

Connect:Direct®

Product Overview

Connect:Direct Product Overview

First Edition

(c) Copyright 2009 Sterling Commerce, Inc. All rights reserved.

STERLING COMMERCE SOFTWARE

*****TRADE SECRET NOTICE*****

THE STERLING SECURE PROXY SOFTWARE ("STERLING COMMERCE SOFTWARE") IS THE CONFIDENTIAL AND TRADE SECRET PROPERTY OF STERLING COMMERCE, INC., ITS AFFILIATED COMPANIES OR ITS OR THEIR LICENSORS, AND IS PROVIDED UNDER THE TERMS OF A LICENSE AGREEMENT. NO DUPLICATION OR DISCLOSURE WITHOUT PRIOR WRITTEN PERMISSION. RESTRICTED RIGHTS.

This documentation, the Sterling Commerce Software it describes, and the information and know-how they contain constitute the proprietary, confidential and valuable trade secret information of Sterling Commerce, Inc., its affiliated companies or its or their licensors, and may not be used for any unauthorized purpose, or disclosed to others without the prior written permission of the applicable Sterling Commerce entity. This documentation and the Sterling Commerce Software that it describes have been provided pursuant to a license agreement that contains prohibitions against and/or restrictions on their copying, modification and use. Duplication, in whole or in part, if and when permitted, shall bear this notice and the Sterling Commerce, Inc. copyright notice. As and when provided to any governmental entity, government contractor or subcontractor subject to the FARs, this documentation is provided with RESTRICTED RIGHTS under Title 48 52.227-19. Further, as and when provided to any governmental entity, government contractor or subcontractor subject to DFARs, this documentation and the Sterling Commerce Software it describes are provided pursuant to the customary Sterling Commerce license, as described in Title 48 CFR 227-7202 with respect to commercial software and commercial software documentation.

These terms of use shall be governed by the laws of the State of Ohio, USA, without regard to its conflict of laws provisions. If you are accessing the Sterling Commerce Software under an executed agreement, then nothing in these terms and conditions supersedes or modifies the executed agreement.

Where any of the Sterling Commerce Software or Third Party Software is used, duplicated or disclosed by or to the United States government or a government contractor or subcontractor, it is provided with RESTRICTED RIGHTS as defined in Title 48 CFR 52.227-19 and is subject to the following: Title 48 CFR 2.101, 52.227-19, 227.7201 through 227.7202-4, FAR 52.227-14, and FAR 52.227-19(c)(1-2) and (6/87), and where applicable, the customary Sterling Commerce license, as described in Title 48 CFR 227-7202 with respect to commercial software and commercial software documentation including DFAR 252.227-7013, DFAR 252.227-7014, DFAR 252.227-7015 and DFAR 252.227-7018, all as applicable.

The Sterling Commerce Software and the related documentation are licensed either "AS IS" or with a limited warranty, as described in the Sterling Commerce license agreement. Other than any limited warranties provided, NO OTHER WARRANTY IS EXPRESSED AND NONE SHALL BE IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR USE OR FOR A PARTICULAR PURPOSE. The applicable Sterling Commerce entity reserves the right to revise this publication from time to time and to make changes in the content hereof without the obligation to notify any person or entity of such revisions or changes.

Connect:Direct is a registered trademark of Sterling Commerce. Connect:Enterprise is a registered trademark of Sterling Commerce, U.S. Patent Number 5,734,820. All Third Party Software names are trademarks or registered trademarks of their respective companies. All other brand or product names are trademarks or registered trademarks of their respective companies.

Sterling Commerce, Inc.

4600 Lakehurst Court Dublin, OH 43016-2000 *
614/793-7000

Contents

Chapter 1 About this Guide	5
Chapter 2 What is Connect:Direct?	7
Benefits	7
Features	7
Platforms	8
Connect:Direct Servers and Clients	9
Connect:Direct User Interfaces	10
Chapter 3 Working With Connect:Direct	11
Laying the Foundation	11
Local Node Definition	11
Local User Authorities	11
Remote User Proxies	11
Configuration Settings for the Local Node	12
Remote Node Definitions	12
Netmap Checking	12
Defining the Work Connect:Direct Will Perform	12
Process Language	13
Creating Connect:Direct Processes	14
Managing the Work	15
Tools to Help You Manage Processes	16
Chapter 4 Extending the Capabilities of Connect:Direct	19
Enhanced Security	19
Secure+ Option	19
Sterling External Authentication Server	20
Certificate Wizard Certificate Management Tool	20
Sterling Secure Proxy	20
Unattended File Management with File Agent	21

Enterprise Management with Sterling Control Center	22
Service Level Management.	22
Asset Management	22
Configuration Management.	22
Other Tools/Options to Extend Capabilities.	23
Sterling File Accelerator	23
Windows SDK	23
SNMP Agent	23
Clustering Solutions	23
Additional Connect:Direct Products.	23
Connect:Direct Select	23
Connect:Direct FTP+.	24
Speciality Products	24
SWIFTNet	24

About this Guide

The *Connect:Direct Product Overview* is an introduction to the basic benefits, concepts, and components of Connect:Direct. In addition, the *Connect:Direct Product Overview* provides information about supplemental products that extend the capabilities of Connect:Direct, as well as specialized versions of Connect:Direct.

This guide presents information as generically as possible to capture concepts that are most common to the product. Information about how specific Connect:Direct platforms implement these concepts and others can be found in the documentation for those Connect:Direct products.

What is Connect:Direct?

Connect:Direct is point-to-point (peer-to-peer) file-based integration middleware meant for 24x365 unattended operation, which provides assured delivery, high-volume, and secure data exchange within and between enterprises. It is optimized for high performance and throughput and moves files containing any type of data (text, EDI, binary, digital content, image) across multiple platforms, disparate file systems, and disparate media. It is used by many industries throughout the world to move large volumes of data and for connecting to remote offices.

Benefits

Connect:Direct offers the following benefits:

- ◆ **Predictability**—Assures delivery via automated scheduling, checkpoint restart, and automatic recovery/retry. If a data transmission is interrupted, the transmission tries to restart at a predefined interval for a configured amount of time. All activity and statistics are logged so that there are verifiable audit trails of all actions.
- ◆ **Security**—Ensures customer information stays private through a proprietary protocol and offers basic security through authentication and user proxies. Supports a comprehensive cryptographic solution (Secure+ Option) that provides strong mutual authentication using X.509 certificates, SSL, and TLS data encryption, and data integrity checking. For more information about Secure+ Option and other products that enhance Connect:Direct's security model, see Chapter 4, *Extending the Capabilities of Connect:Direct*.
- ◆ **Performance**—Handles the most demanding loads, from high volumes of small files to terabyte files.

Features

Connect:Direct offers the following features:

- ◆ Provides automation through easy-to-use Process definition and scripting. Multi-step Processes manage data movement as well as pre- and post-processing.
- ◆ Provides automation through scripting, scheduling, and watch directories.

- ◆ Automatically establishes connection to remote server when data is ready for transfer. Automatic session retry re-establishes an interrupted connection; work resumes at the point of failure.
- ◆ Offers flexible security options to control access to data, network, or system resources. Interfaces to operating system and vendor-supplied access control and security software.
- ◆ Supports a comprehensive cryptographic solution (Secure+ Option).
- ◆ Provides checkpoint/restart and automatic session retry.
- ◆ Supports local and remote administration, configuration, and Process management through a browser user interface.
- ◆ Supports non-intrusive integration to existing applications through the Command Line Interface (CLI), which can be used in batch files or scripts. Also supports direct use by applications through APIs.
- ◆ Provides a complete audit trail of data movement through extensive statistics logs.
- ◆ Supports extensive configuration options for flexibility of deployment, management of network resources and optimization of data transfer performance.
- ◆ Provides optional data compression that is configurable for maximum compression or optimal use of system resources.
- ◆ Supports all major file types, media, and record formats across multiple platforms. Data exchange is independent of content.

Platforms

Typically, Connect:Direct is installed on a mainframe, UNIX, or Windows server at a central processing site and is used to communicate with other Connect:Direct sites in the business's network. Connect:Direct offers multi-platform implementations tailored to each of the following operating systems:

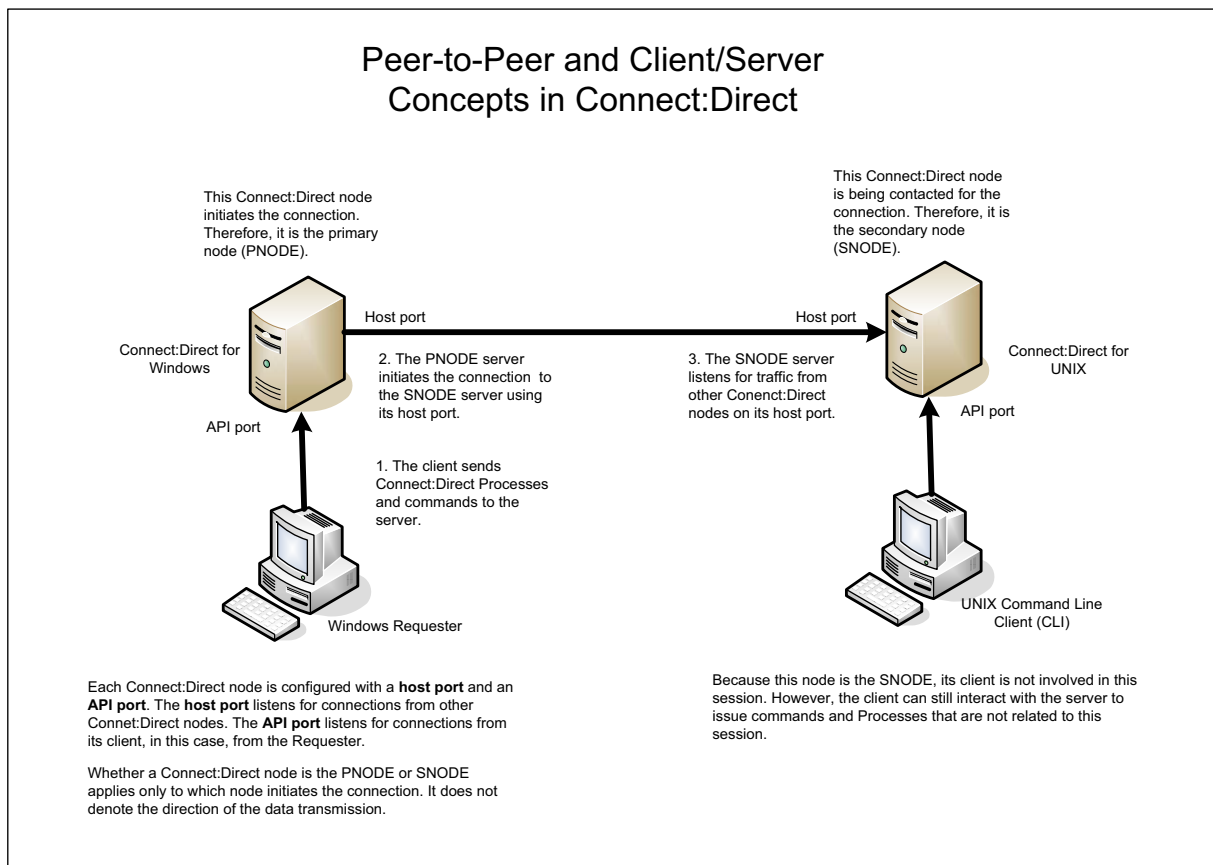
- ◆ z/OS
- ◆ UNIX (Sun, HP UX, AIX, Linux)
- ◆ Windows
- ◆ OpenVMS
- ◆ HP NonStop (Tandem)
- ◆ VM
- ◆ VSE
- ◆ i5/OS (OS/400)

Connect:Direct Servers and Clients

A Connect:Direct client is used to communicate with a Connect:Direct server regarding the work that will be performed. Connect:Direct offers the following types of client interfaces: Web browser interface, graphical user interface (GUI), command line client (CLI), and panels.

Each data transfer involves a local and a remote Connect:Direct server (also referred to as nodes). The two servers work together to perform the work in a peer-to-peer relationship. The server initiating the connection is the primary node (PNODE) for the connection, and the server receiving the connection is the secondary node (SNODE). A Connect:Direct server can manage multiple concurrent connections with other Connect:Direct servers and can act as both a PNODE and an SNODE.

The following figure shows the relationships between Connect:Direct clients and servers during peer-to-peer sessions:



Connect:Direct User Interfaces

The following user interfaces serve as clients to Connect:Direct servers:

- ◆ **Connect:Direct Browser User Interface** allows you to create, submit, and monitor Connect:Direct Processes from an Internet browser, such as Microsoft Internet Explorer or Mozilla Firefox. You can also perform Connect:Direct system administration tasks, such as viewing and changing the network map or initialization parameters (with the appropriate authority level). The specific administration tasks that you can perform depend on the Connect:Direct platform that your browser is signed on to and your security level.

Connect:Direct Browser User Interface can be used as a client for Connect:Direct for Windows, UNIX, z/OS, and HP NonStop servers. It is available for free download from the Sterling Commerce Customer Center site.

- ◆ **Connect:Direct Requester** is a graphical user interface that allows you to attach to Connect:Direct servers to perform file transfers; run remote programs or batch jobs; and create, submit, and monitor Connect:Direct Processes. You can also perform Connect:Direct system administration tasks, such as setting up and maintaining Connect:Direct users and network maps.

Connect:Direct Requester can be used as a client for Connect:Direct for Windows, UNIX, and OpenVMS servers.

- ◆ **Command Line Interface (CLI)** allows you to issue Connect:Direct commands and monitor Connect:Direct Processes. CLIs are available in Connect:Direct for Windows, UNIX, HP NonStop, and OpenVMS.
- ◆ Some platforms contain panel-driven user interfaces, such as the Connect:Direct for z/OS ISPF Interactive User Interface.
- ◆ Application programming interfaces (APIs) in Connect:Direct enable customers to tie-in their applications to Connect:Direct.
- ◆ Sterling Control Center provides a system-wide view of your Connect:Direct servers that enables you to monitor and manage your resources from a central location, including the capability of managing your Connect:Direct server configurations.

Working With Connect:Direct

Before you can work with Connect:Direct, you need to understand the building blocks of information Connect:Direct relies upon to make connections and perform work in your enterprise, as well as the tools that are available to help you manage that work.

Laying the Foundation

To perform work in your enterprise, Connect:Direct relies on building blocks of information that define the local and remote nodes, users who can access those nodes, and the functions they can perform.

Local Node Definition

During installation, you define a local node for Connect:Direct. The local node definition specifies information, such as the operating system, default user ID, TCP/IP address, and port number. After installation, you can change the local node's settings and define remote nodes. In addition to the default user ID you specify for a local node, you can add other users who will access that node.

Local User Authorities

After you define a user ID for each user who has access to the local node, you can restrict the ability of each user to perform certain tasks by defining user authorities for each user ID. For example, you can permit a user to submit a Process but not to monitor or delete Processes.

Connect:Direct has two types of users: administrators and general users, and each type has a set of default privileges. You can use these user templates to assign user authorities and restrict user privileges. Local user authorities provide one type of authentication in Connect:Direct. An alternative method of authentication is available using remote user proxies. For a listing of the default authorities for each type, see the product documentation for your Connect:Direct platform.

Remote User Proxies

User proxy definitions (referred to as secure point of entry on the mainframe) contain remote user information for operations initiated from remote Connect:Direct nodes. These definitions identify a proxy relationship between a user ID at a remote Connect:Direct node and a local user ID. This mapping of remote and local user IDs enables users at remote Connect:Direct nodes to submit work

to the local Connect:Direct node without explicitly defining user IDs and passwords in the Processes, eliminating the need to share passwords with your trading partners. User proxies also define what each user ID can do on the local Connect:Direct node.

Configuration Settings for the Local Node

Initialization parameters determine various Connect:Direct settings that control system operation. The initialization parameters file is created when you install Connect:Direct and can be updated as needed. Some of these settings may be overwritten in the netmap, user authorities, user proxies, and Processes.

Remote Node Definitions

The Network Map, or netmap, is a file created during the Connect:Direct installation that identifies the remote nodes that each local node can communicate with and the communication information needed to establish a connection. You create a remote node entry in the network map for each remote node that the local node communicates with. Each network map entry contains information about the remote node, such as the remote node name, operating system, session characteristics for a protocol, and transfer and protocol information about the available communications paths and their attributes.

Netmap Checking

In addition to defining the remote nodes that communicate with the Connect:Direct node, the network map can be used to perform a security function. Netmap checking verifies that inbound sessions are from a node defined in the network map; if the node is not in the network map, the connection fails.

Defining the Work Connect:Direct Will Perform

The Connect:Direct Process language provides instructions that tell Connect:Direct the work to perform in your enterprise. A Connect:Direct Process contains special statements and parameters that perform data movement and manipulation activities such as:

- ◆ Moving files between different Connect:Direct servers
- ◆ Running jobs, programs, and commands on the Connect:Direct server
- ◆ Starting other Processes
- ◆ Monitoring and controlling Processes
- ◆ Handling processing errors

Processes can be linked to network and application activities, generating a continuous cycle of processing. For example, a network message can trigger a file transfer that is used by another application. As a Process executes and after it completes, audit information is available to analyze and use for future processing.

Processes contain parameters that control Process attributes such as:

- ◆ Scheduling information—Setting a Process to run at a specific day and time. Processing can be scheduled to run automatically at a specified date or interval, without any operator intervention.

- ◆ Integration with existing security systems—Specifying user IDs and passwords within a Process that allow it to work within your existing network security system.
- ◆ Data transmission integrity—Specifying checkpoint and restart intervals within a file transmission so that if a transmission fails, it restarts automatically from the most recent checkpoint.
- ◆ Compression—Performing data compression for Copy operations for shorter transfer times.
- ◆ User notification—Automatically notifying users of successful and unsuccessful transfers.

These parameters can be specified within the actual Process or you can specify them when you submit the Process. Any parameters you provide when you submit a Process override the parameters coded in the Process.

Process Language

A Connect:Direct Process uses its own scripting language that defines the work that you want the Process to do. The following are the statements used in Connect:Direct Processes:

Statement	Description
PROCESS	<p>Defines general Process characteristics. This statement is always the first statement in a Process. Among the items the Process statement specifies are:</p> <ul style="list-style-type: none"> ◆ The name of the secondary node in the Process ◆ The Process priority ◆ When to start the Process ◆ Who to notify upon completion ◆ Whether Connect:Direct should keep a copy of the Process to execute in the future
COPY	<p>Performs a data transfer. The COPY statement also specifies various file transfer options, including:</p> <ul style="list-style-type: none"> ◆ File allocation ◆ File disposition options ◆ File renaming ◆ Data compression options
RUN JOB	Submits a job or application to the host operating system. The Process continues running and does not wait for the submitted job or application to complete. This is known as asynchronous processing.
RUN TASK	Submits a job or application to the host operating system. The Process waits for the job or application to complete before continuing. If the job or application does not complete, the rest of the Process does not run. This is known as synchronous processing.
SUBMIT	Submits a Process from within another Process. The SYMBOL statement enables Processes to be modular. This enhances processing flexibility, as you can modify Process modules as necessary without altering the master Process.

Statement	Description
SYMBOL	Replaces symbolic strings within a Process with parameter values. The SYMBOL statement eliminates the need to hard-code file names and values within a Process. Instead, the SYMBOL statement allows values to be substituted within a Process, enabling a Process to be reused for different file transfers.
Conditional (IF, EIF, ELSE, EXIT, GOTO)	Controls Process execution by testing Process step return codes with conditional logic statements. For example, if a file transfer successfully completes, the Process can use the SUBMIT statement to initiate a second Process. If the file transfer fails, the Process can send an error message to the operator.
pend	Indicates the end of a Process. This statement is only valid for Connect:Direct for UNIX, OpenVMS, and Windows.

The Process statement must be the first statement in a Process. The statements after the Process statement can follow in any sequence. Each statement uses parameters to control Process activities such as execution start time, user notification, security, or accounting data. These parameters can be specified within the Process or you can specify them when you submit the Process. The parameters for a statement vary according to platform.

The following example shows a Process that copies a file from UNIX to z/OS. The Process was initiated from the UNIX node. The **ckpt** parameter specifies that no checkpoints will be taken:

```

zOSxx    process      snode=zOS.node
          startt = (Monday, 08:30:00 am)
          notify = unixuser@unixhost
step01   copy  from  (file=file1
                    pnode)
          ckpt=no
          to      (file=file2
                  dcb=(dsorg=PS,
                      recfm=FB,
                      lrecl=80,
                      blksize=2400)
                  space=(TRK,(1,,))
                  snode
                  disp=rpl)
          pend

```

Detailed information about Connect:Direct Processes, including graphical demonstrations, statement formats, parameter definitions, and example Processes are available online at <http://www.sterlingcommerce.com/Documentation/processes/processhome.html>.

Creating Connect:Direct Processes

After you define your business need, you can create a Process for execution in the following ways:

- ◆ Through the Process Builder feature of the Connect:Direct Browser User Interface, a Web-based interface to a Connect:Direct server. The Connect:Direct Browser User Interface is distributed with Connect:Direct and Sterling Control Center and is also available for download from the Sterling Commerce Customer Center portal.

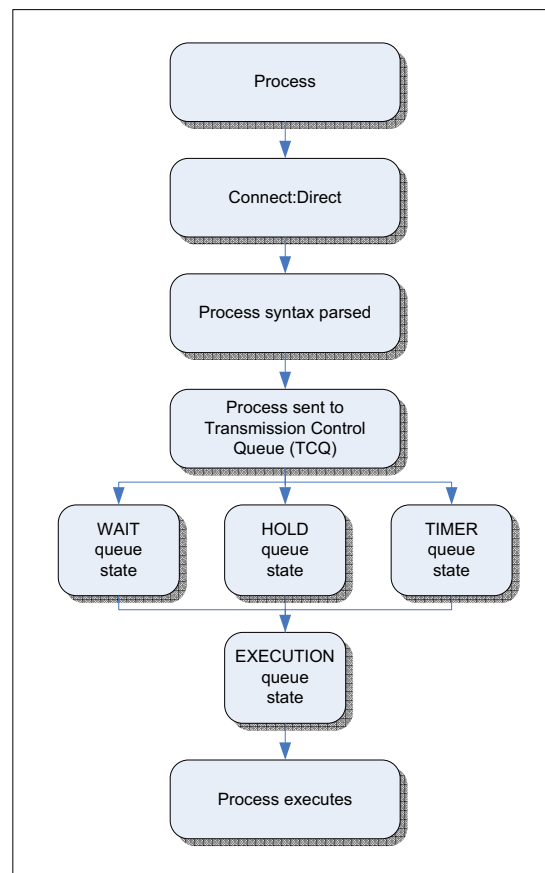
The Process Builder is a GUI that enables you to build, modify, and save Processes. The Process Builder handles Connect:Direct Process syntax rules automatically. The Process Builder eliminates the typographical mistakes made when creating Processes with a text editor. You can also validate Process syntax and submit completed Processes from the Process Builder.

You can use the Process Builder to modify Processes created with a text editor. Likewise, Processes created with the Process Builder feature can be edited with a text editor.

- ◆ Through the Connect:Direct Requester for Windows, which is a graphical interface to Connect:Direct for Windows.
- ◆ A text file that is submitted to a Connect:Direct server through a batch utility, command line, or a user written program through the Connect:Direct Application Program Interface (API).
- ◆ Through the Connect:Direct for z/OS IUI. See the *Connect:Direct for z/OS User's Guide* for information about the IUI.

Managing the Work

After you create Processes, you submit them for execution. The following illustration shows how a Process executes:



The following table explains the Process steps:

Step	Description
Process submitted	A user submits a Process from a Connect:Direct Process library or from the Connect:Direct Browser.
Process syntax parsed	The parser within Connect:Direct verifies the Process syntax.
Process sent to Transmission Control Queue (TCQ)	<p>If the Process passes syntax checking, it is placed in the appropriate work queue according to Process parameters, such as priority, class, and start time. The Connect:Direct work queues are jointly referred to as the TCQ. A Process is in one of the following states in the TCQ:</p> <ul style="list-style-type: none"> ♦ EXECUTION—The Process is executing. ♦ WAIT—The Process is waiting until a connection with the SNODE is established or available. Processes in the WAIT queue state may also be waiting for their turn to execute on an existing session. ♦ HOLD—Process execution is on hold. The Process may have been submitted with a HOLD or RETAIN parameter. The Process is held on the queue until released by an operator or the SNODE connects with a request for held work. The HOLD queue state also applies to Processes that stop executing when an error occurs. ♦ TIMER—The Process was submitted with a STARTT parameter that designates the time, date, or both that the Process should execute. Processes that initially failed due to inability to connect with the SNODE or because of a file allocation failure can also be in this queue state waiting for their retry interval to expire. Such Processes will retry automatically. <p>A queued Process can be queried and manipulated through Connect:Direct commands such as SELECT, CHANGE, DELETE, FLUSH, and SUSPEND PROCESS. For complete information on the Connect:Direct commands and the various queues, refer to the Connect:Direct user's guide for your platform.</p> <p>A message indicating that the Process was submitted successfully is created when the Process is placed into the TCQ. The Process statements have been checked for syntax, but the Process may not have been selected for execution.</p>
Process Executes	The Process is selected for execution based on Process parameters and the availability of the SNODE.

Tools to Help You Manage Processes

Connect:Direct provides tools to allow you to manage Processes. These tools include:

- ♦ **Process Monitor**—Use this tool to view Processes in the Transmission Control Queue (TCQ), release held Processes, change the status of a Process, and delete a Process.
- ♦ **Process Notification Utility**—Use this utility to change the notification method you defined when you installed Connect:Direct to notify users of Process execution.
- ♦ **Message Lookup**—If you need to troubleshoot the meaning of an error message, use this utility to view more explanation about an error message.
- ♦ **SNMP**—If you want to use SNMP to capture messages, you can identify which messages you want to include and determine if messages are trapped or logged to the event log.

- ◆ **CRC checking**—A cyclic redundancy check (CRC) determines whether the data that Connect:Direct receives over the network has been altered in transmission or not. To ensure data integrity during the transmission, a CRC is generated for the entire buffer, including the header. CRC checking works by calculating a short, fixed-length binary sequence for each block of data and sending/storing them together. When a block is read or received, the calculation is repeated. If the new CRC does not match the one calculated earlier, Connect:Direct stops the Process execution and restarts the Process from the last checkpoint record. CRC checking can only be performed for TCP/IP Processes and cannot be enabled when running Secure+ Option, because data integrity is a native part of Secure+ Option.
- ◆ **CLI**—The command line interface (CLI) provides commands to access queues and manage Processes. These commands enable you to control Process execution, view Process status and results, and affect the Connect:Direct server. Issue these commands through or in a native command text format through the Applications Programming Interface (API).
- ◆ **Connect:Direct Browser User Interface**—Connect:Direct Browser User Interface allows you to build, submit, and monitor Connect:Direct Processes from an Internet browser, such as Microsoft Internet Explorer. You can also perform Connect:Direct system administration tasks, such as viewing and changing the network map or initialization parameters, from Connect:Direct Browser. The specific administration tasks that you can perform depend on the Connect:Direct platform that your browser is signed on to and your security level.
- ◆ **File Agent**—Connect:Direct File Agent is a feature of Connect:Direct which provides unattended file management. File Agent monitors watched directories to detect new files. When File Agent detects a new file, it either submits a default Process or evaluates the file using rules to override the default Process and to determine which Process to submit. You create rules to submit different Processes based on the following properties:
 - ◆ Specific or partial file names
 - ◆ File size
 - ◆ System events

Extending the Capabilities of Connect:Direct

You can extend capabilities of Connect:Direct through the Managed File Transfer (MFT) suite of products and options.

Enhanced Security

Connect:Direct contains basic security consisting of user authentication and user proxies that enable you to control who has access to the Connect:Direct server and what actions they are allowed to perform. Enhanced security is available through the following additional MFT products.

Secure+ Option

For a more complete, full-security solution, the Secure+ Option is available. This is a separate, licensing option of Connect:Direct that enables you to select one of three security protocols to use to secure data during electronic transmission: Transport Layer Security (TLS), Secure Sockets Layer protocol (SSL) or Station-to-Station protocol (STS). The SSL and TLS protocols provide three levels of security:

- ◆ The first level of security is server authentication. It 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 that it has not expired and that it has been issued by a certificate authority the trading partner trusts.
- ◆ The second level of security, called client authentication, requires that the trading partner send its own certificate. If enabled, the Connect:Direct server requests certificate information from the trading partner, after it returns its certificate information. If the client certificate is signed by a trusted source, the connection is established.
- ◆ The third level of security requires that a certificate common name be verified. The Connect:Direct Secure+ Option server searches the certificate file it receives from the trading partner and looks for a matching certificate common name. If the server cannot find the certificate common name, communication fails.

Secure+ Option includes the following encryption algorithms:

- ◆ Symmetric—AES, DES, 3DES, RC4
- ◆ Asymmetric—RSA

- ◆ FIPS—Leverages Crypto-C, which is Sterling Commerce's FIPS 140-2 validated security module on the UNIX and Windows platforms and leverages the IBM eServer cryptographic coprocessor on the mainframe. The following FIPS-validated algorithm implementations are supported in Secure+ Option:
 - ◆ DES, FIPS 46-3, NIST Certificate #160
 - ◆ 3DES, FIPS 46-3, NIST Certificate #100
 - ◆ SHA-1, FIPS 180-1, NIST Certificate #89
 - ◆ AES, FIPS 197, NIST Certificate #5
 - ◆ DSA, FIPS 186-2, NIST Certificate #70

FIPS compliance can be achieved with Connect:Direct only by installing Secure+ Option and enabling FIPS mode on the supported platforms.

Sterling External Authentication Server

As part of the Secure+ Option, you can use the Sterling External Authentication Server to implement extended authentication and validation services for your Sterling Commerce products. The Sterling External Authentication Server is a separate, GUI-configurable application that allows you to validate certificates against certificate revocation lists (CRLs). You can also configure multifactor authentication using SSL client certificates, SSH keys, user ID and password, and client IP address as factors. You can enable application outputs to allow you to map attributes, such as login credentials that are returned to a query, to outputs you specify.

Certificate Wizard Certificate Management Tool

The Sterling Certificate Wizard is a component of the Secure+ Option and is available as a free download. It is a standalone, Java application you can use to generate and obtain the certificates necessary for secure connections that use the Secure Sockets Layer (SSL) protocol, the Transport Layer Security (TLS) protocol, as well as SMIME messaging and SSH keys.

Sterling Secure Proxy

For further security of your Connect:Direct network, you can use Sterling Secure Proxy as an application proxy in your DMZ. When used as a reverse proxy, Sterling Secure Proxy ensures that the node has the authority to connect. If the node is authorized, the proxy provides a session break and establishes a new connection to connect to the Connect:Direct node inside the company.

As a forward proxy, it allows an internal node to connect to a Connect:Direct node outside of your secure environment. The internal node connects to the forward proxy in the DMZ. The forward proxy then sends connection information to the external Connect:Direct node. The session break ensures that the company node is protected and does not have a direct connection to the external node. The external Connect:Direct node is unaware that Sterling Secure Proxy is deployed and believes it is connecting to the internal Connect:Direct node.

Sterling Secure Proxy also provides user authentication to ensure that the external node is authorized to connect to Sterling Secure Proxy. As an extension of user authentication, you can use Sterling External Authentication Server to make use of an external database, such as Active Directory or Lightweight Directory Access Protocol (LDAP), to perform Connect:Direct node authentication and certificate authentication.

Sterling Secure Proxy also provides the following security features:

- ◆ SSL or TLS using certificates—Ensures that the connection between Sterling Secure Proxy and the internal and external nodes uses SSL or TLS.
- ◆ Support for Hardware Security Modules (HSM)—Stores and protects your certificates.
- ◆ Support for connection routing—Allows you to route incoming connections using the following methods:
 - ◆ Direct Routing—Routes incoming connections directly to the trusted company server.
 - ◆ PNODE routing—Allows the inbound node to determine what SNODE it connects to.
 - ◆ Certificate-based routing—Allows Sterling Secure Proxy to determine the internal server to route the connection to, based on the distinguished name in the certificate.
- ◆ Support for step injection—Allows you to insert Connect:Direct Process statements into the communications session with the SNODE independent of the PNODE Process statements. These injected statements can provide real-time notification of file delivery, invoke applications, run operating system jobs and commands, and submit other Connect:Direct Processes, all without the need to provide an exit program on the SNODE or without changing the PNODE Process. The results of these steps are logged in the statistics file of the SNODE.

In addition to providing proxy services for Connect:Direct, Sterling Secure Proxy also provides proxy support to for FTP, SFTP (SSH), HTTP, and HTTPS, allowing you to extend your managed file transfer enterprise to Sterling Integrator and Sterling File Gateway.

Unattended File Management with File Agent

Connect:Direct File Agent is a component of Connect:Direct that provides unattended file management. It provides monitoring and detection capabilities that enhance the automation you accomplish with Connect:Direct Processes.

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

- ◆ Watch for any file to appear in one or more watched directories and submit a default Connect:Direct Process after detecting the newly added file.
- ◆ Override the default Connect:Direct Process specified and apply either watched file event rules or system event rules that are enabled for the configuration. If the criteria for a rule are met, File Agent submits the Connect:Direct Process associated with that rule.
- ◆ You can create File Agent rules based on the following properties:
 - ◆ Full or partial name of the file detected in a watched directory. The watched directory can be a local directory on the Connect:Direct server or a network drive.
 - ◆ Size of the file detected in a watched directory
 - ◆ System event title or contents

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

Enterprise Management with Sterling Control Center

Sterling Control Center provides centralized management and monitoring of large-scale, distributed Connect:Direct server environments. It enables you to enhance operational productivity and improve the quality of service for Connect:Direct file transfers and activities in your environment from one central location through:

Service Level Management

- ◆ Helps answer the questions, “Where is my file?” and “Are my service level agreements being met?” by providing a system-wide view of all your Connect:Direct servers across different platforms and locations in real time
- ◆ Allows you to monitor the overall health of the environment through server status indicators
- ◆ Allows you to setup an early warning system for exceptions regarding critical processing windows and server events in the form of proactive notifications (e-mails, SNMP traps, and GUI alerts)
- ◆ Helps you ensure that your file transfer environment is functioning at the level you need it to by consolidating information for throughput analysis, capacity planning, post-processing operational or security audits, and workload analysis
- ◆ Allows you to release or delete Connect:Direct Processes from a central location

Asset Management

- ◆ Helps answer the questions, “Where is my Connect:Direct software installed and running?” and “Is it in compliance with license agreements?”
- ◆ Helps you track network assets by capitalizing on its server monitoring capabilities. A feature called Guided Node Discovery (also called Node Discovery) lets you find all Connect:Direct servers that a managed Connect:Direct server communicates with.
- ◆ Helps you ensure that your server licenses are up to date and facilitates license distribution to the managed Connect:Direct servers in your environment.

Configuration Management

- ◆ Helps you answer the questions, “Are my Connect:Direct servers configured correctly?” and “Do they comply with our security policy?”
- ◆ Provides a centralized, simplified means of managing the configurations of your Connect:Direct for UNIX, Windows, and z/OS servers by:
 - ◆ Providing a common interface for managing and auditing Connect:Direct server configurations
 - ◆ Normalizing parameters across platforms that might have different names and value pairs
 - ◆ Providing platform-specific syntax checking and easy-access tooltip help
 - ◆ Providing a means for updating, viewing, auditing, and tracking versions (including rollback functionality) of configuration data for Connect:Direct servers, such as netmap nodes, functional authorities, and initialization parameters
 - ◆ Generating an audit log that identifies all changes that are made to the configuration and who makes them

Other Tools/Options to Extend Capabilities

There are several tools/options that extend the functionality available in Connect:Direct:

Sterling File Accelerator

A UDT (UDP-based Data Transfer) solution that provides faster file transfers for high-volume files than TCP over high-speed networks with high latency.

Windows SDK

The Software Development Kit can be used to integrate Connect:Direct operations into your company's applications. The SDK uses a 32-bit interface for C and C++ as well as an OLE automation server for Visual Basic applications. The SDK also provides ActiveX controls for Submit Process and Select Statistics commands. The tools available in the SDK include: C API functions, C++ Class interface, ActiveX control interface, direct automation servers, and user exits.

SNMP Agent

The Connect:Direct SNMP Agent is a proxy agent that enables a Connect:Direct server to provide information to SNMP network management stations, which provides access to the following information:

- ◆ General condition of the Connect:Direct server
- ◆ Alerts for events requiring further investigation, such as possible security violations, failing Processes, and session failure.

Clustering Solutions

Sterling Commerce provides support for clustered environments such as IBM Sysplex, Symantic Veritas, Sun Solaris Cluster, and Microsoft Cluster Server.

Additional Connect:Direct Products

You can extend the capabilities of a single Connect:Direct server with Connect:Direct Select and Connect:Direct FTP+.

Connect:Direct Select

Connect:Direct Select provides reliable and secure unattended data delivery between remote sites where Connect:Direct is installed.

In its basic configuration, a Connect:Direct Select node sends files from a watch directory or e-mail inbox to a Connect:Direct server and receives files from the Connect:Direct server. You can also

configure Connect:Direct Select to send files to other computers as e-mail attachments, to route files to multiple destinations, and to perform additional processing on received files.

Connect:Direct FTP+

Connect:Direct FTP+ is a solution that is designed to operate as simply as common FTP. It provides a simple, reliable, and secure way to transfer files between a Connect:Direct server at a central processing center and remote sites. Connect:Direct FTP+ operates like an FTP client. It can initiate send or receive operations with the Connect:Direct server, but the server cannot initiate transfers with Connect:Direct FTP+. The complete FTP command set is supported, whether from a command line or a script. Commands that do not have equivalent Connect:Direct operations are accepted and an appropriate message is generated.

While Connect:Direct FTP+ is as simple to use as common FTP, it provides additional benefits not available in FTP. These include:

- ◆ Assured, reliable data delivery. Connect:Direct FTP+ has checkpoint and restart capability. All activity and statistics are logged, so there are verifiable audit trails of all actions.
- ◆ Secure data delivery. Connect:Direct FTP+ is compatible with Connect:Direct Secure+, so that data can be safely sent in an encrypted format, safe from hackers and data thieves.
- ◆ Data integrity checking. Connect:Direct ensures the integrity of the transferred data and verifies that no data is lost during transmission.
- ◆ Seamless integration into Connect:Direct environments. Because Connect:Direct FTP+ is a Sterling Commerce product, it is easily integrated into existing Connect:Direct networks, with minimal changes required to the Connect:Direct server.

You can install Connect:Direct FTP+ on Windows, UNIX, or Linux computers.

Speciality Products

SWIFTNet

Connect:Direct UNIX for SWIFTNet and Connect:Direct Windows for SWIFTNet are special Connect:Direct solutions that were developed to work with SWIFTNet, which is a highly secure, proprietary network in Europe used by financial institutions. The Connect:Direct SWIFTNet solution supports the FileAct (real-time file transfer service) SWIFT service.