Informatica® Intelligent Cloud Services
July 2024

File Transfer

Informatica Intelligent Cloud Services File Transfer
July 2024

Publication Date: 2024-07-12

Table of Contents

Preface

Use *File Transfer* to learn how to exchange files between Informatica Intelligent Cloud Services℠ and remote partners. Learn how to configure file servers and create file server users.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Intelligent Cloud Services web site

You can access the Informatica Intelligent Cloud Services web site at http://www.informatica.com/cloud. This site contains information about Informatica Cloud integration services.

Informatica Intelligent Cloud Services Communities

Use the Informatica Intelligent Cloud Services Community to discuss and resolve technical issues. You can also find technical tips, documentation updates, and answers to frequently asked questions.

Access the Informatica Intelligent Cloud Services Community at:

https://network.informatica.com/community/informatica-network/products/cloud-integration

Developers can learn more and share tips at the Cloud Developer community:

https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers

Informatica Intelligent Cloud Services Marketplace

Visit the Informatica Marketplace to try and buy Data Integration Connectors, templates, and mapplets:

https://marketplace.informatica.com/

Data Integration connector documentation

You can access documentation for Data Integration Connectors at the Documentation Portal. To explore the Documentation Portal, visit https://docs.informatica.com.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Intelligent Cloud Services Trust Center

The Informatica Intelligent Cloud Services Trust Center provides information about Informatica security policies and real-time system availability.

You can access the trust center at https://www.informatica.com/trust-center.html.

Subscribe to the Informatica Intelligent Cloud Services Trust Center to receive upgrade, maintenance, and incident notifications. The Informatica Intelligent Cloud Services Status page displays the production status of all the Informatica cloud products. All maintenance updates are posted to this page, and during an outage, it will have the most current information. To ensure you are notified of updates and outages, you can subscribe to receive updates for a single component or all Informatica Intelligent Cloud Services components. Subscribing to all components is the best way to be certain you never miss an update.

To subscribe, on the Informatica Intelligent Cloud Services Status page, click **SUBSCRIBE TO UPDATES**. You can choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

Informatica Global Customer Support

You can contact a Global Support Center through the Informatica Network or by telephone.

To find online support resources on the Informatica Network, click **Contact Support** in the Informatica Intelligent Cloud Services Help menu to go to the **Cloud Support** page. The **Cloud Support** page includes system status information and community discussions. Log in to Informatica Network and click **Need Help** to find additional resources and to contact Informatica Global Customer Support through email.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at https://www.informatica.com/services-and-training/support-services/contact-us.html.

CHAPTER 1

File transfer

You can either use B2B Gateway or the Data Integration REST API sendfiles resource to exchange files.

To exchange files with a remote partner, configure your organization's file servers associated with the File Integration Service to securely communicate with the partner's servers. The File Integration Service is a Secure Agent service that runs advanced file transfer protocols.

You can configure the following types of file servers to exchange files with remote partners:

AS2 server

To receive files from partners with AS2 file transfer, configure an AS2 server to receive files from remote AS2 servers.

To send AS2 files to a partner's server, configure a connection, and then send the files to the partner using the Informatica Intelligent Cloud Services REST API. For more information, see the help for the AS2 Connector in the Data Integration help.

For example, you want to exchange EDI messages with a partner's AS2 server. To receive files from the partner, you configure your file server to accept files from the partner's server. To send files to your partner's server, you configure an AS2 connection for the partner. Then you send a POST request using the sendfiles REST API resource to transfer the EDI messages to the partner's server.

HTTPS server

To exchange files with partners with HTTPS file transfer, configure an HTTPS server so that partners can connect to the server, upload files to the server and download files from the server.

SFTP server

To exchange files with partners with SFTP file transfer, configure an SFTP server so that partners can connect to the server, and upload to and download files from the server.

MLLP server

The Minimal Lower Layer Protocol (MLLP) protocol is used to transfer healthcare industry messages, such as HL7 messages. HL7 is a messaging specification for healthcare information systems. To transfer healthcare industry messages with the MLLP protocol, configure an MLLP server so that partners can connect the server, upload files to the server, and download files from the server.

Proxy server

You can install and configure one or more file integration proxy servers in the demilitarized zone (DMZ). The partners' servers then communicate with the proxy servers instead of communicating directly with the organization's file servers. Multiple file servers can use the same file integration proxy server.

You can install proxy servers on Windows and Linux operating systems.

For each remote partner that exchanges files with your organization, you create a file server user account. You define the protocol accessibility for the file server user, that is, AS2, HTTPS, SFTP, or various combinations of these servers. A home directory is created or assigned to each file server user. You can

define network shared locations to the user's home directory, and define folder level and file level permissions for the user.

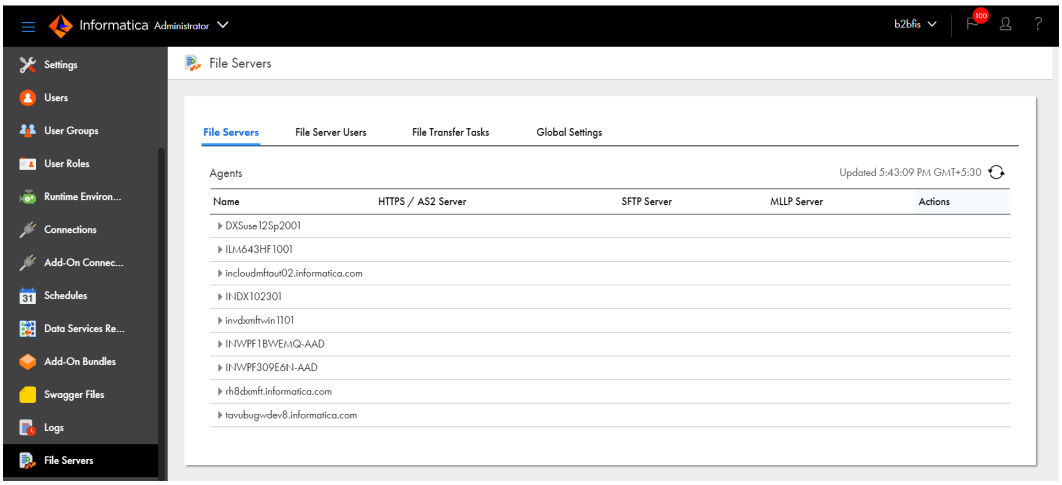
You can monitor file transfer jobs on the **File Transfer Logs** page in Monitor. For information about monitoring file transfer jobs, see the Monitor help.

CHAPTER 2

File server configuration process

Configure file servers, file server users, and global settings to exchange files between remote partners and your Informatica Intelligent Cloud Services organization.

You can configure file servers for each Secure Agent that uses the File Integration Service. Configure file servers on the **File Servers** page in Administrator. The **File Servers** page lists all of the runtime environments and Secure Agents in your organization that can use the File Integration Service.



Enabling external partners to exchange files with your organization includes the following tasks:

- Configure file server properties. You can configure an AS2, HTTPS, SFTP, and MLLP server .
- Optionally, install and configure one or more proxy servers as intermediaries between the partner's file servers and the organization's file servers.
- Configure server users for remote partners so that they can exchange files with your server.
- Specify default folders where the files are exchanged.

Before you begin

Before you configure file servers, ensure that you have the appropriate licenses and that you exchange public keys with the partner.

To ensure that your organization can exchange files with a remote server, complete the following tasks:

1. Send your public keys to the partner.

2. Receive the partner public keys.
3. Import the partner public keys to your trust store.
4. Configure the file server settings.

Note:

- Ensure that the File Integration Service is running on the Secure Agent. For information about checking the status of Secure Agent services, see *Secure Agent Services*.
- Ensure that you have sufficient privileges to create, read, update, delete, and set permissions on file servers.

CHAPTER 3

File servers

Configure file servers to exchange files with remote partners.

You can configure the following servers:

- AS2 server. Receives files from partners with AS2 file transfer.
- HTTPS server. Partners connect to the server to upload and download files.
- SFTP server. Partners connect to the server to upload and download files.
- MLLP server. Partners connect to the server to transfer healthcare industry messages.
- Proxy server. An intermediary between the partner's file servers and the organization's file servers.

Configuring a file server

Configure properties for a file server to exchange files between the server and remote partners.

1. In Administrator, select **File Servers**.
2. On the **File Servers** tab, select the Secure Agent that runs the File Integration Service that you want to use to exchange files with the remote servers.
3. On the **File Server for agent** page, select the tab for the type of server to configure, HTTPS server, AS2 server, SFTP server, or proxy server.
4. Configure the file server properties, and then click **Save**.

AS2 server configuration properties

For each runtime environment that uses the File Integration Service, you can configure an AS2 server to receive files from remote AS2 servers.

You configure AS2 server properties on the **AS2 Server** tab of the **File Server for agent** page.

Configure the following types of properties:

- General
- SSL
- Listeners
- Message security

- MDN (Message Disposition Notifications)
- Upload restrictions

General properties

The following table describes general AS2 server properties:

Property	Description
Enable AS2 Server	Whether to enable the AS2 server. When not enabled, the AS2 server cannot receive files. Default is disabled.
AS2 Server Id	Name or ID used by the sender. Note the following rules for the ID: - The value is case sensitive. - The ID can contain up to 128 ASCII characters, special characters, and spaces.
Port	Port number for the AS2 server. Default is 15400.
Local Address	Local address of the AS2 sever.
Enable SSL	Whether to use SSL encryption in communications with remote AS2 servers. Default is disabled.

SSL properties

The following table describes the SSL properties:

Property	Description
SSL Protocol	Whether to use the SSL or TLS protocol to secure HTTPS connection. Select one of the following values: - TLS. A new version of SSL, Transport Layer Security is used to secure the transmission. - SSL. A traditional Secure Socket Layer protocol is used to secure the transmission. Default is SSL.
Enabled SSL Protocols	Specify the permissible TLS and SSL versions separated with a comma. The supported versions are: - TLS: TLSv1.2, and TLSv1.3 - SSL: SSLv2Hello and SSLv3 When a value is not specified, all the versions for the selected protocol are enabled.
Client Authentication	Whether the client must have a certificate to authenticate with the server. Choose one of the following values: - None. The SSL connection runs without checking certificates and the user is authenticated with a password. If any of the information being transmitted requires a certificate, the connection fails. - Required. The SSL connection will not connect or authenticate a user unless a valid certificate is available. - Optional. The SSL connection looks for a valid certificate, but continues with password authentication if a certificate is not present.

Property	Description
Key Store Location	Location of the key store that stores the private key and associated certificates that the client uses to authenticate communications with the File Integration Service. Include a path and a file name.
Key Store Password	Password to access the key store.
Key Store Type	Type of the private key store. Use one of the following values: - JKS - PKCS12
Key Alias	Key alias or certificate for the private key used to sign the MDN.
Trust Store Location	The path to the trust store file that the File Integration Service uses for HTTPS communication.
Trust Store Password	Password to access the trust store.
Trust Store Type	Type of trust store. Use one of the following values: - JKS - PKCS12

Listeners properties

You can add multiple server listeners to an AS2 server. Use a server listener to configure the AS2 server with a specific port number and local address. To add a server listener to the list, click **Add Listener**.

The following table describes the add listener properties:

Property	Description
Name	Name of the server listener.
Port	Port number of the server that the listener monitors.
Local Address	Local address of the server listener.
Enable SSL	Whether to enable SSL over HTTPS connection to communicate with the AS2 listener . When disabled, use HTTP instead of HTTPS to establish a connection with the AS2 listener. Default is disabled.
SSL Protocol	Applies when you enable SSL. Whether to use the SSL or TLS protocol to secure HTTPS connection. Select one of the following values: - TLS. A new version of SSL, Transport Layer Security will be used to secure the transmission. - SSL. A traditional Secure Socket Layer protocol is used to secure the transmission.

Property	Description
Enabled SSL Protocols	Applies when you enable SSL. Specify the permissible TLS and SSL versions separated with a comma. The supported versions are: - TLS: TLSv1.2, and TLSv1.3 - SSL: SSLv2Hello and SSLv3 When no value is specified, all the versions for the selected protocol are enabled.
Client Authentication	Whether the client must have a certificate to authenticate with the server. Choose one of the following values: - None. The SSL connection runs without checking certificates and the user is authenticated with a password. If any of the information being transmitted requires a certificate, the connection fails. - Required. The SSL connection will not connect or authenticate a user unless a valid certificate is available. - Optional. The SSL connection looks for a valid certificate, but continues with password authentication if a certificate is not present.
Key Store Location	Location of the key store that stores the private key and associated certificates that the client uses to authenticate communications with the File Integration Service. Include a path and a file name.
Key Store Password	Password to access the key store.
Key Store Type	Type of private key store. Use one of the following values: - JKS - PKCS12
Key Alias	A unique name assigned to a key in a Key Store.
Trust Store Location	The path to the trust store file that the File Integration Service uses for HTTPS communication.
Trust Store Password	Password to access the trust store.
Trust Store Type	Type of trust store. Use one of the following values: - JKS (Java Key Store) - PKCS12 (Public-Key Cryptography Standards)

Message security properties

The following table describes basic message security properties:

Property	Description
Encryption Required	Whether files received by the File Integration Service must be encrypted. Default is enabled.
Signature Required	Whether files from the remote AS2 server must contain a digital signature. If a signature is required, the File Integration Service rejects any messages without the signature. Default is enabled.

Property	Description
Authentication Required	Whether the user is required to authenticate. Default is disabled.
Decryption Certificate Alias	Key alias or certificate used to decrypt incoming messages. The alias references a certificate in the key store. All partners who send AS2 messages must have the public portion of this certificate.

MDN properties

The following table describes message receipt properties:

Property	Description
MDN Signature Certificate Alias	Alias that refers to the private key that the AS2 server uses to sign the message receipt. The private key is in the default private key store.
Asynchronous MDN Automatic Approval	Whether to send a return receipt automatically or manually.
Enabled Proxy for Async MDN	Determines if a proxy server is enabled for Asynchronous MDN. Default is disabled.
Proxy Type	Type of proxy server to use for the connection. Select one of the following types: - SOCKS. You can use SOCKS version 4 or 5. - HTTPS. - Informatica File Server proxy. Verify with your network administrator which proxy server type to use.
Host	Host name or IP address of the proxy server on your network.
Port	Port number of the proxy server on your network. If left blank, the default port for HTTP is 80 and the default port for SOCKS is 1080.
User	User name to use for login when connecting to the proxy server.
Password	Password for connecting to the proxy server. Required if your network uses the proxy server to create HTTP or HTTPS connections.

Upload restrictions properties

You can specify the types of files to allow or deny in an AS2 file upload. The following table describes the properties that control upload restrictions:

Property	Description
File Extension Filter Type	Whether to accept or deny the extensions in the File Extensions list. Use one of the following values: - Do Not Filter. Accept all file types. - Accept. Accept files with the extensions listed in the File Extensions property. - Deny. Do not allow files with the extensions listed in the File Extensions property.
File Extensions	List of file extensions. Add the file extensions that correspond to the File Extension Filter Type. For example, to accept .csv and .txt files, in the File Extension Filter Type property, select **Accept**, and then add csv and txt to the list of file extensions. To add an extension to the list, type the extension in the text box and click **Add**. To remove an extension from the list, highlight the extension and click **Delete**.
File Extension Case Sensitive	Whether to factor case when you filter using the file extensions list. When enabled, files with extensions that do not match the case used in the File Extensions list cannot be uploaded. For example, if the file extension list includes csv but not CSV, files with the extension of csv can be uploaded but files with the extension of CSV cannot be uploaded.
Allow Files with Extension	Whether to enable the file extension filter. When enabled, the file extension properties configured on this page determine which file types can be uploaded. Default is enabled.
Allow Files with No Extension	Whether to allow files that do not include the extension in the file name. Default is enabled.
Allow Files with No Name	Whether to allow files with no name. The Secure Agent saves files without a name using the following format: `as2data_<datetime>` where datetime is the current time stamp including milliseconds. Default is enabled.
File Name Suffix Timestamp (Optional)	Whether to append timestamp to the file name. When enabled, the timestamp is suffixed to the file name.
Max Upload Size	Maximum file size that the AS2 server can upload, in megabytes. Default is 5 MB.
When File Exists	Choose the action to be performed when a file that already exists in the folder is received again. Select one of the following options: - Rename: Rename the newly received file. - Append: Append the changes to the existing file. - Overwrite: Overwrite the existing file with the newly received file. - Error: Display an error if the file already exists.

HTTPS server configuration properties

For each runtime environment that uses the File Integration Service, you can configure an HTTPS server to exchange files with remote HTTPS servers.

You configure HTTPS server properties on the **HTTPS Server** tab of the **File Server for agent** page. You must have the HTTPS license to exchange files through HTTPS servers.

Configure the following types of properties:

- General
- SSL
- Listeners
- MDN (Message Disposition Notifications)
- Upload restriction

General properties

The following table describes general HTTPS server properties:

Property	Description
Enable HTTPS Server	Whether to enable the HTTPS server. When not enabled, the HTTPS server cannot receive files. Default is disabled.
Port	Port number of the HTTPS server. Default is 15400.
Local Address	Local address of the HTTPS sever.
Enable SSL	Whether to use SSL encryption in communication with remote HTTPS servers. Default is disabled.

SSL properties

The following table describes the SSL properties:

Property	Description
SSL Protocol	Whether to use the SSL or TLS protocol to secure HTTPS connection. Select one of the following values: - TLS. A new version of SSL, Transport Layer Security is used to secure the transmission. - SSL. A traditional Secure Socket Layer protocol is used to secure the transmission. Default is SSL.
Enabled SSL Protocols	Specify the permissible TLS and SSL versions separated with a comma. The supported versions are: - TLS: TLSv1.1,TLSv1.2, and TLSv1.3 - SSL: SSLv2Hello and SSLv3 When a value is not specified, all the versions for the selected protocol are enabled.

Property	Description
Client Authentication	Whether the client must have a certificate to authenticate with the server. Choose one of the following values: - None. The SSL connection runs without checking certificates and the user is authenticated with a password. If any information being transmitted requires a certificate, the connection fails. - Required. The SSL connection will not connect or authenticate a user unless a valid certificate is available. - Optional. The SSL connection looks for a valid certificate, but continues with password authentication if a certificate is not present.
Key Store Location	Location of the key store that stores the private key and associated certificates. Client uses the key store file to authenticate communication with the File Integration Service. Include a path and a file name.
Key Store Password	Password to access the key store.
Key Store Type	Type of private key store. Use one of the following values: - JKS - PKCS12
Key Alias	Key alias or certificate for the private key used to sign the MDN.
Trust Store Location	The path to the trust store file that the File Integration Service uses for HTTPS communication.
Trust Store Password	Password to access the trust store.
Trust Store Type	Type of trust store. Use one of the following values: - JKS - PKCS12

Listeners properties

You can add multiple server listeners to an HTTPS server. Use a server listener to configure the HTTPS server with a unique port and local address. To add a server listener to the list, click **Add Listener**.

The following table describes the add listener properties:

Property	Description
Name	Name of the server listener.
Port	Port number of the server that the listener monitors.
Local Address	Local address of the server listener.
Enable SSL	Whether to enable SSL over HTTPS connection to communicate with the AS2 listener. When not enabled, use HTTP instead of HTTPS to establish a connection with the HTTPS listener. Default is disabled.

Property	Description
SSL Protocol	Applies when you enable SSL. Whether to use the SSL or TLS protocol to secure HTTPS connection. Select one of the following values: - TLS. A new version of SSL, Transport Layer Security will be used to secure the transmission. - SSL. A traditional Secure Socket Layer protocol is used to secure the transmission.
Enabled SSL Protocols	Specify the permissible TLS and SSL versions separated with a comma. The supported versions are: - TLS: TLSv1.2, and TLSv1.3 - SSL: SSLv2Hello and SSLv3 When no value is specified, all the versions for the selected protocol are enabled.
Client Authentication	Whether the client must have a certificate to authenticate with the server. Choose one of the following values: - None. The SSL connection runs without checking certificates and the user is authenticated with a password. If any of the information being transmitted requires a certificate, the connection fails. - Required. The SSL connection will not connect or authenticate a user unless a valid certificate is available. - Optional. The SSL connection looks for a valid certificate, but continues with password authentication if a certificate is not present.
Key Store Location	Location of the key store that stores the private key and associated certificates that the client uses to authenticate communications with the File Integration Service. Include a path and a file name.
Key Store Password	Password to access the key store.
Key Store Type	Type of the private key store. Use one of the following values: - JKS - PKCS12
Key Alias	Alias of a certificate to configure a listener for an HTTPS connector.
Trust Store Location	The path to the trust store file that the File Integration Service uses for HTTPS communication.
Trust Store Password	Password to access the trust store.
Trust Store Type	Type of trust store. Use one of the following values: - JKS - PKCS12

MDN properties

The following table describes message receipt properties:

Property	Description
Proxy Type	Type of proxy server to use for the connection. Select one of the following types: - SOCKS. You can use SOCKS version 4 or 5. - HTTPS. - Informatica File Server proxy. Verify with your network administrator which proxy server type to use.
Host	Host name or IP address of the proxy server on your network.
Port	Port number of the proxy server on your network. If left blank, the default port for HTTP is 80 and the default port for SOCKS is 1080.
User	User name to use for login when connecting to the proxy server.
Password	Password for connecting to the proxy server. Required if your network uses the proxy server to create HTTP or HTTPS connections.

Upload restrictions properties

You can specify the types of files to allow or deny in an HTTPS file upload.

The following table describes the properties that control upload restrictions:

Property	Description
File Extension Filter Type	Whether to accept or deny the extensions in the File Extensions list. Use one of the following values: - Do Not Filter. Accept all file types. - Accept. Accept files with the extensions listed in the File Extensions property. - Deny. Do not allow files with the extensions listed in the File Extensions property.
File Extensions	List of file extensions. Add the file extensions that correspond to the File Extension Filter Type. For example, to accept .csv and .txt files, in the File Extension Filter Type property, select **Accept**, and then add csv and txt to the list of file extensions. To add an extension to the list, type the extension in the text box and click **Add**. To remove an extension from the list, highlight the extension and click **Delete**.
File Extension Case Sensitive	Whether to factor case when you filter using the file extensions list. When enabled, files with extensions that do not match the case used in the File Extensions list cannot be uploaded. For example, if the file extension list includes csv but not CSV, files with the extension of csv can be uploaded but files with the extension of CSV cannot be uploaded.
Allow Files with Extension	Whether to enable the file extension filter. When enabled, the file extension properties configured on this page determine which file types can be uploaded. Default is enabled.
Allow Files with No Extension	Whether to allow files that do not include the extension in the file name. Default is enabled.

Property	Description
Allow Files with No Name	Whether to allow files without a name. The Secure Agent saves files without a name using the following format: `as2data_<datetime>` where <datetime> is the current time stamp including milliseconds. Default is disabled.
Max Upload Size(MB)	The file size limit in megabytes for the HTTPS server upload. Default is 5 MB.

SFTP server configuration properties

For each runtime environment that uses the File Integration Service, you can configure an SFTP server to exchange files.

You configure SFTP server properties on the **SFTP Server** tab of the **File Server for agent** page. Configure the following types of properties:

- General properties
- Algorithms properties
- Host keys properties
- Upload restriction properties

General properties

The following table describes general SFTP server properties:

Property	Description
Enable SFTP Server	Whether to enable the SFTP server. When not enabled, the SFTP server cannot receive or send files. Default is disabled.
Port	Port number for the SFTP server. Default is 15002.
Local Address	Local IP address for the SFTP sever.
Enable SCP	Whether to use session control protocol (SCP) to create the connection. Default is disabled.
Idle Timeout	Number of seconds that the connection is idle before is closes. Default is 300.
Maximum Logins	Maximum number of users that can be logged in to the server concurrently. Default is 500.
Login Failure Delay	Delay between failed login attempts, in seconds. Default is 0.

Property	Description
Maximum Login Failures	Number of allowed login failures for a user. Default is 5.
Welcome Message	Message to show when the connection to the server is established.

Algorithms properties

Enable the following algorithm types in the **Algorithms** section of the **SFTP Server** tab:

- Cipher algorithms
- Message Authentication Code (MAC) algorithms
- Compression algorithms
- Key exchange algorithms

When you configure the use of algorithms for SFTP file exchange, consider the following rules and guidelines:

- You can move algorithms between the **Available** and **Selected** lists. The File Integration Service applies the algorithms that are listed in the **Selected** list.
- If no algorithms are selected for an algorithm type, the File Integration Service applies all the algorithms that are listed in the **Available** list.
- The File Integration Service applies the algorithms in the order in which they are listed, from the top of the list to the bottom of the list. You can use the up and down arrows to change the order of the algorithms in list.

Host keys properties

The following table describes host keys properties:

Property	Description
RSA Key File Location	Location of the RSA host key file.
RSA Key Passphrase	Passphrase for the RSA key.
DSA Key File Location	Location of the DSA host key file.
DSA Key Passphrase	Passphrase for the DSA key.

Upload restrictions properties

You can specify the types of files to allow or deny in an SFTP file exchange. The following table describes the properties that control upload restrictions:

Property	Description
File Extension Filter Type	Whether to accept or deny the extensions in the File Extensions list. Use one of the following values: - Do Not Filter. Accept all file types. - Accept. Accept files with the extensions listed in the File Extensions property. - Deny. Do not allow files with the extensions listed in the File Extensions property. Default is **Do Not Filter**.
File Extensions	List of file extensions. Add the file extensions that correspond to the File Extension Filter Type. For example, to accept .csv and .txt files, in the File Extension Filter Type property, select **Accept**, and then add csv and txt to the list of file extensions. To add an extension to the list, type the extension in the text box and click **Add**. To remove an extension from the list, highlight the extension and click Delete.
File Extension Case Sensitive	Whether to factor case when you filter using the file extensions list. When enabled, files with extensions that do not match the case used in the File Extensions list cannot be uploaded. For example, if the file extension list includes csv but not CSV, files with the extension of csv can be uploaded but files with the extension of CSV cannot be uploaded. Default is disabled.
Allow Files with No Extension	Whether to allow files that do not include the extension in the file name. Default is disabled.
Allow Files with Extension	Whether to enable the file extension filter. When enabled, the file extension properties configured on this page determine which file types can be uploaded. Default is enabled.

MLLP server configuration properties

For each runtime environment that uses the File Integration Service, you can configure an MLLP server to exchange files with remote MLLP servers.

The Minimal Lower Layer Protocol (MLLP) protocol is used to transfer healthcare industry messages, such as HL7 messages. HL7 is a messaging specification for healthcare information systems.

You configure MLLP server properties on the **MLLP Server** tab of the **File Server for agent** page.

Configure the following types of properties:

- General
- Kafka Connections
- Listeners

General properties

The following table describes general MLLP server property:

Property	Description
Enable MLLP Server	Specify whether to enable the MLLP server. When disabled, the MLLP server cannot receive files.

Kafka Connections

The following table describes the Kafka Connections properties:

Property	Description
Connection Name	Specify the Kafka connection that you want to use for MLLP servers. Click **Select** to view the list of available Kafka connections. Select the option corresponding to the Kafka connection that you want to use, and click **OK**. Required if you select Kafka as the target type for your listener.

Listeners properties

You can add multiple server listeners to an MLLP server. Use a server listener to configure the MLLP server with a unique port and local address.

To add a server listener to the list, click **Add Listener**. You can start or stop individual listeners. You must save the edits made to the listener configuration before you start or stop the listener. The MLLP server must have at least one listener.

Note: You can also edit and delete the existing listeners. Before you modify or delete a listener, make sure that it isn't running.

The following table describes the properties that you need to configure when you add a new listener:

Property	Description
Name	Name of the MLLP server listener. The name of the listener must be unique.
Port	Port number of the server that the listener monitors.
Local Address	IP address of the server hosting the port to which file server listens. The Port and Local Address combination must be unique.
Idle Timeout	Number of seconds that the connection is idle before is closes. Default is 300.
Validate Message	Specify whether the listener validates the structure of the HL7 messages in accordance to HL7 version 2.8.1. Select one of the following values: - Yes. The listener validates the HL7 messages. - No. The listener does not validate the HL7 messages.

Property	Description
Target Type	Select one of the following target types: - Kafka: Stores the messages in the specified Kafka connection. If you select Kafka, select a topic for your Kafka connection. - File: Stores the messages as a file in the specified directory. if you select File, specify the **Target Location** and **Filename Prefix**.
Topic Name	The Kafka topic where you want to publish the messages. Click **Select** to view the list of available Kafka topics for your connection. Select the radio button corresponding to the Kafka topic that you want to use, and click **OK**.
Target Location	The location where you want to store the messages.
Filename Prefix	The prefix that you want to use for the message file names.

Proxy server configuration properties

For each runtime environment that uses the File Integration Service, you can configure one or more proxy servers.

You configure proxy server properties on the **Proxy Server** tab of the **File Server for agent** page. The latest available file integration proxy version appears on this tab.

Note: You must also install the proxy server in the DMZ. For more information, see "Installing a file integration proxy server" on page 25.

To add a proxy server, click **Add Proxy Configuration**, configure server settings, and click **Save**.

Configure the following types of properties:

- General properties
- Service mappings properties, which associate internal file servers with the proxy server

General properties

The following table describes general proxy server properties:

Property	Description
Enabled	Whether or not the proxy server is enabled. Default is Yes.
Controller Address	External IP address of the server in the DMZ on which the proxy server listens for control connections from the organization file servers.
Controller Port	Port number for the server in the DMZ on which the proxy server listens for control connections from the organization file servers. Default is 9100.

Property	Description
Minimum Number of Threads	Minimum number of threads that are reserved for connections to the location where the proxy server is installed. Default is 10.
Maximum Number of Threads	Maximum number of simultaneous requests that the proxy server can handle. Default is 2000.
Thread Keep Alive Time	The number of seconds idle threads wait before terminating. Default is 60.

Service mappings properties

To configure service mappings for the proxy server, in the **Proxy Server Configuration** page, click **Add** next to **Service Mappings**, configure the mapping parameters, and click **OK**. You can add as many service mappings as required to associate internal file servers with the proxy server.

The following table describes the service mappings properties:

Property	Description
Label	Label of the mapping.
From Address	IP address of the proxy server.
From Port	Port number of the proxy server.
To Address	IP address of the internal file server.
To Port	Port number of the internal file server.
Load Balancer Rule	Name of the load balancing rule to use with the mapping. The name of the rule must be identical to the name that appears in the `proxy.xml` file, which is part of the proxy server installation. For more information, see "Installing a file integration proxy server" on page 25.

Installing a file integration proxy server

Install a file integration proxy server in the DMZ and configure server parameters. You can install the server on Windows and Linux operating systems.

Note: You must also enable the proxy server and configure server properties in Informatica Intelligent Cloud Services, in Administrator. For more information, see "Proxy server configuration properties" on page 24.

To install the fis-proxy-server_<version>.zip file, perform the following steps:

1. Download the `fis-proxy-server_<version>.zip` file from the following locations and copy the file to the server in the DMZ:
   - Linux. $<Secure Agent installation directory>/downloads/FileIntegrationService
   - Windows. %<Secure Agent installation directory>%\downloads\FileIntegrationService
2. Download Java 1.8 (OpenJDK or Oracle) and install it on the server in the DMZ.

3. From the `fis-proxy-server_<version>/bin` folder, edit one of the following files:
   - On a Windows operating system, edit `setenv.bat`.
   - On a Linux operating system, edit `setenv.sh`.

   a. Set JAVA_HOME to the JDK Home or the JRE home of Java 1.8.

   b. Set the folder path of fis-proxy-server to FIS_PROXY_HOME.
4. From the `fis-proxy-server_<version>/config` folder, edit the `proxy.xml` file and set values for the following variables:

Variable	Description
controllerAddress	External IP address of the server in the DMZ on which the proxy server listens for control connections from the organization file servers.
dataAddress	Internal IP address of the server in the DMZ on which the proxy server listens for data connections from the organization file servers.
proxyAddress	IP address of the server in the DMZ on which the proxy server listens for incoming connections.
forwardProxyLocalAddress	IP address of the server in the DMZ on which the proxy server establishes outbound connections to remote servers as a forward proxy.

   If required, change the port numbers.
5. To start the proxy server, run one of the following commands:
   - On a Windows operating system, run `fis-proxy.bat start`.
   - On a Linux operating system, run `fis-proxy.sh start`.
6. To stop the proxy server, run one of the following commands:
   - On a Windows operating system, run `fis-proxy.bat stop`.
   - On a Linux operating system, run `fis-proxy.sh stop`.

   The proxy server saves logs in the `fis-proxy-server_<version>/logs` folder.

Stopping and starting a file server

You can stop or start a File Integration Service file server on the **File Servers** page. Stop and start a file server after you make configuration changes.

Stopping and starting HTTPS, AS2, SFTP, and MLLP servers

To stop or start an HTTPS, AS2, SFTP, or an MLLP server, perform the following actions:

1. In Administrator, select **File Servers**.
2. On the **File Servers** tab, click the arrow next to the name of the Secure Agent that runs the server.
3. From the **Actions** menu, choose the option to start or stop the server.

   Informatica Intelligent Cloud Services adds an entry in the audit log to indicate the action.

Stopping and starting a proxy server

To stop or start a proxy server, perform the following actions:

1. In Administrator, select **File Servers**.
2. On the **File Servers** tab, select the Secure Agent that runs the File Integration Service on which to stop or start the proxy server.
3. On the **File Server for agent** page, select the **Proxy Server** tab.
4. From the Actions menu of the server to stop or start, select **Stop** or **Start**.

   Informatica Intelligent Cloud Services adds an entry in the audit log to indicate the action.

CHAPTER 4

File server users

Create a user account for each remote partner that exchanges files with your organization. The user account enables the partner to exchange files with your server.

For each remote partner, configure the following types of properties:

- General properties such as user name, email address, and password.
- Server-specific properties for HTTPS, AS2, and SFTP servers.
- Folder permissions.

Note: File server user accounts are different from Informatica Intelligent Cloud Services user accounts. File server user accounts enable remote partner users to exchange files with your organization's file servers. Informatica Intelligent Cloud Services user accounts enable your users to access your Informatica Intelligent Cloud Services organization.

Configuring a file server user

Configure partner users so that partners can exchange files with your organization.

When you create a file server user, the user receives an email from Informatica Intelligent Cloud Services. If you choose to include a system-generated password when you configure the user, a generated password is included in the email.

1. In Administrator, click **File Servers** > **File Server Users**.
2. Click **Add User**.
3. Perform the following actions, and then click **Save**:
   - Enter general information about the user.
   - To enable the user to send files to AS2 servers in the organization, enable the AS2 protocol and configure AS2 settings.
   - To enable the user to exchange files with SFTP servers in the organization, enable the SFTP protocol and configure SFTP settings.
   - To enable the user to exchange files with HTTPS servers in the organization, enable the HTTPS protocol and configure HTTPS settings.
   - Add folder and file permissions for the user. By default, the user has all permissions on the default home directory.

File server user properties

Configure properties for file server users.

General properties

The following table describes general properties for the user:

Property	Description
Username	User name for the file server user.
Description	Description for the user.
Company name	User account name of the remote partner that exchanges files with your organization.
Email	The user's email address.
Password Generation	Whether to create a password for the user or enable the system to create a system-generated password. Passwords must include the following characteristics: - Must be at least eight characters long. - Must have at least one upper case letter. - Must have at least one digit. - Must have at least one of the following special characters: `@ $ ! & * ~ - _`

AS2 server properties

The following table describes AS2 server properties for the file server user:

Property	Description
Enable AS2 Protocol	Whether or not the AS2 protocol is enabled. Disable this option when you do not want the AS2 server to receive files. Default is enabled.
Authentication Type	Whether to require a **Password**, **Certificate**, **Both**, or **Either**. If **Password** is used for authentication, the password generation that you defined in the **General** tab is used. If **Certificate** is used for authentication, the Client Authentication setting for the AS2 server must be set to Optional or Required.
Digest Algorithm	If **Certificate**, **Both**, or **Either** is used for authentication, select the SHA fingerprint of the partner certificate. Select one of the following values: - SHA1 - SHA224 - SHA256 - SHA384 - SHA512
Certificate Fingerprint	Enter the SHA fingerprint based on the selected digest algorithm.
AS2 ID	The AS2 ID of the partner user.

Property	Description
Signature Certificate Alias	Private key alias to use to sign the message. The private key is located in the default private key store.
Default Upload Folder	The location where AS2 files are saved when received. The default location is the default home directory for the user. If blank, the files are saved to the home directory. For more information, see Chapter 6, "Global settings" on page 35.

SFTP server properties

The following table describes SFTP server properties for the file server user:

Property	Description
Enable SFTP Protocol	Whether or not the SFTP protocol is enabled. Disable this option when you do not want the SFTP server to send and receive files. Default is enabled.
Authentication Type	Whether to require a **Password**, **Public Key**, **Both** or **Either**. If a password is used for authentication, the password generation that you defined in the **General** tab is used. If a **Public Key** is used for authentication, you must place the key on the Secure Agent.
Public Key Location	Absolute path to the location of the public key on the Secure Agent. Applies when the **Public Key**, **Both**, or **Either** is used for authentication.

HTTPS server properties

The following table describes HTTPS server properties for the file server user:

Property	Description
Enable HTTPS Protocol	Whether or not the HTTPS protocol is enabled. Disable this option when you do not want the HTTPS server to receive files. Default is enabled.
Authentication Type	Whether to require a **Password**, **Certificate**, or **Either**. If a password is used for authentication, the password generation that you defined in the **General** tab is used. If **Certificate** is used for authentication, the Client Authentication setting for the HTTPS server must be set to Optional or Required.

Property	Description
Digest Algorithm	If **Certificate**, **Both**, or **Either** is used for authentication, select the SHA fingerprint of the partner certificate. Select one of the following values: - SHA1 - SHA224 - SHA256 - SHA384 - SHA512
Certificate Fingerprint	Enter the SHA fingerprint based on the selected digest algorithm.

Folder permissions properties

By default, a home directory and a user name are created for the user under the default home directory that is defined in the file servers **Global Settings** tab, and the user has all permissions on their home directory. You can edit the user's home directory to be in a different location.

To add permissions to other folders and files, click **Add** and define the permissions.

The following table describes folder permissions properties for the user:

Property	Description
Alias	An alias for the folder or file to which you grant permissions. The alias appears under the **Name** column in the **File Server User** page.
Path	Path to the folder or file to which you grant the user permissions.
Type	Determines whether the permissions are on a folder or on a file.
Folder Permissions	The user's permissions on the folder.
File Permissions	The user's permissions on the file.
Disk Space Restriction	Whether to restrict the disk space that the user can use on the folder, and, if yes, the allowed space on the disk. Applies to folder permissions.

IP filter properties

The following table describes IP filter properties for the file server user:

Property	Description
Enable IP Filter	Whether or not to enable an IP filter for the file server user. Default is disabled.
Filter Type	Select the filter type. Select one of the following options: - Black list. Denies access to the specified IP addresses and permits access to all other IP addresses. - White list. Permits access to the specified addresses and denies access to all other IP addresses. Default is white list.
Filter Entries	Enter a list of IP addresses that will either be denied or permitted access based on the selected filter type. Click **Add** to add multiple rows. Enter an IP address in a single, range, or Classless Inter-Domain Routing (CIDR) notation format. Do not leave spaces between hyphens or slashes in ranges or the CIDR notation format. For example, enter 10.1.4.1/24 or 10.1.4.1-10.1.255.255.

Deleting a file server user

You might want to delete a file server user if the user no longer works with your organization..

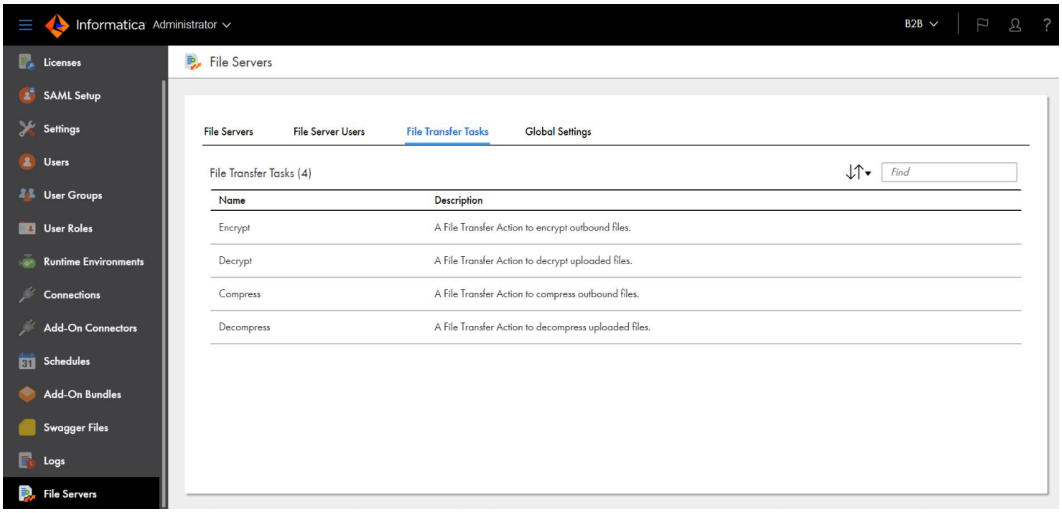
1. In Administrator, select **File Servers** > **File Server Users**.
2. In the row that contains the user name, click Actions and select **Delete User**.

CHAPTER 5

File transfer tasks

File transfer tasks are associated with the inbound and outbound process of the partner.

The **File Servers** page lists all the runtime environments and Secure Agents in your organization that can use the File Integration Service.



The **File Transfer Tasks** tab lists predefined file transfer tasks that can be used to run actions when files are received or sent to the file servers. The tab lists the projects in a read-only mode.

The **File Transfer Tasks** tab includes the following predefined file transfer tasks:

Name	Description
Encrypt	A file transfer task that uses PGP to encrypt outbound files when transferring them from the source location to the home directory of the file server user.
Decrypt	A file transfer task that uses PGP to decrypt uploaded files when transferring them from the home directory of file server user to the target location.
Compress	A file transfer task that compresses outbound files when transferring them from the source location to the home directory of file server user. You can choose one of the following compression methods: Zip, Tar, or Gzip.
Decompress	A file transfer task that decompresses uploaded files when transferring them from the home directory of file server user to the target location. You can choose one of the following decompression methods: Unzip, Untar, or Gunzip.

You can use the REST APIs to run the pre-defined tasks. You can also run the tasks using B2B Gateway.

For more information, see *REST API Reference*.

CHAPTER 6

Global settings

Configure properties that apply to all file servers configured for file transfer.

Folder settings

Configure the **Target Location** property to specify the default directory where all files received from remote servers are stored. User-specific home directories are created under the global home directory.

Note: Whenever you change the value of the default home directory you must stop and start the file servers.

SMTP server settings

The following table lists the SMTP server settings that apply to all remote file servers:

Property	Description
Host	Host name for the SMTP configuration to use for an email type MDN.
Port	Port on which the SMTP is running.
Username	User name to connect to the SMTP server.
Password	Password for the SMTP user.
Connection Type	Type of SMTP connection. Select one of the following values: - normal - implicitSSL - explicitSSL Default is normal.
From Email	Email address from which the email MDN is sent.
From Name	Name shown in the email.

PGP settings

Configure the **Public Key Ring** and **Secret Key Ring** to specify the directory where the public and secret key are stored. If the path is not specified, the default PGP key ring path is used.

Note: You can use the PGP Command Line Interface (PGP-CLI) to edit the configuration properties file when you have multiple Secure Agents. You must restart the FIS application for the PGP setting changes to reflect in the `pgp-configuration.properties` file. The configuration file is present in the `conf` folder of the PGP client that is bundled with the FIS package.

Encryption settings

The following table lists the encryption settings that apply to all remote file servers:

Property	Description
Key Store Location	Location of the key store that stores the private key and associated certificates that the client uses to authenticate communications with the File Integration Service. Include path and file name.
Key Store Password	Password to access the key store.
Key Store Type	Type of the private key store. Use one of the following values: - JKS - PKCS12 Default is JKS
Key Alias	Key alias or certificate for the private key used to sign the MDN.
Trust Store Location	The path to the trust store file that the File Integration Service uses for HTTPS communications.
Trust Store Password	Password to access the trust store.
Trust Store Type	Type of the trust store. Use one of the following values: - JKS - PKCS12 Default is JKS

INDEX