# Table of Contents

- Introduction ........................................................................................................................................... 3
- Supported File Transfer Protocols and Hosts/Ports .............................................................................. 3
- Naming Conventions ............................................................................................................................... 3
- Accessing the Service ............................................................................................................................. 3
- Uploading Files ......................................................................................................................................... 3
- Downloading Files Shared by Customer Support ...................................................................................... 4
- Protocol #1 – HTTPS Detailed UI Walkthrough ....................................................................................... 5
- Protocol #2 – SFTP ..................................................................................................................................... 10
- Protocol #3 – FTPS .................................................................................................................................... 11
- FTPS and SFTP From z/OS ...................................................................................................................... 12
  - Setting up your environment for FTPS transfers ............................................................................... 12
    - Creating the certificates ................................................................................................................... 12
    - To use RACF to prepare your environment .................................................................................... 12
    - To use CA Top-Secret to prepare your environment ..................................................................... 12
    - To use CA-ACF2 to prepare your environment ............................................................................. 15
  - Transferring Data ................................................................................................................................... 15
    - Preparing files for transfer .............................................................................................................. 16
    - Executing file transfers ................................................................................................................... 17
    - To execute an FTPS transfer ............................................................................................................ 18
    - To Execute an SFTP transfer ............................................................................................................ 18
    - Verifying and communicating results ............................................................................................ 19
- FAQ ............................................................................................................................................................... 20
  - Which file transfer protocol is best to use? ........................................................................................... 20
  - Why do I receive a zip file when I download a file using a web browser (HTTPS)? .............................. 20
  - Why do I see a file created/modified greater than 30 days when uploaded files are deleted after 30 days? .................................................................................................................................................. 20
  - What IPs should be whitelisted if my security policies require whitelisting? ...................................... 21
- Known Issues .............................................................................................................................................. 22
Introduction
To enhance the protection of files shared with us, BMC has implemented a secure file transfer service supporting SFTP, FTPS, and HTTPS protocols. This service is an alternative to attaching a file to a Case via BMC Support Central, and must always be used for files which exceed the 2GB limit for Case attachment file size. Files that are 2GB or smaller can be attached directly to Cases.

Supported File Transfer Protocols and Hosts/Ports
The protocols available are as follows:

- Protocol #1 - HTTPS – URL: https://mft.bmc.com (direct access via web browser)
- Protocol #2 - SFTP - host mft.bmc.com and port 22 (requires client application)
- Protocol #3 - FTPS (implicit) - host mft.bmc.com and port 990 (requires client application)

Naming Conventions
To ensure that Cases are resolved as quickly as possible, it is important that Customer Support be able to efficiently locate uploaded files. We ask that you create a separate folder for each Case, and only place files related to that Case in the folder. More details on the folder naming convention are in the usage sections below.

Accessing the Service
- Before you can access any of file transfer services, you must have a Support Central registered account with at least one associated Support subscription. If you have not previously registered on Support Central, click here to register. To complete your registration / subscription, you will need access to your company email account, and a valid Support ID and PIN.

If you have problems registering, please contact Customer Care by email (customer_care@bmc.com) or by phone.

NOTE: Your home folder is created the first time you access one of the services. BMC cannot create your home folder for you, so we suggest you use your web browser to access the HTTPS service as soon as you have completed the registration process, so your home folder is ready for use.

To perform secure file transfers from mainframe systems, please see FTPS and SFTP from z/OS.

Uploading Files
- When you log-in, you will be placed in your personal home folder.
- Accounts and folders are individual – you will only see your folders and files.
- Uploading a file
  - When you need to upload one or more files related to a Case, please create a folder for that Case in your home folder, and name it ‘case_<case number>’ (case_012345). That will allow Support to locate your files efficiently.
- Once you have uploaded the needed files, please let Customer Support know by updating the Case on Support Central, or by replying to an existing email from us.
- **NOTE:** for security, files you upload are deleted from the repository after 30 days.

**Downloading Files Shared by Customer Support**

- Because accounts are individual, Customer Support cannot place files directly in folders you created for uploading files, your folders are read-only for Support. For us to share a file with you, Support must specifically share an “outgoing” folder with you.
- When Customer Support shares a folder with you, you will receive an email with a link in to allow you to accept or reject the shared folder. Unless you believe you received the invitation in error, **please click the link to accept the sharing invitation.**
- Once you accept a shared folder, it will be shown in your home folder when you log in.
- Shared folders are folder with a ‘two people’ icon 📦.
- Customer Support has been instructed to name shared “outgoing” folders using a naming convention similar to the one to be used for your folders ‘outgoing case_<case number>’ (outgoing_case_543210).
Protocol #1 – HTTPS Detailed UI Walkthrough

Login screen (https://mft.bmc.com)

DISCLAIMER:

By using this site, you acknowledge and agree that BMC will process Personal Information according to its BCR Policy and Privacy Policy. Processing of Customer Support data is further described in BMC Support Privacy Policy.

By downloading from this site you acknowledge that you are responsible for complying with the export laws and regulations of the United States and all other relevant countries for export and re-export.

Note: for BMC Employees - you will have to be on the BMC network/VPN to login.
When you log in for first time you will see an empty home folder.

When you need to share a file for a Case, create a folder for the Case following the folder naming convention ‘case_<case number>’.
Click the folder name to open it.

In the folder view, you can use drag and drop to upload files.
Once the upload completes, please update your Case via Support Central or by replying to a prior email to let Customer Support know that you’ve provided the requested information.

When Customer Support needs to provide a file to you, they will *share a folder with you individually*. You will get an email like this example. Unless you think you received the invitation in error, please immediately click ‘Accept the Folder’ to access it.
Alternatively, in the web interface, you can click to open the ‘Shared Files’ folder, then click ‘Accept’ from the gear icon by the shared folder name.

The shared folder/files will be visible in your home folder.
Protocol #2 – SFTP

You can choose any client to connect and use the SFTP protocol, and each one will be slightly different, all have similar requirements.

The image below is an example using Filezilla. The Host is set to ‘sftp://mft.bmc.com’ and a valid username and password supplied.
Protocol #3 – FTPS

You can choose any client to connect and use the FTPS protocol, and each one will be slightly different, all have similar requirements.

The image below is an example using Filezilla. The Host is set to ‘ftps://mft.bmc.com’ and a valid username and password supplied.
FTPS and SFTP From z/OS

Setting up your environment for FTPS transfers
FTPS requires two ports; a control port and a data port. Please verify that your FTPS Client has these ports open.

- The control port (or listening port) is **990**
- The data port range for passive/extended passive is **30000 – 32000**

To set up your environment for FTPS transfers, use your system security package to authorize your security certificate and all users who will need to transfer data. Complete the appropriate procedure:

- **Creating the certificates**
- **To use RACF to prepare your environment**
- **To use CA Top-Secret to prepare your environment**
- **To use CA-ACF2 to prepare your environment**

**Note:** The following procedures simply outline the required tasks and commands. Consult your system security administrator to prepare for using the FTPS method in your environment.

Creating the certificates
Your IBM z/OS system must have the DigiCert Global Root G2 security certificate. Typically, the certificate resides in a sequential, variable-blocked data set.

If the certificate is not present, you must complete the following steps before proceeding:

1. Download the DigiCert Global Root G2 from:
   
   https://docs.bmc.com/docs/display/bmcmainframe/Security+certificates

2. Create a sequential, variable-blocked (LRECL 255, BLKSIZE 32760 recommended) data set to contain the certificate on your z/OS system. Assign a data set name that identifies the contents (for example, 'SYS1.CA.CERT').

   1. Copy and paste the DigiCert Global Root G2 certificate into SYS1.CA.CERT
      a. **Include the dashed top and bottom lines. Preserve the existing case, and do not change any characters in this text.**

To use RACF to prepare your environment

1. Ensure that your IBM RACF database contains an entry for the DigiCert Root Server Certificate.
2. If the certificate (SYS1.CA.CERT) is not present in your RACF database, add it by entering the following command:

```
RACDCERT CERTAUTH
   ADD('SYS1.CA.CERT') -
   TRUST -
   WITHLABEL('DigiCert Global Root G2')
```

**NOTE:** If you receive a duplicate error that the certificate already exists in your security database, you can proceed to step 5.

3. If Status line in your certificate (SYS1.CA.CERT) is not set to TRUST, change the status:

```
RACDCERT -
   ALTER { -
   LABEL('DigiCert Global Root G2’) -
   } -
   CERTAUTH -
   TRUST
```

4. For each user who is authorized to transfer files to the BMC FTP site, complete these steps:
   a. Create a RACF keyring:

```
RACDCERT ADDRING(FTP.TLS.KEYRING) ID(userID)
```

5. Connect the certificate to the newly created keyring:

```
RACDCERT -
   CONNECT{ -
   CERTAUTH -
   USAGE(CERTAUTH) -
   LABEL('DigiCert Global Root G2') -
   RING(FTP.TLS.KEYRING) -
   }
```

6. Refresh the RACLST DIGTCERT and DIGTRING classes:

```
SETROPTS RACLST(DIGTCERT DIGTRING) REFRESH
```

7. Create a SYSFTPD data set (FTP DATA) that contains the following entries:

```
SECURE_MECHANISM TLS
    or
TLSMECHANISM   ATTLS ; IF USING AT-TLS

KEYRING userid/FTP.TLS.KEYRING
    or
KEYRING *AUTH*/* ; Virtual keyring

SECUREIMPLICITZOS FALSE ; Required

FWFRIENDLY TRUE
DEBUG SEC ; OR DEBUG ALL
EPSV4 TRUE ; DIRECTS THE CLIENT TO USE EPRT AND
EPSV commands on IPv4 sessions.

PASSIVEIGNOREADDR TRUE
SECURE_HOSTNAME OPTIONAL;

8. Grant access to other users who need to use the service by issuing the following commands:

PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(<userid>)
ACCESS(UPDATE)
PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(<userid>) ACCESS(READ)
SETR RACLIST(FACILITY) REFRESH

To use CA Top-Secret to prepare your environment

1. Create keyring:
   Issue the below command to create the keyring.
   
   TSS ADD(<Acid>) KEYRING(FTP.TLS.KEYRING) LABELRING('DigiCert Global Root G2')

2. Add the ROOT certificate:
   Issue the below command to add the certificate to the top secret database.

   TSS ADD(CERTAUTH) DIGICERT(cacert) dcdsn('SYS1.CA.CERT')
   LABELCERT('DigiCert Global Root G2') TRUST

3. Add the certificates to the keyring
   Issue the below command to add the keyring:
   
   TSS ADD(<Acid>) KEYRING(FTP.TLS.KEYRING) RINGDATA(CERTAUTH,cacert)
   USAGE(CERTAUTH)

4. Grant access permission to read key rings and certificates:
   Issue the below commands to allow users to use the keyring and certificates:

   TSS PER(<Acid>) IBMFAC(IRR.DIGTCERT.LISTRING) ACC(UPDATE)
   TSS PER(<Acid>) IBMFAC(IRR.DIGTCERT.LIST) ACC(READ)
To use CA-ACF2 to prepare your environment

1. Create a keyring:

   Set profile(user) div(keyring)
   Insert <userID.ringID> ringname(<ringname>)

   “userID” is the TSO ID.
   “ringID” is the keyring record that will be created in ACF2.
   “ringname” is the keyring name.

2. Install the Global Root Security certificate using the below CA-ACF2 command:

   Set profile(user) div(certdata)
   Insert CERTAUTH.<ROOTcertname> dsn('SYS1.CA.CERT') label(DigiCert Global Root G2) TRUST

   “ROOTcertname” is the certificate name.
   “SYS1.CA.CERT” is the dataset name where you wish to upload the certificate in mainframe
   “DigiCert Global Root G2” is the label of the certificate you are installing

3. Connect the certificate to the keyring

   SET PROFILE(USER) DIV(KEYRING)
   Connect certdata(CERTAUTH.<ROOTcertname>) keyring(<userID>.FTP.TLS.KEYRING ) usage(certauth)

   “ROOTcertname” is the certificate name.
   “userID” is the TSO ID.
   “ringID” is the keyring record that will be created in ACF2.

4. Grant access to users to use the service

   $KEY(IRR) TYPE(FAC)
   DIGTCERT.LIST UID(user UID string) SERVICE(READ) ALLOW
   DIGTCERT.LISTRING UID(user UID string) SERVICE(UPDATE) ALLOW

5. Do a rebuild

   F ACF2,REBUILD(USR),CLASS(P)
   F ACF2,OMVS(CERTDATA)
   F ACF2,REBUILD(FAC)

   While specifying the keyring for connection user has to specify “<userID>/<ringname>” for successful connection. For example, if userID is user1 and ringname is keyring1 then user has to specify “user1/keyring1”

6. List a Keyring (Optional):

   Set profile(user) div(keyring)
   List ftp.tls.keyring
Transferring Data

After setting up your environment, you can exchange files with BMC by completing the following procedures:

- Preparing files for transfer
- Executing file transfers
- Verifying and communicating results

Preparing files for transfer

Listed below are different ways to prepare the file for transfer. BMC recommends using AMATERSE to compress the original data set and BINARY mode transfer of the compressed copy.

- Compress the data set by using the AMATERSE utility, as shown in the following example. AMATERSE stores the DCB information on the original data set in the compressed copy, prevents errors with variable-length records, and significantly reduces the number of bytes transferred.

```
//TERSE      EXEC  PGM=AMATERSE,PARM=PACK
//SYSPRINT   DD   SYSOUT=* 
//SYSUT1     DD   DISP=SHR,DSN=hlq.Inumber.DATA.REPRO 
//SYSUT2     DD   DSN= hlq.Inumber.DATA.TERSE, 
 //   DISP=(NEW,CATLG,DELETE),UNIT=DISK, 
 //   SPACE=(CYL,(200,100),RLSE), 
 //   BLKSIZE=27648 
//*   DCB attributes after TERSE
//*    Organization . . . : PS
//*    Record format . . . : FB
//*    Record length . . . : 1024 
//*    Block size . . . . : 27648. 
/*
```

- If you are transferring a non-linear VSAM file (for example, SMF/CMF records or historical data sets), execute the IDCAMS REPRO utility to produce a sequential data set as shown in the following example:

```
//COPY       EXEC  PGM=IDCAMS,REGION=4M 
//SYSPRINT   DD    SYSOUT=* 
//HISTDS     DD    DISP=SHR,DSN=vsamDataSetName 
//SEQ        DD    DSN=hlq.Inumber.DATA.REPRO, 
 //   DISP=(NEW,CATLG,DELETE), 
 //   UNIT=SYSDA,SPACE=(CYL,200), 
 //   DCB=(RECFM=VB,LRECL=32000,BLKSIZE=0) 
//SYSIN      DD *
//   REPRO INFILE(HISTDS) -
//   OUTFILE(SEQ)
/*
```

Note: While attaching files to the case has a maximum size of 2GB, BMC recommends FTPing ALL SVCDUMPs rather than attaching to a case. This ensures the formatting of the file will be correct.
DCB attributes after REPRO
Organization . . . : PS
Record format . . . : VB
Record length . . . : 32000
Block size . . . . : system-determined

- If you are transferring a linear data set (for example, some registry data sets), use fixed record format on the sequential copy and a logical record length equal to the CISIZE of the VSAM data set as shown in the following example:

```
//COPY EXEC PGM=IDCAMS,REGION=4M
//SYSPRINT DD SYSOUT=*  
//REGISTRY DD DISP=SHR,DSN=vsamLDSDataSetName  
//SEQ DD DSN=hlq.Inumber.DATA.REPRO,  
// DISP=(NEW,CATLG,DELETE),  
// UNIT=SYSDA,SPACE=(CYL,(200,100),RLSE),  
// DCB=(RECFM=FB,LRECL=4096,BLKSIZE=0)  
//SYSIN DD *  
REPRO INFILE(HISTDS) -  
OUTFILE(SEQ)  

/*  
DCB attributes after REPRO  
Organization . . . : PS  
Record format . . . : FB  
Record length . . . : 4096 (CISIZE of input data set)  
Block size . . . . : system-determined  
*/
```

Executing file transfers

The procedure that you use to execute a file transfer depends on your chosen transfer method:

- To execute an FTPS transfer
- To execute an SFTP transfer

Before you Begin

To download a sample FTPDATA for transfer, see:

**KA 180309**

Keep the following guidelines in mind:

- When you edit JCL, set CAPS OFF and NUM OFF.
- When you edit JCL, delete any unneeded text from columns 73 through 80. Clearing these columns is important because the transfer process reads all 80 characters of input. You might need to scroll to see the contents of columns 73 through 80.

*Note:* Clearing these columns is important because the transfer process reads all 80 characters of input. You might need to scroll to see the contents of columns 73 through 80.
To execute an FTPS transfer

1. Create a job step to execute the FTPS transfer of a file, as shown in the following example:

```plaintext
//FTP EXEC PGM=FTP,PARM='(EXIT'
//*
//STEPLIB DD DSN=TCPIP.SEZATCP,DISP=SHR
//SYSFTPD DD DISP=SHR,DSN=hlq.FTP.CERT.JCL(FTPDATA) ← Sample see KA180309
//SYSPRINT DD SYSOUT=* 
//OUTPUT DD SYSOUT=* 
//INPUT DD *

mft.bmc.com 990
Your Support Central Login (email address)
Your Support Central Password
bin
mkdir Case_XXXXXXXX
cd Case_XXXXXXXX
put 'yourMainframeDataSetName' Cnnnnnnn.contentType.trs
quit
/*
```

2. Submit the JCL for execution.

To Execute an SFTP transfer

1. Add your password to the askpass.sh script file, which is located in your z/OS UNIX home directory.

2. Create JCL to execute the transfer job.

   The following example shows a transfer job for IBM Ported Tools.

   ```plaintext
   //STEPNAME EXEC PGM=BPXBATCH,
   // PARM=('sh sftp Your_Support_Central_Email@mft.bmc.com')
   //SYSPRINT DD SYSOUT=* 
   //STDIN DD PATH='/home/userID/sftpCmds'
   //STDOUT DD PATH='/home/userID/bpxout.txt', PATHOPTS= (OCREAT,OTRUNC,OWRONLY),PATHMODE=SIRWXU
   //STDERR DD PATH='/home/userID/bpxerr.txt', PATHOPTS= (OCREAT,OTRUNC,OWRONLY),PATHMODE=SIRWXU
   //STDENV DD *
   DISPLAY=FOO
   SSH_ASKPASS=/home/userID/askpass.sh
   /*
   ```

   **WARNING:** If your Support Central password or dataset name contains any of the below characters, your batch job will fail. These characters have special meaning in UNIX and cause failures.

   `$   >    <    (     )    '    “    `   /   |   &   ;`

   You will either need to change your BMC Support Central password/Dataset name or FTP using FTPS or windows-based FTP.
3. Create a new member in your z/OS UNIX home directory and put your FTP transfer commands into this member. You can use any valid name for this member. The following examples use sftpCmds.

```bash
!cp "//'yourMainframeDataSetName'" Cnnnnnnn.contentType.trs
mkdir Case_XXXXXXXX
cd Case_XXXXXXXX
binary
put Cnnnnnnn.contentType.trs
!rm  Cnnnnnnn.contentType.trs
quit
```

**Note:** Ensure local USS filesystem has sufficient space to hold ‘yourMainframeDataSetName’

4. Submit the JCL for execution.

**Verifying and communicating results**

When the file transfer is complete, verify that the transfer was successful and notify BMC. Use the following procedure:

1. To confirm that the transfer was successful, check for authentication messages such as those in the following example:

   ```
   EZA1736I  mft.bmc.com 990
   EZA1554I Connecting to: mft.bmc.com 198.147.194.180 port: 990.
   EZA2895I Authentication negotiation succeeded
   EZA2919I Session starts with protection on the data connection
   ```

2. After each transfer completes successfully, inform BMC of the transfer by either updating your case on the BMC Support Central website or sending an e-mail message to customer_support@bmc.com.

3. Provide the following details for every file that you send:
   - BMC Case number
   - The size of the file in bytes (usually displayed by the FTP client program after transferring each file)
   - The organization of the original data set (sequential, partition, or copy of VSAM data set)
   - The type of data in the file (for example, SVC dump, SMF, GTF, and so on) and other relevant information such as the name of the affected system, task, or region

BMC recommends using AMATERSE to compress the original data set and BINARY mode transfer of the compressed copy. If you did not use, include all the following information in your update:

- Mode of transfer (ASCII or BINARY)
- Record format (RECFM) of the original data set
- Logical record length (LRECL) of the original data set
- Type of compression used (i.e. AMATERSE, IDCAMS REPRO, etc.)
FAQ

Which file transfer protocol is best to use?

In terms of speed, HTTPS or FTPS are recommended as they are faster than SFTP.

Why do I receive a zip file when I download a file using a web browser (HTTPS)?

If you click a single file icon or link as in the image below, you will just download that one file. If you click the check box(es) next to one or more files and then click the download button at the bottom of the screen, the tool will download a zip file containing the file(s) selected — even if only one file is selected.

Why do I see a file created/modified greater than 30 days when uploaded files are deleted after 30 days?

That is a file shared with you by BMC. Files you upload are deleted after 30 days, files BMC shares with you are kept in the repository for six months.
What IPs should be whitelisted if my security policies require whitelisting?

Hostname = mft.bmc.com

Primary Addresses:

198.147.194.181
198.147.194.182

Secondary Address (in a failover situation):

198.175.230.239
Known Issues

If you are logged-in to the web browser interface (HTTPS) when you click “Accept the Folder” in the sharing invitation email, the folder will appear to be shared, but will not be accessible.

This is a known bug that our application vendor will fix at some point in the future.

If this happens to you, please ask Customer Support to share the folder with you again, and ensure that you are not logged-in the web browser interface when you click ‘Accept the Folder.’