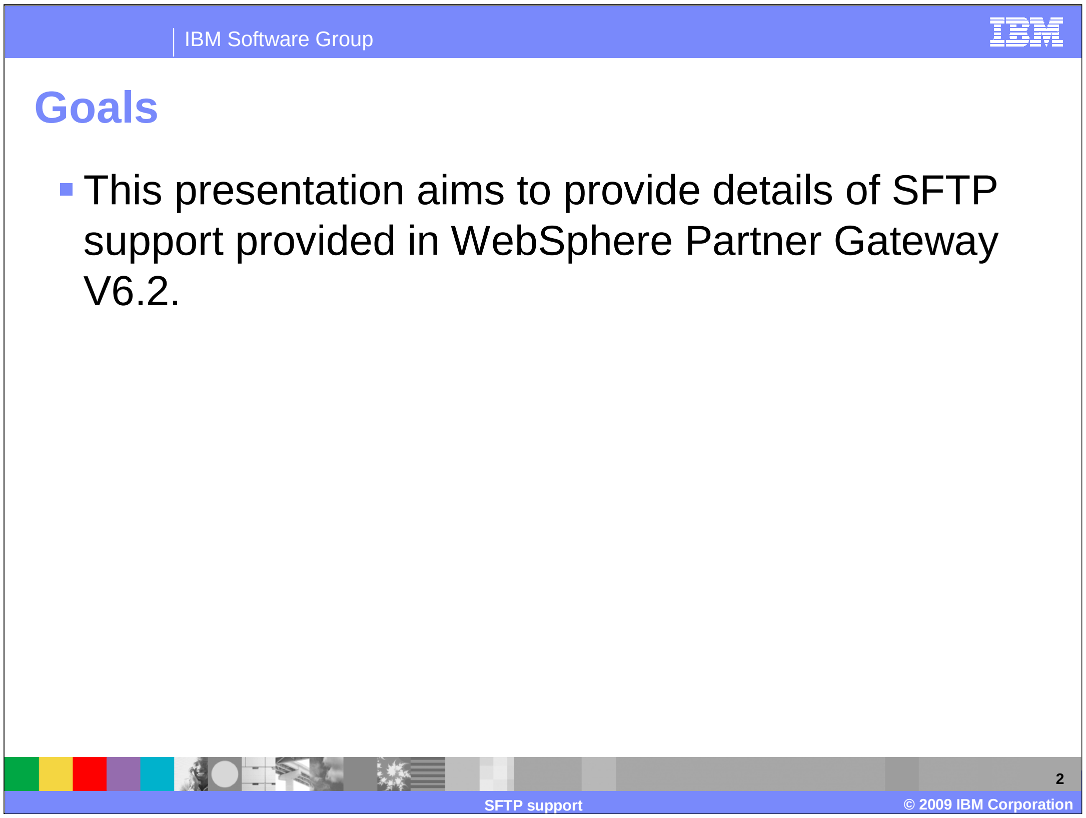
IBM Software Group

IBM WebSphere Partner Gateway V6.2

SFTP support

Updated January 30, 2009

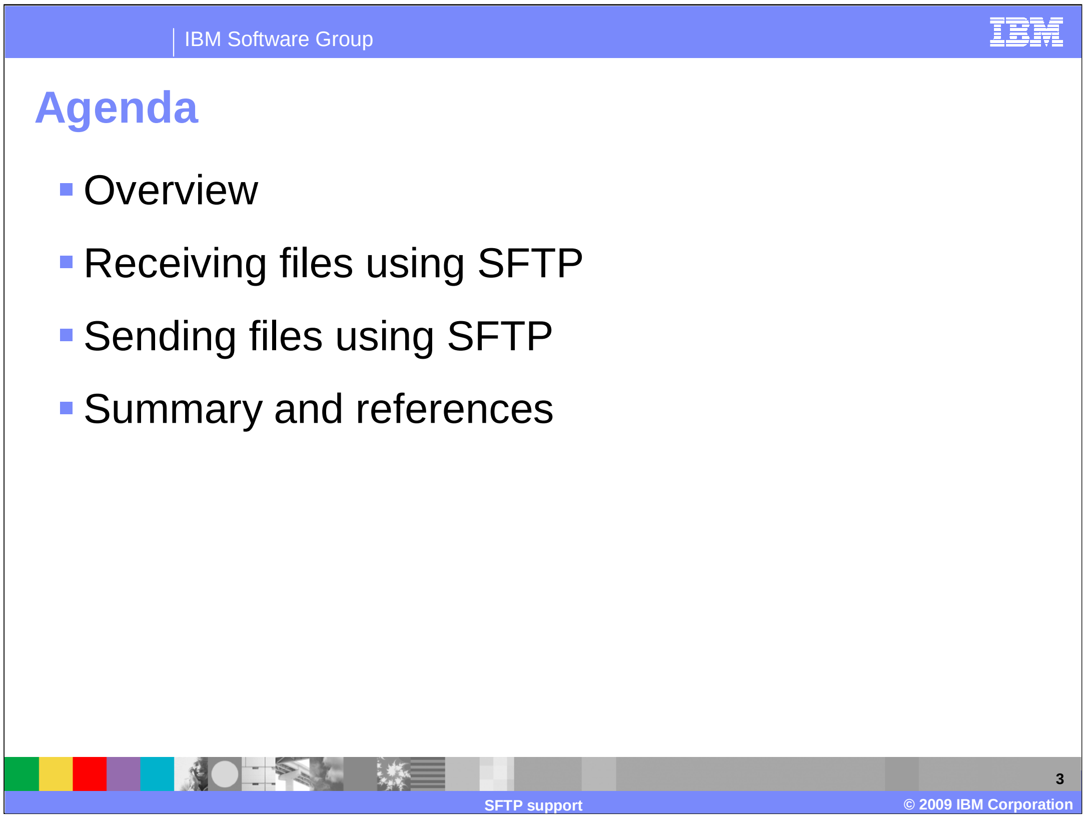
WebSphere® Partner Gateway 6.2 provides SFTP functionality for receiving and sending documents. This presentation is about SFTP support in WebSphere Partner Gateway 6.2.



Goals

- This presentation aims to provide details of SFTP support provided in WebSphere Partner Gateway V6.2.

The goal of this presentation is to provide the details of using SFTP in WebSphere Partner Gateway V6.2.



Agenda

- Overview
- Receiving files using SFTP
- Sending files using SFTP
- Summary and references

This presentation will cover the overall SFTP functionality provided in WebSphere Partner Gateway. It also includes the security aspects. It will then cover the details of configuration steps that must be carried out for receiving and sending files using SFTP. It will end with a summary of topics covered and references.

IBM Software Group

Section

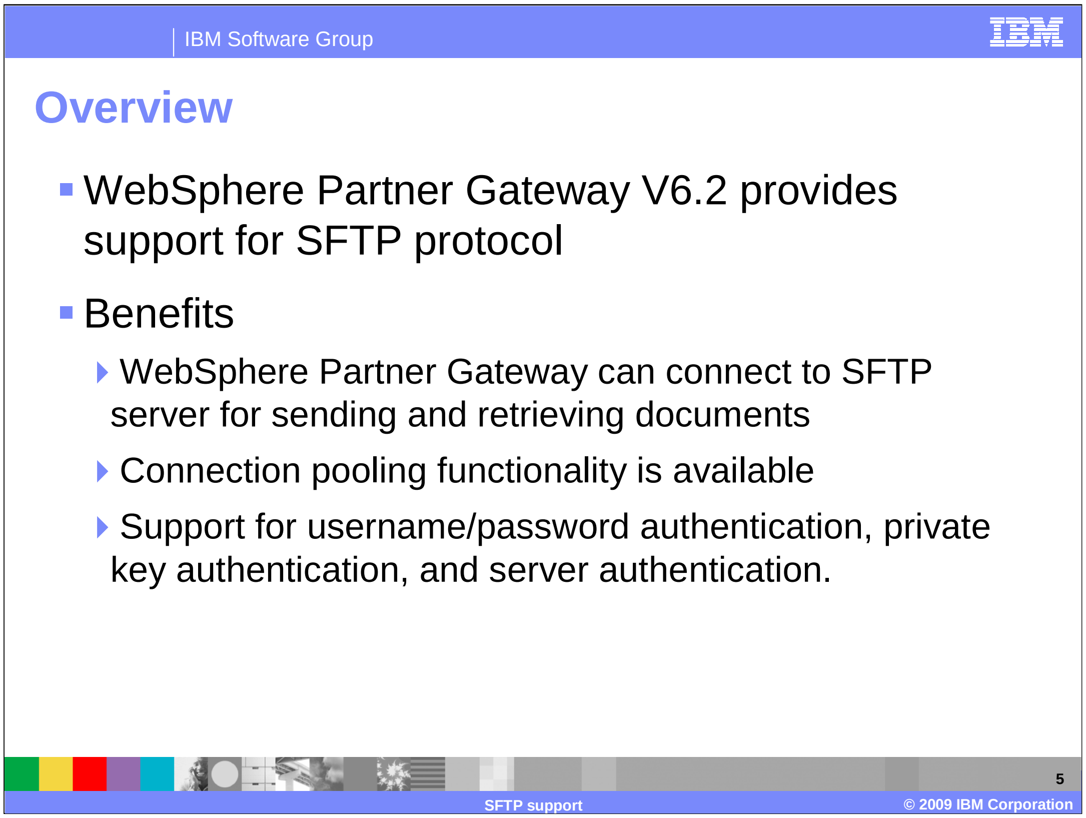
Overview

4

SFTP support

© 2009 IBM Corporation

This section will provide a overview of SFTP support in WebSphere Partner Gateway.



IBM Software Group

Overview

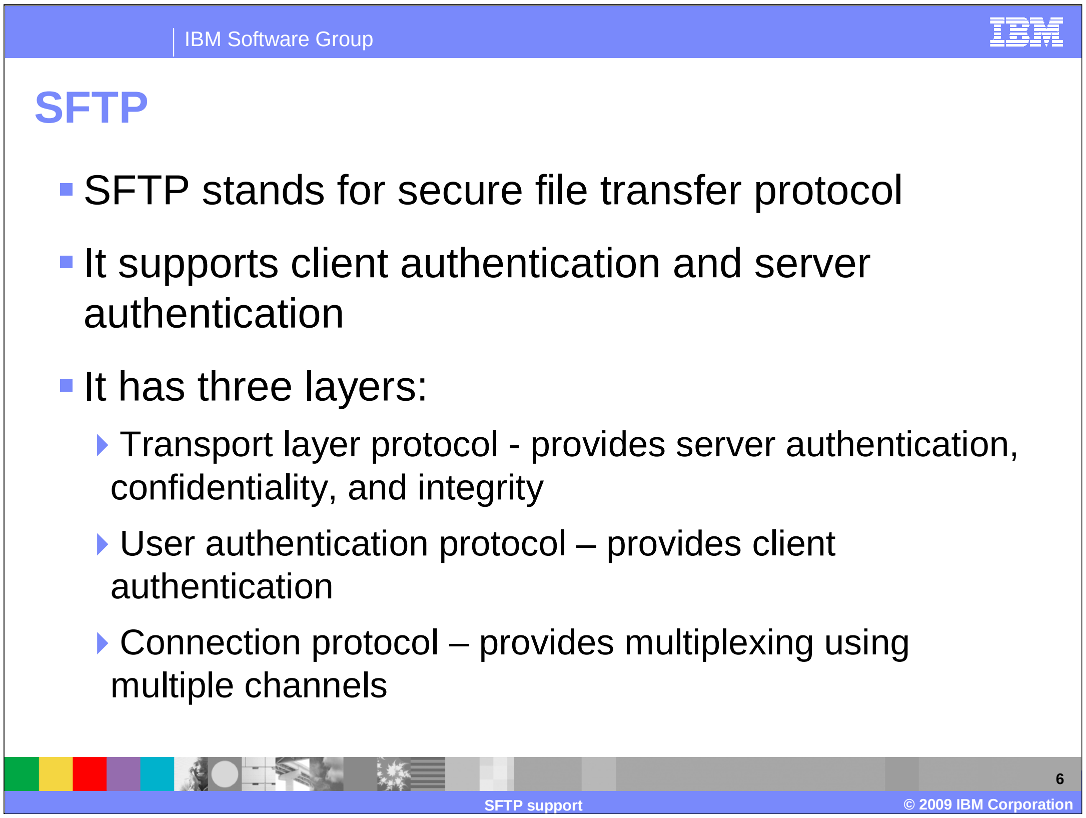
- WebSphere Partner Gateway V6.2 provides support for SFTP protocol
- Benefits
  - WebSphere Partner Gateway can connect to SFTP server for sending and retrieving documents
  - Connection pooling functionality is available
  - Support for username/password authentication, private key authentication, and server authentication.

5

SFTP support

© 2009 IBM Corporation

SFTP stands for Secure File Transfer Protocol. It is different from FTP (File Transfer Protocol). It provides the functionality of message integrity, confidentiality, and authentication. It also provides multiplexing of documents using different channels. In WebSphere Partner Gateway, there is an additional benefit of connection pooling, as the SFTP functionality is provided using J2C resource adapter.



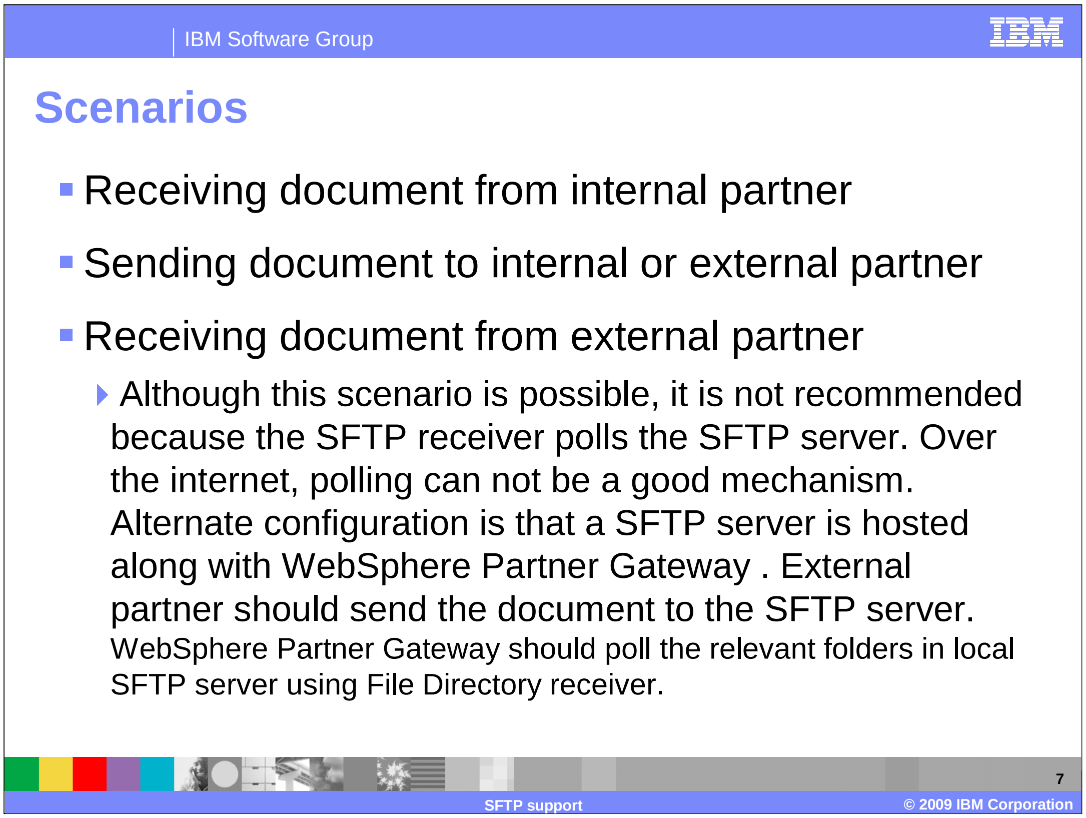
SFTP

- SFTP stands for secure file transfer protocol
- It supports client authentication and server authentication
- It has three layers:
  - Transport layer protocol - provides server authentication, confidentiality, and integrity
  - User authentication protocol – provides client authentication
  - Connection protocol – provides multiplexing using multiple channels

Both client and server authentication can be used. Client authentication can be based on username and password, or private key and passphrase. SFTP protocol consists of three layers - transport layer protocol, user authentication protocol, and connection protocol. Transport layer protocol provides server authentication, confidentiality, and message integrity. In server authentication, client authenticates the server to verify that it is connecting to the correct server. The documents exchanged between client and server should be confidential and should be protected from any eavesdropping. This is achieved using encryption. Message integrity means that the message or document reaches the destination without modification, that is, the document that is sent and received are the same and is not tampered. This is achieved using message digests.

User authentication protocol provides client authentication.

Connection protocol provides the multiplexing of documents using different channels.



IBM Software Group

Scenarios

- Receiving document from internal partner
- Sending document to internal or external partner
- Receiving document from external partner
  - Although this scenario is possible, it is not recommended because the SFTP receiver polls the SFTP server. Over the internet, polling can not be a good mechanism. Alternate configuration is that a SFTP server is hosted along with WebSphere Partner Gateway . External partner should send the document to the SFTP server. WebSphere Partner Gateway should poll the relevant folders in local SFTP server using File Directory receiver.

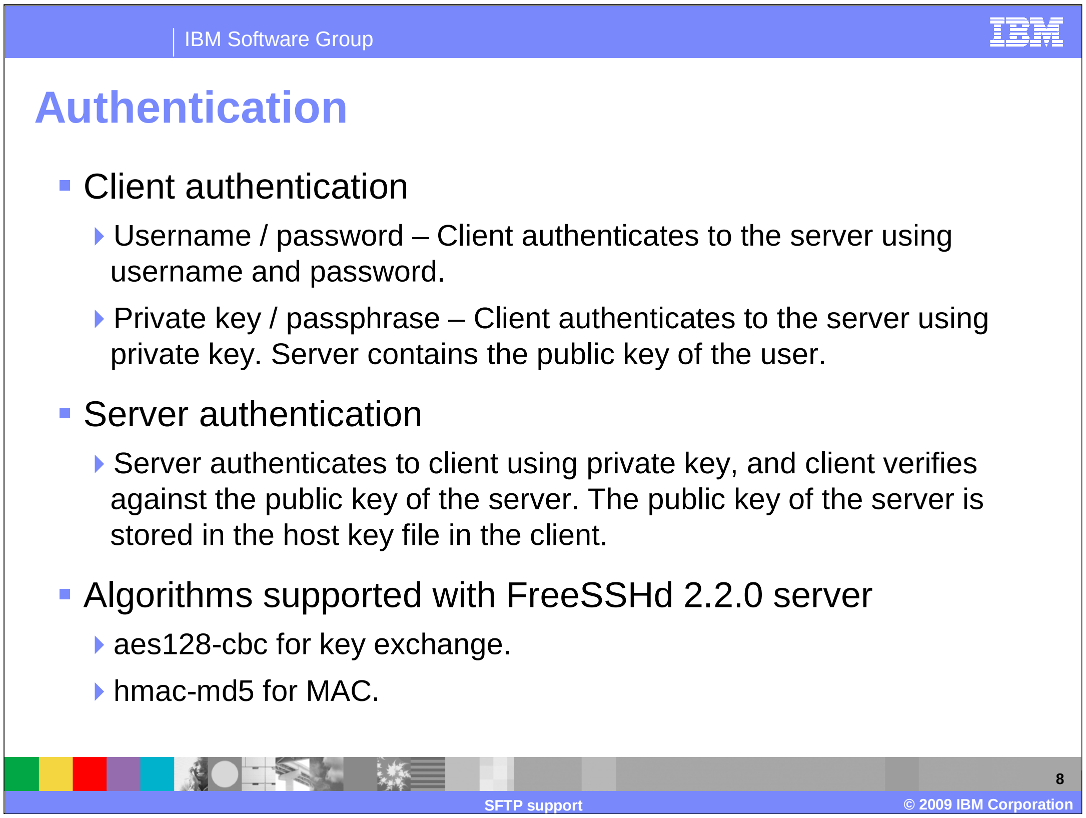
7

SFTP support

© 2009 IBM Corporation

This slide mentions the scenarios in which SFTP protocol can be used in WebSphere Partner Gateway. An internal partner is a trading partner that either hosts the hub, or is a central trading partner in the trading community, and does business with other trading partners in the trading community. Hence, an internal trading partner can be within the enterprise hosting the hub.

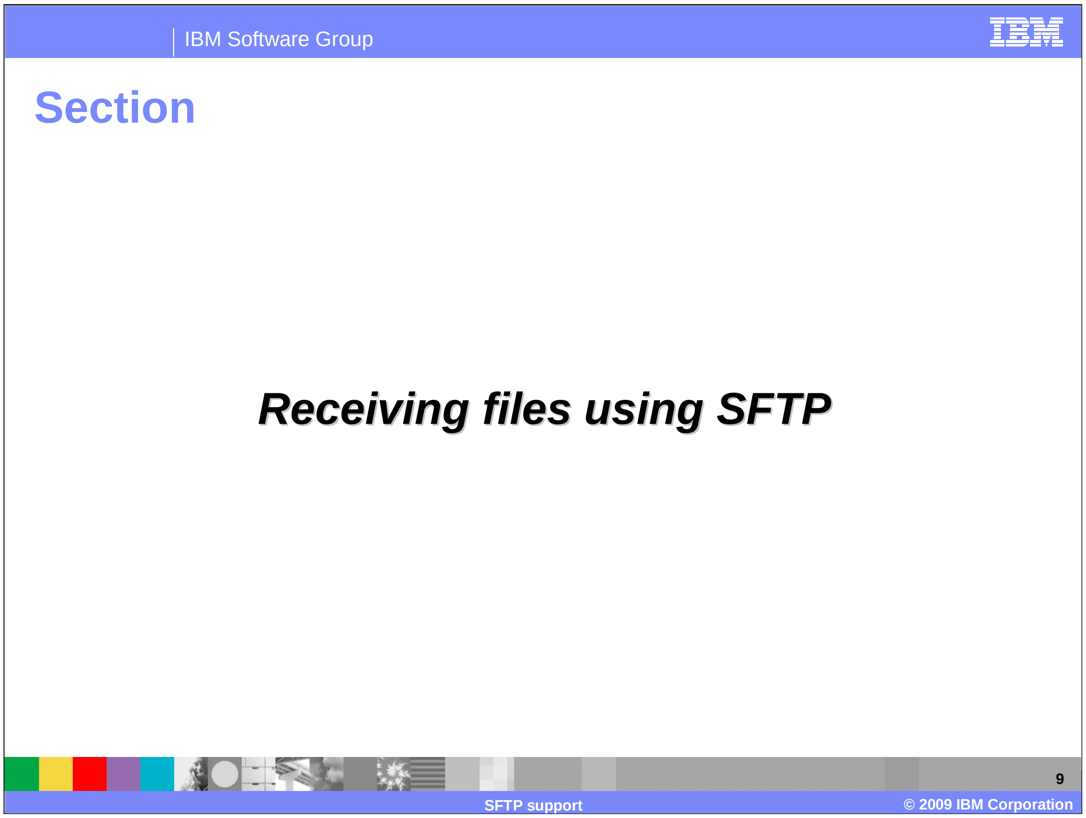
An external trading partner is a trading partner doing business with an internal trading partner.



Authentication

- Client authentication
  - Username / password – Client authenticates to the server using username and password.
  - Private key / passphrase – Client authenticates to the server using private key. Server contains the public key of the user.
- Server authentication
  - Server authenticates to client using private key, and client verifies against the public key of the server. The public key of the server is stored in the host key file in the client.
- Algorithms supported with FreeSSHd 2.2.0 server
  - aes128-cbc for key exchange.
  - hmac-md5 for MAC.

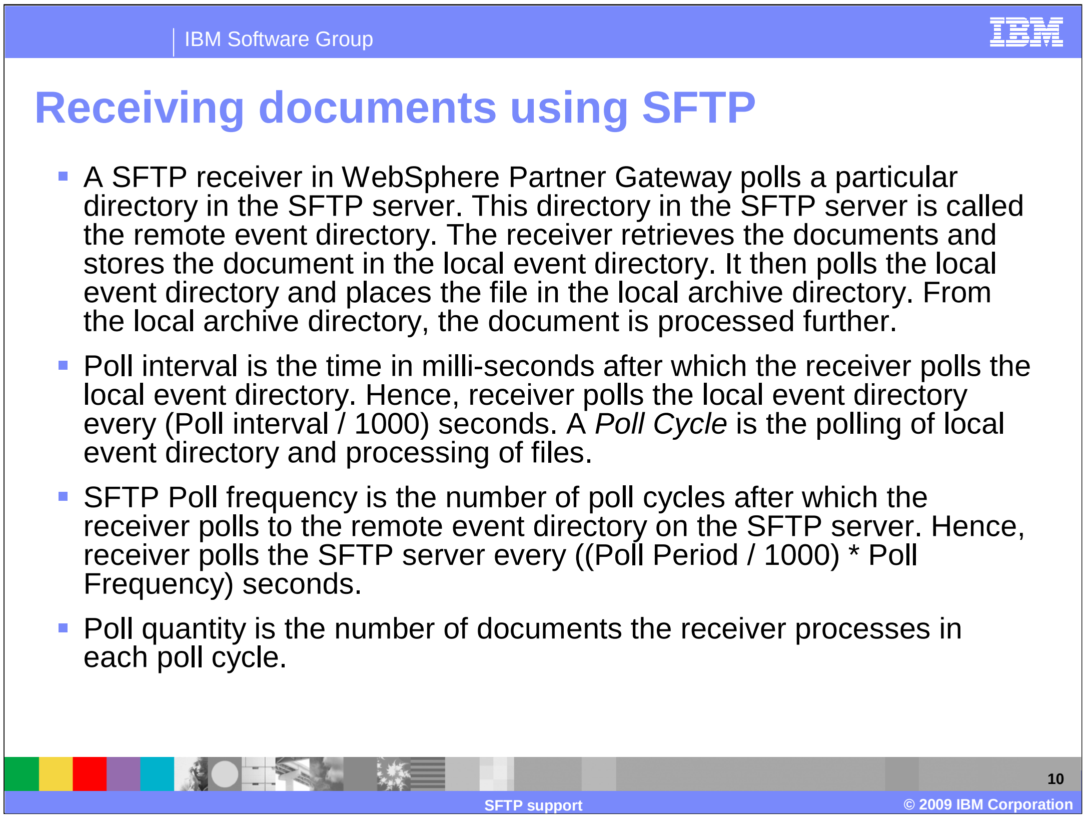
If server authentication is disabled, the client will trust any server and will connect to it if other connection parameters are correct. It is recommended to always enable server authentication.



Section

Receiving files using SFTP

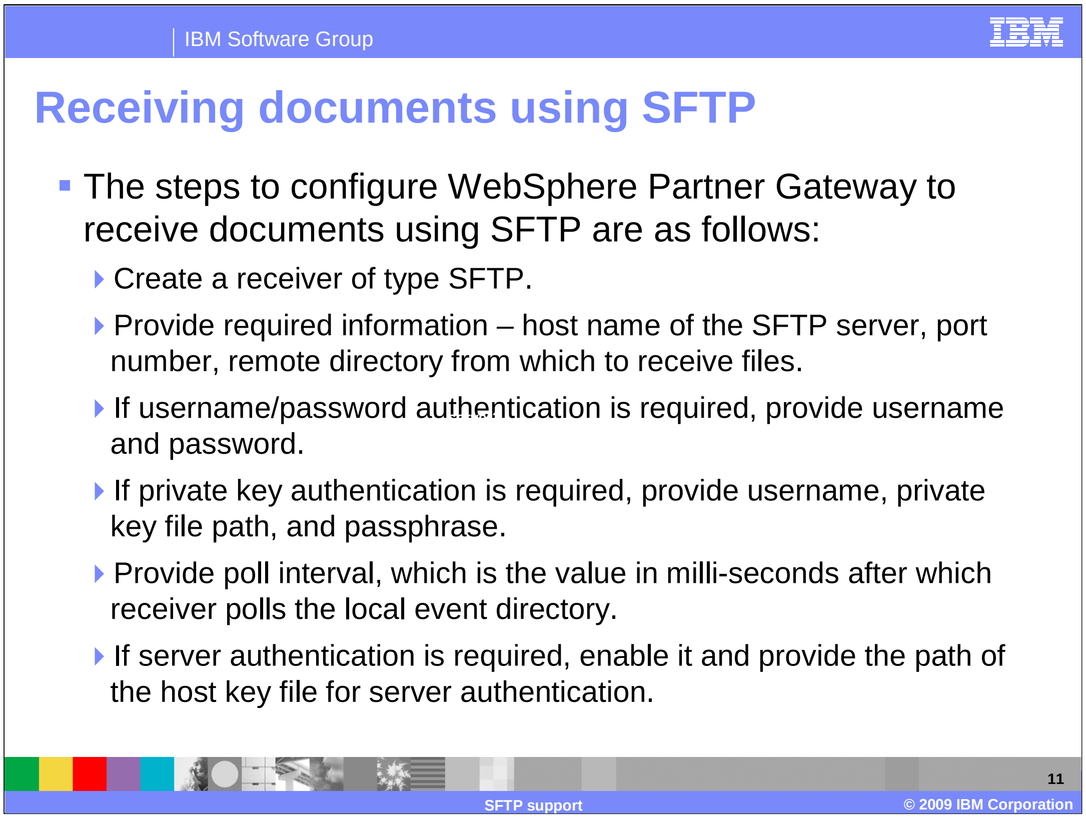
This section will provide details of configuration for receiving files using SFTP.



Receiving documents using SFTP

- A SFTP receiver in WebSphere Partner Gateway polls a particular directory in the SFTP server. This directory in the SFTP server is called the remote event directory. The receiver retrieves the documents and stores the document in the local event directory. It then polls the local event directory and places the file in the local archive directory. From the local archive directory, the document is processed further.
- Poll interval is the time in milli-seconds after which the receiver polls the local event directory. Hence, receiver polls the local event directory every (Poll interval / 1000) seconds. A *Poll Cycle* is the polling of local event directory and processing of files.
- SFTP Poll frequency is the number of poll cycles after which the receiver polls to the remote event directory on the SFTP server. Hence, receiver polls the SFTP server every ((Poll Period / 1000) * Poll Frequency) seconds.
- Poll quantity is the number of documents the receiver processes in each poll cycle.

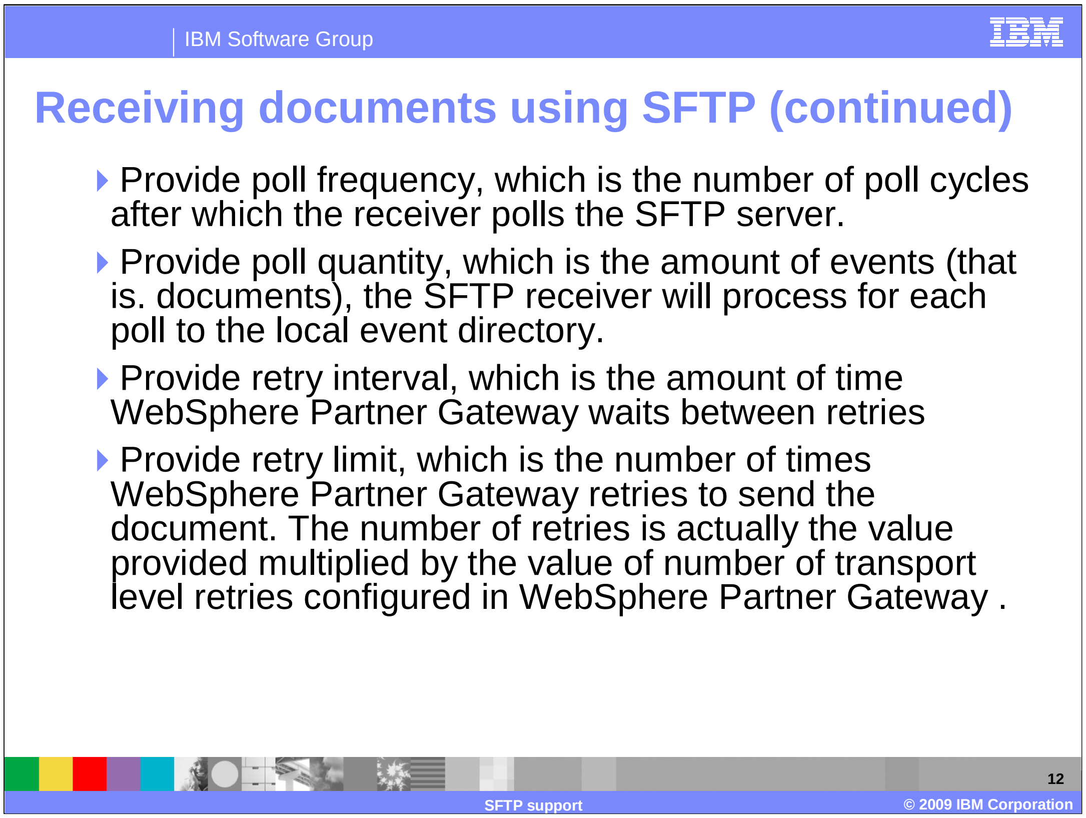
This slide explains how SFTP adapter works and other concepts like poll interval, poll frequency, poll cycle, and poll quantity.



Receiving documents using SFTP

- The steps to configure WebSphere Partner Gateway to receive documents using SFTP are as follows:
  - Create a receiver of type SFTP.
  - Provide required information – host name of the SFTP server, port number, remote directory from which to receive files.
  - If username/password authentication is required, provide username and password.
  - If private key authentication is required, provide username, private key file path, and passphrase.
  - Provide poll interval, which is the value in milli-seconds after which receiver polls the local event directory.
  - If server authentication is required, enable it and provide the path of the host key file for server authentication.

This slide explains the steps to configure an SFTP receiver.

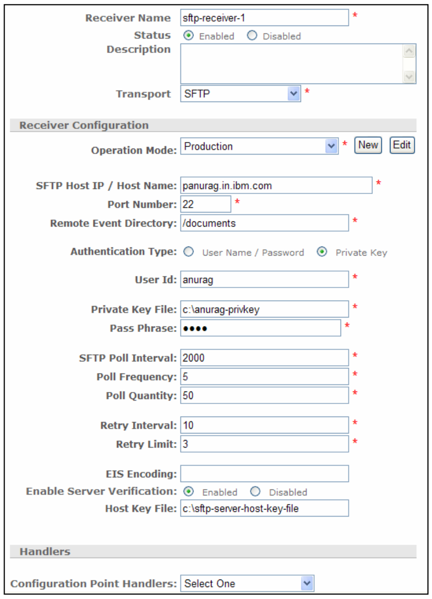


Receiving documents using SFTP (continued)

- Provide poll frequency, which is the number of poll cycles after which the receiver polls the SFTP server.
- Provide poll quantity, which is the amount of events (that is. documents), the SFTP receiver will process for each poll to the local event directory.
- Provide retry interval, which is the amount of time WebSphere Partner Gateway waits between retries
- Provide retry limit, which is the number of times WebSphere Partner Gateway retries to send the document. The number of retries is actually the value provided multiplied by the value of number of transport level retries configured in WebSphere Partner Gateway .

IBM Software Group

Receiving documents using SFTP



Receiver Name: sftp-receiver-1 *

Status: ● Enabled ○ Disabled

Description:

Transport: SFTP *

Receiver Configuration

Operation Mode: Production * New Edit

SFTP Host IP / Host Name: panurag.in.ibm.com *

Port Number: 22 *

Remote Event Directory: /documents *

Authentication Type: ○ User Name / Password ● Private Key

User Id: anurag *

Private Key File: c:\anurag-privkey *

Pass Phrase: •••• *

SFTP Poll Interval: 2000 *

Poll Frequency: 5 *

Poll Quantity: 50 *

Retry Interval: 10 *

Retry Limit: 3 *

EIS Encoding:

Enable Server Verification: ● Enabled ○ Disabled

Host Key File: c:\sftp-server-host-key-file

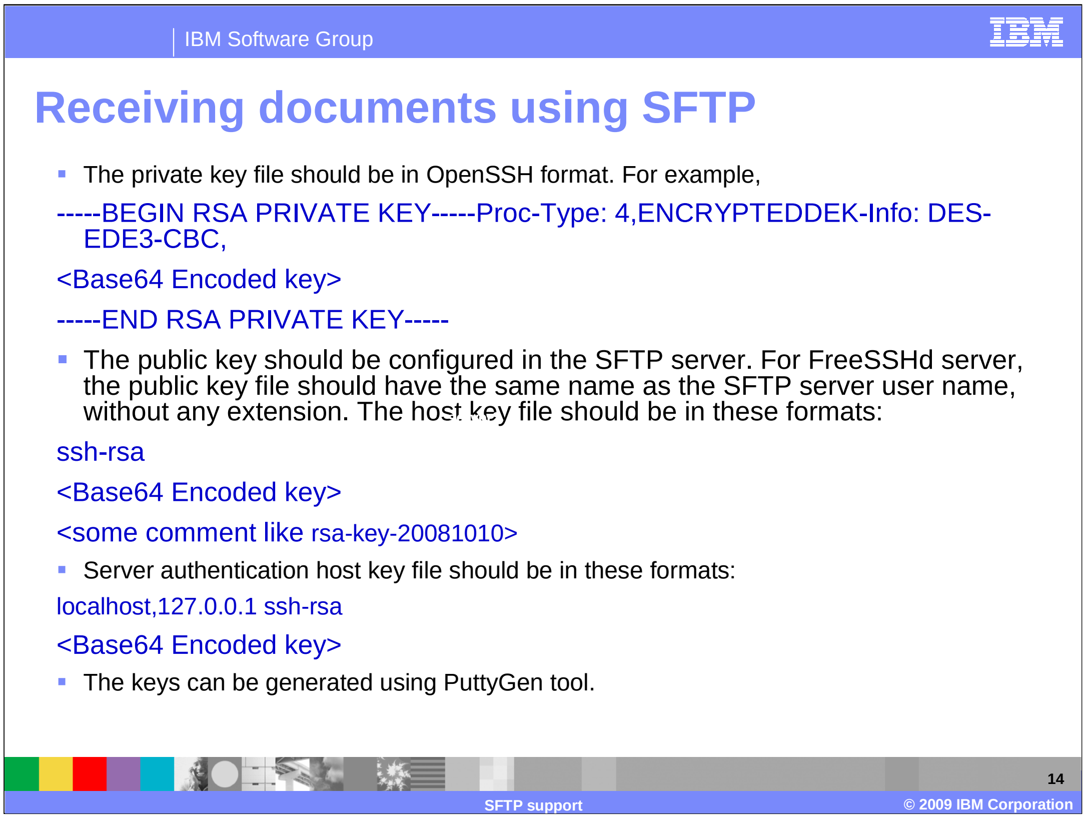
Handlers

Configuration Point Handlers: Select One

13

SFTP support

This slide shows a screen capture of an SFTP receiver in edit mode.



Receiving documents using SFTP

- The private key file should be in OpenSSH format. For example,

-----BEGIN RSA PRIVATE KEY-----Proc-Type: 4,ENCRYPTEDDEK-Info: DES-EDE3-CBC,

<Base64 Encoded key>

-----END RSA PRIVATE KEY-----

- The public key should be configured in the SFTP server. For FreeSSHd server, the public key file should have the same name as the SFTP server user name, without any extension. The host key file should be in these formats:

ssh-rsa

<Base64 Encoded key>

<some comment like rsa-key-20081010>

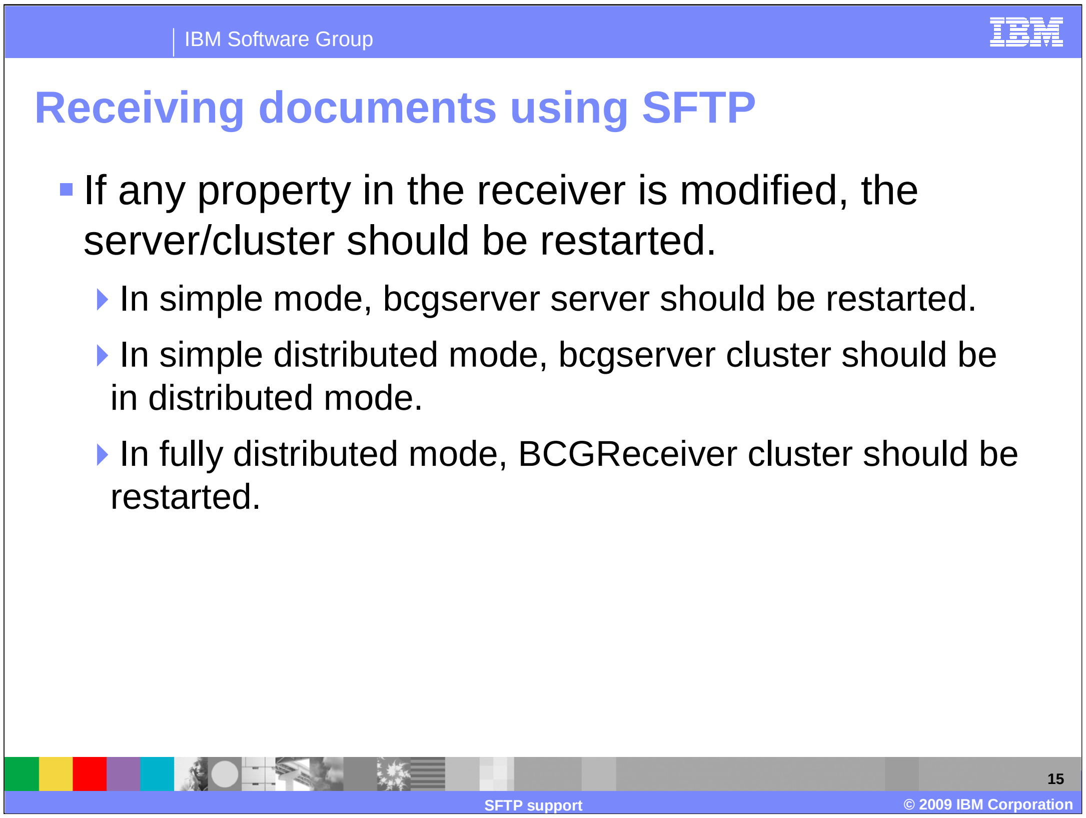
- Server authentication host key file should be in these formats:

localhost,127.0.0.1 ssh-rsa

<Base64 Encoded key>

- The keys can be generated using PuttyGen tool.

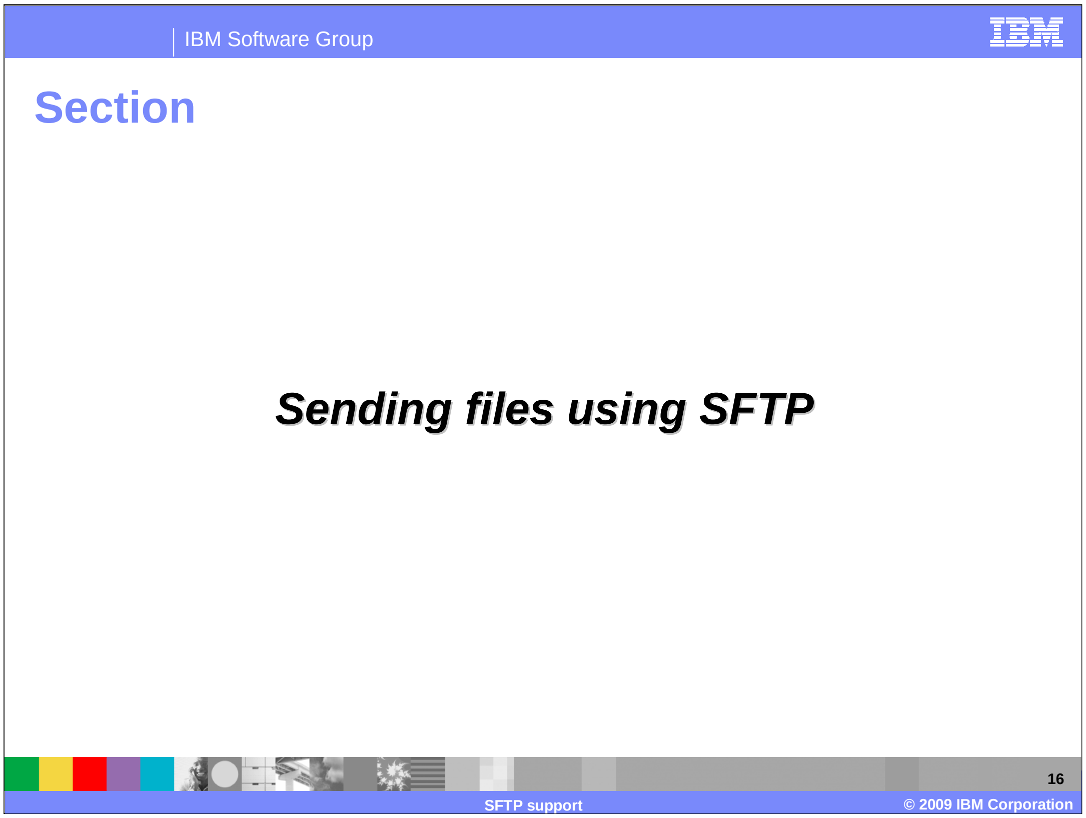
This slide describes the details of the formats supported for private key, public key, and host key file. The OpenSSH format is supported by the PuttyGen tool.



Receiving documents using SFTP

- If any property in the receiver is modified, the server/cluster should be restarted.
  - In simple mode, bcgserver server should be restarted.
  - In simple distributed mode, bcgserver cluster should be in distributed mode.
  - In fully distributed mode, BCGReceiver cluster should be restarted.

This slide mentions an important point regarding editing of properties of SFTP receiver.



IBM Software Group

IBM

Section

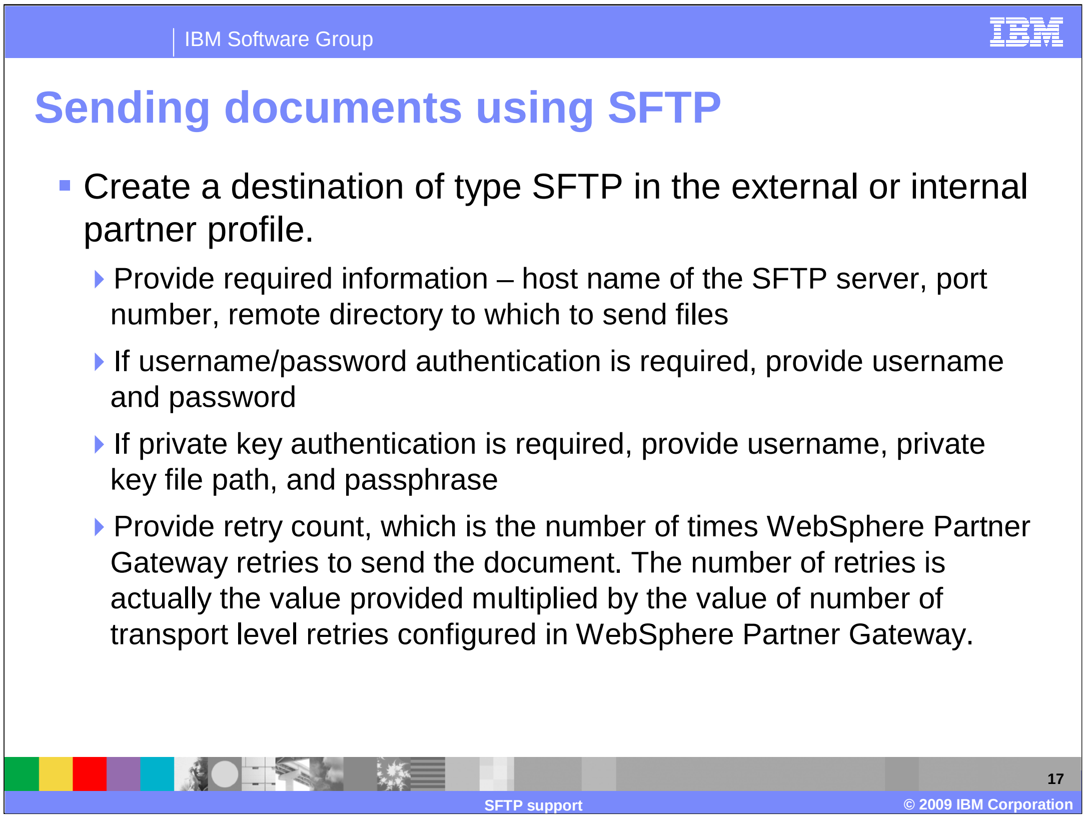
Sending files using SFTP

16

SFTP support

© 2009 IBM Corporation

This section will provide details of configuration for sending files using SFTP.



IBM Software Group

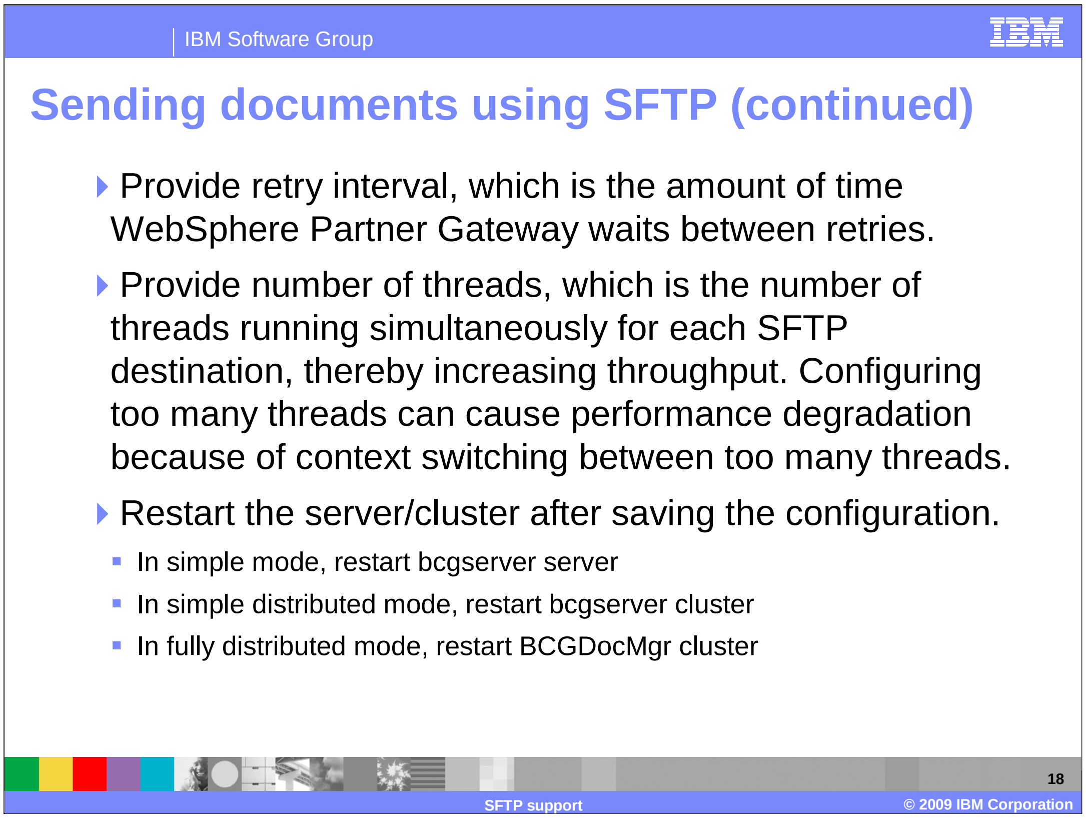
Sending documents using SFTP

- Create a destination of type SFTP in the external or internal partner profile.
  - Provide required information – host name of the SFTP server, port number, remote directory to which to send files
  - If username/password authentication is required, provide username and password
  - If private key authentication is required, provide username, private key file path, and passphrase
  - Provide retry count, which is the number of times WebSphere Partner Gateway retries to send the document. The number of retries is actually the value provided multiplied by the value of number of transport level retries configured in WebSphere Partner Gateway.

17

SFTP support

This slide explains the configuration required for configuring a destination for SFTP to send documents using SFTP.

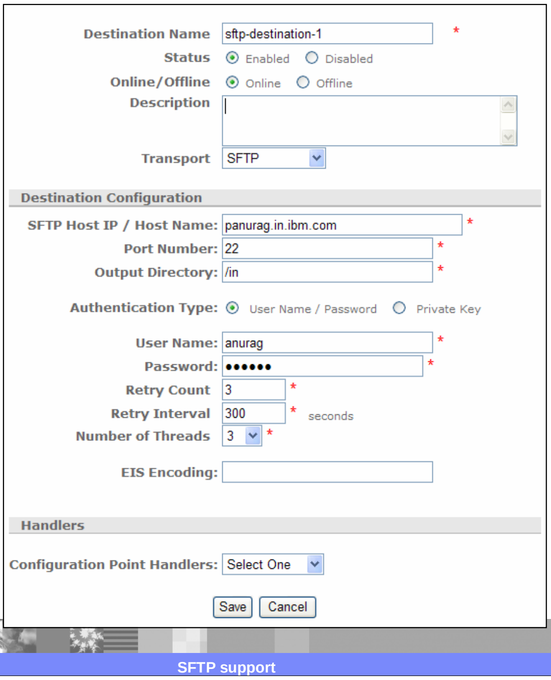


Sending documents using SFTP (continued)

- Provide retry interval, which is the amount of time WebSphere Partner Gateway waits between retries.
- Provide number of threads, which is the number of threads running simultaneously for each SFTP destination, thereby increasing throughput. Configuring too many threads can cause performance degradation because of context switching between too many threads.
- Restart the server/cluster after saving the configuration.
  - In simple mode, restart bcgserver server
  - In simple distributed mode, restart bcgserver cluster
  - In fully distributed mode, restart BCGDocMgr cluster

IBM Software Group

Sending files using SFTP



Destination Name	sftp-destination-1 *
Status	● Enabled ○ Disabled
Online/Offline	● Online ○ Offline
Description	
Transport	SFTP

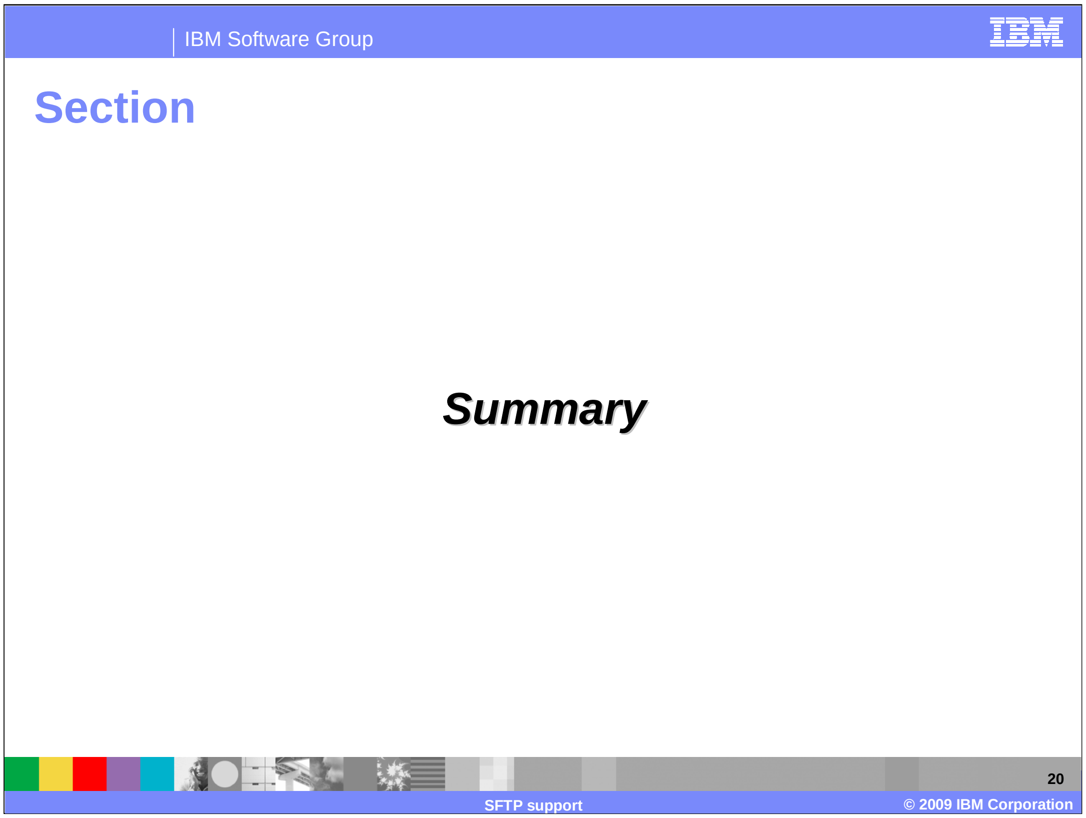
Destination Configuration

SFTP Host IP / Host Name:	panurag.in.ibm.com *
Port Number:	22 *
Output Directory:	/in *
Authentication Type:	● User Name / Password ○ Private Key
User Name:	anurag *
Password:	•••••• *
Retry Count	3 *
Retry Interval	300 * seconds
Number of Threads	3 *
EIS Encoding:	

Handlers

Configuration Point Handlers:	Select One

This slide shows a screen capture of an SFTP destination in edit mode.



IBM Software Group

Section

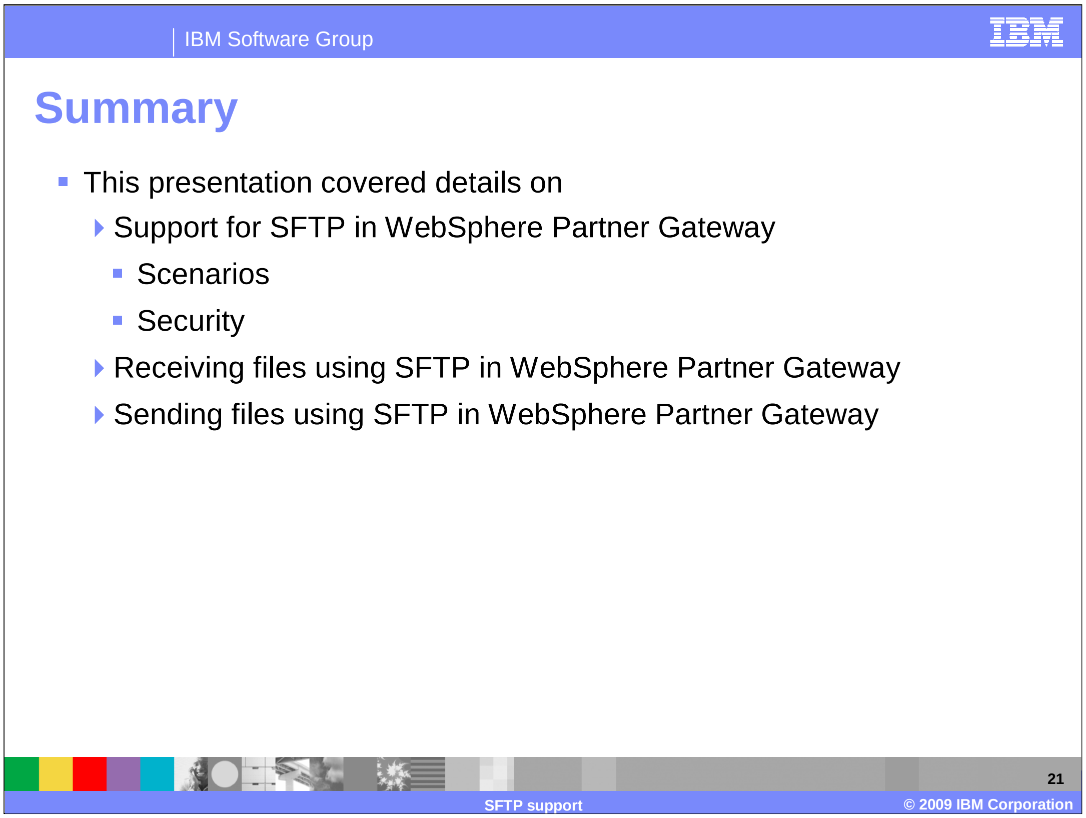
Summary

20

SFTP support

© 2009 IBM Corporation

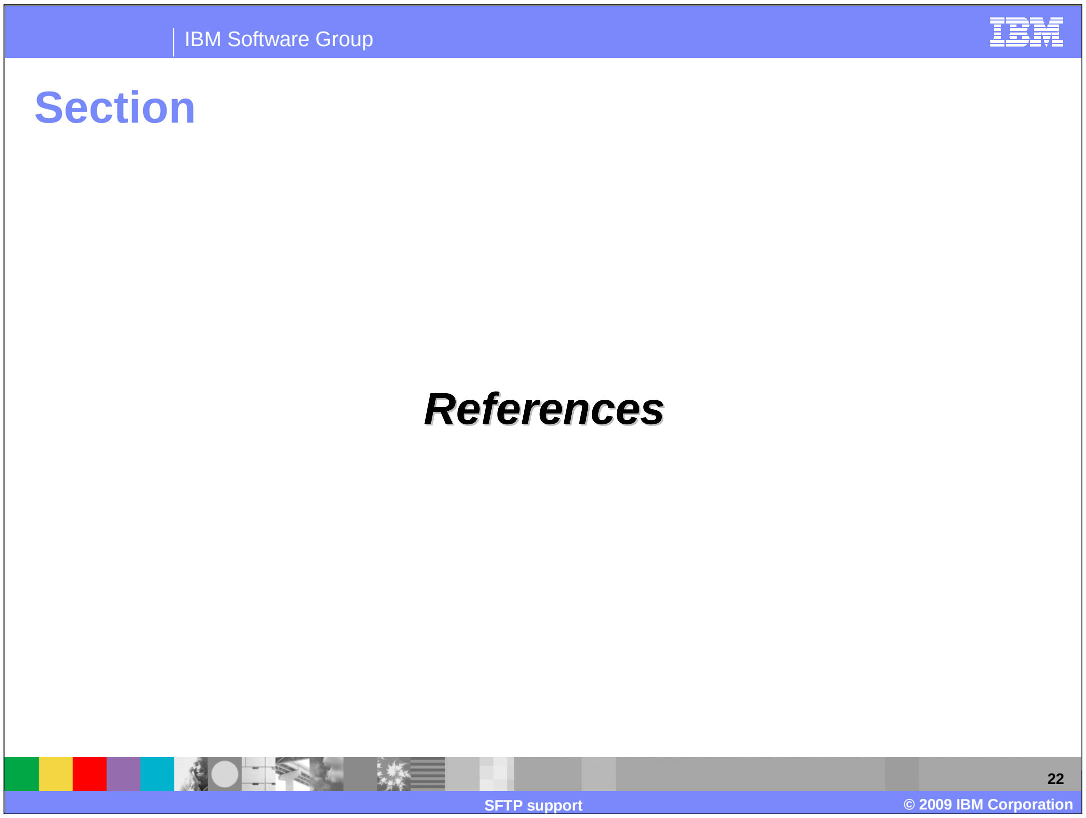
This section will provide a brief summary of this presentation.



Summary

- This presentation covered details on
  - Support for SFTP in WebSphere Partner Gateway
    - Scenarios
    - Security
  - Receiving files using SFTP in WebSphere Partner Gateway
  - Sending files using SFTP in WebSphere Partner Gateway

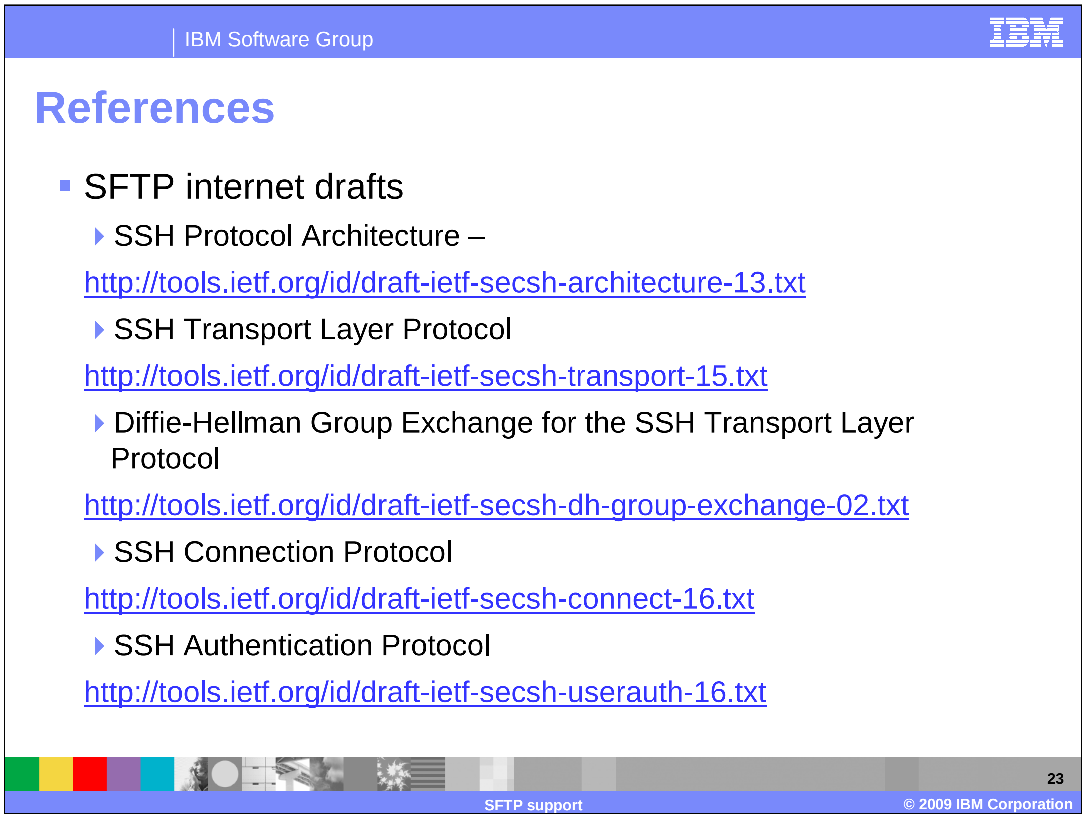
This presentation covered the SFTP support in WebSphere Partner Gateway V6.2. Various scenarios in which SFTP can be used, security functionality provided and details of configuration for receiving and sending documents using WebSphere Partner Gateway were discussed.



Section

References

This section will provide relevant references.



References

- SFTP internet drafts
  - SSH Protocol Architecture –

    http://tools.ietf.org/id/draft-ietf-secsh-architecture-13.txt
  - SSH Transport Layer Protocol

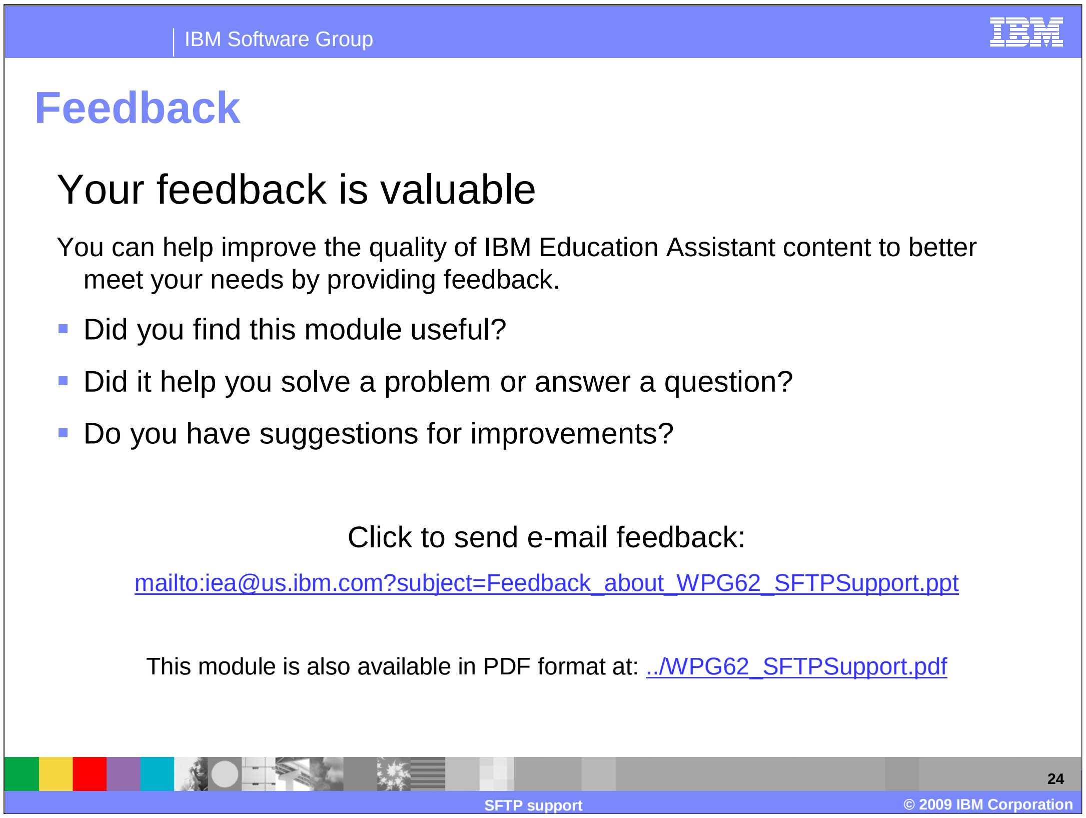
    http://tools.ietf.org/id/draft-ietf-secsh-transport-15.txt
  - Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol

    http://tools.ietf.org/id/draft-ietf-secsh-dh-group-exchange-02.txt
  - SSH Connection Protocol

    http://tools.ietf.org/id/draft-ietf-secsh-connect-16.txt
  - SSH Authentication Protocol

    http://tools.ietf.org/id/draft-ietf-secsh-userauth-16.txt

The slide provides the links to the RFCs relevant to SFTP support in WebSphere Partner Gateway 6.2.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

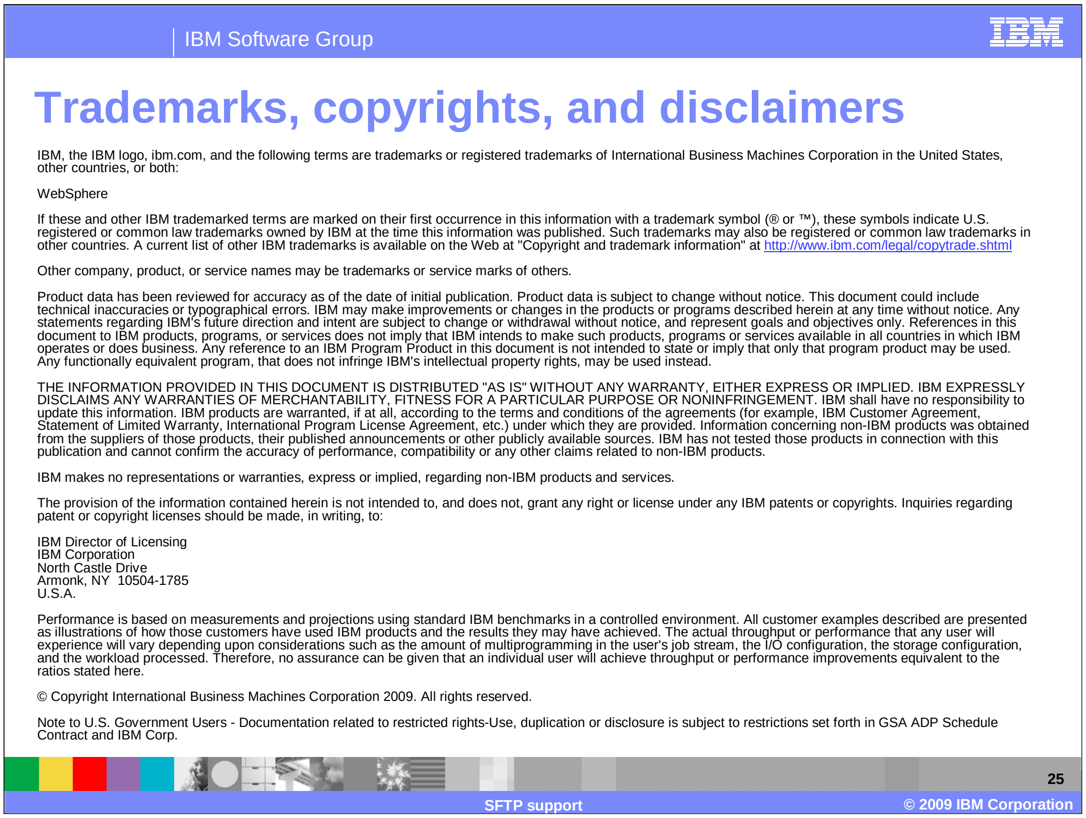
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WPG62_SFTPSupport.ppt

This module is also available in PDF format at: ../WPG62_SFTPSupport.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, copyrights, and disclaimers

IBM, the IBM logo, ibm.com, and the following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

WebSphere

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of other IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

Other company, product, or service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.