	After updating the database the engine folder could not be found
3877	Node is under high load
3888	Missing suffix of original file
3893	No response from agent
3917	Open file resulted in fail
3918	Error when compressing.
3919	Compression has got error

Error message ID	Error description
3925	Undefined webhook reply
3926	Webhook response failed
3933	Stop extraction resulted in fail
3934	Directory not supported
3955	Failed to invoke extension
3958	Failed to login with Single Sign-On enabled
3959	Do single sign-on with an unsupported directory
3971	Error in statistic info db
3972	Error querying statistic info db rowid
3973	Error querying statistic info db rowid
3996	File upload rejected due to insufficient disk space.
3999	Database error: configuration query
4000	Database error: configuration query
4001	Unable to apply patch to revert configuration
4002	Reverted configuration is invalid, hash not matching
4003	Database error: configuration query
4005	Database error: insert configuration
4006	Database error: configuration query

Error message ID	Error description
4007	Database error: configuration query
4008	Database error: configuration query
4009	Migration failed. Cannot create log directory
4022	Database error: user query
4023	Database error: Failed to delete user directory
4024	Database error: Failed to delete user directory
4025	Database error: Failed to delete user directory
4026	Database error: Failed to delete user directory
4027	Database error: Failed to delete user directory
4031	Error delete physical quarantine file
4033	Database error: error deleting all records
4034	Database error: Failed to delete records
4041	Error adding file to quarantine
4044	Failed to insert new request
4045	Failed to insert scan result
4046	Failed to clean incompleted requests
4047	Database error: update verdict count per hour
4048	Database error: update DLP count per hour

Error message ID	Error description
4049	Could not finalize scan requests
4050	Failed to insert new batch
4051	Database error: getting scan request id from hours
4052	Database error: getting verdicts statistics by hours
4053	Database error: getting DLP statistics by hours
4054	Database error: getting verdicts statistics by hours
4055	Database error: getting statistics info
4056	Database error: getting statistics info
4057	Database error: error deleting all records
4058	Database error: Failed to delete records
4062	Database error: error querying what to delete
4066	Database error: cloud
4069	Error in statistics DB
4070	Error in statistics DB: get rule id by name
4071	Error in statistics DB: rule not found
4072	Error in statistics DB: get metascan statistics
4073	Error in statistics DB: get CDR statistics
4074	Error in statistics DB: get DLP statistics

Error message ID	Error description
4075	Error in statistics DB: get vulnerabilities statistics
4076	Error in statistics DB: wrong type for top file types
4077	Error in statistics DB: get file types statistics
4081	Could not remove file from sanitized storage
4082	Could not remove file from sanitized storage
4084	Postgres issue
4089	Error in dlp database
4091	Coud not found the key to decrypt proxy password
4093	Error in sanitize database
4096	Database error: Failed to delete user directory
4097	Error in package staging process
4098	Error in get engine by state
4099	Error in get engine configuration
4100	Error in get engine schema
4101	Database error: user query
4102	Database error: Failed to delete user directory
4104	Database error: Failed to delete user directory
4106	Database error: Failed to delete user directory

3.8 Security settings on web console

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

3.8.1 Enabling HTTPS

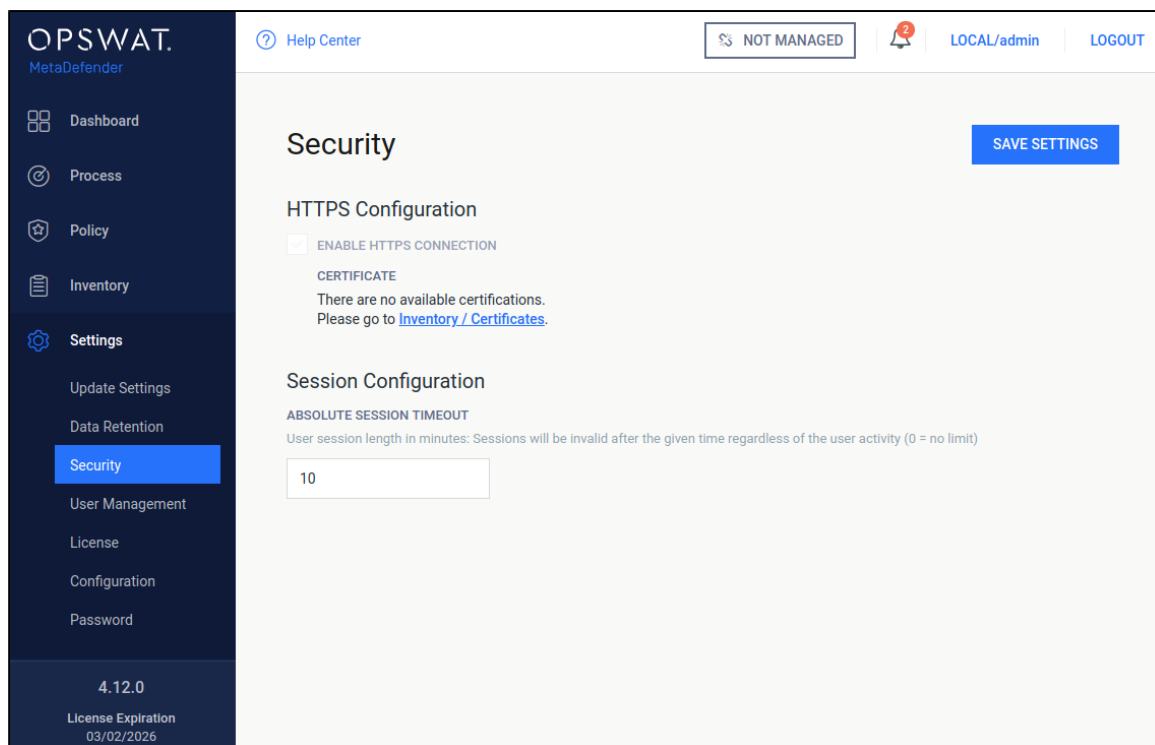
MetaDefender Core supports accessing Web UI and REST interface via HTTPS. This feature is not enabled by default. There are two ways to enable the feature:

- 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.

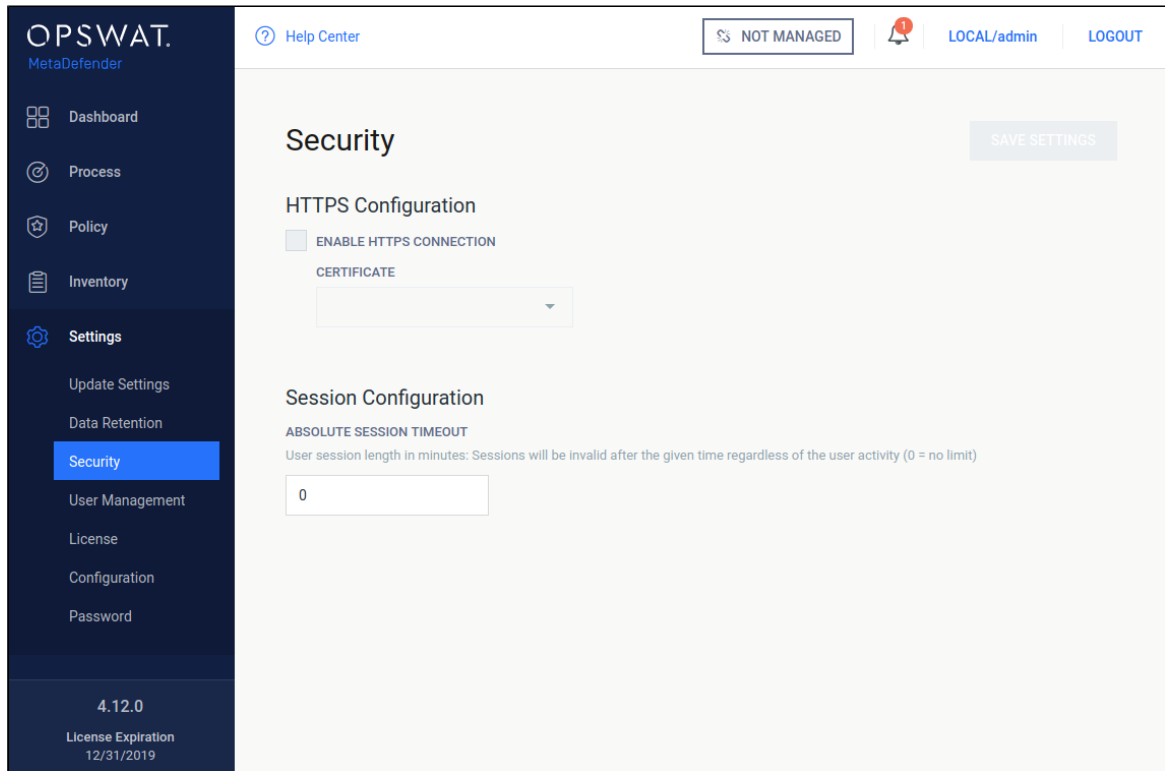
Enabling HTTPS via Management Console

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

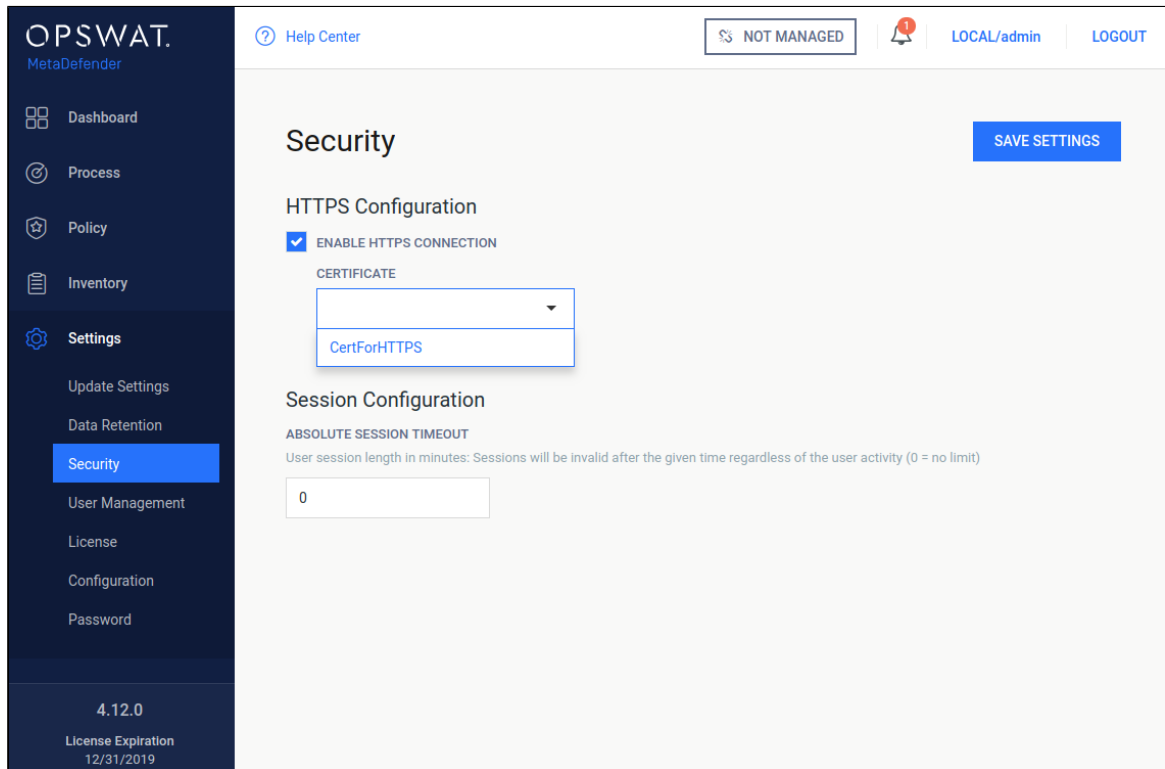


The screenshot shows the OPSWAT MetaDefender web console interface. The left sidebar contains navigation options: Dashboard, Process, Policy, Inventory, Settings (highlighted), Update Settings, Data Retention, Security (highlighted), User Management, License, Configuration, and Password. The main content area is titled 'Security' and features a 'SAVE SETTINGS' button. Under 'HTTPS Configuration', there is a checkbox for 'ENABLE HTTPS CONNECTION' which is currently unchecked. Below this, it states 'CERTIFICATE: There are no available certifications. Please go to [Inventory / Certificates](#).' Under 'Session Configuration', there is a section for 'ABSOLUTE SESSION TIMEOUT' with a description: 'User session length in minutes: Sessions will be invalid after the given time regardless of the user activity (0 = no limit)'. A text input field contains the value '10'.

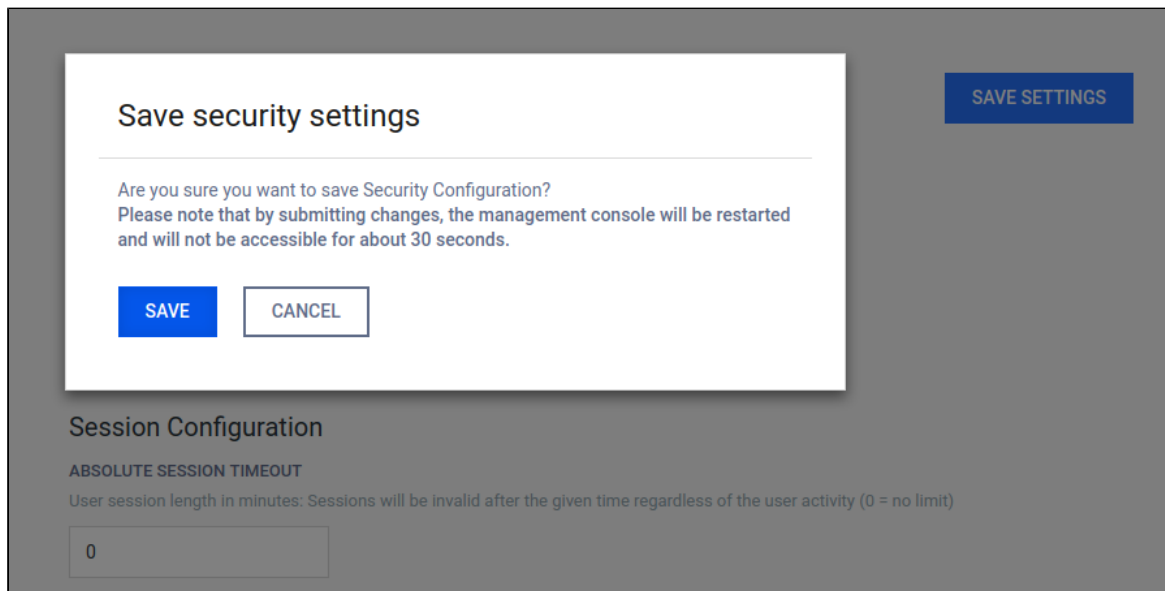
2. If there's no certificate-key pair added to the inventory, [please go to Inventory](#)→[Certificates](#) page and add one that is desired to use for securing HTTP connections.



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



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



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

Enabling HTTPS via configuration files (more configuration modes supported)

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.



Advanced web server configurations (applicable to both Linux and Windows platform)

1.) Explicitly allow specific TLS versions, optionally with preferred ciphers. For example:

```
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";

ssl_protocols tlsv1.1 tlsv1.2
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256
```

2.) Use SSL private key and(or) certificate which is encrypted with a passphrase. Strongly recommended to put the passphrase file(s) into a secured vault where only MetaDefender Core can access.

A reference for typical practice: <https://www.nginx.com/blog/protecting-ssl-private-keys-nginx-hashicorp-vault/>

```
ssl on;

ssl_certificate "C:/Program Files/OPSWAT/Metadefender Core
/nginx/cert.pem";
ssl_certificate_key "/etc/keys/secretkey.pass";

ssl_certificate_key "C:/Program Files/OPSWAT/Metadefender
Core/nginx/your_encrypted.key";
ssl_password_file "/etc/keys/private.pass";

ssl_protocols tlsv1.1 tlsv1.2
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256
```

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

❗ '\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\nnginx\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.

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.

OPSWAT.
MetaDefender

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

4.12.0
License Expiration
03/02/2026

Help Center

NOT MANAGED

LOCAL/admin | LOGOUT

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

3.8.3 Password Policy

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

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

At least 1 uppercase letter of European languages (A through Z)

At least 1 lowercase letter of European languages (a through z)

At least 1 base 10 digits (0 through 9)

At least 1 non-alphanumeric characters (special characters): (~!@#\$%^&* _+=`|(){}

[];:"<>.,?/\)

The screenshot displays the OPSWAT MetaDefender web interface. The top navigation bar includes a 'Help Center' link, a 'NOT MANAGED' status indicator, a notification bell with a red '1', and user information 'LOCAL/admin' with a 'LOGOUT' link. The left sidebar contains a menu with items: Dashboard, Process, Policies, Inventory, Settings (highlighted), Update Settings, Data Retention, Security (highlighted), User Management, License, Configuration, Password, and Email Configuration. The main content area is titled 'Security' and features a 'SAVE SETTINGS' button. It is divided into three sections:

- HTTPS Configuration:** Includes a checkbox for 'ENABLE HTTPS CONNECTION' (unchecked), a 'CERTIFICATE' section stating 'There are no available certifications. Please go to [Inventory / Certificates](#).'
- Session Configuration:** Includes a section for 'ABSOLUTE SESSION TIMEOUT' with the description 'User session length in minutes: Sessions will be invalid after the given time regardless of the user activity (0 = no limit)' and a text input field containing '0'.
- Password Policy:** Includes three settings: 'ENFORCE PASSWORD HISTORY' (input: 0), 'MINIMUM PASSWORD LENGTH' (input: 0), and 'PASSWORD MUST MEET COMPLEXITY REQUIREMENTS' (checkbox: unchecked).

 The bottom of the sidebar shows the version '4.16.0' and 'License Expiration 2026-12-31'.

3.9. Configuring proxy settings

How can I set proxy server for the product

Linux

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

Restart `ometascan` service to take effect

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](#).

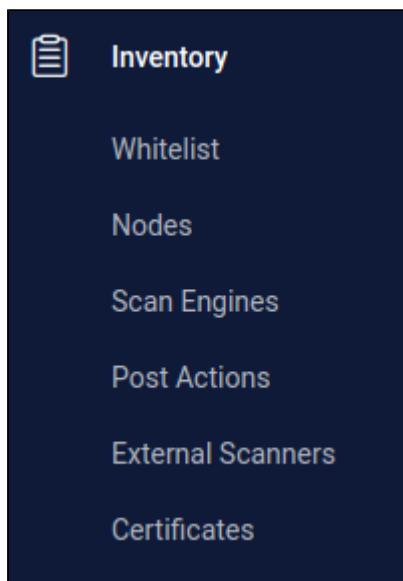
i You might need to configure Windows proxy to bypass local addresses if you can't access Web Management Console from the host itself. Consult netsh documentation for additional configuration options.

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 processing 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
- If the command path contains space character, then must nest the command path into double quote. For example: `"C:\Test Space\Hello.exe"`
- **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

 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": "4fb0083cd3cd966817c1ee4fa3f02519d05eca0b57c2bf71109
d3bd69acebd41",
  "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/Modules** menu it is possible to configure custom **Yara sources**.

Modules

Last update: an hour ago | Next update: in 3 hours | [Edit Update Settings](#)

MODULE	LAST UPDATE	ACTIVITY	ENGINE	DATABASE	ENABLED
Metascan	8 hours ago	2/4 processing engines are active			▼
Deep CDR i	5 days ago	Active on 1/1 node	5.4.3-1617	5.1.1	<input checked="" type="checkbox"/>
Proactive DLP i	4 days ago	Active on 0/1 node	1.0.3-155 (disabled)	06/30/2019	<input type="checkbox"/>
Threat Intelligence	5 days ago	Active on 0/1 node	1.0-12 (disabled)	1.0-12	<input type="checkbox"/>
File-Based Vulnerability Assessment	2 days ago	Active on 0/1 node	4.2.416.0-89 (disabled)	1561989579 1562011012 (downloaded)	<input type="checkbox"/>
Utilities	5 days ago	3/3 engines are active			▲
ENGINE NAME	PLATFORM	NODES	ENGINE	DATABASE	ENABLED
FileType	Microsoft Windows	🟢	5.2.7-431	5.2.7-431	<input checked="" type="checkbox"/>
Archive engine	Microsoft Windows	🟢	5.2.6-452	5.2.6-452	<input checked="" type="checkbox"/>
Yara	Microsoft Windows	🟢	3.8.1-64	3.8.1-84	▲ <input checked="" 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

ADD **CANCEL**

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.

Please note that the included Yara modules are the following:

- [Magic](#)
- [Hash](#)
- [Dotnet](#)
- [Macho](#)
- [Dex](#)
- [Cuckoo](#)
- [Androguard](#)

For more details, check [Yara modules documentation](#).

3.12 Server Configurations

3.12.1 Email Configuration

Users with administrator privilege on MetaDefender Core are allowed to setup email configurations for SMTP in order to enable password recovery feature (please check [3.1.1. Password Recovery](#)).

The screenshot shows the 'Server Configuration' page in the OPSWAT MetaDefender Core interface. The page is titled 'Server Configuration' and has two tabs: 'Email' (selected) and 'Proxy'. There are two buttons at the top right: 'CLEAR SETTINGS' and 'SAVE SETTINGS'. Below the tabs, a note states: 'These configurations are applicable to the reset password feature.' The configuration fields are as follows:

- SERVER HOST:** A text input field containing 'Server host'.
- SERVER PORT:** A text input field containing '0'.
- CONNECTION TYPE:** A dropdown menu with 'TCP' selected.
- AUTH METHOD:** A dropdown menu with 'AUTH PLAIN' selected.
- User authentication:** A section with three input fields:
 - EMAIL:** A text input field containing 'Email'.
 - USERNAME:** A text input field containing 'Username'.
 - PASSWORD:** A text input field containing 'Password'.

Server configuration

Properties	Description	Option
SERVER HOST	SMTP server host	IP address / Domain all accepted
SERVER PORT	SMTP server port	Some default common ports: <ul style="list-style-type: none">• 25 (TCP)• 465 (SSL)

Properties	Description	Option
		<ul style="list-style-type: none"> • 587 (TLS)
CONNECTION TYPE	Specify type of connection between MetaDefender Core and SMTP server	<ul style="list-style-type: none"> • TCP (Unsecured email transmission protocol) • SSL (Secured email transmission protocol) • TLS (Secured email transmission protocol)
AUTH METHOD	Specify the authorization protocol connecting to SMTP server	<ul style="list-style-type: none"> • AUTH PLAIN • AUTH LOGIN (preferred)

User authentication

Properties	Description
EMAIL	Email address
USERNAME	Username for SMTP authentication
PASSWORD	Password for SMTP authentication

Please make sure to hit "SAVE SETTINGS" button once configuration is done.

Otherwise "CLEAR SETTINGS" button once hit will clear up all mail settings on the page.

3.12.2 Proxy Configuration

Since MetaDefender Core 4.19.0, proxy configuration is possible via management console UI, and with proxy authentication support. MetaDefender Core no longer relies on system configurations to obtain the proxy setting, but it will control the thing itself.

Server configuration

Properties	Description	Option
SERVER	Proxy server host address	IP address / Domain all accepted
PORT	Proxy server port	Some default common ports: <ul style="list-style-type: none"> • 3128 (Squid) • 49152 (ProxySG)

User authentication

Properties	Description
USERNAME	Username for proxy authentication
PASSWORD	Password for proxy authentication

Please make sure to hit "SAVE SETTINGS" button once configuration is done.

4. Process files with MetaDefender Core

There are several ways to scan files with MetaDefender Core:

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

Process Files via REST API

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

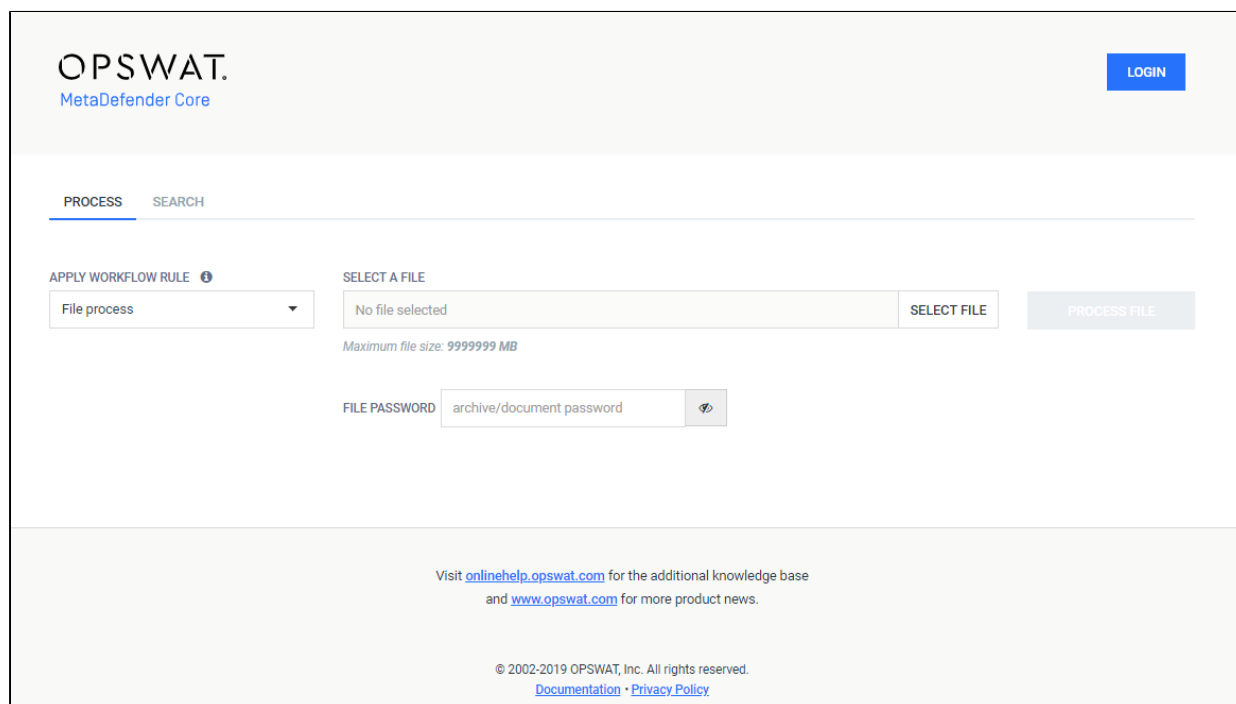
Chunked transfer encoding is not supported to upload files for processing.

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](#).

Process Files via Web Interface

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



The screenshot shows the OPSWAT MetaDefender Core web interface. At the top left is the OPSWAT logo and "MetaDefender Core" text. A blue "LOGIN" button is in the top right. Below the logo are two tabs: "PROCESS" (active) and "SEARCH". The main area contains a form for file processing. On the left, there is a dropdown menu for "APPLY WORKFLOW RULE" with "File process" selected. In the center, there is a "SELECT A FILE" section with a text input showing "No file selected", a "SELECT FILE" button, and a "PROCESS FILE" button. Below this, it says "Maximum file size: 9999999 MB". At the bottom of the form, there is a "FILE PASSWORD" field with the text "archive/document password" and a small icon. At the bottom of the page, there is a footer with the text: "Visit onlinehelp.opswat.com for the additional knowledge base and www.opswat.com for more product news." and "© 2002-2019 OPSWAT, Inc. All rights reserved. [Documentation](#) · [Privacy Policy](#)".

Scan

Choose what to process and how

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

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.

5. Deep CDR (Data Sanitization)

On processing result UI, users can have more insights on sanitization outcome returned by Deep CDR engine (under DEEP CDR DETAILS tab), this feature has been introduced since MetaDefender Core v4.15.0. For integration via REST API, please check [Forensic Info](#).

To learn more about Deep CDR technology on MetaDefender Core, please check the [Deep CDR user guide](#).

PROCESS NEW FILE

recursive_multiple_level.xlsx

DOWNLOAD PROCESSED ARCHIVE

File Allowed
Show reason ▾

Workflow Rule applied: MetaDefender Email Security

SCANNING ENGINES 0 / 2

None of the engines found a threat

DEEP CDR SANITIZED

PROACTIVE DLP PROACTIVE DLP NOT CONFIGURED

FILE-BASED VULNERABILITY ASSESSMENT ||||

No vulnerability found

UPLOADED 2019-07-04 07:48:19 GMT+7	SCANNED 2019-07-04 07:48:19 GMT+7
FILE TYPE Microsoft Excel Workbook	FILE SIZE 437.6 KB

MD5 3d641d141c31fb9e0fafbdfa07e2f7b6	 COPY
SHA1 662e0868a560bd0219cc4511f49a0a263da5af83	 COPY
SHA256 ffb66cbbf1f1cb2e1a7ddc3e1b854275fc14e33473134ecf8af61d64d08b...	 COPY

ORIGINAL FILE
 EXTRACTED FILES

METASCAN
DEEP CDR DETAILS

ACTION	OBJECT	COUNT	FILENAME	DESCRIPTION
	DDE	2		
	external sheet	1		
	DOCX file		Microsoft_Word_Document.docx	Processed successfully.
	image	1		

PROCESS NEW FILE

DOWNLOAD PROCESSED FILE

File Allowed
Workflow Rule applied: File process

SCANNING ENGINES
None of the engines found a threat 0 / 4

DEEP CDR SANITIZED

PROACTIVE DLP PROACTIVE DLP NOT CONFIGURED

FILE-BASED VULNERABILITY ASSESSMENT
No vulnerability found ||||

UPLOADED 2020-05-18 18:40:35 GMT+7	SCANNED 2020-05-18 18:40:35 GMT+7
FILE TYPE Adobe Portable Document Format	FILE SIZE 17.3 MB

MD5 210d0f12a53137eae52840069a560363	 COPY
--	----------


SHA1 9940e4822b3bd1cc18a2e56632c70cbfbb6aabb1	 COPY
---	----------

SHA256 ee3183680b6c8eedf0db5439025ef597800f0d1600f16ca0a8cb3c93219bc4e5	 COPY
---	----------

METASCAN DEEP CDR DETAILS

ACTION	OBJECT	COUNT	FILENAME	DESCRIPTION
Sanitized	image	3		
Removed	hyperlink	259		▼
			http://10.0.1.100:8081/callback	
			http://10.0.1.100:8081/listenback	
			http://2016.eicar.org/86-0-Intended-use.html	
			http://Collectorz.com	
			http://Coriolis.io	

6. Proactive DLP

 Proactive DLP requires separate licensing for MetaDefender Core to enable this technology module.

With Proactive DLP technology, MetaDefender Core can detect, block or prevent sensitive data leaking in data transferring over networks.

Please check out more details at [Proactive DLP user guide](#)

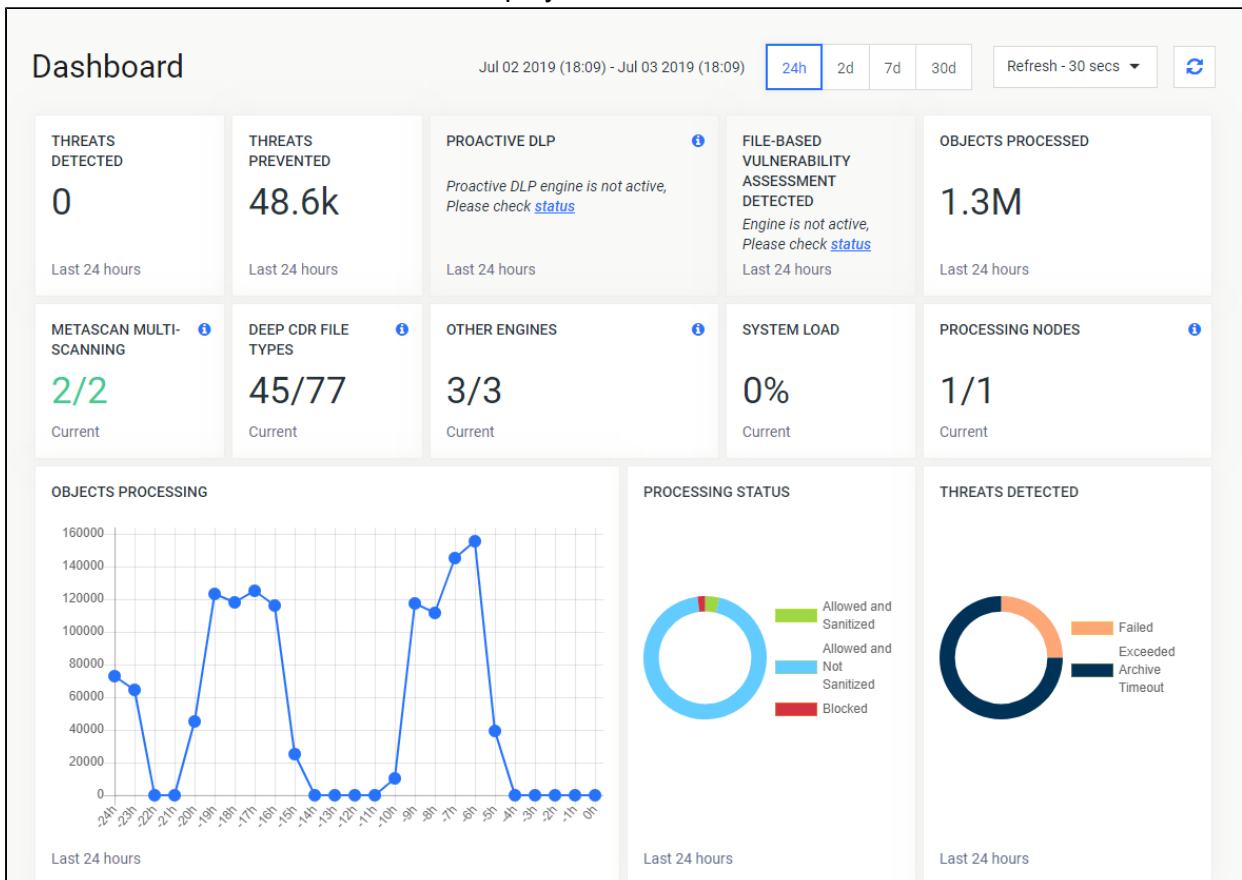
7. Operating MetaDefender Core

- 7.1. Dashboard
- 7.2. Inventory Management
- 7.3. Regular Maintenance
- 7.4 Import/Export configuration
- 7.5. Database Defragmentation and Optimization
- 7.6. Reporting
- 7.7. Statistics

7.1. 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.

Processing history

The Scan History page shows information on all scans made on the MetaDefender Core. Search and filter are also supported against each scan result attribute.

The screenshot displays the 'Processing History' page in the OPSWAT MetaDefender Core interface. The page features a sidebar on the left with navigation options: Dashboard, Overview, Statistics (BETA), Processing History (selected), Quarantine, Update History, Config History, Process, Policies, Inventory, and Settings. The main content area shows a table of scan results with the following columns: RESULT, FILENAME, RULE, SOURCE, USERNAME, DURATION, and START TIME. The table contains four rows of data:

RESULT	FILENAME	RULE	SOURCE	USERNAME	DURATION	START TIME
No Threat Detected	Downloads.7z	File process	:1	LOCAL/admin	373 ms	2020-08-26 11:32:07
Blacklisted	Downloads.7z	File process	:1	LOCAL/admin	346 ms	2020-08-26 11:31:51
No Threat Detected	Downloads.7z	File process	:1	LOCAL/admin	401 ms	2020-08-26 11:31:19
No Threat Detected	Migration done.PNG	File process	:1	LOCAL/admin	31 ms	2020-08-26 11:31:12

The interface also includes a top navigation bar with 'NOT MANAGED', 'LOCAL/admin', and 'LOGOUT' buttons. The main content area has a 'Processing History' title, 'Settings', and 'Refresh' buttons. There are also 'CLEANUP' and 'EXPORT TO STIX' buttons. The table has search filters for 'Filter by action', 'Filter by status', and 'Filter by hash'. The table is paginated, showing 1 page of 20 items per page.

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.

The screenshot displays the scan results for a file named 'ProcessMonitor.zip'. At the top right, there are buttons for 'PROCESS NEW FILE' and 'DOWNLOAD PROCESSED ARCHIVE'. The main status is 'File Allowed' with the note 'Workflow Rule applied: File process'. Below this, a 'SCANNING ENGINES' section shows '0 / 4' engines. The engines listed are DEEP CDR (SANITIZED), PROACTIVE DLP (N/A, PROACTIVE DLP NOT CONFIGURED), and FILE-BASED VULNERABILITY ASSESSMENT (No vulnerability found). To the right, file metadata is shown: UPLOADED (2019-09-11 16:31:54 GMT+7), SCANNED (2019-09-11 16:31:54 GMT+7), FILE TYPE (ZIP Archive), and FILE SIZE (1.1 MB). Below this, three hash values are provided with 'COPY' buttons: MD5 (2d5632d0ac7378c6c13392334c242bb1), SHA1 (802a53532cc95884a900ef48db5350d2b919f31e), and SHA256 (3a0ce29f1654468a470d8b4e0f5f163a428ddab7bf0ea37b0cef504362cb94dd). At the bottom, a table shows the results for the original files:

FILES (1 - 3 SHOWN OF 3)	RESULT
✓ Procmon.exe	No Threat Detected
✓ procmon.chm	No Threat Detected
✓ Eula.txt	No Threat Detected

Navigation controls at the bottom include a page indicator '1' and a 'SHOW 20 per pages' dropdown.

On the Processing history page you can also search for:

- MD5, SHA1, SHA256 hashes
- File name (and you can limit search result for a specific scan result, and for specific username who submitted files)

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.

7.2. Inventory Management

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

- [7.2.1. Certificates](#)
- [7.2.2. Modules](#)
- [7.2.3. Nodes](#)
- [7.2.4. Skip by hash](#)

7.2.1. Certificates

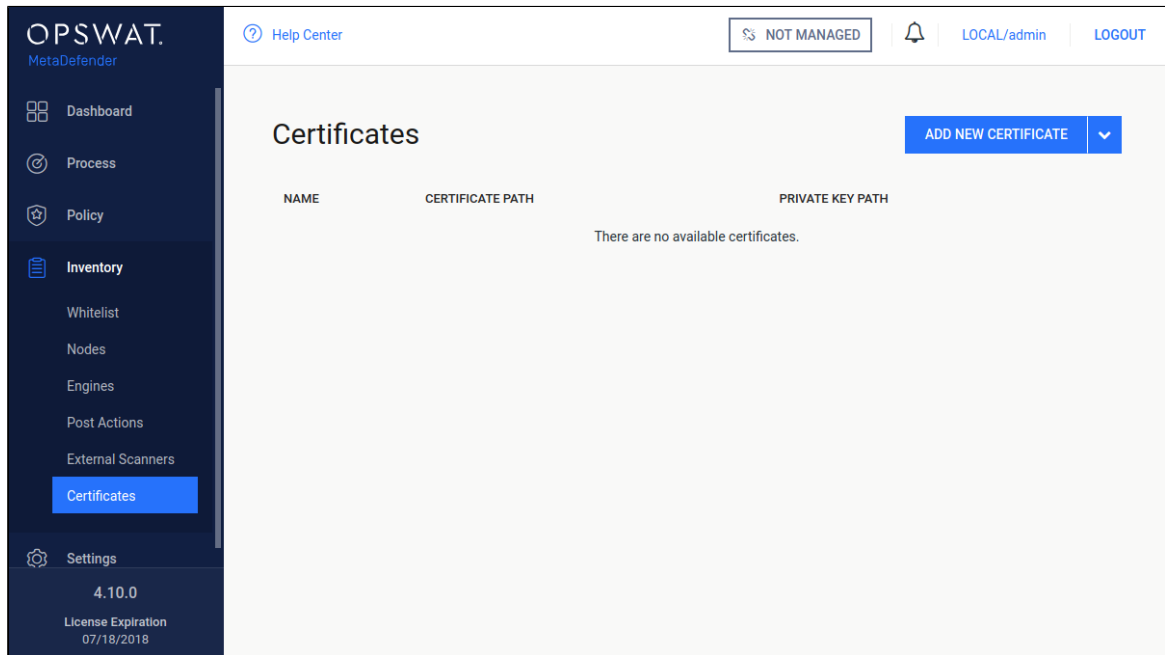
On this page, path to certificates and private keys for signing scan batches or HTTPS configuration can be given.



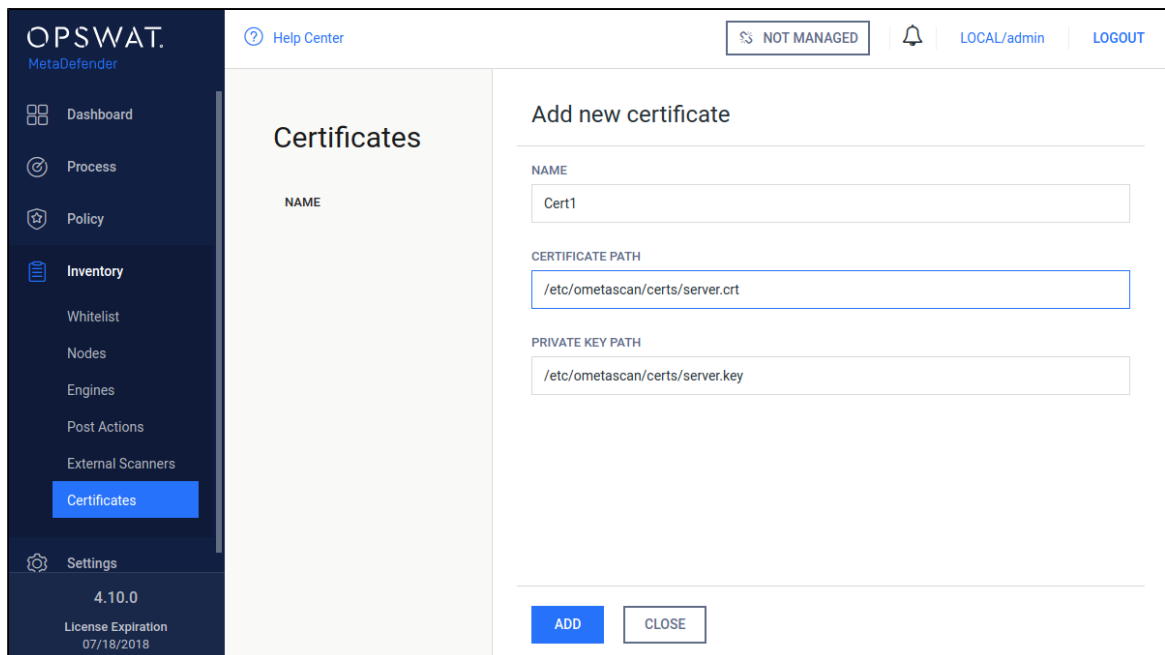
- Certificate should be in a Base64-encoded X.509 certificate file (.crt, .cer) format.
- Private key should be a privacy-enhanced electronic mail file (.pem) format and it should not be locked by password.

Adding certificate-key pair to the inventory

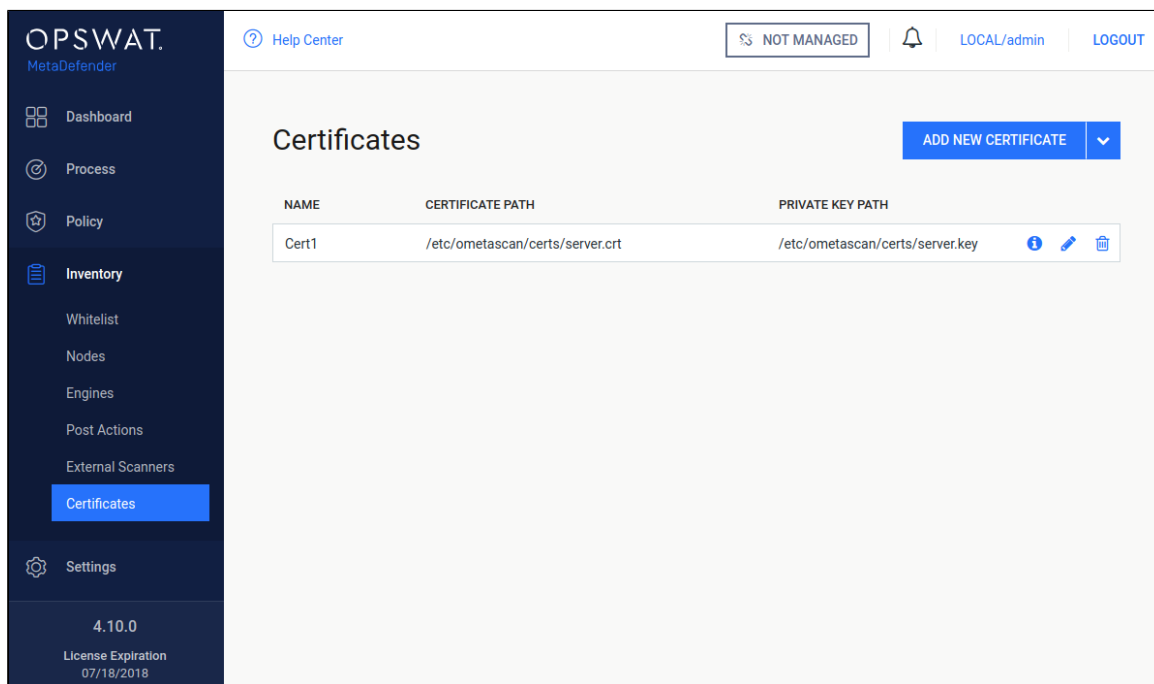
1. Go to **Inventory**→**Certificates** page
2. Click on **Add new certificate** button



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

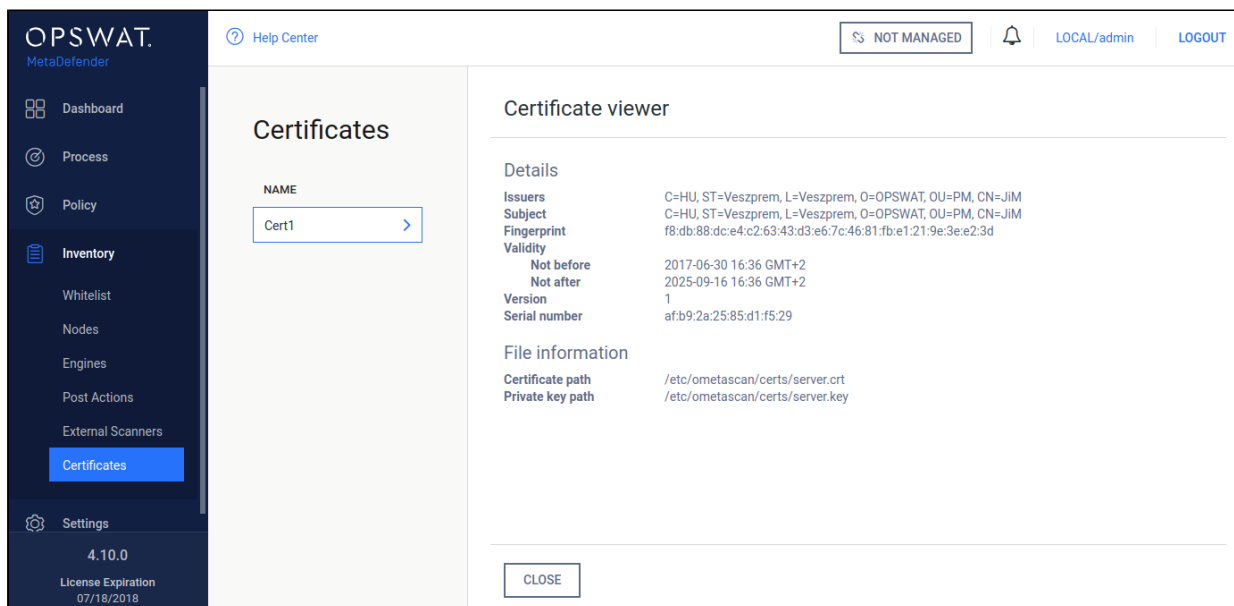


4. Click **Add** button



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 screenshot shows the OPSWAT MetaDefender interface. The top navigation bar includes 'Help Center', 'NOT MANAGED', a notification bell, 'LOCAL/admin', and 'LOGOUT'. The left sidebar lists various system components, with 'Certificates' highlighted. The main content area displays a 'Certificates' list with one entry, 'Cert1'. A 'Modify certificate' dialog is open, allowing users to edit the certificate details. The dialog fields are: NAME (Cert1), CERTIFICATE PATH (/etc/ometascan/certs/server.crt), and PRIVATE KEY PATH (/etc/ometascan/certs/server.key). The dialog concludes with 'OK' and 'CLOSE' buttons.

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

7.2.2. Modules

Engine type details

Under the **Modules** 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 'Modules' management interface in OPSWAT MetaDefender. The main table lists various security modules, their last update times, activity status, and associated engine and database versions. A sub-table for 'Utilities' provides a detailed view of individual engines, including their platform (Microsoft Windows), node status, and specific engine and database versions. Each engine entry includes a toggle switch to enable or disable it. The interface also features a sidebar with navigation options and a top navigation bar with user information and a 'NOT MANAGED' status indicator.

MODULE	LAST UPDATE	ACTIVITY	ENGINE	DATABASE	ENABLED
Metascan	8 hours ago	2/4 processing engines are active			▼
Deep CDR ⓘ	5 days ago	Active on 1/1 node	5.4.3-1617	5.1.1	🔴
Proactive DLP ⓘ	4 days ago	Active on 1/1 node	1.0.3-155	06/30/2019	🔴
Threat Intelligence	5 days ago	Active on 1/1 node	1.0-12	1.0-12	🔴
File-Based Vulnerability Assessment	2 days ago	Active on 1/1 node	4.2.416.0-89	1561989579 1562011012 (staging)	🔴
Utilities	5 days ago	3/3 engines are active			▲
ENGINE NAME	PLATFORM	NODES	ENGINE	DATABASE	
FileType	Microsoft Windows	🟢	5.2.7-431	5.2.7-431	🔴
Archive engine	Microsoft Windows	🟢	5.2.6-452	5.2.6-452	🔴
Yara	Microsoft Windows	🟢	3.8.1-64	3.8.1-84	▼ 🔴

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.

Pin & Unpin engines (for auto-update prevention)

Engine and its database can be pinned to prevent it from being applied new updates when you allow auto update on Core. To pin it, just mouse over desired engine / database, and there you will see a "pin" icon

OPSWAT MetaDefender

Help Center NOT MANAGED LOCAL/admin LOGOUT

Modules

Auto update turned off | [Edit Update Settings](#)

MODULE	LAST UPDATE	ACTIVITY	ENGINE	DATABASE	ENABLED
Metascan	2 days ago	10/12 processing engines are active			
ENGINE NAME	PLATFORM	NODES	ENGINE	DATABASE	
Ahnlab	Microsoft Windows		3.4.3.1 (11912)-51	1564745160 (2 days)	
Avira	Microsoft Windows		4.10.0-89	1564592203 (5 days)	
Bitdefender	Microsoft Windows		11.0.1.12-65	1564733100 (2 days)	
ClamAV	Microsoft Windows		0.100.1-82	1564734060 (2 days)	
Cyren	Microsoft Windows		6.2.0-39	201908021111 (2 days)	
ESET	Microsoft Windows		1462 (20150625)-25	1564704000 (3 days)	
Ikarus	Microsoft Windows		5.1.5-182 (disabled)	101801	
K7	Microsoft Windows		12.8.0.1-41	1564739920 (2 days)	

When pinned successfully, you are supposed to see a pin icon right next to that affected item indicating that:

OPSWAT MetaDefender

Help Center NOT MANAGED LOCAL/admin LOGOUT

Modules

Auto update turned off | [Edit Update Settings](#)

MODULE	LAST UPDATE	ACTIVITY	ENGINE	DATABASE	ENABLED
Metascan	2 days ago	10/12 processing engines are active			
ENGINE NAME	PLATFORM	NODES	ENGINE	DATABASE	
Ahnlab	Microsoft Windows		3.4.3.1 (11912)-51 (pinned)	1564745160 (2 days)	
Avira	Microsoft Windows		4.10.0-89	1564592203 (5 days)	
Bitdefender	Microsoft Windows		11.0.1.12-65	1564733100 (2 days)	
ClamAV	Microsoft Windows		0.100.1-82	1564734060 (2 days)	
Cyren	Microsoft Windows		6.2.0-39	201908021111 (2 days)	
ESET	Microsoft Windows		1462 (20150625)-25	1564704000 (3 days)	
Ikarus	Microsoft Windows		5.1.5-182 (disabled)	101801	

Some notes:

- You can pin engine and database individually on same engine
- When pinned, that means no auto update can be applied on that part (engine / database), even when user triggers "Update All" button

To allow applying auto update back, just click on pinned icon again.

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="text"/>	<input type="text"/>

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 and then click on that line, then hit **Settings**. The edit page is displayed.

Engine Configuration

SAVE SETTINGS

[Revert to default](#)

GENERAL CONFIGURATION ⓘ

INCLUDE SANITIZATION DETAILS ⓘ

INCLUDE PROCESSED OBJECTS ⓘ

IMAGE MEMORY LIMIT (MB) ⓘ

3072

NUMBER OF IMAGE PROCESSING THREADS ⓘ

1

PDF CONFIGURATION ⓘ

REMOVE MACRO ⓘ

REMOVE EMBEDDED OBJECT ⓘ

REMOVE HYPERLINK ⓘ

Remove hyperlink annotations only ▼

CLOSE

Choose your desired configurations and click **Save Settings**, then Close.

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 enable_pcre=0 scan_pdf=1</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.</p> <p>max_scan_size: The maximum amount of data to scan for each container file. Certain files (e. g. documents, archives, etc.) may 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.</p> <p>deep_scan:</p> <p>0 - Do not scan the whole file if it is a big file 1 - Scan full file, it may take significantly higher time</p> <p>enable_pcre : only available on the Linux version, enable this configuration will increase the detection rate but may affect performance</p> <p>scan_pdf: extract objects in PDF files to scan</p>
Avira	<pre>[engine] heuristic_scan=1 extract_archive=0 detect_all_types=1 enable_pup_scan=1</pre>	<p>heuristic_scan:</p> <p>0 - Disable heuristic detection. 1 - Lazy heuristic detection. This is the lowest possible mode, detection is not very good, but the false positives number will be low. 2 - Normal heuristic detection. 3 - High heuristic detection. This is the highest possible mode, but the false positives number will be high.</p> <p>enable_pup_scan: only available on Windows</p>
ESET		

Scan engine	Configuration	Note
	[engine] heuristic_scan=1 extract_archive=0 enable_pup_scan=1	
Ahnlab	[engine] extract_archive=0 enable_cloud_scan=0 enable_pup_scan=0	enable_pup_scan: only available on Windows
BitDefender	[engine] extract_archive=0	
CYREN	[engine] extract_archive=0 enable_pup_scan=0	
QuickHeal	[engine] heuristic_scan=0 extract_archive=0 enable_pup_scan=0	
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.

Scan engine	Configuration	Note
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: 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 deep_scan =1	deep_scan : 0 - lower memory usage 1 - default; high detection rate, but a bit slower and more resources usage
McAfee		

Scan engine	Configuration	Note
	[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	
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	
STOPzilla	[engine] extract_archive=0	
Symantec		

Scan engine	Configuration	Note
	[engine] server=127.0.0.1:1344 heuristic_scan=1 extract_archive=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	
Comodo	[engine] heuristic_scan=1 extract_archive=0	
Trend Micro and Trend Micro House Call	[engine] enable_pup_scan=0	
Xvirus	No configuration	
RocketCyber	No configuration	
CrowdStrike Falcon ML	No configuration	
Windows Defender	No configuration	
Microsoft Security Essentials	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
- Cloud scan feature (enable_cloud_scan) only sends file signatures to AV servers to analyze

7.2.3. 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

The screenshot shows the OPSWAT MetaDefender interface. The main content area is titled "Process Nodes" and contains a table with the following data:

ADDRESS	ACTUAL LOAD	CPU CORES	FREE DISK SPACE	TOTAL MEMORY	NODE VERSION	OS	INSTALLED ENGINES	STATUS
localhost	100%	4	93.27 GB	15.99 GB	4.16.0	Microsoft Windows Server 2016 Datacenter	11/11	✓

The left sidebar includes navigation items: Dashboard, Process, Policies, Inventory (with sub-items: Modules, Skip by Hash, Nodes, Post Actions, External Scanners, Certificates), and Settings. The bottom left corner shows the version "4.16.0" and "License Expiration 2026-12-31". The top right corner displays "NOT MANAGED", a notification icon, and user information "LOCAL/admin" with a "LOGOUT" link.

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 blue sidebar with navigation options: Dashboard, Process, Policies, Inventory, Modules, Skip by Hash, Nodes (highlighted), Post Actions, External Scanners, Certificates, and Settings. The main content area is divided into two panels. The left panel, titled 'Process Nodes', contains a table with columns 'ADDRESS', 'ACTUAL LOAD', and 'INSTALLED ENGINES'. A single row shows 'localhost', '44%', and '11/11' with a right-pointing arrow. The right panel, titled 'Node details', shows the node is operational. It lists details: ADDRESS (localhost), OS (Microsoft Windows Server 2016 Datacenter), and VERSION (4.16.0). A green circle highlights 'ENGINES 11/11'. Below this are three tabs: ISSUES, MODULES (selected), and HARDWARE INFO. The MODULES tab contains a table with columns: MODULE, TYPE, VERSION, DATABASE, and ACTIVE. The table lists several modules, all with green checkmarks in the ACTIVE column.

ADDRESS	ACTUAL LOAD	INSTALLED ENGINES
localhost	44%	11/11

MODULE	TYPE	VERSION	DATABASE	ACTIVE
Archive engine	Archive	5.2.6-452	5.2.6-452	✓
Ahnlab	Anti-Malware	3.4.3.1 (11912)-51	1562160240 (up to date)	✓
Avira	Anti-Malware	4.10.0-89	1562148551 (2 days)	✓
ClamAV	Anti-Malware	0.100.1-82	1562140980 (up to date)	✓
DLP	Proactive DLP	1.0.3-155	06/30/2019	✓
Data sanitization	Deep CDR	5.4.3-1617	5.1.1	✓
ESPE	Anti-Malware	1.0.0-156212000	1562112000	✓

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.

7.2.4. 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 displays the 'Skip by Hash' configuration page in the OPSWAT MetaDefender interface. The page includes a search bar, a filter for 'Show only' (with checkboxes for SKIP ENGINES, WHITELIST, and BLACKLIST), and a table of skip engines. The table has three columns: HASH, ENGINES, and COMMENT. Two entries are shown:

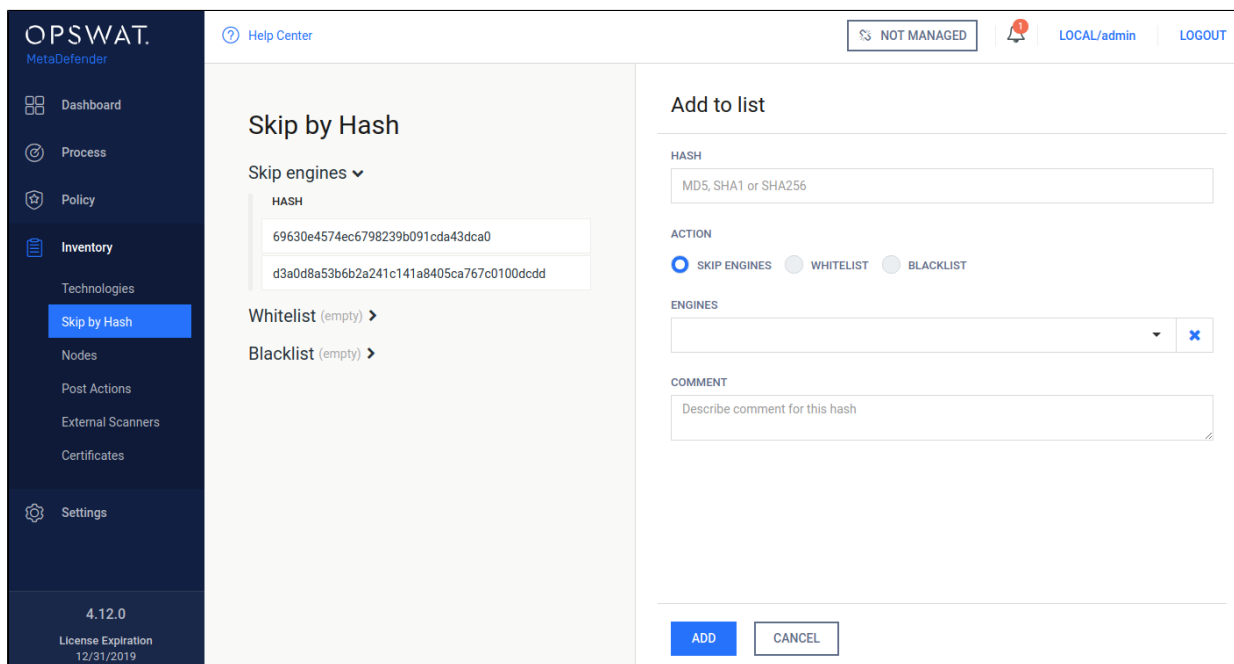
HASH	ENGINES	COMMENT
69630e4574ec6798239b091cda43dca0	ClamAV	pseudo virus
d3a0d8a53b6b2a241c141a8405ca767c0100dcdd	ESET, Bitdefender	a file

Below the table, there are sections for 'Whitelist (empty) >' and 'Blacklist (empty) >'. The interface also shows a sidebar with navigation options like Dashboard, Process, Policy, Inventory, and Settings, along with version information (4.12.0) and license expiration (12/31/2019).

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.

7.3. 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.

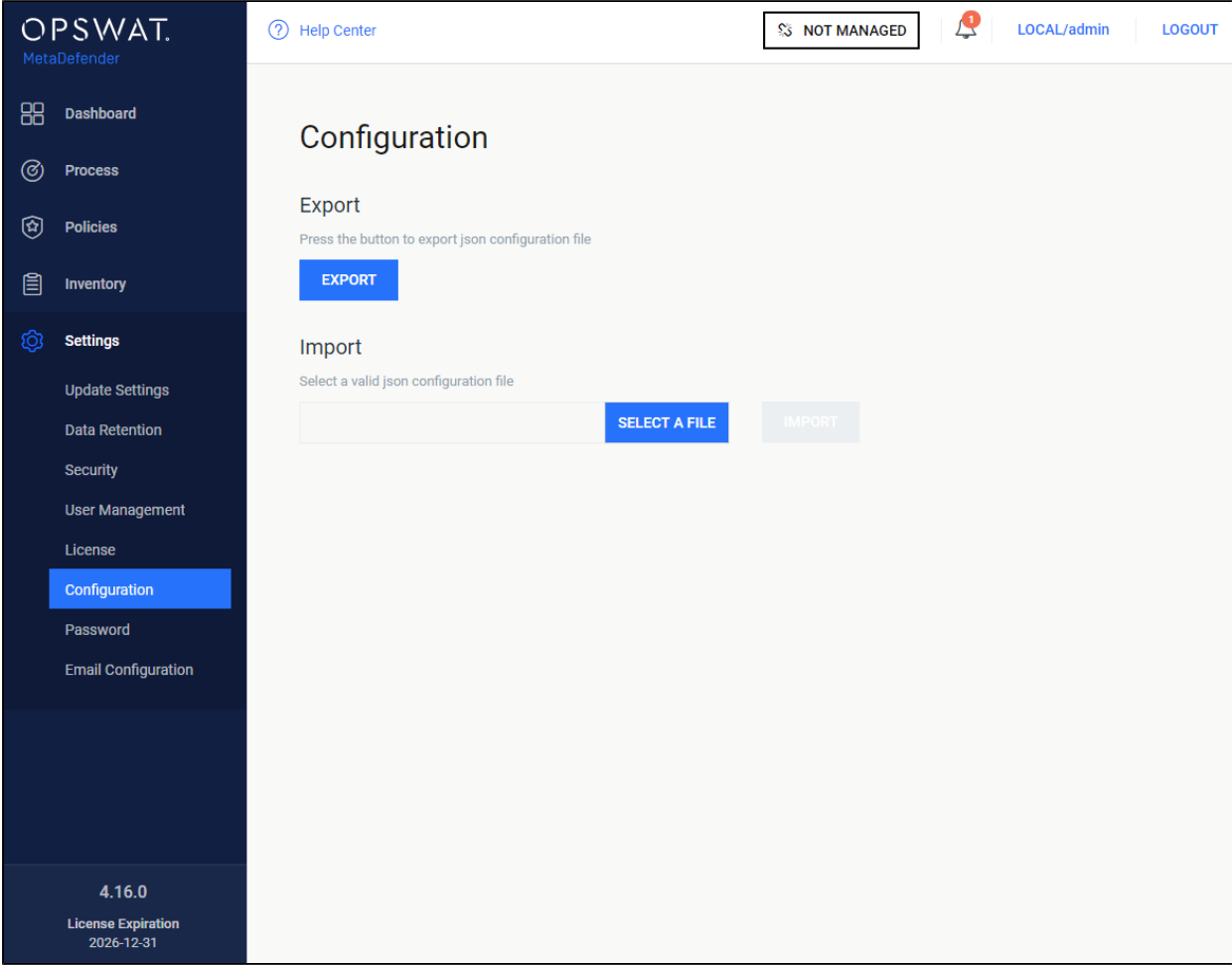
Checking Engines / Databases Health

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.

7.4 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.

7.5. Database Defragmentation and Optimization



Since MetaDefender Core 4.19.0 comes with PostgreSQL DBMS, the database defragmentation and optimization is performed silently in the background, thus the Maintenance UI page is deprecated since Core 4.19.0

When your scan database grows big, it might cause performance degradation (e.g. timeout on client requests).

Since MetaDefender Core 4.18.0, admin user will be notified on the UI (also in product logs) when the processing history database file size exceeds over 10 GB.

Admin user is supported to perform database maintenance including defragmentation and optimization without loss of actual scan data under **Settings > Maintenance page**. As a result, your database file size could be reduced which helps boost processing performance tremendously over usage time.

Caution: Please only use this feature when your entire scanning service is at rest.

Dashboard

Process

Policies

Inventory

Settings

[Update Settings](#)

[Data Retention](#)

[Maintenance **BETA**](#)

[Security](#)

[User Management](#)

[License](#)

[Reporting **BETA**](#)

[Configuration](#)

[Password](#)

[Email Configuration](#)

4.18.0

License Expiration
2026-12-31

Database Defragmentation and Optimization

Rebuild and optimize the processing history database which helps:

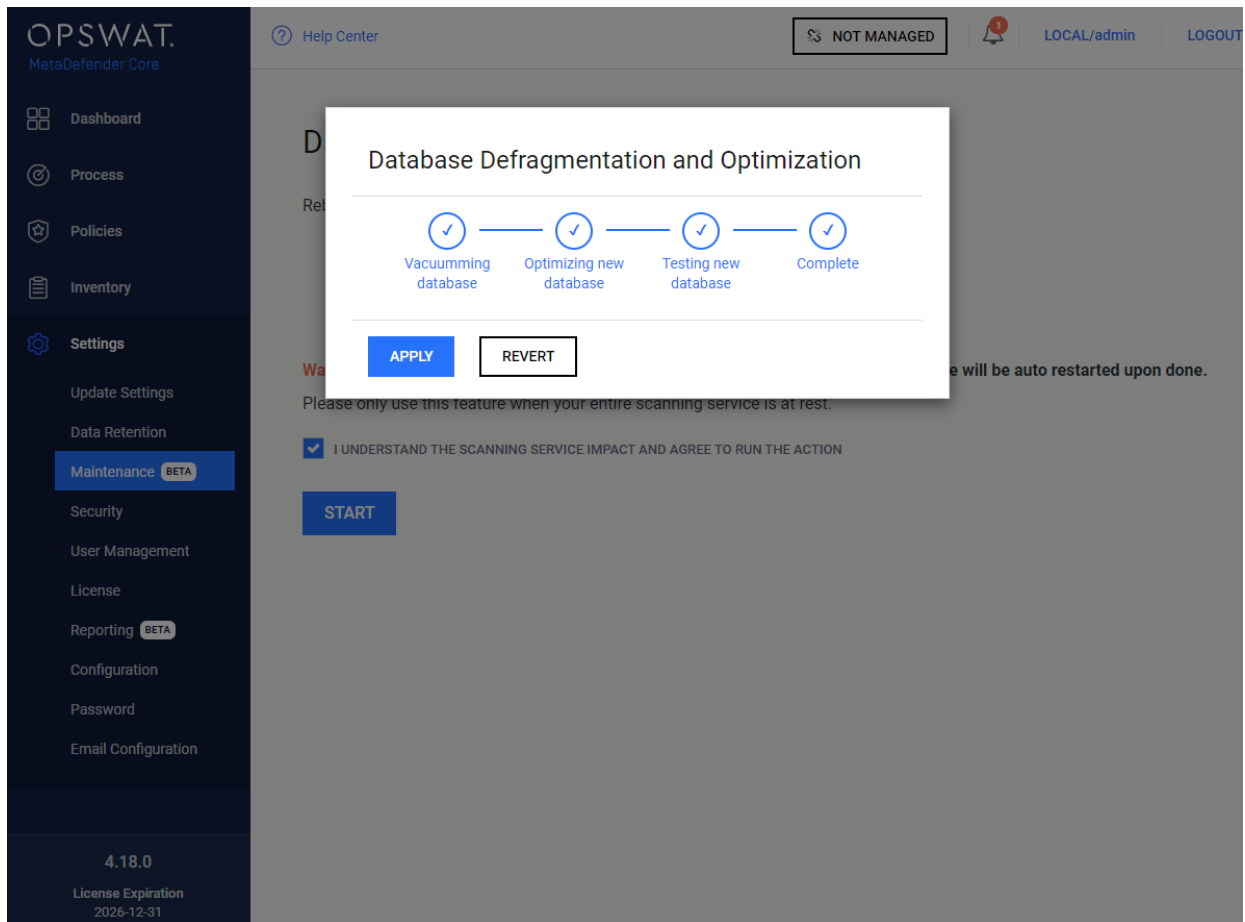
- Reduce database file size
- Improve data query time
- Improve file processing time

Warning! This action might take up to a few minutes, and the **MetaDefender Core service will be auto restarted upon done.**

Please only use this feature when your entire scanning service is at rest.

I UNDERSTAND THE SCANNING SERVICE IMPACT AND AGREE TO RUN THE ACTION

[START](#)



Hitting “APPLY” to apply all changes and restart MetaDefender Core service (or “REVERT” to roll back changes).

By default, only the “admin” user role can see this Maintenance page and make the changes, but you can configure to grant access to other user roles if desired.

The screenshot displays the OPSWAT MetaDefender Core interface. On the left is a dark sidebar with navigation options: Dashboard, Process, Policies, Inventory, Settings (with sub-options: Update Settings, Data Retention, Maintenance (BETA), Security, User Management, License, Reporting (BETA), Configuration, Password, Email Configuration), and version information (4.18.0, License Expiration 2026-12-31). The main content area is titled 'User Management' and contains a table of roles:

ROLENAME	DISPLAY NAME	NUMBER OF USERS	NUMBER OF DIRECTORIES
admin	Administr...	1	0
security_a...	Security a...	0	0
security_a...	Security a...	0	0
help_desk	Help desk	0	0

To the right of the table is a 'Modify role' panel with various settings and radio button options:

- Workflow templates: NONE, READ-ONLY, FULL (selected)
- Security zones: NONE, READ-ONLY, FULL (selected)
- Inventory:
 - Nodes: NONE, READ-ONLY, FULL (selected)
 - Modules: NONE, READ-ONLY, FULL (selected)
- External settings: NONE, READ-ONLY, FULL (selected)
- Skip by hash settings: NONE, READ-ONLY, FULL (selected)
- Certificates: NONE, READ-ONLY, FULL (selected)
- Settings:
 - Data retention: NONE (selected), READ-ONLY, FULL
 - Maintenance: NONE (selected), READ-ONLY, FULL
 - Reporting: NONE (selected), READ-ONLY, FULL
 - User management: NONE (selected), READ-ONLY, FULL
 - License: NONE (selected), READ-ONLY, FULL
 - Update settings: NONE, READ-ONLY, FULL (selected)
 - Scan settings: NONE, READ-ONLY, FULL (selected)
- API access:
 - Processing result fetching: NONE, SELF-ONLY, ANYONE (selected)
 - Download processed file: NONE, SELF-ONLY, ANYONE (selected)

At the bottom of the 'Modify role' panel are 'OK' and 'CANCEL' buttons.

7.6. Reporting

By enabling this feature in MetaDefender Core, you will help us gain more visibility on your processing load and how our product is being used, and thus we could improve our product to accommodate your use-case better.

MetaDefender Core will only report your processing statistics data and product configurations on a daily basis, we do not collect and report any of your sensitive data i.e. processed file names, user credentials.

You can disable this feature, or configure to select which information to collect, and what specific time the data to be collected in **Settings > Reporting** anytime.

OPSWAT. MetaDefender Core

Help Center

NOT MANAGED LOCAL/admin LOGOUT

Reporting

Daily reporting to OPSWAT servers to help OPSWAT gain more insight.
We do not collect any of your sensitive data (processed file names, user credentials etc.).

ENABLE REPORTING

SCHEDULED TIME TO SEND REPORT

03 : 00

INCLUDED INFORMATION TO SEND

- FILE SCANNED INFORMATION
- DEEP CDR INFORMATION
- PROACTIVE DLP INFORMATION
- VULNERABILITIES INFORMATION
- NODES INFORMATION
- ACTIVATION KEY

SAVE SETTINGS

4.18.0
License Expiration 2026-12-31

By default, only the “admin” user role can see this Maintenance page and make the changes, but you can configure to grant access to other user roles if desired.

OPSWAT. MetaDefender Core

Help Center

NOT MANAGED LOCAL/admin LOGOUT

User Management

ROLES

ROLENAME	DISPLAY NAME	NUMBER OF USERS	NUMBER OF DIRECTORIES
admin	Administr...	1	0
security_a...	Security a...	0	0
security_a...	Security a...	0	0
help_desk	Help desk	0	0

Modify role

- Workflow templates NONE READ-ONLY FULL
- Security zones NONE READ-ONLY FULL
- Inventory
 - Nodes NONE READ-ONLY FULL
 - Modules NONE READ-ONLY FULL
 - External settings NONE READ-ONLY FULL
 - Skip by hash settings NONE READ-ONLY FULL
 - Certificates NONE READ-ONLY FULL
- Settings
 - Data retention NONE READ-ONLY FULL
 - Maintenance NONE READ-ONLY FULL
 - Reporting NONE READ-ONLY FULL**
 - User management NONE READ-ONLY FULL
 - License NONE READ-ONLY FULL
 - Update settings NONE READ-ONLY FULL
 - Scan settings NONE READ-ONLY FULL
- API access
 - Processing result fetching NONE SELF-ONLY ANYONE
 - Download processed file NONE SELF-ONLY ANYONE

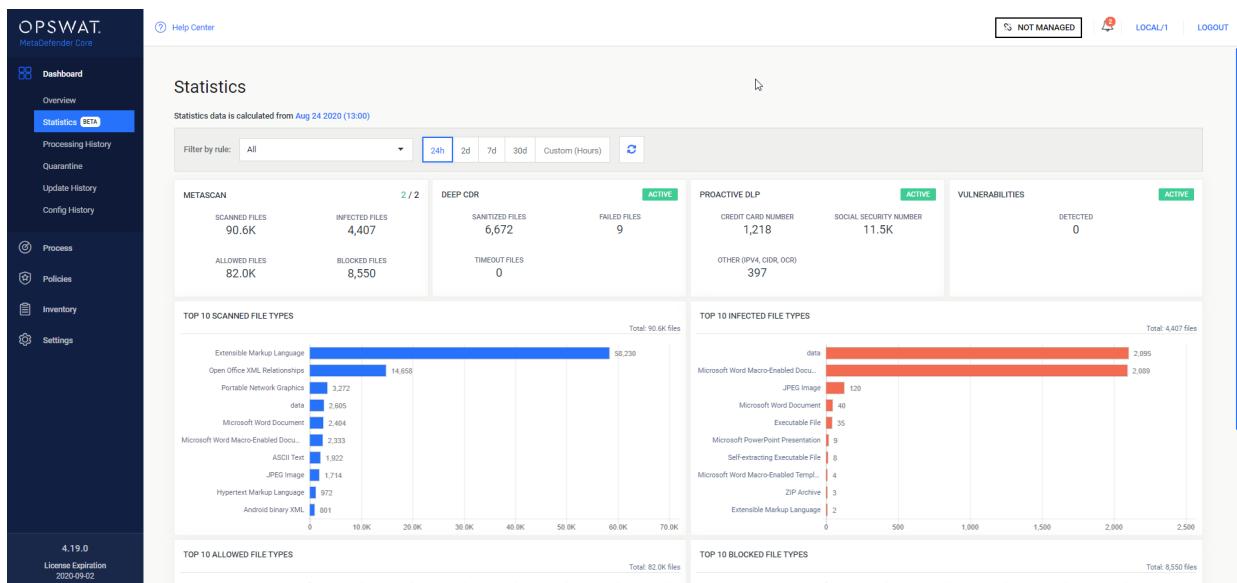
OK CANCEL

4.18.0
License Expiration 2026-12-31

7.7. Statistics

i Since MetaDefender Core 4.19.0, we have tremendously improved the calculation mechanism to boost up speed on the history processing statistics data, especially with big chunks of data with million historic records.

Featured in an interactive UI help you gain deeper insights on your processing filtered by every workflow rule, breaking down into each file type. You are also supported to select a time range to calculate statistics data.



Hitting “RELOAD” to enforce a full statistics data calculation against the newest processing data, otherwise, MetaDefender Core will try to load cached data (if existed).

8. 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: ([8.1.3.2. Fetch processing 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) ([8.1.3.2. Fetch processing result](#))



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

8.1. MetaDefender API

- [8.1.1. Sessions](#)
- [8.1.2. Licensing](#)

- [8.1.3. Processing files](#)
- [8.1.4. Processing files in batch](#)
- [8.1.5. Download Sanitized Files](#)
- [8.1.6. Vulnerability Info In Processing Result](#)
- [8.1.7. Skip by hash](#)
- [8.1.8. Get version of components](#)
- [8.1.9. Configuration related APIs](#)
- [8.1.10. Yara](#)
- [8.1.11. Webhooks](#)

8.1.1. Sessions

- [8.1.1.1. Login / Create a Session](#)
- [8.1.1.2. Logout / Destroy a Session](#)

8.1.1.1. 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.

8.1.1.2. 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.

8.1.2. Licensing

- [8.1.2.1. Activate License Online](#)
- [8.1.2.2. Uploading License Key File](#)
- [8.1.2.3. Get Current License Information](#)

8.1.2.1. 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 8.1.1.1. 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.

8.1.2.2. 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 [8.1.2.3. 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.

8.1.2.3. 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 8.1.1.1. 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.

8.1.3. Processing files

- [8.1.3.1. Process a file](#)
- [8.1.3.2. Fetch processing result](#)
- [8.1.3.3. Processing results](#)
- [8.1.3.4. Cancel a file processing](#)
- [8.1.3.5. Fetching available processing rules](#)

8.1.3.1. Process 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 [8.1.3.2. Fetch processing result](#).



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

Multipart form upload is not supported, instead please consider using batch submission [8.1.4. Processing files in batch](#)



Since MetaDefender Core 4.19.0, the request will be refused immediately with HTTP (S) error code 400 when MetaDefender Core does not have sufficient free disk space to handle. This is to avoid upload time being wasted.

Request	Value
Method	POST
URL	/file

Request HTTP header parameters:

name	type	required	value
apikey	string	false	

name	type	required	value
			Session id, can be acquired by 8.1.1.1. Login / Create a Session
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 8.1.3.5. Fetching available processing rules)
workflow	string	false	name of the selected workflow (deprecated, use "rule" header parameter instead)
archivepwd	string	false	<p>password for archive (URL encoded UTF-8 string)</p> <p>Multiple passwords is also supported, format: archivepwd<X></p> <ul style="list-style-type: none"> • X: Could be empty • When having value, X must be a number ≥ 1 <p>For example:</p> <p>archivepwd1: "fox"</p> <p>archivepwd2: "cow"</p> <p>archivepwd3: "bear"</p>
metadata	string (JSON format)	false	<p>could be utilized for:</p> <ul style="list-style-type: none"> • Additional parameter for pre-defined post actions and external scanners (as a part of STDIN input). • Customized macro variable for watermarking text (Proactive DLP engine feature).

name	type	required	value
			<ul style="list-style-type: none"> Additional context / verbose information for each file submission (appended into JSON response scan result). <p>For example: {"client_ip":"10.0.1.100", "custom_para":"ABC"}</p>
callbackurl	string (<protocol://><ip domain>:<port></path>)	false	<p>Client's URL where MetaDefender Core will notify scan result back to whenever scan is finished (webhooks model). See details at 8.1.11.1. Individual file processing</p> <p>Note: Support both non-secure (HTTP) and secured protocol (HTTPS). In case of secured protocol HTTPS, only TLS 1.2 or above is accepted by Core on the data transportation encryption between Core and remote server (client).</p> <p>For example:</p> <ul style="list-style-type: none"> http://10.0.1.100:8081/listenback https://test.yourdomain.io/webhook

Request body should contain the the content to be scanned.

Successful response

HTTP status code: 200

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

Error response

API key is invalid (only applicable when apikey header is sent)

HTTP status code: 400

```
{  
  "err": "Invalid apikey given"  
}
```

Callback URL is invalid (only applicable when callbackurl header is sent)

HTTP status code: 400

```
{  
  "err": "Callback url is invalid."  
}
```

Body data and filepath header are provided at the same time (only applicable when filepath header is sent)

HTTP status code: 400

```
{  
  "err": "Both body data and local file path were given."  
}
```

Internal error during processing batch (only applicable when callbackurl header is sent)

HTTP status code: 400

```
{  
  "err": "Can not scan in given batch."  
}
```

Batch is closed when file is not uploaded properly (only applicable when callbackurl header is sent)

HTTP status code: 400

```
{  
  "err": "Batch closed during file upload."  
}
```

Out of disk space for file upload request

HTTP status code: **400**

```
{  
  "err": "File upload denied due to insufficient disk space."  
}
```

Callbackurl header exists, but empty (only applicable when callbackurl header is sent)

HTTP status code: **403**

```
{  
  "err": "No callback url given."  
}
```

Content-Length header is missing from the request

HTTP status code: **411**

```
{  
  "err": "Missing Content-Length header"  
}
```

Body input is empty

HTTP status code: **422**

```
{  
  "err": "File is empty"  
}
```

Internal error

HTTP status code: **500**

```
{  
  "err": "Internal error"  
}
```

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

File size is larger than permitted maximum size

HTTP status code: **500**

```
{
  "err": "Failed to request scan. File size exceeded the
maximum size permitted by your configuration."
}
```

Need to perform local file scan, however, the file defined in filepath header is inaccessible (only applicable when filepath header is sent)

HTTP status code: **500**

```
{
  "err": "File not found, invalid path or access."
}
```

License has been expired

HTTP status code: **500**

```
{
  "err": "License is expired"
}
```

There's no rule for scanning

HTTP status code: **500**

```
{
  "err": "No available rule is present for scanning."
}
```

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.

8.1.3.2. Fetch processing result

- [8.1.3.2.1. Webhook mechanism](#)
- [8.1.3.2.2. Polling mechanism](#)
 - [8.1.3.2.2.1. Archive file result \(all child files in one response\)](#)
 - [8.1.3.2.2.2. Archive file result \(pagination fashion\)](#)

8.1.3.2.1. Webhook mechanism

Retrieving Analysis Reports Using Webhook

By providing a `callbackurl` header in the File submission request, once the analysis is complete, the entire analysis report will be automatically send to the `callbackurl`. No need for additional calls or polling mechanism to retrieve the analysis reports.

For more details, see:

- [8.1.3.1. Process a file](#)
- [8.1.11. Webhooks](#)

8.1.3.2.2. Polling mechanism

Retrieve Processing Results Using Data ID

Analysis is done asynchronously and each analysis request is tracked by a data ID. Initiating file analysis and retrieving the results need to be done using two separate API calls. This request needs to be made multiple times until the analysis is complete. Analysis completion can be traced using “process_info.progress_percentage” value from the response.

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

Retrieve Processing 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 8.1.3.5. Fetching available processing rules)
apikey	string	false	User's session id, if 8.1.3.1. Process a file has API key sent, then API key is required for fetching

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

Successful response

HTTP status code: 200

```

{
  "data_id": "8101abae27be4d63859c55d9e0ed0135",
  "dlp_info": {
    "certainty": "High",
    "errors": {

    },
    "filename": "OPSWAT_Proactive_DLP_CCN_proactive-dlp-processed_by_OPSWAT_MetaDefender_8101abae27be4d63859c55d9e0ed0135.pdf",
    "hits": {
      "ccn": {
        "display_name": "Credit Card Number",
        "hits": [
          {
            "after": "123 Cherry Lane st.",
            "before": "Card Number",
            "certainty": "Very High",
            "certainty_score": 100,
            "hit": "XXXXXXXXXXXXXXXX1938",
            "isRedacted": true,
            "severity": 0
          }
        ]
      },
      "ssn": {
        "display_name": "Social Security Number",
        "hits": [
          {
            "after": "",
            "before": "Social Security Number:",
            "certainty": "High",
            "certainty_score": 100,
            "hit": "XXXXXXX2315",
            "isRedacted": true,
            "severity": 0
          },
          {
            "after": "",
            "before": "• Your reference number is",
            "certainty": "Low",
            "certainty_score": 8,
            "hit": "XXXXX3578",
            "isRedacted": false,
            "severity": 0
          }
        ]
      }
    }
  },
}

```

```

"metadata_removal": {
  "result": "not removed"
},
"redact": {
  "result": "redacted"
},
"severity": 0,
"verdict": 1,
"watermark": {
  "result": "added"
}
},
"file_info": {
  "display_name": "OPSWAT_Proactive_DLP_CCN.pdf",
  "file_size": 75906,
  "file_type": "application/pdf",
  "file_type_description": "Adobe Portable Document Format",
  "md5": "c4863c8ce44fb7ae84eb48c9b78f8b5e",
  "sha1": "a33c72a996a9603d479e3dff3d23bf619c975fbe",
  "sha256": "b9fdc10b47950b9e503ef4dc0ef42d28e7c37ccd749d4a5dcd7
d9b3218996b7f",
  "upload_timestamp": "2020-03-12T08:37:05.412Z"
},
"process_info": {
  "blocked_reason": "Sensitive Data Found",
  "file_type_skipped_scan": false,
  "outdated_data": [
    "sanitization",
    "enginedefinitions"
  ],
  "post_processing": {
    "actions_failed": "",
    "actions_ran": "Sanitized",
    "converted_destination": "",
    "converted_to": "",
    "copy_move_destination": "",
    "sanitization_details": {
      "description": "Sanitized successfully.",
      "details": [
        {
          "action": "removed",
          "count": 2,
          "object_name": "hyperlink"
        }
      ],
      "sanitized_file_info": {
        "file_size": 2312,
        "sha256": "3603748179C79628AE4025E5252456286DC57FA7A42
0799B9EE268AFB884DB9E"
      }
    }
  ]
}
}

```



```

    },
    "processing_time": 4804,
    "profile": "File process",
    "progress_percentage": 100,
    "queue_time": 15,
    "result": "Blocked",
    "user_agent": "webscan",
    "username": "LOCAL/admin",
    "verdicts": [
        "Sensitive Data Found"
    ]
},
"scan_results": {
    "data_id": "8101abae27be4d63859c55d9e0ed0135",
    "progress_percentage": 100,
    "scan_all_result_a": "Sensitive Data Found",
    "scan_all_result_i": 20,
    "scan_details": {
        "ClamAV": {
            "def_time": "2020-03-11T11:08:00.000Z",
            "eng_id": "clamav_1_windows",
            "location": "local",
            "scan_result_i": 0,
            "scan_time": 336,
            "threat_found": "",
            "wait_time": 3
        }
    },
    "start_time": "2020-03-12T08:37:05.427Z",
    "total_avs": 1,
    "total_time": 4804
},
"vulnerability_info": {
    "verdict": 0
},
"yara_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
 - eng_id: the unique identification string for the 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
- username: user identifier who submitted scan request earlier
- 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 [8.1.6. Vulnerability Info In Processing Result](#)
- dlp_info: information on matched sensitive data
 - certainty: describes how certain the hit is, possible values:
 - Very Low

- Low
- Medium
- High
- Very High
- errors: a list of error objects (empty if no errors happened), each error object contains following keys:
 - scan: scan related error description
 - redact: redaction related error description
 - watermark: watermark related error description
 - metadata_removal: metadata removal related error description
- filename: output processed file name (pre-configured on engine settings under Core's workflow rule)
- 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
 - certainty: text version of "certainty_score", possible values:
 - Very Low
 - Low
 - Medium
 - High
 - Very High
 - certainty_score: is defined by the relevance of the given hit in its context. It is calculated based on multiple factors such as the number of digits, possible values: [0-100]
 - hit: the matched data
 - isRedacted: file was redacted or not

- severity (NOTE: this field is deprecated): can be 0 (detected) or 1 (suspicious)
- metadata_removal: result of metadata removal
 - result: result of the metadata removal process, possible values:
 - "removed"
 - "not removed"
 - "failed to remove"
- redact: result of redaction
 - result: result of the redaction process, possible values:
 - "redacted"
 - "not redacted"
 - "failed to redact"
- watermark: result of watermarking
 - results: result of the watermarking process, possible values:
 - "added"
 - "not added"
 - "failed to add"
- severity (NOTE: this field is deprecated): represents the severity of the data loss, possible values:
 - 0 - Certainly is data loss
 - 1 - Might be data loss
- 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)
- yara_info: information on data that matched yara rules
 - hits: detailed results that contains:
 - the name of the matched rules
 - a description

- verdict: the overall result for the scanned file.
 - 0 - clean
 - 1 - found matched data
 - 2 - suspicious
 - 3 - failed
 - 4 - not scanned

Please find possible overall and per engine scan results [here](#).

Response (not existing data_id)

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.

8.1.3.2.2.1. Archive file result (all child files in one response)



This endpoint API is not recommended to use against big archive file (contains numerous child files inside recursively), otherwise expecting to have performance degradation on the product.

It is highly recommended to use [8.1.3.2.2.2. Archive file result \(pagination fashion\)](#) instead.

Retrieving Analysis Reports Using Data ID containing all files in archive

Using this method under `extracted_files` key all the info about extracted files will be listed recursively.

Request	Value
Method	GET
URL	/archive/{data_id}

Successful response containing all extracted files

HTTP status code: 200

```
{
  "data_id": "8a8150d5b2aa4367be44f4a19c8dbb57",
  "dlp_info": {},
  "file_info": {
    "display_name": "testzip.zip",
    "file_size": 480,
    "file_type": "application/zip",
    "file_type_description": "ZIP Archive",
    "md5": "0197200212f86efb5ac23150feab45c0",
    "sha1": "084b89478b099a98971f62dc3aacbf3f7808d1a4",
    "sha256": "9f6e906a3c4c8581687a63fb768bca244081e9940dc43a07a9c
c6cb073e1a52a",
    "upload_timestamp": "2019-03-25T07:48:25.003Z"
  },
  "process_info": {
    "blocked_reason": "",
    "file_type_skipped_scan": false,
    "post_processing": {
      "actions_failed": "",
      "actions_ran": "",
      "converted_destination": "",
      "converted_to": "",
      "copy_move_destination": ""
    }
  },
  "processing_time": 79,
  "profile": "File process",
  "progress_percentage": 100,
  "queue_time": 3,
  "result": "Allowed",
  "user_agent": "webscan",
  "username": "LOCAL/admin",
  "verdicts": [
    "No Threat Detected"
  ]
}
```

```

},
"scan_results": {
  "data_id": "8a8150d5b2aa4367be44f4a19c8dbb57",
  "progress_percentage": 100,
  "scan_all_result_a": "No Threat Detected",
  "scan_all_result_i": 0,
  "scan_details": {},
  "start_time": "2019-03-25T07:48:25.006Z",
  "total_avs": 1,
  "total_time": 76
},
"vulnerability_info": {
  "verdict": 0
},
"yara_info": {},
"extracted_files": [
  {
    "data_id": "3b503f416ald40ffacf79a8141baale7",
    "dlp_info": {},
    "file_info": {
      "display_name": "test.zip",
      "file_size": 168,
      "file_type": "application/zip",
      "file_type_description": "ZIP Archive",
      "md5": "9a061b387f4d94babel3be5aa7c80077",
      "sha1": "b70a3bcaa67217b410211a8e6511c8f14b571ce1",
      "sha256": "1af488779d0fabf4b4bc7d920627d85c7256b4241bfda486cec6ba278eea1192",
      "upload_timestamp": "2019-03-25T07:48:25.013Z"
    },
    "process_info": {
      "blocked_reason": "",
      "file_type_skipped_scan": false,
      "post_processing": {
        "actions_failed": "",
        "actions_ran": "",
        "converted_destination": "",
        "converted_to": "",
        "copy_move_destination": ""
      },
      "processing_time": 69,
      "profile": "File process",
      "progress_percentage": 100,
      "queue_time": 5,
      "result": "Allowed",
      "user_agent": "webscan",
      "username": "LOCAL/admin",
      "verdicts": [
        "No Threat Detected"
      ]
    }
  },
],

```



```

"scan_results": {
  "data_id": "3b503f416ald40ffacf79a8141baale7",
  "progress_percentage": 100,
  "scan_all_result_a": "No Threat Detected",
  "scan_all_result_i": 0,
  "scan_details": {
    "ClamAV": {
      "def_time": "2019-03-24T08:46:29.000Z",
      "eng_id": "clamav_1_linux",
      "location": "local",
      "scan_result_i": 0,
      "scan_time": 3,
      "threat_found": "",
      "wait_time": 2
    }
  },
  "start_time": "2019-03-25T07:48:25.018Z",
  "total_avs": 1,
  "total_time": 55
},
"vulnerability_info": {
  "verdict": 0
},
"yara_info": {},
"extracted_files": [
  {
    "data_id": "1014ec91e0b246489fa357ce1d02f8b1",
    "dlp_info": {},
    "file_info": {
      "display_name": "test.txt",
      "file_size": 2,
      "file_type": "text/plain",
      "file_type_description": "ASCII text",
      "md5": "60b725f10c9c85c70d97880dfe8191b3",
      "sha1": "3f786850e387550fdab836ed7e6dc881de23001b",
      "sha256": "87428fc522803d31065e7bce3cf03fe475096631e5e
07bbd7a0fde60c4cf25c7",
      "upload_timestamp": "2019-03-25T07:48:25.025Z"
    },
    "process_info": {
      "blocked_reason": "",
      "file_type_skipped_scan": false,
      "post_processing": {
        "actions_failed": "",
        "actions_ran": "",
        "converted_destination": "",
        "converted_to": "",
        "copy_move_destination": ""
      },
      "processing_time": 47,
      "profile": "File process",

```

```

        "progress_percentage": 100,
        "queue_time": 4,
        "result": "Allowed",
        "user_agent": "webscan",
        "username": "LOCAL/admin",
        "verdicts": [
            "No Threat Detected"
        ]
    },
    "scan_results": {
        "data_id": "1014ec91e0b246489fa357ce1d02f8b1",
        "progress_percentage": 100,
        "scan_all_result_a": "No Threat Detected",
        "scan_all_result_i": 0,
        "scan_details": {
            "ClamAV": {
                "def_time": "2019-03-24T08:46:29.000Z",
                "eng_id": "clamav_1_linux",
                "location": "local",
                "scan_result_i": 0,
                "scan_time": 0,
                "threat_found": "",
                "wait_time": 4
            }
        },
        "start_time": "2019-03-25T07:48:25.029Z",
        "total_avs": 1,
        "total_time": 35
    },
    "vulnerability_info": {
        "verdict": 0
    },
    "yara_info": {}
}
]
},
{
    "data_id": "a80f3b43192843f28998abcfe073c3be",
    "dlp_info": {},
    "file_info": {
        "display_name": "test.txt",
        "file_size": 2,
        "file_type": "text/plain",
        "file_type_description": "ASCII text",
        "md5": "60b725f10c9c85c70d97880dfe8191b3",
        "sha1": "3f786850e387550fdab836ed7e6dc881de23001b",
        "sha256": "87428fc522803d31065e7bce3cf03fe475096631e5e07bb
d7a0fde60c4cf25c7",
        "upload_timestamp": "2019-03-25T07:48:25.012Z"
    },
    "process_info": {

```

```

    "blocked_reason": "",
    "file_type_skipped_scan": false,
    "post_processing": {
      "actions_failed": "",
      "actions_ran": "",
      "converted_destination": "",
      "converted_to": "",
      "copy_move_destination": ""
    },
    "processing_time": 33,
    "profile": "File process",
    "progress_percentage": 100,
    "queue_time": 3,
    "result": "Allowed",
    "user_agent": "webscan",
    "username": "LOCAL/admin",
    "verdicts": [
      "No Threat Detected"
    ]
  },
  "scan_results": {
    "data_id": "a80f3b43192843f28998abcfe073c3be",
    "progress_percentage": 100,
    "scan_all_result_a": "No Threat Detected",
    "scan_all_result_i": 0,
    "scan_details": {
      "ClamAV": {
        "def_time": "2019-03-24T08:46:29.000Z",
        "eng_id": "clamav_1_linux",
        "location": "local",
        "scan_result_i": 0,
        "scan_time": 0,
        "threat_found": "",
        "wait_time": 1
      }
    },
    "start_time": "2019-03-25T07:48:25.015Z",
    "total_avs": 1,
    "total_time": 23
  },
  "vulnerability_info": {
    "verdict": 0
  },
  "yara_info": {}
}
]
}

```

Using this method the following fields will not be shown compared to /file request containing extracted files

- files_extracted_count
- files_in_archive
- first_index
- page_size
- worst_data_id

Also the "outdated_data" field will only be shown in the root archive.

Response (not existing data_id)

HTTP status code: 200

```
{
  "61dfffeaa728844adbf49eb090e4ece0e": "Not Found"
}
```

Response (requested file is not an archive)

HTTP status code: 200

```
{
  "61dfffeaa728844adbf49eb090e4ece0e": "Invalid request"
}
```

Error response

Unexpected event on server

HTTP status code: 500

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

8.1.3.2.2.2. Archive file result (pagination fashion)

Request	Value
Method	GET
URL	/file/{data_id}?first={start_item}&size={number_of_items_next}

Request HTTP header parameters

name	type	required	value
rule	string	false	the name is the desired rule to query for (see 8.1.3.5. Fetching available processing rules)
apikey	string	false	User's session id, if 8.1.3.1. Process a file has API key sent, then API key is required for fetching
first	number	true	The first item order in the list child files of archive file
size	number	true	The number of items to be fetched next, counting from the item order indicated in <code>first</code> header

Successful response with archive detection

HTTP status code: 200

```
{
  "data_id": "d7016058f0874d12b98a8c1ece9d3ea9",
  "dlp_info": {...},
  "extracted_files": {
    "files_extracted_count": 2,
    "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",
        "process_info": {
          "blocked_reason": "",
          "progress_percentage": 100,
          "result": "Allowed"
        },
        "progress_percentage": 100,
        "scan_all_result_a": "Whitelisted",
        "scan_all_result_i": 7,
        "scanned_with": 0
      },
      {
        "data_id": "7cb298eb42614ca9bc87a4de4acad436",
        "detected_by": 2,
```

```

        "display_name": "samplezip.tar.gz/[Content]
/samplezip/eicar",
        "file_size": 69,
        "file_type": "text/plain",
        "file_type_description": "EICAR virus test files",
        "process_info": {
            "blocked_reason": "Infected",
            "progress_percentage": 100,
            "result": "Blocked"
        },
        "progress_percentage": 100,
        "scan_all_result_a": "Infected",
        "scan_all_result_i": 1,
        "scanned_with": 2
    },
    ],
    "first_index": 0,
    "page_size": 20,
    "worst_data_id": "7cb298eb42614ca9bc87a4de4acad436"
},
"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": "6ec5e258141528f004a43f7d25163a1c7486df76fde7976
a793b140b11eda95d",
    "upload_timestamp": "2015-08-14T12:46:59.360Z"
},
"scan_results": {
    "last_file_scanned": "eicar",
    "data_id": "d7016058f0874d12b98a8c1ece9d3ea9",
    "progress_percentage": 100,
    "scan_all_result_a": "Infected",
    "scan_all_result_i": 1,
    "scan_details": {
        "Engine1": {
            "def_time": "2015-08-13T09:32:48.000Z",
            "eng_id": "engine1_1_linux",
            "location": "local",
            "scan_result_i": 0,
            "scan_time": 1,
            "wait_time": 3,
            "threat_found": ""
        },
        "Engine2": {
            "def_time": "2015-08-10T00:00:00.000Z",
            "eng_id": "engine2_1_linux",
            "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": {
    "blocked_reason": "Infected",
    "file_type_skipped_scan": false
    "outdated_data": [
        "enginedefinitions"
    ],
    "post_processing": {
        "actions_ran": "",
        "actions_failed": "",
        "converted_to": "",
        "copy_move_destination": "",
        "converted_destination": ""
    },
    "processing_time": 400,
    "progress_percentage": 100,
    "user_agent": "webscan",
    "username": "LOCAL/admin",
    "profile": "File scan",
    "queue_time": 20,
    "result": "Blocked",
},
"vulnerability_info": {...},
"yara_info": {...}
}

```

Completed response description with archive detection:

- **extracted_files**: information about extracted files
 - **files_extracted_count**: the number of extracted files
 - **files_in_archive**: array of files in archive
 - **detected_by**: number of engines reported threat
 - **scanned_with**: number of engines used for scanning the file
 - **first_index**: it tells that from which file (index of the file, 0 is the first) the result JSON contains information about extracted files. (default=0)

- `page_size`: it tells how many files the result JSON contains information about (default=20). So by default, the result JSON contains information about the first 20 extracted files.
- `worst_data_id`: data id of the file that has the worst result in the archive
- `scan_results`
 - `last_file_scanned` (stored only in memory, not in database): If available, the name of the most recent processed file

Please find complete scan result at [8.1.3.2.2. Polling mechanism](#)

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.

8.1.3.3. Processing results

Possible overall and per engine scan results

scan_result_a	scan_result_i
No Threat Detected	0
Infected	1
Suspicious	2
Failed	3

scan_result_a	scan_result_i
Cleaned / Deleted	4
Scan Skipped - Whitelisted	7
Scan Skipped - Blacklisted	8
Exceeded Archive Depth	9
Not Scanned	10
Encrypted Archive	12
Exceeded Archive Size	13
Exceeded Archive File Number	14
Password Protected Document	15
Exceeded Archive Timeout	16
File type Mismatch	17
Potentially Vulnerable File	18
Canceled	19
Sensitive data found	20
Yara Rule Matched	21
Potentially Unwanted Program	22
Unsupported file type	23
In Progress	255

8.1.3.4. Cancel a file processing

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>
}
```

8.1.3.5. Fetching available processing rules

The response is an array of available rules

Request	Value	Note
Method	GET	
URL	/file/rules	
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, or2. 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.

8.1.4. Processing files in batch

- [8.1.4.1 Initiate Batch](#)
- [8.1.4.2. Scan file in batch](#)
- [8.1.4.3. Status of Batch](#)
- [8.1.4.4. Close Batch](#)
- [8.1.4.5. Download Batch Signed Result](#)
- [8.1.4.6. Cancel Batch](#)

8.1.4.1 Initiate Batch

Initiate Scan Batch

Url	/file/batch
Method	POST

Request HTTP header parameters:

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

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>
}
```

8.1.4.2. 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 [8.1.3.1. Process a file](#):

Header	Description
batch (OPTIONAL)	Batch id to scan with, coming from 8.1.4.1 Initiate Batch (If it is not given, it will be a single file scan.)
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)

8.1.4.3. Status of Batch

Status of Scan Batch

Url	/file/batch/<batch_id>
Method	GET

Header	Description
apikey (OPTIONAL)	User's session id, if API key header set on 8.1.4.1 Initiate Batch , then it is required

Result Code	Description
200	Batch status given successfully

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

HTTP status code: 200

Note that "files_in_batch" list maximum 50 results by default, and it is pagination controlled by "first" and "size" parameter.

For example: /file/batch/<batch_id>/first=50&size=100

```
{
  "batch_files": {
    "batch_count": 4,
    "files_in_batch": [
      {
        "data_id": "24c8b5dadd48445989ac3431544fdc34",
        "detected_by": 4,
        "display_name": "eicar.com",
        "file_size": 68,
        "file_type": "application/octet-stream",
        "file_type_description": "EICAR virus test files",
        "process_info": {
          "blocked_reason": "Infected",
          "progress_percentage": 100,
          "result": "Blocked",
          "verdicts": [
            "Infected"
          ]
        },
        "progress_percentage": 100,
        "scan_all_result_a": "Infected",
        "scan_all_result_i": 1,
        "scanned_with": 4
      },
      {
        "data_id": "4bfb5dfff13084d909f1afc97353cfca8",
        "detected_by": 0,
        "display_name": "windows-database.yml",
        "file_size": 2205,
```

```

"file_type":"text/plain",
"file_type_description":"ASCII Text",
"process_info":{
  "blocked_reason":"",
  "progress_percentage":100,
  "result":"Allowed",
  "verdicts":[
    "No Threat Detected"
  ]
},
"progress_percentage":100,
"scan_all_result_a":"No Threat Detected",
"scan_all_result_i":0,
"scanned_with":4
},
{
"data_id":"cdab9c5089994091babe5a1fc16e5a69",
"detected_by":0,
"display_name":"ChromeSetup.exe",
"file_size":1214008,
"file_type":"application/x-dosexec",
"file_type_description":"Executable File",
"process_info":{
  "blocked_reason":"",
  "progress_percentage":100,
  "result":"Allowed",
  "verdicts":[
    "No Threat Detected"
  ]
},
"progress_percentage":100,
"scan_all_result_a":"No Threat Detected",
"scan_all_result_i":0,
"scanned_with":4
},
{
"data_id":"8c29974a819d41eb8c5c9a9418e0d600",
"detected_by":0,
"display_name":"install-2.4.4.exe",
"file_size":3476784,
"file_type":"application/x-dosexec",
"file_type_description":"Self-extracting Executable
File",
"files_extracted_count":50,
"process_info":{
  "blocked_reason":"",
  "progress_percentage":100,
  "result":"Allowed",
  "verdicts":[
    "No Threat Detected"
  ]
}

```



```

        },
        "progress_percentage":100,
        "scan_all_result_a":"No Threat Detected",
        "scan_all_result_i":0,
        "scanned_with":4
    }
],
"first_index":0,
"page_size":50
},
"batch_id":"b7cc760038324b02908a5c111cb1563d",
"is_closed":false,
"process_info":{
    "blocked_reason":"Infected",
    "file_type_skipped_scan":false,
    "profile":"File process",
    "result":"Blocked",
    "user_agent":"mdicapserver",
    "username": "LOCAL/admin"
},
"scan_results":{
    "batch_id":"b7cc760038324b02908a5c111cb1563d",
    "scan_all_result_a":"Infected",
    "scan_all_result_i":1,
    "start_time":"2019-07-29T12:19:46.118Z",
    "total_avs":0,
    "total_time":18403
},
"user_data":"http://localhost:8008/"
}

```

HTTP status code: 500, 403, 400

```

{
    "err": <error message>
}

```

8.1.4.4. 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**

Note that "files_in_batch" list maximum 50 results by default, and it is pagination controlled by "first" and "size" parameter.

For example: /file/batch/<batch_id>/first=50&size=100

```
{
  "batch_files": {
    "batch_count": 4,
    "files_in_batch": [
      {
        "data_id": "24c8b5dadd48445989ac3431544fdc34",
        "detected_by": 4,
        "display_name": "eicar.com",
        "file_size": 68,
        "file_type": "application/octet-stream",
        "file_type_description": "EICAR virus test files",
        "process_info": {
          "blocked_reason": "Infected",
          "progress_percentage": 100,
          "result": "Blocked",
          "verdicts": [
            "Infected"
          ]
        }
      }
    ]
  }
}
```

```

    },
    "progress_percentage":100,
    "scan_all_result_a":"Infected",
    "scan_all_result_i":1,
    "scanned_with":4
  },
  {
    "data_id":"4bfb5dff13084d909f1afc97353cfca8",
    "detected_by":0,
    "display_name":"windows-database.yml",
    "file_size":2205,
    "file_type":"text/plain",
    "file_type_description":"ASCII Text",
    "process_info":{
      "blocked_reason":"",
      "progress_percentage":100,
      "result":"Allowed",
      "verdicts":[
        "No Threat Detected"
      ]
    },
    "progress_percentage":100,
    "scan_all_result_a":"No Threat Detected",
    "scan_all_result_i":0,
    "scanned_with":4
  },
  {
    "data_id":"cdab9c5089994091babe5a1fc16e5a69",
    "detected_by":0,
    "display_name":"ChromeSetup.exe",
    "file_size":1214008,
    "file_type":"application/x-dosexec",
    "file_type_description":"Executable File",
    "process_info":{
      "blocked_reason":"",
      "progress_percentage":100,
      "result":"Allowed",
      "verdicts":[
        "No Threat Detected"
      ]
    },
    "progress_percentage":100,
    "scan_all_result_a":"No Threat Detected",
    "scan_all_result_i":0,
    "scanned_with":4
  },
  {
    "data_id":"8c29974a819d41eb8c5c9a9418e0d600",
    "detected_by":0,
    "display_name":"install-2.4.4.exe",
    "file_size":3476784,

```

```

        "file_type": "application/x-dosexec",
        "file_type_description": "Self-extracting Executable
File",
        "files_extracted_count": 50,
        "process_info": {
            "blocked_reason": "",
            "progress_percentage": 100,
            "result": "Allowed",
            "verdicts": [
                "No Threat Detected"
            ]
        },
        "progress_percentage": 100,
        "scan_all_result_a": "No Threat Detected",
        "scan_all_result_i": 0,
        "scanned_with": 4
    }
],
    "first_index": 0,
    "page_size": 50
},
"batch_id": "b7cc760038324b02908a5c111cb1563d",
"is_closed": false,
"process_info": {
    "blocked_reason": "Infected",
    "file_type_skipped_scan": false,
    "profile": "File process",
    "result": "Blocked",
    "user_agent": "mdicapserver",
    "username": "LOCAL/admin"
},
"scan_results": {
    "batch_id": "b7cc760038324b02908a5c111cb1563d",
    "scan_all_result_a": "Infected",
    "scan_all_result_i": 1,
    "start_time": "2019-07-29T12:19:46.118Z",
    "total_avs": 0,
    "total_time": 18403
},
"user_data": "http://localhost:8008/"
}

```

HTTP status code: 500, 403, 400

```

{
    "err": <error message>
}

```

8.1.4.5. 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)
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_shal_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
```



```

6T2pGZrwbQuiFGrGTMZOvWMSpQtNl+tCCXlT4mWqJDRwuMGrI4DnnGzt3IKqNws4
Qyo9KqjMIPwnXZAmWpm3FOKe4sFwc5fpawKO01JZewDsYTDxVj+cwXwFxbE2yBiF
z2FAHwfopwaH35p3C6lkcgp2k/zgAlnBluzACUI+MKJ/G0gv/uAhj1OHJQ3L6kn1
SpvQ41/ueBjlunExqQSYD7GtZ1Kg8uOcq2r+WISE3Qc9MpQFFkUVl1mgWGwYDuN3
Zsez95kCAwEAAa7MHkwCQYDVR0TBAlwADAsBg1ghkgBhvhCAQ0EHxYdT3BlblNT
TCBHZW51cmF0ZWQgQ2VydG1maWNhdGUwHQYDVR0OBBYEFFlfyRO6G8y5qEFKik15
ajb2ft7XMB8GA1UdIwQYMBaAFcNsLT0+KV14uGw+quK7Lh5sh/JTMA0GCSqGSIb3
DQEBBQUAA4ICAQAT5wJFPqervbja5+90iKxild0QVtVGB+z6aoAMuWK+ggi0vgvr
mu9ot2lvTSCSnRhjeiP0SIdqFMORmBtOCfk/kYDp9M/91b+vS+S9eAlxrNCB5VOF
PqxEPp/wvlrBcE4GBO/c6HcFon3F+oBYCsUQbZDKSSZxhDm3mj7pb67FNbZbJIzJ
70HDsRe2004oiTx+h6g6pW3cOQMgIAvFgKN5Ex727K4230B0NidGkzuj4KSML0NM
s1SAcXZ410oSKNjy44BVEzv0ZdxTDrRM4EwJtNyggFzmtTuV02nkUj1bYYC5f0L
ADr6s0XMyaNk8twlWY1YDZ5uKDPVRVbfIGcQ0uJIzIvemhuTrofh8pBQQNkPRDFT
RqliTo1Ihh13/F11kXk1WR3jTjNb4jHX71IoXwpwp767HAPKGhjQ9cFbnHMETkro
RlJYdtRq5mccDtwT0GFyoJLLBZdHMHJz0F9H7FNk2tTQQMhK5MVYwg+LIaee586
CQVqfbscp7evlgjLW98H+5zylRHAgO2G79aHljNKmp9BOuq6SnEglEsiWGVtu2l
hnx8SB3sVJZHeer8f/UQQwqbAO+Kdy70NmbSaqaVtp8jOxLiidWkwSyRTsuU6D8i
DiH5uEqBXExjrj0FslxcVKdVj5glVcSmkLwZKbEU1OKwleT/iXFhvooWhQ==
-----END CERTIFICATE-----

```

...

HTTP status code: 500, 403, 400

```

{
  "err": <error message>
}

```

8.1.4.6. 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>
}
```

8.1.5. 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 [8.1.3.1. Process a file](#). In case of sanitizing the content of an archive, the data_id of contained file can be found in [8.1.3.2. Fetch processing result](#).

Request HTTP header parameters:

name	type	required	value
apikey	string	false	Session id, can be acquired by Login / Create a Session If API key was set on 8.1.3.1. Process a file then it is required

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.

8.1.6. Vulnerability Info In Processing 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

8.1.7. Skip by hash

- [8.1.7.1. Get 'skip by hash' list](#)
- [8.1.7.2. Modify 'skip by hash' list](#)

8.1.7.1. Get 'skip by hash' list

Fetching whitelist

The response containing the whitelist, blacklist and skip engine rules;

Request	Value
Method	GET
URL	/admin/config/skip

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**

```
{
  "blacklist": {
    "edecbf6bd03ef340e0c6cd438a4069c2": {
      "comment": "example3"
    }
  },
  "skip": {
    "13d8b8329bd2f668e6a889f32feaa48c832dbf0c": {
      "comment": "example4",
      "engines": [
        "totaldefense"
      ]
    },
    "7f6cf37bd817f2c7572f5467578d38bb4dc7080b": {
      "comment": "Example1",
      "engines": [
        "eset",
        "clamav"
      ]
    }
  },
  "whitelist": {
    "6e340b9cffb37a989ca544e6bb780a2c78901d3fb33738768511a30617afa01d": {
      "comment": "example5"
    }
  }
}
```

```
      "df72d035b31b1ff89f752e83af14b9e9dcf4913d9954f074546860d10b690
8fb": {
  "comment": "example2"
}
}
```

The response contains three objects: blacklist, whitelist, skip. Each object represents a list of hashes (md5, sha1 or sha256) and the corresponding information.

Skip: comment, engines(array)

Whitelist and Blacklist: comment

Error response

Internal error

HTTP status code: 404

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

Invalid api key or rights

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.

8.1.7.2. Modify 'skip by hash' list

The API for change of the "skip by hash"

Request	Value
Method	PUT
URL	/admin/config/skip

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
skip	object	true	Contains a hash object that contains a comment and an array of the engines to be skipped
blacklist	object	true	

Example:

```
{
  "blacklist": {
    "edecbf6bd03ef340e0c6cd438a4069c2": {
      "comment": "example3"
    }
  },
  "skip": {
    "13d8b8329bd2f668e6a889f32feaa48c832dbf0c": {
      "comment": "example4",
      "engines": [
        "totaldefense"
      ]
    },
    "7f6cf37bd817f2c7572f5467578d38bb4dc7080b": {
      "comment": "Example1",
      "engines": [
```



```

        "eset",
        "clamav"
    ]
  },
  "whitelist": [
    {
      "hash": "6e340b9cffb37a989ca544e6bb780a2c78901d3fb33738768511a30617afa01d",
      "comment": "example5"
    },
    {
      "hash": "df72d035b31b1ff89f752e83af14b9e9dcf4913d9954f074546860d10b6908fb",
      "comment": "example2"
    }
  ]
}

```

The request body containing whitelist's rules in array under "whitelist" key;

Each object in the array represents a whitelist:

comment: same comment for detailed more information this whitelist settings.

engines: containing engine id's strings in array

hash: md5, sha1 or sha256 hash

Successful response

HTTP status code: **200**

```

{
  "blacklist": [
    {
      "hash": "edecbf6bd03ef340e0c6cd438a4069c2",
      "comment": "example3"
    }
  ],
  "skip": [
    {
      "hash": "13d8b8329bd2f668e6a889f32feaa48c832dbf0c",
      "comment": "example4",
      "engines": [
        "totaldefense"
      ]
    },
    {
      "hash": "7f6cf37bd817f2c7572f5467578d38bb4dc7080b",
      "comment": "Example1",
      "engines": [
        "eset",
        "clamav"
      ]
    }
  ]
}

```

```
"whitelist": {
  "6e340b9cffb37a989ca544e6bb780a2c78901d3fb33738768511a30617afa
01d": {
  "comment": "example5"
  },
  "df72d035b31b1ff89f752e83af14b9e9dcf4913d9954f074546860d10b690
8fb": {
  "comment": "example2"
  }
}
```

The response returned the modified whitelist

Each object in the array represents a whitelist:

comment: same comment for detailed more information this whitelist settings.

engines: containing engine id's strings in array

hash: md5, sha1 or sha256 hash

Error response

Internal error

HTTP status code: 404

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

Invalid api key or rights

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.

8.1.8. Get version of components

- [8.1.8.1. Fetching Engine / Database Versions](#)
- [8.1.8.2. Get Product Version](#)

8.1.8.1. 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>"  
}
```

8.1.8.2. Get Product Version

Fetch details about the product version.

Request	Value
Method	GET
URL	/version

Successful response

HTTP status code: **200**

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

Error response

Unexpected event on server

HTTP status code: **500**

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

Note: Check Metadefender Core server logs for more information.

8.1.9. Configuration related APIs



All APIs below require authentication. You must send your **apikey** in header parameter.

```
apikey:<your_unique_apikey>
```

- Processing history clean up
- Quarantine clean up
- Audit records (update history) clean up
- Sanitized file clean up
- Update settings
 - Explanation
- Default settings
- Roles
- Users
- Import
- Update
- Change password
- Nodes
- Engines
- Pin engine to prevent auto-updates
- Unpin engine to apply auto-updates
- Enable engines
- Disable engines
- Session settings
- Webhook configurations - Retrieval
- Webhook configurations - Modification

Processing history clean up

(cleanup records older than)

PUT /admin/config/scanhistory

Properties

Property	Value
DESCRIPTION	Setting processing history cleanup time. The cleanup range is defined in hours .

Property	Value
URL	http://<server>:<port>/admin/config/scanhistory
REQUIRED RIGHTS	retention: [read, write]
HTTP METHOD	PUT
CONTENT TYPE	json
BODY	<pre>{"cleanuprange": 24}</pre>

Response

Result code	Value	Description
200	<pre>{ "cleanuprange": 24 }</pre>	Request processed successfully.
403		The apikey is missing or invalid.

Result code	Value	Description
	<pre>{ "error": "Access denied"} </pre>	
405	<pre>{ "error": "Access denied"} </pre>	The user has no rights for this operation.

Result code	Value	Description
	<pre> d " } </pre>	
500	<pre> { " e r r " : " E r r o r w h i l e m o d i f y i n g c o n f i g u r a t i o n </pre>	Internal server error.

Result code	Value	Description
	<pre>" }</pre>	

Quarantine clean up

(cleanup records older than)

PUT /admin/config/quarantine

Properties

Property	Value
DESCRIPTION	Setting quarantine cleanup time. The cleanup range is defined in hours .
URL	http://<server>:<port>/admin/config/quarantine
REQUIRED RIGHTS	retention: [read, write]
HTTP METHOD	PUT
CONTENT TYPE	json
BODY	<pre>{"cleanuprange" : 24}</pre>

Response

Result code	Value	Description
200	<pre>{ " c l e a</pre>	Request processed successfully.

Result code	Value	Description
	<pre> n u p p r a n g e " : 2 4 } </pre>	
403	<pre> { " e r r " : " A c c e s s d e n i e d " } </pre>	The apikey is missing or invalid.
405	<pre> { " e r r " : " A c c e s s d e n i e d " } </pre>	The user has no rights for this operation.

Result code	Value	Description
	<pre> r : " A c c e s s d e n i e d " } </pre>	
500	<pre> { " e r r " : " E r r o r w h i l e m o d i f y i </pre>	Internal server error.

Result code	Value	Description
	<pre> ngconfiguration " } </pre>	

Audit records (update history) clean up

(cleanup record older than)

PUT /admin/config/auditlog

Properties

Property	Value
DESCRIPTION	Setting audit records (update history) cleanup time. The cleanup range is defined in hours .
URL	http://<server>:<port>/admin/config/auditlog
REQUIRED RIGHTS	retention: [read, write]
HTTP METHOD	PUT
CONTENT TYPE	json
BODY	<pre> {"cleanupprange" : 24} </pre>

Response

Result code	Value	Description
200	<pre>{ "cleanuptime": 24 }</pre>	Request processed successfully.
403	<pre>{ "error": "Access denied"</pre>	The apikey is missing or invalid.

Result code	Value	Description
	<pre>{ d }</pre>	
405	<pre>{ "error": "Access denied" }</pre>	The user has no rights for this operation.
500	<pre>{ "error": "Error" }</pre>	Internal server error.

Result code	Value	Description
	<pre> h i l l e m o d i f y i n g c o n f i g u r a t i o n " } </pre>	

Sanitized file clean up

(cleanup records older than)

PUT /admin/config/sanitize

Properties

Property	Value
DESCRIPTION	Setting sanitized files cleanup time. The cleanup range is defined in minutes .
URL	http://<server>:<port>/admin/config/sanitize

Property	Value
REQUIRED RIGHTS	retention: [read, write]
HTTP METHOD	PUT
CONTENT TYPE	json
BODY	<pre>{ "maxage" : 360 }</pre>

Response

Result code	Value	Description
200	<pre>{ "maxage" : 360 }</pre>	Request processed successfully.
403	<pre>{ "error" : " A</pre>	The apikey is missing or invalid.

Result code	Value	Description
	<pre> { "access_denied": } </pre>	
405	<pre> { "error": : "Access denied" } </pre>	The user has no rights for this operation.
500	<pre> { "error": } </pre>	Internal server error.

Result code	Value	Description
	<pre> r : " E r r o r w h i l e m o d i f y i n g c o n f i g u r a t i o n " } </pre>	

Update settings

(reference: [Update settings](#))

PUT /admin/config/update

Properties

Property	Value
DESCRIPTION	Setting processing history cleanup time. The cleanup range is defined in hours .
URL	http://<server>:<port>/admin/config/update
REQUIRED RIGHTS	update: [read, write]
HTTP METHOD	PUT
CONTENT TYPE	json
BODY	<pre> { "autoupdateperiod": 240, "deleteafterimport": true, "disabledupdate": [{ "days": "5-7", "from": 480, "to": 960 }, { "days": "1-2", "from": 480, "to": 960 }], "pickupfolder": "/tmp/core-data /update_autoadd", "source": "internet" } </pre>

Response

Result code	Value	Description
200	<pre> { </pre>	Request processed successfully.

Result code	Value	Description
	<pre> " a u t o u p d a t e p e r i o d " : 2 4 0 , " d e l e t e a f t e r i m p o r t " : t r u e </pre>	

Result code	Value	Description
	<pre>e , " d i s a b l e d u p d a t e " : [{ " d a y s " : " 5 - 7 " , " f r o m " : 4</pre>	

Result code	Value	Description
	<pre> 8 0 , " t o " : 9 6 0 } , { " d a y s " : " 1 - 2 " , " f r o m " : 4 8 0 , " t o " </pre>	

Result code	Value	Description
	<pre> : 9 6 0 }] , " p i c k u p f o l d e r " : " / t m p / c o r e - d a t a / u p d a t e - </pre>	

Result code	Value	Description
	<pre> a u t o a d d " , " s o u r c e " : " i n t e r n e t " } </pre>	
403	<pre> { " e r r " : " A c c e s </pre>	The apikey is missing or invalid.

Result code	Value	Description
	<pre> s d e n i e d " } </pre>	
405	<pre> { " e r r " : " A c c e s s d e n i e d " } </pre>	The user has no rights for this operation.
500	<pre> { " e r r " : " </pre>	Internal server error.

Result code	Value	Description
	<pre> Error whil elem oddi fyn gco nf ig ura tio n" } </pre>	

Upon successful modification, in the response you must see the same JSON structure you have just set.

Explanation

There are three update methodology.

The actual method depends on the source setting:

```
"source": "internet"
```

OR

```
"source": "folder"
```

OR

```
"source": "manual"
```

When 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 *autoupdateperiod* key's value.

```
"autoupdateperiod": 240
```

The value is representing **minutes** (how often the product will check for updates on the internet)

You can set when NOT to distribute update packages to scan nodes:

```
"disabledupdate": [  
  {  
    "days": "1",  
    "from": 480,  
    "to": 960  
  },  
  {  
    "days": "5-7",  
    "from": 480,  
    "to": 960  
  }  
]
```

This is a JSON array, in which you can define the time period when you do not want to distribute update packages to scan nodes.

The JSON below mean that from Friday to Sunday (*week starts on Monday (1), ends on Sunday (7)*) from 8:00 to 16:00 you do not want to distribute packages.

From and *to* is the distance in **minutes** from 0:00 (*8:00 → 480 minutes, 16:00 → 960 minutes*)

```
{  
  "days": "5-7",
```

```
    "from": 480,  
    "to": 960  
  },
```

When selecting **folder** as an update source, then the most important settings are:

```
"deleteafterimport": true  
  
AND  
  
"pickupfolder": "/tmp/core-data/update_autoadd"
```

deleteafterimport means if you want to clean the pickup folder after the updates have been applied,

pickupfolder sets the folder where the core will look for update files.

Default settings

```
{  
  "autoupdateperiod": 240,  
  "deleteafterimport": true,  
  "disabledupdate": [],  
  "pickupfolder": "/tmp/core-data/update_autoadd",  
  "source": "internet"  
}
```

Roles

(Create new role)

POST /admin/role

Properties

Property	Value
DESCRIPTION	Add a new user role to the system.
URL	http://<server>:<port>/admin/role
REQUIRED RIGHTS	users: [read, write]

Property	Value
HTTP METHOD	POST
CONTENT TYPE	json
BODY	<pre> { "name": "new_role", "display_name": "New Role", "rights": { "agents": ["read", "write"], "cert": ["read", "write"], "configlog": ["read", "write"], "engines": ["read", "write"], "external": ["read", "write"], "license": ["read", "write"], "quarantine": ["read", "write"], "retention": ["read", "write"], "rule": ["read", "write"],], </pre>

Property	Value
	<pre> "scan": ["read", "write"], "scanlog": ["read", "write"], "skip": ["read", "write"], "update": ["read", "write"], "updatelog": ["read", "write"], "users": ["read", "write"], "workflow": ["read", "write"], "zone": ["read", "write"] } </pre>

Response

Result code	Value	Description
200	<pre> { "d </pre>	Request processed successfully.

Result code	Value	Description
	<pre> display_name : "NewRole" , editable : true , id : 6 , </pre>	

Result code	Value	Description
	<pre> " n a m e " : " n e w _ r o l e " , " r i g h t s " : { " a g g e n t s " : [" r e a </pre>	

Result code	Value	Description
	<pre> d " , " w r i t e "] , " c e r t " : [" r e a d " , " w r i t e "] , " c o n f </pre>	

Result code	Value	Description
	<pre> i g l o g " : [" r e a d " , " w r i t e "] , " e n g i n e s " : [" r e a d " , </pre>	

Result code	Value	Description
	<pre> "write"], . } , "user-count": 0 } </pre>	
400		Failed to apply changes.
403	<pre> { "error": : </pre>	The apikey is missing or invalid.

Result code	Value	Description
	<pre> " A c c e s s d e n i e d " } </pre>	
405	<pre> { " e r r " : " A c c e s s d e n i e d " } </pre>	The user has no rights for this operation.
500	<pre> { " </pre>	Internal server error.

Result code	Value	Description
	<pre> { "error": "Error while modifying configuration" } </pre>	

Users

(Create new users)

POST /admin/user

Properties

Property	Value
DESCRIPTION	Add a new user to the system.
URL	http://<server>:<port>/admin/user
REQUIRED RIGHTS	users: [read, write]
HTTP METHOD	POST
CONTENT TYPE	json
BODY	<pre>{ "api_key": "b8a4b52f19de88e365aa4f7e403fa91b 352f", "directory_id": 1, "display_name": "asdasd", "email": "asd@asd", "name": "asdasd", "password": "asd", "roles": ["1", "2", ...], "ui_settings": { "refresh_rate": "{\"value\":30}", "time_period": "{\"value\":24,\" unitInHour\":1}", ... } }</pre>

Response

Result code	Value	Description
200	<pre>{</pre>	Request processed successfully.

Result code	Value	Description
	<pre> " a p i - k e y " : " 0 d f 0 d 1 6 8 c 3 3 3 e 4 3 b 2 d 6 7 c 6 2 0 a 8 d a 4 8 c e 9 0 4 c " </pre>	

Result code	Value	Description
	, " d i r e c t o r y - i d : 1 , " d i s p l a y - n a m e : " a s d a s d s d " , "	

Result code	Value	Description
	<pre> e m a i l " : " a s s d @ a s s d " , " i d " : 2 , " n a m e " : " a s s d a s s d " , " r i g h </pre>	

Result code	Value	Description
	<pre> t s ": { " a g e n t s ": [" r e a d " , " w r i t e "] , " c e r t ": [" r e </pre>	

Result code	Value	Description
	<pre> ad " , " write "] , " configlog ": [" read " , " write "] , </pre>	

Result code	Value	Description
	<pre> " e n g i n e s " : [" r e a d " , " w r i t e "] , . . . } , " r o l e s " : [</pre>	

Result code	Value	Description
	<pre> " 1 " , " 2 "] , " u i - s e t t i n g s " : { " r e f r e s h - r a t e " : " { \ " </pre>	

Result code	Value	Description
	<pre> value \ : 30 } , " time - period " : " { \ " value \ : 24 , \ " uni </pre>	

Result code	Value	Description
	<pre> t I n H o u r \ " : 1 } " } </pre>	
400		Failed to apply changes.
403	<pre> { " e r r " : " A c c e s s d e n i e d " } </pre>	The apikey is missing or invalid.

Result code	Value	Description
405	<pre data-bbox="470 369 558 1198"> { "error": "Access denied" } </pre>	The user has no rights for this operation.
500	<pre data-bbox="470 1281 558 1966"> { "error": "Error while" } </pre>	Internal server error.

Result code	Value	Description
	<pre> { "o d i f y i n g c o n f i g u r a t i o n " } </pre>	

Import

(Import configuration from file)

POST /admin/import

Properties

Property	Value
DESCRIPTION	Import configuration from file.
URL	http://<server>:<port>/admin/import
REQUIRED RIGHTS	Administrators right
HTTP METHOD	POST
CONTENT TYPE	json

Property	Value
BODY	<p>Already exported config json.</p> <pre> { "config": { "policy.rule.rule": { "items": [{ "active": true, "allow_cert": false, "allow_cert.cert": "None", ... }] } } } </pre>

Response

Result code	Value	Description
200	<pre> { "result": "Successful" } </pre>	Request processed successfully.

Result code	Value	Description
	<pre data-bbox="469 329 561 654"> ported" } </pre>	
304	<pre data-bbox="469 725 561 871"> { } </pre>	The configuration has not changed.
400	<pre data-bbox="469 949 561 1973"> { "error": "Unable to parse JSON body" } </pre>	The format of the configuration file is invalid.

Result code	Value	Description
	<pre> " } </pre>	
400	<pre> { " e r r " : " U n a b l e t o i m p o r t n e w c o n f i g u r a t i o n " } </pre>	Internal server error.

Result code	Value	Description
403	<pre data-bbox="470 369 558 1198"> { "error": "Access denied" } </pre>	<p data-bbox="582 347 1300 425">The apikey is missing, or the user has no rights for this operation.</p>
500	<pre data-bbox="470 1288 558 1960"> { "error": "Unable to save" } </pre>	<p data-bbox="582 1265 853 1299">Internal server error.</p>

Result code	Value	Description
200	<pre data-bbox="470 376 560 1861"> { "result": "Updated trigger successfully." }</pre>	Request processed successfully.
403	<pre data-bbox="470 1933 560 1966"> {</pre>	The apikey is missing or invalid.

Result code	Value	Description
	<pre>{ "error": "Access denied"} </pre>	
405	<pre>{ "error": "Access denied"} </pre>	The user has no rights for this operation.

Result code	Value	Description
	<pre>{ " }</pre>	
500	<pre>{ " e r r o r " : " E r r o r o r t e r i g g e r i n g u p d a t e " }</pre>	Internal server error.

Change password

(Modify user password)

POST /user/changepassword

Properties

Property	Value
DESCRIPTION	Modify the password set for the user identified by apikey.
URL	http://<server>:<port>/user/changepassword
REQUIRED RIGHTS	
HTTP METHOD	POST
CONTENT TYPE	json
BODY	<pre>{ "old_password": "oldpassword", "new_password": "newpassword" }</pre>

Response

Result code	Value	Description
200	<pre>{ "result": "Successful" }</pre>	Request processed successfully.

Result code	Value	Description
	<pre>ful</pre>	
400	<pre>{ "error": "Access denied" }</pre>	The apikey is missing or invalid.
405	<pre>{ "error": "Access</pre>	The user has no rights for this operation.

Result code	Value	Description
	<pre> s s d e n i e d " } </pre>	
500	<pre> { " e r r " : " P a s s w o r d m o d i f i c a t i o n f a i l e </pre>	Internal server error.

Result code	Value	Description
	<pre>d " }</pre>	

Nodes

(Get node list and statuses)

GET /stat/nodes

Properties

Property	Value
DESCRIPTION	Get the list of connected nodes and status of all of them.
URL	http://<server>:<port>/stat/nodes
REQUIRED RIGHTS	agents: [read]
HTTP METHOD	GET

Response

Result code	Value	Description
200	<pre>{ " e x t e r n a l _ n o</pre>	Request processed successfully.

Result code	Value	Description
	<pre> des-allowed: false, "max-nodes-count": 1, "status" </pre>	

Result code	Value	Description
	<pre> s " : [{ " a d d r e s s " : " , " c p u - c o r e s " : 8 , " e n g i n e s " : [</pre>	

Result code	Value	Description
	<pre> { "active": true, "db-ver": "5.1.0-304", "def-tim </pre>	

Result code	Value	Description
	e " : " 1 9 7 0 - 0 1 - 0 1 T 0 0 : 0 0 : 0 0 . 0 0 0 Z " , " e n g - n a m e " : " A r c h i -	

Result code	Value	Description
	<pre> v e n g i n e " , " e n g - v e r " : " 5 . 1 . 0 - 3 0 4 " , " e n g i n e - t y p e " : </pre>	

Result code	Value	Description
	<pre> " a r c h i v e " , " i d " : " 7 z - 4 - l i n u x " } , { " a c t i v e " : t r u e , </pre>	

Result code	Value	Description
	<pre> " d b - v e r " : " 2 5 0 5 0 " , " d e f - t i m e " : " 2 0 1 8 - 1 0 - 1 9 T 0 7 : 0 1 : </pre>	

Result code	Value	Description
	1 6 . 0 0 0 Z " , " e n g - n a m e " : " C l a m A V " , " e n g - v e r " : " 0 . 1 0 0 .	

Result code	Value	Description
	2 - 1 0 4 " , " e n g i n e - t y p e " : " a v " , " i d " : " c l a m a v - 1 - l i n	

Result code	Value	Description
	<pre> u x " }] , " f r e e - d i s k - s p a c e " : 1 7 3 9 9 3 4 4 3 3 2 8 , " i d " : " : </pre>	

Result code	Value	Description
	<pre> 6 9 " ' " i s s u e s " : [{ " d e s c r i p t i o n " : " l e n g t h s a r e n o t d </pre>	

Result code	Value	Description
	<pre> e p l o y e d t o t h i s n o d e " , " s e v e r i t y " : " w a r n i n g " }] , " l </pre>	

Result code	Value	Description
	o a d " : 1 4 , " o s " : " L i n u x M i n t 1 8 .3 S Y l v i a " , " s c a n _ q u e u e 	

Result code	Value	Description
	<pre> " : 0 , " t o t a l _ m e m " : 4 0 1 0 0 , " v e r s i o n " : " 4 . 1 3 . 1 " }] } </pre>	

403	<pre>{ "error": "Access denied" }</pre>	The apikey is missing or invalid.
405	<pre>{ "error": "Access denied" }</pre>	The user has no rights for this operation.

Result code	Value	Description
	<pre>d " }</pre>	

Engines

(Get the list of engines)

GET /stat/engines

Properties

Property	Value
DESCRIPTION	Get the list of engines and status of all of them.
URL	http://<server>:<port>/stat/engines
REQUIRED RIGHTS	Need "full details" visibility for at least one of the workflow rules. When the visibility is set for "Everybody", then the apikey is not required.
HTTP METHOD	GET

Response

Result code	Value	Description
200	<pre>[{ " a b a n d o n "</pre>	Request processed successfully.

Result code	Value	Description
	<pre> e d " : f a l s e , " a c t i v e " : t r u e , " d e f - t i m e " : " " , " d o w n l o </pre>	

Result code	Value	Description
	a d - p r o g r e s s " : 1 0 0 , " d o w n l o a d - t i m e " : " 2 0 1 8 - 1 2 - 0 3 T 1 2	

Result code	Value	Description
	<pre> : 4 1 : 4 3 . 8 4 1 Z " , " e n g - i d " : " 7 z - 4 - l i n u x " , " e n g - n a m e " : </pre>	

Result code	Value	Description
	<pre> " A r c h i v e e n g i n e " , " e n g - t y p e " : " B u n d l e d e n g i n e " , " e n </pre>	

Result code	Value	Description
	<pre> g - v e r " : " 5 . 1 . 0 - 3 0 4 " , " e n g g i n e - t y p e " : " a r c h i v e " , " s t </pre>	

Result code	Value	Description
	<pre> a t e " : " p r o d u c t i o n " , " t y p e " : " e n g i n e " } , { " a b a n d o n </pre>	

Result code	Value	Description
	<pre> e d " : f a l s e , " a c t i v e " : t r u e , " d e f - t i m e " : " 2 0 1 8 - 1 0 - 1 1 9 </pre>	

Result code	Value	Description
	T 0 7 : 0 1 : 1 6 . 0 0 0 Z " , " d o w n l o a d - p r o g r e s s " : 1 0 0 , " d o w n l	

Result code	Value	Description
	o a d - t i m e " : " 2 0 1 8 - 1 2 - 0 3 T 1 2 : 4 1 : 4 3 . 9 0 1 Z " , " e n g - i d " : "	

Result code	Value	Description
	<pre> c l a m a v - l - l i n u x " , " e n g - n a m e " : " C l a m A V " , " e n g - t y p e " </pre>	

Result code	Value	Description
	<pre> : " B u n d l e d e n g g i n e " , " e n g g - v e r " : " 0 . 1 0 0 0 . 2 - 1 0 4 " , " e n g g i </pre>	

Result code	Value	Description
	<pre> n e - t y p e " : " a v " , " s t a t e " : " p r o d u c t i o n " , " t y p e " : " e n g </pre>	

Result code	Value	Description
	<pre> i n e " } , { " a b a n d o n e d " : f a l s e , " a c t i v e " : f a l s e , " d e </pre>	

Result code	Value	Description
	f - t i m e " : " , " d o w n l o a d - p r o g r e s s " : 1 0 0 , " d o w n l o a d - t	

Result code	Value	Description
	i m e " : " 2 0 1 8 - 1 2 - 0 3 T 1 2 : 4 1 : 4 3 . 9 6 1 Z " , " e n g - i d " : " c l a m a	

Result code	Value	Description
	v - 1 - w i n d o w s " , " e n g - n a m e " : " C l a m A V " , " e n g - t y p e " : " B	

Result code	Value	Description
	u n d e r l i n e e n g i n e " , " e n g i n e - v e r " : " 0 . 9 9 . 2 - 2 4 " , " e n g i n e - t y	

Result code	Value	Description
	<pre> "pe": "average", "state": "downloaded", "type": "engine" </pre>	

Result code	Value	Description
	<pre> } , { " a b a n d o n e d " : f a l s e , " a c t i v e " : t r u e , " d e f _ t i m e </pre>	

Result code	Value	Description
	<pre> e " : " , " d o w n l o a d - p r o g r e s s " : 1 0 0 , " d o w n l o a d - t i m e " : </pre>	

Result code	Value	Description
	" 2 0 1 8 - 1 2 - 0 3 T 1 2 : 4 1 : 4 3 . 9 9 1 Z " ' " e n g - i d " : " d s - 3 - w i n -	

Result code	Value	Description
	<pre>e " , " e n g - n a m e " : " D a t a s a n i t i z a t i o n " , " e n g - t y p e " : " B</pre>	

Result code	Value	Description
	u n d l e d e n g g i n e " , " e n g g - v e r " : " 5 .2 .8 - 7 7 8 - 3 3 8 " , " e n g g i n	

Result code	Value	Description
	<pre>e - t y p e " : " d s " , " s t a t e " : " p r o d u c t i o n " , " t y p e " : " e n g i</pre>	

Result code	Value	Description
	<pre> n e " } , { " a b a n d o n e d " : f a l s e , " a c t i v e " : t r u e , " d e f _ </pre>	

Result code	Value	Description
	t i m e " : " 2 0 1 6 - 0 6 - 1 3 T 0 0 : 0 0 : 0 0 . 0 0 0 Z " , " d o w n l o a d _ p r o g	

Result code	Value	Description
	r e s s " : 1 0 0 , " d o w n l o a d - t i m e " : " 2 0 1 8 - 1 2 - 0 3 T 1 2 : 4 1 : 4 3 . 	

Result code	Value	Description
	<pre> 8 2 0 Z " , " e n g _ i d " : " f i l e t y p e _ l _ l i n u x " , " e n g _ n a m e " : " </pre>	

Result code	Value	Description
	F i l l e T Y P e " , " e n g - t Y P e ": " B u n d l e d e n g i n e " , " e n g - v e r " 	

Result code	Value	Description
	: " 5 . 3 0 . 0 7 1 9 2 0 1 5 - 2 5 9 " , " e n g i n e - t y p e " : " f i l e t y p e " ,	

Result code	Value	Description
	<pre> " s t a t e " : " p r o d u c t i o n " , " t y p e " : " e n g i n e " } , . . .] </pre>	

Result code	Value	Description
403	<pre>{ "error": "Access denied" }</pre>	The apikey is missing or invalid.
405	<pre>{ "error": "Access denied" }</pre>	The user has no rights for this operation.

Result code	Value	Description
	<pre>d " }</pre>	
500	<pre>{ " e r r " : " E r r o r q u e r y i n g e n g i n e l i s t " }</pre>	Internal server error.

Pin engine to prevent auto-updates

(Pin engines to prevent applying automatic updates on them. Manual updates still can be applied.)

POST /admin/engine/{engineId}/pin

Properties

Property	Value
DESCRIPTION	Set engine to be pinned.
URL	http://<server>:<port>/admin/engine/{engineId}/pin
REQUIRED RIGHTS	engines : [read, write]
HTTP METHOD	POST

Header Parameters

Header	Description	Allowed Values	Required
apikey	Authentication	<your_unique_apikey>	YES
type	Pin engine or database to prevent applying automatic updates on it. (If the type is not defined both engine and database will be pinned.)	engine / database	NO

Response

Result code	Value	Description
200	<pre>{ " r e s u l t " : " E n .</pre>	Request processed successfully.

Result code	Value	Description
	<pre>g i n e i s p i n n e d " } { " r e s u l t " : " D a t a b a s e i s p i n n e d " }</pre>	

Result code	Value	Description
	<pre>{ "result": "Both engine and database are pinned"</pre>	
400		Bad request.

Result code	Value	Description
	<pre>{ "error": "The type header value has to be engineering or data"</pre>	

Result code	Value	Description
	<pre> { b a s e : " } </pre>	
403	<pre> { " e r r " : " A c c e s s d e n i e d " } </pre>	The apikey is missing or invalid.
405	<pre> { " e r r " : " A c </pre>	The user has no rights for this operation.

Result code	Value	Description
	<pre> { "e r r o r" : "C a n n o t p i n t h e e n g i n e" } </pre>	
500	<pre> { "e r r o r" : "C a n n o t p i n t h e e n g i n e" } </pre>	Internal server error.

Result code	Value	Description
	<pre data-bbox="502 331 529 1332"> { "error": "Cannot print the data base" } </pre> <pre data-bbox="502 1451 529 1957"> { "error": "Error ha </pre>	

Result code	Value	Description
	s o c c u r r e d . E n g i n e i s p i n n e d / u n p i n n e d , D a t a b a s e i s p i n n	

Result code	Value	Description
	<pre> { "engineId": "unpinned" } </pre>	

Unpin engine to apply auto-updates

(Unpin engines so automatic updates will be applied on them.)

PUT /admin/engine/{engineId}/unpin

Properties

Property	Value
DESCRIPTION	Set engine to be unpinned.
URL	http://<server>:<port>/admin/engine/{engineId}/unpin
REQUIRED RIGHTS	engines : [read, write]
HTTP METHOD	POST

Header Parameters

Header	Description	Allowed Values	Required
apikey	Authentication	<your_unique_apikey>	YES
type	Unpin engine or database to applying automatic updates on it.	engine / database	NO

Header	Description	Allowed Values	Required
	(If it is not defined both engine and database will be unpinned.)		

Response

Result code	Value	Description
200	<pre> {"result": "Engine is unpinned"} </pre> <pre> {"result": "Database is unpinned"} </pre>	Request processed successfully.
400	<pre> {"err": "The type header value has to be 'engine' or 'database'"} </pre>	Bad request.
403	<pre> {"err": "Access denied"} </pre>	The apikey is missing or invalid.
405	<pre> {"err": "Access denied"} </pre>	The user has no rights for this operation.
500	<pre> {"err": "Can't unpin the engine"} </pre> <pre> {"err": "Can't unpin the engine"} </pre>	Internal server error.

Result code	Value	Description
	<pre>{"err": "Error has occurred. Engine is pinned/unpinned, Database is pinned/unpinned"}</pre>	

Enable engines

(Enable to use engine on the nodes)

POST /admin/engine/{engineId}/enable

Properties

Property	Value
DESCRIPTION	Enable to use the selected engine on the nodes.
URL	http://<server>:<port>/admin/engine/{engineId}/enable
REQUIRED RIGHTS	engines : [read, write]
HTTP METHOD	POST

Response

Result code	Value	Description
200	<pre>{ "r e s u l t " : " E</pre>	Request processed successfully.

Result code	Value	Description
	<pre> ngin enabled } </pre>	
403	<pre> { "error": "Access denied" } </pre>	The apikey is missing or invalid.
405	<pre> </pre>	The user has no rights for this operation.

Result code	Value	Description
	<pre>{ "error": "Access denied"} </pre>	
500	<pre>{ "error": "Cannot enable"} </pre>	Internal server error.

Result code	Value	Description
	<pre>engine"</pre>	

Disable engines

(Disable to use engine on nodes)

POST /admin/engine/{engineId}/disable

Properties

Property	Value
DESCRIPTION	Disable to use the selected engines on the nodes.
URL	http://<server>:<port>/admin/engine/{engineId}/disable
REQUIRED RIGHTS	engines: [read, write]
HTTP METHOD	POST

Response

Result code	Value	Description
200	<pre>{ "result"</pre>	Request processed successfully.

Result code	Value	Description
	<pre> " : " E n g g i n e i s d i s a b l e d " } </pre>	
403	<pre> { " e r r " : " A c c e s s d e n i e d " } </pre>	The apikey is missing or invalid.

405	<pre>{ "error": "Access denied" }</pre>	The user has no rights for this operation.
500	<pre>{ "error": "Cannot disabl</pre>	Internal server error.

Result code	Value	Description
	<pre> { "sessionTimeout": 300000, "allowDuplicateSession": true, "allowCrossIpSessions": true, "absoluteSessionTimeout": 0 }</pre>	

Session settings

(Configure settings for session generated upon a successful login)

PUT /admin/config/session

Properties

Property	Value
DESCRIPTION	Configure settings for session generated upon a successful login See more at 8.1.1.1. Login / Create a Session
URL	http://<server>:<port>/admin/config/session
REQUIRED RIGHTS	Administrators right
HTTP METHOD	PUT
CONTENT TYPE	json
BODY	<pre>{ "absoluteSessionTimeout": 0, "allowCrossIpSessions": true, "allowDuplicateSession": true, "sessionTimeout": 300000 }</pre>

Response

Result code	Value	Description
200	<pre>{ "absolute session nT imeout" : 0, "allow wC r o s s I</pre>	Request processed successfully.

Result code	Value	Description
	<pre> p s e s s i o n s " : t r u e , " a l l o w D u p l i c a t e s e s s i o n " : t r u e , " </pre>	

Result code	Value	Description
	<pre> s e s s i o n T i m e o u t : 3 0 0 0 0 0 } </pre>	
403	<pre> { " e r r ": " A c c e s s d e n i e d " } </pre>	The apikey is missing or invalid.

Result code	Value	Description
	<pre> " } </pre>	
405	<pre> { " e r r " : " A c c e s s d e n i e d " } </pre>	The user has no rights for this operation.
500	<pre> { " e r r " : " E r r o r w h </pre>	Internal server error.

Result code	Value	Description
	<pre> { "ilmodifyconfiguration" } </pre>	

Webhook configurations - Retrieval

(Retrieve webhook supported settings)

GET /admin/config/webhook

Properties

Property	Value
DESCRIPTION	Getting settings supported for webhook mode
URL	http://<server>:<port>/admin/config/webhook
REQUIRED RIGHTS	Administrators right

Property	Value
HTTP METHOD	GET

Response

Result code	Value	Description
200	<pre>{ "maxretrytime": 3, "delayduration": 10</pre>	<p>Request processed successfully.</p> <p>+ maxretrytime: number of allowed retries sending callback to client when failed</p> <p>+ delayduration and delayprogression: in milliseconds.</p> <p><u>For example:</u> maxretrytime= 3</p> <p>Sending callback failed for some reasons</p> <ul style="list-style-type: none"> • 1st retry triggered after delayduration (ms) • 2nd retry triggered after delayduration+ delayprogression (ms) • 3rd retry triggered after delayduration+ 2*delayprogression (ms)

Result code	Value	Description
	<pre> 0 0 , " d e p l a y p r o g r e s s i o n " : 1 0 0 0 } </pre>	
403	<pre> { " e r r " : " A c c e s s </pre>	The apikey is missing or invalid.

Result code	Value	Description
	<pre>{ "denied": true }</pre>	
405	<pre>{ "error": { "message": "Access denied" } }</pre>	The user has no rights for this operation.
500	<pre>{ "error": { "message": "Internal server error" } }</pre>	Internal server error.

Result code	Value	Description
	<pre> n t e r n a l s e r v e r e r r o r " } </pre>	

Webhook configurations - Modification

(Retrieve webhook supported settings)

PUT /admin/config/webhook

Properties

Property	Value
DESCRIPTION	Modifying settings supported for webhook mode
URL	http://<server>:<port>/admin/config/webhook
REQUIRED RIGHTS	Administrators right
HTTP METHOD	PUT
CONTENT TYPE	json
BODY	

Property	Value
	<pre> { "maxretrytime": <number>, "delayduration": <number>, "deplayprogression": <number> } </pre> <p>+ maxretrytime: number of allowed retries sending callback to client when failed</p> <p>+ delayduration and delayprogression: in milliseconds.</p> <p><u>For example:</u> maxretrytime= 3</p> <p>Sending callback failed for some reasons</p> <ul style="list-style-type: none"> • 1st retry triggered after delayduration (ms) • 2nd retry triggered after delayduration+ delayprogression (ms) • 3rd retry triggered after delayduration+ 2*delayprogression (ms)

Response

Result code	Value	Description
200	<pre> { "maxretrytime": <number> } </pre>	Request processed successfully.

Result code	Value	Description
	<pre> m b e r > , = d e l a y d u r a t i o n = : < n u m b e r > , = d e p l a y p r o g r e s s </pre>	

Result code	Value	Description
	<pre> { "error": { "code": "InvalidApiKey" } } </pre>	
403	<pre> { "error": { "code": "AccessDenied" } } </pre>	The apikey is missing or invalid.
405	<pre> { "error": { "code": "UserNoRights" } } </pre>	The user has no rights for this operation.

Result code	Value	Description
	<pre> r r ": " A c c e s s d e n i e d " } </pre>	
500	<pre> { " e r r ": " I n t e r n a l s e r v e r e r r " } </pre>	Internal server error.

Result code	Value	Description
	<pre> { "ror" } </pre>	

8.1.10. Yara

- [8.1.10.1. Get Yara sources](#)
- [8.1.10.2. Modify Yara sources](#)
- [8.1.10.3. Generate Yara package](#)
- [8.1.10.4. Get status of Yara package generation](#)

8.1.10.1. Get Yara sources

Request	Value
Method	GET
URL	/admin/config/yara/sources

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**

```

{
  "local_sources": [
    {
      "source": "/mnt/yara",

```

```

        "state": "enabled"
    }
],
"http_sources": [
    {
        "source": "http://onlineyarasources.net/source.zip",
        "state": "disabled"
    }
]
}

```

The response contains the current sources.

Each object in the array represents a source:

source: path or the url of the source

state: state of the source (can be enabled or disabled)

Error response

Internal error

HTTP status code: 500

```

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

```

Invalid api key or rights

HTTP status code: 403

```

{
    "err": "Access denied"
}

```

Note: Check Metadefender Core server logs for more information.

8.1.10.2. Modify Yara sources

Request	Value
Method	PUT
URL	/admin/config/yara/sources

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
http_sources	array	true	containing the new http sources
local_sources	array	true	containing the new local sources

Example:

```
{
  "local_sources": [
    {
      "source": "/mnt/yara",
      "state": "enabled"
    }
  ],
  "http_sources": [
    {
      "source": "http://onlineyarasources.net/source.zip",
      "state": "disabled"
    }
  ]
}
```

The request body contains local sources and http sources as an array;

Each object in the array represents a source:

source: path or the url of the source

state: state of the source (can be enabled or disabled)

Successful response

HTTP status code: 200

```
{
  "local_sources": [
```



```
{
  {
    "source": "/mnt/yara",
    "state": "enabled"
  }
],
"http_sources": [
  {
    "source": "http://onlineyarasources.net/source.zip",
    "state": "disabled"
  }
]
}
```

The response contains the modified data of sources.

Error response

Internal error

HTTP status code: 500

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

Invalid api key or rights

HTTP status code: 403

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

Invalid data

HTTP status code: 500

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

Note: Check Metadefender Core server logs for more information.

8.1.10.3. Generate Yara package

Request	Value
Method	POST
URL	/yara/generate

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**

```
{
  "status": "idle",
  "start_time": "",
  "issues": {
    "general": [
      {
        "severity": "warning",
        "message": "Error while extracting network source. Can
not open destination."
      }
    ],
    "<source>": [
      {
        "severity": "warning",
        "message": "The given local source does not exists."
      }
    ],
  }
}
```

The response is the is the actual state of generation process.

status: can be "idle", "error" or "inprogress"

start_time: used only when status is inprogress, otherwise its empty.

issues: stores a map of issues. Each key represents the according source, except "general", which contains general errors occurred during the generation process.

Error response

Internal error

HTTP status code: 500

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

Invalid api key or rights

HTTP status code: 403

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

Note: Check Metadefender Core server logs for more information.

8.1.10.4. Get status of Yara package generation

Request	Value
Method	GET
URL	/yara/package

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**

```
{
  "status": "idle",
  "start_time": "",
  "issues": {
    "general": [
      {
        "severity": "warning",
        "message": "Error while extracting network source. Can
not open destination."
      }
    ],
    "<source>": [
      {
        "severity": "warning",
        "message": "The given local source does not exists."
      }
    ],
  }
}
```

The response is the is the actual state of generation process.

status: can be "idle", "error" or "inprogress"

start_time: used only when status is inprogress, otherwise its empty.

issues: stores a map of issues. Each key represents the according source, except "general", which contains general errors occurred during the generation process.

Error response

Internal error

HTTP status code: **500**

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

Invalid api key or rights

HTTP status code: **403**

```
{
```

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

Note: Check Metadefender Core server logs for more information.

8.1.11. Webhooks

- [8.1.11.1. Individual file processing](#)
- [8.1.11.2. Batch processing](#)
- [8.1.11.3. Query webhooks status](#)

8.1.11.1. Individual file processing

By default, REST Client is expected to keep querying Core for analysis result upon file submission (polling mode), but client can switch from polling to webhooks mode by setting **callbackurl** header mentioned in [8.1.3.1. Process a file](#) .

When configured properly on file analysis request, Core will proactively send callback to client's specified URL (method: POST) with the full analysis result, whenever that analysis is finished. The client will no longer need to keep querying Core for temporary analysis results (polling).

Successful response

HTTP status code: 200

```
{
  "data_id": "61df feaa728844adbf49eb090e4ece0e"
}
```

Error response

Callback URL is invalid

HTTP status code: 400

```
{
  "err": "Callback url is invalid."
}
```

When analysis is finished on MetaDefender Core, POST request will be made to the specified URL address (that was passed as **callbackurl** header in file submission request). The body of the request will contain the full analysis result. See more about full scan result example at [8.1.3.2. Fetch processing result](#)

8.1.11.2. Batch processing

By default closing batch will not be successful while inner files are still being processed, and expecting client to keep retrying to close batch again later.

Client can switch from this polling to webhooks mode by setting **callbackurl** header mentioned in [8.1.4.4. Close Batch](#) . When configured properly on batch closing request, Core will:

- Monitor all inner files until they are all done
- Close that batch,
- Proactively notify back to client's designated URL with a full batch result.

By doing so, REST client will use batch closing API just to confirm that all inner files submitted successfully tied to that batch. REST Client will no longer be required to wait for all inner files to finish the analysis in order to close the batch.

MetaDefender Core will take care of the rest and will notify client (via callbackurl) when batch is closed and the analysis for the entire batch is available to client.

URL	/file/batch/<batch_id>/close/callback
Method	POST

Header	Type	Required	Description
apikey	string	No	User's session id, if it was set for creation it is required
callbackurl	string (<protocol://><ip domain>:<port></path>)	Yes	Client's URL where MetaDefender Core will notify batch result back to whenever batch is closed successfully (webhooks model). See details at 8.1.11.2. Batch processing For example: http://10.0.1.100:8081 /callback

Result Code	Description
200	Callback URL is set successfully
400	Bad request, (e.g.: wrong header values, batch is already closed, invalid API key)
403	Access denied
404	Batch not found
500	Internal server error

Successful response

HTTP status code: **200**

```
{
  "<batch_id>": "Callback url set"
}
```

Error response

Callback URL is invalid

HTTP status code: **400**

```
{
  "err": "Callback url is invalid."
}
```

Callback URL is missed

HTTP status code: **403**

```
{
```

```
}
  "err": "No callback url given."
}
```

When batch is closed successfully on Core, a batch result will be automatically sent to URL address which pre-configured via **callbackurl** header. See more about batch result example at [8.1.4.4. Close Batch](#)

8.1.11.3. Query webhooks status

Prior to being notified by Core when webhooks mode is set, client can anytime ask Core for file / batch processing webhooks status

URL	<ul style="list-style-type: none">• File processing: <code>/file/webhook/<data_id></code>• Batch processing: <code>/file/webhook/<batch_id></code>
Method	GET

Header	Type	Required	Description
apikey	string	No	User's session id, if it was set for creation it is required

Result Code	Description
200	Webhooks status is fetched successfully
400	Bad request, (e.g.: wrong header values, invalid API key)
403	Access denied
404	Webhooks status is not found callbackurl header wasn't added for the specified data_id
500	Internal server error

Successful response

HTTP status code: **200**

```
{
```



```

    "data_id": string,
    "request_time": string,
    "status_code": number,
    "url": string
}

```

"status_code": indicates the status of callback sent from Core to designated remote server.

Successful		
	200	Callback was sent successfully
Failed		
	403	ContentAccessDenied The access to the remote content was denied (similar to HTTP(S) error 401)
	404	ContentNotFoundError The remote content was not found at the server (similar to HTTP(S) error 404)
	408	TimeoutError The connection to the remote server timed out
	503	HostNotFoundError The remote host name was not found (invalid hostname)
	520	RemoteHostClosedError The remote server closed the connection prematurely, before the entire reply was received and processed
	444	Other error types Reference: https://doc.qt.io/archives/qt-4.8/qnetworkreply.html#NetworkError-enum Enable debug log level on Core for further error description

Error response

Webhooks status not found

HTTP status code: **404**

```
{
  "err": "Webhook status not found."
}
```

Callback URL is not set

HTTP status code: **404**

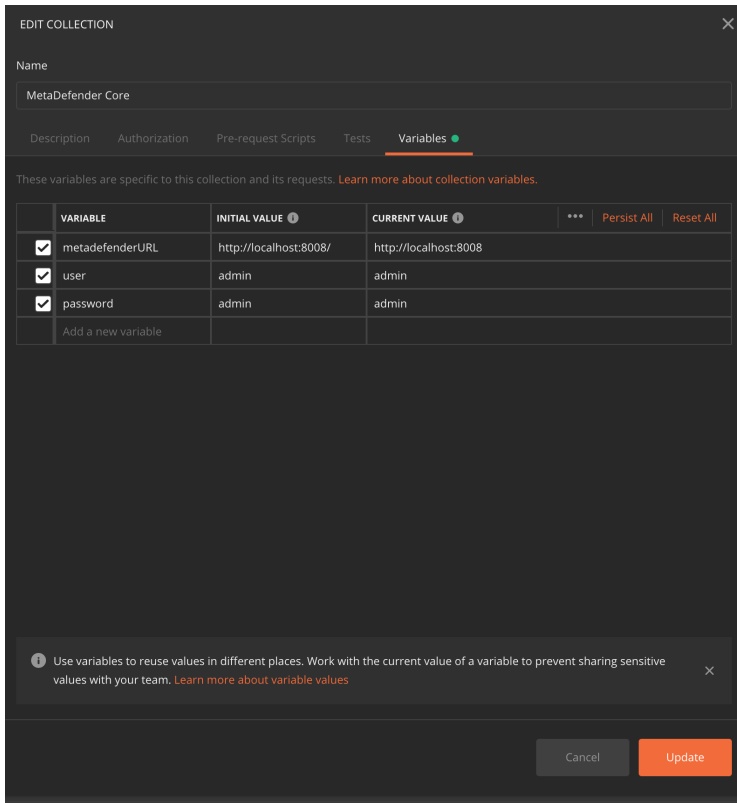
```
{
  "err": "No callback url set."
}
```

8.2. MetaDefender API Code Samples

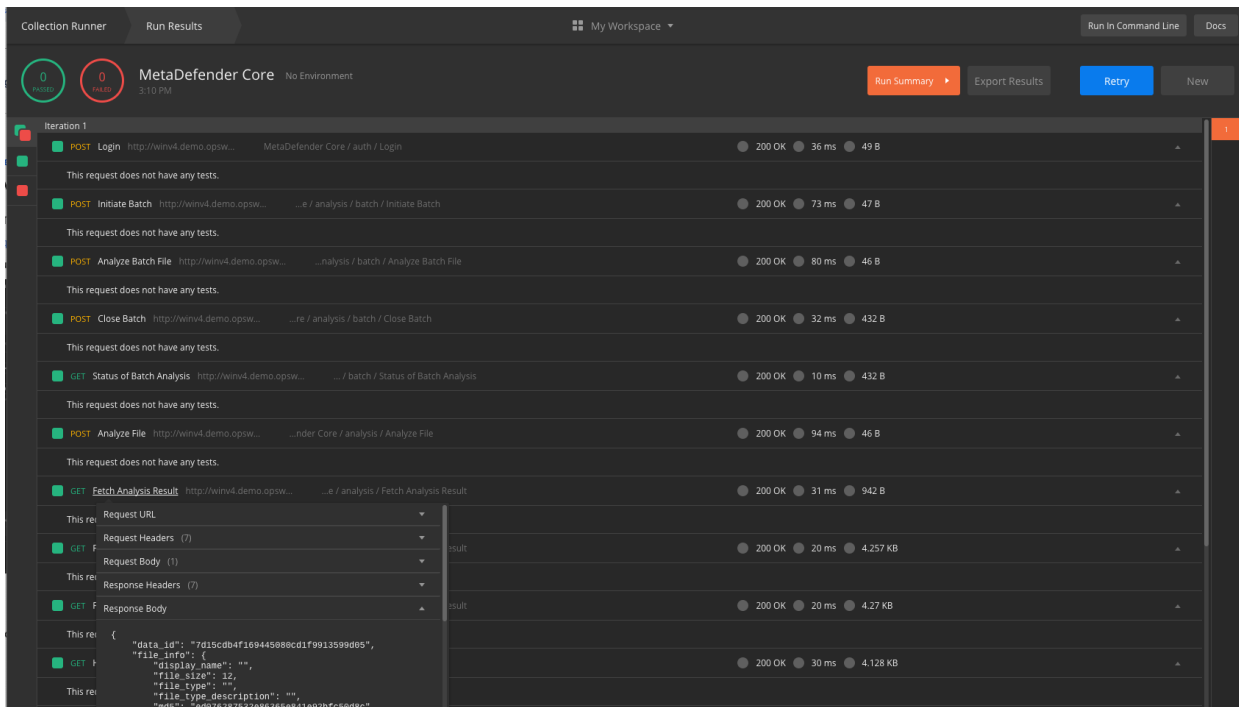
OPSWAT provides some sample codes on [GitHub](#) to make it easier to understand how the MetaDefender REST API works.

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

Also, you can import the [MetaDefender Postman Collection](#), which will give you quick access to the API. After you import it, please update the URL for MetaDefender and the credentials (MetaDefender Core collection → Edit → Variables):



Please note that the requests are chained, so you can use the Runner to run the tests and to see the analysis flow and the requests headers and response:



9. (NEW) MetaDefender Core Developer Guide

\$REDOC_BLOCK\$

10. Advanced MetaDefender Deployment

- [10.1. Scripted license management](#)
- [10.2. Deployment automation support](#)
- [10.3. Cloud Deployment](#)
- [10.4. Multi-node deployment](#)
- [10.5. Using external load-balancer](#)

10.1. 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 [10.4. 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.

10.2. Deployment automation support



For deployment automation support, an ignition file pre-defined by admin user is required, so create it if not existed:

- **Windows:** C:\OPSWAT\ometascan.conf
- **Linux:** /etc/opswat/ometascan.conf

Ignition file could be utilized for either or both of following use-cases:

1. Before installing MetaDefender Core 4.19.0 or above on Linux environment (comes with command line mode supported only), or on Windows via command line: You have to pre-define PostgreSQL server information for MetaDefender Core to work with. Check out details at [2.2.2.1. Installing Metadefender Core \(4.19.0 or newer\) using command line](#)

2. After installing MetaDefender Core for the first time (clean install), then it requires you to go through wizard steps to accept EULA, create a default local admin user, and later import MetaDefender Core configurations. Those steps could be automated using ignition file described in this page.

- [Installation](#)
- [Initialization](#)
 - [Ignition file](#)
 - [Ignition file fields](#)
 - [Ignition file location](#)
 - [Detailed initialization process](#)
- [Configuration](#)

The product supports fully automated deployment. It means that it can be installed and configured with no human interaction.

The automated deployment can be split to three steps on a high level:

1. Installation,
2. Initialization,
3. Configuration.

Error rendering macro 'drawio' : null

Installation

To automate the installation, install the product from the command line and provide the installation-time options as parameters to the installer. For further details see [2.2.2.1. Installing Metadefender Core \(4.19.0 or newer\) using command line](#)

After the installation is complete, the product starts up and waits in a pre-initialized status. The product may be initialized in two ways:

1. Manually using the [1.1.1. Configuration wizard](#), or
2. Automatically using an *ignition file* (see below).



If the automated initialization fails for some reason (e.g. the ignition file is not in place) then the automated initialization may be retried fixing the problem (e.g. placing the ignition file to its lookup location) and restarting the *OPSWAT Metadefender Core* service.

Until the product is in pre-initialized status, it will try the automated initialization every time after a service (re)start.

Error rendering macro 'drawio' : null

Initialization

Initialization is the process of bringing the product to an operable status.

Basically the initialization consists of the following steps:

1. Accept the End User License Agreement (EULA),
2. Import product configuration and
3. Create the first administrator user account.

Error rendering macro 'drawio' : null

Ignition file

The initialization process can be configured in a file called the *ignition file*.

The ignition file must be in *conf* format

✔ Sample ignition file

```
eula=true

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

[config]
import=config_export.json
```

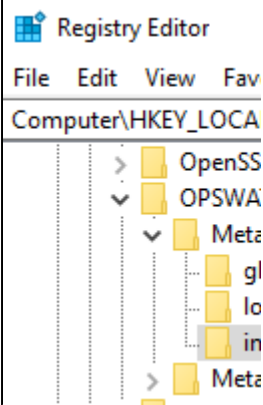
Ignition file fields

The ignition file must have the following fields:

Section	Key	Required	Description
	<code>eula</code>	Mandatory	<p>Whether to accept the End User License Agreement.</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p>i This key must be set to <code>true</code> to accept the EULA. Any other value will cause the initialization to fail.</p> </div>
<code>user</code>		Mandatory	<p>Initial administrator user account properties.</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p>i The Administrator role is granted to the account.</p> </div>
	<code>name</code>		User name for the initial administrator user account.
	<code>password</code>		<p>Password for the initial administrator user account.</p> <div style="border: 1px solid #ff69b4; padding: 5px;"> <p>! WARNING! Clear text password</p> <p>The password in this configuration file must be stored in its clear-text format and as so it may be visible for unauthorized parties.</p> </div>
	<code>email</code>		E-mail address for the initial administrator user account.
<code>config</code>		Optional	Further configuration options. Currently only <code>import</code> is supported.
	<code>import</code>		Path to a file in <code>json</code> format that contains a previously exported configuration to be imported.

Ignition file location


The directory of the ignition file is configurable:

Platform	Configuration method	Configuration section	Configuration key	Configuration example
Windows	Windows Registry	internal	ignition_file_location	
Linux	Configuration file			<pre> MetaDefender [internal] ignition_file </pre>


Detailed initialization process

1. After the product has been started, it looks for the ignition file in the configured (or default) location.
2. If an ignition file is found, then


- a. It gets validated, and if it is valid, then
 - i. Based on the information found in the ignition file:
 - ii. The EULA is accepted,
 - iii. The configuration is imported,
 - iv. The administrator account is created.
 - v. If any of the above steps fails, then the error is logged, and the initialization gets terminated.

 In this case the product starts normally: if for example the basic configuration wizard has not been completed yet, then it must be completed first.


- b. If it is not valid, then the error is logged, and the initialization gets terminated.

 In this case the product starts normally: if for example the basic configuration wizard has not been completed yet, then it must be completed first.

3. If there is no ignition file, then no initialization is performed.

 In this case the product starts normally: if for example the basic configuration wizard has not been completed yet, then it must be completed first.

Error rendering macro 'drawio' : null

 If the automated initialization fails for some reason (e.g. the ignition file is not in place) then the automated initialization may be retried fixing the problem (e.g. placing the ignition file to its lookup location) and restarting the *OPSWAT Metadefender Core* service.

Until the product is in pre-initialized status, it will try the automated initialization every time after a service (re)start.

Configuration

After the initialization is complete, the product is ready with the default and the imported configuration.

This configuration can be later changed calling the configuration API functions. For further details about the API see [8.1.9. Configuration related APIs](#).

10.3. Cloud Deployment

- [10.3.1. AWS Deployment](#)

10.3.1. 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:

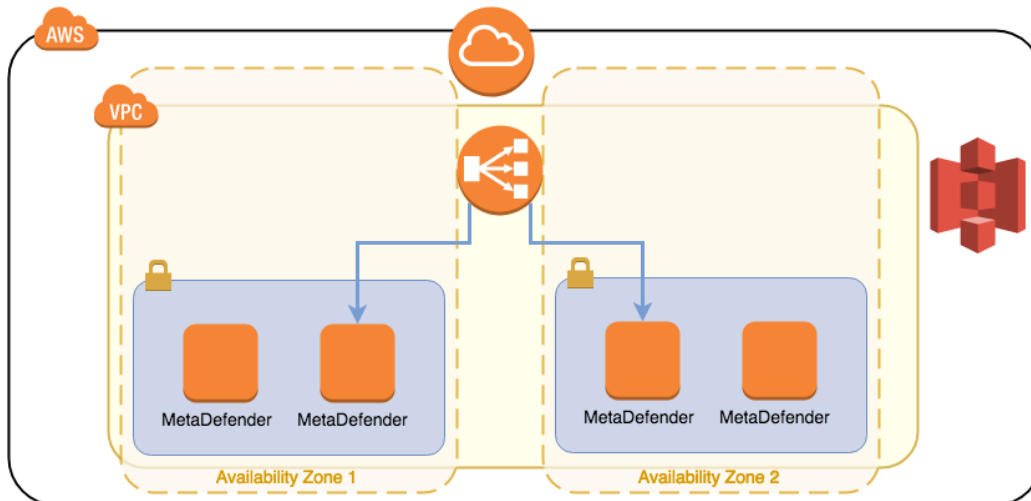
- [10.3.1.1. Install MetaDefender in AWS EC2](#)
- [10.3.1.2. AMI - Single MetaDefender Deployment](#)
- [10.3.1.3. AMI - Distributed MetaDefender Deployment](#)

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:

- [10.3.1.1. Install MetaDefender in AWS EC2](#)
- [10.3.1.2. AMI - Single MetaDefender Deployment](#)
- [10.3.1.3. 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

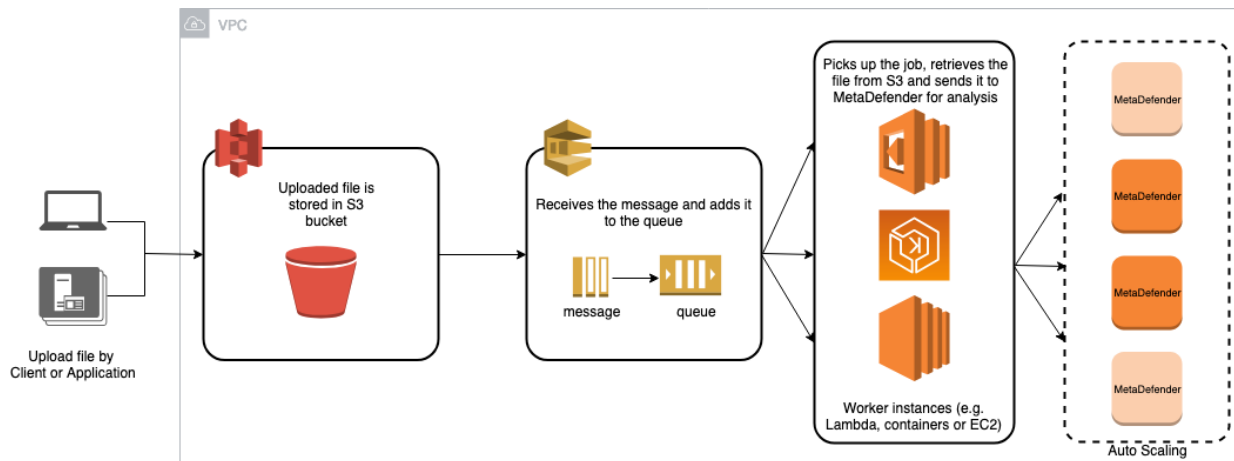
Deployment guidance

Deployment Assets

An ideal deployment in AWS will follow this process:

- Store the files in an S3 bucket before they are submitted to MetaDefender
 - Ideally MetaDefender would be deployed in the same region as the S3 bucket, to avoid additional traffic.
 - However, in the high unlikely event the entire region will fail, S3 provides a Cross-Region Replication, which will insure that the files are still saved and ready to be processed once MetaDefender services are back online.
- 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



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

- [10.3.1.1. Install MetaDefender in AWS EC2](#)
- [10.3.1.2. AMI - Single MetaDefender Deployment](#)
- [10.3.1.3. 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 [10.3.1.3. 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](#).

MetaDefender provides a direct update mechanism for the licensed analysis engines (all the engines listed in Inventory > Technology). The application logic will require a product update, however the licensed engines are automatically updated (in online deployments). Both the engine and the signature updates for Anti-malware engines will be automatically downloaded and deployed on a daily basis. We recommend to configure the product to check for updates at least every 4h (for more details see [3.4. Update settings](#)).

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 engines' signatures 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 queueing 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

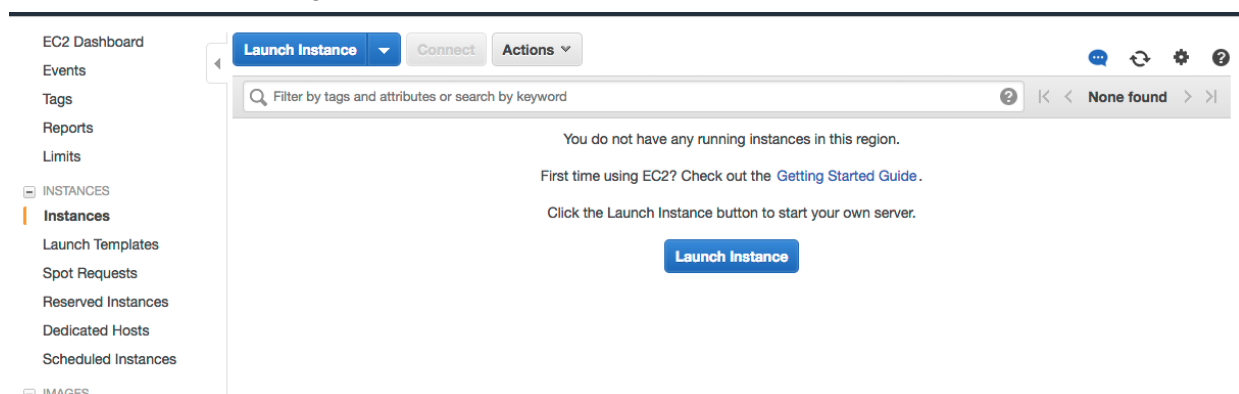
All MetaDefender documentation is available on onlinehelp.opswat.com

Localization

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

10.3.1.1. 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 Name	Architecture	Root Device Type	Virtualization Type	ENA Enabled	Action
Windows	Microsoft Windows Server 2012 R2 Base - ami-10375468	64-bit architecture, [English]	ebs	hvm	Yes	Select
Windows	Microsoft Windows 2012 R2 Standard edition with 64-bit architecture, [English]	64-bit architecture, [English]	ebs	hvm	Yes	Select
Windows	Microsoft Windows Server 2012 Base - ami-a20063da	64-bit architecture, [English]	ebs	hvm	Yes	Select
Windows	Microsoft Windows Server 2008 R2 Base - ami-e432519c	64-bit architecture, [English]	ebs	hvm	Yes	Select
Windows	Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, [English]	64-bit architecture, [English]	ebs	hvm	Yes	Select
Windows	Microsoft Windows Server 2008 SP2 Base - ami-205f3f58 (64-bit) / ami-6cd2b214 (32-bit)	64-bit architecture, [English]	ebs	hvm	No	Select
SUSE Linux	SUSE Linux Enterprise Server 11 SP4 (PV), SSD Volume Type - ami-7eb31906	64-bit architecture, [English]	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	VCPU	Memory (GiB)	Storage	Network	Accelerated Networking	Enhanced Networking
m5.large	General purpose	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
m5.xlarge	General purpose	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
m5.2xlarge	General purpose	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
m5.4xlarge	General purpose	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
m5.12xlarge	General purpose	48	192	EBS only	Yes	10 Gigabit	Yes
m5.24xlarge	General purpose	96	384	EBS only	Yes	25 Gigabit	Yes
m4.large	General purpose	2	8	EBS only	Yes	Moderate	Yes
m4.xlarge	General purpose	4	16	EBS only	Yes	High	Yes
m4.2xlarge	General purpose	8	32	EBS only	Yes	High	Yes
m4.4xlarge	General purpose	16	64	EBS only	Yes	High	Yes
m4.10xlarge	General purpose	40	160	EBS only	Yes	10 Gigabit	Yes
m4.16xlarge	General purpose	64	256	EBS only	Yes	25 Gigabit	Yes
c5.large	Compute optimized	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-91fc88a8 | 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 Additional charges will apply for dedicated tenancy.

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-ia-sa-east)	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

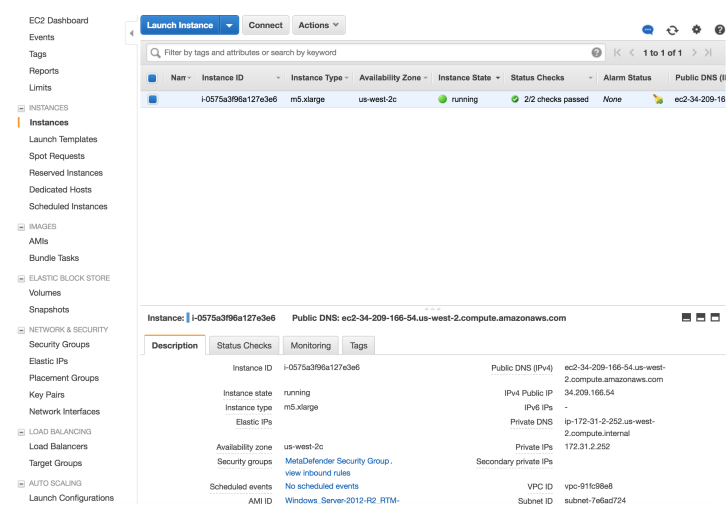
Add Rule

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

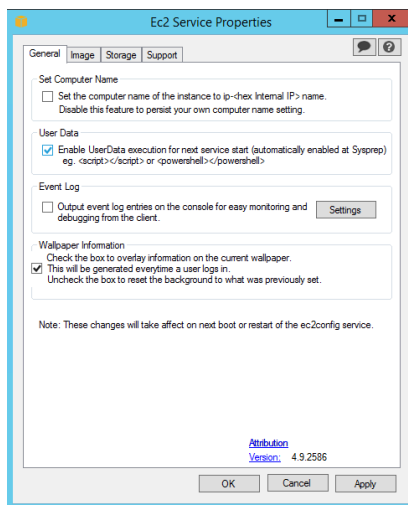
After you review the settings, hit Launch. In a few minutes the instance should become available



7. Additional steps

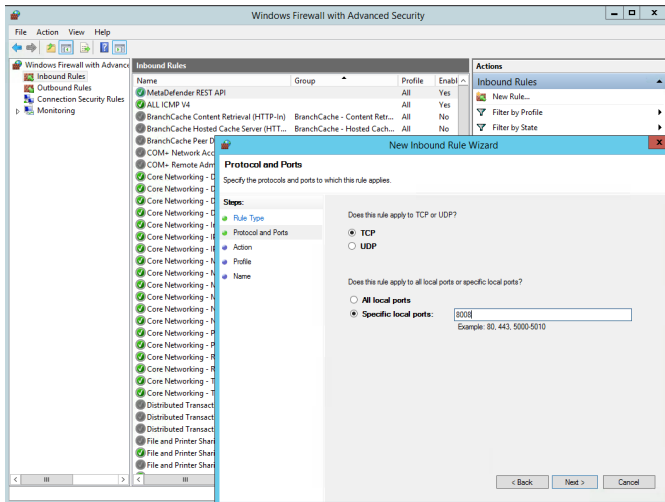
1. User Data

- 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).



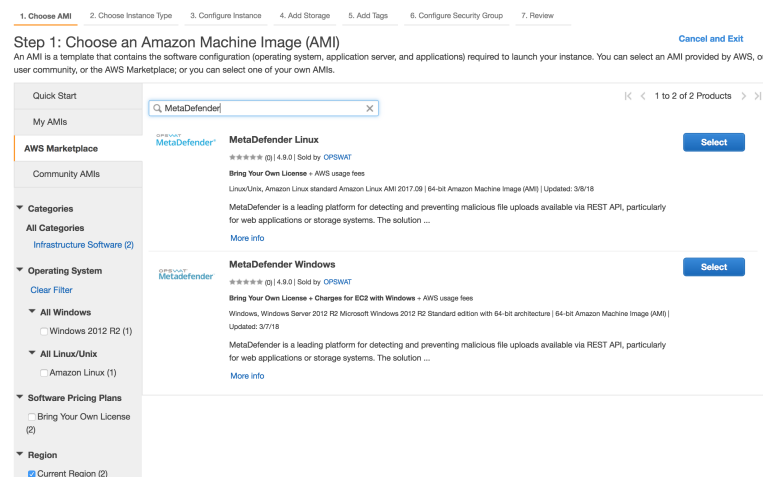
10.3.1.2. AMI - Single MetaDefender Deployment

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: [10.3.1.1. 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 highlighted), '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 with 'm4.xlarge' selected and 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, there are three buttons: 'Cancel', 'Previous', and 'Next'.

3. Finish the wizard, acknowledge that IAM roles are being generated and hit Create

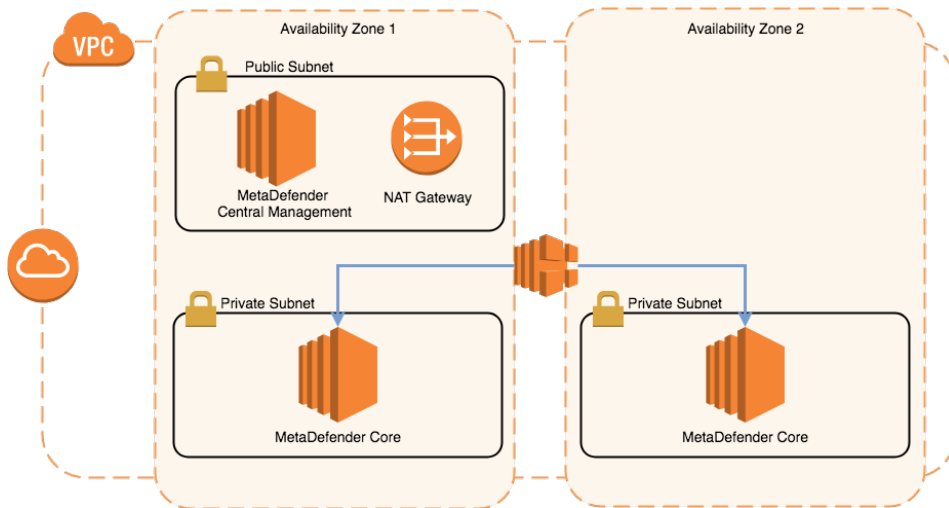
The CloudFormation script will generate the needed resources to provide the following flow:

- 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

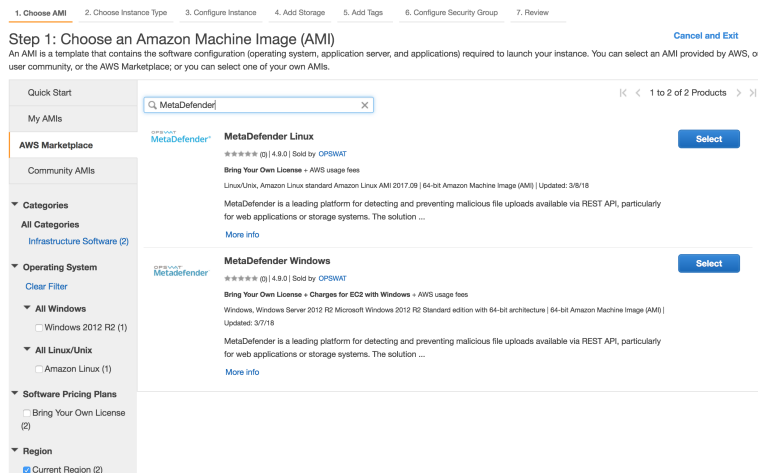
Resources:

- 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



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

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

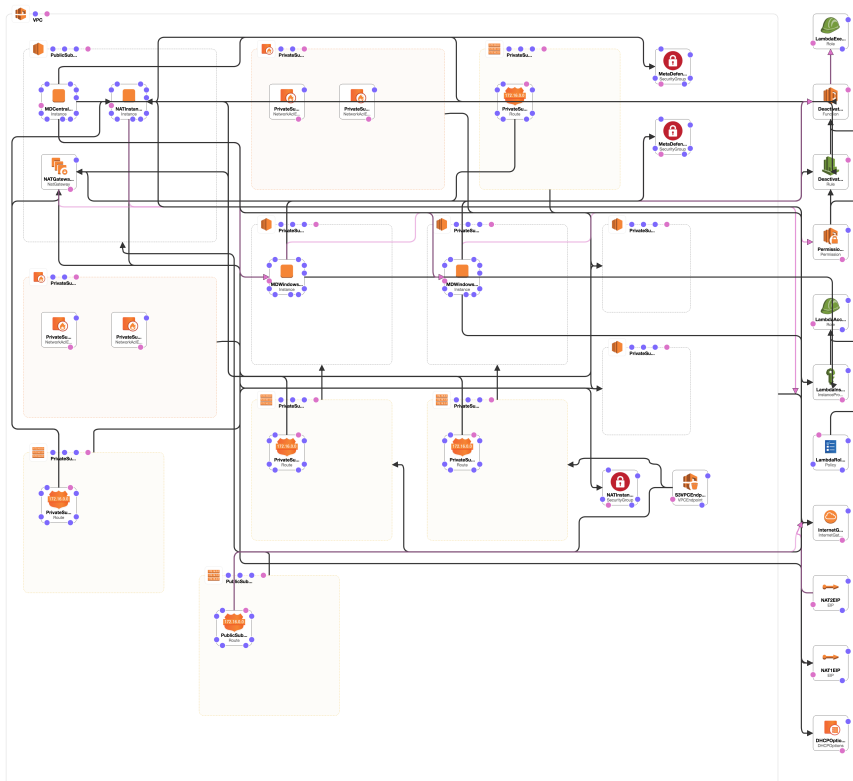
- User Data script (Powershell for Windows and shell for Linux) will be called which will:
 - change the credentials from the default admin/admin to admin /instance-id
- Instance shutting-down / terminate
 - Deactivate Lambda function will call the OPSWAT Activation Server to deregister the existing 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:



10.4. 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 as 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.

10.5. Using external load-balancer

- [10.5.1. HTTP\(S\) - Layer 7 load balancing](#)
- [10.5.2. DNS load balancing](#)

10.5.1. 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 cookie

No.	Stage	Task	Cookie usage
		Save the cookie and the data_id you got from the load-balancer	
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	4.3.4	-
OPSWAT Client	Windows: 7.6.247.0 Mac: 10.4.243.0	-
MetaDefender Email Security	4.3.0	-
MetaDefender ICAP Server	4.3.0	-
MetaDefender Vault	1.3.0	-

10.5.2. 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.
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	-
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	-

11. 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](#)

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?](#)


Engine Clean-up Tool

 For MetaDefender Core 4.18.0 or older, please follow instructions at https://onlinehelp.opswat.com/corev4/Engine_clean-up_instructions.html

Sometimes, during the engines downloading/deployment process, some of them may remain in **"failed"** or **"permanently failed"** status.

In that case, you could perform an engine clean-up by using MetaDefender Core built-in engine sweeper tool:

- Locate the tool in MetaDefender Core installation folder named `ometascan-engine-sweeper`

 Usage: `ometascan-engine-sweeper.exe [options]`
MetaDefender Core v4 Engine Sweeper.

Options:

- `?`, `-h`, `--help` Displays this help.
- `e`, `--engine <engine>` Engine name to clean. (`*` for matching any string, `?` for matching any character)
- `l`, `--list` List installed engines.
- `d`, `--retain-database` Retain engine's database.

- H, --host <host> Host of PostgreSQL server.
- P, --port <port> Port of PostgreSQL server.
- U, --username <username> Username for PostgreSQL server.
- D, --database <database> Database name to connect.

MetaDefender Core 4.19.0 database information to connect

- **Host and port:** Specified while installing Core 4.19.0. In default installation option, MetaDefender Core setups local and connect to PostgreSQL server at `localhost` via port `5432`
- **Username:** Specified while installing Core 4.19.0. In default installation option, MetaDefender Core uses username `postgres`
- **Database name:** MetaDefender Core `metadefender_core_xxxxxxx` - whereas `xxxxxxx` is the 6 characters in lower case following product code name (Windows: MSCW, Linux: MSCL) in your current Deployment ID.

For example: database name should be `metadefender_core_lrmgvs`

The screenshot shows the OPSWAT MetaDefender Core web interface. The left sidebar is dark blue with white text and icons for navigation. The main content area is light gray and displays the 'License Information' page. The license details are as follows:

Field	Value
Product ID:	MSCW-1c-EVAL-UNLIMITED
Product name:	MetaDefender Core for Windows - 1 engine package (Rev.C) - Evaluation
Expiration:	2020-09-30
Max nodes:	1
Max external scanners:	1
Deployment ID:	MSCWLRMgVSrVo1quszbyhmAK9ezcg1JJ4Njq
Activation key:	[Redacted]

Example usages

Assuming we will connect to PostgreSQL server with following info:

- localhost via port 5432
- username = postgres
- database name = metadefender_core_lrmgvs

Example 1: List all installed engines

```
ometascan-engine-sweeper.exe -H localhost -P 5432 -U postgres -D
metadefender_core_lrmgvs -l
```

Then the tool requires you to input PostgreSQL server password for MetaDefender Core (specified while installing MetaDefender Core)

Example output:

```
MetaDefender Core v4 Engine Sweeper.

Data directory detected: "C:/Program Files/OPSWAT/Metadefender
Core/data/"

Enter PostgreSQL password:
Querying installed engines in database...
Installed engines:
"oesis_3_windows"           | "Vulnerability Scanning"
"mdcloud_5_windows"        | "Threat Intelligence"
"7z_13_windows"            | "Archive engine"
"ds_3_windows"             | "Deep CDR"
"yara_5_windows"           | "Yara"
"dlp_8_windows"            | "Proactive DLP"
"clamav_1_windows"         | "ClamAV"
"filetype_1_windows"       | "FileType"
```

Example 2: Remove engine package and database package of Archive engine (e.g. 7z_13_windows)

```
ometascan-engine-sweeper.exe -H localhost -P 5432 -U postgres -D
metadefender_core_lrmgvs -e 7z_13_windows
```

Example output:

```
MetaDefender Core v4 Engine Sweeper.
```

```
Data directory detected: "C:/Program Files/OPSWAT/Metadefender  
Core/data/"
```

```
Enter PostgreSQL password:  
Engine(s) to clean: ("7z_13_windows")
```

```
The OPSWAT Metadefender Core service was stopped successfully.
```

```
The OPSWAT Metadefender Core Node service was stopped  
successfully.
```

```
PostgreSQL connection has lost. Please check the parameters.
```

```
The OPSWAT Metadefender Core service is starting.....  
The OPSWAT Metadefender Core service was started successfully.
```

```
The OPSWAT Metadefender Core Node service is starting...  
The OPSWAT Metadefender Core Node service was started  
successfully.
```

Example 3: Remove engine only (retain its database)

```
ometascan-engine-sweeper.exe -H localhost -P 5432 -U postgres -D  
metadefender_core_lrmgvs -e 7z_13_windows -d
```

Example output:

```
MetaDefender Core v4 Engine Sweeper.
```

```
Data directory detected: "C:/Program Files/OPSWAT/Metadefender  
Core/data/"
```

```
Enter PostgreSQL password:  
Engine(s) to clean: ("7z_13_windows")
```

```
The OPSWAT Metadefender Core service was stopped successfully.
```



```
The OPSWAT Metadefender Core Node service was stopped
successfully.
```

```
PostgreSQL connection has lost. Please check the parameters.
```

```
The OPSWAT Metadefender Core service is starting.....
The OPSWAT Metadefender Core service was started successfully.
```

```
The OPSWAT Metadefender Core Node service is starting...
The OPSWAT Metadefender Core Node service was started
successfully.
```

Example 4: Remove all engines

```
ometascan-engine-sweeper.exe -H localhost -P 5432 -U postgres -D
metadefender_core_lrmgvs -e "*"
```

Example output:

```
MetaDefender Core v4 Engine Sweeper.
```

```
Data directory detected: "C:/Program Files/OPSWAT/Metadefender
Core/data/"
```

```
Enter PostgreSQL password:
```

```
Engine(s) to clean: ("ds_3_windows", "7z_13_windows", "clamav_1_wi
ndows", "mdcloud_5_windows", "oesis_3_windows", "dlp_8_windows", "
filetype_1_windows", "yara_5_windows")
```

```
The OPSWAT Metadefender Core service was stopped successfully.
```

```
The OPSWAT Metadefender Core Node service was stopped
successfully.
```

```
PostgreSQL connection has lost. Please check the parameters.
```

```
The OPSWAT Metadefender Core service is starting.....
The OPSWAT Metadefender Core service was started successfully.
```

```
The OPSWAT Metadefender Core Node service is starting...
The OPSWAT Metadefender Core Node service was started
successfully.
```

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`.

12. Release notes

MetaDefender Core v4.19.0 Released on 27 Aug 2020	This is a major release primarily focused on new features
New features / Behavior changes	
New Database Management System (PostgreSQL) to replace SQLite (Data migration supported)	<p>PostgreSQL is now MetaDefender Core's new database management system to replace its predecessor SQLite. That expects to step by step help the product easily scale out, network based database support, gain better performance, migrate high load bottleneck and native high availability. MetaDefender Core supports users to create a local PostgreSQL server running in the box, or allow leveraging a pre-installed remote PostgreSQL server.</p> <p>Data migration auto runs in background upon product upgrade.</p> <p>For large database migration, MetaDefender Core comes with a web-based data migration to walk users through quick steps to move all your SQLite data to PostgreSQL at ease.</p>
FIPS-140 security compliant	We are now FIPS-140 compliant with a new support for RSA186-4 on OpenSSL
Native proxy management with authentication support	<p>MetaDefender Core now will allow users to control proxy settings for product (instead of using system configuration), and also support authentication for proxy which is not possible on older Core versions.</p> <p>That comes with a UI configuration support on MetaDefender Core management console.</p>

Harden Nginx web server settings for security	Secure MetaDefender Core web server even more based on nginx vendor guideline to protect your MetaDefender server from being vulnerable (i.e. cross site scripting, MIME sniffing, TLSver 1.1 or below forbidden) Still we keep all supported functionalities working as expected.
Nginx web server statistics (on web server report)	Support to enable better statistics for the HTTP Server for web server healthcheck and debugging.
Origin client source address retrieval when running via load balancer	MetaDefender Core now will be able to retrieve your origin client source address even when the client communicates over a load balancer.
Enhanced search for processing history page	Searching by attributes represented via corresponding column on the list.
Enhanced user experience on statistics page	Instant statistics processing data calculated and visualized on UI
Logic improvement to handle better against sanitization timed out	New logic implemented on MetaDefender Core to offload concurrent tasks on Deep CDR engine, and to reduce sanitization timed out as a result.
Enhanced log messages	Log events enhanced with more sufficient and clear information, easier for traceability while troubleshooting.
Pre-check mode for file submission	Refuse file upload immediately when MetaDefender Core does not have enough disk space to handle, expecting to hit error 400. This is to avoid wasting upload time on big files.
Sanitized file information appended into JSON scan result	Including sanitized file size and its SHA-256 hash value.

Blacklist overridden on nested files within archive	New configurable setting to allow overriding blacklist enablement on nested files within an archive.
New engine sweeper tool bundled into the product	New engine sweeper troubleshooting tool tailored for PostgreSQL, and now it is bundled into MetaDefender Core product (not a separate download tool).
Bug fixes	
Setting inputs validation	Threat detection threshold, wizard password and SSO profile settings affected.
Batch signature sometimes contained redundant characters	That could make signature becomes invalid.
Processing time of nested files in archive not calculated correctly	Processing time of nested files could be very big due to incorrect calculation (but actually they are processed much faster).
Statistics page to support multiple users simultaneously	The statistics UI now could handle multiple users query at the same time.
Proactive DLP timeout setting mistakenly reset upon engine restart	The setting was reset back to default value (3 minutes).

12.2 Proactive DLP Release Notes



Proactive DLP features such as redaction and watermark are available with MetaDefender 4.16 or newer.
The features in v2.1 are available with MetaDefender 4.17 or newer.

v2.4.1

Release date: August 8, 2020

- Improved memory usage
- Improved IPv4 and CIDR search
- Added threaded comment search and redaction in Excel files
- Up to 40% speedup when scanning Excel files

v2.4

Release date: July 7, 2020

- Utilize column and row header to improve certainty level in Excel
- Detect sensitive info in file properties with regular expressions
- Custom keyword list for regular expression
- Support redaction feature on Linux
- Performance improvement: faster processing, less resource usage
- [New system requirements on Linux](#)
- End of support Centos 6, Debian 8

v2.3.2

Release date: May 20, 2020

- Better context calculation for Excel and PDF
- Improve IPv4 detection in TXT
- Distinguish between "Failed to detect" and others

v2.3.1

Release date: April 21, 2020

- Threaded comment redaction in Excel files.
- Slightly increased PDF scan performance.
- Improved certainty calculation for MS Office and PDF files.
- Fixed wrong context when a single cell in an Excel file contained the same hit multiple times.

v2.3.0

Release date: April 7, 2020

- Support Optical Character Recognition (OCR) for PDF (Windows only)

- Redact sensitive information for Microsoft Office Excel (XLS/XLSX)
- Better detection method, reduce false positive

v2.2.1

Release date: Feb 12, 2020

- Improve IPv4/CIDR detection performance
- Better handling temp files
- Remove "Parse Binary" option

v2.2

Release date: Jan 6, 2020

- Supports watermark addition for PDF
- Redact sensitive information for Microsoft Office Word (DOC/DOCX)
- Support DLP in Linux with limited functions (work with MetaDefender Core 4.17.1 or newer)
- Redact sensitive information based on certainty level (work with MetaDefender Core 4.17.1 or newer)
- [Sample Regular expressions](#) to detect Personally identifiable information (PII): email, address, full name, date of birth, driver license, phone number, bank account number

v2.1.2

Release date: November 27, 2019

- Better error message when an input PDF file is corrupted

v2.1.1

Release date: October 31, 2019

- Better displaying the words before and after a hit in PDF

v2.1

Release date: September 8, 2019

- Supports IPv4, Classless Inter-Domain Routing (CIDR) detection
- Supports remove metadata for TIFF, GIF file
- Better CCN detection

v2.0.1

Release date: August 15, 2019

- Better watermark and redaction handling when a system is under high load
- Improve CCN detection

v2.0

Release date: June 28, 2019

- Proactive DLP as new name
- Certainty score for sensitive data detection
- Redact sensitive information for text-based PDF file
- Watermark addition for JPEG, TIFF, PNG, GIF
- Supports remove metadata for JPG, PNG file

v1.0.3

Release date: February 18, 2019

- Improve detection for Microsoft Access format
- Improve context for hits
- Improve processing speed (20%)

12.3 File Type module Release Notes

v5.2.26

Release date: September 1, 2020

- Better detection for Microsoft CAB and Installshield CAB file format

v5.2.25

Release date: August 10, 2020

- Improve JPEG, ACE detection
- Improve mismatched detection logic for text file format

v5.2.24

Release date: July 6, 2020

- Support new file type detections: DCM, WEBP, LNK, WSP, JP2, ODS, OTS

v5.2.23

Release date: May 20, 2020

- Support new file type detections: OpenSSL encrypted with a salted password, WDP, ALZ.
- Improve DWT and DWS detection, Encrypted Microsoft Office file detection

12.4 Archive module Release Notes

v5.3.5

Release date: September 1, 2020

- Improve ACE, CAB extraction

v5.3.4

Release date: August 8, 2020

- Support ACE extraction

v5.3.3

Release date: July 6, 2020

- Better split encrypted archive handling
- Improve 7z self-extracting archive processing

v5.3.2

Release date: May 20, 2020

- Support ALZip (ALZ) extraction
- Better EML, MSG extraction

12.4 MetaDefender Core archived release notes

Version v4.18.0

Release Date: 26 May 2020

New features:

- **Single Sign On (SSO) Authentication**
 - Additional to already-supported various authentication models (Local, Active Directory, LDAP), now MetaDefender Core also supports authentication using SSO with widen integration coverage for most of Identity Providers (IDP) via SAML 2.0 and OpenID Connect 1.0 standard support.
- **Brand New MetaDefender Core API Guide (Sample Codes Available)**
 - Brand new design and standardized API documentation (following OpenAPI V3 specification), auto-generated sample codes on various programming languages supported helps your API integration even easier.
- **Database Defragmentation and Optimization**
 - When your scan database grows big, it might cause performance degradation (e.g. timeout on client requests). Now MetaDefender Core administrators can be notified on the UI (also warning logs), and you are supported to perform database defragmentation and optimization including multiple stages to vacuum and defrag your database without loss of actual scan data.

As a result, your database file size could be reduced which helps boost processing performance tremendously over usage time.
- **Comprehensive Statistics On Processing Data**
 - Featured in an interactive UI help you gain deeper insights on your processing filtered by every workflow rule, breaking down into each file type. Last but not least, you are also supported to select time range to calculate statistics data.
- **Data Reporting (Business Intelligence)**
 - When enabled, MetaDefender Core will auto-sync your historic processing data to OPSWAT dedicated servers. That helps us gain more visibility on your processing load and how our product is being used, and thus we could improve our product to accommodate your use-case better. You are supported to customize which piece of information should be shared with OPSWAT, and when to share.

By default, this feature is disabled to respect your privacy rights and save performance impact.
- **Webhook Continuous Improvement**
 - New setting mode to control callback timeout and retry (configurable via REST API)
 - Stability improvement to avoid being stuck on callback and crashing on Node service
- **High Load Processing Improvement**

- When running under high load, file type usually returns "Not Available" caused by various reasons. Product logic enhanced to elaborate causes, and improved stability on the product.

We keep working on this matter to ensure our customers have the most stable product running under high load as much as possible.
- Configurable Behavior On Archive Extraction Failure
 - Configurable settings on workflow rule to let you tweak and decide MetaDefender Core final scan verdict when a processing archive file failed to extract for some reasons.

The default selection on each designated extraction failure reasons (invalid file structure, extracted partially,...) will be different on each workflow rule depending on use-case characteristics. Please make sure you are aware of the new settings and adjust them accordingly tailored to your security demand.
- Archive Extraction Failure Exposure
 - Archive extraction failure reasons exposed to both REST API response and UI.
- Encryption on Archive & Document Sanitized Files
 - Help retain password protection on supported archive and document files (.zip, .7z, .pdf, MS Offices) upon sanitized successfully.
- Sanitization Forensic Details Enhancement
 - When sanitized successfully, an even more comprehensive forensic available on both UI and REST API level letting you know all processed object details (e.g. what exact hyperlink was sanitized).
- Processing File Information Enhancement (File Type Category)
 - File type category is now available on REST API response along with other already-supported file information.
- MetaDefender Core Log Rotation Experience Improvement
 - This feature is now enabled by default applicable to both upgrade and fresh install scenario.
- Workflow Rule For MetaDefender For Secure Storage
 - With the best practice to serve MetaDefender For Secure Storage use-case, we have a new dedicated workflow rule with designated configurations.
- Archive Processing Result Retrieval API Enhancement
 - Applicable to pagination fashion polling `GET /stat/log/scan?first={start_item}&size={number_of_items_next}` , now the action ran information available in JSON response

- FIPS Object Module 2.0 Bundled
 - Operating product in FIPS mode enabled on Operating System

Fixed:

- File Scanning Process Stuck
 - When the custom engines stopped its process for reasons (updating while scanning / crashed), the running scans on Core could not be finished and stayed at 95% forever.
- MetaDefender Core Service Crashed (Webhook Mode)
 - When using webhook mode, and callback can't be sent back to client, the MetaDefender Core service could be crashed.
- Memory Leak While Updating Engines Automatically
 - The memory could be leaked on *ometascan-node* process while updating engines in online mode.
- Scan Details Missing From Recursive Scan Results
 - While fetching scan results on all nested files in big archive file *GET /archive/{data_id}* the "scan_details" field from the top-level root archive was empty.
- Input Field Overflow On Management Console UI
 - Preventing invalid values putting in UI configuration controls (Deep CDR, Archive)
- Archive Timeout File Skipped For Scanning
 - None of AV engines actually scanned archive file when archive timeout occurred

Version v4.17.3

Release Date: 06 Apr 2020

New features:

- Configurable setting to run database optimization
 - Database optimization has been introduced since Core 4.17.0 to help run database queries faster. The downside is while running (for a few seconds), Core queries hold up causing possibly timeout on client side.

This new setting allows users setting specific time to run database optimization task (to avoid peak hours), or just disable to prevent this task from running (to avoid performance degradation while running). Learn more how to configure: [3.2.1. Startup Core Configuration](#)
- Scan database rollback mechanism

- In some circumstances (e.g. Core crashes, out of disk/memory etc.), the atomicity of product database could be compromised causing inconsistent processing scan history returned. Rollback mechanism helps retain that atomicity of database.
- Logging improvement with configurable settings
 - Log rotation for Core, Node, Nginx web server logs (Configurable settings supported). Learn more how to configure: [3.2.1. Startup Core Configuration](#) and [3.2.2. Startup Node Configuration](#)
 - More comprehensive support package (to include engine and database info, Nginx web server info).
 - More informative log message on sanitization related tasks.
 - Sensitive info redacted (on debug level logging mode).
 - Performance impacted warning on both MetaDefender Core GUI and logs when the scan database (ometascan.db.sqlite) starts growing up big (>10 GB).
- Webhook mode continuous refinement
 - Retry to send scan results to client upon network interim disconnected.
 - Resend file scan results to client after Core service restarted.
- New download mechanism for Processing History on MetaDefender Core management console
 - Support IE / Edge web browsers to download processing history report.
- MetaDefender Drive use-case better support when engine packages corrupted
 - Support to re-new engine packages to re-download engine packages again when corrupted (due to upon unexpected reboot).
- Central Management v7 support to revert download source when unhooked
 - Respect skipped scan settings (Whitelist / Blacklist) to keep backward compatibility, and also save Core resource for processing files as well.
- RoleIDs JSON field validated when creating / modifying user
 - Effective to *POST /admin/user* and *POST /user* endpoint REST APIs. Role ID value must be an array of strings according to current user guide.
- Account name value validated on Core wizard setup
 - Effective to "Admin User Setup" screen during wizard setup, "Account name" validated against special characters (e.g. @ & \)
- Better support for sanitized file download when under load

- When under load and certain circumstance with system write failed, the sanitized download on the same file might return 404 HTTP response (not found) to client. Enhanced our Core caching mechanism to ensure next time sanitization on the same file will not rely on the previous failed time.
- Minor UI changes
 - Hide "Edit Workflow" button in "Workflow Templates Management" screen
 - Remove space between date and time in "Definition date" field on "Modules" screen

Fixed:

- Data tunnel between Node and engines could be lost under high load
 - When occurred, expecting to see " process communication timed out" message repeatedly in Node log, and none of engines could be able to scan files.
- Node crashed when swapping engines during update
 - Node could be crashed under certain circumstances, applied to swapping engine instances during update.
- File processing was stuck at 95%
 - Encountered when custom engine stopped its process, all of running tasks on that engine becomes stuck, or when ClamAV engine can't return consistent scan result during its engine update.
- Overflow issue with unexpected inputs
 - Overflow value issue could occur within product causing unexpected behavior or result.
- Unexpected result with non-ASCII password protected document scanning
 - When occurred, document file could not be sanitized properly.
- Proactive DLP displayed wrong result within archive scanning
 - When occurred, Proactive DLP engine could return misleading result (Not scanned) while archive file processing result is "Sensitive Data Found".
- Session expired on IE / Edge web browser
 - When session cleared out, authenticated users could be logged out repeatedly due to session expired error on MetaDefender Core management console.

Version v4.17.2

Release Date: 03 Mar 2020

New features:

- Quarantine cleanup task no longer blocks Core service starting procedure
- Empty file submission is no longer be blocked at REST API level
 - Retain same behavior on Core 4.16.3 or older, to support back some corner use-cases from MD Kiosk and ICAP
- Custom engine initialization enhancement
 - Increased timeout to 10 minutes to support engine deployment on under-specs hardware (formerly 1 minute)
- Processing history report enhancement
 - Added "username" column to the processing history export from MD Core
- Validation mechanism on file scan and batch init REST API changed
 - When using via REST API, no longer validate session cookie, only API key header is validated when exists (same behavior on Core 4.16.3 or older)
- Configurable Proactive DLP timeout is supported
 - Support to adjust timeout for Proactive DLP handling (formerly fixed on 3 minutes)
- Respecting whitelist and blacklist configurations
 - Respect skipped scan settings (Whitelist / Blacklist) to keep backward compatibility, and also save Core resource for processing files as well.
- Response for POST /login no longer returns cookie back to client
 - When using via REST API, by default the response for POST /login no longer returns cookie back to client (same behavior on Core 4.16.3 or older, to avoid breaking F5 LTM scenario with cookie header is auto added)
- Removing failed dummy scan results on Core processing history UI due to upload failure
 - When file upload is failed for some reasons (e.g. network corrupted) between clients and MD Core, dummy record results are still available and displayed on Core processing history UI, but actually MD Core never processed those files, and client never got results from MD Core on those files. Those dummy records will be removed since this version to avoid misleading.

Fixed:

- Deadlock could possibly happen when engine update task is timed out
 - When encountered, all files happens in "Failed" result with "Not available" result for file type analysis after timeout hit (~ 70 seconds), and only Node service relaunched can bring the scanning be operational back.
- Node service could be crashed when archive engine crashed

- When archive engine crashed for some reasons, Node service could be crashed as well (but not happened all the time)
- Core and Node service could be crashed when under high load
 - Core and Node service could be crashed when under high load
- Archive file extraction when timed out, or failed to extract, the original archive itself could not be scanned by AV engines
 - When archive extraction hits timeout or failed to extract, the original archive itself could not be scanned by AV engines
- Core could return 404 not found HTTP(S) response to client for sanitized file download API request
 - When processing the same file many times on Core, it could return 404 not found HTTP(S) response to client (e.g. MD Email) due to file sync issue between Core and Node
- Memory leak issue on Core process
 - The process ometascan could be leaked on memory with auto update mode enabled and Proactive DLP engine is enabled
- Anonymous user can't submit file scan to MD Core web scan UI
 - When not logged in, anonymous user can't submit file scan to MD Core web scan UI (error: Invalid session ID given)
- Core service can't restart due to configurations corrupted while running Proactive DLP engine
 - Core service can't restart due to configurations corrupted while running Proactive DLP engine
- Document files inside sanitized password protected archive file could not be sanitized
 - When document file is also treated as an archive file, there was a bug on archive compression level calculation to prevent document files not being sanitized inside original archive file
- Timeout on hash calculation task resulted as Blocked regardless of "override scan results classified as allowed" setting
 - When this task timed out, regardless what users set on "override scan results classified as allowed" setting, the final verdict were "Blocked"
- Webhook continuous fixes and updates
 - Duplicated callbacks returned to client

- Support retry mode for sending callback to client (when client is temporarily unresponsive etc.)
- Enhance validation callbackurl header against IP version 6 and domain format
- Minor UI fixes
 - Added margin to bottom edge of scan result UI
 - Name of rights under user management did not match to Inventory

Version v4.17.1

Release Date: 06 Jan 2020

New features:

- Archive extraction details
 - Available on both scan result UI and
- Advanced engine configurations enhancement
 - UI interactive and schema based for advanced engine settings
- Proactive DLP engine integration enhancement
- MetaDefender Cloud integration enhancement
 - MetaDefender Cloud API version 4 upgraded
- Engine integration enhancement to avoid product crash
- User validation update for file and batch processing
 - File scan and batch init endpoint API is now validated on API key input when that key information is available.
- More ready for adding password back to sanitized archive and document files
- Minor UI update

Fixed:

- Core could become unavailable to clients when under high load
 - Data communication channel between Core and Node service could be broken when under high load
- Processing giant files (> 50 GB) could be stuck at hash calculation
 - Hash calculation with pre-set timeout value (10 minutes) could be exceeded when processing giant files (> 50 GB) and then stuck at 5% forever
- Scan could be failed with "not available" result for File type analysis when under certain circumstances

- Memory leak issue on Core process
- Temporary files not cleaned up when archive extraction timed out
- Webhook continuous fixes and updates
 - Redundant warning log messages populated even when not using webhook mode
 - Core could be crashed itself when trying to close a not-found batch with callback
 - Callback sent to client with wrong status when Core is restarted
- Visibility level smaller than full details might break batch result display
- Minor UI fixes
 - The field "File Password" on the file processing UI not cleared up after empty file selected

Version v4.17.0.1

Release Date: 27 Nov 2019

Fixed:

- Deadlock issue on batch handling
 - Under certain circumstances, a deadlock issue could encounter locking database from being queried (timeout on REST requests)

Version v4.17.0

Release Date: 14 Nov 2019

New features:

- Callback URL (Webhooks) for file and batch scanning (to avoid polling result from client)
 - Support for individual file and batch scanning to eliminate polling mechanism i.e. MetaDefender Core will notify client based on designated / configurable callback URL whenever an individual scan finished or a batch can be closed.
- Security enhancements
 - Harden MetaDefender Core management console against security vulnerabilities found on pen-test's result
- Log correlation from parent archive file to child files
- Comprehensive failure reason on archive extraction (available on JSON response)
- Sanitization output name on password protected document fully respects value set on UI
 - No longer appended with fixed value "decrypted_document" in output name

- UTF8-encoding password for file scan request via REST
 - File scan REST API now supports "archivepwd" header with encoding password
- Total number of files inside archive (all recursive levels), available on scan result UI
- Archive scanning enhancements
 - Better integration logic with archive engine
 - Support empty folder inside archive engine
 - Not try to extract archive file if extracted size exceeded is anticipated
- Database query optimization
- Processing input refinement
 - Empty file scan request no longer is accepted at API level
- MetaDefender Core's nginx log location no longer requires double backslashes
- UI enhancements
 - Password field supported for password-protected archives or documents on the UI (web scan)

Fixed:

- Relaunching Proactive DLP engine process after timeout could crash Node service
- Nginx custom configuration file and certificates is unexpectedly erased when upgrading MetaDefender Core
- Overall failure on scan could encounter when system goes wrong while analyzing file type
 - When something wrong occurred while analyzing file type, the scan process could be immediately stopped and ended up as overall failed.
- Override scan result setting did not apply properly to empty batch
- Changes on workflow template could interfere Core service
 - Excluding engines in workflow template could make Core service failed to start
- Return incorrect REST response code when closing batch with invalid API key
- Fail to create local user directory under certain settings
 - Creating "Local" user directory type could be failed when "Enhance password policy" setting is unchecked
- Nginx access log location customized on registry is not retained when upgrading MetaDefender Core

- When upgrading MetaDefender Core, nginx log location (nginx_logfile) could be unexpectedly reverted back to default value, not retained to what users configured.
- Minor UI fixes
 - Some display and hyperlink minor issues related to table and navigation
 - Hitting cancel batch button on UI causing error

Version v4.16.3

Release Date: 16 Oct 2019

New features:

- Support new header (metadata) for file submission API
- Enhance MetaDefender Core service starting procedure
- Enhance engine update procedure
- Remove restriction on Core version retrieval REST API

Fixed:

- MetaDefender Core service on Linux could not be started when running on FIPS mode
- MetaDefender Core service could be unexpectedly restarted when engines repeatedly crashed
- Uninstalling MetaDefender Core did not terminate its processes properly (nginx)
- Password protected document could not be decrypted properly for data sanitization
- Uninstalling MetaDefender Core did not clean up its leftover data folder

Version v4.16.2

Release Date: 10 Sep 2019

New features:

- Restrict APIs based on user roles (configurable)
- Support displaying and filtering username on processing history UI
- Enhance logging with Yara matched rules appended
- Upgraded nginx web server component to latest version 1.16.0
- Add new scan result - Unsupported file type
- Refined JSON output when users want to quarantine items which are already in quarantined folder

- Updated UI (minors)

Fixed:

- In-progress files could be deleted mistakenly, causing failures when scanning
- Engines repeatedly disable and re-enable
- File processing could be stuck until archive timeout value reached
- Non UTF-8 characters were not displayed correctly when exporting process history via UI
- Dependency installation issue on Ubuntu 18 & Debian 9

Version v4.16.1

Release Date: 12 Aug 2019

New features:

- Supported to pin & unpin engines and their database on the UI to prevent auto update being applied
- Gently handled timeout on Archive and Deep CDR engines
- New logging mode for archive processing troubleshooting
- Enhanced logic for non-archive file processing
- Limited number of characters on some applicable text fields on the UI
- Enhanced security with unquote service exploit

Fixed:

- Node crash issue when under high load
- Issue with resource manager with in-use temp files
- Memory leaking issue on archive engine process
- Memory leaking issue on Node process
- Batch handling issue causing failure on batch
- Stuck scan issue at 5% when parallelcount_7z_extract is set with definitive number
- Detection issue on Proactive DLP engine with regex rule applied
- UI issue where Yara result is not displayed
- UI visibility issue on Internet Explorer (IE) web browser
- Some other minor UI issues
- Wrong timezone set on exported CSV scan report

Version v4.16.0

Release Date: 08 July 2019

New features:

- Proactive DLP engine (ver 2.0) integration
- Password policy enforcement
- Support archive partial sanitization for Vault and Email integration
- New REST API for local update server source
- Better handle archive sanitization timeout
- Support configurable settings for archive extraction and compression parallel count
- Enhance syslog message format
- Retouch UI
- Better logging with timeout on engines
- Enhance logic to apply engine definition files

Fixed:

- Wrong outcome when archive engine process unexpectedly stopped
- Wrong UI result on sanitization timeout
- Memory leak issue on engine package uploading

Version v4.15.2

Release Date: 19 June 2019

Fixed:

- Stability issue
 - Potential deadlock issue on batch scan handling prevents querying batch information
- Usability issue
 - Enhanced error log messages when the engine process is terminated due to engine timeout
 - Exposed log messages on warning level when there is an archive extraction failure

Version v4.15.1

Release Date: 06 June 2019

New features:

- Partial sanitization use-case for archive file types
- Clarified error messages for terminated engine processes
- New REST API for cleaning up idle batch scans
- UI improvement
- License EULA update

Fixed:

- Stability issue
 - Potential memory handling issue that could cause the node service to crash
 - Empty and read-only files are no longer extracted
- Usability issue
 - Not able to remove abandoned temp. files of archive files when they are empty and read-only
- Security issue
 - AD user credential is not masked properly on the audit log while sending over to AD server for authentication
- Scanning batch REST API issues
- Engine custom configuration
- UI issues
 - Dashboard refresh button sometimes did not work as expected
 - List of processing records didn't show when changing "number records per page" while not staying at first page
 - Not user-friendly error messages when adding duplicate hashes to a blacklist
 - Typos on the UI

Version v4.15.0

Release Date: 06 May 2019

New features:

- Data Sanitization details displayed on Core management console
- User password recovery and reset enforcement
- API rate limiting
- Support Windows Server 2019 (The support is still on beta)

- Suspicious results returned by engines are now configurable to be handled as a different circumstance (infected, ignore)
- Improve usability
 - Return zero for definition dates on non-AV engines' database
 - "Select all" option added to the Data Sanitization page
- Improve handling on node
 - Improve cleanup mechanism on nodes to avoid deleting files in use
 - Improve validation process when starting the node service, support to try creating temp. folder with a configurable timeout

Fixed:

- Fixed stabilization issues that possibly caused Node services to crash
- Scan batch API closing issues
 - No longer returns total time of -1 in response
 - Should not randomly fail due to " 400 - One or more scan is still in progress" even when all linked scans already finished
- Upgrading Core when installed in a non-default installation path prevented users from choosing another folder path by mistake
- UI issues
 - The "Process File" button no longer disappears in case of sanitization failed
 - Max recursive level under archive handling tab must equal 1 or greater
 - non-Unicode file name displayed on web scan UI encoded properly
- Sanitizing empty archive file no longer returns failed

Version v4.14.3

Release Date: 01 Apr 2019

New features:

- Support built-in integration with OPSWAT Central
- New setting for archive sanitization timeout
- Add process time field into CSV exported history report
- Effectively wipe out necessary data from support package
- Revamp Inventory UI page with "Utilities" group

- More relevant REST error message for scan request where file is non-existent / inaccessible
- Syslog message for scan-finish event more comprehensive
- Consolidated scan info for archive scan result fetching
- Add libcurl4 as alternative dependency to libcurl3 for better support on Ubuntu 18.04
- Outputs and indicators for Threat Intelligence feature on Quarantine UI page more relevant and informative

Fixed:

- Node becomes unstable under high load processing
- Closing batch with ongoing scans could result in failed verdict on batch
- Inconsistent behavior with password protected document
- Temporary files are not cleaned up when cancelling an ongoing scan
- Inconsistent returned error message between batch and file scanning via REST
- DLP verdict returns incorrect value for some cases
- Logs in support package did not handle non-Unicode characters

Version v4.14.2

Release Date: 28 Feb 2019

New features:

- New result page, new look and more informative badge

Fixed:

- Engine configurations could not be saved
- Make error message more relative for case where file exceeded the size limit
- Pinning engines and their databases independently

Version v4.14.1

Release Date: 31 Jan 2019

Fixed:

- Missing "pinned" option from "/stat/packages" JSON response
- Inconsistent "progress_percentage" and "result" values
- Hash validation (blacklist/whitelist)
- Upload performance

Version v4.14.0

Release date: 19 Dec 2018

New features:

- [Send quarantined files to MetaDefender Cloud](#) for scanning
- Automation support:
 - Support ignition file to [automate the welcome wizard](#)
 - [Configuration API functions](#) have been documented
- [Enhanced password policy](#) can be enabled for local users
- Files with [Failed to sanitize result can be set to be blocked](#)

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 .Ink 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 monitor Metascan v4 for Linux instances

- Able 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

13. Legal

- [Copyright](#)
- [MetaDefender Export Classification](#)

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.

MetaDefender Export Classification

MetaDefender United States Export Classification Number (ECCN) is 5D002, subparagraph c.1 Exports and re-exports of MetaDefender are subject to U.S. export controls and sanctions administered by the Commerce Department's Bureau of Industry and Security (BIS) under the U.S. Export Administration Regulations (EAR).

This page provides export control information on MetaDefender. MetaDefender provides encryption features that are subject to the EAR and other U.S. laws. These features have been approved for export from the United States, subject to certain requirements and limitations. You may find the information on this page useful for determining exportability to particular countries or parties, and for completing export or shipping documentation, recordkeeping, or post-shipment reporting.

Although we provide the information on this page, you remain responsible for exporting or re-exporting MetaDefender in accordance with U.S. law. We encourage you to seek appropriate legal advice and/or consult the EAR and the BIS Information Technology Controls Division before exporting, re-exporting, or distributing MetaDefender. The information provided here is subject to change without notice.

14. Knowledge Base Articles

- [Page:Are MetaDefender Core v4 upgrades free?](#)
- [Page:Are there any limitations regarding the MetaDefender Core v4 scan engines?](#)
- [Page:Are there any limitations regarding the MetaDefender Core v4 scan engines?](#)
- [Page:Can I control access to the RAM disk in MetaDefender Core v4?](#)
- [Page:Can I control access to the RAM disk in MetaDefender Core v4?](#)
- [Page:Does MetaDefender Core v4 Detect the NotPetya Ransomware?](#)
- [Page:Does MetaDefender Core v4 Detect the NotPetya Ransomware?](#)
- [Page:Does Metadefender Core v4 offer real-time antivirus protection on the system where it is installed?](#)
- [Page:Does the fixing updates for Meltdown and Spectre vulnerabilities affect any engines in MetaDefender Core v4?](#)
- [Page:Does the fixing updates for Meltdown and Spectre vulnerabilities affect any engines in MetaDefender Core v4?](#)
- [Page:Engine clean-up instructions](#)
- [Page:Engine clean-up instructions](#)
- [Page:External scanners in MetaDefender core v4.8.0 and above](#)
- [Page:External scanners in MetaDefender core v4.8.0 and above](#)
- [Page:How can I configure the maximum queue size in Metadefender Core v4 ?](#)
- [Page:How can I find a sanitized file scanned with MetaDefender Core v4?](#)
- [Page:How can I find a sanitized file scanned with MetaDefender Core v4?](#)
- [Page:How can I increase the scaling up performance?](#)
- [Page:How can I run tests to see the different scan results on MetaDefender Core v4?](#)
- [Page:How can I upgrade from Core v4.7.0/v4.7.1 to a newer Core v4.7 release](#)
- [Page:How can I upgrade from Core v4.7.0/v4.7.1 to a newer Core v4.7 release](#)
- [Page:How can the TEMP folder be changed?](#)
- [Page:How do I check if "noexec" flag exists on a Linux OS?](#)
- [Page:How do I check if "noexec" flag exists on a Linux OS?](#)
- [Page:How do I collect verbose debug packages on MetaDefender Core v4 for Linux?](#)
- [Page:How do I collect verbose debug packages on MetaDefender Core v4 for Linux?](#)

- [Page:How do I collect verbose debug packages on MetaDefender Core v4 for Linux?](#)
- [Page:How do I deploy MetaDefender Core v4 to an offline Linux environment?](#)
- [Page:How do I deploy MetaDefender Core v4 to an offline Linux environment?](#)
- [Page:How do I deploy MetaDefender Core v4 to an offline Windows environment?](#)
- [Page:How do I deploy MetaDefender Core v4 to an offline Windows environment?](#)
- [Page:How do I deploy MetaDefender Core v4 to an offline Windows environment?](#)
- [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:How do I remove an engine from my MetaDefender v4 instance?](#)
- [Page:How do I remove an engine from my MetaDefender v4 instance?](#)
- [Page:How do I use MetaDefender Core v4 Workflows ?](#)
- [Page:How do I use MetaDefender Core v4 Workflows ?](#)
- [Page:How long is the support life cycle for a specific version/release of MetaDefender Core v4?](#)
- [Page:How to install MSE on Windows Server 2012 R2 and Windows Server 2016](#)
- [Page:How to install MSE on Windows Server 2012 R2 and Windows Server 2016](#)
- [Page:How to transfer your Metadefender Core v4 scan history database](#)
- [Page:How to transfer your Metadefender Core v4 scan history database](#)
- [Page:Installing .NET Core runtime 3.1 on Linux for Proactive DLP 2.4.0+](#)
- [Page:Is Metadefender Core compromised while scanning files?](#)
- [Page:Is Metadefender Core compromised while scanning files?](#)
- [Page:Is there a virus test I could use to test MetaDefender Core v4?](#)
- [Page:MetaDefender Core v4 shows a large number of files that failed to scan. What can I do?](#)
- [Page:Microsoft Visual C++ 2017 Redistributable requirement for Deep CDR 5.8 or newer](#)
- [Page:Microsoft Visual C++ 2017 Redistributable requirement for Deep CDR 5.8 or newer](#)
- [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 2019-06-21

AN

Are there any limitations regarding the MetaDefender Core v4 scan engines?

Some of the custom engines have limitations in regard to OS compatibility and maximum file size allowed for scanning.

You can see these listed below:

Engine Name	File Size Limitation	OS Limitations
Antiy	900 MB	
Emsisoft	4 GB	
QuickHeal	2 GB	
Symantec		Only supported on Windows Server versions
Windows Defender		Limited to Windows Server 2016 and 2019

Note: This list is accurate for the latest packages of custom engines.

This article applies to MetaDefender Core v4

This article was last updated on 2020-06-20

VM

Can I control access to the RAM disk in MetaDefender Core v4?

Yes, you can set security permissions for the RAM disk just like a regular hard disk. To do so, right-click on that drive, select **Properties**, and then navigate to the Security tab to access security permissions for that drive.

.

This article applies to MetaDefender Core v4

This article was last updated on 2019-10-06

VM

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 2019-06-21

AG

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 32 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.
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 8:

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/>

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/>

VirITeXplorer: http://www.tgsoft.it/italy/news_archivio.asp?id=843

Total Defense: <https://www.totaldefense.com/security-blog/total-defense-products-detect-the-known-variations-of-the-goldeneye-petya-ransomware>

MetaDefender Core 12:

CYREN: <https://blog.cyren.com/articles/petya-ransomware-spreading-fast-using-same-wannacry-exploit>

MetaDefender Core 16:

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/>

Zillya!: <https://ru.tsn.ua/ukrayina/v-antivirusnoy-kompanii-rasskazali-kto-mozhet-stoyat-za-hakerskoy-atakoy-petya-a-i-chem-eto-grozit-885812.html>

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>

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>

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 2019-10-19

VM

Does the fixing updates for Meltdown and Spectre vulnerabilities affect any engines in MetaDefender Core v4?

Note. This article is no longer applicable to our current MetaDefender Core customers since F-Secure is no longer part of our supported AV engines.

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 was last updated on 2019-12-23

VM

Engine clean-up instructions



This tool only works on MetaDefender Core **4.18.0 and older**.

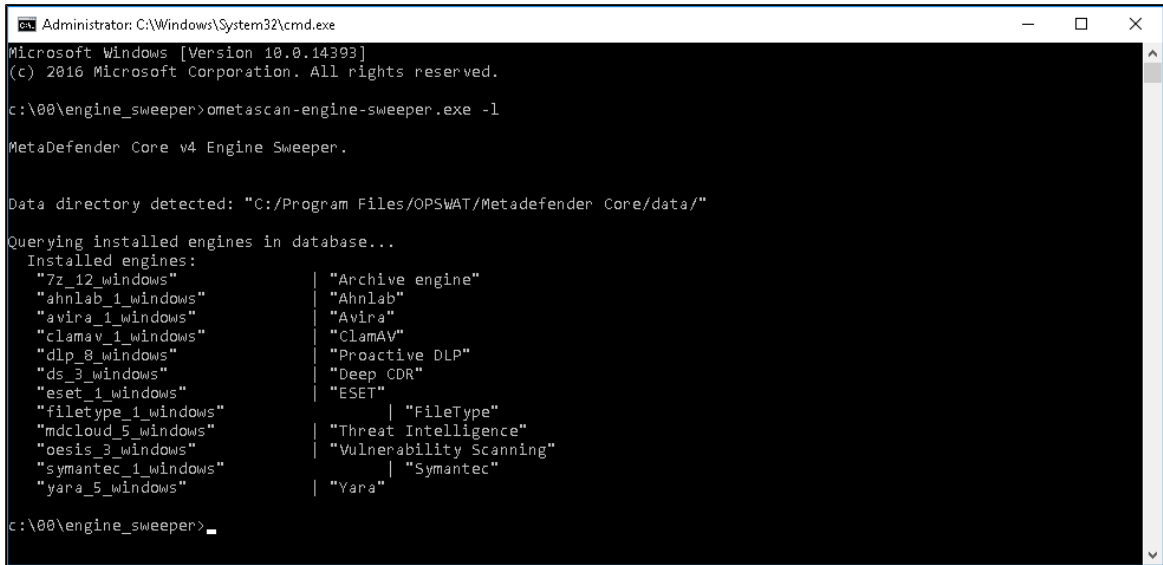
For Metadefender Core **4.19.0+**, please use the instructions at https://onlinehelp.opswat.com/corev4/Engine_Clean-up_Tool.html

Sometimes, during the engines downloading/deployment process, some of them may remain in **"failed"** or **"permanently failed"** status.

In this case, you can perform an engine clean-up by downloading the [engine_sweeper tool](#) and following the next steps:

1. Extract the engine_sweeper.zip package to a temporary location on the server where MetaDefender Core is installed
2. Open a Command Prompt window **as Administrator** and navigate to the temporary folder where you have extracted the archive

3. Run the command **ometascan-engine-sweeper.exe -l** to display a list of all installed engines



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\00\engine_sweeper>ometascan-engine-sweeper.exe -l

MetaDefender Core v4 Engine Sweeper.

Data directory detected: "C:/Program Files/OPSWAT/Metadefender Core/data/"

Querying installed engines in database...
Installed engines:
"7z_12_windows"           | "Archive engine"
"ahnlab_1_windows"       | "Ahnlab"
"avira_1_windows"        | "Avira"
"clamav_1_windows"       | "ClamAV"
"dlp_8_windows"          | "Proactive DLP"
"ds_3_windows"           | "Deep CDR"
"eset_1_windows"         | "ESET"
"filetype_1_windows"     | "FileType"
"mdcloud_5_windows"      | "Threat Intelligence"
"oesis_3_windows"        | "Vulnerability Scanning"
"symantec_1_windows"     | "Symantec"
"yara_5_windows"         | "Yara"

c:\00\engine_sweeper>
```

4. Run the command **ometascan-engine-sweeper.exe -e <engine name from above> -c** to clean the engine having the issues

Note: During the cleanup process, the MetaDefender Core and Node services will be **restarted**, and the Updates Settings Source will be set to **"Manual"**

```
Administrator: C:\Windows\System32\cmd.exe
c:\00\engine_sweeper>ometascan-engine-sweeper.exe -e "Deep CDR" -c
MetaDefender Core v4 Engine Sweeper.

Data directory detected: "C:/Program Files/OPSWAT/Metadefender Core/data/"
Engine to clean: "ds_3_windows"

The OPSWAT Metadefender Core service was stopped successfully.
The OPSWAT Metadefender Core Node service is stopping.
The OPSWAT Metadefender Core Node service was stopped successfully.

>> Cleaning processing...
QSqlDatabasePrivate::addDatabase: duplicate connection name 'enginesdb', old connection removed.
Cleaning updates/av folder..
  Succeed to remove folder: "ds_3_windows_D5Sn9G"
  Done

Cleaning engine records in enginesdb..
  Done

Cleaning updates/db folder..
  Succeed to remove folder: "ds_3_windows_21ci3k"
  Done

Cleaning database records in databasesdb..
  Done

Cleaning engine folder...
  Done

Disabling auto-update...
  Done

The OPSWAT Metadefender Core service is starting.
The OPSWAT Metadefender Core service was started successfully.

The OPSWAT Metadefender Core Node service is starting.
The OPSWAT Metadefender Core Node service was started successfully.

>> Cleaning finished
c:\00\engine_sweeper>_
```

5. Check the engine in Inventory > Modules as it should now be grey. (e.g. Deep CDR in the following screenshot)

Modules					
Auto update turned off Edit Update Settings					
MODULE	LAST UPDATE	ACTIVITY	ENGINE	DATABASE	ENABLED
Metascan	9 hours ago	5/5 processing engines are active			
Deep CDR	No available engine				
Proactive DLP	9 hours ago	Active on 1/1 node	2.2.1-1580392154	1582875907-8638	
Threat Intelligence	9 hours ago	Active on 1/1 node	4.0-42	1585094400	
File-Based Vulnerability Assessment	9 hours ago	Active on 1/1 node	4.2.416.0-108	1585144565	
Utilities	9 hours ago	3/3 engines are active			

6. Revert your Updates Settings Source from "Manual" to your previous setting and trigger an update, for the engine to re-deploy successfully
7. More parameters that can be used with this tool can be found in the next screenshot

```

Administrator: C:\Windows\System32\cmd.exe
c:\00\engine_sweeper>ometascan-engine-sweeper.exe -?
Usage: ometascan-engine-sweeper.exe [options]
MetaDefender Core v4 Engine Sweeper.

Options:
  -?, -h, --help           Displays this help.
  -e, --engine <engine>   Engine name to clean.
  -l, --list               List installed engines.
  -d, --retain-database    Retain engine's database.
  -c, --retain-config      Retain engine configurations.

c:\00\engine_sweeper>

```

If you have followed all of these steps and your engines are still unusable, please see [how to create a support package](#), login into [OPSWAT Portal](#) and open a ticket with us, having the support package attached.

This article applies to MetaDefender Core Windows v4.18.0 and older

This article was last updated on 2020-09-30

WM

External scanners in MetaDefender core v4.8.0 and above

Disclaimer

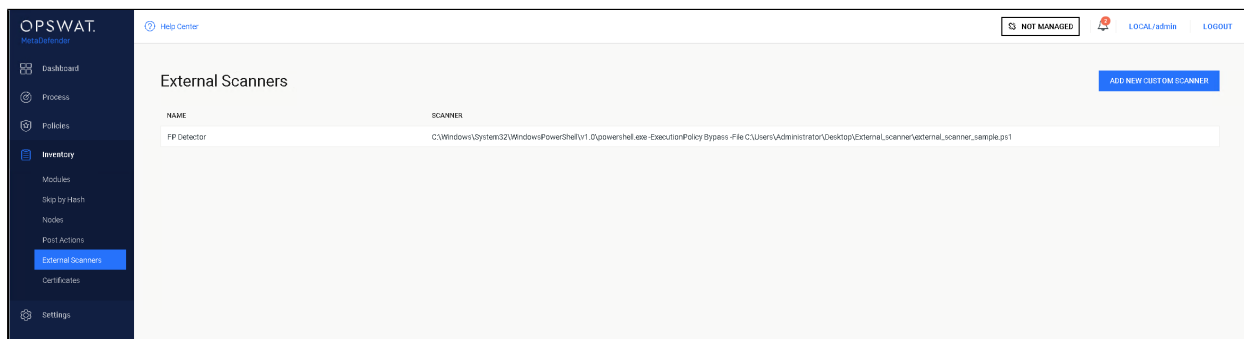
This sample script is provided for illustrative purposes only and is not guaranteed to be functional in a production environment.

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 the other engines but before the 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:



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 suspicious files 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 analyzed:

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 the 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 the 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 2019-10-06

VM

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:

```
{
  "max_queue_per_agent": 700
}
```

An example of a successful response can be found below :

HTTP status code: **200**

Response contains information about the modified scan configuration

```
{  
  "max_queue_per_agent": 700  
}
```

In case the configuration change was not correct, an error response like the one below will be returned :

Internal error

HTTP status code: **500**

```
{  
  "err": "Error while modifying configuration"  
}
```

This article applies to Metadefender Core v4 product

This article was last updated on 2019-06-28

MM

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 2019-06-21

MM

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 Core Management Console→Settings→User Management→Admin user use the apikey in the apikey header.

This works for both Linux and Windows.

Approach B

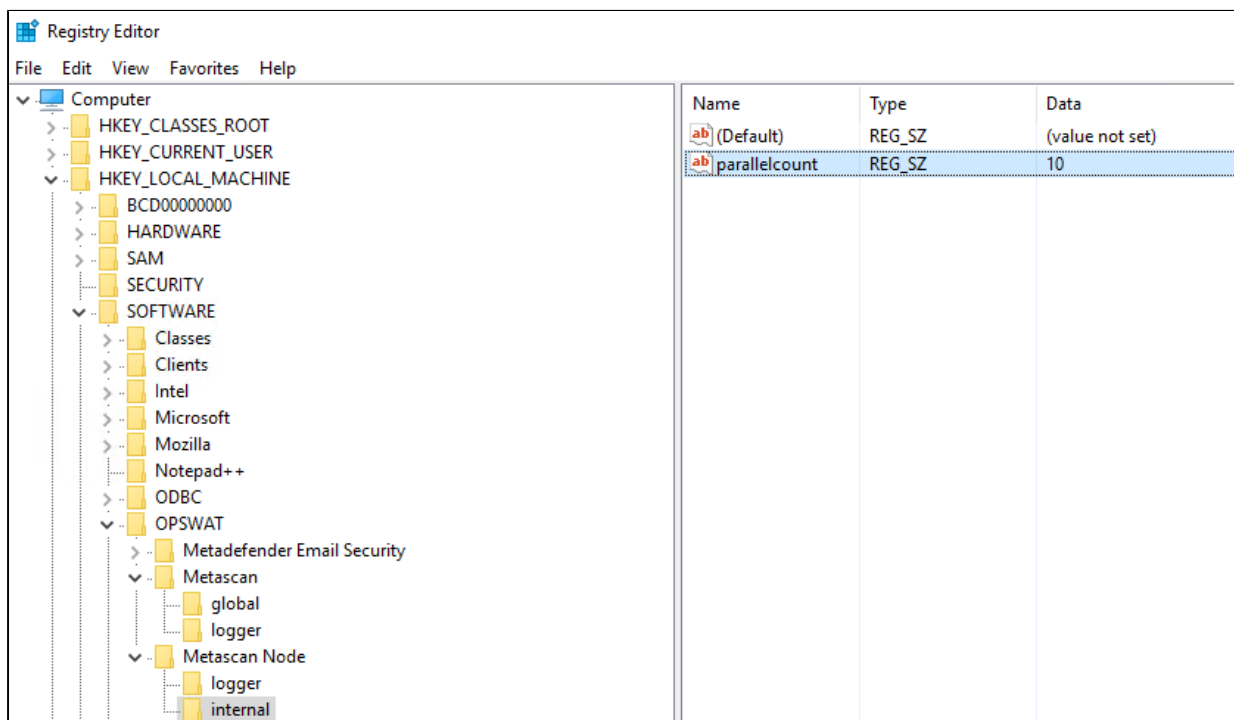
Another way to better utilize your CPU, if you have 16-32+ cores, is to increase the parallel number of scans running per engine. This way you can tell the Node how many scans should run simultaneously per engine. This applies to engines supporting multi-threaded scan.

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 the 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 file `/etc/ometascan-node/ometascan-node.conf` by adding "`[internal] parallelcount=the new config value`" 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 2019-10-06

VM

How can I run tests to see the different scan results on MetaDefender Core v4?

The following test cases explain how to obtain the possible scan results from MetaDefender Core v4.

- **No Threat Detected:** Test this result by scanning any file you are certain is clean (e.g., a newly created text file)
- **Infected/Known:**
 1. Download an EICAR test file from https://www.eicar.org/?page_id=3950
 2. Scan the file.
- **Suspicious:** This result is usually caused by an engine's heuristic algorithm. Since each engine has its own unique heuristic algorithms, we do not have sample files for each of the engines
- **Blacklisted:** Test this result by adding the file to be tested, to the blacklist. For instructions on how to add files to the blacklist, please refer to the [MetaDefender Core Documentation](#)
- **Whitelisted:** Test this result by adding a file by its name or its mime-type to the **Skip** option and scanning it. For more instructions on how to whitelist files, please refer to the [MetaDefender Core Documentation](#)
- **Exceeded Archive Size:**
 1. Configure "**Max total size of extracted files**" to a small value (i.e. 5 MB). This setting can be found on the MetaDefender Core Management Console under Policies→Workflow Rules→Select Workflow Rule→Archive Tab.
 2. Create an archive file with a total size greater than 5 MB (after extraction).
 3. Scan the file.
- **Exceeded Archive File Number:**
 1. Configure "**Max number of files extracted**" with a small value (i.e. 10). This setting can be found on the MetaDefender Core Management Console under Policies→Workflow Rules→Select Workflow Rule→Archive Tab.
 2. Create an archive file that contains more than 10 files (after extraction).
 3. Scan the file.

- **Password encrypted document/archive:** Scanning a password protected/encrypted document will produce this result. Currently, MetaDefender Core does not support decryption of encrypted files on the Management Console, only via REST API
- **Exceeded Archive Depth:** Test this result by configuring a lower recursion level than the current archive depth settings (Policies→Workflow Rules→Select Workflow Rule→Archive Tab)
- **Failed to scan:** Test this result by sending a file to scan which has no read permissions or is invalid. Alternatively, if no engine is in the MetaDefender Core installation and scan is enabled through the Security Rule configurations, this will be the final result
- **Mismatch:**
 1. Test this result by enabling the "**Detect File Type Mismatch**" option from the "**Policies**", tab "Scan" under the section inside of the "**Workflow Rule**" you are using.
 2. Alternatively, this result can be tested by changing the original extension of a file to different extension (i.e. test.docx → test.pdf) and scanning the file.
 3. Note that the option "**Detect File Type Mismatch**" only applies to workflows.
- **Potentially Vulnerable File:** Clean files can be marked as vulnerable if the Vulnerability Engine identifies known application vulnerabilities which are then reported by severity level. For more information on the Vulnerability Engine, please refer [here](#)

This article pertains to MetaDefender Core v4

This article was last updated on 2019-10-06

VM

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 contain an issue that can cause configuration data loss during an 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 are any *.war or *.shm files that exist 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 2019-10-06

VM

How can the TEMP folder be changed?

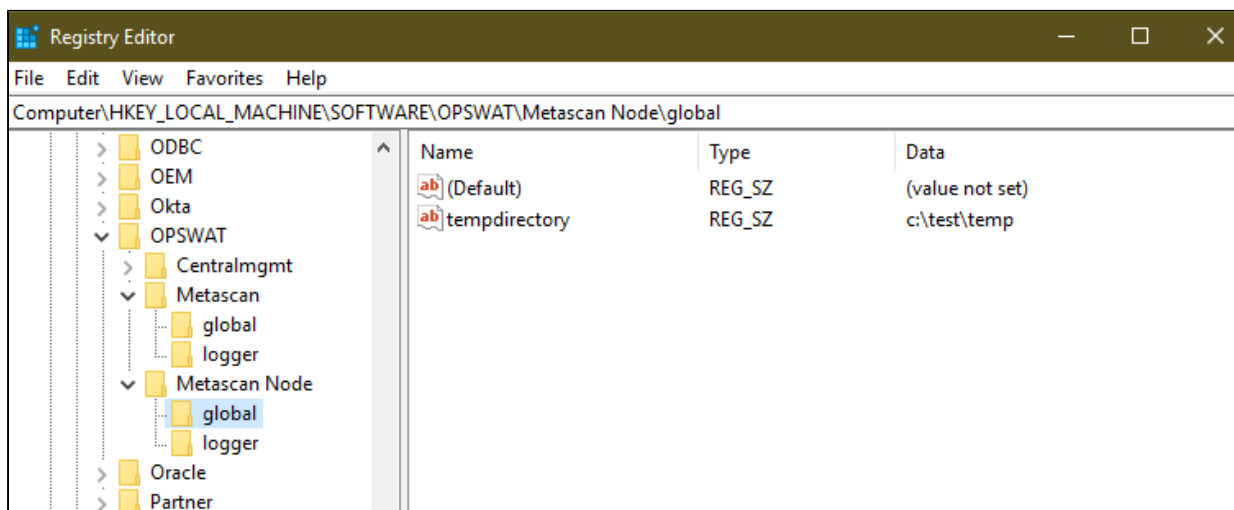
The "**temp** folder", or the "**resources** folder" is the location where the scanned files are getting written down for the Nodes to scan.

The temporary folder is used to store the following files:

- *EICAR Standard Anti-Virus Test File* for engine testing (see https://www.eicar.org/?page_id=3950)
- all the uploaded files to scan/process
- all the extracted files during archive handling while scanning/processing a file
- the file generated with sanitization before being 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:

- For MetaDefender Core 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,
- For MetaCefender Core versions lower than 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 2019-08-09

VM

How do I check if "noexec" flag exists on a Linux OS?

On Linux, MetaDefender Core deploys its engines and files in the /var/lib and /usr/lib folders. Depending on your file mount security policy, you may have mounted /var or /usr with the flag "noexec". The "noexec" flag essentially will not allow any direct execution of binaries from the mounted filesystem/folder. In essence, if this flag exists, MetaDefender Core will not be able to launch its engine processes. This will result in an engine with a "permanently_failed" module.

To check if "noexec" flag exists on /var or /usr simply do the following

- Run Terminal and use one of the following commands:
- **findmnt -l | grep noexec**

```

administrator@administrator-HVM-domi:~$ findmnt -l | grep noexec
/sys          sysfs      sysfs      rw,nosuid,nodev,noexec,relatime
/proc        proc       proc       rw,nosuid,nodev,noexec,relatime
/dev/pts     devpts    devpts    rw,nosuid,noexec,relatime,size=620,ptmxmode=000
/run         tmpfs     tmpfs     rw,nosuid,noexec,relatime,size=814076k,node=755
/sys/kernel/security securityfs securityfs rw,nosuid,nodev,noexec,relatime
/run/lock    tmpfs     tmpfs     rw,nosuid,nodev,noexec,relatime,size=5120k
/sys/fs/cgroup cgroup    cgroup2   rw,nosuid,nodev,noexec,relatime,nodelegat
/sys/fs/cgroup/systemd cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,xattr,na
/sys/fs/pstore pstore    pstore    rw,nosuid,nodev,noexec,relatime
/sys/fs/cgroup/devices cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,devices
/sys/fs/cgroup/hugetlb cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,hugetlb
/sys/fs/cgroup/perf_event cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,perf_event
/sys/fs/cgroup/bkno cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,bkno
/sys/fs/cgroup/rdma cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,rdma
/sys/fs/cgroup/cpuset cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,cpuset
/sys/fs/cgroup/memory cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,memory
/sys/fs/cgroup/net_cls_net_prio cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,net_cls,net_prio
/sys/fs/cgroup/cpu_cputacct cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,cpu,cputacct
/sys/fs/cgroup/freezer cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,freezer
/sys/fs/cgroup/pids cgroup    cgroup    rw,nosuid,nodev,noexec,relatime,pids

```

OR

- **mount | grep noexec**

```
administrator@administrator-HVM-domU: ~
File Edit View Search Terminal Help
administrator@administrator-HVM-domU:~$ mount | grep noexec
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,node=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=814076k,node=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,node=755)
cgroup on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,none=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetbl)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/bkilo type cgroup (rw,nosuid,nodev,noexec,relatime,bkilo)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
```

- Using the commands above will reveal if there is a mount point with the “noexec” flag
- If /var or /usr exist on the list, then you must remove the “noexec” flag with the following command:
 - **mount -o remount,rw,exec /var**
 - **mount -o remount,rw,exec /usr**

This article applies to MetaDefender Core v4 Linux

This article was last updated on 2020-20-02

AA

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):

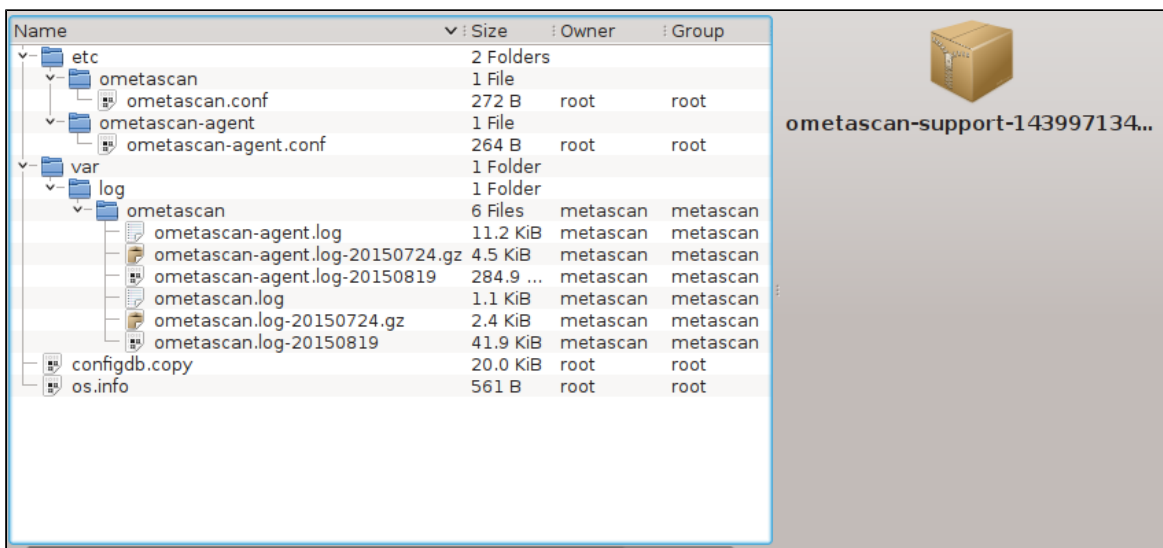
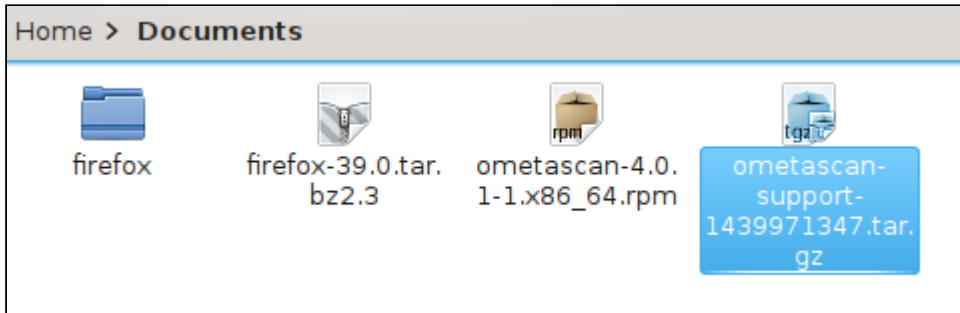
```
[root@localhost Documents]# sudo sh /usr/bin/ometascan-collect-support-data.sh
/usr/bin/ometascan-collect-support-data.sh: line 5: lsb_release: command not found
/usr/bin/ometascan-collect-support-data.sh: line 7: lsb_release: command not found
tar: Removing leading `/' from member names
Support 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").



- During the script run the output "/usr/bin/ometascan-collect-support-data.sh: line 16: lsb_release: command not found" is expected. The package is still being generated.

- The timestamp in the filename changes every run.



This article applies to MetaDefender Core v4 Linux

This article was last updated on 2019-06-21

AG

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:

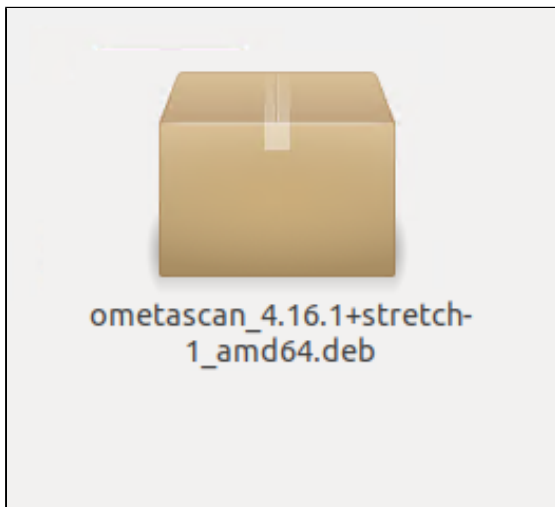
1. Install MetaDefender Core on the offline server.
2. Activate your license.
3. Install and configure the MetaDefender Update Downloader utility.

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/>. Complete the required steps of the [basic configuration wizard](#).
2. Go to **Settings > License**.
3. Log in to the OPSWAT Portal and navigate to the MetaDefender Offline Activation page.
4. Fill in the requested information about your license and Deployment ID

Metadefender Offline Activation

Metadefender Package

Metadefender Core v4.x - all packages

Activation Key *

87g 7u88 w4b4 872b 488 0275 4277 888g

Requested Number of Nodes *

1

Deployment ID *

MSCWVN8iW4edviVJ1kDEZXLsYc36ZYGdRBh8

Optional Description

This helps you to identify this deployment
on OPSWAT License portal

Request Unlock Key

5. Apply that key to your MetaDefender Core server via the Management Console.

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

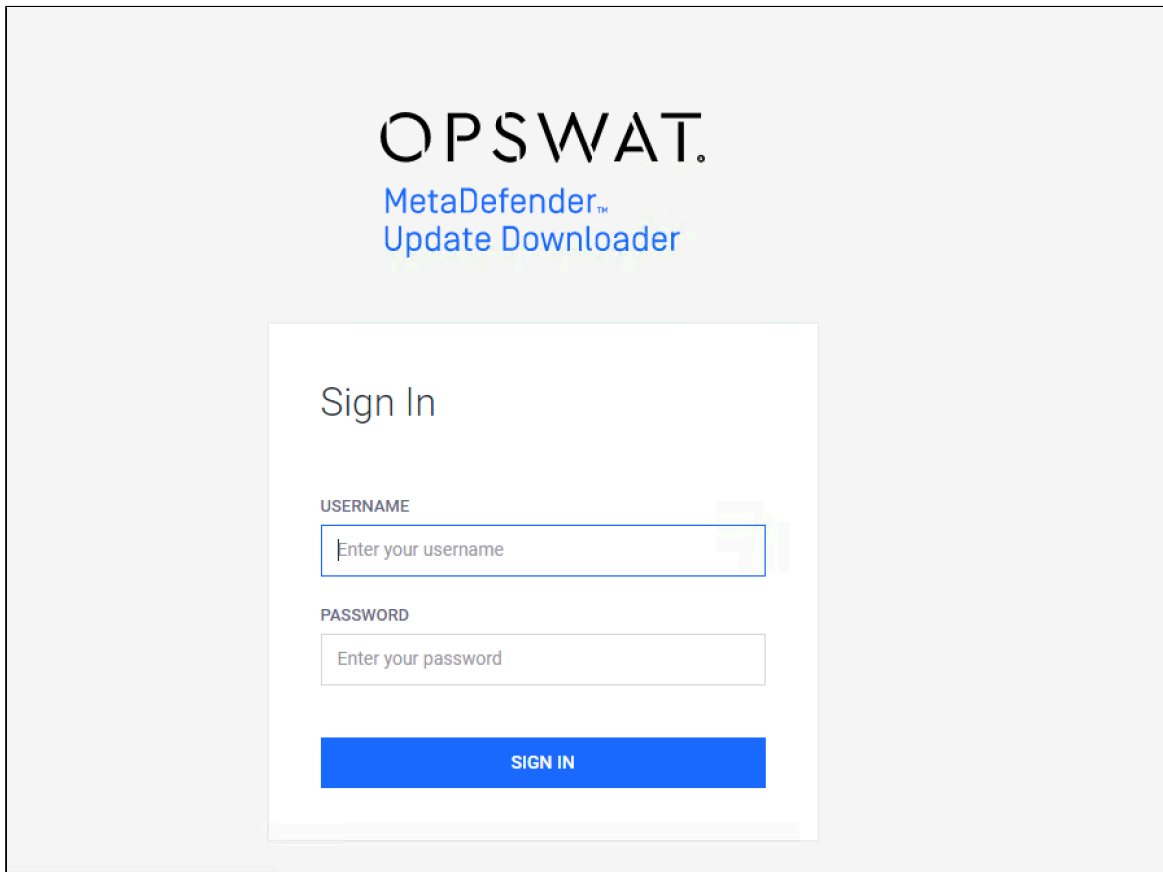
MSCWVN8iW4edviVJ1kDEZXLsYc36ZYGdRBh8.yml

Installing the MetaDefender Update Downloader utility

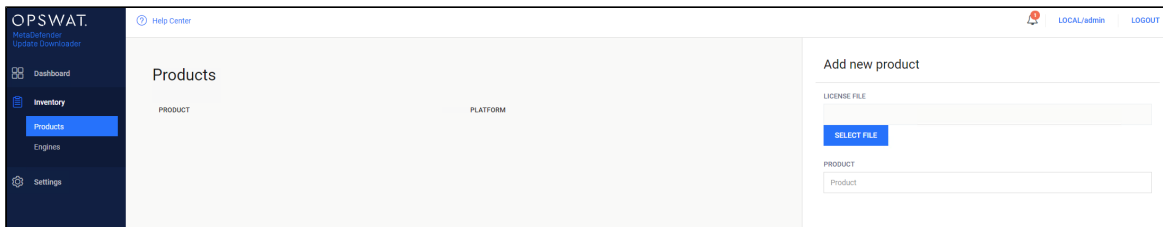
If your MetaDefender Core server is deployed offline, you will need to use the Update Downloader utility to download the anti-malware definition updates to be applied to the server. You can download the Update Downloader utility from the [OPSWAT Portal](#).

Once you have installed the Update Downloader, apply your license key to activate the product:

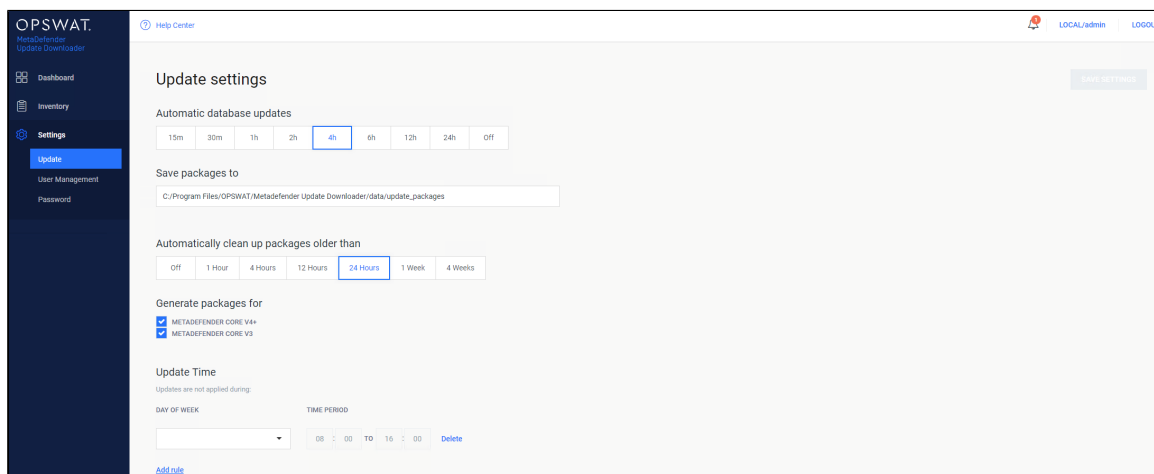
1. Log into the Update Downloader Management Console at <http://<server>:8028/>.



2. Add your product on the Inventory page, Product tab. (For versions older than 2.4.0 MetaDefender Update Downloader must first be activated. Go to Settings → License and add your license)



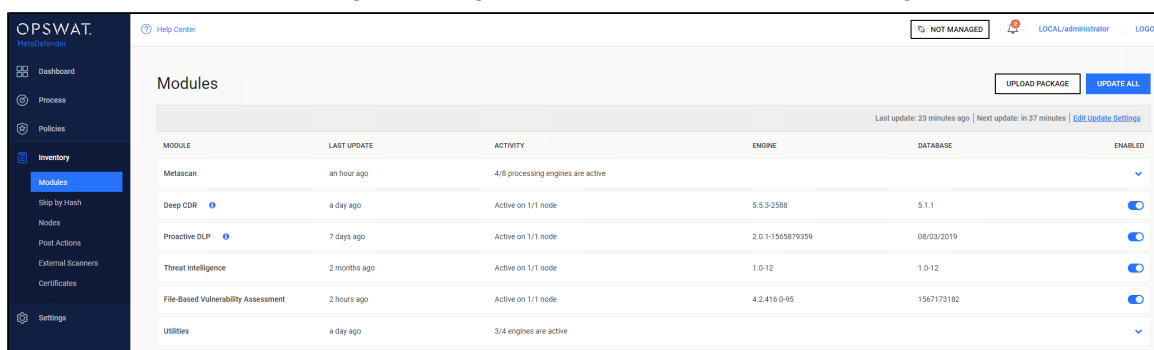
3. Update the configuration for update download and package generation on the Settings page of the Management Console.



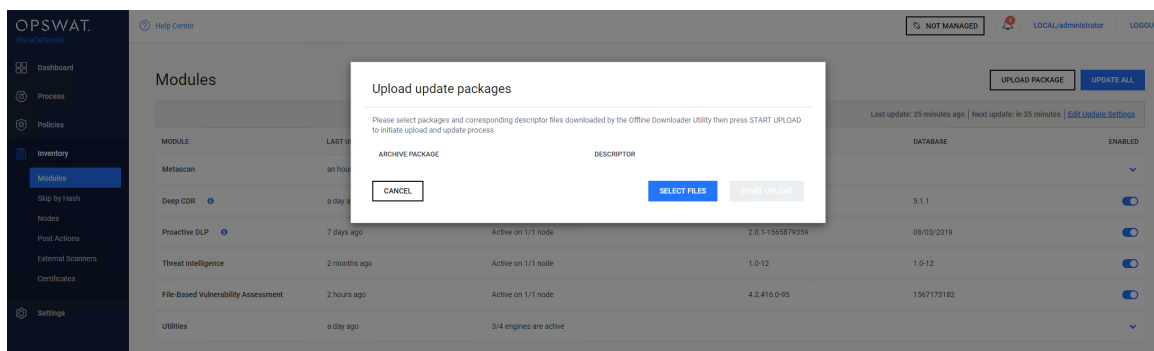
Applying offline updates

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 updated 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 2019-07-05

AG

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/>. Complete the required steps of the [basic configuration wizard](#).
2. Go to **Settings > License**.
3. Log in to the OPSWAT Portal and navigate to the MetaDefender Offline Activation page.
4. Fill in the requested information about your license and Deployment ID

Metadefender Offline Activation

Metadefender Package

Metadefender Core v4.x - all packages

Activation Key *

87g 7u88 v4x 8728 488 4887 4887 888

Requested Number of Nodes *

1

Deployment ID *

MSCWVN8iW4edviVJ1kDEZXLsYc36ZYGdRBh8

Optional Description

This helps you to identify this deployment
on OPSWAT License portal

Request Unlock Key

5. Apply that key to your MetaDefender Core server through the Management Console.

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

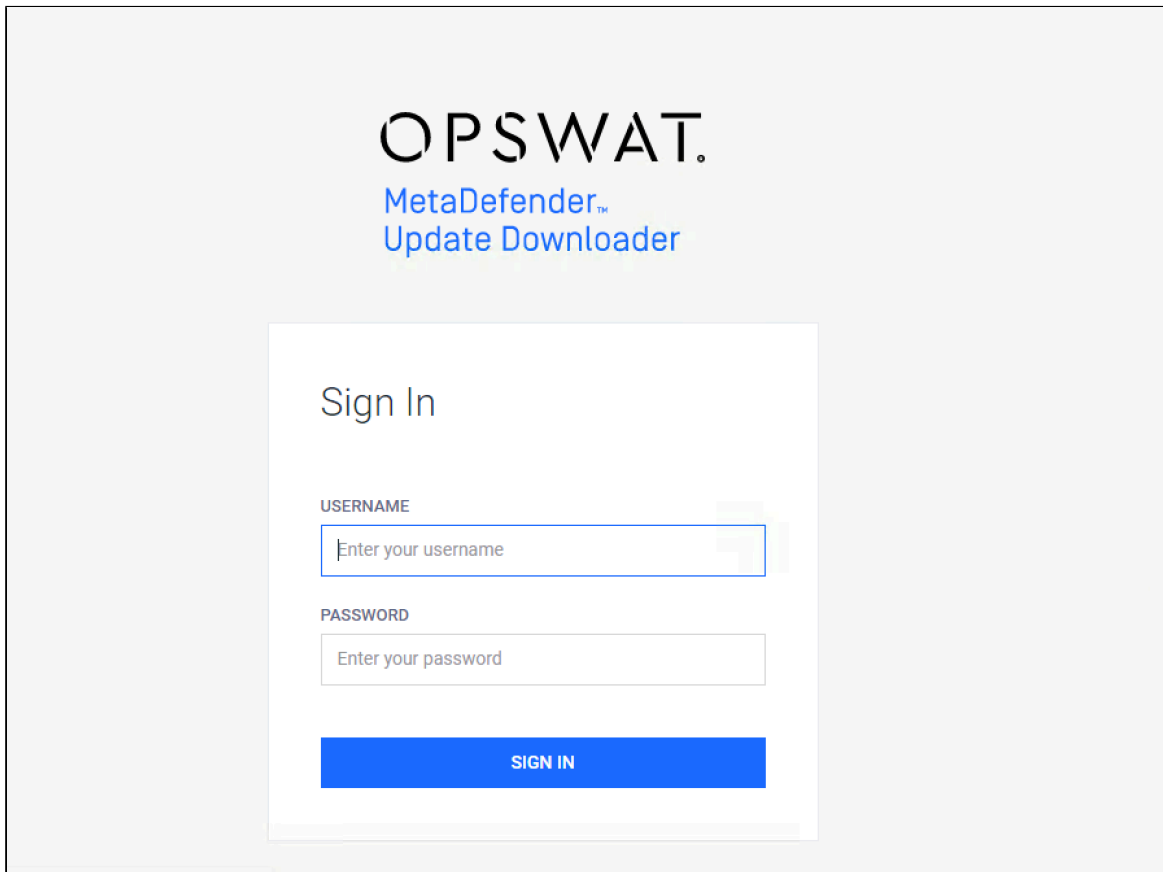
MSCWVN8iW4edviVJ1kDEZXLsYc36ZYGdRBh8.yml

Installing the MetaDefender Update Downloader utility

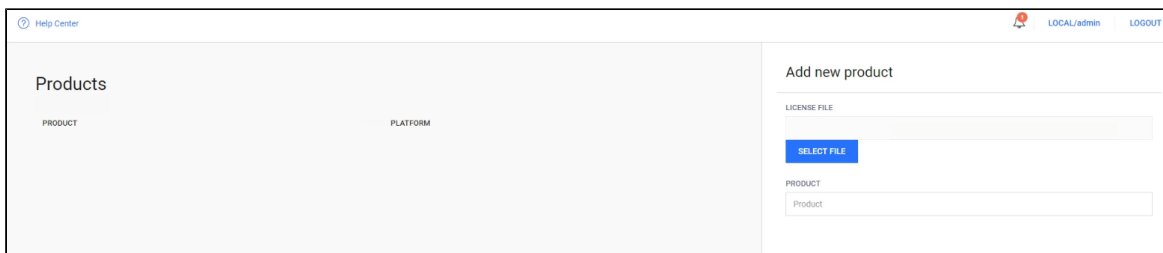
If your MetaDefender Core server is deployed offline, you will need to use the Update Downloader utility to download the anti-malware definition updates to be applied to the server. You can download the Update Downloader utility from the [OPSWAT Portal](#).

Once you have installed Update Downloader, apply your license key to activate the product.

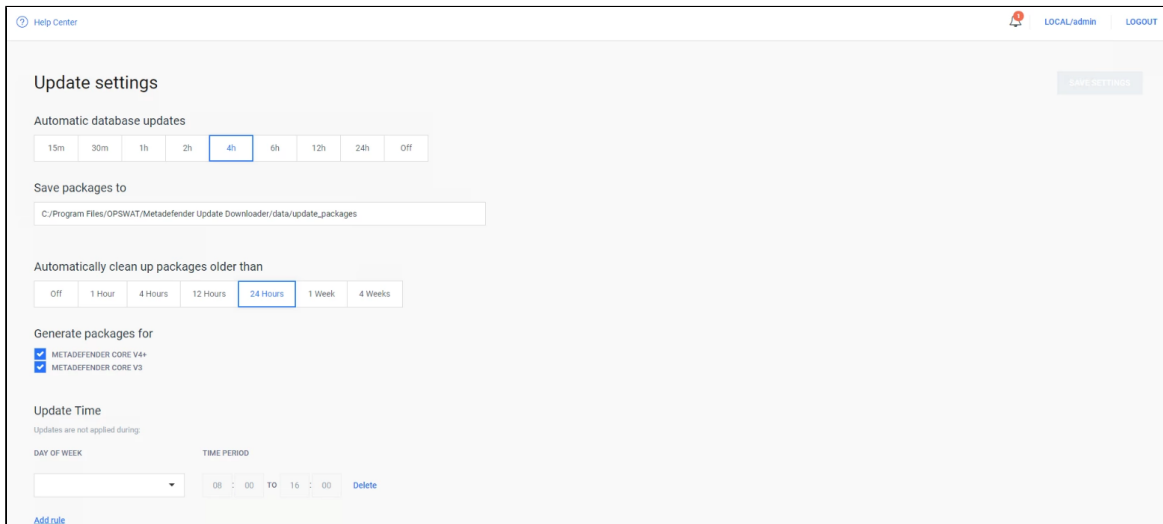
1. Log into the Update Downloader Management Console at <http://<server>:8028/>.



2. Add your product on the Inventory page, Product tab. (For versions older than 2.4.0 MetaDefender Update Downloader must first be activated. Go to Settings → License and add your license)



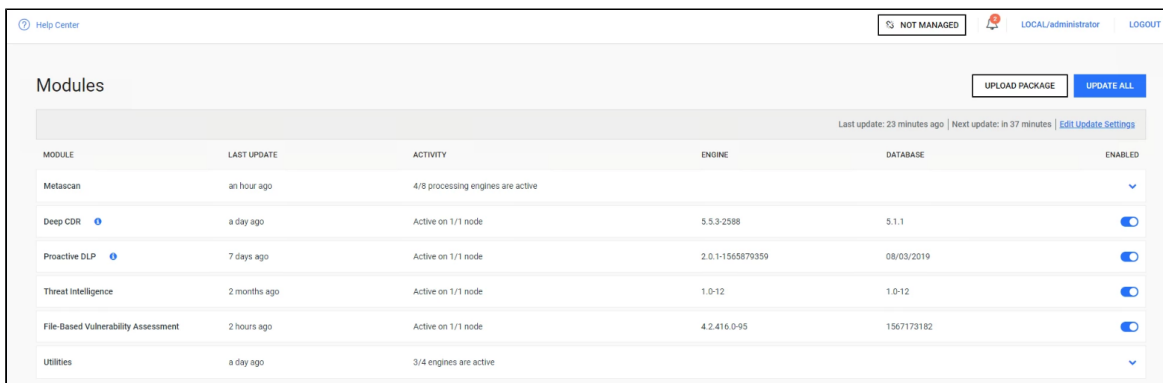
3. Update the configuration for update download and package generation on the Settings page of the Management Console.



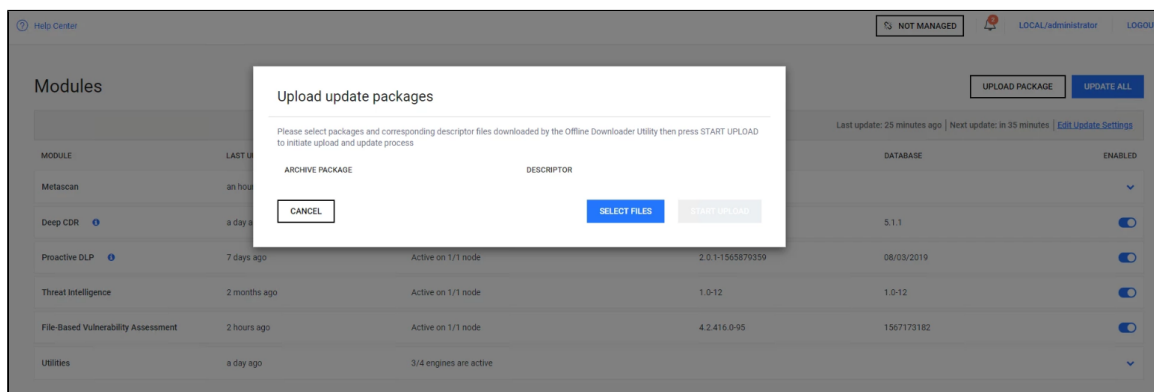
Applying offline updates

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 2019-08-30

AG

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 following from the real-time protection:

- the OPSWAT installation folder which by default also includes the folder where MetaDefender Core is creating its temporary files
- the **ometascan**, **ometascan-node**, **engineprocess**, **engineprocess32** and **nginx** processes (note that some engines will need to run on different process instances (e.g.: ClamAv) that are managed by the **engineprocess** parent process)

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 and 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 are using **Symantec Endpoint Protection** as your local AV, please adjust the settings as instructed in [this KB article](#).

If you need help on how to add an exception rule to exclude a given folder from scanning for an 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 2020-07-16

VM

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://go.opswat.com/s/cases>
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 2019-07-05

AN

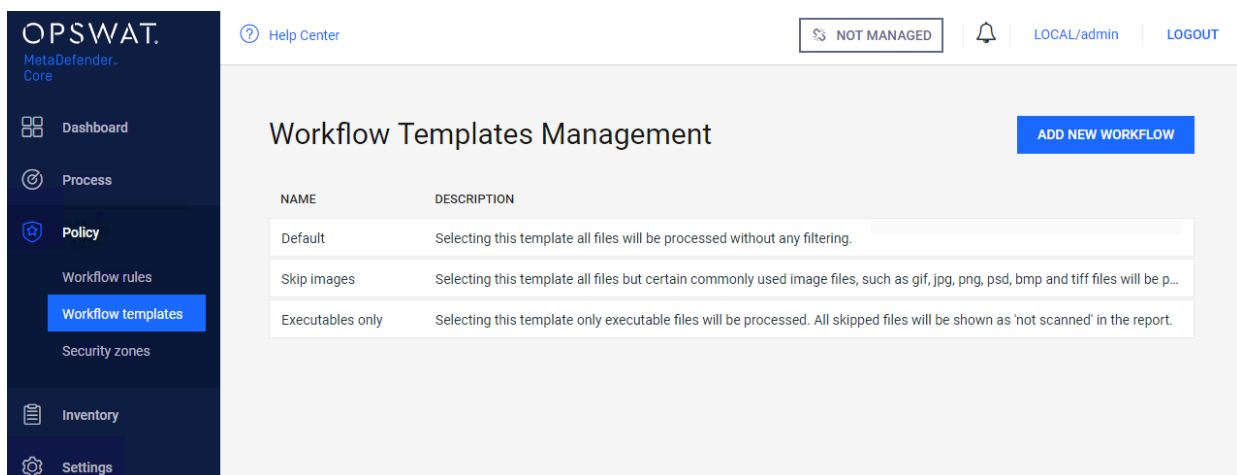
How do I use MetaDefender Core v4 Workflows ?

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 have 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

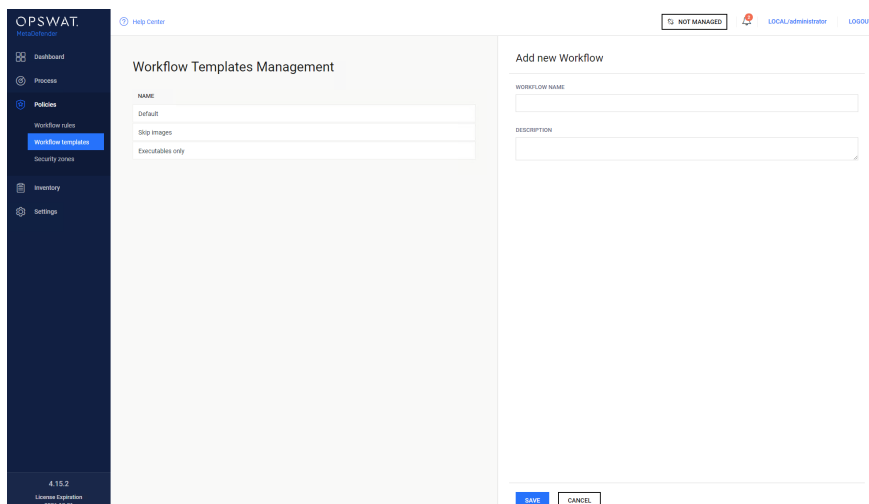
As an administrator, you define Workflows and apply them to the security policies that will determine how files get processed. MetaDefender Core v4 provides three predefined Workflows out-of-the-box: "Default", "Skip Images", and "Executables only".



The screenshot shows the 'Workflow Templates Management' page in the MetaDefender Core v4 interface. The page features a dark blue sidebar on the left with navigation options: Dashboard, Process, Policy (highlighted), Workflow rules, Workflow templates (highlighted in blue), Security zones, Inventory, and Settings. The main content area has a title 'Workflow Templates Management' and an 'ADD NEW WORKFLOW' button. Below the title is a table with two columns: 'NAME' and 'DESCRIPTION'. The table lists three predefined workflows: 'Default', 'Skip images', and 'Executables only'. At the top right of the main area, there is a 'NOT MANAGED' status indicator, a notification bell, and user information 'LOCAL/admin' with a 'LOGOUT' link.

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.

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.



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 2019-07-04

AG

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 release supported life-cycle.

Release number	Release date	End-of-life date
4.19.0	27 Aug 2020	
4.18.0	26 May 2020	27 Feb 2022

4.17.3	06 Apr 2020	26 Nov 2021
4.17.2	02 Mar 2020	06 Oct 2021
4.17.1	06 Jan 2020	02 Sep 2021
4.17.0.1	27 Nov 2019	06 Jul 2021
4.16.3	16 Oct 2019	27 May 2021
4.16.2	10 Sep 2019	16 Apr 2021
4.16.1	12 Aug 2019	10 Mar 2021
4.16.0	08 Jul 2019	12 Feb 2021
4.15.2	19 Jun 2019	08 Jan 2021
4.15.1	06 Jun 2019	19 Dec 2020
4.15.0	06 May 2019	06 Dec 2020
4.14.3	01 Apr 2019	06 Nov 2020
4.14.2	28 Feb 2019	01 Oct 2020
4.14.1	01 Feb 2019	28 Aug 2020
4.14.0	24 Dec 2018	01 Aug 2020
4.13.2	07 Dec 2018	24 Jun 2020
4.13.1	01 Nov 2018	07 Jun 2020
4.12.2	04 Oct 2018	01 May 2020
4.12.1	27 Sep 2018	04 Apr 2020
4.12.0	17 Sep 2018	27 Mar 2020

4.11.3	30 Aug 2018	17 Mar 2020
4.11.2	29 Aug 2018	02 Mar 2020
4.11.1	08 Aug 2018	01 Mar 2020
4.10.1	23 May 2018	08 Feb 2020
4.10.0	02 May 2018	23 Nov 2019
4.9.1	08 Mar 2018	02 Nov 2019
4.9.0	11 Dec 2017	09 Sep 2019
4.8.2	11 Oct 2017	08 Jun 2019
4.8.1	05 Oct 2017	11 Jun 2019
4.8.0	07 Jul 2017	29 Mar 2019
4.7.2	31 May 2017	06 Jan 2019
4.7.1	16 May 2017	30 Nov 2018
4.6.3	04 Apr 2017	15 Nov 2018
4.6.2	15 Mar 2017	03 Oct 2018
4.6.1	03 Feb 2017	14 Sep 2018
4.6.0	07 Jan 2017	03 Aug 2018
4.5.1	12 Oct 2016	07 Jul 2018
4.5.0	30 Sep 2016	11 Apr 2018
4.4.1	10 Aug 2016	29 Mar 2018
4.3.0	12 May 2016	09 Feb 2018

4.2.0	19 Feb 2016	11 Nov 2017
4.1.0	30 Sep 2015	18 Aug 2017
4.0.1	10 Aug 2015	29 Mar 2017
4.0.0	16 Jul 2015	09 Feb 2017

This article pertains to all supported releases of MetaDefender Core v4

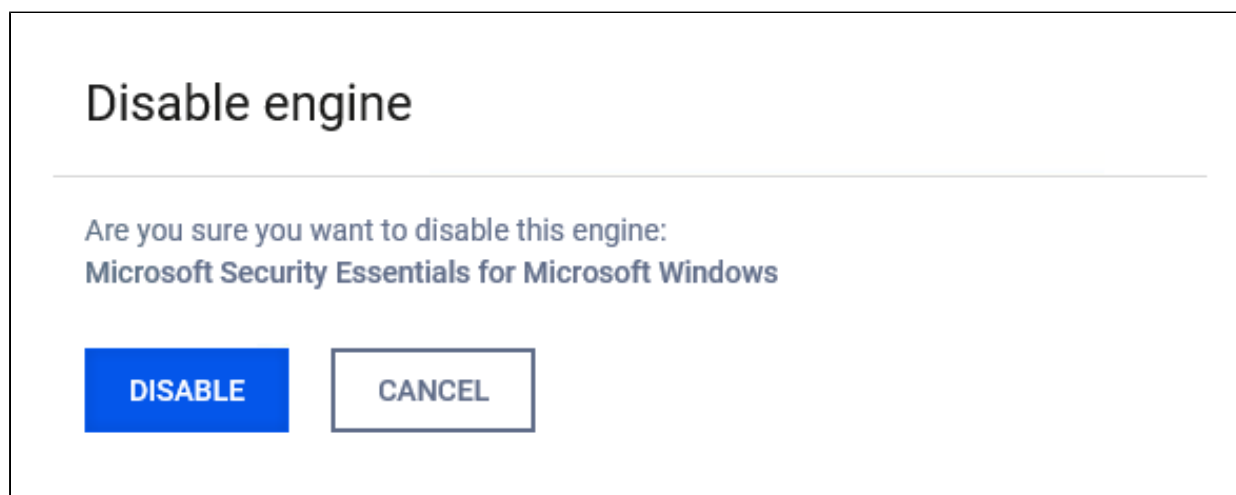
This article was last updated on 2020-09-09

VM

How to install MSE on Windows Server 2012 R2 and Windows Server 2016

MSE on Windows Server 2012 R2

- Install MetaDefender Core with MSE engine as licensed option
- MSE will fail to deploy
- Open MetaDefender Core Management Console
- Navigate to Inventory - Technologies and expand the Anti-malware engines list
- Disable MSE from the list (please note that version numbers might be different)



- The engine should show as inactive

Microsoft Security Essentials

[Settings](#)

STATUS	INACTIVE
VERSION	4.3.0216.0-33 (disabled)
DATABASE VERSION	1544616743
DEFINITION UPDATES	
NODES	☐

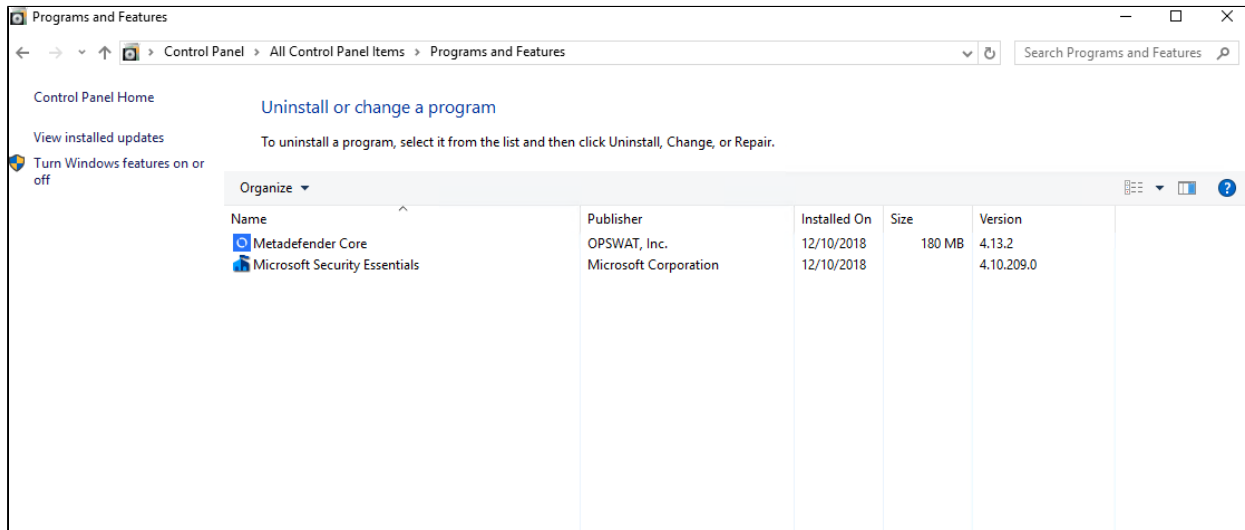
ENABLE

CLOSE

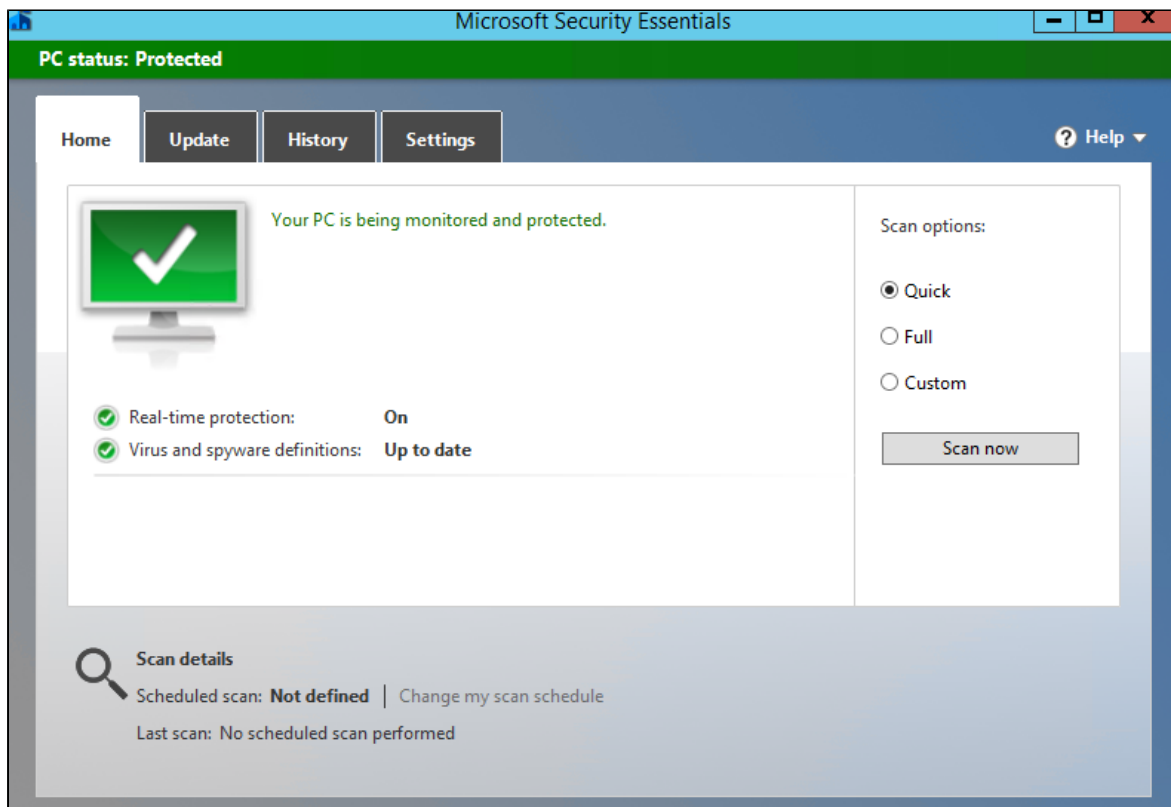
- Download the following archive which contains an install script - [install_on_windows_server.zip](#)
- Go to the following link : <https://www.microsoft.com/en-us/download/details.aspx?id=5201> and download the MSE installer

<input type="checkbox"/> ENUS\amd64\MSEInstall.exe	14.4 MB
--	---------

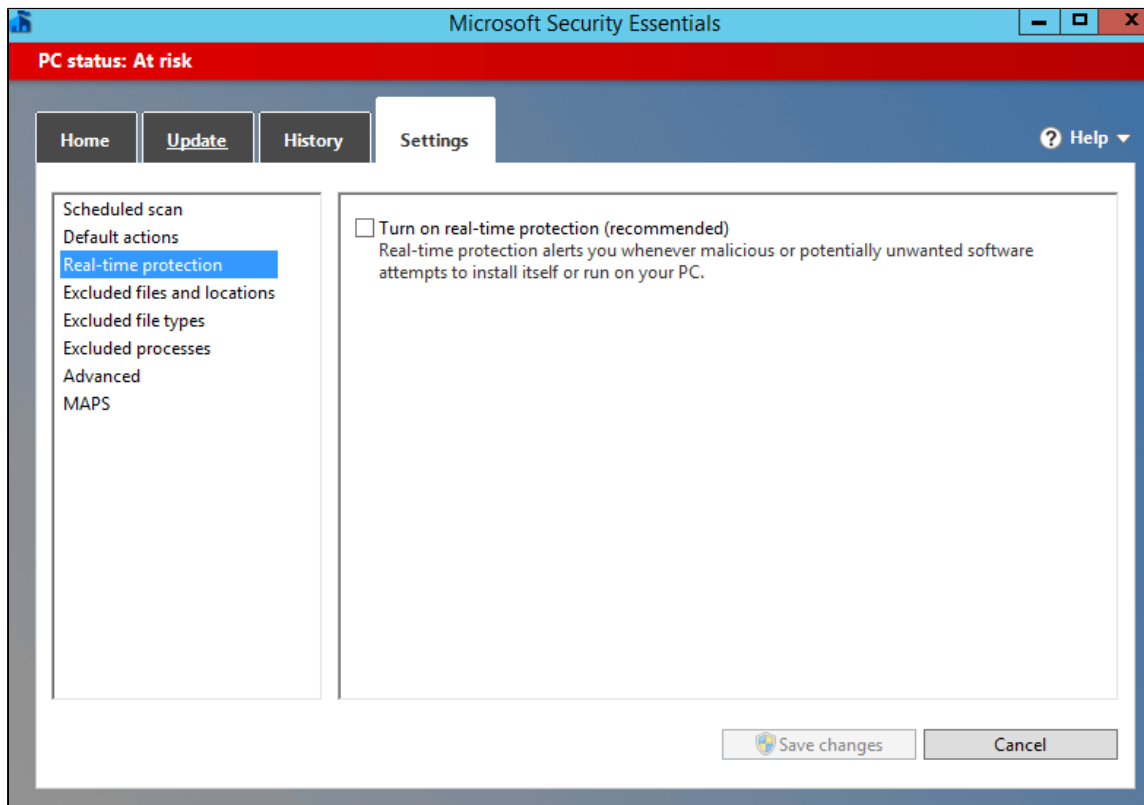
- Rename the installer that was downloaded to "MSEInstallx64"
- Place the install script and the downloaded installer in the same folder
- Run install_on_windows_server with admin rights from the above folder
- Wait a few mins for the script to run and for the CMD window to go away
- **Please note that Windows Firewall might be enabled if it was previously disabled**
- Check the "Programs and Features" section in "Control Panel" to see if MSE is showing up



- Search for Microsoft Security Essentials in the Start Menu and open it




- Go to Settings - Real-time protection and disable it



- It is OK for it to be red, we just disabled Real-Time Protection
- Enable MSE in MetaDefender Core UI
- The engine might show up as not deploying in the beginning
- Wait 5-10 mins, the engine should deploy

Microsoft Security Essentials [Settings](#)

STATUS	ACTIVE
VERSION	4.3.0216.0-33
DATABASE VERSION	1544616743
DEFINITION UPDATES	✓ Up to date (up to date)
NODES	

DISABLE **CLOSE**

MSE on Windows Server 2016

- Install MetaDefender Core with MSE as a licensed engine
- MSE will fail to deploy because of conflict with Windows Defender included in Windows Server 2016
- Open MetaDefender Core Management Console
- Navigate to Inventory - Technologies and expand the Anti-malware engines list
- Disable MSE from the list (please note that version numbers might be different)


Disable engine

Are you sure you want to disable this engine:
Microsoft Security Essentials for Microsoft Windows

DISABLE **CANCEL**

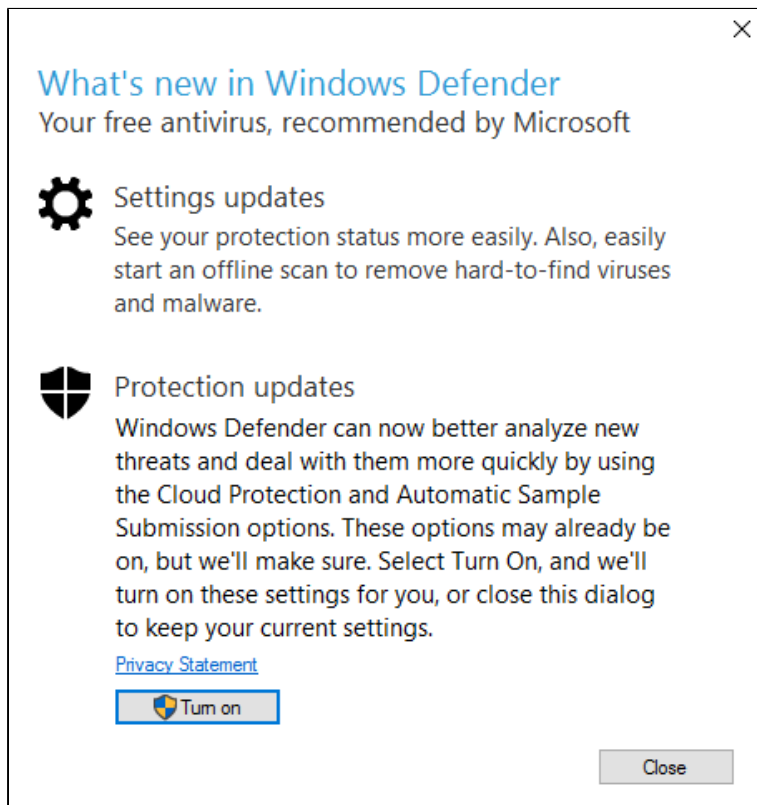
- The engine should show as inactive

Microsoft Security Essentials [Settings](#)

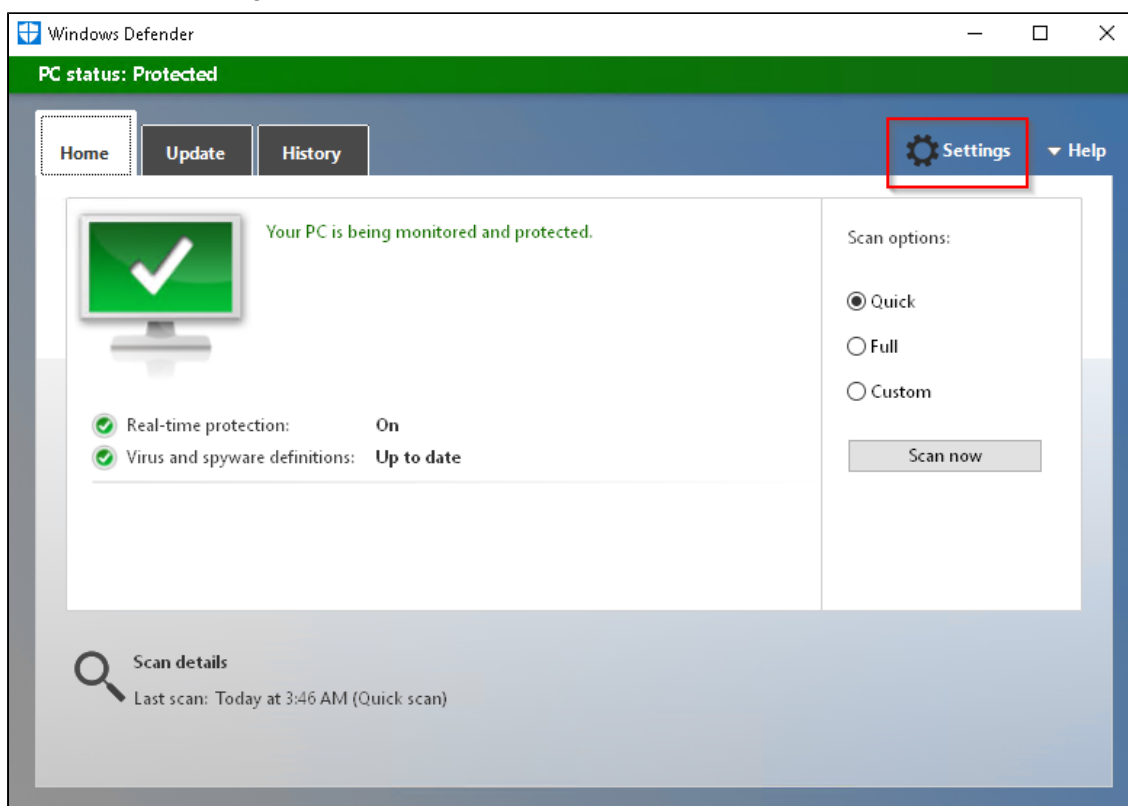
STATUS	INACTIVE
VERSION	4.3.0216.0-33 (disabled)
DATABASE VERSION	1544616743
DEFINITION UPDATES	
NODES	

ENABLE **CLOSE**

- Open Windows Defender
- If the following pop up shows up, please click the Close button



- Go to Settings and disable all options related to Windows Defender



Windows Defender protects your computer against viruses, spyware, and other malicious software. Open Windows Defender to use it.

[Open Windows Defender](#)

Real-time protection

This helps find and stop malware from installing or running on your PC.

Off

Cloud-based Protection

Get Real-time protection when Windows Defender sends info to Microsoft about potential security threats. This feature works best with Automatic sample submission enabled.

Off

[Privacy Statement](#)

Automatic sample submission

Allow Windows Defender to send samples of suspicious files to Microsoft, to help improve malware detection. Turn this off to be prompted before sending samples to Microsoft.

Off

[Privacy Statement](#)

Exclusions

Windows Defender won't scan excluded files, making your PC more vulnerable to malware.

[Add an exclusion](#)

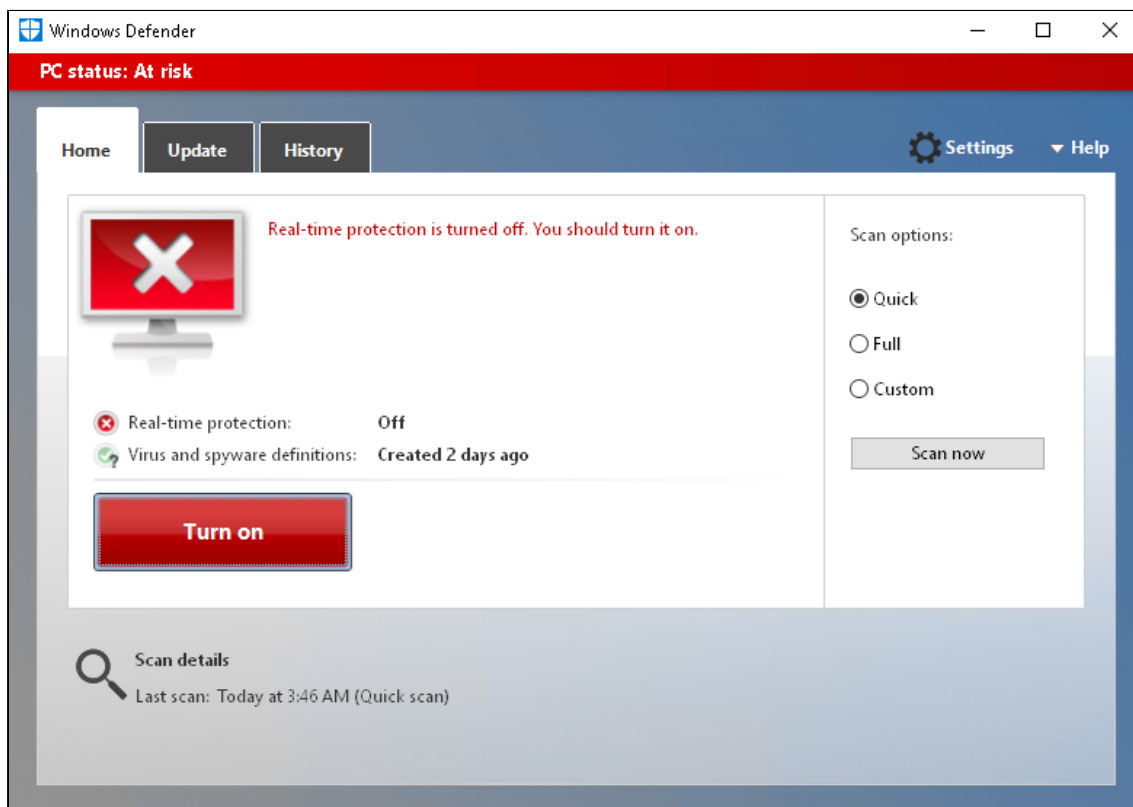
Enhanced notifications

Windows Defender sends notifications to help ensure you are informed about the health of your PC. Even if this option is turned off, you'll still get critical notifications for issues that need immediate attention.

Off

[Privacy Statement](#)

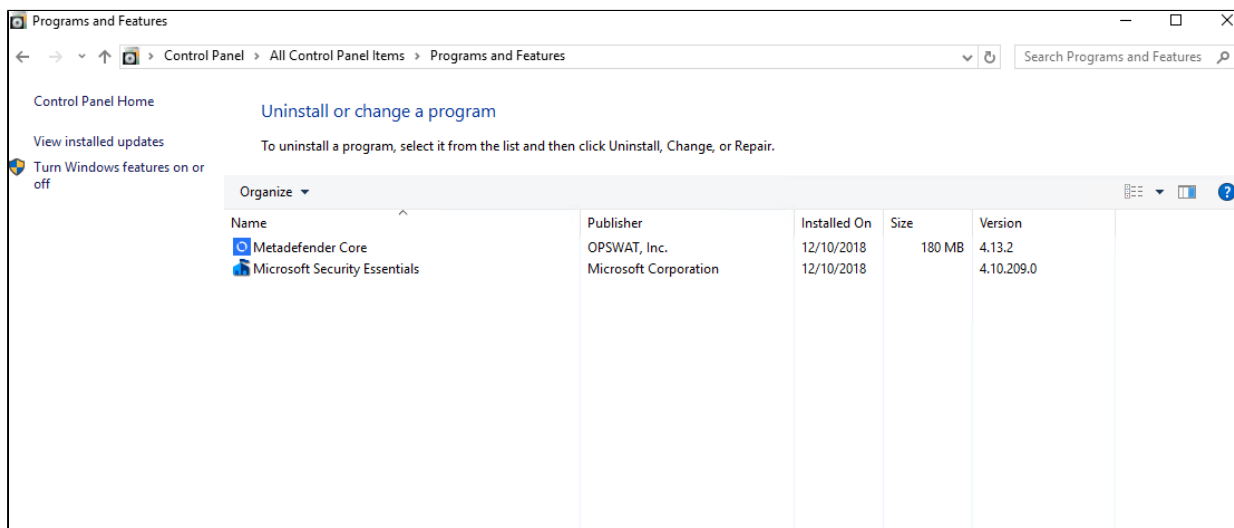
- Check Windows Defender to make sure Real-Time Protection is disabled
- It is OK for it to be red, we just disabled Real-Time Protection



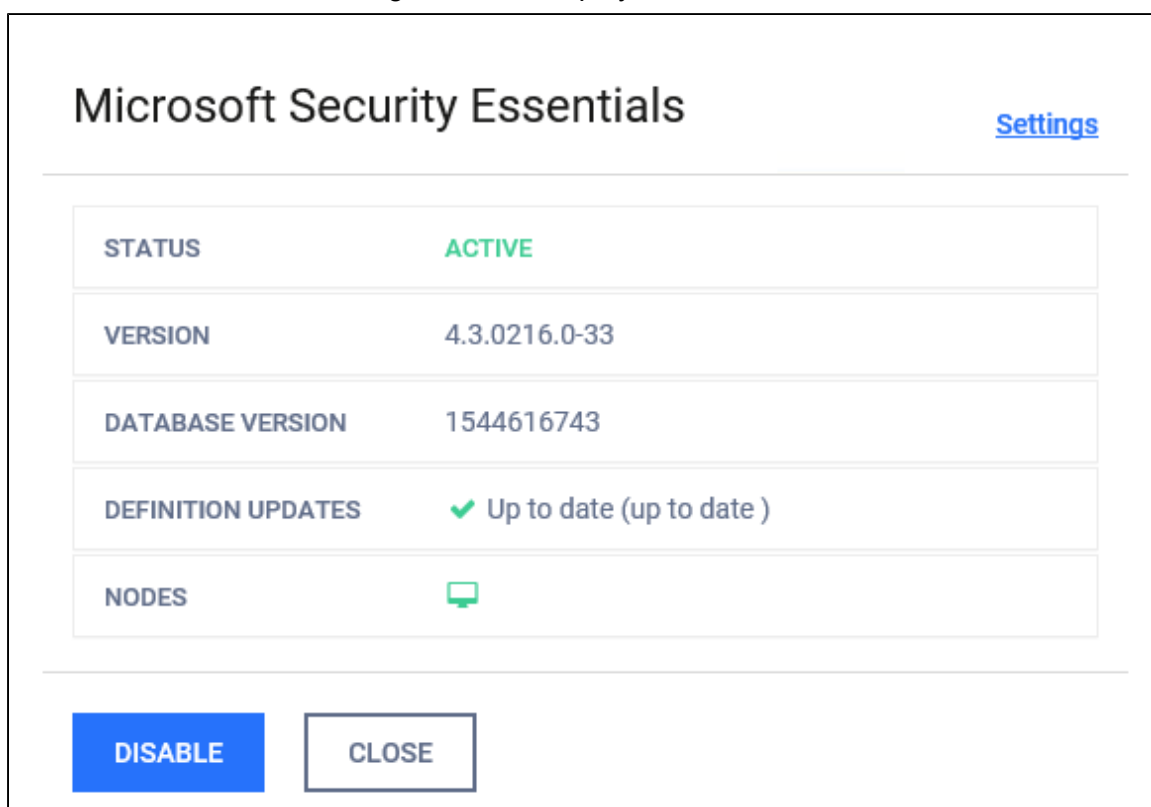
- Download the following archive which contains an install script - [install_on_windows_server.zip](#)
- Go to the following link : <https://www.microsoft.com/en-us/download/details.aspx?id=5201> and download the MSE installer



- Rename the installer that was downloaded to "MSEInstallx64"
- Place the install script and the downloaded installer in the same folder
- Run install_on_windows_server with admin rights from the above folder
- Wait a few mins for the script to run and for the CMD window to go away
- Check "Programs and Features" to see if MSE is showing up



- Enable MSE in MetaDefender Core UI
- The engine might show up as not deploying in the beginning
- Wait 5-10 mins, the engine should deploy



*This article applies to MetaDefender Core v4
This article was last updated on 2019-10-06*

VM

How to transfer your Metadefender Core v4 scan history database

In order to transfer your Metadefender Core v4 scan history database, please follow the instructions below:

1. Stop the MetaDefender Core services on both machines (source and target) 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 located in C:\Program Files\OPSWAT\MetaDefender Core\data) on the source machine. If there are any *.war or *.shm files in this folder, it means that the services are still running. Please be sure to stop the services correctly (no running *ometascan.exe* and *ometascan-node.exe* processes)
3. Copy the *ometascan.db.sqlite* file from the installation folder of the source machine to a safe place on your target machine
4. Create a backup of the *ometascan.db.sqlite* file from the target machine
5. Replace the *ometascan.db.sqlite* file from the target machine with the *ometascan.db.sqlite* file from the source machine
6. Start the MetaDefender Core services using the following commands:

```
net start ometascan  
net start ometascan-node
```

7. Login to the web management interface of the target machine and check the "Processing History" tab.

This article pertains to MetaDefender Core v4

This article was last updated on 2019-10-06

VM

Installing .NET Core runtime 3.1 on Linux for Proactive DLP 2.4.0+

Starting with Proactive DLP version 2.4.0, the engine will require .NET Core to be installed on all **Linux** machines.

Please use the following instructions to install .NET Core based on your OS:

CentOS 7

```
sudo rpmkeys --import "http://pool.sks-keyservers.net/pks/lookup?op=get&search=0x3fa7e0328081bff6a14da29aa6a19b38d3d831ef"
sudo su -c 'curl https://download.mono-project.com/repo/centos7-stable.repo | tee /etc/yum.repos.d/mono-centos7-stable.repo'
sudo rpm -Uvh https://packages.microsoft.com/config/centos/7/packages-microsoft-prod.rpm
sudo yum install -y libgdiplus
sudo yum install -y dotnet-runtime-3.1
```

CentOS 8

```
sudo rpmkeys --import "http://pool.sks-keyservers.net/pks/lookup?op=get&search=0x3fa7e0328081bff6a14da29aa6a19b38d3d831ef"
sudo su -c 'curl https://download.mono-project.com/repo/centos8-stable.repo | tee /etc/yum.repos.d/mono-centos8-stable.repo'
sudo dnf install -y libgdiplus
sudo dnf install -y dotnet-runtime-3.1
```

RHEL 7

```
rpmkeys --import "http://pool.sks-keyservers.net/pks/lookup?op=get&search=0x3fa7e0328081bff6a14da29aa6a19b38d3d831ef"
su -c 'curl https://download.mono-project.com/repo/centos7-stable.repo | tee /etc/yum.repos.d/mono-centos7-stable.repo'
subscription-manager repos --enable=rhel-7-server-dotnet-rpms
yum install libgdiplus
yum install rh-dotnet31-dotnet-runtime-3.1
scl enable rh-dotnet31 bash
scl enable libgdiplus bash
```

Modify ometascan-node.service

```
sudo nano /usr/lib/systemd/system/ometascan-node.service
```

Change the ExecStart value from the original ***/usr/sbin/ometascan-node*** to ***/usr/bin/scl enable rh-dotnet31 -- /usr/sbin/ometascan-node***

Restart the services

```
sudo systemctl daemon-reload
sudo systemctl restart ometascan-node
```

In case of failure see detailed instructions here:

<https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-manager-rhel7>
https://access.redhat.com/documentation/en-us/net_core/3.1/html/getting_started_guide/gs_install_dotnet

RHEL 8

```
rpmkeys --import "http://pool.sks-keyservers.net/pks/lookup?op=get&search=0x3fa7e0328081bff6a14da29aa6a19b38d3d831ef"
su -c 'curl https://download.mono-project.com/repo/centos8-stable.repo | tee /etc/yum.repos.d/mono-centos8-stable.repo'
dnf install libgdiplus
dnf install dotnet-runtime-3.1
```

Follow the instruction in RHEL 7 to modify ometascan-node.service

In case of failure see detailed instructions here:

https://access.redhat.com/documentation/en-us/net_core/3.1/html/getting_started_guide/gs_install_dotnet

Debian 9

```
sudo apt update
sudo apt install -y apt-transport-https dirmngr gnupg ca-certificates wget
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 3FA7E0328081BFF6A14DA29AA6A19B38D3D831EF
echo "deb https://download.mono-project.com/repo/debian stable-stretch main" | sudo tee /etc/apt/sources.list.d/mono-official-stable.list
wget -O- https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor > microsoft.asc.gpg
sudo mv microsoft.asc.gpg /etc/apt/trusted.gpg.d/
wget https://packages.microsoft.com/config/debian/9/prod.list
sudo mv prod.list /etc/apt/sources.list.d/microsoft-prod.list
sudo chown root:root /etc/apt/trusted.gpg.d/microsoft.asc.gpg
sudo chown root:root /etc/apt/sources.list.d/microsoft-prod.list
sudo apt-get update
sudo apt-get -y install dotnet-runtime-3.1 libgdiplus
```

Debian 10

```
sudo apt update
sudo apt -y install apt-transport-https dirmngr gnupg ca-
certificates wget
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-
keys 3FA7E0328081BFF6A14DA29AA6A19B38D3D831EF
echo "deb https://download.mono-project.com/repo/debian stable-
buster main" | sudo tee /etc/apt/sources.list.d/mono-official-
stable.list
wget -O - https://packages.microsoft.com/keys/microsoft.asc | gpg
--dearmor > microsoft.asc.gpg
sudo mv microsoft.asc.gpg /etc/apt/trusted.gpg.d/
wget https://packages.microsoft.com/config/debian/10/prod.list
sudo mv prod.list /etc/apt/sources.list.d/microsoft-prod.list
sudo chown root:root /etc/apt/trusted.gpg.d/microsoft.asc.gpg
sudo chown root:root /etc/apt/sources.list.d/microsoft-prod.list
sudo apt-get update
sudo apt-get -y install dotnet-runtime-3.1 libgdiplus
```

Ubuntu 16.04

```
sudo apt update
sudo apt install -y apt-transport-https ca-certificates wget
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-
keys 3FA7E0328081BFF6A14DA29AA6A19B38D3D831EF
echo "deb https://download.mono-project.com/repo/ubuntu stable-
xenial main" | sudo tee /etc/apt/sources.list.d/mono-official-
stable.list
wget https://packages.microsoft.com/config/ubuntu/16.04/packages-
microsoft-prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
sudo apt-get update
sudo apt-get install -y dotnet-runtime-3.1 libgdiplus
```

Ubuntu 18.04

```
sudo apt update
sudo apt install -y gnupg ca-certificates apt-transport-https wget
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-
keys 3FA7E0328081BFF6A14DA29AA6A19B38D3D831EF
echo "deb https://download.mono-project.com/repo/ubuntu stable-
bionic main" | sudo tee /etc/apt/sources.list.d/mono-official-
stable.list
```



```
wget https://packages.microsoft.com/config/ubuntu/18.04/packages-  
microsoft-prod.deb -O packages-microsoft-prod.deb  
sudo dpkg -i packages-microsoft-prod.deb  
sudo add-apt-repository universe  
sudo apt-get update  
sudo apt-get install -y dotnet-runtime-3.1 libgdiplus
```

In case you can't find your system listed here, or you have issues during the installation, please follow this link and select your corresponding OS for detailed instructions and troubleshooting steps: [Microsoft .Net Core runtime 3.1 installation guide for Linux](#)

If you have followed all of these steps and your engines are still unusable, please see [how to create a support package](#), login into [OPSWAT Portal](#) and open a ticket with us, having the support package attached.

This article applies to MetaDefender Core v4 Windows

This article was last updated on 2020-06-25

VM

Is Metadefender Core compromised while scanning files?

If MetaDefender Core does not support a sandbox scanning model (sandbox or a container that runs in a quarantine mode), it means that, while scanning threats, the files will be extracted to disk, and infected files can compromise the Core-System. Is it correct?

Answer: Writing a malicious file to the disk does not mean it can do any harm. To activate malware, files should be interpreted. We do not interpret or run them, we only use them as bitstreams, so Metadefender Core should not be compromised.

This article applies to MetaDefender Core v4

This article was last updated on 2019-10-06

VM

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.

An EICAR Test File can be downloaded from https://www.eicar.org/?page_id=3950. 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](#).

This article applies to MetaDefender Core v4

This article was last updated on 2019-10-06

VM

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 the product 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 following the next steps:

1. In your web browser, navigate to the MetaDefender Core Management Console at **http://localhost:8008/** (you may need to log in under admin privilege)
2. On the left menu, navigate to Policies → 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 the "Scan" tab
5. Uncheck the option "Scan failure threshold" shown below:

Modify Rule

ARCHIVE **SCAN** DEEP CDR PROACTIVE DLP 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

SAVE CHANGES CANCEL

*This article applies to MetaDefender Core v4 Windows and Linux
This article was last updated on 2019-10-06*

VM

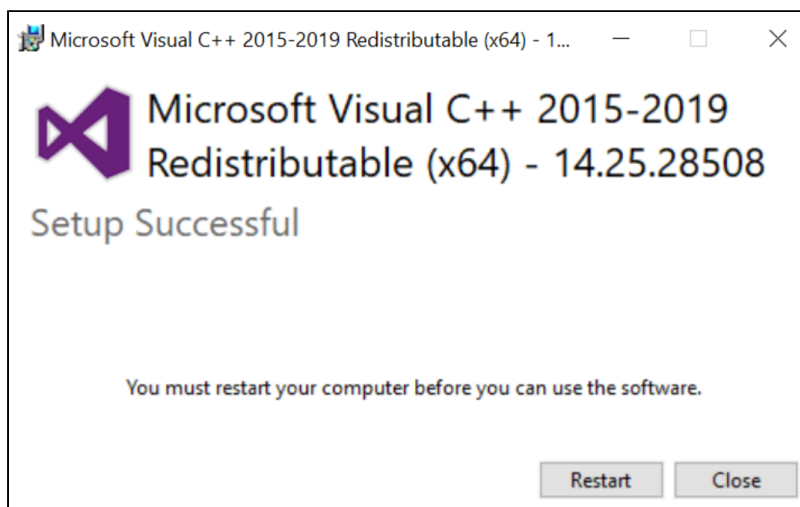
Microsoft Visual C++ 2017 Redistributable requirement for Deep CDR 5.8 or newer

How to install Microsoft Visual C++ 2017 Redistributable?

Visit the [Microsoft website](#) to download installers, we recommend customers to download and install both 64bit and 32bit for future usage although the 64bit version needed for Deep CDR:

- 32bit: https://aka.ms/vs/16/release/vc_redist.x86.exe
- 64bit: https://aka.ms/vs/16/release/vc_redist.x64.exe

If the installation process requires the system to be restarted, you can ignore it.



You don't need to restart MetaDefender service either, there is **NO downtime** for your running systems.

What happens if you haven't installed Visual C++ 2017?

Case 1: If you have a fresh installation of MetaDefender Core, the CDR 5.8+ engine will be marked as "**permanent_failed**" and Deep CDR module cannot be used:

OPSWAT. MetaDefender Core

Dashboard
Process
Policies
Inventory
Modules
Skip by Hash
Nodes
Post Actions
External Scanners
Certificates
Settings

4.17.1
License Expiration 2026-12-31

Help Center NOT MANAGED LOCAL/admin LOGOUT

Modules

Auto update turned off | [Edit Update Settings](#)

MODULE	LAST UPDATE	ACTIVITY	ENGINE	DATABASE	ENABLED
Metascan	an hour ago	1/1 processing engine is active			▼
Deep CDR	20 minutes ago	Active on 0/1 node	5.8.0-4143 (permanently failed)	5.1.1	🔴
Proactive DLP	No available engine				🔴
Threat Intelligence	No available engine				🔴
File-Based Vulnerability Assessment	No available engine				🔴
Utilities	an hour ago	2/2 engines are active			▼

Case 2: If you have a working version of CDR 5.7.4 or older, the new CDR 5.8+ will be marked as **“permanently failed”** but the Deep CDR will still work using the older version, **unless you disable/re-enable the engine.**

If you disable/reenable the engine, the old CDR module will be deleted and replaced by the new one, going back to "Case 1" mentioned above.

OPSWAT. MetaDefender Core

Dashboard
Process
Policies
Inventory
Modules
Skip by Hash
Nodes
Post Actions
External Scanners
Certificates
Settings

4.17.1
License Expiration 2026-12-31

Help Center NOT MANAGED LOCAL/admin LOGOUT

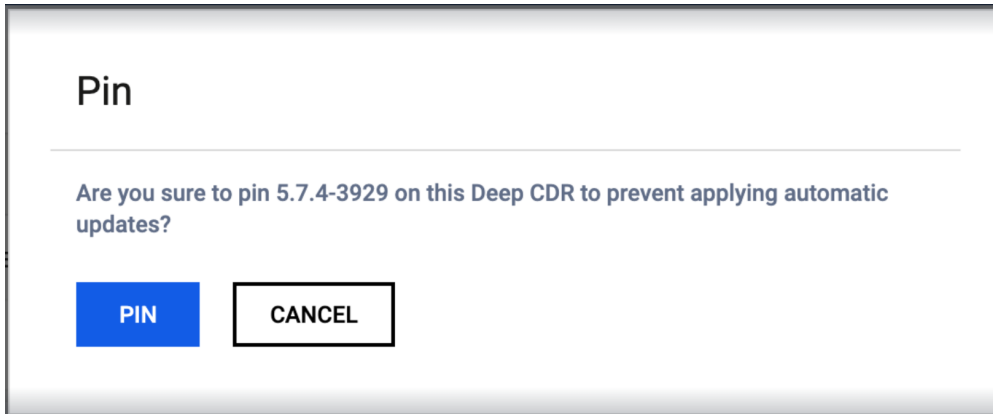
Modules

Auto update turned off | [Edit Update Settings](#)

MODULE	LAST UPDATE	ACTIVITY	ENGINE	DATABASE	ENABLED
Metascan	an hour ago	1/1 processing engine is active			▼
Deep CDR	2 minutes ago	Active on 1/1 node	5.7.2-3906 5.8.0-4143 (permanently failed)	5.1.1	🔴
Proactive DLP	No available engine				🔴
Threat Intelligence	No available engine				🔴
File-Based Vulnerability Assessment	No available engine				🔴
Utilities	an hour ago	2/2 engines are active			▼

What should you do if you can't install Visual C++ 2017?

If no outage is allowed or you require more time to go through the approval process to install the Visual C++ 2017 requirement, you have the option to "Pin the engine", which will lock the Deep CDR module to the current version. Make sure you pin the engine, not the database. Once the requirement is met, you can unpin it and MetaDefender Core will download and rollout the new Deep CDR version.



More details about the Pin function: <https://onlinehelp.opswat.com/corev4/Modules.html>

What should you do if Deep CDR 5.8+ becomes "permanently failed"?

As we mentioned above, if you accidentally disable/re-enable the engine, the engine will become "permanently failed" and cannot be used anymore. Please follow the next steps in order to get the CDR engine back in production:

- if you **can** install Visual C++ 2017, just install it. After installing the dependency, please **disable/re-enable** the engine so the CDR 5.8+ can be deployed successfully.
- if you **cannot** install Visual C++ 2017, you need to perform the following steps to get CDR 5.7.4 back in production:
 - Temporarily stop "automatic update" on MetaDefender Core by accessing Settings > Update Settings and setting the Update Mode to "Manual")
 - [Follow this KB](#) to clean up current Deep CDR version, choose ds_X_Y to clean
 - Manually upload CDR 5.7.4 engine package:
 - Contact Customer Support to provide you with the CDR 5.7.4 package
 - Extract the received archive (cdr_5_7_4_windows.7z) to a temporary location
 - Access the MetaDefender Core UI > Inventory > Modules

- Click on Upload Package and select the two files extracted in the temporary location
- Pin the engine so that new Deep CDR releases won't overwrite the 5.7.4 version.
- Turn on the automatic updates back on from the MetaDefender Core UI > Settings > Update Settings.

If you have followed all of these steps and your engines are still unusable, please see [how to create a support package](#), login into [OPSWAT Portal](#) and open a ticket with us, having the support package attached.

This article applies to MetaDefender Core v4 Windows

This article was last updated on 2020-03-27

VM

Post actions in MetaDefender Core V4.8.0 and above

Disclaimer

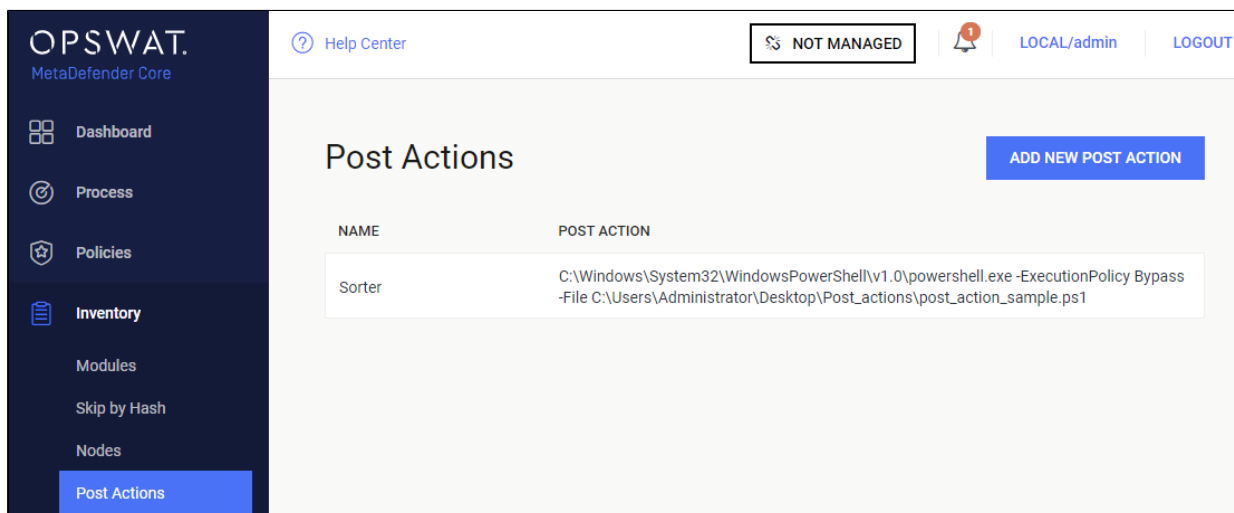
This sample script is provided for illustrative purposes only and is not guaranteed to be functional in a production environment.

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:



You will need to specify the location from where Powershell is running in your system followed by:

- -ExecutionPolicy Bypass
- -File <PathToYourScriptFile>

We created a sample Powershell script that sorts the files according to their results. (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 the currently scanned file is invalid

4 - the destination path of either allowed/blocked or both, are 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 2019-10-06

VM

Queue mechanism on Metadefender Core v4

The below article will help understand the queue mechanism in MetaDefender Core V4

The main topics that are covered are the following:

- Queue mechanism in general
- Queue size for requests
- Limit of concurrent connections
- Max file size allowed

Queue mechanism in general

The files are stored on the Node side, Core simply proxies them to the Node. Each item in the queue is handled/managed by a workflow (a thread) on the Core side.

If there is a free engine slot then Core instructs the Node to scan a specific item in the queue by the engine. The core starts processing the queue on the "first come first served" basis, however, this doesn't determine the end time of the processing.

Node uses max 1/4 of the max queue size for archive processing (this applies to all archives processed at a time, not to each one). This means if you send only one file into the queue which is an archive, the extraction fills the queue only up to 1/4 of the queue size, to leave room for further files, but provide parallel processing also.

Queue size for requests

There are no separate queues for Core and Node. Node is the one that handles the queue.

The default queue size is set to 500. To increased/decreased this value please refer to the following KB: [How can I configure the maximum queue size in MetaDefender Core v4?](#)

The number of items in the queue can be extracted from the results of the REST API call `/stat/nodes`.

There is not significant usage of memory by the items found in the queue.

We have one thread per queue item on the Core side (this was tested with 20k parallel threads).

Limit of concurrent connections

The limit of concurrent connections is based on OS limitations:

*Windows has a 4K limit

*Linux has a 65K limit

The practical amount of concurrent connections is about 1K.

There is no limitation of concurrent connections set on the license.

Max file size allowed

Limited by the available disk size of the Node.

This article applies to MetaDefender Core v4

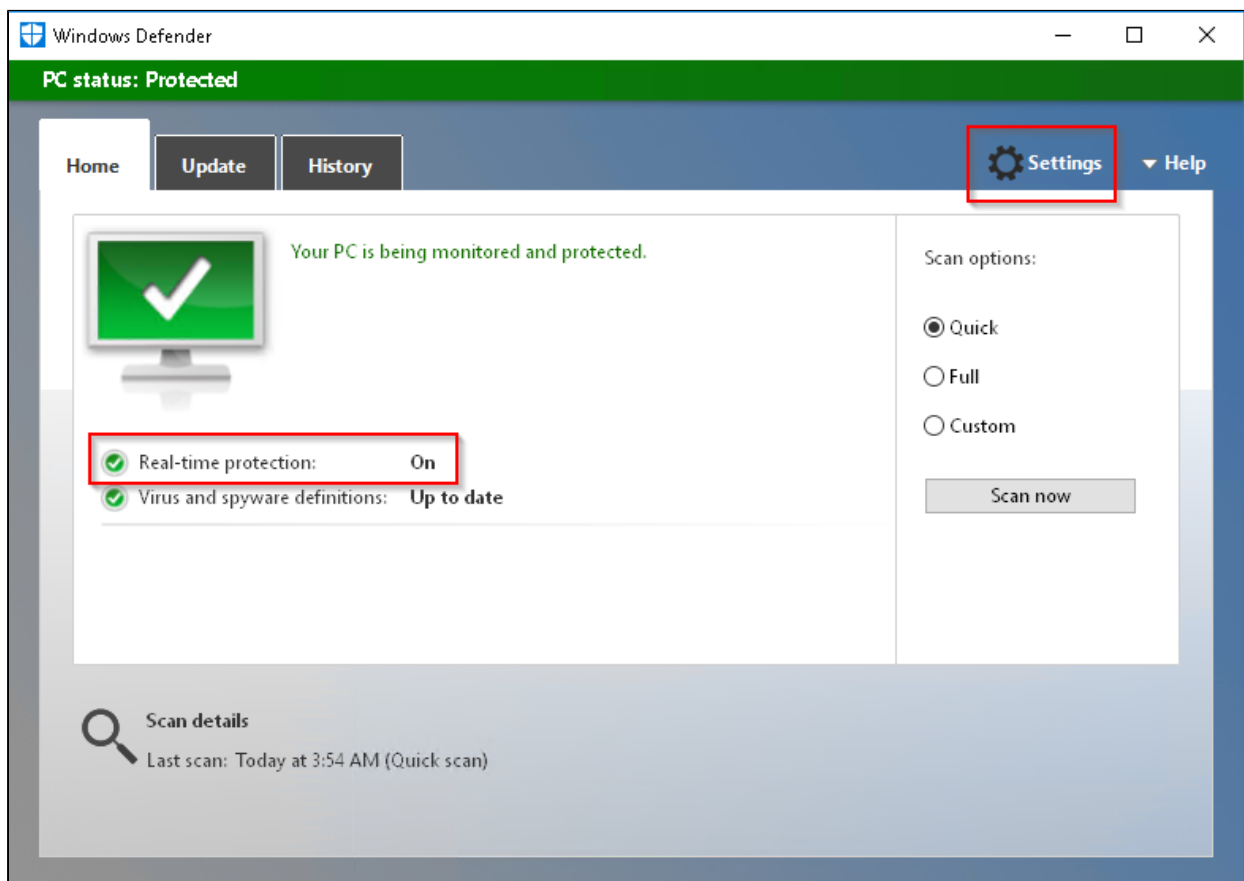
This article was last updated on 2020-05-27

VM

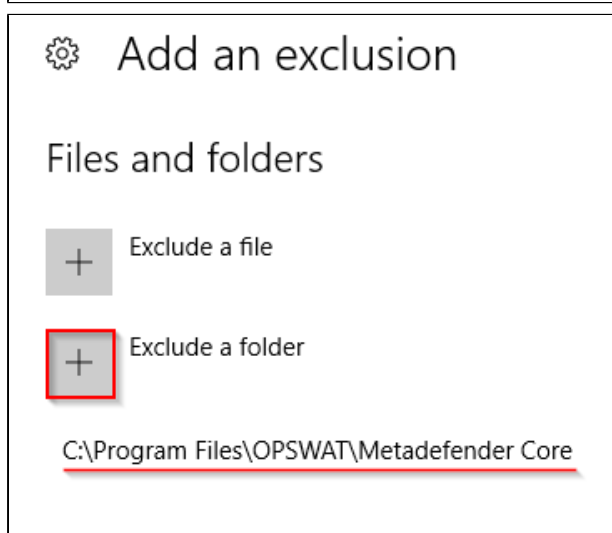
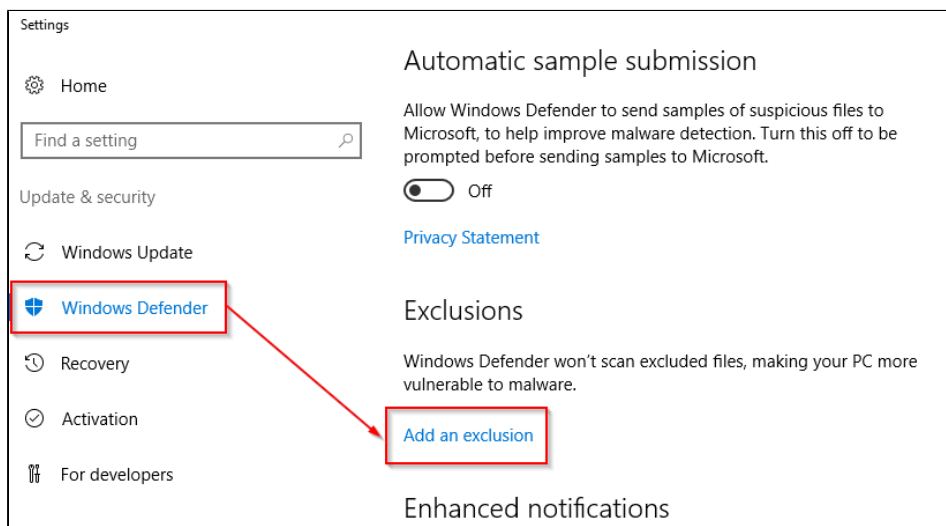
Setting up Windows Defender as a custom engine in MetaDefender Core

In order to use Windows Defender as a custom engine in MetaDefender Core, the following conditions must be met:

- Supported OS: Windows Server 2016/2019.
- Real-time protection must be turned on.



- The MetaDefender Core installation folder must be whitelisted:



- Passive Mode must be enabled for Windows Defender:
 - download the [windows_defender_passive_mode](#) archive and extract it
 - execute the ***enable_windows_defender_passive_mode.reg*** to automatically add the following 2 keys to the registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows  
Advanced Threat Protection]  
"DisableRoutinelyTakingAction"=dword:00000001  
"ForceDefenderPassiveMode"=dword:00000001
```

- if you want to change Windows Defender back to active mode, execute the ***disable_windows_defender_passive_mode.reg*** or modify the two above registries to 00000000

Considering that this custom engine uses the native Windows Defender available on the system, the behavior of the engine relies on your Windows Defender local settings.

So, for example, if you do not want to submit files to Microsoft servers using the cloud feature, you should turn these settings off in the Windows Defender configuration.

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

[Submit a sample manually](#)

This article applies to MetaDefender Core v4

This article was last updated on 2020-06-11

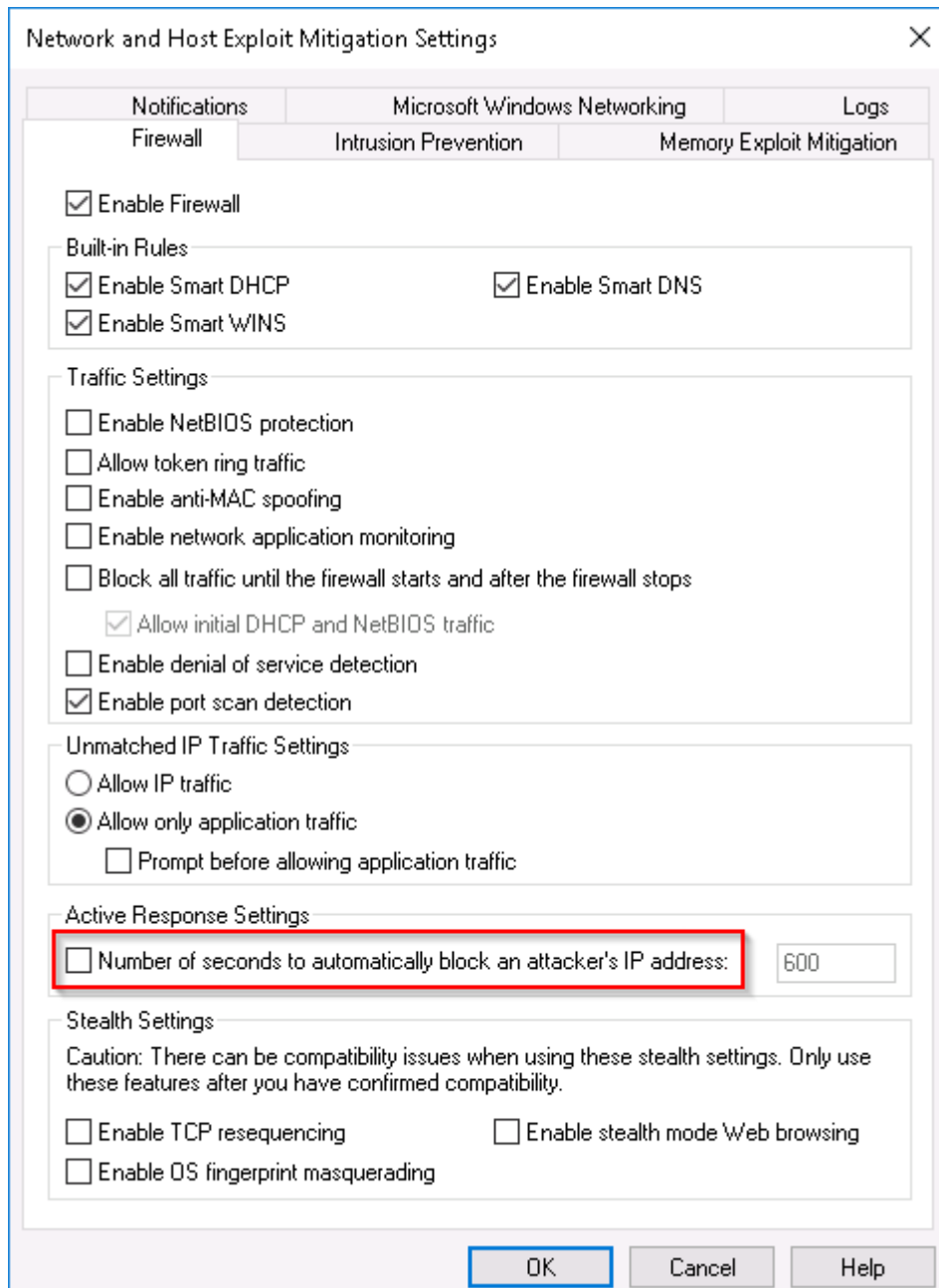
VM

Symantec Endpoint Protection settings

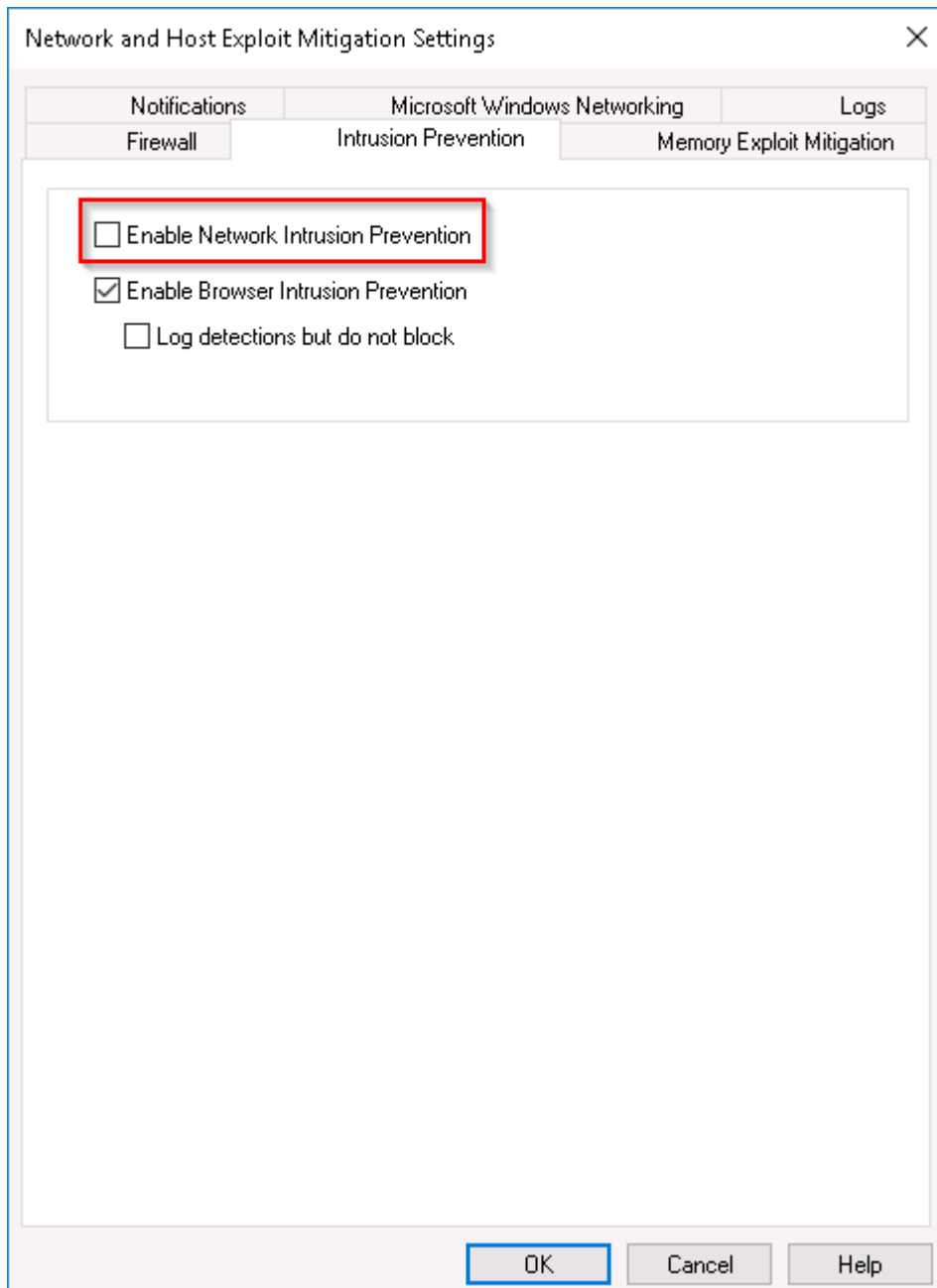
If Symantec Endpoint Protection (SEP) is used as a local AV on the machine where MetaDefender Core resides, it can interfere with the correct functioning of the OPSWAT product.

Please change the following SEP settings to ensure everything is working as expected:

1. Exclude the folder where MetaDefender Core is installed, from the SEP real-time protection: **Add security risk exception > Folder > C:\Program Files\OPSWAT**
2. Uncheck **“Number of seconds to automatically block an attacker's IP address”** from **Network and Host Exploit Mitigation Settings > Firewall**



3. Uncheck **“Enable Network Intrusion Prevention”** from **Network and Host Exploit Mitigation Settings > Intrusion Prevention**



If you have followed all of these steps and you are still experiencing issues, please see [how to create a support package](#), login into [OPSWAT Portal](#) and open a ticket with us, having the support package attached.

This article applies to MetaDefender Core v4 Windows

This article was last updated on 2020-07-16

WM

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:

- Filetype group
- MIME-type
- Filename

The documentation is here https://onlinehelp.opswat.com/corev4/3.6.2._Workflow_template_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 whose 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 whose 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 whose 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 2019-10-06

VM

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 Template does not get applied directly to the file, the Workflow Rule is associated with 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 2019-10-06

AG

What are the differences between TrendMicro and TrendMicro HouseCall anti-malware engines?

The main difference between **Trendmicro** and **Trendmicro HouseCall** engines is the database: TrendMicro uses an Enterprise database while TrendMicro HouseCall uses a Consumer database.

Consumer (TrendMicro HouseCall) = home users (e.g. Titanium); may also contain bleeding edge due to less false positive concerns and therefore may have more detections.

Enterprise (TrendMicro) = business products (e.g. OfficeScan); tuned towards minimizing false positive at the cost of possibly fewer detections.

This article applies to MetaDefender Core v4

This article was last updated on 2018-10-06

VM

What does "Potentially Vulnerable File" result mean?

"Potentially Vulnerable File" are files associated with vulnerable components or specific application versions determined by [OPSWAT's File-Based Vulnerability Assessment technology](#). It gives IT administrators the ability to:

- Check certain types of software for known vulnerabilities before installation
- Scan systems for known vulnerabilities when devices are at rest
- Quickly examine running applications and their loaded libraries for vulnerabilities

This article applies to MetaDefender Core v4

This article was last updated on 2019-12-23

VM

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

	Included in MetaDefender Core v3?	Included in MetaDefender Core v4?
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
Sanitize clean and blocked files (Windows)	YES	YES
Sanitize clean and blocked files (Linux)	N/A	YES
API		
REST v1	END-OF-LIFE	NOT PLANNED

	Included in MetaDefender Core v3?	Included in MetaDefender Core v4?
REST v2	YES	YES
COM	YES	NOT PLANNED
Upload files using chunked encoding	YES	NOT YET
Support for other MetaDefender products		
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 2019-08-02

AG

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 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 metadata 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 metadata 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 metadata 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.

- Ansi Text (*.txt)
- ASCII Text
- CSV (Comma-separated values) (*.csv)
- 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 Office Open XML 2007, 2010, 2013, and 2016 (*.xlsx)
- 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 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)

- 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)
- XML (*.xml)

This article applies to MetaDefender Core v4

This article was last updated on 2019-06-28

AG

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 cases, used interchangeably. But from a strict definition standpoint, 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
777	777 compressed archive
??_	Microsoft KWAJ compressed (Phil Katz's 'deflate')
@@@	DOS 2.0-3.2 Backup control info
_01	Compaq QRST disk image

Supported file type	Description
{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
3D2	Cyber Studio CAD-3D v2 object
3DB	3DMark database
3DM	Cadent 3D Model
3DMF	QuickDraw 3D Metafile (binary)
3DP	3Digi Parameters

Supported file type	Description
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
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

Supported file type	Description
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
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

Supported file type	Description
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)
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

Supported file type	Description
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
ACD	ALAN game
ACDB	Audio Calibration DataBase
ACE	ACE compressed archive
ACF	DB/TextWorks Database Access Control
ACI	ACI development appraisal data

Supported file type	Description
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
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

Supported file type	Description
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
AEP	After Effects Project
AERO	Aero Studio song
AES	AES Crypt encrypted
AF3	ABC FlowCharter chart
AFA	Astrotite compressed archive

Supported file type	Description
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
AIA	Adobe Illustrator Action
AIC	Advanced Image Coding bitmap
AIF	EPOC/Symbian Application Info
AIF/AIFF	AIFF Audio Interchange File Format
AIFC	

Supported file type	Description
	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
ALC/VLC	AcuCorp AcuCOBOL license
ALE	Avid Log Exchange
ALIAS	Find and Run Robot (FARR) alias
ALM	Aley's Module v1.0

Supported file type	Description
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
AMOS	AMOS Pro source
AMR	AMR (Adaptive Multi Rate) encoded audio
AMS	Extreme's Tracker module
AMT	ABBYY Finereader language data

Supported file type	Description
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)
ANJUTA	Anjuta IDE project
ANK	Children of the Nile city
ANL	SimLife Animal
ANM	DeluxePaint Animation

Supported file type	Description
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
APE	Monkey's Audio
APEX	AVM APEX sample studio sound bank
APF	MightyFax
API	Adobe Acrobat Reader Plugin

Supported file type	Description
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
APPXMANIFEST	Windows 8 Appx Package Manifest
APR	Apadana Project
APS	AProSys module
APT	Adaptive Prediction Tree (APT) encoded bitmap

Supported file type	Description
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
ARH	Squash compressed archive
ARI	ARRIRAW image
ARJ	ARJ compressed archive
ARK	DS Squeeze archive
ARL	Aureal Aspen sound bank

Supported file type	Description
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
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

Supported file type	Description
ASC/TXT	PGP clear text signed message
ASCX	Microsoft ASP.NET Web User Control
ASD	ASD Archiever 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
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

Supported file type	Description
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
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

Supported file type	Description
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
AVS	Winamp Advanced Visualization Studio File
AW	Microsoft Answer Wizard
AWD	Artweaver Document
AWL	AWL programming language (Var. 1)
AWLIVE	Active WebCam live capture

Supported file type	Description
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
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

Supported file type	Description
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
BBL	BibTeX Generated Bibliography
BBSONG	Beepola chiptune
BBX	BrainBox neural net
BC	Big Crunch compressed file
BCIF	BCIF bitmap

Supported file type	Description
BCK	BackupExpress Pro
BCO	Bitstream Compressed Outline font
BCPKG	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
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

Supported file type	Description
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
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

Supported file type	Description
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
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

Supported file type	Description
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
BMF	BMF v1.x bitmap
BMFC	AngelCode Bitmap Font Generator Configuration
BMG	Message string storage
BMM	Bleeper Music Maker music

Supported file type	Description
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
BONK	Bonk compressed audio
BOOK	FrameMaker book
BOOTSKIN	BootSkin Vista theme
BOT	Soldat Bot Information
BP	BP SoundMon 2 module

Supported file type	Description
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
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

Supported file type	Description
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
BTAPP	uTorrent Application
BTD	Power To-Do List Data
BTG	Binary TerraGear - FlightGear scenary data
BTPC	BTPC encoded bitmap
BTR	FrontPage Binary-tree index

Supported file type	Description
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
BX	BX Embrilliance font
BXB	BasicX compiled bytecode
BXL	Accelerated Designs PCB Library
BXU	PictureGear Studio file
BXY	NuFX archive (with Binary II header)

Supported file type	Description
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)
CAB	InstallShield compressed Archive
CAD	CadStd drawing
CAF	Cal3D Animation File
CAG	Capella gallery data file
CAI	SeeYou flight data

Supported file type	Description
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
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)

Supported file type	Description
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
CCA	Multimedia Fusion - Click'n'Create file
CCB	CocosBuilder info
CCBI	CocosBuilder exported info
CCC	TeslaCrypt/Cryptowall encrypted
CCD	

Supported file type	Description
	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
CDDS	Midtown Madness 3 data
CDE	MicroHof Code
CDF	Affymetrix Chip Definition File (Text)
CDF/NC	NetCDF Network Common Data Form

Supported file type	Description
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	ComputerEyes Raw Data Format low-res bitmap
CE2	ComputerEyes Raw Data Format hi-res bitmap
CEB	Apabi eBook
CED	EEGLAB Channel Data

Supported file type	Description
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
CFOSSPEED	cFosSpeed registration key
CFP	CoverFactory Project
CFT	CFast Animation
CGC	Colour Genie high level tape image
CGM	Computer Graphics Metafile (Clear Text)

Supported file type	Description
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
CHR	BGI (Borland Graphics Interface) font
CHT	Harvard Graphics Chart (v2.x)
CHT/SCT	SPSS template
CHZ	ChArc compressed archive
CI	CyberTracker Instrument

Supported file type	Description
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
CKF	Casio Keyboard File
CKT	CircuitMaker schematic
CL2	Hy-Tek Meet Results
CL2ARC	Comic Life 2 Archive
CL4	Easy CD Creator 4 Layout

Supported file type	Description
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
CLR	3ds UI colors
CLS	Visual Basic class definition
CMA	OCaml bytecode (library)
CMAP/PAL/IFF	IFF Color Map
CMATE	ControllerMate programming

Supported file type	Description
CMB	Reason Combinator Instrument Patch
CMBL	Vernier Logger Pro data
CMC	Comic Collector Collection data
CMD5	CrystalMaker Data format (v5-6)
CMD5/CMDF/CMMF	CrystalMaker Data format (generic)
CMDF	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
CMX	Corel Metafile Exchange Image (Legacy)
CMZ	Compressed archive
CN	Copy Numbers format
CNC3REPLAY	Command and Conquer 3 replay
CNDF	Compressed Channel Data File

Supported file type	Description
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
COMFYCAKESSAVE-MS	Comfy Cakes saved game
COMICDOC	Comic Life Document
COMICLIFE	Comic Life Document
COMPANYLOGO	CompanyLogoDesigner project file
COMPILED	Flare3D Shader Language Compiled
COMPOSITEFONT	Windows Composite Font
COMX	COMX-35 program
CONF	fswebcam configuration
CONTACT	Windows Contact

Supported file type	Description
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
CPG	Cool Page Project
CPH	Corel PrintHouse image
CPI	AVCHD Clip Information
CPIO	CPIO archive (binary)
CPJ	WinOnCD Project
CPK/CAK/FILM	Sega CPK video
CPL	Corel Color Palette

Supported file type	Description
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
CRPLUGIN	ComicRack plugin
CRS	StepMania Course
CRT	C64 Cartridge image
CRU	Crush compressed archive
CRV	Corel PhotoPaint Tone Curve

Supported file type	Description
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
CSDL	ADO.NET Conceptual Schema Definition Language
CSF	Cal3D Skeleton File
CSH	Adobe Photoshop Custom Shape
CSM	CASL compiled PalmPilot program

Supported file type	Description
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
CTM	OpenCTM 3D mesh
CTP	CrazyTalk Project
CTS	TreeSheets project
CTT	MSN Messenger Saved Contact List

Supported file type	Description
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
CURXPHEME	CursorXP theme
CUS	Delitracker Customplay module
CVA	Compaq Diagnostics
CVC	Cybiko Video Container video
CVD	Calamus Vector Document
CVF	Jet-VoiceMail audio data
CVG	Calamus Vector Graphic
CVP	WinFax Cover Page
CVS	Satori Paint Canvas

Supported file type	Description
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
CZIP	ZipGenius encrypted compressed archive
DAT/FH11	Freehand 11 Project
DAT/LOG	LabVIEW binary Datalog
DAT1	NeoRAGEx savestate

Supported file type	Description
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
DBH	PC-File database header
DBI	Isearch Database Info
DBK	Orcad Schematic Capture Backup
DBK/XML	DocBook document

Supported file type	Description
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
DCM	KiCad Documentation
DCM/DIC/DICOM	DICOM medical imaging bitmap
DCOL/IFF	IFF Direct Color bitmap
DCR	Director - Shockwave movie

Supported file type	Description
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
DEPEND	Code::Blocks Dependencies
DEPLOYPROJ	Deployment Manager configuration
DEPOT	HP-UX Software Distributor catalog depot
DER	DER encoded X509 Certificate

Supported file type	Description
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)
DFONT	Macintosh OS X Data Fork Font
DFT	Solid Edge Draft Document
DFU	Device Firmare Upgrade format (generic)
DFW	Derive for Windows (generic)

Supported file type	Description
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
DIN/BIN	DESI-III drawing
DIP	DipTrace PCB
DIS	DRI Display Manager Display
DIT	Studio Printer Dither method

Supported file type	Description
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
DMD	Oracle SQL Developer Data Model
DMF	D-Lusion Music Format module
DMG	Macintosh Disk image (BZ2 compressed)
DMI	DMIS input data

Supported file type	Description
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
DOC/ST	1ST Word Plus Document
DOC/WS	WordStar document (gen)
DOC/WS2	WordStar 2000 document
DOC/WS5	WordStar 5 document

Supported file type	Description
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
DPS	DivX Skin
DPT	Kingsoft Presentation template
DPW	Decision Pad Worksheet (v2.x)
DPX	

Supported file type	Description
	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
DRW	CADS Planner drawing
DRW/DSF	Micrografx Designer Drawing (v3.1)
DRX	DaVinci Resolve eXchange data

Supported file type	Description
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
DSM	DeSmuME Movie capture
DSN	ISIS Schematic file
DSP	MS Developer Studio Project

Supported file type	Description
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)
DTQ	Visual Database Tools Query
DTS	DTS encoded audio
DTSCONFIG	SQL Server Integration Services Configuration

Supported file type	Description
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
DWA	Project Dogwaffle animation (generic)
DWD	DiamondWare Digitized audio
DWF	Autodesk Design Web Format

Supported file type	Description
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)
DXS	DeleD scene
DYF	Audio DiffMaker file set
DYL	Psion Library

Supported file type	Description
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
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

Supported file type	Description
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
EDOC	Electronically certified Document
EDX	EDraw Max drawing
EED	EEDraw Drawing
EFE	Ensoniq EPS family instrument

Supported file type	Description
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
EJPG	Encrypted JPEG bitmap
EKB	ZMC VisualTablet data
ELC	Combustion 2 Particle Library
ELD	EasyLanguage Document

Supported file type	Description
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
EMS	Electronic Music System v6 module
EMULECOLLECTION	eMule Collection file
EMW	Resident Evil player model data
EMX	Rational Software Architect Model

Supported file type	Description
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
EOT/FNTDATA	Embedded OpenType font
EP	Pencil sketch
EP/EPW/EZP/TXT	EasyPlot save file
EPA	Award BIOS logo bitmap (136x126) (v1)

Supported file type	Description
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
ERF	BioWare Entity Resource File
ERS	Earth Resource Mapping Raster
ERV	Earth Resource Mapper Vector
ERWIN	ERwin model

Supported file type	Description
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
ETL	Window tracing/diagnostic binary log
EU4	Europa Universalis IV saved game
EV2	Emblaze Video 2 video
EV3	LEGO Mindstorms EV3 project

Supported file type	Description
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
EXE/COM	SymbOS Executable
EXE/OBJ	QDOS executable
EXM	HP Palmtop 95/100/200LX Sys.Manager compliant Executable
EXR	OpenEXR High Dynamic-Range bitmap

Supported file type	Description
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
FACE/FAC	FaceSaver bitmap
FACET	Facet file
FACT	ElectricImage 3D file
FACTORY	Simplify3D Factory session data

Supported file type	Description
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
FBL	iGO map
FBM/CBM	Fuzzy Bitmap
FBP7	FinalBuilder 7 Project
FBS	FBIde session

Supported file type	Description
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
FCW	FastCAD for Windows drawing (generic)
FD2	EasyPrint PictureMate borders
FDAT	Fiasco Database: data file
FDB	FT/Pro Form

Supported file type	Description
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
FET	FET Timetable
FF	Call of Duty game data
FFDATA	ABBYY eForm Filler data
FFE	Microsoft DirectInput Force Feedback Effect

Supported file type	Description
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
FIDX	Fiasco Database: index File
FIF	Fractal Image Format bitmap
FIG	Cabri figure
FIL	AVG Antivirus Vault file

Supported file type	Description
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
FLM	Adobe FilmStrip
FLOW	Expression SketchFlow data
FLP	Activstudio Flipchart
FLSX/FLWX	FileLocator Pro workspace/search (v8.0)

Supported file type	Description
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)
FNC	Vue D'Esprit 4 function definition
FNF	PTC FEM Neutral Format model
FNK	FunkTracker module
FNS	Free Notes document

Supported file type	Description
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)
FP7	FileMaker Pro database (v7-11)
FPAGE	XPS FixedPage object
FPF	IKEA Kitchen Planner Document
FPG	DIV Games Studio Graphics Library

Supported file type	Description
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
FRO	A-Robots Fighting Robot Object
FRX	Microsoft Visual Basic Form
FS	Final Burn savestate
FSB	FMOD Sample Bank Format

Supported file type	Description
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
FTM	Face The Music module
FTR	File-Type Rule
FTS	Windows Help Full-Text Search index file
FTW	Family Tree Maker Family Tree

Supported file type	Description
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
FXR	WinFax Sent / Received document
FZ	Flexible Image Transport System bitmap (compressed)
FZB	Fritzing Bin module

Supported file type	Description
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
GA3	Graphical Analysis 3 document
GAB	WinDev Controls' Styles description
GADGET	Microsoft Vista Sidebar Gadget (CAB - Obsolete)

Supported file type	Description
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
GBR	GameBoy Sound System GBR dump
GBS	GameBoy Sound System dump
GBT	GFI Backup Task

Supported file type	Description
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
GDM	General DigiMusic module
GDOC	Google Drive Document link
GDP	GUI Design Studio Project

Supported file type	Description
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
GFS	GGFileSPlit File Fragment
GFT	GSP Family Tree
GFX	

Supported file type	Description
	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
GLA	Sothink SWF Easy Project
GLADE	Glade UI design

Supported file type	Description
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)
GO/PRB	Ishi Format Go game
GOB	Dark Forces Game data archive

Supported file type	Description
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
GRA	Chasys Draw IES Gradient
GRAFFLE	OmniGraffle Drawing

Supported file type	Description
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
GRINDEX	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
GRZ	GRZip compressed archive
GSC	GS-Calc workbook

Supported file type	Description
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
GUI	GUI Design Studio design
GUIDE	Amigaguide hypertext document

Supported file type	Description
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
H2PATTERN	Hydrogen Pattern
H2SONG	Hydrogen song

Supported file type	Description
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
HDZ	KeyShot environment
HE5	Hierarchical Data Format Release 5

Supported file type	Description
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
HIR	C64 Hires bitmap
HIV/DAT	Windows NT Registry Hive (generic)

Supported file type	Description
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
HPI	Hemera Photo-Object Image
HPK	HPACK compressed archive

Supported file type	Description
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
HTR/HAPTAR	Haptek Compressed file
HUD	HUD Maker

Supported file type	Description
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
IB3	ICDRAW group icon bitmap
IBCC	Apple Application Information Table

Supported file type	Description
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
IDW	AutoDesk Inventor drawing
IDX	Java Applet cache index

Supported file type	Description
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
IKMP	IK Multimedia Preset
IL3	particleIllusion library

Supported file type	Description
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
IMN	IncrediMail notifier
IMO	iMON Setting file

Supported file type	Description
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
INX	Inkscape extension descriptor
IOBJ	Visual Studio Intermediate Object

Supported file type	Description
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	Ipix Spherical Panorama
IPYNB	IPython notebook
IQY	Microsoft Web query
IRCP	IRIDAS Composite playlist

Supported file type	Description
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
ITC2	iTunes Cover Flow Data (v2)
ITL	iTunes Music Library

Supported file type	Description
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
IWI	Infinity Ward Image bitmap
IXL	DB/TextWorks Database Indexed List

Supported file type	Description
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
JBI	Motoman Relative Job
JCE	JWPce document
JCEKS	Java SunJCE KeyStore
JCF	JTAG Chain File
JCI	JTAG Chain Information
JCLIC	JClic project
JCP	JCreator Project

Supported file type	Description
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
JNG	JPEG Network Graphics bitmap
JNILIB	JNI Library

Supported file type	Description
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
JRXML	JasperReports JRXML report definition
JSB	JavaScript Bean file

Supported file type	Description
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
JWR	LegaSuite GUI Runtime
JZLIB	Lemur Module

Supported file type	Description
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
KDS	KD Player Skin
KDX	Google Earth import definition

Supported file type	Description
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
KIN	Kinemage protein language
KK3	Kaleidoscope Kreator 3 workspace

Supported file type	Description
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
KPR	KOffice KPresenter Presentation
KPX	Kid Pix project

Supported file type	Description
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
KVTML	KWordQuiz learning file
KW3	KanjiWORD document

Supported file type	Description
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
LAV	DNA Sequence Alignment
LAY	Sprint Layout Printed Circuit Design (v6.0)

Supported file type	Description
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
LFM	Lazarus Form
LFP	Lytro Light Field Picture web format

Supported file type	Description
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
LIN	X-Plane Painted Line
LIQ	Liquid Tracker module

Supported file type	Description
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
LOC	Topografix's EasyGPS/TerraByte Location file
LOG	Cabrillo Log (v2.0)

Supported file type	Description
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
LRPREV	Lightroom preview data
LRTEMPLATE	Adobe Photoshop Lightroom Template

Supported file type	Description
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	LinkTreeNode document
LUACODEC	Reason Remote Lua Codec
LVA	Logitech Video Effects Avatar
LVF	Lightweight Video Format video

Supported file type	Description
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
LZC	Need for Speed game data
LZH/LHA	LHARC/LZARK compressed archive (generic)

Supported file type	Description
LZMA	LZMA compressed archive
LZO	lzop 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
M4A/MP4	AAC Audio in MP4 container
M4B	iTunes Audio Book

Supported file type	Description
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
MANIFEST	Windows Manifest - Visual Stylesheet XML file
MAP	3by5 Index

Supported file type	Description
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
MBI	MBasic source
MBM	EPOC/Symbian MultiBitMap

Supported file type	Description
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
MCML	Media Center Markup Language
MCO	MSN Messenger Wink

Supported file type	Description
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
MDD	MDict resource
MDF	Microsoft SQL Server database (generic)

Supported file type	Description
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
MEG	MEGA data format
MEI	Music Encoding Initiative format

Supported file type	Description
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
MGB	Paragon 5 Gameboy Tracker module
MGF	L3DT Map Group File

Supported file type	Description
MGOURMET3	MacGourmet 3 document
MGR	MGR bitmap (modern, 8bit aligned)
MGS	MSX Gigamix MGSDRV3 music
MGT	Megatracker module
MHD	Metalmage 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)
MINIPSF2	PSF2 Playstation 2 Sound Format rip (Mini)
MINIQSF	QSF Capcom QSound Format rip (Mini)

Supported file type	Description
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
ML	Musicline module
MLAPPINSTALL	MATLAB app installer

Supported file type	Description
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
MMM	Adobe Type Manager Multiple Master Metrics
MMMS	MetaMind Machine Sequence

Supported file type	Description
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
MODEL	CATIA model
MODFEM	Femap Model

Supported file type	Description
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
MPCPL	MediaPlayer Classic Playlist
MPD	DASH Media Presentation Description

Supported file type	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
MQO	Metasequoia 3D scene
MQV	Sony / Mobile Quicktime Video

Supported file type	Description
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
MSF	Mozilla Mail Summary file
MSH	Fluent mesh

Supported file type	Description
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
MSG	Mail Message
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
MTM	MultiTracker module

Supported file type	Description
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 Transportable File
MUS/MYR	Myriad Harmony / Melody assistant music
MUSE	Emacs Muse project
MUSIC	SuperTux Music
MUSINK	Musink music score
MUX	MUX video
MV	Miva Script

Supported file type	Description
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
MWDECK	Magic Workstation Deck

Supported file type	Description
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
MZP	MOZART Percussion map

Supported file type	Description
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
NCB	Microsoft C/C++ program database

Supported file type	Description
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
NDX	WinDev Index

Supported file type	Description
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
NGB	NonoPocket nonogram

Supported file type	Description
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
NLM	Netware Loadable Module

Supported file type	Description
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)
NPY	NumPy data

Supported file type	Description
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
NSP	Computerized Speech Lab NSP audio

Supported file type	Description
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)
NUV	NuppelVideo (MythTV) video

Supported file type	Description
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
OAD	Notaro document

Supported file type	Description
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
ODCL	Open Dialog Control Language for AutoCAD

Supported file type	Description
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
OFFP	Origin Function Plot
OFR/OFS	OptimFROG encoded audio
OFT	Outlook Form Template
OFW	TopLevel Forms Form
OGG	OGG Vorbis audio

Supported file type	Description
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
OND	Lotus Notes Encapsulated Memo

Supported file type	Description
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
OPX	EPOC OPL eXtension

Supported file type	Description
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
OUT	Lua 4.0 bytecode

Supported file type	Description
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
P00/S00/R00/U00	PC64 flexible container format

Supported file type	Description
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
PACK	Git pack format

Supported file type	Description
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
PATCH	RCS/CVS diff output

Supported file type	Description
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
PBZ	Pebble firmware

Supported file type	Description
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)
PCU	XProfan Compiled Unit

Supported file type	Description
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
PDU	Protocol Data Unit message data

Supported file type	Description
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
PFB	Adobe PostScript Type 1 Font

Supported file type	Description
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
PHF	Photo Font

Supported file type	Description
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
PISKEL	Piskel sprite

Supported file type	Description
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
PLBM	IFF Planar Bitmap

Supported file type	Description
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
PMC	Print Magic Card

Supported file type	Description
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
POD	Plain Old Documentation format

Supported file type	Description
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
PPJ	Premiere project

Supported file type	Description
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)
PR4	Harvard Graphics Presentation

Supported file type	Description
PRC	PMD 85 emulator recording
PRD	Microsoft Printer Definition
PREFS	Amiga Preferences
PREXPOR	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
PRS	SNS-HDR Preset

Supported file type	Description
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
PSL	Pattern Space Layout format

Supported file type	Description
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
PT36	ProTracker 3.6x module

Supported file type	Description
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 Trekkkr 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
PUP	Puppy Linux DotPup installer package

Supported file type	Description
PURBLEPAIRSSAVE-MS	Microsoft Purple Pairs Saved game
PURBLESHOPSAVE-MS	Microsoft Purple 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
PWI	Pocket Word document

Supported file type	Description
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
PZ3	Poser scene

Supported file type	Description
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
QFILTER	Apple Quartz Filter

Supported file type	Description
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
QRS	SlickRun MagicWord Pack

Supported file type	Description
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)
QWS	Quartus Workspace

Supported file type	Description
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
RAR	RAR compressed archive (gen)

Supported file type	Description
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)
RBXL	Roblox Location

Supported file type	Description
RBXM/RBXM	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
REAPEAKS	REAPER media peak information (v1.0)

Supported file type	Description
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
RFN/RFP/RFX	RoboForm saved data

Supported file type	Description
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
RLC	Radiant LoopCAD Project

Supported file type	Description
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
RNQS	Pokemon Randomization Quick Settings

Supported file type	Description
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
ROTECT	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
RPS	Propellerhead Software Reason Song

Supported file type	Description
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
RTC	Office Live Meeting Connection

Supported file type	Description
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	Applmage 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
RVPROJ2	RPG Maker VX Ace Project

Supported file type	Description
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	Expert Witness compression Format SMART disk image

Supported file type	Description
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
SA	Sonic Arranger module
SA2	Surprise! AdLib Tracker 2.0 module

Supported file type	Description
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
SBJ	Superbase Project
SBK	Emu Sound Font v1.0

Supported file type	Description
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
SCEN	Caligari TrueSpace Scene (v2.x)
SCENE	3D Master Scene

Supported file type	Description
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
SCRIPTTERMINOLOGY	AppleScript Terminology
SCRIVX	Scrivener XML document

Supported file type	Description
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
SDLPPX	SDL Trados Studio Project Package
SDLPROJ	SDL Trados Studio Project

Supported file type	Description
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
SEP	ChemSep project
SEQ	Cyber Paint Sequence

Supported file type	Description
SER	SER format video
SES	Cool Edit / Audition Session
SESSION	Session Manager Firefox Backup
SEX	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
SFVIDCAP	Sony Foundry Video Capture project
SFW	

Supported file type	Description
	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
SHFBPROJ	Sandcastle Help File Builder Project

Supported file type	Description
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
SID2	Sidmon II module

Supported file type	Description
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
SKCHR	SketchChair document

Supported file type	Description
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
SLK	SYLK - SYmbolic LinK data

Supported file type	Description
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
SMT	Memo File Apollo Database Engine

Supported file type	Description
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
SNK	Strong Name Key

Supported file type	Description
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
SPC	Crimson Editor language specification file

Supported file type	Description
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
SPR	Brother PowerNote spreadsheet

Supported file type	Description
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
SRR	ReScene Release data

Supported file type	Description
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
ST*	GetDataBack Scan trace

Supported file type	Description
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
STM/STX	Scream Tracker module

Supported file type	Description
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
STZ	stz compressed data

Supported file type	Description
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
SVF	Simple Vector Format (generic)

Supported file type	Description
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
SWS	PowerDesigner WorkSpace

Supported file type	Description
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
T@0	Timeline schedule (v2.0)

Supported file type	Description
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
TBASICCX	thinBasic Console scripts (obfuscated)

Supported file type	Description
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)
TD0	

Supported file type	Description
	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 cartridge 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
VVVVVV	VVVVVV 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 2019-11-04.

VM

What is the frequency of signature/definition updates?

There are two parameters that determine the frequency of signature/definition updates:

- The frequency with which each antivirus vendor releases an update

- The configuration setting on your MetaDefender Core or MetaDefender Kiosk installation that specifies the time interval between system checks and applying new updates.

Most of the antivirus vendors release definitions at least once per day. Many have multiple daily releases. Some vendors release updates on weekends while others do not.

If you use OPSWAT's online update mechanism to apply updates (i.e. via direct internet connection) then you can configure the update interval to suit your needs. The default setting that comes with a new installation of MetaDefender Core or MetaDefender Kiosk is every 4 hours (once per day).

If you are using manual updates (aka offline updates) the frequency is controlled by how often you download and apply the offline update package from OPSWAT.

This article pertains to MetaDefender Core v4


This article was last updated on 2019-10-06


VM

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 accurate functioning of the 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 2019-07-26

VM

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.

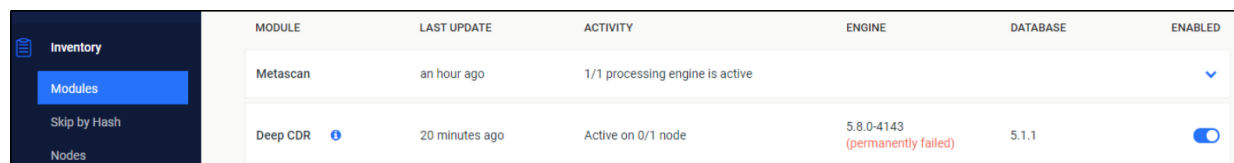
This article applies to MetaDefender Core v4

This article was last updated on 2019-08-19

VM

What should I do if an engine is in "failed" or "permanently failed" status?

Sometimes, during the engines downloading/deployment process, some of them may remain in **"failed"** or **"permanently failed"** status.



The screenshot shows the 'Inventory' page with a sidebar on the left containing 'Inventory', 'Modules', 'Skip by Hash', and 'Nodes'. The main content area is a table with columns: MODULE, LAST UPDATE, ACTIVITY, ENGINE, DATABASE, and ENABLED. The table contains two rows: 'Metascan' and 'Deep CDR'. The 'Deep CDR' row shows a status of 'permanently failed' in red text.

MODULE	LAST UPDATE	ACTIVITY	ENGINE	DATABASE	ENABLED
Metascan	an hour ago	1/1 processing engine is active			<input type="checkbox"/>
Deep CDR	20 minutes ago	Active on 0/1 node	5.8.0-4143 (permanently failed)	5.1.1	<input checked="" type="checkbox"/>

In this case, you can do the following:

- Make sure your system adheres to our [system requirements](#) (check the engine "Third Party Dependencies" section) .
- Go to Inventory → 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 only engine that 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 → Modules page.
- Try executing an engine clean-up by [following this KB](#).
- Starting mid-April 2020 we are going to gradually release each module with a new compiler, beginning with CDR 5.8 engine.

- Make sure that VC Redist C++ 2017 is installed on your system in order for the engines to deploy successfully.
- We recommend installing both the 32bit: https://aka.ms/vs/16/release/vc_redist.x86.exe and the 64bit: https://aka.ms/vs/16/release/vc_redist.x64.exe versions (No downtime required).
After the dependency install, please disable/re-enable the affected engine and it should deploy successfully (become green)
- If for some reason you can't install VC redist C++ 2017 until the release of CDR 5.8, please check the solution by [following this CDR KB](#).

If you have followed all of these steps and your engines are still unusable, please see [how to create a support package](#), login into [OPSWAT Portal](#) and open a ticket with us, having the support package attached.

This article applies to MetaDefender Core v4

This article was last updated on 2020-03-27

VM

What temporary folder do Custom Engines use ?

At the moment, there are 6 Custom Engines which use C:\Windows\temp as temporary folder, instead of the Metadefender Core folder:

- Filseclab
- Huorong
- MSE
- Windows Defender
- Netgate
- Systweak

This article applies to MetaDefender Core v4

This article was last updated on 2019-10-17

VM

Where can I submit false positives detected by MetaDefender Core v4?

Below is a list of addresses where you can send false positives detected by MetaDefender Core V4:

AegisLab

Email: <https://www.aegislab.com/reportfp>

AhnLab

Email 1: v3sos@ahnlab.com

Email 2: e-support@ahnlab.com

Antiy

Email: submit@antiy.com

Avira AntiVir

Submission: <https://www.avira.com/en/analysis/submit>

BitDefender

Submission: <http://www.bitdefender.com/submit>

Email: oemsamples@bitdefender.com

ClamAV

Submission: <https://www.clamav.net/reports/fp>

Comodo

Email: <https://www.comodo.com/home/internet-security/submit.php>

Cyren / F-PROT

Submission: <https://kb.cyren.com/av-support/?/Tickets/Submit/RenderForm/7>

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

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: windexend@submit.microsoft.com

Submission: <https://www.microsoft.com/security/portal/submission/submit.aspx>

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>

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: support-en@anti-virus.by

Xvirus

Email: samples@xvirus.net

Submission: <https://xvirus.net/submit>

Zillya

Email: virus@zillya.com

Submission: <https://zillya.com/support>

Webroot SMD

Email: support@brightcloud.com

This article applies to MetaDefender Core v4

This article was last updated on 2020-07-09

VM

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, CAB, ARJ, LHA, LZH, RPM, DEB, LZMA, WIM, DMG, XAR, MSM, SFX, XZ, VDI, VHD, CPIO, HFS, APK, GZ, MSI, TAZ, TGZ, TBZ, BZ2, VIB, AR, ALZ, TSE, TSEC, TSEZ, ACE. Metadefender Core can also extract self-extracting archives created by both 7zip, WinRAR, PKZIP, IExpress
- Microsoft Office Documents (e.g., DOCX files) are detected as archive files by default

- Email/Calendar files (e.g., EML, MSG, ICS) are extracted to scan header, body, attachments
- For more information, please see the screenshot below:

The screenshot displays the configuration page for the 'ARCHIVE' feature in MetaDefender Core. The page has a navigation bar with 'ARCHIVE', 'SCAN', 'DEEP CDR', and 'PROACTIVE DLP' tabs, and a 'MORE' dropdown menu. The 'ARCHIVE' tab is selected. The settings are as follows:

- ENABLE ARCHIVE HANDLING** ⓘ
- MAX RECURSION LEVEL** ⓘ: 5
- MAX NUMBER OF FILES EXTRACTED** ⓘ: 200
- MAX TOTAL SIZE OF EXTRACTED FILES [IN MEGABYTES]** ⓘ: 200
- ENABLE SCAN OF ORIGINAL UNEXTRACTED ARCHIVE** ⓘ
- ENABLE EXTRACTION OF OFFICE DOCUMENTS** ⓘ
- TIMEOUT FOR ARCHIVE ANALYSIS [IN MINUTES]**: 3

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 2019-09-12

VM

Why does the deployment ID appear NULL In MetaDefender Core v4?

MetaDefender Core's license activation/trial key request depends on the deployment ID. The deployment ID can be NULL if MetaDefender core couldn't fetch the required HW/OS related information. Most of the time, this issue is caused by not having a default route set up. To see if you already have a default route or if you want to set up one on your own, please click the link below if you are running MetaDefender Core on Windows:

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/route_ws2008

To see the default route and/or your network settings under a Linux distribution, please consult your distribution's administrator guide.

Note: OPSWAT recommends enabling at least one network card when using MetaDefender Core v4, even if it's not linked to any network.

This article pertains to MetaDefender Core v4

This product was last updated on 2019-12-23

VM

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 Modules(Technologies) tab in the management console: from the sidebar menu, go to Inventory → Modules(Technologies).

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 (the specified number should be less than or equal to your free license slots for this product)

To check the status of the Data Sanitization engine, you can go to Inventory → Modules (Technologies).

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 2019-10-06

VM

Why is the scan stuck in "processing" state on WebScan UI, when the Core Processing History shows that it is already finished?

If a file is submitted for scan via webUI, the webUI will make 999 queries as part of the polling process. If the file analysis takes longer than that (progress percentage hasn't reached 100), the webUI will stop polling and it will look like it has frozen.

A webpage refresh will reset the query counter and the webUI will continue fetching results.

This article applies to MetaDefender Core v4

This article was last updated on 2019-12-23

VM

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 2019-10-06

VM