OPSWAT.

MetaDefender

MetaDefender Client 4.1.22

Table of Contents

About This Guide

Welcome to the MetaDefender Client user guide. This guide is intended to provide the information you need to:

- Install, configure, and manage MetaDefender Client.
- Learn about new features, updated features, and bug fixes on each MetaDefender Client Release (i.e. each product version's release notes)
- Learn about frequently asked questions and additional concepts through our library of knowledge base articles

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

Key Features of MetaDefender Client

- File scanning and processing with MetaDefender Core workflows, including:
  - Multi-scanning for malware with more than 30 leading anti-malware engines
  - Heuristic analysis to detect more unknown and targeted attacks
  - Vulnerability Engine
  - File Type Verification
  - Archive Extraction
- Enumeration and scanning of running processes and loaded libraries
- Blocking of USB & CD/DVD media until they have been scanned by MetaDefender and found clean

Supported Operating Systems

MetaDefender Client is only supported on the following operating systems. Both 32 and 64 bit operating systems are supported.

- Windows 7
    - Requires Service Pack 1 and Microsoft updates KB2533623 and KB3033929
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server Small Business Server standard FE (version: 2011 Standard)
    - Requires KB2533623 installed http://go.microsoft.com/fwlink/p/?linkid=217865
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

1. MetaDefender Client

The MetaDefender Client can be installed on endpoints and run in the background, monitoring for any USB storage devices or discs that are inserted into the system. When a removable device is detected, MetaDefender Client will block access to that device and prompt the user to initiate an action. The user can do the below actions on the removable device:

- **Copy files from drive** - Allows users to specify files, which if found clean will be copied to the "MetaDefender" folder on the desktop. If the file is suspicious, it will not be copied.
- **Unblock drive** - Scans the entire drive, if the drive is found clean then it unlocks the drive. Once unblocked, the drive should work as normal, it is fully accessible from Windows Explorer.
- **Copy files to drive** - Allows users to copy files to a drive without scanning it with MetaDefender. This enables users to skip the scanning process if read access to the USB is not required.

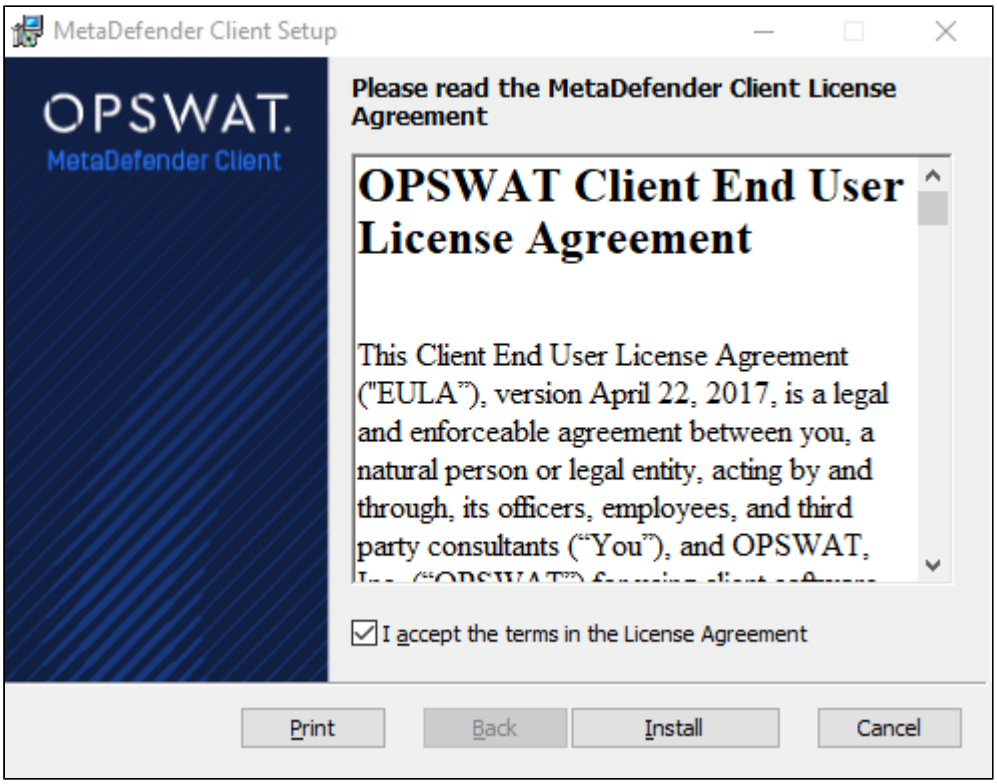
The MetaDefender Client also supports users scan their device with options:

- Running processes and associated libraries
- Boot Records
- System Drives
- USB
- CD/DVD

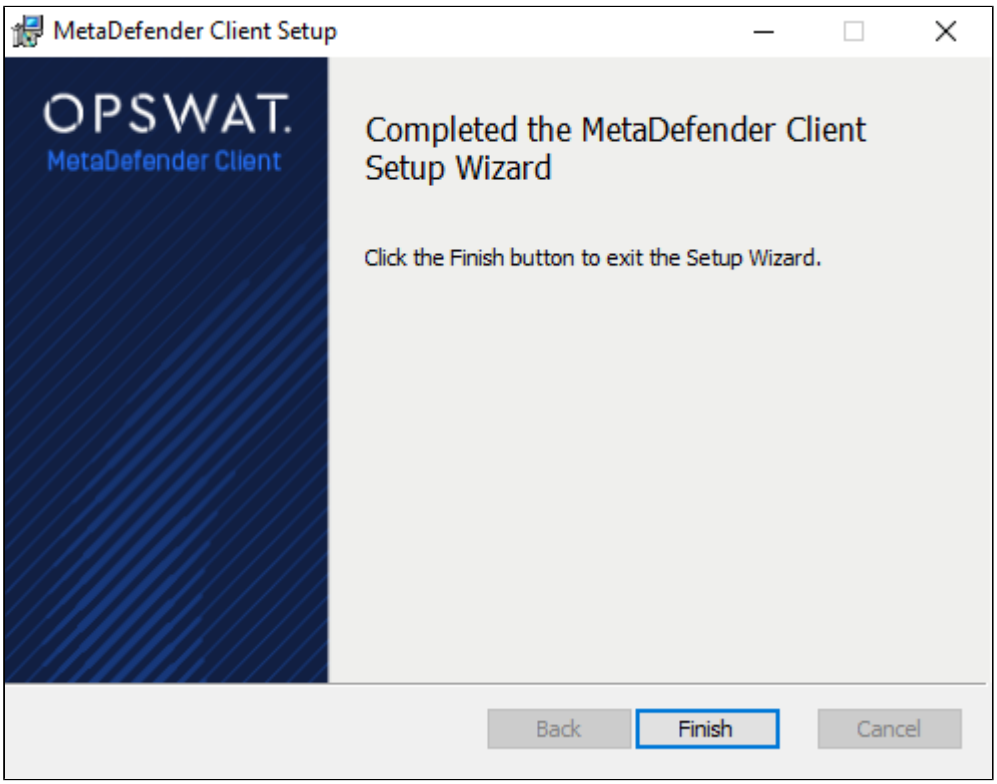
1.1 Install using the Install Wizard

1. Launch the installer by double-clicking on the MSI file

2. Accept the End User License Agreement



3. After the installation has completed, click the 'Finish' button



4. Confirm that the MetaDefender Client is running by looking for the icon in the system tray.

1.2 Install using the Command Line

The following command line options are available with the MetaDefender Premium Client installation package.

Command	Description	Example Usage
/i	Install the MetaDefender Client	msiexec /i MetaDefender-Client.msi
/x	Uninstall the MetaDefender Client	msiexec /x MetaDefender-Client.msi
/q	Run the MetaDefender Client installation silently	msiexec /i MetaDefender-Client.msi /q
/L	Create an installation log file	msiexec /i MetaDefender-Client.msi /q /L c:\clientinstall.log
URL=<CM url>	Central Management address	msiexec /i MetaDefender-Client.msi /q URL=127.0.0.1:8018
GROUP=<CM group>	Group from Central Management (optional)	msiexec /i MetaDefender-Client.msi /q URL=127.0.0.1:8018 GROUP=clients

Client Distribution

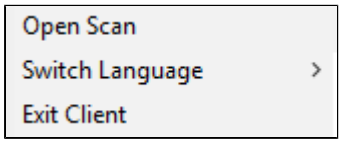
To distribute & manage Clients among multiple endpoints with OPSWAT Central Management v5, we recommend using Active Directory to push out the Clients and install using URL and GROUP keys.

1.3 Using the MetaDefender Client

Launching MetaDefender Client

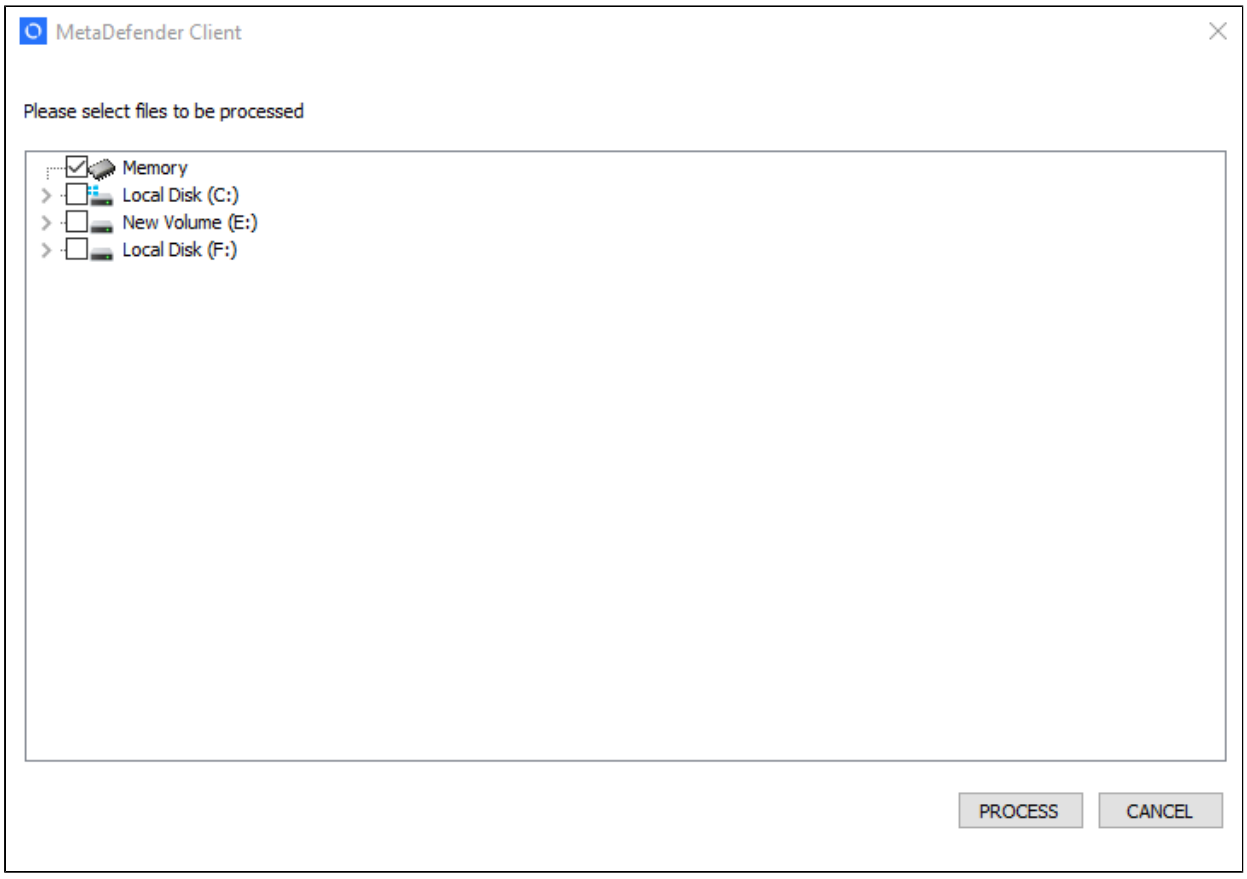
When installed, the Client will run as a persistent service.
Access to the Client is available via the system tray.
Left-clicking the system tray icon will bring up the Client UI.

Right-clicking the system tray icon provides multiple options:



Open Scan

Opens a browse window to quickly select files from the system to be processed.



Switch Language

Provides the ability to switch the language of the text displayed on the Client UI.
Restarting the "MDClient" service or exiting the Client will allow for the switch to take effect.
If a desired language is not supported, please contact OPSWAT to request support.

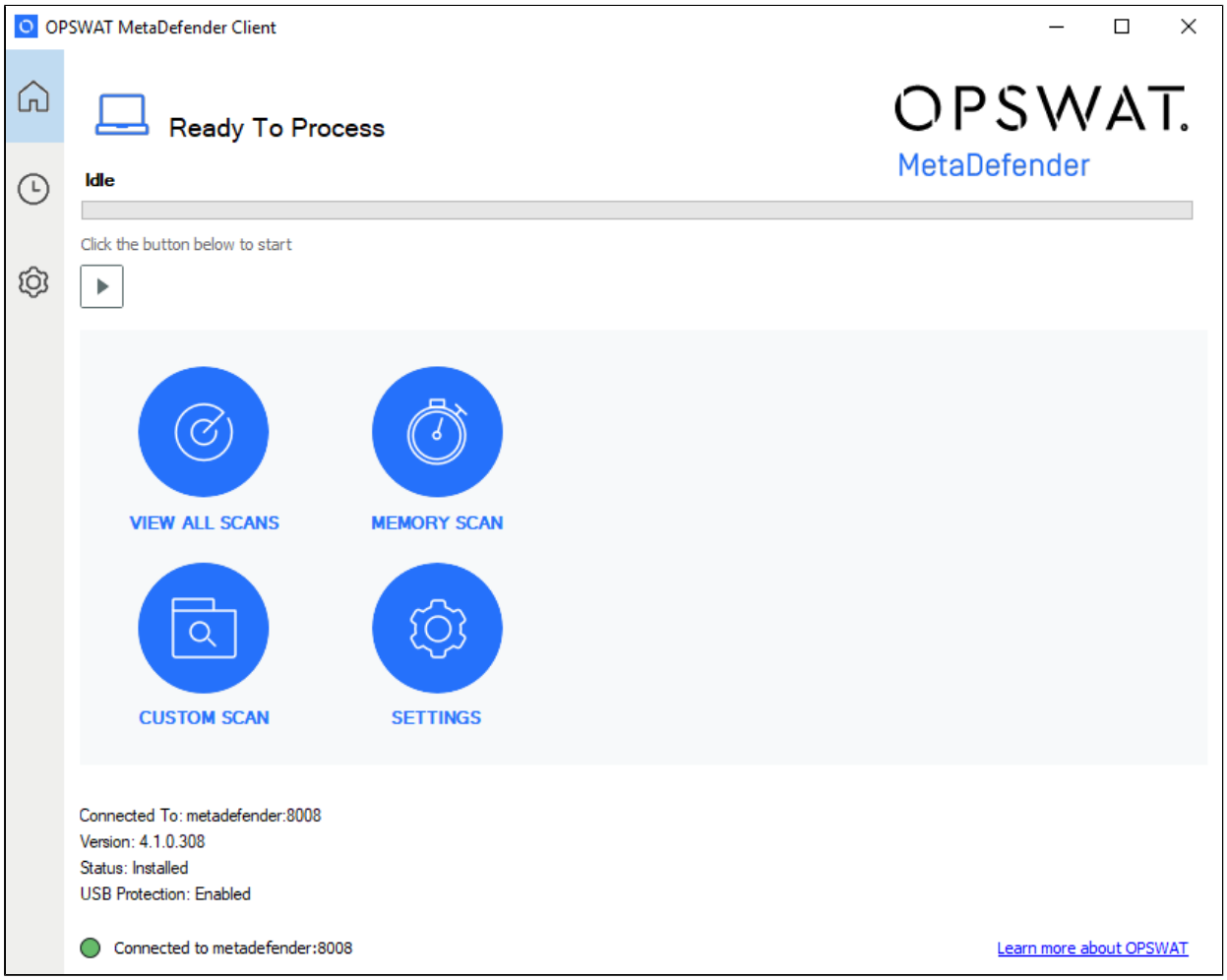
Exit Client

Allows the ability to restart the Client UI.

The following sections give an overview of the end user experience in using the MetaDefender Client UI.

1.3.1 Home Page

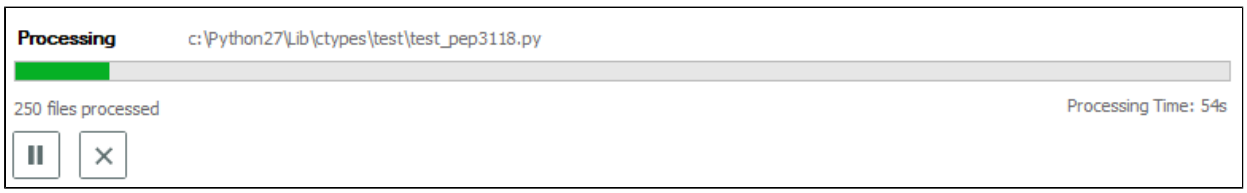
The home page provides quick access options and high level information of the Client status.



Progress Bar

The top of the home screen shows the progress of a current running task, "Idle" if no task is running.
The play icon allows to start a new task to process selected files from the system.

If a current task is running, it can be paused or canceled.



Left Panel

The left panel allows for quick navigation among sections of the Client UI:

- Home
- Tasks

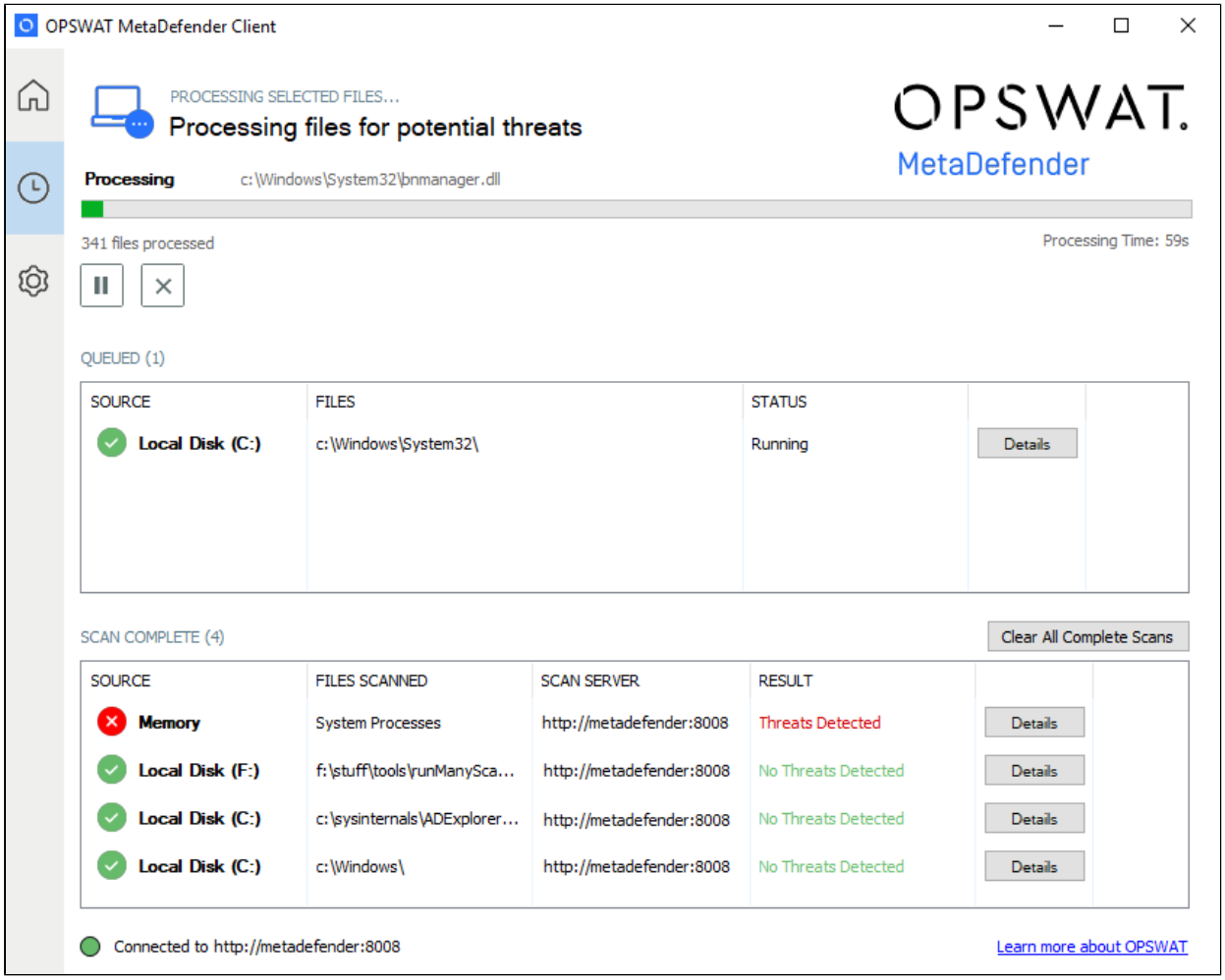
- Settings

Quick Access Options

- View All Scans - navigates to the Tasks page to view all Queued and Completed scan tasks
- Memory Scan - launches a new scan task for all running system processes
- Custom Scan - launches the browse window to start a new task to process selected files from the system
- Settings - navigates to the Settings page to configure the Client

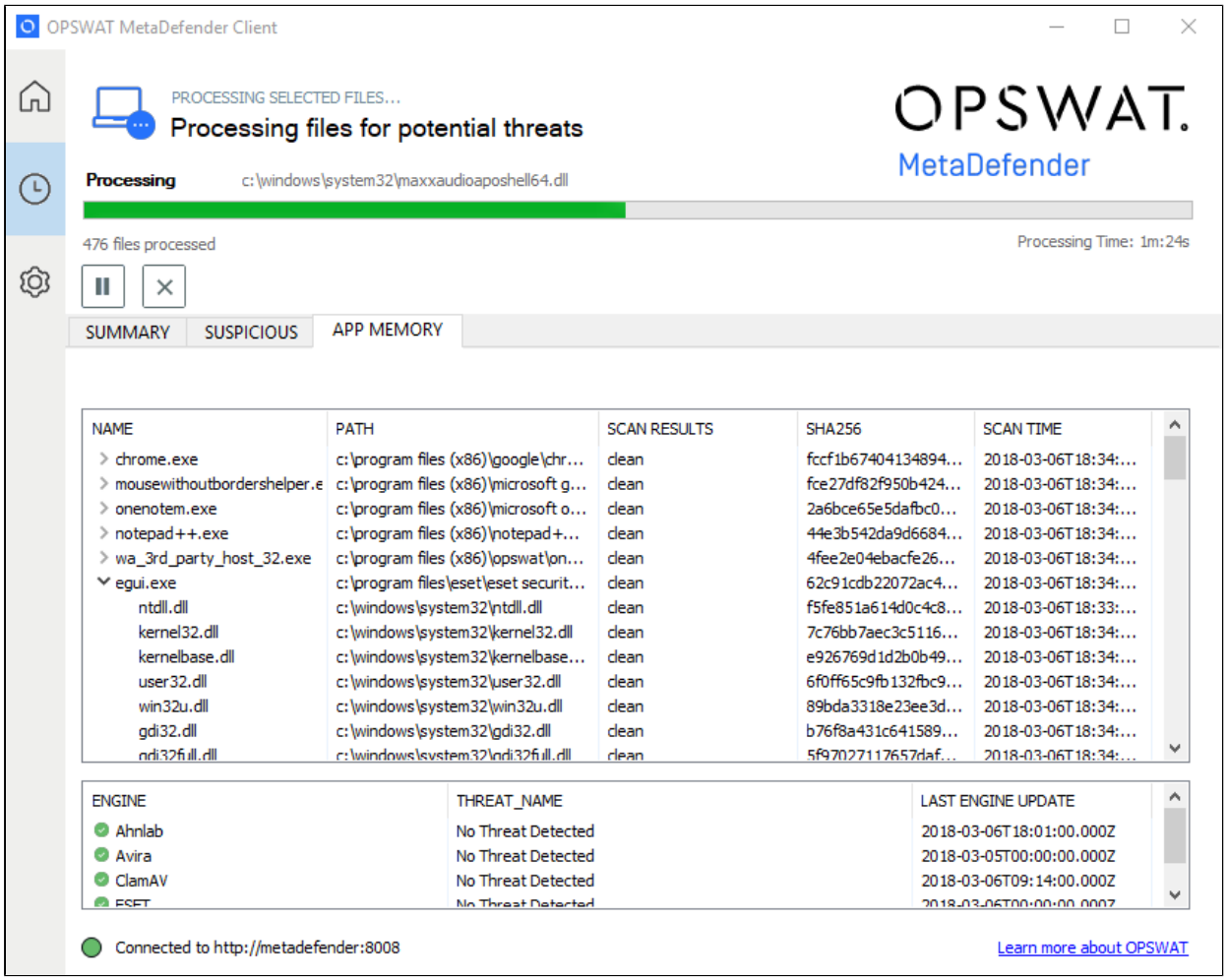
1.3.2 Tasks Page

The tasks page provides visibility of queued and completed scan tasks with the ability to view the details of a specific task.

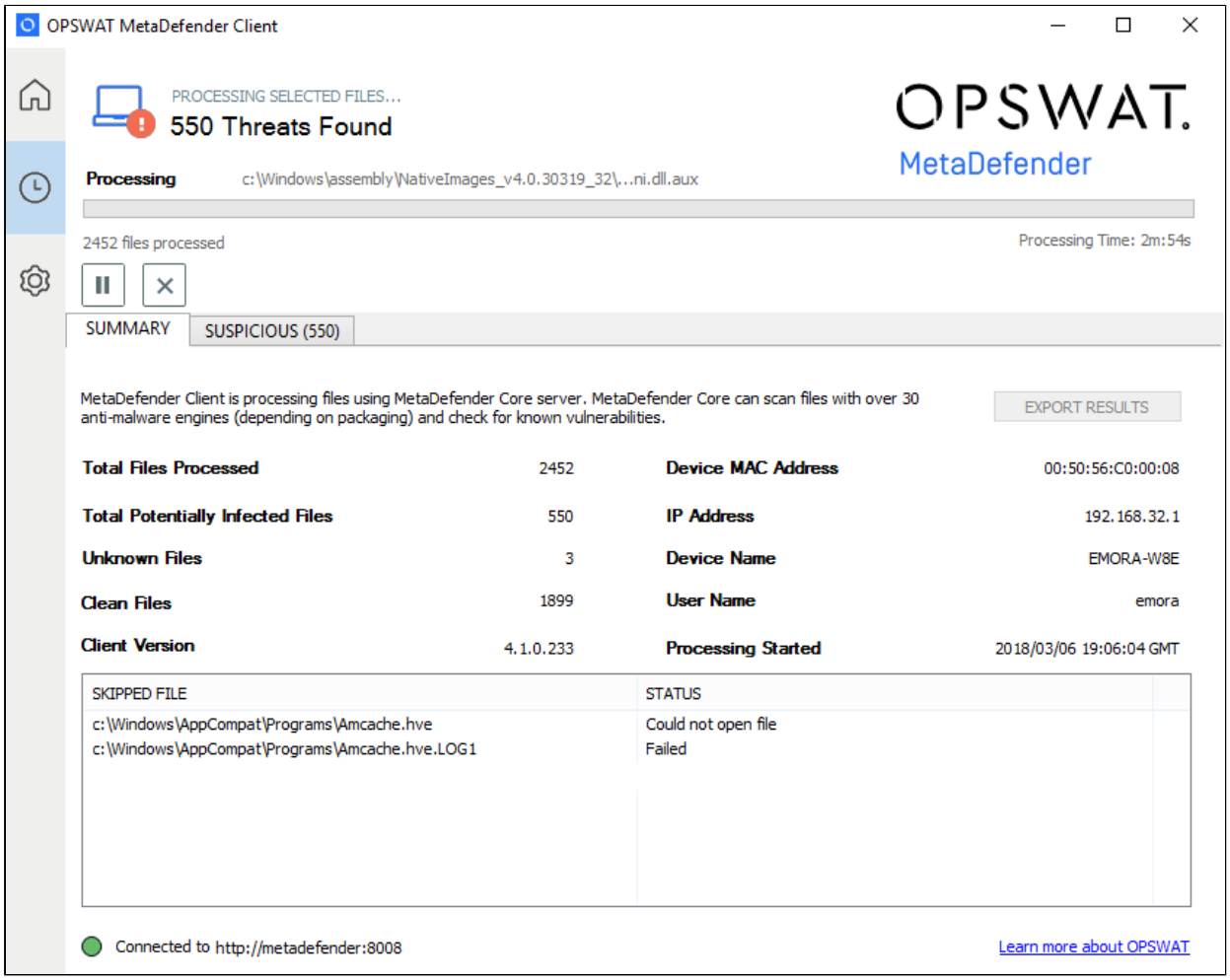


Details

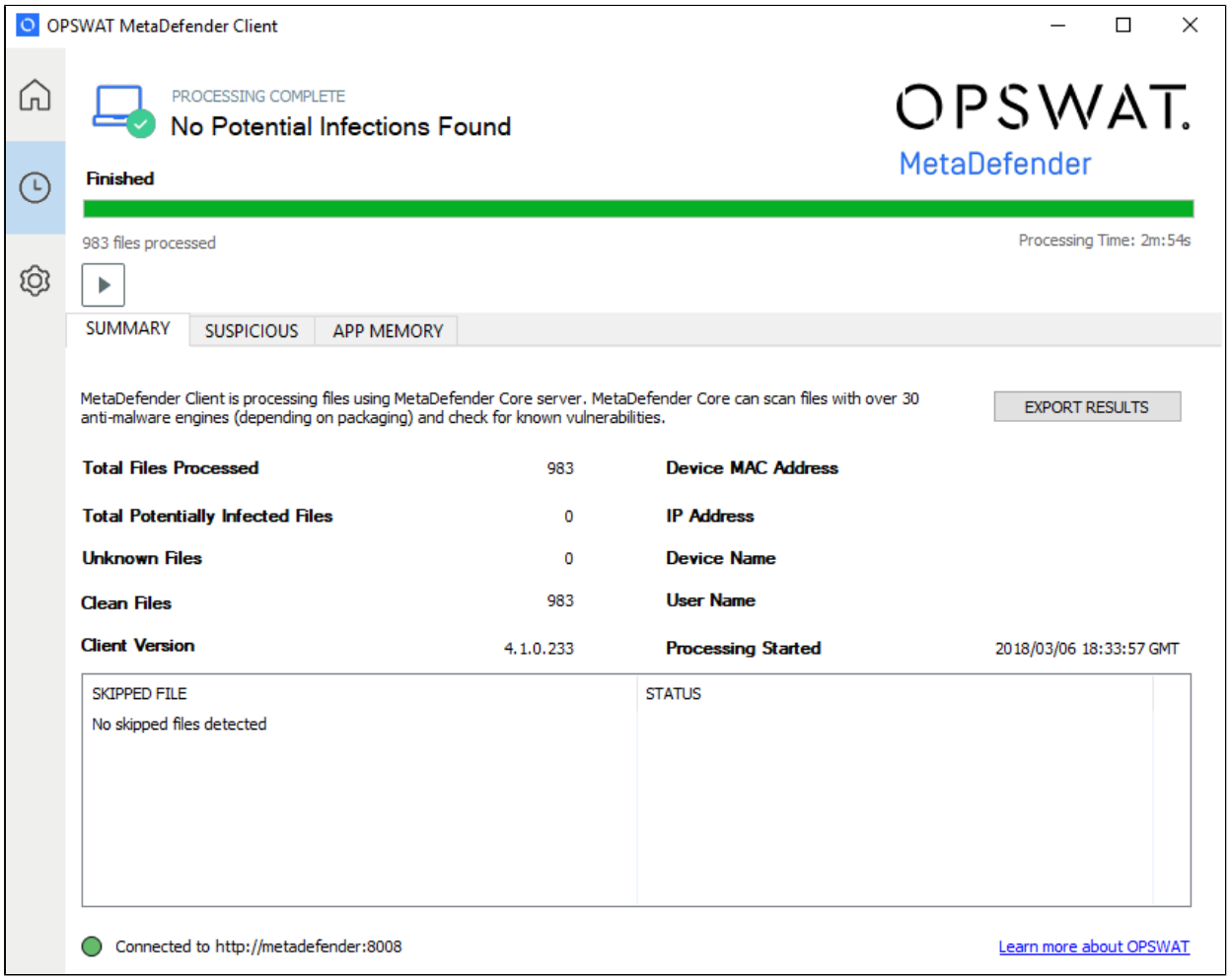
The summary of a currently running or completed task or can be viewed by clicking 'Details' for the specific task.
If a Memory scan task was chosen, an App Memory tab will list the current running processes. Each process can be expanded to show the associated loaded libraries and their scan results as well.



Any issues with files will be listed in the Summary tab within the Skipped File window.



When the scan has finished the overall result will be shown at the top of the Client UI.

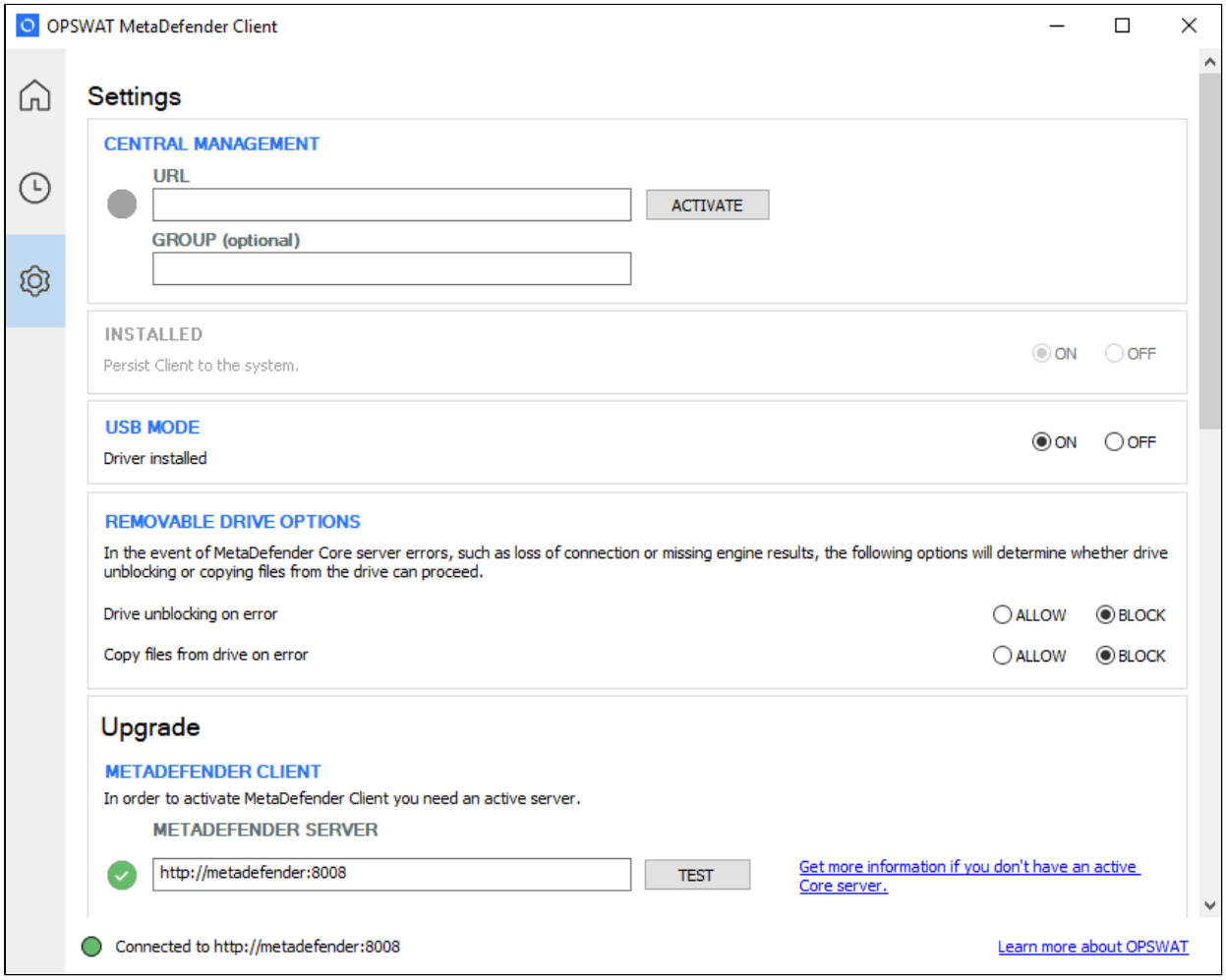


Exporting Scan Report

Scan reports can be saved in either text, PDF, or CSV format by clicking on the 'Export Results' button on the top right of the Summary tab.

1.3.3 Settings Page

The settings page allows the ability to configure the Client.



Settings	Description
Central Management URL	URL of the Central Management
Central Management Group	Specific group in Central Management that the Client should be included in
Installed	Ensures the Client will be installed on the system and running as a service
USB Mode	Enables blocking of inserted USB and CD/DVD devices when Client is installed
Drive unblocking on error	

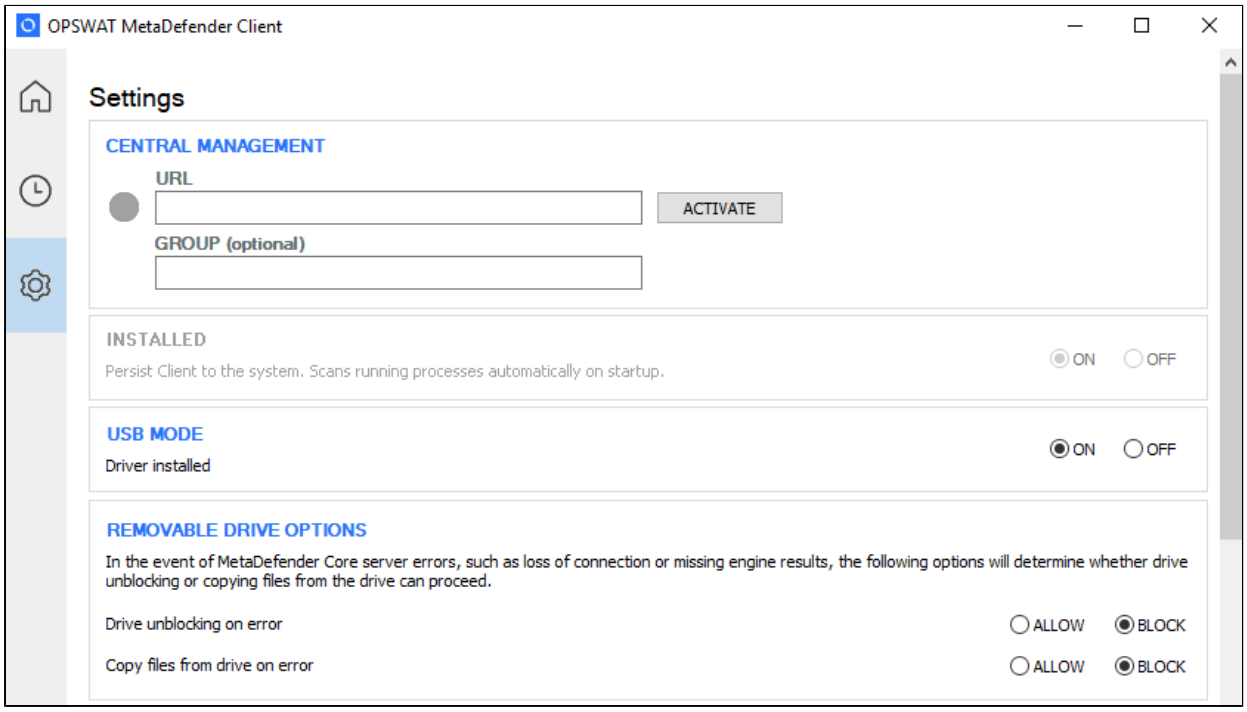
Settings	Description
	If USB Mode is enabled, this specifies whether Client allows or blocks a drive when a MetaDefender error occurs
Copy files from drive on error	If USB Mode is enabled, this specifies whether Client allows or blocks copying files from a drive when a MetaDefender error occurs
MetaDefender Server	URL of the MetaDefender used to process files
User Agent	The user agent Client provides to MetaDefender for rule/workflow security restrictions
Rule	Specifies the security rule Client should use for MetaDefender v4
Workflow	Specifies the workflow profile Client should use for MetaDefender v3
API Key	API Key used for processing files with MetaDefender v3 (if one is set)
Disable Hash Checking	Disables attempting to check for file's hash result before processing
MetaDefender.com API Key	API Key used for processing files with MetaDefender Cloud
Upload allowed/blocked files to MetaDefender Vault	Enables uploading allowed or blocked files to MetaDefender Vault after processing

Settings	Description
	Note: files will be uploaded within a zip named with the upload timestamp
MetaDefender Vault URL	URL to the MetaDefender Vault to upload files
MetaDefender Vault Authentication Token	MetaDefender Vault administrator token used to allow files to be uploaded
Always upload to a Vault guest account	If enabled, a guest user id will be generated to retrieve files with If disabled, files will be uploaded as the logged in user ***Note: if any upload fails, files will be uploaded as a guest user***
Use File Sanitization	With data sanitization enabled in MetaDefender, this will provide the option to download available sanitized versions of files
Copy only sanitized file, do not copy original	When copying files to the system, only the available sanitized version will be copied over
Copy from media location	Specifies the location where clean files will be copied

1.3.4 Device Protection

Enable Device Protection

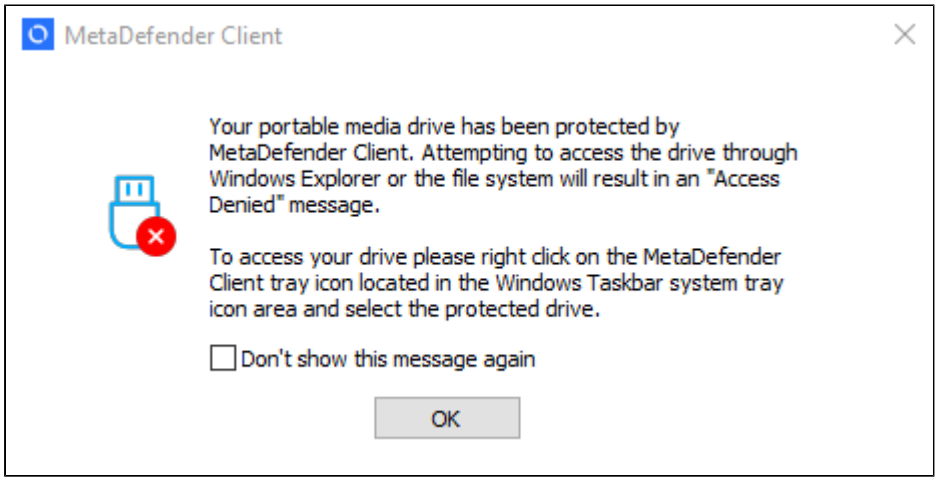
The MetaDefender Client device protection can be enabled by going to Settings → USB Mode → Driver installed → On.
This can only be enabled after the Client is installed.

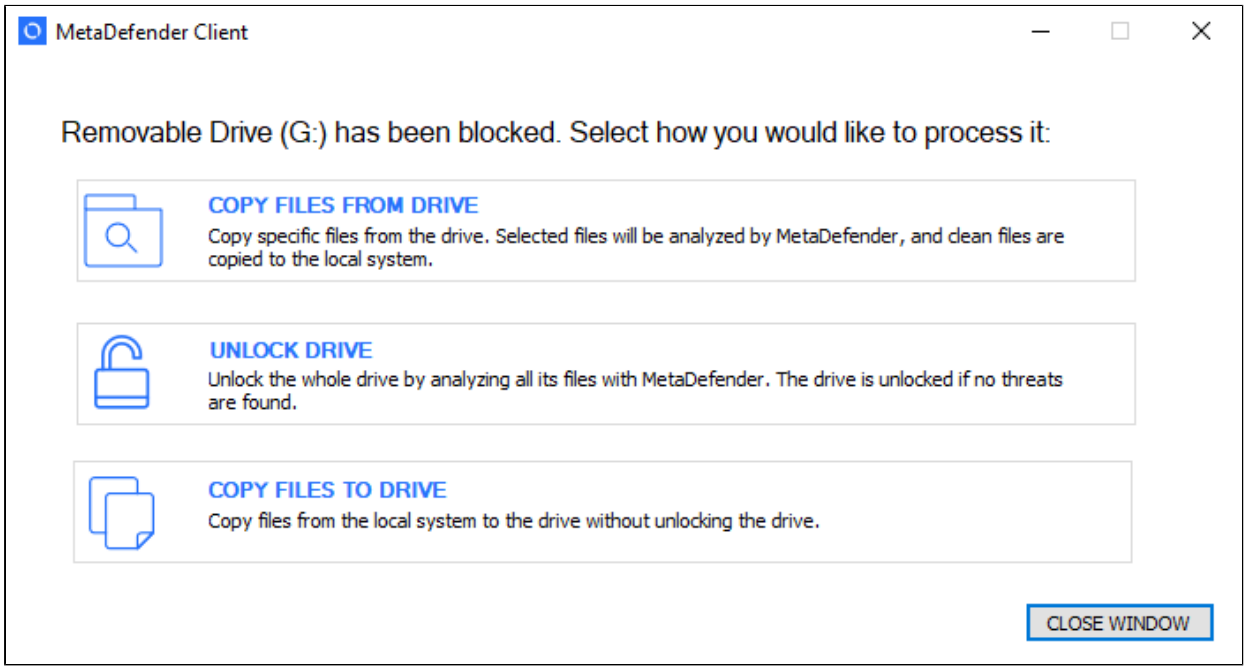


Using Device Protection

Once installed, the MetaDefender Client will run as a Windows service, and will monitor the endpoint for any insertion of USB media or CD/DVD discs. Access to inserted devices will be blocked until they have been scanned by MetaDefender. The only way the device can be used without going through the MetaDefender Client is by uninstalling the MetaDefender Client.

When a USB or disc is inserted, MetaDefender Client will prompt the user to decide how to handle the device.

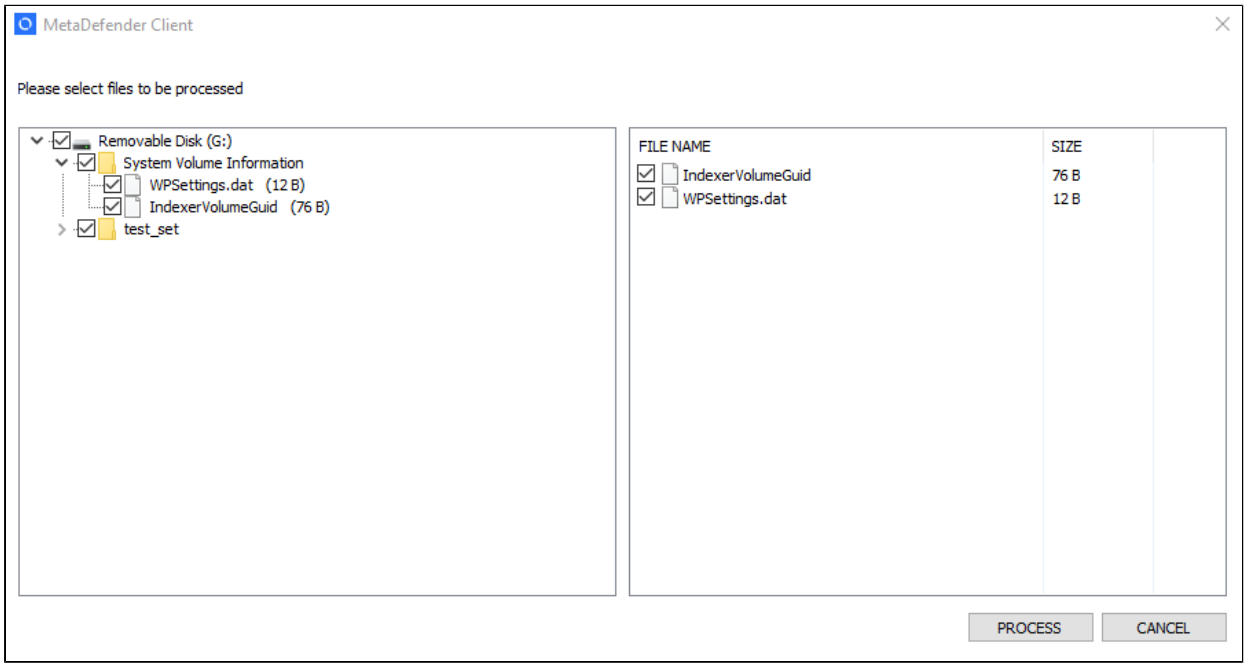




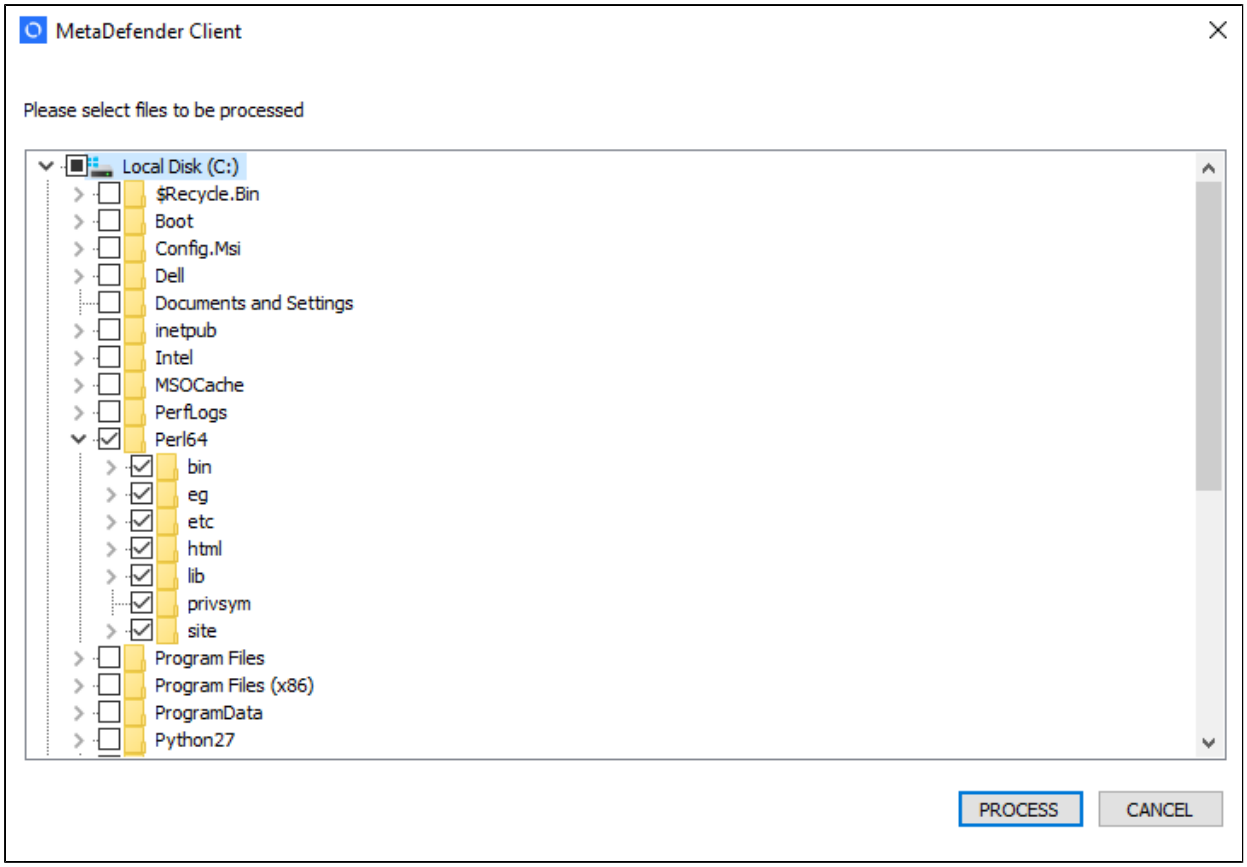
The user can select one of three options

1. Copy files from drive - The user can select which files on the drive they would like to scan
2. Unlock drive - The entire drive will be scanned
3. Copy files to drive - The user can select which files to copy to the USB drive without scanning

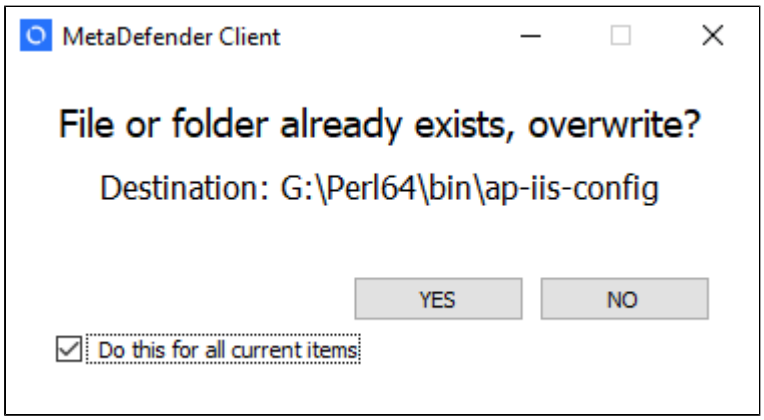
If the user chooses the 'Copy files from drive' option, they will be able to select which files on the media are to be scanned.



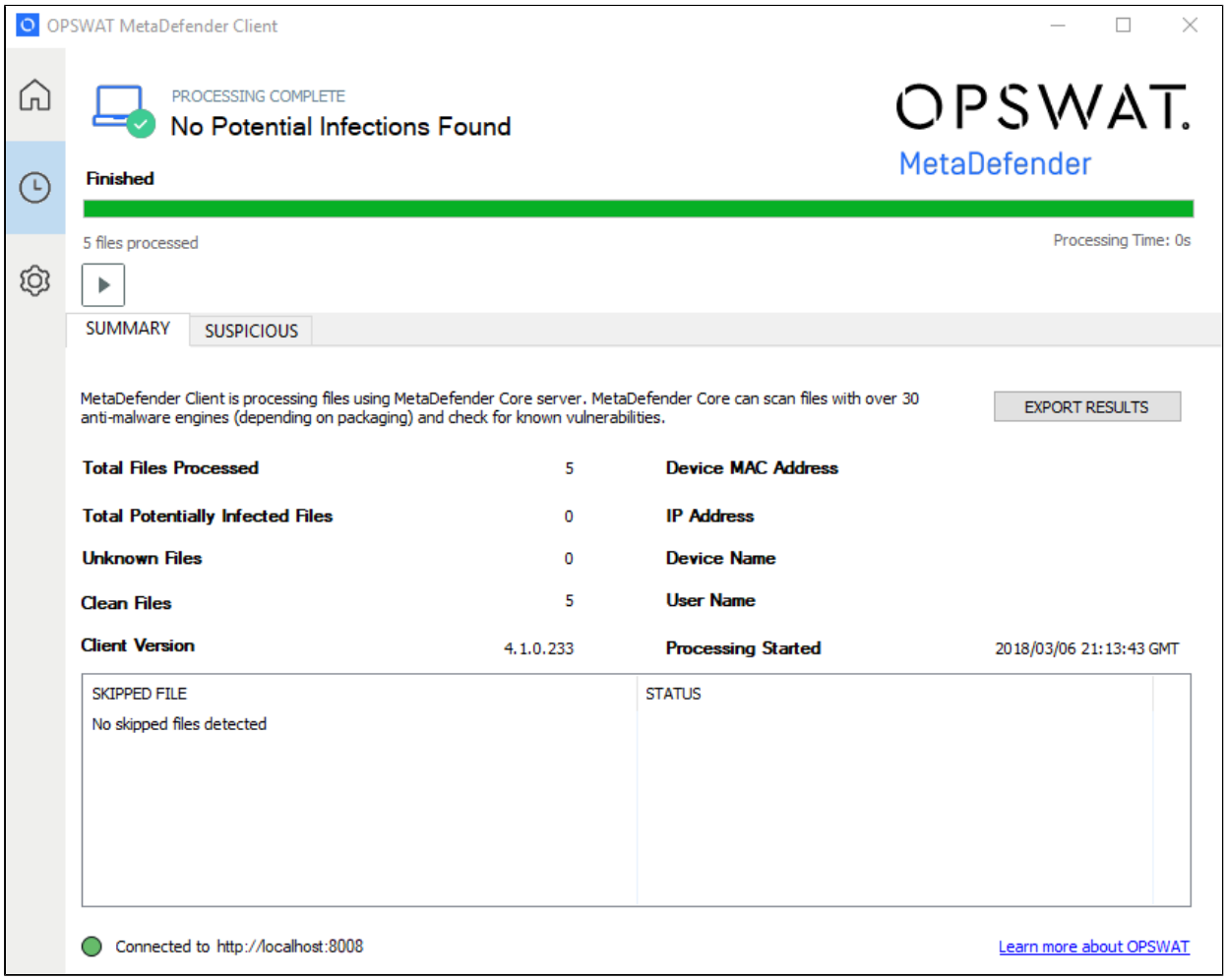
If the user chooses the 'Copy files to drive' option, they will be able to select which files on their system should be copied to the device. If this option is selected, the drive will not be scanned and the user will not have read access to the drive.



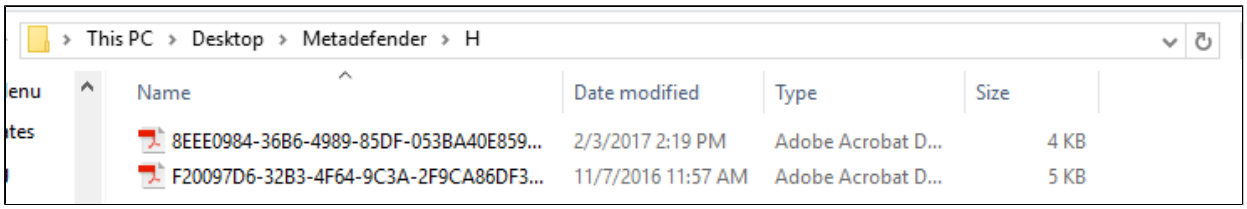
If a file already exists on the USB, the user will be prompted to choose whether or not they want to overwrite the file.



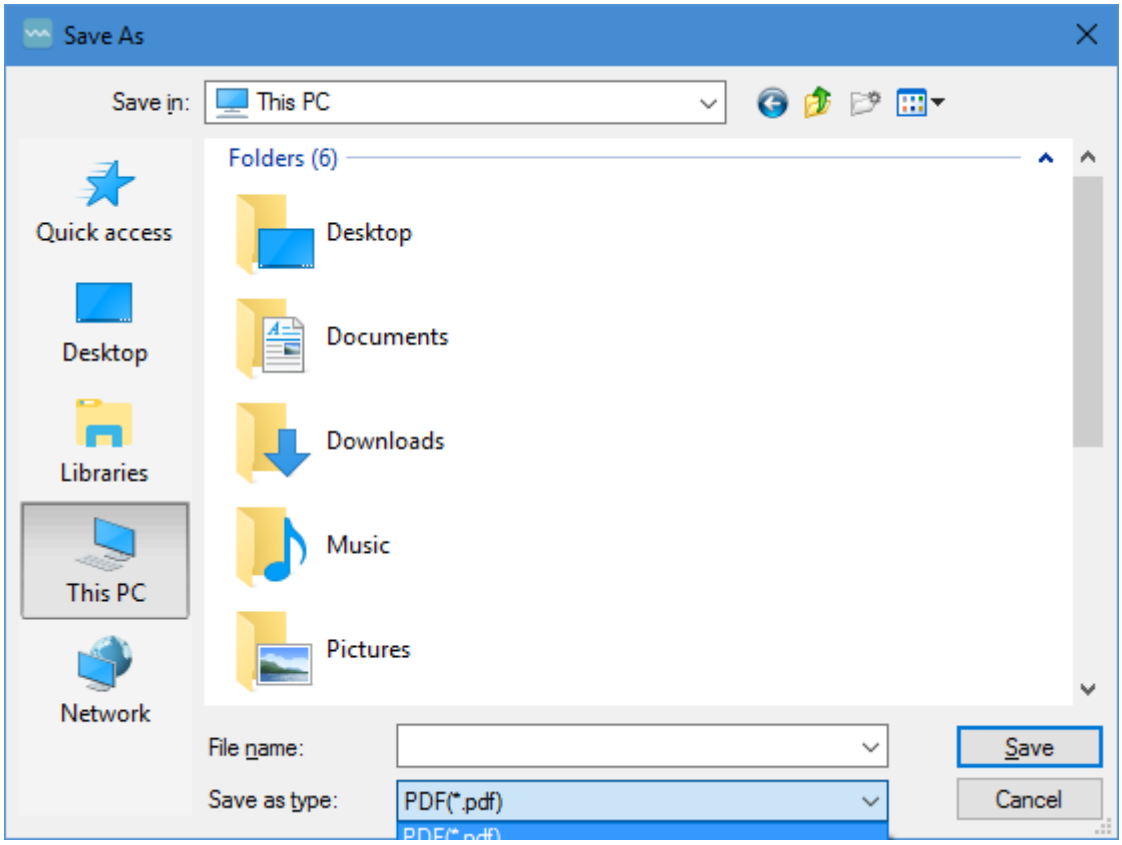
After all of the files have been processed a summary will be displayed to the user. If the 'Unlock drive' option was chosen and no threats were found, the drive will become accessible to the user.



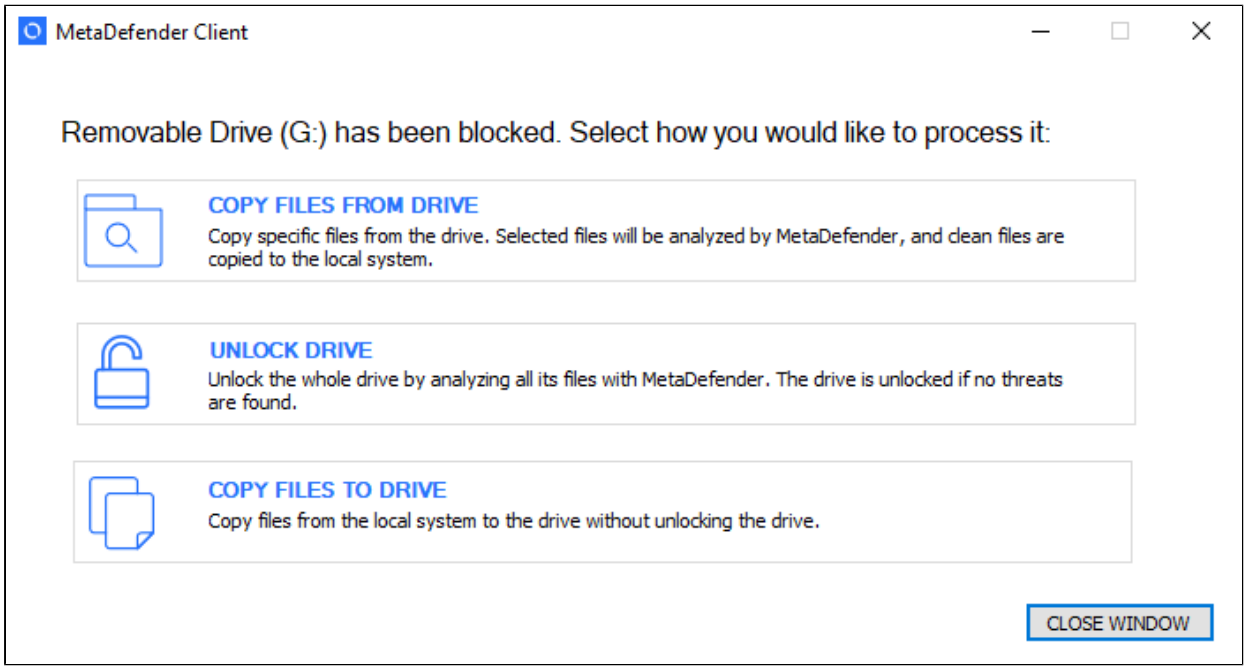
The user can choose to go to the directory of files that were scanned. If they chose the 'Unlock drive' option this will be the drive itself, but if they chose the "Copy files from drive' option this will be a directory on their desktop where files were copied.



They can also choose to save a report of the scan session in PDF, text, or CSV format.



1.3.5 Media Manifest



To utilize the Media Manifest feature the user should select the "Unlock drive" option. Once the client begins scanning the removable media, it performs the following steps:

1. Looks for an OPSWAT Media Manifest file on the removable media
2. Checks to make sure the Certificate that is signing the Media Manifest is trusted by the client
3. Checks each file on the removable media against the Media Manifest to make sure it has not been modified
    a. If a file has not been modified and the Media Manifest states it is allowed, then the file is not uploaded for scanning, and is considered clean
    b. If a file has not been modified and the Media Manifest states it is blocked, then the file is uploaded for scanning
4. Any files found that have been added to the removable media since the generation of the Media Manifest are scanned against the configured server

Note: The client must be provided with the certificates it should consider trusted. The client will look in the following folders to locate all trusted certificates.

1. %ALLUSERSPROFILE%\OPSWAT\.ssh\
2. %USERPROFILE%\.ssh\
3. %APPDATA%\.ssh\
4. %APPDATA%\OPSWAT\.ssh\

If the trusted certificate is not in any of the directories above, the client can also verify certificate trust if the root Certificate Authority certificate is installed. OPSWAT recommends automating the deployment and installation of trusted certificates to the client using an AD Push or similar technique. A Certificate Authority certificate can also be installed for an individual client by copying the .crt file over, right clicking on it, and selecting "Install Certificate."

1.4 Configuring through the config file

The MetaDefender Premium Client can be configured by updating the %appdata% \MetaDefenderApp\client_config.json file after MetaDefender Premium Client installation. Changes will be applied the next time the MetaDefender Premium Client is started.

Note: Take care in modifying the client_config.json file. If there are errors in the file, the MetaDefender Premium Client may not start.

Key	Value Type	JSON Key Pair Example	Default Value
servers			

Key	Value Type	JSON Key Pair Example	Default Value

	JSON array	"servers": [
		{
		"url": "http://<ip or dns>:8008",
		"apikey": "1234"
		}
		]
			"server": [
			{
			"url": "http://me
			8008",
			"apikey": ""
			}
			]

user_agent	string	"user_agent":"md_client"	"MDClient"
rule	string	"rule":"client"	" "
workflow	string	"workflow":"client"	" "
disable_hash_check	boolean	"disable_hash_check":false	false

Key	Value Type	JSON Key Pair Example	Default Value
allow_exit	boolean	"allow_exit":true	true
allow_user_selection	boolean	"allow_user_selection":true	false
scan_type	string array	"scan_type":["physical", "process"]	["removable", "p
log_file	file path	"log_file":""	"%AppData% \\MetaDefende

Key	Value Type	JSON Key Pair Example	Default Value
force_usb	boolean	"force_usb":true	false
copy_clean_location	file path	"copy_clean_location":""	"%USERPROF \\Desktop\\Meta
copy_to_maintain_dir_structure	boolean	"copy_to_maintain_dir_structure": false	false
hide_usb_warning	boolean	"hide_usb_warning":false	false
unblock_on_error	boolean	"unblock_on_error":false	false
copy_on_error	boolean	"copy_on_error":false	false

Key	Value Type	JSON Key Pair Example	Default Value
hide_drive_unlock	boolean	"hide_drive_unlock":false	false
hide_drive_browse	boolean	"hide_drive_browse":false	false
hide_drive_copy	boolean	"hide_drive_copy":false	false
max_file_size	integer	"max_file_size":52428800	1000000 MB

media_manifest.
trust_only_manifest
	boolean	"media_manifest": {
		"trust_only_manifest":false
		}
			false

Key	Value Type	JSON Key Pair Example	Default Value

media_manifest.days_trusted	integer	"media_manifest": {
		"days_trusted":30
		}
			30

pdf_report_dir	string	"pdf_report_dir":"D:\\"	" "
use_file_sanitization	boolean	"use_file_sanitization":true	false
delete_original_sanitized_file	boolean	"delete_original_sanitized_file": true	false

Key	Value Type	JSON Key Pair Example	Default Value
default_language	integer	"default_language":13	9
exclude_engines	string array	"exclude_engines":["engine1", "engine2"]	[ ]

vault	JSON object	"vault": {
		"allowed": {
		"enabled":true,
		"auth_token":"1234",
		"copy_to_url":"http://VaultServer:8000/vault_rest",
		"guest_only" false
		},
			"vault": {
			"allowed": {
			"enabled":false
			"auth_token":""
			"copy_to_url":"
			"guest_only" fa
			},
			"blocked" {

Key	Value Type	JSON Key Pair Example	Default Value

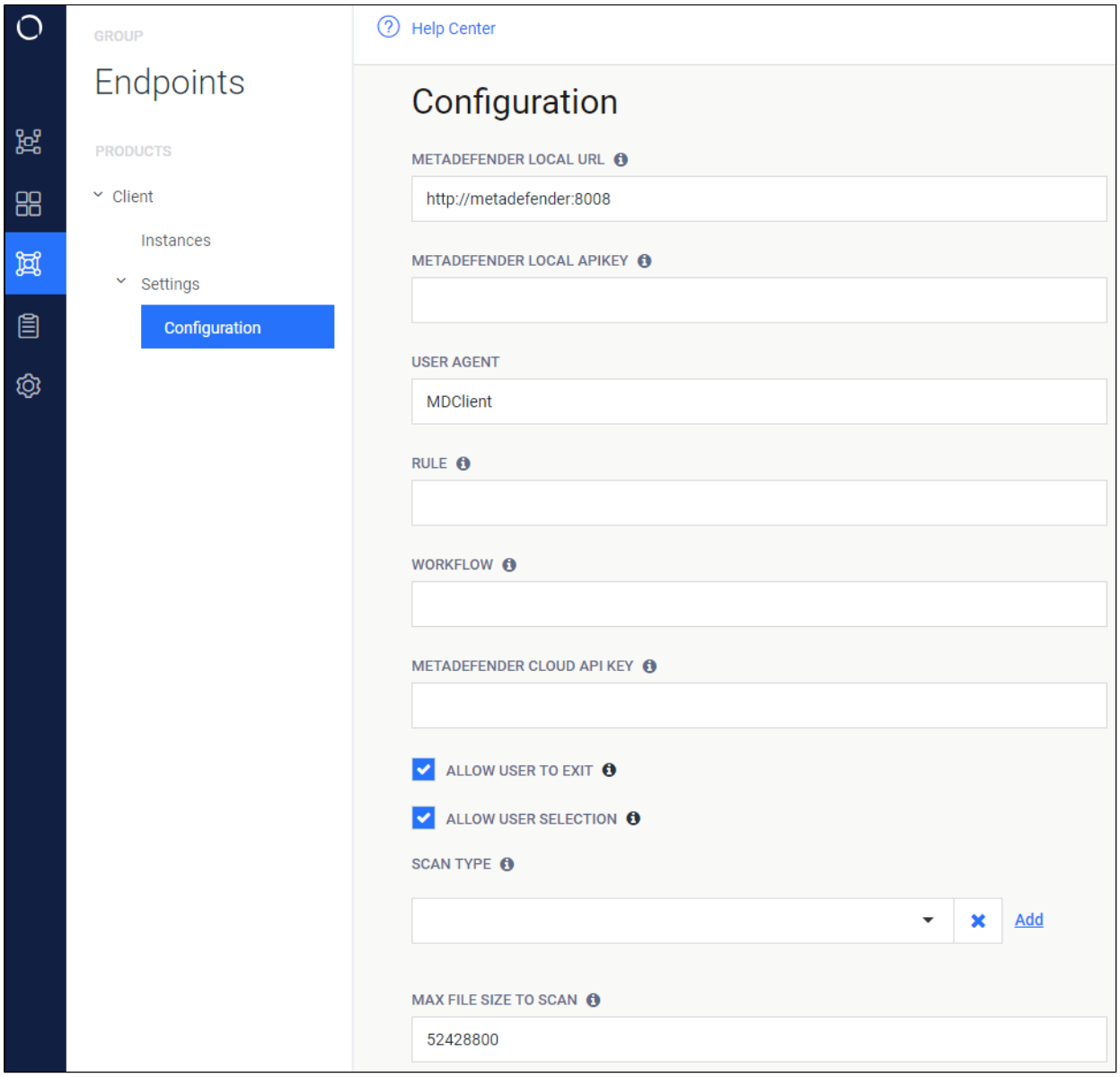
		"blocked" {
		"enabled":false,
		"auth_token":"",
		"copy_to_url":"",
		"guest_only":false
		}
		}
			"enabled":false
			"auth_token": "
			"copy_to_url": "
			"guest_only":fa
			}
			}

1.5 Configuring through Central Management

Multiple MetaDefender Clients can be configured from a Central Management.
Some changes will take effect at the next restart of Client.

To point MetaDefender Client to Central Management either the Client is installed with the Central Management parameters or the settings are set on the Client settings page.
Refer to the Central Management documentation for further details on how to setup managing MetaDefender Clients.

When a Client is centrally managed, the settings will no longer be allowed to be changed on the Client itself, only through Central Management.



Settings	Description
MetaDefender Local URL	URL of the MetaDefender used to process files
MetaDefender Local API Key	API Key used for processing files with MetaDefender v3 (if one is set)
User Agent	The user agent Client provides to MetaDefender for rule/workflow security restrictions
Rule	

Settings	Description
	Specifies the security rule Client should use for MetaDefender v4
Workflow	Specifies the workflow profile Client should use for MetaDefender v3
MetaDefender Cloud API Key	API Key used for processing files with MetaDefender Cloud
Allow User to Exit	Allow the user to exit through the UI
Allow User Selection	Allow the user to select scan type through the UI
Scan type	The type of scan that is performed if "Allow User Selection" is not checked
Max File Size to Scan	The maximum size of the file to process with MetaDefender (in Bytes)
Disable Checking Hash	Never perform hash lookups, always upload files to MetaDefender for processing
Engines to Exclude from Results	Engine(s) to not be included in the final MetaDefender result output This will modify the final allowed/blocked result of a processed file
Log File Location	Path to store the location for an auto-generated log
Enable Media Drive Protection	All USB/CD/DVD media inserted into the endpoint will be blocked and require processing by MetaDefender before use

Settings	Description
Hide Locked Drive Warning	Disable displaying the warning message of a blocked drive upon insertion
Hide Drive Unlock Option	Disallow a user from unlocking a blocked drive
Hide Drive Browse Option	Disallow a user from copying files from a blocked drive to the system
Hide Drive Copy Option	Disallow a user from copying files from the system to a blocked drive
Drive Unblocking on Error	Drive unblocking can proceed in the event of MetaDefender server errors
Copy Files from Drive on Error	Copying files from the drive can proceed in the event of MetaDefender server errors
Copy Clean File Location	The folder to copy clean files to, from the removable media in Browse File mode
Maintain Directory Structure for Copy	Maintain the directory structure of files on the media in the copy to destination
Use File Sanitization	Check for a sanitized copy of the file generated by MetaDefender
Copy Only Sanitized File, Do Not Copy Original	Dictates if the original file will be removed, or keep it alongside the sanitized copy
UI Display Language	Language the UI will be displayed in

Settings	Description
Upload Allowed/Blocked Files to MetaDefender Vault	Allowed/Blocked files will be uploaded to MetaDefender Vault
URL	URL of the MetaDefender Vault server to upload files to
Authentication Token	Vault admin authentication token used for uploading files
Always Upload to a Vault Guest Account	Uploads will be sent to a newly created guest account
Media Manifest	Client will utilize a Media Manifest existing on the media inserted
Block All Files Not Found on Manifest	Any file not found in the Media Manifest will be immediately blocked and Client will not attempt to process the file with MetaDefender
Days to Trust Manifest	The maximum days to use a Media Manifest result
Client Admin Password Hash	Hashed administrative password. This will be used to uninstall the Client or disable USB blocking. The input to this field MUST be in the format <salt>:<iterations>:<password hash>. Use the "–hash_password" command line option for Metadefender.exe to generate a password hash. See section 2.1 Generating and using the Administrator Password for more information
Allow Disabling of USB Blocking	Allow the user to use the Admin Password to disable USB blocking until next restart

2. Command Line Interface

The MetaDefender Client CLI can be run from the command line with the options as described in the table below.

The CLI executable is MetaDefender.exe found at the root of your installation directory.

Example:

C:\Program Files (x86)\MetaDefender Client\MetaDefender.exe <option>=<value> ...

Command Line Options

A list of available command line options is also available by running the MetaDefender Client executable from the command line without any options

Option	Value Types	Example(s)	Commen
server	<standard url>	-server=http://127.0.0.1:8008/	Specifies URL of th MetaDefe server to
rule	String	-rule=Client	Specifies MetaDefe security r process f ***Note: Or applicab MetaDef***
apikey	String	-apikey=13e5f8h4r3s	Specifies MetaDefe apikey ***Note: Or applicab MetaDef***

Option	Value Types	Example(s)	Commen
workflow	String	-workflow=Client	Specifies MetaDefe workflow process f ***Note: Or applicab MetaDef***
verbose	n/a	-verbose	Enables logging o
user_agent	<val>	-user_agent=MDClient	Specifies value of user_age will be pr MetaDefe
cloud_api_key	String	-cloud_api_key=13e5f8h4r3s	Specifies to use wi MetaDefe Cloud
scan_type	A list of one or more of the following strings • physical • system • removable • process • remote	-scan_type="system|process|physical|removable|remote" -scan_type="process|physical|removable" -scan_type=process	Indicates type of sc MetaDefe Client sh • **ph** all dri (e re • **sy** on sy dri

Option	Value Types	Example(s)	Commen
			• **re** - a re m • **pr** on sy pr • **re** ne dri ***Note: Ar invalid paramet be ignor a warnin***
scan_location	"C:\somedir|C:\somefile"	-scan_location="c:\somedir with space|c:\somefile"	Specifies location files and/ directorie scanned ***Note: A is neede directori*** ***Note: inv malform paths wi ignored***
exclude_drive	E:|F:	-exclude_drive=E:|F:	Excludes scan *Only dri supporte currently

Option	Value Types	Example(s)	Commen
report_dir	Directory Path	-report_dir="%AppData%\logs\"	Specifies location v scan logs be saved option is specified file will be generate
report_type	One or more of the following strings • pdf • txt • csv	-report_type=csv	Specifies type of lo write out end of sc ***Note: De txt if opt not spec option is unavaila***
max_file_size	<val> [GB|G|MB|M|KB|K]	-max_file_size=512KB	Specifies maximun files for w MetaDefe Client wil with MetaDefe ***Note: Ar greater t max file display "Exceed Size"***
hash_password	String	--hash_password 123qwe	Generate password for use in Manager

Option	Value Types	Example(s)	Commen
			See 2.1 Generati using the Administ Passwor more infc

2.1 Generating and using the Administrator Password

The Metadefender Client CLI can also be used to generate the administrator password hash. This password is used to uninstall the Client or allow the user to disable USB blocking until next restart.

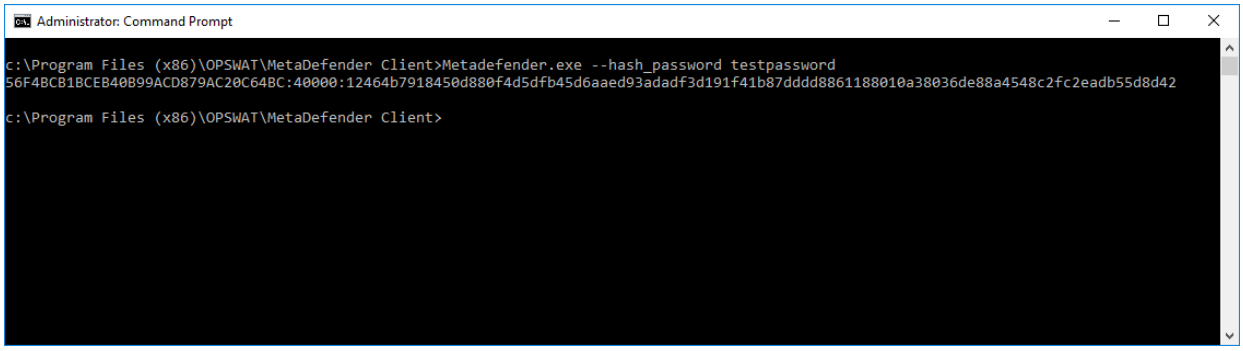
To generate the password hash, use the "–hash_password" command followed by your desired password.

Usage:

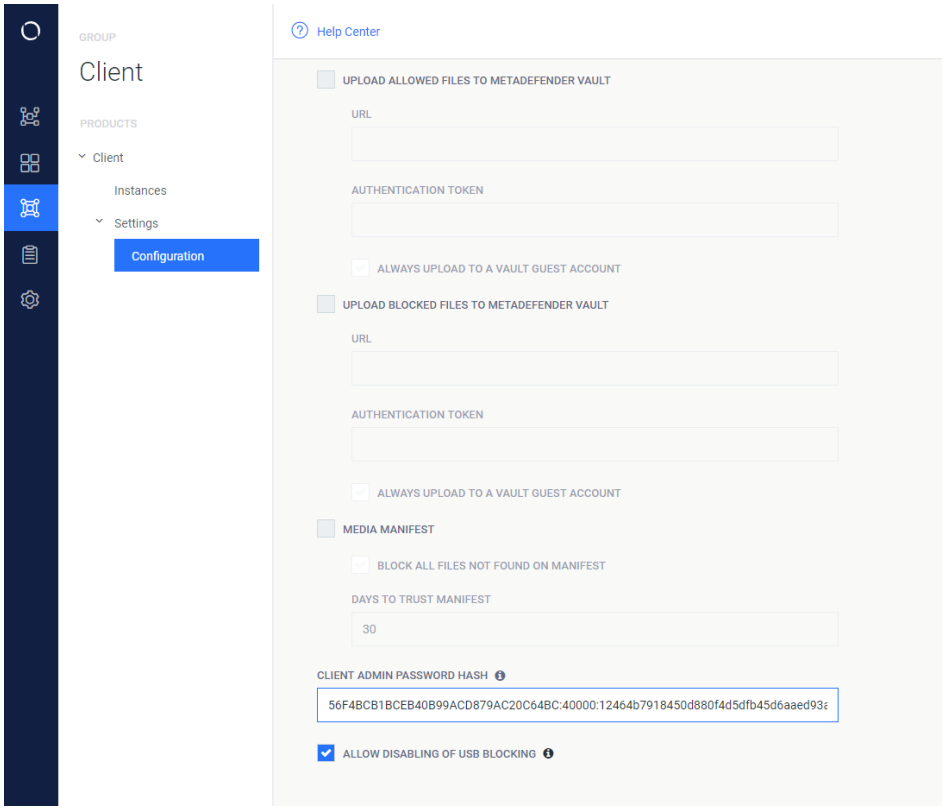
For example, if your desired password is "testpassword", you would use the following command:

C:\Program Files (x86)\MetaDefender Client\MetaDefender.exe --hash_password testpassword

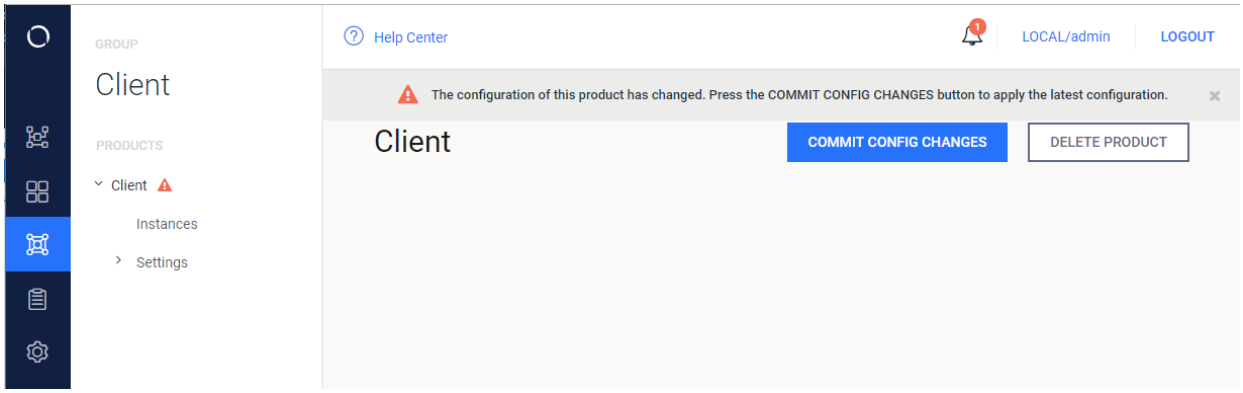
The output will look like the following:



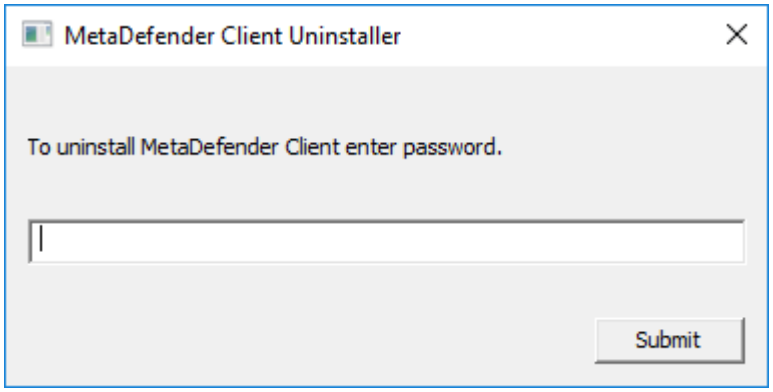
Copy this hashed password to your Central Management settings in the "CLIENT ADMIN PASSWORD HASH" field:



Next, click "SAVE SETTINGS", then open up your Metadefender Client group and click "COMMIT CONFIG CHANGES" to apply this password to all Client instances managed by Central Management.



Now when users attempt to uninstall the Client they will be prompted to enter this password before they are able to uninstall:


MetaDefender Client Uninstaller
To uninstall MetaDefender Client enter password.
Submit

3. MetaDefender Client Release Notes

Tips and Known Issues

4.1.22 MetaDefender Client release 17 Dec, 2019	MetaDefender Client 4.1.22 is a maintenance release primarily focused on bug fixes
Enhancement	
Delete all MD local folder when uninstall	MetaDefender Client deletes folders: %appdata%MetaDefenderApp, %appdata%MetaDefenderApp-Installer, %appdata%Metadefender-Local, %appdata%Metadefender-Installer
Fixed	
Scan file with "Failed to connect to host or proxy"	Client retries when fails
Copy result incorrect	Add some more result action
Crashed when scanning boot record	Crash is fixed
"stop_scan" field in exporting file is N/A	This field is not N/A
File size information is incorrect via client UI	File size is shown correctly

Previous Releases

3.1. Archived MetaDefender Client Release Notes

Tips and Known Issues

- If MetaDefender Client is reporting an error in scanning a file, the file should first be scanned through the MetaDefender Core's web interface to determine the cause of the error.

4.1.22 Release

Change log

- Enhancement: Delete all MD local folder when uninstall
- Fixed: Scan file with "Failed to connect to host or proxy"
- Fixed: Copy result incorrect
- Fixed: Crashed when scanning boot record
- Fixed: "stop_scan" field in exporting file is N/A
- Fixed: File size information is incorrect via client UI

4.1.21 Release

Change log

- Fixed: MD client is crashed when process scan is in queued
- Fixed: Client do not maintain read only flag after scanning

4.1.20 Release

Change log

- Fixed: Overlapped notification when there are more than 1 notification
- Enhance: Add volume ID to report

4.1.19 Release

Change log

- Fixed: The client crashed
- Fixed: %appdata%\MetaDefenderApp folder is not deleted after uninstalling
- Fixed: Un able to read the manifest file
- Fixed: Sometimes activities of notifications runs wrong when exporting file

4.1.18 Release

Change log

- Fixed: The client was hung if it cannot upload files to MetaDefender Vault
- Fixed: Last engine update has presented a wrong datetime
- Fixed: Disable media blocking option was greyed out
- Fixed: The client got stuck when exporting massive files
- Fixed: Missing " boot records" option in Scan Options

4.1.17 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Fixed: The client doesn't show scan history after a device is rebooted
- Fixed: The service path contained spaces and was unquoted
- Fixed: Disable media blocking option is greyed out

4.1.16 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Fixed: Last engine update has presented a wrong datetime
- Fixed: Both pause and play button show at same time
- Fixed: Disable media blocking option is greyed out
- Fixed: Wrong filename encoding in report

4.1.15 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Enhance: Support for AccessData FTK Imager mounted drive
- Fixed: MetaDefender Client was c rashed when the time is empty string
- Fixed: When connect to default server, UI shows MetaDefender.com and medadefender.com:8008
- Fixed: Selecting file for scan details in suspicious tab doesn't remain selected
- Fixed: MetaDefender Client can not install on Windows 7
- Fixed: MetaDefender Client does not apply new path
- Fixed: MetaDefender Client does not show information on Windows Japanese

4.1.14 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Fixed: C rashed when scan file containing Japanese/Chinese characters
- Fixed: Files containing %%% in the filename don't get copied.
- Fixed: Add a field in the configuration file to allow hiding or showing the Compliance tab
- Fixed: C ouldn't install MD Client 4.1.12 on Japanese Windows
- Fixed: Invalid path containing Japanese/Chinese characters

4.1.13 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Fixed: Copy the file only, not contain the directory structure
- Fixed: Can not copy allowed files in manifest when disconnect network
- Fixed: App create " MetaDefende " folder
- Fixed: Wrong behaviour when check "Block All Files Not On Manifest"

4.1.12 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Fixed: App crash during uninstall
- Fixed: Command line with parameter
- Fixed: File permission to show on MD client popup
- Fixed: close dialog popup when close main screen
- Fixed: Override GROUP with CLI command
- Enhance logic for unblock/copy on error

4.1.11 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Convert to local time zone on UI and report
- Fixed: Empty folders don't get copied
- Fixed: Fix scan result due to "Override scan result classified as allowed" setting

- Fixed: Skip symbolic link folder
- Fixed: Indicate when any files fails to sanitize in UI

4.1.10 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Added a new section into scan reports/summary, Potential Vulnerable Files, to list potentially vulnerable files which have no threat detected.
- Fixed: client's IP address was shown as 0.0.0.0 on Central Management.
- Fixed: scanning process was hang until a user clicked Details to see the scan's result.
- Fixed: Client UI loaded the default language, English, instead of a configured language on Central Management when a user first logs in.
- Fixed: Allow users to unblocked CD/DVD if scanning gets error when the setting "Drive unblocking on error" is set to "Allowed"
- Fixed: sanitized files were not copied to defined location if enabled

4.1.9 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Added a new key into configuration file to define a location to generate a scan report automatically after finishing a scan
- Fixed: a scan report couldn't open in Adobe Acrobat
- Fixed: empty folders don't get copied
- Fixed: missing File Scan Path in the pdf scan report
- Fixed: .csv scan result format file is broken

4.1.8 Release

Distributions included in release

- MetaDefender Premium Client

Change log

- Fixed critical bug causing core scans to hang
- Fixed bug where Central Management settings were not populated to all users on a machine
- Fixed MetaDefender Core V3 support
- Corrected minor bug were connection status displayed inaccurate information

4.1.7 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Improvements & Maintenance
- Full visibility to scan network drives
- General bug fixes

4.1.6 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Significant improvement to scan time
- Added File Vulnerability information for executables scanned

- Fixed problem where service would stop with non-admin users
- General bug fixes

4.1.5 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Added optional uninstall password to further lockdown the system
- Added the ability to temporarily disable the client using the uninstall password
- Added warning to settings page if you move away and haven't saved changes
- Fixed bug that would not allow you to sanitize a file and save the results with the same name
- Added sorting to suspicious file tab
- Better retry logic when server is to busy or unavailable
- Added link to OPSWAT Privacy Policy

4.1.4 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Fixed high priority bug where MetaDefender Client would not onboard or heartbeat with Central Management

4.1.3 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Over all stability fixes
- Fixed crash bug with removable media
- Fixed bug dealing with copying from root of a blocked media
- Refined CLI, added verbose flag
- Enabled MetaDefender Cloud as backup server
- Fixed system resource leak
- Fixed bug where systray would not appear on slower systems

4.1.2 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- Fixed Sanitization with Post Actions
- Fixed GDI Leak
- Fixed Play Button behavior when previous scan was against removable media
- Better Hebrew Localization
- Handle File Size of 0
- Fixed CURL Timeout
- Rebooting will lock removable media
- Fixed scanning against MetaDefender V3
- Better CLI support

4.1.1 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- General bug fixes
- Fixed memory leak
- Corrected Data Sanitization behavior with Vault

4.1.0 Release

Distributions included in release

- MetaDefender Free Client
- MetaDefender Premium Client

Other Changes

- New UI and unified functionality
- Multiple historic scans
- MetaDefender Vault integration

4.0.18 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

Other Changes

- Rebranding
- General bug fixes

4.0.17 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

Other Changes

- Added additional requirement in file to enable data sanitization
- General bug fixes

4.0.16 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- Localization of strings supported (English, Japanese, and Hebrew included by default)

Other Changes

- The 'View Processed Files' button has been removed from the MetaDefender Local Client

4.0.15 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- None

Other Changes

- Option to maintain directory structure when MetaDefender USB Client copies to the local system
- Fixed bug where inserting multiple USB drives and then removing one would exit MetaDefender USB Client for other drives

4.0.14 Release

Distributions included in release

- MetaDefender Cloud Client

New Features

- None

Other Changes

- Update to use new MetaDefender Cloud URL

4.0.13 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- None

Other Changes

- 4.0.12 regression fix

4.0.12 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- MetaDefender USB Client can run under non-admin accounts after being installed with admin privileges

Other Changes

- MetaDefender Client does not need a connection to a MetaDefender Core server to be installed
- Reprocess option to start new scan session on MetaDefender Client without physically ejecting drive

4.0.11 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- Data Sanitization Support
- Files can be deleted from browse dialog

Other Changes

- Additional options for handling contents of media manifest file
- MetaDefender Client will not require access to a MetaDefender Core server if all files are present in the media manifest
- The dialog displayed to the user when a USB is inserted has been updated
- MetaDefender Client can run on systems with lower screen resolutions
- The MetaDefender Cloud Client now excludes results from Filseclab, STOPzilla, ByteHero, and Xvirus

4.0.10 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client
- MetaDefender USB Client

New Features

- Media manifest validation done for Browse option in MetaDefender USB Client

Other Changes

- Drives are not displayed in Windows Explorer until they have been unlocked
- File sizes are displayed in Browse window
- Certificates for Media Manifest validation can be stored in the Windows certificate store
- Minor bug fixes

4.0.9 Release

Distributions included in release

- MetaDefender USB Client

New Features

- Validation of MetaDefender Kiosk media scan manifests

Other Changes

- Minor bug fixes

4.0.8 Release

Distributions included in release

- MetaDefender Cloud Client

New Features

- Application CleanUp Tab

Other Changes

- User interface improvements
- Minor bug fixes

4.0.7 Release

Distributions included in release

- MetaDefender Cloud Client

New Features

- None

Other Changes

- Vulnerability detection improvements

4.0.6 Release

Distributions included in release

- MetaDefender Cloud Client

New Features

- Detection for operating system vulnerability MS17-010, which is the vulnerability exploited by the WannaCry virus

Other Changes

- None

4.0.5 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client

New Features

- Compliance Tab (only applies to MetaDefender Cloud Client)
- Vulnerabilities Tab (only applies to MetaDefender Cloud Client)
- Option to automatically run MetaDefender Client when logging in to Windows

Other Changes

- IP Scan tab has been removed (only applies to MetaDefender Cloud Client)
- The mdproxy.exe included in the MetaDefender Client package is now digitally signed by OPSWAT
- Usability improvements

4.0.4 Release (Internal Only)

4.0.3 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender USB Client

New Features

- Option to copy files to USB drive without scanning

Other Changes

- Minor UI changes

4.0.2 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender USB Client

New Features

- First Release of MetaDefender USB Client

Other Changes

- Support HTTPS on MetaDefender Core server
- Better handling of non-English file names

4.0.1 Release

Distributions included in release

- MetaDefender Local Client
- MetaDefender Cloud Client

New Features

- Release of MetaDefender Cloud Client

Other Changes

- The CLI report_type option 'text' has been changed to 'txt'
- Changed the CLI option -save to -persist_config
- Fixed issue where logging to a long file path caused MetaDefender Client to crash

4.0.0 Release

Distributions included in release

- Metadefender Local Client

New Features

- Support for HTTPS
- Command Line Interface

Other Changes

- Better handling of locked and temp files
- Removed limit on maximum file size to upload against MetaDefender Core V4
- Added CLI generation of CSV and PDF report types
- Better handling of additional scan return types

Changes in 3.12.5

- Better handling of Malformed URLs that are inputted in the MetaDefender Core Server URL dialog

- Resolved an issue where the splash screen did not close under older operating systems (e.g. Windows 7 64bit)
- Removed files from the MetaDefender Client package which caused the package to be detected as encrypted archive
- Improved performance by adding a hash lookup for existing scan results before uploading a file for scanning
- Added support for network mapped drives
- Improved the reporting of processes with infected DLLs in the exported report
- Added support for files that have been whitelisted or blacklisted on the Metadefender Core Server

4. Knowledge Base Articles

- Page:How long is the support life cycle for a specific version/release of MetaDefender Client?
- Page:How to configure the automatic generation of MetaDefender Client scan reports?
- Page:How to create a specific security rule for MetaDefender Client 3.12.5 in MetaDefender Core V4?
- Page:How to fix MetaDefender Client "Fatal Error!" with MetaDefender Core over HTTPS?
- Page:How to scan mapped drives with MetaDefender Client?
- Page:What encrypted media are supported by MetaDefender Client?
- Page:What is running during the Metadefender Core client's initializing process?
- Page:Why does the Avira engine flag the Metadefender Client as infected ?

How long is the support life cycle for a specific version/release of MetaDefender Client?

OPSWAT provides support on each release of MetaDefender Client 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.

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
4.1.21	06 Nov 2019	
4.1.20	02 Oct 2019	06 May 2021
4.1.19	27 Aug 2019	02 Apr 2021
4.1.18	23 Jul 2019	27 Feb 2021

4.1.17	18 Jun 2019	23 Jan 2021
4.1.16	07 May 2019	18 Dec 2020
4.1.15	09 Apr 2019	07 Nov 2020
4.1.14	15 Mar 2019	09 Oct 2020
4.1.13	19 Feb 2019	15 Sep 2020
4.1.12	04 Jan 2019	19 Aug 2020
4.1.11	12 Dec 2018	04 Jul 2020
4.1.10	07 Nov 2018	12 Jun 2020
4.1.9	02 Oct 2018	07 Nov 2019
4.1.8	04 Sep 2018	02 Oct 2019
4.1.7	26 Jul 2018	04 Sep 2019
4.1.6	19 Jun 2018	26 Jul 2019
4.1.5	22 May 2018	19 Jun 2019
4.1.3	26 Apr 2018	22 May 2019
4.1.2	26 Mar 2018	26 Apr 2019
4.1.1	12 Mar 2018	26 Mar 2019
4.0.17	12 Jan 2018	12 Mar 2019
4.0.16	11 Dec 2017	12 Jan 2019
4.0.15	29 Nov 2017	11 Dec 2018
4.0.14	15 Nov 2017	29 Nov 2018

4.0.12	10 Oct 2017	15 Nov 2018
4.0.11	07 Sep 2017	10 Oct 2018

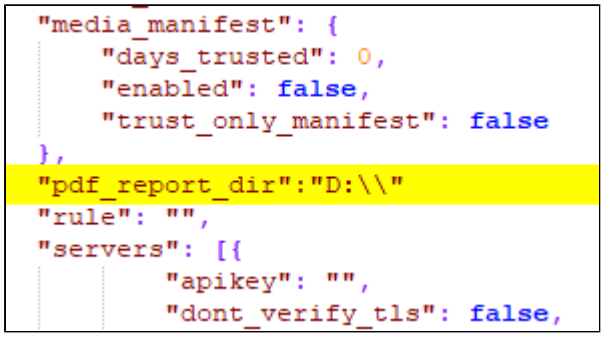
This article pertains to all supported releases of MetaDefender Client
This article was last updated on 2019-11-13
VM

How to configure the automatic generation of MetaDefender Client scan reports?

MetaDefender Client permits the automatic generation of scan reports that are normally only available by exporting the scan details after a scan has been completed. This is done by editing the **client_config** file of MetaDefender Client (not available on Central Management console).

1. Navigate to C:\Users\%%%username%%% \AppData\Roaming\MetaDefenderApp\client_config.json
2. Add the string, "pdf_report_dir":"<a path where you want to save scan reports>"
3. Save the .json file

This configuration will only be applied if MetaDefender Client has appropriate privileges to write to the destination directory.



Note: This feature is only supported on MetaDefender Client 4.1.9 or later.

This article applies to MetaDefender Client version 4.1.9+ and MetaDefender Core 4.x

This article was last updated on 2019-10-24

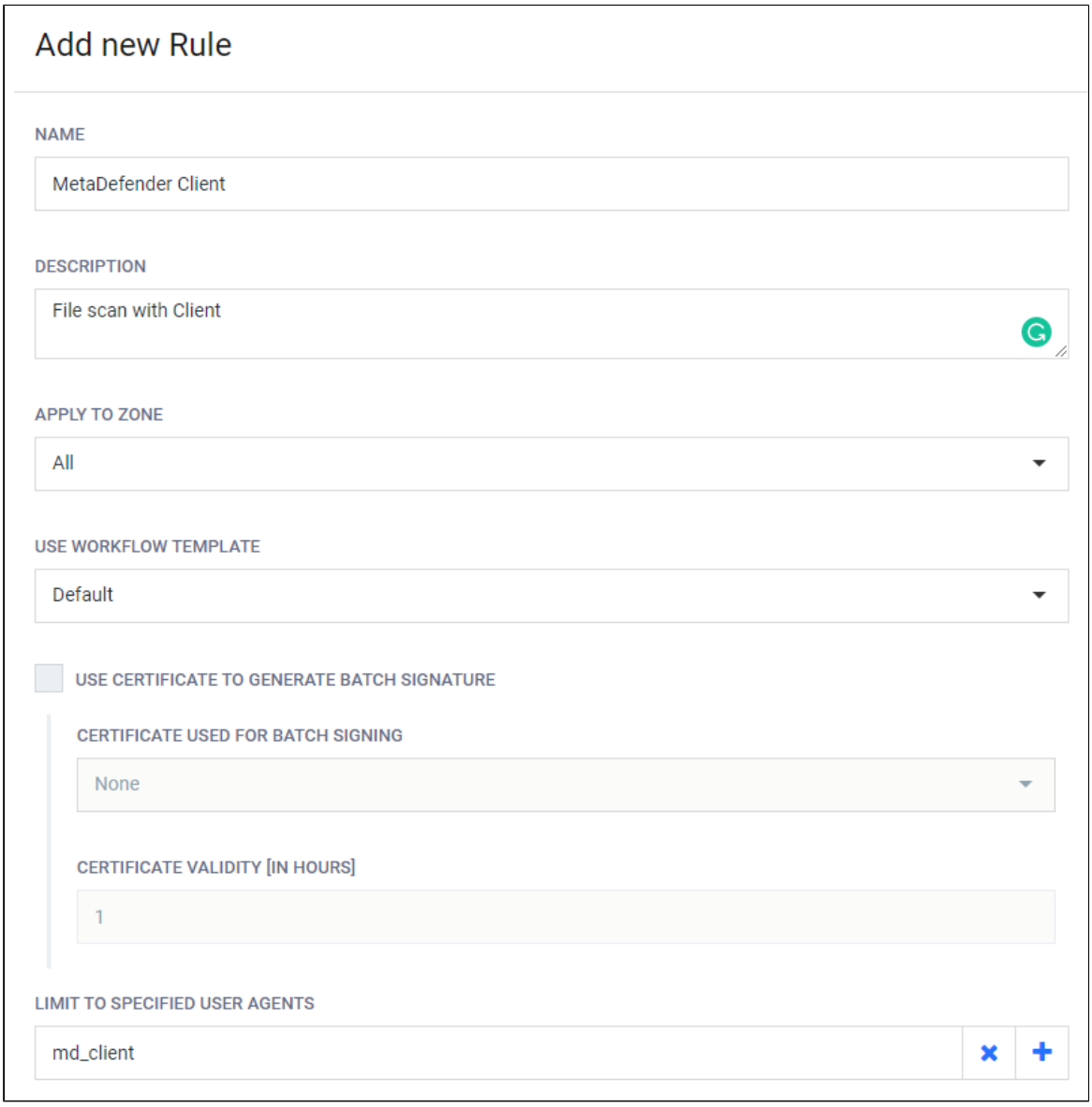
VM

How to create a specific security rule for MetaDefender Client 3.12.5 in MetaDefender Core V4?

By default, when MetaDefender Client 3.12.5 scans with MetaDefender Core v4.x, the "File process" security rule is used.

MetaDefender Core v4.x processes scan requests with the first security rule that matches the request (by default, the "File process" rule is used). If you would like MetaDefender Client to scan files with a different rule, please follow the instructions below:

1. Open the Management Console of MetaDefender Core.
2. On the left side panel, click on **Policies** section and choose **Workflow rules**.
3. Click the **Add New Rule** button on the top right. A pop-up window will open.
4. Be sure the **LIMIT TO SPECIFIED USER AGENTS** is set to **md_client.** See the screenshot below.
5. Save the rule by clicking the **SAVE** button.

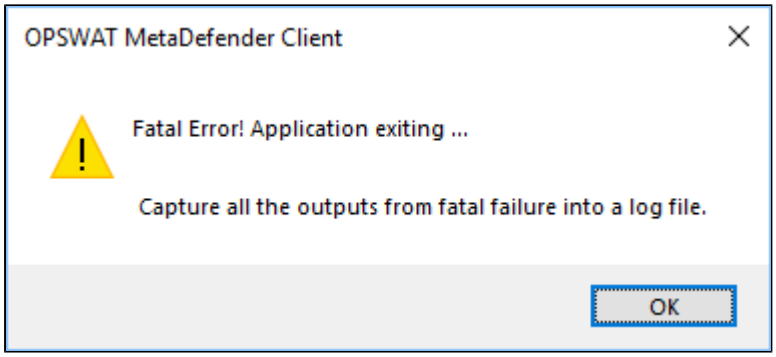


6. After the new rule has been saved it will be listed as the last rule in the priority list. Drag the newly created rule to the top of the list, this way, MetaDefender Core attempts to match this rule before others included in the list.

This article applies to MetaDefender Client version 3.12.5 and MetaDefender Core 4.x
This article was last updated on 2019-10-24
VM

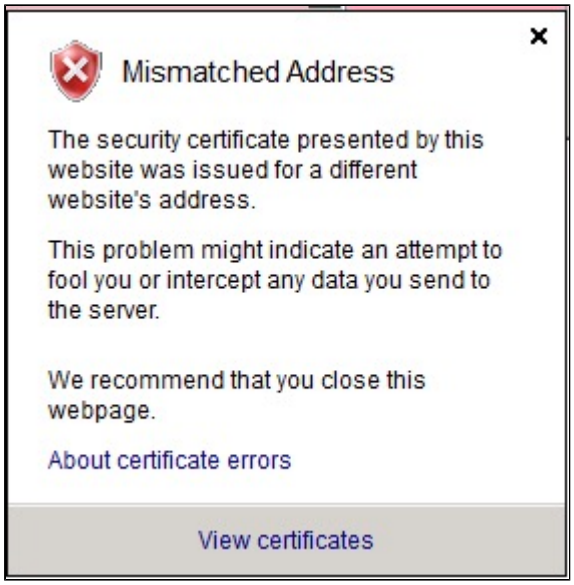
How to fix MetaDefender Client "Fatal Error!" with MetaDefender Core over HTTPS?

If MetaDefender Core has been configured to run over **HTTPS** with a self-signed certificate, you may receive a fatal error message when connecting MetaDefender Client to the MetaDefender Core server. This error is caused by an incorrectly created certificate.



To fix this, ensure that the **Common Name** set during certificate creation matches the **HostName/ServerName** of the **MetaDefender Core** machine.

For example, if the MetaDefender Core machine's hostname is "Server1" and you input "Server2" as the **Common Name** when creating the **SSL,** you will receive an error with the notification that the certificate's address is mismatched.



After the certificate is created, run the MetaDefender Client and specify the hostname and port of the MetaDefender Core machine (e.g. https://server2:8008/).

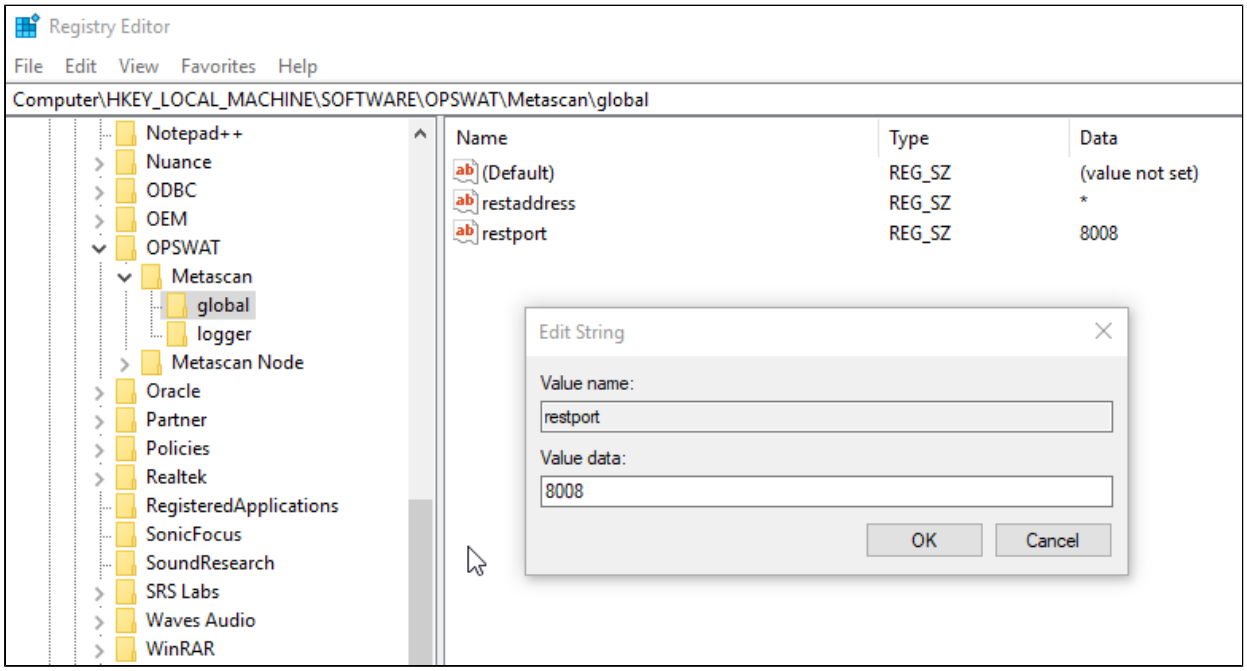
This will **NOT** work if the value is the IP of the MetaDefender Core machine (e.g. https://88.64.12.55:8008/)

Note: Even though the MetaDefender Core is configured to run over HTTPS, the port used will remain on 8008 (see above URL examples). If port 443 is desired, Metadefender Core must be configured to run on this port (443), instead of 8008.

To change the port of a MetaDefender Core instance:

1. Navigate to the registry editor.
2. Open HKEY_LOCAL_MACHINE/SOFTWARE/OPSWAT/Metascan/global.
3. Change the value of the restport key.

After the value has been changed, ometascan and ometascan-node services must be restarted. Input the new URL when prompted by the Client (e.g. https://server2:443).



*For information on how to configure MetaDefender Core to run over **HTTPS**, please see our documentation:*

- *For MetaDefender Core v3 - https://onlinehelp.opswat.com/corev3/Enabling_HTTPS.html*
- *For MetaDefender Core v4 - https://onlinehelp.opswat.com/corev4/3.8._Configuring_SSL.html*

This article pertains to MetaDefender Client 4.0.1. and above
This article was last updated on 2019-10-24.
VM

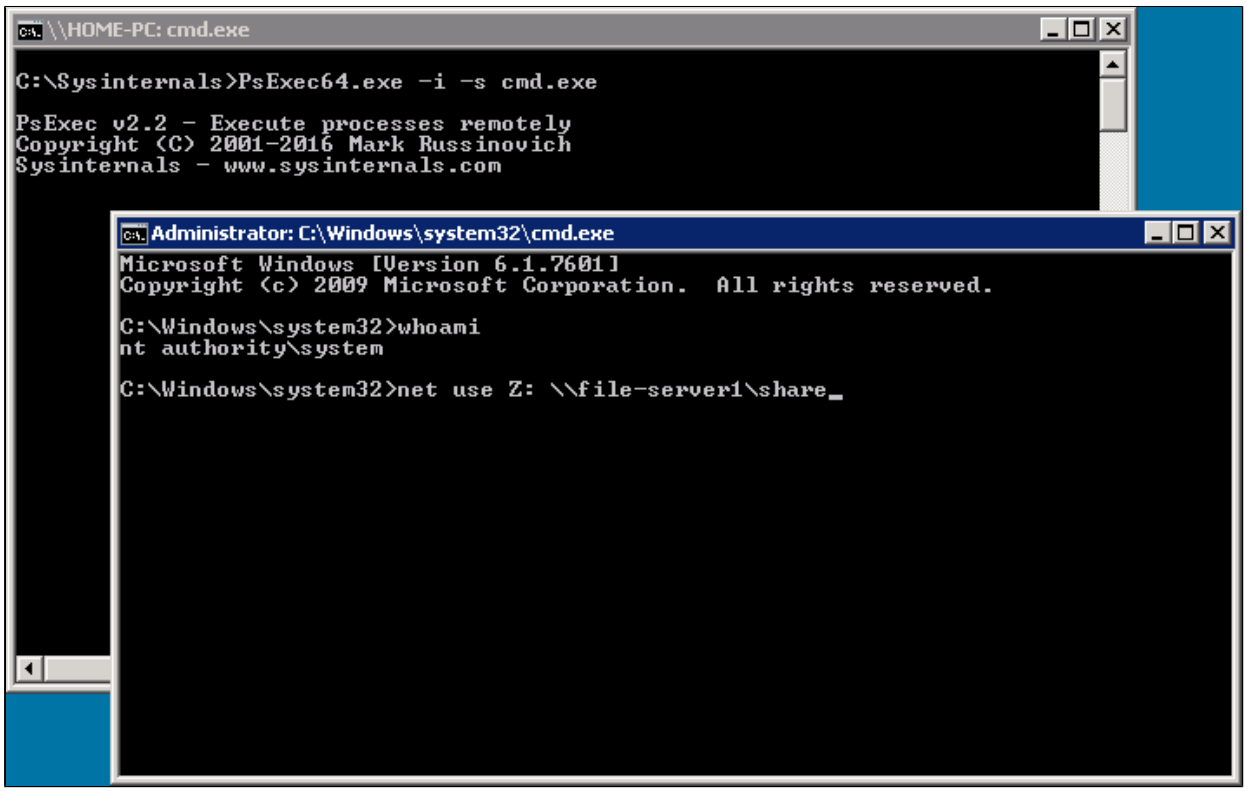
How to scan mapped drives with MetaDefender Client?

MetaDefender Client can scan files in mapped network drives if the drive is mapped under administrator privilege on any system that can reach your MetaDefender Client server. If you would like to initiate scans through the command line using the MetaDefender Client server itself, see below.

***Note:** The mapped drive will be marked as a "Disconnected Network Drive" in Windows Explorer. This is only a display issue, the mapped drive can be used in the same way as a typical mapped drive is used.*

In order to scan mapped drives with MetaDefender Client, the mapped drive must be created under the SYSTEM account:

1. Download **PsExec64.exe** or **PsExec64.exe**, depending on your OS bitness (32 or 64), from the "**Sysinternals Security Utilities**" suite at https://docs.microsoft.com/en-us/sysinternals/downloads/security-utilities
2. Place the **PsExec64.exe** tool on the machine where the mapped drive is to be created E. g. C:\Sysinternals\PsExec64.exe
3. Open a command prompt with elevated privileges.
4. Navigate to the directory where PsExec64.exe was copied. E.g. "cd C:\Sysinternals"
5. Execute the following command to open a command prompt as the SYSTEM user: " **psexec.exe –i –s cmd.exe**"
6. In the new command prompt window that just opened, execute the following command: " **whoami**"
7. Confirm that the current command prompt is running as "**nt authority\system**".
8. Execute the following command to mount the mapped drive: "**net use <desired drive letter> <UNC path to map to>**" E.g. "**net use Z: \\file-server-1\share**"



MetaDefender Client should now successfully scan the mapped drive and the mapped drive should be accessible to all users on the computer.

This article applies to MetaDefender Client
This article was last updated on 2019-10-25.
VM

What encrypted media are supported by MetaDefender Client?

Please consult the following table for the supported encrypted media:

Supported Encrypted Media
Biocryptodisk-ISPX
Apricorn Aegis Secure Key
Apricorn Aegis Padlock
Apricorn Aegis Fortress
Apricorn Aegis Bio
Kingston DataTraveler 2000

If you have questions or are using a product that is not on the above table, please contact support.

In general, Encrypted Media that advertises as "Software-Free" or "Software-Less" is more likely to be supported by the MetaDefender product line.

This article pertains to MetaDefender Client 4.0.1 or above
This article was last updated on 2019-10-31
VM

What is running during the Metadefender Core client's initializing process?

During the initializing process, MetaDefender Core client loads libraries needed to connect to the MetaDefender Core REST API and count the running processes and files on the system that require scanning. The amount of time this process requires will depend on the disk's I/O speed.

This article applies to MetaDefender Client
This article was last updated on 2019-11-01
VM

Why does the Avira engine flag the Metadefender Client as infected ?

Upon the release of MetaDefender Core v3.12.5, the MetaDefender Client self executable file generated from the management console gets flagged as infected by the Avira engine.

This is a false positive and OPSWAT is working with the vendor to fix this issue.

Currently, the MetaDefender Client that is available from portal.opswat.com, is properly signed and will not be detected as infected.

This article pertains to MetaDefender Client 3.12.5.
This article was last updated on 2019-11-01
VM

5. Legal

Copyright

DISCLAIMER OF WARRANTY

OPSWAT Inc. makes no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages.

COPYRIGHT NOTICE

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.