OPSWAT.

MetaDefender

MetaDefender Vault Quick User Guide 1.2.6

Quick User Guide

Purpose of This User Guide

This is quick start user guide intended to cover the part you must know. For full user guide, go to https://onlinehelp.opswat.com/vault/.

Getting Started

Before Installation

Before you begin the installation, ensure that MetaDefender Vault System Requirements are met. If you are installing MetaDefender Vault on the same server as Metadefender Kiosk and/or Metadefender Core, the server must meet the cumulative system requirements of all the products.

To download Metadefender MetaDefender Vault, please visit OPSWAT Portal MetaDefender Vault section.

MetaDefender Vault Standalone Portal Deployment

MetaDefender Vault provides rich user interface for administrators and regular users. The installation consists of the following:

- Installing and configuring MetaDefender Vault, as described in Installing using The Install Wizard
- Configuring user access and user management, as described in Creating User Accounts Through Active Directory
- Optionally configuring the following to maximize MetaDefender Vault functionality:
    - Multi-scanning and Data Sanitization - Integrating Metadefender Core
    - Notifications

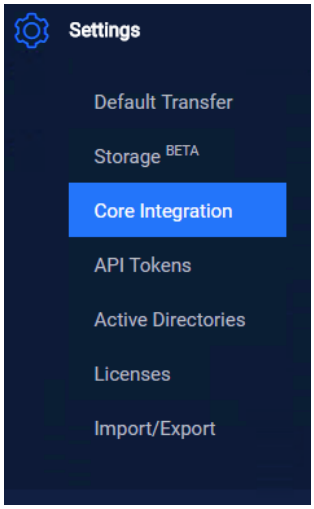
Deployment with Kiosk and Diode

MetaDefender Vault provides seamless integration with Metadefender Kiosk which helps protect your network by enabling control over the flow of data into and out of your organization. Metadefender Kiosk can be used as a media scanning station on your own hardware or on OPSWAT's custom-made kiosks. Typically, media such as USB devices, DVDs, card readers, SD cards, flash drives, or floppy disks, are scanned by Metadefender Kiosk by inserting the media device into the appropriate drive. The installation consists of the following:

- Install Metadefender Kiosk
- Configuring Kiosk to integrate to MetaDefender Vault

Integrating Metadefender Core

In order to integrate MetaDefender Vault with Metadefender Core please navigate to ***Settings*** → ***Core Integration*** in the left menu.



You can configure MetaDefender Vault to use the Metadefender Core add-on to specify

- Anti-malware multi-scanning
- Data sanitization (CDR)
- Other security criteria required for a file to be downloadable from MetaDefender Vault.

Use the Metadefender Core Management Console to configure a file scanning policy that encompasses your security criteria. This requires purchasing, installing, and configuring Metadefender Core.

Note that this user guide does not detail the Metadefender Core configuration steps; those steps are available in the Metadefender Core User Guide.

Advanced configuration and high availability

Follow Configuring MetaDefender Vault to work with Metadefender Core in order to configure Metadefender Core in MetaDefender Vault.

Follow Create a Metadefender Core rule that will apply only to MetaDefender Vault in order to create a Metadefender Core rule that only applies to files uploaded in MetaDefender Vault.

The following settings apply to all users and all files uploaded via MetaDefender Vault. Changing any of these setting will only affect files uploaded after the setting has been changed.

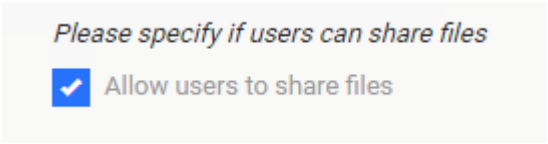
You can configure the default settings by going to ***Settings*** → ***Global Settings*** **.** Please note that you will need administrator privileges.

Authentication required / No authentication

This setting specifies if the files uploaded using MetaDefender Vault can be downloaded with or without requiring the user to log in before downloading.

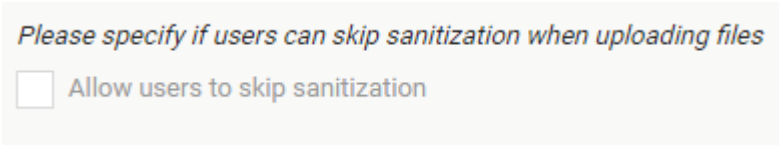
Allow users to share files

This option specifies if file sharing between users is allowed or not.



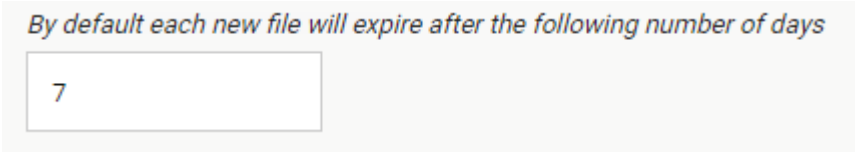
Skipping sanitization

This option, if turned on, allows users to specify if they would like to skip sanitization when uploading files.



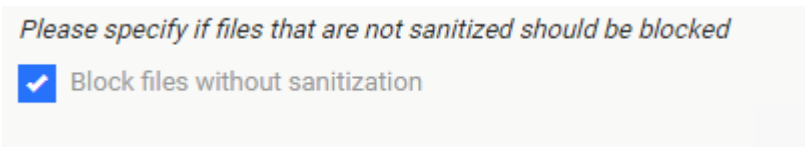
File default expiration

Every file has its own expiration so files will not be stored on the server permanently, this is configurable by administrator.



Block files without sanitization

This option, if turned on, will ensure that files that were not sanitized are not available for download and will reach "*Blocked: No Sanitization*" state.



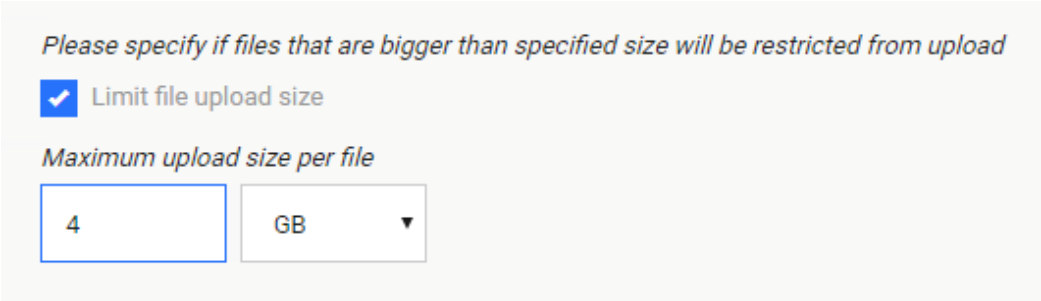
Please note that in order for this feature to work 7. Supervisor Approval must be **enabled.**

Please note that in order for this feature to work 2. Multi-scanning and Data Sanitization must be **configured**.

Please note that *Blocked: No Sanitization* state can only by changed by administrators by approving the file in Pending Approval page. Also make a note of the fact that **supervisors** cannot allow a file in *Blocked: No Sanitization* state even by approving it.

Limit upload size per file

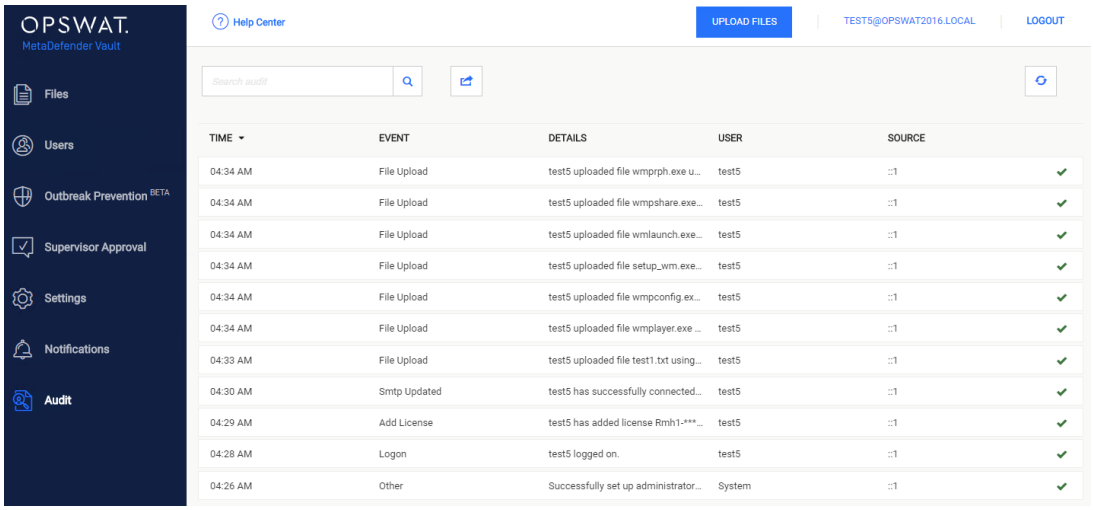
Enable this option if you wish to set a maximum size limit when a file is uploaded



Audit Log

Each event that is triggered by an action (user based or automatically) is recorded by the system and is visible in the Audit log. This feature allows Administrators to track events and data transfers on the system. Only users with the administrator role are able to view the Audit log.

The time, event details, user, source and status of the action are listed. You can filter the events by entering text in the search box and also sort based on column headers.



Export Audit Log

You can export the audit data in a CSV (comma separated values) file. This can be loaded in any 3rd party application, or saved in another internal database.

Retention and Syslog integration

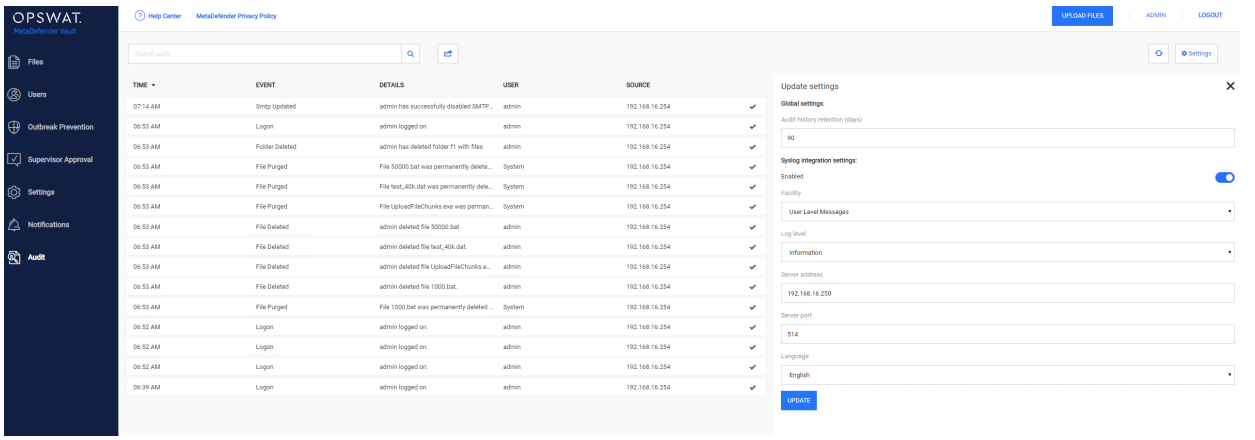
In order to change audit settings please go to **Audit** page and click the **Settings** button in the top right.

This field allows you to configure a retention period for audit events. Any events older than the specified period of time will be automatically removed.

Syslog integration settings

Enabling this integration will instruct Vault to send any audit event to the configured Syslog server.

> Please note that only UDP protocol is supported for now. Because of this, Vault will not be able to validate the connection to the Syslog server. A test message will be sent if the configuration was successful.



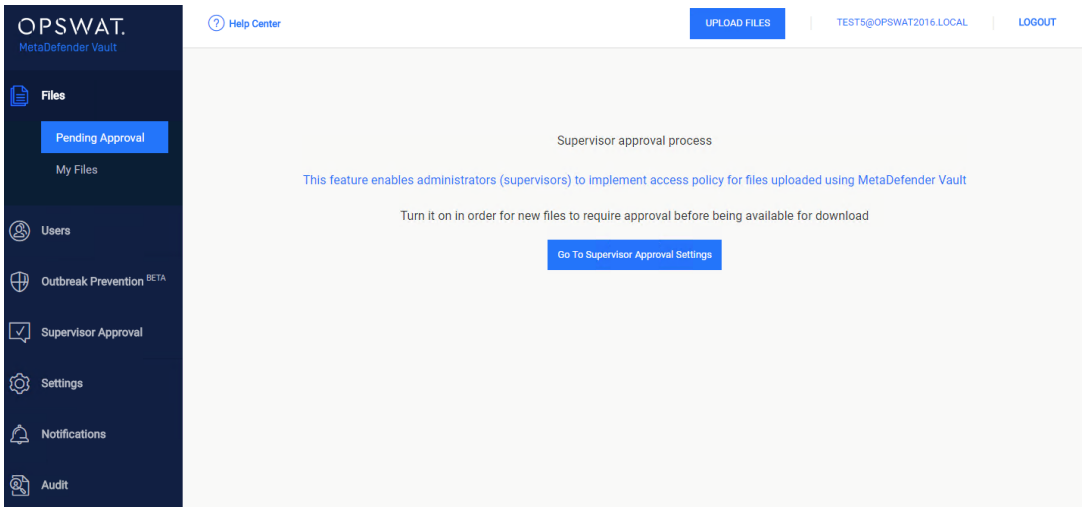
The following settings are available for configuration:

Setting	Description	Default value
Facility	The type associated with Vault events	User Level Messages

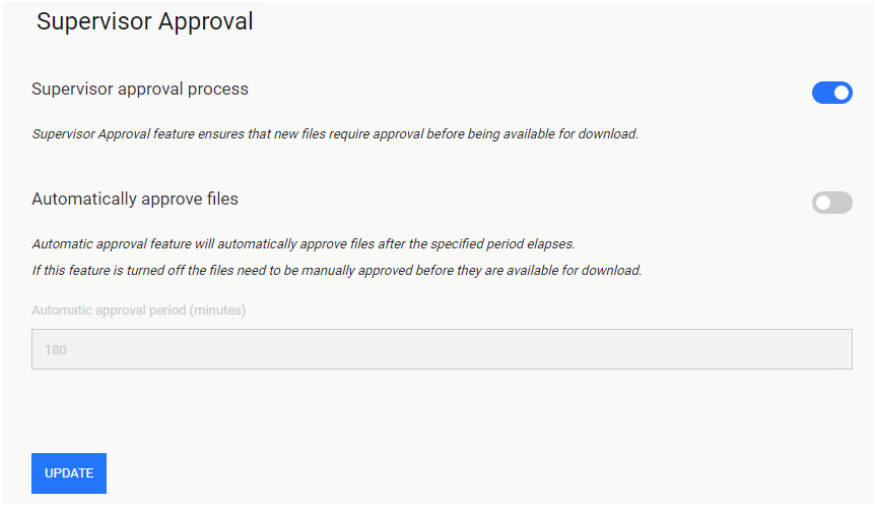
Setting	Description	Default value
Log level	Determines which messages get sent to the Syslog server, it filters out any message less important than that selected	Information
Server address	The address of the server where the Syslog is located	0.0.0.0
Server port	The open port on the Syslog server for accepting messages	514
Language	The language to use for logging messages	English

This features enables administrators (supervisors) to implement access policy for files uploaded using MetaDefender Vault.

Enabling supervisor approval feature



- Go to ***Files*** → ***Pending Approval*** and click Go To Supervisor Approval Settings
- After this you will be redirected to Approval settings. Here you will need to enable the Supervisor Approval Process and select Update.
- When enabling the Supervisor Process, another option will be available: Automatically approve files.



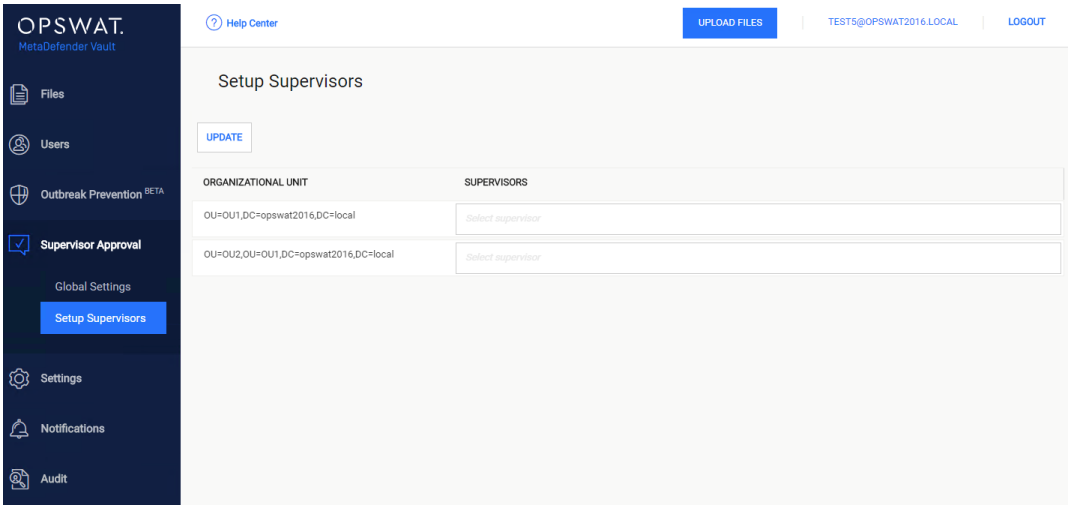
By doing this you will ensure that each file uploaded by your users requires an administrator's (supervisor) approval before it can be downloaded or shared.

Automatic approval

Turning on the *automatic approval feature* ensures that uploaded files are automatically approved after the specified period. Supervisors can still manually approve them or revoke approval if they want to.

Configure supervisors

A user with the **supervisor role** can perform approval or revoke approval for files. The local administrator account is always a supervisor, but you can configure more supervisor by going to ***Supervisor Approval*** → ***Setup Supervisor*** page.



This configuration page allows you to specify one or more supervisor for each of your included organization units. Learn how to include or exclude an organizational unit by going to User Filtering Configuration.

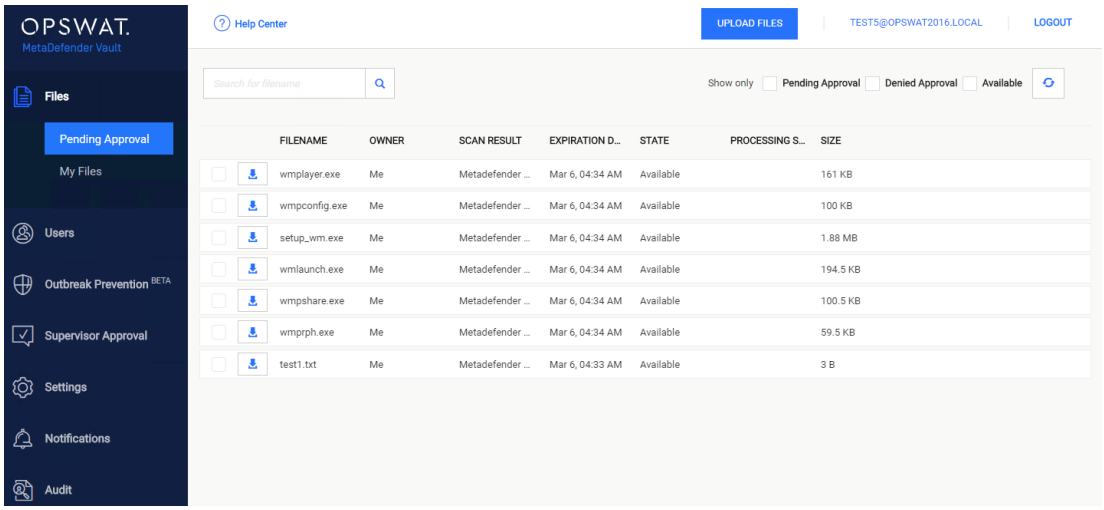
Each supervisor can only approve or reject files of his supervised users (in the same organizational unit). An organizational unit can have any number of supervisors, including none.

Please note that if no supervisors are assigned to an organizational unit the only user that can approve or deny access to files is the local administrator.

Click the Update button when you are done.

Pending Approval Page

This page allows supervisors to manage files shared using MetaDefender Vault.



On the last column the following options are available:

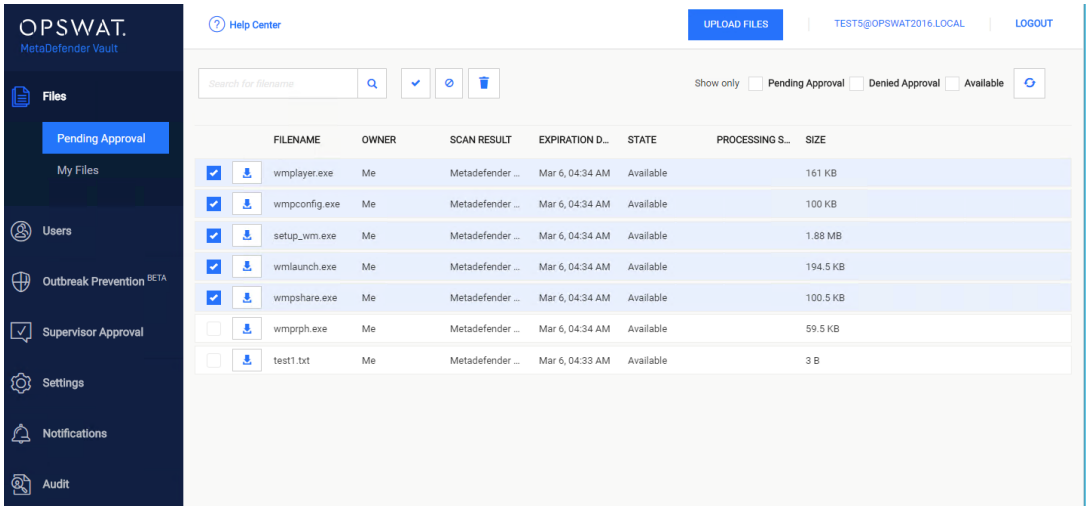
- Approve file: make the file available for download
- Revoke approval: deny access to download the file

On the top of the page the following options are available:

- Refresh: refresh the grid, without removing filters
- Filter Only Pending Approval : show only files that require a supervisor's approval
- Filter Only Denied Approval: show only files that have been denied approval
- Filter Available: show only files that are available/approved by supervisor

Multiple files approval/revoke

Supervisors can also manage multiple files to be approved or revoked at the same time, and not individually.



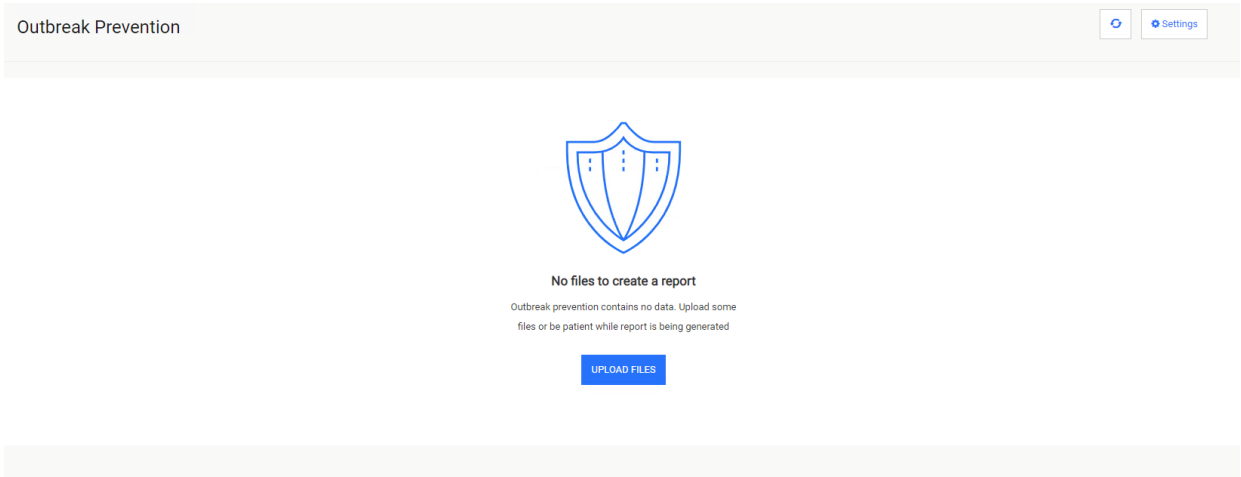
By selecting multiple files, the three button appear:

- Approve
- Revoke Approval
- Delete

Outbreak Prevention ensures that your organization can handle false negatives results and that your users are not exposed to **zero-day vulnerabilities** by locking any new file and re-scanning it automatically for a specified period of time. An overview regarding file processing and detection activity can be seen in Outbreak Prevention as well.

> **Note**
>
> In order to enable Outbreak Prevention you first need to navigate to *Settings → Core Integration* and enable integration with Metadefender Core. *Outbreak Prevention* feature cannot be used without Metadefender Core.

Upload files to create a report.

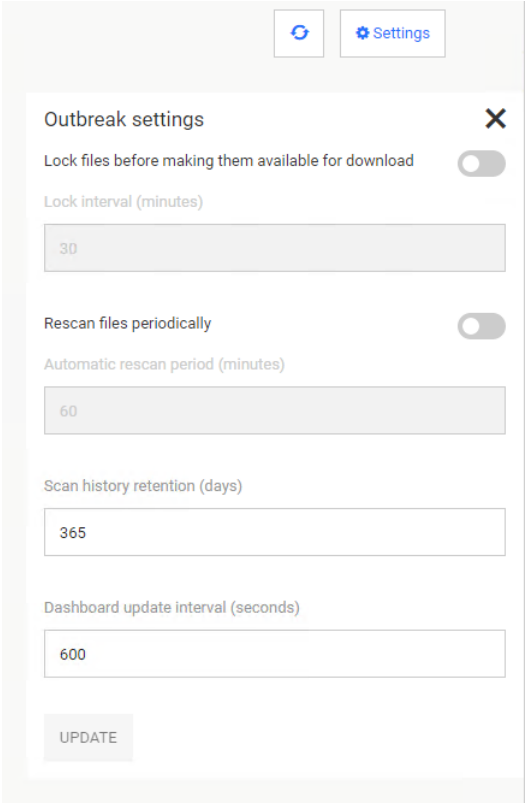


Enable file locking

In order to enable file locking you need to go to Outbreak Prevention page and go to **Setting** button

Lock interval represents the period of time for which the files will remain locked (unavailable for download) before they are automatically unlocked by MetaDefender Vault. For example, if you specify 1800 seconds a new file will be locked for 30 minutes and then automatically unlocked.

Please note that a locked file will be processed again by Metadefender Core before unlocking it.

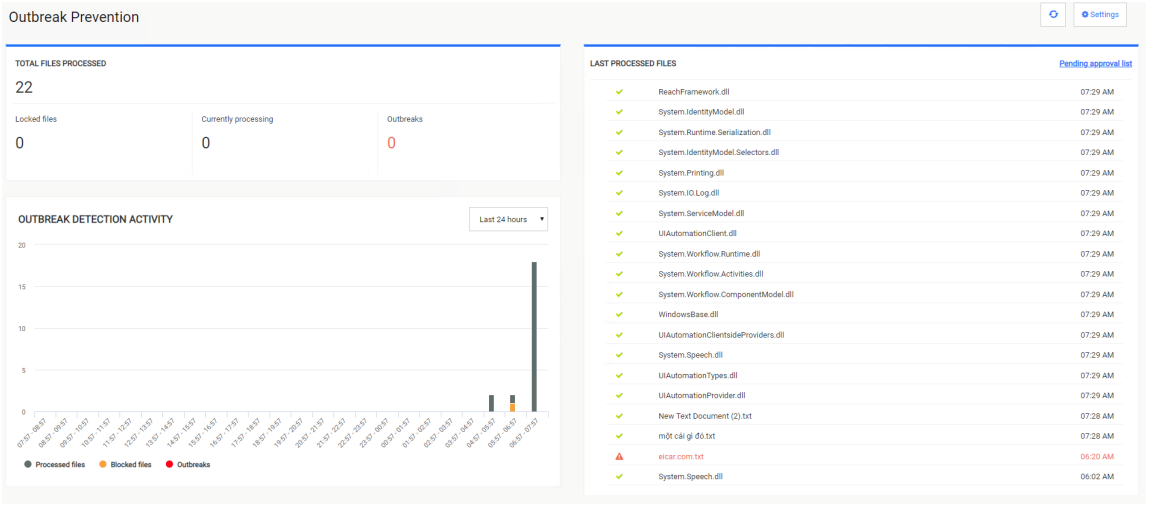


Enable periodic automatic re-scan

In order to enable automatic re-scanning of files you need to go to Outbreak Prevention page and navigate to **Settings** button**.**

Automatic rescan period represents the period of time after which the files will be processed by Metadefender Core again. For example, if you specify 3600 seconds any stored file will be processed again each hour (files are re-scanned hourly).

After you upload files you will be able to see Total Files Processed and Detection Activity


Outbreak Prevention
Settings
TOTAL FILES PROCESSED
22
Locked files
0
Currently processing
0
Outbreaks
0
OUTBREAK DETECTION ACTIVITY
Last 24 hours
20
15
10
5
0
Processed files
Blocked files
Outbreaks
LAST PROCESSED FILES
Pending approval list
ReachFramework.dll 07:29 AM
System.IdentityModel.dll 07:29 AM
System.Runtime.Serialization.dll 07:29 AM
System.IdentityModel.Selectors.dll 07:29 AM
System.Printing.dll 07:29 AM
System.IO.Log.dll 07:29 AM
System.ServiceModel.dll 07:29 AM
UIAutomationClient.dll 07:29 AM
System.Workflow.Runtime.dll 07:29 AM
System.Workflow.Activities.dll 07:29 AM
System.Workflow.ComponentModel.dll 07:29 AM
WindowsBase.dll 07:29 AM
UIAutomationClientsideProviders.dll 07:29 AM
System.Speech.dll 07:29 AM
UIAutomationTypes.dll 07:29 AM
UIAutomationProvider.dll 07:29 AM
New Text Document (2).txt 07:28 AM
một cái gì đó.txt 07:28 AM
eicar.com.txt 06:20 AM
System.Speech.dll 06:02 AM