First Look: Managed File Transfer (MFT) with Interoperability Productions

Version 2019.4
2020-01-28

InterSystems Corporation   1 Memorial Drive   Cambridge MA 02142   www.intersystems.com

First Look: Managed File Transfer (MFT) with Interoperability Productions
InterSystems IRIS Data Platform Version 2019.4 2020-01-28

InterSystems Corporation disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

For Support questions about any InterSystems products, contact:

InterSystems Worldwide Response Center (WRC)

Tel:	+1-617-621-0700
Tel:	+44 (0) 844 854 2917
Email:	support@InterSystems.com

Table of Contents

First Look: Managed File Transfer (MFT) with Interoperability Productions

This First Look introduces the Managed File Transfer (MFT) integration option in InterSystems IRIS® data platform, which enables easy inclusion of a third-party file transfer service directly into an InterSystems IRIS production. This First Look also includes step-by-step directions for using MFT with a new production.

To browse all of the First Looks, including those that can be performed on a free evaluation instance of InterSystems IRIS, see InterSystems First Looks.

1 Benefits of Using MFT with InterSystems IRIS

Many sites that have an InterSystems IRIS production also use a file transfer service such as Box, Dropbox, or Accellion kiteworks for secure, HIPAA-compliant file sharing. However, use of such services is dependent on the end-users being willing to use it. And when there is no enforcement, they may easily forget to do so or sometimes simply opt to send a file as an attachment. By integrating an MFT service into your production, you can ensure that files are always sent securely. An additional benefit is that there is less risk of misplaced or misdirected files, since the production can automatically route sensitive files as needed to and from the correct locations, and follow proper workflows.

Consider the following use case: an employment agency contracts out routine physicals or drug tests on prospective employees to an outpatient medical testing facility. Both the testing facility as well as the employment agency are responsible for ensuring secure data transfers of private information to and from each other. However, while the medical facility may already have in place procedures for HIPAA compliance and may already use a secure file transfer service, the employment agency may not have the infrastructure in place to handle the required level of security. An MFT-enabled InterSystems IRIS production set up at either end simplifies the use of a standardized file transfer service for all such communications.

MFT is also very useful for an organization that needs to submit the same file to both internal and external locations, or when a single department receives files that need different processing depending on the sender. For example, suppose a car dealership needs to transmit signed customer financial documents to both their headquarters as well as to a financial institution. Suppose additionally that the Sales department has different processes than the Leasing department, even though both departments must submit the same types of information to the same bank. These differences could lead to confusion and misplaced or misrouted paperwork. Further, the dealership cannot and should not send customers' signed financial or other personal data as attachments to regular emails. Using an InterSystems IRIS production with MFT integration simplifies the submission and routing procedures, so that the correct documents go to the correct department for the appropriate processing, thus reducing the chances of lost documents.

2 How Does it Work?

InterSystems IRIS provides business hosts that you can add to productions and configure, with no programming needed. These business hosts support the Box, DropBox, and Accellion kiteworks services. Once you have added these business hosts and configured them, the production can easily retrieve files from end-user accounts, or put files into those accounts, or both.

InterSystems IRIS authorizes access to the third-party transfer services using the Open Authorization Framework version 2.0 (known as OAuth 2.0). When you configure the InterSystems IRIS production to use the transfer service, you establish that production as an authorized user of the transfer service account. This allows the production to pull files from and place files into any of the directories under that account, such as those assigned to individual end-users. Access by these individual end-users are not affected at all in any way, and they can continue to place and retrieve files as before.

3 Trying MFT: Create an MFT-Enabled Production

Integrating MFT into an InterSystems IRIS production requires only a few steps: first, create and initialize the connection to the transfer service, and then include the appropriate business hosts that enable the production to talk directly with the transfer service. You can see just how easy it is by following the steps in this section to create a production that copies files between your Accellion kiteworks account and your local desktop system. If you are more comfortable with or already have access to Box or DropBox, just substitute the items for your service wherever kiteworks is used.

Important: The production created using these instructions uses default settings for the sake of simplicity. When creating a live production, InterSystems highly recommends that you adjust the settings as appropriate for your environment, particularly those related to security and your own particular InterSystems IRIS instance. For example, the **Redirect URL** mentioned below uses `http` instead of `https`, not a good practice in production.

Want to try an online video-based demo of InterSystems IRIS interoperability features? Check out the Interoperability QuickStart!

3.1 Before You Begin

To use this procedure, you will need a running instance of InterSystems IRIS. Your choices for InterSystems IRIS include several types of licensed and free evaluation instances; the instance need not be hosted by the system you are working on (although they must have network access to each other). For information on how to deploy each type of instance if you do not already have one to work with, see Deploying InterSystems IRIS in *InterSystems IRIS Basics: Connecting an IDE*.

You will also need administrative access to an account on Accellion kiteworks; you can create a free trial account at https://www.accellion.com/kiteworks/.

3.2 Create an SSL/TLS Configuration

Create an SSL/TLS configuration using the following procedure:

1. Open the Management Portal for your instance in your browser, using the URL described for your instance in *InterSystems IRIS Basics: Connecting an IDE*.
2. Navigate to the SSL/TLS configuration page (**System Administration** > **Security** > **SSL/TLS Configurations**).
3. Click **Create New Configuration** and for the **Configuration Name** field, enter `MFTTLSConfig`. Leave all other fields as is, and click **Save** to save this new configuration.

3.3 Register Your InterSystems IRIS Instance at the Transfer Service

You will next need to create an app (entry) for this MFT production on the transfer service itself. In a separate browser window or tab, go to the management page for your Accellion kiteworks account and perform these steps.

1. In the Management Portal, go to the **Customs Applications** page, which is under **Application > Client Management** (for version kw2017.02.04).

2. Add a new entry, and specify a name for the application such as **`ISCFileTransferApp`**.
3. Make sure **Authorization Code** and **Enable Refresh Token** are selected.
4. In the **Redirect URI** field, enter the URL http://*server*:*port*/csp/sys/oauth2/OAuth2.Response.cls, where *server* and *port* are the host identifier and web server port for you instance. For example, for a cloud instance, the URL might be

   ```
   http://35.192.42.98:52773/csp/sys/oauth2/OAuth2.Response.cls
   ```

   A locally installed instance could use localhost in the *server* field.

   This is the URL that kiteworks uses to contact the InterSystems IRIS instance.
5. Click **Add Application** and record the security tokens (**Client Application ID** and **Client Secret Key**) that are displayed. You will use this information later, when creating the SSL/TLS connection on InterSystems IRIS.

   Important: This information is available to you *only* at this time, so you must record it immediately. If you do not have this information when creating the SSL/TLS connection on the InterSystems IRIS production, then you must generate this information again and use the new values to create the SSL/TLS connection.

3.4 Add Directories at the Transfer Service

Now navigate to the main kiteworks (non-administrative) **Folders** page which displays your files and directories, and create two new top level directories, one named `FilesReceived` in which to receive files, and one named `FilesToSend` from which files are sent.

3.5 Add Directories Accessible to InterSystems IRIS

You should now create two directories on your instance's host in which InterSystems IRIS will access files. The way to do this depends on the type of instance you are using, as follows:

- For an instance deployed by ICM, use the **icm exec** command with the **-machine** and **-interactive** options to open a bash shell inside the container in which the instance is running, for example:

  ```
  icm exec -command bash -machine MYIRIS-AM-TEST-0004 -interactive
  ```

  You can then create the directories on the container file system.

- For any containerized instance, whether licensed or Community Edition, use the command **docker exec -it** *container_name* **bash** to open a bash shell in the container (the name of a Community Edition container is **`try-iris`**). Then create the directories on the container file system.
- For InterSystems Learning Labs, use the command-line terminal in the integrated IDE to create new folders in the Shared folder; you can browse to these in the Management Portal under /home/project/shared.
- For an installed instance, create the directories on the local file system.

This text assumes the following directory paths for an installed instance on a Windows system; substitute the paths of the actual directories you create.

```
C:\InterSystems\ToRemote
C:\InterSystems\FromRemote
```

3.6 Create the MFT Connection

Next, you need to register the transfer service on Intersystems IRIS by creating an MFT connection object. To do this, return to the Management Portal, and go to the **Managed File Transfer Connections** page (**System Administration** > **Security** > **Managed File Transfer Connections**). Click **Create Connection**. Specify values for the fields as follows, then click **Save**:

Field Name	Value
Connection Name	`KiteSecured`
File management service	`Kiteworks`
SSL/TLS configuration	`MFTTLSConfig`
Email address	The email address of your kiteworks administrator, such as *`MFTadmin@yourcompany.com`*
Base URL	The root URL to kiteworks for your organization, such as *`https://yourcompany.kiteworks.com/`*
OAuth 2.0 application name	`ISCFileTransferApp`
OAuth 2.0 client id	The **Client Application ID** retrieved earlier from kiteworks
OAuth 2.0 client secret	The **Client Secret Key** retrieved earlier from kiteworks
OAuth 2.0 redirect URL	Leave blank. Once you fill in the **Host name** and **Port**, this field automatically populates with the **Redirect URI** value provided earlier.
Use TLS/SSL	*(clear check box)*
Host name	The host identifier for your instance.
Port	The web server port for your instance.
Prefix	*(leave blank)*

3.7 Get an Access Token

The **Managed File Transfer Connections** page is displayed again with all available connections, including the new one that you just created. If that connection's status is `Not Authorized`, then:

1. Click **Get Access Token** to display the OAuth consent page from kiteworks, which identifies the name of the app as you had registered it earlier (**`ISCFileTransferApp`**).
2. Click **Grant Access** to authorize the access. This redisplays the **Connections** list, with the status of the new MFT connection now listed as `Authorized`.

3.8 Create the Namespace

In order to create a production, you must have an interoperability-enabled namespace. If you have already created an interoperability-enabled namespace, you can use that for this production. To create a new interoperability-enabled namespace, use the following procedure. (The namespaces created when you first install InterSystems IRIS are not interoperability-enabled.)

1. On the home page of the Management Portal, select **System Administration** > **Configuration** > **System Configuration** > **Namespaces** to go to the **Namespaces** page.
2. On the **Namespaces** page, select **Create New Namespace**. This displays the **New Namespace** page; follow the instructions for using this page in Create/Modify a Namespace in the "Configuring InterSystems IRIS" chapter of the *System Administration Guide*, making sure that the **Enable namespace for interoperability productions** check-box is selected.
3. Select **Save** near the top of the page and then select **Close** at the end of the resulting log.

3.9 Create the Production

Next, you need to switch into the new namespace to create the new production itself.

1. Go to the home page of the InterSystems IRIS Management Portal, and locate the namespace identifier in the center part of the top banner. Click the **Switch** link to bring up the **Namespace Chooser**.
2. Select the namespace you just created (for example, **`ForMFT`**), and click **OK**.
3. Now navigate to the **Production** page (**Interoperability** > **Configure** > **Production**).
4. Click **New** to bring up the **Production Wizard**.
5. For **Package**, select **INFORMATION** from the pulldown.
6. Enter a **Production Name** such as NewMFTProduction.
7. Leave the **Production Type** as **Generic**, and click **OK** to create the production.

For more information about productions, see "Introduction to Productions" in the "Introduction to InterSystems IRIS Interoperability" chapter of the *Introducing Interoperability Productions* guide.

3.10 Create Business Operations and Business Services

Remain in the newly-created production and add the four business operations and services required for file transport (one business operation and one business service for each direction):

Name of Business Host	Host Type	Use For
`SecureToRemoteOffice`	Business Operation	Sending files to transfer service
`GatherLocalFiles`	Business Service	Sending files to transfer service
`StoreFilesLocally`	Business Operation	Receiving files from transfer service
`ReceiveFromRemoteOffice`	Business Service	Receiving files from transfer service

3.10.1 Create and Configure: SecureToRemoteOffice

`SecureToRemoteOffice` is the business *operation* for sending files to the transfer service. To add this to the production:

1. Click the plus sign next to **Operations**.
2. Select the **Operation Class** EnsLib.MFT.Operation.Passthrough.
3. Enter the **Operation Name** SecureToRemoteOffice.
4. Make sure that **Enable Now** is unchecked, and leave the other fields alone.
5. Click **OK** to add the operation.
6. Select the operation, then from the panel on the right-hand side go to the **Settings** tab.

7. In the **Basic Settings** section, configure the following only:

Field Name	Value	Description
Enabled	*(check the box)*	Enables this business host
MFT Connection Name	`KiteSecured`	Name of the SSL/TLS configuration created earlier
Default MFT Folder	`/FilesReceived/`	Name of the top level *receiving* directory at the transfer service
Default Filename Specification	`%f`	Template for creating the name of the received file

8. Leave all other fields with their default settings, and click **Apply** to save your changes.

3.10.2 Create and Configure: GatherLocalFiles

`GatherLocalFiles` is the business *service* for gathering the files to send from InterSystems IRIS. To add this to the production:

1. Click the plus sign next to **Services**.
2. Select the **Service Class** EnsLib.File.PassthroughService.
3. Enter the **Service Name** GatherLocalFiles.
4. Make sure that **Enable Now** is unchecked, and leave the other fields alone.
5. Click **OK** to add the service,
6. Select the service, then from the panel on the right-hand side go to the **Settings** tab.
7. In the **Basic Settings** section, configure the following only:

Field Name	Value	Description
Enabled	*(check the box)*	Enables this business host
File Path	`C:\InterSystems\ToRemote\`	Directory on your local system containing the files to send (substitute the correct path if different).
File Spec	`*`	Regular expression for the names of files to send
Target Config Names	`SecureToRemoteOffice`	Business host that accepts input from this business service

8. Leave all other fields with their default settings, and click **Apply** to save your changes.

3.10.3 Create and Configure: StoreFilesLocally

`StoreFilesLocally` is the business *operation* for storing the received files in InterSystems IRIS. To add this to the production:

1. Click the plus sign next to **Operations**.
2. Select the **Operation Class** EnsLib.File.PassthroughOperation.
3. Enter the **Operation Name** StoreFilesLocally.
4. Make sure that **Enable Now** is unchecked, and leave the other fields alone.
5. Click **OK** to add the operation.
6. Select the operation, then from the panel on the right-hand side go to the **Settings** tab.
7. In the **Basic Settings** section, configure the following only:

Field Name	Value	Description
Enabled	*(check the box)*	Enables this business host
File Path	`C:\InterSystems\FromRemote\`	Directory on your local system to store the received files (substitute the correct path if different).
File Name	`%f_%Q%!+(_a)`	Syntax for the names of files to send. For uniqueness, InterSystems recommends incorporating a date and timestamp into the filenames.

8. Leave all other fields with their default settings, and click **Apply** to save your changes.

3.10.4 Create and Configure: ReceiveFromRemoteOffice

ReceiveFromRemoteOffice is the business service for receiving files from your transfer service. To add this to the production:

1. Click the plus sign next to **Services**.
2. Select the **Service Class** EnsLib.MFT.Service.Passthrough.
3. Enter the **Service Name** ReceiveFromRemoteOffice.
4. Make sure that **Enable Now** is unchecked, and leave the other fields alone.
5. Click **OK** to add the service.
6. Select the service, then from the panel on the right-hand side go to the **Settings** tab.
7. In the **Basic Settings** section, configure the following only:

Field Name	Value	Description
Enabled	*(check the box)*	Enables this business host
MFT Connection Name	`KiteSecured`	Name of the SSL/TLS configuration created earlier
MFT Source Folders	`/FilesToSend`	Name of the top level *sending* directory at the transfer service
Files to Retrieve	*(leave blank)*	Template for the name (types) of files to collect from the remote location
Target Config Names	`StoreFilesLocally`	Business host that accepts input from this business service

8. Leave all other fields with their default settings, and click **Apply** to save your changes.

3.11 Test the Production

Now that you've created the production, it's time to try it out! Just drag and drop a file into the designated folders at your local directory and at the third party transfer services, and watch them appear at the other location.

1. Start the production by clicking the **Start** button along the top, and then **OK** on the **Start Production** dialog.
2. To verify sending a file to kiteworks:
   a. Using your operating system's directory explorer, navigate to the directory you specified in the **FilePath** field when adding the *GatherLocalFiles* business service (`C:\InterSystems\ToRemote\` or a different directory that you created).
   b. Place a file in that location.
   c. Go to kiteworks and navigate to the `/FilesToRemote/` folder, (the directory you specified in the **Default MFT Folder** field when adding the *SecureToRemoteOffice* business operation).
   d. Refresh your view of the folder until the new file appears. This is usually within a few seconds, if not sooner.
3. To verify receiving a file from kiteworks:
   a. Go to kiteworks and navigate to the `/FilesToCentral` folder (the directory you specified in the **DefaultMFTFolder** field when adding the *ReceiveFromRemoteOffice* business service).
   b. Place a file in that location.
   c. Using your OS directory explorer, navigate to the directory you specified in the **FilePath** field when adding the *StoreFilesLocally* business operation (`C:\InterSystems\FromRemote\` or a different directory that you created).
   d. Refresh your view of the directory until the new file appears. This is usually within a few seconds, if not sooner.

Congratulations, you've just successfully created a working production using MFT!

4 Learn More About MFT

For more information, see:

- Video Introduction to Managed File Transfer
- *Enabling Productions to Use Managed File Transfer Services*