**Sterling B2B Integrator** and **Sterling File Gateway**

**Sterling Commerce**

<https://en.wikipedia.org/wiki/Sterling_Commerce>

What is **IBM Sterling File Gateway**?

Sterling File Gateway is an application for transferring files between partners by using different protocols, conventions for naming files, and file formats. Sterling File Gateway uses the Sterling B2B foundation, which includes IBM® Sterling B2B Integrator, Sterling Standards, and the Sterling platform. The capabilities that are delivered are similar to the features found in Advanced File Transfer and IBM Sterling Connect:Enterprise® for UNIX, plus new functionality. Use Sterling File Gateway for movement of large and high-volume file transfers, with end-to-end visibility of file movement in a process-oriented and highly-scalable framework. This framework alleviates file transfer challenges, such as protocol and file brokering, automation, and data security.

Sterling File Gateway supports integration with:

Sterling B2B Integrator Mailbox

IBM Sterling Control Center

IBM Sterling Secure Proxy

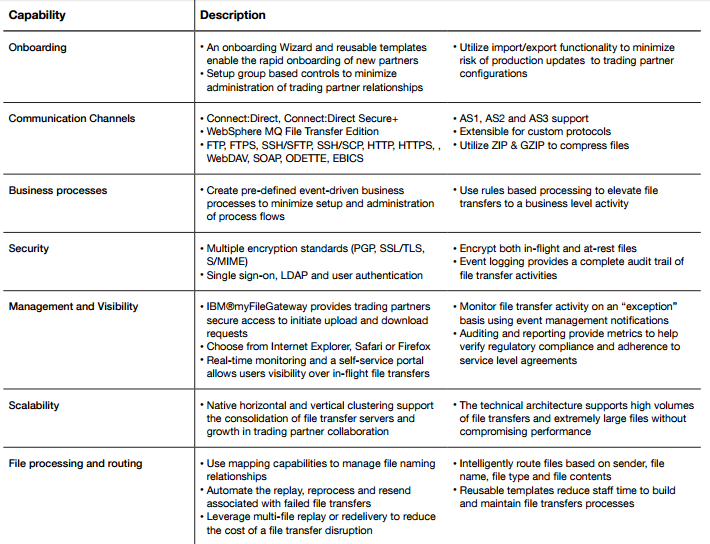
IBM Sterling Connect: Direct® for UNIX server products

IBM Sterling Connect: Direct  
IBM WebSphere® MQ File Transfer Edition

Sterling File Gateway, which is delivered on the Sterling B2B Integrator platform with a unique application URL, provides single sign-on access to the Sterling B2B Integrator administrative console through menu selection.

What are the **features of Sterling File Gateway**?

1. **File/File name Transformations** – Mapping of input to output file names; system-wide, group, and partner-specific policies; common file processing tasks such as compression/decompression, PGP encryption/decryption, and signing.
2. **File Transfer Visibility** – Events are recorded for monitoring and reporting; detailed tracking for input-output file structure processing and dynamic route determination; ability to view and filter Sterling File Gateway data flows for all users.
3. **Replay/Redeliver** – One click replay/redeliver capability that allows users to reprocess one or multiple transmissions from the beginning or to resend one or multiple processed files to specific delivery destinations.
4. **Notifications** – Partners and operators can subscribe to be notified about events by email.
5. **Predefined business processes** – Define common behaviors in file-transfer scenarios, reducing the need for customization.
6. **Extensibility** – Custom event codes, protocols, facts, and consumer identification policies can be added to support unique scenarios.
7. **Broad Communications Protocol Support** – FTP, FTP/S, SSH/SFTP, SSH/SCP, IBM® Sterling Connect:Direct®, and IBM WebSphere® MQ File Transfer Edition are supported upon installation, and additional protocols (such as AS2, AS3, or Odette FTP) may be configured through use of the extensibility feature.
8. **Partner Interface** (myFileGateway) – Web browser-based interface that enables partners to upload/download files, subscribe to notifications of events, manage passwords, search and view file transfer activity, and generate reports about file transfer activity.
9. **Flexible Mailbox Structures** – Ability to specify mailbox structures that leverage pattern matching policies and specify attributes that must be true of all partners or a subset of partners.
10. **Dynamic Routing** – Consumer derived at run-time, either through mailbox structure, file name, business process-derived consumer name, or map-derived consumer name.
11. **Partner On boarding** – Easy-to-use graphical user interface to onboard partners and configure the various combinations of communication protocols to enable Sterling File Gateway operations.



How **Sterling B2B Integrator** and **Sterling File Gateway** work together?

Sterling File Gateway utilizes the Sterling B2B foundation, which includes Sterling B2B Integrator, Sterling Standards, and the Sterling platform, to deliver capabilities similar to those found in Sterling Advanced File Transfer and Sterling Connect:Enterprise® for UNIX, while adding new features and functionality. Within Sterling File Gateway, Sterling B2B Integrator is known as the B2B Console, and is accessed from the Tools menu. Administrative functions such as creating and managing user accounts, permission groups, and security keys for Sterling File Gateway are handled in Sterling B2B Integrator.

Sterling File Gateway utilizes the communication adapters of Sterling B2B Integrator, which include the following:

* FTP Server adapter
* FTP Client adapter
* SFTP Server adapter
* SFTP Client adapter
* HTTP Server adapter
* HTTP Client adapter
* Connect:Direct Server adapter
* Command Line adapter 2 (for PGP)

**Types of Users**

There are several types of users, referred to as personas, which can be created using Sterling File Gateway. They are:

* **System Administrator** - installs and maintains system software. Handles functions that require access to Sterling Integrator. Creates initial administrative users. Configures services and adapters for sending and receiving files. Manages extensibility features. Moves resources and configurations between systems.
* **Integration Architect** - creates partner groups, communities, routing channel templates, producer file structures, and consumer file structures.
* **Route Provisioner** - creates and manages partners, group membership, and routing channels.
* **Operator** - monitors system status and file activity. Troubleshoots problems with Partner activity, generates reports, uses logs, and subscribes for their own notifications. Can create, read (view), update and delete communities and partners.
* **Partner User** - uploads and downloads files from the myFileGateway partner interface, or sends and receives files through one of the communications protocols. Views their activity, subscribes for their notifications about their activities, manages their password, and generates reports about their activities. Are producers and consumers.

What is **Web application myFileGateway**?

Partners send and retrieve files from the Web application myFileGateway. To log in to myFileGateway, a valid user account is required. This user account is created when a Route Provisioner on boards the partner. From within myFileGateway, partners can:

* Upload or download files.
* Search for routes they participated in.
* View recent activity and status for file transfers they participated in.
* Generate reports for activity they participated in.
* Change their password.
* Subscribe to notifications.

What are the **Advantages of IBM Sterling B2B Integrator**?

Sterling B2B Integrator is designed to be configured strategically around the specific processes crucial to your company's success. Its systematic and managed approach supports your integration requirements for both transaction-oriented and batch processes, and works with both pre-existing Electronic Data Interchange (EDI) protocols and Internet-based XML protocols. You can enable your existing systems to integrate past, present, and future technologies and practices

**Terminology**

This section explains of the Sterling B2B Integrator specific terminology that we use in B2B world.

***Business processes***

Sterling B2B Integrator’s approach to integration is centered on business process management. A business process is a goal-driven, ordered flow of activities that accomplishes a business objective. Using Sterling B2B Integrator, organizations can integrate the activities that make up their business processes. Common examples of such activities include:

* XML, EDI, and proprietary file translation, transformation, and filtering
* Human interaction through a browser interface (such as reviewing and approving data)
* Content-based routing of messages
* Data publishing
* Extended process models that integrate the execution of a B2B protocol, such as AS2, with enterprise system integration, such as invoking the SAP adapter.

Organizations can create and coordinate activities into business process models, extending the automation of processes and increasing the value of e-business operations. An example of a simple business process is the fire-and-forget publishing of a business event to a group of interested participants. The steps that comprise the process trigger the process and the subsequent publishing of the event to the interested parties.

A complex business process might require multiple interactions among many applications in a start-and-stop, request-response mode, along with human interaction, occurring over a long period of time.

***Services and adapters***

A service is a set of instructions that the Business Process Engine uses to perform an activity in a business process. Adapters are services that connect the Business Process Engine and other system components to dissimilar systems and applications outside of the Sterling B2B Integrator environment. Business processes can send, pause, retrieve, and fully interact with adapters.

Services and adapters are reusable. Organizations can include them in multiple business process models. Adapters either receive input from or provide output to outside systems. Adapters provide noninvasive integration with enterprise resource planning (ERP), supply chain management (SCM), customer relationship management (CRM), other packaged applications, enterprise applications, communication protocols, messaging solutions such as IBM WebSphere, and databases.

The following process summarizes the way adapters work within a business process:

1. The business process progresses to the application adapter step.
2. The adapter calls a third-party application to perform an activity.
3. The system records the modified state (context) of the process and related data.
4. The business process continues to the next service or adapter.

**Improved FTP security**

Allowing for **encryption of data**, **managed file transfer** software keeps user IDs and passwords secured while in flight. Many offerings of managed file transfer software also include a **checksum** feature that allows a business to guarantee that the data being transferred is in its original form and has not been corrupted or tampered with. Additionally, managed file transfer software allows companies to utilize non-repudiation that allows trading partners to be notified when the transfer has been received successfully, subsequently reducing the risk for conflicts or litigation. For file transfer, namely multi-enterprise file transfers, an organization cannot dispute that they received a file whenever a message disposition notification is given by specific protocols saying that the transfer is complete. This message disposition notification is a digital signature that the receiver did receive the transfer.

**What is Managed File Transfer (MFT)?**

Even with the availability of technologies such as web services and Web 2.0, file transfer still remains one of the most common ways for enterprises to exchange data. As more data is exchanged intra-enterprise and multi-enterprise, the need for more efficient means of moving files has become prevalent. This has brought about the concept of **managed file transfer**. Typically, managed file transfer refers to software solutions that allow for secure transfer of data from one location to another. A managed file transfer system introduces control, management, and auditability to address problems that arise when file transfers are used to integrate or connect business systems in the organization. Generally, managed file transfer solutions have features such as reporting the completion status of file transfers, auditing, global visibility, automation, and non-repudiation. These features are specifically designed to overcome the common challenges surrounding the enterprise use of FTP.

According to Gartner “Managed file transfer software and services enable users to manage and monitor file transfers within and between organizations.”

In this definition Gartner uses “manage” and “monitor” to highlight and explain the key differences between MFT and FTP.

**Manage** – means to manage all file transfers using one interface (one place) across all business units, operations, systems, applications, partners, etc.

**Monitor** – means to monitor all file transfers in one centralized location which in turn means better governance, compliance and reduced IT costs

Managed file transfer addresses the need that organizations have to configure, track, and audit file transfer activity consistently. Typically, an organization using managed file transfer has the following needs:

* **Auditability**: File transfer activity must be logged so that administrators can determine where each file is sent and when the transfer occurred. The transfer log needs to be centrally accessible.
* **Security**: File transfer requests require acceptance from authorized people or application systems.
* **Recoverability and reliability:** Network or other errors that interrupt a transfer must not cause the transfer to be abandoned or partial files to be received.
* **Platform connectivity:** File transfers must span multiple platforms.

The ideal managed file transfer architecture contains automation, centralized and event-based logging, centralized monitoring, centralized setup and management, and a documented and standardized transport. The infrastructure contains:

* The ability to secure files in transit
* Flexibility in file transfers
* Granular user control over file transfers
* Monitoring of a file’s journey
* Auditing of transfers
* Visibility of transfers
* Checkpoint restart of transfers

Sterling B2B Integrator 5.2 System Requirements?

System requirements for IBM® Sterling B2B Integrator vary with your business needs and system environment. Contact your Sterling B2B Integrator sales representative to help you evaluate performance and system usage requirements.

Contributing factors include (but are not limited to) the following:

1. Number of transactions processed.
2. Amount of data being transferred.
3. Whether you run Sterling B2B Integrator with or without perimeter servers.
4. Whether your environment is clustered (multiple node) or non-clustered (single node).

The following sections list the platforms and databases that are supported by Sterling B2B Integrator:

1. Platforms
2. Databases

The following sections list minimum system requirements, and other information, needed to install and run Sterling B2B Integrator on particular platforms:

1. IPv6 Capabilities
2. UNIX/Linux Requirements
3. Windows Requirements
4. iSeries Requirements

The following sections list additional information that is needed to install and run Sterling B2B Integrator: v JCE Requirements (All Platforms)

1. JDBC Driver Requirements (All Databases)
2. Perimeter Server Requirements (UNIX/Linux and Windows)
3. Internet Browser and Plugin Requirements (All Platforms)
4. Map Editor and Graphical Process Modeler System Requirements
5. Supported Third Party Software

What's New in Sterling B2B Integrator?

* Sterling B2B Integrator 5.2 Enhancements
* Soft Stop of Sterling B2B Integrator

Sterling B2B Integrator 5.2 now has the ability to gracefully stop the system—allowing existing processes the opportunity to complete, be transferred to other cluster nodes or be saved for resumption after restart. This saves time by eliminating the need to manually examine and resume processes after a restart.

The soft stop functionality combined with a rolling restart of nodes will allow for minimal interruption of processing. You can initiate the soft stop command from either the UI or from the command line.

The soft stop UI provides the ability to interactively step through the shutdown process allowing for:

1. The transfer of a running business processes to other cluster nodes or to the database for recovery
2. The ability to control the completion of queued business processes on the local node
3. The ability to show the status of adapter activity and open sessions Performance Tuning Utility

Sterling B2B Integrator 5.2 includes an updated utility that calculates the tuning parameter values for you. You can use the Performance Tuning utility to tune and configure Sterling B2B Integrator according to your needs.

Queue settings can be changed, as well as memory allocations, JVM settings, and pool settings. Additionally, future Sterling B2B Integrator patches will not overwrite the performance tuning changes made by the Performance Tuning utility.

Sterling B2B Integrator License Files

You no longer need to contact IBM to acquire a license file prior to product installation. Product functionality is grouped into large offering areas. During installation, you must select the product offerings applicable to your purchase and a bundled license file will be used.

Sterling Standards Library 8.0

Applying Sterling B2B Integrator, Release 5.2 automatically includes Sterling Standards Library 8.0. Your specific standards implementation will depend upon the terms of your licensing agreement.

Sterling Standards Library version 8.0 enables support for the following X12 5010 HIPAA transactions:

* v 5010 220A1 834
* v 5010 221A1 835
* v 5010 222A1 837
* v 5010 223A2 837
* v 5010 224A2 837
* v 5010 279A1 270
* v 5010 279A1 271

**Sterling B2B Integrator for Financial Services** Overview?

Sterling B2B Integrator for Financial Services is the solution that enables banks, broker-dealers, investment managers, and market infrastructures in payments, securities, treasury and trade to optimize financial sector process integration—both internally and with external enterprises and communities—for secure end-to-end management of financial data exchange.

This product leverages components of Sterling B2B Integrator to enable file transfer and translation capabilities using financial-industry transport types and messaging formats. Enhanced reporting and notification tools provide improved insight into business processes, furthering your goal to create a sustainable competitive advantage. Available components include pre-built support for financial standards and protocols, services, adapters, code lists, pre-loaded DTDs and schemas in the Map Editor, and tools such as Reporting Services and the SWIFT Editor.

With Sterling B2B Integrator for Financial Services, you can integrate existing systems with a gateway solution offering visibility and simplified error/exceptions management, including routing of files and messages into legacy systems. This complete and streamlined automation of processes can help you reduce costs, increase revenue, and improve customer satisfaction while leveraging Sterling B2B Integrator security features to provide secure, non-repudiated exchange of B2B information.

Depending on your needs, Sterling B2B Integrator for Financial Services can be a simple file transfer solution for financial documents, a translation engine supporting financial standards and those of your back office systems, or a complex full gateway solution involving all types of file transfer, intelligent routing, translation, and transmission activities. Your solution can be configured to be fully convertible between payments networks, platform agnostic, and deployed behind the corporate firewall. If needed, IBM® Support can help you customize Sterling B2B Integrator for Financial Services to enable full payload inspection and customized visibility into documents processed. Sterling B2B Integrator for Financial Services is highly scalable to suit your evolving needs.

Sterling B2B Integrator for Financial Services makes process continuity of business finance part of your organization's integrated value chain, shared by the business partners and financial institutions that make up your B2B communities.

Sterling B2B Integrator for Financial Services Supported Standards and Protocols?

The diversity of communications systems and standards makes it difficult to respond to customer demands for better and more comprehensive service. Sterling B2B Integrator for Financial Services' built-in support for financial standards reduces the information technology costs involved in custom coding and enables you to more cost-effectively integrate disparate systems to overcome information silos. Pre-defined financial standards are automatically loaded into the Sterling B2B Integrator Map Editor graphical mapping tool, including code lists. With Sterling B2B Integrator for Financial Services, you can translate and move data among many different environments.

The following financial services standards are supported, but are not limited to:

1. FIX, FIXML, FpML, IFX
2. ISO 8589, 20022, and 150222, including TWIST
3. XBRL
4. NACHA ACH
5. SWIFTNet FIN MT messages (2005 & 2006) and SWIFTNet MX messages (including those specific to SWIFT Solutions)
6. TARGET2
7. EBA STEP2

Sterling B2B Integrator for Financial Services supports batch and real-time protocols, including:

* FTP and FTP/S;
* SSH/SFTP;
* Sterling Connect:Direct®;
* HTTP/s;
* dial-up communications;
* SMTP;
* SOAP,
* MQ,
* JMS, and MSMQ messaging;
* AS2, and
* RosettaNet.

In addition to the full suite of available Sterling B2B Integrator protocol support, Sterling B2B Integrator for Financial Services also supports the SWIFTNet InterAct and FileAct protocols for financial services communications.

GPM Terminology

The following terms and definitions will assist you in understanding the GPM.

1. GPM – Web-deployed graphical interface tool you use with Sterling B2B Integrator to create and modify business processes. The GPM converts your graphical business process models into BPML source code, saving you the effort of writing code.

In the GPM, you construct your business process models, coordinating the flow of activities in a graphical depiction of the ordered steps. The GPM provides icons representing the services, adapters and BPML instructions that make up your process models.

In addition, you configure related service parameters through the GPM, create rules and conditions within your process models, and you can validate the process models and check them in to Sterling B2B Integrator from within the GPM.

The GPM recognizes BPML code written in a text editor. Therefore, in the GPM, you can open a .bpml file created in a text editor and view its graphical representation, and toggle between BPML and graphic view.

While the GPM is an included feature of Sterling B2B Integrator, it does not automatically install with Sterling B2B Integrator, because it operates as a separate, Web-deployed application. You must install the GPM on your client computer after you have installed Sterling B2B Integrator.

1. BPML – An XML-based language used to describe (model) and run business processes.
2. Java Web Start – The tool that Sterling B2B Integrator uses to ensure proper deployment of the GPM. Each time you open the GPM application, Java Web Start checks the Web server to determine whether a new version of the GPM is available. When a new version is available, Java Web Start automatically updates the files on the client computer and opens the GPM.

What is mean by Web Extensions? How do you use it in SI?

The processes that support your business usually include both human activities and computer-assisted automation. Yet, historically, integration technologies have targeted only the automated aspects of an integration project, such as low-level messaging, file transfer, or EDI. With Sterling B2B Integrator Web Extensions, you can build the human interaction points into your business process models.

Web Extensions uses advanced XML standards so that you can easily integrate your Web Extensions applications (forms) into your business process models and use Java Server Pages (JSP) to create forms pages.

Technically, Web Extensions is a collection of Sterling B2B Integrator services called Human Interaction services. The Graphical Process Modeler (GPM) depicts these services as icons in the user interface. You include these icons in your business process models by selecting the appropriate service wherever human interaction must occur.

Web Extensions can be used for:

* Supporting human interaction steps within otherwise automated processes, such as:
* Advanced exception or approval processing before data automatically passes into enterprise systems or out to business partners
* Expense reporting
* Creating e-commerce Web sites such as an online store with shopping cart functionality.
* Improving partner and customer collaboration through secure selective data sharing by easily deploying partner self-service applications (such as payment, order, and shipment status forms).
* Enabling small trading partners to interact with your business processes by configuring data transformation from the online forms to EDI or XML.

What is EDIINT?

EDI over the Internet (EDIINT) is a working group of the Internet Engineering Task Force (IETF). Formed in February of 1996, EDIINT was chartered by the IETF to create a set of secure protocols for sending EDI data over the Internet. The two EDIINT standards that have been certified are AS1 and AS2.

How Does AS2 Work?

AS2 provides an Internet solution for securely exchanging EDI over the Internet using Multipurpose Internet Mail Extensions (MIME) and the hypertext transmission protocol (HTTP) instead of the simple mail transport protocol (SMTP) as the transport protocol. AS2 specifies the means to connect, deliver, validate, and reply to (receipt) data in a secure and reliable way. AS2 does not concern itself with the content of the EDI document, only the transport.

AS2 essentially creates a wrapper around EDI flat files that enables sending them over the Internet, instead of using a dial-up connection to a value-added network (VAN). AS2 is a real-time technology that provides security and encryption around the HTTP packets.

What are the benefits of Using AS2?

AS2 provides faster, almost instantaneous data transfers directly to your network and reduces the points of failure in data transmissions. Using AS2 eliminates day-to-day value-added network (VAN) charges and long distance dial-ups. AS2 also provides increased reliability and sped, improving supply-chain efficiency. Listed below are some of the main benefits of using AS2:

* 24x7 availability
* Designed to push data securely and reliably over the Internet
* Fast and reliable connectivity
* Encryption ensures that only the sender and receiver can view the data
* Digital signatures ensure authentication
* AS2 detects if the document was altered during transmission
* Non-repudiation of receipt confirms that the intended party received the data
* Faster turn-around time for business processes

What is required to Exchange Data Using AS2?

* A dedicated persistent Internet connection
* A web server with your EDIINT software

What is the Risk for Using AS2?

There is no more risk involved with transactions over AS2 then there would be with any form of normal e-Business transactions. If there is any risk with AS2, it is far outweighed by the cost savings implicit in its operation.

What is PGP?

Pretty Good Privacy was originally developed by Phillip Zimmerman to provide a means of secure communication in an insecure electronic environment. “Pretty Good” is an understatement – the framework it is based on, PKI (Public Key Infrastructure) and its encryption standards (it can use Diffie-Helman or RSA algorithms of varying strengths), have been subjected to rigorous cryptanalysis.

PGP has since grown into a more versatile application under the direction of its current owner, Network Associates (www.nai.com). Until the most recent release PGP has been completely open source, allowing anyone to review the code and suggest improvements.

How does PGP work?

When someone starts using PGP, they generate a Key Pair. These are really just text files that look like gibberish to a human. The keys can be created at various levels of strength – 512, 1024, or 2048 bit strengths are used. The higher the number, the stronger the encryption value of the key. One key of the pair is the Private Key – this key should always be kept safe and never given to anyone. The other key is the public key – this key should be given to as many people as possible.

What are the uses of PGP?

The most commonly used aspect of PGP is the signing and encryption of email or files. “Signing” a document is a way of verifying the integrity of the original work.

The method is as follows:

1. Make a digest or “hash” of the file or email. A hash is an algorithm that produces (theoretically) a unique output (the hash) from a given input (the message).
2. Add the hash to the end of the message.
3. When someone wants to verify that the message has not been modified, they run the hash algorithm on the message and compare it to the hash at the end of the message. If the signatures match, the message has not been altered.

How does Encryption works?

Encryption is a method of changing plaintext (text that is readable by humans) into cipher text (text that is meaningless to humans). There are many different ways of encryption, some stronger than others. Two main categories of encryption are symmetric and asymmetric.

In symmetric cryptography, the same key that encrypts a file also decrypts it. In asymmetric cryptography, which is what PGP uses, one key (the public key) encrypts the file, and the other key (the private key) decrypts it. So, if user A wants to send an encrypted message to user B, user A would first obtain user B’s public key.

This is possible because public keys are meant to be widely distributed. Then user A encrypts the message using user B’s public key. The encrypted message can now only be decrypted with B’s private key, which only he possesses. Not even user A, who wrote the message, can decrypt what he has encrypted, because he does not possess user B’s private key. This ensures that the message is unreadable by anyone other than user A. Encryption and signing are often combined.

In this scenario, user A would use user B’s public key to encrypt the message, then use his own private key to sign the message. This will ensure that no one but user B can read the message, and when user B receives it, he can be assured that the message was not altered. To read the message, userB would first use user A’s public key to verify that the signature matches. Then user B would use his private key to decrypt the message that user A wrote.

**About Partners**

Sterling File Gateway enables the exchange of files between partners through routing channels that are set up to connect specific partners. Partners that send files into Sterling File Gateway are referred to as producers, and those that retrieve files are referred to as consumers. **A partner can be a producer, a consumer, or both** from an operational standpoint. Route Provisioners create, edit, and delete partners. Before partners can be created, though, it is important that the System Administrator configure any communications adapters the partners may need to use so that permissions are set correctly.

Each partner is associated with exactly one community. If consumer partners will use SFTP, create the remote SSH Profile before creating the partners. If partners will use PGP, perform the following before creating the partners:

• Install PGP server

• Start CLA2Client.jar process

• Modify PGPCmdline Service in B2B Console

• Create a PGP Profile named AFTPGP Profile in the B2B Console

When a partner is created in Sterling File Gateway, the following objects are created to support the partner:

• A Sterling Integrator user account

• A Sterling Integrator mailbox using the partner name

• A Sterling Integrator virtual root for the user and mailbox

The user account is automatically assigned to the File Gateway Partners Users group, or the custom group which is set as default group in filegateway\_ui.properties file. The user group users are assigned to have specific permissions that are granted to the users. See About Permissions.

If the partners will be authenticated outside of Sterling File Gateway, the System Administrator must establish your authentication server and Authentication Management System before you create the partners. Do not remove or reorder the authentication servers in the customer\_overrides.properties file after creating partners associated with them.

To apply a password policy other than the default password policy provided in Sterling Integrator, the System Administrator must create the new policy in Sterling Integrator before you create the partners. Select the new policy from the list when creating the partners.

|  |  |
| --- | --- |
| Field | Description |
| Partner Name | A unique name with a maximum of 100 characters. Spaces are allowed. Two partners cannot have the same Partner Name. You cannot modify the Partner Name after the partner is created. |
| Partner Code | The Partner Code field is optional. If not specified, a Partner Code is generated based on the Partner Name, up to the first 24 alphanumeric characters, when the partner is created.  A maximum of 24 alphanumeric characters. Only characters from the US-ASCII alphabet, numbers, and special characters of underscore, dash and period are Partner Code permitted. Two partners cannot have the same Partner Code. You cannot modify the Partner Code after the partner is created. |
| Address | Address of the Partner. Optional. |
| City | City of the Partner. Optional. |
| State | State or province the Partner operates in. Optional. |
| Zip or Postal Code | Postal code for the Partner. Optional. |
| Telephone Number | Phone contact number for the Partner. Required. |
| Country | Select from the list. Required. Default is UNITED STATES. |
| Time Zone | Select from the list. Required. Default is (GMT-05:00) Eastern Time (US & Canada). |
| Email Address | E-mail address of the Partner. Required. |

**About Routing Channels**

Routing channels match incoming producer files to the appropriate consumer, then transform the file and file name according to the policies of the consumer. Route Provisioners create routing channels. Before routing channels can be created, the Integration Architect must have already created a routing channel template and the Route Provisioner must have created the producer and consumer Partners.

For a static routing channel, the consumer is explicitly identified during the configuration, and there is only one consumer. For a dynamic routing channel, no consumer is explicitly specified. The routing channel permits routing to any consumer belonging to the consumer group specified in the routing channel template.

You cannot create duplicate routing channels. A routing channel using the same routing channel template, producer, and consumer is a duplicate. At least one parameter must be different, with one exception. When using a static routing channel template where the ConsumerName or ConsumerCode fact is specified for the producer file structure in the outer file layer, or in the second file layer for ZIP files, you can use the same static routing channel template for multiple consumers.

**The File Transfer Protocol (FTP)**

It is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.  FTP server works on port 21.

Parameters required for FTP Get or PUT:

Remote Hostname / IP Address

Username

Password

Path

While transferring data over the network, four data representations can be used:

**ASCII mode:** Used for text. Data is converted, if needed, from the sending host's character representation to "8-bit ASCII" before transmission, and (again, if necessary) to the receiving host's character representation. As a consequence, this mode is inappropriate for files that contain data other than plain text.

**Binary mode:** The sending machine sends each file byte for byte, and the recipient stores the byte stream as it receives it. (Image mode support has been recommended for all implementations of FTP).

**Web browser support**

Most common web browsers can retrieve files hosted on FTP servers. FTP URL syntax is

**ftp://[user[:password]@]host[:port]/url-path** (The bracketed parts are optional).

**SSH File Transfer Protocol / Secure File Transfer Protocol or SFTP**

It is a network protocol that provides file access, file transfer, and file management over any reliable data stream. It was designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH) version 2.0 to provide secure file transfer capabilities. The SFTP protocol allows for a range of operations on remote files which make it more like a remote file system protocol. An SFTP client's extra capabilities include resuming interrupted transfers, directory listings, and remote file removal.

The basic elements of configuring an SFTP connection are:

**Server Validation:** Ensuring the SSH server is validated is an important issue in SFTP. By default an attempt will be made to validate the server using the client's local store of server public keys. Typically, the server's public key is stored in either a file containing that single key, or in a file often called **known\_hosts** which can contain a number of public keys for different servers. When the client connects to the server, the server's public key is returned and compared with the available public keys stored in the client.

**Client Authentication:** Clients are authenticated by either username and password, or private key and private key passphrase. In the first case, the user requires an account on the server that is set up for SFTP access. In the second case, the user's public key must be registered with the server (typically by copying it into an **authorized\_keys** file on the server), and the user's private key must be loaded by the client. A third method known as keyboard-interactive authentication is also supported.

**Client Authentication**

The most commonly used forms of client authentication are by username/password or by public/private keys. Note that some SFTP servers are set up to disallow password authentication by default, in which case username/password connection attempts will fail unless password authentication is enabled in the server configuration file.

SSH implementations use a file called known\_hosts which is loaded by clients to validate servers. Typically, this file is generated when a command-line client first connects to a server - a prompt asks if the server should be added to the list of known hosts.

The known\_hosts file contains a list of approved servers and their public keys.

A single line in a known\_hosts file looks like this:

edtmobile,10.0.0.3 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAt60CtjBMxiOOqgqfFtKZHY3g99uZpuh5E143FTO4dw+EHWNKemoWq59FMFMIZfSLyUpWmsjVT3PP1bczOXP1OSn967kxLB/w7Xr84B1ZrTLwuR/ilq73HpgO7A8pdEJN7ybprzhs5CBEgaLQo2pOxfqRYyc8TO2ADnZ1WwtjW48=

The **first field is** the **hostname**, i.e. the SSH server. The IP address is also listed - a number of comma separated hostnames and IP addresses can be listed. **The second field is** the applicable **public key algorithm** -"ssh-rsa" (for RSA key pairs) or "ssh-dss" (for DSA key pairs). **The third field is** the **public key** encoded using base 64.

The known\_hosts file normally consists of multiple lines, one for each of the hosts that the client may wish to connect to. It is quite typical for a host to have entries in two lines, so that both RSA and DSA public keys can be listed. Note that the server may send back an RSA key or a DSA key. If known\_hosts only contains a DSA key for the host, and an RSA key is returned, server validation will fail. The server can be forced to send back a particular type of key

Client authentication can be either by password, by public/private keys, or by keyboard-interactive authentication.

**Password authentication** is generally the easiest to try first, although some SFTP servers are set up to disallow password authentication, in which case the connection attempt will fail unless password authentication is enabled in the server configuration file. The user name and password should be that of the SSH user that the client is logging in as.

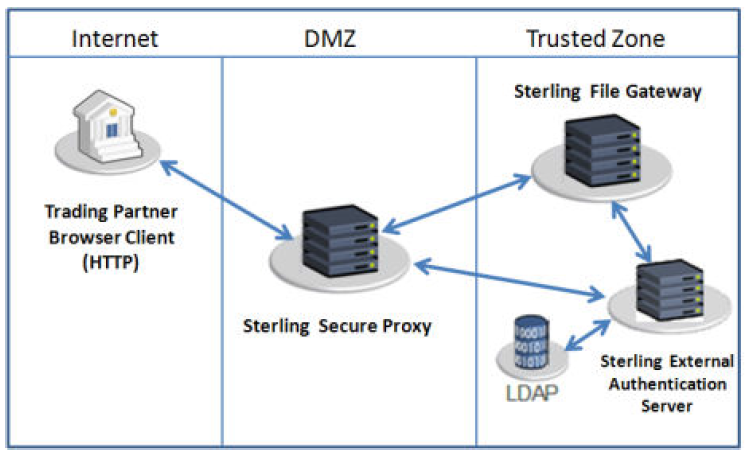
**Public key authentication**, here SSH clients and servers authenticate each other via public/private key pairs. Each must have access to their own private key, and they must have access to each other's public key (unless server validation is disabled). You should ensure that the server's public keys are loaded by the client

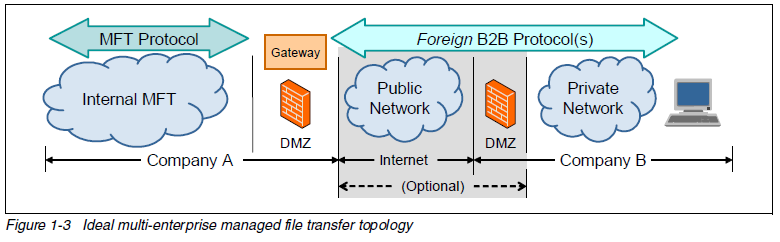
The client's public key must be registered with the SSH server, typically by copying it into the server's authorized\_keys file. There are no formal standards for SSH private key files, however three main formats are in common use.

|  |  |
| --- | --- |
| **Private Key Type** | **Start of key** |
| OpenSSH | -----BEGIN DSA PRIVATE KEY----- |
| SSH.com | ---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ---- |
| PuTTY | PuTTY-User-Key-File-2: |

The format is automatically detected when the file is loaded.

**Flow of data**





**Sterling Connect:Direct**

Sterling Connect:Direct is a point-to-point (peer-to-peer), file-based integration solution that is designed for around-the-clock, unattended operation. It provides assured delivery and high-volume, secure data exchange within and between enterprises. It is designed to move files that contain any type of data (for example text, EDI, binary, digital content, or image) across multiple platforms, disparate file systems, and disparate media, while maintaining high performance levels and throughput. Many industries throughout the world use Sterling Connect:Direct to move large volumes of data and to connect to remote offices. Unlike FTP implementations, Sterling Connect:Direct eliminates the need for manual intervention in data delivery, improving personnel productivity and the reliability of business processes.

Sterling Connect:Direct provides the following **benefits**:

**Predictability** – Files can be sent using assured delivery through automated scheduling, checkpoint restart, and automatic recovery or retry. If a file transfer is interrupted, Sterling Connect:Direct attempts to resume the transfer at a predefined interval for a configured duration of time. The activity and statistics that are associated with the file transfer are logged to provide an audit trail that accounts for all actions taken during a file transmission.

**Security** – The Sterling Connect:Direct proprietary protocol and user authentication through user proxies allows customer information to remain private during the file transfer. Featuring security options to control data access, network access, or access to system resources, Sterling Connect:Direct can interface with operating system and vendor-supplied access control and security software. The optional implementation of IBM Sterling Connect:Direct Secure Plus gives organizations the ability to use a comprehensive cryptographic solution for strong mutual authentication using X.509 certificates, SSL and TLS data encryption, and data integrity checking.

**Performance** – Sterling Connect:Direct can handle demanding file transfer workloads, including high volumes of small files and transmission of large, terabyte size files. Additionally, Sterling Connect:Direct provides optional data compression that is configured for maximum compression or compression based on the optimal use of system resources.

**Sterling Connect:Direct additional features**

The Sterling Connect:Direct Secure Plus option is available to provide a full security solution. This option is a separate, additional licensing option of Sterling Connect:Direct. Sterling Connect:Direct Secure Plus enables organizations to use security protocols to secure data during electronic transmission. The protocols that are available for use include Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Station-to-Station (STS).

The SSL and TLS protocols provide the following levels of security:

**Layer 1: Server authentication** - Server authentication is activated when a trading partner connects to a Connect:Direct server. After the initial handshake, the Connect:Direct server sends its digital certificate to the trading partner. The trading partner checks expiry and for a trusted certificate authority.

**Layer 2: Client authentication** - For client authentication, the trading partner must send its own certificate. When client authentication is enabled, the trading partner’s certificate is requested after the server authentication is complete. The Connect:Direct server verifies that the client certificate is signed by a trusted source before establishing the connection.

**Layer 3: Common certificate verification** - The Sterling Connect:Direct Secure Plus server searches the certificate file that is received during client authentication for a matching certificate.

**File Agent**

Sterling Connect:Direct contains a component called File Agent that provides unattended file management through monitoring and detection capabilities that can enhance automation in Connect:Direct processes.

You can configure Sterling Connect:Direct File Agent to operate in the following ways:

Watch for any file to appear in a watched directory. When the added file is detected, submit a default Connect:Direct process.

Use a watched file event rule or system event rule that is enabled for configuration to override a default Connect:Direct process. When the criteria for a rule is met, the File Agent submits the Connect:Direct process that is associated with that rule.

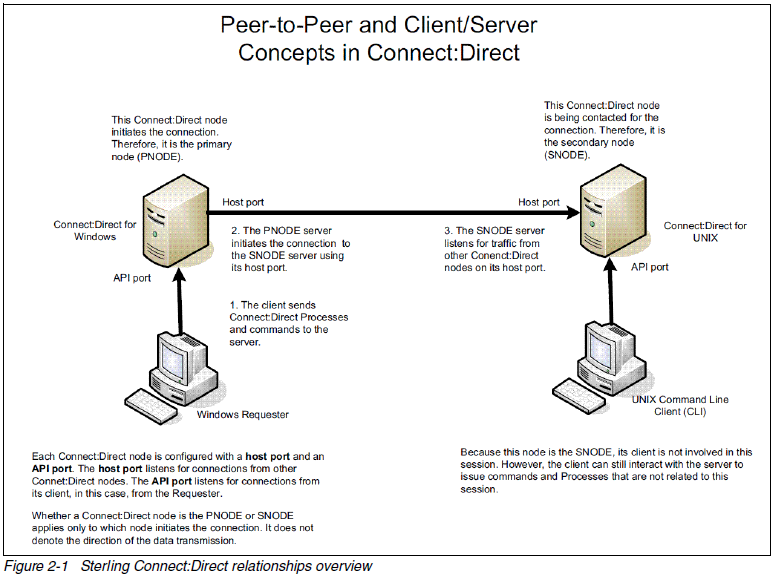
Create File Agent rules based on the following properties:

– A full or partial name of the file is detected in a watched directory. The watched directory can be a local directory on the Connect:Direct server or a network drive.

– The size of the file is detected in a watched directory.

– A system event title or contents exist.

File Agent is distributed with Sterling Connect:Direct for UNIX, Windows, and z/OS®. It can also be downloaded from the Sterling Commerce Customer Center portal.



**Architectural overview**

Sterling Connect:Direct includes the following components that define the local and remote nodes, the users who can access the nodes, and the functions that users can perform:

***Local nodes*** are defined during installation. The definition specifies information such as the operating system, default user ID, TCP/IP address, and port number that is associated with the local node. You can modify these settings after installation.

***Local user authorities*** restrict the ability of each user to perform certain tasks. Sterling Connect:Direct has two types of users:

– Administrators

– General users

Each type of user has a set of default privileges. These default privileges can act as templates to assign to other user authorities and to restrict user access.

***Remote******user******proxies*** contain remote user information for operations that are initiated from a remote Connect:Direct node. The definition identifies a proxy relationship between a user ID at a remote node and a local user ID. This mapping of user IDs allows for remote nodes to submit work without explicitly defining user IDs and passwords in the processes and eliminates the need to share passwords with trading partners.

***Client interfaces*** allow communication with the Connect:Direct server. The client interfaces offered include a web browser interface, a GUI, a command-line interface (CLI), and panels.

**Clustering Solutions**

<https://en.wikipedia.org/wiki/Computer_cluster>

**Capabilities**

Sterling Connect:Direct supports around-the-clock, unattended operations using the following built-in features:

Automation and management

– Schedules jobs on a one-time, recurring, or continuous basis

– Assigns and manage file transfer workloads to internal queues

– Uses event-driven alert notification

– Integrates with back-end systems using process language builds scripts

– Gains programmatic access to transfers from other applications through API and SDK

Assured file delivery

– Checkpoint restart

– Automatic recovery from network interruptions

– Automated alert notifications for success or failure

Security and compliance

– Standard Sterling Connect:Direct

• Interfaces with operating system security for user authentication

• Provides a complete audit trail of data movement through extensive statistics logs

– Sterling Connect:Direct Secure Plus

• User authentication

• X.509 certificates for authentication

• Data encryption (SSL/TLS)

• Certificate and ***Certificate Revocation List (CRL) checking***

• FIPS 140-2 and Common Criteria certification

– Sterling Secure Proxy for the Sterling Connect:Direct protocol

• DMZ-based authentication, session break, and SSL termination

• No file stored in the DMZ

• No inbound ports opened in the firewall

• Validation of the Sterling Connect:Direct protocol

Multiple platform support

– Operating systems support

• z/OS and z/VSE™

• OpenVMS

• i5/OS® (OS/400®)

• UNIX and Linux®

• Windows

• HP NonStop

• Sterling Connect:Direct Select (Java™ version that can run on multiple platforms)

– Network protocols support

• TCP/IP

• SNA

• UDT (UNIX 4.0, z/OS 4.8, Windows 4.5)

Sterling Connect:Direct ensures data delivery to the correct destination within the correct time window, allowing the receiving application to process and act upon it consistently.

***Cyclic redundancy check (CRC) and CLI***

Cyclic redundancy check (CRC)

The CRC checking determines whether data received by Sterling Connect:Direct over the network has been altered during transmission. To allow for **data integrity** during the transmission, CRC is generated for the entire buffer, including the header. ***CRC calculates a short, fixed-length binary sequence for each block of data and for sending or storing them together.*** When a block is read or received, the calculation is repeated. If the new CRC does not match the earlier calculation, the process execution is stopped and restarted from the last checkpoint record. CRC is performed only for TCP/IP processes and cannot be used with the Sterling Connect:Direct Secure Plus Option, which uses its own data integrity checking natively.

CLI

The CLI provides commands to access queues and manage processes. The commands enable users to control the process execution and to view the process status and results. The commands are issued in a native command text format through the Sterling Connect:Direct API.