# Metadefender Secure File Transfer Quick User Guide 1.1.9

# 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/sft/.

## Getting Started

### Before Installation

Before you begin the installation, ensure that SFT System Requirements are met. If you are installing SFT 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 SFT, please visit OPSWAT Portal Metadefender Secure File Transfer section.

### SFT Standalone Portal Deployment

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

- Installing and configuring SFT, 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 SFT functionality:
    - Multi-scanning and Data Sanitization - Integrating Metadefender Core
    - SMTP For Notifications

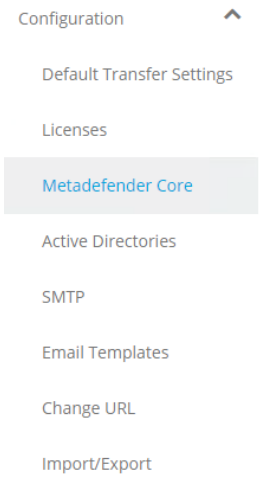
### Deployment with Kiosk and Diode

SFT 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 SFT

## Integrating Metadefender Core

In order to integrate Metadefender Secure File Transfer with Metadefender Core please navigate to Configuration → Metadefender Core in the left menu.




You can configure SFT 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 SFT.

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 SFT to work with Metadefender Core in order to configure Metadefender Core in SFT.

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

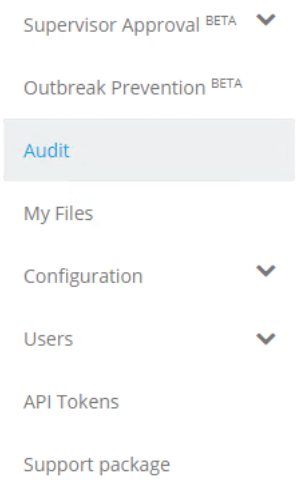
## Authentication for File Download and Expiration

By default, file download requires authentication. Administrator can change this setting so that a link to file download can be shared with someone who is not part of the user group.

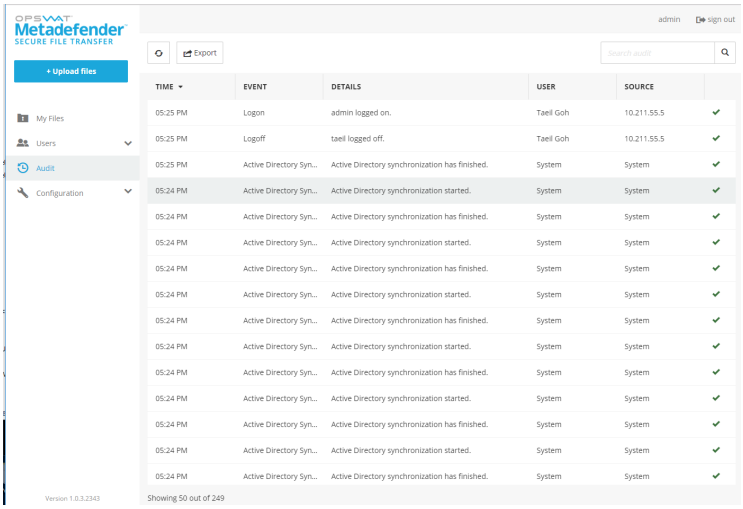
Every file has its own expiration so files will not be stored on the server permanently, this is configurable by administrator.

## 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 button is visible in the left menu.




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.



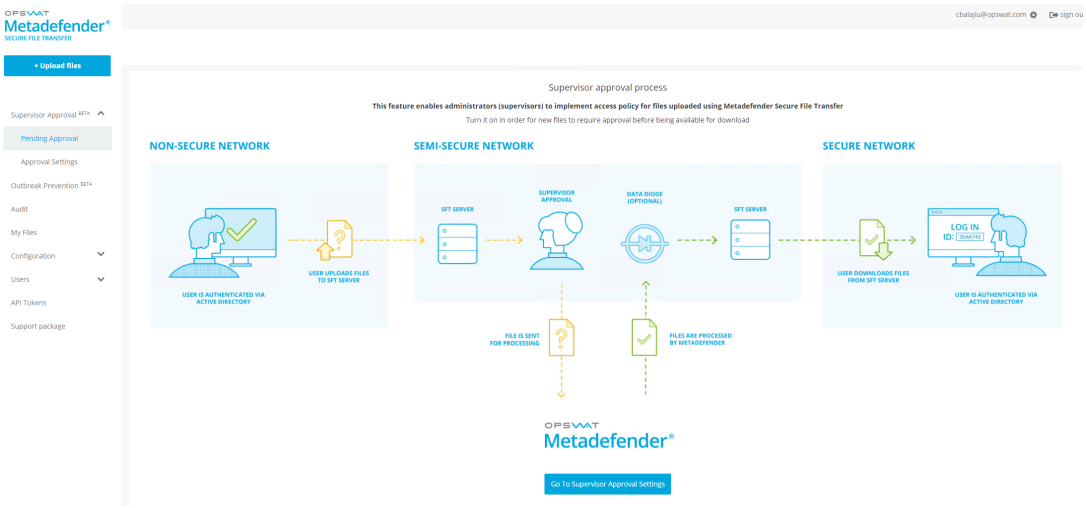

## Export Audit Log

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.

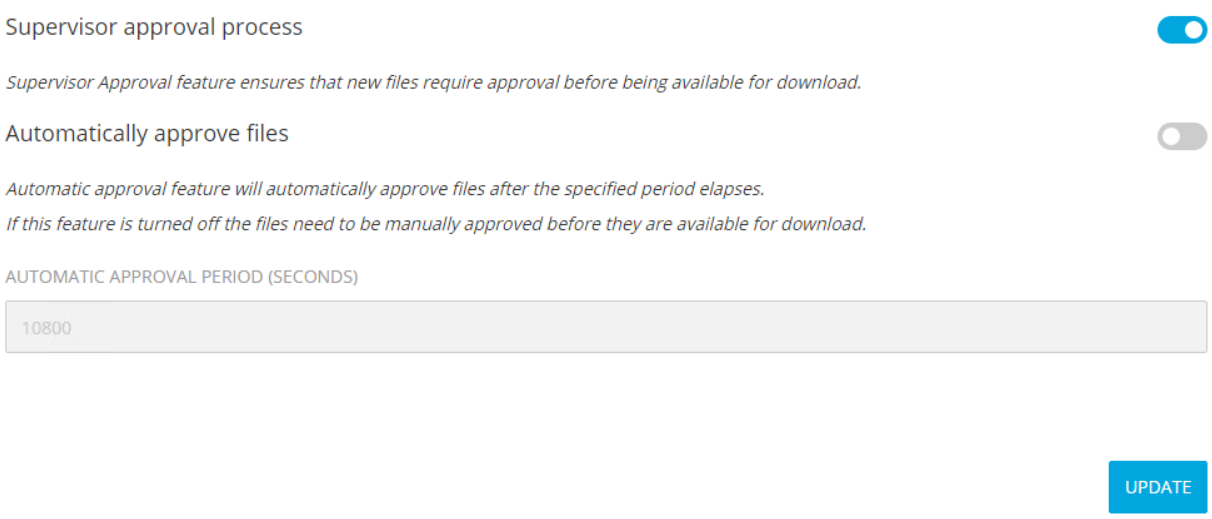
This features enables administrators (supervisors) to implement access policy for files uploaded using Metadefender Secure File Transfer.

## Enabling supervisor approval feature

- Go to Supervisor Approval → Pending Approval, and here 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

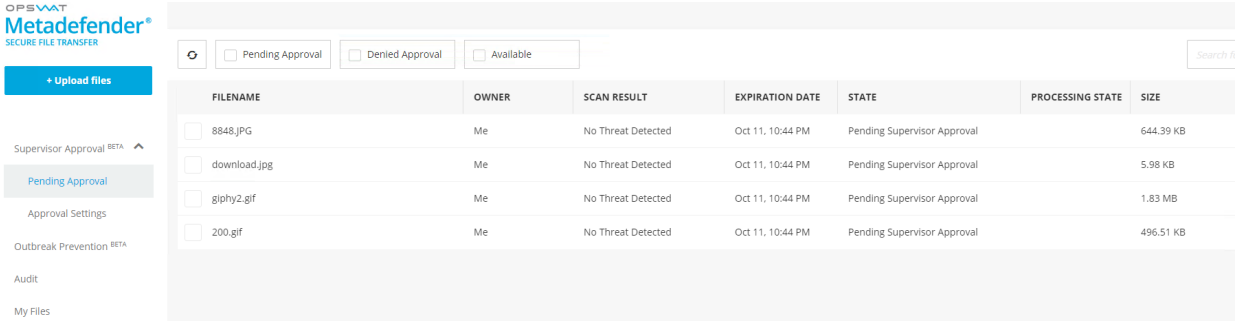
Turning on the *automatic approval feature* ensures that uploaded files are automatically approved after the specified period. Supervisors can still manually approve them or revoke approval if they want to.

## Configure supervisors

An 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 User Filtering Configuration.

## Pending Approval Page

This page allows supervisors to manage files shared using Metadefender Secure File Transfer.




On the last column the following options are available:

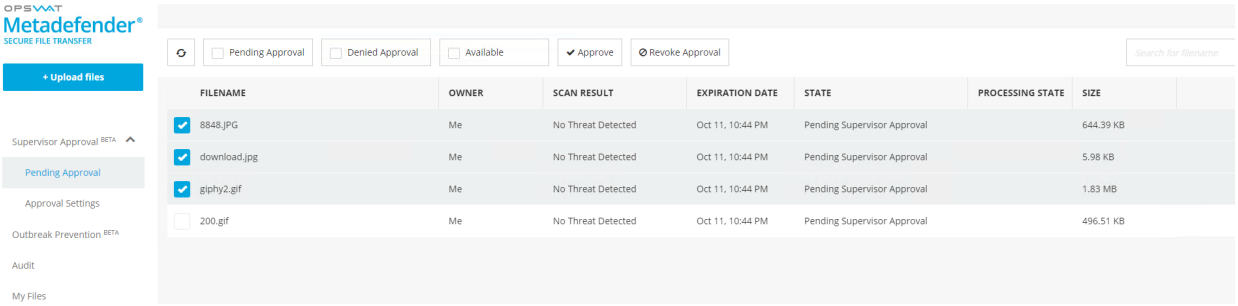
- Approve file: make the file available for download
- Revoke approval: deny access to download the file

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 two button appear:

- Approve
- Revoke Approval

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.

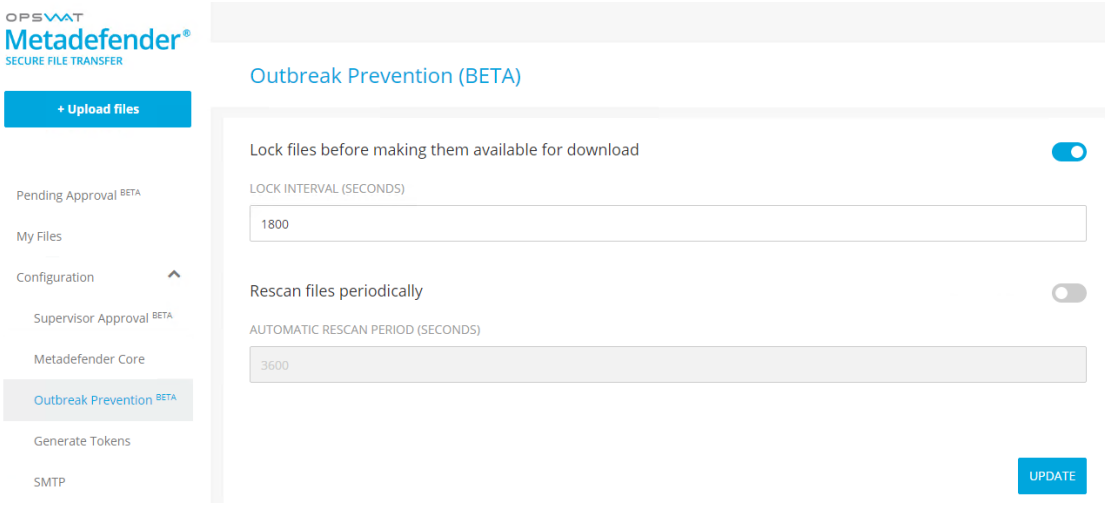
> **Note**
>
> In order to enable Outbreak Prevention you first need to navigate to *Configuration → Metadefender Core* and enable integration with Metadefender Core. *Outbreak Prevention* feature cannot be used without Metadefender Core.

### Enable file locking

In order to enable file locking you need to go to *Configuration → Outbreak Prevention* page and turn it on.

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

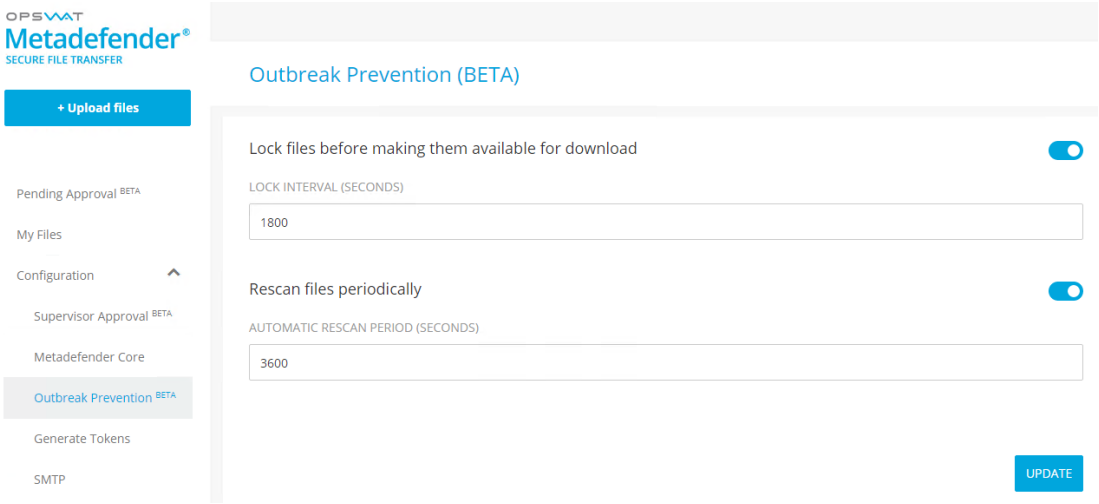
Please note that a locked file will be processed again by Metadefender Core before unlocking it.




### Enable periodic automatic re-scan

In order to enable automatic re-scanning of files you need to go to *Configuration → Outbreak Prevention* page and turn it on.

**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).




## Note

Please note that automatic re-scanning of files has a big impact on performance. If your storage contains a large number of files or many files with increased size this the *Automatic rescan period* might be exceeded. In this case we suggest using increased values (more than one hour) for both **lock interval** and **automatic rescan period.**