Managed File Transfer

QualityNet | MFT

Managed file transfer ("MFT") refers to a software or a service that manages the secure transfer of data from one computer to another through a network (e.g., the Internet). MFT is a managed file transfer solution that automates and secures file transfers using a centralized enterprise-level approach. MFT is a comprehensive solution that will manage file transfer, file sharing, secure FTP, and automation needs through a single interface. MFT is the Enterprise Services replacement for Axway Data Exchange.

Managed File Transfer (MFT) provides the ability to transfer files securely to another user. Users must be registered in HARP and have an MFT **Web User** role approved to send and receive files. Recipients of PHI / PII must be onboarded to MFT and senders may not utilize non-registered user option when sending PHI / PII. In addition, elevated permissions can be granted as **Administrators** to perform development work or request designation as a **Security Official**.

For information on the MFT application please refer to the MFT Confluence link - https://qnetconfluence.cms.gov/display/HS/Managed+File+Transfer.

For more information about HARP, please refer to the HARP Confluence page - https://qnetconfluence.cms.gov/display/HS/HARP.

For questions please contact the Service Center Help Desk via email at - *ServiceCenterSOS@cms.hhs.gov*

Prerequisites to Getting Access to MFT

Before requesting any role the prerequisite is that you have established a HARP account and your organization has onboarded with HARP. If you currently have an EIDM or EUA account, then you can go to HARP page and Login using EIDM/EUA credentials. Otherwise, if you do not have an EIDM or EUA account, then you need to request a HARP ID. If you already have a HARP ID, there is no need to create a new one.

Recipients of PHI / PII must be onboarded to MFT and senders may not utilize non-registered user option when sending PHI / PII.

Because HARP is a prerequisite, we will be targeting organizations who have already onboarded with HARP. If an organization has not identified and designated a Security Official for their organization, none of the requests from that organization will be approved.

QUICK START GUIDE

Step 1: Designate Security Official (SO) for Organization

Each organization designates a Security Official. This role will allow that individual to approve Web User role requests within their organization.

Step 2: Register for a HARP account

If you currently have an EIDM or EUA account then go to HARP page https://harp.cms.gov/ and Login using EIDM/EUA credentials

If you do not have an EIDM or EUA account then **Get HARP ID.** For instructions on obtaining a HARP ID, visit the **How to get a HARP ID Help Page**.

If you already have a HARP ID, there is no need to create a new one.

Notification Listserv

To receive notifications with news, release and maintenance information, sign up for the MFT ListServ. Users can be request to be added to our subscriber list by clicking on the link and following the instructions below:

ListServ Sign-up

1. On the page select the Private Lists tab
2. Enter Your Information
3. Select the checkbox next to MFT Notify: Managed File Transfer (MFT) Notifications
4. Click Submit

To unsubscribe from this list please send 'unsubscribe' to mft-notify-leave@mailer.qualitynet.org.

Need Help ?

- **CCSQ Support Central:** Provides you with multi-program support to submit a new ticket, and track the status of an existing case, incident, or request. No login required. https://cmsqualitysupport.servicenowservices.com/ccsq_support_central
- **Service Center:** For any MFT related issues or questions, Please contact the Service Center Support Team.

  Phone: (866) 288-8914 (TRS:711)

  Slack: #help-service-center-sos

  Email: ServiceCenterSOS@cms.hhs.gov

  Hours of Operation: 24/7

Step 3: Request Role

Once your HARP account has been created, log into HARP and request a User Role:

- Select the “Managed File Transfer” Program
- Select your Organization
  - Don't see your organization listed?
- Select a User role (Security Officer (SO) or Web User)

Visit the **How to get a HARP ID Help Page** to view a helpful video on requesting user roles.

Step 4: Access MFT

- Log into MFT using your HARP credentials: https://qnetmft.cms.gov.
- Enter your HARP ID
- Enter your HARP password

MFT WORK REQUEST PROCESS GUIDE

For Custom MFT work or enhancement requests, users will need to submit requests by completing the MFT Secure Form "MFT Request Form". This Secure Form allows users to submit requests /enhancements for the MFT application.

- MFT Work Request Process - MFT Work Request Process Guide.pdf
- MFT Work Request SOP - MFT Work Requests SOP.pdf

Links to user resources for MFT

- MFT User Web Guide - MFT_Web_Guide_v1.2.docx
- MFT End User Guide - MFTEndUserGuide_04302021.docx
- MFT Procedure for Custom Work Requests - MFT Work Requests SOP.pdf
- MFT Custom Work Request Process Guide - MFT Work Request Process Guide.pdf

---

User Definitions

MFT has two types of users, standard MFT Web users and Custom MFT Web Users and Administrators

1. **Standard MFT Web Users** - This primary group is defined as having the ability to send and receive files securely with others. Every HARP user can get this type of access.
   - Action requested: To get access, each organization must first designate a Security Official. This role will allow that individual to approve Web User role requests within their organization.
   - Once onboarded the designated SO receives a welcome letter via email.
   - Organizations that have contractors under them (i.e., hospitals, facilities, etc.) would follow the same model by designating a Security Official (SO) for their organization that would then be approved by the parent SO (i.e., EQRS, CDAC, etc.). These entities would also appear on the selection list and would be handled the same way as a known organizations would be.
2. **Custom MFT Web Users, Administrators, Security Officials** - This group of users are organizations that require custom onboarding and work flows.
   - Full engagement onboarding process including kick-off through an request intake form.
   - Organization to discuss responsibility level (ESS or organization performing the work).
   - Any organization that wants more than the initial MVP release falls under this category.

News & Updates

12/02/2021: As of December 2nd, 2021, any work requests or enhancement requests for Managed File Transfer (MFT) must be submitted via the MFT Secure Form "MFT Request Form". This Secure Form allows users to submit requests/enhancements for the MFT application. If you do not have access to MFT or need assistance with filling out the request, please contact Austin McGowan at amcgowan@tantustech.com. Once the form is completed, a JIRA number will be issued, and the work will be prioritized.

03/30/2021: (Update) As of March 30th, 2021, all files stored in MFT that have not been modified in the past 30 days will be removed from the MFT application. Beginning March 30th 2021, any future files stored in MFT that have not been modified in the past 30 days will be deleted from the MFT application in accordance to the newly implemented 30 day retention policy. The 30 day retention policy will not apply to files stored on the MFT platform that are managed by your organization through your S3 bucket.

12/17/2020: The MFT website was migrated from the .org URL to the new .gov URL on December 16, 2020. Users will access the MFT Website using the following new URL:https://qnetmft.cms.gov. This change will not impact your access to the MFT website.

12/16/2020: The Axway SFT (Data Exchange) application has been decommissioned and is no longer available.

MFT (Managed File Transfer) is the Enterprise Services replacement for Axway SFT (Data Exchange). A link providing MFT onboarding information is provided below. MFT requires users to be registered in HARP and have a MFT Web User role to send and receive files. For information on the MFT application please refer to the MFT Confluence link - https://qnetconfluence.cms.gov/display/HS/Managed+File+Transfer.For more information about HARP, please refer to the HARP Confluence page - https://qnetconfluence.cms.gov/display/HS/HARP.

12/11/2020: The intermittent issues with creating / removing users in MFT from 12/10/2020 has been resolved. If you are still experiencing issues with accessing MFT after your account has been approved, please submit a ticket to the QNET Helpdesk.

12/10/2020: Reminder: The MFT website will be migrating from a .org URL to a .gov URL on December 16, 2020. Users will access the MFT Website using the following new URL: https://qnetmft.cms.gov. This change will not impact your access to the MFT website.

08/27/2020: MFT-Notify distribution list. Users can request to be added to list on https://www.qualitynet.org/ to receive MFT release and maintenance information. Choose 'Subscribe to Email Updates' / ' then choose 'Private Lists' / Enter User Information / then check 'MFT Notify: Managed File Transfer (MFT) Notifications' / and click 'Submit'.

03/11/2020: If your email address needs to be updated in MFT, please log on to HARP and update your email address accordingly. If you updated your email address in HARP prior to 3/9/2020 and it is not reflected in MFT, please log into HARP, revert back to your previous email address, update and then subsequently update to the desired email address. Once the update occurs on HARP, the change will be reflected in MFT.

03/11/2020: The MFT Team has identified a maximum threshold of 45 GB for secure file transfers through the MFT web application. Files in excess of this size will not be processed. Because the files are transferred via HTTPS, there are transfer limitations depending on the browser used. If you have a file in excess of 2 GB, you must use either Firefox or Chrome. Internet Explorer and Microsoft Edge have thresholds of 2 GB and under and files attempted to be transferred through these browsers in excess of 2 GB will not be processed.

03/04/2020: Managed File Transfer (MFT) will be unavailable this evening March 4th after 8:00 pm for 15 minutes to perform routine maintenance.

FAQs

GENERAL | ACCESS | Working in MFT

General

Managed file transfer ("MFT") is an application for the CMS HCQIS community to securely transfer data files over the internet. MFT provides the capabilities for transferring data files from person-to-person(s) using MFT Secure Mail or from person-to-system (i.e. Amazon S3 Bucket) through MFT Secure Forms.

The MFT transfer capabilities are provided by the GoAnywhere MFT COTS product.

All MFT users MUST have an CMS Okta account and On-Board to the CMS HARP application and be granted access by their Security Official to access MFT. MFT users log into the MFT Web Console to access the secure transfer functions (i.e. Secure Mail, Forms, local Files).

Recipients of PHI / PII must be onboarded to MFT and senders may not utilize non-registered user option when sending PHI / PII.

Internal users; i.e., the Centers for Medicare & Medicaid Services (CMS) and CMS Contractors, can exchange messages and files with internal users and also external users such as providers and vendors.

The MFT web user is the end user; this person will have the ability to complete person to person secure file transfers. All MFT users MUST have an CMS Okta account and On-Board to the CMS HARP application and be granted access by their Security Official to access MFT. MFT users log into the MFT Web Console to access the secure transfer functions (i.e. Secure Mail, Forms, local Files). Recipients of PHI / PII must be onboarded to MFT and senders may not utilize non-registered user option when sending PHI / PII.

The Security Official (SO) is a person that is designated by a line of business (LoB) or other CMS contractor who has the authority to approve requests for managed file transfer access made by users within that particular line of business or contract.

Access

Yes, a HARP ID is required to access MFT. All MFT users MUST have an CMS Okta account and On-Board to the CMS HARP application and be granted access by their Security Official to access MFT. MFT users log into the MFT Web Console to access the secure transfer functions (i. e. Secure Mail, Forms, local Files).

Recipients of PHI / PII must be onboarded to MFT and senders may not utilize non-registered user option when sending PHI / PII.

For instructions on this process, visit the HARP page.

A registered MFT user with a HARP ID can send a file through MFT to a non-registered user. The non-registered user can retrieve the file without having a HARP ID. The non-registered user receiving secure mail is unable to respond back to the sender or send a file. The sender will need to ensure the "**Require Registered Users"** checkbox is NOT checked when sending a message.

Recipients of PHI / PII must be onboarded to MFT and senders may not utilize non-registered user option when sending PHI / PII.

Visit the HARP page for instructions on how to register for a HARP account.

Users must register for a HARP ID. Once the HARP account has been created, log into HARP and request a User Role.

- Log into HARP and request a User Role
- Select the “Managed File Transfer” Program
- Select your Organization
- Select a User role (Security Officer (SO) or Web User)

Security Official Role

- The Security Official (SO) is a person that is designated by a line of business (LoB) or other CMS contractor who has the authority to approve requests for managed file transfer access made by users within that particular line of business or contract
- It is initially up to the CMS representative for the LoB to designate themselves as SO or appoint another SO
    - As an example, the CMS representative could be your Product Owner
    - You will need to identify your CMS representative before onboarding
- The initial SO must be designated and approved before any access will be granted to requests to utilize managed file transfer functionality
- There can be more than one SO appointed as determined by the CMS LoB representative
- It is the determination of the CMS LoB representative to on how they want to implement SO roles for the LoB as well as the contractors under their LoB. Until this methodology is known and published, we will not prioritize
- If you are unsure who your SO is, you will need to contact your CMS representative to have them make that determination
- The SO only approves the web user role or other SOs for the LoB.
- HARP Security Official Role video HARP Page.

PM3 is currently handling both individual request and bulk updates. PM3 is currently loading the first SO. The first SO can then approve additional SO request.

Check with their SO to confirm the name they should be looking for.

If they do not know who their SO is, then PM3 should be contacted.

When an individual from your line of business /organization requests access to MFT, they will select an organization. This label represents what the users will see in the selection list.

Administrative User Role

- MFT has numerous capabilities that can be leveraged for customized development of workflows and functions. The administrator role in this instance acts as a developer.
- When an individual from your line of business /organization requests access to MFT, they will select an organization. This label represents what the users will see in the selection list.
- Out of the box, the main function of MFT is to provide person to person secure file transfers. If more functionality is needed then a customized onboarding process is required including filling out a custom RFI form.
- Requesting an admin role requires going through a custom onboarding.

- If yes, a member of the onboarding team will reach out to you to obtain documentation on the type(s) of PHI / PII being transferred after the initial line of business / organization has been onboarded
- Recipients of PHI / PII must be onboarded to MFT and senders may not utilize non-registered user option when sending PHI / PII.

Out of the box, the main function of MFT is to provide person to person secure file transfers.

- If no, no further action needs to be taken.
- If yes, a member of the onboarding team will reach out to you after the initial line of business / organization has been onboarded to begin a request intake form on functionality needed.

Out of the box, the main function of MFT is to provide person to person secure file transfers. It is assumed that all organizations require, at least, standard MFT Web User access. Please review the End User Guide. After reviewing the End User Guide documentation, do you believe your organization(s) users require more MFT capabilities than a standard Web User role provides (Person to Person Secure File Transfer)?

- MFT Procedure for Custom Work Requests - MFT Work Requests SOP.pdf
- MFT Work Request process Guide - MFT Work Request Process Guide.pdf

1. Getting my HARP ID HARP Help Page
2. HARP User Profile HARP Help Page
3. HARP Security official Role video HARP Help Page
4. HARP User Roles HARP Help Page

Working in MFT

- MFT User Web Guide - MFT_Web_Guide_v1.2.docx
- MFT End User Guide - MFTEndUserGuide_04302021.docx
- MFT Procedure for Custom Work Requests - MFT Work Requests SOP.pdf
- MFT Work Request process Guide - MFT Work Request Process Guide.pdf

A video is currently under development.

Log into:

- Web Users: https://qnetmft.cms.gov.
- Enter your HARP ID
- Enter your HARP password

If you have a file in excess of 2 GB, you must use either Firefox or Chrome, which have been identified as having a threshold of about 40 GB. Internet Explorer and Microsoft Edge have thresholds of 2 GB and under and files attempted to be transferred through these browsers in excess of 2 GB will not be processed. There are no known constraints on the number of attachments but the total cumulative size of the files applies as referenced above.

Users can request to be added to MFT Notify list at https://www.qualitynet.org/ to receive MFT release and maintenance information. Choose 'Subscribe to Email Updates' / choose 'Private Lists' / Enter User Information / then check 'MFT Notify: Managed File Transfer (MFT) Notifications' / and click 'Submit'.

- Service Center

1-866-288-8912 (TRS: 711) from 7:00 AM to 7:00 PM CT Monday through Friday, or via email at *ServiceCenterSOS@cms.hhs.gov*