

1. MFT Operational Intelligence	2
1.1 MFT Operational Intelligence User Guide	3
1.1.1 Get started	4
1.1.2 Install MFT Operational Intelligence	5
1.1.2.1 Install MFT Operational Intelligence on Linux	6
1.1.2.2 Install MFT Operational Intelligence on Windows Server	18
1.1.2.3 Set up MFT OI for QLTs on a Windows install	20
1.1.2.4 Upgrade MFT Operational Intelligence	21
1.1.3 Connect SecureTransport and Transfer CFT to MFT OI	27
1.1.4 Enable the File Resubmit feature for SecureTransport transfers	31
1.1.5 Time and rhythms	34
1.1.6 Plan your first week	37
1.1.7 Begin using MFT OI	39
1.1.8 Dashboard navigation	67
1.1.9 Configure watched participants and products	78
1.1.10 Manage units	82
1.1.11 Configure participant and product Role Based Access Control (RBAC)	85
1.1.12 Enable the SNMP protocol	87
1.1.13 Scan files and set window definitions for file arrival pattern detection	89
1.1.14 Review progress	99
1.1.15 Notifications	101
1.1.16 Advanced features	105
1.1.16.1 Set up the Event Router with MFT OI	107
1.1.17 Frequently asked questions	124
1.1.18 Capacity planning	137
1.1.19 Sizing	142
1.1.20 Release notes for MFT Operational Intelligence	143

MFT Operational Intelligence

Welcome to the user guide for MFT Operational Intelligence.

First things first

You may have never used a product quite like MFT Operational Intelligence (MFT OI). To make the most of your first experience with MFT OI, take a few minutes and read this guide. Please begin by reading this [important](#) topic. Additionally, you may find answers to questions in the [FAQs](#).

Key features

The following high-level features form part of this release:

- Capacity Planning: Sizing Guidance published, allowing you to resource your MFT OI server/VM correctly
- Self-Service Start-Up: The installation and configuration process is accessible/achievable by a non-technical person by gathering configuration upfront to enable deployment in a matter of minutes.
- OOTB Dashboards: With a Global Overview landing page, attention is placed on the topics requiring your attention or action, leading to more drill-down views, whether it is the performance of transfer activity globally, from a particular product instance, or from a particular participant
- Expected File Windows Templates: Auto-prediction of expected transfer activity based on extended use of ADI's ML/Baselining features
- Self-Service Notifications: Business users can easily configure who will receive notifications when key scenarios arrive. The option to directly alert stakeholders to unexpectedly high levels of exceptions at Global, Product (SecureTransport or Transfer CFT nodes), and Participant levels

Plan your initial deployment

There are four initial phases to starting out with MFT OI, which should take a matter of a few hours spread over two days:

1. Installing the product and connecting to the SecureTransport or Transfer CFT instances that feed it.
2. Understanding the information that you see in the dashboards.
3. Configuring watched participants and watched products (what are those? Check the FAQs).
4. Validating the information reported by MFT OI against what you expect to see

Once you have completed these steps, there are three additional aspects to validate.

This second set deals with file transfer patterns and will require another about an hour or two for a few more days. One significant component of the value of MFT Operational Intelligence is its ability to detect patterns in the arrival of files. Patterns are based upon the count of files received for a participant during 1-hour intervals on a given day of the week. For example, here is a pattern of files expected for a watched participant on the current day:

The second part of getting to know MFT OI requires:

1. Selecting patterns detect by Operational Intelligence to be monitored.
2. Validating the ability of MFT OI to detect when a pattern is followed on a matching hour and day.
3. Verifying that MFT OI also detects when transfers do not follow the pattern (that is, the minimum count of files is not reached during the expected file window).

Of course, the most important part is to record your feedback, noting anything we didn't explain clearly enough or any ideas on how to improve the product scope or features.

We'll gladly listen and take them into account for the product's development.

Thanks for your help!

Next

[Install MFT Operational Intelligence](#)

MFT Operational Intelligence User Guide

This guide is for users who install, configure and use MFT Operational Intelligence.

Quick reference links

- [Get started](#)
- [Time and rhythms](#)
- [Frequently asked questions](#)

Get more help

The following are additional resources.

Documentation

For user documentation about other Axway products and services, visit the [documentation portal](#).

Support

If you still have questions after reviewing the [FAQs](#), contact the Axway Global Support team.

Axway Global Support provides worldwide 24 x 7 support for customers with active support agreements. Email support@axway.com or visit [Axway Support](#).

Training

Axway offers [training](#) across the globe, including on-site instructor-led classes and self-paced online learning.

Jun 16, 2026

Get started

Welcome to the user guide for MFT Operational Intelligence.

First things first

You may have never used a product quite like MFT Operational Intelligence (MFT OI). To make the most of your first experience with MFT OI, take a few minutes and read this guide. Please begin by reading this [important](#) topic. Additionally, you may find answers to questions in the [FAQs](#).

Key features

The following high-level features form part of this release:

- Capacity Planning: Sizing Guidance published, allowing you to resource your MFT OI server/VM correctly
- Self-Service Start-Up: The installation and configuration process is accessible/achievable by a non-technical person by gathering configuration upfront to enable deployment in a matter of minutes.
- OOTB Dashboards: With a Global Overview landing page, attention is placed on the topics requiring your attention or action, leading to more drill-down views, whether it is the performance of transfer activity globally, from a particular product instance, or from a particular participant
- Expected File Windows Templates: Auto-prediction of expected transfer activity based on extended use of ADI's ML/Baselining features
- Self-Service Notifications: Business users can easily configure who will receive notifications when key scenarios arrive. The option to directly alert stakeholders to unexpectedly high levels of exceptions at Global, Product (SecureTransport or Transfer CFT nodes), and Participant levels

Plan your initial deployment

There are four initial phases to starting out with MFT OI, which should take a matter of a few hours spread over two days:

1. Installing the product and connecting to the SecureTransport or Transfer CFT instances that feed it.
2. Understanding the information that you see in the dashboards.
3. Configuring watched participants and watched products (what are those? Check the FAQs).
4. Validating the information reported by MFT OI against what you expect to see

Once you have completed these steps, there are three additional aspects to validate.

This second set deals with file transfer patterns and will require another about an hour or two for a few more days. One significant component of the value of MFT Operational Intelligence is its ability to detect patterns in the arrival of files. Patterns are based upon the count of files received for a participant during 1-hour intervals on a given day of the week. For example, here is a pattern of files expected for a watched participant on the current day:

The second part of getting to know MFT OI requires:

1. Selecting patterns detect by Operational Intelligence to be monitored.
2. Validating the ability of MFT OI to detect when a pattern is followed on a matching hour and day.
3. Verifying that MFT OI also detects when transfers do not follow the pattern (that is, the minimum count of files is not reached during the expected file window).

Of course, the most important part is to record your feedback, noting anything we didn't explain clearly enough or any ideas on how to improve the product scope or features.

We'll gladly listen and take them into account for the product's development.

Thanks for your help!

Next

[Install MFT Operational Intelligence](#)

Install MFT Operational Intelligence

This section describes prerequisites and how to install MFT Operational Intelligence (MFT OI).

MFT OI consists of two components:

- Axway Decision Insight (ADI): Axway's analytics platform
- MFT OI: The comprehensive application that runs on the platform

During installation, upload the installation file containing ADI and MFT OI. The file also contains scripts to automate the installation and configuration of both products. Barring any errors, the installation should take a few minutes.

Prerequisites

This section describes the installation prerequisites.

Hardware

Install the MFT OI software on a Linux server or virtual machine using the sizing described in the [Sizing for MFT OI](#) page.

Operating system

Supported operating systems include:

- Linux
- RHEL8
- Ubuntu 16.04
- Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019, 2022 running on-premise or in Microsoft Azure cloud

Next

[Connect SecureTransport and Transfer CFT to MFT OI](#)

Install MFT Operational Intelligence on Linux

This page describes the steps required to install MFT Operational Intelligence on a Linux machine or server.

User limits

Check and adjust the root user's limits on the server where you are installing MFT OI. The table has the required settings for parameters that may require adjusting.

Parameter	Limit
max user processes	at least 65536
open files	at least 65536
max memory size	unlimited
virtual memory	unlimited

To check the current limits set on the Linux server or VM hosting MFT OI, use the following command:

```
ulimit -a
```

The system responds with a listing similar to this:

```
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority     (-e) 0
file size               (blocks, -f) unlimited
pending signals         (-i) 31152
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files              (-n) 31152
pipe size               (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
real-time priority      (-r) 0
stack size              (kbytes, -s) 8192
cpu time                (seconds, -t) unlimited
max user processes      (-u) 31152
virtual memory          (kbytes, -v) unlimited
file locks              (-x) unlimited
```

You can use the `ulimit` command to adjust the limits as needed.

```
ulimit -m unlimited

ulimit -n 65536
ulimit -u 65536
ulimit -v unlimited
```

Alternatively, you can adjust the hard limits by editing the `limits.conf` file in the `/etc/security/` folder on the Linux server or VM hosting MFT OI.

You can add more entries to set limits for the root user at the bottom of the file (see example).

```
#<domain>      <type>  <item>      <value>
#
#*              soft    core         0
#*              hard    rss          10000
#@student       hard    nproc        20
#@faculty       soft    nproc        20
#@faculty       hard    nproc        50
#ftp            hard    nproc        0
#@student       -       maxlogins     4
root            -       nproc        65536
root            -       nofile       65536
# End of file
```

If you choose to edit the user limits in `limits.conf`, once you have updated the file, you must disconnect all terminal sessions. Changes only take effect after you log in again.

Software

Download the following from the Axway website:

- The latest version of MFT Operational Intelligence **MFT OI V1.0.20230713**
- Decision Insight YYYYMMDD-NN Linux CLI installer tar file where YYYYMMDD-NN indicates the date-based release number.
 - The Decision Insight file to download uses the following format: `DecisionInsight_2.0.0_Install_linux-x86-64_BNYYYYMMDDNN.tar.gz`
 - We recommend using the latest available version of Decision Insight
 - **MFT OI V1.0.20230713** requires Decision Insight V2.0.20230116-04 or higher to run properly

Before installing

Read the following before continuing. Once you have completed these preparations, you can move on to uploading the install package.

Time and time zones

The dashboards and analysis in MFT OI are time-based, which has two implications for your installation. The first deals with the accuracy of the time settings for the server, as discussed in the next section. The second deals with time zones. As discussed in the following sections, if the server where MFT OI is installed is configured to be in the same time zone as those who view the dashboards, you do not have to configure time zone settings. If users are in a different time zone than where MFT OI is running, read [time zone settings](#) for options.

Accurate time settings

As dashboards and analysis in MFT OI are time-based, make sure the wall clock setting is correct on the system where you are installing. The time should be correct if your system uses automatic time configuration such as NTP. You want to avoid a situation where the current time on your watch tells you it is 7:14, and the system says it is 7:28. This has the potential to make interpreting what you see on a dashboard challenging. Precision is not required down to the second level; keeping time within a minute or two is not an issue. You can check the time on your system with the `date` command. If it is not set correctly, you can set it with the `timedatectl` command, for example:

```
timedatectl set-time 18:19:20
```

Time zone settings

MFT OI is set up to consider activity during a current day and is therefore sensitive to the time zone setting as to the start and end of the day. The setting affects how data is displayed on the dashboard, and because of that, you may need to set the time zone of the host system. When practical, the time zone should be set to be the same as the one where the dashboards are used. See *Why does MFT OI care about the date, time, and time zone settings?* in [the FAQs](#) for an explanation. If you need to change the time zone on your MFT OI system, it is important that you do it now. Once you install MFT OI, the time zone cannot be changed. If you need help checking your time zone or changing it, see *How do I check and change the time zone on my system?* in [the FAQs](#).

Dashboard access

MFT OI supports two means of dashboard access: unsecured (via HTTP) and secured (via https). You can decide before installation which method you choose to use. You can also change your selection after installation. The way you select the option is different before and after installation. The process for selecting either now is documented here. To change after installation, see [Advanced features](#).

Unsecured dashboard access

By default, MFT OI uses port 8080 for unsecured access to the solution. The address to view dashboards is: `http://<system name or IP address>:8080`

If needed, you can change the default port number during installation. After installation, you can make modifications as described in the [Advanced features](#) section.

Secured dashboard access

During installation, you have the option to select secured communication for dashboard access. MFT OI, by default, uses port 8443 for secured access to the solution. That is, the secured address to view dashboards is:

`https://<system name or IP address>:8443`

You can change the default port number after the installation as described in [Advanced features](#).

If you plan to configure secure communications, your Keystore must be available in the location you reference before you start the installation script.

Administrative user password

MFT OI uses "admin" as the default administrator user ID, which cannot be changed. During installation, you are asked to provide the password for the admin user. You can prepare now for installation by deciding the password for the admin user.

Encryption

MFT OI uses a database to store information for the purposes of historical, analytics, and real-time display. For security, that database is encrypted. There are three questions about the encryption during the installation process:

1. A location where the install process generates the salt for the encryption key (a salt file, if you are unsure of the term, is used to help protect the hash generated by the encryption key)
2. A location to store the encryption key hash
3. The encryption key password

There are defaults for the first two if you do not have particular security requirements to locate them in specific locations. You should prepare the encryption key password you want to use.

Deploying MFT Operational Intelligence

Two approaches are set out below:

- A step-by-step, self-service guide to installing MFT OI that utilizes auto-installation scripts to assist in the process
- A more advanced 'Silent Install' approach is covered.

Self-Service MFT Operational Intelligence Installation

The following sections describe the necessary steps once the MFT Operational Intelligence installer files have been acquired.

Upload the install package

First, create a directory on the host system from where you install MFT OI. This does not have to be the destination for the installed MFT OI, only where the installation scripting and sources are launched. For example:

```
mkdir /opt/mftoi
```

Next, place the two downloaded files and license files in the new directory. Then, go on to the next step.

1. The Decision Insight platform release file (DecisionInsight_2.0.0_Install_linux-x86-64_BN2023011604.tar.gz). This file contains the Axway analytic platform that supports the MFT OI application.
2. MFTOI Installer file (MFT_ProductExtension_MFTOIv20230713_linux-x86-64_BN20230714.zip)
3. Your license key file (with the extension .licence), which is needed to use MFT OI.

Unzip the MFT OI installer file

Expand the MFT OI installer package with the unzip command, e.g., `unzip {MFTOI Installer package}`. You must specify the exact file name (replacing the XX in the example):

```
MFT_ProductExtension_MFTOIv20230713_linux-x86-64_BN20230714.zip
```

This creates files in the directory that are required for the installation:

1. Install scripts, config files, and other supporting files.
2. MFTOI appx and properties.xml files (the MFTOI application).

When the MFT OI installation package is unzipped, a sub-directory named **Linux-installer** is created containing the extracted contents of the package. Then, put these files in the same location as the license and Decision Insight installation.

Ensure all the files (DecisionInsight_2.0.0_Install_linux-x86-64_BN2023011604.tar.gz and the file ending in .licence) are in the same directory before continuing.

The spelling of the file extension is licence. While this is misspelled, that is the correct extension.

The results of expanding the install zip file and copying the license and tar files should produce contents as follows:

```
-rw-r--r--. 1 root root      938 Sep  8 14:18 decision_insight.config
-rw-r--r--. 1 root root 1215837 Sep  7 15:57 mft_oi_App.appx
-rw-r--r--. 1 root root    3054 Sep  7 15:57 mft_oi_App.properties.xml
-rwxr-xr-x. 1 root root     928 Sep  7 15:57 mft_oi_banner.sh
-rw-r--r--. 1 root root     233 Sep  9 13:20 mft_oi_install.config
-rwxr-xr-x. 1 root root   26179 Sep  7 15:57 mft_oi_install.sh
-rwxr-xr-x. 1 root root    1896 Sep  7 15:57 mft_oi_splash.sh
-rwxr-xr-x. 1 root root    6331 Sep  7 15:57 test.sh
-rwxr-xr-x. 1 root root     187 Sep  7 15:57 wait_for_log_line.sh
```

Link the install configuration to the license file

You need to edit the configuration file for the installation to point to your license file. The configuration file to be edited is mft_oi_install.config. The contents of the file, as released, are:

```
1. adiversion=20230116
2. adiinstalldir=/root/linux-installer/node_ad
3. importdate="-28 days"
4. license=
```

Copy the entire name of the licence file and paste it after the = sign on line 4. Save the file.

To enable silent installation, the following line must be added to the mft_oi_install.config file

```
ACCEPT_GENERAL_CONDITIONS=yes
```

The installation path (adiinstalldir) can be absolute or relative.

By adding this line, you are agreeing to the following [Axway General Conditions](#):

You hereby accept that the Axway Products and/or Services shall be governed exclusively by the Axway General Terms and Conditions located at Axway_General_Conditions unless an agreement has been signed with Axway, in which case such agreement shall apply.

The importdate is the time when the application should be deployed. You no longer have to adjust the import date as this is now calculated and set for you on line 3. Take care if you edit this value, as this should be a recent time and must be after the time the DecisionInsight platform is deployed. This is now automatically configured for you.

When the files and changes are in place, you are ready to move to the next step.

Do you need to change the port number for unsecured dashboard access?

To change the default 8080 to a different port, edit the decision_insight.config file in the install directory. The contents of the file (ignoring the line numbers) are:

```
[conf/platform.properties merge]
systar.platform.name=DecisionInsight
osgi.service.http.port=8080
systar.krypton.scheduler.collector.defaultComputingLag=30 seconds

com.axway.mftoi.qlt.url=qlt:0.0.0.0:1305
com.axway.mftoi.qlt.keystore.path=../security/keyStore.jks
com.axway.mftoi.qlt.keystore.password=
com.axway.mftoi.qlt.keystore.keyPassword=
com.axway.mftoi.qlt.truststore.path=../security/trustStore.jks
com.axway.mftoi.qlt.truststore.password=
com.axway.mftoi.qlt.cipherSuites=
com.axway.mftoi.qlt.secureSocketProtocols=

com.axway.mftoi.smtp.address=
com.axway.mftoi.smtp.password=
com.axway.mftoi.smtp.username=

[conf/jvm.conf merge]
-Xmx16G
```

Edit the value of 8080 on line 3 to be the port number you want and save the file.

To choose a different service name for the service, adjust line 2. For example:

```
systar.platform.name=DecisionInsight8081
```



The following line was removed from the file as the default import time is now set to 1 month before the current date.

```
systar.titanium.initialPeriodValidTimeEnd=2021-09-01T00:00:00.000
```

Time zones

Do you want all users to see a consistent time zone presented in dashboards?

As explained in [time zone settings](#), you have the chance to implement that now. Add the statement as the last line of the [conf/platform.properties merge] block in the `decision_insight.config` file shown above.

```
com.systar.carbon.dashboard.server.timezone=true
```

Specifying a time zone for the installation

At the end of the file, under the `jvm.conf merge` line, add the `timezone`. For example, `-Duser.timezone=Europe/London`

```
[conf/jvm.conf merge]
-Xmx16G
-Duser.timezone=Europe/London
```

Install MFT OI

To install MFT OI, navigate to the `install` folder created when you expanded the installation package.

The user must execute all the shell scripts for the installer to work.

Check this using the long list (`ll` or `ls -l`) function, and if not, use the following command:

```
chmod u+x *.sh
```

By default, the installer provides a menu to assist in choosing the steps to deploy MFT OI.

If you require help at the command line, use the `-h` or `--help` with the main `mft_oinstall.sh` script.

```
./mft_oi_install.sh -h
./mft_oi_install.sh --help
```

When ready, call the installation script:

```
./mft_oi_install.sh
```

```

      / \
     / \  ^
    / \  /
   / \ /
  / \ /
 / \ /
A X W A Y

M   M   FFFFF   TTTTT   OOOOO   IIIII
MM  MM  F       T       O  O   I
M MM M  FFF     T       O  O   I
N   M   F       T       O  O   I
M   M   F       T       OOOOO   IIIII

Starting install
Reading config settings
Getting version number
Getting Service name from decision_insight.config
Service Name: DecisionInsight87922

HTTPS is not enabled. Configuring HTTP
port set to 8792
Validating script configuration

Press any key to continue
```

In this example, the Service Name is set as DecisionInsight87922, with port 8792 and HTTP to be used.

There is a prompt to "Press any key to continue" to allow the script to be aborted (ctrl+c) at this point should you notice any changes required to the configuration.

(We abort our installation to change the configuration to have the Service Name DecisionInsight8792 and restart.)

If okay to process, press any key.

The script presents a menu by default (without using any additional parameters).

```

      / \
     / \  ^
    / \  /
   / \ /
  / \ /
 / \ /
A X W A Y

M   M   FFFFF   TTTTT   OOOOO   IIIII
MM  MM  F       T       O  O   I
M MM M  FFF     T       O  O   I
N   M   F       T       O  O   I
M   M   F       T       OOOOO   IIIII

1) Test Prerequisites
2) Full Deployment as a root user (service)
3) Full Deployment as a non-root user
4) Install DecisionInsight only (inc Prerequisites Test)
5) Register and Start DecisionInsight as a service
6) Start DecisionInsight as a non-root user
7) Deploy MFTOI
8) Uninstall
9) Quit
Please enter your choice between 1 and 9 : 
```

To deploy a full installation, choose option 2 or 3. Other options are provided to complete the deployment in stages should multiple resources be required (for example, Option 5. Register and Start DecisionInsight as a service).

For the full deployment or the installation of DecisionInsight, the installer prompts you to accept the software's Axway General Terms and Conditions. To accept, enter Y at the prompt and press return.

```

      A   DDDD DDDD IIIII N   N GGGGG
    A A D D D D I   NN N G
  A A D D D D I   NN N N G GGG
AAAAA D D D D I   N N N G G
  A A DDDD DDDD IIIII N   NN GGGGG

```

```

OOOOO PPPPP EEEEE RRRRR A TTTT IIIII OOOOO N   N A L
O O P P E R R A A T I O O NN N A A L
O O PPPPP EEE RRRR A A T I O O NN N A A L
O O P E R R AAAAA T I O O N N N AAAAA L
OOOOO P EEEEE R R A A T IIIII OOOOO N NN A A LLLLLL

```

```

IIIII N   N TTTT EEEEE L L IIIII GGGGG EEEEE N N CCCC EEEEE
I N N T E L L I G E NN N C E
I N N N T EEE L L I G GGG EEE N N N C EEE
I N N N T E L L I G G E N N N C E
IIIII N NN T EEEEE LLLLL LLLLL IIIII GGGGG EEEEE N NN CCCC EEEEE

```

You hereby accept that the Axway Products and/or Services shall be governed exclusively by the Axway General Terms and Conditions located at [https://cdn.axway.com/u/Axway_General_Conditions_version_april_2014_eng%20\(France\).pdf](https://cdn.axway.com/u/Axway_General_Conditions_version_april_2014_eng%20(France).pdf), unless an agreement has been signed with Axway in which case such agreement shall apply.

Do you agree? [Y]es / [N]o ☒

After you agree to the license, the installation proceeds. The next part verifies that you have set the user limits as required and, if successful, prompts you to enter the admin password:

M	M	FFFFF	TTTTT	00000	IIIIII		
MM	MM	F	T	0	0	I	
M	MM	M	FFF	T	0	0	I
N	M	F	T	0	0	I	
M	M	F	T	00000	IIIIII		

```
Initiating checks with failure count set to 0.
```

```
Prerequisites Validated.
Creating start time file
```

Begining Decision Insight installation process

Unzipping file

Installing DecisionInsight

```
Using installer 'DecisionInsight_20210719-01' from /opt/beta_0.19/installer/DecisionInsight_20210719-01
Installing node in ../MFTOI-136/node_20210719
Copying product from installer
Deploying node template
Applying configuration file decision_insight.config
Platform Initialization:
Generate Admin Password
```

Once you enter the admin password, you are asked to re-enter it. If both passwords match, the next questions involve database encryption.

```
Please confirm the admin password:
Admin password hash generated in file /opt/mftoi/install/node_20210412/var/data/default.hash
Admin password hash generated in file: /opt/mftoi/install/node_20210412/var/data/default.hash
Admin password generation done.
Generate Encryption Key
Please specify the encryption.salt absolute folder path where a random encryption salt will be generated :
[/opt/mftoi/install/node_20210412/var/data/titanium-temporal]:
Creating path: [/opt/mftoi/install/node_20210412/var/data/titanium-temporal]
Please specify the encryption key file path where the encryption key will be generated (can be absolute or relative to the platform conf folder):
[/opt/mftoi/install/node_20210412/conf]:
Please enter the encryption password:
Please confirm the encryption password:
```

You can see the three questions about database encryption. The defaults for the first two are shown in brackets. If you hit enter, the process uses the defaults. Unless you have specific security requirements, the defaults work without a problem.

The third question asks you for the password itself. Once entered, you are asked to re-enter it. If both keys match, the process continues.

The next step of the process asks if you wish to secure communications. If you want to use unsecured communications, press **n** at the prompt, and the installation continues to completion. If you want secure communications, enter **y**, and the process asks you to describe the security options.

To secure communications, you must answer three questions regarding the Keystore:

1. The path to your keystore
2. The password to your Keystore
3. The password for the certificate in the Keystore.

```
Please confirm the encryption password:
Salt file [/opt/mftoi/install/node_20210412/var/data/titanium-temporal/encryption.salt] created.
Encryption file [/opt/mftoi/install/node_20210412/conf/encryption.key] created
Encryption key generation done.
Secure communications
Do you want to secure communications? [y]/n y
Please enter the path to the keystore: /etc/keystore
Please enter the keystore password:
Please confirm the keystore password:
Please enter the keystore key password:
Please confirm the keystore key password:
Secure communication done.
```

In the above example, the Keystore is in the `/etc/keystore` directory.

After you have specified the location of the keystore, you are prompted to enter the keystore password. As with previous passwords in the installation process, you are asked to confirm by entering it twice. If they match, you are asked to enter the keystore key password. This password also requires confirmation.

If both passwords are confirmed, secure communications are configured. After this, dashboards are no longer accessible on port 8080 but on port **8443**. This value can be changed. For explanations on how to achieve this, see [Advanced features](#).

The last line in the example above, `Secure communication done`, indicates this section of the installation is complete.

If you had answered the question the other way about secure communications, the sequence of messages would have skipped the questions about the keystore:

```
Secure communications
Do you want to secure communications? [y]/n n
Secure communication done.
```

After the message about secure communications, the installation continues through a number of steps and is completed normally. A message similar to the following is displayed:

```

Decision Insight (DI) Installed at ../MFTOI-136/node_20210719

Getting Service name from decision_insight.config
Service Name: DecisionInsight8792
OS distribution is rhel
setting service auto run levels using chkconfig
DI Service registered as DecisionInsight8792.
Creating import directory and copying MFTOI applicaiton files.

Starting DecisionInsight8792

Waiting for 'Platform started' to appear in '../MFTOI-136/node_20210719/var/log/node.log'
2021-09-13 13:05:16,456 [Domain-platform-18-nodeAvailabilityMonitor] INFO platform.nodeAvailabilityMonitor - Platform
started {"args": {"duration": "17.292 sec"}}

DI Service DecisionInsight8792 has been started.

Waiting for 'File import done' to appear in '../MFTOI-136/node_20210719/var/log/node.log'
2021-09-13 13:05:21,709 [Domain-platform-27-nodeAvailabilityMonitor] INFO carbon-provisioning.directoryImporter - Fil
e import done {"args": {"file": "/opt/beta_0.19/MFTOI-136/node_20210719/var/data/carbon-provisioning/autoimport/incom
ing/mft_oi_App.appx"}}
*** MFT Operational Intelligence application has been successfully imported. ***
Checking routes have started...
01_ConsumeTrackedObject
Waiting for 'Integration.01_ConsumeTrackedObject) started' to appear in '../MFTOI-136/node_20210719/var/log/integrati
on.log'
2021-09-13 13:05:24,856 [Domain-aluminium-engine-84-contextRuntimeFactory.eef9f070-fad0-440e-1774-839774600801] INFO
org.apache.camel.impl.engine.AbstractCamelContext - Apache Camel (Integration.01_ConsumeTrackedObject) started in 89
6ms
Route Integration - 01_ConsumeTrackedObject started
02_CompleteInProcessTransfer
Waiting for 'Integration.02_CompleteInProcessTransfer) started' to appear in '../MFTOI-136/node_20210719/var/log/inte
gration.log'
2021-09-13 13:05:24,146 [Domain-aluminium-engine-81-contextRuntimeFactory.0000000c-0001-0000-1786-f607b1200801] INFO
org.apache.camel.impl.engine.AbstractCamelContext - Apache Camel (Integration.02_CompleteInProcessTransfer) started
in 466ms
Route Integration - 02_CompleteInProcessTransfer started
03_UpdateProductInstance
Waiting for 'Integration.03_UpdateProductInstance) started' to appear in '../MFTOI-136/node_20210719/var/log/integrat
ion.log'
2021-09-13 13:05:24,160 [Domain-aluminium-engine-82-contextRuntimeFactory.0000000c-0001-0000-177f-8dcb7a000801] INFO
org.apache.camel.impl.engine.AbstractCamelContext - Apache Camel (Integration.03_UpdateProductInstance) started in 4
82ms
Route Integration - 03_UpdateProductInstance started
99_TimerCloseTransfers
Waiting for 'Integration.99_TimerCloseTransfers) started' to appear in '../MFTOI-136/node_20210719/var/log/integratio
n.log'
2021-09-13 13:05:24,168 [Domain-aluminium-engine-78-contextRuntimeFactory.eef9f070-fad0-440e-176f-33ef76d00001] INFO
org.apache.camel.impl.engine.AbstractCamelContext - Apache Camel (Integration.99_TimerCloseTransfers) started in 469
ms
Route Integration - 99_TimerCloseTransfers started

installer]# █

```

That final message should be displayed about the process being completed successfully. In case of an issue, one or more error messages display instead of the success message.

Uninstall

When an installation fails, you may need to back out of the current installation before restarting.

Check the contents of the node.log file in the <install path>/var/log/ directory, which should highlight any error. Enter:

```
tail -200 {{install path}}/var/log/node.log
```

There is an option as part of the installer to uninstall MFT OI. This attempts to stop any service or process running Decision Insight, unregister it, and create an archive of the log files before cleaning the installation.

The extracted Decision Insight source remains, but this can be deleted if no longer required.

See the topic: *How can I clean up after an unsuccessful install?* in [the FAQs](#) on removing the partial installation in preparation for restarting the installation at *Unzip the Package* step above.

Installation validation

After normal completion, check to make sure you can log on and see the dashboard. You should now be able to log on to the MFT OI application installed in the previous section. To do so, navigate to the appropriate URL:

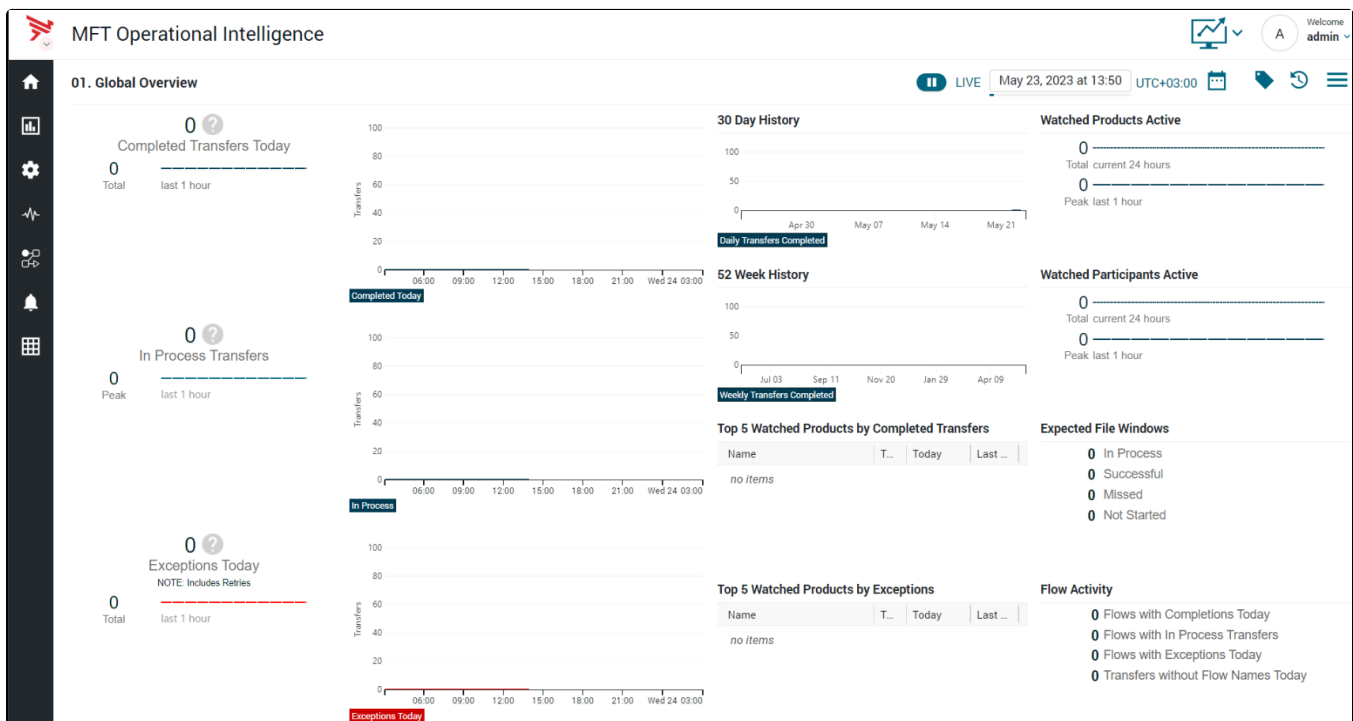
```
http://<host>:<port>/ui  
or  
https://<host>:8443/ui
```

Where:

- **<host>** is the name or IP address of the server on which MFT OI is installed
- **<port>** is the value set for the **http port** parameter in the **config** file as described in *Dashboard Access*, above.

Sign in to MFT OI as the application administrator using the *admin* username and the password you defined during the installation:

Upon successful login, you should observe an empty instance of the **01. Global Overview** dashboard. If you see a page of thumbnails, click on the Home icon in the left-hand menu to display the Global Overview dashboard. This is the default dashboard for administrative users of MFT OI and resembles the screenshot below:



You have successfully installed the MFT OI application and the Decision Insight platform it runs on.

Advanced MFT Operational Intelligence installation

An advanced "Silent Install" deployment methodology is also supported within MFT Operational Intelligence

Silent install (no prompt)

For a Silent installation, additional configuration is required to provide the admin user password and encryption hash to the *decision_insight.config* file, which is used during installation.

An example of the additional lines are:

```
[var/data/default.hash overwrite]  
4095:2b6e8c51c1dd840aa17a5f4bc9332b4fa352f8cd33f54262:47baaaebf159428fc98adaece419bfa07e28d67bf3ec3231  
  
[conf/encryption.key overwrite @base64]  
Et7KgHv7K8qZM0yoszvug==
```

To enable a silent installation, add the following line to the *mft_oi_install.config* file:

```
ACCEPT_GENERAL_CONDITIONS=yes
```

QLT connection settings

The `decision_insight.config` contains the parameters to configure the QLT connection, whether it is secured or unsecured.

```
com.axway.mftoi.qlt.url=qlt:0.0.0.0:1305
com.axway.mftoi.qlt.keystore.path=../security/keyStore.jks
com.axway.mftoi.qlt.keystore.password=
com.axway.mftoi.qlt.keystore.keyPassword=
com.axway.mftoi.qlt.truststore.path=../security/trustStore.jks

com.axway.mftoi.qlt.truststore.password=
com.axway.mftoi.qlt.cipherSuites=
com.axway.mftoi.qlt.secureSocketProtocols=
```

SMTP settings

The `decision_insight.config` contains the parameters to configure the SMTP server for email notifications

```
com.axway.mftoi.smtp.address=
com.axway.mftoi.smtp.password=

com.axway.mftoi.smtp.username=
```

License and certificates

After installing MFTOI, the license is saved in the installation directory:

```
/root/linux-installer/node_adi/lib/licences
```

To remove or add a new license, stop the node and make the changes. Then, restart the node for the new license to be activated.

Install MFT Operational Intelligence on Windows Server

This page describes how to install MFT OI using the automated deployment scripts available for Windows Servers.

Pre-installation steps

- Move the installation archive `MFT_ProductExtension_MFT0Iv20230713_win-x86-64_BN20230714.zip` to the chosen install location on the assigned Windows Server.
- Extract the contents by right-clicking the archive and selecting **Extract All**.
- Select **Extract** in the dialog box button to accept the default (and required) location. This creates a further sub-folder, named **windows-installer**, for the extracted content.
- Double-click the **windows-installer** folder to access it.
- Move the ADI installer to the newly created **windows-installer** subfolder.

When finished, the **windows-installer** folder should contain the following items:

- `decision_insight.config`
- `mft_oi_install.bat`
- `mft_oi_install.ps1`
- `mft_oi_install.psd1`
- `Util Folder`
- `mft_oi_APP.appx`
- `mft_oi_App.properties`
- `mft_oi_APP.properties.xml`
- `mft_oi_uninstall.bat`
- `mft_oi_uninstall.ps1`
- the license file
- `DecisionInsight_2.0.0_Install_win-x86-64_BNYYYYMMDDNN.zip`
This is the Decision Insight installer where YYYYYMMDDNN is the date/build number of the ADI version downloaded

Working with the Embedded Analytics configuration file

There is also information referenced in the `mft_oi_install.psd1` file that may need adjusting. An example file looks like this:

```
adiversion = '20230116'  
adiinstalldir = 'node'  
importdate = '-28 days'  
license = 'axway-internal-window.licence'
```

The automated installation process carries out an ADI version check, setting the default installation directory and application import date.

- **adiversion** - The ADI version referenced must match the one that has been downloaded
- **adiinstalldir** - You can leave the default value of **'node'**
- **importdate** - The date on which the installation/import is being carried out is automatically calculated.
- **license** - Copy the entire name of the `license` file and paste it after the `=` sign on line 4.

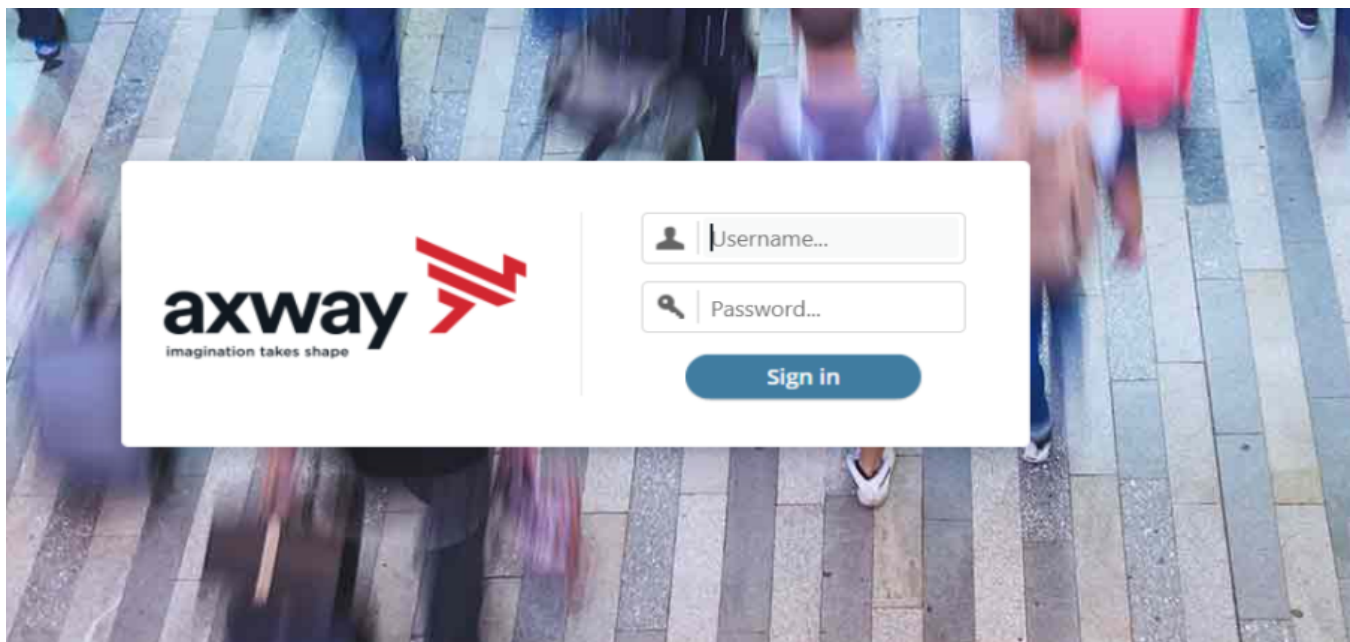
Installing MFT Operational Intelligence on Windows

The automated install script that has been prepared is now available in the **windows-installer** folder:

- Navigate to the **windows-installer** folder;
- Run the automated script by clicking the **mft_oi_install.bat** file. You may need to accept an admin advisory message to proceed.

Check that the installation was successful

Log on to the MFT Operational Intelligence application admin GUI of the instance installed in the previous section: <https://<host>:<port>>. The default user name and password are admin/admin.



Silent install (no prompt)

For a Silent installation, additional configuration is required to the "decision_insight.config" file, which is used during the installation process, and to the "mft_oi_install.ps1".

"Decision_insight.config" must contain default.hash and encryption.key properties for the installation be run without user prompts.

An example file with these settings would look like this:

```
[var/data/default.hash overwrite]
4095:2b6e8c51c1dd840aa17a5f4bc9332b4fa352f8cd33f54262:47baaaebf159428fc98adaece419bfa07e28d67bf3ec3231

[conf/encryption.key overwrite @base64]
Et7KgHv7K8qQzM0yoszvug==
```

In the file mft_oi_install.ps1 file, add the line ACCEPT_GENERAL_CONDITIONS = 'yes' like this:

```
@{
    adiversion = '20230116'
    adiinstalldir = 'node'
    importdate = '-28 days'
    license = 'axway-internal-window.licence'
    ACCEPT_GENERAL_CONDITIONS = 'yes'
}
```

Once these two files are updated, run the mft_oi_install.ps1 script from a PowerShell command line with the -noPrompt option: `.\mft_oi_install.ps1 -noPrompt`

The silent installation is ready to start.

You must run the PowerShell as administrator.

Set up MFT OI for QLTs on a Windows install

Configure the QLT connection

After the installation is complete, you can configure the QLT secure connection. Before making any changes, you must stop the service.

- To do this configuration, you have to check if the Keystore and Truststore exist for MFT OI.
- If there is no Keystore present, use the instructions in the following section to generate a self-signed server certificate and import it into a Keystore and truststore.

1. Create a Keystore that contains the server certificate. This would be possible only with the path DecisionInsight folder\lib\jre\bin

```
keytool -genkey -alias MFTOI -keyalg RSA -keypass <PASSWORD> -storepass <PASSWORD> -keystore MFTOI-keystore.jks
```

Replace <PASSWORD> with a password of your choice.

Export the certificate into a .cer file

```
keytool -export -alias MFTOI -storepass <PASSWORD> -file server.cer -keystore MFTOI-keystore.jks
```

Replace <PASSWORD> with a password of your choice.

This generates the two files:

MFTOI-keystore.jks

server.cer

2. Add the server certificate to a truststore that contains the CA of the server certificate

```
keytool -import -v -trustcacerts -alias MFTOI -file server.cer -keystore MFTOI-truststore.jks -keypass <PASSWORD> -storepass <PASSWORD>
```

Replace <PASSWORD> with the password of the keystore.

This generates the file: [MFTOI-truststore.jks](#)

Set up QLTs

To enable QLTs, make the following changes in the conf/platform.propertiesfile

```
com.axway.mftoi.qlt.url=qlts:0.0.0.0:1303?sslContextParameters=#qltSslContextParameters
com.axway.mftoi.qlt.keystore.path=${com.systar.platform.conf.dir}/MFT OI-keyStore.jks
com.axway.mftoi.qlt.keystore.password=<KEYSTORE_PASSWORD>
com.axway.mftoi.qlt.keystore.keyPassword=<KEY_PASSWORD>
com.axway.mftoi.qlt.truststore.path=${com.systar.platform.conf.dir}/MFT OI-trustStore.jks
com.axway.mftoi.qlt.truststore.password=<TRUSTSTORE_PASSWORD>
```

Example

After furnishing the parameters, the new configuration resembles the following:

```
com.axway.mftoi.qlt.url=qlts:0.0.0.0:1303?sslContextParameters=#qltSslContextParameters
com.axway.mftoi.qlt.keystore.path=C:\\OIInstall\\windows\\MFTOI-keystore.jks
com.axway.mftoi.qlt.keystore.password=parola
com.axway.mftoi.qlt.keystore.keyPassword=parola
com.axway.mftoi.qlt.truststore.path=C:\\OIInstall\\windows\\MFTOI-truststore.jks
com.axway.mftoi.qlt.truststore.password=parola
```

When the changes are complete, start the service.

Upgrade MFT Operational Intelligence

The following steps describe how to upgrade MFT Operational Intelligence (MFT OI).

MFT OI consists of two components:

- Axway Decision Insight (ADI): Axway's analytics platform
- MFT OI: The comprehensive application that runs on the platform

An upgrade can impact either ADI or MFT OI. The following sections will detail how to upgrade each component individually



Before upgrading the MFT OI application, you should perform any required ADI platform upgrade step.

Upgrade a node to a new Decision Insight version

Stop the node

For information about how to stop a node, see [Manage a node under Linux](#) or [Manage a node under Windows](#).

Change node settings before the upgrade

In the `NODE_DIR/conf/platform.properties`, add the property `com.systar.aluminium.contexts.autostart=false`. This setting helps prevent data loss the first time you start your node after the upgrade.

Upgrade

To upgrade the node, you need to download the ZIP installer corresponding to the DI version you want to upgrade to.

Navigate to the `NODE_DIR/bin` and launch the `tnd-upgrade` script: `tnd-upgrade --product {ZIP_installer_path}`

Linux example

```
tnd-upgrade.sh --product /myInstallers/DecisionInsight_2.0.0_Product_linux-x86-64_BNXXXXXXXXXX.tar.gz
```

Windows example

```
tnd-upgrade.bat --product S:/myInstallers/DecisionInsight_2.0.0_Product_win-x86-64_BNXXXXXXXXXX.zip
```

Start the node

For information about how to start a node, see [Manage a node under Linux](#) or [Manage a node under Windows](#).

Verify your upgrade

If the node upgrade was performed correctly, the node automatically migrates the database to the new version and creates a checkpoint upon migration.

Also, in the Monitoring & Support area of the MFT-OI in the About section, you can check if the version matches your preferences.

Successful upgrade

Once you have verified that your upgrade is successful, follow these steps:

1. Remove the `com.systar.aluminium.contexts.autostart=false` property from `NODE_DIR/conf/platform.properties`. Your routes will start again in automatic mode (along with the node) if the node is configured this way.
2. Either start your routes manually or restart the node so your routes start with the node if the node is configured this way.
3. Unlock the checkpoint created before the upgrade.

Upgrade MFT OI

To upgrade from MFT OI v1.0 to a newer version, you need the application. The newer version of the application provides updated processing logic, dashboards, and notifications.

Preparatory steps

It is best practice to stop the Data Integration routes in Space Integration to make the upgrade as efficient as possible. This ensures that the platform does not consume new data during the upgrade. You must resume the data integration once the upgrade is completed.

Before starting the upgrade, you have the option to make a manual checkpoint. See https://docs.axway.com/bundle/DecisionInsight_LATEST_allOS_en_HTML5/page/checkpoint.html for details.

Export the properties file before the upgrade

If the values of the properties from Alerts, Integration, and Initializers spaces are personalized, they are not kept after the MFT OI upgrade. It's highly recommended to export them before upgrading the application and then re-import.

The screenshot shows the 'MFT Operational Intelligence' interface. On the left sidebar, the 'Properties' menu item is highlighted with a black arrow. The main panel is titled 'Properties' and has a dropdown menu set to 'Alerts', also indicated by a black arrow. Below this, there is a table of properties with columns for Name, Type, Password, and Value. The properties listed are LogLevelA, LogLevelB, SMTPAddress, SMTPFrom, SMTPPassword, SMTPUsername, SNMP_HOST, and SNMP_PORT. Each property has a corresponding Type dropdown and a Value input field. A 'New property' button is located at the top right of the table.

Name	Type	Password	Value
LogLevelA	Simple	☐	INFO
LogLevelB	Simple	☐	DEBUG
SMTPAddress	From node property	☐	com.axway.mftoi.smtp.address
SMTPFrom	Simple	☐	mftoinotif_noreply@axway.com
SMTPPassword	From node property	☐	com.axway.mftoi.smtp.password
SMTPUsername	From node property	☐	com.axway.mftoi.smtp.username
SNMP_HOST	From node property	☐	com.axway.mftoi.snmp.host
SNMP_PORT	From node property	☐	com.axway.mftoi.snmp.port

The screenshot shows the 'MFT Operational Intelligence' interface. On the left sidebar, the 'Application' menu item is highlighted with a black arrow. The main panel is titled 'Application' and contains fields for Name, Current version, Valid from, and Time format. Below these fields are 'Import' and 'Export' buttons, with the 'Export' button highlighted by a black arrow. The 'Documentation' section provides links to download HTML archives and single HTML files. The 'Past versions' section shows a table with columns for Valid time, Created by, Version, and Actions, but it currently displays 'No past version'.

Name*: MFT Operational Intelligence

Current version*: v1.0.1 [New Version](#)

Valid from: Oct 21, 2022 03:00

Time format: ☐ 12-hour ☒ 24-hour
Toggles between 12-hour (am/pm) and 24-hour format for the time displayed in time machine, time tags and instant parameters in the HTML view.

[Import](#) [Export](#)

Documentation

- Download HTML archive (best for offline browsing)
- Download Single HTML file (best for printing and PDF conversion)

Past versions

Valid time	Created by	Version	Actions
No past version			

To export the properties file, you require the password:

Export application and/or properties

×

Select the spaces you want to export. At least one space must be selected.

✓

Space name

Contains properties

✓

Alerts

✓

✓

Analysis

✓

Classifiers

✓

DynamicInstances

✓

Initializers

✓ (Passphrase required)

✓

Instances

✓

Integration

✓ (Passphrase required)

✓

Model

✓

Rhythms

✓

01. Global Overview

✓

02. Transfer Overview

✓

02.1 Transfer Summary

✓

02.2 Exceptions Summary

✓

02.3 Transfer Details

Download application file

Download properties file

Passphrase:

•••••

Passphrase is used to encrypt the values in the export file.

The same passphrase will be required when importing this file into a deployment.

Confirmation:

•••••

Does not match the passphrase

Close

Preserving the data set in the notifications after the MFT OI upgrade

After the MFT OI upgrade, the data set in the notifications (email address, message subject, and body of the notifications) is lost. To recover them, export the appx, but select **only** the Rhythms space (this is the safest option). This creates a backup for the notifications files.

MFT Operational Intelligence

Administration

Application

Logo

Spaces

Roles

Users

Model

Entities

Diagram

Rhythms

Classifiers

Dashboards

Perspectives

Images

Icon sets

Runtime settings

Notification options

Application

Name*: MFT Operational Intelligence

Current version*: v1.0.20230331

Valid from: Mar 01, 2023 00:00

Time format: 12-hour 24-hour

Toggles between 12-hour

Import Export

Documentation

Download HTML archive (best for offline use)

Download Single HTML file (best for presentation)

Past versions

Valid time

Jan 01, 2023 00:00 - Feb 28, 2023 23:59

Nov 22, 2022 00:00 - Dec 31, 2022 23:59

Sep 20, 2022 00:00 - Nov 21, 2022 23:59

Export application and/or properties

×

Select the spaces you want to export. At least one space must be selected.

Space name

Contains properties

Alerts

✓

Analysis

Classifiers

DynamicInstances

Initializers

✓ (Passphrase required)

Instances

Integration

✓ (Passphrase required)

Model

Rhythms

01. Global Overview

02. Transfer Overview

02.1 Transfer Summary

02.2 Exceptions Summary

02.3 Transfer Details

03. Flow Overview

04. Expected File Overview

04.1 Expected File Summary

Download application file

Download properties file

Selected spaces do not contain any properties

Close

Import the newer version of the application

To upgrade the MFT OI, open the Configuration Application Import. From the Import menu, select **Choose a file to upload** and open the MFT_ProductExtension_(version).appx

In the Version Configuration section, choose 'Create new version from' and set the time at the beginning of the current day(for example, October 01, 2022 00:00).

Import an application and/or properties - Configuration

Application file:

MFT Operational Intelligence (Version_0.19 Upgrade Prep).appx

Change

Properties file:

Choose a file to upload

Version configuration:

Create new version from

Feb 01, 2022 00:00

The cluster will recompute all impacted attributes from the selected date

Override last version

The latest version will be overridden, without creating a new version

The cluster will recompute all impacted attributes from the last version starting date

Version description:

v0.19

Application spaces

Space name

Upgrade_Prep

Continue

If everything is done properly, the following message will be displayed: Application has been successfully imported.

After the MFT OI upgrade, the properties file must be imported from the same page as the export:

Import an application and/or properties - Configuration

Application file: Choose a file to upload

Properties file: Choose a file to upload

Version configuration:

Create new version from Nov 18, 2022 00:00

The cluster will recompute all impacted attributes from the selected date

Override last version

The latest version will be overridden, without creating a new version

The cluster will recompute all impacted attributes from the last version starting date

Version description:

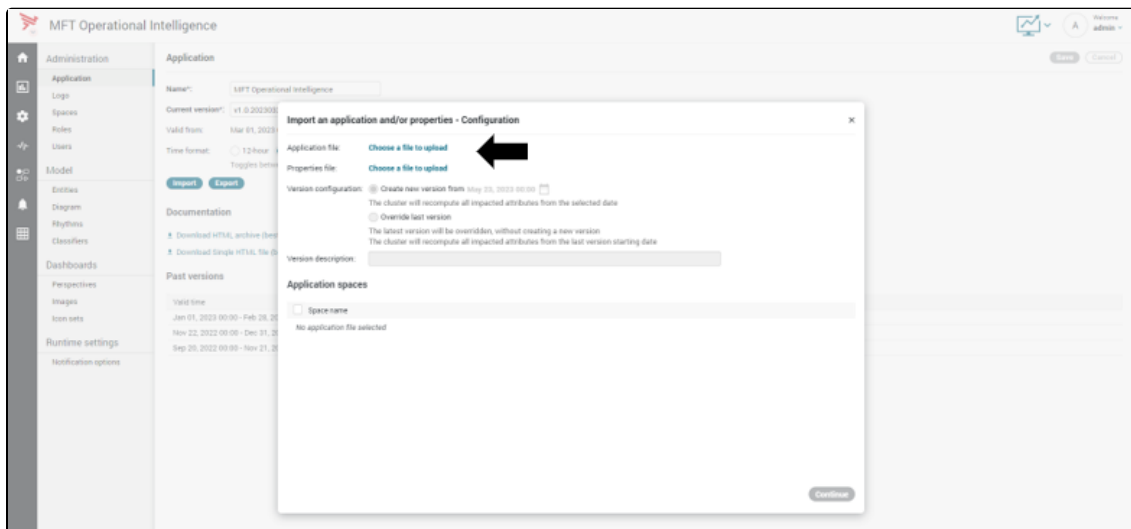
Application spaces

Space name

No application file selected

Continue

The final step is to import the application backup to restore the notification details.



You must start the data integration routes again following the import.

For information about application imports, see the [Decision Insight Documentation](#).

Post upgrade action

IMPORTANT If upgrading MFT Operational Intelligence, it is important to ensure that the Participant to User Role Based Access Control (RBAC) is correctly configured. Please refer directly to [the documentation section](#) in this manual that covers this topic (especially the [Important note for first-time use of Units for customers upgrading from MFT OI V1.0](#)).

Connect SecureTransport and Transfer CFT to MFT OI

Supported products

MFT Operational Intelligence supports the following products and versions:

Product	Supported version	Documentation
Transfer CFT	3.6 SP4	Transfer CFT 3.6 Users Guide
	3.9	Transfer CFT 3.9 User Guide
SecureTransport	5.5-20210729 and higher	SecureTransport 5.5 Getting Started Guide

Once the MFT Operational Intelligence installation is complete, you can connect SecureTransport and Transfer CFT to direct transfer events to MFT OI. MFT OI reads QLT events (the same as in Sentinel) and uses the same port numbers. You configured the QLT port number during the installation and will need it for the next steps.

The default port is 1305, but if you want to use another port, you should apply the changes to both ends of the connection (to MFT OI and the SecureTransport or Transfer CFT server),

Configure SecureTransport

1. Log on to the SecureTransport user interface using the IP address of each SecureTransport instance, for example, <https://10.10.10.10:8444>, where 10.10.10.10 is an example. Your actual addresses will differ.
2. Select the **Setup** icon (second from the top in the left-hand menu bar), and click the Axway Sentinel/DI selection in the submenu.
3. In the Host field, enter the IP address of the Operational Intelligence VM. Do *not* select Use Secure Connection.
4. Click **Test Connection**.

 **SecureTransport** 5.5-20201029 (2695)

**Setup**
Certificates
FTP Settings
AS2 Settings
SSH Settings
Admin Settings
PeSIT Settings
AdHoc Settings
Database Settings
**Axway Sentinel/DI**
Server License
Command Logging
Transfer Logging
Holiday Schedule
Mail Templates
Miscellaneous
ICAP Settings

Axway Sentinel/Decision Insight Events

Configure how SecureTransport sends events to Axway Sentinel or Decision Insight.

Settings
☒ Send Events to Axway Sentinel or Decision Insight Server

Axway Sentinel/Decision Insight
Host*: Test Connection
Port*: Connection successful.
☐ Use Secure Connection
☐ Verify Certificate
☐ Enable FIPS Transfer Mode
☐ Send Heartbeat to Axway Sentinel Every: Minutes ?

Events
Available Event States:

>

>>>

<

<<<

ACKED
AVAILABLE (ST_VAS)
AVAILABLE (XFBTransfer)
CANCELED
DECRYPTED
DECRYPTING
DELETED
ENCRYPTED
ENCRYPTING
ENDED_TO_ACK

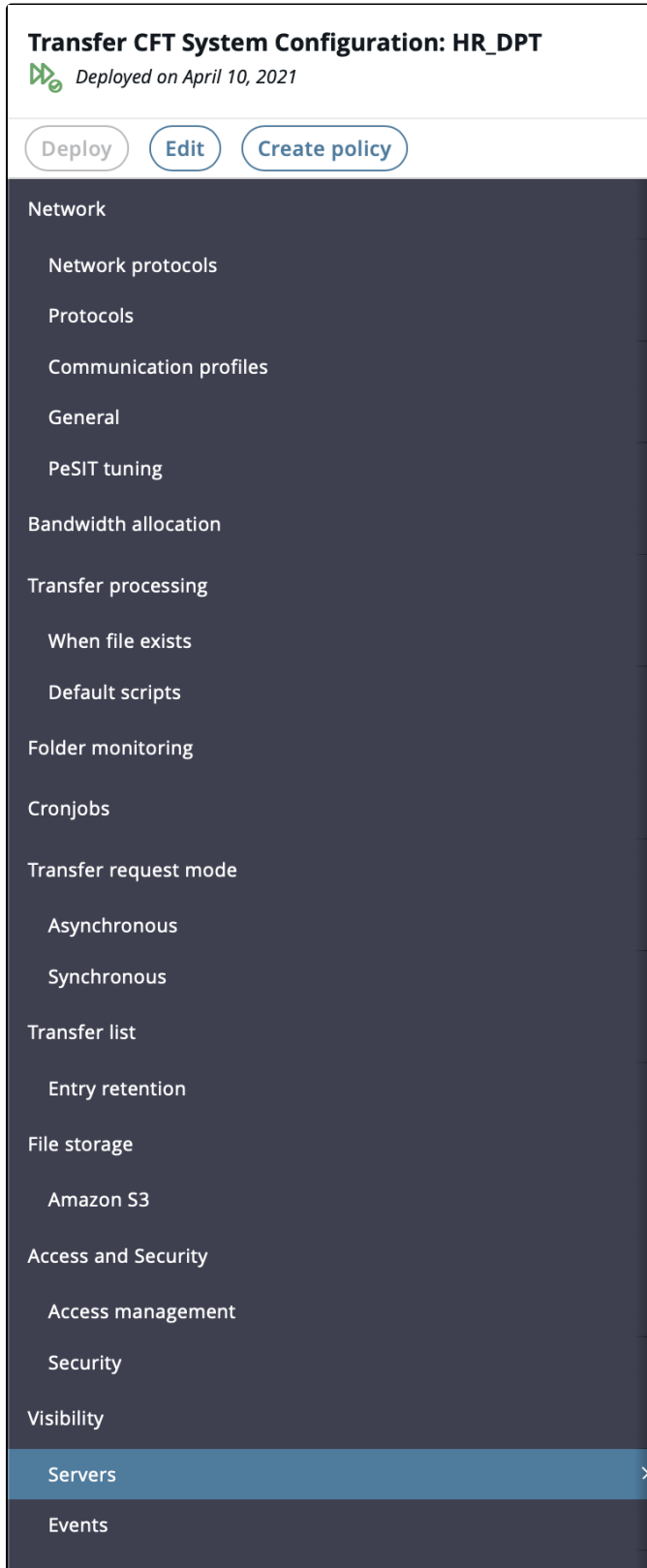
If you receive the "Connection Successful" response, your connection has been set up correctly. Scroll to the bottom of the page and click **Save**:

☐ Maintain link data when Sentinel or Decision Insight reporting is disabled

Save

Configure Transfer CFT

Log on to the Transfer CFT user interface directly or through Flow Manager. This example uses the Flow Manager UI for the Transfer CFT Configuration. From the Transfer CFT configuration interface, select **Visibility > Servers**.



1. Ensure that **Visibility** is enabled.
2. Select **No** for **Enable SSL/TLS**.

3. Select **External** for the server.
4. Enter the OI VM IP address:

5. Deploy the configuration change.

Now that SecureTransports and/or Transfer CFTs are connected to receive events in MFT Operational Intelligence go to **Routes** from **Data Integration, Initializers** space, and perform the following actions:

1. Stop the last two routes that have already started.
2. Start the routes except for 10_RemoveSTServer and 17_RemoveUnit, wait 5 seconds, and then stop them.
3. Restart all these routes except for 10_RemoveSTServer and 17_RemoveUnit. You must wait 5 seconds after the restart. These actions aim to initialize and bring up all the routes.

You should now be able to view SecureTransport and/or Transfer CFT events in MFT Operational Intelligence.

Next

Enable the File Resubmit feature for SecureTransport transfers

MFT Operational Intelligence

Welcome admin ▾

02.3 Transfer Details

LIVE Jul 28, 2022 at 10:14 UTC+03:00

This Cycle ID		Parent Cycle ID		Child Cycle IDs		In Process Duration		Transfer Completion at End	
XFw9pXL6GXywwHvkxGqkr4dKe1YX		XFCNm+akG1aOjzUyMyBUtobyxu5MX		no items		-		410 ms	

Status Success Flow Name 0001-EZEDemoFlow Group Name N Core ID 6b2d94cb-221f-4d14-98e5-5968096b341c Alert 0		Is SSL 0 Is End 1 Exception 0 Creation time Thu 28 Jul 08:27:39 End time Thu 28 Jul 08:37:44		Transfer Summary Transfer summary no items		Exception Summary no items		Inflight no items		Failed no items	
--	--	---	--	--	--	--------------------------------------	--	-----------------------------	--	---------------------------	--

Sender Snapshot :

Orig. Sender ID	ST_RELAY
Application	FlowManagerApplication
Comment	
File Name	0001-test-5c0793bb-bfad-4d41-9a8a-507499ea7b7e.dat
File Path	interfaces/amft-testb-shared-space/default_bu_base_folder\$ST_RELAY\stfs\objects\408f09082432a5f0182433bc532008c\5099ff6d-1657-4
File Size (bytes)	2,063
File Type	B
Is Server	0
Local ID	a348ca43-6691-4c7e-9e82-de46e89e34ff
Participant	partner_xfb_target_1 Unspecified
Product	st-fm-plugin_allbackward
Product Type	SecureTransport
Remote Addr.	192.168.112.11
Retry of Maximum	0 of 5
Return Code	0
Return Message	
Site	0001-EZEDemoFlow_partnerXfbTarget1_sftp_both-st-plugin
Source Application	

Receiver Snapshot :

Final Receiver ID	
Application	
Comment	
File Name	
File Path	
File Size (bytes)	
File Type	
Is Server	
Local ID	
Participant	
Product	
Product Type	
Remote Addr.	
Retry of Maximum	0 of 0
Return Code	
Return Message	
Site	
Target Application	

Sending Transfer History

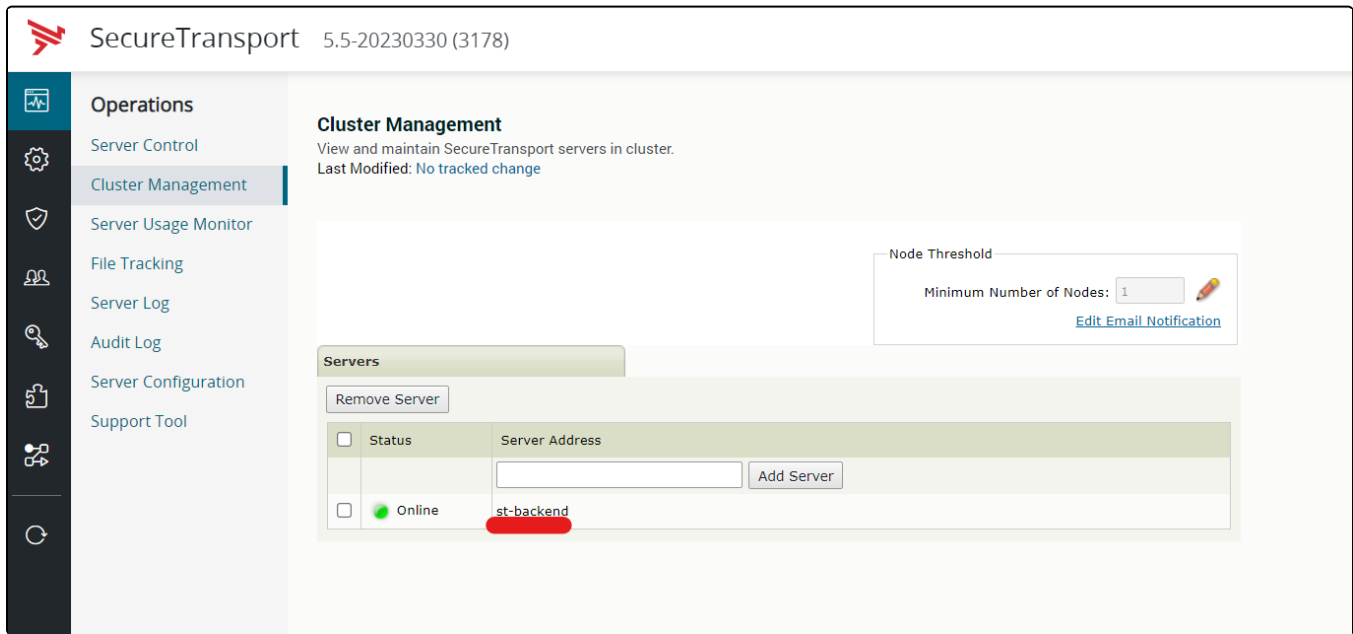
State	Type	Sender ID	State Entered
TO_EXECUTE	SecureTransport	ST_RELAY	08:27:39.655
SENDING	SecureTransport	ST_RELAY	08:27:39.719
SENT	SecureTransport	ST_RELAY	08:27:40.065

Receiving Transfer History

State	Type	Receiver ID	State Entered
-------	------	-------------	---------------

The SecureTransport's ID, which has to be set in units, depends on the type of installation.

For a SecureTransport cluster installation, the ID is displayed in the Cluster Management space from the Operations menu.

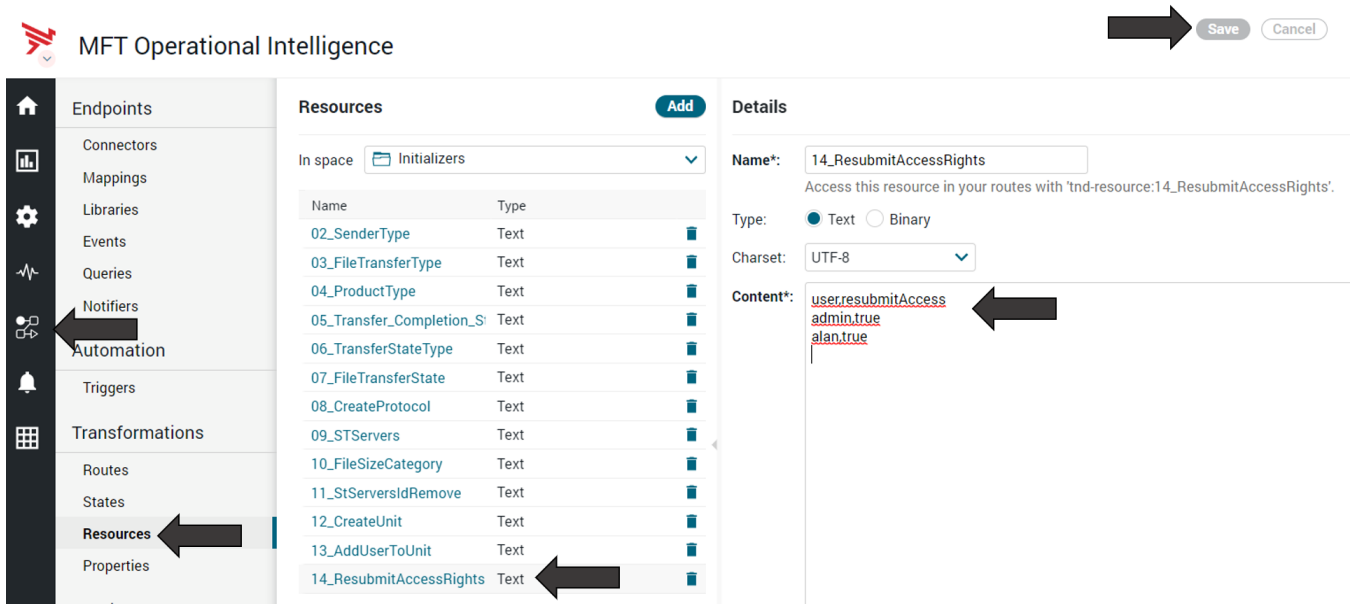


For a standalone installation, the ID is the hostname.

Assign permissions to users to give them access to the file resubmit feature.

1. Navigate to the **Data Integration/Resources/Initializers** space.
2. Click the Resource **14_ResubmitAccessRights**.
3. Under the first line, populate the Content panel in the Details section of the display with the following comma-separated information:
 - User ID
 - Resubmit Access Status (set to **true**)
4. Click **Save**.

*The SecureTransport server ID should be the same as the **Product Name** from the Transfer Summary.



- Enter the target ST Server's Password Encryption key in the lowest entries in the Data Integration/Properties screen.
- The password must be specified in both **Initializers** and **Integration** spaces.



MFT Operational Intelligence

Global Overview | Transfer Summary | Exceptions Summary | Flow Overview | Expected File Overview

Endpoints

- Connectors
- Mappings
- Libraries
- Events
- Notifiers
- Automation
- Triggers
- Transformations
- Routes
- States
- Resources
- Properties**
- Runtime
- Logs

Properties

In space: Initializers

Name	Type	Password	Value
LogLevelA	Simple	☐	INFO
LogLevelB	Simple	☐	DEBUG
ST_SERVER_PASSWORD_ENCRYPTED	Simple	☐	True
ST_SERVER_PASSWORD_ENCRYPTION_K	Simple	☒	*****

- Navigate to the **Data Integration/Routes, Initializers** space.
- Start the Route **09_ConfigureSTServers**.
- Start the Route **21_UpdateResubmitAccessRights**.



MFT Operational Intelligence

Endpoints

- Connectors
- Mappings
- Libraries
- Events
- Queries
- Notifiers
- Automation
- Triggers
- Transformations
- Routes**
- States
- Resources
- Properties
- Runtime
- Logs

Routes

In space: Initializers

Name	State	Actions
01_initGlobal	Stopped	
02_SenderType	Stopped	
03_FileTransferType	Stopped	
04_ProductType	Stopped	
05_Transfer_Completion_Ste	Stopped	
06_TransferStateType	Stopped	
07_FileTransferState	Stopped	
08_CreateProtocol	Stopped	
09_ConfigureSTServers	Stopped	
10_RemoveSTServer	Stopped	
11_FileSizeCategory	Stopped	
12_CreateUnit	Started	
17_RemoveUnit	Stopped	
18_CreateProduct	Stopped	
19_CreateParticipant	Stopped	
20_AddAllParticipants	Started	
21_UpdateResubmitAccessf	Started	
22_UnitButtons	Started	

Next > Time and rhythms

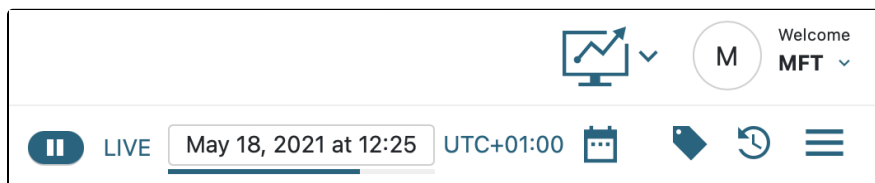
Time and rhythms



One of the most important elements in MFT Operational Intelligence is time. To better understand what you are seeing on the dashboards, read this topic if you read nothing else in this guide.

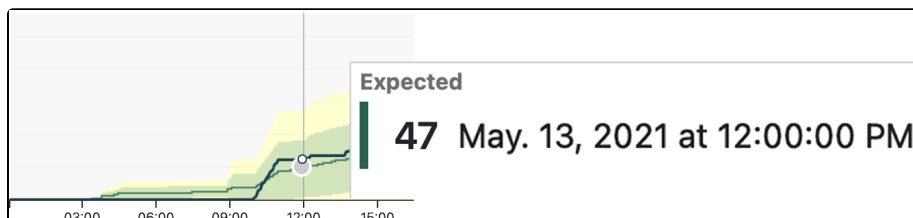
Viewing time and rhythms

MFT OI may be unique to you in how it handles time and information display. The place to see time information on your dashboards is in the upper right-hand corner:

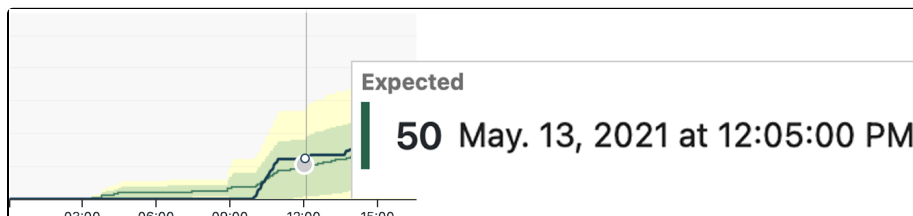


Notice the blue-colored bar below the date and time. That is a completion bar that fills in from left to right. When the bar completes, the dashboard automatically refreshes to display any new data received since the previous display. The time between dashboard updates is the “rhythm” of the dashboard. A rhythm is a normal pace at which data displayed on that dashboard is updated.

Like dashboards, *data* also has a rhythm. If you look at the first of the two charts below, you can see that there were 47 transfers expected today at 12:00.



Now move the cursor one tick forward in time. This creates the image below, where 50 transfers are expected by 12:05.



The time reported advances by 5 minutes for that one step to the right. The *rhythm* of the metric is 5 minutes. In other words, the count of expected items is only updated every 5 minutes.



Because of underlying rhythms, there are always some delays between when events happen in the monitored MFT environment and when the matching information is displayed.

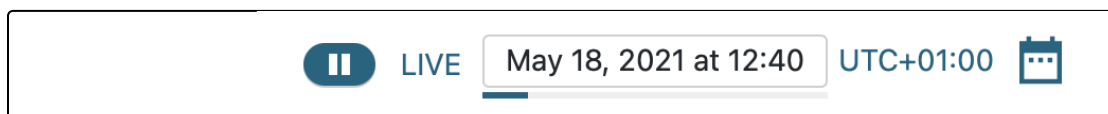
That means a transfer submitted “now” only appears when the dashboard next refreshes.

MFT OI is an analytic tool. It receives data in real time but displays information based on the rhythm defined for each type of data. Real-time display is not required to develop or show analysis, machine learning, or predictions.

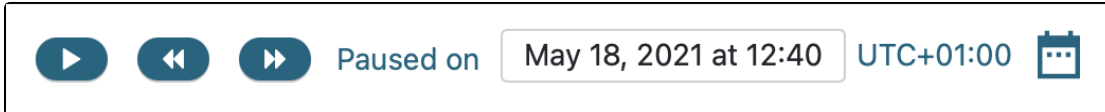
The upside of this approach is the ability to *time travel*. To look at the situation as it occurred.

Time navigation

Using the **time navigation** controls, you can navigate to see the dashboard view at a previous point in time. You can access the controls by clicking the “pause” button, the date and time box, or the calendar icon. Some of the important aspects of time appear in the top right.



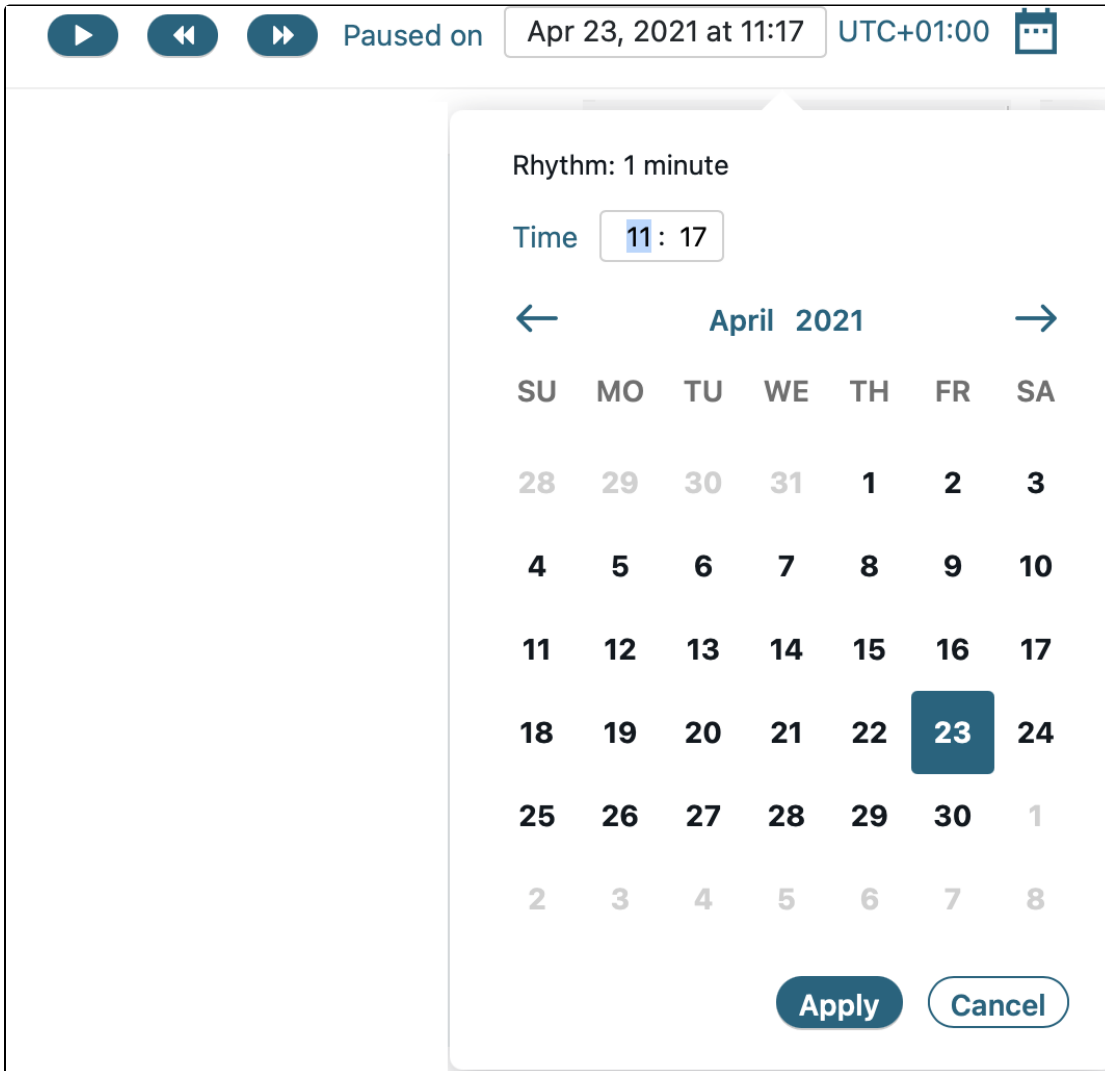
This contains time navigation controls. You can click the pause icon to prevent the dashboard from updating. When paused, OI displays additional controls:



Clicking the rewind and forward icons moves the dashboard forward or back in time by one *rhythm* interval. Click it to see how much time changes; that's one way to find the rhythm of the dashboard you are viewing.

Time replay

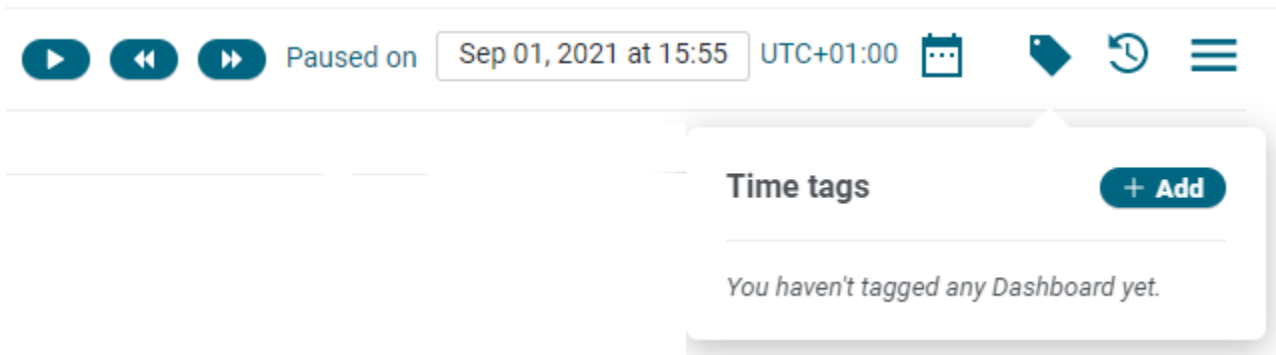
You can also click into the date/time field or the calendar icon to have direct access to time navigation:



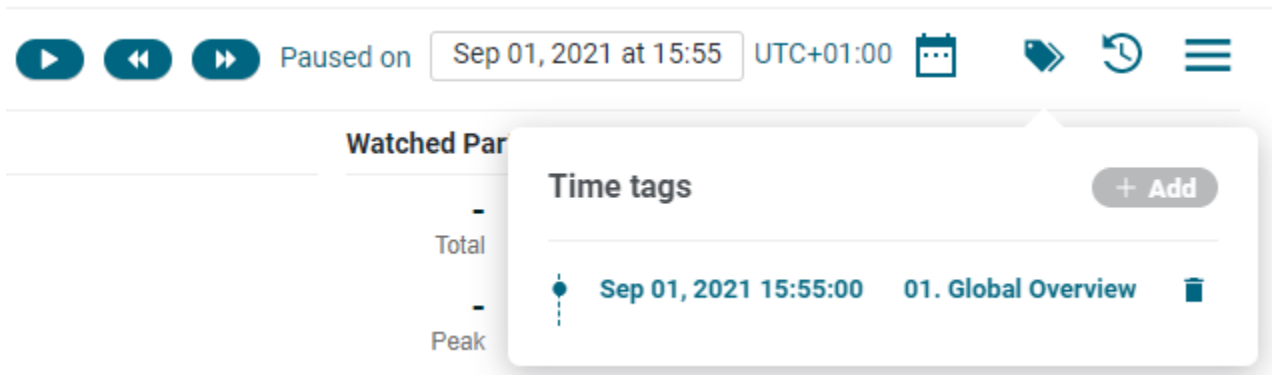
Change the time and date to navigate to a specific point in the past. This causes MFT OI to **replay** the dashboards and transfers exactly as they were at that time. You can also see the rhythm of this dashboard at the top of the dialog box. That's the other way to find the rhythm of the dashboard.

Time tags

If you see something you want to revisit later, you can 'bookmark' the dashboard and time using the **Time tags** function.



Click **+Add** to display the **Time tags**:



There are two separate entries for these **Time tags** - the date and time and the dashboard name. Clicking the date and time takes you to that point in time on the current dashboard, which is useful for looking at another perspective at the same time. To return to the dashboard at that point in time, click the dashboard name, for example, Global Overview.

To delete the Time tag, click the trash can icon.

Thanks for reading this section. It should help you get the most out of MFT Operational Intelligence.

Next

[Plan your first week](#)

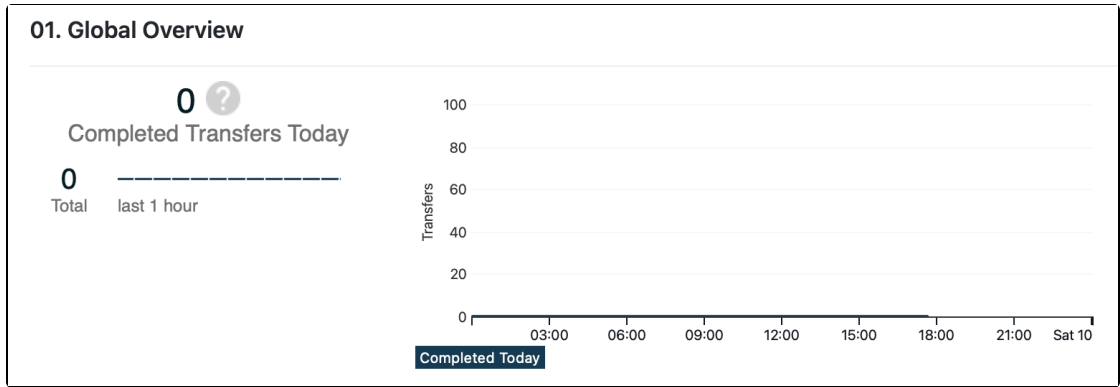
Plan your first week

While some analytics that power MFT Operational Intelligence are available on the first or second day, others need time to develop. The following schedule can help you understand when to expect the features to be visible.

The first day

When MFT OI starts running, it immediately begins learning the activity profile in your environment. That profile will not appear on the first day. While the dashboards on that first day will not show advanced features, you can see a history of transfers and failures on the Transfer Summary, Exception Summary, and Transfer Details.

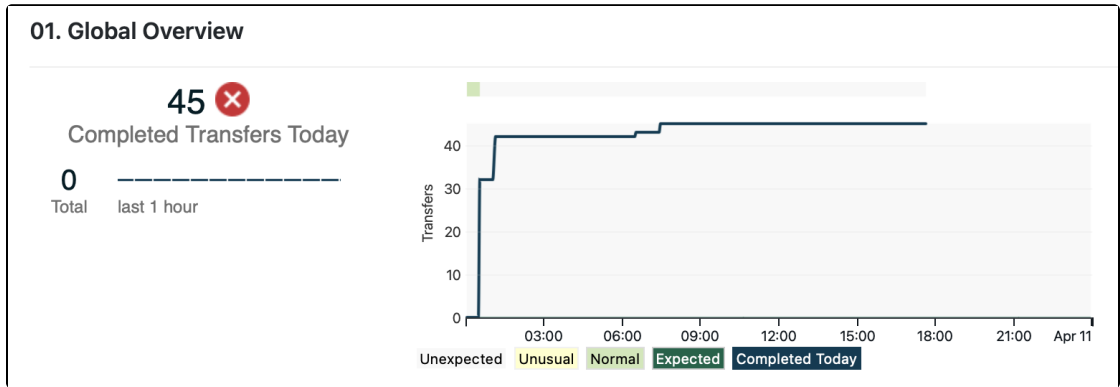
Other dashboards are less interesting. Below is an extract from the Global Overview dashboard on the first day after installation:



In this example, no data has been received to display. Even when data starts to appear, it will lack some of the essential details.

The second day

After 24 hours, the first level of analytics will start to be visible. For comparison, here is the same extract one day after the one above:

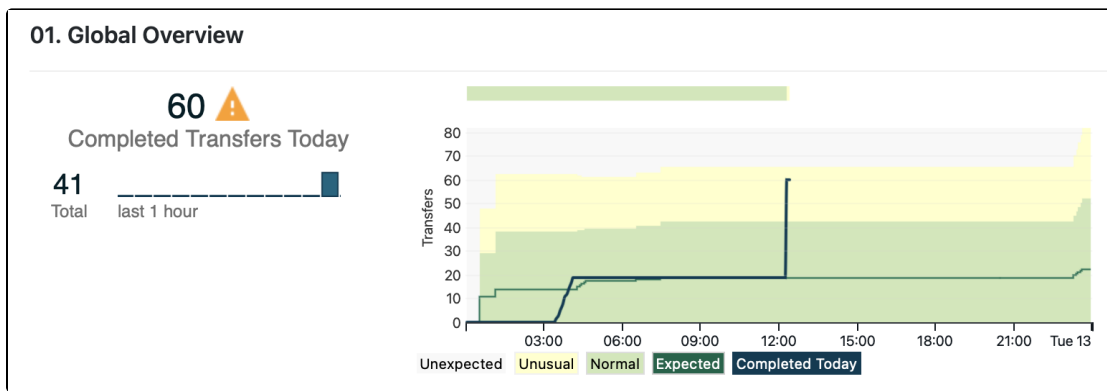


Two significant changes you may notice are:

- The large chart on the right has more items in the legend.
- The large number on the left now displays a red X icon, indicating that 45 is considered “unexpected” based on your history. Since there is not much history to date, the evaluation on this second day is not very accurate.

After the second day

From 48 hours after installation and beyond, the evaluations become increasingly accurate. Here is how that same chart appears on the third day:



This guide explains how to interpret the information in the charts later. But now you know when to expect this analytic to begin working.

The first week

Once data has been arriving at your MFT OI instance, you should begin tailoring its configuration to match your business and operational focus. The first step in that direction involves configuring what MFT OI calls *products*.

What's a product?

MFT OI uses the term *product* to mean an instance of Transfer CFT or SecureTransport. Every instance of Transfer CFT or ST that emits events received by MFT OI will be displayed as a *product* on the Product Summary dashboard and listed in any associated transfers in the Transfer Summary, Exceptions Summary, and Transfer Details. In some environments, there are many instances of Transfer CFT (hundreds to thousands in large installations), and not all are equally important. The same is true if you have large numbers of SecureTransport instances; some may have more significance than others.

The next step in configuring MFT OI during the first week involves configuring participants.

What's a participant?

A participant in MFT OI is any *source* or *destination* of a transfer. An external partner is a participant. An internal application is also a participant. In some cases, relay middleware may also be considered a participant. Every partner, application, or relay mentioned in an event received by MFT OI will be displayed as a *participant* on the Participant Summary dashboard and listed in any associated transfers in the Transfer Summary, Exceptions Summary, and Transfer Details. Some participants (partners or applications) may be more important to the success of your business or MFT operations than others.

You can only set participants configured as *Watched* to monitor for expected file patterns.

Configuring Important Products and Participants

Because some products or participants may be more important than others, MFT OI provides a way to select those for individual attention. MFT OI uses the term *watched* for these selected products and participants.

While selecting participants or products to watch is optional, there are some advantages to that status. Firstly, the Global Overview dashboard displays information about Watched products and participants.

More importantly, detecting and predicting file arrivals only applies to Watched participants. You cannot use the prediction capability if you do not select some participants to be watched.

You should review the section on [Configuring Watched Participants and Watched Products](#) to learn how to select them, and you plan to do that as soon as MFT OI receives data from multiple products and participants.

After the first week

The Watched Participants need a week of activity for file pattern data to be available. You should plan to do this as soon as you can to see the potential value of this feature.

Scanning for and reviewing potential file arrival patterns is described in [Scan files and set window definitions for file arrival pattern detection](#).

Next

[Begin using MFT OI](#)

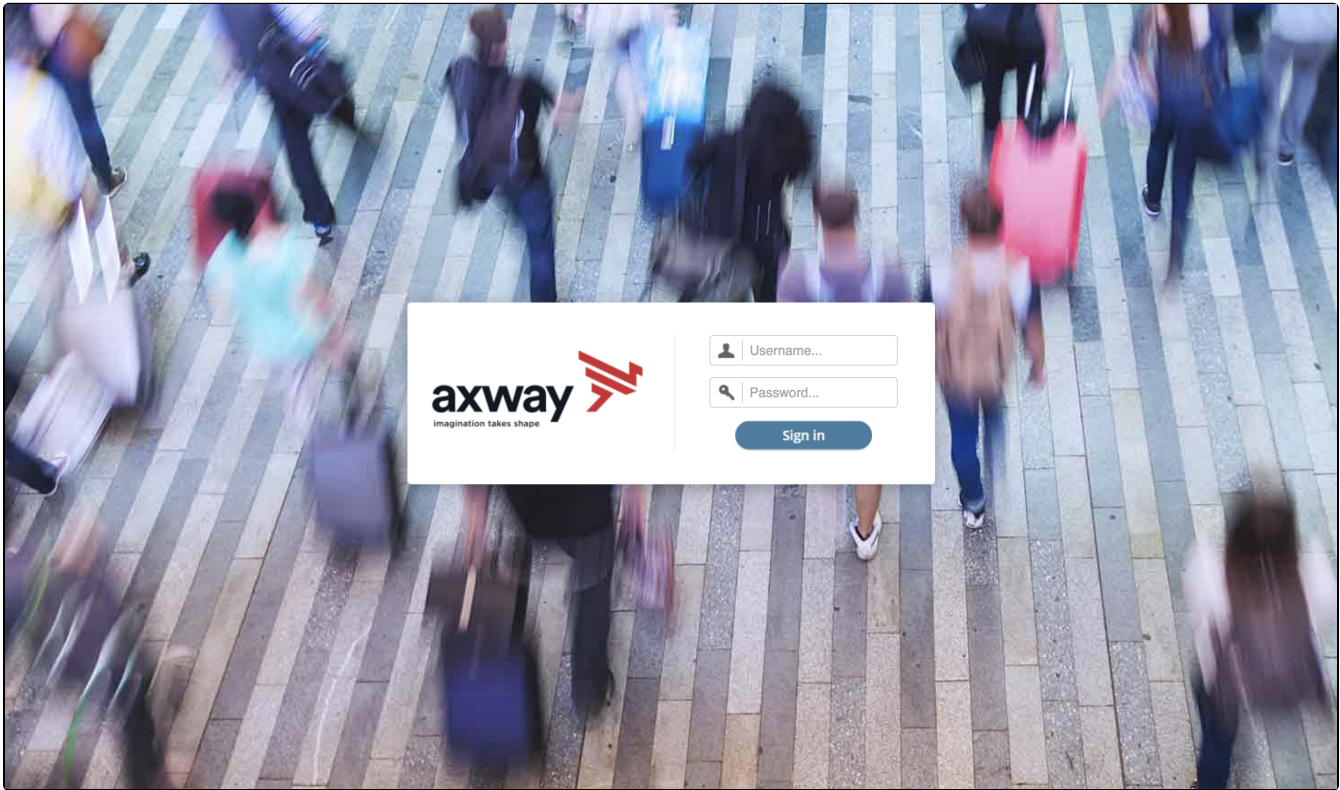
Begin using MFT OI

Once MFT OI is installed and running, you can begin using it. If you used the installation defaults, MFT OI runs on a server you can access with either an IP address or a hostname. If, for example, MFT OI is installed and running on a host named "mftoi," access Operational Intelligence with either of these URLs:

- <http://mftoi:8080/ui/>
- <https://mftoi:8443/ui/>

The port numbers 8080 and 8443 are the defaults, but the installer may have modified these during or after [installation](#). If you cannot connect using the URL and port number, verify with the installer as to the correct name, access method, and port.

MFT OI displays a sign on-screen even if you do not specify the HTML5 interface.

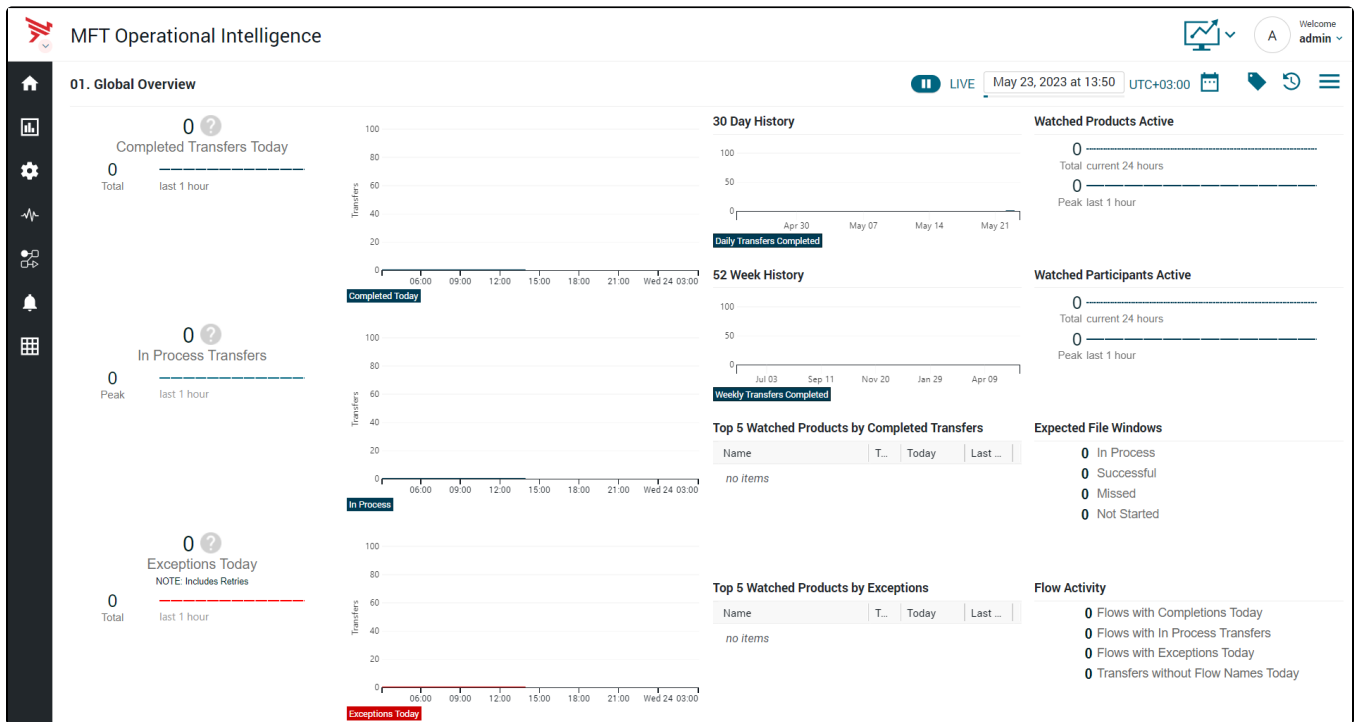


Enter the username and password for MFT OI and click **Sign in**.

Global Overview: The home page

When you sign in, MFT OI opens the Global Overview or, **All Dashboards**, depending on the last state of the application. If you do not see the Global Overview, click the Home icon in the left-hand menu bar. The Global Overview is the application's "home page" that summarizes activity across all monitored MFT systems.

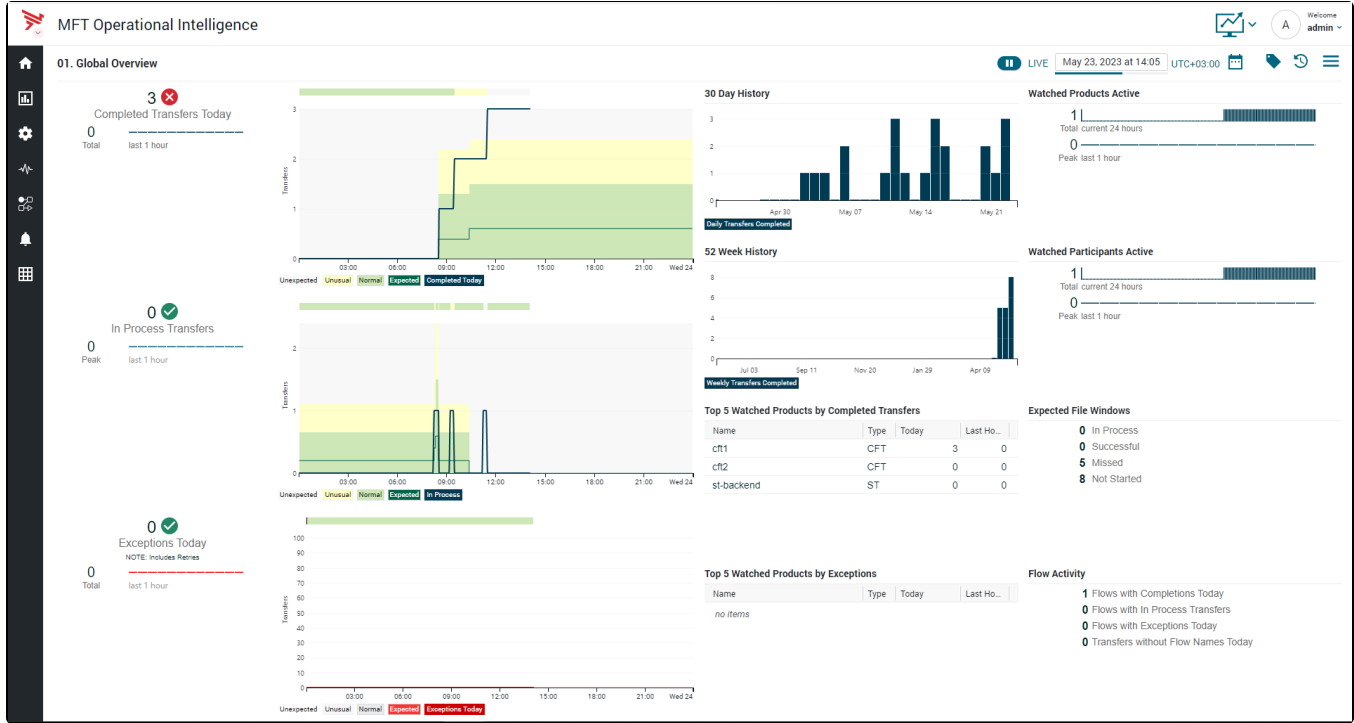
After starting MFT OI, the dashboards do not look like much. The initial screen probably excludes any analytics providing MFT OI value. For example, when data first starts to arrive, the home page may look like this:



When data starts arriving, a limited amount of information is available for display, and more configuration is still required ([Configure Watched Participants and Products](#)).

The dashboard quickly improves. If you have questions about what is shown on the dashboard (that gray icon, for example), please see [the FAQs](#).

You might find it useful to see what a dashboard looks like after Operational Intelligence has had more time to understand your systems. For example:

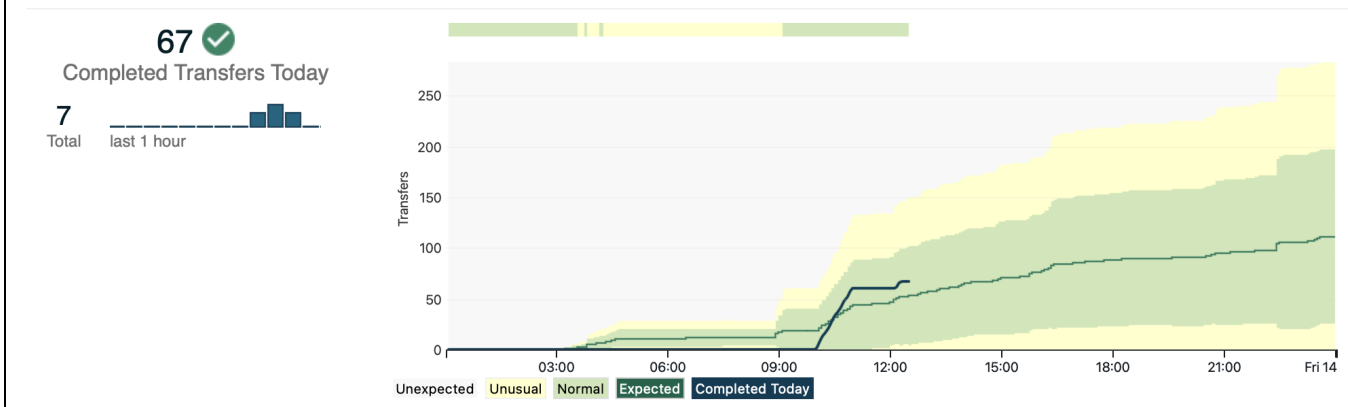


The next sections provide a quick tour of the Global Overview dashboard over time.

Global Overview: Completed Transfers

From the top left, the first section displays transfers that were completed today.

01. Global Overview



The Completed Transfers section deals with transfers that have been **completed** successfully during the current day.



The current day is defined based on the 24-hour day in the configured time zone for MFT OI. See *Why does MFT OI care about date, time, and time zone settings?* in [the FAQs](#).

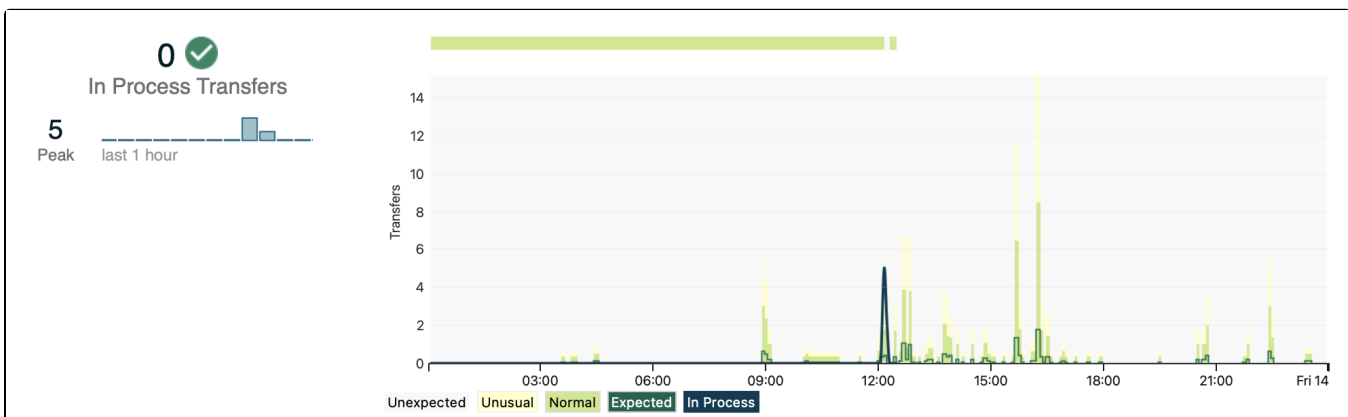
The dashboard displays:

1. The count of transfers completed today (67), with an evaluation icon (see below).
2. The count of transfers completed in the last hour (7), with a spark chart of when those transfers arrived relative to the current hour. This chart is based on a rolling 60 minutes, with each bar representing 5 minutes. In the example above, a total of 7 transfers took place within the last hour as shown by the number to the left of the spark chart.
3. The large chart to the right with a line showing the number of transfers for the current day. This chart is based on a 24-hour day, starting and ending at midnight. This is a cumulative count. The number of transfers will continue to increase all day. The count resets at midnight and starts over with the new day. There is a summary bar across the top of the chart, the main body of the chart, and the legend at the bottom:
 - The summary bar (green, yellow, and then green in the screenshot above) shows how the principal metric – the count of transfers completed today in this case – is evaluated at each data point in the chart so far today.
 - The chart shows the evolution of the count of completed transfers today compared to what was expected and the value ranges for the evaluation icon at each point.
 - The legend:
 - The dark blue line shows the value of the count of completed transactions.
 - The dark green line represents what the count is **expected** to be based on historical analysis
 - The green shaded area covers the range of values that are considered **normal** for a day like today
 - The yellow shaded area shows the range of values that are outside of the expected range. These represent a potential warning-level condition that something **unusual** is happening.
 - Values in the gray area are so far outside of expectations as to be considered **unexpected** and may represent a situation that requires immediate attention.

Evaluation icons, like the green checkmark and the yellow triangle in the screenshot above, are based on the comparison of monitored values and thresholds. In this case, the thresholds are set dynamically using baselines. See *What are baselines?* in [the FAQs](#) for more information on how evaluations are generated.

Global Overview: In Process Transfers

Continue the tour to the section directly below Completed Transfers, the section for In Process Transfers.

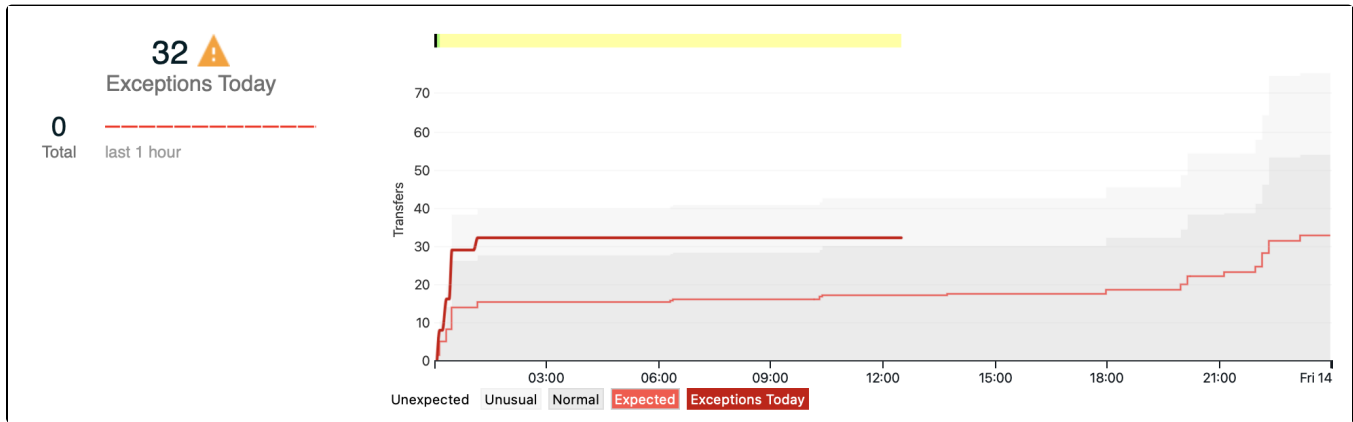


The three parts in this section are similar to the ones in Completed Transfer:

- The count of currently in process, with an evaluation icon. The count is currently 0. Because transfers typically have a short duration, and it may require a number of concurrent transfers to show a value here.
- Below that count is a spark chart for each 5-minute block over the rolling 60 minutes covered by the chart, with each bar representing the count of transfers active at the end of the 5-minute interval. The count to the left of the small chart is the peak number of transfers in process during any interval (that peak is 5 in this example).
- The large chart to the right with the status bar across the top, a line showing the number of transfers concurrently in process during the current day, and the same expected line and shaded areas as you saw for the completed transfers. Also, like the completed transfers chart, this chart is based on a 24-hour day. Unlike completed transfers, this is an *instantaneous* count – sampled at five-minute intervals.

Global Overview: Exceptions Today

Next, look at the last section on the left side of the home page, the one that shows Exceptions Today.

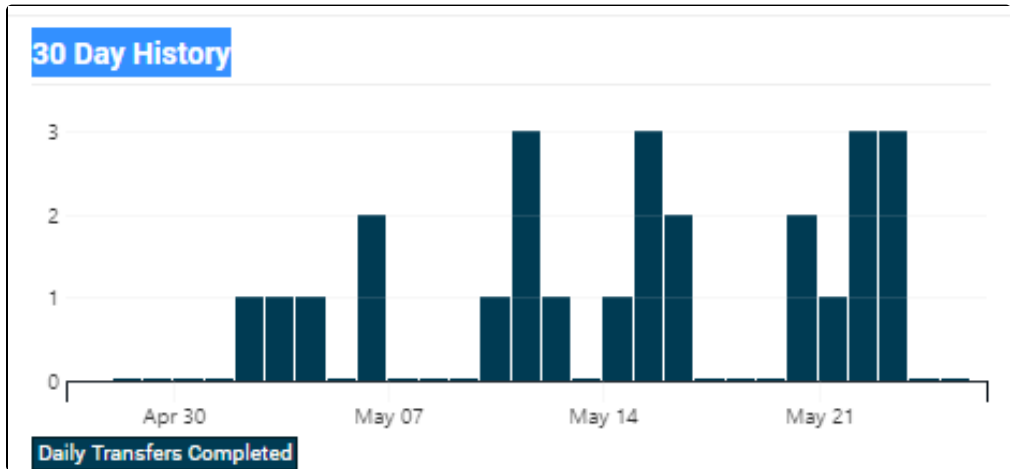


The three parts in this section are similar to the Completed Transfers section, with:

1. The count of transfers in an "exception" status is done for those that either completed abnormally or failed to complete with a normal status and also for every attempt which failed after using the "Resubmit" option.
2. The total count of exceptions reported in the last hour, with a rolling 60-minute spark chart of those exceptions.
3. The large chart shows the status bar, the cumulative number of exceptions for the current day, and the evaluation areas. The expected line and shaded areas are different colors for exceptions in the count of exceptions today.

Global Overview: 30-Day History

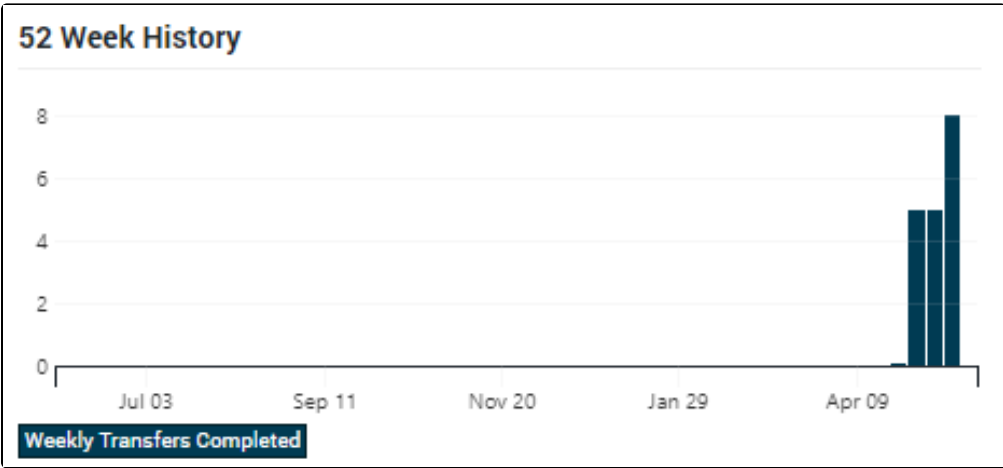
In the center, at the top of the Global Overview dashboard, there is 30 Day History dashboard.



Every bar from this dashboard is showing the number of completed transfers of a day.

Global Overview: 52-Week History

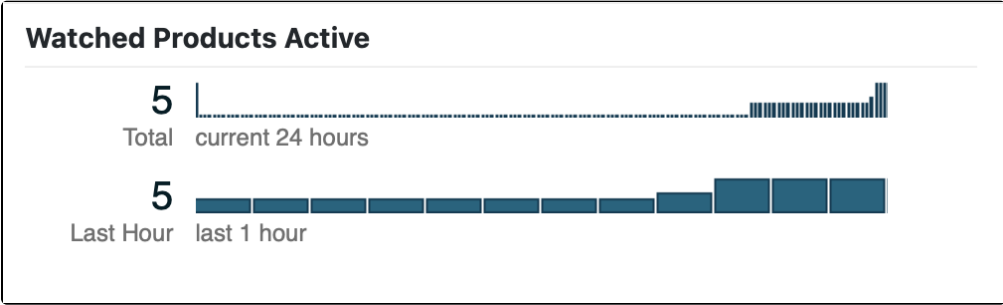
Under 30 Day History dashboard, there is a long-term metric, 52 Week History dashboard.



For this graph, the data is computed once a week, on Sundays. Every bar is showing the sum of the transfers from a week (Monday to Sunday).

Global overview: Watched Products Active

A section for active Watched Products is on the right-top side of the Global Overview dashboard.



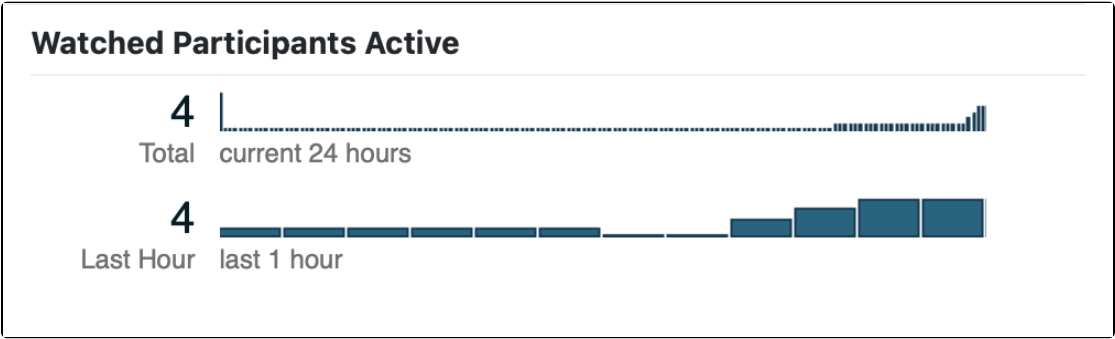
If you don't yet understand watched Products, check *What are Watched Products and Watched Participants?* in [the FAQs](#). If you want to configure some of your product instances to be Watched, see [Configure watched participants and products](#). There are two parts to this portion of the dashboard. Both show the count and a spark chart of Watched Products active. One covers the current 24 hours and the other the current 60 minutes. Both charts have the data point for every 5 minutes during the interval, and new data points are added at the right and crawl to the left.

A product is considered *active* if there has been at least one transfer during the associated interval.

The information in this section is provided as a *yardstick* to see if recent activity and activity today across watch products meet your expectations.

Global Overview: Watched Participants Active

On the right-hand side at the top of the Global Overview dashboard is a section for active Watched Participants.



This information is similar to the Watched Products section but shows the counts of active Participants with at least one transfer during the corresponding interval.

Global Overview: Top 5 Watched Products

In the middle of the Global Overview dashboard is a section for two categories of Top 5 Watched Products.

Top 5 Watched Products by Completed Transfers (only first 5 rows)				
Name	Type	Today	Last Hour	
rh_ghofme2_m-jvr	CFT	52,706	4,226	
VLQONEN	CFT	20,591	2,897	
VLQONEQ	CFT	1,130	93	
ewvdkhl6236.wm.gwf.yywrt	CFT	406	117	
cft1	CFT	57	0	
Top 5 Watched Products by Exceptions				
Name	Type	Today	Last Hour	
VLQONEN	CFT	189	23	
rh_ghofme2_m-jvr	CFT	140	7	
ewvdkhl6236.wm.gwf.yywrt	CFT	18	8	

The top section shows the top 5 Watched Products in terms of transfers completed today. The list also shows the count of completed transfers in the last hour. The second section shows the top 5 Watched Products in terms of the count of failed transfers today, with a column for the exceptions in the last hour.

Global Overview: Window summary

This section of the Global Overview dashboard displays summary information about the Expected File Windows or pattern of file transfers for Watched Participants.

Expected File Windows	
0	In Process
0	Successful
0	Missed
0	Not Started

Global Overview: Flow Activity

The Flow Activity is the last section with information on the Global Overview dashboard.

Flow Activity

171

Flows with Completions Today

0

Flows with In Process Transfers

2

Flows with Exceptions Today

76,409

Transfers without Flow Names Today

Dashboards

When you sign in to MFT OI and click the Dashboards button, the dashboard list displays containing thumbnails of all available dashboards.

This is a page that displays all available dashboards, split into Main Dashboards and Supporting Dashboards. For example:

MFT Operational Intelligence

Global Overview

Transfer Summary

Exceptions Summary

Flow Overview

Expected File Overview

Participant Overview

All dashboards

Main dashboards

Supporting dashboards

01. Global Overview

02. Transfer Overview

03. Flow Overview

04. Expected File Overview

05. Participant Overview

06. Product Overview

02.1 Transfer Summary

02.2 Exceptions Summary

02.3 Transfer Details

04.1 Expected File Summ...

05.1 Participant Summary

06.1 Product Summary

30. Configuration Data

97. Units

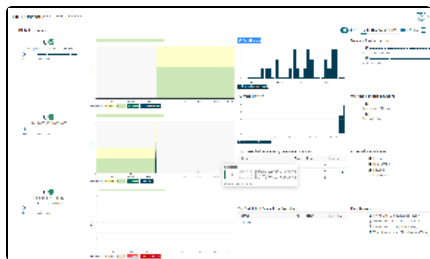
98. Undefined Products

99. Navigation Header

The following sections describe the various dashboards.

Key dashboards

Global Overview – Described in the previous section.



Transfer Overview – Lists the transfers from a certain period of time and filters them by sender and receiver side but also by other attributes.

02. Transfer Overview

Participants

Flow Overview - Lists the various flows (when Flow Manager is deployed) that transfer activity has followed.

03. Flow Overview

Participants

Expected File Overview – The primary display for information on expected file transfer patterns. *Expected File Overview* gives a view of all *Expected File Windows* for all *Watched Participants* based on their status from "In Process" to "Not Yet Started". As of Week 2 and beyond, this dashboard has more detail with *Watched Participants* configured and *Windows* defined.

04. Expected File Overview

Participants

Participants

Participants

Participant Overview - Provides an overview of the various Participants detected in the MFT activity, split between two tables of whether you have defined the Participant as Watched or Unwatched.

05. Participant Overview

Product Overview - Provides an overview of the various Products detected in the MFT activity, split between two tables of whether you have defined the Product as Watched or Unwatched, with the ability to switch the Watched status.

06. Product Overview

Supporting dashboards

Transfer Summary – Lists recent transfers with the ability to filter the list; see *Viewing transfer activity* below.

02.1 Transfer Summary

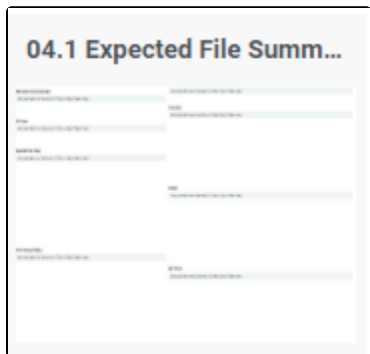
Exceptions Summary – Lists all recent transfers classified as exceptions; see the details in the *Something went wrong? - Exception summary* section.

02.2 Exceptions Summary

Transfer Details – Links to another dashboard, such as Transfer Summary or Exceptions Summary, display details about the most recent event received for the selected transfer as well as a history of previous events. See *Transfer Details - Viewing transfer details* below.



Expected File Summary – this is the detailed display for information on expected file transfer performance for a particular Watched Participant. See 6.8 for an explanation of the *Expected File Summary*. There is more detail on this as of Week 2 and beyond.



Participant Summary – displays an overview of daily activity by a "participant." See 6.7 for an explanation of the term *participant*.



Product Summary – Summarizes the activity for any connected ST or Transfer CFT instance. See 6.6 for more information about *products*.



Configuration Data- The space where a unit and an ST product can be added, edited, or deleted.

30. Configuration Data

Category	Item	Value	Unit	Notes
General	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
Configuration	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
	Unit	100	100	

Units - Displays a unit where only the allowed ones can be added from all participants, users and products listed.

97. Units

Category	Item	Value	Unit	Notes
General	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
Configuration	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
	Unit	100	100	

Undefined Products – This dashboard is only here to display debug information should MFT OI receive an event from a server for which it cannot determine the Product type. For now, you can safely ignore it.

98. Undefined Products

Category	Item	Value	Unit	Notes
General	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
Configuration	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
	Unit	100	100	

Navigation Header– This is a special-purpose dashboard that is not really a dashboard at all. More about that later. For now, you can safely ignore it.

99. Navigation Header

Category	Item	Value	Unit	Notes
General	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
Configuration	Unit	100	100	
	Unit	100	100	
	Unit	100	100	
	Unit	100	100	

The menu bar

There are two versions of the menu bar: one for normal users and one for users with admin rights. If you are using the default "admin" user to access MFT Operational Intelligence, the menu options for admins display.

The admin-level menu looks like this:



Where the icons have the following functions:



Home – Displays the home page dashboard, Global Overview



Dashboards – Opens the list of dashboards as shown in the previous section



Configuration – Admin function to configure the MFT OI application.



Monitoring & Support – An admin section that can be useful in debugging issues.



Data Integration – Yet another admin function focused on managing data from QLT events.



Notifications – This is the section used to create and manage alerts.



Windows – A section for administrators to configure file arrival windows.

Transfer Summary - Viewing transfer activity

The transfer summary dashboard is a good place to start monitoring transfers:

At the top, you can use several filters to narrow the list of transfers displayed. Depending upon the field type in the filter, you will be given choices for refining your search. For example, to define a filter on Filename to find any file that contains "ACH":

02.1 Transfer Summary

For Search Period=Last 1 hours

For:

Filters:

One important note on filters. Once you define a filter, the color of the filter changes to indicate you have made a selection. However, making a selection does not apply the filter. To do that, you need to click Submit. Until you click the Submit button, it will be highlighted as displayed below:

For:

Filters:

That dark color is your only indication that the Submit button has not been clicked and the filter has not been applied. Click Submit to accept your filter definition(s). After you click Submit, MFT OI displays the selected filters:

For:

Filters:

Navigating to transfer details

The information displayed in the Transfer Summary dashboard is just that, a summary. The fields visible are:

Selected Transfers (only first 500 rows)														
	Flow Name	Creation time	Direction	Filename	Receiver ID	Sender ID	Participant	State	Status	Protocol	Location	Product Type	Product Name	File Size (bytes)
Details	(none)	Tue 18 Jan 11:11:34.820	S	EZYKZVZV3UQ44341.N3307045	VX55713F	V517619Q	Participant	SENT	Success	P81T_H9_E	M088204A	CFT	Product Name	5,120
Details	(none)	Tue 18 Jan 11:11:34.816	S	EZYKZVZV3UQ44341.N3307045	VV51316F	V517619Q	Participant	SENT	Success	P81T_H9_E	M088204A	CFT	Product Name	5,120
Details	(none)	Tue 18 Jan 11:11:34.813	S	EZYKZVZV3UQ44341.N3307045	V8016MGP	V517619Q	Participant	SENT	Success	(none)	M088204A	CFT	Product Name	0

To see more details about an individual transfer, click on the [Details](#) field. This link will take you to the **Transfer Details** dashboard.



The last field, Cycle ID, is also a link to the **Transfer Details** dashboard. Clicking the Cycle ID opens the Transfer Details dashboard in a new browser tab. This leaves your search filters in the summary dashboard while allowing you to inspect the details of the transfer.

- To see more transfers related to the transfer's flow, click the **Flow Name** field. Even if there is no flow name (as in this example), there is still a hyperlink (none) for the field. This link will take you to the **Flow Overview** dashboard filtered by the name of the Flow selected.
- To see more details about the Participant of this individual transfer, click on the Participant field. This link takes you to the **Participant Summary** dashboard for the respective Participant.
- To see more details about the Product of this individual transfer, click on the Product Name field. This link takes you to the **Product Summary** dashboard for the respective Product.

Transfer Details - viewing the details of a selected transfer

The information displayed in the Transfer Details contains more information about a transfer than the summary dashboard.

If you go directly from All dashboards on Transfer Details, no information is visible at this moment.

Drilling down from the Transfer Summary displays the sender and receiver information.


MFT Operational Intelligence










Welcome

admin


LIVE


May 29, 2023 at 11:25


UTC+03:00

This Cycle ID

MFTOI-225_2+TR001/B01

Parent Cycle ID

no items

Child Cycle IDs

no items

In Process Duration

-

Transfer Completion at End

-

Status

Success

Flow Name

0022-EZESimpleFlo

Group Name

N

Core ID

Alert

0

Is SSL

1

Is End

0

Exception

0

Creation time

Mon 29 May 08:14:19

End time

Mon 29 May 08:24:19

Transfer Summary

Exception Summary

Inflight

Failed

Transfer Summary

no items

no items

no items

Sender Snapshot

:

Orig. Sender ID

Linking

Application Comment

File Name

CycleLink.txt

File Path

CycleLink.txt

File Size (bytes)

23,456,789

File Type

Is Server

Local ID

Participant

Awkay Unspecified

Product

- : st-backend

Product Type

SecureTransport

Remote Addr.

Retry of Maximum

0 of 3

Return Code

Return Message

Site

Source Application

Receiver Snapshot

:

Final Receiver ID

Linking

Application Comment

File Name

CycleLink.txt

File Path

CycleLink.txt

File Size (bytes)

23,456,789

File Type

Is Server

Local ID

Participant

Awkay Unspecified

Product

- : st-backend

Product Type

SecureTransport

Remote Addr.

Retry of Maximum

0 of 3

Return Code

Return Message

Site

Target Application

Sending Transfer History

State	Type	Sender ID	State Entered
RECEIVING	SecureTransport	-	08:14:19.829
SENDING	SecureTransport	-	08:14:19.833
SENT	SecureTransport	-	08:14:19.834
POST_PROC	SecureTransport	-	08:14:19.835

Receiving Transfer History

State	Type	Receiver ID	State Entered
TO_EXECUTE	SecureTransport	-	08:14:19.828
RECEIVED	SecureTransport	-	08:14:19.830
POST_PROC	SecureTransport	-	08:14:19.831

The top area contains the most recent information about the transfer. This information is mostly from the last event received by MFT OI. Some of the information displayed is held over from previous events rather than allowing the partial information provided by some events to remove details as the transfer moves toward completion.

The central area is divided into two sections where information about the sender and the receiver is visible.

The bottom table provides a historical trace of events seen during the progress of the transfer on both sender and receiver. These two sections are the best areas to verify that MFT OI displays the information you expect from the file transfers it monitors.

Exception Summary - Something went wrong?

MFT OI also reports information on transfers it considers to be an exception. What is an exception? Please check [the FAQs](#). Any exceptions seen for the current day are summarized in the Exceptions Summary:

02.2 Exceptions Summary | Search Period: Last 1 hours

For: Search Period

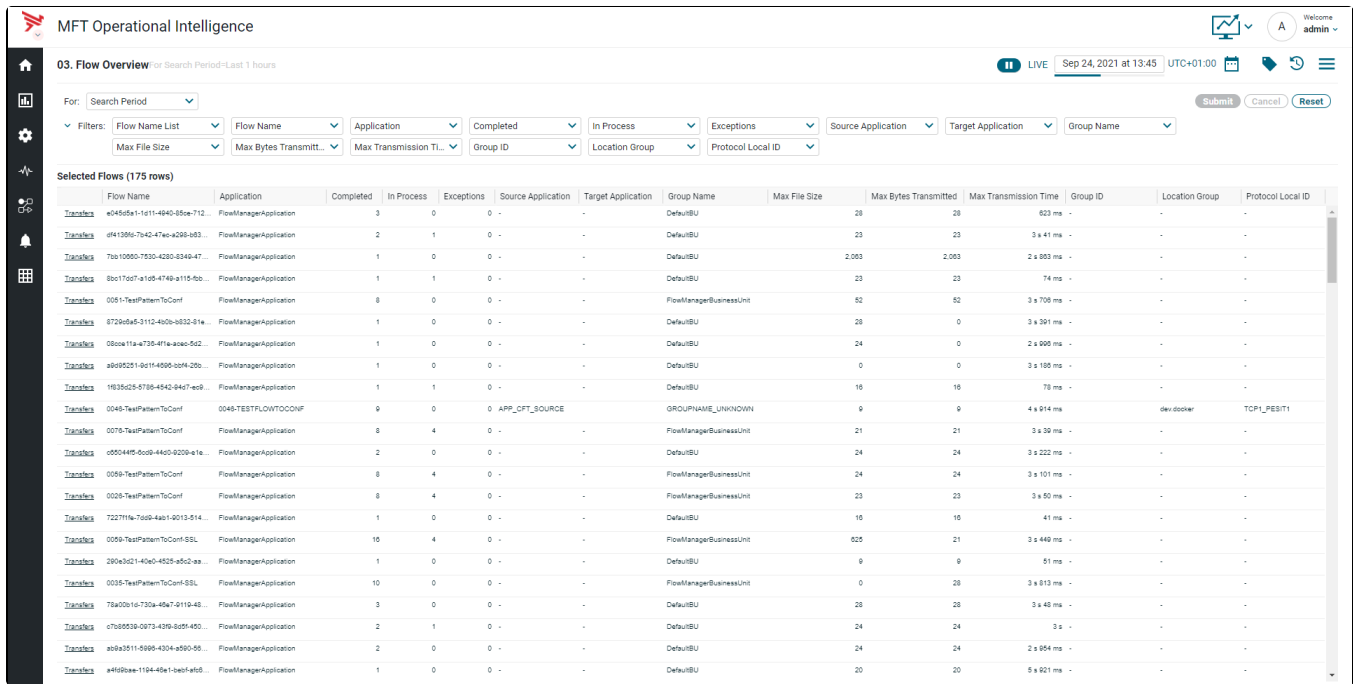
Filters:
 Creation Time
 Filename
 Direction
 Receiver ID
 Flow Name
 Sender ID
 State
 Protocol
 Location
 Participant
 Product Name
 Product Type
 Cycle ID
 Transfer Summary

	Flow Name	Creation time	Direction	Filename	Receiver ID	Sender ID	Participant	State	Protocol	Location	Product Type	Product Name	File Size (bytes)	Cycle ID
Details	(local)	Fri 24 Sep 12:56:54.940	S	YLD1.KR051911.320502.23285320	N870750S	V517654V	VADICEC	CANCELED	P81T_H9_E	PBM/VSPBF	CFT	VACQENIN	88.094	XF46zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:56:54.945	S	YLD1.KR051911.320502.23285320	UB489171	YRRKRHBQV	VADICEC	CANCELED	(none)	PBM/VSPBF	CFT	VACQENIN	0	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:56:54.217	S	YCR1.BNF#B861.T254Z4VU.N175...	N870750Q	V517659F	P81T_H9_E	CANCELED	P81T_H9_E	M080452	CFT	VACQENIN	84.992	XF54uPwCnK1mX7c3ZF8P8j0v
Details	(local)	Fri 24 Sep 12:45:00.889	S	YCR1.BNF#B861.T254Z4VU.N175...	N870750Q	V517659F	P81T_H9_E	CANCELED	P81T_H9_E	M080452	CFT	VACQENIN	84.992	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:45:46.587	S	YJR1.EOU#RQI2.Q3910X5L.O395...	N870737R	V517654V	P81T_H9_E	CANCELED	P81T_H9_E	PBM/VSPBF	CFT	VACQENIN	84.992	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:42:26.560	S	ODAI.COQZP811.V368A29	P518542H	V517654Z	ZFA8	CANCELED	(none)	M08042J	CFT	evvdb0238.sm.pdf...	0	XF31d0ZQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:42:26.574	S	ODAI.COQZP811.V368A29	P518542H	V517654Z	ZFA8	CANCELED	(none)	M08042J	CFT	evvdb0238.sm.pdf...	0	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:36:17.261	S	jflu.com/gfswden/mrnfms/bss/EJ...	R579653Q	V517619Q	P81T_H9_E	CANCELED	P81T_H9_E	M080204A	CFT	ch_photom2.mzv	0	XF44uPwCnK1mX7c3ZF8P8j0v
Details	(local)	Fri 24 Sep 12:32:30.407	S	YLD1.KR051911.320502.23284204	N870750S	V517654V	VADICEC	CANCELED	P81T_H9_E	PBM/VSPBF	CFT	VACQENIN	88.094	XF54uPwCnK1mX7c3ZF8P8j0v
Details	(local)	Fri 24 Sep 12:32:30.475	S	YLD1.KR051911.320502.23284204	UB489171	YRRKRHBQV	VADICEC	CANCELED	(none)	PBM/VSPBF	CFT	VACQENIN	0	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:32:54.745	S	jflu.com/gfswden/mrnfms/bss/EJ...	R579653Q	V517619Q	P81T_H9_E	CANCELED	P81T_H9_E	M080204A	CFT	ch_photom2.mzv	0	XFMCQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:31:07.175	S	YCR1.BNF#B861.T254Z4VU.N175...	N870750Q	V517659F	P81T_H9_E	CANCELED	P81T_H9_E	M080452	CFT	VACQENIN	84.992	XF31d0ZQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:12:56.142	S	ODAI.COQZP811.V368A29	P518542H	V517654Z	ZFA8	CANCELED	(none)	M08042J	CFT	evvdb0238.sm.pdf...	0	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:12:42.202	S	YLD1.KR051911.320502.23284275	N870750S	V517654V	VADICEC	CANCELED	P81T_H9_E	PBM/VSPBF	CFT	VACQENIN	88.094	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:12:42.280	S	YLD1.KR051911.320502.23284275	UB489171	YRRKRHBQV	VADICEC	CANCELED	(none)	PBM/VSPBF	CFT	VACQENIN	0	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:12:38.433	S	ODAI.COQZP811.V368A29	P518542H	V517654Z	ZFA8	CANCELED	(none)	M08042J	CFT	evvdb0238.sm.pdf...	0	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:06:03.573	S	YJR1.ENH589ZM.BQ10804J.N175...	N870737R	V517654V	P81T_H9_E	CANCELED	P81T_H9_E	PBM/VSPBF	CFT	VACQENIN	84.992	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 12:07:49.073	S	YCR1.BNF#B861.T254Z4VU.N175...	N870750Q	V517659F	VADICEC	CANCELED	P81T_H9_E	M080452	CFT	VACQENIN	84.992	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 11:52:52.597	S	YCR1.BFE#E111.V494Z29	ONWH2	V517659F	VADICEC	CANCELED	CFT	M080452	CFT	VACQENIN	364.544	XF26zGwZtEzcQvWzOmDmZSoUy
Details	(local)	Fri 24 Sep 11:44:19.067	S	YCR1.BFE#E111.V494Z29	ONWH2	V517659F	VADICEC	CANCELED	CFT	M080452	CFT	VACQENIN	196.609	XF26zGwZtEzcQvWzOmDmZSoUy

Navigation from this summary works the same as the Transfer Summary dashboard by clicking on Details or Cycle ID to reach the Transfer Details, the Flow name to reach Flow Overview, Participant for Participant Overview, and Product for Product Summary.

Flow Overview

The Product Overview dashboard provides a summary of all the transfer activity today from the perspective of the Flow the transfer followed:



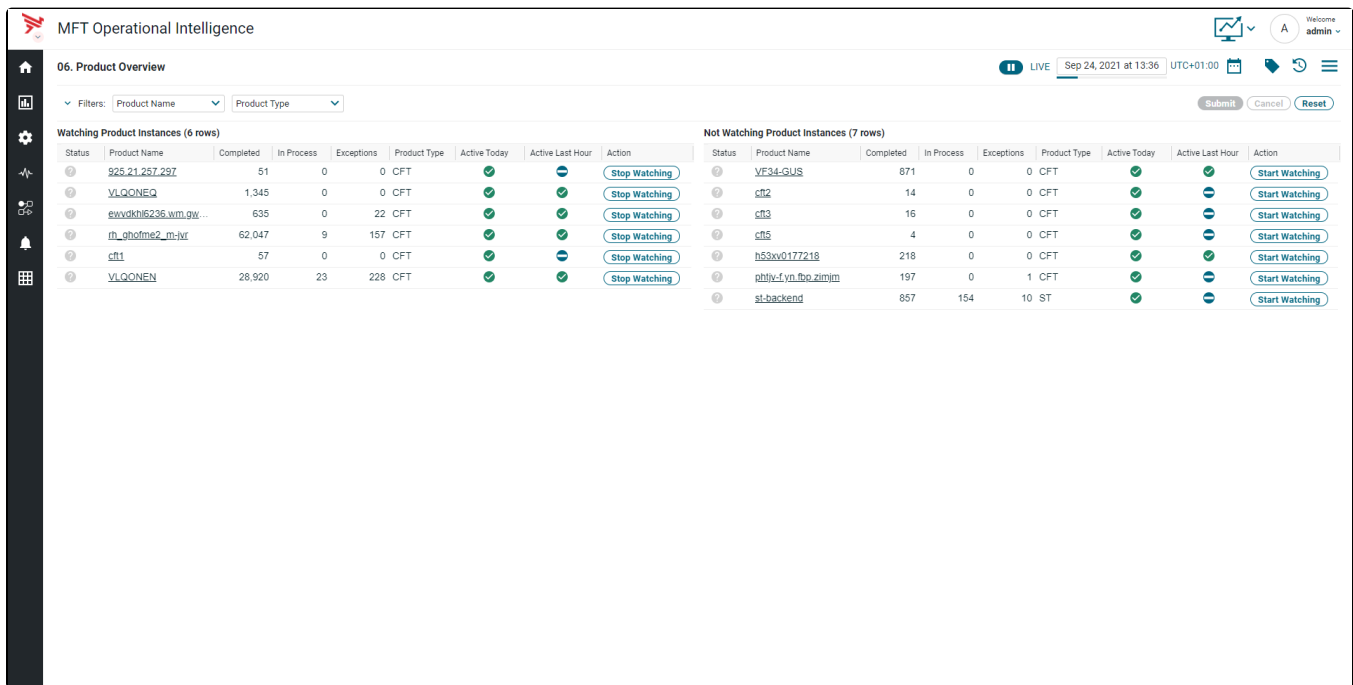
Like the Transfer Summary and Exception Summary dashboards, the Flow Overview dashboard also allows filtering the list of flows.

This does not change the counts of the transfers in the columns displayed, only the flows which match the filter criteria. For example, you could search for those flows with no activity today or more than a certain level of activity today.

Additionally, you can drill down to the list of transfers for a selected flow by clicking the **Transfers** column, which redirects to the Transfer Summary dashboard with the selected Flow Name selected in the filtering.

Product Overview screen

The Product Overview dashboard provides a summary of all the products of both Watched and Unwatched categorization.



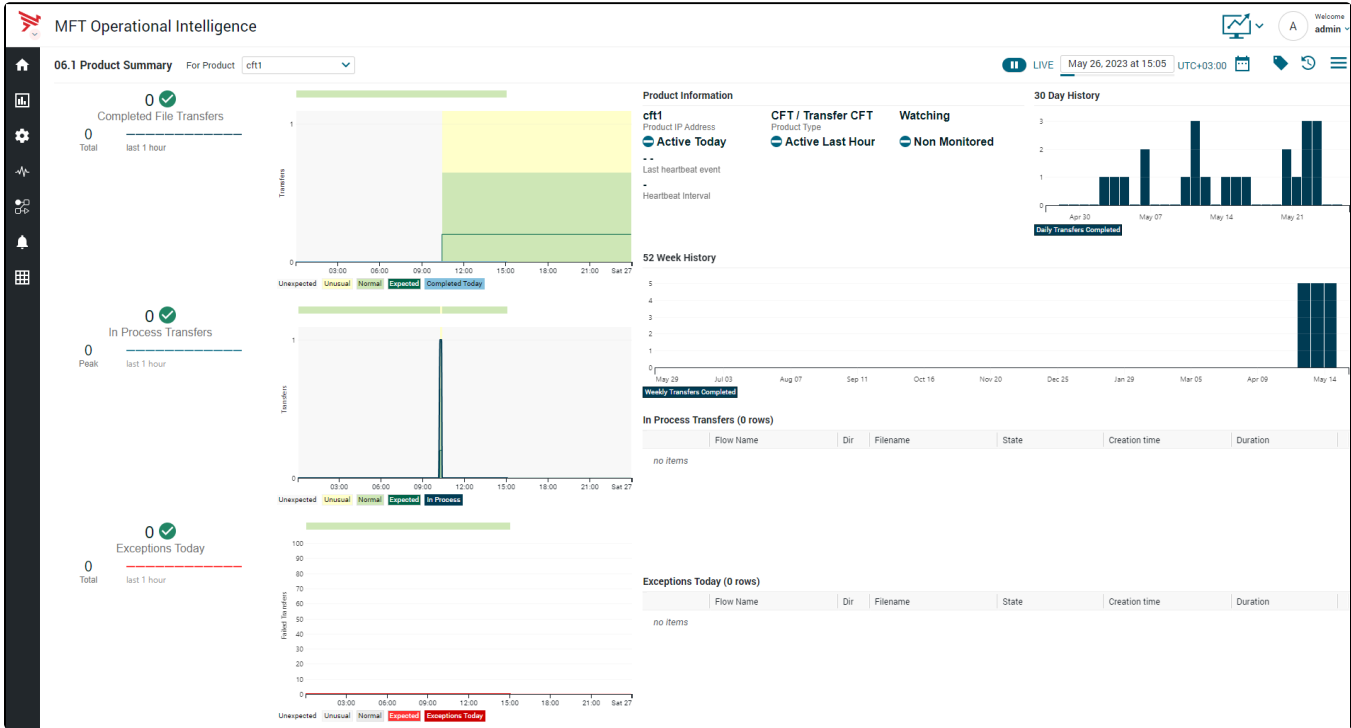
It provides summary information of:

- Global Status of the Product
- Product Name (IP Address)
- Number of Transfers Completed Today (successfully)
- Number of Transfers In Process
- Number of Transfers in Exception
- Indicator of Transfer Activity Today
- Indicator of Transfer Activity in the last hour
- Action button (to Stop or Start Watching the Product)

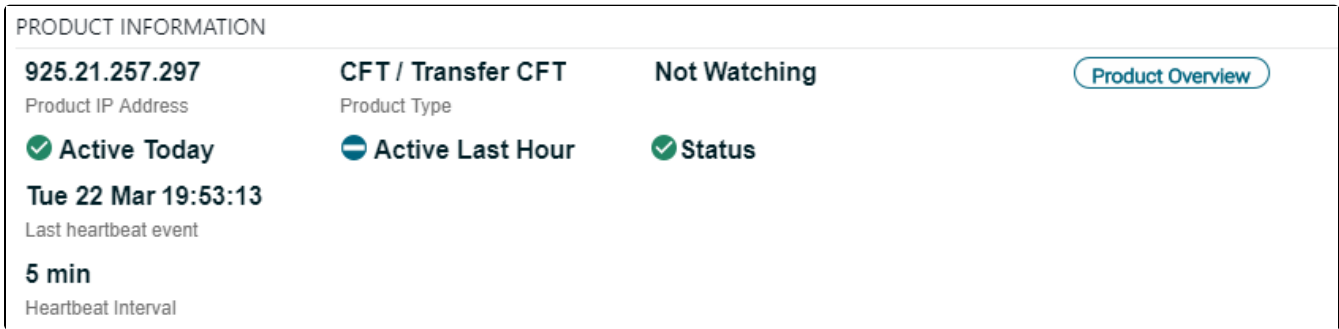
To drill down into more information about a specific Product, click on the Product Name to be redirected to the Product Summary dashboard.

Product Summary screen

The product summary dashboard resembles the Global Overview, with the information reported restricted to a single Transfer CFT or SecureTransport instance.



The sections on the left-hand side are conceptually the same as those on the Global Overview. On the top middle side, the section contains information on the product instance, configuration, activity and heartbeat information:



The pieces of information that may not be obvious are:

Watching/Not Watching - this refers to the status of the product as being *watched* or *not watched*. See the FAQs for more information on Watched Products.

The icons next to **Active Today** and **Active last hour** indicate if MFT OI has seen activity for the selected product in the matching time range using the following indicators:

	Activity Detected
	No Activity Detected

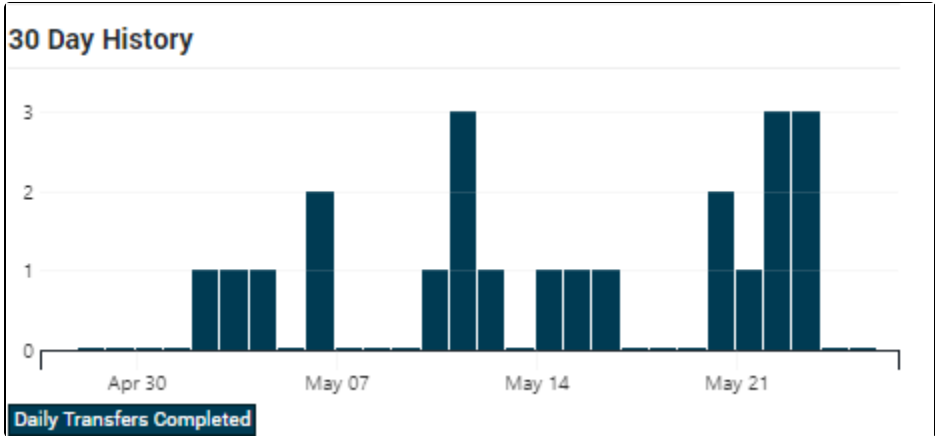
Heartbeat Information

- Last heartbeat event - The time of the last received heartbeat event
- Heartbeat interval - The expected interval between heartbeats

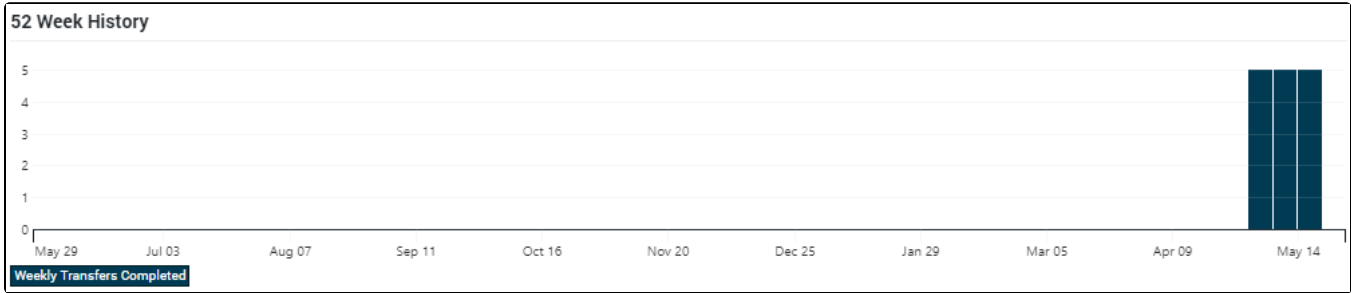
Status - An evaluation of the status of the product based on the heartbeat data using the following indicators:

	Not Monitored - No heartbeat has been detected
	Recently Active - A heartbeat has been received within the expected interval
	Warning - A heartbeat has not been received within a one-minute threshold after the expected interval
	Unreachable - When a heartbeat has not been received after the expected interval and one-minute threshold

In the **30-Day History** dashboard, from the top-right side of the page, the vertical bars indicate the number of daily completed transfers of the selected product.



The dashboard below, **52 Weeks History**, summarizes the selected product's weekly completed transfers (Monday to Sunday).



Participant Overview screen

The Participant Overview dashboard provides a summary of all the Participants of both Watched and Unwatched categorization.

MFT Operational Intelligence

05. Participant Overview

LIVE Sep 24, 2021 at 13:44 UTC+01:00

Watched Participants

Status	Participant	Completed	In Process	Exceptions	Windows In Process	Successful Windows	Missed Windows	Windows Not Started	Active Today	Active Last Hour
?	partner_xfb_target_1	94	68	3	0	0	0	0	0	0
?	axway	299	0	0	0	2	2	0	0	0
?	LVR	10	0	0	0	0	0	0	0	0
?	BJAAVQA	2	0	0	0	0	0	0	0	0
?	gksv	36	0	0	0	0	0	0	0	0
?	rbx	0	0	0	0	0	0	0	0	0
?	CHYLRRG	14	0	0	0	0	0	0	0	0

Unwatched Participants

Status	Participant	Completed	In Process	Exceptions	Active Today	Active last hour
?	BCQKEQE	0	0	0	0	0
?	CQBV	8	0	0	0	0
?	GWBFRXG	54	0	0	0	0
?	IYREDBS	14	0	0	0	0
?	J2196	12	0	0	0	0
?	LQ00IO	0	0	0	0	0
?	LVRLP3FB	31	0	0	0	0
?	LVRLOE	1,853	5	31	0	0
?	LVRLOEFB	46	0	1	0	0
?	LVRLOH	7	0	2	0	0
?	LVRLOM4V	56	0	0	0	0
?	LVRLOQ	16	0	0	0	0
?	LVRLOQR	3,992	3	17	0	0
?	LVRLOQS	17	0	0	0	0

It provides summary information of:

- Global Status of the Participant
- Participant Name (code)
- Number of Transfers Completed Today (successfully)
- Number of Transfers In Process
- Number of Transfers in Exception
- Indicator of Transfer Activity Today
- Indicator of Transfer Activity in the last hour

The configuration to watch or stop watching a Participant is within the Windows Template Configuration, available via the left menu bar.

MFT Operational Intelligence

Window templates

Participant settings

Participant settings

Scan settings

Window settings

Total participants : 80 (no participants selected)

Start watching Stop watching

ID	Name	Status	Actions
☐ aew_fvtszan			Start watching
☐ aew_kixhy			Start watching
☐ aew_kixhyvo			Start watching
☐ aew_uk_agbgzzi			Start watching
☐ app_at_source			Start watching
☐ app_at_ssl			Start watching
☐ axway		WATCHED	Stop watching
☐ BCQKEQE			Start watching
☐ BJAAVQA		WATCHED	Stop watching
☐ CHYLRRG		WATCHED	Stop watching
☐ CQBV			Start watching
☐ dop_fvtszan			Start watching
☐ dop_kixhy			Start watching
☐ dop_kixhyvo			Start watching
☐ dop_uk_agbgz			Start watching
☐ dop_uk_agbgzzi			Start watching
☐ gksv		WATCHED	Stop watching
☐ GWBFRXG			Start watching
☐ IYREDBS			Start watching
☐ J2196			Start watching
☐ l6_mpagv			Start watching
☐ LQ00IO			Start watching
☐ LVR		WATCHED	Stop watching
☐ LVRLP3FB			Start watching
☐ LVRLOE			Start watching
☐ LVRLOEFB			Start watching
☐ LVRLOH			Start watching
☐ LVRLOM4V			Start watching
☐ LVRLOQ			Start watching
☐ LVRLOQR			Start watching
☐ LVRLOQS			Start watching

For Watched Participants 4 additional columns related to the expected file pattern Windows are visible:

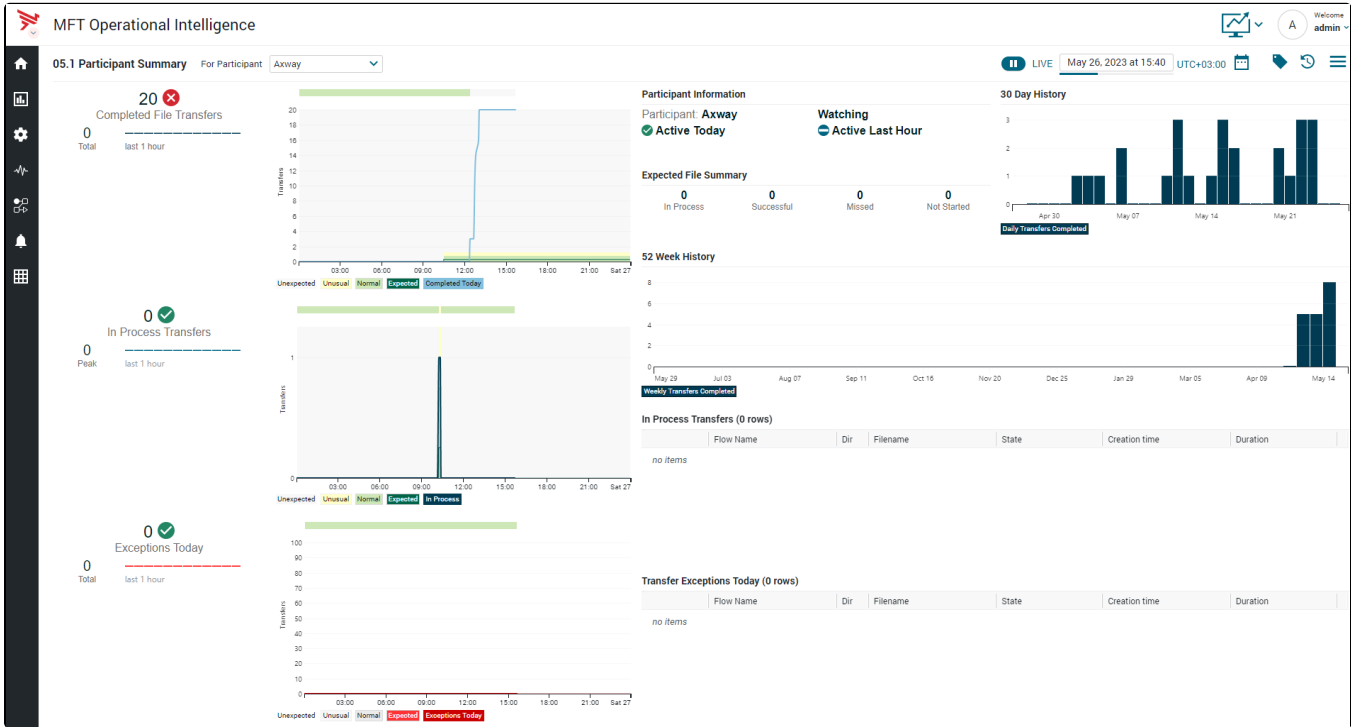
- Number of Windows In Process (0 or 1)
- Number of Successful Windows Today

- Number of Missed Windows Today
- Number of Windows Not Started Today

To drill down into more information about a specific Participant, click the participant's name to be redirected to the **Participant Summary** dashboard.

Participant Summary screen

The participant summary dashboard resembles the Global Overview and Product Summary dashboards, with the information reported in this case restricted to a single endpoint or application.



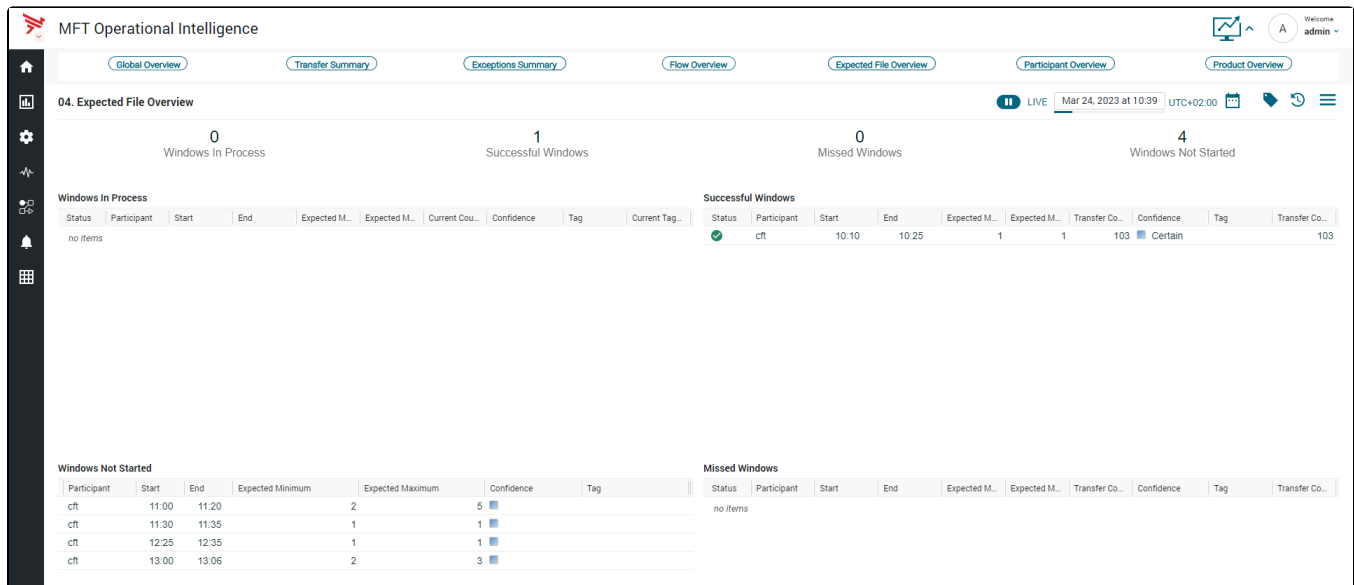
All the sections in this dashboard are similar to the Product Summary above, with one exception, Expected File Summary pagelet:

Expected File Summary			
1 In Process	2 Successful	0 Missed	3 Not Started

The **Window Summary** section consolidates information about the status of Expected File Windows for this participant today. For more information, see the description for Expected File Windows Today, below, and [the FAQs](#) for an explanation about File Windows. In this example, three expected file windows have not yet started; one is currently being monitored, and 2 previous windows were successfully passed.

Expected File Overview screen

The Expected File Overview dashboard provides a summary of all the Expected File Window patterns of transfer activity defined for the current day for all Watched Participants.



The dashboard is split into five sections:

- Summary of the Windows Today
- Windows In Process
- Windows Not Started
- Successful Windows
- Missed Windows

The summary provides the totals for Windows today.

The remaining four sections provide, when applicable:

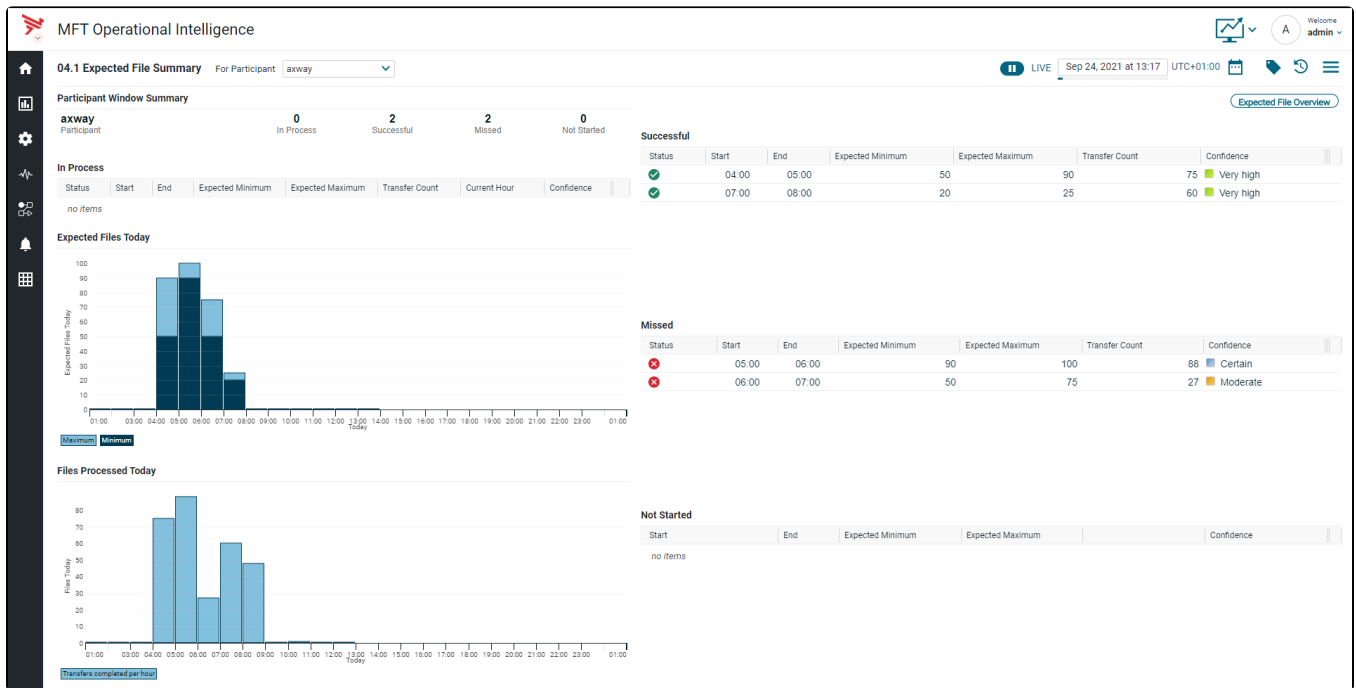
- Status
- Participant
- Start/End time range of the window
- Expected Minimum successful file transfers during the Window
- Expected Maximum successful file transfers during the Window
- Current / Transfer Count
- Confidence (only In Process or completed Windows have a visible Confidence label)
- Tag- an alpha-numeric text string to check for the arrival (or otherwise) of a specifically named file either with a full or substring match. **NOTE** it is case insensitive.
- Current Tag Count

To drill down to investigate a Window, click on the Participant to redirect to the Expected File Summary dashboard.

Expected File Summary - What are the expected file transfer patterns for a specific Watched Participant today

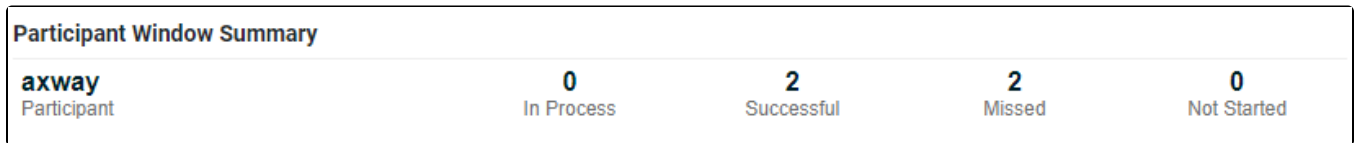
The concept of Expected Files has the potential to be one of the most useful aspects of MFT OI. The value comes from the fact that every MFT operation has some files that are critical for either functional or business success. MFT OI has a built-in function to help you identify and monitor those important files. The process that detects patterns is documented in the [Scan files and set window definitions for file arrival pattern detection](#) section. The Expected File Windows Today dashboard tracks current activity and compares those results to the expected files.

This dashboard focuses on the selected participant and the status of expected file windows for the current day.



Let's look through the sections of this dashboard one at a time.

Participant Window Summary



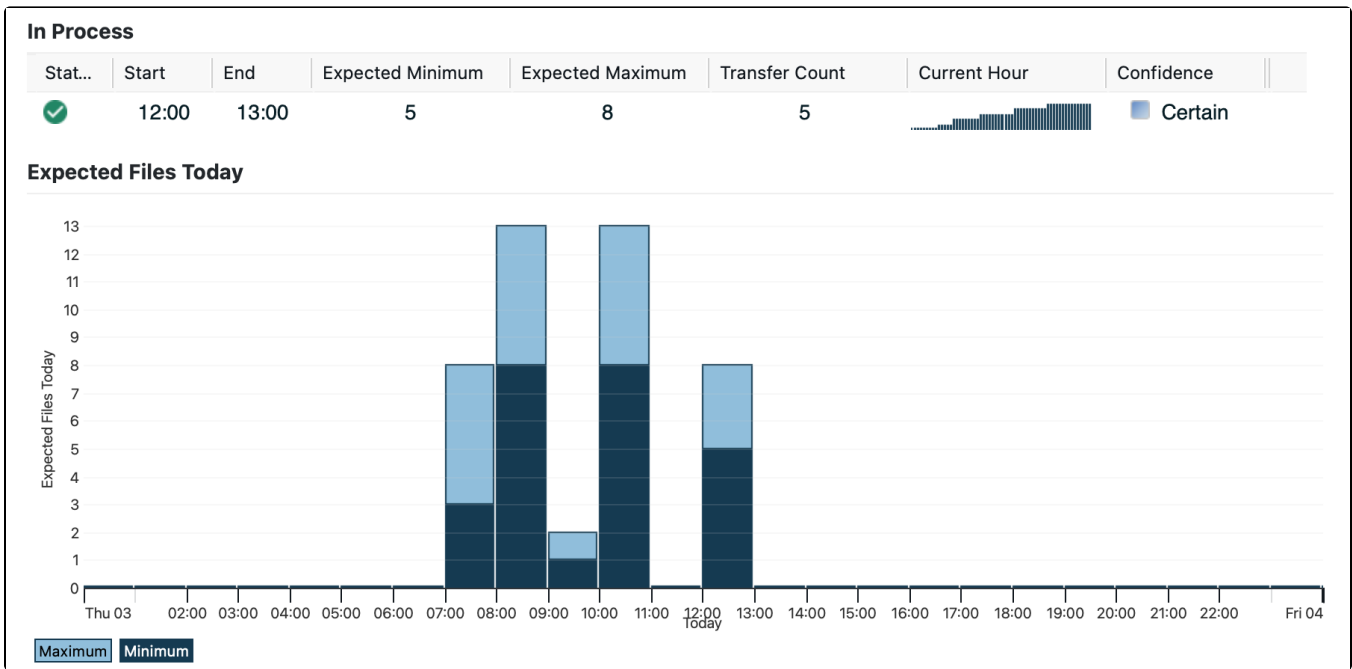
This section summarizes the activity shown on the rest of the dashboard. The section displays:

- The name of the selected participant (axway)
- The count of windows where the monitoring of file counts is **In Process** (0)
- The count of windows where the comparison of files received and files expected passed as **Successful** (2)
- The count of windows where the comparison of files received and files expected **Missed** expectations (2)
- The count of windows for which the monitoring of file counts as **Not Started** (0)



To Configure Windows select the left menu button  to take you to the **Windows Template** interface.

In Process / Expected Files Today - Monitoring in Process



When there is an active check-in process, the two sections of In Process and Expected Files Today work together. A window is *in process* if the current time is between the start and end times defined for the window.

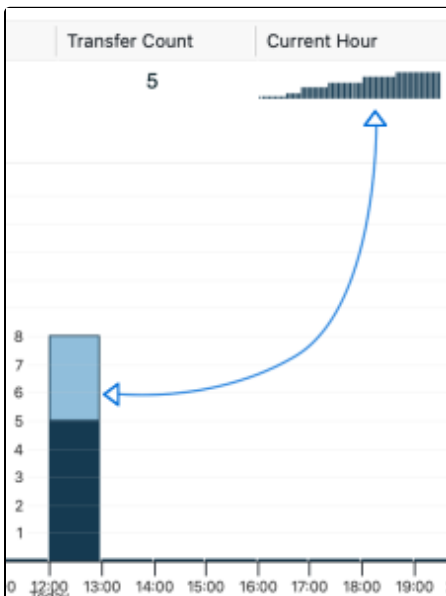
In Process

The In Process section displays the details of the current window. The contents of the section are:

- The status evaluation. This has a warning state (⚠️) if the expected minimum count of files has not been reached and is successful (✓) once the minimum count has been received.
- Start / End columns provide the time range (hour) for this expected file window.
- Expected Minimum / Expected Maximum. This is the range for the count of files expected during this window.
- Transfer Count. This is the number of file transfers counted as part of the current window.
- Current Hour. This is a sparkline chart of the number of files included in the count of files for the current window.
- Confidence. This is the confidence level associated with the window.

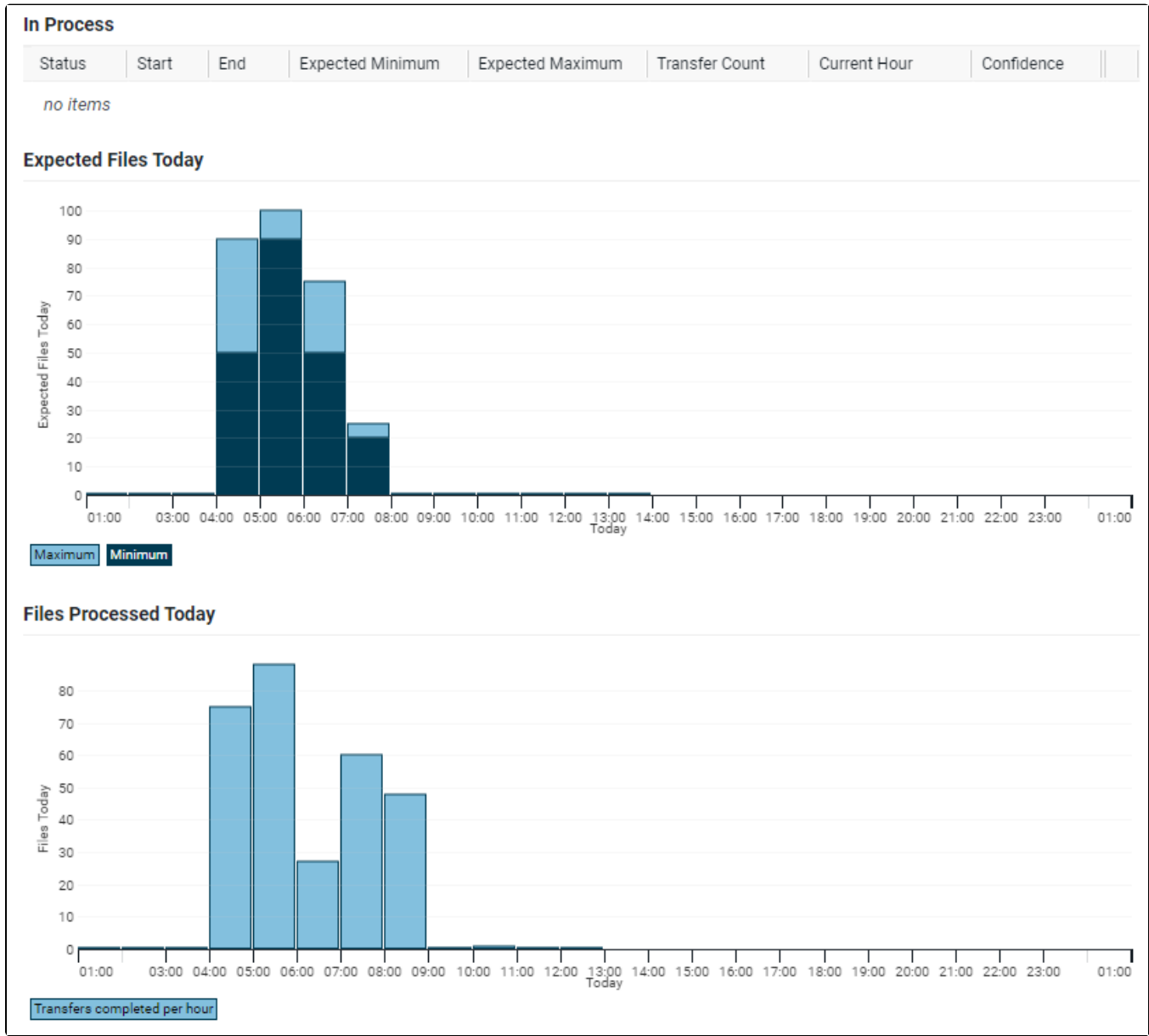
Expected Files Today

The Expected Files Today section contains a column chart showing the expected minimum and maximum count of expected files for each hour during the current day. The sparkline chart shown with the In Process section corresponds to the column shown for the same hour.



To track the progress of the current transfer count for the In Process window, you can compare the values displayed in the transfer count / current hour sections with the column chart for the most recent hour.

Expected Files Today / Files processed Today - No Monitoring in Process



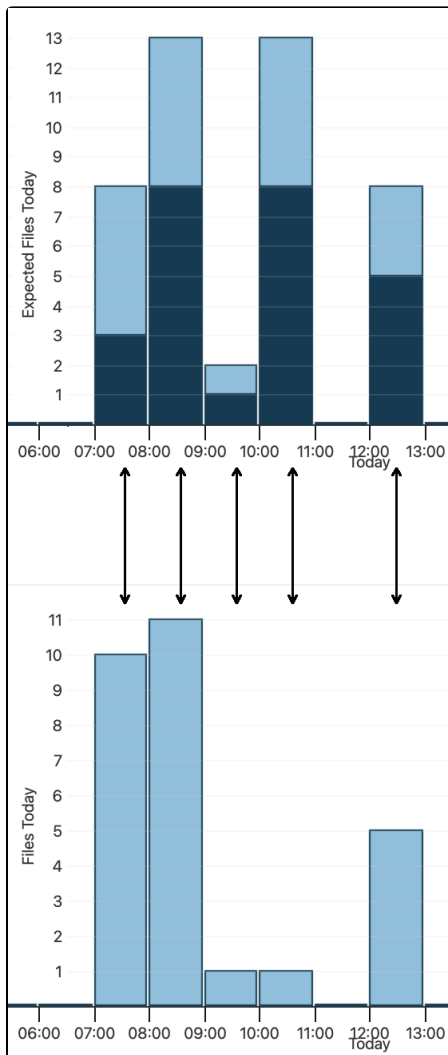
When there is no active check-in process, the two sections of Expected Files Today and Files Processed Today work together.

Expected Files Today

The Expected Files Today section contains a column chart showing the expected minimum and maximum count of expected files for each hour during the current day.

Files Processed Today

The Files Processed Today section contains a column chart showing the actual count of transferred files for each hour during the current day. The comparison to be made here is to compare the values for each hour with the matching hours in the other chart.



Passed

Successful						
Status	Start	End	Expected Minimum	Expected Maximum	Transfer Count	Confidence
✓	04:00	05:00	50	90	75	Very high
✓	07:00	08:00	20	25	60	Very high

The Passed section contains information for each successful expected file window for the current day. The fields in this section are:

- The status evaluation. In this section, the evaluation is always successful (✓).
- Start Time / End Time. This is the time range for the expected file window.
- Expected Minimum / Expected Maximum. This is the range for the count of files expected during the window.
- Transfer Count. This is the number of file transfers counted as part of the window.
- Confidence. This is the confidence level associated with the window.

Missed

Missed						
Status	Start	End	Expected Minimum	Expected Maximum	Transfer Count	Confidence
✗	05:00	06:00	90	100	88	Certain
✗	06:00	07:00	50	75	27	Moderate

The Missed section contains information for each *unsuccessful* expected file window for the current day. The fields in this section are:

- The status evaluation. In this section, the evaluation will always be failed (❌).
- Start Time / End Time. This is the time range for the expected file window.
- Expected Minimum / Expected Maximum. This is the range for the count of files expected during the window.
- Transfer Count. This is the number of file transfers counted as part of the window.
- Confidence. This is the confidence level associated with the window.

Not Started

Not Started				
Start Time	End Time	Expected Minimum	Expected Maximum	Confidence
10:00	11:00	8	13	Certain
12:00	13:00	5	8	Certain

The Not Started section lists each upcoming expected file window for the remainder of the current day. The fields in this section are:

- **Start Time/End Time.** This is the time range for the expected file window.
- **Expected Minimum/Expected Maximum.** This is the range for the count of files expected during the window.
- **Confidence.** This is the confidence level associated with the window.

Configuration Data

In this section, the users create units and configure SecureTransports.

The units can be added in the upper pagelet using the button **Add a Unit**. The purposes of the two other buttons, **Edit** and **Delete a Unit**, are to modify or to erase existing units.

You cannot delete the **admin** unit.


MFT Operational Intelligence



Welcome
admin

Global Overview
Transfer Summary
Exceptions Summary
Flow Overview
Expected File Overview
Participant Overview
Product Overview

30. Configuration Data

 LIVE
Mar 27, 2023 at 15:16
UTC+03:00





Add a Unit
Delete a Unit

Action

ID:

Name:

UnitOwnerEmail:

Apply

Cancel

Unit Management

Unit ID	Unit Name	Unit Owner Email	Edit this Unit
1	1	info@SW2RDAPP4768.pcloud.axway.int	Edit
	2	rmvaleanu@axway.com;admin@axway.com	Edit
	Unit2Name	webmaster@SW2RDAPP4768.pcloud.axway.int	Edit
	admin	admin@axway.com	Edit
	unit1Name	info@SW2RDAPP4768.pcloud.axway.int	Edit
	unit3name	-	Edit

ST Server Management

ST Server ID	ST Server Name	ST Server Address	ST Server Login	Edit this ST Server
ST-end	unit1	10.133.133.47:9444	admin	Edit
st-backend	ST_test	10.133.129.94:9444	admin	Edit

Add a ST Server

Delete a ST Server

Save

Restore

Warning: Restore will remove ST and Unit instances not in the file

In the second page, you can add SecureTransport details using the button **Add a ST Server**. You can edit or delete an existing SecureTransport using the **Edit** and **Delete a ST Server** buttons.

MFT Operational Intelligence

Global Overview Transfer Summary Exceptions Summary Flow Overview Expected File Overview Participant Overview Product Overview

30. Configuration Data LIVE Mar 27, 2023 at 15:24 UTC+03:00

Unit Management

Action

ID: Enter a text

Name: Enter a text

Address: Enter a text

Login: Enter a text

Password: Enter a text

Apply Cancel

Unit ID	Unit Name	Unit Owner Email	Edit this Unit
1	1	info@SW2RDAPP4768.pcloud.axway.int	Edit
2	2	rmvaleanu@axway.com;admin@axway.com	Edit
Unit2ID	Unit2Name	webmaster@SW2RDAPP4768.pcloud.axway.int	Edit
admin	admin	admin@axway.com	Edit
unit1ID	unit1Name	info@SW2RDAPP4768.pcloud.axway.int	Edit
unit3ID	unit3Name	-	Edit

Add a ST Server Delete a ST Server

ST Server ID	ST Server Name	ST Server Address	ST Server Login	Edit this ST Server
ST-end	unit1	10.133.133.47:9444	admin	Edit
st-backend	ST_test	10.133.129.94:9444	admin	Edit

Save Restore Warning: Restore will remove ST and Unit instances not in the file

The button **Save** from the page footer is used to save all data from this page in order to preserve them after an upgrade.

MFT Operational Intelligence

Global Overview Transfer Summary Exceptions Summary Flow Overview Expected File Overview Participant Overview Product Overview

30. Configuration Data LIVE Mar 27, 2023 at 17:39 UTC+03:00

Unit Management

Add a Unit Delete a Unit

Unit ID	Unit Name	Unit Owner Email	Edit this Unit
1	1	info@SW2RDAPP4768.pcloud.axway.int	Edit
2	2	rmvaleanu@axway.com;admin@axway.com	Edit
Unit2ID	Unit2Name	webmaster@SW2RDAPP4768.pcloud.axway.int	Edit
admin	admin	admin@axway.com	Edit
unit1ID	unit1Name	info@SW2RDAPP4768.pcloud.axway.int	Edit
unit3ID	unit3Name	-	Edit

Add a ST Server Delete a ST Server

ST Server ID	ST Server Name	ST Server Address	ST Server Login	Edit this ST Server
ST-end	unit1	10.133.133.47:9444	admin	Edit
st-backend	ST_test	10.133.129.94:9444	admin	Edit

Action

Comment to place at top of file: Enter a text

Full path and filename on server: Enter a text

Apply Cancel

Save Restore Warning: Restore will remove ST and Unit instances not in the file

A value is set as a header inside the saved file and this file's path has to be set in the **Action** window.

The **Restore** button is used to import the saved data after the upgrade. The values of the attributes are overwritten.

MFT Operational Intelligence

Welcome admin

Global OverviewTransfer SummaryExceptions SummaryFlow OverviewExpected File OverviewParticipant OverviewProduct Overview

30. Configuration DataLIVEMar 27, 2023 at 17:41UTC+03:00

Add a UnitDelete a Unit

Unit ID	Unit Name	Unit Owner Email	Edit this Unit
1	1	info@SW2RDAPP4768.pcloud.axway.int	Edit
2	2	rmvoleanu@axway.com;admin@axway.com	Edit
Unit2ID	Unit2Name	webmaster@SW2RDAPP4768.pcloud.axway.int	Edit
admin	admin	admin@axway.com	Edit
unit1ID	unit1Name	info@SW2RDAPP4768.pcloud.axway.int	Edit
unit3Id	unit3name	-	Edit

Add a ST ServerDelete a ST Server

ST Server ID	ST Server Name	ST Server Address	ST Server Login	Edit this ST Server
ST-end	unit1	10.133.133.47:9444	admin	Edit
st-backend	ST_test	10.133.129.94:9444	admin	Edit

Action

Full path and filename on server:

ApplyCancel

SaveRestore

Warning: Restore will remove ST and Unit instances not in the file

Next

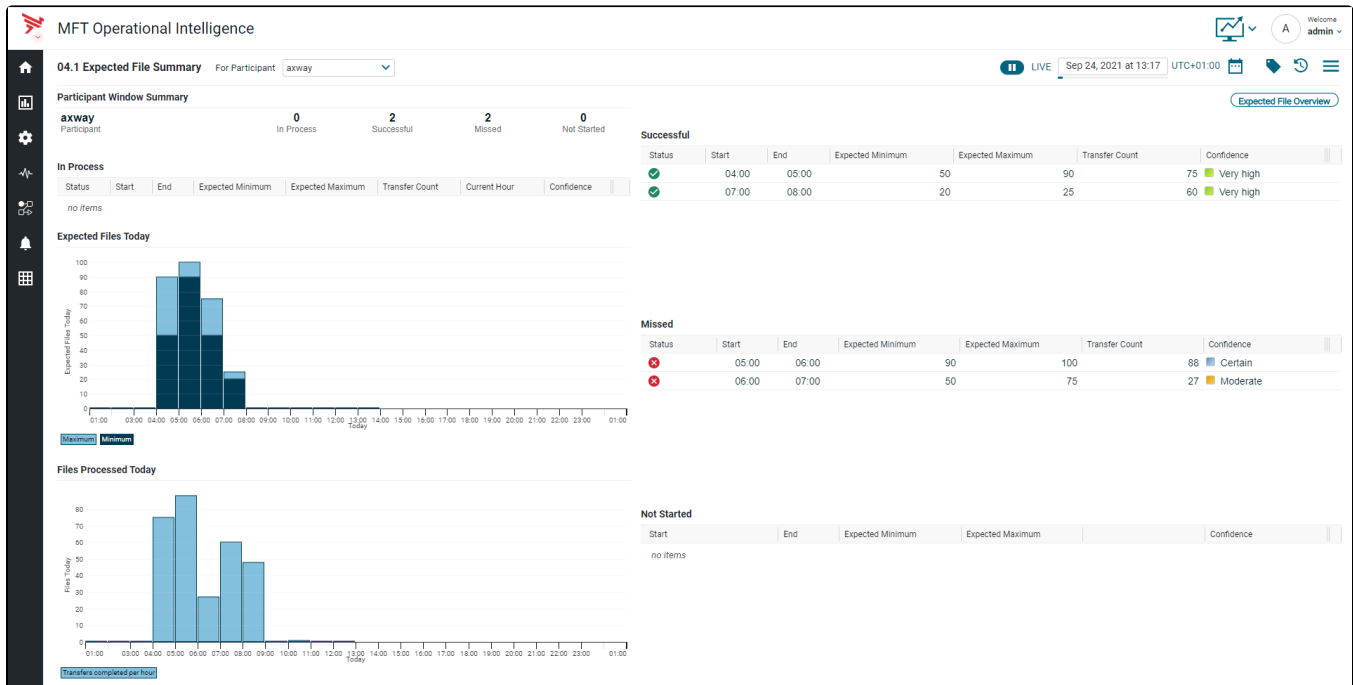
Dashboard navigation

Dashboard navigation

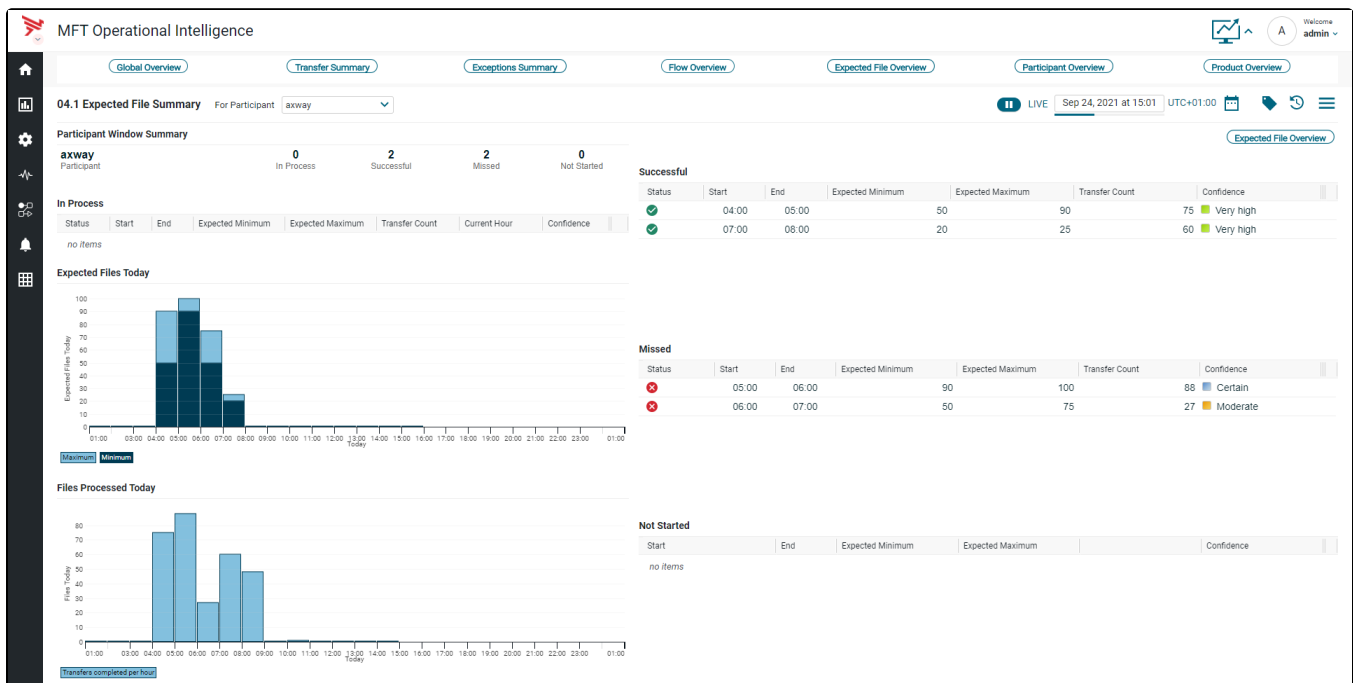
MFT Operational Intelligence provides several methods of navigating between dashboards. One of those uses a conceptual dashboard in the Dashboard list called the Navigation Header or Mini Navigation Dashboard, which is not a stand-alone dashboard but is used in conjunction with other dashboards. In the top right section of any dashboard, this icon displays:



The down arrow in this icon indicates that clicking the icon slides the mini dashboard "down" to reveal it at the top of the dashboard. For example, if you were viewing the dashboard in its default setting, you would see:



If you click the mini dashboard icon's down arrow, OI will display the mini navigation dashboard at the top:



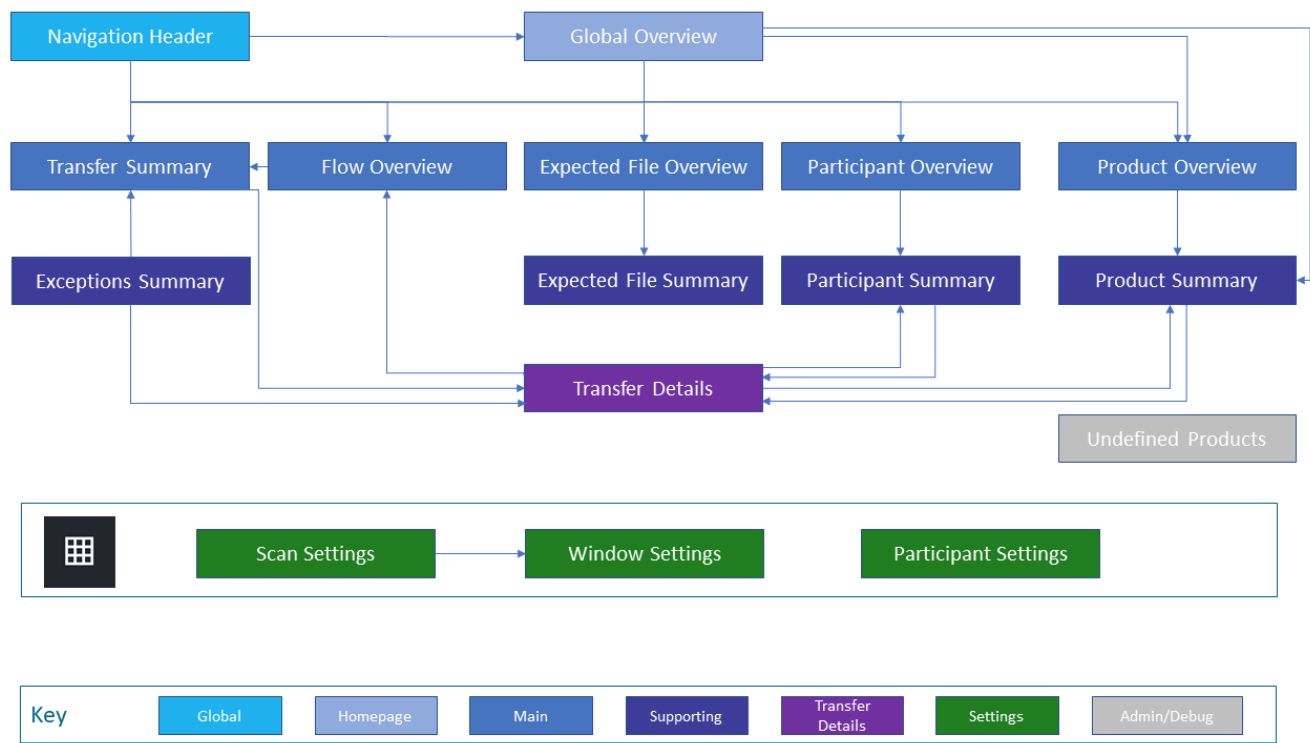
Each button in the mini dashboard takes you to the associated dashboard. The mini dashboard remains displayed until you click the mini dashboard's up icon.



Navigation links

The mini navigation dashboard is not the only way to navigate. Each dashboard is built with navigation to assist your flow through OI, with options to drill down to more detail or to a related perspective in most cases.

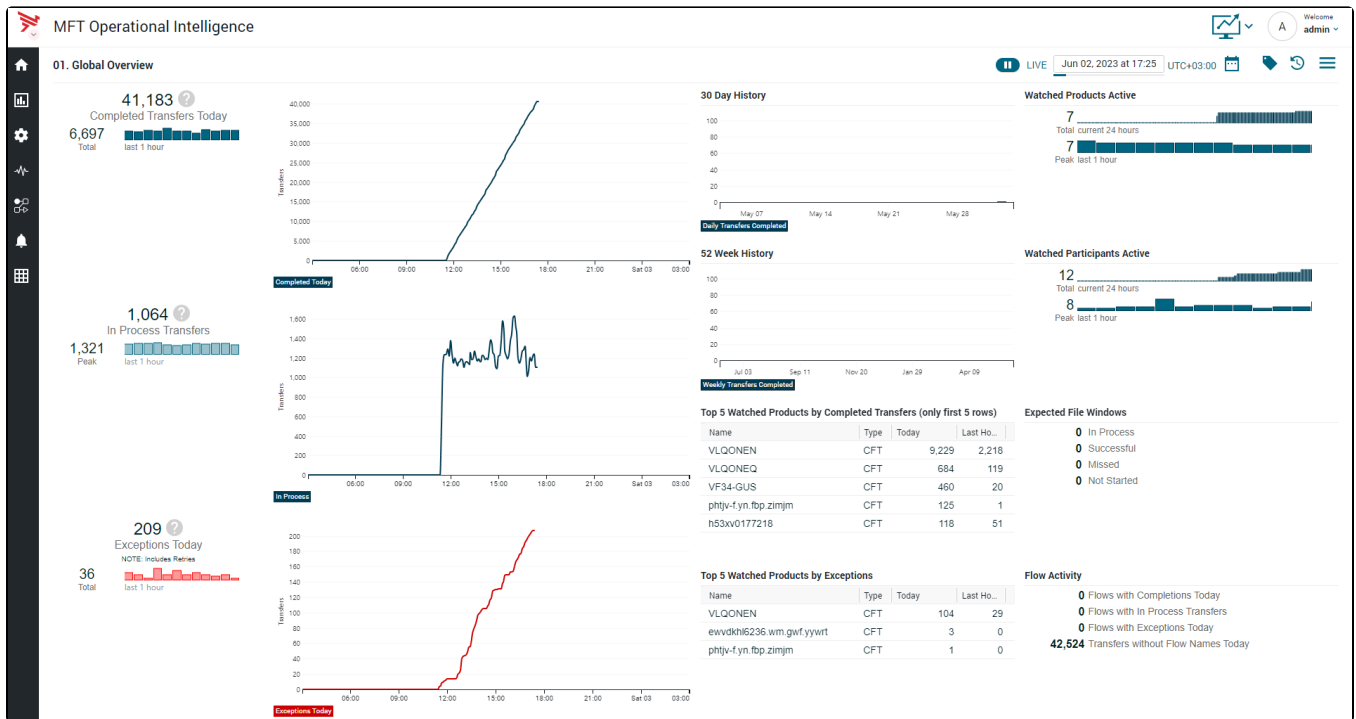
Here is an image of the general flow of navigation links:



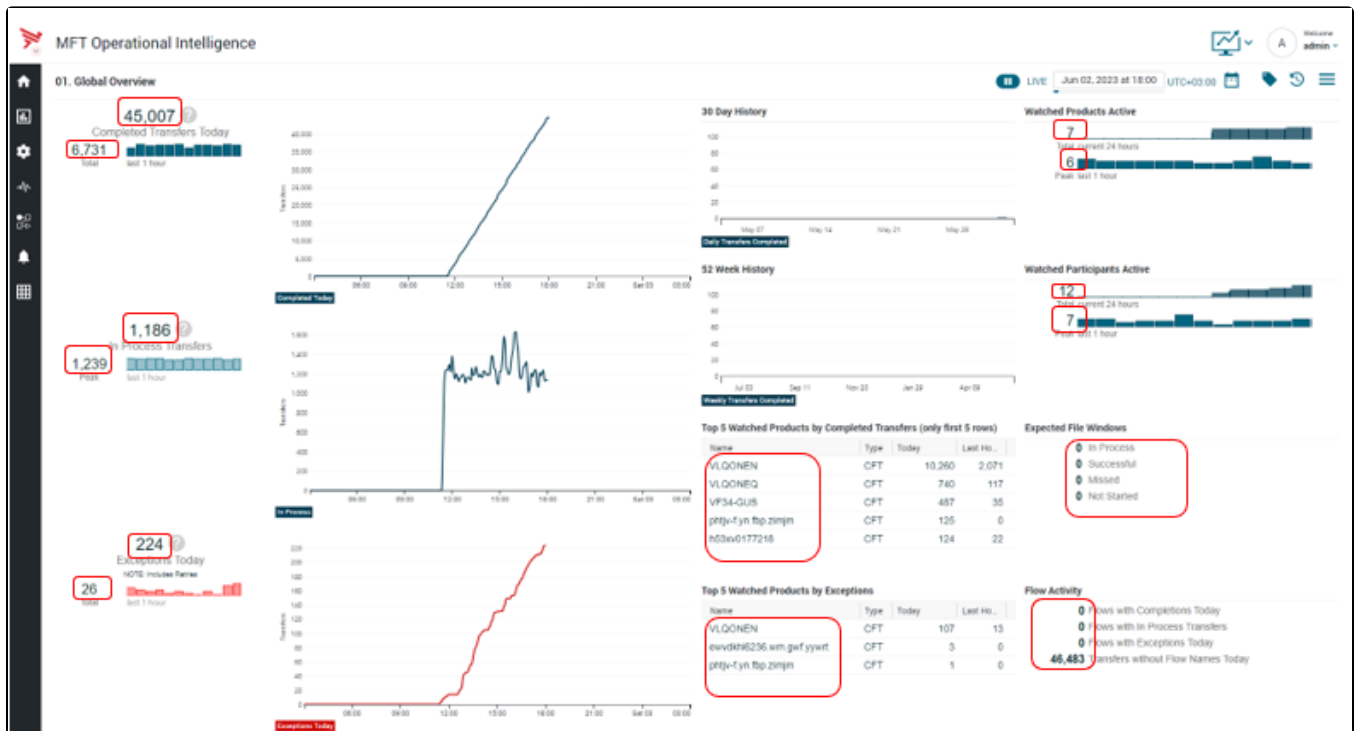
Dashboard links

All primary dashboards contain links to related dashboards. The following sections explain how the navigation works for each primary dashboard.

Global overview



The links for the Global Overview dashboard are located across the dashboard:



Transfer summary

- If the Transfer is still In Process (status of Processing), an action button of Complete Transfer would be visible under Inflight in the top right of the screen.
- If the Transfer is not an Exception, a button link will be visible under Transfer Summary to navigate back to the Transfer Summary dashboard.
- If the Transfer is an Exception, a button link will be visible under Exception Summary to navigate back to the Exceptions Summary dashboard, and the button under Transfer Summary to navigate back to the Transfer Summary dashboard will not be visible.

Depending on how you navigate to the details, some navigation buttons are also available. If the previous dashboard was Transfer Summary, there is a navigation button back to Transfer Summary. If you link to Transfer Details from Exception Summary, the return link is to the Exception Summary.

MFT Operational Intelligence

02.2 Exceptions Summary For Search Period-Last 1 hours

For

Filters:

Creation Time

Filename

Direction

Receiver ID

Flow Name

Sender ID

State

Protocol

Location

Participant

Product Name

Product Type

Cycle ID

Selected Transfers (65 rows)

	Flow Name	Creation time	Direction	Filename	Receiver ID	Sender ID	Participant	State	Protocol	Location	Product Type	Product Name	File Size (bytes)	Cycle ID
2023-06-06 10:39:20.995	02023-06-06 10:39:20.995	S	PA21.ZIM72054.V2178429	US33E11P	V0884040	US33E11P	CANCELLED	(none)	W0882040	CPT	US33E11P	0	US33E11P-V0884040-V2178429	
2023-06-06 10:39:20.991	02023-06-06 10:39:20.991	S	PA21.ZIM72058.V2178429	US33E11P	V0884040	US33E11P	CANCELLED	(none)	W0882040	CPT	US33E11P	0	US33E11P-V0884040-V2178429	
2023-06-06 10:39:20.844	02023-06-06 10:39:20.844	S	3p0umcmbe0a0g0e0240C02T...	V0781023	V0781023	US33E11P	CANCELLED	(none)	W0882040	CPT	US33E11P	0	US33E11P-V0781023-V0781023	
2023-06-06 10:39:20.844	02023-06-06 10:39:20.844	S	3p0umcmbe0a0g0e0240C02T...	V0781023	V0781023	US33E11P	CANCELLED	PSB_HIS_E	W0882040	CPT	US33E11P	3,512,320	US33E11P-V0781023-V0781023	
2023-06-06 10:17:03.909	02023-06-06 10:17:03.909	S	3p0umcmbe0a0g0e0240C02T...	P9178908P	V0781023	US33E11P	CANCELLED	PSB_HIS_E	W0882040	CPT	US33E11P	80,176	US33E11P-P9178908P-V0781023	
2023-06-06 10:14:47.902	02023-06-06 10:14:47.902	S	3p0umcmbe0a0g0e0240C02T...	V0882040	V0781023	US33E11P	CANCELLED	PSB_HIS_E	W0882040	CPT	US33E11P	1,871,212	US33E11P-V0882040-V0781023	
2023-06-06 10:13:46.208	02023-06-06 10:13:46.208	S	3p0umcmbe0a0g0e0240C02T...	V0781023	V0781023	US33E11P	CANCELLED	PSB_HIS_E	W0882040	CPT	US33E11P	1,853,884	US33E11P-V0781023-V0781023	
2023-06-06 10:13:46.217	02023-06-06 10:13:46.217	S	3p0umcmbe0a0g0e0240C02T...	V0781023	V0781023	US33E11P	CANCELLED	(none)	W0882040	CPT	US33E11P	0	US33E11P-V0781023-V0781023	
2023-06-06 10:09:10.841	02023-06-06 10:09:10.841	R	3p0umcmbe0a0g0e0240C02T...	V0781023	V0884012P	US33E11P	CANCELLED	PSB_HIS_E	W0882040	CPT	US33E11P	0	US33E11P-V0884012P-V0781023	
2023-06-06 10:09:10.841	02023-06-06 10:09:10.841	S	3p0umcmbe0a0g0e0240C02T...	V0882040	V0781023	US33E11P	CANCELLED	PSB_HIS_E	W0882040	CPT	US33E11P	1,878,284	US33E11P-V0882040-V0781023	
2023-06-06 10:00:20.007	02023-06-06 10:00:20.007	S	PA21.ZIM63850.V0780429	V040210P	V0780987P	US33E11P	CANCELLED	PSB_HIS_E	W0882040	CPT	US33E11P	0	US33E11P-V0780987P-V0780429	
2023-06-06 10:00:20.007	02023-06-06 10:00:20.007	S	PA21.ZIM63850.V0780429	US33E11P	V0780987P	US33E11P	CANCELLED	(none)	W0882040	CPT	US33E11P	0	US33E11P-V0780987P-V0780429	
2023-06-06 10:00:20.007	02023-06-06 10:00:20.007	S	PA21.ZIM63850.V0780429	US33E11P	V0780987P	US33E11P	CANCELLED	PSB_HIS_E	W0882040	CPT	US33E11P	0	US33E11P-V0780987P-V0780429	
2023-06-06 10:00:20.007	02023-06-06 10:00:20.007	S	PA21.ZIM63850.V0780429	US33E11P	V0780987P	US33E11P	CANCELLED	(none)	W0882040	CPT	US33E11P	0	US33E11P-V0780987P-V0780429	
2023-06-06 10:00:20.007	02023-06-06 10:00:20.007	S	PA21.ZIM63850.V0780429	V040210P	V0780987P	US33E11P	CANCELLED	PSB_HIS_E	W0882040	CPT	US33E11P	0	US33E11P-V0780987P-V0780429	
2023-06-06 10:00:20.007	02023-06-06 10:00:20.007	S	PA21.ZIM63850.V0780429	V040210P	V0780987P	US33E11P	CANCELLED	PSB_HIS_E	W0882040	CPT	US33E11P	0	US33E11P-V0780987P-V0780429	
2023-06-06 10:00:20.007	02023-06-06 10:00:20.007	S	PA21.ZIM63850.V0780429	US33E11P	V0780987P	US33E11P								

A button to navigate to the Transfer Summary dashboard is also provided at the top of the screen.

On the Flow Overview dashboard, only the first column displaying Transfers navigates to another dashboard, Transfer Summary, selecting the Flow Name in the filtering criteria.

MFT Operational Intelligence

03. Flow Overview For Search Period: Last 1 hours LIVE Sep 24, 2021 at 13:45 UTC+01:00

For: Search Period

Filters: Flow Name List, Flow Name, Application, Completed, In Process, Exceptions, Source Application, Target Application, Group Name, Max File Size, Max Bytes Transmitt..., Max Transmission TL..., Group ID, Location Group, Protocol Local ID

Selected Flows (175 rows)

Flow Name	Application	Completed	In Process	Exceptions	Source Application	Target Application	Group Name	Max File Size	Max Bytes Transmitted	Max Transmission Time	Group ID	Location Group	Protocol Local ID
Tranctes #04505a1-1d11-4040-850a-712...	FlowManagerApplication	3	0	0	-	-	DefaultBU	28	28	623 ms	-	-	-
Tranctes dM1399b-7b42-476a-a299-083...	FlowManagerApplication	2	1	0	-	-	DefaultBU	23	23	3 s 41 ms	-	-	-
Tranctes 7bb10960-7530-4280-8349-47...	FlowManagerApplication	1	0	0	-	-	DefaultBU	2,063	2,063	2 s 953 ms	-	-	-
Tranctes 8bc176d7-a168-4749-a115-fb...	FlowManagerApplication	1	1	0	-	-	DefaultBU	23	23	74 ms	-	-	-
Tranctes 0051-TestPatternToConf	FlowManagerApplication	8	0	0	-	-	FlowManagerBusinessUnit	82	82	3 s 706 ms	-	-	-
Tranctes 8726da0-3112-402b-8832-81e...	FlowManagerApplication	1	0	0	-	-	DefaultBU	28	0	3 s 391 ms	-	-	-
Tranctes 080ce11e-a735-4f1e-ae0e-8d2...	FlowManagerApplication	1	0	0	-	-	DefaultBU	24	0	2 s 696 ms	-	-	-
Tranctes #a095251-9d11-4595-3d46-2b...	FlowManagerApplication	1	0	0	-	-	DefaultBU	0	0	3 s 188 ms	-	-	-
Tranctes 1b35525-5700-4542-94c7-a69...	FlowManagerApplication	1	1	0	-	-	DefaultBU	16	16	78 ms	-	-	-
Tranctes 0045-TestPatternToConf	0045-TESTFLOWTOCONF	9	0	0	APP_CPT_SOURCE	-	GROUPNAME_UNKNOWN	9	9	4 s 914 ms	-	dev:docker	TCP_IPESIT1
Tranctes 0079-TestPatternToConf	FlowManagerApplication	8	4	0	-	-	FlowManagerBusinessUnit	21	21	3 s 39 ms	-	-	-
Tranctes e050445-5d09-4440-9200-a1e...	FlowManagerApplication	2	0	0	-	-	DefaultBU	24	24	3 s 222 ms	-	-	-
Tranctes 0059-TestPatternToConf	FlowManagerApplication	8	4	0	-	-	FlowManagerBusinessUnit	24	24	3 s 101 ms	-	-	-
Tranctes 0029-TestPatternToConf	FlowManagerApplication	8	4	0	-	-	FlowManagerBusinessUnit	23	23	3 s 90 ms	-	-	-
Tranctes 722711e-7d69-4ae1-9d13-514...	FlowManagerApplication	1	0	0	-	-	DefaultBU	16	16	41 ms	-	-	-
Tranctes 0059-TestPatternToConf-SSL	FlowManagerApplication	16	4	0	-	-	FlowManagerBusinessUnit	625	21	3 s 440 ms	-	-	-
Tranctes 290e6021-40e0-4525-a502-a...	FlowManagerApplication	1	0	0	-	-	DefaultBU	9	9	51 ms	-	-	-
Tranctes 0035-TestPatternToConf-SSL	FlowManagerApplication	10	0	0	-	-	FlowManagerBusinessUnit	0	28	3 s 813 ms	-	-	-
Tranctes 78a07016-732a-46a7-0119-48...	FlowManagerApplication	3	0	0	-	-	DefaultBU	28	28	3 s 48 ms	-	-	-
Tranctes c7bd8539-0973-439-bd9f-450...	FlowManagerApplication	2	1	0	-	-	DefaultBU	24	24	3 s	-	-	-
Tranctes a08a3111-5995-4304-a590-05...	FlowManagerApplication	2	0	0	-	-	DefaultBU	24	24	2 s 954 ms	-	-	-
Tranctes #4f6b8e-1194-45a1-ba6f-a6b...	FlowManagerApplication	1	0	0	-	-	DefaultBU	20	20	6 s 821 ms	-	-	-

Expected File Overview

MFT Operational Intelligence

04. Expected File Overview LIVE Sep 24, 2021 at 13:17 UTC+01:00

0 Windows In Process 2 Successful Windows 2 Missed Windows 0 Windows Not Started

Windows In Process

Status	Participant	Start	End	Expected Minimum	Expected Maximum	Current Count	Confidence
no items							

Successful Windows

Status	Participant	Start	End	Expected Minimum	Expected Maximum	Transfer Count	Confidence
✓	axway	04:00	05:00	50	90	75	Very high
✓	axway	07:00	08:00	20	25	60	Very high

Windows Not Started

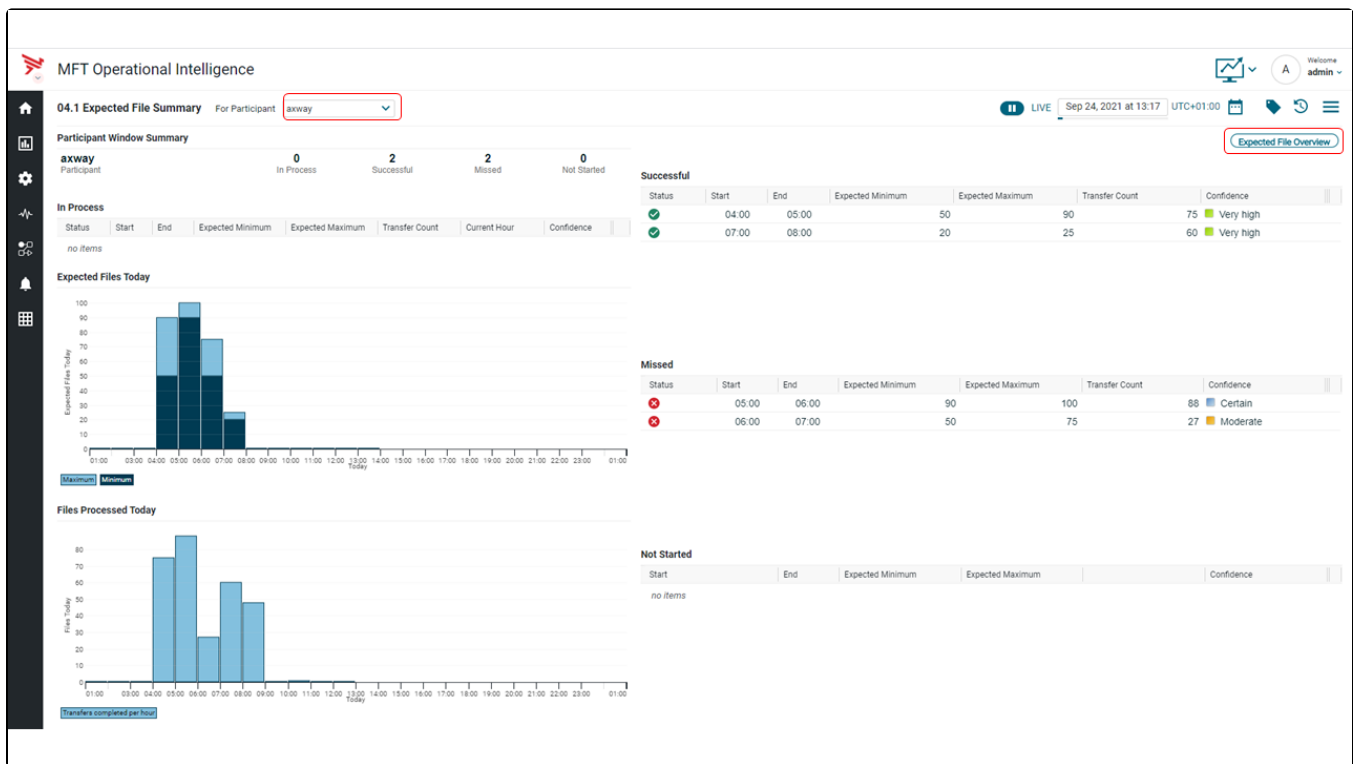
Participant	Start	End	Expected Minimum	Expected Maximum	Transfer Count	Confidence
no items						

Missed Windows

Status	Participant	Start	End	Expected Minimum	Expected Maximum	Transfer Count	Confidence
✗	axway	05:00	06:00	90	100	88	Certain
✗	axway	06:00	07:00	50	75	27	Moderate

From the Expected File Overview dashboard, each of the four tables provides a link based on the Participant, which redirects to the Expected File Summary dashboard with that Participant selected.

Expected file summary



It is possible to update the selected Participant by using the drop-down menu.

A button in the top right of the Expected File Summary dashboard redirects to the Expected File Overview dashboard (to return to view other Windows).

There is no link from the Expected File Summary dashboard to the interface screen for Windows Settings, which allows you to configure windows for watched participants. However, this is available via the Windows button on the left menu bar.

Participant overview

05. Participant Overview

Watched Participants

Status	Participant	Completed	In Process	Exceptions	Windows In Process	Successful Windows	Missed Windows	Windows Not Started	Active Today	Active Last Hour
?	partner_xfb_target_1	94	68	3	0	0	0	0	✓	✓
?	axway	299	0	0	0	2	2	0	✓	✓
?	LVR	10	0	0	0	0	0	0	✓	✓
?	BJAAVQA	2	0	0	0	0	0	0	✓	✓
?	gksv	36	0	0	0	0	0	0	✓	✓
?	rbx	0	0	0	0	0	0	0	✓	✓
?	CHYLRRG	14	0	0	0	0	0	0	✓	✓

Unwatched Participants

Status	Participant	Completed	In Process	Exceptions	Active Today	Active last hour
?	BCQKEQE	0	0	0	✓	✓
?	CQBV	8	0	0	✓	✓
?	GWBFRXG	54	0	0	✓	✓
?	IYREDBS	14	0	0	✓	✓
?	J2196	12	0	0	✓	✓
?	LQOIO	0	0	0	✓	✓
?	LVRLP3FB	31	0	0	✓	✓
?	LVRLOE	1,853	5	31	✓	✓
?	LVRLOEFB	46	0	1	✓	✓
?	LVRLOH	7	0	2	✓	✓
?	LVRLOM4V	56	0	0	✓	✓
?	LVRLOQ	16	0	0	✓	✓
?	LVRLOQR	3,992	3	17	✓	✓
?	LVRLOQS	17	0	0	✓	✓

Clicking the entry in the Participant column will navigate to the Participant Summary for the matching participant.

Participant summary



There are multiple navigation options from the Participant Summary dashboard.

- The Global summary (panels on the left) typically navigates to the Transfer Summary dashboard with the Participant selected in the filtering.
- Exceptions in the Last 1 hour navigate to the Exceptions Summary dashboard with the Participant selected in the filtering.
- There is a navigation button in the top right to navigate to the Participant Overview dashboard.
- From the Expected File Summary table, clicking any number will redirect to the Expected File Summary dashboard with the Participant selected.
- From either 'In Process Transfers' or 'Transfer Exceptions Today' tables
 - Clicking Details takes you to the Transfer Details dashboard for the specific transfer.
 - Clicking Flow Name takes you to the Flow Overview dashboard, where the Flow Name is filtered to match that of the transfer.

Product overview

MFT Operational Intelligence

06. Product Overview

Filters: Product Name Product Type

Watching Product Instances (6 rows)

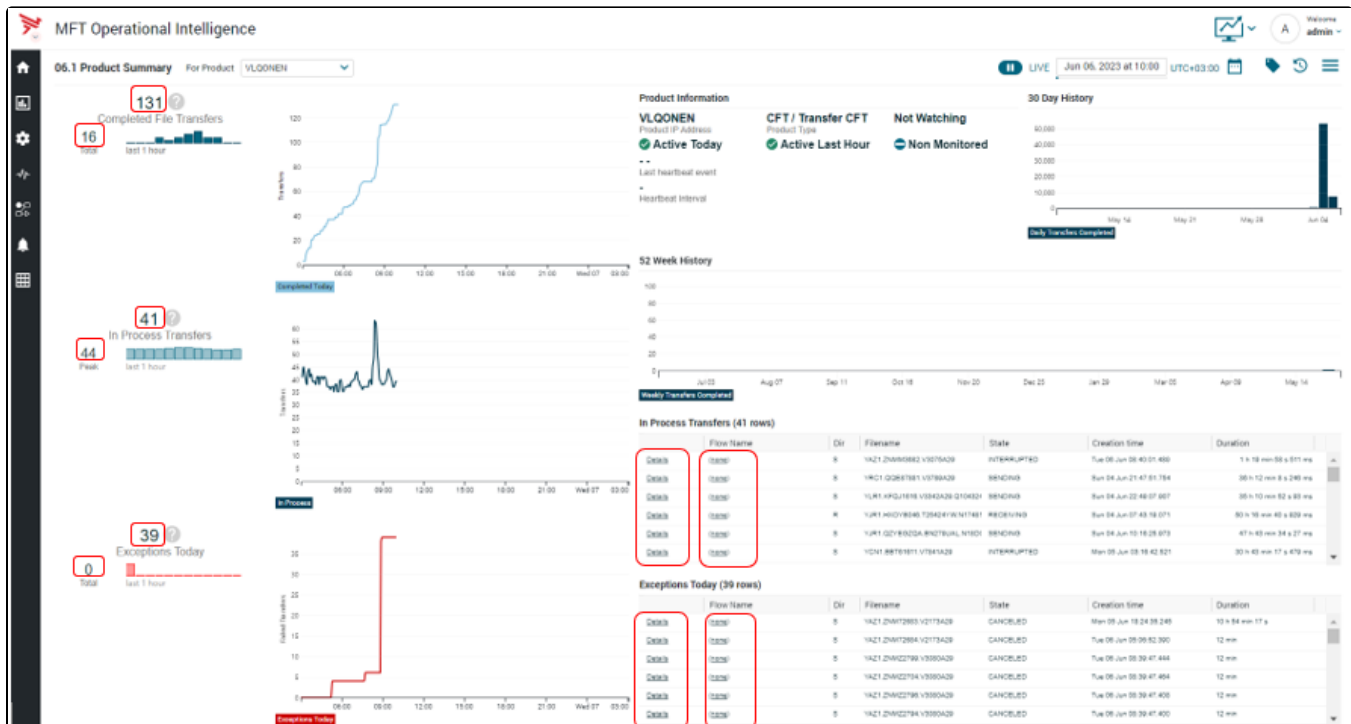
Status	Product Name	Completed	In Process	Exceptions	Product Type	Active Today	Active Last Hour	Action
1	925.X1.257.297	51	0	0	CFT	✓	✓	Stop Watching
2	VLQONEQ	1,345	0	0	CFT	✓	✓	Stop Watching
3	ewydkh6236_wm.qw	635	0	22	CFT	✓	✓	Stop Watching
4	rh_ghofme2_m-hr	62,047	9	157	CFT	✓	✓	Stop Watching
5	ctf1	57	0	0	CFT	✓	✓	Stop Watching
6	VLQONEN	28,920	23	228	CFT	✓	✓	Stop Watching

Not Watching Product Instances (7 rows)

Status	Product Name	Completed	In Process	Exceptions	Product Type	Active Today	Active Last Hour	Action
1	VFA4-GUS	871	0	0	CFT	✓	✓	Start Watching
2	ctb2	14	0	0	CFT	✓	✓	Start Watching
3	ctb3	16	0	0	CFT	✓	✓	Start Watching
4	ctb5	4	0	0	CFT	✓	✓	Start Watching
5	h53bv0177218	218	0	0	CFT	✓	✓	Start Watching
6	phhy-f.vp.fpe.zim(m	197	0	1	CFT	✓	✓	Start Watching
7	st-backend	857	154	10	ST	✓	✓	Start Watching

Clicking the entry in the Product column navigates to the Product Summary for the matching Product Instance.

Product summary



There are multiple navigation options from the Product Summary dashboard

- The Global summary (panels on the left) typically navigate to the Transfer Summary dashboard with the Product selected in the filtering.
- Exceptions in the Last 1 hour navigate to the Exceptions Summary dashboard with the Product selected in the filtering.
- There is a navigation button in the top right to navigate back to the Participant Overview dashboard.
- From either 'In Process Transfers' or 'Transfer Exceptions Today' tables
 - Clicking 'Details' will take you to the Transfer Details dashboard for the specific transfer.
 - Clicking Flow Name will take you to the Flow Overview dashboard with the Flow Name filtered to match that of the transfer.

Interface screen links

Two of the interface screens also contain links.

Participant settings

Window templates

Participant settings

Scan settings

Window settings

Participant settings

Total participants : 88 (no participants selected)

Start watching Stop watching

ID	Name	Status	Actions
☐ aew_fvltszan			Start watching
☐ aew_kixhy			Start watching
☐ aew_kixhyvo			Start watching
☐ aew_uk_agbgzzi			Start watching
☐ app_st_source			Start watching
☐ app_st_ssl			Start watching
☐ axway		WATCHED	Stop watching
☐ BQKEQE			Start watching
☐ BJAAVQA		WATCHED	Stop watching
☐ CHYLRRG		WATCHED	Stop watching
☐ CQBV			Start watching
☐ dop_fvltszan			Start watching
☐ dop_kixhy			Start watching
☐ dop_kixhyvo			Start watching
☐ dop_uk_agbgz			Start watching
☐ dop_uk_agbgzzi			Start watching
☐ gksv		WATCHED	Stop watching
☐ RWBRYR			Start watching

Clicking the ID of a Watched Participant will take you to the Windows Settings for the associated participant.

Scan settings

 MFT Operational Intelligence

 Welcome
admin

Window templates

Participant settings

Scan settings

Window settings

Day of week

Automatic scan: ☐

This is the scheduling of the window template service
if checkbox is not selected, the service must be run manually

Scan frequency: 3 1 week, starting on sunday

Scan period: 3 1 week, starting on sunday

Define the length of history to scan for the pattern analysis

Apply pattern: ☐ Automatically ☒ Manually

Scan for all watched participants now

Scan last performed : Not available

ID	Name	Applied templates	Unapplied templates
axway		4	0
BJAAVQA		0	0
CHYLRRG		0	0
gksv		0	0
LVR		0	0
partner_xfb_target_1		0	0
rbx		0	0

The navigation links on the Scan Settings interface screen lead to the Windows Settings interface for the same participant as the one clicked.

Next

[Configure watched participants and products](#)

Configure watched participants and products

You might be wondering what the terms Participants and Products mean.

What's a product?

MFT OI uses the term product to mean an instance of Transfer CFT or SecureTransport. Every instance of Transfer CFT or SecureTransport that emits events received by MFT OI is displayed as a Product on the Product Summary dashboard and listed in any associated transfers in the Transfer Summary, Exceptions Summary, and Transfer Details.

What's a participant?

A participant in MFT OI is any source or destination of a transfer. An external partner is a participant. An internal application is also a participant. Relay middleware may be considered a participant in some cases. Every partner, application, or relay mentioned in an event received by MFT OI is displayed as a Participant on the Participant Summary dashboard and listed in any associated transfers in the Transfer Summary, Exceptions Summary, and Transfer Details. Only Watched Participants are scanned for Expected Files.

For more information, please see [Frequently Asked Questions](#).

The way that MFT OI manages Products and Participants allows you to select certain ones to be "watched" more closely than others. If you have hundreds of Transfer CFTs or thousands of applications and partners sending and receiving files, it would be normal for some of them to be more important to the operation's success than others.

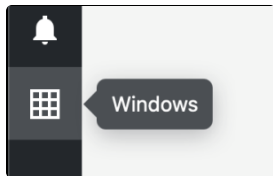
You designate important instances by configuring them to be watched. You should configure at least one Product and Participant to have the Watched status.

 The feature that automatically detects file transfer patterns only examines **Watched Participants**. If you want to have file patterns detected for a given application or partner, you must first configure them to be watched.

The way you configured watched products and watched participants is different. The following sections show you how to configure each type.

Configure watched participants

To configure a participant as watched, select the **Windows** icon from the left-hand menu bar:



OI responds by displaying the **Window templates** submenu. Select **Participant settings** in the menu:

MFT Operational Intelligence (BETA)

Windows

Participant settings

Scan settings

Window settings

Participant settings

Total participants : 7 (no participants selected)

☐

ID

☐ AlbertsOps

☐ axway

☐ best

☐ coby

☐ rdmOperations

☐ sally

☐ SECURETRANSPORT

Name

Status

Actions

WATCHED

WATCHED

WATCHED

WATCHED

Start watching

Start watching

WATCHED

Stop watching

Stop watching

Stop watching

Stop watching

Start watching

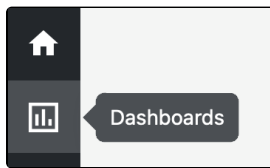
Start watching

Stop watching

Click **Start Watching** or **Stop Watching** to start or stop watching a participant. You can click the checkboxes to start or stop watching groups of participants or all of them at a time by clicking on the check box next to ID in the menu bar. When the number of participants is large enough to make locating individual ones easy, you can use the search box to limit the number of instances displayed.

Configure watched products

To configure a product as watched, select the **Dashboards** icon from the left-hand menu bar:



In the dashboard list, click the **Product Overview** thumbnail:



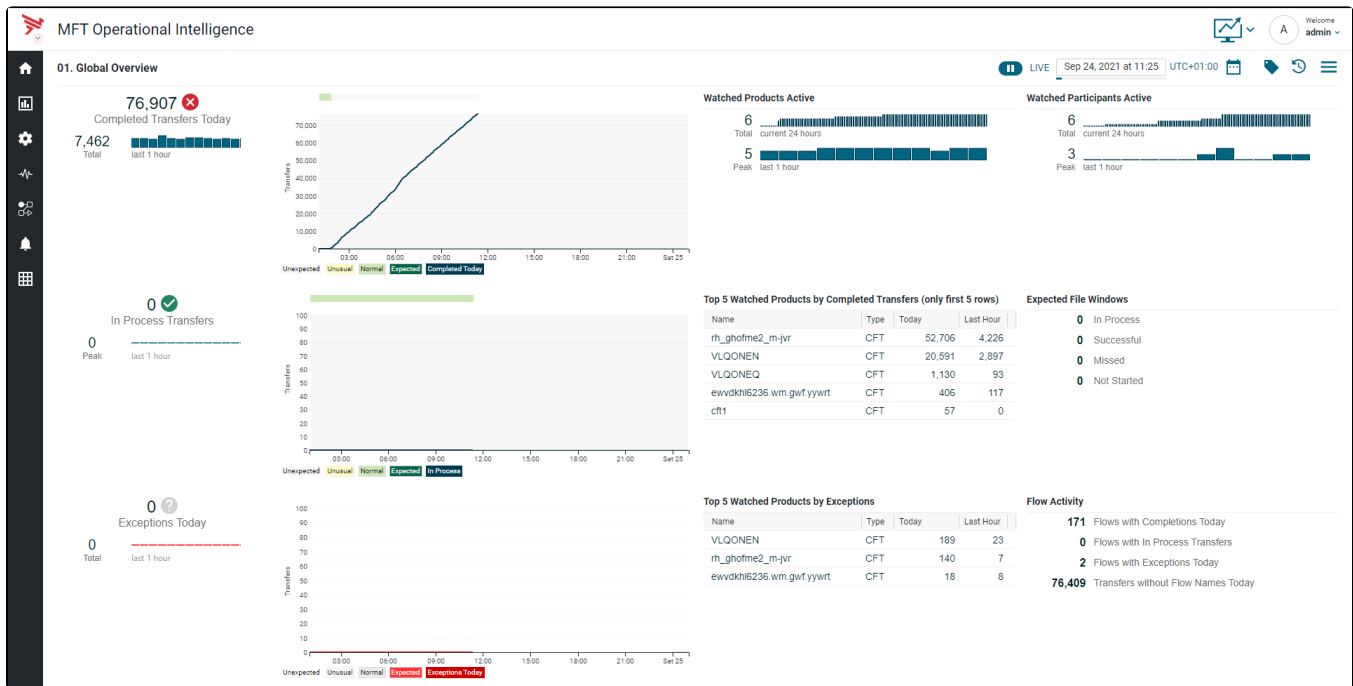
OI responds with the associated dashboard:

A screenshot of the '06. Product Overview' dashboard in the MFT Operational Intelligence interface. The dashboard has a header with the title '06. Product Overview' and a status bar showing 'LIVE' and 'Sep 24, 2021 at 13:36 UTC+01:00'. Below the header, there are two main sections: 'Watching Product Instances (6 rows)' and 'Not Watching Product Instances (7 rows)'. Each section contains a table with columns for 'Status', 'Product Name', 'Completed', 'In Process', 'Exceptions', 'Product Type', 'Active Today', 'Active Last Hour', and 'Action'. The 'Watching' section shows products like '925.21.257.297', 'VLQONEQ', 'ewydkh6236_wm.gw...', 'm_ghome2_m-jvr', 'cft1', and 'VLQONEN'. The 'Not Watching' section shows products like 'VF34-GUS', 'cft2', 'cft3', 'cft5', 'b53yv0177218', 'pnhv-f.vh.fop.zimm', and 'st-backend'. Each row in the 'Action' column has a 'Stop Watching' or 'Start Watching' button. The dashboard also includes a left-hand menu bar with various icons and a top-right corner with a user profile and navigation icons.

You can click the Start Watching and Stop Watching icons to take the associated action for the Product instance next to the icon. OI responds to the click with a green checkmark. The status of the selected product changes immediately; however, you only see that change reflected the next time the dashboard updates.

Watched products and participants on dashboards

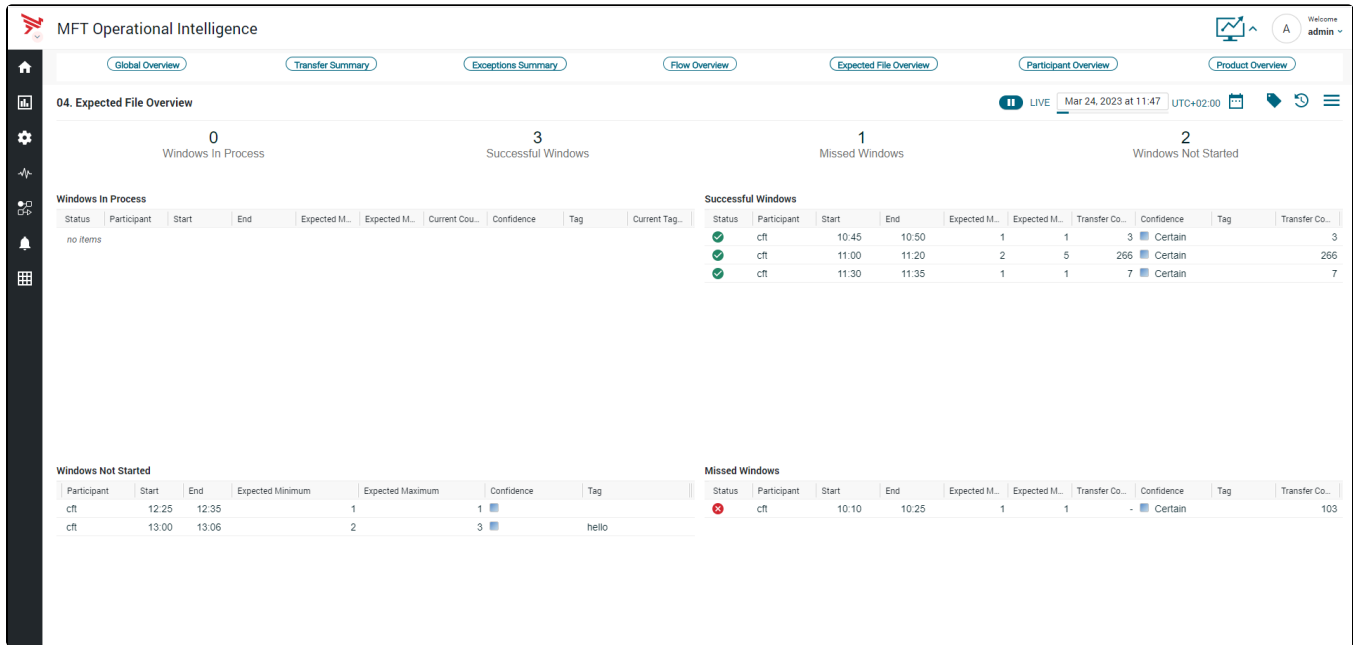
Once you have configured your watched items, the Global Overview home page begins to show information on them, which looks something like this:



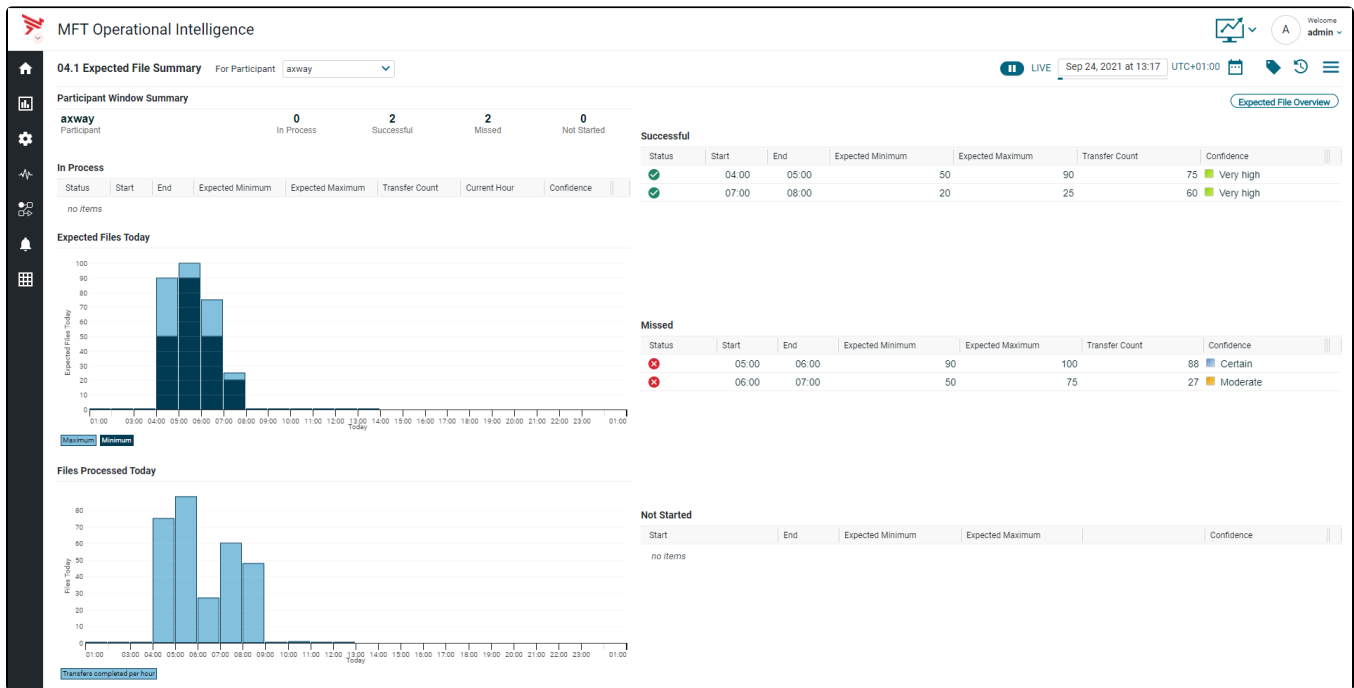
You can see that there are counts and charts at the top for the number of watched products and participants active today and in the last hour. There are also lists of the top 5 watched products in terms of volume of transfers and exceptions.

You also see data start to appear for your Watched Participants in the Expected File Overview and the Expected File Summary dashboards:

Expected File Overview



Expected File Summary



For now, you do not see any windows defined. That takes separate actions you take after running the solution for at least one week.

Next

Managing units

Manage units

A unit is a space where you configure user rights for certain participants and products.

Creating a Unit

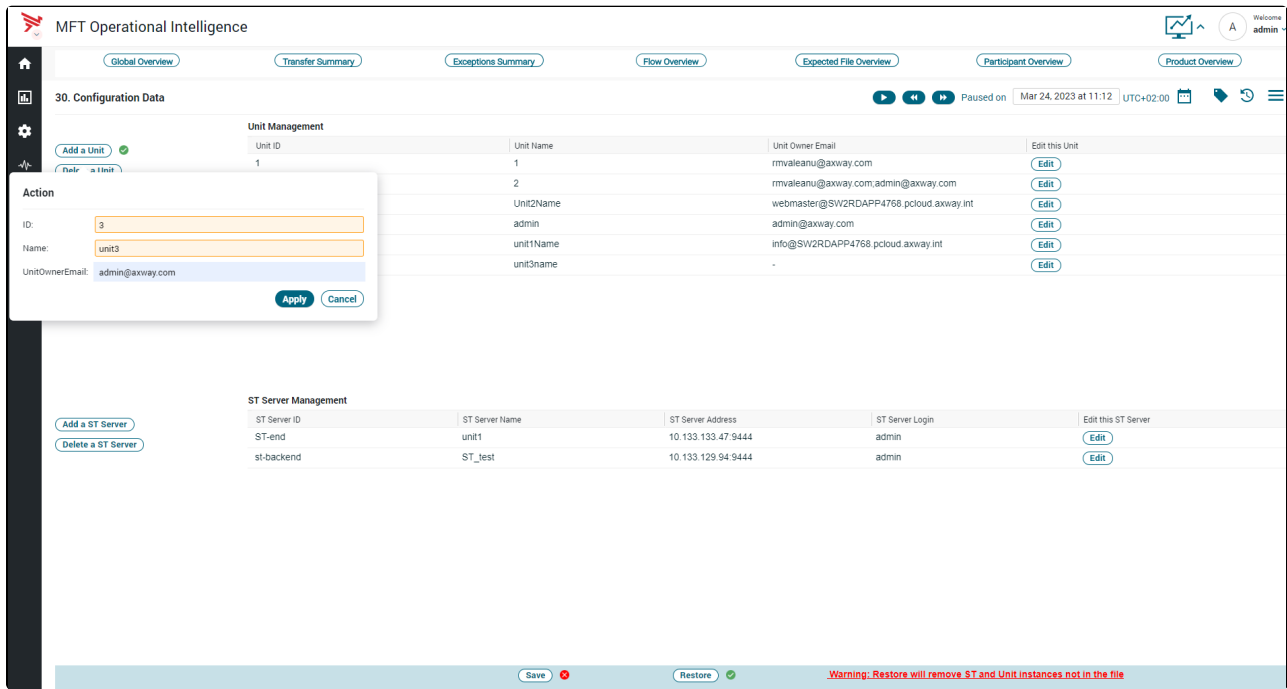
This is implemented using the following steps:

1. Navigate to **30. Configuration Data** dashboard
2. Ensure that the Route **30_AddEditDeleteSaveRestore_STServerUnit** from the **Initializers** space is started.



3. Click the **Add a Unit** button:

- For each required Unit, values must be provided in the following fields: Id, Name, and UnitOwnerEmail (multiple units can be configured at once, and multiple email addresses can be added separated by a semicolon)
- When the listing is complete, click **Apply**.



A Unit can be **edited** or **deleted** using the buttons from the upper pagelet of the dashboard **Configuration Data**.

MFT Operational Intelligence

Global Overview Transfer Summary Exceptions Summary Flow Overview Expected File Overview Participant Overview Product Overview

30. Configuration Data LIVE Mar 24, 2023 at 11:28 UTC+02:00

Unit Management

Add a Unit Delete a Unit

Action

ID of the Unit to be deleted: 1

Apply Cancel

Unit ID	Unit Name	Unit Owner Email	Edit this Unit
1	1	rmvaleanu@axway.com	Edit
2	2	rmvaleanu@axway.com,admin@axway.com	Edit
Unit2ID	Unit2Name	webmaster@SW2RDAPP4768.pcloud.axway.int	Edit
admin	admin	admin@axway.com	Edit
unit1ID	unit1Name	info@SW2RDAPP4768.pcloud.axway.int	Edit
unit3ID	unit3Name	-	Edit

ST Server Management

Add a ST Server Delete a ST Server

ST Server ID	ST Server Name	ST Server Address	ST Server Login	Edit this ST Server
ST-end	unit1	10.133.133.47.9444	admin	Edit
st-backend	ST_test	10.133.129.94.9444	admin	Edit

Save Restore Warning: Restore will remove ST and Unit instances not in the file

MFT Operational Intelligence

Global Overview Transfer Summary Exceptions Summary Flow Overview Expected File Overview Participant Overview Product Overview

30. Configuration Data LIVE Mar 24, 2023 at 11:28 UTC+02:00

Unit Management

Add a Unit Delete a Unit

Action

Name: unit1

UnitOwnerEmail: admin@axway.com

Apply Cancel

Unit ID	Unit Name	Unit Owner Email	Edit this Unit
1	1	rmvaleanu@axway.com	Edit
2	2	rmvaleanu@axway.com,admin@axway.com	Edit
Unit2ID	Unit2Name	webmaster@SW2RDAPP4768.pcloud.axway.int	Edit
admin	admin	admin@axway.com	Edit
unit1ID	unit1Name	info@SW2RDAPP4768.pcloud.axway.int	Edit
unit3ID	unit3Name	-	Edit

ST Server Management

Add a ST Server Delete a ST Server

ST Server ID	ST Server Name	ST Server Address	ST Server Login	Edit this ST Server
ST-end	unit1	10.133.133.47.9444	admin	Edit
st-backend	ST_test	10.133.129.94.9444	admin	Edit

Add users when upgrading



Important

The following section is important for first-time use of Units for customers upgrading from MFT OI V1.0.

It is recommended that you add all Users to the **admin Unit**. This ensures that you experience no interruption in your experience of MFT OI post-upgrade. Once new Units are created with the relevant Users and Participants configured, non-admin users can be safely removed from the **admin Unit**.

After an application upgrade, all participants from the **admin Unit** can be re-added by starting the route **20_AddAllParticipants**:

Configure participant and product Role Based Access Control (RBAC)

MFT OI contains an RBAC feature in which users are only exposed to analytics/data pertaining to their affiliated partners with the following configuration. This is done by grouping Users, Participants, and Products into a **Unit**. Users who are members of a particular Unit will be exposed to data relating to all the Participants and Products assigned to that unit.

Adding and removing Users, Participants, and Products to a Unit

You can add and remove Participants, Users, and Products for an existing Unit by navigating to Dashboard **97. Units**

MFT Operational Intelligence

97. Units For Unit 1

Participants from unit

Participant	Remove Participant
Axway	Remove Participant

All Participants

Participant	Add Participant to a Unit
Axway	Add Participant
John	Add Participant

Users from unit

User	Remove User
user1	Remove User

All users

User	Add User to a Unit
admin	Add User
user1	Add User

Products from unit

Product	Remove Product from a Unit
cft1	Remove Product
cft2	Remove Product
st-backend	Remove Product

All Products

Product	Add Product to a Unit
SL2RDAPP040354	Add Product
cft1	Add Product
cft2	Add Product
cft4	Add Product
mft-env	Add Product
st-backend	Add Product
st-backend2	Add Product

- The right half of the display includes all available Participants, Users, and Products currently configured in MFT OI.
- The left half of the display indicates those Participants, Users, and Products who are members/assigned of/to the currently selected Unit.

Steps

1. Select the required Unit from the **For Unit** drop-down box that is adjacent to the dashboard title in the top left of the display.
2. Add the required Participants to the Unit by clicking the **Add Participant** button (in the **All Participants** panel) adjacent to each Participant to be added to the selected Unit.
3. Add the required Users to the Unit by clicking the **Add User** button (in the **All Users** panel) adjacent to each of those Users to be added to the selected Unit.
4. Add the required Products to the Unit by clicking the **Add Product** button (in the **All Products** panel) adjacent to each Product to be added to the selected Unit.
5. Remove Participants from the selected Unit by clicking the **Remove Participant** button (in the **Participants from unit** panel) adjacent to each Participant to be removed from the selected Unit.
6. Remove Users from the selected Unit by clicking on the **Remove User** button (in the **Users from unit** panel) adjacent to each User to be removed from the selected Unit.
7. Remove Products from the selected Unit by clicking the **Remove Products** button (in the **Products from unit** panel) adjacent to each Product to be removed from the selected Unit.

The user will have access only to the transfers done after its creation.

If a user is added in more than one unit on more participants and products, they can visualize all the transfers done on these participants and products.

Once a user is allowed on a specific participant, the following dashboards are updated:

- 02. Transfer Overview
- 02.1 Transfer Summary
- 02.2 Exceptions Summary
- 05. Participant Overview
- 05.1 Participant Summary

For the allowed products, the information is filtered in the dashboards:

- 02. Transfer Overview
- 02.1 Transfer Summary
- 02.2 Exceptions Summary
- 06. Product Overview
- 06.1 Product Summary



The dashboard 01. Global Overview displays all the transfers unfiltered by participants or products.

Next

[Enabling the SNMP protocol](#)

Enable the SNMP protocol

This page describes how to use the SNMP Trap component. Simple Network Management Protocol (SNMP) is an internet standard protocol used for monitoring. The SNMP Trap component sends SNMP Traps to an SNMP server. After adding the SNMP service on Windows and installing the SNMP viewer application, you can set the protocol on MFT OI.

Enabling without MFT OI

Use the following method if you have not installed MFT OI.

1. Unzip the installation archive.
2. Navigate to the installation folder and open the "decision_insight.config" file.
3. Set the SNMP host and port:

Example

```
com.axway.mftoi.snmp.host=10.128.232.8
com.axway.mftoi.snmp.port=162
```

4. Complete the installation, go to Routes, and start the "SnmpNotification" route.
5. Go to the **Notifications** menu and start notifications.



After installing MFT OI, go to the "platform.properties" file in node/conf and note that the host and port of the SNMP protocol are also visible here:

```
com.axway.mftoi.smtp.address=
com.axway.mftoi.smtp.password=
com.axway.mftoi.smtp.username=
com.axway.mftoi.snmp.host=10.128.232.8
com.axway.mftoi.snmp.port=162
```

Enabling with MFT OI

Use one of the following methods if you have already installed MFT OI.

From the "platform.properties"

1. Stop the DI service.
2. Navigate to the "platform.properties" file in node/conf and set the SNMP host and port:

```
com.axway.mftoi.qlt.url=qlt:0.0.0.0:1307
com.axway.mftoi.qlt.keystore.path=../security/keyStore.jks
com.axway.mftoi.qlt.keystore.password=
com.axway.mftoi.qlt.keystore.keyPassword=
com.axway.mftoi.qlt.truststore.path=../security/trustStore.jks
com.axway.mftoi.qlt.truststore.password=
com.axway.mftoi.qlt.cipherSuites=
com.axway.mftoi.qlt.secureSocketProtocols=
com.axway.mftoi.smtp.address=
com.axway.mftoi.smtp.password=
com.axway.mftoi.smtp.username=
com.axway.mftoi.snmp.host=10.128.232.8
com.axway.mftoi.snmp.port=162
```

- Start the service
- Go to Routes and start "SnmpNotification" route
- Go to the Notifications menu and start the notifications

Directly in the OI interface

From Data Integration, navigate to Properties > Alerts space

Endpoints

Connectors

Mappings

Libraries

Events

Queries

Notifiers

Automation

Triggers

Transformations

Routes

States

Resources

Properties

Runtime

Logs

Properties

In space Alerts

Name	Type	Password	Value
LogLevelA	Simple	☐	INFO
LogLevelB	Simple	☐	DEBUG
SMTPaddress	From node property		com.axway.mftoi.smtp.address
SMTPfrom	Simple	☐	mftoinotif_noreply@axway.com
SMTPpassword	From node property		com.axway.mftoi.smtp.password
SMTPusername	From node property		com.axway.mftoi.smtp.username
SNMP_HOST	Simple	☐	10.128.232.8
SNMP_PORT	Simple	☐	162

- Complete the SNMP host and port fields where the Type for both is set to "Simple."
- Go to Routes and restart "SnmpNotification" route.
- Go to the Notifications menu and ensure they are started.

Next

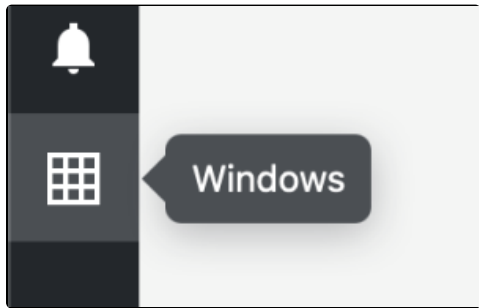
[Scan files and set window definitions for file arrival pattern detection](#)

Scan files and set window definitions for file arrival pattern detection

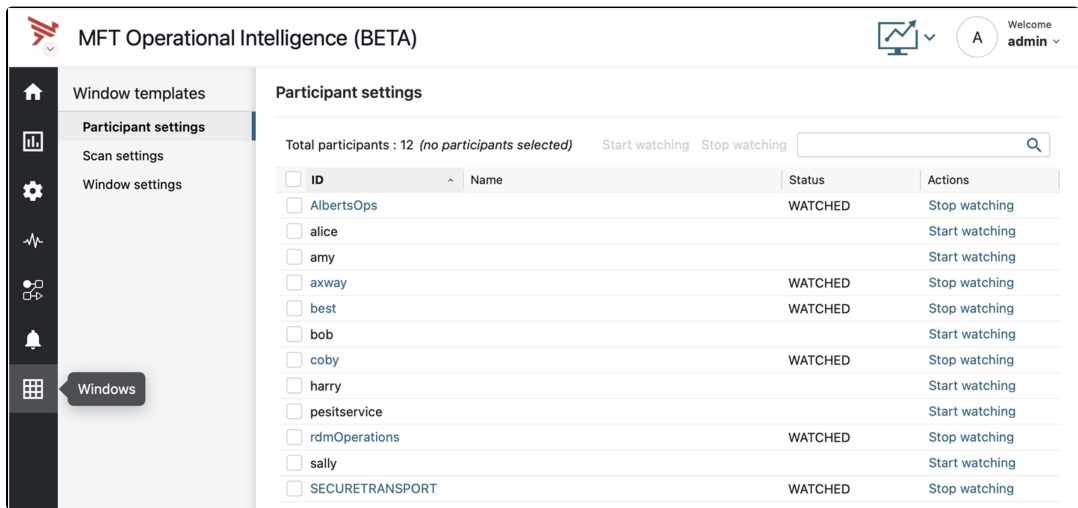
After running MFT OI with watched participants defined for a week, you can begin the next phase of validating file transfer patterns (in MFT OI, file transfer patterns involve terms such as **Windows**, **Window Templates**, and **Expected File Windows**). Check the FAQs for background information, if needed.

Scanning for Window templates

MFT OI can detect patterns after one week. Detected patterns are referred to as **Templates**. To start looking for detected patterns, select the **Windows** icon from the left-hand menu bar:



This returns the list of watched and unwatched participants as described in [Configure watched participants and products](#). Because only **Watched participants** are considered for monitoring expected file transfers, you may select additional participants at this point.



Next, navigate to the **Scan settings**, the second option under the same **Window templates** sub-menu. If no scans have been performed at this point, the Scan settings interface looks like this:

MFT Operational Intelligence (BETA)

Window templates

Participant settings

Scan settings

Window settings

Scan settings

Day of week

Automatic scan: ☐

This is the scheduling of the window template service
if checkbox is not selected, the service must be run manually

Scan frequency: 3 weeks

Scan period: 3 weeks

Define the length of history to scan for the pattern analysis

Apply pattern: ☐ Automatically ☒ Manually

Scan for all watched participants now

Scan for settings by clicking the **Scan for all watched participants now** button.

MFT Operational Intelligence (BETA)

Window templates

Participant settings

Scan settings

Window settings

Scan settings

Day of week

Automatic scan: ☐

This is the scheduling of the window template service
if checkbox is not selected, the service must be run manually

Scan frequency: 3 weeks

Scan period: 3 weeks

Define the length of history to scan for the pattern analysis

Apply pattern: ☐ Automatically ☒ Manually

Scan for all watched participants now

After the scan completes, Operational Intelligence updates the date/time the last scan was completed, as shown in the image below.

MFT Operational Intelligence (BETA)

Window templates

Participant settings

Scan settings

Window settings

Scan settings

Day of week

Automatic scan: ☐

This is the scheduling of the window template service
if checkbox is not selected, the service must be run manually

Scan frequency: 3 weeks

Scan period: 3 weeks

Define the length of history to scan for the pattern analysis

Apply pattern: ☐ Automatically ☒ Manually

Scan for all watched participants now

Scan last performed : May 06, 2021 01:08:02

The scan is relatively quick. If this is not the first file pattern scan and the scan detects no new patterns, the only indication of the successful completion of the scan is the update to the date and time.

The first time you scan watched participants for file transfer Window, the screen displays two columns for each Watched Participant, one for Window Templates (which would be all zeros, this first time) and one for New Templates. The New Templates column displays the counts of the detected patterns. The table lists the name of each Watched Participant and the detected patterns (**New Templates**).

Scan settings

Day of week

Automatic scan: ☐

This is the scheduling of the window template service. If checkbox is not selected, the service must be run manually.

Scan frequency: 1 week, starting on Sunday

Scan period: 3 days, 1 week, starting on Sunday

Define the length of history to scan for the pattern analysis.

Apply pattern: ☐ Automatically ☒ Manually

Scan now Scan last performed: Mar 28, 2023 15:12:15

ID	Name	Applied templates	Unapplied templates
account1		0	2
partner_xfb_source_1		0	2
ST_RELAY		1	2

Next, apply some of these New Templates.

Reviewing Window templates

To review and apply new templates detected for an individual participant, click the participant's ID in the table. In this example, the participant's ID is ST_RELAY:

Scan now Scan last performed: Mar 28, 2023 15:12:15

ID	Name	Applied templates	Unapplied templates
account1		0	2
partner_xfb_source_1		0	2
ST_RELAY		1	2

In this set of examples, MFT Operational Intelligence detected 2 file transfer patterns that it is proposing to the admin user as Window templates. There were 2 detected for Fridays. When clicking the name of a Watched Participant in the **Scan settings** interface, MFT OI responds by displaying the **Window Settings** for that participant.

Window settings

Participant: ST_RELAY

Day of week: Friday

Select: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

A total of 2 unapplied templates found. **Apply detected templates**

Time start: 00:00 Duration: 1 hours **Add new window template**

Start	End	Duration	Notice before closure	Confidence	Min count	Max count	Tag (optional)
10:43	10:53	10 minutes	0 minutes	Certain	1	1	hello

In this image, the 2 templates for the participant were detected, but they were not deployed yet. Do you see the line below Friday? This line indicates that only a template was deployed, and other two templates exist for this day but have not been applied.

Applying window templates

To continue the example and apply some or all of the detected templates, click the tab for Friday.

Apply scans

Applied templates

Interval	Confidence	Count
10:43 - 10:53	Certain	1 - 1

Scanned templates

☐ Show identicals and locked

Interval	Confidence	Consistency	Count	Info
10:00 - 11:00	Certain	100 %	1 - 1	
14:00 - 15:00	Certain	100 %	1 - 1	

Apply **Cancel**

The image in the left section shows the template which is already applied. The section on the right lists the two unapplied templates the scan detected for Fridays.

The meanings of the columns in this section are:

- Interval – The time range that was scanned to detect this template

- Confidence and Consistency – These are measures of how consistent the file arrivals have been during the scan
- Count – The range of file counts observed by the scan

If you conduct the scan after only one week, the values do not show any variability because there was only one data point to consider. After more time has elapsed, changes to the Confidence, Consistency, and Count fields appear.

To apply the scanned templates, click the checkboxes for the templates you wish to apply.

Apply scans

Applied templates

Interval	Confidence	Count
10:43 - 10:53	Certain	1 - 1

Scanned templates

☐ Show identicals and locked

☒ Interval	Confidence	Consistency	Count	Info
☒ 10:00 - 11:00	Certain	100 %	1 - 1	
☒ 14:00 - 15:00	Certain	100 %	1 - 1	

← Merge selection

Apply

Cancel

Once at least one of the Scanned templates is selected, the **Merge selection** button becomes active. When you click **Merge selection**, the selected templates are moved to the Applied templates section, and the **Apply** button at the bottom of the dialog box is enabled.

Apply scans

Applied templates

Interval	Confidence	Count
10:00 - 11:00	Certain	1 - 1
10:43 - 10:53	Certain	1 - 1
14:00 - 15:00	Certain	1 - 1

Scanned templates

☐ Show identicals and locked

☐ Interval

Confidence

Consistency

Count

Info

No items

← Merge selection

Apply

Cancel

To accept the templates in the Applied templates section, click **Apply**. Operational Intelligence responds by updating the Window settings page:

Window settings

Participant: ST_RELAY

Day of week

Select: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

All templates applied

Time start: 00 : 00 Duration: 1 hours

Add new window template

Start	End	Duration	Notice before closure	Confidence	Min count	Max count	Tag (optional)
10:00	11:00	1 hour	0 minutes	Certain	1	1	
10:43	10:53	10 minutes	0 minutes	Certain	1	1	hello
14:00	15:00	1 hour	0 minutes	Certain	1	1	

Save

Cancel

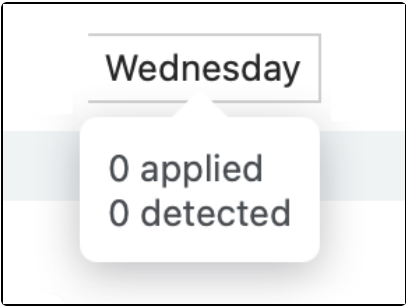
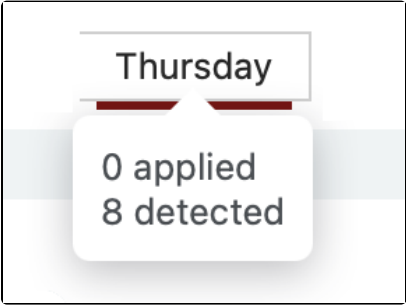
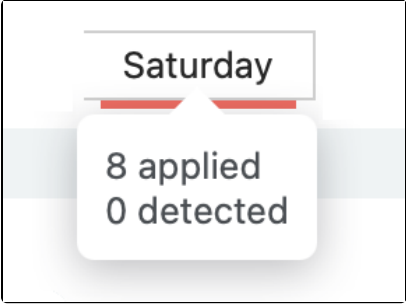
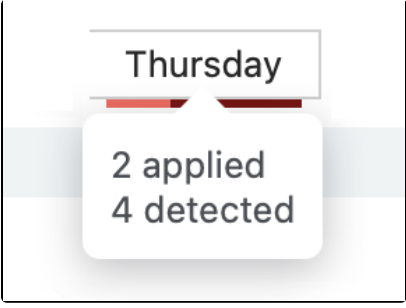
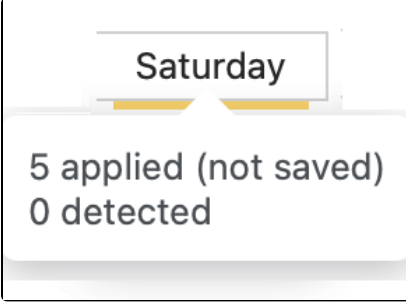
In addition to displaying the selected templates in the bottom section of the page, the colored line under the highlighted Friday tab has changed. The *Day tab colors* section describes the different colors used for the template combinations for each day.

You can continue to review the scan settings for different days of the week until all the detected templates have either been applied or reviewed and not applied. When you finish your selections, click **Save**. No changes are applied to the participant's window template settings until you click **Save**. After you **Save** your changes, the color bars for the associated days change to the associated colors for applied templates.

About day tab colors

The day of the week in the **Window settings** interface screen includes indicators to show the current state of **Window templates** for the selected participant. The day tabs' tooltips pop up when you mouse over them. Understanding the meaning of the colors can be helpful in knowing the current status of the file prediction window at a glance, as described below.

Color	Indicates
-------	-----------

 Wednesday 0 applied 0 detected	No Bar This day has no templates applied or detected for this participant.
 Thursday 0 applied 8 detected	Solid Dark Red Bar An MFT Operational Intelligence scan detected at least one new template for this day and participant, yet no templates have been applied.
 Saturday 8 applied 0 detected	Solid Light Orange Bar All templates detected from every scan to date have been applied for this day and participant.
 Thursday 2 applied 4 detected	Mixed Dark Red and Light Orange Bar Represents a mix of the two previous indicators. At least one template has been detected without being applied, and at least one template has been applied for the day and participant. The relative width of each section of the bar represents the ratio of new and detected not applied templates.
 Saturday 5 applied (not saved) 0 detected	Solid Yellow Bar All detected templates have been merged and applied (either new or previous templates), changes have been made to the template configuration (added, deleted, locked, or unlocked), and the changes have not yet been saved.

Friday

3 applied (not saved)
5 detected

Mixed Yellow and Light Brown Bar

The mix of yellow and light brown is similar to the description above for the solid yellow bar, where:

- At least one template is not applied
- At least one template was applied (either new or previously applied)
- Changes were made to the template configuration (added, deleted, locked, or unlocked)
- Changes were not saved

The width of each portion of the bar represents the ratio of applied/detected-not-applied templates.

About Window templates

The most important part of the **Window settings** interface is the bottom portion that displays the file arrival windows for the selected participant and day.

Time start: 00 : 00 Duration: 1 hours Add new window template

Start	End	Duration	Notice before closure	Confidence	Min count	Max count	Tag (optional)	
10:00	11:00	1 hour	0 minutes	Certain	1	1		
10:43	10:53	10 minutes	0 minutes	Certain	1	1	hello	
14:00	15:00	1 hour	0 minutes	Certain	1	1		

The following table sets out the key parameters of MFT OI **Window templates**:

Parameter	Description
Start	The time when the Windows template becomes active.
Duration	The number of hours for which the Windows template is active (default 1).
Notice before closure	The number of minutes before a window will be missed when the participant must be warned.
Confidence	Indicates the level of confidence in the repeatability of the detected pattern. Selections are: Low, Moderate, High, Very high, and Certain.
Min Count	The minimum number of expected files. Evaluation checks fail if this number of actual transfers is not attained.
Max Count	The maximum number of expected files. There is no check if this interval's maximum number of files is exceeded.
Tag (optional)	A keyword set for an expected file from a participant. Used when checking for a specific name of an expected file (or a sub-string thereof).

Modifying window templates

You can edit **window templates** once they have been applied. The editable fields are:

- Notice before closure
- Confidence
- Min count
- Max count
- Tag

The Duration set in minutes is now supported.

MFT OI does not let you define an illogical template by setting the **Minimum count** to be greater than the **Maximum count**:

Time start: 00 : 00 Duration: 1 hours Add new window template

10:00	11:00	1 hour	0 minutes	Certain	10	1		
10:43	10:53	10 minutes	0 minutes	Certain	1	1	hello	
14:00	15:00	1 hour	0 minutes	Certain	1	1		

On the right-hand side of the template, you can see a red icon to indicate an error in the definition. There is also an "undo" icon. Clicking **Undo** reverts the definition to the previously saved state.

Locking, unlocking, and deleting window templates

You can also change the “lock” status for a template. When a template is locked, it cannot be edited or modified by a new template. The importance of this last function, preventing changes from being modified by a new template, is explained below.

- To lock a template, click the padlock symbol () at the left of the template row.
- Locked templates display a red padlock ().

Window settings

SaveCancel

Participant: ST_RELAY

Day of week

Select: MondayTuesdayWednesdayThursdayFridaySaturdaySunday

All templates applied

Time start: 00 : 00Duration: 1hoursAdd new window template

Start	End	Duration	Notice before closure	Confidence	Min count	Max count	Tag (optional)	
 10:00	11:00	1 hour	0 minutes	Certain	1	10		
 10:43	10:53	10 minutes	0 minutes	Certain	1	1	hello	
 14:00	15:00	1 hour	0 minutes	Certain	1	1		

When you click the unlocked/locked icon for a template, the icon changes the icon to the other state. An unlocked icon becomes locked, and the locked icon changes to unlocked. You must click **Save** to apply changes to the lock status of any template. You can tell that the current changes in the image above have not been saved because the Day tab color is yellow (changes not saved). It changes back to the expected color after you click **Save**.

You can also remove the definition of any existing template. The trash/bin symbol () is to the right of the template row to delete a template that is no longer required.

 You can delete a locked template. The lock status does not prevent you from deleting a template.

When you click the icon to remove a template, Operational Intelligence grays out the template definition, reveals the undo icon, and adds an information mouse-over icon:

Window settings

SaveCancel

Participant: ST_RELAY

Day of week

Select: MondayTuesdayWednesdayThursdayFridaySaturdaySunday

All templates applied

Time start: 00 : 00Duration: 1hoursAdd new window template

 10:00	11:00	1 hour	0 minutes	Certain	1	10		
 10:43	10:53	10 minutes	0 minutes	Certain	1	1	hello	
14:00	15:00	1 hour	0 minutes	Certain	1	1		

This template will be deleted on save

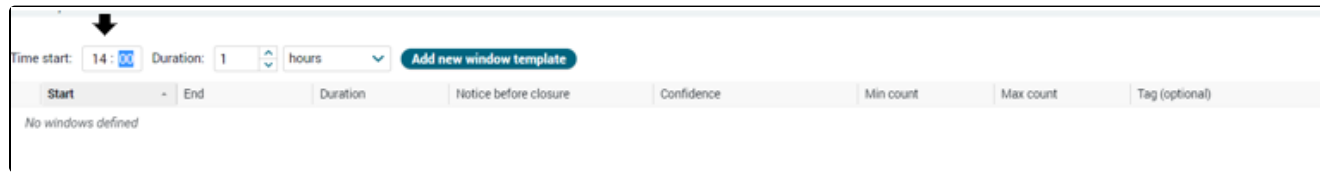
 To avoid receiving notifications about missed windows once a participant is no longer watched, the first step is to delete all the windows configured for that participant. Once completed, the next step is to stop watching the selected participant.

Manually creating and applying a window template

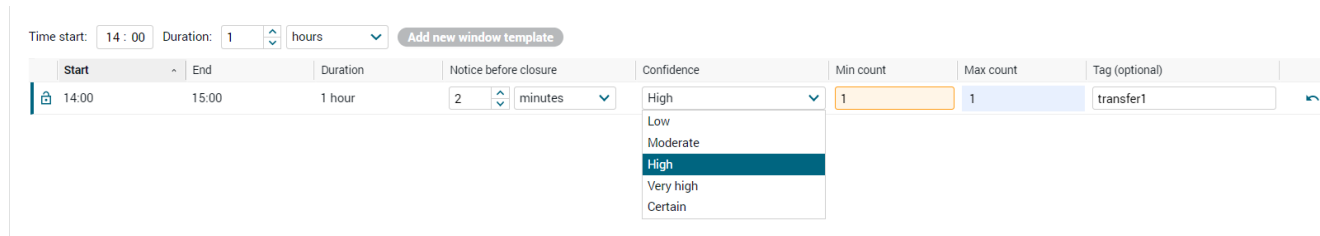
If the expected activity with a partner is already known/understood, it can bypass the need to wait for enough data to accrue for pattern detection and directly create and apply Window templates manually.

You can add a new window template directly from the window settings screen as follows:

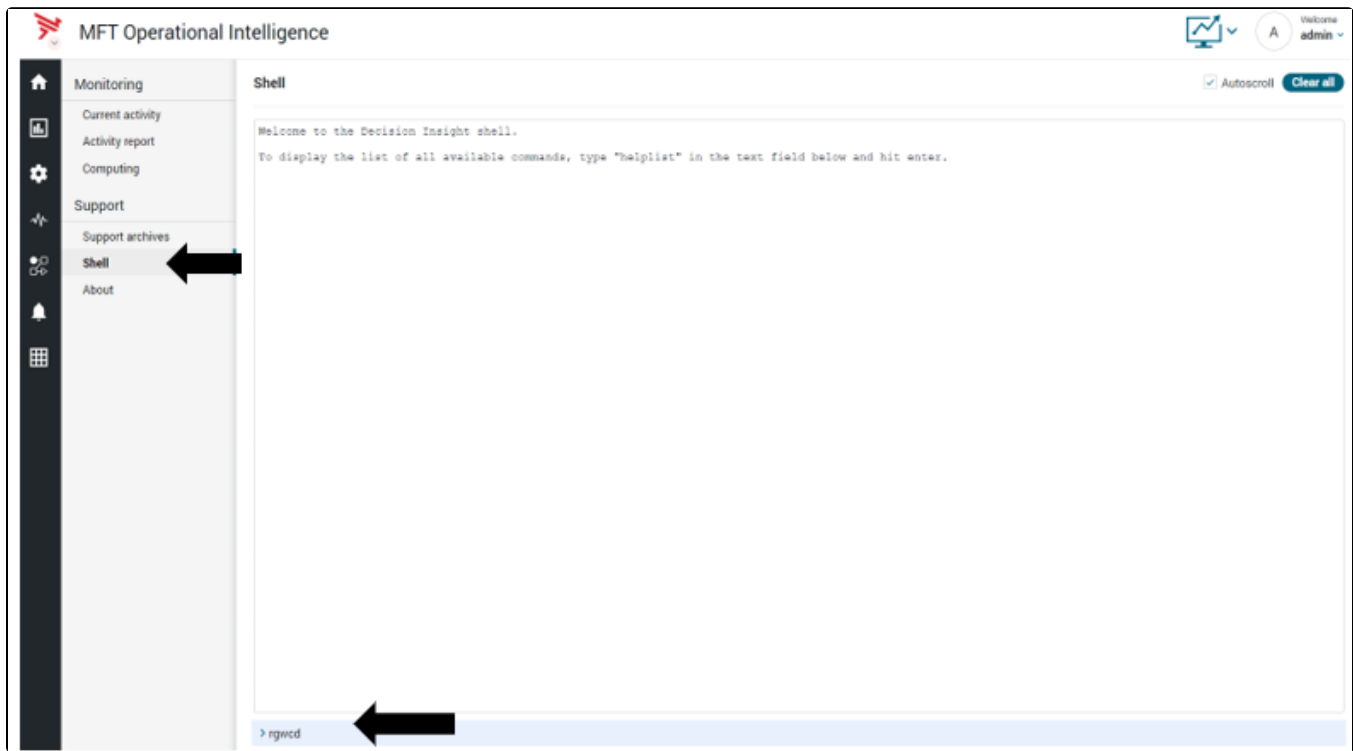
- Edit the hour portion of the Time start box:



- Click **Add new template**. MFT OI creates a new entry at the associated time with default values for Confidence, Min count, and Max count. You can edit these fields to match your definition:



- After you complete the definition, click Save to apply your changes. The new window will be visible the next day. Also, when you want to make some changes to a window, they are visible the next day.
- To make changes visible immediately, from the Monitoring and Support menu, select **Support > Shell**, and enter the command "rgwcd".
- You should run the shell command as needed when you add, edit, or delete a window template.



- The new windows are visible in the dashboard 04. Expected File Overview.

Using the lock status to prevent updates

One of the important functions of locking a Window template is to prevent new automatically-detected templates from overwriting the correct definition of the number of files expected. For example, consider this situation:

Day of week

Select:

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

A total of 1 unapplied template found.
Apply detected templates

Time start:

00 : 00

Duration:

1

hours

Add new window template

Start	End	Duration	Notice before closure	Confidence	Min count	Max count	Tag (optional)	
10:00	11:00	1 hour	0 minutes	Certain	1	10		
10:43	10:53	10 minutes	0 minutes	Certain	1	1	hello	
14:00	15:00	1 hour	0 minutes	Certain	1	1		

This participant has a window template defined for 10:00 with a minimum of 1 file expected and 10 maximum. When the admin user applies recently detected templates, the pop-up dialog box appears:

Apply scans

Applied templates

Interval	Confidence	Count
10:00 - 11:00	Certain	1 - 10
10:43 - 10:53	Certain	1 - 1
14:00 - 15:00	Certain	1 - 1

Merge selection

Scanned templates

Show identicals and locked

Interval	Confidence	Consistency	Count	Info
10:00 - 11:00	Certain	100 %	1 - 1	

Apply

Cancel

The new template definition for 10:00 has a maximum of 10 files. This is more than the business requirement of 1. If this update were merged with the existing template, it would overwrite the value that defines the business requirement.

How can you avoid this situation?

Lock the requirement that you know to be correct. When the template is locked, the Window setting screen looks like this:

Day of week

Select:

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

All templates applied

Time start:

10 : 43

Duration:

10

minutes

Add new window template

Start	End	Duration	Notice before closure	Confidence	Min count	Max count	Tag (optional)	
10:00	11:00	1 hour	0 minutes	Certain	1	10		
10:43	10:53	10 minutes	0 minutes	Certain	1	1	hello	
14:00	15:00	1 hour	0 minutes	Certain	1	1		

In this case, the option **Apply detected templates** is no more available:

Day of week

Select:

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

All templates applied

Time start:

00 : 00

Duration:

1

hours

Add new window template

Start	End	Duration	Notice before closure	Confidence	Min count	Max count	Tag (optional)	
10:00	11:00	1 hour	0 minutes	Certain	1	10		
10:43	10:53	10 minutes	0 minutes	Certain	1	1	hello	
14:00	15:00	1 hour	0 minutes	Certain	1	1		

The 10:00 to 11:00 window, as shown on the left, is locked. The newly discovered 10:00-11:00 template is not offered to merge with the templates to monitor the participant.

Enabling missed window notifications to dynamically assign email recipients

- Add one or more email addresses separated by a semicolon (;) to **UnitOwnerEmail**.

Review progress

This topic describes how to review your progress with MFT Operational Intelligence.

Reviewing how the first week has gone

In the section on [Planning Your first week](#), there is an example timeline set out. Look at the following and see how your progress lines up:

	Progress Checklist Item	Started	In Progress	Completed
1	MFT Operational Intelligence is installed.	☐	☐	☐
2	MFT OI is running, and dashboards are visible.	☐	☐	☐
3	Events from SecureTransport and Transfer CFT are being sent to MFT OI.	☐	☐	☐
4	Data from the events are visible on the dashboards.	☐	☐	☐
5	Become familiar with the navigation path from Global Overview through to Transfer Details, Product Summary, Participant Summary, or Expected File Summary patterns requiring attention.	☐	☐	☐
6	Information on transfers is reported accurately in the Transfer Summary, Exception Summary, and Transfer Details dashboards.	☐	☐	☐
7	Baselines, the line for Expected, and the shaded areas for Normal, Unusual, and Unexpected, are displayed on the dashboards.	☐	☐	☐
8	The configuration for Watched Participants and Watched Products succeeded appear.	☐	☐	☐
9	The counts for active Watched Participants and Watched Products are displayed on the Global Overview dashboard.	☐	☐	☐
10	After the first week, click the <i>Scan for all watched participants now</i> button in detected New Templates.	☐	☐	☐
11	File arrivals shown on the Expected File Windows Today dashboard are evaluated in terms of File Windows.	☐	☐	☐
12	The email configuration for Notifications is set, and Notifications are being sent out.	☐	☐	☐

Other topics for long-term success are:

- ☐ Secured the application access via HTTPS (recommended to do this during the initial deployment)
- ☐ Secured communications between MFT and MFT OI (using QLTS) see the section on Advance Features (recommended to do this during the initial deployment)
- ☐ Reviewed and updated the selection of Watched Participants (adding/removing)
- ☐ Reviewed and updated the selection of Watched Products (adding/removing)
- ☐ Reviewed and edited additional Expected File Transfer Windows for Watched Participants
- ☐ Becoming familiar with using Time Navigation and Time Tags to investigate a scenario across different dashboards

Validating results and getting support

Are there issues with your success on that list?

If you are having problems obtaining results, please refer to the [Frequently asked questions](#) section.

Getting support

If you still have questions after reviewing the FAQs, contact the [Axway Global Support team](#).

Notifications

MFT Operational Intelligence enables you to configure email notifications whenever there is a critical transition of a classifier state. To use the notifications function, perform the following steps:

1. Set the SMTP setting in the decision_insight.config file.
2. Configure the notifications.
3. Start the EmailNotification route in the Alerts space.

SMTP Settings

The MFT Operational Intelligence notifications require that you set an SMTP server and credentials.

```
com.axway.mftoi.smtp.address
com.axway.mftoi.smtp.password
com.axway.mftoi.smtp.username
```

These can be set either before installation or after:

- **Before Installation** - Add the values to the properties in the decision_insight.config file before you run the installer.
- **After Installation** - Add them directly to the platform.properties file in the Decision Insight conf directory. Then restart Decision Insight.

The smtp.address must include the protocol (a full URL) for the address. For example, smtp://<smtp server>:<smtp port>

SMTP Address Configuration

```
com.axway.mftoi.smtp.address=smtp://smtp.gmail.com:25
```

Notifications

MFT Operational Intelligence comes with five Notifications already set up, **InProcessTransfers**, **WatchedParticipantExceptions**, **WatchedProductExceptions**, **FailedTransfer**, and **MissedWindow**.

The following section details how to use a Notification.

Step	Action
1	To access the Notifications, click the Notification icon  in the left-hand menu.
2	Click on the Name of the notification you want to use
3	In the Details section, add an email address in the To field of the Notifiers section. This will set the recipient of the notification
4	(Optional) The email subject and message can also be set here by completing the Subject and Message fields Each notification comes with a default subject and message
5	(Optional) Additional attributes can be included in the email notification by clicking on the Add Attribute button to add them to the context. These attributes can then be added to the email message using curly brackets, for example {ParticipantName}
6	Once the configuration of the Notification is complete, click the start button  next to the Name of the Notification.



The triggering of the Notification is configured under the **Raise When** section. This determines what state transition will cause the Notification to be triggered, for example, from Normal to Unexpected or from Unusual to Unexpected.

EarlyWarning

This Notification is triggered at the time of a Window Closure **minus** the value contained in the **Notice before closure** field. This attribute indicates the number of minutes when the user wants to be warned before missing a window. Its value must be smaller than the time set for that window.

InProcessTransfers

This Notification is triggered if the number of in-progress transfers is above normal. It is configured to trigger when the state transitions from unusual to unexpected or from normal to unexpected. The InProcessCount and CompletedTransferCount attributes are included in the email message.

WatchedParticipantExceptions

This Notification will be triggered if the number of transfer exceptions for a Watched Participant is above normal. It is configured to trigger when the state transitions from normal to unusual or from normal to unexpected. The ParticipantName and ExceptionCount attributes are included in the email message.

 This Notification is designed only to send an email notification for watched participants and does not work if the Watched attribute is removed from the context.

WatchedProductExceptions

This Notification will be triggered if the number of transfer exceptions for a Watched Product is above normal. It is configured to trigger when the state transitions from normal to unusual or from normal to unexpected. The ProductInstance, ExceptionCount, and ProductType attributes are included in the email message.

 This Notification is designed only to send an email notification for watched products and does not work if the Watched attribute is removed from the context.

FailedTransfer

This notification is triggered if a transfer transitions to an exception status, for example, if a transfer does not successfully complete a flow. The email message contains relevant information about the transfer, such as CycleId, Flow, File name, Sender, and Receiver.

If a transfer fails, the SecureTransport server retries to send it 5 times consecutively. Each attempt is sent to MFTOI. To avoid creating 5 different entries with 5 different Cycle IDs, the closing time of failed transfers is set to 10 minutes. The notification email is sent after the flow's closure.

MissedWindow

This notification is triggered at the end of a window if the number of actual transfers is less than the expected minimum for that window and/or the tag set in that window does not match the file name expected. The email contains information about the window such as the id, start and end time, the actual and expected minimum transfer counts as well as the set tag and the number of transfers where this tag is matched.

In general, a successful window succeeds one or more successful closed transfers. However, there are a few exceptions. For the following transfers, they do not need to be closed for the window to be successful:

- On the sender, a transfer sent from a Transfer CFT server has to end in SENT or COMPLETED state during a window for it to be successful
- On the receiver, a transfer received by a Transfer CFT server has to end in a RECEIVED state during a window for it to be successful
- On the sender, a transfer sent from an ST server has to end in the SENT state during a window for it to be successful
- On the receiver, a transfer received by an ST server has to end in a RECEIVED state during a window for it to be successful.

EmailNotification Route

The notifications trigger the EmailNotification route and use the supplied SMTP settings to send out an email.

Follow these steps to get the EmailNotification route working

Step	Action
1	Select the Data Integration icon  in the left-hand menu
2	Select Routes under the Transformations heading on the left
3	Select Alerts in the space dropdown
4	Click the start button  next to the EmailNotification route

After a server restart

Should the MFT OI application have been restarted either by the underlying DecisionInsight platform or the server it is running on being restarted, even to load a new configuration, the steps to start the Notifications and EmailNotification Route need to be reapplied - restarted.

You can change the configuration to remove these additional steps by selecting the **Start with node** option for each **Notification** and clicking **Save**.

Step	Action
1	To access the Notifications, click on the Notification icon  on the left-hand menu.
2	Click the Name of the notification to use.
3	Click the Start with node radio button next to Options under the Key of the Notification.
4	Click Save .
5	Once the configuration of the Notification is complete, click the start button  next to the Name of the Notification

MFT Operational Intelligence
Welcome admin

[Global Overview](#)
[Transfer Summary](#)
[Exceptions Summary](#)
[Flow Overview](#)
[Expected File Overview](#)
[Participant Overview](#)
[Product Overview](#)

Notifications

Add

Details

Save Cancel

Name

EarlyWarning

FailedTransfer

InProcessTransfers

MissedWindow

WatchedParticipantExce

WatchedProductExcepti

Name*: EarlyWarning

Key: EarlyWarning

Options: ☒ Manual start ☒ Start with node

Classifier: Closurenoticestatus as Closure notice status of Window at instant

Context: closureDuration as closureDuration of Window at instant format

Add attribute

Above context attributes values can be referenced inside a notifier fields using their alias between braces, like {alias}

Raise when

Icon	Notifier
☒	SNMP
☒	Email

Message: An expected activity window is due to close in {closureDuration} and the minimum number of expected

To: info@SW2RDAPP4768.pcloud.axway.int;
webmaster@SW2RDAPP4768.pcloud.axway.int

Subject: Early Warning - {closureDuration} before Window is Missed

Message: An expected activity window is due to close in {closureDuration} and the minimum number of expected

This step would also need to be applied to the EmailNotification Route:

Step	Action
1	 Select the Data Integration icon in the left-hand menu
2	Select Routes under the Transformations heading on the left
3	Select Alerts in the space dropdown
4	Check the Route is started  (or start the route as per the steps above)
5	Click the start with a node radio button next to the EmailNotification route
6	Click Save

```
<?xml version="1.0" encoding="UTF-8"?>
<routes xmlns="http://camel.apache.org/schema/spring" xmlns:u="http://www.systar.com/aluminium/camel-util">

  <route>
    <!-- Start Route - Set last restart DateTime-->
    <from uri="timer://initConsumeTrackedObject?repeatCount=1"/>
    <setHeader name="dtLastRestart">
      <simple>${date:now}</simple>
    </setHeader>
    <log loggingLevel="((LogLevelA))" message="EmailNotification Route Started at: ${headers[dtLastRestart]}/">
  </route>

  <route>
    <!-- For testing. Allows injection of test messages -->
    <from uri="direct:InjectMessage"/>
    <log message="Message injected \nMessage Body:\n${body}"/>
    <unmarshal>
      <csv delimiter="," skipHeaderRecord="true" useMaps="true"/>
    </unmarshal>
    <split>
      <simple>${body}</simple>
      <to uri="direct:SendEmail"/>
    </split>
  </route>

  <route>
    <from uri="tnd-notifier:Email"/>
    <log loggingLevel="((LogLevelA))" message="EmailNotification Triggered ${body}"/>

    <choice>
```

Advanced features

This section provides details for users that require additional options from the standard installation.

- [Platform properties](#)
- [SecureTransport and Transfer CFT secure communications](#)
- [Configure HTTPS communication](#)
- [Standardize time zones for all dashboard users](#)
 - [Before the installation](#)
 - [After MFT OI is installed](#)

Platform properties

MFT Operational Intelligence runs on Axway's analytics platform, Decision Insight. Some features you may wish to change are maintained in the Decision Insight `platform.properties` file. This file is in the `conf` directory under the **install/node_*** directory.

This file controls several features of MFT OI. After making changes to any values in the properties file, you will need to stop and restart Decision Insight. See [the FAQs > How do I stop and start MFT OI?](#) to learn how to stop and restart the MFT OI application.

SecureTransport and Transfer CFT secure communications



Secure communication is highly recommended.

The page on [Connect SecureTransport and Transfer CFT to MFT Operational Intelligence](#) provides steps that must be followed to deliver the transfer updates to MFT OI.

You can configure secure communications from Transfer CFT or SecureTransport in MFT OI.

To enable qtls, you must make changes to several entries in the **platform.properties** file in the MFT OI installation path:

- `com.axway.mftoi.qlt.url`: reference the qtls protocol instead of qlt
- `com.axway.mftoi.qlt.keystore.path`: set the path to the JKS Keystore
- `com.axway.mftoi.qlt.keystore.password`: password to use to open Keystore
- `com.axway.mftoi.qlt.keystore.keyPassword`: password to use to open key in Keystore
- `com.axway.mftoi.qlt.truststore.path`: path to the JKS truststore
- `com.axway.mftoi.qlt.truststore.password`: password to open truststore
- `com.axway.mftoi.qlt.cipherSuites` and `com.axway.mftoi.qlt.secureSocketProtocols`: Adapt as needed (empty value will use the platform default secured values)

After making these changes, stop and then restart the platform for the changes to be applied. (See [the FAQs > How do I stop and start MFT OI?](#) to learn how to stop and restart the MFT OI application.)



These changes can be applied before installing MFT OI by adding these values to the `decision_insight.config` file. The installer will then add them to the `platform.properties` file during the deployment of the MFT OI application.

If you require more information on securing the communication channel, if you are migrating from using Sentinel or wish to use the Sentinel Event Router, please see the [Getting EventRouter Setup to work with the MFT Operational Intelligence](#) subpage.

Configure HTTPS communication

To enable secure communication over HTTP, you must change several entries in the `platform.properties` file. By default, that section displays as follows (the line numbers reflect their position in the file):

```
4.      # Specify the listening TCP port for HTTP request
5.      org.apache.felix.http.enable=true
6.      org.osgi.service.http.port=8080
7.      # Specify the listening TCP port and the keystore for HTTPS request
8.      org.apache.felix.https.enable=false
9.      org.osgi.service.http.port.secure=8443
10.     org.apache.felix.https.keystore=changeit
11.     org.apache.felix.https.keystore.password=changeit
12.     org.apache.felix.https.keystore.key.password=changeit
```

To enable secure communication:

- line 8: change the `https.enable` flag to `true`
- line 10: specify the path to the Keystore
- line 11: enter the password to the Keystore
- line 12: enter the password of the key to the Keystore

If you wish to require that all users use https, you need to disable the HTTP access:

- line 5: set the `http` flag to `false`.

After making the changes and saving the file, stop and restart Decision Insight (see [the FAQs](#)) to implement the configuration changes in the application. Once restarted, the https interface will be active.

You can find additional information, if required, in the [online documentation](#).



These changes can be applied before installing MFT OI by adding these values to the `decision_insight.config` file. The installer will then add them to the `platform.properties` file during the deployment of the MFT OI application when the choice to secure communications is chosen during the execution of the installer.

Standardize time zones for all dashboard users

As described in [the FAQs](#) > *Why does MFT OI care about date, time, and time zone settings*, if time zones for dashboard users and the time zone settings for the MFT OI server are different, you may want to configure MFT OI to use the server time zone for the display of dashboards for all users.

You can make this change before or after the installation process by adding this property:

```
com.systar.carbon.dashboard.server.timezone=true
```

Before the installation

If you have not completed the MFT OI installation, once the `mft_oi_install.zip` file is expanded, add the property as the last line in the `decision_insight.config` file. You will find the file in the **install** directory. Once you have made the change, you can continue with the installation.

After MFT OI is installed

If you have completed the MFT OI installation, add the property that changes the dashboard server time zone at the end of the `platform.properties` file. That file is located in the **install** directory under the directory named **node_YYYYMMDD** (where YYYYMMDD is a date). Under the **node** directory is the subdirectory **conf**. The `platform.properties` file is located in this directory.

After making the changes and saving the file, stop and restart MFT OI. See [the FAQs](#) > *How do I stop and start MFT OI?* to implement the configuration changes in the application. Once restarted, all users will see the information presented in the dashboards based on the server's time zone setting.

You can find additional information in the [online documentation](#).

Set up the Event Router with MFT OI

This section describes configuring the Event Router to allow events routed from Axway MFT products SecureTransport, Transfer CFT, and Flow Manager through the Event Router to MFT OI.

EventRouter can dispatch events to one or several targets and control the type of events sent and in which mode.

For MFT product details, refer to the following documents:

- https://docs.axway.com/bundle/FlowManager_20_allOS_en_HTML5/page/sentinel.html
- https://docs.axway.com/bundle/TransferCFT_38_UsersGuide_allOS_en_HTML5/page/Content/uconf/uconf_sentinel.htm
- https://docs.axway.com/bundle/TransferCFT_38_UsersGuide_allOS_en_HTML5/page/Content/interop/sentinel_ssl.htm
- https://docs.axway.com/bundle/SecureTransport_55_AdministratorGuide_allOS_en_HTML5/page/Content/AdministratorsGuide/setup/t_st_Sentinel.htm
- https://docs.axway.com/bundle/MFT_Operation_Intelligence_019_en_HTML5/page/advanced_features.html

Most scenarios are described, and sample setups are provided:

- EventRouter sends events to multiple targets (for example, Sentinel and MFT OI)
- EventRouter receiving QLTs events
- EventRouter receiving non-SSL QLT events
- EventRouter sending QLT events to target(s)
- EventRouter sending QLTs event to target(s)
- EventRouter uses mutual authentication to target

Install and deploy the Event Router

Deployment Architecture

EventRouter is used to dispatch events to one or several targets. If MFT OI is added to an existing or new MFT environment, EventRouter is typically used to send events to the existing monitoring solution (for example, Sentinel or EA4ST) and the new MFT OI application.

EventRouter can be installed close to the reporting products (for example, SecureTransport or CFT), or it can be installed close to the monitoring product (for example, Sentinel or MFT OI).

For MFT environments with existing monitoring solutions (for example, Sentinel is already deployed), the least impactful architecture is to install EventRouter on the same server as Sentinel with the same listening port and set of certificates as Sentinel. This means no changes have to be made to the existing MFT products.

Installation

EventRouter can be installed without the SSL option and reconfigured afterward to allow SSL connectivity.

The installation is not part of this document. We will assume that EventRouter is already installed in non-SSL mode and functional.

Refer to the Event Router installation guide at <https://support.axway.com/en/documents/document-details/id/1432287>

Certificate management

Ideally, when replacing the Sentinel integration point with EventRouter, the same certificates used in Sentinel should be imported into EventRouter. That guarantees no new certificates have to be imported into the reporting MFT products.

The following page explains how to extract those certificates from Sentinel.



You can skip this step if you would like to use new certificates.

Extract certificates from Sentinel Keystores

To extract certificates from the existing Sentinel installation where <Sentinel> is the installation path of Sentinel, follow these steps:

Step 1

Locate the Keystore and truststore used in Sentinel by checking the conf/trkserver.xml file:

```
more <Sentinel>/conf/trkserver.xml | grep jks
<filename>/opt/axwy/Sentinel/conf/security/keystore.jks</filename>
<filename>/opt/axwy/Sentinel/conf/security/truststoreSS0.jks</filename>
```

Step 2

Export user certificate from the Sentinel Keystore:

```
keytool -importkeystore -srckeystore <Sentinel>/conf/security/keystore.jks -destkeystore ssl_user_cert.p12 -srcstoretype JKS -deststoretype PKCS12 -deststorepass axway*
```

Once you run the command, you are prompted for your Keystore password.

Step 3

If you have multiple Certificate Authorities (CAs) in your truststore, identify the alias of the CA certificate that was used to sign the user certificate by running:

```
keytool -list -v -keystore <Sentinel>/conf/security/keystore.jks
```

Look for the issuer, for example:

```
Issuer: CN=PassPort, OU=R&D, O=Axway, L=Bucharest, C=RO
```

Then list the truststore with:

```
keytool -list -v -keystore <Sentinel>/conf/security/truststoreSS0.jks
```

Find the CA alias by looking for the owner (matching the issuer from above):

```
Alias name: passport
```

```
Creation date: Mar 25, 2019
```

```
Entry type: trustedCertEntry
```

```
Owner: CN=PassPort, OU=R&D, O=Axway, L=Bucharest, C=RO
```

Step 4

Export the CA certificate of the truststore as PKCS12 (using the alias from step 3)

```
keytool -importkeystore -srckeystore <Sentinel>/conf/security/truststoreSS0.jks -destkeystore sentinel-truststore.p12 -srcalias passport -srcstoretype JKS -deststoretype pkcs12
```

You are prompted for the password of the Sentinel truststore.jks file and the new p12 file.

Step 5

Convert the p12 CA file into DER:

```
openssl pkcs12 -in sentinel-truststore.p12 -out ssl_ca_cert.pem  
openssl x509 -in ssl_ca_cert.pem -out ssl_ca_cert.der -outform DER
```

You should now have the two files generated:

- ssl_user_cert.p12
- ssl_ca_cert.der

Generate an encryption key in the Event Router

The Event Router utility **agtcrypt** allows the encrypting of confidential information used by Event Router. This setup encrypts the password for the private key associated with the user certificate.

This section describes how to generate the encryption key (step 1) and then encrypt the certificate password (step 2) of the user certificate password.

The **agtcrypt** utility is located in the EventRouter binary directory.

Step 1

Generate an encryption key:


```
agtcrypt --genkey --keyfname $trk_home_dir/conf/crypt.key --saltfname $trk_home_dir/conf/crypt.salt --pass <PASSWORD>
```

Replace <PASSWORD> with a password of your choice.



The password must be at least 8 characters long, contain upper and lower case characters, at least one numeric character, and contain at least one of the special characters @#\$%.

This password is used to generate the encryption key.

Step 2

Encrypt certificate password:

```
agtcrypt --encrypt --keyfname $trk_home_dir/conf/crypt.key --text <P12 Password> --textfname $trk_home_dir/conf/ssl_user_cert.pw
```

Replace <P12 Password> with the password you want to encrypt; in this case, the password used for the user certificate is in p12 format.

The encrypted password is now saved in \$trk_home_dir/conf/ssl_user_cert.pw

You have to configure MFT OI to allow secure communication from EventRouter. If no Keystore or truststore exists for MFT OI, you must create them in steps 1 and 2.

Generate Keystore and Truststore for MFT OI

A keystore and truststore must be imported into MFT OI to enable SSL communication. If no Keystore is present, generate a self-signed server certificate and import it into a Keystore and truststore. The generated files are used in the section Setup MFT OI for QLTs.

Step 1

Create a Keystore that contains the server certificate

```
keytool -genkey -alias MFT-OI -keyalg RSA -keypass <PASSWORD> -storepass <PASSWORD> -keystore MFT-OI-keystore.jks
```

Replace <PASSWORD> with a password of your choice.

Export the certificate into a .cer file

```
keytool -export -alias MFT-OI -storepass <PASSWORD> -file server.cer -keystore MFT-OI-keystore.jks
```

Replace <PASSWORD> with the Keystore password.

This generates two files:

- MFT OI-keystore.jks
- server.cer

Step 2

Add the server certificate to a truststore that contains the CA of the server certificate

```
keytool -import -v -trustcacerts -alias MFT-OI -file server.cer -keystore MFT-OI-truststore.jks -keypass <PASSWORD> -storepass <PASSWORD>
```

Replace the <PASSWORD> entries with their respective passwords for the keypass and storepass as used in step 1.

This generates the file: MFT-OI-truststore.jks

Step 3

Export the CA certificate of the truststore as PKCS12

```
keytool -importkeystore -srckeystore MFT-OI-truststore.jks -destkeystore MFT-OI-truststore.p12 -srcalias MFT-OI -srcstoretype jks -deststoretype pkcs12
```

You are prompted for the password of the MFT-OLtruststore.jks file and the new p12 file.

Step 4

Convert the p12 CA file into PEM:

```
openssl pkcs12 -in MFT-OLtruststore.p12 -out MFT-OI_CA.pem
```

Step 5

Convert the PEM CA file into DER:

```
openssl x509 -in MFT-OI_CA.pem -out MFT-OI_CA.der -outform DER
```

This generates the file: MFT OI_CA.der

Import EventRouter CA in MFT OI

If mutual authentication between EventRouter and MFT OI is required, the CA of the client (in this case EventRouter) must be imported into the truststore of the server (MFT OI).

Switch to the MFT OI server, and follow the steps below:

If keytool is not installed on the server, one can be found at the location: <MFT OI_install_dir>/node_<id>/product/DecisionInsight_<id>/lib/jre/bin

Ensure the certificate ssl_ca_cert.der and the truststore MFT-OLtruststore.jks are located on the MFT OI server.

```
keytool -import -trustcacerts -alias ER_CA -file ssl_ca_cert.der -keystore MFT-OLtruststore.jks
```

You are prompted for the password of the MFT-OLtruststore.jks file.

Set up the Event Router

Configure SSL

Assuming the Event Router is installed in non-SSL mode, a few things must be configured to enable SSL. The steps might differ depending on the Event Router sending and/or receiving in SSL mode.

For both cases, modify *conf/trkagent.ini* to point to the SSL definition file and the encryption key generated in the previous chapter.

The installation path in each environment might look different.

```
[AGENT]
[...]
encrypt_key_file="/opt/axway/SentinelEventRouter/conf/crypt.key"
security_profile_file="/opt/axway/SentinelEventRouter/conf/sslconf.ini"
[...]
```

Receiving QLTs

To set the Event Router to listen on an SSL port, modify *conf/trkagent.ini* as follows:

```
[TCPSOURCE]
[...]
sap=0
sapssl=<nnnn>
profile=ERSERVER
[...]
```

Replace <nnnn> with the server listening port. If replacing Sentinel, this is typically 1303.

If no SSL is required, set the value sap="<no SSL listening port>". This is typically 1305 or 1325.

Modify *conf/sslconf.ini* file to import the certificates used by EventRouter to receive an SSL connection from the reporting product.

Modify the section for `ERSERVER` (or the name set in the `TCPSOURCE` section from the file above).

```
[ERSERVER]
SSL_USER_CERTIFICATE_FILE = $trk_home_dir/conf/ssl_user_cert.p12
SSL_USER_CERTIFICATE_FORMAT = PKCS12
SSL_USER_CERTIFICATE_PASSWORD_FILE = $trk_home_dir/conf/ssl_user_cert.pw
SSL_CA_CERTIFICATE_FILE = $trk_home_dir/conf/ssl_ca_cert.der
SSL_CA_CERTIFICATE_FORMAT = DER
SSL_VERIFY_POLICY = optional
SSL_CIPHER_SUITE = 49199,156,157,49191,60,61
SSL_VERSION_MIN = TLS_1.2
```

The two certificates `ssl_user_cert.p12` and `ssl_ca_cert.der` are the ones created in the section `Extract Certificates from Sentinel Keystores`. If Sentinel certificates are not used, any other user certificate and CA can be imported here. `ssl_user_cert.pw` is the encrypted password generated in chapter 3.2. Generate the Encryption Key in EventRouter above.

The reference to cipher suits and numbers can be found in the Addendum of this document.

Supported ciphers for each product and version of Transfer CFT, Sentinel, SecureTransport, and MFT Operational Intelligence can be found in the official product guides or respective configuration parameters for each product.



If EventRouter is installed on the same server as Sentinel and should replace its listening port, make sure to update the Sentinel configuration to change the listening port to avoid any port conflicts. Locate the listening ports in `<Sentinel>/conf/trkserver.xml`:

For SSL listening port:

```
<Service activate="true" host="<Sentinel host>" id="QLT-XML" poolSize="10"
port="1303">
[...]
```

For a non-SSL listening port:

```
<Service activate="true" host="<Sentinel host>" id="AUTO" poolSize="50"
port="1305">
[...]
```

Restart Sentinel after changes are made:

```
./stopserver
./startserver -b
```

Sending QLTs

To set the Event Router to send via SSL to the default target, modify `conf/trkagent.ini` as follows:

```
[defaulttarget]
[...]
```

If `ssl` is set to "yes," Event Router sends via SSL to the default target. The default target can be Sentinel or MFT OI.

If you have multiple targets, continue to set up as described in the section `Multiple targets`.

If ssl is set to “no”, EventRouter sends via non-SSL to the default target. You can still send via SSL to additional targets if this value is set to “no” as described in section 4.2.1. SSL target.

Now modify **conf/sslconf.ini** file to import the CA certificate from the target that is used by EventRouter to establish an SSL connection with the target.

This is the public certificate of the truststore created in the section Generate Keystore and Truststore for MFT OI (step 5) in DER format.

Modify the section for SENTINEL (or create a new profile name).

```
[SENTINEL]
SSL_CA_CERTIFICATE_FILE = $trk_home_dir/conf/MFT_OI_CA.der
SSL_CA_CERTIFICATE_FORMAT = DER
SSL_CIPHER_SUITE = 49199,156,157,49191,60,61
SSL_VERSION_MIN = TLS_1.2
```

The reference to cipher suits and numbers can be found in the Addendum of this document. Supported ciphers for each product and version of Transfer CFT, Sentinel, SecureTransport, and MFT OI can be found in the official product guides or respective configuration parameters for each product.

If the receiving server requires mutual authentication, a user certificate will need to be added as well:

```
SSL_USER_CERTIFICATE_FILE = $trk_home_dir/conf/ssl_user_cert.p12
SSL_USER_CERTIFICATE_FORMAT = PKCS12
SSL_USER_CERTIFICATE_PASSWORD_FILE = $trk_home_dir/conf/ssl_user_cert.pw
```



If you use mutual authentication, make sure to import the CA of your user certificate in the target's truststore.

Set up a target

The targets for EventRouter are defined in the **conf/target.xml** file. By default, one target with the name “DEFAULT” is set up. Details of this target are configured in the [defaulttarget] section of the conf/trkagent.ini file.

SSL target

If the [defaulttarget] profile in **conf/trkagent.ini** is set up with the option ssl=yes (as shown in the section Sending QLTs).

EventRouter will automatically use an SSL connection to send events to the default target, even if not specified in the **conf/target.xml** file.

```
<TrkEventRouterCfg>
  <TrkXml version="1.0" />
  <EventRouter name="DEFAULT">
  </EventRouter>
  <Target name="DEFAULT" defaultXntf="yes" defaultXml="yes">
  </Target>
</TrkEventRouterCfg>
```

When adding additional targets to the EventRouter configuration, make sure to include the option ssl="yes" and profile="<SECURITY PROFILE>" in the <Access> element of the target definition in the **conf/target.xml** file.

<SECURITY PROFILE> should be replaced with the section name defined in the security profile file (**conf/sslconf.ini**), e.g:

```
<TrkEventRouterCfg>
  <TrkXml version="1.0" />
  <EventRouter name="DEFAULT">
  </EventRouter>
  <Target name="DEFAULT" defaultXntf="yes" defaultXml="yes">
  </Target>
  <Target name="OI" defaultXntf="yes" defaultXml="yes">
  <Access addr="OI.corp.com" port="1315" ssl="yes" profile="SENTINEL"/>
  </Target>
</TrkEventRouterCfg>
```

Multiple targets

To send events to multiple targets, add additional target definitions to the file **conf/target.xml** by using the element.

This example shows how to add two additional targets, “OI_PROD” using SSL profile “Sentinel” and “OI_DEV” using no SSL.

```
<TrkEventRouterCfg>
  <TrkXml version="1.0" />
  <EventRouter name="DEFAULT">
  </EventRouter>
  <Target name="DEFAULT" defaultXntf="yes" defaultXml="yes">
  </Target>
  <Target name="OI_PROD" defaultXntf="yes" defaultXml="yes">
  <Access addr="MFT OI.prod.com" port="1303" ssl="yes"
  profile="SENTINEL"/>
  </Target>
  <Target name="OI_DEV" defaultXntf="yes" defaultXml="yes">
  <Access addr="MFT OI.dev.com" port="1305" ssl="no"/>
  </Target>
</TrkEventRouterCfg>
```

For details on how to set multiple targets, consult the EventRouter User Guide “About setting the Target Parameters” and “Target Parameters”

Exclude Tracked Objects

MFT OI consumes only events coming from the Tracked Object “XFBTRANSFER.” Sometimes, Transfer CFT is configured to send not only XFBTRANSFER events but also XFBLOG events.

You can configure the EventRouter to not send events from the Tracked Object XFBLOG to a specific target.

Change the **target.xml** file to include this condition:

```
<TrkEventRouterCfg>
  <TrkXml version="1.0" />
  <EventRouter name="DEFAULT">
  </EventRouter>
  <Target>
  [...]
  </Target>
  <Route object="XFBTRANSFER" default_Notify="NotifyIf">
  </Route>
  <Route object="XFBLOG" default_Notify="NotNotifyIf">
  <Condition notify="NotNotifyIf" target="OI" if="[CycleId]NOT' '>
  </Condition>
  </Route>
</TrkEventRouterCfg>
```

If multiple targets are defined, you can add a new Condition tag for each target.

Configure Event Router for large-volume events

In many cases, the Event Router receives a lot of events. To increase the capacity of the Event Router, you can increase the number of allowed incoming connections to the Event Router and increase its own buffer file.

Change the max_message value in the [defaulttarget] section of the **trkagent.ini** file to increase the buffer file:

```
max_messages=50000000
```

Change the incoming_max value in the [TCPSOURCE] section of the trkagent.ini file to increase the number of allowed connections to the Event Router:

```
incoming_max=250
```

Regenerate the configuration

If any of the configuration files have been modified, it is necessary to regenerate the configuration as follows:

```
agtcmd stop
agtcmd -setup
agtcmd start
```

Verify target connectivity

To verify the target definitions are loaded correctly, run:

```
agtcmd display
```

To force a connection to the targets to check the connectivity even without incoming events:

```
agtcmd force -t default
agtcmd force -t <additional target name>
```

Replace <additional target name> with the target name defined in **conf/target.xml**.

Set up QLTs

MFT OI has to be configured to allow secure communication from EventRouter. **This is configured on the MFT OI server**, in the file system, and in the User Interface (web page).

If no keystore or truststore exists for MFT OI, you have to create them as described in the section Generate Keystore and Truststore for MFT OI.

To enable QLTs, make the following changes in the **<MFT OI Installation path>/conf/platform.properties** file:

```
com.axway.mftoi.qlt.url=qlts:0.0.0.0:1303?sslContextParameters=#qltSslContextParameters
com.axway.mftoi.qlt.keystore.path=${com.systar.platform.conf.dir}/MFT_OIkeyStore.jks
com.axway.mftoi.qlt.keystore.password=<KEYSTORE_PASSWORD>
com.axway.mftoi.qlt.keystore.keyPassword=<KEY_PASSWORD>
com.axway.mftoi.qlt.truststore.path=${com.systar.platform.conf.dir}/MFT_OItrustStore.jks
com.axway.mftoi.qlt.truststore.password=<TRUSTSTORE_PASSWORD>
```

Stop the MFT OI platform and then start it back up again to reload the configuration. (See [the FAQs > How do I stop and start MFT OI?](#)).



This configuration can be established before the MFT OI is installed by configuring these details in the decision_insight.config file, which is used to configure the platform.properties file during deployment of the MFT OI application.

Require mutual authentication

If mutual authentication between EventRouter and MFT OI is required, the CA of the client (in this case, the Event Router) must be imported into the truststore of the server (MFT OI).

This is explained in section 3.4, Import EventRouter CA in MFT OI.

To enforce mutual authentication in MFT OI, the MFT OI application must be running.

Login to the MFT OI UI; the web address configured during installation, for example, <http://<address including port number>>.

Access the Data Integration pages in the left pane.



MFT Operational Intelligence

Endpoints

Connectors

Mappings

Libraries

Events

Queries

Notifiers

Data integration

Automation

Triggers

Transformations

Routes

States

Resources

Properties

Runtime

Logs

Connectors Add

In space

Alerts

Alerts

Analysis

Classifiers

DynamicInstances

Initializers

Instances

Integration

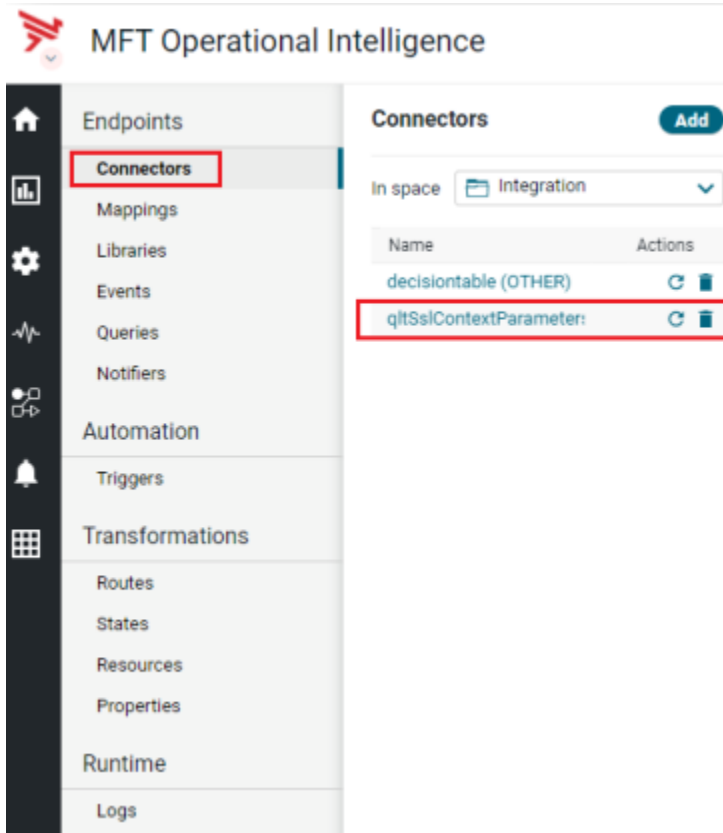
Model

Rhythms

Name

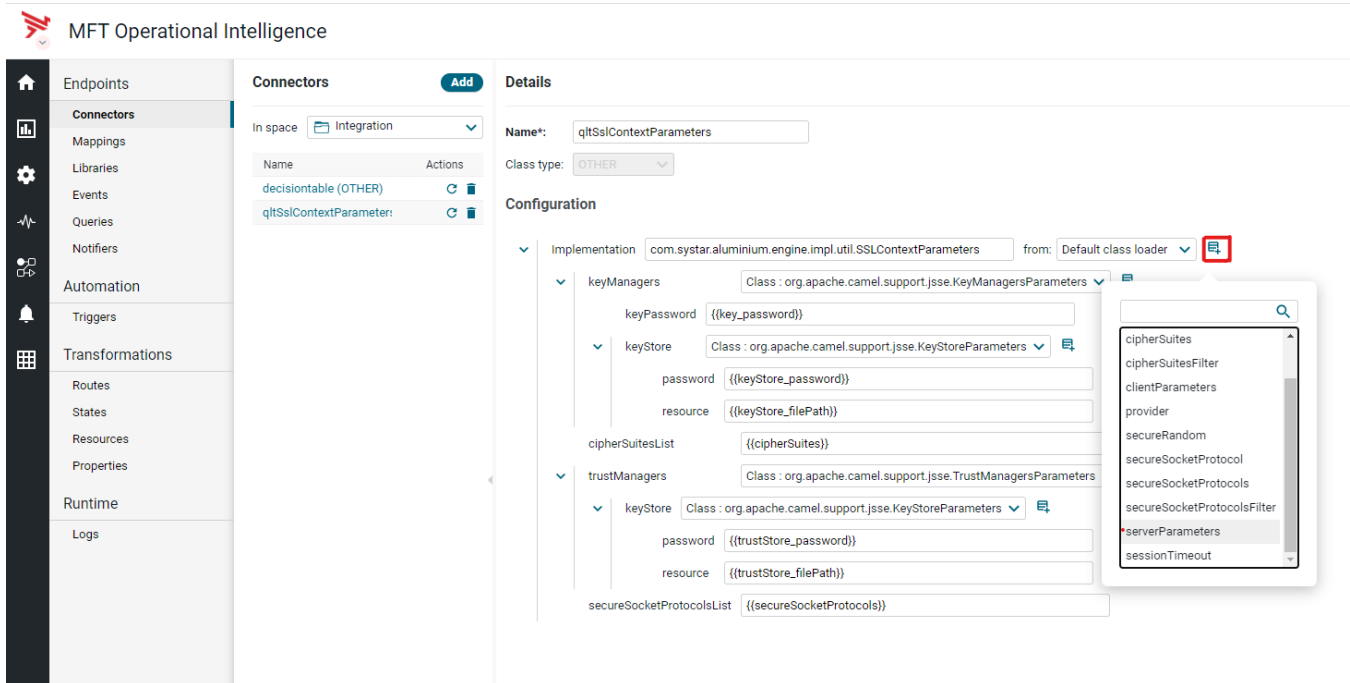
No item

Browse to Endpoints > Connectors > In space: Integration



The majority of the configuration already exists, but Mutual Authentication is not required for all, so this must be updated as required.

To update the connector **qItSslContextParameters** with the additional setting, click the top right add icon (list with a +) and select serverParameters:



Update the connector qItSslContextParameters with the additional serverParameters "clientAuthentication."

Details

Name*:

Class type: OTHER ▼

Configuration

Implementation com.systar.aluminium.engine.impl.util.SSLContextParameters from: Default class loader ▼ ⓘ

keyManagers Class : org.apache.camel.support.jsse.KeyManagersParameters ▼ ⓘ

keyPassword

keyStore Class : org.apache.camel.support.jsse.KeyStoreParameters ▼ ⓘ

password

resource

cipherSuitesList

trustManagers Class : org.apache.camel.support.jsse.TrustManagersParameters ▼ ⓘ

keyStore Class : org.apache.camel.support.jsse.KeyStoreParameters ▼ ⓘ

password

resource

secureSocketProtocolsList

serverParameters Class : org.apache.camel.support.jsse.SSLContextServerParameters ▼ ⓘ

certAlias
cipherSuites
cipherSuitesFilter
clientParameters
provider
secureRandom
secureSocketProtocol
secureSocketProtocols
secureSocketProtocolsFilter
sessionTimeout

The ServerParameters are automatically filled as above, but the parameter must be added. Click the bottom right add icon (list with a +) and select "clientAuthentication" from the list.

Details

Name*:

Class type:

Configuration

Implementation

com.systar.aluminium.engine.impl.util.SSLContextParameters

from: Default class loader

keyManagers

Class : org.apache.camel.support.jsse.KeyManagersParameters

keyPassword

{{key_password}}

keyStore

Class : org.apache.camel.support.jsse.KeyStoreParameters

password

{{keyStore_password}}

resource

{{keyStore_filePath}}

cipherSuitesList

{{cipherSuites}}

trustManagers

Class : org.apache.camel.support.jsse.TrustManagersParameters

keyStore

Class : org.apache.camel.support.jsse.KeyStoreParameters

password

{{trustStore_password}}

resource

{{trustStore_filePath}}

secureSocketProtocolsList

{{secureSocketProtocols}}

serverParameters

Class : org.apache.camel.support.jsse.SSLContextServerParameters

camelContext

cipherSuites

cipherSuitesFilter

clientAuthentication

secureSocketProtocols

secureSocketProtocolsFilter

sessionTimeout

An additional text box for the clientAuthentication displays to set this value.

Available values are:

- NONE: No client authentication is required or requested.
- WANT: Client authentication requested.
- REQUIRE: Client authentication is required.

In this example, the value is set to REQUIRE, and EventRouter has to present its client certificate (see section 4.1.2 Sending QLTs).

Details

Name*:

Class type: OTHER ▼

Configuration

Implementation from: Default class loader ▼ 

keyManagers

Class : org.apache.camel.support.jsse.KeyManagersParameters ▼ 

keyPassword

keyStore

Class : org.apache.camel.support.jsse.KeyStoreParameters ▼ 

password

resource

cipherSuitesList

trustManagers

Class : org.apache.camel.support.jsse.TrustManagersParameters ▼ 

keyStore

Class : org.apache.camel.support.jsse.KeyStoreParameters ▼ 

password

resource

secureSocketProtocolsList

serverParameters

Class : org.apache.camel.support.jsse.SSLContextServerParameters ▼ 

clientAuthentication

Once completed, click the Save button on the top right of the page.

Once saved, the connector needs to be refreshed to load all current values.

Connectors

Add

In space Integration ▼

Name	Actions
decisiontable (OTHER)	 
qltSslContextParameter:	 

This Connector is used by the Data Integration Transformations Routes, where the connection to QLT with the additional parameters is used.



MFT Operational Intelligence

Endpoints

Connectors

Mappings

Libraries

Events

Queries

Notifiers

Automation

Triggers

Transformations

Routes

States

Resources

Properties

Runtime

Logs

Routes

Add

In space

Integration

Name

State

Actions

01_ConsumeTrackedObject

Started

02_CompleteInProcessTrans

Started

03_UpdateProductInstance

Started

99_TimerCloseTransfers

Started

Currently, this is only the first Route in the Integration Space "01_ConsumeTrackedObject". You must restart this route.

Click the stop button under Actions next to the named route:



MFT Operational Intelligence

Endpoints

Connectors

Mappings

Libraries

Events

Queries

Notifiers

Automation

Triggers

Transformations

Routes

States

Resources

Properties

Runtime

Logs

Routes

Add

In space

Integration

☐

Name

State

Actions

☐ 01_ConsumeTrackedObject Started

☐ 02_CompleteInProcessTrans Started

☐ 03_UpdateProductInstance Started

☐ 99_TimerCloseTransfers Started

It should not be required to stop and restart the platform to reload the configuration in this instance if this has already been carried out to complete the previous steps. However, it is acceptable to restart the platform at this point.

Addendum

List of cipher suites

List of cipher suite numbers and their details:

Suite Number	Authentication	Confidentiality	Integrity
49199	ECDHE + RSA authentication	AES-128 GCM	SHA-256
49200	ECDHE + RSA authentication	AES-256 GCM	SHA-384
49191	ECDHE + RSA authentication	AES-128	SHA-256
49192	ECDHE + RSA authentication	AES-256	SHA-384
156	RSA authentication	AES-128 GCM	SHA-256
157	RSA authentication	AES-256 GCM	SHA-384
60	RSA authentication (512, 1024, 2048, or 4096)	AES-128	SHA-256
61	RSA authentication (512, 1024, 2048, or 4096)	AES-256	SHA-256
47	RSA authentication (512, 1024, 2048, or 4096)	AES-128	SHA-1
53	RSA authentication (512, 1024, 2048, or 4096)	AES-256	SHA-1

10	RSA authentication (512, 1024, 2048, or 4096)	Triple DES	SHA-1
5	RSA authentication (512, 1024, 2048, or 4096)	RC4	SHA-1
4	RSA authentication (512, 1024, 2048, or 4096)	RC4	MD5
59	RSA authentication (512, 1024, 2048, or 4096)	None	SHA-256
2	RSA authentication (512, 1024, 2048, or 4096)	None	SHA-1
1	RSA authentication (512, 1024, 2048, or 4096)	None	MD5

Useful OpenSSL commands

- Generate a self-signed certificate:

```
openssl req -x509 -newkey rsa:4096 -keyout er_key.pem -out er_cert.pem -sha256 -days 3650
pass = axway
Country Name (2 letter code) :US
State or Province Name (full name) :Illinois
Locality Name (eg, city) :Lockport
Organization Name (eg, company) :Axway
Organizational Unit Name (eg, section) :PSO
Common Name (e.g. server FQDN or YOUR name) :eventrouter.localdomain
Email Address []:
```

- Generate the PKCS file from the PEM key and certificate:

```
openssl pkcs12 -export -out <myPKCS12>.p12 -inkey <myKey>.pem -in <myCert>.pem
```

- Generate the PKCS file from the PEM key and certificate:

```
openssl pkcs12 -in <myPKCS12>.p12 -out <myCert>.crt -nodes
```

- Extract a certificate from PKCS12:

```
openssl pkcs12 -in <myPKCS12>.p12 -out <myKey>.key -nodes -nocerts
```

- Extract a key:

```
openssl pkcs12 -in <myPKCS12>.p12 -out <myKey>.key -nodes -nocerts
```

- Convert PEM cert to DER:

```
openssl x509 -in <myCert>.pem -out <myCert>.der -outform DER
```

- Convert PEM key to DER:

```
openssl rsa -inform PEM -outform DER -text -in <myKey>.pem -out <myKey>.der
```

- Get a certificate from the server:

```
openssl s_client -showcerts -connect <servername>:<port>
```

- Add PEM certs to the PKCS7 file:

```
openssl crl2pkcs7 -nocrl -certfile er_cert.pem -certfile mftoi.pem -certfile adi.pem -out trusted_CAs.p7b
```

- List contents of PKCS7 container (PEM):

```
openssl pkcs7 -print_certs -in trusted_CAs.p7b | grep -i subject
```

- Add certs (PEM to DER) to the PKCS7 file:

```
openssl crl2pkcs7 -nocrl -inform PEM -certfile er_cert.pem -certfile mftoi.pem -certfile adi.pem -outform DER -  
out trusted_CAs_DER.p7b
```

- List contents of the PKCS7 container (DER):

```
openssl pkcs7 -print_certs -in trusted_CAs.p7b | grep -i subject
```

Frequently asked questions

If you have questions about MFT OI, the installation process, the dashboards, or other aspect of MFT OI, review the contents of this section and see if your question has already been answered. If not, [click here to see how to ask for support](#).

- [Why did I get a message about downloading a Flash Player?](#)
- [What is the gray question mark, and what does it mean?](#)
- [What are baselines?](#)
- [What do the shaded areas on the charts mean?](#)
- [Why does my chart show no baseline?](#)
- [Why are there no or few transfers shown as "in process"?](#)
- [What is an exception for MFT OI?](#)
- [How do I see information for some day other than the current day?](#)
- [What are watched products and participants?](#)
 - [What's a product?](#)
 - [What's a participant?](#)
- [What are expected files, windows, and window settings?](#)
- [What's an expected file window?](#)
- [Why is my dashboard still blank? Everything is zero!](#)
- [Why does MFT OI care about the date, time, and time zone settings?](#)
- [Can I customize or make design changes to MFT Operational Intelligence?](#)
- [How do I check and change the time zone on my system?](#)
- [How do I stop and start MFT OI?](#)
 - [Stopping MFT OI](#)
 - [Starting MFT OI](#)
- [How can I clean up after an unsuccessful install?](#)
 - [Using the Installer](#)
 - [Using command-line instructions](#)
 - [If installed as a Service](#)
 - [If run as a nohup program \(not as a Service\)](#)
 - [If DecisionInsight was not started / already stopped](#)
- [I'm a DecisionInsight or Embedded Analytics user. How can I use MFT OI?](#)
 - [I have Embedded Analytics for SecureTransport \(EA4ST\). Do I need to stop it running?](#)
 - [I have Embedded Analytics for SecureTransport \(EA4ST\). Can I run them in parallel?](#)
 - [I have DecisionInsight or Embedded Analytics for API \(EA4API\). Do I need to stop it running?](#)
 - [I have Sentinel; can I run it in parallel with MFT OI?](#)
- [Why don't I receive email notifications?](#)
- [Why do some time data have an asterisk next to it?](#)
- [How can 'In Process' transfers be closed in bulk](#)
- [How can I resubmit ST transfers that have failed](#)
- [What is the default data retention period for MFT OI, and how can I change it?](#)
- [What does the status of a transfer mean?](#)

Why did I get a message about downloading a Flash Player?

You might see a message like this:

Axway Decision Insight requires the Adobe Flash Player 12.0.0 or above. [Download latest Flash Player](#)

Decision Insight, the platform that runs MFT OI, has legacy support for a flash interface. You can work around this by making sure that the web address used ends in "/ui" rather than "/app"

What is the gray question mark, and what does it mean?

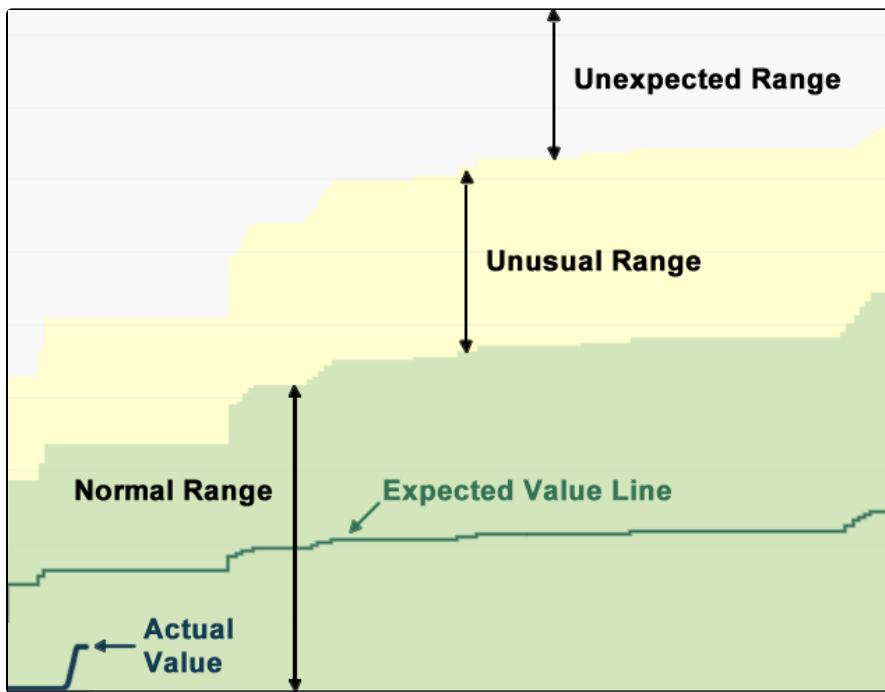
MFT OI provides you with both hard data about MFT operations – like the count of 4 completed transfers – and an *opinion* of the data in the display. MFT OI's opinion of the current activity level on the first day of operation is ... that there is no opinion to offer. That is because MFT OI does not have enough

information to draw any conclusions. When you see that gray icon like this ...  ... you will know that MFT OI is waiting for more information to form an opinion. To develop an opinion, MFT OI needs to build a baseline of the indicators it measures.

[Back to Top](#)

What are baselines?

A *baseline* is an MFT OI means of applying machine learning to history to estimate and evaluate current activity. Baselines are one of the tools used by MFT OI to determine if the recent activity is normal. When you look at a baseline in a chart, you will see five pieces of information:



The definition of the ranges is that each range represents a collection of probabilities based on observation. The normal range represents the set of values that occur most frequently in recent history. The expected value line is the average of the most frequent values and is typical of the performance of that metric at the corresponding time of day. The unusual range represents the set of values that are just outside the allowable standard deviation of the average. The unexpected range exceeds the acceptable standard deviation. Metric values in the unusual range represent behavior that may be an issue requiring attention.

When the actual value of a metric is within the Normal Range, MFT OI will evaluate the metric as Normal, with a checkmark icon. Values within the Unusual Range will display as a yellow exclamation mark icon, while anything outside those two ranges, the Unexpected Range, will be represented with a red x icon.

[Back to Top](#)

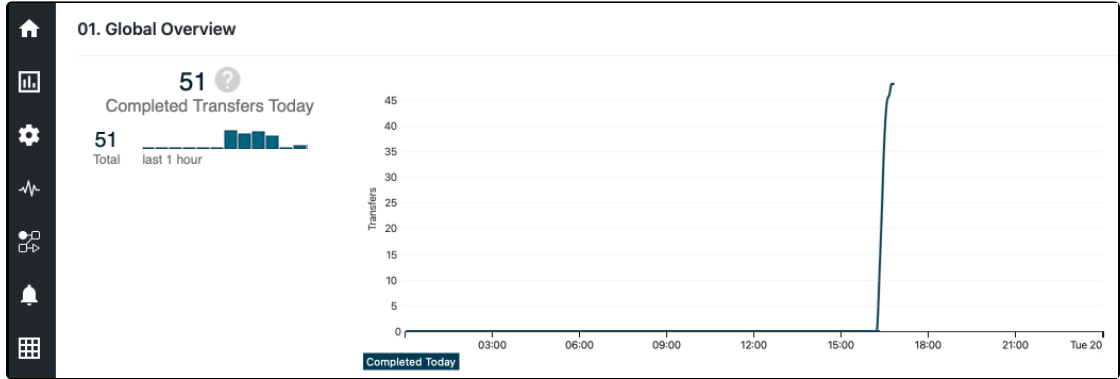
What do the shaded areas on the charts mean?

The shaded areas on charts display information from baselines, with different zones representing different evaluations of expected behavior, whether Normal, Unusual, or Unexpected (see above).

[Back to Top](#)

Why does my chart show no baseline?

When MFT OI has too little information to develop a baseline, it does not display them on the charts. For example, you might see a display like this one:



If this is the first day the MFT OI is running, your charts will have only one line – a dark blue or red one that the legend tells you the metric's value. Other items will be visible as more data is collected.

[Back to Top](#)

Why are there no or few transfers shown as "in process"?

Your chart may or may not show any transfers in process. The count is *sampled*, meaning the logic inside MFT OI looks to see how many transfers are in progress at that precise instant once a minute. In many environments, transfers have short durations, measured in seconds or less rather than minutes or hours. The result is the count of in-process transfers can be quite low, even in situations with a large number of transfers that do not require a significant amount of time to complete.

[Back to Top](#)

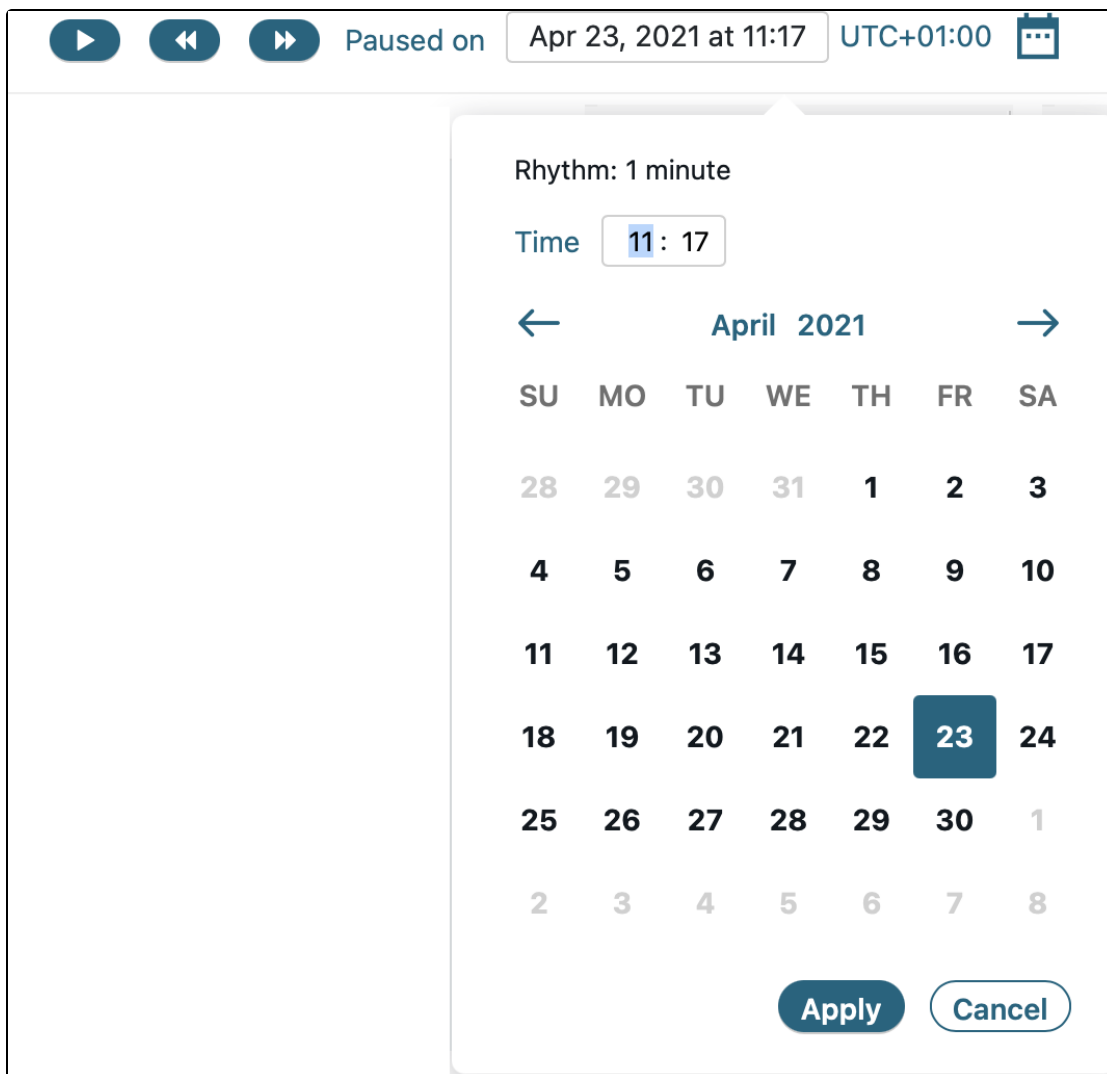
What is an exception for MFT OI?

The basic answer is MFT OI considers a transfer an exception if it does not complete normally. That means that any transfer within SecureTransport that fails after reaching the maximum number of retries is an exception. Retried transfers are not exceptions. Transfers that are canceled are also counted as an exception as they did not complete with normal status.

[Back to Top](#)

How do I see information for some day other than the current day?

Moving to different days is controlled by the time navigation controls in the top right corner:



The controls allow you to change the time and date or jump forward / backward in time. After moving in time, you can always return to the current time by clicking the "play" icon.

[Back to Top](#)

What are watched products and participants?

There is a special class of products and participants that are referred to as *Watched*. When watching a product or participant, it is singled out for special attention and monitoring by MFT OI. You will be able to see the differences in how products and participants are displayed in the dashboards. See the next two sections for more information on products and participants.

What's a product?

MFT OI uses the term product to mean an instance of Transfer CFT or SecureTransport. Every instance of Transfer CFT or ST that emits events received by MFT OI will be displayed as a Product on the Product Summary dashboard and listed in any associated transfers in the Transfer Summary, Exceptions Summary, and Transfer Details.

What's a participant?

A participant in MFT OI is any source or destination of a transfer. An external partner is a participant. An internal application is also a participant. Relay middleware may be considered a participant in some cases. Every partner, application, or relay mentioned in an event received by MFT OI will be displayed as a Participant on the Participant Summary dashboard and listed in any associated transfers in the Transfer Summary, Exceptions Summary, and Transfer Details. Only Watched Participants are scanned for Expected Files.

[Back to Top](#)

What are expected files, windows, and window settings?

The purpose behind file patterns and file windows is to detect situations where important and critical transfers do not occur when expected. There are two aspects of monitoring important file transfers:

- Determining what file transfers to monitor, and
- Monitoring to ensure those expected file transfers take place.

MFT OI works behind the scenes to detect file transfer patterns for Watched Participants. Admin users have the option to review the detected patterns to decide which to apply to be monitored. These definitions create *file transfer windows* to be monitored. Admins can also manually create file transfer windows for Watched Participants when patterns are not automatically detected.

Once you define windows, MFT OI compares file transfers as they complete with the expected file transfer windows.

[Back to Top](#)

What's an expected file window?

Expected File Windows are one of the significant features of MFT OI. The basic concepts are:

- There are some files from certain sources where the arrival of that file is important
- For some important files, arriving on time is necessary for the business operation
- Knowing when important files do not arrive on time can prevent unwanted impact

An Expected File Window is the means to detect when important files do not arrive in the time and volume expected.

[Back to Top](#)

Why is my dashboard still blank? Everything is zero!

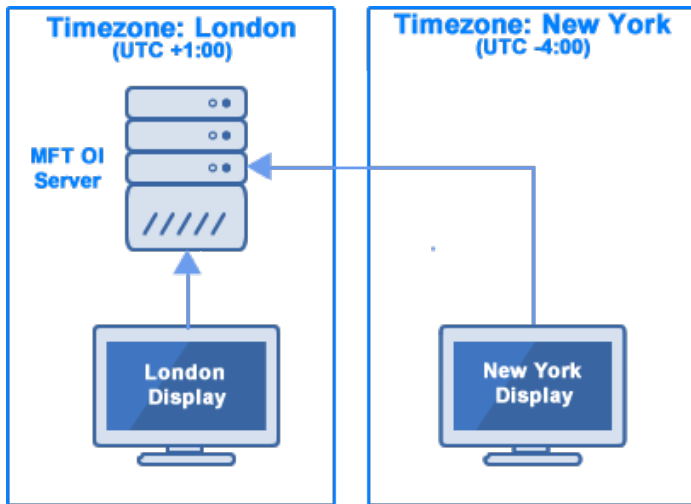
If MFT OI is running and you still see no values on your dashboard, it may mean there is a problem, or it may not. Before further debugging, please read section 3 on how MFT OI deals with time. If time is not the issue, then it probably means that MFT OI is not receiving any QLT events. Check the information in the section [Connect SecureTransport and Transfer CFT to MFT OI](#) for possible answers.

[Back to Top](#)

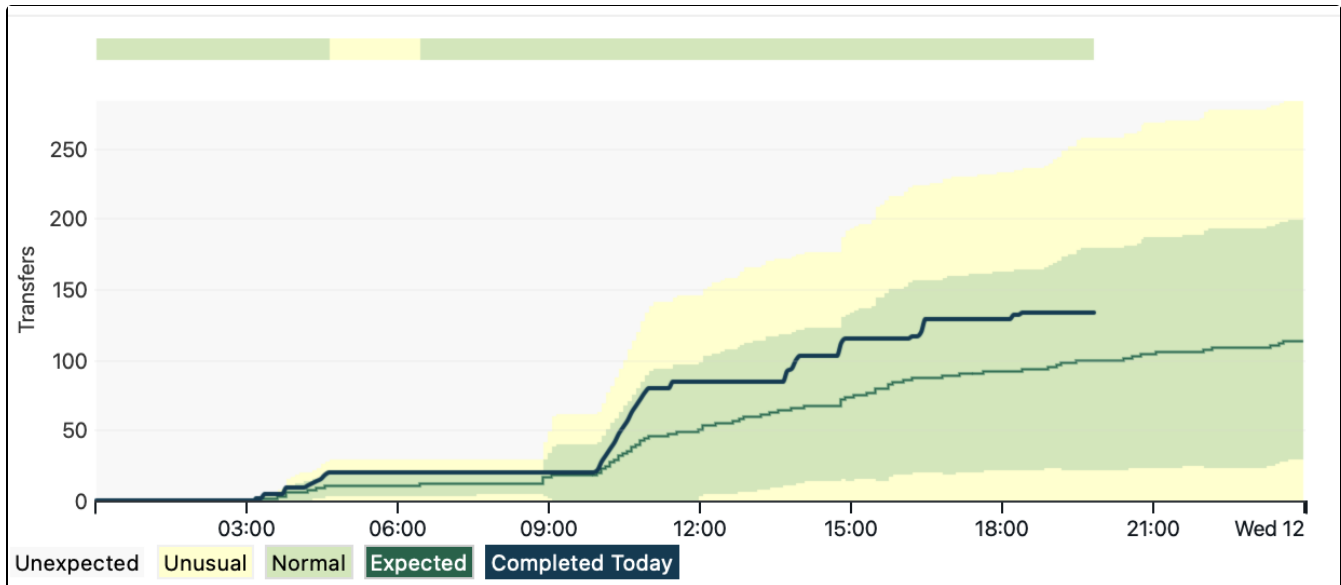
Why does MFT OI care about the date, time, and time zone settings?

You may wonder why MFT OI is sensitive about the accuracy of the date and time settings. The answer is that you want to understand when items and values reported on the dashboard occurred. If the time of the MFT OI virtual machine is, for example, 45 minutes behind the actual time, then the task of matching an incident to the actual time will be difficult.

Additionally, the settings you choose for the time zone are also important. MFT OI organizes information into 24-hour days. If the user viewing dashboards is not in the same time zone as the system hosting the MFT OI application, the display of the "day" in graphs will be offset by the difference between the relative times.

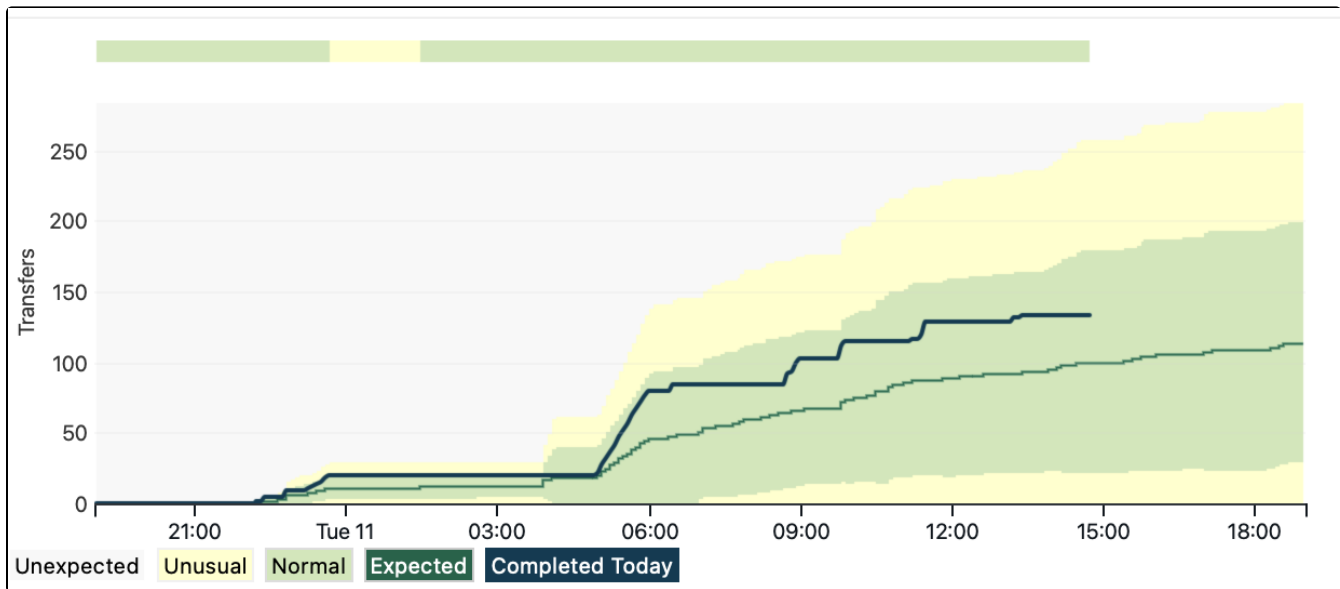


For example, if MFT MFT OI is installed in London, the display as seen in London will have the charts aligned with the 24-hour day in London:



You can see the chart range runs from midnight on Tuesday the 11th to midnight on Wednesday the 12th.

If, on the other hand, the display is viewed in New York, it will have the display shifted by the time difference between London and New York:



In this case, the time range on the chart runs from 19:00 on Tuesday, the 11th, to 19:00 on Wednesday.

A configuration option is available to align all user dashboards with the server time, which will have the graph ranges line up on the normal midnight-midnight view. See the Standardized Time Zones for All Dashboard Users section in the [Advanced Features](#) section.

[Back to Top](#)

Can I customize or make design changes to MFT Operational Intelligence?

No, customizations or design changes are not permitted for the following reasons:

- MFT Operational Intelligence is a Decision Insight application that is designed to work 'out of the box' in delivering a suite of pre-configured dashboards and alerts. There are regular new releases that cannot account for any changes that may have been implemented on a customer site. This means that when upgrading to a new release of MFT Operational Intelligence, all the customized content (and any other changes) are lost.
- The resource sizing guide for MFT Operational Intelligence is derived using the OOTB runtime content. Customizing or extending content most likely leads to increased demand on available resources, and as a result, it potentially invalidates the sizing guide.

How do I check and change the time zone on my system?

There are several ways to display the current time zone on your Linux server:

```
date # returns the date, time, time zone, year
timedatectl # returns a list of time information and the time zone
ls -l /etc/localtime # shows the link to local time zone
```

You can see sample results from the commands here:

```
[root@SL2RDAPP037525 ~]# date
Tue Sep 19 16:02:25 EEST 2023
[root@SL2RDAPP037525 ~]# ls -l /etc/localtime
lrwxrwxrwx 1 root root 36 Mar 17 2023 /etc/localtime -> /usr/share/zoneinfo/Europe/Bucharest
[root@SL2RDAPP037525 ~]# timedatectl
      Local time: Tue 2023-09-19 16:03:06 EEST
      Universal time: Tue 2023-09-19 13:03:06 UTC
        RTC time: Tue 2023-09-19 13:03:03
        Time zone: Europe/Bucharest (EEST, +0300)
      NTP enabled: n/a
      NTP synchronized: no
      RTC in local TZ: no
      DST active: yes
      Last DST change: DST began at
                      Sun 2023-03-26 02:59:59 EET
                      Sun 2023-03-26 04:00:00 EEST
      Next DST change: DST ends (the clock jumps one hour backwards) at
                      Sun 2023-10-29 03:59:59 EEST
                      Sun 2023-10-29 03:00:00 EET
```

To change the time zone for the system, you can use one of two methods. Both methods require that you know the correct name for the time zone you wish to set. To get the list of time zones, you can use the command:

```
timedatectl list-timezones
```

You can also find the list of time zones by listing the contents of `/usr/share/zoneinfo`.

Once you have the proper name for the desired time zone, you can set it directly with the command:

```
timedatectl set-timezone <your_time_zone>
```

Or by removing the current link from `/etc/localtime` and replacing it with one of your choices. For example:

```
timedatectl set-timezone <your_time_zone>
```

Or, if your closest city is Los Angeles (which is in the America region), you could use:

```
ln -s /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

Or, if you are in Moldova in the Europe region, you could use:

```
ln -s /usr/share/zoneinfo/Europe/Chisinau /etc/localtime
```

[Back to Top](#)

How do I stop and start MFT OI?

Stopping MFT OI

You can control MFT OI from a terminal session if you need to bring it down. Log in to the server where you installed MFT OI. In this example, the installation was made in the `/opt/mftoi` folder. Based on that folder location, to stop MFT OI, use the following commands:

```
cd /opt/mftoi/install/node_20210412/bin
./tnd-stop.sh
```

That brings down the Decision Insight platform and the MFT OI application that runs on the platform.

Starting MFT OI

If MFT OI is stopped or not running, you can control it from a terminal session. Log in to the server where you installed MFT OI. In this example, the installation was made in the /opt/mftoi folder. Based on that folder location, to start MFT OI, use the following commands:

```
cd /opt/mftoi/install/node_20210412/bin
nohup ./tnd-start.sh > ../var/log/tnd-start.log 2>&1&
```

That will start Decision Insight and the MFT OI application. The standard output from the application will be directed to the tnd-start.log file in the node_20210412/var/log directory.

[Back to Top](#)

How can I clean up after an unsuccessful install?

To remove all traces of an unsuccessful install, the recommended approach is to do the following:

Using the Installer

Run the installer with the following command. This is the recommended method.

```
./mft_oi_install.sh uninstall
```

Or, you can run the installer to access the menu and choose to uninstall.

```
./mft_oi_install.sh
```

```

  A X W A Y

M   M   FFFFF TTTT   OOOOO IIIII
MM  MM  F      T      O  O  I
M MM M  FFF    T      O  O  I
N   M  F      T      O  O  I
M   M  F      T      OOOOO IIIII

1) Test Prerequisites
2) Full Deployment as a root user (service)
3) Full Deployment as a non-root user
4) Install DecisionInsight only (inc Prerequisites Test)
5) Register and Start DecisionInsight as a service
6) Start DecisionInsight as a non-root user
7) Deploy MFTOI
8) Uninstall
9) Quit
Please enter your choice between 1 and 9 : █
```

Choose Option 8.

These options will create an archive of the logs in case you wish to investigate or provide them to Axway for support.

Using command-line instructions

If installed as a Service

- Stop the DecisionInsight service

```
service DecisionInsight stop
```

- Unregister the DecisionInsight service.

If the installation script was able to progress to the point where it unzipped the DecisionInsight platform, it is possible that DecisionInsight was successfully registered as a service.

To check the services running, use:

```
service --status-all
```

To remove the service, take the following steps. From the **install** directory:

```
cd node_20210412/bin/  
./tnd-service-unregister.sh
```

If run as a nohup program (not as a Service)

Find the process running the DecisionInsight platform.

Find the DecisionInsight deployed directory, as the process ID is saved as a PID file when starting DecisionInsight.

```
cat ${adiinstalldir}/var/run/pid
```

Otherwise:

```
ps -ef | grep "bin/tnd-start.sh"
```

If DecisionInsight was not started / already stopped

If you receive a "no such file or directory" or similar when you try to change to the node directory, then the service was not registered and you can continue to the next step.

- Remove the deployed directories.

From the **deployed** directory:

```
cd ..  
rm -rf {deployed directory}
```

[Back to Top](#)

I'm a DecisionInsight or Embedded Analytics user. How can I use MFT OI?

I have Embedded Analytics for SecureTransport (EA4ST). Do I need to stop it running?

If you are already running Embedded Analytics for SecureTransport and want to run MFT OI, this can be achieved with a separate instance.

You do not need to stop EA4ST, as these are separate products and do not provide identical information.

Using the MFTOI installation script to quickly deploy DecisionInsight and the MFTOI application is recommended, rather than standing up the DecisionInsight deployment via another method.

However, you will need to consider how ST will provide the data via QLT to MFTOI as well as EA4ST. You require an Event Router to share the same data with both products. This sits between ST and the EA4ST / MFTOI products and sends the QLT messages to multiple points.

This is required as both products will require a unique connection across QLT.

I have Embedded Analytics for SecureTransport (EA4ST). Can I run them in parallel?

If you are already running Embedded Analytics for SecureTransport and want to run MFTOI in parallel, the first point is that they are separate products and don't provide identical information.

As a separate product, MFTOI requires its own deployment of DecisionInsight on its own server.

Using the MFTOI installation script to deploy DecisionInsight and the MFTOI application quickly is recommended, rather than standing up the DecisionInsight deployment via another method.

Also, you must consider how ST will provide the data via QLT to MFTOI as well as EA4ST. To share the same data with both products, you require an Event Router. This sits between ST and the EA4ST / MFTOI products and sends the QLT messages to multiple points.

This is required as both products will require a unique connection across QLT.

I have DecisionInsight or Embedded Analytics for API (EA4API). Do I need to stop it running?

If you are already running Embedded Analytics for API Manager / Gateway, and you wish to run MFTOI, this can be achieved with a separate server.

It is recommended to use the MFTOI installation script to deploy DecisionInsight and the MFTOI application quickly rather than stand up the DecisionInsight deployment via another method.

You do not need to stop EA4API as these are separate products and do not provide the same information.

I have Sentinel; can I run it in parallel with MFT OI?

If you are already running Sentinel for monitoring Transfer CFT and you wish to run MFTOI in parallel, the first point is that they are separate products and don't provide identical information.

As a separate product, MFTOI requires its own server for the deployment of DecisionInsight.

Also, you will need to consider how ST will provide the data via QLT to MFTOI as well as Sentinel. To share the same data with both products, you require an Event Router. This sits between CFT / ST and the Sentinel / MFTOI products and sends the QLT messages to multiple points.

This is required as both products will require a unique connection across QLT.

Why don't I receive email notifications?

If the notification was not received, the first thing to do is check the spam section of the email.

Second, check the "EmailNotification" route log from the Alerts space. If the log looks like the image below, there is a problem with the email address associated with the notification.

2022-02-24T13:54:45.486Z	Alerts.EmailNotification route6	INFO	Sending email notification. Headers: {kafka.KEY=1725652874304684033, kafka.TOPIC=Notifier_dbf024b4-e616-41b3-17bd-f...
2022-02-24T13:54:45.481Z	Alerts.EmailNotification route3	INFO	EmailNotification Triggered (_data={CycleID=MFTOI-225_1+TR001/A07, Direction=S, Filename=LugnzXbjc.qtk, FlowName=00...
2022-02-24T13:53:26.249Z	Alerts.EmailNotification route1	INFO	EmailNotification Route Started at: Thu Feb 24 15:53:26 EET 2022

Why do some time data have an asterisk next to it?

Occasionally, MFT OI receives a transfer that is missing the time information (EVENTTIMESTAMP for ST or EVENTDATETIME for CFT). In this scenario, MFT OI generates the time data internally, using the time it receives the transfer update. An asterisk is then displayed next to the time on the dashboards to indicate that this hasn't come from the transfer.

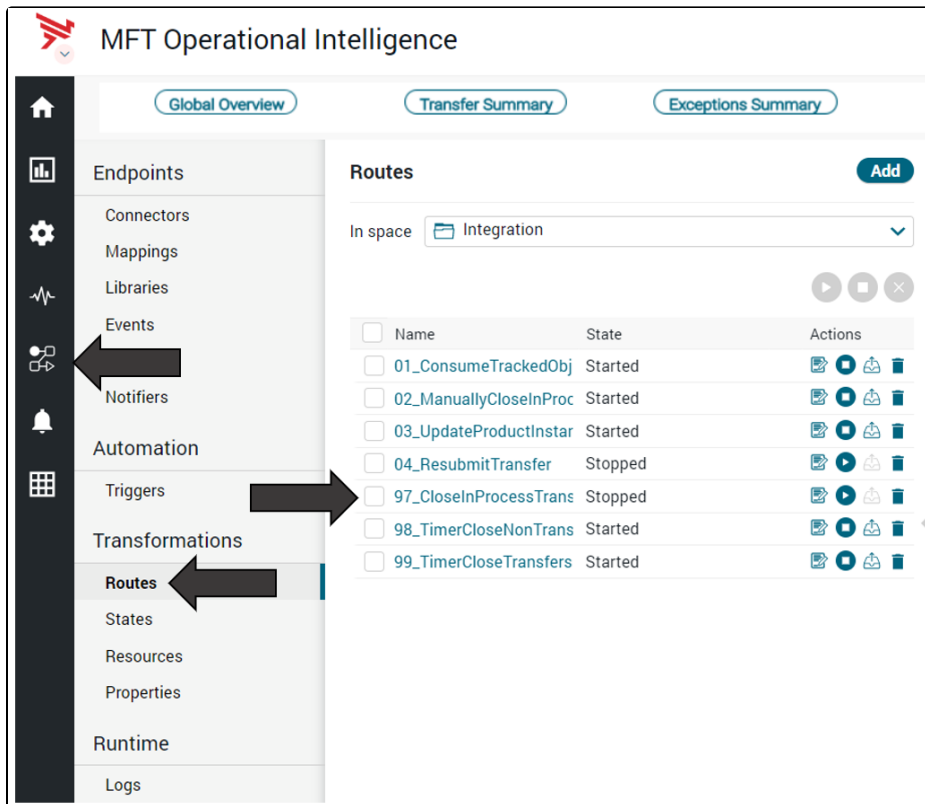
Time State Entered	Time State Left	Time in State
Tue 01 Mar 16:39:00.259*		17 h 17 min 59 s 742 ms*

This applies to the following dashboard fields:

- Transfer Detail
 - Creation Time
 - Time State Entered
 - Time In State
- Transfer Summary
 - Creation Time
- Flow Overview
 - Max Transmission Time
- Exception Summary
 - Creation Time

How can 'In Process' transfers be closed in bulk

In Process can be closed in Bulk by executing the route **97_CloseInProcessTransfers** that is available in the Data Integration screens



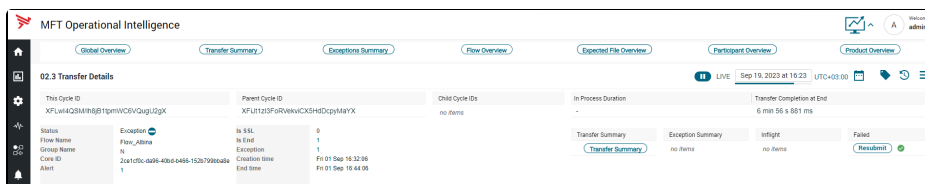
[Back to Top](#)

How can I resubmit ST transfers that have failed

This feature is available through the **Resubmit** button in the **02.3 Transfer Details** dashboard and is only visible for transfers in a Failed state. It enables you to resubmit an already processed file transfer to SecureTransport and reprocess already failed transfers easily without the need to log on to the backend system every time this is needed.

NOTES:

- The **Resubmit** button is visible and usable only by users having the specific rights set with the resource **14_ResubmitAccessRights** (see details: [Enabling the File Resubmit feature for SecureTransport transfers](#))
- On a SecureTransport cluster architecture, the resubmit request is sent to the primary node. If the SecureTransport primary node does not have all the information to resubmit (The tracking table is not synchronized), the request returns an error.



What is the default data retention period for MFT OI, and how can I change it?

The default retention time for Configuration entities (for example, Products, Participants) is six months and one month for Transaction entities (for example, transfers).

The modification of a retention period of data from one hour to a longer interval is possible from the Configuration menu on Entities. After selecting one entity from the list, the retention period can be changed from the Details page.

Details

SaveCancel

Name*: SecureTransport Server

Space*: Model

Description:

Type*:

☐ Configuration
Such entities are stable over time. Select this type for entities representing customers, countries, organizations, steps, etc. The instances of this type of entities are exported in application files if they are linked to a space.

☐ Transaction
Such entities are created and deleted over time. Select this type for entities representing transactions, payments, shipments, etc.

Retention period:

☐ Unlimited
Data will be kept forever. Unlimited retention can impact storage consumption and performances.

☒ Limited to 6 months

Set the retention period for the entity and its attributes. Closed instances and their values will be removed from the system when this period is over.

What does the status of a transfer mean?

All the transfers are closed in OI within 10 minutes from the last state update. The status shows to users if a transfer was a success or not, and it depends on the last state received. For example, if the last state of a transfer is SENT and if this state is not changed in 10 minutes, then this transfer is closed with the status SUCCESS.

Depending on the following states, the status of a transfer can be:

STATE	STATUS
AVAILABLE	NonTransfer
CONSUMED	
DELETED	
INTERRUPTED	
SUBMITTED	
TO_EXECUTE	
CANCELED	Exception
ENDED_TO_NACK	
FAILED	
RECEIVING	Processing
SENDING	
ACKED	Success
CLOSED	
COMPLETED	
ENDED_TO_ACK	
POST_PROC	
POST_PROC/ARCHIVED	
RECEIVED	
RENAMED	
ROUTED	
SENT	
SUSPENDED	

Capacity planning

This topic provides information for capacity planning and outlines performance results for MFT Operational Intelligence (MFT OI) that can be used for planning production deployments.

Who should read this

This topic is for architects responsible for the deployment of MFT OI and the underlying infrastructure requirements.

Before reading this, you should have:

- A good understanding of the concepts and architecture of MFT OI
- An accurate idea of the workload characteristics and performance objectives for your organization

Performance considerations

To provide the required performance when your workload includes important amounts of data, use servers with more processor cores. When your workload includes important amounts of data, use servers with more physical memory and allocate this memory to the MFT OI process.

Test settings

For the tests, the data simulator was used to produce file transfers using the QLT protocol for five days with a constant throughput. The data was pushed in batches every 5 seconds. To make sure MFT OI could sustain the load in case of a spike in the data, we sent data at a higher rate than the one presented in the thresholds below. We assumed users were sending 1% of the monthly throughput in an hour and tried to sustain it for the whole duration of the test.



Because we wanted to sustain the equivalent of 1% of the monthly load over an hour, the real throughput tested is 7.2 times more than the theoretical throughput described below. This is assuming a 30-day month.

For example, for 2M, the actual throughput is $2M/100*24*30 = 14.4M$

We started by using Axway Decision Insights (ADI) default settings for memory usage. This means that we allocated a max of 16GB of RAM to the ADI process and of that 16 GB, two were allocated to the in-memory database.

Test environment

The tests were run on a single-node configuration. To run the tests, a data simulator was used, allowing us to generate some traffic for MFT OI at various throughputs expressed in the number of file transfers.

The tests were run on AWS using [EC2 T3 Instances](#). We ended up using three different instance types:

Name	vCPUs	Memory (GB)
t3.large	2	8
t3.xlarge	4	16
t3.2xlarge	8	32

Monitored values

To evaluate the results of the tests, we monitor the following elements:

- The time taken by the route "direct://ProcessMessage2" in Space 01_ConsumeTrackedObject used to absorb events
- The five slowest computed values, and how long it takes to compute all the values during the entire test and calculate the average time for each computed attribute
- The CPU used
- The memory used

Test results



All processing times are presented in milliseconds

50k - 2M transfers per month

6GB of memory is enough to handle up to 2 million transfers per month. At that throughput, 3 out of the 5 slowest computing takes less than a second. Data integration functions properly even though the mean processing time for one message is higher than on other benchmarks (10 milliseconds). The memory used can go up to the limit, but it is released regularly.

EC2 configuration

Instance type	Total memory	MFT OI memory
t3.large	8G	6G

Data injection (times in ms)

This table presents the total number of messages processed by the data-integration route and the maximum and average times to process one of those messages.

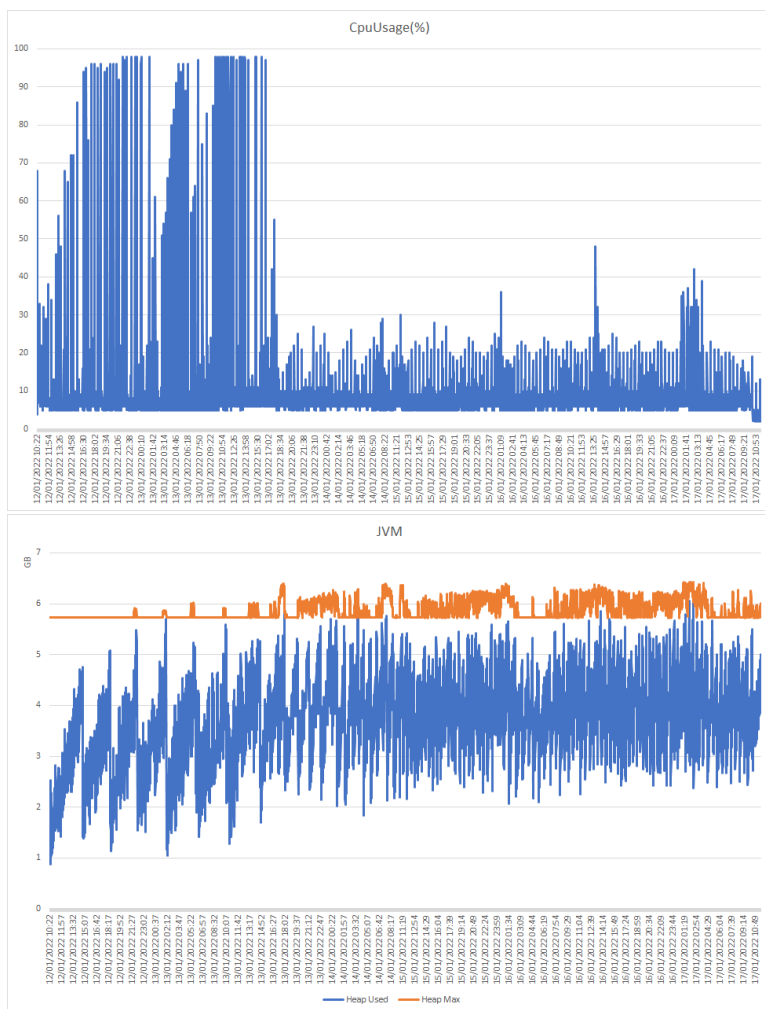
Effective monthly transfers	Total events	Max event processing time	Average event processing time
20M	72M	12 000ms	10ms

Computed attributes

This table presents the five slowest computed attributes using the average time it took to compute them once.

Attribute name	Average processing time (in ms)
[Flows],# transfers completed - last 1 hour	2247.521
[Flows],# transfers completed Exception - last 1 hour	2186.223
[Flows],Max. Transmission Time - last 5 mins	1080.905
[ProductInstance],# transfers completed - last 5 min	884.844
[ProductInstance],# transfers completed Exceptions - Today	755.099

CPU and Memory



15M monthly transfers

10GB of memory is enough to handle up to 15 million transfers per month. At that throughput, 4 out of the 5 slowest computing takes more than 2 seconds. Data integration functions properly with a mean processing time for one message that is low (4 milliseconds). The memory used can go up to the limit, but it is released regularly.

EC2 configuration

Instance type	Total memory	MFT OI memory
t3.xlarge	16G	10G

Data injection (times in ms)

This table presents the total number of messages processed by the data-integration route and the maximum and average times to process one of those messages.

Effective monthly transfers	Total events	Max event processing time	Average event processing time
143M	240M	4 480ms	4ms

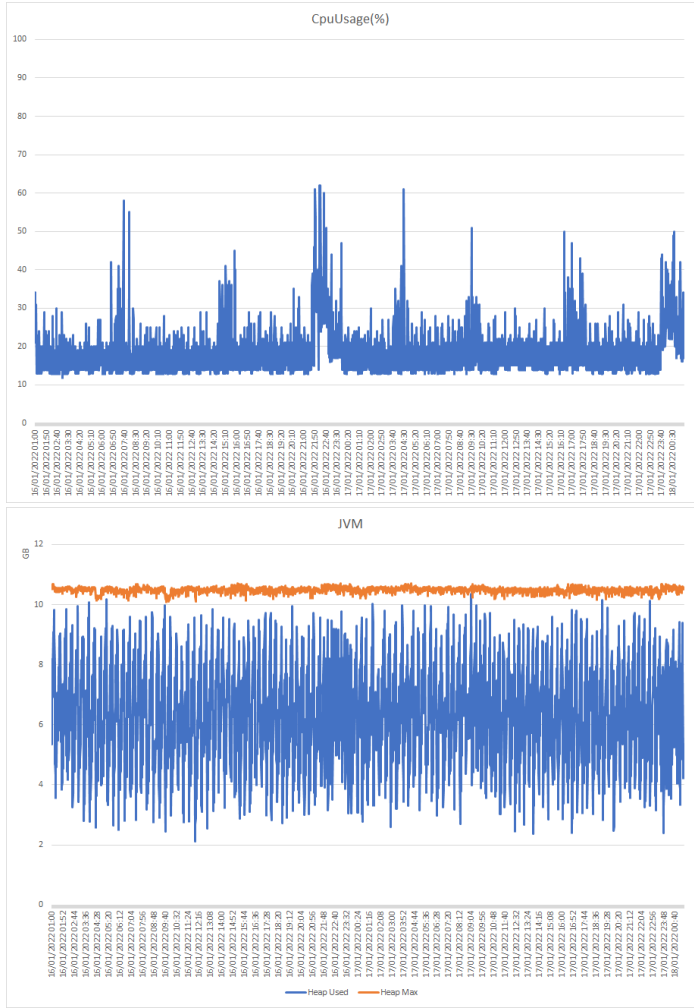
Computed attributes

This table presents the five slowest computed attributes using the average time it took to compute them once.

Attribute name	Average processing time (in ms)
[Flows], # transfers completed - last 1 hour	5512.082

[Flows], # transfers completed Exception - last 1 hour	5053.722
[Flows],Max. Transmission Time - last 5 mins	2336.310
[ProductInstance],# transfers completed - last 5 min	2204.717
[Participant],# transfers completed in Process (1 min)	1801.335

CPU and Memory



25M monthly transfers

20GB of memory is enough to handle up to 15 million transfers per month. At that throughput, 4 of the 5 slowest computing takes more than 2 seconds. Data integration functions properly with a mean processing time for one message that is low (3 milliseconds). The memory used can go up to the limit, but it is released regularly.

EC2 configuration

Instance type	Total memory	MFT OI memory
t3.2xlarge	32G	20G

Data injection (times in ms)

This table presents the total number of messages processed by the data-integration route and the maximum and average times to process one of those messages.

Effective monthly transfers	Total events	Max event processing time	Average event processing time
-----------------------------	--------------	---------------------------	-------------------------------

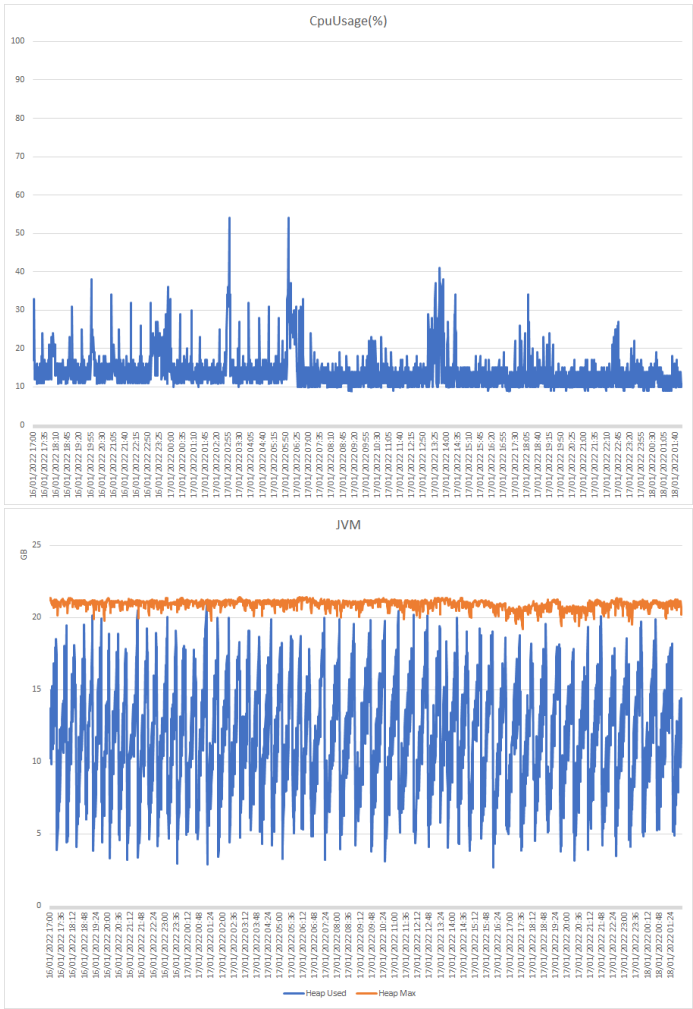
246M	425M	2 257ms	3ms
------	------	---------	-----

Computed attributes

This table presents the five slowest computed attributes using the average time it took to compute them once.

Attribute name	Average processing time (in ms)
[Flows], # transfers completed - last 1 hour	5670.967
[Flows], # transfers completed Exception - last 1 hour	5239.425
[ProductInstance],# transfers completed - last 5 min	2388.513
[Participant],# transfers completed in Process (1 min)	2134.936
[ProductInstance],# transfers completed Exceptions - last 5 min	1982.068

CPU and Memory



Sizing

This topic provides information to help you configure MFT Operational Intelligence. Multiple benchmarks were run based on different customer profiles to get a suitable configuration to enable the application to run with acceptable performance.

The following describes the configuration you may require, but they are merely guidelines. You may need to adjust your configuration in real-life situations.

Configuration by customer profile

Use the following table to determine the quantity of RAM by the server and the number of CPUs required for your profile depending on the number of transfer-related events that are expected to be processed each month. A single file transfer will encompass multiple events enabling us to track the different states of that transfer.

Volume handled	RAM on the server	RAM for MFT OI	vCPU
50K - 500k	8G	6G	2
500K - 2M	8G	6G	2
2M - 5M	16G	10G	4
5M - 8M	16G	10G	4
8M - 15M	16G	10G	4
15M - 25M	32G	20G	8

Performance measurement

Performance is deemed acceptable when you can navigate inside a dashboard with a good response time and when incoming data is absorbed without latency.

The performance of the application depends on several criteria:

- **The number of file transfers** – Direct impact on workload and performance. More file transfers mean more data to process and persist.
- **Peak throughput** – You may have a reasonable average daily number of file transfers, yet have a massive throughput during a set period of time. This huge throughput can impact performance and make dashboards unavailable during peak throughput.
- **The number of instances of analytics dimensions and computed attributes** – The more dimension instances and computed attributes you have, the more time is needed to compute and update them.
 - in the case of MFT OI an important dimension to take into account is the number of "Participant" instances. Our tests were run using 300 different Participants. The higher the number of participants and the more the performance will be affected.



The number of live instances (transfers started but not completed yet) and their lifetime also impact performance in general.

This means that you can have a better performance with a large number of daily transfers where every transfer has a very short lifetime as opposed to an application with fewer transfers that each have a longer lifetime.

Disk space measurement

The disk space required depends on the following criteria:

- Number of file transfers
- Number of instances of analytics dimensions and computed attributes

The following table presents the daily increase in used disk space as well as the total disk space required according to the retention period configured in the application

Volume handled	Disk space required for one day of data	Total disk space for 6 months of data
50K - 500k	272M	55G
500K - 2M	1.3G	220G
2M - 5M	3.0G	530G
5M - 8M	4.8G	860G
8M - 15M	8.9G	1.7T
15M - 25M	14.7G	2.6T

Release notes for MFT Operational Intelligence

Document version: January 2023

These Release Notes apply to the general availability (GA) release of Axway MFT Operational Intelligence 1.0.20240112.

MFT Operational Intelligence new features and enhancements

Corrections and enhancements

Case ID	Internal ID	Description
01440722	MFTOI-563	Notifications for failed transfers are now sent immediately after a transfer enters the Failed state.

Previous corrections and enhancements

The release of MFT OI V1.0.20231222 provides the following enhancements:

Case ID	Internal ID	Description
-	MFTOI-523	Increased the performance by 17%.
01505419	MFTOI-624	Route 03_UpdateProductInstance starts with no error
	MFTOI-625	An end-user can now view transfers that occurred before they were added to a unit, but not before the user was created.

Known issues

Internal ID	Description
MFTOI-508	The Retry button was not visible in MFT OI when the File Archiving option was enabled in SecureTransport.
MFTOI-507	A transfer is closed within 10 minutes even if, in the meantime, it receives new states
MFTOI-521	Inaccurate kpi of transfer success in a window

Zero2One installation

MFT Operational Intelligence provides a scripted installation that takes you from zero (nothing installed) to one (product installed, configured, and operational) in less than 20 minutes.

Guided testing

The product documentation for the initial release of MFT Operational Intelligence includes step-by-step illustrations of what to expect from the solution as it learns your MFT environment. Because MFT Operational Intelligence takes a few days to digest the analytics on the profile of your operations, the planning guide explains what you will see in the product's dashboards as that learning process unfolds.

Supported platforms

MFT OI only runs on 64-bit Linux and currently only supports the following distributions:

- Red Hat Enterprise Linux: 7.x, 8.x
- Ubuntu: 20 LTS
- Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 (2019 and 2022 pending validation)

Interoperability with Axway products

Support for Axway SecureTransport 5.5

MFT Operational Intelligence can track transfers with Axway SecureTransport version 5.5.

Other versions are operational, but the resulting analytics are not as precise.

Support for Axway Transfer CFT 3.9 and 3.6 SP4

MFT Operational Intelligence can track transfers with Axway Transfer CFT versions 3.9 and 3.6 SP4. Other versions are operational, but the resulting analytics are not as precise.