



# Secure File Transfer User Guide for BMC Customers

August 28, 2019

## 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 .....	13
To use CA Top-Secret to prepare your environment.....	15
To use CA-ACF2 to prepare your environment.....	16
Transferring Data .....	17
Preparing files for transfer .....	17
Executing file transfers.....	18
To execute an FTPS transfer .....	19
To Execute an SFTP transfer.....	19
Verifying and communicating results .....	20
FAQ.....	21
Which file transfer protocol is best to use? .....	21
Why do I receive a zip file when I download a file using a web browser (HTTPS)?.....	21
Why do I see a file created/modified greater than 30 days when uploaded files are deleted after 30 days? .....	21
What IPs should be whitelisted if my security policies require whitelisting?.....	22
Known Issues.....	23

## 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](mailto: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>)



User Name

Password

Login

**DISCLAIMER:**

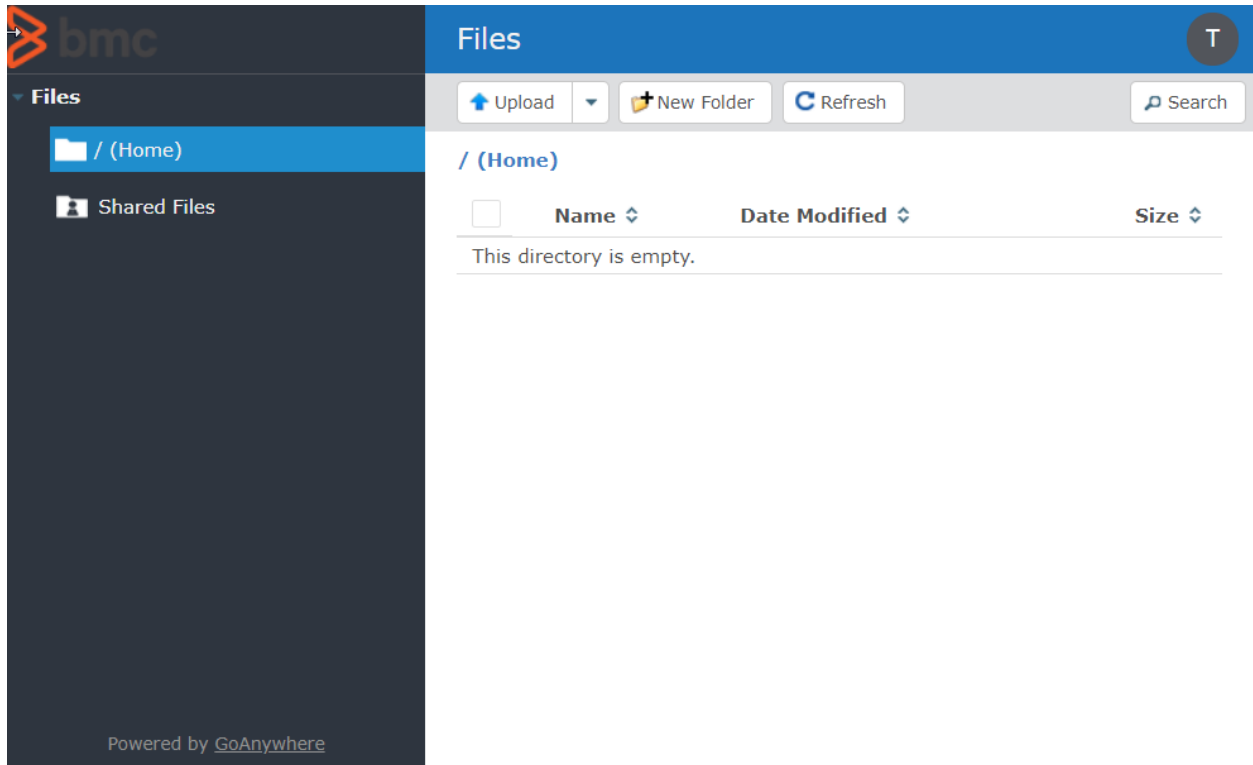
By using this site, you acknowledge and agree that BMC will process Personal Information according to its [BCR Policy](#) and [Privacy Policy](#). Processing of Customer Support data is further described in [BMC Support Privacy Policy](#).

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.

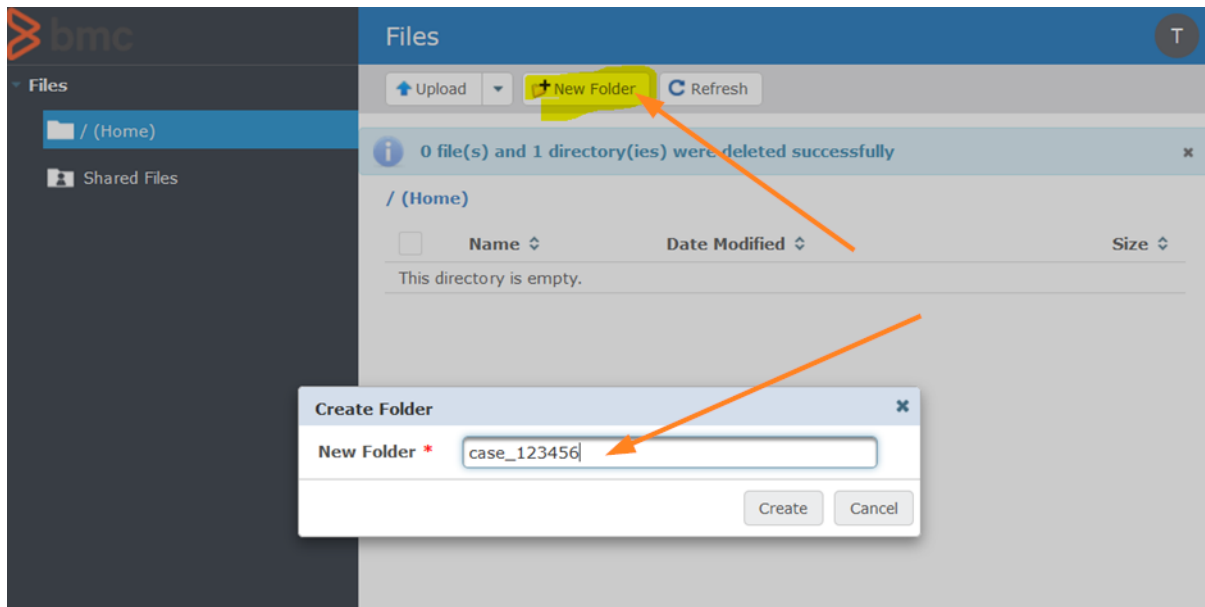
**Note: for BMC Employees - you will have to be on the BMC network/VPN to login.**

Powered by [GoAnywhere](#)

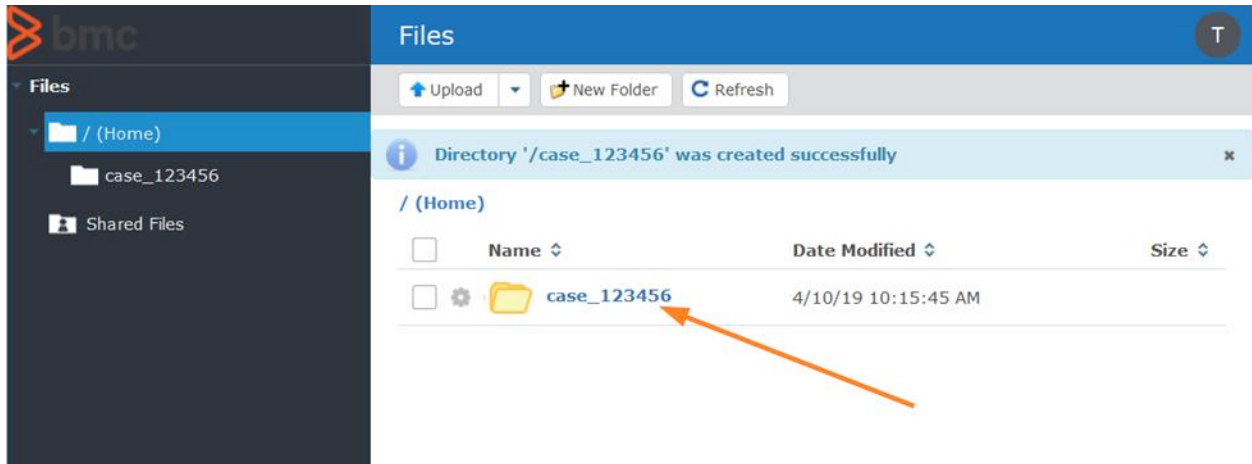
When you log in for first time you will see an empty home folder.



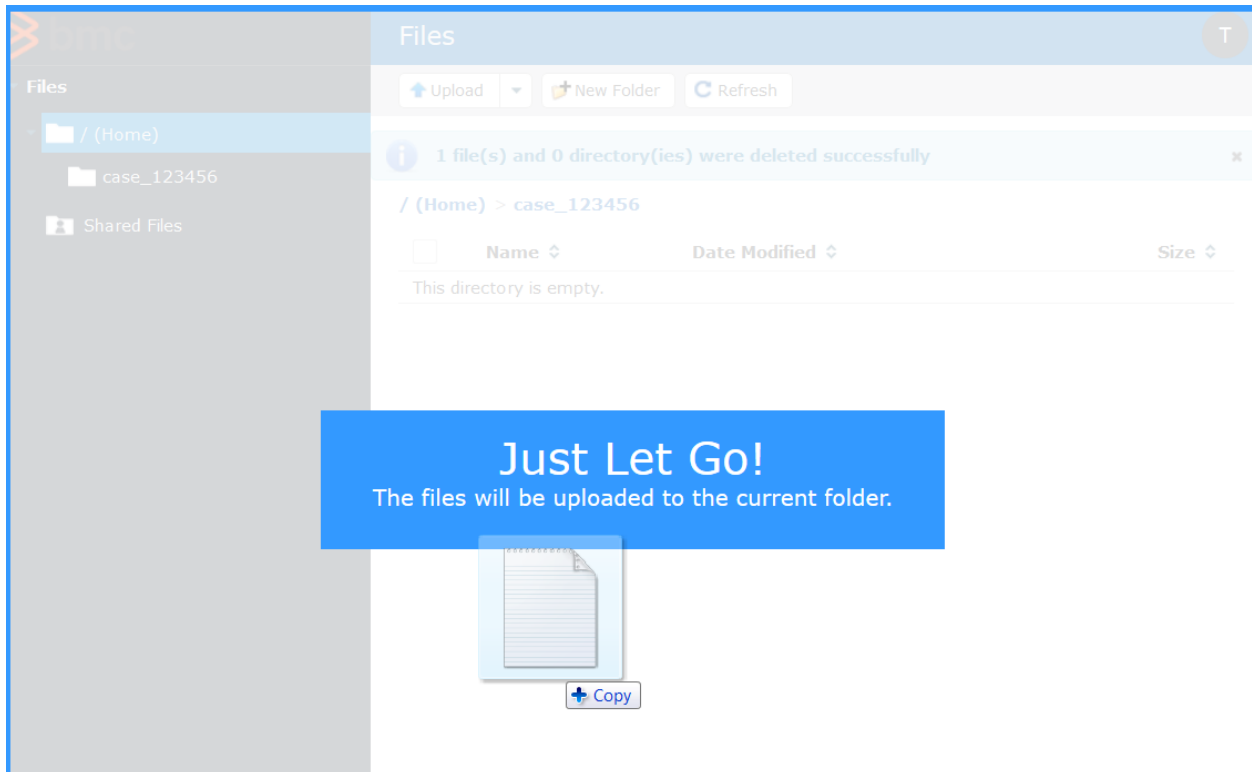
When you need to share a file for a Case, create a folder for the Case following the folder naming convention 'case\_<case number>'.



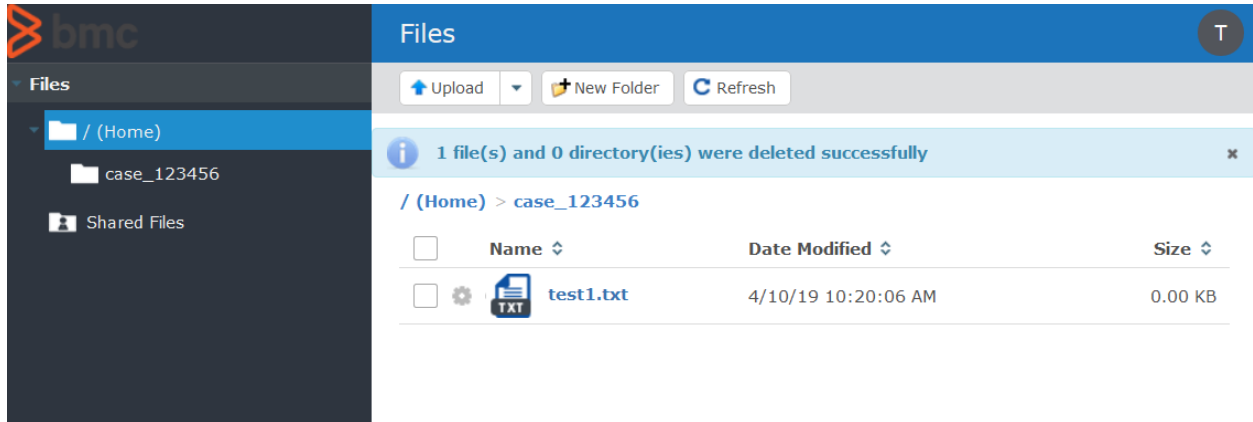
Click the folder name to open it.



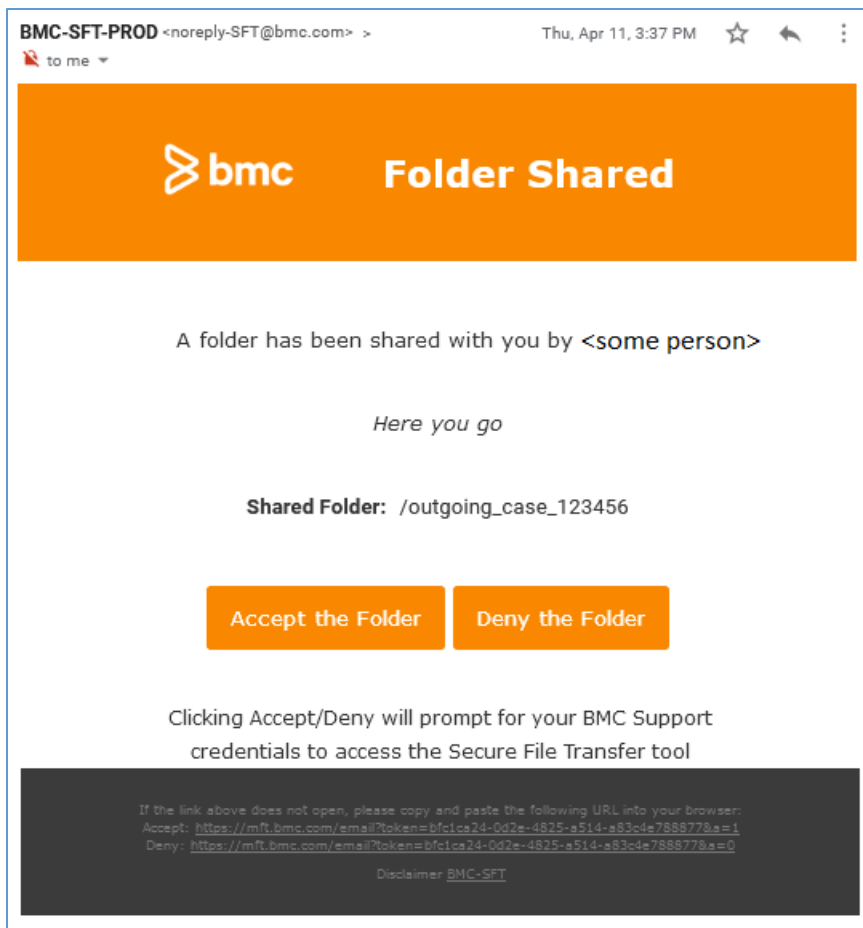
In the folder view, you can use drag and drop to upload files.



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.

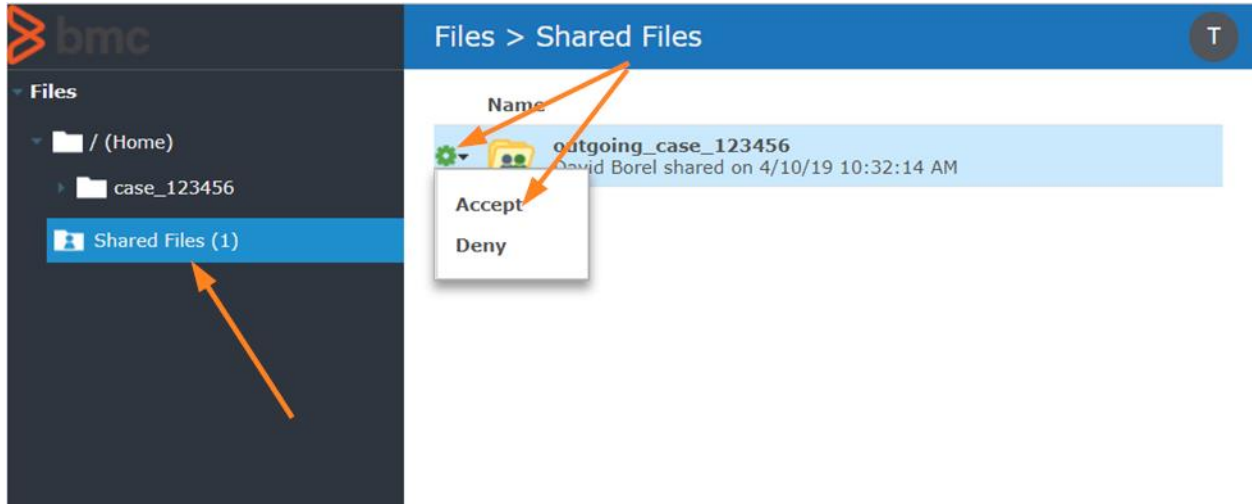


When Customer Support needs to provide a file to you, they will **share a folder with you individually**. You will get an email like this example. Unless you think you received the invitation in error, please immediately click '**Accept the Folder**' to access it.

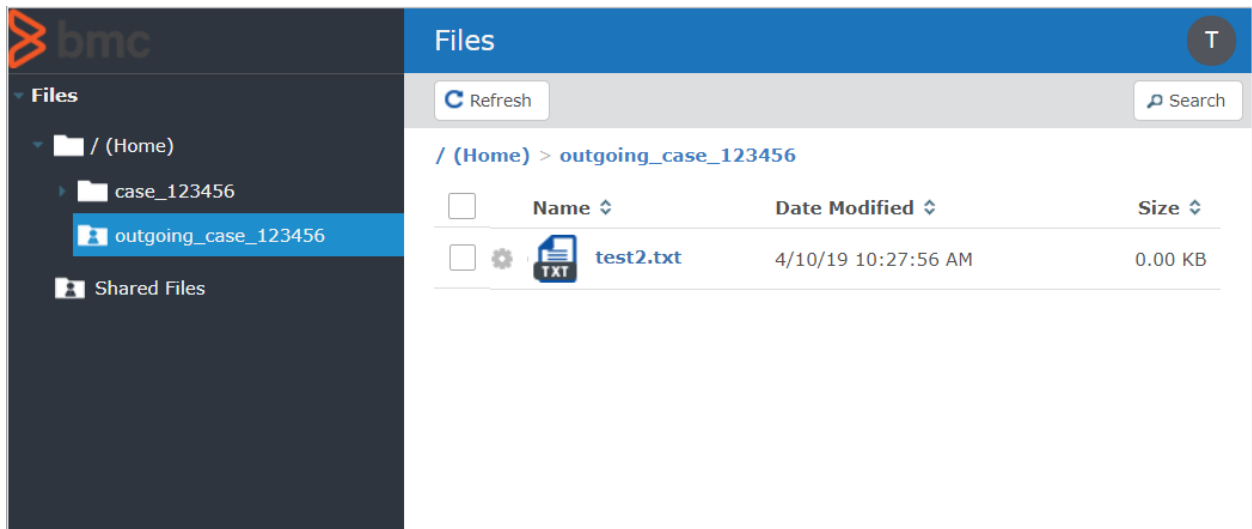




Alternatively, in the web interface, you can click to open the 'Shared Files' folder, then click 'Accept' from the gear icon by the shared folder name.



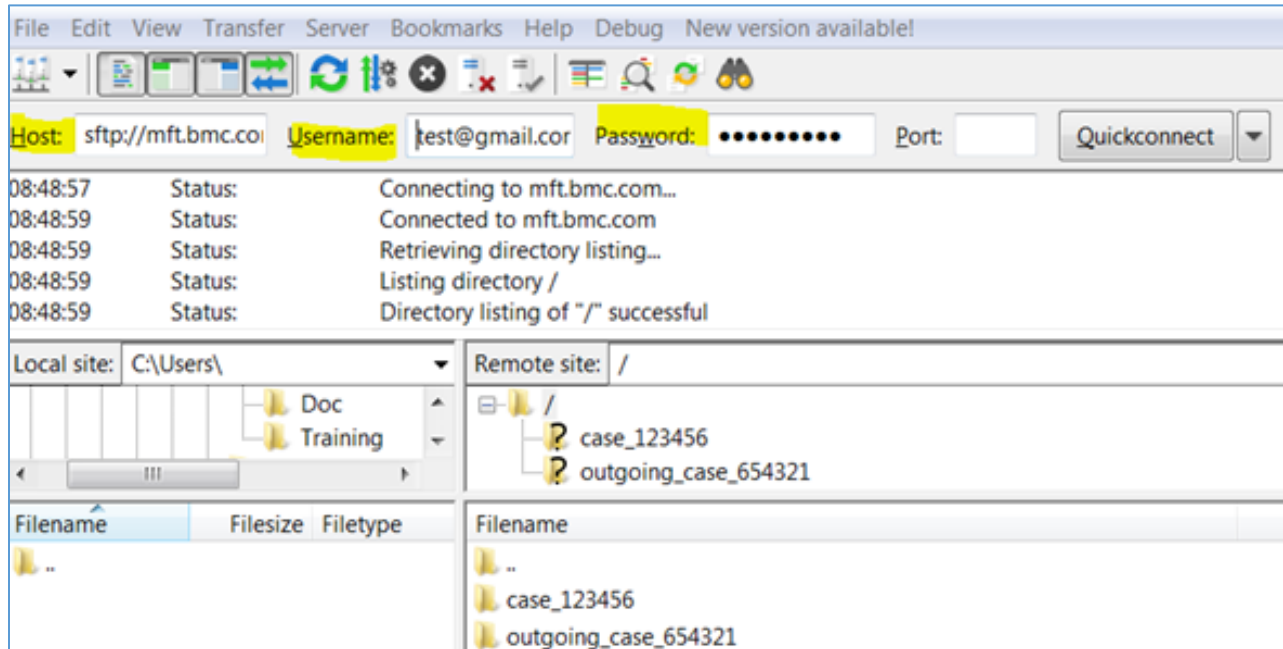
The shared folder/files will be visible in your home folder.



## 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.

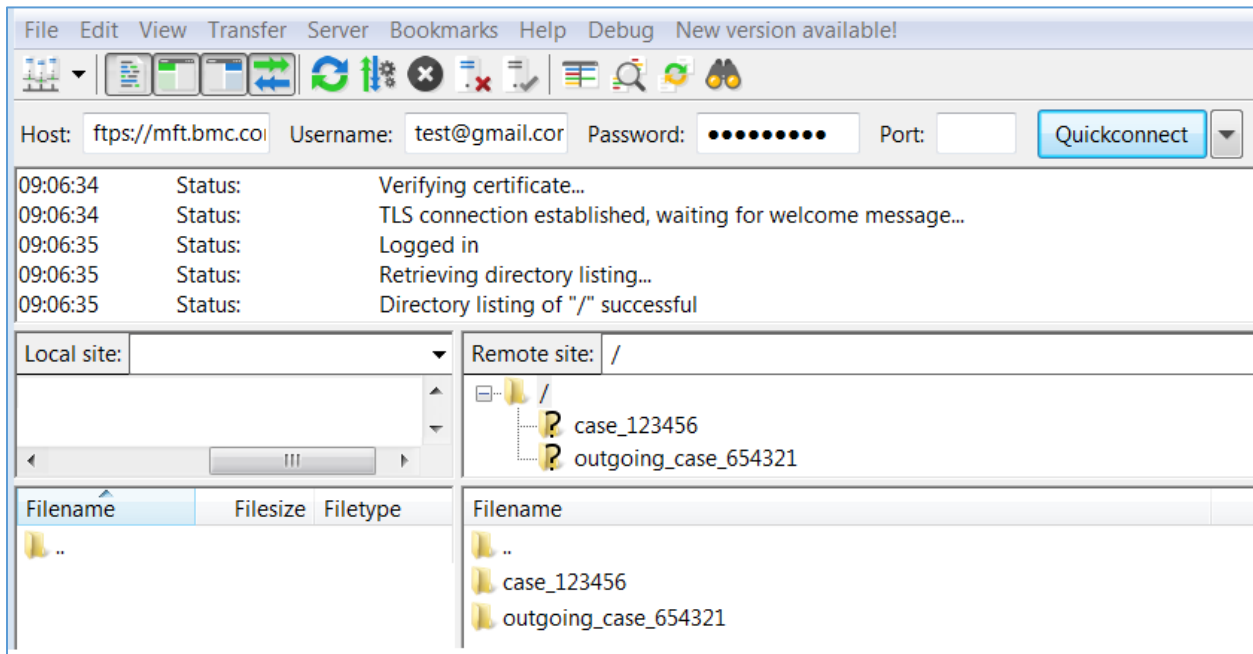
The image below is an example using Filezilla. The Host is set to 'sftp://mft.bmc.com' and a valid username and password supplied.



## 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

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 two valid security certificates. Typically, the certificates reside in a sequential, variable-blocked data set.

If the certificates are not present, you must complete the following steps before proceeding:

1. Download the three certificates (DigiCert Global Root CA, DigiCert SHA2 Secure Server CA, and BMC MFT Security certificate) 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').
3. Copy and paste the DigiCert Global Root CA 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.**
4. 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.INTER.CERT').
5. Copy and paste the DigiCert SHA2 Secure Server CA certificate into SYS1.INTER.CERT
  - a. **Include the dashed top and bottom lines. Preserve the existing case, and do not change any characters in this text.**
6. 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.BMC.CERT').
7. Copy and paste the BMC MFT Security certificate into SYS1.BMC.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 CA')
```

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

```
RACDCERT -  
  ALTER ( -  
    LABEL('DigiCert Global Root CA') -  
  ) -  
  CERTAUTH -  
  TRUST
```

4. Ensure that your IBM RACF database contains an entry for the DIGICERT SHA2 Secure Server CA.
5. If the certificate (SYS1.INTER.CERT) is not present in your RACF database, add it by entering the following command:

```
RACDCERT CERTAUTH -  
  ADD('SYS1.INTER.CERT') -  
  TRUST -  
  WITHLABEL('DigiCert SHA2 Secure Server CA')
```

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

```
RACDCERT -  
  ALTER ( -  
    LABEL('DigiCert SHA2 Secure Server CA') -  
  ) -  
  CERTAUTH -  
  TRUST
```

7. Ensure that your IBM RACF database contains an entry for the BMC Certificate.
8. If the certificate is not present in your RACF database, add it by entering the following command:

```
RACDCERT ID(userid) -  
  ADD('SYS1.BMC.CERT') -  
  TRUST -  
  WITHLABEL('mft.bmc.com')
```

9. If Status line in your certificate is not set to TRUST, change the status:

```
RACDCERT ID(userid) -  
  ALTER ( -  
    LABEL('mft.bmc.com') -  
  ) -  
  TRUST
```

10. 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)
```

b. Connect the certificate to the newly created keyring:

```
RACDCERT -  
  ID(userID) -  
  CONNECT( -  
  CERTAUTH -  
  USAGE(CERTAUTH) -  
  LABEL('DigiCert Global Root CA') -  
  RING(FTP.TLS.KEYRING) -  
  )
```

```
RACDCERT -  
  ID(userID) -  
  CONNECT( -  
  ID(userid) -  
  USAGE(SITE) -  
  LABEL('DigiCert Global Root CA') -  
  RING(FTP.TLS.KEYRING) -  
  )
```

c. Connect the certificate to the newly created keyring:

```
RACDCERT -  
  ID(userID) -  
  CONNECT( -  
  CERTAUTH -  
  USAGE(CERTAUTH) -  
  LABEL('DigiCert SHA2 Secure Server CA') -  
  RING(FTP.TLS.KEYRING) -  
  )
```

```
RACDCERT -  
  ID(userID) -  
  CONNECT( -  
  CERTAUTH -  
  USAGE(SITE) -  
  LABEL('DigiCert SHA2 Secure Server CA') -  
  RING(FTP.TLS.KEYRING) -  
  )
```

11. Refresh the RACLIST DIGTCERT and DIGTRING classes:

```
SETROPTS RACLIST(DIGTCERT DIGTRING) REFRESH
```

12. Create a SYSFTPD data set (FTPDATA) that contains the following entries:

```
KEYRING FTP.TLS.KEYRING  
SECURE_MECHANISM TLS
```

## To use CA Top-Secret to prepare your environment

1. If the security certificate is not in trusted status in your z/OS environment, upload the certificate and change the status by entering the following Top-Secret command:

```
TSS ADD(CERTAUTH) DIGICERT(cacert) DCDSN('user1.cacert') TRUST
LABLCERT('CA Certificate')
TSS ADD(ftpServer) KEYRING(srvring) RINGDATA(CERTAUTH,cacert)
USAGE(CERTAUTH)
```

2. Add the certificate to the ID:

```
TSS ADD(acID) DIGICERT(certName) -
DCDSN(dataSetName) TRUST
```

3. Add a keyring to the ID:

```
TSS ADD(acID) KEYRING(keyringName)
```

4. Add the certificate to the keyring:

```
TSS ADD(acID) KEYRING(keyringName) -
RINGDATA(acID,certificate)
```

5. (optional) List a keyring:

```
TSS LIST(ftpServer) KEYRING(srvring)
```

## To use CA-ACF2 to prepare your environment

1. If the certificate is not in trusted status in your z/OS environment, upload the certificate and change the status by entering the following CA-ACF2 command:

```
Set profile(user) div(certdata)
Insert FTPserver.suffix dsn('user1.svrcert') label(Server Certificate)
Connect certdata(FTPserver.suffix) keyring(FTPserver.ring)
usage(personal) default
```

2. Create a keyring:

```
Set profile(user) div(keyring)
```

- a. Insert userID ringname(FTPserver) Connect the certificate to the newly created keyring:

```
RACDCERT -
  ID(userID) -
  CONNECT( -
  CERTAUTH -
  USAGE(CERTAUTH) -
  LABEL('DigiCert SHA2 Secure Server CA') -
  RING(FTP.TLS.KEYRING) -
  )
```

- b. Connect the certificate to the newly created keyring:

```
RACDCERT -
  ID(userID) -
  CONNECT( -
  CERTAUTH -
  USAGE(SITE) -
  LABEL('DigiCert SHA2 Secure Server CA') -
  RING(FTP.TLS.KEYRING) -
  )
```

3. Refresh the RACLIST DIGTCERT and DIGTRING classes:

```
SETROPTS RACLIST(DIGTCERT DIGTRING) REFRESH
```

4. Create a SYSFTPDATA data set (FTPDATA) that contains the following entries:

```
KEYRING FTP.TLS.KEYRING
SECURE_MECHANISM TLS
```



## Transferring Data

**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.

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)
/*
```

```

//*   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

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:

```
//FTP EXEC PGM=FTP, PARM='(EXIT'  
//*  
//STEPLIB DD DSN=TCPIP.SEZATCP, DISP=SHR  
//SYSFTPD DD DISP=SHR, DSN=hlq.FTP.CERT.JCL(FTPDATA)  
//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_XXXXXXXXX  
cd Case_XXXXXXXXX  
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.

```
//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.

```
!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](mailto: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.)

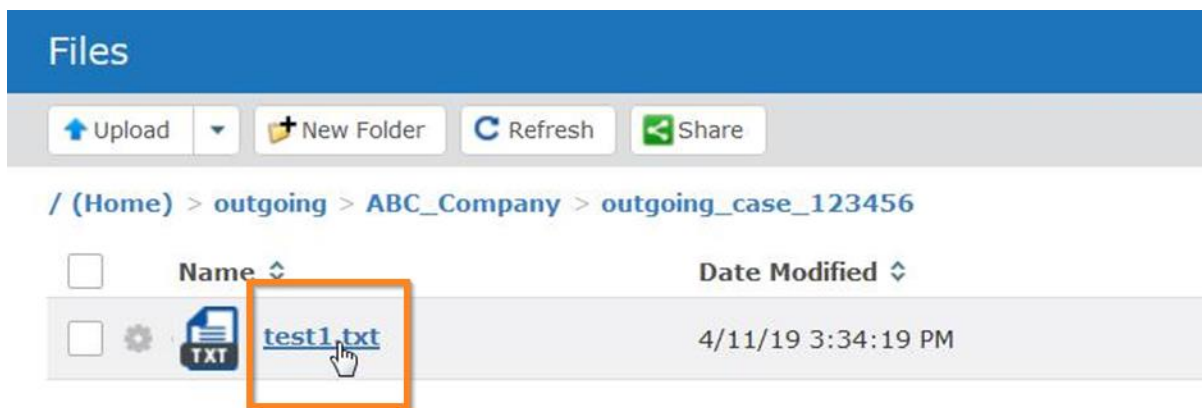
## FAQ

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.’

