Connect:Direct File Agent

Configuration Guide

Version 1.3.00

Sterling Commerce
An IBM Company

Connect:Direct File Agent Configuration Guide Version 1.3.00

First Edition

Sterling Commerce, Inc.

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

Contents

Chapter 1

Managing Files with Connect:Direct File Agent

Connect:Direct File Agent is the component of Connect:Direct that provides unattended file management. Before using Connect:Direct File Agent, you must plan how to configure it to automate file management for your site. After planning what you need to accomplish, configure File Agent to connect to a Connect:Direct server, watch the directories that files of interest will be added to, and submit a specified Connect:Direct Process to the server when a file is detected.

Connect:Direct File Agent

Connect:Direct File Agent provides monitoring and detection capabilities that enhance the automation you accomplish with Connect:Direct Processes. You cannot create Processes with File Agent; however, File Agent variables can pass arguments to a Process. File Agent does not delete, copy, or move files directly, but it helps you accomplish such tasks by submitting the Process you specify in the configuration to the Connect:Direct server. Before you configure File Agent, you must create and test the Connect:Direct Process that you intend to specify as the default Process in the File Agent configuration.

Using the File Agent configuration interface and Help system, you define the *default configuration file* (Default_Config.ser). The default configuration file defines the Connect:Direct server that Connect:Direct File Agent communicates with; the directory, or directories, that File Agent monitors; and how a file added to a watched directory or a detected system event is processed.

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 the default Process after detecting the newly added file.
- Override the default Process specified and apply either *watched file event* rules (Submit Process rule) or *system event* rules that are enabled for the configuration. File Agent applies a *watched file event* rule to a detected file by checking file properties to determine whether criteria specified by the rule are met. A *system event* rule checks whether a system event meets criteria specified by the rule. If all 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
- ✦ Size of the file detected in a watched directory
- ✦ System event title
- ✦ System event contents (as included in a stack trace)

You can specify more than one rule in a File Agent configuration; each rule can have File Agent submit a different Process.

Note: Although you can create multiple rules as part of a File Agent configuration, File Agent rules processing ends once all criteria for a rule are met. Therefore, you should specify rules so that those with more specific criteria (properties) are listed first in the configuration.

For optimum performance, you should configure Connect:Direct File Agent to communicate with the Connect:Direct node where it is installed. You can configure File Agent to use continuous signon and remain connected to the API port for the Connect:Direct server at all times, or configure it to connect to the port only when it needs to. File Agent is available on UNIX, Windows, and z/OS operating systems. When you use Connect:Direct for UNIX or Windows, the watched directory is a UNIX path name or a Windows path to the directory. When you use Connect:Direct for z/OS, the watched directory can be a fully specified HFS path name for a file or a directory, a fully specified MVS data set name, a partial MVS data set name, or the name of a partitioned data set (PDS) or partitioned data set extended (PDSE).

File Agent can monitor multiple directories, including local and network directories. File Agent scans the watched directories you specify in the configuration for newly added files (unless you specify a rule to force other operation). By default, Connect:Direct File Agent scans a watched directory once each minute. For example, if you start File Agent at 1:00 p.m., a file added to that watched directory at 12:55 a.m. is not detected. If you start File Agent at 1:00 p.m., and a file is placed in the watched directory at 1:01 p.m., then File Agent detects this newly added file. File Agent detects a file only one time, unless the file is accessed and saved with a later timestamp.

Using Connect:Direct File Agent requires an understanding of Connect:Direct Processes, operating systems, and scripting (for regular expression operator use with File Agent rules).

Running File Agent

You can run File Agent from a UNIX or MS-DOS command line, configure it to start automatically as a Windows Service at system startup, or configure it to run from a Windows shortcut. Use the command line to verify that File Agent is working correctly or to specify an alternate configuration file. After you run File Agent from the command line to verify that File Agent is operating correctly, run it using the method that requires the least user intervention.

When File Agent runs as a Windows service, it is fully automated, requiring little user intervention. On UNIX, you can modify the initialization sequence of the computer to call the cdfa.sh script and run Connect:Direct File Agent whenever you restart the computer. On z/OS, you must run the appropriate job to start the File Agent configuration interface, or to start or shut down File Agent.

You can run more than one File Agent on the same or different hosts. You can also monitor a directory with more than one file agent. Refer to *Configuring the Gate Keeper for Multiple File Agent Instances* on page 19 for more information.

File Agent Logging

File Agent logs system information to the console and three separate log files. The level of information that is written to the logs is configurable. For more information, refer to *Configuring File Agent Logging* on page 78.

File Agent Monitoring

File Agent can send SNMP traps to Sterling Control Center or other third-party software to monitor File Agent activity. To use this feature, you must modify the File Agent configuration. For more information, refer to *Monitoring File Agent* on page 82.

File Agent Configuration Interface and Help

Instructions for configuring File Agent are available in the online Help system that you access from the configuration interface. Field-level Help is displayed in the bottom pane of the configuration interface. Clicking **Help** displays the online configuration procedures.

Planning the File Agent Configuration

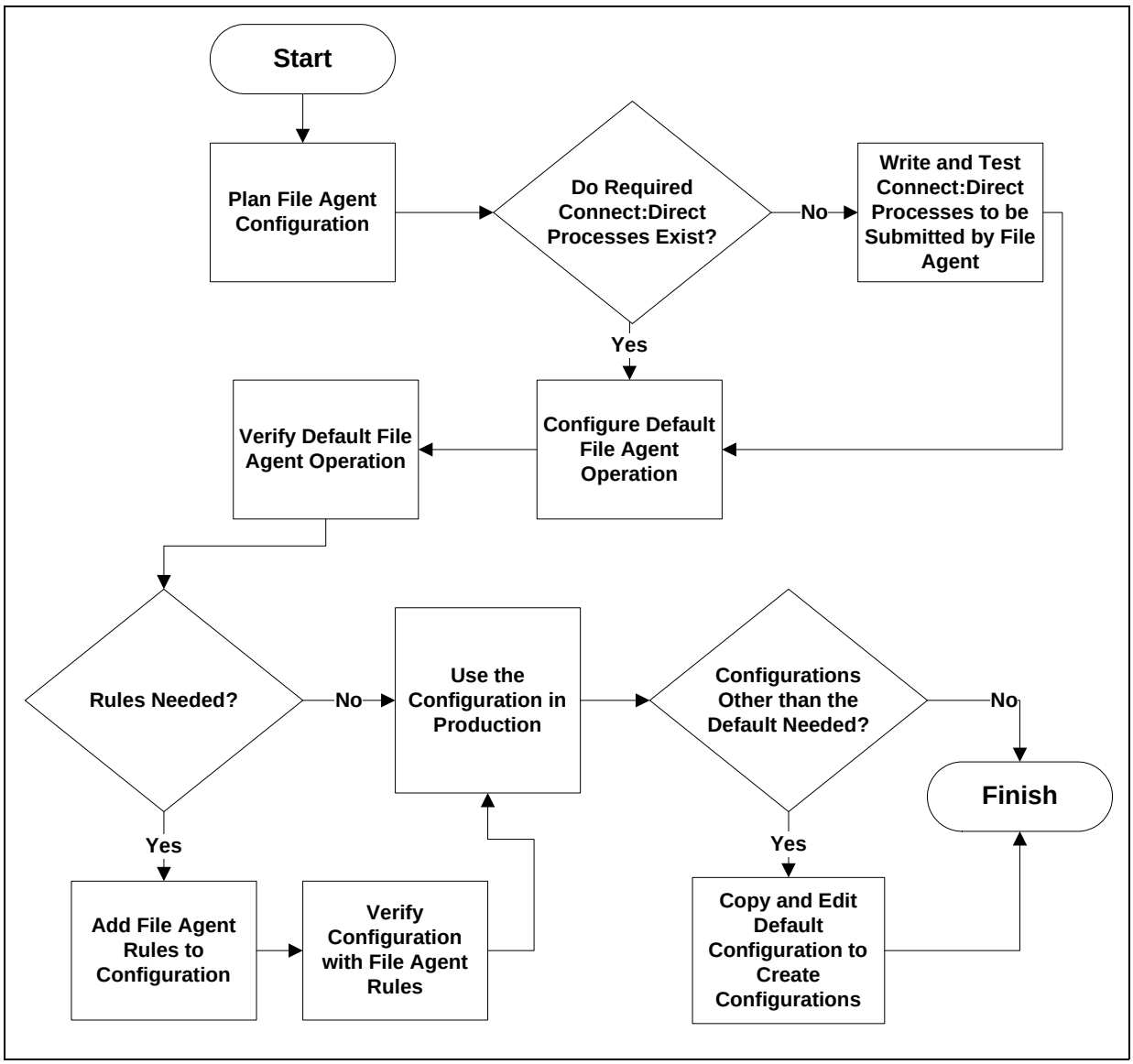
Before you begin configuring File Agent, you must choose or create the Connect:Direct Processes that perform the actions you want to automate. You configure File Agent to connect to the Connect:Direct server and to monitor and detect conditions (such as a file addition to a directory). At detection, Connect:Direct File Agent submits the Process for executing actions that need to be performed in response to those conditions.

Refer to the *Connect:Direct File Agent Configuration Scenarios* on page 15 to review some configuration scenarios that can help you understand File Agent configuration. The File Agent Help documents the following incremental approach to configuration:

- Specify the server connection, a default Process, and the watched directory.
- Run a test from the command line and use the log to verify that the default File Agent configuration is working correctly.
- After you verify the default configuration, you can create and validate File Agent rules, one by one, by running File Agent in verbose mode.
- After you successfully create a default configuration, you can use the file as the basis for other configuration files.

Use the *File Agent Worksheet* on page 11 to gather the information you need to configure File Agent. Contact your system administrator for the site-specific information necessary to establish a connection to the Connect:Direct server. Make copies of this worksheet if you have to configure File Agent on multiple Connect:Direct servers.

The following diagram illustrates the flow of steps for setting up File Agent for use in a production environment.



File Agent Worksheet

Connect:Direct Server Connection Information	
User ID for API (for connecting to the Connect:Direct server) **Required** Must match the user ID used to submit the default Process.	_____
Password for API (for connecting to the Connect:Direct server) **Required** Must match the password used to submit the default Process.	_____
API host DSN name (name of the host on which the Connect:Direct server is located) **Required**	_____
API port (default =1363) 1–5 digit port number that Connect:Direct File Agent uses to connect to the Connect:Direct server API. **Required**	_____
Gate Keeper port (default=65530) Port used to track directory monitoring and ensure that multiple File Agents do not monitor a single directory. **Required** Refer to *Configuring the Gate Keeper for Multiple File Agent Instances* on page 19 for more information on Gate Keeper functionality	_____
Gate keeper DNS name (optional) (default=127.0.0.1)	_____
Default Process and Watched Directory Information	
Watched directories: **Required** For Windows and UNIX, one or more valid specifications of paths (Windows) or pathnames (UNIX). For z/OS, one or more fully specified HFS pathnames of a file or directory, or a full or partial MVS data set name.	
List one valid entry per line.	
Monitor sub directories (default=Yes)	
Continuous signon (default=No)	

Default Process and Watched Directory Information	
Default Process: Windows and UNIX: Valid path and name of the file that contains the default Process on the Connect:Direct server. z/OS: Member Name in DMPUBLIB **Note:** If you do not specify a default Process or create a rule, no processing is performed when a file or event is detected.	_____ _____
Default arguments (See Help for complete list.) Argument string to pass to the default Process in the following format: &FA_*XXXX_XXX*. **Note:** The percent sign (&) and period (.) are required.	_____
Error Process:	_____
Error arguments	_____
Process class (default=1) **Required**	_____
Process priority (default=1)	_____
Watched file interval (default=1 minute)	_____
File completion delay (default=1 minute)	_____
File Agent unique name (default=FileAgent) **Required** Unique name for each File Agent instance to be monitored by Sterling Control Center.	_____
SNMP listener address Address of the SNMP trap receiver. This is required when monitoring File Agent with Sterling Control Center.	_____
SNMP listener port Listening port of the SNMP trap receiver. This is required when monitoring File Agent with Sterling Control Center	_____

SNMP source port range Ports or port ranges used to pass through a firewall to the SNMP trap receiver, including Sterling Control Center, when File Agent is behind a firewall. Type the ranges in the format nnnn-nnnn, separated by commas, for example, 5555-7777, 8888-8890, 9999.	_____
Refresh Configuration Whether configuration changes are in effect immediately (Yes) or after stopping and starting File Agent (No).	_____

Note: If you are using X Windows, the X11 display variable is used to connect to the GUI server for terminal emulation. The File Agent Configuration Interface will display on the monitor specified for the X11 display variable. If you want to display the File Agent Configuration Interface on a Windows computer, you must specify the network ID of the terminal you want to use for displaying the File Agent Configuration Interface.

Considerations for a Large Number of Watch Directories

There are two considerations when watching a very large number of directories: scan time and log space. File Agent scans each watch directory, then waits for the time specified in the watch interval, then repeats the cycle. With a large number of watch directories, each scan takes more time.

To keep each log file at a manageable size yet still keep enough current log data, the logging system uses a combination of MaxFileSize and MaxBackupIndex settings in the log4j.properties file to control logging. The MaxFileSize setting allows each file to grow only to a specified size, and the MaxBackupIndex setting specifies how many backup files are allowed. Multiplying these two settings will give you the maximum amount of disk space. Since there are three different logs, you would add the maximum disk space for each enabled log to get the maximum disk space for all File Agent logging.

You can modify the MaxFileSize and MaxBackupIndex for each log to meet your requirements. The MaxFileSize should not be larger than the amount a text editor can easily edit, so 32MB is the recommended upper limit for this setting. The MaxBackupIndex can be as large as you want and depends on how much log history you would like to keep and how much disk space you have available.

To modify MaxFileSize:

1. Open the log4j.properties file in the installation directory.
2. Modify one or more of the following log files:

Log File	Modify This Value
CDFA.log	log4j.appender.R.MaxFileSize=*1000KB*
CDFA_verbose.log	log4j.appender.V.MaxFileSize=*1000KB*
CDFA_stats.log	log4j.appender.S.MaxFileSize=*1000KB*

To Modify MaxBackupIndex:

1. Open the log4j.properties file in the installation directory.
2. Modify one or more of the following log files:

Log File	Modify This Value
CDFA.log	log4j.appender.R.MaxBackupIndex=*10*
CDFA_verbose.log	log4j.appender.V.MaxBackupIndex=*10*
CDFA_stats.log	log4j.appender.S.MaxBackupIndex=*10*

Sterling Commerce has tested with 50,000 watch directories using MaxFileSize=32MB and MaxBackupIndex=10 with no adverse effects except those considerations noted above.

Considerations for a Large Number of Files in a Watch Directory

Once File Agent has scanned a watch directory, it submits a Connect:Direct Process for each available file that it finds. If there are a large number of files in a watch directory, the time it takes to submit the Processes is larger than if it were handling just a few files during each scan. Also, watch directories with a large numbers of files will not be scanned as often because of the time it takes to do an individual scan.

Also, consider that the Connect:Direct Server you are using must be able to handle the number of Processes that File Agent submits. There may also be a limit on the number of Processes it will run concurrently.

Sterling Commerce has tested with over 50,000 files in a watch directory with no adverse effects. The checkpoint file contained over 50,000 entries and files transferred appropriately. An upper limit to the number of files in a watch directory has not been determined, but will depend on the amount of memory the system has available.

Considerations for Shared Directories

If the File Agent watch directory is a shared directory and the connection to the shared directory is lost, then a log entry indicates that File Agent does not have read/write access to the directory. When the connection to the directory is restored, then File Agent can access the directory on the next scan.

Connect:Direct File Agent Configuration Scenarios

The following examples illustrate typical scenarios for using Connect:Direct File Agent. Fields that are not required to be set for the operation demonstrated in the example are not included in the tables of configuration parameters. Required fields are indicated by an asterisk (*) in the File Agent Configuration Interface, and all fields are described in field-level Help.

The sample scenarios have the following assumptions:

- You have configured the site-specific parameters required to establish a connection to the Connect:Direct server where File Agent is installed (see the *File Agent Worksheet* on page 11 for a description of the parameters required to establish the connection).
- The Connect:Direct Processes used in the File Agent scenarios have been created.

Detecting a File Added to a Watched Directory on a z/OS System

Some users need to access a report file that is expected to be transferred to a location that only administrators can access. The sample values in the table configure File Agent to perform the following processing:

- Monitor the watched data set called EASTERN.Q1.REPTS.
- Submit a default Process called DEFPROC. The default Process has been created to copy a file detected in the watched data set to a specified location for access by users.

Tab	Field	Sample or Description
File agent	Watched directories	Type EASTERN.Q1.REPTS to specify the fully qualified MVS data set name to monitor.
	Default Process	Type DEFPROC, the member name for the Process in DMPUBLIB. **Note:** If no default Process is specified and the file does not match a rule, then no processing occurs.

Detecting a VSAM Data File Added to a Watched Directory on a z/OS System

Each month, users in the accounting department need to access a VSAM data file that contains their company's monthly payroll information. The name of the data file containing this information is VSAM.mm.yy.PAYCHECKS.DATA where mm is the month and yy is the year. The data file is expected to be transferred to a location that only administrators can access.

The Connect:Direct administrator configured File Agent to watch for any file containing the string, VSAM.**.**.PAYCHECKS, and then to copy it to the directory location the accounting users could access. When the administrator tested File Agent, she discovered that the Process had been submitted three times because File Agent was triggered for the following VSAM files when the VSAM cluster was created:

- VSAM.mm.yy.PAYCHECKS
- VSAM.mm.yy.PAYCHECKS.INDEX
- VSAM.mm.yy.PAYCHECKS.DATA

To configure File Agent to watch only for VSAM data files and not other VSAM-related files, the administrator modified the match string and specified VSAM.**.**.PAYCHECKS.DATA as the the VSAM data set to watch. She configured File Agent to perform the following processing:

- Monitor the watched data set called VSAM.**.**.PAYCHECKS.DATA
- Submit a default Process called DEFPROC. The default Process has been created to copy a file detected in the watched data set to a specified location for access by users.

Tab	Field	Sample or Description
File agent	Watched directories	Type VSAM.**.**.PAYCHECKS.DATA to specify the fully qualified VSAM data set name to watch.
	Default Process	Type DEFPROC, the member name for the Process in DMPUBLIB. **Note:** If no default Process is specified and the file does not match a rule, then no processing occurs.

Detecting a File by File Size on a Windows System

Customer transaction files are regularly transferred into the Windows directory c:\monthend\datafile. Files larger than 1 MB require special processing that will automatically be performed on files in a certain directory.

The sample values in the table configure File Agent to perform the following processing:

- Monitor the watched directory c:\monthend\datafile
- Apply the rule titled "find big file” to detect files larger than 1 MB.
- Override the default Process and submit a Process that is associated with the Check file size rule. This fixbigfile.cdp Process will copy a file larger than 1 MB from the c:\monthend\datafile directory to the c:\reprocess directory.
- Pass the path and file name of the file that meets the criteria for the "find big file” rule to the Process fixbigfile.cdp.

Tab	Field or Dialog Box	Actions and Sample Entry
File agent	**Watched directories** field	Specify the directory to monitor. Type the path of the directory to monitor: **c:\monthend\datafiles**

Tab	Field or Dialog Box	Actions and Sample Entry
Rules	**Create rule** dialog box	Click **New** and type the name you want to give the rule in the field: **find big file** Click **find big file** in the list of rules and click **Edit**.
	Match criteria list for rule "find big file"	Specify the criterion to check for a detected file. Select the default criterion name, **Not enabled: system event title matches " "** and click **Edit match**.
	Edit match criterion for rule "find big file" dialog box	◆ Click **Enabled** to enable the criteria you are about to specify. ◆ Click **Size of the newly arrived file** ◆ Click **Matches** to display the options for the comparison. Click **Greater than** to define the how the file size should compare. ◆ Type **1048576** in the **Compare size** field and click **OK**.
	Process name field	Scroll down to view the **Submit Process information for watched file event rule "find big file"**. Type the directory path and file name of the Process that File Agent submits when the Find big file rule detects a match: **c:\processes\fixbigfile.cdp** Click **Done** and then click **Save**.

Detecting a System Event by Title on a Windows System

IndexOutOfBoundsException is the title of an event that indicates a number is outside of an expected range. In the following example, File Agent is used to detect an event with IndexOutOfBoundsException in the title, pass a string (the event title) to a Connect:Direct Process, and then submit a Process to the Connect:Direct server that will perform actions the environment requires for this type of event. In this scenario, the event IndexOutOfBoundsException could indicate activity that a network administrator should investigate. Because the site uses a Connect:Direct mailbox system, the configuration will include the administrator's account to be notified when Connect:Direct File Agent submits a Process for the IndexOutOfBounds rule.

The sample values in the table configure File to perform the following processing:

- Override the default Process and submit \processfolder\oo_boundserrproc.cdp
- Send a message to the mailbox system account for the administrator after submitting the oo_boundserrproc.cdp Process for the rule.

Tab	Dialog Box, Window, or Field	Description/Example
Rules	**Create rule** dialog box	Type **index out of bounds** as the name of the rule you are creating.
	Match criteria list for rule "index out of bounds" window	Select the default criteria **Not enabled: System event title matches " "** and click **Edit match**.
	Edit match criterion for rule "index out of bounds" dialog box	◆ Click **Enabled** to enable the criteria you are about to specify. ◆ Click **System event title** as the criterion to match for the rule. ◆ Click **Matches** on the drop-down field to see the options for comparison to a string. ◆ Click **Contains** to specify how the compare string should relate to a system event title that File Agent detects. ◆ Type **IndexOutofBounds** as the **Compare String** to indicate that the system event title should include this string. ◆ Click **OK**.
	Submit Process information for system event rule "index out of bounds" window	Type information into the fields that will define the Process to submit and the mailbox user to notify after the Process is submitted.
	Process name field	Type **c:\processfolder\errproc.cdp** to specify the path and file name for the Process File Agent submits when a file meets the rule criteria.
	Notification userid field	Type **adminjim@company.com** to specify the user to notify when File Agent submits the Process.

Passing the UNIX Pathname for a Detected File to a Process

Because Connect:Direct File Agent can watch multiple directories for the appearance of a new file, the Connect:Direct Process that File Agent is to submit to the server at the appearance of a new file might need to reference the Windows path or UNIX path name for the detected file as part of commands and statements in the Process.

In the following example, a UNIX path name is passed to the default Process, copynewfile.cdp.

Tab	Dialog box, Window, or Field	Sample Entry
File agent	**Watched directories**	Type one UNIX path name per line for each location File Agent is to monitor for the appearance of files: **user/bin/monthend/** **quartend/easterndiv/errorfiles** **managers/special/reports**
	Default Process	Type the UNIX path name and file name for the Connect:Direct Process to run when a file is detected in any watched directory specified: **user/bin/admin/copynewfile.cdp** The path name where File Agent detected a new file is passed to this Process.
	Default arguments	Type the File Agent variable for passing the UNIX path name, including the leading percent sign (%) and the ending period (.): **&FAP=%FA_PATH_FOUND.** In this example, **&FAP** is the variable to which File Agent will pass the UNIX path name where the file was detected. **%FA_PATH_FOUND.** is the File Agent variable used to indicate the information to pass to the Connect:Direct Process.

Configuring the Gate Keeper for Multiple File Agent Instances

The File Agent gate keeper keeps track of the directories that multiple File Agents are configured to watch. If more than one File Agent monitors the same directory, the gate keeper determines which File Agent monitors that directory. This prevents more than one File Agent from monitoring files in the same directory.

If you are using one instance of File Agent or do not have multiple File Agents monitoring the same directory, set the Gate keeper DNS name to blank for all of your File Agent configurations. This will turn off the gate keeper and improve File Agent performance.

If you have multiple File Agents monitoring the same directory, use the same Gate keeper DNS name and Gate Keeper port for all File Agent configurations. The File Agent with the address that matches the configured gate keeper address becomes the File Agent gate keeper. If you have File

Agent installed on different servers, decide which File Agent to use as the gate keeper and use its Gate keeper DNS name and Gate Keeper port for all File Agent configurations.

In the following example, multiple File Agents installed on the same server are configured to monitor the C:\invoices directory. All File Agent configurations use the same Gate Keeper port, Gate keeper DNS name, and Watched directory. When a file is detected in the C:\invoices directory, the default process, copynewfile.cdp, is submitted.

Tab	Dialog box, Window, or Field	Sample Entry
File agent	Gate Keeper port	Type the gate keeper port number that File Agent connects to. **65530** (default)
	Gate keeper DNS name	Type the host name of the File Agent gate keeper. **10.10.10.10**
	Watched directories	Type one directory per line for each location File Agent is to monitor for the appearance of files: **C:\invoices**
	Default Process	Type the Windows path name and file name for the Connect:Direct Process to run when a file is detected in any watched directory specified: **C:\CDProcesses\copynewfile.cdp**

Tips for Using Connect:Direct File Agent

Review the following processing and operational guidelines before you use File Agent in a production environment.

- You must monitor your standard output log files to detect problems or failures in File Agent or configure File Agent to send SNMP traps to Sterling Control Center or another SNMP monitoring application.
- The configuration interface is displayed when you attempt to start File Agent if the .ser configuration file you are executing contains errors. Review your configuration file and correct the errors.
- You cannot configure e-mail alerts to notify you when errors occur unless you are using Sterling Control Center with Connect:Direct.
- If you have to stop and restart File Agent, existing files in the watched directories are not detected for processing unless you remove them and put them back with a new timestamp, or use the UNIX touch command to alter their timestamp.
- File Agent detects a file only once unless the file is accessed and saved with a new timestamp.
- To run File Agent with a configuration file other than Default_Config.ser, you must stop and restart File Agent manually from the command line and specify the name of the configuration file to use.

- For optimum performance, configure File Agent to communicate with the Connect:Direct node on the same server.
- To determine the version of File Agent that you are running, you must start File Agent in verbose mode or check the CDFA.log.
- Obtain the latest version of File Agent from the Sterling Commerce Support On Demand Web site. See the Connect:Direct release notes for your platform for instructions.

Chapter 2

Creating and Verifying the Configuration

Before you start Connect:Direct File Agent in a production environment, you must create and validate the default configuration. The following procedures guide you through the steps of creating the default configuration and validating that configuration before and after you add a rule:

- Creating and Verifying the Default_Config.ser File
- Creating and Validating Rules

Note: Running Connect:Direct File Agent from the command line is practical only for testing and troubleshooting configurations, or for special processing other than that defined by the default configuration file, Default_Config.ser.

After you validate the default configuration, you can complete the procedures in *Managing Configuration Files* on page 47 to modify the default configuration as required for your enterprise, add a new configuration file, edit or delete existing configuration files, and, if necessary, define site-specific configuration files for mass distribution. Each time you modify a configuration, validate the changes before using File Agent with that configuration in a production environment.

Creating and Verifying the Default_Config.ser File

To run Connect:Direct File Agent, you must create the default configuration file (Default_Config.ser). The default configuration file defines the Connect:Direct server that Connect:Direct File Agent communicates with; the directory, or directories, that File Agent monitors; and how a file added to a watched directory or a detected system event is processed.

The default configuration file you define in the following procedure includes no File Agent variables or rules. After you verify the operation of a default configuration, you can refer to *Overriding the Default Configuration with Rules* on page 34 to create a flexible configuration with rules and *Using File Agent Variables* on page 30 for instructions on using variables.

Creating the Default Configuration File

To create the Default_Config.ser file:

1. Start the configuration interface:
   - On a Windows system, select **Start>Programs >Connect Direct File Agent> Configure Connect Direct File Agent**. Connect:Direct File Agent starts and displays the configuration interface.
   - On a UNIX system, change to the directory where Connect:Direct is installed (/cdunix/file_agent/), and type **cdfa -C** at the command prompt.

     Note: The **-C** parameter is case-sensitive. You must type a capital **C**.

   - On a z/OS system, submit and run the *CDFACONF* job to execute the File Agent GUI. See the *Optional Installation Tasks* chapter in *Connect:Direct for z/OS Installation Guide* for instructions if you have not started the File Agent GUI.
2. Select **Default_Config** in the Configurations window and click **Edit** on the **File Agent** tab. Default_Config displays in red when you first start the File Agent configuration interface because the file has not been saved. After you specify details for your network in the required fields and save the configuration, the default file displays in black to indicate that it is ready for use.
3. Using the information from the File Agent Worksheet provided in Managing Files, identify the Connect:Direct server that Connect:Direct File Agent connects to and the default Process information. Type the information in fields on the **File Agent** tab as follows:
   - Userid for API
   - Password for API
   - API host DSN name
   - API port
   - Gate Keeper port
   - Watched directories
   - Process class

   The following table describes all parameters for the default configuration file. An asterisk (*) before a field on the configuration interface indicates a required parameter. Specify any other parameters required to configure File Agent to operate on your site.

Parameter	Description
Comments	Type comments to describe the configuration. Comments are not used during the execution of File Agent.
Userid for API	**Required**. Type the userid to use when connecting to the Connect:Direct server. This field is case-sensitive.

Parameter	Description
Password for API	**Required**. Type the associated password for the userid. This is the password that allows you to connect to the Connect:Direct server. This field is case-sensitive.
API host DNS name	**Required**. Type the DNS name of the host where the Connect:Direct server is located, or the IP address in the form nnn.nnn.nnn.nnn.
API port	**Required**. Type the 1–5 digit port number that Connect:Direct File Agent uses to connect to the Connect:Direct server API. If you do not specify a port number, the default port number, 1363, is used.
Gate Keeper port	**Required**. Type the 1–5 digit port number that Connect:Direct File Agent uses to connect to the gate keeper. Use any available port number higher than port 10000. If you do not specify a port number, the default port number, 65530, is used. The first File Agent to connect to the gate keeper port keeps track of watched directories to ensure that only one File Agent is monitoring a location.
Watched directories	**Required**. Type an operating system-specific, valid entry on a line to indicate a location to watch. Use multiple lines to specify multiple locations to watch. You can skip lines for readability; File Agent ignores blank lines. For Windows or UNIX, type the path to the directory to watch. For z/OS systems, specify any of the following types of entries to indicate the location to watch: ◆ A fully specified HFS pathname of a directory ◆ A fully specified MVS data set name, such as HLQ.MONTHLY.PAYROLL ◆ A partial MVS data set name, such as HLQ.MONTH%%.PAY** ◆ A partitioned data set (PDS) name or a partitioned data set extended (PDSE) name File Agent uses the date to determine when a PDS member or dataset was modified. With a PDS member, the last modification date is used. For an executable file, File Agent looks at members of a load module PDS to determine their binder link date. If no date is found, File Agent uses the creation date of the PDS where it resides. When matching patterns in z/OS, the percent sign (%) matches a single character, the single asterisk (*) matches a single node level, and two asterisks (**) match all node levels from the point of placement. Refer to the appropriate operating system manuals for information about pattern matching rules. When a VSAM file is created on a z/OS system, three files are generated: the actual data file, an index file, and a cluster file. To prevent File Agent from triggering a process for each of these files, be sure your naming rules specify on the data file. For an example of handling this behavior, refer to *Detecting a VSAM Data File Added to a Watched Directory on a z/OS System* on page 15.
Monitor sub directories	Select Yes (the default) to monitor the Watched directories and sub-directories, or select No to monitor the Watched directories only.

Parameter	Description
Continuous signon	Select Yes to stay connected to the API port whenever Connect:Direct File Agent is active, or select No (the default) to have File Agent disconnect and reconnect each time Processes are submitted after a directory scan. File Agent scans the directories, then submits Processes for any files found during the scan. If Continuous signon is No, File Agent will sign on to the Connect:Direct server the first time it submits a Process for a file found during the scan, and will close the connection to the Connect:Direct server when all Processes have been submitted for files found during the scan. When files are found during a subsequent scan, File Agent will open a new connection to the Connect:Direct Server. Use this option if there are more than a few minutes between files being placed in the watched directories. If Continuous signon is Yes, File Agent will open a new connection to the Connect:Direct Server the first time that a Process is submitted for a file found during the scan, and will leave that connection to the Connect:Direct server open until File Agent is stopped. Use this option if files are placed in the watched directories more or less continuously.
Gate keeper DNS name	Type the name of the host for the File Agent gate keeper, or the IP address in the format nnn.nnn.nnn.nnn. The gate keeper keeps track of watched directories so that the same directory is not watched by more than one File Agent. When multiple File Agents are running, the first File Agent to connect to the gate keeper port becomes the gate keeper. A gate keeper is not required if only one File Agent is running or if each watched directory is only listed in the configuration of one File Agent instance. To disable the gate keeper, set this parameter to blank: the gate keeper port is ignored. If multiple instances of File Agent monitor the same network directory, a gate keeper DNS name must be provided.
Default Process	Type the name of the Process to submit when a file is detected by Connect:Direct File Agent. This default Process is submitted if there is not a rule defined for the file. **Note:** The userid and password used to submit the default Process must be the same as those used to connect to the Connect:Direct server. On z/OS systems, the default Process is specified as the Member Name in DMPUBLIB. On Windows or UNIX, this includes directories in the path to the Process and the name of the Process file. File Agent must have read access to the path and file on Windows and UNIX. In addition, the userid and password used to submit the default Process must match the userid and password used to connect to the server.

Parameter	Description
Default arguments	Type the argument string that will be passed to the default Process. When arguments contain special characters, enclose the argument string in double quotes. See *Using File Agent Variables* on page 30 for a description of all variables File Agent supports as default arguments. For example, in Windows, type **&ARG1="%FA_FILE_FOUND."** to assign the path and filename of the file that File Agent detected passed as the symbolic variable &ARG1 to the Process that File Agent submits. The leading percent (%) and ending period (.) are required with all variables. See *z/OS Process Arguments Example* on page 33 for examples of variable use.
Error Process	Type the name of the Process to submit when an internal code error occurs in Connect:Direct File Agent, such as a java.lang.null pointer exception. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Windows or UNIX, this is the pathname of the file that contains the Process. File Agent must have read access to the path and file on Windows or UNIX.
Error Arguments	Type the argument string that will be passed to the error Process. File Agent uses only the following variable. Using any other variable produces undefined results. The leading percent (%) character and the ending period (.) are required. %FA_FILE_FOUND. — The default value is the full text of the Exception message.
Process Class	**Required.** Type the numeric class that the Process submitted to the Connect:Direct server should use for execution. The Process class number is a value between 1-255 and is used to determine the order in which a Process is executed. Refer to Connect:Direct documentation for more information.
Process Priority	Type the numeric priority to use for execution of the Process File Agent submits to the Connect:Direct server. The Process priority is a number between 0-15 that determines the order of Process execution. Refer to the Connect:Direct documentation for more information.
Watch file interval	Type the number of minutes that you want Connect:Direct File Agent to wait before checking the watch directories for files. By default, Connect:Direct File Agent checks the watch directories for files once each minute. This field specifies how long File Agent waits between directory scans. If you need to transfer files quickly after they are placed into the watched directories, specify a short Watch file interval. However, if there aren't many files placed into the watched directories, set a longer Watch file interval so that File Agent is not scanning the watched directories as often. There is a trade-off between the processing time that File Agent uses to scan the directories and the need to transfer the files quickly.

Parameter	Description
File completion delay	Type the number of minutes that you want Connect:Direct File Agent to wait before a detected file is considered to be complete.This field is optional. The default time is 1 minute. This field only applies to UNIX systems. With many UNIX applications, different tasks can access the same file simultaneously. This may cause problems if Connect:Direct File Agent detects that a file is present in the watched directory and uses it before another application has closed it. Set this delay to allow an application to finish with the file before Connect:Direct File Agent accesses the file.
File Agent unique name	**Required**. Provide a unique name for each File Agent instance running on the same host or on a different host, while monitoring similar network drives, and configured to submit processes to the same Connect:Direct node. This ensures the unique identity of each File Agent instance by Sterling Control Center. Failing to do so results in Control Center treating multiple instances of File Agent as one.
SNMP listener address	Type the address for the SNMP trap receiver, such as Sterling Control Center. Connect:Direct File Agent uses this address to send SNMP traps for statistics. This field is optional. You can obtain this information from your Sterling Control Center system administrator.
SNMP listener port	Type the port used by the SNMP trap receiver, such as Sterling Control Center. Port 1163 is the default. This field is optional.
SNMP source port range	Type the ports or port ranges used to pass through a firewall to the SNMP trap receiver, such as Sterling Control Center, when File Agent runs behind a firewall. You can specify a maximum of 5 port ranges. This field is optional. Type the ranges in the format nnnn-nnnn, separated by commas, for example, 5555-7777, 8888-8890, 9999. Contact the Sterling Control Center system administrator if you do not know this information.
Refresh Configuration	Select Yes to refresh the configuration after modifying the configuration without restarting File Agent. The default setting is No. **Note:** The Gate Keeper port setting will not be refreshed unless you restart File Agent.

4. Click **Save**. If the file is complete, the listing for Default_Config changes from red to black to indicate that the configuration file has been created and is ready for use.

If you leave any required fields blank, a dialog box displays to list those fields. Click **Cancel** to supply the missing information. Incomplete configuration files can be saved, but cannot be used for Connect:Direct File Agent operation.

Note: Incomplete configuration files are saved as .inc files in the File Agent installation directory and are listed in red in the Configurations window of the configuration interface.

5. If you have made changes that you have not saved, a save confirmation dialog box appears. Click **OK** to save the changes.
6. Click **Exit**. If you have made changes that you have not saved, an exit confirmation dialog box appears. Click **OK** to save the changes and exit the configuration interface.

The **Refresh Configuration** option is dynamic. You can select **Yes** or **No** and File Agent will detect the option when you change the configuration. If you select **No**, you must restart File Agent for the configuration changes to take effect.

Verifying the Default Configuration

To start File Agent in verbose mode and verify that the configuration is working correctly:

1. Start Connect:Direct File Agent from the command line with your Default_Config.ser file:

Note: The command parameters are case-sensitive.

- On a Windows computer, type **cdfa -v -cdefault_config.ser** at a command prompt.

Note: If you want to display the parameters on the title bar of the command window, type **cdfa1.bat -v -cdefault_config.ser** at a command prompt.

- On a UNIX computer, type **cdfa -v -cDefault_Config.ser** at a command prompt.
- On a z/OS computer, add the following parameters to the Execution job on the $FAJAVA line and submit the Execution job:

```
$FAJAVA -Dsci.config=FAconfiguration -jar fasat.jar -cdefaultconfig.ser
```

See *Running Connect:Direct File Agent in a z/OS Environment* for a sample File Agent execution job.

2. Copy a file to the watched directory. The directory **C:\watch** is used in this example.
3. Verify that the log displays information similar to the following, depending on your operating system and the name of the watched directory and the file you copied to it.

As the following sample from a Windows log shows, Connect:Direct File Agent did not detect a file during the scan of the C:\watch directory at 4:01:34. However, the scan at 4:02:34 detected a file, C:\watch\dailyreport, and one command was attempted and accepted.

```
October 22, 2005 4:01:34 PM CST   94 Thread[Thread-0,5,main]      Product
"Connect:Direct File Agent" is active with 5 services.

Connect:Direct Version 1.00.08 Copyright Sterling Commerce Inc. 2003 - 2006, GA
fix 00000000 Date 2005/02/10
Connect:Direct Copyright Sterling Commerce Inc. 2003 - 2005, GA fix 00000000 Date
2005/09/23
November 22, 2005 4:01:34 PM CST  665 Thread[FADron1 /FILAGEN,5,main]  Processing
directory: "C:\watch"
November 22, 2005 4:01:34 PM CST  665 Thread[FADron1 /FILAGEN,5,main]  Completed
directory: "C:\watch"
November 22, 2005 4:01:34 PM CST  665 Thread[FADron1 /FILAGEN,5,main]  directory
scan ending, commands attempted 0, commands accepted 0
November 22, 2005 4:02:34 PM CST  673 Thread[FADron1 /FILAGEN,5,main]  Processing
directory: "C:\watch"
November 22, 2005 4:02:34 PM CST  693 Thread[FADron1 /FILAGEN,5,main]  New file
found is: "C:\watch\dailyreport 11/24/2003 16:58:58"
November 22, 2005 4:02:34 PM CST  693 Thread[FADron1 /FILAGEN,5,main]  Completed
directory: "C:\watch"
November 22, 2005 4:02:34 PM CST  944 Thread[FADron1 /FILAGEN,5,main]  directory
scan ending, commands attempted 1, commands accepted 1
. . .
```

If the log does not validate the configuration, see *Troubleshooting* on page 85, and contact your system administrator to verify the information for the required parameters.

Using File Agent Variables

To pass file details to the Process that Connect:Direct File Agent submits, you can specify the appropriate variable in the **Default arguments** field on the **File Agent** tab of the File Agent configuration interface.

Observe the following rules when you specify variables:

- The starting percent sign (%) and the ending period (.) shown with variables are required.
- Enclose argument strings that contain special characters in double quotes.
- Enclose spaces and vertical bars in double quotation marks to avoid problems when variables are passed to a Connect:Direct Process.

Usage	Variable	Description
All Operating Systems		
Path and file	%FA_0. to %FA_99.	The number included in this variable represents a component of the name of the detected file, as delimited by the file delimiter, in sequence. For example, if the full file name is /usr/watch/test file.active.txt, then %FA_0 is usr, %FA_1 is watch, and so on.
	%FA_FILE_FOUND.	On Windows and UNIX, the default value is the path and file name of the detected file. On z/OS systems, the default value is the entire name of the file that File Agent detected, including any member name. This variable supports PDSE long member names. For example, when you specify this variable, File Agent could pass the following member name: CUST.BENEFITS(PAYROLLPDSELONGNAME).
Current date and time	%FA_DATE.	The current date for the detected file. This value has 8 characters that represent the year, month, and day, for example, 20040903.
	%FA_DATE_DAY.	The current day, for example, 31.
	%FA_DATE_MONTH.	The current month, for example, 01.
	%FA_DATE_YEAR.	The current year, for example, 2004.
	%FA_NUM.	The millisecond timestamp. If multiple files are sent within the same second, they will get different millisecond values, for example, 13143512345, 13143512346, and 13143512347.
	%FA_TIME.	The current time. This value has 6 characters to represent the hour, minutes and seconds (format (hhmmss) using a 24-hour clock.
	%FA_TIME_HOUR.	The current hour, for example, 13.
	%FA_TIME_MINUTES.	The current minute, for example, 24.
	%FA_TIME_SECONDS.	The current second, for example, 35.

Usage	Variable	Description
Modification date and time	%FA_FDATE.	The date a detected file was last modified. This value has 8-characters representing year, month, and day, for example, 20040903.
	%FA_FDATE_DAY.	The day a file was last modified, for example, 21.
	%FA_FDATE_MONTH.	The month in which a file was last modified, for example, 09.
	%FA_FDATE_YEAR.	The year in which a file was last modified, for example, 2004.
	%FA_FTIME_HOUR.	The hour a file was last modified, for example, 22.
	%FA_FTIME_MINUTES.	The minute a file was last modified, for example, 24 will be passed for a file last modified at 6:24.
	%FA_FTIME_SECONDS.	The second a file was last modified, for example, 35.
	%FA_FTIME.	The time a file was last modified. This value has 6-characters representing hour, minutes, and seconds (hhmmss) using a 24-hour clock, for example, 153842.
UNIX and Windows		
File name and path	%FA_EXT_FOUND.	On Windows and UNIX, the file extension of the file that was added, for example, .txt.
	%FA_EXT_FOUND_NP.	On Windows and UNIX, the file extension of the file that was added, but without the period before the file extension. For example, if the file added is file.txt, using the %FA_EXT_FOUND_NP variable will result in txt being passed (the extension with no period included).
	%FA_NAME_FOUND.	On Windows and UNIX, the name of the file that was added, for example, myfile.
	%FA_NOT_PATH.	On Windows and UNIX, the file name with the file extension, without any path. For example, if the full file name is /usr/watch/test file.active.txt, then %FA_NOT_PATH. is resolved as test file.active.txt.
	%FA_PATH_FOUND.	On Windows and UNIX, the path of the file that was added, for example, on Windows, C:\watch\, and on UNIX, /home/user/watch.
Windows Only		
	%FA_DRIVE_FOUND.	On Windows, the default value is the drive where the added file is located, for example, C:.
z/OS systems		

Usage	Variable	Description
File and member	%FA_BASEFILE_FOUND.	The default value is the name of the file that was added, without the member name. This variable is only valid for PDS on z/OS operating systems, for example, CUST.BENEFITS.
	%FA_MEMBER_FOUND.	The default value is "." This variable is only valid for PDS on z/OS operating systems. PDSE long member names are supported. For example, the following member name is valid: PAYROLLPDSELONGNAME.

Windows or UNIX Process Arguments Example

The following example demonstrates the operation of File Agent variables as Process arguments on a Connect:Direct server running UNIX.

The following arguments were specified in the **Default arguments** field of the configuration:

&F="%FA_FILE_FOUND."

Note: The variable &F must be included in the default Process to perform the necessary tasks after the File Agent detects a new file.

When the file payroll.txt appears in watched directory home/watch1/, then File Agent passes the following argument string to the default Process: &F=/home/watch1/payroll.txt.

z/OS Process Arguments Example

For example, if you type the following Process arguments:

&BASEFILE="%FA_BASEFILE_FOUND. &MEMBER=%FA_MEMBER_FOUND. &FILE=%FA_FILE_FOUND."

The following argument strings are submitted to the Process:

- The watched directory (a PDS) is CUST.PROCLIB and member PAYROLL changes. File Agent passes the following to the associated Process:

  arg string= &BASEFILE="CUST.PROCLIB &MEMBER=PAYROLL &FILE=CUST.PROCLIB(PAYROLL)"

- The watched directory file is CUST.*, and member BENEFITS of PDS CUST.PARMFILE changes. File Agent passes the following to the associated Process:

  arg string= &BASEFILE="CUST.PARMFILE &MEMBER=BENEFITS"

- The watched directory is CUST.GDGBASE.* and CUST.GDGBASE.G0223V00 is created. File Agent passes the following to the associated Process:

  arg string= &BASEFILE="CUST.GDGBASE.G0223V00 &MEMBER=."

Overriding the Default Configuration with Rules

Rules enable you to define conditions that override the operation defined by the default File Agent configuration. When you specify rules for a configuration, File Agent monitors one or more watched directories, but also performs some additional steps:

- Instead of only monitoring watched directories for file activity, File Agent also checks for the criteria specified in a rule.
- Instead of submitting the default Process for the configuration after detecting activity in a watched directory, File Agent submits the Process specified for the first rule for which all criteria match.

Rules are not required; they are an option available for overriding the default Process when you need to perform specific actions after File Agent detects certain conditions. You must define the conditions as criteria for a File Agent rule. File Agent can check criteria for two types of rules: system event rules and submit Process rules (watched file event rules).

During internal processing, Connect:Direct File Agent detects significant system events, for example exception errors, which can be processed against rules. You can design a rule to test for an exception event and if the event is detected, submit a Process designed to perform appropriate actions in response to that exception event. See *Creating a System Event Rule* on page 43 for more information. You can also create rules to test for events that are written to the system log.

When a configuration file rules specified and Connect:Direct File Agent detects a file in a watched directory, it submits the default Connect:Direct Process to the Connect:Direct server. Typically, the default Connect:Direct Process contains generic processing steps that can be applied to a variety of files. You can create a watched file event rule (Submit Process rule) to have File Agent submit a specified Process after detecting a file that matches certain criteria. Watched file event rules enable more refined filtering of files in watched directories and submission of a Connect:Direct Process that performs actions required after detecting a particular type of file. See *Creating and Validating a Watched File Rule* on page 37 for a sample watched file event rule.

Match Criteria and Operators

A File Agent rule includes one or more match criteria and operators that specify how Connect:Direct File Agent evaluates a compare string against a detected file or system event. The Process specified for a rule is submitted to the Connect:Direct server only when the evaluation results in a match.

Match criteria and compare string define the conditions that Connect:Direct File Agent checks for. For a submit Process rule, match criteria are based on the file name or file size of the file that File Agent detects in a watched directory. For a system event rule, match criteria are based on the title or the contents of a system event.

Note: System event rules based on event contents are for use when File Agent can analyze a stack trace for the event. Some system events may not qualify.

Operators define how File Agent tests for the match criteria using the compare string to evaluate properties of a detected file (watched file event rule) or a system event (system event rule). Each

rule can have one or more match criteria. If you define more than one criterion to match in a rule, all criteria must be met before the rule is processed.

Review the operator functions in the following table for information about how rules are processed, the guidelines for creating rules, and perform the procedures in *Creating and Validating Rules* on page 37 before you attempt to create File Agent rules.

Operator	Function
Matches	Use to define a rule which specifies that File Agent searches only the directory specified by the path for the file name or the system event that match the specified compare string exactly. The compare string can include the wildcard characters asterisk (*) and question mark (*?). For example, typing c:\devfiles\quality\test* as the string to match causes File Agent to process the rule after detecting any file name beginning with test in the c:\devfiles\quality directory. The matches operator requires an exact match for any character except wildcards. This operator requires careful planning to filter files successfully. Unless you match only on the end of a file name, you must include the path as part of the match string. For example, *.txt will correctly match any file in the watch directory ending in .txt. However, 09*.txt will not match on a file 09March.txt. Instead, use: <*watch directory pathname*>/09*.txt where <*watch directory pathname*> is the full path to the watch directory, such as c:\devfiles\quality\09*.txt.
Not matches	Use to define a rule based on characters you want to exclude. The path and file name or system event are checked against the compare string so that File Agent processes the rule when it detects any characters other than those specified in the string. The compare string can include the wildcard characters asterisk (*) and question mark(?).
Contains	Use to define a rule in which File Agent searches all directories and subdirectories in the watched directory for the file name or system event that contains the text specified as compare string. This is the most versatile operator because it requires only that the compare string exists in any position within the string.
Equals	Use to define an exact match between the fully qualified path and file name or size of the detected file or the title or contents of a system event and the text string or size specified for comparison. This operator requires an exact match for every character position, so it should be used only when you know the entire file name. **Note:** Do not use this operator to match 0-byte files.
Less than	Requires that the detected file is smaller than the size specified for comparison. **Note:** To match a 0-byte file, you must specify **1** in the **Compare size** field with the **Less than** operator.
Greater than	Requires that the detected file is larger than the size specified for comparison.

Rules Processing

Override the default Process specified in the default configuration by including one or more rules when you want to address specific file processing needs. Although you create rules to define conditions for File Agent to detect, it is the Connect:Direct Processes associated with rules that perform actions to accomplish tasks. You can enable and disable rules by selecting or clearing the **Enabled** check box on the **Rules** tab of the configuration interface.

Defining rules can be challenging, and requires understanding of networks, operating systems, and Connect:Direct. The understanding of Connect:Direct Processes is essential because the Connect:Direct File Agent component simply performs monitoring; Processes submitted to the Connect:Direct server accomplish the actions you want performed.

Connect:Direct File Agent processes rules as follows:

- Only enabled rules are searched.
- Rules are searched in the order that they are listed on the **Rules** tab.
- Only enabled match criteria are tested.
- When match criteria are met for a rule, that rule is processed and no further rules processing is performed. File Agent executes a maximum of one rule for each file or system event detected.
- When a file matches a rule but the rule specifies no Process, nothing happens.

Guidelines for Defining Rules

Observe the following guidelines when you define rules:

- When you create multiple rules of the same type, define the rule with the most specific criteria first because rules are searched in the order that they are created. The rule hierarchy is displayed on the associated **Rules** tab. If the first rule listed is general, there will always be a match, and subsequent rules will never be processed.

  For example, assume that you need to create the following two rules:

  - One rule tests for all files that start with the text string *pay.*
  - Another rule test for all files that start with the text string *pay* and are larger than 2000 bytes.

  Because the second rule has the more specific criteria, you must create it first so that it is listed first on the **Submit Process rules** tab; otherwise, it will never be processed.

  Note: You can change the order of the rules listed on the **Rules** tab. Refer to *Reordering Rules* on page 45 for instructions.

- Create and validate one rule at a time to verify that the rules produce the expected result.

Creating and Validating Rules

Before you put Connect:Direct File Agent in a production environment, complete the following procedures to create and validate rules.

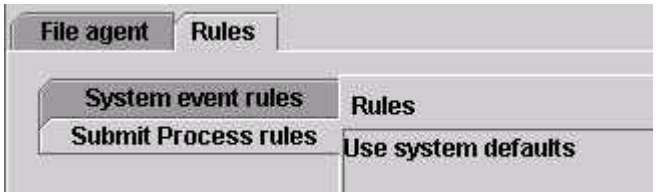
Creating and Validating a Watched File Rule

Complete the following procedures to create and validate a watched file rule (submit Process rule) that tests for a file name that contains a text string, for example, *daily*, and submits the default Connect:Direct Process, for example, *C:\daily.cdp*.

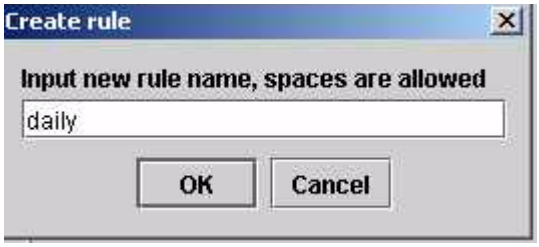
Creating a Watched File Rule

Complete the following procedure to create and validate a watched file rule that tests for a file name that contains a specified string:

1. Select the Default_config file from the Configurations window.
2. Click the **Rules** tab.



3. Select the **Submit Process rules** tab and click **New**. The **Create rule** dialog displays.

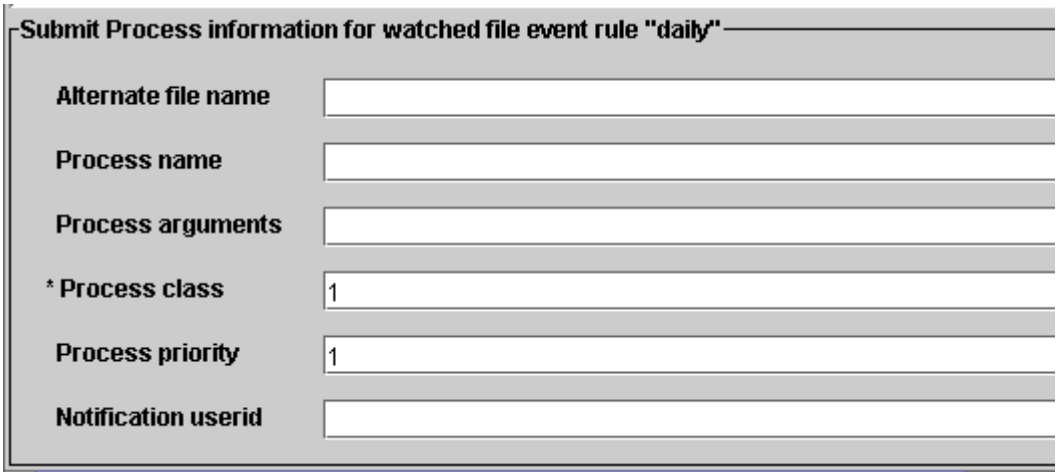


4. Type a name for the rule and click **OK**. The sample rule defined in this example is named *daily*. The rule is added to the list of rules.
5. Select the rule and click **Edit**.

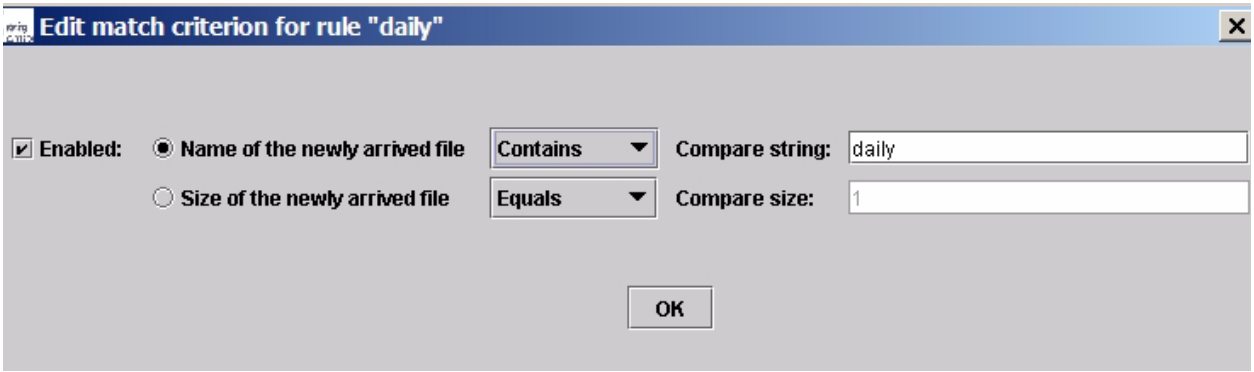
The Match criteria list (top) and the Submit Process information (bottom) display in the right pane of the GUI. These two areas must contain information as follows for the rule:

- Match criteria list—A list of conditions that must be met before the rule is applied to the detected file or event.

- Submit Process information—These parameters specify the Process File Agent submits to the Connect:Direct server. This Process is submitted only when there is a match for the associated rule.



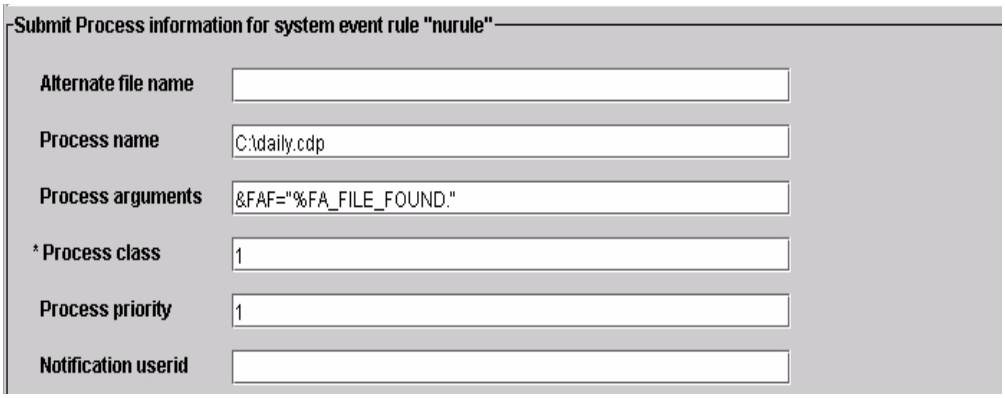
6. Choose the first item in the Match criteria list and click **Edit match**. The Edit match criterion window is displayed.



7. Click **Enabled** to enable the match criterion.

8. Click the option that indicates the property of the file to test. You can match either the name or the size of the newly arrived file. In this example, the option **Name of the newly arrived file** is selected.
9. Click the **Matches** arrow to display the drop down list of operators. In this example, **Contains** is selected as the operator for the match criterion.

   Using Contains as the operator enables File Agent to search all subdirectories in the watched directory and to match for the name of the file in the compare string in any position (beginning, end, or middle) for a match. Characters other than those specified in the compare string can be included before and after the string and an exact match is not required. See *Match Criteria and Operators* on page 34 for details about using other operators.
10. Type the portion of the file name you expect File Agent to detect in the **Compare string** field, for example, **daily**. Include the absolute path of the file. When the compare string is correct, click **OK** to close the Edit match criterion window.
11. Define the Process information in **Submit Process information**.



   In this example, File Agent submits the Process C:\daily.cdp to the Connect:Direct server. Specify the following Process arguments: **&FAF="%FA_FILE_FOUND."**

   File Agent passes the path and file name for the detected file to the symbolic variable &FAF; this variable is included in the Connect:Direct Process (c:\daily.cdp) that File Agent submits.

Parameters you can specify in the Submit Process information section operate as described in the following table:

Parameter	Description
Alternate file name	Type the name of an alternate file to process for this event. If you specify an alternate file name, File Agent uses the name of alternate file instead of the name of the file detected in a watched directory. That is, File Agent evaluates variables against the alternate file name and when submitting a Process, passes the results to the Process as arguments. For example, with the alternate file name alt.txt specified, File Agent detects the file q1sales.txt in watched directory c:\reports\ as a match for an enabled rule. Although the argument string &F="%FA_FILE_FOUND." is specified as the Process arguments, File Agent will pass the string alt.txt to the Process it submits. With no alternate file name specified, File Agent would pass c:\reports\q1sales.txt to the Process submitted after detection, as specified by the File Agent variable (%FA_FILE_FOUND.).
Process name	Type the name of the Process to submit. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Windows and UNIX, this is the path and file name of the file that contains the Process. File Agent must have read access to the path and file on Windows or UNIX. Type an asterisk in this field to copy the default Process name from the **File Agent** tab.
Process arguments	Type the Process variable and argument string that will be passed to the Process specified by the rule. For example, type: **&F="%FA_DATE."** to have the current date for the detected file passed as the symbolic variable &F to the Process that File Agent submits. File Agent allows use of the variables described in *z/OS Process Arguments Example* on page 33. The leading percent (%) character and the ending period (.) are required for all variables. When arguments contain special characters, enclose the argument string in double quotes.
Process Class	Type the numeric class that the Process submitted to the Connect:Direct server should use for execution. This can be a value between 1-255 and is used to determine the order in which a Process is executed. For more information, refer to the Connect:Direct documentation for your platform.
Process Priority	Type the numeric priority that the Process submitted to the Connect:Direct server should use for execution. This can be a value between 0-15 and is used to determine the order in which a Process is executed. Refer to Connect:Direct documentation for more information.
Notification userid	Type the userid to notify when the Process completes if your platform is configured to support notification. If this field is blank, or if your platform is not configured to support notification, no user is notified.

12. After specifying parameters on the Submit process information window, click **Done** under the Match criteria list.
13. The **Rules** tab is displayed again, with the rule listed. However, you must enable the rule before Connect:Direct File Agent can use it.
14. Click the **Enabled** check box on the right to enable the rule.
15. Click **Save** to save the configuration file.

The **Refresh Configuration** option is dynamic. You can select **Yes** or **No** and File Agent will detect the option when you change the configuration. If you select **No**, you must restart File Agent for the configuration changes to take effect.

Validating a Watched File Rule

After you define a watched file rule, complete the following procedure to validate that it works correctly before you add more rules:

1. Start Connect:Direct File Agent from the command line with the Default_Config.ser file, which now contains a rule:
   - On a Windows computer, type **cdfa -cdefault_config.ser** at a command prompt to start Connect:Direct File Agent.

     Note: If you want to display the parameters on the title bar of the command window, type **cdfa1.bat -cdefault_config.ser** at a command prompt.

   - On a UNIX computer, type **cdfa -cDefault_Config.ser** at a command prompt to start Connect:Direct File Agent.
   - On a z/OS computer, you must edit the script for the Execution job if you want to specify which configuration file to use. Type the command parameter and the configuration file name on the $FAJAVA line and then submit the Execution job.

     Note: The command parameters are case-sensitive.

2. Create a file with the word you specified in the compare string (for example, *daily)* in the name and copy it to the watched directory you specified in *Creating the Default Configuration File* on page 24.
3. Confirm that the Process (for example, daily.cdp) that you want to use for testing has been created on the Connect:Direct server.

4. Verify that the log displays information similar to the following sample. Some lines may differ from the example because of operating system differences and the use of different parameter definitions.

```
...
Connect:Direct Copyright Sterling Commerce Inc. 2003 - 2004, GA fix 00000000 Date
2004/03/12
November 22, 2004 3:51:33 PM CST  663 Thread[FADron1 /FILAGEN,5,main]  Processing
directory: "C:\watch"
November 22, 2004 3:51:33 PM CST  663 Thread[FADron1 /FILAGEN,5,main]  Completed
directory: "C:\watch"
November 22, 2004 3:51:33 PM CST  663 Thread[FADron1 /FILAGEN,5,main]  directory
scan ending, commands attempted 0, commands accepted 0
November 22, 2004 3:52:33 PM CST  671 Thread[FADron1 /FILAGEN,5,main]  Processing
directory: "C:\watch"
November 22, 2004 3:52:33 PM CST  691 Thread[FADron1 /FILAGEN,5,main]  New file
found is: "C:\watch\dailyreport 11/24/2003 16:58:58"
November 22, 2004 3:52:33 PM CST  771 Thread[FADron1 /FILAGEN,5,main]  The
matching rule criteria and actions are :
Rule (daily) type(watch_file)
 Match Criteria (Enabled: Name of the newly arrived file Contains  "daily"      )
End Match Criteria

RuleAction type(watch_file) email(false) transfer(false) store(false)
emailattachfile(false) emailID() emailSubject(An email notification from the
CONNECT:Direct Remote Agent) emailBody(A file event has occurred)
xStoreFileName(null) xStoreEncoding(null) xStoreNewEncoding(null)
xEmailFileName(null) xEmailEncoding(null) xEmailNewEncoding(null)
xCDSnodeUid(null) xCDSnodeFileName(null) xCDPnodeFileName(null)
xCDXferType(null) xCDMBCSCodePage(null) xCDMBCSNewCodePage(null)
xCDMBCSLocalCodePage(null) xCDMBCSLocalNewCodePage(null) xCDCompress(null)
xCDCkpt(null) xCDDisp(null)
 priority(1) class(1) pnodeUid() pnodePwd(********) snodeUid() snodePwd(********)
notifyUid() pnodeAcct() snodeAcct() procName(C:\daily.cdp)
procArgs(&F=%FA_FILE_FOUND.) AltName()

 End Rule(daily)

November 22, 2004 3:52:33 PM CST  771 Thread[FADron1 /FILAGEN,5,main]  Completed
directory: "C:\watch"
November 22, 2004 3:52:34 PM CST   51 Thread[FADron1 /FILAGEN,5,main]  directory
scan ending, commands attempted 1, commands accepted 1
```

If the log does not validate the application of the rule, see *Troubleshooting* on page 85.

5. Repeat this procedure until you validate the rule.

   After you have validated this rule, you can add more rules one at a time. Be sure to validate each rule before adding another one.

Tip: The Connect:Direct File Agent system log for Windows may contain many lines of information, especially with multiple rule use. Instead of checking each line of the log, use a line editor or other utility to search for key phrases related to details you need to check. For example, use the Windows Notepad accessory to search for a rule name, directory path, or date.

Creating a System Event Rule

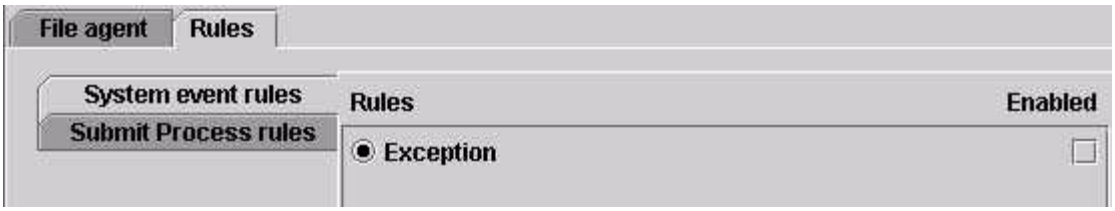
With a system event rule, File Agent compares a system event title or system event contents with the string you specify. An example of a system event title is RAAction for a remote agent action event. The contents of an event is something related to the event, such as a message. For example, the following message can be the contents of an event: `Process submitted to Connect Direct: File_Test.`

Use the following procedure to create a system event rule that tests for exception errors, submits a Process, and passes the text of the exception error to Connect:Direct.

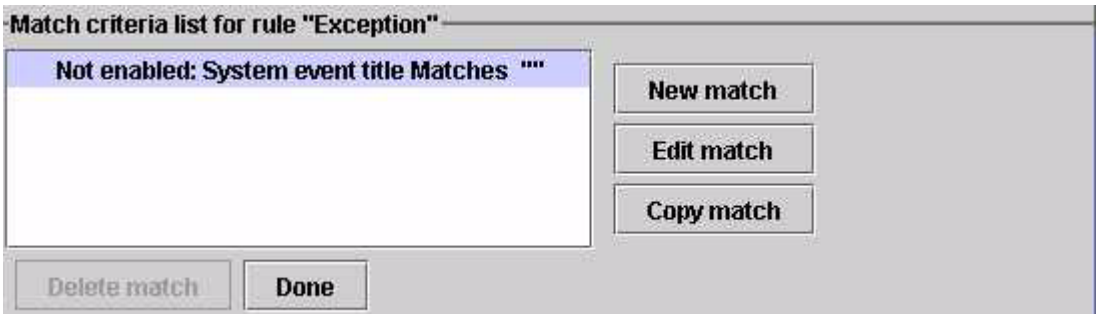
In this sample scenario, Connect:Direct File Agent submits a Process (ErrProc.cdp) to the Connect:Direct server when an Exception error event matches the rule named *Exception*.

1. Select the **Default_Config.ser** from the Configurations window.
2. Click the **Rules** tab.
3. Click **System event rules**.
4. Click **New** to create a new rule.
5. Type the name of the rule in the **Create rule** dialog box and click **OK**. For this example, the rule is called *Exception*.

6. Select the new rule you created and click **Edit**.



7. Click **Edit match** to modify the criteria for this rule.

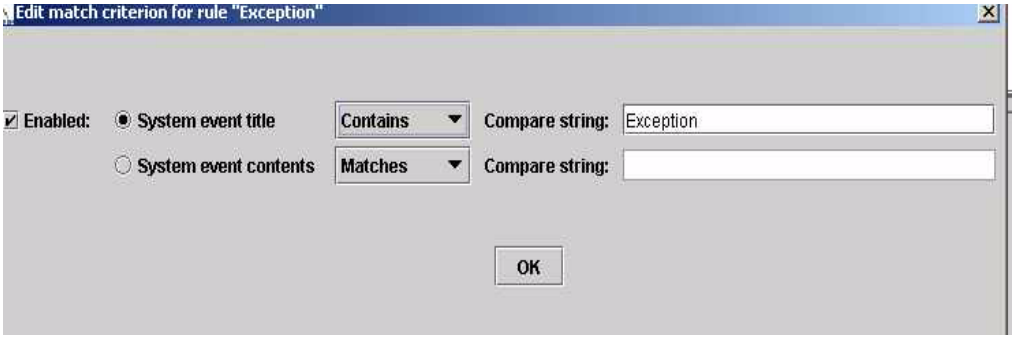


8. Click **Enabled** to enable your match criteria.

9. Select **System event title** and choose **Contains** as the operator.

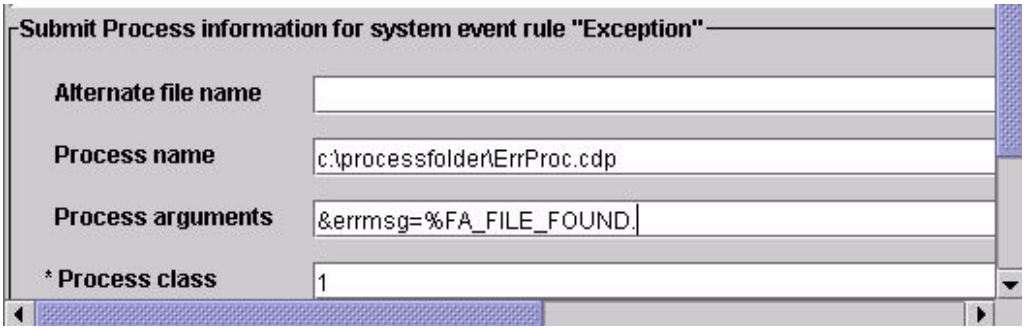
   The Contains operator tests for the characters of the string in a system event title. The characters must be in exact order, but they can occur in any position (beginning, middle, or end).

10. In the **Compare string** field, type **Exception** to check for a system event title that includes these characters. Using Contains for the match enables you to specify a portion of the event title without specifying all characters in the title. The compare string is shorter and the rule is more likely to be processed because you have allowed for flexibility in the matching.



11. Click **OK** to return to the rule definition.
12. Scroll to **Submit Process information** and enter the Process information as shown in the following example.

Note: For system event rules, the only valid Process argument variable is %FA_FILE_FOUND.



The Connect:Direct error Process specified in this sample scenario, ErrProc.cdp, contains the following code that defines a default value for the argument &errMsg= so that when you specify the variable &errMsg="%FA_FILE_FOUND.", File Agent passes the actual text of the error message to the Connect:Direct Process.

In the Process, a run task step calls a script that appends the message text to an Exceptions file; however, you can handle the exception text as necessary for your site:

```
/*BEGIN_REQUESTER_COMMENTS
    $PNODE$="EAST1_CHI" $PNODE_OS$="Windows"
    $SNODE$="EAST1_CHI" $SNODE_OS$="Windows"
    $OPTIONS$="WDOS"
  END_REQUESTER_COMMENTS*/

SYSLOG PROCESS
  &errMsg="'Default error message'"
  SNODE=EAST1_CHI

 RUN TASK PNODE (PGM=Windows)
  SYSOPTS="pgm(c:\temp\syslog.bat) args(&errMsg)"

PEND
```

13. Click **Done** to return to the **Rules** tab.
14. Click **Enabled** to enable the rule.
15. Click **Save** to update your changes to the configuration.

The **Refresh Configuration** option is dynamic. You can select **Yes** or **No** and File Agent will detect the option when you change the configuration. If you select **No**, you must restart File Agent for the configuration changes to take effect.

Reordering Rules

Complete the following procedure to reorder Submit Process rules and System event rules by moving up or down the hierarchy of rules.

1. On the **Rules** tab, select the rule you want to move.
2. Do one of the following:
   - To move the rule up one level, click **Up**.
   - To move the rule down one level, click **Down**.
3. Repeat steps 1 and 2 until the rules are in the desired order.
4. Click **Save**.
5. Click **OK** in the Save confirmation dialog box.

Note: The save confirmation dialog box only appears if there is unsaved data.

The **Refresh Configuration** option is dynamic. You can select **Yes** or **No** and File Agent will detect the option when you change the configuration. If you select **No**, you must restart File Agent for the configuration changes to take effect.

Connect:Direct File Agent Configuration File Hierarchy

When Connect:Direct File Agent is running as a Windows Service, it uses the Default_Config.ser configuration file. When it is started manually, Connect:Direct File Agent uses the following hierarchy to determine the configuration file to use:

- If you start Connect:Direct File Agent from a command line with the **cdfa -c***configurationfilename* command, Connect:Direct File Agent uses the specified configuration file. For example, **cdfa -cmonthend.ser** starts Connect:Direct File Agent with the configuration file named monthend.ser. See Appendix B, *Command Line Parameters*, for a list of command line parameters.
- If you do not specify the **-c** option with the **cdfa** command, Connect:Direct File Agent looks for a configuration file that matches the name of the computer it is running on. For example, if Connect:Direct File Agent runs on a computer named Host1, and a configuration file named Host1.ser exists in the File Agent directory, Connect:Direct File Agent uses the Host1 configuration file.

  On a Windows computer, you can view the computer name by selecting **Start>Settings>Control Panel>System** and selecting the **Computer Name** tab or **Network Identification** tab.

  For a UNIX or Linux computer, see the operating system documentation to determine how to find the computer name.
- If you do not specify the **-c** option with the **cdfa** command and there is no configuration file that matches the computer name, Connect:Direct File Agent uses the Default_Config.ser configuration file in the installation directory.

Chapter 3

Managing Configuration Files

After you define a default configuration, you can use the following procedures to manage configurations and rules:

- Creating a New Configuration File
- Editing a Configuration File
- Deleting a Configuration File
- Creating Multiple Configurations with the Copy Function
- Creating Multiple Configurations with the cdfa -g Command
- When you create multiple configuration files from the command line, observe the rules for using variables in the configuration template file.
- Locking a Configuration File for Distribution
- Copying a Rule
- Deleting a Rule
- Enabling and Disabling a Rule
- Editing a Rule
- Using Variables in Rules
- Saving a Configuration in a Text File

Managing Configurations

Use these procedures to add, edit, and delete configuration files and to create configuration files for mass distribution:

- Creating a New Configuration File
- Editing a Configuration File
- Deleting a Configuration File
- Creating Multiple Configurations with the Copy Function
- Creating Multiple Configurations with the cdfa -g Command

- ✦ When you create multiple configuration files from the command line, observe the rules for using variables in the configuration template file.
- ✦ Locking a Configuration File for Distribution

Creating a New Configuration File

You can add a new configuration file by copying, renaming, and changing the parameters for an existing configuration. You may need another configuration file to accommodate special-purpose processing, for example, for end-of-month processing or seasonal transaction activity. Using a different configuration file can also be helpful when you need to connect to a different Connect:Direct Server or submit Connect:Direct Processes with a different Process class and priority for execution. You can also create a new configuration so that you can test its operation without affecting the default configuration. New configuration files you create are saved with a .ser extension in the File Agent directory and are visible on the Configurations window of the File Agent configuration interface.

To create a new configuration file:

1. Select the file that you want to copy from the Configurations window.
2. Click **Copy** on the Configurations window.
3. Type the name of the new file in the **Copy configuration** dialog box and click **OK**.

   The configuration file is added to the Configurations window.
4. Select the new configuration file from the Configurations window. Click **Save** on the **File Agent** tab.
5. Click **Edit** on the **File agent** tab.
6. Change the **File Agent** tab settings as necessary. The following table describes all of the configuration file parameters. An asterisk (*) before a field name indicates a required parameter.

Parameter	Description
Comments	Type comments to describe the configuration. Comments are not used during the execution of File Agent.
Userid for API	**Required**. Type the userid to use when connecting to the Connect:Direct server. This field is case-sensitive.
Password for API	**Required**. Type the password to use when connecting to the Connect:Direct server. This field is case-sensitive.
API host DNS name	**Required**. Type the name of the host where the Connect:Direct server is located, or the IP address in the form nnn.nnn.nnn.nnn.
API port	**Required**. Type the 1–5 digit port number that Connect:Direct File Agent uses to connect to the Connect:Direct server API. If you do not specify a port number, the default port number, 1363, is used.

Parameter	Description
Gate Keeper port	**Required**. Type the 1–5 digit port number that Connect:Direct File Agent uses to connect to the gate keeper. Use any available port number higher than port 10000. If you do not specify a port number, the default port number, 65530, is used. The first File Agent to connect to the gate keeper port keeps track of watched directories to ensure that only one File Agent is monitoring a location.
Watched directories	**Required**. Type one or more directories or files. Type one fully qualified entry on each line. Blank lines are ignored to enhance readability. On Windows and UNIX, an entry can be the pathname of a file or a directory. On z/OS systems, an entry can be any of the following: ◆ A fully specified HFS pathname of a file ◆ A fully specified HFS pathname of a directory ◆ A fully specified MVS data set name, such as HLQ.MONTHLY.PAYROLL ◆ A partial MVS data set name, such as HLQ.MONTH%%.PAY** **Note:** When matching patterns in data set names, the % matches a single character, the single asterisk (*) matches a single node level, and the double asterisk (**) matches all node levels from the point of placement. Refer to the IBM document *DFSMS: Managing Catalogs (*SC26-7409-03) for information about using the catalog search interface with wildcards and other generic filter keys. You can specify a partitioned data set (PDS) or a partitioned data set extended (PDSE) in the watched directories field. File Agent uses the date to determine when a PDS member or data set was modified. With a PDS member, the last modification date is used. For an executable file, File Agent checks members of a load module PDS to determine their binder link date. If no date is found, File Agent uses the creation date of the PDS where it resides. When a VSAM file is created on a z/OS system, three files are generated: the actual data file, an index file, and a cluster file. To prevent File Agent from triggering a process for each of these files, be sure your naming rules specify on the data file. For an example of handling this behavior, refer to *Detecting a VSAM Data File Added to a Watched Directory on a z/OS System* on page 15.
Monitor sub directories	Select Yes (the default) to monitor the Watched directories and sub-directories, or select No to monitor the Watched directories only.

Parameter	Description
Continuous signon	Select Yes to stay connected to the API port whenever Connect:Direct File Agent is active, or select No (the default) to have File Agent disconnect and reconnect each time Processes are submitted after a directory scan. File Agent scans the directories, then submits Processes for any files found during the scan. If Continuous signon is No, File Agent will sign on to the Connect:Direct server the first time it submits a Process for a file found during the scan, and will close the connection to the Connect:Direct server when all Processes have been submitted for files found during the scan. When files are found during a subsequent scan, File Agent will open a new connection to the Connect:Direct Server. Use this option if there are more than a few minutes between files being placed in the watched directories. If Continuous signon is Yes, File Agent will open a new connection to the Connect:Direct Server the first time that a Process is submitted for a file found during the scan, and will leave that connection to the Connect:Direct server open until File Agent is stopped. Use this option if files are placed in the watched directories more or less continuously.
Gate keeper DNS name	Type the name of the host for the File Agent gate keeper, or the IP address in the format nnn.nnn.nnn.nnn. The gate keeper keeps track of watched directories so that the same directory is not watched by more than one File Agent. When multiple File Agents are running, the first File Agent to connect to the gate keeper port becomes the gate keeper. A gate keeper is not required if only one File Agent is running or if each watched directory is only listed in the configuration of one File Agent instance. To disable the gate keeper, set this parameter to blank: the gate keeper port is ignored. If multiple instances of File Agent monitor the same network directory, a gate keeper DNS name must be provided.
Default Process	Type the name of the Process to submit when a file is detected by Connect:Direct File Agent. This default Process is submitted if there is not a rule defined for the file. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Windows or UNIX, this is the pathname of the file that contains the Process. File Agent must have read access to the path and file on Windows or UNIX.
Default arguments	Type the argument string that will be passed to the default Process. File Agent uses the variables described in *z/OS Process Arguments Example* on page 33. The leading % character and the ending "." are required for variables.
Error Process	Type the name of the Process to submit when an internal code error occurs in Connect:Direct File Agent, such as a java.lang.null pointer exception. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Windows or UNIX, this is the pathname of the file that contains the Process. File Agent must have read access to the path and file on Windows or UNIX.
Error Arguments	Type the argument string that will be passed to the error Process. File Agent uses only the following variable. Using any other variable produces undefined results. The leading % character and the ending "." are required.

Parameter	Description	
	%FA_FILE_FOUND.	The default value is the full text of the Exception message.
Process Class	Type the numeric class that the Process submitted to the Connect:Direct server should use for execution. This can be a value between 1-255 and is used to determine the order in which a Process is executed. Refer to Connect:Direct documentation for more information.	
Process Priority	Type the numeric priority that the Process submitted to the Connect:Direct server should use for execution. This can be a value between 0-15 and is used to determine the order in which a Process is executed. Refer to Connect:Direct documentation for more information.	
Watch file interval	Type the number of minutes that you want Connect:Direct File Agent to wait before checking the watch directories for files. By default, Connect:Direct File Agent checks the watch directories for files once each minute. This field specifies how long File Agent waits between directory scans. If you need to transfer files quickly after they are placed into the watched directories, specify a short Watch file interval. However, if there aren't many files placed into the watched directories, set a longer Watch file interval so that File Agent is not scanning the watched directories as often. There is a trade-off between the processing time that File Agent uses to scan the directories and the need to transfer the files quickly.	
File completion delay	Type the number of minutes that you want Connect:Direct File Agent to wait before a detected file is considered to be complete.This field is optional. The default time is 1 minute. This field only applies to UNIX systems. With many UNIX applications, different tasks can access the same file simultaneously. This may cause problems if Connect:Direct File Agent detects that a file is present in the watched directory and uses it before another application has closed it. Set this delay to allow an application to finish with the file before Connect:Direct File Agent accesses the file.	
File Agent unique name	**Required**. Provide a unique name for each File Agent instance running on the same host or on a different host, while monitoring similar network drives, and configured to submit processes to the same Connect:Direct node. This ensures the unique identity of each File Agent instance by Sterling Control Center. Failing to do so results in Control Center treating multiple instances of File Agent as one.	
SNMP listener address	Type the address for the SNMP trap receiver, such as Sterling Control Center. Connect:Direct File Agent uses this address to send SNMP traps for statistics. This field is optional. You can obtain this information from your Sterling Control Center system administrator.	
SNMP listener port	Type the port used by the SNMP trap receiver, such as Sterling Control Center. Port 1163 is the default. This field is optional.	

Parameter	Description
SNMP source port range	Type the ports or port ranges used to pass through a firewall to the SNMP trap receiver, such as Sterling Control Center, when File Agent runs behind a firewall. You can specify a maximum of 5 port ranges. This field is optional. Type the ranges in the format nnnn-nnnn, separated by commas, for example, 5555-7777, 8888-8890, 9999. Contact the Sterling Control Center system administrator if you do not know this information.
Refresh Configuration	Select Yes to refresh the configuration after modifying the configuration without restarting File Agent. The default setting is No. **Note:** The Gate Keeper port setting will not be refreshed unless you restart File Agent.

7. Click the **Rules** tab to override the default behavior of Connect:Direct File Agent. When you copy a configuration file, any rules for the original configuration file are copied to the new configuration file.

   See *Guidelines for Defining Rules* on page 36 for information about setting up rules.

8. Click **Save**.

   If you left any required fields blank, a window is displayed listing the fields. You can either:

   - Click **Cancel**, then supply the missing information.
   - Click **OK** to save an incomplete configuration for future editing. Incomplete configurations are saved with .inc file extensions, and are displayed in red in the Configurations window. Connect:Direct File Agent cannot use an incomplete configuration.

9. Click **OK** in the Save confirmation dialog box.

   Note: The save confirmation dialog box only appears if there is unsaved data.

10. Click **Exit**.

    Note: An exit confirmation dialog box is displayed if there is unsaved data.

11. Start Connect:Direct File Agent.

    - On a Windows computer, type **cdfa -c*configfile*.ser** at a command prompt to start Connect:Direct File Agent, where *configfile* is the name of the configuration file you want to use.

      Note: If you want to display the parameters on the title bar of the command window, type **cdfa1.bat -c*config.ser***.

- On a UNIX computer, type **cdfa -c*configfile*.ser** at a command prompt to start Connect:Direct File Agent, where *configfile* is the name of the configuration file you want to use.
- On a z/OS system, you must edit the script for the Execution job if you want to specify which configuration file to use. You type the command parameter and the configuration file name on the $FAJAVA line. Then you can submit the Execution job.

Note: The command parameters are case-sensitive.

If Connect:Direct File Agent cannot connect to the Connect:Direct server, see *Troubleshooting* on page 85.

Editing a Configuration File

To edit a configuration file:

1. Select the file that you want to edit from the Configurations window.
2. Click the tab that you want to change (**File Agent** or **Rules**).
3. Click **Edit**.
4. Change the settings as necessary. See the parameter table in *Creating a New Configuration File* for definitions.
5. Click **Save** to save the updated configuration file.

   If you left any required fields blank, a window is displayed listing the fields. You can either:

   - Click **Cancel**, then supply the missing information.
   - Click **OK** to save an incomplete configuration for future editing. Incomplete configurations are saved with .inc file extensions, and are displayed in red in the Configurations window. Connect:Direct File Agent cannot use an incomplete configuration.
6. Click **OK** in the Save confirmation dialog box.
7. Click **Exit**.

Note: An exit confirmation dialog box is displayed if there is unsaved data.

The **Refresh Configuration** option is dynamic. You can select **Yes** or **No** and File Agent will detect the option when you change the configuration. If you select **No**, you must restart File Agent for the configuration changes to take effect.

Deleting a Configuration File

1. Select the configuration file that you want to delete from the Configurations window.
2. Click **Delete**.
3. Click **OK** in the Delete confirmation dialog box.

To restart the configuration interface with default values, delete all configurations, exit the Configuration window, and restart the configuration interface. The configuration is regenerated with the default values.

Creating Multiple Configurations with the Copy Function

Rather than have the Connect:Direct File Agent client sites create their own configurations, a Connect:Direct server site can create configuration files and distribute them to Connect:Direct File Agent client sites. This reduces the possibility of typing errors and ensures consistent configurations throughout the Connect:Direct network.

You can create multiple configuration files by copying an existing configuration file, naming the new configuration file, and changing the configuration information.

In the following procedure, assume that you want to create three new configuration files named FA1, FA2, and FA3 for distribution.

1. Select the file that you want to copy from the Configurations window.
2. Click **Copy**.
3. Type the name of the new file (**FA1**) in the Copy configuration dialog box and click **OK**.
4. Select the **FA1** configuration file from the Configurations window.
5. Click **Edit**.
6. On the **File Agent** tab, change the following fields.

Parameter	Description
Comments	Type comments to describe the configuration. Comments are not used during the execution of File Agent.
Userid for API	**Required.** Type the userid to use when connecting to the Connect:Direct server. This field is case-sensitive.
Password for API	**Required.** Type the password to use when connecting to the Connect:Direct server. This field is case-sensitive.
API host DNS name	**Required.** Type the name of the host where the Connect:Direct server is located, or the IP address in the form nnn.nnn.nnn.nnn.
API port	**Required.** Type the 1–5 digit port number that Connect:Direct File Agent uses to connect to the Connect:Direct server API. If you do not specify a port number, the default port number, 1363, is used.
Gate Keeper port	**Required**. Type the 1–5 digit port number that Connect:Direct File Agent uses to connect to the gate keeper. Use any available port number higher than port 10000. If you do not specify a port number, the default port number, 65530, is used. The first File Agent to connect to the gate keeper port keeps track of watched directories to ensure that only one File Agent is monitoring a location.

Parameter	Description
Watched directories	**Required**. Type a path (Microsoft Windows), pathname (UNIX) to specify a Windows or UNIX directory. Type one valid entry on each line. Blank lines are ignored to enhance readability. For z/OS systems, specify any of the following types of entries: ◆ A fully specified HFS pathname of a file ◆ A fully specified HFS pathname of a directory ◆ A fully specified MVS data set name, such as HLQ.MONTHLY.PAYROLL ◆ A partial MVS data set name, such as HLQ.MONTH%%.PAY** **Note:** When matching patterns in data set names, the % matches a single character, the single asterisk (*) matches a single node level, and the double asterisk (**) matches all node levels from the point of placement. Refer to the IBM document *DFSMS: Managing Catalogs (*SC26-7409-03) for information about using the catalog search interface with wildcards and generic filter keys. For z/OS systems, you can also specify a partitioned data set (PDS) or a partitioned data set extended (PDSE) in the watched directories field. File Agent uses the date to determine when a PDS member or data set was modified. With a PDS member, the last modification date is used. For an executable file, File Agent looks at members of a load module PDS to determine their binder link date. If no date is found, File Agent uses the creation date of the PDS where it resides. When a VSAM file is created on a z/OS system, three files are generated: the actual data file, an index file, and a cluster file. To prevent File Agent from triggering a process for each of these files, be sure your naming rules specify on the data file. For an example of handling this behavior, refer to *Detecting a VSAM Data File Added to a Watched Directory on a z/OS System* on page 15.
Monitor sub directories	Select Yes (the default) to monitor the Watched directories and sub-directories, or select No to monitor the Watched directories only.
Continuous signon	Select Yes to stay connected to the API port whenever Connect:Direct File Agent is active, or select No (the default) to have File Agent disconnect and reconnect each time Processes are submitted after a directory scan. File Agent scans the directories, then submits Processes for any files found during the scan. If Continuous signon is No, File Agent will sign on to the Connect:Direct server the first time it submits a Process for a file found during the scan, and will close the connection to the Connect:Direct server when all Processes have been submitted for files found during the scan. When files are found during a subsequent scan, File Agent will open a new connection to the Connect:Direct Server. Use this option if there are more than a few minutes between files being placed in the watched directories. If Continuous signon is Yes, File Agent will open a new connection to the Connect:Direct Server the first time that a Process is submitted for a file found during the scan, and will leave that connection to the Connect:Direct server open until File Agent is stopped. Use this option if files are placed in the watched directories more or less continuously.

Parameter	Description
Gate keeper DNS name	Type the name of the host for the File Agent gate keeper, or the IP address in the format nnn.nnn.nnn.nnn. The gate keeper keeps track of watched directories so that the same directory is not watched by more than one File Agent. When multiple File Agents are running, the first File Agent to connect to the gate keeper port becomes the gate keeper. A gate keeper is not required if only one File Agent is running or if each watched directory is only listed in the configuration of one File Agent instance. To disable the gate keeper, set this parameter to blank: the gate keeper port is ignored. If multiple instances of File Agent monitor the same network directory, a gate keeper DNS name must be provided.
Default Process	Type the name of the Process to submit when a file is detected by Connect:Direct File Agent. This default Process is submitted if there is not a rule defined for the file. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Windows or UNIX, this is the pathname of the file that contains the Process. File Agent must have read access to the path and file on Windows or UNIX.
Default arguments	Type the argument string that will be passed to the default Process. File Agent uses the variables described in *z/OS Process Arguments Example* on page 33. The leading % character and the ending "." are required.
Error Process	Type the name of the Process to submit when an internal code error occurs in Connect:Direct File Agent, such as a java.lang.null pointer exception. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Windows or UNIX, this is the pathname of the file that contains the Process. File Agent must have read access to the path and file on Windows or UNIX.
Error Arguments	Type the argument string that will be passed to the error Process. File Agent uses only the following variable. Using any other variable produces undefined results.The leading % character and the ending "." are required. %FA_FILE_FOUND. The default value is the full text of the Exception message.
Process Class	**Required.** Type the numeric class that the Process submitted to the Connect:Direct server should use for execution. This can be a value between 1-255 and is used to determine the order in which a Process is executed. Refer to Connect:Direct documentation for more information.
Process Priority	Type the numeric priority that the Process submitted to the Connect:Direct server should use for execution. This can be a value between 0-15 and is used to determine the order in which a Process is executed. Refer to Connect:Direct documentation for more information.

Parameter	Description
Watch file interval	Type the number of minutes that you want Connect:Direct File Agent to wait before checking the watch directories for files. By default, Connect:Direct File Agent checks the watch directories for files once each minute. This field specifies how long File Agent waits between directory scans. If you need to transfer files quickly after they are placed into the watched directories, specify a short Watch file interval. However, if there aren't many files placed into the watched directories, set a longer Watch file interval so that File Agent is not scanning the watched directories as often. There is a trade-off between the processing time that File Agent uses to scan the directories and the need to transfer the files quickly.
File completion delay	Type the number of minutes that you want Connect:Direct File Agent to wait before a detected file is considered to be complete.This field is optional. The default time is 1 minute. This field only applies to UNIX systems. With many UNIX applications, different tasks can access the same file simultaneously. This may cause problems if Connect:Direct File Agent detects that a file is present in the watched directory and uses it before another application has closed it. Set this delay to allow an application to finish with the file before Connect:Direct File Agent accesses the file.
File Agent unique name	**Required**. Provide a unique name for each File Agent instance running on the same host or on a different host, while monitoring similar network drives, and configured to submit processes to the same Connect:Direct node. This ensures the unique identity of each File Agent instance by Sterling Control Center. Failing to do so results in Control Center treating multiple instances of File Agent as one.
SNMP listener address	Type the address for the SNMP trap receiver, such as Sterling Control Center. Connect:Direct File Agent uses this address to send SNMP traps for statistics. This field is optional. You can obtain this information from your Sterling Control Center system administrator.
SNMP listener port	Type the port used by the SNMP trap receiver, such as Sterling Control Center. Port 1163 is the default. This field is optional.
SNMP source port range	Type the ports or port ranges used to pass through a firewall to the SNMP trap receiver, such as Sterling Control Center, when File Agent runs behind a firewall. You can specify a maximum of 5 port ranges. This field is optional. Type the ranges in the format nnnn-nnnn, separated by commas, for example, 5555-7777, 8888-8890, 9999. Contact the Sterling Control Center system administrator if you do not know this information.
Refresh Configuration	Select Yes to refresh the configuration after modifying the configuration without restarting File Agent. The default setting is No. **Note:** The Gate Keeper port setting will not be refreshed unless you restart File Agent.

7. Click **Save**.
8. Repeat steps 1 through 8 for the FA2 and FA3 sites, changing information and renaming the configuration files for each site.

   You should now have four configuration files in the File Agent directory:

   - Default_Config.ser
   - FA1.ser
   - FA2.ser
   - FA3.ser
9. E-mail each configuration file to the appropriate Connect:Direct File Agent client site, with the following instructions:
   - Copy the configuration file into the File Agent directory.
   - Rename it to Default_Config.ser.

Creating Multiple Configurations with the cdfa -g Command

The **cdfa -g** command creates multiple configuration files for implementations with a large number of Connect:Direct File Agent sites. This command uses a configuration template and a text-based build file to create the configuration files, which can then be sent through e-mail to client sites. This reduces the amount of configuration that the Connect:Direct File Agent site must perform.

In the following procedure, assume that you want to create three new configuration files for distribution named FA1, FA2, and FA3.

1. Use the configuration interface to create a configuration named Template. (You can name it whatever you want.)
2. Modify the Template configuration settings as necessary for your site. However, type variables into the following fields:

Tab	Field	Variable
File Agent	Password for API	&passwd.
	API host DNS name	&netmap.

   Variables are user-defined. See *Configuration Template Variable Rules* on page 60 for more information about variables.
3. Save the Template configuration file.
4. Use a text editor to create a configuration build file named build.cfg. (You can give the file any name you want.)

5. Insert the following text into the build.cfg file. Bold text indicates the values to change for each client.

```
#FA1's unique configuration
copy Template
&passwd=PROCEED1
&netmap=CDFA1
save FA1
#FA2's unique configuration
copy Template
&passwd=FORWARD23
&netmap=CDFA2
save FA2
#FA3's unique configuration
copy Template
&passwd=MUSTER43
&netmap=CDFA3
save FA3
```

   See *Configuration Build File Variable Rules* on page 60 for build file syntax.

6. Save the build.cfg file in any directory. In this example, it is saved in the c:\ directory.
7. Change your directory to the Connect:Direct File Agent installation directory.
8. Type **cdfa -g c:\build.cfg** at a command prompt. Be sure to specify the complete path to the build.cfg file. This command is case-sensitive.

   Using this example, Connect:Direct File Agent builds three new configuration files based on the values in the template and the build.cfg file. You should now have five configuration files in the File Agent directory:

   - Default_Config.ser
   - FA1.ser
   - FA2.ser
   - FA3.ser
   - Template.ser

9. E-mail the FA1.ser, FA2.ser, and FA3.ser configuration files to the appropriate Connect:Direct File Agent client site, with the following instructions:

   - Copy the configuration file into the File Agent directory.
   - Rename the configuration file to Default_Config.ser.

Configuration Template Variable Rules

When you create multiple configuration files from the command line, observe the rules for using variables in the configuration template file.

- All variable statements in the configuration template consist of an ampersand (&), a user-defined variable name, and a period. For example:
  - &userid.
  - &netmap.
- The variable name is case-sensitive. For example, &userid and &USERID are considered two different variables.
- Variables can be used for any text field. You cannot use a variable for a numeric field.
- Be careful when specifying a variable as part of a file name. For example, assuming that the &userid. value is user1, c:\&userid.txt results in c:\user1txt, with no period separating user1 and txt. In this case, the variable definition should have two periods. For example, c:\&userid..txt, which results in c:\user1.txt.

Configuration Build File Variable Rules

When you create build file variable rules, observe the rules for using variables in the configuration template file.

- All variables in the configuration build file consist of an ampersand (&), a variable name, an equals sign (=), and a substitution value. The trailing period is not included in the configuration build file. For example:
  - &userid=client1
  - &netmap=WIN.CLIENT2
- The variable name is case-sensitive. For example, &userid and &USERID are considered two different variables.
- Connect:Direct File Agent removes all leading and trailing spaces from the substitution value.
- The build file can also have comments, which must be on a separate line and begin with a number sign (#), for example *#FA1's unique configuration*.

Locking a Configuration File for Distribution

You can lock a Connect:Direct File Agent configuration file to prevent changes to it. This ensures that any configurations that you distribute remain static.

To lock a configuration file, add the following command to the build.cfg file you created in *Creating Multiple Configurations with the cdfa -g Command* on page 58.

```
lock configurationfilename
```

This command saves the configuration file specified in *configurationfilename* and locks it against any additional changes.

In the following example, a configuration file named Eastern43 is created and locked:

```
#Eastern43 configuration
copy Template
&passwd=Prescott5
&netmap=CDEast1
lock Eastern43
```

When a configuration file is locked, no one, not even the configuration creator, can unlock or change it. However, you can replace a locked configuration file with a new file that has the same file name, if necessary.

Locked configuration files appear in the configuration list on the configuration interface. However, you cannot select them. To start Connect:Direct File Agent with a locked configuration file, you must do one of the following:

- Start Connect:Direct File Agent with the **cdfa -c***configurationfilename* command, where *configurationfilename* is the name of the locked configuration. For example, **cdfa -cregion5.ser**. On a z/OS system, you must edit the script for the Execution job and type this information on the $FAJAVA line. On a Windows or UNIX system, you can edit the .lax file to always start File Agent with this parameter. Refer to *Running Connect:Direct File Agent from the UNIX Command Line with a Specific Configuration File* on page 72 for information about editing this file.
- If you do not use the **cdfa** command to start Connect:Direct File Agent, assign the locked configuration file a name that matches the name of the computer where Connect:Direct File Agent is running. For example, if Connect:Direct File Agent runs on a computer named Host1, name the locked configuration file **Host1.ser**.
- Saved the locked file as **Default_Config.ser** (the default configuration file).

Managing Rules

Use the following procedures to manage rules:

- Copying a Rule
- Deleting a Rule

- ✦ Enabling and Disabling a Rule
- ✦ Editing a Rule
- ✦ Using Variables in Rules

Copying a Rule

You can copy an existing rule to create a new rule. Complete the following steps to copy a rule.

1. Select the configuration file that you want to work with from the Configurations window.
2. Click the **Rules** tab.
3. Click the tab that contains the rule that you want to copy.
4. Select the rule that you want to copy, then click **Copy**.
5. Type the name of the new rule that you are creating, then click **OK**.
6. Edit the rule to modify match criteria, Process information, or both.
7. Click **Done**.

Deleting a Rule

You can delete a rule that is no longer needed. Complete the following steps to delete a rule.

1. Select the configuration file that you want to edit from the Configurations window.
2. Click the **Rules** tab.
3. Click the tab that contains the rule that you want to delete.
4. Select the rule that you want to delete, then click **Delete**.
5. Click **Yes** in the Delete rule confirmation dialog box.

Enabling and Disabling a Rule

When you create a rule, it is disabled by default. You must enable a rule to activate it. Complete the following steps to enable or disable a rule.

1. Select the configuration file that you want to edit from the Configurations window.
2. Click the **Rules** tab.
3. Click the tab that contains the rule that you want to enable or disable.
4. Enable or disable the rule:
   - Click the **Enabled** check box to activate the rule.
   - Clear the **Enabled** check box to deactivate the rule.

Editing a Rule

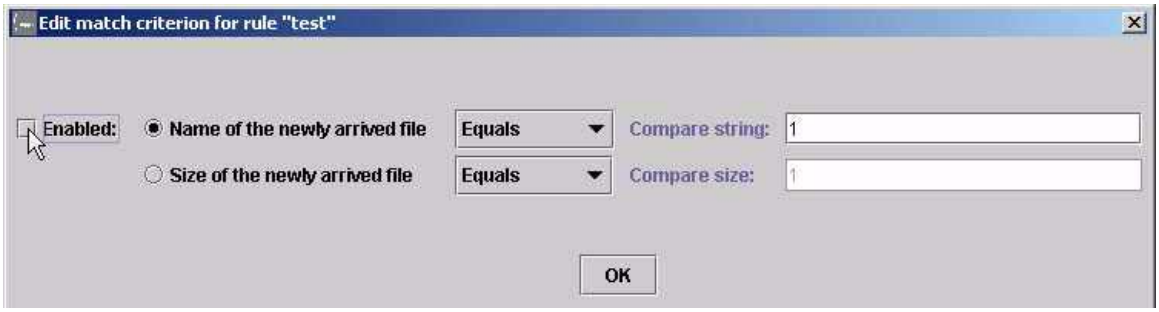
After you define a rule, you can edit match criteria and Process information. You can copy match criteria to create new criteria, delete match criteria, edit match criteria, and enable or disable match criteria. You can modify or delete Process information.

Note: When a rule contains no Process information and Connect:Direct File Agent matches a file with the rule criteria, nothing happens.

To edit a rule:

1. Select the configuration file that you want to edit from the Configurations window.
2. Click the **Rules** tab.
3. Click the tab for the type of the rule that you want to edit. Click the **System event rules** tab to edit a rule based on system events or click the **Submit Process rules** tab to edit a rule based on a detected file.
4. Select the name of the rule that you want to modify.
5. Select the information to modify:
   - To modify match criteria:
     - Select an item from the match criteria list and click the button for the operation that you want to perform. You can create a new match criteria or edit or copy the selected match criteria.

     - From the Match criteria window, select the property to change, define the criteria and operators as necessary, enable the criteria, and click **OK** to return to the match criteria list. The additional criteria or changed criteria is displayed in the Match criteria list.



   - To modify Process information, scroll to the field that you want to edit and define the Process information as necessary.
6. Click **Done** to return to the **Rules** tab.

Using Variables in Rules

You can specify variables to substitute text in any field of a rule. Connect:Direct File Agent uses the following variables. The leading percent (%) and the ending period (.) are required.

Note: For system event rules, the only valid variable is %FA_FILE_FOUND.

Usage	Variable	Description
All Operating Systems		
Path and file	%FA_0. to %FA_99.	The number included in this variable represents a component of the name of the detected file, as delimited by the file delimiter, in sequence. For example, if the full file name is /usr/watch/test file.active.txt, then %FA_0 is usr, %FA_1 is watch, and so on.
	%FA_FILE_FOUND.	On Windows and UNIX, the default value is the path and file name of the detected file. On z/OS systems, the default value is the entire name of the file that File Agent detected, including any member name. This variable supports PDSE long member names. For example, when you specify this variable, File Agent could pass the following member name: CUST.BENEFITS(PAYROLLPDSELONGNAME).
Current date and time	%FA_DATE.	The current date for the detected file. This value has 8 characters that represent the year, month, and day, for example, 20040903.
	%FA_DATE_DAY.	The current day, for example, 31.
	%FA_DATE_MONTH.	The current month, for example, 01.
	%FA_DATE_YEAR.	The current year, for example, 2004.
	%FA_NUM.	The millisecond timestamp. If multiple files are sent within the same second, they will get different millisecond values, for example, 13143512345, 13143512346, and 13143512347.
	%FA_TIME.	The current time. This value has 6 characters to represent the hour, minutes and seconds (format (hhmmss) using a 24-hour clock.
	%FA_TIME_HOUR.	The current hour, for example, 13.
	%FA_TIME_MINUTES.	The current minute, for example, 24.
	%FA_TIME_SECONDS.	The current second, for example, 35.

Usage	Variable	Description
Modification date and time	%FA_FDATE.	The date a detected file was last modified. This value has 8-characters representing year, month, and day, for example, 20040903.
	%FA_DATE_DAY.	The day a file was last modified, for example, 21.
	%FA_FDATE_MONTH.	The month in which a file was last modified, for example, 09.
	%FA_FDATE_YEAR.	The year in which a file was last modified, for example, 2004.
	%FA_FTIME_HOUR.	The hour a file was last modified, for example, 22.
	%FA_FTIME_MINUTES.	The minute a file was last modified, for example, 24 will be passed for a file last modified at 6:24.
	%FA_FTIME_SECONDS.	The second a file was last modified, for example, 35.
	%FA_FDATE_TIME.	The time a file was last modified. This value has 6-characters representing hour, minutes, and seconds (hhmmss) using a 24-hour clock, for example, 153842.
UNIX and Windows only		
File name and path	%FA_EXT_FOUND.	On Windows and UNIX, the file extension of the file that was added, for example, .txt.
	%FA_EXT_FOUND_NP.	On Windows and UNIX, the file extension of the file that was added, but without the period before the file extension. For example, if the file added is file.txt, using the %FA_EXT_FOUND_NP variable will result in txt being passed (the extension with no period included).
	%FA_NAME_FOUND.	On Windows and UNIX, the name of the file that was added, for example, myfile.
	%FA_NOT_PATH.	On Windows and UNIX, the file name with the file extension, without any path. For example, if the full file name is /usr/watch/test file.active.txt, then %FA_NOT_PATH. is test file.active.txt.
	%FA_PATH_FOUND.	On Windows and UNIX, the path of the file that was added, for example, on Windows, C:\watch\, and on UNIX, /home/user/watch.
Windows only		
	%FA_DRIVE_FOUND.	On Windows, the default value is the drive of the file that was added, for example, C:.
z/OS systems only		

Usage	Variable	Description
File and member	%FA_BASEFILE_FOUND.	The default value is the name of the file that was added, without the member name. This variable is only valid for PDS on z/OS operating systems, for example, CUST.BENEFITS
	%FA_MEMBER_FOUND.	The default value is "." This variable is only valid for PDS on z/OS operating systems. PDSE long member names are supported, for example, PAYROLLPDSELONGNAME.

Windows/UNIX Example

If you configure Process arguments as:

```
&FAF=%FA_FILE_FOUND.
```

Then when the watched directory is /home/watch1/ and the file payroll appears in the watched directory, the following argument string is submitted to the Process. &FAF=/home/watch1/payroll

z/OS Examples

If you configure Process arguments as:

```
&FA=%FA_BASEFILE_FOUND. &LM=%FA_MEMBER_FOUND. &BC=”%FA_FILE_FOUND.”
```

Then the following argument strings are submitted to the Process for each scenario:

1. The watched directory PDS is CUST.PROCLIB and member PAYROLL changed.

   arg string= &FA=CUST.PROCLIB &LM=PAYROLL &BC="CUST.PROCLIB(PAYROLL)"

2. The watched directory file is CUST.*, and member BENEFITS of PDS CUST.PARMFILE has changed.

   arg string= &FA=CUST.PARMFILE &LM=BENEFITS

3. The watched directory is CUST.GDGBASE.* and CUST.GDGBASE.G0223V00 is created.

   arg string= &FA=CUST.GDGBASE.G0223V00 &LM=.

Saving a Configuration in a Text File

You can create a text file that contains all of the configuration details and rules for a File Agent configuration. The password for the API connection will be written as asterisks.

Complete the following procedure to save your File Agent rules and configuration details to a text file:

1. Select the configuration file that you want to save as a text file from the **Configurations** window.

If you imported the configuration .ser file into File Agent, you must click **Edit**, make any required changes to the configuration, and click **Save**.

2. Click **Save to a text file** from the **File agent** tab.

   The text file is written to the File Agent installation directory as *configuration_name*.txt. Once the text file is created, when you update the configuration .ser file and click **Save**, you update both the configuration .ser file and the configuration text file.

3. Verify that the text file displays information similar to the following sample. Some lines may differ from the example because of operating system differences and the use of different parameter definitions.

```
************************************************************
  Configuration Details for Default_Config
************************************************************
Comments:
Userid for API: user01
Password for API: ****
API host DNS name: prodhost
API port: 1363
Gate Keeper port: 65530
Watched directories: C:\Output\Binary
Monitor sub directories: true
Continuous sign-on: false
Gate Keeper DNS name:
Default Process:
Default arguments:
Error Process:
Error arguments:
Process class: 1
Process priority: 1
Watch file interval: 1
File completion delay: 0
File Agent unique name: FileAgent
SNMP listener address: controlcenter.prod.domain.com
SNMP listener port: 1163
SNMP source port range:
Refresh Configuration: false

************************************************************
 Submit process rules:
************************************************************
Rule Name: S-1
Enabled: true
Match Criteria (Enabled: Size of the newly arrived file Greater than  "1")
Alternate file name:
Process Name: C:\Process\FileAgent.cdp
Process Arguments: &F=%FA_FILE_FOUND. &dir=%FA_0.\%FA_1. &D=%FA_DRIVE_FOUND.
&P=%FA_PATH_FOUND. &N=%FA_NAME_FOUND. &E=%FA_EXT_FOUND. &G=%FA_FDATE.
&R=%FA_FTIME. &A=%FA_FDATE_MONTH. &AS=%FA_DATE_MONTH. &DE=%FA_DATE_YEAR.
&TT=%FA_NOT_PATH. &PP=%FA_TIME_HOUR. &OP=%FA_TIME_MINUTES. &IO=%FA_TIME_SECONDS.
&FN=%FA_NUM.
Process Class: 1
Process Priority: 1
Notification userid:

Rule Name: S-2
Enabled: false
Match Criteria (Enabled: Size of the newly arrived file Greater than  "1")
Alternate file name:
Process Name: C:\Process\FileAgent.cdp
Process Arguments: &F=%FA_FILE_FOUND. &N=%FA_NAME_FOUND. &E=%FA_EXT_FOUND.
Process Class: 1
Process Priority: 1
Notification userid:
```

```
************************************************************
 System event rules:
************************************************************
Rule Name: System
Enabled: true
Match Criteria (Enabled: System event contents Contains  "java"       Not enabled:
System event title Matches  ""       Not enabled: System event title Matches  "")
Alternate file name:
Process Name:
Process Arguments:
Process Class: 1
Process Priority: 1
Notification userid:
```

Chapter 4

Operating Connect:Direct File Agent

After you install and verify the operation of your default configuration, use the following procedures for your operating system to run Connect:Direct File Agent.

Running Connect:Direct File Agent on a Windows or UNIX OS

Use these procedures to start and stop Connect:Direct File Agent in a Windows or UNIX environment. Running Connect:Direct File Agent automatically is the best way to take maximum advantage of its capabilities.

Running Connect:Direct File Agent as a Windows Service

When you run Connect:Direct File Agent as a Windows service, the application runs automatically when Windows starts.

Note: You must use the command line instead of running File Agent as a Windows service if you need to verify operation, run in verbose logging mode, or use an alternate configuration file.

To configure Connect:Direct File Agent to start automatically when you restart a Windows computer:

1. Configure Connect:Direct File Agent as described in *Creating and Verifying the Default_Config.ser File* on page 23.
2. Select **Start>Control Panel>Administrative Tools>Services**. The Windows Services dialog box is displayed.
3. Right-click **Connect Direct File Agent** in the list of services and select **Properties**. A properties dialog box is displayed.
4. On the **General** tab, Select **Automatic** as the **Startup Type**.
5. Click **OK**.

The File Agent service will not start without a valid configuration. If you try to start the **Connect:Direct File Agent** Windows service without a valid configuration and the service is set up to **Allow service to interact with desktop**, File Agent will launch the configurator and the service will appear to start in the Windows Services dialog box.

Starting Connect:Direct File Agent Automatically on a UNIX Computer

To configure Connect:Direct File Agent to start automatically whenever you restart your UNIX computer, modify the computer's initialization sequence to call the cdfa.sh script.

Starting Connect:Direct File Agent from a Windows Shortcut

You can start File Agent from a Windows shortcut on your desktop. This can be helpful if you want to run File Agent with a different configuration file. To start File Agent from a shortcut, complete the following procedure to place command line parameters in the shortcut. *Command Line Parameters* on page 91 contains command line parameter syntax and descriptions.

To place the parameters in a shortcut:

1. Create a Windows shortcut to the cdfa file (usually located in C:\Program Files\FileAgent).
2. Right-click on the shortcut and select **Properties**.
3. Add the desired parameter after the cdfa command, outside of the quotation marks. For example, to add a parameter starting Connect:Direct File Agent with the configuration file monthend.ser, the command string is:

   ```
   "C:\Program Files\FileAgent\cdfa" -cmonthend.ser
   ```

   If you want to display the parameters on the title bar of the command window, use **cdfa1.bat** instead of **cdfa**.
4. Click **OK** to close the shortcut properties.

Running Connect:Direct File Agent from the UNIX Command Line with a Specific Configuration File

When you run Connect:Direct File Agent in a Windows or UNIX environment, you can run the program from a command line and use command line parameters. Refer to *Command Line Parameters* on page 91 for a list of parameters.

Windows Command

If you want to run Connect:Direct File Agent and always specify a parameter, you can edit the *.lax file* for File Agent. A .lax file is an installation file that sets runtime properties for an application. For example, you may want to run File Agent and always use a specific configuration file. To do this, you must edit the .lax file and add the parameter *-cabc.ser*.

The three .lax files are described in the following table.

File	Description
cdfa$.lax	Runs Connect:Direct File Agent as a Windows service.
cdfac.lax	Runs Connect:Direct File Agent as a GUI configurator.
cdfa.lax	Runs Connect:Direct File Agent from a command window.

When you edit the appropriate .lax file, scroll to the command line arguments field and enter the parameters, as shown in the following example:

```
#   LAX.COMMAND.LINE.ARGS
#   ---------------------
#   what will be passed to the main method -- be sure to quote arguments with spaces
in them

lax.command.line.args=\-cabc.ser\
```

UNIX Commands

If you want to run Connect:Direct File Agent in a UNIX environment, you can use the following command line prompts:

Command	Description
cdfa -C	Runs Connect:Direct File Agent as a GUI configurator.
cdfa	Runs Connect:Direct File Agent from a command window.

Shutting Down Connect:Direct File Agent in a Windows or UNIX Environment

To safely shut down Connect:Direct File Agent in a Windows or UNIX environment, you can create an empty file named “shut” in the File Agent installation directory. File Agent will detect the empty file and delete it before shutting down. The following commands create an empty shut file in a File Agent installation directory on a UNIX system:

```
cd <installation directory>
echo "" > shut
```

Shutting Down Connect:Direct File Agent as a Windows Service

To shut down Connect:Direct File Agent running as a Windows Service:

1. From the **Start** menu, select **Settings**>**Control Panel**>**Administrative Tools**>**Services.**
2. Find Connect:Direct File Agent and stop the Service.

Running Connect:Direct File Agent in a z/OS Environment

When you run Connect:Direct File Agent in a z/OS environment, you run jobs to start the Configuration interface, and to start or shutdown File Agent. This section describes File Agent information that applies to the z/OS environment only.

Using Installation Variables

If you are running File Agent on a z/OS computer, you create and name a File Agent JCL data set during the installation process. All installation variables are saved in this JCL. Refer to *Installing Connect:Direct for z/OS*, in the *Connect:Direct for z/OS Installation Guide* for more information.

Using Command Line Parameters

On a z/OS system, you start Connect:Direct File Agent with the Execution job. Therefore, if you want to use command line parameters, such as -v or -g, you must edit the script for the Execution job and include these parameters in the script. The following screen shows a sample execution job script.

```
//PS010   EXEC PGM=IKJEFT01
//STDIN     DD PATH='&A&B&C&D./FAEXEC.in',
//             PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//             PATHMODE=(SIRWXU,SIRGRP,SIROTH)
//STDOUT    DD PATH='&A&B&C&D./FAEXEC.out',
//             PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//             PATHMODE=(SIRWXU,SIRGRP,SIROTH)
//STDERR    DD PATH='&A&B&C&D./FAEXEC.err',
//             PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//             PATHMODE=(SIRWXU,SIRGRP,SIROTH)
//SYSTSPRT   DD SYSOUT=*
//SYSPRINT   DD SYSOUT=*
//CMD1       DD *
 export DISPLAY=amo-dev2:0.0
 export RUN_DIR=/u/kstic1/bubba/yum
 export RUN_DIR=$RUN_DIR''
 export RUN_DIR=$RUN_DIR''
 export RUN_DIR=$RUN_DIR''
 export JV1='/ZOS12/usr/lpp/java130/IBM/J1.3/bin/java'
 export JV2=''
 export JV3=''
 export JV4=''
 export FAJAVA=$JV1$JV2$JV3$JV4
 export PATH=$PATH:$RUN_DIR
 export LIBPATH=$LIBPATH:$RUN_DIR
 echo "Lib path is.." $LIBPATH
 echo "path is.." $PATH
 echo "Execution directory is..." $RUN_DIR
 echo "JAVA executable is" $FAJAVA
 echo "DISPLAY variable is" $DISPLAY
 cd $RUN_DIR
 sizeCheck
 abc=$?
 if [  $abc -lt 180 ]; then
   echo " insufficent region size:" $abc
   exit 9
 fi
 $FAJAVA -Dsci.config=FAConfiguration -jar fasat.jar -cabc.ser
```

Note: You can edit the line that begins with $FAJAVA (shown in bold) to add the command line parameters.

Using Data Sets

On z/OS systems, you can configure File Agent to watch data sets that can include different file types and have differences in data set organization. Be sure to consider the relevant file characteristics of the generation data group (GDG), partitioned data set (PDS), or partitioned data set extended (PDSE) when one is a File Agent watched directory.

Using File Agent with SMS-Managed GDGs

When you run File Agent on z/OS, it scans catalogs and captures details that describe files, such as data set organization, catalog type, and volume. File Agent uses this metadata to detect file changes and distinguish between files as required for operation. For example, File Agent uses metadata from

the data set to distinguish between sequential (DSORG=PS) and partitioned (DSORG=PO) data sets.

If File Agent is watching for changes in a GDG (Generation Data Group) that is SMS-managed, roll in can be deferred. If roll in is deferred, the timing of changes to file details that File Agent uses for operation can cause unexpected performance. For example, File Agent can detect a previously detected file as newly added, or detect a file type in error. A file that File Agent originally detects as non-VSAM, after a second cataloging, can be detected as GDG. To prevent unpredictable operation when you use File Agent to watch GDGs that can have SMS-deferred roll in, you can force File Agent to operate without evaluating the file metadata that can change.

Configuring File Agent for SMS-Deferred Roll In

Configuring File Agent to watch the trigger file for the GDG instead of the actual file can prevent operational issues caused by SMS-deferred roll in for GDGs. Alternatively, you can configure File Agent to use command line options for ignoring certain details for files. To use the command line options that change how File Agent captures details when watching a GDG, you must edit the script for the File Agent execution job to modify File Agent Java parameters ($FAJAVA line) and specify the command line options to use.

The following command line options enable File Agent to log events and ignore certain file metadata:

Command Line Option	Description
--verboseevents	Enables event logging to STDOUT. With event logging on, you can view event details in a log file.
--ignoreos390catalogtype	Replaces the catalog type (for example, A, H, or G) of the detected file with dashes (-).
--ignoreos390volumes	Replaces the volume serial list for the detected file with dashes.
--ignoreos390filetype	Replaces the PDS or DSN characters of the detected file with dashes.

Modifying the Script for the File Agent Execution Job

To use the command line options described in *Configuring File Agent for SMS-Deferred Roll In*, you must modify the File Agent job execution script.

The following example shows the lines that enable the command line options and modify the File Agent Java parameters in bold:

```
...
 export JV1='/ZOS12/usr/lpp/java130/IBM/J1.3/bin/java'
 export JV2=''
 export JV3=''
 export JV4=''
 export FAJAVA=$JV1$JV2$JV3$JV4
 export PATH=$PATH:$RUN_DIR
 export LIBPATH=$LIBPATH:$RUN_DIR
 echo "Lib path is.." $LIBPATH
 echo "path is.." $PATH
 echo "Execution directory is..." $RUN_DIR
 echo "JAVA executable is" $FAJAVA
 echo "DISPLAY variable is" $DISPLAY
 export f1='--ignoreos390catalogtype'
 export f2='--ignoreos390volumes'
 export f3='--ignoreos390filetype'
 export f4='--verboseevents'
  cd $RUN_DIR
  sizeCheck
  abc=$?
    if [  $abc -lt 180 ]; then
    echo " insufficent region size:" $abc
    exit 9
  fi
$FAJAVA -Dsci.config=FAConfiguration -jar fasat.jar -cabc.ser $f1 $f2 $f3 $f4
```

Enabling the command line options as shown above changes how File Agent captures the file metadata. In following sample metadata, pds is the data set organization, A is the catalog type, and USER15 is the volume:

```
(LOs390/pds;A;USER15;)
```

The following table shows how File Agent detects the metadata shown above after command line options are implemented:

Command Option	File Metadata as Captured by File Agent
--ignoreos390catalogtype	(LOs390/pds;-;USER15;)
--ignoreos390volumes	(LOs390/pds;A;------;)
--ignoreos390filetype	(LOs390/---;A;USER15;)

Shutting Down Connect:Direct File Agent on z/OS

To shut down Connect:Direct File Agent in the z/OS environment, you run the Shutdown job. For more information about running the Shutdown job, refer to the *Connect:Direct for z/OS Administration Guide.*

Note: If you cancel the File Agent Execution job, two data sets are created in the File Agent installation directory, ceedump* and hpitrace*. You can delete these data sets periodically to save space.

Ending a Connect:Direct File Agent Configuration Session

To end a session using the configuration interface:

1. Click **Exit** to close the configuration interface.
2. Click **Yes** on the **Exit confirmation prompt**.

Configuring File Agent Logging

File Agent logs system information to the console and three separate log files. The following logs are available:

Log File	Description
Console Log	Contains information at the INFO levels which includes error messages generated by File Agent and basic information about the files found and what action was taken on the file. The console log is enabled by default.
CDFA.log	Contains information at the INFO level which includes error messages generated by File Agent and basic information about the files found and what action was taken on the file. This log file is enabled by default.
CDFA_verbose.log	Contains information at the DEBUG level which includes all system activity. This file is not enabled by default and is only written when File Agent is running in verbose mode. Refer to *Configure File Agent to Run in Verbose Mode* on page 79.
CDFA_stats.log	Contains only one line per file with process submission (successful or not) information. This log file is enabled by default. Information in this file is only available at the INFO level. Do not modify the setting for this log file.

You can change the level of information generated for each log (except the CDFA_stats.log) by modifying the log4j.properties file in the installation directory. The following log levels are available:

Log Level	Description
WARN	Writes error messages generated by File Agent.
INFO	Writes error messages and basic information that you may want to reference on a daily basis regarding files and actions. Information is written to CDFA.log and CDFA_verbose.log.
DEBUG	Writes all information related to File Agent activity. Information is written to CDFA_verbose.log.

Change Console Logging Level to WARN

To change the level setting for a log to WARN so that only error messages are displayed:

1. Open the log4j.properties file, located in the installation directory.
2. Change the appropriate setting to WARN, as follows:

Log Level	Description
For the console log	log4j.appender.C.threshold=WARN
For CDFA.log	log4j.appender.R.threshold=WARN
For CDFA_verbose.log	log4j.appender.V.threshold=WARN

Change Console Logging Level to DEBUG

To change the level setting for a log to DEBUG so that only error messages are displayed:

1. Open the log4j.properties file, located in the installation directory.
2. Change the appropriate setting to DEBUG, as follows:

Log Level	Description
For the console log	log4j.appender.C.threshold=DEBUG
For CDFA.log	log4j.appender.R.threshold=DEBUG
For CDFA_verbose.log	log4j.appender.V.threshold=DEBUG

Configure File Agent to Run in Verbose Mode

1. Open the log4j.properties file, located in the installation directory.
2. Add **V** to the *log4j.rootLogger=* line as follows: log4j.rootLogger=DEBUG, R, C, **V**.

Chapter 5

Status Reporting and Monitoring

After you install and verify the operation of your default configuration, use the following procedures to check the status and monitor Connect:Direct File Agent.

Reviewing File Agent Status Information

When you verify configurations or troubleshoot operation, you may need to review status information for Connect:Direct File Agent. On Windows, Connect:Direct File Agent creates a snaps subdirectory in the File Agent installation directory and directs log files there.

No logs are created for Linux and UNIX, but you can use your Connect:Direct commands to monitor Process activity. On Connect:Direct UNIX and Connect:Direct for z/OS systems, the DEBUG parameter of the SUBMIT command can monitor and trace execution of Processes submitted by Connect:Direct File Agent. Refer to the *Connect:Direct for UNIX User's Guide* or the *Connect:Direct for z/OS User's Guide* for information about tracing Process execution.

Note: No logging occurs when you run Connect:Direct File Agent as a service, unless an error occurs.

File Agent provides several levels of status information:

- System log–A log of all system activity. A system log is only created if you run verbose, or if an error occurs. If you are not running verbose, the system log appears in the snaps subdirectory of the installation directory when an error occurs. The snaps subdirectory is created when the first event occurs.

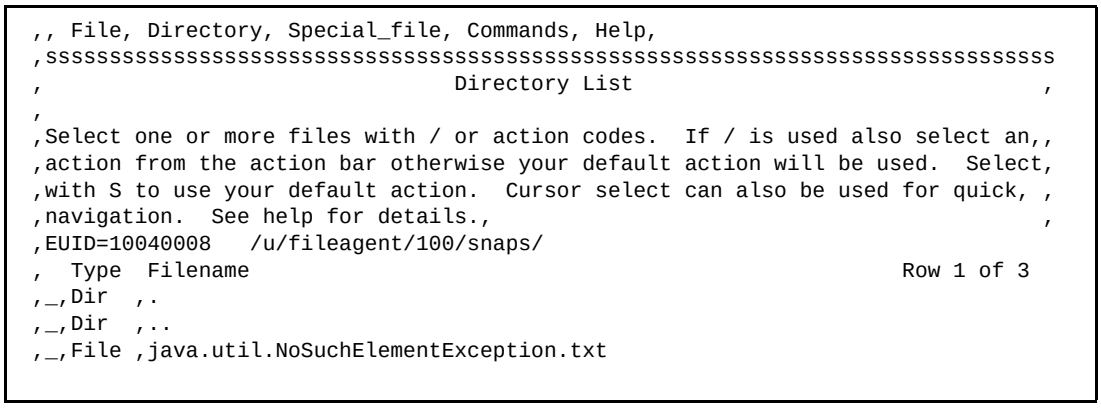
  If you are using File Agent rules in your configuration or if you have more than a few watched directories, the File Agent system log may contain many lines of information. After you become familiar with the phrases that the log uses for status details, you can use the Find command of a line editor such as Windows Notepad to locate those phrases and quickly check status.

  File Agent system log files provide detailed information about Connect:Direct File Agent operation. Among the details provided are the following:

  - Connect:Direct File Agent version

- Application status and the number of services
- Date, time, and other details for each directory scan
- Number of commands attempted and accepted for a directory scan
- Rule and match criteria details from the configuration interface

✦ First Failing Status (FFS) log–One or more logs created when an error occurs.View the *snaps* subdirectory of the File Agent installation directory to obtain FFS statuses. The *snaps* directory is created as needed, and contains the FFS logs for any errors encountered by File Agent. The following screen shows the contents of the snaps subdirectory.



Monitoring File Agent

You can use Sterling Control Center or other SNMP trap receivers to monitor your File Agent instance with SNMP traps.

To use this feature, modify your File Agent configuration.

Configure File Agent

To configure File Agent to be monitored by Sterling Control Center or other SNMP monitoring software, configure the following parameters in the File Agent configurator:

✦ File Agent unique name—Type a unique name for File Agent, in order for Sterling Control Center to distinguish between multiple instances of File Agent running from the same IP address. Configure this parameter only if you want to monitor File Agent with Sterling Control Center.

✦ SNMP listener address—Type the address for the SNMP trap receiver (such as Sterling Control Center). Connect:Direct File Agent uses this address to send SNMP traps for statistics. This field is optional.

You can obtain this information from your Sterling Control Center system administrator.

✦ SNMP listener port—Type the port used by the SNMP trap receiver (such as Sterling Control Center). Port 1163 is the default. This field is optional.

- SNMP source port range—When File Agent runs behind a firewall, type the ports or port ranges used to pass through a firewall to the SNMP trap receiver (such as Sterling Control Center). You can specify a maximum of 5 port ranges. This field is optional.

  Type the ranges in the format nnnn-nnnn, separated by commas. For example, 5555-7777, 8888-8890, 9999.

  You can obtain this information from your Sterling Control Center system administrator.

Configure Sterling Control Center

To configure Sterling Control Center to monitor File Agent, configure the following parameters:

- Server Address—Type the File Agent server address.
- SNMP Listener Address—Type the address of the Control Center SNMP listener. This value must match the SNMP listener address value configured in File Agent.
- SNMP Listener Port—Type the port of the Control Center SNMP listener. This value must match the SNMP listener port value configured in File Agent.

SNMP Trap Information

When the File Agent SNMP parameters are properly configured, the following information is sent from File Agent using the SNMP traps:

- File Agent is active (heartbeat)—Sent at startup and every scan interval
- File Agent has submitted a process
  - For all submit attempts, SNMP trap includes Connect:Direct server name, filename, rule name (or default), and message ID from submit (success or failure)
  - If the process submit is successful, SNMP trap includes process name and process number
- File Agent configuration has changed

The first 25 characters of the File Agent unique name and the first 100 characters of the rule name are sent in the SNMP trap. File Agent also sends time zone difference, connect type, and local node (File Agent unique name) with every trap.

Error Reporting

Any errors that occur during the SNMP trap processing are sent to the File Agent log files. Error messages are as follows:

- Could not register an SNMP listener
- SNMP Cannot get source port
- SNMP Cannot get source port in range
- SNMPBadValueException caught
- SNMP UnknownHostException caught
- SNMP IOException caught

Appendix A

Troubleshooting

To troubleshoot Connect:Direct File Agent operation, you may need to check the following details to identify and resolve issues:

- Format Connect:Direct File Agent variables as described in *z/OS Process Arguments Example* on page 33
- Set appropriate permissions for watched directories
- Specify valid Connect:Direct server parameters in the File Agent configuration
- Check for inactivity from files arriving in watched directories before File Agent starts
- Check that required File Agent rules are enabled
- Confirm that the most specific rule is in first position
- Confirm that all File Agent rules specify a Process to perform actions
- Correct syntax errors in Processes

Refer to the problems and solutions that follow to identify and resolve other issues that occur when you use Connect:Direct File Agent.

Problem	Solution
Connect:Direct File Agent does not start and displays a **Cannot run without a valid configuration** message.	The configuration (.ser) file is missing. See *Creating and Verifying the Default_Config.ser File* on page 23 to create a configuration file.

Unable to determine the version of File Agent running on Windows.	Click the Start Menu. Click **Programs>Accessories>Command Prompt**. At the MS-DOS prompt, use the **cd** command to change to the File Agent installation directory. Type **cdfa -v -cdefault_config.ser** and press **Enter**. See *Command Line Parameters* on page 91 to read about File Agent command line parameters. A message including the File Agent version, similar to the following message is displayed:
	`Arguments on entry:`
	`Arguments listing complete`
	`May 8, 2006 2:16:32 PM CDT 783 Thread[Thread-0,5,main] Product Connect:Direct FileAgent Version 1.0.08 Copyright Sterling Commerce Inc. 2003, 2005, GA fix 00000004 Date 2005/02/06`

Connect:Direct File Agent runs with the wrong configuration file.	Connect:Direct File Agent uses the following hierarchy when determining what configuration file to use: ◆ If you specify the cdfa command with the -c option, Connect:Direct File Agent uses the specified configuration file. For example, **cdfa -cmonthend.ser** starts Connect:Direct File Agent with the configuration file named monthend.ser. ◆ If you do not specify the -c option at startup, Connect:Direct File Agent looks for a configuration file that matches the name of the computer it is running on. For example, if Connect:Direct File Agent runs on a computer named Host1, and a configuration file named Host1.ser exists in the cdfa directory, Connect:Direct File Agent uses the Host1 configuration file. On a Windows computer, you can determine the computer name by selecting **Start<Settings>Control Panel>System** and selecting the **Network Identification** tab. On a UNIX or Linux computer, see the operating system documentation to determine how to find the computer name. ◆ If you do not specify the -c option and no configuration file exists that matches the computer name, Connect:Direct File Agent uses the Default_Config configuration file.

Problem	Solution
Connect:Direct File Agent starts, but no activity occurs.	◆ Type **cdfa -v** to start Connect:Direct File Agent in verbose mode to obtain more details. ◆ Verify with the Connect:Direct system administrator that the Connect:Direct server is active. ◆ Run the File Agent Configuration Interface to check that you have specified watched directories in the File Agent configuration. ◆ Check that no other application is accessing a file that File Agent should detect. File Agent cannot process files that are in use by other applications. ◆ Verify that the File Agent is running with exclusive access to the specified gate keeper port number. ◆ The Connect:Direct system administrator should verify that the Connect:Direct server is properly configured for a connection with Connect:Direct File Agent. See the Installation Guide for your platform for information about configuring the Connect:Direct server for Connect:Direct File Agent.
Connect:Direct File Agent compares the Compare String for a rule against the fully qualified path of the file found, not just against the file name	◆ File Agent is designed to compare the Compare String against the fully qualified path of the file found, but if necessary, you can redefine your match criteria to have it match against the file name, for example: In UNIX, specify: '*/abc*' or '/my_watchdir/abc*' Windows: '*\abc*' or 'C:\My_Watchdir\abc*' This forces pattern matching at the file name level only.
A rule should produce a match, but does not occur.	This could be caused by several conditions: ◆ File Agent supports multiple rules in a configuration. If more than one rule applies, only the first rule encountered produces a match. When a match occurs, rules processing ends. The first rule should always contain the most specific criterion because rules are searched in the order listed on the Rules tab. If the first rule is too general, then it will always match and subsequent rules will never be processed. ◆ Match criteria are case-sensitive. For example, USER1 will not match User1 or user1. ◆ Verify that the match criteria *and* the rule are enabled. ◆ If the rule has multiple match criteria, all match criteria must match for the rule to apply. See *Rules Processing* on page 36 for more information.
Security properties not found, using default message is displayed when Connect:Direct File Agent starts.	This message is produced by the Java Virtual Machine (JVM), not Connect:Direct File Agent. It may be caused by having more than one JVM installed on your computer. It does not affect Connect:Direct File Agent operation and can be ignored.

Problem	Solution
When monitoring a watched directory, File Agent scans the subdirectories of the watched directory, although this is not required.	Edit the rule to use the Matches operator to force File Agent to detect only the directory specified in the path and ignore the subdirectories. To prevent unpredictable operation, be sure to specify this rule first.
File Agent causes a parser error instead of operating as configured.	Early versions of File Agent experienced parser errors when filenames or directory names specified in the configuration contained embedded spaces. You can download Connect:Direct File Agent from the Support on Demand web site. Log in to Support on Demand. Click **Connect** under Product Family Support, choose **Product Updates**, and then click **Connect:Direct**. Click the option that corresponds to your platform, then and download and install the latest version of File Agent available.
On z/OS, SCBC085I is received during an attempt to resolve a symbolic in a File Agent rule.	This error occurs when a symbolic is enclosed in double quotes in the File Agent rule. To remove the double quotes from the symbolic, run the File Agent Configuration Interface and access the File Agent rules fields as described in *Editing a Rule* on page 63.
On z/OS, File Agent scans GDG files that are managed by SMS, and causes two destination files to be written for one source file.	You will need to apply software fixes to resolve this problem. For V4R4, apply fix T035471 (PUT4402). For V4R5, apply fix T035648 (PUT4501).
File Agent is detecting files and submitting a Process, but no other action occurs.	File Agent works with the Connect:Direct Processes you create, but this Connect:Direct component performs no actions other than detecting files in a specified location and submitting the specified Process. The actions you need to perform in response to file detection are performed by your Connect:Direct Processes. Refer to *Understanding Connect:Direct Processes* for information about creating Processes. To access Connect:Direct documentation online, go to https://support.sterlingcommerce.com. Log in to the site, and then click **Connect:Direct Support**. Click **Connect**, and then click **Documentation** to select the document you need.
After restarting File Agent, files in the watched directory are not processed, even though processing was interrupted before it was completed.	File Agent detects a file in a watched directory only one time. If processing is interrupted, files must be removed and replaced with a new timestamp, or in the case of UNIX systems, you can use the touch command to alter the timestamp so that File Agent will detect the files.

Problem	Solution
Some files moved into the watched directory are not processed according to the File Agent configuration, although other files are processed as expected.	Confirm that no other application is accessing the files that File Agent should detect in the watched directory. Test the files in the watched directory for file corruption. Determine whether a synchronization problem is occurring because files are copied into the watched directory before File Agent starts. For Connect:Direct File Agent to detect files in a watched directory, files must be transferred into the watched directory after Connect:Direct File Agent starts. File Agent starts and assumes that any files already in watched directories were sent previously and should not be detected as a change in the watched directory. To determine whether synchronization of the agent and the transfer of the files in question is the issue: 1 Stop File Agent and remove all files from the monitored directory (or directories). 2 Start File Agent from the command prompt. (For example, in Windows, from the \Program Files\FileAgent directory, type: **cdfa -v > cdfa.log** to turn on verbose logging and send the output to a file.) 3 Place the files that were not processed according to the configuration into the monitored directory (or directories) and let File Agent run for a few minutes. 4 Check to see if File Agent processed the files according to the configuration and check the logging details output to the file. If the files that were not processed according to the configuration are now processed, the issue was caused by certain files being copied into the watched directory before Connect:Direct File Agent started monitoring.
File Agent is detecting files, but File Agent is not submitting the Process that it should submit after detecting a file.	Check the user identification and password information. The user ID and password used to Submit the Process must be the same as the user ID and password used when File Agent connected to the Connect:Direct server.
After disabling a rule in the configuration, Connect:Direct File Agent is still processing files as if the rule is enabled.	You must restart File Agent before it can recognize that the rule has been disabled.
Spaces in the graphical interface display as boxes when Connect:Direct File Agent runs in an X Windows emulator.	This is due to X Windows configuration and behavior. Contact the X Windows emulator vendor for a solution.
Receive the following error during a z/OS batch configuration job: `Can't connect to X11 window server using '`*`hostname`*`:0.0' as the value of the DISPLAY variable.`	Please make sure that your setup environment variable DISPLAY correctly or issue xhost command on X server to include this host. Then restart the configurator. Verify that the Alias provide in the DISPLAY is accessible to both the File Agent mainframe and PC platforms. Use NSLOOKUP command on the mainframe or Windows PC and Connect:Direct IUI NM gethostname function on the mainframe to look up the alias name.

Problem	Solution
Receive the following error during a z/OS batch configuration job: `Can't connect to X11 window server using '`*`hostname`*`:0.0' as the value of the DISPLAY variable.`	Please make sure that your setup environment variable DISPLAY correctly or issue xhost command on X server to include this host. Then restart the configurator. Verify the following: ◆ Mainframe to PC connection is passing through Firewall. Exceed uses ports 6000 - 6063. These ports must be allowed to come through the firewall. ◆ Exceed is allowing the Mainframe host access because of Exceed Security setting. Use Exceed Xconfig utility to set Security to allow DISPLAY host access or allow all hosts access.

Appendix B

Command Line Parameters

You can specify the following parameters when you type the **cdfa** command to start Connect:Direct File Agent. These parameters are case sensitive.

Command	Description
cdfa	Starts Connect:Direct File Agent.
cdfa1.bat	On Windows systems, starts Connect:Direct File Agent and displays parameters on the command window. Use in place of **cdfa**.
-c*configfile.ser*	Specifies the Connect:Direct File Agent configuration file (specified in *configfile.ser*) to use instead of any other configuration file. For example, **cdfa -cmonthend.ser** starts Connect:Direct File Agent with the configuration file named monthend.ser.
-C	Starts the configuration interface, for example, **cdfa -C**.
-g *configbuild*	Specifies that Connect:Direct File Agent create one or more configuration files from the configuration template and the text file specified in *configbuild*. See *Creating Multiple Configurations with the cdfa -g Command* on page 58 for more information about this command.
-u*xx*	Specifies the country code that Connect:Direct File Agent should use in place of the default country code. For example, **cdfa -ufr** starts Connect:Direct File Agent using France as the country code.
-l*xx*	Specifies the language code (*xx*) that Connect:Direct File Agent should use in place of the default language. For example, **cdfa -lfr** starts Connect:Direct File Agent using French.
-v	Runs in verbose mode. No internal log is kept and all actions are displayed on the monitor. For example, **cdfa -v**.

Commerce Software. You are solely responsible for the download, installation and use of any software product made available via such third party websites, and for compliance with any and all terms and conditions accompanying the third party software products. Sterling Commerce does not provide information directly to, and has no control over, such third party web sites. Accordingly, Sterling Commerce does not endorse or affirm, and makes no representations or warranties in respect of, such web sites, the information provided therein, or any software obtained therefrom.

2) Third Party Software

Portions of the Sterling Commerce Software may include products, or may be distributed on the same storage media with products ("Third Party Software") offered by third parties ("Third Party Licensors"). Sterling Commerce Software may include Third Party Software covered by the following copyrights: Copyright (c) 1998-2002 Aaron M. Renn (arenn@urbanophile.com). Copyright (c) 1999-2004 The Apache Software Foundation. Copyright (c) 1999-2007 Hewlett-Packard Development Company, LP. Copyright (c) 1998-2007 IBM Corporation. Copyright (c) 1999, 2003, 2004, International Business Machine Corporation and Others. Contains IBM 32-bit Runtime Environment for AIXtm, Javatm 2 Technology Edition, Version 1.4 Copyright IBM Corporation 1999, 2002. Copyright (c) 1997-2008 Sun Microsystems, Inc. Copyright 1998-2001 Wes Biggs. Copyright 2008 Acresso Software Inc. and/or InstallShield Co. Inc. All rights reserved by all listed parties.

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, 12.212, 52.227-19, 227.7201 through 227.7202-4, FAR 52.227-14(g)(2)(6/87), and FAR 52.227-19(c)(2) and (6/87), and where applicable, the customary Sterling Commerce license, as described in Title 48 CFR 227-7202-3 with respect to commercial software and commercial software documentation including DFAR 252.227-7013(c) (1), 252.227-7015(b) and (2), DFAR 252.227-7015(b)(6/95), DFAR 227.7202-3(a), all as applicable.

References in the documentation to Sterling Commerce products, programs, or services do not imply that Sterling Commerce intends to make these available in all countries in which Sterling Commerce operates.

Printed in the United States of America

WARRANTY DISCLAIMER
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, 12.211, 12.212, 52.227-19, 227.7201 through 227.7202-4, FAR 52.227-14(g)(2)(6/87), and FAR 52.227-19(c)(2) and (6/87), and where applicable, the customary Sterling Commerce license, as described in Title 48 CFR 227-7202-3 with respect to commercial software and commercial software documentation including DFAR 252.227-7013(c) (1), 252.227-7015(b) and (2), DFAR 252.227-7015(b)(6/95), DFAR 227.7202-3(a), all as applicable.

The Sterling Commerce Software and this 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.

Except as otherwise set forth below, the Third Party Software is provided 'AS IS' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. FURTHER, IF YOU ARE LOCATED OR ACCESSING THIS SOFTWARE IN THE UNITED STATES, ANY EXPRESS OR IMPLIED WARRANTY REGARDING TITLE OR NON-INFRINGEMENT ARE DISCLAIMED.

As set forth below, certain of the Third Party Licensors assert the following terms with respect to their respective products. Such terms shall only apply as to the specific Third Party Licensor product and not to those portions of the product derived from other Third Party Licensor products or to the Sterling Commerce Software as a whole.

THE APACHE SOFTWARE FOUNDATION SOFTWARE

The Sterling Commerce Software is distributed with or on the same storage media as the following software product (or components thereof), Apache Log4J ("Apache 2.0 Software"). Apache 2.0 Software is free software which is distributed under the terms of the Apache License Version 2.0. A copy of License Version 2.0 is found in the following directory file for the individual pieces of the Apache 2.0 Software: <FileAgent Install Location>/thirdparty.

Unless otherwise stated in a specific directory, the Apache 2.0 Software was not modified. Neither the Sterling Commerce Software, modifications, if any, to Apache 2.0 Software, nor other Third Party Code is a Derivative Work or a Contribution as defined in License Version 2.0. License Version 2.0 applies only to the Apache 2.0 Software which is the subject of the specific directory file and does not apply to the Sterling Commerce Software or to any other Third Party Software. License Version 2.0 includes the following provision:

"Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License."

HEWLETT PACKARD

The Sterling Commerce Software is distributed on the same storage media as the Hewlett-Packard Software which contains Java Runtime Environment 1.6.00. for HP-UX PA-RISC, Copyright © 1999-2007 Hewlett-Packard Development Company, L.P. All rights reserved ("HP JRE PA-RISC Software") and HP-UX Java Runtime Environment for the Java™ 2 Platform Standard Edition 6, version 6.0.01, Copyright © 1999-2007 Hewlett-Packard Development Company, L.P. All rights reserved ("HP JRE Software"). Additional license information for each product is located at <FileAgent Install Location>/jre and applies only to the HP JRE PA-RISC Software and HP JRE Software and not to the Sterling Commerce Software or to any other Third Party Software.

Both the HP JRE PA-RISC Software and the HP JRE Software includes the following notice: "Some third-party code embedded or bundled with the [HP JRE and HP JRE PA-RISC] Software is licensed to you under terms and conditions as set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions contained in the "AS IS" Warranty Statement shall apply to all code distributed as part of or bundled with the [HP JRE and HP JRE PA-RISC] Software."

US Government Rights Notice - HP JRE PA-RISC Software. Confidential Computer Software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and12.212, Commercial Computer Software, Computer Software documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

US Government Restricted Rights – HP JRE Software. The [HP JRE] Software and any accompanying documentation have bee developed entirely at private expense. They are delivered and licensed as "commercial computer software" as defined in DFARS 252.227-7013 (Oct 1988), DFARS 252.211-7015 (May 1991) or DFARS 252.227-7014 (Jun 1995), as a "commercial item" as defined in FAR2.101(a), or as "Restricted computer software" as defined in FAR 52.227-19 (Jun 1987) (or any equivalent agency regulation or contract clause), whichever is applicable. You have only those rights provided for such Software and any accompanying documentation by the applicable FAR or DFARS clause or the HP standard software agreement for the product involved. The owner is Hewlett-Packard Company, 3000 Hanover Street, Palo Alto, California 94304.

You will only find the JRE license information for the HP JRE UX Software and the HP JRE PA-RISC Software in the specified directory if the Sterling Software and Third Party Software are installed on a HEWLETT PACKARD system.

IBM

The Sterling Commerce Software is distributed on the same storage media as the IBM Runtime Environment for AIX, Java Technology edition v.6, 32 bit 1.6.0, Copyright © 1998-2007 IBM Corporation ("IBM JRE Software"). All Rights Reserved. Other copyright acknowledgements may be found in the 'Notices' file in the IBM JRE Software. The IBM JRE Software is provided pursuant to an OEM Agreement between Sterling Commerce and IBM.

U.S. Government Users Restricted Rights- Use, duplication or disclosure restricted by the GSA ADP Schedule Contract with the IBM Corporation.

To the extent IBM has included license information in the IBM JRE Software, you will only find such JRE license information in the IBM JRE Software if the Sterling Software and Third Party Software are installed on an IBM system.

REGEXP SOFTWARE AND GETOPT SOFTWARE

The Sterling Commerce Software is distributed on the same storage media as the gnuRegexp.jar
software (Copyright (C) 1998-2001 Wes Biggs) (“Regexp Software”), and gnuGetopt.jar software (Copyright © 1998-2002 Aaron M. Renn (arenn@urbanophile.com) (“Getopt Software”). The Regexp Software and Getopt Software are independent from and not linked or compiled with the Sterling Commerce Software. The Regexp Software and Getopt Software are free software products which can be distributed and/or modified under the terms of the GNU Lesser General Public License version 2.1 or GNU Library Public License version 2, respectively, both as published by the Free Software Foundation.

Copies of the applicable GNU Licenses are provided at:

<FileAgent Install directory>/thirdparty.

These licenses only apply to the Regexp Software and the Getopt Software and do not apply to the Sterling Commerce Software, or any other Third Party Software.

The Regexp Software and Getopt Software are distributed WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

SUN MICROSYSTEMS INC. ("SUN")

The Sterling Commerce Software is distributed on the same storage media as the JAVAtm Platform, Standard Edition Runtime Environment, Version 6 for the following platforms: Solaris Intel, Solaris SPARC, and Linux Intel, as well as the Java Cryptography Extension, all Copyright © 2008 Sun Microsystems, Inc. (collectively "Sun JRE Software"). All Rights Reserved. The license terms for the Sun JRE Software are located at <FileAgent Install Location>/jre.

The Sun JRE Software includes the following notice: "Additional copyright notices and license terms applicable to portions of the Sun JRE Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party open source/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Sun JRE Software in this distribution.”

The Sun JRE Software license terms for also require the inclusion of the following notice:
“This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at http://oss.software.ibm.com/ico4j/.”

The Java Cryptography Extension is distributed pursuant to the following notice:

Unlimited Strength Java Cryptography Extension

Due to import control restrictions for some countries, the Java Cryptography Extension (JCE) policy files shipped with the Java SE Development Kit and the Java SE Runtime Environment allow strong but limited cryptography to be used. These files are located at

<java-home>/lib/security/local_policy.jar
<java-home>/lib/security/US_export_policy.jar

where <java-home> is the jre directory of the JDK or the top-level directory of the Java SE Runtime Environment.

An unlimited strength version of these files indicating no restrictions on cryptographic strengths is available on the JDK web site for those living in eligible countries. Those living in eligible countries may download the unlimited strength version and replace the strong cryptography jar files with the unlimited strength files.

If [Sun JRE] Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in [Sun JRE] Software and accompanying documentation will be only as set forth in this agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

You will only find the JRE license information for Sun JRE Software in the specified directory if the Sterling Software and Third Party Software are installed on a SUN system.

The license terms for JRE, Sun Java 2 Runtime Environment require the inclusion of the following notice:

“This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at http://oss.software.ibm.com/ico4j/.”

The Sterling Commerce Software is also distributed with the following Sun products whose license terms are located as follows: the Sun JavaBeans™ Activation v.1.0.2 (“Sun JavaBeans Software”) license terms are located at <File Agent Install Location>/thirdparty, and Sun Java Mail 1.2 (“Java Mail Software”) license terms are located at <File Agent Install Location>/thirdparty, the license terms for certain redistributables found in the JAVAHELP(tm) Version 1.12_01, ("JavaHelp Software”) are located at <File Agent Install Location>/thirdparty, and each license applies only to the specific Sun Software which is the subject of the directory file and not to the Sterling Commerce Software or to any other Third Party Software

SUN, Sun Microsystems, the Sun Logo, Solaris Java, Jini, Forte, Staroffice, Starportal and iPlanet, and all related trademarks and logos that are referred to or displayed in the Sterling Commerce Software or the related documentation are trademarks or

registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Neither the name of Sun Microsystems, Inc. nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

The Sun licenses identified in this section only apply to the Sun product identified herein and which is the subject of the directory where the license is located. Such licenses do not apply to the Sterling Commerce Software or to any other Third Party Software.