OPSWAT.

MetaDefender™ Kiosk

MetaDefender Kiosk Windows v4.7.6

Table of Contents

Installation 1

Installing / Upgrading MetaDefender Kiosk 1
Kiosk System Requirements 2
Installing MetaDefender Kiosk Using the Install Wizard 7
Installing MetaDefender Kiosk from the Command Line 14
Configuring the Management Console for initial use 15
Managing License Information 18
Upgrading MetaDefender Kiosk 20
  Backing Up and Restoring the Configuration 21
  Upgrading from MetaDefender Kiosk 3.X 23
How many models of MetaDefender Kiosk are there? 24
Does MetaDefender Kiosk support multiple languages or customisation? 25
Performance measurement of post-procesed files 28
  Copying to Directory 29
  Copying to MFT 31
  Copying to User Media 35
Performance measurement of Self Scan 37
Performance measurement 39
Database password protection 47

Configuration 48

Configuring with MetaDefender Core 48
Configuring with MetaDefender Managed File Transfer 50
  Arbit Data Diode configuration 52
Configuring with Central Management 54
Trusting an HTTPS OPSWAT product 55

Operating 57

Overview 57
Management Console 66
Login Settings 70
Resources 86
Kiosk Survey 87
Country of Origin 88
About page 90
Kiosk Workflows 91
Workflows Page 92
Properties & Membership 99
Managing User Questions 104
Allowed Media Types 105
Selecting a Server to Process Files 108
Selecting How to Handle Processed Files 118
Custom Command Line Script 129
Managing Printing Options 131
Managing Logging Options 133
Email Session Report 135
Retrieve Files 138
Using the Kiosk User Interface 143
Logging In on the User Authentication Screen 146
Inserting Digital Media 153
Unlocking Encrypted Devices 155
Processing Digital Media 158
Processing Encrypted Archives 168
Processing Disk Image Files 170
Viewing the Session Results 176
Copying Files 189
Retrieving Files from an External Source 195
OPSWAT Media Validation Agent 200

Advanced Deployment 207

Additional Kiosk Configuration 207
UI Localization / Customization 210
Watchdog Behavior 213
Configuring Global Kiosk Settings 214
Configuration Field Descriptions and Default Settings 223
Visitor Management 235
Session Logs 239
Visitor Logs 244
Syslog settings 245
Alert Sound Customization 249
Branding and Logo Customization 250
Disclaimer Screen Customization 252
Self Scan 255
Developer Guide 259
Custom Authentication Module 260
Quarantine Manager Command Line Interface 276
Recommended Deployment of MetaDefender Kiosk(s) in Secure Facilities 278
Configuring ADFS as SAML Identity Provider 285
Microsoft Entra ID Integration 291
Encrypted Device Verification And Approval 308
Setup Microsoft SharePoint or OneDrive as storage 312
Setup for Thales (formerly Gemalto) smart card for user authentication 326
Setup RFID card for user authentication 355
Configure OAuth email authentication - Microsoft 365 (Graph API) 362

Troubleshooting 365

Troubleshooting Issues 365

Knowledge Base 367

Can a Syslog event be generated when an infection is found by MetaDefender Kiosk? 367
Why does Kiosk pause on the final screen after scan session "settings"? 369
Can I add groups from Active Directory to MetaDefender Kiosk Workflow Profiles? 371

Can I extend MetaDefender Kiosk by adding Custom Engines or Signatures? 373
Can I run MetaDefender Kiosk using a non-administrator account? 375
Can I upload files to a file server after they have been scanned by MetaDefender Kiosk? 376
How can MetaDefender Kiosk and Managed File Transfer (formerly Vault) be configured to work with an Arbit Data Diode? 377
How does MetaDefender Kiosk do file type detection? 379
How do I revert MetaDefender Kiosk to a previous state using Deep Freeze software? 382
How do I copy and save files to a mapped drive with MetaDefender Kiosk? 384
How do I set the Restart MetaDefender option for MetaDefender Kiosk Watchdog on Windows 8 and above? 389
How long is the support life cycle for a specific version/release of MetaDefender Kiosk? 391
How do I set up and use the Media Manifest feature in MetaDefender Kiosk? 393
How do I use the Copy & Go feature in MetaDefender Kiosk? 399
What are the running processes of MetaDefender Kiosk? 403
What does Remediated File mean in MetaDefender Kiosk? 404
What is the difference between the Format, 1-Pass, 3-Pass, and 7-Pass options in the MetaDefender Kiosk wipe functionality? 406
What is the frequency of MetaDefender Kiosk's antivirus signature/definition updates? 410
How to completely uninstall MetaDefender Kiosk 412
How do I create a support package for MetaDefender Kiosk? 413
How do I exit the MetaDefender Kiosk user interface? 415
Is Kiosk Active Directory integration possible? 416
How can I generate an API key on the Kiosk side? 421
How can I create a new workflow? 423
Can I have a backup (Core) server integrated with Kiosk? 426
Does MetaDefender Kiosk support encrypted devices? 429
After license renewal does the product activation happen automatically (if the license key is the same)? 433
How do I use Simplified Workflow? 434
How to increase session timeout via API? 438
Does adding a second MFT in the Kiosk serve as a high-availability mechanism? 440
Why does Kiosk showing a very large number of hidden partitions when scanning DVD/CD? 441
Why is Kiosk Skipping Files? 442

How do I check the version of a Kiosk Hardened/Secure Image “install.wim” file? 447
Can MetaDefender Kiosk be configured to handle large volumes of scans more quickly? 450
How to remotely Shutdown or Restart the System from the Kiosk UI? 452
Does the MetaDefender Kiosk hardened image support Windows 11? 454
Why files are copied to Admin accounts instead of AD account in MFT? 455
How do I configure MetaDefender Kiosk to use a Gmail account for email notifications? 457
How do I configure SMTP server on MetaDefender Kiosk to send notification to M365 tenant? 460
How to Set Up OPSWAT Kiosk to Copy Files to a Secondary Location for an AD User? 462
How do I verify my Kiosk Image type? 463
Why are some of the keys on the physical keyboard not responsive in MetaDefender Kiosk? 465
Why doesn’t my MetaDefender Kiosk start? 466
Why is MetaDefender Kiosk not recognizing floppy drives? 471
Does a CVE affect MetaDefender Kiosk? 473
Why do I receive Kiosk License mismatch error? 476
Why is the Kiosk not detecting devices? 477
Why retrieving the Kiosk file history not working for sessions with a large number of files? 479
Why am I experiencing a "Login Denied" error when attempting to send a test email for scan results from the MetaDefender Kiosk? 481
Why does OMVA agent not working as expected? 482
Which Kiosk Hardware Model am I using? 483
Why can I not execute script file like .VBS or .PS1.... in Hardened Image 488
How do I resolve issues with OPSWAT Media Validation Agent not detecting USB after Certificate installed? 490
Why am I receiving "LDAP is unsupported" when trying to configure an AD server on a Kiosk instance managed by Central Management v8? 493
How to resolve slow USB Detection on Kiosk Tower with Floppy Drive? 497
Why does MetaDefender Kiosk System Administration Service fail to start? 498
Why is my MD Kiosk disabled on Secure Image and how to resolve it? 500

Hardened Image 502

Overview 502
Kiosk OOBE Initial Setup Guide 503
MetaDefender Kiosk Hardened Image deployment 509

Kiosk Hardening 514
Configuring the Web Server 517
Disabling Windows Hot Keys 521
Boot Hardening Option 523
Anti-tamper Hardening Option 525
Network Hardening Policies Option 529
Enable Windows Defender within Kiosk 535
Enabling BitLocker for KIOSK Hardened Image 536
Setting BIOS Password on KIOSK Devices (DELL) 543
Change Kiosk autologon password 545
Disabling Windows Update 547
Auto-Upgrade Kiosk Hardened Image 555
Release Notes 560
Archived Release Notes 561

Secure Image 567

Overview 567
Release notes 568
Archived Release Notes 569
Secure Image Deployment Wizard 572
Creating Secure Image Deployment flash drive 573
MetaDefender Kiosk Secure Image Deployment 576

Release Notes 581

Release Notes 581
OMVA - Release Notes 591
Archived Release Notes 593
Known Limitations 670
CVE-2024-52925 672

Installing / Upgrading MetaDefender Kiosk

Before you begin the installation, you should ensure that system requirements are met. You can install MetaDefender Kiosk by either using the embedded Install Wizard or from the Windows command line.

Once you finish installation and harden the Kiosk, you can deploy and launch the Kiosk UI for usage.

> **Info**
> This section does not cover installation of MetaDefender Core or Managed File Transfer. Refer to each product's respective user guide for more information.

Kiosk System Requirements

Hardware requirements

MetaDefender Kiosk System Requirements

When MetaDefender Kiosk is installed on a **separate system** from MetaDefender Core, the following specifications are required:

- **Processor:** Quad-core or higher
- **Memory:** Minimum 4 GB RAM
- **Storage:** At least 10 GB available hard drive space
- **Operating System:** 64-bit architecture version

If MetaDefender Kiosk and Core are installed on the **same system**, please refer to the MetaDefender Core user guide for detailed system requirements.

Software requirements

Supported File Systems

- Windows
- FAT16/ FAT32/ exFAT
- Ext2/3/4
- HFS Plus
- HFSX
- APFS

Operating System

- 64-bit architecture required
- **Windows:**
  - Windows 7 (with Service Pack 1, KB2533623, and KB3033929)
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows 11 (version 24H2)
- Windows Installer 4.5 or higher

Dependencies

- **OPSWAT MetaDefender Core:** Required for multi-scanning capabilities. Can be installed on the same or a separate system. Refer to the MetaDefender Core user guide for specific requirements.

Note: Maintaining the operating system with the latest updates is strongly recommended.

Security requirements

The system administrators are required to make a Kiosk machine more secure by following these actions:

1. Set a BIOS password
2. Enable TPM and Secure Boot in the Windows system
3. Turn on BitLocker encryption

Kiosk is expected to be operated on a local, physical system. Operating a Kiosk in a remote desktop session is not supported. It is recommended to disable RDP access to the kiosk system if it is not required for your deployment environment.

Installed third party components

The following third party components are installed as part of the MetaDefender Kiosk installation process. These components may be shared with other applications.

All of these are required by MetaDefender Kiosk. Uninstalling them may result in unexpected behavior of other applications.

Component	Details
Microsoft Visual C++ redistributable	• Microsoft Visual C++ 2010 Redistributable - x86 • Microsoft Visual C++ 2010 Redistributable - x64 • Microsoft Visual C++ 2012 Redistributable - x86 • Microsoft Visual C++ 2012 Redistributable - x64 • Microsoft Visual C++ 2013 Redistributable - x86 • Microsoft Visual C++ 2013 Redistributable - x64 • Microsoft Visual C++ 2017 Redistributable - x86 • Microsoft Visual C++ 2017 Redistributable - x64
Paragon Software (optional)	• APFS for Windows by Paragon Software • HFS+ for Windows by Paragon Software • Linux File Systems for Windows by Paragon Software

Installed services

The following list are services that MetaDefender Kiosk depends on for operating.

Product Services	Additional Information
MetadefenderSVC	
ometascan, ometascan-node, ometascan-postgresql (Core v4.19+)	If Core is installed locally to Kiosk
Third Party Services	
ParagonAPFSMounter	If *APFS for Windows by Paragon Software* is installed
apmwinsrv	If *HFS+ for Windows by Paragon Software* is installed
ParagonLinuxFSMounter	If *Linux File Systems for Windows by Paragon Software* is installed
Windows Services	
Winmgmt	This service has dependencies on other Windows services

Required available ports

The following ports need to be available for the machine MetaDefender Kiosk is installed on.

Component/service	Port
MetaDefender Kiosk Web Console	8009
MongoDB	27019

Application directories and registry key

Installation location

Installation directory can be configured. Default location is `C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client`.

Application directory

The `%ProgramData%\OPSWAT` directory is used for storing MetaDefender Kiosk application data.

Registry key

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\OPSWAT` is the registry key for all OPSWAT products.

Real Time Protection \ Antivirus exclusion requirements

Real Time Protection (RTP) from any 3rd party software may adversely affect Kiosk operation as it will likely interfere with Kiosk's handling of media. It is recommended to either fully disable RTP or create exclusions to allow Kiosk to function and scan media without any interruptions.

Disabling Real Time Protection (RTP)

If setting up hardware not provided by OPSWAT, or your license key is not including Windows Defender as a part or MultiScan engine, ensure that Windows Defender Real Time Protection is disabled:

- Under `Virus & threat protection settings` disable `Tamper Protection`
- Under `Local Group Policy Editor`: *Computer Configuration* > *Administrative Templates* > *Windows Components* > *Microsoft Defender Antivirus* > *Real-time Protection* → *Turn off real-time protection* to `Enabled`
- Apply and reboot the system

Directories exclusion settings if RTP must be on

If your policy does not allow for RTP to be disabled, it is necessary to exclude these directories:

- Kiosk installation folder
  - `C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client`
- Kiosk application data folders
  - `C:\ProgramData\OPSWAT`
  - C:\Users\<username>\AppData\Local\OPSWAT\Metadefender Kiosk
  - C:\Users\<username>\AppData\Roaming\metadefender-kiosk
  - C:\Users\<username>\AppData\Roaming\metadefender-kiosk-electron
- Paragon software folder
  - C:\Program Files (x86)\Paragon Software
- any known drive letters media will be mounted to when inserted

For Core, please refer to this knowledge base article on RTP exclusions.

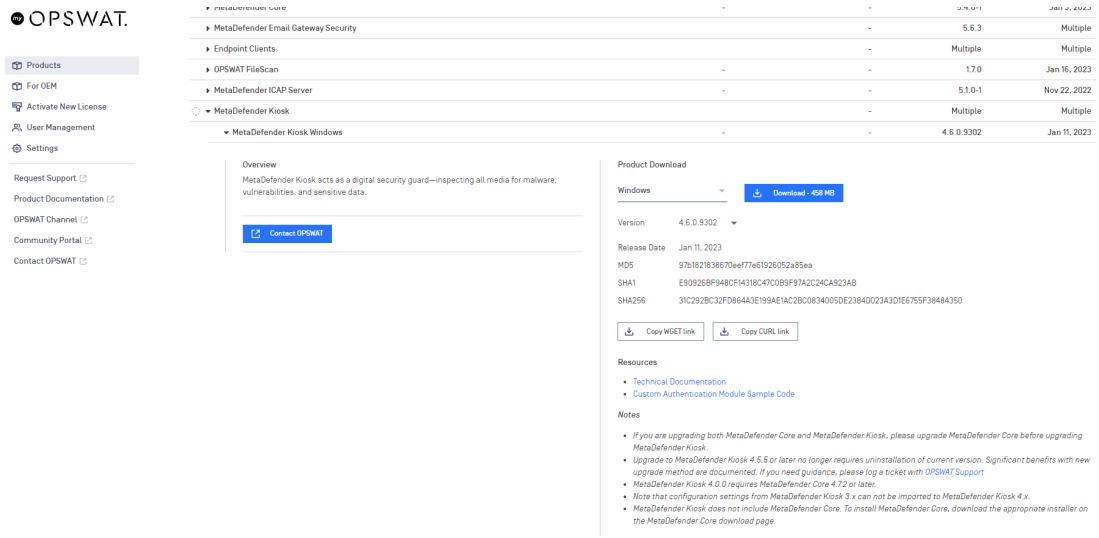
> **Info**
> These steps may need to be redone after a Windows update since it may cause the Windows Defender settings to be reset.

Programs not removed during uninstall

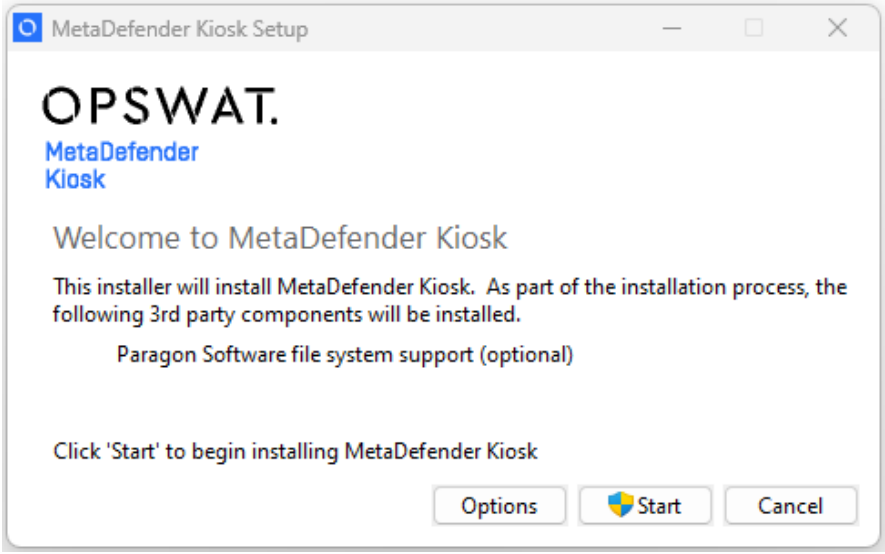
The Microsoft redistributables are not removed when MetaDefender Kiosk is uninstalled.

Installing MetaDefender Kiosk Using the Install Wizard

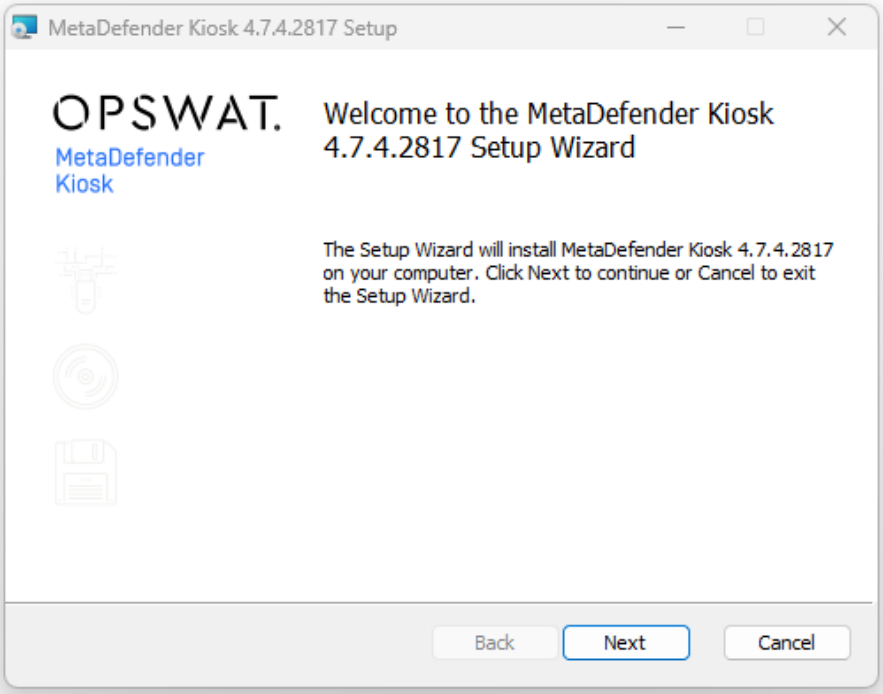
Step 1: Log into My OPSWAT and within the `Products` section find `MetaDefender Kiosk Windows` to download the latest installer.



Step 2: Double click the downloaded executable. The Welcome window appears.

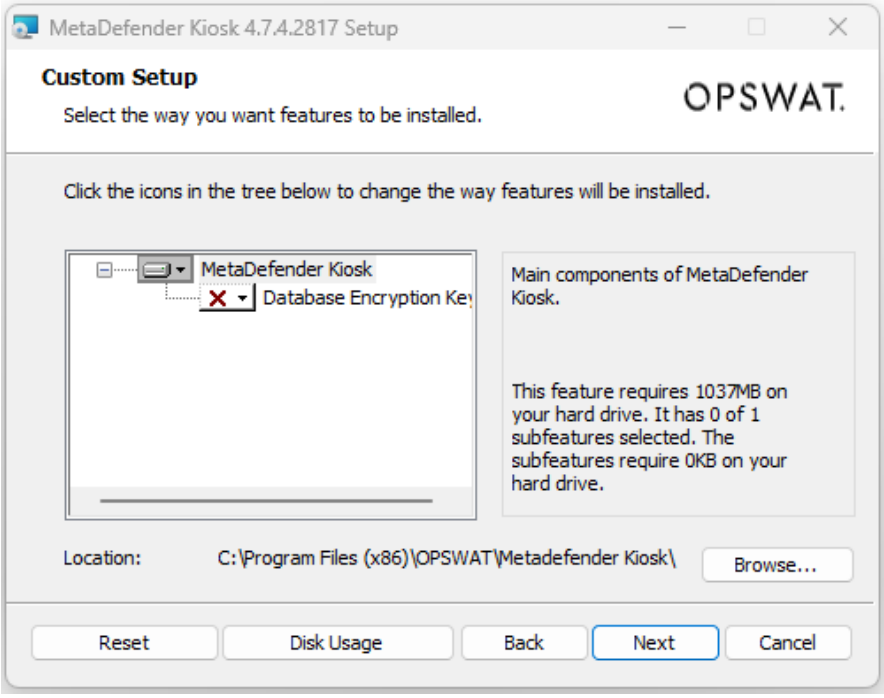


Step 3: Click **Start**. The Setup Progress window appears, followed by the Setup Wizard Welcome window.



Step 4: Click **Next**. The End User License Agreement window appears.

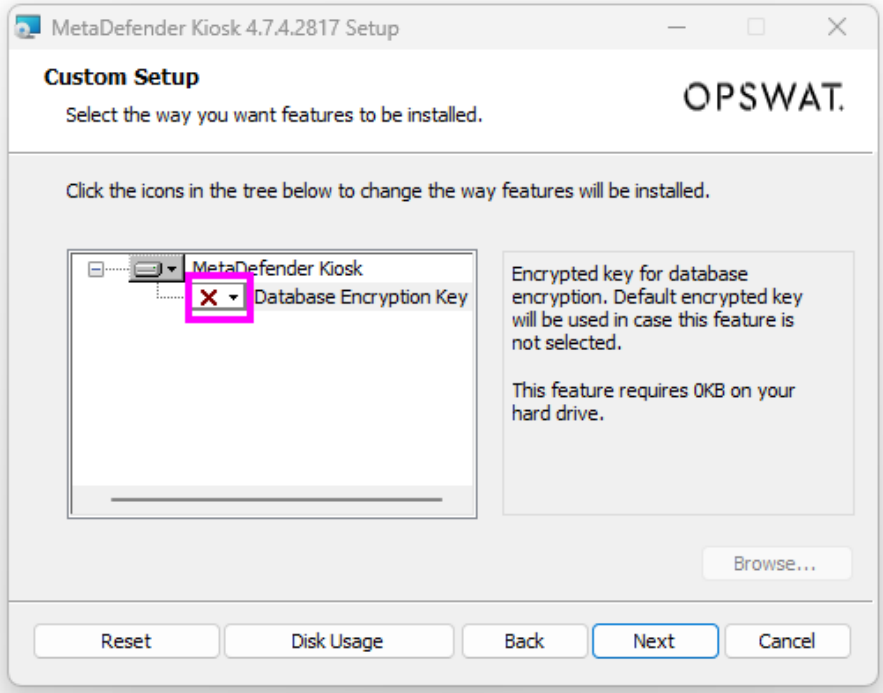
Step 5: Read the EULA, select the **I accept the terms in the License Agreement** checkbox, and then click **Next** . The Custom Setup window appears.



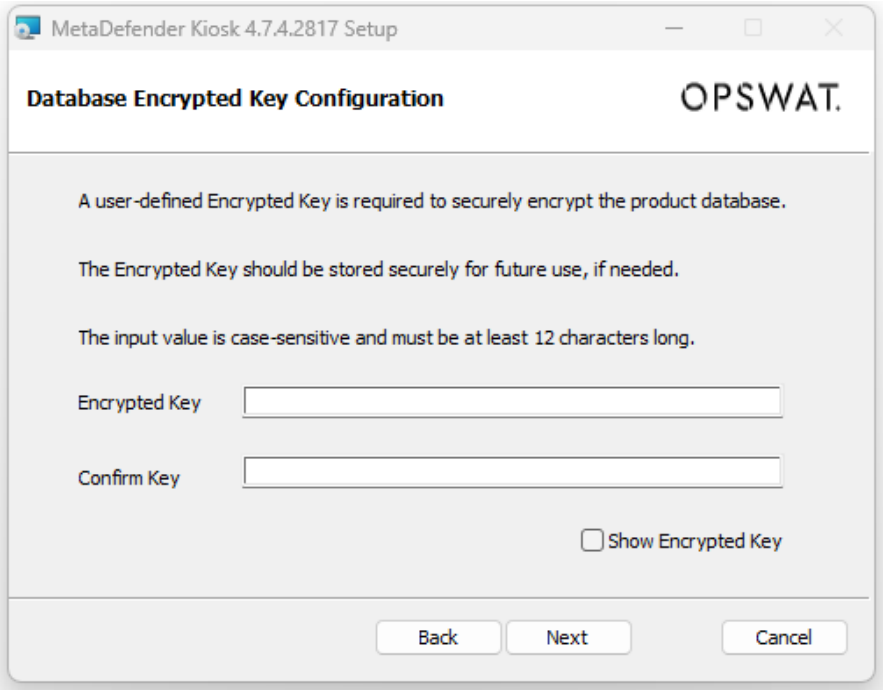
Step 6: If required, change the default location of the MetaDefender Kiosk components using the **Browse** button. Click **Disk Usage** to view a window that displays the disk space requirements for MetaDefender Kiosk and the amount of available disk space for the selected location. Click **Reset** to reset the location back to default.

> **Note**
> It is recommend to install MetaDefender Kiosk in the default location

Step 7: The KIOSK database is password-protected. For enhanced security, KIOSK allows you to input an encryption key as an additional layer of protection for the database. To enable this feature, click the dropdown menu and choose either "`Will be installed on local hard drive`" or "`Entire feature will be installed on local hard drive`." Refer to Database password protection for more details about password generation.



Step 8: Click **Next,** if **Database Encryption Key** is enabled, the Database Encrypted Key Configuration window appears:

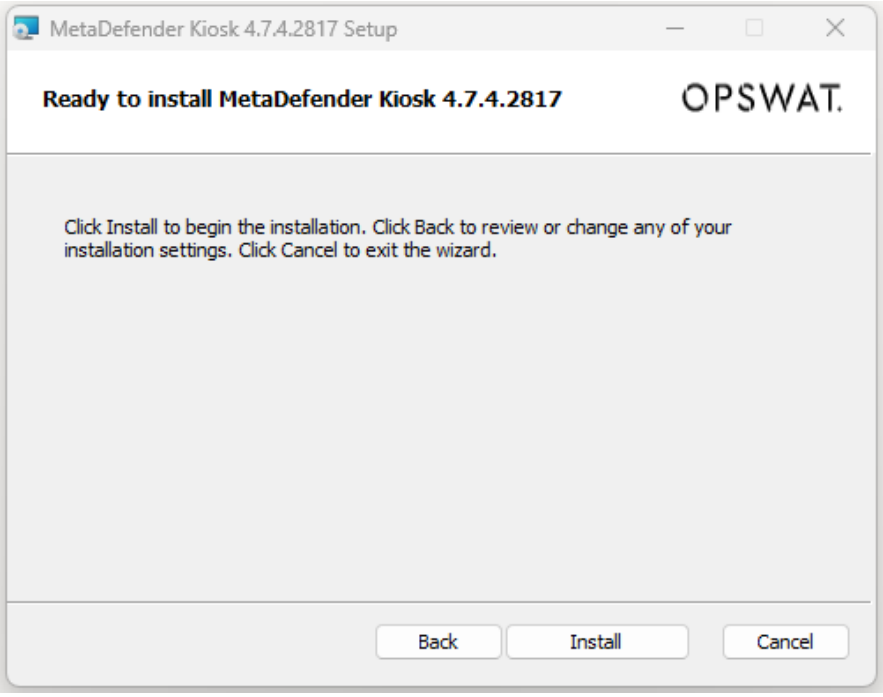


Warning

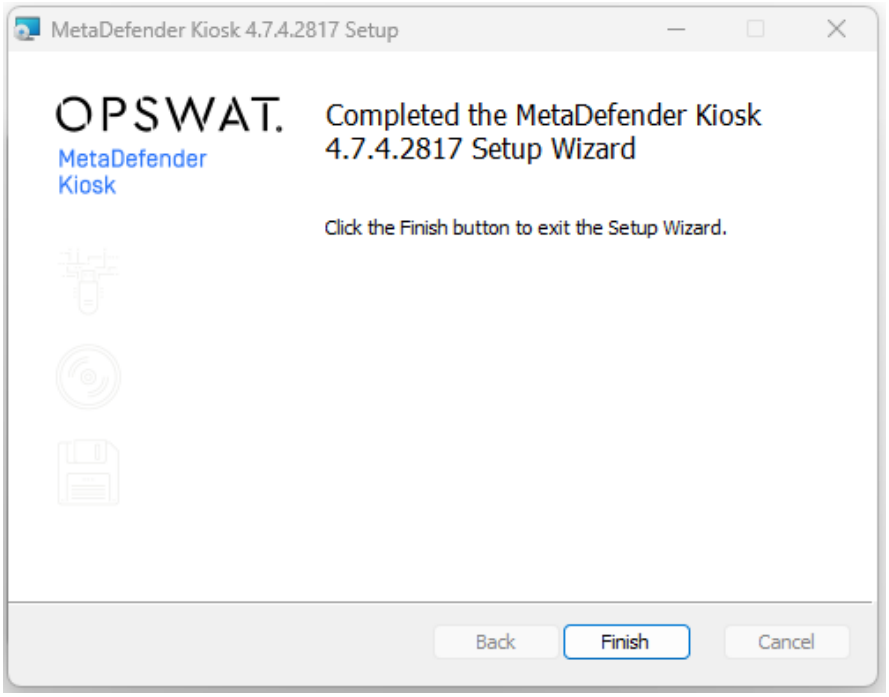
The encryption key should be securely stored for future use to recover the database password if necessary.

The input value is case-sensitive and must be at least 12 characters long.

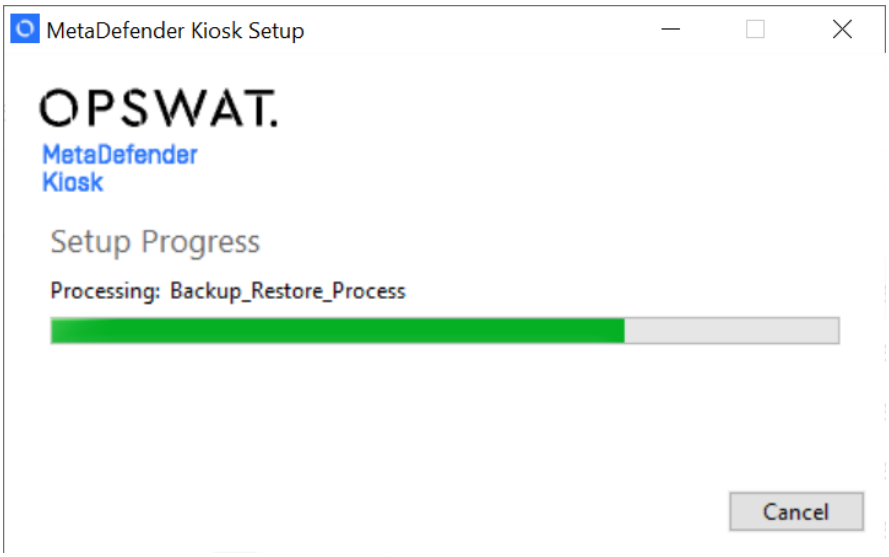
Step 9: Click **Next**, the ready to install window appears



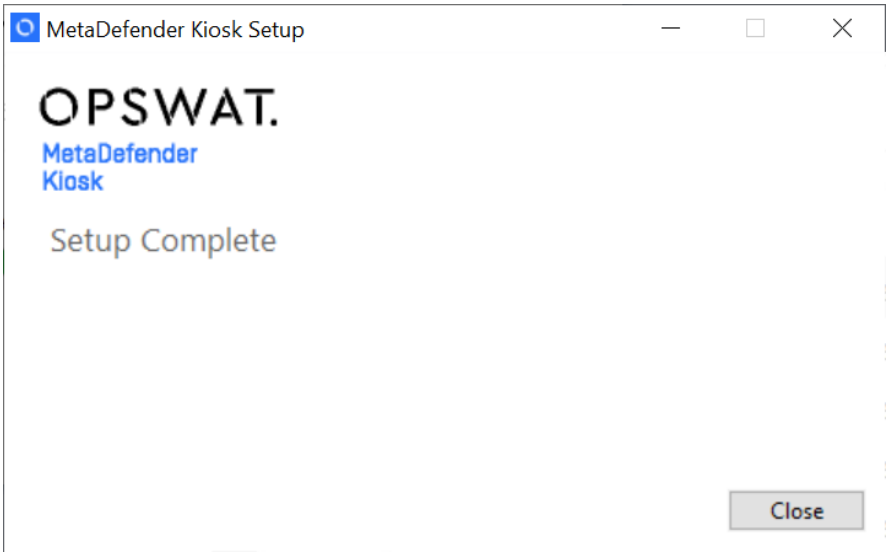
Step 10: Click **Install**. A window appears displaying the status of the installation process, followed by the Completed window.



Step 11: Click **Finish**. An additional process of restoring session history will appear if a previous version of Kiosk was already installed on the system.



Step 12: Wait until the Setup Complete window appears.



Step 13: Click **Close**. MetaDefender Kiosk is now installed.

Installing MetaDefender Kiosk from the Command Line

Command line options

The following command line options are available with MetaDefender Kiosk. All arguments are case sensitive.

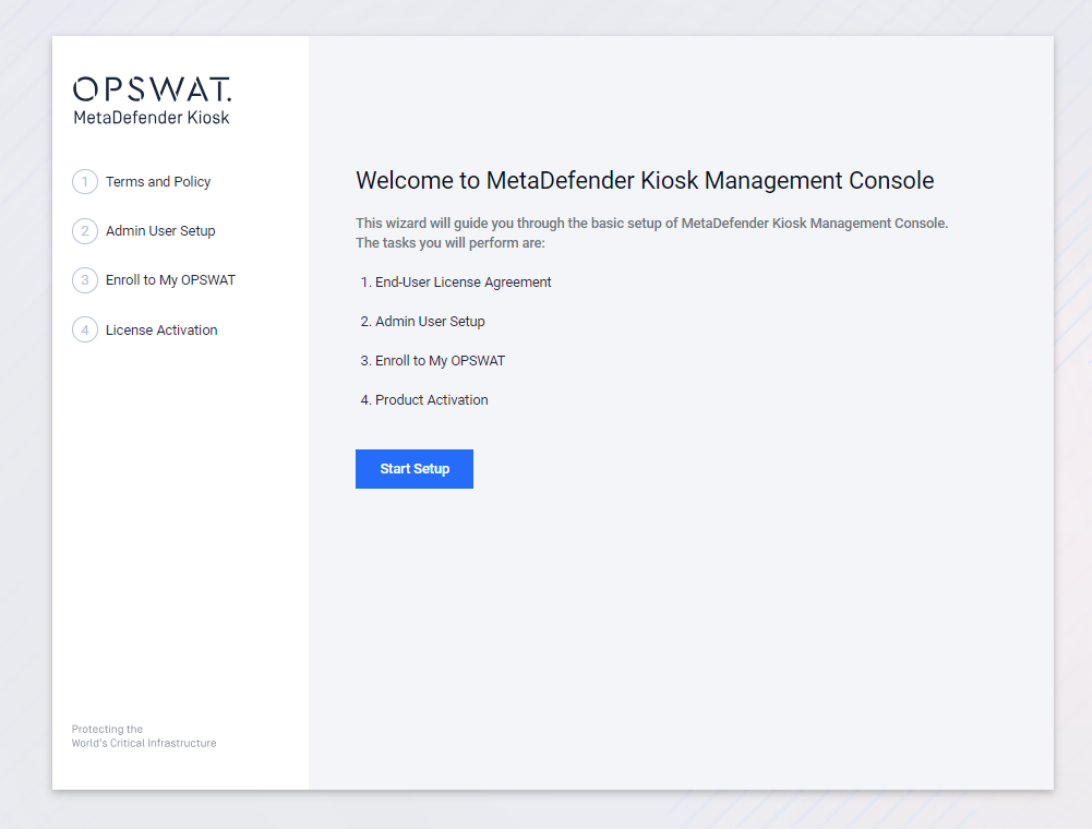
Command Line Option	Description	Example
/install	Install MetaDefender Kiosk	C:\MetaDefender_Kiosk.exe /install
/uninstall	Uninstall MetaDefender Kiosk	C:\MetaDefender_Kiosk.exe /uninstall
/log <log-file-name>	Create installation log file	C:\MetaDefender_Kiosk.exe /log c:\omsinst.log
/quiet	Run MetaDefender Kiosk installation/uninstallation silently	C:\MetaDefender_Kiosk.exe /quiet C:\MetaDefender_Kiosk.exe /uninstall /quiet
INSTALLLOCATION= <install-path>	Sets the installation location for MetaDefender Kiosk	C:\MetaDefender_Kiosk.exe /i INSTALLLOCATION="C:\MetaDefender"

Configuring the Management Console for initial use

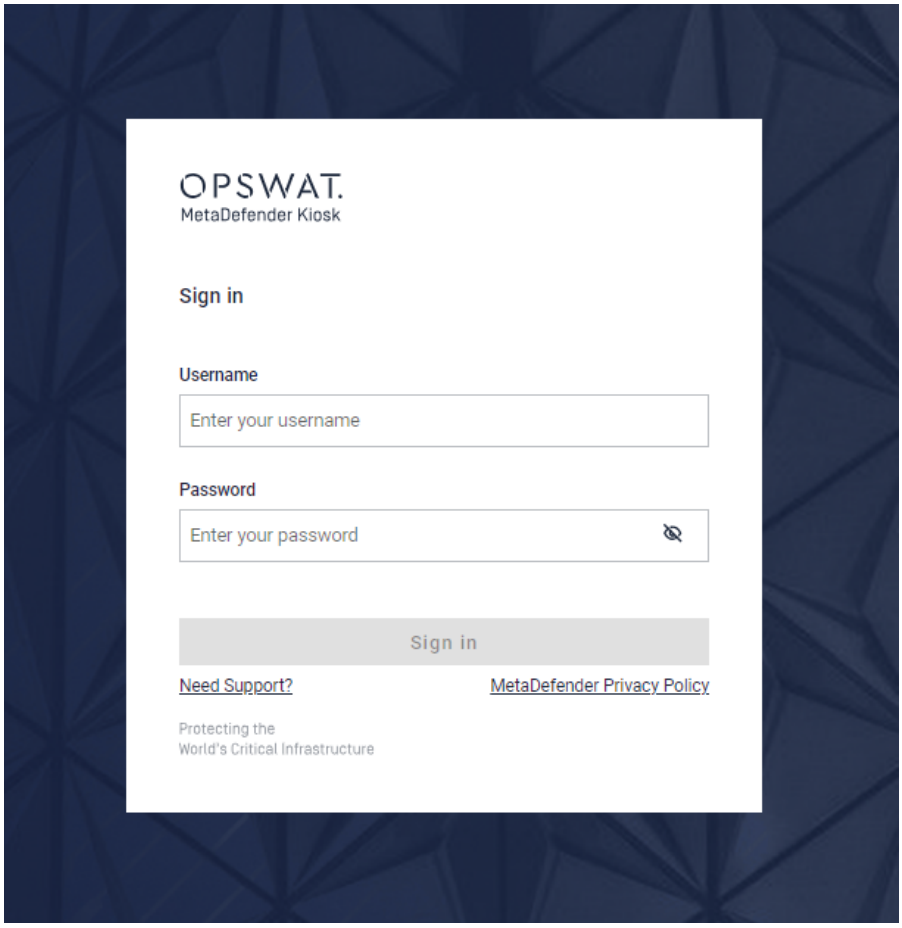
The Management Console can be accessed by navigating to `http://localhost:8009`

An administrator user must be created to log into the Management Console after installing Kiosk for the first time. When navigating to the Management Console a configuration wizard will be presented:

Follow the directions to accept the EULA, create an administrator user and activate the product license. After successful completion, the newly created user will be logged in.

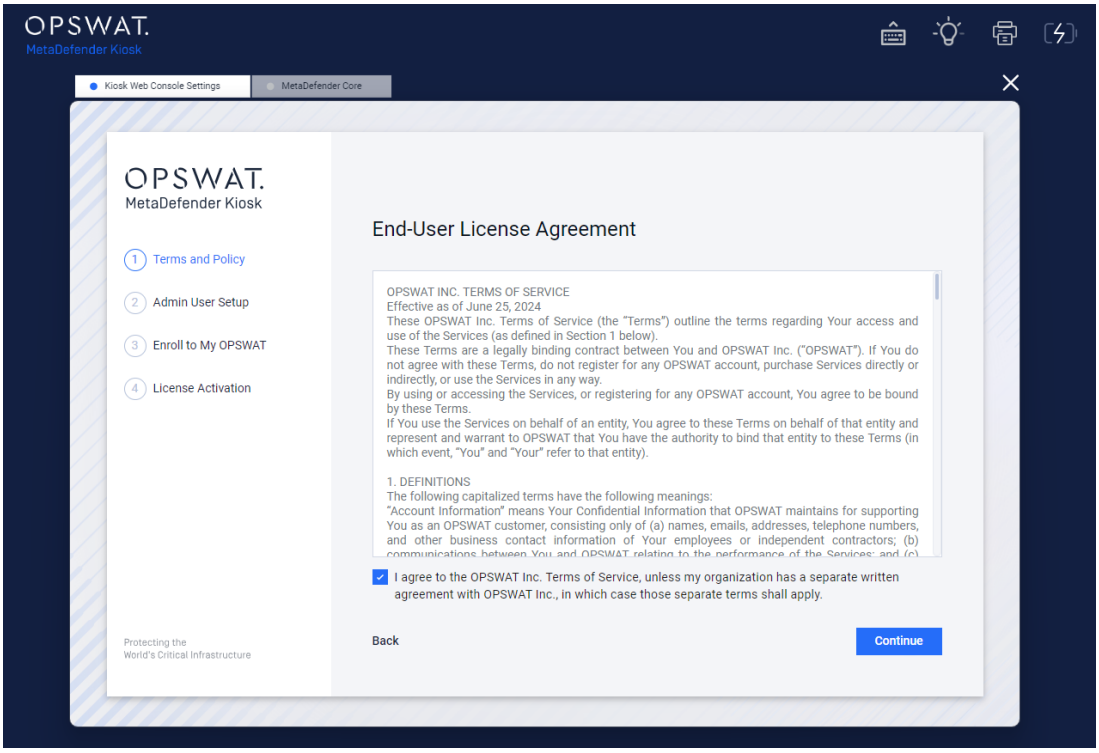


Each time the Management Console is accessed, the login screen will be displayed.



On **Kiosk version 4.7.2 or newer**, Administrators can configure Kiosk directly from the Kiosk UI without exiting the application.

To access the Kiosk WebMC directly from the Kiosk UI, click on the gear icon on the top right corner of the screen. An interface will be shown allow Administrators to configure Kiosk and Core.

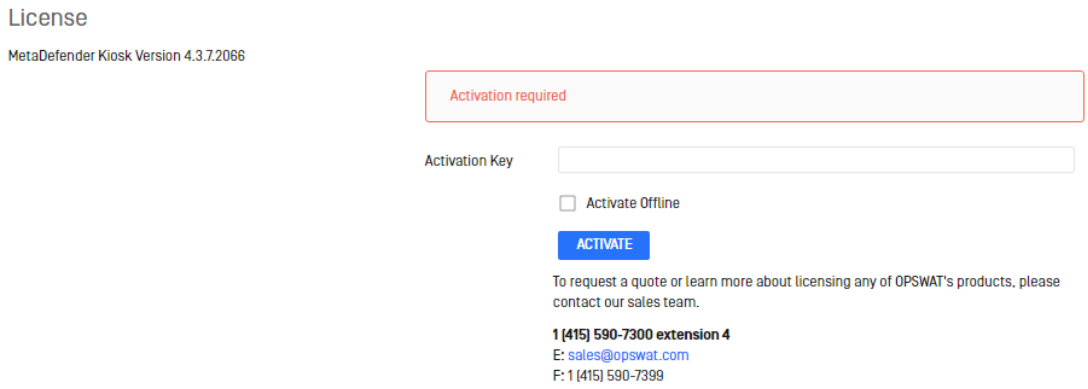


Embedded Kiosk WebMC on Kiosk UI

Info
Embedded Kiosk and Core WebMC on Kiosk UI is only available on Kiosk version 4.7.2 or newer

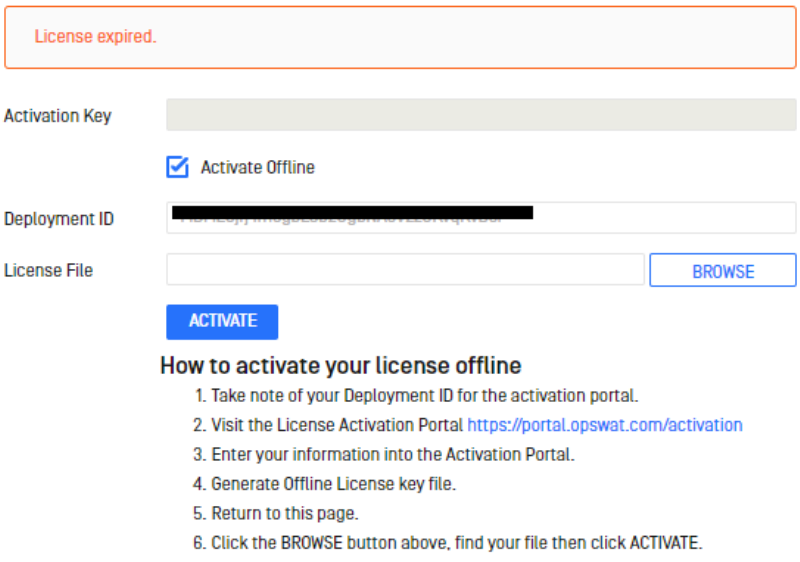
Managing License Information

MetaDefender Kiosk requires a valid license to be applied before use. The MetaDefender Kiosk activation key can be applied on the License page in the Management Console.



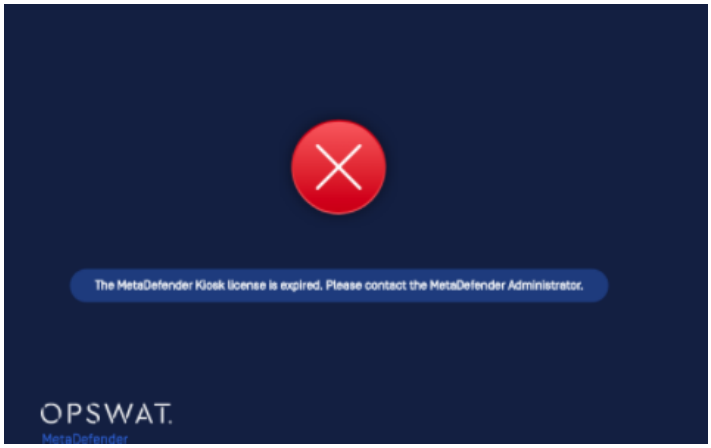
activation required

Offline activation can be done if MetaDefender Kiosk is not connected to the Internet. Follow the instructions on the License page to activate MetaDefender Kiosk.



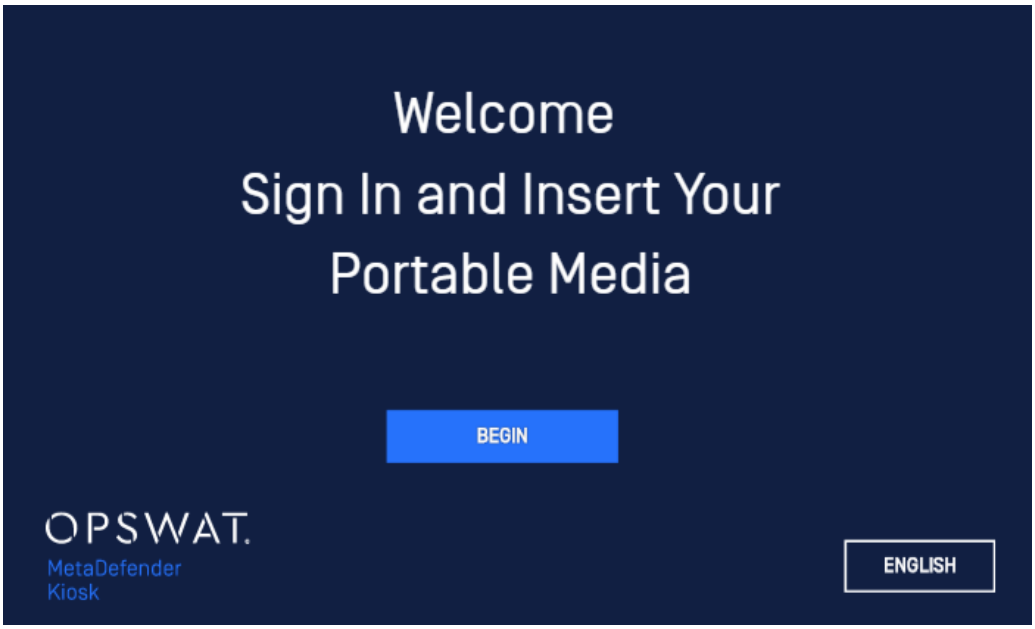
license expired

If the MetaDefender Kiosk license has expired or is invalid, the MetaDefender Kiosk user interface displays an error and does not allow users to proceed.



red x

On successful activation, the home screen will display the Welcome page.



Upgrading MetaDefender Kiosk

Announcement
As of Kiosk 4.5.5, upgrading no longer requires uninstallation of an existing version. The installer can now be ran with a Kiosk already installed.

Upgrade from Kiosk 4.6.0
As a critical issue with login via AD authentication, Kiosk 4.6.0 was removed and unable to be upgraded in place. To upgrade to the latest version from the Kiosk 4.6.0, the following actions should be followed:

1. Remove the `Log` folder in the installation directory
2. Generate a support package from the Management Console
3. Uninstall Kiosk 4.6.0
4. Install the latest version
5. Configure Kiosk from the beginning. The support package from step `2` can be utilized to verify any missed settings or contact OPSWAT Support for more details.

Upgrade to a new version of Kiosk by running its installer using one of the following methods:

1. Wizard
2. Command Line

Installing Kiosk without uninstalling the previous version helps all configurations, workflow settings, and session history retained.

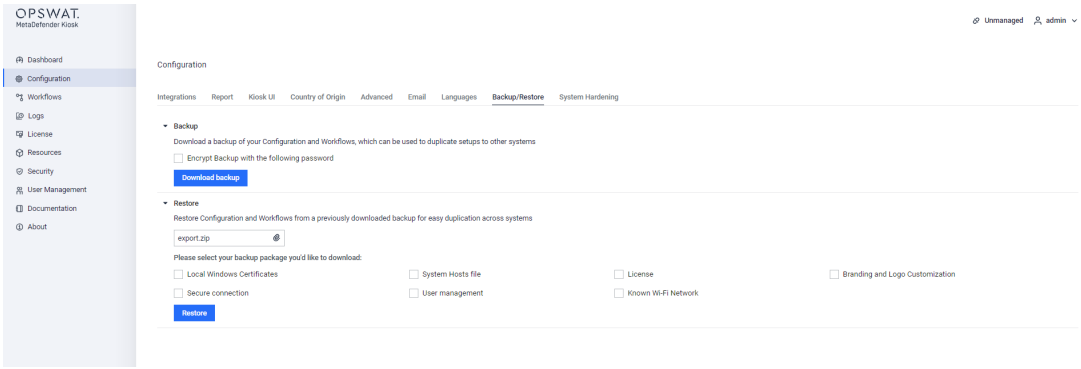
On manual uninstallation, session history will be lost and not retained after the installation of a new version.

Warning
Upgrading from an old version (4.3.X) might cause the Management Console to be inaccessible. A system restart should make it work.

Backing Up and Restoring the Configuration

Import from Kiosk 4.6.0 backup
As a critical issue with login via AD authentication, Kiosk 4.6.0 was removed and unable to be upgraded in place. As the result, the import of Kiosk version 4.6.0 backup is not supported either. The Kiosk administrator is advised to configure the Kiosk from the beginning.

To backup and restore Kiosk configurations, select **Configuration**, select **Backup/Restore**.



Backup and restore Kiosk configuration on Kiosk 4.7.2 or newer

Downloading the configuration backup

Click **Download Backup** to download an archive containing the Kiosk configurations.

Restoring the configuration backup

To restore the Kiosk configurations, click on the **clip icon** to upload the configuration backup file, and click **Restore**.

On **Kiosk version 4.7.2 or newer**, Administrator can select additional system settings to restore:

- Local Windows Certificates: Restore all trusted certificates from Certificate Microsoft Management Console (MMC)
- System Hosts file: Restore the custom Hosts file at *C:\Windows\System32\drivers\etc\hosts*
- License: Restore the activated Kiosk license
- Branding and Logo Customization: Restore logo and branding files found in *C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\en\resources*
- Secure connection: Restore the security certificate and enable Secure Connection option
- User management: Restore configured User Directories (AD, SSO and Entra ID) and accounts
- Known Wi-Fi network: Restore the known Wi-Fi networks

- Computer host name: Restore the computer name **(only available in Kiosk 4.7.3)**
- Kiosk sound: Restore custom Kiosk sound file **(only available in Kiosk 4.7.3)**
- MD Core configurations: Restore the configurations and license of MetaDefender Core **(only available in Kiosk 4.7.3)**

Issue when importing the configuration of Core 5.14 when certificate(s) is included
When importing a Core (version 5.14) configuration that includes certificate settings into Kiosk 4.7.5 or earlier, the import will fail. As a result, the connection from Kiosk and My OPSWAT to Core may be disrupted if Core URL was changed from HTTPS to HTTP.

Info
On Kiosk version 4.7.2 or newer, Administrator can backup and restore additional system settings.

Upgrading from MetaDefender Kiosk 3.X

Migrating a deployment from MetaDefender Kiosk 3.X to MetaDefender Kiosk 4.X requires additional steps because of the differences in Kiosk 3.X and 4.X. In addition to the standard upgrade procedure, be aware of the following when upgrading from MetaDefender Kiosk 3.X to MetaDefender Kiosk 4.X.

Upgrade Considerations

1. MetaDefender Kiosk 4.X uses a different licensing mechanism than MetaDefender Kiosk 3.X. Please contact OPSWAT to obtain your replacement license for MetaDefender Kiosk 4.X
2. MetaDefender Kiosk backup configurations from 3.X cannot be imported to 4.X
3. MetaDefender Kiosk 4.X requires MetaDefender Core 4.8.1 or later
4. MetaDefender Kiosk 4.X only supports installation on 64-bit operating systems

How many models of MetaDefender Kiosk are there?

Apart from our Kiosk software product, we can also deliver “Software + Hardware” packages.

Customers can choose between our K or L series of Kiosks. More information for each respective version can be found on our site.

K series - https://www.opswat.com/products/metadefender/kiosk/k-series

L series - https://www.opswat.com/products/metadefender/kiosk/l-series

Mobile Kiosk - https://www.opswat.com/products/metadefender/kiosk/mobile-kiosk

Brochure - https://static.opswat.com/uploads/files/MetaDefender-Kiosk-Brochure-EN.pdf

For more information on the available version feel free to contact our sales team - https://www.opswat.com/get-started

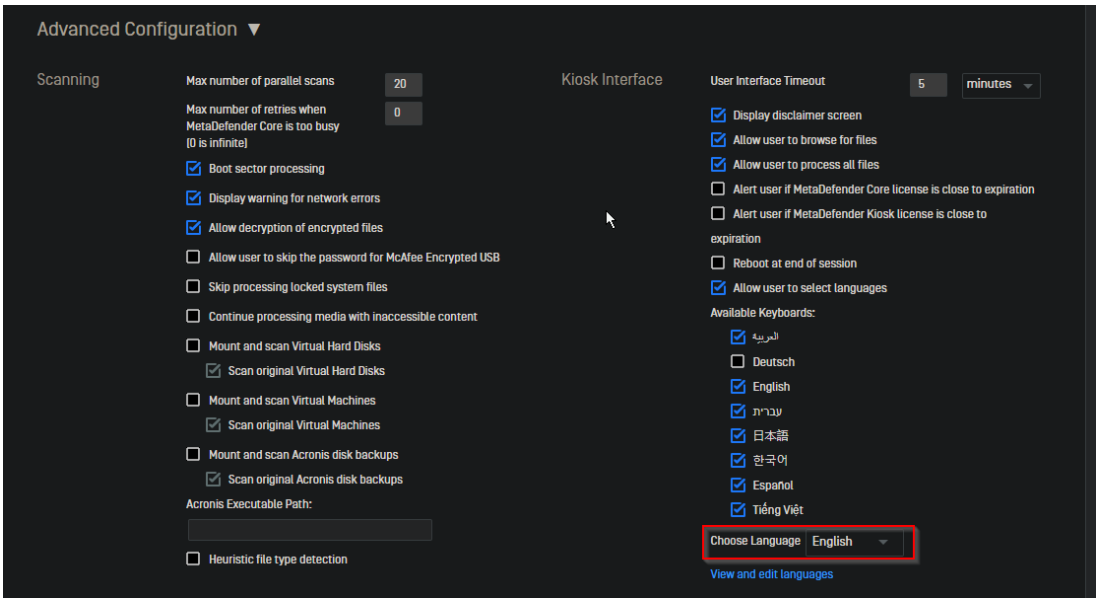
Support
If **Further Assistance** is required, please proceed to log a Support Ticket with the OPSWAT team.

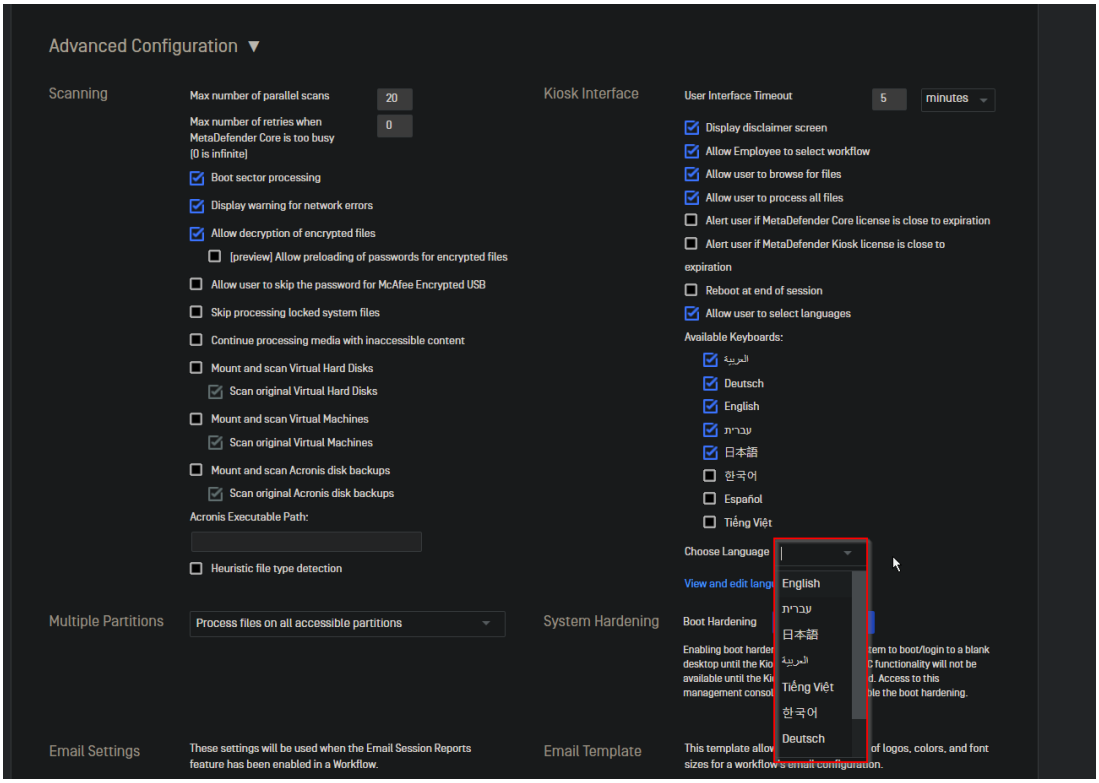
Does MetaDefender Kiosk support multiple languages or customisation?

The language displayed in MetaDefender Kiosk can be changed from the Choose Language drop-down menu in the Configuration section of the Management Console.

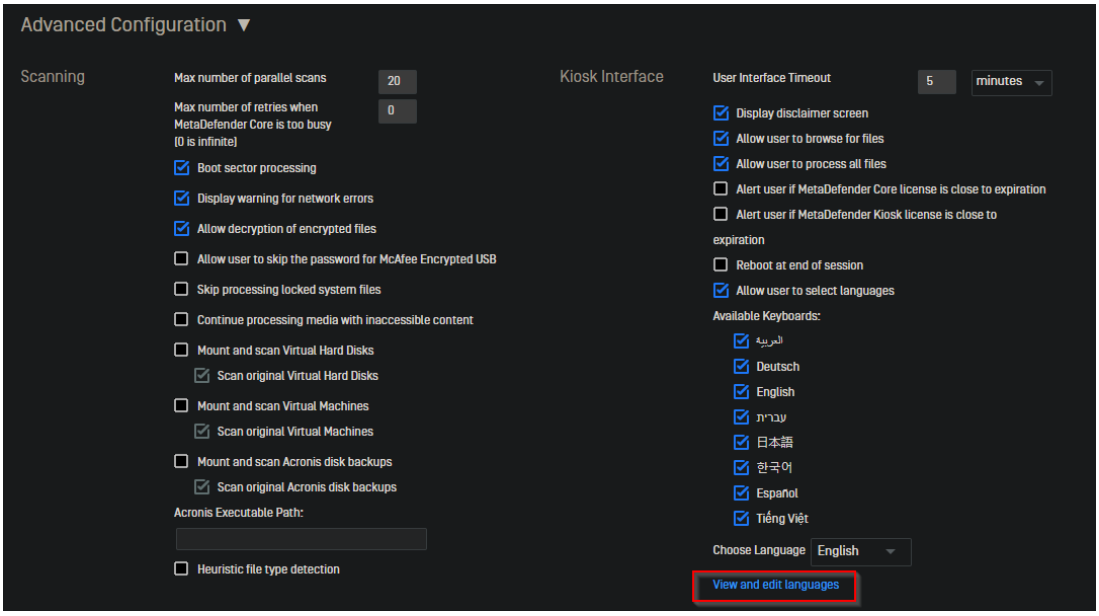
The default languages included are:

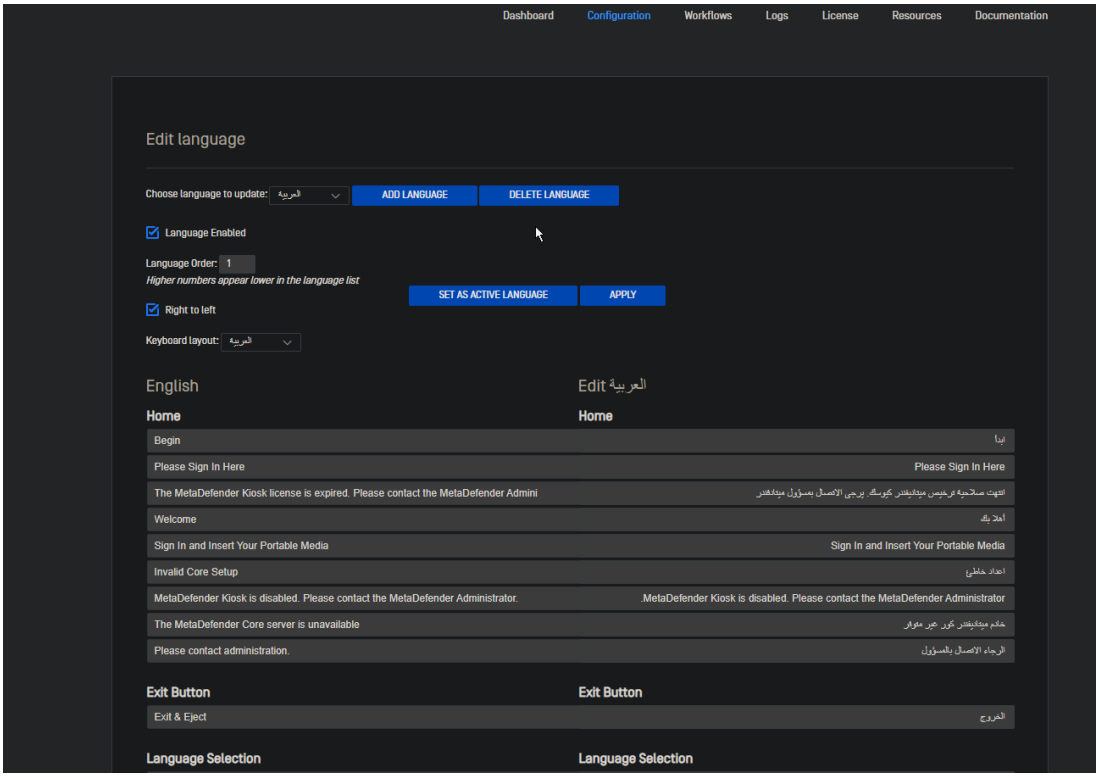
English; Arabic; French; German; Hebrew; Japanese; Korean; Spanish; Vietnamese





If you wish to add a language to the MetaDefender Kiosk UI or edit the translations of any of the existing languages, click View and edit languages.





Support

If **Further Assistance** is required, please proceed to log a Support Ticket with the OPSWAT team.

Performance measurement of post-procesed files

Performance measurement of using multiple threads for post-processing

Copying to Directory

1. Environment

Using the K1001 model device in the local test environment. This is a controlled, isolated environment.

Server	vCPU	Memory (GB)	OS	Disk type
MD KIOSK (K1001)	24	32	Windows 10 IoT Enterprise	SSD

Storage Device (stores data & connects to MD KIOSK server)

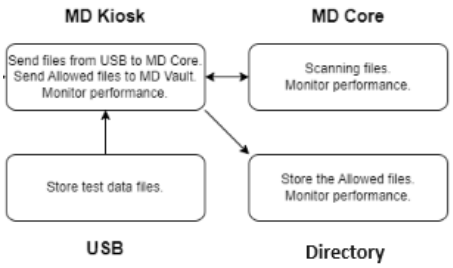
2TB HDD LaCie Rugged Thunderbolt USB-C

Network Bandwidth

1 Gigabit Ethernet

2. Test flow

Files are scanned by MD Core and Allowed files are uploaded to Directory.



3. Dataset

Dataset of 900,000 files totaling ~1TB

4. Product versions to be tested

- MD Kiosk 4.6.6
- MD Core 5.8.0
  - Anti-virus: 1 engine ESET
  - DLP: off
  - CDR: off

- Vulnerability: off
- Archive: off
- FileType: 6.5.1

5. Test result

Scan time: 11h 56m 17s

File Explorer	1 thread	50 threads
more than **6 hours**	• Copy time: **7h 3m 39s** • Throughput (files/hour): 127,463.7	• Copy time: **4h 16m 2s** • Throughput (files/hour): 210,910

Copying to MFT

1. Environment

Using the K1001 model device in the local test environment. This is a controlled, isolated environment.

Server	vCPU	Memory (GB)	OS	Disk type
MD KIOSK (K1001)	24	32	Windows 10 IoT Enterprise	SSD
MD CORE (K1001)	24	32	Windows 10 IoT Enterprise	SSD
MFT (VAULT)	16	32	Windows Server 2022	SSD

USB Storage Device (stores data & connects to MD KIOSK server)

128GB KINGSTON DataTraveler Exodia DTX

Client (runs the Python scripts & collects measurement values)

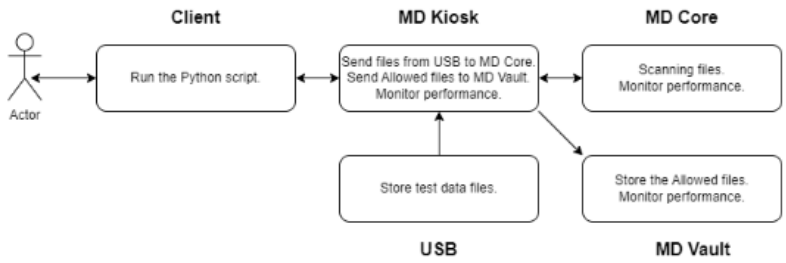
- OS: Windows 2022
- vCPU: 8 cores
- Memory: 16GB

Network Bandwidth

10 Gigabit Ethernet

2. Test flow

Files are scanned by MD Core and Allowed files are uploaded to MFT.



3. Dataset

Detailed information of the dataset below will be used for testing:

File category	File type	Number of files	Total size (MB)	Average File Size (MB)
Adobe	PDF	370	385 MB	1.0 MB
Executable	EXE	45	309.5 MB	6.9 MB
	MSI	15	45.75 MB	3.1 MB
Image	BMP	80	515 MB	6.4 MB
	JPG	420	237.5 MB	0.6 MB
	PNG	345	169 MB	0.5 MB
Media	MP3	135	865 MB	6.4 MB
	MP4	50	500 MB	10.0 MB
Office	DOCX	235	190 MB	0.8 MB
	DOC	225	486 MB	2.2 MB
	PPTX	365	860 MB	2.4 MB
	PPT	355	1950 MB	5.5 MB
	XLSX	340	283.5 MB	0.8 MB
	XLS	335	284.5 MB	0.8 MB
Text	CSV	100	236 MB	2.4 MB
	HTML	1075	76 MB	0.1 MB
	TXT	500	210 MB	0.4 MB
Archive	ZIP	Compressed files: 10 Extracted files: 270	Compressed size: 125.5 MB Extracted size: 156.5 MB	Avg compressed size: 12.6 MB Avg extracted size: 0.6 MB

Sumarry (compressed):

- **Number of files:** 5000
- **Total size (MB):** 7728.5 MB

- **Average File Size (MB):** 1.55 MB average file size

Sumarry (extracted):

- **Number of files:** 5260
- **Total size (MB):** 7759.5 MB
- **Average File Size (MB):** 1.48 MB average file size

Largest file size: 24.7 MB

Smallest file size: 5 KB

4. Product versions to be tested

- MD Kiosk 4.6.6
- MD Core 5.8.0
  - Anti-virus: 5 engines (AhnLab, Avira, ClamAV, ESET, Microsoft Defender)
  - DLP: 2.18.0
  - CDR: 6.8.1
  - Vulnerability: 4.2.416.0
  - Archive: 6.5.1
  - FileType: 6.5.1
- MD MFT 3.6.0.0

5. MD Core settings

The performance will be measured as below MD Core settings.

General settings

- Turn off data retention
- Turn off the engine update

Archive extraction

- Enable engine
- Max recursion level: 99999999
- Max number of extracted files: 99999999
- Max total size of extracted files: 99999999
- Timeout: 10 mins
- Handle archive extraction task as
  - Failed: true
  - Partially: true

Filetype

- Enable engine
- Timeout: 5 mins

Metascan

- Enable 8 engines
- Max file size: 99999999
- Global scan timeout: 20 mins
- Per-engine scan timeout: 5 mins

CDR

- Enable

DLP

- Enable

Archive Compression

- Enable

6. Test result

Scan time: 21 minutes

Copy options	1 thread	4 threads	7 threads
Upload files and preserve directory structure	42 minutes	17 minutes	12 minutes
Upload files, preserve directory structure and send scan results	50 minutes	10 minutes	12 minutes
Upload a zip archive containing the files	2 minutes	2 minutes	2 minutes

Copying to User Media

1. Environment

Using the K1001 model device in the local test environment. This is a controlled, isolated environment.

Server	vCPU	Memory (GB)	OS	Disk type
MD KIOSK (K1001)	24	32	Windows 10 IoT Enterprise	SSD

Source media

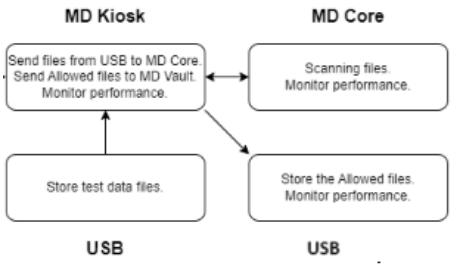
64GB Sandisk Cruzer Glide USB 3.0

Destination media

64GB Kanguru FlashTrust USB 3.0

2. Test flow

Files are scanned by MD Core and Allowed files are uploaded to User Media.



3. Dataset

Dataset of 15,000 files totaling +37GB

4. Product versions to be tested

- MD Kiosk 4.6.6
- MD Core 5.8.0
  - Anti-virus: 1 engine ESET
  - DLP: off
  - CDR: off

- Vulnerability: off
- Archive: off
- FileType: 6.5.1

5. Test result

Scan time: 1h 2m 26s

1 thread	50 threads	100 threads
• Copy time: **28m 47s** • Throughput (files/hour): 31,250	• Copy time: **28m 26s** • Throughput (files/hour): 31,914.9	• Copy time: **29m 22s** • Throughput (files/hour): 30,612.2

Performance measurement of Self Scan

Environment

Using the KIOSK devices in the local test environment.

Model	CPU	Memory (GB)	Disk type	OS
K1001	Intel Core i9-13900 Cores: 24 Logical processors: 32 Base speed: 2.00 GHz	32	SSD	Windows 10 IoT Enterprise LTSC Version: 21H2
K2100	Intel Core i7-8665U Cores: 4 Logical processors: 8 Base speed: 2.11 GHz	16	SSD	Windows 10 IoT Enterprise LTSC Version: 21H2
K3001	Intel Core i9-12900 Cores: 16 Logical processors: 24 Base speed: 2.40 GHz	32	SSD	Windows 10 IoT Enterprise LTSC Version: 21H2

Product Information

- MetaDefender Core version 5.9.0
- Engines:
  - 8 AV engines: AhnLab, Avira, Bitdefender, ClamAV, ESET, K7, Quick Heal, Vir.IT eXplorer
  - Archive: 7.0.1-4917

Test Summary

K1001	4.6.7	4.6.8
Total files	239 715	227 449
MD Core version	5.9.0	5.9.0
Throughput (files/hour)	14 181.2	155 994.8
Scan duration	**16h 39m 10s**	**1h 26m 32s**

K2100	4.6.7	4.6.8
Total files	368 681	335 130
MD Core version	5.9.0	5.9.0
Throughput (files/hour)	13 805.8	34 994.5
Scan duration	**26h 30m 22s**	**9h 23m 59s**

K3001	4.6.7	4.6.8
Total files	360 192	239 422
Throughput (files/hour)	14 178	96 844.3
Scan duration	**24h 50m 33s**	**2h 25m 14s**

Performance measurement

1. Product Information

Product versions to be tested:

- MetaDefender Kiosk 4.7.5
- MetaDefender Managed File Transfer 3.8.0
- MetaDefender Core 5.14.0
- Engines:
  - Metascan:
    - 20 AV engines package + Crowdstrike when testing with CAB file
    - MAX AV engines package when testing with mixed dataset
    - 8 AV engines package when testing with mixed dataset
  - Deep CDR: 7.4.0
  - Proactive DLP: 2.22.1
  - Archive: 7.4.0
  - FileType: 7.4.0
  - File-Based Vulnerability Assessment: 4.2.416.0

2. Environment

MetaDefender Kiosk devices

Using the KIOSK devices in the local test environment. MetaDefender Core is installed on the same system as MetaDefender Kiosk.

Model	CPU	Memory (GB)	Disk type	OS
K1001 (Dell 7410)	Intel Core i9-13900 Cores: 24 Logical processors: 32 Base speed: 2.00 GHz	32	SSD	Windows 10 IoT Enterprise LTSC Version: 21H2
K1001 (Dell 7420)	Intel Core i9-14900 Cores: 24 Logical processors: 32 Base speed: 2.00 GHz	32	SSD	Windows 10 IoT Enterprise LTSC Version: 21H2
K2100	Intel Core i7-1260U Cores: 10 Logical processors: 12 Base speed: 1.10 GHz	32	SSD	Windows 10 IoT Enterprise LTSC Version: 21H2
K3001	Intel Core i9-12900 Cores: 16 Logical processors: 24 Base speed: 2.40 GHz	32	SSD	Windows 10 IoT Enterprise LTSC Version: 21H2

Storage Device

Using to store the dataset and connect to the Kiosk device: 128GB SanDisk USB 3.2 Gen 1

MFT Server

In case the MD Kiosk sends files to MD MFT after scanning, MD MFT is a virtual machine with the following specifications:

OS	vCPU	Memory (GB)	Disk type	Network bandwidth (Gbps)
Windows Server 2022	8	16	SSD	10 Gb Ethernet

Client

Using to run the Python script. The Client is a virtual machine with the following specifications:

OS	vCPU	Memory (GB)	Disk type	Network bandwidth (Gbps)
CentOS Linux 7.9	8	16	SSD	10 Gb Ethernet

3. Test flows

- Flow 1: MD Kiosk sends CAB file to MD Core (21 AV engines) for scanning.
- Flow 2: MD Kiosk sends Mixed dataset to MD Core (MAX AV engines) for scanning.
- Flow 3: MD Kiosk sends Mixed dataset to MD Core (8 AV engines) for scanning.
- Flow 4: MD Kiosk sends Mixed dataset to MD Core for scanning, and Allowed files are copied to MD MFT.

4. Dataset

CAB file:

- Extracted files: 849 479
- Total size of extracted files: 26.5 GB

Mixed dataset:

- Summary (compressed):
  - Number of files: 5000
  - Total size: 7728.5 MB
  - Average file size: 1.55 MB
- Summary (extracted):
  - Number of files: 5260
  - Total size: 7759.5 MB
  - Average file size: 1.48 MB
- Largest file size: 24.7 MB
- Smallest file size: 5 KB

File category	File type	Number of files	Total size (MB)	Average file size (MB)
Adobe	PDF	370	385 MB	1.0 MB
Executable	EXE	45	309.5 MB	6.9 MB
	MSI	15	45.75 MB	3.1 MB
Image	BMP	80	515 MB	6.4 MB
	JPG	420	237.5 MB	0.6 MB
	PNG	345	169 MB	0.5 MB
Media	MP3	135	865 MB	6.4 MB
	MP4	50	500 MB	10.0 MB
Office	DOCX	235	190 MB	0.8 MB
	DOC	225	486 MB	2.2 MB
	PPTX	365	860 MB	2.4 MB
	PPT	355	1950 MB	5.5 MB
	XLSX	340	283.5 MB	0.8 MB
	XLS	335	284.5 MB	0.8 MB
Text	CSV	100	236 MB	2.4 MB
	HTML	1075	76 MB	0.1 MB
	TXT	500	210 MB	0.4 MB
Archive	ZIP	Compressed files: 10 Extracted files: 270	Compressed size: 125.5 MB Extracted size: 156.5 MB	Avg compressed size: 12.6 MB Avg extracted size: 0.6 MB

5. MetaDefender Core settings

General settings

- Turn off data retention
- Turn off the engine update

- Max size:
  - File scan: 9999999999999 MB
  - URL file download: 9999999999999 MB

Metascan

- Enable engines depend on the testing package
- Per AV engine scan: 1 min
- Global scan: 10 mins
- File download: 5 mins

Deep CDR

- Enable engine
- 135 file types

Proactive DLP

- Enable engine

Archive Extraction

- Enable engine
- Max recursive level: 99999999
- Max number of files extracted: 99999999
- Max total size of extracted files: 99999999
- Timeout: 90 mins

Archive Compression

- Enable engine

FileType

- Enable engine
- Timeout: 5 mins

File-Based Vulnerability Assessment

- Enable engine

6. Test Summary

> **Info**
> Due to a technical issue, the scan results for K1002 (Dell 7420) will be based on the previous results obtained with Core 5.13.0 and Kiosk 4.7.3.

Flow 1: MD Kiosk sends CAB file to MD Core (21 AV engines) for scanning.

Device	Duration	Avg. CPU Usage	Avg. Memory Usage	Avg. Disk Speed (KB/s)	Throughput (objects/hour)	Throughput (objects/hour)
K1001 (Dell 7410)						
K1002 (Dell 7420)	3 hours 27 minutes	50.4%%	57.6%	Read: 2,451.8 Write: 17,118.4	246,659	0.3
K2100	7 hours 24 minutes	91.9%	50.8%	Read 1,256.4 Write 7,865.7	114,714.3	0.1
K3001	4 hours 14 minutes	67.8%	52.8%	Read 2,186.1 Write 11,357.2	200,527.4	0.2

Flow 2: MD Kiosk sends Mixed dataset to MD Core (MAX AV engines) for scanning.

Device	Duration	Avg. CPU Usage	Avg. Memory Usage	Avg. Disk Speed (KB/s)	Throughput (objects/hour)	Throughput (files/hour)
K1001 (Dell 7410)						
K1001 (Dell 7420)	2 hours 21 minutes	53.2%	69.6%	Read: 5,759.6 Write: 10,892.1	54,182.7	2,129.9
K2100	5 hours 3 minutes	88.4%	55.2%	Read 3,070 Write 6,393.1	25,187.7	990.3
K3001	2 hours 50 minutes	69.3%	73.9%	Read 7,396.2 Write 13,534.7	44,764.5	1,759.9

Flow 3: MD Kiosk sends Mixed dataset to MD Core (8 AV engines) for scanning.

Device	Duration	Avg. CPU Usage	Avg. Memory Usage	Avg. Disk Speed (KB/s)	Throughput (objects/hour)	Throughput (files/hour)
K1001 (Dell 7410)	36 minutes	36.3%	42.4%	Read 9,627.8 Write 16,248.2	210,572.5	8,268.3
K1001 (Dell 7420)	34 minutes	34.3%	39.6%	Read 9,663.6 Write 11,680.4	224,683.2	8,832.2
K2100	1 hour 13 minutes	79.6%	41.5%	Read 4,323.4 Write 6,826	104,058.8	4,090.9
K3001	48 minutes	53.4%	44.0%	Read 8,067.8 Write 11,564.3	157,808.21	6,204.8

Flow 4: MD Kiosk sends Mixed dataset to MD Core for scanning, and Allowed files are copied to MD MFT.

Device	Duration	Avg. CPU Usage	Avg. Memory Usage	Avg. Disk Speed (KB/s)	Avg. Network Speed (KB/s)	Throughput (objects/hour)	Throughput (files/hour)
K1001 (Dell 7410)							
K1001 (Dell 7420)	20 minutes	59.6%	36.7%	Read 28,855.8 Write 45,143.1	Receive 40.3 Send 6,737.9	534,171.1	15,000
K2100	36 minutes	49.7%	38.5%	Read 8,928 Write 10,438.8	Receive 27.5 Send 4,597.5	248,804.4	8,356.5
K3001	25 minutes	34.7%	36.8%	Read 13,645.2 Write 12,335.3	Receive 7.2 - Send 1.2	302,825.3	11,889

Database password protection

The KIOSK database is password-protected to safeguard sensitive customer information and ensure secure KIOSK operations.

Each KIOSK has a unique database password, accessible only by the KIOSK services on that specific system. The password is generated using three components:

- Hardware information specific to that KIOSK.
- A KIOSK security salt.
- User input provided during installation, adding an optional extra layer of security as outlined in Installing MetaDefender Kiosk Using the Install Wizard.

Info
The password is created once and retained during KIOSK upgrades.

The database password and the user-input encrypted key are both hashed and securely stored for internal usage at:

- `C:\ProgramData\OPSWAT\Metadefender\blue`
- `C:\ProgramData\OPSWAT\Metadefender\green`

Warning
Missing these files can lead to a critical failure of the KIOSK, as the system will be completely unable to authenticate to the database.

Configuring with MetaDefender Core

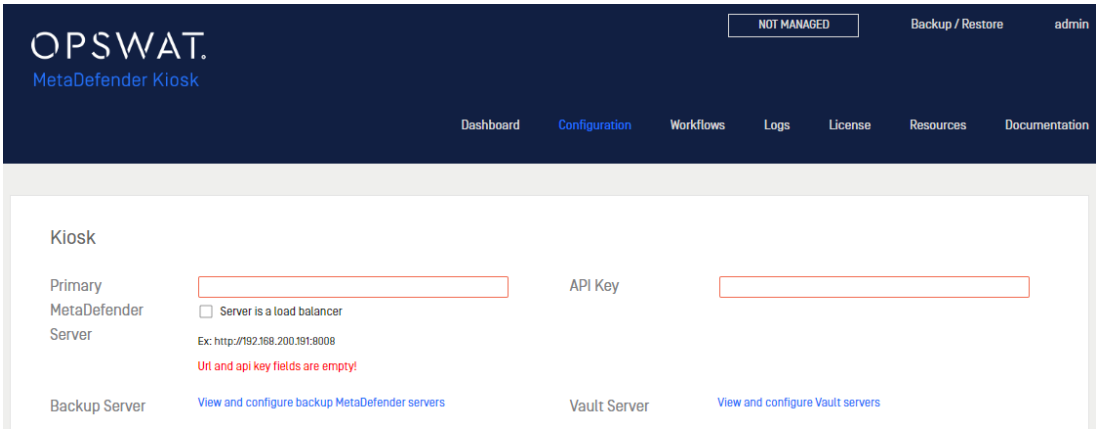
MetaDefender Kiosk requires MetaDefender Core for multi-scanning functionality.

Setting up MetaDefender Core with MetaDefender Kiosk consists of the following steps:

Detecting the MetaDefender Core server URL

If MetaDefender Core is installed on a remote machine from Kiosk, the server URL must be specified.

1. Access your MetaDefender Kiosk Management Console at `http(s)://<ip or dns>:8009`. You can also access the Kiosk Management Console using Windows **Start** > **OPSWAT** > **MetaDefender Kiosk Management Console**.
2. Click **Configuration** and enter your MetaDefender Core URL



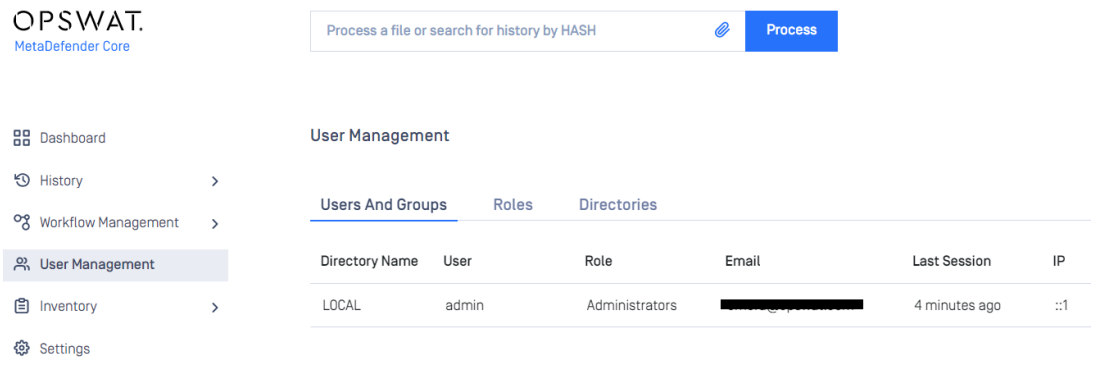
3. Additional backup servers can be added in case the primary server becomes inaccessible, its license expires, or other issues the primary server might encounter.

Authenticating the Core connection

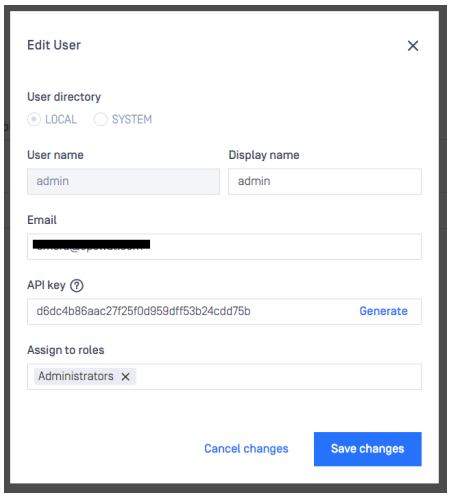
You must authenticate your connection by obtaining an API key from the MetaDefender Core Management Console.

> **Info**
> MetaDefender Kiosk requires the MetaDefender Core API key to be assigned an `Administrator` role

1. Access the MetaDefender Core Management Console
2. Select `User Management`



3. Click the desired user with an Administrator role and copy the contents of the `API key` field. If an API key has not been previously generated click the `Generate` link and make sure to save changes.



4. Return to the MetaDefender Kiosk Management Console and click the `Configuration` tab
5. Paste your Core API key value in the `API Key` field

Associating workflows in Kiosk to workflows in Core

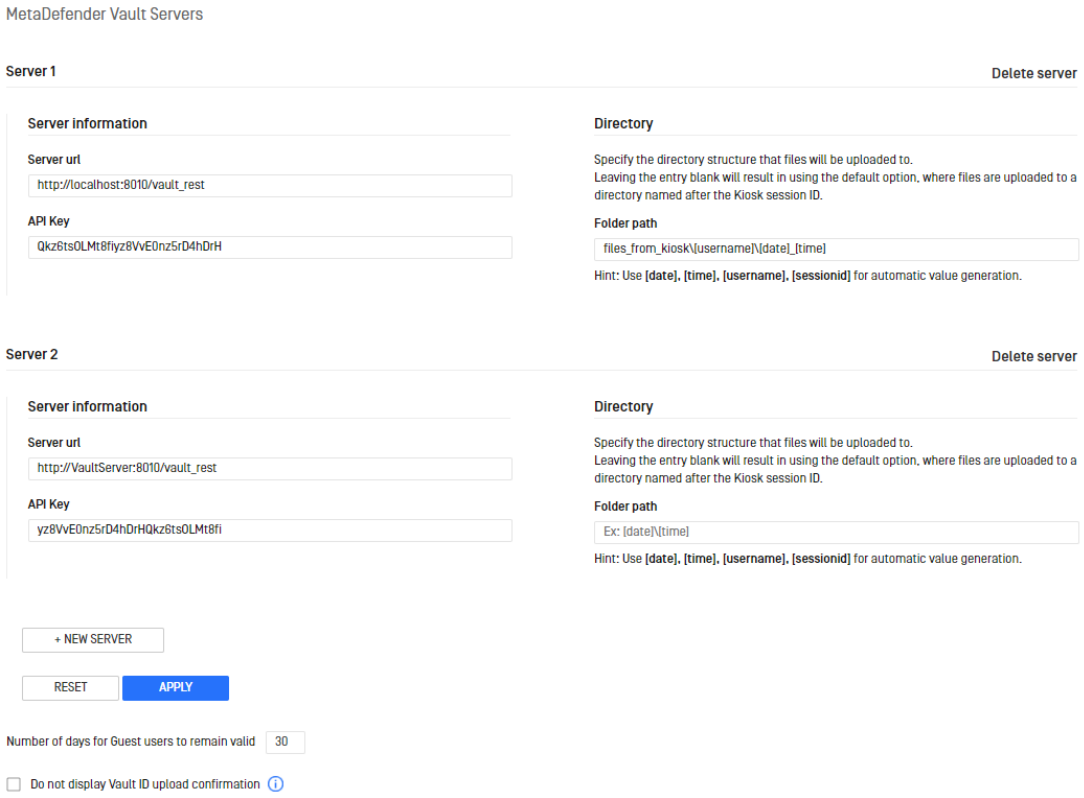
Refer to Selecting a Server to Process Files

Configuring with MetaDefender Managed File Transfer

> **Info**
> It is recommended for both Kiosk and MFT to be connected to the same user directory in order for the integration to work seamlessly

MFT servers are configured from the Kiosk global configuration page. In the MFT Server section, click `View and configure MFT servers`. This will open the `MetaDefender MFT Servers` page where multiple servers can be added and configured.

Each entry is validated for a successful connection. Once a MFT server is added, it can be selected in all sections of the configuration where a MFT server is required.



- **Server url** MFT REST server's URL
- **API Key** API key obtained from the MetaDefender Managed File Transfer management interface

- **Folder path** The directory structure specified in which files are uploaded to. The default is a root folder of the respective Kiosk session ID.
    - **[date]** current date (Year-Abbreviated month-Day), e.g. 2020-Mar-10
    - **[time]** time of session (Hour-Minute-Second), e.g. 18-42-28
        - Note: [18:42:28] is invalid name on Windows OS, [18-42-28] is used instead
    - **[username]** user logged into the Kiosk session
    - **[sessionid]** Kiosk session id

Number of days for Guest users to remain valid indicates how long a guest user is valid before MFT removes the user and files associated to it.

Do not display MFT ID upload confirmation a MFT ID will not be displayed when files are uploaded

For installing a MFT self-signed certificate, it is necessary to add the certificate configured on MFT into the Kiosk configuration. Please refer to Trusting an HTTPS OPSWAT product to add a certificate into the Kiosk configuration.

Arbit Data Diode configuration

This guide describes how to deploy MetaDefender Kiosk, an Arbit data diode, and a MetaDefender Managed File Transfer server for the following use case.

1. Portable media is scanned by MetaDefender Kiosk
2. Clean files are passed through an Arbit data diode to a MFT Server
3. User downloads files from the MFT server

System Deployment

The following should be done before configuring the individual systems.

1. Install MetaDefender Kiosk with MetaDefender Core on the low-side network
2. Install the Arbit data diode with the receiving side in the low-side network and the transmitting side on the high side network
    a. Assign a static IP address to the low side
    b. Assign a static IP address to the high side
3. Install the MFT server on the high side network
    a. Assign a static IP address

MFT Server Configuration

1. Create the known user accounts on the MFT server
    a. Note the account that should be used as the 'from' account for files coming from MetaDefender Kiosk
2. Generate the Authorization api key

Arbit Data Diode Configuration

1. Define the URL list on the high side of the data diode to include the MFT server
    a. URL List includes:
        i. http://<MFT IP Address>:8000/vault_rest/file
        ii. http://<MFT IP Address>:8000/vault_rest/transfer
        iii. http://<MFT IP Address>:8000/vault_rest/transfer_diode
        iv. http://<MFT IP Address>:8000/vault_rest/transfer_file
        v. http://<MFT IP Address>:8000/vault_rest/transfer_file_diode
        vi. http://<MFT IP Address>:8000/vault_rest/file/status/<file_id>
        vii. http://<MFT IP Address>:8000/vault_rest/file/<file_id>
        viii. http://<MFT IP Address>:8000/vault_rest/folder_content/<id>/<start>/<count>
        ix. http://<MFT IP Address>:8000/vault_rest/root_folder
        x. http://<MFT IP Address>:8000/vault_rest/files/my/<start>/<count>

xi. http://<MFT IP Address>:8000/vault_rest/transfer_file_chunk_diode
xii. http://<MFT IP Address>:8000/vault_rest/authenticate
xiii. http://<MFT IP Address>:8000/vault_rest/scan

MetaDefender Kiosk Configuration

1. Configure the appropriate MetaDefender Kiosk workflow to enable Copy To MFT in the post-action
2. Put in the URL of the data diode low-side receiver
    a. http://<diode low-side IP address>:8080/pitcherrestapi/transfer/<URL List>
3. Enter the Authorization token generated by the MFT Server
4. Enter the Sender MFT account that was created on the MFT server

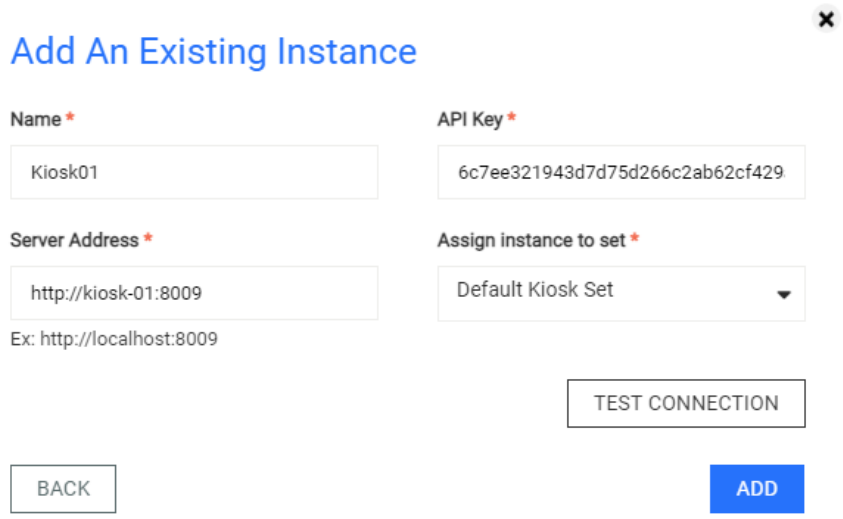
Configuring with Central Management

Management consists of configuring the global configuration, workflow settings, and viewing health / license status of multiple Kiosk instances. This guide outlines how to add a Kiosk instance to Central Management, please refer to Central Management documentation for further product details.

Adding a Kiosk instance

1. Access the Central Management Console at `http(s)://<ip or dns>:9000`
2. On the left hand panel navigate to `Inventory` → `MetaDefender Kiosk`
3. Click `Add New Instance` in the right hand corner
4. Click `Add an existing Instance` in the pop up panel
5. Fill in the required fields `Name`, `Server Address`, `API Key`, `Assign instance to set`, and click `Add`

> **Info**
> The value for the `API Key` field is the generated API key of an administrator user of MetaDefender Kiosk. Refer to management console user information on how to generate it.



Trusting an HTTPS OPSWAT product

To ensure MetaDefender Kiosk operates correctly with another OPSWAT product configured to use HTTPS (refer to the respective product's user guide for HTTPS setup), the security certificates must be fully trusted on the MetaDefender Kiosk system.

Certificate must be valid and trusted
The security certificates need to be valid and trusted by the MetaDefender system. Otherwise, Kiosk will encounter issues when integrating with other products (in HTTPS).

If a certificate chain is in use, the Kiosk system must fully trusted the chain (root certificate, intermediate certificates and end-entity certificate)

Trusting self signed certificates

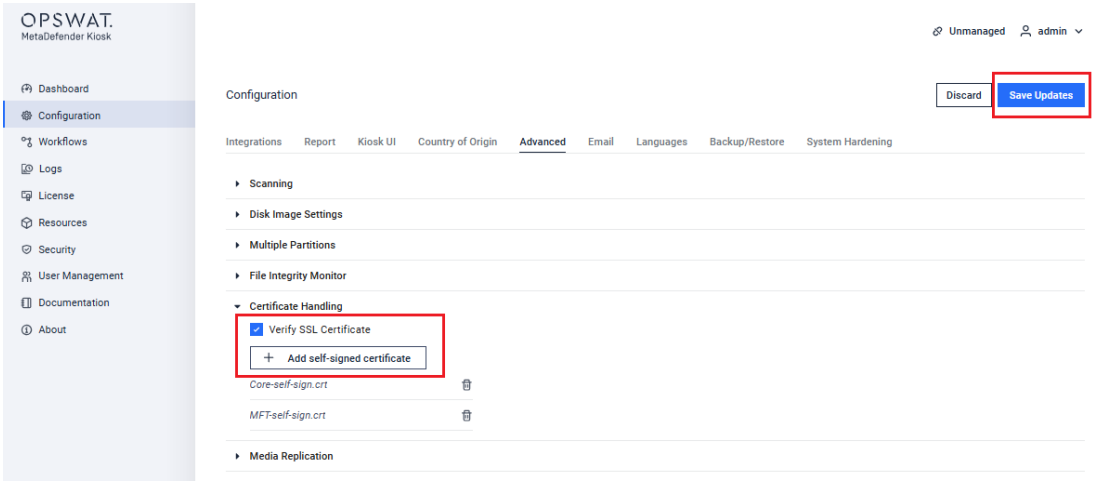
To trust self signed certificates, the public certificates from the other product must be added to the Kiosk configuration.

From Kiosk WebMC, navigate to **Configuration**, select **Advanced**, expand **Certificate Handling**

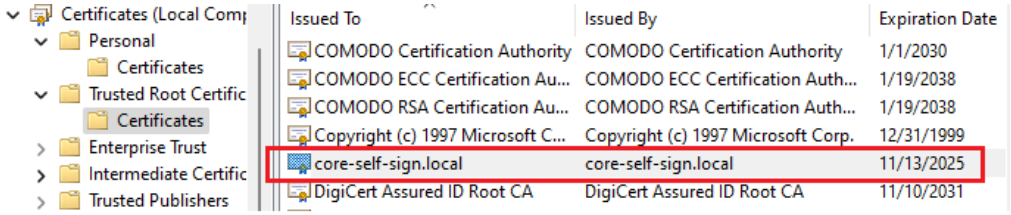
Step 1. Enable **Verify SSL Certificate**

Step 2. Click on **Add self-signed certificate**, browse to the public certificates and upload

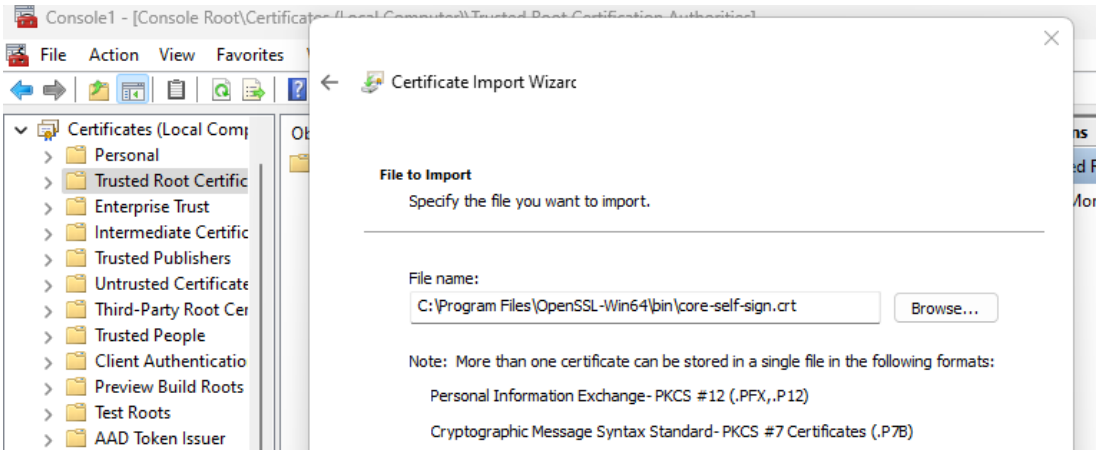
Step 3. Click on **Save Updates**



Once the certificates are added, they will be stored in Microsoft Certificate Store (Trusted Root Certification Authority).



Alternatively, administrators can add certificates directly to Microsoft Certificate Store (as screenshot below), but they will not appear under Kiosk WebMC.



Overview

MetaDefender Kiosk helps protect your network by enabling control over the flow of data into and out of your organization. It can be used as a media scanning station on your own hardware or on OPSWAT's custom-made kiosks. Media such as USB devices, DVDs, SD cards, flash drives, or floppy disks are processed by Kiosk. After the scan is complete, Kiosk generates a detailed report.

This user guide covers installing, configuring, upgrading, using, and troubleshooting MetaDefender Kiosk.

Key Features

- Protection against zero-day attacks (MetaDefender Core integration)
- Customized data security policies
- Control over data flow
- Active Directory authentication
- Custom Authentication
- Portable Media support including floppy disks, SD cards, CDs, DVDs, encrypted USB, and more
- UI localization
    - Contains bundled language translations and the ability to manually additional languages
- Securely wipe USB drives
- Easier system hardening

User authentication

MetaDefender Kiosk has the following authentication features:

- Active Directory authentication
- Support for Custom Authentication Module

Peripheral media

MetaDefender Kiosk automatically detects multiple peripheral media insertions for the following media types:

- USB devices
- CDs/DVDs/Blu-ray
- Card readers
- SD cards
- Floppy disks

Info
Not all USB devices are currently supported. If you have a specific device you need supported, please contact OPSWAT support.

Encrypted USB devices

MetaDefender Kiosk can unlock encrypted USB devices with a given password and process its contents. Kiosk supports the following encrypted USB devices:

Device	Software Version	Firmware Version	Scanning	Wipe	File Handling	Notes
Avira-Iron-Drive I	InfoPure - 3.201812	-	✔	▯	✔	
Biocryptodisk-ISPX	-	-	✔	-	-	
Buffalo RUF2-HSCT	PASSWORD - 2.67	-	✔	✔	✔	
Buffalo RUF3-HSL	OPEN_HS - 2.68	-	✔	✔	✔	Not supported as copy -to destination with all encrypted scan source devices, except **SanDisk Cruzer Enterprise FIPS Edition** and **Bitlocker USBs**.
DataLocker Sentry 3 FIPS	6.8.1.0	3.05	✔	✔	✔	
DataLocker Sentry ONE	6.8.1.0	03.05	✔	✔	✔	Versions managed with SafeConsole are also supported
DataTraveler Vault Privacy 3.0 - (DTVP30)	3.0.1.1		✔	✔	✔	
DataTraveler Vault Privacy 3.0 - (DTVP30M-R)	4.8.2.1		✔	✔	✔	
Integral Courier FIPS 197	1.0.3.1	-	✔	-	-	
IronKey D250	3.4.3.0		✔	✔	✔	
IronKey D300	3.4.3.0		✔	✔	✔	

Device	Software Version	Firmware Version	Scanning	Wipe	File Handling	Notes
IronKey D300S	3.4.3.0		✔	✔	✔	Re-enter the password when the use of an incorrect password has not been supported yet.
IronKey D500S	3.4.3.0		✔	✔	✔	
IronKey S1000	6.7.0.0		✔	✔	✔	
Kanguru Defender Elite 30	-	-	✔	✔	✔	
Kanguru Defender Elite 200	4.0.8.1	-	✔	✔	✔	
Kanguru Defender Elite 300	-	-	✔	✔	✔	
Kanguru Defender 2000	5.1.6.8	-	✔	✔	✔	
Kanguru Defender 3000	5.6.8.0	-	✔	✔	✔	
McAfee Complete Data Protection	4.3.0.224	-	✔	✘	-	McAfee File and Removable Media Protection client is installed on the system that MetaDefender Kiosk is installed.

Device	Software Version	Firmware Version	Scanning	Wipe	File Handling	Notes
Trellix File and Removable Media Protection *As of December 30, 2022, McAfee File and Removable Media Protection is now known as Trellix File and Removable Media Protection (Trellix FRP)*	5.4.3.170	-	✔	✔	✔	Trellix File and Removable Media Protection client is installed on the system that MetaDefender Kiosk is installed.
Microsoft BitLocker	-	-	✔	✔	✔	Supports BitLocker To Go using passwords. MetaDefender Kiosk does not support BitLocker encryption using key files, smart cards, or VHD (Virtual Hard Drive) BitLocker encryptions.
SanDisk Cruzer Enterprise FIPS Edition	2.5 SDK 1.2.10.12	6.615	✔	-	-	
SanDisk Cruzer Contour U3 based USB	4.08 U3 Launchpad - 1,6,1,1	-	✔	-	-	
SDMS MkIII AES Duoulock	1.0.0.8	1.21	✔	✔	✔	
USB Flash Security	4.1.12.17	-	✔	-	-	

Device	Software Version	Firmware Version	Scanning	Wipe	File Handling	Notes
Viasat Eclypt	4.1.14	-	✔	✔	✔	The Eclypt Management Application (`ema-ui.exe`) must be installed on the system in order to unlock the device.
Viasat Freedom 600	4.1.14	-	✔	✔	✔	The Eclypt Management Application (`ema-ui.exe`) must be installed on the system in order to unlock the device.
Viasat Freedom 100	4.1.14	-	✔	✔	✔	The Eclypt Management Application (`ema-ui.exe`) must be installed on the system in order to unlock the device.

Warning
Encrypted devices are not supported by OPSWAT Media Validation Agent (OMVA)

Media handling

MetaDefender Kiosk's media handling features include the following:

- Can process drives with multiple partitions
- Can process full or partial media
- Can wipe/format USB drives
- Supports integration with MetaDefender Managed File Transfer for uploading files for processing or uploading/downloading processed files
- USB device soft eject
- CD/DVD eject

Processing files

MetaDefender Kiosk uses MetaDefender Core to process files. MetaDefender Core has the following processing features:

- Scanning with multiple anti-malware engines
- Data sanitization
- Application vulnerability detection
- Heuristics for zero-day threats
- Archive extraction
- File type verification
- Workflow engines

Processing session results

After processing media, MetaDefender Kiosk allows you to view detailed logs and print results.

Customizable interface

The MetaDefender Kiosk user interface includes multiple display languages:

- English
- Arabic
- Hebrew
- Korean
- Vietnamese
- German
- Japanese
- Spanish
- French

With the additional support of customizing the bundled languages or adding other languages.

On-screen keyboards are also supported for all of these languages.

System hardening

MetaDefender Kiosk comes with a variety of system hardening features for additional security:

- Disables autorun of inserted media
- Users can only exit by pressing `ALT+S` and if Kiosk is configured to require a password to exit, entering the exit password
- User interface blocks direct access to the underlying system and unnecessary keystrokes
- Runs automatically on system startup

Defending against BadUSB devices

A range of BadUSB devices, including well-known ones like RubberDucky and BashBunny, mimic standard USB Flash Storage devices in appearance. However, beneath their facade, they utilize a USB keyboard interface when connected to host systems. These malicious devices execute keystroke sequences designed to initiate processes, establish shell access, and manipulate system configurations using shortcuts, among other tactics.

With the built-in MetaDefender Kiosk hardening measures, Kiosk significantly enhances its immunity against keyboard-based BadUSB attacks. This safeguards against keystrokes originating from BadUSB devices, which attempt to trigger shortcuts or interact with the Windows OS, by effectively suppressing such attempts. Moreover, the scanning of storage space on BadUSB devices remains intact, thereby enabling the identification and reporting of any malware that may be detected.

Management Console

The MetaDefender Kiosk Management Console allows you to manage the MetaDefender Kiosk system through a web browser.

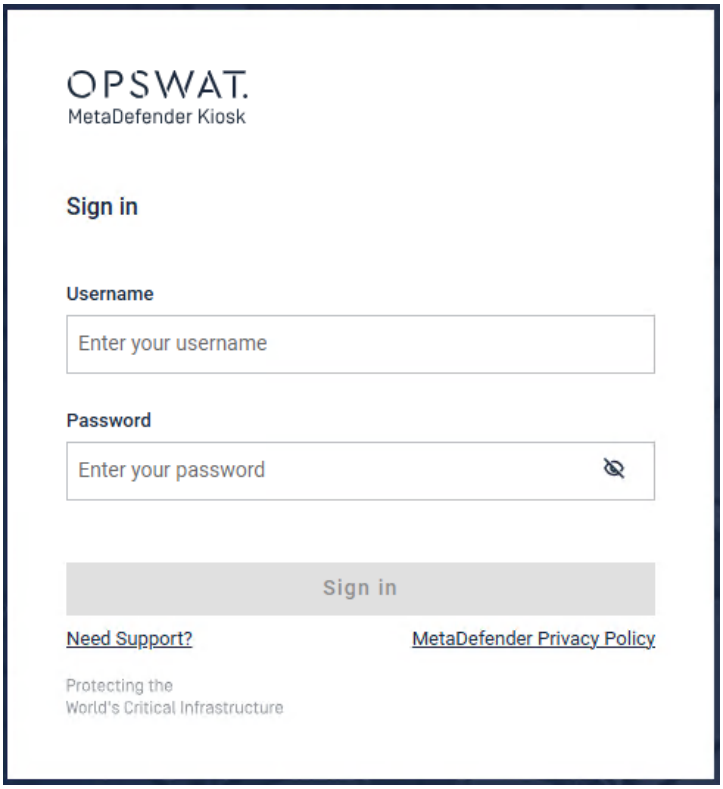
Supported browsers

- Chrome
- Firefox
- Edge

Access to the console

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 Management Console.

A user must log in to access the management console. The username is case-insensitive. A user can either be local to the management console or from a connected user directory. For local users, a maximum of 5 unsuccessful login attempts are allowed until the management console disallows any further logins for 30 minutes. For users from a user directory, any lock out security is expected to be handled on the user directory side. Once logged in, if no activity is made for some time, the idle user will be automatically logged out.



Kiosk Console login

Access allowed for each role

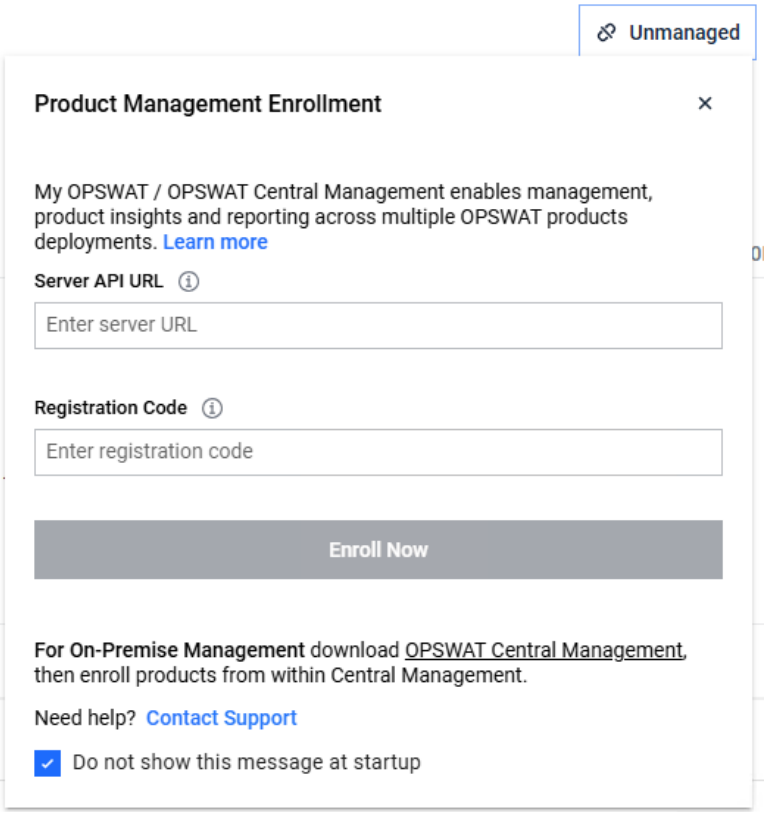
An administrator is allowed to access all features of the Management Console

An auditor is only allowed to view and retrieve logs; no changes can be made to the Kiosk under this role

	User role	
Management Console section	**Administrator**	**Auditor**
Dashboard	✔	✔
Configuration	✔	●
Workflows	✔	●
Logs	✔	✔
License	✔	●
Resources	✔	✔
Documentation	✔	✔
Central Management Details	✔	✔
• Disconnect (when managed)	✔	●
Backup/Restore	✔	●
Security	✔	●
Login Settings	-	-
• User Directories	✔	●
• Local Users	✔	●
• Change Password (*local user only*)	✔	✔

Product Management Enrollment

Logging in to the Management Console will display an enrollment dialog menu:



Product management enrollment

This is currently an experimental feature phase rollout to allow enrolling & managing a Kiosk with `My OPSWAT`.

Viewing basic instance inventory and license information will be supported in a future `My OPSWAT` release in September 2023.

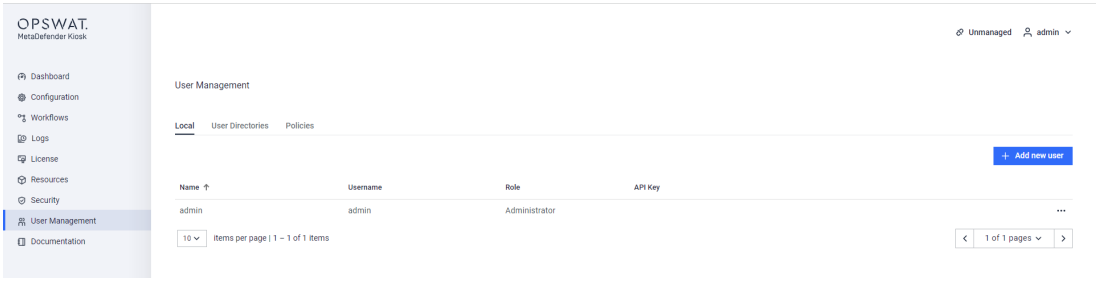
Further management capabilities will be rolled out in subsequent releases.

Kiosk will continue to fully support On-Premise Management via Central Management v7 - read Configuring with Central Management for further guidance.

Review Continue reading for more details on the Management Console and configuration settings.

Login Settings

Management Console users are managed in the **User Management** section.



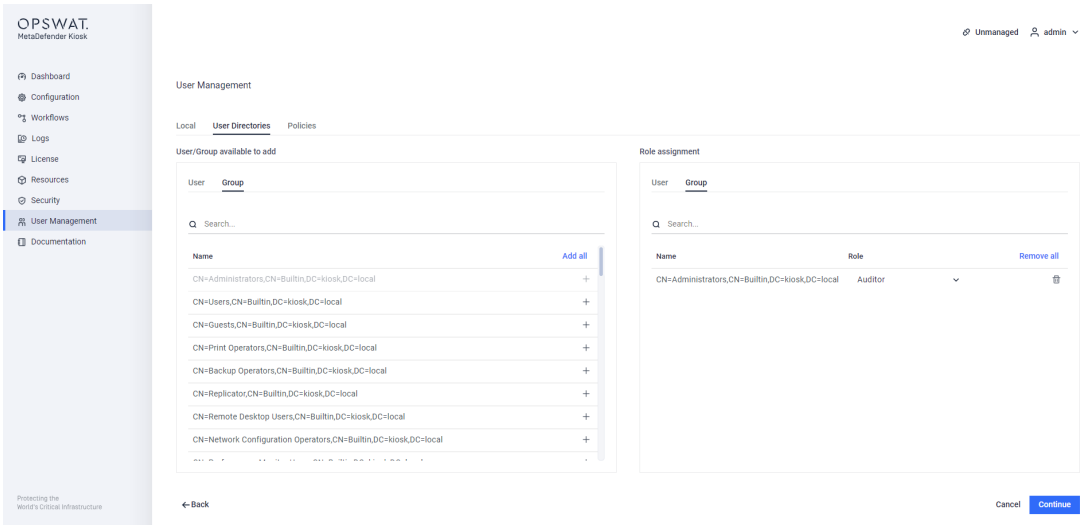
User Management configuration page

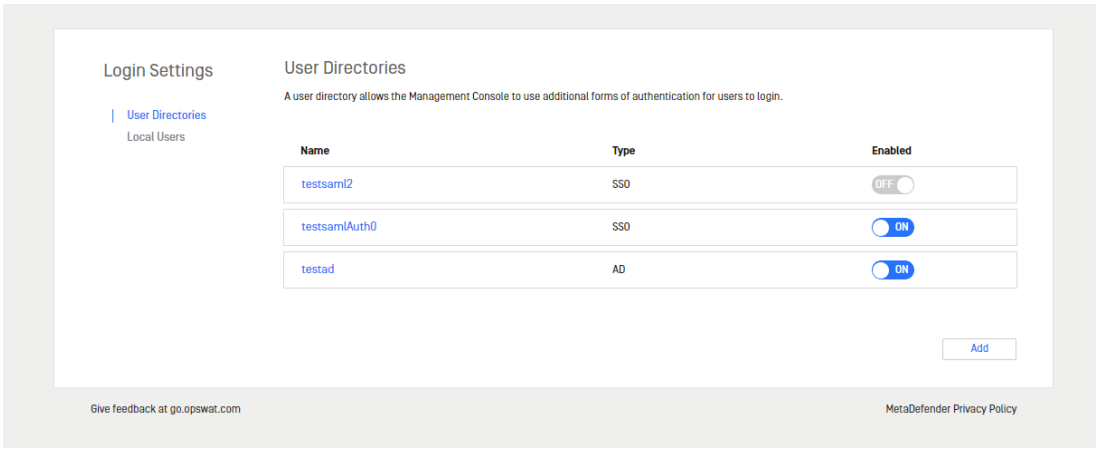
This page consists of multiple sections:

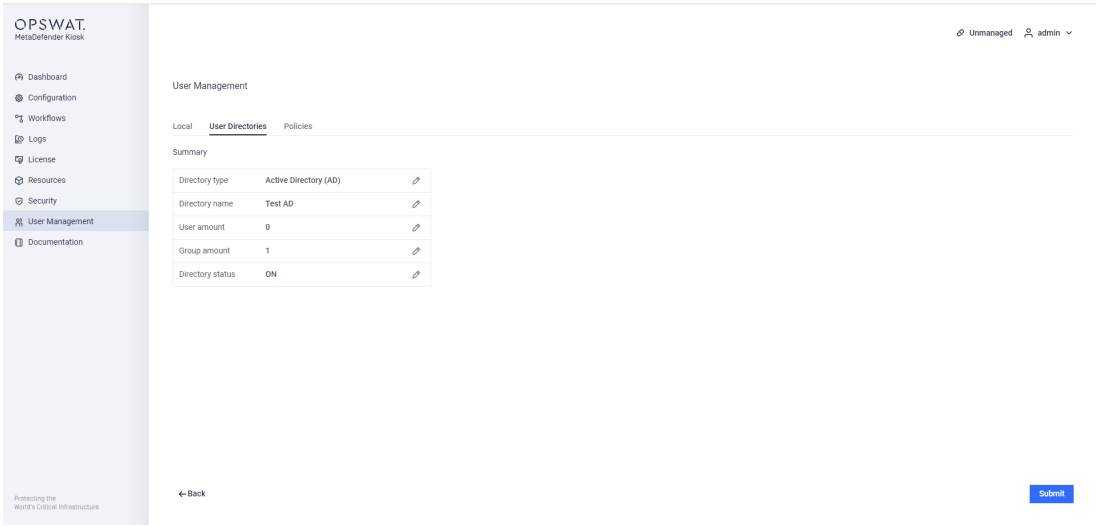
- **User Directories** manage Active Directory (AD) integration or Single Sign-On (SSO)
- **Local** manage the local users of the Management Console
- **Policies** manage remote login permission to the Management Console

> **Info**
> The user configurations in **Login Settings** only affect access to the management console. **Login Settings** does not affect who can log into the KIOSK UI itself.

User Directories



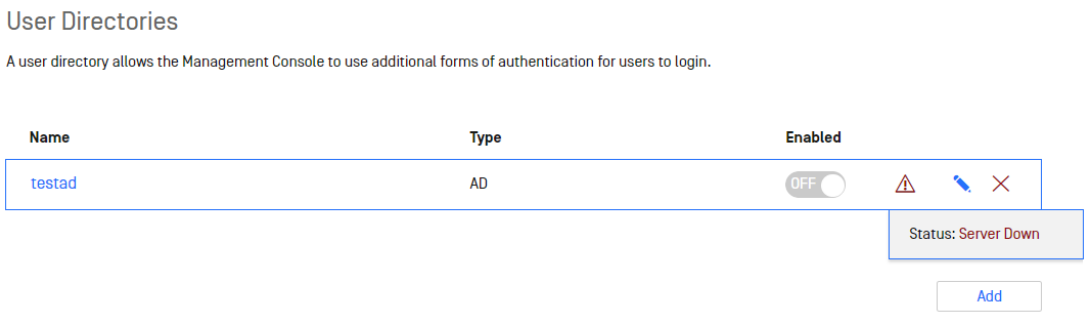




The **User Directories** section is used to create and configure User Directories for the management console. Clicking the **Add** button will open a wizard to create a new User Directory:

- How to configure an AD User Directory (section 3.1.2)
- How to setup an SSO User Directory to connect to an Identity Provider that supports SAML 2.0 (section 3.1.3)

When enabling an AD user directory, a quick connection check is performed. If a connection is not established, an error indictor will appear. The user directory will remain disabled until the connection is restored.

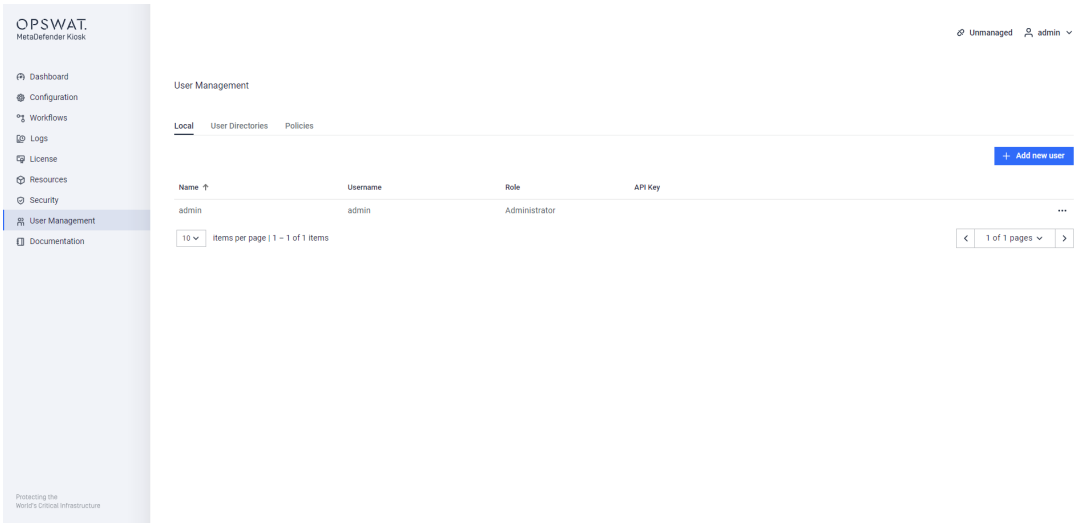


Local Users

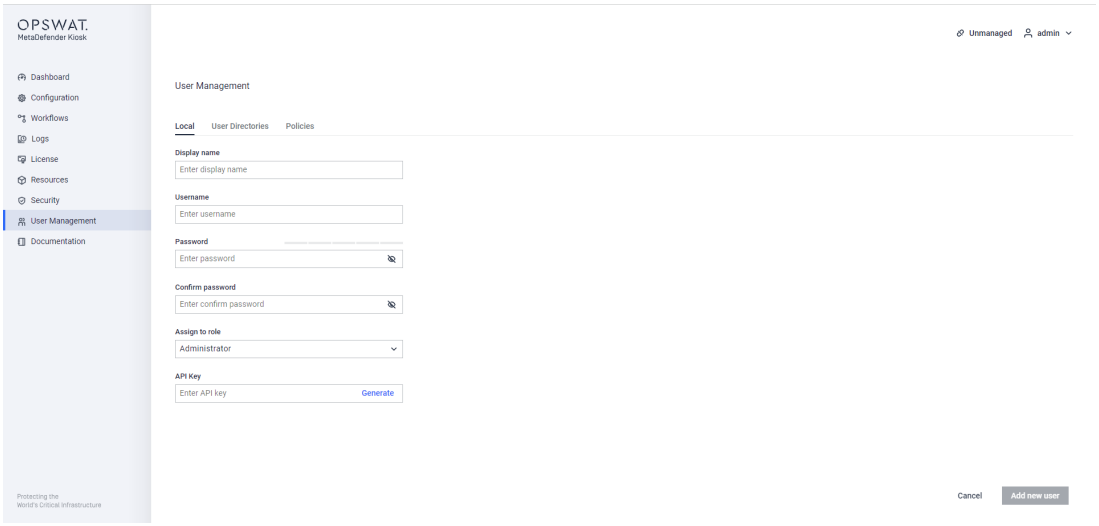
Users are local to the Management Console and are separated from the users assigned to Kiosk workflows. Local users can be created from any user with an Administrator role. For a user that is logged in from a user directory, they cannot edit or delete any local user.

Creating a new user

Step 1. Click **Add new user**



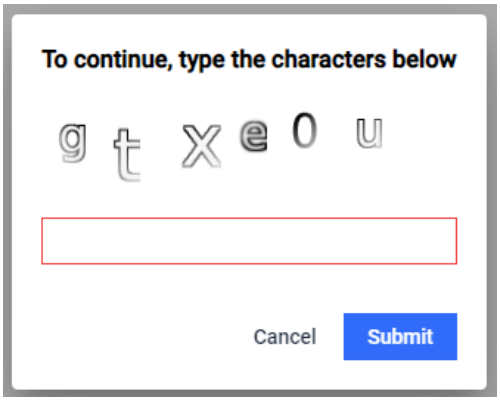
Step 2. Input the user information



- **Display name:** user name used in any logs, such as which user logged in to the WebMC
- **Account name:** user name used to log in to the WebMC
- **Password**: used for logging into the WebMC
- **Assign to role**: the created user could be Administrator or Auditor role
- **API Key**: used for integrations to other products such as Central Management, click *Generate* to fill in the box

Step 3. Type the characters of captcha

To prevent automation of the user creation process, a captcha will be displayed for administrators to confirm and continue. The random sequence of 6 characters and numbers expires after 1 minute. If input does not match what is displayed, a new sequence is generated again.

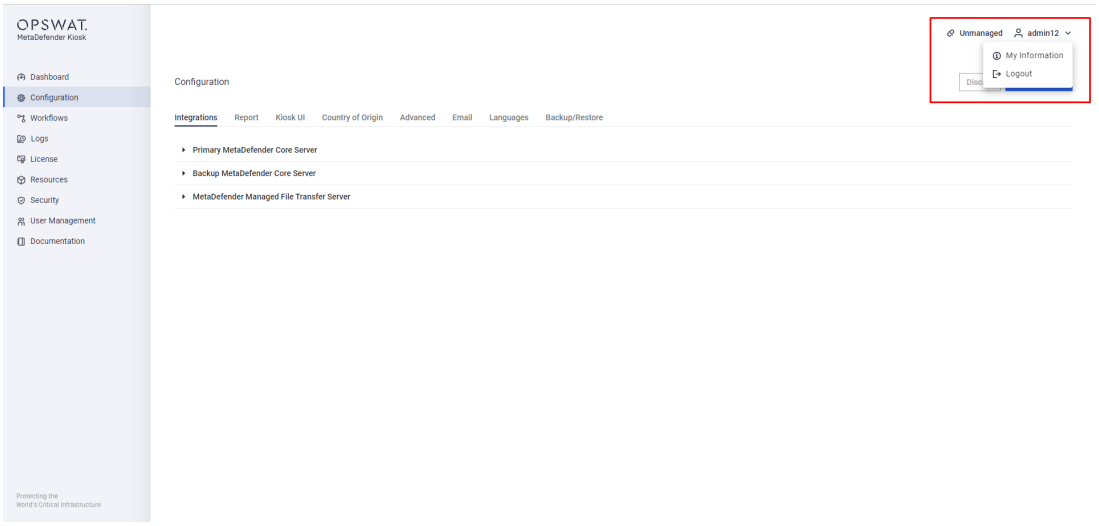


Once a user is created, it is requested to change its password at the first attempt to log in to the mgmt console. A maximum of 50 users can be created. Local administrators can add/modify/delete any user and change their own respective password. Local auditors can only change their own password, they cannot view any other users.

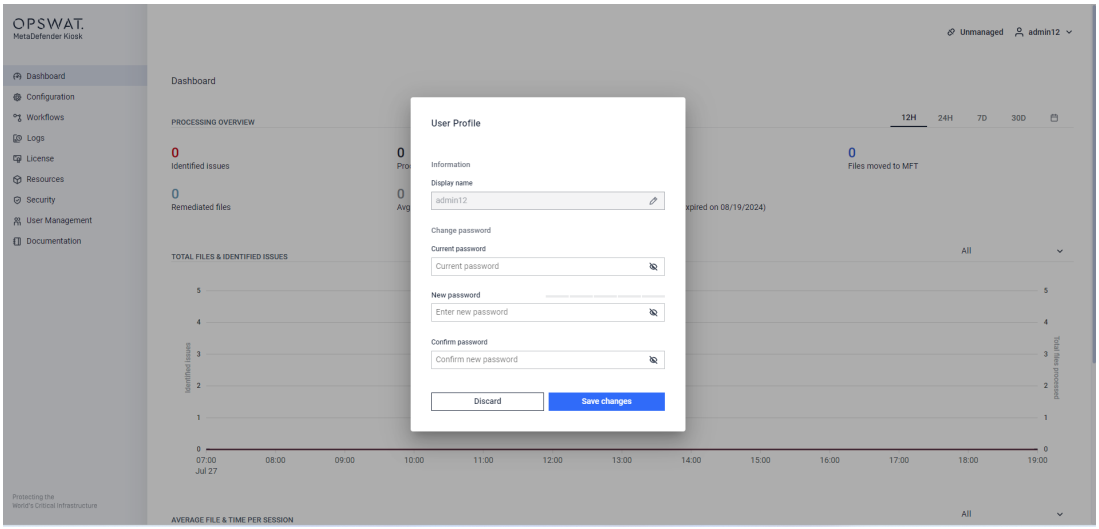
Note: Account name is case-insensitive from 4.4.12 release. Case-sensitive account names from backward are upgraded and kept unchanged.

Change the current password

Step 1. Navigate to the top right drop down > **My infomation**

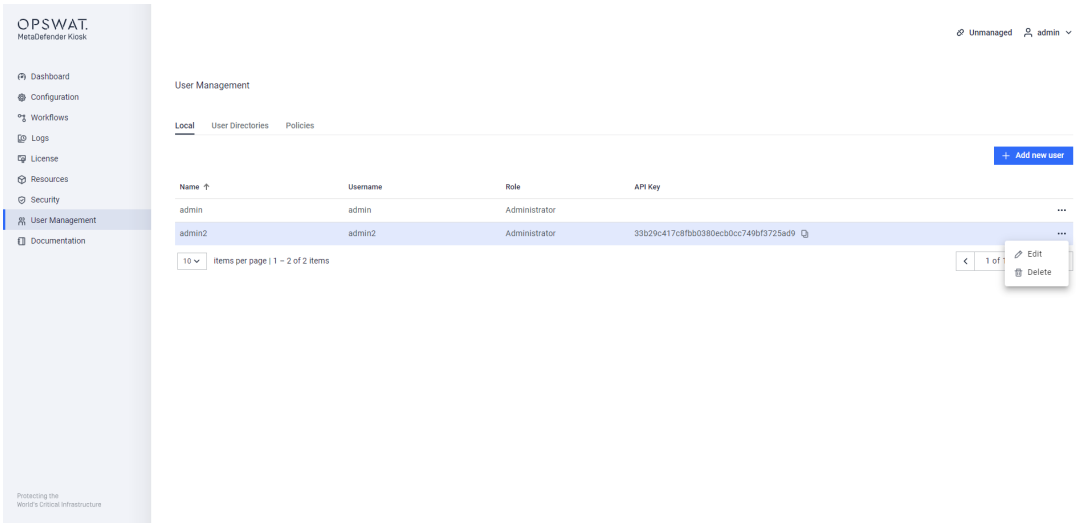


Step 2. Enter your curent password and new one. You can also edit your display name.



Step 3. **Save changes** and you will be required to log in again with a new password.

Manage the current users



The administrative users are authorized to oversee the following user management tasks:

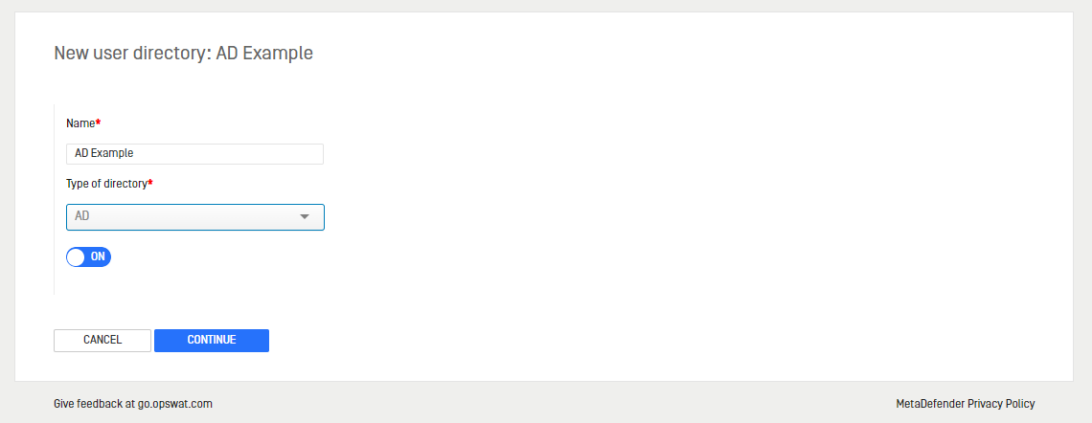
- Modify display names
- Manage user roles
- Update the API Key
- Delete any user except themselves

Active Directory

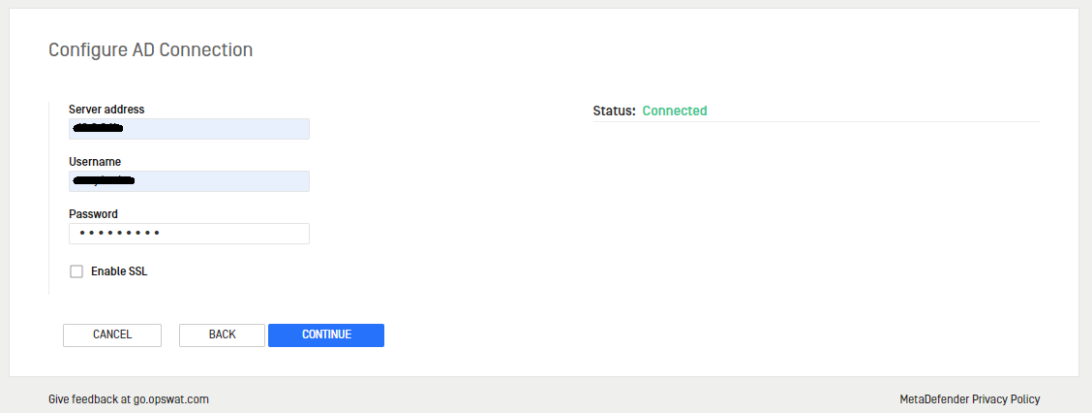
Active Directory login format
Once configured, Kiosk (version 4.7.4 or newer) supports AD login with following format:

- Username
- Domain\Username
- Username@Domain

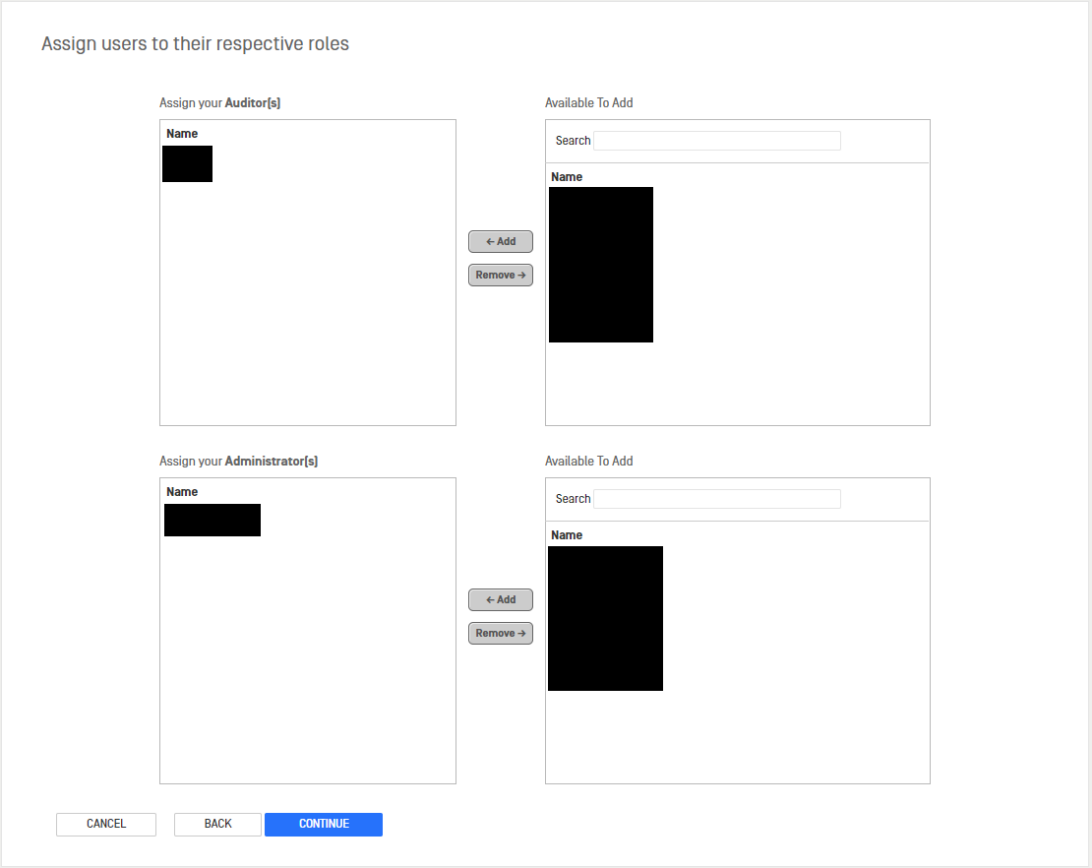
Select **AD** in the **Type of directory** dropdown to configure a User Directory for Active Directory users. Give your User Directory a name and use the toggle button to enable or disable this directory. Click **CONTINUE** to go to the next page.



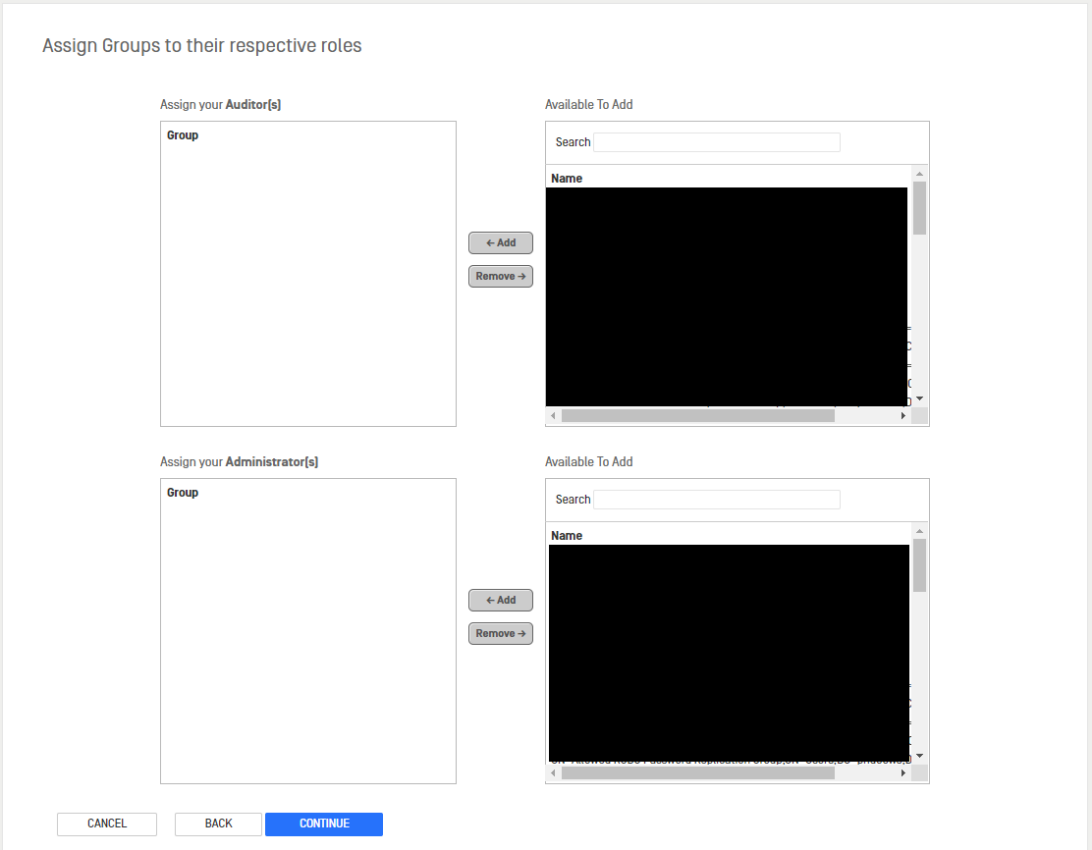
The next page is where the AD connection is configured. After the credentials are entered, the status of the connection is shown on the right. The **CONTINUE** button will be disabled until a valid connection can be made and the status shows “Connected” as shown below:



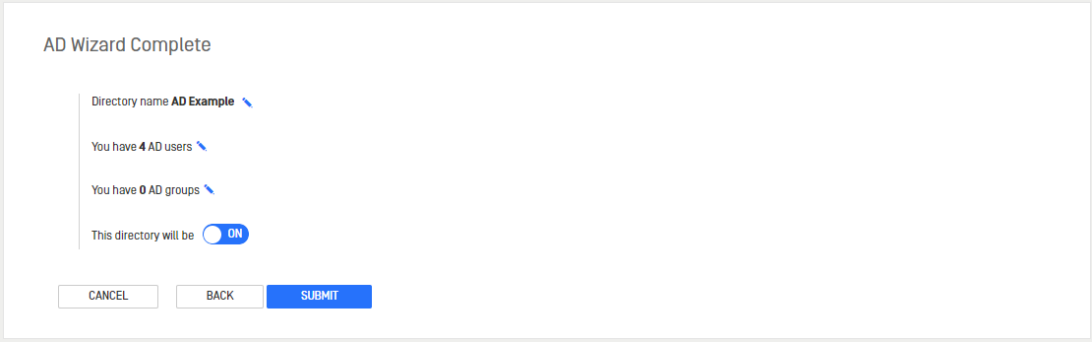
The next page allows you to assign users to either the Administrator or Auditor role.



The next page allows configuration of groups to the different roles



The final page shows a summary of the User Directory configuration and gives the option to edit before saving. Use the **SUBMIT** button to save the User Directory.



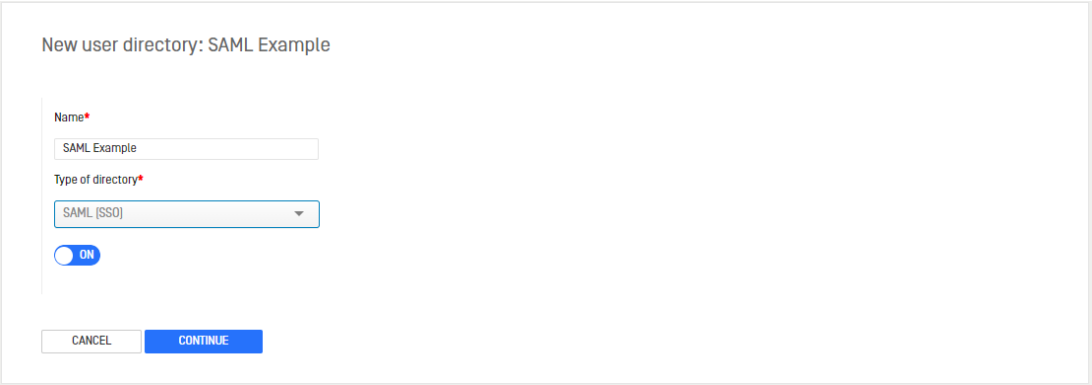
SAML 2.0

Kiosk supports Okta and ADFS as the SSO Identity Provider. See Configuring ADFS as SAML Identity Provider for more detail about configuring ADFS.

The following example will use Okta as the SSO Identity Provider

> **Info**
> Multiple SAML User Directories can be configured but only one can be enabled at a given time.

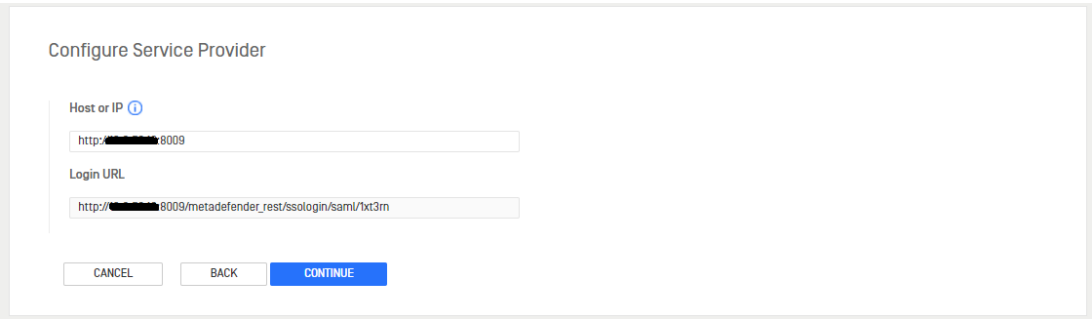
Select **SAML (SSO)** in the menu to create a **User Directory** that integrates with a SAML 2.0 SSO Identity Provider (IdP). Switch the toggle button to **ON** to enable this User Directory. As soon as it is submitted, any other User Directories configured with SAML (SSO) will be automatically disabled. Switching to **OFF** only creates the User Directory and will not change any currently enabled User Directories.



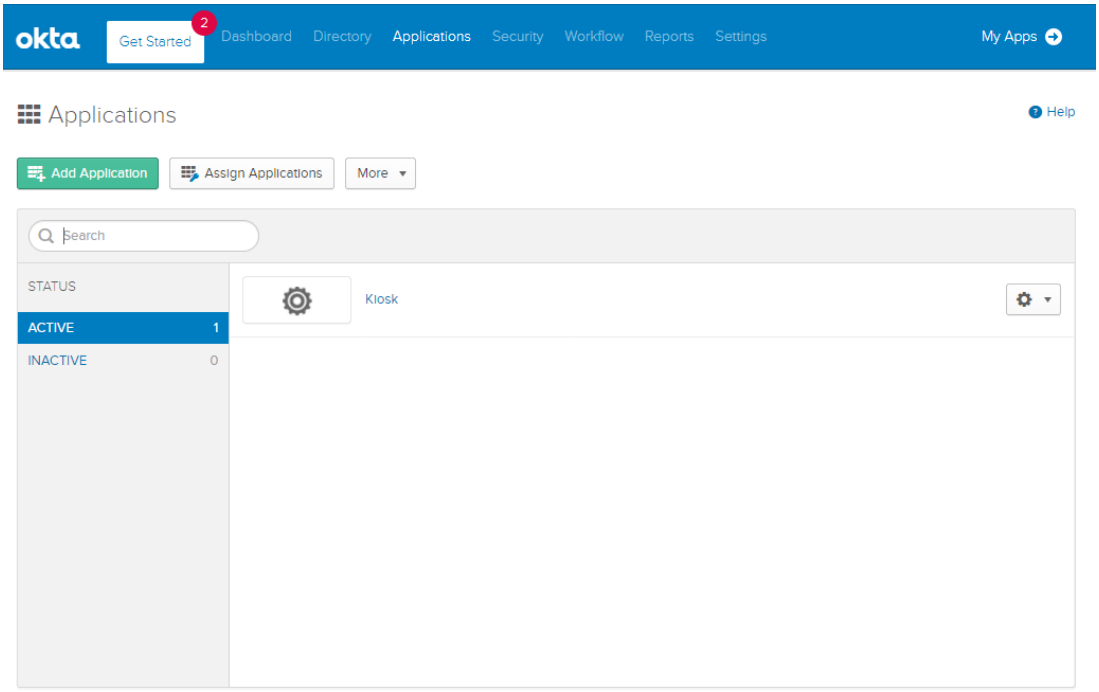
Click **CONTINUE** to go to the **Configure Service Provider** page. This will set up the login URL the Identity Provider uses to redirect after a successful login. Fill in **Host or IP** to generate the **Login URL**.

> **Info**
> Make sure to enter a URL in **Host or IP** that can be accessed by all of the users that will log in through SSO.

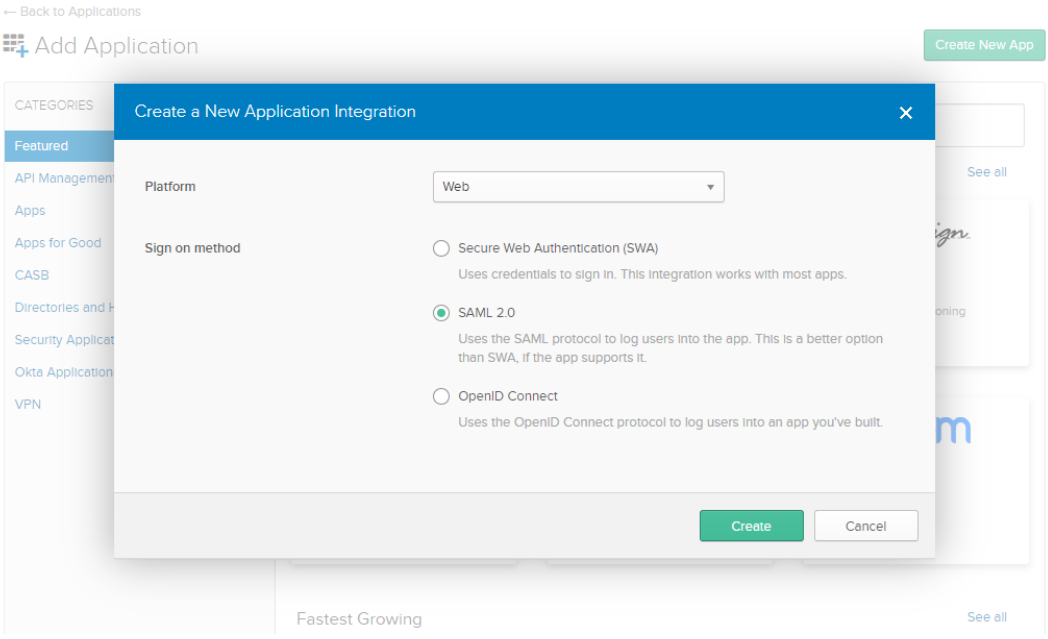
Use the value in **Login URL** when setting up the application in your Identity Provider



Keep this tab open in your browser then open up your IdP admin page to the section where Applications are added. In Okta, it looks like the following:

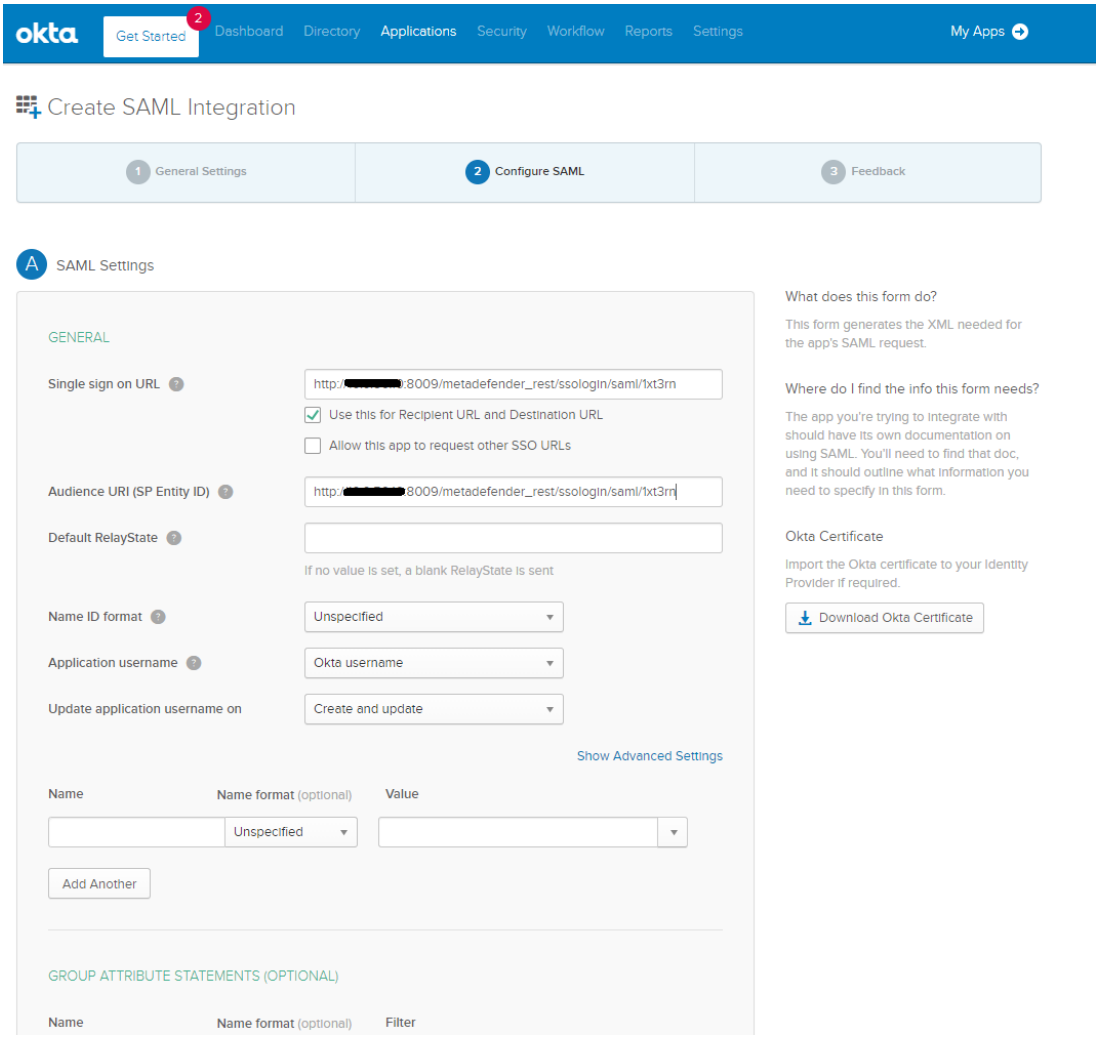


Select the option to add an application and then choose to create a new application that uses SAML 2.0. The way to create a new SAML 2.0 application will vary between Identity Providers. Refer to the documentation for your IdP for more details. In Okta, it looks like the following:

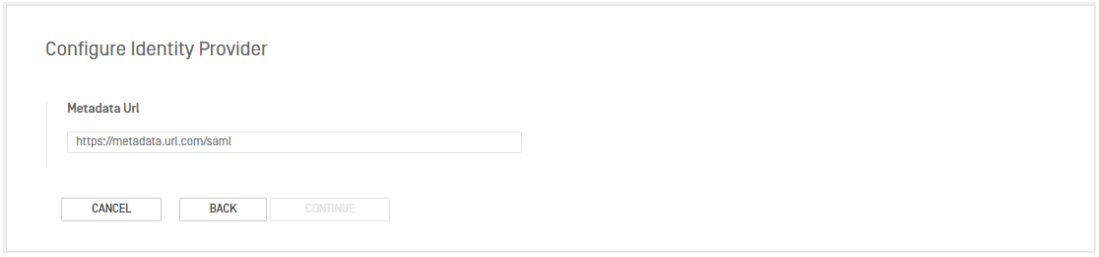


Continue until the step where the Identity Provider will ask for the Single Sign-on or Login URL. Switch back to your tab with the Kiosk User Directory setup. Copy and paste the **Login URL** from Kiosk into the Identity Provider application setup and finish the setup.

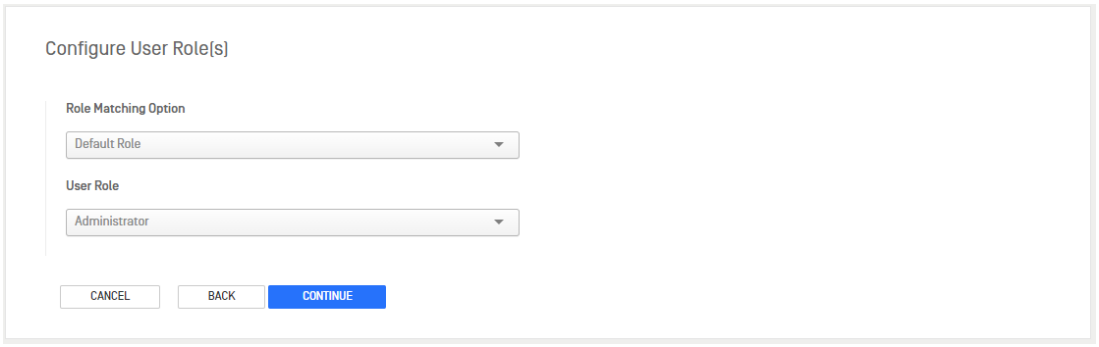
There may be multiple places where you will need to enter this login URL. In Okta you will need to enter it in the **Single sign on URL** section and the **Audience URI (SP Entity ID)** section. Refer to your Identity Provider documentation for information.



You should now have access to the Identity Provider metadata URL for your newly setup application. Go back to Kiosk and click **CONTINUE** to go to **Configure Identity Provider**. Copy and paste the metadata URL into the **Metadata URL** section.



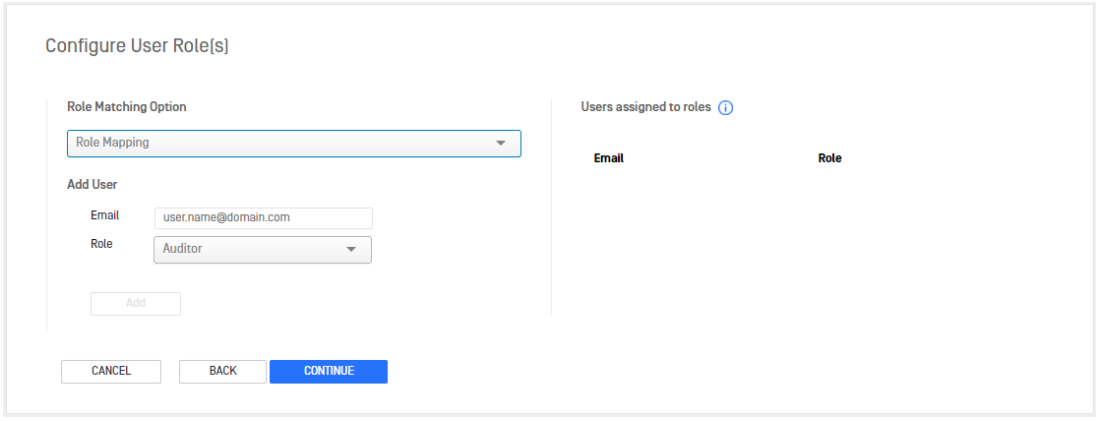
Click **CONTINUE** to go to **Configure User Role(s)**. Here you will configure the role users will get when they log in using SSO.



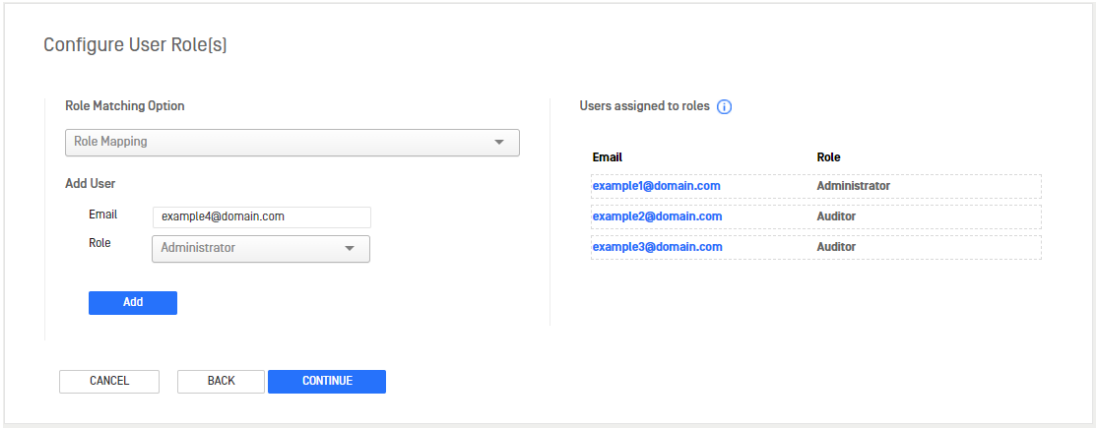
Role Matching Option allows you to choose between:

- **Default Role**: assign one user role to anyone that successfully signs in through SSO
- **Role Mapping:** assign specific users to specific roles

Select **Role Mapping** to show the list of assigned users.

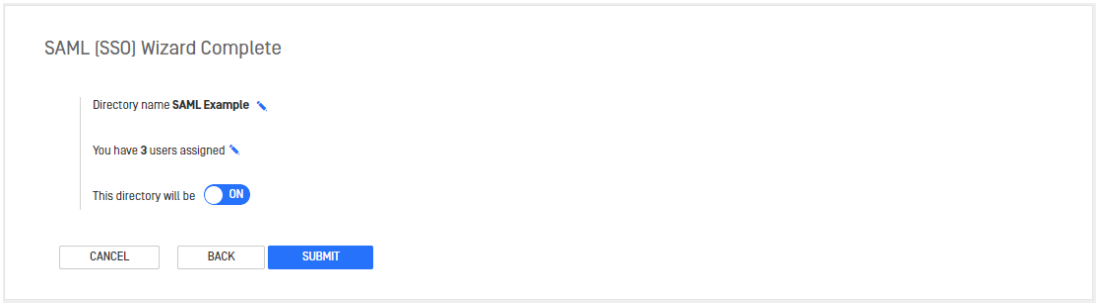


Fill in the email address or user name in the **Add User** section and use the dropdown to select a role. Click **Add** to add the user to **Users assigned to roles.**



Click **CONTINUE** to go to **SAML (SSO) Wizard Complete** and review the User Directory configuration. Use the **BACK** button to go back and make any changes if needed.

Click **SUBMIT** to create the User Directory. If the toggle is set to **ON**, SSO will now be enabled for any users attempting to log in to the Management Console.



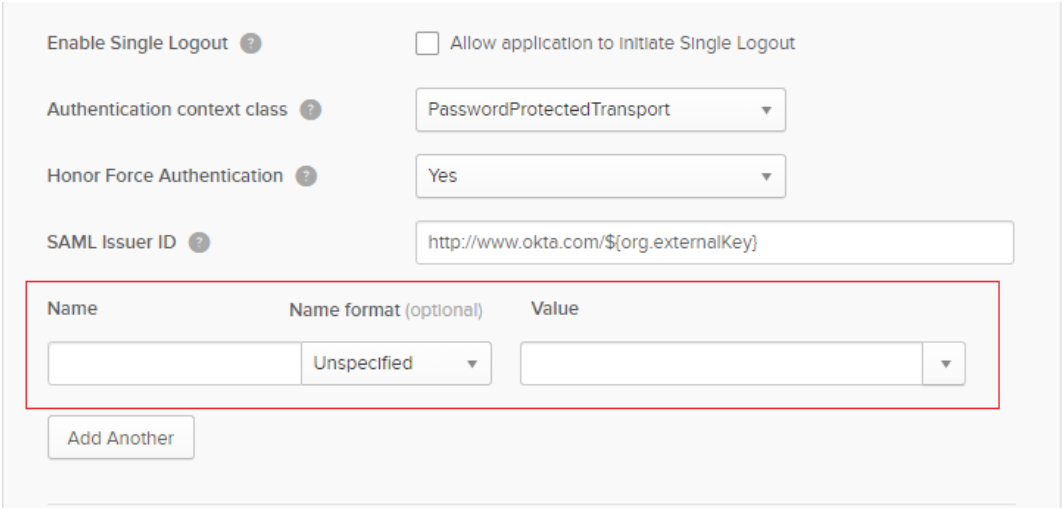
SAML Validation Logging

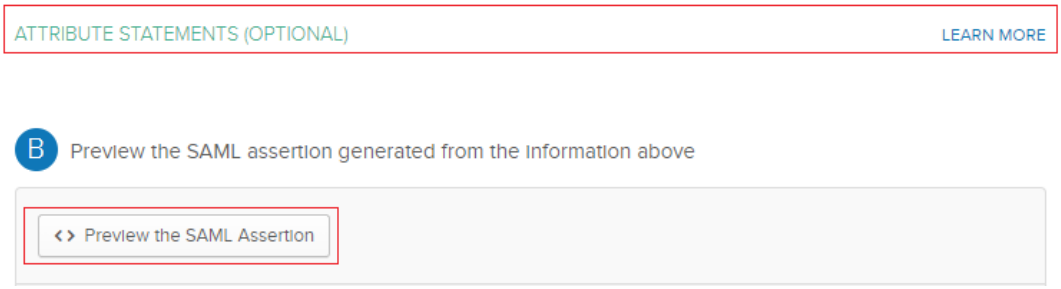
SAML authentication logging exists in the Kiosk logging directory (<kiosk install dir>\Log) within omdauth.log. There may be some verbose logging such as: "*Failed to compare notAfter timestamp to required regex notAfter=*". This is not a critical error and should not have an affect on the basic usage of SSO login for the Management Console. It does indicate that the *SessionNotOnOrAfter* attribute is not being provided by the IdP.

| SessionNotOnOrAfter [Optional] \nSpecifies a time instant at which the session between the principal identified by the subject (Kiosk) and the SAML authority (IdP) issuing this statement MUST be considered ended. |

If it is desired to use this attribute, please refer to your Identity Provider documentation to either enable the attribute or add it as a custom attribute.

Per the Okta example, it can be added as a custom attribute in **SAML Settings** -> **General** -> **Show Advanced Settings:**





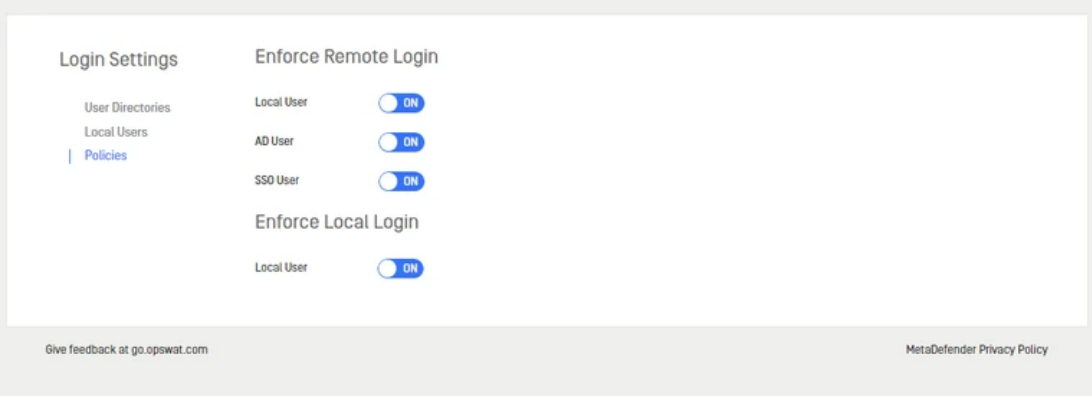
Then preview the SAML Assertion to ensure it is correct:

```
<saml:AuthnStatement SessionIndex="WDE5aBYjNEj_9IjCFiK0E1YelZT"
SessionNotOnOrAfter="2013-10-10T02:36:35.043Z" AuthnInstant="2013-10-
09T16:36:35.023Z">
  <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</
saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>
```

Policies

By default, all users are allowed to log in remotely or locally to the management console.



Enforce remote login

This controls the policy for allowing users to log in to the management console from a remote system. Administrators can disallow only remote login by turning off the policy.

Enforce local login

This controls the policy for allowing users to log in locally to the management console. Administrators can disallow only local login by turning off the policy.

> **Warning**
> To disable `Local user` in both **Enforce Remote Login** and **Enforce Local Login**, the prerequisite is that at least one user directory is enabled and has an admin user/group.

Resources

The Resources section in the Management Console interface contains different links to other OPSWAT solutions that can be used to compliment the usage of the Kiosk.

OPSWAT Media Validation Agent - Download the .msi to install the agent on any endpoint.

OMVA Tool - Downloads the companion .exe to configure the admin password and various other settings for the OPSWAT Media Validation Agent.

Central Management - Link to `My OPSWAT` to download the latest Central Management releases.

MetaDefender Core - Link to `My OPSWAT` to download the latest Core releases.

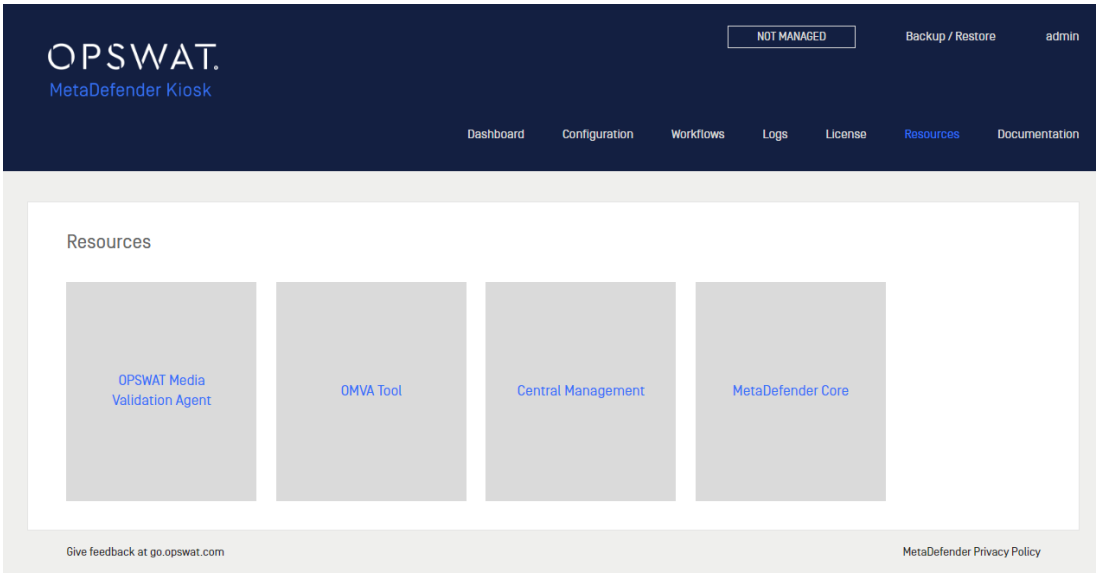
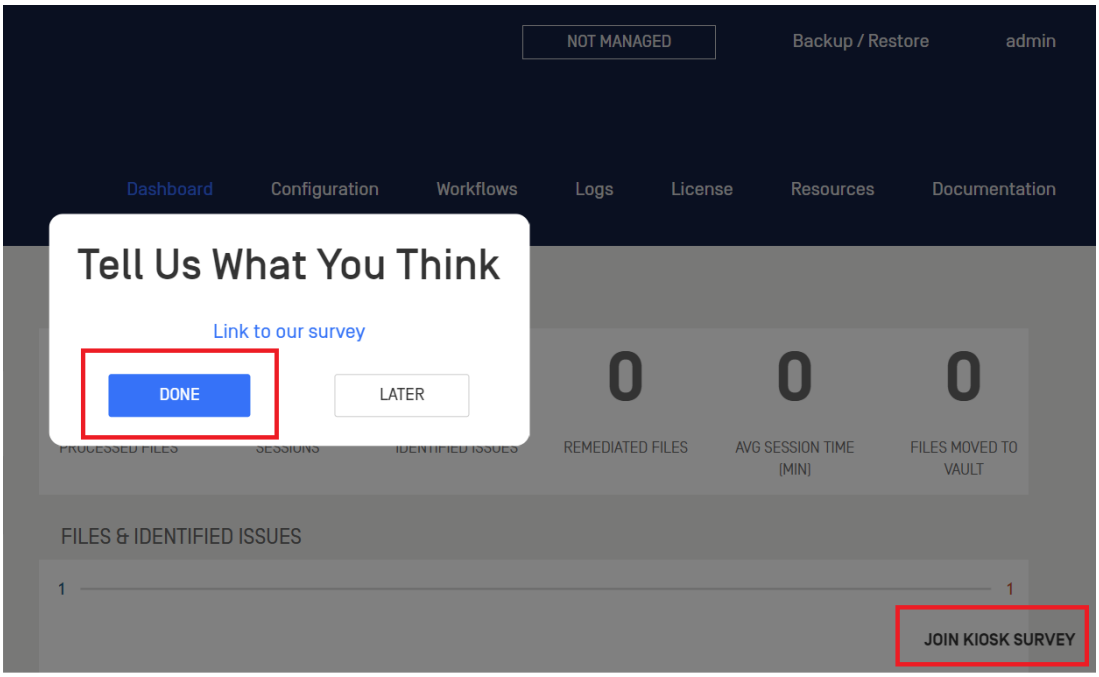


Image: OPSWAT Media Validation Agent option on MetaDefender Kiosk Management Console.

Kiosk Survey

As part of product improvement and development, OPSWAT recommends administrators of Kiosk to do a Net Promoter Score (NPS) survey. The survey is performed via an internet-connected Management Console and repeated yearly.



A popup with the survey link appears after an administrator successfully logs in. Once clicking on the link, the admin is navigated to a new tab for the survey. After completing the survey, the admin should click on **DONE** to prevent Kiosk to prompt for the survey again. The survey will be requested for again in another year.

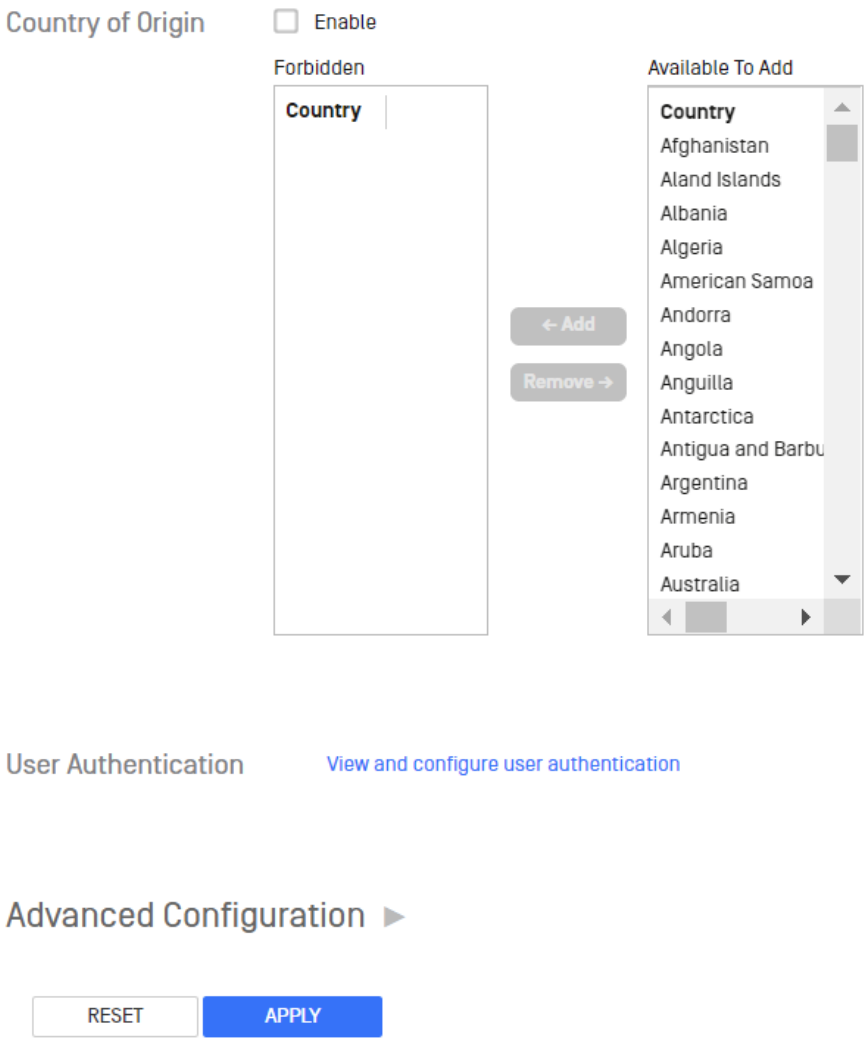
The admin can ignore the survey link by clicking on **LATER**. Once an admin is ready to participate in the survey, clicking on the right bottom floater “JOIN KIOSK SURVEY“ will bring up the survey prompt again.

Country of Origin

Kiosk is able to detect source country where files are created from. The Country of Origin (COO) feature helps the Kiosk admin add more restrictions on the scanning result by specifying countries, which the publisher resides in, as forbidden. Files published from forbidden countries are considered as blocked, even they are clean from Metadefender Core scan result. Kiosk keeps scan result from Metadefender Core if no COO associates with the files.

Due to performance priority, only executable files (.exe, .dll) are supported for COO detection. Files reported by Metadefender Core as blocked is not processed with COO.

To support COO, the admin needs to enable COO and add countries to the forbidden list. Empty forbidden list equals to COO disabling.

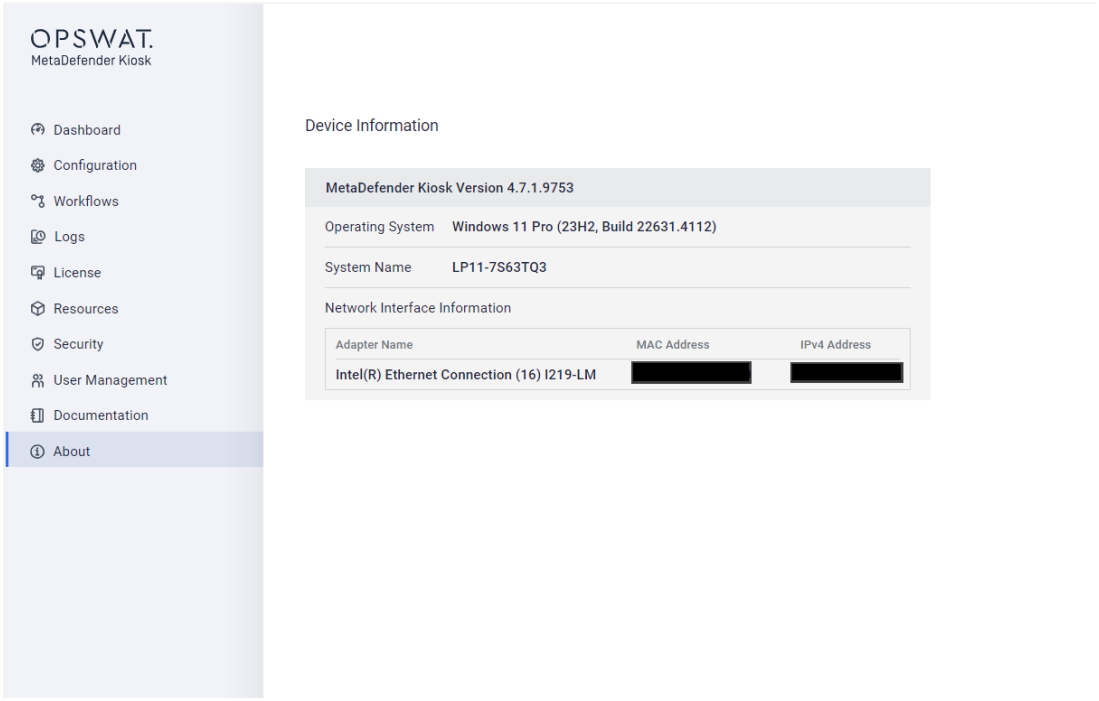


Notes: Kiosk bases on internal database to identify COO of files. Files from companies not existing in the internal database might result as no COO.

About page

The About page will display the following device information:

- **Operating system**: Details the specific version of Windows installed on the KIOSK device.
- **System Name**: The computer name designated for the KIOSK device.
- **Network configuration**: Exhibits all active network adapters on the device, including the Adapter name, MAC Address, and IPv4 Address.



About page

Kiosk Workflows

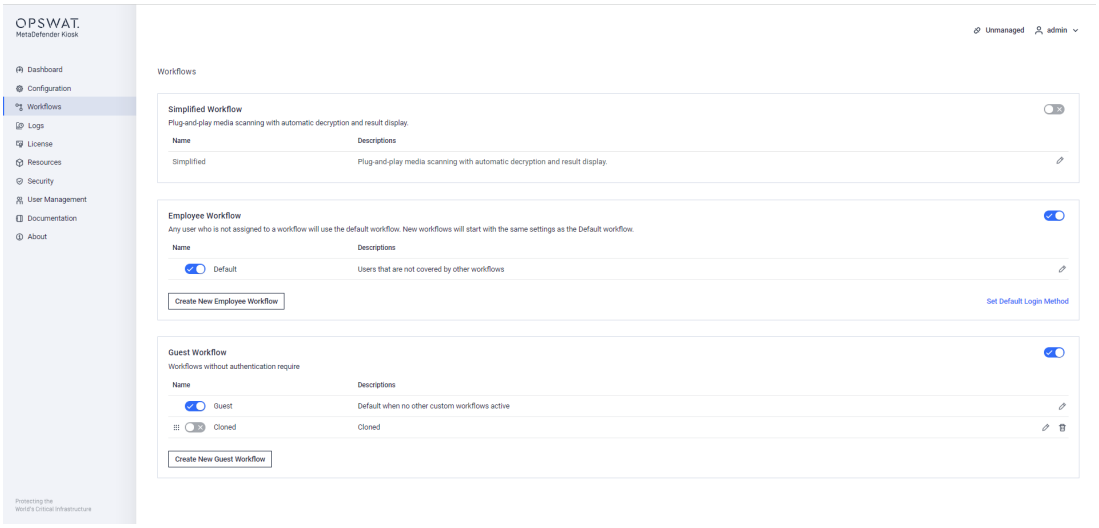
MetaDefender Kiosk lets you assign different Kiosk options to different groups of users, called workflows. You can create new workflows and edit any default ones. The Workflows Page page contains all workflows in MetaDefender Kiosk.

For each workflow, you can do the following:

- Properties & Membership
- Managing User Questions
- Allowed Media Types
- Selecting a Server to Process Files
- Selecting How to Handle Processed Files
- Custom Command Line Script
- Managing Printing Options
- Managing Logging Options
- Email Session Report
- Retrieve Files

Workflows Page

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.



Workflows

There are 3 workflow groups: Simplified, Employee and Guest group. Workflows in the Employee group requires 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.

Note: Workflows labeled with an "!" do not match with any existing Core workflow rules. You must select a corresponding MetaDefender Core in the 4.5. Selecting a Server to Process Files section.

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.

Selfscan always uses the default workflow of Employee group in regardless of the group or the workflow is enabled/disabled.

Default workflows

Name	Description
Simplified	Plug-and-play media scanning with automatic decryption and result display
Default	Users that are not covered by other workflows
Guest	Default when no other custom workflows active

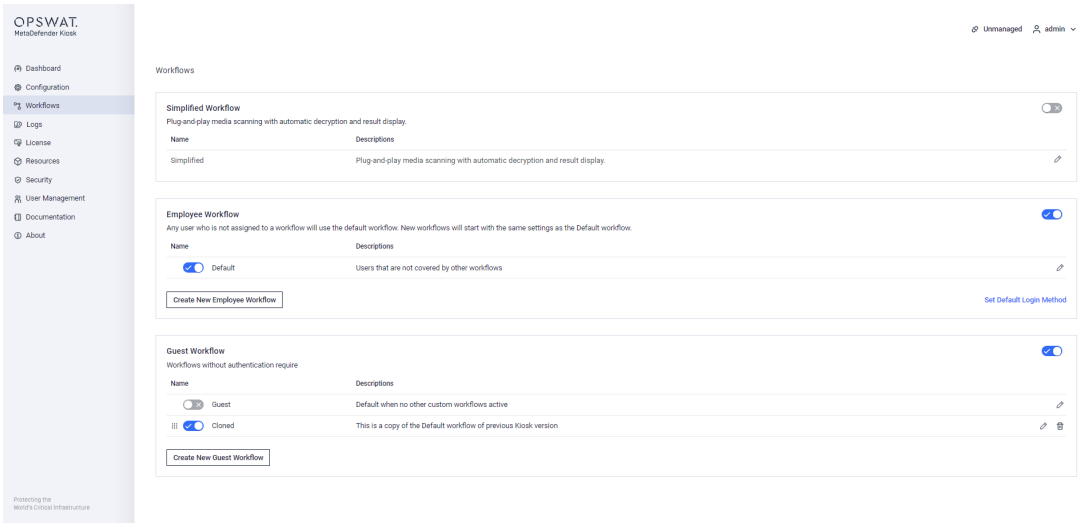
Creating a new workflow

To create a new workflow, click **Create New Employee/Guest Workflow**. You will be guided through the process of creating a new MetaDefender Kiosk Workflow. After the workflow has been created, each step in the workflow can be edited independently. A newly created workflow is always disabled by default.

Workflows after upgrade

Any workflows existing in the previous (prior to 4.5.6) version must be kept the same after the upgrade. The previous version's Default workflow must become Default in Employee group; The previous version's Guest workflow must become default Guest in Guest group.

In a very particular case where the Default workflow of the previous version is selected in non-authentication mode, then after the upgrade to 4.5.6 or higher, that Default workflow of the previous version is cloned as a custom workflow in Guest group, with new name "Cloned" and set as the only one enabled. This particular behavior would keep same behavior after the upgrade to 4.5.6.



Cloned workflow after upgrading from version less than 4.5.6

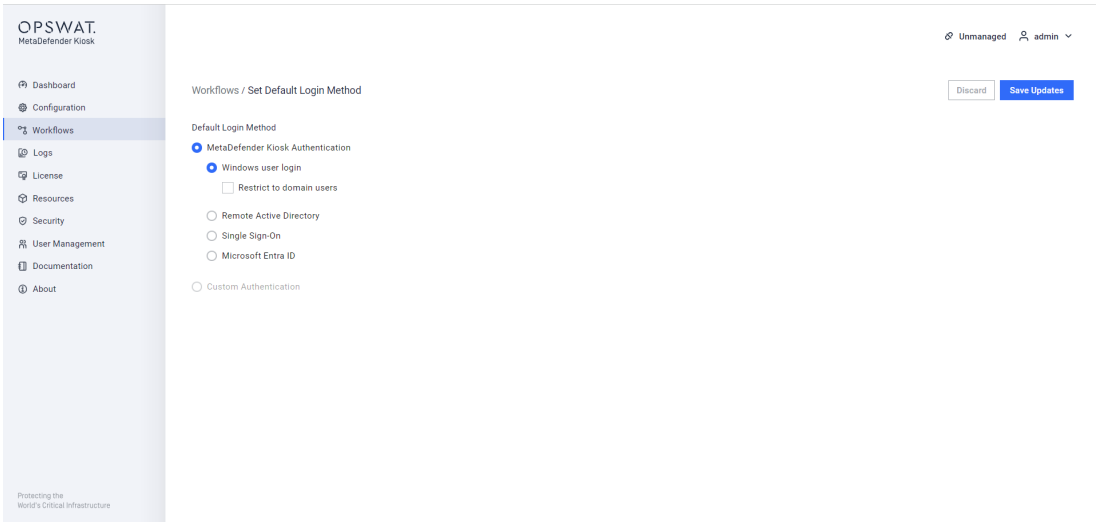
Select Default Login Method

> **Info**
> User Authentication Method
>
> As of Kiosk 4.5.6, User Authentication has been moved from the Configuration page to Workflows page as a User Authentication Method link.
>
> Since Kiosk 4.6.6, User Authentication Method has been renamed to Select Default Login Method

The Select Default Login Method link helps to configure and select default user authentication method.

Windows user login

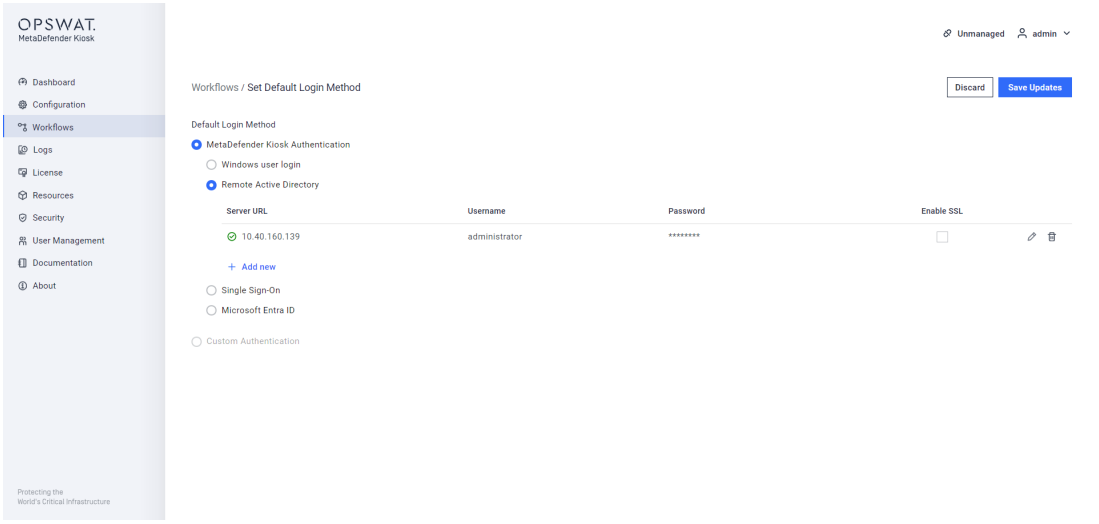
The Windows user login allows only local system users to log on Kiosk UI. The Kiosk administrator can choose whether to restrict the users by domain. If selected, only users on the same domain as the system are allowed to use MetaDefender Kiosk. If this is not selected, users will be able to enter authentication information for users on any domain as well as local system users.



Windows user login option

Remote Active Directory

The Remote Active Directory allows both local and AD users to do. The address of the remote Active Directory server, as well as user credentials to authenticate against the server are required. These credentials will be used to retrieve the list of users from the remote AD server for the purposes of assigning users to specific workflows.

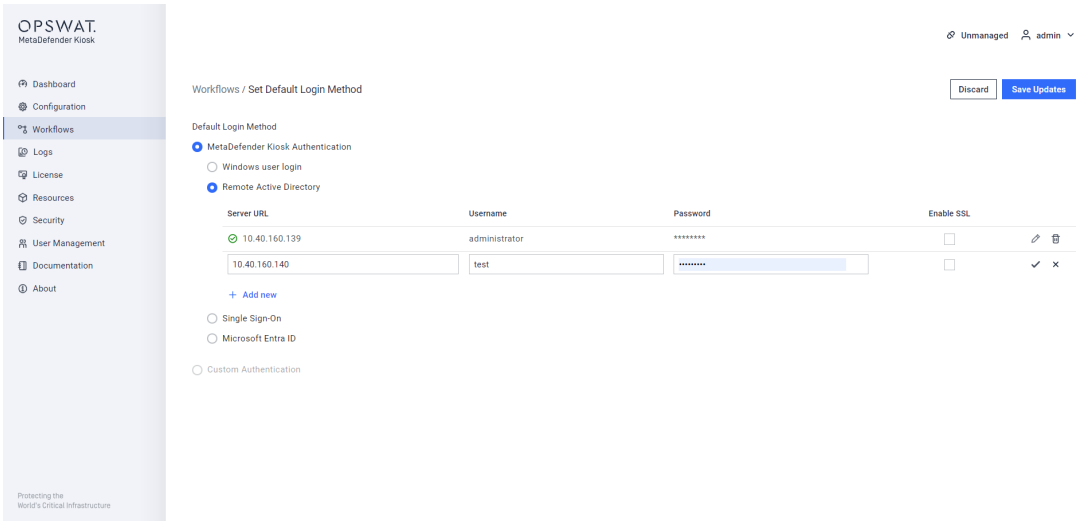


Add new Remote Active Directory

Multiple Active Directories can be configured. Click `Add new` to add a server to the list and "Delete server" on the right hand side to delete the specific entry. The "Status" indicator will show in real time whether Kiosk is able to connect to the AD server. For "Server address", input can either be the IP or DNS name of the AD server; "<ip or dns name>:<port>". The default port 389 (636 if SSL is enabled) will be used if one is not supplied.

> **Warning**
> With KIOSK configuration in My OPSWAT:
>
> - The port must be entered, even if it is the default one.
> - The username must include the domain

Once SSL enabled, the server address should be in FQDN (Full Qualified Domain Name) format, for example:

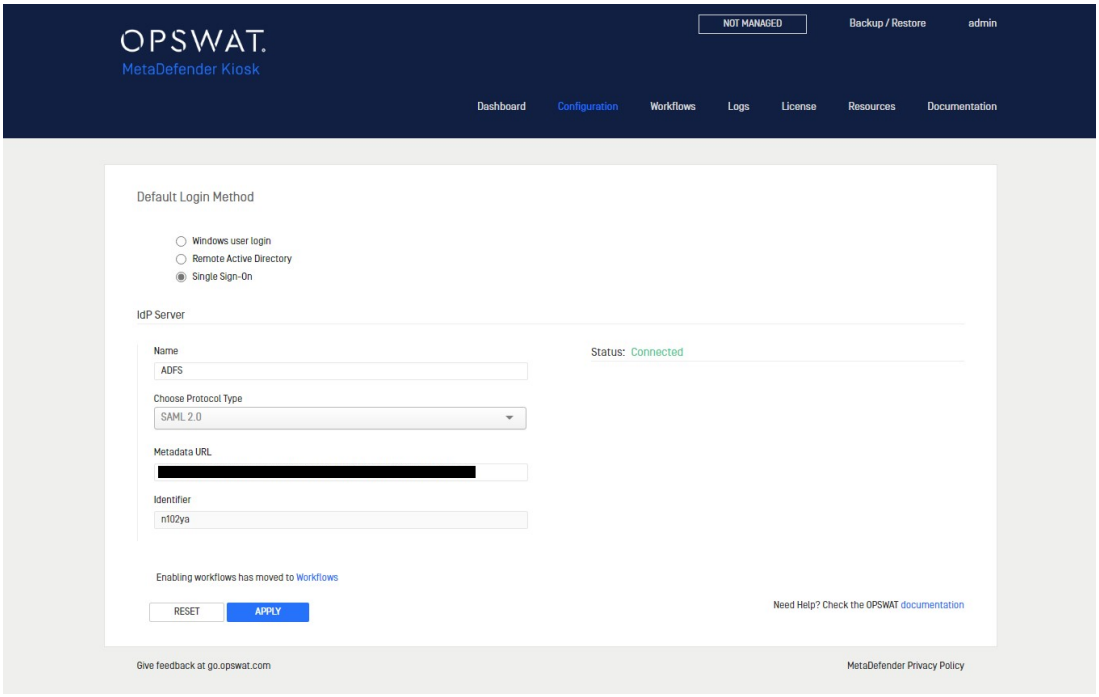


Adding second AD

Single Sign-On

The Single Sign-On allows users log in through a SAML IdP server which acts as the central authority for authenticating users and issuing security tokens.

- **Name:** Specify name of the IdP server
- **Choose Protocol Type:** SAML 2.0 is supported
- **Metadata URL**: used for fetching metadata of the IdP server
- **Identifier:** unique identifier generated by Kiosk that will be assigned to each **Relying Party Trust** (RPT)



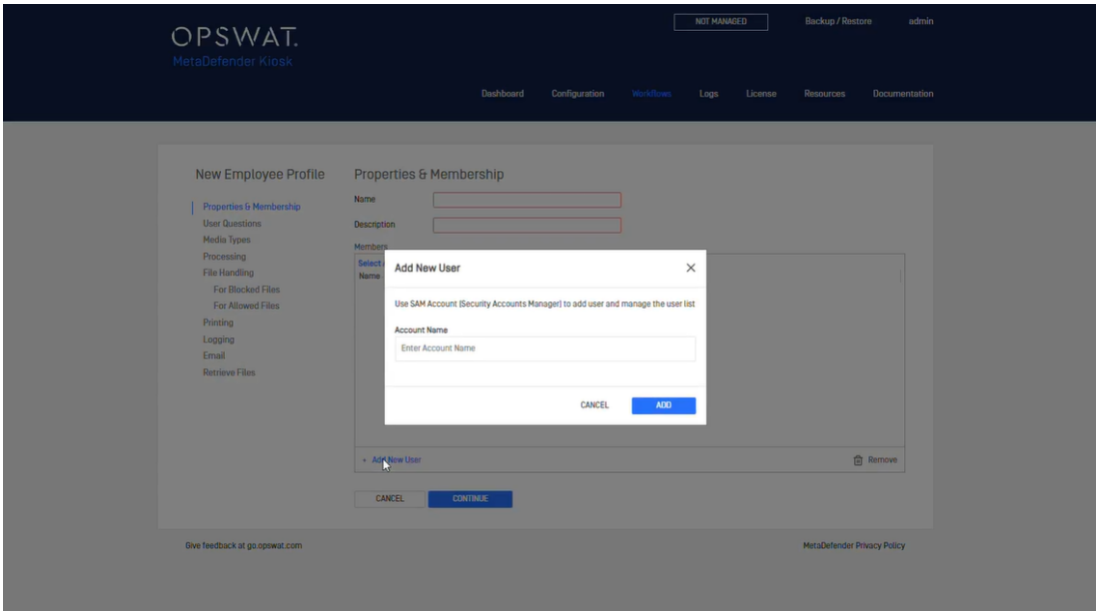
The Kiosk administrator must configure Kiosk as one **Relying Party Trust** on IdP server to complete the integration.

> **Info**
> Kiosk UI **Relying Party Trust** format:
>
> <http/https>://**localhost**:<port>/metadefender_rest/**uissologin**/saml/<identifier>
>
> Please modify the elements enclosed in <> to match your Kiosk's configuration. It must be **localhost** for Kiosk UI login

See Configuring ADFS as SAML Identity Provider for more detail to configure ADFS as SAML IdP.

The "Status" indicator will show in real time whether Kiosk is able to connect to the Idp server.

For the purposes of assigning SSO log in users to a specific workflow, the SAM (Security Accounts Manager) accounts of users need to be added manually to Properties & Membership of that workflow.



Custom Authentication

If User Authentication enabled, the Kiosk administrator can choose between using the default MetaDefender Kiosk authentication or using a custom authentication module that has been installed on that MetaDefender Kiosk. For more information, see 11.1. Custom Authentication Module.

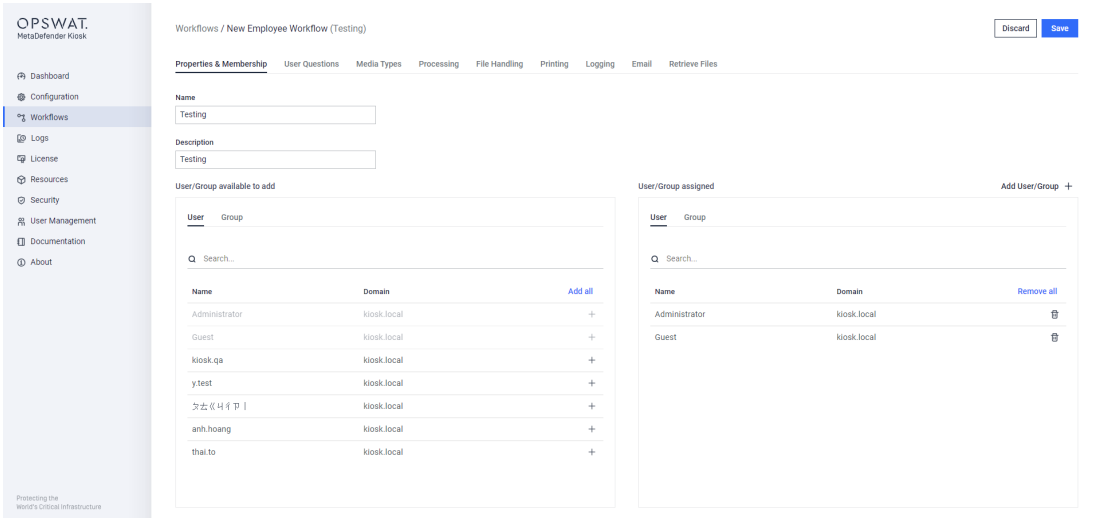
Properties & Membership

The Properties & Membership page lets you specify the name and description for a MetaDefender Kiosk workflow. It also lets you manage the users or groups assigned to that workflow. To be able to configure workflows with users, the Kiosk system must be part of the domain or be able to authenticate with a remote Active Directory. To be able to configure workflows with groups, the Kiosk system must be able to authenticate with a remote Active Directory.

Each user or group can be assigned to multiple workflows but only one workflow is selected for a session. See Logging In on the User Authentication Screen for more details

1. Assignment from available User/Group

When set up with AD authentication, if the KIOSK can successfully query users and groups, the `User/Group available to add` section will show users and groups from all configured ADs in their respective `User` and `Group` tabs.

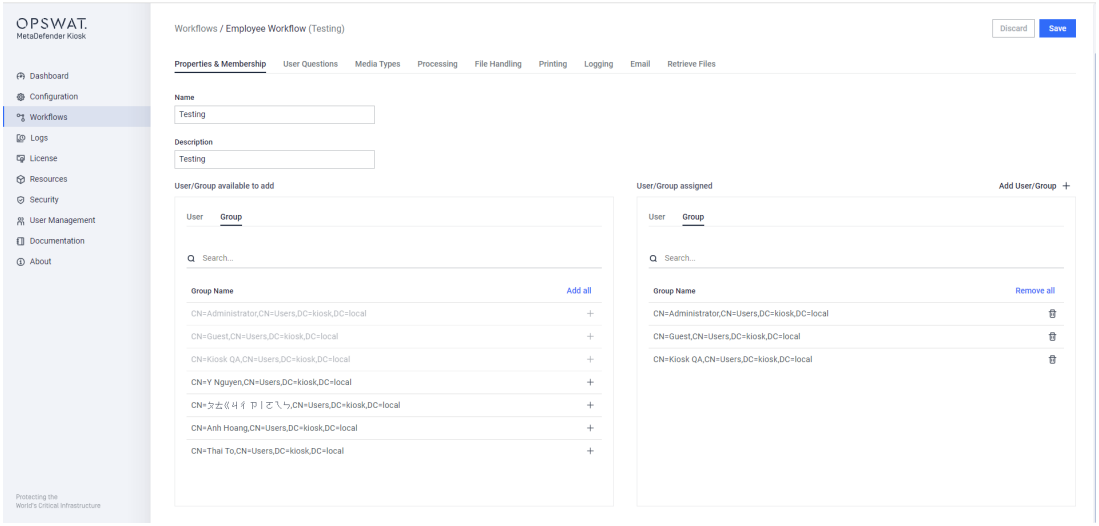


Properties & Membership configuration for user page

The admin can also specify a user/group in the search box, the search will narrow down the available data which contain the search pattern. Different from Visitor Management, manage the search accepts sAMAccountName (an attribute in AD server) to search through AD server.

Flow the following steps to assign users/groups to the workflow:

Step 1. Select user(s)/group(s) from the `User/Group available to add` section by clicking on (+) or `Add all` buttons on corresponding tab.



Properties & Membership configuration for group page

> **Info**
> To reduce the loading duration, only 500 users/groups are loaded for each tab.

Step 2. The chosen user(s)/group(s) will be grayed out in the `User/Group available to add` section and displayed in the `User/Group assigned` section for review and adjustment.

Step 3. Click on `Save` to finish.

2. Manually input User/Group assignment

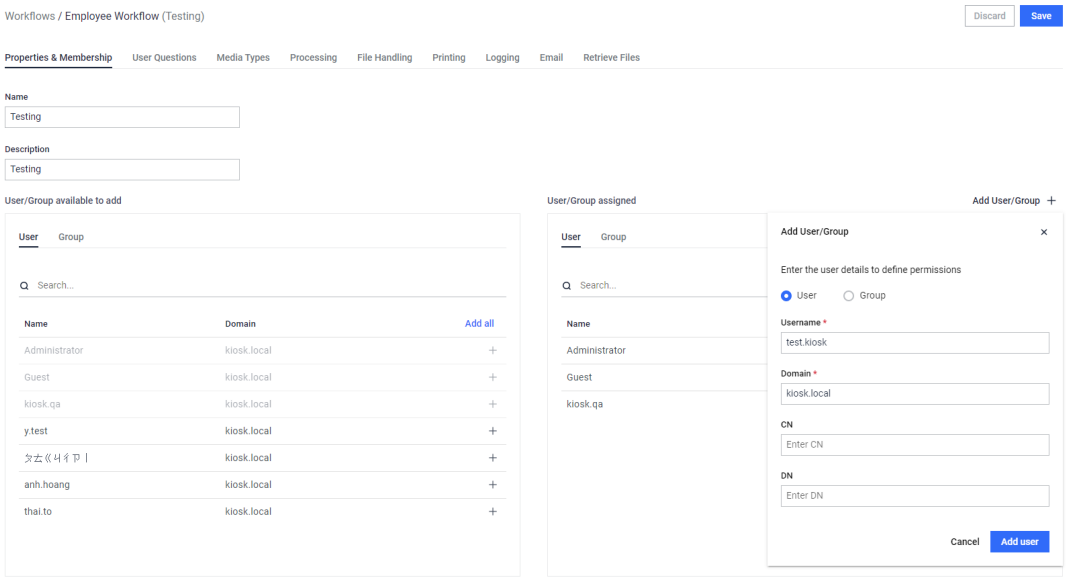
The KIOSK feature enables the manual addition of users or groups along with their identity information.

a. Manually input a user

Step 1. Click on `Add User/Group` button on the top right of `User/Group assigned` section

Step 2. On appeared window, check on `User` option.

Step 3. Enter the user identity information.



Manually input a user

In which:

- **Username** (required): sAMAccountName of the user
- **Domain** (required): Domain to which the user belongs
- **CN** (optional): Common name of the user
- **DN** (optional): Distinguished Name of the user

Step 4. Click on **Add user** button.

Step 5. The added user(s) will be displayed in the `User/Group assigned` section for review and adjustment.

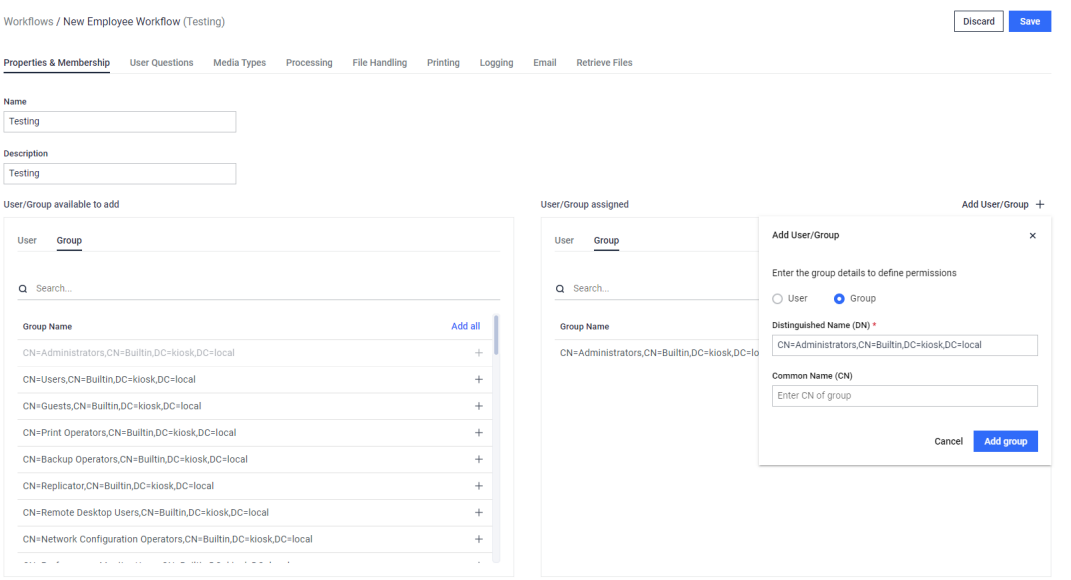
Step 6. Click on `Save` to finish.

b. Manually input a group

Step 1. Click on `Add User/Group` button on the top right of `User/Group assigned` section.

Step 2. On appeared window, check on `Group` option.

Step 3. Enter the group identity information.



Manually input a group

In which:

- **Distinguished Name** (required): the Distinguished Name (DN) of that group. For example: `CN=Administrators,CN=Builtin,DC=kiosk,DC=local`
- **Common name** (optional): the Common Name (CN) of that group.

> **Info**
> A **DN** is a sequence of relative distinguished names (RDN) connected by commas. See Distinguished Name for more details about syntax and example.

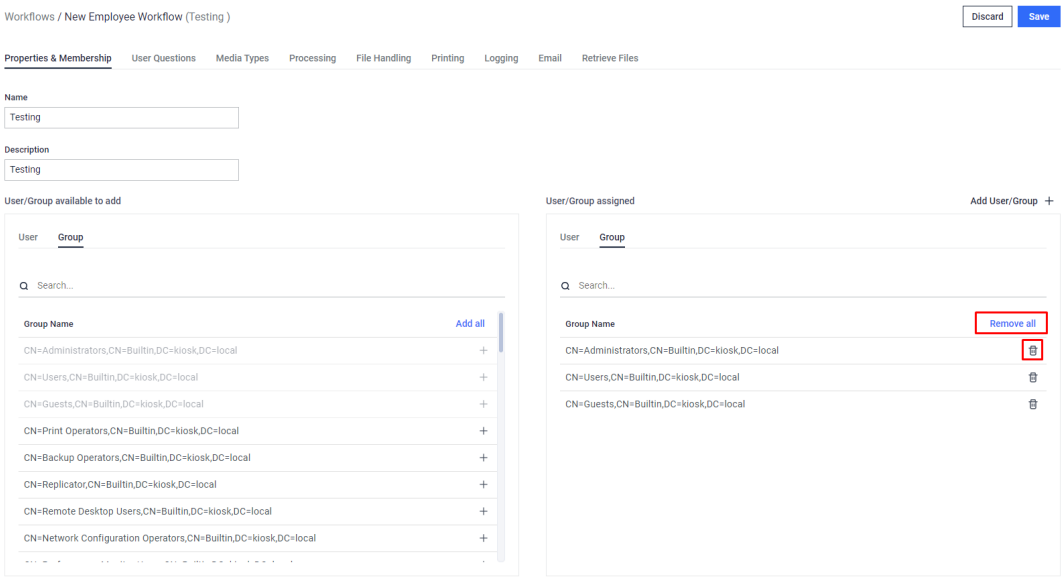
Step 4. Click on `Add group` button.

Step 5. The added group(s) will be displayed in the `User/Group assigned` section for review and adjustment.

Step 6. Click on `Save` to finish.

3. Remove users/groups from the assigned workflow

Step 1. Click on detele icon to delete specific users/groups on `User/Group assigned` section or `Remove all` button to remove all of added ones.



Remove an assigned group

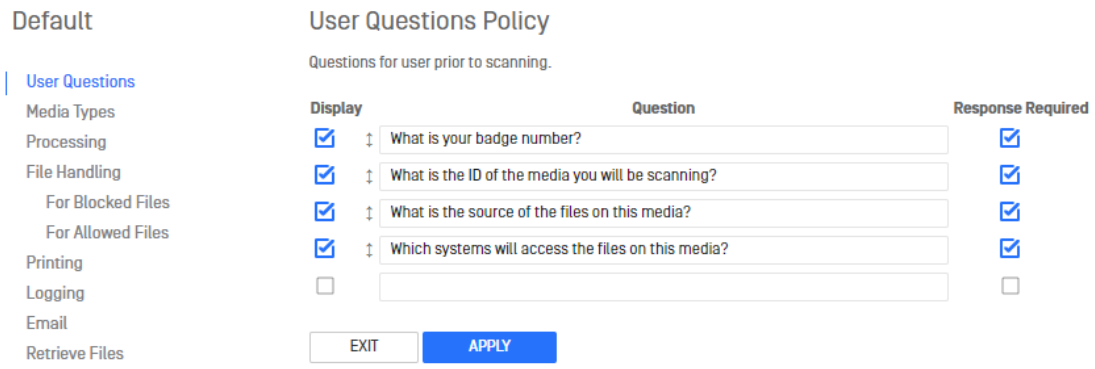
Step 2. Click **Save** to finish.

4. Important notes

- If there are connection issues with Active Directories, Kiosk might take longer to retrieve users and groups. The timeout for the user/group fetching from each AD is about 1 minute. The more ADs with connection issues, the longer the fetching is.
- When an AD is not available at some time, the user belonging to a workflow is not able to log in Kiosk UI, the admin can check the application log to trouble shoot any login failure in this case.
- When an user is removed from AD, the workflow is not synced up with that removal. The admin must remove that user from the workflow.

Managing User Questions

The User Questions Policy page lets you create questions for users to answer before processing files. You can require that these questions be answered before the user is allowed to continue. Any required responses are stored in the User Question section of the session log.



Allowed Media Types

This section configures which media types MetaDefender Kiosk can process for the selected workflow.

CD/DVD

Processing files from a disc is supported when selected.

Specific requirements exist when using discs to copy files to.

Floppy

Processing files from a floppy disk is supported when selected.

When enabled, a button to detect the floppy disk is displayed on the `Insert Media` screen.

The floppy disk must be inserted prior to clicking the button.

Phone

Processing files from Android and iPhone devices is supported when selected.

Scanning media content on an iPhone is supported by default.

iTunes can be additionally installed to ensure even deeper scanning, such access to system files, downloads, etc...

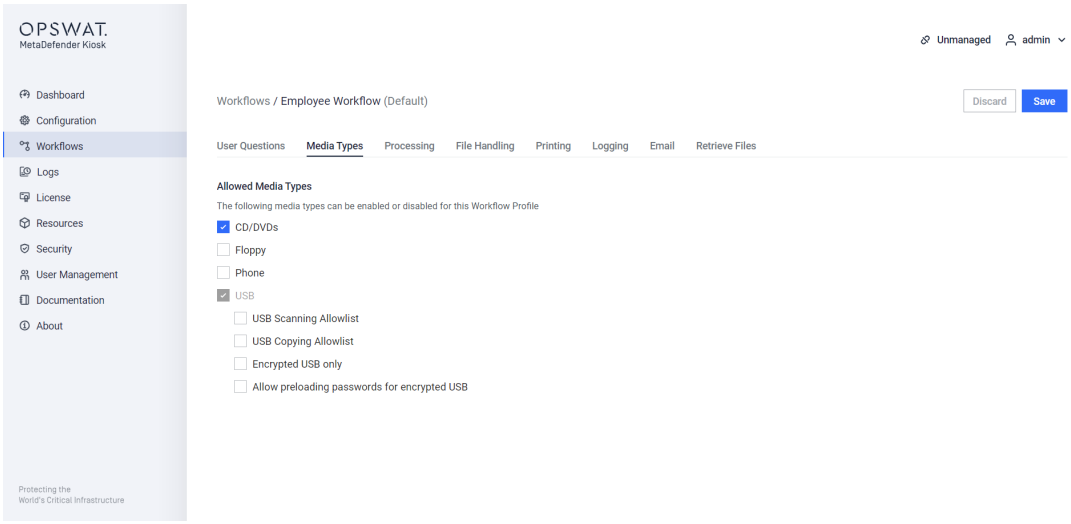
> **Info**
> In some instances, an iPhone may not be recognized upon connection. This may be due to trust settings configured between the device and system which may require to reset Location & Privacy settings on the device.

USB Allowlisting

The USB Allowlist functionality permits to define a list of USB devices that can be processed by MetaDefender Kiosk.

Any USB that has a device ID that either equals or contains any of the items in the allowlist will be permitted for processing.

The allowlists can include as many items as the administrator would like to define.



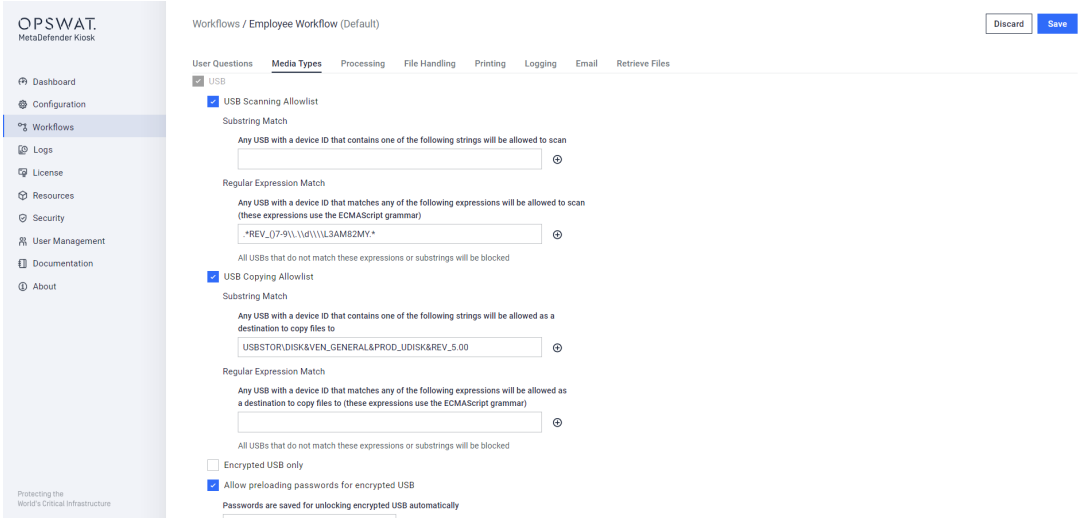
Media Types configuration

USB Scanning Allowlist

Only USBs that match the allowlist are accepted for scanning.

USB Copying Allowlist

Only USBs that match the allowlist can be used as a media destination to copy/move files to.USB Scanning Allowlist



USB Scanning and Copying Allowlist

Example of an allowlist entry and devices whose IDs would either result in them being allowed or denied:

Allowlist entry:
`USBSTOR\DISK&VEN_GENERAL&PROD_UDISK&REV_5.00`

Device ID	Allowed
`USBSTOR\DISK&VEN_GENERAL&PROD_UDISK&REV_5.00\208&0`	images/s/en_GB/7201/e9483755159fbecaf5aef9b1eebd09
`USBSTOR\DISK&VEN_GENERAL&PROD_UDISK&REV_5.00\336&0`	images/s/en_GB/7201/e9483755159fbecaf5aef9b1eebd09
`USBSTOR\DISK&VEN_GENERAL&PROD_UDISK&REV_**5.01**\404&0`	images/s/en_GB/7201/e9483755159fbecaf5aef9b1eebd09

Info
Device IDs of USBs from previous scan sessions can be found in the Session History page

Encrypted USB Only

Only encrypted USBs are accepted for scanning and copy-to.

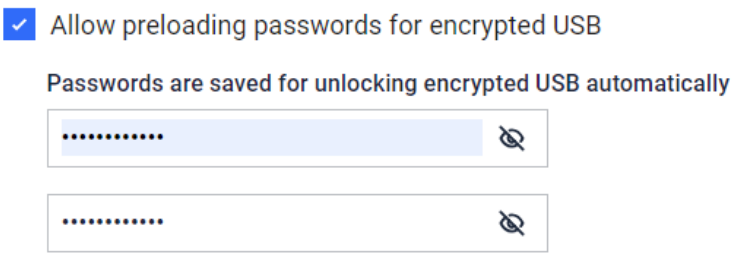
The admin can combine this option with `USB Scanning Allowlist` and `USB Copying Allowlist`

Allow preloading passwords for encrypted USB

Kiosk will automatically decrypt the encrypted USB using a list of preloaded passwords for scanning only.

The maximum number of passwords that can be added is 2.

When enabled, password prompt will not display, but caution is strongly recommended because incorrect passwords can cause data loss or device damage.

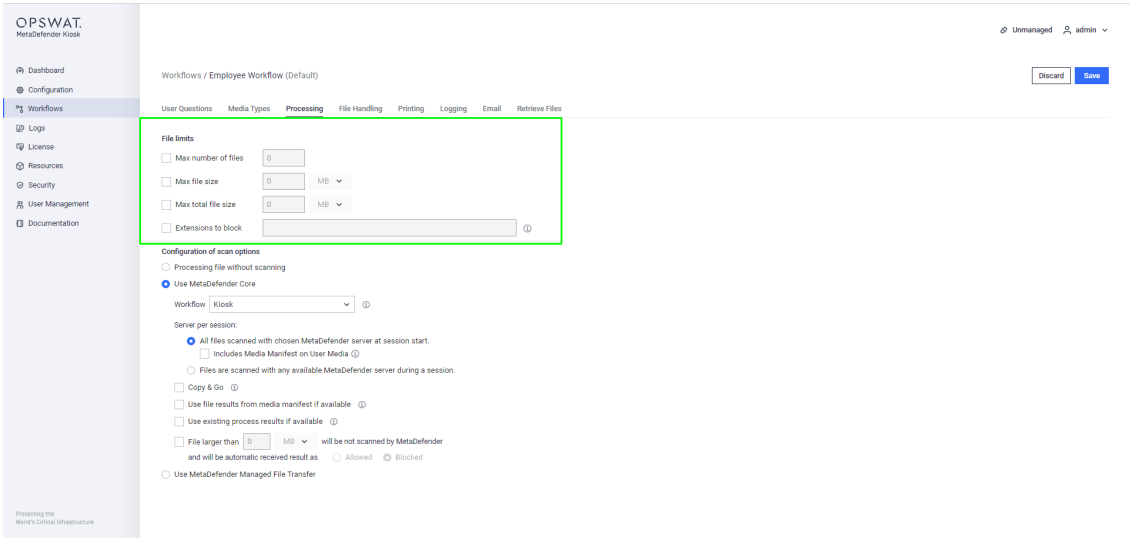


Selecting a Server to Process Files

I. File limits

Tactics: Configure specific rules to restrict users from initiating a scan session at pre-processing phase.

Benefit: Allow users to optimize and choose data size, file extensions which will be scanned on Kiosk later manually.



If the users select files that exceed applied configured rules, they cannot initiate a scan session. Those rules will be applied to both **Browse** and **Process All** in **Processing options**. The appropriate messages will appear on Kiosk UI and prevent the users from starting the session.

Limited number of files

Configuring the maximum number of files that the user can select. The minimum value that can be input is 0, max is 100,000,000.

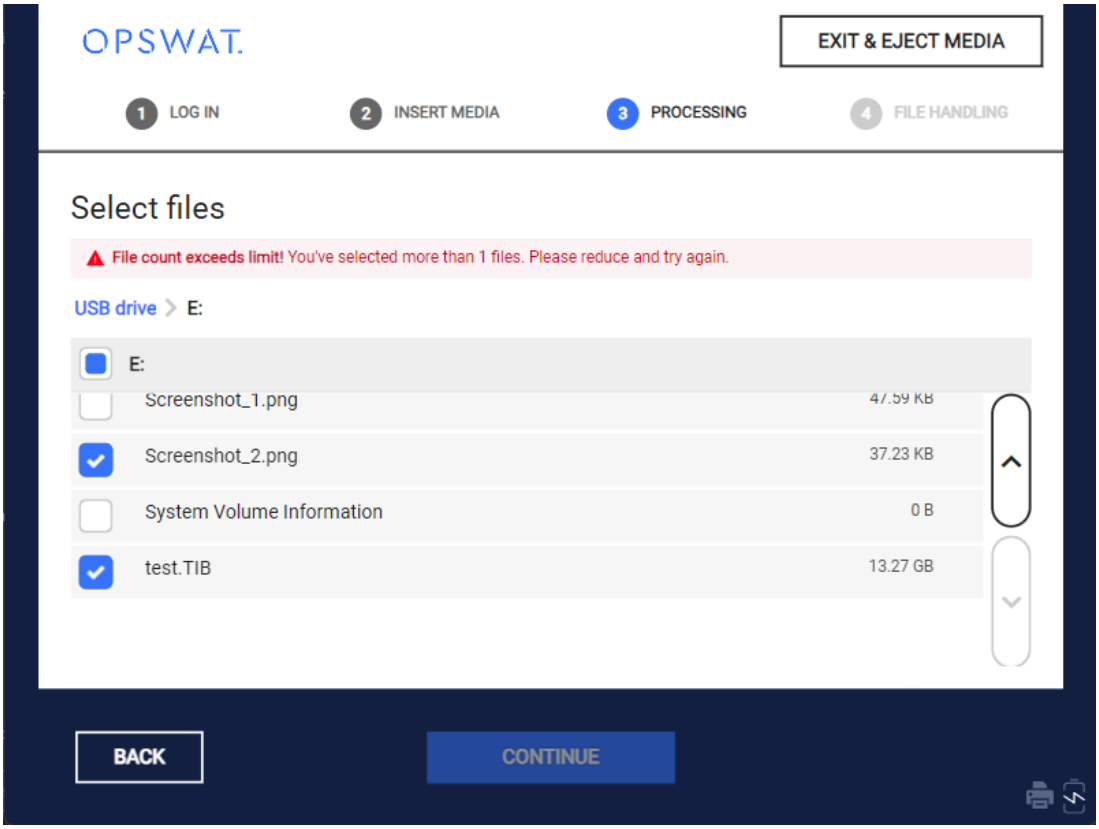


Image: "File count exeeds limit" notification on Kiosk UI

Limited file size

Configuring the maximum size of each file, measured in megabytes (MB) or gigabytes (GB). The minimum value that can be input is 0, maximum is 10,000.

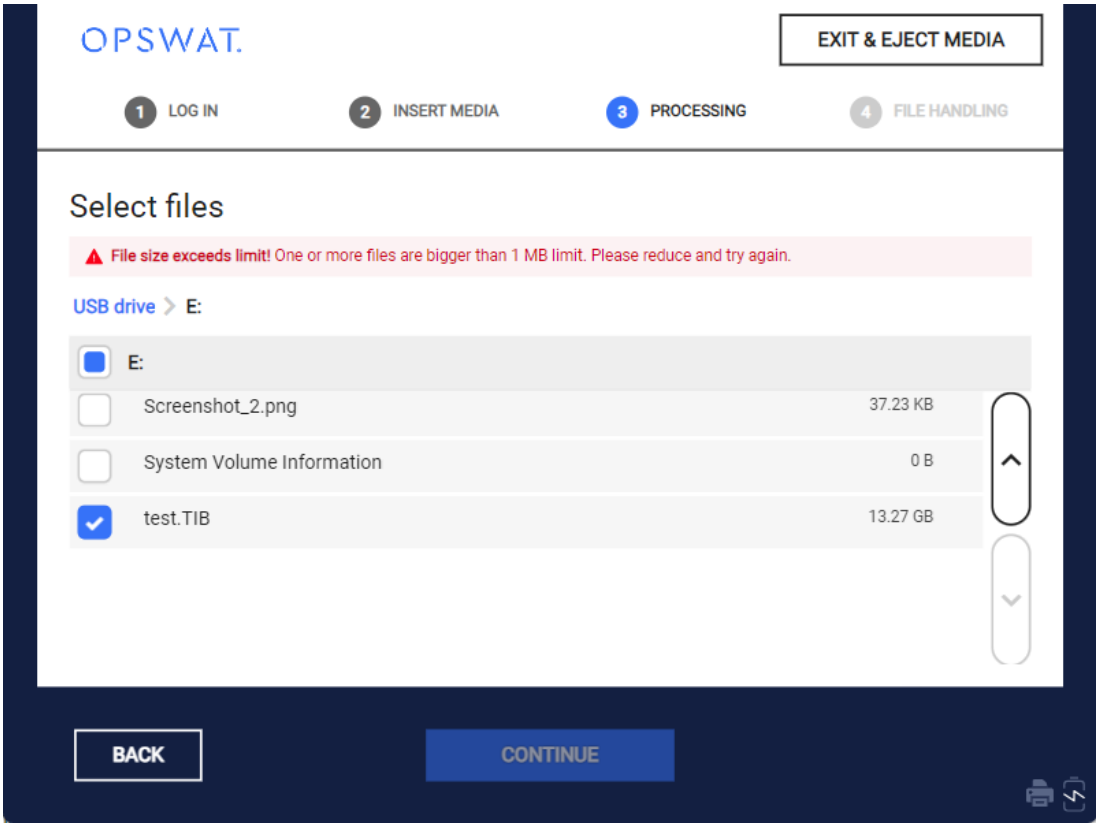


Image: "File size exeeds limit" notification on Kiosk UI

Limit of total file size

Configuring the maximum total size of all selected files, measured in megabytes (MB) or gigabytes (GB). The minimum value that can be input is 0, max is 10,000.

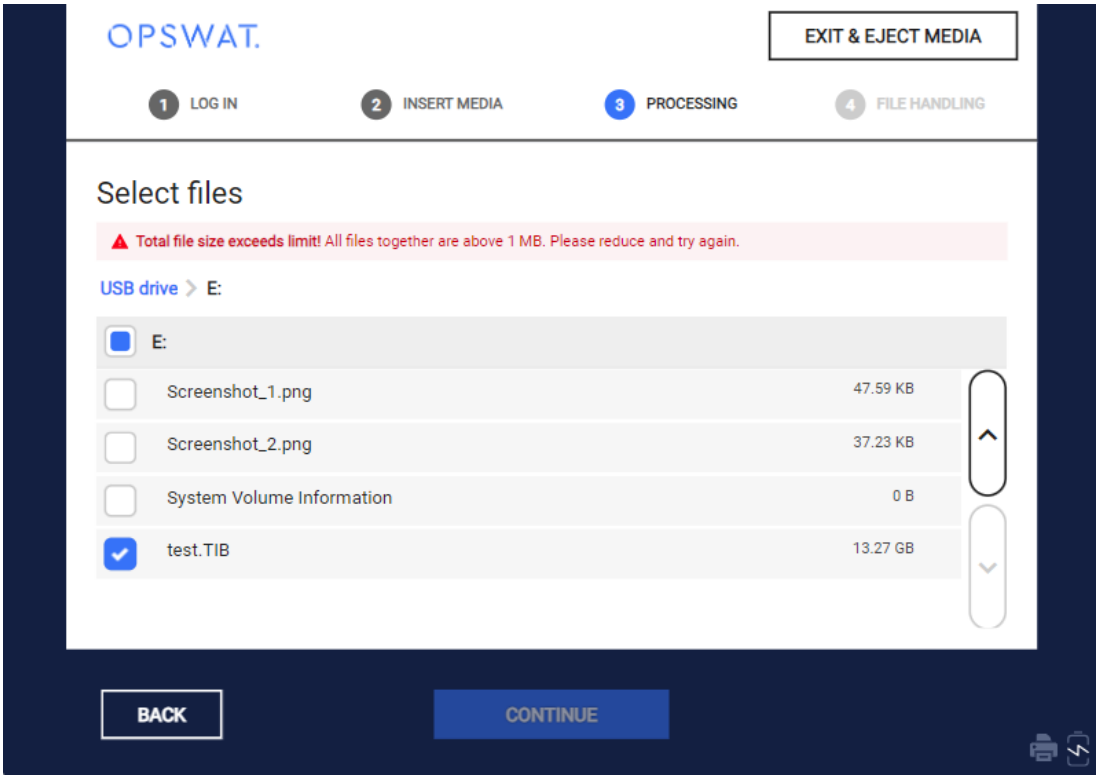


Image: "Total file size exeeds limit" notification on Kiosk UI

Blocked file extensions

List of blocked extensions that user cannot select to scan. The user needs to input at least one file extension in order to activate this feature. Extension in list is separated by semicolon (;).

Image: "Blocking file extensions" option on Kiosk Configuration

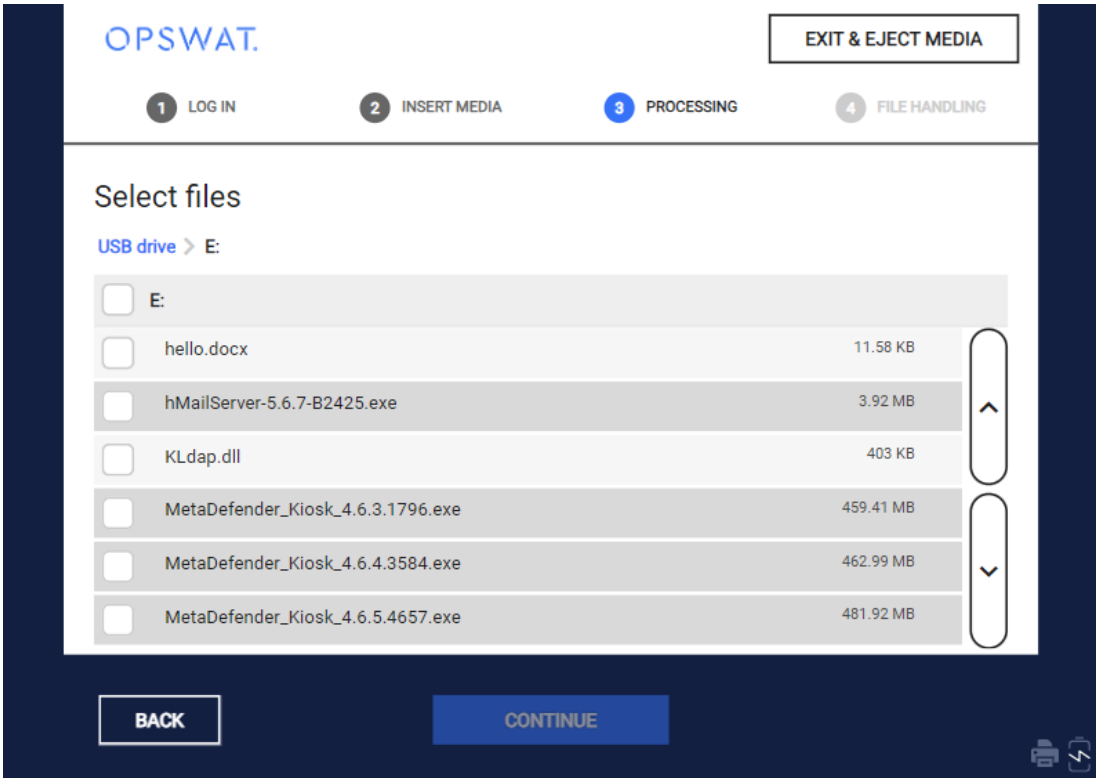


Image: Blocked file on Kiosk UI (after applying blocking .exe file extension on Management Console)

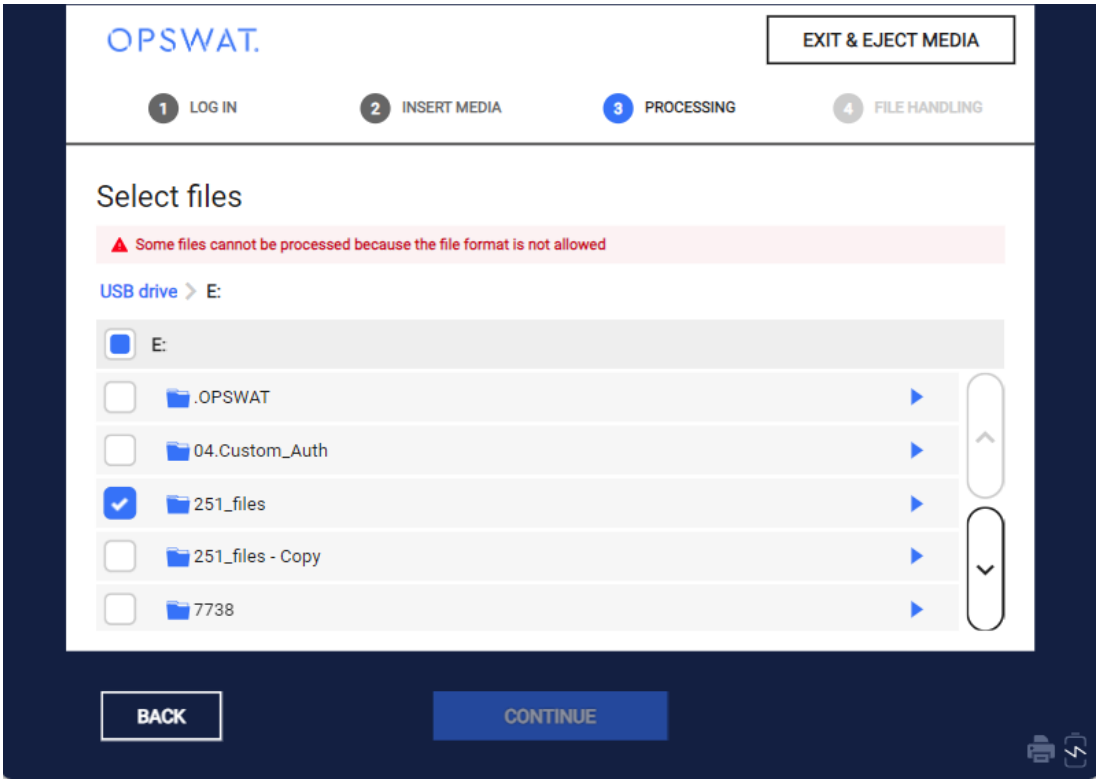


Image: Notification appears on Kiosk UI when selecting folders contain blocked file extensions

> **Info**
> **Process All**: A "Limit Exceeded" attention will be displayed if any values surpass their respective threshold.

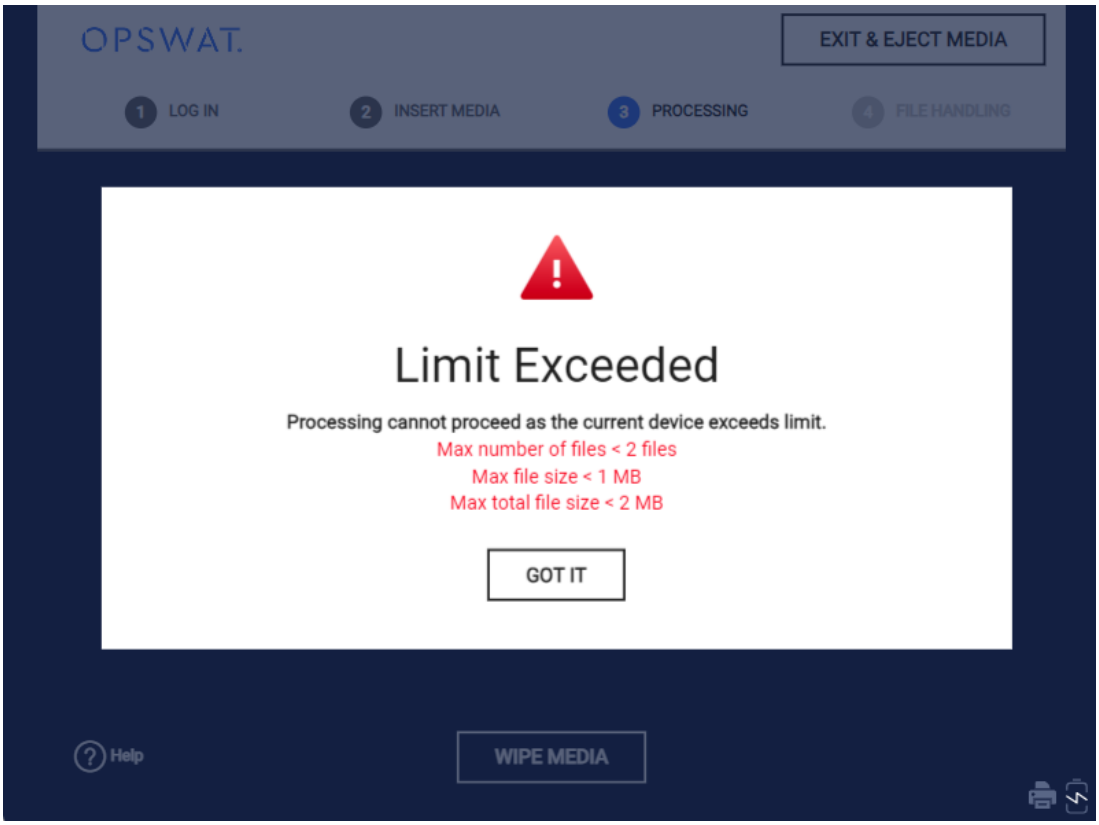


Image: "Limit Exceeded" notification on Kiosk UI for Process All

> **Note**
> Scan limits is not available for Simplified Workflow

II. Processing

1. Do not proceed files with a MetaDefender or MFT server

In the case of no scan requirements, the admin can choose neither MetaDefender nor MFT. With this option, only file handling can be executed.

The hash calculation of files can be disabled with option `Do not calculate file hashes` to speed up the duration of the session.

Image: "Do not proceed files with MetaDefender or MFT Server" option on Kiosk configuration page

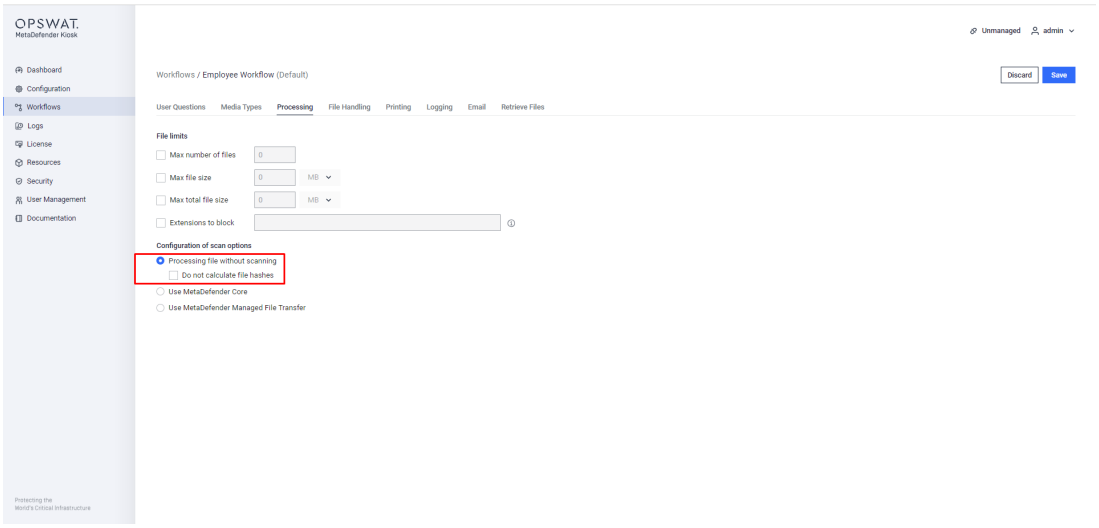


Image: "Processing file without scanning" option on Kiosk configuration page

2. Use MetaDefender Core server

MetaDefender Kiosk requires a MetaDefender Core server in order to use the multi-scanning technologies and functionalities. The MetaDefender Core server can be installed on the same system as MetaDefender Kiosk or on another machines. The MetaDefender Core server used is configured in the Primary MetaDefender Server option on the Configuration settings page.

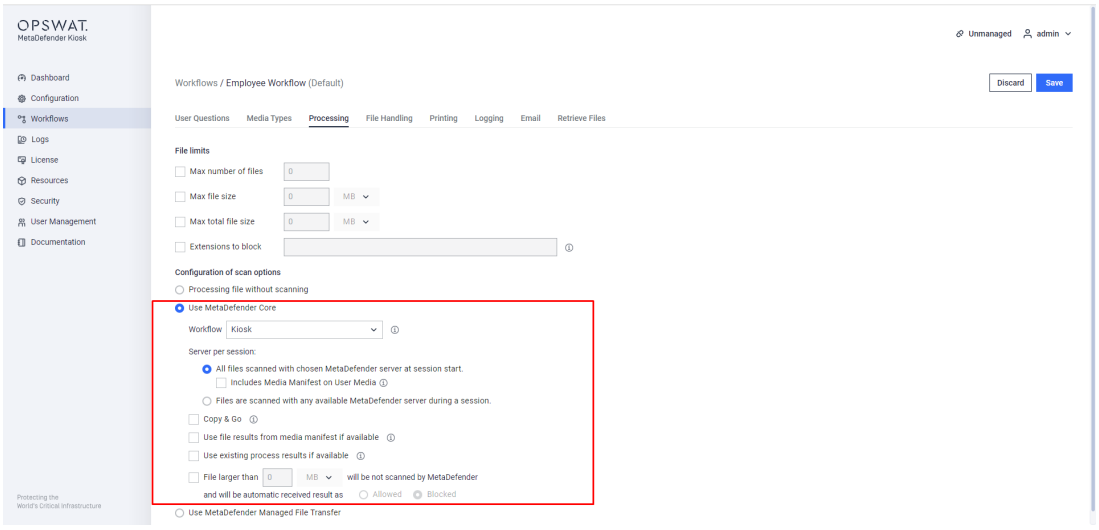


Image: "Use MetaDefender Core" option on Kiosk Configuration page

Workflow Rule

The Workflow Rule drop-down menu determines which MetaDefender Core workflow rule is used to process files from MetaDefender Kiosk.

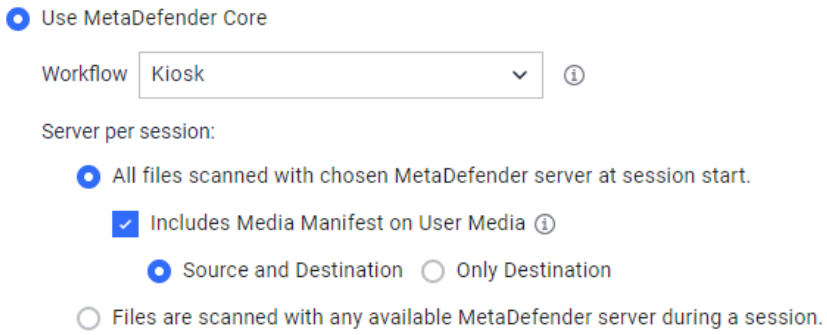
There are two processing methods to utilize a MetaDefender server:

Files are only processed with the available MetaDefender server chosen at the start of a session

The default behavior is an available MetaDefender server will be selected at the beginning of a session. Any errors encountered with the server will cause Kiosk to retry processing the file with the server.

Include Media Manifest on User Media

When used with MetaDefender Core version 4.8.0+, a media manifest can be added to media processed by MetaDefender Kiosk. This setting enables the creation of a signed Media Manifest that contains the scan results for all files that were scanned as part of the session. This manifest can be validated by other MetaDefender products.



The KIOSK allows choosing the storage location for the manifest.

- **Source and Destination**: By default, the manifest will be saved on both the scanned media and the destination media configured on the User media page.
- **Only Destination**: The manifest will be exclusively stored on the destination media.

Files are processed with any available MetaDefender server during a session

The second processing method allows Kiosk to choose any available server (Primary + Backups) during a session. If any connection failure occurs during the session, Kiosk will re-attempt processing the file on the next available server. With this method selected, the Media Manifest feature cannot be carried out. When viewing files processed under this method in Core's history, they will be displayed individually rather than being grouped into a session entry. All other features are allowed regardless of the processing method selected.

Copy & Go

Files to process are copied from the media to the system for processing later. Users are informed to remove their media when the copy has finished. Once the session is finished, all processed files are removed from the system. The system must have enough free space to accommodate all the files to process.

Use file results from media manifest if available

Kiosk can also validate files according to the Media Manifest file that exists on the media to be processed. If a file is found on the media but not found within the manifest, it will be sent to MetaDefender for processing. The certificate with which the manifest is signed by needs to be trusted on the system, else Kiosk cannot trust the manifest and will send files for processing.

Use existing process results if available

Kiosk can retrieve previously existing results for files by performing a hash lookup instead of uploading a file to MetaDefender for processing. This cannot be used in conjunction with Media Manifest since the manifest always contains the latest results.

File larger than ## [MB/GB] will be not scanned by MetaDefender

A maximum file size can be specified for files to be processed by MetaDefender, all files larger than this will still be processed by Kiosk without being processed by MetaDefender. The files that are larger are treated as configured allowed or blocked due to the reason `"Exceeded file size"` .

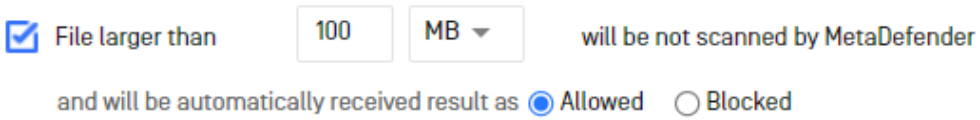
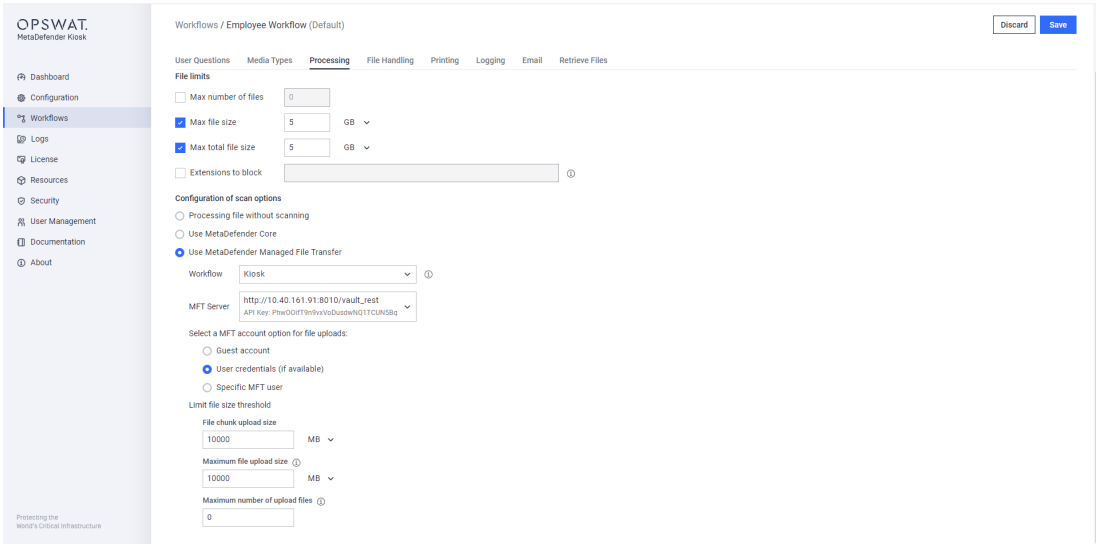


Image: Choose file size that will be scanned and proceeded by MetaDefender Kiosk

III. Using MFT Server

To reduce user time spent at the Kiosk, processing files can be offloaded to a MFT server connected to a MetaDefender Core. Files will be uploaded directly from Kiosk to MFT, once uploading is done, the session will complete and the user may remove their media and proceed. Meanwhile, MFT will send the uploaded files to MetaDefender to process and, based on the configuration, notify the user when the files are ready for retrieval.



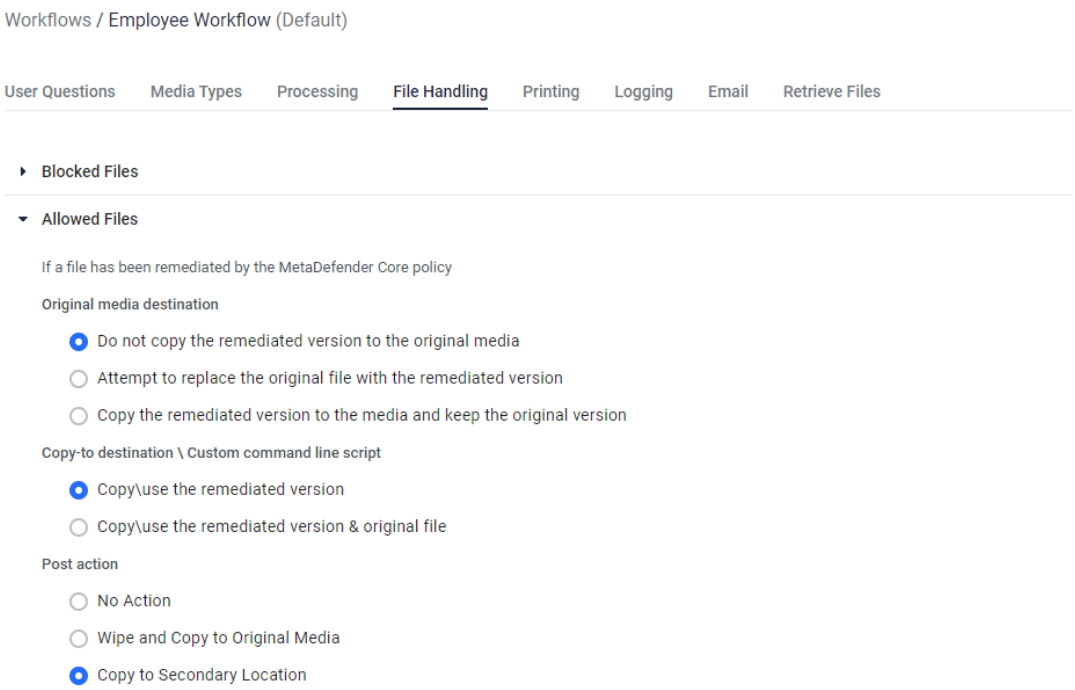
- **Workflow:** MD Core workflow rule that MFT will use to proceed the uploaded files
- **MFT Server:** See 6. Configuring with MFT for instructions and more details
- **Select a MFT account option for file uploads:** Choose a MFT account option in this section
    - **Guest account:** A temporary guest login ID is created and displayed to the Kiosk user both on the scan results screen as well as in the digital and printed logs.

    - **User credentials:** Use the designated user login credentials for logging into the MFT server.
    - **Specific MFT user:** Transmit files directly to a specified user on the MFT system. (This can be useful when custom authentication users do not match users synced with MFT)
- **File Chunk Upload Size:** Size of chunks a file will be broken into for uploading to MFT. The acceptable input range for values is from 0 to 10000 MB/GB.
- **Maximum File Upload Size:** files exceeding the maximum size is not uploaded to MFT server. The acceptable input range for values is from 0 to 10000 MB/GB.
- **Maximum Number Of Upload Files:** upload files until the upload count reaches the maximum. The acceptable input range for values is from 0 to 10000.

> **Info**
> If upload authentication fails, files will be uploaded to a MFT guest account

Selecting How to Handle Processed Files

The File Handling page is divided into two sections: actions to take on blocked files and actions to be taken on allowed files. You can set different file handling options for each, including copying to either new media or a network path.



"File Handling for Allowed Files" option on Kiosk Configuration page

Remediated file handling

If file sanitization (Deep CDR) and redaction (Proactive DLP) have been configured on the MetaDefender Core, the Kiosk will download the remediated file which stands for the sanitized file or redacted file if any. There are three selections for handling a remediated file with the original media.

- **Do not copy the remediated version to the original media** (the default selection) Specifies that a remediated file will not be copied to the original media and the original file will be left untouched.
- **Attempt to replace the original file with the remediated version** Specifies that the remediated file will be copied to the original media and the original file will be deleted.
- **Copy the remediated version to the media and keep the original version** Specifies that the remediated file will be copied to the original media and the original file will be left untouched.

For a copy-to destination or custom command line script set:

- **Copy/use the remediated version** (the default selection) If a remediated version of a file exists, that will be copied to the destination, or utilized in the script, configured in favor of the original file.
- **Copy/use the remediated version & original file** If a remediated version of a file exists, it will be copied to the destination or utilized in the script configured along with the original file.

Stop processing media when a predefined number of blocked files are found

Selecting this option will cause a Kiosk session to stop processing immediately when the preset number of blocked files is found. Kiosk will alert the user that preset numbers blocked files were found and go directly to the session summary after the user has acknowledged the message.

Info

- The number of blocked files can be higher than the setting.
- Max value of blocked files can be set is 1000.

Taking no action or removing files

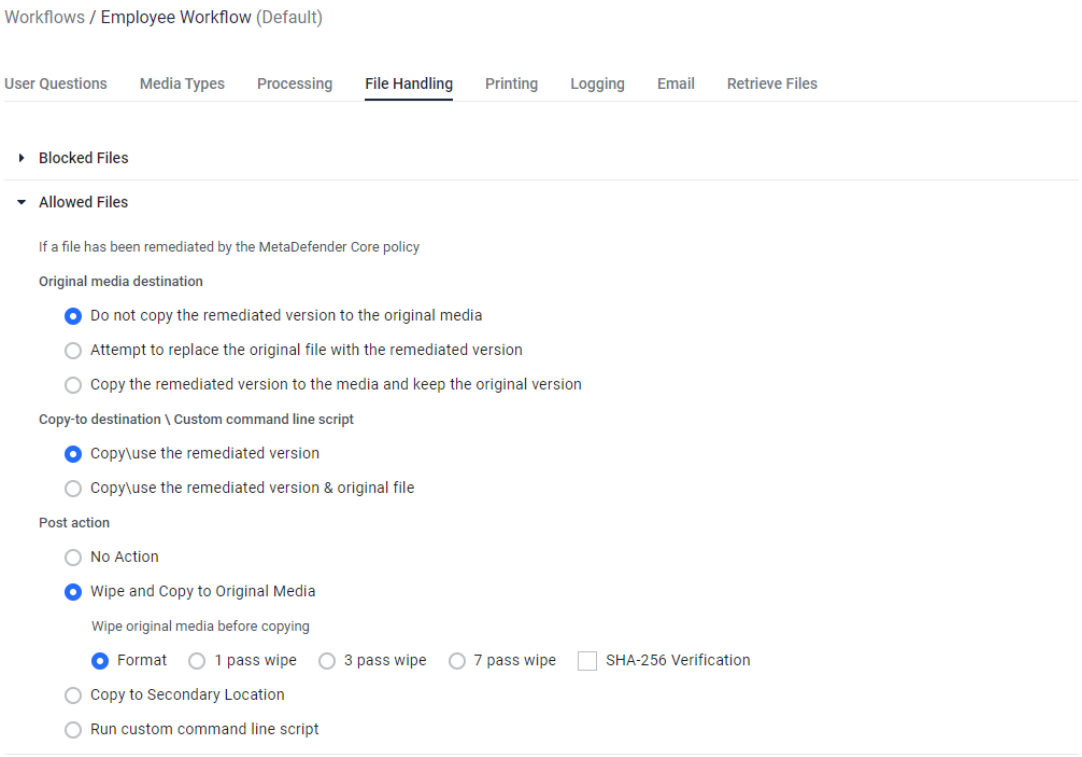
To take no action on blocked or allowed files, select the **No Action** radio button. To remove any non-remediated blocked files, select the **Remove file** radio button and select an option from the drop-down menu:

- **Quarantine blocked files in Kiosk**: blocked file will be added to the Kiosk quarantine and removed from the original media
- **Quarantine blocked files in Core**: blocked file will be added to the Core quarantine (if configured on Core) and removed from the original media
- **Remove all blocked files from media**: blocked file will be removed from the original media
  - **Prompt User for Confirmation**: user will be prompted whether to delete all blocked files at the results screen
- **Remove selected blocked files from media**: Kiosk will show all blocked files; and Administrator can select and remove the blocked files from the original media
  - **Prompt User for Confirmation**: user will be prompted whether to delete the selected blocked files

Copying Allowed files to Original Media

Warning
This option will delete all files and perform a disk format\wipe on the original media before copying ONLY the allowed files back to the original media.

This option is only available for allowed files. After enabling this option, standard wipe options of Format, 1, 3, or 7 pass wipe are selectable. Please note that the pass wipe options will take significantly more time to complete.

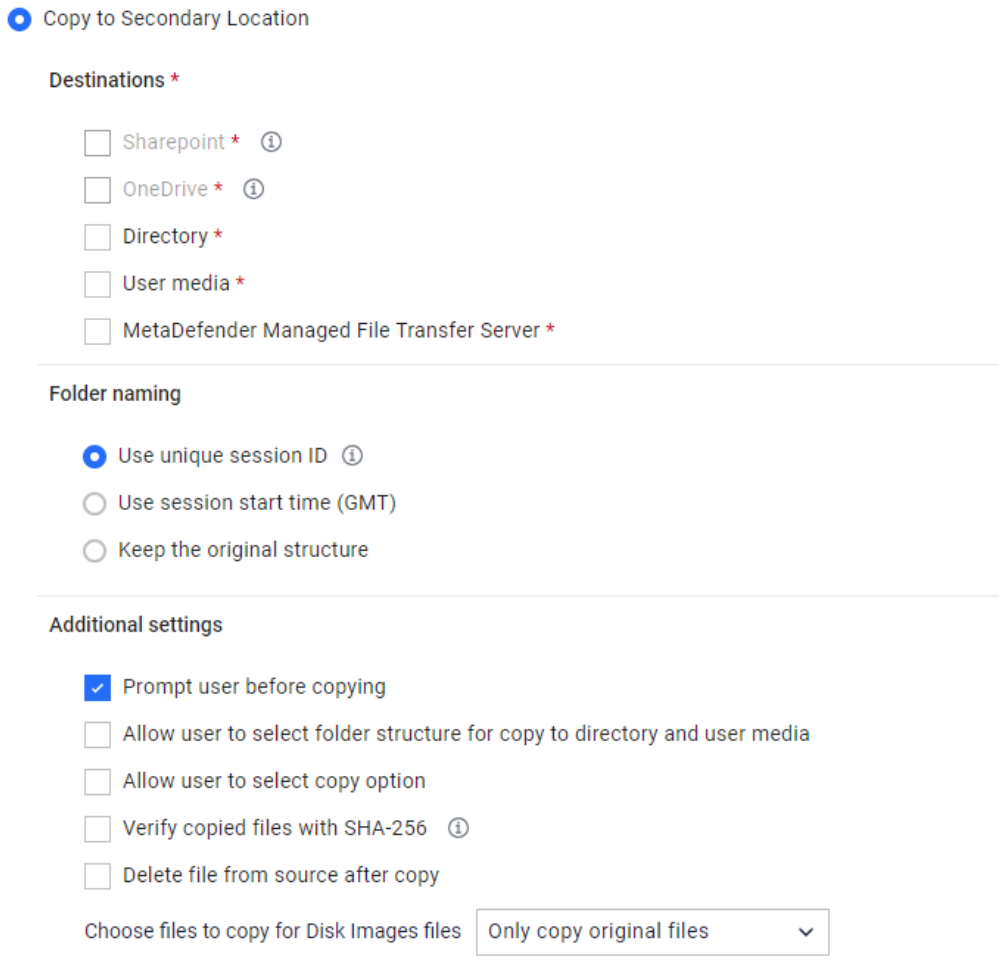


"File Handling for Allowed files" on Kiosk configuration page

Copying files to a designated locations

Note: If a file has been remediated by MetaDefender Core's Data Sanitization and Copy to is selected here, the remediated file will be copied to the desired location, not the original file.

You can configure files to be copied to a designated location in the Copy to section.



Prompt user before copying

By default, a user will have to initiate copying files from session results screen. If prompting is disabled, files will be copied automatically before the session results are displayed.

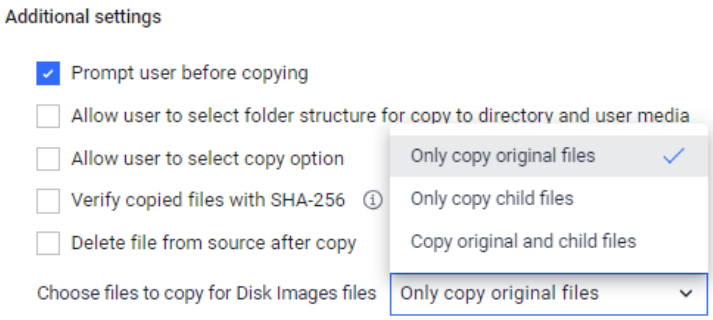
Folder structure

MetaDefender Kiosk will copy files to the location specified by one of the three naming conventions selected:

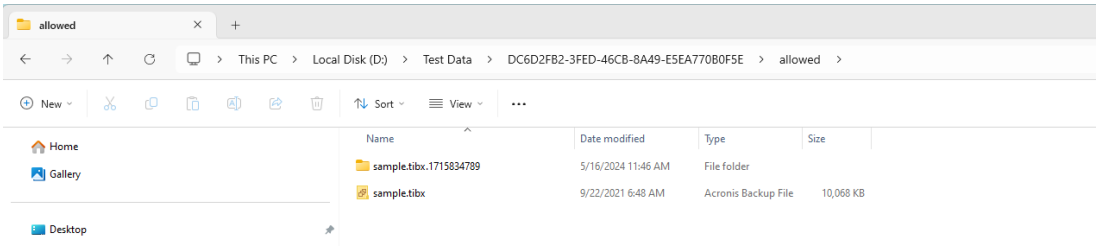
- **Directory named with the unique session ID:** Copies files to a directory identified by the session ID.
- **Directory named with the session start time (GMT):** Copies files to a directory identified by the session start time.
- **Keep the same folder structure as on original media (no subfolders):** Copies files to the same directory as in the original media.

Processing virtual disk files

You can select to copy the original files and child files of disk image files that were mounted to scan. By default, only the original files are copied.



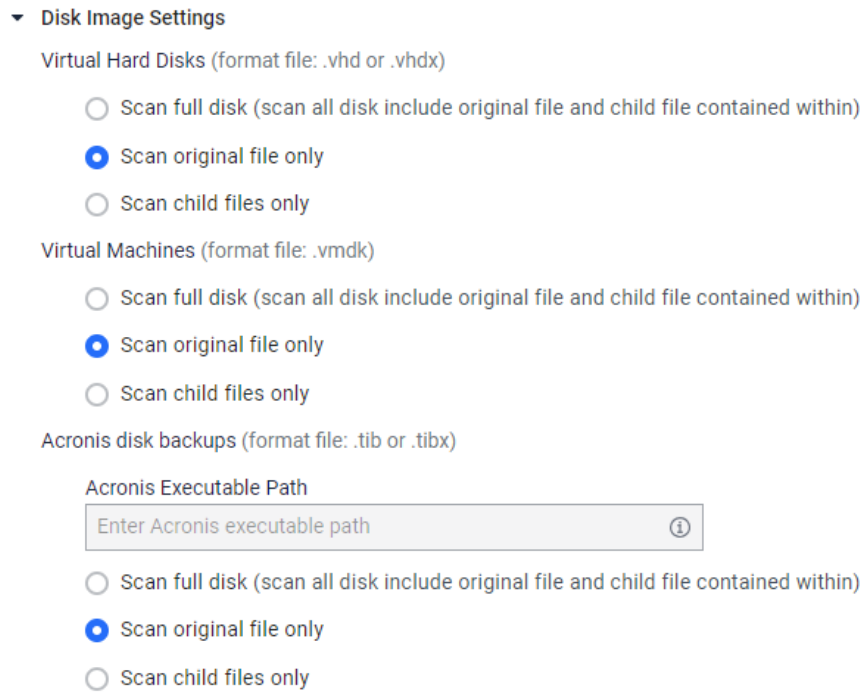
The child files inside the disk image will be copied to the destination on the folder whose name is constructed from the original file name and timestamp suffixes. The child file folder will be in the same folder structure as the original files.



Original and child files are copied to destination folder

Notes:

- This option is available for both allowed and blocked file settings.
- Kiosk will not modify the content of original disk image files.
- This option only takes effect for the disk image type that is enabled mounting and scanning option at global configuration for disk image files. If the disk image type is disabled mount and scan, only the original file is scanned and copied to destination.

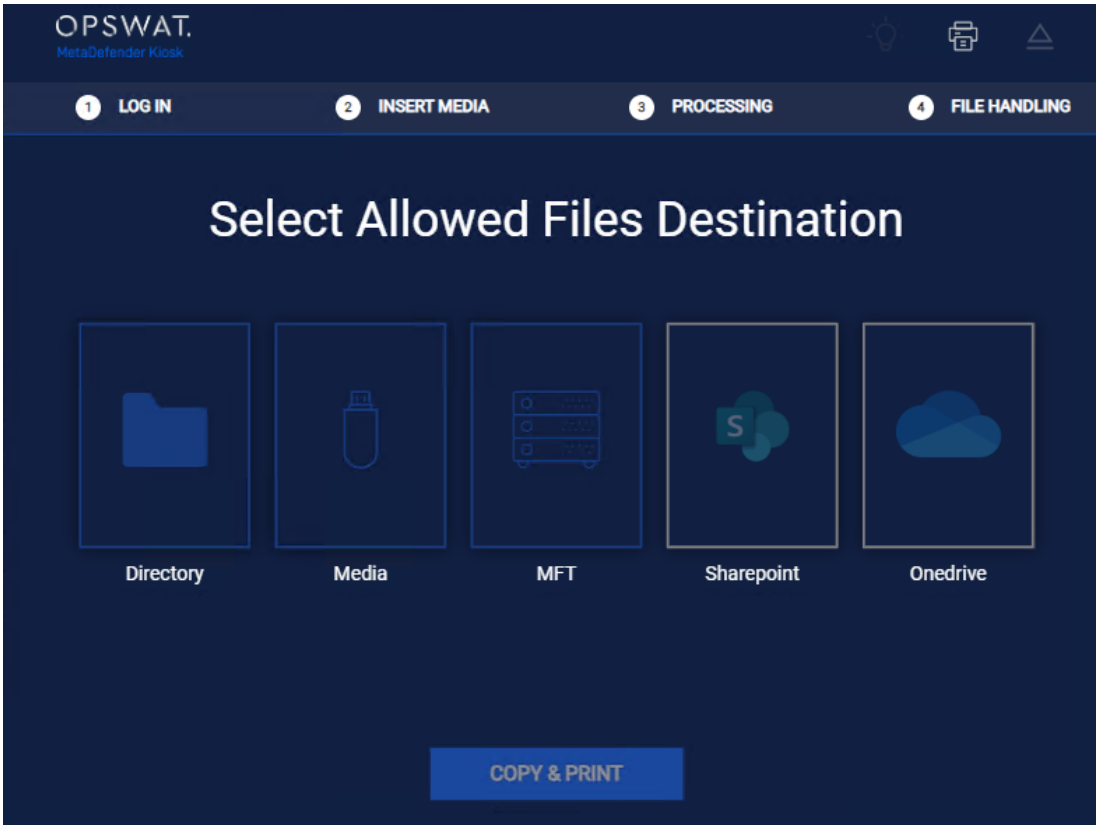


Allow user to select folder structure for copy to directory and user media

This allows users to select the folder structure (outlined above) before copying files.

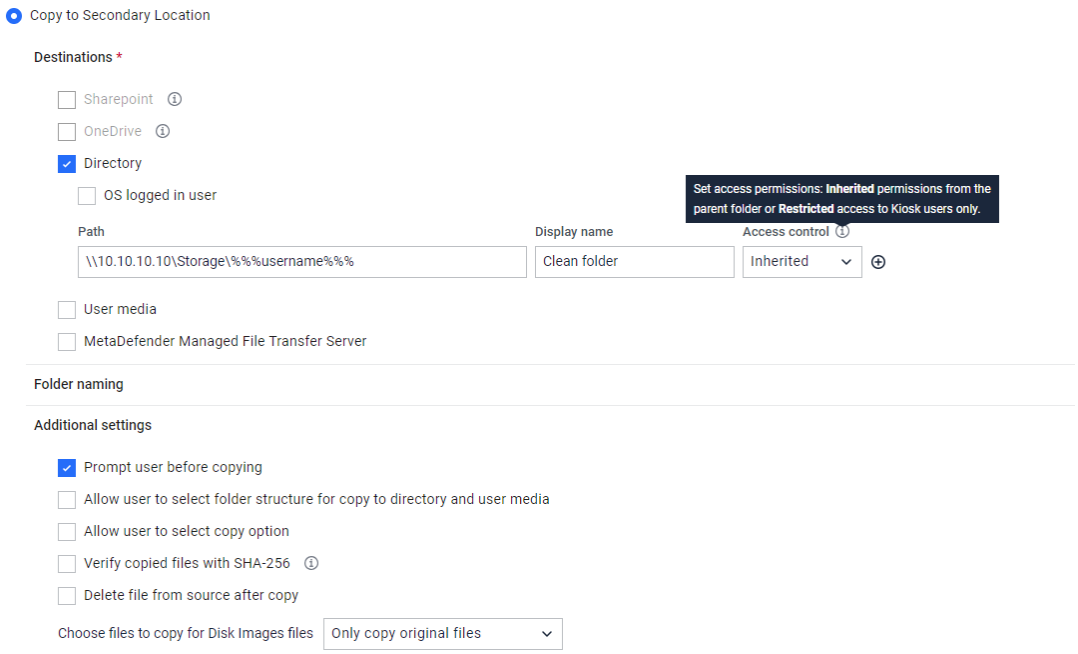
Allow user to select copy option

This allows users to select which enabled copy option to run at the end of a session. For example, if copying to a Directory and User Media is set, a user can choose to run both, neither or only one. If multiple directories are configured, a user will be able to choose among the list of configured directories.



Directory

The Directory option allows you to specify locations for blocked or allowed files. Files will be copied to all configured directories by default. The copy to directory uses AD user's credentials that is logged into the Kiosk session for copying privileges.



- **Path**: indicates the destination location files will be copied to.
- **Display Name:** indicates the value that is displayed on the UI to the user for selection.
- **Access Control** (only available on Employee workflow): grant permissions of the files and folders when copying destination locations.
  - **Inherited**: Files and folders will inherit the same permissions as the parent folder
  - **Restricted**: Only Kiosk authenticated users will have the permissions to access their files and folders
- **OS logged in user:** An Admin can enable utilizing the OS logged in user's credentials if the copy initially fails with the AD user credentials.

Info

- Maximum number of directories can be added is 100
- ***Path*** and ***Display Name*** must be unique
- ***Access Control*** option is only available on Kiosk version 4.7.2 or newer
- If ***Allow user to select copy option*** is enabled, then the user will be able to browse and select which directories will be utilized, including the sub-directories

You can copy files to a remote server (i.e. network share) by providing a UNC path. To allow for more restrictive permissions on a network share, a MetaDefender Kiosk workflow will need to be created containing users that have, at minimum, write permission to the network share. When a user logs into a session, MetaDefender Kiosk will attempt to use the permissions of the user to copy files to the network share.

Pro tips

The predefined '%%%username%%%' variable can be used within the designated location in the ***Path*** field to allow MetaDefender Kiosk to copy files to a folder (e.g. 'username'). This is for the user logged into the session.

Responses to user questions can also be utilized in the ***Path*** field via the predefined '%%%userresponse#%%%' variable, where '#' is the number of the response to the corresponding user question. For example, to utilize the answer to the question 2, the variable to use would be '%%%userresponse2%%%'. If no response to the question was given or no such question exists for the user response to exist (e.g. %%%userresponse999%%%), then the variable will exist in the path created.

Restricted directories

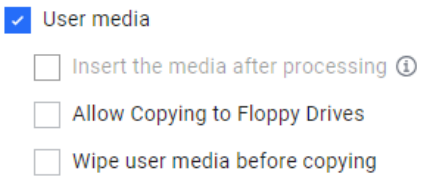
Following directories are restricted and cannot be used:

- C:\Windows
- C:\Program Files
- C:\Program Files (x86)
- C:\ProgramData
- C:\Users

User media

Selecting the `User media` checkbox will prompt users to insert secondary media to copy files to.

Supported media are USB, CD/DVD (must be blank and non-finalized), and Floppy.



`Insert the media after processing` - (option **only** applies to a Copy&Go session) this locks users to insert the media after all files are processed. If disabled, users can insert the secondary media at the start of a session.

`Allow Copying to Floppy Drives` - displays a floppy disk detection button to copy files to floppy.

`Wipe user media before copying` - displays the wipe option to automatically apply to the destination media before files are copied to it.

> **Warning for wiping user media**
> The wiping of CD/DVD is not supported by Kiosk, if user try to copy to a disc with data, the warning message will be shown and inform user to try again with blank disc.
>
> This process may take a long time if the destination media is large or multiple pass wipes are configured
>
> These encrypted media types do not support secure wipe: BitLocker, McAfee, and Flash Security

MetaDefender Managed File Transfer Server

- **MFT Server:** See 6. Configuring with MFT for instructions and more details
- **Select a MFT account option for file uploads:** Choose a MFT account option in this section
- **Select how files will be uploaded to MFT:** Choose a file upload option
- **File Chunk Upload Size:** Size of chunks a file will be broken into for uploading to MFT
- **Synchronize with Data Diode**: Alleviates any issues seen with uploading files through a data diode (**note**: *this will increase overall upload time*)

MFT account options for file uploads

- **Always upload to a MFT guest account** A temporary guest login ID is created and displayed to the Kiosk user both on the scan results screen as well as in the digital and printed logs. By default, the Guest ID is concealed on the screen result for security reasons, click on eye icon to reveal it.
- **Attempt to use user credentials if they are available** Kiosk uploads files to the user account that matches the one used during authentication
- **Enter MFT user to upload files to** Kiosk uploads files to the user account supplied (this can be useful when custom authentication users do not match users synced with MFT)

> **Info**
> If upload using the user credentials authentication fails, files will be uploaded to the MFT using guest account

MFT file upload options

- **Upload files and preserve directory structure** Files are upload to MFT while maintaining the directory structure
- **Upload files, preserve directory structure and send scan results** In addition to the previous option, files are uploaded along with their scan result obtained from Core. MFT will opt to use these results rather than rescanning the uploaded files.
- **Upload a zip archive containing the allowed files** Files are packaged into one zip resulting in one file upload to MFT.

Only Copy Remediated Files

> **Info**
> This option only exists for blocked files.

If enabled, only remediated versions of blocked files will be copied to the destination. Any blocked file that was not remediated will not be copied.

SHA-256 Verification

If enabled, MetaDefender Kiosk compares the hash value of files on the target directory with the ones from the original directory. Any mismatches are displayed and logged. No retry of the copy is performed in the case of a hash value mismatch.

Delete after copy

Select this checkbox if you want MetaDefender Kiosk to delete the blocked or allowed file after copying it to the specified location.

Run custom command line script

> **Administrator Caution**
> Enabling Custom Command Line Script may introduce potential security risks. It is recommended that only experienced administrators enable and manage this setting, taking full responsibility to implement appropriate security measures and monitor for any vulnerabilities.

Kiosk will execute the custom command line script at post-processing phase. See Custom Command Line Script for more details.

Custom Command Line Script

How To Configure

> **Administrator Caution**
> Enabling Custom Command Line Script may introduce potential security risks. It is recommended that only experienced administrators enable and manage this setting, taking full responsibility to implement appropriate security measures and monitor for any vulnerabilities.

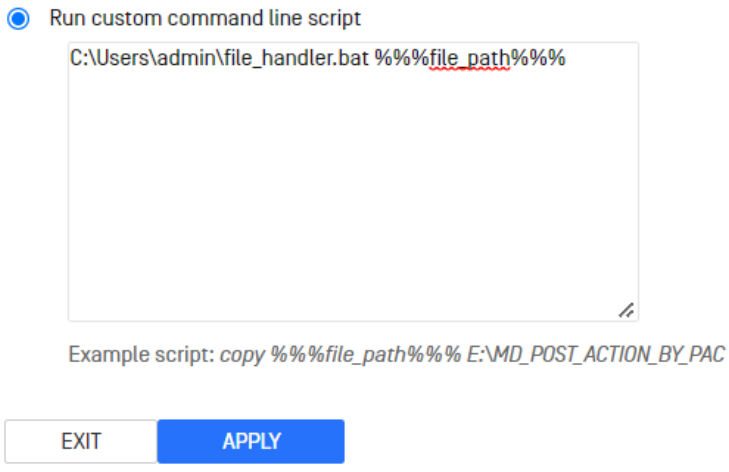
Post-processing scripts can be configured via the `Run custom command line script` option. Variables from the table below can be used in the scripts.

One command can only be configured for the script. For multiple commands, a batch or powershell script should be created and then called from the command line script.

For example, the following command line will call a batch script that will copy the file that was analyzed by Kiosk to `E:\MD_POST_ACTION_BY_PAC` folder and delete after the copy.

file_handler.bat none

```
echo off
set file=%1
copy /y %file% E:\MD_POST_ACTION_BY_PAC
del /q %file%
```



After entering your script, click `Apply`.

> **Warning**
> Be sure to test the script before configuring with Kiosk as the script is not validated.
>
> Paths or parameters (excluding Pre-defined variables for scripts) containing blanks should be surrounded in "quotes".

Pre-defined variables for scripts

Variable	Description	Notes
%%%file_path%%%	The absolute path of the file scanned	
%%%threat_name%%%	The name of the threat found by the engines	This variable only applies to infected scan results (`scan_all_result_i = 1`)
%%%scan_finished%%%	The time when the scan was finished	Local time of the kiosk system
%%%ticket_id%%%	A random number assigned to each Kiosk session	
%%%scan_results%%%	Integer representation of the scan result	
%%%process_result%%%	The process outcome • **Allowed** • **Blocked**	

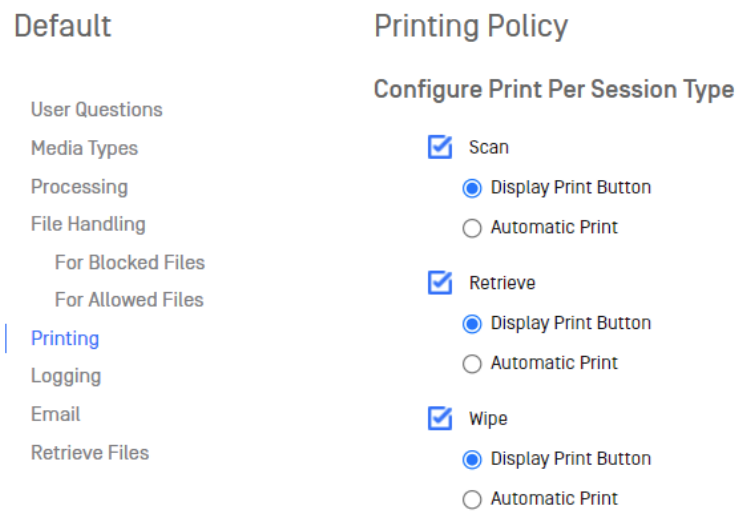
Running a Powershell script

To execute a Powershell script, the corresponding group policy needs to be set. See About Execution Policies under `USE GROUP POLICY TO MANAGE EXECUTION POLICY`. Enable `Turn on Script Execution` -> select `Allow all scripts`

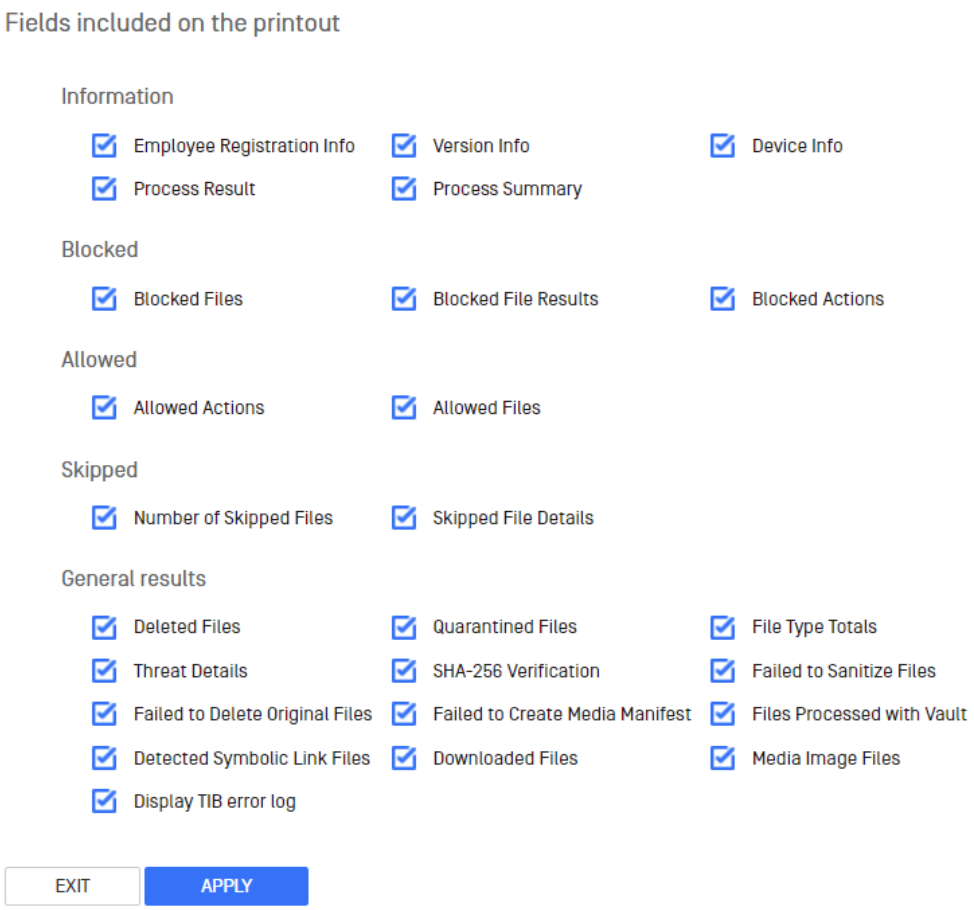
Managing Printing Options

The Printing Policy page lets you determine whether users have the option to print a receipt of their session and if so, what information will be included on the receipt. The printing is enabled/disabled separately for each action Scan/Retrieve/Wipe.

Note: MetaDefender Kiosk will use the printer which is set to default on the system. In case the printer prints to PDF files instead of real device, output PDF files are generated in "C:\Users<username>\AppData\Local\OPSWAT\Metadefender Kiosk\PrintToFile". Users are not able to select location for PDF files because Kiosk is in full screen hardened mode which does not show any other windows.



Kiosk administrators can configure in details what are included/excluded in/from the report.

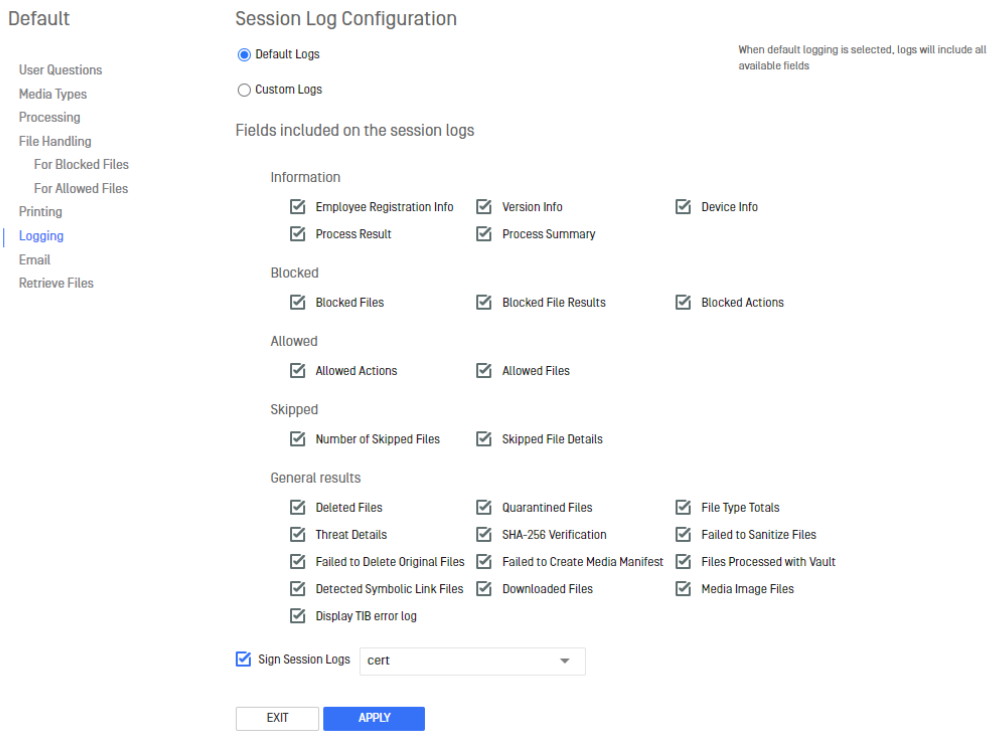


Notes:

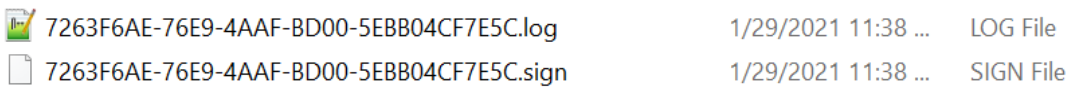
1. Skipped files are
    - Over-sized files (Upload to MFT for process)
    - Locked system files (Current)
    - Files which are unable to send to core by many reasons (failed to open, failed to send to core,....).
2. Blocked files are those reported “blocked” by Metadefender Core

Managing Logging Options

The Session Log Configuration page allows the selection of which sections to include in the session log file. Session log location and format is configurable in the global configuration.



For each workflow, session logs can be digitally signed if certificates are available. See Setting up HTTPS for adding certificates to Kiosk. By default, "Sign Session Logs" is disabled. When enabled, the signature of the session log is generated along with the log:



Warning
Certificates with passwords are not supported for signing session logs.

The signature file can be used to validate the session log to ensure contents have not been tampered with and the signature was signed with a trusted certificate. OpenSSL can be used to perform this validation.

none

```
Sample batch script to validate using OpenSSL's command line

@echo OFF
set /p sessionlog="Enter the session log file path: "
set /p signature="Enter the sign file path: "
set /p certificate="Enter the certificate file path: "
set openssl="C:\Program Files (x86)\OPSWAT\Metadefender
Kiosk\Client\REST\Data\openssl.exe"
echo Verifying "%sessionlog%" using signature "%signature%" and certificate
"%certificate%"

%openssl% x509 -inform pem -in %certificate% -pubkey -noout > publickey
%openssl% enc -d -A -base64 -in %signature% -out sign
%openssl% dgst -sha256 -verify publickey -signature sign %sessionlog%

del publickey
del sign

pause
```

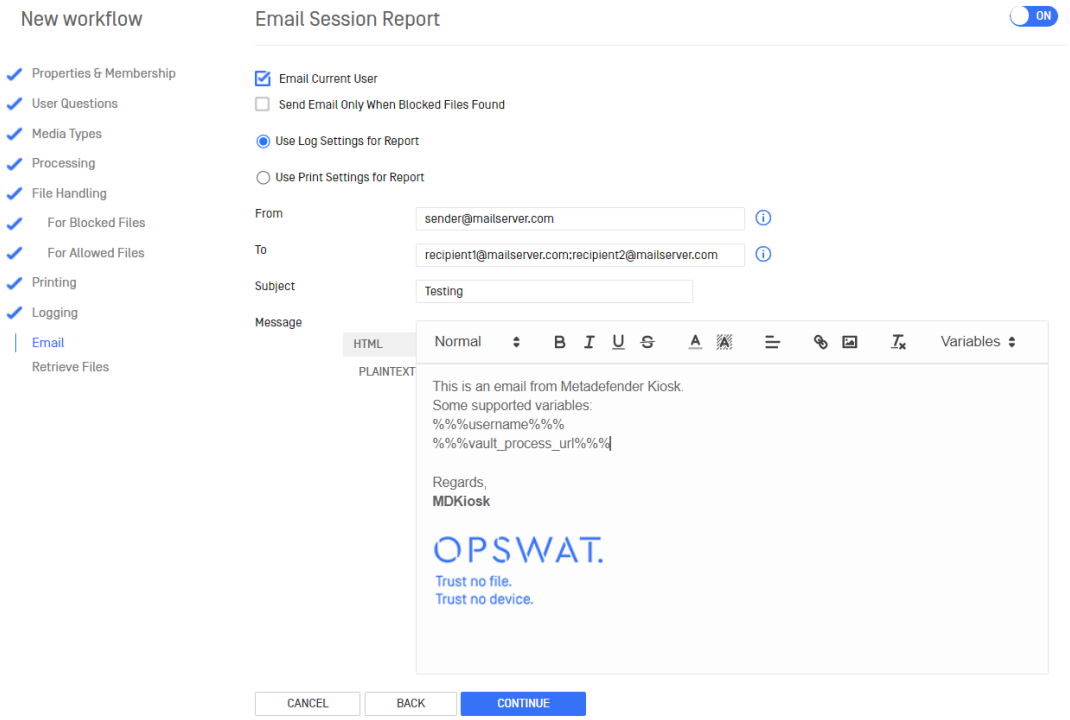
Email Session Report

The Email Session Report page lets you set up automatic emails that are sent to a designated recipient after each session is completed. To enable this feature, move the slider on the right hand side of the page to [On]. [Email Current User] allows the ability to send the session report to the AD user currently logged in to the Kiosk session or allow a Guest user to input an email address. [Send Email Only When Blocked Files Found] will not send an email for every session, only for a session where a blocked file was found. [Use Log Settings for Report] will send the session log as an attachment. [Use Print Settings for Report] will send the session printout as an attachment.

SMTP settings are necessary to be configured to allow sending emails. Configuration can be done in the Advanced Configuration section of the Configuration page. The email template composed in the Configuration page is applied for new workflow creation as a HTML email format, but the Kiosk admin can switch to Plain text. The content of HTML and Plaintext email can be different.

Some predefined variables are supported to generate session-constraint values. These variables are escaped with corresponding values configured in the WF and the receiver can see them in the email body. The admin can get the meaning of each variables via information icon on each variable

Variable	Description
%%%session_id%%%	The Kiosk session ID
%%%username%%%	Username logged into this session. For guest, the username is Guest
%%%date%%%	The date of the Kiosk session
%%%start_time%%%	The start time of the Kiosk scanning session
%%%end_time%%%	The end time of the Kiosk scanning session
%%%device_model%%%	The model of the inserted media
%%%device___serial_number%%%	The serial number of the inserted media
%%%device___media_type%%%	The device type of the inserted media
%%%device_id%%%	The device ID of the inserted media
%%%total___files_scanned%%%	The total files are scanned by Kiosk
%%%blocked_files%%%	The number of blocked files by Kiosk
%%%allowed_files%%%	The number of allowed files by Kiosk
%%%skipped_files%%%	The number of files is skipped scanning by Kiosk
%%%remediated_files%%%	The number of files is remediated by Kiosk
%%%vault_process_url%%%	MFT server URL where files are processed
%%%vault_access_id%%%	Login IDs to access files uploaded to MFT
%%%vault_allowed_url%%%	MFT URL where allowed files are copied to
%%%vault_blocked_url%%%	MFT URL where blocked files are copied to
%%%vault_download_url%%%	MFT URL where files are downloaded from



Existing workflows are not updated with new email template.

Note:

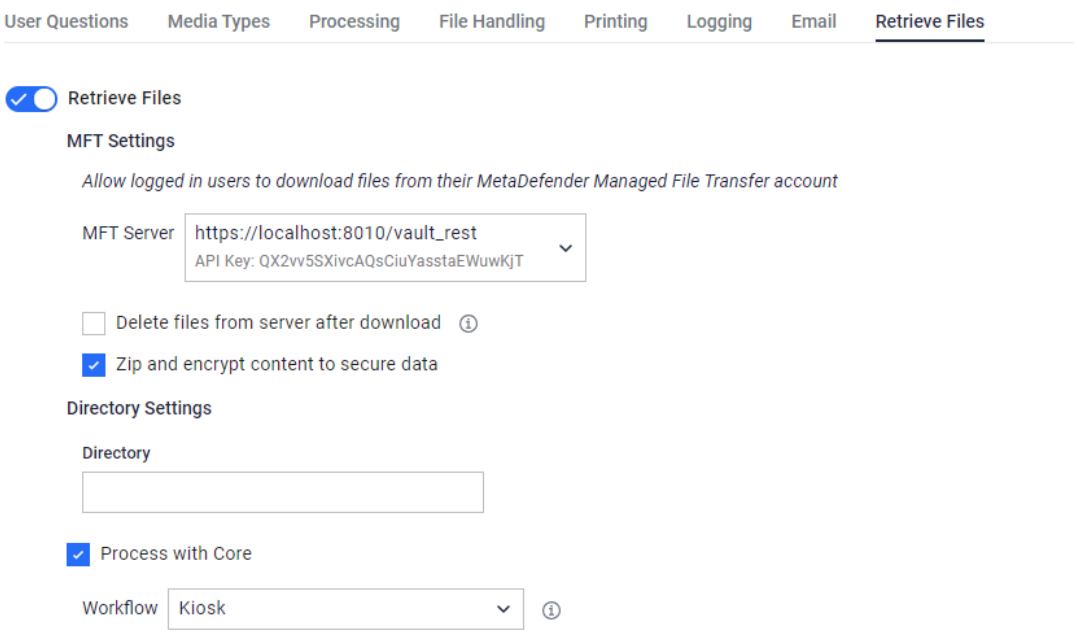
1. The maximum of size of an attachment is 25MB which is the limit for popular email sending providers and clients like Gmail, Outlook, SendGrid, etc. In case the session log is over 25MB, it is divided into approximately 25MB files where each file is sent in separate emails.
2. The image attached in email should be a low-resolution logo not exceeding 100KB and only one in the email
3. Multiple recipients are separated by semi-colon.
4. Identical recipients have to receive duplication emails.

Retrieve Files

The Retrieve Files page lets you allow users to download files from an outside source to the media connected to Kiosk. Supported sources are MFT and local or shared network directory.

Users from a Remote Active Directory (view *Enabling user authentication* in 8.3. Configuring Global Kiosk Settings) can retrieve files from all supported sources . Users logged in from Windows user login are not supported for file retrieval.

Guests are allowed to retrieve files from MFT only and are required to enter a MFT Owner ID to access files. See 9.9. Retrieving Files from an External Source



MFT

When an AD user logs in to a Kiosk session, the same login credentials will be used for accessing the user's account on MFT. When a Guest user has uploaded files to MFT server, a MFT owner ID for that session is generated at MFT and is used as an input for guest to retrieve files later. Refer to 6. Configuring with MFT to enable MFT server selection.

Info
It is recommended for both Kiosk and MFT to be connected to the same user directory in order for the integration to work seamlessly.

Warning
Retrieving files from MFT or directory via SSO is not yet supported.

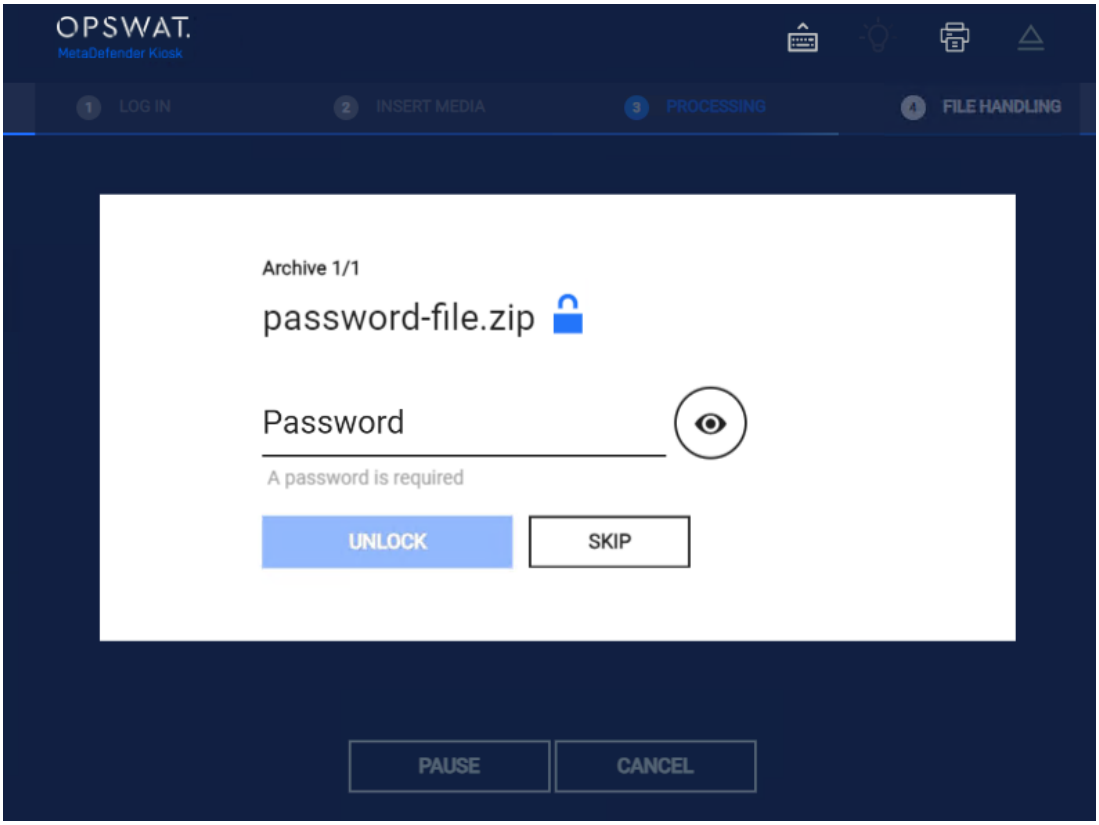
Delete files from server after download

With this enabled, files that are successfully downloaded will be marked for deletion on MFT. MFT's background worker will later proceed to delete the file.

Zip and encrypt content to secure data

With this enabled, files that are successfully downloaded from MFT will be compressed into a zip archive with password protection before copying to the media.

User will be required to enter the encryption password.



Notes

- Max length of the password is 100
- Special characters are not supported: " !"#$%&'()*+,-./:;<=>?@[]^_`{|}~"

Directory

Local directory or network share is supported. Guests cannot retrieve files from a directory.

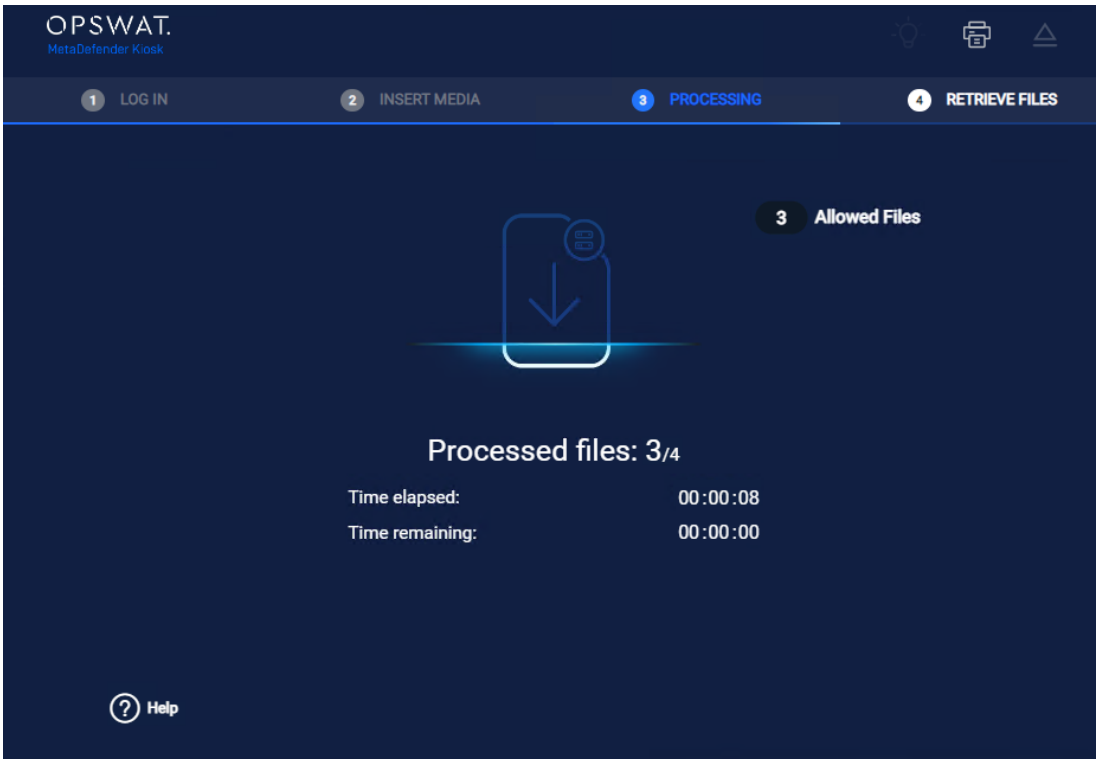
Variables can be used to create folder name or to map the home folder of the end users

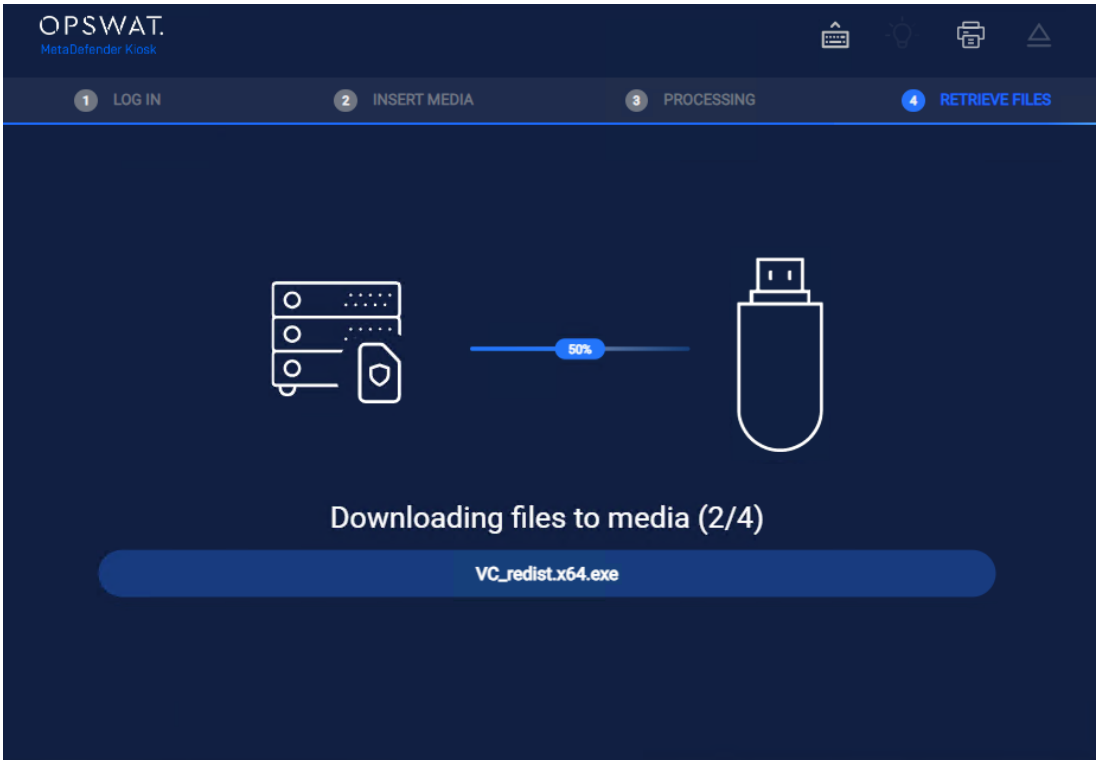
- The *%%%username%%%* variable is supported to map the user that is logged in to the Kiosk session to their own personal directory.
- Responses to user questions can also be utilized via the predefined '*%%%userresponse#%%%*' variable, where '#' is the number of the response to the corresponding user question.
    - For example, to utilize the answer to the question 2, the variable to use would be '*%%%userresponse2%%%*'. If no response to the question was given or no such question exists for the user response to exist (e.g. *%%%userresponse999%%%*), then the variable will exist in the path created. The user's credentials are used to access the directories contents, ensure security permissions are set accordingly.

Process with Core

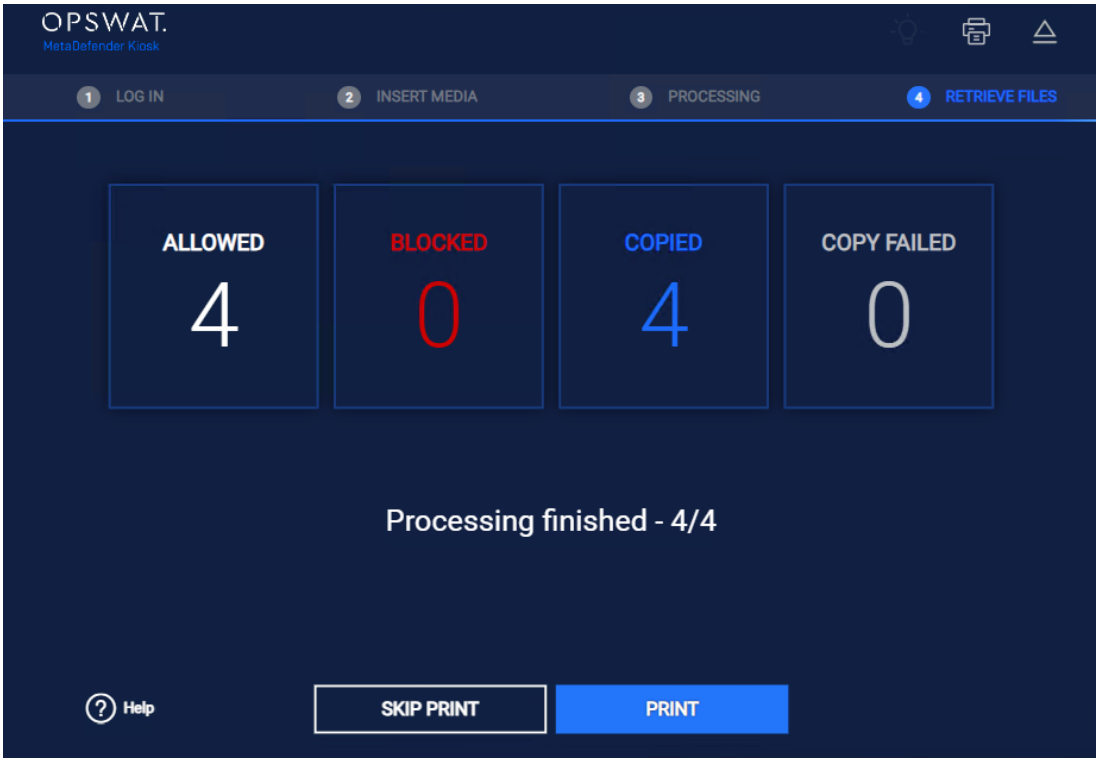
Files retrieved from a MFT or directory can be run through Core and the rule specified.

User can see the file scanning progress from Core





After the file scan is completed, a summary of scan result is displayed on the screen



If the file is allowed, it will be copied to the media inserted. If the file is modified by CDR or DLP, the remediated file will be downloaded to the media rather than the original file.

Using the Kiosk User Interface

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

The exact experience will depend on how each MetaDefender Kiosk instance is configured.

Launching MetaDefender Kiosk

Warning
Before v4.6.2, MetaDefender Kiosk accepted all of sensitive keystrokes including the combinations that could be abused to gain system control, even by using HID attack platforms. From 4.6.2 moving forwards, those sensitive and vulnerable-to-abuse keystrokes are disabled, and only re-anabled when KIOSK UI application is not running. Generally, only keystrokes really applicable on KIOSK input areas are allowed.

The MetaDefender Kiosk application automatically launches upon system startup. If there is a system malfunction and you restart the system, MetaDefender Kiosk re-initializes upon startup.

After startup, the idle screen is displayed:

If the MetaDefender Kiosk license is expired or invalid, the MetaDefender Kiosk application displays an error and does not allow usage:

Adjusting screen brightness

Users have the option to directly adjust screen brightness on the KIOSK UI, especially beneficial for setups in dimly lit surroundings or during low battery situations.

The KIOSK offers 5 levels of brightness adjustment. Simply click on the brightness icon to raise or lower the screen brightness.

Adjusting screen brightness on KIOSK UI

Limitations
For external monitor:

- The monitor should support DDC/CI (Command Interface) for proper brightness control.
- Brightness control may not work properly when connected to the monitor via a hub.

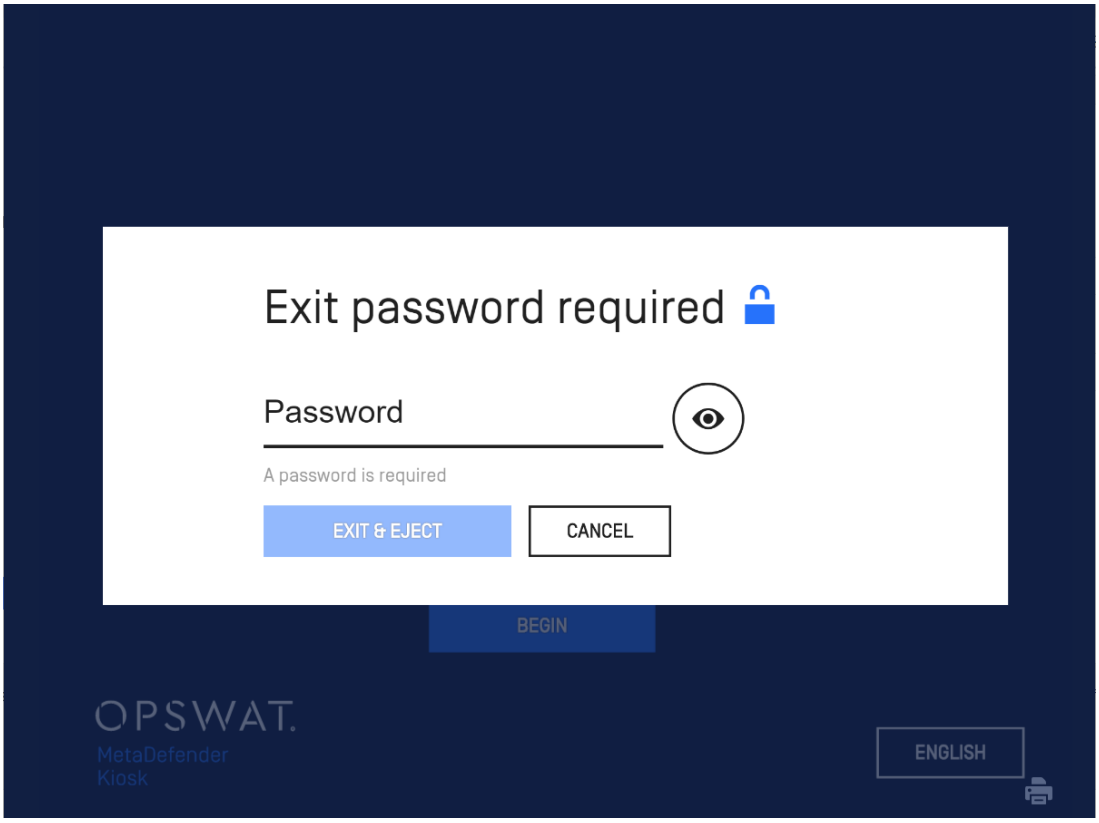
Exiting the User Interface

`Alt+S` is used to exit the UI.

When exiting the UI, it may take a few minutes if Kiosk is in the middle of processing media. It is not recommended to exit the UI while Kiosk is processing media.

It is strongly suggested to set Exit Credentials (either a password or AD administrator credentials) in order to prevent users from accessing the underlying system. If the Kiosk software is experiencing any malfunction, the UI will not be able to exit and close. The system administrator will have to have to reboot the machine and diagnose the services' operation in Safe Mode.

When the exit password is configured



Logging In on the User Authentication Screen

When the Guest group and Employee group enabled, Kiosk users must login either as a Guest or an Employee user account. When either is disabled, the selection of login type is unnecessary.

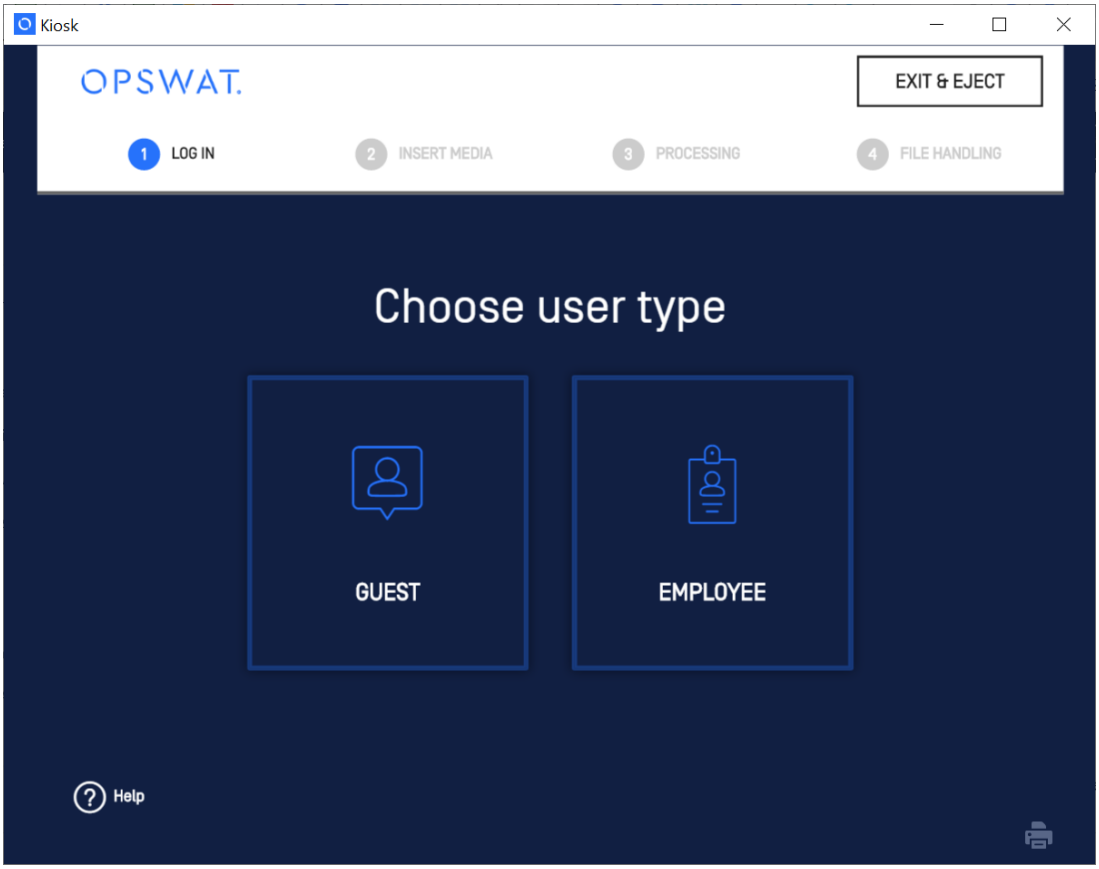


Image: "Choose user type" screen on Kiosk UI

When Kiosk users log in with an Employee account, the Login screen is displayed for the users to enter their credentials. Active Directory with nested group is supported for user credentials

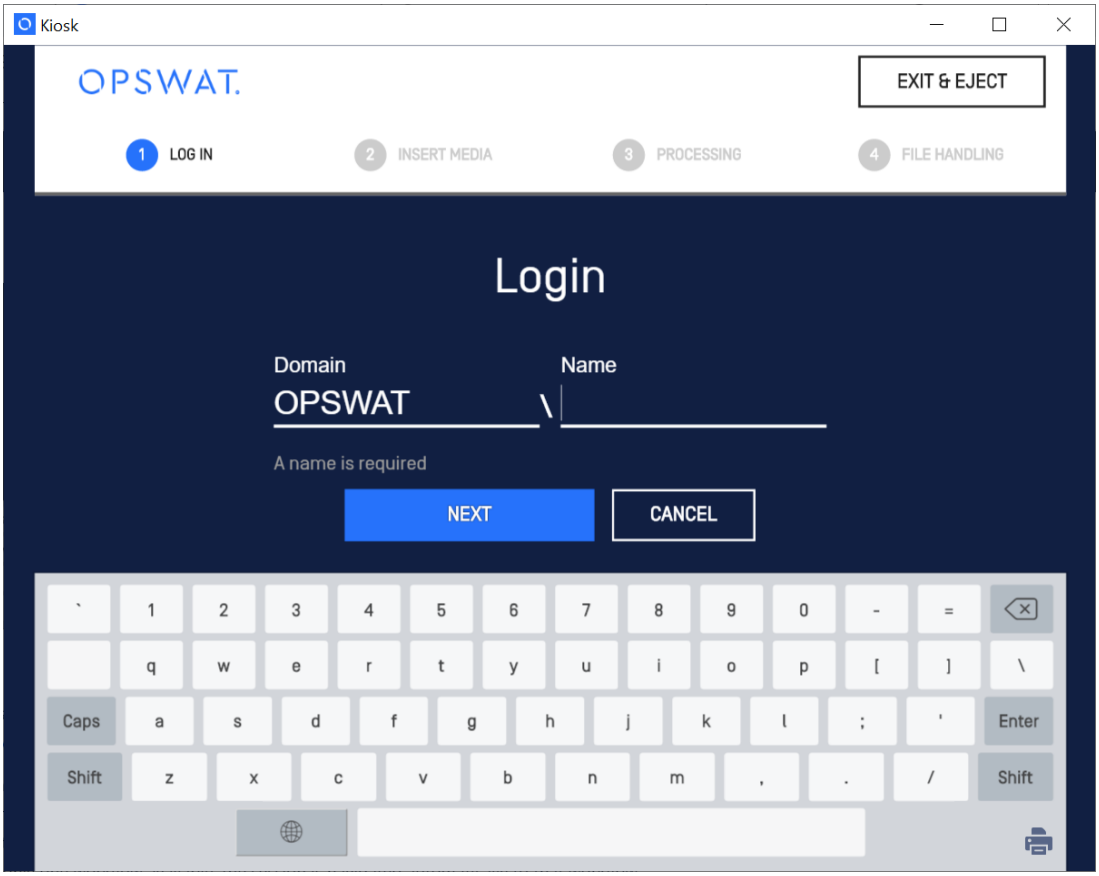


Image: Kiosk Login session on Kiosk UI

When Single Sign-On (SSO) is set as default login method for Employee to authenticate, Kiosk will display `Sign In` screen of the configured SSO for user to to enter their credentials.

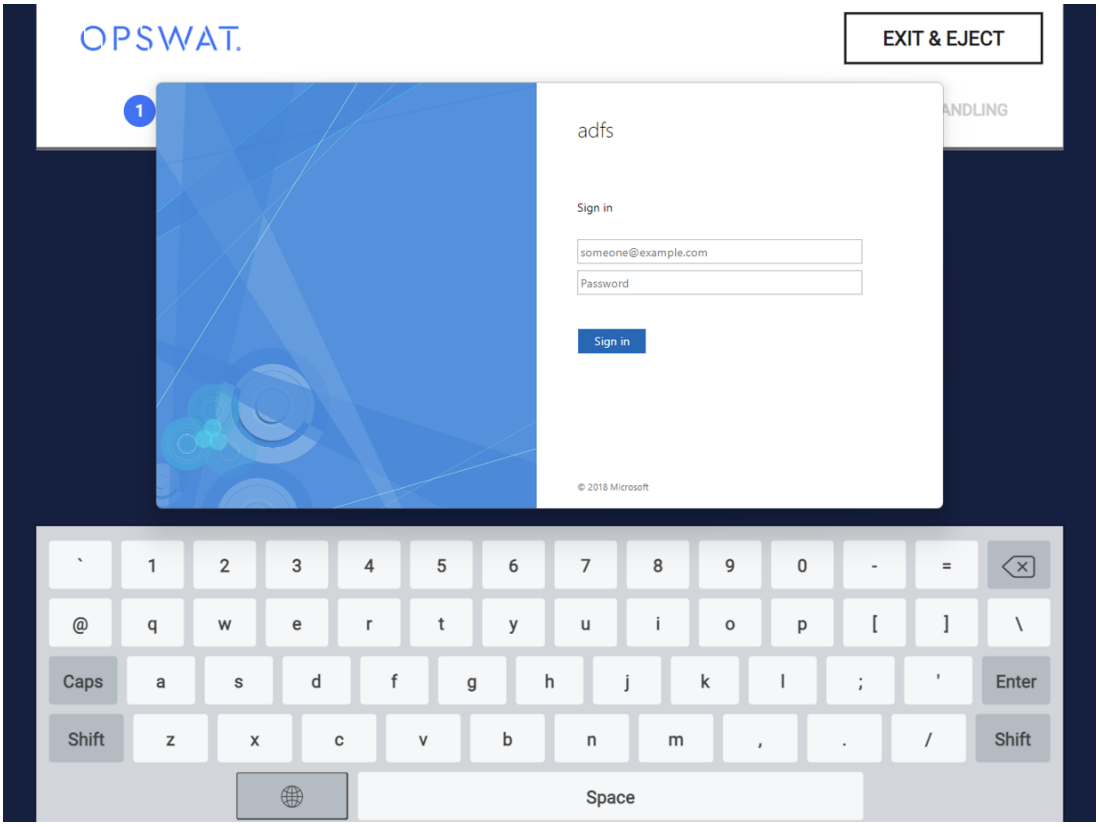


Image: SSO screen appeared after login session on Kiosk UI

When Kiosk users log in as Guest, they don't have to provide any credential.

After logging in with either your Windows credentials or as a Guest, your workflow is determined by the workflow settings configured in the MetaDefender Kiosk Management Console. If there are multiple workflows available for the logged in user (Employee or Guest), the user must select which workflow to proceed with. In case there is only one workflow available, the session is navigated automatically across that workflow.

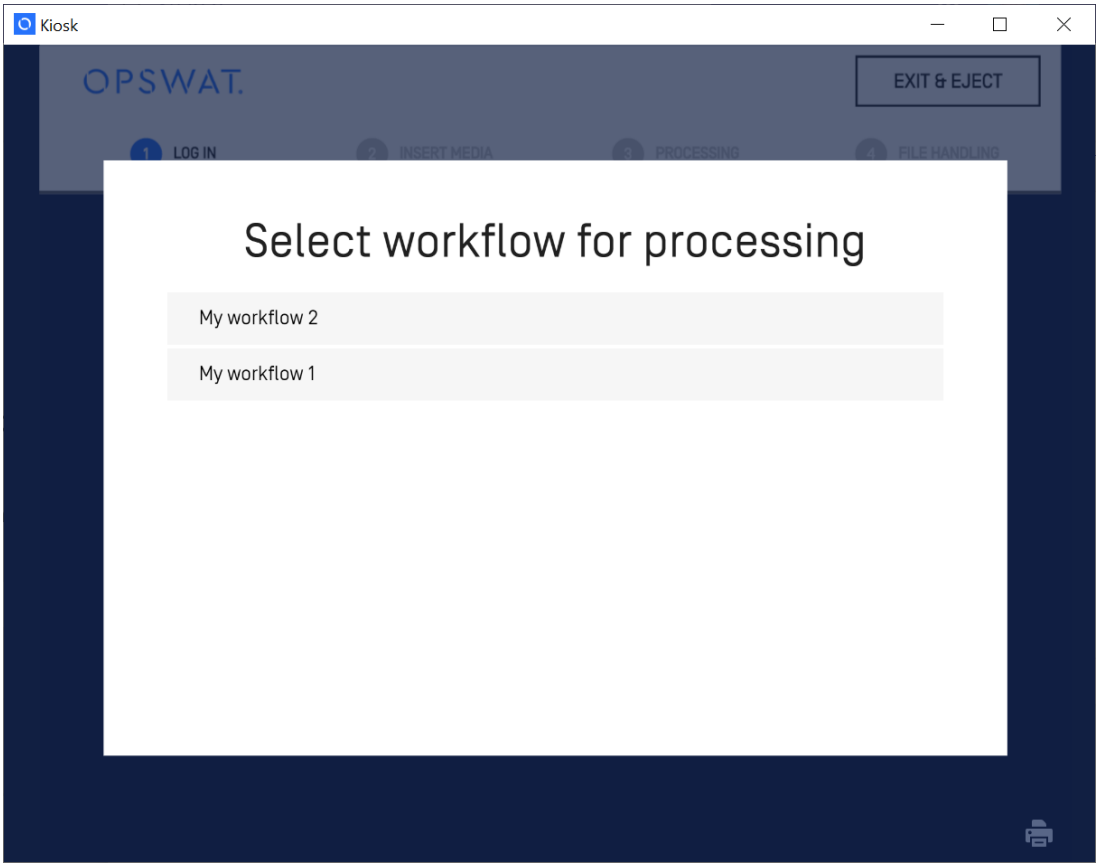


Image: "Select workflow for processing" tab for employees on Kiosk Ui

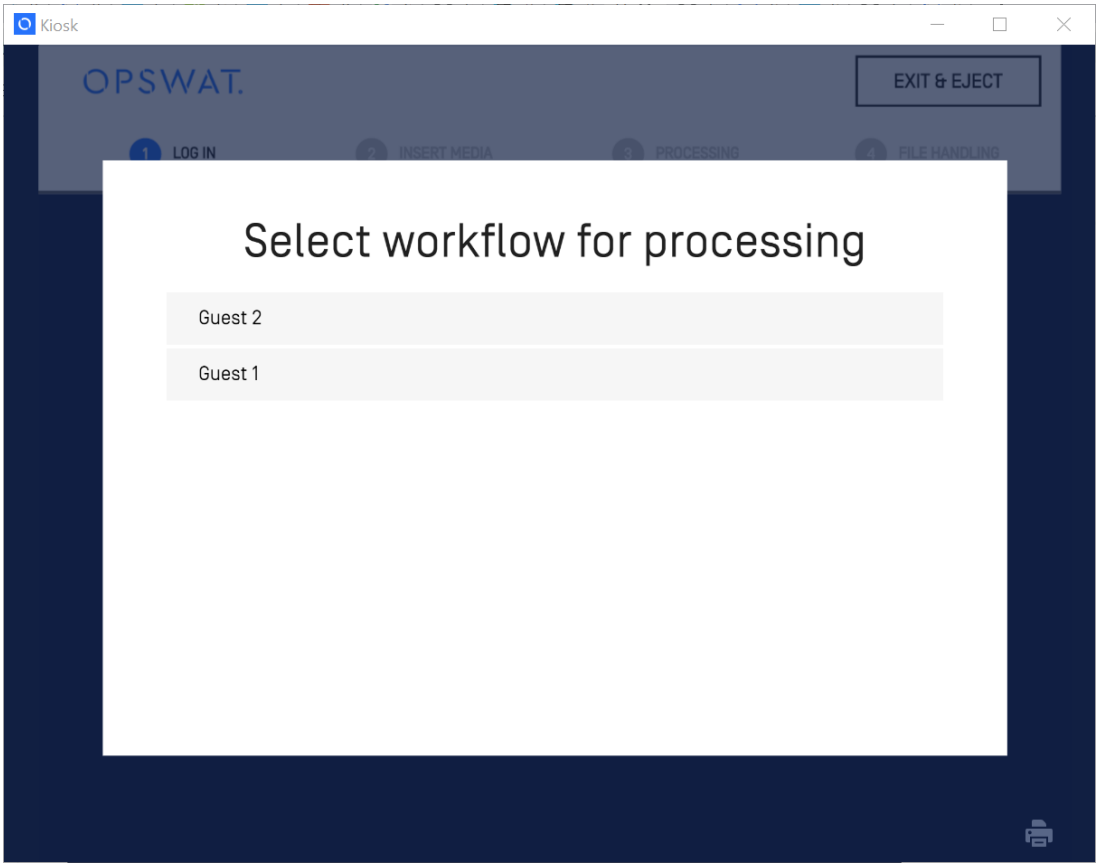
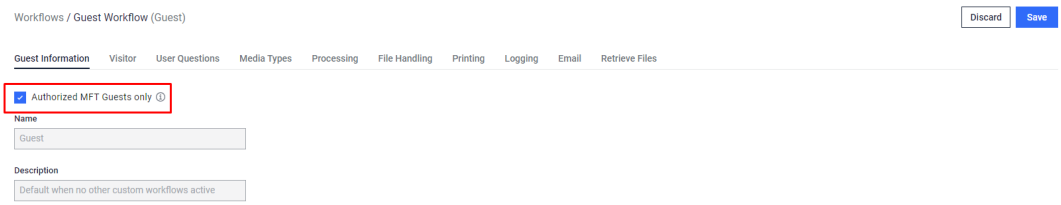


Image: "Select workflow for processing" tab for Guest on Kiosk Ui

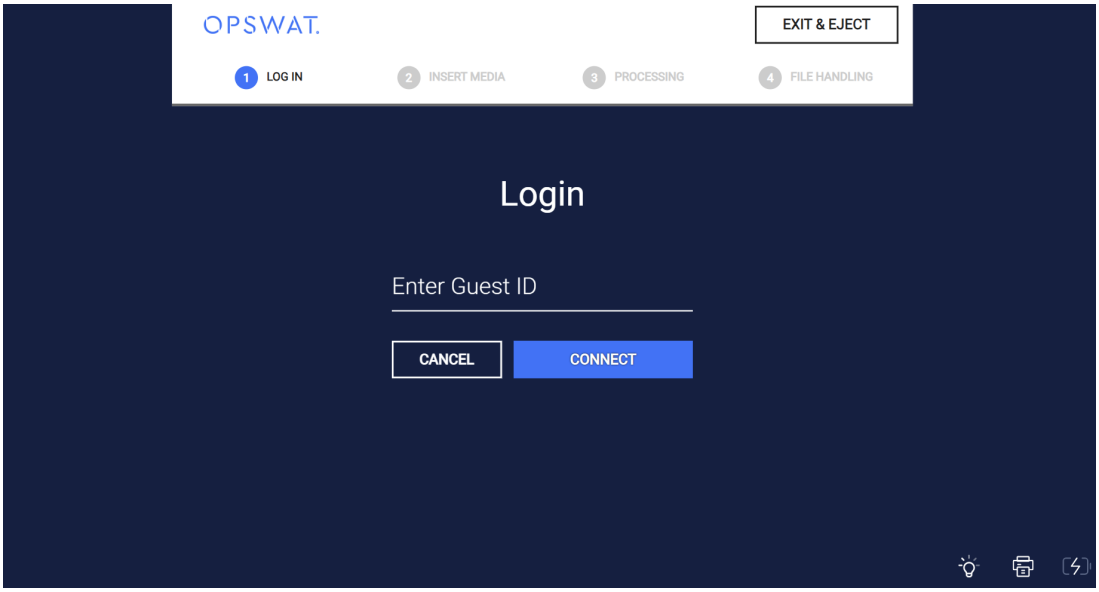
For more information on configuring multiple workflows, see the Workflows Page.

Authorizing MFT Guest ID

If the administrator has activated the "**Authorized MFT Guests only**" option for the Guest Workflow to manage these Guest IDs manually instead of depending on automatic generation by the KIOSK, the user utilizing that guest workflow will need to input the provided MFT Guest ID to initiate the session.



Authorized MFT Guests only option on WebMC



Guest user is required to enter the provided MFT Guest ID

The Guest ID should consist of 6 to 255 characters. Upon clicking the **CONNECT** button, the KIOSK will verify the existence of the Guest ID in the configured MFT to initiate the session.

The verified Guest ID will facilitate to retrieve files or copy files to the corresponding guest account on the MFT server.

Answering User Questions

User questions are displayed If your workflow profile (either as a guest or domain user) specifies user questions. **Previous** and **Next** allow to traverse between questions. Answer the questions and then click **Submit** .

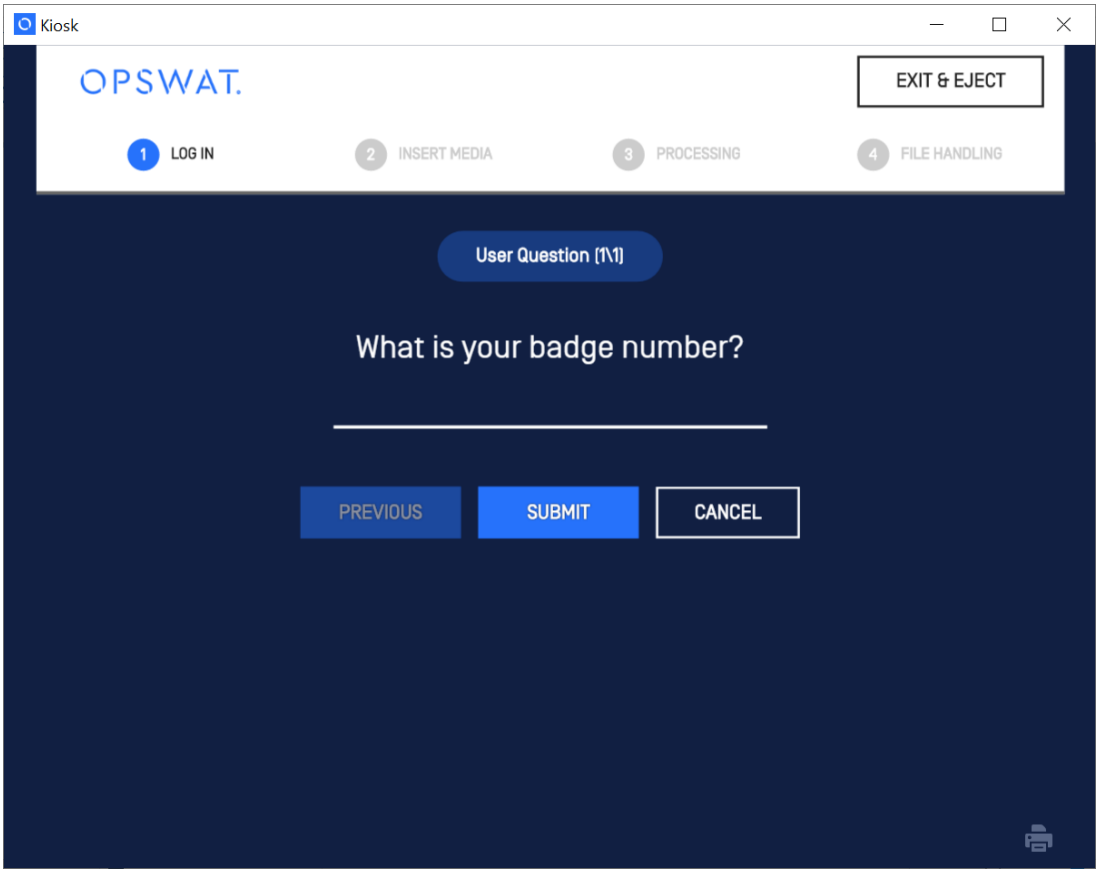
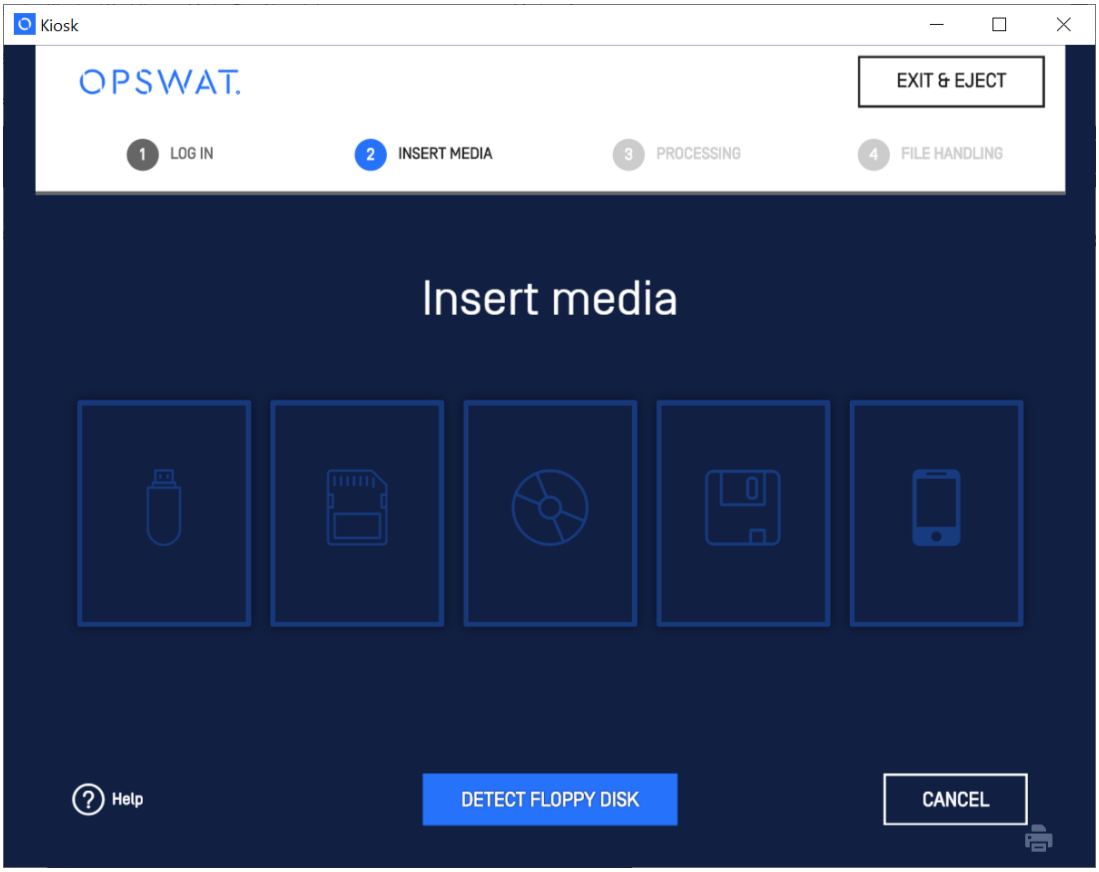


Image: "Specific user question" session on Kiosk UI

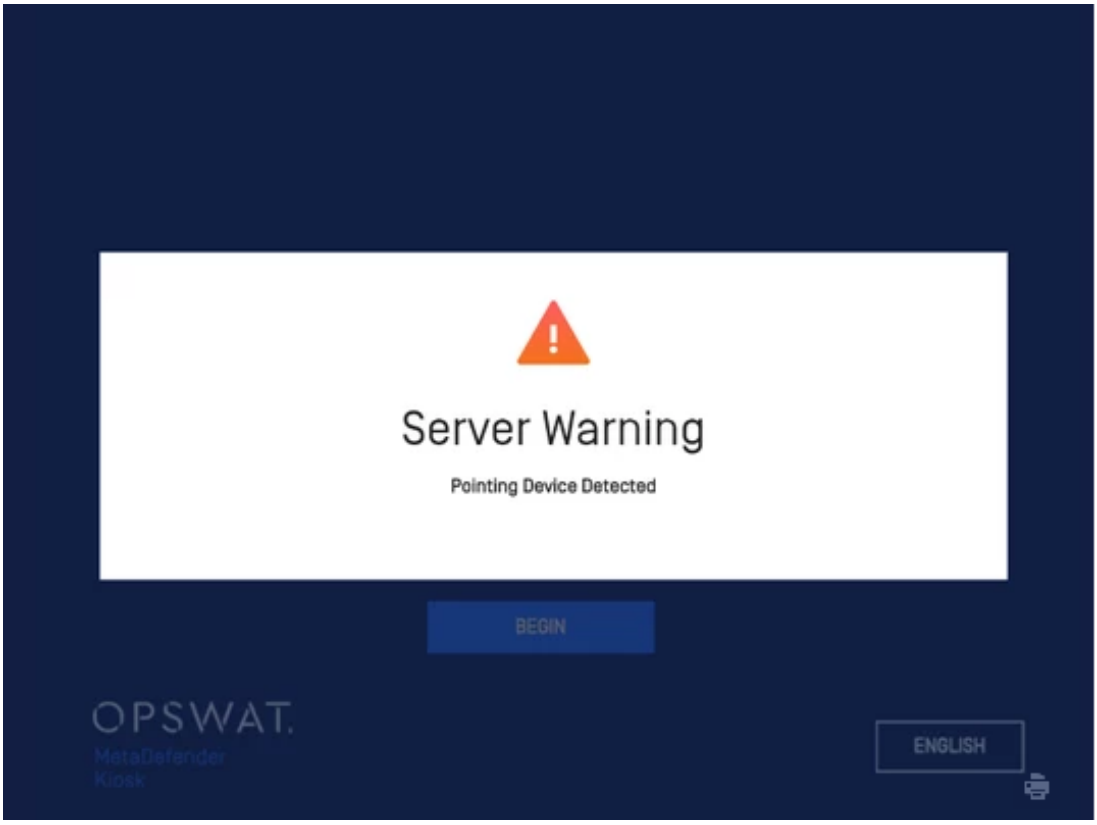
Inserting Digital Media

After the login process is complete and, if applicable, all user questions have been submitted, the Insert Media screen displays.



At any point during a session, if a device is inserted that Kiosk cannot process, an alert will pop up indicating it detected a new device.

For example, in the event a mouse is connected:


Server Warning
Pointing Device Detected
BEGIN
OPSWAT.
MetaDefender
Kiosk
ENGLISH

Unlocking Encrypted Devices

If the device you are trying to scan is encrypted, a prompt to unlock the device is displayed. See the Overview for a list of encrypted USB drives that are supported.

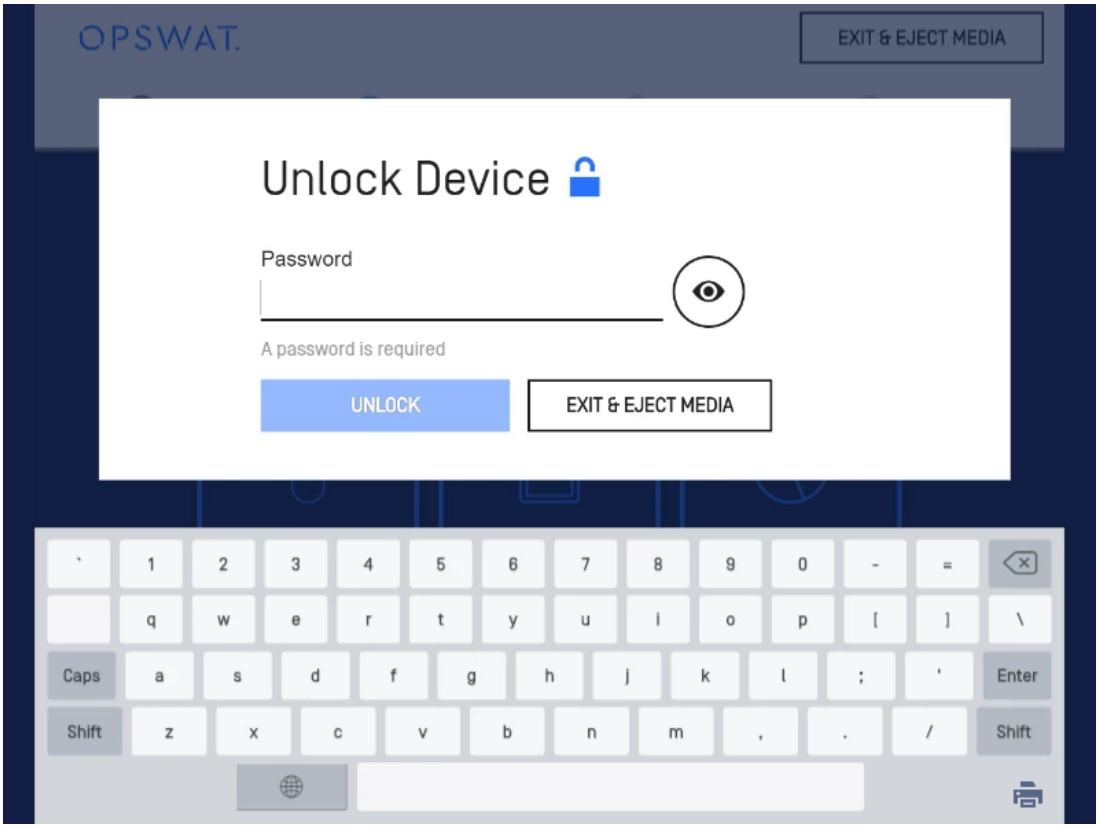


Image: "Unlock Device" option for encrypted removable media

Kiosk allows users to retry to unlock the device in case of wrong password or other failure. The number of retry times is not limited. Carefully input the correct password to avoid data loss or device damage.

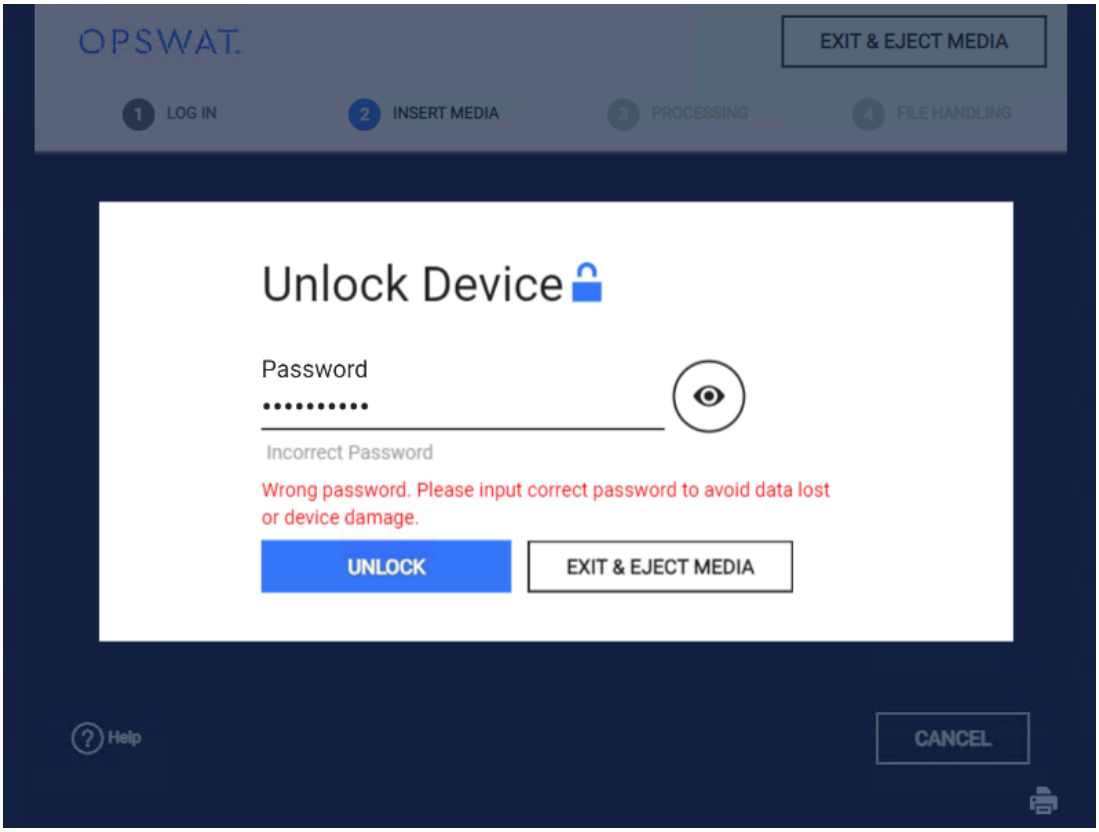


Image: User can retry to fill out wrong password on Kió·

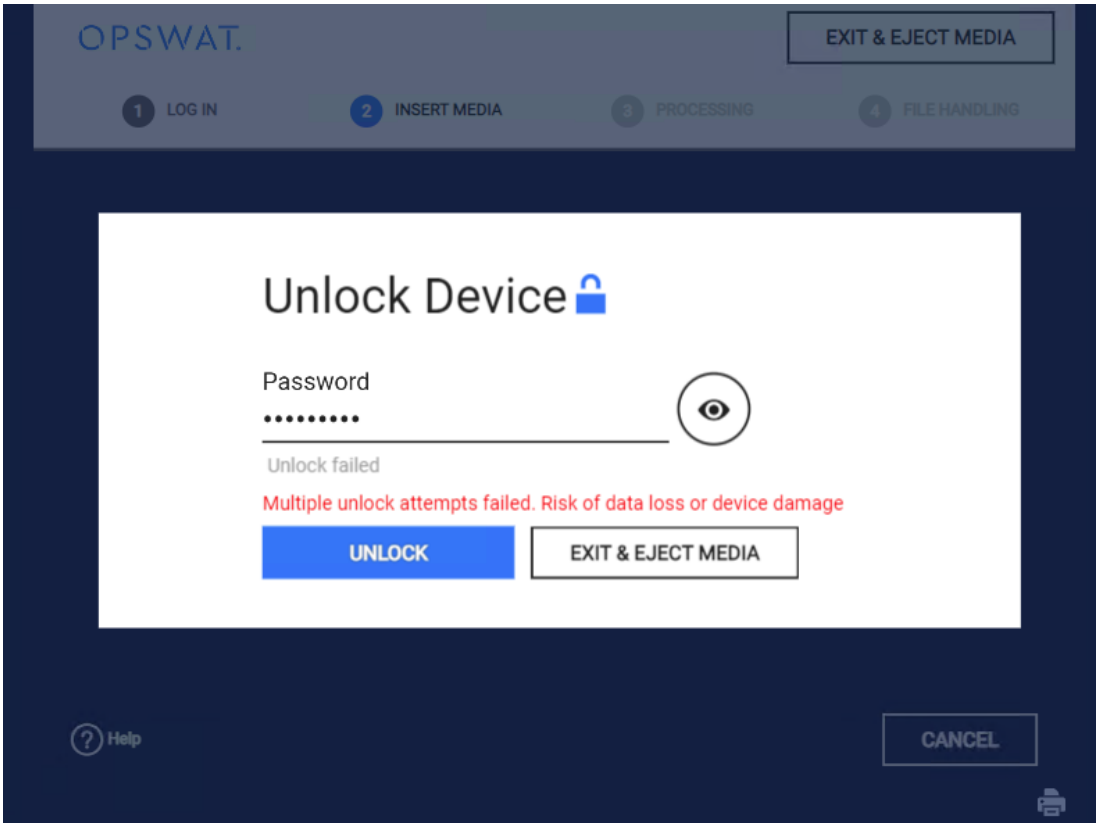
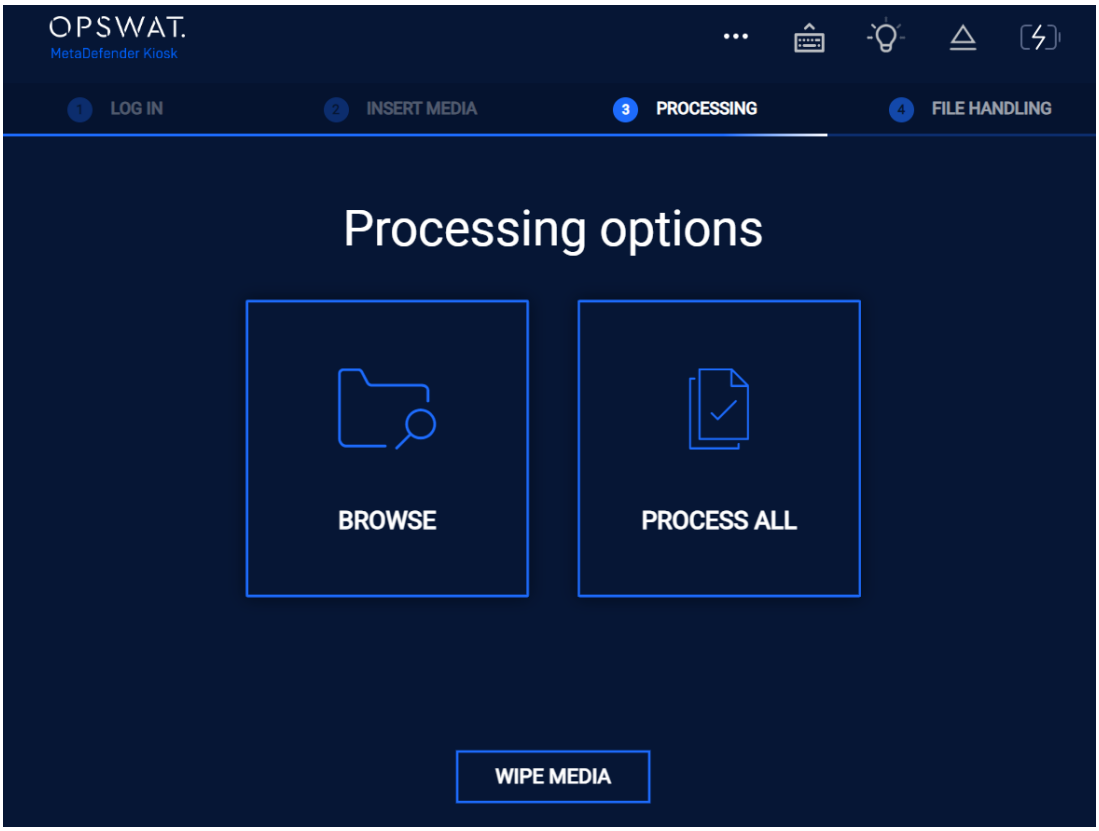


Image: After input wrong password many times, the warning text will be appeared on Kiosk UI to prevent user damage the device

Processing Digital Media

1. Insert the media you want to proceed. The "Processing options" screen will appear on Kiosk UI.
2. Click **Browse** . (If you want to proceed the entire media, click **Process All** and skip to step 5) All detected removable media devices will be displayed.

Note: Click **Wipe Media** to remove all data from the detected media and overwrite the entire disk with random data, it will depends on the configuration settings in the MetaDefender Kiosk Management Console.



3. Select the drive, folders, or files (including system files) you want to scan and click **Continue**. Files are displayed on pages for directories with a large amount of files and can be navigated via the Previous Page and Next Page buttons.

Remark: Boot Sector in the figure below are the Master Boot Record and Volume Boot Record; they will be proceeded when user click into that option on Kiosk UI.

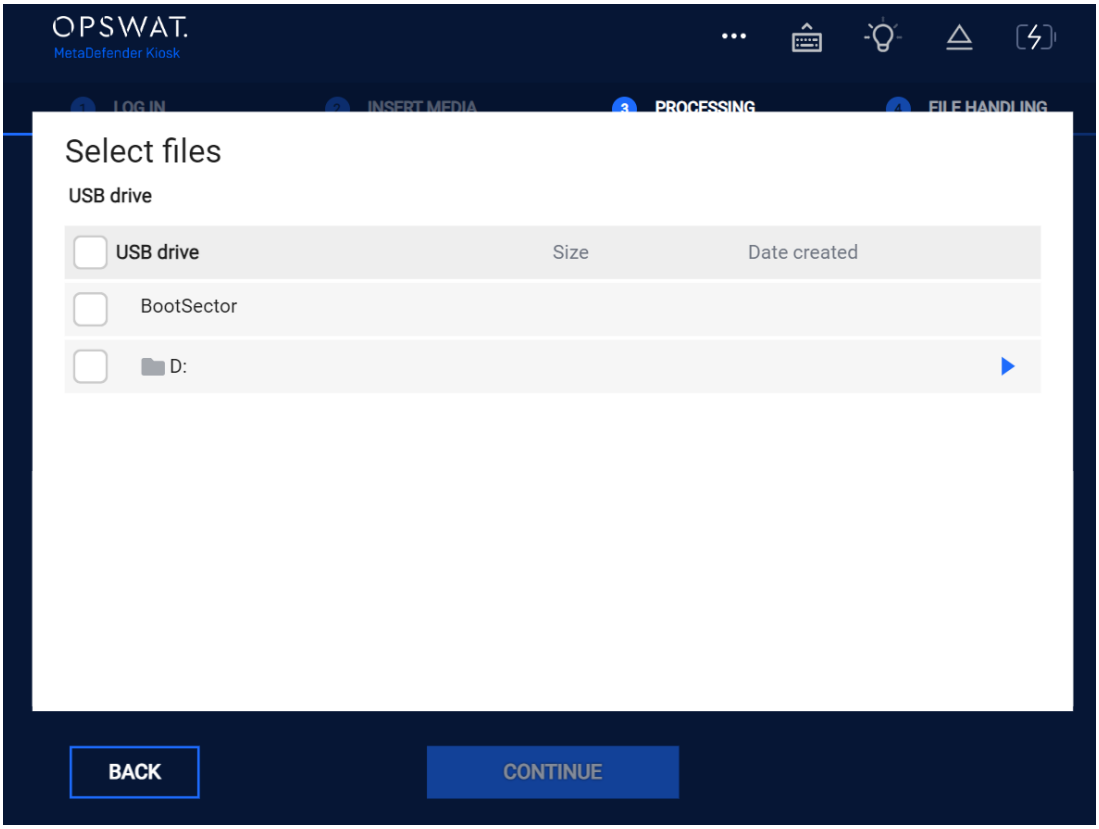
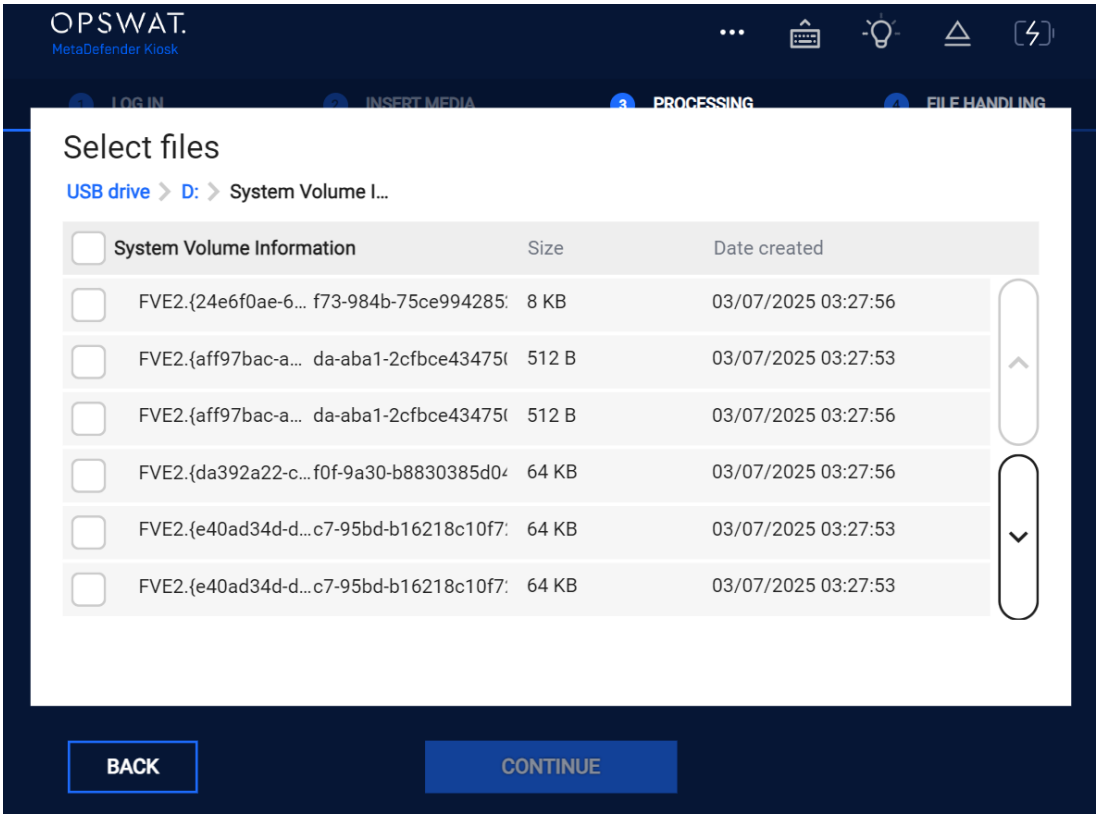


Image: "Boot Sector" option on Kiosk UI



Note: If the Size Summary is set, users can observe the total size of selected files and folders.

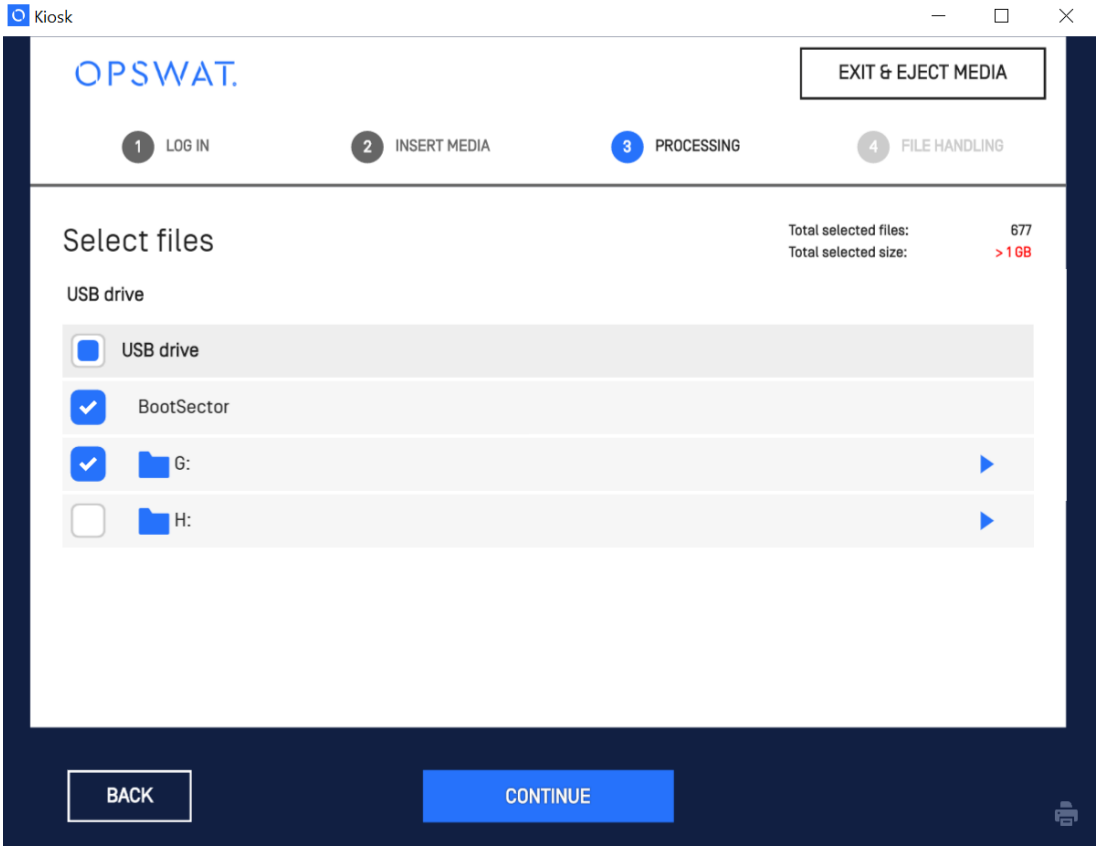


Image: Total selected files and size on Kiosk UI (on the top right corner)

4. The "Processing files" on Kiosk UI displays following information:
    a. How many files scanned by the Kiosk (e.g. allowed files, blocked files, skipped files)
    b. Scanning duration: demonstrated by percentage number on USB icon, when the scanning is completed, the percentage number will be 100%.
    c. The number of files of processed out of the total number files to be processed
    d. Total elapsed time when scanning the files.
    e. Total remaining time requirement for Kiosk to scan all the selected data and files on Kiosk.

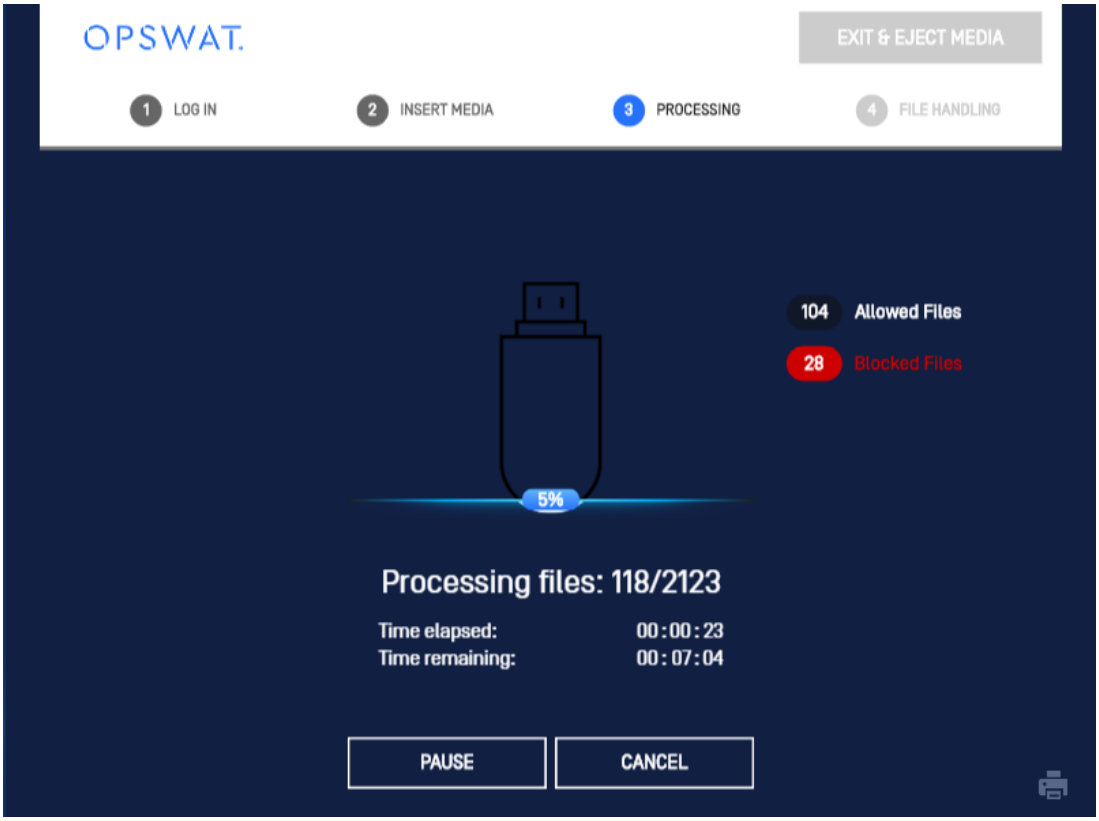


Image: "Processing files" display concept on Kiosk UI

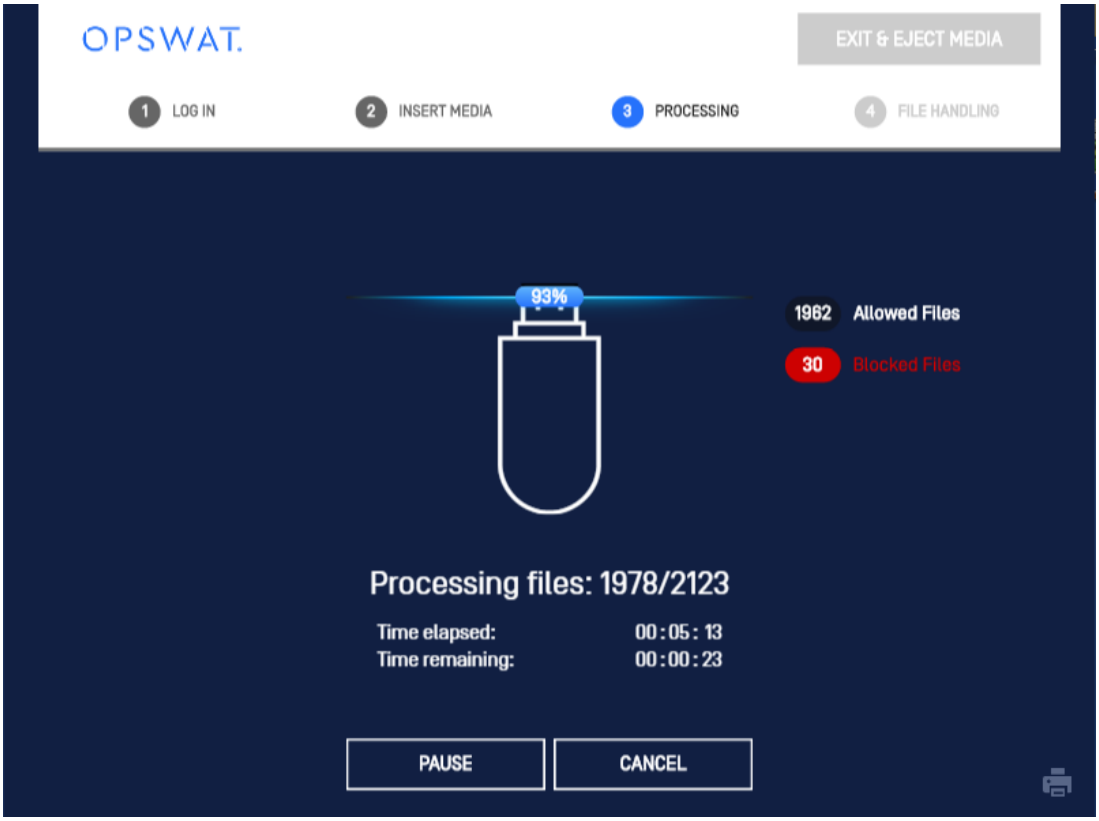


Image: "Processing files" display concept on Kiosk UI

Note: If the inserted media does not have Windows-readable partitions, or if multiple partitions have been disabled in the MetaDefender Kiosk Management Console and the drive has multiple partitions, the **No volumes mounted for the selected device** error message appears and you will be returned to the Idle screen. This error message also appears if MetaDefender Kiosk is unable to read a partition because it is a private or encrypted partition.

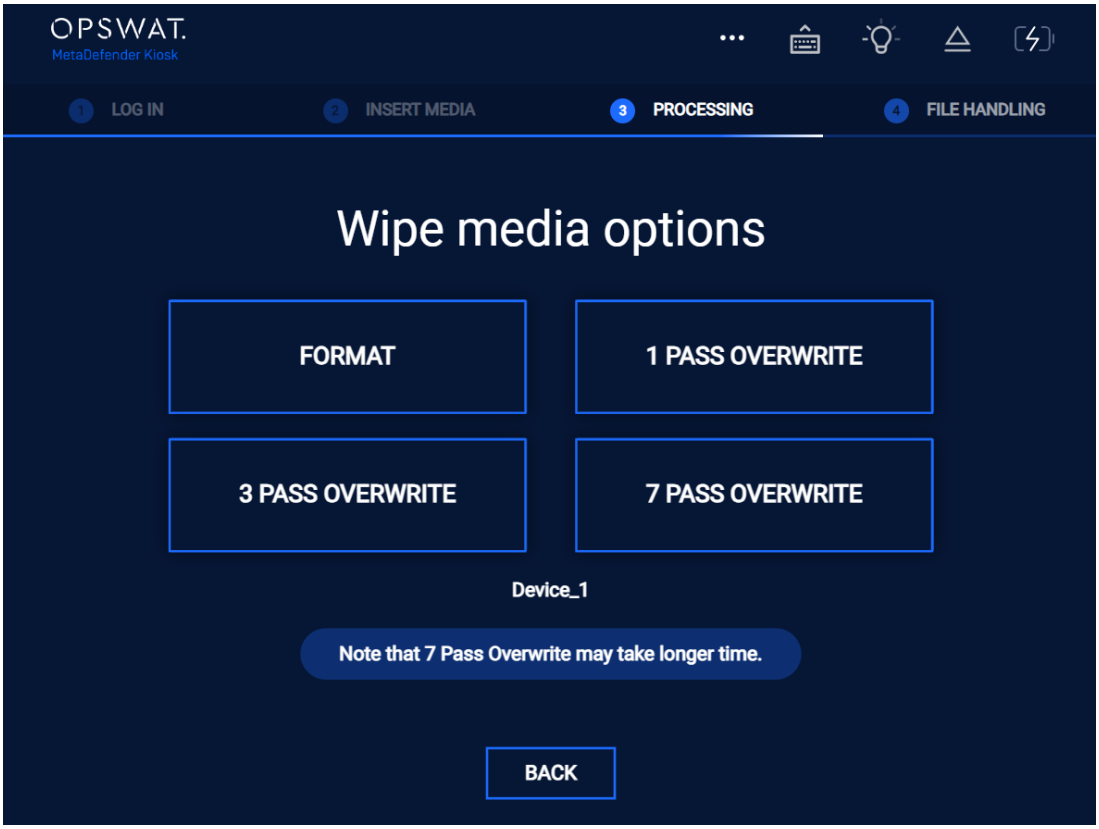
5. If at least one encrypted archive is found and encrypted archive decryption is enabled in the MetaDefender Kiosk Management Console, a list of the encrypted files is displayed. See 9.5. Processing Encrypted Archives for additional information.
6. When the scanning process is complete, the Sessions Results screen will be displayed. See 9.6. Viewing the Session Results.

Note: If you click **Cancel** during scanning process, the Session Results screen will be displayed. If media is removed during scanning, the session will end and return to the idle screen.

Wiping Media

Media can be wiped to delete all files on the device and the data hardly recovered even using specialized tools that can read the remnants of files that were previously on the disk.

Multiple removable media devices can be inserted at the wipe option selection screen, after that the wipe selection will be applied to all the removable media device plugged in. Detailed index of the devices will be displayed under each option.



There are four options:

- Format
- 1 Pass Overwrite
- 3 Pass Overwite
- 7 Pass Overwrite

Format is the fastest option, but it simply removes the references to the files on the drive without overwriting those portions of the drive. The 1, 3, and 7 pass wipe options write over the entire drive with differing algorithms, making it much more difficult to retrieve the data that was originally stored on the drive. The United States Department of Defense (DoD) recommends using a 7 pass wipe to clean media. OPSWAT does a low-level sector by sector wipe of the media.

Using the wipe feature will completely erase and reformat ALL information on the device. This includes the partition table and master boot record along with any file system information.

Algorithm Details

Num. of Passes	Algorithm Steps in Order	Security Standard
1	1. Pseudorandom	• British HMG Infosec Standard 5, Baseline Standard • Australian Government ICT Security Manual 2014 - Controls
3	1. All 1's 2. All 0's 3. Pseudorandom	• U.S. DoD Unclassified Computer Hard Drive Disposition* • U.S. Air Force System Security Instruction 5020** • U.S. Navy Staff Office Publication NAVSO P-5239-26 • British HMG Infosec Standard 5, Enhanced Standard _We use pseudorandom instead of a fixed pattern as our final pass *_We select 0xFF and 0x00 (reverse of standard), then pseudorandom data instead of a fixed character for our final pass
7	1. All 1's 2. All 0's 3. Pseudorandom 4. Pseudorandom 5. Pseudorandom 6. Pseudorandom 7. Pseudorandom	• Bruce Schneier's Algorithm: Applied Cryptography, ISBN 0-471-12845-7

Wiping will occur among each media one-by-one with the final results displayed at the end.

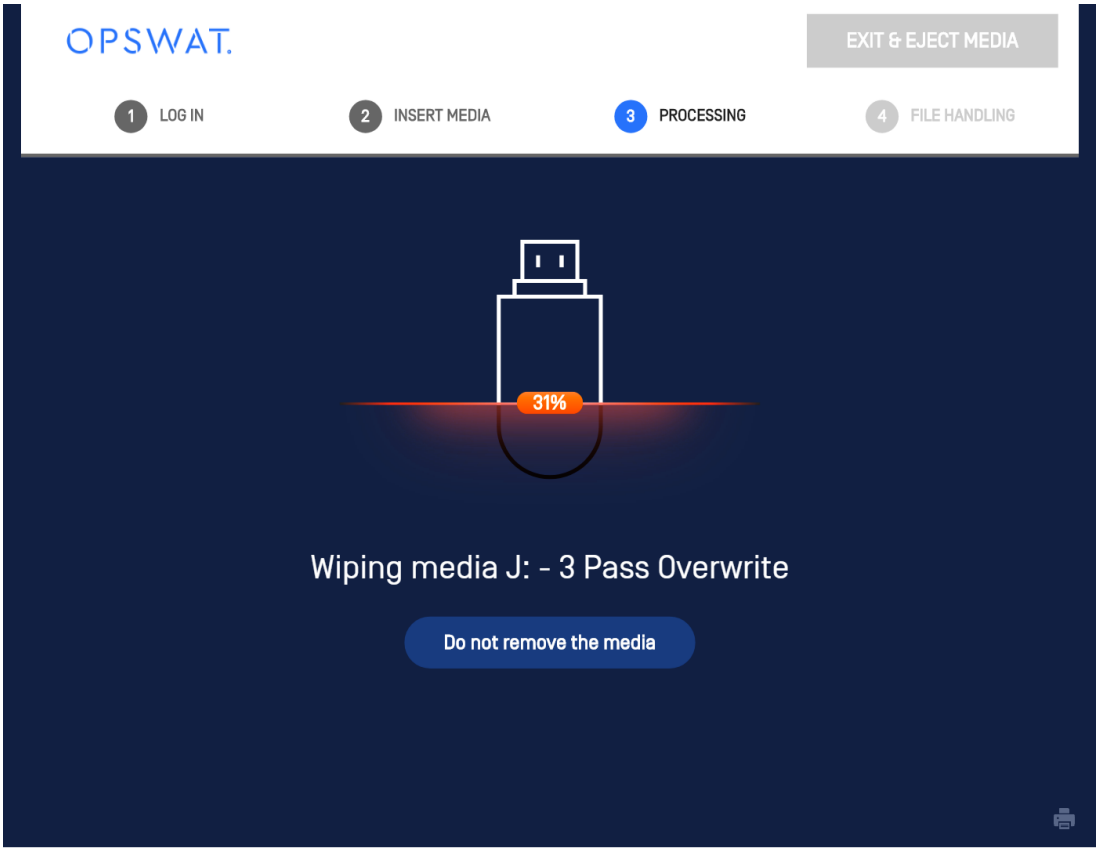
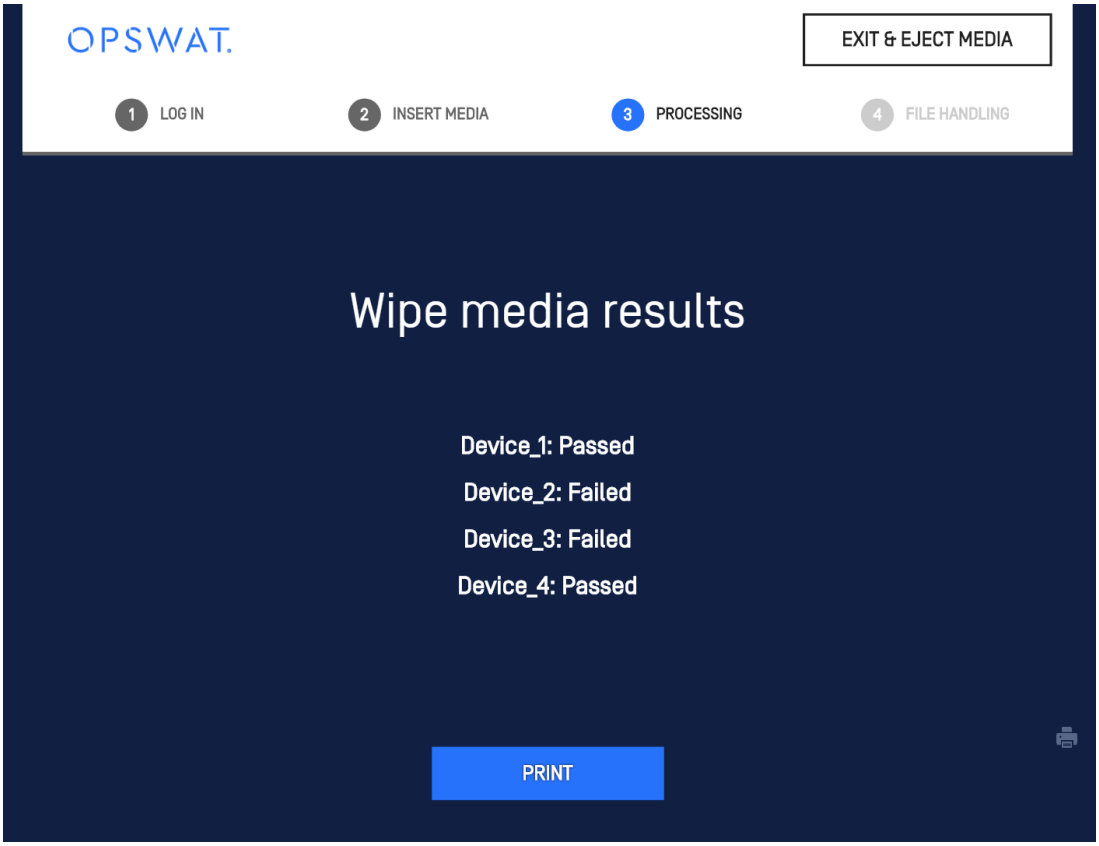


Image: Wiping media on 1 removable media device using "3 Pass Overwrite" option

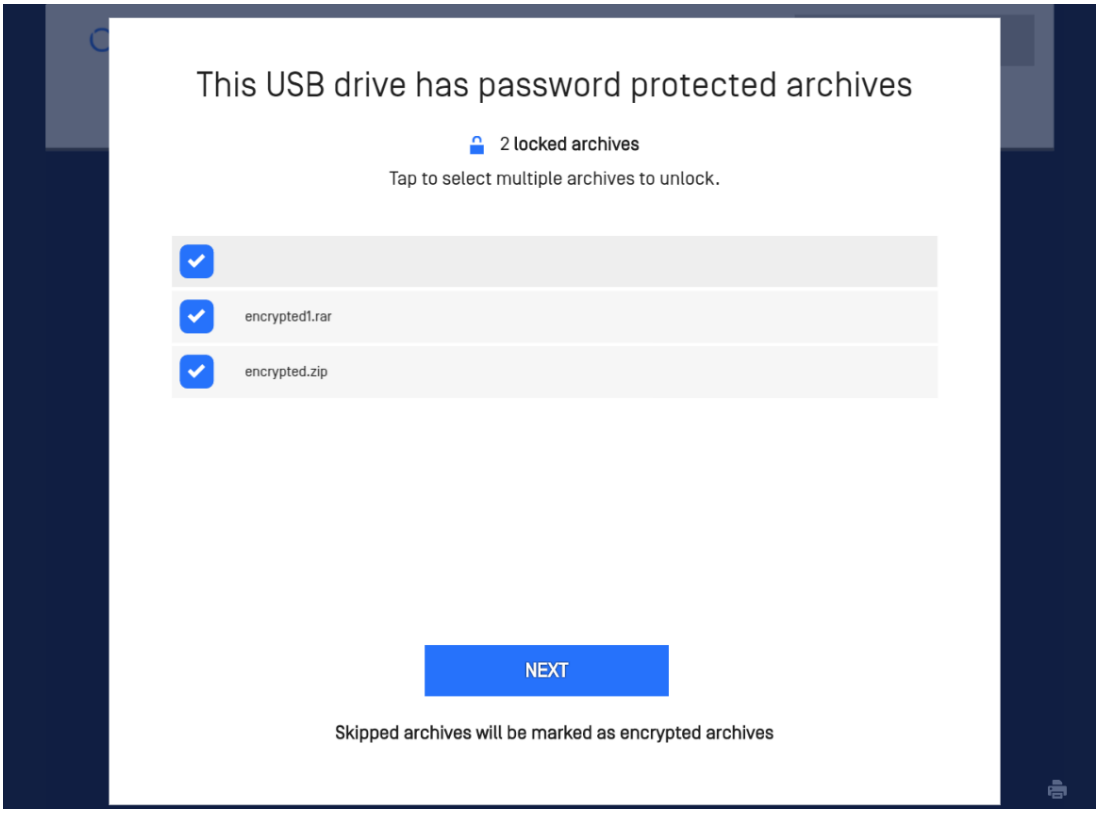


Image" Wipe media results on Kiosk UI

Info
The wiping of CD/DVD is not supported by Kiosk, `Wipe Media` button is not available with this media type.

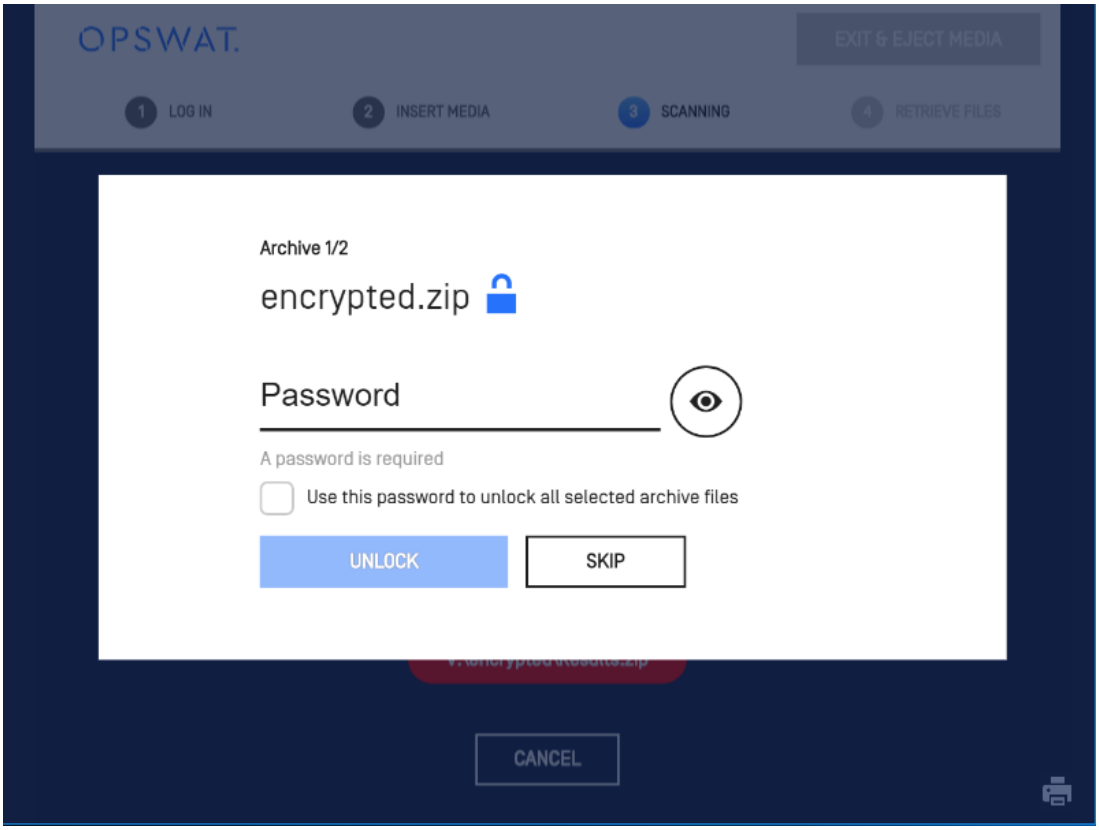
Processing Encrypted Archives

If at least one encrypted archive is found during processing (as described in 9.4. Processing Digital Media) and encrypted archive decryption is enabled, a list of the encrypted files encountered is presented.



To process encrypted archives:

1. Select the checkbox next to one or more of the encrypted archives. A password screen will appear:



2. Enter the password for the encrypted archive and then click **Submit** .

Note: If you selected multiple encrypted archives, you are prompted to enter different passwords for each archive or select to apply the same password to all archives. **Note:** Kiosk tries each password for all archives until it can extract it or failed, so a wrong password for an archive A might be a correct one for archive B, as a result the archive B might not be asked again for password.

3. Click **Unlock** to scan the selected encrypted archives . If the encrypted archives are successfully unlocked, the Session Results appear.

Note: Click **Skip** to bypass the encrypted archives and go directly to the Session Results screen.

4. If another encrypted archive is found within a previous archive, the user will be re-prompted to enter a password until a successful unlock or skip is chosen.

Processing Disk Image Files

The Kiosk functionality enables comprehensive deep scanning of disk image files by seamlessly mounting and scanning all nested files within, ensuring thorough analysis even in the presence of multiple layers of disk image files.

Supported disk image file types

- Virtual Hard Disks (.VHD or .VHDX)
- Virtual Machines (.VMDK)
- Arcronis Disk backups (.TIB or .TIBX)

Configuration to scan disk image files

See Disk Image Files for more detail to configure scanning for each type of disk image file.

The scanning flow

1. User select the disk image files to scan

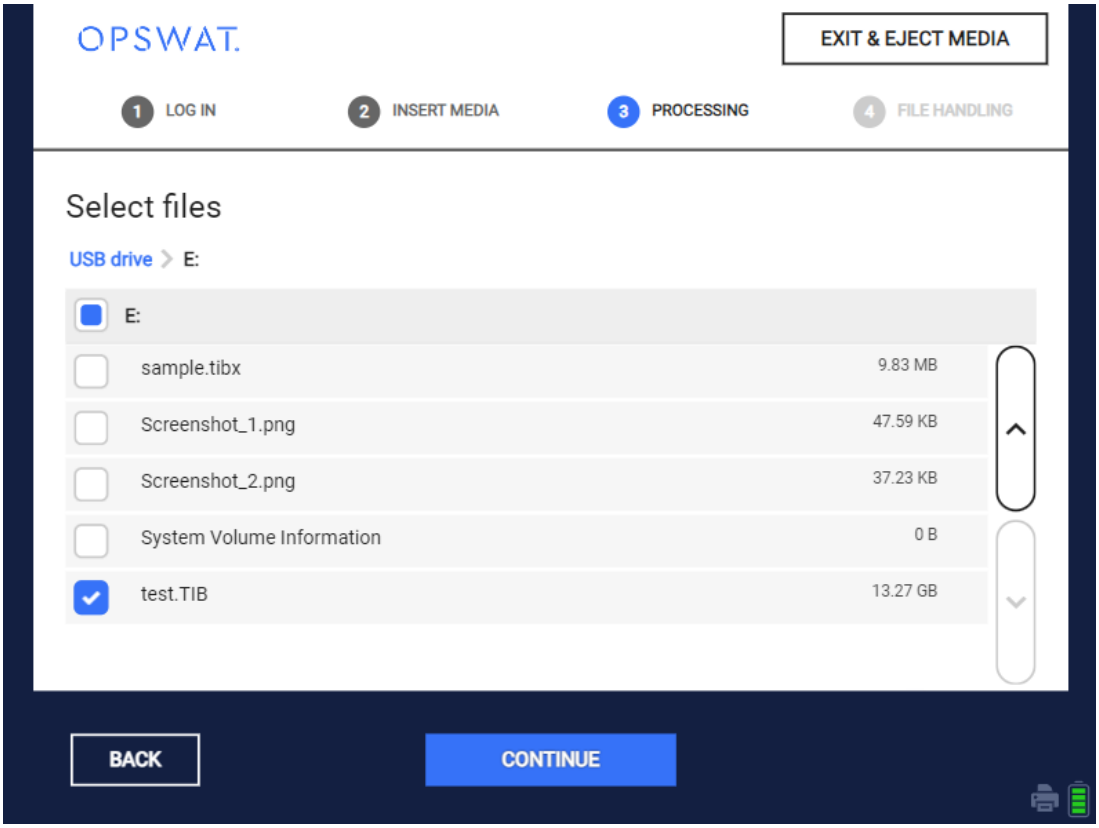


Image: User selects disk image file to scan

2. Kiosk prepares for scanning

Kiosk will mount and enumerate all child files to scan.

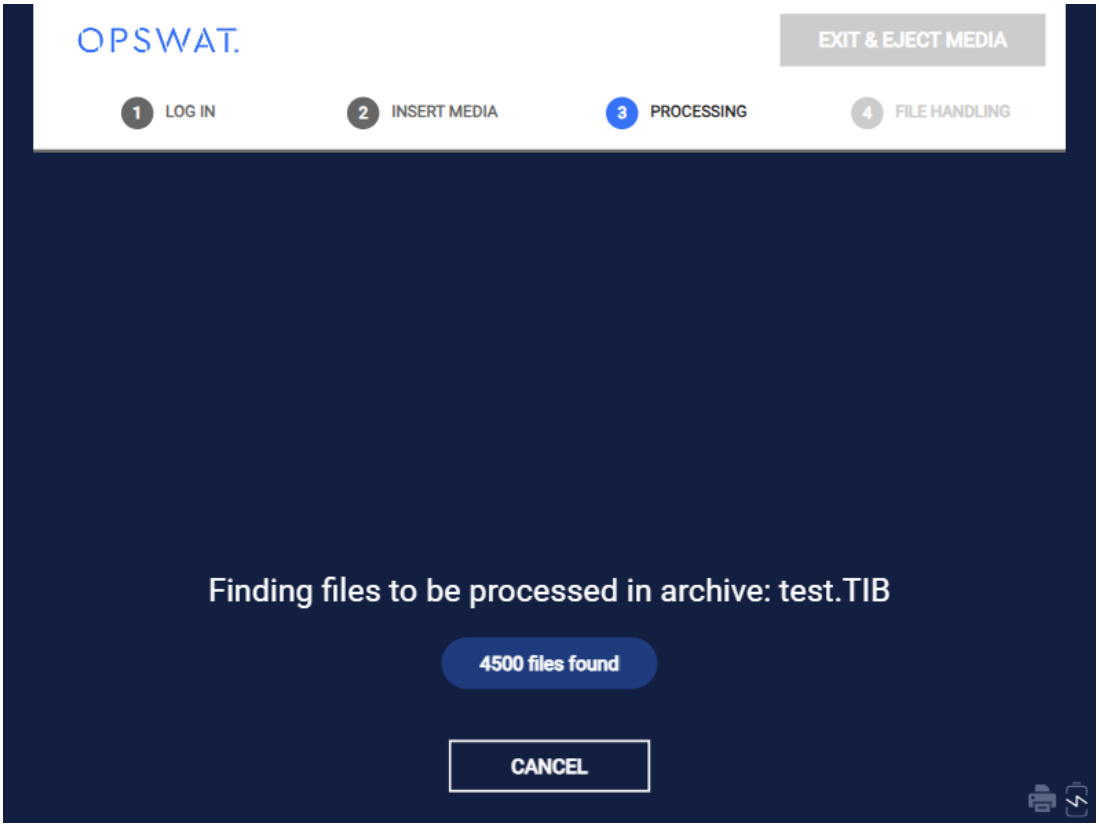


Image: Kiosk is mounting and enumerating files inside the TIB file

For any nested disk image files inside the selected one, Kiosk will mount and scan all of them according to option mounting and scanning corresponding to that types of disk image.

For example, If the `test.TIB` contains the `A.vhd` file inside:

- When `Mount and scan Virtual Hard Disks` is enabled, Kiosk will mount and scan A.vhd file as well.
- When `Mount and scan Virtual Hard Disks` is disabled, Kiosk will not mount A.vhd file, only original file A.vhd file is processed.

3. Scanning

Kiosk scans all enumerated files and show the progress of current processing disk image file on the UI.

From Kiosk v4.6.8, the child files inside the disk image is added into the **Processed files** for better statistics and estimation remaining time.

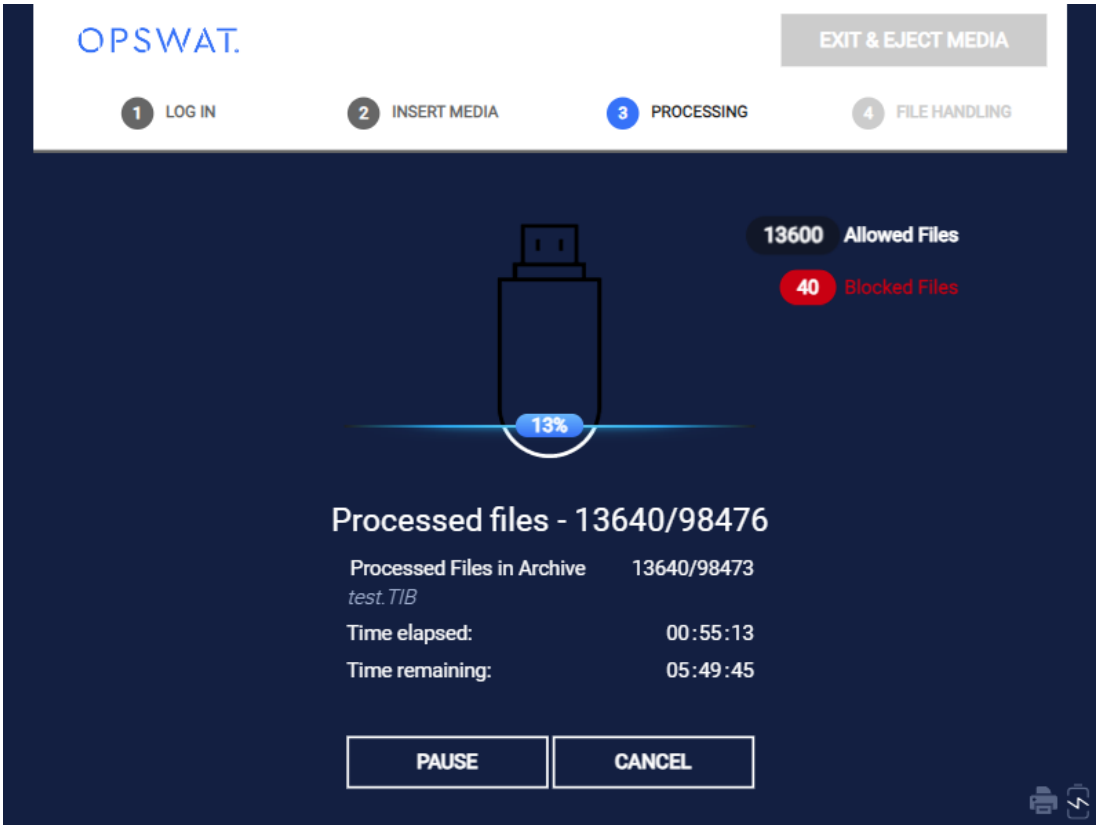


Image: Kiosk is scanning test.TIB file

4. Reporting

Kiosk UI

User can view the detailed result of original file and child files on Kiosk UI.

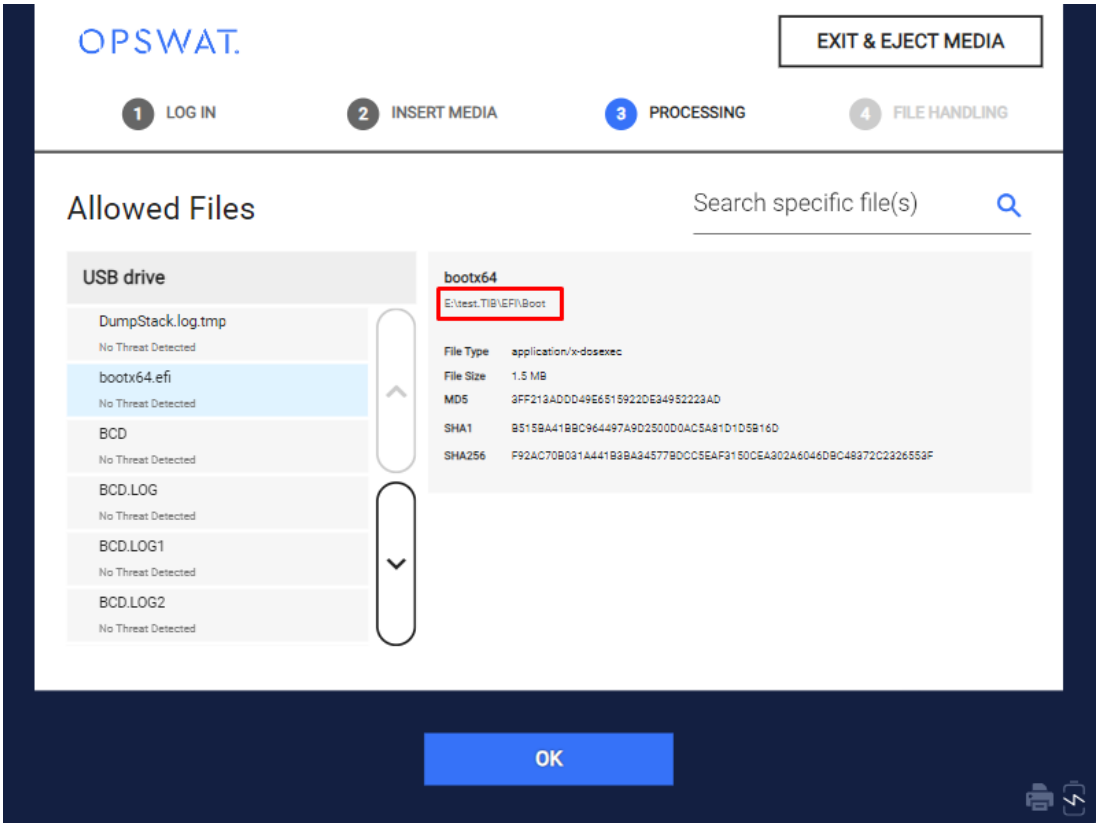
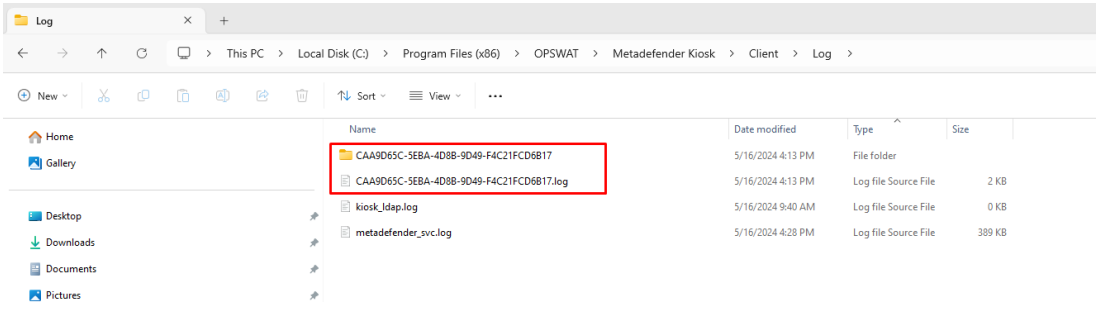


Image: Detailed result of allowed files on Kiosk UI

> **Warning**
> This view can only display a maximum of 500 files

Session Log

Beside the primary report, Kiosk will create a folder named session ID to gather all reports of disk image files.



The primary report contains the final result of the disk image file selected by the user. Meanwhile, Kiosk will generate a separate report for the child files. This additional report will be named as the original file and will follow the same format as the primary report.

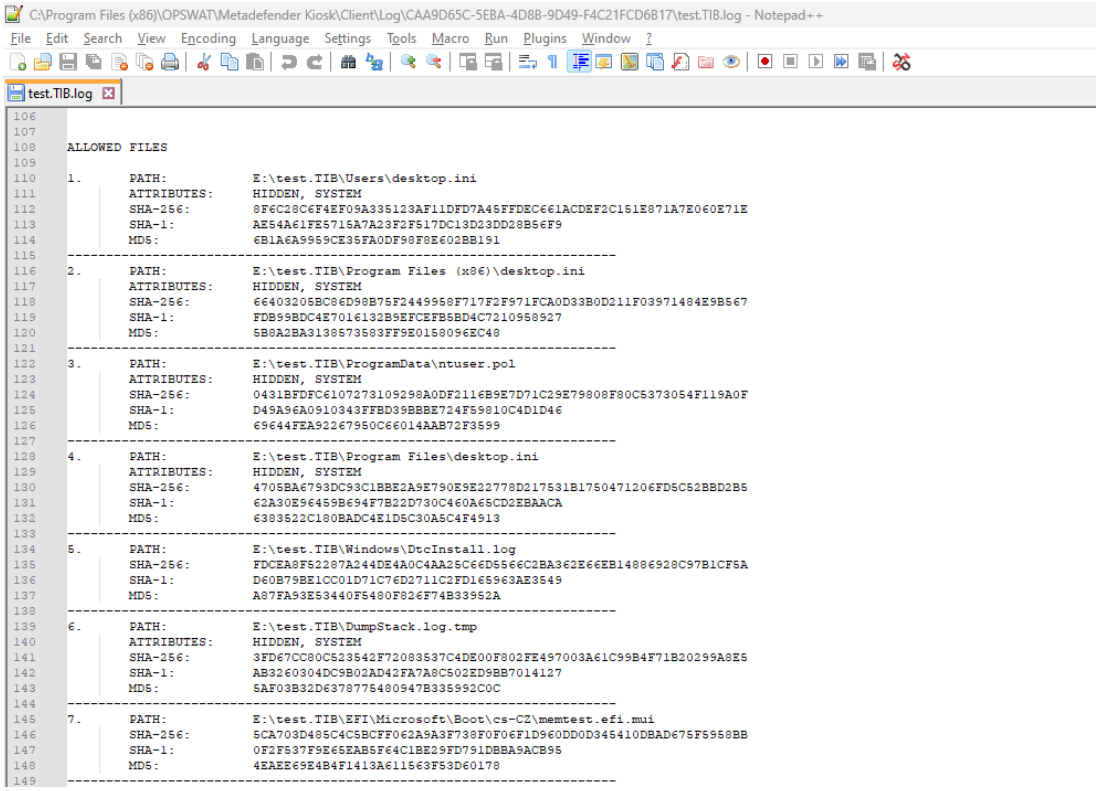


Image: Detailed result of child file insde test.TIB

5. Post processing actions

See Processing virtual disk files for more details.

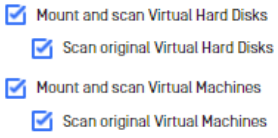
Notes

The Session History on Kiosk WebMC and Print result will display only the disk image files selected by the user, excluding their respective child files.

For some TIB files, two limitations are addressed with Acronis tool.

1. Filenames ending with numbers are considerred invalid
2. Same filename with different extension, e.x: *somefile.tib* and *somefile.tibx* are considered invalid.

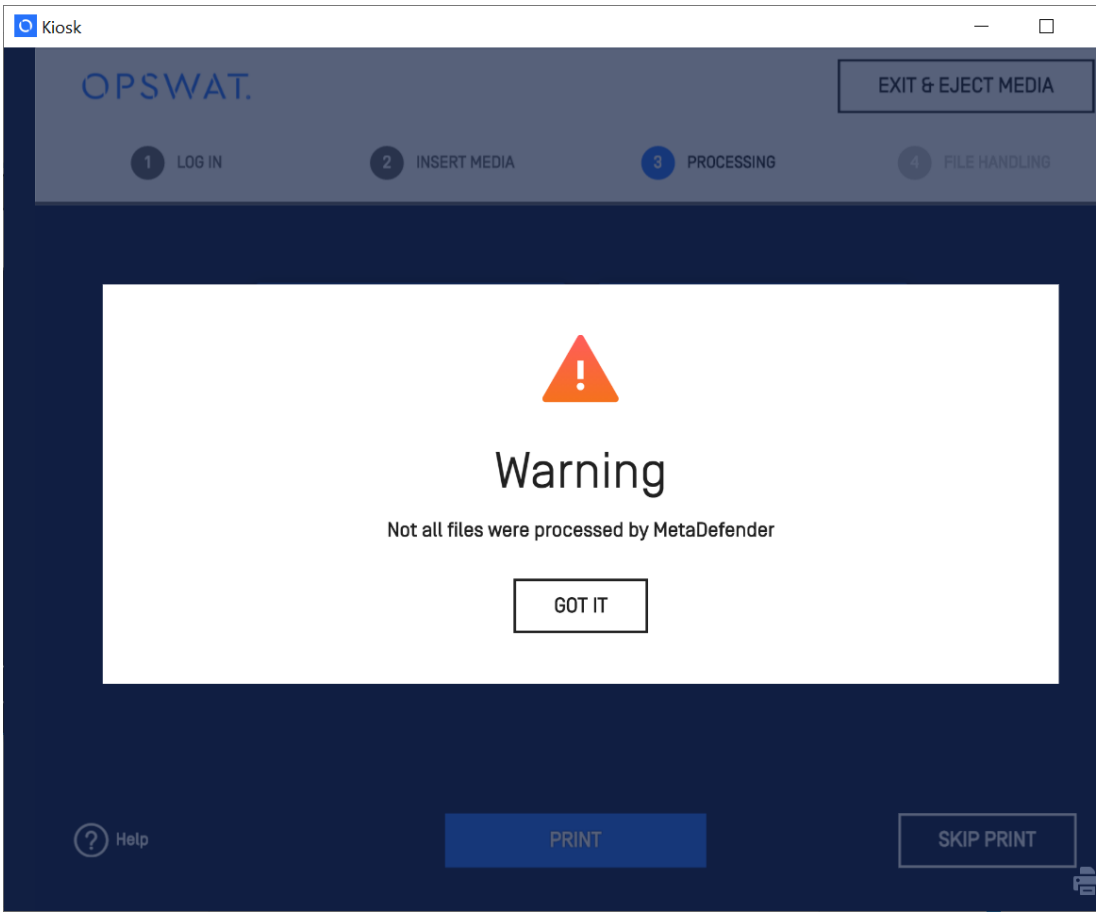
VMDK files with Windows and Linux filesystems are supported. In case of Linux filesystem, Kiosk may failed to mount it on Windows. Kiosk will covert the VMDK file to VHDX file then mount to scan if `Mount and scan Virtual Hard Disks` is enabled along with `Mount and scan Virtual Machines.`



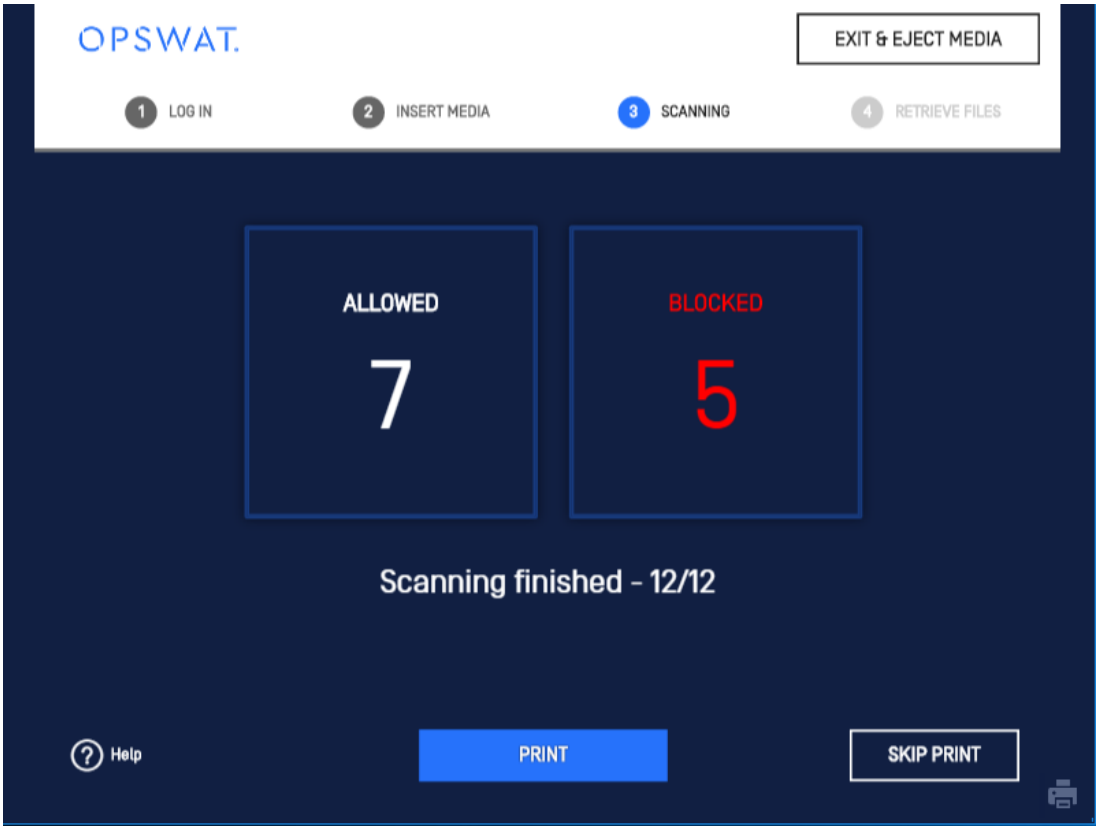
Viewing the Session Results

After media has been processed, the session results appear.

If any file was not processed by MetaDefender, a warning will pop up indicating that not all files were processed.



The session results include whether processing was completed or aborted, the number of files allowed and blocked and the total number of files processed.

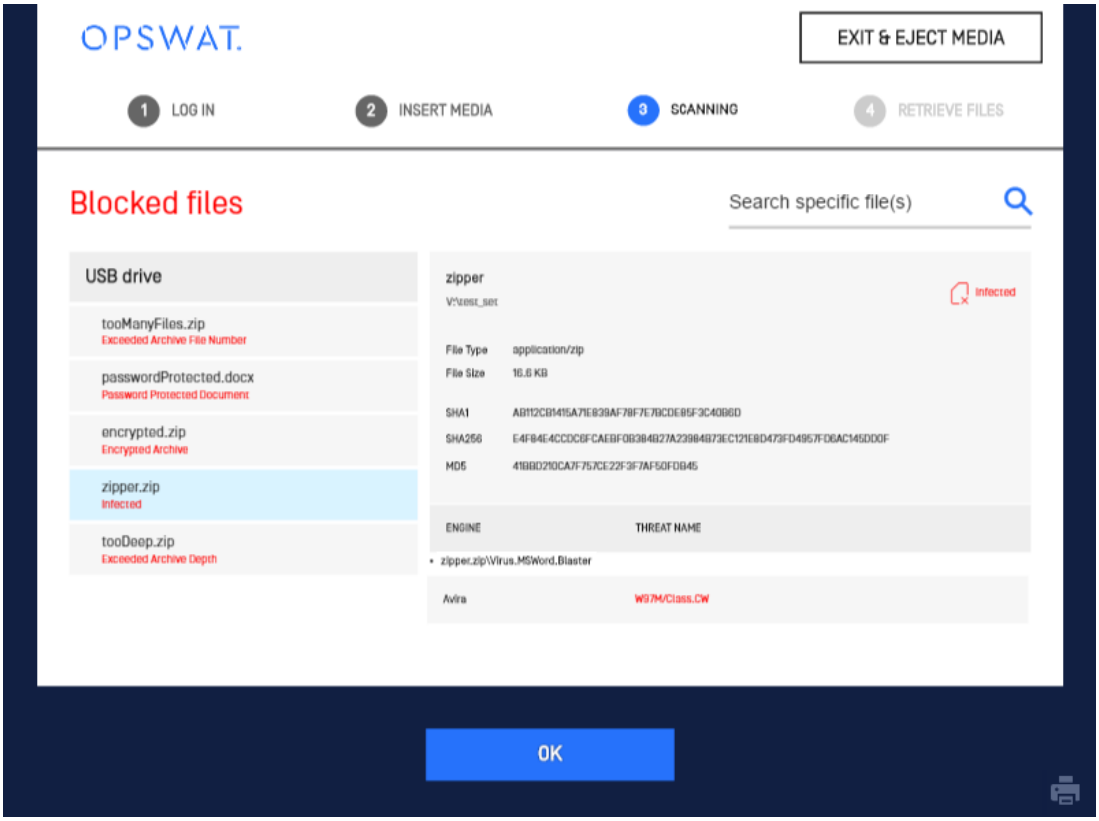


The session result page includes the following buttons:

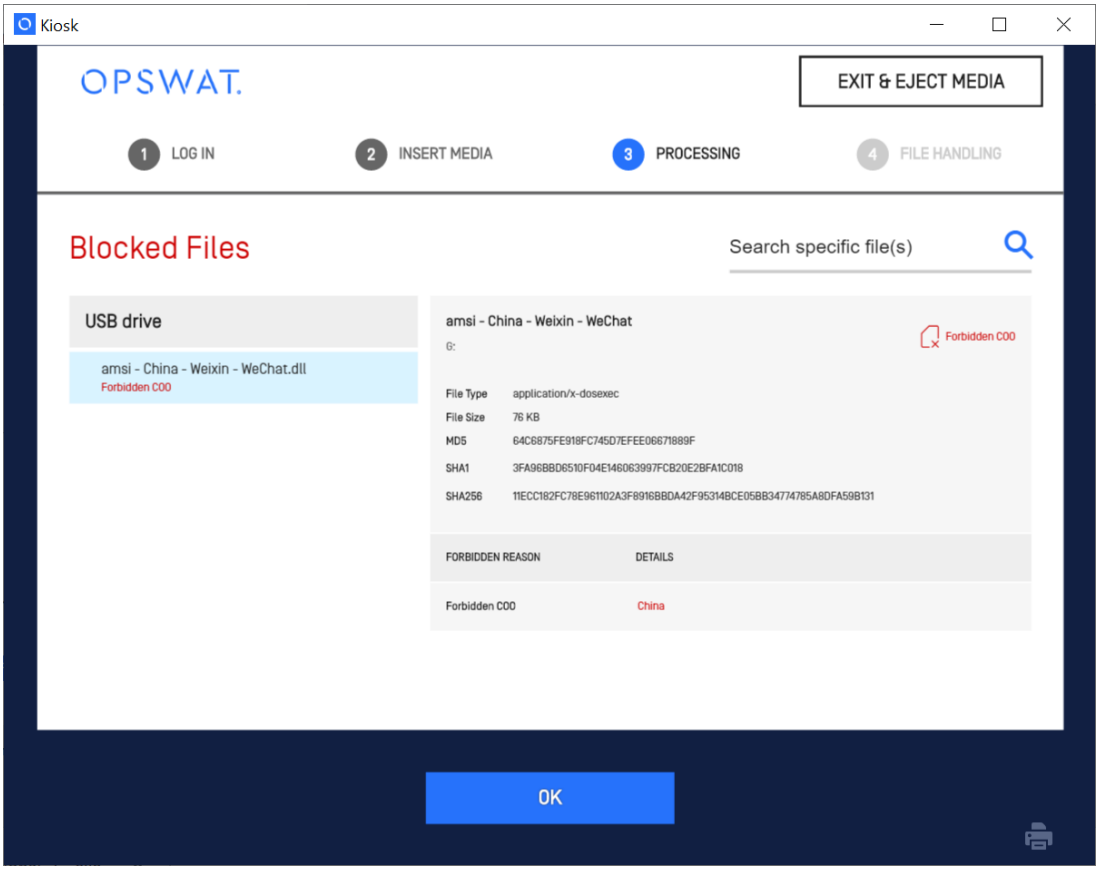
- **Allowed:** If allowed files are found, then the Allowed count will appear. Click this button to go to the Allowed file summary screen.
- **Blocked:** If blocked files are found, then the Blocked count will appear. Click this button to go to the Blocked file summary screen.
- **Copy & Print:** Clicking this button will begin the file transfer process to any destination configured. If printing is enabled, the session results will be printed to the default printer.

Viewing details about blocked files

The Blocked File Details screen displays the blocked files detected by MetaDefender Kiosk during processing. You can click a blocked file to view more details.

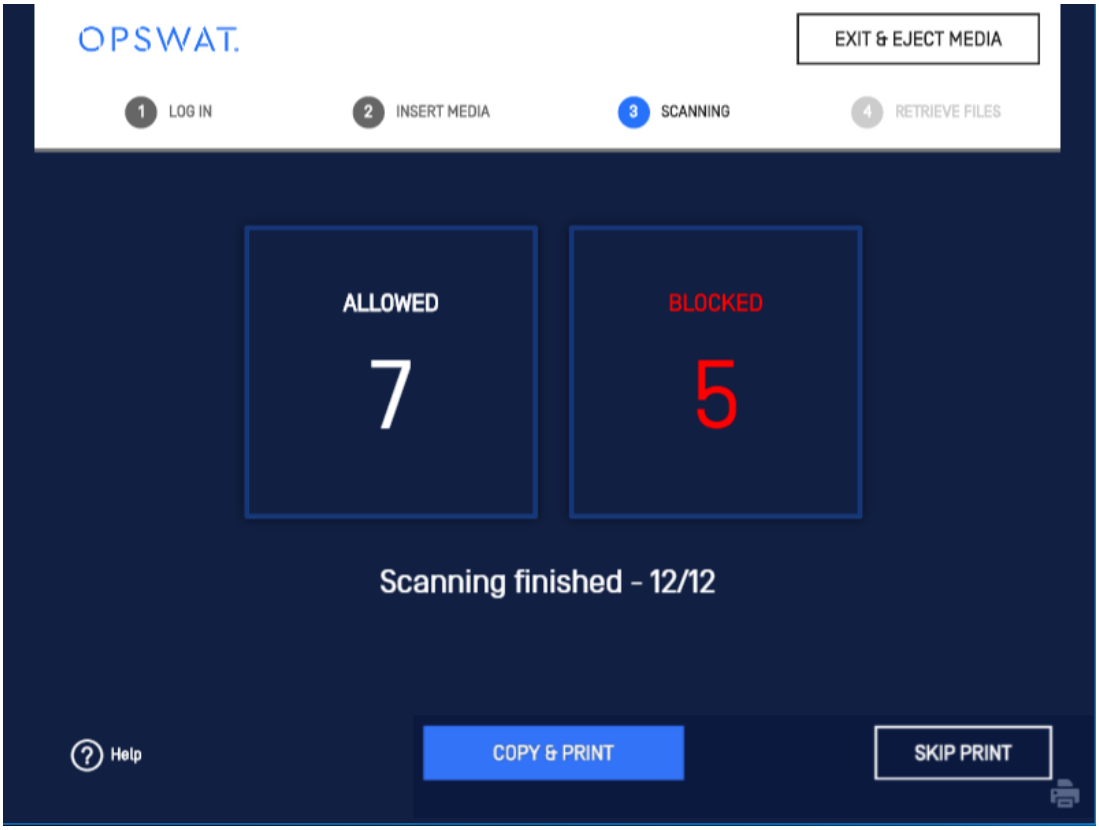


Some files published from countries in the COO forbidden list are reported as blocked as well.

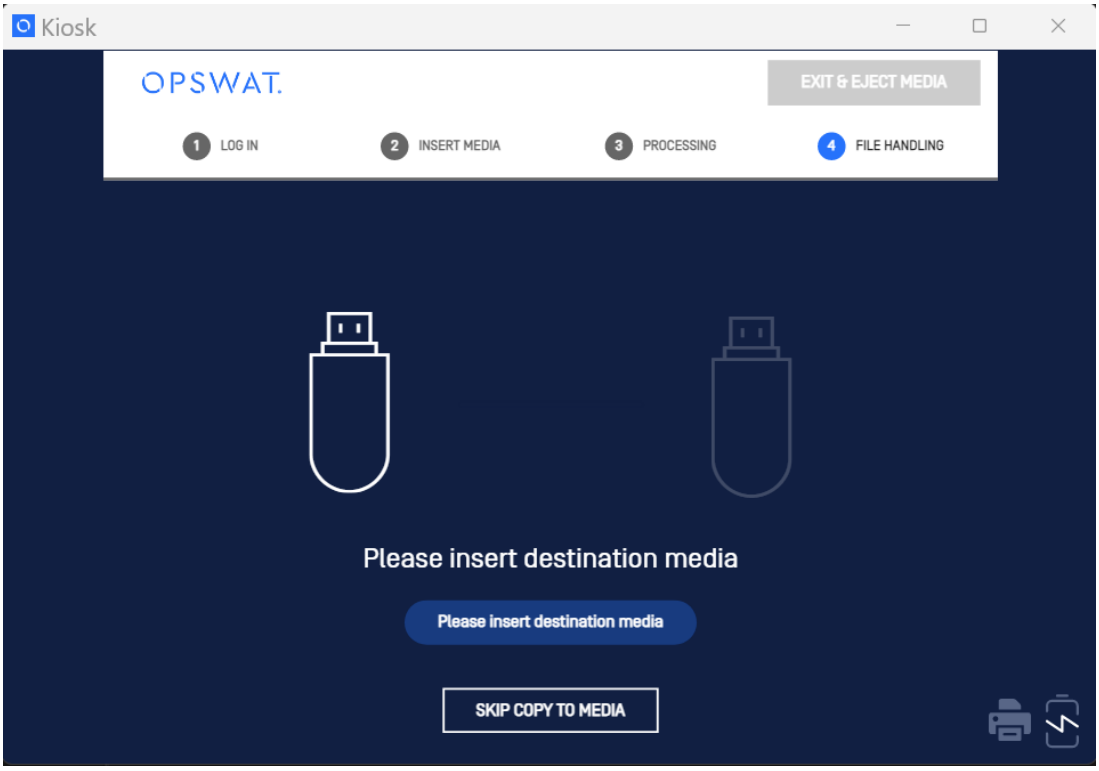


Data Included in the Kiosk Session Log File

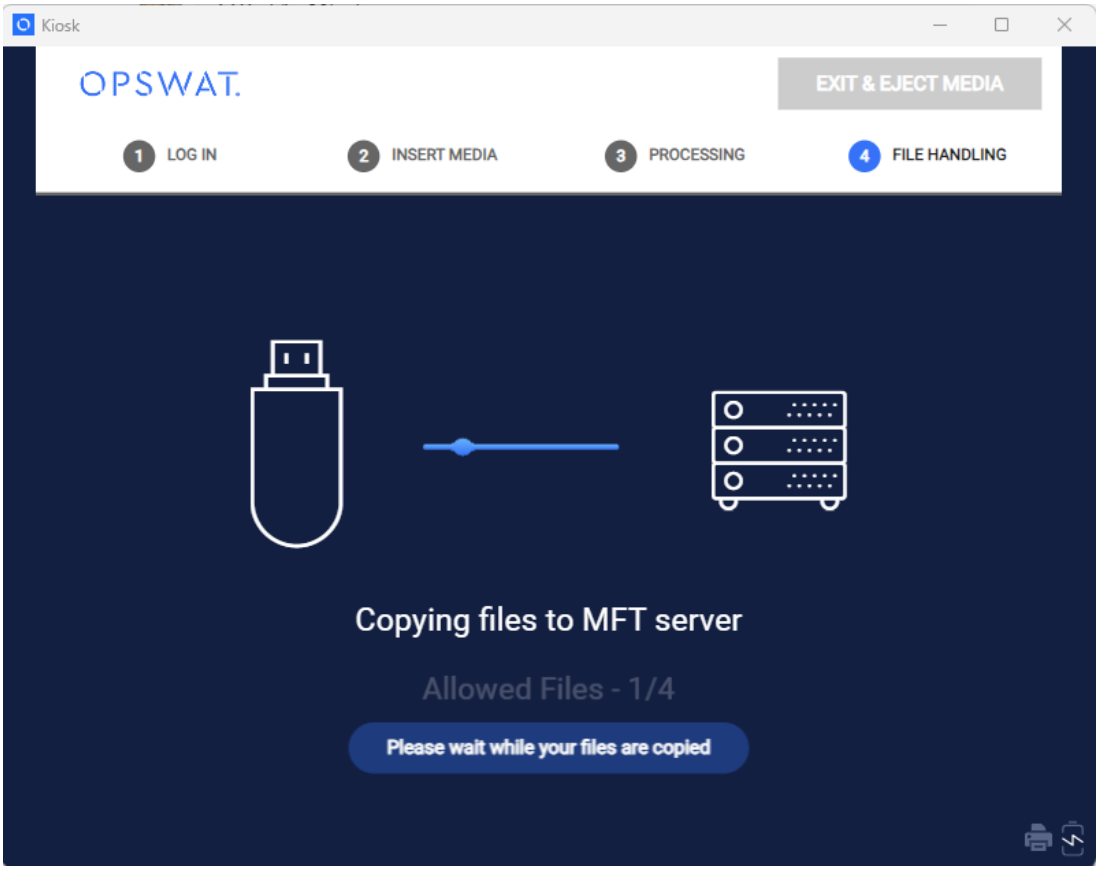
After scanning is complete, button [Copy&Print] or [Print] might appear, depending on settings in the workflow.



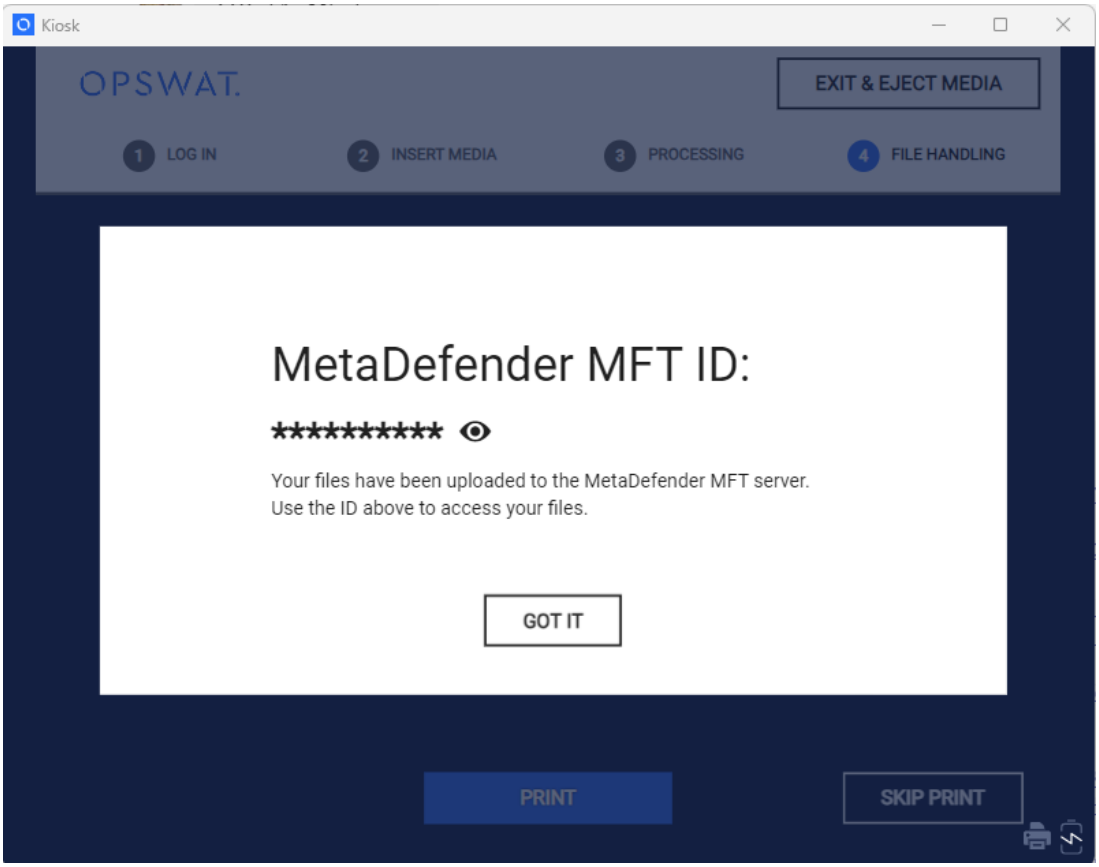
If the current workflow is configured to copy allowed/blocked files to user media, then user is required to insert another media. User should not pull out the source media or the session will be terminated.



If the current workflow is configured to copy allowed/blocked files to MFT server, user will see the copy progress. It might take time depending on network bandwidth and file sizes.



In case of uploading to MFT server, the uploaded files can be accessed later from MFT with the same user credential that has been loggend into the Kiosk session. In case of guest login, the file owner MFT ID is generated and concealed on the screen result for security reasons, click on the eye icon to reveal it.



See 9.6. Viewing the Session Results for more information.

The following information is included in the printout.

Data Item	Description
User ID	If you are using Windows authentication, this is your Windows user ID. If you are not using Windows authentication, this is blank.
Profile	The MetaDefender Kiosk profile that was used for this session
Session ID	The unique session ID generated for this MetaDefender Kiosk processing session
Scan Completion Status	PROCESSING FINISHED SUCCESSFULLY or PROCESSING ABORTED!
Process Start Time	Processing start time
Process Finish Time	Processing finished time
MetaDefender Kiosk Version	The product version of the MetaDefender Kiosk application
MetaDefender Core Version	The product version of the MetaDefender Core server
MetaDefender Managed File Transfer Version	The product version of the MetaDefender Managed File Transfer server if used to process files
Download URL	The URL where files were attempted to be retrieved from
Device Information	Section that includes identifying information for the physical media device that was scanned, if available, from the device
Manufacturer	Manufacturer of the media that was processed
Model	The model of the physical media that was processed
Serial Number	The serial number of the physical media that was processed
Device ID	A unique ID of the device whose value can be used for USB allowlisting
Media Type	The type of physical media that was processed
Partition Count	The number of partitions on the device
Hidden partition Count	The number of hidden/unsupported partitions on the device

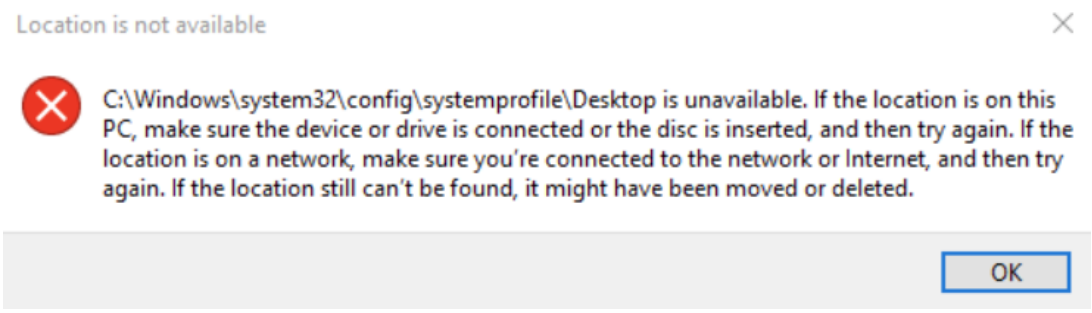
Data Item	Description
Partition Name • *Bootable*	Name of the partition on the device and whether it is a bootable partition
Disk Usage	The amount of space used / the total size of the drive
Scanning System	The machine name of the MetaDefender Kiosk system where the processing was done
Wipe Result	The result if the device was attempted to be wiped
Full Media Scanned	Indicates whether all of the files on the media were scanned by MetaDefender (excludes "Not Scanned" & "Failed" results)
Full Media Processed	Indicates whether all of the files on the media were processed through the entire Kiosk workflow (e.g. MetaDefender processing + file handling)
Total Files Scanned	The total number of files scanned by MetaDefender
Total Files Processed	The total number of files processed by MetaDefender Kiosk
Total Files Not Processed	The total number of files not processed by MetaDefender Kiosk, usually in the case that the session was canceled during processing
Downloaded Files	The total number of files successfully retrieved
Failed to Download	The total number of files unsuccessfully retrieved
Blocked Files	Section that includes a summary of the files blocked by the profiles defined in MetaDefender
<blocked result>	List of blocked results returned by MetaDefender, for more details on the results please refer to the MetaDefender documentation
Blocked Actions Taken	Section that includes a summary of the actions taken on blocked files
Remediated	The number of files remediated by MetaDefender
Quarantined	The number of files quarantined by MetaDefender Kiosk or MetaDefender

Data Item	Description
Deleted	The number of files deleted by MetaDefender Kiosk
Post Action Ran	The number of files processed by the post action script defined in MetaDefender Kiosk
Copied To Media	The number of files copied to another device
Copied To Directory	The number of files copied to another location
Copied To MFT Server	The number of files copied to a MetaDefender Managed File Transfer server
Moved To Media	The number of files moved to another device
Moved To Directory	The number of files that were moved to another location
Moved To MFT Server	The number of files moved to a MetaDefender Managed File Transfer server
Copied to [media, directory, MFT Server]	The location where files were copied
Moved to [media, directory, MFT Server]	The location where files were moved
Allowed Actions Taken	Section that includes a summary of the actions taken on allowed files. The descriptions are the same as those described above for blocked files.
Skipped Files	The number of files skipped by configuration set in MetaDefender Kiosk
File Type Totals	The number of files of each file type that were included in the processing session
Deleted Files	The list of files removed during processing. Each file will have the PATH, ATTRIBUTES and SHA-256 listed.
Quarantined Files	The list of files quarantined during processing. Each file will have the PATH, ATTRIBUTES and SHA-256 listed.
Quarantine Failures	The list of files failed to be quarantined during processing. Each file will have the PATH, ATTRIBUTES and SHA-256 listed.

Data Item	Description
Skipped Files	The list of files that were configured to be skipped from being scanned by MetaDefender Core. Each file will have the PATH, ATTRIBUTES and SHA-256 listed.
Files Failed SHA-256 Verification	The list of files that failed SHA-256 verification during copy/move (if SHA-256 Verification was enabled). Each file will have the PATH, ATTRIBUTES, SHA-256 and REASON listed.
Files Failed to be Remediated	The list of files that failed to be remediated. Each file will have the PATH, ATTRIBUTES and SHA-256 listed.
Files Failed to be Deleted	The list of files that failed to be deleted. Each file will have the PATH, ATTRIBUTES and SHA-256 listed.
Files Sent to MFT for Processing	The list of files sent to MFT for processing. Each file will have the PATH listed.
Detected Symlink Files (not scanned)	The list of symbolic links found that were not processed. Each link will have the PATH listed.
Files Downloaded	The list of files successfully retrieved. Each file waill have the PATH listed.
Files Failed to Download	The list of files that failed to be retrieved. Each file will have the PATH listed.
Allowed Files	The list of allowed files in the session. Each file will have the PATH, ATTRIBUTES and SHA-256 listed.

Path	The relative path to the given file
Attributes	Displays if a file has "Hidden" and/or "System" attributes enabled
SHA-256	The hash value of the given file
Threat Name	The name of the infection for the given file
Scan Result	The scan result of the detected file threat
Detected File Type	The detected content type of the file
File Type Description	The description of the detected file type
Reason	The reason the file has been included in the current list
Process Server	The server url the file was processed on

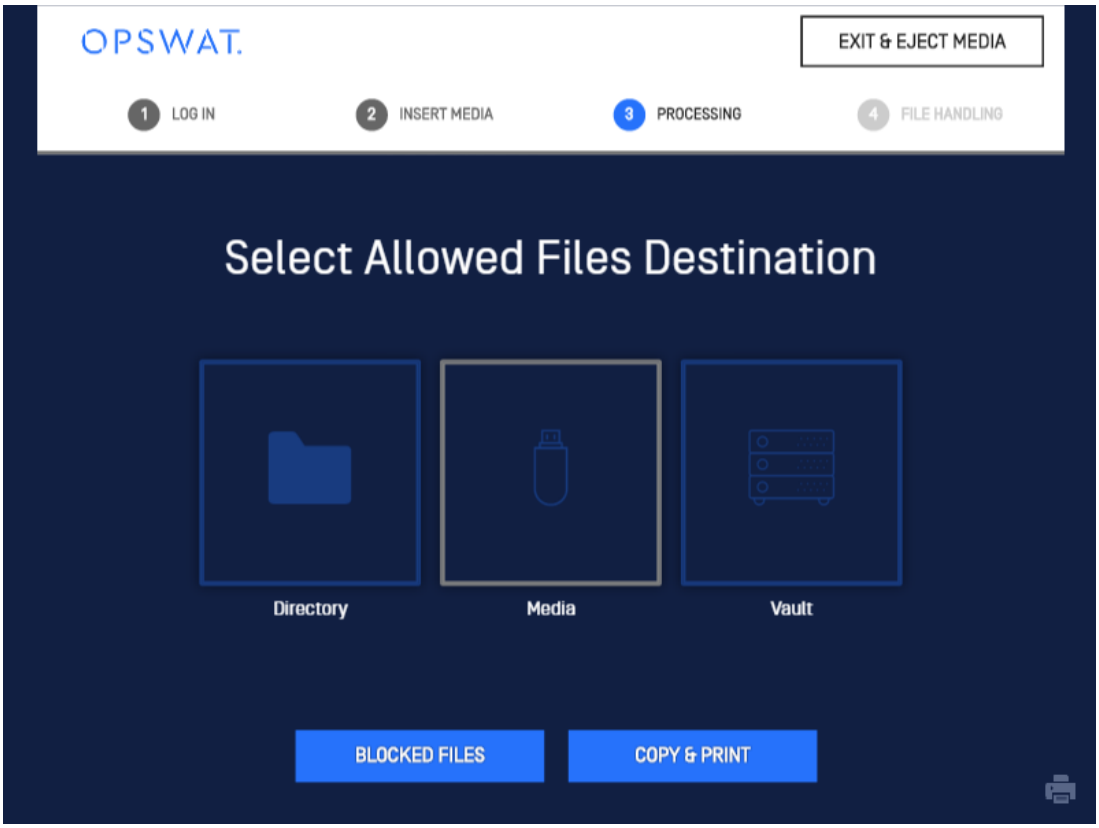
Note: The printing process is executed on windows system profile and might need an accessible Desktop folder for that profile. If the Desktop folder is not available, Kiosk will temporarily create it and remove it after the printing is complete. Kiosk might also change the access permission of the parent folder of the Desktop to full control to create the subfolder Desktop and restore its original permissions when the printing is complete. However, if IT administrators have changed the permission to Denied, Kiosk keep everything unchanged. Please ask the IT to change its permission or just proceed the printing by clicking OK when the warning popup "Location is not available" occurs.

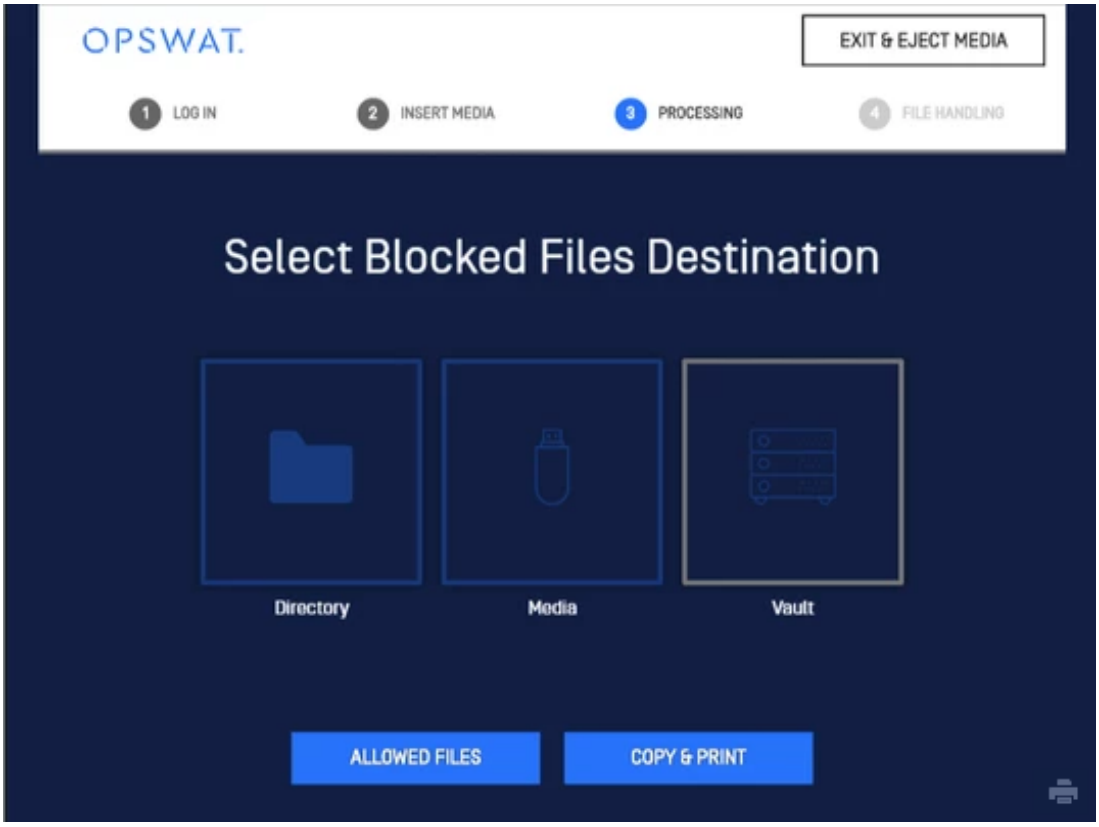


Copying Files

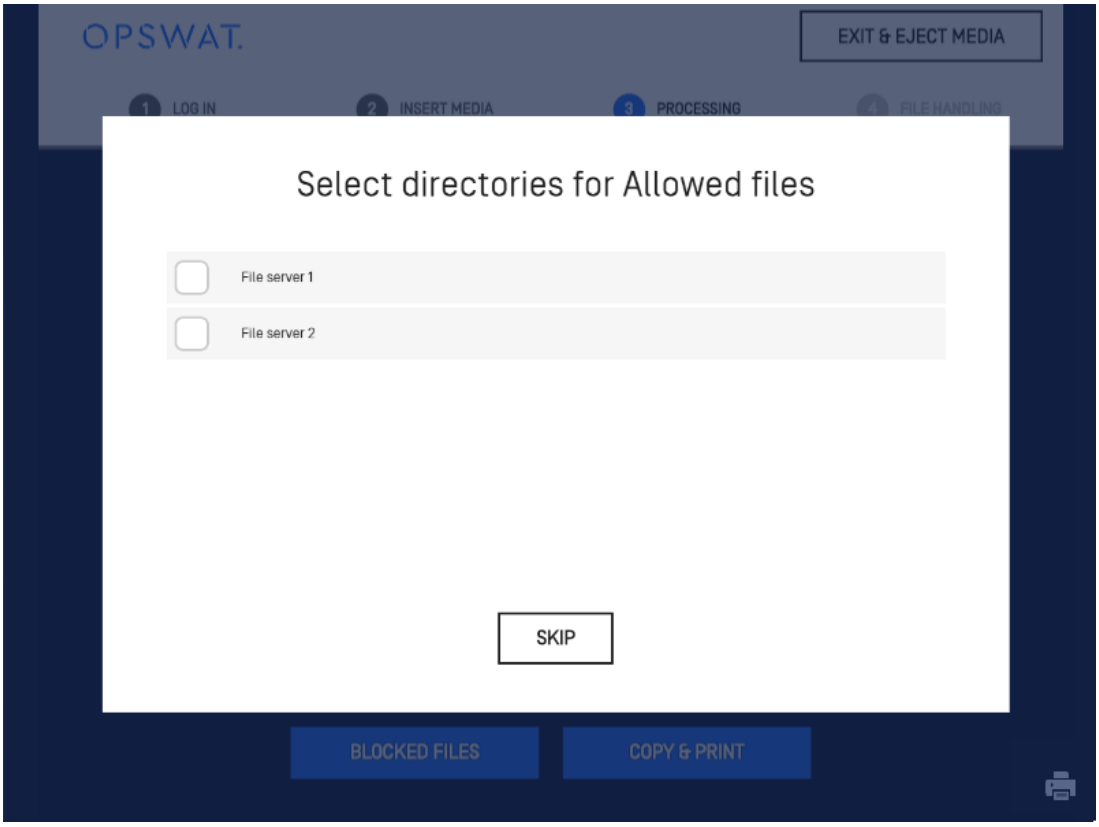
Selecting which copy option to run

If `Allow user to select copy option` is enabled (for each respective allowed/blocked designation), the file handling option screen will allow users to select the destination for files. Navigating between allowed and blocked is possible when the option is enabled for both. Selection is done by clicking each option to run (a check mark indicates the option is selected and will be performed) and then hitting the `Copy` button.





When Directory is selected, another window will pop up to allow the directory destination selection.



Copying files to another media

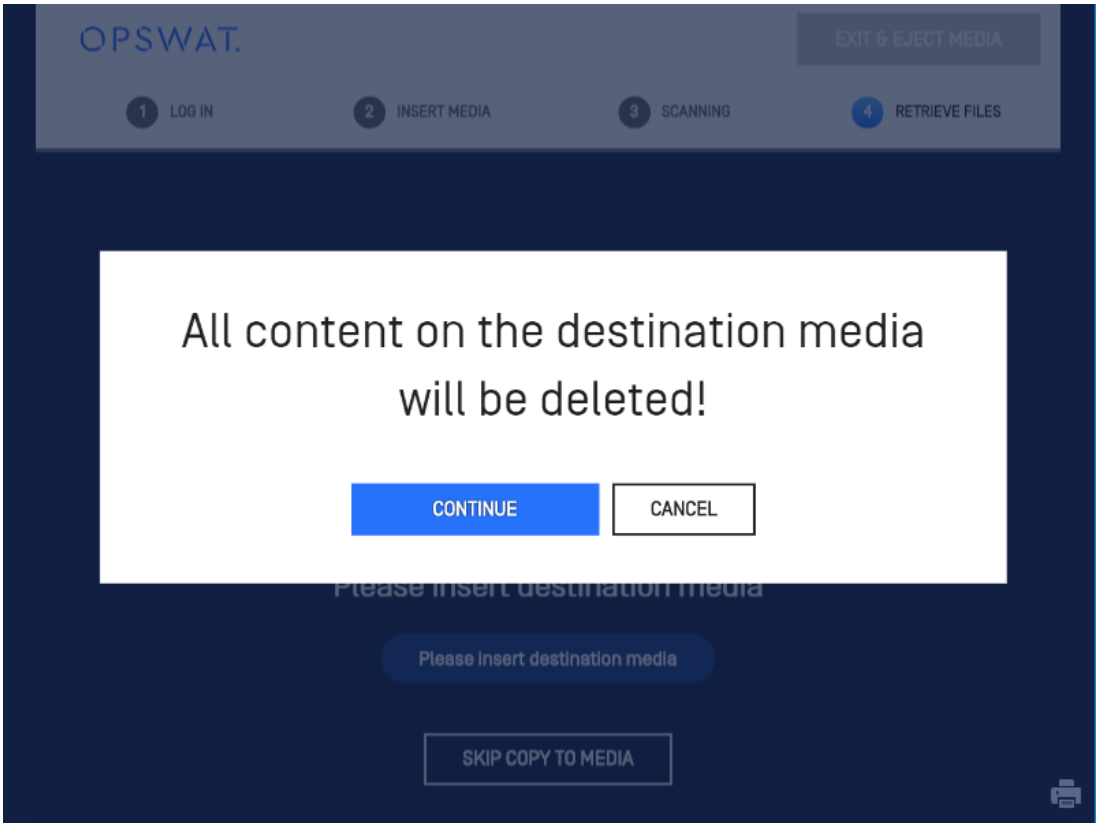
Copy-to Media Support Chart

Media Type	Supported	Additional Info
USB	✔	
CD/DVD/Blu-Ray (R or RW)	✔	Disc must be blank and non-finalized
Floppy	✔	If copying to floppy is enabled, the *Detect Floppy Disk* button must be clicked after inserting a floppy
SD Card	✔	
Hard Disk Drive	✔	

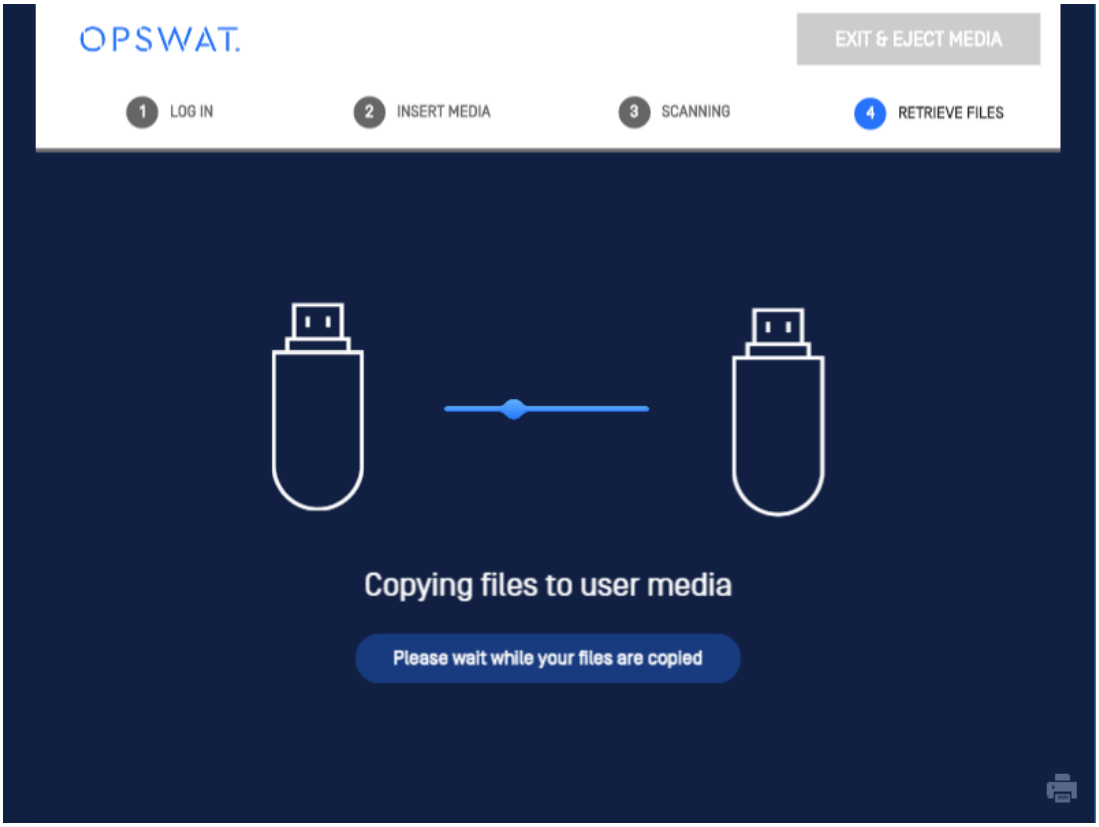
Info
If an encrypted device is inserted as the media to copy to, there will be a prompt to enter the password to unlock the media before files are copied.

If your workflow specifies copying scanned files to other media, you are prompted to insert the media to which you want to copy your files. If you do not want to copy the files, click **Skip Copy to Media** . The original source media must remain connected to MetaDefender Kiosk to successfully copy the files.

If the user media is configured to be wiped before copying, a prompt will alert the user that the destination media will be wiped.



Select 'Continue' to have the media wiped and copy files to or 'Cancel' to be taken back to insert another media to copy files to.


OPSWAT.
EXIT & EJECT MEDIA
1 LOG IN
2 INSERT MEDIA
3 SCANNING
4 RETRIEVE FILES
Copying files to user media
Please wait while your files are copied

Retrieving Files from an External Source

Purpose: Enhance diverse workflows for media handling options after users login on Kiosk UI successfully.

Tactics: The user can select two options: processing the files on the media or retrieving files on Kiosk UI.

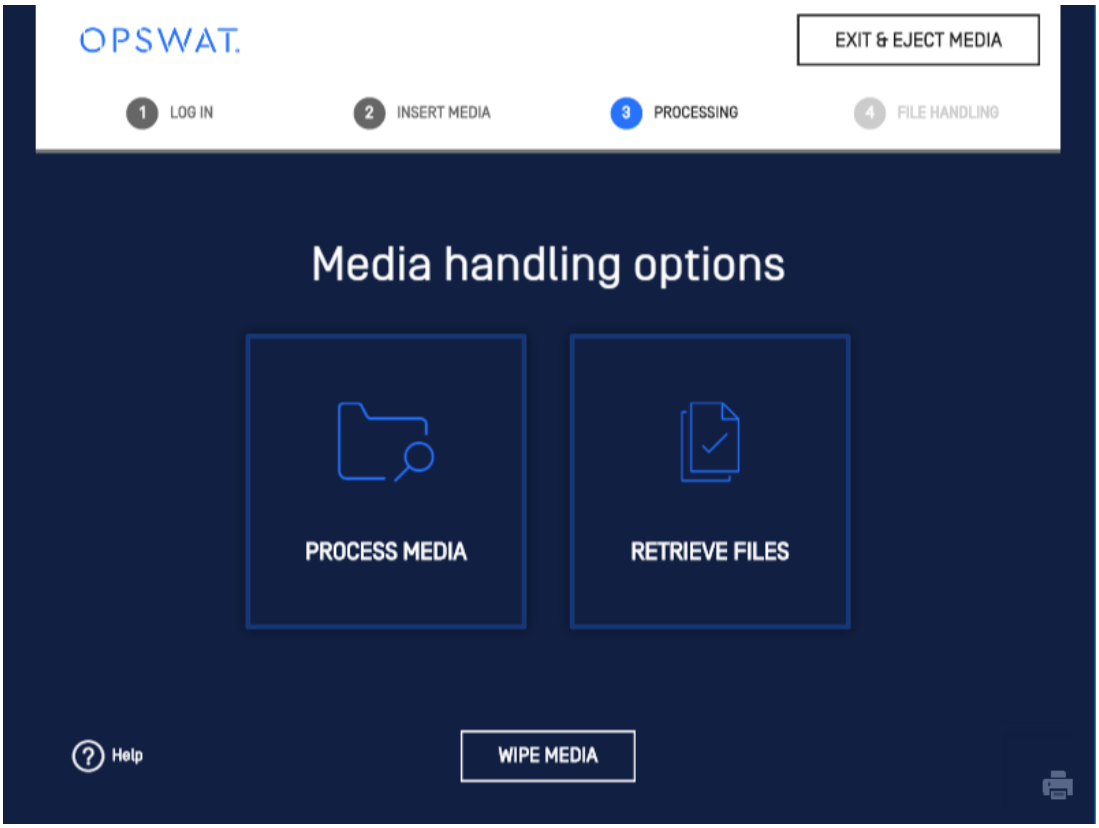
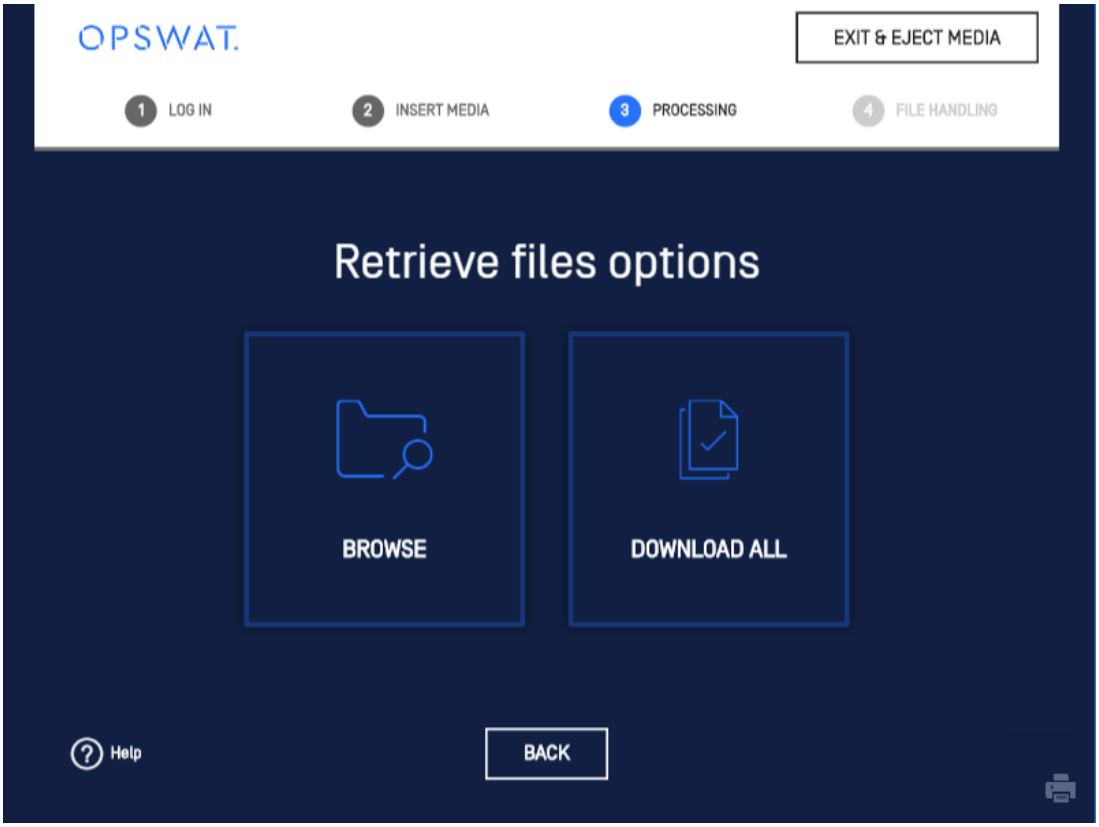


Image: "Media Handling Options" on Kiosk UI

After selecting to "Retrieve files" option, users can click `BROWSE` files to download specific files or choose `DOWNLOAD ALL` option to download all the files.

Note: When both options **" Allow user to browse for files"** and **"Allow user to process all files"** are disabled at Kiosk Interface configuration, the Kiosk will automatically select the "retrieve files options".



Image" "Retrieve files options" on Kiosk UI

If user choose to pick "Guest login" option, an MFT owner ID will be required and there is space for users to fIll out information.

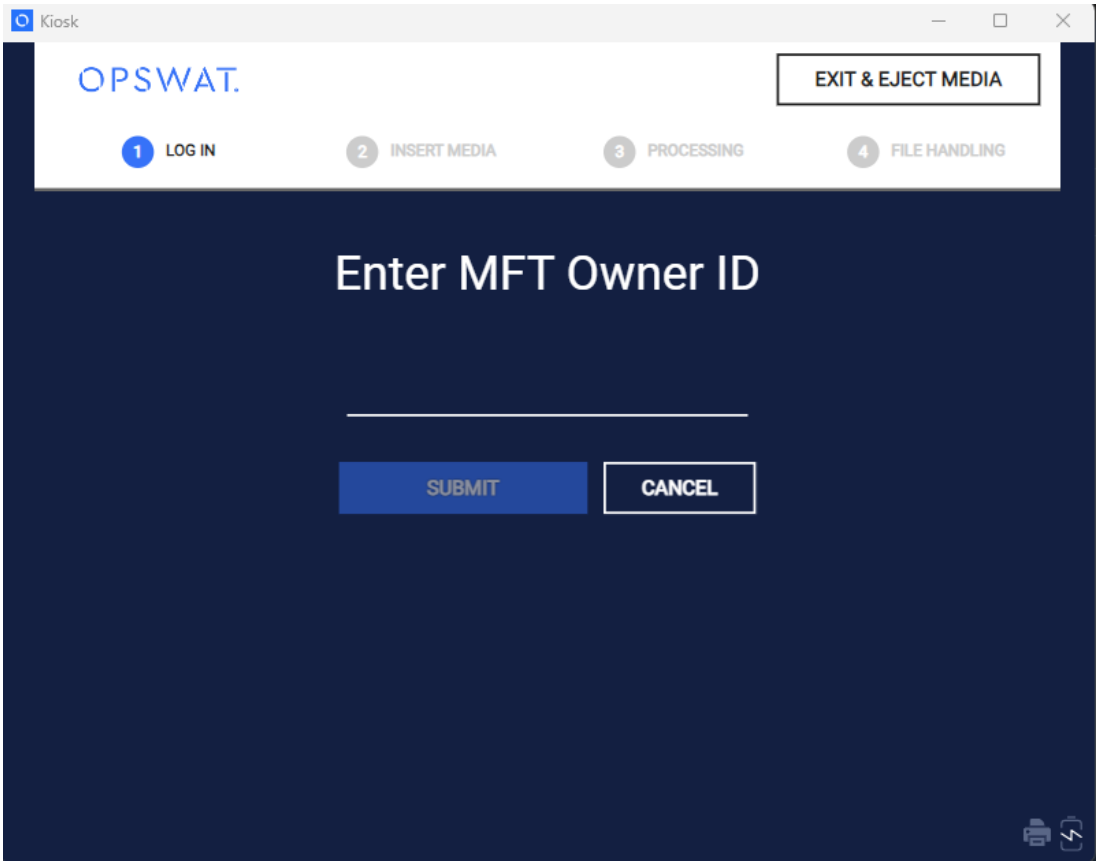


Image: "Enter MFT Owner ID" on Kiosk UI

The data and files are available from MFT for downloading when they have "No Threat Detected" scan results and also remarked as "Available" or "Remediated" status. Those files are also marked in black colour in the MFT Files window. Files in other status are neither displayed nor available for downloading.

On Kiosk UI, the Browse view demonstrates that the system allow users to select specific files or data that are Available to download from MFT.

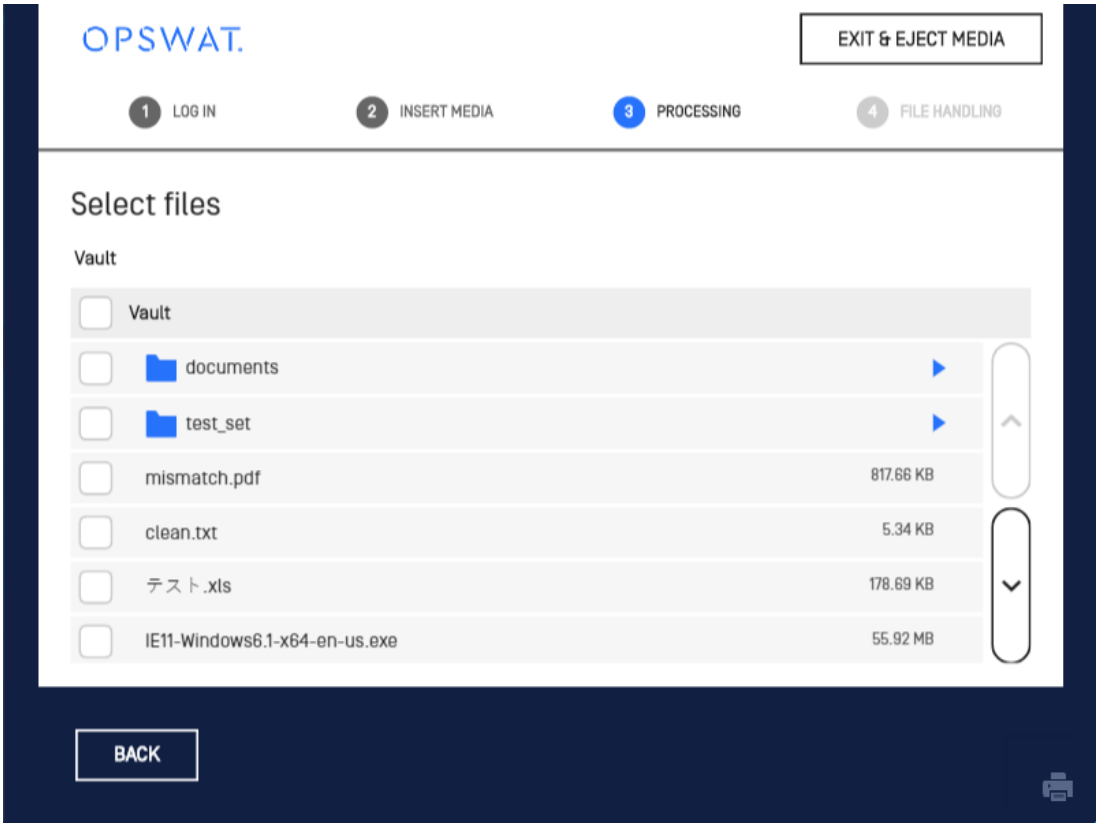


Image: Browse view with MFT file downloading options

If there is not enough data storage space on the media to download files, an alert will pop up to notify the amount of required data storage to retrieve the files.

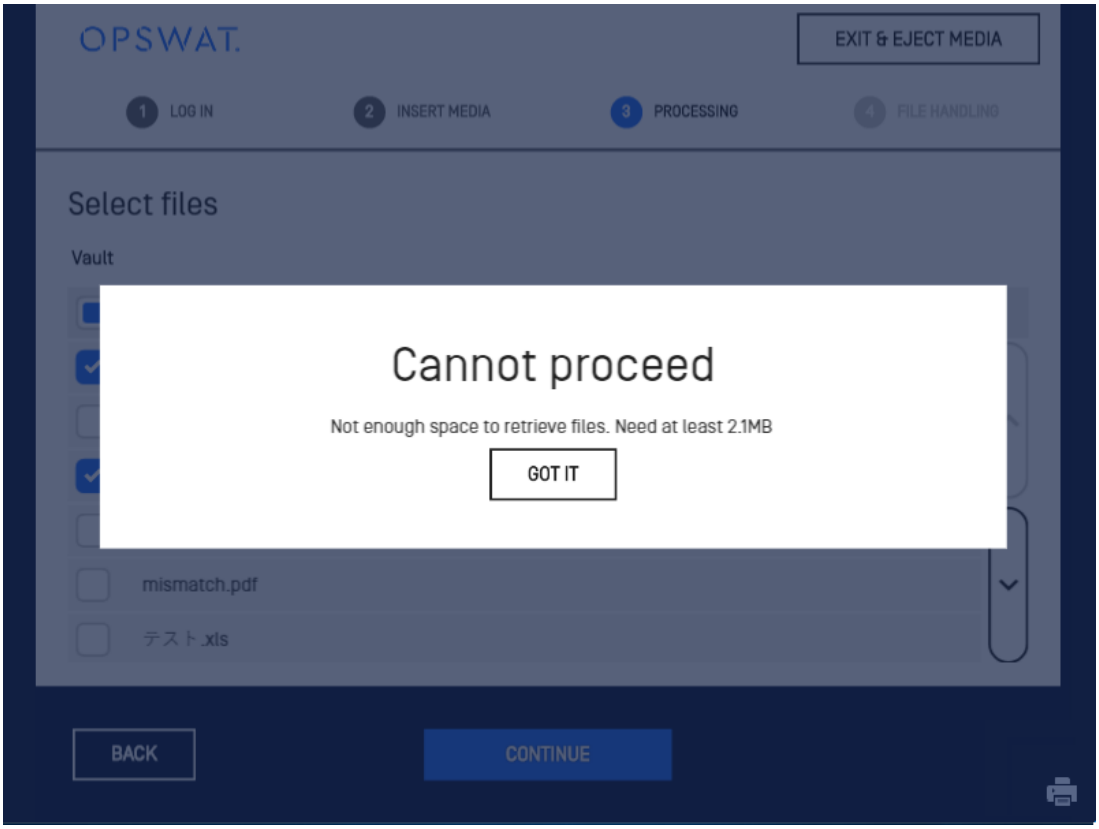


Image: "Cannot proceed" tab pop-up when there is not enough data space on Kiosk

OPSWAT Media Validation Agent

The OPSWAT Media Validation Agent (OMVA) is a lightweight tool that is deployed on Windows endpoints ensuring that the contents of media can only be accessed if it has been processed & allowed by MetaDefender Kiosk. With the media manifest feature enabled, after media is processed by MetaDefender Kiosk, it will contain a media manifest that is digitally signed and hashes of all the clean and approved files. When an endpoint has OMVA installed, any media that is inserted is first checked for a valid digital signature from the Kiosk and then a hash check is performed verifying that the contents of the media have not been altered.

Limitation
Encrypted devices supported by Kiosk are not supported by OMVA

Supported Operating Systems

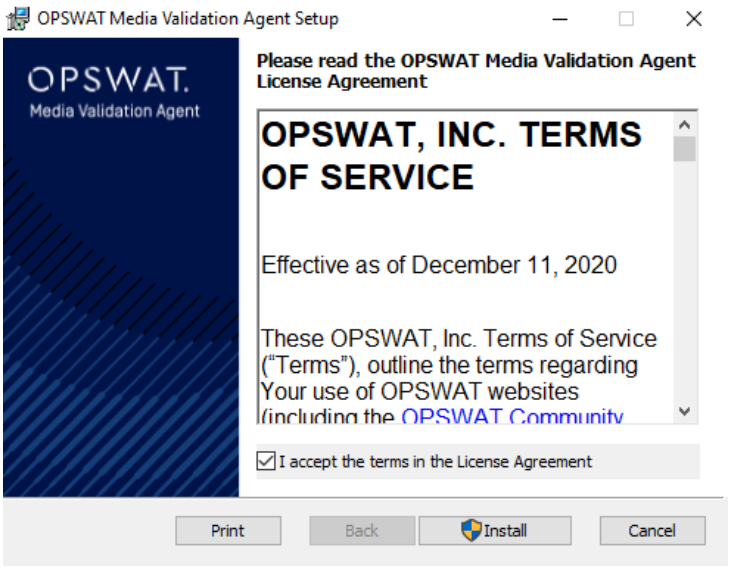
OMVA is supported on the following operating systems (32\64 bit):

- Windows XP SP3
- Windows Vista
- Windows 7
  - Requires Service Pack 1 and Microsoft updates KB2533623 and KB3033929
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11
- 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*
- Windows Server 2019*
- Windows Server 2022*

> **Info**
> *Any server OS requires KB4474419 installed (https://support.microsoft.com/en-us/help/4474419/sha-2-code-signing-support-update)

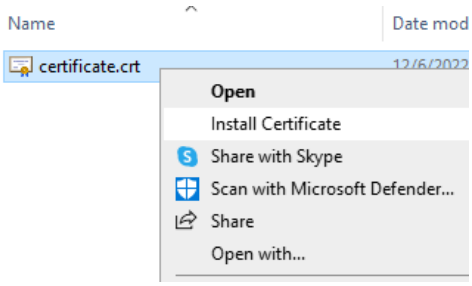
Installing the Agent

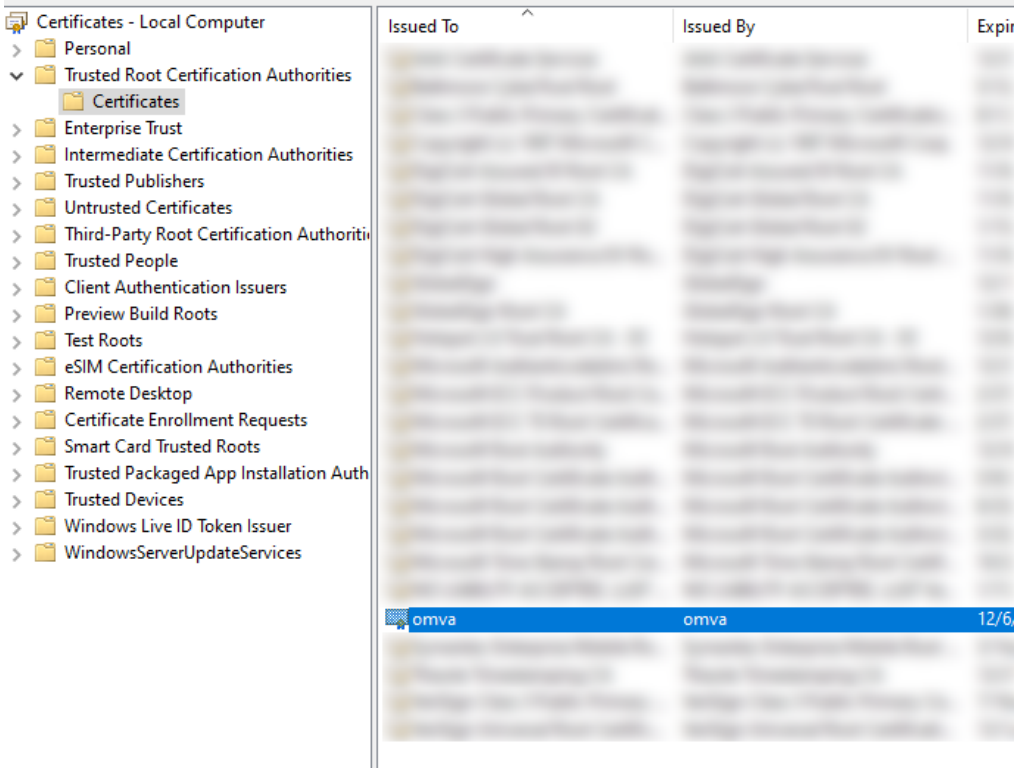
The OMVA installer can be obtained from the Kiosk Resources page or My OPSWAT. Run the .msi obtained on the Windows endpoint.



The Agent must be provided with the certificates it should consider trusted. The Agent will look in `%ALLUSERSPROFILE%\OPSWAT\.ssh\` to locate all trusted certificates.

If the trusted certificate is not in the directory, the Agent 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 end-point by copying the .crt file over, right clicking on it, and selecting `Install Certificate`.



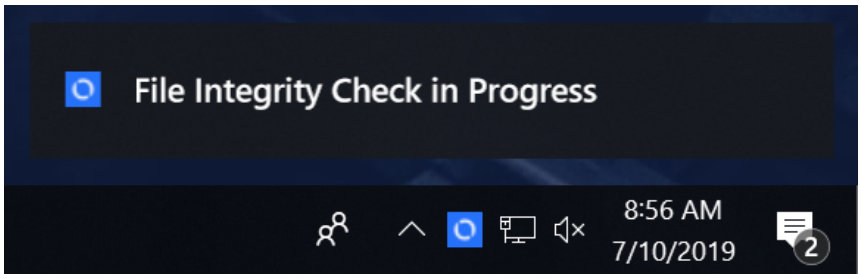


Usage / Verification of the Media

Insert the media to the endpoint.

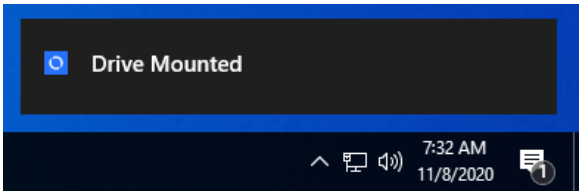
The Validation Agent will begin checking the media according to these steps:

1. Looks for an OPSWAT Media Manifest file on the media
2. Checks to make sure the Certificate that signed the media manifest is trusted
3. Checks each file on the removable media against the media manifest to make sure it has not been modified

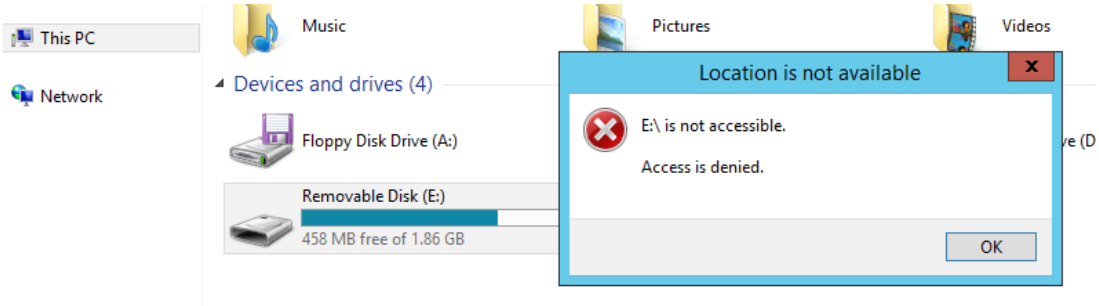


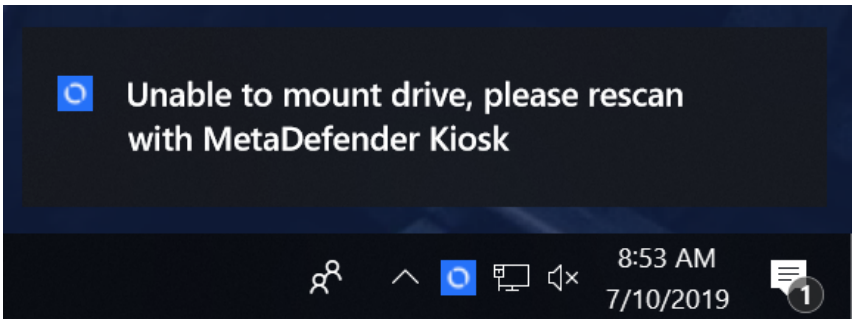
Result of Verification

If the manifest is found to have all files on the media recorded and unmodified, the media will be allowed to be accessed on the endpoint:



If the manifest is found to be invalid or files on the media are found to be missing/modified from the manifest, the media will be blocked from being accessed on the endpoint:





Info
The Validation Agent takes an "all-or-nothing" approach. Any invalid file or manifest will result in the entire media being blocked. There is no access to a subset of valid files.

Logging

OMVA logs JSON formatted messages of its operation. This can be used to determine the validation ran on the system and identify any media that was blocked. Logging can be found in the OMVA install directory:
`%PROGRAMFILES(X86)%\OPSWAT\OPSWAT OMVA\LOG\omva_logs.json`

When extracting logs from the file, the JSON objects must be wrapped within square brackets "**[ ]**" to allow for proper parsing.

log JSON object structure json

```
{
    "date": utc formatted string
    "event_code": event code integer
    "level": log level string
    "message": message string
    "hostname": system hostname string
    "username": username of logged-in user string
}
```

Event Code	Description	Notes
0	Validation begin - USB inserted	contains additional `user_data` string field in the json message
1	File result error	
2	Validation end - Media validation result	
3	Signature Result	

sample logging json

```
{
    "date": "2021-04-22T17:28:11Z",
    "event_code": 0,
    "level": "info",
    "message": "USB inserted - Volume{0f1895d7-d714-4030-9b2c-3aeacb631d1b}",
    "hostname": "Workstation3186",
    "username": "company/userA",
    "user_data": "[Kiosk] SessionID: 81E60795-67D8-4A34-8792-90D6E403D039 ||
User: abc || System: Kiosk1 || Device ID:
SCSI\\DISK&VEN_MSFT&DISK\\2&1F4FFE&0&0001 || Start Time: 2021-07-08 16:10:01"
},
{
    "date": "2021-04-22T17:28:15Z",
    "event_code": 1,
    "level": "info",
    "message": "G:\\files\\spreadsheet.xlsx - File not found in Media Manifest",
    "hostname": "Workstation3186",
    "username": "company/userA"
},
{
    "date": "2021-04-22T17:28:20Z",
    "event_code": 2,
    "level": "info",
    "message": "Unable to mount drive, please rescan with MetaDefender Kiosk",
    "hostname": "Workstation3186",
    "username": "company/userA"
}
```


Configuration of the Agent

Registry configuration:

For Wins 32 bit: `HKLM\SOFTWARE\OPSWAT\OPSWAT-OMVA`

For Wins 64 bit: `HKLM\SOFTWARE\WOW6432Node\OPSWAT\OPSWAT-OMVA`

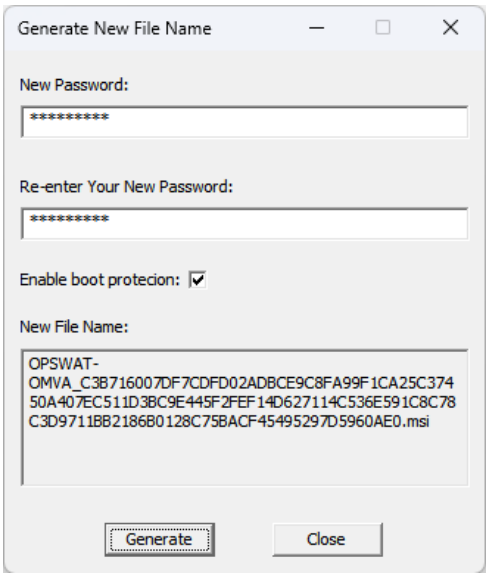
Key	Type	Description
days_trusted	REG_SZ or REG_DWORD	The maximum days to use a media manifest result If blank or omitted, the manifest is trusted forever

Uninstalling the Agent

Uninstalling the agent requires the password: `Opswat1234!` to successfully complete

OMVA Tool

Run `OPSWAT-OMVA-Tool.exe` obtained from the Kiosk Resources page before installing OMVA on endpoints.



Enter in the new password to configure. Click `Generate` to create a new filename for the OMVA installer. Download the new OMVA installer from the Resources page. Copy the `New File Name` and rename the installer. Installing this renamed file on all endpoints will ensure the uninstall password adheres to what was configured in the tool.

When the ***"Enable boot protection"*** __option __is checked, the OMVA application block access to any external removable media drives that are connected before the system boots up.

To update existing installations, the previous OMVA must be uninstalled with the default password. Then install the newly renamed OMVA installer.

Additional Kiosk Configuration

Dashboard

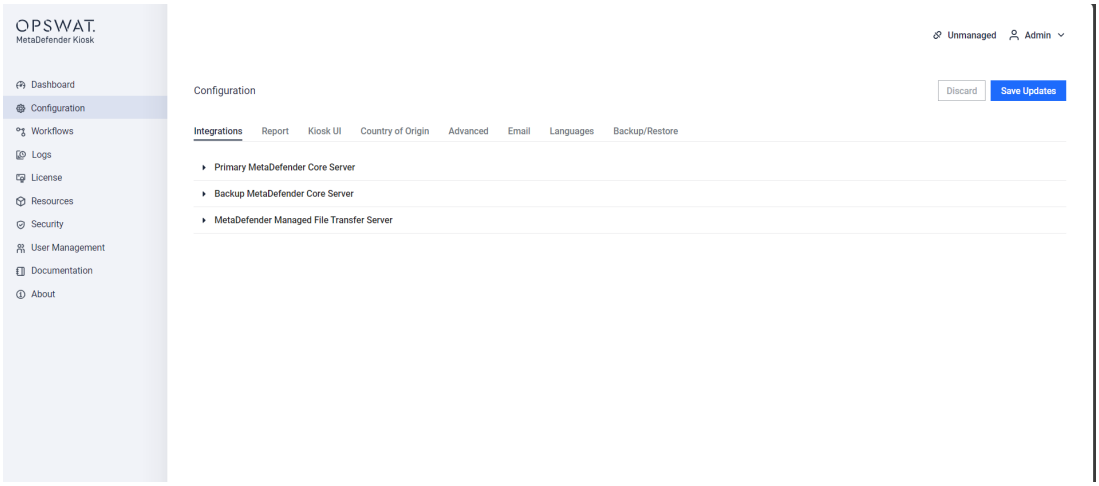
The Dashboard will be the first page that is seen when logging in to the MetaDefender Kiosk Management Console. This page provides a summary of all of the files that have been processed by MetaDefender Kiosk.

Configuration

The Configuration page allows you to configure all MetaDefender Kiosk settings that apply to all users of MetaDefender Kiosk.

Note:

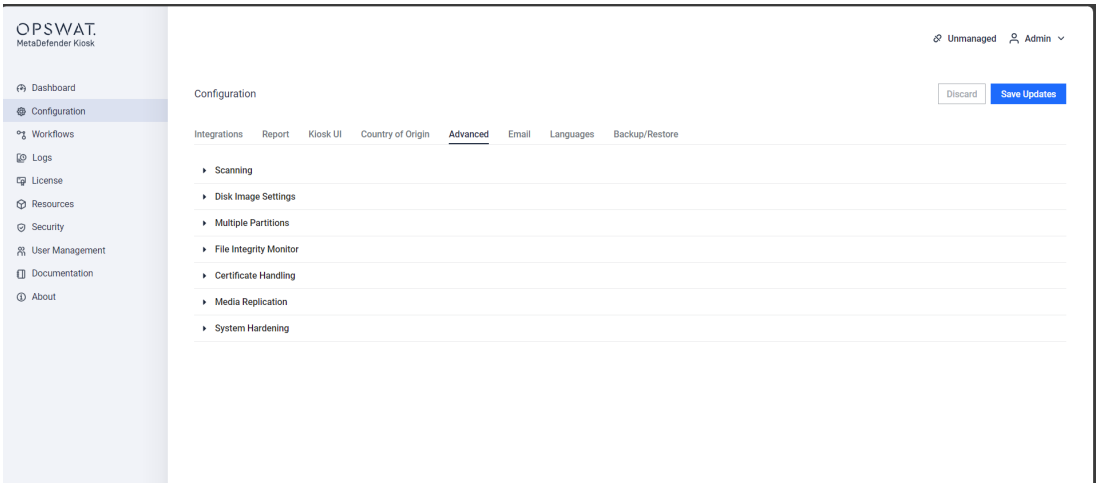
- In case the directory path for session log is not able to created, the default path is used instead.
- Session log can be saved in network shared folder with AD user's credentials that is logged into the Kiosk session for saving privileges. An Admin can enable utilizing the OS logged in user's credentials if the saving initially fails with the AD user credentials.



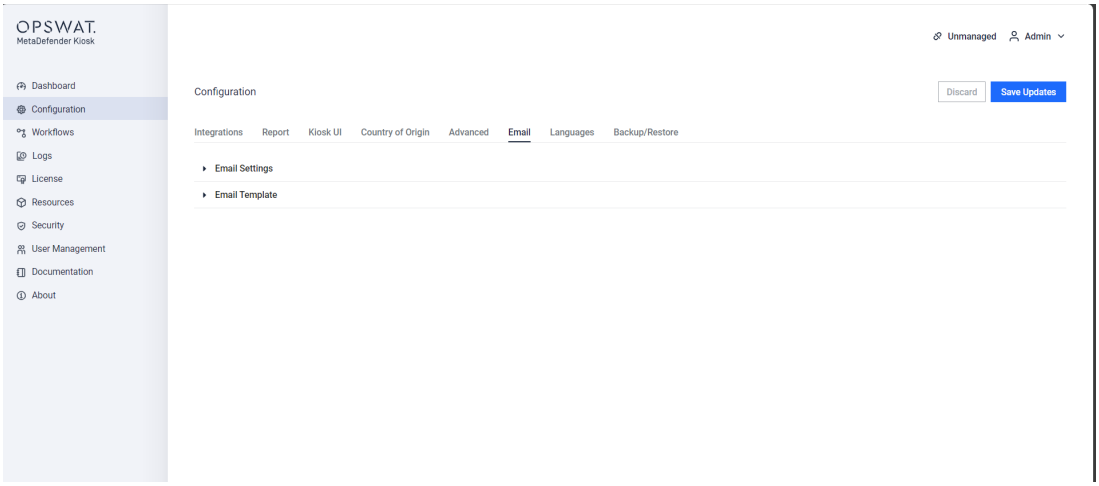
Advanced Configuration

Advanced configuration options can be set by expanding the 'Advanced Configuration' section of the Configuration page.

Advanced Configuration for Scanning



Advanced Configuration for Email


OPSWAT.
MetaDefender Kiosk
Dashboard
Configuration
Workflows
Logs
License
Resources
Security
User Management
Documentation
About
Unmanaged
Admin
Configuration
Discard
Save Updates
Integrations
Report
Kiosk UI
Country of Origin
Advanced
Email
Languages
Backup/Restore
Email Settings
Email Template

UI Localization / Customization

Purpose: change the default language for better localized user experience

The language displayed in MetaDefender Kiosk can be changed from the `Choose Language` drop-down menu in the Configuration section of the Management Console.

The default languages included are:

- English
- Arabic
- French
- German
- Hebrew
- Japanese
- Korean
- Spanish
- Vietnamese

Edit a language

Click `View and edit languages` if you wish to add a language or edit existing languages displayed on the Kiosk UI.

Choose which language to edit from `Choose language to update` drop-down menu. When finished, click `Save Custom` to save changes.

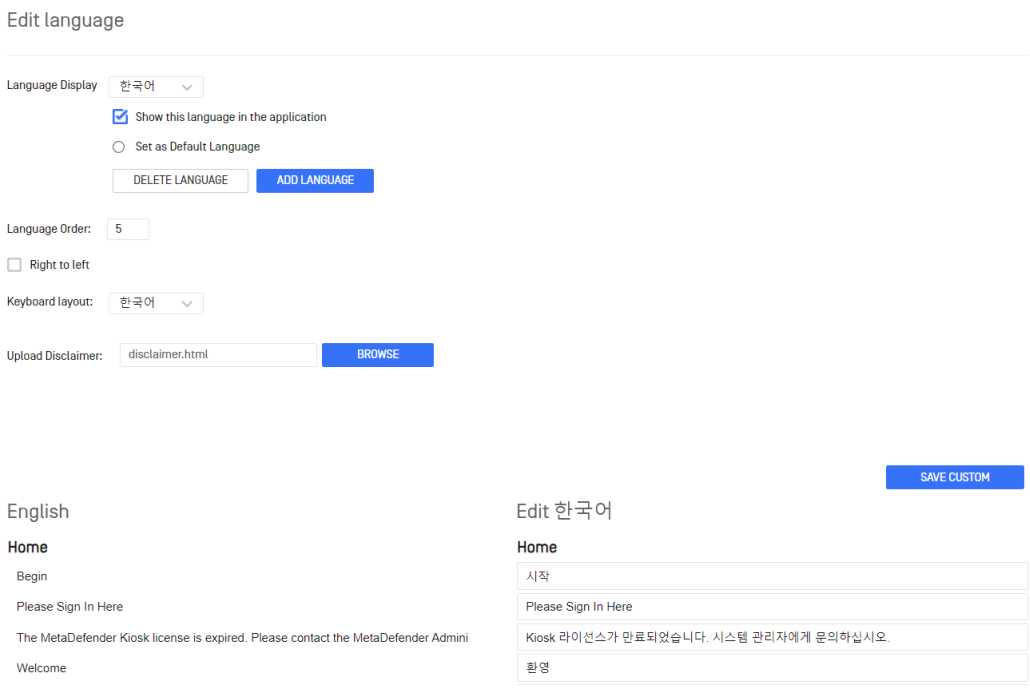


Image: Choose Language Display option on Kiosk configuration page

Info

The default English language translations cannot be edited as it serves as a language template.

To modify the English language, you must add a new language which will serve as a customized English translation.

The languages (including the default English) can be disabled by unchecking `Show this language in the application`

Add a language

Click `Add Language` to add a new language, then type in the desired language name. On the following page, create translations for the text to be displayed in MetaDefender Kiosk. Each string has a max limit of characters to avoid any display issues on the UI. It is recommended to keep messages as concise as possible.

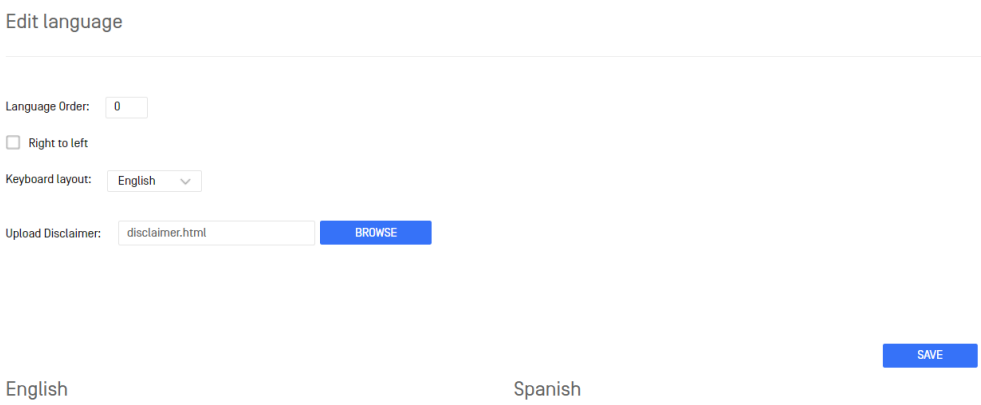


Image: Adding new language on Kiosk configuration page

- If the language you are adding reads right to left, make sure to check `Right to left` option
- Languages can be either disabled or enabled through the Management Console. Disabled languages will not be available to Kiosk users as options.
- The `Language Order` value will determine the order in which languages are displayed to Kiosk users when they are selecting a language in the Kiosk user interface. Lower numbers will be displayed first.
- `Upload Disclaimer` value will show the corresponding disclaimer HTML file of that language. By default, the Opswat's EULA in English will be used. However, you have the option to browse and upload your own customized disclaimer file to replace it. For more detailed information, please refer to Disclaimer Screen Customization

Once finished, click `Save` at the bottom of the page and the language will now appear in the `Choose Language` drop down.

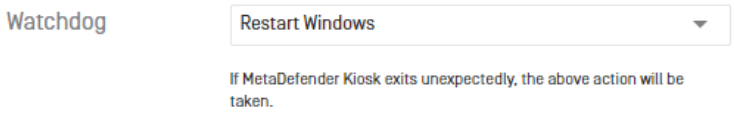
Allow users to select languages

`Configuration -> Advanced Configuration -> Allow user to select languages` controls whether users can select which language to use from the UI. If the option is deselected, the current active language will be locked in and users will not be able to modify the language to display.

Watchdog Behavior

The watchdog is an additional process that monitors the running processes of the MetaDefender Kiosk. In the case where the Kiosk exits unexpectedly, the watchdog will run a specified action to take.

Configure watchdog behavior



Action	Description
Do nothing	No action will be performed, the system will remain on the secure desktop
Restart MetaDefender Kiosk	MetaDefender Kiosk will be restarted while the system remains on the secure desktop For a brief moment, a blank secure desktop will be displayed before the MetaDefender Kiosk starts up again
Log out of Windows	The user currently logged into Windows will have their session terminated and be logged out The system will exit out to the Windows OS login
Lock Windows	The user currently logged into Windows will be locked out The system will exit out to the Windows OS login where the admin must log back into Windows
Restart Windows	The Windows system will be rebooted The system will either return back to the Windows OS login or be logged in to the default Windows user (this is dependent on the system's automatic login settings)

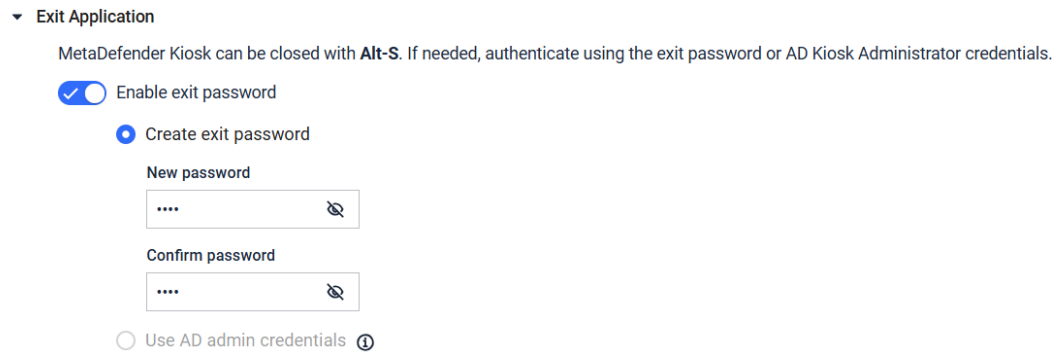
Configuring Global Kiosk Settings

The Configuration page lets you configure global settings for MetaDefender Kiosk.

Protect closing the Kiosk

It is highly recommended to set exit credentials to protect the Kiosk scanning User Interface from being closed by users.

Two options exist to protect exiting the Kiosk UI:



Exit password

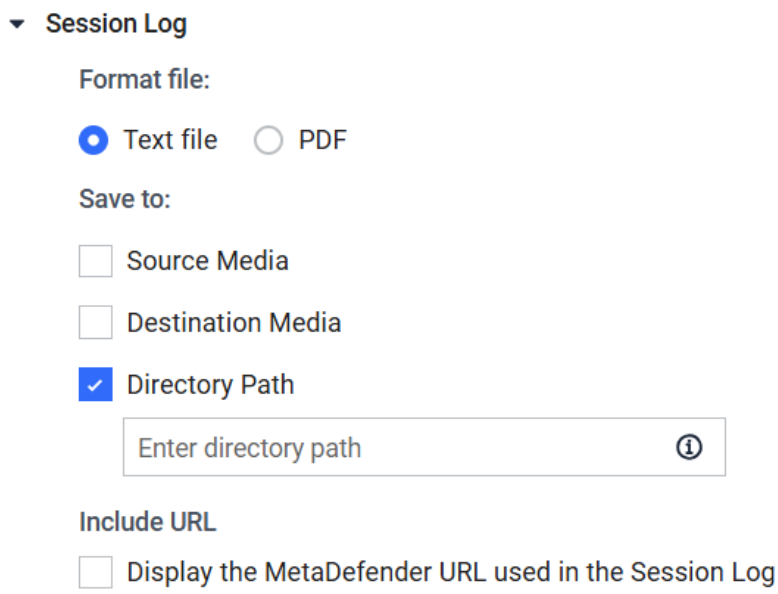
Select this options to require users to enter a password when exiting the Kiosk. After selecting this checkbox, two fields appear: **New password** and **Confirm password**.

Kiosk Administrator's credentials

Select this option to allow AD users, that are assigned as administrative users of the Management Console, to close the Kiosk UI. Upon attempting to close the UI, a prompt will be displayed to enter AD credentials.

Configuring session log files

You can save session log files as a text or PDF file, and choose to save log files to a specific location on the system or to the processed media. By default, MetaDefender Kiosk saves session log files to the Log folder in the MetaDefender Kiosk installation directory.



To save session log files:

1. Select the **Save as Text File** or **Save as PDF** radio button, depending on the output type of the session log files you prefer.
2. Select the destination to save the session logs
    a. By default, Kiosk will automatically save the session logs to the local Kiosk's log folder. The admin can change to a different location by providing **Directory Path**
    b. In addition, the admin can also configure to save session logs to **Source Media** and **Destination Media**
3. **Display the MetaDefender URL used in the session log** allows for the MetaDefender URL, that was used for the session, to be displayed in the log file. This is useful when configuring a backup Core server and determining which server was used for a particular session.

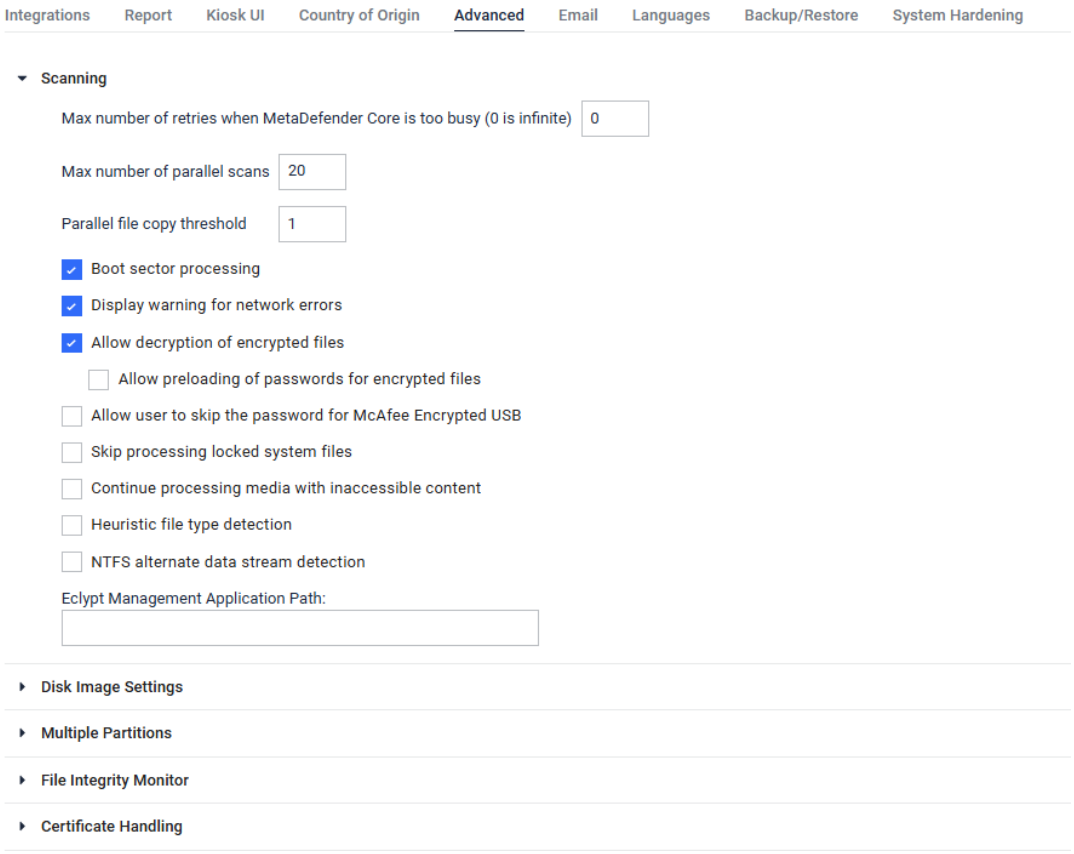
Note: The save options are independent from each other. You can save session logs locally and/or save it to the processed media or disable session log files altogether.

Auto Export Logs

The session and/or file history can be configured to be automatically exported to a specified directory path in CSV format. By default, the history will be exported to the Kiosk's log directory. The frequency dictates how often the automatic export will run.

Setting advanced configuration options

You can set advanced configuration options by expanding the Advanced Configuration section of the Configuration page.

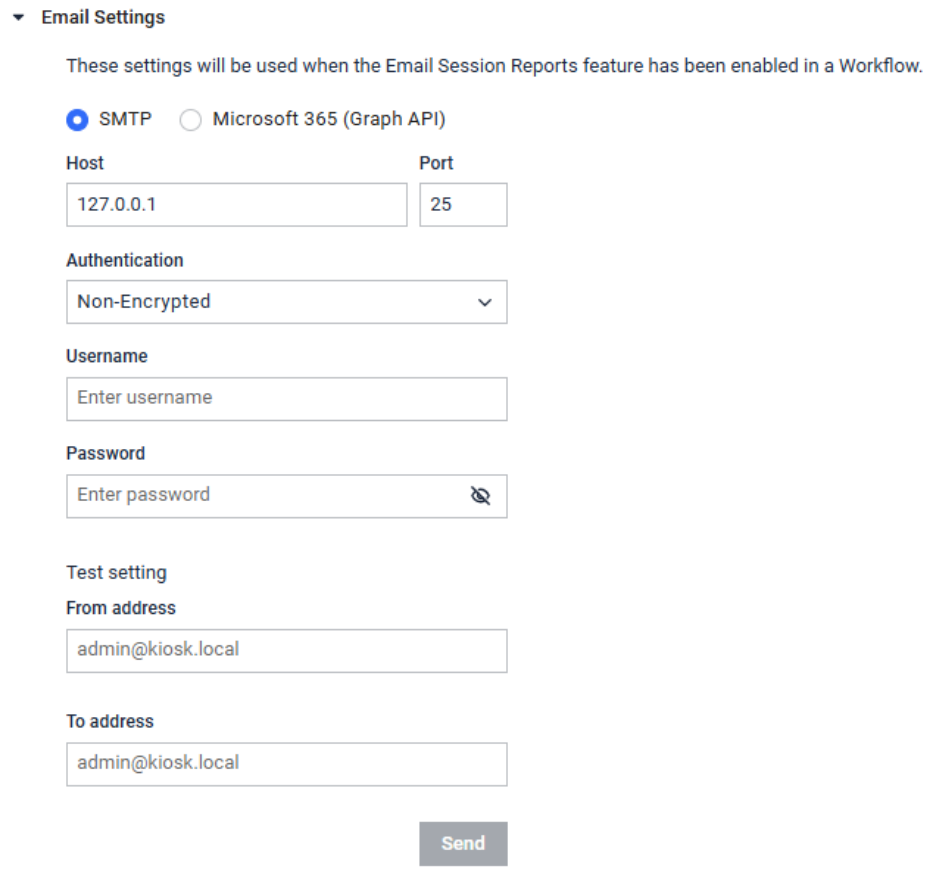


Allow preloading of passwords for encrypted files

This allows users to provide passwords of encrypted archives before scanning. The Kiosk application detects encrypted files and asks users to provide passwords in advance so that the scanning can proceed without waiting for user input.

Email Settings

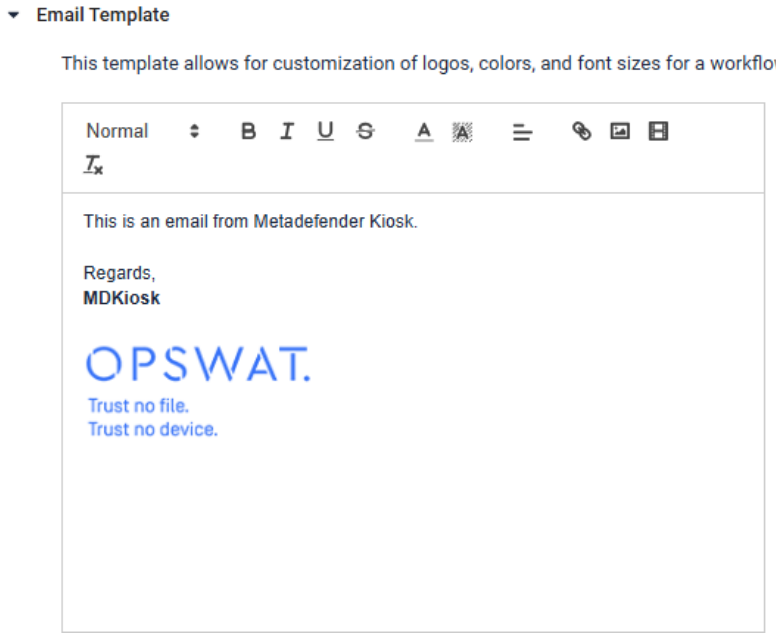
The admin can configure SMTP server to support for email sending at session termination. It's advised to use SMTP mail server, not relay. The username and password are authenticated to login to mail server. Any sender configured to appear as a From field in the email header must be an email address that the username has permission to send as. See Email Session Report or Visitor Management for email header settings



To configure oAuth email authentication with Microsoft 365 (Graph API), please refer to this guide.

The admin can verify if the email configuration is correct by providing existing email addresses as [From Address] and [To Address] and proceeding SEND. [From Address] must be an email that the username has permission to send as.

Email Template



The email template allows Kiosk admin to prepare common email content in HTML format. It will apply for email part in the workflow creation. This template aims to email signature with a company logo. The logo attached in the template should be a low resolution not exceeding 100KB and only one.

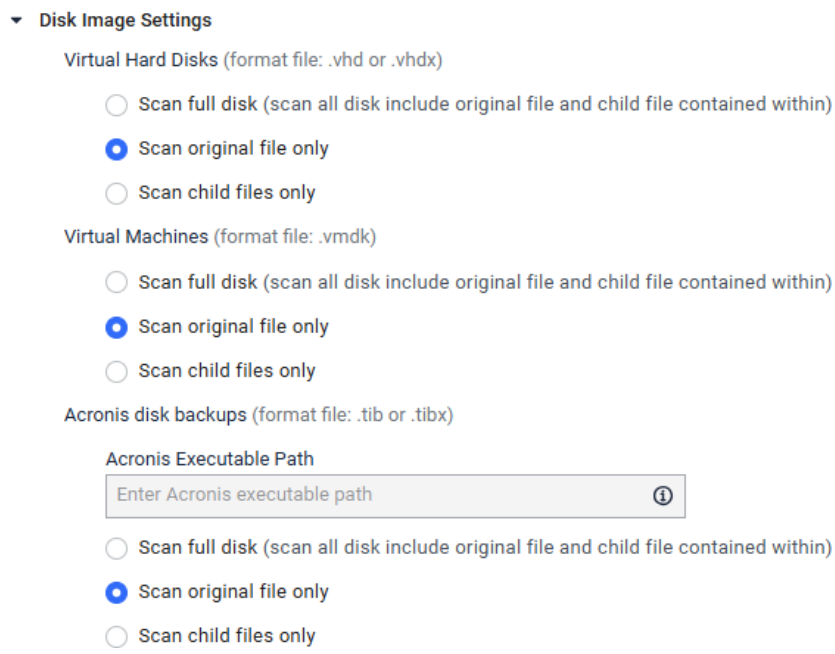
The email template does not apply for testing email.

Disk Image Files

The administrator can configure Kiosk to scan 3 types of disk images:

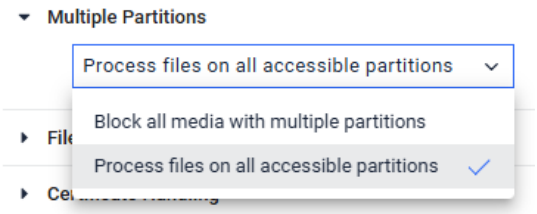
1. Virtual Hard Disks refer .VHD or .VHDX files
2. Virtual Machines refer .VMDK files
3. Arcronis Disk backups refers to .TIB or .TIBX files. The path of the Acronis executable is necessary. For example: C:\Program Files\Acronis\CommandLineTool\acrocmd.exe

Contents within a disk backup created by Acronis can be processed when Acronis backup software is installed on the system. When enabling Kiosk to process the contents in a backup, the path to the Acronis command line executable must be provided (e.g. `C:\Program Files\Acronis\CommandLineTool\acrocmd.exe`). This will allow the disk backup to be mounted to the system for Kiosk to access. The disk backup will be unmounted once the Kiosk session is finished.



See (Link Removed) for more details about the options.

Multiple Partitions



Option	Single Windows Partition	Only Windows Partitions	Mixed Windows and Non Windows Partitions	Only Mac / Linux Partitions
Block all media with multiple partitions	SCAN ONE	BLOCKED	BLOCKED	BLOCKED
Process files on all accessible partitions	SCAN ALL	SCAN ALL	SCAN ALL	SCAN ALL

The SCAN ALL action will mount every partition it can successfully mount. All partitions will be scanned by "Process All." The file browser will have the ability to select files on any partition.

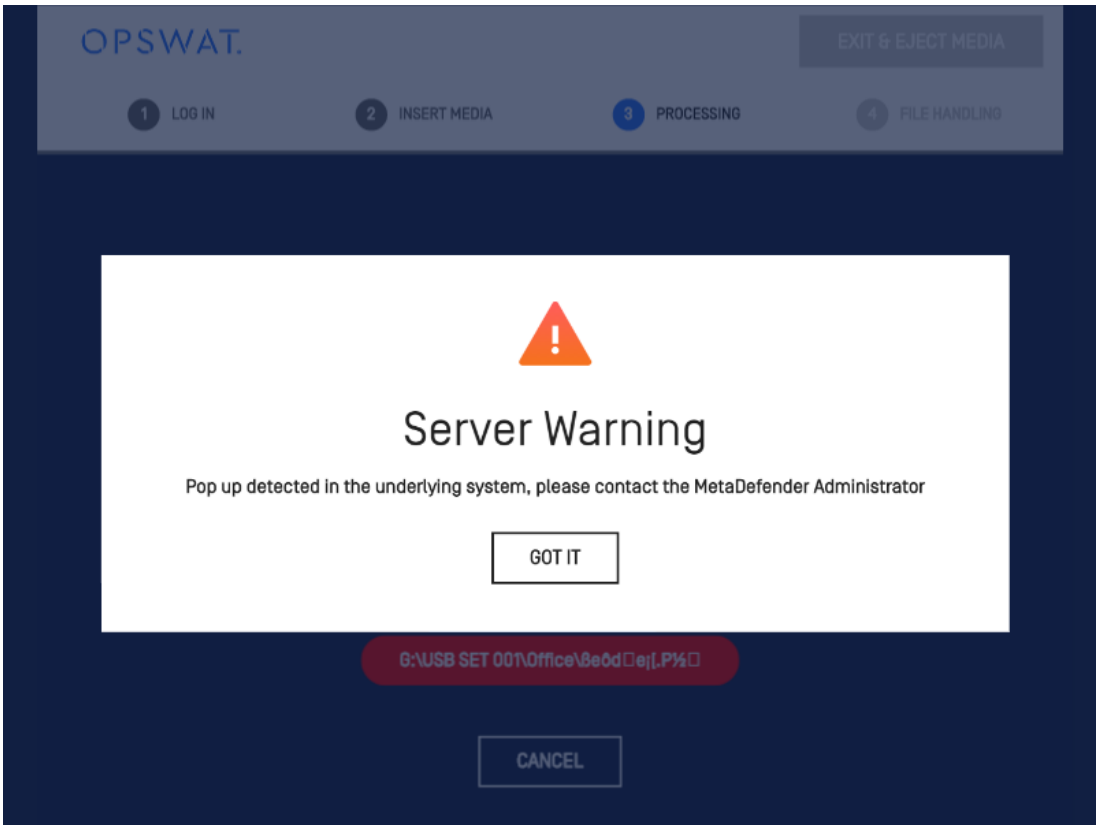
Managing the display language

You can also change the default language displayed in MetaDefender Kiosk from the Choose Language drop-down menu. Options include English, Arabic, Hebrew, Korean, Vietnamese, German, Japanese, Spanish and French . If you wish to add a language to the MetaDefender Kiosk UI or edit the translations of any of the existing languages, click **View and edit languages** .

Pop Up Detection

Enabling pop up detection will allow Kiosk to detect any windows/pop ups open on the underlying desktop and notify the user. Any pop up that triggers the detection will be logged to the Application Log on the WebMC, along with the process that owns it. *Time Open Threshold* indicates how long a pop should be open until Kiosk notifies that a pop up needs attention. *Process Allowlist* specifies any process whose pop ups will be ignored from triggering the detection. *Notification Action* indicates what action Kiosk will take to notify the user:

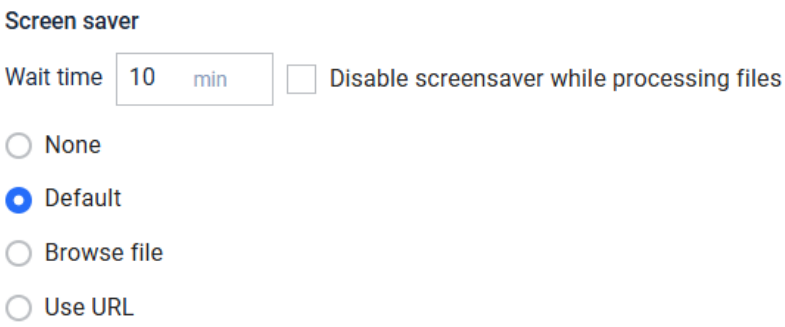
- *Display warning* - a warning will be displayed indicating that there is a pop up that requires attention
- *Display warning and disable Kiosk* - warning displayed with the addition of canceling any running session and disallowing any new session to be started until the Administrator attends to the pop up. This requires closing the UI, handling the pop up and starting Kiosk again.



Screensaver

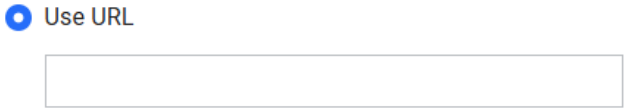
Kiosk screensaver helps protect the LCD lifetime or to play company introduction video or ads. Kiosk disables Windows system screensaver and support an alternative in the settings. By default, a built-in screensaver is selected. The admin can select desired video or image from an URL or local sources.

To change the screensaver settings, navigate to **Configuration**, select **Kiosk UI**, expand **Customize Theme**. Select the source of the screensaver video or image



- **Browse file**: Click on the clip icon to select and upload a local media file to use as screensaver

- **Use URL:** Provide the URL links to the media files. Kiosk must have permissions to access and play the media file.



- **Disable screensaver while processing files:** When enabled, Kiosk will not play screensaver at the file scanning and scan result screens.

Info

- Supported media types:
  - **Video**: MP4, 3GP, MKV, MOV, OGV, MPEG-4, WebM
  - **Image**: JPG, PNG, ICO, GIF, SVG, WEBP
- This list is fully supported when uploading with Google Chrome browser, other browsers can make some of the media types cannot be previewed.
- If the video or URL is invalid, the default will be played instead.
- In OCM mode, [**Browse file**] is disabled.
- Starting from version 4.6.1, the customized screensaver can be retained during the upgrading process.

Self Scan and Screen saver

If Self Scan is triggered while the screen saver is active, the screen saver remains running.

Configuration Field Descriptions and Default Settings

The following table provides a brief description and default values for the Kiosk Configuration screen.

Basic Configuration

Configuration Setting	Description	Default Value	Range
Primary MetaDefender Server	URL of the primary MetaDefender server	(Blank)	
API Key	The API Key of the primary MetaDefender server, if one is set	(Blank)	
Server is a load balancer	Indicates that the primary server is a load balancer for MetaDefender If checked, the API key is disabled	Unchecked	
Periodically test Core servers every # hours	Periodic interval in which Kiosk will send an EICAR test file to test the Core server detection. An alert will be logged if no engines detect the EICAR file.	0 hour	0 disables the periodic check Min: 1 hour
Backup Server	Additional MetaDefender servers for the Kiosk to use if the primary is inaccessible (URL & API Key)	Empty	
MFT Server	MFT servers to be used among different workflows (URL & Admin API key)	Empty	
Printer Setup	Select the color of the printing output: `Black & White` or `Color`	`Black & White`	
Side margins	Left and right margin length	3	0 or greater Recommended settings: 3 for a Zebra printer 200 for a Laser Jet

Configuration Setting	Description	Default Value	Range
Display the MetaDefender URL in the session printout	The URL of the MetaDefender server (Core or MFT) used for a session will be displayed on the printout	Disabled	
Include page numbers	Include the page number on each printed page	Enabled	
Custom introduction message	Add a special header message to the first page of the printout	Disabled	
Custom logo	Add a logo image to the first page of the printout	Disabled	Recommended max image size of 400 x 400
Session Log > Destination Media	Enables a session text/PDF log to be created at the end of a session on the source media. *This will not apply to read-only media such as discs or USBs that are not writable.*	Disabled If enabled, the log will be saved to the root of the source media	
Session Log > Destination Media	Enables a session text/PDF log to be created at the end of a session on the destination media. *This will not apply to read-only media such as discs or USBs that are not writable.*	Disabled If enabled, the log will be saved to the root of the destination media	
Session Log > Directory Path	Enables a session text/PDF log to be created at the end of a session in a specified location (local or network share)	Enabled Logging directory: `<kiosk install dir>\Client\Log`	
Save as Text File / Save as PDF	Specifies whether the session log will be a text or PDF file	Text file	
Display the MetaDefender URL in the session log	The URL of the MetaDefender server (Core or MFT) used for a session will be displayed in the log file	Disabled	

Configuration Setting	Description	Default Value	Range
Wipe Method	Specifies which wipe options to display to the user	All wipe methods shown	0,1,3,7 pass wipe
Exit password	Require password when terminating the Kiosk UI (ALT+S)	Disabled	
Kiosk Administrator's credentials	Require AD Management Console Admin credentials to close the Kiosk UI	Disabled	

Watchdog	Custom action watchdog that will run when the Kiosk UI is unexpectedly terminated	`Restart Windows`	Options:
			`Do nothing`
			`Restart MetaDefender Kiosk`
			`Log out of Windows`
			`Lock Windows`
			`Restart Windows`

Export Session History	Enables auto export of session history (in CSV)	Disabled	
Export File History	Enables auto export of files history (in CSV)	Disabled	
Frequency	Interval between history exports	1 hour	Min: 1 hour Max: 365 Days
Export Path	Directory where the history will be exported to	(Blank - `<kiosk install dir>\Client\Log`)	

Configuration Setting	Description	Default Value	Range
Country of Origin	COO engine detects the country an exe\dll binary originated from and marks the binary as blocked if the country is configured to be forbidden	Disabled	
Image Media	Enables an image of the inserted media to be taken with the FTK Imager configured	Disabled	
FTK Imager Path	The full path to the FTK Imager executable that handles imaging the media (ftkimager.exe)	(Blank)	
Image Type	The image type FTK will output	RAW/DD	
Fragment Size	The size of chunks the image will be separated into	1 GB	0 disables fragmenting the image Min: 1 Max: 1024 (Min\Max per unit: KB - TB)
Compression Level	The compression applied to the image	0	Min: 0 (no compression) Max: 9 (best compression)
Encrypt with password	Enables the image to be encrypted with a password. The password is the name of the user logged in to the session and the id of the session: "<sessionID><username>"	Disabled	

Configuration Setting	Description	Default Value	Range
Encryption certificate path	The full path to a X.509 certificate to encrypt the image with. Supported certificate formats: • PKCS#12 / PFX (*.p12, *.pfx) • PEM (*.pem) • Stand-alone public key only (*.cer, *.crt, *.der)	(Blank)	
MFT Server	MFT entry to upload the image to	(Blank)	
Directory	Directory to upload the image to	(Blank)	

Advanced Configuration

Configuration Setting	Description	Default Value	Range
Max number of parallel scans	Maximum amount of concurrent file processing requests Kiosk will make to a MetaDefender server	20	0 or greater
Max number of retries when MetaDefender Core is too busy	Maximum amount of retries that Kiosk will attempt on a file when the Core server notifies that it is too busy to handle new requests. Once the maximum amount of retries is reached for a file, the session will be canceled.	0	0 for infinite 100 or greater
Boot sector processing	Allows processing of the first 512 bytes of an input media's partitions\disks. When enabled, these boot sector files can be selected during browse or are automatically included when 'Process All' is selected. Boot sector files cannot be included in file handling operations at the end of a session.	Enabled	
Display warning for network errors	Display a warning to the user regarding network issues with the Core server while files are being processed	Enabled	
Allow decryption of encrypted archives	Allows you to input passwords when encrypted archives are detected	Enabled	
Allow user to skip entering a password for McAfee Encrypted USB	In the case that a McAfee encrypted drive is set to unlock via other means instead of a password, a user can skip entering a password	Disabled	
Skip processing locked system files	Enables skipping of system files on media that Core cannot access and will typically result in a failed scan	Disabled	
Continue processing media with inaccessible content	Action to take when media has deeply nested directories that Kiosk cannot access	Disabled	
Mount and scan Virtual Hard Disks	Allow processing of the contents within an VHD\VHDX file	Disabled	
• Scan original Virtual Hard Disks	Enables sending the entire VHD\VHDX file to MetaDefender after all contents have been processed	Enabled	
Mount and scan Virtual Machines	Allow processing of the contents within a VMDK file Only VMDK with Windows file systems are currently supported.	Disabled	

Configuration Setting	Description	Default Value	Range
• Scan original Virtual Machines	Enables sending the entire VMDK file to MetaDefender after all contents have been processed	Enabled	
Mount and scan Acronis disk backups	Allow processing of the contents within an Acronis disk backup	Disabled	
• Scan original Acronis disk backups	Enables sending the entire Acronis disk backup to MetaDefender after all contents have been processed	Enabled	
Acronis Executable Path	The full path to the Acronis executable that handles mounting the disk backup (acrocmd.exe)	(Blank)	
Heuristic File Type Detection	Kiosk will heuristically group similar file type extensions for reporting	Disabled	
NTFS alternate data stream detection	Kiosk will display a warning in a file's details in both the result UI and reports if alternate data streams are detected in the file. Alternate data streams will not be scanned - they will be ignored.	Disabled	
Eclypt Management Application Path	The full path to the Eclypt Management Application that handles unlocking the Viasat drives (ema-ui.exe)	(Blank)	
Choose File Scanning Option (***Kiosk 4.7.2 or newer***)	Available options: • Select files: User can select files for processing • Process all files: User has to process all files in the media • Select or process all files: User can select between 'Select files' or 'Processing all files' options • Disable file processing: Kiosk does not process files	Select or process all files	

Configuration Setting	Description	Default Value	Range
User Interface Timeout	The Kiosk UI will automatically switch back to the idle screen if there is no user action within a specified time on the final screens of the session.	5 minutes	Min: 60 seconds Max: 20160 minutes (2 weeks)
Display disclaimer screen	Display the disclaimer screen to a user when a new session is started	Enabled	
Display scan estimation time	Display the scan estimation time to a user when a scan session is processing	Enabled	
Allow user to browse for files	Allow user to select files before processing media	Enabled	
Allow user to process all files	Allow user to select to process the entire media	Enabled	
Alert user if MetaDefender Core license is close to expiration	Alerts you on the Kiosk idle screen if the Core license is close to expiration	Disabled	
Alert user if MetaDefender Kiosk license is close to expiration	Alert you on the Kiosk idle screen if the Kiosk license is close to expiration	Disabled	
Reboot at end of session	Specifies if the system should reboot after a session is completed or canceled. Exiting the Kiosk UI (ALT+S) during the session is not part of this option.	Disabled	
Allow user to select languages	Allow user to select which language the Kiosk UI's text will be displayed as. If this setting is disabled, the default language selected will be locked in.	Enabled	
Available Keyboards	The keyboards allowed for users to select within the on-screen Kiosk keyboard	All keyboards enabled	
Choose Language	The default language to be used for the UI	English	

Configuration Setting	Description	Default Value	Range
Multiple Partitions	Selects the method for processing files on partitions	Process files on all accessible partitions	
Parallel File Copy Threshold	Enhance performance by maximizing the number of concurrent files copied to the secondary location. This setting applies to all types of secondary locations including Directory, User media, and MFT Server.	1 Default value is recommended for copying to MFT.	Min: 1 Max: 100
Boot Hardening - [Enable] [Disable]	Enables/Disables the process that causes the taskbar on the desktop not to load when Windows is logged in to run Kiosk, thereby disallowing any PC functionality until the Kiosk starts.	Disabled	
Anti-tamper Hardening - [Enable] [Disable]	Enables/Disables security enhancement to prevent escaping the Kiosk UI while running. Your system needs to be restarted to finish the changes.	Disabled	
Active Keyboard Filter	Configure the keyboard filter to disable access certain key on the keyboard. Only available if Anti-tamper Hardening is enabled.	Enabled	
Host	IP or DNS of SMTP server	127.0.0.1	
Port	Port of the SMTP server	25	
Enable SSL	Enable the use of SSL	Disabled	
Username	Username to authenticate to the SMTP server	(Blank)	
Password	Password to authenticate to the SMTP server	(Blank)	

Configuration Setting	Description	Default Value	Range
Email Template	Template for customizing logos, colors, and font sizes for a workflow's email configuration		
Enable (Pop Up Detection)	Enables Kiosk to detect any windows / pop ups open on the system	Disabled	
Time Open Threshold	Threshold, in minutes, for a pop up to be open to trigger notification	5 minutes	Min: 1 minute Max: 60 minutes
Notification Action	Action to be taken when a pop up exceeds the time open threshold	Display warning	
Process Allowlist	Ignore pop ups from the processes listed	(Blank)	
File Integrity Monitor	Enables the File Integrity Monitor, which will shut Kiosk down if any unauthorized changes are made in the Kiosk install directory	Kiosk: disabled	
Server	File Integrity Monitor server location	Kiosk: (blank)	
Port	Port to connect to the File Integrity Monitor server	Kiosk: 0	
Username	User name to log into File Integrity Monitor server	Kiosk: (blank)	
Password	Password to log into File Integrity Monitor server	Kiosk: (blank)	
Verify SSL Certificates	Enables verification of SSL certificates when connecting to Core\MFT via HTTPS	Enabled	
Add CA Cert	Add any self-signed or specialized certificates used for Kiosk to successfully verify	(blank)	

Configuration Setting	Description	Default Value	Range
Log Retention - Application Log	Specifies the length that Application Log entries will exist before being automatically deleted.	Never	Never - 12 months
Log Retention - Session History	Specifies the length that Session History entries will exist before being automatically deleted. File history associated with the expired session history will also be deleted.	Never	Never - 12 months
Log Retention - Service log file size limit	Specifies the size that Service log file will exists before being automatically deleted.	500MB	Min: 25MB Max: 500MB
Size Summary - Display	Displays the total files and size of selected files\folders when browsing for files.	Disabled	
Size Summary - Max size to stop calculating	Kiosk stops calculating the selected files and folders if the accumulated size exceeds this threshold value. This prevents users from waiting a long time when the total size is large.	2 MB	Min: 1 MB Max: 1024 GB

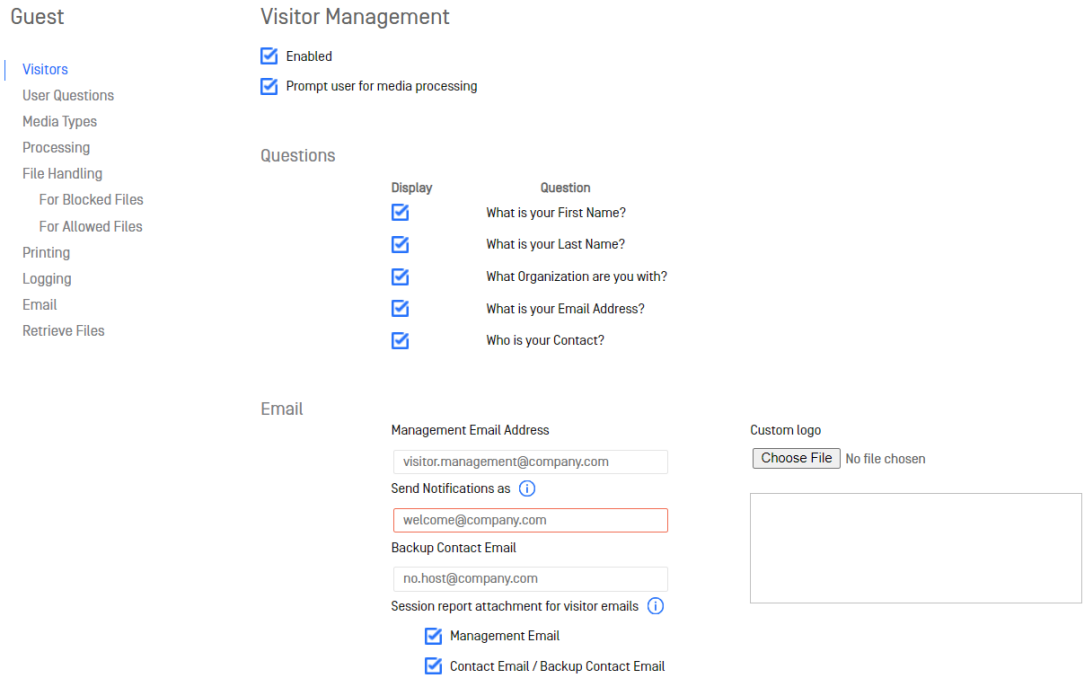
Visitor Management

Visitor Management enables a formal check-in process for guests that visit your organization. The settings for Visitor Management are available for all Guest workflows. The Kiosk admin can configure Visitor Management for individual Guest workflow through the Guest workflow editor.

Visitor questions

When a guest logs in with a Visitor-enabled guest workflow, he is routed through the check-in process. He will be initially presented with check-in questions to gather further information of the visitor. The email answer in the visitor [Questions] will be used to receive check-in summary and session report (if configured) attachment.

Prompt user for media processing



This setting allows for visitors to bring files into your organization. After logging in and answering the check-in questions, the user will be asked if files are being brought in. If so, the user will be routed through the Guest workflow for processing the files. However, even with [Prompt user for media processing] enabled, if nothing enabled in the workflow [User Questions], then the guest will be navigated directly to the workflow for processing the files without any promt windows. User should insert their media into the Kiosk for scanning. If he does not scan anything and decides to [Cancel] or [Exit&Eject], then the check-in is considered incomplete, as a result no check-in summary emails are sent.

Email

Automated emails are sent contacts and management and the guest himself to notify the necessary parties when he has arrived and successfully checked-in. The SMTP settings must be set on the Configuration page to ensure emails are sent.

The session log is always attached to the email.

Management Email Address

Address to send a notification email containing the guest login information and PDF attachment of all the signed agreements for your organization's records.

Send Notification As

This is a mandatory input. It appears as a From field in the email header.

Backup Contact Email

When a guest user checks in, they are required to identify their contact person in the organization. This primary contact will be notified via email that their guest has arrived and completed check-in. If the primary contact's email cannot be found, the backup contact is notified of the guest's arrival along with the login information.

Session report attachment for visitor emails

When a guest finishes his checkin procedure with file processing or retrieval activity, the session report file can be attached in the Management or Contact/Backup email. The admin can configure to attach it or not in the emails.

Custom logo

Logo to include in the PDF document of the agreements signed by the visiting guest.

Badge Printer

Print user information to a badge that the guest can wear. User information:

- Name
- Company
- Contact Name
- Date
- MFT Guest ID (if files were uploaded to MFT)
- MFT URL (url to retrieve uploaded files from)

Configured Printer

Specific printer to be used for printing the guest badge.

Printers

List of printers connected to the system to allow selection of the one to print the guest badge.

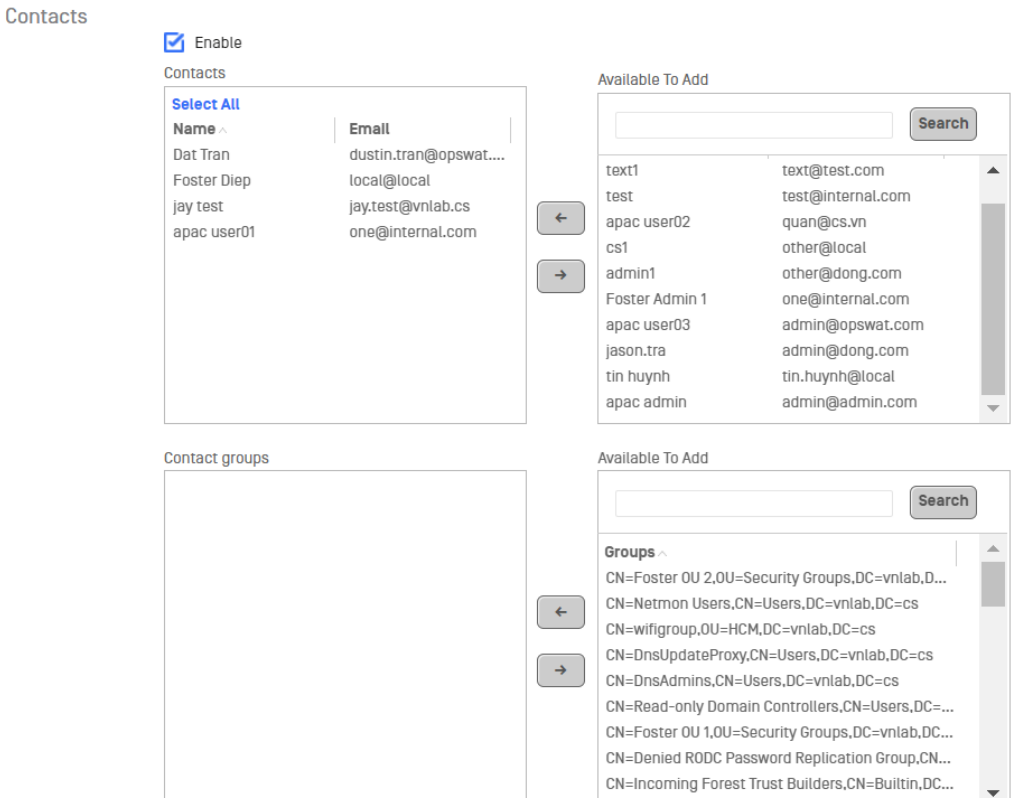
Contacts

During check-in, a guest will be prompted to input their contact's name. While entering the name, filtered results from the Available Contacts will display on the screen to allow for easy selection for the guest.

Available Contacts

List of users that a guest can select when specifying their contacts during check-in. The Contact list is built from Active Directory server. Once AD is configured, the Contacts area will load and display users fetched from AD server. Not all users will be loaded but if the admin scrolls the slider down to the bottom, more contacts will be fetched and displayed. Only users with email address are available to add as Contacts. The Kiosk admin can add users or groups of users as Contact.

The admin can specify a displayName (an attribute in AD server) to search through the AD. This is different from the search in [Properties & Membership] in creating a workflow, where the search accepts sAccountName.



Info
The [Import all AD Contacts] is not available from version 4.5.7. For any previous versions with [Import all AD Contacts] enabled, the upgrade to to 4.5.7+ will not automatically add all users to Contacts but the admin must manually add who as contact as he wants.

Agreements

Specify any agreements to be acknowledged and signed by all visitors. A copy of all the signed agreements will be generated and sent in the management notification email and accessible via the Visitor Log in the management console.

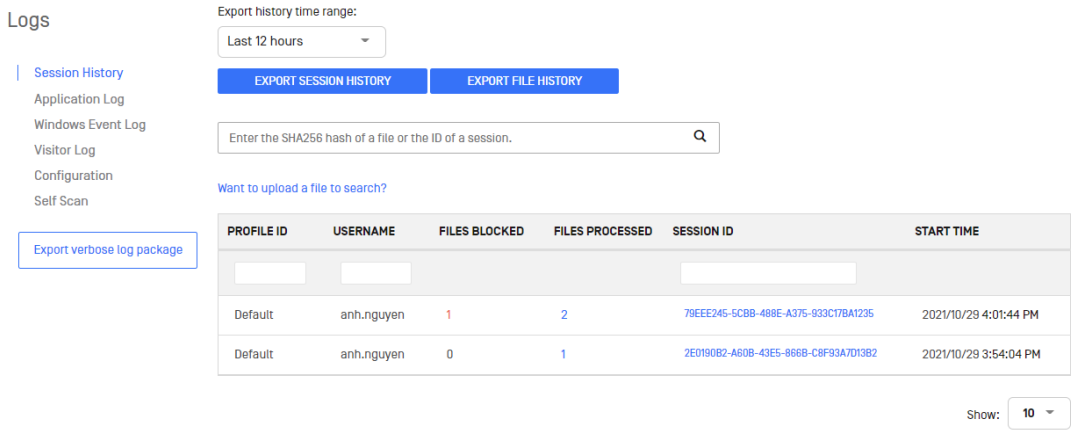
Variables from the guest login can be utilized in the text box of the agreement:

- %GUEST_NAME% - the guest's full name
- %COMPANY% - guest's company

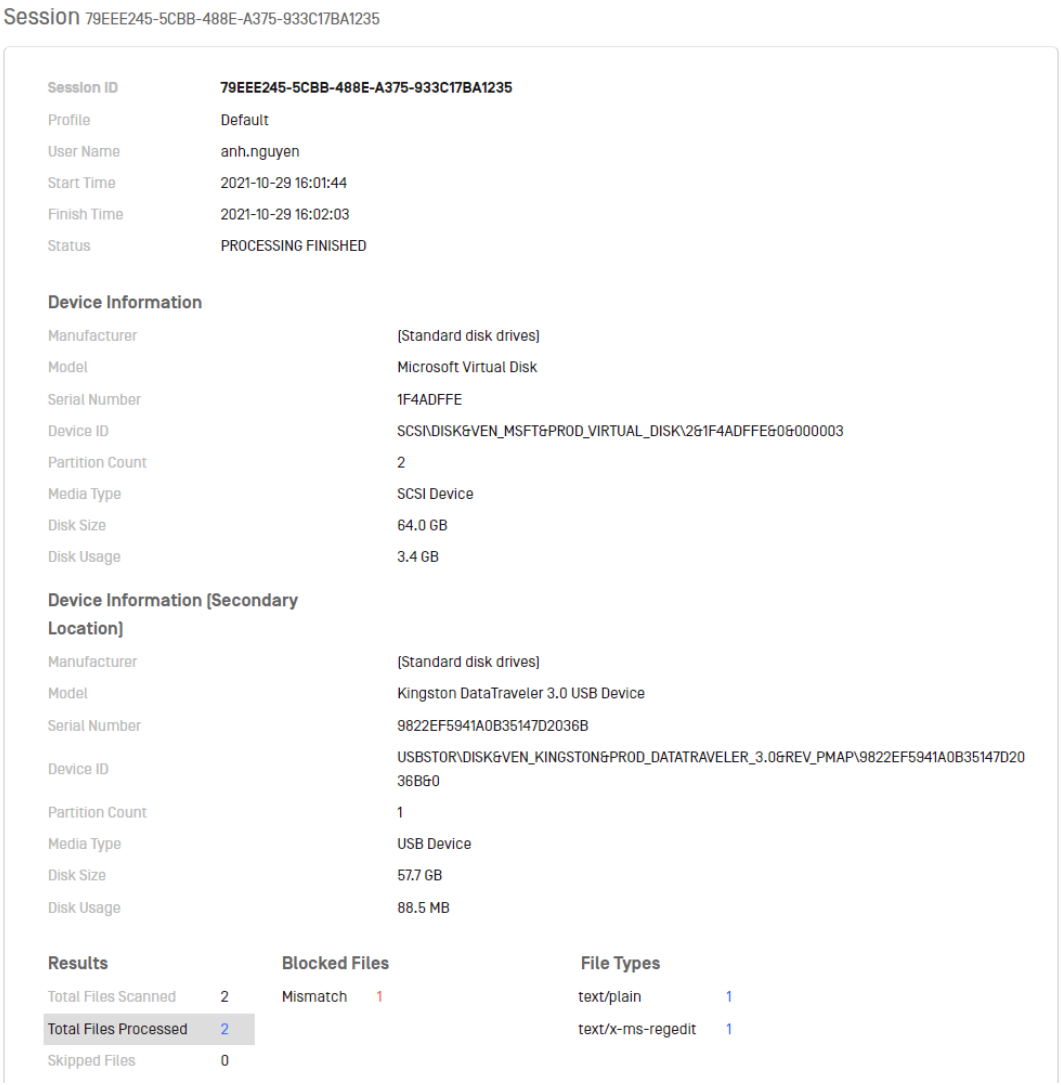
Session Logs

Viewing session details

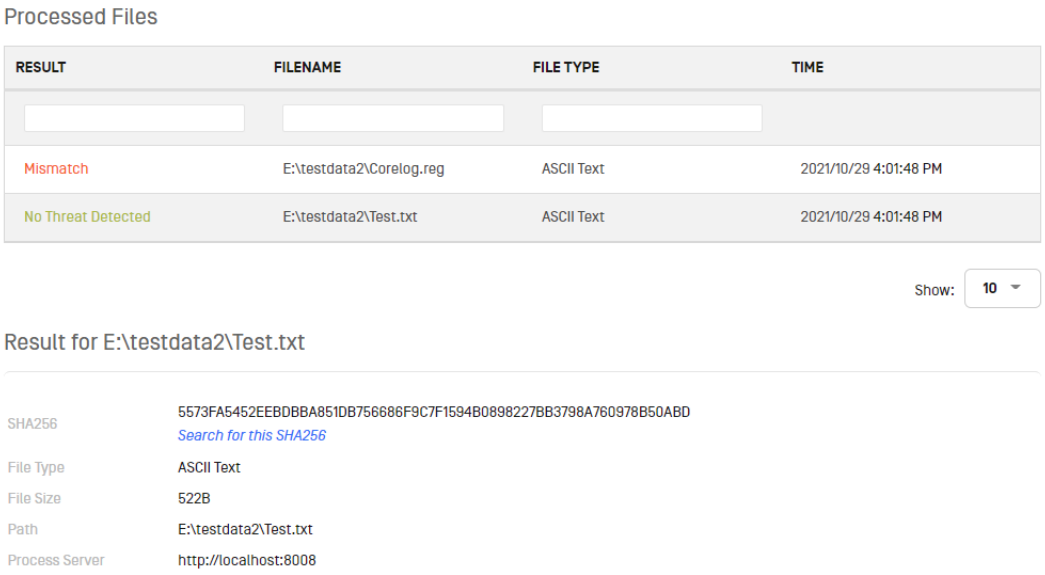
MetaDefender Kiosk displays the most recent scanning sessions on the Logs page.



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



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



Export Session or File History to CSV

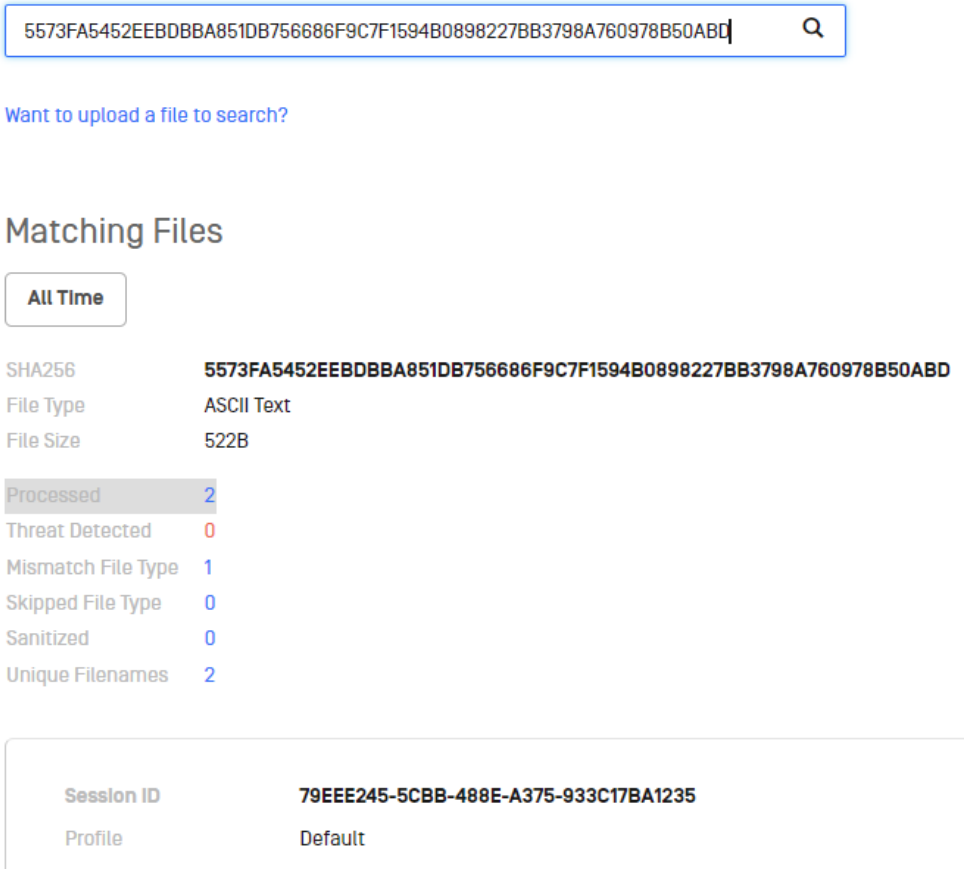
The session or file history can be exported, on demand, to a CSV file based on the time range selected. Automated history export can be configured on the Configuration page.

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.

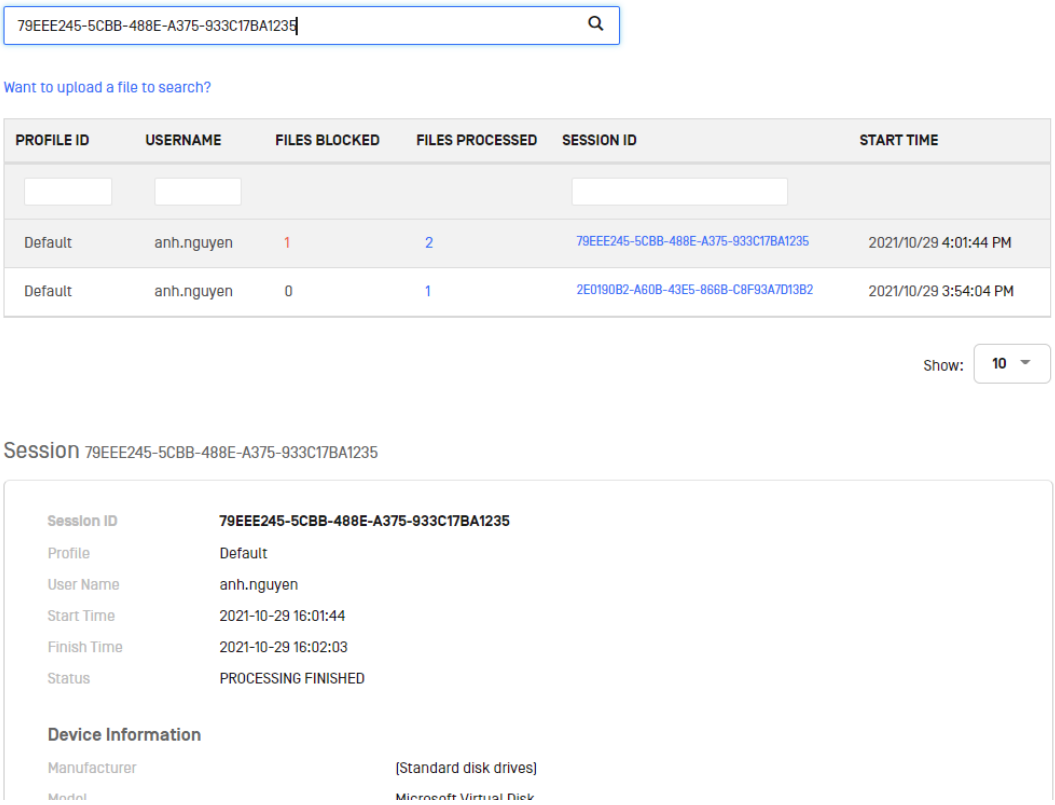
Exported file history contains information on *Session ID, User ID, File Name, SHA-256 hash, Scan Result, Scan Result Description and Scanning System.*

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.



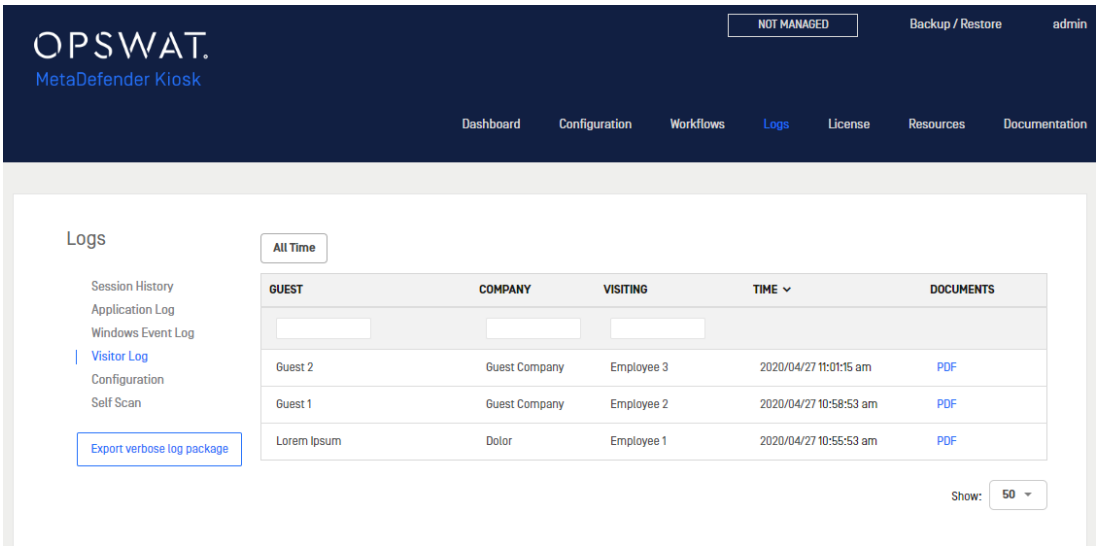
Searching by specific file name

Click **Want to upload a file to search** to upload a file to check if it has been processed by MetaDefender Kiosk.

If you search by SHA256 hash code, MetaDefender Kiosk displays a summary of all of the times that file was processed by MetaDefender Kiosk.

Visitor Logs

History of visitors\guests can be viewed in the Logs → Visitor Log section of the Kiosk's Management Console.

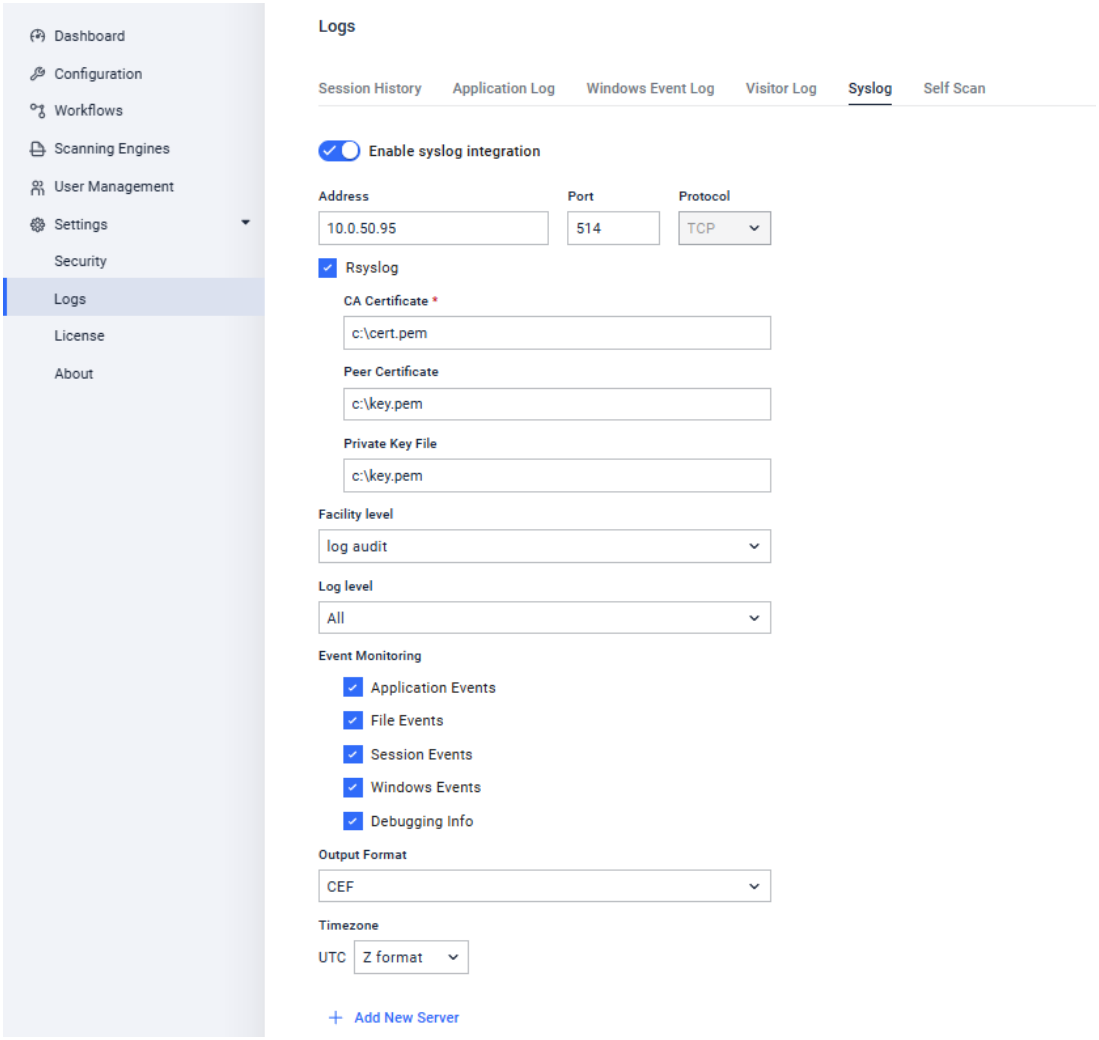


The history table contains pertinent information of the specific guest check-in.

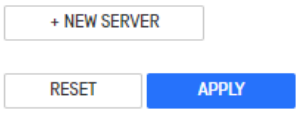
Column	Description
Guest	Full name of the guest
Company	The company from which the guest is visiting from
Visiting	The contact person in your organization the guest is visiting
Time	The time in which the guest checked-in
Documents	Download link to retrieve the PDF document of the agreements the guest signed If blank, the guest was not prompted to sign any agreements

Syslog settings

The syslog settings are configured under Settings → Logs → Syslog:



Setting	Description	Default Value
Address	Where the syslog messages are sent	
Port	The open port for accepting syslog messages	514
Protocol	Select between using UDP or TCP	UDP
Enabled	Enables usage of the syslog server	Enabled
Rsyslog	Enables usage of syslog over TLS	Disabled
• **CA Certificate**	Path to CA certificate. Used to sign all of the other certificates. The CA cert must be trusted by all clients and servers.	<empty>
• **Peer Certificate**	Path to the certificate that conveys the Kiosk client identity	<empty>
• **Private Key File**	Path to the private key file, used to properly decrypt the traffic	<empty>
Facility Level	How Kiosk appears in syslog messages	User-level
Log Level	Determines which messages get sent to the syslog server, it filters out any message less important than that selected	All
Event Monitoring	Determines which types of events are logged	Application File Session
Output Format	Select the format of the message between standard "syslog" or "CEF"	syslog



Select **new server** to add a new syslog server to the list; **remove** to delete a server. Select **reset** to revert the settings back to how Kiosk is currently configured. Select **apply** to set Kiosk settings to how they appear on this page.

syslog Message Format

The KIOSK syslog message format follows the BSD syslog standard:

```
<PRI> <Timestamp> <Hostname> <Product ID> <KIOSK Process ID> <eventCode> <logType> <Message>
```

Example: <14> 2025-03-07T15:15:15+09:00 Kiosk-K1001 MDM[12752] eventCode='000000', logType='databaseLog', Configuration reloaded

Component	Description	Value(s)
PRI	The priority field, combining the facility and severity level	Following the BSD legacy syslog. <PRI> = (<facility> * 8) + <severity> Facility values (between 0 and 23) and Severity values (between 0 and 7)
Timestamp	The timestamp of the message.	Timestamp follows the **ISO 8601** standard.
Hostname	The system name of KIOSK	-
Product ID	Short product ID	MDM
Kiosk Process ID	The process ID of Kiosk	[#]
eventCode	6 digit code to indicate the type of event	**000000** - Unclassified **100000** - Allowed file found **100001** - Blocked file found **100002** - User successful login event **100003** - Configuration changed **100004** - UI event **100005** - Service event **100006** - Authentication event (error or failure) **100007** - Database event **100008** - Device event **100009** - HTTP event **100010** - Session event **100011** - File event **100012** - Low disk space event **100013** - CimTrak deny event **200000** - Session ended
logType	Event monitoring log type	**databaseLog** - Application Events **fileLog** - File Events **sessionLog** - Session Events **windowsEventLog** - Windows Events **serviceLog** - Debugging Info
Message	The content of the message	Text or JSON formatted content

CEF Message Format

Base Format: CEF:<Version>|<Vendor>|<Product>|<Version>|<EventCode>|<Message>|<Severity>|<Extension>

Example: CEF:0|OPSWAT|MDM|4.7.3.2454|100010|sessionLog|6|msg=Configuration reloaded

KIOSK syslog severity levels

Numerical Code	Severity
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Information
7	Debug

Alert Sound Customization

To change the alert sound when blocked files are detected, replace <Kiosk install directory>\Client\en\resources\sounds\alarm.wav with your own .wav file.

The file name must be maintained or MetaDefender Kiosk will not recognize the sound to play.

Branding and Logo Customization

Some of the images and logos in the MetaDefender Kiosk end user interface can be changed by replacing the images installed. The original dimensions of the images are expected to be preserved for optimal display.

Theme Customization

Customize Theme interface is only available on Kiosk 4.7.4 or later
For Kiosk 4.7.3 or older, text color changes are not supported, and logos need to be uploaded to the local folder. Please prefer to Branding and Logo Customization for Kiosk 4.7.3

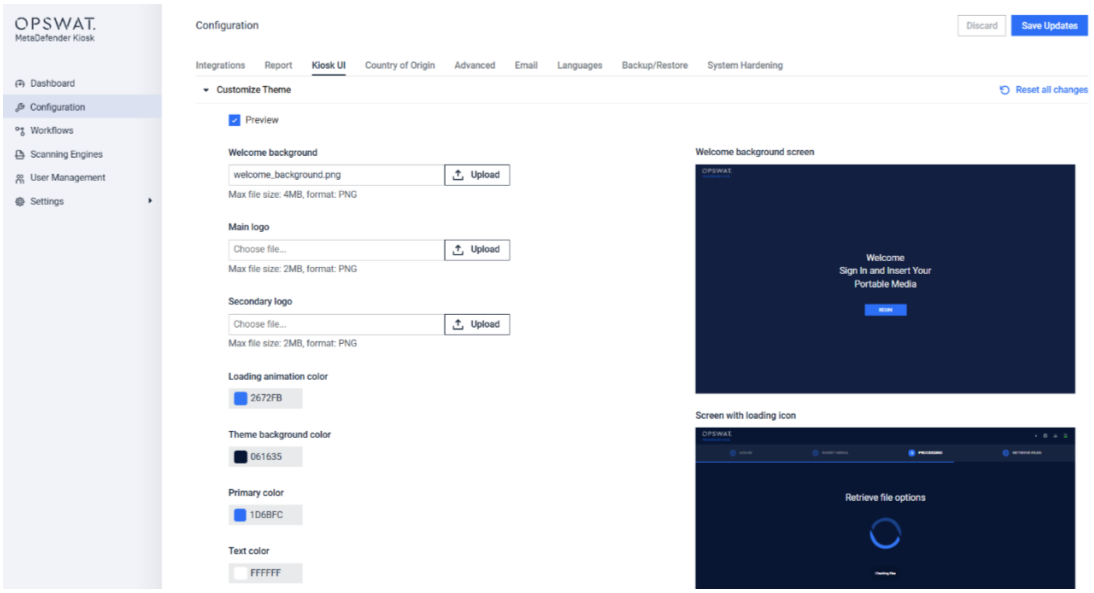
Known issues when importing a configuration from older Kiosk versions!
Logos may not be fully restored when importing an older configuration:

- Top center logo ("logo.png") will not be restored
- Footer logo ("secondary-logo.png") will not be used. It will instead use the provided Header logo ("header-logo.png") or OPSWAT's default logo.

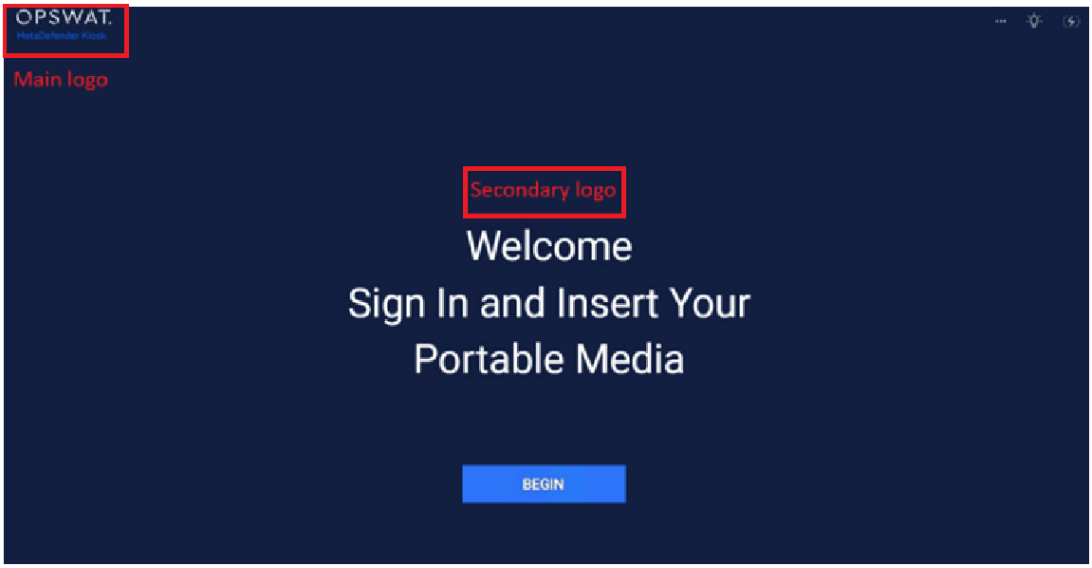
Footer Logo ("secondary-logo.svg") is no longer in use
Kiosk 4.7.4 or later does not use Footer logo ("secondary-logo.svg"), instead, it will use Main logo.

In Kiosk version 4.7.4 or later, we introduce "Customize Theme" interface allows administrators to interactively change logos and colors.

To customize the Kiosk UI, navigate to **Configuration**, select **Kiosk UI**, expand **Customize Theme.** Preview option allows administrators to see real-time changes when logos or text colors are changes.

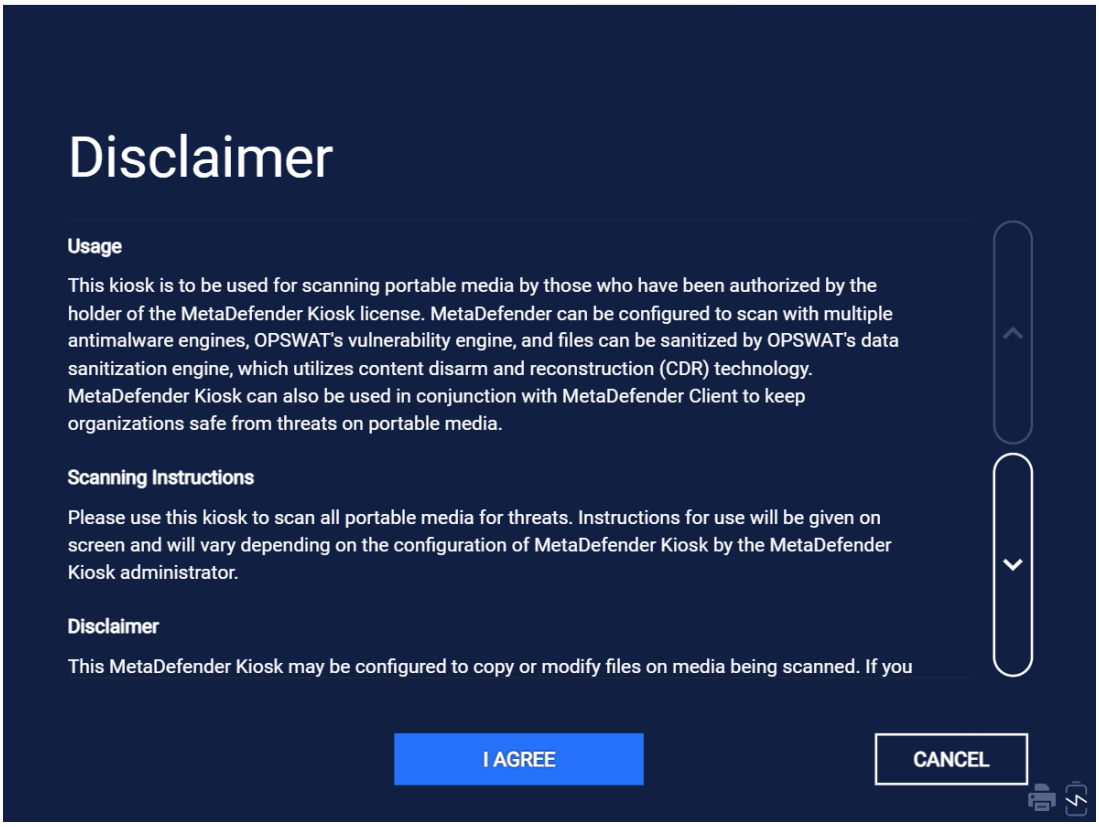


Logo positions:



Disclaimer Screen Customization

As default setting, the disclaimer screen at the beginning will show the OPSWAT's EULA (End-User License Agreement) in English.



To change content of this screen to specific languages, create and upload your own customized disclaimer file at `Edit language` configuration page.

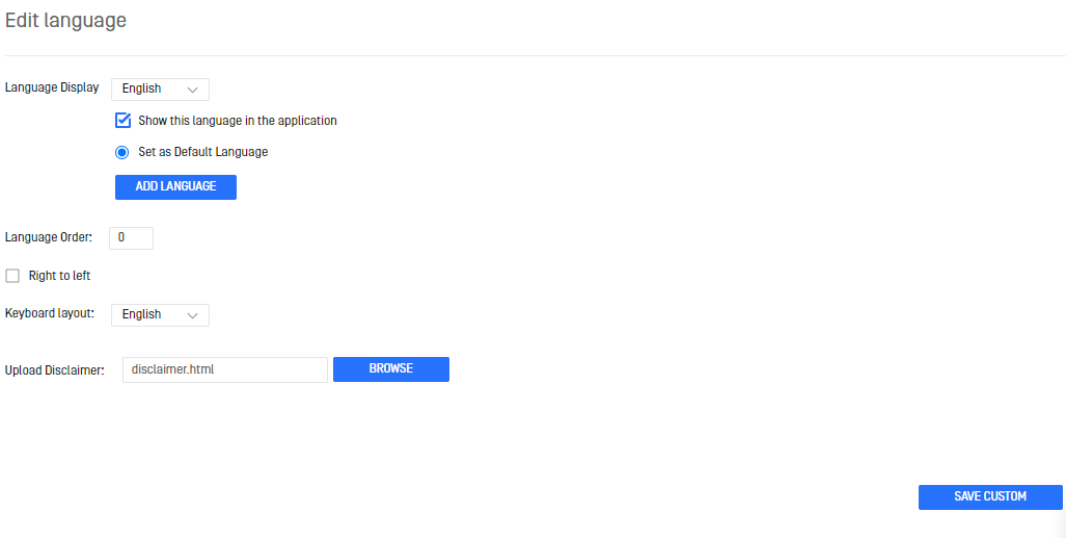


Image: "Upload Disclaimer" option on Kiosk configuration page

The reference disclaimer file can be found at following file directory on Windows: `C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\en\resources\disclaimers\disclaimer.html` .

You can also create your own customized disclaimer file following this guideline:

- File format is .html
- You can only use limited HTML Elements only, with heading `<h>`, paragraph `<p>` and line break `<br>` tags

For example:

html

```
<h6>Heading 1</h6>
<p>Paragraph 1</p>
<br/>
<h6>Heading 2</h6>
<p>Paragraph 2</p>
```

If disclaimer file is valid and uploaded successfully, it will be shown in `Upload Disclaimer` value with the name following the format `disclaimer_{lang_id}.html`

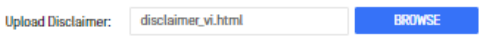
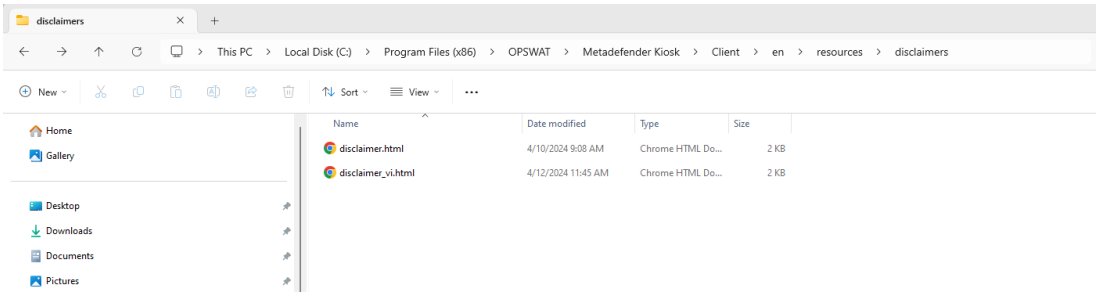


Image: Click Browse to upload your Disclaimer file

The corresponding HTML file will be also added to the same folder directory of the reference file.

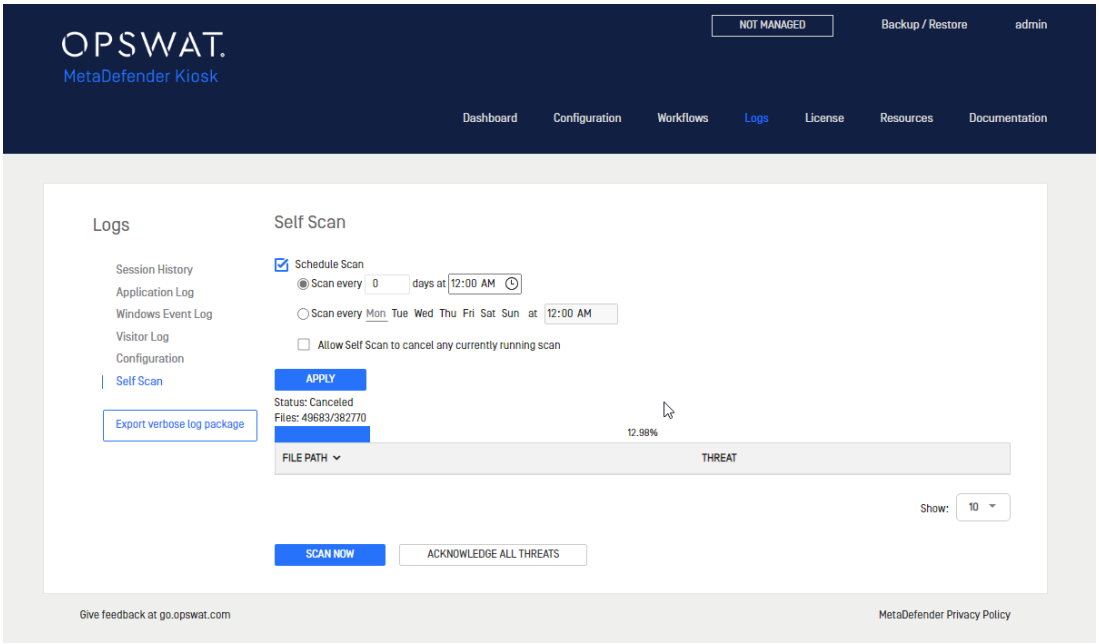


Info

- Default EULA will be shown if there is no disclaimer.html or valid customized disclaimer file of a specific language in the disclaimer folder.
- Customized disclaimer files will be kept during upgrading Kiosk.
- From verion 4.6.7, customized disclaimer files will be included in the backup configuration settings archive to restore disclaimer settings on this or a different Kiosk system.

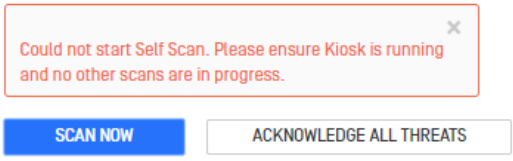
Self Scan

MetaDefender Kiosk has the ability to do a full scan of the system drive to search for threats and shut down Kiosk if necessary. The Kiosk UI must be up and running for this feature to work. It is recommended that in a networked environment that you remotely access the Kiosk's web management console to initiate the on-demand self scanning feature. Configuration options for this feature are found in the Logs section. You can choose to scan the system now or schedule scans to reoccur at the time of your choosing after a configurable number of days or on certain weekdays.

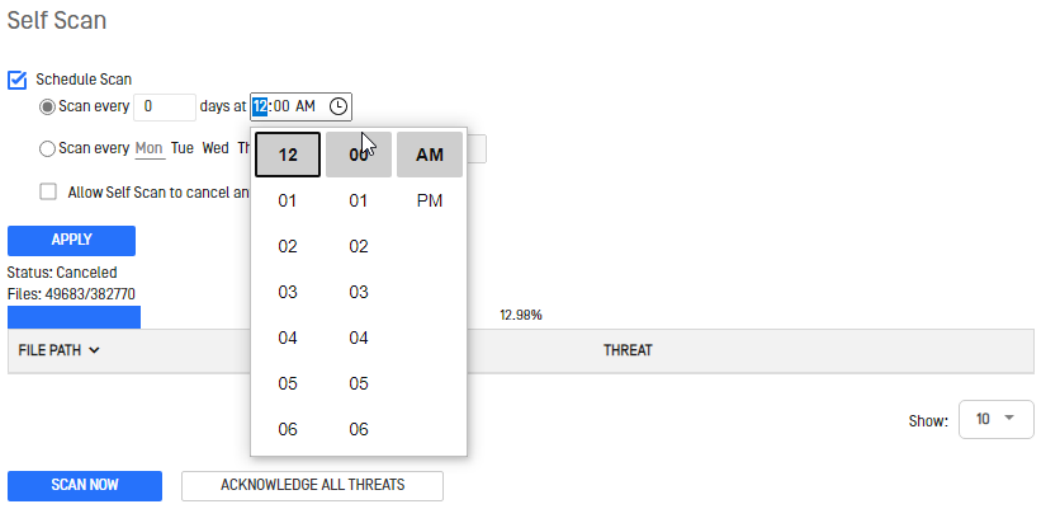


Scan Now

Clicking the "SCAN NOW" will cause Kiosk to immediately start a Self Scan if no other scans are running. If the Kiosk UI is not running or another scan is currently in progress you will see the following error:



Scheduling Self Scans



Checking the "Schedule Scan" checkbox will open up the Self Scan Scheduler where you can configure Kiosk to run a self scan at a specific time after a certain number of days or on certain weekdays.

The first option, the value for "days" must be greater than 0. Setting this value to 0 will disable scheduled self scans.

The second option, you could have multiple choices. At least a weekday must be selected.

By default, the Self Scan will not run if any other scans are currently running. This can be bypassed by checking the "Allow Self Scan to cancel any currently running scan" checkbox. WARNING: This will cancel any scan that is running during the scheduled time and you may not get the full results from the canceled scan.

Acknowledging Threats

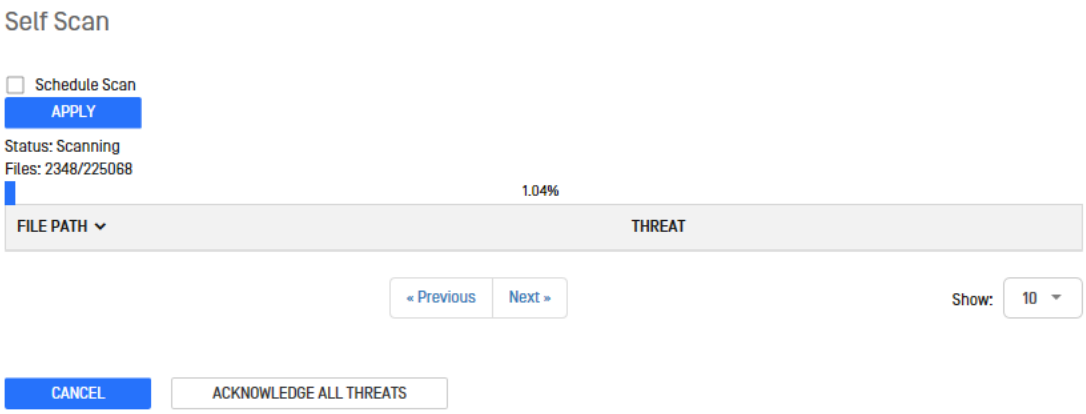
Kiosk Self Scan will run a scan based on the settings in the Default Kiosk workflow. If any infected files are found, the Kiosk UI will be disabled and show a message alerting the user to contact the Kiosk Administrator. Any files marked "Infected" by this scan are displayed on the table with File Path and Threat information. Your Kiosk administrator can use this information to investigate these files if needed.

If the Kiosk is managed by My OPSWAT, that specific Kiosk instance will receive a critical health status alert to notify the Administrator.

Health status message on My OPSWAT

Once the Kiosk Administrator has investigated these files, the "ACKNOWLEDGE ALL THREATS" button is used to re-enable the Kiosk UI and clear the threat information from this table.

Monitoring Running Scans

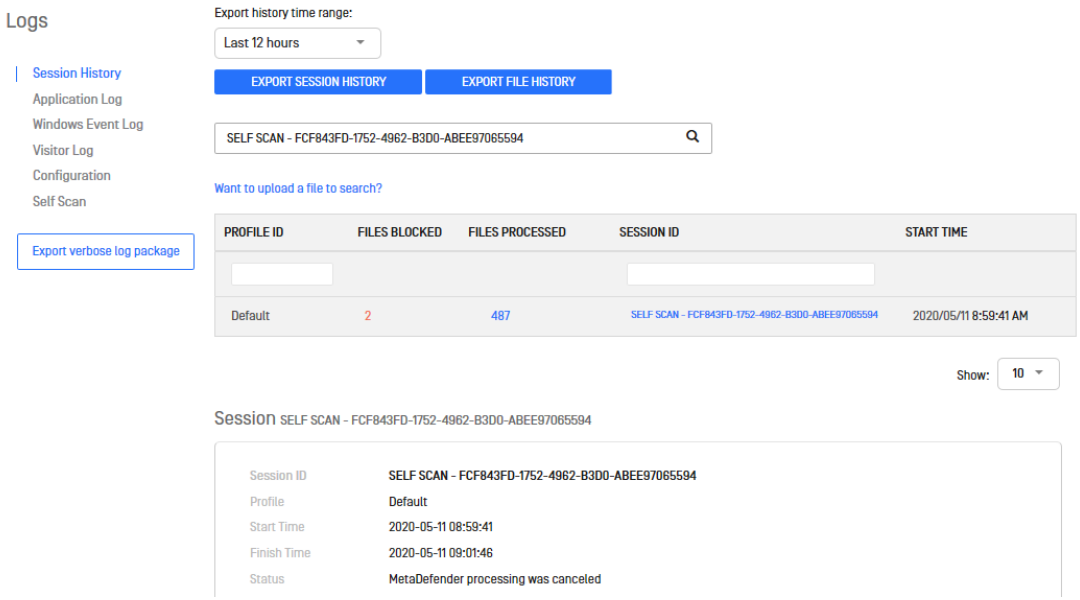


You can monitor the progress of the Self Scan from this same configuration page. Here you can see the current status, how many files have been scanned, and a progress bar showing the percentage complete.

Self Scans can potentially take hours to complete based on the size of the system hard drive. In the event you need to cancel a Self Scan you can use the "CANCEL" button. This will stop the Self Scan and free up the Kiosk UI for other scans.

Checking Self Scan Results

All threats found during a Self Scan will be displayed on the Threats table but you can also see the full scan results in the Session History page in the Logs section. All Self Scans will have "SELF SCAN -" at the beginning of their Session ID.



Developer Guide

Custom Authentication Module

This section provides instructions for developers who intend to build or integrate their own authentication method of their users into MetaDefender Kiosk. We recommend that you have a strong understanding of C/C++ before reading this section.

The bundled code included in this section is a sample of how the authentication module can be implemented. You should modify the contents in each method described in this section to accommodate your integration needs. You can remove any additional methods in the sample code not described in this section if not needed.

> **Info**
> Any configuration pertaining to the custom authentication module are not saved if you uninstall and re-install MetaDefender Kiosk. You must keep a copy of your module before uninstalling and then copy it back to the same directory once your installation or upgrade is complete.

System requirements

The system requirements for implementing custom authentication are as follows:

- MetaDefender Kiosk 3.2.0 or later
- Visual Studio 2017 or later
- .NET 4.5 or later for running the sample UI in the `Custom Authentication Sample` (**optional**)

Steps to deploy custom authentication

The steps necessary to deploy custom authentication are as follows:

1. Obtain a custom authentication template package from the My OPSWAT downloads
2. Implement the custom authentication interface & build the custom authentication module (`authenticationModule.dll`)
3. Deploy the custom authentication module
4. Configure MetaDefender Kiosk to use the custom authentication

---

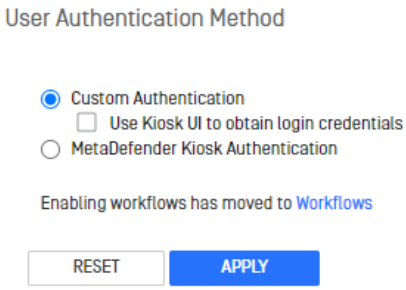
Enabling custom authentication

After successfully building the custom authentication module, you can enable the module.

1. Place the module (`authenticationModule.dll`) in the expected directory (e.g., `<Kiosk Install Directory>\Client\Authentication`)

2. Open the MetaDefender Kiosk Management Console and go to the `Workflows` tab
3. Within the `Employee Workflows` section, click on `User Authentication Method`
4. Select `Custom Authentication` and click **Apply**

> **Info**
> If Custom Authentication does not appear, the authentication module is either named incorrectly or not in the expected directory.



Custom authentication template

The following section describes the C++ code in the custom authentication template.

Init

This is the first method called when the Kiosk service starts up and loads the authentication module. Any dependencies necessary to initialize for the module should go here.

cpp

```
int Init
(
        bool *showUI
)
```

Arguments	Description
showUI	Output indicates if the authentication module has a UI to display to the user • **True:** Has a UI • **False:** Has no UI

Return Values	Description
0	The module initialized correctly
Non-zero	Initialization failed and the module cannot be used

Verify

This method initiates the authentication process to run. The return value is not a result of the user passing authentication. It indicates if the authentication process was successful or not.

cpp

```
int Verify
(
        wchar_t **verifiedID,
        wchar_t *desktopName,
        wchar_t **password
)
```

Arguments	Description	Notes
verifiedID	The ID associated with the user that successfully authenticated. If a user is denied, then this is empty.	Implementer must allocate the memory required
desktopName	MetaDefender Kiosk uses a second desktop for security reasons. If your authentication process has a UI to display to the user, this will indicate the desktop in which your authentication process will be launched.	Disregard if your authentication process does not require a UI
password	The verified user's credentials which allows Kiosk to handle post processing permissions. If you do not want Kiosk to have the user's permissions, leave this empty.	Implementer must allocate the memory required

Return Values	Description
0	Verification ran successfully
Non-zero	Verification failed to run

Deinit

This method is called when the Kiosk is stopped. Any resources acquired by your module should be released and any unsaved data should be stored.

cpp

```
int Deinit()
```

Arguments	Description
	No arguments are required for this function

Cancel

This method is called when the user tries to cancel while verification is running.

cpp

```
int Cancel()
```

Arguments	Description
	No arguments are required for this function

Return Values	Description
0	The cancel request was accepted
Non-zero	The cancel request was denied

FreeString

This method is called to free allocated memory for `wchar_t **`. Kiosk calls this function when finished with the values allocated by your functionality.

cpp

```
int FreeString
(
        wchar_t **stringToFree
)
```

Arguments	Description	Notes
stringToFree	Double pointer to `wchar_t`	This function must be de-allocated in the same way that memory is allocated

Return Values	Description
0	The allocated memory was successfully released
Non-zero	The allocated memory failed to be released

Using the Custom Authentication Tester

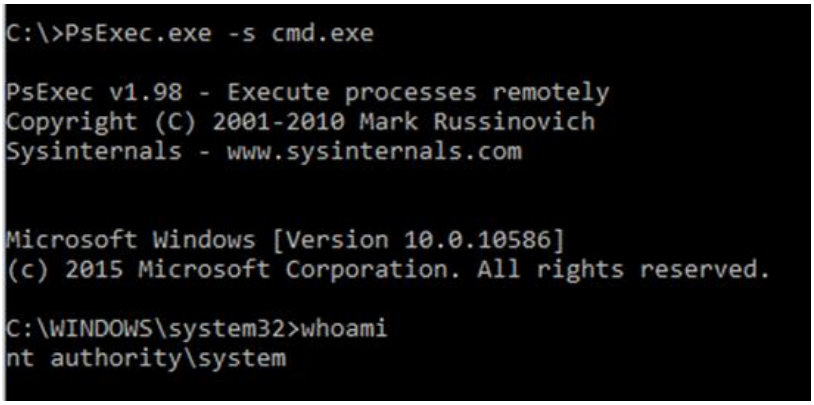
The custom authentication testing package includes a file called TestCustomAuthentication.exe that lets you test and troubleshoot your authentication module before using it with MetaDefender Kiosk.

TestCustomAuthentication.exe behaves similarly to the component MetaDefender Kiosk uses to load the authentication module. Since MetaDefender Kiosk runs under a SYSTEM context, you should also run the authentication module under SYSTEM. Attempting to run the authentication module as any other user may invalidate the module's results. You must run TestCustomAuthenticationModule.exe under SYSTEM to properly load authenticationModule.dll and test the methods.

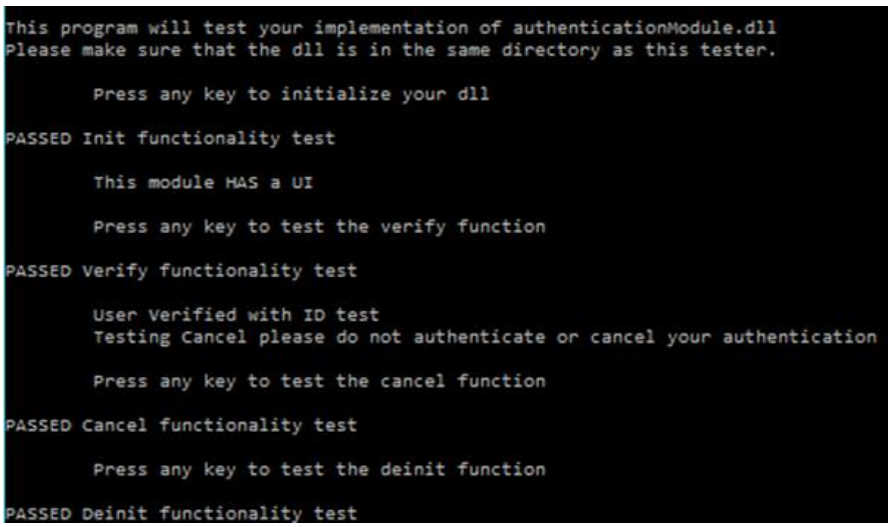
You can use Windows Sysinternals to run the tool as SYSTEM.

To run the custom authentication tester:

1. Download `PsExec`
2. Open a command prompt (as an administrator) to where `PsExec` is installed and enter `PsExec.exe -s cmd.exe`



3. Navigate to the `<Kiosk Install Directory>\Client\Authentication` directory
4. Run `TestCustomAuthentication.exe`. At all points of method testing, the tester pauses and allows you to control when to move on to the next test
5. A `PASSED` or `FAILED` result will be displayed



pcProx Plus RFID Reader Custom Authentication Module

- Overview of Module
- Required Components
- Configuration
  - Reader Configuration
    - pcProxConfig Installation
  - Adding pcProx Custom Authentication Module to MetaDefender Kiosk
  - Using the pcProx Custom Authentication Module

Overview of Module

This documentation describes usage of the pcProx Plus RFID Reader custom authentication module. This authentication module can be used to allow RFID cards to be used for MetaDefender Kiosk authentication.

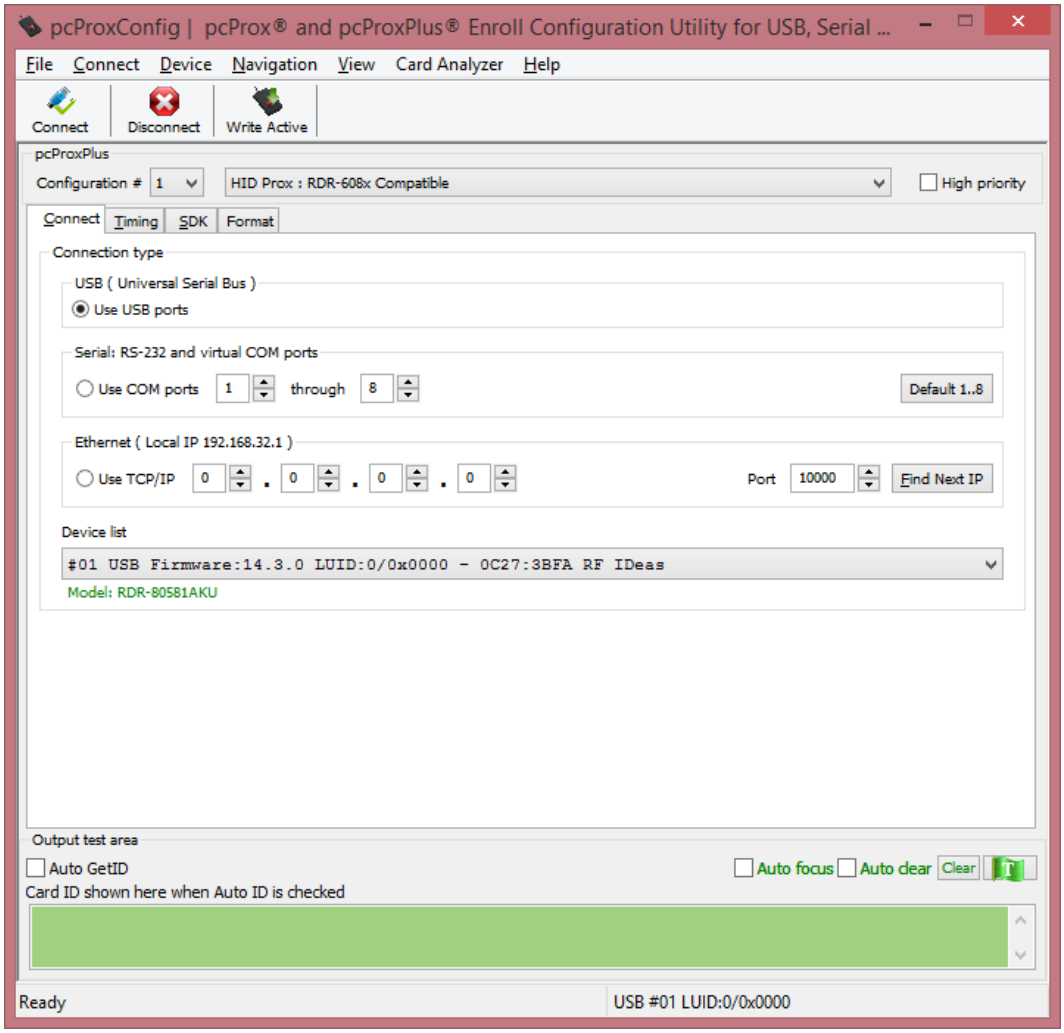
Required Components

- Installed MetaDefender Kiosk
- pcProx Plus RFID Reader
  - https://www.rfideas.com/support/product-support/pcprox-plus
- pcProxConfig reader configuration tool
  - Download available at https://www.rfideas.com/support/product-support/pcprox-plus
  - Documentation available at https://www.rfideas.com/files/downloads/manuals/Enroll_Plus_Wiegand_Manual.pdf
- pcProx Plus RFID Reader Custom Authentication Module
  - Compiled binaries and source available on My OPSWAT

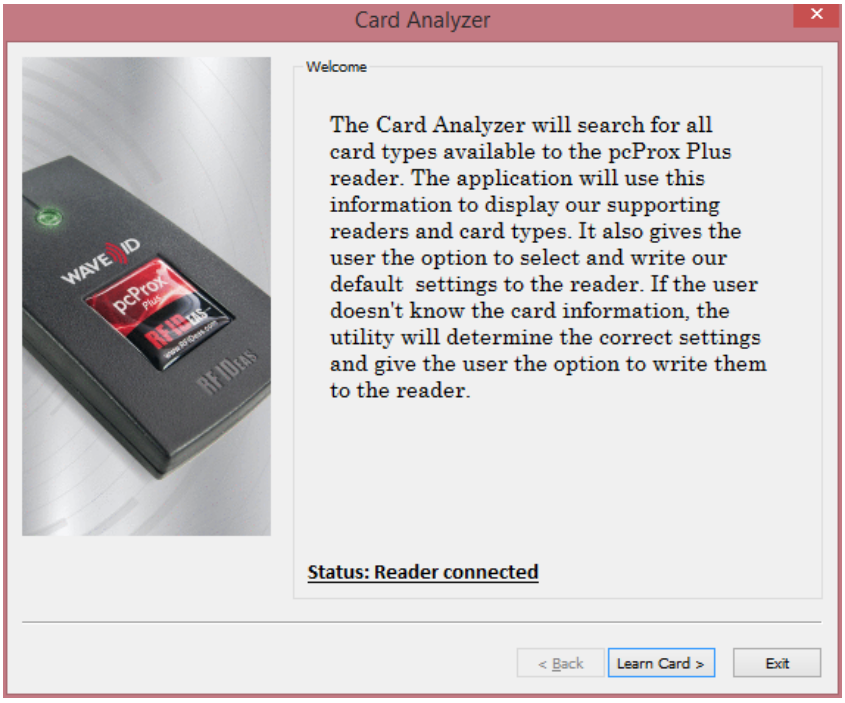
Reader Configuration

pcProxConfig Installation

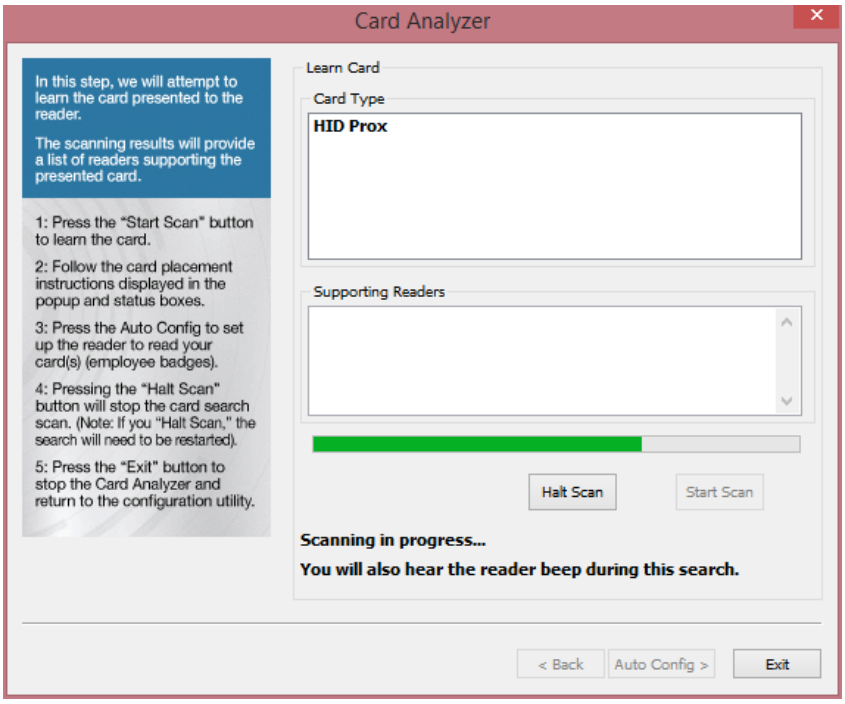
1. Download the pcProxConfig installer from https://www.rfideas.com/support/product-support/pcprox-plus
2. Run the installer to install the pcProxConfig configuration tool
3. Connect the pcProx reader to the Metadefender Kiosk system and wait for the driver to be installed. The LED on the reader will turn red
4. Launch the pcProxConfig tool, the device should be automatically detected



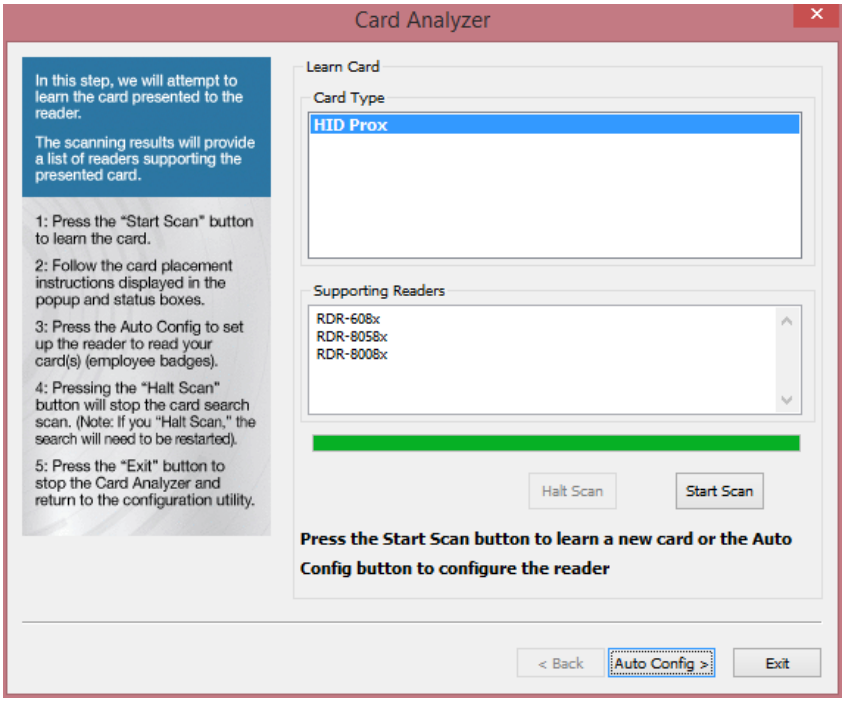
5. If the reader is not automatically detected you can click on the `Connect` button to detect the reader
6. The reader should be shown in the device list
7. Select `Card Analyzer` from the menu



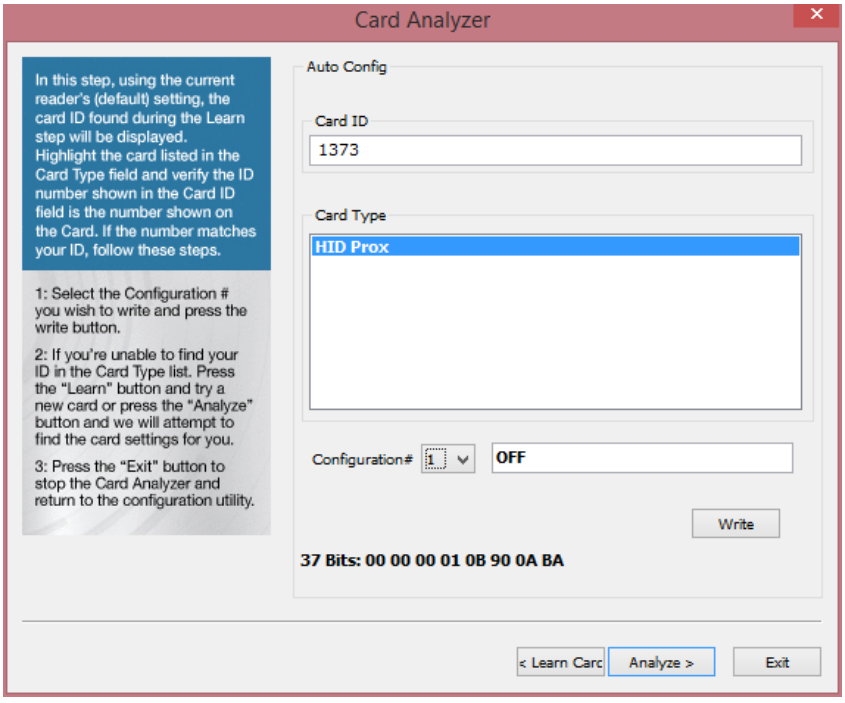
6. Click 'Learn Card'
    a. Click Start Scan, and when prompted put the RFID card that you want the device to learn on the scanner. The card will need to stay on the reader until the scanning is complete.



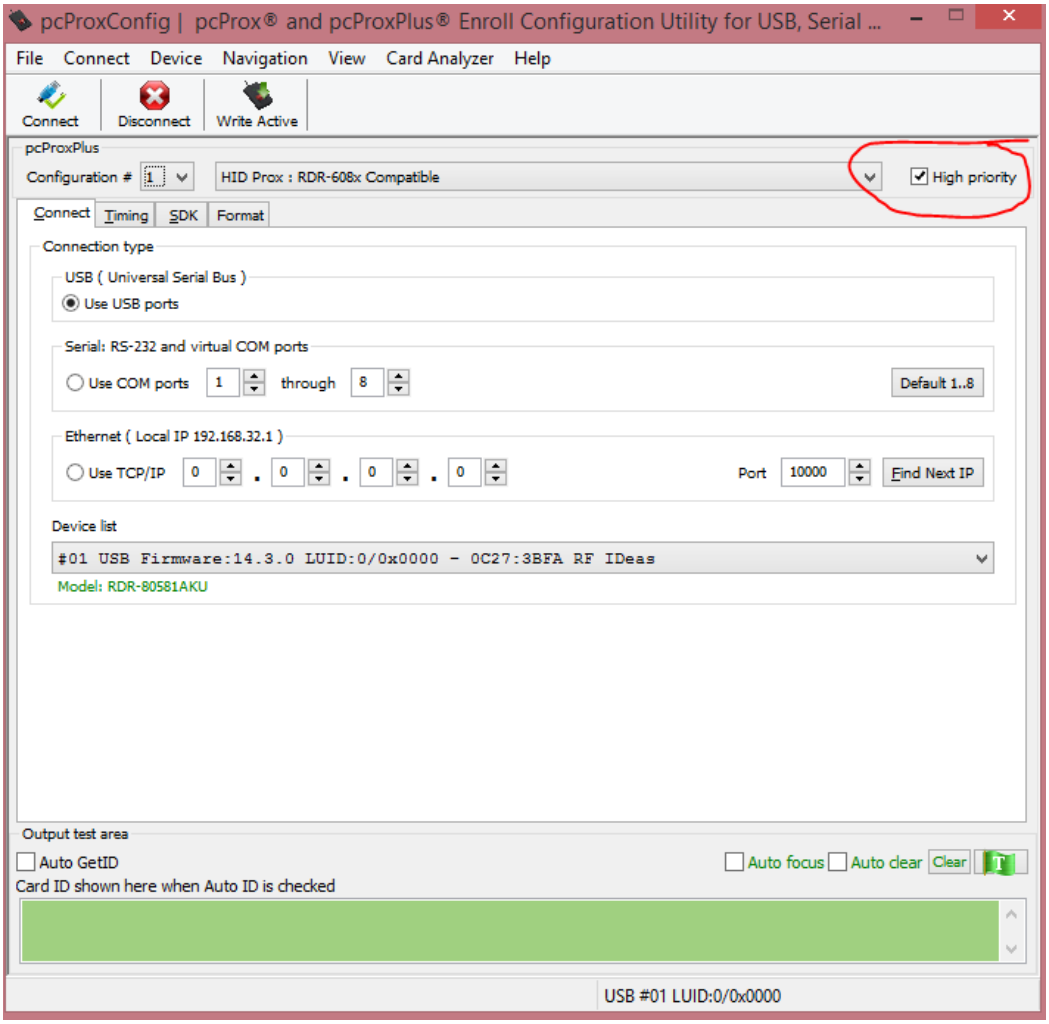
3.



7. Click the 'Auto Config>' button
8. Select the Configuration # to set and click the 'Write' button



9. After the configuration has been written click 'Exit' to close the Card Analyzer dialog or click the 'Learn Card' button to learn another card type
10. Confirm that the configuration has the 'High priority' checkbox selected



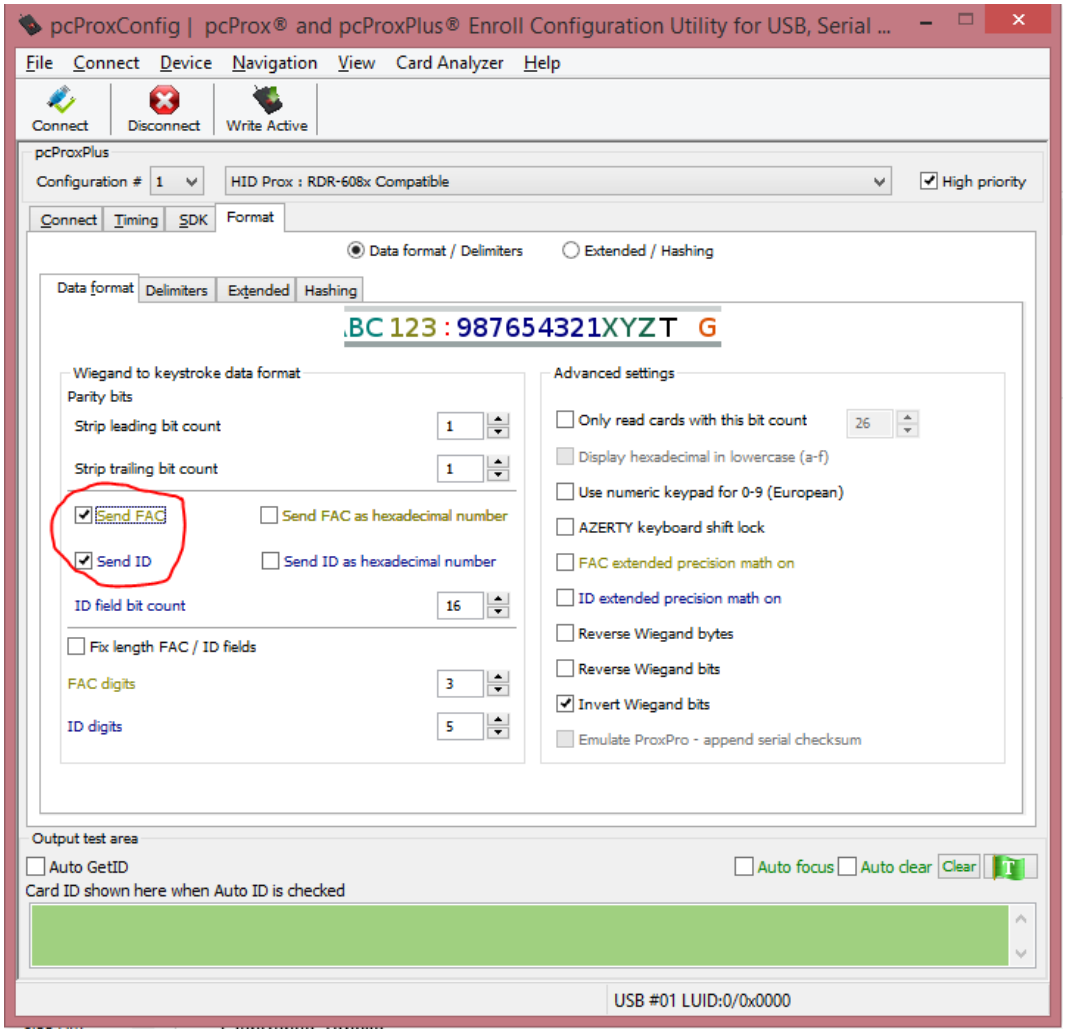
2. If two configurations are saved make sure this is selected for both

    11. Select the 'Format' tab. On the 'Data Format' subtab do the following.

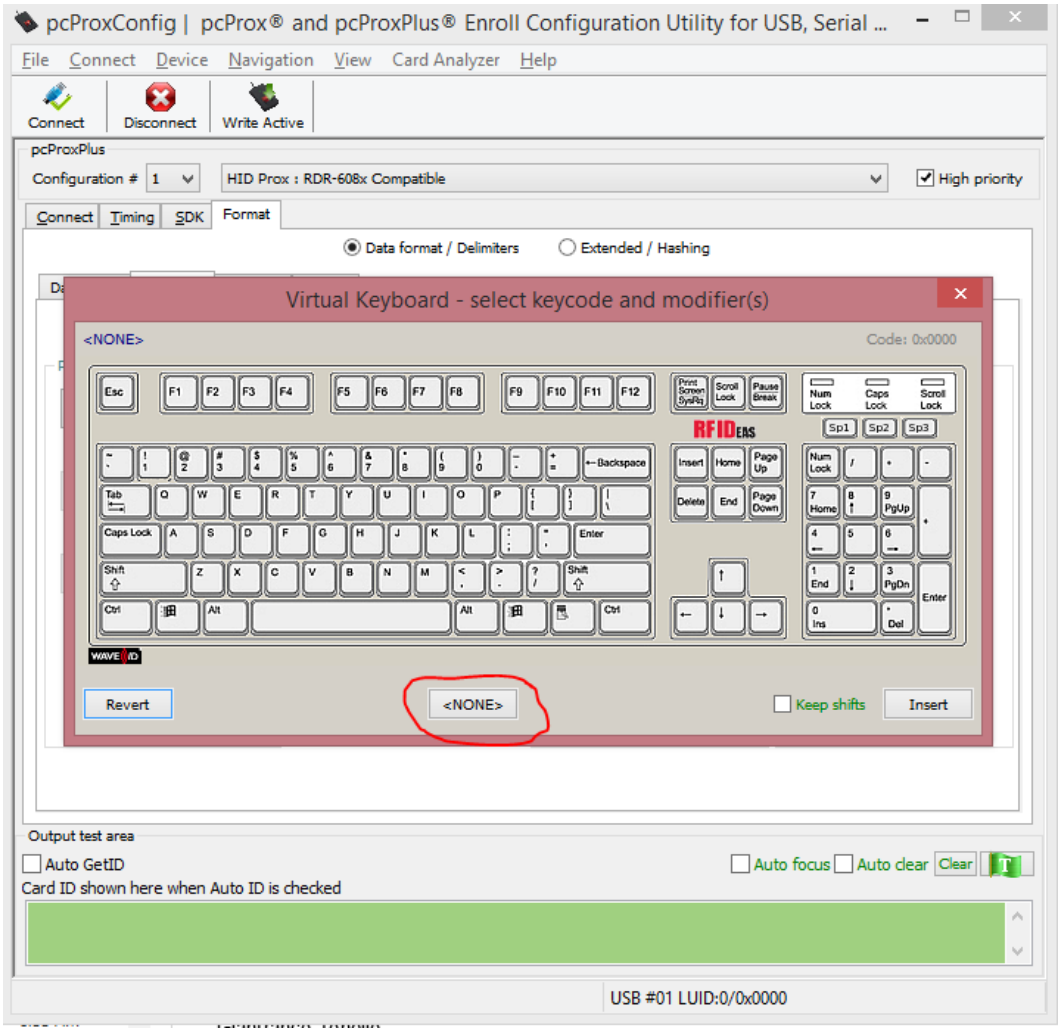
        a. Confirm the 'Send ID' checkbox is selected

        b. OPSWAT recommends that the 'Send FAC' checkbox is also selected

3.

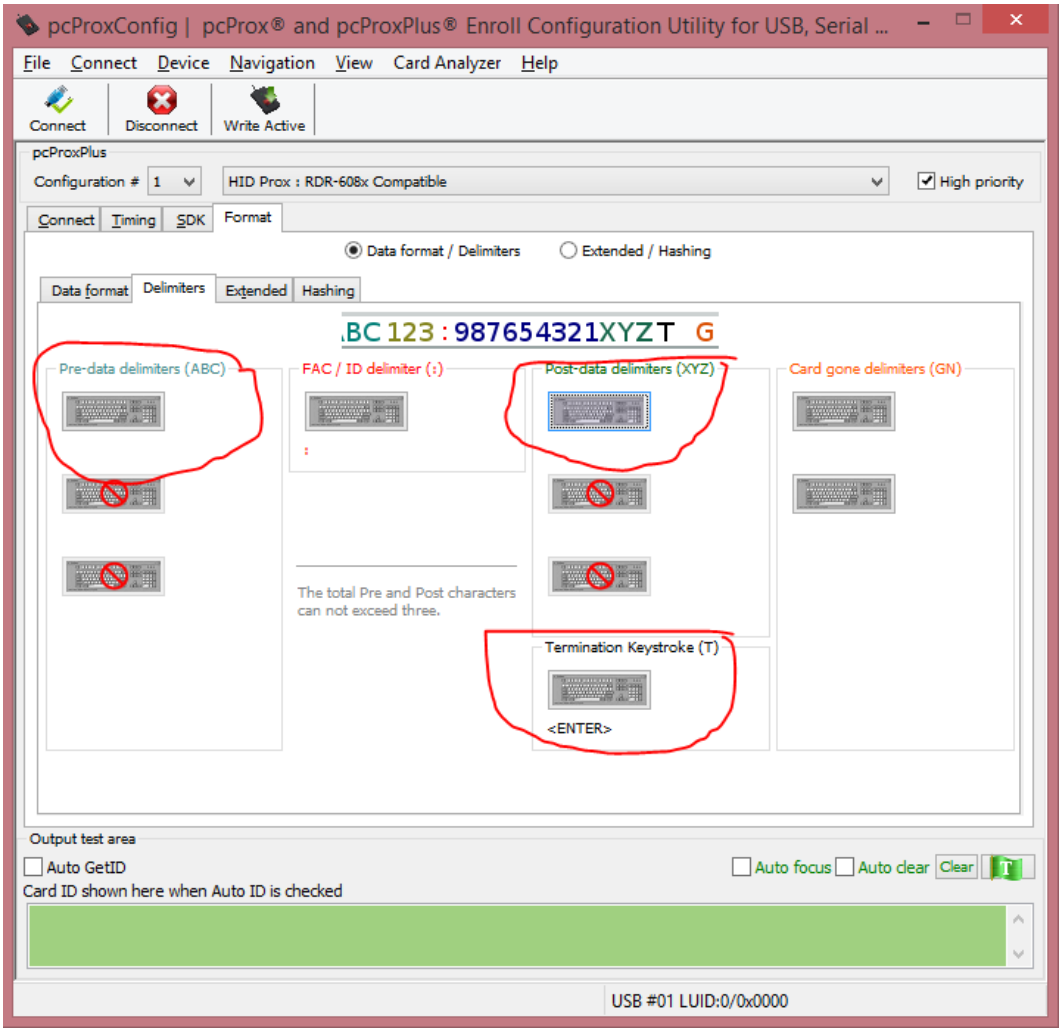


12. On the 'Delimiters' subtab, do the following
    a. Confirm the Pre-data delimiter is set to <NONE>



3. Confirm the Post-data delimiter is set to <NONE>

4. Confirm the Termination Keystroke is set to <ENTER>



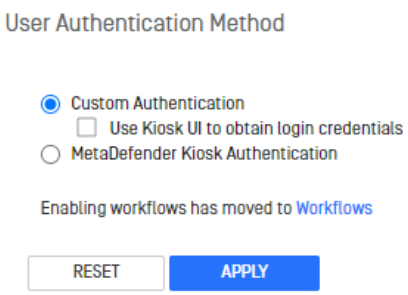
13. Click the 'Write Active' button to save the configuration. If there are two configurations set this needs to be done for both configurations.
14. Test the configuration by opening the Notepad application and scanning a card. The card ID should be written into Notepad.

Adding the pcProx Custom Authentication Module to MetaDefender Kiosk

1. Copy the following files from the custom authentication module download package into your `C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\Authentication` directory
    a. authenticationModule.dll
    b. CustomAuthExample.exe
    c. omsConfig_CAM.ini
    d. db
2. If you would like to restrict users to the RFID cards that are listed in the database
    a. Set the property validate_ID=1 in omsConfig_CAM.ini

b. Open the 'db' file with a text editor, such as Notepad. Update/add the valid card IDs (can be read by pcProxConfig tool, step 14) with the corresponding user names in the format <Card ID>:<Name>. Only card IDs that are listed in this file can be used for authentication.

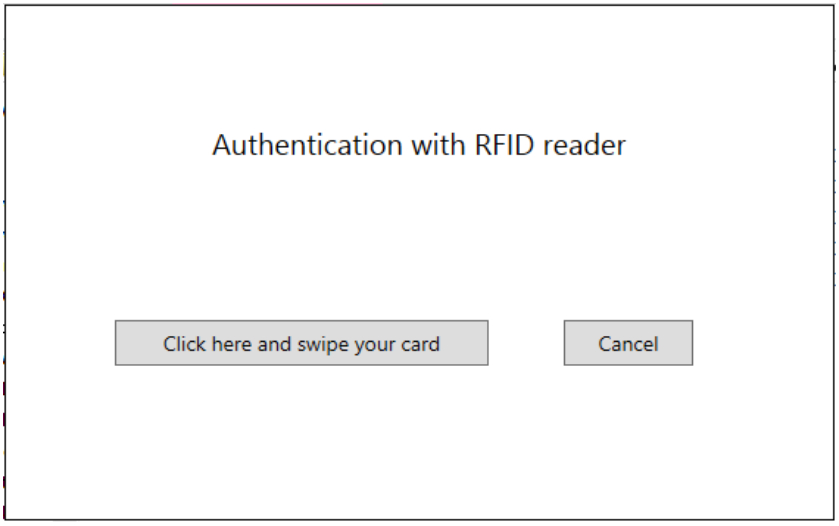
3. In the MetaDefender Kiosk Management Console, enable Custom Authentication. Configuration → User Authentication → View and configure user authentication → User Authentication → Custom Authentication



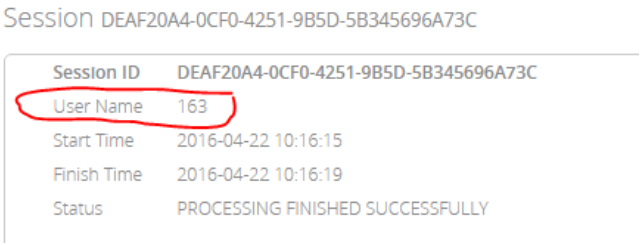
2. Click the 'Apply' button

Using the pcProx Custom Authentication Module

1. Users will be prompted to scan their RFID badge



2. The ID from the card will be saved as the user ID for the session
   a. In the session log viewable through the Management Console



2. On the scan receipt

3. In the saved text log file

Quarantine Manager Command Line Interface

You can use the MetaDefender Kiosk Quarantine Manager CLI (omsQMCLI.exe) to browse and manage quarantines. The size of the MetaDefender Kiosk quarantine is limited to 100 MB.

> **Warning**
> The MetaDefender Kiosk Quarantine Manager CLI must be executed with administrator privilege.

Help

Syntax: help

This function prints the available command line options.

Quarantine file

Syntax: quarantine <file path> <threat name>

This command adds the specified file to the quarantine database under the given threat name.

Delete file

Syntax: delete <file path>

This command permanently deletes a file which has been quarantined.

Note: Disk space will be reused without returning to the OS.

Restore file

Syntax: restore <quarantine ID> [target directory]

This command restores a quarantined file back to the original location. If a file already exists with the same name, a number will be appended to the file name. You can override the location the file is to be restored to by specifying the target directory.

Browse quarantine

Syntax: list [<minimum number of quarantines to display>]

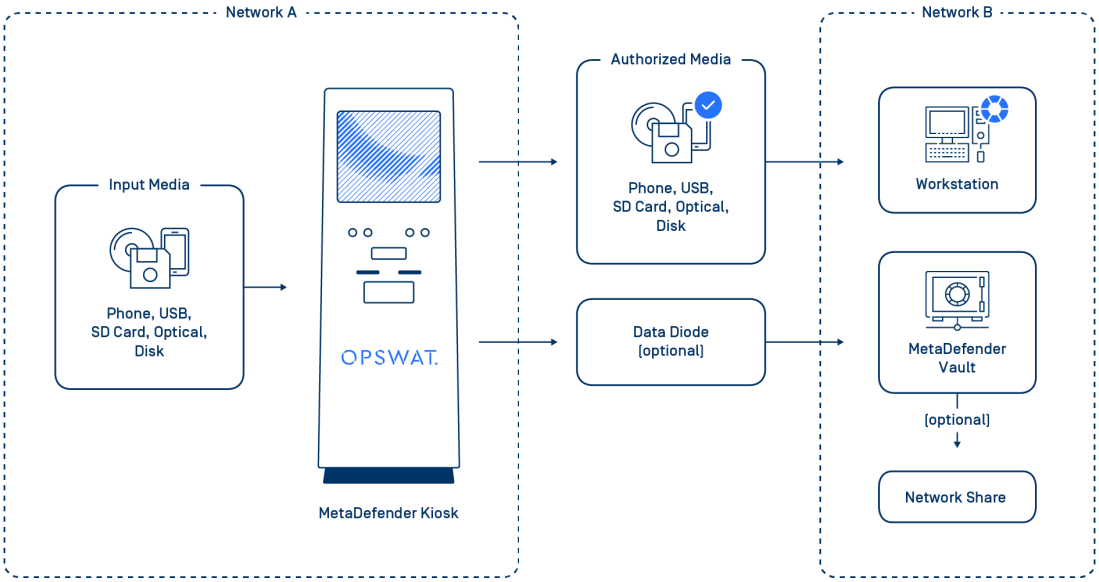
This command lists quarantined files.

Recommended Deployment of MetaDefender Kiosk(s) in Secure Facilities

Overview

OPSWAT's MetaDefender Kiosk product is deployed by organizations to scan portable media and detect and prevent threats contained on such media and prevent their introduction to secure networks and systems. The intention of this document is to outline OPSWAT's recommended deployment for MetaDefender Kiosk systems within a high security environment. Specifically, this covers the deployment of MetaDefender Kiosk systems to meet the requirements for handling digital media.

Recommended Deployment Diagram



MetaDefender Kiosk Deployment Options

For each deployment aspect below, OPSWAT has recommendations for different deployment options. In many cases, there are multiple deployment options that have trade-offs between security, usability, cost, or all three. When different options are available an attempt is made to describe the trade-offs between the different options.

Distributed vs Standalone Deployment Model

MetaDefender Kiosk and MetaDefender Core can be installed either on the same system or on separate systems that are accessible over a network. Although both options are secure, OPSWAT recommends considering the following advantages of each.

Advantages of a Distributed Deployment Model

1. The MetaDefender Kiosk system can be protected by a system imaging product (see the System Imaging section below) without the loss of anti-malware definitions (see the Upgrading Anti-malware Engine Definitions section below) that have been applied to the MetaDefender Core component
2. Separation of the MetaDefender Kiosk and MetaDefender Core components means that compromising the MetaDefender Kiosk system does not compromise the MetaDefender Core system or vice versa
3. If multiple MetaDefender Kiosks are using the same MetaDefender Core the anti-malware definitions only need to be updated on the MetaDefender Core server. This allows the definitions to be updated on a more frequent basis which increases the security against new outbreaks and zero-day attacks
4. MetaDefender Core servers can be located in a different physical location than the MetaDefender Kiosk system. This has multiple advantages
    a. The MetaDefender Core system can be located in a more easily accessible area and thus be updated with anti-malware definition updates more frequently
    b. If the MetaDefender Kiosk system is physically compromised it does not affect the MetaDefender Core system
5. MetaDefender Core server can be deployed on Linux, reducing the likelihood the same threat could compromise both the Kiosk and Core systems.

Advantages of a Standalone Deployment Model

1. No networking infrastructure or configuration is required
2. Kiosks can be relocated without any additional modifications

Network Traffic Restrictions

These recommendations are only applicable if the MetaDefender Kiosk systems are networked.

The following functionality of MetaDefender Core and MetaDefender Kiosk require network access to other systems

- Remote configuration of MetaDefender Core and Kiosk
    - Application of antimalware engine definition updates to MetaDefender Core
    - Changes to workflows
    - Other configuration change
- Distributed Deployment of MetaDefender Core and Kiosk
    - Transfer of files to be scanned
    - Retrieval of scan results
- Post Scan File Handling
    - Upload of files from MetaDefender Kiosk to MetaDefender Managed File Transfer (if configured as a file handling option in workflows)
    - Copying of files from MetaDefender Kiosk to a network path (if configured as a file handling option in workflows)

OPSWAT recommends restricting the allowed traffic to only that necessary for the functionality needed in a deployment. OPSWAT recommends using a product designed for this purpose to tightly restrict the traffic that is allowed. OPSWAT can provide recommendations on specific products that have been tested with MetaDefender for

compatibility. If such a device is not used, OPSWAT recommends restricting network traffic to only the ports required for operation of the MetaDefender Kiosk systems using Windows Firewall as well as restricting traffic to specific trusted MAC addresses.

System Reboot & System Restore

MetaDefender Kiosk provides the option to restart the kiosk after each scanning session. This supplemental action allows for a full reset of memory and other system resources utilized during a session. If business requirements make restarting the kiosk after each session unfeasible, a scheduled task can be set to restart the kiosk systems on a regular basis (e.g., every night).

Extreme caution can be exercised when handling suspicious media. A system restore point can be created to ensure a known working clean state can be recovered in the event of unexpected failures.

- All configuration changes or MetaDefender Kiosk upgrades will be lost every time the system is restored if the restore point is not kept up to date.
- If MetaDefender Core is installed on the same system as MetaDefender Kiosk all updates will be lost upon system restore. This includes all antimalware engine definition updates that have been applied. See the section on the advantages and disadvantages of choosing a distributed vs standalone deployment model.
- All scan logs that are stored on the system will be lost upon system restore. To maintain logs, MetaDefender Kiosk must be configured to save session logs to another system.

MetaDefender Kiosk Hardening

OPSWAT recommends following the instructions in the MetaDefender Kiosk user guide to harden the MetaDefender Kiosk systems.

Maintenance Policy

Updating Antimalware Engine Definitions

1. MetaDefender Core antimalware engine definitions should be updated by following the instructions in the MetaDefender Core documentation
2. For downloading offline definition updates, OPSWAT recommends using the MetaDefender Update Downloader
3. OPSWAT recommends updating the antimalware engine definitions as often as is possible, preferably daily

Upgrading MetaDefender

1. MetaDefender Core and MetaDefender Kiosk should be upgraded by following the upgrade instructions in the product documentation
2. OPSWAT recommends that when possible all deployments should be on the latest versions of MetaDefender Core and MetaDefender Kiosk. For more information on OPSWAT's support policy for specific versions of MetaDefender Core and Kiosk please refer to OPSWAT's MetaDefender support Policy
3. When systems are upgraded it is recommended that the configuration settings from the previous installation are exported and archived so that they are available in case systems need to be restored to a previous version
4. OPSWAT recommends always upgrading both MetaDefender Core and MetaDefender Kiosk at the same time

Configuration Options

User Authentication and MetaDefender Kiosk Workflows

MetaDefender Kiosk enables authentication of users before starting a scanning session. OPSWAT recommends enabling user authentication for the following reasons.

- Identification of which user scanned each piece of media that was scanned by MetaDefender Kiosk for audit purposes
- Usage of different user workflows for different groups of users (see section on Multiple User Workflows)

MetaDefender Kiosk supports the use of custom authentication modules, which allow each organization to integrate their authentication method (e.g. RFID card, badge scanner, IC card, etc) with their MetaDefender Kiosk. This allows an organization to link scan sessions to their existing authentication systems. Depending on the authentication system used, a custom authentication module may have to be developed for deployment. Contact OPSWAT for more information on what a specific system would require.

Multiple User Workflows

OPSWAT recommends configuring multiple user workflows to process files from different users. Each workflow should be configured to restrict the types of files to the minimum those users are expected to need to complete their jobs. File types that are more risky (e.g. EXEs or Archive files) should be limited to the users that are expected to bring in those types of files and need them to complete their work and should be blocked for all other users.

Authentication and MetaDefender Managed File Transfer

If files are being uploaded to a MetaDefender Managed File Transfer server after scanning there are two options for uploading the files

1. Upload to a MFT user account - This is an option if the user credentials are available to the MetaDefender Kiosk system. This would most likely be the case if MetaDefender Kiosk and MetaDefender Managed File Transfer are both on the same network and are using the same Active Directory server for authentication.
2. Upload to a MFT guest user account - This is an option to create a guest user account that is used for a specific file upload. This can be used when either user credentials are not available to MetaDefender Kiosk or there are guest users scanning files on the MetaDefender Kiosk.

Data Sanitization

Data sanitization is the process of removing potentially dangerous objects within files or modifying the files to neutralize threats, even if they are not detected by any antimalware products. MetaDefender Core's data sanitization technology allows administrators to specify that certain types of files are sanitized even if no threat is detected. Although this results in greater security and a reduction in the risk to unknown threats, there is a tradeoff in that the usability of sanitized files is sometimes less than the original file.

- For the highest level of security, OPSWAT recommends that data sanitization is applied to all document and image types that are supported unless the potential loss of usability in those files is too great for business reasons.

Note that a sanitized file will have a different hash than the original file, even if there was no threat in the original file.

Post-Scan File Handling

OPSWAT recommends that files are copied to a new location after scanning so that original media does not need to be used in a secure area. Files should be restricted to those allowed by the defined security workflow. MetaDefender Kiosk offers multiple options for moving files to a new location after scanning.

Options for Networked Environments

The most secure option if the MetaDefender Kiosk system is on a network is to upload the files to a MetaDefender Managed File Transfer server. The advantages of uploading to MetaDefender Managed File Transfer is that the files can be uploaded to a specific user's account or a guest account, and access is limited to that user. All file uploads and downloads are tracked, and an audit log is available for compliance officers to see when files were uploaded and downloaded from the server. This can help to track when files are accessed in a network and by whom.

If MetaDefender Managed File Transfer is not used, files can also be copied to a network share into a directory tied to the user who authenticated on the MetaDefender Kiosk system.

Option for Non-networked Environments

If the MetaDefender Kiosk system is not deployed on a network OPSWAT recommends using the functionality to copy clean files to user provided media, allowing original media to not be used on the secure network. OPSWAT would recommend either copying to pre-approved media that is only used in the secure network or to static media, such as CDRs. If copied to pre-approved rewritable media, such as USB drives, OPSWAT recommends a policy to wipe that media after use and before the next time the media is used as the destination media. MetaDefender Kiosk's wipe functionality can be used for this purpose.

Session Logging

MetaDefender Kiosk Supports three types of logging of individual scan sessions. All three can be enabled or disabled independently of each other.

1. **Save session log to a text file** - Saves a text log for each session to the default log directory or a directory specified by the administrator, however if the files are saved locally they will not be retained if the system is restored as recommended in the System Restore section above. To retain these session logs they should be pushed to a centralized network location.
2. **Save session log to scanned media** - Saves the text log for a session to the media that was scanned. This allows a record of the scan to be saved on the media that was scanned, however a file will not be written if the original media is read-only.
3. **Send session log to e-mail recipient** - This allows all scan logs to be collected into a single e-mail account, however it does require that the MetaDefender system has access to a mail server to send the e-mail.

If logs from the MetaDefender systems are required outside of the secure network, OPSWAT recommends the use of a data diode to transfer files out of the network. OPSWAT can recommend different vendors to meet this need upon request.

Common Questions about MetaDefender Kiosk

1. **How many MetaDefender Kiosk systems are needed in a deployment?**
    a. We believe that the appropriate number of units would be the number required to give end users a chance to scan media however and wherever they are bringing it into a secure area. So, if there are three entrances a kiosk can be located at each entrance. If employees and/or visitors are also expected to scan media that is already within the secure area then a kiosk should also be in a location that is convenient for users to access within the secure area.

2. **What are the recommended physical locations for MetaDefender Kiosk systems to ensure steady availability to all end-users?**
    a. We recommend that MetaDefender Kiosk stations are located at all entrances to secure areas, and that users are required to scan any portable media before bringing them into secure areas.
3. **Which organization functional unit should be the owner of the MetaDefender Kiosk systems (to maintain, update, …etc)?**
    a. The appropriate department should be the one that is able to handle definition and software updates to the MetaDefender Kiosk systems. The necessary skills include basic Windows operating system knowledge as well as comfort with configuration and deployment of secure networks.
4. **Do you recommend deploying MetaDefender Kiosk in a standalone or distributed environment? What are the pros and cons of different deployment options?**
    a. A majority of our current customers have deployed MetaDefender Kiosk systems as standalone systems not connected to any network. Although this is a secure deployment option, we think that the most secure solution is to deploy MetaDefender Kiosks on an isolated network, with multiple MetaDefender Kiosk systems using a shared backend MetaDefender Core server. The advantages of this deployment model are the following:
        i. The MetaDefender Core server can be located in a central location that is physically easier to access to apply engine definition updates
        ii. The MetaDefender Core server can be on a high performance server so that better scanning performance can be achieved versus standalone systems
        iii. A single centralized MetaDefender Core server can have more scanning engines than multiple standalone MetaDefender Core servers at the same total cost
        iv. The MetaDefender Kiosk systems can be restored to a known ‘clean’ state if necessary without losing engine definitions that have been applied
    b. The disadvantage of going with a distributed deployment is maintenance of the network and the existence of the central MetaDefender Core server but we generally feel that the benefits listed above outweigh the additional costs
5. **How frequent should antimalware engine definitions be updated?**
    a. We recommend updating the engine definitions as often as is possible, preferably once a day if it is feasible. The ability to update virus definitions more frequently is a major advantage to having a distributed deployment model with a central MetaDefender Core server.
6. **How do you recommend laptops or tablets are scanned for threats?**
    a. Devices such as laptops or tablets can be scanned with our MetaDefender Client product on an isolated network. This client can be run on the device either when the system is already running or can be included on a 'boot' or 'live' CD or USB that is used to boot the system into a limited operating system.
7. **Can MetaDefender Kiosk detect BadUSB?**
    a. With BadUSB based attacks, the USB device has been modified to act as a different type of device (e.g. a keyboard or other peripheral) instead of a flash USB drive. Since this is done at a firmware level, there is no way for the system, and the MetaDefender Kiosk software, to know that is is anything besides the type of device it is identifying itself as, however just as the MetaDefender Kiosk UI is hardened against being compromised by a physical keyboard it would protect against a ‘fake’ keyboard or other input device that a BadUSB device is pretending to be.
8. **Does MetaDefender Kiosk provide any protection when the kiosk UI is not running?**
    a. If the MetaDefender Kiosk software is not running there is no additional protection on the system provided by MetaDefender Kiosk.
9. **Is it possible for m alicious code to compromise the Kiosk UI?**

a. OPSWAT is not aware of any way that a client can be compromised.

10. **If the Kiosk UI is compromised is there a way for the Server to be compromised as well?**
    a. If the Kiosk were to be compromised, it does have system or network access to the server. What OPSWAT would recommend as the most secure deployment option would be have MetaDefender Kiosk and MetaDefender Core on separate systems on the same isolated network, and a device restricting network traffic between the Kiosk and the Core server to restrict traffic between the Kiosk and the server to only the traffic necessary for scanning. OPSWAT can recommend devices to provide this functionality. In addition, the MetaDefender Core server can be deployed on Linux, reducing the likelihood the same threat could compromise both the Kiosk and Core systems.
11. **Is it possible for malicious code to be written to the MetaDefender Core server and compromise the Server?**
    a. All files are written to the temporary directory, which can optionally be set to the RAM drive, and then removed immediately after scanning so they will not remain on the server.
12. **If multiple MetaDefender Kiosk systems are deployed on the same isolated network could a compromised MetaDefender Kiosk system compromise other MetaDefender Kiosk systems ?**
    a. OPSWAT is not aware of any way that a MetaDefender Kiosk system could compromise another MetaDefender Kiosk system on the same network. However, for additional security, having a device that restricts traffic to only that required for scanning files can be added between the MetaDefender Kiosk system and the network. OPSWAT can recommend devices that provide this functionality.
13. **If a MetaDefender Kiosk system is compromised could it infect media being scanned?**
    a. OPSWAT is not aware of any way the Kiosk could be compromised to act in this fashion, however for additional security the Kiosk could be restored to a known 'clean' state after each scanning session. OPSWAT can provide recommendations on tools that can be used to provide this functionality.
14. **If a MetaDefender Core server is compromised could it infect media being scanned?**
    a. The MetaDefender Core server does not interact with the media being scanned in any way.
15. **What provisions/safeguards are in place to assure that an infected file is not skipped during a scan session either because a scan was cancelled or because a user did not select that file to be scanned?**
    a. If any files are not scanned on the media, either because the user cancels a scan or because they browse to select the files that are to be scanned, within the scan session log is a notification that the entire media was not scanned. OPSWAT also recommends that the functionality of copying to user provided media or to a MetaDefender Managed File Transfer server is used to ensure only files that have been scanned without any threats detected are used on a secure network.
16. **Is there any known instance where a MetaDefender Kiosk system has been compromised in the past?**
    a. OPSWAT is not aware of any deployed MetaDefender Kiosk system that has been compromised.

Configuring ADFS as SAML Identity Provider

This section provides instructions for administrator to configure ADFS as SAML Identity Provider for authenticating to Kiosk UI and Kiosk Web Management Console.

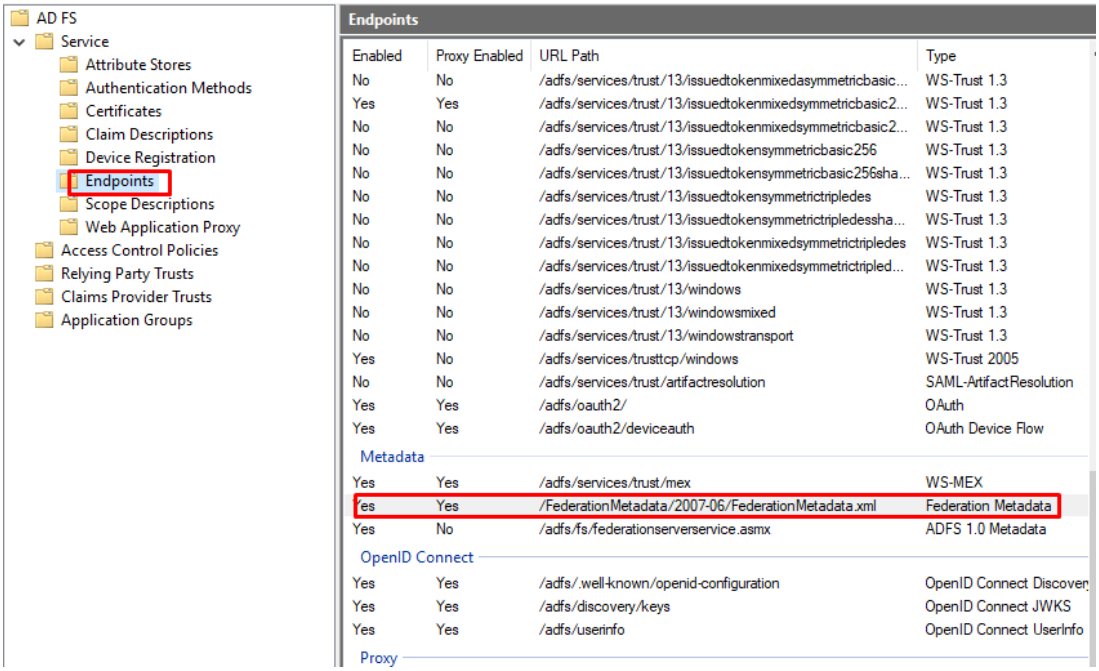
I. Configure ADFS server

- On Windows Server 2019/2022, enable role “Active Directory Federation Services”
- Ensure service “Active Directory Federation Services” - “adfssrv” - is running.
- Create a certificate (self-signed is acceptable) for the ADFS server.

II. Configure ADFS as SAML Identity Provider for Kiosk

Pre-conditions

- Make sure Kiosk system can access ADFS via domain name, e.g. `https://adfs.local`
- Enable HTTPS on Mangement Console. See Enable HTTPS for more detail.
- Get metadata URL from the ADFS server

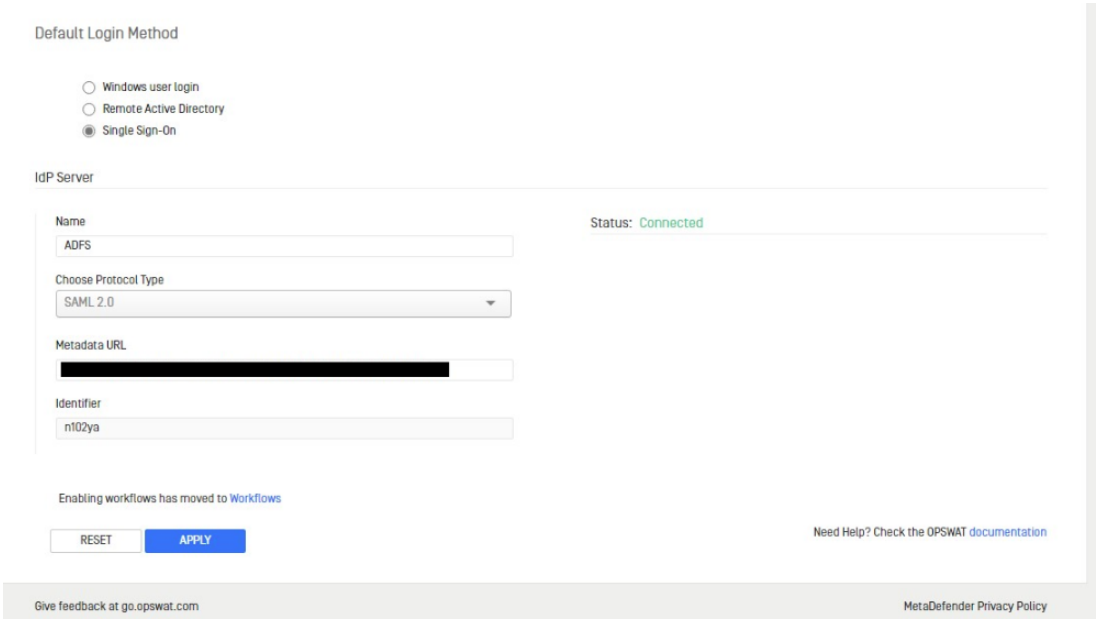


Step 1: Get the *Login URL*

Login URL will be used as **Relying Party Trust Identifier** on ADFS Management

Login URL for Kiosk UI:

1. On Kiosk WebMC, navigate to the **Workflows** tab, click on **Select Default Login Method**
2. Select **Single Sign-On**, and select **Protocol Type**, in this case using **SAML 2.0,** then enter **Name**
3. Enter the metadata URL into the Kiosk console according to the format: `https://<ADFS server_name>/FederationMetadata/2007-06/FederationMetadata.xml`
4. **Identifier** will be automated generated → Check if the status is `Connected` and then click on **Apply**



Info

Kiosk UI **Login URL** format:

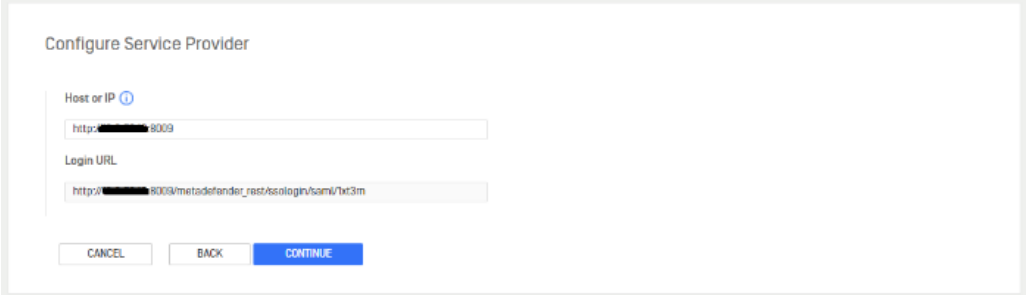
<http/https>://**localhost**:<port>/metadefender_rest/**uissologin**/saml/<identifier>

Please modify the elements enclosed in <> to match your Kiosk's configuration. It must be **localhost** for Kiosk UI login.

Login URL for Kiosk Console:

Select **SAML (SSO)** in the menu to create a **User Directory** that integrates with a SAML 2.0 SSO Identity Provider (IdP). Switch the toggle button to **ON** to enable this User Directory. As soon as it is submitted, any other User Directories configured with SAML (SSO) will be automatically disabled. Switching to **OFF** only creates the User Directory and will not change any currently enabled User Directories.

Click **CONTINUE** to go to the **Configure Service Provider** page. This will set up the login URL the Identity Provider uses to redirect after a successful login. Fill in **Host or IP** to generate the **Login URL**.



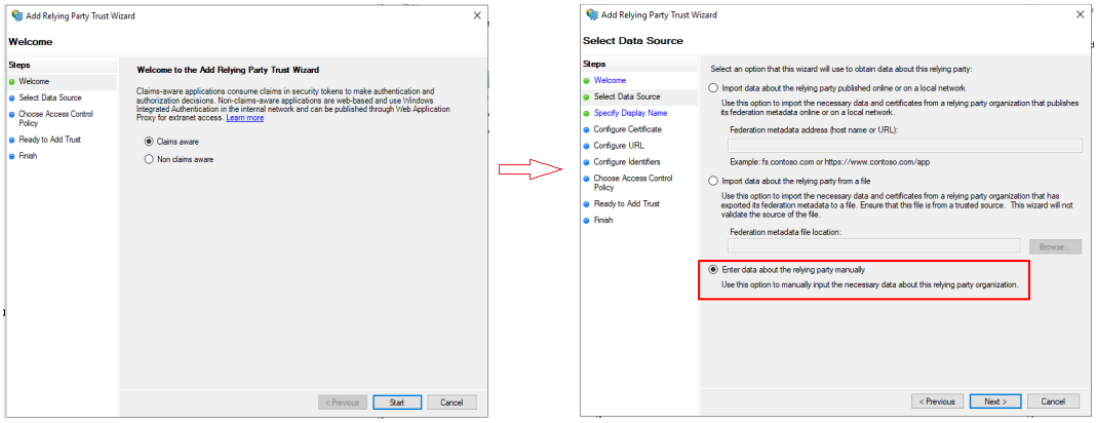
Info
Kiosk console **Login URL** format:

<http/https>://localhost:<port>/metadefender_rest/**ssologin**/saml/<identifier>

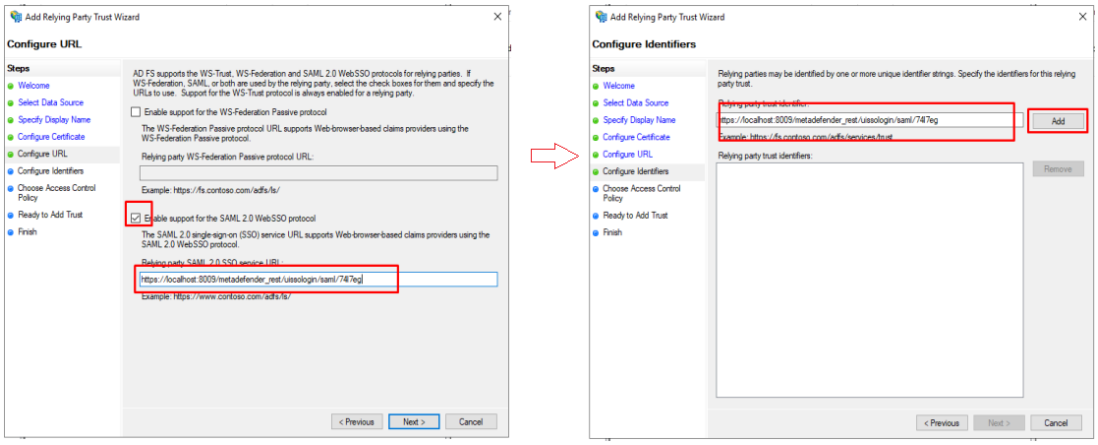
Step 2: On ADFS server, open “ADFS Management“.

Step 3: Add Relying Party Trust

1. Navigate to **Tools** → ADFS Management, select **Relying Party Trust,** and then click on **Add Relying Party Trust**.
2. Select **Claims aware** from the **Relying Party Trust Wizard** and click on **Start** button.



3. Enter **Display name** and then click on **Next** twice
4. Perform the following two steps
    a. Check on **Enable support for the SAML 2.0 Web SSO protocol** option and then enter the **Relying party SAML 2.0 service URL**.
    b. Enter the **Login URL** from **Step 1** as **Relying party trust identifier** and click on **Add**



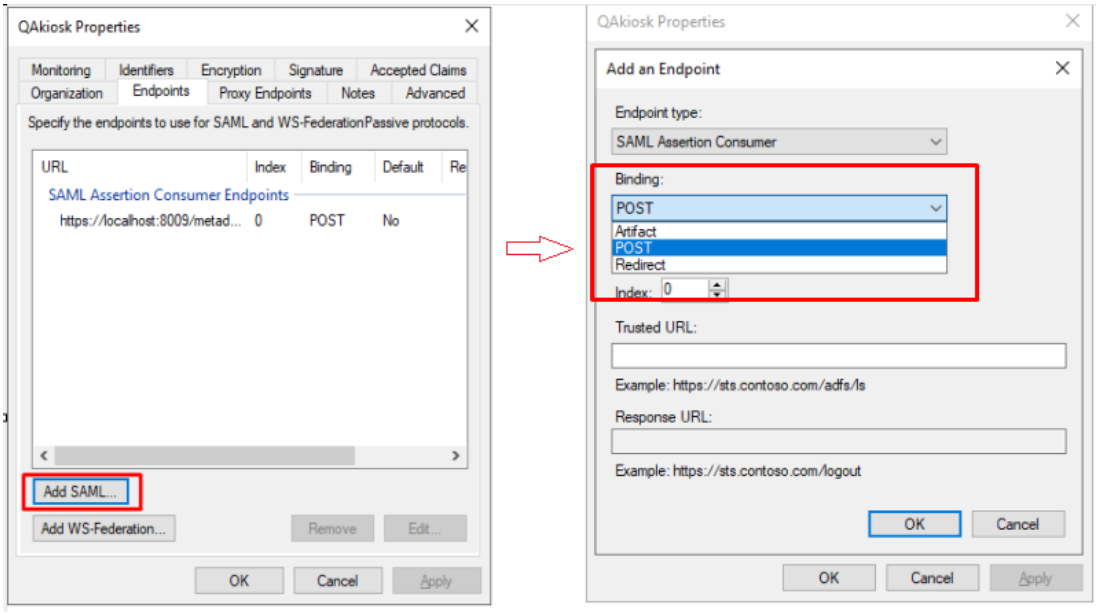
5. Click on **Next** 3 times and then **Close**

Step 4: Define the ADFS claim rules

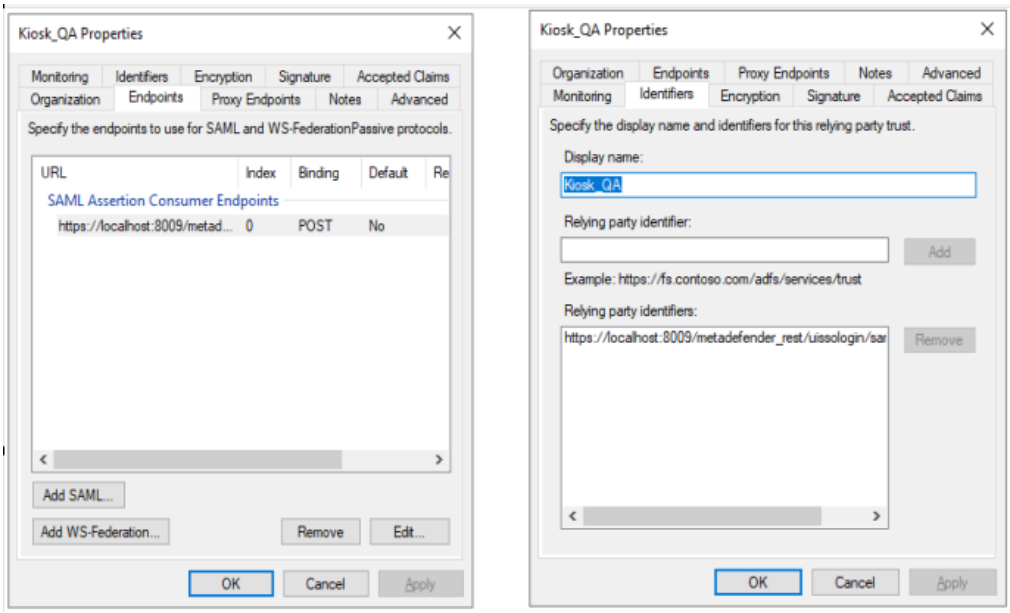
1. Go to the **Edit Claim Issuance Transform Rules** tab and click **Add Rules** to launch the **Add Transform Claim Rule Wizard**.
2. In the **Choose Rule Type** panel, choose **Send LDAP Attribute as Claims** and click **Next**.
3. Type the **Claim rule name** in the respective field
4. From the **Attribute store** drop-down list, choose **Active Directory**. In the **Mapping of LDAP attributes to outgoing claim types** section, choose the following values from the respective
    a. **For Kiosk UI:** [Require] LDAP Attribute: **SAM-Account-Name**, Outgoing Claim Type: **Name ID**
    b. **For Web Console:** [Require] LDAP Attribute: **User-Principal-Name**, Outgoing Claim Type: **Name ID**
5. Click on **Finish**

Notes

- Make sure the Binding method is POST (not Artifact)



- Any updates in Login URL must be updated on both **Identifiers** and **Endpoints** tabs → **Apply**



III. Configure many Kiosks - using as many Relying Party Trusts on ADFS

1. Configure each Kiosk as a seperate Relying Party Trust, using II. Configure ADFS as SAML Identity Provider for Kiosk

2. Each Kiosk must have a different Identifier.

IV. Configure many Kiosks - using one Relying Party Trust on ADFS

1. Not support to config directly from Kiosk, will need OCM for this.
2. Add all Kiosks to one OCM set of Kiosks.
3. Config from OCM using II. Configure ADFS as SAML Identity Provider for Kiosk
4. Make sure all Kiosk have the same port number and SSL is enabled.

Microsoft Entra ID Integration

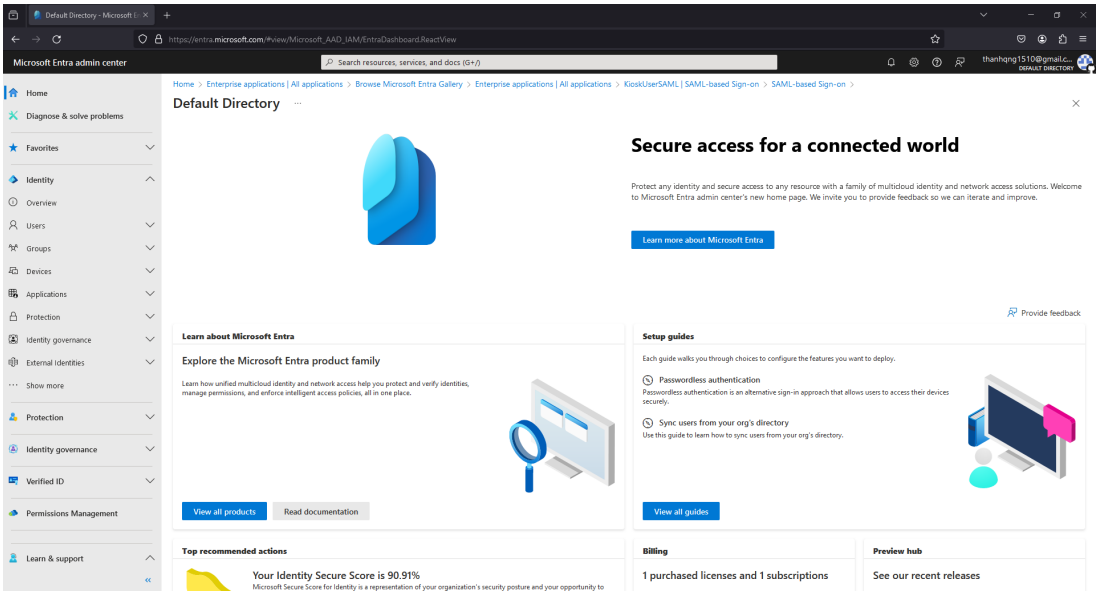
This section provides instructions for administrator to configure Microsoft Entra ID as SAML Identity Provider for authenticating to KIOSK UI and Web Management Console.

Procedure to set Microsoft Entra ID as login method for KIOSK UI or WebMC

The login configuration for KIOSK UI and KIOSK WebMC are distinct and should be set up separately, and all the steps should be repeated. This document outlines the same and unique configuration steps for both WebMC and UI. When configuring the KIOSK UI login, refer to the UI instructions and disregard the WebMC sections, and vice versa.

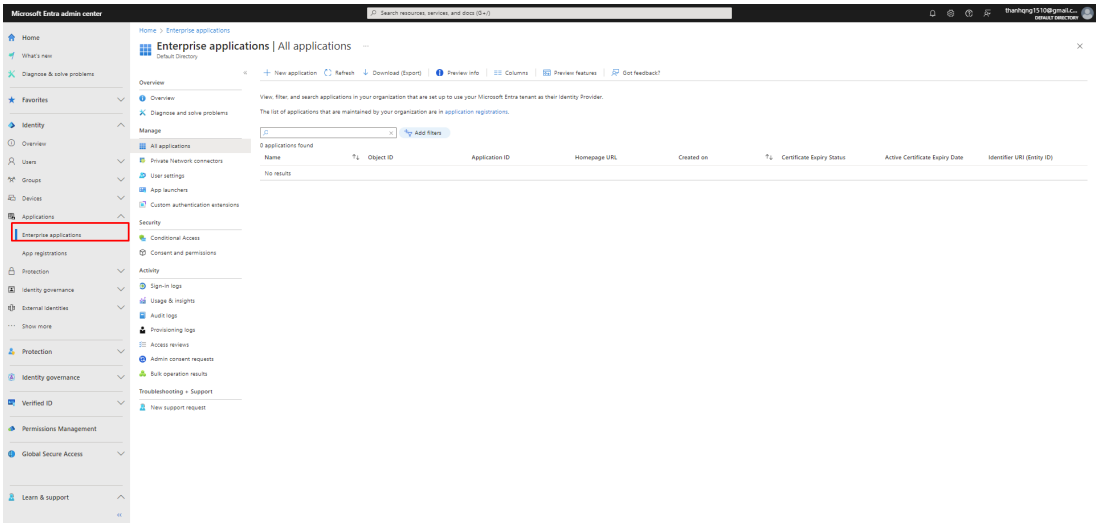
1. Application Registration

Step 1. Access the Microsoft Entra admin center using your administrative credentials.



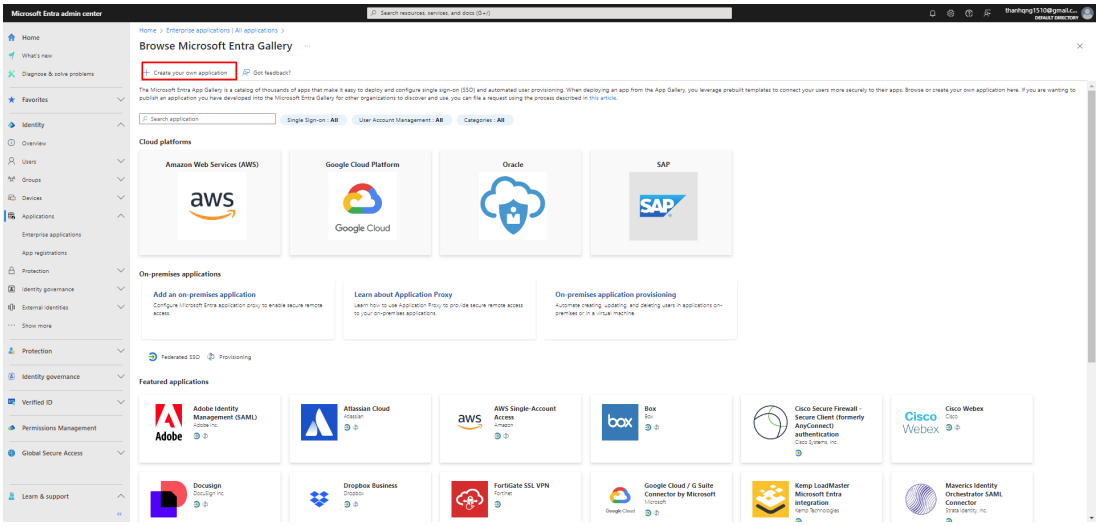
Microsoft Entra admin center

Step 2. Navigate to the **Identity > Applications > Enterprise applications** section.



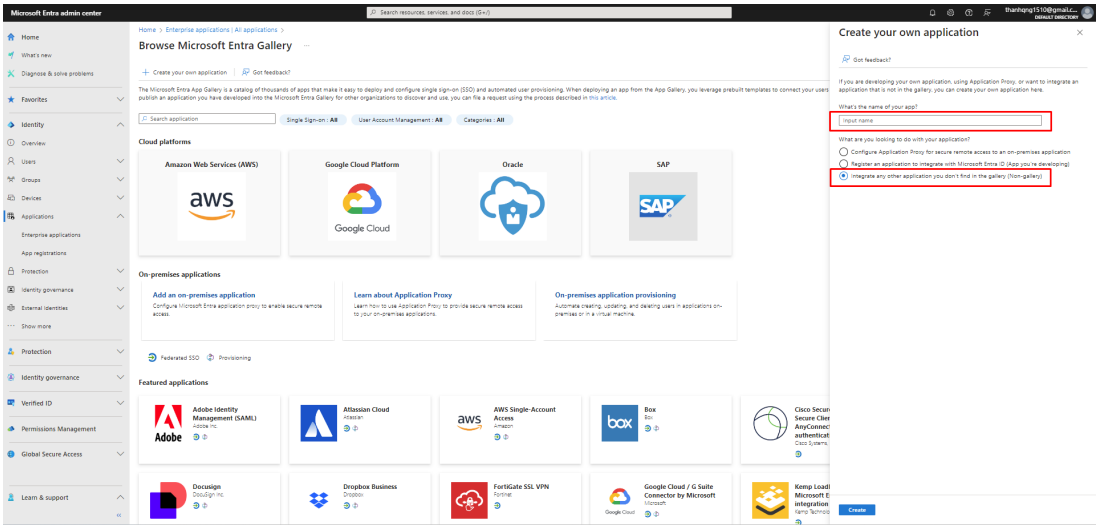
Enterprise applications

Step 3. Select **New application** and choose the **Create your own application** option.



New application menu

Step 4. Assign a descriptive name for your application and select I**ntegrate any other application you don't find in the gallery (Non-gallery).**



Create your own application

Step 5. Click **Create** to complete the application registration process.

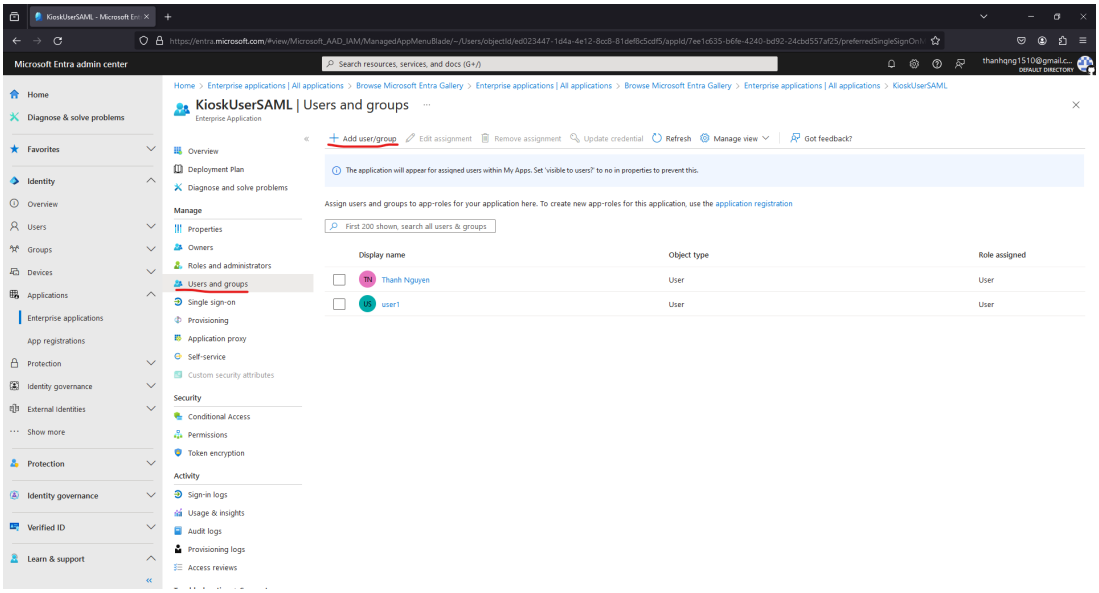
2. User Assignment on Entra ID

Step 1. Navigate to the created application overview page.

Step 2. Select **Users and groups**.

Step 3. Click **Add users/groups**.

Step 4. Choose the users or groups you intend to grant access to the application and click **Assign** to complete the user assignment process.

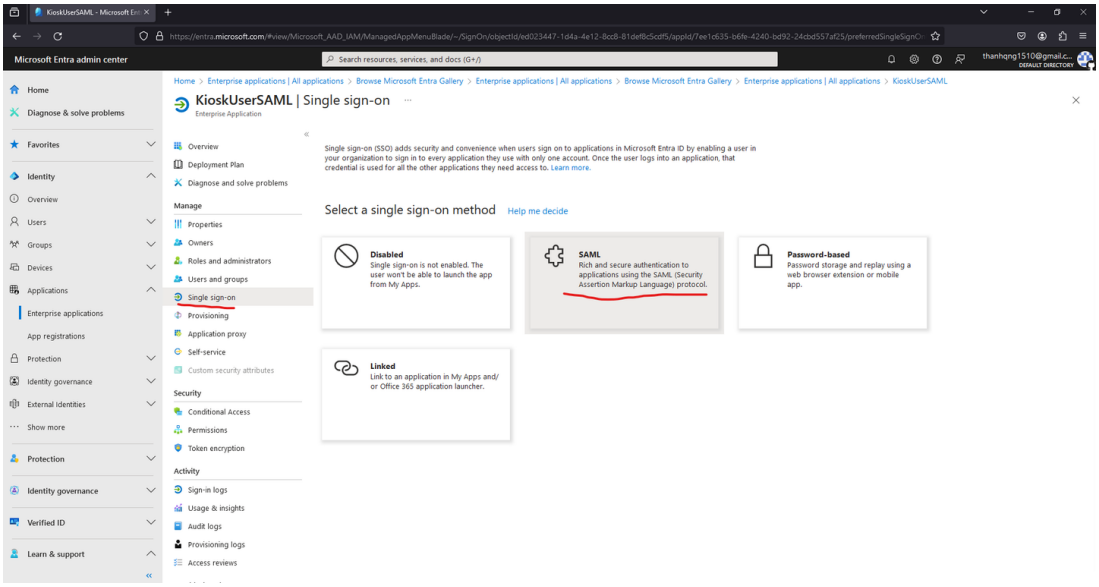


User and groups assignment page

3. Get App Federation Metadata Url

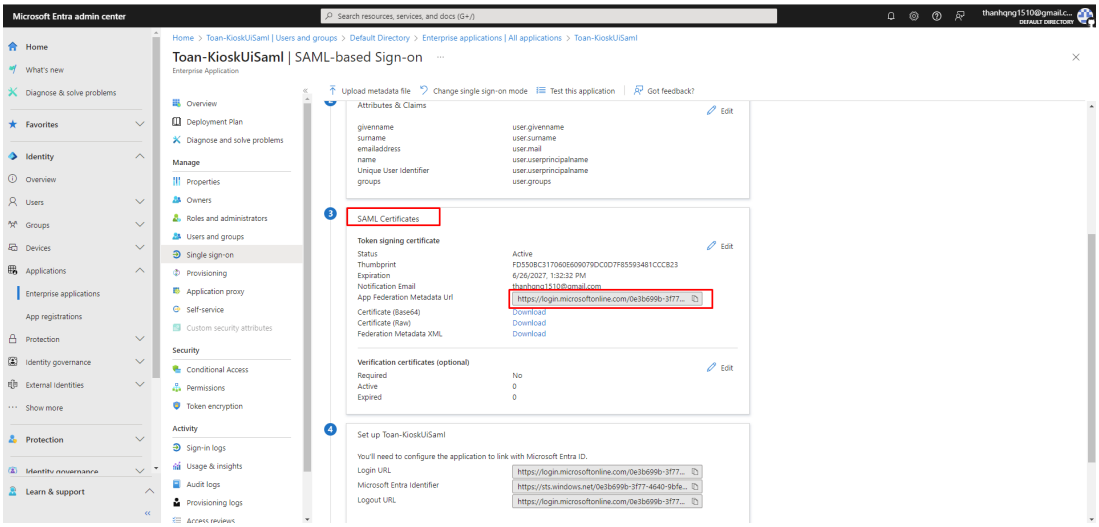
Step 1. Within the application overview page, navigate to the **Single sign-on** section.

Step 2. Choose **SAML** as the designated mode.



Single sign-on configuration

Step 3. Scroll down to section 3 (**SAML Certificates**), and copy the **App Federation Metadata Url**.

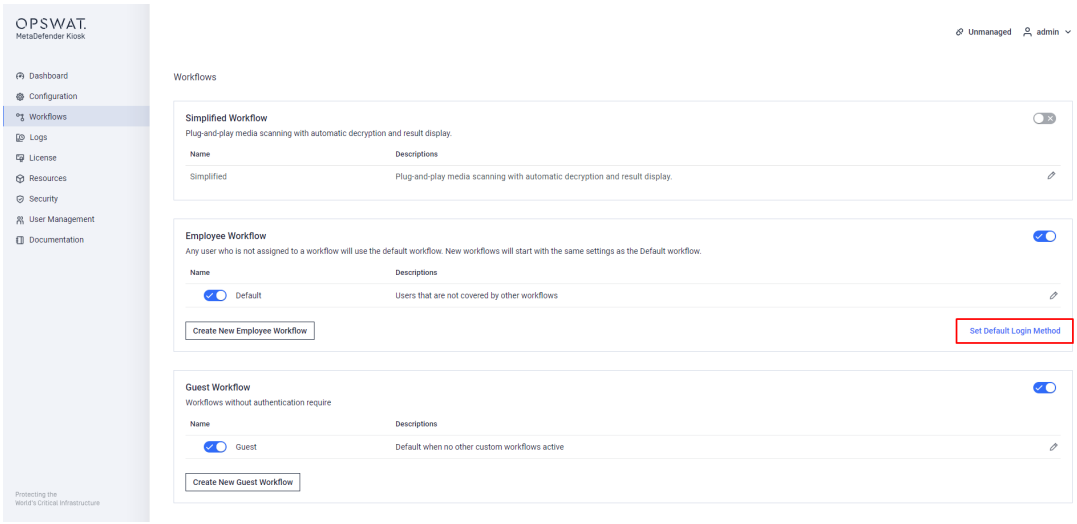


SAML Certificates configuration

4. Configuration on WebMC

4.1. Set up authentication method for KIOSK UI

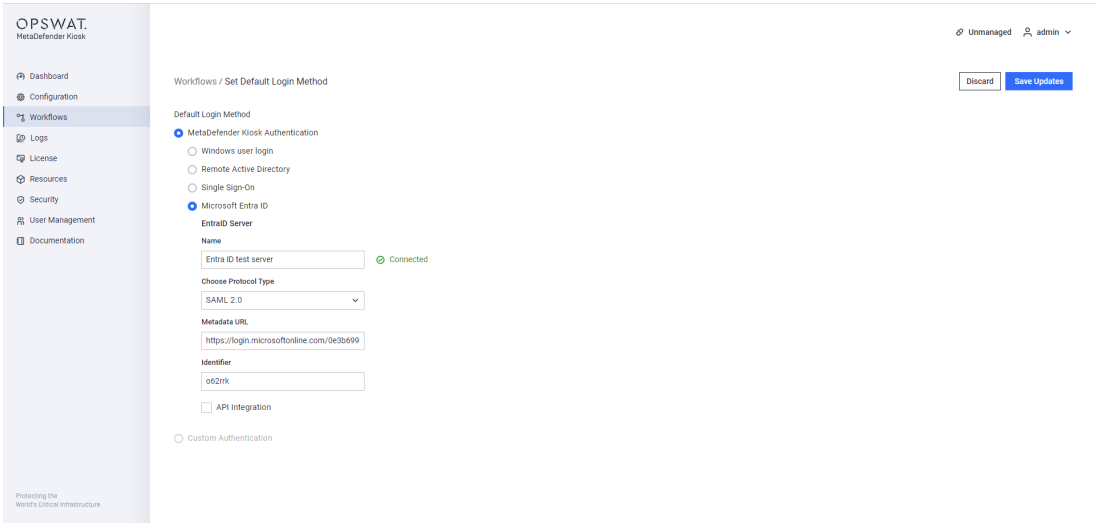
Step 1. Switch to the **Kiosk Console Management**, login with Administrative account, navigate to **Workflows** > **Set Default Login Method**



Set Default Login Method for authentation to KIOSK UI

Step 2. Select **Microsoft Entra ID** on **MetaDefender Kiosk Authentication**

Step 3. Assign a descriptive name and paste the **App Federation Metadata Url** earlier to the **Metadata URL.** If setup properly, an identifier will appear.



Microsoft Entra ID configuraion on WebMC

Step 4. Create the **Login URL** with the provided **Identifier** value following the format:

Format of Login URL for KIOSK UI
<http/https>://localhost:***<port>***/metadefender_rest/uissologin/saml/***<Identifier>***

Substitute the placeholder enclosed in angle brackets <> with the present configuration of the **Kiosk Console Management server** and the identifier value you previously copied. "localhost" must not be modified.

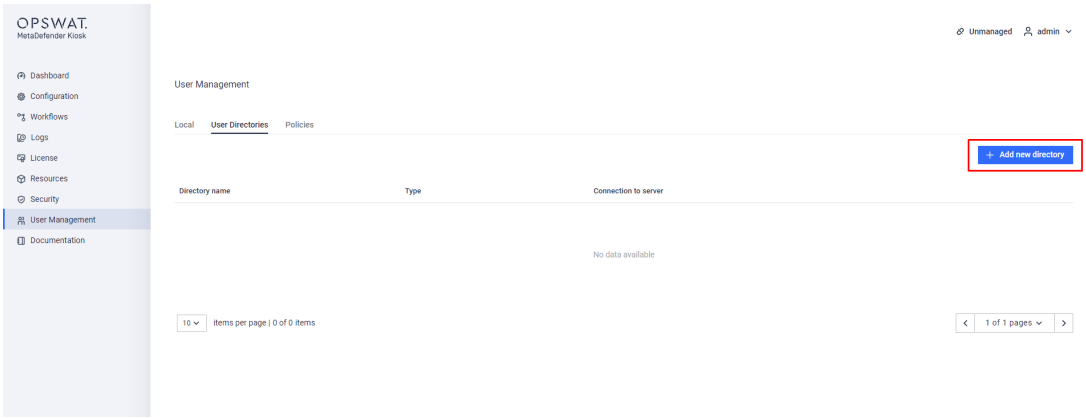
Step 5. Copy the **Login URL** for 5. Configuring SAML Single Sign-On

Info
API Integration is an optional advanced feature to enable fetching users from Entra ID server for Workflows assignment and contact adding. See Integrate with Microsoft GraphAPI and fetching Users/Groups for more details.

Step 6. Click on **Save Updates** to apply the changes

4.2. Set up authentication method for KIOSK WebMC

Step 1. Switch to the **Kiosk Console Management**, login with Administrative account, Navigate to **User Management > User Directories > Add new directory**



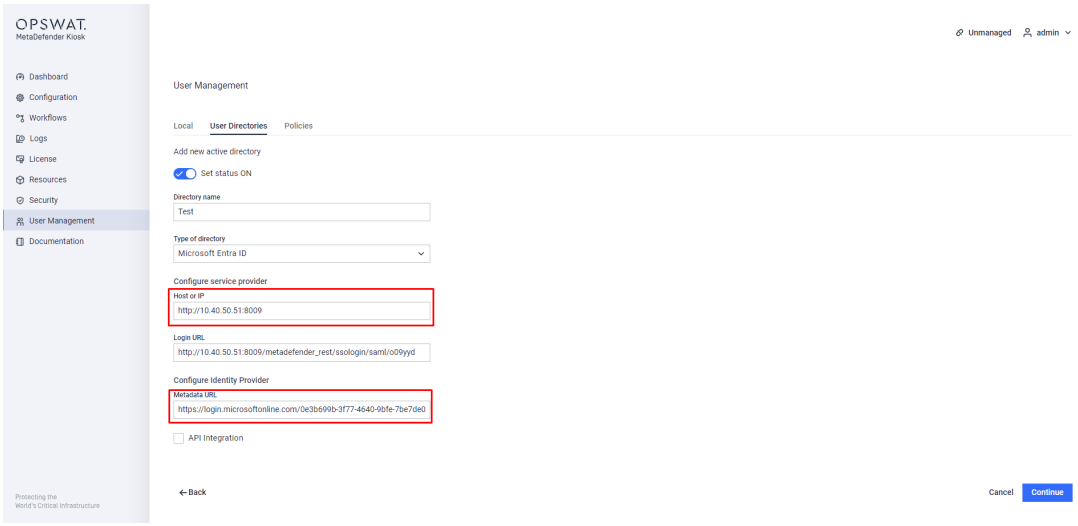
Add new directory for authentation to KIOSK WebMC

Step 2. Select **Microsoft Entra ID** type

Step 3. Assign a descriptive name and paste the **App Federation Metadata Url** earlier to the **Metadata URL.**

Step 4. Input **Host or IP** as your KIOSK WebMC remote access URL following the format:

Format of WebMC remote access URL
<http/https>://localhost:***<port>***/metadefender_rest/ssologin/saml/***<Identifier>***



Step 5. Copy the **Login URL** for step 5. Configuring SAML Single Sign-On

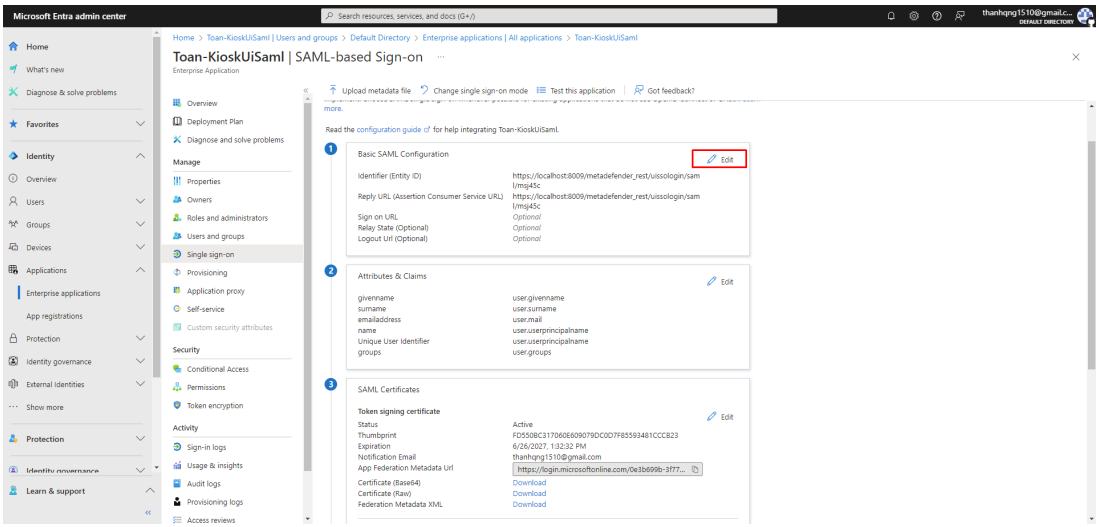
> **Info**
> **API Integration** is an optional advanced feature to enable fetching users from Entra ID server for Workflows assignment and contact adding. See Integrate with Microsoft GraphAPI and fetching Users/Groups for more details.

Step 6. Click **Continue** and finish steps for intial setup

5. Configuring SAML Single Sign-On

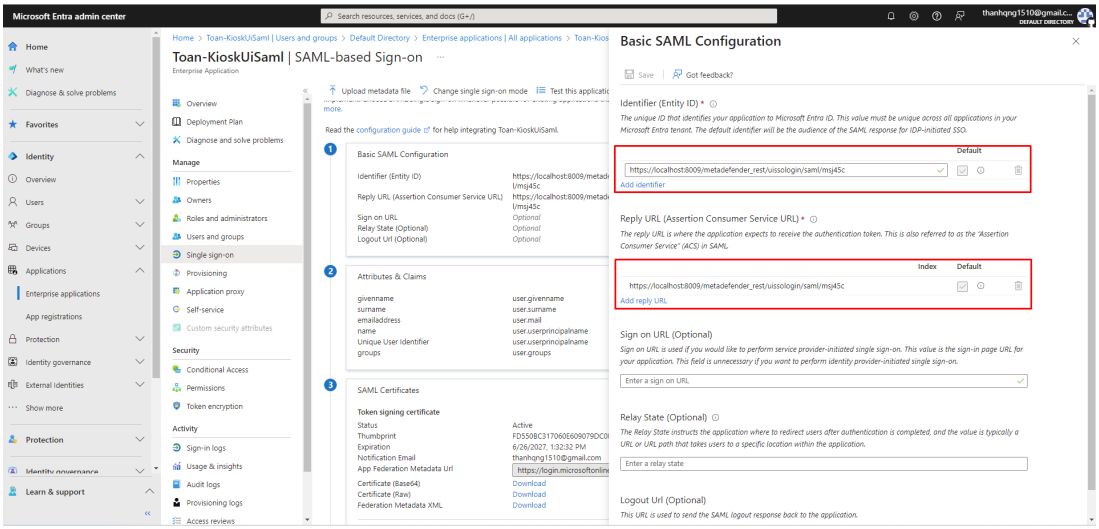
5.1. Basic SAML Configuration

Step 1. Switch back to the **Microsoft Entra admin center,** in the **Single sign-on** section. Scroll up to section 1 (**Basic SAML Configuration**), click on **Edit**.



Editting Identifier (Entity ID)

Step 2. Within field **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)**, enter the Login URL that copied earlier.



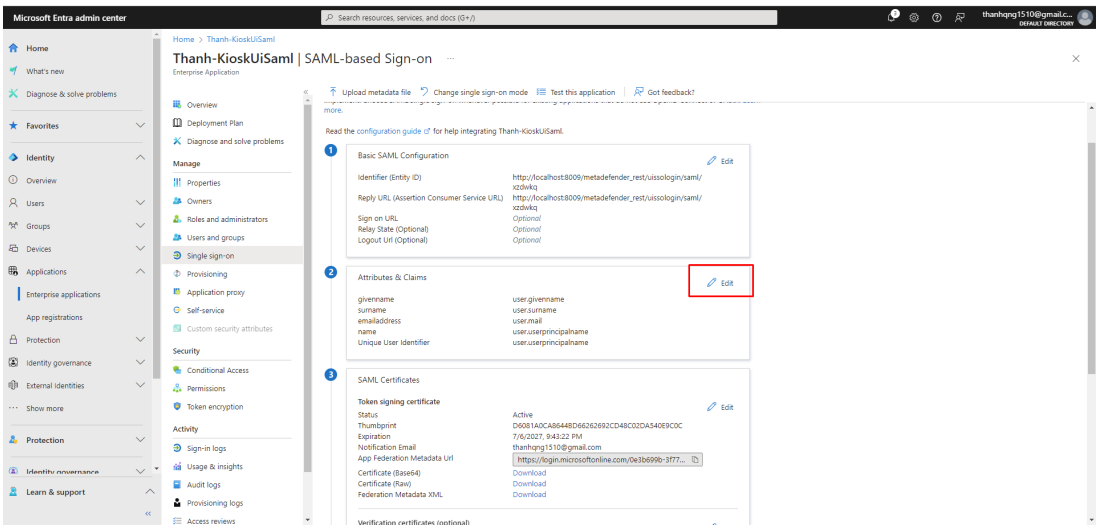
Change the configuration with provided Identifer

Step 3. Click **Save** to finalize the SAML configuration.

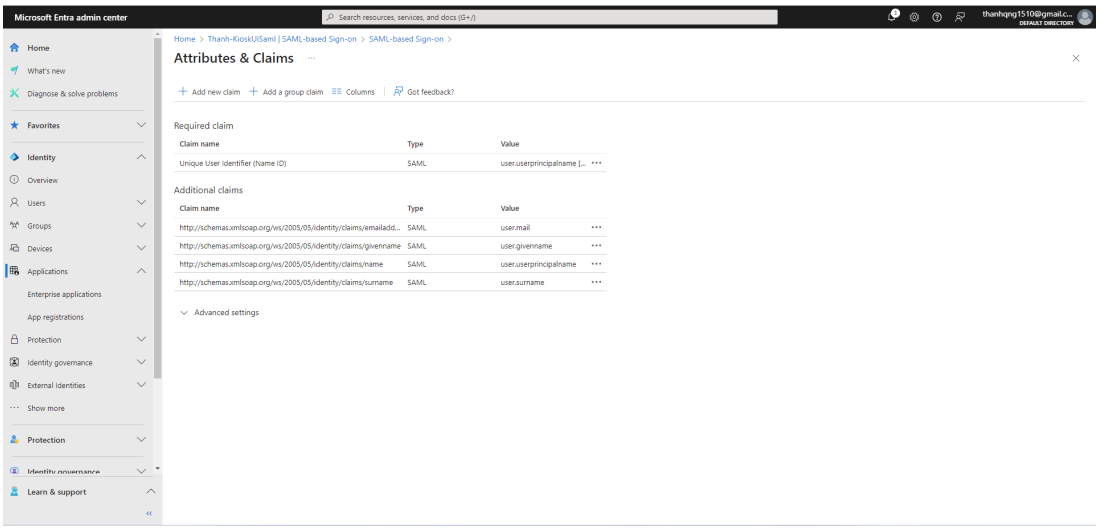
5.2 Enable groups to login to SAML SSO

The following steps need to be completed if you want all users of a group are able to login into your application

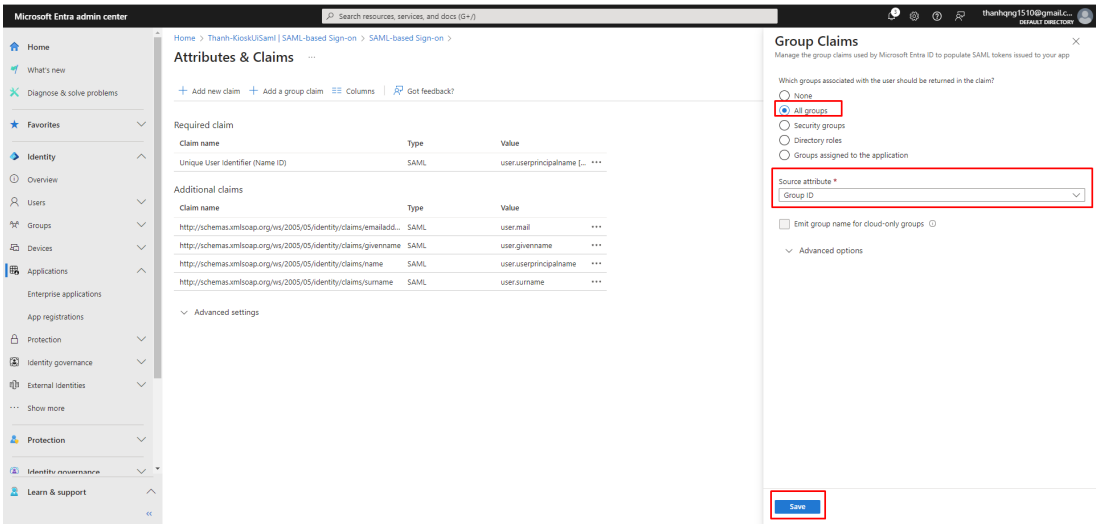
Step 1. Edit Attributes & Claims for Group assigning



Step 2. Click on **Add a group claim**



Step 3. Configure the **Group Claims** as following and click **Save**



Configuring the Group Claims

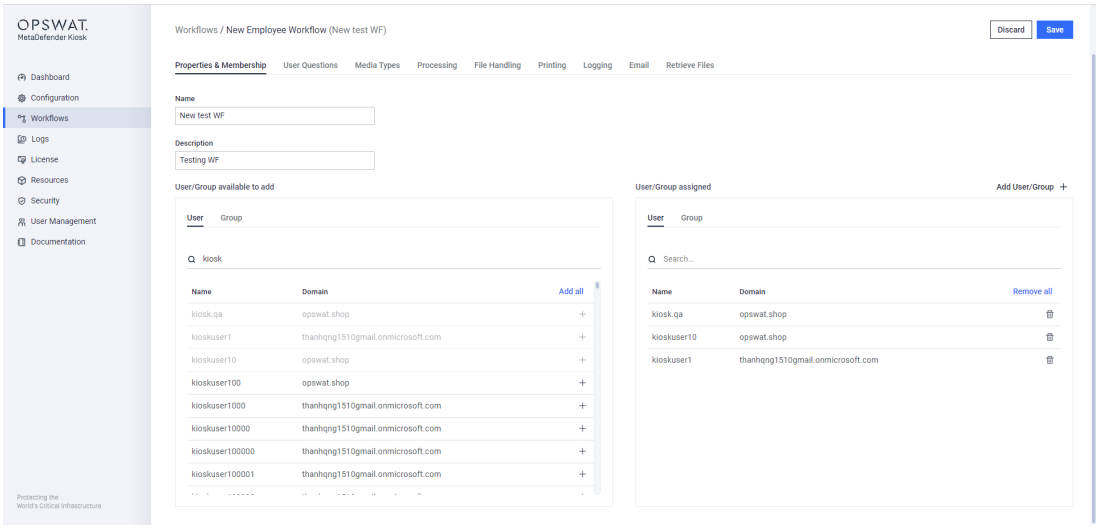
6. User assignment configuration on WebMC

KIOSK supports user assignments after finishing the integration by:

- Manual adding with the UPN and Display Name
- Add from **User/Group available to add** with **API Integration** is enabled.

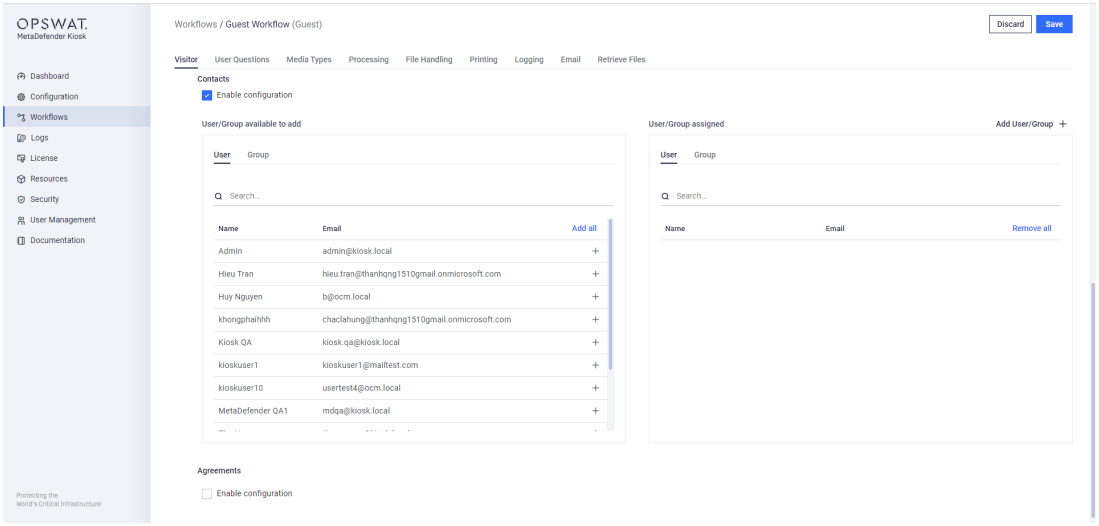
6.1. User Assignment for login to KIOSK UI

You can assign the user/group to the specific Workflows of KIOSK by adding on **Workflows** > **Create/Edit Workflow** > **Properties & Membership**



Properties & Membership assignment with fetched users/groups from Entra ID on WebMC

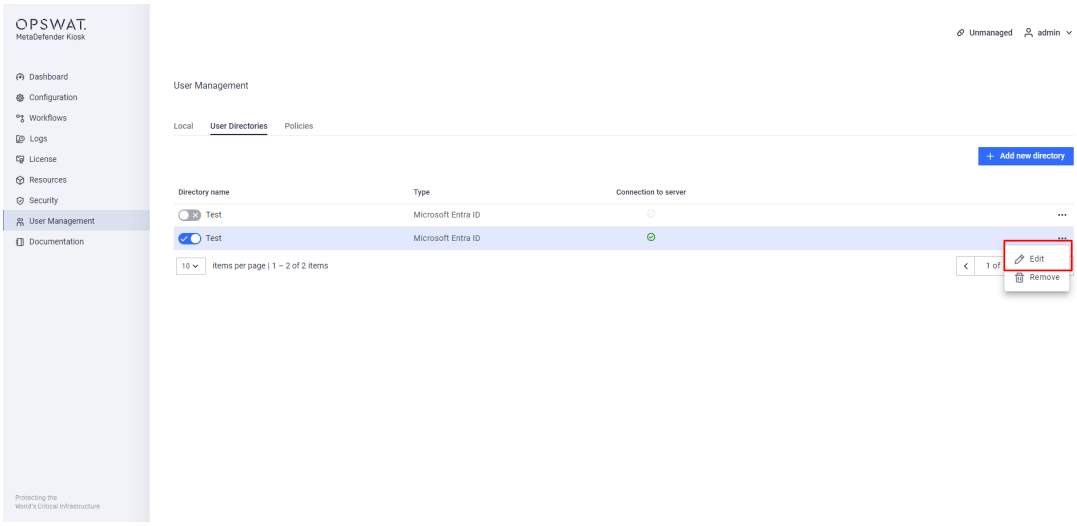
You can add the user/group as reference contact of visitor on KIOSK UI at **Workflows** > **Guest workflows** > **Visitor** > **Contacts**



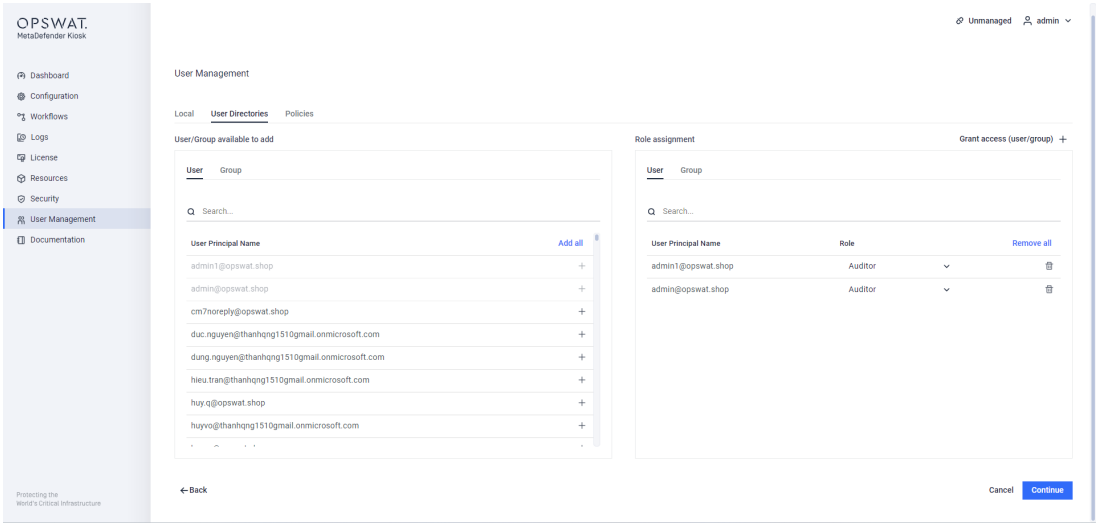
Contacts adding for Visitor management workflow on WebMC

6.2. User assignment for login to KIOSK WebMC

Step 1. Assign a user to specific role by navigating to **User Managerment** > **User Directories** > **Edit**



Step 2. Click **Continue**, select **Role matching option**



Role assignment to login to KIOSK WebMC

Step 3. Click **Coninue** and finish the settings.

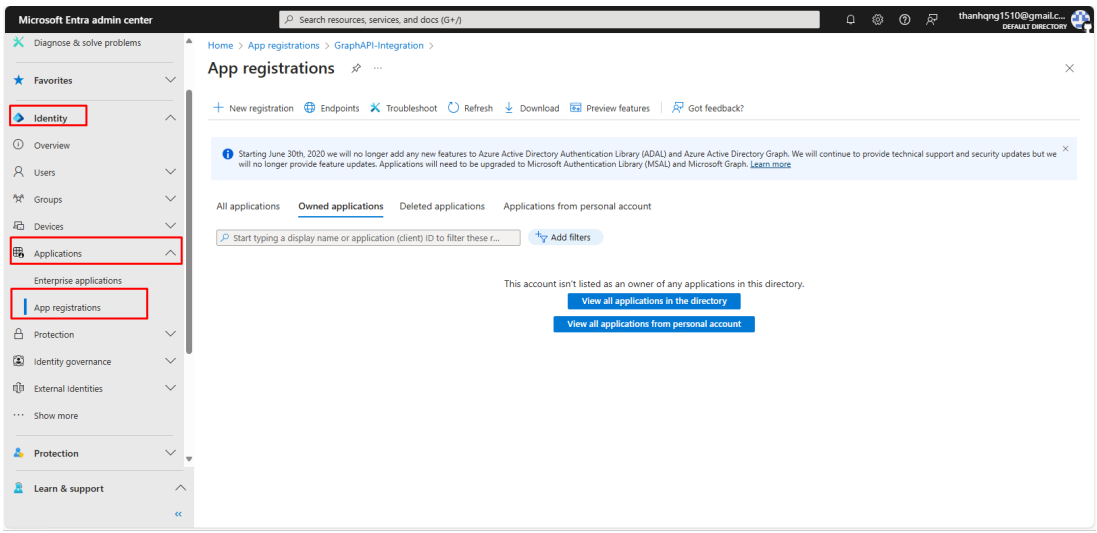
Integrate with Microsoft GraphAPI and fetching Users/Groups

The optional feature "**API Integration**" enables KIOSK deeply integrate with Microsoft Entra ID to get the users from the Microsoft Entra ID server and put to **User/Groups available to add** section for Workflows assignment or Contacts visitor adding.

1. GraphAPI Application Registration

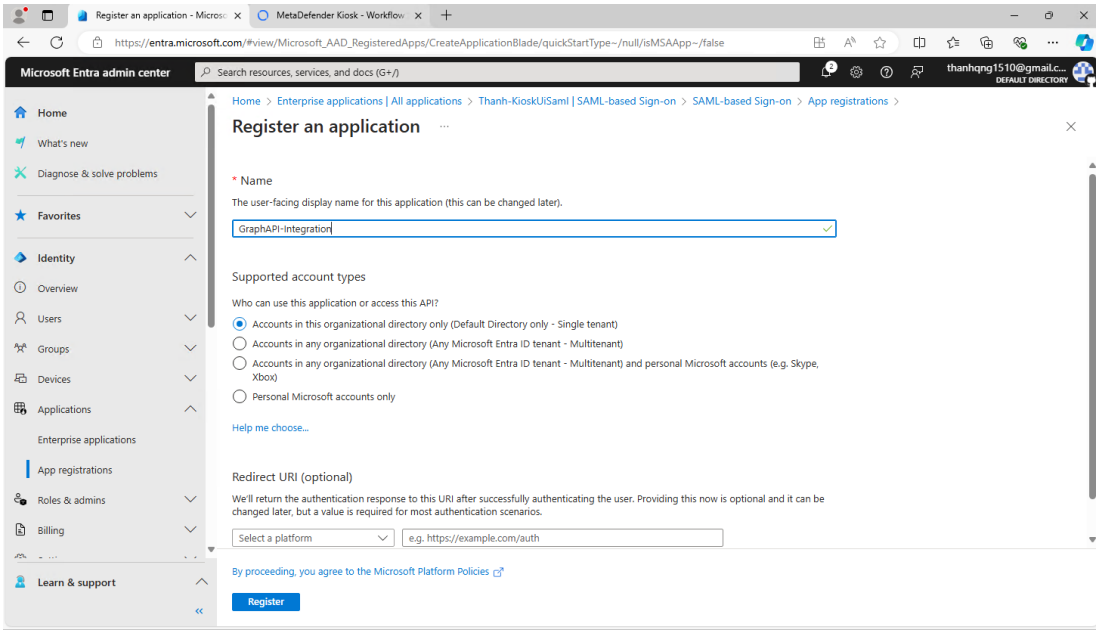
> **Info**
> KIOSK requires a separate application registration with specific permissions to access user and group information within a tenant.

Step 1. Access the Microsoft Entra admin center (Microsoft Entra admin center) using your administrative credentials. Navigate to the **Identity > Applications > Enterprise applications** section.



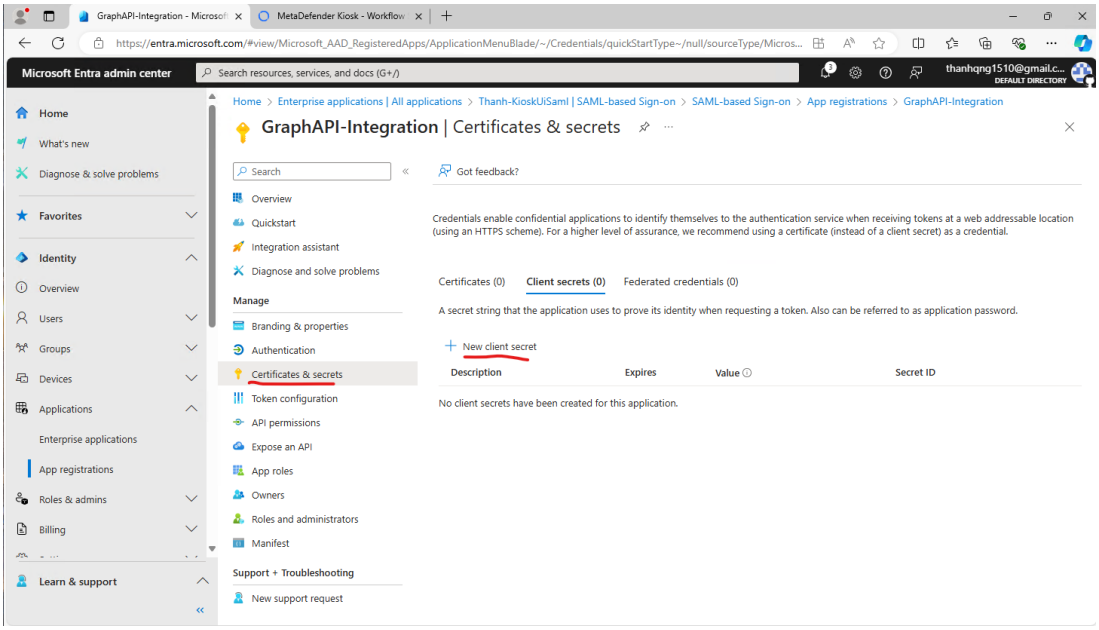
App registration configuration page

Step 2. Select **New registration** and choose a descriptive name for your registration, then hit **Register**.



Register an application page

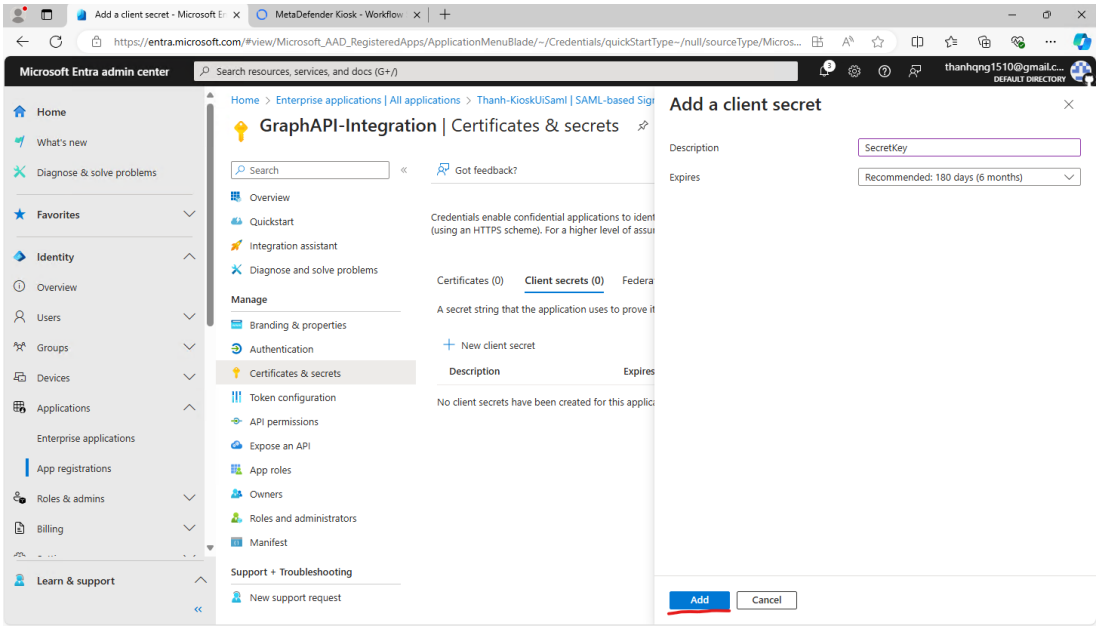
Step 3. Within the **Registration Overview Page**, click the **Certificates & secrets** blade, and hit **New client secret.**



Get new client secret

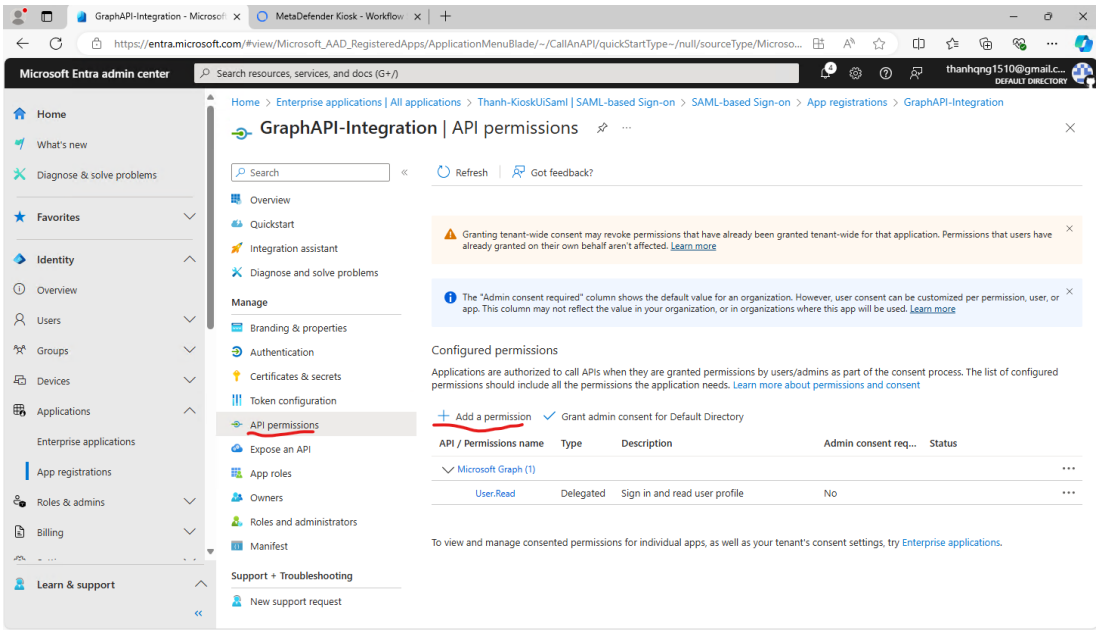
Step 4. Set the description and expires time for the secret, then hit **Add**. Note **Client Secret** down for using later.

> **Warning**
> The **Client Secret** is accessible for viewing immediately after creation, but subsequently hidden.



Add a client secret

Step 5. Next, click the **API permissions** page and click **Add a permission**.



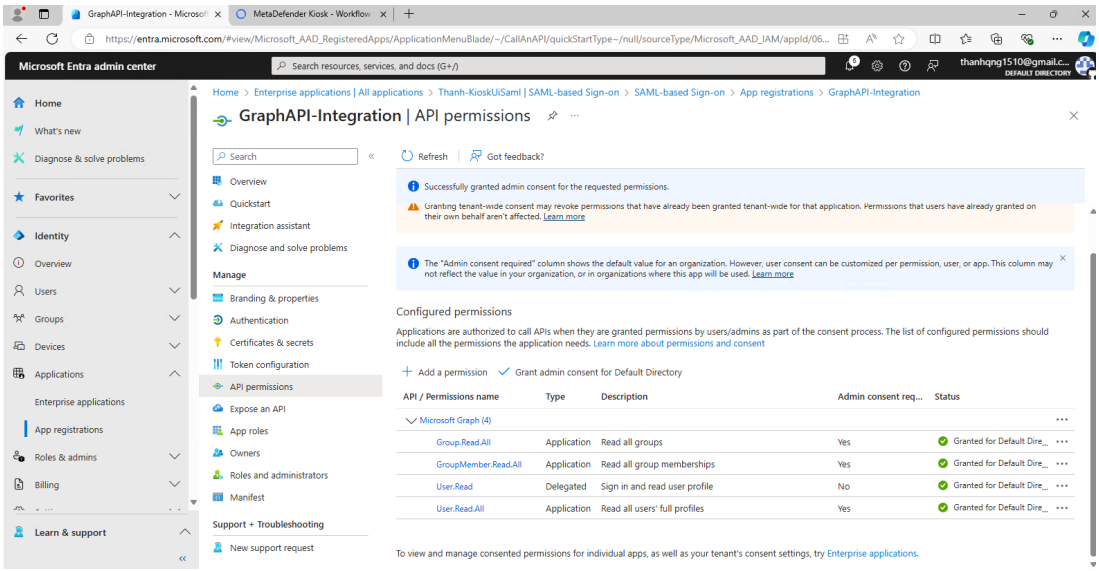
API permissions page

Step 6. Within tab **Request API permissions**, select **Microsoft APIs > Microsoft Graph > Application permissions.** Then search and add these permissions:

- **User.Read.All** permission to query users from tenant.

- **Group.Read.All** permission to query groups from tenant.
- **GroupMember.Read.All** permission to query users within groups.

After adding all permissions, hit the button **Grant admin consent for Default Directory.** Review the permissions below.

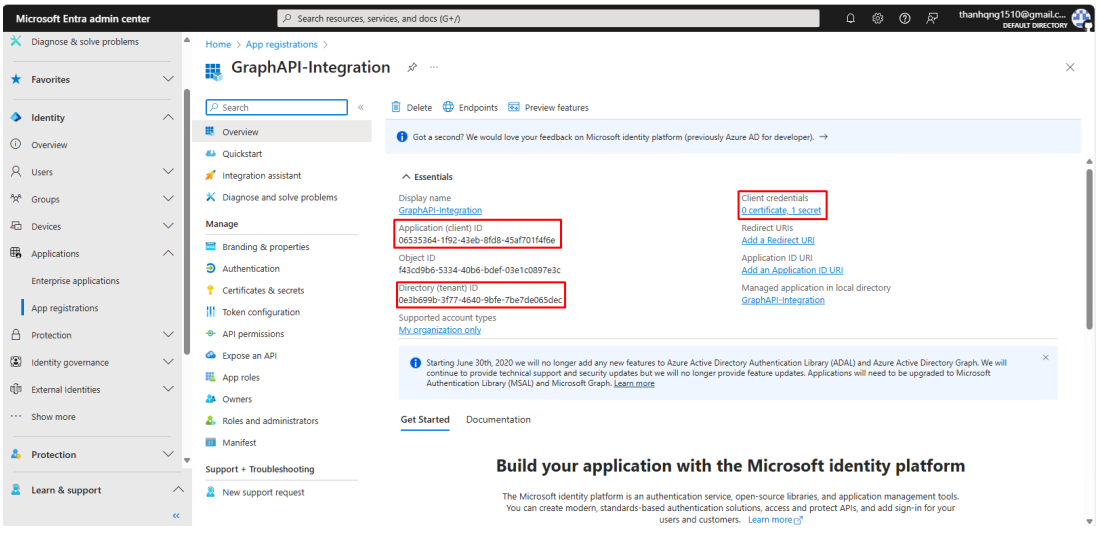


Adding all needed permissions

2. Configure GraphAPI Integration

Step 1. Switch to the **Overview Page**, note down these values:

- Application (client) ID.
- Directory (tenant) ID.
- Client secret.

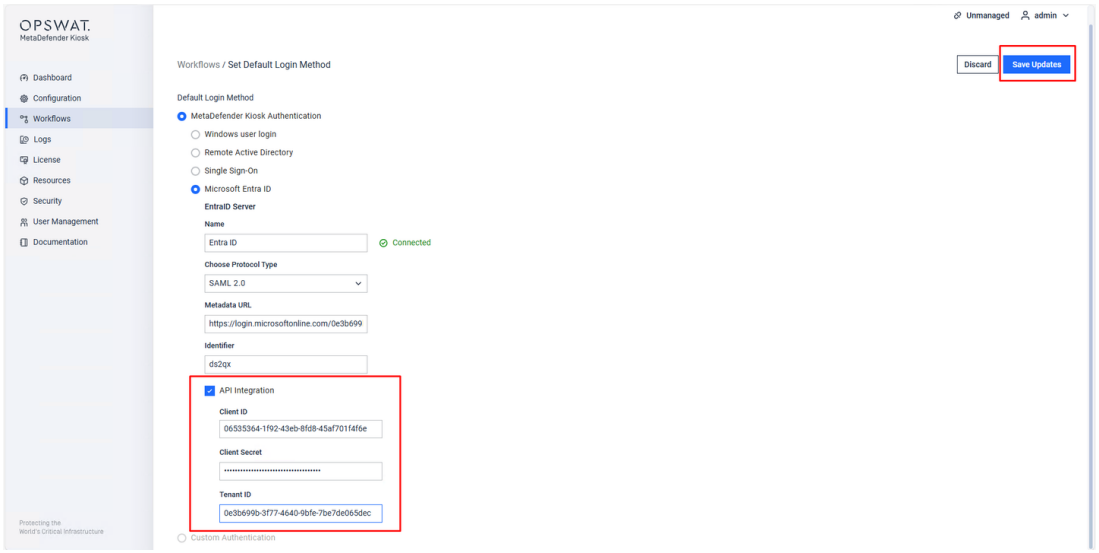


Necessary input that will be used on WebMC

Step 2. Switch to the **Kiosk Console Management**, login with Administrative account.

Step 3. Navigate to **Workflows > Set Default Login Method > Microsoft Entra ID**.

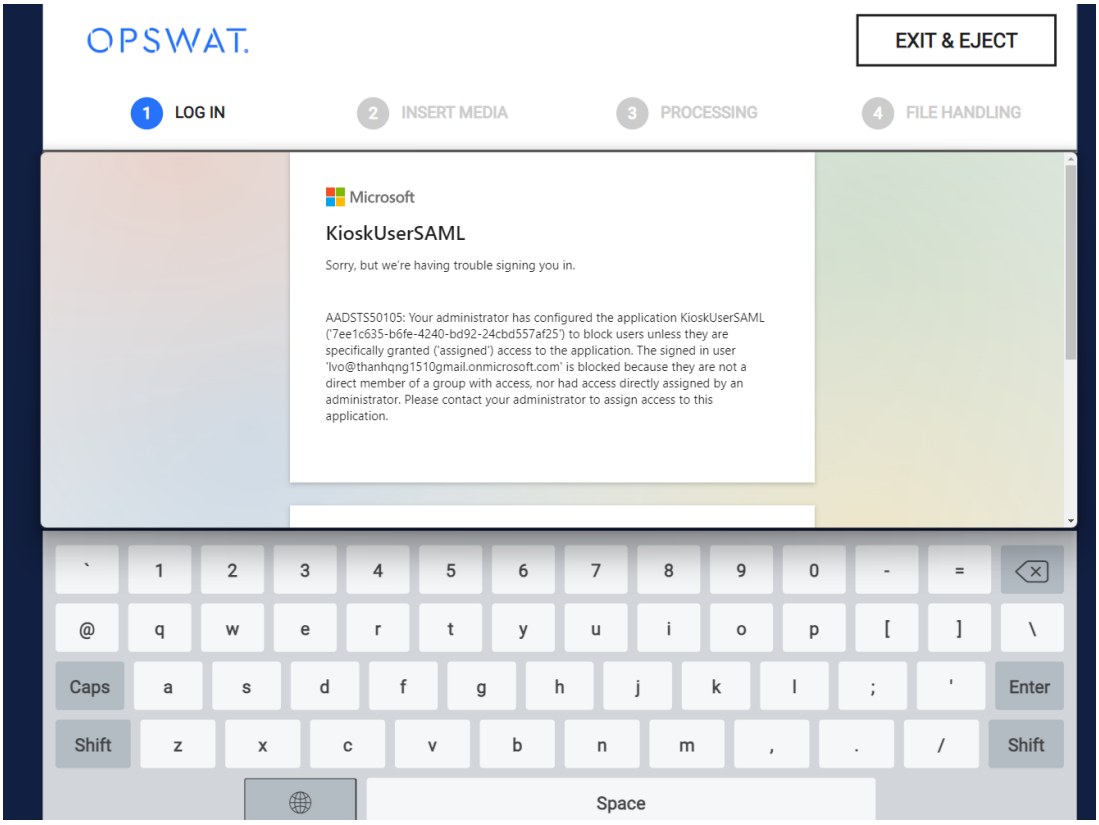
Step 4. Enable **API Integration**, then input 3 fields **Client ID**, **Client Secret** and **Tenant ID**. Then hit **Save Update**.



API Integration configuration on WebMC

Sign in to the KIOSK using your Microsoft Entra ID account

- When authorized user wants to login on the Kiosk Interface Application, they must provide their **User Principle Name.** This property has the format of <username>@<domain>.
- **Un-authorized users** tries to login to the **Kiosk Interface Application** will result in the following error.



Failed to login due to permission

> **Warning**
> Retrieving files from MFT or directory via SSO is not yet supported.

Set up for multiple KIOSKs using mass configuration on OCM/My OPSWAT

Mass configuration for managed/enrolled KIOSK instances can be accomplished by using the group setting functionality within OCM (OPSWAT Central Management) and My OPSWAT.

All KIOSKs within the group setting can authenticate with Microsoft Entra ID using identical Metadata URLs and Reply URL.

Encrypted Device Verification And Approval

The Kiosk system protection functionality will check file integrity in the unlocked partitions of encrypted peripheral media devices before decryption. The encrypted devices containing unauthorized data will be spotted and require approval before being added to the data whitelisting and usable with the Kiosk system

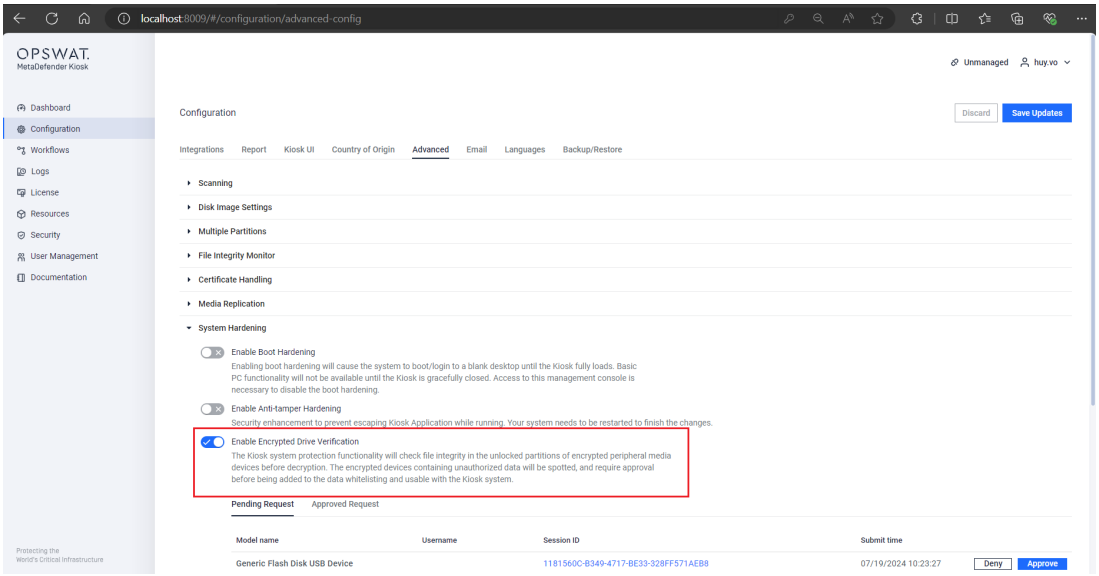
Enabling the feature

Step 1. Navigate to the Configuration Page

- Log in to the Web Management Console with the your administrative credential.
- Go to the **Configuration** page, which can be found under the **Advanced** tab in the menu.

Step 2. Enable Encrypted Drive Verification

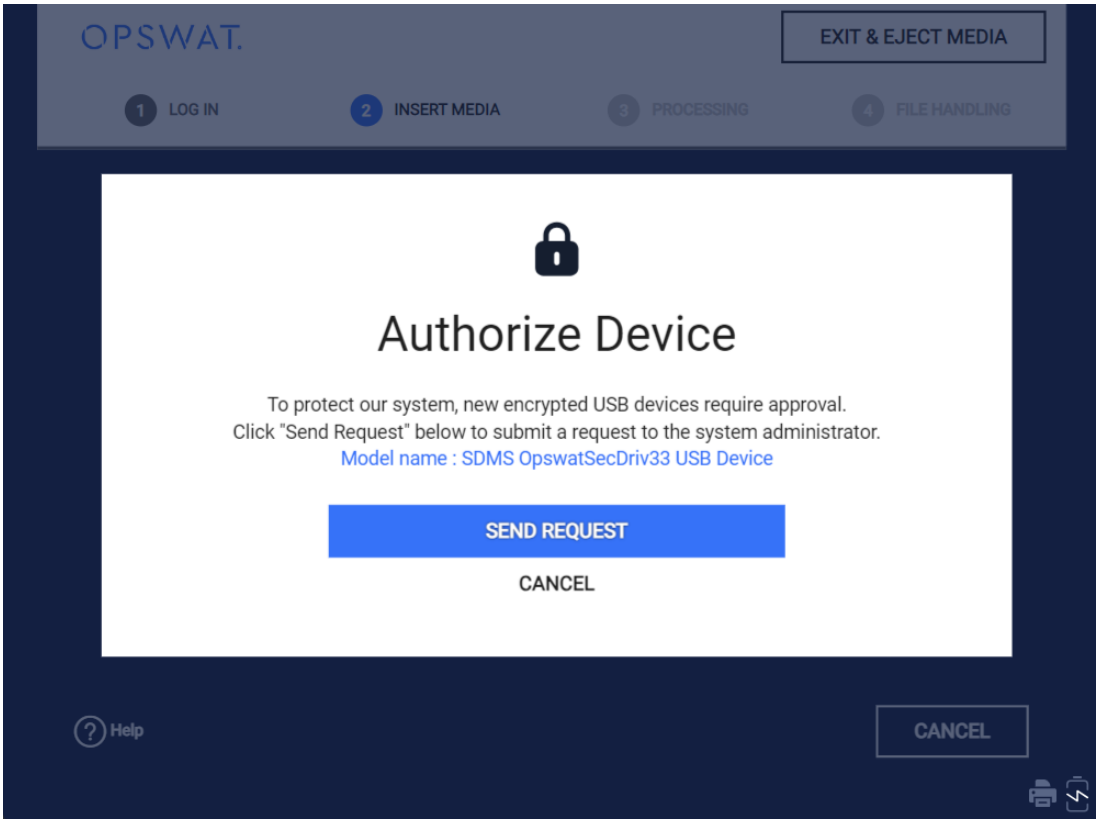
- Locate the option for **Encrypted Drive Verification** within the configuration settings.
- Enable this feature by toggling the switch.
- Click on **Save Updates** to apply the new settings.



Enable Encrypted Drive Verification

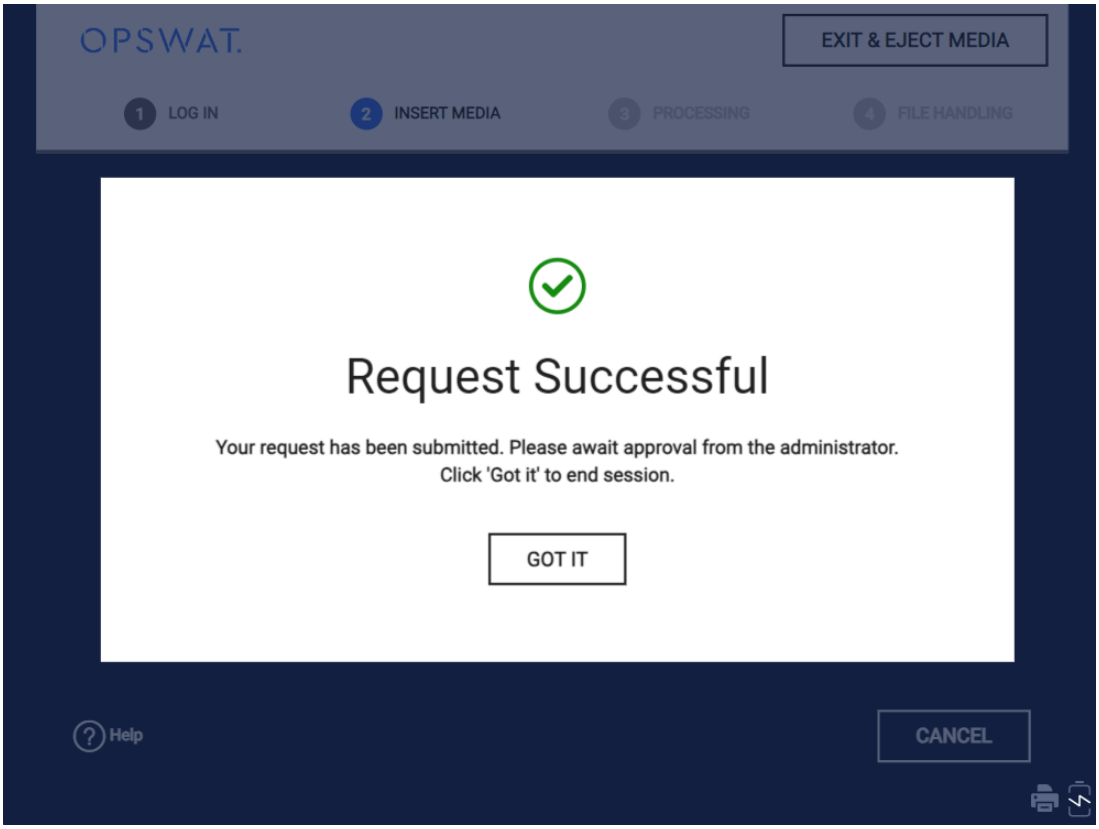
How it works on KIOSK UI

- When a user connects an encrypted USB device for scanning or data copying, the application will verify if the device has been authorized by an administrator:
    - If approved, a dialog box will request the user to input the password to unlock the encrypted device.
    - If not approved, a dialog box will notify the user that approval is required for the device.



Authorize Device notification

- Upon clicking the "Send Request" button, a notification will be sent to the administrator when they log in to the WebMC, indicating a new device approval request.

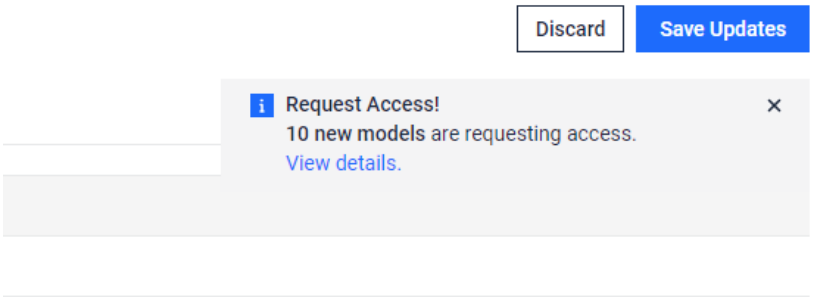


Request has been sent successful

Approval Process

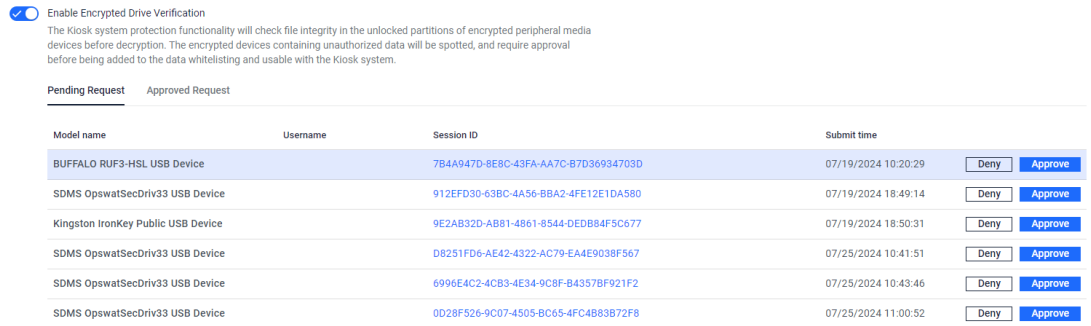
Notification of Pending Requests

Upon login, the administrator will be presented with a notification showing the count of pending device approval requests.

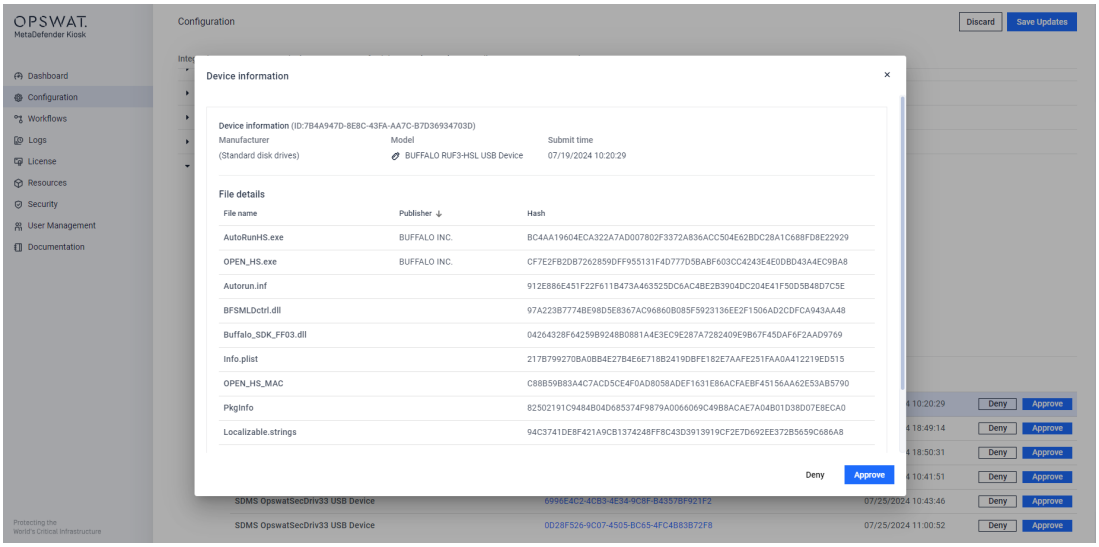


Reviewing Device Requests

- Administrators can access the Web Management Console to review pending device approval requests. They can navigate to the Pending Requests section to view the list of requests from users.



- Administrators can access detailed information about each request, including a list of files stored on the unlocker partition of the device.



Approving or Denying Requests

- Upon reviewing the device details, the administrator can choose to approve or reject the request. If approved, the device will be included in the list of validated devices and the request will be moved to **Approved Request** section.
- The admin must click on **Save Updates** to finish the approval process.

Notes and limitations

This feature is supported with mass configuration on OPSWAT Central Management (OCM) with Set Setting:

- The approved requests will be applied to all instance.
- Only the request from reference KIOSK instance are shown on Set Setting for approval.

This feature has not been supported on My OPSWAT yet.

Setup Microsoft SharePoint or OneDrive as storage

Checks for issues with file upload to Microsoft SharePoint or OneDrive
When Kiosk failed to upload files to Microsoft SharePoint or OneDrive, issues could be caused by misconfigurations. Including:

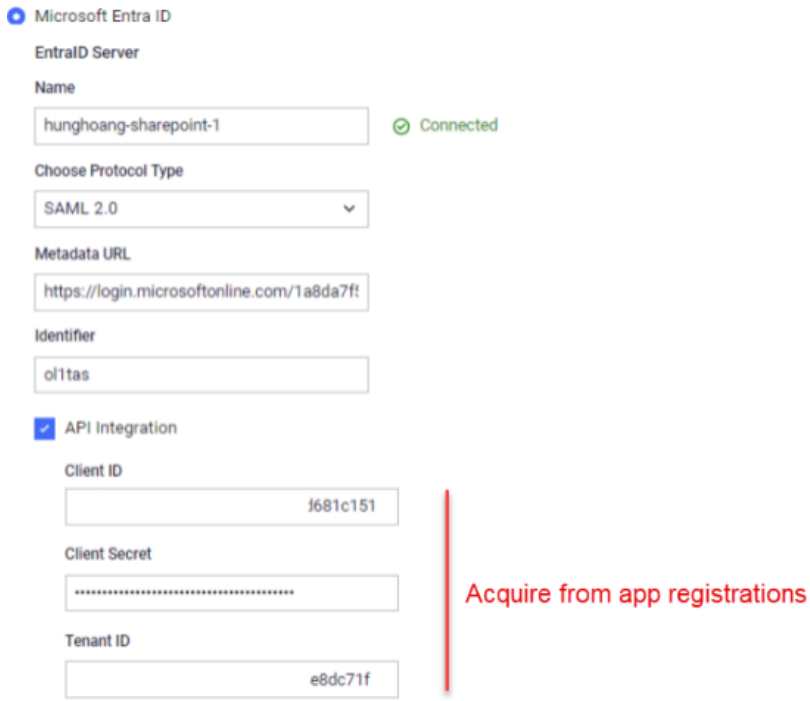
- Unable to login to Kiosk UI via SSO due to the users haven't been assigned to the Enterprise Application
- Missing redirect URI for OAuth2.0
- Missing API permissions (Sites.ReadWrite.All, Users.Read)
- Missing Office 365 license or the license does not cover SharePoint or OneDrive
- When adding or changing Office 365 license, it may take some time for the changes to take effect
- Invalid input when configuring SharePoint or OneDrive in Kiosk WebMC (e.g missing "/" for relative path)

Please verifying all potential causes above, and collect the Support Package if you still encounter issues uploading files to SharePoint or OneDrive

1. Enable Microsoft Entra ID with API Integration

Step 1. From Kiosk WebWC, select **Workflows**, under **Employee Workflows**, select **Set Default Login Method**. Enable SSO **Microsoft Entra ID**. Please refer to Microsoft Entra ID Integration for details

Step 2. For SharePoint and OneDrive integrations, enable **API integration**

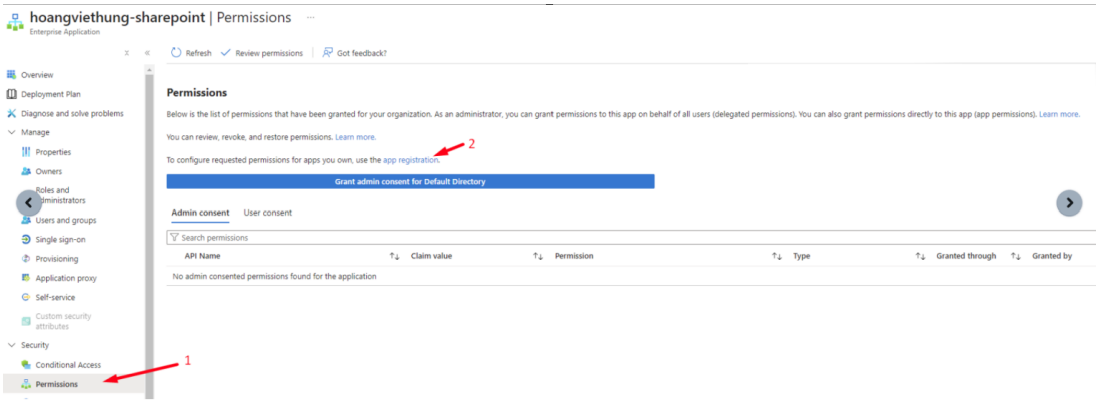


Follow the instruction to acquire the following information from **app registrations**

- Client ID
- Client Secret
- Tenant ID

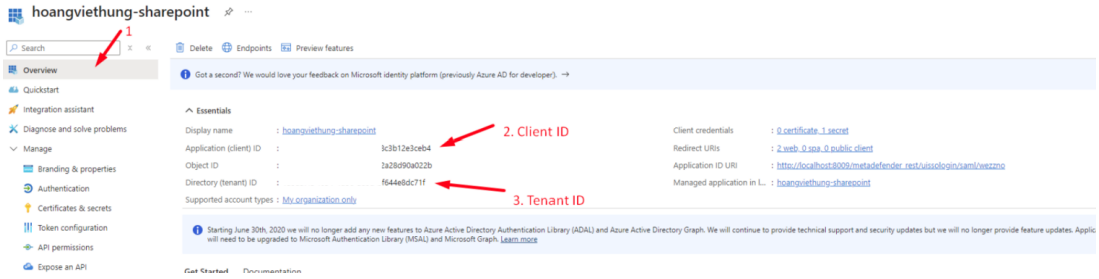
Notes: API Integration option must be enabled to configure SharePoint or OneDrive as storage

Step 3. Open the Enterprise Application created at step 1. Expand **Security**, select **Permissions**, click on **app registration**



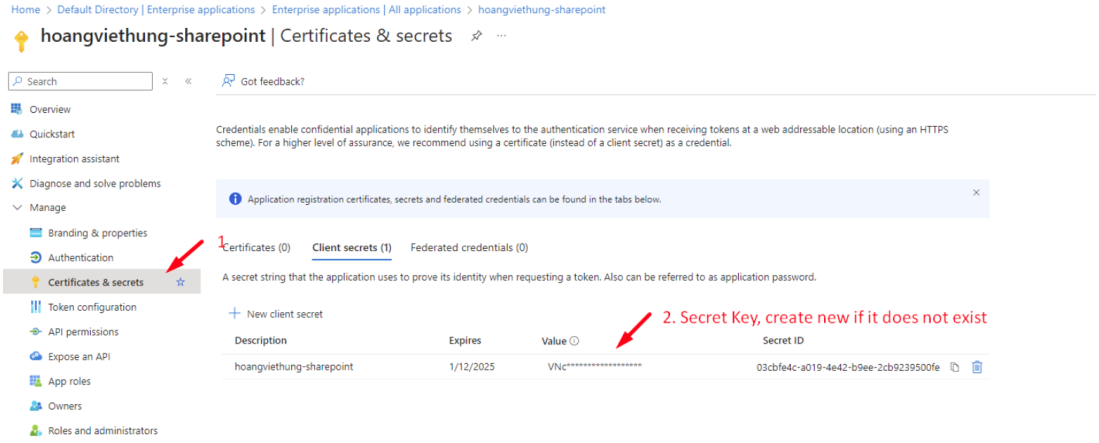
Access app registration

Step 4. From **app registration** page, select Overview. Here you can find **Client ID** and **Tenant ID**



Acquire Client ID and Tenant ID

Step 5. Expand **Manage**, select **Certificates & secrets**, select **Clients secrets**. Here you should find Secret Key. Please create a new client secret if one does not exist.



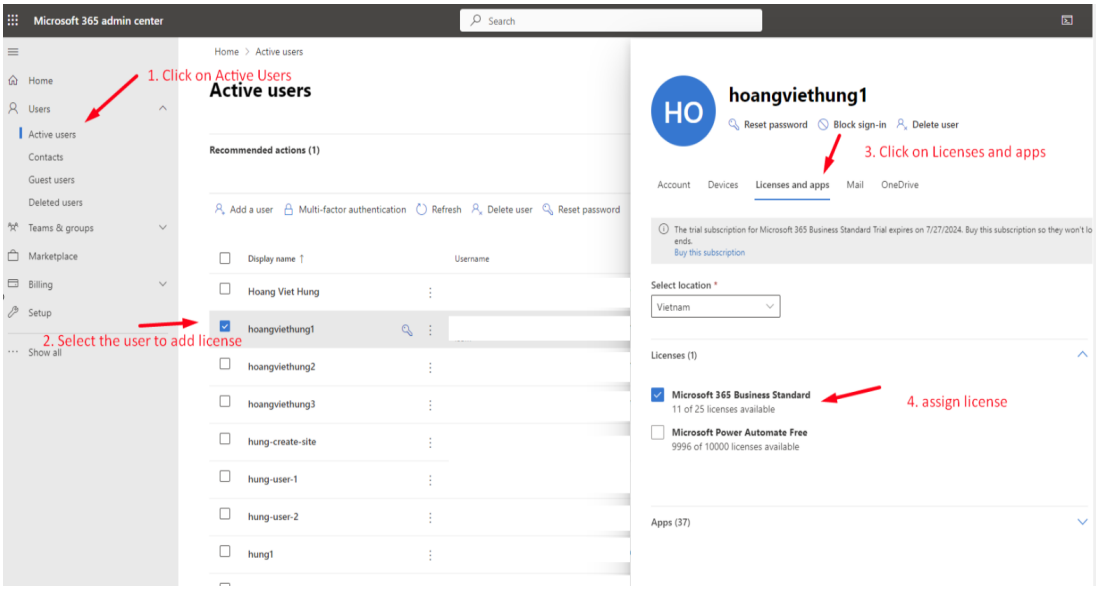
Acquire Client Secret

Notes: You MUST assign users to the Enterprise Application to allow them to login via SSO. Please follow Enterprise Entra ID Integration for setup details

2. Verify the Office 365 license on users

Step 1. Go to https://admin.microsoft.com/ to access Microsoft 365 Admin Center

Step 2. Expand **Users**, select **Active users**, select the user(s), select **License and apps**, enable **Microsoft 365 Business Standard**. Click **Save changes**



Verify and add license for users

Missing Microsoft 365 license Business Standard for users

After assigning Microsoft 365 license Business Standard for user, it may take about 10 minutes for the changes to take effect.

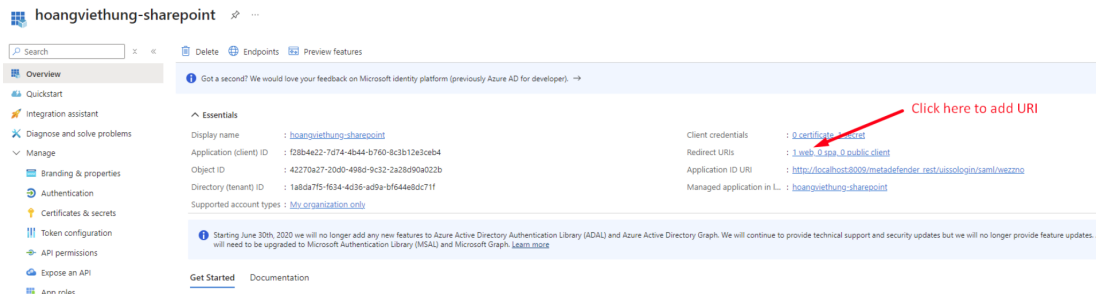
If the user account doesn't have license, you will encountered the following error message in Kiosk service log:

*"message":"**You do not have access to create this personal site or you do not have a valid license**"*

3. Configure Redirect URI for Oauth2.0

For authorization before uploading files to SharePoint or OneDrive, you need to configure Redirect URI in app registration

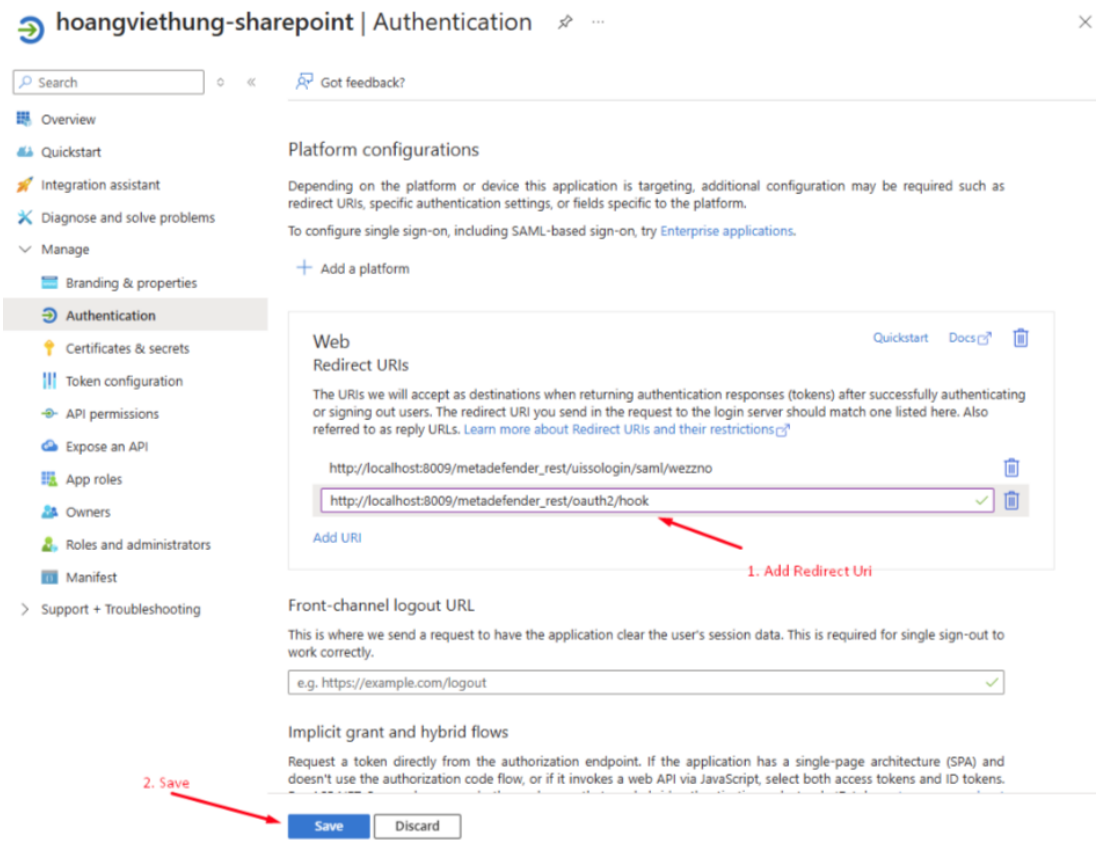
Step 1. In app registration, click on **Redirect URI** link to add a new URI



Add Redirect URI for Oauth2.0

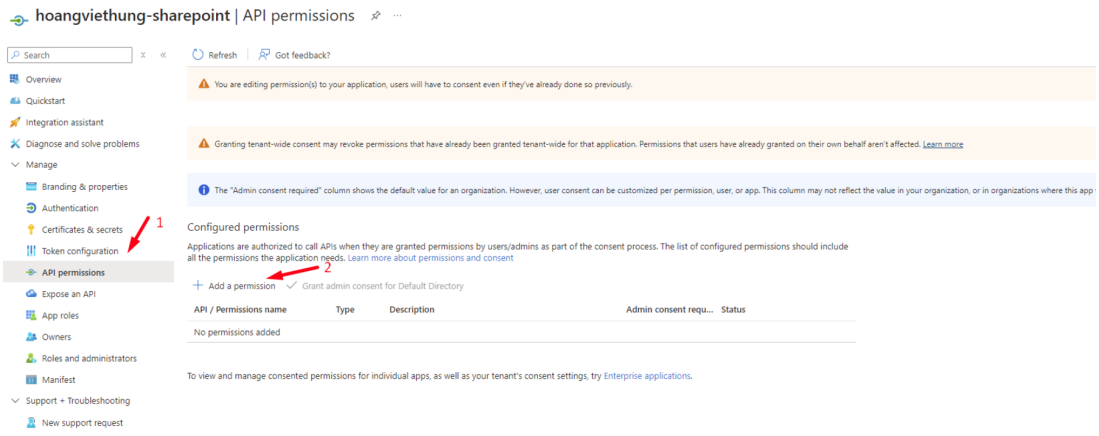
Step 2. Put in the Redirect URI. Click Save

Format for Redirect URI for Kiosk UI
<http/https>://localhost:*<port>*/metadefender_rest/oauth2/hook



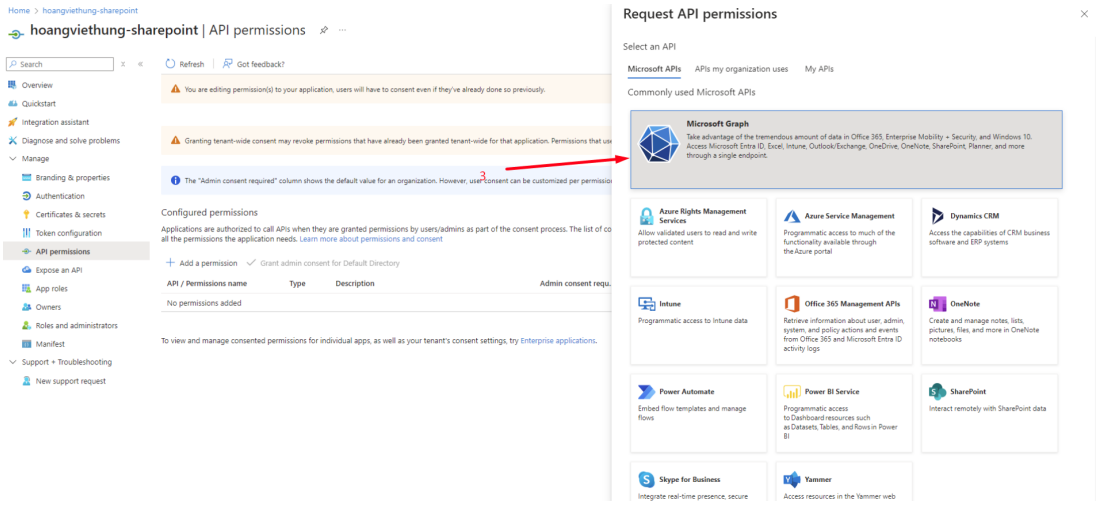
4. Grant API permissions that needed to upload files to SharePoint or OneDrive

Step 1. From app permissions, expand **Manage**, click on **API permissions**. Click **Add a permission**



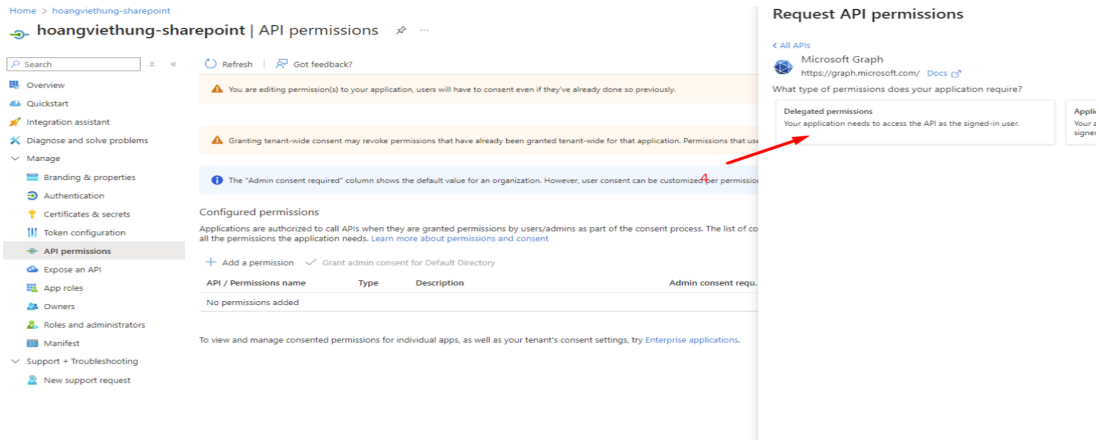
Add API Permissions for registered app

Step 2. Select **Microsoft Graph**



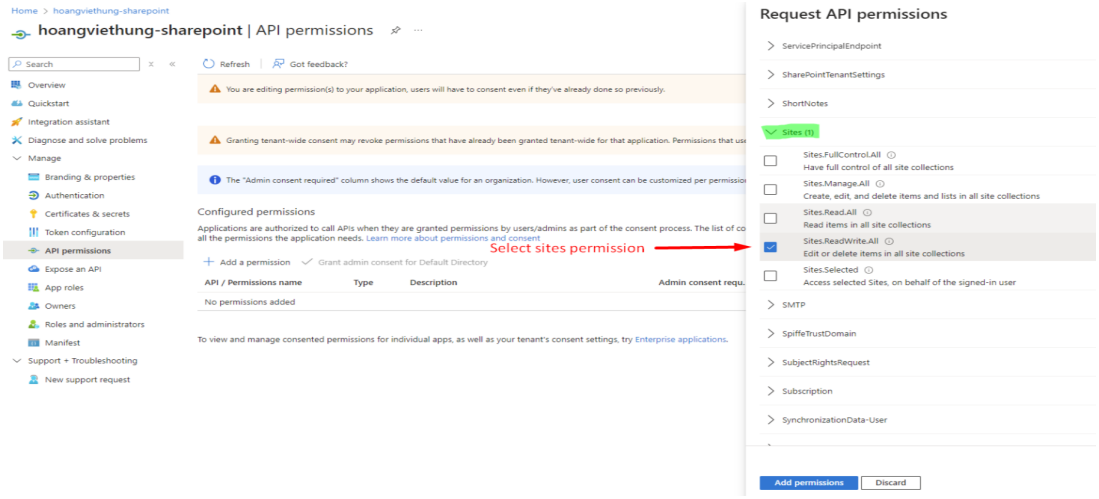
Select Microsoft Graph API

Step 3. Select **Delegated permissions**



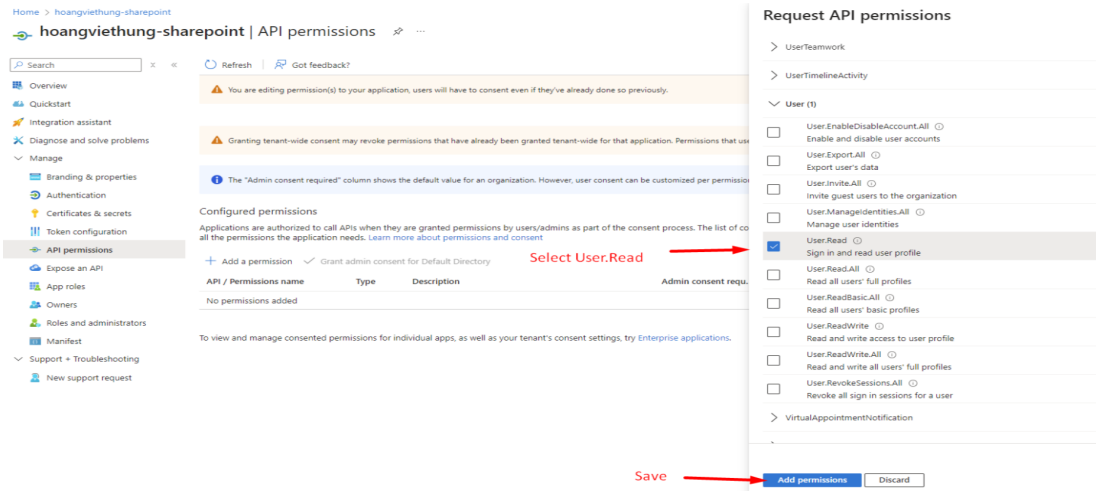
Select Delegated permissions

Step 4. Expand **Sites**. Enable **Sites.ReadWrite.All** permission



Enable Sites.ReadErite.All permission

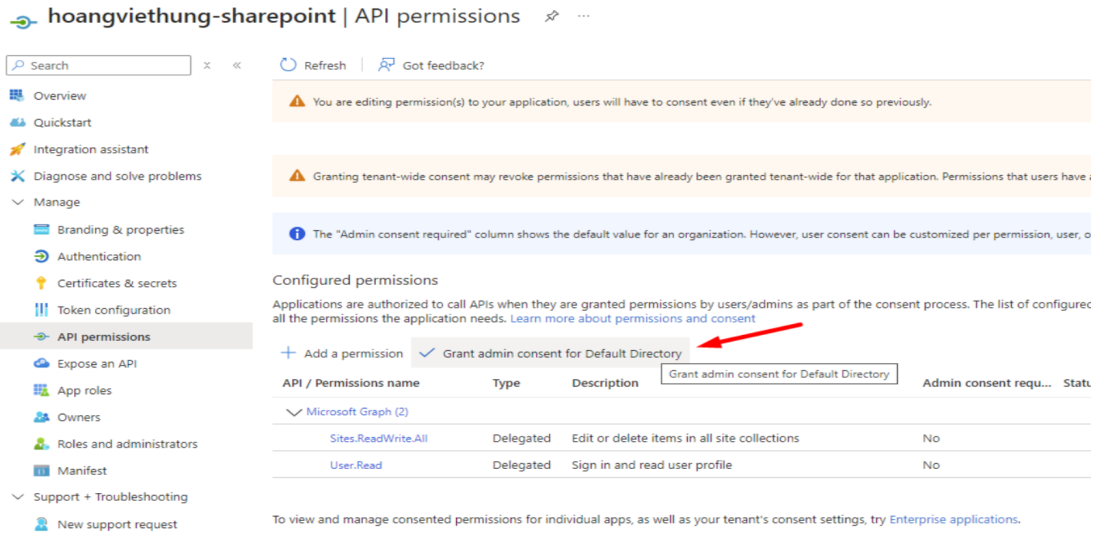
Step 5. Expand **User**. Enable **User.Read** permission



Enable User.Read permission

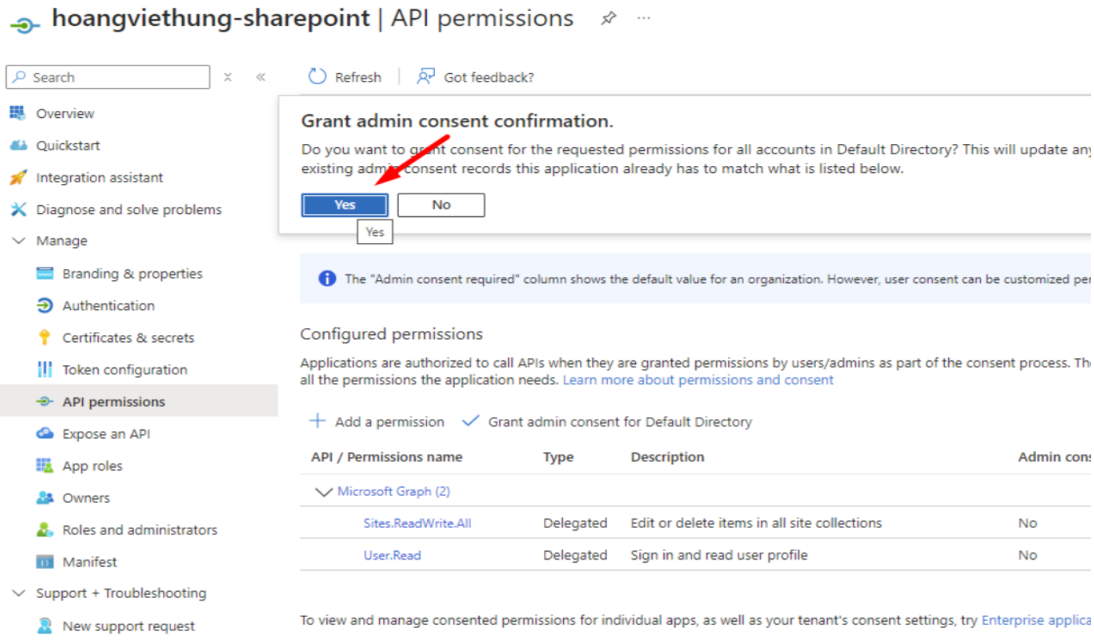
Step 6. Back to API permission page, click on **Grant admin consent for Default Directory**

> **Reminder**
> It is important to enable **Grant admin consent for Default Directory**



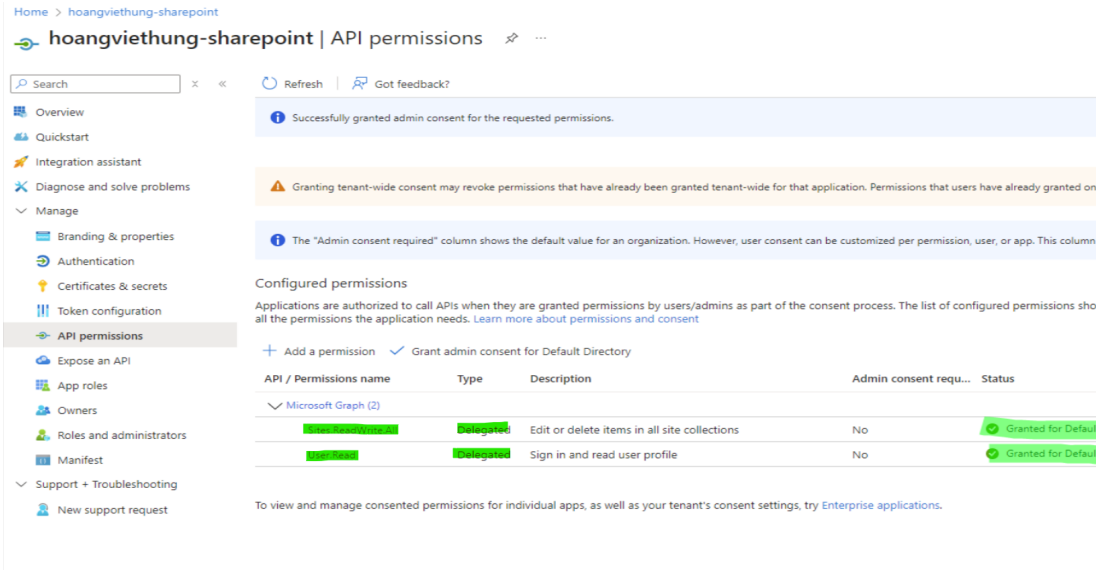
Grant admin consent for Default Directory

- When a popup appears, select **Yes** to enable the setting



Enable Grant admin consent for Default Directory

Step 7. After adding permissions and enable Grant admin consent for Default Directory. You should have a summary page similar as below



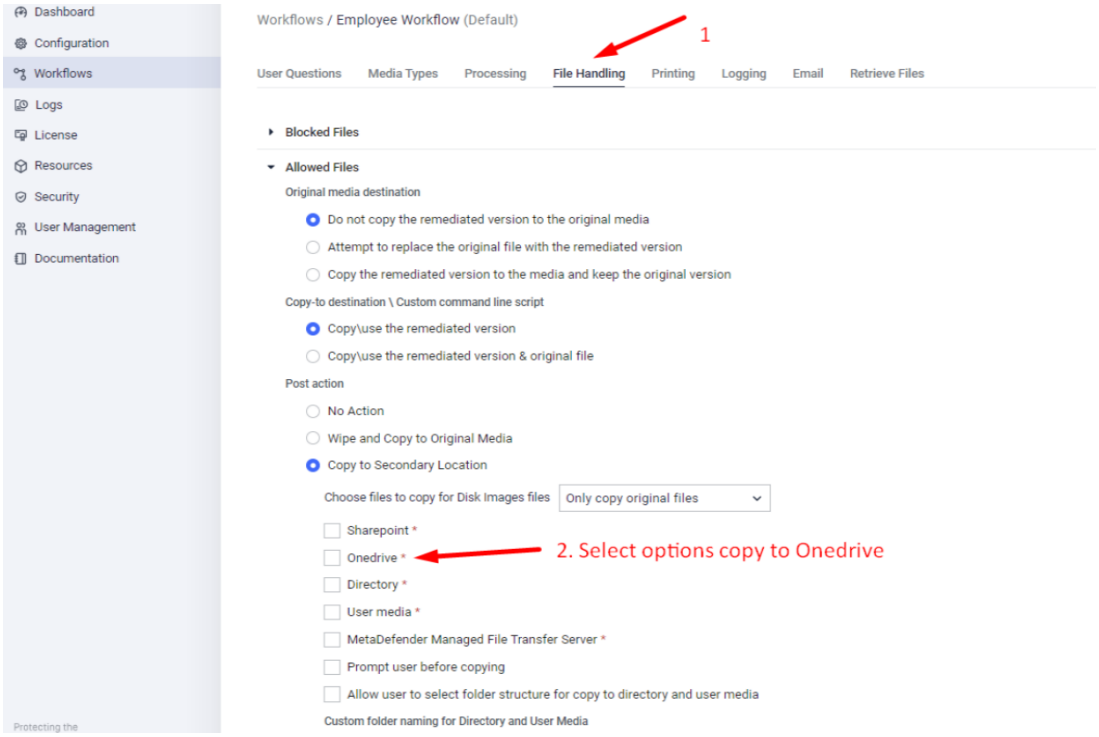
Summary of API permissions

5. Configure Kiosk WebMC to upload processed files to OneDrive

Step 1. From Kiosk WebMC, go to **Workflows**, select **Employee Workflow**, Select **File Handling**

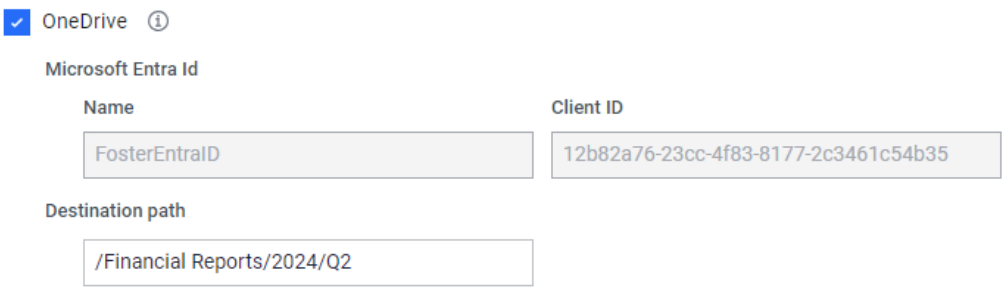
- Blocked Files: to copy blocked files to OneDrive
- Allowed Files: to copy allowed files to OneDrive

Assuming we want to copy allows files to OneDrive. Expand **Allowed Files**, Select **Copy to Secondary Location**, Select **OneDrive**



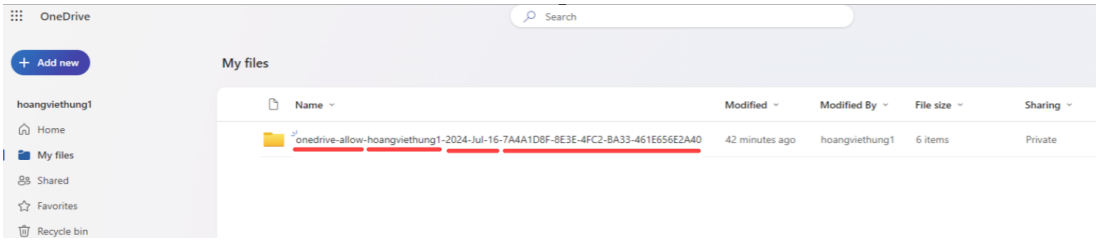
Enable copy allowed files to OneDrive

Step 2. Provide the information



- **Microsoft Entra ID:** Select the profile created above.
- **OneDrive folder name:** Provide the format of OneDrive folder name where you would like the files to be uploaded. Variables can be used for dynamic naming, for example, [username], [date], [time], etc.
- **Destination Path:** The relative path where the uploading folder will be stored.
  - */Financial Reports/2024/Q2* as example from the screenshot above
  - *Destination Path* supports %%%username%%% and %%%userresponse#%%% variables, please refer to *Directory Naming* for more information.
  - If you want to upload files into the user's personal folder. Please enter *Root*, or leave this field empty

Example of OneDrive folder name format

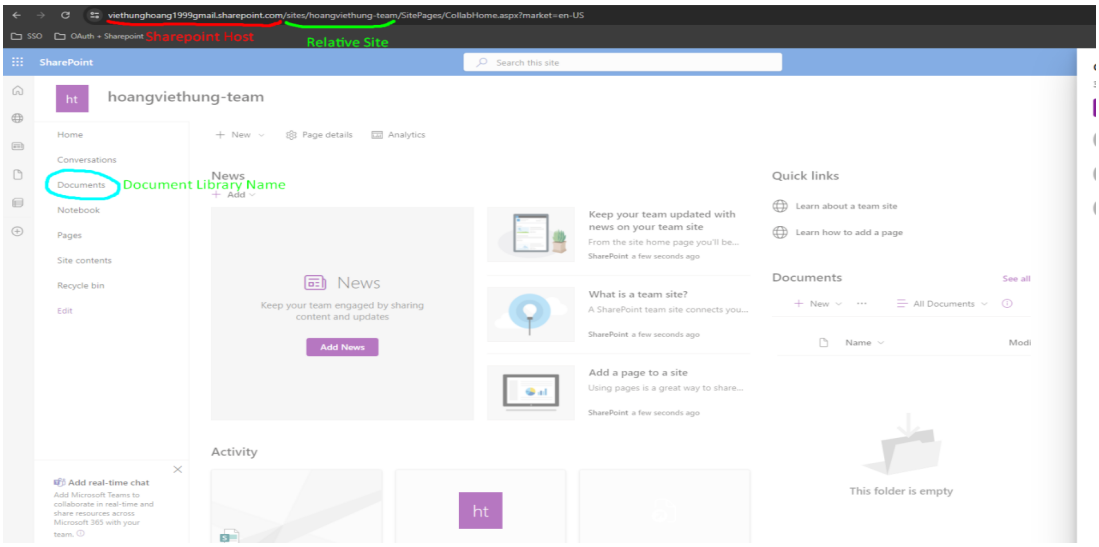


Example of OneDrive folder name format

6. Configure Kiosk WebMC to upload processed files to SharePoint

> **The site owner can access files**
> When uploading files to SharePoint as a member of the site, only the file owner can see their files. However, the site owner can also see the files.

Step 1. Acquire SharePoint Site information



Group membership of the site

Based on the information from the screenshot:

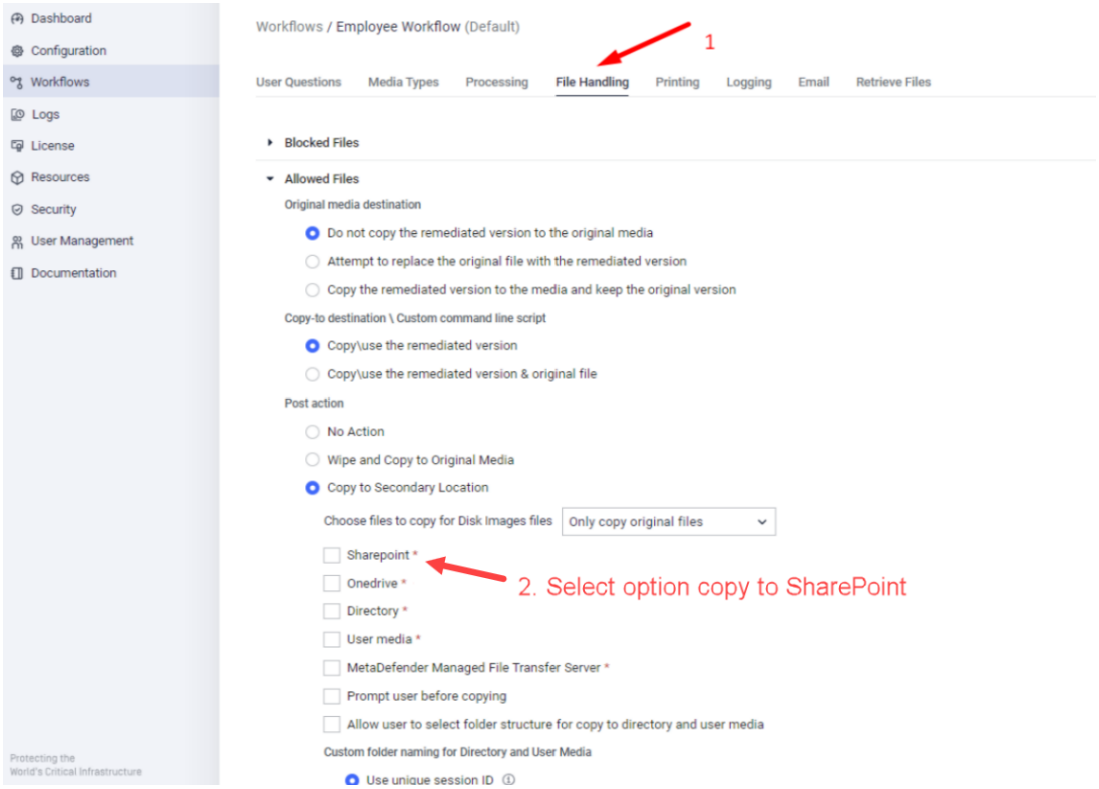
- SharePoint Host Domain: ***viethunghoang1999gmail.sharepoint.com*** as example from the screenshot
- Current Site Relative Path: ***/sites/hoangviethung-team*** as example from the screenshot
- Document Library Name: ***Documents*** as example from the screenshot

Step 2. Configure Kiosk WebMC to upload processed file to SharePoint

From Kiosk WebMC, go to **Workflows**, select **Employee Workflow**, Select **File Handling**

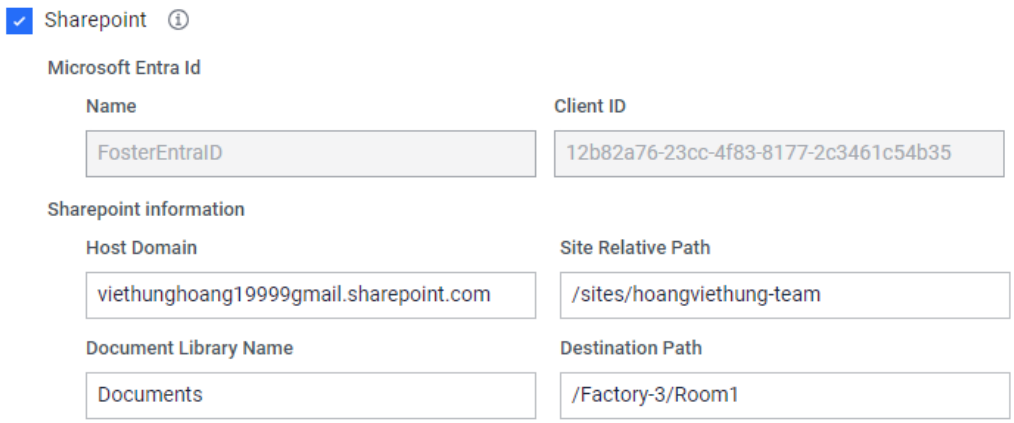
- Blocked Files: to copy blocked files to SharePoint
- Allowed Files: to copy allowed files to SharePoint

Assuming we want to copy allows files to SharePoint. Expand **Allowed Files**, Select **Copy to Secondary Location**, Select **OneDrive**



Enable copy allowed files to SharePoint

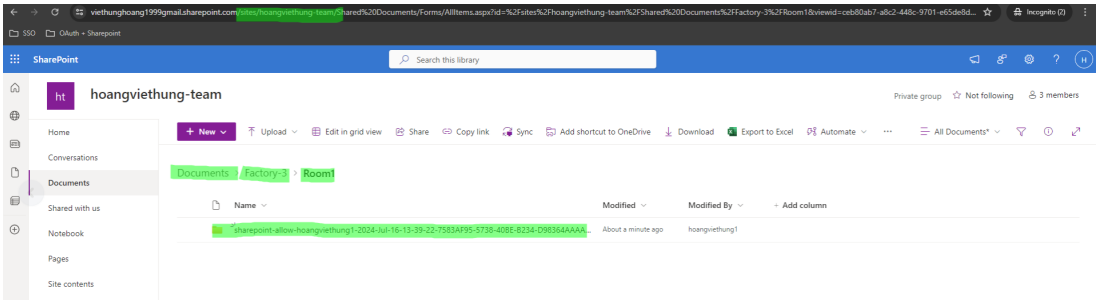
Step 2. Provide the information



- Microsoft Entra ID: select the created profile

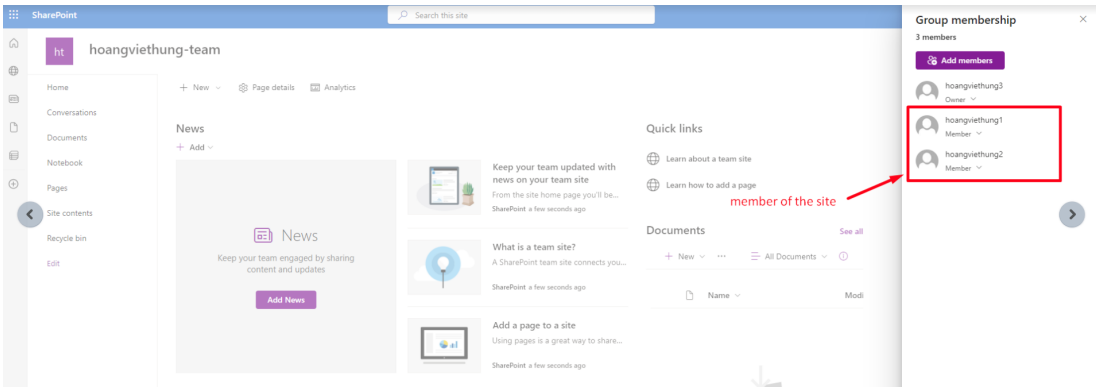
- Host Domain: Provide SharePoint Domain name
  - *viethunghoang1999gmail.sharepoint.com* as example from the screenshot above
- Site Relative Path: Relative path to the site
  - */sites/hoangviethung-team* as example from the screenshot above
- Document Library Name
  - *Documents* as example from the screenshot above
- Destination Path: The relative path from the root of the document library where the uploading folder will be stored
  - */Factory-3/Room1* as example from the screenshot above
  - *Destination Path* supports %%%username%%% and %%%userresponse#%%% variables, please refer to *Directory Naming* for more information.
  - If you want to upload files into the root of the document library. Please enter *Root*, or leave this field empty

Example of successful upload to SharePoint



Example of successful upload to SharePoint and its folder structure

Comparison of Site Owner vs Site Member access levels



Group membership as example from the screenshot

- *hoangviethung3* is site owner
- *hoangviethung1* is site member

- *hoangviethung2* is site member

When a file is uploaded to SharePoint by a site member (*hoangviethung1*), only the file owner (*hoangviethung1*) can view and access the file. Other site member (*hoangviethung2*) cannot see or access the files. However, the site owner (*hoangviethung3*) can view and access all files, including those uploaded by other site member (*hoangviethung1* for example)

Setup for Thales (formerly Gemalto) smart card for user authentication

The purpose of this guide is to demonstrate the process of setting up a smart card for authentication in MetaDefender Kiosk. In this example, we use a **Thales (formerly Gemalto) smart card**. Please note that this guide is for reference only, for the most accurate instructions, refer to the setup documentation provided by your smart card providers.

Smart card authentication requires proper setup and configurations on **Domain Controllers**, **Active Directory** and **Kiosk**.

- **Root Certificate Authority (CA) certificate** must be created
- **Domain Controllers** must be configured and trust the root CA certificate
- **Kiosk host machine** must join the domain

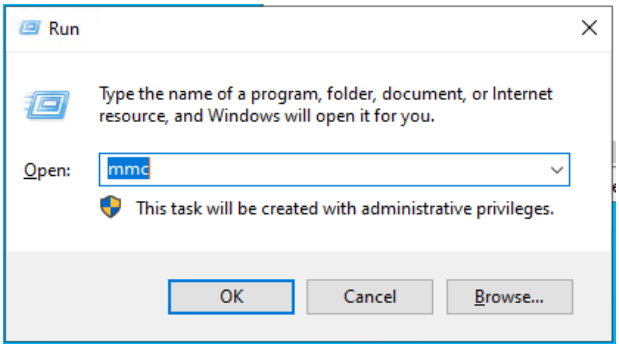
The instruction bellow assumes requirements mentioned above have been met. Configuring these requirements are out of the scope of this document.

> **Smart card compatibility**
> Kiosk 4.7.2 or later should support all ISO 7816-compliant microprocessor-based smart cards.
>
> If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

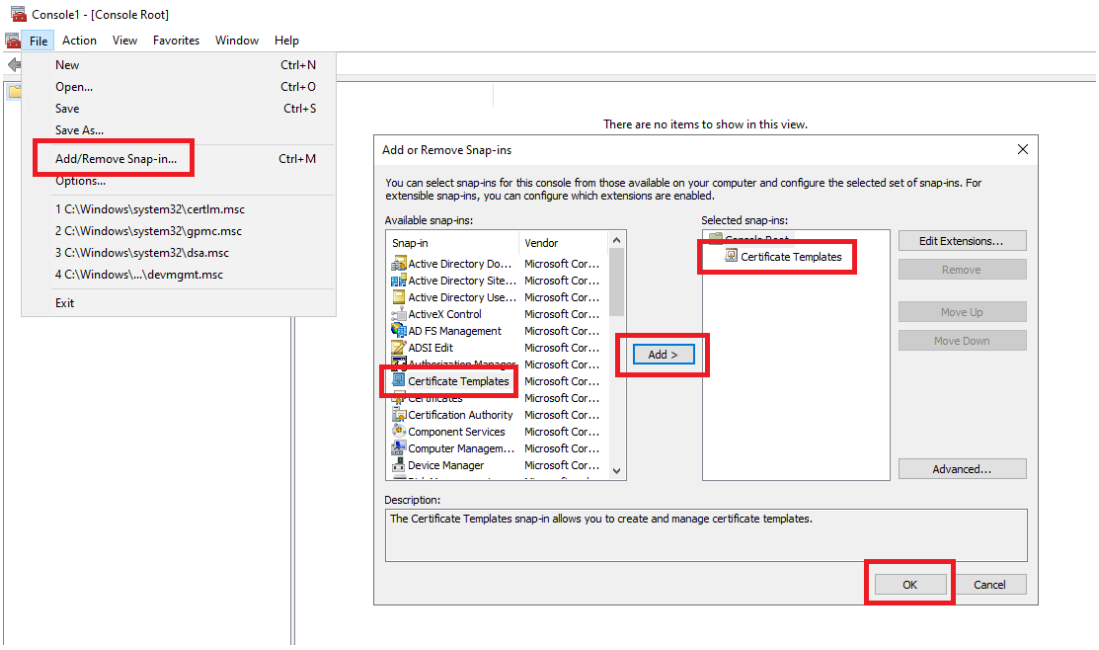
1. Certificate Template configuration

Step 1. Open **Certificate Template**

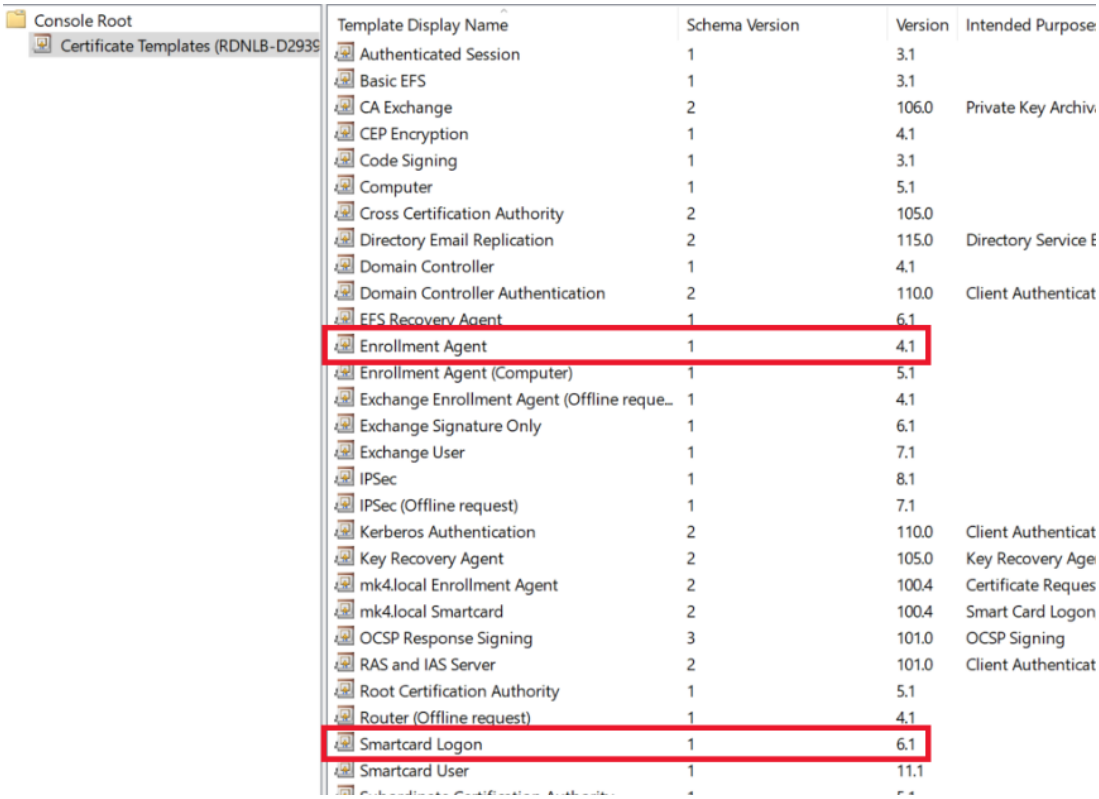
- Press **Win + R**, type **mmc**, and open it with Administrator permissions



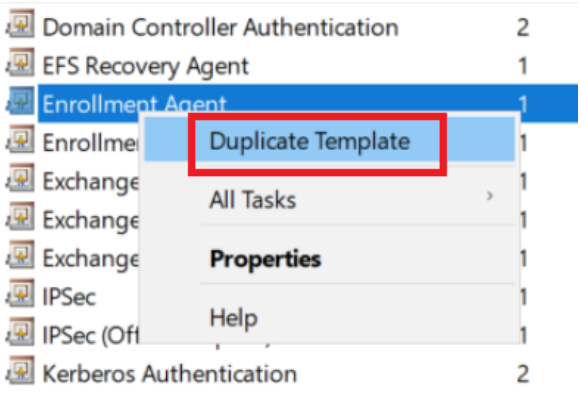
- In the MMC window, select **File**, select **Add/Remove Snap-in**. From the list, select **Certificate Template** and click **Add**. Then, click **OK**.



Step 2. Duplicate two highlighted certificate templates (**Enrollment Agent** and **Smartcard Logon**) to create your own Smartcard certificate Template.

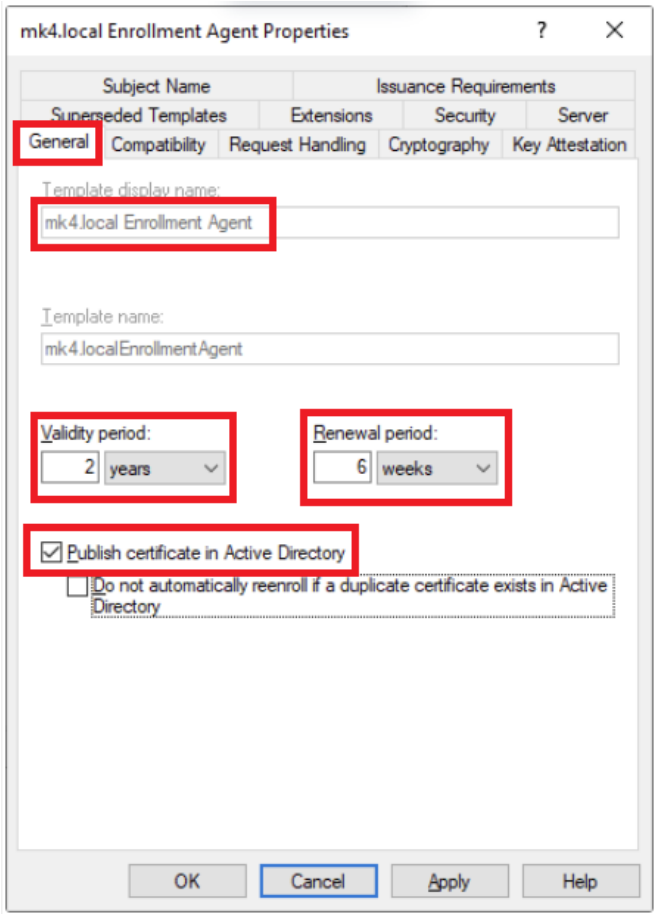


- Right-click on each of these templates. Select **Duplicate Template**.

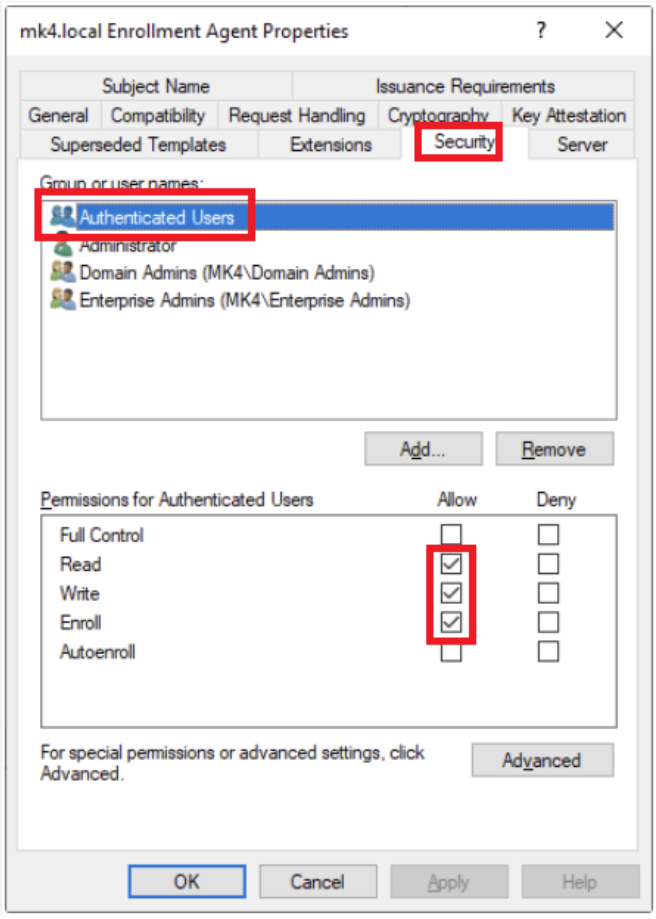


Step 3. Setup for **Enrollment Agent** template

- Go to **General** tab:
  - Change **Template display name** to <domain-name> Enrollment Agent. e.g mk4.local Enrollment Agent
  - Set **Validity period** to 2 years
  - Set **Renewal period** to 6 weeks
  - Enable **Publish certificate in Active Directory**



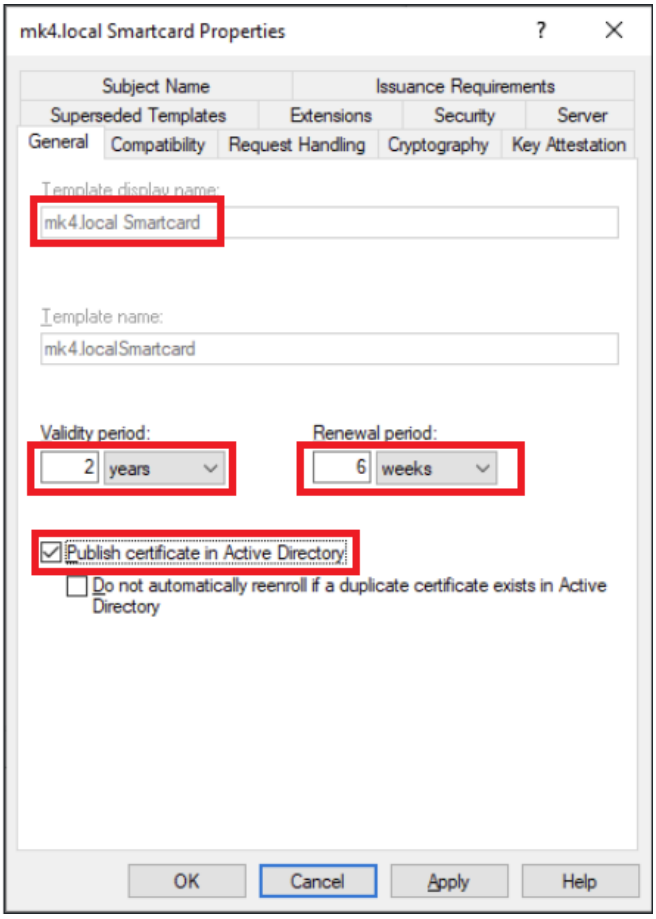
- Go to **Security** tab
    - Add **Read**, **Write** and **Enroll** permissions to **Authenticated Users**



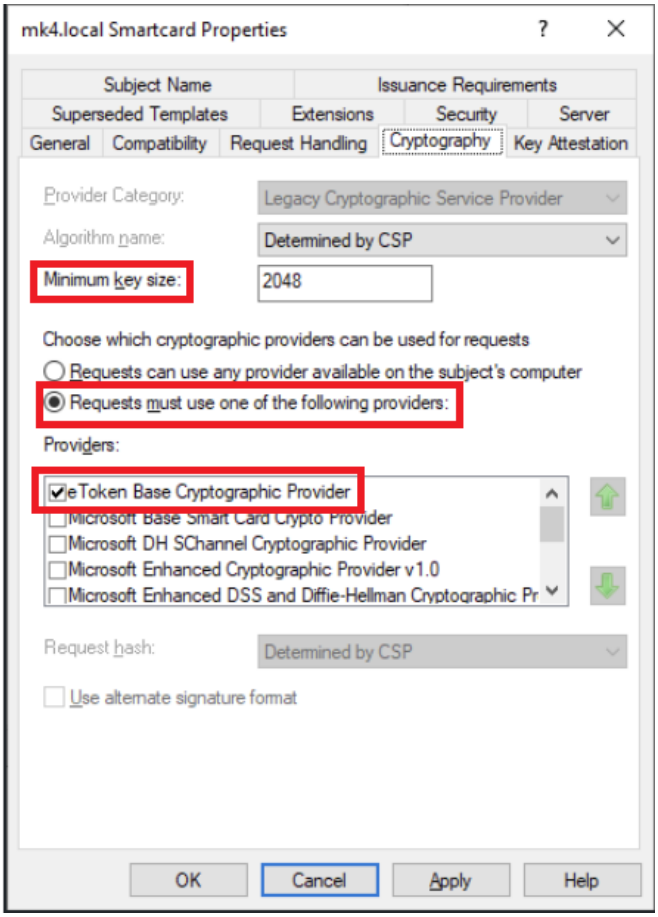
- Click **OK** to duplicate the template

Step 4. Setup for Smartcard Logon template

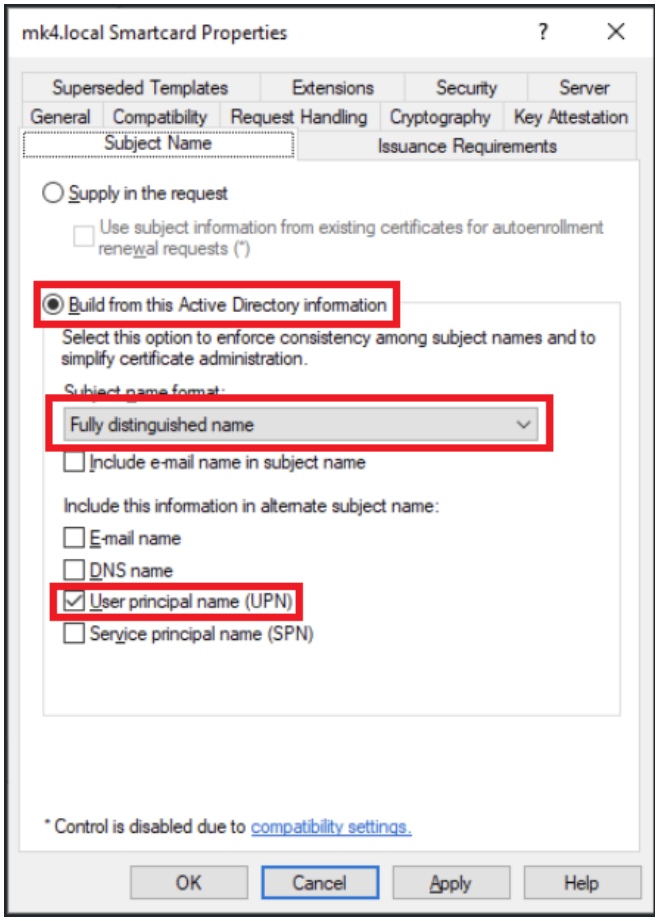
- Duplicate Smartcard Logon template
- Go to **General** tab
    - Change **Template display name** to <domain-name> Smartcard. e.g mk4.local Smartcard
    - Set **Validity period** to 2 years
    - Set **Renewal period** to 6 weeks
    - Enable **Publish certificate in Active Directory**



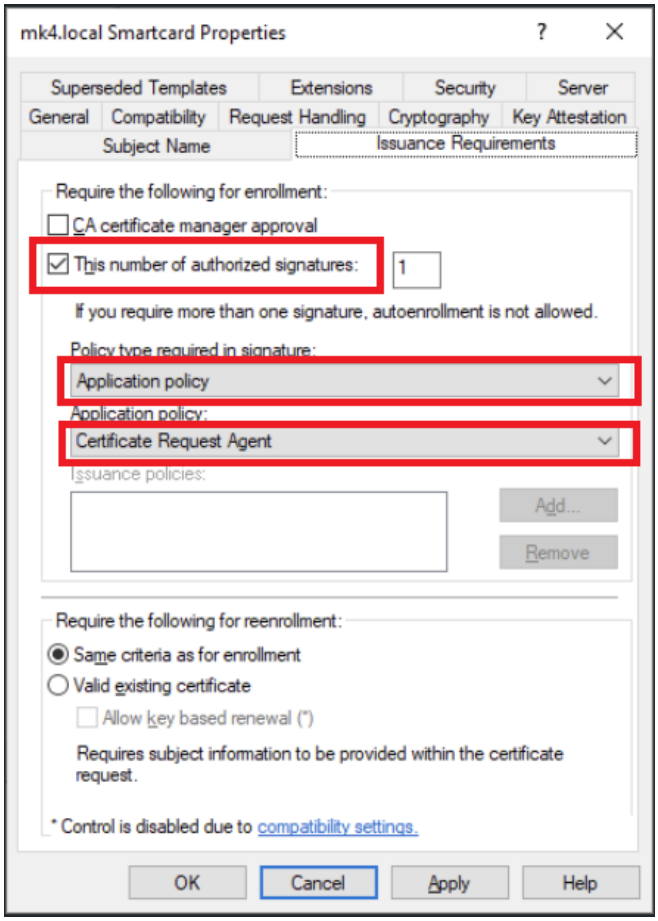
- Go to **Cryptography** tab
  - Set **Minimum key size** to 2048
  - Select **Requests must use one of the following providers**, and enable **eToken Base Cryptographic Provider**



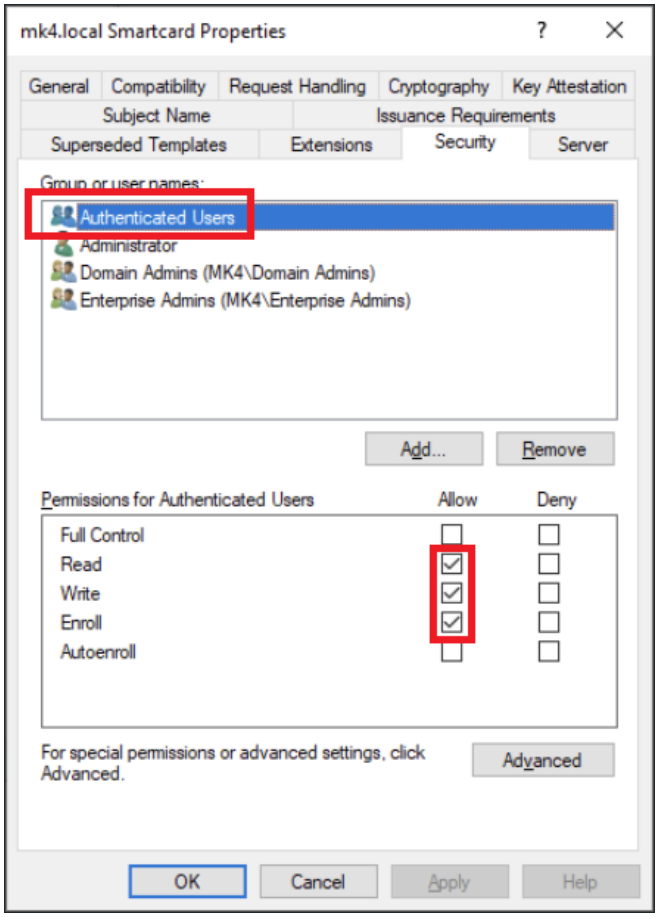
- Go to **Subject Name** tab
  - Select **Build from this Active Directory information**. Under **Subject name format**, select **Fully distinguished name** and enable **User principal name (UPN)**



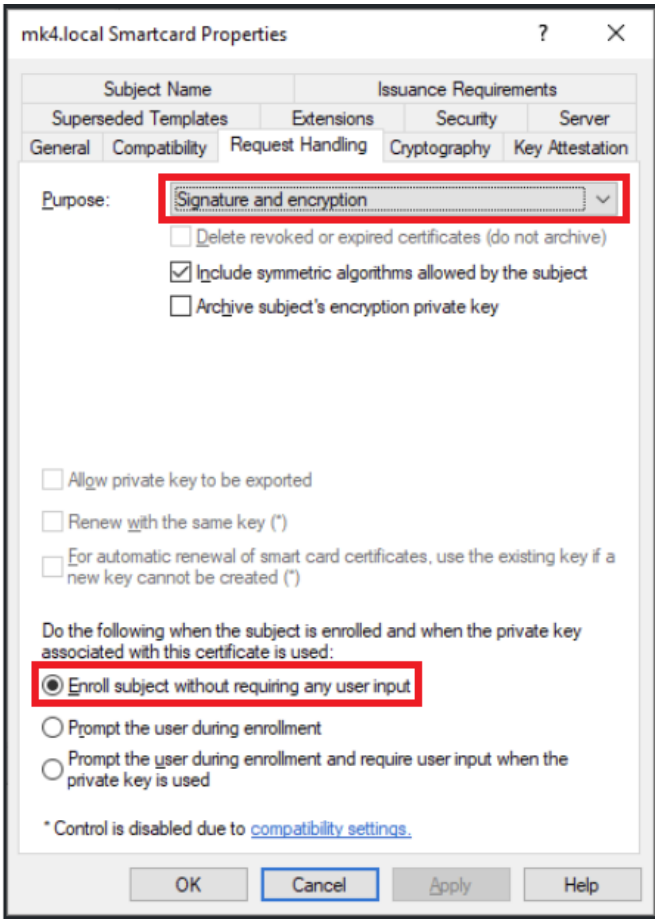
- Go to **Issuance Requirements** tab
  - Enable **This number of authorized signatures**, and set value of 1
  - Under **Policy type required in signature**, select **Application policy**
  - Under **Application policy**, select **Certificate Request Agent**



- Go to **Security** tab
    - Add **Read**, **Write** and **Enroll** permissions to **Authenticated Users**



- Go to **Request Handling** tab
  - Under **purpose**, select **Signature and encryption**, and enable **Include symmetric algorithms allowed by the subject**
  - Select **Enroll subject without requiring any user input**



- Click **OK** to duplicate the template

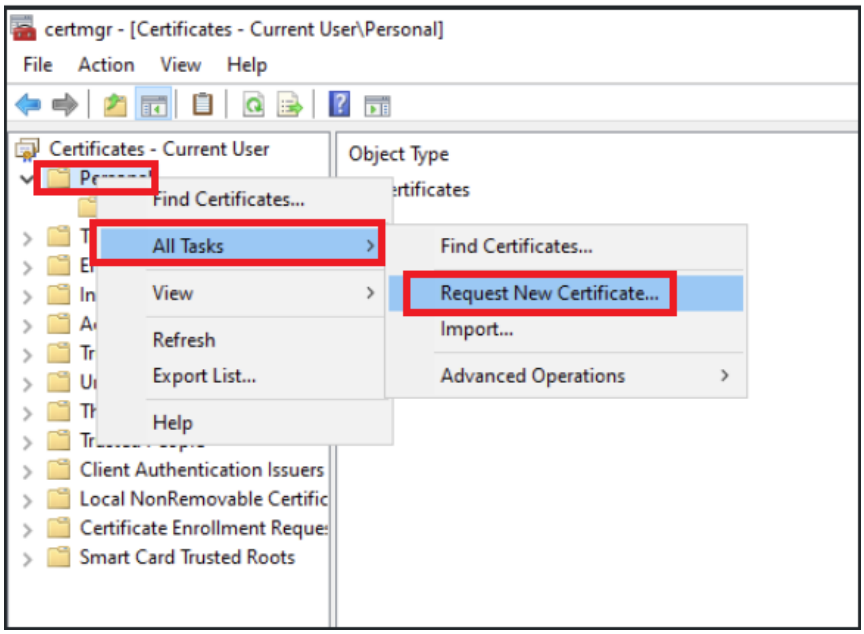
2. Enrollment Agent certificate

Step 1. Open **Certificate Manager**

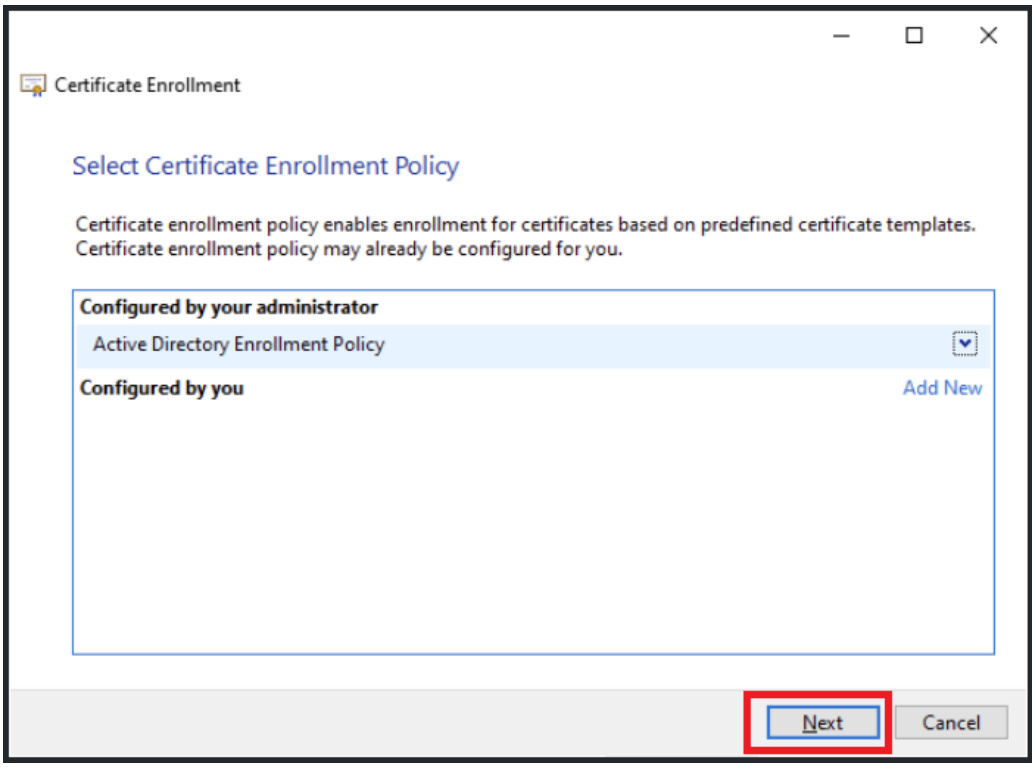
- Press **Win + R**, type **certmgr.msc**, and open it with Administrator permissions

Step 2. Request new certificate

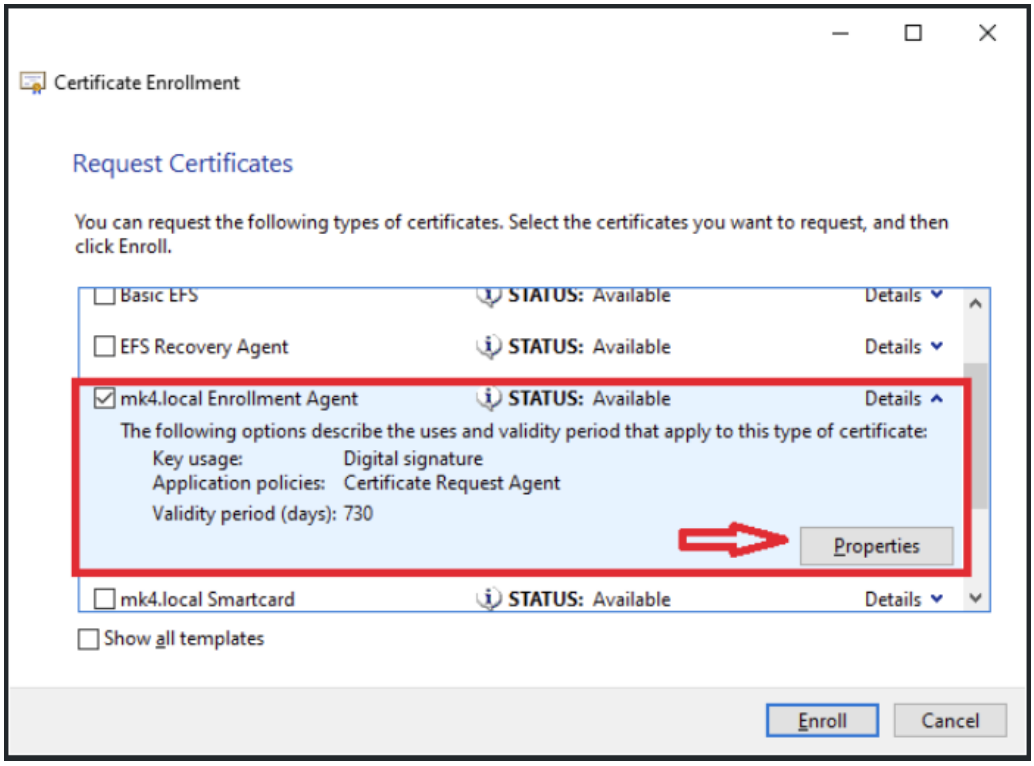
- Under Certificate Manager, right-click on **Personal**, select **All Tasks**, select **Request New Certificate**



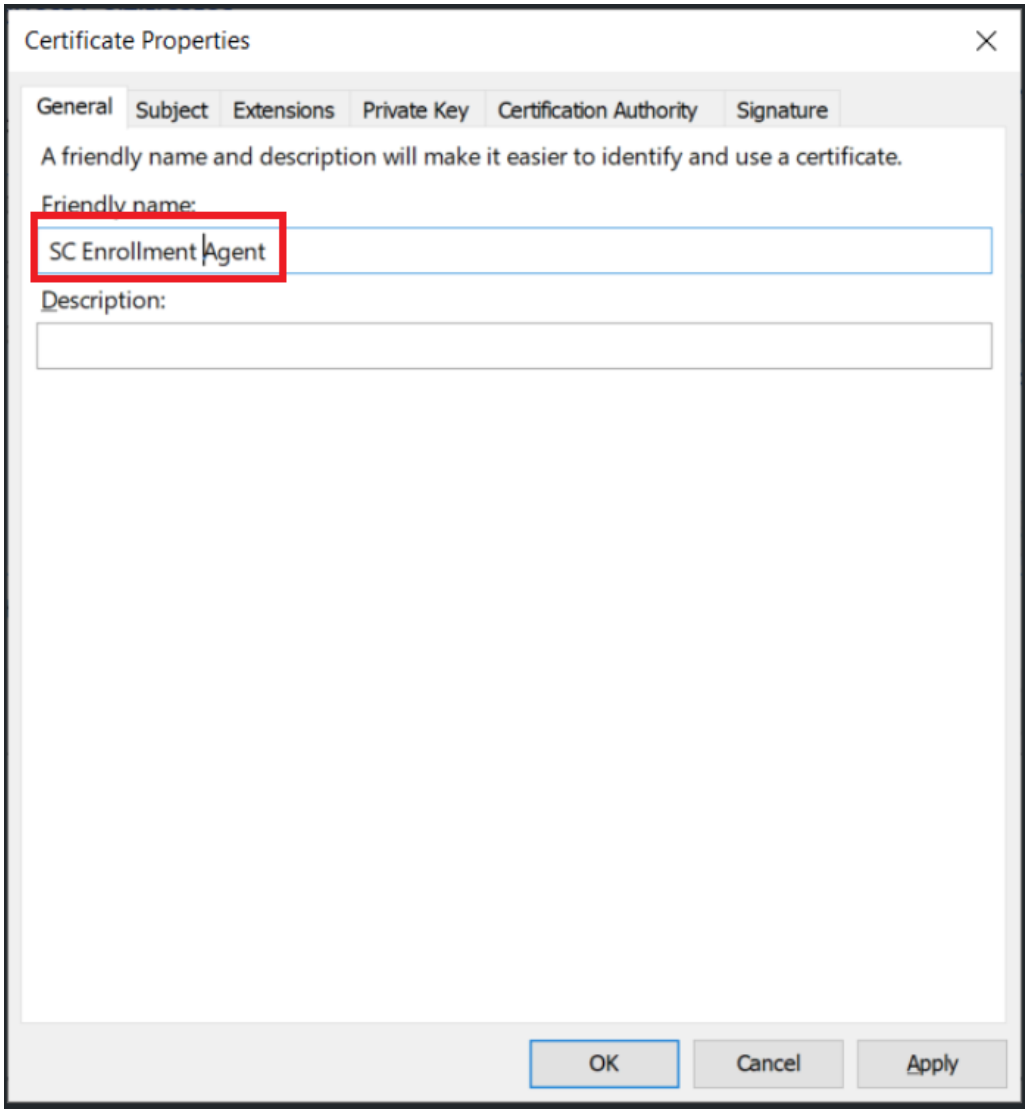
- in Certificate Enrollment Policy, select **Next** to continue



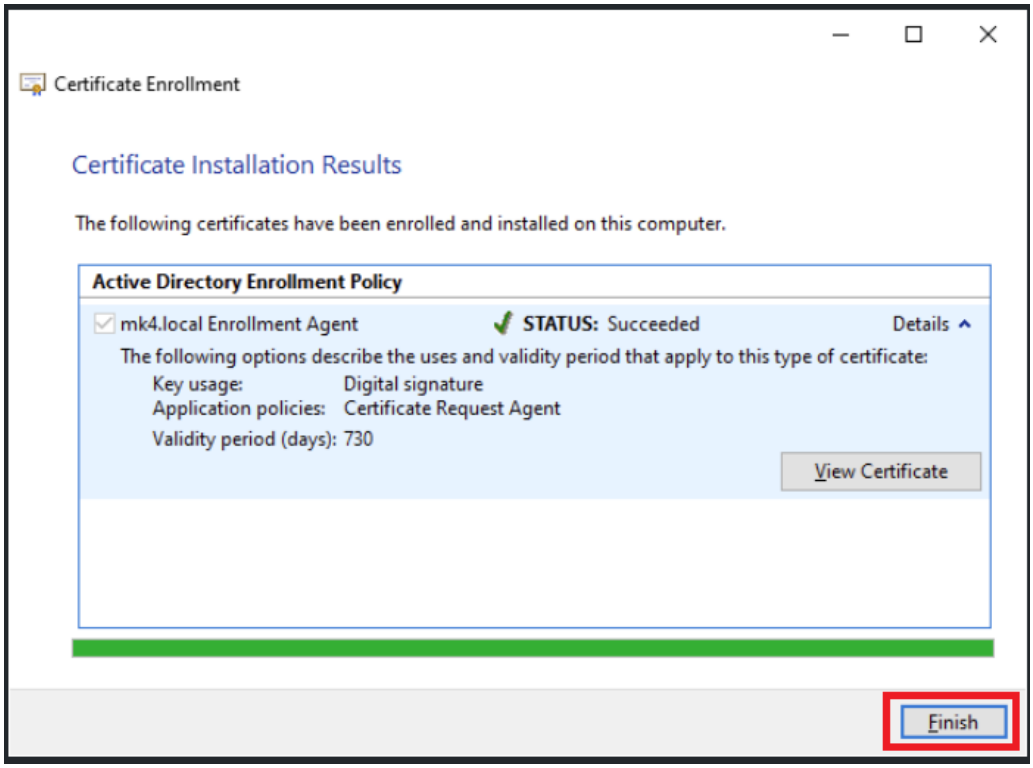
- Select **<domain-name> Enrollment Agent** created in previous steps, click on **Properties**



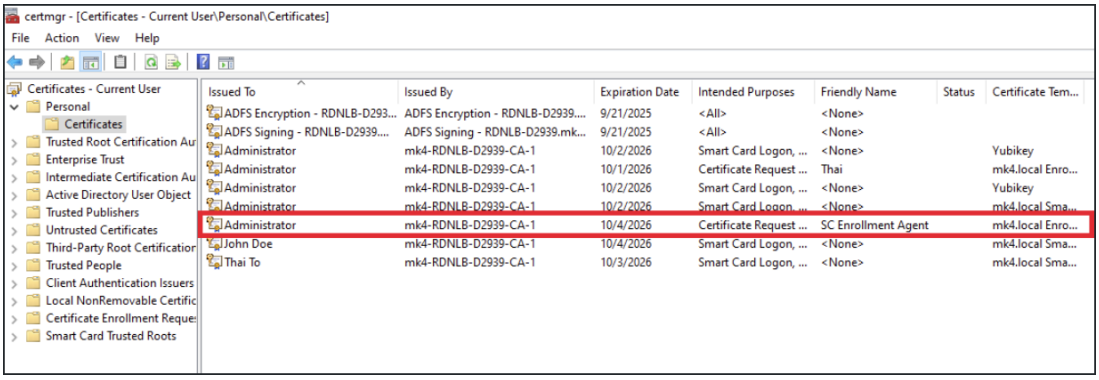
- Provide a **friendly name** for this certificate, click Apply, then click **OK**



- Click **Finish** to end the process

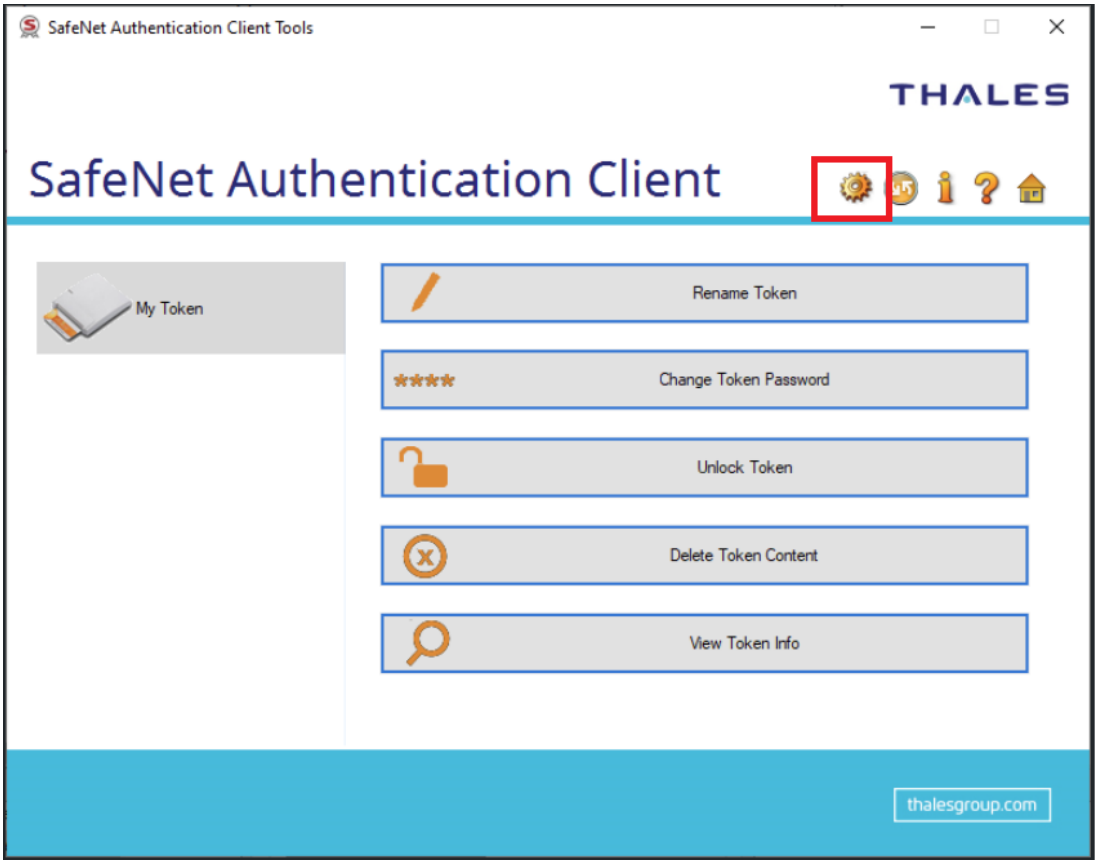


- A new Enrollment Agent certificate is now created and shown under Certificate section.

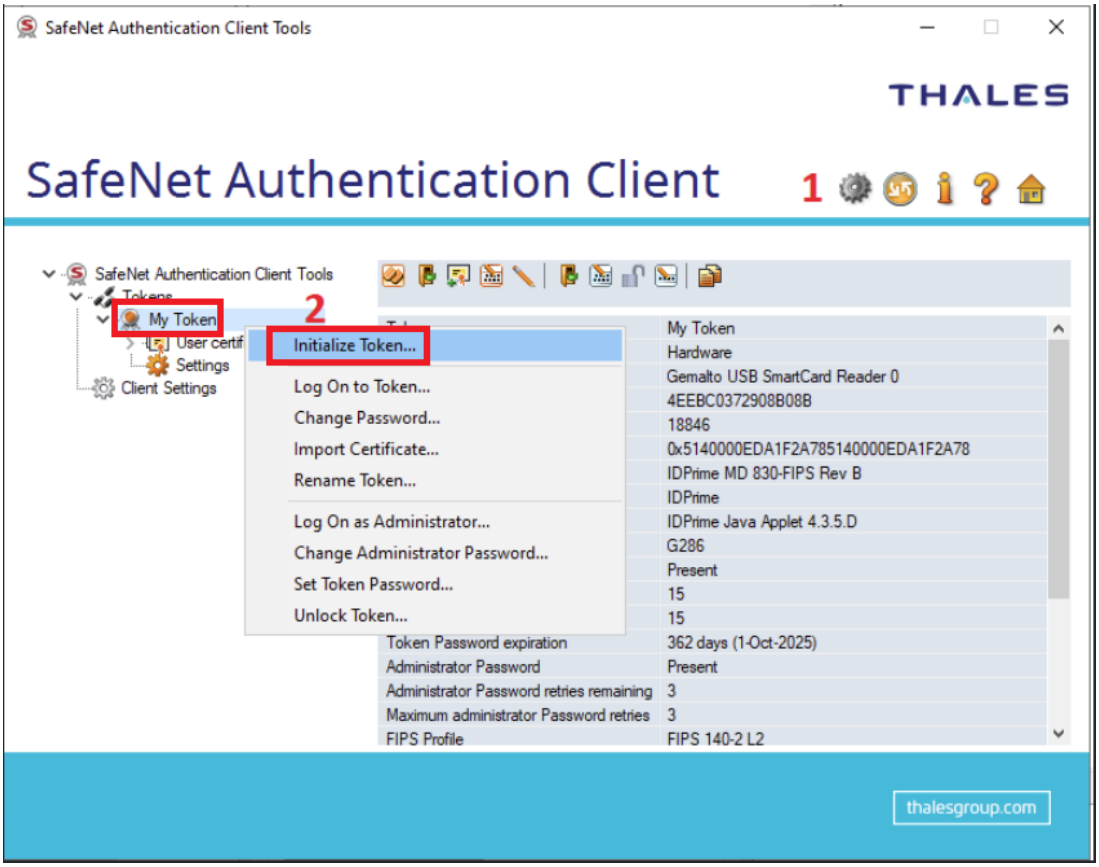


3. Smart card Initialization

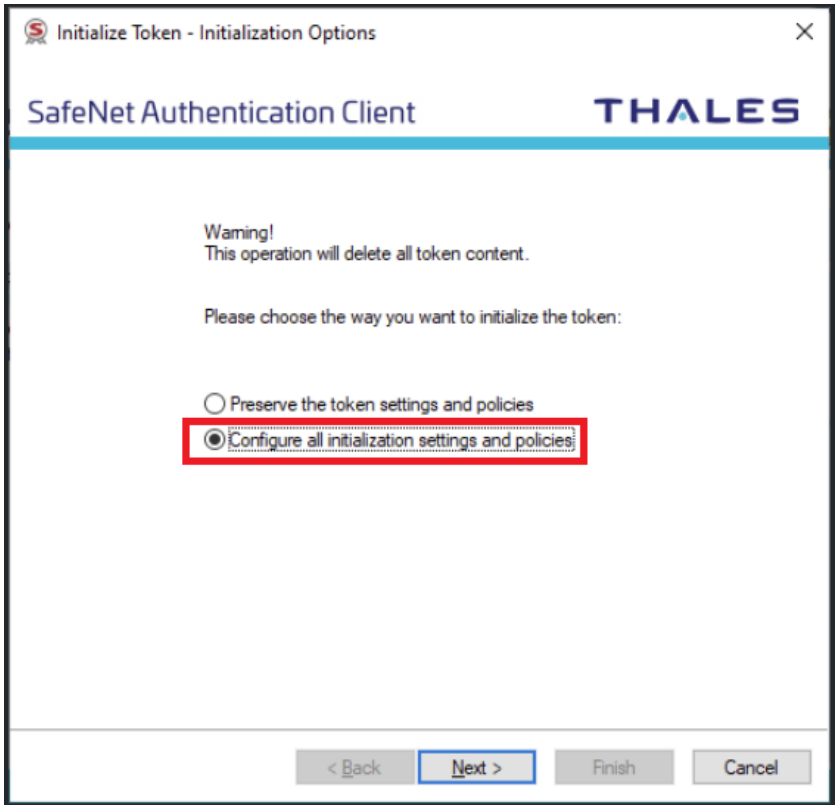
- Open **Safenet Authentication Client**, and inset the smart card. Click on the gear icon to open **Advanced View**.



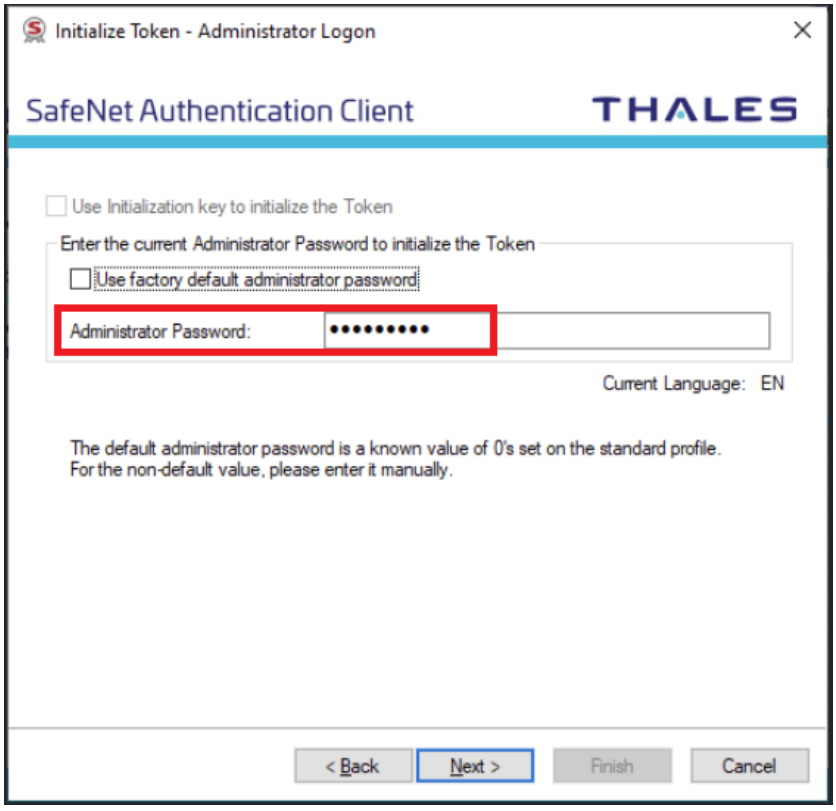
- Right-click on **My Token**, select **Initialize Token**



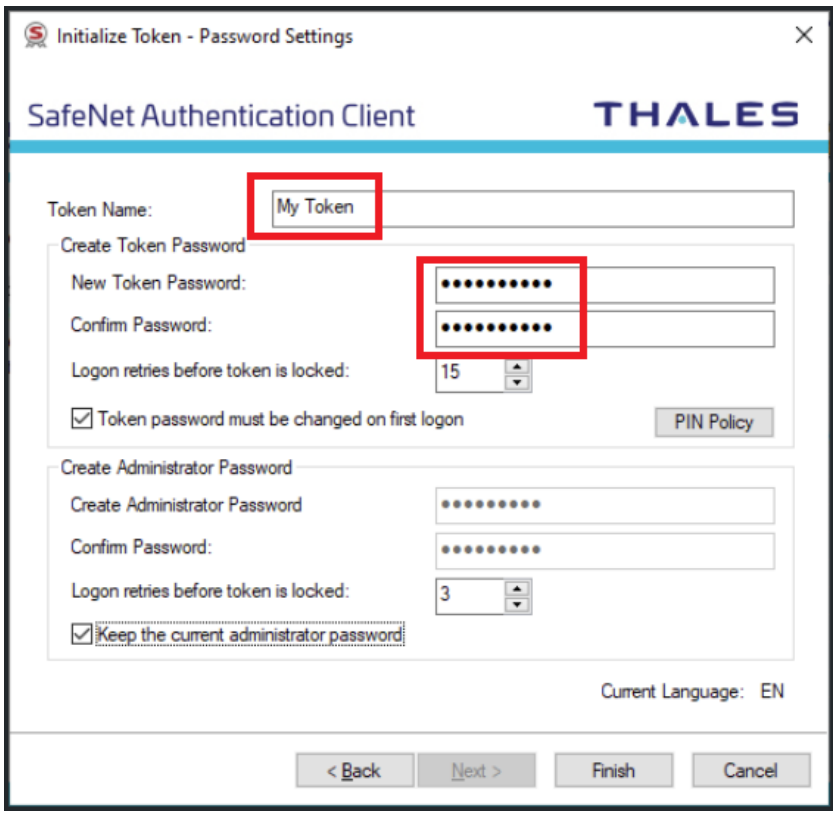
- Select **Configure all initialization settings and policies**



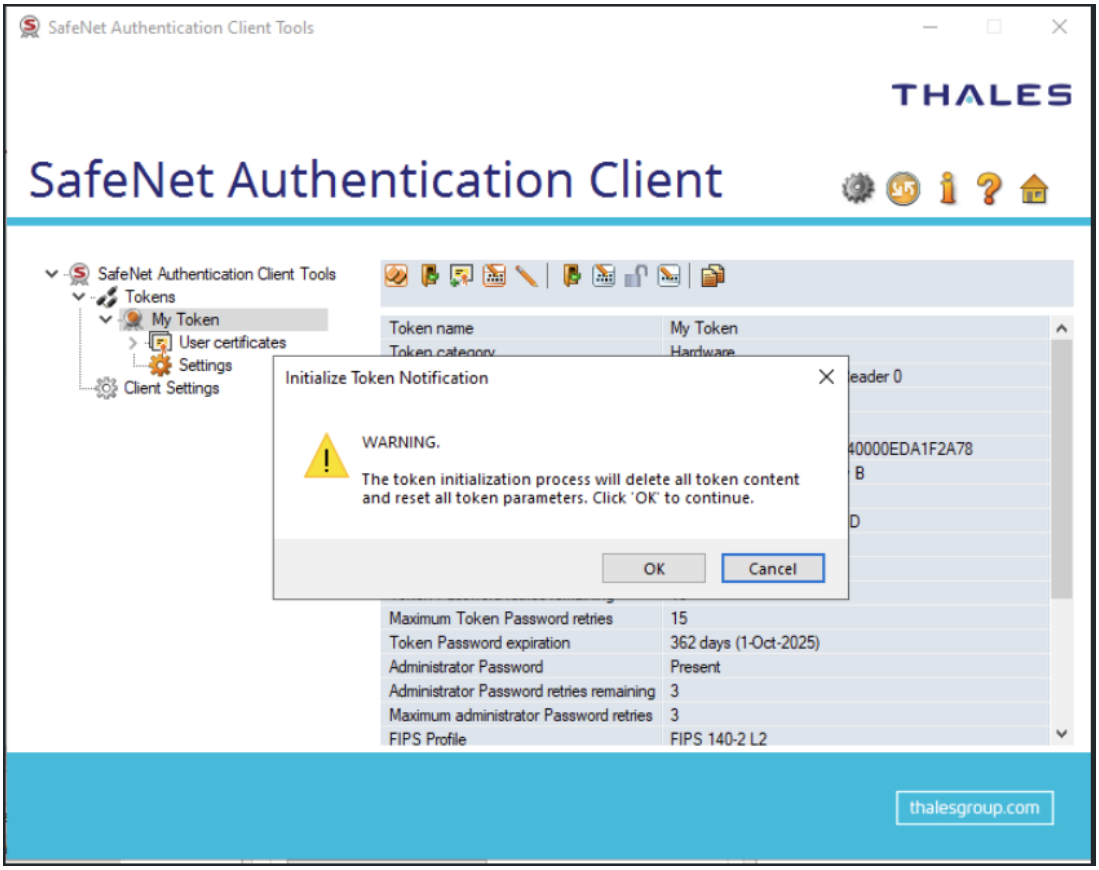
- Provide **Administrator Password** to initialize the Token, click Next



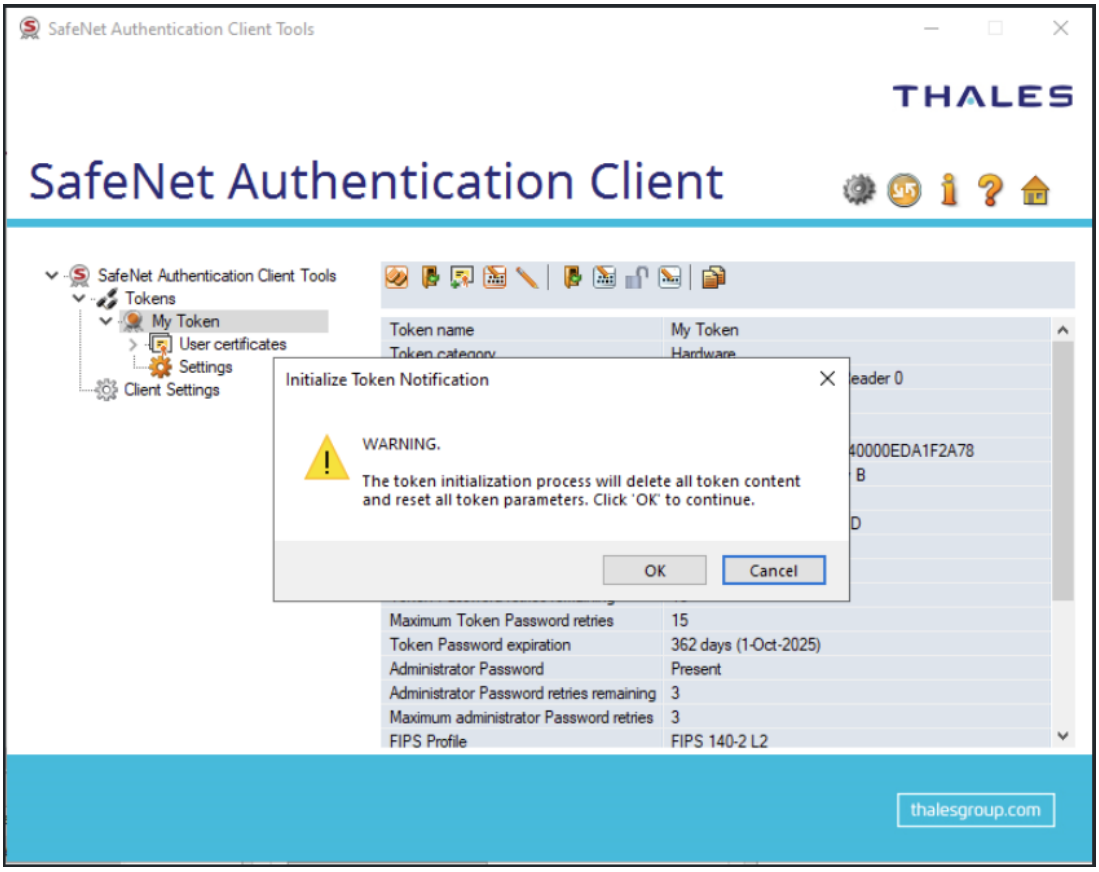
- Provide **Token Name** and **Token Password**. Other settings are optional. Enable **Keep the current administrator password** if don't want to create a new one



- A warning of data clearance will appear. Click **OK**.



- The smart card is successfully initialized.



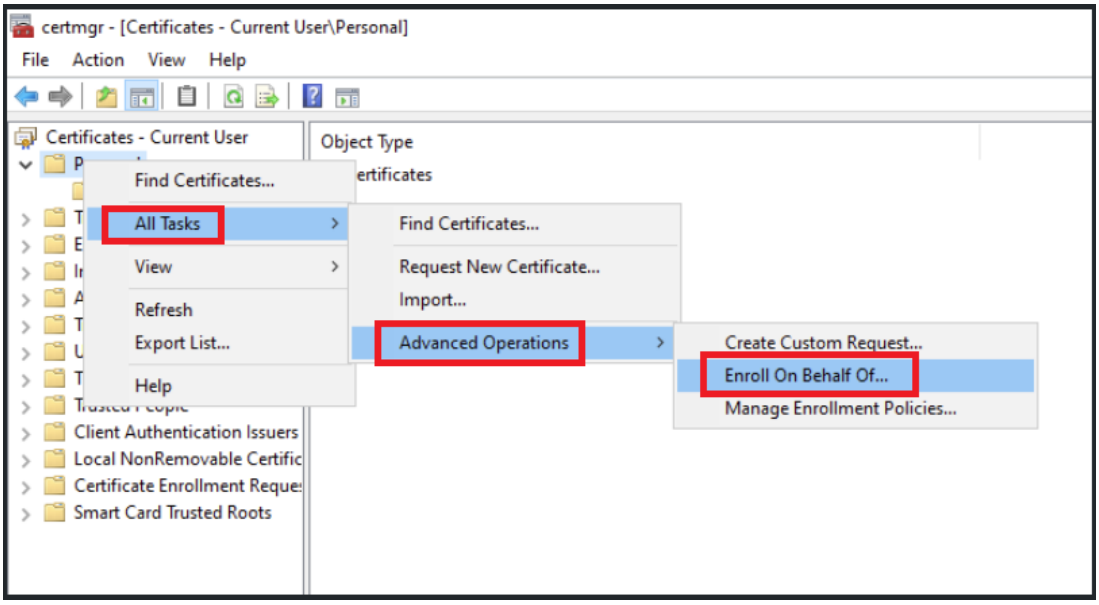
4. User Enrollment

Step 1. Open Certificate Manager

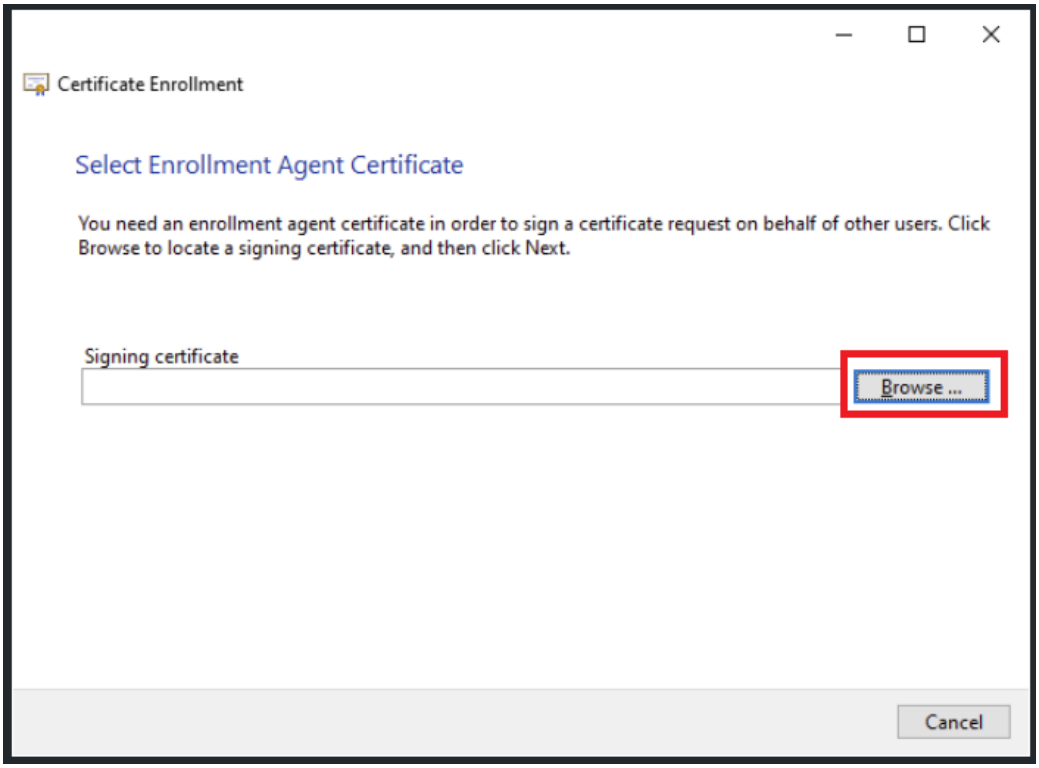
- Press **Win + R**, type **certmgr.msc**, and open it with Administrator permissions

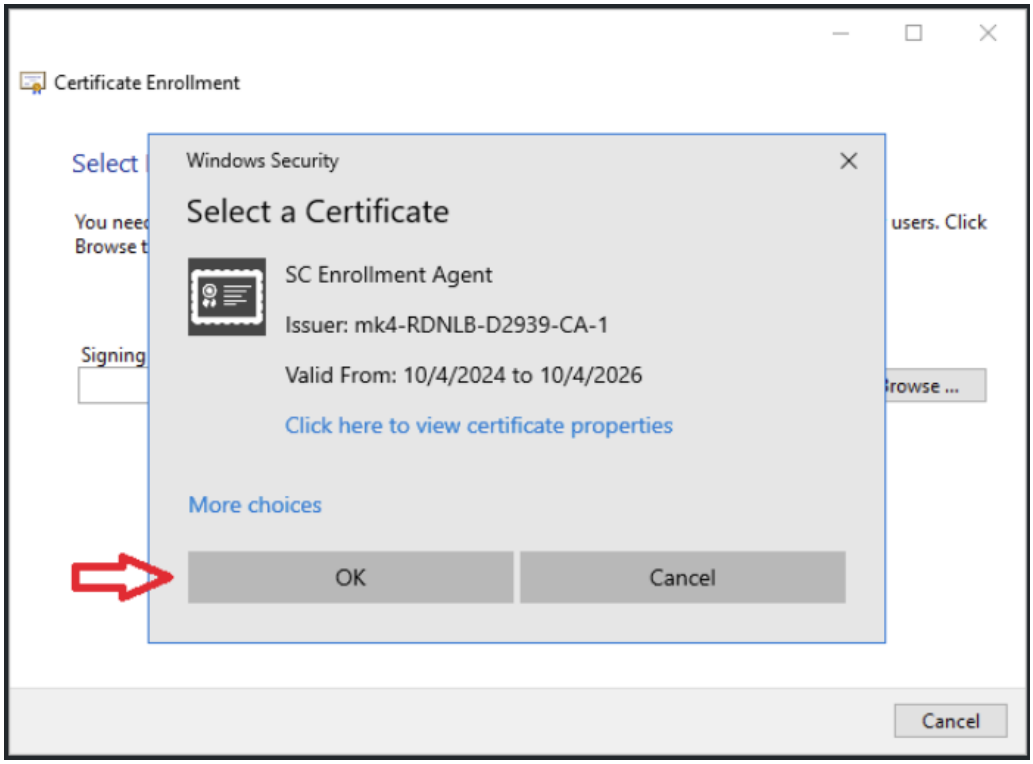
Step 2. Enroll Users

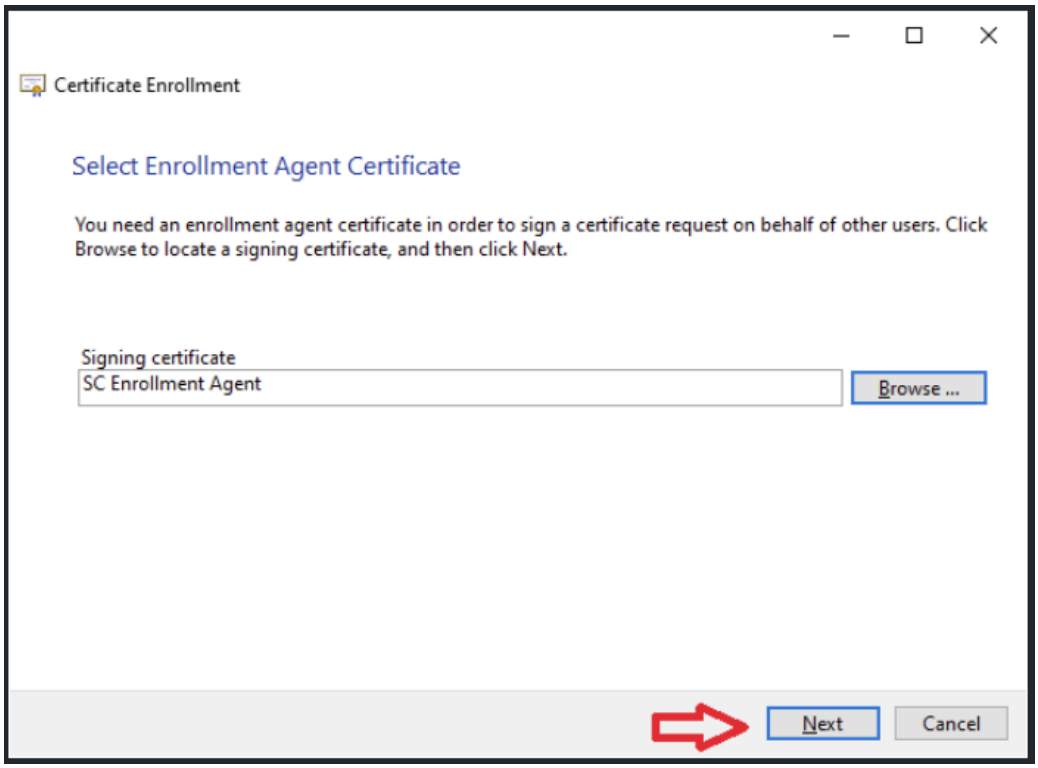
- In Certificate Manager, Right-click on **Personal**, Select **All Tasks**, Select **Advanced Operations**, Select **Enroll on Behalf of...**



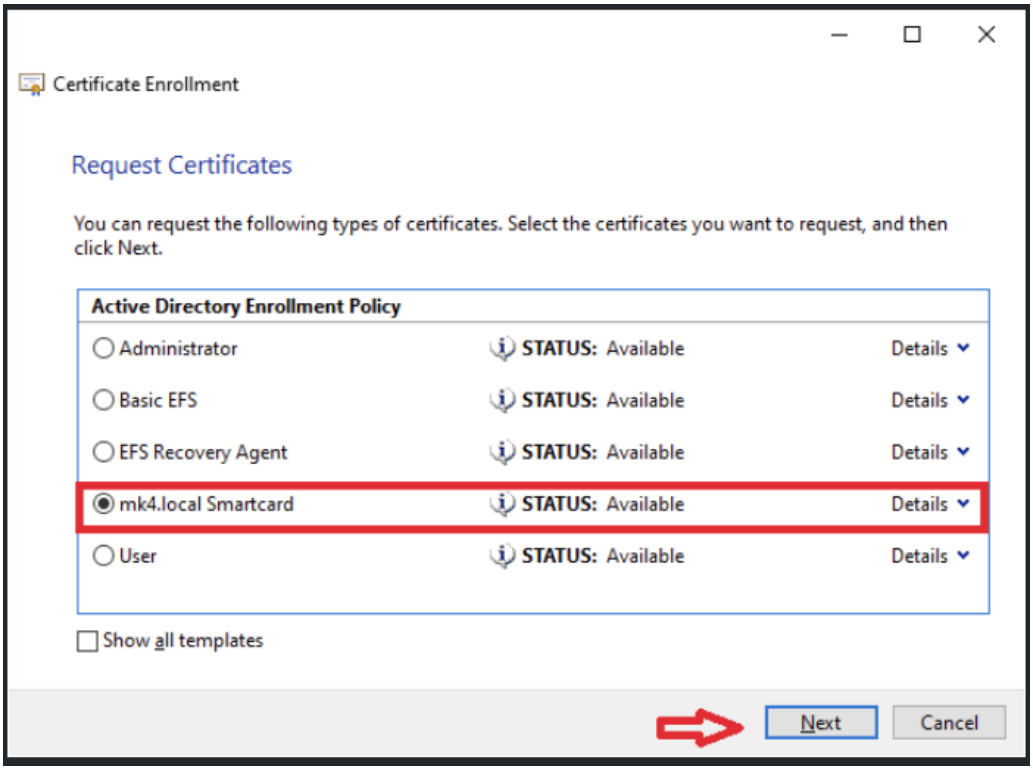
- Keep default settings and click **Next** until **Select Enrollment Agent Certificate**. Click **Browse**. Select a certificate for Enrollment Agent



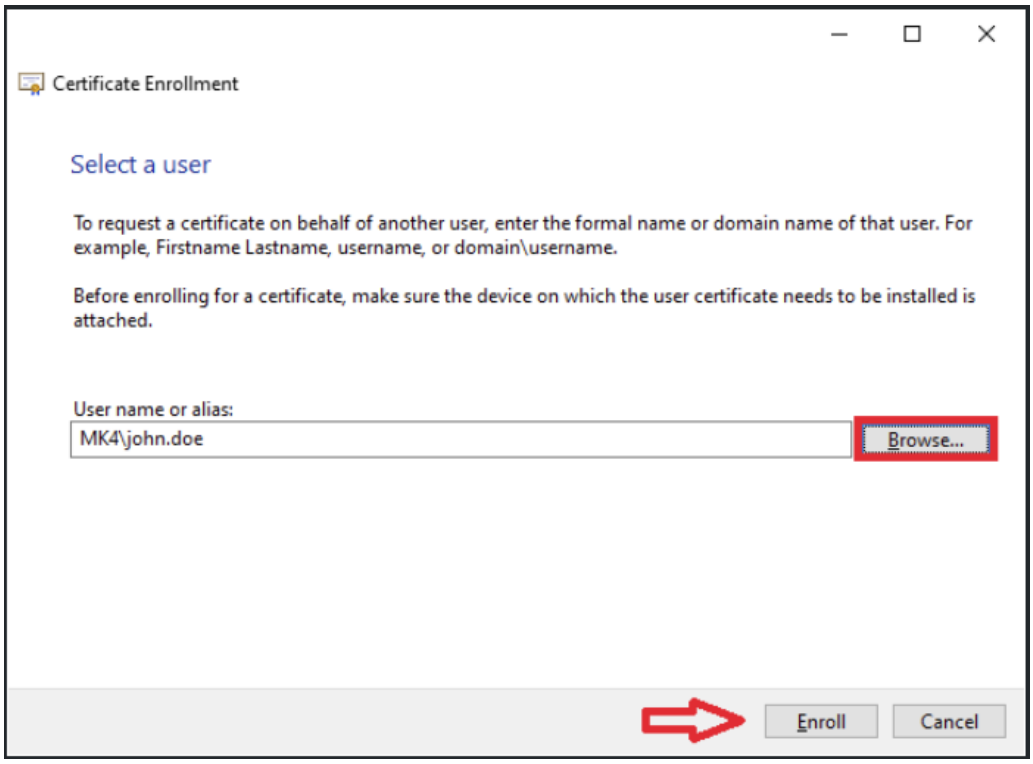




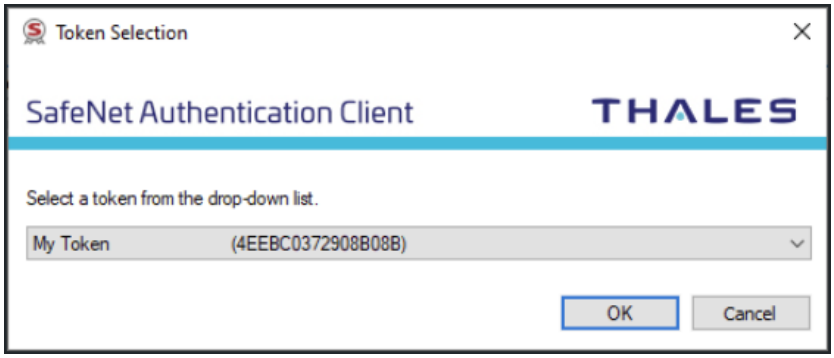
- Select **<domain-name> Smartcard template** created from previous steps. Click **Next**



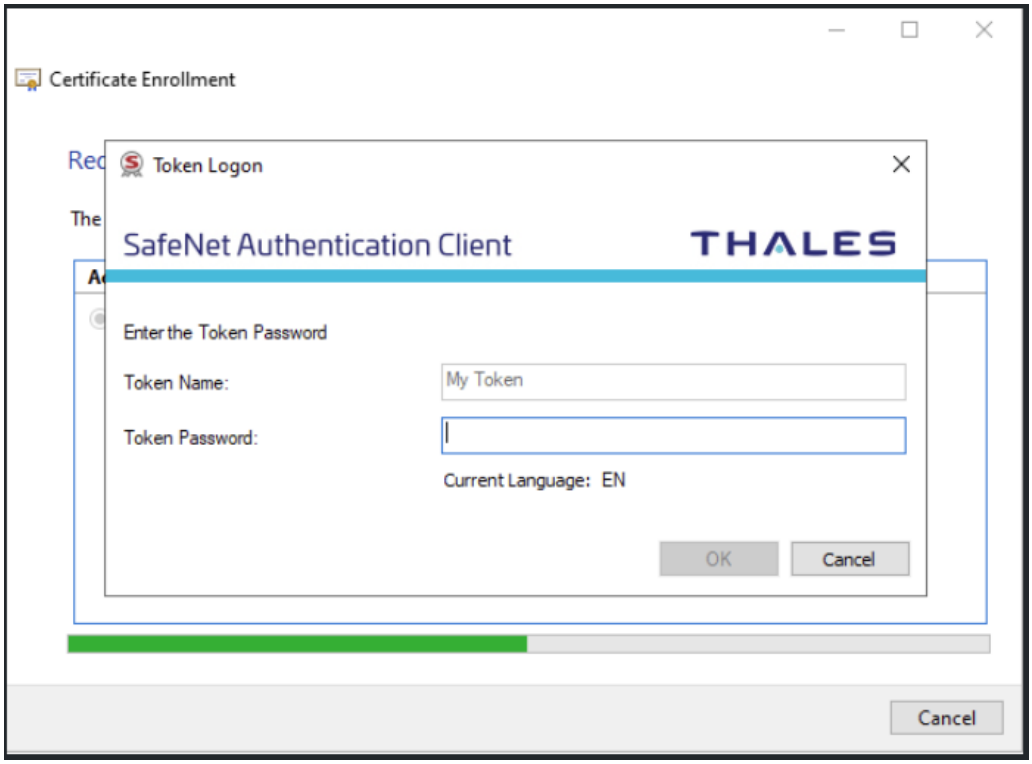
- Click **Browse** and select the user to enroll it to smart card. Click **Enroll** to finish the process



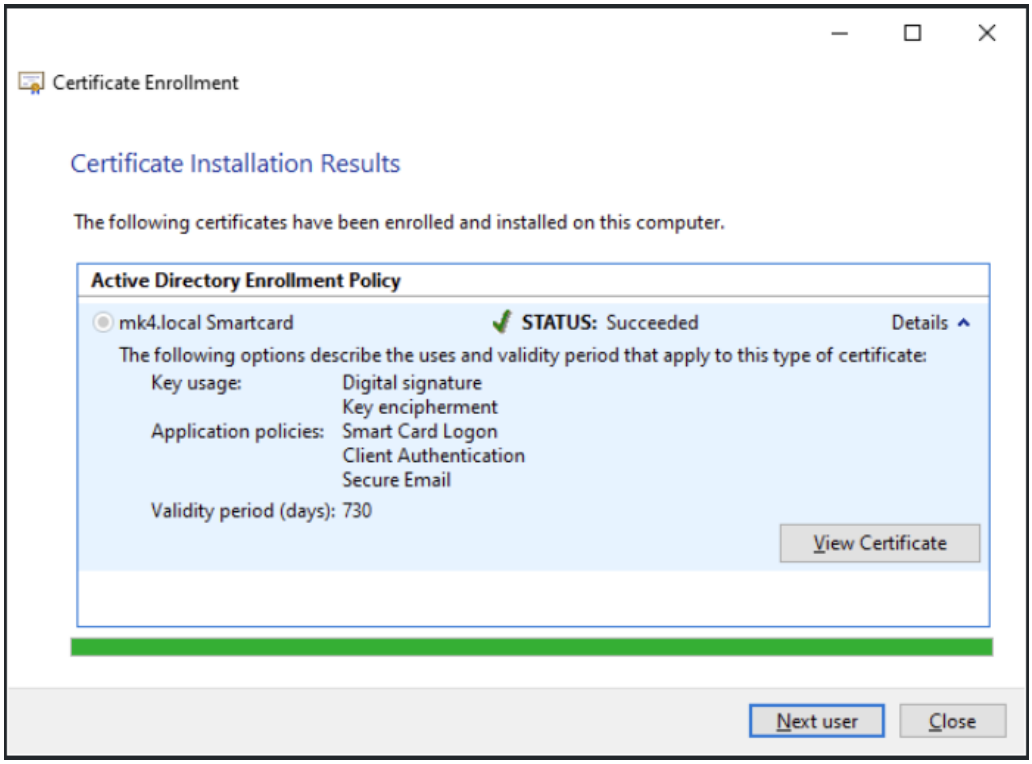
- Insert the smart card to the reader and select its token in Token Selection



- Enter the **Token Password** and click **OK**

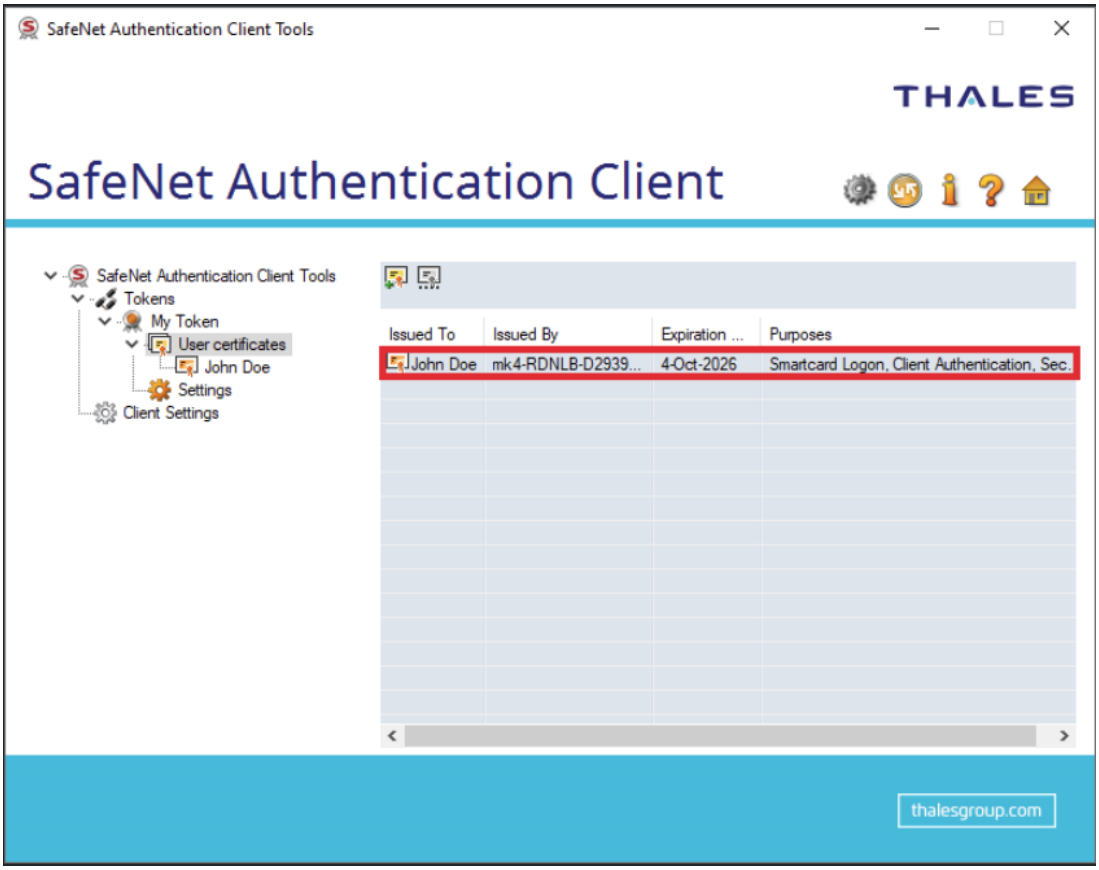


- Wait for the enrollment to finish and click **Close** to exit, or click **Next user** to enroll another user



Info
When multiple users were enrolled to the smart card, Kiosk will only grant access to the most recent enrolled user.

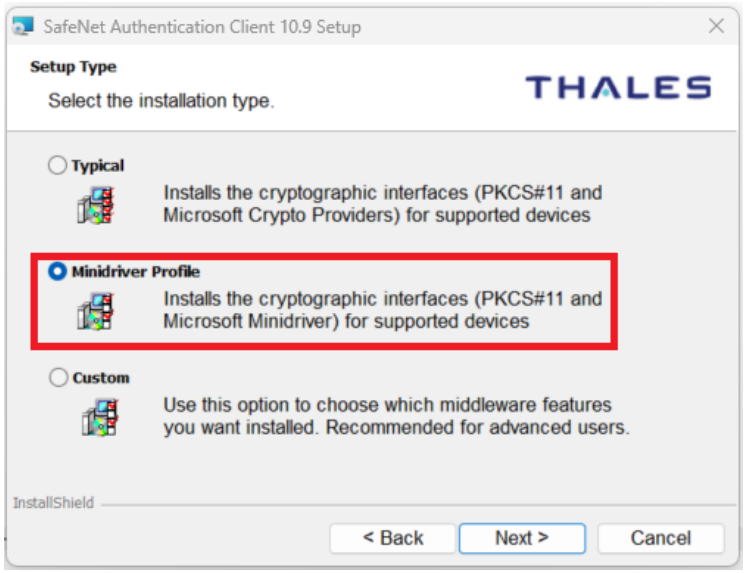
- Enrolled user will appear under **User certificates**



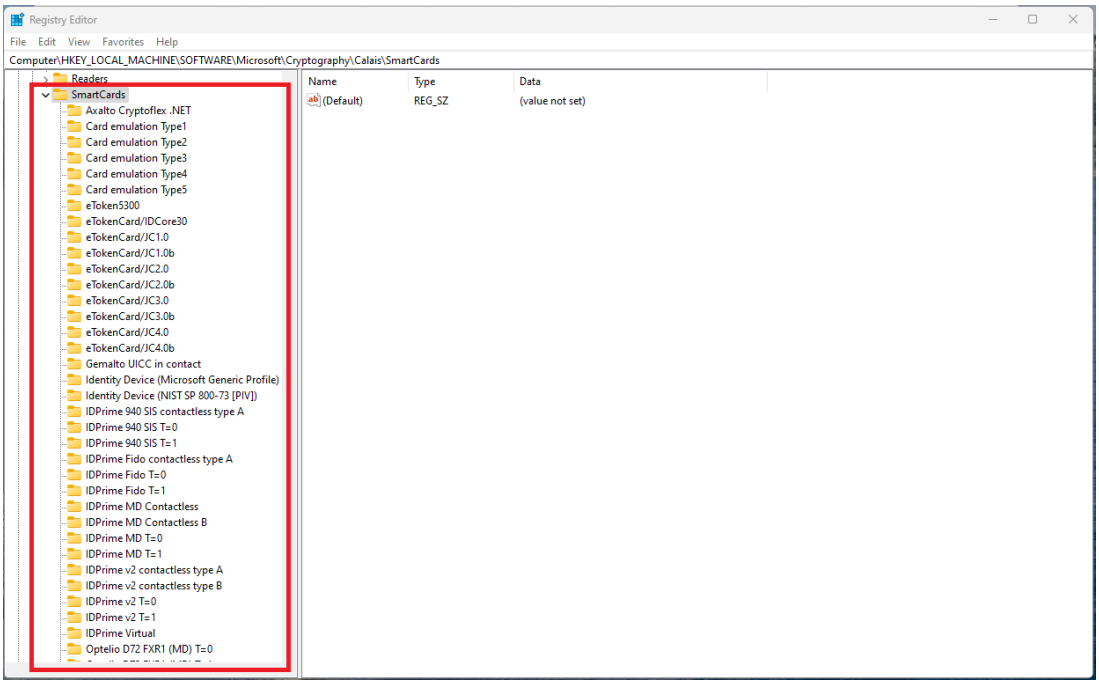
5. Install Smart Card Reader driver on the Kiosk machine

On the Kiosk machine, it is essential to install the appropriate drivers for your smart card Reader

- Please refer to your smart card provider's website for the correct drivers. For reference, we use SafeNet Authentication Client, which includes drivers for Thales (formerly Gemalto) smart card readers
- When running SafeNet Authentication Client installer, you will be given two options: **Typical** (including client and drivers) or **Minidriver Profile** (drivers only). Select **Minidriver Profile**



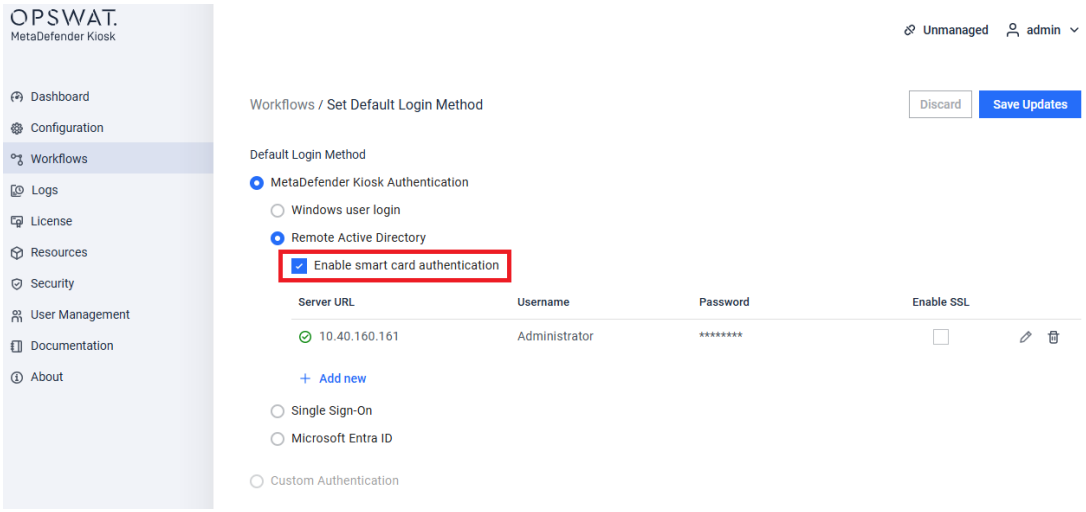
- After completing the driver installation, you can verify that the installation was successful by checking the registry. Open the **Registry Editor** and navigate to
  - **Computer\HKEY*LOCAL*** MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards**
- Here, you should see the list of all installed drivers



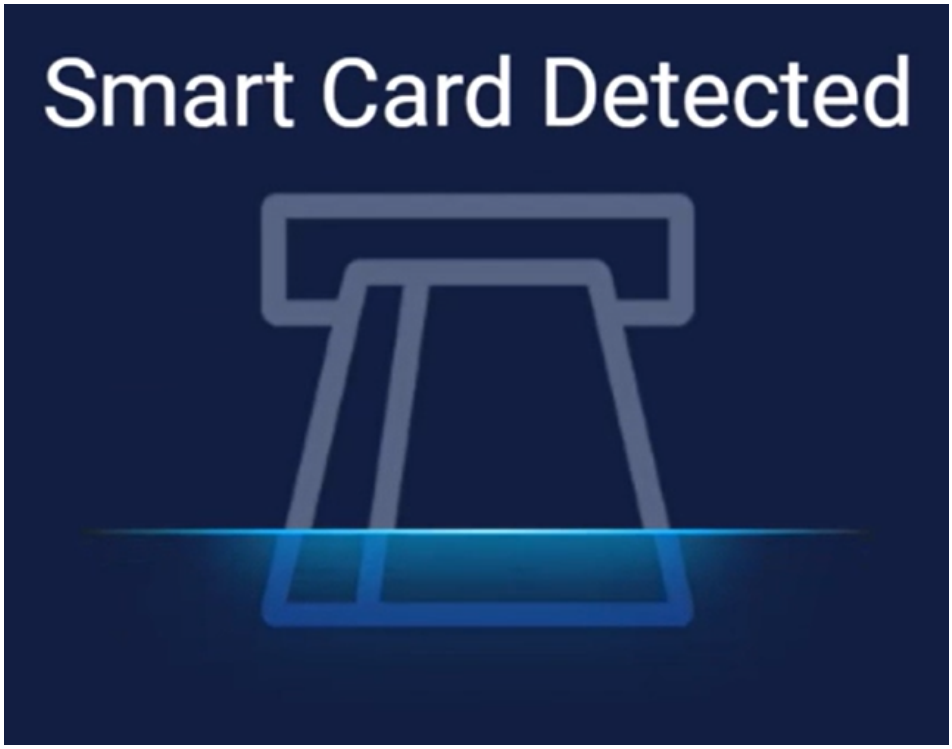
6. Enable smart card detection on Kiosk configuration

- From Kiosk WebMC, navigate to **Workflows**, click on **Set Default Login Method**. Select **MetaDefender kiosk Authentication**, select **Remote Active Directory**, check **Enable smart card authentication**.

Active Directory is required
To use smart card reader authentication, Active Directory must be enabled and configured.



- When enabled smart card authentication, an icon will appear in the Kiosk UI during the authentication process. Users can swipe their smart card for authentication.


Smart Card Detected

Setup RFID card for user authentication

Overview

This guide demonstrates the prerequisites and process of setting up an RFID Smart Card reader for authentication in MetaDefender Kiosk. Please note that this guide is for reference only. For the most accurate instructions, refer to the setup documentation provided by your Smart Card providers.

Prerequisites

RFID Card Reader

MetaDefender Kiosk supports integration with RFID Smart Card readers in keyboard emulation (or wedge) modeand are configured to terminate output with an <Enter>. Most common card readers that can be configured to meet these prerequisites should work with Kiosk. We have specifically tested with the following models:

- DUALi DE-620 RF card reader
- ELATEC TWN4 MultiTech 2 LF HF RFID reader

Quick tips to check if the RFID Card Reader compatibility with Kiosk

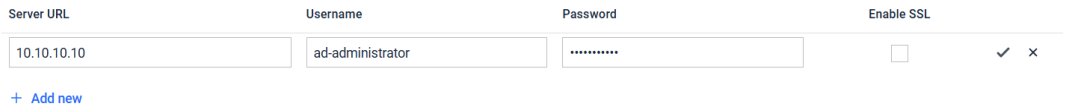
1. Connect the RFID card reader to a PC and open Notepad. Ensure the cursor is active in Notepad
2. Swipe the card. If a number appears (ending with <Enter>), the card is using HID
3. Swipe the card again. If the same number appears on a new line, the card is supported

Active Directory

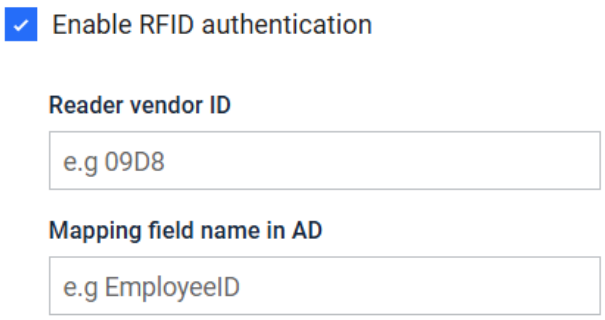
MetaDefender Kiosk requires a connection to an Active Directory server in order to authenticate and map users to their RFID card. A field in Active Directory must be made available and Kiosk granted the appropriate permissions to write to that field in order to maintain the mapping.

Integrate with AD and Enable RFID authentication

- From **Kiosk WebMC**, navigate to **Workflows**, under **Employee Workflow**, click on **Set Default Login Method**, select **MetaDefender Kiosk Authentication**, select **Remote Active Directory.**
    - Click on **Add new** and provide the information of your Active Directory server for integration

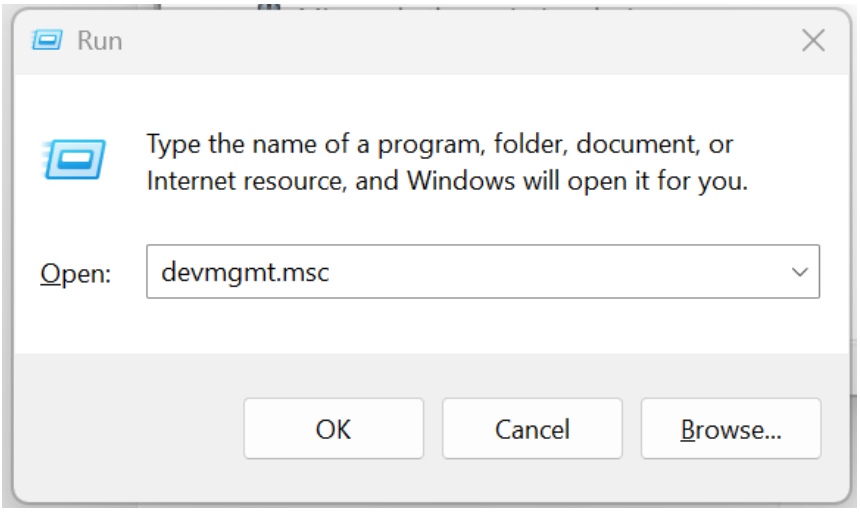


- Click on **Enable RFID authentication**. Provide the information below:
  - **Reader vendor ID**: RFID reader vendor ID can be found in the Device Manager (see the steps)
  - **Mapping field name in AD**: Provide a custom field in AD user attributes to store RFID card code. If not provided, Kiosk uses EmployeeID by default

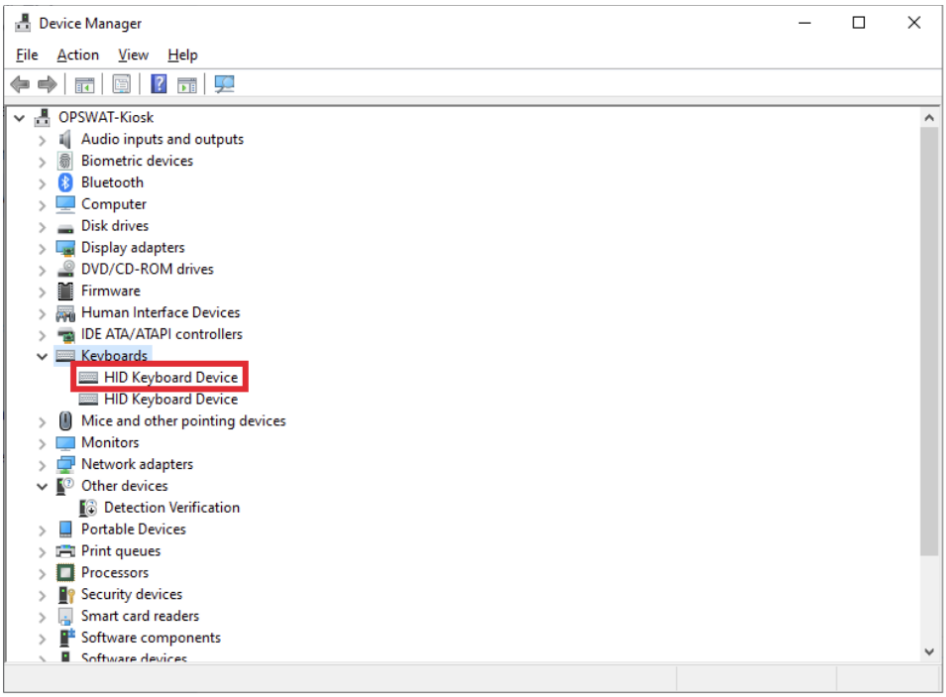


Acquire RFID reader vendor ID

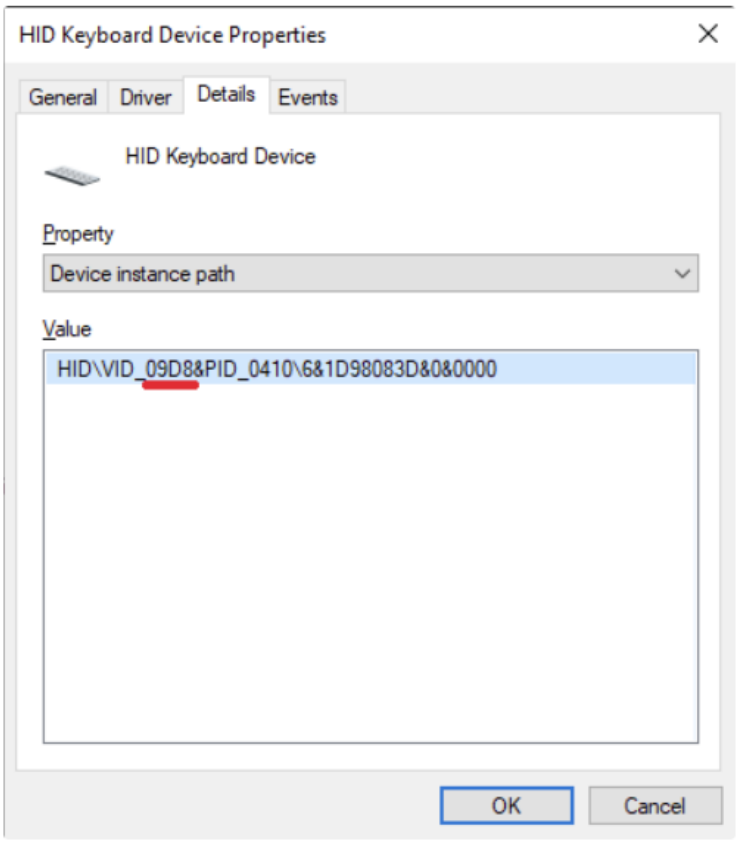
- Press **Win + R**, type **devmgmt.msc**, and open it with Administrator permissions



- Under **Device Manage**r, navigate to **Keyboards,** plug in the RFID reader to the Kiosk system. The first **HID Keyboard Device name** should be the RFID reader

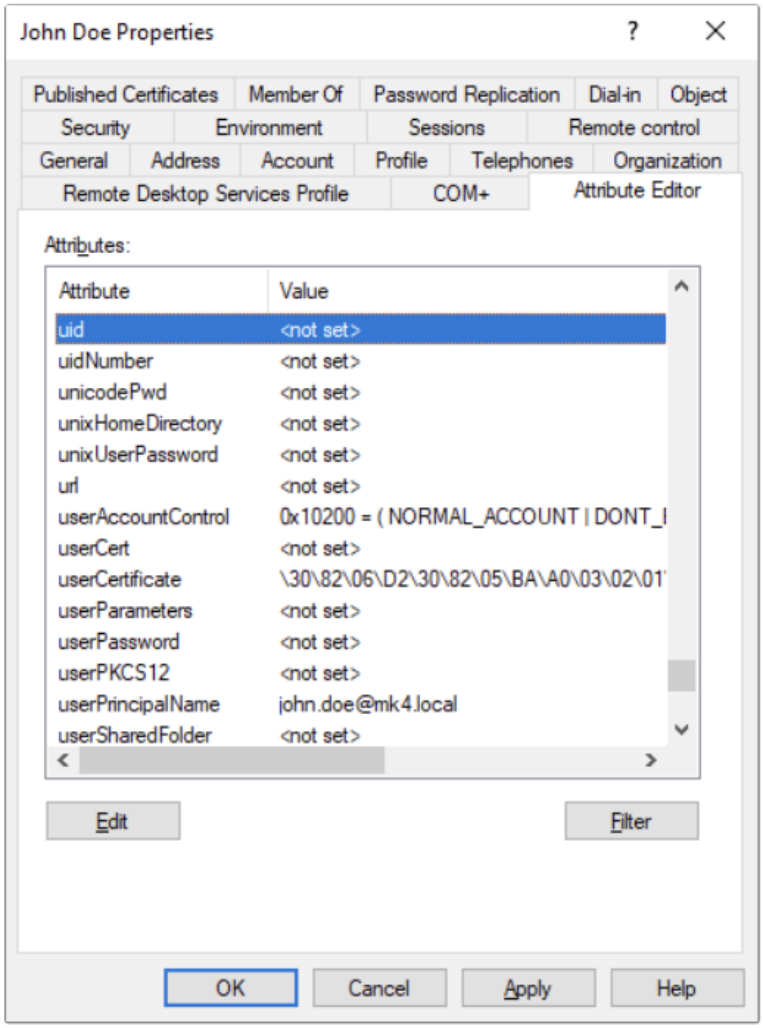


- Double-click on **HID Keyboard Device ID**. It should pop up a properties window, click on **Details** tab, change **Property** to **Device instance path** to verify the value.
    - You should see the value similar as the example below. **Reader vendor ID** is the 4 characters after "VIC_", in this example, it is **09D8**



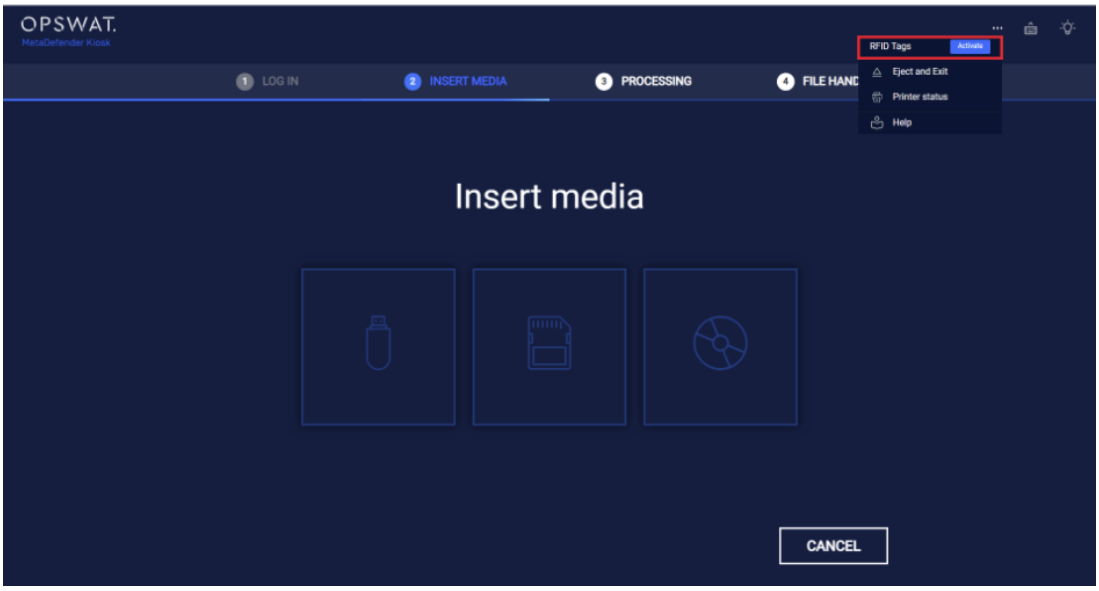
Mapping field name in AD

- Open **Active Directory User and Computers** and select **Properties** of a user. Go to **Attribute Editor** tab, you can use any available attribute for Kiosk to set RFID card code. For example, **uid**

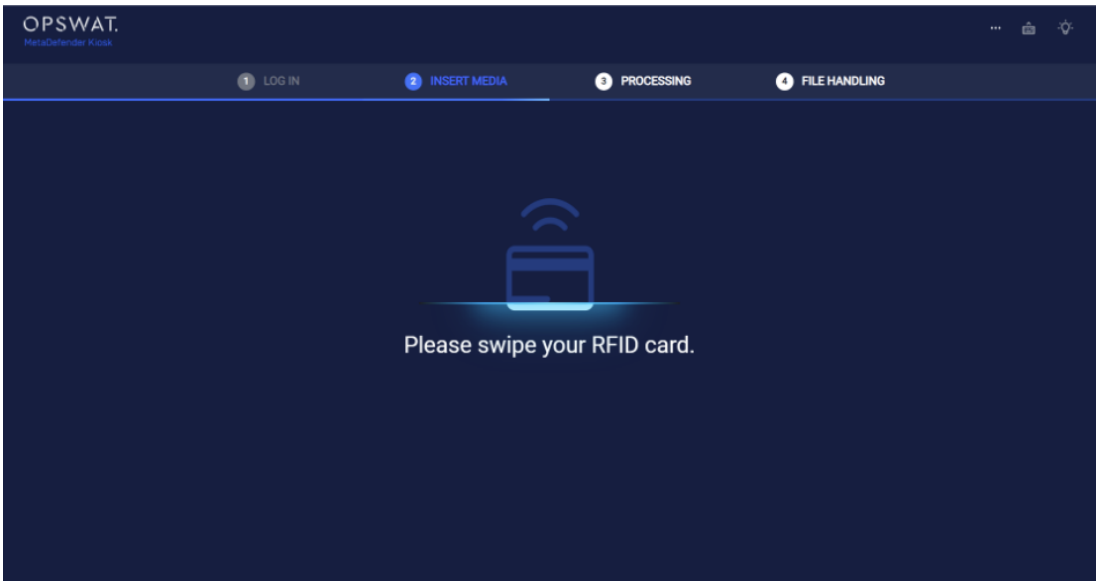


Register RFID for a Kiosk user

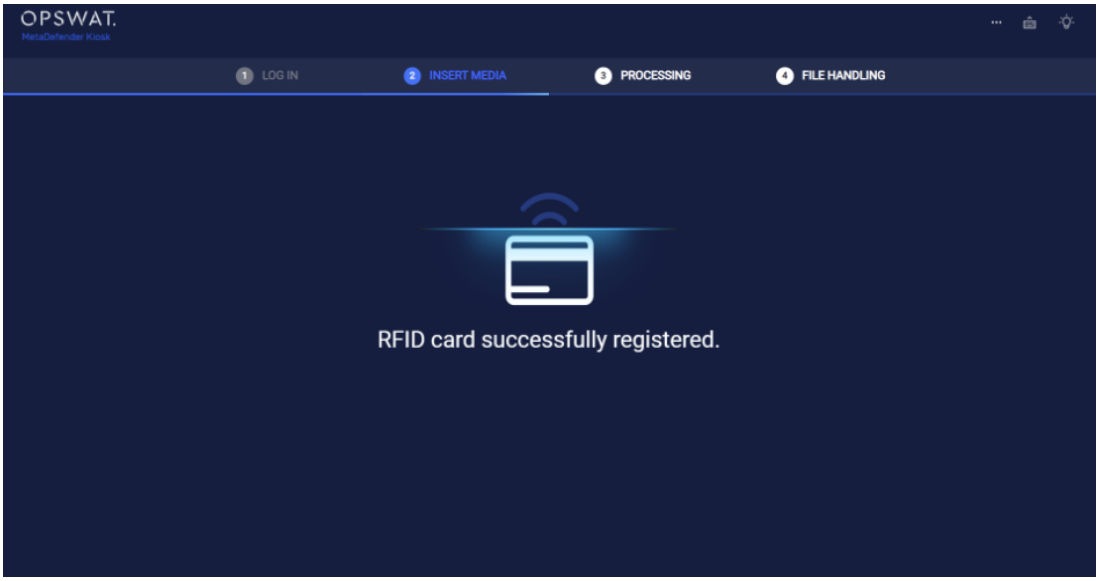
- Once the setup of RFID authentication is successfully completed, open **Kiosk UI**, select **Employee Workflow** and login with an AD account
- At the **Insert media** screen, the user can register the RFID card if it is not yet registered, Click on **... icon** to access more settings, click on **Active** button next to **RFID tags**



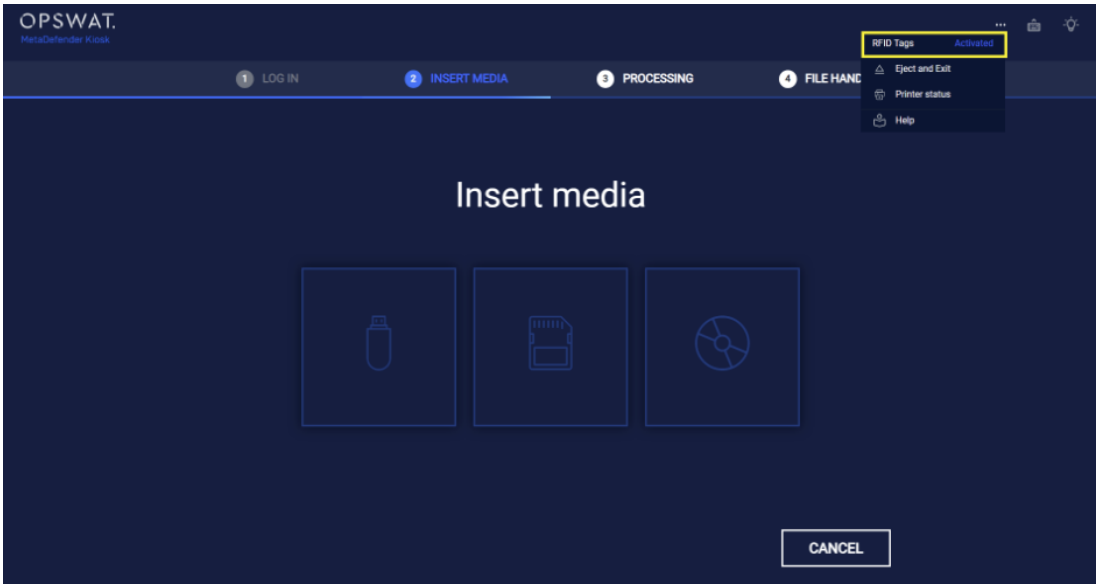
- Kiosk will request the user to swipe a RFID card for registration



- When successfully register an RFID card, Kiosk will show the screen below



- The user can verify if their RFID card is registered to their account by clicking on **... icon** to access more options. If the card is registered, Kiosk will display **Activated** next to **RFID tags**. Once activated, the user can authenticate to Kiosk simply by swiping their RFID card



Configure OAuth email authentication - Microsoft 365 (Graph API)

Overview

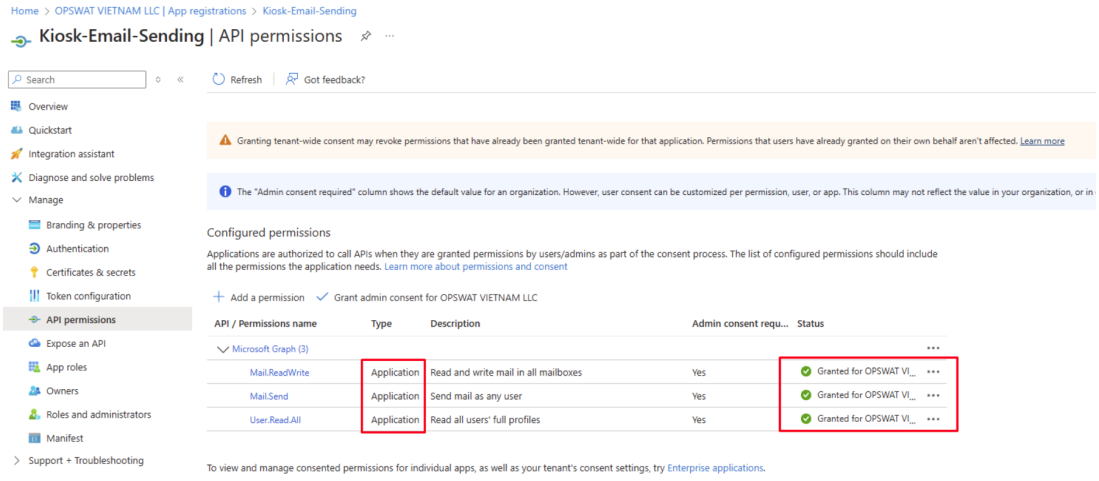
This section provides administrators with step-by-step instructions to configure Microsoft 365 (Graph API) for OAuth email authentication, enabling the system to send email reports and notifications.

Prerequisites

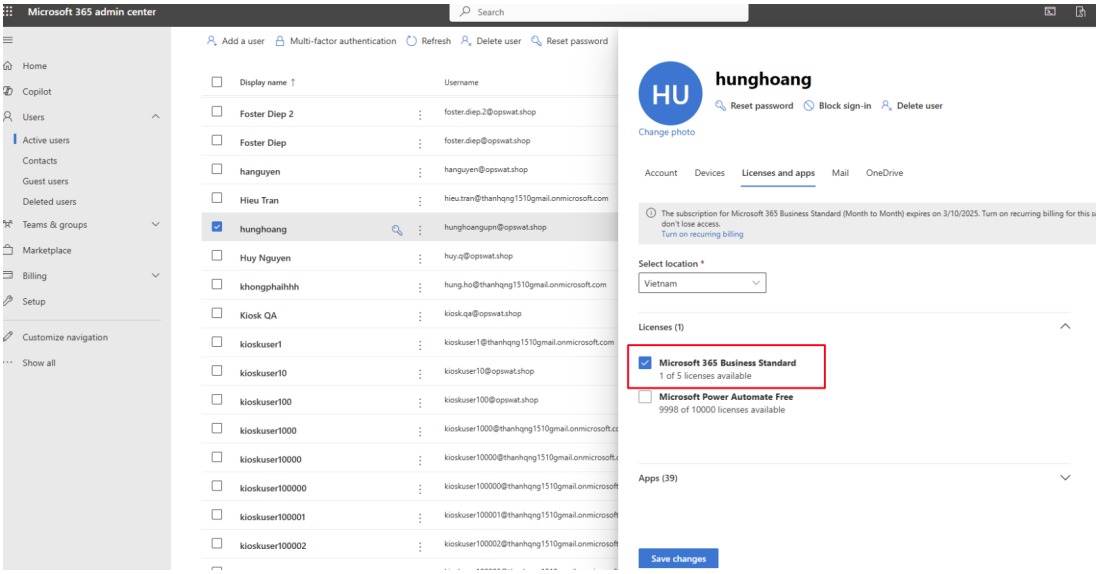
- ** Application Registration in Entra ID:
- *To use Microsoft 365 (Graph API), an application must be registered in Entra ID. Follow this guide for step-by-step instructions on registering an application
- ** Microsoft 365 license for email:
- *The account which will send email notifications and reports must have an assigned Microsoft 365 license

Configure Microsoft 365 (Graph API) for OAuth email authentication

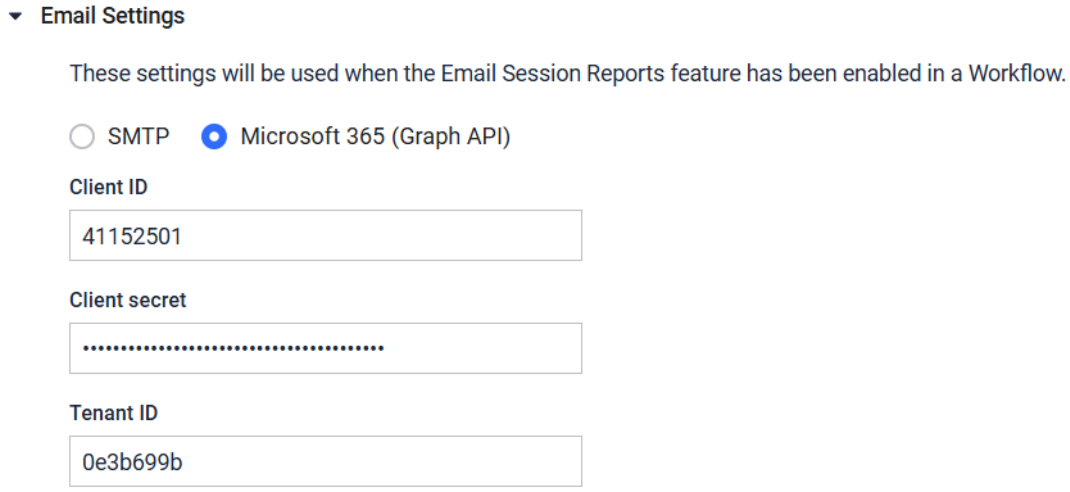
Step 1. Create an Application in Entra ID. Assign the following **application permission**s and **grant admin consent** for the selected permissions



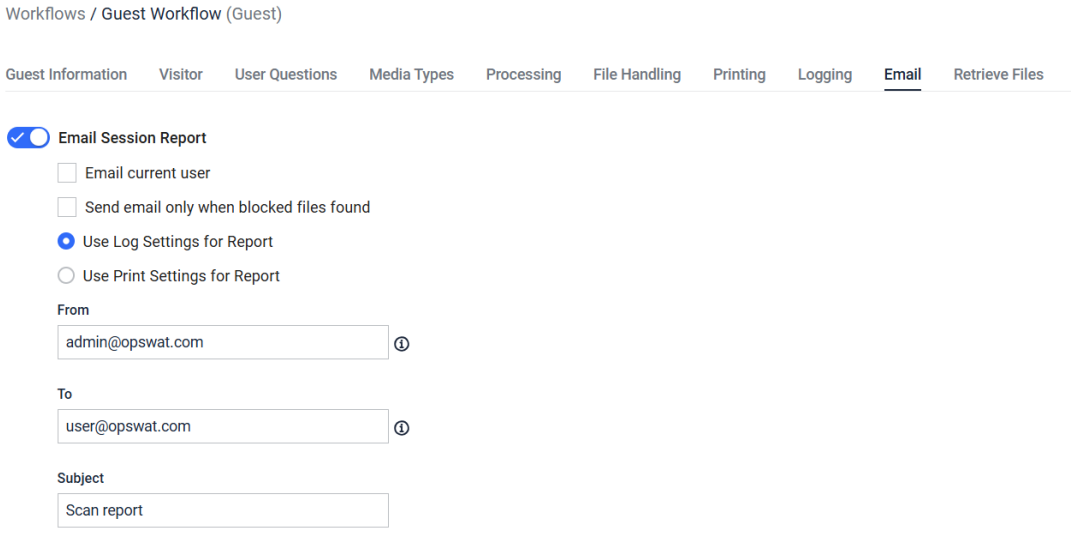
Step 2. Login to https://admin.microsoft.com/ as an **Administrator**. Assign the required **Microsoft 365 license** to the user who will send email reports and notifications



Step 3. From **Kiosk WebMC**, navigate to **Configuration**, select **Email**, expand **Email Settings**, select Microsoft 365 (Graph API). Enter the **Client ID**, **Client Secret** and **Tenant ID** acquired from Step 1.



Step 4. Configure sending email session report under **Kiosk WebMC**, select **Workflows**, select **Email**.



Email account requirements

The email account used to send email reports must have an active Microsoft 365 license and the necessary privileges to send emails.

Troubleshooting Issues

UI

With some high resolution touch screens, click events from a mouse are not registered if the Scale and Layout display setting is set to greater than 100%. Workaround is to hold the right mouse button to ensure the left button click is respected.

Physical Input Devices

Customers have reported some localization issues with older versions of Windows 10 and physical input devices (e.g. keyboard, mouse, etc...). If you experience these issues, please try updating the system to see if it resolves the issue. If the issue persists, please contact Customer Support.

License Activation

If online license activation does not work through a proxy server, ensure the WinHTTP settings are configured. First, proxy settings should be configured in Internet Explorer. Then, open a command prompt as Administrator and run `netsh winhttp import proxy source=ie`. Kiosk should now be able to route the license activation through the proxy.

Joining a Hardware Kiosk to a domain

In some cases, joining a Kiosk to a domain will fail. The Netlogon service fails to start with error: "Windows could not start the Netlogon service on Local Computer. Error 1058...". Verify if any recent network settings have been modified. Restart the system to ensure network setting changes have been correctly applied and the Netlogon service can start as expected.

Generate Support Package

A support package contains essential information about the operating system and the MetaDefender Kiosk application, which OPSWAT support requires to troubleshoot any issues that arise.

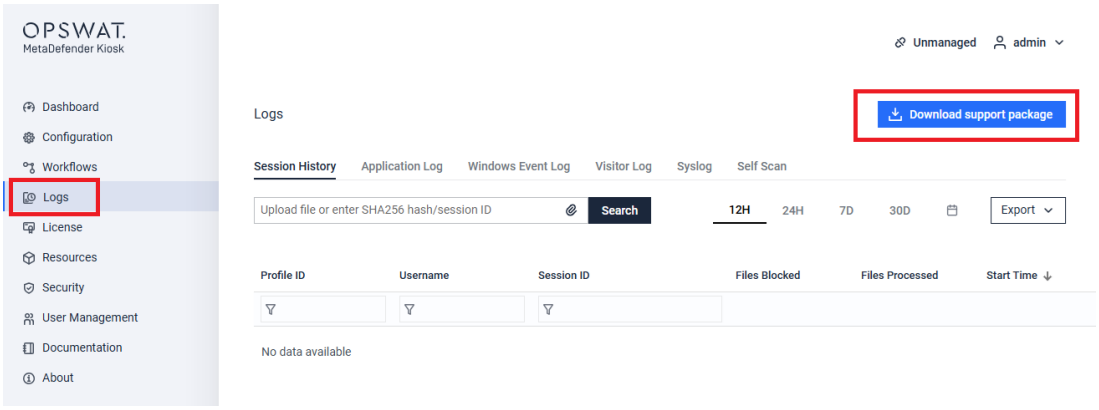
Content of the support package

The support package contains the following elements:

- **configuration files**
- **log files**
- **system information**
- **directory and files information**
- **registry key configuration**

Creating the package

From **Kiosk WebMC**, navigate to **Logs** section. Click on **Download support package**. The support package will be named *MetaDefender___Kiosk_Debug.zip.*



Alternatively, we can collect these information via command line tool. Run cmd.exe with administrator permissions, run the following command line:

```
"C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\omdDebugTool.exe" ALL
```

```
C:\Windows\System32>"C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\omdDebugTool.exe" All
Read registry key "db_instance" : localhost

Read registry key "db_port" : 27019

Collecting windows event log...

Collecting MongoDB event...

Read registry key "mongo_bin_dir" : C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\Mongo\64+\

Collecting MongoDB logs...

Read registry key "mongo_log_dir" : C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\Mongo\log\

Collecting registry key...
Running command: C:\ProgramData\OPSWAT\Metadefender\KioskRegTool\RegApp.exe export /hkey HKLM /keypath SOFTWARE\WOW6432N
ode\OPSWAT\MD4M /export "C:\Users\FOSTER~1.DIE\AppData\Local\Temp\Metadefender_Kiosk_Debug_12172024_1412\MetadefenderReg
Key.reg"
Collecting REST version...

Read registry key "rest_dir" : C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\REST\
```

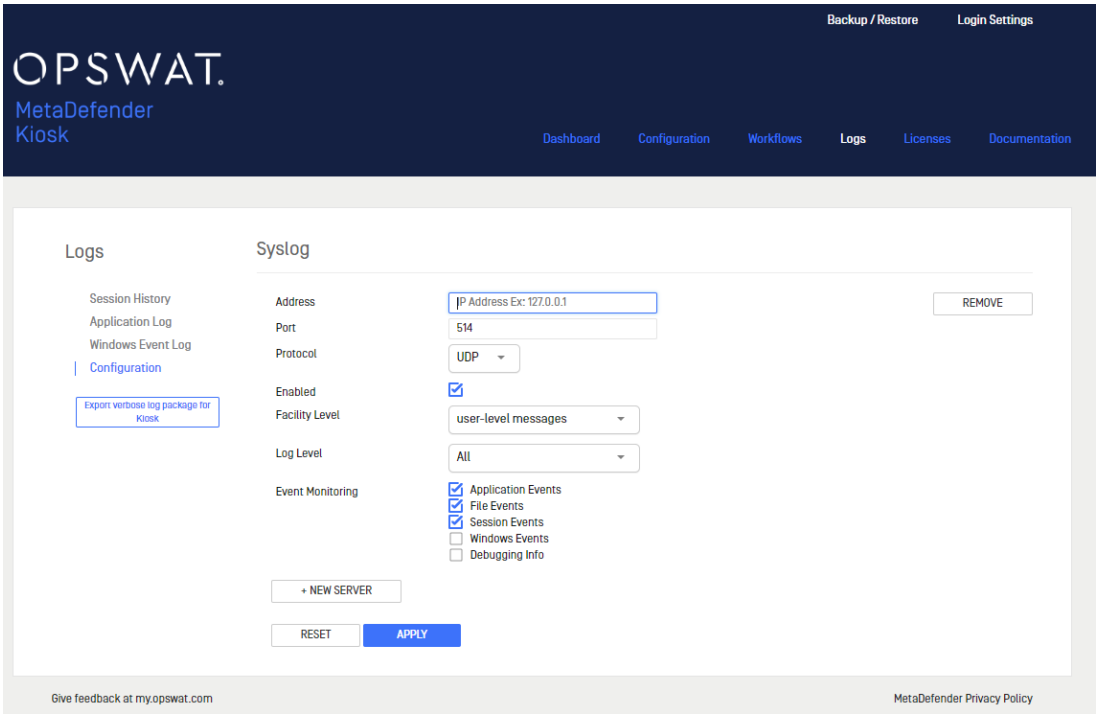
The logs will be collected and stored under *`C:\Users<user-name>\AppData\Local\Temp\MetadefenderKiosk`` Debug`_*

Can a Syslog event be generated when an infection is found by MetaDefender Kiosk?

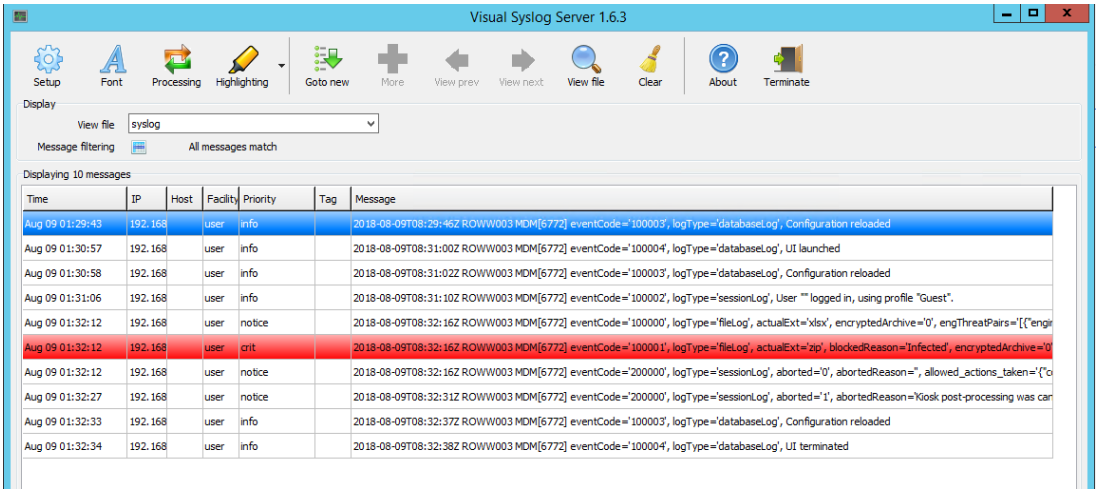
Pro Tip:
Syslog, also known as System Logging Protocol, is designed to send system log and event messages from a network of devices to a centralized syslog server for monitoring, review and remediation.

Yes.

When the Syslog is configured under **Logs>Configuration>New Server** (as illustrated in the screenshot below), MetaDefender Kiosk will log infected file events by default.



The example below, highlighted in red, illustrates how an EICAR test file is logged with its own unique event code - in this case, 100001.



Support:

If you have followed all of the steps above but are still unable to **Generate a Syslog Event When an Infection is Found by MetaDefender Kiosk**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

Why does Kiosk pause on the final screen after scan session "settings"?

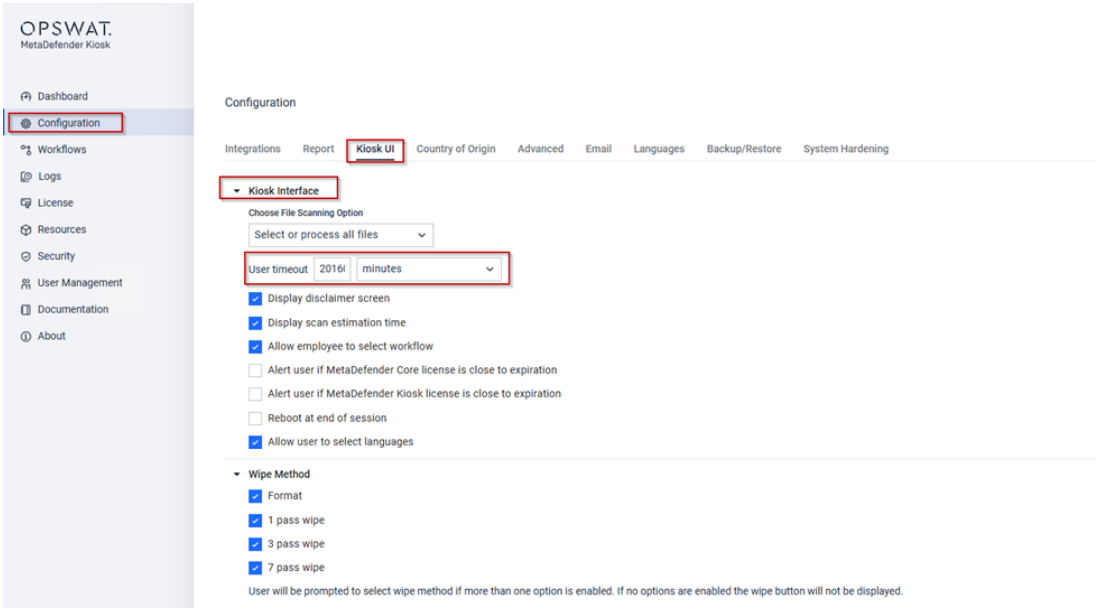
An important note related to the enhancement request described in the release notes listed below would be the necessary steps to address the timeout value and how to set it up.

https://www.opswat.com/docs/mdkiosk/v4.7.3/release-notes/release-notes

Kiosk does not automatically end the session	After the scanning session is completed, Kiosk pauses on the final screen for user acknowledgement.

Increasing or decreasing the timeout value from the Kiosk UI User timeout tab will result in adjusting the pause after a session is completed.

Max value for this tab can be set to 20160 min (2 weeks).



Support

If you encounter any issues or require further assistance, please contact OPSWAT support via My OPSWAT.

Our support team will be able to provide you with the necessary guidance and resolution for any license-related concerns.

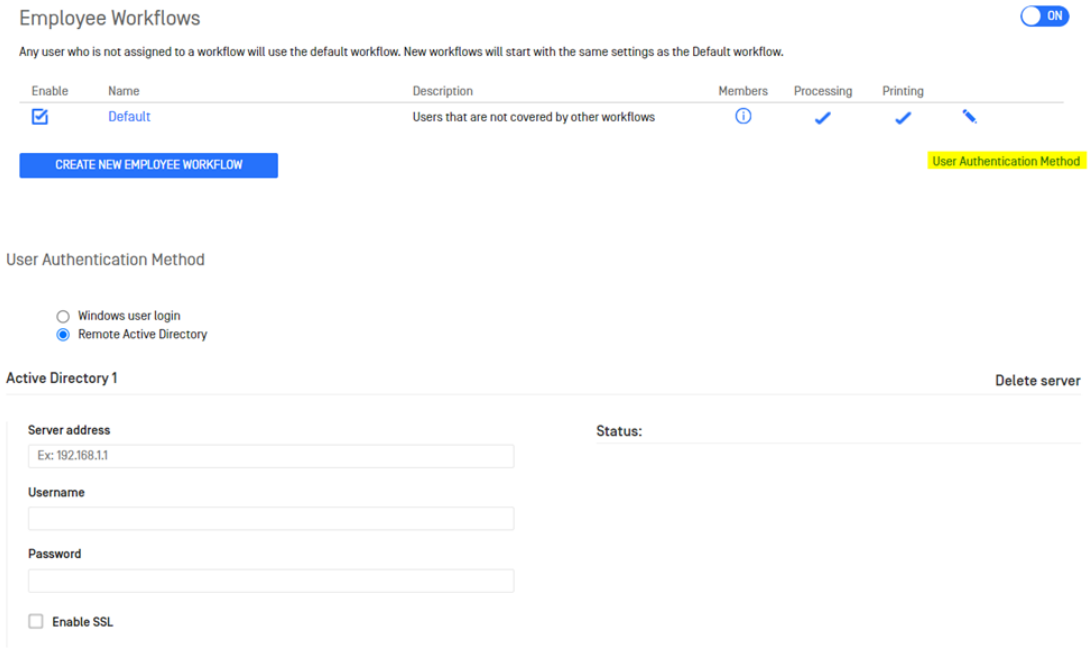
Can I add groups from Active Directory to MetaDefender Kiosk Workflow Profiles?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows or Linux systems.

Yes, you can.

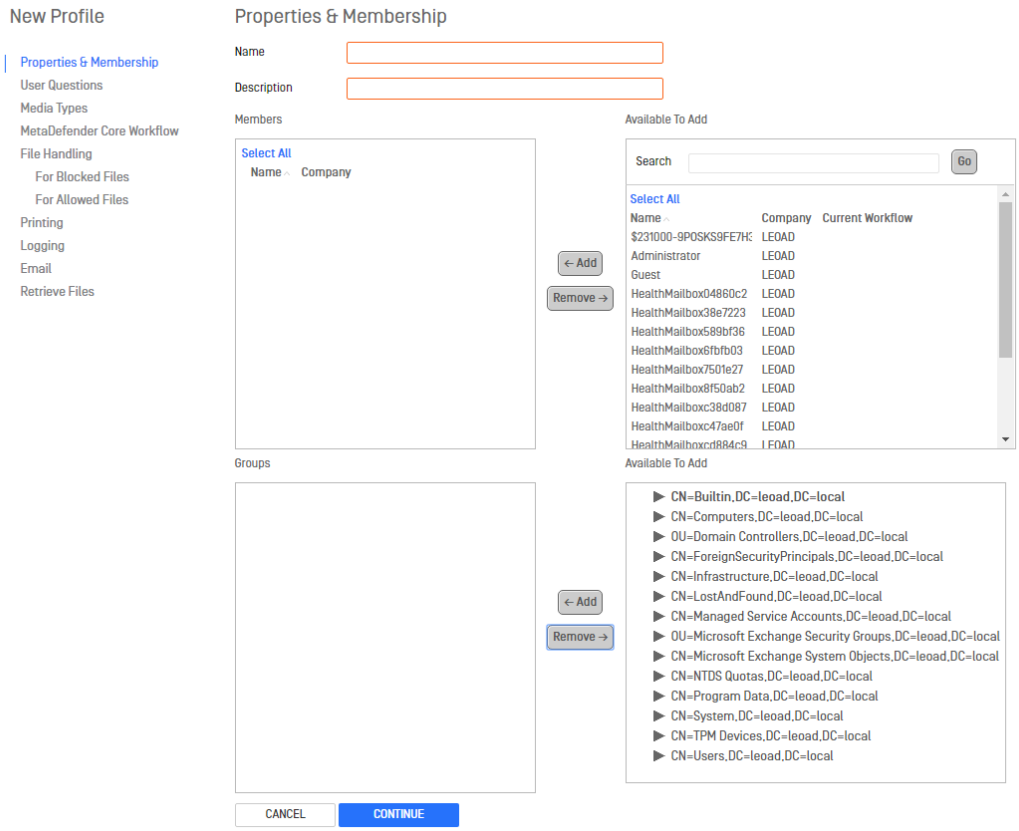
To add user groups from **Active Directory** to MetaDefender Kiosk **Workflow Profiles**, please follow the instructions below.

1. Connect to an Active Directory via the **MetaDefender Kiosk Management Console>Workflows>Employee Workflows>User Authentication Method**, as illustrated in the screenshot below.



Please Note:
The user will need read/write rights on Active Directory in order to effect these changes.

2. Create or edit a profile via the **MetaDefender Kiosk Management Console** > **Workflows** tab, as illustrated in the screenshot below.



3. Add groups by selecting them from the list and clicking the **Add** button.

Support:
If you have followed all of the steps above but are still unable to **Add Groups from Active Directory to MetaDefender Kiosk Workflow Profiles**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

Can I extend MetaDefender Kiosk by adding Custom Engines or Signatures?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows or Linux systems.

Yes.

Whether you require additional malware scanning, sensitive data scanning, or other forms of file scanning, it is possible to significantly extend the scanning capabilities of MetaDefender Kiosk.

This can be done by adding custom scan engines to the MetaDefender Core instance that the Kiosk is configured to scan files with.

Adding scan engines and external scanners to your MetaDefender Core instance (and updating these engines with the maximum available signatures/definitions) is one way to ensure optimal scanning performance from any associated MetaDefender Kiosk.

Pro Tip:
MetaDefender Core's engine options include 30+ Metascan AV engines, External Scanners, Deep CDR, Proactive DLP and more.

To learn more about adding, activating and utilizing these options, please click the associated link below.

- Metascan Engine Options and Requirements
- Engine Package Options
- External Scanners
- Deep CDR
- Proactive DLP

Support:
If you have any difficulty **Configuring and Using Custom Engines or Signatures**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

Can I run MetaDefender Kiosk using a non-administrator account?

No, it is **not possible** to run MetaDefender Kiosk using a limited-privilege account. The core functionality of MetaDefender Kiosk requires admin access to the host OS and this is not expected to change in the future versions.

To preserve the integrity of your Kiosk environment, you are encouraged to follow the steps outlined in the MetaDefender Kiosk Documentation.

Can I upload files to a file server after they have been scanned by MetaDefender Kiosk?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows or Linux systems.

Yes, you can.

There are multiple ways in which files can be moved to a file server after they have been scanned by MetaDefender Kiosk.

All of the following options can be configured as part of your MetaDefender Kiosk Workflows:

1. Files can be uploaded to a MetaDefender Managed File Transfer server via built-in integration with MetaDefender Kiosk.
2. Files can be copied to a specified network path.
3. Files can be uploaded to a file server by running a custom script.

Administrator Caution
Enabling Custom Command Line Script may introduce potential security risks. It is recommended that only experienced administrators enable and manage this setting, taking full responsibility to implement appropriate security measures and monitor for any vulnerabilities.

Pro Tip:
For more information on each method listed above, please Read This.

Support:
If you have any difficulty **Uploading Files to a File Server After Scanning Them With MetaDefender Kiosk** , please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

How can MetaDefender Kiosk and Managed File Transfer (formerly Vault) be configured to work with an Arbit Data Diode?

This article describes how to deploy MetaDefender Kiosk, an Arbit data diode, and a MetaDefender Managed File Transfer server for the following use case:

1. Portable media is scanned by MetaDefender Kiosk.
2. Clean files are passed through an Arbit data diode to a Managed File Transfer server.
3. User downloads files from the MFT server.

System Deployment

Do the following before configuring the individual systems:

1. Install MetaDefender Kiosk with MetaDefender Core on the low side network.
2. Install the Arbit data diode with the receiving side in the low side network and the transmitting side on the high side network.
    a. Assign a static IP address to the low side.
    b. Assign a static IP address to the high side.
3. Install the MFT server on the high side network.
    a. Assign a static IP address.

MFT Server Configuration

1. Create the user accounts on the MFT server.
    a. Note the account that should be used as the 'from' account for files coming from MetaDefender Kiosk.
2. Generate the authorization token.

Arbit Data Diode Configuration

1. Define the URL list on the high side of the data diode to include the MFT server.
    a. URL list includes http://:8000/Vault_rest/file

MetaDefender Configuration

1. Configure the appropriate MetaDefender Kiosk workflow profile to enable Copy To MFT in the post-action.
2. Put in the URL of the data diode low-side receiver.
    a. http://<diode low-side IP address>:8080/pitcherrestapi/transfer/<URL List>
3. Enter the authorization token generated by the MFT server.

4. Enter the Sender MFT account that was created on the MFT server.

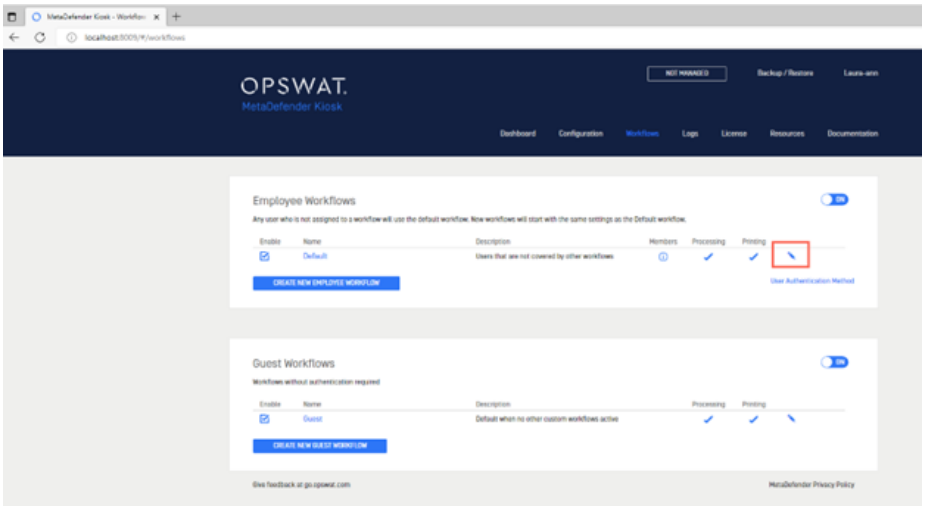
How does MetaDefender Kiosk do file type detection?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows or Linux systems.

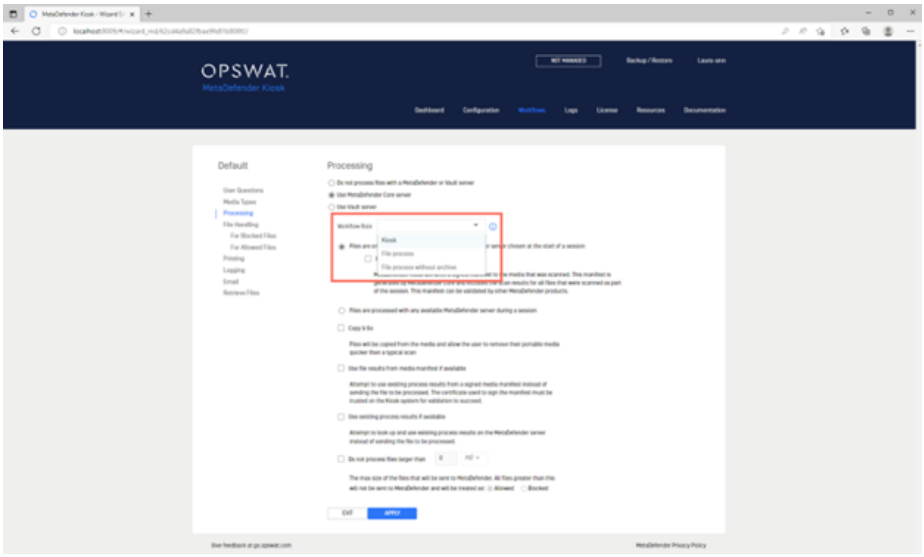
One key feature of the MetaDefender Kiosk solution is its advanced file-type detection capability (a.k.a. file-type analysis/file-type mismatch/file mismatch analysis, etc.), driven by Kiosk's integration with MetaDefender Core.

To enable Kiosk's file-type analysis feature:

- Open your **Kiosk Management Console>Workflows** tab.
- Click the *edit* icon on the relevant user workflow

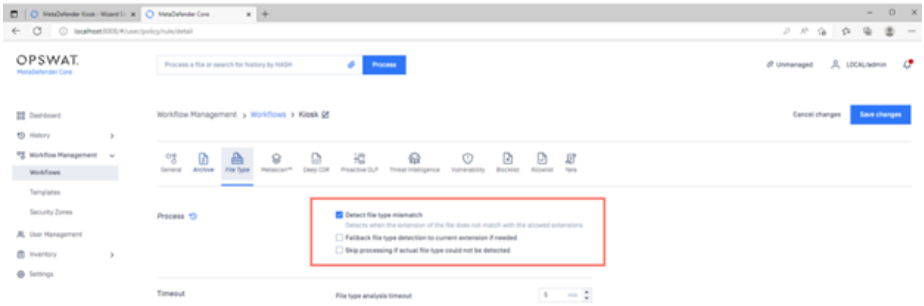


- Assign the appropriate workflow (a workflow with file-type detection enabled) under **Processing>Workflow Rule**, as illustrated below:



To enable or configure the file-type analysis feature on a given workflow:

1. open your **Core Management Console>Workflow Management>Workflows** tab
2. open any Kiosk-associated workflow
3. make changes under the **File Type** tab, as illustrated in the screenshot below.



Pro Tip:
For the full list of 4500+ file-types supported by MetaDefender Core's file-type detection feature, please Read This Article

Support:
If you have any difficulty **Configuring and Assigning Workflows to Enable Kiosk's File-Type Detection Feature**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

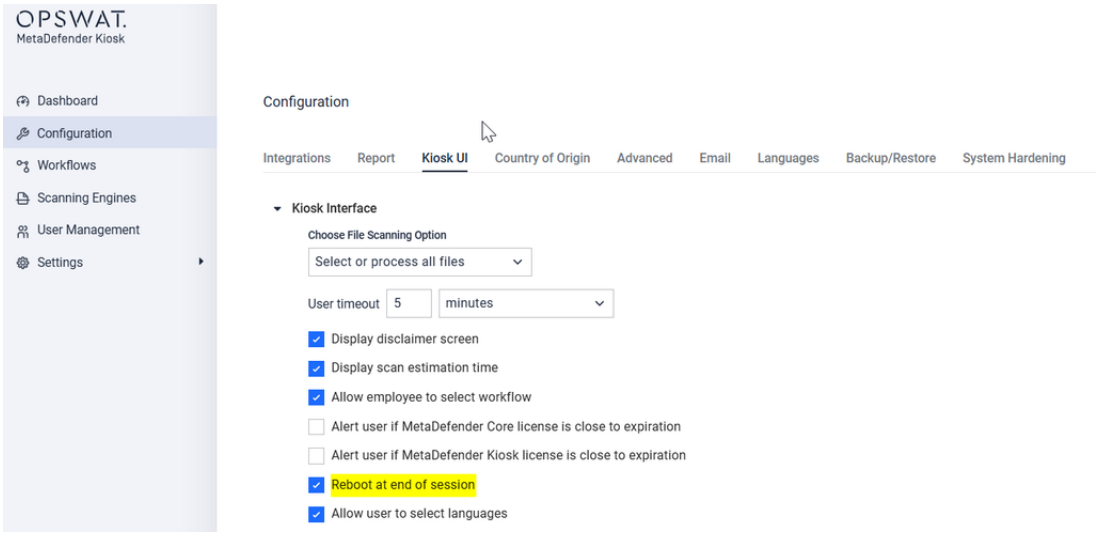
How do I revert MetaDefender Kiosk to a previous state using Deep Freeze software?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows or Linux systems.

Faronics Deep Freeze Enterprise software can be used to restore the MetaDefender Kiosk to its optimal original state after every scan session.

To configure your system to revert after each session, please follow the steps below:

- Ensure that Deep Freeze Enterprise edition is available.
- Install Deep Freeze Enterprise edition *without* enabling **Deep Freeze Local Policies.**
- Go to your **Kiosk Management Console>Configuration>Kiosk UI> Kiosk Interface**, then enable the Kiosk to **Reboot At End Of Session** as highlighted in the image below.



- Configure Kiosk to your preferences and then activate the product.
- Finally, take the system snapshot with your Faronics Deep Freeze software.

Pro Tip:
Faronics Deep Freeze 'protects endpoints by Freezing a snapshot of a computer's desired configuration and settings defined by the IT Admin. With an instant reboot, any unwelcome or unwanted changes are removed from the system, restoring it to its pristine Frozen state.'

Support:
If you have any difficulty **Reverting MetaDefender Kiosk to a Previous State Using Deep Freeze Software**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

How do I copy and save files to a mapped drive with MetaDefender Kiosk?

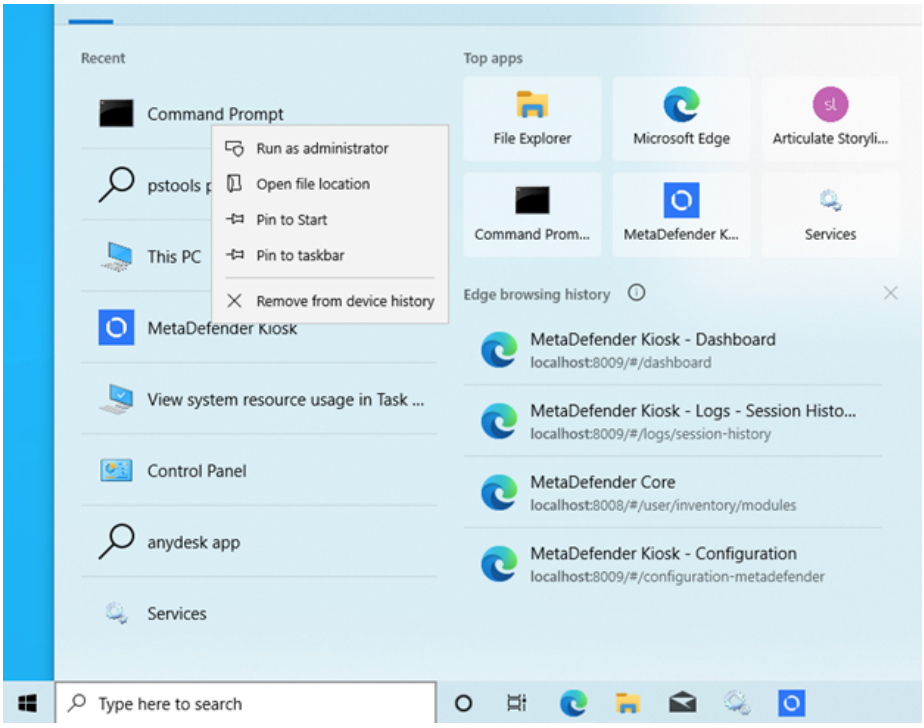
Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows or Linux systems.

Pro Tip:
A mapped drive/ network drive is a shortcut to a shared resource (folder, file, etc.) that is physically stored in a different location (on a remote FTP server, website, laptop, etc.) but appears in your directory system, just like one of your local drives (like the C or D drive, for example).

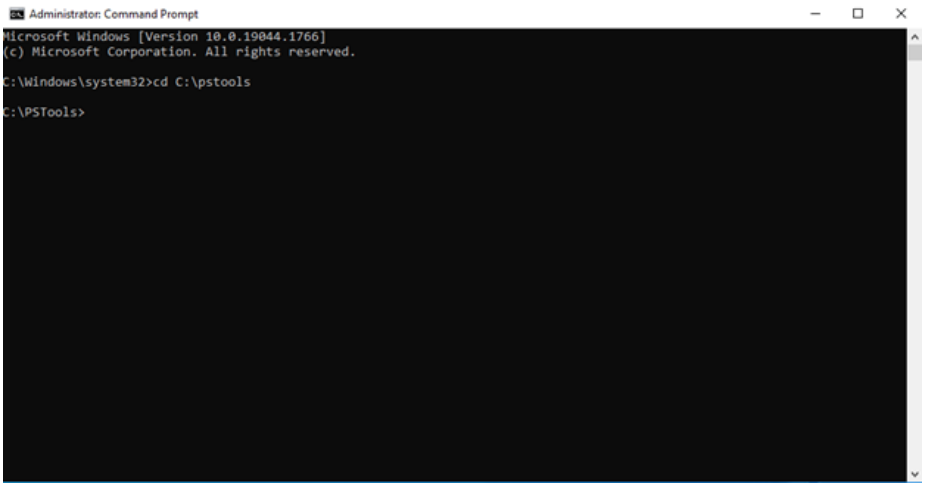
In order to save files to a mapped drive from MetaDefender Kiosk, the mapped drive must first be created under the **SYSTEM** account.

To do this, please follow the instructions below:

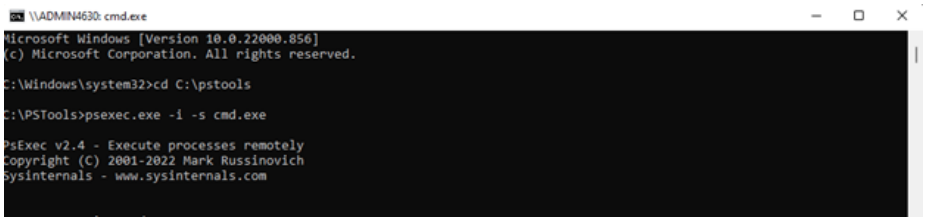
- Download the **psexec.exe.zip** file from Microsoft's Sysinternals Security Utilities suite by visiting this Webpage, then extract it and delete the original zip file.
- Now, place the psexec.exe tool on the machine where you want the mapped drive to be created (e.g. **C:\PSTools\psexec.exe**).
- Open the command prompt, right click and select: **Run as Administrator.**



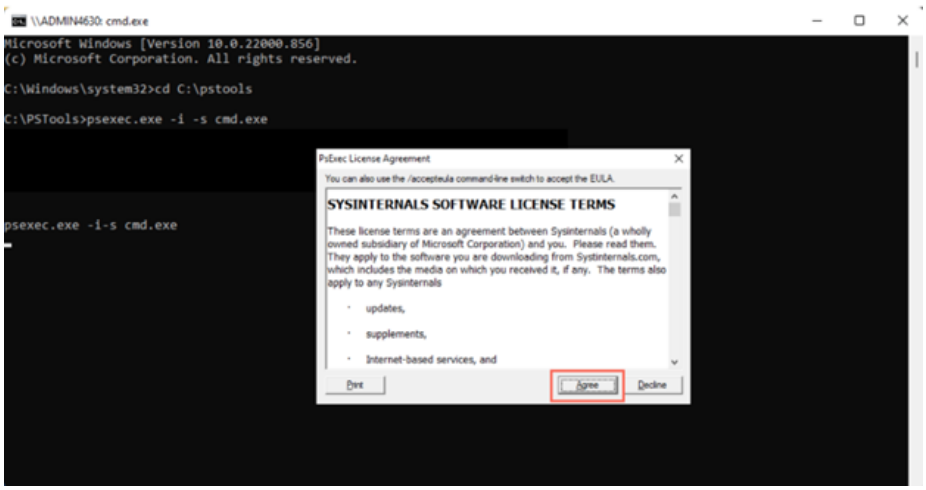
- In the command prompt, navigate to the directory where psexec.exe was copied (e.g. **cd C:\pstools,** as illustrated in the screenshot below).



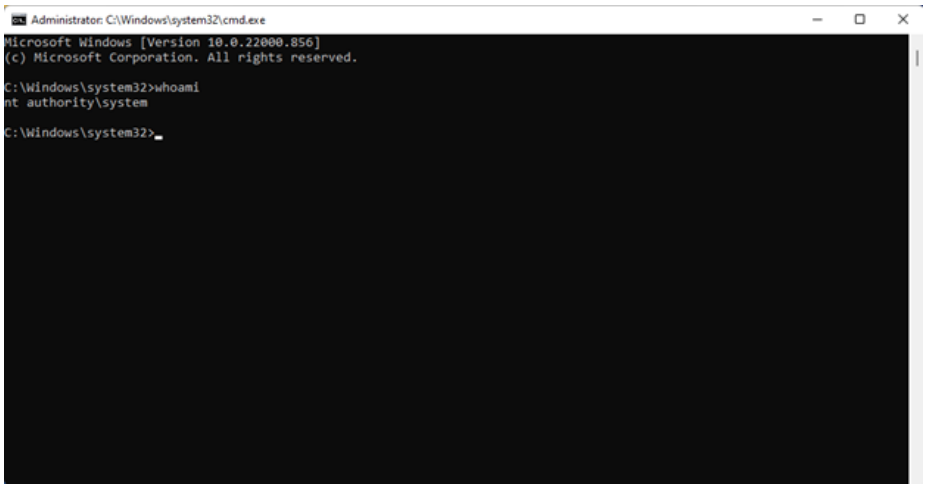
- Enter the following command **psexec.exe -i -s cmd.exe**, as illustrated in the screenshot below: `psexec.exe -i -s cmd.exe`



- If the Sysinternals pop-up appears, click **Agree**, as illustrated in the screenshot below.



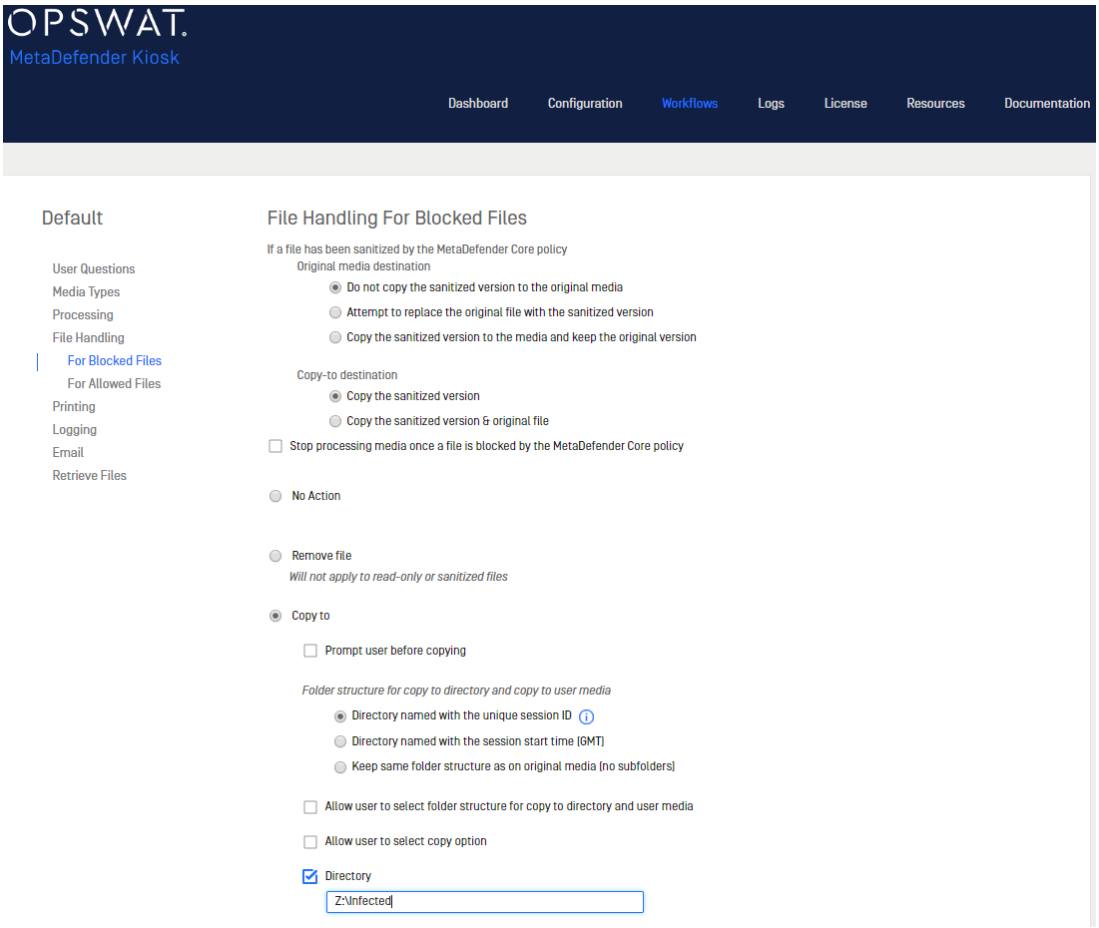
- An elevated command prompt window will open.
- Enter the command: `whoami` to confirm that the new command prompt is running as: **nt**



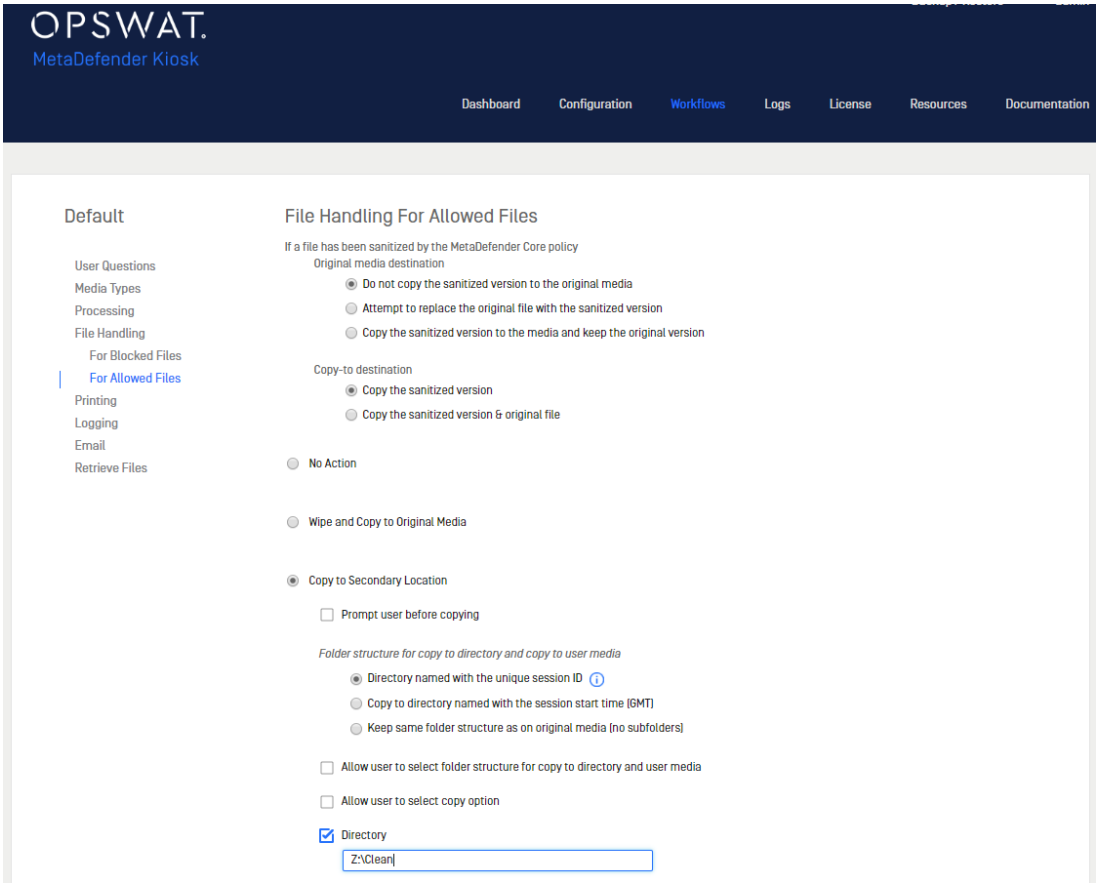
- Enter the following command to mount the mapped drive: **use <desired drive letter> <UNC path to map the drive to>** (e.g. net use Z: \file-server-1\share).

Your mapped drive has been created and mounted. Next, you must configure MetaDefender Kiosk to copy and save both blocked and allowed files to the newly created mapped drive, as follows:

- Once the mapped drive is in place, go to your **Console>Workflows Tab** and click on the relevant workflow.
- Inside your chosen workflow, go to **File Handling>For** and select the **Copy to** radio button.
- Enter the map drive location, as illustrated in the screenshot below.



- Now, go to **File Handling>For Allowed Files** and select the **Copy to** radio button.
- Enter the map drive location, as illustrated in the screenshot below.



- Finally, click **Finish** to save your changes.

MetaDefender Kiosk can now copy and save both blocked and allowed files to the mapped drive.

Support:
If you have any difficulty **Saving Files To a Mapped Drive With MetaDefender Kiosk**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

How do I set the Restart MetaDefender option for MetaDefender Kiosk Watchdog on Windows 8 and above?

The following information is for users who would like to set the MetaDefender Kiosk Watchdog to the "Restart MetaDefender" option when running on Windows 8 or above.

In order for the Watchdog to be able to restart the MetaDefender Kiosk UI automatically, you will need to fully disable User Account Control (UAC) in the Windows OS. This is because in Windows 8 and above Microsoft has made the process of launching an interactive process from a service extremely difficult due to the security holes this could potentially open up. The most effective way to disable UAC is to make a change to a registry value:

1. Click **Start** and type regedit.msc to open the Registry Editor.
2. Open the registry key at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System then find the EnableLUA registry value.
3. Set EnableLUA to 0.
4. Restart Windows.

Alternatively, you can adjust your Local Group Policy settings to disable UAC. You can only access the Group Policy Editor if you have the Professional, Enterprise, or Ultimate edition of the Windows OS.

1. Click **Start** and type "gpedit.msc" to open the Group Policy Editor.
2. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
3. After clicking Security Options, the right panel populates with your policies. Locate the ones for User Account Control.
4. Set **Run all administrators in Admin Approval Mode** to "Only elevate executables that are signed and validated."
5. Set **Switch to the secure desktop when prompting for elevation** to "Disabled"
6. Restart Windows.

Note:

Info
The steps described above will completely disable UAC on this machine. Please check with your system administrators before disabling this important Windows security feature.

Related articles :

http://winaero.com/blog/how-to-turn-off-and-disable-uac-in-windows-10/

http://www.computerperformance.co.uk/win8/windows8-uac-disable.htm

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

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases.

OPSWAT provides support on each release of MetaDefender Kiosk for 18 months after the publication of the **following** release of the product. So, once a new release is published, you have 18 more months of support on the previous release.

Keep in mind, however, that bug fixes and enhancements are applied only to the next release of a product, not to the current release or historical releases - even when those releases are still under support.

In some cases, hot-fixes can be provided for the current release of the product, and then incorporated as regular fixes in the next release.

Pro Tip:
OPSWAT highly recommends that users regularly upgrade to the latest version of MetaDefender Kiosk and not wait until the end of a release's support cycle.

Current versions incorporate state-of-the-art features and necessary bug fixes, and are freely available for all license holders to download.

To upgrade, follow these steps:

1. Browse Release Notes for details on the latest MetaDefender Kiosk version release.
2. Visit My OPSWAT to download a new version under the relevant package license.

Visit Installation Documentation for step-by-step instructions on how to install the MetaDefender Kiosk solution.

MetaDefender Kiosk Support Lifecycles:

Release number	Release date	End-of-life date
4.7.3	30 Dec 2024	
4.7.2	04 Nov 2024	30 Jun 2026
4.7.1	24 Sep 2024	04 May 2026
4.7.0	29 Jul 2024	24 Mar 2026
4.6.8	16 May 2024	29 Jan 2026
4.6.7	17 Apr 2024	16 Nov 2025
4.6.6	26 Mar 2024	17 Oct 2025
4.6.5	5 Jan 2024	26 Sep 2025
4.6.4	14 Nov 2023	05 Jul 2025
4.6.3	31 Aug 2023	14 May 2025
4.6.2	26 Jun 2023	03 Mar 2025
4.6.1	8 May 2023	26 Dec 2024

Please Note:
The versions not mentioned on this page are no longer supported.

Support:
For any issues or queries regarding supported versions of our **MetaDefender Kiosk** solution, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

How do I set up and use the Media Manifest feature in MetaDefender Kiosk?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows systems

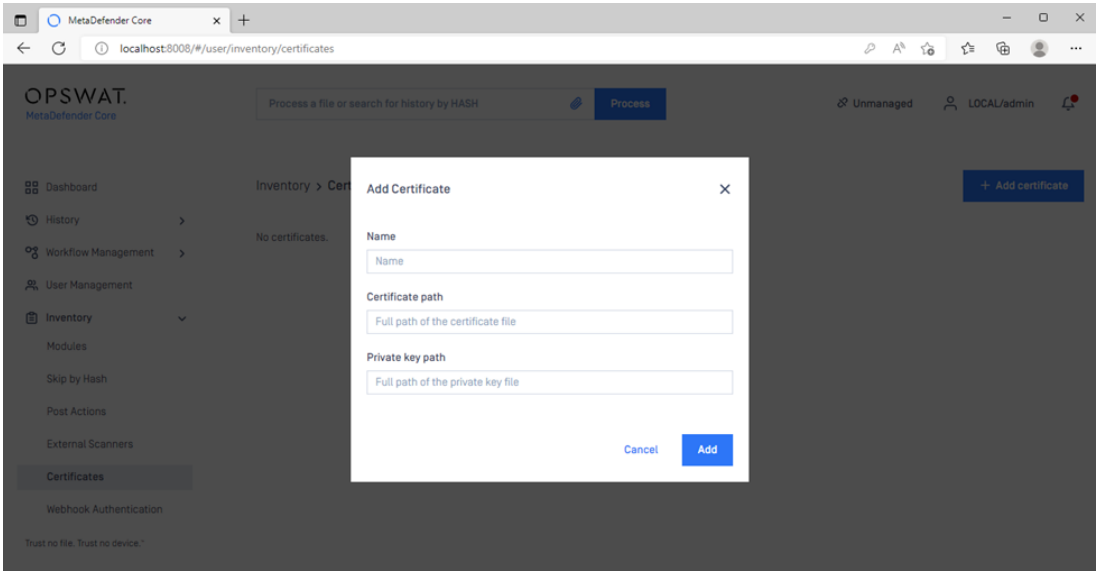
Pro Tip:
A Media Manifest is a digitally signed file that lists the hashes of all the files that were cleaned and approved by MetaDefender Kiosk during its session.

This article covers the entire course of Media Manifest setup and usage in MetaDefender Kiosk, including:

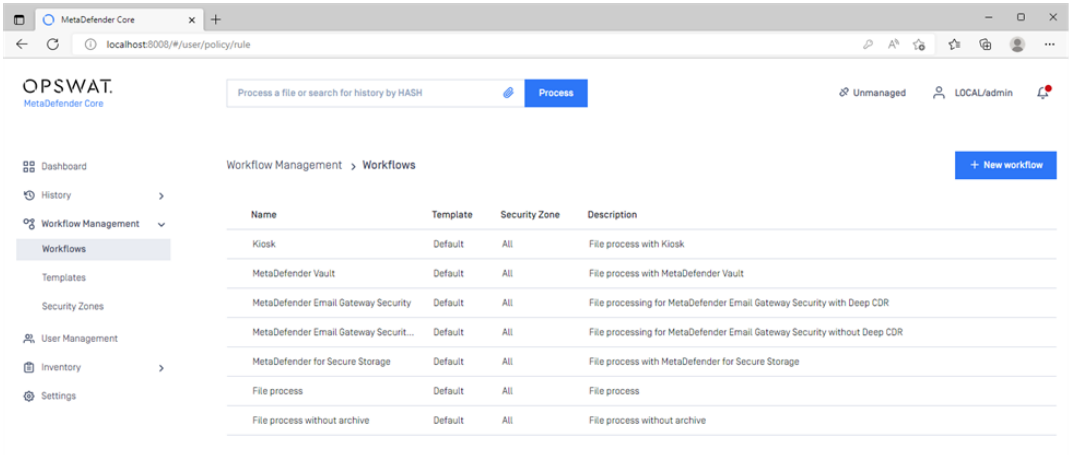
1. Setting up the certificate for digital signing (via MetaDefender Core)
2. Enabling the Media Manifest feature (via MetaDefender Kiosk)
3. Utilizing Media Manifest (via the OPSWAT Media Validation Agent)
4. Media validation flow.

Setting up the certificate for digital signing (via MetaDefender Core)

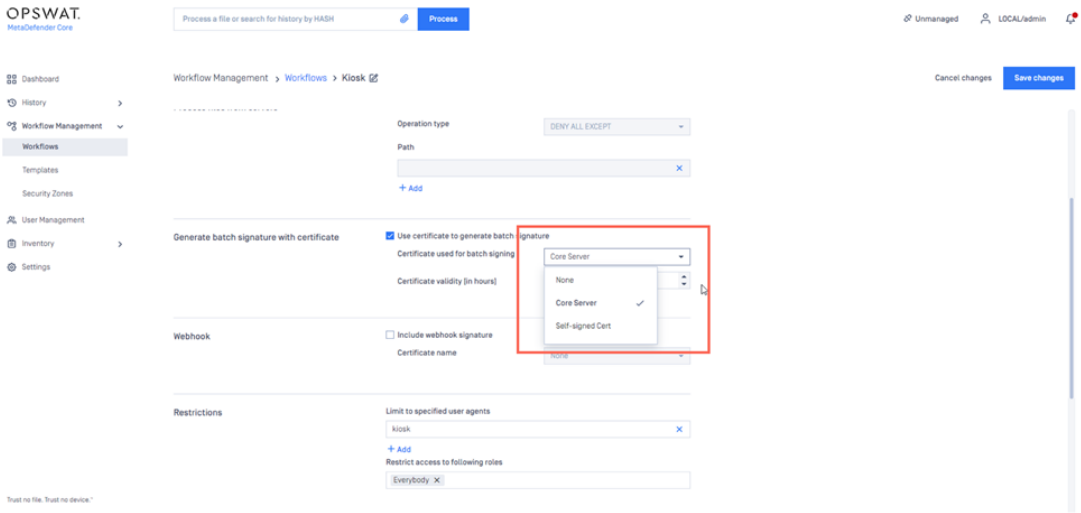
1. Go to your **MetaDefender Core Management Console>Inventory>Certificates** to add a certificate that will be used for digital signing.



2. For more information on adding certificates, please Read This and This.
3. Now, go to **Core Management Console>Workflow Management>Workflows** to open the appropriate workflow.

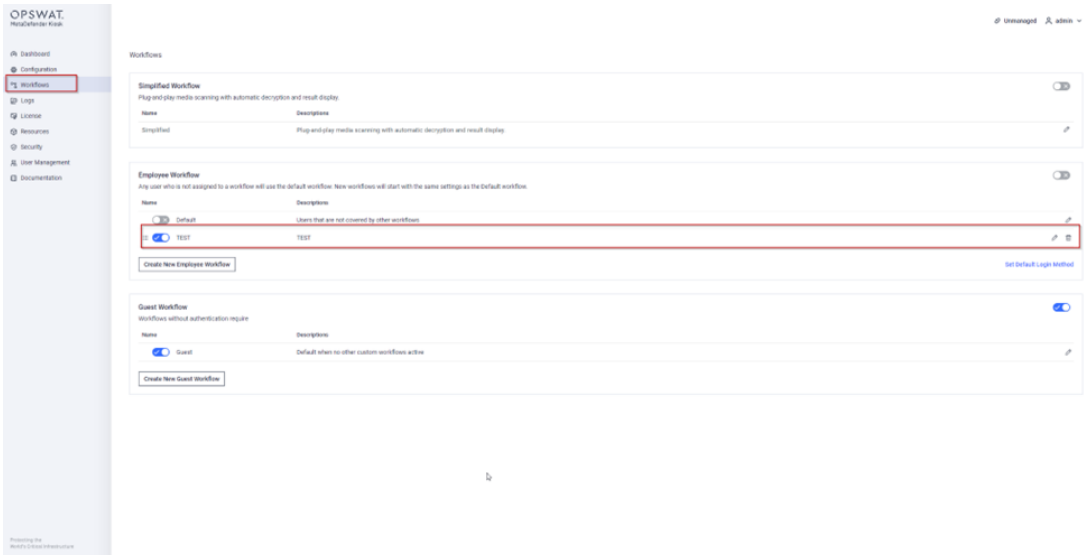


4. Assign the certificate you created to the workflow, as illustrated in the screenshot below.

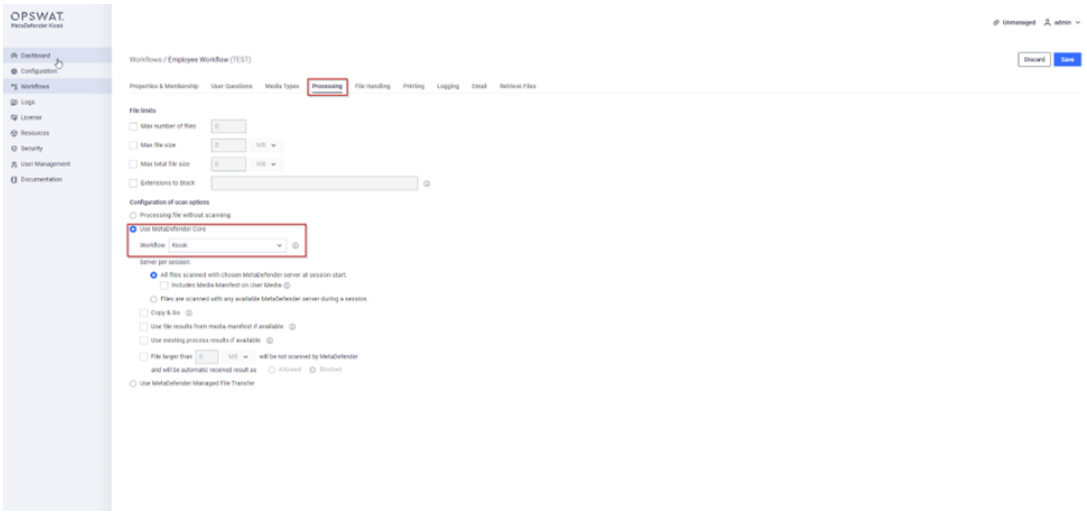


Enabling the Media Manifest feature (via MetaDefender Kiosk)

1. Enable Media Manifest in Kiosk by going to the **MetaDefender Kiosk Management Console>Workflows**, then clicking the edit icon on the appropriate workflow, as highlighted in the screenshot below.



2. Now, go to the **Processing** section to assign the appropriate workflow rule (i.e. the workflow configured in the Core Management Console) and select the **Include Media Manifest** option, as illustrated below.

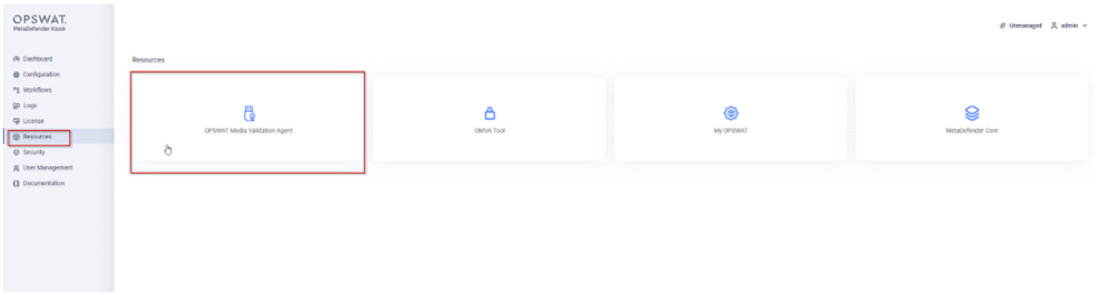


3. Finally, click **Apply** to activate your selections.

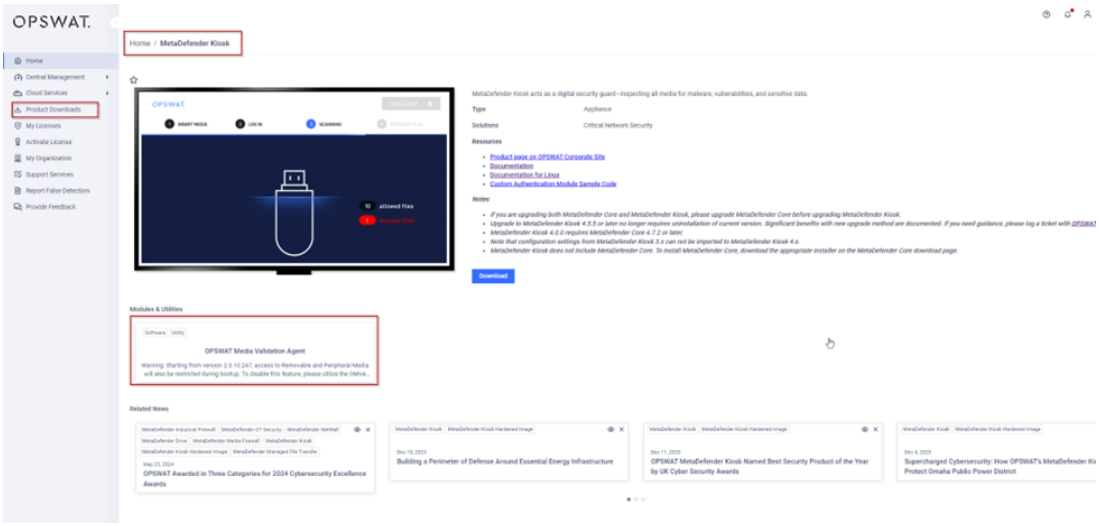
Utilizing Media Manifest (via the OPSWAT Media Validation

Agent)

1. Go to **MetaDefender Kiosk Management Console>Resources** to download the OMVA, as illustrated in the screenshot below.



2. Alternatively, go to the **Opswat Portal>Products>Endpoint Clients** section to download the OMVA, as shown below.



3. Follow the **Setup Wizard** to install the agent on the appropriate endpoint. Please Read This for more information.

4. Finally, install the **Public Key** of your certificate to the endpoint.

Media validation flow

1. In order to process files from external media, Kiosk sends them to the associated MetaDefender Core instance.
2. MetaDefender Core then generates a manifest listing all the files that it processed during the Kiosk session, signed with a digital certificate.
3. The Kiosk then downloads this manifest to the processed media, along with the processed files.
4. This media can now be inserted into any endpoint that has the OPSWAT Media Validation Agent installed.
5. The OMVA will then check the hashes of the files in the media manifest against the files physically located on the media.
6. All Media devices will be blocked if any discrepancies are noticed.

Support:
If you are having difficulty **Setting Up the Media Manifest Feature in MetaDefender Kiosk**, please follow these instructions on How To Create a Support Package, before logging a Support Case with the OPSWAT team.

How do I use the Copy & Go feature in MetaDefender Kiosk?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows or Linux systems.

Copy & Go is a time-saving feature designed to streamline the Kiosk experience by allowing users to copy their files to the Kiosk before scanning.

This means users can remove their portable media much sooner than the traditional scan, which requires that the media remain connected to the Kiosk. Following the scan, all copied files will be deleted from the Kiosk system.

Pro Tip:
There are benefits and drawbacks to enabling the Copy & Go feature, and it is only appropriate and effective for certain use cases.

Therefore, please review this article in-full before enabling the Kiosk Copy & Go feature.

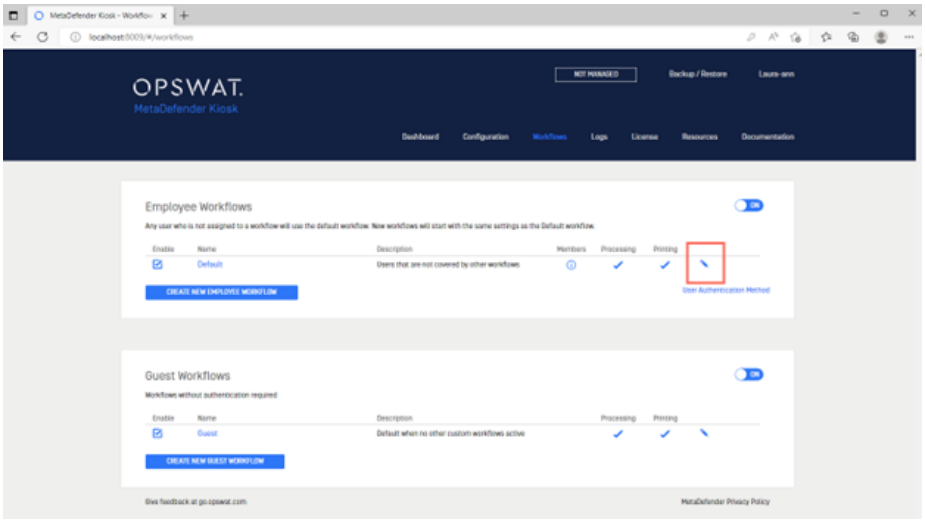
When to use Copy & Go

Copy & Go is ideal for users who need a faster experience at the Kiosk, such as when users need to scan hundreds or thousands of files, and copying files would be significantly faster than standing and waiting at the Kiosk for the scan to finish.

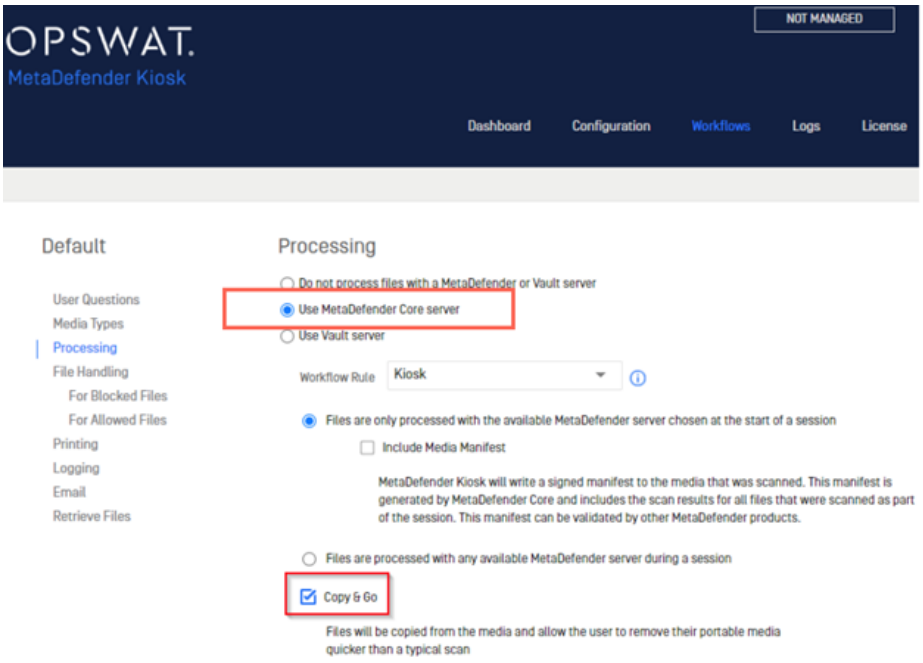
On the other hand, Copy & Go is *not* recommended for users scanning a small number of files, as the overall time saved by copying would be negligible.

How to enable Copy & Go

- Go to your **Kiosk Management Console>Workflows**, then click the *edit* icon on the appropriate workflow, as highlighted in the screenshot below:



- Go to the Processing section, as illustrated below, ensuring that both the **Use Core Server** and the **Copy & Go** options are selected.



- Finally click **Apply** to save your settings.

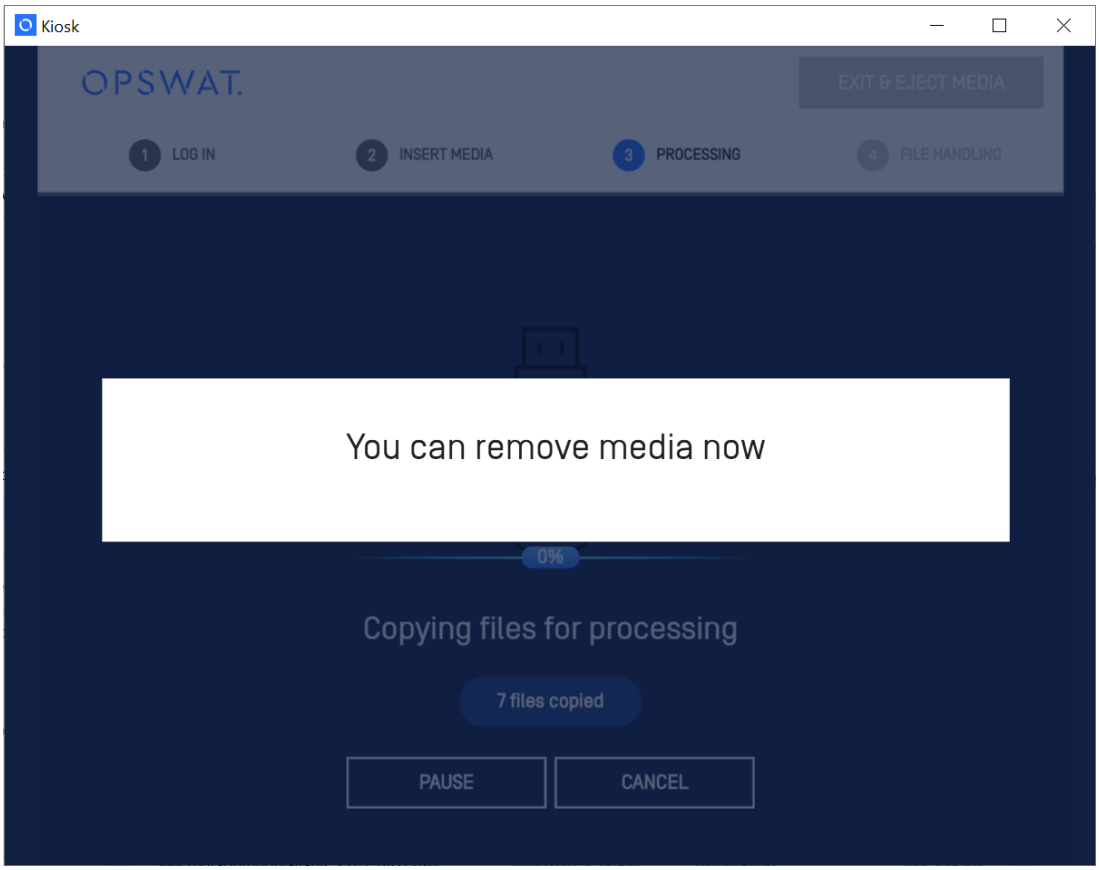
> **Please Note:**
> Enabling the Copy & Go feature will automatically disable any previously enabled **Workflow File Handling** option that copies or moves files to the original media.

The standard Copy & Go flow

The standard process flow for Copy & Go runs as follows:

1. The user logs into the Kiosk and follows the prompts to insert their media.
2. The user then selects their files for scanning
3. The files are automatically copied to the Kiosk
4. A pop-up prompts the user to remove their media, which still contains the original files
5. The copied files are scanned by Kiosk
6. A scan report is produced
7. Depending on settings, processed files may be copied to the associated MetaDefender Managed File Transfer or to another specified location at this point
8. The copied and scanned files are then deleted from the MetaDefender Kiosk.

The Copy & Go enabled Kiosk process is similar to the standard Kiosk process, except for steps 3. and 4. above, that allow the user to remove their media early and then go on their way.



The Workflow will then continue to scan the files and produce a report. With Copy&Go, some actions that need human response, like email address input, password for encrypted media,... are moved prior to scanning so that user can prepare in advance; some actions that Kiosk can select a default option, like Print or Skip, Copy or Skip,... are waiting for user inputs within 3 seconds or default actions (Print, Copy...) will be proceeded.

Warnings

- **Hard drive space**
  - The Copy & Go feature will copy all of the selected files to the Kiosk system.
  - Therefore, the amount of free hard drive space should be closely monitored when using Copy & Go, to ensure the Kiosk system does not run out of space.
- **Malicious files**
  - Copy & Go may open up the Kiosk system to infection in the event that malicious files exist on the media, which then get copied to the Kiosk system.
- **Disabled Workflow features**
  - Any Workflow option that copies files back to the original media will be automatically disabled when Copy & Go is enabled.
  - This includes File Remediation options that remediate the files on the original media or copy remediated versions of the files back to the original media after scanning.
- **Media should still be considered UNSAFE when Copy & Go is enabled**
  - Copy & Go copies files from the original media to the Kiosk system and then ejects the original media unchanged.
  - The removable media should therefore still be treated as unsafe and unscanned.

Support:
If you have any difficulty **Using MetaDefender Kiosk's Copy & Go Feature**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

What are the running processes of MetaDefender Kiosk?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows systems.

Looking over task manager you will be able to see:

- Kiosk Custom Authentication Handler - omdCAMHandler.exe
- MetaDefender Kiosk Service - MetadefenderSVC.exe
- MetaDefender WatchDog - omsMD4MHelper.exe
- Metascan DB Controller - omsDBCtrller.exe
- Metascan Post Action Center - omsPACenter.exe
- MongoDB - mongod.exe

Support:
If you have any issue regarding the **Expected Running Processes of MetaDefender Kiosk**, please follow these instructions on How To Create a Support Package, before logging a Support Case with the OPSWAT team.

What does Remediated File mean in MetaDefender Kiosk?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows or Linux systems.

A remediated file is any file that has been processed by MetaDefender Kiosk to remove hidden (and possibly malicious) content, including embedded objects and potential exploits or redact sensitive information, while preserving the visible contents of the file.

The remediated file will maintain its original file format and extension, unless the Kiosk (and MetaDefender Core) has been explicitly set up to convert suspicious files to another format as part of the sanitization process.

For example, a remediated PDF will maintain the PDF format and extension, and will be accessible by a PDF reader.

Some of the actions performed as part of remediation include:

Sanitization

- Removal of all attachments and document action
- Removal of all annotations
- Removal of JavaScript from other scripts within the document
- Making any form fields present in PDF files uneditable and inaccessible, so that the user cannot update values within the file
- Removal of all hyperlinks.

Redaction

- Redact/Substitution sensitive information
- Watermark files

MetaDefender Kiosk supports remediation for many of the most common document file types. Should you have a requirement for a file type that is not currently supported by the Kiosk, please follow the instructions below to contact support.

Although we cannot make any commitments regarding inclusion of a suggested file type, we are always striving to include new, commonly used file types to better meet the needs of our customers.

Support:
If you have any issue regarding the **File Remediation in MetaDefender Kiosk**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

What is the difference between the Format, 1-Pass, 3-Pass, and 7-Pass options in the MetaDefender Kiosk wipe functionality?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows systems.

Pro Tip:
If thus configured, MetaDefender Kiosk will, after scanning and sanitizing files as part of its session workflow, wipe the user's original media before copying the remediated files to it.

There are 3 areas where wipe/format can be configured and each serve their own purpose:

- Configuration → Wipe Method

For enabling the Wipe session type to wipe\format inserted media; can be multiple media

- Workflows → <workflow> → File Handling → For <Blocked, Allowed> Files → Copy to → User Media → Wipe user media before copying

For enabling the ability to wipe the destination media before copying files over

- Workflows → <workflow> → File Handling → For Allowed Files → Wipe and Copy to Original Media

For enabling the ability to clear out the scanned media's content and restore back only the allowed files

This functionality is enabled as an added security measure intended to leave no trace of the original, possibly malicious or corrupt files on the user's removable media.

Format, **1-pass**, **3-pass** and **7-pass** describe various media-wipe processes, with respectively increasing levels of effectiveness.

The more effective the method, the more secure the method, and the more unlikely it is that any of the original data will be recoverable from the media post-wipe.

Format is the fastest (and least effective) of these methods, as it simply removes references to the files on the drive without physically overwriting the files themselves.

The 1, 3 and 7 pass wipe options physically overwrite all data stored on the drive with a range of differing algorithms, making retrieval of the original data much more unlikely.

The wipe/overwrite options are the only way to fully erase the contents of a drive or removable media.

Pro Tip:
The numbers **1**, **3** and **7** refer to the number of passes made during the wiping process. It follows that choosing the 7-pass option will be the most effective way of erasing your drive.

The United States Department of Defense recommends using a 7-pass wipe to clean media.

For all wipe options, OPSWAT conducts a low-level (meaning sector by sector) wipe of the media, which is the slower and more rigorous method of data erasure.

WARNING:
Enabling the wipe feature will completely erase and reformat all information and data on your device. This includes the partition table and master boot record, along with any file system information.

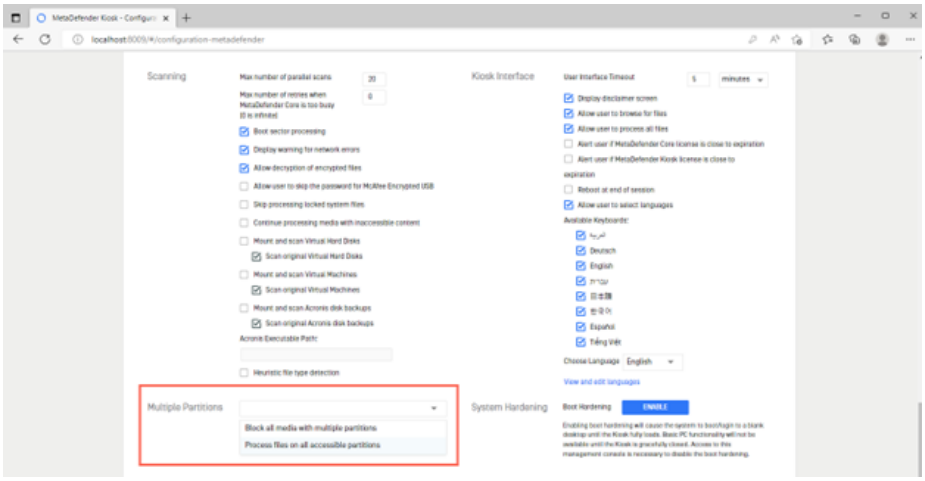
Algorithm Details

Num. of Passes	Algorithm Steps in Order	Security Standard
1	1. Pseudorandom	• British HMG Infosec Standard 5, Baseline Standard • Australian Government ICT Security Manual 2014 - Controls
3	1. All 1's 2. All 0's 3. Pseudorandom	• U.S. DoD Unclassified Computer Hard Drive Disposition* • U.S. Air Force System Security Instruction 5020** • U.S. Navy Staff Office Publication NAVSO P-5239-26 • British HMG Infosec Standard 5, Enhanced Standard *We select 0xFF and 0x00 (reverse of standard), then pseudorandom data instead of a fixed character for our final pass
7	1. All 1's 2. All 0's 3. Pseudorandom 4. Pseudorandom 5. Pseudorandom 6. Pseudorandom 7. Pseudorandom	• Bruce Schneier's Algorithm: Applied Cryptography, ISBN 0-471-12845-7

Encrypted or private partitions

If a device has an encrypted or private partition, MetaDefender Kiosk may not be able to read it. For more information, please read Known Limitations of MetaDefender Kiosk.

Media with non-primary encrypted partitions can be blocked via the **MetaDefender Kiosk Management Console>Configuration>Advanced Configuration>Multiple Partitions**, as illustrated in the following screenshot.

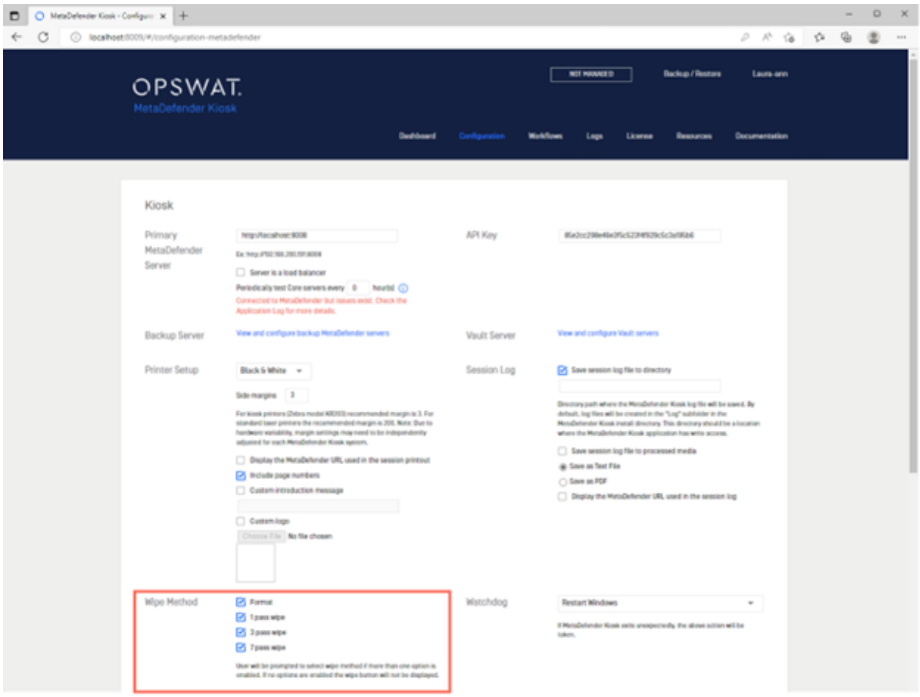


The OPSWAT team highly recommends using the wipe functionality so that, should a drive contain any non-readable encrypted or private partitions, these will be thoroughly wiped along with any malicious or threatening files they contain.

How to configure the Kiosk Media

Wipe feature

To configure Kiosk's wipe functionality, go to the **MetaDefender Kiosk Management Console>Configuration>Wipe Method** and select the appropriate options, as illustrated in the screenshot below.



Support:
If you have any queries regarding the **MetaDefender Kiosk's Media Wipe Functionality**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

What is the frequency of MetaDefender Kiosk's antivirus signature/definition updates?

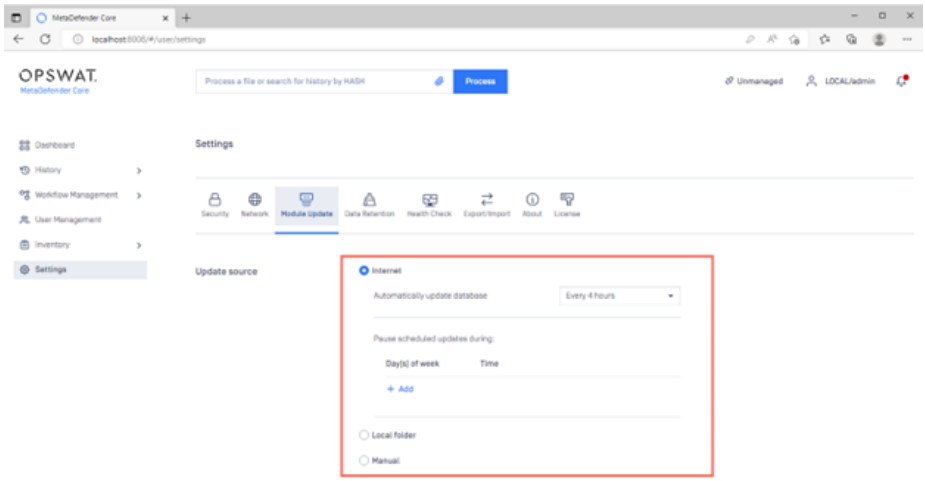
Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases.

MetaDefender Kiosk relies on its underlying MetaDefender Core server to manage antivirus engine signature/definition updates.

The frequency of these updates is configured via the MetaDefender Core server to which the Kiosk is connected, and is also dependent on the frequency with which AV engine vendors release their updates.

So, the two parameters that determine the frequency of signature/definition updates are:

- The configuration setting on your MetaDefender Core installation which specifies the time interval between system checks and applying new updates. Go to your **MetaDefender Core Management Console>Settings>Module Update** to make changes, as highlighted in the image below.



- The frequency with which each antivirus vendor releases an update. Most vendors release definitions at least once per day, while many have multiple daily releases. Some vendors release updates over weekends, while others do not. Due to the high frequency of signature/definition updates, it is recommended that you allow for updates at least once per day.

Please Note:
If you use OPSWAT's online update mechanism to auto-apply updates (i.e. via direct internet connection), you can configure the update interval to suit your needs.

The default setting for MetaDefender Core V4 and above is once every 4 hours.

If you are using the manual update option (i.e. not automated, offline updates), the frequency is controlled by how often you manually download and apply the offline update packages from My OPSWAT.

Support:
If you have any difficulty **Configuring and Applying MetaDefender Kiosk and Core's Regular AV Engine Signature/Definition Updates**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

How to completely uninstall MetaDefender Kiosk

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows system.

There is no mechanism to retrieve kiosk password if admin user forgot the login password for Kiosk management console except for a complete uninstallation.

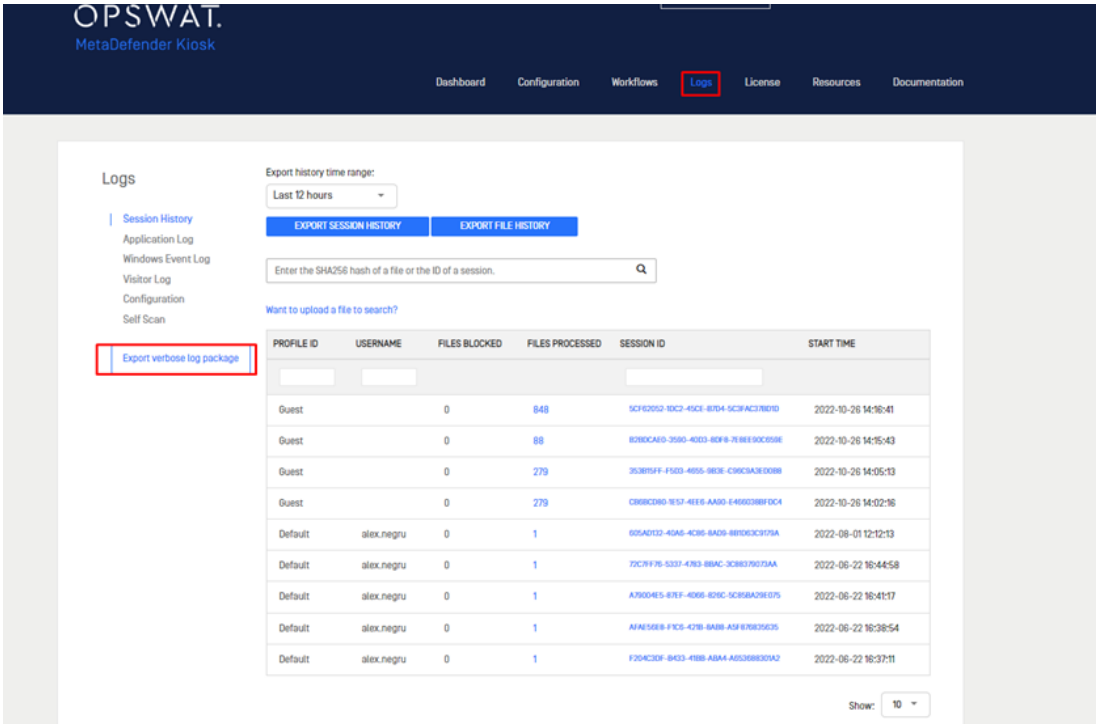
1. Uninstall Kiosk from control panel
2. Navigate to **C:\ProgramData\OPSWAT\Metadefender**
3. Remove **KioskBackup** and **kiosk_config.zip**

Note: The folder KioskBackup available from 4.5.5+, and this will completely remove all Kiosk configuration.

Support:
If you have followed all of the steps above but are still unable to **completely uninstall MetaDefender Kiosk**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

How do I create a support package for MetaDefender Kiosk?

In order to create a MetaDefender Kiosk support package users must access the Kiosk console (ex: http://localhost:8009), navigate to the “Logs tab” and select “export verbose logs”.



Once the process is finished, it will result in the creation of a zip archive containing the necessary support logs.

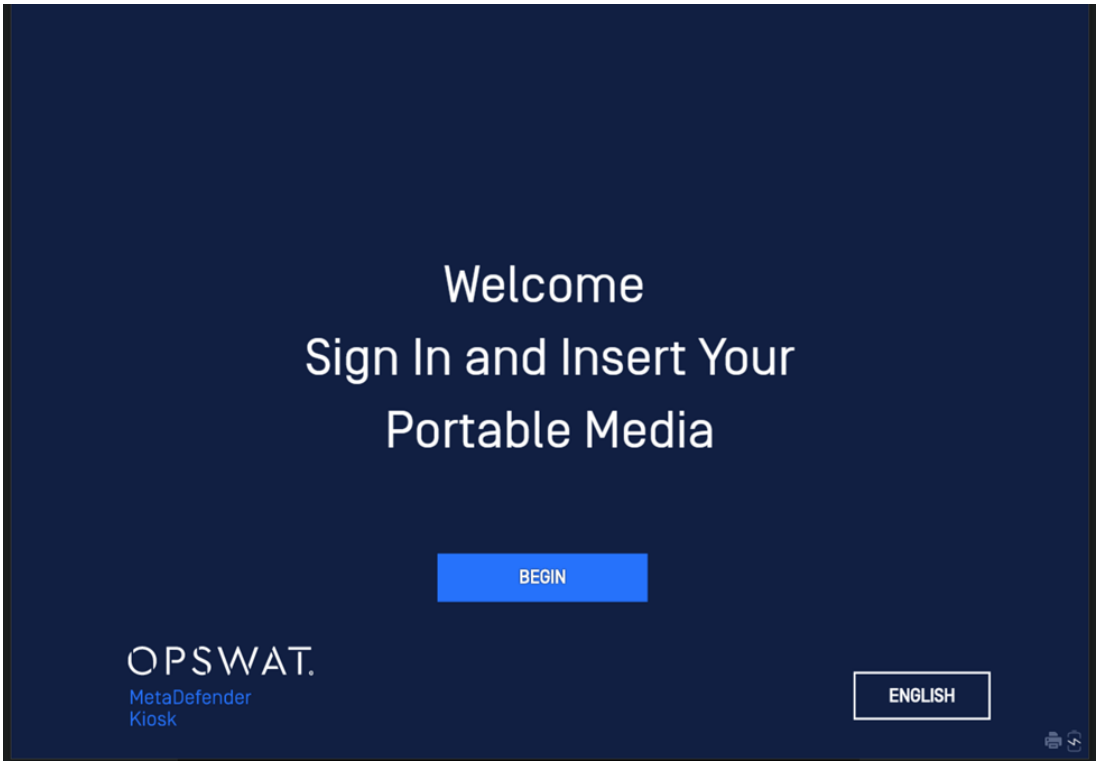
The support package contains the following elements:

- Configuration files.
- Log files.
- System information
- Directory and files information.
- Registry key configuration

Support:
If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

How do I exit the MetaDefender Kiosk user interface?

In order to exit the MetaDefender Kiosk's user interface (if no other restrictions are in place), a simple `Alt+S` is enough to close the user console.

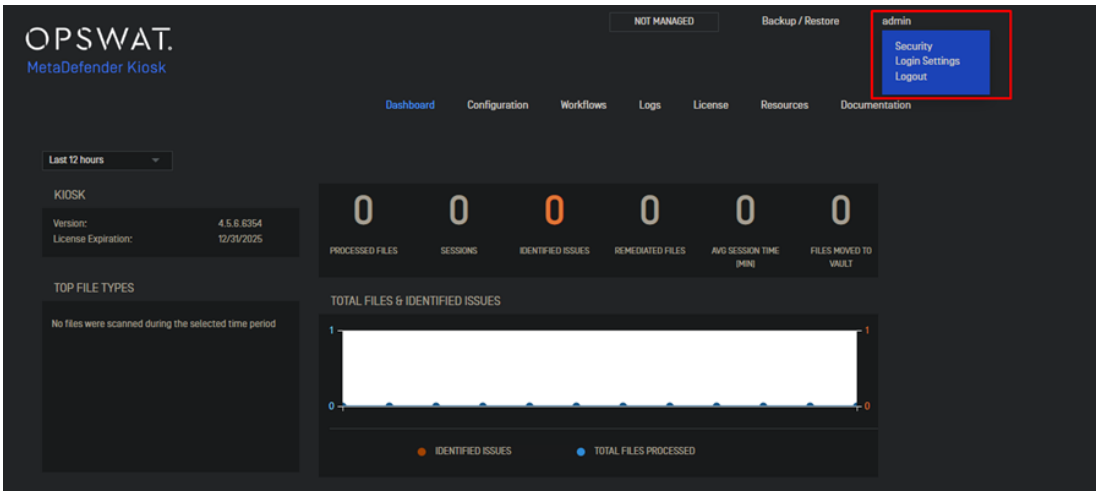


Support:
If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

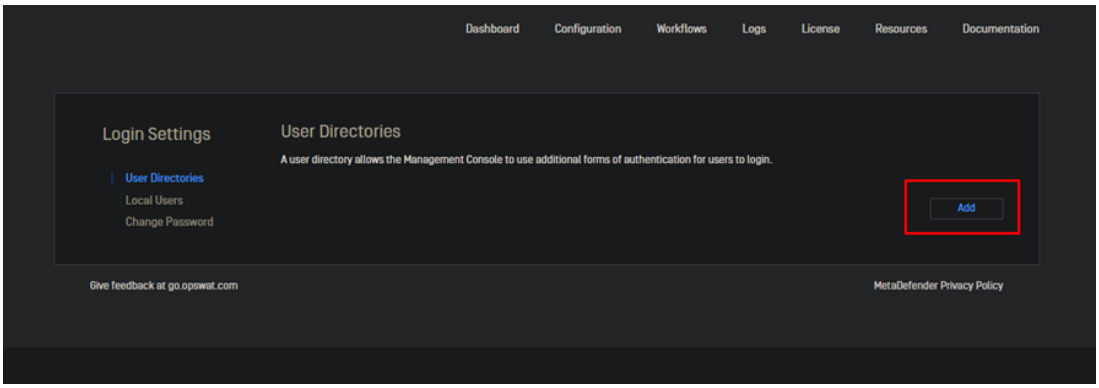
Is Kiosk Active Directory integration possible?

In order to perform a successful Kiosk Active Directory (AD) integration, the following steps must be followed:

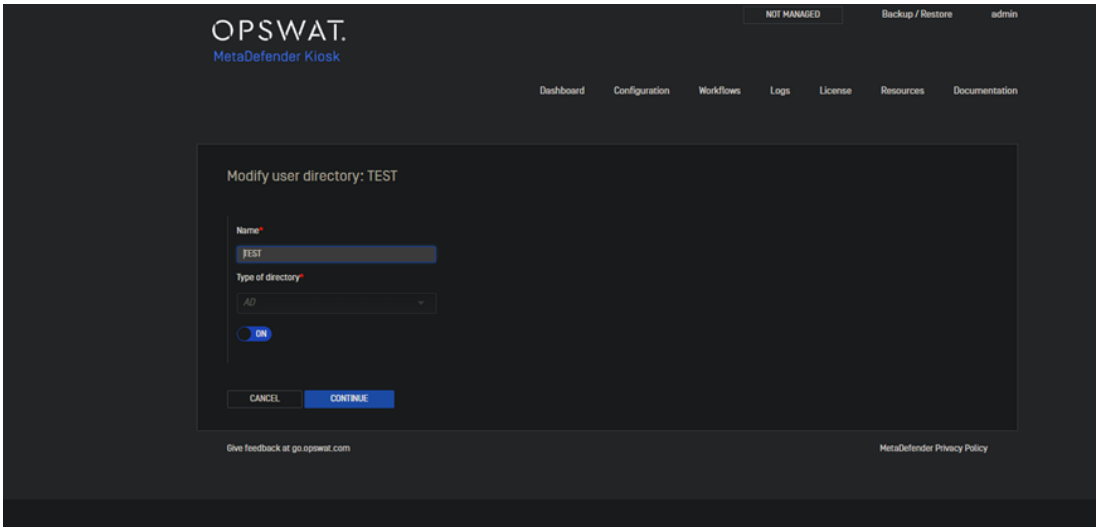
1. Navigate to the Kiosk console to admin (icon)/login settings



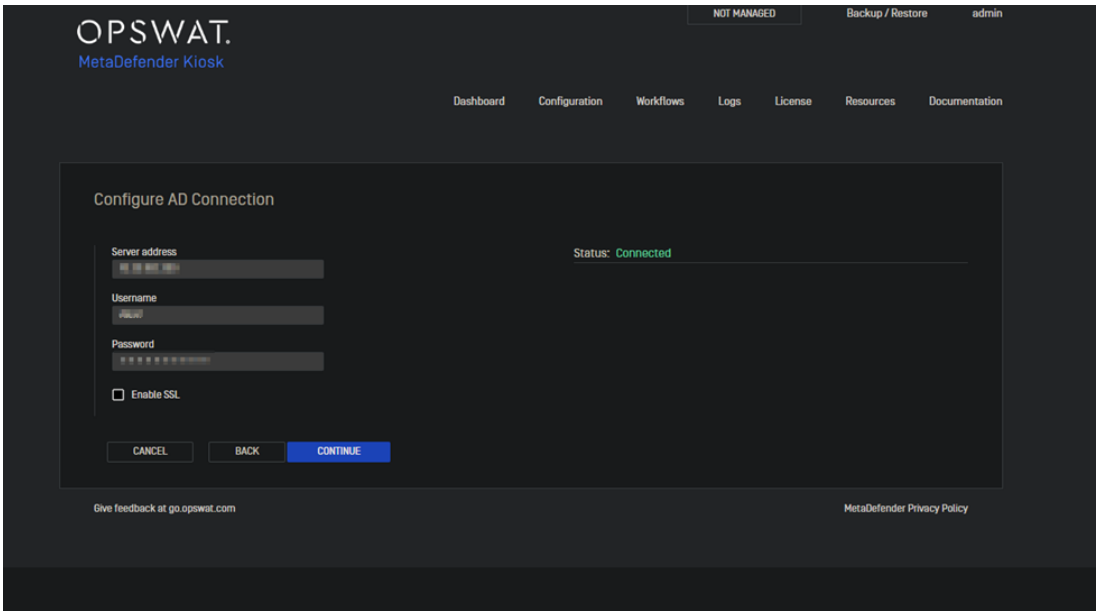
2. Select the User directories tab from the login settings list



3. Select the type of directory from the drop-down list (AD in this situation)

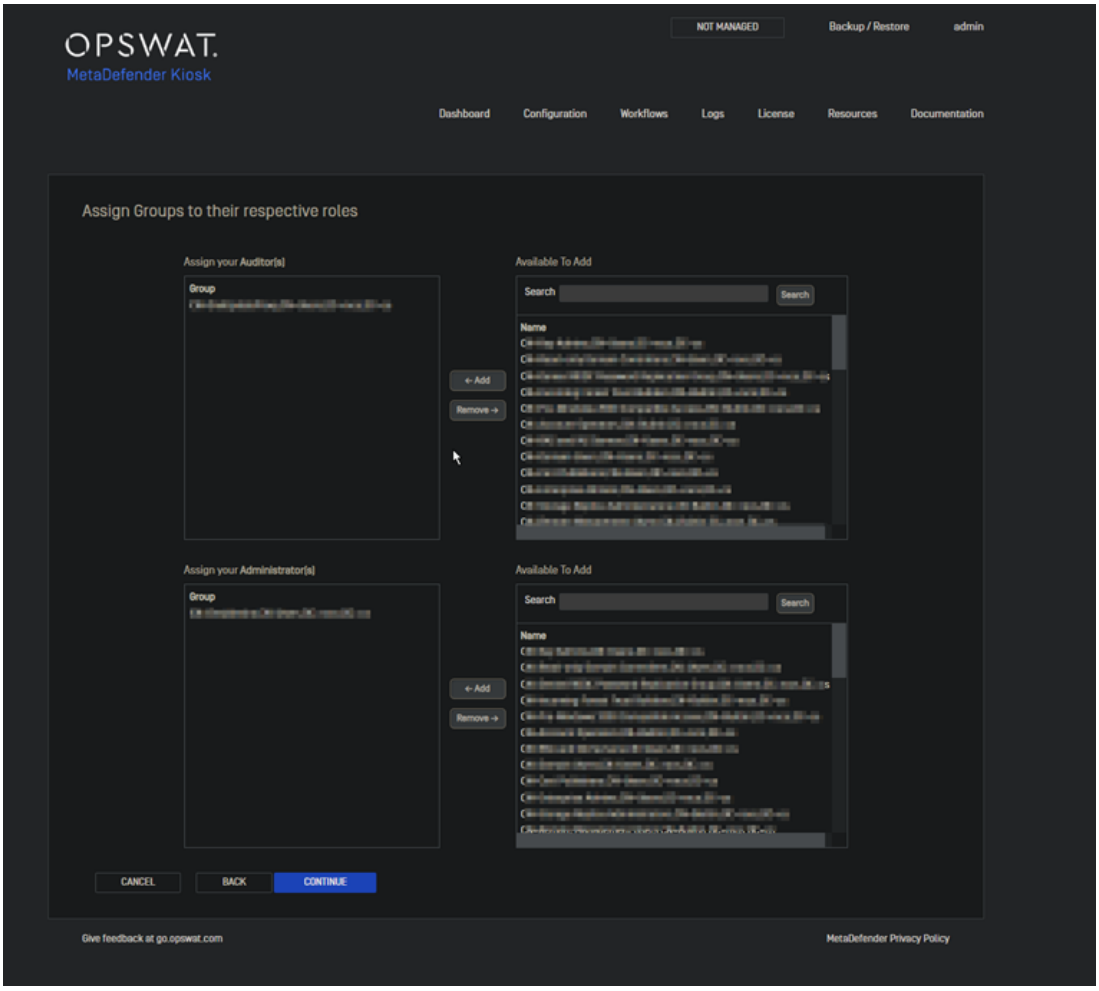


4. Fill in the correct credentials and select the continue tab (make sure the AD server is reachable from the Kiosk side)

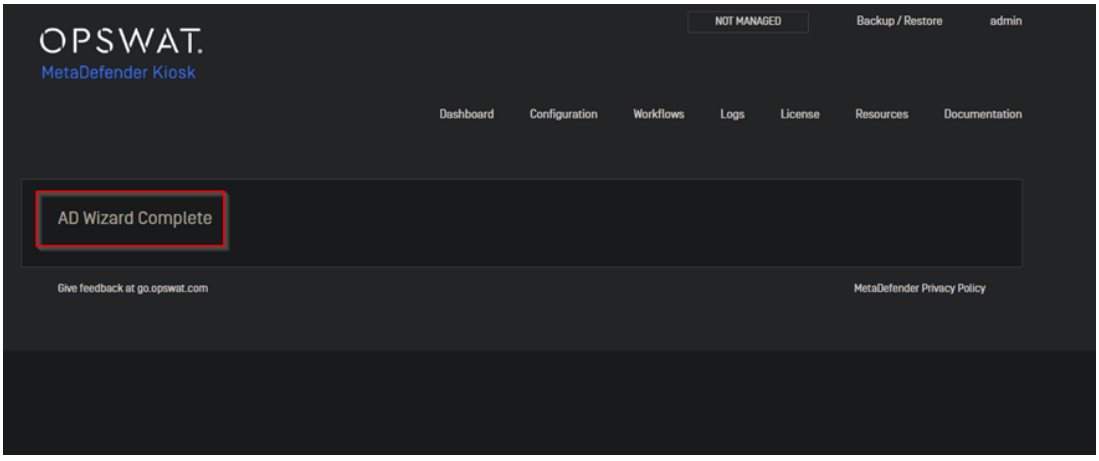


5. The next page allows you to assign users to either the Administrator or Auditor role.

6. The next page allows the configuration of groups to the different roles



7. After completing the steps mentioned above you should get the following confirmation at the final stage of the process.



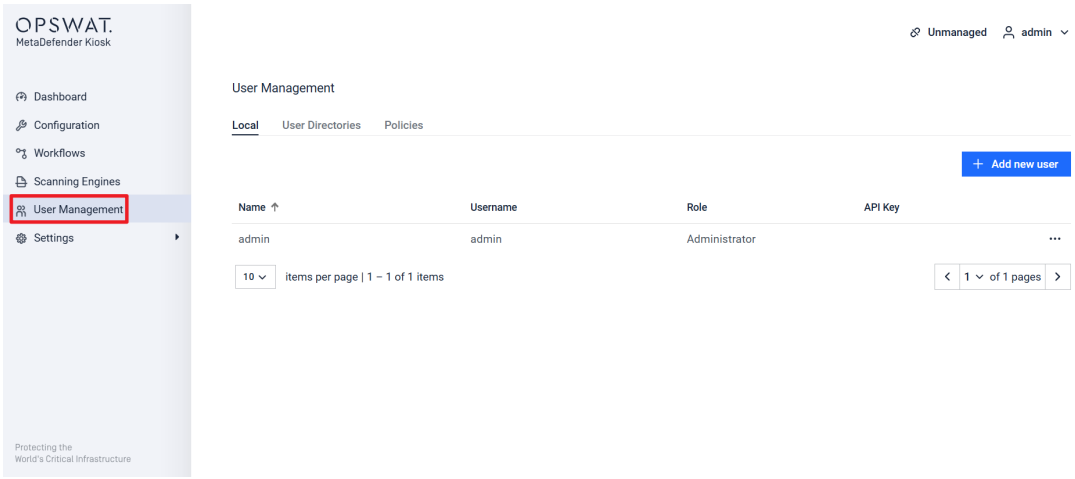
Support:
If **Further Assistance** is required, please proceed to create a support case or chat with our support engineer.

How can I generate an API key on the Kiosk side?

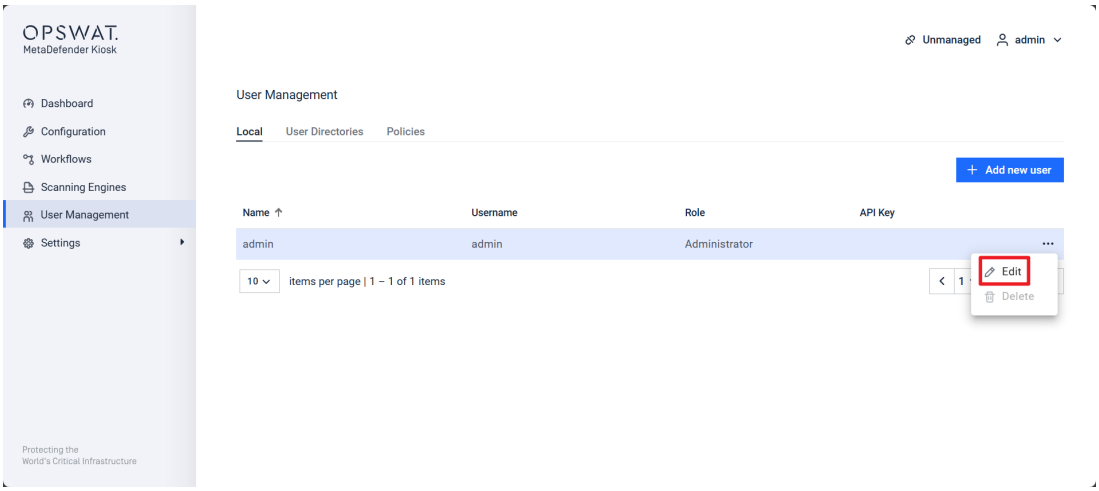
> **Check Your Version:**
> This article applies to all MetaDefender Kiosk releases **after version 4.7.0**, deployed on both Windows and Linux systems.

In order to generate an API key on the KIOSK side (necessary for different OPSWAT product integrations) you will need to take the following steps:

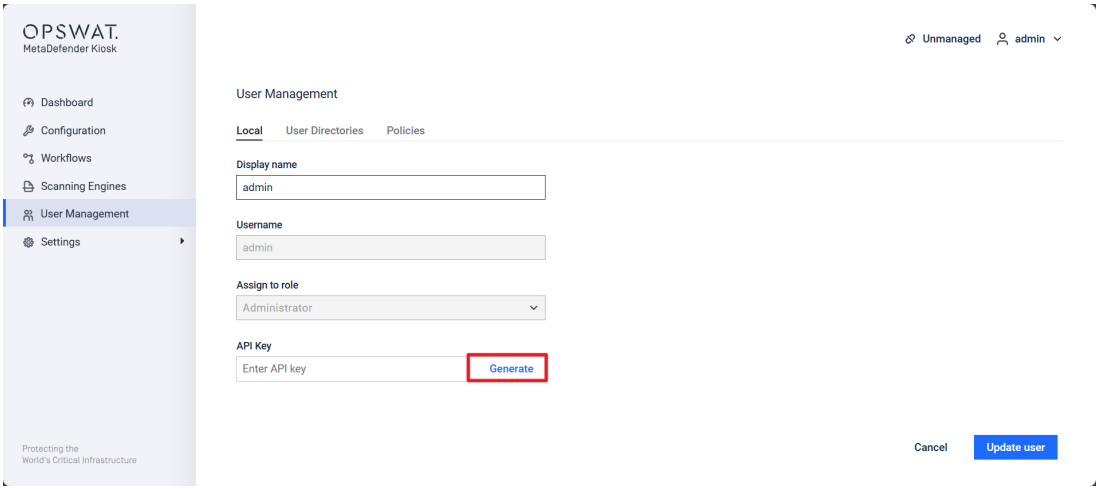
1. Navigate to the **User Management** tab.



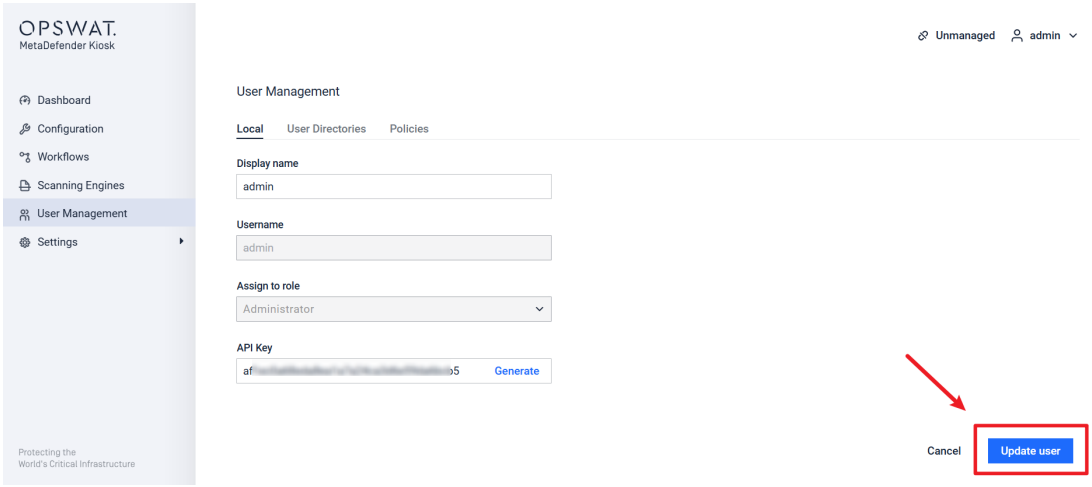
2. Select the user for whom you want to generate an API key, then click the three dots > **Edit**.



3. Click **Generate** to create the API key.



4. After generating the API key, click **Update User** to apply the changes.



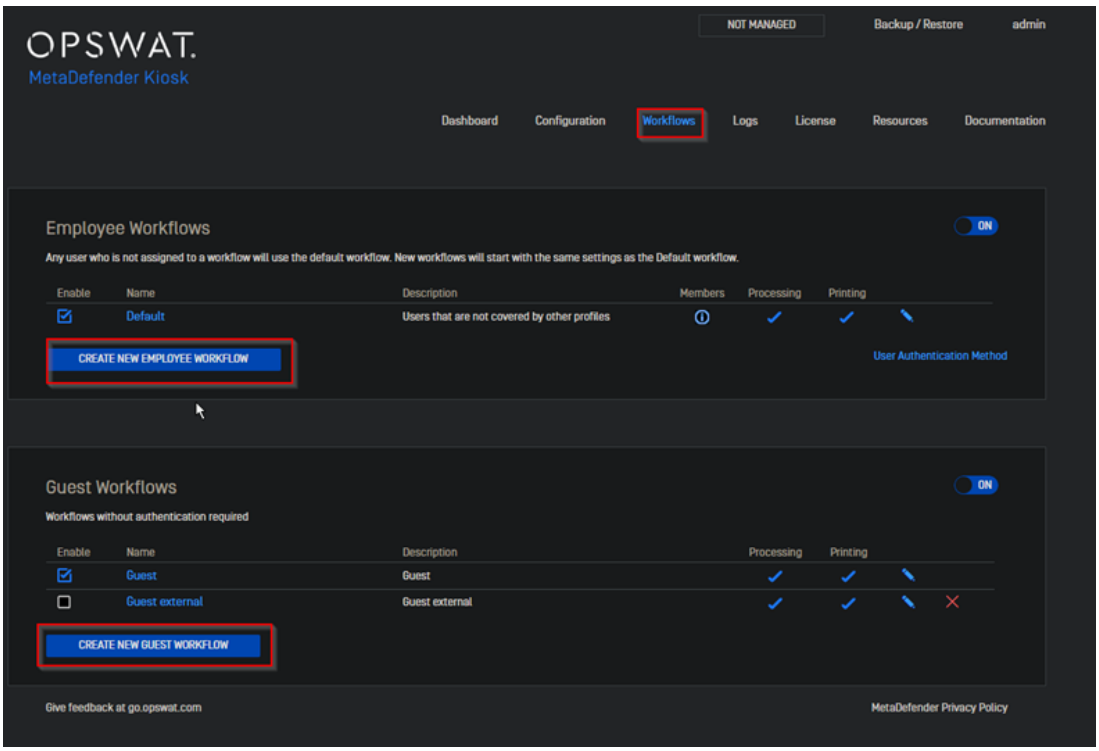
Once all the steps above have been completed the API key will be saved for the selected user and can be used in different integrations. (The API key does not have an expiration date).

Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

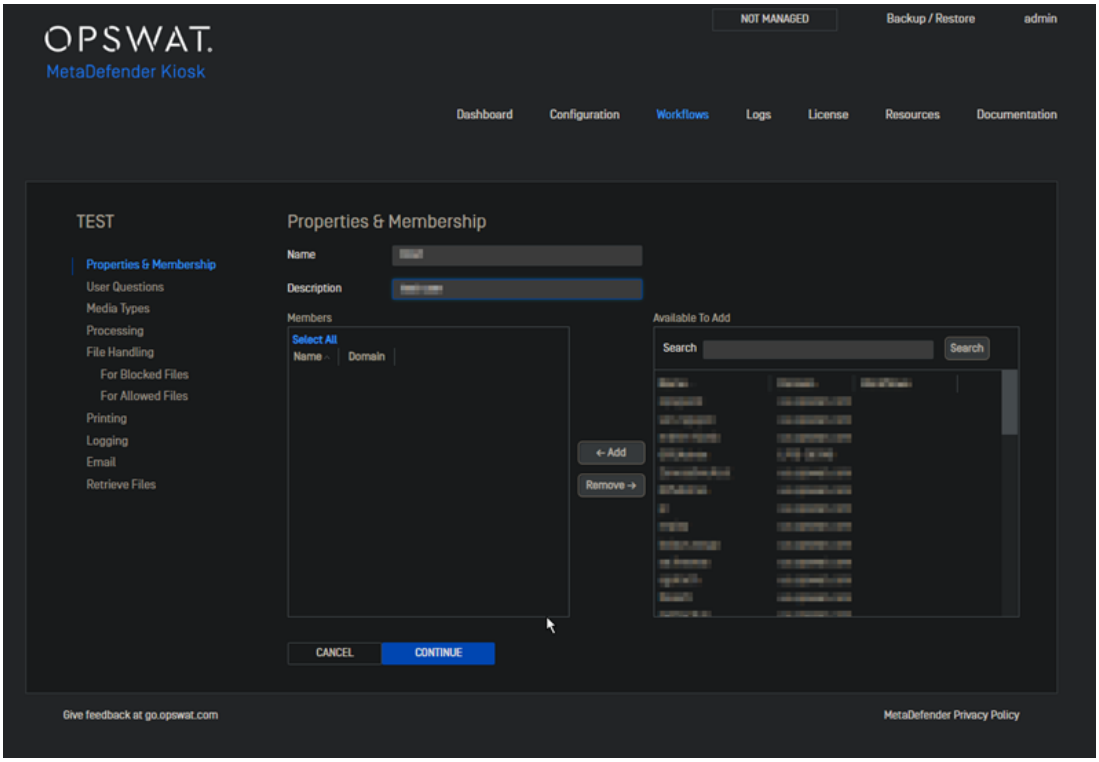
How can I create a new workflow?

Our MetaDefender Kiosk product has some built-in workflows for Employees and Guests after a fresh install, but new workflows can be created by following the steps mentioned below:

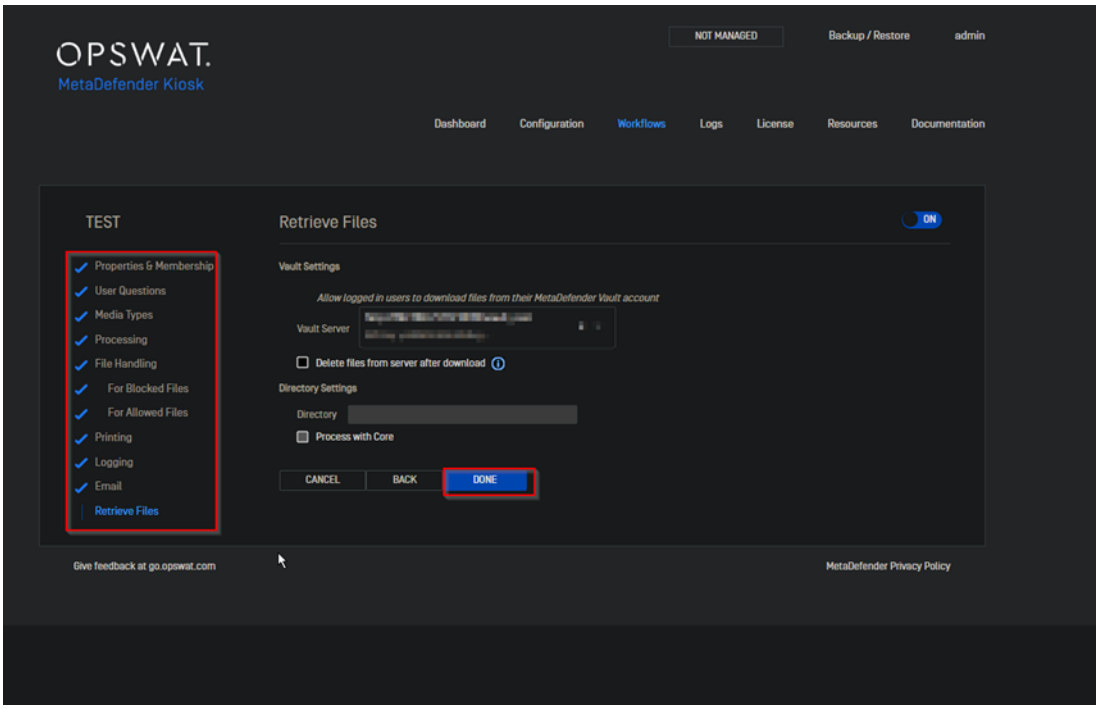
1. Navigate to the workflows tab and select the desired option (Employees or Guests).

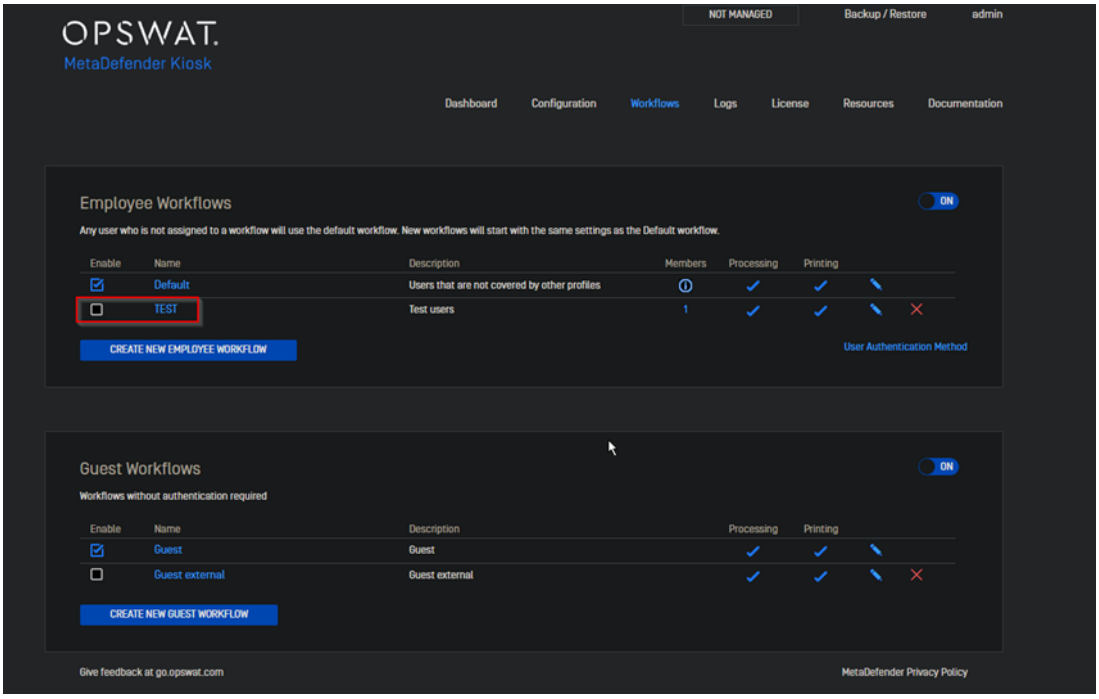


2. Enter the Name for the workflow and description. At this stage, you can also select the users that will be a part of this workflow.



3. After going through all the tabs highlighted in the image below and selecting the Done tab the workflow will be created and should be observable from the console.



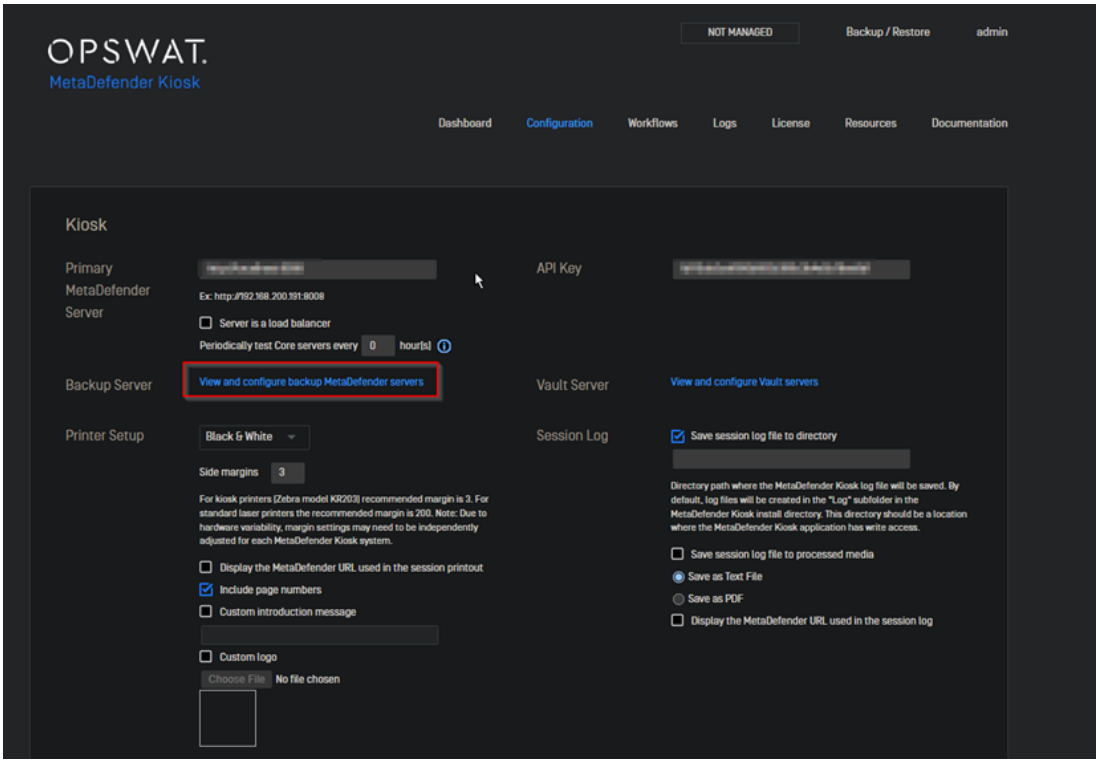


Support:
If **Further Assistance** is required, please proceed to create a support case or chat with our support engineer.

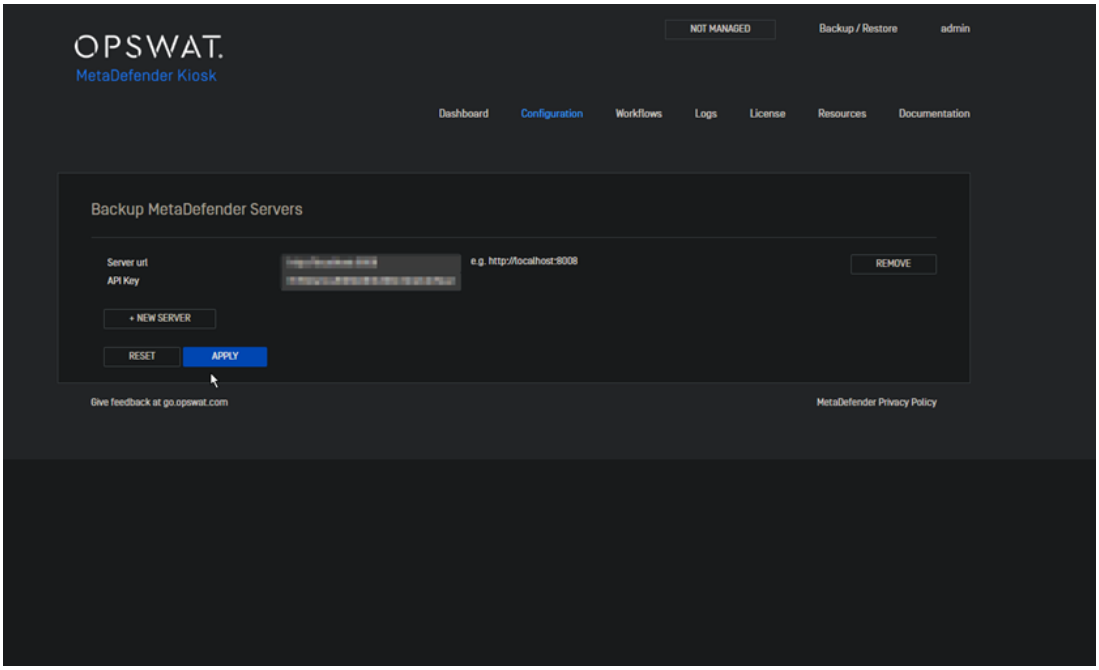
Can I have a backup (Core) server integrated with Kiosk?

In order to set up a back-up Core server from the Kiosk side you will have to take the following steps:

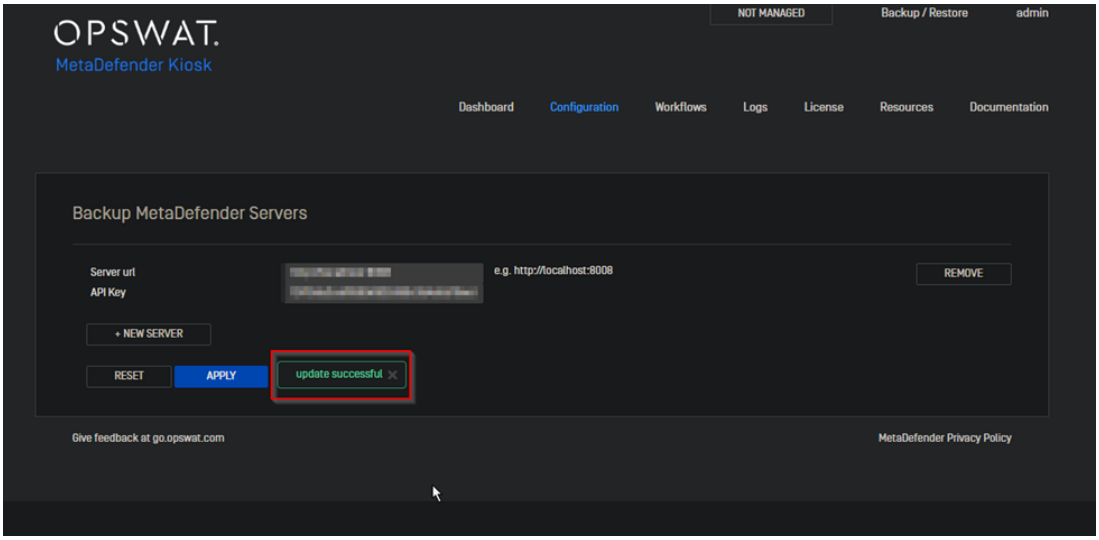
1. Navigate to the Kiosk console/Configuration tab and select “View and configure backup MetaDefender servers”.



2. Select the New Server option and add the necessary information (Server URL and API key from the core deployment).



3. After entering the necessary information, the “update successful” notification should be visible.



Support:
If Further Assistance is required, please proceed to create a support case or chat with our support engineer.

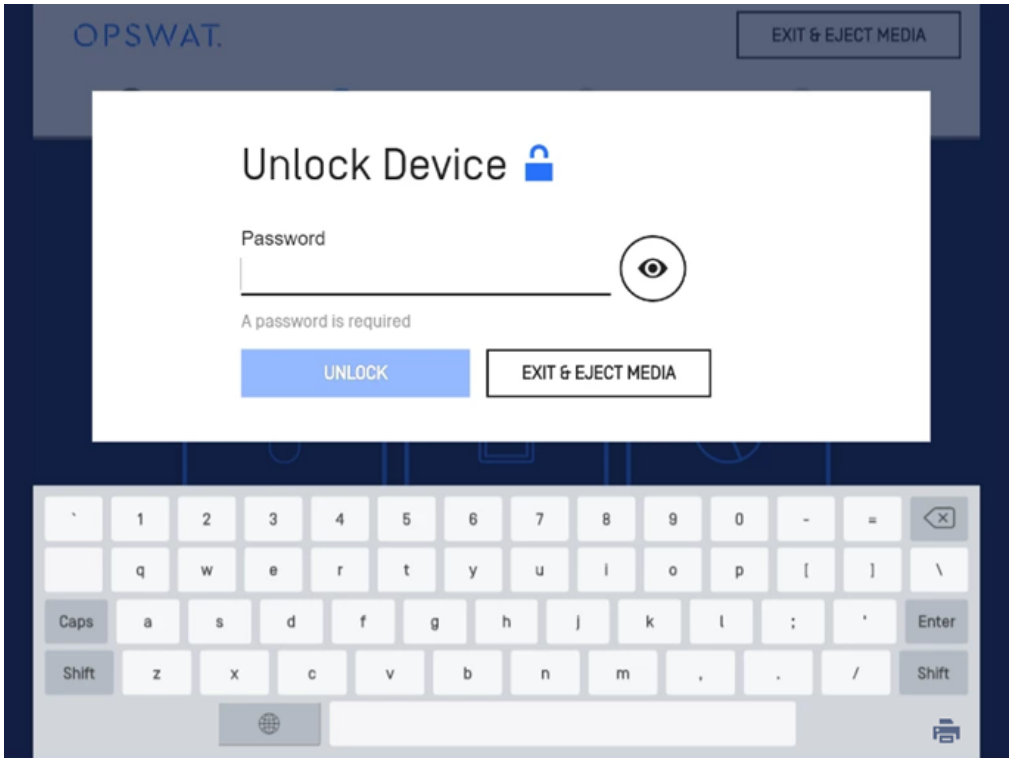
Does MetaDefender Kiosk support encrypted devices?

MetaDefender Kiosk can unlock encrypted USB devices with a given password and process their contents. Kiosk supports the following encrypted USB devices:

Device	Software Version	Firmware Version	Scanning	Wipe	File Handling	Notes
Avira-Iron-Drive I			Yes	No	Yes	
Biocryptodisk-ISPX			Yes			
Buffalo RUF2-HSCT			Yes	Yes	Yes	
Buffalo RUF3-HSL			Yes	Yes	Yes	
DataLocker DL4 FE			Yes	Yes	Yes	
DataLocker K350			Yes	Yes	Yes	
DataLocker Sentry ONE			Yes	Yes	Yes	Versions managed with SafeConsole are also supported
DataLocker Sentry 3 FIPS			Yes	Yes	Yes	
Integral Courier FIPS 197			Yes	Yes	Yes	
Kanguru Defender Elite 30			Yes	Yes	Yes	
Kanguru Defender Elite 200			Yes	Yes	Yes	
Kanguru Defender Elite 300			Yes	Yes	Yes	
Kanguru Defender 2000			Yes	Yes	Yes	
Kanguru Defender 3000			Yes	Yes	Yes	
McAfee Complete Data Protection			Yes	No		
Microsoft BitLocker			Yes	No		

Device	Software Version	Firmware Version	Scanning	Wipe	File Handling	Notes
SanDisk Cruzer Enterprise FIPS Edition			Yes			
SanDisk Cruzer Contour U3 based USB			Yes			
USB Flash Security			Yes			
SDMS MkIII AES Duoulock			Yes		Yes	
Kingston DataTraveler Vault Privacy 3.0			Yes		Yes	
Ironkey - S1000			Yes		Yes	
Ironkey - D250			Yes		Yes	
Ironkey - D300			Yes		Yes	

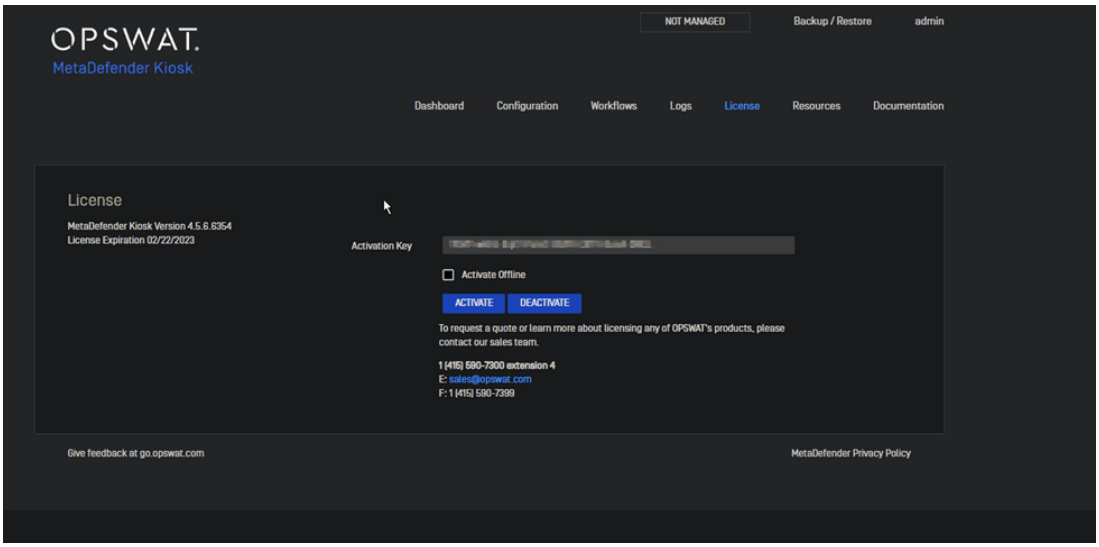
If the device you are trying to scan is encrypted, a prompt to unlock the device is displayed.



Support:
If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

After license renewal does the product activation happen automatically (if the license key is the same)?

In special situations where the renewal process is completed and the license values regarding products and expiration dates are changed (but the license key remains the same), new license information will be updated after the customer uses the same activation key for the Kiosk deployment. The license activation is not done automatically.



For offline environments, users will need to go through the activation steps and generate a new .yml file.

Support:
If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

How do I use Simplified Workflow?

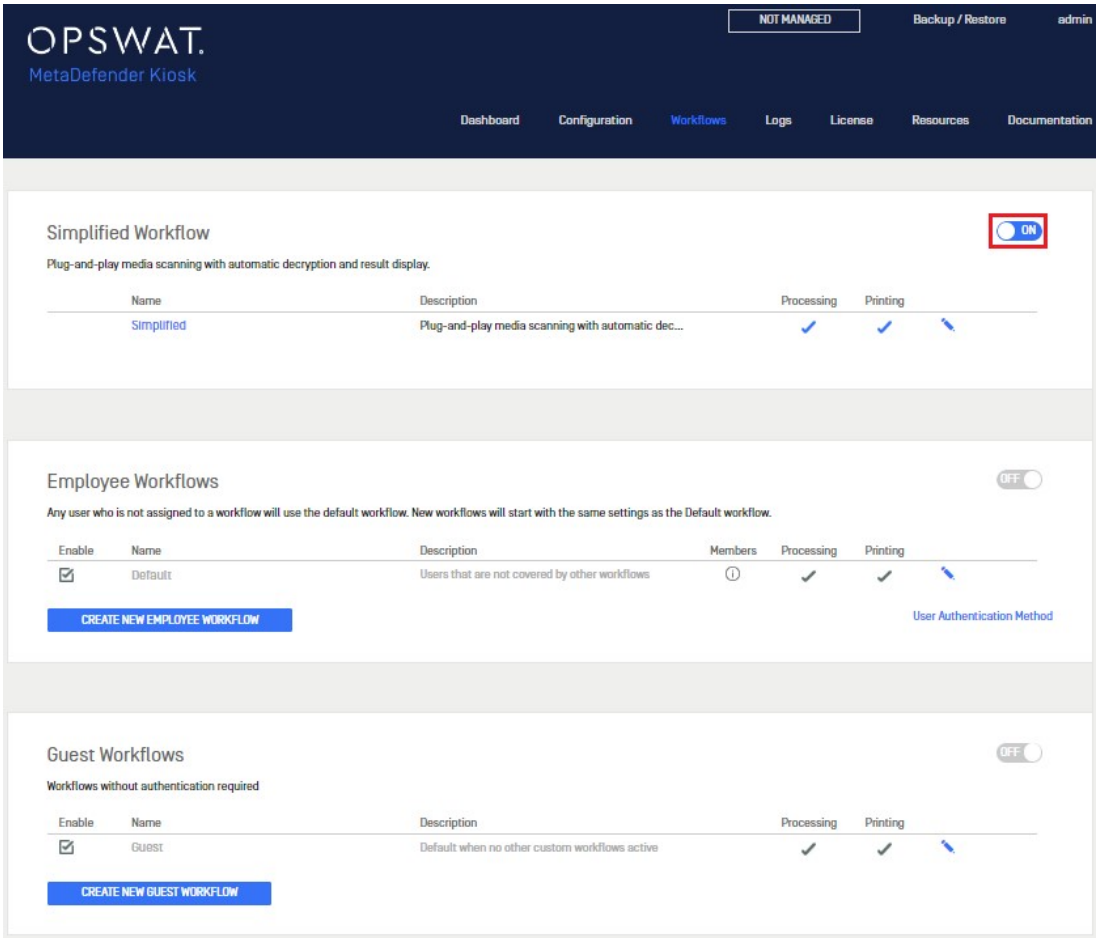
Our MetaDefender Kiosk product has a built-in Simplified workflow after a fresh install to support plug-and-play media scanning with automatic decryption and result display.

The process of Simplified Workflow is minimal as follows:

1. Kiosk will directly display the Insert Media screen
2. The Kiosk will automatically decrypt the encrypted USB using a list of preloaded passwords if any
3. The Kiosk will do the scanning and then display the end result as long as the USB is plugged
4. Once the USB is unplugged, it will show the Insert Media screen once again and wait for another USB

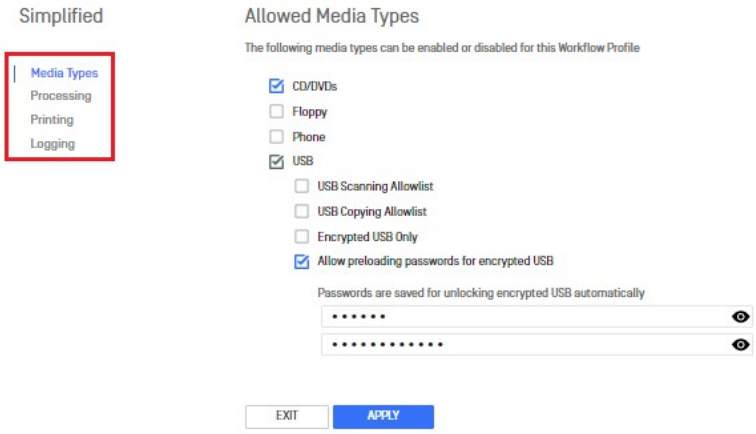
How to enable Simplified Workflow

1. Navigate to the Workflows tab and enable Simplified Workflow group.



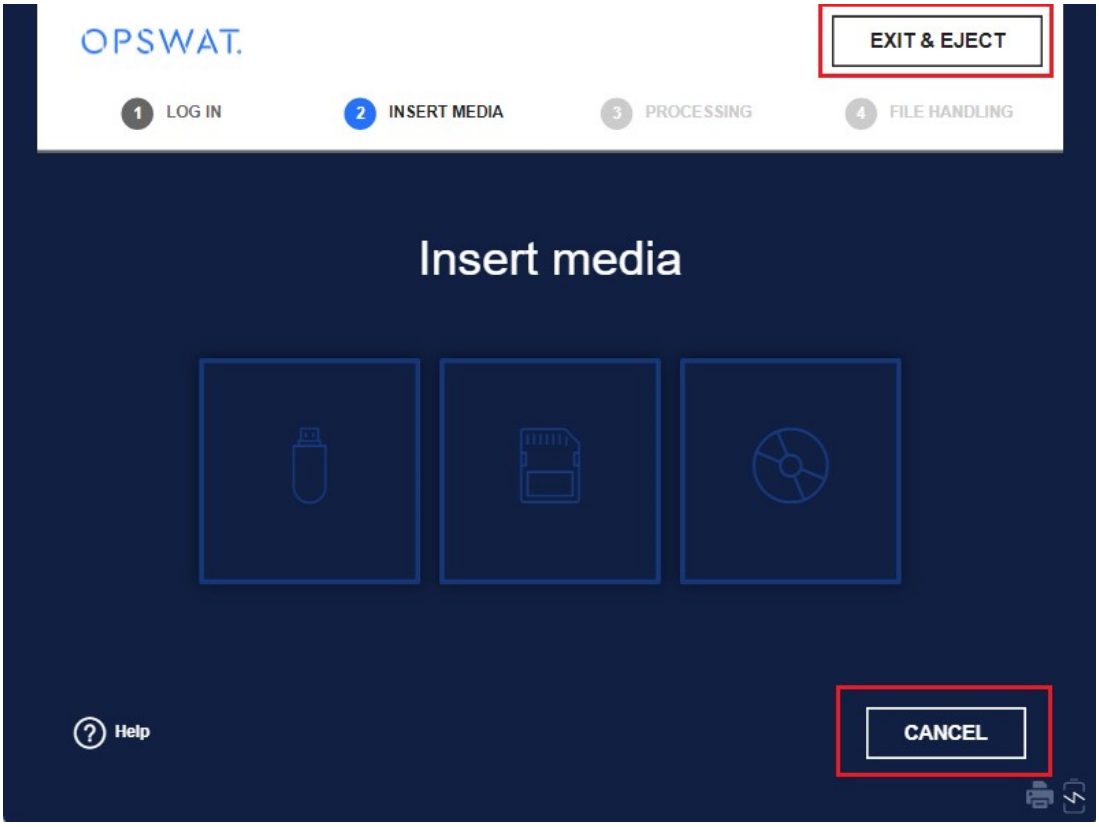
> **Info:**
> If **Simplified Workflow** group is enabled, **Employee Workflows** and **Guest Workflows** groups are disabled automatically, and vice versa.

2. **Simplified workflow** only supports to configure **Media Types**, **Processing**, **Printing** and **Logging**.



Usage Notes

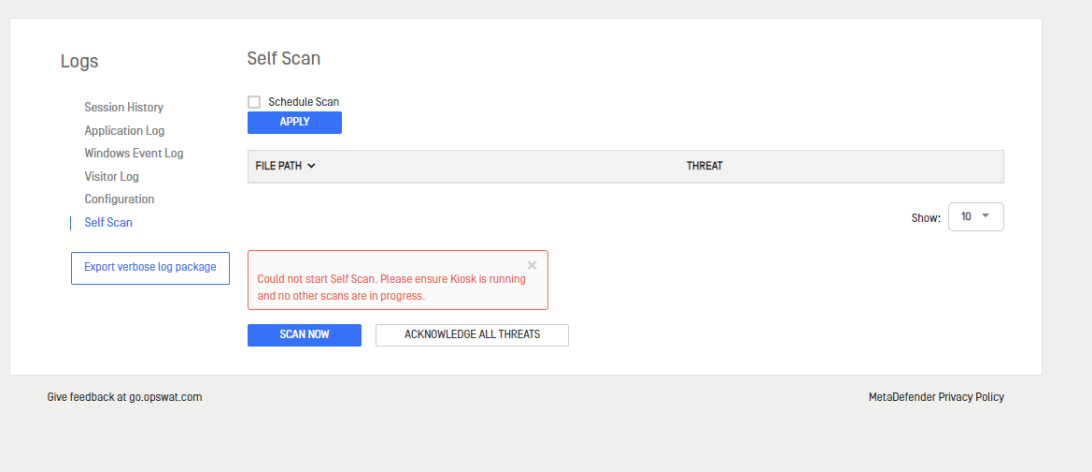
- **Simplified workflow** does not support **Retrieve Files** or other Post actions (**Allowed/Blocked File Handling**, **Email),** excluding **Printing** the report.
- If there are any configuration changes, manually reloading the Kiosk UI by clicking **Exit & Eject** or **Cancel** button is required to take effect.



Warning:

Simplified WF will directly display the *Insert Media* screen, which means KIOSK has already started a session. When clicking *SCAN NOW* for Self Scan, it will alert other scans are in progress.

Configure Schedule Self Scan and enable *"Allow Self Scan to cancel any currently runnning scan"* to trigger Self Scan instead.

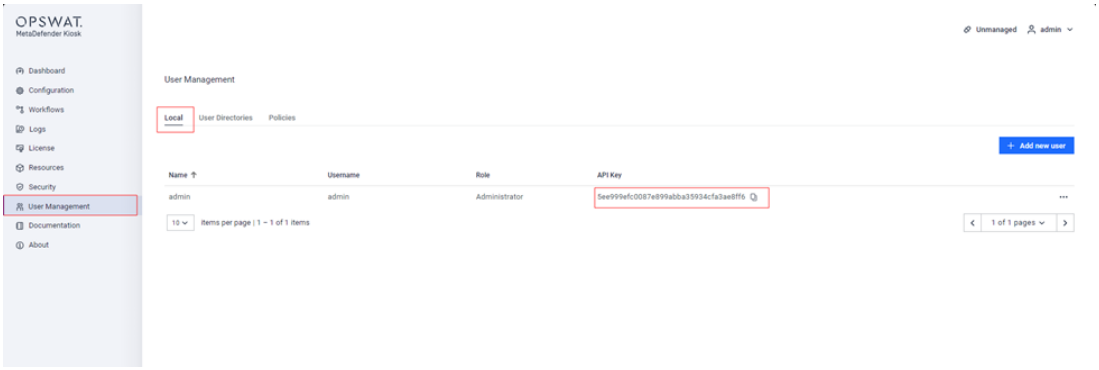


Support:
If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

How to increase session timeout via API?

To increase the session timeout on the Kiosk console via API call you will need the following resources from the Kiosk instance:

- An API key generated from the Kiosk console.

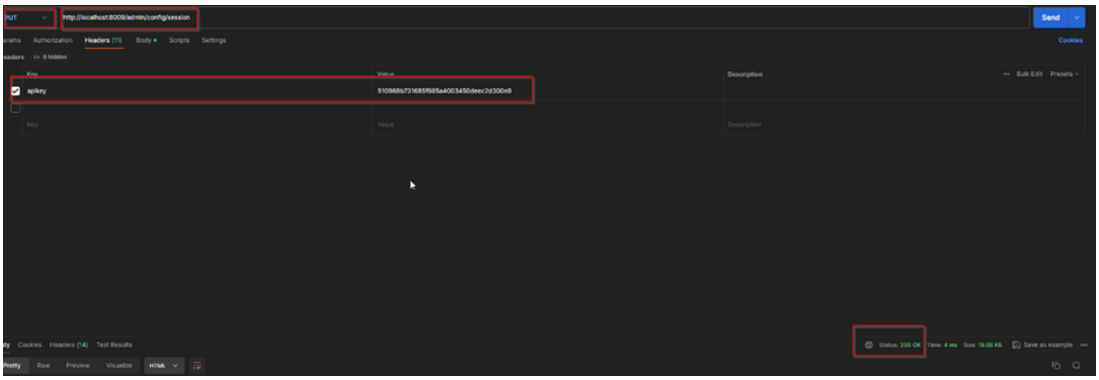


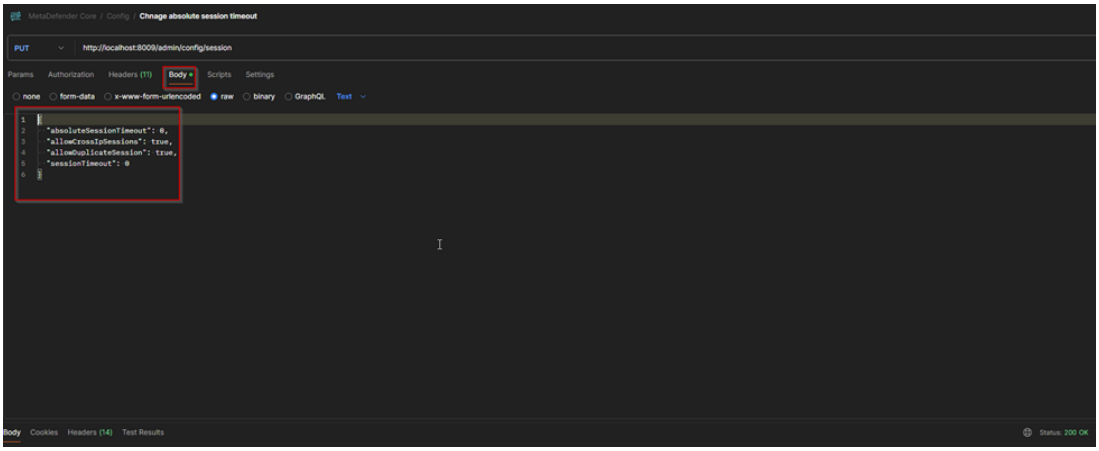
- A valid URL from the Kiosk instance we are trying to make this change.

Once we have the two items mentioned above, we will need to use the following API call to make the change to the session timeout value:

bash

```
curl --request PUT \ --url 'http://localhost:8009/admin/config/session' \ --
header 'Content-Type: application/json' \ --header 'apikey: {apikey}' \ --data '{
"absoluteSessionTimeout": 0, "allowCrossIpSessions": true,
"allowDuplicateSession": true, "sessionTimeout": 300000 }'
```





The value for the highlighted images from above is set to milliseconds.

Having the “0” value as can be seen in the image above will result in the timeout setting to be disabled.

Support:
If **Further Assistance** is required, please proceed to create a support case or chat with our support engineer.

Does adding a second MFT in the Kiosk serve as a high-availability mechanism?

Note:
The feature allowing the addition of multiple MFTs (Managed File Transfers) in the Kiosk is not intended as a high-availability mechanism. Here's a detailed explanation of how this functionality works.

The option to configure multiple MFTs in the Kiosk is designed to support different workflows. It allows users to assign specific MFTs to individual workflows based on requirements.

Adding a second MFT does not create a high-availability setup. There is no failover mechanism to switch to the secondary MFT if the primary MFT becomes unavailable.

Similarly, the Kiosk does not support a round-robin approach for load balancing between MFTs. Each workflow must explicitly select which MFT it uses, and the system will not automatically alternate between them.

Support:
If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

Why does Kiosk showing a very large number of hidden partitions when scanning DVD/CD?

This issue is caused by an unsupported partition count on DVD/CD, results in the partition count being 0, while there is 1 DVD/CD is mounted.

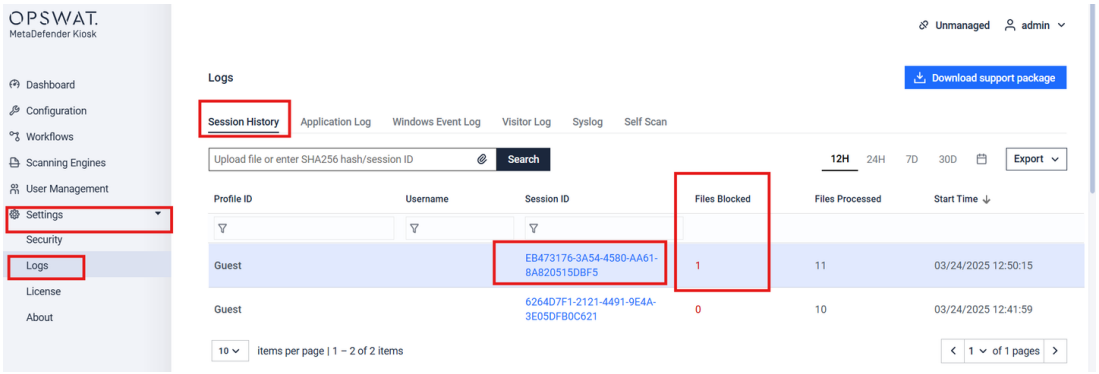
To resolve this issue, upgrade to **Kiosk version 4.7.3** or later. This update includes the necessary fixes to support the correct partition count on DVD/CD devices.

Support:
If Further Assistance is required, please proceed to create a support case or chat with our support engineer.

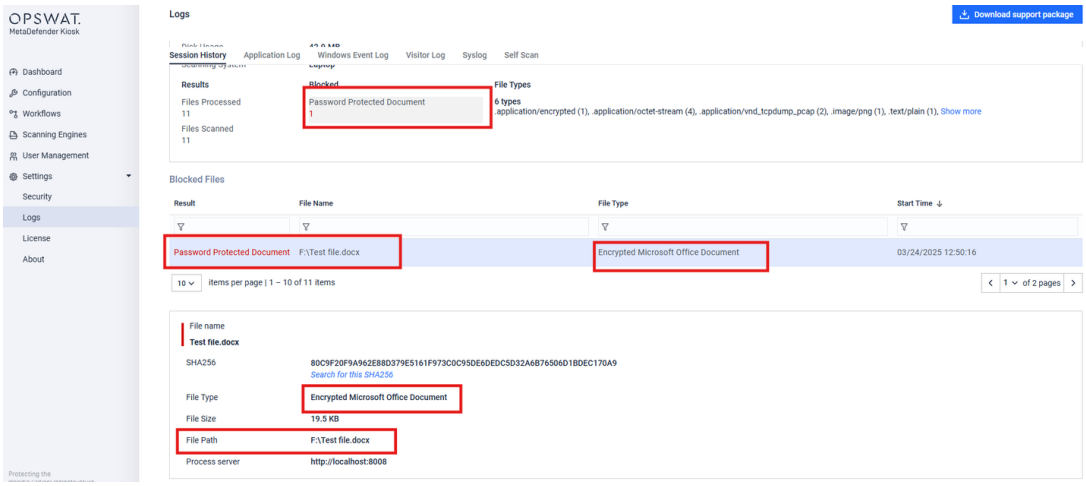
Why is Kiosk Skipping Files?

View the session history for more details regarding Skipped Files

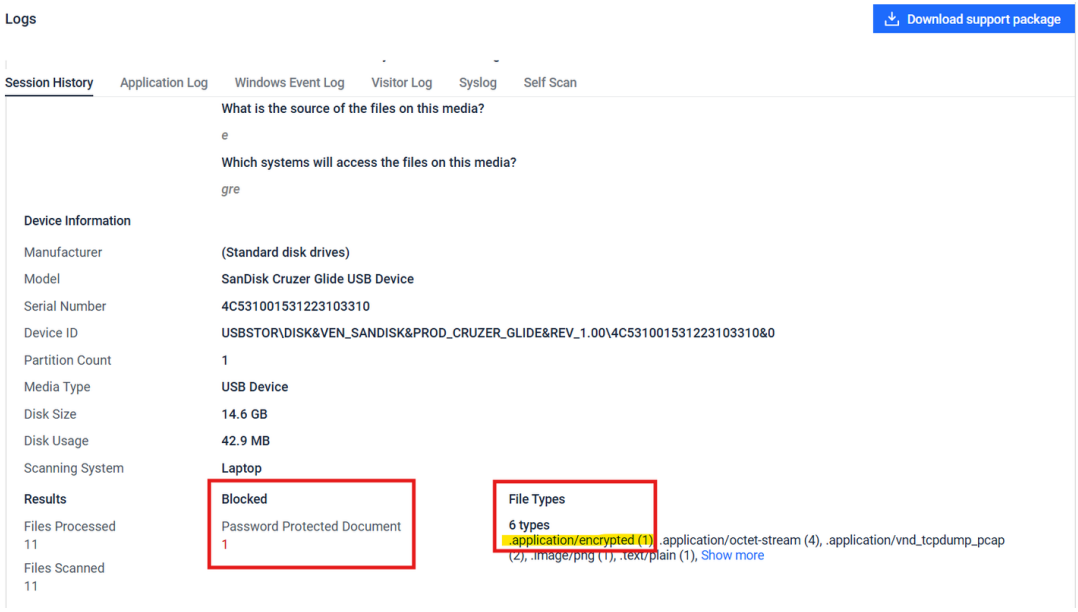
- Navigate to “Settings” > “Logs” > “Session History”. Here you can click on the “Session ID” for more information.



1. Media scanned contains **encrypted** or **password-protected** files that MetaDefender Core cannot unlock. You can view these under “Files Blocked” for more details, click on the “Blocked” reason to view “File Path”, “Process Server”, “File Type”, “File Name”, “SHA256” hash.

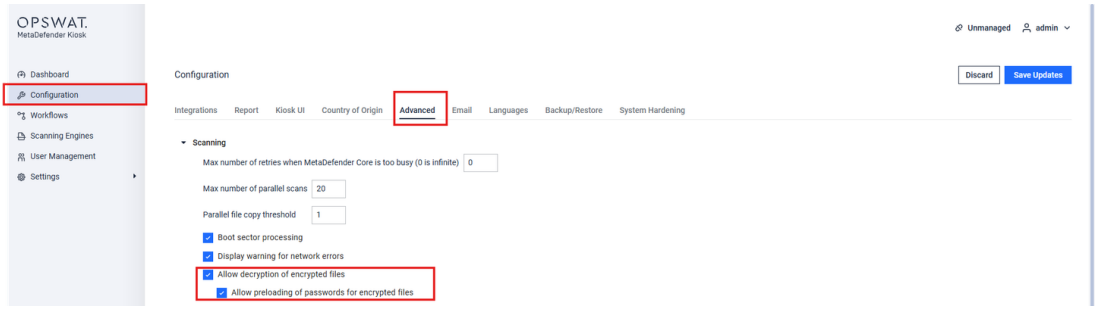


Continue to scroll down for further details

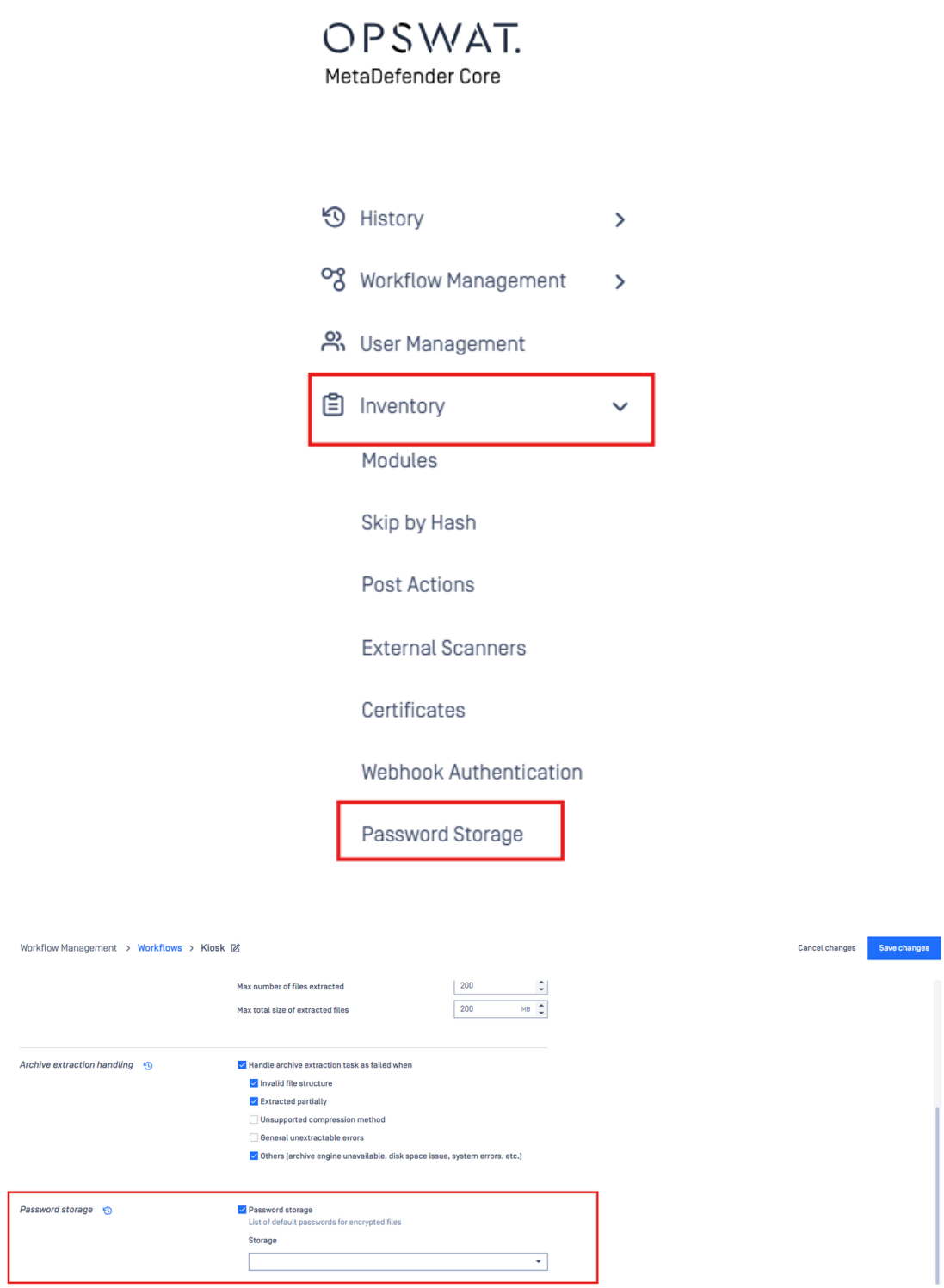


When scanning Media, if Kiosk detects a password-protected file, it will prompt the user to enter the password. If a password is not entered, the file will be skipped.

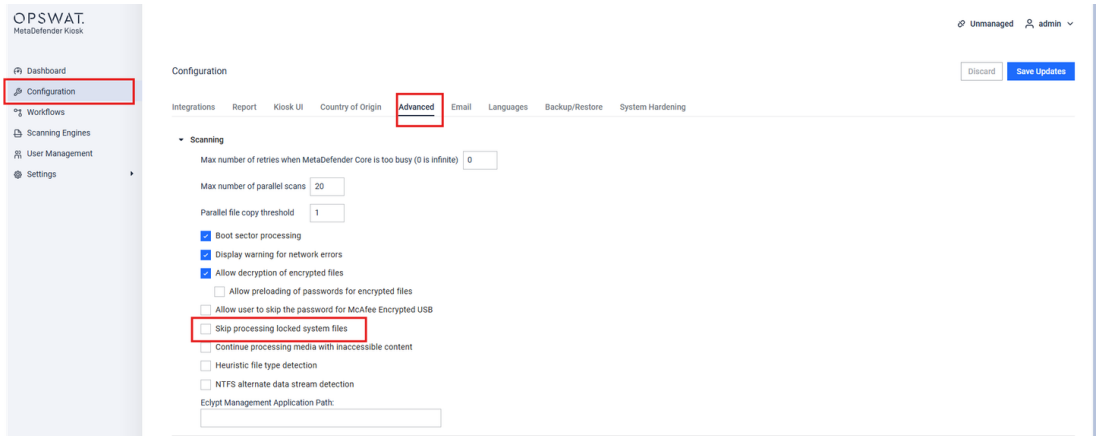
Kiosk allows you to pre-load passwords into the Kiosk Web Management console and MetaDefender Core Web Management console.



On the MetaDefender Core > Workflow Management > Workflows > “Kiosk” workflow > “Archive” tab, you can select predefined passwords



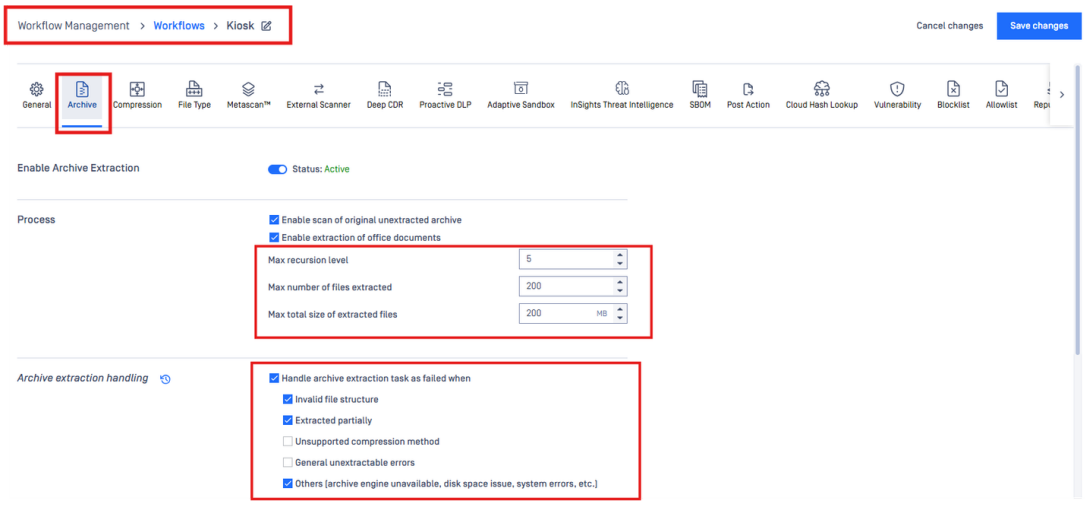
System files may be locked, if you have “Skip processing locked system files”, these files will be skipped.



2. Scan exceeded archive size or file failed to scan

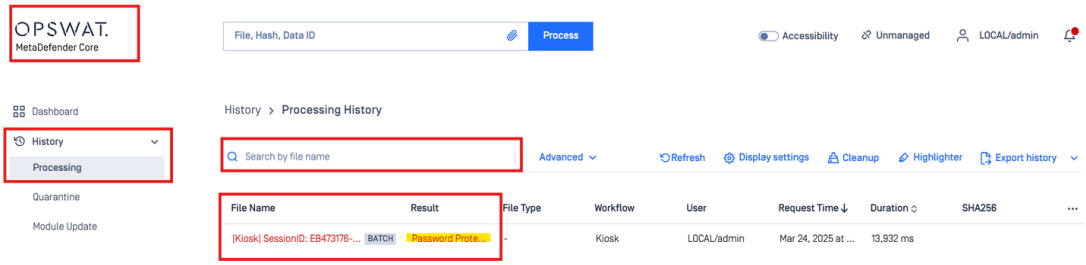
Under MetaDefender Core > Workflow Management > Kiosk > Archive

- You can select limits for archive files, defining how deep you want to scan the file. If these limits are reached and the file has not been fully scanned yet, this can result in a “skipped file” or “blocked file”. Increase these limits and scan the file again.
- If you have “Handle archive extraction task as failed when” checked, the file may be skipped if the following occur: “Invalid file structure”, “Extracted partially”, “Unsupported compression method”, “general unextractable errors”, “others [archive engine unavailable, disk space issue, system errors, etc.]”. We suggest viewing the file under “Kiosk session log” to view the specific reason for the file.
-



You can also navigate to MetaDefender Core to view the reason [you can search by session ID to narrow down scan]

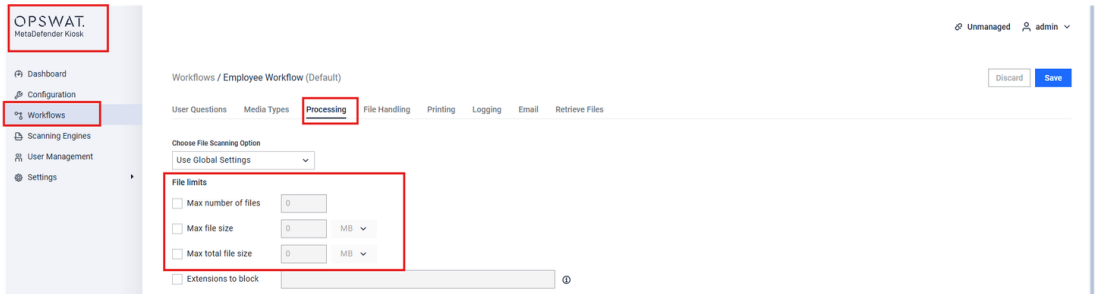
MetaDefender Core > Processing History > Processing > Select Kiosk scan



3. Overall File Size is too big

Under MetaDefender Core > Workflow Management > Workflows > Kiosk, you can increase the default file scan sizes.

If you also have file sizes specified on the workflow, you can increase them under MetaDefender Kiosk > Workflows > Select workflow used for scan [Guest or Employee] > Processing > File limits



Support:
If **Further Assistance** is required, please proceed to log a support case or chatting with our support engineer.

How do I check the version of a Kiosk Hardened/Secure Image “install.wim” file?

> **Check Your Version:**
> This article applies to all MetaDefender Kiosk Hardened/Secure Image releases deployed on Windows systems.

There are a few ways to check the version of an “install.wim” image, without having to deploy the image on a Kiosk hardware:

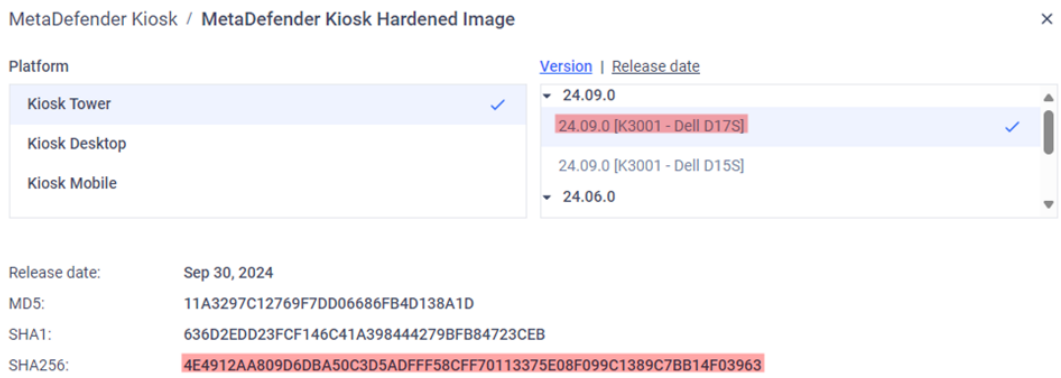
Solution 1:

Calculating the hash of the “install.wim” image and comparing it to the published hash on My OPSWAT

powershell

```
> Get-FileHash -Path .\install.wim -Algorithm SHA256

SHA256 4E4912AA809D6DBA50C3D5ADFFF58CFF70113375E08F099C1389C7BB14F03963
```



In this example, the hash of “install.wim” matches the hash for Kiosk Hardened Image 24.09 K3001.

Solution 2: For Secure Image only

Run the Get-WimInfo command to check the description of an “install.wim” image:

powershell

```
> DISM /Get-WimInfo /WimFile:.\install.wim
Deployment Image Servicing and Management tool
Version: 10.0.26100.1150
Details for image : .\install.wim
Index : 1
Name : Kiosk Secure Image 4.7.1
Description : MD Core 5.11.1 | MD Kiosk 4.7.1 | Release Q4 2024
The operation completed successfully.
```

Solution 3: For Hardened Image 24.06.0 and later

Mount the “install.wim” image and check its registry directly.

- You can mount the image by using DISM GUI.
- Alternatively, mount the image with the following commands:

powershell

```
> DISM /Mount-Wim /WimFile:<path_to_wim_file> /Index:<index_number> /MountDir:
<mount_directory>
```

Note:
Replace <*path_to_wim_file*> with the path to your .wim file, <*index_number*> with the index of the image you want to mount (e.g., 1 for "Windows 10 Kiosk Image"), and <*mount_directory*> with the directory where you want to mount the image.

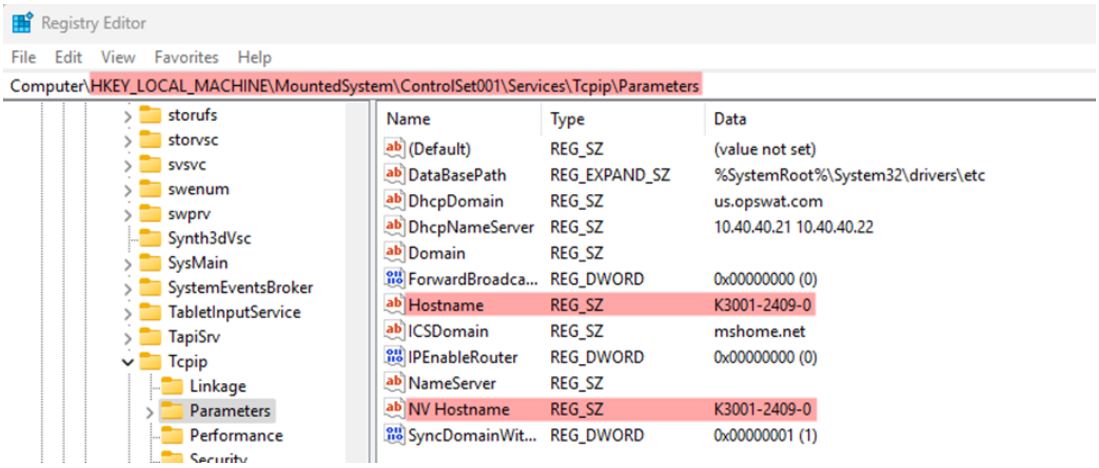
Inspect the registry:

1. Open the registry editor.
2. Load the registry hive from the mounted image:

- Select HKEY_LOCAL_MACHINE.
- Go to File > Load Hive.
- Navigate to the mounted directory and open Windows\System32\Config\SYSTEM.
- Give it a temporary name (e.g., MountedSystem).

3. Find the hostname:

- Navigate to HKEY_LOCAL_MACHINE\MountedSystem\ControlSet001\Services\Tcpip\Parameters.
- Look for the Hostname and NV Hostname values.



In this example, the hostname of this “install.wim” is K3001-2409-0, so that is its Hardened Image version.

Unload the registry hive:

1. Select the loaded hive (e.g., MountedSystem).
2. Go to File > Unload Hive.

After this, unmount the “install.wim” image:

- Unmount from the DISM GUI (if you mounted it using this method).
- Or, with the following command:

powershell

```
> DISM /Unmount-Wim /MountDir:<mount_directory> /Discard
```

Support:
If you have followed the instructions above but are still unable determine the version of the “install.wim” image for Kiosk Hardened/Secure Image, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

Can MetaDefender Kiosk be configured to handle large volumes of scans more quickly?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows or Linux systems.

Yes, it can.

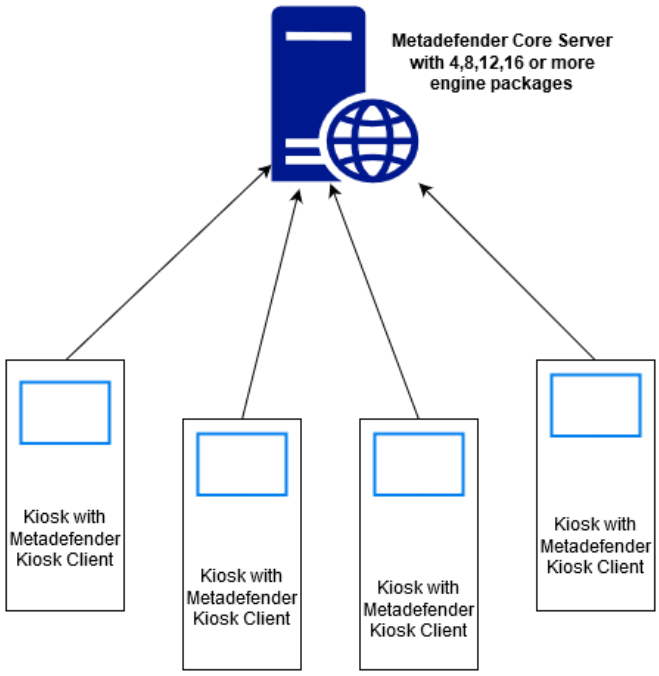
The performance and configuration of the associated MetaDefender Core instance can drastically limit the performance of your MetaDefender Kiosk solution.

Please Note:
MetaDefender Core is greatly affected by its host hardware's specifications.

Standard Kiosk units are intended to be portable, convenient and easy to set up; as a result, these units are limited in size and airflow, making them more suitable for standard usage with medium traffic.

Customers requiring high volume scans and faster performance should consider a distributed configuration where the MetaDefender Kiosk module is maintained on the Kiosk and the MetaDefender Core module is maintained on a powerful remote server.

The diagram below illustrates the distributed configuration:



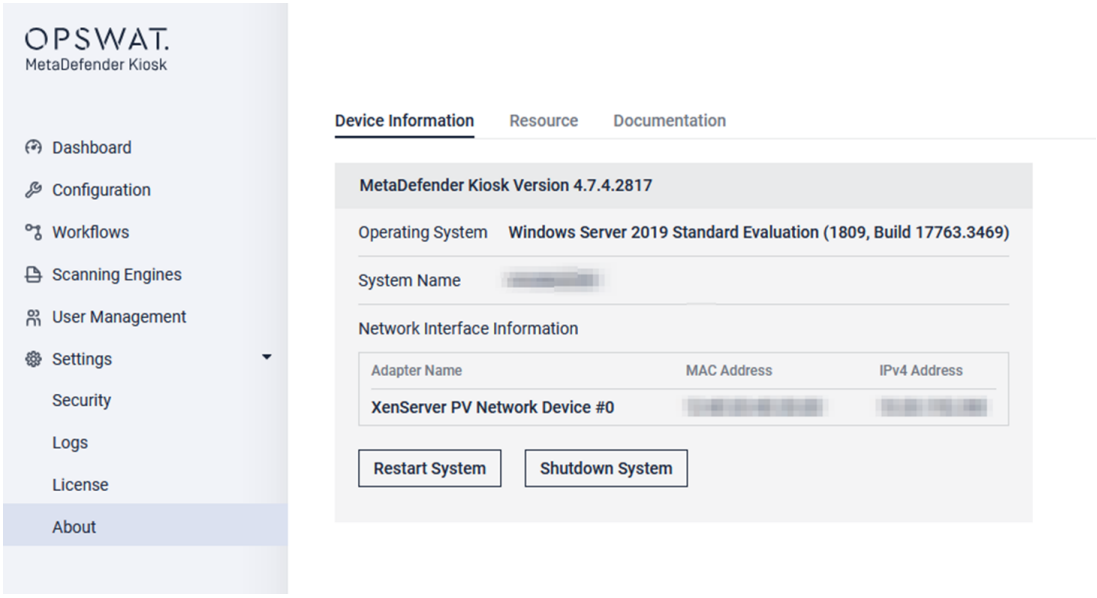
Support:
If you are having difficulty **Setting Up a Distributed Configuration for MetaDefender Kiosk**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

How to remotely Shutdown or Restart the System from the Kiosk UI?

Starting with **MetaDefender Kiosk version 4.7.3**, administrators can remotely restart or shut down a Kiosk machine directly from the **MetaDefender Kiosk Management Console**. This feature is particularly useful for managing remote deployments without requiring physical access to the Kiosk machine.

Important Note: If your machine is configured to require a login (e.g., Windows login), restarting the system will stop at the login screen. An administrator will need to log in locally or through a remote management solution to complete the boot process.

Restarting or Shutting Down the Kiosk



1. In the **Device Information** view, you will see **System** or **Network Interface Information** details
2. Look for the buttons labeled:
    a. **Restart System**
    b. **Shutdown System**
3. Click the relevant button to initiate the desired action:
    a. **Restart System:**
        i. Triggers a standard Windows restart.
        ii. If the machine is configured with a login prompt, it will require manual login after reboot.
    b. **Shutdown System:**
        i. Powers down the Kiosk machine entirely. You will need physical access or remote power management to turn it back on.

Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Does the MetaDefender Kiosk hardened image support Windows 11?

Check Your Version
This article applies to all MetaDefender Kiosk releases deployed on Windows systems.

Answer

No, the MetaDefender Kiosk hardened image does not support Windows 11.

The current hardened image utilized by MetaDefender Kiosk is based on Windows 10 IoT Enterprise LTSC 2021 (21H2, Build 19044).

Additional Information

MetaDefender Kiosk Hardened Image was built on the Enterprise Windows version that follows the LTSC (Long-Term Servicing Channel) model. This version is specifically designed for IoT devices, providing essential services and functionalities tailored for IoT environments. In contrast, Windows Professional is primarily intended for personal use and does not offer the same level of support for IoT applications.

We are using **Windows 10 IoT Enterprise LTSC 2021 (19044), which remains under Microsoft's mainstream support until January 12, 2027, and extended support until January 13, 2032.**

This version will continue to receive Windows updates, including security patches and antivirus definition updates for Windows Security.

Reference: Microsoft Lifecycle Policy - Windows 10 IoT Enterprise LTSC 2021

Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why files are copied to Admin accounts instead of AD account in MFT?

Check Your Version:
This article applies to all Kiosk versions and MFT version 3.8.0 or newer

Problem

Kiosk and MFT are configured to the same Active Directory. After upgrading MFT to 3.8.0 or later, you may encounter the following issue:

When users log in with Active Directory credentials, files that are supposed to be uploaded to the user's directory on MFT are instead uploaded to the admin's MFT directory.

In the kiosk log, you may see entries like the following:

```
[1728] [Apr 07, 12:20:44:852] authentication.cpp#244 Authentication::GetProfilesName(): {91F78BA2-B699-4C40-B321-061C35F7089C} [Kiosk UI] User "aaa" of domain "" logged in at AD "example.com" | LDAP code: 0
...
[8972] [Apr 07, 12:21:40:734] metadefender.cpp#5190 Metadefender::ScanWithVault(): {91F78BA2-B699-4C40-B321-061C35F7089C} Initializing upload to Vault server failed with user credentials, attempting to use guest account
[8972] [Apr 07, 12:21:40:798] sft.cpp#752 SFT::CreateGuestAccountForSFT(): {91F78BA2-B699-4C40-B321-061C35F7089C} Could not create guest account - HTTP Code: 403 - Code Description: Forbidden - HTTP Response: {"message":"You're not authorized to access this resource.","ui_message_key":"API_UNAUTHORIZEDRESOURCE","status_code":"Forbidden"} - Network Info: No error (0)
[8972] [Apr 07, 12:21:40:798] sft.cpp#960 SFT::ConfigureGuestAccountForScan(): {91F78BA2-B699-4C40-B321-061C35F7089C} Could not create guest account:
```

In the MFT rest log, you may see errors such as:

```
2025-04-07 12:21:40,285 105 ERROR   An exception occurred while doing: "InitGroupTransferDiode". Status code: BadRequest. Message: The file uploader group is required
2025-04-07 12:21:40,473 158 ERROR   Access forbidden (403) for user [5Djlc6BjB8hP3fUQRsi6uA6YVXHSlD] to resource [Account.CreateGuest]
2025-04-07 12:21:40,473 105 ERROR   An exception occurred while doing: "CreateGuestAccount". Status code: Forbidden. Message: You're not authorized to access this resource.
```

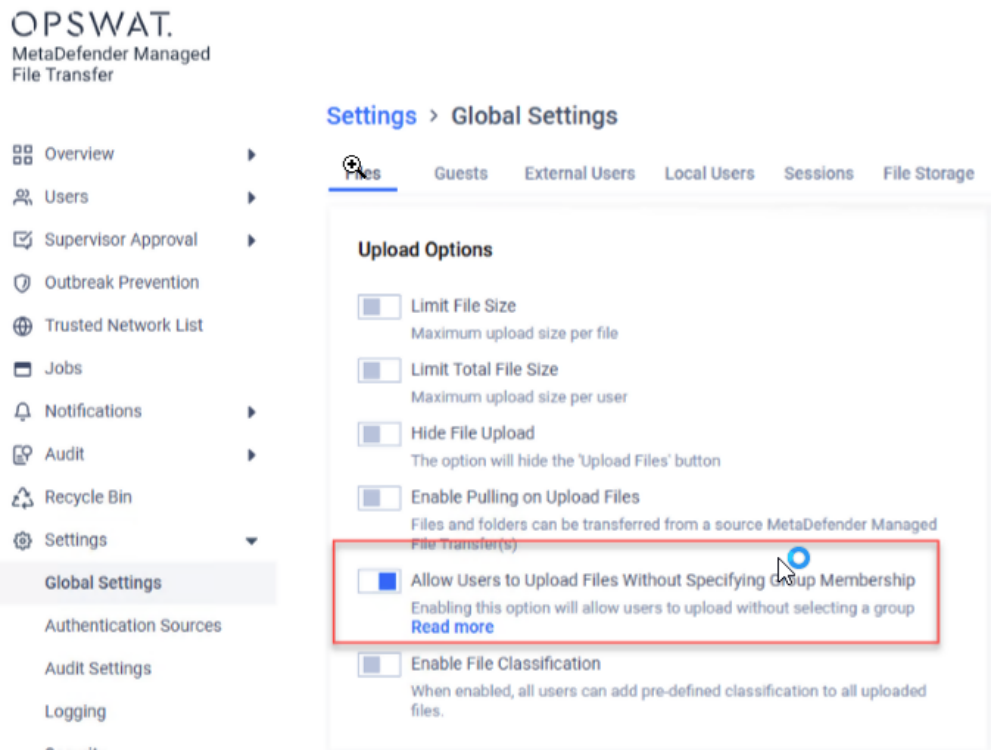
Root cause

Starting in version 3.8.0, MFT introduces the ability for administrator to manage both Active Directory and Local groups on the “Trusted Network” page. This feature allows administrators to specify which groups are permitted or denied access to upload and download files, providing better control over file access and security.

In earlier MFT versions, upload requests from Kiosk to MFT did not require group membership to be specified. However, starting in MFT 3.8.0, if group membership is not provided, the request failed. To prevent data loss, files are instead assigned to the admin account by default.

Solution

Go to **MFT management console** and navigate to: **Settings** > **Global Settings** > **File** tab, then enable the following option: “**Allow Users to Upload Files Without Specifying Group Membership**”



Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

How do I configure MetaDefender Kiosk to use a Gmail account for email notifications?

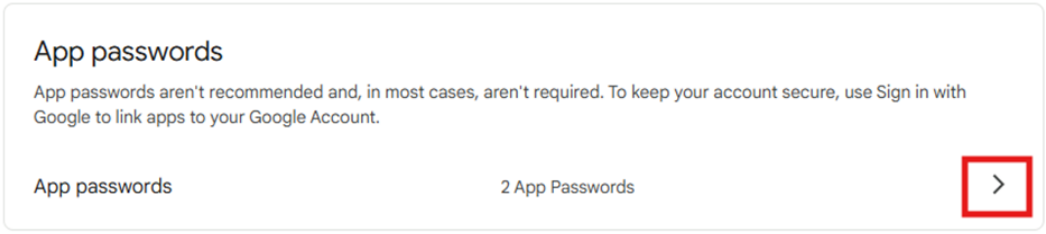
Solution

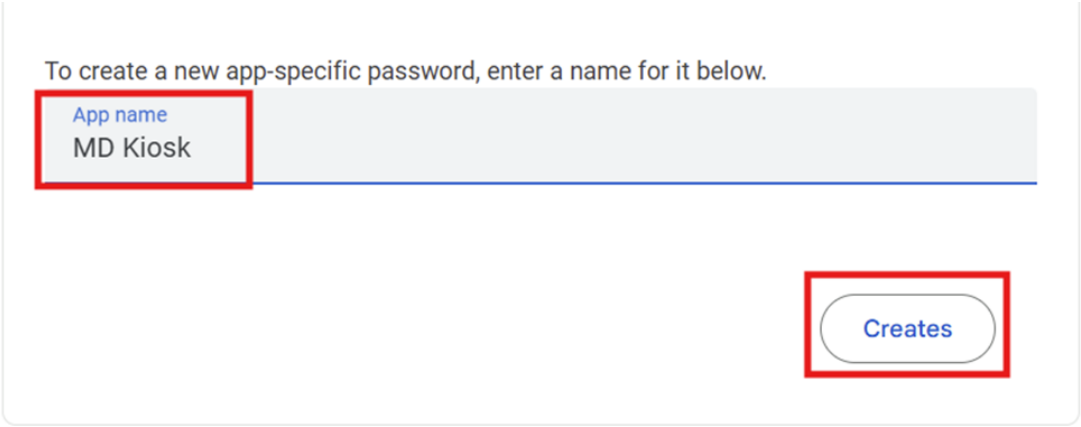
To be able to send notification to your Gmail mailbox from MetaDefender Kiosk, the following fields should be configured properly:

- Email settings: **SMTP**
- Host: **smtp.gmail.com**
- Port: **587**
- Authentication: **StartTLS**
- Username: username of the Gmail mailbox which will be used as a sender.
- Password: App password created for Gmail mailbox provided under “Username” field.
- From address: Need to provide the same email address

In order to achieve that, the following configuration should be done on Gmail mailbox account:

1. Create App password for Gmail account
    a. Login to https://myaccount.google.com/security
    b. Under "Signing in to Google":
        i. Enable 2-Step Verification
        ii. Scroll down to section “App passwords” and click arrow in front of “App passwords”

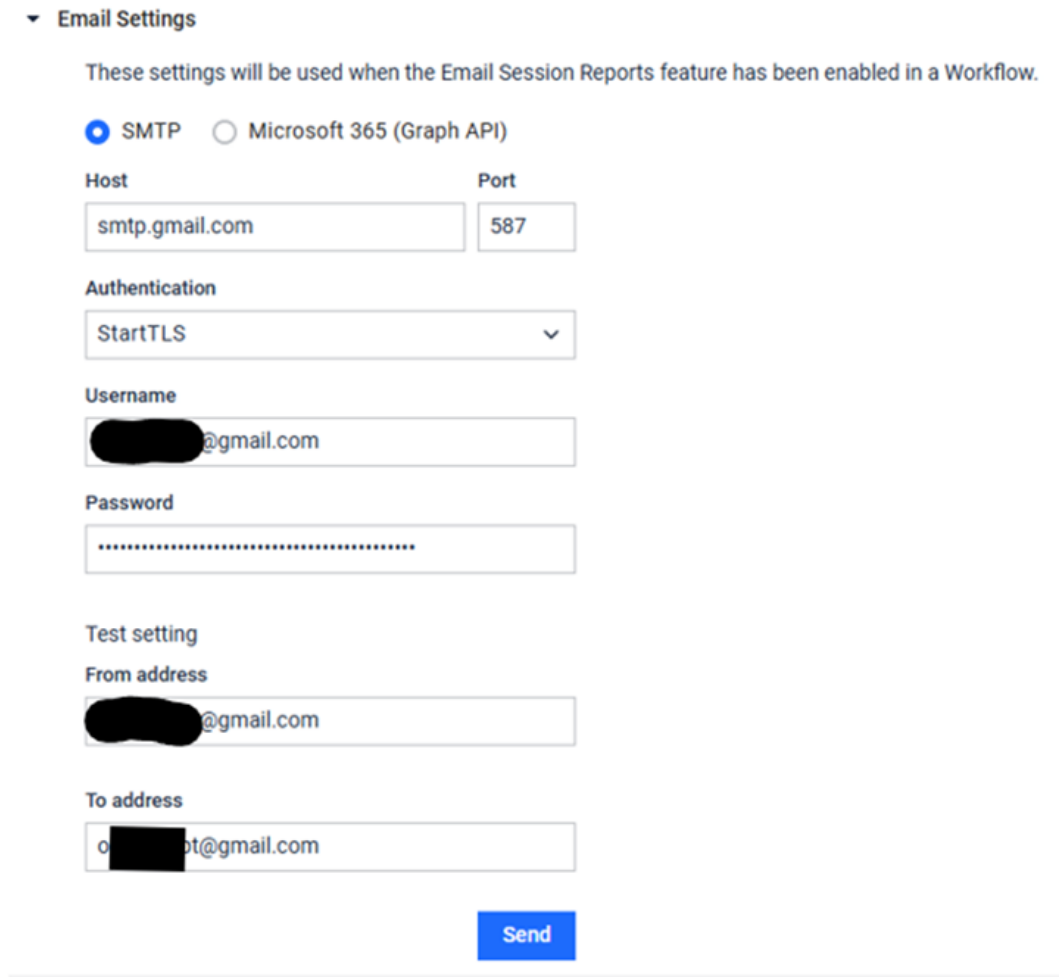




- In the new page opened, write a name for your App password and click "Creates"
- Save the App password generated and click “Finished”. Further we will use the App password generated as password for mailbox used for MetaDefender Core configuration as mentioned above and as in below example.

Example:

IMPORTANT: For field “Password” use App password created under Gmail account and not use the password which you use to login on Gmail mailbox.



Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

How do I configure SMTP server on MetaDefender Kiosk to send notification to M365 tenant?

Solution

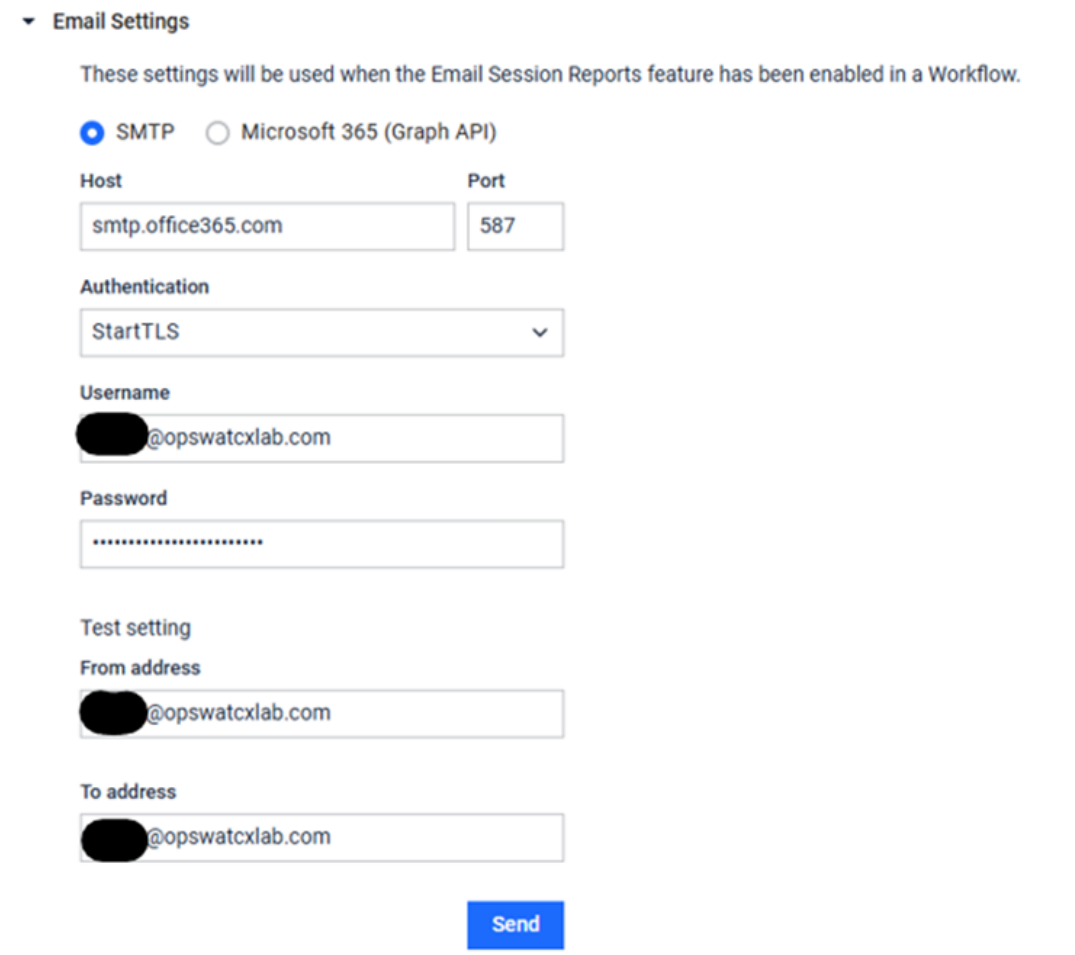
To be able to send notification to your M365 tenant from MetaDefender Kiosk, the following fields should be configured properly:

- Email settings: **SMTP**
- Host: **smtp.office365.com**
- Port: **587**
- Authentication: **StartTLS**
- Username: Email address for sender of notification, it should be a real mailbox which is licensed on M365 side. Normally in M365 is called UPN and it's the same one as Primary SMTP Address.
- Password: password of the mailbox provided under "Username" field

Section "**Test settings**" provide the option to test SMTP configuration, but there should be provided real email addresses in order to be able to receive the email by recipient set.

More details about M365 URLs can be found checking following link: Microsoft 365 URLs and IP address ranges - Microsoft 365 Enterprise | Microsoft Learn

Example:



Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

How to Set Up OPSWAT Kiosk to Copy Files to a Secondary Location for an AD User?

This article provides step-by-step instructions for configuring OPSWAT Kiosk to copy files processed by the Kiosk to a secondary network location for Active Directory (AD) authenticated users.

Prerequisites:

AD setup is required as this is regarding AD users. How to setup AD for Workflows:

https://www.opswat.com/docs/mdkiosk/knowledge-base/can-i-add-groups-from-active-directory-to-metadefender-kiosk-wor

***Steps to Configure*:**

1. **Login into MD Kiosk Web UI**
    a. Navigate to **Workflows → Employee Worflows → File Handling**
2. **Configure Post Action**
    a. Under **Post Action**, select **Copy to Secondary Location**.
    b. Activate **Directory** and fill out the required fields:
        i. **Path**: Enter the remote network location path (Example: \192.168.0.1\test\folder).
        ii. **Display Name:** Provide an appropriate name that identifies this location clearly.
        iii. Setup the **Access Control** for either **Inherited** or **Restricted**:
            i. **Inherited**: Files and folders will inherit the same permissions as the parent folder
            ii. **Restricted**: Only Kiosk authenticated users will have the permissions to access their files and folders

Important:

- Setting **Access Control** to **Restricted** is critical, as this limits file and folder permissions specifically to users who authenticate through the Kiosk.
- The OPSWAT Kiosk feature for copying files only supports Windows network shared folders. Using a file-sharing system on Linux is not supported by this feature.
- This configuration is available for both Allowed & Blocked settings in the File Handling setting.

How do I verify my Kiosk Image type?

> **Check Your Version:**
> This article applies to all MD Kiosk versions

MetaDefender Kiosk supports multiple deployment types on Windows. The following instructions will help you verify whether your system is using the Kiosk Hardened Image, Secure Image, or the standalone Kiosk Software.

1. Via the support package.

When exporting the Kiosk support package, a file named `imageType.info` is included. You can open this file using Notepad to view the deployment type.

Software Edition: The user installed the Kiosk software manually.

Hardened Image: The OS was flashed with a Hardened Image.

Secure Image: The OS was flashed with Secure Image

> **Info:**
> The method above only applies to MD Kiosk 4.7.1 or above

2. Via registry.

You can browse this registry to check the Kiosk information HKLM\SOFTWARE\WOW6432Node\OPSWAT\MD4M

“harden_image” = 0 means The user installed the Kiosk software manually.

“harden_image” = 1 means The OS was flashed with a Hardened Image.

“secure_image” = 1 means The OS was flashed with Secure Image.

> **TIPS:**
>
> - Customers who purchase Kiosk Hardware will receive the Kiosk Hardened Image pre-installed as the operating system.
> - **Secure Image** is a specialized version of the Hardened Image, enhanced with a File Integrity Monitoring feature. This edition requires an additional license and is available for selected Kiosk hardware or upon request.

Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why are some of the keys on the physical keyboard not responsive in MetaDefender Kiosk?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows systems.

Please Note:
In the case of certain keys and key combinations (that would allow access to the underlying OS interface) being unresponsive, this is not an error.

As a fundamental MetaDefender Kiosk security requirement, OPSWAT has ensured that the Kiosk application is the only accessible interface on the system for non-administrative users.

To ensure this security feature, the Kiosk system ignores certain keys on the keyboard that can be used individually and in combination with other keys to close an application and access the underlying interface and other programs.

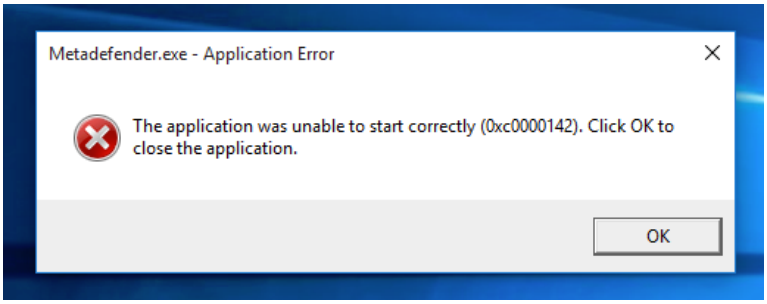
We have had requests from users to enable these keys for certain use cases, and our development team is actively researching ways to meet security requirements while still providing the convenience of certain critical keys on the keyboard.

Support:
If you have any difficulty **Accessing and Using Kiosk Administrative Controls Or the Kiosk Itself Due To Unresponsive Keys**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

Why doesn't my MetaDefender Kiosk start?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows systems.

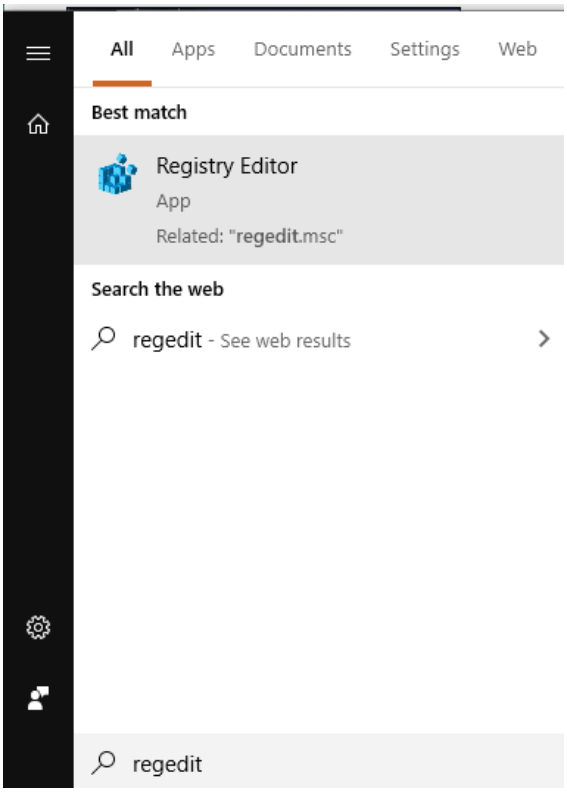
If your MetaDefender Kiosk fails to start, and you see the error message pictured below, it may be due to performance and slow speed issues on the machine hosting the Kiosk.



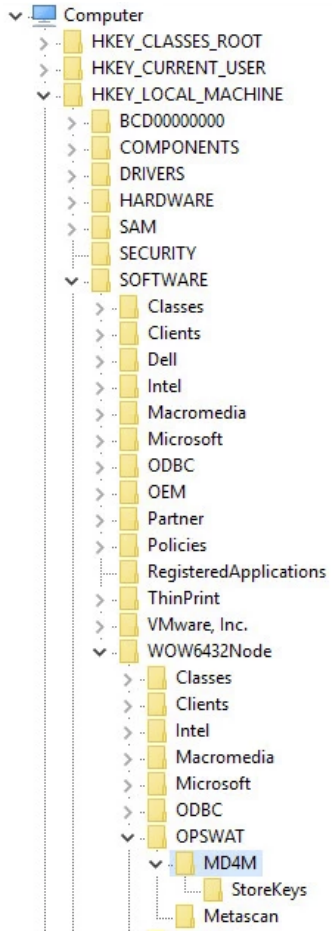
There are a variety of possible reasons for this, ranging from an underpowered CPU and low RAM, to a slow hard disk and numerous possible system errors.

To fix this issue, you will need to create a string registry key entitled **launch_delay_seconds** in the folder at path: **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\OPSWAT\MD4M** and you will need to set it to any value greater than zero.

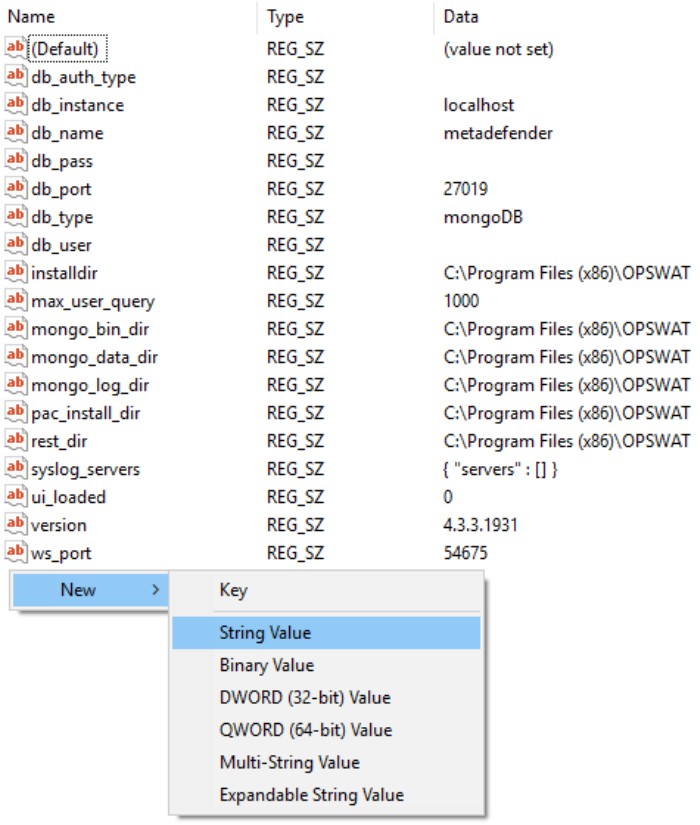
To set this registry key, open the Windows Regedit utility before following the steps below:



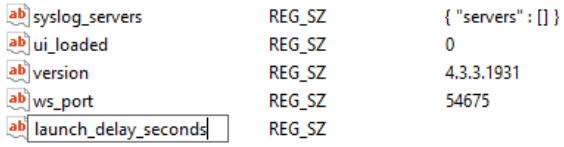
- Navigate to the folder at **\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\OPSWAT\MD4M**, as illustrated below.



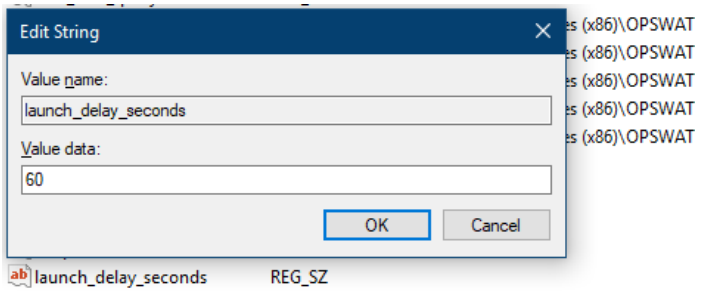
- Right-click, then choose **New>String Value** from the dropdown menu, shown in the screenshot below.



- Name the new value **launch_delay_seconds**



- Double click the newly assigned String and assign it a value greater than 0 (eg. 60) seconds



- Open an elevated command prompt (as Administrator) and enter the following commands in order to restart MetaDefender Kiosk and MetaDefender Kiosk REST service:
  - net stop metadefenderSVC

- net stop omdrest *
- net start omdrest *
- net start metadefenderSVC

Please Note:
*omdrest Service only applies to Metadefender Kiosk versions older and including 4.4.0.

Support:
If you have followed the instructions above but are still **Unable To Start Your MetaDefender Kiosk**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

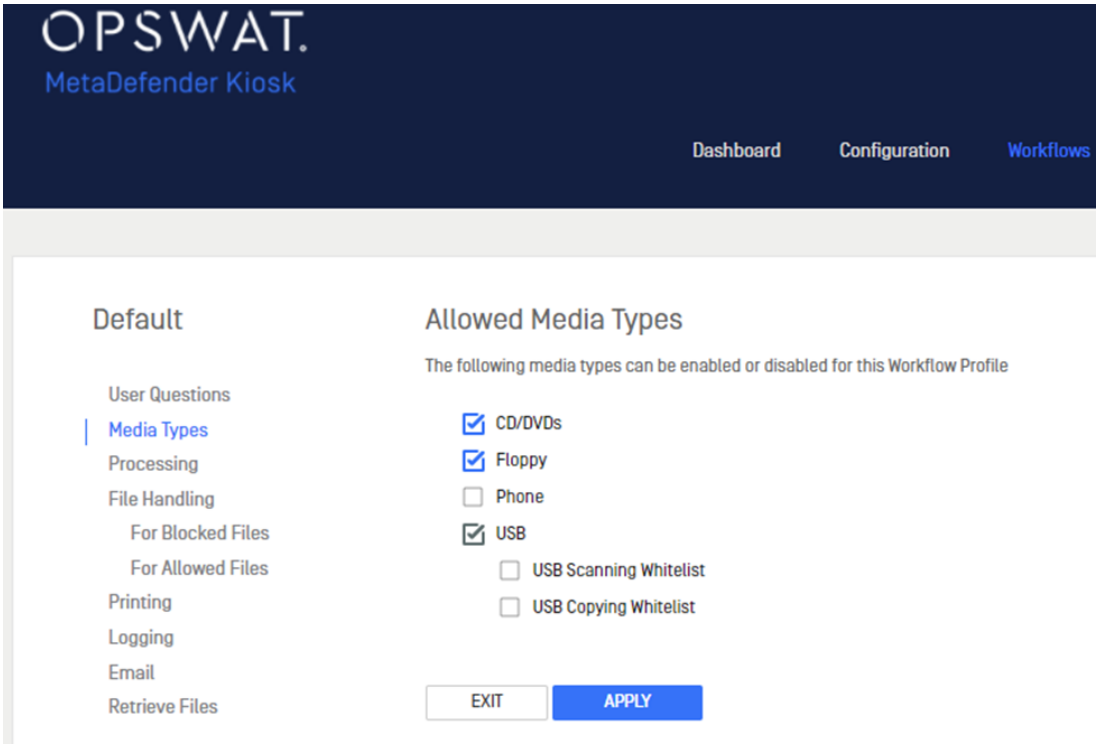
Why is MetaDefender Kiosk not recognizing floppy drives?

Check Your Version:
This article applies to all MetaDefender Kiosk V4 releases deployed on Windows or Linux systems.

MetaDefender Kiosk supports uploading to and from floppy drives, however, floppy drive access is disabled by default.

To configure your MetaDefender Kiosk to recognize floppy drives, please do the following:

1. Go to your MetaDefender **Kiosk Management Console>Workflows>MediaTypes**
2. Now, select the **Floppy** checkbox, as illustrated below, then click **Apply** to save your settings.



Support:
If you have followed the instructions above but **Your Floppy Drive Is Still Not Being Recognized By MetaDefender Kiosk**, please follow these instructions on How To Create a Support Package, before creating a support case or chatting with our support engineer.

Does a CVE affect MetaDefender Kiosk?

In today's rapidly evolving digital landscape, understanding the impact of security vulnerabilities is more crucial than ever. The Common Vulnerabilities and Exposures (CVE) list is an invaluable resource for identifying potential security risks associated with software products. This article provides a comprehensive overview of various CVEs, helping you determine whether MetaDefender Kiosk for Windows is affected. By staying informed about these vulnerabilities, you can take proactive measures to protect your systems and data from potential threats.

CVE	Summary
CVE-2024-5535	MetaDefender Kiosk for Windows is not impacted by CVE-2024-5535. The Kiosk system does not include OpenSSH's server (Kiosk remains unaffected by CVE-2024-5535).
CVE-2024-6387	MetaDefender Kiosk for Windows is not impacted by CVE-2024-6387. The Kiosk system does not include OpenSSH's server (Kiosk remains unaffected by CVE-2024-6387).
CVE-2024-40898	MetaDefender Kiosk for Windows does not use Apache HTTP Server and is not affected by CVE-2024-40898. Users of the Kiosk product can remain assured that this vulnerability does not impact their systems.
CVE-2024-27348	MetaDefender Kiosk for Windows does not utilize Apache HugeGraph-Server in its architecture. As a result, it is not susceptible to the CVE-2024-27348 vulnerability. The components and dependencies of Kiosk have been thoroughly reviewed, and there is no association with the affected versions or functionalities of Apache HugeGraph-Server
CVE-2018-25103	MetaDefender Kiosk for Windows does not use lighttpd, it is not affected by the vulnerabilities identified in CVE-2018-25103. Users of Kiosk can rest assured that this specific security issue does not pose any risk to their systems.
CVE-2024-34342	MetaDefender Kiosk for Windows does not use the react-pdf nor pdf.js so it is not affected by the vulnerabilities identified in CVE-2024-34342.
CVE-2018-15133	MetaDefender Kiosk for Windows is not impacted by CVE-2018-15133
CVE-2024-1874	MetaDefender Kiosk for Windows is not impacted by CVE-2024-1874
CVE-2024-2457	MetaDefender Kiosk for Windows is not impacted by CVE-2024-2457
CVE-2024-24576	MetaDefender Kiosk for Windows is not impacted by CVE-2024-24576
CVE-2024-3566	MetaDefender Kiosk for Windows is not impacted by CVE-2024-3566
CVE-2024-27980	MetaDefender Kiosk for Windows is not impacted by CVE-2024-27980
CVE-2024-4367	MetaDefender Kiosk for Windows does not use neither react-pdf nor pdf.js so it's not affected
CVE-2024-40725	MetaDefender Kiosk for Windows doesn't use Apache HTTP Server so it's not affected
CVE-2019-9082	MetaDefender Kiosk for Windows doesn't use either PHP or Think PHP so it's not affected
CVE-2024-4577	MetaDefender Kiosk for Windows doesn't use either PHP or Think PHP so it's not affected

Support:
If **Further Assistance** is required, please proceed to log a support case or chat with our support engineer.

Why do I receive Kiosk License mismatch error?

When attempting to license MD Kiosk and encountering the "License Mismatch" error, it indicates that there is a discrepancy between the provided license and the Deployment ID associated with the machine. The Deployment ID is a unique identifier generated for each machine during the licensing process.

The error commonly occurs when the Deployment ID of the machine was generated incorrectly or has become outdated. To resolve this issue, a simple procedure can be followed:

1. Rename the machine to a random name: By changing the machine's name, we trigger a change in the system's identification.
2. Restart the machine: The restart ensures that the new machine name is applied and the necessary system components are updated accordingly.
3. Rename the machine back to its original name: After the restart, revert the machine's name to its original value.
4. Restart the machine again: This additional restart forces the Deployment ID generating algorithm to recalculate the Deployment ID based on the updated machine name.

By following these steps, the system generates a fresh and accurate Deployment ID that aligns with the provided license. This effectively resolves the "License Mismatch" error and allows the licensing process to proceed smoothly.

It's worth noting that the exact procedure may vary depending on the specific software or system being used. However, the fundamental principle remains the same: by modifying the machine name, restarting the machine, and then restoring the original name followed by another restart, we trigger the recalculation of the Deployment ID, ensuring its alignment with the provided license.

Remember to consult the software's documentation or reach out to the appropriate support channels for any specific instructions or troubleshooting steps related to the licensing process.

Support:
If **Further Assistance** is required, please proceed to create a support case or chat with our support engineer.

Why is the Kiosk not detecting devices?

If your Kiosk is not detecting devices, several factors may be causing the issue. Below are common causes and their potential solutions.

Windows Defender Real-Time Protection

Windows Defender may block the Kiosk application from recognizing USB devices. Try disabling real-time protection using a Group Policy Object (GPO) to see if it resolves the issue.

Malfunctioning USB Port or Device

A faulty USB port or an incompatible USB device might prevent detection. Test different ports or devices to identify the issue.

WMI Service Failure

The Windows Management Instrumentation (WMI) service is crucial for detecting USB devices. If this service fails, the Kiosk may not recognize devices. Reinstalling the operating system and Kiosk software has resolved this issue in some cases.

Driver Conflicts

A connected floppy disk drive without a disk can create driver conflicts, leading to detection failures. Disabling or disconnecting such devices may resolve the issue.

Software or Hardware Glitch

Temporary software or hardware glitches may disrupt USB detection. Restart the Kiosk device and its services to see if the issue resolves.

USB Drivers or Windows Issues

Outdated or corrupted USB drivers can interfere with detection. Updating or reinstalling USB drivers, or reimaging the Kiosk, can resolve the issue.

Event Handling in Windows

Windows event message handling issues may prevent proper USB detection. Upgrading the Kiosk application or reimaging the device could resolve this.

Device Insertion Timing

All external USB devices, such as SD card readers and floppy disk drives, should be connected before starting the MetaDefender Kiosk application. Otherwise, they may not be recognized.

Unsupported Remote Operation

The Kiosk is designed for local use. Running it in a remote desktop session is unsupported and may result in detection failures.

By following these troubleshooting steps, you should be able to identify and resolve the issue preventing the Kiosk from detecting devices. If problems persist, consider reaching out to support for further assistance.

Support:
If Further Assistance is required, please proceed to create a support case or chat with our support engineer.

Why retrieving the Kiosk file history not working for sessions with a large number of files?

Issue

When exporting the Kiosk file history, the process seems to take an excessive amount of time and is never completed.

Cause

This issue occurs because Nginx has a default 3-minute wait period for the report to be generated. If the report includes sessions with a large number of processed files, it may exceed this time limit, leading to a timeout.

Solution

To resolve this issue, increase the `proxy_read_timeout` setting in the Nginx configuration file.

Steps to Modify the Nginx Configuration:

1. Locate the dynamic.conf file. By default, it is located at: C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\REST\conf\dynamic.conf
2. Open the file in a text editor with administrative privileges.
3. Increase the proxy_read_timeout value to a higher duration, such as 1200 seconds (20 minutes) or more, depending on your requirements.

Example Configuration:

```
rewrite /metadefender_rest/(.*)$ /$1 break;
proxy_pass http://127.0.0.1:8019;
proxy_send_timeout 180s;
proxy_read_timeout 1200s;
proxy_set_header Host $host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
```

4. Save the changes and restart the MetaDefender Kiosk service for the new settings to take effect.

After increasing the timeout, exporting the file history should be completed successfully even for large reports.

Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why am I experiencing a "Login Denied" error when attempting to send a test email for scan results from the MetaDefender Kiosk?

When you are configuring Email settings and receiving Login Denied error, this error is typically not coming from OPSWAT. There are a couple things that you can confirm to help resolve this issue:

1. Confirm that the username and password are entered correctly and there are no extra spaces or characters being added by accident. Also, manually type the username and password instead of copying and pasting.
2. Confirm that an App Password has been created for the SMTP account as necessary. Once an App password is created, then go ahead and re-enter the username and password.
3. If you are still running into Login Denied error, go ahead and check the Email Server logs to see the exact cause of the error.

Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why does OMVA agent not working as expected?

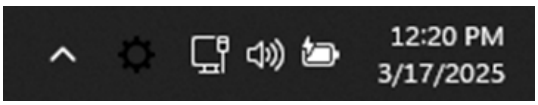
If you encounter scenarios where everything is setup correctly on the Kiosk/Core/OCM side regarding OMVA functionality as described below, please consider the following limitation that might be impacting OMVA functionality:

Due to faulty settings on the MetaDefender Core side

- Please make sure the “Skip hash calculation “is not enabled on the MetaDefender Core side on the workflow rule to avoid any OMVA inconsistencies.
- Having this option enabled on the MetaDefender Core workflow-rule will result in the media validation process involving the OMVA agent to not function as expected.

Due to faulty time-date settings on the OMVA device

- Please make sure the date/time is set up correctly on the OMVA machine (on an OS level) to avoid any OMVA inconsistencies.
- Having the wrong date/time setup on the OMVA (in comparison to the MetaDefender Core/Kiosk machine) device might result in the validation process not functioning as intended.



Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Which Kiosk Hardware Model am I using?

Check Your Version
This article applies to OPSWAT Kiosk Hardware only.

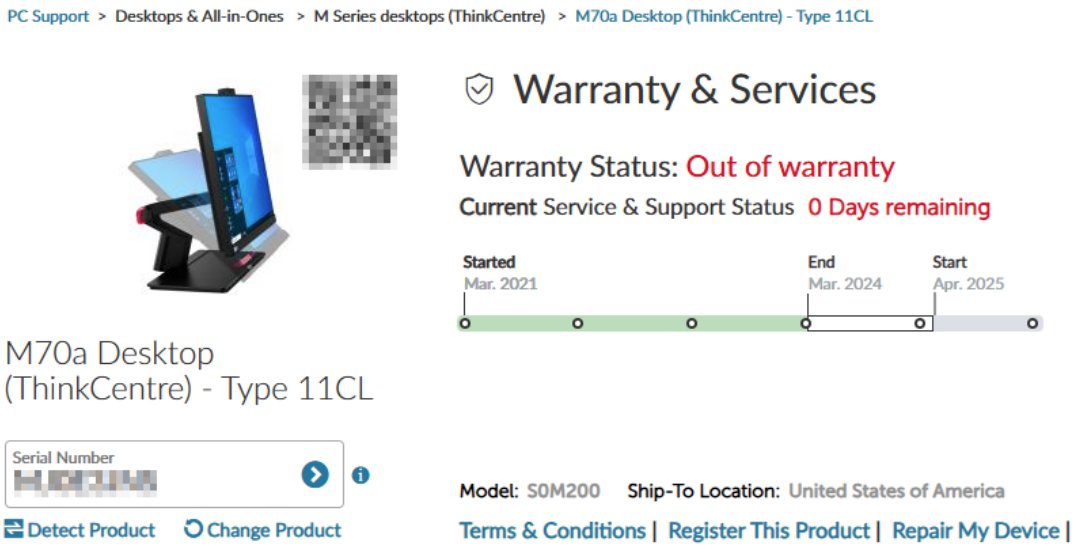
Kiosk hardware comes in multiple variants. The actual hardware models may vary over time. The list below shows the vendor hardware models associated with each kiosk hardware name.

Kiosk Category	Hardware Model	Vendor Hardware Model
Kiosk Tower (K3XXX)	K3000 (Obsoleted)	OptiPlex 5060 Small Form Factor
	K3001	OptiPlex 7000 (D17S)
		OptiPlex 7090 (D15S) (D17S)
		OptiPlex XE4 (D17S)
	K3001-CB	OptiPlex XE4 (D17S)
Kiosk Mobile (K2XXX)	K2001 (Obsoleted)	Surface Pro 7
	K2100	Dell 7220
		Dell 7230
Kiosk Desktop (K1XXX)	K1000 (Obsoleted)	Lenovo M820z
	K1001	Lenovo M70a (End of Sale)
		Dell 7410
		Dell 7420
Kiosk Mini	Kiosk Mini	Dell 7230
Kiosk L100x	L1001	Lenovo M70a (End of Sale)
		Dell 7410
		Dell 7420

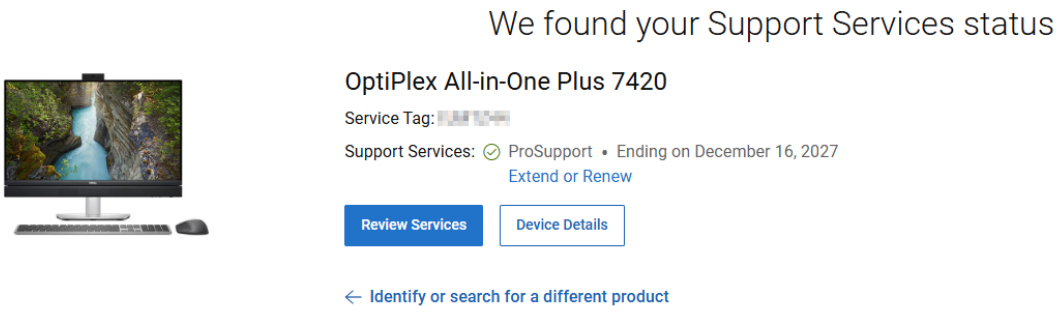
How do we verify the Vendor hardware model?

To verify the vendor hardware model, use the serial number (Service Tag for Dell) and check the warranty lookup page for complete hardware details.

Lenovo: Lenovo Warranty Check | Device Warranty Lookup | Lenovo Support US

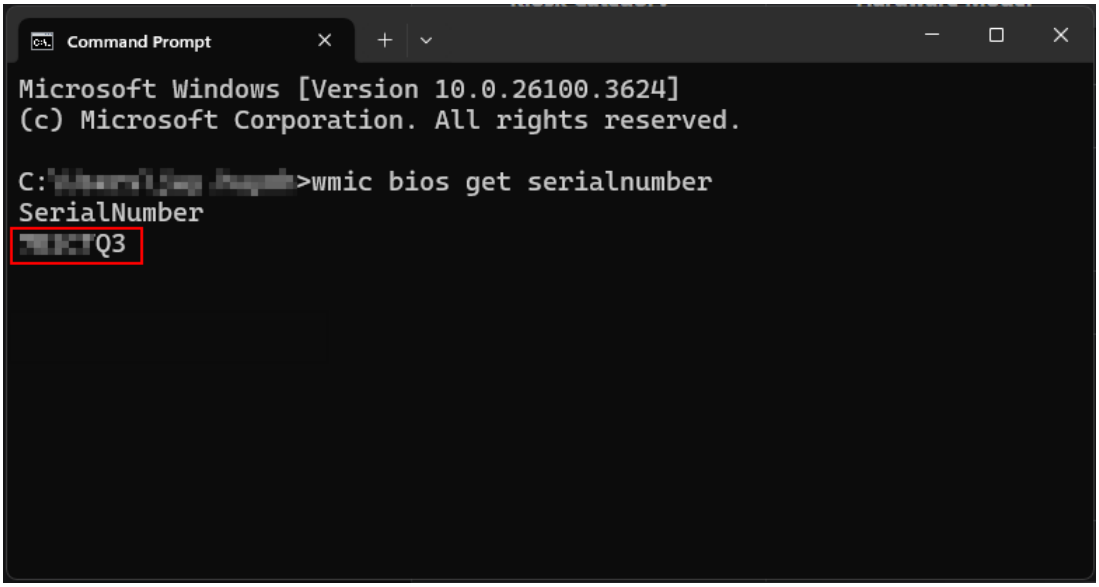


Dell: Support Services & Warranty | Dell US



Below are some methods to get the Serial Number (ServiceTag):

- Using CMD: **wmic bios get serialnumber**



- Locate the manufacturer's label and check for the Serial Number (Service Tag - Dell). Dell 7410:

Especially with K3001, you need to verify whether the Reg Model is D15S or D17S

Lenovo M70a:

Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why can I not execute script file like .VBS or .PS1.... in Hardened Image

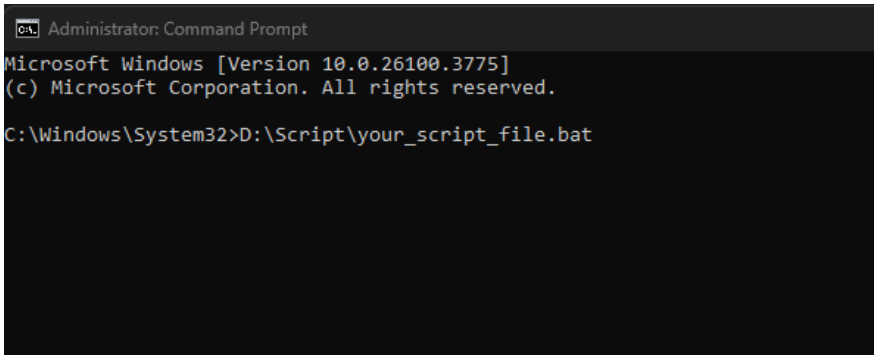
> **Check Your Version:**
> This article applies to all MD Kiosk Hardened Image versions

One of the security features of the Kiosk Hardened Image is the restriction of executable file types such as `.bat`, `.ps1`, `.vbs`, `.reg`, and others, which can run potentially harmful commands on the system. This helps prevent unauthorized execution and enhances protection of the Kiosk system at the backend.

How to resolve this situation:

To execute these file types on the Hardened Kiosk Image, you must manually open Command Prompt or PowerShell with administrator privileges, then run the file directly from the console.

For example:



> **Warning**
> There will be another restriction on other services like .vbs,... In those cases, please contact Support for further instructions.

> **Support:**
> If **Further Assistance** is required, please proceed to log a **support case or chat with our support engineer**.

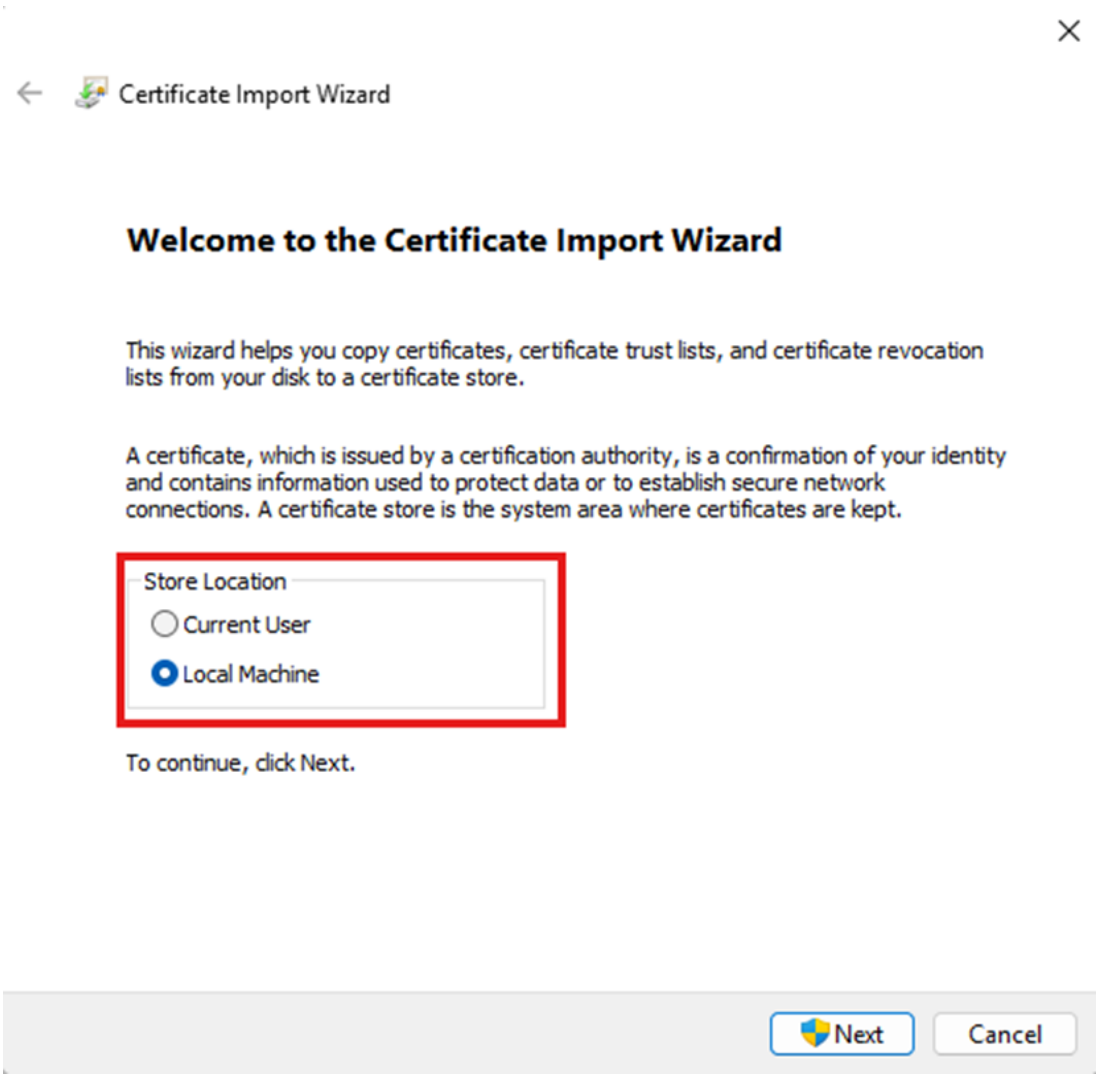
How do I resolve issues with OPSWAT Media Validation Agent not detecting USB after Certificate installed?

Issue:

When the user takes the USB drive that has been wiped by the Kiosk, then they scan the now empty USB drive, then plug it into a computer with OMVA installed, the customer is getting an error that says, unable to mount the USB drive. However, within the drive there is a .OPSWAT folder with the certification.

Solution:

Please confirm that when adding the certificate to the Trusted Root Certificate Authorities, that Local Machine option is selected and not the Current Users for the Store Location.



Steps to check via MMC:

1. Open MMC in Windows
2. Click on File
3. Click on Add/Remove Snap-in
4. Click on Certificate under the Available Snap-ins
5. Click on Add
6. Check to see if the Store location is set to Current User or Local Machine

How to retrieve OMVA logs:

After following the above steps the OMVA still cannot mount the USB drive, please submit a case to the support team. When submitting a case, please provide OMVA logs. Please follow the steps below on how to retrieve OMVA logs:

- OMVA logs JSON formatted messages of its operation. This can be used to determine the validation ran on the system and identify any media that was blocked.
- Logging can be found in the OMVA install directory: `%PROGRAMFILES(X86)%\OPSWAT\OPSWAT OMVA\LOG\omva_logs.json`
- When extracting logs from the file, the JSON objects must be wrapped within square brackets "**[ ]**" to allow for proper parsing

sample logging


```
{
    "date": "2021-04-22T17:28:11Z",
    "event_code": 0,
    "level": "info",
    "message": "USB inserted - Volume{0f1895d7-d714-4030-9b2c-3aeacb631d1b}",
    "hostname": "Workstation3186",
    "username": "company/userA",
    "user_data": "[Kiosk] SessionID: 81E60795-67D8-4A34-8792-90D6E403D039 || User: abc || System:
Kiosk1 || Device ID: SCSI\\DISK&VEN_MSFT&DISK\\2&1F4FFE&0&0001 || Start Time: 2021-07-08 16:10:01"
},
{
    "date": "2021-04-22T17:28:15Z",
    "event_code": 1,
    "level": "info",
    "message": "G:\\files\\spreadsheet.xlsx - File not found in Media Manifest",
    "hostname": "Workstation3186",
    "username": "company/userA"
},
{
    "date": "2021-04-22T17:28:20Z",
    "event_code": 2,
    "level": "info",
    "message": "Unable to mount drive, please rescan with MetaDefender Kiosk",
    "hostname": "Workstation3186",
    "username": "company/userA"
}
```


Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

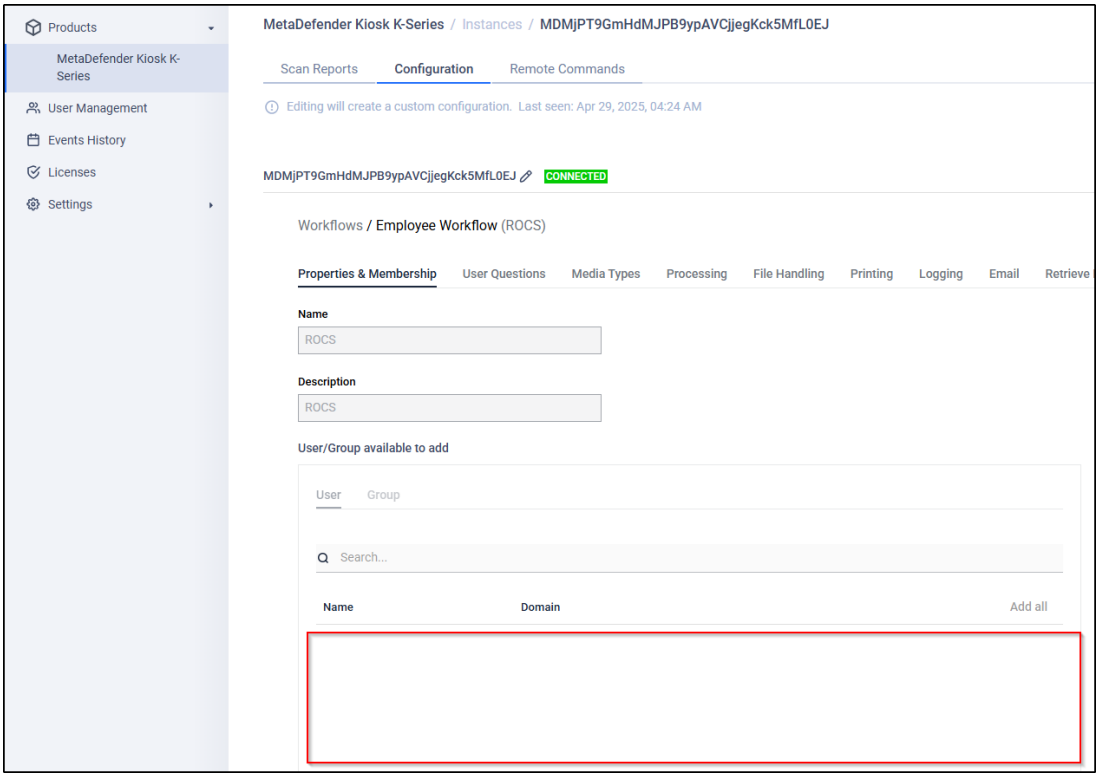
Why am I receiving "LDAP is unsupported" when trying to configure an AD server on a Kiosk instance managed by Central Management v8?

When managing a MetaDefender Kiosk instance using Central Management (OCM) v8 on-premises, you may encounter one of the following two scenarios when configuring an AD server:

1. **Error During Kiosk AD Configuration from OCM**

When configuring the Kiosk AD from within OCM, an error message stating **"LDAP is unsupported"** appears. This occurs even though the same AD settings work when configured directly on a standalone (non-managed) Kiosk instance.

2. **Empty Users and Groups After adding the Kiosk to OCM** If the AD was already configured on a Kiosk instance and that instance is later imported into OCM, the AD user and group lists may be empty. Attempts to revalidate the settings from the OCM side will result in the same **"LDAP is unsupported"** error.



Root Cause This issue occurs due to the format of the AD bind credentials or the need for anonymous bind support on the AD server.

Resolution

To successfully bind the Kiosk to Active Directory via OCM:

Option 1: Use Fully Qualified Bind Username

Ensure the bind username includes the domain, using either of the following formats:

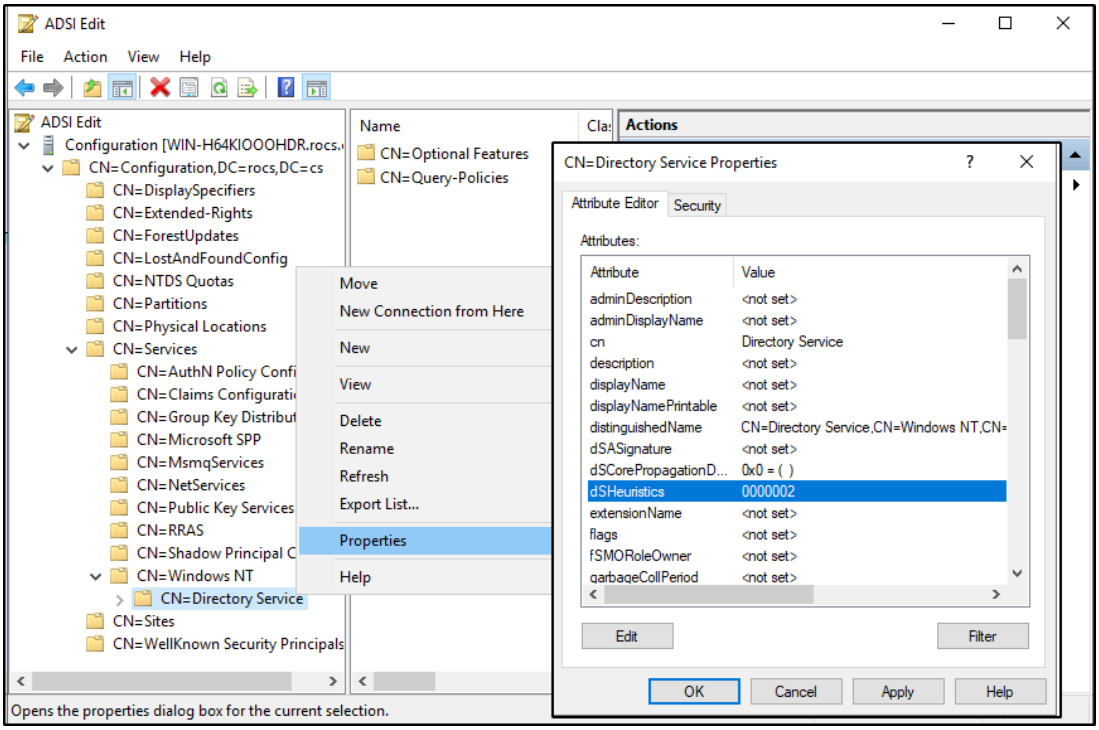
- `domain\username`
- `username@domain.test`

Option 2: Enable Anonymous Bind on Active Directory

If using a non-domain-qualified username, you must enable anonymous bind on the AD server:

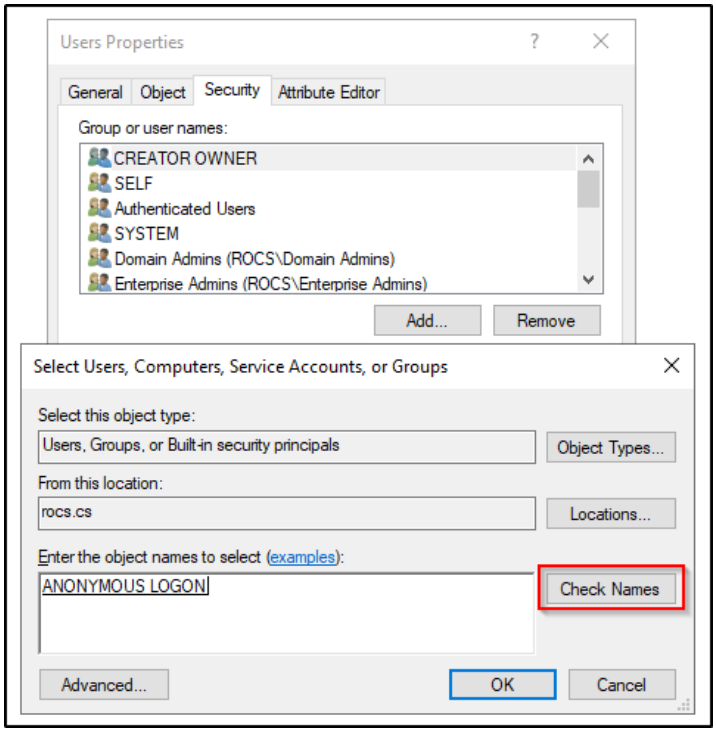
Step 1: Modify the dSHeuristics Attribute

1. Open **ADSI Edit** on the Active Directory server (`Start Menu > Search > ADSI Edit`).
2. Right-click **ADSI Edit** and select **Connect To...**
3. In “Select a well-known naming context,” choose **Configuration**.
4. Navigate to: `DC=<your domain>` > `CN=Configuration` > `CN=Services` > `CN=Windows NT` > `CN=Directory Service`
5. Open **Properties** of "Directory Service."
6. Set the `dSHeuristics` attribute to `0000002`. If it already has a value, modify only the **seventh digit** to `"2"`.



Step 2: Grant Read Permissions to Anonymous Logon

1. Open **Active Directory Users and Computers**.
2. Right-click the domain or relevant OU and select **Properties > Security**.
3. Add **ANONYMOUS LOGON** and grant **Read** permissions as needed.



Step 3: Verify Access

After completing these changes, confirm that anonymous users can access the intended directory parts without authentication and that the users and groups are available when configuring the Kiosk AD from Central Management v8

Security Considerations Enabling anonymous bind introduces potential security risks. Ensure:

- Access is limited to only the necessary directory objects and attributes.
- All changes align with organizational security policies and compliance standards.

Applies To

- MetaDefender Kiosk
- Central Management (OCM) v8
- Microsoft Active Directory

Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

How to resolve slow USB Detection on Kiosk Tower with Floppy Drive?

Symptom

In MetaDefender Kiosk versions 4.7.4 and prior, systems running MetaDefender Kiosk software, including the Kiosk Tower or devices with a connected floppy drive, encounter substantial delays in USB device detection.

Cause

By design, the Kiosk scans through all available drives during media detection. When a floppy drive is connected, the system may hang while attempting to detect it, significantly slowing down USB detection.

Solution

Upgrade to MetaDefender Kiosk version 4.7.5, which includes improvements to the USB detection process. Refer to Release Notes - MetaDefender Kiosk Windows for details. After upgrading, restart the system to apply the changes. Be aware that the first restart may take longer if a floppy drive is connected.

Notes

- This issue is specific to devices with a connected floppy drive, such as the Kiosk Tower.
- A system restart is required after upgrading to Kiosk 4.7.5 to apply the changes.

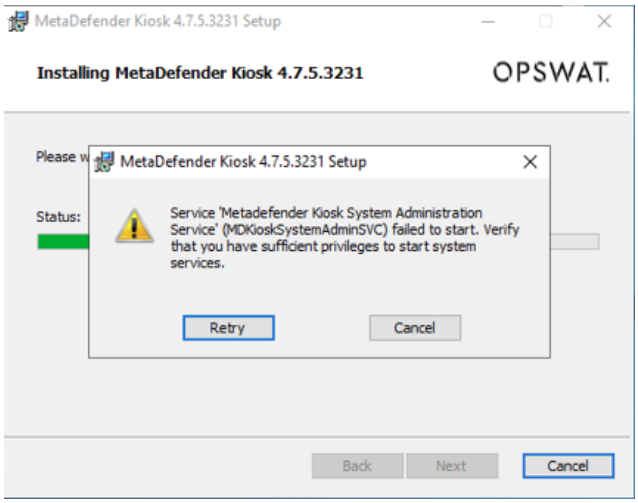
Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why does MetaDefender Kiosk System Administration Service fail to start?

Info:
This KB applies to new installations of MetaDefender Kiosk version 4.7.5 as well as upgrades from a previous version to 4.7.5

Starting with version 4.7.5, MetaDefender Kiosk enables administrators to configure network settings - including both Ethernet and Wi-fi - directly through the Kiosk Web Management Console (WebMC). If a machine does not have the **Wireless Networking feature** installed (Windows Server does not include it by default), the Kiosk service may fail to start. In such cases, the following error may be displayed

```
Service 'Metadefender Kiosk System Administration Service' (MDKioskSystemAdminSVC) failed to start. Verify that you have sufficient privileges to start system services.
```



Additionally, the Windows System Event log may contain the following entries:

```
A timeout was reached (30000 milliseconds) while waiting for the Metadefender Kiosk System Administration Service to connect.
```

The Metadefender Kiosk System Administration Service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion.

Solution

To resolve this issue, install the Wireless Networking feature as follows:

- Open PowerShell with administrative privileges
- Run the following command:

```
Install-WindowsFeature Wireless-Networking -Restart
```

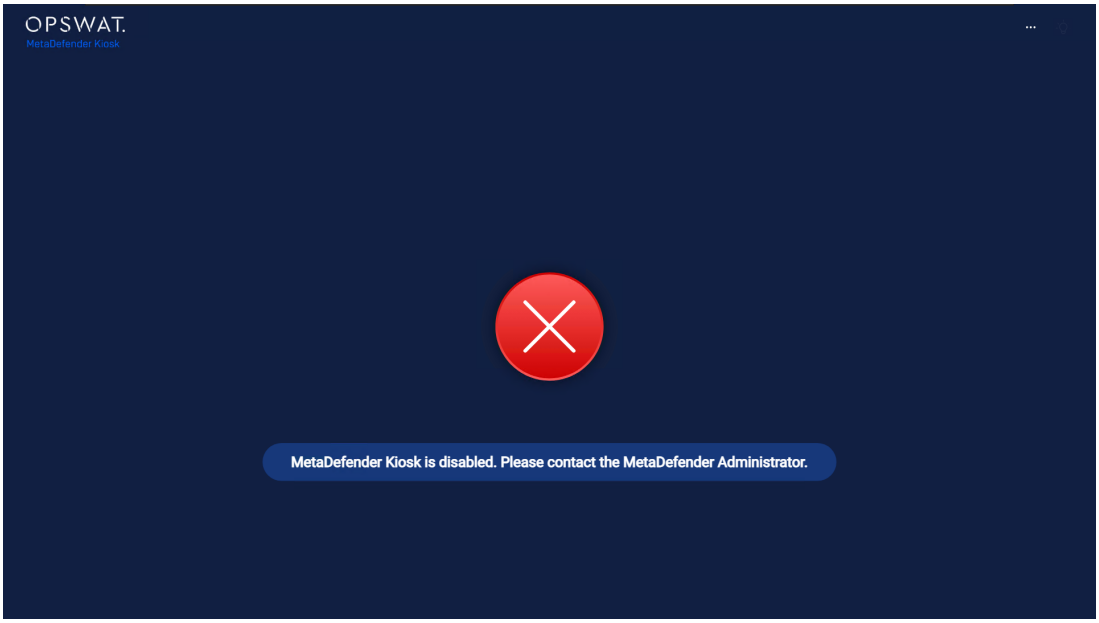
After the system restarts, proceed with the Kiosk installation or upgrade process again.

Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Why is my MD Kiosk disabled on Secure Image and how to resolve it?

Check Your Version:
This article applies to all MD Kiosk Secure Image versions

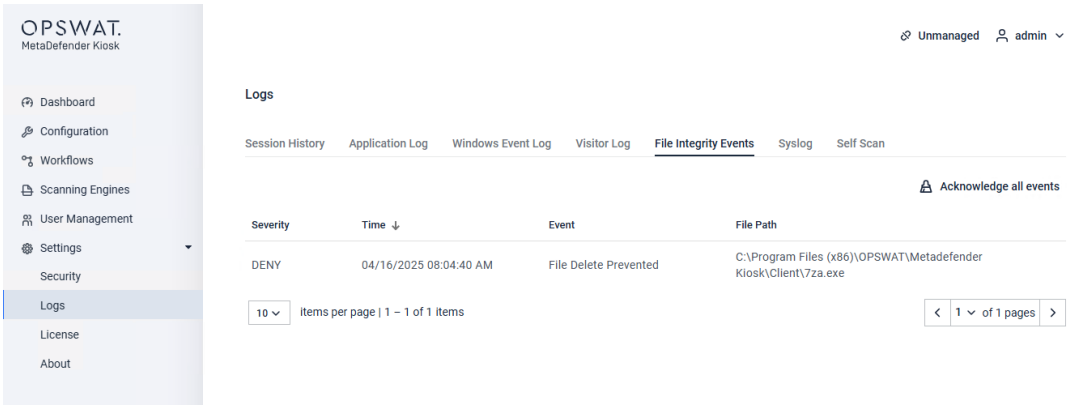
One of the unique features of the Secure Image is File Integrity Monitoring, which is integrated with the Kiosk UI. The system continuously monitors the Kiosk installation folder for unauthorized modifications. If any unauthorized action is detected, it will be blocked, a signal will be sent to the Kiosk service, and the Kiosk UI will be terminated immediately. The following error message will be displayed:



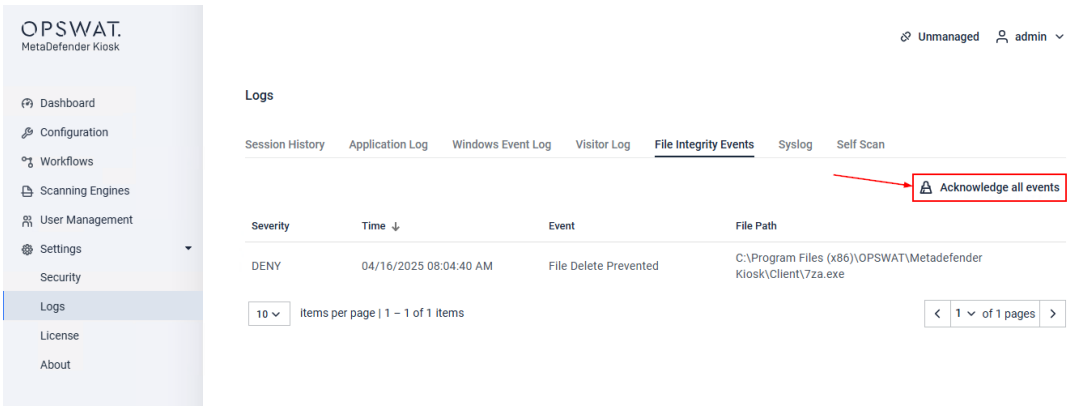
How to resolve this situation:

When this screen appears, the administrator must close the Kiosk UI to access the Kiosk console locally or connect to it remotely from another computer.

From the Console, find Settings > Logs > File Integrity Event. Then you will see the list of detected actions that caused the Kiosk disabled.



After verifying that the reason for the modification has been investigated, you can select **Acknowledge Event** to confirm and clear the existing alerts. You may then start the Kiosk launcher



Support:
If **Further Assistance** is required, please proceed to log a **support case or chatting with our support engineer**.

Overview

The Kiosk Hardened Image is a customized Windows operating system for the Kiosk series. Those hardened OS images are built to strengthen the Kiosks against cyberattacks by configuring the operating system and removing unnecessary applications. This method is also widely used in OT/ICS cybersecurity with following security-related task such as:

- Limiting access.
- Disabling unnecessary default features.

Benefits of Hardened Image

Security Enhancements

Improve security and reduce data breaches of MetaDefender Kiosk, prevent unauthorized access and malware by creating a secured system and reducing its attack surface, especially from unknown removable media devices brought to the critical facilities on a day-to-day operation.

Performance Breakthrough

Strengthen overall performance of the MetaDefender Kiosk by deleting unnecessary programs and services, and removing unneeded features that support to lower storage requirements and power consumption.

Deployment flexibility

Kiosk Hardened Image is expansive and adaptive to various OT/ICS organizations, and critical infrastructure worldwide, easy to deploy and install with MetaDefender Kiosk & MetaDefender Core altogether.

Compliance Need

Supports compliance with industry-specific regulations and standards.

Kiosk OOBE Initial Setup Guide

Overview

The Out-of-box Experience (OOBE) initial setup is available on the latest MetaDefender Kiosk Hardened Image (25.02.0) to streamline the configuration process. This step-by-step setup wizard guides users through essential settings, enabling quick and effortless setup without requiring advanced technical expertise.

Scope of support

- Kiosk Hardened Image (25.02.0 or later)
- Local MetaDefeder Core with bundled license
- Activation online or via My OPSWAT

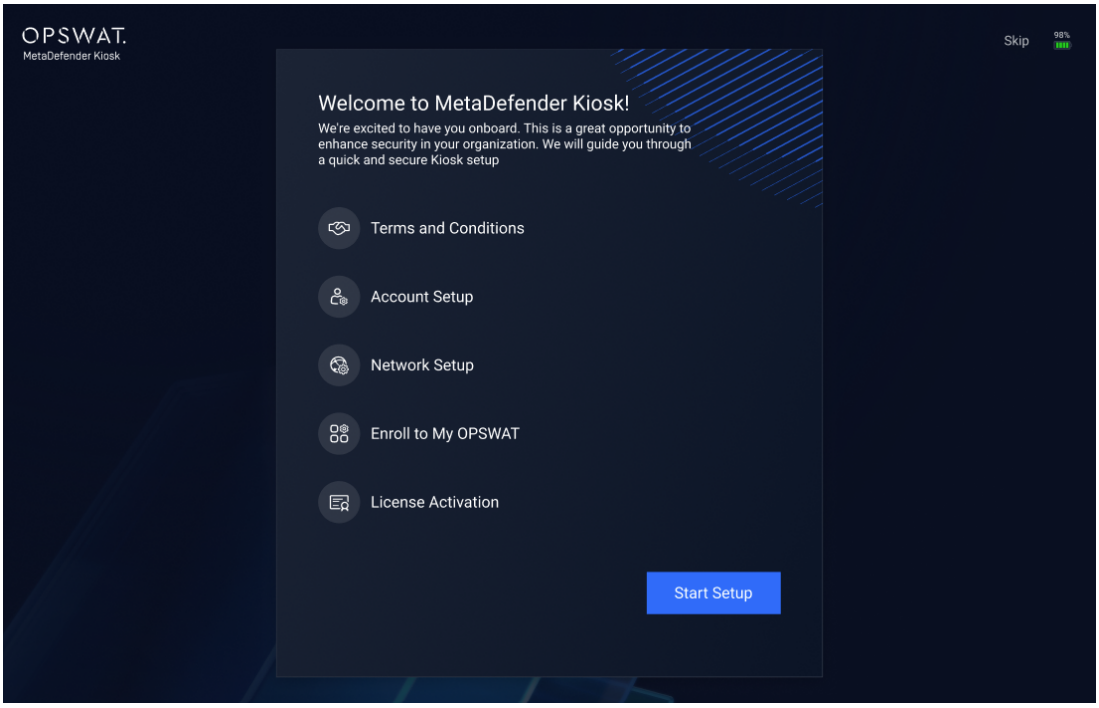
Kiosk Initial Setup

Step 1. Power on the Kiosk devices. Kiosk should automatically login and launch the OOBE wizard

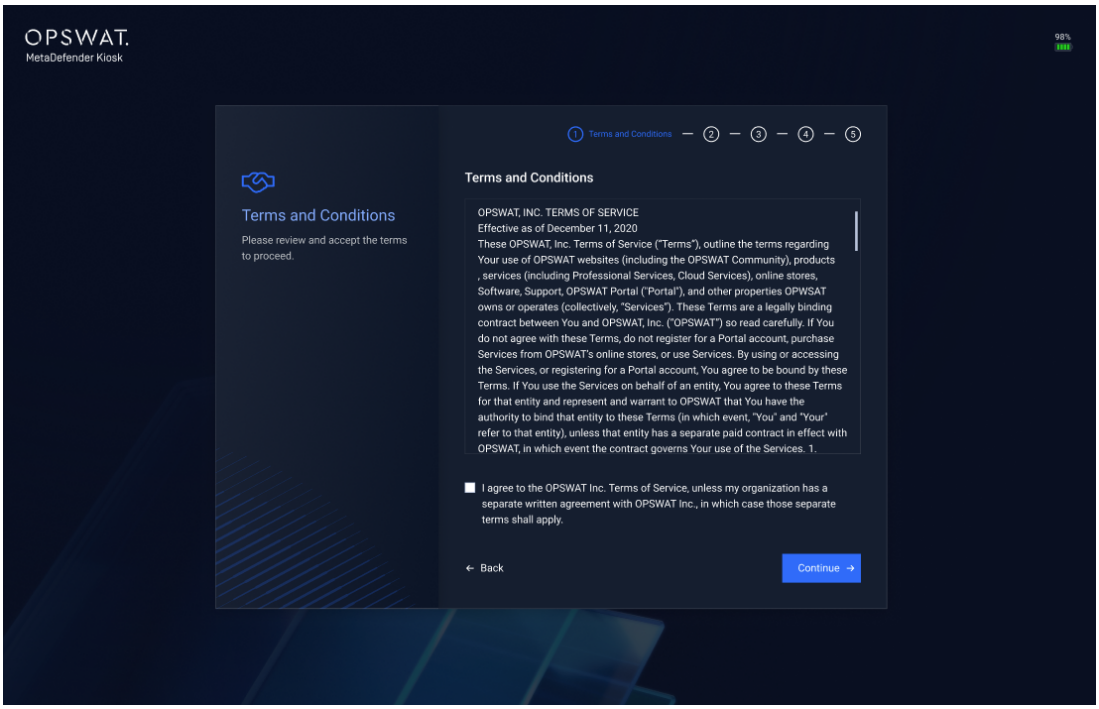
Exit Kiosk OOBE Wizard
Alt+S can be used to exit the OOBE Wizard to setup and configure Kiosk and Core manually. If you exit the Kiosk OOBE before an administrator account was created (step 2), Kiosk will automatically reopen the OOBE at the next Windows startup.

Default Windows login credentials
If for some reason, Kiosk device stopped at the Windows login screen, you can manually login with default credentials

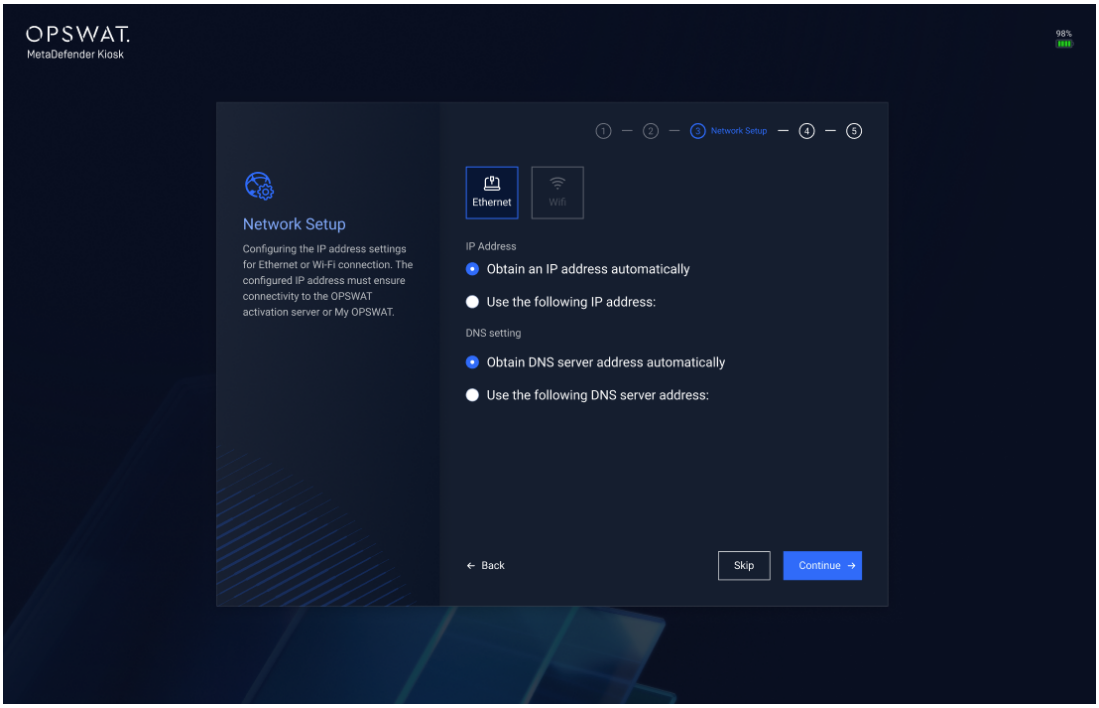
- **Username**: KioskUser
- **Password**: Contact the Customer Support to get the default password



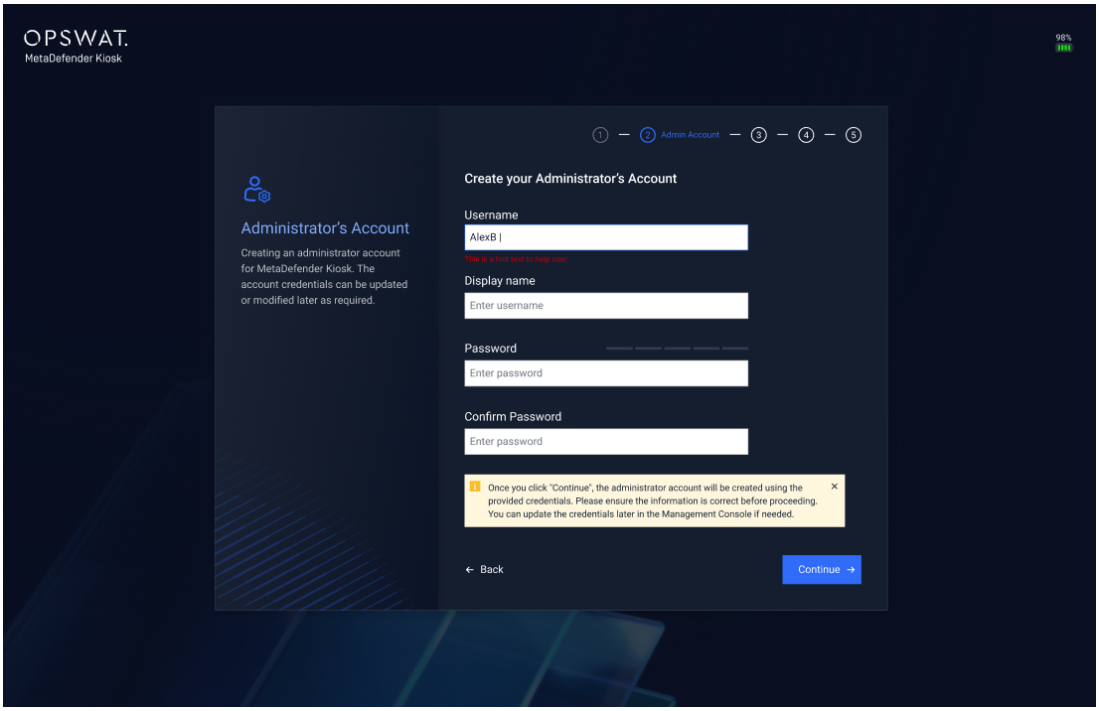
Step 2. Review and accept the End-User License Agreement by ticking the checkbox, then **Continue**



Step 3. Configure the network settings to connect to the internet



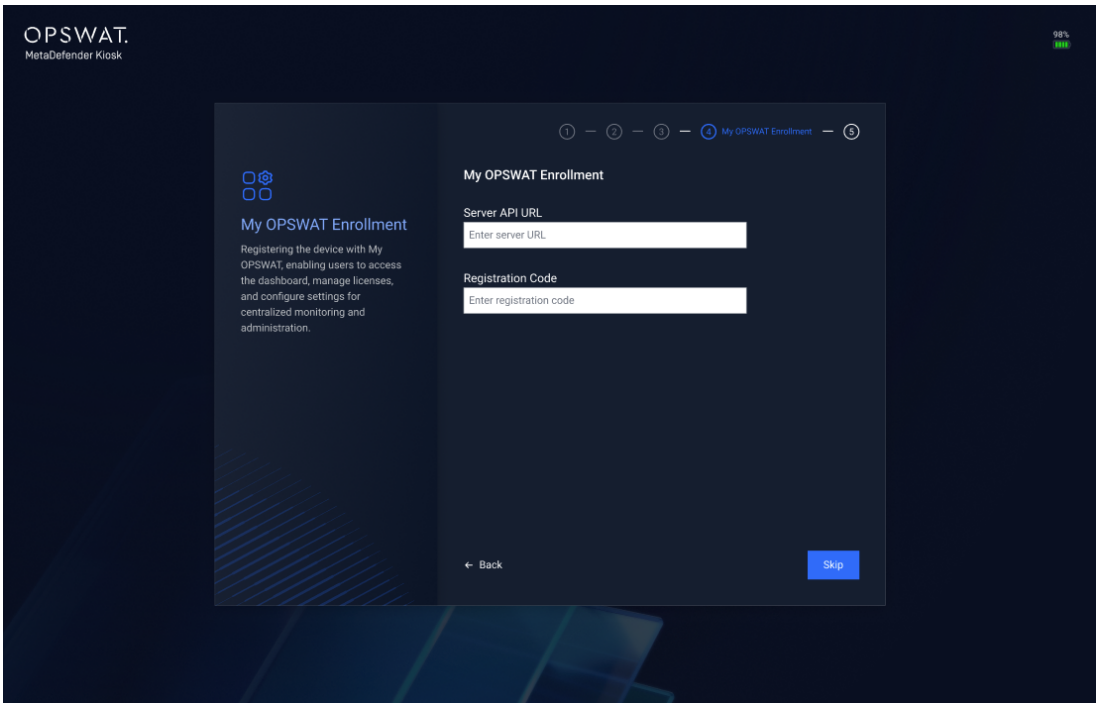
Step 4. Provide details to create an administrator account for MetaDefender Kiosk and Core applications



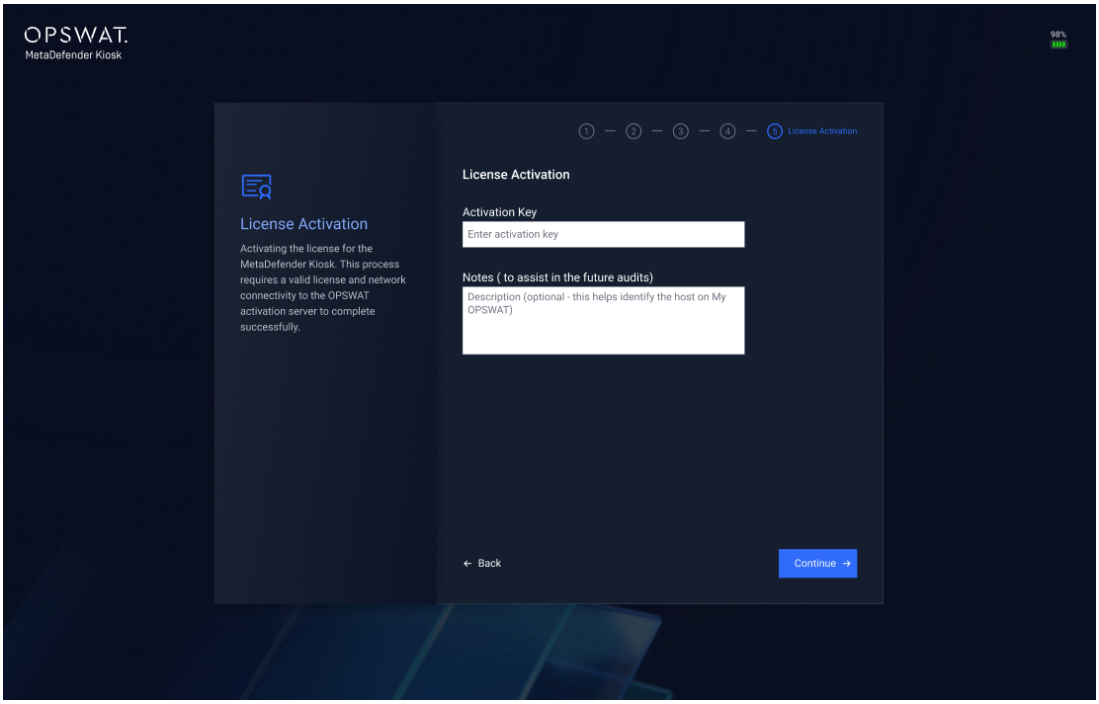
Step 5. (Optional) If you already have a My OPSWAT account, you can enroll the Kiosk device for streamlined license activation and management process.

My OPSWAT enrollment

If you do not have My OPSWAT account or do not want to enroll Kiosk to My OPSWAT, you can skip by clicking on **Skip** button.

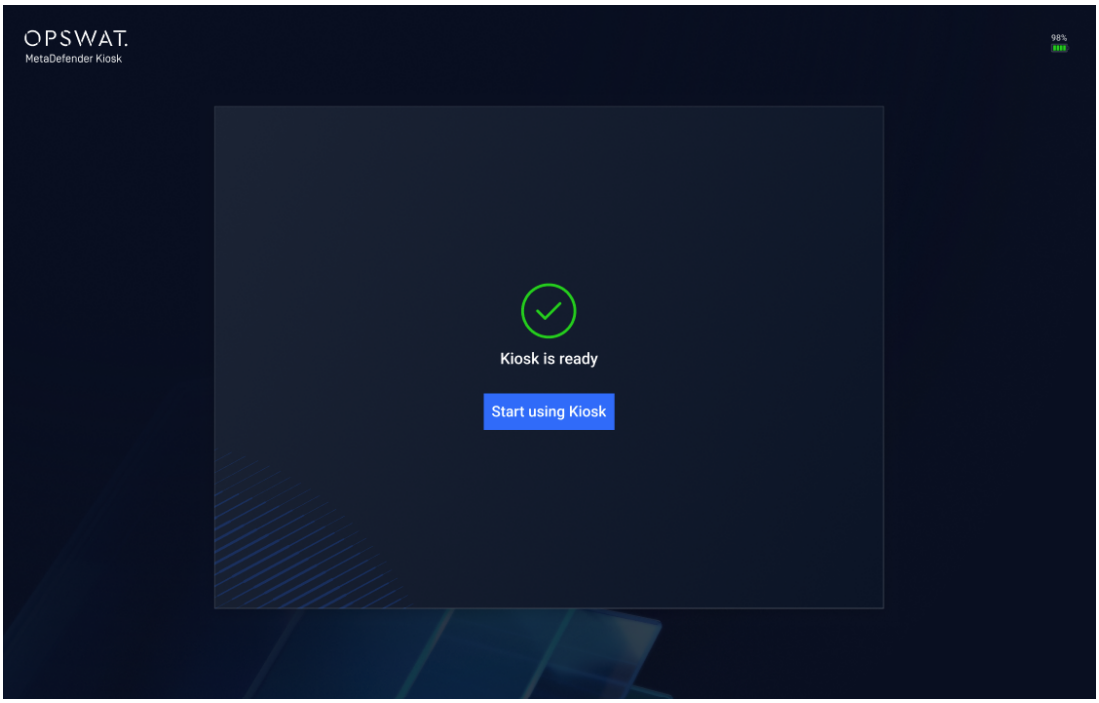


Step 6. Enter the bundled Kiosk license to activate the device

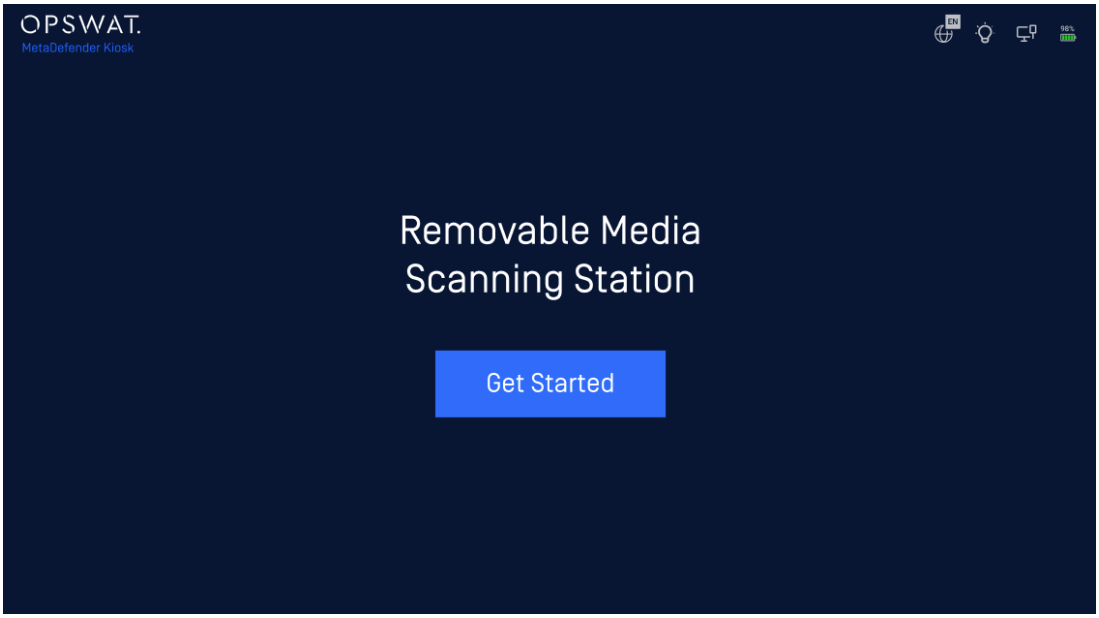


Step 7. The Kiosk will automatically download the required scanning engines based on the provided license.

Step 8. Once the scanning engines are successfully deployed, click **Finish** to complete the setup



Step 9. Kiosk will automatically launch the Kiosk UI and be ready to scan your media



MetaDefender Kiosk Hardened Image deployment

Follow the steps to create a bootable flash drive containing the hardened Kiosk image to facilitate the efficient deployment of MetaDefender Kiosk on various Kiosk hardware models

Requirements:

1. A PC running Windows 7/8/8.1/10 or 11
2. A USB flash drive with a storage capacity of at least 32GB.

Step 1: Download Deployment Tool and Kiosk Hardened Image

Download the following packages:

1. The Deployment Tool: WinPEBootable.vhd
2. Kiosk Hardened Image corresponding to the model of the device at My OPSWAT Portal. There are available images on Product Downloads page:
    a. Kiosk Tower:
        - K3001 - Dell 17s
        - K3001 - Dell 15s
    b. Kiosk Desktop:
        - K1001 - Lenovo M70a
        - K1001 - Dell 7410 Intel
    c. Kiosk Mobile:
        - K2100 - Dell 7220
        - K2100 - Dell 7230

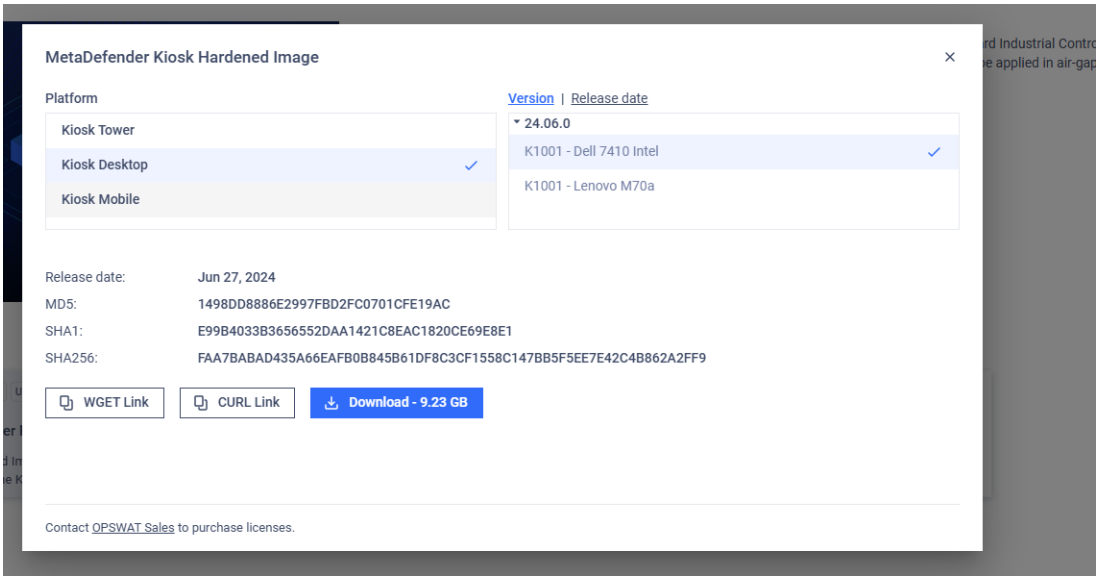


Image: Download page of MetaDefender Kiosk Hardemed Image on My OPSWAT Portal

Info
The download page for MetaDefender Kiosk Hardened Image on My OPSWAT Portal is accessible only to logged-in accounts in the Organization that has a valid license for MetaDefender Kiosk K-Series.

Step 2: Creating the Kiosk deployment flash drive

1. Create bootable USB

Download Rufus tool (version 3.15.1812 is recommended) to format and create bootable USB flash drive by the following steps:

1. Open Rufus and insert the USB drive.
2. Select your USB drive under "Device".
3. Click **SELECT** and select the downloaded **WINPEBootable.vhd**.
4. Click **START.**

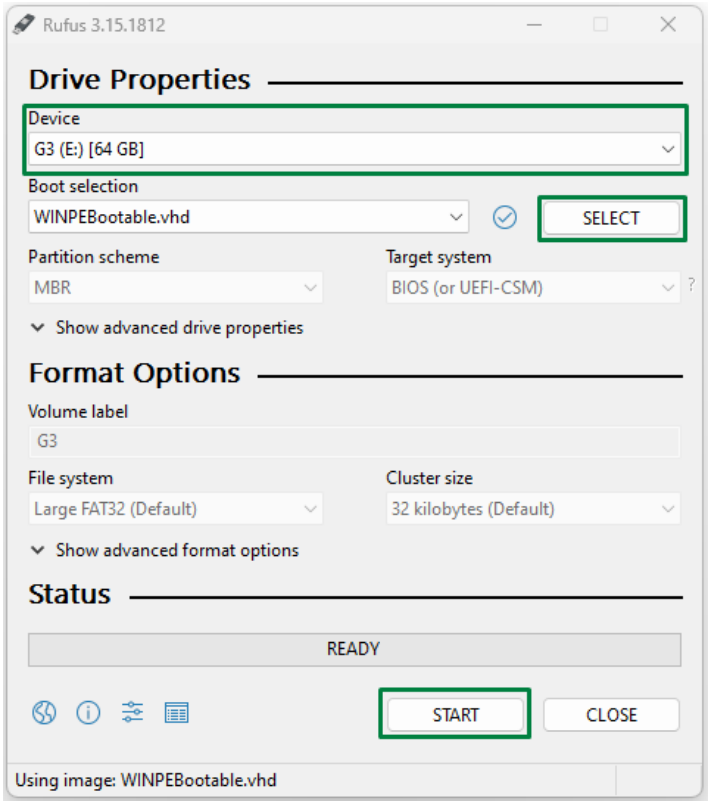


Image: Rufus 3.15 UI to create bootable USB

Please Note:
The USB flash drive will now be formatted, so any data on the drive will be lost.

The setup process takes around 20 minutes to complete.

2. Copy MetaDefender Kiosk Hardened Image

The USB now consists two partitions:

- **WINPE**: To store the WinPE files used for booting to winPE for deployment actions.
- **KioskImage**: To store the deployed image.

Copy the downloaded MetaDefender Kiosk Hardened image file (install.wim) to the **KioskImage** partition to finish the flash USB creation.

Step 3: Flashing a device with the bootable Kiosk USB drive

To install MetaDefender Kiosk on a new device by using your newly created Kiosk deployment flash drive, do the following:

1. Boot Into WinPE Environment

1. Plug USB into Kiosk Hardware

2. Restart/Power on the device.
3. Keep pressing F12 during booting up to open Boot Menu
4. Select the created USB as boot up media (base on device name)
5. Press enter.

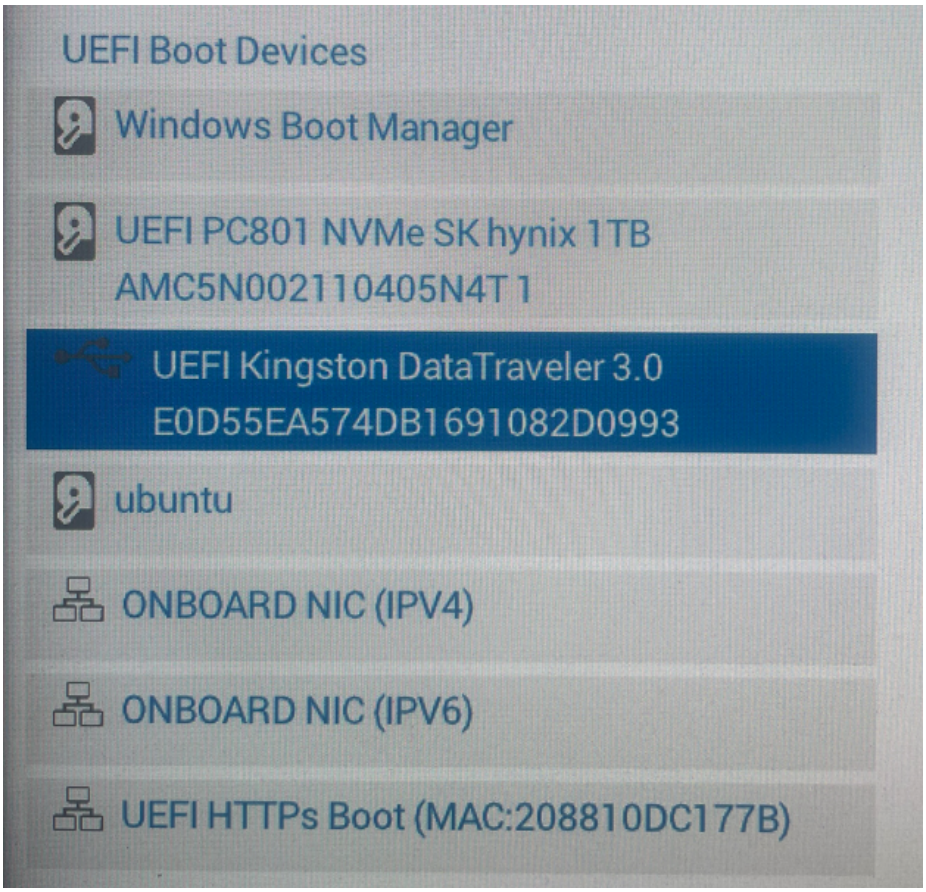


Image: UEFI boot Devices menu on BIOS

2. Deploy Hardened Image

Following the boot into the WinPE environment, a command prompt window will appear.

Please respond to the prompts in the command window:

1. Select the drive where you want to install the image. Keep in mind that all data on that drive will be permanently erased.
2. Decide whether you want to perform a full-pass wipe. Note that a full-pass wipe will take significantly longer.
3. Choose whether you want to restart the device once the installation is complete.

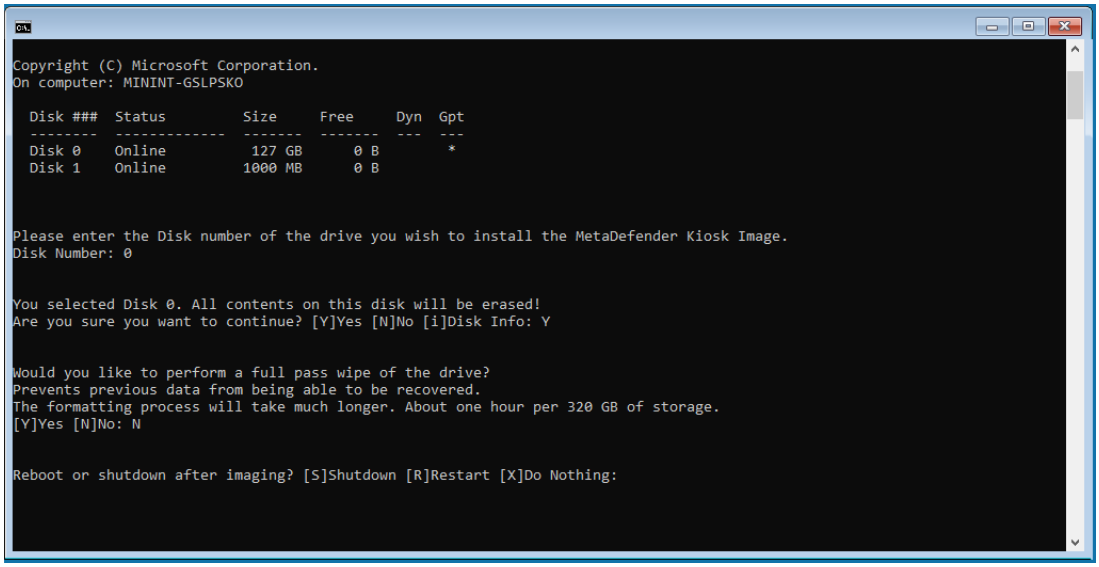


Image: Command prompt window on WinPE environment

Step 4: Post Installation Actions

- Change default log-in information for the local windows account:
  - **Username**: KioskUser
  - **Password**: Contact the Customer Support to get the default password.
- To activate MetaDefender Core, you will need to run the **Setup Wizard** on MetaDefender Core, as follows:
  - Go to http://localhost:8008 and follow the **Wizard** in order to create an account and activate MetaDefender Core.
- Connect Kiosk to MetaDefender Core by following the instructions Here.
- To activate MetaDefenderKiosk, you will need to run the **Setup Wizard** on MetaDefender Kiosk, as follows:
  - Go to http://localhost:8009/ and follow the **Wizard** in order to create an account and activate MetaDefender Kiosk.
- Finally, accept any changes from baseline in the Kiosk UI.

Support:
If you have followed the instructions above but are **Unable To Install And Run MetaDefender Kiosk Using A Bootable Kiosk Flash Drive**, please follow these instructions on How To Create a Support Package, before logging a Support Ticket with the OPSWAT team.

Kiosk Hardening

> **Info**
> OPSWAT recommends that the following additional setup is performed if MetaDefender Kiosk is deployed on a dedicated system.

Auto login

If MetaDefender Kiosk is being used on a dedicated system we recommend that the Windows system on the kiosk is configured to auto-login into the account with Administrator privileges that Kiosk will run with. If the Kiosk system is part of a domain additional steps may be required to allow this.

User Access Control (UAC)

OPSWAT recommends that UAC is disabled on systems that are being used as dedicated MetaDefender Kiosks. If UAC is not disabled MetaDefender Kiosk's watchdog functionality may not work correctly.

There are two ways to completely disable UAC in Windows:

By editing the registry

1. Click **Start** and type `regedit.exe` to open the Registry Editor
2. Navigate to the registry key at **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Policies > System**
3. Set `EnableLUA` to `0`
4. Restart Windows

By adjusting Local Group Policy settings

1. Click **Start** and type `gpedit.msc` to open the Group Policy Editor
2. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**
3. Right pane is populated with policies, locate the ones for User Access Control and set:
    a. **User Account Control: Only elevate executables that are signed and validated** → *Enabled*
    b. **User Account Control: Switch to the secure desktop when prompting for elevation**→ *Disabled*
4. Restart Windows

Windows Update

Install all patches and updates available through Windows Update. Once all updates are installed, OPSWAT recommends that automatic updates are turned off to prevent system reboots.

1. Navigate to **Start > Control Panel > Windows Update > Change settings**
2. Select **Never check for updates** from the menu
3. Click **Apply** or **OK** and close the dialog box

If turning off automatic updates is not desired, a process must be configured to restart the MetaDefender Kiosk system. We recommend using standard organizational patch practices and tools.

Setting the power saving options

Select the maximum performance power saving option.

1. Navigate to **Start > Control Panel > Power Options**
2. Click **Change plan settings**
3. Click **Change advanced power settings**
4. Select **High Performance** from the menu
5. Click **OK**

Disabling mouse cursor pointer

> **Info**
> This configuration is optional. Once these steps are taken, there will be no visible mouse pointer.

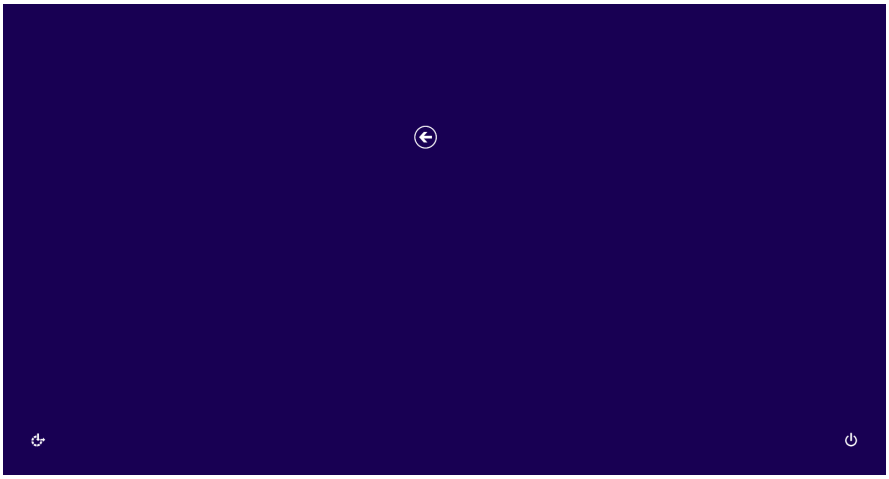
OPSWAT recommends that mouse cursor points are turned off after MetaDefender Kiosk has been configured. If the system touchscreen configuration software does not have this feature, it can be done manually by following the steps below:

1. Navigate to **Start > Control Panel > Mouse**
2. Click the **Pointers** tab
3. Browse to `C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\blank.cur`
4. Customize each pointer type to the provided blank pointer: `blank.cur`
5. Click **Apply** and close the dialog box.

Disabling hotkeys

By default, the Kiosk will ignore any command that is a combination of Ctrl and another key.

The `Ctrl + Alt + Del` combination is disabled once you launch the Kiosk. When a user presses these keys, it is expected to see a screen with no options displayed.



If you want to disable completely where nothing happens, please follow how to disable Windows hot keys.

Other system hardening configuration

MetaDefender Kiosk does the following system hardening when installed:

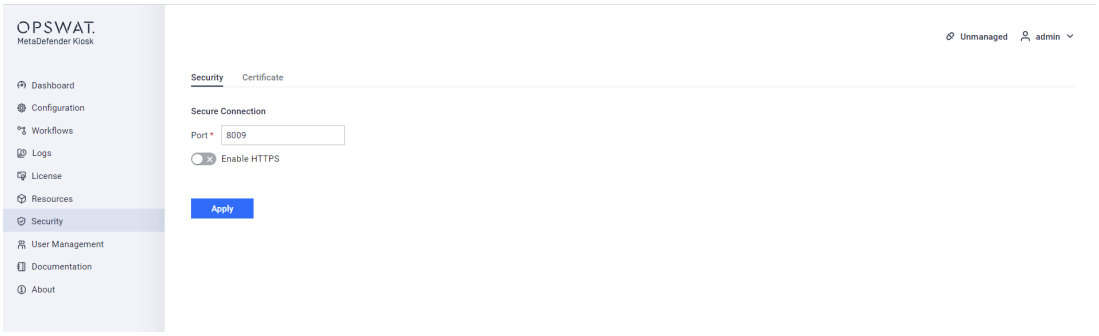
- Disables auto-run on all plug-and-play media and drives
- Captures and disables all hotkey combinations such as the `Windows Key`, `Alt+Tab`, etc... when Kiosk is running

Configuring the Web Server

MetaDefender Kiosk's Management Console relies on a REST interface which runs on HTTP by default. The following can be used to further configure the REST server to harden the system.

Changing the default port

1. From the management console navigate to the `Security` page (Administrator role is required to view this setting).



Change default port configuration

2. In `Port`, change the value to any port that is valid and click `Apply`

Setting up HTTPS

By default, communication with the Management Console is not encrypted. If HTTPS is enabled, the server can enforce secure connections between client and server on an SSL channel.

Prerequisites

- Kiosk version **must** be greater than or equal to **4.4.5**
- Must have a certificate on the kiosk system
- If the private key is encrypted you must create a file that contains the passphrase on the system
- Note down the file paths for the certificate, private key, and or passphrase file

How to create a self signed certificate (optional)

> **Info**
> This is for testing purposes only. Self signed certificates may have limited functionality due to the nature of self signing.

Using a terminal - with passphrase bash

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem
```

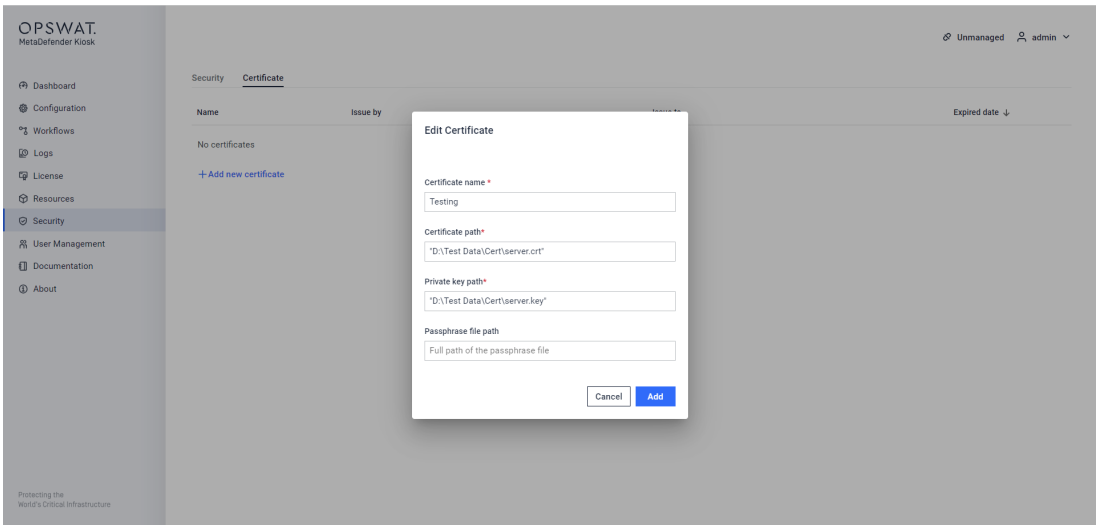
Then create your passphrase file and enter your passphrase into it.

Using a terminal - without passphrase bash

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -nodes
```

Adding a certificate

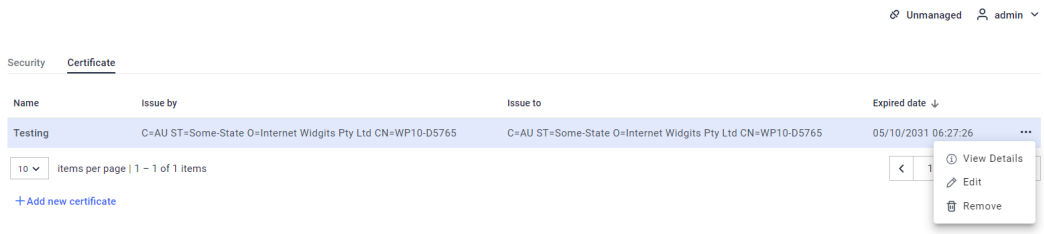
1. After completing the prerequisites you should have a certificate and private key on the system
2. From the management console navigate to the `Security` > `Certificate` page
3. Click Add new certificate
4. Fill the required input fields and click `Add`



Add Certificate on the KIOSK WebMC

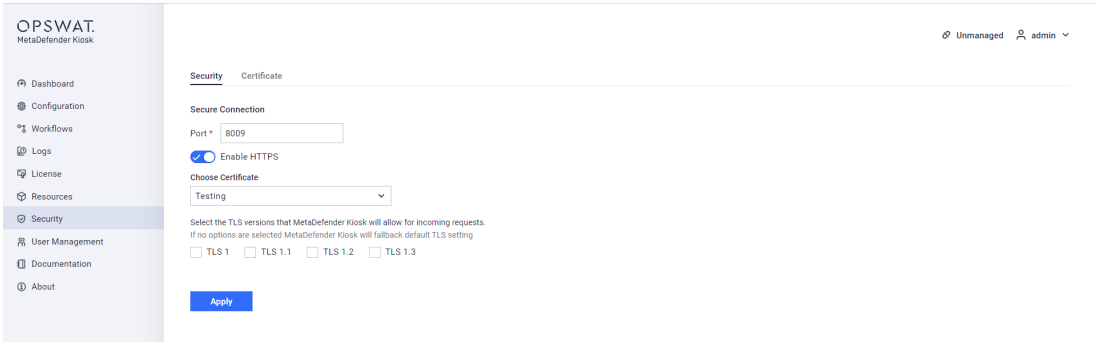
> **Info**
> Kiosk will validate these fields and display an error at the top of the screen if an issue is detected

The page will display the successfully added certificate, which can be modified or removed, except for the one currently in use.



Manage the added certificates

Enabling HTTPS



Enable HTTPS

1. From the management console navigate to the `Security` page
2. Click the `Enable HTTPS` checkbox
3. Select the preferred certificate
4. Choose the preferred TLS settings (if no options are selected then Kiosk will fall back to default TLS settings)
5. Click `Apply`
6. The Kiosk will restart its internal components and apply the changes selected

> **Info**
> This process may take approximately one minute to complete

7. Once the Kiosk services have restarted, a new tab should open that directs to the Kiosk page. If the tab does not automatically open, then click the hyperlink on the results page to open the new tab.

Disabling Windows Hot Keys

You can completely disable Windows hot keys `Ctrl+Alt+Delete` and `Windows+L` from performing any actions when pressed.

Disabling Ctrl+Alt+Delete

1. You must first disable `Windows secure logon`, so that you do not need to press `Ctrl+Alt+Delete` from the Windows login screen. Use one of the following procedures:

- Windows 7
- Windows 8
- Windows 10
- Windows 2008

2. While signed in as an Administrator, open the command line and run the following command:

none

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Keyboard Layout" /v "Scancode Map"
/t REG_BINARY /d 00000000000000000300000004de01de04be01d0000000000 /f
```

3. Log out of the system and log in again. To re-enable `Ctrl+Alt+Delete`, run the following command line.

none

```
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\Keyboard Layout" /v "Scancode
Map" /f
```

Disabling Windows+L

Run the following command line:

none

```
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
"DisableLockWorkstation" /t REG_DWORD /d 1 /f
```

To re-enable `Windows+L`, run the following command line:

none

```
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
"DisableLockWorkstation" /t REG_DWORD /d 0 /f
```

Boot Hardening Option

Purpose

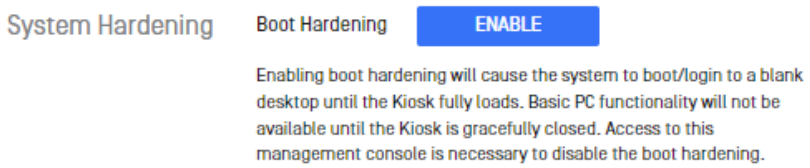
This article document shows how to enable “Boot Hardening Option” for MetaDefender Kiosk during system configuration.

Solution

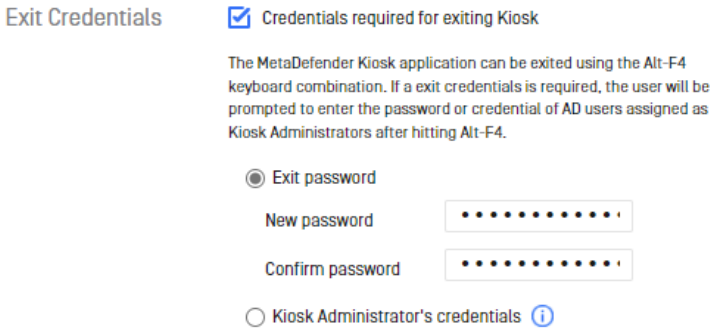
To set up “Boot hardening option” in MD Kiosk, please read through the following guidance for step-by-step instructions.

Setup Progress	Description
Step 1	Access to Kiosk Web Management Console
Step 2	Choose "Configuration" tab.
Step 3	Click Advanced Configuration on the webpage.
Step 4	Click "Enable" button to activate Boot Hardening option in "System Hardening" category. Enabling boot hardening will cause the system to boot/login to a blank desktop until the Kiosk fully loads. Basic PC functionality will not be available until the Kiosk is gracefully closed. Access to this management console is necessary to disable the boot hardening.
Step 5	Enable "Exit Credentials" function by clicking Credentials required for existing Kiosk. The MetaDefender Kiosk application can be exited using the Alt+S keyboard combination. If a exit credentials is required, the user will be prompted to enter the password or credential of AD users assigned as Kiosk Administrators after hitting Alt+S.
Step 6	Click "Apply"

Screenshot



Picture 1: Enable "Boot Hardening" option on Configuration page.



Picture 2: Activate "Exit Credentials" to combine with "Booth Hardening" option for better protection.

Detail benefits when enabling "Boot hardening option" in MD Kiosk

· Prevent unauthorized users from accessing desktop functionalities on PC.

· AD can access to desktop after gracefully close Kiosk applications by Alt+S.

Detail benefits when activate "Exit Credentials" function in MD Kiosk

· Prevent unauthorized personnels to turn off Kiosk functions on the device.

· Guarantee continuous system operation without disruption.

Support

If you encounter any problems with this guide or if the steps provided do not work, please contact [OPSWAT Support] (https://www.opswat.com/support).

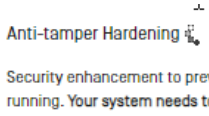
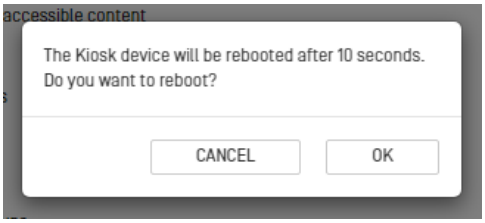
Anti-tamper Hardening Option

Purpose

This article document shows how to enable “Anti-Tamper Hardening Option” for MetaDefender Kiosk during system configuration.

Solution

To set up “Anti-tamper hardening option” in MD Kiosk, please read through the following guidance for step-by-step instructions.

Setup Progress	Description
Step 1	Access to Kiosk Web Management Console
Step 2	Choose "Configuration" tab.
Step 3	Click Advanced Configuration on the webpage.
Step 4	Click "Enable" button to activate "Anti-tamper Hardening" option in "System Hardening" category. A spinner appears when KIOSK is doing the secure enhancements on the system. 
Step 5	Then click RESTART button for the changes to take effect. And click OK to confirm, your KIOSK will restart. 
Step 6	Click "Apply"

Detail benefits when enabling “Anti-tamper hardening option” in MD Kiosk

When enabling the feature, default Windows input compounds will be blocked and cannot be exploited to escape KIOSK mode. The following default Windows hotkeys/shortcuts will be disabled (besides the ones being mentioned in https://docs.opswat.com/mdkiosk/operating/disabling-windows-hot-keys)

- Filter keys
- Sticky keys
- Toggle keys
- Mouse keys

- High Contrast shortcut
- Ctrl - Shift - Esc
- Other Winkey compounds
- Edge Swipe, Cortana, On-screen keyboard, Magnifier

To exit the KIOSK application, press Alt+S, this is the only method to terminate the KIOSK application.

Active Keyboard Filter

> **Info**
> The "Active Keyboard Filter" feature is only available when "Anti-tamper Hardening" is enabled.

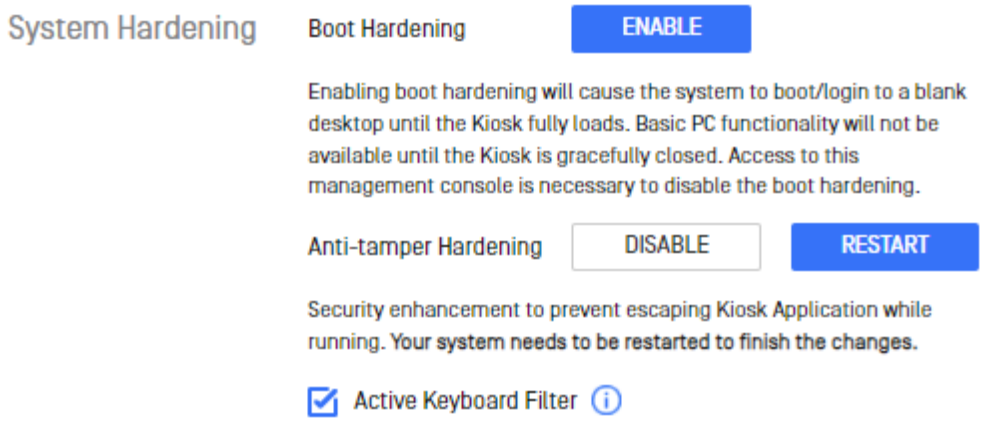
Default Configuration: By default, when the "Active Keyboard Filter" option is not enabled, users can utilize most of the Windows key combinations without any restrictions.

Enabling "Active Keyboard Filter": Upon enabling the "Active Keyboard Filter," KIOSK will block the majority of keys/key combinations on Windows to enhance system security. KIOSK will only allow the following keys/key combinations to function:

- Keys from A to Z
- Keys from 0 to 9
- Ctrl + C
- Ctrl + V
- Alt + S
- Shift
- Caps Lock
- Backspace

This restriction aims to strengthen the system's protection by limiting keyboard inputs to essential and secure commands. Users are encouraged to carefully consider the implications of enabling the "Active Keyboard Filter" option for their specific security requirements.

> **Warning**
> The Kiosk UI needs to be restarted for this option to take affect.



Support

If you encounter any problems with this guide or if the steps provided do not work, please contact [OPSWAT Support] (https://www.opswat.com/support).

Network Hardening Policies Option

Purpose

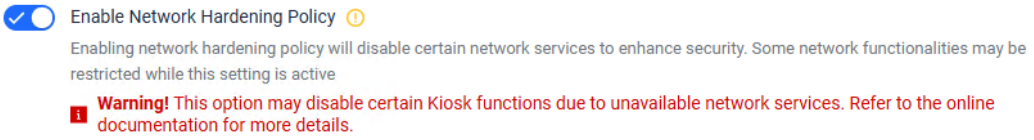
This article document shows how to enable “Network Hardening Policies Option” for MetaDefender Kiosk during system configuration and what changes will be applied.

Solution

To set up “Network Hardening Policies Option” in MD Kiosk, please read through the following guidance for step-by-step instructions.

Step 1. Access Kiosk WebMC, navigate to Settings, select System Hardening

Step 2. Enable Network Hardening Policies, then click Save Setting. A prompt will appear requesting a system restart.



Step 3: Restart the machine to apply the setting.

System changes when the option is enabled

When the **Network Hardening Policies** option is enabled, certain network-related services will be disabled to enhance system security. As a result, some Kiosk functionalities that rely on these services may be limited or unavailable. Below is a list of affected features

Feature	Use case	Network Hardening Policies is disabled	Network Hardening Policies is enabled
Activation	Activate license online	✔	
Engine Update	Update scanning engine online	✔	
File processing with the local Core	Process files with the local MD Core	✔	✔
File processing with the remote Core	Process files with the remote MD Core	✔	
Active Directory	Login to Kiosk with Active Directory accounts	✔	
Encrypted USBs	Process files on encrypted USBs	✔	✔
USBs with multiple partitions	Process files in media multiple partitions	✔	✔
Virtual disks (VHD, VMDK, TIB)	Process files on virtual disk (VHD, VMDK, TIB)	✔	✔
Phone, CD, DVD, Blue-ray, Floppy Disk	Process files on different media types (Phone/CD/DVD/Blu-ray/Floppy Disk)	✔	✔
MFT Integration	Process, send and retrieve files with MFT	✔	
Shared folder	Copy files and save session logs to a shared folder	✔	
Secure connections (HTTPS)	Enable Secure Connections (HTTPS)	✔	✔
Watchdog	Watchdog to monitor the system behavior	✔	✔
Email notification	Send email notification for the scan completion	✔	
Syslog	Integrate with syslog server	✔	

Feature	Use case	Network Hardening Policies is disabled	Network Hardening Policies is enabled
System hardening	Enable other Kiosk system hardening options	✔	✔ (except for RDP feature)
Windows Firewall	Turn on/off Windows Firewall service	✔	✘ (Firewall service is disabled)
Network and IP Address	Configure Kiosk's IP address	✔	✘
Export/import Kiosk configurations	Export or import Kiosk configuration files	✔	✔
Kiosk Hardened Image Upgrade	Upgrade Kiosk Hardened Image online or via Folder	✔	✘

Following network-related services will be disabled:

Service	Default Status	When Network Hardening Policies is enabled
AJRouter	Manual	Disabled
ALG	Manual	Disabled
BFE	Automatic	Disabled
BITS	Manual	Disabled
CDPSvc	Manual	Disabled
cloudidsvc	Manual	Disabled
CscService	Manual	Disabled
Dhcp	Automatic	Disabled
Dnscache	Automatic	Disabled
DoSvc	Manual	Disabled
dot3svc	Manual	Disabled
DsSvc	Manual	Disabled
DusmSvc	Manual	Disabled
Eaphost	Manual	Disabled
edgeupdate	Automatic	Disabled
edgeupdatem	Manual	Disabled
fdPHost	Manual	Disabled
FDResPub	Manual	Disabled
IKEEXT	Manual	Disabled
InstallService	Manual	Disabled
Intel(R) Capability Licensing Service TCP IP Interface	Manual	Disabled
iphlpsvc	Automatic	Disabled
IpxlatCfgSvc	Manual	Disabled

Service	Default Status	When Network Hardening Policies is enabled
McpManagementService	Manual	Disabled
MicrosoftEdgeElevationService	Manual	Disabled
MSDTC	Manual	Disabled
NcaSvc	Manual	Disabled
NcbService	Manual	Disabled
NcdAutoSetup	Manual	Disabled
Netlogon	Manual	Disabled
Netman	Manual	Disabled
netprofm	Manual	Disabled
NetSetupSvc	Manual	Disabled
NgcCtnrSvc	Manual	Disabled
NgcSvc	Manual	Disabled
NlaSvc	Automatic	Disabled
nsi	Automatic	Disabled
PeerDistSvc	Manual	Disabled
PolicyAgent	Manual	Disabled
PrintNotify	Manual	Disabled
QWAVE	Manual	Disabled
RasMan	Automatic	Disabled
SharedRealitySvc	Manual	Disabled
shpamsvc	Manual	Disabled
SmsRouter	Manual	Disabled
SNMPTRAP	Manual	Disabled

Service	Default Status	When Network Hardening Policies is enabled
SstpSvc	Manual	Disabled
TrkWks	Manual	Disabled
W32Time	Manual	Disabled
Wcmsvc	Automatic	Disabled
wcncsvc	Manual	Disabled
WebClient	Manual	Disabled
WEPHOSTSVC	Manual	Disabled
WFDSConMgrSvc	Manual	Disabled
WinHttpAutoProxySvc	Manual	Disabled
WlanSvc	Automatic	Disabled
wlpasvc	Manual	Disabled
WManSvc	Manual	Disabled
workfolderssvc	Manual	Disabled
WPDBusEnum	Manual	Disabled
WwanSvc	Manual	Disabled

Enable Windows Defender within Kiosk

Kiosk can detect Windows Defender. In such a case, Kiosk will add an exclusion list, which is all volume characters from C to Z. The exclusion list will prevent Windows Defender from scanning and quarantining files from USB.

In a domain joined computer, the administrator could configure tamper protection to protect security settings. Kiosk will not have the ability to change the exclusion list of Windows Defender.

You can check the status of Windows Defender tamper protection by the following PowerShell command.

```
Get-MpComputerStatus | Select-Object -ExpandProperty TamperProtectionSource
```

If it returns "Signatures", it means the tamper protection is controlled by local source and could apply changes from local.

Enabling BitLocker for KIOSK Hardened Image

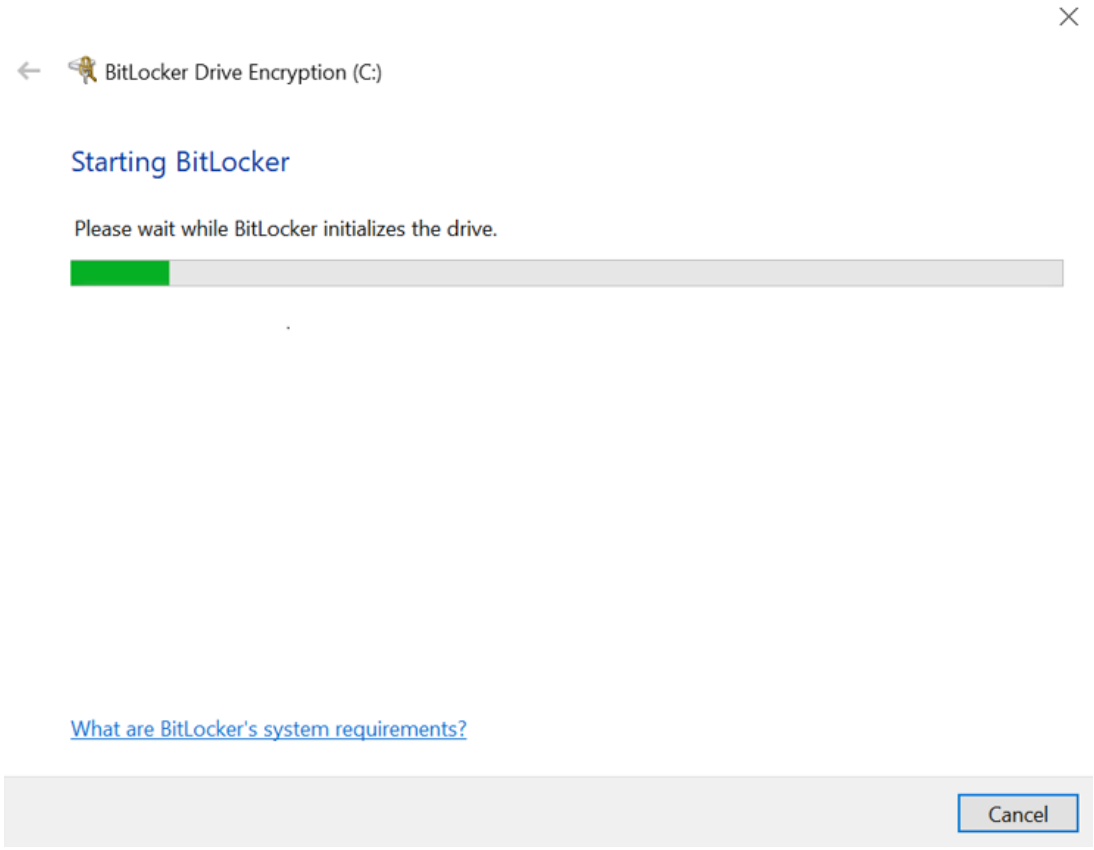
> **Info**
> By default, Hardened Image devices do not have BitLocker enabled. Admins can enable BitLocker by following the steps below.

Step 1: Open Control Panel from the system's Start menu.

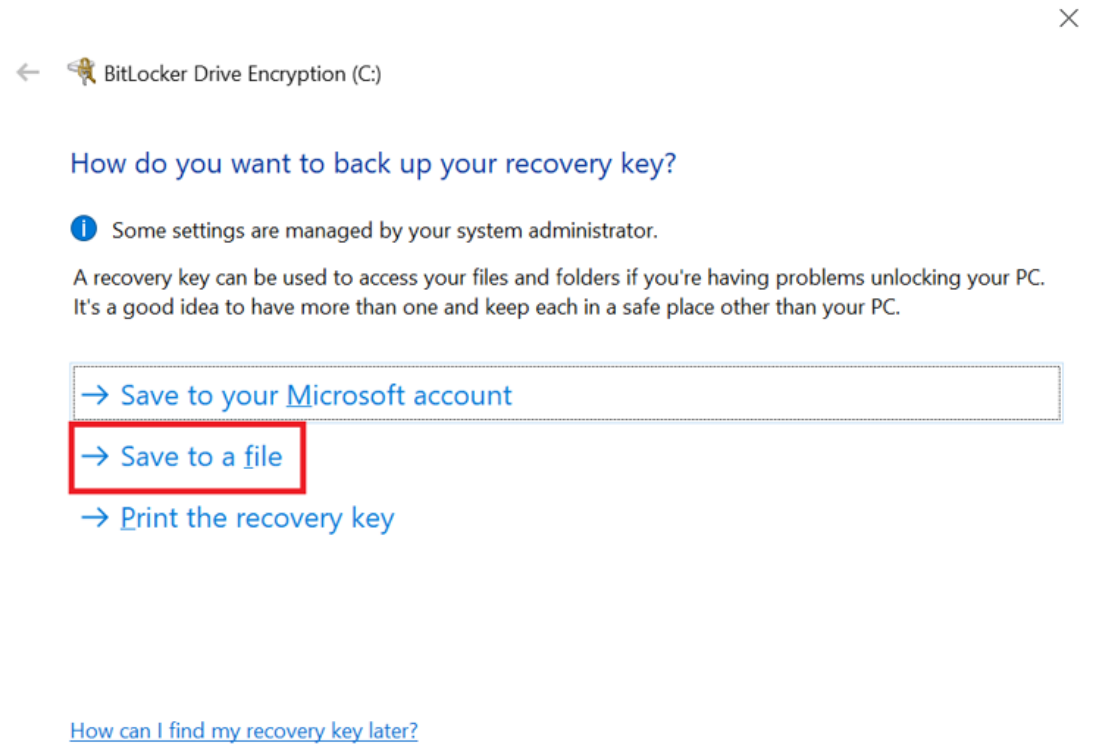
Step 2: Navigate to System and Security, then select BitLocker Drive Encryption.

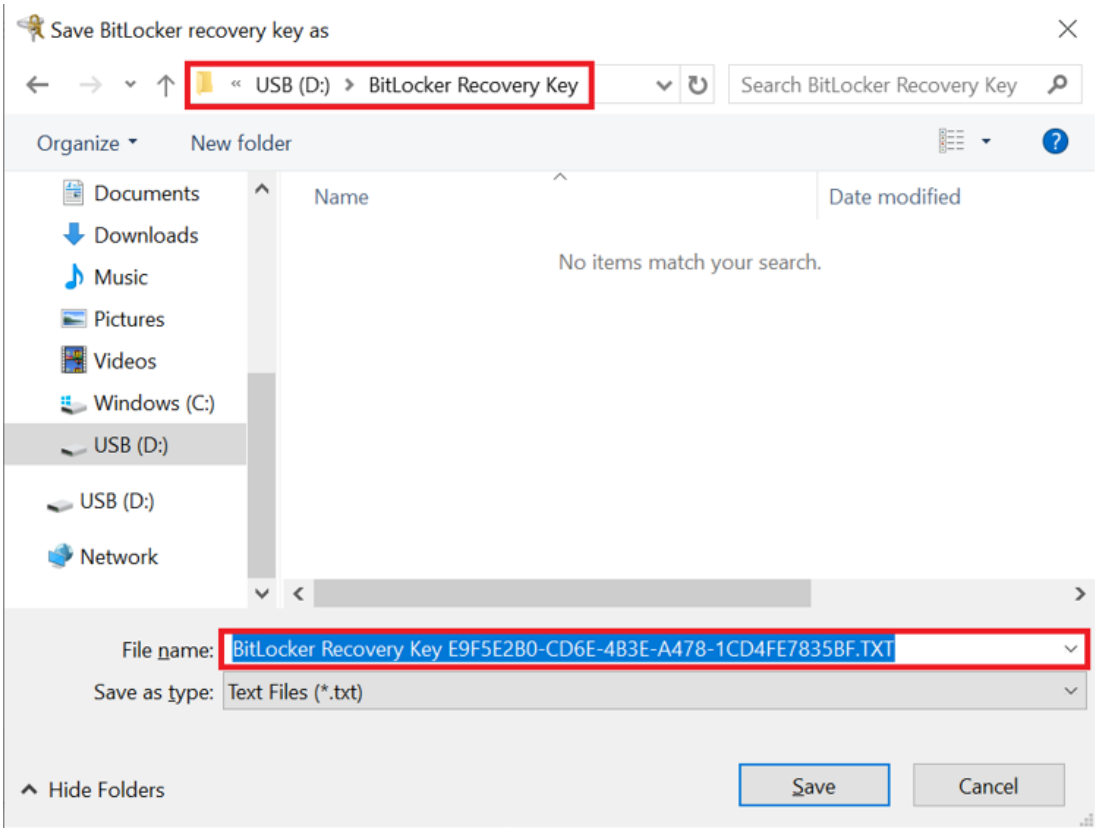
Step 3: Choose "Turn on BitLocker."

Step 4: The initialization process for the drive's basic information begins immediately.____×

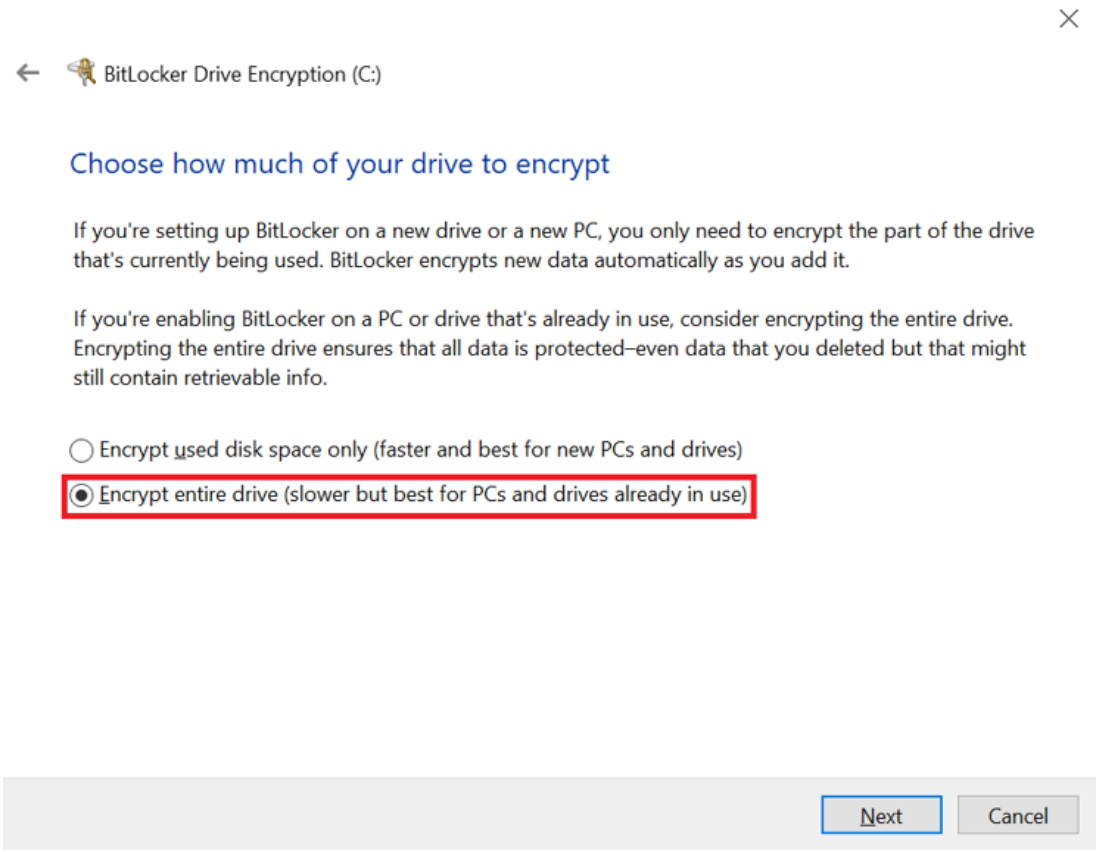


Step 5: After the initialization process, it is essential to back up the recovery key to facilitate drive recovery when needed. Please manage the recovery key file in a secure location.

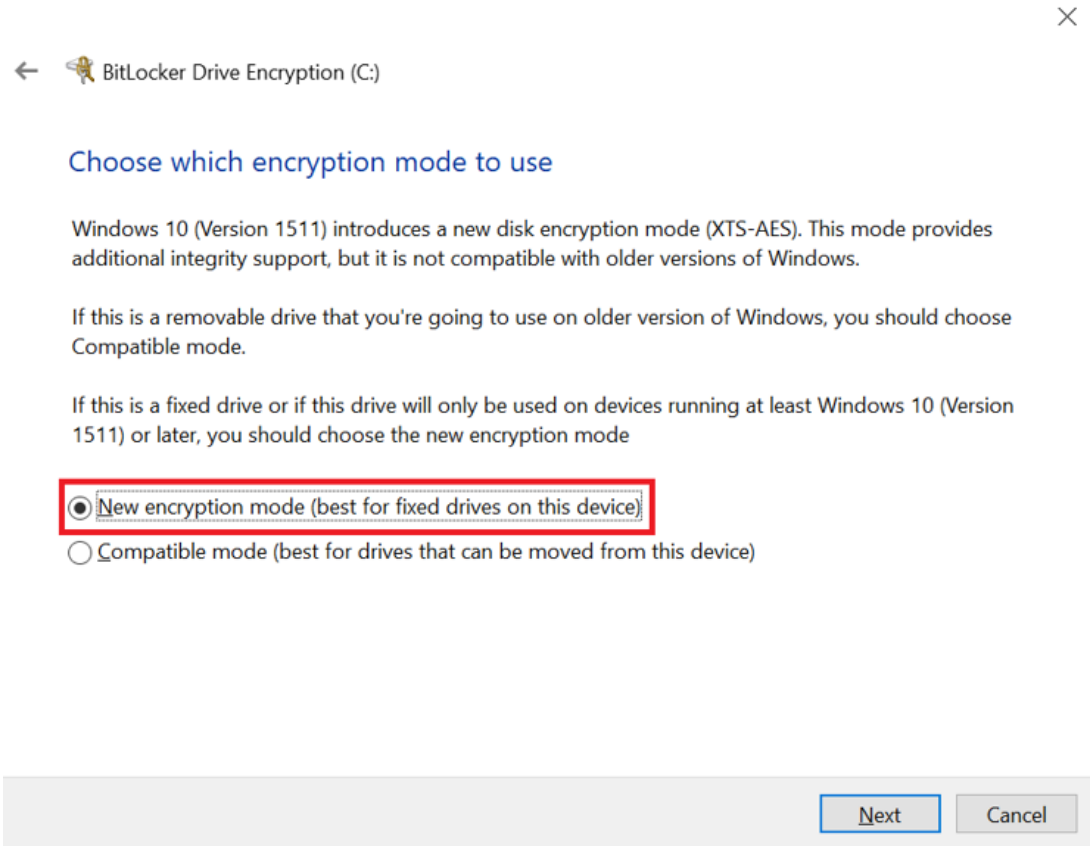

BitLocker Drive Encryption (C:)
How do you want to back up your recovery key?
Some settings are managed by your system administrator.
A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.
→ Save to your Microsoft account
→ Save to a file
→ Print the recovery key
How can I find my recovery key later?
Next
Cancel


Save BitLocker recovery key as
USB (D:) › BitLocker Recovery Key
Search BitLocker Recovery Key
Organize
New folder
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
USB (D:)
USB (D:)
Network
Name
Date modified
No items match your search.
File name: BitLocker Recovery Key E9F5E2B0-CD6E-4B3E-A478-1CD4FE7835BF.TXT
Save as type: Text Files (*.txt)
Hide Folders
Save
Cancel

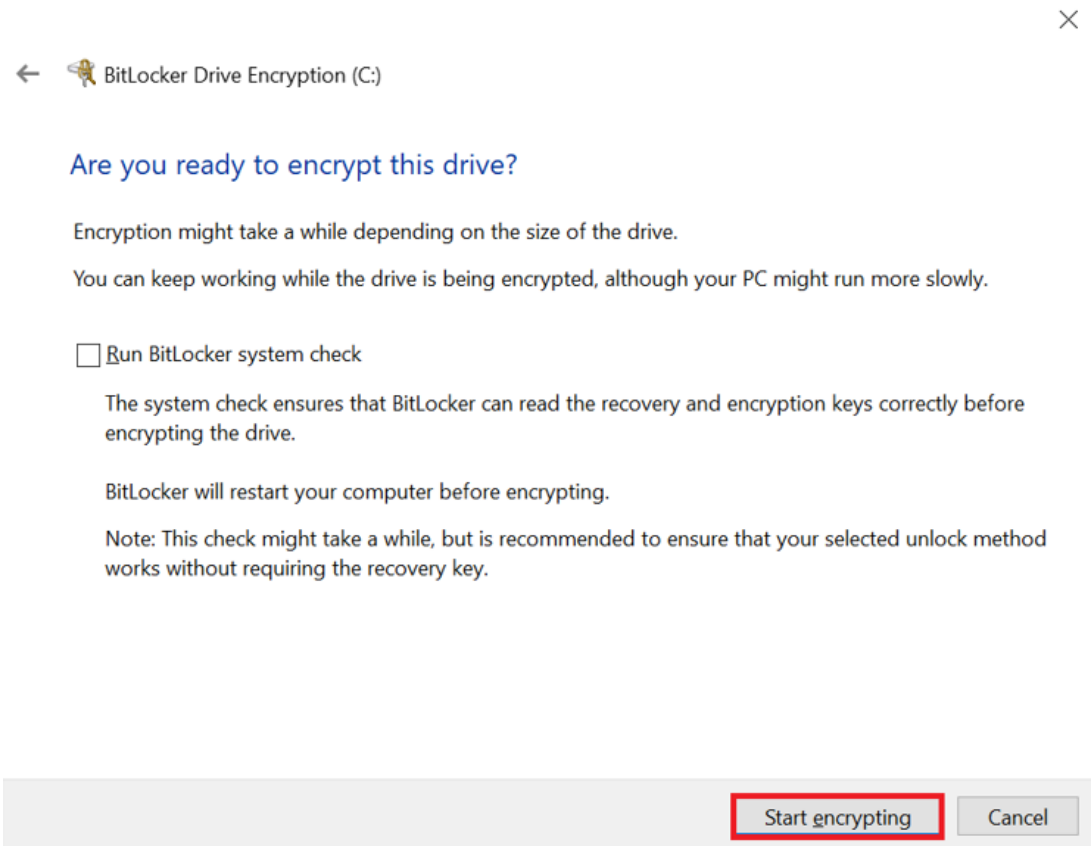
Step 6: Following the backup of the recovery key, select "Encrypt entire drive (slower but best for PCs and drives already in use)" in the next step.



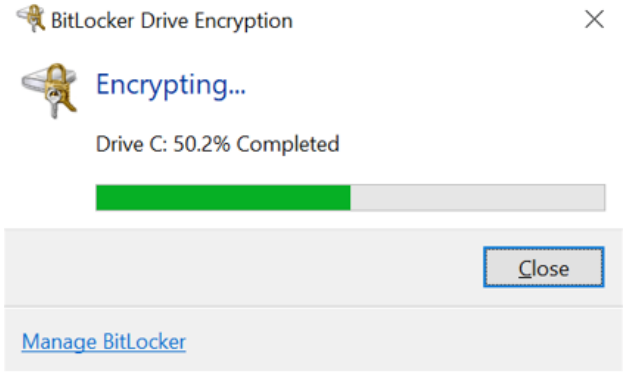
Step 7: Select **New encryption mode (best for fixed drives on this device)**



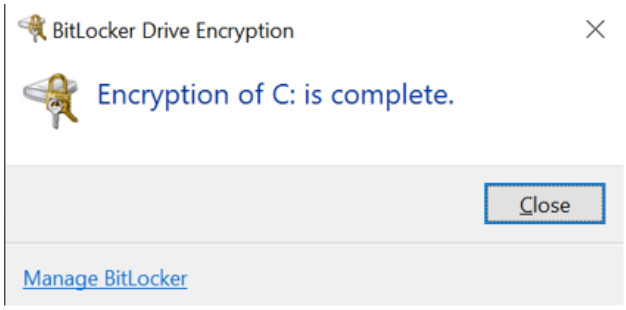
Step 8: Once all information is configured, the system will confirm the request before initiating the drive encryption. Select "Start Encrypting" to commence the encryption process.



Step 9: The drive encryption process will commence afterward. The duration depends on the size of the drive and may take some time.



Step 10: After the encryption is completed, the system will notify that the device has been encrypted. BitLocker serves as a protective measure against unauthorized access to the drive.


BitLocker Drive Encryption
Encryption of C: is complete.
Close
Manage BitLocker

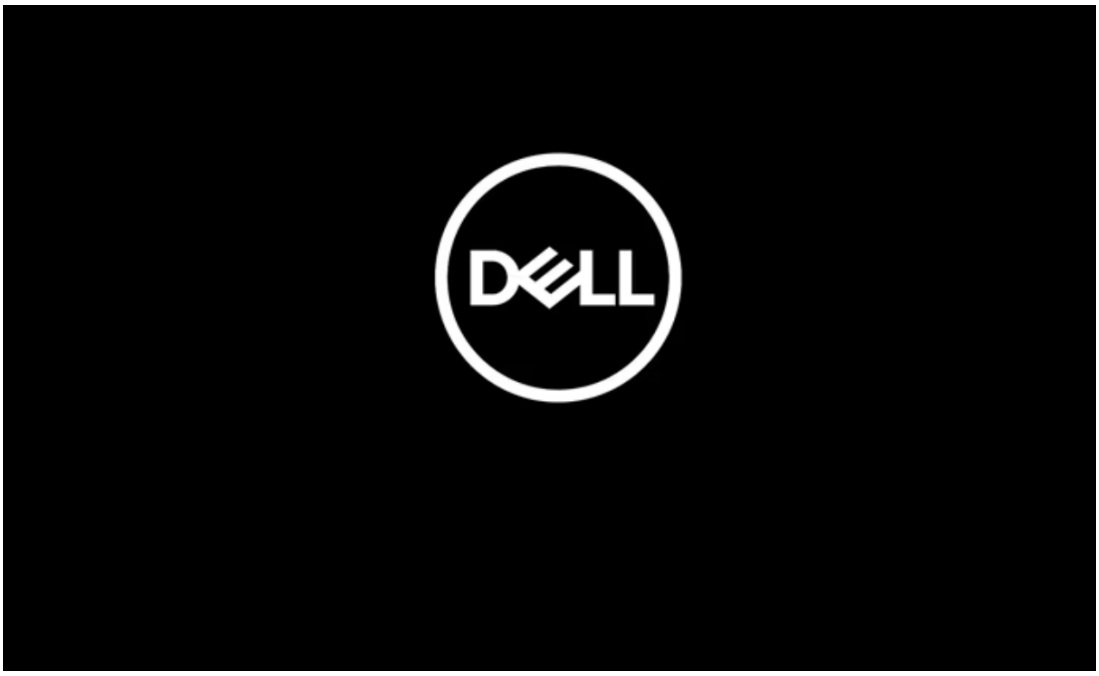
Setting BIOS Password on KIOSK Devices (DELL)

Administrators can enhance security on KIOSK DELL devices by setting a BIOS password to prevent unauthorized access to the BIOS.

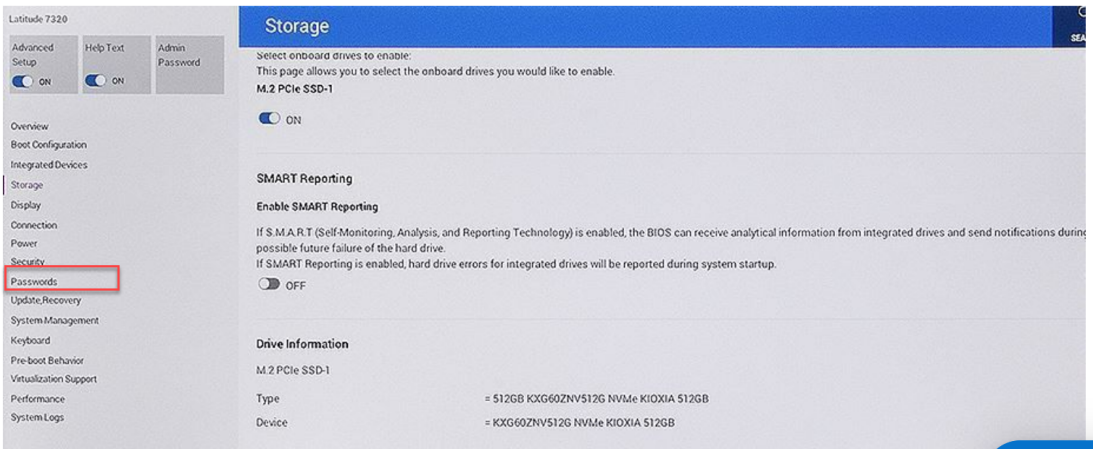
To achieve this, administrators need to follow these steps:

Step 1: Start the system.

Step 2: At the Dell logo screen, press the **F2** key several times until you enter the BIOS or System Setup.

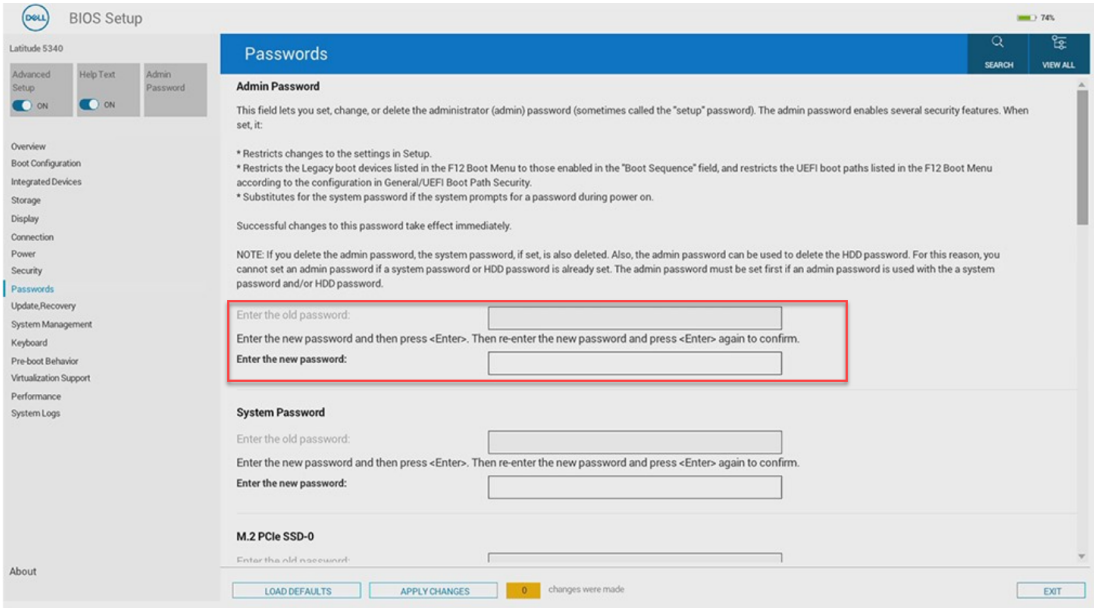


Step 3: In the BIOS Setup screen, select "Passwords" and press Enter, bringing up the Passwords screen.



Step 4: On the Admin Password screen, create a password in the "Enter the new password" field and press Enter.

Step 5: Re-enter the new password and press Enter again to confirm.



Step 6: Click "APPLY CHANGES" to save the changes as prompted by the message.

Step 7: Select Exit, the computer will restart, and the BIOS system will now have a password set in place.

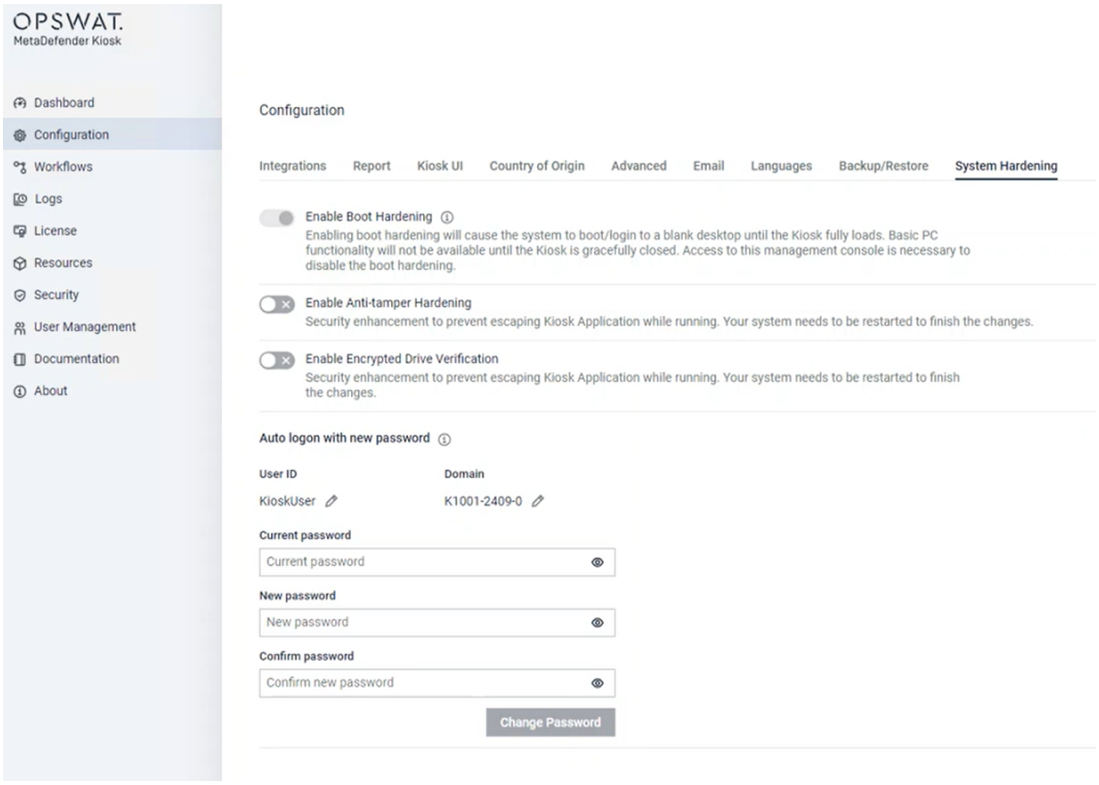
Change Kiosk autologon password

The latest versions of Kiosk Hardened Image are configured with Windows autologon to enhance the security level. With Kiosk version 4.7.2, Administrator can change the autologon password directly from Kiosk WebMC.

To change the autologon password, select **Configuration**, select **System Hardening Image**, provide **Current password** and **New password**, click **Change Password.**

When applying the change, the password will be applied directly to the system. Kiosk does not store this information.

> **Info**
> **Change autologon password** option is only available on Kiosk Hardened Image with Kiosk version 4.7.2 or newer.
>
> This feature is not yet supported by My OPSWAT.



Disabling Windows Update

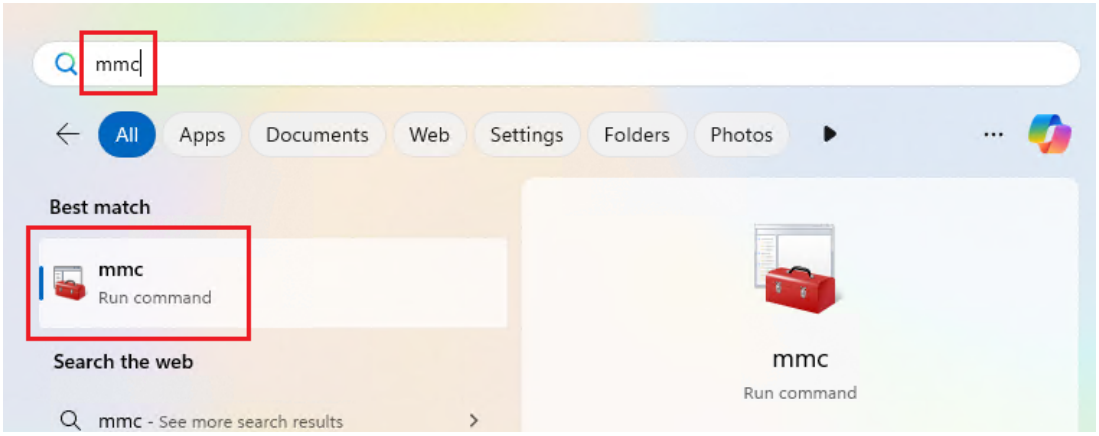
On Kiosk Hardened Image, Windows Update is enabled by default to ensure the latest security updates are automatically downloaded and applied. However, if you prefer to disable automatic Windows update on the Kiosk, please follow the instruction below.

> **Security Risks**
> It is best practice to keep automatic Windows updates enabled to ensure the latest security updates are applied promptly, keeping the system secure. Disabling automatic updates could lead to the system vulnerable to security risks.

Disable Windows Update and Update Orchestrator Services

Step 1. Open **Microsoft Management Console (MMC)**

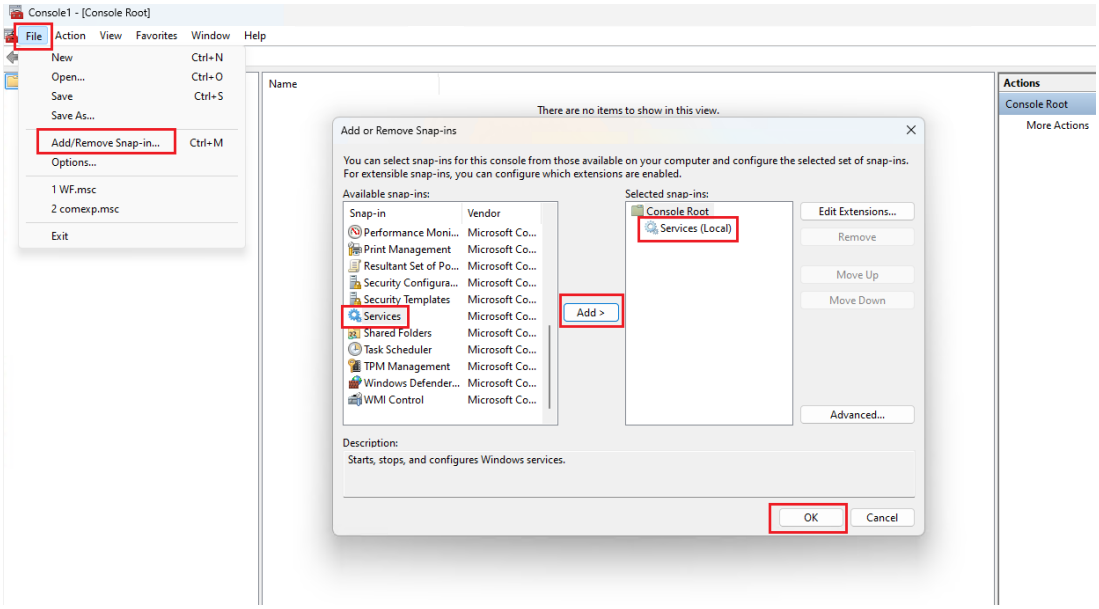
- Go to the Start menu, type **mmc**, and open it with Administrator permissions



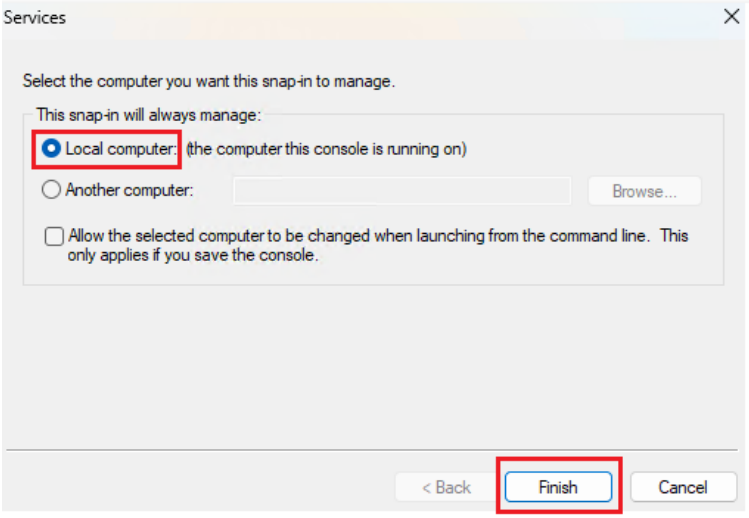
Open Microsoft Management Console (MMC)

Step 2. Add the **Services Snap-in**

- In the MMC window, select **File**, select **Add/Remove Snap-in**.
- From the list, select **Services** and click **Add**. A popup Window will appear, select **Local computer**, click **Finish**. Then, click **OK**.



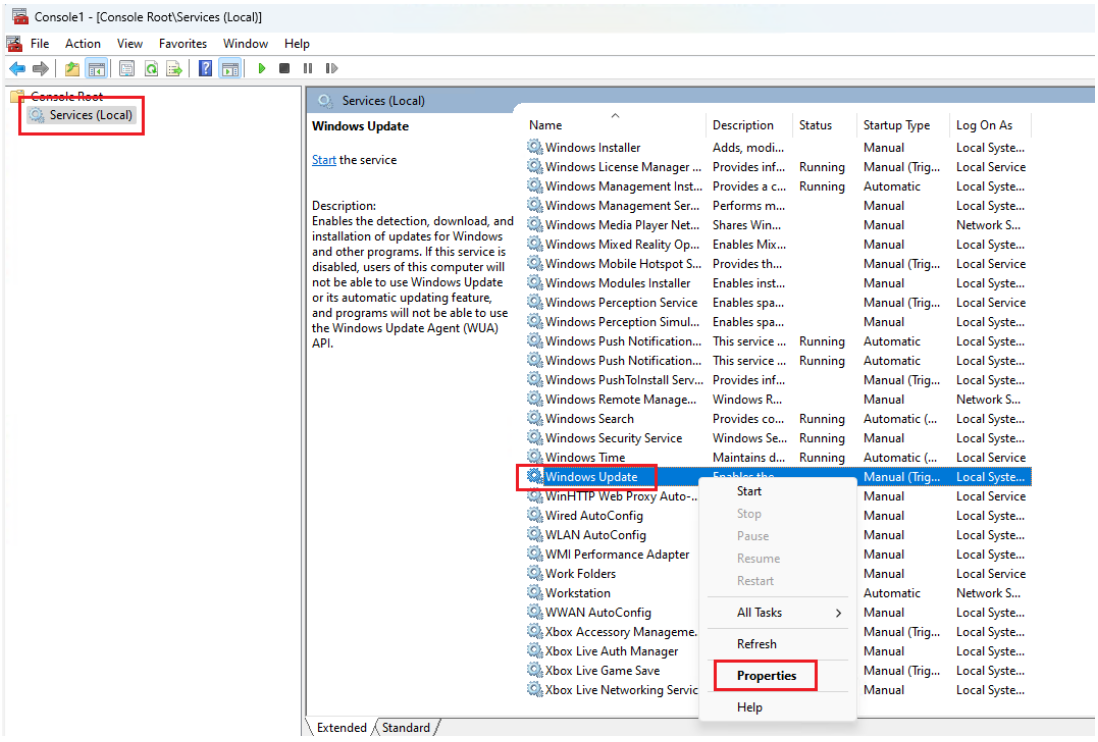
Add Services Snap-in in MMC



Select Local Computer to add Service Snap-in

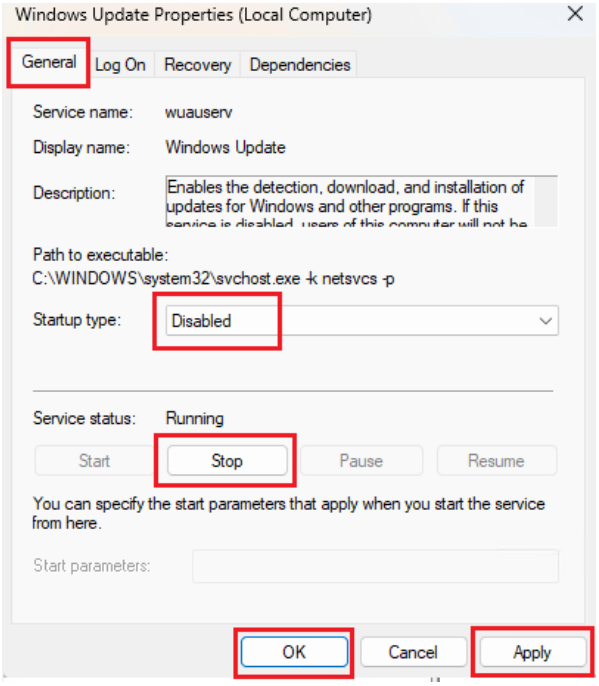
Step 3. Disable the **Windows Update service**

- In the Services list, find **Windows Update** service. Right-click on it and select **Properties**.



Open Properties of Windows Update service

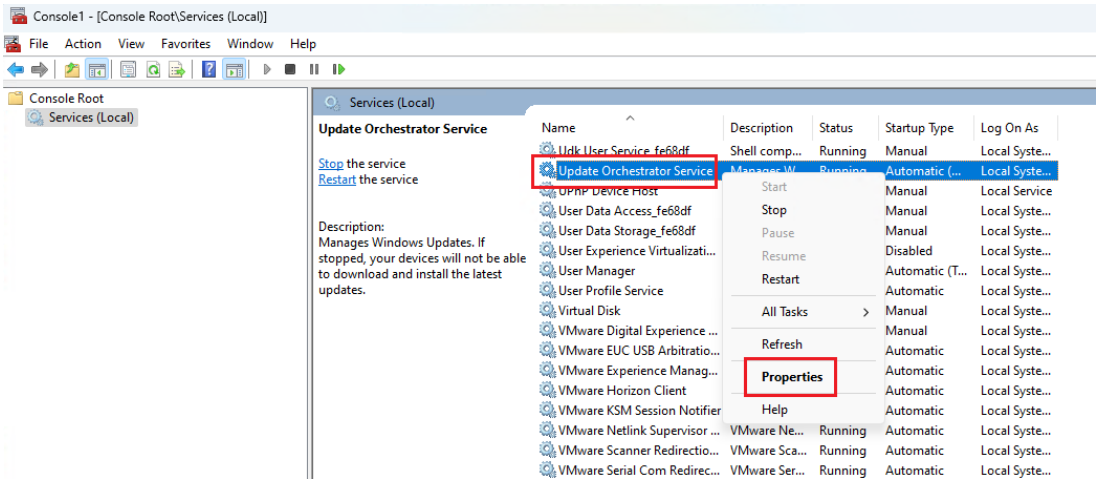
- Under the **General** tab, set **Startup type** to **Disabled**.
- Click **Stop** to halt the service, then click **Apply** and **OK**.



Disable Windows Update service

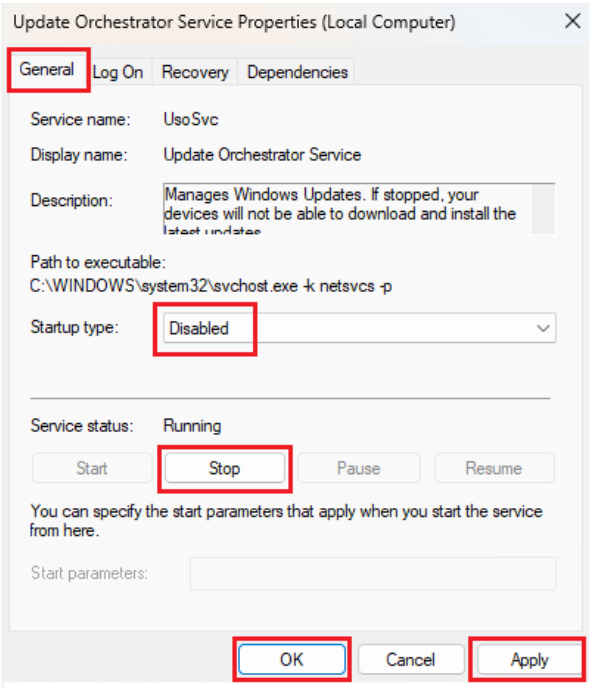
Step 4. Disable **Update Orchestrator service**

- Still in Services list, find **Update Orchestrator Service**. Right-click on it and select **Properties**.



Open Properties of Update Orchestrator Service

- Under the **General** tab, set **Startup type** to **Disabled**.
- Click **Stop** to halt the service, then click **Apply** and **OK**.

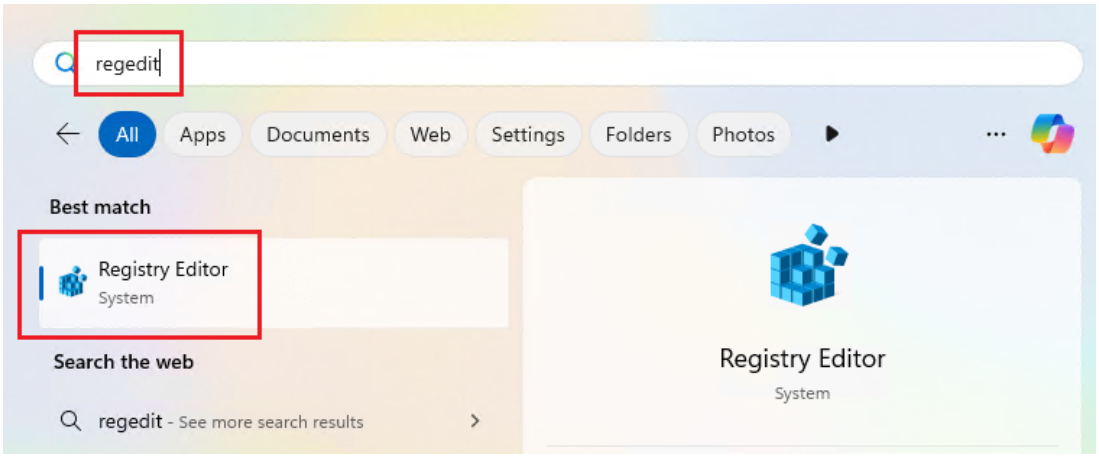


Disable Update Orchestrator Service

Prevent Windows Update from being automatically re-enabled

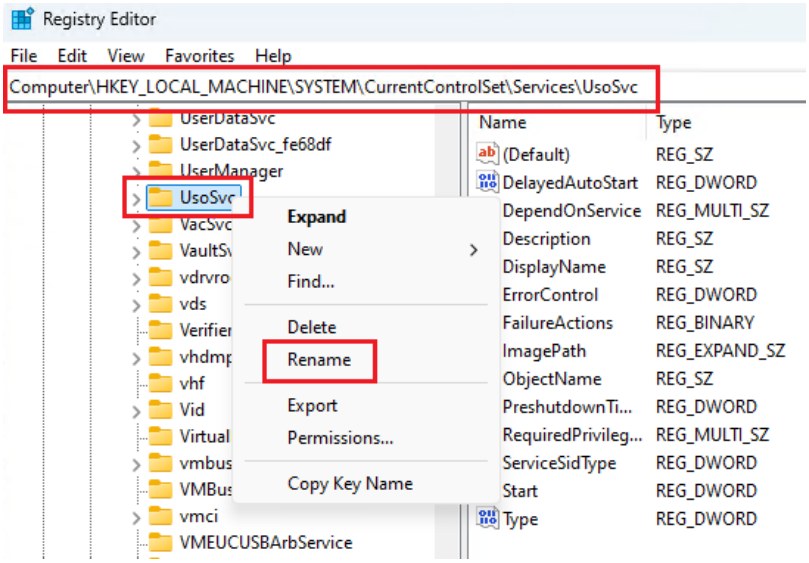
Step 1. Rename **Registry Keys**

- Go to Start menu, type **regedit**, and open it with Administrator permissions

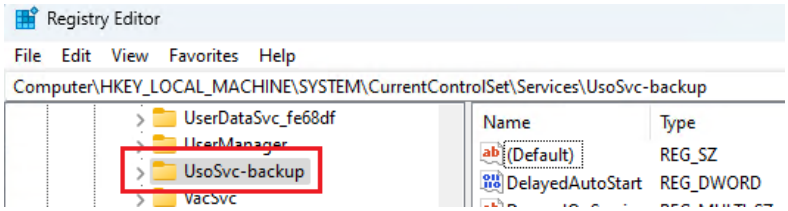


Open Registry Editor

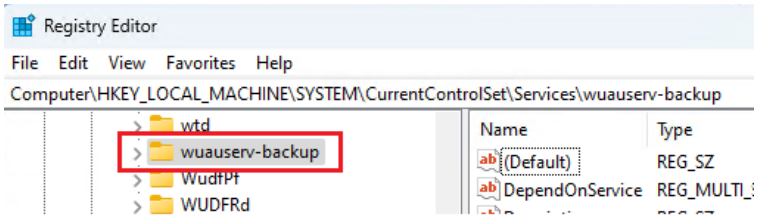
- Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`.
- Rename the following **registry keys**:
  - `usoSvc` to `usoSvc-backup`
  - `wuauserv` to `wuauserv-backup`



Rename Registry Keys



UsoSvc Registry Key after renamed



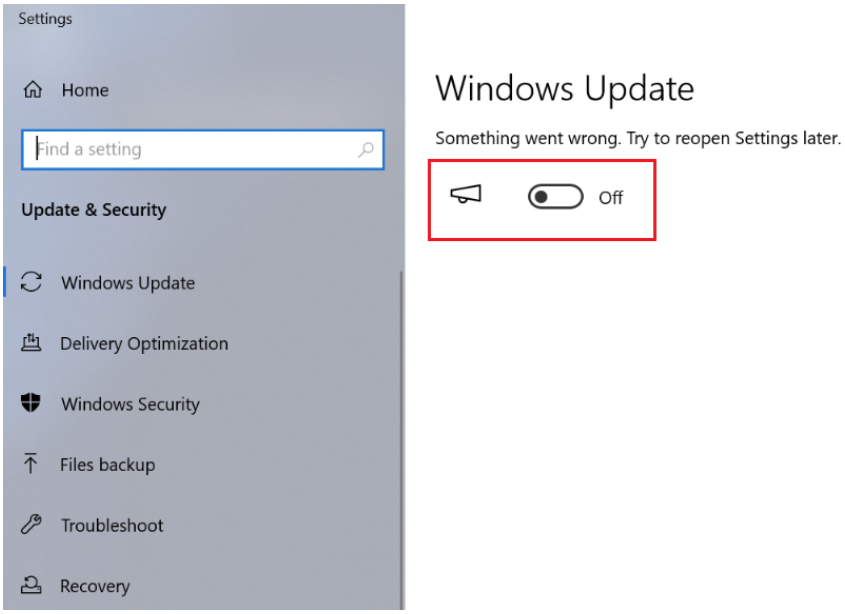
wuauserv Registry Key after renamed

Step 2. Reboot the Kiosk system

- Restart the system to apply the changes.

Step 3. Verify Windows Update status

- After reboot, go to Start menu, type **Windows Update settings** , and open it. Verify to ensure the Windows Update was disabled

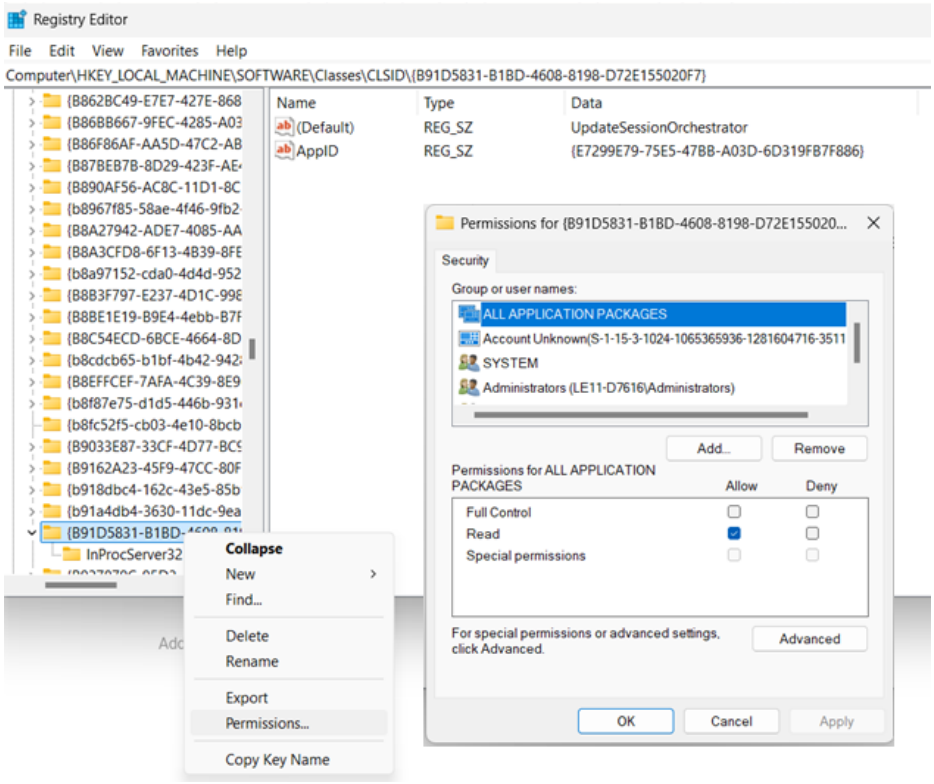


Verify Windows Update status

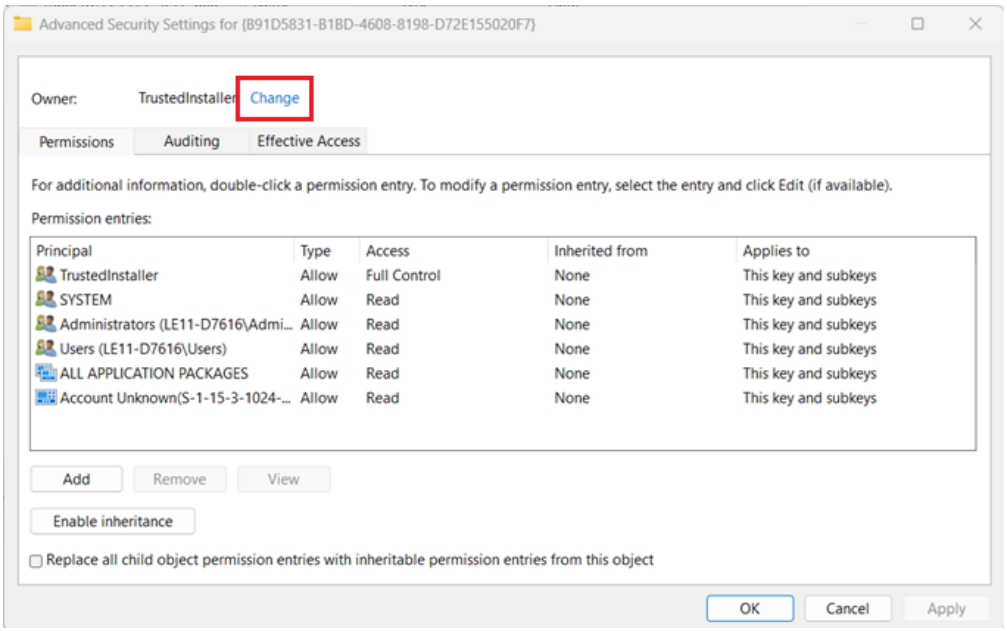
Prevent removed services from being registered by DCOM

Step 1. Run **registry** with Administrators permissions, and navigate to HKEY_LOCAL _MACHINE\SOFTWARE\Classes\CLSID{B91D5831-B1BD-4608-8198-D72E155020F7}

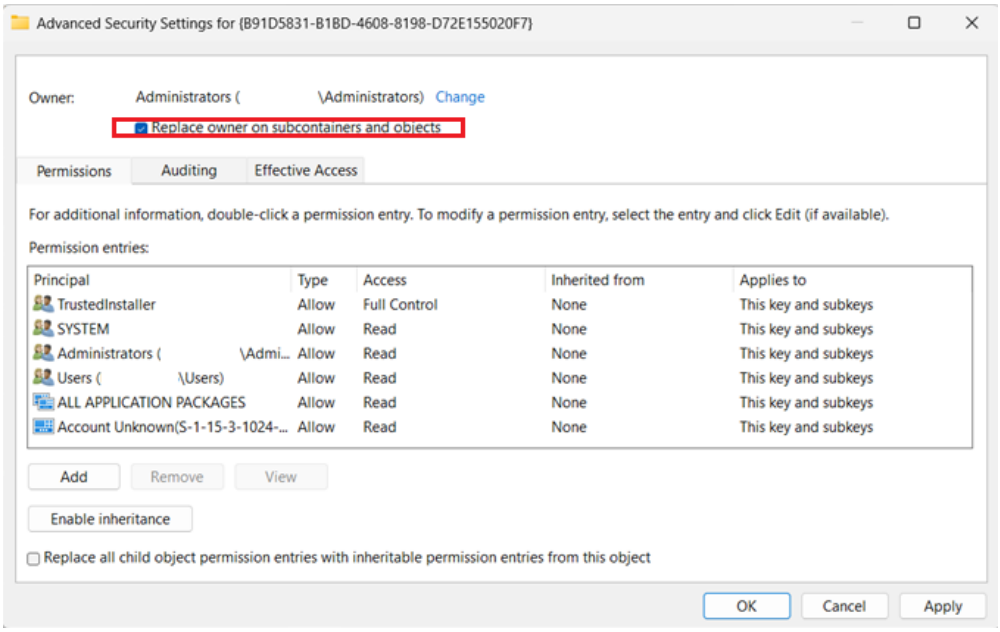
Step 2. Right click on the key, select **permissions**



Step 3. Click on Advanced. Under Advanced Security Settings, Click on Change the owner



Step 4. Input **BUILTIN\Administrators** under object name, click **Check names** to verify the username, click **OK** to save the setting. Make sure you select **Replace owner on subcontainers and objects**, click Apply



Step 5. Rename the key to HKEY_LOCAL_ MACHINE\SOFTWARE\Classes\CLSID{B91D5831-B1BD-4608-8198-D72E155020F7}**_backup**

Step 6. Repeat step 2-4 to change the **permissions** of the key back to **NT Service\TrustedInstaller**

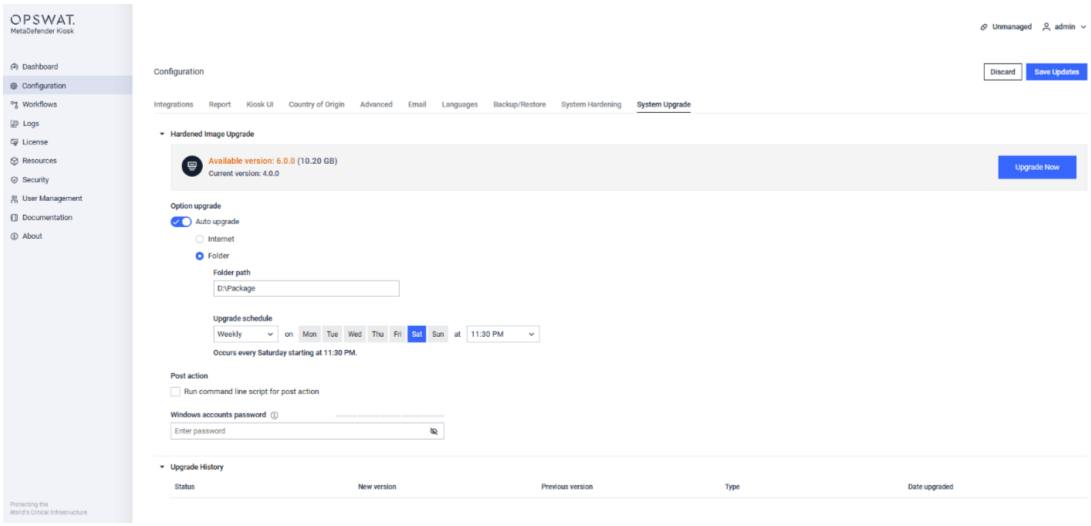
Step 7. Repeat the step 2-5 to change the key name HKEY_LOCAL_ MACHINE\SOFTWARE\Classes\CLSID{e60687f7-01a1-40aa-86ac-db1cbf673334} to **HKEY*LOCAL* MACHINE\SOFTWARE\Classes\CLSID{e60687f7-01a1-40aa-86ac-db1cbf673334}_backup**

Auto-Upgrade Kiosk Hardened Image

Kiosk Hardened Image version 25.01.0 (bundled with Kiosk Application 4.7.3) introduced a new feature that allows administrators to automatically upgrade Kiosk Hardened Image directly from Kiosk WebMC.

Upgrade Settings

To perform the upgrade, from **Kiosk WebMC**, navigate to **Configuration**, select **System Upgrade**.



- **Upgrade Options**:
  - **Auto upgrade:** If this option is disabled, the system will not perform any upgrades.
  - **Internet:** The Kiosk system verifies and downloads the version of Kiosk Hardened Image from My OPWAT.
  - **Folder**: Administrators can specify a folder path containing the Kiosk Hardened Image files. The system will automatically download and use these files for the upgrade.
    - Please reach out to OPSWAT Technical Support for offline Kiosk Hardened Image package.

Info

- The Kiosk Hardened Image can also be downloaded directly from My OPSWAT. The size of the image files would be about 10 GBs, please ensure the internet speed and storage space are adequate.
- If a network source is used as Upgrade option, please ensure the Windows account used to log in to the Kiosk system has the necessary permissions to access the network resource. For example, If Kiosk uses a domain account for Windows logon, this account must have access to the assigned network folder.

- **Upgrade schedule:** Specify the local system time when the Kiosk system should download and install the upgrade image.
    - Additionally, administrators can initiate the upgrade immediately by clicking on **Upgrade Now**
- **Post action:** If a post-upgrade **batch script** is provided, the Kiosk system will automatically execute this script after the upgrade is successfully completed.
- **Windows account password**:
    - To restore existing Windows accounts and their associated passwords on the Kiosk system, administrators must provide the account password in this field. The account will automatically be enabled with autologon.
    - If this field left empty, Kiosk will not restore existing accounts and will instead apply default Kiosk credential

Configuration backup and restore

During the upgrade, the Kiosk system automatically backups and restores essential system and product settings (for more information, please refer to this link)

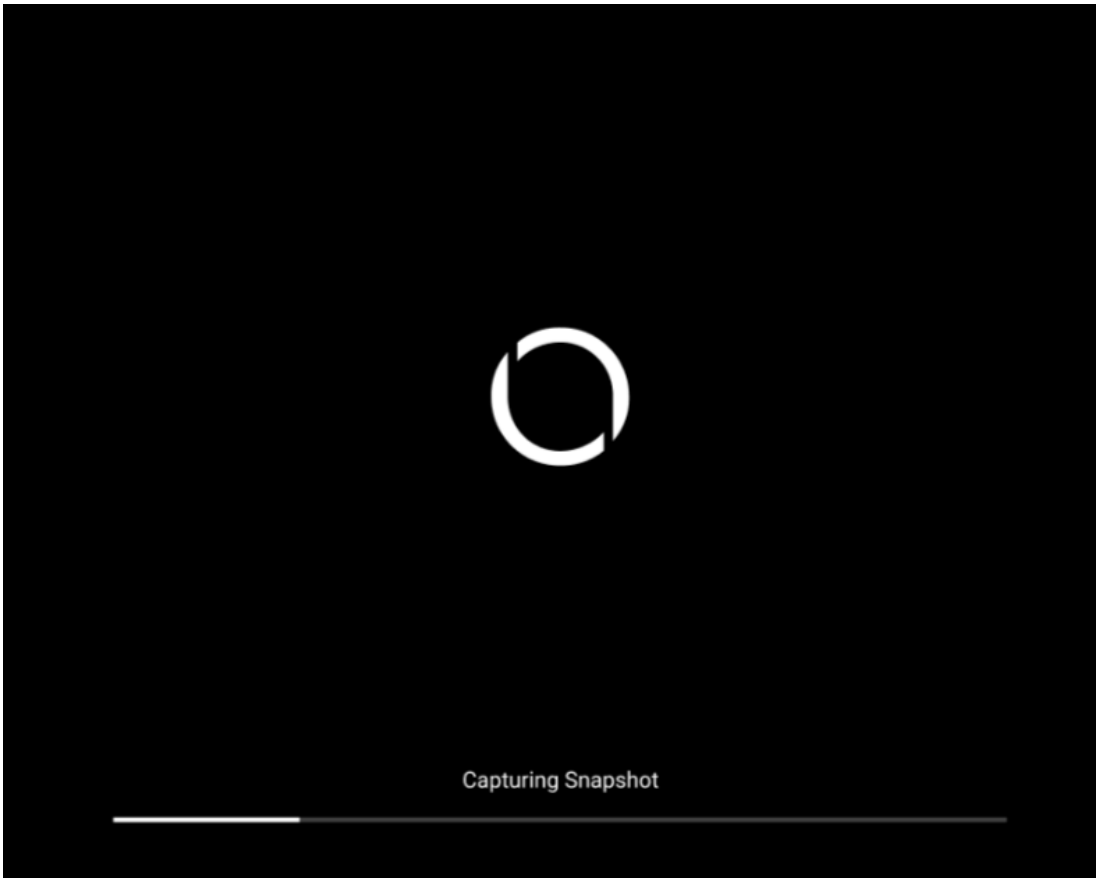
- System settings:
    - Computer host name
    - Windows local accounts (if the password is provided)
    - System hosts file (C:\Windows\System32\drivers\etc\hosts)
    - Trusted Windows certificates in Certificate Microsoft Management Console (MMC)
    - Network settings (DHCP/Static, Wi-Fi network, IP Address)
- Product configurations
    - Kiosk and Core licenses
    - Kiosk and Core configurations
    - Kiosk session history
    - Quarantine files from MD Core
    - Kiosk User Management settings
    - Secure connection (HTTPS) certificate and setting
    - Kiosk branding and logo customization
    - Instance management on My OPSWAT (if applicable)

Limitation of Kiosk Hardened Image 25.02.0

- **Local MetaDefender Core support only:** The upgrade process supports only a local hosted MetaDefender Core. In the Kiosk WebMC settings under **Configuration > Integration > MetaDefender Core**, the value must be set to either **'localhost'**, **'127.0.0.1'**, or left blank.
- **Consistent setting values:** Critical setting such as the **Core API key** and **DB PIN** must match the value used during backup process. If these values differ, the restoration process may fail.
- **MetaDefender Core online-activated support only**: Offline-activated or license activations via My OPSWAT are not supported to upgrade.
- **Wi-Fi with Credentials not supported**: Wi-Fi configurations that requires user credentials are not supported by the backup process.
- **Quarantine files backup:** Kiosk only supports backing up quarantine files from MD Core. The quarantine files will not be shown from Core WebMC, downloading quarantine files must be done via REST API here.
- **Upgrade Now** option is not supported on My OPSWAT or OCM.

Upgrade process overview

- **Initiation:** The upgrade begins either when the scheduled time is reached or when the "Upgrade Now" button is clicked. The Kiosk system automatically downloads the latest version of the Kiosk Hardened Image. The download time may vary depending on the Internet speed.
- **Backup and preparation:** The Kiosk system backs up the required configurations and settings before proceeding. Administrators will see a warning message indicating that the system will restart several times to perform the upgrade.
- **Upgrade execution:** The system prepares the environment and a separate partition will be created to store a snapshot of the current state. Ensure that the system has at least 40% free storage space available to accommodate the snapshot creation and upgrade process.

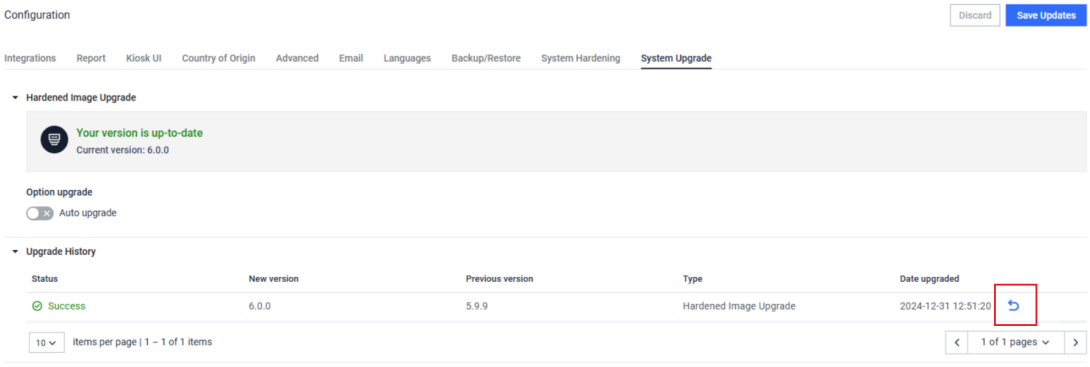


Warning
The cancellation of upgrading process is not yet supported in Kiosk Hardened Image 25.02.0

Error Handling and rollback

If an issue occurs during the upgrade process, Kiosk will automatically restore the system using the created snapshot to ensure continuity

From **Upgrade History** section, administrators can click on the **rollback icon** to revert to a previous version of success upgrade if desired


Configuration
Discard
Save Updates
Integrations
Report
Kiosk UI
Country of Origin
Advanced
Email
Languages
Backup/Restore
System Hardening
System Upgrade
Hardened Image Upgrade
Your version is up-to-date
Current version: 6.0.0
Option upgrade
Auto upgrade
Upgrade History
Status
New version
Previous version
Type
Date upgraded
Success
6.0.0
5.9.9
Hardened Image Upgrade
2024-12-31 12:51:20
10
items per page | 1 – 1 of 1 items
1 of 1 pages

Release Notes

KIOSK Hardened Image 25.05.0	
30 May 2025	
MD KIOSK version	**4.7.6** Release Notes
MD Core version	**5.14.1** Release Notes
Windows OS version	Windows 10 IoT Enterprise LTSC (21H2, Build 19044.5854)
What's new	
Application and system updates	Updated applications and system components to the latest versions (Windows 10 IoT Enterprise LTSC (21H2, Build 19044.5854), MD Kiosk 4.7.6, MD Core 5.14.1) to ensure optimal performance, security, and compatibility.
Support model Dell Pro 24 All-in-One Plus Desktop	Kiosk Hardened Image now supports a new model - Dell Pro 24 All-in-One Plus Desktop
Enabling App & Browser Control to for security enhancement	App & Browser Control is now enabled by default in the Kiosk Hardened Image, enhancing protection against untrusted apps, files, and websites.
Disabling handwriting feature	Handwriting feature is disabled to simplifies the user interface and removes unnecessary input options.
Disabling WSearch	WSearch and its associated DCOM services are disabled to improve system stability

Archived Release Notes

KIOSK Hardened Image 25.04.0	
19 April 2025	
MD KIOSK version	**4.7.5** Release Notes
MD Core version	**5.13.3** Release Notes
Windows OS version	Windows 10 IoT Enterprise LTSC (21H2, Build 19044.5737)
What's new	
Application and system updates	Updated applications and system components to the latest versions (Windows 10 IoT Enterprise LTSC (21H2, Build 19044.5737)), MD Kiosk 4.7.5, MD Core 5.13.3) to ensure optimal performance, security, and compatibility.
Improved Out-of-box Experience Initial Setup Wizard	The UX of Out-of-box Experience is redesigned to provide more intuitive, streamlined, and visually improved interface. The new user experience makes it easier and faster to get started.
Enhanced Auto-Upgrade process for Kiosk Hardened Image	The auto-upgrade for Kiosk Hardened image has been improved for greater stability. This release also includes refined messages and visual enhancements for a better user experience. Certificates stored in .SSH folder will be fully backup.
Kiosk Hardened Image upgrade supports in My OPSWAT	Kiosk Hardened Image upgrade options are now supported in My OPSWAT, allowing administrators to manage software updates more efficiently
Included required dependency for SBOM engine	JDK dependency is included to ensure SBOM engine will deploys successfully without requiring any additional steps
Improve USB detection time in Kiosk devices with floppy drive connected	Optimized USB detection performance in environments where floppy disk drive is present.

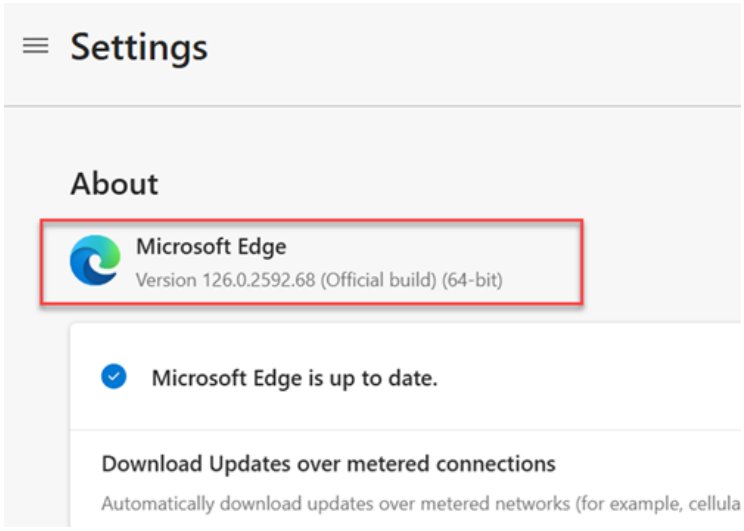
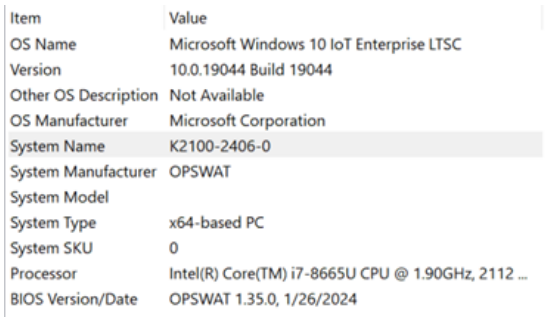
KIOSK Hardened Image 25.03.0	
28 February 2025	
MD KIOSK version	**4.7.4** Release Notes
MD Core version	**5.13.3** Release notes
Windows OS version	Windows 10 IoT Enterprise LTSC (21H2, Build 10944.5608)
What's new	
Application and system updates	Updated applications and system components to the latest versions (Windows 10 IoT Enterprise LTSC (21H2, Build 10944.5608), MD Kiosk 4.7.4, MD Core 5.13.3) to ensure optimal performance, security, and compatibility.
Updated BIOS version	Updated BIOS to the latest version.
Include BIOS version information in description	BIOS version information is included in the Hardened Image description to enhance troubleshooting process.

KIOSK Hardened Image 25.02.0	
28 February 2025	
MD KIOSK version	**4.7.4** Release Notes
MD Core version	**5.13.2** Release notes
Windows OS version	Windows 10 IoT Enterprise LTSC (21H2, Build **19044.5371**)
What's new	
Application and system updates	Updated applications and system components to the latest versions (Windows 10 IoT Enterprise LTSC (21H2, Build 19044.5487), MD Kiosk 4.7.4, MD Core 5.13.2) to ensure optimal performance, security, and compatibility.
Initial Setup Wizard	On the first startup, Kiosk automatically launches an initial setup wizard, allowing the administrator to create an account and activate the license
Enhanced Auto-Upgrade for Kiosk Hardened Image	The auto-upgrade for Kiosk Hardened image has been improved for greater stability. This release also includes refined wording and visual enhancements for a better user experience.
Disable camera on Kiosk K1001	Camera is disabled on Kiosk K1001 by default

KIOSK Hardened Image 25.01.1	
7 February 2025	
MD KIOSK version	**4.7.3** Release Notes
MD Core version	**5.13.0** Release notes
Windows OS version	Windows 10 IoT Enterprise LTSC (21H2, Build **19044.5371**)
What's new	
System updates	Updated system components to the latest versions to ensure optimal performance, security, and compatibility.
Backup and restore IP address of MD Core	Kiosk backups include and restore the configured IP address of MD Core

KIOSK Hardened Image 25.01.0	
30 December 2024	
MD KIOSK version	**4.7.3** Release Notes
MD Core version	**5.13.0** Release notes
Windows OS version	Windows 10 IoT Enterprise LTSC (21H2, Build **19044.5247**)
What's new	
System updates	Updated system components to the latest versions to ensure optimal performance, security, and compatibility.
Auto Upgrade Kiosk Hardened Image	With MetaDefender Kiosk 4.7.3 bundled in Kiosk Hardened Image 25.01.0, administrators can initiate the upgrade for Kiosk Hardened Image (25.01.0 or later) directly from Kiosk WebMC. The upgrade process backs up essential system and product configurations, automatically downloads the latest version of Kiosk Hardened Image, and performs the upgrade. In case of failure, Kiosk would automatically revert to the previous version to ensure continuity.
Enable RDP (Remote Desktop Protocol) from Kiosk WebMC	Administrators can enable RDP (Remote Desktop Protocol) through Kiosk WebMC. Once enabled, Kiosk will modify the necessary services and settings.

KIOSK Hardened Image 24.09.0	
30 September 2024	
MD KIOSK version	**4.7.1.9897** Release Notes
MD Core version	**5.11.1** Release notes
Windows OS version	Windows 10 IoT Enterprise LTSC (21H2, Build **19044.4894**)
What's new	
System updates	Updated system components to the latest versions to ensure optimal performance, security, and compatibility.

KIOSK Hardened Image 24.06.0	
27 June 2024	
MD KIOSK version	**4.6.8** Release Notes
MD Core version	**5.10.0** Release notes
Windows OS version	Windows 10 IoT Enterprise TLSC 21H2 (Build **19044.4529**)
What's new	
Update MS Edge Application	In the new hardened image, only the MS Edge browser is included, and it has been updated to the latest version. 
Hostname Naming Convention	The hardened image version information will be included in the hostname of the hardened image. This will help customers easily identify the version of the hardened image deployed on the KIOSK machine. The format is: `<DeviceModel>-<YYMM>-<version>` (e.g., `K2100-2406-0`: The first release in June 2024 for K2100 device). 
Enhanced Hardening for KIOSK	In this version, additional hardening measures have been applied to enhance the security of the KIOSK device.

Item	Value
OS Name	Microsoft Windows 10 IoT Enterprise LTSC
Version	10.0.19044 Build 19044
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	K2100-2406-0
System Manufacturer	OPSWAT
System Model	
System Type	x64-based PC
System SKU	0
Processor	Intel(R) Core(TM) i7-8665U CPU @ 1.90GHz, 2112 ...
BIOS Version/Date	OPSWAT 1.35.0, 1/26/2024

Overview

The MetaDefender Kiosk Secure Image is a Pro-Service solution that ensures the Kiosk Operating System remains unmodified and untampered with during operation by creating a baseline of the Operating System and continuously monitoring for any changes. If any unexpected changes occur, the system halts until the alert is resolved. The MetaDefender Kiosk Secure Image is an enhancement for file integrity and regulatory compliance auditing, providing administrators with better control and visibility into their security operations.

Easy deployment methods are also available using the Secure Image Deployment Wizard. The Image provides driver package for the specific hardware of the K1001, K3000, incorporating the most stable versions of OPSWAT MetaDefender Core and MetaDefender Kiosk.

The following deployment and setup instructions for the MetaDefender Kiosk Secure Image are intended solely for customers who have purchased Secure Image as an additional Pro-Service.

Benefits of Secure Image

File Integrity Monitoring (FIM)

The Kiosk Secure Image includes a File Integrity Monitoring (FIM) feature that prevents and alerts the Kiosk administrator to any unauthorized modifications in the Kiosk installation directory.

The FIM logs an event whenever an unauthorized modification is detected and disables the Kiosk UI until a Kiosk administrator acknowledges the event in the Logs > File Integrity Monitoring section.

Enhanced Group Policy

The Kiosk Secure Image enhanced the Local Group Policy, which includes AppLocker policies to prevent unauthorized software installation and script execution.

Additionally, other Local Group Policies are implemented to enhance the security of the Kiosk hardware, including account lockout policies and more.

All-in-one Package Deployment

The Kiosk Secure Image includes All-In-One driver packages and automatic Windows activation for all supported hardware, eliminating the need to separate the image into different versions.

Once the deployment is complete, the driver package will be removed to conserve disk space.

Quarterly Releasing

The Kiosk Secure Image will be released quarterly and will include Windows security updates, Group Policy enhancements, and more.

To apply the new release, you need to re-image the entire Kiosk Hardware OS. You can back up the MD Core and MD Kiosk configurations to restore them after re-imaging the Kiosk Hardware

Release notes

Kiosk Secure Image Q2 - 2025

Release Date	Apr 14th, 2025
MD Core Version	5.13.3 Release Notes
MD Kiosk Version	4.7.4.2902 Release Notes
OS Version	Windows 10 IoT Enterprise LTSC (21H2, Build **19044**)
Supported Model	K1001 (Lenovo), K1001 (Dell-7410), K3000
Changes:	• Updated system components to the latest versions to ensure optimal performance, security, and compatibility. • Updated MD Core and MD Kiosk version.
Notice:	This is the last release for Hardware model **Kiosk K3000**. If you are still using K3000, please contact with Sales team or Support team for further dicussion

Archived Release Notes

Kiosk Secure Image Q1 - 2025

Release Date	Jan 8th, 2025
MD Core Version	5.13.0 Release Notes
MD Kiosk Version	4.7.3.2454 Release Notes
OS Version	Windows 10 IoT Enterprise LTSC (21H2, Build **19044**)
Supported Model	K1001 (Lenovo), K1001 (Dell-7410), K3000
Changes:	• Updated system components to the latest versions (**KB5048652**) (**KB5046541**) to ensure optimal performance, security, and compatibility. • Enhanced Group policy. • Enhanced AIO-Driver Installation process. • Microsoft Visual C++ Redistributable for Visual Studio 2015-2022 included. • Windows Autologon applied.

Kiosk Secure Image Q4 - 2024

Release date	Oct 1st, 2024
MD Core version	5.11.1 Release Notes
MD Kiosk version	4.7.1.9897 Release Notes
OS version	Windows 10 IoT Enterprise LTSC (21H2, Build **19044**)
Supported Model	K1001 (Lenovo), K1001 (Dell 7410), K3000
Changes:	• Updated system components to the latest versions to ensure optimal performance, security, and compatibility. • Enhanced Group policy. • The image is now included with the Windows Recovery Partition deployment, ensuring Windows functionality and fixing the issue where the Windows update package cannot be installed due to a missing Windows Recovery Partition.

Kiosk Secure Image Q3 - 2024

Release date	05 Aug, 2024
MD Core version	5.10.1 - Release Notes
MD Kiosk version	4.7.0.9392 - Release Notes
OS Version	Windows 10 IoT Enterprise LTSC (21H2, Build **19044**)
Supported Model	K1001 (Lenovo), K1001 (Dell 7410), K3000
Changes:	
New OS version	• Upgraded Windows version to Windows 10 IoT 21H2 - Build 19044
New FIM version	• Compatible with Windows 10 IoT 21H2 • Fixed the previous issue with Windows Defender detection and the FIM Exclusion list issue.
Enhancements:	• Replaced the previous startup method (utilizing VBScript) with Hardening Mode, developed by the Kiosk Application, to prevent black screen issues from earlier versions. • Updated system components to the latest versions for enhanced performance, security, and compatibility. • Additional information is displayed in the background. • MD Kiosk can now be upgraded by running a newer installer version without losing File Integrity Management settings.
Hardware supporting	Discontinued K1000, K2xxx, K3001. Will continue on demand only.

Secure Image Deployment Wizard

Overview

This version of the Kiosk Secure Image Deployment Tool is now called Secure Image Deployment Wizard and has been enhanced with a user-friendly UI/UX design. It incorporates a built-in touch screen for seamless interaction with the deployment tool, providing clear and concise information. Additionally, it displays the processing status for each step of the deployment process.

It also offers a logging feature to keep a record of activities and provides the option to force a reboot in the event of an "Error" occurrence.

Creating Secure Image Deployment flash drive

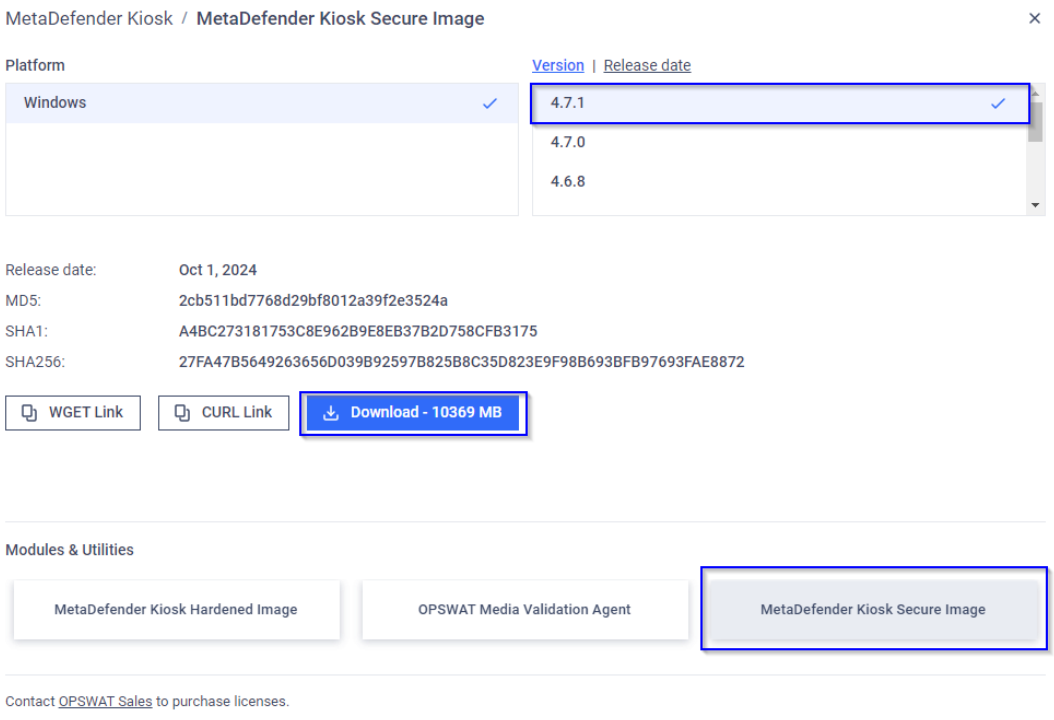
Follow the steps to create a bootable flash drive containing the Kiosk Secure Image to facilitate the efficient deployment of MetaDefender Kiosk on various Kiosk hardware models

Requirements:

- A PC running Windows 7/8/8.1/10 or 11
- A USB flash drive (USB 3.0 or above) with a storage capacity of at least 32GB.

Step 1: Download Secure Image Deployment Wizard and Image Package

1. Download the Secure Image Deployment Wizard: **WINPEBootable.vhd**
2. When licensed, you can see the **MetaDefender Kiosk Secure Image** download section inside the **MetaDefender Kiosk** download page on MyOPSWAT Portal

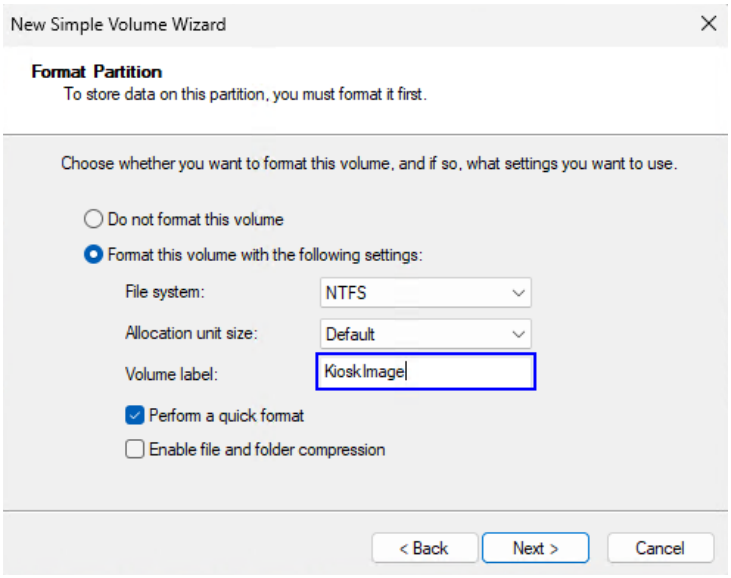


Download page of MetaDefender Kiosk Secure Image on My OPSWAT Portal

Step 2: Create bootable flash drive

Download Rufus tool (version 4.5 is recommended) to format and create bootable USB flash drive by the following steps:

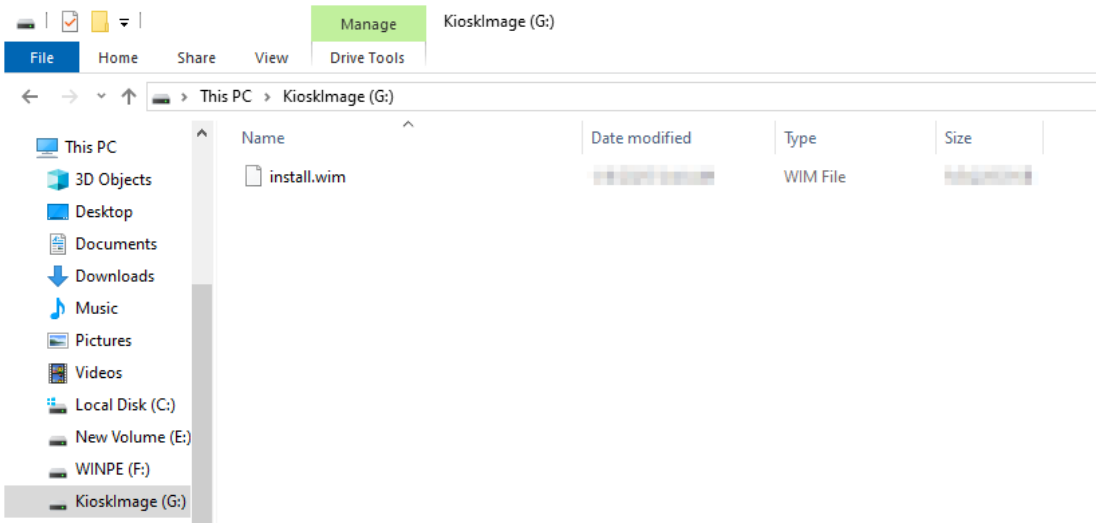
1. Open Rufus and insert the USB drive.
2. Select your USB drive under "Device".
3. Click **SELECT** and select the downloaded **WINPEBootable.vhd**.
4. Click **START.**
5. The drive now has the WINPE partition for booting to the WinPE environment for deployment
6. Using Windows **Disk Management** to format the ***Unallocated space*** of the USB Driver and name it **KioskImage**. This partition will be used for storing the Secure Image package.



Note:
The USB flash drive will now be formatted, so any data on the drive will be lost.

Step 3: Copy Secure Image to the flash drive

1. Input the flash drive to the computer.
2. Copy the file **install.wim** which downloaded from the Step 1 to the **KioskImage** partition.



*** WINPEBootable.vhd**

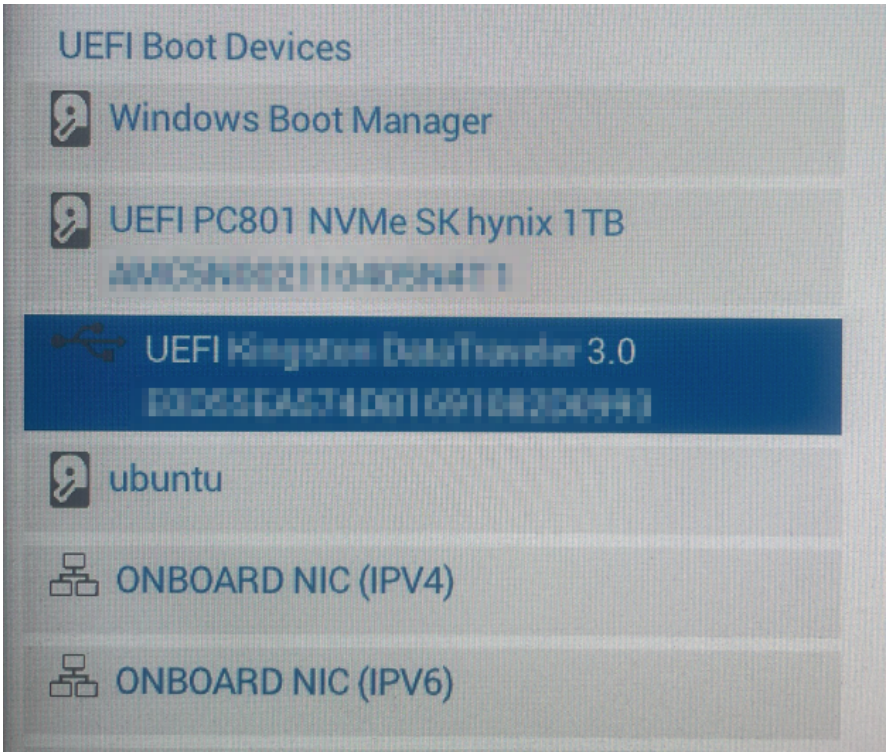
- MD5: 7F4C6B37D941D073039AF291834B78C0
- SHA-1: 1F359A80C412720EE8C6B5902329B7E3AB174548
- SHA-256: C4B770AB55755575BE3C1C97107C0E8CF5D3C261F7671177C861AF5A7770E9B7

MetaDefender Kiosk Secure Image Deployment

Step 1: Boot into Secure Image flash-drive

If you don't have the Secure Image flash-drive ready, please follow Creating Secure Image Deployment flash drive

1. Plug USB into **Kiosk Hardware**.
2. Restart/Power on the device.
3. Keep pressing **F12** during booting up to open **Boot Menu**
4. Select the created USB as boot up media (base on device name)
5. Press **Enter**.

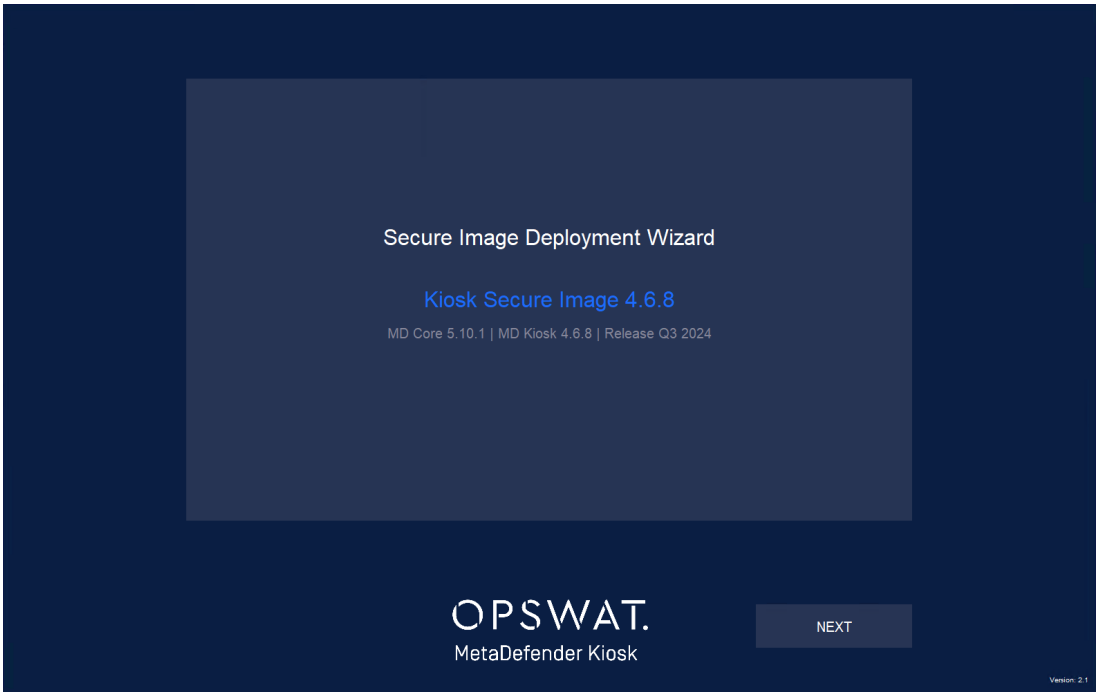


Boot Menu from the Kiosk K1001 (Dell 7410)

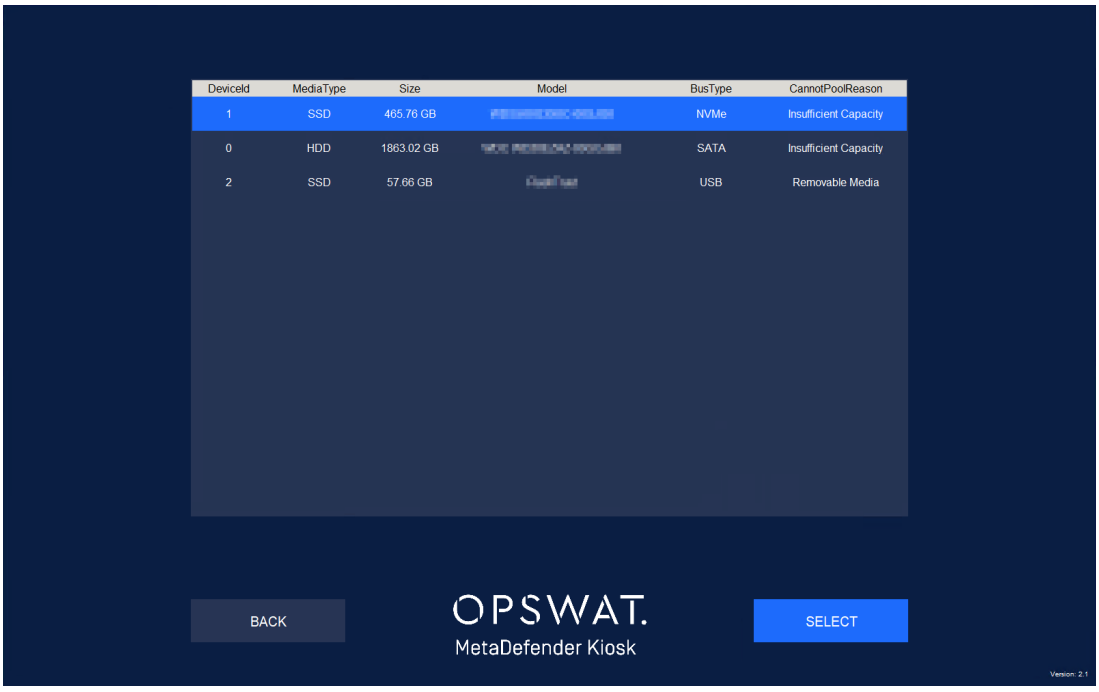
Step 2: Deploy Secure Image

- Following the boot into the WinPE environment, the Deployment Wizrd will appear.

You can see the Image information and click **Next** button to continue to the next step.

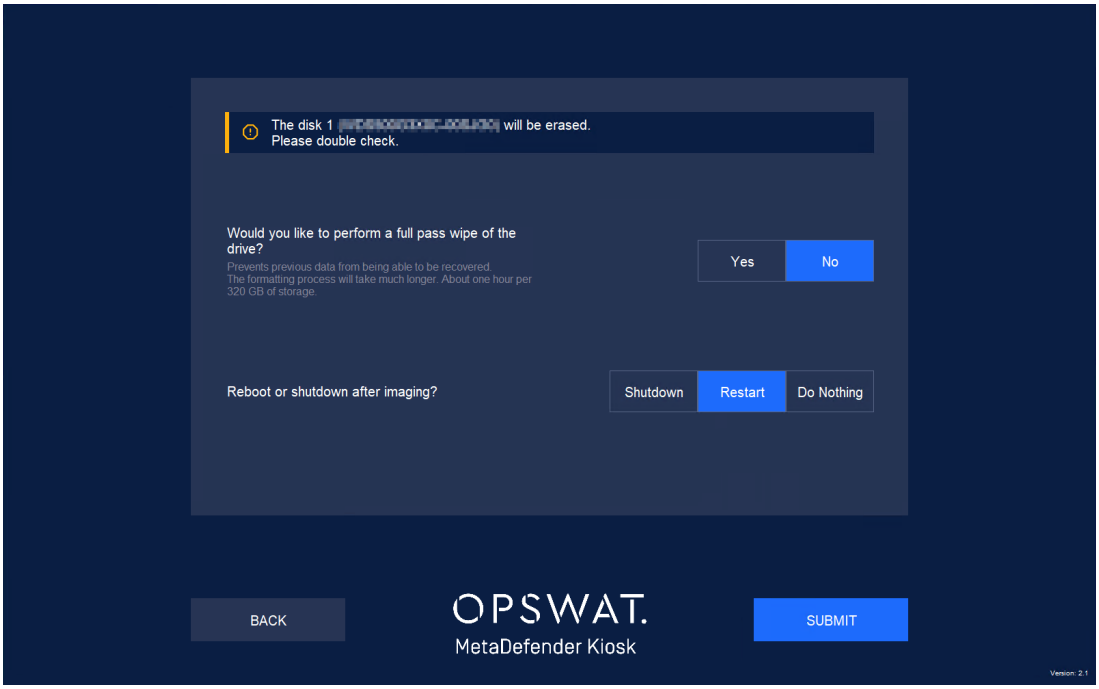


- Choose the disk to apply the image on the next screen.

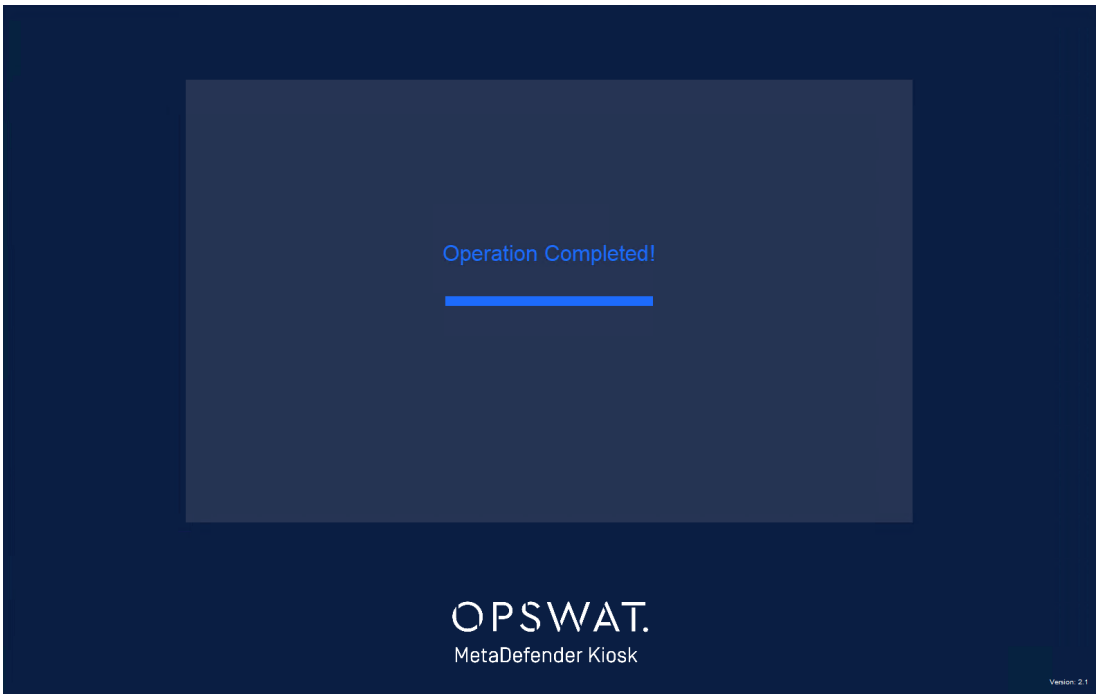


Warning
Make sure that you choose the right disk in this step. The selected disk will be erased for installation

- Choose the desired options, then click the SUBMIT button to start the installation.



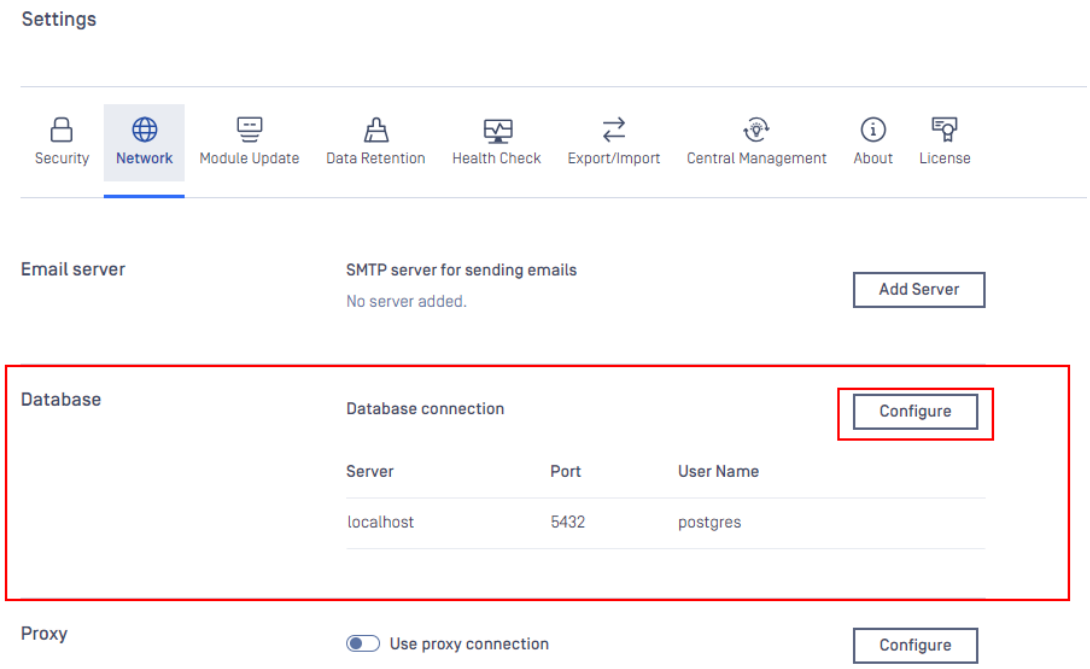
- The process will be processed automatically.



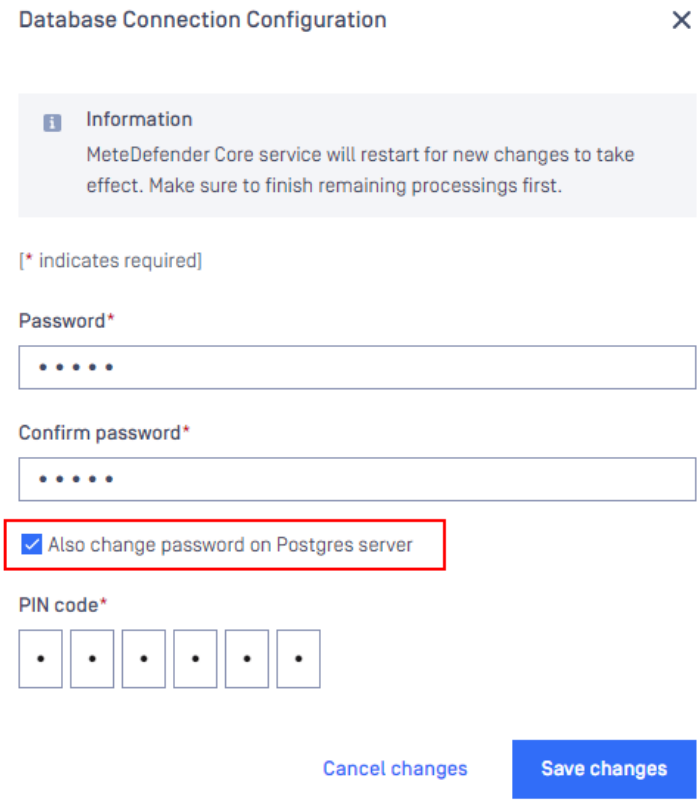
Step 3: Post Deployment Actions

- Change default log-in information for the local windows account:
  - **Username**: KioskUser
  - **Password**: Contact the Customer Support to get the default password.
- To activate MetaDefender Core, you will need to run the **Setup Wizard** on MetaDefender Core, as follows:
  - Go to http://localhost:8008 and follow the **Wizard** in order to create an account and activate MetaDefender Core.
- To activate MetaDefenderKiosk, you will need to run the **Setup Wizard** on MetaDefender Kiosk, as follows:
  - Go to http://localhost:8009/ and follow the **Wizard** in order to create an account and activate MetaDefender Kiosk.
- Connect Kiosk to MetaDefender Core by following the instructions Here.
- Change MD Core Database credential:

From MD Core console, navigate to Settings > Network > Database > Configure



Enter a new password, check the option “Also change password on Postgres Server”



Warning
A PIN code is required for this step. If you haven't setup the PIN code, please set up a PIN code.

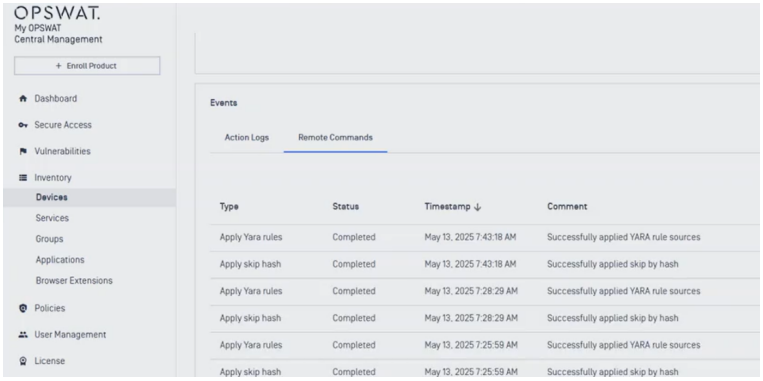
Support:
If you have followed the instructions above but are **Unable To Install And Run MetaDefender Kiosk Using A Bootable Kiosk Flash Drive**, please log a Support Ticket with the OPSWAT team.

Release Notes

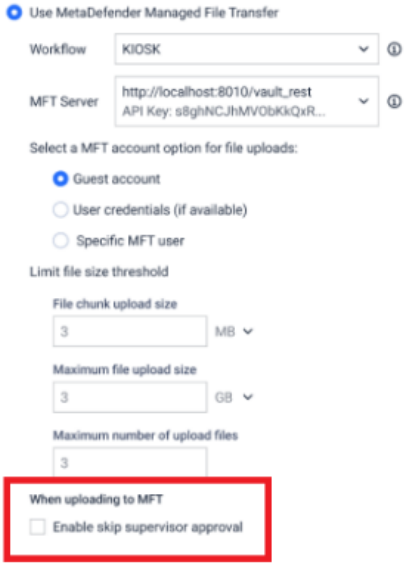
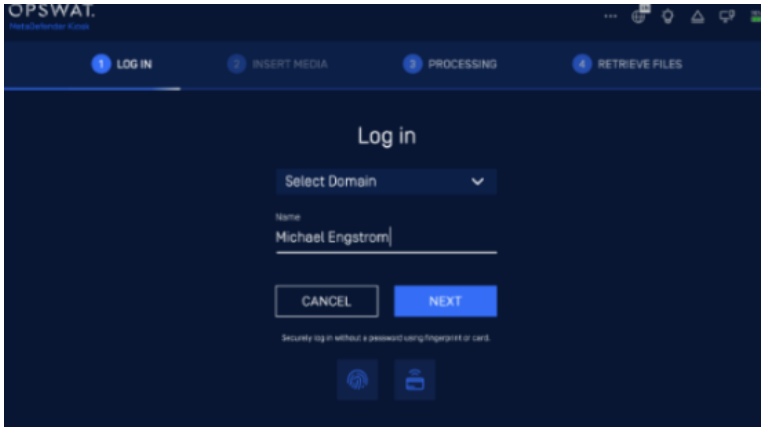
MetaDefender Kiosk 4.7.6

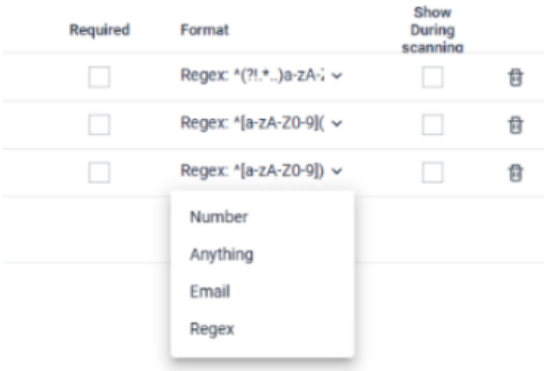
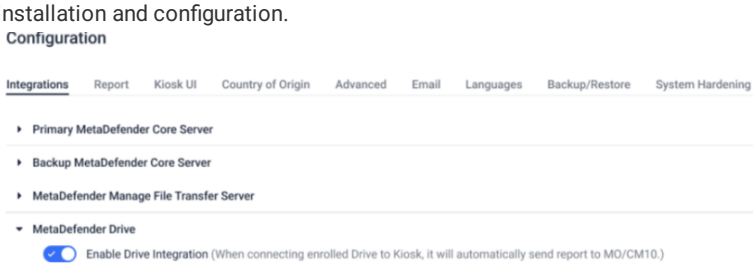
23 May 2025

New Features

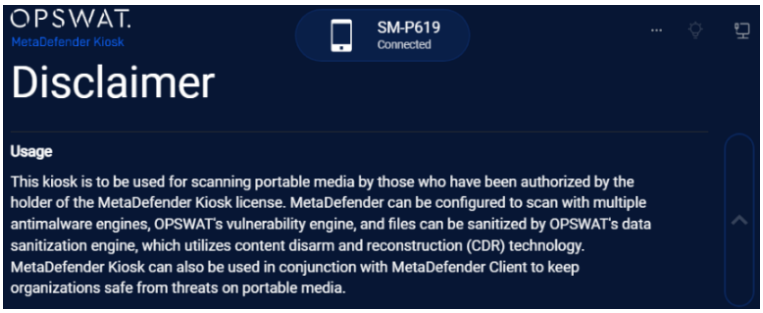
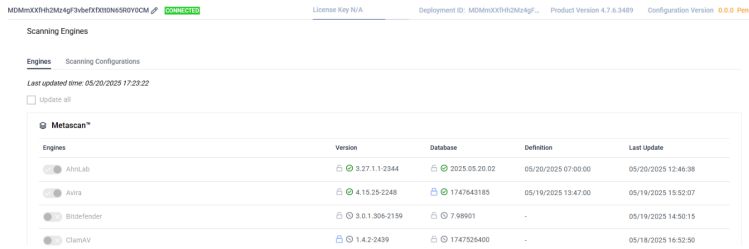
Centralized YARA and file hash management via CM10	Central Management now supports centralized importing of YARA rules and file hashes via REST API. Kiosk will seamlessly apply these items to the embedded Core engine, enabling streamlined, centralized policy enforcement across all connected Kiosk devices. 
Flexible icon visibility controls	Administrators can now choose to hide interface icons entirely or tuck them under the dropdown menu ("..."). These new options give you finer control over the Kiosk UI and let you deliver a cleaner, more customized experience for end users. ▾ Customize Menu bar

MetaDefender Kiosk 4.7.6

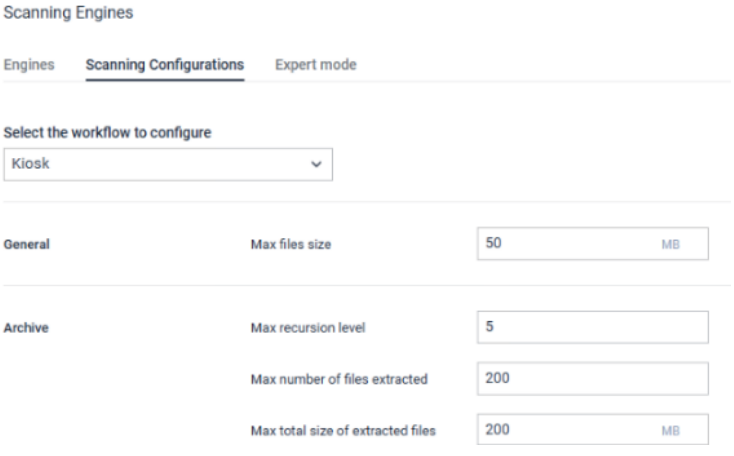
Supervisor MFT approval bypass option	Kiosk introduces a new setting that allows administrators to bypass supervisor MFT approval directly from the Kiosk console. This provides greater flexibility for configuring diverse use cases and streamlining workflows. 
Optional domain selection for active directory login	Kiosk now offers administrators the option to enable domain selection on the login screen when integrated with Active Directory. Enabling this feature displays a domain dropdown, helping users select the correct domain and simplifying the login experience. 

MetaDefender Kiosk 4.7.6	
Enhanced validation for predefined question responses	Administrators can now specify input formats for predefined questions, choosing from free text, number, email, or custom regular expressions (Regex). Users must enter data in the required format to proceed, improving data accuracy and consistency. 
New scanning engine status indicator	The Kiosk UI now displays a status indicator for scanning engines. If an engine encounters issues, a warning (exclamation mark) or critical (cross) icon will appear, signaling the severity. This enhancement improves user awareness and helps administrators quickly identify and address engine problems.
Kiosk supports integration with MetaDefender Drive	Kiosk now supports direct integration with MetaDefender Drive. When an MD Drive is connected, Kiosk automatically uploads stored scan reports to the enrolled Central Management, removing the need for separate SDK installation and configuration. 
Enhancements	-

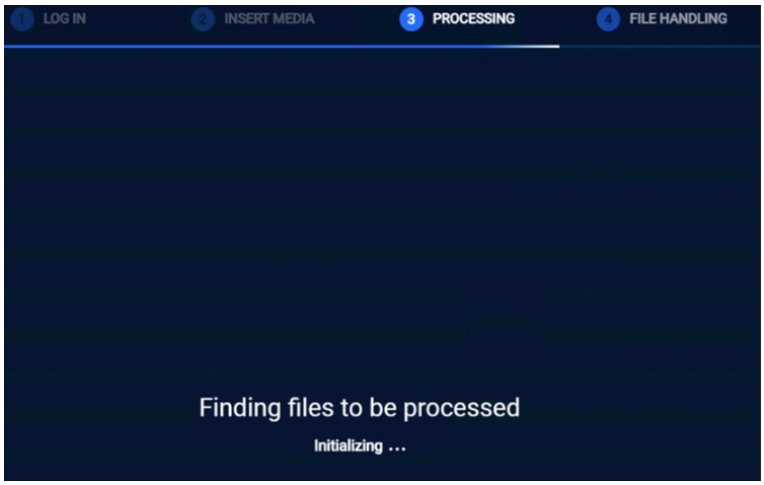
MetaDefender Kiosk 4.7.6

Enhanced media detection across all Kiosk processing screens	Kiosk now detects inserted media (e.g., USB drives) from any screen. When media is inserted, a popup notification confirms detection. If media is inserted while on the Welcome screen, Kiosk will automatically proceed to the User Agreement screen and begin the scanning process. On the Media Detection screen, the detected media is automatically selected for scanning, streamlining the user experience 
Manage scanning engines from Central Management	Kiosk now supports managing scanning engines via My OPSWAT and OPSWAT Central Management, enabling easier configuration and consistent engine updates across multiple devices. 
Option to disable SD Card scanning	Kiosk now provides the ability to disable SD card scanning. This allows administrators to tailor the interface for a cleaner, more streamlined user experience when SD card support is not required.

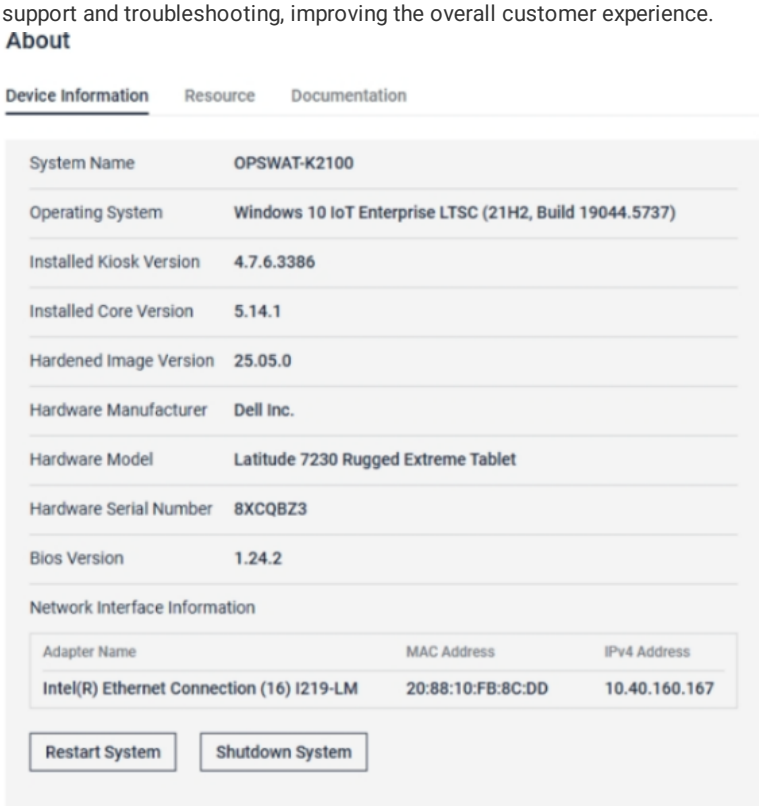
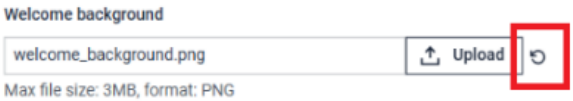
MetaDefender Kiosk 4.7.6

Improved display for Smart Card or RFID as primary login option	When Smart Card or RFID authentication is enabled, Kiosk will now display it as the default login method. Users can still switch to username and password login if preferred, providing flexibility while prioritizing secure access.
Additional client identifier is included when uploading files to MetaDefender Core and MFT	When uploading files to MetaDefender Core and MFT, Kiosk now sends additional client identifiers (hostname, Kiosk ID, username and timestamp) to Core and MFT. This improves My OPSWAT's ability to correlate data and enhances traceability for each scanned file.
New 'Scanning Configurations' tab in Kiosk console	Kiosk now includes an additional **'Scanning Configurations'** tab, enabling administrators to configure basic workflow settings directly within the Kiosk console. More advanced settings will be introduced in future releases to further enhance this feature. 

MetaDefender Kiosk 4.7.6

Improved display during file scan initialization	In previous versions, Kiosk displayed “0 files found” while searching for files to process, which caused confusion for end users. This has been improved to show “Initializing...” during the search to provide clearer feedback. 
Improved unsent scan report synchronization	Kiosk will now automatically synchronize any unsent scanning reports (for example, due to connectivity disruptions) to My OPSWAT once the connection is restored. Additionally, when a Kiosk instance is newly enrolled, any existing locally stored scan data will be sent to My OPSWAT, ensuring improved data consistency and completeness.
Enhanced “About” page with system details	The Kiosk “About” page has been enhanced to display additional details, including the Core version, hardened image version, hardware specifications, service tag, and more. This expanded view provides valuable information for

MetaDefender Kiosk 4.7.6

	support and troubleshooting, improving the overall customer experience. 
Unified Kiosk About page in Central Management	The Kiosk About page in Central Management is now aligned with the version displayed on the Kiosk console, ensuring consistency and improving usability across platforms.
Improved CD/DVD scanning performance	Kiosk now optimized CD/DVD scanning to reduce scan time and enhance the overall user experience, ensuring faster and more efficient processing of optical media.
Support for manifest generation with Unicode characters in file names	Kiosk now fully supports generating manifest files containing Unicode characters in file names (e.g Japanese). By leveraging Unicode APIs and converting file names to UTF-16, Kiosk ensures reliable manifest creation across systems with different locale settings and code pages, enhancing compatibility and reducing encoding-related issues.
Revert customization settings to default	Kiosk now includes an option to revert customization settings, such as logo, color scheme, and other visual elements, back to their default values, making it easier to undo changes and restore the original appearance. 

MetaDefender Kiosk 4.7.6	
Secondary logo now displayed on session end screen	Kiosk now displays the secondary logo on the session end screen, aligning with branding customizations and improving visual consistency across the user experience.
Improved Hebrew translation in Kiosk UI	Kiosk UI improved Hebrew translations, providing a clearer and more accurate user experience for Hebrew-speaking users.
Enhanced support for simultaneous SharePoint and Entra ID (OIDC) integration	Kiosk now supports configuring SharePoint and Microsoft Entra ID (OIDC) simultaneously. Files are correctly transferred under the authenticated user's credentials, ensuring accurate file handling across both MFT and SharePoint/OneDrive workflows.
Support for export and import of offline activated Core	Kiosk now supports exporting and importing configurations of MetaDefender Core instances that were activated offline or via volume license on Central Management. This will also allowed Kiosk Hardened Image to be upgraded with offline-activated Core
Enhance Kiosk Hardened Image Upgrade for greater stability and error handling	Enhanced Kiosk Hardened Image Upgrade with improved stability and bug fix. Critical failures (such as failed to backup Core license) during configuration restoration are now logged in the upgrade history, and ensure the system will automatically roll back to a stable state when needed
Security enhancements	Various security issues have been addressed to enhance the overall security of the system
Bugs	
Resolved Error when saving Syslog settings	Resolved an issue that caused an "Error Saving" message when setting up a Syslog server in Kiosk. The problem was related to how log level settings were handled. With this fix, Syslog configuration now works as expected, regardless of the selected log level.
Known issues	
Backup and restore fails with embedded Core using HTTPS certificate requiring passphrase	Kiosk cannot perform backup and restore when the embedded Core is configured to use HTTPS with a certificate that requires a passphrase.
Upgrade fails when Network Policy Hardening is enabled	When the Network Policy Hardening is enabled, certain network services are disabled as part of the security configuration. This prevents some components (such as firewall and network settings) from being backed up, causing the Kiosk upgrade process failed.

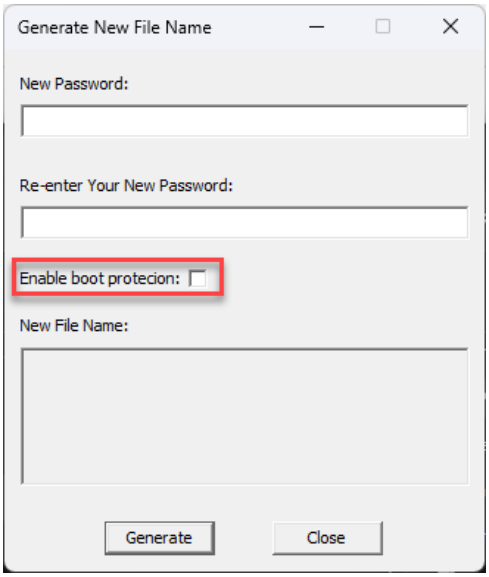
MetaDefender KIOSK Documentation

The users can consult this web page or, alternatively, they can download the manual in pdf format from the link below:

MetaDefender KIOSK manual (SHA256:
45F48BE7A796B9C01FF1DD056C5D400B961A6C0B67727CB3E427D89F65BF73AD).

OPSWAT MetaDefender AGD documentation_v1.2 (SHA256:
45F48BE7A796B9C01FF1DD056C5D400B961A6C0B67727CB3E427D89F65BF73AD).

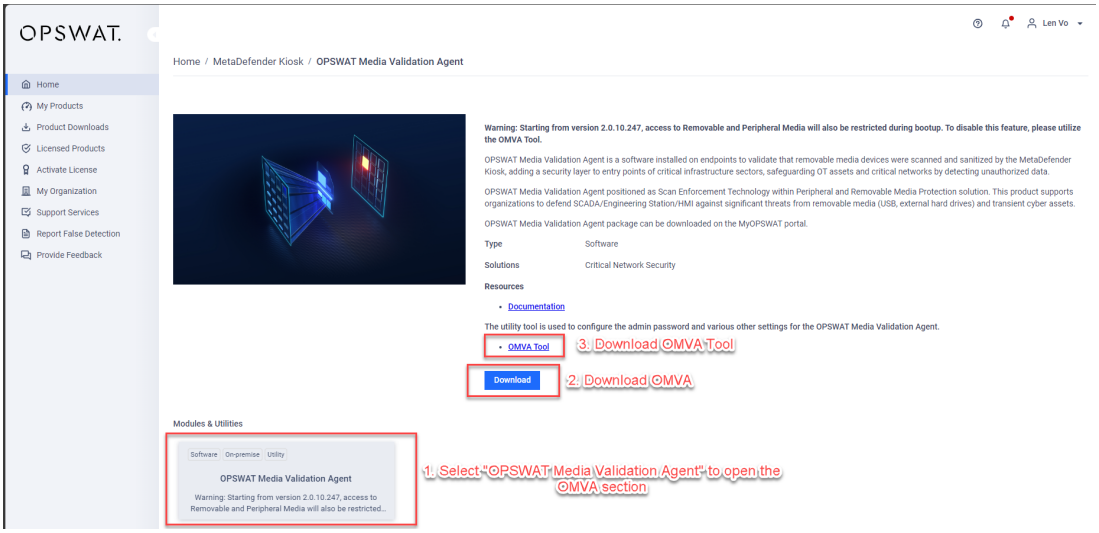
OMVA - Release Notes

OMVA 2.0.10.247	
23 April 2024	
Enhancements	
Boot Protection Enabled	In the latest version, OMVA will validate removable drives immediately after installation and rebooting the machine. This feature enhances the security of the system by blocking potentially harmful removable drives upon boot. Previous versions of OMVA did not block removable drives after rebooting the machine. **Note**: In case administrators do not wish to enable this feature in the new version, they can disable this feature by configuring it using the OMVA Tool and generating a new OMVA installation file for installation on the system. 
Fixed Bugs	
Failed to validate removable devices	Resolved issue where OMVA failed to validate and block certain removable devices.

Downloading OMVA and OMVA Tool:

The new version of OMVA and OMVA Tool are published on the MyOPSWAT Portal.

1. Go to the MyOPSWAT Portal website (https://my.opswat.com) and log in to your account.
2. Navigate to the MetaDefender Kiosk page from the Home Page (https://my.opswat.com/home/metadefender-kiosk) and select the OPSWAT Media Validation Agent module.
3. You can then proceed to download OMVA and OMVA Tool.



Archived Release Notes

Info
Due to documentation changes, offline copy of documentation is no longer available via the Management Console.

4.7.5

MetaDefender Kiosk 4.7.5	
10 April 2025	
New Features	
Sending files to specific MFT users or email addresses via Kiosk	Kiosk now enables end users to send files directly to designated MFT recipients using their username or email address, streamlining the file transfer process.
Send processed file to MFT accounts without authentication required	Kiosk introduces a new option that allows administrators to configure the Kiosk to send processed files to MFT accounts without requiring prior user authentication
Enforce user-selected file classification for file scanning and storing	Kiosk introduces file classification tags prior to scanning, ensuring compliance with data categorization policies. Classified files are seamlessly transferred to MFT along with their metadata.
Kiosk supports OpenID Connect (OIDC) protocol for SSO and Entra ID	Kiosk now supports OpenID Connect (OIDC) protocol for Single Sign-On (SSO) and Entra ID. With this new support, Kiosk allows users to transfer files without pre-logging into MFT first.
Hardening option to disable Network-related services from Kiosk WebMC	Kiosk now supports OpenID Connect (OIDC) protocol for Single Sign-On (SSO) and Entra ID. With this new support, Kiosk allows users to transfer files without pre-logging into MFT first.
Kiosk supports tombstone files on removal	Administrators can enable tombstone files to replace blocked files from both source and destination, providing traceability of removals.
Manage Network Settings from Kiosk WebMC and My OSPWAT	KKiosk now allows administrators to manage network settings directly through the Kiosk WebMC and My OPSWAT (CM7 not supported). System IP addresses and related configurations can be easily modified within the WebMC interface.
Dedicated workflow for Self-scan	Kiosk supports a dedicated Self-Scan workflow, enables administrators to configure scanning settings more effectively for user-specific needs.
Option to display question responses during file scans	Administrators can configure Kiosk to display question responses during file scans for improved usability and context awareness.
Apply background image to all Kiosk UI screens	Kiosk now allows administrators to apply a custom background image across all Kiosk UI screens, providing greater flexibility and branding opportunities for user interface customization
Support Biocryptodisk ISPX Track encrypted USB	Added support for Biocryptodisk ISPX Track encrypted USB device
Enhancements	-

MetaDefender Kiosk 4.7.5	
Improve USB detection time in Kiosk devices with floppy drive connected	UOptimized USB detection performance in environments where floppy disk drive is present.
Enhance Kiosk Hardened Image Upgrade for greater stability and UX/UI	Enhanced Kiosk Hardened Image Upgrade with improved stability, better UX/UI, and bug fixes
Kiosk UI displays network status	The network status is now displayed directly on the Kiosk UI for better management and support.
"Upgrade Now" and "Rollback" are supported in My OPSWAT	"Upgrade Now" and "Rollback" options are now supported in My OPSWAT, allowing administrators to manage software updates more efficiently
UI enhancement in Media Selection to avoid confusion	Improve Kiosk UI in Media Selection screen to prevent certain elements from appearing as buttons to avoid confusions
Disable timeout on Kiosk UI	Administrators can disable the timeout for Kiosk UI entirely, preventing session interruptions and improving user experience.
Include file size in scan history	Processed files in scan history includes a file size column for improved visibility and tracking
Improve handling of unmountable VMDK and TIB files	Improve handling VMDK and TIB files that cannot be mounted. Kiosk will now block these files to maintain security.
Security enhancements	Various security issues have been addressed to enhance the overall security of the system.
Bugs	
Resolved incorrect file assignment for non-existence MFT Users	Fixed an issue where files uploaded to a non-existent MFT user were incorrectly assigned to the admin account instead of the Guest account.
Resolved Kiosk crash during email parsing	Fixed an issue where Kiosk could crash while parsing email content.
Resolved Unexpected Return to Setup Wizard	Fixed an issue where Kiosk could unexpectedly return to the initial setup wizard.
Known issues	
Files are uploaded to MFT Guest ID when uploads fail	When uploading multiple files from Kiosk to MFT, failed uploads may be incorrectly redirected to the MFT Guest account and displayed to the user

MetaDefender Kiosk 4.7.5	
Kiosk may become unresponsive when wiping encrypted IronKey S1000 USB	When wiping an encrypted IronKey S1000 USB drive, it may cause the Kiosk to become unresponsive

4.7.4

MetaDefender Kiosk 4.7.4	
7 March 2025	
Fixed Bugs	
Fixed issue with black screen after upgrade in-place from an older version	Fixed an issue where Kiosk got stuck on a black screen after an in-place upgrade from an older version with the "Boot Hardening" feature enabled.
21 February 2025	
New Features	
Enhanced Kiosk UI customization	Administrators can now update the logo and background image directly from WebMC. Additionally, you can customize the background and text colors for a more tailored user experience.
Select Blocked Files for Removal	Kiosk introduces a new option that allows users to select specific blocked files for removal, providing more control and flexibility
Kiosk-Generated Manifest File for Improved File Control	Administrators can configure to generate the manifest file directly from Kiosk system. This manifest enhances control over which files are allowed or blocked before being uploaded to MetaDefender Core, ensuring better integration with MD Endpoint and MD Firewall.
Support OAuth Email Authentication for Microsoft 365 (Graph API)	Kiosk now supports OAuth authentication for email integration with Microsoft 365 (Graph API)
SSO Integration with OIDC Support	Kiosk now supports integration with SSO Identity Providers using the OIDC protocol, verified with Manage Engine SSO
Support retrieving file from MFT with SSO OIDC	Supports retrieving files from MFT (version 3.9.0.1 or later) when configuring with SSO OIDC
Manage Core configuration directly in Kiosk WebMC	Kiosk WebMC now supports direct management of MetaDefender Core configurations, including scanning engine status and updates. Additional Core configuration options will be introduced in future updates
Option to disable screensaver while scanning files	Kiosk introduces a new option that allows administrators to disable the screensaver while scanning files and reviewing scan result.
User Questions support Multi-Language	User questions now support multiple languages. When switching to a different language, the user questions will automatically update to match the selected language
Enhancements	

MetaDefender Kiosk 4.7.4	
Enhanced Auto-Upgrade for Kiosk Hardened Image	The auto-upgrade for Kiosk Hardened image has been improved for greater stability. This release also includes refined wording and visual enhancements for a better user experience. Administrators can now upgrade Kiosk Hardened Image via OCM.
Kiosk application supports Windows 11	Kiosk application now supports Windows 11, ensuring compatibility and performance on the latest operating system
Session log file information is now recorded in the manifest generated by Kiosk	Information of Session log files is now recorded in the manifest generated by Kiosk, ensuring compatibility with OMVA when media containing session log files is used
Restructure layout of settings in Kiosk WebMC	Layout of settings have been restructured for a cleaner and more intuitive experience
Improved AD Login Format Support in Kiosk WebMC and UI	Kiosk WebMC and UI now support Active Directory login using multiple formats, including: • Username • Domain\Username • Username@Domain This enhancement provides greater flexibility for user authentication.
Eject and Exit Button Now Visible in Kiosk UI Settings Bar	The Eject and Exit button is now displayed in the Kiosk UI settings bar, providing users with a clearer and more accessible way to exit the interface.
Support for filenames with special characters in OneDrive file transfers	Enhance file transfer to OneDrive by adding support for filenames with special characters
Bugs	
Fixed Deployment ID change not reflecting in Kiosk UI	Resolved an issue where the Deployment ID change did not update correctly in the Kiosk UI, causing license activation failures. The UI now correctly reflects the Deployment ID
Fixed configuration save issue after upgrade	Kiosk version 4.7.4 fixed an issue where data fields is missing after upgrading from an older version (such as 4.6.3) prevented the Guest workflow configuration from being saved.

4.7.3

MetaDefender Kiosk 4.7.2	
27 December 2024	
New Features	
Auto Upgrade Kiosk Hardened Image	In MetaDefender Kiosk version 4.7.3, administrators can initiate the upgrade for Kiosk Hardened Image (version 25.01.0) directly from Kiosk WebMC. The upgrade process backs up essential system and product configurations, automatically downloads the latest version of Kiosk Hardened Image, and performs the upgrade. In case of failure, Kiosk would automatically revert to the previous version to ensure continuity.
Enable RDP (Remote Desktop Protocol) from Kiosk WebMC	Administrators can enable RDP (Remote Desktop Protocol) through Kiosk WebMC. Once enabled, Kiosk will modify the necessary services and settings.
Support for RFID card authentication	Kiosk now supports RFID card authentication. The user can register and associate a new RFID card with their AD account.
Support timezone for syslog messages	Administrators can now configure timezone when integrating with the syslog server.
Support for new encrypted USB Devices	Kiosk supports the following encrypted USB devices: • DataLocker Sentry 3.0 • DataTraveler Vault Privacy 3.0 (DTVP30M-R)
Support MongoDB password during Kiosk installation	During the Kiosk installation process, administrator can set a password for the MongoDB database for encryption.
Enhancements	
Improved Configuration Backup and Restore	Additional information included in Configuration Backup and Restore: • Computer host name • Custom Kiosk sound file • Windows Security Certificates • Configurations of MetaDefender Core
Kiosk does not automatically end the session	After the scanning session is completed, Kiosk pauses on the final screen for user acknowledgement.
Improved information in Kiosk UI startup process	The initial process of starting the Kiosk UI has been broken down into smaller steps to provide more detailed information and improve troubleshooting.

MetaDefender Kiosk 4.7.2	
Show the created date of files when selecting files	Kiosk UI now shows the creation date of files on the selection screen for files processing.
Kiosk instance remains enrolled in My OPSWAT	Once a Kiosk instance is enrolled in My OPSWAT, it remains enrolled indefinitely and will not unenroll automatically. It can only be unenrolled if an administrator manually deletes or unenrolls the instance
Support SCSI USB devices	The Kiosk now supports copying processed files to SCSI USB devices
Improve character counting accuracy for foreign languages	Improve the character counting method to ensure greater accuracy when enforcing character limits for some foreign languages which require the use of Input Method Editor (IME), for example, Hebrew

4.7.2

MetaDefender Kiosk 4.7.2	
04 November 2024	
Hidden MD Core Console from KIOSK UI	In this new KIOSK version, access to the MD Core Console has been disabled in the KIOSK UI to address certain security concerns.
18 October 2024	
New Features	
Support for Smartcard authentication	Kiosk now supports Smartcard for user authentication. **Limitation:** Authentication for MFR file retrieval is not supported
Embedded Management Console within Kiosk UI for streamlined configuration	Administrators now can access and manage configurations directly from the Kiosk UI without exiting the application. A gear icon on the top right opens Kiosk Management Console for configuration.
Support copying processed files to SharePoint and OneDrive	Administrator now can configure the option to copy processed files to SharePoint or OneDrive directories. Before utilizing this feature, it is necessary to setup Microsoft Entra ID with API integration. If the destination path is left empty, Kiosk will automatically copy the files to the root folder.
Configuration backup and restore enhancement	This update includes additional configurations for backup and restore functionality. Administrators can choose the specific configurations to restore: • Local Windows Certificates: Restore all trusted certificates from Certificate Microsoft Management Console (MMC) • System Hosts file: Restore the custom Hosts file at C:\Windows\System32\drivers\etc\hosts • License: Restore the activated Kiosk license • Branding and Logo Customization: Restore logo and branding files found in C:\Program Files (x86)\OPSWAT\Metadefender Kiosk\Client\en\resources • Secure connection: Restore the security certificate and enable Secure Connection option • User management: Restore configured User Directories (AD, SSO and Entra ID) and accounts • Known Wi-Fi network: Restore the known Wi-Fi networks (***Notes****__: this feature is only available in Kiosk version 4.7.2 or later*)

MetaDefender Kiosk 4.7.2	
Change logon password on Kiosk Hardened Image	Administrators can now change user logon password directly from Kiosk Management Console on Kiosk Hardened Image. (***Notes:*** *This feature is only available on Kiosk Hardened Image. This settings cannot configured via My OPSWAT and the Set setting of OCM*)
Enhancements	
Permission control on end user folders when copying files	When Kiosk is configured to copy processed files to a destination folder, the Administrator can choose to copy the files to the end user's folder with specific permissions. • Inherited: Files and folders will inherit the same permissions as the parent folder • Restricted: Only the file owner will have the permissions to access the files and folders
Support on-screen French (AZERTY) keyboard layout	Kiosk now supports on-screen keyboard for French (AZERTY) layout.
Support on-screen Chinese (Traditional) layout	Kiosk now supports on-screen keyboard for Chinese (Traditional) layout.
Display file progress and results for file retrieval	Kiosk now shows the file scanning progress and results when retrieving files.
Hide on-screen keyboard with physical keyboard connected	When a physical keyboard is connected, Kiosk will automatically hide the on-screen keyboard. Administrators can click the keyboard icon on the top right corner to toggle the visibility of the on-screen keyboard.
Improve stability when generating Kiosk support package	Improve stability when generating Kiosk support package.
Improve stability of database when scanning files	Improved stability of database to avoid performance impact when scanning large volumes of files
Improve AD authentication mechanism to prevent user account lockout	In the previous versions, multiple failed sign-in attempts to the Kiosk UI could cause users to be locked out due to Active Directory policies. This new version enhances the AD authentication mechanism to prevent unnecessary fallback methods, reducing the risk of user account lockouts during login attempts.
Enhanced Self-scan on all drives	All drives in the system will be scanned when using Self-scan feature, including the boot sector. When malicious files are detected in the boot sector, Kiosk will lock the system and inform the Administrator.

MetaDefender Kiosk 4.7.2	
Support more variables in Email Session Report template	Kiosk supports more variables in Email Session Report template: • session_id: Kiosk session ID • start_time: Start time • end_time: Finish time • device_model: Media model • device_serial_number: Media serial number • device_media_type: Media type • device_id: Media ID • total_files_scanned: Total files were scanned • blocked_files: Number of files were blocked • allowed_files: Number of files were allowed • skipped_files: Number of files were skipped scanning • remediated_files: Number of files were remediated
Enable select files or process all files at workflow level	In the new version, Administrator can configure enable select files or process all on each individual workflow. • Select files: User can select files for processing • Process all files: User has to process all files in the media • Select or process all files: User can select between 'Select files' or 'Processing all files' option • Disable file processing: Kiosk does not process file • Use Global Settings: Apply the Global Settings (under configurations > Kiosk UI > Choose Files Scanning Option)
Support unlocking encrypted USBs with passwords containing special characters	Kiosk supports unlocking encrypted USB devices with passwords containing special characters.
Enhanced visual appeal and engagement for Kiosk UI	Several components of the Kiosk UI have been updated with a modern design, enhancing visual appeal and user engagement.
Known Issues	
Cannot apply Disclaimer via OCM or My OPSWAT Set settings	After applying a custom Disclaimer from the Set settings in OCM or My OPSWAT, the custom Disclaimer does not apply to instance within the Set. This will be addressed in the next version.

4.7.1

MetaDefender Kiosk 4.7.1	
24 September 2024	
Enhancements	
Support burning files over 2GB to DVDs and Blue-rays	Users can now burn single or multiple files larger than 2GB to DVDs and Blu-rays, removing size limitations.
Enhance logging for troubleshooting	Logs have been enhanced to include additional information, providing more context and details for troubleshooting.
Fixed Bugs	
Issue with entire email displayed in Bold text when Heading was used	Resolve the issue that caused entire body of email to appear in Bold text when Heading setting was used. Only intended section will now use bold format, ensuring accurate email presentation.
Issue with failing to create backup file	Resolved issue where Kiosk failed to generate backup files when large crashdump files were present, causing the backup process to fail. This fix excludes crashdump files from the backup, including only the necessary files to ensure a smooth backup and restore process.
Unable to modify AD settings when AD server is unreachable	After upgrading Kiosk, users were unable to modify Active Directory (AD) server settings if the AD server was not reachable. If the AD server is accessible, the settings can be changed without any issues. This fix ensures settings can be changed even when the AD server is unreachable.
Empty workflow page after importing configuration backup	Resolve issue when importing a configuration backup, the workflow page appeared empty due to certain fields not being included in the backup. This fix ensures that all necessary fields are automatically included when importing a backup.
Cannot enable Boot Hardening feature	Resolve issue where users were unable to enable Boot Hardening feature. After enabling the setting and refreshing the page, the setting reverted to being disabled. This fix ensures that the Boot Hardening setting remains enabled after being applied.
Kiosk UI became unresponsive when scanning large files containing numerous encrypted archive files	Kiosk UI became unresponsive when scanning large files containing numerous encrypted archive files. This fix optimizes the scanning process to improve stability and prevent the UI from becoming unresponsive when handling large files with many encrypted archives.
High memory consumption in Kiosk service during scan results display	The Kiosk service was consuming a high amount of memory when displaying scan results for a large number of files. This fix optimized memory usage when displaying large scan results.

MetaDefender Kiosk 4.7.1	
Kiosk UI hangs when connection to Core is lost	Resolve issue where Kiosk UI would hang when the connection to the Core was lost. This fix ensures that the Kiosk UI automatically attempts to reconnect to the Core when the connection is lost, allowing it to resume file scanning.
Security enhancements	Various security issues have been addressed to enhance the overall security of the system.
30 August 2024	
New Features	
Screen Brightness Controls	Users can adjust screen brightness directly on the KIOSK UI, which is particularly useful for installations in low-light environments.
Display OS Name and IP Address	The OS name and IP address of the KIOSK are now displayed on the KIOSK console, making it easier to identify and manage the OS and network configuration of the device.
Support for new encrypted USB Devices	The KIOSK supports the following encrypted USB devices: • USB DataTraveller DTVP30M-R • USB IronKey D300S • USB IronKey D500S
Session log storage on secondary media	Administrators can now configure the KIOSK to save session logs to secondary media during file copy operations. Previously, session logs were stored on the source USB only. *(Note: Session logs are currently not included in the manifest file, so the USB will not be unblocked with OMVA. You can use MetaDefender Endpoint (Standalone) to access the files on the USB.)*
MFT Guest ID verification support	Administrators can now control Guest IDs rather than relying on automatic generation by the KIOSK. Before starting a scan using the Guest workflow, users must input pre-existing MFT Guest IDs generated on the Managed File Transfer (MFT) system.
Manifest storage configuration	Administrators can configure the KIOSK to store the manifest only on the secondary USB instead of both the source and secondary USBs, ensuring the integrity of the source USB data.
Log file size retention support	Enhanced logging control and optimized storage space by supporting log file size retention.
Enhancements	

MetaDefender Kiosk 4.7.1	
Windows Registry Interaction Update	To mitigate security risks flagged by some Endpoint Detection and Response (EDR) systems, functions previously relying on reg.exe to interact with the system registry have been updated to use the Windows API, improving system integrity and compliance with security standards.
Copy to Original DVD Support in Copy&Go	The KIOSK now supports copying clean data back to the original DVD during the Copy&Go process, addressing customer needs for this functionality.
Additional hash information in Manifest File	SHA-1 and MD5 hash values have been added to the manifest file, allowing customers to audit and query scan information more easily.
Support for double quote character in passwords	The KIOSK now allows the double quote character (") in passwords when adding certificates to the system.
Sanitized files list in KIOSK UI results	The KIOSK UI now shows a list of files that were sanitized, providing users with detailed scan results and a better understanding of why certain files were blocked or allowed.
Fallback Mechanisms for File Copy Operations	Implemented essential fallback mechanisms to handle exceptions during file copy operations to the secondary USB, ensuring more robust and reliable performance.
Watchdog Feature Improvement	Enhanced the Watchdog feature to ensure that the KIOSK does not restart after pressing the keyboard combination (ALT + S) when the "Reboot at the end of session" option is enabled. This improvement prevents unintended restarts and ensures a smoother user experience.
MFT Guest Code Visibility	Users can now configure the visibility of the MFT Guest Code in the KIOSK UI, allowing more time to record the code for easier file retrieval.
Security Enhancements	Various security issues have been addressed to enhance the overall security of the system.
Fixed Bugs	
Issue with Custom Authentication Configuration on OCM7	Resolved an issue where administrators were unable to edit the configuration of custom authentication on OCM7. This fix restores full control over authentication settings for administrators.

4.7.0

MetaDefender Kiosk 4.7.0	
09 August 2024	
Webpage loading on KIOSK Console	Optimized resources on the webpage to enhance the user experience.
Fixed Bugs	
Issue with Certificate Configuration	Resolved issues related to configuring certificates on the KIOSK Console, making it easier for admins to manage certificates. (**Note**: *From this version onwards, to enhance security, KIOSK will no longer support private keys using insecure DES encryption.*)
Issue with Configuring "Exit Credential"	This version addresses the issue where KIOSKs were unable to update the "Exit Credential" configuration from OCM/My OPSWAT through Set/Group settings.
29 July 2024	
New Features	
Innovate the KIOSK Web Management Console	The KIOSK Web Management Console has been totally revamped with a more streamlined and user-friendly design, making it easier than ever to configure your KIOSK.
Support Microsoft Entra ID Authentication on Kiosk UI and Web Management Console	Officially support to configure Microsoft Entra ID as new authentication method for both KIOSK UI and Console through the SAML 2.0 protocol. See Microsoft Entra ID Integration for more details.
Encrypted Drive Verification and Approval	The Kiosk system protection functionality will check file integrity in the unlocked partitions of encrypted peripheral media devices before decryption. The encrypted devices containing unauthorized data will be spotted and require approval before being added to the data whitelisting and usable with the Kiosk system. See Encrypted Device Verification And Approval for more details.

MetaDefender Kiosk 4.7.0	
Continuous support for My OPSWAT integration	The administrator can now centrally manage KIOSK(s) from My OPSWAT with the following additional product functionalities: • Configuration • Workflows • Logs • Product license activation • Uploading custom disclaimer
Support UK keyboard layout	Users can now input UK characters from the Kiosk UI by using the UK keyboard.
Enhancements	
Enhance stability and security of KIOSK application	Carry out database improvements and update third-party dependencies to the most recent stable version.
Enable searching through the KIOSK Console session history by submitting a large file	The user can now submit a file larger than 200MB to search for in the KIOSK Console session history.
Compatible support with the new version of CimTrak	Compatible support when integrating with CimTrak 4.1.41
Improve the printing process	Eliminate KIOSK usage or creation of PowerShell script when utilizing the printer to align with the whitelisting service.
Fixed Bugs	
Issue copying the remediated file after scanning	Fixed the issue cannot copy the remediated file that was downloaded from MD Core after scanning to a shared folder with Kiosk logged-in user permission
Issue when retrieving files from the network share	Ensure that the authorized AD user can retrieve files from a network share.

MetaDefender Kiosk 4.7.0	
Issue when unlocking Kanguru Defender 3000 with the latest firmware	Enhance KIOSK compatibility when unlocking the encrypted USB Kanguru Defender 3000 with firmware version 5.6.7.0
Known Issues	
Issue whelssue when upgrading in-place from older versionsn upgrading in-place from older versions	KIOSK has upgraded several 3rd party components in this version. Therefore, when upgrading from very old KIOSK versions, administrators should uninstall the current KIOSK version to clean up the system before reinstalling version 4.7.0. After reinstalling, configurations will be retained as they were before.
Issue with Custom Authentication on OCM7	Administrators cannot edit the configuration of custom authentication on OCM7. This will be addressed in our next versions.

4.6.8

4.6.8	
16 May 2024	
New Features	
Support for Trellix Encrypted USB	KIOSK can now decrypt and scan Trellix encrypted USB drives using a USB password.
Post-Scan Actions for files inside disk image files	After scanning, KIOSK can copy files from within disk image files to a network share/MFT/Media. Details here: Processing virtual disk files
Support for scanning nested Disk Image Files	The KIOSK functionality enables comprehensive deep scanning of disk image files by seamlessly mounting and scanning all nested files within, ensuring thorough analysis even in the presence of multiple layers of disk image files.
Enhancements	
Improved scan speed for small files	We have enhanced the scanning mechanism to speed up the processing of small files. The self-scan speed has significantly improved in this version. Detailed performance metrics are available on this page: Performance measurement of Self Scan
Enhanced Scan Limits setting for file extensions	Administrator can configure file extensions that users are not allowed to select for processing in the KIOSK UI. **Note:** Scan limits do not apply to the Simplified Workflow.
Improved UX for scanning disk image files	KIOSK now displays the scanning progress for files inside disk image files, and users can view detailed scan results for these files after scanning (via the KIOSK UI or session logs).
Improved application log for engines status	Detailed engines information and status are now shown in the application log when issues occur.
On-Screen Keyboard on KIOSK UI for ADFS Login	An on-screen keyboard is now available for login using ADFS on the KIOSK UI.

4.6.8	
Enhanced Authentication with Nested AD Groups	KIOSK now more accurately authenticates users within nested AD groups.
Improved detection of external CD/DVD ROM	Users can scan CD/DVD after starting a session on KIOSK and connecting an external USB CD/DVD ROM.

4.6.7

4.6.7	
17 April 2024	
Memory Optimization	Addressed an issue where the KIOSK UI experienced excessive memory usage when scanning with a high number of threads. Optimizations have been applied to the memory management processes of KIOSK UI, specifically tailored to handle large-scale thread operations more efficiently.
12 April 2024	
Features	**Descriptions**
Customizable Disclaimer Page	Administrators can customize the disclaimer page of the KIOSK user interface. Admins can create a custom disclaimer page using an HTML file and upload this custom page for the corresponding language. (**Note**: Currently, there is a limitation where customized disclaimer files cannot be applied to group instances from CM7.)
Enhancements	
File Limit Settings	Implemented features to limit file size, total number of files, and total file size when users choose to copy files to a network shared drive without processing through Metadefender Core. (**Note**: These limits do not apply to retrieving files from MFT).
Disable USB Scan	Administrators can now disable the USB scan feature on the KIOSK UI. Administrators need to disable the "Allow user to browse for files" and "Allow user to process all files" options in the KIOSK console. In this case, users will only be able to perform other actions (such as: Retreive file from MFT) on the KIOSK UI.
Improved UX for Copying Files to CD/DVD	Enhanced user experience when copying files to CD/DVD. Currently, KIOSK does not support wipe for CD/DVD. If an administrator configures wipe before copying files to CD/DVD and a user attempts to copy files to a CD/DVD with existing data, KIOSK will display an error message and allow the user to change to another blank CD/DVD to copy files.
Fixed Bugs	
MFT File Retrieval Issue	Fixed an issue where files could not be retrieved from MFT when the option "Do not process files with Metadefender or MFT server" was enabled. This issue has been resolved in this version.
Login Issue for Users in AD Groups with Hebrew Characters	Fixed an issue where users couldn't log in if they belonged to an Active Directory group with Hebrew characters in the group's common name.
Known Issues	

4.6.7	
The simplified workflow with the file size limitation	The simplified workflow is currently optimized to streamline user operations. So the limits related to file size/total file are not yet supported on the simplified workflow.

4.6.6

4.6.6

26 March 2024	
Security Update	Improved security measures for the KIOSK Console to enhance overall system security.
27 February 2024	
Features	**Descriptions**
Support for ADFS Authentication in KIOSK UI and Console	Admin can configure authentication for KIOSK (Console/UI) through the SAML protocol. More info
Password Requirements Before Copying Files to USB	User can enter a password to encrypt files retrieved from MFT before copying them to the destination USB.
File Size Limitation for Scanning	Limit the size of files that users can select for scanning. Admins can configure the maximum size of files on the KIOSK/CM console that users are allowed to scan through KIOSK UI.
Total File Size Limitation	Limit the total size of files that users can select for scanning. Admins can configure the maximum size of the total files on the KIOSK/CM console that users are allowed to scan through KIOSK UI.
Total File Quantity Limitation	Limit the total number of files that users can select for scanning. Admins can configure the total file quantity on the KIOSK/CM console that users are authorized to scan through the KIOSK UI.
File Blocking by Extension	Supports users blocking files by file name extension. Admins can configure file extensions that they want to block on the KIOSK/CM console. KIOSK will block these file extensions without uploading them to MD Core server to get scanning results.
Display Incident Detections on CM Console	Supports users tracking incident detections on the CM Console. Admins can track incidents originating from KIOSK, users, or sessions.
Support for Encrypted USB Viasat UK Freedom 100	Added support for encrypted USB Viasat UK Freedom 100.
Embedded Sandbox Engines in KIOSK	Supports scanning files with an embedded Sandbox engine in KIOSK.
Enhancements	

4.6.6	
Improved File Copy Speed	Improved file copy performance by increasing the number of threads copying files simultaneously. Admins can configure the thread count on the KIOSK/CM console. More info

Fixed Bugs	
Could not select files for scanning Issue	Fixed the issue where users could not select files for scanning when the "Email current user" option is enabled.
Issue with custom language configuration on KIOSK Console	Enhanced upgrade mechanism to ensure system configurations are updated correctly.
KIOSK UI Freezing	Addressed issue where KIOSK UI would occasionally freeze when performing tasks with encrypted USB.
Black Desktop Screen on Hardened Image	Fixed issue where the screen turns black after running KIOSK for a period of time on the hardened image.
CD/DVD Ejection Issue	Fixed issue where KIOSK would fail to perform tasks after users ejected CD/DVD while scanning with KIOSK.
Issue with Manifest File	Improved checks and handling for manifest files to ensure more accurate system operation with manifest files in the new version.
Unable to save user password at "Enter Vault server to upload files to" option	Fixed issue the users were unable to save their password after updating the password for "Enter Vault server to upload files to" previously.
Wipe Data on Bitlocker Drive	Fixed issue where users couldn't delete data on Bitlocker drive when wiping the drive with KIOSK.

4.6.5

4.6.5 Hotfix **5 Jan 2024**	**Major release with new features and enhancements**
Failed to copy archives with large child files	A critical issue when transfering a large amount of files to MFT has been found and fixed

4.6.5 **28 Dec 2023**	
Features	
Navigate to Sub-Folders on Network Drive	Users can now navigate to sub-folders on a network drive when performing a Copy-To operation
Hidden Partition Information in Scan Report	Added information about hidden partitions in the scan report for comprehensive insights
Improved Remaining Scan Time Calculation	Enhanced the accuracy of calculating the remaining scan time
Enforce Local Login Setting	Introduced a setting to enforce local login, enhancing security measures
Stop Processing Files on Block	Added support to halt the scanning process when a specific number of files are blocked
Hide Default English Language in KIOSK UI	The administrator now has the option to hide the default English language in the KIOSK UI
Improved Scan Result Display Speed	Enhanced the speed of displaying scan results for a more efficient user experience
Anti-Tamper Feature Configuration	Enhanced the anti-tamper feature, allowing detailed configuration from the KIOSK console. (UI restart required after updating "Active Keyboard Filter" setting)
Enhancements and fixes	
Improved AD User Authentication	Improved the ability to authenticate with Active Directory (AD) user credentials without requiring domain information input on the KIOSK UI
Syslog Result Log Suppression	Enhanced KIOSK to suppress result logs to syslog at the beginning of the scanning process

4.6.5 Hotfix **5 Jan 2024**	**Major release with new features and enhancements**
Enhanced Security	Implemented additional security measures for a more robust system.

Fixed Bugs	
DataLocker Sentry ONE Unlock Issue	Resolved the issue where DataLocker Sentry ONE did not unlock during slow connections to its management server
UI Hang during Copy-To to Insufficient USB Capacity	Fixed the UI hang issue when performing Copy-To to a USB with insufficient capacity
KIOSK User Login Issue after Assigning to Primary AD Group	Fixed the issue where users couldn't log in with KIOSK after being assigned to the primary group in AD
Disk Management issue with OMVA	In the latest release of OMVA (version 2.0.9), we have addressed an issue where OMVA was not functioning optimally with Symantec and Disk Management.

Known Issues and limitations.	
Exit Credential Feature Configuration Reset	There is a known issue where the configuration of the Exit Credential feature may be reset after upgrading to the new version
Unable to save user password at "Enter Vault server to upload files to" option	Will be addressed in the next version
Data are not deleted after wipe Bitlocker	

4.6.4

14 November 2023	Major release with new features and enhancements
Features	
Enhance Security with Anti-tamper Hardening OptionCopy&Go secondary media handling	When enabling the feature from WebMC, default Windows input compounds will be blocked and cannot be exploited to escape KIOSK mode. • ***Notes: The shortcut to turn off KIOSK application is changed to ALT+S***
Automatically unlock and process encrypted USBs with organization password	Organization-level alternative decryption security keys can be provided in management console and used as pre-configured password (max to 2 entries) to unlock encrypted USBs.
Simplified workflow	This new and minimal workflow is introduced to support plug-and-play media scanning with automatic decryption and result display (notes: when it is ON, the full workflows for Employee and Guest are disabled.)
Support files redaction, complete the workflows with Data Leak Prevention	Besides sanitizing infected files and detecting potential leak, KIOSK now is able to redact/substitute sensitive information and watermark files. • ***Notes: The new term for sanitized and redacted is now Remediated***
Support rescan retrieved files from Vault	• Previously KIOSK allows to rescan the retrieved files from a directory, now this feature is available for an integrated Vault.
Support HCI network volume	The new version of OMVA 2.0.8 comes with new KIOSK is compatible with Cluster Shared Volumes in HCI (Hyperconverged infrastructure)
Enhancements and fixes	
For Hardened image	• KIOSK is compatible with Windows Defender • KIOSK starts from service.
Improve the self-scan feature	It's now possible to schedule self-scan on a certain weekday
Enhance the labeling of CD-ROM/DVD/BD-ROM in the scan result	Scan results and log now show the correct media type for CD/DVD and Blueray disc
Several defects have been addressed.	

14 November 2023	**Major release with new features and enhancements**
Known Issues and limitations.	Will be addressed in our next versions.
The power options in Start Menu sometimes disappear after closing KIOSK.	
Sometimes, File Explorer will be triggered behind KIOSK Application.	
KIOSK currently does not have the capability to retry entering the password for Kanguru Defender 3000.	
Set Settings cannot apply Anti-tamper Hardening to all KIOSK instances.	
Cannot trigger Self Scan by clicking SCAN NOW because Simplified workflow already starts a session.	**Workaround solution:** Admin can configure Schedule Self Scan and enable option ***Allow Self Scan to cancel any currently running scan*** to trigger Self Scan

4.6.3

31 August, 2023	Release focused on enhancements and bug fixes
Features	
Copy&Go secondary media handling	Introduced new button to allow choosing to insert secondary media at the start or end of a Copy&Go session A new config option now exists in File Handling of a workflow to only allow inserting secondary media at the end of a session
Exit Kiosk with administrator AD credentials	Extended the configuration to allow exiting the Kiosk with AD administrator credentials
NTFS ADS detection	Added ability to detect and warn that an Alternative data stream was found in a processed file. This information can be seen in session history and in the reports.
Disable Vault ID display	Vault server configuration allows to disable showing any Vault ID information on the UI
Support for additional encrypted devices	• DataLocker Sentry ONE • Viasat Eclypt • Viasat Freedom 600
`My OPSWAT` integration	Initial preparation for basic inventory & license reporting support in a future `My OPSWAT` release (end of September)

4.6.2

	Vulnerability fixes
26 June, 2023	**OMVA Release: 2.0.7.174**
Features	
Security note	The system administrators are required to make Kiosk machine more secured by following actions: 1. Set a BIOS password 2. Enable TPM and Secure Boot in the Windows system 3. Turn on BitLocker encryption
Fixes	
System hardening	• Disable keystrokes to maintain uninterrupted Kiosk operation and reduce interference (CVE-2023-36657) • Prevent unintended executables to be ran (CVE-2023-36658) • Prevent overly long input (CVE-2023-36659)

4.6.1

8 May, 2023	**Security patch release - 4.6.1.9996**
Fixes	
System hardening	Optimized Windows system settings to maintain uninterrupted Kiosk operation and reduce interference

18 April, 2023	Release - 4.6.1.9995
Features	
Preloading passwords for encrypted archives	Allows users to preload list of passwords for encrypted archives before the scanning
Enforce remote login	Administrators can disable remote login for local, AD, or SSO users
Screensaver	Kiosk can play a video after a predefined amount of idle time
SDMS MkIII AES Duoulock support	SDMS MkIII AES Duoulock can be unlocked and processed
Media types	The admin can configure Kiosk to accept encrypted USBs only
Fixes/Enhancements	
SSL certificates	Certificates added in the management console are stored in the Microsoft Certificate Store
Copying to disc	Fixed issue that prevented copying from one disc to another in the same session
Password protected archive\document handling	Corrected issue where certain passwords would not unlock files and Kiosk would re-prompt for input. Improved encrypted archive handling when scanning with Vault.
Time filter in custom log display	Removed the custom time setting in Dashboard, Application Log, Windows Event Log, & Visitor Log
Verbose log compression	The support package is compressed at the highest level
Time format of [time] for Vault server	hh:mm:ss is changed to hh-mm-ss
Scanning duration	Enhancement of performance when utilizing existing process results
Copy&Go	All preparation actions need to be done prior to the scanning and the session ends without additional user actions

4.5.8

11 October, 2022

Features	
Statistic information for Central Management	Added a periodic system health check and provided detail of session statistics for Central Management, for tracking purposes.
Hide Vault access ID on UI	The Vault access ID is now hidden on the UI. Users can temporarily reveal the ID for 3 seconds.
Sessions finish automatically	Enhanced the ability to complete session automatically without waiting for user actions. The session waits on pages where user input is required or results are necessary to view.
Visitor Management configuration	Specific visitor questions can now be enabled/disabled. Management or Contact persons can be configured to not receive session reports attached to visitor check-in emails. If no further questions are configured in a workflow, visitors are navigated to media detection screen immediately.
Fixes/Enhancements	
UI unresponsiveness	Scanning a large amount of data may cause the Kiosk UI to hang indefinitely. Kiosk can detect this hanging, terminate and revive the UI to the state where hanging occurred.
Scanning archive files	Fixed mounting issues with TIB/VMDK/VHD archive files.
File retrieval	Encrypted devices are now supported in file retrieval.

4.5.7

30 August, 2022

Features	
SMTP configuration	Sender input is mandatory for email settings (e.g., `From` field). The configured user for SMTP access needs to have permission to send as a configured email sender.
Email improvements	Session reports can be emailed to multiple recipients. Pre-defined variables can be inserted into the body of the email to show some select data from a session.
Password change required on first login	Newly created users are required to change their password on their first login to the Management Console
Active Directory configuration in Visitor Management	Administrators can configure both AD users and groups as Contacts for Guests
Auto-selection of workflow	Administrators can either let employees select a workflow or automatically move forward with the first matched workflow an employee can use
Fixes/Enhancements	
Custom command script	The syntax now works the same as on a DOS terminal
Scanning Pause/Resume	Pausing a scan requires additional confirmation
User authentication	Corrected the display for custom authentication on changes of `Display disclaimer screen`. Authentication performance was also improved.
Performance enhancement for AD queries	Sped up the performance when connecting/querying to AD server

4.5.6

24 May, 2022	**This release focused on new features** **OMVA Release: 2.0.6.167**
Features	
Non-authenticated workflows	Kiosk administrator can create multiple workflows for guests to select on demand.
Email template	Emails can now be customized with logos, text colors, and font sizes for workflows.
Fixes/Enhancements	
Visitor configuration	Corrected issue where loading a large amount Active Directory users would take a long time for Visitor Contact configuration.
Retrieval page	Direct navigation to the Vault retrieval page occurs when only one retrieval option is enabled.
syslog data	Expanded session data in json format for syslog messages.

4.5.5

28 March, 2022	This release focused on new features and bug fixes/enhancements
Features	
Upgrade in-place	Upgrade of Kiosk no longer requires uninstallation of the previous version. This allows for history logs to be maintained in between version upgrades. The original upgrade method still operates the same.
Copy empty folder	Empty folders from scanning sources are copied to local/network destination after scanning
Fixes/Enhancements	
Skipped file reporting	Files not able to send to Core for scanning are now considered as Skipped files. Customer can configure to show/hide skipped files in their workflow printing options.
Trust self-signed certificates	Administrators can add self-signed certificates to trust directly in the Management console
File integrity monitoring	Corrected issue where Kiosk would be disabled by file monitoring when the feature was disabled
Stale processing results	Any change to a Core workflow will require a file to be analyzed to ensure results reflect the latest policy configured
Self Scan	Inaccessible system files are skipped during a Self Scan to avoid indefinite retries to scan

4.5.4

20 December, 2021	This release focused on new features and bug fixes/enhancements
Features	
Country of Origin	The Country of Origin feature helps administrators add more restrictions on the scanning result by specifying which countries a publisher resides in as forbidden. Files published from forbidden countries are considered blocked.
Configurable printing per session type	Allows printing to be enabled/disabled separately for each action Scan/Retrieve/Wipe
Fixes/Enhancements	
Scan result for encrypted archives in Copy&Go mode	Fixed issue that showed both Allowed and Blocked status on the same file
Slow processing time for a large dataset	Improved performance in processing large datasets

4.5.3

2 November, 2021	This release focused on bug fixes and enhancements
Features \ Enhancement	
Skip Print button displayed for all session flows	Added `Skip Print` button when `Print` button is displayed
Editing workflow with many AD members assigned	Optimized performance with workflow loading to allow workflows with a large amount of members assigned to be edited
Support for updated encrypted device software versions and retrieving files	Added support for updated versions of some encrypted device software and corrected instances where retrieved files were download to incorrect volumes leading to failures
Fixed	
Reports being stripped from emails	Modified content type in email reports to prevent specific email policies from blocking attachments
Retrieve files to disc	Fixed issue that prevented files to be retrieved and copied to a disc
Session history failing to load in certain cases	Corrected background sorting of session history that caused for sessions to not be displayed in the Management Console

4.5.2

16 September, 2021	This release focused on support for nested group login, archive file selection, session report sent for Visitor Management and bug fixes
Features	
Nested group support for login	Active Directory with nested group supported for login in Kiosk UI
Archive file selection	Support multiple selection of password protected archives to scan
Visitor Management	Session report is sent to Manager, Contact, and Guest
Fixed	
Phone detection	Fixed issue with phones not being detected
Central Mgmt config push affecting SSL settings	Prevented export/upgrade of certificate settings
Mismatch file result display in Session History	Corrected the display of mismatch result in session report
Configuration import	Fixed issue where certain settings were not maintained on a configuration import
Email session report	Correct cases where email was sent without a sender
Browse window	Refined UI browsing page

4.5.1

27 July, 2021	**This release focused on blank disc detection, CM set settings, and OMVA logging enhancements.** **OMVA Release: 2.0.5.137**
Features	
OMVA Logging	Accessible logging in json format generated when plugging & validating media into a machine with OMVA installed
Printer Status	New icon on UI to show current printer status
Session history username filtering	Able to filter Session History in the Management Console by username
Fixed	
Copy file to disc	Corrected detection of a blank disc as destination media to copy files to
"Set Settings" applied to all instances	Fixed issues causing Central Management failing to "set settings" to other Kiosks. Extending timeout settings in CM may be necessary
Workflow selection	Adjusted workflow selection for better usability
Session log saved to network share	Fixed case where the session log was not properly saved to a network shared folder
Management Console login	Modified Management Console behavior to only allow a user to be logged in from a single browser
USB whitelisting	Serial number to include vendor name and model

4.5.0

Note
Management Console support for Internet Explorer has been dropped

15 June, 2021	**This release focused on User workflow selection, adding Spanish translation and other bug fixes.** **OMVA Release: 2.0.4.130**
Features	
User workflow selection	A user may now be assigned to multiple workflows either by direct assignment or group assignment. When logging in to a Kiosk session, users will be presented with their assigned workflows to choose.
Spanish translation	Added support for default Spanish translation
Mail configuration test	When configuring SMTP settings, administrators may now test their settings within the mgmt console
Fixed	
OMVA failing to validate media after a reboot	Fixed issue where media validation no longer worked after reboot in certain domain environments
Saving session logs to network shares	Corrected issue that prevented session logs from saving to networks shares due to permission issues
Allow sessions to end automatically	Modified session flow to adhere to UI timeout settings when the session is done
Active Directory load when editing workflows	Further enhancements to speed up the AD user & group loading when a workflow is edited
Local user password restrictions	Removed extra restrictions on passwords for local users and increased the minimum length to 12 characters

4.4.12

6 May, 2021	**This release focused on file limit configuration with Vault processing, correcting VMDK with Linux file systems and other bug fixes.**
Features	
Vault processing - File size limit	File sizes can now be limited to dictate what is uploaded to Vault for processing
Vault processing - File count limit	The amount of files can now be limited when processing files with Vault
Copy-to media device info in logging	When files are copied to secondary media, the device information of this media is now included in the session logging
Fixed	
Processing VMDKs with Linux file systems	Fixed issue with failing to process contents in a VMDK with Linux file systems
Processing discs with CDFS file system	Corrected detection error the prevented processing discs with CDFS file system
Hebrew language display	Restored Hebrew display when browsing for files and selecting copy-to directories
Management Console login case insensitivity	Modified mgmt console login to not require case sensitive username input
Retrieve available files from Vault	Enhanced Vault file retrieval to not display files that are not approved by a supervisor
Email reports	Fixed issue where email reports were sent to incorrect recipients with similar names

4.4.11

6 April, 2021	This release focused on syslog support for TLS over TCP and other features & bug fixes.
Features	
syslog support for TLS over TCP	syslog can now be configured to send messages using TLS
USB Copying Whitelist and Retrieving files	The whitelist to allow USBs to copy files to now also applies to retrieving files from Vault or directory
Battery percentage display	If MetaDefender Kiosk is deployed on a battery powered system (i.e. tablet\laptop) a battery power indicator will be displayed on the user interface in the bottom right corner
Disable hash calculation for non-processing session	For workflows where no processing is configured, the hash calculation of files can be disabled to allow for a faster session completion time
Fallback to OS logged in user when copying files to a directory	File handling to copy files to a directory now has the ability to enable copying files as the OS logged-in user if copying using the Kiosk user session credentials fails
Fixed	
Media detection	Corrected further issues with media detection: • encrypted devices being detected as CDROM • media insertion not being detected after a wipe event
Wipe functionality	Corrected further issues with wiping media: • encrypted device handling attempting to wipe the un-encrypted disc partition • wiping hanging on completion • device detection not operating after a wipe event
AD User & Group load in workflows	Improved the mechanism to load the list of AD users & groups to better handle large amounts
Retrieve files from Vault	Fixed a case where authenticating a user to Vault for retrieving files was failing
Send email only when blocked files are found	Restored the expected behavior of the workflow email setting to only send a session report email when a blocked file is found in a session

Notes
Added a survey in the Management Console to collect feedback

4.4.10

4 February, 2021	This release focused on Digital session log signing and bug fixes.
Features	
Digital signing of session logs	Session logs can now be digitally signed with a configured certificate to ensure logs have not been tampered with
Supported browsers for the Management Console	The Management Console supports Chrome, Firefox, and Edge browsers. Internet Explorer and others are not officially supported
Fixed	
Media detection	Enhanced media detection logic to reduce inconsistent issues with misdetection or improper identification of media
Copy & Go and copying to user media destination	Copying files to a secondary media is now supported when Copy & Go processing is enabled
SSO Management console login from a remote system	Fixed a redirection issue that caused users to not be navigated into the mgmt console after a successful SSO login
Guest workflow file retrieval	Corrected issue where Guests were not allowed to retrieve files if certain user authentication settings were set

4.4.9

12 January, 2021	**This release focused on user experience enhancements & bug fixes.** **OMVA Release: 2.0.3.96**
Features	
Estimated time remaining display during processing	Processing progress indicator now shows current time elapsed and estimated time remaining
Retrieve files from Vault as a Guest	Guests can retrieve files from Vault using a Guest ID
Multiple copy-to directory support	Multiple copy-to directories can be configured in file handling. Users can select which directory to copy to when the user copy selection is enabled.
Browse file selection totals	Options for browsing files can now be set to display the number of files selected and the total size of the selection
Fixed	
File\Session history export	Corrected issues with the export taking too long to generate and timing out connections
Retrieve files from Vault as an AD user	Fixed problems with retrieving files from Vault for certain AD user configurations
OMVA multiple media manifest support	Adjusted OMVA support for handling multiple media manifests on a device

4.4.8

8 December, 2020	**This release focused on Single Sign On user login to the Management Console & bug fixes.** **OMVA Release: 2.0.2.94**
Features	
SSO authentication for the Management Console	Management Console login settings have been expanded to allow connecting an Identity Provider via SAML 2.0
Fixed	
Custom workflow editor load time for a large AD	Reduced the amount of time it takes to load the AD user\group list when editing a custom workflow
Periodic Core test	Fixed eicar test string generation that was affecting the detection rate
OMVA non-ascii path support	Corrected OMVA support for handling file paths with non-ascii characters which would result in blocking media

4.4.7

10 November, 2020	**This release focused on Active Directory user login to the Management Console & bug fixes.**
Features	
Allow AD users to log in to the Management Console	Management Console login settings have been expanded to allow connecting Active Directories to allow users/groups to login
Fixed	
Session log directory in Central Management	Fixed validation error that prevented setting the session log directory from Central Mgmt
Automatic export	Corrected non-ascii errors with automatic export and added Scanning System information to the csv

4.4.6

13 October, 2020	This release is focused on bug fixes.
Features	
Configurable result for un-processed large files	Management Console administrators can now specify if a file should be allowed or blocked if it exceeds the file size limit for sending a file to MetaDefender Core.
Fixed	
Floppy drives consistently spinning	Fixed issue where certain floppy drive models would spin up consistently while Kiosk was running
Workflow login selection	Corrected instances where mapping a logged in user to a workflow did not follow the configured order
File size process limit	Adjusted file size calculation to prevent errors with setting file size limit for processing files
Core URL validation	Repaired error detection that would prevent connecting a Core via hostname

4.4.5

15 September, 2020	This release is focused on simplifying HTTPS configuration within the Management Console and bug fixes.
Features	
Configure HTTPS from the Management Console	Management Console administrators can now configure listening port and HTTPS settings from within the Management Console
Configurable boot sector processing	Boot sector files can now be disabled from appearing in browsing for files to process and not included when processing all contents of media
Fixed	
UNC file path support for retrieving files	Fixed issues where retrieving files from a UNC path would fail
User question display in session export	Session export data now displays the user question and answer to the question in order
Copying files to disc	Corrected instances where long file paths were failing to be copied to discs

4.4.4

18 August, 2020	This release is focused on Configuring the order workflow profiles are used to map a user to, periodic testing of Core servers and bug fixes.
Features	
Configure order of workflow profiles	Custom workflow profiles can now be manually adjusted to indicate the order in which users are identified to belong to
Periodic Core test	Kiosk can be configured to periodically send an EICAR file to ensure Core's detection is functioning
Fixed	
Email session report	Corrected issues with connecting to SMTP, sending emails to the logged in user and guest users
Authentication failure when Remote AD SSL is enabled	Fixed active directory communication to not attempt the default LDAP port when SSL is enabled
Automatic export of session\file history logs	Export log path configuration was failing to save and the file history export was lacking information, this has all been corrected
UNC path support for session logs	Fixed issue that prevented configuring a UNC path for specifying where session logs were written out to

4.4.3

16 July, 2020	**This release is focused on Copy & Go processing, ability to retrieve files from a directory and configuring the install password for OMVA** **OMVA Release: 2.0.1.92**
Features	
Copy & Go processing	New Core processing option that allows copying files to the system and removing media before file processing begins
Retrieving files from a directory	Ability to retrieve files from a local or network share and run the files through Core before copying to the inserted media
OMVA configurable uninstall password	The uninstall password can now be modified for deployments to endpoints
Whitelist for secondary media	Whitelist can now be specified for copy-to media
Fixed	
Language import	Corrected issue where languages were not allowed to be edited after importing configuration of a previous release
IP support for SMTP host configuration	Fixed issue where connecting to an SMTP host configured by IP would fail
Hostname for syslog	syslog server can now be configured by either IP address or hostname
Users and Groups synced in workflows on Central Mgmt	The users and groups re-assigned to other workflows on Central Mgmt now updates as expected and syncs to the Kiosk instance's settings

4.4.2

5 June, 2020	This release is focused on fixing issues with remote Active Directory support
Fixed	
Remote Active Directory connection and assigning users and groups to a workflow	Fixed domain identification issues that would block adding an AD server. Corrected problems where displaying the users and groups of a server would fail.
Usability of selecting groups to assign to a workflow	Added the ability to search the groups list to find specific entries

4.4.1

15 May, 2020	This release is focused on adding support for multiple AD servers and log retention
Features	
Multiple Active Directory support	Multiple active directories can now be added to expand the coverage of users allowed to use Kiosk
Automated log retention	Application logs and session history can now be set to automatically clean up records older than a configured time span
Fixed	
Issues with user authentication and foreign language passwords	Fixed issues where users could not authenticate when their passwords contained foreign characters
Username & user response variables for the copy-to directory	Copy-to directory validation has been fixed to allow the user name and user response variables
UI exit password setting	Fixed an issue where the exit password was changed when user authentication settings were modified
Offline systems could not locally access the mgmt console	Updated internal management console settings to allow offline systems to access the console locally
Selecting groups to add to a workflow	Only allowed groups are displayed to assign to a workflow
Central Management v7 configuration sync	Corrected many issues where settings disappeared from the Central Management view or were applied incorrectly

4.4.0

16 April, 2020	This release is focused on adding NGINX to serve the Management Console, allowing Guests to receive summary reports via email, and providing passwords with encrypted archives when processing with Vault
Features	
NGINX serving the Management Console	IIS Express has been replaced with NGINX to power the Management Console
Guests can email session reports	Guests are now prompted to enter an email to session reports, when emailing reports is enabled
Send passwords with encrypted archives when processing with Vault	When an encrypted archive is identified, a password can be input to submit the file to Vault for processing
Support for Kanguru Defender Elite 200	Added support for processing Kanguru Defender Elite 200 USB
Fixed	
Setting custom export date range	Fixed the date selection to allow setting a custom date range to export session or file history
OMVA install via automated deployments	Modified OMVA installation to work successfully in remote deployments
Hash verification copy failure with extension-less files	Corrected an issue with hash verification failing on files without an extension
Copying files to a network share as Guest	Copying to a network share now utilizes the credentials of the user logged in to the system to copy files in the Guest workflow

4.3.11

13 March, 2020	**This release is focused on the flexibility with the Vault copy-to directory structure, file deletion confirmation for users and other bug fixes**
Features	
Specify Vault copy-to directory structure	Administrators can now indicate the directory structure of how files are uploaded to Vault when configuring a Vault server
Allow users to confirm to delete all blocked files	When blocked file handling is set to delete files, an Administrator can now allow users to confirm whether the blocked files should be deleted or not
Fixed	
Copy-to media blocked with OMVA	Copying all allowed files to a secondary media that was wiped would still cause OMVA to block the media. This workflow has been modified to allow OMVA to unblock the media as expected.
Configure syslog settings from Central Management	A managed instance's syslog settings can now be configured via Central Management v7
Single password use to unlock multiple encrypted archives	Fixed an issue where the checkbox to supply a single password to multiple encrypted archives was not being respected
AD groups are only allowed to be added to a workflow profile	Only AD group objects will be allowed to be added to a workflow profile to reduce confusion with authentication issues
Sanitized file handling with the custom command line script	Corrected an issue where sanitized files were not handled in a configured script

4.3.10

11 February, 2020	This release is focused on bug fixes
Fixed	
Detection of multiple Linux partitions	A device with multiple non-Windows partitions can now be browsed through and processed
Vault entry changes applied automatically to selections	Any changes made to an entry in the Vault server list are automatically applied across all configured selections of that specific server
Windows XP+ support for OPSWAT Media Validation Agent	OMVA now supports Windows XP and above
Report files quarantined by Core	Files quarantined by Core are now reported on the session summary without having to configure to have the files removed
Language menu button on the on-screen keyboard	Corrected button behavior where the keyboard language button would remain open despite clicking away from it

4.3.9

14 January, 2020	This release is focused on Vault upload to user configuration and bug fixes
Features	
Specify Vault user to upload files to	New configuration option allows for specifying a Vault user to upload files to in addition to the previous settings of uploading to the user logged into Kiosk or a guest account
Fixed	
Retrieve files from Vault	Fixed issues with downloading files from Vault among multiple users
File sizes displayed in browse	Corrected the file size display when browsing for files

4.3.8

10 December, 2019	This release is focused on Imaging Media and bug fixes
Features	
Image Media	New process flow allows for an image to be created of the inserted media and uploaded to a specified location (e.g. Vault or directory)
Fixed	
IIS Express 10 support	Kiosk REST service now runs uninterrupted if the underlying IIS Express is upgraded to version 10
Updated German language strings	German language strings are now up-to-date
Blocked sound playback	Fixed an issue where the sound byte to alert for blocked files would not play at times

4.3.7

12 November, 2019	This release is focused on Visitor Management and bug fixes
Features	
Visitor Management	Visitor management allows the ability for guest users to check-in to an organization via the Kiosk. During the check-in process the guest user accepts any agreements specified by the organization, a badge for the visitor can be printed and contact\admin personnel are automatically notified when a guest has arrived.
Fixed	
Korean keyboard character composition	Onscreen Korean keyboard has been fixed to correctly combine Hangul characters
Device whitelisting applies to destination media	Device whitelisting is now applied to destination media, in addition to the source media used for processing
Copy files to IronKey USB	Corrected behavior where files were copied to the wrong volume for specific IronKey USBs

4.3.6

8 October, 2019	This release is focused on Management Console enhancements when Kiosk is managed and bug fixes
Features	
Management Console settings locked when instance is managed	The Management Console now has the ability to show details when it is managed. If managed, changes to settings are disabled. Currently supported for Central Management v5, v7 in the future.
Configure the length of time a Vault guest account is valid	Administrators can now specify how long a created Vault guest account can remain valid
Fixed	
Processing system files	Enhancements made in attempting to process system files that may be potentially locked
File integrity monitor event	Upgraded the visibility of a file integrity monitor event to be included in the syslog application events

4.3.5

10 September, 2019	This release is primarily focused on bug fixes
Features	
Delete after retrieving files	Retrieving files from Vault can now be configured to delete the files from the server after download
Fixed	
Copy to disc folder structure	Copying to disc no longer creates a Session ID directory when the no subfolders option is enabled
Settings display on Central Mgmt v7	Fixed issues with some fields being improperly displayed in Central Mgmt
LDAP groups workflow profile assignment	Corrected an error where a users logging in to Kiosk were not identified under a user group assigned to a workflow profile

4.3.4

13 August, 2019	**Release focused on adding Kiosk high availability, Layer 7 load balancer support and bug fixes**
Features	
Ability for Kiosk to use multiple backup servers during a session	Multiple backup servers can now be configured in the global configuration. Within a workflow profile, it can be designated for Kiosk to attempt processing a file among any available MetaDefender server during a session.
Support for Layer 7 Load Balancer with MetaDefender	A Load Balancer can now be selected as the primary server for processing files
Regular expression support for media whitelisting	Media whitelisting can accept regular expression rules for more flexibility in configuring allowed devices
Option to disable SSL verification	Certain offline environments cannot successfully verify SSL certificates due to the network structure. Kiosks in these special instances can be configured to workaround these limitations.
Fixed	
Issue with MetaDefender verification only working through TLS 1.0	MetaDefender connection testing in the Management Console has been fixed to utilize the latest security protocols when available (e.g. TLS 1.2)
Virtual keyboard input	Corrected ability to insert/delete characters within an input text box rather than only at the ends of the input
Unlock for IronKey D300 Managed devices	Updated ability to handle different versions of IronKey D300 Managed devices
Interface timeout not triggered while waiting for media to be inserted	Fixed the interface timeout to apply while waiting for media to be inserted
Updated Custom Authentication Module template	Custom Authentication Module template & tester have been updated to 64bit

4.3.3

9 July, 2019	Release focused on adding Kiosk self scan and bug fixes
Features	
Kiosk self scan	Allows the user to periodically or on demand utilize the MetaDefender Kiosk to scan its file system for possible infection
File handling option to copy allowed files to the original media	New copy-to route will wipe the original media and copy all allowed files back to it
Select to not submit special archive files, mounted by Kiosk, to Core	Only applicable to Acronis backups, virtual hard disks and/or VMware virtual machines. Can now choose to withhold these files from Core if its contents have already been processed.
Prompt users for the password to password protected documents	When password protected documents are encountered (Word, PDF, Excel), they will now be prompted for passwords for processing their contents.
Generate a log message and warn the user when disk capacity reaches 80%	To help our customers ensure that the Kiosk has sufficient space to operate, it will generate a log message when disk capacity has reached 80% or higher.
Updated Custom Authentication Module sample code to include 64-bit	To better facilitate CAM users in upgrading from V3 to V4, the CAM sample code has been cleaned up and generated in 64-bit
Fixed	
Kiosk failing to quarantine read-only files	Read-only files are now supported for quarantining
Fixed VHD mounting that was broken by recent Windows 10 updates	Windows 10 updates changed the case of the name of the drive being attached. Fixed parsing to handle variable case string.

4.3.2

11 June, 2019	**Release focused on adding the OPSWAT Media Validation Agent, support for Avira-Iron-Drive, and bug fixes**
Features	
Added the OPSWAT Media Validation Agent	The OPSWAT Media Validation Agent can be downloaded from the Management Console Resources section. This agent can be used to ensure media is processed by a Kiosk before it can be mounted on an endpoint.
Support for Avira-Iron-Drive	Files can now be processed within or copied to an Avira-Iron-Drive.
Fixed	
Changes made to the disclaimer not being updated	Corrected issue where making changes to the disclaimer content were not reflected in the UI
Sentry 3 FIPS unlock enhancement	Enhanced the unlock mechanism for Sentry 3 FIPS to correctly unlock versions with different behavior
Disabling boot hardening may hang	Fixed disabling the boot hardening to not cause a hang and fail to update the correct status on the mgmt console for some cases
Central Mgmt synchronization error	Added more protection to avoid issues with Central Mgmt configuration pushes failing

4.3.1

15 May, 2019	**Release focused on fixing Management Console logins for all timezones**
Fixed	
Login to the Management Console	Corrected issue where login to the Management Console would fail on certain systems

4.3.0

14 May, 2019	Feature release focused on adding user support for the Management Console, support for Non-Windows file systems and minor bug fixes
Features	
User login for the Management Console	User login is now required to access the Management Console *In keeping parity with MetaDefender, custom integrations to the REST API with passwords will no longer function. You must set up an API key per user. When installing, you must use the creation wizard to create your first admin user. Admin credentials are no longer created automatically.
Support for Non-Windows file systems	Processing media content in Ext2/3/4, HFS Plus, HFSX, and APFS file systems is supported
Discs allowed to retrieve files from Vault	Retrieving files from Vault can now be downloaded to a disc
Fixed	
Enabling boot hardening	Security enhancements made to allow boot hardening for all systems
File handling count display	A count of the current file progress is now displayed when files are copied/moved to a destination
Product activation through a proxy	Online activation can now complete successfully via a proxy server

4.2.15

18 April, 2019	Feature release focused on internal enhancements for Central Management
Fixed	
Improvements for Central Management	Under the hood enhancements to allow the management of Kiosk instances to be smoother

4.2.14

9 April, 2019	Feature release focused on adding support for VMware virtual machines and bug fixes
Features	
Mount and scan VMware virtual machines	Added support for processing within VMDK files
French translation	French language can now be selected as one of the default languages
Upload files to Vault	Vault upload in the file handling of a workflow can now be specified to upload files singularly (with the addition of file scan results) or all packaged within a zip
Password prompt for nested encrypted archives	Password prompt will be displayed for encrypted archives found within encrypted archives
Integral Courier encrypted USB support	Integral Courier can be unlocked and processed
Kingston IronKey D300 Managed support	Kingston IronKey D300M can be unlocked and processed
Fixed	
CEF Extension field format	The Extension field in the CEF messages have been fixed to conform to correct CEF standard
German language	German language strings have been expanded upon

4.2.13

12 March, 2019	Feature release focused on processing contents within virtual hard disks and minor fixes
Features	
Mount and scan VHD & VHDX	Added support for processing within virtual hard disk files
Fixed	
Copying sanitized files would fail for certain users logged into a Kiosk session	All users are now able to copy sanitized files to the desired destination
LDAPS connection	Connecting to a directory server via LDAPS has been improved

4.2.12

12 February, 2019	Feature release focused on system boot hardening, folder navigation on Vault and allowing copying original with sanitized files
Features	
System boot hardening	With boot hardening enabled the taskbar on the desktop will be not be loaded, thereby disallowing any PC functionality to a user until the Kiosk starts.
Folder navigation when retrieving files from Vault	When browsing for files to download from Vault, folders can be accessed and downloaded to the desired media.
Copy the original file along with the sanitized version	New configuration option added for Copy-To actions that will allow an administrator to specify copying the original file along with the sanitized version.
Fixed	
Emails not being sent to the user logged into the Kiosk session	Kiosk can now identify the email address of the logged in user from a remote AD server.
LDAPS authentication failure	Users can authenticate using LDAPS functionality with improved routing.
Handling sanitized file naming convention	Now an incremental number is only appended to the file name during copy to avoid file collisions.

4.2.11

8 January, 2019	Feature release focused on allowing multiple devices to be wiped in one session and stability enhancements
Features	
Wipe multiple devices in one session	Multiple devices can be inserted at the wipe option selection screen for the wipe to be performed on all devices
Warning message is displayed if a file is not processed by MetaDefender	A warning message is displayed before the session results screen if any file is not processed by MetaDefender
Fixed	
Backup server selection when the primary MetaDefender instance is unable to process files	The decision to use a backup MetaDefender server has been enhanced to ensure a primary MetaDefender instance is not used when it is unable to process files. Any MetaDefender instance that reports problematic issues will be noted on the Mgmt Console and the issue logged in the application log.
syslog message format for TCP	Some syslog messages were missing line breaks which caused parsing issues for some syslog management systems when receiving data over TCP
Enhanced retry mechanism for files that are unable to be opened	Certain files have some permissions that block Kiosk from accessing them to upload the file to MetaDefender for processing. The ability to retry on these files and allow for successful upload has been enhanced. This does not apply to locked system files.
Processing an iPhone with iTunes installed	After installing iTunes and then selecting files from an iPhone to process, the selected files would not be processed. Functionality has been restored.

4.2.10

11 December, 2018	Feature release focused on expanding support for processing non-Windows file systems and simplifying blocked files reported in session reports.
Features	
Blocked results directly reported from MetaDefender	Beforehand, Kiosk would group specific blocked reasons under special categories (e.g. Encrypted Archive & Password Protected Document → Password Protected). This would result in confusion when reading session summary reports and verifying specific file counts against the MetaDefender processing history. Blocked results are no longer grouped under special categories, they are grouped according to the result returned from MetaDefender.
Fixed	
Blocked results directly reported from MetaDefender	Beforehand, Kiosk would group specific blocked reasons under special categories (e.g. Encrypted Archive & Password Protected Document → Password Protected). This would result in confusion when reading session summary reports and verifying specific file counts against the MetaDefender processing history. Blocked results are no longer grouped under special categories, they are grouped according to the result returned from MetaDefender.
Custom command line script not running	There was an issue with the component that runs custom command line script - failing to start and complete the configured actions. This has been fixed.
syslog CEF format	syslog messages sent in CEF were not formatted according to specifications which caused parsing issues in SIEM servers. The main body of the message is now sent in the Extension section and the log type is sent in the Name section. The severity level has also been corrected to meet the CEF specification.
Processing mobile phones with Vault	Fixed upload failures when attempting to process a mobile phone with MetaDefender Vault.

4.2.9

13 November, 2018	Feature release focused on email, user selection of copy-to directories and stability improvements
Features	
Configuration to only send an email report when a blocked file is detected	The email report can now be specified to be sent only when a blocked file in a session is found, rather than sending an email after every session.
Allow users to select the folder structure of copied files	Users can now be allowed to select whether to create a high level directory for files to be copied to or maintain the same folder structure as the original processed media.
Fixed	
Enhanced progress display for processing TIB files	Modified TIB processing experience to follow the archive processing flow. Files within a TIB are displayed during progress, the TIB itself is counted as one file & an indicator in the right hand corner will notify the user that an archive is being processed.
UI will remain responsive when processing large datasets	Processing large datasets would cause the UI to stop showing updated progress from being displayed near the completion of a session, giving the impression that the UI was hanging. Progress reporting has been modified to allow the UI to be responsive under large datasets for the duration of a session.
Finding users in groups assigned to workflow profiles	With a group assigned to a workflow profile, when a user would log in to Kiosk, there were instances where a user that is a member of the group was not correctly associated not provided the expected workflow profile. This has been fixed.
SD card detection failure	Certain SD card readers present information of the media differently, which caused the Kiosk to not detect it. Media detection has been updated to handle this case.
Hash verification when copying to a network share	Hash verification has been fixed to work with verifying files were copied correctly to a network share.
Translated strings not updating on the UI	A few translatable strings were not being updated for display in the UI. These have been identified and fixed. The default Japanese language strings have also been updated.

4.2.8

22 October, 2018	Maintenance release focused on Central Management compatibility
Fixed	
Tab selection in Central Management	Scrolling through configuration sections has been removed in the latest Central Management 5.2.3. Overflow sections are now selectable from a dropdown menu.
Vault server configuration import from Central Management	Due to the change in how Vault server settings are saved in Kiosk, only partial Vault settings were being imported over. This has been rectified.

4.2.7

11 October, 2018	Feature release focused on media manifest validation and improvements for stabilized processing
Features	
Media Manifest Validation	Previously, Kiosk only saved signed manifests to the media that had been processed. Kiosk can now be configured to validate and utilize results from a manifest found on the media to process.
Logo and Intro Text on Receipt Printout	A logo and introduction text can be configured to print onto a session receipt.
Fixed	
Process failure logging is now more transparent	If Kiosk fails to send a file to the MetaDefender server, the reason will be displayed in the UI and session result log & printout. Any network connection errors contributing to failures or MetaDefender failures reported to Kiosk will be logged in the Application Log in the Kiosk Management Console. Messages will contain HTTP codes, description and network error messages to enable admins to take proactive action.
Updated bundled 7z component to version 18.05	Due to vulnerability issues with older versions, the bundled 7z binaries were updated to the latest version.
Retry logic improved when retrieving results from MetaDefender	In previous versions, if an error from MetaDefender prevented Kiosk from obtaining results, it would fail quickly and show that the file failed to process. Kiosk will now try harder to receive correct results from MetaDefender if a file has been successfully sent for processing.
Removed curl error logging when a session is canceled	Canceling a session can result in canceling active connections between the MetaDefender server & Kiosk. This would result in an unnecessary large amount of curl error logs that are now removed under this specific condition.

4.2.6

Release Date: 11 September, 2018

Features

- Added support for processing iPhones
- Ability for users to select which file handling actions to take
- Added support for DataLocker Sentry 3 FIPS
- syslog messages can output in CEF format

Fixed

- Files sizes are displayed when browsing files to process

- Added more display data to the session log & printout
    - File attributes, partition information, symbolic links found
- Fixed issues with session log generation
- Added ability to navigate through user questions
- Enhanced loading process upon startup
- Core quarantine results are now reflected in the Kiosk results

4.2.5

Release Date: 14 August, 2018

Features

- Offload processing to a Vault server connected to MetaDefender
- Ability to Pause and Resume file processing
- Enable/disable the Default workflow to restrict user login

Fixed

- Adjustments to automatic printing at the end of a session
- Fixed copying to a network share when a Remote Active Directory is configured
- Support copying between encrypted media of the same type
- Configurable footer printing for the session receipt

4.2.4

Release Date: 10 July, 2018

Features

- Added support for processing android phones
- Added support for processing within Acronis TIB files
- Ability to view and assign user groups to a workflow profile

Fixed

- Syslog messages can be configured to send over TCP
- Defined more event codes for syslog messages
- Enhanced ability to handle large nested directories
- WebMC session history will display if a result is from a hash lookup

4.2.3

Release Date: 12 June, 2018

Features

- Added LDAPS support for Remote AD servers
- Ability to set the apikey during installation

- Display file names of files in a large archive during processing

Fixed

- Extended syslog support to multiple servers
- Fixed login issue with users assigned to a workflow profile
- Corrected browsing for files in nested directories with similar names
- Improved the speed for copying files

4.2.2

Release Date: 21 May 2018

Features

- Functionality to alert if a popup is open on the underlying system
- Events can be configured to broadcast to a syslog server

Fixed

- File browse window can handle large number of files in a directory
- Fixed issue with querying users from a remote AD
- Ensuring a session ID is always generated for reports
- Updated Central Mgmt integration to further validate configuration settings
- Added ability to view the MetaDefender Privacy Policy from the Management Console

4.2.1

Release Date: 16 April, 2018

Features

- Ability to download files from Vault
- Configure session and file history CSV export run automatically
- Added support for Kingston DataTraveler 400 G2
- Email session reports to the logged in Kiosk session user

Fixed

- Modified font display with foreign languages
- Fixed issue with Central Mgmt settings import
- Enhanced various logging with more specific information

4.2.0

Release Date: 20 February, 2018

Features

- Rebranded Kiosk

- Ability to be managed by Central Management
- Added support for Kanguru Defender Elite 300
- Session and file history can be exported to CSV
- Kiosk can be configured to allow file handling to run automatically

Fixed

- Fixed issue with reporting wipe progress for large devices
- Improved media handling
- Added new configuration
  - allow users to skip entering passwords for McAfee drives
  - disable warning of network errors
- Enhanced license activation

4.1.1

Release Date: 30 November, 2017

Features

- None

Fixed

- Fixed issue in uploading files to SFT accounts when authentication is done by a custom authentication module
- Sanitized files are copied to temporary storage instead of original media
- Fixed issue in creating a new language
- Fixed issue where session finish time was reported incorrectly in Kiosk logs

4.1.0

Release Date: 26 October, 2017

Features

- Support for additional models of encrypted USB drives
  - Ironkey S1000
  - Ironkey D300
  - Kingston DataTraveler Vault Privacy 3.0
  - Kingston DataTraveler 2000
  - Kingston DataTraveler 4000
- Answers to user questions can be used in the path specified for post scan file handling
- When copying blocked files, administrators have the option of only copying files that have been sanitized

Fixed

- The Metadefender Kiosk Management Console now has a default password ('admin') after installation

- Cancelling a scan will cancel scans in progress on the Metadefender Core server
- Kiosk will retry scans that initially fail on the Metadefender Core server
- Improvements in the Japanese language keyboard
- Language keyboards can be disabled from the Kiosk UI

4.0.2

Release Date: 18 September, 2017

Features

- Metadefender Kiosk can be configured to check for existing scan results before sending a file to Metadefender Core

Fixed

- The Browse and Scan All options will not be displayed in the Kiosk UI if they are disabled
- Media wipes are now logged as sessions
- Media manifests are uploaded with files that are copied to a Metadefender SFT server
- Vulnerability details are displayed if Metadefender Core has the Metadefender Vulnerability engine enabled

4.0.1

Release Date: 28 July, 2017

Features

- Signed scan manifests can be written to processed media (requires Metadefender Core 4.8.0 or later)

Fixed

- Improvements in uploading files to a Metadefender SFT server
- Session scan logs are included in a configuration export

4.0.0

Release Date: 5 July, 2017

Features

- New Kiosk user interface
- Optional 'Disclaimer' Screen in Kiosk workflow
- Support for user selected language

Fixed

- Re-implementation of drive wipe functionality
- Move to new licensing mechanism
- 32-bit operating systems are no longer supported
- Minimum required version of Metadefender Core is 4.7.2

- Configuration can not be imported from versions prior to 4.0.0

3.4.6

Release Date: 25 July, 2017

Features

- None

Fixed

- Fixed issue where Kiosk sometimes didn't launch after system restart
- Minor bug fixes

3.4.5

Release Date: 25 April, 2017

Features

- Alert dialog shown to the user when a non-memory USB device is inserted
- Devices can be limited to those whitelisted by device ID

Fixed

- The only Metadefender Kiosk workflows included by default will be the 'Default' and 'Guest' workflows
- Mechanism to retrieve device serial IDs has been improved

3.4.4

Release Date: 14 March, 2017

Features

- None

Fixed

- Metadefender Kiosk will now attempt to detect a second media if the first one detected fails
- Error message shown when files can not be removed by Metadefender Kiosk

3.4.3

Release Date: 7 February, 2017

Features

- Support for USB Flash Security encrypted drives
- Option to whitelist files larger than a specified size
- Allow administrator to disable 'Process All' option

Fixed

- Addressed issue in using Kiosk over HTTPS
- Better handling of scan results from Metadefender Core 4.x
- System files on Bitlocker encrypted devices can optionally be excluded from scanning

3.4.2

Release Date: 13 December, 2016

Features

- Metadefender Kiosk can now be configured to abort scans as soon as a blocked file is found
- Multiple Metadefender Core servers can be defined for redundancy
- Support for wiping encrypted USBs
- Alert sound can be customized

Fixed

- Better reporting of mismatched files that are found within archives
- SMTP settings for emailed session reports are now configured globally
- Estonian keyboard layout is now supported for the onscreen keyboard
- Options for handling multiple partitions have been simplified to either block devices with multiple partitions or scan all available partitions

3.4.1

Release Date: 9 November, 2016

Features

- None

Fixed

- Kiosk user will now be prompted to confirm before destination media is wiped before files are copied to it

3.4.0

Release Date: 27 October, 2016

Features

- Each Metadefender Kiosk workflow specifies a specific Metadefender Core workflow or rule to use
- Files identified as potentially vulnerable by Metadefender Core's vulnerability engine are shown in the scan results
- Metadefender Kiosk will now scan the boot sector of any media

Fixed

- The Metadefender Kiosk session log page user interface has been updated
- Potential security vulnerability with Ctrl-L key combination has been closed
- Better handling of McAfee encrypted USB devices

- Requires Metadefender Core 3.12.4 or later

3.3.6

Release Date: 30 September, 2016

Features

- Built in user authentication now supports remote Active Directory authentication.
    - Note that for remote Active Directory authentication provided user credentials are not used when files are copied as a post action.

Fixed

- Metadefender Kiosk will validate SSL certificates when using HTTPS to communicate to the Metadefender Core server. If Metadefender Core is using a self-signed certificate, this certificate must be installed on the Metadefender Kiosk machine, otherwise validation will fail.
- The Metadefender Kiosk UI will reset after the scanned media has been removed when at the scan results page

3.3.5

Release Date: 1 September, 2016

Features

- Encrypted drives can now be used as the "Copy To" destination
- Drives that are being copied to can now be wiped before files are copied

Fixed

- Server settings for e-mail notifications are now configured in Metadefender Kiosk instead of in Metadefender Core

3.3.4

Release Date: 8 July, 2016

Features

- Compatible with Metadefender Core 4.4 and later versions
- Support for Kanguru 2000 and 3000 encrypted USBs
- More flexibility allowed in the destination directory when "Copy To" post action is enabled
- Scan session log can be saved as a PDF

Fixed

- High security workflow included by default in installation
- Kiosk UI now scales to higher resolutions
- Count of files sent to a Metadefender Secure File Transfer server added to Management Console dashboard

3.3.3

Release Date: 31 May, 2016

Features

- Non-guest Metadefender Kiosk profiles can now upload to Metadefender SFT guest accounts

Fixed

- Updated onscreen Japanese keyboard
- Metadefender Kiosk can now be used with a Metadefender Core server that has an API key set
- Fixed bug where files on read-only media that are sanitized were not getting copied as part of the file handling part of the workflow
- Several hotkeys are now automatically disabled when the UI is running
- Additional minor bug fixes

3.3.2

Release Date: 19 April, 2016

Features

- Scan reports can now be sent by e-mail after the scanning session is complete
- The file upload chunk size for uploading files to a Metadefender SFT server is now configurable.

Fixed

- The sender e-mail address is no longer required when uploading files to a Metadefender SFT server
- Additional strings have been added to the Kiosk UI and can be modified through the Management Console
- The encryption method for passwords saved in the Metadefender Kiosk configuration has changed. Importing configuration from versions prior to Metadefender Kiosk 3.3.2 will not import passwords.

3.3.1

Release Date: 15 March, 2016

Features

- None

Fixed

- Better cancellation of a scan in progress
- Fixed issue when browsing blank media
- Correct detection of unencrypted Kanguru devices
- Database and Windows events can be viewed through the Management Console

3.3.0

Release Date: 30 January, 2016

Features

- The name of the product is now Metadefender Kiosk
- Administrators have the option to restrict access to domain users when Windows authentication is enabled

Fixed

- Fixed bug in importing saved configuration
- IIS Express component has been upgraded to version 8.0

3.2.0

Release Date: 23 December, 2015

Features

- Metadefender now uses Metascan workflows (Metascan versions 3.10.1 and later)
- Custom authentication modules are supported
- Windows 10 support

Fixed

- None

3.1.0

Release Date: 31 October, 2015

Features

- Metascan functionality can now be configured within the Metadefender Management Console. This is only supported for Metascan servers version 3.9.5 or later.
- Support for floppy disks as the copy destination in post-actions

Fixed

- Custom time periods can be set for the statistics displayed on the Metadefender dashboard

3.0.12

Release Date: 30 September, 2015

Features

- Upload to Policy Patrol Secure File Transfer (Requires version 2.2 or later of SFT) is now available as a post action
- The Metadefender Management Console has an updated look and feel, matching the Metascan Management Console

Fixed

- The security and compatibility of the Metadefender Management Console has been improved by replacing the PHP component with JavaScript
- Stability of the data sanitization post-action has been improved
- Fixed issue where floppy disk drives on non-English operating systems were not being recognized

- Fixed issue where in certain circumstances Metadefender might not start automatically upon system restart

3.0.11

Release Date: 31 August, 2015

Features

- None

Fixed

- Updated kiosk UI strings for non-English languages
- Improved support for
  - Ironkey D250 encrypted USBs
  - Kanguru Elite Defender 30 USBs
  - Kingston encrypted USBs
- If Windows authentication is enabled, non-local (i.e. domain) users are now required to specify their domain

3.0.10

Release Date: 30 July, 2015

Features

- None

Fixed

- Resolved issue where files would fail to copy to network locations when SHA-256 hash verification was enabled
- Resolved issue in displaying large number of files in Metadefender's browse dialog
- Support for file type conversion from image files has been removed. Conversion from PDF is now only supported to sanitized PDF. For customers that will be exporting Metadefender workflows that used this functionality OPSWAT recommends that these conversions are disabled before exporting.

3.0.9

Release Date: 30 June, 2015

Features

- None

Fixed

- Reduced the latency in loading workflow configuration when there are many user accounts on the associated active directory server
- Resolved race condition where Metadefender occasionally did not start upon system startup when installed on Windows 8 or newer operating systems
- Improved behavior when multiple instances of Metadefender are running on the same system

3.0.8

Release Date: 22 May, 2015

Features

- Windows 8.1 and 2012 R2 are now supported
- Buffalo RUF2-hsc-2gt Encrypted USBs are now supported
- McAfee Complete Data Protection Encrypted USBs are now supported
- EncryptDisc media is now supported
- Kanguru Defender Elite 30 USB devices are now supported
- Metadefender Idle Screen can be customized
- German and Korean translations of the Metadefender kiosk UI

Fixed

- Hashes of files are re-verified when the 'Copy To' post action command is used
- Better handling of network failures when scanning with a remote Metascan server

3.0.7

Release Date: 22 December, 2014

Features

- Scan logs can be saved to the media being scanned
- Recent sessions now listed in the Metadefender Management Console logs page
- Support for Buffalo SecureLock encrypted devices
- Receipt can be configured to print automatically

Fixed

- More details available in the scan result screen for files that failed to scan
- Kiosk user can be alerted when Metadefender license is close to expiration
- New HTML documentation available through the Management Console
- Romaji input supported on Japanese keyboard
- More robust support for Kingston DataTraveler encrypted USBs
- Bitlocker encrypted drives are now supported on Windows 8.1
- Other minor changes

3.0.6

Release Date: 4 November, 2014

Features

- Support for Ironkey D250 encrypted USBs
- Support for BitLocker (password) encrypted devices
- Vietnamese and Japanese user interface available by default

Fixed

- User account credentials used for post actions when Windows authentication is enabled
- Better indication when potential threats are found
- Additional scan result details included in text log file
- Debug log package available for download in Management Console
- Additional printout configuration options

3.0.5

Release Date: 1 August, 2014

Features

- Added Support of KIOSK UI localization
- Added predefined KIOSK UI Localization for Hebrew & Arabic
- Added additional predefined profiles
- More configuration for printouts

Fixed

- Fixed error when scanning empty media
- Improved accuracy of timestamps in logs
- Improved error handling and logging for errors
- Updated logs to include scan failure reason
- Clearer notification when a threat is found
- Add ability to set password in Metadefender Management Console
- Various bug fixes

3.0.4

Release Date: 8 May, 2014

Features

- Copy to user provided media as post-action
- Username is available as a variable in post-actions when Windows login is enabled

Fixed

- Improved archive handling
- Improved physical keyboard support
- Scan is aborted if connection with Metascan server is interrupted (when Metascan is on separate machine)
- Improved handling when Metascan server is operating at maximum capacity
- Fixed potential issue where Metadefender failed to launch due to latency of Windows desktop preparation
- Better logging for interruptions during post processing
- Minor bug fixes
- UI improvements

3.0.3

Release Date: 8 November, 2013

Features

- None

Fixed

- Fixed print formatting issues

3.0.2

Release Date: 27 September, 2013

Features

- Search for processing result by file upload
- Ability to export processing logs
- Allow search results to be bookmarked for later reference
- Display more detailed progress during file enumeration
- Improved Metadefender Management Console
- Improved formatting for built-in kiosk printers

Fixed

- Fixed bug that was preventing restoration of default and guest profiles
- Prevent users from being added to more than one workflow profile

3.0.1

Release Date: 5 July, 2013

Features

- User Authentication
- Customizable User Profiles
- Configurable User Questions
- Filtering by File Type
- Web-Based Metadefender Management Console
- System Restore with Deep Freeze
- File Type Conversions
- Enhanced Post-Processing Options
- New End User Workflow
- Option to Restart After Each Session
- Comprehensive Logging for all Processed Files
- Support for Kingston encrypted USB drives
- Handling USB with partially corrupted file system

Known Limitations

Handling Multiple Devices

MetaDefender Kiosk does not allow multiple devices to be processed at the same time.

Each device must be inserted independently.

Non-Windows Partitions

Wiping non-Windows partitions is not currently supported.

While non-Windows partitions are generally supported for USBs and other media, they are not supported within a VMDK file.

USB Hubs

If a USB hub with multiple USB drives is inserted into a MetaDefender Kiosk system for processing, Kiosk will only scan the first device reported to Windows.

This is not guaranteed to be the same device each time the USB hub is inserted.

OPSWAT does not recommend connecting drives to MetaDefender Kiosk through a USB hub.

Private or encrypted partitions

If a device has a private, or encrypted partition, MetaDefender Kiosk may not be able to read it. Encrypted drives can be scanned as described in Unlocking Encrypted Devices. Non-primary encrypted partitions can be blocked in the MetaDefender Kiosk Management Console. If a drive does not have any readable partitions, you can use MetaDefender Kiosk's wipe functionality to clean the drive and ensure that there are no hidden partitions. Refer to the Advanced Options section of Configuring Global Kiosk Settings for additional information.

User Account Control

If UAC is not disabled, MetaDefender Kiosk's watchdog functionality may not work as expected.

Other Known Issues

- Kiosk is expected to be operated on a local, physical system. Operating the Kiosk in a remote desktop session is not supported.
- All external USB drives, such as SD card readers, floppy disk drives, and CD ROM drives, must be inserted before MetaDefender Kiosk is started.
- Kingston encrypted devices have issues unlocking when used as a copy-to device with source media that is non-Kingston encrypted.
- For certain encrypted devices (e.g. Kanguru, Ironkey and Kingston), unlocking may fail even with the correct password if a user interacts with the Kiosk UI during the process of unlocking.

CVE-2024-52925

Description

In OPSWAT MetaDefender Kiosk before 4.7.0, arbitrary code execution can be performed by an attacker via MD Kiosk Unlock Device feature for software encrypted USB drives

References

https://docs.opswat.com/mdkiosk/release-notes

https://www.opswat.com/products/metadefender/kiosk

https://www.opswat.com/

Severity

CVSS v3.1 Vector

NIST: NVD

Base Score: 6.8

Vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Weakness Enumeration

CWE-284: Improper Access Control

Known Software Configurations

OPSWAT MDKIOSK up to (excluding) 4.7.0

Discoverer

armasuisse CYD Campus

OPSWAT.