OPSWAT

AGD Documentation

MetaDefender Core & MetaDefender Kiosk
Evaluation Assurance Level (EAL): EAL4+, augmented with ALC_DVS.2, ALC_FLR.2, AVA_VAN.5

TOE Reference:	MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6
Version	v1.8
Date	2025-11-03
Classification:	PUBLIC

Version history

Version	Date	Author	Description
v1.0	2024-08-30	OPSWAT	The first version of the AGD documentation.
v1.1	2024-10-11	OPSWAT	MetaDefender Kiosk version update
v1.2	2025-03-07	OPSWAT	Amendments based on the 1st analysis cycle
v1.3	2025-06-17	OPSWAT	Amendments based on the 2nd analysis cycle
v1.4	2025-07-08	OPSWAT	ST reference update
v1.5	2025-08-08	OPSWAT	Amendments based on the 3rd analysis cycle
v1.6	2025-08-26	OPSWAT	New ST reference
v1.7	2025-10-14	OPSWAT	New ST reference
v1.8	2025-11-03	OPSWAT	New ST reference

Table of Contents

1 Introduction

This Security Target (ST) defines the OPSWAT MetaDefender Core & MetaDefender Kiosk Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

OPSWAT MetaDefender Kiosk is a cybersecurity solution for protecting your critical network and assets against removable media threats. MetaDefender Core is a backend component that provides centralized file analysis orchestration capabilities. MetaDefender Core is powered by a suite of cybersecurity technologies such as Multiscanning, Deep CDR, Proactive DLP, Adaptive Sandbox and others to detect, analyze and eliminate malware and zero-day attacks. MetaDefender Kiosk is a front-end component that is used as a media scanning workstation.

Table 1 - TOE Reference

TOE Name	MetaDefender Advanced Threat Prevention solution
TOE Reference	MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6
TOE Version and Release Date	MetaDefender Core • Version: v5.14.2 • Release date: 2025-05-28 MetaDefender Kiosk • Version: v4.7.6 • Release date: 2025-06-14

This document was created to fulfil the following assurance requirements of [CC_P3]:

- Operational user guidance (AGD_OPE.1)
- Preparative procedures (AGD_PRE.1)

1.1 Purpose

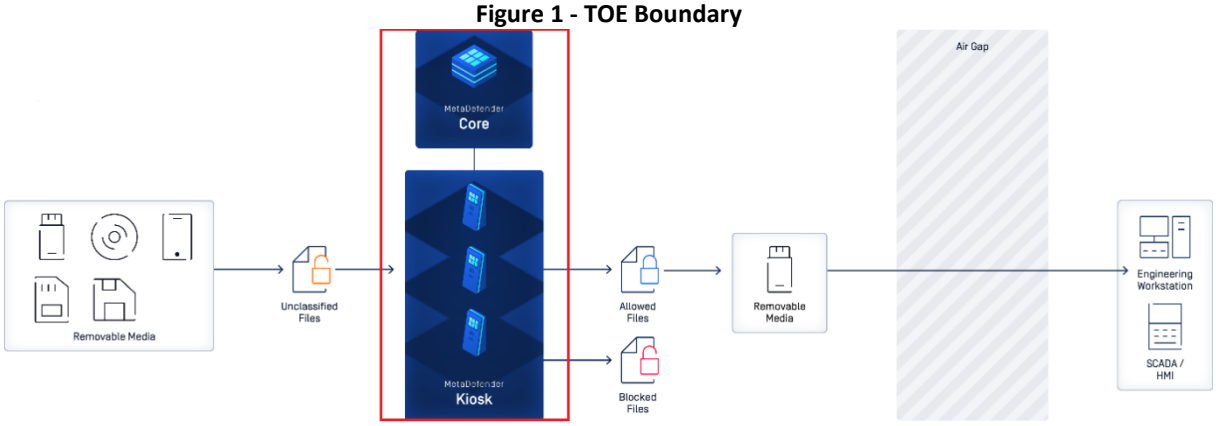
This document provides guidance on the secure installation and secure use of the TOE for the Common Criteria (CC) Evaluation Assurance Level 4 Evaluated Configuration. This should be used as the guiding document for the installation and administration of the TOE in the CC-evaluated configuration. The official MetaDefender Core v5.14.2 & MetaDefender Kiosk v4.7.6 documentation should be referred to and followed only as directed within this document.

1.2 TOE Configuration

The figure below illustrates the TOE operational environment containing TOE and non-TOE components, that also defines TOE boundary.

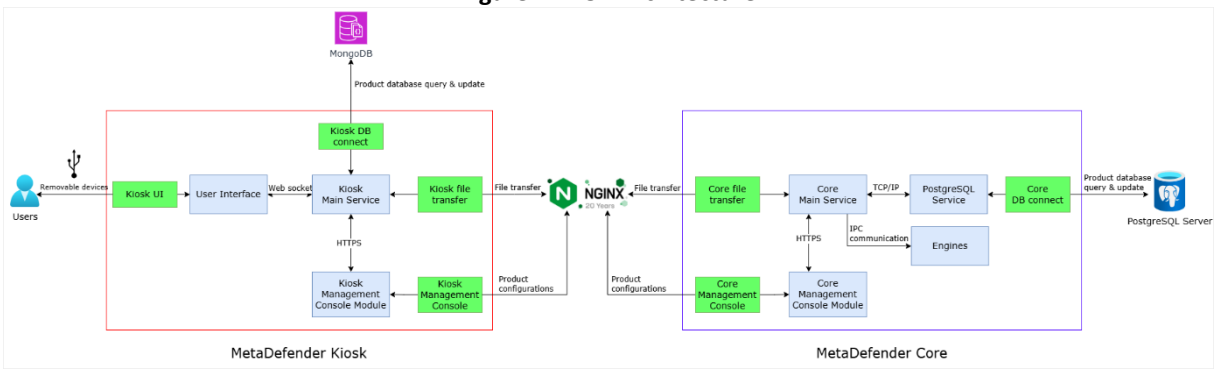
TOE in the red box includes two different components (applications): MetaDefender Kiosk and MetaDefender Core (with engines / technologies underneath).

Figure 1 - TOE Boundary



1.3 TOE architecture

Figure 2 - TOE Architecture



The TOE includes the following subsystems and modules:

- **MetaDefender Core**
  - **Core Main Service**: Service serves as the backend of the system. It acts as the primary interface for receiving requests from clients, as a central point for task distribution, coordinating and assigning jobs to different modules, consolidating results. It receives requests from clients, such as file scans, and determines the appropriate actions to be taken. When a file is submitted for scanning, the Core Main service is responsible for routing the file to the appropriate engines according to the specified workflow rule for analysis.
  - **PostgreSQL Service**: The Core Main Service incorporates a PostgreSQL service as a backend database. This PostgreSQL service is responsible for storing and managing critical data such as scan results, history, statistics, workflow rules and system configurations.
  - **Engines**: A collection of OPSWAT technology modules. The relationship and communication between the Core Main service and Engines is crucial for the system's functionality. These engines are designed to perform analysis, inspection and sanitization of files and data. Some engines focus on a specific aspect of analysis such as malware scanning, behavior analysis, or file type verification. It can detect a wide range of threats such as malware,

vulnerabilities, and sensitive data. It also can sanitize and prevent possibilities of malicious content.

- **Core Management Console Module:** This console serves a user-friendly interface for authorized users such as system administrators to monitor and manage MetaDefender Core system. From the console, authorized users can configure system settings, define workflow rules, monitor processing history, check statistics, generate reports and perform various administrative tasks.

- **MetaDefender Kiosk**
  - **User Interface**: This is a Windows application used to display the user interface. It shows the UI for users to interact and scan peripheral devices. When users perform actions from the UI, it calls several APIs through the Kiosk Main Service to retrieve the necessary information and display the results to the user.
  - **Kiosk Main Service**: This is the background service of KIOSK running on Windows. It handles various KIOSK system tasks (authentication, scanning, performing post actions, etc.). It provides protocols for other components to communicate with and returns results for display to the end user.
  - **Kiosk Management Console Module:** This is a webpage for administrators to configure system settings. The console calls APIs to the Kiosk Main Service to load the current configurations. After the administrator makes adjustments, the KIOSK Console calls APIs through the Kiosk Main Service to update the new configurations. The MetaDefender Kiosk Management Console TSFI allows you to manage the MetaDefender Kiosk system through a web browser. The Management Console can be accessed through *http(s)://<MetaDefender Kiosk system>:8009*. After an initial, fresh installation, a configuration wizard is displayed to setup the Kiosk Management Console Module .

Table 2 - Subsystems, modules, TSFIs

Subsystem	Module	TSFI	Functions	TSF
MetaDefender Core	Core Main Service	Core file transfer	File transfer	File Threat Analysis Protected Communication Security Management
	PostgreSQL Service	Core DB connect	Database Connect	File Threat Analysis User Authentication
	Engines	-	File Analysis	File Threat Analysis
	Core Management Console Module	Core Management Console	File Processing	File Threat Analysis Protected Communication User Authentication Security Management
			Dashboard	Protected Communication

				User Authentication Security Management
			History	Protected Communication User Authentication Security Management
			Workflow Management	Protected Communication User Authentication Security Management
			Inventory	Protected Communication User Authentication Security Management
			User Management	Protected Communication User Authentication Security Management Key generation and destruction
			General Settings	Protected Communication User Authentication Security Management Key generation and destruction
			Licensing	Protected Communication User Authentication Security Management
MetaDefender Kiosk	User Interface	KIOSK UI	Application UI	User Authentication Protected Communication
	Kiosk Main Service	Kiosk file transfer	File discover and transfer	Protected Communication

		Kiosk DB connect	Database Connect	Protected Communication Security Management
	Kiosk Management Console Module	Kiosk Management Console	Dashboard	Protected Communication User Authentication Security Management
			Configuration	Protected Communication User Authentication Security Management
			Workflow	Protected Communication User Authentication Security Management
			Session Logs	Protected Communication User Authentication Security Management

There are non-TOE components which are not affect the TOE security listed in [ST] section 1.3.4 Non-TOE Software/Firmware/Hardware from which the following are shown in this figure:

- NGINX
- MongoDB
- PostgreSQL Server

2 Operational User's Guide

The user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, whether it is misleading or unreasonable.

2.1 Functions, privileges, and appropriate warnings

2.1.1 Product functions

- Use with Vault Server
- Email password recovery
- Custom scanners

- Yara rule sources
- Cloud based scanning by 3rd party malware engines
- Sending files to MetaDefender Cloud
- Decryption / unlock of password protected files
- Kiosk visitor management

2.1.2 MetaDefender Core functions

- **File transfer**: This function receives file transferred from Kiosk for scanning and provide results.
- **Database Connect**: This function enables connections to the database and queries the necessary information to display on other components.
- **File Analysis**: This function analyzes and processes files with Engines, then provides detailed results.
- **File Processing**: This feature likely involves scanning, analyzing, and processing files for malware, security threats, vulnerabilities, or sensitive data. It includes functionalities such as file upload, scanning, threat detection, sanitization, file type verification, and reporting.
- **Dashboard**: This function displays results, detected threats, metrics, statistics, and insights regarding file scans, security status, and system health. It provides users with a visual overview of the system's operation, executive report and security posture.
- **History**: The processing history maintains a log of file processing activities, scan results, user actions, module update and configuration events. It enables users to track the history of file scans, threats, incidents, and changes made within the system for auditing purposes.
- **Workflow Management**: This facilitates the configuration of modules, detection policy, blocklist and allowlist. It allows users to define rules for processing files and customize workflows to suit specific requirements.
- **Inventory**: This feature offers a repository of information about all modules, certificates, post actions, external scanners, list of hashes for blocklist and allowlist.
- **User Management**: This involves the administration of user accounts, user directories, roles, permissions, and access controls. It includes functionalities for user authentication, authorization, and user group management customization.
- **General Settings**: These consist of many different settings such as Module Update, Data Retention, Network, Security, Session, Health Check that users can adjust to customize the system according to their needs.
- **Licensing**: This provides an activation feature and outlines the rights of users regarding the usage, modules, and expiry date of customer's purchase.

Table 3 - MetaDefender Core Roles and available functions

Role	TSFI	Function	Warning
Administrators	Core file transfer	File transfer	- Both body data and download link were given. - Callback URL is invalid.

			- File upload rejected due to insufficient disk space - Missing Content-Length header. - File is empty. - Local file scan feature is disabled. - Failed to request scan. File size exceeded the maximum size permitted by your configuration. - Failed to request scan. Try again later. - File not found, invalid path or access. - License is expired - No available rule is present for scanning. - Server is too busy. Try again later.
Administrators	Core DB connect	Database Connect	- There's a problem when connecting to the database. Please contact your administrator.
Administrators	Core Management Console	File Processing	- You are not authorized to use any scan configuration. Contact your system administrator. - The selected file is empty. - No file selected - File selected larger than + {rule.max_file_size} + MB - No file selected + {rule.max_file_size} + MB - Did not receive data_id from server! - The HASH or Data ID is not valid - The Data ID was not found - You are not authorized to view scan results. - Error occurred - The HASH was not found - The hash is not valid - An error occurred while cancelling the process.
	Core Management Console	Dashboard	- An error occurred when fetching statistic information. - An error occurred while downloading report. - An error occurred while modifying the Settings. - Support is only available for the maximum time window of 1 year

	Core Management Console	History/Processing History	- An error occurred while cleaning up. - Hash's length should be 32, 40 or 64.
	Core Management Console	History/Config and Update history	- An error occurred while loading history.
	Core Management Console	Workflow management	- Can not create item. - Can not update item. - Error: duplicate hash - Can not clone item. - Ordering error. - No changes detected. - Validation failed. - Can not load menu - An error occurred while loading - Can not load mapping schema - Can not load remote field. - Can not load data. - An error occurred while create tabs order - Rule names must be unique
	Core Management Console	History/Quarantine	- An error occurred while cleaning up. - An error occurred while modifying settings. + {server error} - An error occurred when deleting records. - An error occurred when sending records to MetaDefender Cloud. - An error occurred when pinning record. ${server error} - An error occurred while protecting records - An error occurred while unprotecting records. - An error occurred when sending record to Adaptive Sandbox. - An error occurred while sending records to Adaptive Sandbox. - An error occurred when sending record to SBOM. - An error occurred when sending records to SBOM. - Hash length should be 64. Please note that only SHA256 is supported at the moment

			- Data ID length should be 32
	Core Management Console	Inventory\Modules	- Manual update triggering failed - An error occurred while saving configuration. - Source package generating failed - Source: ${source} is still disabled. - Source: ${source} is still enable. - An error occurred while deleting source. - An error occurred while removing module. - No option selected to remove.
	Core Management Console	Inventory\Skip by hash	- An error occurred while deleting the hash. - An error occurred while loading available engines.
	Core Management Console	Inventory\External scanner	- An error occurred while deleting the external scanner. - An error occurred while loading the external scanners.
	Core Management Console	Inventory\Post action	- An error occurred while deleting the post action - An error occurred while loading the post actions.
	Core Management Console	Inventory\Certificate Inventory\Webhook Authentication	- An error occurred while deleting the certificate. - An error occurred while deleting the certificate
	Core Management Console	Inventory\Password Storage	-
	Core Management Console	User Management	- An error occurred while loading - Item already exists
	Core Management Console	Settings\General	- Max queue size must be less than or equal 40000!
	Core Management Console	Settings\Email Notification	-
	Core Management Console	Settings\Health Check	- An error occurred while saving modification.

	Core Management Console	Settings\Security	- An error occurred while setting PIN code - An error occurred while saving modification - An unexpected error occurred. Please try again.
	Core Management Console	Settings\Network	- Seems something went wrong. Please try again later. - Seems something went wrong. Please check your email configurations again - An error occurred while configuring database connection. - Please provide username and password of Master Proxy - An error occurred while loading email configuration - An error occurred while loading proxy configuration - An error occurred while changing database password - Failed to connect to database - An error occurred while testing database connection.
	Core Management Console	Settings\Data retention	- Settings updated failed. + {server error}
	Core Management Console	Settings\Import/ Export	- Can not download config.
	Core Management Console	Settings\Central Management	- An error occurred while loading configuration - An error occurred while saving modification - An error occurred while disconnecting from Central Management. Please, try again later!
	Core Management Console	Licensing	- Deactivation failed. - An error occurred while activation. - An error occurred while delete backup license - An error occurred while nominate license - An error occurred while activation. - An error occurred while backup. - Failed to get available licenses, - Failed to get OLMS activation information - Failed to test connection

Security administrators	Core Management Console	All except User Management, Licensing, Config History, Dashboard\Executive Report, Inventory\Password Storage, Settings\Email Notification, Settings\Security, Settings\Network, Settings\Data Retention, Settings\Export/Import, Settings\Central Management.	Like above
Security auditor	Core Management Console	All except Dashboard\Executive Report, Inventory\Password Storage, Settings\Email Notification, Settings\Network, Settings\Export/Import, Settings\Central Management.	Like above
Help desk	Core Management Console	All except Dashboard\ Executive Report and System Health, User Management, Licensing, Inventory\Password Storage, Settings\Email Notification, Settings\Security,	Like above

		Settings\Network, Settings\Module Update, Settings\Data Retention, Settings\Health Check, Settings\Export/ Import, Settings\Central Management, History\Config history, History\Quarantine, Inventory\Certificates, Inventory/Webhook authentication.	
Anonymous	Core Management Console	File processing	Like above

2.1.3 MetaDefender Kiosk functions

- **Application UI**: This function allows users to interact with the KIOSK system through interface pages. Users can perform actions such as selecting a workflow, authenticating, choosing files to scan, and selecting post-scan actions.
- **Database Connect**: This function enables connections to the database and queries the necessary information to display on other components.
- **File discovery and transfer**: This function allows users to discover files on a USB device and transfer them to MD Core for scanning.
- **Dashboard**: This function provides a summary of all files processed by MetaDefender Kiosk. It is the first function encountered when logging into the console, offering an overview of processing activities.
- **Configuration**: This function allows administrators to configure global settings on the KIOSK system.
- **Workflow:** This function enables administrators to configure workflows for Employees and Guests.
- **Session Logs:** This function provides information about scanning sessions, enabling administrators to perform audits when necessary.

Table 4 - MetaDefender Kiosk Roles and available functions

Role	TSFI	Function	Warning
Administrator	Kiosk Management Console	Configuration	- Error! No API key specified - Invalid Core server url or API key - Path is required - Invalid file path - Invalid email - File is empty. Please select a file with content., - Please fill out mandatory fields before saving configuration - Unsupported configuration format
		Dashboard	NA
		Workflow	- Failed to save. Missing some required fields
	Kiosk DB Connect	Database Connect	- Page not found
Auditor	Kiosk Management Console	Session Logs	- Attach file is not found
User/Guest	KIOSK UI	Application UI	- A name is required - Error loading the authentication module - Incorrect Name or Password - Inaccessible content found on the media, processing will continue - File could not be opened
	Kiosk file transfer	File discovery and transfer	- Invalid Core Setup Please contact administration. - MetaDefender processing was aborted because a blocked file was found - File exceeds maximum allowed size on MetaDefender - Not all files were processed by MetaDefender - Connection lost with MetaDefender - MetaDefender processing was canceled, - Unknown aborted reason - Invalid media. Not enough space available for copy. Need at least … - Session timeout

			- Connection to MetaDefender has been interrupted, attempting to connect... - MetaDefender is too busy

2.2 MetaDefender Core functions

Brief introduction of the user-accessible functions in the TOE scope.

2.2.1 File transfer

Purpose: MetaDefender Core provides a function that receives files transferred from KIOSK for analysis and scanning via REST API. Data ID is returned via REST API response. KIOSK can fetch scan results with that Data ID via REST API.

Method of use: send files from KIOSK, call REST API to post file of MetaDefender Core or analyze file via Web Interface of MetaDefender Core.

Parameters:

- Filename: while file is sent to MetaDefender Core via REST API, clients such as KIOSK, Web Interface put name of its file into “filename” header.
- File content: must be added to HTTP request body.

For more details, please see chapters “Process Files via REST API” and “Analyze File (Asynchronous mode)” of [MDCore].

2.2.2 Database Connect

Purpose: MetaDefender Core provides a function to connect to a PostgreSQL database and retrieve necessary information to display and update data from other components within the system.

Method of use: Users can update PostgreSQL server information via Core Management Console.

Local DB Parameters: database user credential and database information.

Remote DB parameters: admin user credentials, server, port

For more details, please see chapter “Database Management” of [MDCore].

2.2.3 File Analysis

Purpose: MetaDefender Core analyze files with Engines and provide analysis results.

Method of use: This is internally connected to Core Main Service. When Core Main Service receives files from Core file transfer or Core Management Console, Core Main Service distributes files to Engines for analysis, Engines will process the files with preconfigured workflow settings and return results to Core Main Service.

For more details, please see chapter “Process files with MetaDefender Core”, “Analyze File (Asynchronous mode)” and “Fetch Analysis Result” of [MDCore].

2.2.4 File Processing

Method of use: MetaDefender Core provides 2 ways for users to process files: Web Interface (via Core Management Console) and REST API (via Core File Transfer).

By default, anonymous users[1] and authorized users can access both ways to post files to MetaDefender Core, and anonymous users can process files with only two workflow rules "File process" and "File process without archive". Administrators can change and restrict access.

Figure 3 - File Processing

Parameters:

On Web Interface (Core Management Console), users can upload a file in the form above. After selecting a file, two options will appear beneath the form. The first option "Password protected file?" is for users to input password if the file is password protected. The second option, a dropdown list, is an option to choose Workflow Rule. Users select a workflow rule from the dropdown list, for example, "File process" to process the file and input password if the file is password protected.

Raw binary file content must be packed in a single payload and streamed over to MetaDefender Core.

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

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

Figure 4 – File Processing with parameters

[1] Through Core REST API, when the user does not put in "apikey" header, it means there is an anonymous user.

TSF response or message:

- Success: Show up a result page where users can see metadata, processing result, verdict, and details.
- Error:
    - Callbackurl and/or apikey are invalid.
    - Invalid user information or Not Allowed
    - Content-Length header is missing from the request.
    - Body input is empty.
    - Unexpected event on server
    - Server is too busy, scan queue is full. Try again later.

Via REST API, MetaDefender Core recommends using the JSON-based REST API.

1. Upload a file to scan (POST /file), then receive data_id from response: (Scan File API) Note: The performance depends on: number of engines, type of file to be scanned, MetaDefender Core's hardware.
    - TSF response or message:
        1. Success: HTTP 200 and Data ID of the file
        2. Error:
            1. HTTP 400 and “Callbackurl and/or apikey is invalid.”
            2. HTTP 403 and “Invalid user information or Not Allowed”
            3. HTTP 411 and “Content-Length header is missing from the request.”
            4. HTTP 422 and “Body input is empty.”
            5. HTTP 500 and “Unexpected event on server”
            6. HTTP 503 and “Server is too busy, scan queue is full. Try again later.”
2. Fetch the result with previously received data_id (GET /file/{data_id}) until scan result belonging to data_id doesn't reach the 100 percent progress_percentage: (GET Fetch Analysis Result API).
    - TSF response or message:
        1. Success: HTTP 200 and entire analysis report generated by MetaDefender Core.

2. Error:
    1. HTTP 405 and “Access denied”
    2. HTTP 500 and “Unexpected event on server”

For more information see section “Process files with MetaDefender Core” in [MDCore].

2.2.5 Dashboard

Method of use: MetaDefender Core provides a general overview of MetaDefender Core status and allows you to configure its options of the default auto refresh rate.

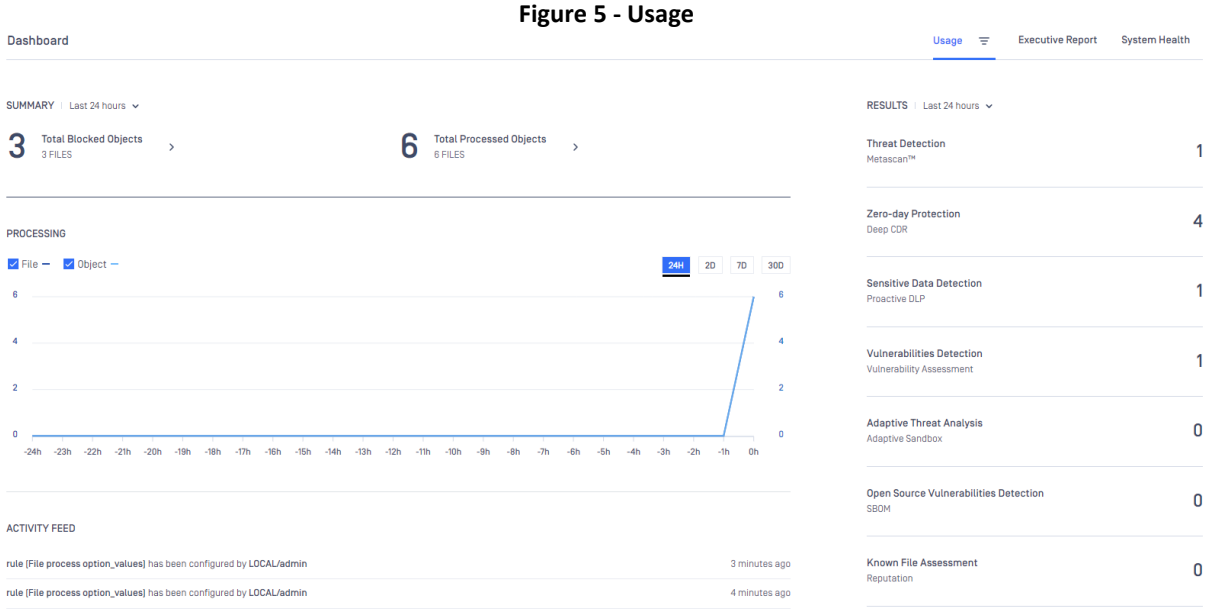
The Dashboard consists of 3 subpages: Usage, Executive Report and System health.

Usage 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 an archive engines)
- Number of connected nodes
- Number of scanned objects in the last 30 days
- Statistics on number of processed files in time
- Statistics on processing results

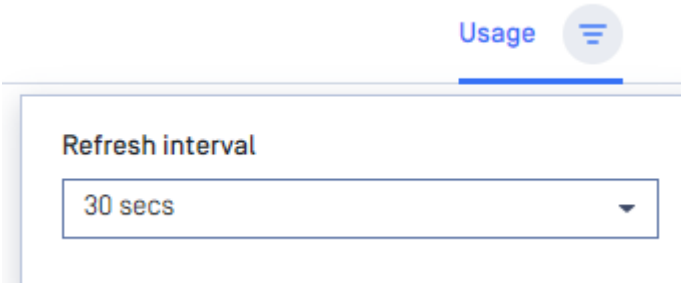
Administrators, Security administrators and Security auditor can access this page.

Figure 5 - Usage



Both the default refresh rate (default is 30 seconds) and the span of time displayed (24 hours) can be changed.

Figure 6 – Usage refresh interval



The Executive Report page is to provide all needed statistics processed data.

- Number of blocked/processed objects
- Number of results/filetypes (doughnut chart)
- Average processing time
- Average file size
- Top 10 Countries Detected
- Top 10 Vendors Detected
- Number of Reputation Detected
- Number of Threats Detected by Adaptive Sandbox
- Number of Threats Detected by Multiscanning
- Number of Objects Sanitized
- Number of Sensitive Data Detected
- Number of Vulnerabilities Detected
- Number of Vulnerabilities Detected by SBOM

The span of time displayed (24 hours) and workflow can be changed. There is an ability to export a PDF format of this report.

Only the Administrators can access this page.

Figure 7 - Executive Report filter

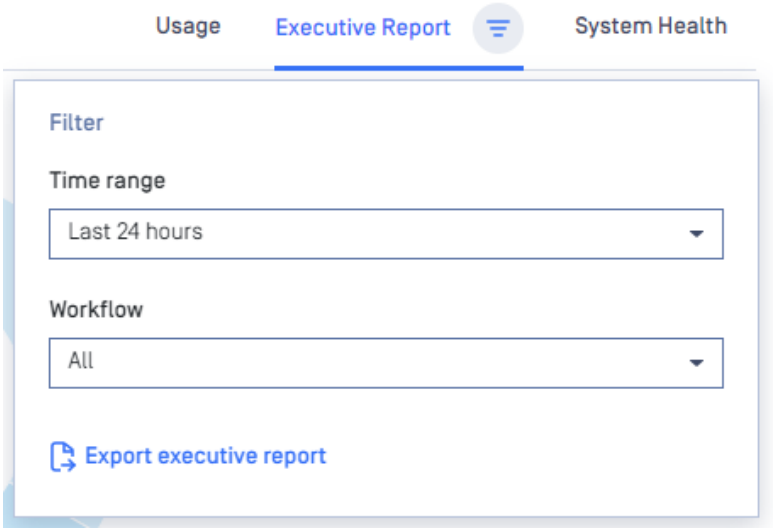
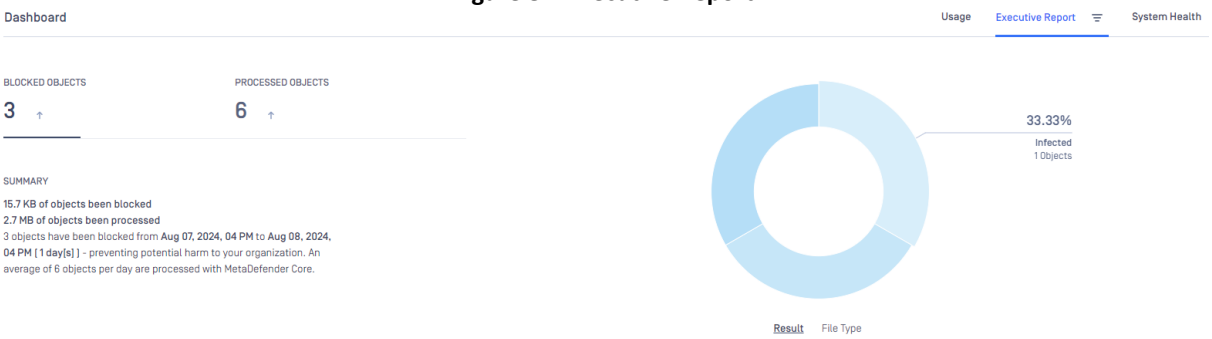
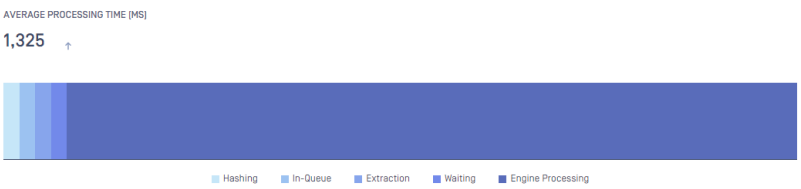
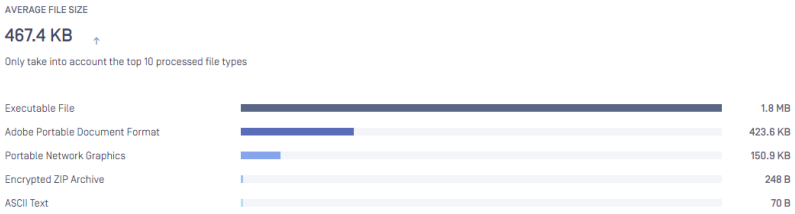
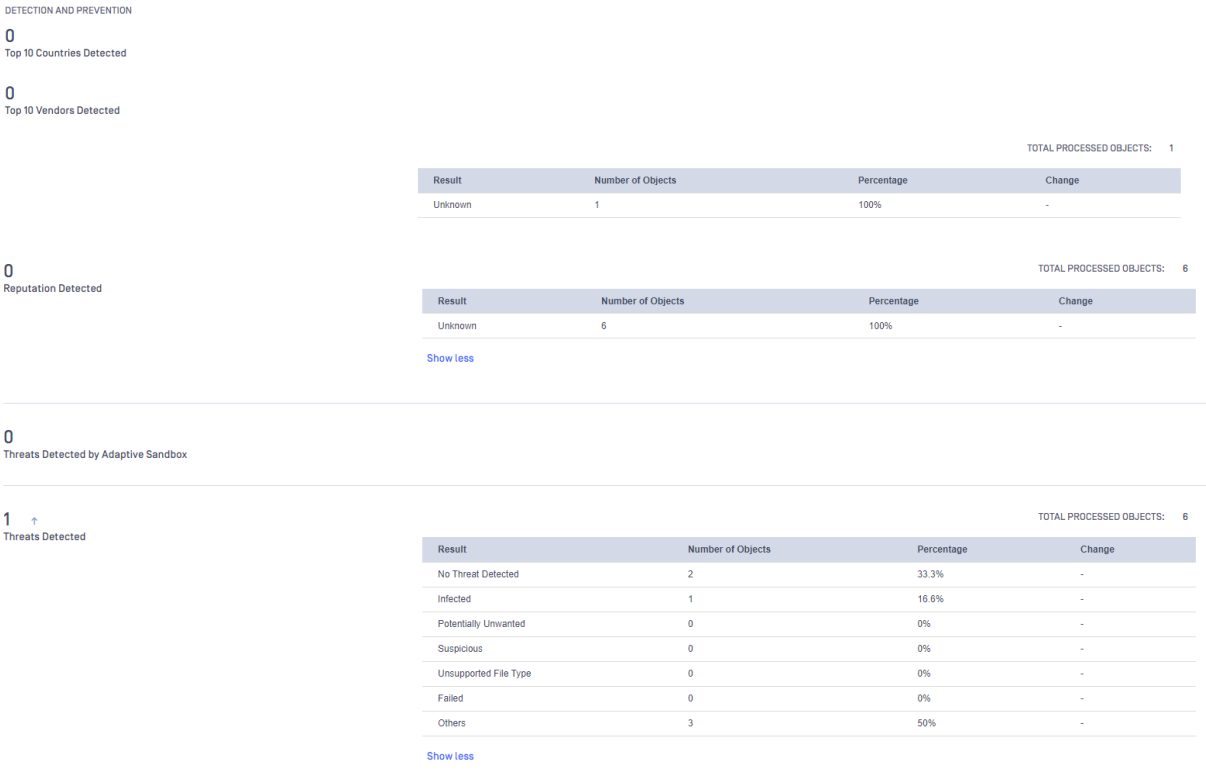


Figure 8 – Executive Report





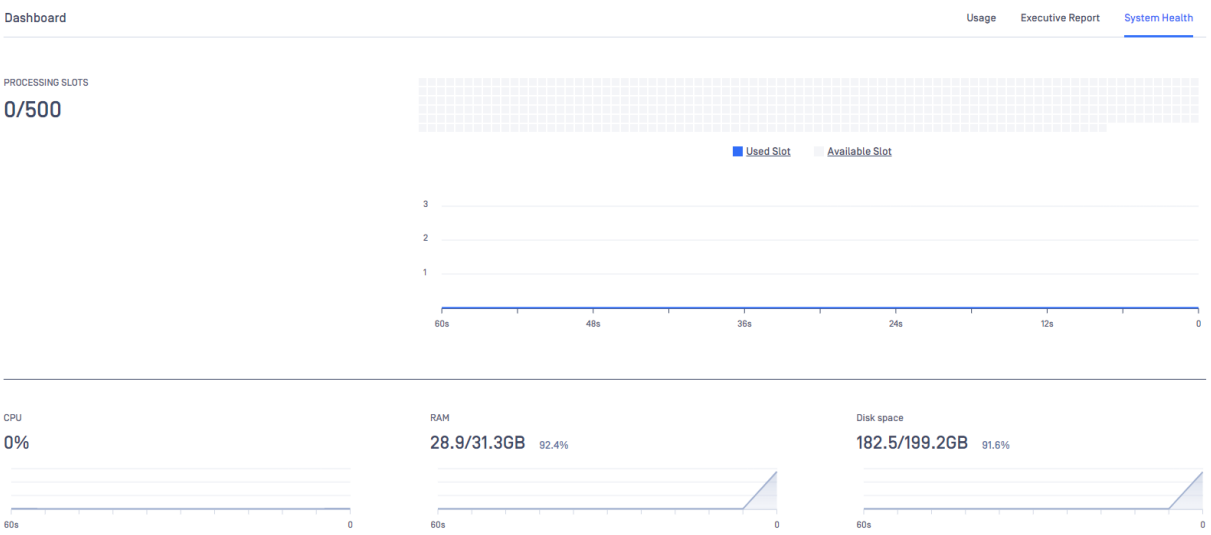




System Health page provides the current system resource status (CPU, memory and disk) and processing performance (scan queue) of MetaDefender Core server.

Administrators, Security administrators and Security auditor can access this page.

Figure 9 - System Health

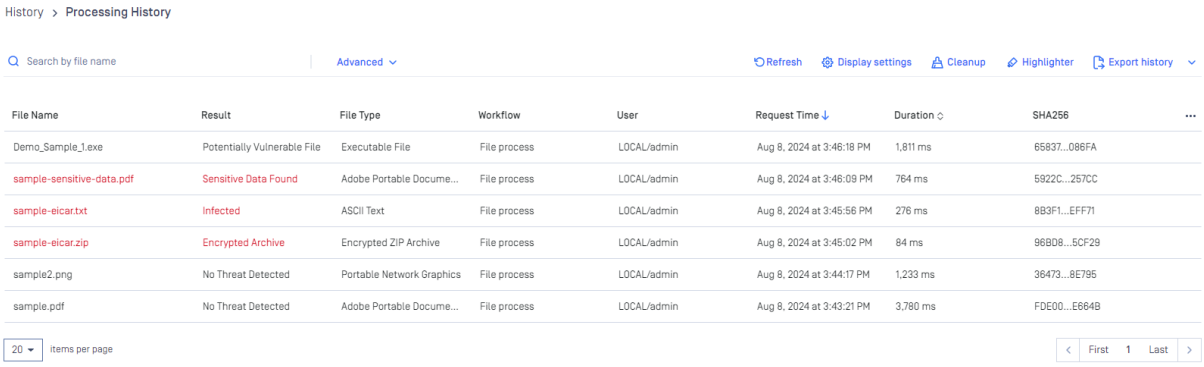


2.2.6 History

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

Administrators, Security administrators, Security auditor and Help desk can access this.

Figure 10 – Processing History

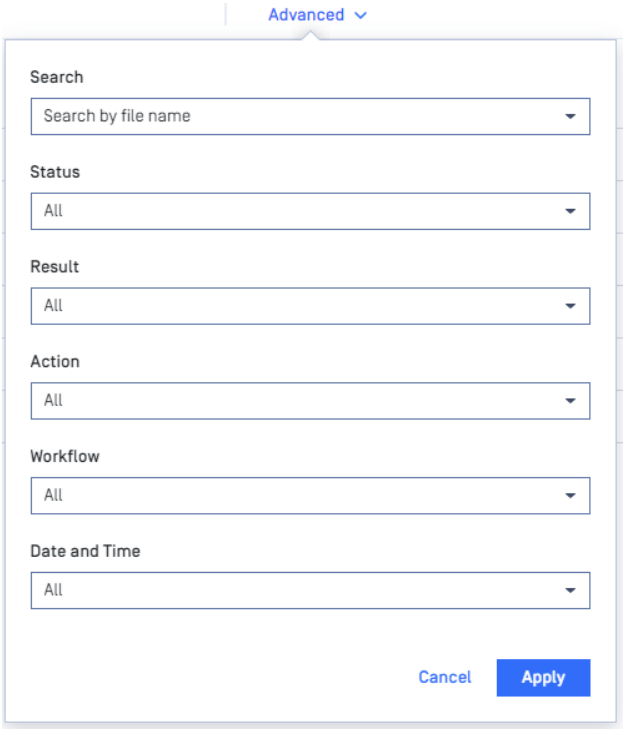


On the Processing History page, users can search for:

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

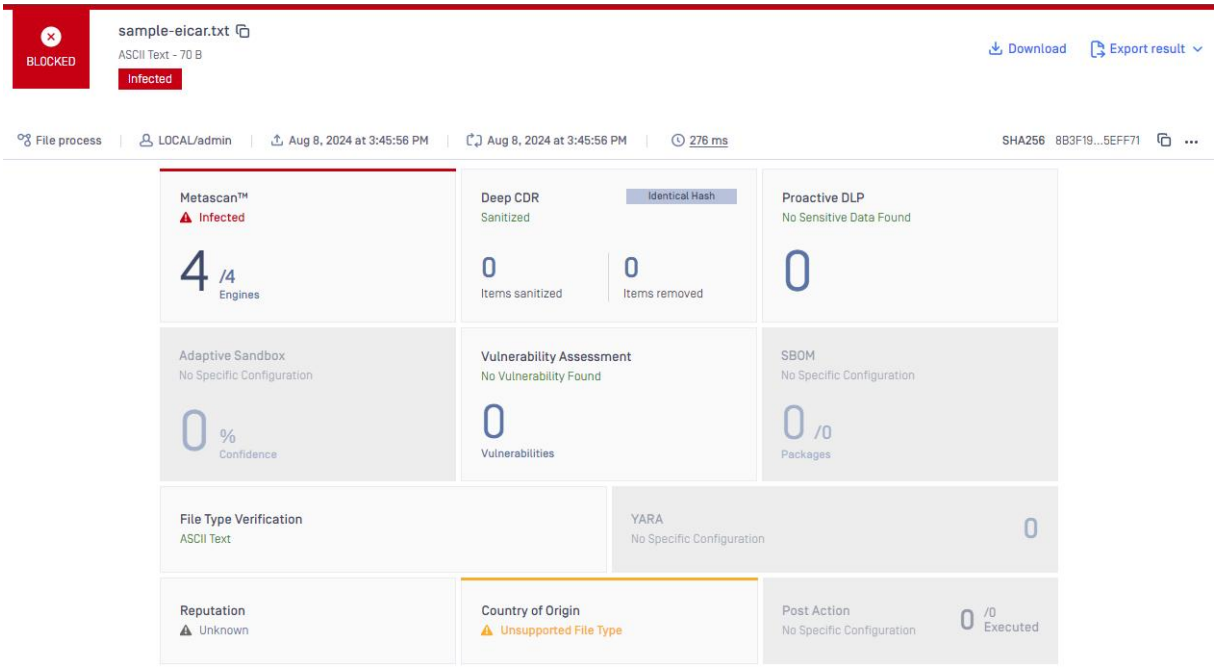
With many search filters: status, result, action, workflow, datetime.

Figure 11 – Processing History search filter



When clicking on a record, it will popup details for processing result, verdict and analyze details.

Figure 12 – Processing result



There is an option to export scan history in CSV or STIX format. For the export, the Result filter can also be applied.

Administrators, Security administrators, Security auditor and Help desk can access this.

- Users can export STIX file by clicking on STIX export button. In addition to set Result filter, STIX file will contain only blocked scans. After the desired time range is 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.

Figure 13 – Export history

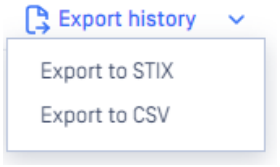
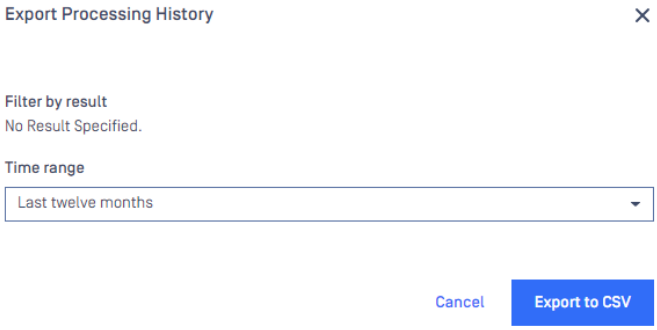


Figure 14 – Export history with filter



For more details, please see chapters “Processing history”, “Quarantine”, “Update history” and “Configuration history” of [MDCore].

2.2.7 Workflow Management

MetaDefender Core can be configured to use different scanning profiles (Workflow Rules) for different clients. Users can tailor workflow rules for their desired purpose and use case.

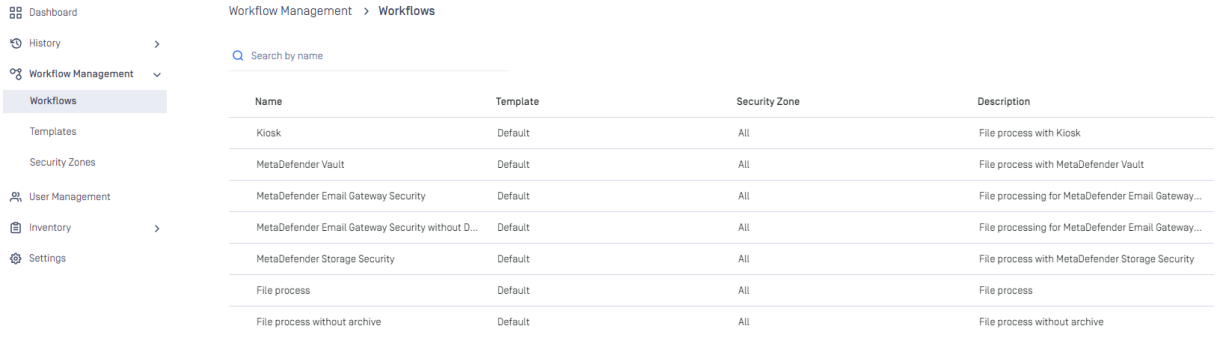
When MetaDefender Core receives a scan request through REST API, it will match the source address through the zones in the list of rules and apply the first matching rule's workflow. The processing request then will be processed based on this specific workflow.

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.

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.eAdministrators and Security administrators can access and make changes to this feature. Security auditor and Help desk can view only.e

For more details, please see chapter “Workflow Configuration Template” of [MDCore].

Figure 15 – Workflow Management



2.2.8 Inventory

Modules: display all the installed engines with details such as engine type, engine version, definition version, status, elapsed time since last update, etc.

Skip by hash: where Administrators can define rules on what files (hashes) should be in blocklist/allowlist, which engines should skip what files.

Certificates: on this page, the path to certificates and private keys for signing scan batches or HTTPS configuration can be configured.

Webhook Authentication: Administrators can request MetaDefender Core to generate a private-public key pair which is used for hardening the security of authentication between the application and client while using Webhook.

External scanners: where Administrators can configure their scanner so that the application integrates and operates the scanners as its own scan engines.

Post actions: Administrators can add and configure a post action which runs after the scan of the file for any post functionality such as copying files, etc.

Password storage: Administrators can add and manage a list of password storage which contains 10 passwords at max. The product will use those passwords for file decryption.

Administrators and Security administrators have full permissions on the configuration under Inventory including Modules, Certificates, Webhook authentication, External scanners, Post actions, Skip by hash settings.

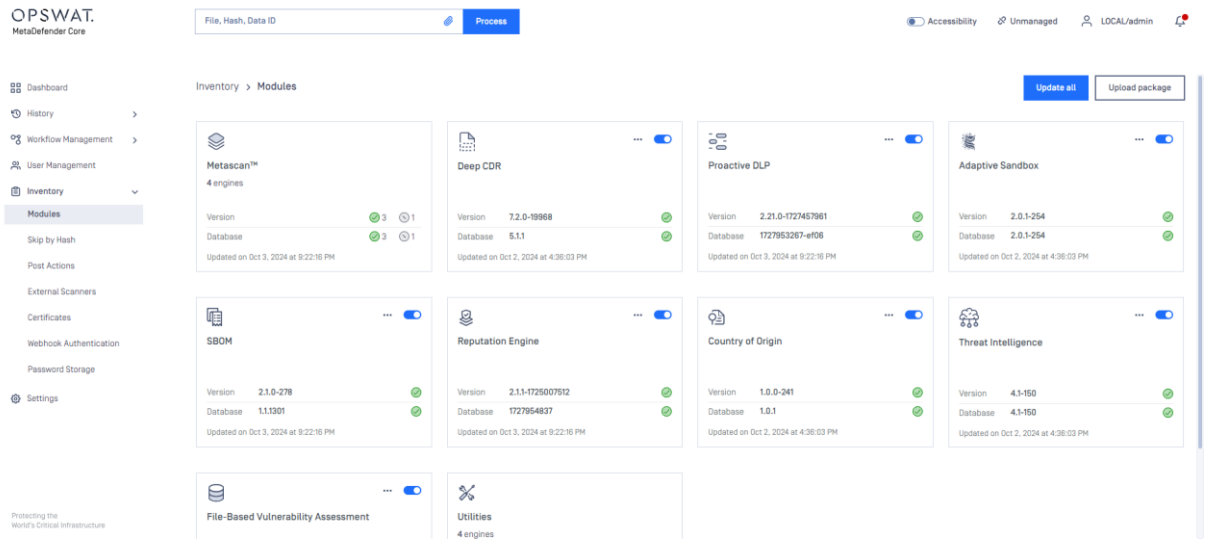
Administrators have full permission to Password storage.

Security auditor can view those settings only.

Help desk can view Modules, Post actions, External scanners, Skip by hash settings. Help Desk cannot view Certificates, Webhook authentication, Password storage.

For more details, please see chapter “Inventory management” of [MDCore].

Figure 16 – Inventory\Modules



2.2.9 User Management

MetaDefender Core provides a feature for managing users, groups, user directories and roles. User can find it in Settings > User Management menu in the Core Management Console.

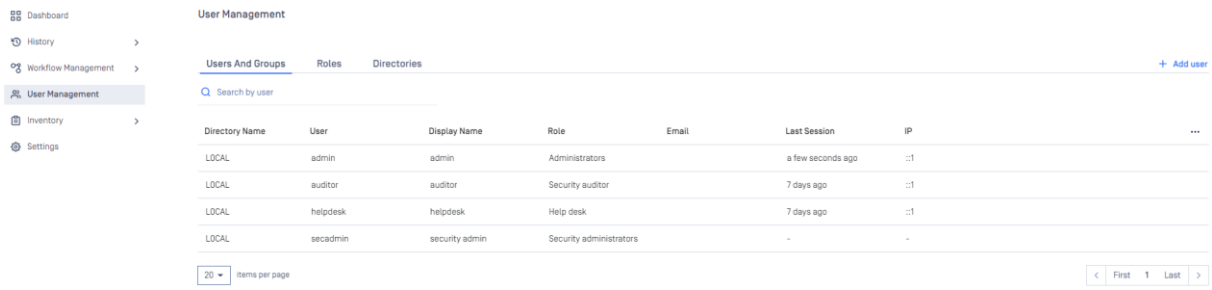
Administrators can

- Add a new user or AD group
- Modify (and view) existing user's or AD group's properties
- Delete an existing user or AD group

Administrators can access and make changes to this feature. Security administrators and Security auditor can view only. Help desk cannot access this feature.

For more details, please see chapter “User management” of [MDCore].

Figure 17 – User Management



2.2.10 General Settings

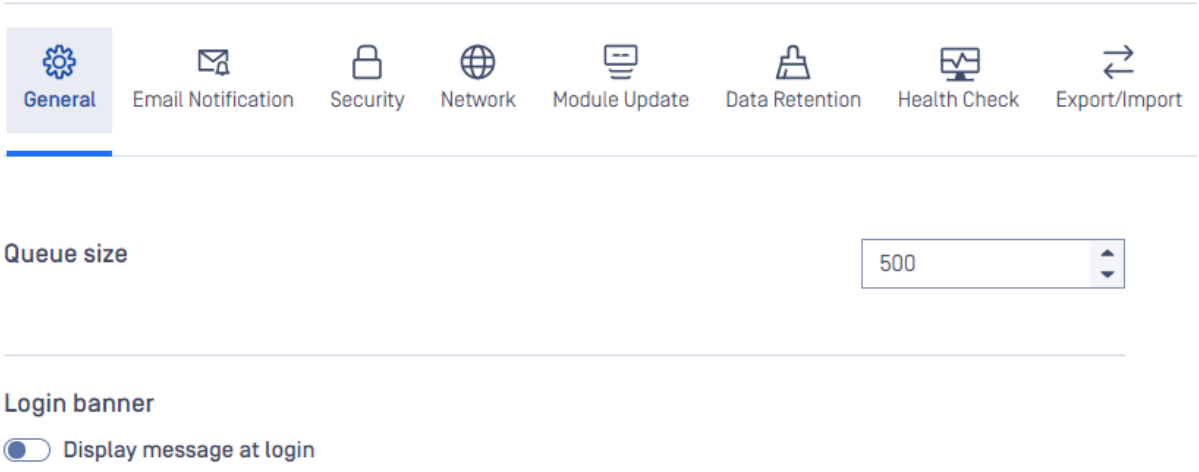
This consists of many settings of MetaDefender Core:

- Email Notification
- Security
- Network
- Module Update
- Data Retention
- Health Check
- Export/Import

General: Including queue size setting and login banner setting.

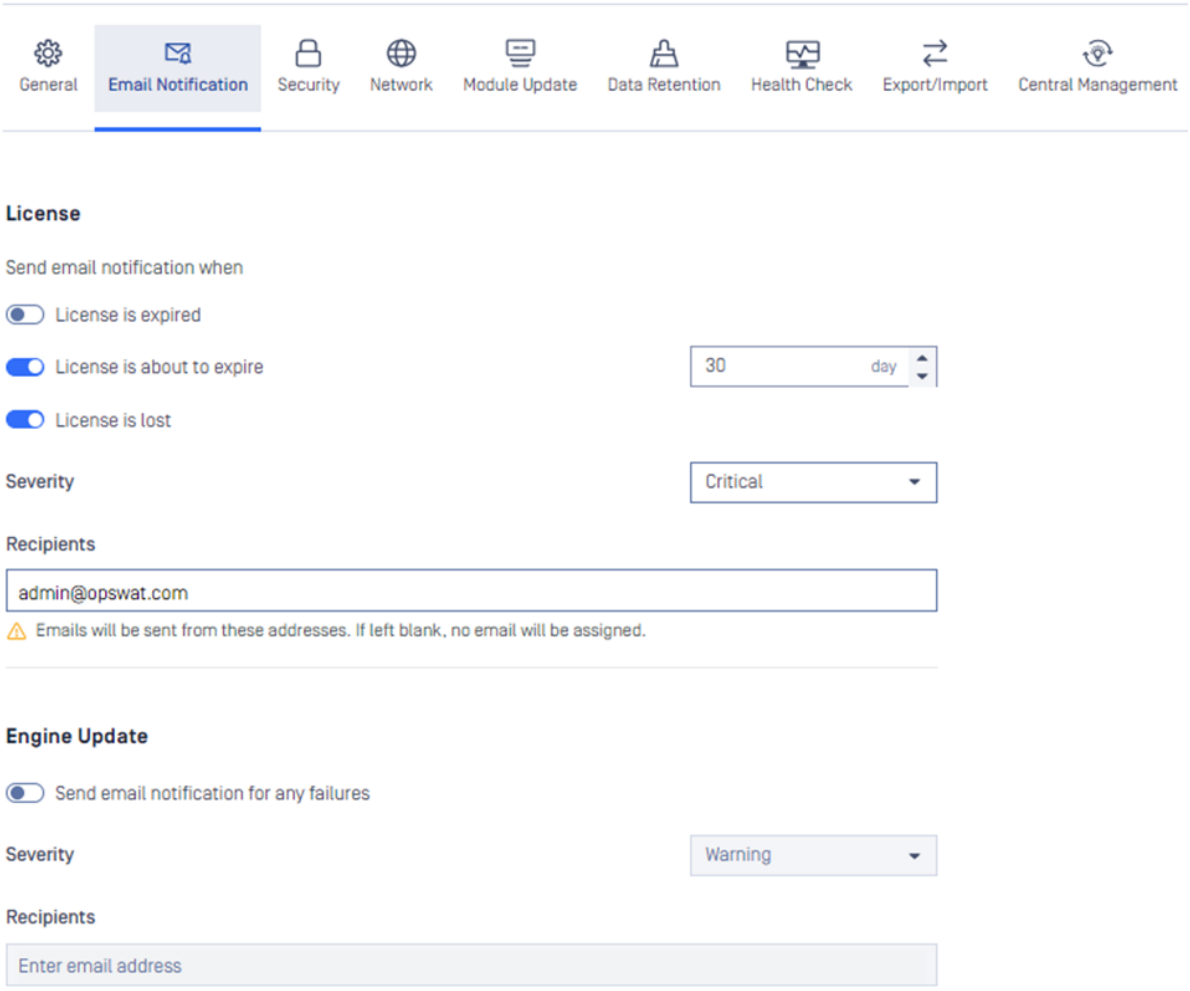
The Administrators and Security administrators have full permission to configure queue size setting. Security auditor and Help desk can view only.

The Administrators has full permission to configure the login banner setting. Security administrators, Security auditor, Help desk cannot access the setting.



Email Notification: Administrators has full permission to configure this setting. Security administrators, Security auditor, Help desk cannot access the settings.

For more details, please see the chapter “Email Notification” of [MDCore].

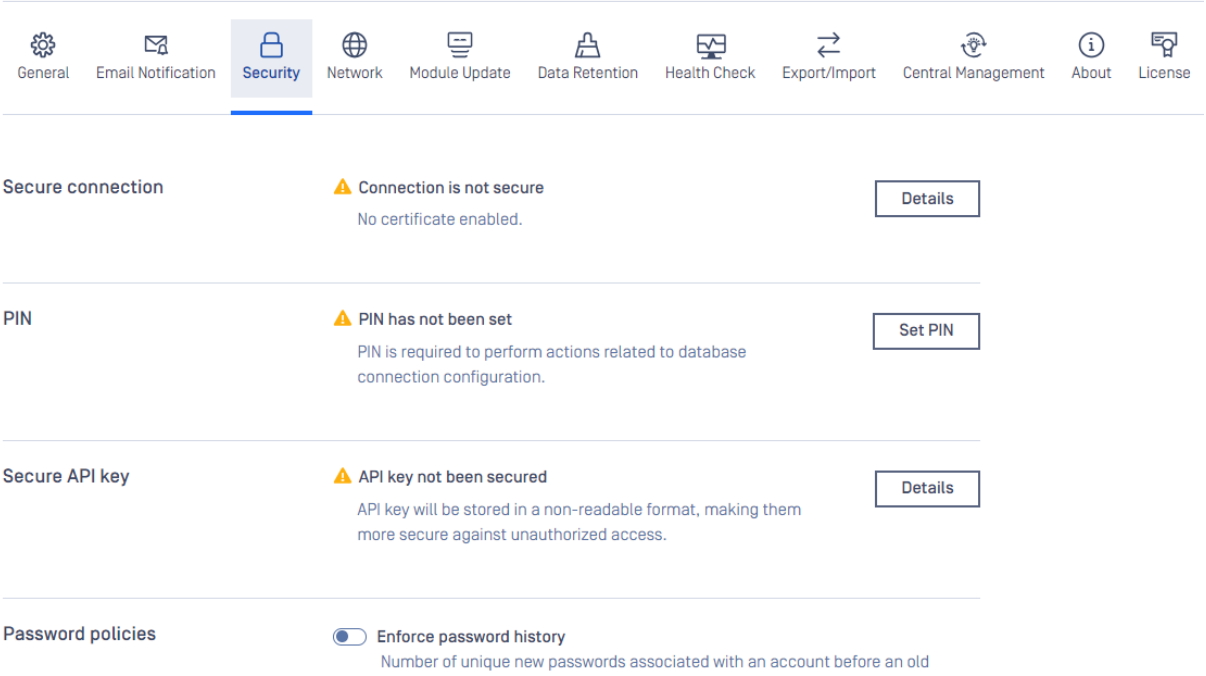


Security: Administrators can configure HTTPS, Password policy, Session timeout, etc. Security administrators can configure HTTPS only. Security auditor can view only. Help desk cannot access these settings.

For more details, please see the following chapters of [MDCore]:

- Password Policy
- Session Timeout
- Enabling HTTPS

Figure 18 - Security settings



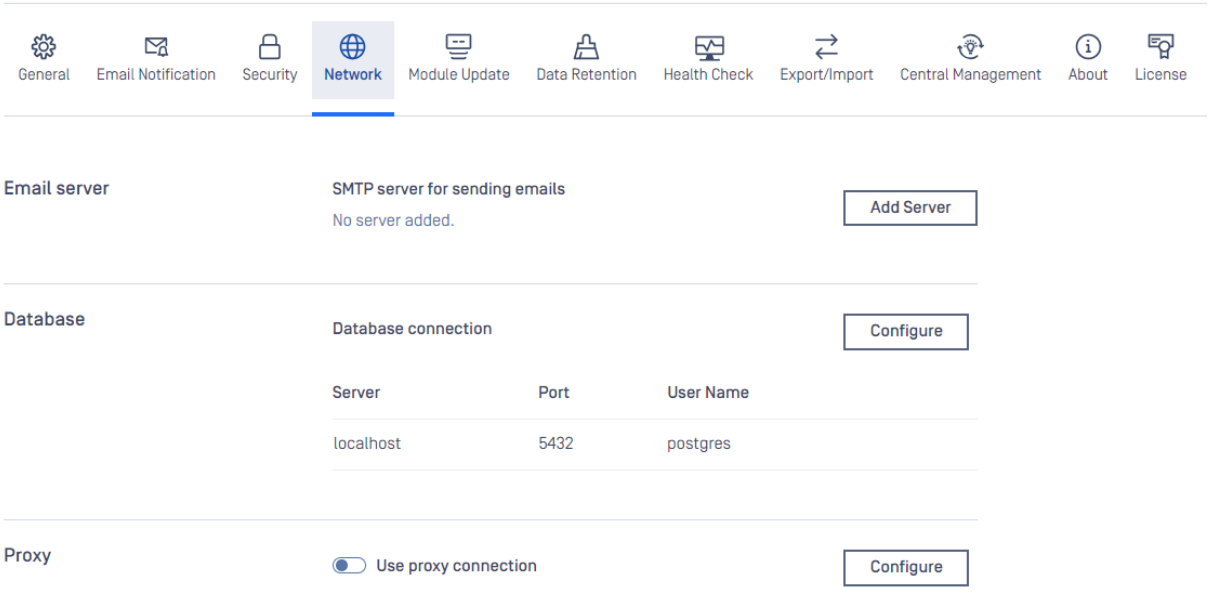
Network: users with administrator privilege on MetaDefender Core are allowed to

- Setup email configurations for SMTP to enable password recovery feature.
- Configure proxy setting and authentication.
- Configure database connection and authentication

For more details, please see the following chapters of [MDCore]:

- Database Management
- Email Configuration
- Proxy Configuration

Figure 19 – Network settings

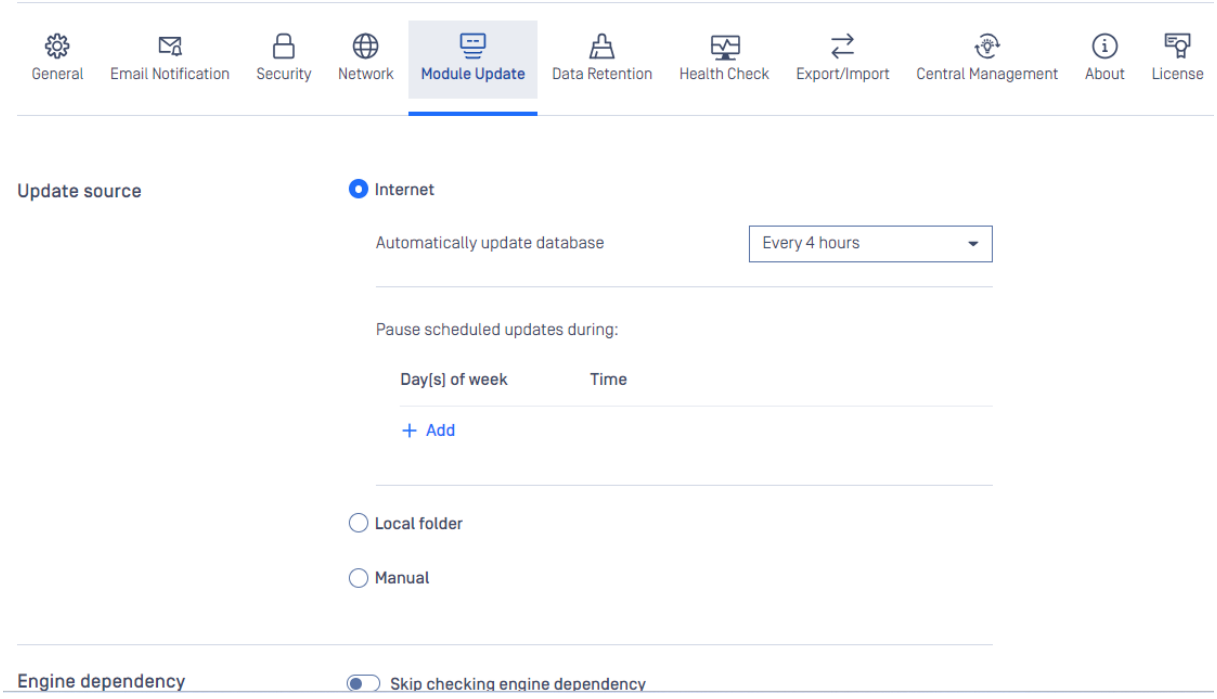


Module Update: these settings provide different methods of module update mechanism.

Administrators and Security administrators can make changes to these settings. Security auditor can view only. Help desk cannot access it.

For more details, please see chapter “Engines Update Configuration” of [MDCore].

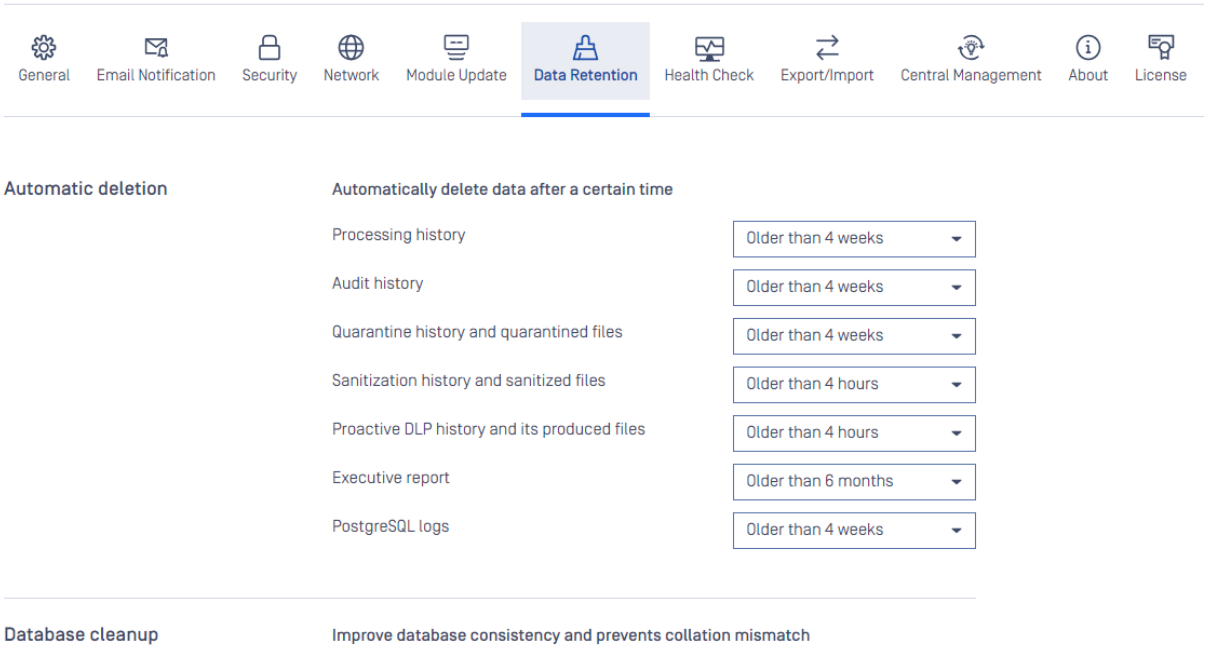
Figure 20 – Module Update settings



Data retention: Administrators is allowed to configure data retention settings to automatically clean up scan results, quarantined files, audit log, statistics, sanitized files, Postgres logs if it is older than the defined value.

For more details, please see chapter “Data Retention” of [MDCore].

Figure 21 – Data retention settings

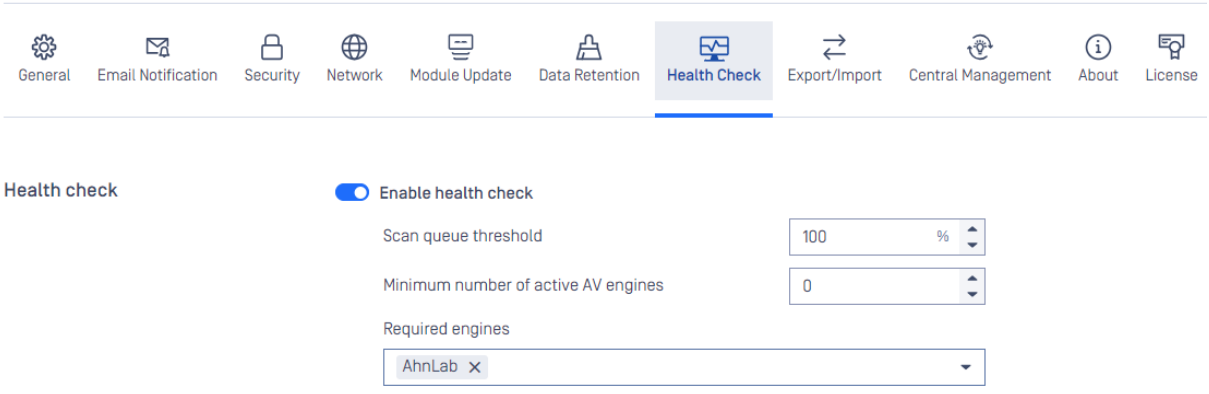


Health check: supports you to verify MetaDefender Core readiness in terms of file processing and licensing, before deciding to submit files and avoiding time and resources being wasted predictably.

Administrators and Security administrators are allowed to configure health check settings. Security auditor can view only. Help desk cannot access the settings.

For more details, please see chapter “Health Check API Configuration” of [MDCore].

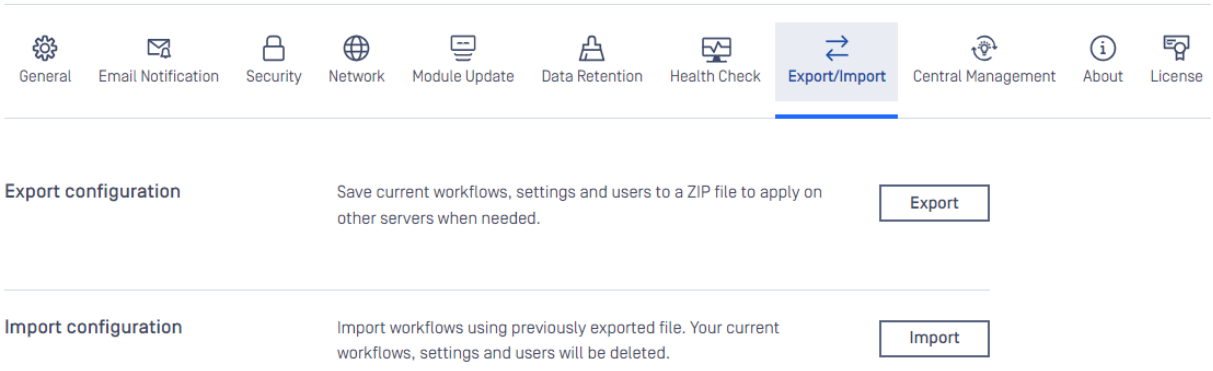
Figure 22 – Health check settings



Export/import: only the Administrators can export and import the current configuration and workflow rule of the MetaDefender Core application.

For more details, please see chapter Import/Export configuration of [MDCore].

Figure 23 – Export/Import



2.2.11 Licensing

There are 4 different options for product activation:

- Online activation: MetaDefender Core will connect directly to the OPSWAT licensing server online, and acquire its license based on your Activation key and its Deployment ID.
- License Management Server: Requiring a separate product called License Management Server. Administrators need to provide host, port, and token to connect to that server.
- Offline activation: Requiring you to upload a license file (.yml). That license file could be retrieved by activating your license via OPSWAT Portal. Follow the instructions displayed for details.
- Request trial key online: For evaluation purposes, you can receive a trial Activation key via email. Follow the instructions displayed for details.

For more details, please see chapter “License Activation” of [MDCore].

The Administrators and Security administrators can view this page. Only the Administrators can deactivate or activate license.

Figure 24 – License information

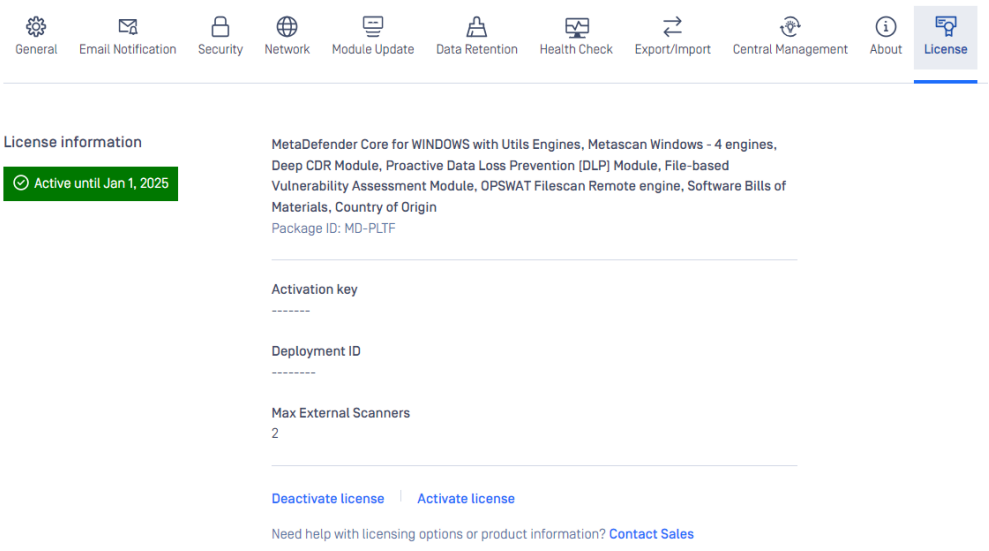


Figure 25 - License activation

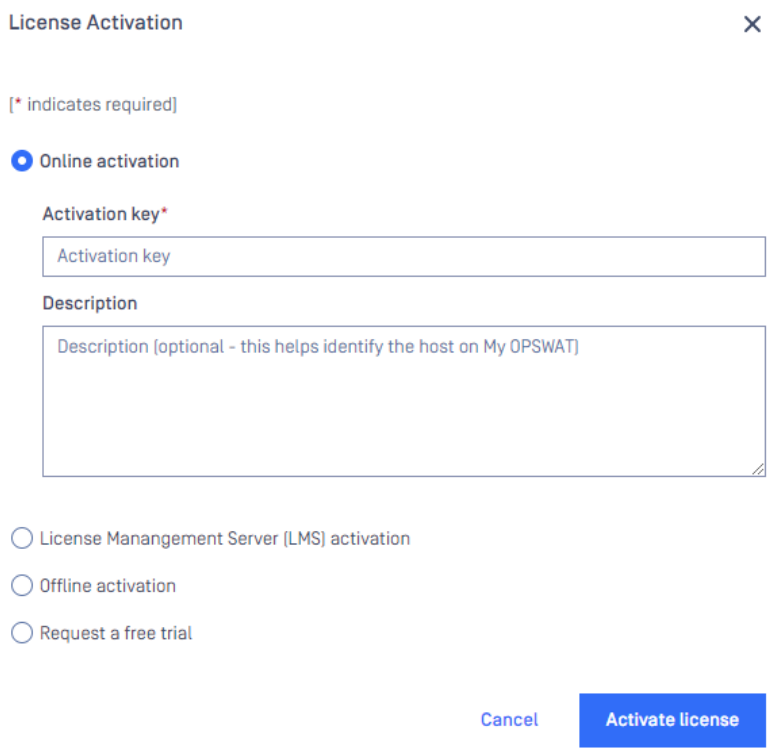


Figure 26 – License management server activation

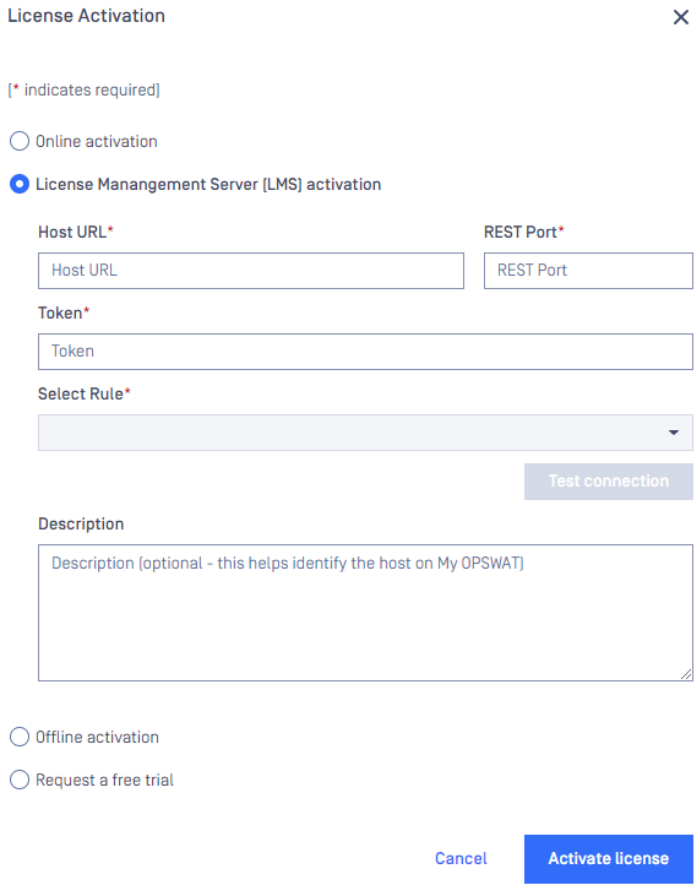
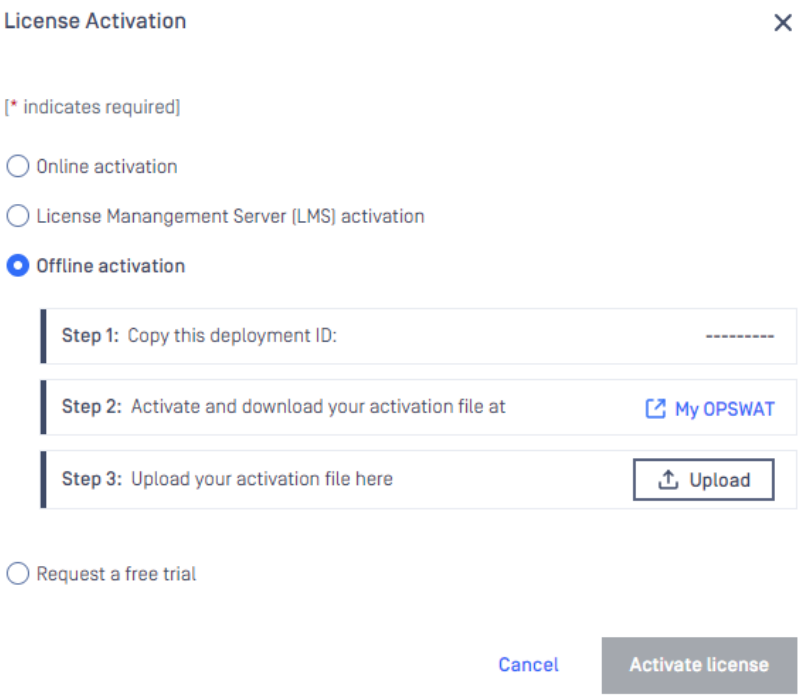
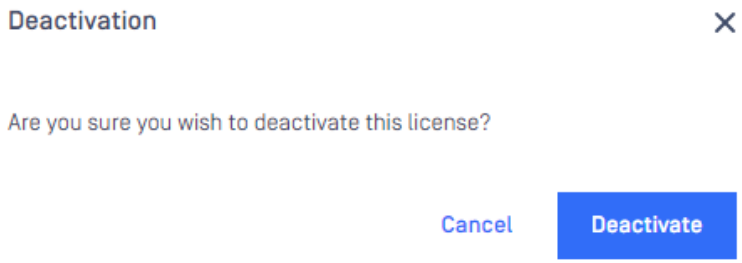


Figure 27 – Offline activation



Only Administrators can deactivate a license.

Figure 28 – License deactivation



2.3 MetaDefender Kiosk functions

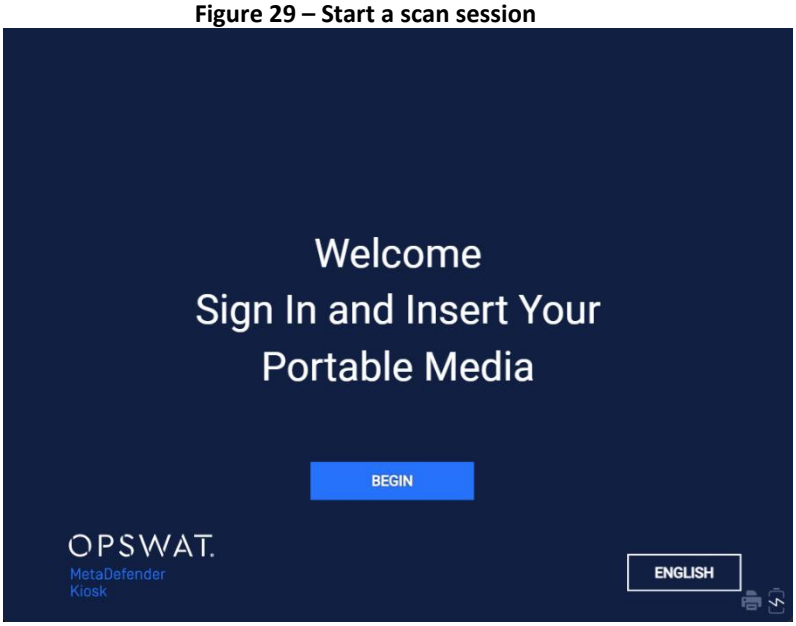
2.3.1 Application UI

Purpose/Method of use: KIOSK provides a user-friendly interface to perform file scanning tasks. MetaDefender Kiosk helps protect your network by enabling control over the flow of data into and out of your organization. It can be deployed as a media scanning station on your own hardware or on OPSWAT's custom-made kiosks.

To use the KIOSK application, follow these steps:

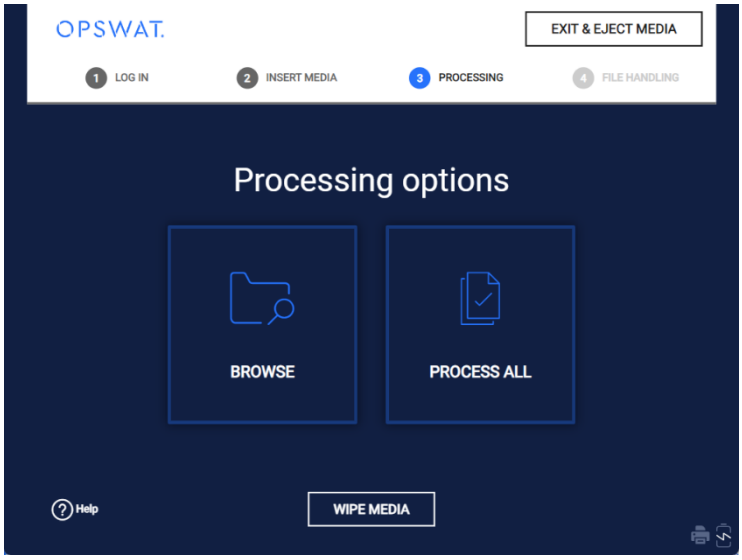
1. **Initiate the session:**
   The user interacts with the Application UI to start a session. The user must read and accept the disclaimer before proceeding with authentication (Guest/Employee).

Figure 29 – Start a scan session



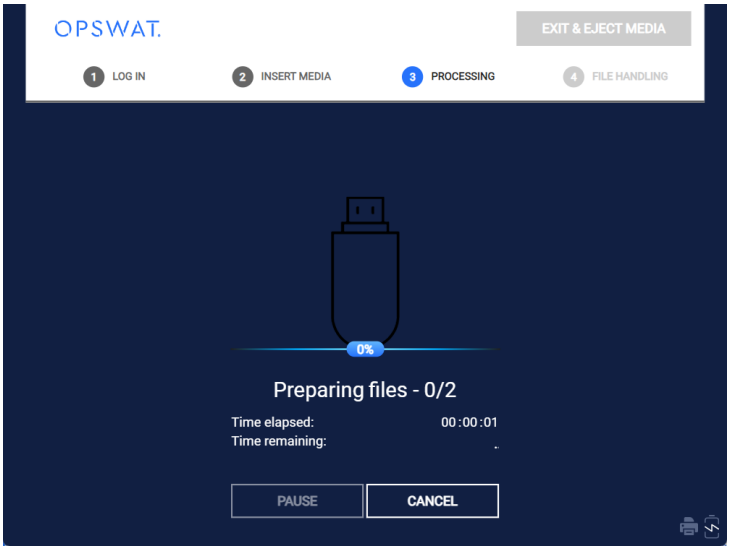
2. **Prepare the Media:**
   Insert the media you want to scan, such as USB devices, DVDs, SD cards, flash drives, or floppy disks, into the appropriate port on the KIOSK station.
3. **Initiate the Scan:**
   The KIOSK interface will guide you through the scanning process. Select the scanning options as needed and start the scan.

Figure 30 – Scanning options



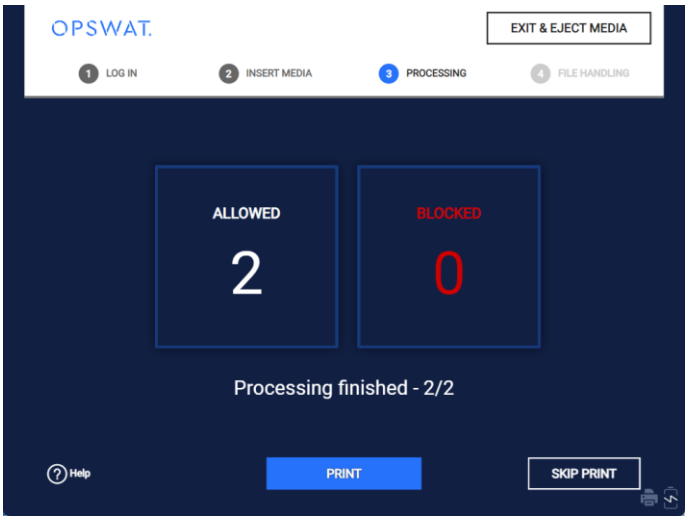
4. **Processing the Media:**
   KIOSK will analyze the content of the inserted media, scanning for any potential threats or unwanted data according to the configured security policies.

Figure 31 – Scanning progress



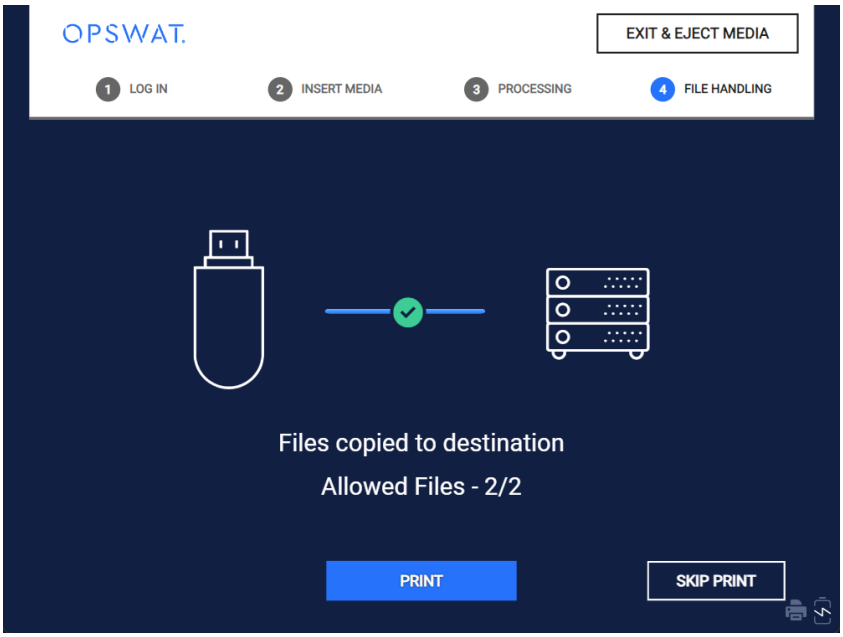
5. **Review the Results:**
   Once the scan is complete, KIOSK generates a detailed report. Review the report to understand the status of the scanned files, including any actions that were taken (e.g., files blocked or sanitized).

Figure 32 – Review result



6. **Next Steps:**
   Depending on the results, you can choose to allow the files, sanitize them, or take other necessary actions as recommended by the report.

Figure 33 – Scanning options



For more information see section **Using the Kiosk User Interface** in [MDKiosk].

2.3.2 File discovery and transfer

Purpose/Method of use: KIOSK provides a function that lists all files on a removable device, allowing users to select either the entire content or specific files within the device for scanning. After the user selects the files to be scanned, KIOSK transfers these files to MetaDefender Core for analysis and scanning. The results are returned via a REST API response.

For more information see section **Processing Digital Media** section at [MDKiosk].

2.3.3 Database Connect

Purpose/Method of use: Database Connect is utilized by various components within the system, including KIOSK UI, Services, and KIOSK Console management, to retrieve necessary data and display it to the user. To establish a connection to the database, components make requests through the Kiosk Main Service. The Kiosk Main Service then connects to the database (MongoDB) to query the required data. All database connections to MongoDB are made through port 27019 and secured with a password.

Parameters:

- Database connection server: localhost:27019
- Database name: metadefender
- Authentication credentials: KioskAdmin:<password>

2.3.4 Dashboard

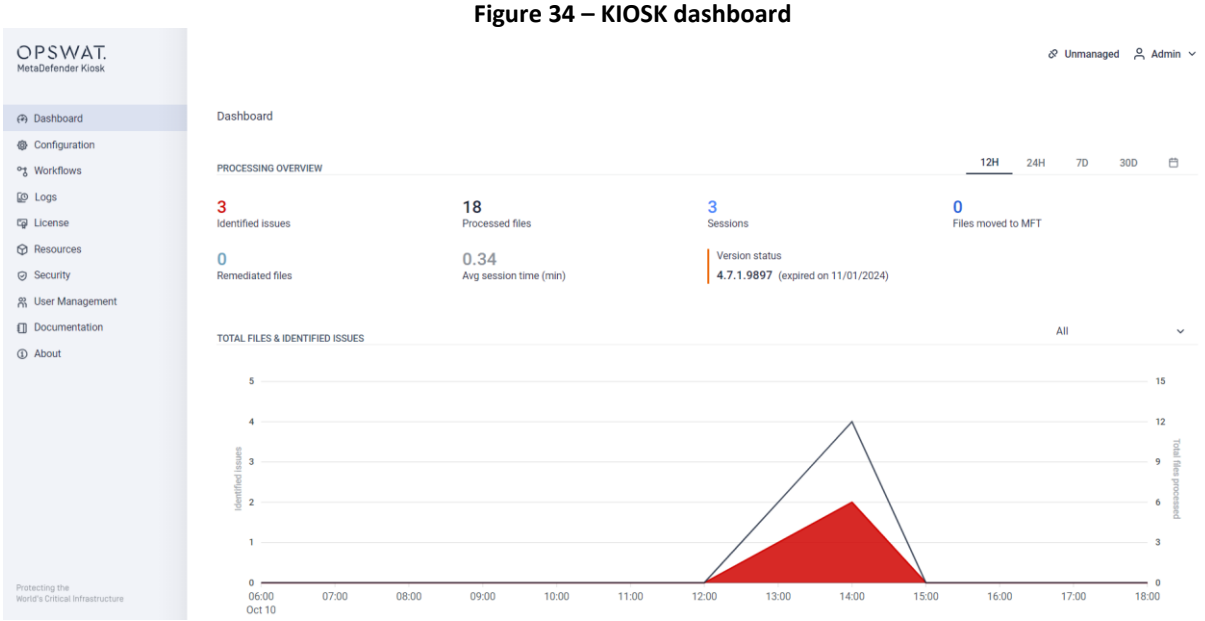
The Dashboard will be the first page that is seen when logging in to the MetaDefender Kiosk Management Console. This page provides a summary of all of the files that have been processed by MetaDefender Kiosk.

Administrators can view the following overall information about the Kiosk system:

- **Instance Information**: Displays license details and the currently installed Kiosk version.
- **Overall Scan Results**: Shows the total number of files/sessions processed by the Kiosk, the number of files with detected issues and those remediated, and the average time/files processed per session.
- **Top File Types**: Provides statistics on the most frequently processed file types with Kiosk.

Additionally, Administrators can select a time range to query the above information.

Figure 34 – KIOSK dashboard

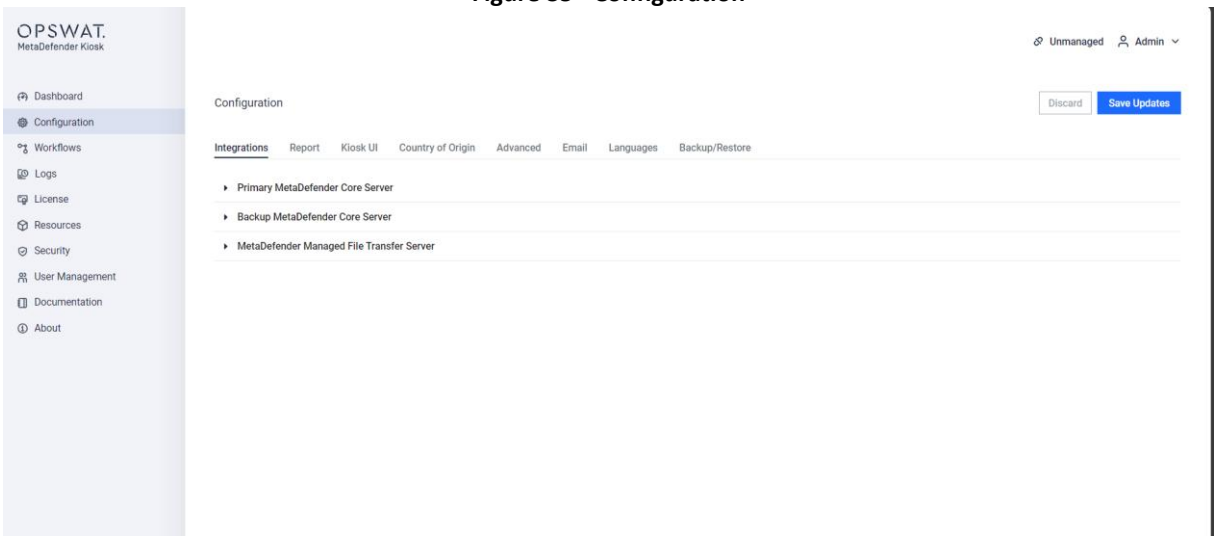


For more information see section **Dashboard** in [MDKiosk].

2.3.5 Configuration

The Configuration page allows you to configure all MetaDefender Kiosk settings that apply to all users of MetaDefender Kiosk. Detailed configurations can be found in the chapter 'Configuring Global Kiosk Settings' in the [MDKiosk] user guide

Figure 35 - Configuration

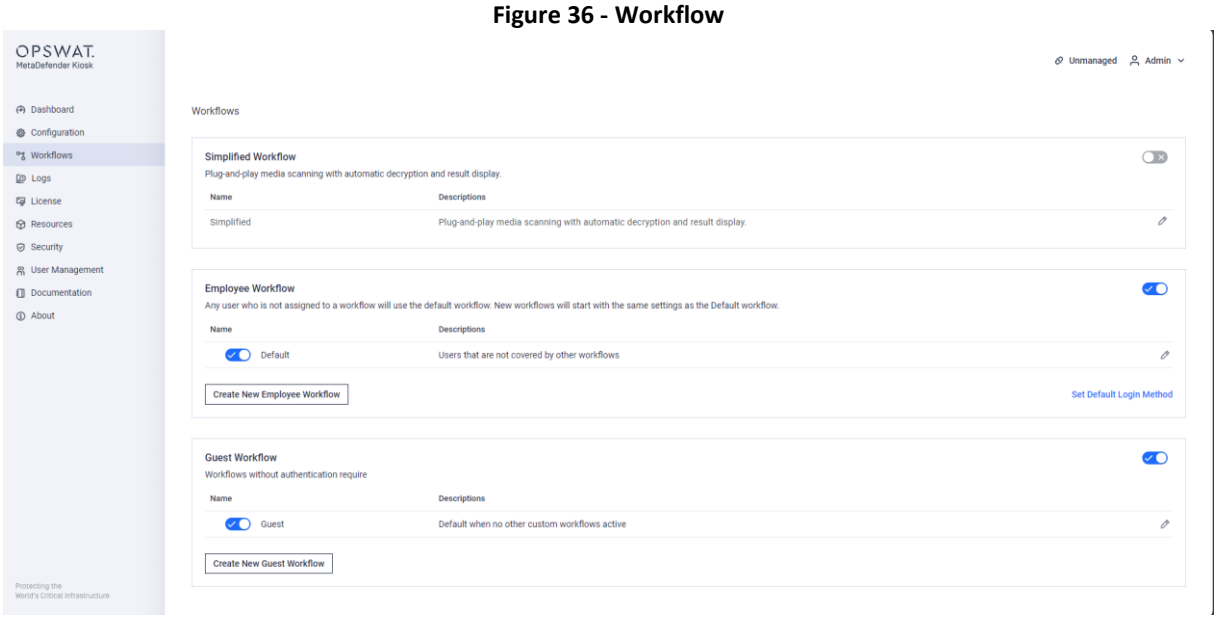


For more information see section **Configuration** in [MDKiosk].

2.3.6 Workflow

Workflows can be created or edited on the Workflows page of the Kiosk Management Console. Workflows define sets of individual work behaviors for different users/groups/guests.

Figure 36 - Workflow



There are 3 workflow groups: Simplified, Employee and Guest group. Workflows in the Employee group require authentication while the Guest and Simplified do not. Each group can

be enabled or disabled but there must be at least one group enabled at a time. If Simplified group is enabled, Employee and Guest groups are disabled, and vice versa.

In each group, there must be at least one workflow enabled. The default workflows in each group are created and enabled by the installer. However, the default workflow in each group might be disabled after the upgrade to keep consistent to the settings of previous version. Any workflow can be edited even its group is disabled. Default WF in each group cannot be deleted, but editable.

For the Simplified group, only the Simplified workflow is created and set as the default workflow. See How do I use Simplified workflow for more detail.

For the Employee group, each user or user group can join multiple workflows but only one workflow is selected for a session. Users that are not included in any workflows will be assigned to the Default. Each user or group can join multiple workflows but only one workflow is selected for a session. See 9.1. Logging In on the User Authentication Screen for more details

Note: *Any users that are not included in one of the defined workflows will be assigned the Default workflow (if "Default login" is enabled).*

For the Guest group, there is a bit different from the Employee. The administrator can create additional custom guest workflows but there must be either default guest workflow or customs are enabled. The default and custom guest workflow should never be both enabled at the same time.

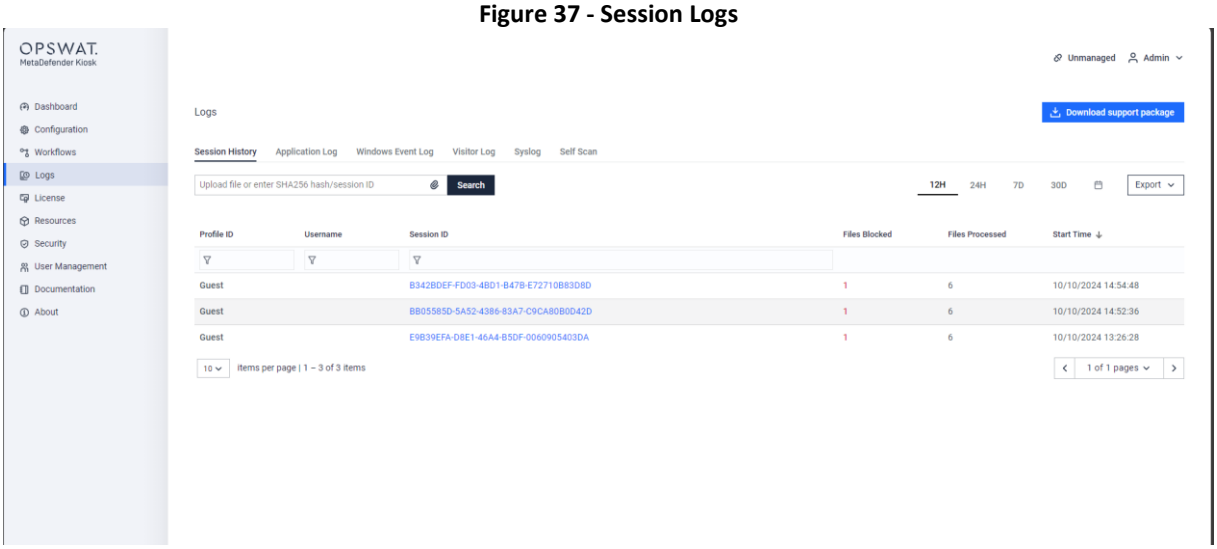
For more information see section **Kiosk Workflows** in [MDKiosk].

2.3.7 Session Logs

1. **Viewing session details**

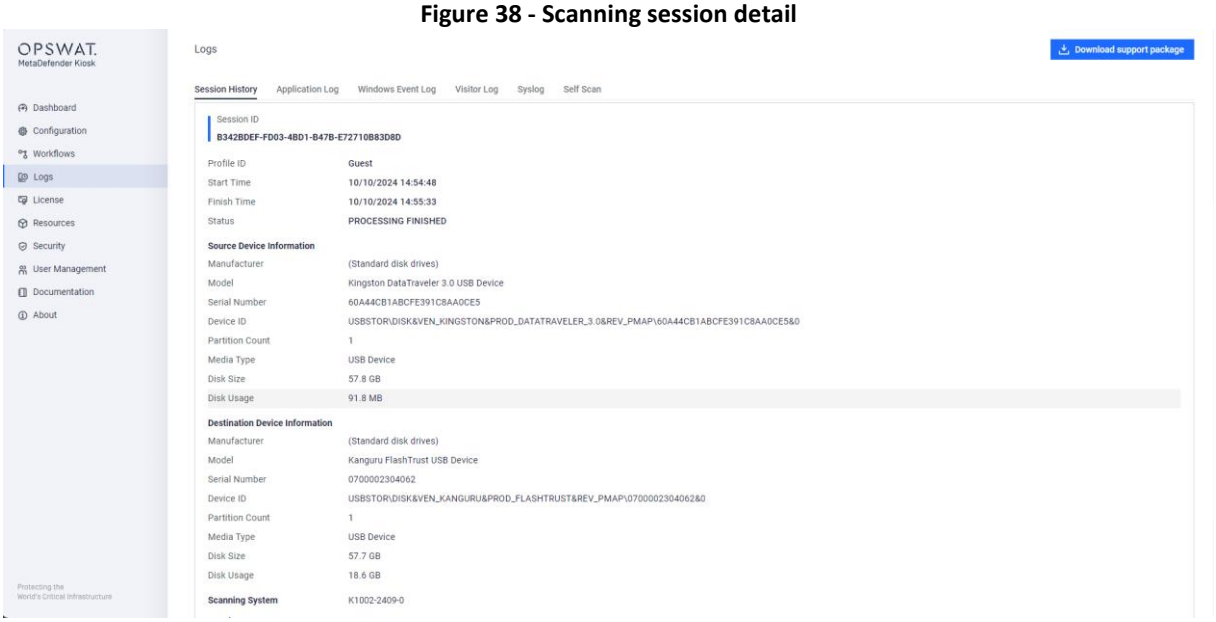
MetaDefender Kiosk displays the most recent scanning sessions on the Logs page.

Figure 37 - Session Logs



You can select any of these sessions to view details from that scanning session.

Figure 38 - Scanning session detail



Similarly, you can click see the details of each file in the list of total files processed.

Figure 39 - Details per files

Results

Result	File Name	File Type	Start Time
Infected	D:\eicar.txt	ASCII Text	10/10/2024 14:54:49
No Threat Detected	D:\transparent.png	Portable Network Graphics	10/10/2024 14:54:49
No Threat Detected	D:\ca.pem	Security Certificate	10/10/2024 14:54:49
No Threat Detected	D:\Reenable_RDP.ps1	PowerShell Script	10/10/2024 14:54:49
No Threat Detected	D:\metadefender.sessions.json	JavaScript Object Notation	10/10/2024 14:54:49
No Threat Detected	D:\DS-1393.pdf	Adobe Portable Document Format	10/10/2024 14:54:48

2. Export Session or File History to CSV

The session or file history can be exported, on demand, to a CSV file based on the time range selected. Automated history export can be configured on the Configuration page.

Exported session history contains information on SessionID, User ID, Scan Start Time, Scan End Time, Total Files Scanned, Total Files Processed, Total Files Size, Total Files Skipped, Total Files Allowed, Total Files Blocked, Scanning System, Device ID, Device Type, Device Manufacturer, Device Model, Device Serial Number and User Question responses. Some sessions with secondary destination media will show the second at the next line.

Exported file history contains information on Session ID, User ID, File Name, SHA-256 hash, Scan Result, Scan Result Description and Scanning System.

3. Searching by file hash or session ID

You can also search MetaDefender Kiosk logs by either file hash (SHA256) or by MetaDefender Kiosk session ID on the Session History page. If you search by session ID, MetaDefender Kiosk displays a summary of the results of that session. For more information see section **Session Logs** in [MDKiosk].

2.4 Security Relevant Events

Table 5 – Security relevant events

Security relevant Event	Role	User function	Action to take
Unable to connect to MD Core	Administrator	KIOSK File Transfer	Verify the configuration of MD Core on the KIOSK Console to ensure its correct. Check the application log in the KIOSK Console for detailed connection error information. Perform a connection test between the KIOSK and MD Core.
License Expired	Administrator, Auditor	Application UI, KIOSK Console Management	The Administrator needs to activate the KIOSK license from the KIOSK Console.
Unable to connect to PostgreSQL database	Administrators	Database Connect	Administrators to check database connection, check PostgreSQL log for error information, try to restart PostgreSQL service and Core Main service.
License expired/invalid	Administrators	Licensing	Administrators need to purchase and activate a license for MetaDefender Core.
None	User/Guest	None	None
None	Security administrators, Security auditor, Help desk, Anonymous	None	None

2.5 Modes of Operation

There are two modes of operation for MetaDefender Core:

- Standalone Mode (for details please see section Standalone mode of [MDCore])
- Shared Database Mode (for details please see section Shared Database mode of [MDCore])

There is one mode of operation for MetaDefender Kiosk:

- Full screen hardened mode

2.6 Security Measures to be Followed

Table 6 - Security Objectives for the Operational Environment

Objective	Description
OE.ADMIN	Administrators shall be trustworthy and follow guidance.
OE.USER	Non-administrative users of the TOE shall be trustworthy and follow guidance.
OE.PHYSICAL	TOE components shall be protected from unauthorized physical access.
OE.TIME	The IT environment will provide a reliable time source.

3 Preparative Guidance

3.1 Acceptance of the TOE

The following step should be taken to confirm that you have received the correct version of the TOE:

a) OPSWAT software products are delivered to customers through an electronic download process. Once the purchase of a software product has been processed through the OPSWAT order fulfillment system, an activation key and download instructions are sent to the customer via email. A URL hyperlink to the portal website (https://my.opswat.com/) is communicated to the customer as part of the download instructions. The customer can check the validity of the installation package by verifying the SHA256 has posted on the my.opswat.com portal.

b) The customer registers on the OPSWAT portal and gets an email when access to the portal is granted. The customer logs in to portal and navigates to product download page. OPSWAT will inform the users about the Software reference that needs to be installed to be compliant with the current certification in [MDCore] and [MDKiosk]. Also, the customer can select the appropriate product version himself as specified in the TOE Security Target. The downloads are subject to digital signature verification as part of installation.

c) During the product installation, the customer is required to enter the activation key (delivered as part of the initial email) which enables the product to function. After the product is activated, depending on the package purchased, the application downloads entitled engines to the customer environment. Only after the entitled engines are downloaded, does the application function correctly.

The AGD Documentation, [MDCore], and [MDKiosk] are available on the following pages:

- https://www.opswat.com/docs/mdcore/v5.14.2/installation/metadefender-core-documentation
- https://www.opswat.com/docs/mdkiosk/v4.7.6/release-notes/release-notes
- OPSWAT MetaDefender AGD documentation (this document) is available on both links above with the corresponding hash value.

The hash values for integrity protection can be found in [ST] section 1.4.1.1 Guidance Documents, and also, they are available on the websites.

Every other product related documentation is available through the OPSWAT's Technical Documentation for OPSWAT Products page (https://www.opswat.com/docs/mdcore, https://www.opswat.com/docs/mdkiosk), where always the latest documentation is published.

3.2 TOE Installation

The installation information for both MetaDefender Core and MetaDefender Kiosk, could be found in the following sections and the referred sections of the user manuals [MDCore] and [MDKiosk].

3.2.1 MetaDefender Core

In chapter Recommended System Configuration of [MDCore] the minimum system requirements and third-party dependencies are listed.

3.2.1.1 Installation

The installation of MetaDefender Core for Windows and Linux is described in section Installation of [MDCore].

There are two modes of operation:

- Standalone Mode (one database per MetaDefender Core)
- Shared Database Mode (one database for more than one MetaDefender Core)

These modes of operation do not affect the operation of the MetaDefender Core, or the TOE, just defines the type on database connection used.

Add firewall exception rule to allow both inbound and outbound connections:

- Protocol: TCP.
- Port: 8008.

To prevent anti-malware products from interrupting ongoing scans when real-time protection is enabled, it is recommended to exclude the following from real-time protection:

- Exclude full installation path of MetaDefender Core.
- Exclude the temporary upload path used by MetaDefender Core.
- Exclude "engineprocess.exe", "engineprocess32.exe", "ometascan.exe", "postgres.exe" and "nginx.exe" processes.

The description can be found in chapter "Can local AVs interrupt ongoing scans?" of [MDCore].

3.2.1.2 Setup

After the installation a setup wizard helps the user to do the initial configuration of the TOE. The description of this process can be found in the Wizard Setup section of [MDCore].

After a successful installation and setup, the license should be activated. The description of the activation can be found in section License Activation of [MDCore].

Enabling “Detect file type mismatch” setting under Workflow Management / Workflows / [Workflow name] / File Type. This will block files if their actual file type differs from their file type extension.

To maximize the effectiveness of the scanning process and ensure that the system utilizes the full scope of licensed engines for scanning and protection, all engines included in the license should be enabled in Workflow Rule settings. You can also tick supported file types of each engine, configure filtering conditions to make the engine run correspondingly. The description can be found in section “Workflow Configuration Template” of [MDCore].

It is mandatory that users enable HTTPS for all network connections to the application. The instruction can be found in section “Enabling HTTPS” of [MDCore].

3.2.1.3 Product upgrading

The preparation and the upgrade process of MetaDefender Core is described in section Product Upgrading of [MDCore].

3.2.2 MetaDefender Kiosk

In section Kiosk System Requirements of [MDKiosk] the hardware, software, and security requirements. There are third-party dependencies listed which are also required.

3.2.2.1 Installation

The installation steps of the MetaDefender Kiosk can be found in sections Installing MetaDefender Kiosk Using the Install Wizard of [MDKiosk].

Mongo DB password is generated during installation. When installing using the Wizard, the user is able to input an encryption key as an additional layer of protection for the database. To enable this feature, the steps can be found in section Installing MetaDefender Kiosk Using the Install Wizard of [MDKiosk].

Add firewall exception rule to allow both inbound and outbound connections:

- Protocol: TCP.
- Port: 8009.

3.2.2.2 Setup

The initial configuration of MetaDefender Kiosk can be found in section Configuring the Kiosk Management Console for initial use of [MDKiosk].

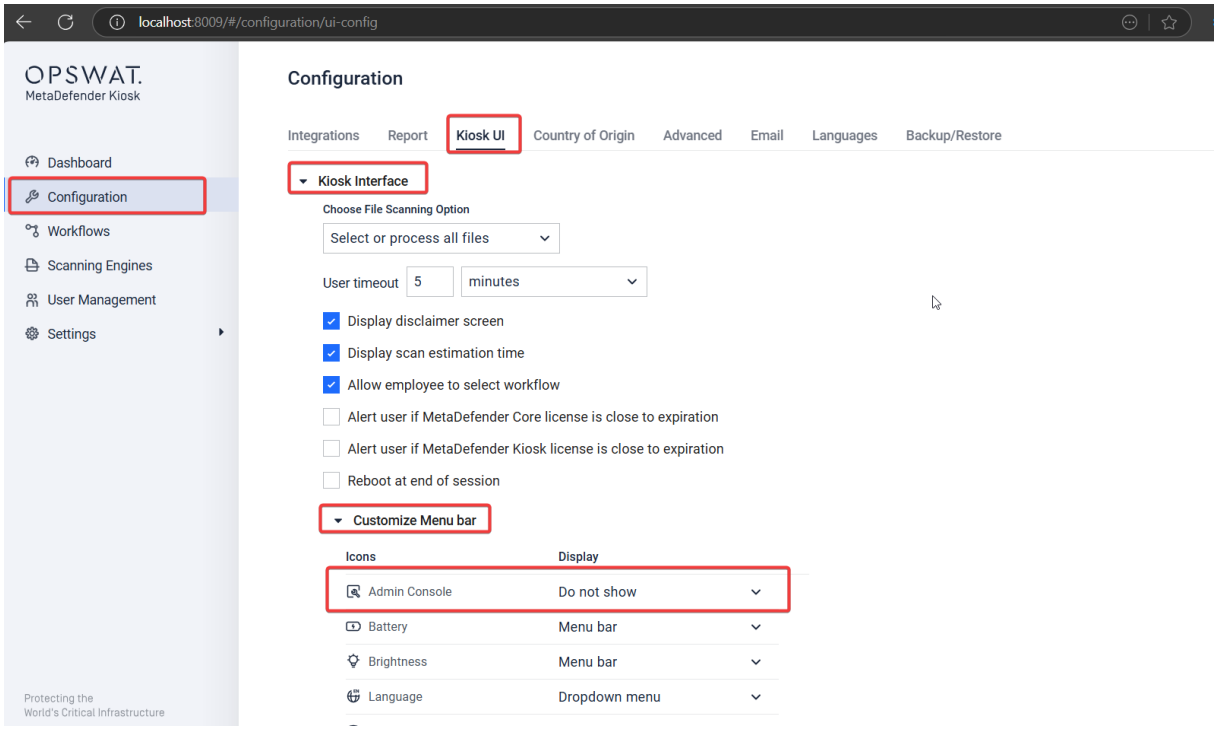
The license activation and management are described in the section Managing License Information of [MDKiosk].

It is mandatory that users enable HTTPS for all network connections to the application. The instruction can be found in section “Enabling HTTPS” of [MDKiosk].

To enhance system security, it is required to disable the "Admin Console" from the Kiosk UI by following the steps below:

- Login to the Kiosk Console Management interface.
- Navigate to the "Configuration" section.

- Go to the "Kiosk UI" tab.
- Expand the "Kiosk Interface" section.
- Expand the "Customize Menu Bar" subsection.
- Locate the "Admin Console" option.
- Set it to "Do not show".



This setting ensures that administrative functions are not accessible from the Kiosk user interface, thus reducing the surface area for potential misuse or unauthorized access.

3.2.2.3 Product upgrading

The upgrade process described can be found in the Upgrading MetaDefender Kiosk section of [MDKiosk].

4 Bibliography

[CC_P1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[CC_P2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[CC_P3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

[MDCore] MetaDefender Core - v5.14.2_2025-11-03.pdf, 2025-11-03

[MDKiosk] MetaDefender Kiosk - v4.7.6_2025-11-03.pdf, 2025-11-03

[ST] Security Target MetaDefender Core & MetaDefender Kiosk Evaluation Assurance Level (EAL): EAL4+, augmented with ALC_DVS.2, ALC_FLR.2, AVA_VAN.5, v1.9, 2025-11-03