
Support for Integrated SFTP Server in IBM® WebSphere® Partner Gateway

© Copyright IBM Corporation 2010. All rights reserved.



Table of contents

1.	Introduction.....	3
2.	Installing Integrated SFTP Server.....	3
3.	Uploading a Host Key for the SFTP Server.....	4
3.1	Uploading the Host Key from Load New Certificate Page	4
3.2	Uploading the Host Key from Load SFTP Keys Page	4
4.	Configuring SFTP Server Properties	4
5.	Starting and Stopping the SFTP Server	5
6.	SFTP User Management	5
7.	SFTP Reports	6
8.	SFTP Connections	6
9.	Events.....	6
10.	Known Problems and Workarounds	6

1. Introduction

WebSphere Partner Gateway 6.2 has extended support for SFTP integrated server (FTP over SSH). It is an enhancement to the existing integrated FTP server.

The supported version of SSH protocol is SSH v2 (SSH2). The SSH server implements the SFTP subsystem for file transfer, after which the SFTP client (includes WebSphere Partner Gateway receivers and destinations) can connect to the SFTP server. Before the file transfer is initiated, the authentication is done and a secure SSH channel is established between the client and the server.

The Integrated SFTP Server uses the Apache SSHD libraries. The SFTP commands implementation is as per the ietf draft of SSH File Transfer Protocol.

Note: High availability and failover is not supported in this release.

2. Installing Integrated SFTP Server

The SFTP Server is installed with the existing Integrated FTP Server and can be within the DMZ zone. It should be accessible over the internet.

The Hub administrator has to manually configure the firewall.

Using IBM® Update Installer for WebSphere Software (UPDI) 7.0.0.1 and above, update the existing integrated FTP installation with Integrated SFTP server. For installing the Integrated SFTP server, the Integrated FTP Server has to be installed as a prerequisite.

Note: The installation has start / stop scripts for SFTP Management server.

On Windows platform, the Integrated SFTP Management Server can be optionally installed as a service. This can be done using the `serviceSFTP.bat` file that is available in the `<FTP_INSTALL>/bin` folder.

To install the service, execute `serviceSFTP.bat install`.

After successful installation of Integrated SFTP Management Server service, you can start and stop this service.

To uninstall the service, execute `serviceSFTP.bat uninstall`.

3. Uploading a Host Key for the SFTP Server

The SFTP Server requires a Host key. This is the key which is presented to the clients for server authentication. The clients cannot connect to the server if the Host key is missing. You can upload the Host key for SFTP Server using either of these methods:

- Upload keystore from the Load New Certificate page
- Upload a key from the Load SFTP Keys page

3.1 Uploading the Host Key from Load New Certificate Page

In the load certificates wizard, the **Is this certificate for SFTP Server Authentication** checkbox is added to the **Provide certificate details** page.

Note: JKS, JCEKS, and PKCS12 keystores are supported.

In the edit page of certificate details page, **SFTP Server Authentication** check box is added.

For more details on loading and editing certificates, refer to *WebSphere Partner Gateway Hub configuration Guide*.

3.2 Uploading the Host Key from Load SFTP Keys Page


To load SFTP keys, perform the following steps:

1. Navigate to **Account Admin > Profile > Certificates**. In partner login, if you want to upload SFTP keys, navigate to **Account Admin > Profile > Certificates**.
2. Click **Load SFTP Keys**.
3. Click **Browse** and select the Key file from your local. This key is used for key based authentication.
4. Enter the **Password**. The password for the key to be uploaded.

Note: You can upload only PEM keys using **Load SFTP Keys** window.

4. Configuring SFTP Server Properties

To configure SFTP Server properties, perform the following tasks:

1. Navigate to **System Administration > FTP Administration > SFTP Properties**.
2. Click  to open the editable page of SFTP Server properties.
3. Enter the value for the following properties:
 - **bcg.sftp.port** – port on which SFTP Server is started
 - **max-auth-requests** - maximum SFTP Server login attempts allowed
 - **auth-timeout** – the allowed idle time while logging into SFTP Server
4. Click **Save**.

Note: Restart the Server whenever you modify the Server properties.

5. Starting and Stopping the SFTP Server

The SFTP runs within the SFTP management server. As a result, whenever the SFTP management server is started, the SFTP server also gets started automatically. The default port of SFTP management server is 2050.


To start the server on a different port, add

```
bcg.config.ftpmanagement.sftpmgmt.port=<port> to the ftpserver.init
properties file.
```

This will replace the default port value with the value you provide in <port>.

If you start the server without configuring the Host key, a warning message is displayed – “Warning: No host key defined for the server.”

To start and stop the SFTP Server from the console, perform the following tasks:

1. Navigate to **System Administration > FTP Administration > Server Start / Stop**.
2. Click  icon against SFTP Server to start it. A message confirming the successful start of SFTP Server appears.

Note: The  icon stops the SFTP server.

To start and stop the SFTP Server from command prompt, execute `./startsftpmgmtserver.sh` and `./startsftpmgmtserver.bat` for linux and Windows respectively.



6. SFTP User Management

This section describes the SFTP server features included for a user.

Note: A user can be enabled for both FTP and SFTP.

Both Password and Key based authentication methods are supported for an SFTP User. Optionally, you can upload a key and enter the password for the SFTP User.

Creating SFTP User:

1. Navigate to **Account Admin > Profile > User**.
2. Click **Create**.
3. From the list of Users, click  to view User details.
4. In the view User screen, click **FTP Configuration**.
5. The following are the new fields added for Integrated SFTP Server:
 - **SFTP user Enabled** – if the SFTP server is in disabled state, click *Enabled*.
 - **Key (SFTP only)** – click **Browse** to upload a public key. The uploaded file is used for key based authentication. The  icon indicates that a Key is already uploaded.
 - **Password (SFTP only)** – the password for the key to be uploaded.
Note: As part of JR37932 fix, this field has been removed from WebSphere Partner Gateway 6.2 Fixpack 5 onwards.

7. SFTP Reports

To view SFTP Server statistics:


1. Navigate to **Tools > FTP Reports > Statistics**.
2. In **Server Type**, select **SFTP Server**. The server details are displayed in read-only mode.

The fields of SFTP Server are same as that of FTP server. Refer to *FTP Statistics* section of *WebSphere Partner Gateway Administrators guide*.

8. SFTP Connections

The Integrated SFTP Server will have a connection report similar to FTP Server. The connections page has options to disconnect an existing connection. The connections report will be shown in the existing FTP Connections report.

To view SFTP connections:

1. Navigate to **Tools > FTP Reports > Connections**.
2. In the connections list page, select *SFTP Server* in the **Server Type**. A list of all SFTP Server connections is displayed.
3. Click  icon against the appropriate SFTP Server to disconnect it.

9. Events

In the Events code page of the console, the range of SFTP events is from BCG620001 to BCG620008.

10. Known Problems and Workarounds

The following are the known problems and their workarounds:

- Document delivery to a SFTP Destination created on WPG 6.2 FP4a that is connected to a running Integrated SFTP Server fails with the following error: "Caused by: com.ibm.j2ca.ftp.exception.FTPOperationException: 2: No such file: <directory location>". The workaround is to have a dummy folder in the output directory of the SFTP Destination.

Note: This problem is resolved in WebSphere Partner Gateway v6.2 Fixpack 5 using APAR JR36766.

- When you replace a PEM with a JKS for SFTP Server Authentication and restart the SFTP server, an error may be logged in the SFTP log. The workaround for this is to restart the SFTP Server again.