Sterling Control Center™

System Administration Guide

Version 5.2

Sterling Commerce
An IBM Company

Sterling Control Center System Administration Guide
Version 5.2

First Edition

Sterling Commerce, Inc.
4600 Lakehurst Court Dublin, OH 43016-2000 *
614/793-7000

Contents

Appendix G Sterling Control Center Variables 231

Appendix H Modify log4j to Retain Log Files 253

Appendix I Copy Configuration Objects Between Installations 259

Appendix J Failover Configuration 265

Appendix K High Availability in the Microsoft Cluster Service Environment 275

Appendix L High Availability in the Veritas Cluster Server Environment 279

Chapter 1

Use the System Administration Guide

The *Sterling Control Center System Administration Guide* is for programmers, network operations staff, and system administrators—basically, everyone who maintains the Sterling Control Center system and the managed servers it monitors. After you have planned your implementation, read the *Sterling Control Center Getting Started Guide* for installation instructions specific for your environment.

Once you have installed Control Center and you are ready to add the building blocks that make up your system, the *Sterling Control Center System Administration Guide* will help you with the following tasks:

Task	**For More Information, See**
Starting and stopping Sterling Control Center	Chapter 2, *Start and Stop Sterling Control Center*
Managing and manipulating Control Center objects, such as rules, users, and calendars	Chapter 3, *Managing Control Center Objects*
Creating data visibility groups	Chapter 4, *Manage Data Visibility Groups*
Adding roles and users	*Manage Roles* on page 31 *Manage Users* on page 39
Adding servers and server groups to Sterling Control Center	*About Managing Servers* on page 47 *Manage Server Groups* on page 62
Creating actions and rules	*About Actions* on page 77 *About Rules* on page 69
Creating service level criteria (SLCs)	Chapter 8, *Manage Service Level Criteria*
Creating calendars and schedules	Chapter 9, *Manage Schedules and Calendars*
Creating email lists for use in notifications	Chapter 10, *Manage Email Lists*
Creating metadata	Chapter 11, *Manage Metadata*

Task	For More Information, See
Running Guided Node Discovery to identify additional servers	Chapter 12, *Perform Guided Node Discovery*
Creating and running reports	Chapter 13, *Reports*
Changing system-wide settings	Chapter 14, *Sterling Control Center Settings*
Accessing other systems, such as Sterling Integrator, Sterling File Gateway, and Connect:Direct to perform maintenance tasks	Chapter 15, *Administering Other Systems*
Archiving, restoring, and deleting Sterling Control Center database records	Chapter 16, *Database Administration*
Reviewing and fine-tuning the components of your system including your hardware and network that Control Center runs on, the Control Center engine and console, and the databases your data is stored in	Chapter 17, *Tuning Sterling Control Center*
Researching Sterling Control Center event types	Appendix A, *Event Type Descriptions*
Troubleshooting Sterling Control Center administration	Appendix B, *Administrative Troubleshooting*
Using the predefined actions and rules that ship with Control Center	Appendix C, *Predefined Actions and Rules*
Researching message IDs used in setting up rules and SLCs	Appendix D, *Message IDs for Rules*
Doing batch creation of certain Control Center objects	Appendix E, *Create Multiple Objects*
Using regular expressions in wildcard SLCs and other Sterling Control Center entities to match text or numeric strings that follow a particular pattern	Appendix F, *Regular Expressions*
Using Control Center variables in operating system command actions, server command actions, Sterling Control Center e-mails and workflow SLCs	Appendix G, *Sterling Control Center Variables*
Changing the properties files of the Control Center Engine and Console Logs to facilitate how log files can be retained for backup and archive procedures	Appendix H, *Modify log4j to Retain Log Files*
Exporting the Sterling Control Center configuration objects from a source Control Center installation to a target Control Center installation to prepare for disaster recovery or to go from a test to a production instance	Appendix I, *Copy Configuration Objects Between Installations*

Task	For More Information, See
Providing recovery support in case of hardware failures in Control Center	Appendix J, *Failover Configuration*
Providing high availability failover support in the Microsoft Cluster Environment	Appendix K, *High Availability in the Microsoft Cluster Service Environment*
Providing high availability failover support in the Veritas Cluster Server Environment	Appendix L, *High Availability in the Veritas Cluster Server Environment*
Specifying parameters to use as a key in rules. Also useful to map server-specific information to general Sterling Control Center terms in Activity monitors and statistics or properties screens.	Appendix M, *Keys and Fields*
Collecting Sterling Integrator process data to use in rules, metadata rules, SLCs, and reports.	Appendix N, *Collecting Sterling Integrator Process Data*
Monitoring Sterling File Gateway file transfers	Appendix O, *Monitoring File Transfers Performed by Sterling File Gateway*

Chapter 2

Start and Stop Sterling Control Center

This chapter describes the following:

- ✦ Start the Control Center Engine
- ✦ Stop the Control Center Engine

Start the Control Center Engine

The Control Center engine must be running for users and administrators to have access to the Console and manage servers. In Windows, the engine is set at installation to start automatically. This setting can be changed so the engine starts manually. The engine can also be set to start automatically in UNIX.

Manually Start the Engine on a UNIX Operating System

To start the Sterling Control Center engine on a UNIX operating system:

1. Log in as **root**, or as the user who installed the engine.
2. Change the current working directory on the computer where the engine is installed to *Sterling Control Center installation directory*/bin.
3. Type **sh runEngine.sh**.

Change the Engine Startup Setting

You can set the Control Center engine to start automatically whenever the engine’s computer boots up, or manually.

To set the Control Center engine to start automatically in UNIX:

Insert a command line into a startup file. Because UNIX configurations vary, consult your UNIX administrator for the exact procedure and command syntax.

To change the Control Center engine startup setting in Windows:

1. Click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.

The **Services** window is displayed.

2. Right-click **Sterling Control Center v5.2 Engine** and select **Properties**.
3. Choose **Automatic** or **Manual** from the **Startup Type** list box.

Manually Start the Engine in Windows

This section provides the engine startup settings requiredfor a manual start in Windows.

To start Sterling Control Center, do one of the following:

- To start Sterling Control Center as a Windows service, click **Start > Settings > Control Panel > Administrative Tools > Services** to display the **Services** window, then right-click **Sterling Control Center v5.2 Engine**, and click **Start**.
- From a command window (click **Start > Programs** > **Accessories > Command Prompt**), change to the root directory, and type ***install directory*\ControlCenter\bin\ runEngine$.exe**.
- In Windows Explorer, double-click **runEngine$.exe** in the *install directory*\ ControlCenter\bin directory.
- In Windows Explorer, double-click **runEngine.bat** in the *install directory*\ ControlCenter\bin directory.

Note: If you start Sterling Control Center using the batch (.bat) or .exe file, the Sterling Control Center v5.2 Engine Service displays the status as Not Started.

Manually Start the Engine Remotely in Windows

You can also start the Sterling Control Center engine service from a remote computer using the Windows command line interface.

To start the Control Center engine remotely:

From a command line interface, type the following:

sc “*EngineHost* start runEngine$”

where *EngineHost* is the DNS name of the computer where the engine is running.

Note: You must have administrative permissions for the Sterling Control Center v5.2 engine service to perform this function.

Cold Start Control Center

When the engine is restarted, it collects all statistical records from the monitored servers, including statistical records generated while Control Center was inactive. If the engine was inactive for several hours, unnecessary statistics could fill up the Control Center database and unimportant SLC events could be generated. Cold starting the Control Center engine avoids this issue.

To cold start the Control Center engine on UNIX:

1. Change the current working directory to *install directory*/bin.
2. Type **sh runEngineCold.sh**.

To cold start the Control Center engine on Windows:

1. Open the *Sterling Control Center install directory*\bin.
2. Double-click the file **runEngineCold.bat**.

Stop the Control Center Engine

Working from a Console or from a command line, you can stop the engine and disconnect all Consoles.

From the Console:

To stop the engine and disconnect all Consoles:

1. Click **Control Center** > **Stop Control Center**.
2. Click **OK** in the confirmation windows.

To stop only the Console:

Click **Control Center** > **Exit Console**.

To stop only the engine on a Windows computer:

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Right-click the **Sterling Control Center v5.2 Engine** program, and click **Stop**.

From a command line:

To stop the engine and disconnect all Consoles:

1. Run ***install directory*\bin\stopEngine.bat** (Windows) or ***install directory*/bin/ stopEngine.sh** (UNIX).
2. Supply your Sterling Control Center user ID and password when prompted.

Note: Control Center checks to make sure you have permission to issue a shutdown request before initiating shutdown.

Chapter 3

Managing Control Center Objects

For greater ease of use, the Sterling Control Center console handles many components (referred to here as *objects*) in standard ways. So if you have duplicated a role in the Roles listing, for example, you know how to begin duplicating a calendar schedule in the Schedules listing.

This chapter contains the following sections:

- Filter Objects
- Add New Objects
- Duplicate Objects
- Check Object Properties
- Obtain an Object's Audit Log
- Print Listings of Objects
- Save Listings of Objects
- Cross-Reference Objects
- Remove Objects

Filter Objects

You can limit the number of items that display in many Control Center listings by specifying filter criteria. Filtering a listing can make it more manageable to work with. You can filter listings of the following Control Center objects:

◆ Actions	◆ Netmap Node Entries
◆ Activity Monitor	◆ On-Demand Reports
◆ Adapters	◆ Reports Schedules
◆ Alerts Monitor	◆ Roles

- Automated Reports
- Calendars
- Daemons
- Data Visibility Groups
- Email Lists
- Functional Authorities
- Initialization Parameters
- Metadata Actions
- Metadata Rules
- Netmap Communication Paths
- Netmap Modes
- Report Schedules
- Rules
- Rules Schedules
- Secure+ Cipher Suites
- Secure+ Key Certificates
- Secure+ Nodes
- Secure+ Trusted Certificates
- Servers
- SLC Groups
- User Proxies
- Users

To filter a listing:

1. In the listing, click ▽ . The Filter Listing window displays.
2. Select a **Key**. Available keys depend upon the object.
3. Select an **Operator**. Available operators depend on the key’s data type (numeric or character).

Character Data Operators	Numeric Data Operators
Matches	Equals
Doesn’t Match	Doesn’t Equal
Contains	Is Greater Than
Doesn’t Contain	Is Less Than
Reg Ex	Is Greater Than or Equal to
Wildcard	Is Less Than or Equal to

4. Enter a **Value** by which to limit the listing.

> **Note:** Multiple Value entries result in a listing of items for which *all* specified values are true. Separating Value entries with the pipe character (|) results in a listing of items for which *any* of the specified values is true.

5. Click **OK** to filter the listing, or click **Cancel** to return without filtering.
6. Sort on any column by clicking on the column heading.
7. Refine the list further by repeating the procedure on the now-filtered listing. To revert to the unfiltered listing, click ☒ .

Add New Objects

Adding a new object to many Control Center lists is easy and involves using a common button. The kinds of objects you can add in this way include:

◆ Actions	◆ Report Schedules
◆ Calendars	◆ Roles
◆ Column Layout Views	◆ Rules
◆ Data Visibility Groups	◆ Rules Schedules
◆ Metadata Actions	◆ SLC Groups
◆ Metadata Rules	◆ Users

To add a new object:

1. In the listing for the object (for example, the Rules listing or the Workflow SLCs listing), click **+**. A Create wizard displays.
2. Complete the Create wizard. Refer to the Help or the *Sterling Control Center System Administration Guide* for more on the fields that make up the wizard. On the Finish page, click **Finish** to create the new item.

Duplicate Objects

Duplicating objects in Control Center is easy and involves using a common button. Duplicating is a quick way of creating a new object from a similar existing one while avoiding having to input every data field.

The kinds of objects you can duplicate in this way include:

◆ Actions	◆ On-Demand Reports
◆ Calendars	◆ Report Schedules
◆ Column Layout Views	◆ Roles
◆ Data Visibility Groups	◆ Rules
◆ Email Lists	◆ Rules Schedules
◆ Metadata Actions	◆ SLC Groups
◆ Metadata Rules	◆ Users

To duplicate an object:

1. In the listing for this object (such as the Rules listing or the Workflow SLCs listing), select the item you want to duplicate and click 🗐 . A Create wizard displays, with all fields filled in.
2. Supply a unique **Name** for the new object.
3. Make changes to any other fields as necessary, clicking **Next** to page through the wizard.
4. On the Finish page, click **Finish** to create the new item.

Check Object Properties

Checking the properties of Control Center objects is easy and standardized. The kinds of objects whose properties you can check in this way include:

- Actions
- Calendars
- Column Layout Views
- Data Visibility Groups
- Metadata Actions
- Metadata Rules
- Report Schedules
- Roles
- Rules
- Rules Schedules
- SLC Groups
- Server Groups
- Servers
- Users

To check properties for an object:

1. In the listing for the object (such as the Rules listing or the Workflow SLCs listing), do one of the following:
   - Select the item and click 📋 .
   - Double-click the item.

   The properties dialog displays the object’s properties.
2. Click **OK** to return to the listing.

Obtain an Object’s Audit Log

You can get an audit log for any object contained in a listing. The types of objects included in listings include:

◆ Actions	◆ Report Schedules
◆ Calendars	◆ Roles
◆ Daemons	◆ Rules
◆ Data Visibility Groups	◆ Rules Schedules
◆ Email Lists	◆ Secure+ Cipher Suites
◆ Functional Authorities	◆ Secure+ Key Certificates
◆ Initialization Parameters	◆ Secure+ Nodes
◆ Metadata Actions	◆ Secure+ Trusted Certificates
◆ Metadata Rules	◆ SLCs
◆ Netmap Communication Paths	◆ User Proxies
◆ Netmap Node Entries	◆ Users
◆ Netmap Modes	

To get an object’s audit log:

1. Display the listing. For example, to display the listing of rules, click Manage > Rules and Actions > Rules.
2. Right-click the listing and select Audit Log.

Print Listings of Objects

Printing listings in Control Center is easy and involves using a standard procedure.

The kinds of listings you can print out include:

◆ Actions	◆ Netmap Modes
◆ Automated Reports	◆ On-Demand Reports

- Calendars
- Daemons
- Data Visibility Groups
- Email Lists
- Functional Authorities
- Initialization Parameters
- Metadata Actions
- Metadata Rules
- Netmap Communication Paths
- Netmap Node Entries
- Roles
- Report Schedules
- Report Schedules
- Rules
- Rules Schedules
- Secure+ Cipher Suites
- Secure+ Key Certificates
- Secure+ Nodes
- Secure+ Trusted Certificates
- SLC Groups
- User Proxies
- Users

To print a listing, do one of the following:

- Right-click the listing and click **Print List**.
- Click **Ctrl+P**.

Save Listings of Objects

You can save listings of many Control Center objects to PDF. Saving involves using a standard save button.

The kinds of listings you can save to PDF include:

- Actions
- Automated Reports
- Calendars
- Daemons
- Data Visibility Groups
- Email Lists
- Functional Authorities
- On-Demand Reports
- Report Schedules
- Roles
- Rules
- Rules Schedules
- Secure+ Cipher Suites
- Secure+ Key Certificates

◆ Initialization Parameters	◆ Secure+ Nodes
◆ Metadata Actions	◆ Secure+ Trusted Certificates
◆ Metadata Rules	◆ SLC Groups
◆ Netmap Communication Paths	◆ User Proxies
◆ Netmap Modes	◆ Users
◆ Netmap Node Entries	

To save a listing, with the listing open, click 💾.

Cross-Reference Objects

When making decisions about changing or deleting Control Center objects, you can determine whether other objects reference them. Showing any related objects can help you avoid making changes that would adversely affect other parts of the system.

Control Center objects you can cross-reference with other objects include:

◆ Actions	◆ On-Demand Reports
◆ Automated Reports	◆ Report Schedules
◆ Calendars	◆ Roles
◆ Email Lists	◆ Rules
◆ Metadata Rules	◆ Rules Schedules
◆ Metadata Actions	◆ SLC Groups
◆ Message Lists	◆ Users

To cross-reference an object:

1. In the listing (for example, the Users listing or the Rules listing), right-click the item to cross-reference.
2. From the contextual menu that displays, select **Cross-reference**, and then one of the object types listed. The choices depend upon what other objects the object being cross-referenced might be interrelated with. For example, a message list is potentially interrelated with workflow SLC groups and roles. You can also specify All Objects.

   A list is displayed of objects (of the type specified) that reference the object in question.

Remove Objects

Removing objects in Control Center is easy and involves using a common button.

The kinds of objects you can remove from listings in this way include:

◆ Actions	◆ Report Schedules
◆ Automated Reports	◆ Roles
◆ Calendars	◆ Rules
◆ Column Layout Views	◆ Rules Schedules
◆ Data Visibility Groups	◆ Servers
◆ Email Lists	◆ Server Groups
◆ Metadata Rules	◆ SLC Groups
◆ Metadata Actions	◆ Users
◆ On-Demand Reports	

To remove an object:

1. In the listing, select the item you want to remove and click the minus button **(–)**.
2. Click **OK** to remove the item.

Chapter 4

Manage Data Visibility Groups

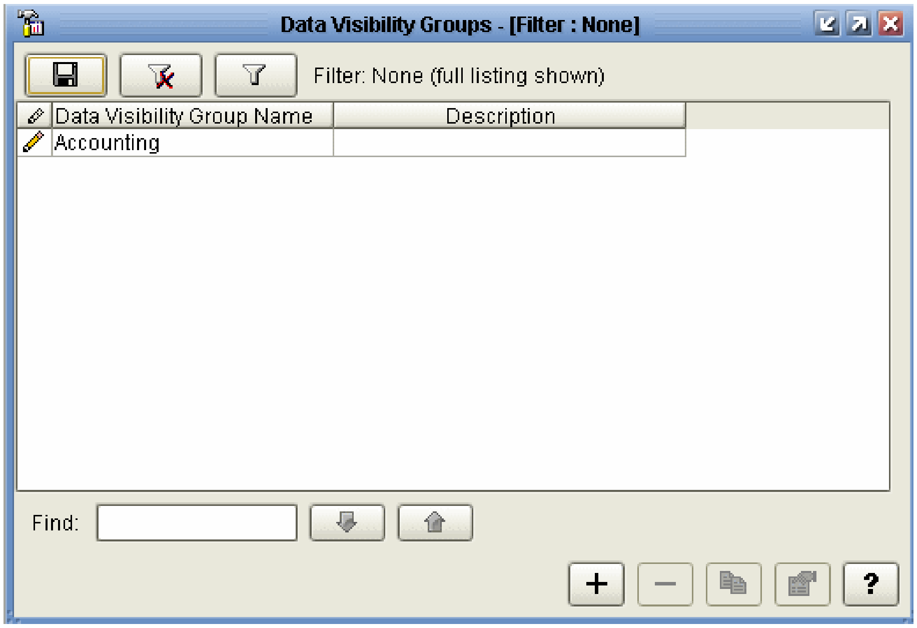
Data visibility groups limit what events (data) a specific user can monitor. For example, when multiple users have access to a single server, a data visibility group (together with a server group) provides a way to segment the data a user can view and act upon for that server. To set up data visibility groups, you specify criteria for segmenting data as needed for your organization. For example, you could segment data into different lines of business (LOBs) or different functional areas, such as accounting or payroll. When events match on any criteria for a data visibility group, that data visibility group name is put into the DVG attribute of the event.

After you define data visibility groups, you assign them to roles, thus restricting the roles. Those roles are then assigned to users. A role can have a server group restriction or data visibility group restriction or both server group and data visibility group restrictions. When restricted roles are assigned to calendars, schedules, email lists, actions, and message lists, you can elect to either make the object visible to all users or only restricted users in the selected roles.

Creating a Data Visibility Group

To create a data visibility group:

1. Select **Manage** > **Data Visibility Group** from the Control Center window to display the **Data Visibility Group** listing.



Data Visibility Groups - [Filter : None]

Filter: None (full listing shown)

Data Visibility Group Name	Description
Accounting	

2. Click **+** to display the **Create Data Visibility Group** wizard.
3. Define a name for the group and provide a description. Click **Next**. See *Data Visibility Group Field Descriptions* on page 29 for definitions of all data visibility group fields.
4. Click + to display the **Create Data Visibility Group Criteria** wizard. You must specify at least one criterion that defines what events (data) a user has access to.
5. Define a name for the criterion and provide a description. Click **Next**.
6. Specify one or more parameters to define the criterion by choosing a **Key** and **Operator** and entering a **Value**. For more information on the keys you can use in parameters, see *Data Visibility Group Field Descriptions* on page 29 and Appendix M, *Keys and Fields*. Click **Next**.
7. Confirm your selections and click **Finish**. The criterion you defined is listed in the Data Visibility Group - Criteria list.
8. Click + to create another criterion. When you have added all criteria for the data visibility group, click Next.
9. Confirm your selections and click **Finish**. Click **Close** to exit the wizard. The data visibility group is displayed in the **Data Visibility Groups** listing.

Displaying the Data Visibility Group Listing

To display the **Data Visibility Groups** listing, from the Control Center window, select **Manage > Data Visibility Group**. To sort on any column, click on the column heading.

Viewing or Changing a Data Visibility Group

If you have the requisite permissions, you can view the information that defines a data visibility group. If you have the requisite permissions, you can change that data visibility group information.

To view or change a data visibility group:

1. Select **Manage > Data Visibility Group** from the Control Center window to display the **Data Visibility Groups** listing.
2. Do one of the following to display the **Data Visibility Groups Properties** window:
   - Select a data visibility group and click
   - Double-click a data visibility group
3. Click the **General**, **Criteria**, and **Summary** tabs to view and change the data visibility group property information as needed. See *Data Visibility Group Field Descriptions* on page 29 for definitions of the fields.
4. Click **Update**. The data visibility group property information is updated.

Data Visibility Group Field Descriptions

The following table describes the fields that specify a data visibility group.

Field	Description
General	
Name	The name for the data visibility group. A data visibility group defines events (data) that users will be able to view and act upon.
Description	A description of the data visibility group.

Field	Description
Criteria	
Parameters	Parameters that specify the data users can monitor. Parameters are specified as keys, operators, values. The following keys are available for use in data visibility groups. See *Keys and Fields* on page 291 for parameter descriptions. Destination File Direction (inBound or outBound) FG.Activity (A or R or D) FG.Arrived File Name FG.Consumer FG.Producer File Agent Name File Agent Rule File Agent Trigger File From Server Local Node (P or S) Orig Node Pnode Account Info Process Name Remote Node Server ID Server Type Servers and Server Groups Source File Step Name Submitter

Chapter 5

Manage Roles and Users

Roles are sets of permissions that specify the Control Center actions users can perform and the servers and server groups they can perform these actions on. You set up roles based on the needs of your organization.

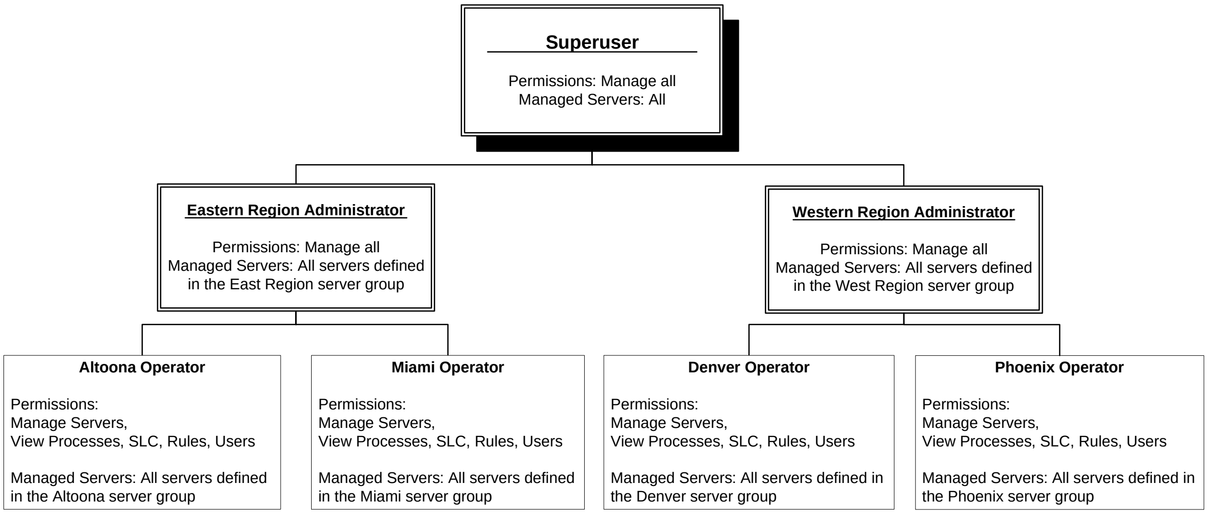
Sterling Control Center is distributed with two roles: superuser and user. The superuser role can perform all Sterling Control Center functions on all managed servers. The superuser can create additional roles or modify existing ones to serve business requirements. For example, a superuser can create a role for a Connect:Enterprise administrator to manage all Connect:Enterprise servers, one for a Connect:Direct administrator to manage all Connect:Direct servers, and one each to manage Sterling Integrator and FTP servers. The superuser can also create roles subordinate to the Connect:Direct, Connect:Enterprise, FTP, and Sterling Integrator administrators, or delegate the creation of subordinate roles to the administrators.

By default the user role can view Sterling Control Center activity but cannot perform management functions such as adding servers or creating SLCs or rules.

Note: Because the predefined user and superuser roles that ship with Control Center are replaced with maintenance releases or upgrades, you should refrain from making changes to those roles. Instead, make copies of those roles and manipulate and use the copies.

Caution: If you make changes to permissions or restrictions for the superuser role, you will be unable to reverse them without reinstalling Sterling Control Center or following manual steps to restore the superuser role. For information on manually restoring this role, see *Manually Restoring the Superuser Role* on page 38.

The following illustration shows a sample role hierarchy:


Superuser
Permissions: Manage all
Managed Servers: All
Eastern Region Administrator
Permissions: Manage all
Managed Servers: All servers defined in the East Region server group
Western Region Administrator
Permissions: Manage all
Managed Servers: All servers defined in the West Region server group
Altoona Operator
Permissions: Manage Servers, View Processes, SLC, Rules, Users
Managed Servers: All servers defined in the Altoona server group
Miami Operator
Permissions: Manage Servers, View Processes, SLC, Rules, Users
Managed Servers: All servers defined in the Miami server group
Denver Operator
Permissions: Manage Servers, View Processes, SLC, Rules, Users
Managed Servers: All servers defined in the Denver server group
Phoenix Operator
Permissions: Manage Servers, View Processes, SLC, Rules, Users
Managed Servers: All servers defined in the Phoenix server group

Subordinate roles cannot be given permissions higher than those of a superior role. Also, subordinate roles can only be given access to the server groups or data visibility groups a superior role can access.

For example, if an Eastern region administrator role has manage permissions on server groups A, B, and C, any roles that he creates can only manage or view server groups A, B, and C (or a subset). Likewise, if a Western region administrator role has only View permissions for a server group, she cannot assign Manage permissions for that group to any subordinate roles.

Permissions

Permissions define the actions that Control Center users can perform. There are three permission levels: Manage, View Only, and None. If a role does not have permission to access a function, that function appears dimmed on the affected user’s console and cannot be selected. After you define a role with restricted access, you can restrict access to actions, rule schedules, SLC schedules, and calendars by associating the restricted role with the item you create.

The following table summarizes Sterling Control Center permissions.

Function	Manage Permission	View Only Permission	None
Servers/Groups	Allows a user to add any Connect:Direct, Sterling Integrator, FTP, or Connect:Enterprise server in your network regardless of server-level restrictions. Manage permission allows the user to: ◆ Add, update, view, and remove servers and server groups ◆ Stop Connect:Direct servers	View server and server group properties and status	Cannot view server/server group status or properties or perform server management functions
Data Visibility Groups	Allows a user to add, update, view, and delete data visibility groups. Only Control Center administrators can manage data visibility groups. To qualify as an administrator, the role must not be server or data visibility group restricted and must have “manage” authority to required elements. If a role qualifies as an administrator, the “manage” permission is allowed; otherwise, only “view” or “none” are allowed.	View data visibility groups	Cannot view data visibility groups
Processes	Delete, suspend, or release processes. View process statistics and properties	View process statistics and properties	Cannot view process statistics and properties or perform process management functions
Alerts	Delete and view Sterling Control Center alerts	View Sterling Control Center alerts.	Cannot view Sterling Control Center alerts or perform alert management functions
Calendars	Create, change, delete, and view calendars	View calendars	Cannot view or perform calendar management functions
SLCs/Schedules	Create, change, delete, and view SLCs and SLC schedules	View SLCs and SLC schedules	Cannot view or perform SLC or schedule management functions
Rules/Schedules	Create, change, delete, and view rules and rule schedules	View rules and rule schedules	Cannot view rules or perform rule management or schedule management functions
Actions	Create, change, delete, and view actions	View actions	Cannot view actions or perform action management functions

Function	Manage Permission	View Only Permission	None
Email Lists	Create, change, delete, and view email lists for automated reports	View email list information	Cannot view email list information or perform email list management functions.
Users	Add, change, delete, and view user information	View user information	Cannot view user information or perform user management functions
Roles	Add, change, delete, and view subordinate roles	View role information	Cannot view role information or perform role management functions
Reports	Generate and view standard Sterling Control Center reports	Cannot access the Sterling Control Center reports function	Cannot access the Sterling Control Center reports function
Automated Reports	Add, change, delete, and view automated report setup information	Cannot access Sterling Control Center automated reports	Cannot access Sterling Control Center automated reports
System Settings	Create, change, and view Sterling Control Center system settings	View Sterling Control Center system settings	Cannot view or change Sterling Control Center system settings
Mobile Device	Can access Sterling Control Center using a mobile device to view and handle alerts; view properties of objects associated with alerts; and monitor server, adapter, and daemon status	N/A	Cannot access Sterling Control Center using a mobile device
Web Access	Auto Login: Allow the user to automatically log into Connect:Direct Browser from the Sterling Control Center console without requiring password authorization	Prompt: Allow the user to log into Connect:Direct Browser from the Sterling Control Center console after requiring password authorization	N/A
View Engine Logs	N/A	View log information	Cannot view
Console Auto Refresh	Allow the role to set the Console Auto Refresh value in System Settings (Console Settings tab) and to set their own refresh setting in Tools > Console Preferences.	Use system setting. Does not allow the role to set Auto Refresh setting or set their own Console Preferences setting.	Require the role to refresh a monitor using the monitor's Refresh button, using the Server > Manual Refresh menu item, or F5 key.

For Web Access permissions, select Auto Login to allow a role to automatically log in to a selected Connect:Direct server using the Connect:Direct Browser User Interface, Sterling Integrator server using the Sterling Integrator Dashboard, or Sterling File Gateway server using myFileGateway. Select Prompt to require the role to provide a user ID and password to log in.

Note: Even if you select Auto Login for a role, if a Connection Dashboard Port value is not specified for a Sterling Integrator managed server, automated login is not accomplished and the Sterling Integrator Dashboard option on the **Manage** menu appears dimmed and cannot be selected.

Node Configuration Permissions

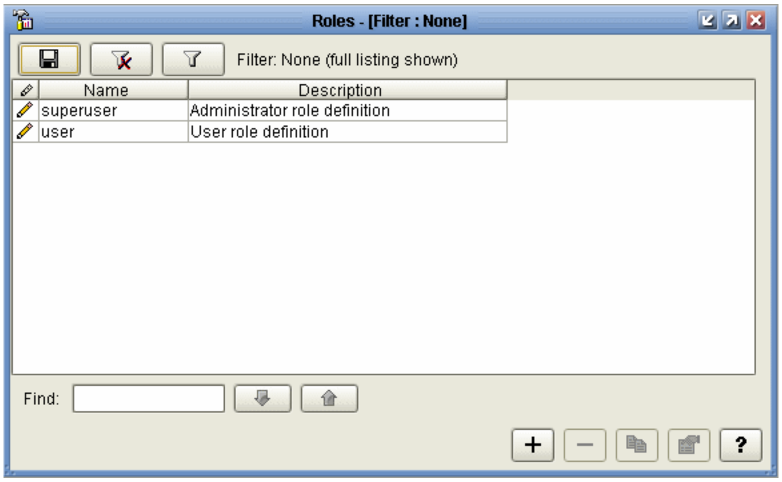
In addition to permissions pertaining to general use of Control Center, a role can be assigned permissions with respect to Control Center’s configuration management capabilities. These permissions are described in the following table:

Function	Manage Permission	View Only Permission	None
Templates	Create, update, and delete templates used in creating Connect:Direct server configuration objects.	View and use templates to create server configuration objects.	N/A
Netmap Entries	Create, update, delete entries for the netmaps of Connect:Direct servers.	View netmap of Connect:Direct servers.	No netmap permissions.
Initialization Parameters	Create, update, delete initialization parameters for a Connect:Direct server.	View Initialization parameters for a Connect:Direct server.	No Connect:Direct server initialization parameter permissions.
User Proxies	Create, update, delete user proxies.	View user proxies for Connect:Direct servers.	No user proxies permissions.
Functional Authorities	Create, update, delete functional authorities.	View user and group functional authorities for Connect:Direct servers.	No functional authorities permissions.
Secure+ Entries	Create, update, and delete entries for Secure+ objects.	View Secure+ objects.	No permissions for Secure+ objects.

Creating a Role

To create a role:

1. Select **Control Center > Roles** from the Control Center window to display the **Roles** listing.



Name	Description
superuser	Administrator role definition
user	User role definition

2. Click **+** to display the **Create Role** wizard.
3. Define a name for the role and provide a description. See *Role Field Descriptions* on page 37 for definitions of all role fields.

   Click **Next**.
4. For restricted roles, select the server groups and/or data visibility groups to which this role should have access and click **Next**.
5. Define the permissions to associate with the role. Refer to *Permissions* on page 32 for a description of the permissions. Click **Next**.
6. Define the node configuration permissions to associate with the role. Refer to *Node Configuration Permissions* on page 35 for a description of the node configuration permissions. Click **Next**.
7. Confirm your selections and click **Finish**. Click **Close** to exit the wizard. The role is displayed in the **Roles** listing.

Displaying the Roles Listing

To display the **Roles** listing:

1. From the Control Center window, select **Control Center** > **Roles**.
2. To sort on any column, click on the column heading.

Viewing or Changing a Role

If you have the requisite permissions, you can view the information that defines a role. If you have the requisite permissions, you can change that role information.

To view or change a role:

1. Select **Control Center > Roles** from the Control Center window to display the **Roles** listing.
2. Do one of the following to display the **Role Properties** window:
   - Select a role and click
   - Double-click a role
3. Click the **General**, **Restrictions, Permissions**, **Node Configuration Permissions**, and **Summary** tabs to view and change the role property information as needed. See *Role Field Descriptions* on page 37 for definitions of the fields.
4. Click **Update**. The role property information is updated.

   If you change role information for a user who is currently signed on to Sterling Control Center, the user's permissions are immediately affected. For example, if a role change removes access to certain functions, those functions are immediately unavailable to the user.

Role Field Descriptions

The following table describes the fields that specify a role:

Note: If you modify a Role that has Server Group or Data Visibility Group restrictions on the Restrictions tab to remove both the Server Group and Data Visibility Group restrictions, the Role will be changed from restricted to unrestricted and any previously created objects that have this role in its list of permissible roles will have this role removed.

Field	Description
General	
Role Name	The name for the role. A role defines a set of permissions that specify what Control Center actions a user can perform and what managed servers he or she can perform these actions upon.
Description	A description of the role.
Restrictions	
	The server groups to associate with the role. To add a server group, highlight a server group in Server Groups and click >. To remove a server group from Selected Server Groups, highlight it and click <.
	The data visibility groups to associate with the role. To add a data visibility group, highlight a data visibility group in Data Visibility Groups and click >. To remove a data visibility group from Selected Data Visibility Groups, highlight it and click <.
Permissions	
	The set of Sterling Control Center actions the role can perform. See *Permissions* on page 32 for a detailed description of each particular permission.

Field	Description
Node Configuration Permissions	
	The set of configuration management actions the role can perform. See *Node Configuration Permissions* on page 35 for a detailed description of each particular permission.

Manually Restoring the Superuser Role

If you have deleted the superuser role or modified it and need to restore it, you can manually restore the superuser role as follows.

1. Stop the Control Center engine.
2. Open the superuser.xml file located in conf\roles.
3. Replace the file's contents with the following:

```
<role>
  <id>superuser</id>
  <ver>1</ver>
  <desc>Administrator role definition</desc>
  <emailLists>manage</emailLists>
  <scheduledReportGroup>manage</scheduledReportGroup>
  <rules>manage</rules>
  <actions>manage</actions>
  <alerts>manage</alerts>
  <processes>manage</processes>
  <users>manage</users>
  <roles>manage</roles>
  <servers>manage</servers>
  <dvgs>manage</dvgs>
  <slcs>manage</slcs>
  <systemSettings>manage</systemSettings>
  <reports>manage</reports>
  <mobileDevice>manage</mobileDevice>
  <webAccess>manage</webAccess>
  <calendars>manage</calendars>
  <serverConfigTemplates>manage</serverConfigTemplates>
</role>
```

4. Save the file.
5. Restart the Control Center engine.

Manage Users

Before a user can log in to Sterling Control Center, the user must be defined. Use the **Users** listing to add users, modify user definitions, and remove users.

For each user you define, you must identify one or more of the following criteria by which to authenticate the user:

- Password
- Host Name
- Windows Domain
- TCP/IP Address

Information is required in one of these four fields. If the user fails to provide the authentication information, an error message warns the user that the information is required.

Additionally, you must define the role each user is authorized to perform when you define the user.

Control Center ships with a default admin user ID named “admin.” Keep the following in mind when dealing with this user ID:

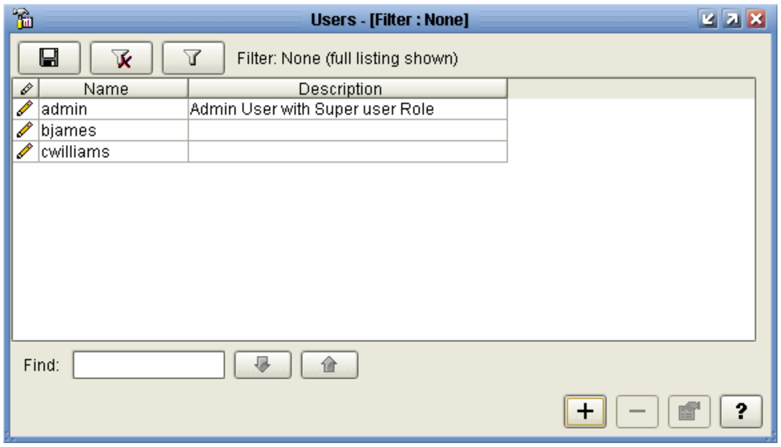
- You cannot delete it.
- It is assigned the superuser role.
- You can change this user’s role to something other than superuser.

Adding Users

You can add users to Control Center. See *User Field Descriptions* on page 41 for detailed definitions of the fields that comprise user information.

To add a user to Control Center:

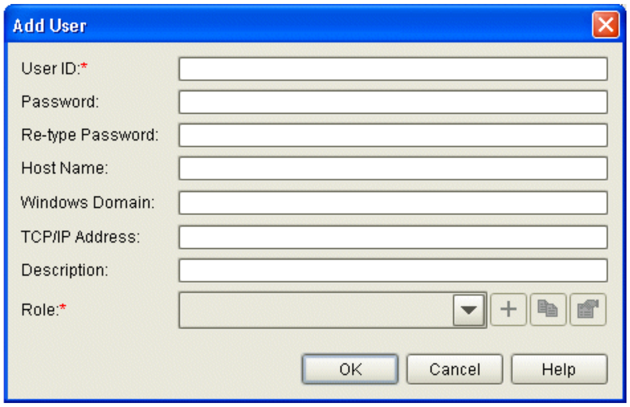
1. Select **Control Center** > **Users** from the Control Center window to display the **Users** listing.



Filter: None (full listing shown)

Name	Description
admin	Admin User with Super user Role
bjames	
cwilliams	

2. Click + to display the **Add User** window.



3. Type the User ID for the user you are defining. (See *User Field Descriptions* on page 41 for a list of all user field definitions.)
4. Provide information in at least one of the following fields to authenticate the user during sign-on:
    - Password and Re-type Password
    - Host Name
    - Windows Domain (except Web console)
    - TCP/IP Address

Note: Information is required in at least one of these four fields to authenticate the user. If the user fails to provide authentication information, an error message warns the user that the information is required.

5. Supply an optional description.
6. Select a role to assign to the user.

Note: You can create a new role by clicking + next to **Role**. You can duplicate an existing role and modify the duplicate by clicking . View a role's properties by selecting the role and clicking .

7. Click **OK**. The user is added to the **Users** listing.

Viewing and Changing User Information

To view and change user information:

1. Select **Control Center** > **Users** from the Control Center window to display the **Users** listing.
2. Do one of the following to display the **User Properties** window:
    - Select a user and click
    - Double-click a user

3. Change the information as required and click **Update**. (See *User Field Descriptions* on page 41 for descriptions of the **Users** listing fields.)

   Note: You must have manage permission to update user information.

   The user information is updated.

User Field Descriptions

The following table describes the fields that define Sterling Control Center users.

Field	Description
User ID	User identification. A code used to identify and authenticate a user who wants to access Sterling Control Center.
Password	A code the user enters to gain access to Sterling Control Center.
Host Name	The host computer through which the user accesses Sterling Control Center.
Windows Domain	The Windows domain from which the user signs in.
TCP/IP Address	The IP address from which the user can sign in.
Description	Descriptive information about the user.
Role	The role, with its attendant permissions, that is assigned to the user.

Setting Password Policy

If you require a password to authenticate users, you can configure Sterling Control Center to accept only passwords that conform to your organization's password policy. This includes the following settings:

- Minimum and maximum password lengths
- Requiring lowercase, uppercase, and special (non-alphanumeric) characters in the password

Note: The ampersand (&), greater than (>), and less than (<) symbols may not be used for special character exclusion in the passwordPolicy.xml file.

- Excluding lowercase, uppercase, and special characters in the password
- Using regular expressions (regex) to define specific password patterns
- Using regular expressions (regex) to define specific patterns to exclude

Modify the passwordPolicy.xml file to configure Sterling Control Center to accept only passwords that conform to your organization's password policy.

Caution: Setting password policy is an advanced procedure requiring knowledge of XML file editing. Back up the passwordPolicy.xml file before performing this procedure.

If you make an XML syntax error when editing the passwordPolicy.xml file, Sterling Control Center may not start. If this occurs, either correct the passwordPolicy.xml file, or replace the edited passwordPolicy.xml file with the backup file, and then restart Sterling Control Center.

These modifications affect only new or modified passwords. Existing passwords continue to work.

Modifying the Password Policy File

You can make changes to the password policy file.

To modify the passwordPolicy.xml file:

1. Make a copy of the passwordPolicy.xml file, located in ControlCenter\conf\security. Name it passwordPolicy.bak.

2. Open passwordPolicy.xml file with a text editor such as Microsoft NotePad. The following example shows the default passwordPolicy.xml file.

```
 <!-- all nested elements are optional, so an empty password policy is valid -->
<passwordPolicy>
  <!-- available for Release 2 -->
  <matchingPatterns>
  <minLength>0</minLength><!-- Omission means that there is no limit -->
  <maxLength>64</maxLength><!-- Omission means that there is no limit -->
   <!-- <required>3</required> --><!-- this number must be less than or equal to the #
patterns listed below -->
   <!-- <patterns> -->
  <!-- <pattern>[a-z]</pattern> --><!-- patterns are Java regex patterns that must match -->
  <!-- <pattern>[A-Z]</pattern> -->
  <!-- <pattern>[0-9]</pattern> -->
  <!-- <pattern>\W</pattern> --><!-- a regex which means special characters -->
  <!-- </patterns> -->
  </matchingPatterns>
  <nonMatchingPatterns><!-- password patterns to exclude -->
  <!-- <patterns> -->
  <!-- <pattern></pattern> --><!-- passwords which match these patterns are not allowed -->
  <!-- </patterns> -->
  </nonMatchingPatterns>
</passwordPolicy>
```

3. To set a minimum password length, type a value between the <minLength> and </minLength> tags. For example, to set the minimum password length at 6 characters, type:

```
<minLength>6</minLength>
```

4. To set a maximum password length, type a value between the <maxLength> and </maxLength> tags. For example, to set the maximum password length at 72 characters, type:

```
<maxLength>72</maxLength>
```

5. To specify the number of patterns that a password must match:

   - Delete the comment marks (<!-- and -->) preceding and following the <!-- <required>3</required> --> tags under the <matchingPatterns> tag.
   - Type the minimum number of patterns that a password must match between the <required> </required> tags. For example, if you want a password to match at least 2 password patterns, type:

   ```
   <required>2</required>
   ```

6. To require certain characters in the password:

   - Delete the comment marks (<!-- and -->) preceding and following the <patterns> and </patterns> --> tags.
   - Delete the comment marks (<!-- and -->) preceding and following the <pattern></pattern> tags you want to require. You can use regex to define more specific password patterns. See *Regular Expressions* on page 229, for more information.

7. To exclude certain characters or combinations in the password:
   - Delete the comment marks (<!-- and -->) preceding and following the <patterns> and </patterns> --> tags following the <nonMatchingPatterns> tag.
   - Delete the comment marks (<!-- and -->) preceding and following the <pattern></pattern> tags.
   - Type the pattern to exclude between the <pattern> and </pattern> tags. For example, if you want to exclude passwords with three consecutive identical characters, type:

     ```
     <pattern>(.)\1\1</pattern>
     ```

8. Save the passwordPolicy.xml file.
9. Restart Sterling Control Center.

Note: The changed password policy takes effect when an existing user tries to change his password or a new user is created that requires a password.

Note: If you enter an incorrect password three consecutive times when logging on, Sterling Control Center removes the user profile information (host name, port number, and user name) from the **Log In** window and closes the window. You must reenter this information to log on.

Example passwordPolicy.xml Files

The following example requires that passwords contain upper case letters, numbers, and special characters.

```
<!-- all nested elements are optional, so an empty password policy is valid -->
<passwordPolicy>
  <!-- available for Release 2 -->
  <matchingPatterns>
  <minLength>0</minLength><!-- Omission means that there is no limit -->
  <maxLength>64</maxLength><!-- Omission means that there is no limit -->
  <required>3</required> <!-- this number must be less than or equal to the # patterns
listed below -->
  <patterns>
  <!-- <pattern>[a-z]</pattern> --><!-- patterns are Java regex patterns that must
match -->
  <pattern>[A-Z]</pattern>
  <pattern>[0-9]</pattern>
  <pattern>\W</pattern> <!-- a regex which means special characters -->
  </patterns>
  </matchingPatterns>
  <nonMatchingPatterns><!-- password patterns to exclude -->
  <!-- <patterns> -->
  <!-- <pattern></pattern> -->
  <!-- passwords which match these patterns are not allowed -->
  <!-- </patterns> -->
  </nonMatchingPatterns>
</passwordPolicy>
```

The following example requires that passwords contain lower case and upper case letters, numbers, and exclude special characters.

```
<passwordPolicy>
  <matchingPatterns>
    <minLength>3</minLength>
    <maxLength>64</maxLength>
    <required>3</required>
    <patterns>
       <pattern>[a-z]</pattern>
       <pattern>[A-Z]</pattern>
       <pattern>[0-9]</pattern>
       <!--   <pattern>\W</pattern> -->
    </patterns>
  </matchingPatterns>

  <nonMatchingPatterns>
    <patterns>
       <pattern>\W</pattern>
    </patterns>
  </nonMatchingPatterns>
</passwordPolicy>
```

The following example requires that passwords be a minimum of 8 characters, a maximum of 64 characters, and contain at least 3 of the following patterns:

- lowercase letters
- uppercase letters
- numbers
- special characters

Also, this example does not allow three consecutive characters in the password.

```
<passwordPolicy>
  <matchingPatterns>
    <minLength>8</minLength>
    <maxLength>64</maxLength>
    <required>3</required>
    <patterns>
      <pattern>[a-z]</pattern>
      <pattern>[A-Z]</pattern>
      <pattern>[0-9]</pattern>
      <pattern>\W</pattern>
     </patterns>
</matchingPatterns>

<nonMatchingPatterns>
     <patterns>
      <pattern>(.)\1\1</pattern>
    </patterns>
  </nonMatchingPatterns>
</passwordPolicy>
```

Chapter 6

Manage Servers

This chapter contains the following subtopics:

- About Managing Servers
- Manage Server Groups
- License Management

Note: For information on monitoring the activity of managed servers, see *Monitoring Server Activity* in the *Sterling Control Center User Guide*.

About Managing Servers

To manage a server using Sterling Control Center, you begin by adding the server. You can manage only the number and types of servers permitted by your Sterling Control Center license. If you try to add another type of server, or more servers than your license permits, Sterling Control Center either displays an error message and prevents you from adding more servers, or it allows you to add servers but dims their icons and disallows communication with them.

Add a Server

To add a server to Control Center:

1. Select **Manage** > **Add Server**. The **Add Server** wizard displays.
2. Type the server name or alias and an optional description. Click **Next**.
3. Select the server type:
    - Connect:Direct with TCP/IP API:
        - Connect:Direct for HP NonStop
        - Connect:Direct for OS/390 or z/OS
        - Connect:Direct for UNIX
        - Connect:Direct for Windows

- Connect:Direct for OS/400
- Connect:Direct Select
- Connect:Enterprise for z/OS
- Connect:Enterprise for UNIX
- Sterling Integrator (SI)
- File Transfer Protocol (FTP) Server – z/OS or WS_FTP
- File Transfer Protocol (FTP) Server – xferlog
- File Transfer Protocol (FTP) Server – IIS
- File Transfer Protocol (FTP) Server – W3C

4. Use the information that you collected in *Add a Server* on page 47 to complete the information requested on the Connection page of the Add Server wizard for Connect:Direct, FTP servers (non-z/OS servers), and Sterling Integrator servers and the OS Type and SNMP Connection pages of the Add Server wizard for Connect:Direct Select, Connect:Enterprise, and FTP – z/OS servers.
5. For FTP servers using an xferlog or IIS log format, click **Advanced** on the Connection page and verify the log file format. For more information, see the field descriptions for *Advanced Settings (for FTP xferlog and IIS log files)* on page 54. After you are finished, click **Update** to continue.
6. For Connect:Direct with TCP/IP API servers, click **Test Connection** to validate the connection information.
7. Optionally, modify the following information when requested.
   - Heartbeat Interval (Connect:Enterprise for z/OS and Connect:Direct Select only)
   - Source Port Numbers (Connect:Direct with TCP/IP API, FTP Server, and Connect:Enterprise for UNIX)
   - Monitor Rest Time
   - Time Zone
   - Use above Time Zone and ignore server-provided UTC Offset
   - Start License Notification *nn* days prior to expiration
8. To specify advanced server settings, click **Advanced** and specify values for the following fields, clicking **Update** to return to the Settings wizard panel:
   - Graphical Activity Monitor expected maximum processes
   - Metadata Rule Handling
   - Max Completed Processes
   - Whether Business Processes are to be monitored (Sterling Integrator only)
   - Whether File Gateway activity is to be monitored (Sterling Integrator only)
   - Connection Timeout

- Tracing

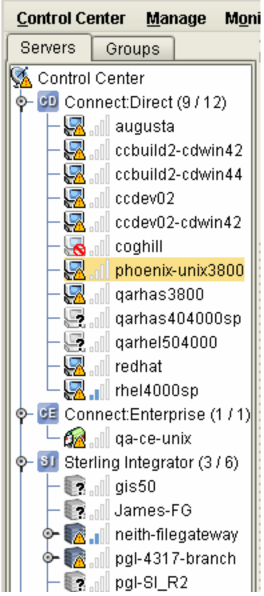
Note: Do not select Tracing Enabled unless instructed by Sterling Commerce support personnel. Tracing significantly impacts performance.

- Check for Configuration Changes (Connect:Direct with TCP/IP API servers)
- Minimum Number of Versions (Connect:Direct with TCP/IP API servers)
- Minimum Age of Versions (Connect:Direct with TCP/IP API servers)

9. Optionally, specify server metadata in any of the ten Server Metadata fields, then click **Next**. The metadata fields are freeform and can be defined in whatever way makes sense for your operation. You can use the metadata fields in reporting and filtering.
10. Optionally, add this server to a server group by selecting a group name in Groups and moving it to Selected Groups by clicking >.
11. Supply contact information for this server:
    - Name
    - Phone
    - E-mail
    - Comments

Note: For more information, see *Server Field Descriptions* on page 52.

12. When you complete the wizard, click **Finish**. The server is added to Control Center. An icon for the server appears in the left panel of the Control Center window.



Control Center
- Connect:Direct (9 / 12)
  - augusta
  - ccbuild2-cdwin42
  - ccbuild2-cdwin44
  - ccdev02
  - ccdev02-cdwin42
  - coghill
  - phoenix-unix3800
  - qarhas3800
  - qarhas404000sp
  - qarhel504000
  - redhat
  - rhel4000sp
- Connect:Enterprise (1 / 1)
  - qa-ce-unix
- Sterling Integrator (3 / 6)
  - gis50
  - James-FG
  - neith-filegateway
  - pgl-4317-branch
  - pgl-SI_R2

If the server icon is overlaid with a question mark (?), either the server is not available and Sterling Control Center does not allow it to be managed, or you made a data entry error (such as typing an incorrect IP address) in the Add Server wizard.

If the server icon is overlaid with a universal no symbol, check your login information.

If the server name is printed in red, the server is down. Review the CCEngine log to investigate the problem (click **Tools** > **Trace Logs)**. Use Server Properties to correct any errors (see *View or Change Server Properties* on page 50).

Optionally, you can group servers together. See *Create a Server Group* on page 62.

View or Change Server Properties

To view or change server properties:

1. In the Sterling Control Center window, double-click the server to view or change. The Server Properties window displays.
2. Click a tab to view server properties under that heading. See *Server Field Descriptions* on page 52 for a description of each field.
3. Change the information as required and click **Update**. The server information is updated.

Note: When you change server information, the server icon may indicate an uncontacted server until Sterling Control Center contacts the server again.

Tip: If the same user ID and password are used to log onto multiple servers, you can use the technique described in *Create Multiple Objects* on page 217, to change the password for all servers at one time instead of changing the password property for each individual server. To see a specific example, go to *How Can I Do a Bulk Update of the Passwords Used by Control Center for Monitored Servers?* in the *Sterling Control Center How-To Guide*.

Set Up a Server to Monitor a Sterling Integrator Cluster

You can monitor a Sterling Integrator clustered instance whether Sterling Control Center is connected to each node in the Sterling Integrator cluster instance individually or to the Sterling Integrator cluster instance through a load balancer. In either case, Control Center ensures continuous monitoring of business process activities in case of any node failure and generates events when any of the cluster nodes are down. In addition, you can see the adapter status of all cluster nodes in a single view.

To set up Control Center to monitor a Sterling Integrator cluster when it is connected to each node individually:

1. On the Sterling Integrator side, create a Web Service called **SCCInteropService** on one of the nodes in the Sterling Integrator cluster. When you create the web service on one of the cluster nodes, it appears on all other cluster nodes, too.This step ensures that Sterling Integrator and Control Center have access to the appropriate process and file transfer data. For detailed instructions, refer to the Sterling Integrator documentation.

2. On the Control Center side, add a server for the Sterling Integrator cluster and for Node Type, select **Sterling Integrator Cluster not through a load balancer**. Specify the host name and ports for each server, and put them in priority order.

To set up Control Center to monitor a Sterling Integrator cluster through a load balancer:

1. On the Sterling Integrator side, create a Web Service called **SCCInteropService** in each node of the Sterling Integrator cluster. For detailed instructions, refer to the Sterling Integrator documentation. This step ensures that Sterling Integrator and Control Center have access to the appropriate process and file transfer data.
2. Configure the load balancer in front of Sterling Integrator to include the host addresses of all nodes in the cluster. The load balancer ensures continuous monitoring of business process activities in case of any node failure.
3. On the Control Center side, add one server to define the overall cluster server (load balancer) and for Node Type, select **Single Sterling Integrator instance or Sterling Integrator through a load balancer**. The host name and ports point to the load balancer, which then gets the data from the individual nodes.

Note: If nodes are dynamically added or removed from a Sterling Integrator cluster monitored by Sterling Control Center, Control Center will not automatically recognize the change. As a result, any adapters on added nodes will not be monitored until Control Center knows about those nodes. For Control Center to recognize when a node has been added or removed, you will either have to stop and start Control Center or pause and resume monitoring of the node.

Monitoring File Agents

You can configure Control Center to monitor Connect:Direct File Agents associated with Connect:Direct servers. While you do not add File Agents like a server, you do need to configure Control Center to monitor them by specifying the address and port the File Agent nodes have been configured to send their traps to. For more information on configuring Control Center to monitor Connect:Direct File Agents, see *File Agent Settings* on page 160 and the *Set Up Control Center to Monitor File Agents* chapter in the *Sterling Control Center Getting Started Guide.*

Note: File agent name must be unique for the Connect:Direct server to which it is submitting processes. If two file agents with the same name are submitting to the same Connect:Direct server, they will be treated as the same file agent.

Server Field Descriptions

The following table describes the fields that detail information on individual servers. The order of fields reflects the order in the Server Properties window.

Field	Description
General	
Name or Alias	The name or alias that identifies a server in the Sterling Control Center window, up to 25 characters. The name/alias must be unique within Control Center. Typically this is the Connect:Enterprise, Connect:Direct, Sterling Integrator, or FTP server name.
Description	A description of the server. To include a link you can click, use one of the following prefixes, and then type the remaining information: http:// ftp:// mailto:// file://
Server Type	
Server Type	The type of server: ◆ Connect:Direct with TCP/IP API ◆ Connect:Direct OS/400 ◆ Connect:Direct Select ◆ Connect:Enterprise z/OS ◆ Connect:Enterprise UNIX ◆ Sterling Integrator (SI) ◆ File Transfer Protocol Server – z/OS or WS_FTP ◆ File Transfer Protocol Server – xferlog ◆ File Transfer Protocol Server – IIS ◆ File Transfer Protocol Server – W3C
Operating System	The server operating system. Display only.
System Version	The Connect:Direct, Connect:Enterprise, Sterling Integrator, or FTP software version. Display only.
Last System Message	Last status message or messages received from the node service monitoring the server. Display only.
Connection	
Server Address	The API address used to establish a session with the Connect:Direct or Connect:Enterprise server.

Field	Description
OS/400 Host Name (OS/400)	The host name for the Connect:Direct OS/400 server.
Library Name (OS/400)	The name of the library in which a Connect:Direct OS/400 server is installed.
SNMP Listener Address	If your Control Center engine has a dual-homed IP stack (e.g., multiple adapters), specify the IP address to which to bind. Otherwise Control Center binds to any available address.
SNMP Listener Port Number	The 1- to 5-digit port number on which Control Center is to listen to receive traps from the server.
API Port (except Sterling Integrator)	The API port number used to access a Connect:Direct, Connect:Enterprise for UNIX, or FTP server. For Connect:Enterprise, the listening port for cmusvid. Connect:Direct default is 1363; must be between 1024 and 65535. FTP default is 21; must be between 1 and 65535.
Log File Name/Directory (FTP servers)	Name of the FTP log file and/or its directory path. If the FTP server’s log has a static name, specify the directory and file name, for example, C:\FtpServer\Logs\server.txt. If the FTP server’s log is dynamic, such that it changes every day or hour, etc., specify only the directory without a file name, for example, **C:\FtpServer\Logs**. If the directory contains files other than the managed FTP server log files, qualify what you enter so that Control Center only monitors information from the appropriate log files or else errors will occur. For example, if all your log files start with ABC, you could enter **ABC*.txt** as a wildcard log name template. Or if your log files have a naming standard, such as, *serverYYYY-MM-DD.log* for a daily rotating log, you would set Log File Name to **C:\FtpServer\Logs\server*.log** to select the changing daily log name and ensure that only the Ftp Server logs are processed.
Agent Address (FTP servers)	The server address of the FTP agent.
Agent Port Number (FTP servers)	The port number for the FTP agent.
Source Port Numbers (Connect:Direct with TCP/IP API and Connect:Enterprise UNIX, FTP servers)	The optional port numbers used to traverse a firewall, if the managed server is behind a firewall. Each port number is 1–5 digits. Acceptable formats are *nnnnn-nnnnn*, or *nnnnn, nnnnn, nnnnn-nnnnn*. Example entries are 5555-5580, 48888-48890, and 5888, 5900-5920. The Sterling Control Center engine uses the first available source port specified when connecting to the server. If none is available, a connection cannot be made. If source ports are used, you should give each server at least two unique ports to choose from.
Web Service Address (Sterling Integrator)	Address of the Sterling Integrator web service.
Node Type (Sterling Integrator)	Type of Sterling Integrator node. Possible values include a single Sterling Integrator instance or cluster not through a load balancer.
Web Service Port (Sterling Integrator)	The port for the Sterling Integrator web service.

Field	Description
Protocol (Sterling Integrator)	The web protocol (HTTP or HTTPS) for Sterling Integrator.
Dashboard Port (Sterling Integrator)	The port for accessing the Sterling Integrator dashboard.
Account List (Connect:Enterprise UNIX)	The accounts on which to retrieve information. If this field is left blank, information for all accounts is retrieved. Separate accounts with commas.
Connection (Connect:Direct)	The protocol (TCP/IP, SSL, or TLS) used for communication with a Connect:Direct TCP/IP API server.
Do not collect process step statistics	Check this box to prevent server management from collecting statistics generated by a Process step. Optional.
Do not monitor this server	Check to prevent server management from monitoring the server. Optional.
Do not allow configuration management on this server.	Check to prevent configuration management from being performed on this server. Optional.
User ID	The user ID used to log on to the server.
Password	The 1- to 64-character password (1–8 characters for z/OS) associated with the user ID. This field is required and case sensitive.
Advanced Settings (for FTP xferlog and IIS log files)	
Available Fields	Fields that can be used to describe your IIS or xferlog record layout. If your FTP server log contains these fields, move them to Selected Fields. Use the Move Up and Move Down buttons to position a particular field in its proper position. Use the <ignored-placeholder> field if your FTP log contains a field that is not listed in Available or Selected Fields.
Selected Fields	Fields included in the FTP xferlog or IIS log file record to be monitored. **Note:** Some fields listed in the Selected Fields list are required. You cannot move required fields to the Available Fields list– they must remain in the Selected Fields list.
Settings	
Monitor Rest Time	The amount of time Control Center waits before polling the server to check status and collect statistics. Values range from 1–3600 seconds (60 minutes) for Connect:Direct and FTP servers (5–3600 seconds for Connect:Direct for Windows and Sterling Integrator), and 1–60 minutes for Connect:Enterprise for UNIX. Setting a lower rest time updates the display of status more frequently but may affect performance. **Note:** For Connect:Direct for Windows, if you set Monitor Rest Time for a new server to less than 5 seconds, the node service bumps that value to 5 seconds the first time the node is polled.

Field	Description
Heartbeat Interval	Interval in seconds within which SNMP trap must be received for server to be considered up. (Connect:Enterprise for z/OS or Connect:Direct Select)
Adapter Status Monitor Rest Time (Sterling Integrator)	The amount of time Control Center waits between polls of adapter status from Sterling Integrator servers. Values range from 1–60 minutes.
UTC Offset	Difference between Time Zone and Coordinated Universal Time (UTC). Display only.
Time Zone	The time zone where the managed server is located. This field is provided for cases in which the server's date/time settings are wrong, or a region's changeover to Daylight Saving Time differs from the national norm. This field also shows the difference between the time zone and Coordinated Universal Time (UTC). **Note:** For a FTP W3C server, check the time zone of the date/time stamp in the log and set the Time Zone to match the time zone of the log file. Since most W3C log files have the date/time stamp in the log in UTC time, set the Time Zone field to **(UTC-00:00) UTC**. Fastream Technologies IQ Web/FTP Server 11.5.5R uses local time in the log date/time stamp whereas InterVation's FileCOPA 4.01 and Microsoft's IIS 5.1 use UTC time.
Use the above Time Zone and ignore server-provided UTC Offset	Select this option when the time zone is not provided by the server, or when it is incorrect.
Start License Notification	The number of days before a server license expiration date to begin generating license expiration events. The range is 1–30 days. The license status is checked daily at midnight engine time. A license expiration event (event type of Server License, message ID of CCNS004E) is generated if the license expires within the specified number of days. Set this value high enough to allow time to obtain and install a new license key.

Field	Description
Start Certificate Expiry Notification	Select an option for the number of days before expiry of trusted or key certificates when Control Center will begin generating events: 1) use the current Control Center system setting for the number of days or 2) specify the number of days for this server. **Note:** This option can be set only for servers that allow configuration management. Certificate expiry checking works only for certificates in Control Center's object repository. To ensure that your certificates are in the repository, you can manually check and add them using Configure Servers > Secure+ > Secure+ Key Certificates or > Secure+ Trusted Certificates. Or, you can automatically check for configuration changes on a daily basis using the “Check for Configuration Changes on Servers” system setting. When a certificate has reached the point when expiry notifications are to be generated, notifications are generated once a day until the certificate’s expiration time changes. **Note:** To act upon certificate expiry events, or notifications, you can use the Certificate Expiry Warning predefined rule to define the number of days before expiry that action will be taken. For more information, see *How Will I Know When My Secure+ Certificates Are About To Expire?* in the *Sterling Control Center How-To Guide*.
Monitor Business Processes (Sterling Integrator)	Check to monitor Sterling Integrator business processes.
BP List (Sterling Integrator)	Click BP List to display a list of all available Sterling Integrator business processes. You can select from this list the business Processes that you want to monitor. **Note:** You must go through the entire procedure to create the server and then return to the Settings tab in the Server Properties window to see this button to select the business processes to monitor.
Monitor File Gateway Activity (Sterling Integrator)	Check to monitor File Gateway events and activities.
Protocols to Monitor (Sterling Integrator)	Protocols you want to monitor with Control Center.
Business Process Selection (for Sterling Integrator servers)	
Monitored	Business processes being monitored by Control Center. Uncheck to exclude.
Business Process	A list of all available Sterling Integrator business processes. Click **Find** to type a string of characters to quickly look up a particular business process and then click the down and up arrows to move from instance to instance. Click **Refresh** to ensure that the list is up-to-date.
Process Data XPath	A path used to access information in a process data XML document. Must begin with the prefix, /ProcessData, for example, /Process Data/FTPClientBeginSession ServiceResults/ServerRepose/Text.

Field	Description
Advanced Settings	
Graphical Activity Monitor expected maximum processes: Use System Settings	Click to set the maximum number of processes that the server is likely to have active at one time to the default value on the System Settings panel, Visualization tab. Used in graphical depictions of server activity.
Graphical Activity Monitor expected maximum processes: Use High Water Mark	Use High Water Mark as the maximum number of processes this server is expected to have active at one time. High Water Mark is a system-generated statistic that indicates the maximum processes that have been active on a server since the value was last reset. Used in graphical depictions of server activity.
Graphical Activity Monitor expected maximum processes: Use other value	Select and enter a number to use a value other than the High Water Mark or System Settings—Visualization in determining maximum number of processes the server is likely to have active at one time. Range = 0 to 2,147,483,647. Used in graphical depictions of server activity.
Metadata Rule handling: Apply Metadata Rules to statistics	Select to apply metadata rules to statistics for this server. For more information, see *Managing Metadata* in the online help or the *System Administration Guide*.
Max Completed Processes	The maximum number of completed events that the Control Center engine will keep in memory and send to the console for display in the Completed Activity Monitor. For the server, the Completed Activity Monitor will never show more rows than this number (1 cache per server) unless data visibility groups are in effect (1 cache per server for the global data visibility group + 1 cache for each specific data visibility group activity) resulting in: Configured number of max completed processes * # of caches For example: Server CDServer with max completed processes set at 50 CDServer with no data visibility specific activity 50 max completed processes * 1 (cache) = 50, resulting in 50 rows displayed CDServer with activity from 1 data visibility group 50 max completed processes * 2 (caches) = 100, resulting in 100 rows displayed CDServer with activity from 2 data visibility groups 50 max completed processes * 3 (caches) = 150, resulting in 150 rows displayed
Connection Timeout	The amount of time the Sterling Control Center engine waits for a response from a server it has attempted to contact. Do not change this value unless you are receiving timeout errors in the engine log for the server in question. The default and minimum is 30 seconds; 120 seconds for Sterling Integrator servers. Maximum value is 600 seconds.

Field	Description
Tracing	Enable or disable tracing for this server. Enabling tracing sends additional debug logging to the CCEngine log for the server. Due to the amount of data sent to the engine log, you should use tracing only when requested by Sterling Commerce Customer Support.
Check for configuration changes (Connect:Direct with TCP/IP API servers)	When to check for configuration changes in servers centrally managed by Sterling Control Center. You can specify that this value default to the value in System Settings, that no checking for configuration changes be done for this server, or to check for configuration changes according to a specified time period.
Minimum number of versions (Connect:Direct with TCP/IP API servers)	The minimum number of versions retained by Control Center for each configuration object type. You can specify that this value default to the one in System Settings or override it with a different value.
Minimum age of version (Connect:Direct with TCP/IP API servers)	The minimum number of days that Control Center should retain a configuration object version. You can specify that this value default to the one in System Settings or override it with a different value.
Queue Limits	
Monitor	Check to monitor the queue.
Queue	ID of the queue to monitor. For Connect:Direct servers, you can choose to monitor the EXEC, HOLD, TIMER, or WAIT queues. For Sterling Integrator servers, you can choose to monitor Queues 0 through 9.
Limit	The maximum number of queued processes allowed for this server before Control Center generates an alert-type warning. If the limit is exceeded, Control Center generates an event of type Server Status with a message ID of CCNS020E. Once the actual number of processes (depth) falls at or below the limit, Control Center generates an event of type Server Status with a message ID of CCNS030I to indicate that the queue is in compliance. For more information, see *Message IDs for Rules* on page 195.
Metadata	
SERVER_DATA_1	Server Metadata 1. The server metadata fields are user-definable fields for writing metadata rules and actions, and for reporting purposes Optional. For more, see *Manage Metadata* on page 129.
SERVER_DATA_2	Server Metadata 2. Optional.
SERVER_DATA_3	Server Metadata 3. Optional.
SERVER_DATA_4	Server Metadata 4. Optional.
SERVER_DATA_5	Server Metadata 5. Optional.
SERVER_DATA_6	Server Metadata 6. Optional.
SERVER_DATA_7	Server Metadata 7. Optional.

Field	Description
SERVER_DATA_8	Server Metadata 8. Optional.
SERVER_DATA_9	Server Metadata 9. Optional.
SERVER_DATA_10	Server Metadata 10. Optional.
Server Groups	
Groups	The server groups to choose from. Move by selecting a server group and clicking >. Optional.
Selected Groups	The server groups to which the server belongs. Move a server out of Selected Groups by selecting it and clicking <. Optional.
Contact Information	
Name	A contact name for the server. Optional. Up to 50 characters.
Phone	Server contact phone number. Optional. Up to 50 characters.
E-mail	Server contact e-mail address. Optional. Special characters allowed. Spaces not allowed.
Comments	Optional contact information for the server. Up to 255 characters.To include a link you can click, use one of the following prefixes, and then type the remaining information: http:// ftp:// mailto:// file://
License	
Customer Name (except Sterling Integrator/FTP)	The name of the customer to whom the license was issued. Display only.
Product (except Sterling Integrator/FTP)	The Sterling Commerce product specified in the license key. Display only.
License Push Supported/Not Supported (except Sterling Integrator/FTP)	This message text indicates whether automated license pushing is supported for this server. Display only.
Operating System (except Sterling Integrator)	The operating system of the Connect:Direct, Connect:Enterprise, or FTP server. Display only.
Expiration Date (except FTP)	Date that the managed server’s license expires. Display only.

Field	Description
Details (except Sterling Integrator/FTP)	Click to view license details for this server. Display only.
License Key (except FTP)	Server license key. Display only.
Last Retrieved (except FTP)	The date and time that the license was last retrieved and validated. Display only.
Retrieve (except FTP)	Click this button to retrieve a new version of the license for this server.
SCI Extensions (Sterling Integrator)	Sterling Integrator system-related licensing and versioning information.
View License Key (Sterling Integrator)	Click this button to view the raw Sterling Integrator license key data. Display only.
Component Licenses (Sterling Integrator)	This display-only listing shows license information for each component licensed in Sterling Integrator, including Sequence #, Product Version, Component, Product ID, IP, Start Date, and Expiration Date.
Server Status	
Processes	The number of executing and nonexecuting Processes found for the server. Display only.
Alerts	The number of alerts issued for this server, broken into high, medium, and low severity. Display only.
Server Version	The version of the managed server. Display only.
License Type (except FTP)	Type of license in place for the server. Display only.
Location (Sterling Integrator)	Location of Sterling Integrator installation files.
Max Concurrent Processes	The maximum number of concurrent sessions that have occurred on the server, the number of times that this maximum was reached, and the last date and time that the maximum was reached. This information is display only, although it can be reset to zero (see *Reset the Maximum Concurrent Session Count for a Server* on page 61).
Reset Watermark	Click to reset the values in Max Concurrent Processes to zero, including maximum number of concurrent sessions, number of times that this maximum was reached, and last date and time the maximum was reached.
Welcome Message (FTP)	An informational message set by the FTP administrator for users of an FTP server. The message may contain directory information, usage guidelines, unauthorized access warnings, server news, or other information.
Last Contact At	Date and time of last contact with the server.
Date/Time in Last Record Retrieved	Date and time the last record was retrieved from the server.

Field	Description
Server is Being Monitored/Server is Paused	Allows authorized user to pause monitoring of the selected server. If the button label reads “Pause,” click it to stop monitoring. If it reads “Resume,” click the button to resume monitoring.
Environment (Sterling Integrator only)	
Field	This column contains the names of variables that pertain to the Sterling Integrator environment.
(Value)	The data values for Sterling Integrator environment variables.

Reset the Maximum Concurrent Session Count for a Server

After you define a server, information about it is displayed in the Server Status Monitor, including the maximum number of concurrent sessions that have occurred, the number of times this maximum number of concurrent sessions was reached, and the last date and time when that occurred. You can reset these values to zero.

To reset the maximum concurrent session count to zero for a server:

1. In the server list, right-click the server in question and select **Properties**.
2. In the **Server Properties** window, click the **Server Status** tab. The current value is displayed in **Max Concurrent Processes**.
3. To reset this value, click **Reset** under **Reset Watermark**.
4. Click **Update**. The watermark is reset.

Remove a Server from Control Center

To remove a server from Control Center:

1. In the server list, right-click the server you want to remove and select **Remove Server**.
2. Click **OK** to remove the server. The server is removed.

   When you remove a server from Sterling Control Center, any server groups, rules, SLCs, and roles that include the server are automatically updated. If the server is the last remaining server associated with a rule or SLC, the rule or SLC is automatically disabled.

   The server is removed from any open monitor windows unless it is the only item displayed in the monitor. In that case, the monitor window closes.

Manage Server Groups

A server group is a customized grouping of your system servers. You define your server groups in the way that makes sense to you. For example, you can group servers by processing center or by server type. You can even group all managed servers into one group to monitor all server activity in one monitor window.

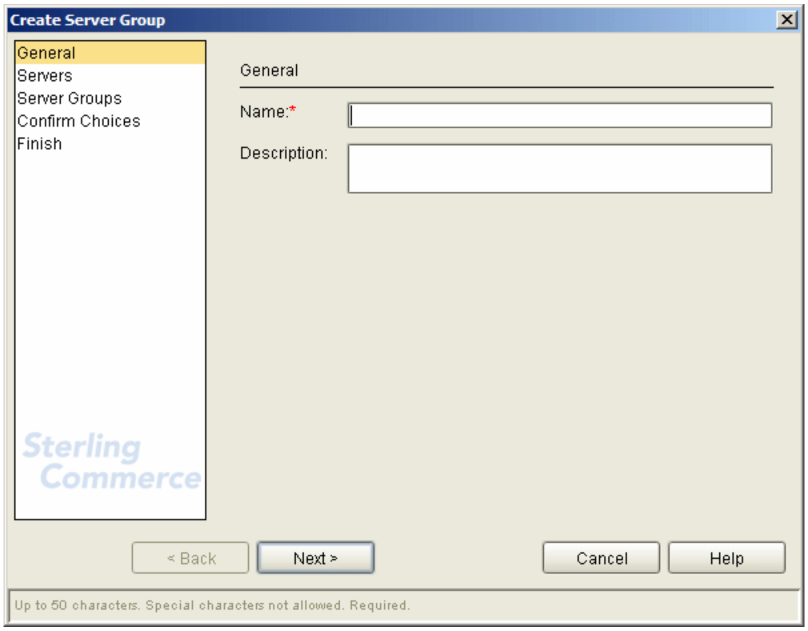
Server group definitions are system wide. For example, if you define two server groups named ConnectDir and ConnectEnt, all Sterling Control Center users in your organization (if they have the necessary permissions) will see these server groups.

You can specify server groups in Sterling Control Center permissions, rules, and SLCs.

Create a Server Group

To create a server group:

1. Select **Manage** > **Add Server Group.** The **Create Server Group** window is displayed.



Up to 50 characters. Special characters not allowed. Required.

2. Type a unique name for the group in **Name**, optionally add a **Description**, and click Next.
3. In **Servers**, select one or more servers to add to the group and click >. Click Next when finished adding servers.

Tip: Add more than one server at a time by holding down **Shift** (for adjacent servers) or **Ctrl** (for non-adjacent servers) while selecting.

For more on filtering the list of available servers, see *Filter Objects* on page 19.

4. To add server groups to this group, select one or more to add to the group and click **>**. Then click **Next**.
5. Review the details of the new group on the Confirm Choices wizard page, then click **Finish**.
6. Click **Close**.

View or Change a Server Group Definition

To view or change a server group:

1. Click the **Groups** tab in the Sterling Control Center window's left pane.
2. Right-click the group and select **Properties**. The **Group Properties** window displays.
3. Add a server to the group by clicking the **Servers** tab, selecting the server in the **Servers** list, and clicking **>** to move it to Selected Servers.
4. Remove a server from the group by selecting the server in the **Selected Servers** list and clicking **<**.
5. Add a server group to the group by clicking the **Server Groups** tab, selecting the group in the **Server Groups** list, and clicking > to move it to Selected Server Groups.
6. Remove a server group from the group by selecting the server group in **Selected Server Groups** and clicking **<**

Tip: Select more than one server at a time by pressing **Shift** (for adjacent servers) or **Ctrl** (for non-adjacent servers) while selecting. Select all servers in a list by pressing **Ctrl + A.**

7. When finished, click **OK**.

Remove a Server Group

To remove a server group:

1. Click the **Groups** tab in the Sterling Control Center window's left pane.
2. Right-click the group to remove and select **Remove Group**.
3. Click **OK**.

When you remove a server group from Sterling Control Center, any rules, SLCs, and roles that referenced the server group are automatically updated. The servers referenced in the server group are not affected.

License Management

Sterling Control Center License Management supports import of server licenses to a central license management repository and ad hoc distribution to managed Connect:Direct servers. Licensing options include assignment of a unique license key to a server and a license key shared among multiple servers.

When a new license key is pushed to a managed server, the server validates the new key and, assuming a valid key, copies it to the appropriate location and begins to use it.

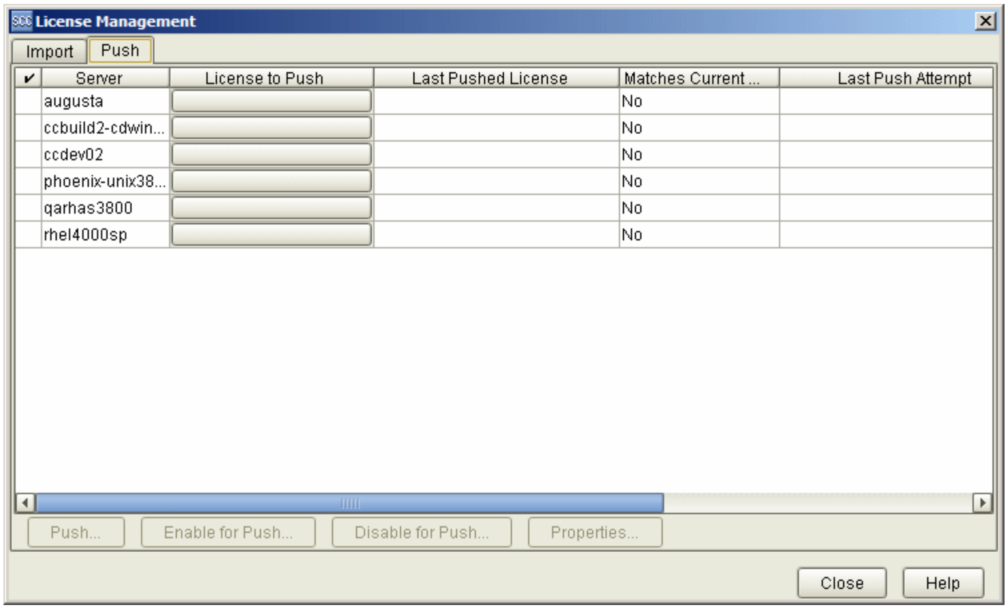
In addition to manually importing licenses, you can set up Control Center to automatically import license key files received via email. You can then manually push those licenses to the appropriate servers. For more information see *Push Licenses to Servers* on page 66 and *Automatically Import Licenses* on page 67.

Note: To push new license keys or make changes to existing keys for a Connect:Direct server, the user ID used by Control Center to connect to the server must have administrator authority on that server. For Connect:Direct for z/OS or OS/390, you must also have an additional authorization flag turned on for the Update Asset Key command. See the *Connect:Direct for z/OS Administration Guide*.

To manage licenses:

Select **Tools** > **License Management**.

The License Management listing displays.



✔	Server	License to Push	Last Pushed License	Matches Current ...	Last Push Attempt
	augusta			No	
	ccbuild2-cdwin...			No	
	ccdev02			No	
	phoenix-unix38...			No	
	qarhas3800			No	
	rhel4000sp			No	

The License Management listing contains license information in two tabbed panes: Import and Push. The Import pane is for importing license data into the Control Center engine License Management repository. The Push pane is for pushing imported licenses to managed servers enabled for license push.

Manually Import Licenses

To import licenses:

1. On the **Import** pane of the License Managemen**t** listing, click **Import**. The Import License Key File wizard displays, starting with the License Key Text page.
2. Do one of the following:
   - Type or paste license key text into the License Key Text text box.
   - Click **File** to navigate to and import a text file containing the license key text.
3. Click **Next** to move through succeeding wizard pages, supplying license ID information and selecting servers to apply the license to.

   Note: You can create a new version of an existing license by selecting an existing license ID.

   You cannot create a new version of a license if a previous version is assigned to a server to which you do not have access.

4. Click **Finish** on the Summary page and then **Close** to exit the Import License Key File wizard.

View and Update Licenses

To view or update license properties:

Do one of the following:

- Select a license in the License Management listing (Import or Push tab) and click **Properties**.
- Double-click the license.
- Right-click the license and select **Properties**.

The License Properties window displays.

To select a license version for a managed server:

1. On the Push tab of the License Management listing, select a server and click its **License to Push** button.

   Note: Only servers that support license push are shown.

2. In the Select a License and a Version window, select a license and version and click **OK**.

To compare license details with those of the license currently assigned to a server:

1. Right-click the license in the License Management listing and select **Compare**. The Compare License Keys window displays. The details of the selected license key and the one currently assigned to the server are displayed side by side. If they match, the message text “Matches: True” is displayed in the lower right corner of the screen. If they do not match, “Matches: False” is displayed in red. Any differences are highlighted in red.
2. To compare against a different license key on the License Management listing, select another license key from either drop-down list.

Delete Licenses

To delete a license:

1. Do one of the following:
   - Right-click the license in the License Management listing and select **Delete**.
   - Select the license and click the **Delete** button.
2. Click the appropriate version of the selected license in Select License–Version and click **OK**.

License Import Field Definitions

The following table defines the fields pertaining to importing licenses for servers.

Field	Description
License ID	The license identifier.
# of Versions	The number of available versions of the license.
Imported By	The user who imported the license.
Imported Date/Time	Date and time of the license import.
Platform	The operating system that this license applies to (if available).
Exp. Date	Expiration date of the license (if available).

Push Licenses to Servers

From the License Management Push tab, you can disable or enable licenses for pushing and view the properties of servers enabled for pushing. You can push imported licenses to servers enabled for pushing.

To disable a server or servers for pushing:

1. Select a server, Shift-click to select contiguous servers, or Ctrl-click to select non-contiguous servers.
2. Click **Disable for Push**.

To enable a disabled server for pushing:

1. Select the server.
2. Click **Enable for Push**.

To push a license to a server or servers in the License Management listing (Push tab):

1. Select the server, Shift-click to select contiguous servers, or Ctrl-click to select non-contiguous servers.
2. Click **Push**.
3. To cancel the push operation, click **Stop Push**.

4. When the push operation is complete, consult the Last Push Result and Last Push Message columns to check on the operation's success. If the operation was unsuccessful, Last Push Result is highlighted in red.

License Push Field Definitions

The following table defines the fields that pertain to pushing licenses to servers.

Field	Description
☑	A check mark indicates that the server is enabled for license push.
Server	The server to which the license is to be pushed.
License to Push	The license to be pushed, that is, sent to the selected server for validation and use.
Last Pushed License	The license that was last successfully pushed to this server.
Matches Current Server License?	Indicates whether this license matches the one currently being used by the server (Y/N).
Last Push Attempt	The date and time when the last license push was attempted for this server.
Last Push Result	The result of the last push attempt.
Last Push Message	The message returned from the last attempted push.

Automatically Import Licenses

Besides manually importing licenses, you can configure Control Center to monitor a POP3 or IMAP mailbox for emails containing license key file attachments. If it finds one in the mailbox, Control Center validates the license, and, if valid, imports it into the License Repository. You can then push the license to the appropriate server(s). For more information on pushing licenses, see *Push Licenses to Servers* on page 66.

Note: This email mailbox should be considered as belonging to Sterling Control Center and should not be shared with any other user.

An event is generated when the license is validated and imported, or when the license does not validate. You can create a rule to notify you when one of these license events occurs so that you can take the appropriate action. For more information on creating this type of rule, see the *Sterling Control Center How-To Guide*.

Note: The email is deleted from the mailbox whether or not it had an attachment.

To set up automatic license import:

1. Click **Control Center** > **System Settings**. The System Settings dialog displays.
2. Click the **License Management** tab.

3. Enter the **E-mail User** and **Password** for the email account to monitor.
4. Enter the email server’s **Host Name** and **Host Port** number.
5. Enter the **E-mail Protocol** (POP3 or IMAP) used.
6. Enter the **Frequency**, in minutes, with which to check for incoming emails with license attachments.
7. Click **Update**.

See *License Management* on page 159 for field definitions.

Chapter 7

Manage Rules and Actions

This chapter describes the following subtopics and procedures:

- About Rules
- Predefined Actions and Rules
- About Actions
- Manage Rules
- Create Multiple Rules

About Rules

A rule is a system instruction that you create and that Sterling Control Center executes automatically. A rule consists of the following parts:

- Criteria that must be met in order for the rule to be applied; for example, a certain return code generated by a file transfer. All criteria in a rule must be met for the rule to be applied.
- One or more schedules that may be associated with a rule. If a schedule is associated with a rule, the rule is applied when the rule's criteria are met *and* a schedule associated with the rule matches.
- An action that is performed when the criteria are met; for example, sending a notification e-mail or generating an alert when a file transfer completes.

Following are examples of rules you can define:

- Generate an alert and an e-mail notification to a system administrator if a Process or file transfer completes with errors
- Monitor a Process or file transfer for specific message IDs, and issue a system command if the message is detected
- Monitor server status and generate an alert if a server error occurs
- Generate an SNMP trap when a Process's return code is 8 or higher

As an example using specific criteria, to monitor all steps in all processes on all servers whose return code was not zero:

Key	Operator	Value
Return Code	Not equal to	0
Event Type	Matches	Process Step Ended

To see a complete list of criteria you can monitor, see *Keys and Fields* on page 291. For more information about how to construct a rule, see *Create a Rule* on page 71.

Predefined Actions and Rules

Sterling Control Center provides predefined actions that generate alerts and predefined rules, including ones that monitor for SLC messages. You can use these actions and rules when creating SLCs to monitor Processes or file transfers. You can also modify the actions and rules as necessary to meet your processing requirements.

See *Use Predefined Actions and Rules in SLCs* on page 92 for how to use predefined rules.

Manage Rules

This section describes the following information:

- About Creating a Rule
- Create a Rule
- Display the Rules Listing
- Using Data Visibility Groups to View Rule Sets
- Change the Order of Rules
- Enable or Disable a Rule

About Creating a Rule

You create rules to define instructions that Sterling Control Center automatically executes. A rule is triggered when a matching event occurs.

Once you create a rule, it is displayed in the Rules listing. Enabled rules are applied in the order in which they are listed in the Rules listing. Therefore, rules with specific criteria should precede rules with general criteria. Only one rule per rule set is triggered per event, so if the first rule is too general a match always occurs and subsequent rules are ignored.

Note: Sterling Control Center ships with predefined rules. See *Predefined Rules* on page 192 for a complete listing.

The following icons are displayed in the Rules listing to indicate a rule's status:

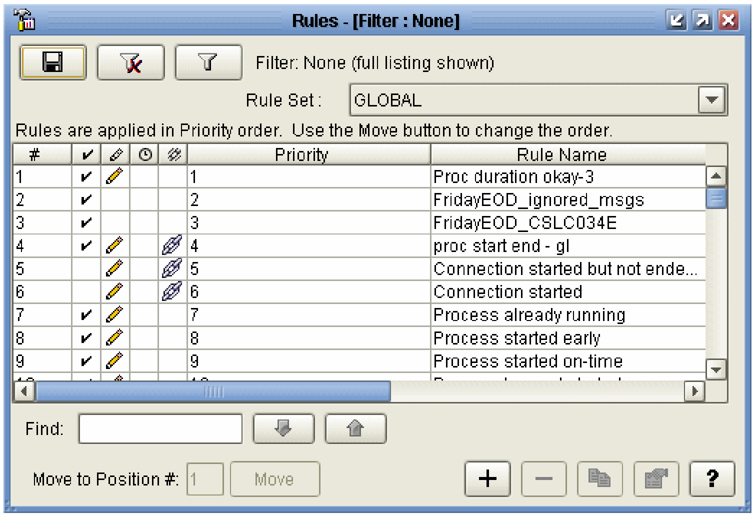
Icon	Description
✓	The rule is enabled.
✏	The rule can be edited by the user viewing the rule.
●	One schedule is associated with the rule and the schedule is enabled.
○	One schedule is associated with the rule and the schedule is disabled.
●●	Multiple schedules are associated with the rule and all schedules are enabled.
●○	Multiple schedules are associated with the rule and some of the schedules are enabled.
○○	Multiple schedules are associated with the rule and all of the schedules are disabled.
🔗	The rule is a linked rule.

Create a Rule

Sterling Control Center comes with a number of predefined rules you can use. You can also create your own new rules.

To create a rule:

1. Select **Manage** > **Rules and Actions** > **Rules** from the Control Center window. The **Rules** listing is displayed.



Rules - [Filter : None]

Filter: None (full listing shown)

Rule Set : GLOBAL

Rules are applied in Priority order. Use the Move button to change the order.

#	✓	✎	◷	⚯	Priority	Rule Name
1	✓	✎			1	Proc duration okay-3
2	✓				2	FridayEOD_ignored_msgs
3	✓				3	FridayEOD_CSLC034E
4	✓	✎		⚯	4	proc start end - gl
5		✎		⚯	5	Connection started but not ende...
6		✎		⚯	6	Connection started
7	✓	✎			7	Process already running
8	✓	✎			8	Process started early
9	✓	✎			9	Process started on-time

Find:

Move to Position #: 1

2. Click **+** to display the **Create Rule** wizard.

Note: For descriptions of Rules fields, see *Rules Field Descriptions* on page 74.

3. Type a **Name** and **Description** for the rule, click **Enable** to enable it, and click **Next**.

4. Specify one or more parameters to further define the rule by choosing a **Key** and **Operator** and entering a **Value**. The list of operators depends on whether the parameter is numeric (Return Code and File Size) or alphanumeric. For more information on the keys you can use in parameters, see *Keys and Fields* on page 291. Click **Next**.

Note: When choosing multiple Values for a single Key, separate the Values with a pipe (|) character and use Reg Ex as the Operator.

5. Select one or more **Schedules** to associate with the rule by moving the schedule (using >) from **Rule / Metadata Schedules** to **Selected Schedules**. Click **Next**.

Note: You can create a new schedule by clicking + below **Rule / Metadata Schedules**. You can duplicate an existing schedule and modify the duplicate by clicking ⧉ . View the properties of a schedule in either **Rule / Metadata Schedules** or **Selected Schedules** by selecting the schedule and clicking 🗎 .

6. Select an **Action** to perform when the defined parameters and schedules are met. For a linked rule, this is the first action to complete when Sterling Control Center detects the initial condition. (For more on actions, see *About Actions* on page 77.) Click **Next**.

> **Note:** You can create a new action by clicking **+** next to **Action**. You can duplicate an existing action and modify the duplicate by clicking . View an action's properties by selecting the action and clicking .

7. If this is a linked rule, take the following steps: Click **Enabled** to enable the linkage. Specify the **Parameters** (conditions) under which the linked rule is to be triggered. Specify a **Resolution Action** to take if the linked rule's condition is resolved before the timeout period has elapsed. Specify a **Non-Resolution Action** to take if the condition remains unresolved after the timeout period has elapsed. And specify the **Timeout** period in minutes.

> **Note:** Process events (Process Started, Process Step Started, Process Step Ended, and Process Ended) are all generated at the same time by Control Center for Connect:Enterprise for z/OS, Connect:Enterprise for UNIX, and most native FTP servers because Control Center only "sees" the file transfer ending event. Be aware of this when writing linked rules for process events for these types of servers.

8. Click **Next** and then **Finish** to add the rule to the **Rules** listing.
9. Click **Close** to close the **Create Rule** wizard.

Display the Rules Listing

The Rules listing lists all rules along with a description and information on their current status. See *About Creating a Rule* on page 70. You can display the listing and sort the columns of information.

To display the **Rules** listing:

1. From the Control Center window, select **Manage > Rules and Actions** > **Rules**.
2. To sort on any column, click on the column heading.

Using Data Visibility Groups to View Rule Sets

From the Rules listing, you can use data visibility groups as a means to filter rules into rule sets.

To view rules by data visibility group:

1. From the Control Center window, select **Manage > Rules and Actions** > **Rules**.
2. From the Rule Set drop down list, select Global to view rules that do not have a data visibility group, or select one of the data visibility groups.

> **Note:** For a data visibility restricted user, the list will contain only the data visibility groups included in the user's role. An unrestricted user will see the Global rule set and all of the data visibility groups.

3. To view a different rule set, select a data visibility group from the Rule Set drop down list.

View or Modify Rule Properties

You can view and make changes to the properties that define a rule.

To view or modify rule properties:

1. Select **Manage > Rules and Actions** > **Rules** from the Control Center window to display the **Rules** listing.
2. Do one of the following to display the **Rule Properties** window:
   - Double-click a rule
   - Select a rule and click
3. Select tabs to display property subgroups and modify properties as necessary. See *Rules Field Descriptions* on page 74 for descriptions of rules fields.

   Note: To make changes, you must have permission to edit the rule. Edit permission is denoted by the ✎ icon.

4. Click **Update**.

Note: If you modify the Rule to change the data visibility group setting in the rule's parameter, the Rules listing panel will automatically change the rule set to the new data visibility group value so that you can see the updated rule in the rule listing once the update is complete.

Rules Field Descriptions

The following table describes the fields that define a rule.

Field	Description
Rule Name	The name of the rule. Required.
Description	Text describing the rule. Optional.
Enabled	Select this option to enable the rule. By default rules are enabled when first created.

Field	Description
Parameters	Selection criteria for further defining the rule. Choose a Key and Operator and enter the Value you want to monitor. For more information on parameters, see *Keys and Fields* on page 291. You must enter at least one parameter. A specific server or server group is required for a server restricted role. A data visibility group is required for a data visibility restricted role. When choosing multiple Values for a single Key, separate the Values with a pipe (|) character and use Reg Ex as the Operator. For easy message ID lookup for Sterling Control Center messages, select Message Id as the Parameter, Matches as the Operator, and then click ... in the Value field. To find and select a message, type any part of the Message ID or text to display matching messages, and click the Insert button. Popup lists are provided for other keys as well, such as Event Type, Data Visibility Groups, and Servers and Server Groups.
Schedules	Schedules to associate with the rule. To add a schedule to the rule definition, highlight the schedule in Rule / Metadata Schedules and click >. To disassociate a schedule from a rule, highlight the schedule in Selected Rule Schedules and click <.
Action	The action to perform when the defined parameters and schedules are met. An action is the activity or activities that Sterling Control Center performs when an event triggers a rule. For more on the types of activities an action can perform, see *About Actions* on page 77.
Linked Rules: Enabled	Click Enabled to make this rule a linked rule. A linked rule specifies a second condition and an action that is performed if the second condition is not resolved within a user-specified timeout period.
Linked Rules: Parameters	The parameters that describe the condition under which the linked rule should be triggered. For more information, see *Create a Rule* on page 71.
Linked Rules: Resolution Action	The action to take if the second condition specified in Linked Rules: Parameters is met prior to the timeout period elapsing.
Linked Rules: Non-Resolution Action	The action to take if the second condition specified in Linked Rules: Parameters is not met before the timeout period elapses.
Timeout	The amount of time after the first conditions are met within which, if the second conditions are met, the resolution action will be taken. If the second conditions are not met within the Timeout period, the nonresolution action will be taken.

Change the Order of Rules

Enabled rules are applied in the order in which they are listed in the **Rules** listing. Rules with specific criteria should precede rules with general criteria. Only one rule per rule set is triggered per event, so if the first rule is too general it may always result in a match, with subsequent rules being ignored.

To change the order of rules:

1. Select **Manage > Rules and Actions** > **Rules** from the Control Center window to display the **Rules** listing.
2. Highlight the rule to reorder.
3. In the **Move selected to position #** field, type the position in which to place the selected rule.
4. Click **Move**.

Note: Be patient while the rule is moved. The Rules listing refreshes when the move is complete.

Note: The rules listing must be sorted in ascending priority order before the move can be accomplished.

Enable or Disable a Rule

Rules must be enabled to be processed. When you first create a rule, it is enabled by default. When you remove the only server or server group used by a rule, the rule is automatically disabled.

To enable or disable a rule:

1. Select **Manage > Rules and Actions** > **Rules** from the Control Center window to display the **Rules** listing.
2. Do one of the following to display the **Rule Properties** window:
   - Select the rule and click 📋.
   - Double-click the rule.
3. Click **Enabled** to place or remove the check mark and click **OK**.

Create Multiple Rules

Sterling Control Center comes with a standalone utility that simplifies creation of multiple actions, rules, and other Control Center objects. The utility is described in *Create Multiple Objects* on page 217.

About Actions

Sterling Control Center performs an action when the occurrence of an event triggers a rule. A Control Center action can perform one or more of the following kinds of activities.

Activity	Description
E-mail	An email address or addresses, or an email list, to which notifications will be sent when the corresponding rule is triggered. Specify the address or addresses, or the email list, to which to send the e-mail, along with the sender e-mail address, a subject line, and message text. You can specify variables to define the e-mail addresses, subject line, and message. You can also send a test e-mail message to make sure an e-mail address is valid. Rather than type multiple addresses individually, you can import a list of email addresses. See *Add Email Addresses to an Action* on page 80.
Alert	Generates a Sterling Control Center alert that an event has occurred. Alerts are displayed in the Active and Handled Alerts monitors.
SNMP trap	Generates an SNMP trap to the SNMP host defined in the Sterling Control Center SNMP Host settings (see *SNMP Hosts Settings* on page 155). SNMP Host system settings must be configured to generate traps.
Operating system command	Executes the specified executable command file on the computer where the Control Center engine is installed, and passes an XML string of the event that triggered the rule to the command file (if no other parameters are passed to the command). You must specify the full path to the command. You can also pass parameters to the command. These parameters can use variables (such as &processName;) which are replaced by the event values. If you designate parameters to pass to the command, Sterling Control Center will not automatically pass the entire XML string of the event to the command. See *Sterling Control Center Variables* on page 231, for the fields to pass as variables. A sample command may be a user-created script that, if a Process fails, writes Process statistics data to a Help desk file. Any user-created scripts should be validated thoroughly before you use them with Sterling Control Center. See the *Sterling Control Center How-To Guide* for an example of an operating system command.

Activity	Description

Server command	Executes the specified command on a Connect:Direct server. You can either select a command template from a list box or type the entire command.
	Note: This activity is not available for Sterling Integrator, Connect:Enterprise, Connect:Direct for OS/400, FTP, or Connect:Direct Select servers.
	The command template contains variables for Process name (&processName;) and Process ID (&processId;). When Sterling Control Center submits the command to the Connect:Direct server, it replaces the variables with the Process name and ID values from the event that triggered the rule.
	For example, if a Process named SENDDATA and numbered 00087654 triggers a rule that sends a DELETE command to the Connect:Direct server, the command template:
	`delete process pname=&processName; pnumber=&processId;`
	translates to:
	`delete process pname=SENDDATA pnumber=00087654`
	See *Sterling Control Center Variables* on page 231 for the fields to pass as variables.
	See the *Sterling Control Center How-To Guide* for an example of a server command.

No operation	Performs no action. Useful when you do not want an alert generated or another action taken. For example, you could have two rules with the same criterion, such as *Server down*, and define them with differing actions: ◆ The first rule has a schedule attached to it (for example, 22:00-23:00 Saturday) when server maintenance is applied. ◆ The second rule has no schedule attached and sends an email to the System Administrator about the server being down. When a server down event occurs during the maintenance window, no email is sent.

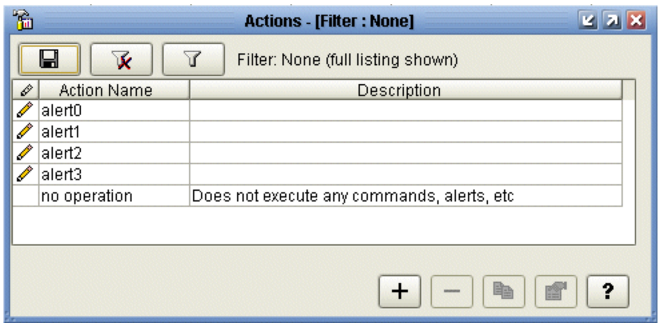
You create an action to define an activity that Sterling Control Center performs when an event triggers a rule. Note the following:

- You can define more than one activity for an action.
- You can import a list of e-mail addresses for the E-mail page. See *Add Email Addresses to an Action* on page 80 for more information.
- Sterling Control Center ships with some predefined actions. See Predefined Rules for a complete listing.

Create an Action

To create an action:

1. Select **Manage** > **Rules and Actions** > **Actions** to display the **Actions** listing.



✎	Action Name	Description
✎	alert0	
✎	alert1	
✎	alert2	
✎	alert3	
	no operation	Does not execute any commands, alerts, etc

2. Click **+** to display the **Create Action** wizard.
3. Type a name and description for the action and click **Next**.
4. To create an email to send whenever the action occurs, define the To, From, Subject, and Message fields. Click To: to specify one or more email lists. (You can create, duplicate, or modify email lists in the Email List window that displays.) Sort the To: list of email addresses in ascending or descending alphabetical order by toggling Sort. Include variables, if you wish, in the Subject line or Message text area. See *Insert Variables* on page 80. To make sure an email address is valid, click **Test**, enter the email address, and click **Send**. Then make sure that the message was received at the destination.
5. To import email addresses, click **Import**. Refer to *Add Email Addresses to an Action* on page 80.
6. Click **Next** to continue.
7. Select the type of alert to generate from the **Alert Severity** drop-down list and click **Next**.
8. Enter information in one or more of the following wizard panels to identify the action criteria:
   - To create SNMP traps, turn on the **Generate SNMP Trap** option.
   - To use operating system commands to define the action, type the commands or the fully-qualified name of a file that contains the commands in the **OS Command** field.
   - To send a command to the Connect:Direct server for execution, type information in the **Server Command** window.
9. Identify the restricted roles that have permission to modify the action.

Note: Unrestricted roles automatically have permission to modify an action.

10. Specify whether the action will be visible to all users or only to the restricted users in the roles you selected. If you make the action visible to all users, you cannot restrict visibility to specific roles after it is created and referenced. Click **Next**.
11. Click **Finish** to add the action to the **Actions** listing.
12. Click **Close** to close the **Create Action** wizard.

Note: For more on specifying the above options, see *Action Field Descriptions* on page 82.

Insert Variables

You can include variables, such as those specifying the action name or event type, when you define an action’s e-mail, OS command, or server command settings. The E-mail, OS Command, and Server Command tabs on the Action Properties window contain fields in which you can insert variables.

To insert a variable when defining an action:

1. Click in one of the text entry fields with an associated Insert Var button.
2. Click **Insert Var**.
3. In the Select Variable window, select a variable and click **OK**.

   The variable is inserted into the text field.

   Note: Use the variable list in the Select Variable window rather than inserting variables by typing them in. If the variable you enter is not contained in the Select Variable list, it will not be substituted.

Add Email Addresses to an Action

You can add email addresses to an action in the form of an email address or an email list or lists.

You can also import a text file that contains a list of email addresses. The addresses in the text file can be delineated by commas or line breaks.

To add an email list to an action:

1. Click **To:**. The Email Lists window displays.
2. Select lists from the Email Lists column and click **>** to move them to Selected Email Lists. You can add, duplicate, or view properties of email lists here too.
3. Click OK.

To import a text file containing a list of email addresses into an action:

1. Select **Manage > Rules and Actions** > **Actions** from the Control Center window to display the **Actions** listing. Double-click the action to open the **Action Properties** window.
2. From the **E-mail** tab, click **Import**.
3. Navigate to the text file containing the e-mail addresses, select it, and click **Import**. The file contents are imported. If you have already made an entry, the new text replaces the existing text.

Export Email Information from an Action

You can export to a text file a list of addresses that have been entered into an action’s To: field.

To export a list of email addresses:

1. Select **Manage > Rules and Actions** > **Actions** from the Control Center window to display the **Actions** listing. Double-click an action to display its properties.
2. From the **E-mail** tab, click **Export**. A file selection window is displayed.
3. Select a location for the text file.
4. Type a name for the text file and click **Export**. The information is exported to a text file.

Sort Email Addresses

Click **Sort** to put the e-mail addresses on the **Create Action - E-mail** window in ascending or descending order.

Display the Actions Listing

To display the **Actions** listing:

1. From the Control Center window, select **Manage > Rules and Actions** > **Actions**.
2. To sort on any column, click the column heading.

View or Modify Actions

To view or modify an action:

1. Select **Manage > Rules and Actions** > **Actions** from the Control Center window to display the **Actions** listing.
2. Do one of the following:
   - Select an action and click
   - Double-click the action.
3. Click in a field to view field-level help. Field-level help is displayed in the status bar.
4. Modify the action information as necessary. See *Action Field Descriptions* on page 82 for definitions of action fields.

   Note: To make changes, you must have permission to edit the action. Edit permission is denoted by the ✎ icon.

5. Click **OK** when finished.

Action Field Descriptions

The following table describes the fields that define an action.

General	
Field Name	**Description**
Name	The name of the action. An action is an activity that Sterling Control Center performs when an event triggers a rule. For more on the activities an action can perform, see *About Actions* on page 77.
Description	Text describing the action. Optional.
E-mail	
Field Name	**Description**
To	The e-mail addresses of recipients to be notified when this action is triggered. Optional.
From	The return e-mail address that will appear on notification e-mails. If you specify a To: address, the From: address is required.
Subject	Text to be inserted in the e-mail's subject line. If you specify a To: address, Subject is required.
Message	The text of the e-mail. Optional.
Alert	
Field Name	**Description**
Alert Severity	A number from 0-3 that indicates how severe or critical the alert is. Severity is indicated on the Queued or Completed Activity monitors, or the Handled or Active Alerts monitors, with a color-coded icon. This field is optional. To choose a severity level, select one of the following: 0–In compliance (no alert icon generated). A severity level 0 alert deletes all previous alerts for the same SLC instance. 1–High severity (red alert icon generated) 2–Medium severity (orange alert icon generated) 3–Low severity (yellow alert icon generated)
SNMP Trap	
Field Name	**Description**
Generate SNMP Trap	Turn on this option to generate an SNMP trap to the host defined in the Sterling Control Center SNMP Host settings. SNMP Host system settings must be configured to generate traps.

OS Command

Field Name	Description
Enter operating system command text	Execute the specified executable command file on the computer where the Control Center engine is installed, and pass an XML string of the event that triggered the rule to the command file (if no other parameters are passed to the command). You must specify the full path to the command. You can also pass parameters to the command. These parameters can use variables (such as &processName;) which are replaced by the event values. If you designate parameters to pass to the command, Sterling Control Center does not automatically pass the entire XML string of the event to the command. See *Sterling Control Center Variables* on page 231, for the fields to pass as variables. Example: An action could specify an operating system command that references a user-created script which, if a Process fails, writes Process statistics data to a Help desk file. See the *Sterling Control Center How-To Guide* for details on setting up such an action. You should thoroughly validate any user-created scripts before using them with Sterling Control Center.

Server Command

Field Name	Description
Server	The name of the server on which to run the server commands entered.
Command Template	A template that gives you suggestions on server command syntax, for use in creating alerts. You can make changes to a command after displaying the template. For example, selecting Delete Process Command from the Command Template displays the following: delete process pname=&processName; pnumber=&processId;

Server Command	A command sent to the Connect:Direct server for execution. You can type the entire command or select a command template. If you select a command template, Sterling Control Center replaces any variables fields (fields beginning with “&” and ending with ";") with the actual values from the event record. For example, selecting Delete Process Command from the Command Template displays the following command: delete process pname=&processName; pnumber=&processId; **Note:** It is not necessary to terminate server commands with an additional semicolon. Sterling Control Center replaces &processName; with the Process name and &processId; with the Process ID from the event. See *Sterling Control Center Variables* on page 231, for the fields to pass as variables. The command must use valid Connect:Direct syntax. See the Connect:Direct documentation for the server platform for information on command syntax.
Permissions	
Field Name	**Description**
Restricted Roles	List of restricted roles defined in Sterling Control Center. Select a role and click < or > to move the role between this field and Selected Roles.
Selected Restricted Roles	Restricted roles with rights to modify this action. If no roles are selected, then only an unrestricted user (admin) can modify this action.
This action is visible to all users	When selected, this option makes the action public and available for selection by all users. Once a public action is referenced by any other object, you cannot make it private by restricting visibility to specific roles/users.
This action is visible to restricted users in these Selected Restricted Roles	When restricted roles are selected, this option allows only restricted users in the selected roles to view/select/edit the action.

Create Multiple Actions

Sterling Control Center comes with a standalone utility that simplifies creation of multiple actions, rules, and other Control Center objects. The utility is described in *Create Multiple Objects* on page 217.

Chapter 8

Manage Service Level Criteria

This chapter discusses the following subtopics and procedures:

- About Service Level Criteria
- SLC Group Components
- The SLC Monitoring Window
- SLC Event Messages
- Create an SLC
- Maintain SLC Groups
- Use Predefined Actions and Rules in SLCs
- Create Multiple SLCs and Schedules

About Service Level Criteria

Service level criteria (SLCs) are performance objectives that require processing to occur within a certain time window. For example, a Connect:Direct process may need to begin by 8:00 p.m. and end by 8:30 p.m. An SLC might monitor for the timeliness of both events. If either does not occur within a certain window, the SLC can be used to notify you of that fact.

Control Center can monitor processing start times, stop times, or durations depending on the type of SLC schedule you define. You can define a rule that creates an alert and then view the alert through the Alerts Monitor.The alert might lead you to investigate to determine why the processing did not occur as expected, and to make corresponding adjustments.

SLCs can be defined to monitor for one or more:

- Connect:Direct Process starts, ends, and durations
- Connect:Direct Process step starts, step ends, and durations
- Sterling Integrator business Process starts, ends, and durations
- Sterling Integrator business Process activity starts, ends, and durations
- Sterling Integrator AFT transfer starts, ends, and durations

- Sterling File Gateway Arrived Files, Routes, and Delivery starts, ends, and durations
- Connect:Enterprise batch arrivals and transmissions
- FTP PUTs and GETs

SLC Group Components

An SLC combined with one or more schedules to define time requirements makes an SLC group.

There are four types of SLC groups:

- Standard—Standard SLC groups monitor specific Process names, file names, etc. Use standard SLC groups when you know the specific item to monitor.
- Wildcard—Wildcard SLC groups monitor Processes, file names, etc. with names that don’t remain constant, such as Batch IDs with the date and time in their names. To specify monitoring criteria in wildcard groups, you can use the wildcard characters asterisk and question mark, or regular expressions (regex).
- Workflow—Workflow SLC groups monitor the flow of related Processes. For example, a workflow SLC can monitor a transaction consisting of three Processes, all of which must run and finish within three hours of the first Process’s initiation.
- Simple—Simple SLCs are created using a question/answer format to define the scenario you want to monitor and to select basic parameters and specify values for those parameters. For more information about simple SLCs, see *About Simple SLCs* on page 107.

There are two types of SLC schedules:

- Calendar schedule—With a calendar schedule, processing must start or end (or both) within a specified time range. For example, a Process might be expected to start between 19:00 and 19:30 and end between midnight and 00:30. Calendar schedules are useful for processing that occurs at a fixed time.

  Note: Start and end times are entered in 24-hour (hh:mm) format.

  A calendar schedule for an SLC has a normal start range (NSR) and a normal end range (NER), or both. For example, you might specify a schedule named Wednesday Evening that defines the NSR as 20:00–21:00 and the NER as 22:00–23:00 on every Wednesday.

  A calendar schedule for a rule has a start date, end day, and end time. For example, you can specify a schedule named First of the Month that begins now and runs the first day of every month with no end date specified.

  Calendar schedules require that you create one or more calendars. A calendar defines the dates on which processing is scheduled to occur. Calendars specify daily, weekly, monthly, or annual processing dates, and also specify exceptions to the normal processing calendar.

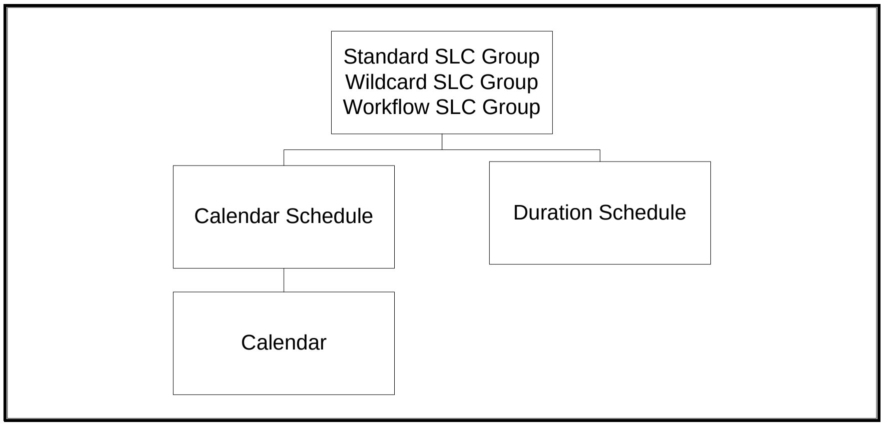
  Sterling Control Center includes eight predefined calendars (Daily, and one for each day of the week) for your use.

- Duration schedule—With a duration schedule, processing can start at any time but must complete within a specified number of hours, minutes, and seconds. Duration schedules use a minimum duration and a maximum duration to define the processing window. They also identify the points at which a given percentage of processing is complete.

Note: Minimum and Maximum Duration times include hours, minutes, and optionally seconds (hhh:mm[:ss]). Hour and minute values are required, even if those values are zero.

Duration schedules are useful for processing that begins at varying times but must run for a certain time interval. For example, a Process may be triggered by completion of a previous Process. Because you cannot predict when the first Process will end, you cannot set a reliable start time for the second Process. However, you can specify that when the second Process does start, it must finish within 30 minutes.

The following illustration shows the SLC components:



To provide greater monitoring flexibility, an SLC group can be associated with multiple schedules. Also, a schedule can be associated with different SLC groups, and a calendar can be associated with multiple schedules.

Note: Assigning more than one schedule, server name, file name, or Process name to an SLC is what makes the SLC an SLC group, because each schedule, server name, file name, or Process name results in a separate SLC instance.

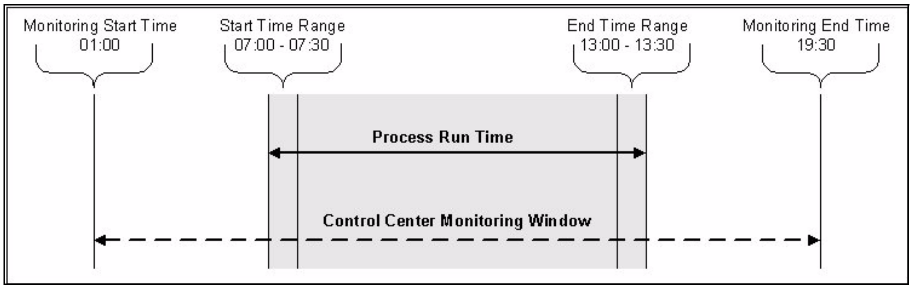
The SLC Monitoring Window

For calendar schedules, Sterling Control Center monitors SLC activity for a specified number of hours before and after the schedule requirements you have set up. The monitoring window is set at wider than the schedule to detect a start that is earlier or an end that is later than expected. For example, if a calendar schedule specifies that a Process must start by 07:00 and end by noon, you might set the SLC to begin monitoring for the Process at 01:00 and stop monitoring for it at 18:00.

For duration schedules, only the end window tolerance value is applicable. Sterling Control Center monitors for a specified number of hours after the maximum duration is reached. For example, if a

Process that should take 20 minutes to complete starts at 14:00, Control Center might be set to monitor for completion until 20:20.

The following illustration shows a sample calendar-schedule SLC monitoring window:



The **Start Window Tolerance** and **End Window Tolerance** fields on the Create SLC Group wizards determine the size of the monitoring window for each SLC. The default is six hours before expected start and six hours after expected end of the schedule requirement.

SLC Event Messages

Whenever a monitored item either meets or fails to meet its SLC, Sterling Control Center generates an SLC event message. You can use SLC event message IDs in rules to trigger an action, such as one that generates an alert to display in the alerts monitors.

See *Message IDs for Rules* on page 195 for a list of SLC event message IDs that Control Center generates and the conditions that cause them.

Create an SLC

You can create these kinds of SLCs:

- Standard
- Wildcard
- Workflow
- Simple

Note: Although simple SLCs are based on workflow SLCs, they differ from workflow SLCs in several ways. For more information about simple SLCs, see *About Simple SLCs* on page 107.

About Creating SLCs

Creating an SLC involves completing the following tasks:

1. Review the processing schedule to determine the times when processing must start and complete, and how long processing can run. In the case of a workflow SLC, determine what relationships, such as contingency, exist among processes in the workflow.
2. Create calendars in Sterling Control Center—or use a predefined calendar—based on your review of the processing schedule. Calendars are used in schedules. The same calendar can be used in multiple schedules.
3. Set up SLC schedules in Sterling Control Center based on your review of the processing schedule and the calendars created in step 2. The same SLC schedule can be used with different SLCs. Multiple SLC schedules can be used with one SLC.
4. Review processing to group different items into SLC groups. For example, if a set of Processes runs at the same time, the Processes should be placed into one SLC group.
5. Create the SLC group.

When you create an SLC group it is displayed in a listing of all groups of its type—standard, wildcard, workflow, or simple (see *Display an SLC Group Listing* on page 90).

SLC Group Status Icons

The SLC group listings display icons that describe each group and give its status. The icons are described in the following table.

Icon	Description
✓	The SLC group is enabled.
✎	The SLC group can be edited by the user viewing it.
🕒	One schedule is associated with the SLC group and the schedule is enabled.
◷	One schedule is associated with the SLC group and the schedule is disabled.
🕒🕒	Multiple schedules are associated with the SLC group and all schedules are enabled.
🕒◷	Multiple schedules are associated with the SLC group and some of the schedules are enabled.
◷◷	Multiple schedules are associated with the SLC group and all of the schedules are disabled.

Maintain SLC Groups

The following SLC maintenance tasks can be used for all SLC types:

- Display an SLC Group Listing
- Using Data Visibility Groups to View SLC Groups

The following tasks can be used for standard, wildcard, and workflow SLC groups:

- View or Modify Properties of an SLC Group
- Add or Remove Schedules from an SLC Group
- Enable or Disable an SLC

Display an SLC Group Listing

You can display a listing of all SLC groups by SLC group type (standard, wildcard, workflow, or simple). The listing shows the SLC group names, a description, and icons that relate information about the group's current status.

Note: For a description of the icons, see *SLC Group Status Icons* on page 89.

To display an SLC group listing:

From the Control Center window, select **Manage** > **Service Level Criteria (SLCs)** > and then select the type of SLC group. The corresponding SLC group listing displays.

Using Data Visibility Groups to View SLC Groups

From the SLC listings, you can use data visibility groups as a means to filter SLCs into sets.

To view SLCs by data visibility group:

1. From the Control Center window, select **Manage > Service Level Criteria (SLC)** > and then select the type of SLC group.
2. From the SLC Set drop down list, select Global to view SLCs that do not have a data visibility group, or select one of the data visibility groups.

   Note: For a data visibility restricted user, the list will contain only the data visibility groups included in the user's role. An unrestricted user will see the Global SLC set and all of the data visibility groups.

3. To view a different SLC set, select a data visibility group from the SLC Set drop down list.

View or Modify Properties of an SLC Group

You can view an existing SLC group and change any of its properties except for the name.

To view or change an SLC group:

1. Select **Manage** > **Service Level Criteria (SLCs)** > and then select the type of SLC group from the Control Center window to display the corresponding listing.
2. Double-click an SLC to display its properties window, or select the SLC and click 📝.
3. Change the information as required and click **Update**. For a description of SLC Group fields, see *Standard and Wildcard SLC Field Descriptions* on page 95, or *Workflow SLC Field Definitions* on page 101.

   The SLC information is updated.

Add or Remove Schedules from an SLC Group

To add or remove one or more schedules for an SLC group:

1. Select **Manage** > **Service Level Criteria (SLCs)** > and then select the type of SLC group from the Control Center window.
2. Double-click an SLC to display its SLC group properties window.
3. Select the **Schedules** tab to display a list of defined schedules.
4. Do one of the following:
   - Add a schedule by highlighting it in the **All Schedules** box and clicking >.
   - Remove a schedule by highlighting it in the **Selected Schedules** box and clicking <.
5. Click **Update** to close the SLC group properties window.

Enable or Disable an SLC

To enable or disable an SLC:

1. Select **Manage** > **Service Level Criteria (SLCs)** > and then select the type of SLC group from the Control Center window.
2. Double-click the SLC you want to enable or disable. The corresponding group properties window is displayed.
3. Select the **Enabled** box on the **General** tab to enable the SLC, or deselect to disable the SLC, and click **Update**. For a Simple SLC, Click the **Enable this SLC** box on the **How will it be identified** screen.
4. Click **Close**.

Note: When you remove from Sterling Control Center the only server or server group that is used by an SLC, the SLC is automatically disabled.

Use Predefined Actions and Rules in SLCs

Sterling Control Center provides predefined actions and rules. You can use these actions and rules to monitor for SLC events and generate alerts when they occur. You can modify the predefined actions and rules as necessary to meet your processing requirements.

These actions and rules are displayed in the **Actions** and **Rules** listings, respectively.

To modify a predefined action or rule:

1. Create an SLC to monitor a Process or file transfer. (See *Create an SLC* on page 88.)
2. Review Predefined Rules to find the rule you wish to modify.
3. Review *Message IDs for Rules* on page 195 to find the message IDs generated by the SLC.
4. Access the rule for each associated message ID. On the Server Groups or Servers tab, select the server group or servers to monitor. (See *Manage Rules and Actions* on page 69.)
5. All predefined rules, except for one, are enabled. (The one exception is the *Monitor rate out of compliance* rule.) If you do not want to use a rule, you must disable it. (See *Enable or Disable a Rule* on page 76.) See Predefined Rules, for a complete listing of the predefined rules.

Create Multiple SLCs and Schedules

Sterling Control Center comes with a standalone utility that simplifies creation of multiple actions, rules, and other Control Center objects. The utility is described in *Create Multiple Objects* on page 217.

Create a Standard SLC Group

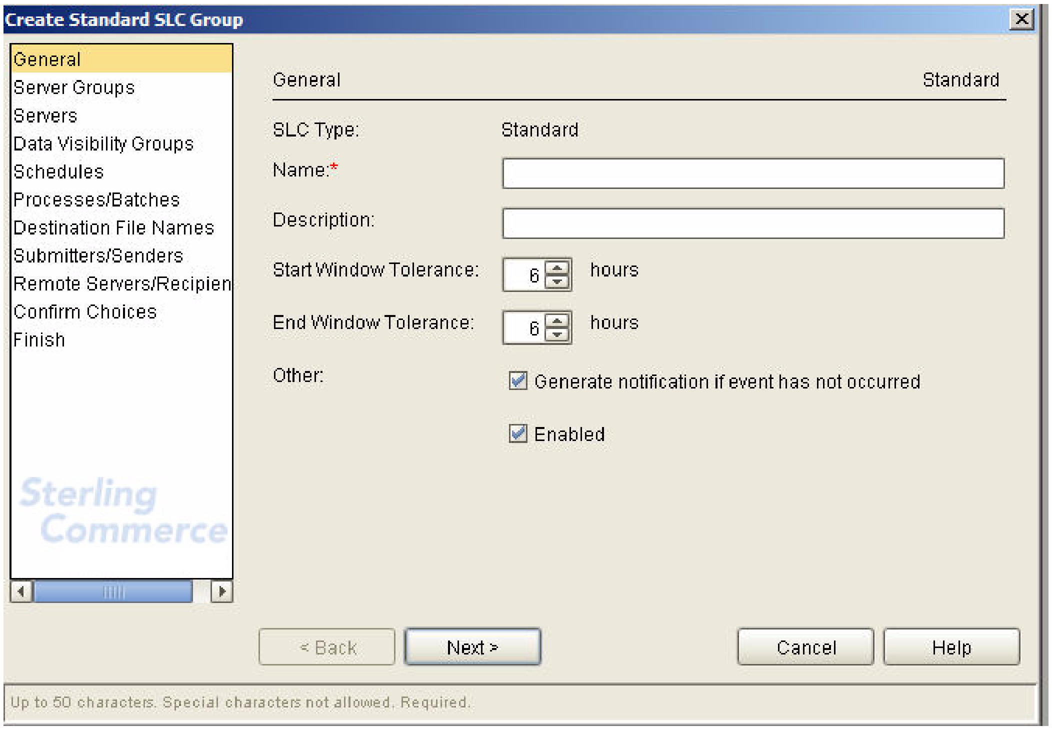
Standard SLC groups are used to monitor the following items:

- Connect:Direct Process starts, ends, and durations
- Connect:Direct Process step starts, step ends, and durations
- Sterling Integrator (Sterling Integrator) business Process starts, ends, and durations
- Sterling Integrator business Process activity starts, ends, and durations
- Sterling Integrator AFT transfer starts, ends, and durations
- Sterling File Gateway Arrived Files, Routes, and Delivery starts, ends, and durations
- Connect:Enterprise batch arrivals and transmissions
- FTP GETs and PUTs

You can import a text file containing a list of Process names, file names within Processes, submitter IDs, batch IDs, or Mailbox IDs into an SLC. See *Import Information into a Standard SLC Group* on page 96 for more information.

To create a standard SLC group:

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Standard SLC Groups**. The Standard SLC Groups listing displays.
2. Click + to display the **Create Standard SLC Group** wizard.



General — Standard

SLC Type: Standard

Name:*

Description:

Start Window Tolerance: 6 hours

End Window Tolerance: 6 hours

Other: ☑ Generate notification if event has not occurred

☑ Enabled

Up to 50 characters. Special characters not allowed. Required.

3. Enter a **Name** and **Description** for the SLC.

Note: For descriptions of standard SLC fields, see *Standard and Wildcard SLC Field Descriptions* on page 95.

4. Select values for the **Monitor Window Tolerance** fields.
5. If you want to be notified when an event does not occur, select the **Generate notification if event has not occurred** field.
6. To enable the SLC, check **Enabled**.
7. Click **Next** to continue.
8. On the **Server Groups** page, identify one or more server groups to monitor by selecting the name in **Groups** and clicking **>** to move it to **Server Groups**. Click **Next** to continue.
9. Identify individual servers to monitor by selecting the server name in **Servers** and clicking **>** to move it to **Selected Servers**. Click **Next** to continue.

Note: You must select at least one server group or server from the lists on the Server Groups and Servers wizard pages.

10. On the **Data Visibility Groups** page, select the data visibility group to associate with this SLC by selecting the name in **Data Visibility Groups** and clicking **>** to move it to **Selected** Data **Visibility Groups**.

Note: If you are a data visibility restricted user, you are required to select a data visibility group for the SLC.

Click **Next** to continue.

11. On the **Schedules** page, identify one or more schedules to associate with the SLC. At least one schedule is required. Click **Next** to continue.
12. In the **Processes/Batches**, **File Names**, **Submitters/Senders**, and **Remote Servers/Recipients** pages, enter the item or items to monitor, or click **Import** to import files containing this information. Click **Next** to move through each of these wizard pages.

Tip: To allow one SLC to monitor multiple instances of the same Process or file name, check Allow Duplicates on the Processes/Batches or File Names pages.

13. On the **Confirm Choices** page, click **Finish**. The SLC is added to Control Center.
14. Click **Close** on the **Finish** page to close the wizard.

If you want the SLC to generate an alert, you must create and enable the corresponding action and rule. See *Manage Rules and Actions* on page 69 or the *Sterling Control Center How-To Guide* for more information.

Standard and Wildcard SLC Field Descriptions

The fields that make up a standard or wildcard SLC are described in the following table.

Field	Description
Name	A unique name for the SLC.
Description	Descriptive information to further identify the SLC.
Start Window Tolerance	The number of hours before the expected start of processing to begin monitoring. The default is 6 hours before the schedule requirements. The range is 0–24 hours.
End Window Tolerance	The number of hours after the expected end of processing to stop monitoring. The default is 6 hours after the schedule requirements. The range is 0–24 hours.
Concurrence Count (Wildcard SLC)	For a wildcard SLC associated with a calendar schedule, the number of SLC instances expected to be seen during the scheduled time. For a wildcard SLC associated with a duration schedule, the number of instances of the SLC that may run at one time.
Other: Generate notification if event has not occurred	Check this option to generate notification of events (an alert) for an SLC when an event fails to occur. If this option is checked and one or more calendar schedules are associated with the SLC, events are generated when service-level criteria are not met. If it is unchecked, events (positive or negative) are generated only if the SLC criteria are met. For example, you might create an SLC to monitor a Process that normally runs at 1pm on Fridays. If the process never runs on Friday, an SLC event would be generated only if this box is checked. If it is not checked, SLC events would be generated only if the Process ran (whether early, on time, or late).
Other: Enabled	Click to enable the SLC.
Groups	The server groups to choose from.
Selected Groups	The server groups (chosen from **Groups**) that this SLC is to monitor. At least one server or server group is required.
Servers	The list of servers to choose from.
Selected Servers	The servers (chosen from **Servers**) that this SLC is to monitor. At least one server or server group is required.
Data Visibility Groups	The list of visibility groups to choose from.
Selected Data Visibility Groups	The data visibility group (chosen from **Data Visibility Groups**) that is associated with this SLC. Only one data visibility group can be selected for an SLC. Data visibility group restricted users must select a data visibility group when creating an SLC (their first Data Visibility Group is automatically selected). Only events applicable to the data visibility group specified will be processed by the SLC.

Field	Description
Expression (Wildcard SLC)	For wildcard SLCs, the regular expression or wildcard definition used in constructing matching criteria (against Processes/batch IDs, filenames, submitters/mailboxes, remote servers). This expression must follow RegEx or wildcard syntax. Regular expressions can be used to match text or numeric strings that follow a particular pattern. Special characters are allowed. To test the value you define in this field, click Test.
RegEx (Regular Expression)	For wildcard SLCs, check to indicate that the above expression is a regular expression.
All Schedules	The list of schedules to choose from.
Selected Schedules	Schedule or schedules to apply to the SLC. At least one schedule is required.
Process Names/Batch IDs	The Connect:Direct Process names or Connect:Enterprise batch IDs to monitor. At least one entry among Process Names/Batch IDs, File Names, Submitters/Sender Mailbox IDs, and Remote Servers/Recipient Mailbox IDs is required.
Allow Duplicates	Check to allow Sterling Control Center to monitor multiple Processes or batches with the same name.
File Names	A list of the destination file names of files copied by a Process. At least one entry among Process Names/Batch IDs, File Names, Submitters/Sender Mailbox IDs, and Remote Servers/Recipient Mailbox IDs is required.
Submitters/Sender Mailbox IDs	A list of submitters or sender mailbox IDs to monitor. At least one entry among Process Names/Batch IDs, File Names, Submitters/Sender Mailbox IDs, and Remote Servers/Recipient Mailbox IDs is required.
Remote Servers/Recipient Mailbox IDs	A list of remote servers or recipient mailbox IDs to monitor. At least one entry among Process Names/Batch IDs, File Names, Submitters/Sender Mailbox IDs, and Remote Servers/Recipient Mailbox IDs is required.

Import Information into a Standard SLC Group

You can import a text file into a standard SLC group. The text file may include information about:

- Connect:Direct or FTP Process names and Sterling Integrator business process names
- File names within Connect:Direct or FTP Processes or Sterling Integrator business process activities
- Connect:Direct or FTP remote servers/recipients
- Connect:Direct or FTP Process or Sterling Integrator business process submitter IDs
- Connect:Enterprise Batch IDs
- Connect:Enterprise sender and recipient Mailbox IDs

To import a file into an SLC:

1. Click **Import** on one of the following SLC Create wizard or Properties pages:
   - **Processes/Batches**
   - **File Names**
   - **Submitters/Senders**
   - **Remote Servers/Recipients**
2. In the Import window that displays, navigate to the text file, select it, and click **Import**. The text is imported. Multiple items must be separated by commas. You can edit the imported text if necessary.
3. Click **Next** to continue.

Export Information from a Standard SLC Group

You can export the following information from a standard SLC group to a text file:

- Connect:Direct or FTP Process names and Sterling Integrator business process names
- File names within Connect:Direct or FTP Processes or Sterling Integrator business process activities
- Connect:Direct or FTP remote servers/recipients
- Connect:Direct or FTP Process or Sterling Integrator business process submitter IDs
- Connect:Enterprise Batch IDs
- Connect:Enterprise sender and recipient Mailbox IDs

To export information from an SLC to a text file:

1. Click **Export** on one of the following SLC Create wizard or Properties pages:
   - **Processes/Batches**
   - **File Names**
   - **Submitters/Senders**
   - **Remote Servers/Recipients**
2. Select a location to store the text file.
3. Type a name for the text file and click **Export**. The information is exported.
4. Click **Next** to continue.

Sorting Information

To put the list of Processes, file names, submitter IDs, Batch IDs, Mailbox IDs, or remote servers in ascending or descending order, Click **Sort**.

Create a Wildcard SLC Group

Use wildcard SLC groups when you do not know or cannot specify the servers, Processes, destination file names, submitter IDs, batch IDs, or mailbox IDs to monitor. To specify the monitoring criteria, you can use either the wildcard characters asterisk (*) or question mark (?) (the default), or regular expressions. See *Regular Expressions* on page 229, for basic regular expression syntax and examples.

To create a wildcard SLC group:

1. Select **Manage > Service Level Criteria (SLCs)** > **Wildcard SLC Groups**. The Wildcard SLC Groups listing displays.
2. Click + to display the **Create Wildcard SLC Group** wizard.
3. Type a **Name** for the SLC and, optionally, a **Description**.

   Note: For field descriptions, see *Standard and Wildcard SLC Field Descriptions* on page 95.

4. For **Start Window Tolerance**, specify the number of hours before a schedule requirement to begin monitoring for SLC activity. For **End Window Tolerance**, specify the number of hours after a schedule requirement to stop monitoring for SLC activity.
5. Specify the **Concurrence Count**. For a wildcard SLC associated with a calendar schedule, specify the number of SLC instances expected to be seen during the scheduled time. For a wildcard SLC associated with a duration schedule, specify the number of instances of the SLC that may run at one time.
6. If you want to be notified when an event does *not* occur, enable the **Generate notification if event has not occurred** field.
7. To enable the SLC, check **Enabled**.
8. Click **Next** to continue.
9. On the **Server Groups** page, identify a server group to monitor by selecting the name in **Groups** and clicking **>** to move it to **Server Groups**. You must select at least one server group or server from the lists on this or the Servers wizard page. Click **Next** to continue.
10. Identify servers to monitor by entering an **Expression**. Select **RegEx** if the expression is a regular expression. You can test the expression by clicking **Test**. (See *Test Expressions* on page 99.) You must make an entry either here or on the Server Groups wizard page. Click **Next** to continue.
11. On the **Data Visibility Groups** page, select the data visibility group to associate with this SLC by selecting the name in **Data Visibility Groups** and clicking **>** to move it to **Selected Data Visibility Groups**.

    Note: If you are a data visibility restricted user, your own data visibility group will be automatically selected.

    Click **Next** to continue.

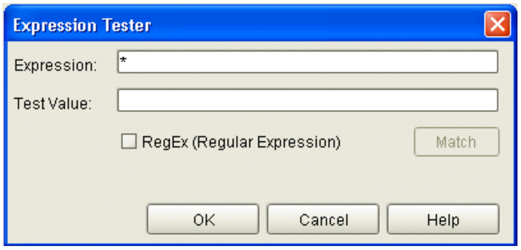
12. On the **Schedules** page, identify one or more schedules to associate with the SLC. At least one schedule is required. Click **Next** to continue.
13. In the **Processes/Batches**, **File Names**, **Submitters/Senders**, and **Remote Servers/Recipients** pages, identify the items to monitor by entering an **Expression**. Select **RegEx** if the expression is a regular expression. You can test the expression by clicking **Test**. (See *Test Expressions* on page 99.) Click **Next** to move through each wizard page.
14. On the **Confirm Choices** page, click **Finish**. The SLC is added to Control Center.
15. Click **Close** on the **Finish** page to close the wizard.
16. If you want the SLC to generate an alert, you must create and enable the corresponding action and rule. See *Manage Rules and Actions* on page 69 or the *Sterling Control Center How-To Guide* for more information.

Test Expressions

The **Expression Tester** window enables you to test standard wildcard and regular expressions. (See *Regular Expressions* on page 229.)

To test an expression:

1. In the Servers, Processes/Batch IDs, File Names, Submitters/Mailbox IDs, or Remote Servers page of the Create Wildcard SLC wizard, or the Create Workflow Milestone page of the Create Workflow Wizard, type an expression in the **Expression** text box and click **Test** (see *Create a Wildcard SLC Group* on page 98 or *Create a Workflow SLC Group* on page 100). The **Expression Tester** window is displayed with the expression you typed.



Expression: *

☐ RegEx (Regular Expression)

2. Type a Test Value to test the expression against. For example, to test the wildcard expression ServX*, you could type `ServX45`. This field is case sensitive.
3. Select **RegEx (Regular Expression)** to test a regular expression.
4. Click **Match**. Depending on whether the value matches the expression, True or False is displayed below the **Match** button. If necessary, verify your wildcard syntax and test again.
5. Click **OK** or **Cancel** to return.

Create a Workflow SLC Group

You use workflow SLC groups to monitor a group of related or sequential processes or process steps. Workflow SLCs monitor related or contingent processes and process steps by tracking them as milestones in a workflow.

In creating a workflow SLC group, you specify information in the following categories:

- General information, such as name and description of the workflow SLC group
- An overall schedule or schedules for the SLC
- Milestones representing the processes or process steps
- A time range/duration for each milestone. These values can be based on the workflow SLC's actual start or its scheduled start.
- Parameters, including optional message lists for generating workflow SLC messages. These messages include jeopardy messages and fire-once messages.

If you want the workflow SLC to generate an alert, you must create and enable the corresponding action and rules. See *Manage Rules and Actions* on page 69, for more information.

To create a workflow SLC group:

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Workflow SLC Groups**. The Workflow SLC Groups listing displays.
2. Click **+** to display the **Create Workflow SLC Group** wizard.
3. On the **General** page, enter general information about the workflow SLC and click **Next** to continue to the next page.

   Note: For a description of each field, see *Workflow SLC Field Definitions* on page 101.

4. On the **Data Visibility Groups** page, select the data visibility group to associate with this SLC by selecting the name in **Data Visibility Groups** and clicking **>** to move it to **Selected Data Visibility Groups**.

   Note: If you are a data visibility restricted user, your own data visibility group will be automatically selected.

   Click **Next** to continue.
5. On the **Schedules** page, move one or more schedules from All Schedules to Selected Schedules by selecting it and clicking **>**. To move a schedule out of the Selected Schedules list, select it and click **<**. Click **Next** to continue to the next page.
6. On the **Parameters** page, enter details regarding how milestone time values are to be handled, the SLC concurrence count, an optional correlator value, and optional Jeopardy and Fire-Once Message Lists.

   For more information on the values you can select for a correlator source, see *Sterling Control Center Variables* on page 231. For more information on message lists, see *Maintain Message Lists* on page 102.

7. Click **Next** to continue to the next page.
8. On the **Milestones** page, add one or more milestones by clicking + and creating the milestone. See *Maintain Milestones* on page 104 for more information.
9. Click **Finish** on the **Confirm Choices** page to confirm the selections you've made.
10. Click **Close** on the **Finish** page to add the SLC to the Workflow SLC listing.

For more details on setting up workflow SLCs, see the examples provided in the *Sterling Control Center How-To Guide*.

Workflow SLC Field Definitions

The following table describes the fields that make up a workflow SLC.

Field	**Description**
Name	The workflow SLC's name.
Description	Text describing the workflow SLC. Optional.
Enabled	Check to enable the workflow SLC. Default is enabled.
Generate notification if event has not occurred	If this option is checked and one or more calendar schedules are associated with the workflow, *and* if the workflow does not run when specified, notifications of events are generated. If the option is unchecked, notifications of events (positive or negative) are generated only if the workflow runs.
Suppress Milestone Messages	Check this option to prevent notifications that pertain to workflow SLC milestones. When this option is checked, only notifications that refer to the workflow SLC itself are generated.
Monitor Window Tolerances: Start	The number of hours before a schedule requirement to monitor for workflow SLC activity. The default is 6 hours before the schedule requirement. The range is 0–24 hours.
Monitor Window Tolerances: End	The number of hours after a schedule requirement to monitor for SLC activity. The default is 6 hours after the schedule requirement. The range is 0–24 hours.
Data Visibility Groups	The list of data visibility groups to choose from.
Selected Data Visibility Groups	The data visibility group (chosen from **Data Visibility Groups**) that is associated with this SLC. Only one data visibility group can be selected for an SLC. Data visibility group restricted users will have their first data visibility group automatically selected. Only events applicable to the DVG specified will be processed by the SLC.
Schedules	The schedule or schedules to associate with the workflow SLC.
Milestone times Relative to: Actual Start of Workflow SLC	Select this option to indicate that milestone times in the workflow SLC are relative to the time that the SLC actually starts. This option and the following option are mutually exclusive, and one is required.

Field	Description
Milestone times Relative to: Scheduled Start of Workflow SLC	Select this option to indicate that milestone times in the workflow SLC are relative to the time that the SLC is scheduled to start. This option and the preceding option are mutually exclusive, and one is required.
Concurrence Count	For a workflow associated with a calendar schedule, the number of workflow instances expected to be seen during the scheduled time. For a workflow associated with a duration schedule, the number of instances of the workflow that may run at one time.
Correlator Source	The value Control Center obtains and uses at runtime to correlate milestones in the workflow SLC. Click **Insert Var** and then select the event element variable to use as the value required in all events making up the workflow SLC instance to be considered complete. For more information on variables you can use, see *Sterling Control Center Variables* on page 231. You can use a different correlator for an individual milestone to override this general Correlator Source, which is used for the entire SLC. For more information, see *Maintain Milestones* on page 104.
Jeopardy List: Message ID	A list of messages used to indicate that a workflow SLC milestone is in danger of failing to complete normally due to a problem with a previous milestone. When a message in the jeopardy list is generated for any milestone, then a jeopardy event will be generated for all milestones in the same workflow that have yet to start. A jeopardy event is an SLC event containing the jeopardy message ID (CSLC229I) along with the name of the milestone and the reason that the milestone is in jeopardy. See *Maintain Message Lists* on page 102.
Fire-Once List: Message ID	Fire-once messages are generated only once per workflow, no matter how many times the condition that triggers them may occur. See *Maintain Message Lists* on page 102.
Milestones	The milestones that comprise the workflow. For more information, see *Maintain Milestones* on page 104.

Maintain Message Lists

As part of the process of managing workflow SLCs, you can create, modify, duplicate, and delete message lists. Message lists can be used as a source of jeopardy messages or fire-once messages. Jeopardy messages signal that a milestone is in danger of failing to complete as scheduled due to a problem with a previous milestone. Fire-once messages display a maximum of once per workflow no matter how many times the condition that triggers them occurs.

You can select any message list to use as a jeopardy list or fire-once list. In other words, in setting up a message list you do not define it as jeopardy or fire-once.

To create a message list:

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Message Lists**.

   Note: You can also manage message lists as part of creating or modifying a workflow SLC. (See *Create a Workflow SLC Group* on page 100.)

2. Click **+**. The **Create Message List** wizard displays.
3. On the **General** page, provide a name and description for the message list and click **Next** to go to the next page.

   Note: For details on the fields that make up a message list, see *Message List Field Definitions* on page 103.

4. On the **Messages** page, select messages to include in the list by any of the following methods and click **Next** to go to the next page:
   - Individually select messages to include in the list by checking them.
   - To select all messages, right-click the listing and select **Select All**.
   - To deselect all messages, right-click the listing and select **Deselect All**.
   - To get suggestions, right-click in the message listing and select **Suggest Jeopardy List** or **Suggest Fire-Once List**. Messages typical of the kind you asked for are automatically checked. You can modify the list by deselecting suggested ones or selecting ones not suggested.
5. On the **Permissions** page, confine permission to manage the message list to a selected role by selecting the role and clicking **>**. Move a role out of **Selected Roles** by selecting it and clicking **<**.
6. Specify whether the message list will be visible to all users or only to the users in the roles you selected. If you make the message list visible to all users, you cannot restrict visibility to specific roles once it has been referenced. Click **Next**.
7. On the **Confirm Choices** page, review your choices and click **Finish**.
8. On the **Finish** page, click **Close**.

To modify a message list:

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Message Lists**.
2. Double-click an item in the **Message Lists** screen, or select it and click . The **Message List Properties** screen displays.
3. Change any of the information detailed in steps 3 through 7 of the procedure for creating a message list. Click **Update** to finish.

Note: For details on the fields that make up a message list, see *Message List Field Definitions* on page 103.

Message List Field Definitions

The following table defines the fields that make up a message list.

Field	Description
Name	The name of the message list.

Field	Description
Description	Text describing the message list.
Messages	The messages that make up the message list.
All Roles	The roles available to select from.
Selected Roles	The restricted roles that have permission to modify this message list. If none is selected, only unrestricted roles have such permission.
This message list is visible to all users	When selected, this option makes the message list public and available for selection by all users.Once a public message list is referenced by any other object, you cannot make it private by restricting visibility to specific roles/users.
This message list is visible to restricted users in these Selected Restricted Roles	When restricted roles are selected, this option allows only restricted users in the selected roles to view/select/edit the message list.

Maintain Milestones

Milestones are the means by which you specify the processes or process steps to be monitored in a workflow SLC.

To create a milestone:

1. On the **Milestones** page of the **Create Workflow SLC Group Wizard** or **Workflow SLC Group Properties**, click **+**. The **Create Milestone** wizard is displayed.

   Note: For more on creating workflow SLC groups, see *Create a Workflow SLC Group* on page 100.

2. On the **General** page, enter general information on the milestone and click **Next** to go to the next page.

   Note: For descriptions of the fields that make up a milestone, see *Milestone Field Definitions* on page 105.

3. On the **Parameters** page, select one or more **Key**s, select an **Operator**, and enter a **Value**. An entry specifying either Server or Server Group is required. Also, either Process Name or Step Name is required. To see information on additional keys you can specify, see *Keys and Fields* on page 291.

   Optionally, you can also enter a Correlator Source. For more information, see *Sterling Control Center Variables* on page 231.

   Click **Next** to go to the next page.

   Note: Users with a restricted role must always specify a Server Group and may optionally specify a Server as well. By specifying both, the SLC will only apply to activity on the server specified as opposed to all servers in the server group.

4. On the **Schedule** page, define duration or calendar schedule values (or both) and press **Next** to continue. A duration schedule requires **Minimum Duration** and **Maximum Duration** values. For a calendar schedule, enter **Normal Start Range Start (NSRs)** and **Normal Start Range End (NSRe)** or **Normal End Range Start (NERs)** and **Normal End Range End (NERe)** values, or both.
5. Confirm choices by clicking **Finish** on the **Confirm Choices** page, then click **Close** on the **Finish** page.

To modify a milestone:

1. On the **Milestones** page of the **Create Workflow SLC Group** wizard or **Workflow SLC Group Properties**, double-click the milestone or select it and click 📋. The **Milestone Properties** window is displayed.
2. Change any of the information, except for Name, as detailed in steps 2 through 4 of the procedure for creating a milestone. Click **Update** on any page to finish.

Milestone Field Definitions

The following table defines the fields that make up a milestone.

Field	Description
Name	A name for the milestone.
Description	Text describing the milestone.
Key	The selection criteria for this milestone, such as Process Name or Submitter ID. To see information on parameters you can use as keys, see *Keys and Fields* on page 291.
Operator	The operator for the selection criterion. Depending on the value you choose for Key, choose from: ◆ Matches ◆ Wildcard ◆ RegEx
Value	The value of the Key to set as the selection criterion.
Correlator Source	The value Control Center obtains and uses at runtime to correlate this individual milestone to other milestones in the workflow SLC. This will override the Correlator Source value set in the Workflow SLC for this milestone only. Click **Insert Var** and then select the event element variable. For more information on variables you can use, see *Sterling Control Center Variables* on page 231. **Note:** If you use a correlator for an individual milestone, you must either specify a correlator for each milestone or one for the workflow SLC itself to use as a default correlator.

Field	Description
Minimum Duration	The minimum amount of time the milestone item is expected to run, in the format hhh:mm:ss. Hours and minutes are required if you specify a value. Example: Type 1 hour and 15 minutes as 1:15. Type 20 minutes as 0:20. Type 15 seconds as 0:00:15.
Maximum Duration	The maximum amount of time the milestone item is expected to run, in the format hhh:mm:ss. Hours and minutes are required if you specify a value. Example: Type 1 hour and 15 minutes as 1:15. Type 20 minutes as 0:20. Type 15 seconds as 0:00:15.
Normal Start Range: Start	The beginning of a time range within which processing is expected to start for a milestone item. This time range is relative to the actual or scheduled start of the workflow. Expressed in 24-hour format. For example, enter 18 hours as 18:00 or 30 minutes as 0:30.
Normal Start Range: End	The endpoint of a time range within which processing is expected to start for a milestone item. This time range is relative to the actual or scheduled start of the workflow. Expressed in 24-hour format. For example, enter 18 hours as 18:00 or 30 minutes as 0:30. End Time cannot be the same as Start time. If the start time is later than the end time, the NSR spans two days.
Normal End Range: Start	The beginning point of a time range within which processing is expected to end for a milestone item. This time range is relative to the actual or scheduled start of the workflow. Expressed in 24-hour format. For example, enter 18 hours as 18:00 or 30 minutes as 0:30.
Normal End Range: End	The endpoint of a time range within which processing is expected to end for a milestone item. This time range is relative to the actual or scheduled start of the workflow. Expressed in 24-hour format. For example, enter 18 hours as 18:00 or 30 minutes as 0:30. End time cannot be the same as Start time. If the start time is later than the end time, the NER spans two days.

Note: Start range and end range times are relative to the scheduled or actual start of the workflow SLC, depending upon whether Milestone Times Relative to: Actual Start of Workflow SLC or Milestone Times Relative to: Scheduled Start of Workflow SLC is checked.

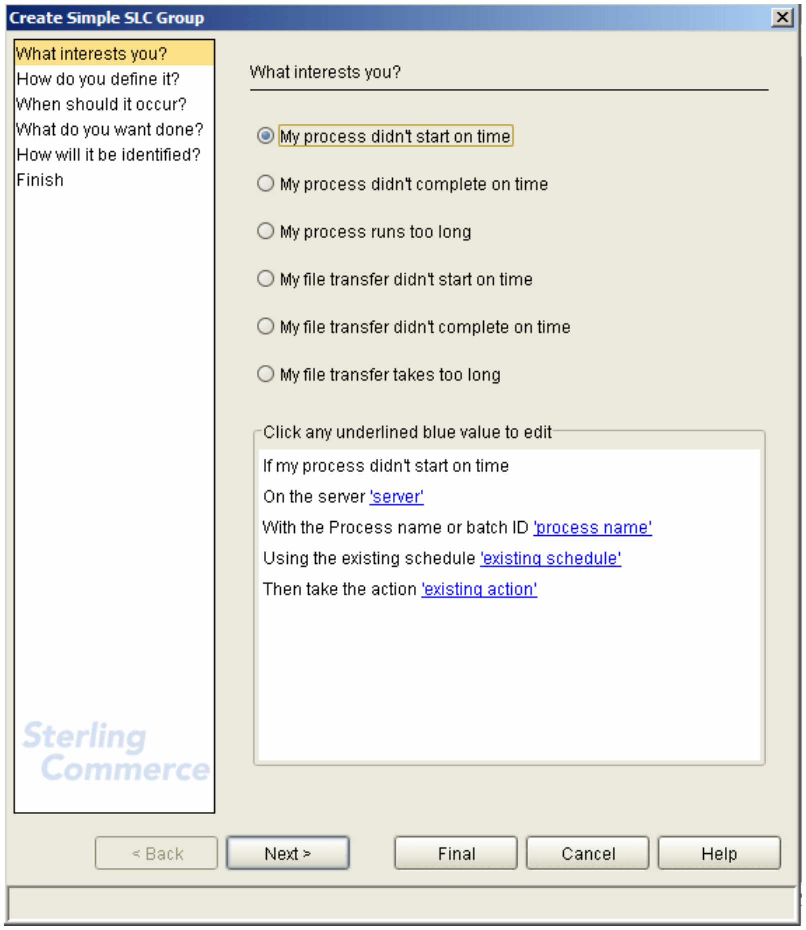
About Simple SLCs

Simple SLCs enable you to create an SLC by answering a few basic questions, specifying values for basic parameters, and giving the SLC a name and description. When you create a simple SLC, all necessary objects to support the SLC, such as rules, actions, and schedules, are also created. The following considerations apply to simple SLCs:

- Although simple SLCs are based on workflow SLCs, simple SLCs support only one milestone.
- After you create them, simple SLC groups are displayed in both the Simple SLC Groups list and in the Workflow SLC Groups list. You can view simple SLC properties from the Workflow SLC Group list, but you cannot edit them from this list. They must be edited from the Simple SLC Groups list.
- Any milestones, calendars, schedules, or actions created for a simple SLC will have the same name as the SLC. Any rules created for a simple SLC will have a rule name of <SLC_Name>_CSLC0XXE or <SLC_Name>_ignored_msgs.
- Any objects created for the SLC are displayed with the listings for those object types, for example, actions. You can view an action created by a simple SLC from the Actions list, but that action can be edited only from the Show Simple SLC Groups.
- When you delete a simple SLC, the objects created for the SLC that have the same name as the simple SLC are also deleted.
- You cannot create a simple SLC that has the same name as an existing calendar, schedule, action, rule or workflow SLC. Conversely, you cannot create a workflow SLC that has the same name as a simple SLC.
- Because the rules generated by simple SLCs are created with specific parameters, they appear at the top of the priority list.
- If your role does not have manage permissions for the objects used to create simple SLCs, such as calendars, schedules, and actions, you will only be able to select existing objects when creating simple SLCs. If your role has view-only permissions, you will not be able to create or update simple SLCs.

Using the Create Simple SLC Group Wizard

The Create Simple SLC Group wizard walks you through the creation of a simple SLC using a question/answer format. Your answer to the first question: “What interests you?”, defines the starting point and structure for building the SLC. When you select an answer, a synopsis of the SLC is displayed in a box at the bottom of the first page. For example, when you select “My process didn’t start on time,” the following is displayed:



What interests you?

● My process didn't start on time

○ My process didn't complete on time

○ My process runs too long

○ My file transfer didn't start on time

○ My file transfer didn't complete on time

○ My file transfer takes too long

Click any underlined blue value to edit

If my process didn't start on time
On the server 'server'
With the Process name or batch ID 'process name'
Using the existing schedule 'existing schedule'
Then take the action 'existing action'

The synopsis of the SLC contains the basic parameters for the scenario you chose. From this first page, you can proceed as follows:

- Click the underlined text to provide values for the basic parameters.

  Note: If you have view-only permissions, you cannot edit the underlined text.

- Click **Next** to cycle through the pages of the wizard to answer the five questions used to define the SLC. As you select answers to the questions, the parameters associated with those answers are displayed in the synopsis. When using this method, you can select additional or different parameters than the basic parameters.
- Click **Final** to move to the last question where you provide a name, description, and data visibility group for the SLC and provide values for the basic parameters required for the SLC.

At anytime before you click **Finish** to complete the SLC, you can click **Back** to return to previous pages to select different answers and to provide values for the parameters associated with those answers.

Create a Simple SLC Group

To create a simple SLC group:

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Simple SLC Groups >Create Simple SLC**. The Simple SLC Group wizard displays.
2. On the **What interests you?** page, select the general scenario that you want to monitor and click **Next**.

> **Note:** As you are answering questions to create a simple SLC, the box at the bottom of the page contains a synopsis of the simple SLC scenario you have chosen. To edit the basic SLC parameters, you can click the underlined text. If you do not want to cycle through the wizard pages, you can click **Final** to go to the Summary page, where you can also edit the basic parameters.

3. On the **How do you define it?** page, select the parameters that specifically define what will be monitored. To specify values for the parameters, click the underlined text. Click **Next** to continue.
4. On the **When should it occur?** page, specify whether the time constraints for the SLC will be based on an existing or a new schedule (with a start/end time range and recurrence), or on a duration of time. To specify values for the time constraints, click the underlined text. Click **Next** to continue.
5. On the **What do you want done?** page, select the action that will be taken when this scenario occurs. To specify values for the action you chose, click the underlined text. Click **Next** to continue.
6. On the **How will it be identified?** page, specify a name and description for the SLC and select a data visibility group.
7. Click **Summary** to review the parameters for the SLC or **Finish** to complete the SLC.
8. Click **Close**.
9. You are notified when the SLC has been created. Click **Close**.

View or Modify Properties of a Simple SLC Group

You can view an existing simple SLC group and change any of its properties except for the name.

To view or change a simple SLC group:

1. Select **Manage** > **Simple SLC Group > Show Simple SLC Groups** from the Control Center window.
2. Double-click a simple SLC to display its properties window, or select the SLC and click 📝. The Create Simple SLC Group wizard displays. To update the simple SLC, either:
   - Click the underlined text to provide values for the basic parameters on the first page.

- Click **Next** to cycle through the pages of the wizard to update the answers to the five questions used to define the SLC. Click the underlined text to edit parameter values in the synopsis.
- Click **Final** to move to the last question where you can edit the description and select a data visibility group for the SLC and provide values for the parameters required for the SLC.

3. When you have completed your updates, click **Finish**.
4. You are notified when the SLC has been updated. Click **Close**.

Enable or Disable a Simple SLC Group

To enable or disable a simple SLC group:

1. Select **Manage** > **Simple SLC Group > Show Simple SLC Groups** from the Control Center window.
2. Double-click a simple SLC group to display its properties window, or select the SLC and click . The Create Simple SLC Group wizard displays.
3. Click **Final** to move to the last question. On this page, select **Enable this SLC** or clear this option to disable the SLC.
4. Click **Finish**.
5. You are notified when the SLC has been updated. Click **Close**.

Chapter 9

Manage Schedules and Calendars

This chapter contains the following sections:

- About Schedules
- Create Schedules
- Maintain Schedules
- About Calendars
- Create a Calendar
- View or Modify a Calendar

About Schedules

Schedules are associated with SLCs and rules.

A schedule associated with an SLC dictates when to monitor.

For a schedule and an event associated with a rule (including a metadata rule), the schedule dictates when events will be matched against the rule's criteria and when they won't be. For example, you may not want a rule to be applied during scheduled downtime. To prevent the rule being applied during that time, you can create two calendar schedules, one that excludes the downtime, and one that includes only the downtime. For the schedule with only downtime, specify an action of No Operation. For the other schedule, specify an action that produces an alert when the rule criteria are met. Then associate the two schedules with the rule.

You must create the schedule first; however, you can now create the schedule as part of the process of creating or editing the rule. (See *Create a Rule* on page 71.)

There are two types of schedule, calendar and duration.

Calendar Schedules

For an SLC calendar schedule, processing must start or end within a specified time range. For example, a Process must start between 19:00 and 19:30 and end between midnight and 00:30.

Calendar schedules are useful for monitoring processing that occurs at fixed times. For a calendar schedule, an event must occur within a defined time range.

An SLC calendar schedule has a normal start range (NSR) and a normal end range (NER). These ranges specify the calendar to use and the time range. For example, you can define a schedule named Wednesday Evening that specifies an NSR of 20:00–21:00 and an NER of 22:00–23:00 every Wednesday.

A calendar schedule requires that you specify one or more calendars. A calendar defines the dates on which processing is scheduled to occur. Calendars specify daily, weekly, monthly, and annual processing dates, and also let you specify exceptions to the normal processing calendar.

Sterling Control Center includes eight predefined calendars (Daily, and Monday through Sunday) for your use.

Note: Calendars are sharable among all schedule types.

Duration Schedules

With a duration schedule, processing can begin at any time but must end within a specified time frame. A duration schedule uses a minimum duration and a maximum duration to define the processing window. It is used to identify the percentage of processing that is complete for an SLC (or a workflow SLC milestone).

Note: A duration schedule can be associated only with an SLC, not with a rule.

For example, a Process may be triggered by the completion of a previous Process. If you cannot predict when the first Process will end, you cannot set a specific expected start time for the second Process. However, you can specify that when the second Process does start, it must finish within 25 to 30 minutes.

Create Schedules

Use the procedures in this section to create new schedules.

Create an SLC Calendar Schedule

To create an SLC calendar schedule:

1. Click **Manage** > **Service Level Criteria (SLCs)** > **SLC Schedules**. The **SLC Schedules** listing displays.
2. Click **+** to display the **Create SLC Schedule** wizard.
3. Select **Calendar Schedule** in the **Schedule Type** field.
4. Type a **Name** and **Description** for the schedule.

5. Select **Enabled** if you want to enable the schedule.
6. Click **Next**.
7. Select an existing **Calendar Name** to use in the schedule.

Note: You can create a new calendar by clicking **+** next to **Calendar Name**. You can duplicate an existing calendar and modify the duplicate by clicking . View a calendar's properties by selecting the calendar name and clicking .

8. Select the **Time Zone** to be used for monitoring.
9. Type the **Normal Start Range (NSR) Start Time** and **End Time**, or the **Normal End Range (NER) End Day**, **Start Time**, and **End Time**—or all of the above—for the schedule.

Note:

1. Enter the times according to the time zone you selected in the previous step.
2. Type the time in 24-hour format. For example, enter 6:00 a.m. as 06:00. Enter 6 p.m. as 18:00. Enter 12:30 a.m. as 00:30.
3. If you specify a time range, supply both the Start Time and End Time.
4. The Start Time and End Time cannot be the same.
5. The maximum difference between the Start Time and End Time, without using End Day, is 23 hours, 59 minutes. Using End Day, you can specify start and end times that are as much as seven days apart.
6. If the Start Time is later than the End Time, the schedule spans two days.

10. Optionally, identify the restricted roles that have permission to modify the schedule. Highlight a restricted role in the **All Roles** window and click **>** to move it to the **Selected Roles** window.

Note: Unrestricted roles already have permission to modify schedules and are not displayed in the list of All Roles.

11. Specify whether the schedule will be visible to all users or only to the users in the roles you selected. If you make the schedule visible to all users, you cannot restrict visibility to specific roles after it has been referenced.
12. Click **Next** and then, on the **Finish** page, click **Finish**.
13. Click **Close** to close the **Create SLC Schedule** window.

Create a Rules Calendar Schedule

To create a rules calendar schedule:

1. Click **Manage** > **Rules and Actions** > **Rule Schedules**. The **Rule/Metadata Schedules** listing displays.
2. Click **+** to display the **Create Rule/Metadata Schedule** wizard.
3. Type a **Name** and **Description** for the schedule.
4. Select **Enabled** if you want to enable the schedule.
5. Click **Next**.

6. Select a **Calendar Name** to use in the schedule.

> **Note:** You can create a new calendar by clicking **+** next to **Calendar Name**. You can duplicate an existing calendar and modify the duplicate by clicking . View a calendar's properties by selecting the calendar name and clicking .

7. Select the **Time Zone** to be used for monitoring.
8. Type the **Start Time**, **End Day**, and **End Time** for the schedule.
9. If you want to check the time that the event occurred to determine if the rule conditions are met, turn on **Check Schedule against when event occurred**.
10. Optionally, identify the restricted roles that have permission to modify the schedule. Highlight a restricted role in the **Restricted Roles** list and click **>** to move it to **Selected Restricted Roles**.

> **Note:** Unrestricted roles already have permission to modify schedules and are not displayed in the list of Restricted Roles.

11. Specify whether the schedule will be visible to all users or only to the users in the roles you selected. If you make the schedule visible to all users, you cannot restrict visibility to specific roles after it has been referenced.
12. Click **Next**, then, on the **Finish** page, click **Finish**.
13. Click **Close** to close the **Rule Schedule** window.

Create a Metadata Calendar Schedule

You can create a calendar schedule to use in defining metadata rules. (For more on metadata rules, see *Manage Metadata Rules* on page 129.)

To create a metadata calendar schedule:

1. Click **Manage** > **Metadata** > **Metadata Schedules**.
2. Follow the procedure *Create a Rules Calendar Schedule* on page 113, beginning with step 2.

Create an SLC Duration Schedule

To create an SLC duration schedule:

1. Click **Manage** > **Service Level Criteria (SLCs)** > **SLC Schedules**. The **SLC Schedules** listing displays.
2. Click **+** to display the **Create SLC Schedule** wizard.
3. Select **Duration Schedule** in the **Schedule Type** field.
4. Type a **Name** and **Description** for the schedule.
5. Select **Enabled** if you want to enable the schedule.
6. Click **Next**.
7. Select a **Calendar** to use in the schedule.

8. Type the **Minimum Duration** in the format hhh:mm:ss. Hours and minutes are required. For example, type 1 hour and 15 minutes as 1:15. Type 20 minutes as 0:20. Type 15 seconds as 0:00:15.
9. Type the **Maximum Duration** in the format hhh:mm[:ss]. Hours and minutes are required. For example, type 1 hour and 15 minutes as 01:15. Type 20 minutes as 00:20. Type 15 seconds as 00:00:15. You must supply both a minimum and a maximum duration. They cannot be the same values. The maximum duration is 167 hours, 59 minutes, and 59 seconds (7 days).
10. Click **Next**.
11. Optionally, identify the restricted roles that have permission to modify the schedule. Highlight a restricted role in **All Roles** and click **>** to move it to **Selected Roles**.

Note: Unrestricted roles already have permission to modify schedules and are not displayed in the list of All Roles.

12. Specify whether the schedule will be visible to all users or only to the users in the roles you selected. If you make the schedule visible to all users, you cannot restrict visibility to specific roles after it is created. Click **Next**.
13. On the Confirm Choices page, click **Finish**.
14. Click **Close** on the Finish page to close the Create SLC Schedule window.

Maintain Schedules

This section describes the following schedule maintenance tasks:

- Display a Schedules Listing
- View or Modify Schedule Properties
- Enable or Disable a Schedule

These procedures can be used for calendar, rules, and duration schedules.

Display a Schedules Listing

To display a schedules listing:

1. From the Control Center window, select one of the following:
   - **Manage > Service Level Criteria (SLCs)** > **SLC Schedules**
   - **Manage > Rules and Actions** > **Rules Schedules**
   - **Manage > Metadata** > **Metadata Schedules**
2. To sort on any column, click on the column heading.

View or Modify Schedule Properties

To view or modify the properties of a schedule:

1. Select one of the following:
   - **Manage** > **Service Level Criteria (SLCs)** > **SLC Schedules**
   - **Manage** > **Rules and Actions** > **Rules Schedules**
   - **Manage** > **Metadata** > **Metadata Schedules**
2. Double-click a schedule in the listing to display the Rule/Metadata Schedule or SLC Schedule Properties window.
3. Click in a field to view field-level help.
4. Modify the fields you want to change. See *Schedule Field Descriptions* on page 116 for descriptions of the fields.

   Note: To make changes, you must have permission to edit the schedule. Edit permission is denoted by the ✎ icon.

5. Click **Update** when finished. Click **Cancel** to exit without saving your changes.

Schedule Field Descriptions

The following table describes the fields that comprise a schedule.

Field	Description
General	
Schedule Type	Type of Schedule. For a rule schedule, the type is always Calendar. An SLC schedule can be a Calendar or Duration schedule.
Name	A name for the schedule.
Description	Text describing the schedule.
Enabled	Select to enable the schedule.
Parameters	
Calendar Name	A calendar for defining when to run the schedule. Control Center ships with a number of calendars from which to choose; or you can add your own.
Time Zone	The time zone to use for the SLC, rule, or schedule. Select a time zone from the pull-down menu. This field also shows the difference between the time zone and Coordinated Universal Time (UTC, also known as Greenwich Mean Time). Arizona has its own time zone, because Arizona does not recognize Daylight Saving Time.
Start Time	(Rules Schedule) The time to begin the schedule. Enter the time according to the time zone you selected and in 24-hour format. If you specify a start time you must also supply an end time. The start time and end time cannot be the same. If the start time is later than the end time, the schedule spans two days.

Field	Description
End Day	(Rules Schedule) The day on which the schedule ends. Select from the following options: Calendar Start Day or Start Day + 1-6 days.
End Time	(Rules Schedule) The time to end the schedule. Enter the time in 24-hour format. If you specify a start time, you must also supply an end time. The start time and end time cannot be the same time. If start time is later than end time, the schedule spans two days.
Check Schedule Against When Event Occurred	(Rules Schedule) Check this option to use the time that the event occurs to determine whether rule conditions are met. This option is automatically checked when you create a new rule. Uncheck to use engine time to determine whether rule conditions are met.
Minimum Duration	(SLC Duration Schedule) The minimum duration processing normally takes.
Maximum Duration	(SLC Duration Schedule) The maximum duration processing normally takes.
Normal Start Range Start Time (NSRs)	(SLC Calendar Schedule) The beginning of a time range when processing normally starts for a monitored item, in 24-hour format.
Normal Start Range End Time (NSRe)	(SLC Calendar Schedule) The end of a time range when processing normally starts for a monitored item, expressed in 24-hour format. NSR end time cannot be the same time as start time. If the start time is later than the end time, NSR spans two days.
Normal End Range End Day	(SLC Calendar Schedule) The day on which the schedule ends. Ranges from calendar start day to calendar start day plus six days.
Normal End Range Start Time (NERs)	(SLC Calendar Schedule) The start of a time range that defines when processing normally ends for a monitored item, in 24-hour format. NER end time cannot be the same time as start time. If the start time is later than the end time, NER spans two days.
Normal End Range End Time (NERe)	(SLC Calendar Schedule) The end of a time range that defines when processing normally ends for a monitored item, in 24-hour format. NER end time cannot be the same time as start time. If the start time is later than the end time, NER spans two days.
Permissions	
All Roles	A list of all restricted roles not yet permitted to modify the schedule.
Selected Roles	The restricted roles permitted to modify the schedule. Unrestricted roles already have permission to modify schedules.
This schedule is visible to all users	When selected, this option makes the schedule public and available for selection by all users. Once a public schedule is referenced by any other object, you cannot make it private by restricting visibility to specific roles/users.
This schedule is visible to restricted users in these Selected Restricted Roles	When restricted roles are selected, this option allows only restricted users in the selected roles to view/select /edit the schedule.

Enable or Disable a Schedule

To enable or disable a schedule:

1. From the **Rule/Metadata Schedules** or the **SLC Schedules** listing, double-click the schedule that you want to enable or disable. The Rule/Metadata Schedule or SLC Schedule Properties window is displayed.
2. Select **Enabled** to add or remove the check mark and click **Update**.

About Calendars

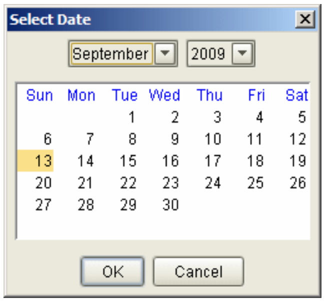
A calendar specifies the dates used in a calendar schedule. This includes how long the calendar remains in effect, and how often processing is repeated (recurrence).

Sterling Control Center comes with predefined calendars for each weekday as well as a daily schedule. You can use these calendars for both rule schedules and SLC schedules, and you can create additional calendars to meet your processing needs.

Create a Calendar

To create a calendar:

1. Select **Manage** > **Calendars**.
2. Click **+** to display the **Create Calendar** wizard.
3. Type a unique meaningful **Name** for the calendar, for example, Month End. The name can be up to 25 characters.
4. Type a **Description** for the calendar.
5. Click **Next** to display the **Recurrence** panel. The **Recurrence** panel specifies how often processing occurs and how long the calendar remains in effect.
6. To select the starting date for the calendar:
    a. Click the **Recurrence Range Start** field to display the calendar, as shown below.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

    b. Select the month, year, and date that you want the calendar to take effect.
    c. Click **OK**.
7. Select **No end date** to leave the calendar permanently in effect, or select an end date for the calendar by doing the following:
    a. Select **Recurrence Range End by**.
    b. Click the date button to display the calendar.
    c. Select the month, year, and date that you want the calendar to end.
    d. Click **OK**.

8. Select a **Recurrence Pattern** (Daily, Weekly, Monthly, or Yearly). The display changes according to the pattern you selected.
9. Select details for the recurrence pattern you selected. See *Recurrence Patterns* on page 120 for more information.
10. Click **Next** to display the **Modifications** panel. The processing dates are highlighted on the calendars based on the recurrence pattern.
11. Click on individual dates to remove them from the recurrence pattern. Click > or < to move forward or backward through the calendar. Click **Reset** to remove all modifications to the calendar. Click **Next** to continue.

Note: Modifications to a recurrence pattern remain in effect until December 31 of the following year, regardless of the recurrence end date. After December 31 of the following year, you must make the modifications again.

12. Optionally, identify the restricted roles that have permission to modify the calendar. Select a role in **Restricted Roles** and click > to move it to **Selected Restricted Roles**.

Note: Unrestricted roles already have permission to modify calendars and are not displayed.

13. Specify whether the calendar will be visible to all users or only to the users in the roles you selected. If you make the calendar visible to all users, you cannot restrict visibility to specific roles after it has been referenced. Click **Next**.
14. Click **Next** to continue.
15. On the Confirm Choices page, click **Finish**.
16. Click **Close** on the Finish page.

Recurrence Patterns

Each recurrence pattern has its own set of parameters. You use these parameters to create calendars to match your processing dates.

The following table lists the four types of recurrence patterns:

Pattern	Description
Daily	Processing occurs every 1–7 days (Monday through Sunday) or every 1–5 weekdays (Monday through Friday). An example is processing that occurs every weeknight.
Weekly	Processing occurs at a specified weekly interval on specified days. An example is payroll processing that occurs every Friday.
Monthly	Processing occurs at a specified monthly interval on a specified day, such as the 7th of each month, or the third Monday of each month. An example is accounts receivable processing that occurs on the last day of each month. If you select the 31st as the date, Sterling Control Center sets the date to the last day of the month.

Pattern	Description
Yearly	Processing occurs once a year on a specified day or date. An example is year-end processing that occurs on January 15.

Display the Calendars Listing

To display the **Calendars** listing:

1. Select **Manage** > **Calendars**.
2. To sort on a column, click the column heading.

View or Modify a Calendar

To view or modify a calendar:

1. Select **Manage** > **Calendars**.
2. Select a calendar name and click or double-click a calendar name to display the **Calendar Properties** window.
3. Click a tab to view its information, or click the **Summary** tab to view an overview of the calendar’s definition.
4. Type in the fields you want to change. See *Calendar Field Descriptions* on page 121 for descriptions of the fields.

Note: To make changes, you must have permission to edit the calendar. Edit permission is denoted by the ✎ icon.

5. Click **Update** when finished.

Calendar Field Descriptions

The following table describes the fields that comprise a calendar.

Field	Description
Name	A name for the calendar.
Description	Text that describes the calendar.

Field	Description
Recurrence Range: Start	Date when the calendar is to start (defaults to creation date).
Recurrence Range: End: No End Date	No end date is set for this calendar.
Recurrence Range: End: End By	The date on which this calendar ends. Defaults to the last day of the year after the creation date. You cannot set it beyond that date.
Recurrence Pattern	The frequency of occurrence (daily, weekly, monthly, or yearly). Select an end time for the recurrence range by clicking the calendar and selecting a date or select No end date to create a nonending recurrence range. Select Daily, Weekly, Monthly, or Yearly to identify how often to run the schedule. For each option, select the recurrence pattern to use. See *Recurrence Patterns* on page 120.
Permissions: Restricted Roles	Restricted roles to select from. Select a role and move to Selected Restricted Roles by clicking >.
Permissions: Selected Restricted Roles	Restricted roles that have permission to modify this calendar.
Permissions: This calendar is visible to all users	When selected, this option makes the calendar public and available for selection by all users. Once a public calendar is referenced by any other object, you cannot make it private by restricting visibility to specific roles/users.
Permissions: This calendar is visible to restricted users in these Selected Restricted Roles	When restricted roles are selected, this option allows only restricted users in the selected roles to view/select/edit the calendar.
Modifications	Shows active and inactive dates for the selected calendar. Active dates are shaded yellow. Click a date to activate or deactivate. Click Reset to reset the calendar to the dates originally set by choosing the Recurrence Pattern on the previous page. Click < to move to a prior month. Click > to move forward to the next month.

Calendar Example

To create a calendar for Monday through Friday processing:

1. Create a calendar with the following values (see *Create a Calendar* on page 119):

Panel	Field	Value
General	Name	Monday-Friday
	Description	Monday through Friday
Recurrence	Start	Today’s date

Panel	Field	Value
	End	No end date
	Recurrence Pattern	Every 1 weekday(s)
Modification	Modifications	Remove holidays per your company schedule

2. Leave all other fields blank or at their default values.

Chapter 10

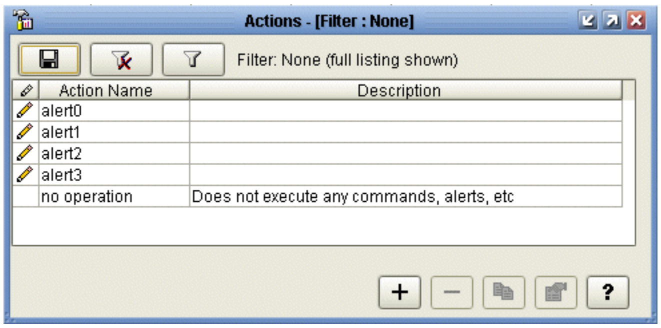
Manage Email Lists

You can create lists of email addresses for groups of users who need to be contacted when an event occurs. These lists can be selected when you create actions.

Create an Email List

To create an email list:

1. Select **Manage** > **Email Lists** to display the **Email List** listing.



Actions - [Filter : None]

Filter: None (full listing shown)

	Action Name	Description
✎	alert0	
✎	alert1	
✎	alert2	
✎	alert3	
	no operation	Does not execute any commands, alerts, etc

2. Click **+** to display the **Add Email List** wizard.
3. Type a name and description for the email list and click **Next**.
4. To add email addresses to the list, click the **To**: field and type the addresses. To import email addresses from a text file, locate the file and click **Import**. To sort the addresses in ascending or descending order, click **Sort**.
5. Click **Next** to continue.
6. Identify the restricted roles that have permission to modify the email list.

Note: Unrestricted roles automatically have permission to modify an action.

7. Specify whether the email list will be visible to all users or only to the users in the roles you selected. If you make the calendar visible to all users, you cannot restrict visibility to specific roles after it is created. Click **Next**.
8. Click **Finish** to add the email list to the **Email List** listing.
9. Click **Close** to close the **Add Email List** wizard.

Note: For more on specifying the above options, see *Email List Field Descriptions* on page 127.

Export Email Information from an Email List

You can export to a text file a list of addresses that have been entered into an email list’s To: field.

To export a list of email addresses:

1. Select **Manage > Email Lists** from the Control Center window to display the **Email List** listing. Double-click an email list to display its properties.
2. From the **E-mail** tab, click **Export**. A file selection window is displayed.
3. Select a location for the text file.
4. Type a name for the text file and click **Export**. The information is exported to a text file.

Display the Email List Listing

To display the **Email List** listing:

1. From the Control Center window, select **Manage > Email Lists**.
2. To sort on any column, click the column heading.

View or Modify Email Lists

To view or modify an email list:

1. Select **Manage > Email Lists** from the Control Center window to display the **Email List** listing.
2. Do one of the following:
   - Select an email list and click
   - Double-click the email list.
3. Click in a field to view field-level help. Field-level help is displayed in the status bar.

4. Modify the email list information as necessary. See *Email List Field Descriptions* on page 127 for definitions of email list fields.

> **Note:** To make changes, you must have permission to edit the email list. Edit permission is denoted by the ✏ icon.

5. Click **OK** when finished.

Email List Field Descriptions

The following table describes the fields that define an action.

General	
Field Name	**Description**
Name	The name of the email list.
Description	Text describing the action. Optional.
E-mail	
Field Name	**Description**
To	The list of e-mail addresses. E-mail lists can be used to notify addressees when an action is triggered.
Permissions	
Field Name	**Description**
Restricted Roles	List of restricted roles defined in Sterling Control Center. Select a role and click < or > to move the role between this field and Selected Restricted Roles.
Selected Restricted Roles	Restricted roles with rights to modify this email list. If no roles are selected, only an unrestricted user (admin) can modify this email list.
This email list is visible to all users	When selected, this option makes the email list public and available for selection by all users. Once a public email list is referenced by any other object, you cannot make it private by restricting visibility to specific roles/users.
This email list is visible to restricted users in these Selected Restricted Roles	When restricted roles are selected, this option allows only restricted users in the selected roles to view/select/edit the email list.

Chapter 11

Manage Metadata

Metadata is data about data. Metadata rules allow you to append additional elements and values to Sterling Control Center events before they are processed by the SLC service or normal rule processing. Metadata rules are applied to all Control Center events, unless you explicitly set them not to be, for statistics collected from specific managed servers. The additional metadata type elements and values are logged in the Control Center Events database.

When a metadata rule matches an event, Control Center appends metadata to the event as lists of key value pairs. You can use these metadata fields as matching criteria when defining conventional rules. Metadata can also be used as filter criteria for reports and alert monitor or activity monitor data.

So not only can metadata rules be used to simplify the specification of your rule and SLC criteria, they can also be used to simplify specification of your report criteria.

Metadata can be used to analyze only new activity going forward. You cannot do retroactive analysis of existing data to which metadata tags have not already been applied.

This chapter addresses the following subjects:

- Manage Metadata Rules
- Manage Metadata Type Mapping
- Manage Metadata Actions

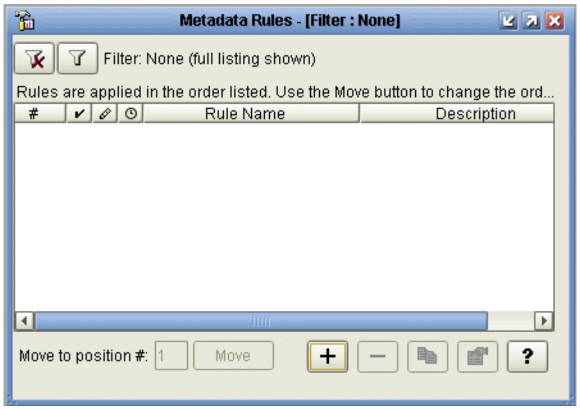
Manage Metadata Rules

You can create new metadata rules, display them, make changes to them, duplicate, reorder, enable, or remove them.

Displaying the Metadata Rules Listing

To display the Metadata Rules listing:

From the Control Center window, select **Manage** > **Metadata** > **Metadata Rules**. The **Metadata Rules** listing is displayed.



Filter: None (full listing shown)

Rules are applied in the order listed. Use the Move button to change the ord...

Creating a Metadata Rule

To create a metadata rule:

1. Select **Manage** > **Metadata** > **Metadata Rules** to display the **Metadata Rules** listing.
2. Click **+** to display the **Create Metadata Rule** wizard.
3. Type a **Name** and **Description** for the metadata rule and click **Next**.

> **Note:** For detailed definitions of metadata rules fields, see *Metadata Rules Field Definitions* on page 132.

4. Select a server group or groups on which to apply the metadata rule by moving the group (using >) from **Groups** to **Selected Groups**. Click **Next**.
5. Select individual servers on which to apply the metadata rule by moving the server (using >) from **Servers** to **Selected Servers**. Click **Next**.

> **Note:** At least one server or server group is required for a restricted role.

6. Optionally, select one or more **Schedules** to associate with the metadata rule by moving the schedule (using < and >) from **Rule/Metadata Schedules** to **Selected Schedules**.

> **Note:** Create a new schedule by clicking **+** below **Rule/Metadata Schedules**. You can duplicate an existing schedule and modify the duplicate by clicking . View the properties of a schedule in either **Rule/Metadata Schedules** or **Selected Schedules** by selecting the schedule and clicking .

7. Click **Next**.

8. Specify one or more selection criteria to further define the metadata rule by choosing a **Key**, an **Operator,** and a **Value** for each parameter. The list of operators depends on whether the key is numeric (for example, Return Code and File Size) or alphanumeric. For more information on keys you can use as rule criteria, see *Keys and Fields* on page 291. Click **Next**.
9. Select a **Metadata Action** to perform when the parameters and schedules are met.

Note: Create a new metadata action by clicking **+** next to **Action**. Duplicate an existing metadata action and modify the duplicate by clicking . View a metadata action's properties by selecting it and clicking . For more on metadata action properties, see *Create Metadata Actions* on page 134.

10. Click **Next** and then **Finish** to add the metadata rule to the **Metadata Rules** listing.
11. Click **Close** to close the **Create Metadata Rule** wizard.

Viewing or Modifying a Metadata Rule

To view or modify a metadata rule:

1. Select **Manage** > **Metadata** > **Metadata Rules** to display the **Metadata Rules** listing.
2. Do one of the following to display the **Metadata Rule Properties** window for a rule:
   - Double-click the metadata rule
   - Select the metadata rule and click
3. Select from among the tabs to display property subgroups and modify properties as needed. See *Metadata Rules Field Definitions* on page 132 for descriptions of metadata rule fields.

Note: To make changes, you must have permission to edit the metadata rule. Edit permission is denoted by the icon.

4. Click **Update**.

Reordering Metadata Rules

As with standard rules processing, an event can match at most one metadata rule. When it matches a metadata rule, all metadata rules lower in the hierarchy are ignored and thus not matched on for that event. You can change the hierarchical order of metadata rules to change which will be matched upon first.

To change the order of metadata rules:

1. In the **Metadata Rules** listing, select the metadata rule to reorder.
2. In the **Move selected to position #** field, type the position in which to place the metadata rule.
3. Click **Move**.

Note: You must sort metadata rules in Priority ascending order before you can change their position in the listing.

Enabling Metadata Rules

To enable or disable a metadata rule:

1. In the **Metadata Rules** listing, do one of the following:
   - Select the metadata rule and click .
   - Double-click the metadata rule.
2. In the **Metadata Rule Properties** window, click **Enabled** to place or remove the check mark.
3. Click **Update**.

Note: When you remove the only server or server group used by a metadata rule, the metadata rule is automatically disabled.

Customizing the Metadata Rules View

To customize the **Metadata Rules** view:

Refer to Customizing Layout Views in *Sterling Control Center User Guide*.

Metadata Rules Field Definitions

Following are definitions for the fields that make up a metadata rule.

Field	Description
Name	The name of the metadata rule.
Description	Text describing the metadata rule.
Groups	Server groups to choose from.
Selected Groups	The server group the metadata rule applies to.
Servers	The list of servers to choose from.
Selected Servers	Servers to which you want the metadata rule to apply.
Rule Schedules	The list of schedules to choose from.
Selected Schedules	The schedules you want associated with the metadata rule.
Parameters	Selection criteria for further defining the rule. Choose a Key and Operator and enter the Value you want to monitor. For more information on parameters, see *Keys and Fields* on page 291.

Field	Description
Parameters: Operator	Operator for defining the metadata rule’s match criteria.
Parameters: Value	A value for further defining the metadata rule’s match criteria.
Actions	The actions to perform when the metadata rule criteria are met.

Manage Metadata Type Mapping

You can append as many as four metadata elements, and values, per Control Center event using metadata actions. The element names are called metadata types. Changing the way metadata elements are labeled is called mapping metadata types.

Caution: Unlike other configuration data, the Metadata Type Mapping for User Data and Server Data is stored in the database, rather than in the local Control Center configuration. If you switch to a new database or reinitialize the existing database during upgrading or for any other reason, the Metadata Type Mapping data will be lost. Make note of these values before switching or initializing the database and reconfigure them afterwards.

To map metadata types:

1. Select **Manage** > **Metadata** > **Metadata Type Mapping**.
2. On the Rules/Actions tab, for each metadata type you wish to map, enter a name that describes the metadata.
3. On the Server Metadata Titles tab, for each server metadata type you wish to map, enter a name that describes the metadata.
4. When finished, click **OK**.

Note: Once you map a metadata type to a new value, that value appears in place of the default in lists of Key selections when you create rules or set filters for metadata actions (for Rules/Actions metadata fields), or when you specify server metadata (for Server Metadata Titles) or for both when you generate reports containing metadata.

Manage Metadata Actions

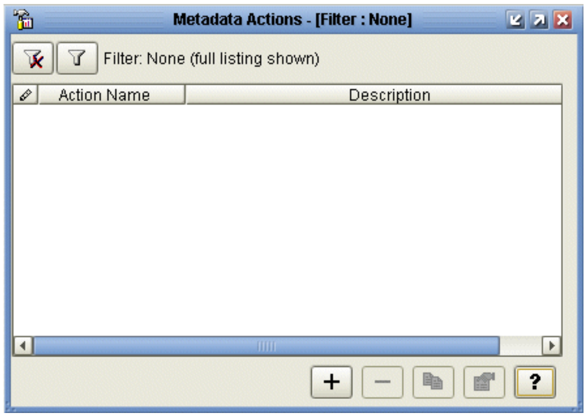
In Sterling Control Center, metadata actions act similarly to conventional ones, but they are used only by metadata rules (and metadata rules can only refer to metadata actions). You manage metadata actions in much the same way as conventional ones. The values in a metadata action are added to events when the metadata rules they are part of match the events.

Display Metadata Actions

To display the Metadata Actions listing:

Select **Manage** > **Metadata** > **Metadata Actions**.

The Metadata Actions listing displays.


Metadata Actions - [Filter : None]
Filter: None (full listing shown)
Action Name
Description
+
−
?

Create Metadata Actions

To create a metadata action:

1. Select **Manage** > **Metadata** > **Metadata Actions** to display the **Metadata Actions** listing.
2. Click **+**. The **Create Metadata Action** wizard displays.
3. Type a **Name** and **Description** for the new metadata action and click **Next** to continue.
4. Enter a metadata value for any field you want to have set when the metadata action is performed.

   Note: To change the label of a metadata field, see *Manage Metadata Type Mapping* on page 133.

5. To include a variable as part of the metadata value for a field, click **Insert Var** to the right of the field. Select a variable from the **Variable** listing. Click **OK** to insert a variable and return to the **Create Metadata Action** wizard.

   Note: For a description of variables, see *Sterling Control Center Variables* on page 231.

6. Click **Next**.
7. If you want to restrict use of this metadata action to certain roles, highlighting the roles in All Roles and click > to move them to Selected Roles. You can also add, duplicate, or check the properties of roles using the buttons located below All Roles.
8. Click **Next**.
9. Click **Finish** and then **Close** to add the action to the **Metadata Actions** listing.

View and Edit Metadata Actions

To view or modify a metadata action:

1. From the **Metadata Actions** listing, do one of the following:
   - Select an action and click
   - Double-click an action
2. Modify the metadata action information as necessary.

Note: To make changes, you must have permission to edit the metadata action. Edit permission is denoted by the ✎ icon.

3. Click **Update** when finished.

Chapter 12

Perform Guided Node Discovery

This chapter consists of the following sections:

- About Guided Node Discovery
- Identify Servers for Node Discovery
- Manage the Explorer List
- Run Node Discovery
- Identify the Status of Servers in the Node Discovery List
- Manage the Discovery List and My List
- Create a Custom View

About Guided Node Discovery

Guided Node Discovery (Node Discovery) allows you to find Connect:Direct servers deployed *in your Enterprise Network*. Node Discovery can be performed on servers managed by Sterling Control Center and ones not managed by Sterling Control Center.

Note: Connect:Enterprise, Connect:Direct Select, FTP, and Sterling Integrator servers do not support Node Discovery.

Summary of Node Discovery Process

The first step in Node Discovery is to specify the time frame and the servers on which to perform it. Then, after you start Node Discovery, the following occurs:

- Sterling Control Center tries to contact each enabled Explorer server.
- After a server is contacted, Control Center obtains the data transmission facility (DTF) address, DTF port, license, and node name and populates the Explorer List with this information. It updates the Last Discovery Date/Time in the Explorer List. Then information from the server’s network map and statistics records (for the time specified) is scanned for other servers with whom the server communicates.

- If a server cannot be contacted, the MsgID and Return Code fields in the Explorer List are updated with information concerning the errors that prevented the connection.
- For each unique trading partner identified in the server's network map or statistics record, a server entry is added to the Discovery List.
- When Node Discovery is complete, other fields in the Explorer List are populated, including return code, last explore range, and last successful Discovery.

Summary of Node Discovery Procedures

To use Node Discovery, you do the following tasks:

Task	Procedure
Identify the servers on which Node Discovery can be performed by adding them to the Explorer List.	*Add a Managed Server to the Explorer List* on page 139
You can add managed servers that are already recognized by Sterling Control Center, or unmanaged servers not defined in Control Center.	*Add an Unmanaged Server to the Explorer List* on page 139
Enable servers for Node Discovery.	*Enable a Server for Discovery* on page 141
Run Node Discovery to identify Connect:Direct nodes with which enabled servers communicate, based on network map entries and statistics records.	*Run Node Discovery* on page 141
Manage nodes for additional Node Discovery as needed.	
◆ Add, edit, or remove servers from the Explorer List.	*Manage the Explorer List* on page 140
◆ Move servers from the Discovery List to Explorer List for Node Discovery or to My List to keep the Discovery list uncluttered.	*Manage the Discovery List and My List* on page 143
◆ Move servers from My List to the Explorer List for Node Discovery.	*Manage the Discovery List and My List* on page 143
◆ Customize any of the Node Discovery views.	*Customizing Layout Views* in the *Sterling Control Center User Guide*

Identify Servers for Node Discovery

Before doing Node Discovery, you add Connect:Direct servers to the Explorer List. You can add servers already managed by Sterling Control Center and unmanaged servers not defined in Control Center.

In order to perform Node Discovery on a server, the credentials specified must be authorized to access a server’s network map information.

After you add a node to the Explorer List, it is displayed with , indicating that the node has not been contacted. To determine whether it can be contacted, enable the node for Node Discovery.

> **Note:** If a server is located during Node Discovery and it is already defined in the Discovery List, Explorer List, or My List, the server is ignored. Servers with identical DTF address and DTF port values are considered duplicates.

Add a Managed Server to the Explorer List

To add a managed server to the Explorer List:

1. Select **Tools** > **Node Discovery**.
2. From the **Explorer List** tab, click **+**. The **Add Server to Explorer List** wizard is displayed.
3. Select **Control Center-Managed Server** and click **Next**.
4. In the **All Managed Servers** box, highlight one or more managed servers to add to the list and click **>** to add them to the Explorer List.
5. Click **Next**.
6. Review the selected servers. If the list is correct, click **Finish** to add the servers. If the list is not correct, click **Back** to make any changes and repeat this procedure.
7. To add more servers, click **Add Another Server** and repeat steps 3–6.
8. Click **Close** to close the wizard.

Add an Unmanaged Server to the Explorer List

To add an unmanaged server to the Explorer List:

1. Select **Tools** > **Node Discovery**.
2. From the **Explorer List** tab, click **+**. The **Add Server to Explorer List** wizard is displayed.
3. Select **Unmanaged Server** and click **Next**.
4. Select the type of server and click **Next**: Connect:Direct with TCP/IP API or Connect:Direct OS/400. Connect:Direct server platforms that operate under TCP/IP API include:
   - Connect:Direct HP NonStop
   - Connect:Direct z/OS or OS/390
   - Connect:Direct UNIX
   - Connect:Direct Windows
5. Do one of the following:
   - If you chose Connect:Direct platforms with TCP/IP API, provide the following required information about the server:
     - API Address

    - API Port
    - User ID
    - Password
  - If you chose Connect:Direct OS/400, provide the following information:
    - Host Name
    - Library Name
    - User ID
    - Password

6. Fill in optional fields with any available information. Refer to the context-sensitive Help for each field for more information.
7. Click **Test Connection** to validate the login information provided.
8. Click **Next**.
9. Review the information about the server. If the information is correct, click **Finish** to add the server.
10. To add another server, click **Add Another Server** and repeat steps 3–9.
11. Click **Close**.

Manage the Explorer List

Use the following procedures to manage the Explorer List.

- View or Modify a Server Definition
- Enable a Server for Discovery
- Disable a Server for Discovery
- Add a Managed Server
- Remove a Server

View or Modify a Server Definition

To modify a server defined in the Explorer List:

1. From the **Node Discovery** window, highlight the server.
2. Click **Properties**.
3. Modify property fields as desired and click **OK**.

Enable a Server for Discovery

To enable a server for Node Discovery:

1. From the **Node Discovery** window, highlight the server to enable and click **Enable for Discovery**.
2. You are informed if a selected server cannot be enabled. Do the following to enable the node for Node Discovery:
   a. Click **Yes** to configure the node.
   b. Type the correct information about the server.
   c. Click **OK**.

Disable a Server for Discovery

To disable a server for Node Discovery:

From the **Node Discovery** window, highlight the server and click **Disable for Discovery**.

Add a Managed Server

See *Add a Managed Server to the Explorer List* on page 139 for instructions on adding managed servers to the list.

Remove a Server

To remove a server from the Explorer list, highlight the server to remove from the **Node Discovery** window and click **-**.

Note: When you remove a server, all discovered nodes associated with this node in either the Discovery List or My List are removed. However, if a node in the Discovery List or My List is associated with the deleted node and another Explorer node, it is not removed.

Run Node Discovery

After you add servers to the Explorer List and enable them for Node Discovery, you are ready to run Node Discovery. Node Discovery searches the statistics records and network map of the servers to identify other servers with which they have communicated.

To run Node Discovery:

1. If necessary, select **Tools > Node Discovery** to open the **Node Discovery** window.
2. From the **Explorer List** tab, click **Run Discovery**. The **Discovery Date Range** dialog is displayed.

3. To identify the date range of statistics records searched:
   a. Click **Start Date**.
   b. Select a date on which to begin searching statistics records.
   c. Click **OK**.
   d. Click **End Date**.
   e. Select an end date for the statistics record search.
   f. Click **OK**.
4. Click **OK**.

After you start Node Discovery, you can close the **Node Discovery** window. Node Discovery continues to search statistics records and network maps of the enabled nodes. A progress bar displays the status of the Node Discovery activity when you reopen the Node Discovery window.

After Node Discovery is complete, Control Center updates the Last Discovery and Last Successful Discovery Date/Time (when applicable) for each enabled Explorer node.

If Control Center cannot contact an enabled Explorer server for Node Discovery, the Return Code, Msg ID, and Message Text fields are updated with information about why the connection failed.

Identify the Status of Servers in the Node Discovery List

The **Node Discovery** window displays the servers that you added to the Explorer List with information about each server. The following icons are displayed with a server to indicate its status:

Icon	Description
🖥	The server is connected and available for Node Discovery.
🖥?	The node either has not been enabled for Node Discovery or cannot be contacted.
✓	The server is enabled for Node Discovery.
📡	The server is managed by Sterling Control Center.

Manage the Discovery List and My List

After Node Discovery has been performed, the **Discovery List** window displays information about servers found during Node Discovery. After Node Discovery has identified a server, the server can be moved to the Explorer List and used to discover additional servers, or it can be moved to My List. My List provides a work area and a place to move discovered nodes to prevent the Discovery List from getting cluttered. The server can also be added to the list of managed servers.

Move a Server to My List

To move a server to My List:

From the **Discovery List** tab, do one of the following:

- Highlight the server to move and click **Move to My List**.
- Right-click the server and select **Move to My List** from the contextual menu.

Move a Server to the Discovery List

To move a server to the Discovery List:

1. From the **My List** tab, do one of the following:
   - Highlight the server to move and click **Move to Discovered List**.
   - Right-click the server and select **Move to Discovered List** from the contextual menu.
2. Completed the required server and license information (at minimum).
3. Click Test Connection to test the connection to this server.
4. Click **OK** to move the server.

Move a Server to the Explorer List

To move a server to the Explorer List:

1. From the **Discovery List** tab or **My List** tab, do one of the following:
   - Highlight the server to move and click **Move to Explorer List**.
   - Right-click the server and select **Move to Explorer List**.
2. Select the type of server: Connect:Direct with TCP/IP API or Connect:Direct OS/400. Connect:Direct server platforms that operate under the TCP/IP API include:
   - Connect:Direct HP NonStop
   - Connect:Direct z/OS or OS/390
   - Connect:Direct UNIX
   - Connect:Direct Windows

3. Do one of the following:
    a. If you chose Connect:Direct with TCP/IP API, provide the following required information about the server:
        - API Address
        - API Port
        - User ID
        - Password
    b. If you chose Connect:Direct OS/400, provide the following information:
        - Host Name
        - Library Name
        - User ID
        - Password
4. Fill in optional fields with any available information. Refer to the Help displayed for each field for more information.
5. Click **Test Connection** to validate the connection to the server.
6. Click **OK** to move the server.

Note: To add a server in the Explorer List to the list of managed servers, see *Add a Server* on page 47.

Show Partners

The Partners Table lists all nodes that have communicated with the selected explorer or discovered node. A node contained in the explorer node's netmap or that shows up in node statistics may also be listed in this table, even if the node in question has never communicated with the selected node. This status is indicated by the check mark in the netmap or statistics column.

To view the partners of an explorer node:

1. In the Node Discovery Explorer List or Discovery List, right-click a server.
2. Select **Show Partners**.

    The Partners Table displays a listing of partner nodes. The columns that comprise the listing are defined in the following table:

Column	Description
#	Row number.
Name or Alias	The server ID.
Node Name	The Connect:Direct node name.
Node Type	Type of Connect:Direct node (D = Discovered, E=Explorer).

Column	Description
From Netmap	A check mark indicates that this node was identified as a partner by virtue of being in the selected node's netmap.
From Stats	A check mark indicates that this node was identified as a partner by virtue of being included in node statistics.
Discovered Time	Time the node was found during Node Discovery.
Comments	User-entered comments.

Add Discovered Node Comments

You can add comments about servers in the Discovery List. Examples of useful comments might include a note to the effect that a server is no longer in use and needs to be removed from the network, or that a server's license needs updating.

To add comments:

1. In the Discovery List, do one of the following:
    - Right-click a server and select **Comments**.
    - Double-click the server.
2. Type comments in the **Discovered Node Comments** window's text box. The maximum number of characters is 2048.
3. Click **OK**.

Remove a Server

To remove a server from the Discovery List or My List:

1. Click the **Discovery List** tab or **My List** tab.
2. Highlight the server or servers to remove from the **Node Discovery** window and click **-**.

Note: When you remove a server from the Explorer List, all discovered nodes associated with that server in either the Discovery List or My List are removed—unless they are associated with another Explorer node.

Create a Custom View

You can rearrange the columns in the **Node Discovery** window to view the information that is important to you. You can create a custom view, hide a column, rearrange columns, save a view, or rename a view you saved on the Explorer List, Discovery List, and My List. Refer to *Customizing Layout Views* in the *Sterling Control Center User Guide* for more information.

Chapter 13

Reports

There are three types of Sterling Control Center reports:

- Standard Sterling Control Center reports are produced from the Control Center console, either on demand (**Reports** > **Define/Run**) or by scheduling them to be run at a certain time and sent to designated recipients via e-mail (**Reports** > **Automate**).

  The Audit Log is a standard report of changes made to Connect:Direct server configuration objects. It can be run as an on-demand report or displayed on screen (by selecting **Tools** > **Audit Log**).

  The System Activity Graph graphically depicts the servers Control Center is currently monitoring. It is available via **Tools** > **System Activity Graph**). Also, the current status of SLCs can be displayed (using **Tools** > **View SLC Monitors**).
- Database reports use SQL queries or a third-party tool such as Crystal Reports to extract data from the Sterling Control Center databases and create the reports. Sterling Control Center provides several sample reports in Crystal Reports format that you can use with the Control Center databases if you already have Crystal Reports. You can also use these samples as templates to design your own reports. *Data for Third-Party Reporting Tools*, in the *Sterling Control Center Reports Guide*, provides details of database schemas, including database tables and field definitions.
- Log file printouts are helpful for troubleshooting installation problems and other support-related issues. The log files are stored in the ..\log subdirectory of the Sterling Control Center installation directory. They can be accessed easily from the Tools menu on the Control Center console (by selecting **Tools** > **Trace Logs**).
- SLC Debug reports are helpful for troubleshooting SLC problems. They can be accessed easily from the Tools menu on the Control Center console (by selecting **Tools** > **Run SLC Debug Report**).

See the *Sterling Control Center Reports Guide* for report descriptions and samples, procedures to produce reports (both on-demand and automated), and report database contents.

Chapter 14

Sterling Control Center Settings

Sterling Control Center settings control system behavior and performance. Most settings are specified during system installation and do not need to be changed. However, you may need to change some settings to accommodate new requirements.

For more information on both engine and console logs, see *Modify log4j to Retain Log Files* on page 253.

The following table describes the tabs on the Control Center System Settings window:

System Setting	Description
Database	Defines the location and type of Sterling Control Center databases (production and staging), how the connections to the databases are established, when to automatically handle alerts, when and how to send data to the staging database, and when and how to automatically purge it from the staging database. See *Database Settings* on page 151 for field definitions. Refer to *Automatically Maintain Control Center Databases* on page 165 for more information on staging and purging. These settings are established during installation. Take caution when changing them because they affect Control Center operation.
E-mail	Specifies the communications parameters used to send e-mail messages. In Control Center, you can create an action to send an e-mail. That action can be referenced by one or more rules, which when triggered will send an e-mail. The E-mail settings control e-mail routing. See *E-Mail Settings* on page 155 for field definitions. You can also customize the e-mail subject and contents. See *Create an Action* on page 79.
SNMP Hosts	Specifies the host computers where Simple Network Management Protocol (SNMP) traps are sent. You can define a Control Center action that sends a trap to an SNMP tool. These traps contain information from the event that can be used for diagnostics. The action can be referenced by one or more rules, which when triggered will send the SNMP trap. See *SNMP Hosts Settings* on page 155 for information about adding, changing, or deleting SNMP hosts.

System Setting	Description
Application Log	Displays the location of the console application log file. The application log stores information about Control Center console activity. The log name is system generated. The log is stored in the ControlCenter\log directory as a text file. If you access the console through Java Web Start, the log file location is shown. The application log setting is view-only. You cannot change it.
Services	Controls the number of simultaneous pollers, as well as settings relating to configuration management. See *Services* on page 157.
Engine Connection	These setting specify the port that the Sterling Control Center engine is configured to listen on for connections from the Control Center console. This setting is defined during Control Center installation and is view only.
Console Settings	Default Graphic Activity Monitor Expected Maximum Processes specifies the default value for that which constitutes a high level of server activity, as depicted by the bar graph beside the server icon in the Servers listing and in graphic visualizations of server activity. Default Console Auto Refresh Setting sets the default number of seconds between automatic refreshes of the activity monitors for users with permission levels that allow for automatic refresh.
License Management	License Key Versions defines the number of license key versions to keep in history. This tab also allows you to control email settings for importing license key information via email.
File Agent	Settings on the File Agent tab let you specify settings Control Center uses to listen for process submissions from file agents associated with managed Connect:Direct servers.

These settings are all system-wide. See *Changing System Settings* on page 150 for the procedures to change them.

You can also specify how to display time on your Sterling Control Center console. This setting, which is not system-wide, is described in *Console Preferences* on page 160.

Changing System Settings

If you have privileges to do so, you can change any of the system settings.

To change system settings:

1. Do one of the following:
   - Select **Control Center** > **System Settings**.
   - Right-click the Sterling Control Center icon ( ) and select **Properties**. The **System Settings** panel is displayed.
2. To change database settings, select the **Database** tab and change the values. For definitions of Database fields, see *Database Settings* on page 151.

3. To change e-mail connection settings, select the **E-mail** tab and change the values. For definitions of the E-mail fields, see *E-Mail Settings* on page 155.
4. To change the SNMP Hosts settings, select the **SNMP Hosts** tab and change the values. For more, see *SNMP Hosts Settings* on page 155.
5. To view the log file name, select the **Application Log** tab. For a definition of this field, see *Application Log* on page 157.
6. To change the simultaneous pollers setting, select the **Services** tab. For a definition of this field, see *Services* on page 157.

Tip: A good rule of thumb for setting this value is to make it the larger of either 7% or 20% of the total number of managed servers. That is, if the number of servers is less than 35, set Simultaneous Pollers to 7; if the number is 35 or greater, set Simultaneous Pollers to the total number of managed servers times 0.20.

7. To view the ports used to connect to the Control Center engine, select the **Engine Connection** tab. For definitions of the Engine Connection fields, see *Engine Connection* on page 158.
8. To change the default value for determining and graphically depicting a server's maximum expected active processes, or to change the number of seconds between automatic refreshes of the activity monitors, select the **Console Settings** tab. For a definition, see *Console Settings* on page 159.
9. To change license management settings, including settings for the email address to which to send emails regarding license expirations, select the **License Management** tab. For definitions of these fields, see *License Management* on page 159.
10. To change File Agent settings, select the File Agent tab. For definitions of these fields, see *File Agent Settings* on page 160.
11. Click **Update** when finished.

Database Settings

Database settings are viewable on the Database tab of System Settings.

To manage database settings:

1. Click **Control Center** > **System Settings**.
2. You can modify database settings depending on role privileges. Click **Update** to save changes.

To view detailed display-only information about the Control Center databases:

1. From the Database tab of System Settings, do one of the following:
   - Click **Production DB Info** (for the production database).
   - Click **Staging DB Info** (for the staging database).
2. To view more detailed database setup information, statistics, and other information, click tabs on the Staging Database or Production Database panel.

3. Refresh the information by clicking **Refresh**.
4. Click **Close** to close the panel.

Database Settings Field Definitions

The following table defines the fields on the Database tab in System Settings.

Field	Definition
Production Database Maintenance Settings	
Automatically Handle Alerts Older Than (Hours)	The number of hours after which alerts should be automatically moved from the Active Alerts monitor to the Handled Alerts Monitor. If this value is set to 0, no alerts are moved.
Movement of Data to Staging Database: Data Older Than (days)	The number of days after which statistical and event data should be moved from the production database to the staging database. The default value is 7. The minimum value is 2.
Movement of Data to Staging Database: Audit Data Older Than (days)	The number of days after which configuration management audit data should be moved from the production database to the staging database. The default value is 7. The minimum value is 2.
Movement of Data to Staging Database: When to Begin Moving Data	The number of minutes between attempts by Control Center to move data from the production database to the staging database. Or, the time of day to begin moving data to the staging database.
Movement of Data to Staging Database: Number of Rows to Select per DB Transaction	The maximum number of production database rows Control Center reads into memory in preparation for moving to the staging database row by row. The default is 4000.
Production Database Display-Only Information	
Database Type	Type of production database. Set at installation. Display only. Values include: ◆ MySQL ◆ Oracle ◆ DB2 ◆ Microsoft SQL
Database Name	Name of the production database. Set at installation. Display only.
Host Name	The computer where the production database is installed. Set at installation. Display only.
Port	The port number used to access the production database. Set at installation. Display only.

Field	Definition
User ID	The user ID you assign to access the production database. Display only.
Average Insert Time	Average time in milliseconds required to add rows to the production database. Display only.
Average Update Time	Average time in milliseconds required to update rows in the production database. Display only.
Average Delete Time	Average time in milliseconds required to move rows from production to staging database. Display only.
Event table rows	Number of table rows of event data in the production database. Display only.
CD Stats table rows	Number of table rows of Connect:Direct statistical data. Display only.
CE Stats table rows	Number of table rows of Connect:Enterprise statistical data. Display only.
Oldest Record	Oldest record in the production database, in days. Display only.
Data Movements Status	Whether or not currently running. Display only.
Last Data Movement Start	Date/time of beginning of last data movement. Display only.
Last Data Movement End	Date/time of end of last data movement. Display only.
Last Data Movement Duration	Time that last data movement took. Display only.
Next Scheduled Data Movement	Date/time of end of next scheduled data movement. Display only.
Staging Database Maintenance Settings	
Purging of Data from Staging Database: Data Older Than (Days)	Automatically purge data older than the days defined in this field from the events and statistics tables in the Control Center staging database. The default value is 30.
Purging of Data from Staging Database: Audit Data Older Than (Days)	Automatically purge configuration management audit data older than the days defined in this field from the events and statistics tables in the Control Center staging database. The default value is 30.
Purging of Data from Staging Database: When To Begin Purging Data: Run Every *n* Minutes	The number of minutes between database purge attempts.
Purging of Data from Staging Database: When To Begin Purging Data: Run Daily at *time*.	The time at which to do a daily purge. Defined as Control Center engine time.
Number of Rows to Select per DB Transaction	The maximum number of database rows Control Center reads into memory in preparation for purging data from the staging database row by row. The default is 4000.

Field	Definition
Staging Database Display-Only Information	
Database Type	Type of staging database. Set at installation. Display only. Values include: ◆ MySQL ◆ Oracle ◆ DB2 ◆ Microsoft SQL
Database Name	Name of the staging database. Set at installation. Display only.
Host Name	The computer where the staging database is installed. Set at installation. Display only.
Port	The port number used to access the staging database. Set at installation. Display only.
User ID	The user ID you assign to access the staging database. Display only.
Average Insert Time	Average time in milliseconds required to add rows to the staging database. Display only.
Average Update Time	Average time in milliseconds required to update rows in the staging database.
Average Delete Time	Average time in milliseconds required to purge rows from staging database. Display only.
Event table rows	Number of table rows of event data in the staging database. Display only.
CD Stats table rows	Number of table rows of Connect:Direct statistical data. Display only.
CE Stats table rows	Number of table rows of Connect:Enterprise statistical data. Display only.
Oldest Record	Oldest record in the staging database, in days. Display only.
Purge Status	Whether or not purge is currently running. Display only.
Last Purge Start	Date/time of beginning of last data purge. Display only.
Last Purge End	Date/time of end of last purge. Display only.
Last Purge Duration	Time that last purge required. Display only.
Next Scheduled Purge	Date/time of end of next scheduled purge. Display only.

E-Mail Settings

The following table defines the fields on the E-Mail tab in System Settings.

Field	Definition
SMTP Host	The required IP address or domain service name for the SMTP server used for sending e-mails. You can enter an address or name up to 255 characters in length.
SMTP Port	The optional 1- to 5-digit port number that the SMTP server listens on. The default value is 25. The maximum value is 65535.
User ID	The optional 1- to 64-character user ID to log on to the SMTP server. This field is case sensitive.
Password	The 1- to 64-character password associated with the user ID for logging on to the SMTP server. Optional.
From E-mail	The From address to specify in outgoing e-mails. Required. Special characters are allowed. **Note:** You can test the From E-mail address by clicking Test, supplying the address, and clicking Send.

SNMP Hosts Settings

SNMP Hosts settings specify the host computers where SNMP traps are sent from Sterling Control Center.

This section details the following information:

- SNMP Host Field Definitions
- Add an SNMP Host
- Edit an SNMP Host
- Remove an SNMP Host

SNMP Host Field Definitions

Following are field definitions for the SNMP Host Settings:

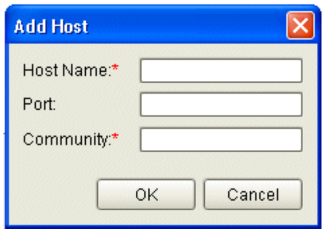
Field Name	Definition
Host Name	The IP address of the server that Control Center sends SNMP traps to. This field is required if you configure the host settings.
Port	The optional 1- to 5-digit port number that the SNMP host listens for traps on. The default value is 162. The maximum value is 65535.

Field Name	Definition
Community	The SNMP community string included in the SNMP traps generated by Control Center. The maximum length is 64 characters. No special characters allowed. Required if you configure host settings.

Add an SNMP Host

To add an SNMP host:

1. Select **Control Center** > **System Settings** to display the **System Settings** window.
2. Select the **SNMP Hosts** tab.
3. Click **Add** to display the **Add Host** window.



4. Type the following information (see *SNMP Host Field Definitions* on page 155 for details):
   - Host Name
   - Port
   - Community (optional)
5. Click **OK**.
6. Click **Add** to add another SNMP host, or click **OK** to close the **System Settings** window.

Edit an SNMP Host

To edit an SNMP host:

1. Select **Control Center** > **System Settings** to display the **System Settings** window.
2. Select the **SNMP Hosts** tab.
3. Double-click the table row to edit, enter your changes, and click **OK**.

Remove an SNMP Host

To remove an SNMP host:

1. Select **Control Center** > **System Settings** to display the **System Settings** window.
2. Select the **SNMP Hosts** tab.
3. Select the host you want to remove.

4. Click **Remove**.
5. Click **OK** on the confirmation window.

Application Log

The following table defines the single field on the Application Log tab in System Settings.

Field	Definition
Log File Name	The application log stores information about Sterling Control Center console activity. The name is system generated. The log is stored in the ControlCenter\log directory as a text file. The application log file name setting is view only. You cannot change it.

Services

The following table defines the single field on the Services tab in System Settings.

Field	Definition
Simultaneous Pollers	The number of threads Sterling Control Center uses to poll Connect servers in collecting server statistics. The minimum and default value is 7. **Note:** A good rule of thumb for setting this value is to make it the larger of either 7 or 20% of the total number of managed servers. That is, if the number of servers is less than 35, set Simultaneous Pollers to 7; if the number is 35 or greater, set Simultaneous Pollers to the total number of managed servers times 0.20.
Check for configuration changes on servers	How often Control Center should check for changes to configuration objects on managed servers. Select Never or specify a time for Run Daily at.
Minimum number of configuration versions	The minimum number of configuration versions Control Center should retain for each configuration object type.
Minimum age of configuration versions	The minimum age of configuration versions that Control Center should retain.

Field	Definition
Start certificate expiry notification	The number of days before expiry of trusted or key certificates when Control Center will begin generating events. The default is 60 days. Certificate expiry checking works only for certificates in Control Center‘s object repository. To ensure that your certificates are in the repository, you can manually check and add them using Configure Servers > Secure+ > Secure+ Key Certificates or > Secure+ Trusted Certificates. Or, you can automatically check for configuration changes on a daily basis using the “Check for Configuration Changes on Servers” system setting. **Note:** This option is available only for servers that support configuration management. When a certificate has reached the point when expiry notifications are to be generated, notifications are generated once a day until the certificate’s expiration time changes. **Note:** To act upon certificate expiry events, or notifications, you can use the Certificate Expiry Warning predefined rule to define the number of days before expiry that action will be taken. For more information, see *How Can I Know When My Secure+ Certificates Are About To Expire?* in the *Sterling Control Center How-To Guide*.

Engine Connection

The following table defines the fields on the Engine Connection tab in System Settings.

Field	Definition
Engine HTTP Port	The HTTP port (for nonsecure connections) that the Sterling Control Center engine listens on. This setting is defined during Control Center installation. Display only.
Engine HTTPS Port	The HTTPS port (for secure connections) that the Sterling Control Center engine listens on. This setting is defined during Control Center installation. Display only.

Console Settings

The following table defines the fields on the Console Settings tab in System Settings.

Field	Definition
Default Graphical Activity Monitor expected maximum processes	The maximum number of processes servers are likely to handle at one time. This value can be overridden for a particular server in Server Properties, the Settings tab. (See *View or Change Server Properties* on page 50.)
Default Console Auto Refresh System Setting in seconds	The default number of seconds to elapse between automatic refreshes of the activity monitors. Users with permission can override this value by setting Change Auto Refresh To under Tools > Console Preferences.

License Management

The following table defines the fields on the License Management tab in System Settings.

Field	Definition
License key versions	The number of license key versions to keep in history.
Email user	The user who is sent emails containing license key information to be imported into Control Center via License Management.
Email user password	The user password for the email user who is sent emails with licenses.
Email hostname	The email system hostname.
Email host port	The email system host port.
Email protocol	The protocol used by the email system (IMAP or POP3).
Frequency (minutes)	How often, in minutes, to check for new license information arriving via email.

File Agent Settings

The following table defines the fields on the File Agent tab in System Settings.

Field	Definition
SNMP Listener Address	IP address from which Control Center listens for process submissions from file agents.
SNMP Listener Port	Port Control Center uses to listen for process submissions from file agents.
Generate No Process Submited Notifications Every *x* Minutes After Last Submit	The number of minutes Control Center will wait for a “Process was submitted” trap from a monitored File Agent before generating an event stating that no submits have recently been initiated.
File Agent Service Status	The status of the File Agent service. (Display only.)

Console Preferences

Console Preferences determines how time is displayed on the console for a particular user, and how often monitors are automatically refreshed.

The Time Preferences settings determine how time is displayed on the Sterling Control Center console for a particular user. This time preference is used for all Sterling Control Center functions that the user performs or views from the console. Time preferences are saved in the user’s profile, so when the user logs on again the same time preferences are used.

Auto Refresh settings determine how often open monitors are automatically refreshed.

To set the time preferences:

1. Select **Control Center > Console Preferences**, then click on the **Time Preferences** tab.
2. Select one of the following time displays:

Display	Description
UTC	Displays the time in Coordinated Universal Time (UTC). **Note:** Since UTC never changes for daylight saving time (DST), do not use UTC for your rule or SLC schedules. Otherwise you most likely will need to manually adjust your schedules to compensate for DST.

Display	Description
Local Time	Displays the time from the computer where the Sterling Control Center console is installed. If you use local time display, verify that the console is displaying the correct time zone. If the time zone is incorrect, manually select the correct time zone from the **Specific Time Zone** list box, or adjust your system's time zone value, as that is where the console obtains this information.
Engine Time	Displays the time from the computer where the Sterling Control Center engine is installed.
Specific Time Zones	Displays the time selected from the list box of standard time zones.

3. Click **Update**. The new time preferences take effect immediately.

To set auto refresh settings:

1. Select **Control Center > Console Preferences**, then click on the **Auto Refresh Settings** tab.
2. Select Use System Setting to use the system setting currently for all users. The current setting is displayed in seconds.
3. Select Change Auto Refresh To and enter a new auto refresh setting in seconds in the text box. The auto refresh setting is changed for the user after you click Update.

Chapter 15

Administering Other Systems

Sterling Control Center allows for direct access to Sterling Integrator, Sterling File Gateway, and Connect:Direct. Your access depends in part on your credentials on those other systems.

This chapter covers the following information:

- Accessing the Connect:Direct Browser User Interface
- Accessing Sterling Integrator and Sterling File Gateway

Accessing the Connect:Direct Browser User Interface

With authorization, you can access Connect:Direct from Sterling Control Center through the Connect:Direct Browser User Interface. From this user interface an administrator can log into Connect:Direct, sign onto a Connect:Direct server, change initialization parameters, and maintain netmap and user authorization information.

To log in to the Connect:Direct Browser User Interface:

1. Right-click a Connect:Direct server in the list of servers.
2. Click **Connect Direct Browser** > **Login Page**. The **Sign On to a Connect:Direct Node** screen displays.

To sign onto a Connect:Direct server:

1. Right-click a Connect:Direct server in the list of servers.
2. Click **Connect Direct Browser > Sign On**. The **Sign On Request Response** screen displays.

To change initialization parameters:

1. Right-click a Connect:Direct server in the list of servers.
2. Click **Connect Direct Browser** > **InitParms**. The **Change Initialization Parameter**s screen displays.

To maintain netmap information:

1. Right-click a Connect:Direct server in the list of servers.
2. Click **Connect Direct Browser** > **NetMap**. The **Select Netmap** screen displays.

To maintain user authorizations:

1. Right-click a Connect:Direct server in the list of servers.
2. Click **Connect Direct Browser** > **User Auth**. The **Select User Authorities Results** screen displays.

Note: For information on administering Connect:Direct, consult the Connect:Direct documentation.

Accessing Sterling Integrator and Sterling File Gateway

With authorization, you can access Sterling Integrator and Sterling File Gateway from Sterling Control Center.

Note: The Dashboard port value in Server Properties (Connection tab) must be specified; otherwise the Sterling Integrator Dashboard option cannot be used.

To access the Sterling Integrator Dashboard and sign onto a Sterling Integrator server as the user designated in server properties:

1. Right-click the Sterling Integrator server.
2. Select **Sterling Integrator Dashboard** > **Login Page**. The Sterling Integrator Dashboard Login screen is displayed.
3. Provide valid Sterling Integrator credentials and click **Sign In**. The **Admin Console Home** screen displays.

Note: For information on administering Sterling Integrator via the Sterling Integrator Dashboard, consult the Sterling Integrator documentation.

To access Sterling File Gateway:

1. Right-click the Sterling File Gateway server.
2. Select **Sterling File Gateway** > **Login Page**.

   The **Sterling File Gateway** Login screen displays.
3. You must provide valid Sterling File Gateway credentials and click **Sign In**.

Chapter 16

Database Administration

Sterling Control Center information is stored in a MySQL, Oracle, Microsoft SQL Server, or DB2 database. To maintain optimal system performance, your database should regularly be staged, purged, and backed up.

For all database types, your database administrator should use the database utilities provided with those products to perform this maintenance.

This chapter addresses the following topics:

- Automatically Maintain Control Center Databases
- Move Data in Bulk to the Staging Database

Automatically Maintain Control Center Databases

When you first install Sterling Control Center you are asked to set up two Control Center databases, a production database and a staging database. Staging is the act of moving data from the production database to the staging database. Once in the staging database the data can then be purged or archived and then purged by the database administrator. You can access the staging database for purging or archival without disrupting data collection into the production database. You can establish an automated staging schedule for the production database and an automated purge schedule for the staging database.

For automated database staging and purge setup, see *Database Settings* on page 151.

Move Data in Bulk to the Staging Database

Note: This method of transferring data refers only to systems where the production and staging databases reside on the same database instance, that is, on the same physical machine and in the same database server. In addition, the production database user ID must have permission to access the staging database tables.

To speed up the transfer of data from the production to the staging database, Control Center automatically moves data in bulk instead of row by row whenever it is possible. To use this more efficient method, Control Center goes through these steps:

- Copies *n* number of rows from production database table to a temporary table

> **Note:** *n* is the **Number of rows to select per DB transaction** specified on the System Settings window. For more information, see *Sterling Control Center Settings* on page 149.

- Copies all the data from the temporary table to the staging database table
- Using the data in the temporary table, deletes all the data from the production database table that has been copied to staging database table

Control Center repeats these steps until all the data up to the desired date is moved to the staging database.

Chapter 17

Tuning Sterling Control Center

Sterling Control Center does much more than display the status of managed servers—it collects activity data from servers, processes the data and, as part of the processing, stores the data in the database. In addition, data processing includes applying rules and SLCs. Control Center's performance is measured by the number of events it processes per second. The major components of Control Center are the Control Center Engine, the Control Center Console, and the database server. All three affect the overall performance and must be run separately on high-powered hardware. Running any component on an underpowered machine will have a negative impact on the overall performance.

To maximize your system's performance, review the guidelines in the following sections and implement those that will work in your environment:

- General Tuning
- Using the Control Center Console Wisely
- Tune the Database Server

For more information from external sources on how to improve performance, see *Additional Reference Information* on page 175.

General Tuning

Multiple threads and services on the Control Center engine simultaneously collect data from different managed servers, process data, and issue database commands to the database server. The database server must be powerful enough to handle all these concurrent requests. Because database operation is I/O intensive, the database server should be run on a machine with fast I/O devices.

Review the following general guidelines related to your environment and network:

- For both UNIX and Windows systems, no other application should be installed on the same file system or drive where Control Center is installed.

  This stems from the fact that Control Center uses checkpoint files to determine the last time it collected activity data from a managed server, and keeps these files in the location where Control Center is installed.

- Do not run any other application, including anti-virus software, on the machine where the Control Center engine is running.
- Make sure that the network connectivity between the Control Center engine and the database server is on a high-speed network.
- Use a multi-CPU machine for the Control Center engine when monitoring a large number of servers. No other tuning will help an underpowered machine.

Tune the Control Center Engine

Review the following general guidelines to tune the Control Center engine:

- Make sure that the Control Center engine is running on adequate hardware.

  To estimate the engine requirements appropriate for your environment, see the *Determining Engine Requirements* appendix in the *Sterling Control Center Getting Started Guide*, which outlines the steps for finding the required hardware. Worksheets and a utility program are provided to assist you in this planning.
- Adjust the number of simultaneous pollers.

  As noted earlier, multiple services simultaneously collect data from different managed servers. The number of simultaneous services that collect data from managed servers is determined by the Simultaneous Pollers setting, which you can change by going to **Control Center**>**System Settings**>**Services**. The recommended setting is 20% of the total number of managed servers. If you specify a number higher than the default setting of 7, you must adjust your heap size.
- If necessary, increase the java heap memory size to accommodate the number of simultaneous pollers Control Center needs. By default, the java process in Control Center uses up to 512 MB.

  To calculate your memory requirement, use the following formula:

  ```
  Heap = 45 MB +
         (Number of simultaneous pollers * 30 MB) +
         (Number of servers *.5 MB) +
         (Number of Completed Processes cached * 1 KB * Number of servers * Average
          Number of Data Visibility Group Activity per servers)
  ```

  If more than 1.5 GB of heap is required, you must use a 64-bit Operating System and install Control Center with the 64-bit JRE. On a 32-bit system, even if you have more than 2 GB physical RAM, the java process cannot use it.
- If required, add more physical memory to your system.

  You should never allocate more memory to heap than the available physical memory on the machine. For example, if your computer has 1 GB physical memory (some of which is used by the operating system), the physical memory available for other processes is less than 1 GB. In that case, you should not specify 1 GB as the max heap size for the java process.

- Reduce the completed processes cache size. To access this setting for a particular server, right-click the server, select **Properties,** click on the **Settings** tab**,** and then click the **Advanced** button. Adjust the value for the Max. Completed Processes accordingly.

  By default, the last 100 completed processes are kept in memory for each server. This cache uses heap memory and approximately 1 KB per entry. When managing a large number of servers, a significant amount of heap memory is used. Reducing the completed processes cache size also reduces the heap memory usage.

- Do not specify too high a value for the system setting, **Number of rows to select per DB transaction** (the default is 4000 rows) because a high value requires a great deal of heap memory if the production and staging databases are in separate database instances.

  In addition, the database server will be forced to do a table scan to select that number of rows instead of using an index, which also slows down the process. To access this setting, go to **Control Center**>**System Settings**>**Database**.

- To reduce processing overhead, including less database usage, consider not collecting process step statistics for Connect:Direct servers. To access this option, select the server, and go to **Properties**>**Connection**.

Caution: If you have any rules or SLCs that depend on the step start and step end events, those SLCs and rules will not work if you do not collect the step statistics. For example, if you enabled this option and you had a rule that watches for a copy step failure, the rule would not work.

- To reduce processing overhead, remove or disable any unused rules and SLCs.
- Adjust both the Production database and Staging database maintenance settings (**Control Center**>**System Settings**>**Database**) to keep the minimum amount of data you need.

  When databases have less data, they perform better, and their insert, update, and seek times are faster. When your performance starts degrading, it could be because there is too much data in the Control Center databases and the activity data collection from the managed servers is falling behind.

  The staging database is not an archive database for permanent storage—you must move the data to a data warehousing type of database.

- Schedule reports to run when there is less activity on the database server, which, in turn, results in less activity in the database server. Running reports during off-peak hours reduces database contention and helps in collecting data from managed servers.
- Set up Server groups and restricted roles, and then assign users to restricted roles. Linking specific users to the specific servers they need to monitor avoids different users monitoring the same server’s activities, which, in turn, reduces overhead on the Control Center engine.
- Do not change the engine’s default log level unless necessary.

  Excessive logging involves intensive file system I/O and slows down processing significantly, thus, severely degrading performance. Control Center log files are used to troubleshoot exceptions. The default logging level is set up to log all abnormal situations and is sufficient in normal production environments. Change the log level only when troubleshooting issues, and once you resolve the issue, change the log level back to the default level.

- To reduce the engine overhead, increase the size of the engine log file (the default size is 1000 KB) by opening the CCEngine.log4j file and changing the value in the line **log4j.appender.R.MaxFileSize=1000KB**.

  If you are monitoring a large number of servers, you may be required to do this because of the growing number of file switches required to keep up with the amount of information going into the log. When the size of the log reaches 1000 KB, a new file is created and the old file is renamed with a number suffixed to the end. If the log file fills up quickly, a log file switch occurs, which slows the engine performance. If the log file size is larger, fewer log file switches will occur resulting in less engine overhead.

- When running reports, narrow the report to a specific server and specific date. By specifying criteria that use an index for the database table involved in the report, less database I/O is performed, making the report run faster. When indexes are used, database table scans are avoided, resulting in less overhead on the database server.

  The indexes and the columns they contain are shown below for the EVENTS and CD_STATS_LOG database tables. To make your report run faster, specify as many columns as possible.

  The EVENTS table contains the following indexes and associated columns:

  ```
  EVENT_ID_INDEX (EVENT_ID)
  SEQ_NUM_INDEX (DATE_TIME, SEQ_NUM, NODE_ID)
  EVENTS_ALERTS_DEL (ALERT, ALERT_DELETED)
  EVENTS_COMPLETED (ACTIONS_COMPLETED)
  EVENTS_TYPE_INDEX (EVENT_TYPE, NODE_ID, NODE_TYPE)
  EVENTS_SLC_INDEX (SLC_SRC_EVENT_ID, SLC_INSTANCE_ID, ALERT, ALERT_DELETED)
  EVENTS_STAT_IDX (NODE_ID, PROC_NAME, PROC_ID, DATE_TIME)
  ```

  The CD_STATS_LOG table contains the following indexes and associated columns:

  ```
  CD_STAT_INDEX (LOG_DATE_TIME, SEQ_NUM, NODE_ID)
  CD_STAT_NODE_INDEX (NODE_ID, PROC_NAME, PROC_NUMBER)
  CD_STAT_NAME_INDEX (NODE_ID, PROC_NAME, PROC_NUMBER, LOG_DATE_TIME)
  CD_EVENT_ID_IX (EVENT_ID)
  ```

- Pause the monitoring on servers that will be down for an extended period of time. By not polling inactive servers, processing overhead for the Control Center engine is reduced.
- Increase the monitor rest time to reduce how often Control Center collects data from the managed server while increasing the amount of data Control Center collects in a single poll. The maximum monitor rest time varies for each type of managed server. For more information, see Monitor Rest Time in the *Sterling Control Center User's Guide*.
- Use an unencrypted connection between the engine and managed servers to reduce CPU usage and improve performance.

Caution: Generally, if any connection is made over the internet, a secured connection is strongly recommended.

Using the Control Center Console Wisely

The Control Center console obtains activity data from the engine for only those servers for which an activity monitor is opened. Server status events and alerts are always collected from the engine regardless of which monitors are opened.

Review the following general guidelines related to using a Control Center console:

- Close any unneeded Completed and Queued Activity monitors. The Control Center console periodically gets activity data from the engine. (The frequency is based on the Auto Refresh rate.) If monitors are not open, the Console does not need to collect activity data, which reduces the processing overhead on the Console and related I/O activities.
- To reduce the overhead on the Console, open Completed and Queued Activity monitors only on the servers whose activities you really want to see. For example, if you are monitoring 1000 servers and the Completed Activity Monitor is opened on all 1000 servers, the monitor will be constantly filled with new activities. This will not only make it difficult for you to find what you are looking for, it will also simultaneously increase the processing overhead for the Console by making it retrieve the activity data for all those servers.
- Use a non-secure connection between the engine and console, unless you are connecting to the engine over the internet. If you are using the internet, a secure connection is strongly recommended.

Caution: Generally, if any connection is made over the internet, a secured connection is strongly recommended.

- To reduce the overhead on the Console, increase the Auto Refresh settings using one of the following methods:
  - Change the **Default Console Auto Refresh System Setting in seconds** setting (Control Center>System Settings).
  - Specify a new value for the **Change Auto Refresh to:** setting (**Control Center>Console Preferences>Auto Refresh Settings**).
- To reduce the number of data requests to the engine, require manual refresh for users who do not need to actively monitor managed servers. Set up roles that use the Manual option for the Console Auto Refresh Permission.
- When you are not using the Console, log out of it. Each console connected to the engine increases the events processing by approximately six events per second on the engine.
- To further improve the engine performance, set up alerts to send e-mail notifications as alert conditions occur instead of requiring users to monitor alerts using the Console.
- When monitoring a large number of servers, use the option, **Sterling Control Center Console - Large Configuration (Greater Than 512 MB, Less Than 1 GB)**, on the Sterling Control Center Launch Page. The large configuration allocates up to 1 GB max heap size, which will improve performance.
- When monitoring a large number of servers, avoid using VPN to connect to the engine. VPN connections are secure and encrypted and as a result, are 2 to 3 times slower than non-secure connections. When you open an activities monitor which covers a large number of managed

servers and activities on those servers, a lot of data has to be transferred over the secure connection, which will slow down performance.

Tune the Database Server

The database plays a crucial role in Control Center by acting as the repository for the data Control Center collects from the monitored servers. The database server must be able to handle all database operation requests issued by the Control Center engine. The ability of the Control Center engine to perform optimally depends on the capacity of the database server, and its hard disk speed is an important factor in providing better performance.

In addition to the guidelines contained in this section, see the *Determining Engine Requirements* appendix in the *Sterling Control Center Getting Started Guide*, to review the Database Sizing worksheet.

The guidelines in this section are broken down into the following area:

- *General Database Tuning* on page 172
- *Guidelines for Oracle Databases* on page 173
- *Guidelines for MS SQL Servers* on page 174
- *Guidelines for DB2 Databases* on page 174
- *Guidelines for MySQL* on page 175

General Database Tuning

Review the following guidelines related to general database tuning:

- Check for known hardware and software problems pertaining to your system.
- Never tune more than one level of your system at a time.
- Put tracking and fallback procedures in place before you install and begin to use Control Center.
- Do not share the database instance with other applications.
- If you use a virus scanner, disable it if it is on the database server. If you cannot disable the virus scanner, at least exclude the database files and directories from the Virus Scanner operation. Also, schedule the scan during off-peak times.
- To avoid disk contention, use different physical disks for data files and log files.
- Rebuild indexes periodically. For the main tables, EVENTS, CD_STATS_LOG, CE_STATS_LOG, rebuild these indexes at least every week.
- Increase the database buffer.
- Use hardware-based RAID (Redundant Array of Independent Disks) technology.
- Use database clustering.

Guidelines for Oracle Databases

Review the following guidelines to tune Oracle databases:

- Use Oracle Real Application Clusters (RAC).
- Use hardware-based RAID (Oracle-recommended RAID 1 for performance).
- The key initialization parameters in Oracle are SGA_MAX_SIZE, PGA_AGGREGATE_TARGET, DB_CACHE_SIZE, and SHARED_POOL_SIZE. If you use ASMM, SGA_TARGET is the key initialization parameter. Tune the following database parameters using the recommended values:
  - Number of open cursors—at least 1000
  - Database block buffers—at least 19200. Sterling Commerce recommends that you set this to 0 if SGA memory is equal to or greater than 0.
  - System Global Area (SGA) memory (10g/11g only)—greater than 0
  - Shared pool size—at least 900000000
  - Large pool size—at least 614400
  - Java Pool size—at least 20971520
  - Number of processes—at least 500
  - Log Buffer—MAX (0.5, (128K * number of CPUs))
  - Sort Area Size—at least 65536
  - Redo Log Files—The behavior of the database writer and archive processes depends on the size of redo logs, thus also influencing performance. Generally, the larger the redo log files, the better the performance. Undersized log files increase checkpoint activity and reduce performance. In addition, to reduce redo log operations, consider using the NOLOGGING option.
  - Keep the **Hit Ratio for the Data** cache above 95%.
  - Create an adequate number of dispatchers. For guidance in this area, go to: http://www.orafaq.com/node/1813.
  - Make sure that the SGA is large enough to accommodate memory reads since physical memory is generally much faster than retrieving data from disk.
  - Measure hit ratios for the library cache of the shared pool with the V$LIBRARYCACHE view. A hit ratio of over 95% is optimal.
  - The general rule of thumb is to make the SHARED_POOL_SIZE parameter 50–150% of the size of your DB_CACHE_SIZE.
  - Adjust the PGA_AGGREGATE_TARGET parameter, which determines how efficiently sorting and hashing operations are performed in your database. Use the following formula to get the optimal value:

```
SELECT ROUND(pga_target_for_estimate/1024/1024) target_mb,
estd_pga_cache_hit_percentage cache_hit_perc, estd_overalloc_count FROM
V$PGA_TARGET_ADVICE
```

Guidelines for MS SQL Servers

Review the following guidelines to tune an MS SQL server:

- Make the computer use background services rather than programs. To change your current setting, right-click on **My Computer**>**Advanced**>S**ettings for Performance**.
- For Server properties, select the Boost SQL server priority.
- To avoid frequent checkpoints, adjust the Recovery interval.

Note: All transactions are very short ones (less than a second).

- Use File Groups for database files.
- To watch for I/O bottlenecks, use the System Performance Monitor to check the Physical Disk :% Disk Time and Physical Disk: Avg. Disk Queue Length parameters. Consistently high values indicate an I/O bottleneck. To improve performance, use a faster disk drive, move files to a second disk, or add disks to a RAID array.
- Adjust the memory allocated to the SQL server.
- Keep an eye on the SQLServer:Buffer Manager: Page reads/sec and SQL Server:Buffer Manager: Page writes/sec parameters.
- Store temporary databases on a fast disk.
- Use hardware-based RAID.

Guidelines for DB2 Databases

Review the following guidelines to tune DB2 databases including the DB2 Universal Database (UDB) multi-user version of DB2:

- Ensure that you have enough disks (6–10 per CPU is a good start). The container for each table space should span all available disks. Some table spaces, such as SYSCATSPACE, and those with a small number of tables do not need to be spread across all disks, while those with large user or temporary tables should.
- Buffer pools should use about 75% (OLTP) or 50% (OLAP) of available memory.
- Perform runstats on all tables, including system catalog tables.
- To configure the database manager, use the Configuration Advisor.
- To restrict logging to a separate high-speed disk, specify this disk by using the NEWLOGPATH database configuration parameter.
- To avoid sort overflows, increase the value specified for the SORTHEAP parameter.
- Table space type should be SMS for the system catalog table space and temporary table spaces and DMS raw (device) or file for the rest. Run db2empfa to enable multi-page file allocation for the SMS table spaces; this will allow SMS table spaces to grow an extent at a time (instead of a page), which can speed up heavy insert operations and sorts which spill to disk.
- Set the database's Transaction per Minute (tpm) parameter to a value closer to your system's events/second figure. At minimum, this value should be set to 3000.
- To reduce database locks, set the isolation level to Uncommitted Read.

Guidelines for MySQL

If you are going to monitor a large number of servers, use the large (my-large.ini) or huge (my-huge.ini) configuration option file when you install MySQL Server. In addition, review the following guidelines to tune MySQL:

- For better performance, tune the following MySQL server variables:
  - key_buffer_size—the size of the buffer used for index blocks. To get better index handling (for all reads and multiple writes), increase this value to as much as you can afford.
  - thread_cache
  - max_connections—set this value to at least Number of Simultaneous Pollers + 10
  - query_cache_type—set to 1 to cache all queries
  - query_cache_size—the amount of memory globally available for query caches. This should be fairly large. For large databases, increase the size.
  - query_cache_limit—the maximum size of each query that can be cached. If the query result is larger than the query cache limit, the result will not be cached. Normally. this is set to 1 MB.
  - thread_cache_size—set this to 30

Additional Reference Information

For more information on performance and tuning, refer to the following sources:

Topic	See
General tuning	*Database Tuning: Principles, Experiments, and Troubleshooting Techniques* by Dennis Shasha and Philippe Bonnet ISBN:9781558607538 Morgan Kaufmann Publishers © 2003 (415 pages)
Oracle databases	*Oracle Database 10g Performance Tuning Tips & Techniques* by Richard J. Niemiec ISBN: 9780072263053 Oracle Press Copyright The McGraw-Hill Companies, Inc. © 2007
Tuning SQL servers	*Professional SQL Server 2005 Performance Tuning* by Steven Wort and et al. ISBN: 9780470176399 John Wiley & Sons (US) Copyright Wiley Publishing, Inc. © 2008
Tuning MS SQL	http://www.mssqltips.com/tip.asp?tip=1112

Topic	See
Tuning DB2 UDB version 8.1 and its databases	http://www.ibm.com/developerworks/data/library/techarticle/dm-0404mcarthur/
General MySQL reference	*MySQL Reference Manual*
Optimizing MySQL for read performance	http://ez.no/developer/articles/tuning_mysql_for_ez_publish/optimizing_for_read_performance
General MySQL performance tuning	http://www.mnxsolutions.com/blog/mysql/mysql-performance-tuning.html
What to tune in MySQL server after installing	http://www.mysqlperformanceblog.com/2006/09/29/what-to-tune-in-mysql-server-after-installation/

Note: All websites referenced above were valid at the time of publication, but URLs may change.

Appendix A

Event Type Descriptions

This appendix contains the following information:

- Event Type Descriptions
- Event Type—Connect:Direct Statistic Record ID Cross-Reference

Event Type Descriptions

This table describes all Sterling Control Center event types.

Event Type	Event Name	Description	Possible Use
01	Process Step Started	For Connect:Direct, indicates that a Process step has started. For Connect:Enterprise, indicates a batch transmission has started. For Sterling Integrator, a business Process activity or AFT file transfer has started. For Sterling File Gateway, a Delivery or Route has started. For FTP, a file transfer has started.	To track Process step starts.
02	Process Step Ended	For Connect:Direct, indicates that a Process step has ended. For Connect:Enterprise, indicates that a batch transmission has ended. For Sterling Integrator, indicates that a business Process activity has ended or AFT file transfer has completed. For Sterling File Gateway, a Delivery or Route has completed. For FTP, a file transfer has completed.	To track completions of steps within Processes.

Event Type	Event Name	Description	Possible Use
03	Process Started	For Connect:Direct, indicates that Process has started. For Connect:Enterprise, indicates a batch transmission has started. For Sterling Integrator, indicates that a business Process has started. For Sterling File Gateway, an Arrived File has started. For FTP, a file transfer has started.	To track Process starts.
04	Process Ended	For Connect:Direct, indicates that a Process has ended. For Connect:Enterprise, indicates that a batch transmission has ended. For Sterling Integrator, indicates that a business Process has ended. For Sterling File Gateway, an Arrived File has completed. For FTP, a file transfer has completed.	To track Process completions.
05	Server Status	Relates various types of server status information.	To track server status.
06	SLC Notification	Service Level Criteria	Use Message ID to determine specific type of SLC event.
07	Server Shutdown Started	—	Not currently used.
08	Server Shutdown	—	Not currently used.
09	Process Status	Generated by a Connect:Direct server and contains details about a queued Process.	Used to track queue movement by Connect:Direct Processes.
10	Server License	Results from a license management check on a managed server.	For notification of expiring licenses.
11	Server Error	Indicates that an error has occurred on a managed server.	To track server status.
12	Server Command	Indicates that a monitored server has initiated a command. See *Event Type—Connect:Direct Statistic Record ID Cross-Reference* on page 179 for a list of Connect:Direct commands associated with this event.	To track Process commands, such as delete, suspend, and resume. To track Netmap modifications on managed Connect:Direct servers.
13	Connection Started	Indicates that a managed server has initiated a session/connection.	To track initiation of sessions which are created for performing file transfers.

Event Type	Event Name	Description	Possible Use
14	Connection Shutdown Started	Indicates that a connection, or session, by a managed server has started to shut down. **Note:** Currently used only for Sterling Integrator managed servers.	To track session status.
15	Sterling Control Center Status	Indicates the status of the Sterling Control Center server.	To track Sterling Control Center server status.
16	Process Queue	Contains data on active and queued Processes on managed servers. Connect:Direct and Sterling Integrator only.	This event is used internally within Sterling Control Center.
17	Process Interrupted	Indicates that a process session was interrupted and the Process may be restarted later. Connect:Direct only.	To track Connect:Direct Processes that ended but will restart.
66	Suppressed SLC Notification	Service Level Criteria Workflow notification suppressed because of “Fire-Once” List.	Used for debugging.

Event Type—Connect:Direct Statistic Record ID Cross-Reference

This table cross-references event types to the Connect:Direct statistic IDs. You can use this information to determine what Connect:Direct activities produce associated Sterling Control Center event types. If a statistic record ID is not listed, Sterling Control Center does not use it.

Event Type	Statistic	Description	Platform				
	Record ID		OS/400	HP NonStop	OS/390 z/OS	UNIX	Windows
Connection Started	SB	Session Begin			X		
	SSTR	Session started				X	X
	SMSES	Session Begin	X				
	SESSSTART	Session Begin		X			

Event Type	Statistic	Description	Platform				
	Record ID		OS/400	HP NonStop	OS/390 z/OS	UNIX	Windows
Server Command	ADNADD	Net map entry added	X				
	ADNCHG	Net map entry changed	X				
	ADNDLT	Net map entry deleted	X				
	CDSTOP	Stop command issued	X				
	CH	Change Process			X		
	CHGP	Change Process Command Issued				X	X
	DELP	Delete Process command issued				X	X
	DP	Delete Process			X		
	FLSP	Flush Process command issued				X	X
	FP	Flush Process			X		
	FS	Suspend Process			X		
	FT	Flush Task			X		
	IK	Inq. AP file			X		
	IT	Inq. Trap			X		
	LCOA	Signon failure					X
	NM	Change Netmap			X		
	NMPR	Change Netmap				X	X
	NUTR	Connect:Direct termination requested					X
	PCDEL	Delete Process	X				

Event Type	**Statistic**	**Description**	**Platform**				
	Record ID		**OS/400**	**HP NonStop**	**OS/390 z/OS**	**UNIX**	**Windows**
Server Command (cont.)	PCFLU	Flush process	X				
	PCHOLD	Held Process	X				
	PCREL	Release Process	X				
	PCSUB	Submit Process	X				
	PCSUS	Suspend Process	X				
	PFLS	Process flushed				X	X
	PS	Process submitted			X		
	SI	Signon attempt			X		
	ST	Stop Connect:Direct command issued			X		
	STOP	Stop Connect:Direct command issued				X	X
	SUBMIT	Submit		X			
	SUBP	Submit command issued				X	X
	TS	Suspend Task			X		
	UM	Update Network Map			X		
	UU	Update User			X		
	XCMM	UNIX sign-on failure					
Server Error	PERR	Process error detected				X	X
	SERR	System error				X	
Server License	APCK	Asset Protection Check					X
	LIEX	License has expired				X	X
	LWEX	License will expire in 14 days				X	X

Event Type	Statistic	Description	Platform				
	Record ID		OS/400	HP NonStop	OS/390 z/OS	UNIX	Windows
Process Status	LEXC	An unknown exception has occurred					X
	QCEX	Queue Change to Exec Queue				X	X
	QCHO	Queue Change to Hold Queue				X	X
	QCTI	Queue Change to Timer Queue				X	X
	QCWA	Queue Change to Wait Queue				X	X
	QE	Queue Change to Exec Queue			X		
	QH	Queue Change to Hold Queue			X		
	QT	Queue Change to Timer Queue			X		
	QW	Queue Change to Wait Queue			X		
Server Status	SD	Connect:Direct Starting			X		
	TF	TCQ Full					
	TL	TCQ Below Defined Threshold					
	TW	TCQ Above Defined Threshold					
	XSTA	User Exit Program Started					
Process Ended	PRED	Process Ended				X	X
	PROCEND	Process Ended		X			
	PT	Process Termination			X		
	SMPTM	Process Ended	X				
	USEC	User Security check issued				X	X
	ZT	Process Termination			X		

Event Type	Statistic Record ID	Description	Platform				
			OS/400	HP NonStop	OS/390 z/OS	UNIX	Windows
Process Started	PI	Process Started			X		
	PROCSTART	Process Started		X			
	PSTR	Process Started				X	X
	SMPST	Process Started	X				
	ZI	Process Started			X		
Process Step Ended	CT	Copy Termination			X		
	CTRC	Copy Control record written				X	X
	IFED	IF statement ended				X	X
	MC	PDS Member Copy			X		
	RJ	Run Job			X		
	RJED	Run Job command completed				X	X
	RT	Run Task			X		
	RTED	Run Task command completed				X	X
	SBED	Submit complete				X	X
	SMSTTM	Process Step Ended	X				
	STEPEND	Process Step Ended		X			
Process Step Started	CI	Copy Step Start			X		
	IF	If statement started			X		
	JI	Run Job Start			X		
	LSST	Local Process Step Started				X	X
	RSST	Remote Process Step Started				X	X
	SMSTST	Process Step Started	X				
	STEPSTART	Process Step Started		X			
	SW	Submit within a Process			X		
	TI	Run Task Start			X		
	UM	Update Network Map			X		

Appendix B

Administrative Troubleshooting

The following table identifies issues you may experience administering Sterling Control Center, along with solutions to fix each issue. For information on issues more relevant to users, see the *Sterling Control Center User Guide*.

System Troubleshooting Issues

Issue	Solution
Logging off UNIX kills the Sterling Control Center process.	Log on as root to the computer where the engine is installed, then start Sterling Control Center.
java.lang.OutOfMemoryError message received when logging on to Sterling Control Center on a HP-UX computer.	Set the HP-UX kernel parameters to the following values to avoid this error: ◆ kernel maxusers–2000 ◆ kernel nproc–5120 ◆ kernel max_thread_proc–3000 ◆ kernel nkthread–8976 ◆ kernel nfile–83968 ◆ kernel maxfiles–4096 ◆ kernel maxfiles_lim–4096 ◆ kernel ncallout–8992 ◆ kernel maxdsiz–2063835136 ◆ ndd tcp_conn_request_max–2048 See the HP-UX documentation for instructions to set these parameters.

Issue	Solution
Not enough space errors received during installation.	◆ Delete unnecessary files to provide more room on your computer. ◆ Close all open applications and rerun the installation.
Getting out-of-memory errors on the Control Center engine server	By default, the Control Center engine's maximum heap size is set to 512 MB. You can increase this value when getting out-of-memory errors or when you increase Simultaneous Pollers in Systems Settings. The guidelines and steps apply both to 32-bit and 64-bit platforms. To calculate your heap requirements, use the following formula: Maximum heap size = 45 MB + (# simultaneous pollers * 30 MB) + (# servers * .5 MB) + (# completed processes cached * 1 KB * # servers) If more than 1.5 GB of heap is required, you must use a 64-bit system. Changing java heap settings in both Windows and UNIX environments involves editing the InstallationInfo.properties file to add an entry, then running the configCC.bat/sh configuration script, and restarting the Control Center engine. To change java heap settings: 1 Make a back up the file InstallationInfo.properties located at ControlCenterInstallDirectory\conf. 2 Open InstallationInfo.properties (located at ControlCenterInstallDir\conf) with a text editor (such as Notepad on Windows or vi on UNIX). 3 Look for line that starts with MAX_HEAP_SIZE. (If it is there, change the value to the desired number). If it is not there, add a line at the end of the file as below. MAX_HEAP_SIZE=-Xmx???m 4 Replace the ??? with the desired number. Example: MAX_HEAP_SIZE=-Xmx1024m 5 Save the file. 6 Run the configCC.sh (UNIX) or configCC.bat (Windows) file located at ControlCenterInstallDirectory/bin. 7 Answer no to all the questions. Merely running the script makes the necessary updates to different runEngine scripts. 8 Stop the engine using stopEngine.sh (UNIX) or stopEngine.bat (Windows). 9 Start the engine using runEngine.sh (UNIX) or runEngine.bat Windows).

Issue	Solution
Rules produce no results.	◆ If you specify multiple criteria, all criteria must be met for the rule to take effect. Try reducing the number of criteria. ◆ Rule values are case-sensitive. Verify you are using the proper case. ◆ Earlier rule criteria was met. Verify that the rules are in proper order. ◆ Verify that the rule is enabled, and, if the rule has a schedule associated with it, the schedule is enabled and active during the time in question. ◆ See *Troubleshooting Rules* in the *Sterling Control Center How-To Guide* for more information.
Expected User and Server Data statistics are not being produced.	Unlike other configuration data, the Metadata Type Mapping for User Data and Server Data are stored in the database, rather than in the local Control Center configuration. If you switched to a new database or reinitialized the existing database during upgrading or for any other reason, the Metadata Type Mapping values were lost. For instructions on how to map metadata types, see *Manage Metadata Type Mapping* on page 133.
No WS_FTP statistics or events are being produced even though no errors occurred during installation of the WS_FTP agent and there are no obvious configuration errors in Control Center.	Verify that the name of the directory where you installed the Sterling Control Center FTP agent does not contain any blanks. If it does, reinstall the agent and make sure the name of the new directory does not contain any blanks.
The Sterling Control Center engine shut down unexpectedly.	When an SQL exception occurs within the Sterling Control Center engine that is not a truncation or duplication exception, Sterling Control Center sends out a notification message CJDB026E. It then shuts down Sterling Control Center. If you want to send a notification that a database error has shut down Sterling Control Center, create a rule that identifies this error message and sends a notification.
A driver exception occurred.	When a driver exception occurs, Sterling Control Center sends out a CJDB013E or CLI025E message.
Cannot find the Control Center Engine log file to identify an installation issue.	To display the engine log file, click Tools > Trace Logs. From the list of links that displays in a browser window, select one that begins with “CCEngine.” The log displays in your default text file application. The Sterling Control Center Engine log file is located in the log directory under the Sterling Control Center engine installation directory. The engine log file name starts with CCEngine.
The Sterling Control Center engine is not starting when activated through the Services panel.	Verify that a valid license key called license.key is available in the /conf directory of the Sterling Control Center engine installation location. Read the Sterling Control Center engine log file for more information.

Issue	Solution
The Sterling Control Center Engine shuts down while it is running, caused by the shutdown of the database server.	Check the Sterling Control Center engine log file for details. If the database server has been shut down, restart the database server and restart the Sterling Control Center engine.
Getting out-of-memory errors on the Control Center engine server	By default, the Control Center engine's maximum heap size is set to 512 MB. You can increase this value when getting out-of-memory errors or when you increase Simultaneous Pollers in Systems Settings. The guidelines and steps apply both to 32-bit and 64-bit platforms. Calculate what the maximum heap size should be using this rule of thumb: Maximum heap size = the larger of 512 MB or 300 MB + (10 MB * number of simultaneous pollers) Changing java heap settings in both Windows and UNIX environments involves editing the InstallationInfo.properties file to add an entry, then running the configCC.bat/sh configuration script, and restarting the Control Center engine. To change java heap settings: 1 Make a back up the file InstallationInfo.properties located at ControlCenterInstallDirectory\conf. 2 Open InstallationInfo.properties (located at ControlCenterInstallDir\conf) with a text editor (such as Notepad on Windows or vi on UNIX). 3 Look for line that starts with MAX_HEAP_SIZE. (If it is there, change the value to the desired number). If it is not there, add a line at the end of the file as below. MAX_HEAP_SIZE=-Xmx???m 4 Replace the ??? with the desired number. Example: MAX_HEAP_SIZE=-Xmx1024m 5 Save the file. 6 Run the configCC.sh (UNIX) or configCC.bat (Windows) file located at ControlCenterInstallDirectory/bin. 7 Answer no to all the questions. Merely running the script makes the necessary updates to different runEngine scripts. 8 Stop the engine using stopEngine.sh (UNIX) or stopEngine.bat (Windows). 9 Start the engine using runEngine.sh (UNIX) or runEngine.bat Windows).

Issue	Solution

When Sterling Control Center connects to the DB2 database using db2java.zip JDBC driver file, one of the following errors is written to the Sterling Control Center log file.
`COM.ibm.db2.jdbc.DB2Exception:`
`[IBM][JDBC Driver]`
`CLI0601E  Invalid statement handle or`
`statement is closed. SQLSTATE=S1000`
or
`COM.ibm.db2.jdbc.DB2Exception:`
`[IBM][JDBC Driver]`
`   CLI0621E Unsupported JDBC server`
`configuration.`
	An incompatibility occurred between the level of db2java.zip and the JDBC Applet Server. Use the db2java.zip file from the DB2 installation location to which you are connecting. Then run the configCC command again.

When using the Microsoft SQL Server, Sterling Control Center creates too many connections on the SQL Server. This can be caused by Sterling Control Center using the JDBC connection pooling mechanism, which maintains a fixed number of connections with the SQL server or using statement pooling which reuses the same JDBC connection with many different SQL Statements. For more details refer the following link: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3BQ313220	If you want to reduce the Connection Pool Size: ◆ Stop the Sterling Control Center engine. ◆ From the Control Center engine installation location, edit the following lines in the /conf/services/system/JDBCService.xml file and change the values to the desired number: §<maxpool>50</maxpool> §<maxconn>100</maxconn> §<initsize>16</initsize> **Note:** Setting the value of any of these fields to less than 16 severely impacts the performance of the Sterling Control Center engine. ◆ Save the modified file. ◆ Restart the Sterling Control Center engine.

Cannot log on when trying to manage a Connect:Direct OS/400 server where the correct user ID and password have been provided. The following error is displayed in the log file:
`ERROR CDTask -`
`javax.security.auth.login.FailedLoginException:`
`com.sterlingcommerce.component.`
`persistence.PersistenceException:`
`java.sql.SQLException: [SQL0204]`
`INITPARMS in <Library name> type`
`*FILE not found.`
	Fix the invalid library name specified for server connection properties.

Appendix C

Predefined Actions and Rules

This appendix describes the predefined rules and actions delivered with Sterling Control Center.

Predefined Actions

The following table lists and describes the predefined actions that ship with Sterling Control Center.

Action	Alert Severity/Result	Comments
no operation	none	Specified when no action is warranted. **Note:** You will not find this pre-defined action in the list of defined actions to edit.
alert0	0-In compliance	Associated with in-compliance SLC rules. An alert0 causes any previous alerts associated with its SLC instance to be automatically handled. For linked rules, can be used for either of the resolution and nonresolution actions.
alert1	1-High	
alert2	2-Medium	
alert3	3-Low	

Predefined Rules

The following table lists and describes the predefined rules that ship with Sterling Control Center. For information on the SLC message IDs referred to in the descriptions, see *Message IDs for Rules* on page 195.

Caution: Changing the action defined for a rule may affect the behavior of SLCs that use that rule.

Rule	Description	Event Type
Bad return code	RC not equal zero - alert1	Process Step Ended
Did not start by end of monitor window	CSLC228E - alert1	SLC Notification
On-time completion in jeopardy	CSLC229I - alert2	SLC Notification
Monitor rate out of compliance	Alert 2 if servers not being polled.	Server Status
Process not submitted by File Agent	CCFA006I - Process not submitted by File Agent in timely fashion	Server Command
File Agent Service Initialization Error	CCFA014E - Triggered if File Agent Service initialization error occurs	Server Command
Certificate Expiry Warning	CCFG229I - alert 1 CCFG230I - alert 1	Server Status
Proc duration exceeded	CSLC044E - alert1	SLC Notification
Proc duration not determ.	CSLC050E - alert3	SLC Notification
Proc duration not ended	CSLC043E - alert2	SLC Notification
Proc duration okay	CSLC042I - alert0	SLC Notification
Proc duration running	CSLC049E - alert3	SLC Notification
Proc duration short	CSLC041E - alert2	SLC Notification
Proc duration suspended	CSLC046E - alert2	SLC Notification
Proc duration way over	CSLC045E - alert1	SLC Notification
Process already running	CSLC031E - alert3	SLC Notification
Process ended early	CSLC036E - alert0	SLC Notification
Process ended late	CSLC039E - alert0	SLC Notification
Process ended on-time	CSLC037I - alert0	SLC Notification

Rule	Description	Event Type
Process has not ended	CSLC038E - alert2	SLC Notification
Process has not started	CSLC034E - alert2	SLC Notification
Process not ended warn	CSLC048E - alert3	SLC Notification
Process not even started	CSLC026E - alert2	SLC Notification
Process not started late	CSLC027E - alert1	SLC Notification
Process not started warn	CSLC047E - alert3	SLC Notification
Process started early	CSLC032E - alert3	SLC Notification
Process started late	CSLC035E - alert2	SLC Notification
Process started on-time	CSLC033I - alert0	SLC Notification
Process still not ended	CSLC040E - alert2	SLC Notification
Process suspended	CSLC046E - alert2	SLC Notification
Staging database down	CJDB032E - alert1	Server Status
Trans dur exceeded	CSLC063E - alert2	SLC Notification
Trans dur exceeded-late	CSLC064E - alert2	SLC Notification
Trans dur not determined	CSLC070E - alert1	SLC Notification
Trans dur okay	CSLC062I - alert0	SLC Notification
Trans dur really late	CSLC065E - alert1	SLC Notification
Trans dur running	CSLC069E - alert0	SLC Notification
Trans dur short	CSLC061E - alert2	SLC Notification
Trans dur suspended	CSLC066E - alert2	SLC Notification
Trans ended - late	CSLC059E - alert3	SLC Notification
Trans ended early	CSLC056E - alert3	SLC Notification
Trans ended ontime	CSLC057I - alert0	SLC Notification
Trans not ended - late	CSLC058E - alert2	SLC Notification
Trans not ended	CSLC068E - alert2	SLC Notification
Trans not even start late	CSLC029E - alert2	SLC Notification
Trans not even started	CSLC028E - alert2	SLC Notification
Trans not started - late	CSLC054E - alert1	SLC Notification
Trans not started	CSLC067E - alert2	SLC Notification
Trans running early	CSLC051E - alert3	SLC Notification

Rule	Description	Event Type
Trans started early	CSLC052E - alert3	SLC Notification
Trans started late	CSLC055E - alert2	SLC Notification
Trans started ontime	CSLC053I - alert0	SLC Notification
Trans still not ended	CSLC060E - alert2	SLC Notification
Trans suspended	CSLC066E - alert2	SLC Notification
Transfer ahead of schedule - 25 dMax	CSLC177I - alert3	SLC Notification
Transfer ahead of schedule - 25 dMin	CSLC171I - alert3	SLC Notification
Transfer ahead of schedule - 50 dMax	CSLC179I - alert3	SLC Notification
Transfer ahead of schedule - 50 dMin	CSLC173I - alert2	SLC Notification
Transfer ahead of schedule - 75 dMax	CSLC181I - alert3	SLC Notification
Transfer ahead of schedule - 75 dMin	CSLC175I - alert3	SLC Notification
Transfer behind schedule - 25 dMax	CSLC178E - alert2	SLC Notification
Transfer behind schedule - 25 dMin	CSLC172E - alert2	SLC Notification
Transfer behind schedule - 50 dMax	CSLC180E - alert2	SLC Notification
Transfer behind schedule - 50 dMin	CSLC174E - alert2	SLC Notification
Transfer behind schedule - 75 dMax	CSLC182E - alert2	SLC Notification
Transfer behind schedule - 75 dMin	CSLC176E - alert2	SLC Notification

Appendix D

Message IDs for Rules

The following table lists selected Sterling Control Center messages. This list can help you create rules triggered by a specific message ID. See the *Sterling Control Center How-To Guide* for examples of message IDs used in rules.

This list is sorted by message ID within the event type.

Event Type	Event Name	Message ID	Message Text
Server and Process Command			
12	Server Command	CNCD015E	Process delete failed. *ServerID*, *Command*, *Reason*
12	Server Command	CNCD016E	Process change failed. *ServerID*, *Command*, *Reason*
12	Server Command	CNCD017E	Process suspend failed. *ServerID*, *Command*, *Reason*
12	Server Command	CNCD018E	Stop server failed. *ServerID*, *Command*, *Reason*
12	Server Command	CNCD031E	Server Added, Id: *ServerID*, by: *UserID*
12	Server Command	CNCD032E	Server Updated, Id: *ServerID*, by: *UserID*
12	Server Command	CNCD033E	Server Deleted, Id: *ServerID*, by: *UserID*
12	Server Command	CNCD034E	Process *Processname* has been deleted by user *UserID*
12	Server Command	CNCD035E	Process *Processname* has been suspended by user *UserID*
12	Server Command	CNCD036E	Process *Processname* has been changed by user *UserID*
12	Server Command	CNCD044E	Server *servername* stopped by user *UserID*.
9	Process Status	CNCD053I	Process moved to the Execution queue.
9	Process Status	CNCD054I	Process moved to the Hold queue. Status is Held initially.
9	Process Status	CNCD055I	Process moved to the Timer queue.
9	Process Status	CNCD056I	Process moved to the Wait queue.
9	Process Status	CNCD061I	Process moved to Hold queue. Status is Held in Error.

Event Type	Event Name	Message ID	Message Text
9	Process Status	CNCD062I	Process moved to Hold queue. Status is Held by Operator.
9	Process Status	CNCD063I	Process moved to Hold queue. Status is Held Retained.
9	Process Status	CNCD064I	Process moved to Hold queue. Status is Held Due to Suspension.
9	Process Status	CNCD065I	Process moved to Hold queue. Status is Held for Call.
9	Process Status	CNCD066I	Process moved to Hold queue. Status is Held Initial.
	Sterling Control Center Status Messages		
10	Server License	CCNS004E	License Expiry Warning. License is about to expire. Days left: {0}
5	Server Status	CCNS006E	Maximum concurrent Processes changed.
5	Server Status	CCNS010I	Server running with emergency key.
5	Server Status	CCNS018E	Monitor rate out of compliance. Server ID: {0} Last poll Date/time: {1} Monitor Rest Time: {2}
5	Server Status	CCNS019E	Certificate expiry notification. Server ID: (0) Certificate: {1} Expires: {2} Days left: {3}
5	Server Status	CCNS020E	Monitored Queue Limit has been exceeded. Server ID: {0} Queue: {1} Limit: {2} Depth: {3}
5	Server Status	CCNS022I	Monitoring paused. Server ID: {0} User ID: {1}
5	Server Status	CCNS023I	Monitoring resumed from pause point. Server ID: {0} User ID: {1}
5	Server Status	CCNS024I	Monitoring resumed from current time. Server ID: {0} User ID: {1}
5	Server Status	CCNS025I	At startup, server found to be paused. Server ID: {0}
5	Server Status	CCNS029I	Monitor rate back in compliance. Server ID: {0} Last poll Date/time: {1} Monitor Rest Time: {2}
5	Server Status	CCNS030I	Monitored Queue Limit back in compliance. Server ID: {0} Queue: {1} Limit: {2} Depth: {3}
5	Server Status	CCTR033E	Server is up. **Note:** For monitored server.
5	Server Status	CCTR034E	Server is down. **Note:** For monitored server.
5	Server Status	CCTR035E	Unable to establish a connection to server. Check Server Service configuration parameters for invalid ID and/or password value, or unsupported level of server.
10	Server License	CCTR040E	License management key file in use only valid for {0} more day(s).
10	Server License	CCTR041E	License expired. A new license management key file must be obtained to restart the product.

Event Type	Event Name	Message ID	Message Text
10	Server License	CCTR046E	Emergency license management key file in use. Valid for {0} more day(s).
5	Server Status	CCTR051E	Connection cannot be established to a Connect:Direct server.
12	Server Command	CCTR052I	Simultaneous pollers value changed by user *UserID* to *nn*.
5	Server Status	CCTR055E	Server is up. **Note:** For managed but not monitored server.
5	Server Status	CCTR056E	Server is down. **Note:** For managed but not monitored server.
5	Server Status	CCTR074E	Connection to server established.
5	Server Status	CCTR083E	Engine shutdown has been initiated by *user name*.
5	Server Status	CCTR101E	Service {0} Updated.
	Server Group Messages		
12	Server Command	CGRP012I	Group created
12	Server Command	CGRP013I	Group updated
12	Server Command	CGRP014I	Group deleted
	Role Messages		
12	Server Command	CROL017E	New role created, ID: {0}, by: {1}, Role: {2}
12	Server Command	CROL018E	Role updated
12	Server Command	CROL019E	Role deleted
	Rule Messages		
12	Server Command	CRUL043E	New Rule Created, ID: *RuleID*, by: *UserID*
12	Server Command	CRUL044E	Rule Updated, ID: *RuleID*, by: *UserID*
12	Server Command	CRUL045E	Rule Deleted, ID: *RuleID*, by: *UserID*
12	Server Command	CRUL050E	Alert Deleted
12	Server Command	CRUL077E	Rule moved down
12	Server Command	CRUL078E	Rule moved up
	Metadata Rule Messages		
12	Server Command	CMDR043E	New metadata rule created, *ID*, by: *UserID*.
12	Server Command	CMDR044E	Metadata rule updated, *ID*, by: *UserID*.
12	Server Command	CMDR045E	Metadata rule deleted, *ID*, by: *UserID*.

Event Type	Event Name	Message ID	Message Text
12	Server Command	CMDR077E	Metadata rule moved down, *ID*, by: *UserID*.
12	Server Command	CMDR078E	Metadata rule moved up, *ID*, by: *UserID*.
12	Server Command	CMDR148E	Server metadata field map updated.
12	Server Command	CMDR149E	Metadata field map updated.
	Rule Action Messages		
12	Server Command	CACT025E	New action created, ID: *ActionID*, by: *UserID*
12	Server Command	CACT026E	Action updated, ID: *ActionID*, by: *UserID*
12	Server Command	CACT027E	Action deleted, ID: *ActionID*, by: *UserID*
12	Server Command	CRUL099I	Server command performed successfully. Server ID: {0}, Command: {1}
12	Server Command	CRUL140I	Server command to be performed. Rule ID: {0}, Action ID: {1}, Event ID: {2}, Server ID: {3}, Command: {4}
	Metadata Rule Action Messages		
12	Server Command	CMDA025E	New action created. ID: *ActionID*, by: *UserID*.
12	Server Command	CMDA026E	Action updated. ID: *ActionID*, by: *UserID*.
12	Server Command	CMDA027E	Action deleted. ID: *ActionID*, by: *UserID*.
	Database Messages		
12	Server Status	CJDB026E	Database outage has occurred. System shutdown initiated.
12	Server Status	CJDB032E	Staging database unavailable.
	User Maintenance Messages		
12	Server Command	CUSR030E	New User Created, ID: *UserID*, by: *UserID*
12	Server Command	CUSR031E	User Updated, ID: *UserID*, by: *UserID*
12	Server Command	CUSR032E	User Deleted, ID: *UserID*, by: *UserID*
	Node Discovery Messages		
12	Server Command	CDIS016E	Deleted Explorer node: *NodeID*.
12	Server Command	CDIS017E	Deleted Discovery node: NodeID.
12	Server Command	CDIS019E	Changed enabled state for node: *NodeID.*
12	Server Command	CDIS028E	Discovery complete.
12	Server Command	CDIS031E	Discovery initiated.

Event Type	Event Name	Message ID	Message Text
	Report Service Messages		
12	Server Command	CRPT006E	Updated report: *ReportID*.
12	Server Command	CRPT007E	Deleted report: *ReportID*.
12	Server Command	CRPT008E	Created report: *ReportID*.
5	Server Status	CRPT012I	High Water Mark Report complete.
	License Service Messages		
5	Server Status	CLIC019I	License removed. ID: *NodeID*, Version: *Version#*, User: *UserID*.
5	Server Status	CLIC020I	License added. ID: *NodeID*, Version: *Version#*, User: *UserID*.
5	Server Status	CLIC027I	License push operation complete.
5	Server Status	CLIC028I	License validation operation complete.
5	Server Status	CLIC050E	License import failed. ID: {0} Version: {1} User: {2}
	File Agent Service Messages		
5	Server Status	CCFA001I	File Agent {0} added for Server ID {1}.
5	Server Status	CCFA002I	File Agent {0} removed from Server ID {1}
5	Server Status	CCFA003I	File Agent {0} for Server ID {1} is up.
5	Server Status	CCFA004I	File Agent {0} for Server ID {1} is down.
12	Server Command	CCFA005I	File Agent {0} for Server ID {1} configuration updated.
5	Server Status	CCFA006I	File Agent {0} for Server ID {1} has not submitted a Process lately. Minutes since submit: {2}
5	Server Status	CCFA007I	File Agent {0} for Server ID {1} submitted a Process.
15	Control Center Status	CCFA008I	File Agent Settings for no process submitted warning time value changed by user {0} to {1}.
15	Control Center Status	CCFA009I	File Agent Settings for SNMP listener port value changed by user {0} to {1}.
15	Control Center Status	CCFA010I	File Agent Settings for heart beat interval value changed by user {0} to {1}.
15	Control Center Status	CCFA0014I	Error starting File Agent trap receiver logic. SNMP Listener port specified may already be in use. Error: {0}
15	Control Center Status	CCFA021I	File Agent Settings for SNMP listener address value changed by user {0} to {1}.
15	Control Center Status	CCFA022I	File Agent Service listening on specified SNMP listener address and port. Address: {0} Port: {1}

Event Type	Event Name	Message ID	Message Text
15	Control Center Status	CCFA023I	File Agent peak unprocessed trap count: {0}
	Email List Messages		
12	Server Command	CEDL025E	New Email List Created, ID: {0}, by: {1}
12	Server Command	CEDL026E	Email List Updated, ID: {0}, by: {1}
12	Server Command	CEDL027E	Email List Deleted, ID: {0}, by: {1}
	Report Schedule Messages		
12	Server Command	CRSC028E	Report Schedule Created. ID: {0}, by: {1}
12	Server Command	CRSC029E	Report Schedule Updated. ID: {0}, by: {1}
12	Server Command	CRSC030E	Report Schedule Deleted. ID: {0}, by: {1}
	Automated Reports Messages		
12	Server Command	CRSC051I	Automated Report Created. ID: {0}, by: {1}
12	Server Command	CRSC052I	Automated Report Updated. ID: {0}, by: {1}
12	Server Command	CRSC053I	Automated Report Deleted. ID: {0}, by: {1}
	Calendar Schedule Messages		
12	Server Command	CCAL006E	Updated calendar: *CalendarID*, by: *UserID*.
12	Server Command	CCAL007E	Deleted calendar: *CalendarID*, by: *UserID*.
12	Server Command	CCAL008E	Created calendar: *CalendarID*, by: *UserID*.
	Rule Schedule Messages		
12	Server Command	CRSC025E	New rule schedule created, *RuleID*, by: *UserID*.
12	Server Command	CRSC026E	Rule schedule updated, *RuleID*, by: *UserID*.
12	Server Command	CRSC027E	Rule schedule deleted, *RuleID*, by: *UserID*.
	Calendar Schedule SLC-Generated Messages		
6	SLC	CSLC026E	*Workflow/Milestone/Step/Process* did not start by NERs. SLC: *SLCID*
6	SLC	CSLC027E	*Workflow/Milestone/Step/Process* did not start by NERe. SLC:*SLCID*
6	SLC	CSLC030E	*Workflow/Milestone/Step/Process* started. SLC: *SLCID*
6	SLC	CSLC031E	*Workflow/Milestone/Step/Process* running prior to start of monitoring. SLC: *SLCID*

Event Type	Event Name	Message ID	Message Text
6	SLC	CSLC032E	*Workflow/Milestone/Step/Process* started prior to NSRs. SLC: *SLCID*
6	SLC	CSLC034E	*Workflow/Milestone/Step/Process* did not start by NSRe. SLC: *SLCID*
6	SLC	CSLC035E	*Workflow/Milestone/Step/Process* started after NSRe. SLC: *SLCID*
6	SLC	CSLC036E	*Workflow/Milestone/Step/Process* ended before NERs. SLC: *SLCID*
6	SLC	CSLC037I	*Workflow/Milestone/Step/Process* ended. SLC: *SLCID*
6	SLC	CSLC038E	*Workflow/Milestone/Step/Process* did not end by NERe. SLC: *SLCID*
6	SLC	CSLC039E	*Workflow/Milestone/Step/Proces*s ended after NERe. SLC: *SLCID*
6	SLC	CSLC040E	*Workflow/Milestone/Step/Process* did not complete before the end of the monitoring window. SLC: *SLCID*
6	SLC	CSLC046E	*Workflow/Milestone/Step/Process* suspended. SLC: *SLCID*
6	SLC	CSLC047E	*Workflow/Milestone/Step/Process* did not start by NSRs. SLC: *SLCID*
6	SLC	CSLC048E	*Workflow/Milestone/Step/Process* running after NERs. SLC: *SLCID*
	Duration Schedule SLC-Generated Messages		
6	SLC	CSLC033I	*Workflow/Milestone/Step/Process* started. SLC: *SLCID*
6	SLC	CSLC041E	*Workflow/Milestone/Step/Process* ended before dMin. SLC: *SLCID*
6	SLC	CSLC042I	*Workflow/Milestone/Step/Process* ended when expected - between dMin and dMax. SLC: *SLCID*
6	SLC	CSLC043E	*Workflow/Milestone/Step/Process* did not end by dMax. SLC: *SLCID*
6	SLC	CSLC044E	*Workflow/Milestone/Step/Process* ended after dMax. SLC: *SLCID*
6	SLC	CSLC045E	*Workflow/Milestone/Step/Process* did not complete before the end of the monitoring window. SLC: *SLCID*
6	SLC	CSLC049E	*Workflow/Milestone/Step/Process* did not end by dMin. SLC: *SLCID*
6	SLC	CSLC050E	*Workflow/Milestone/Step/Process* duration could not be determined - was running before monitoring started.
6	SLC	CSLC171I	File Transfer ahead of schedule (25% dMin)
6	SLC	CSLC172E	File Transfer behind schedule (25% dMin)
6	SLC	CSLC173I	File Transfer ahead of schedule (50% dMin)
6	SLC	CSLC174E	File Transfer behind schedule (50% dMin)
6	SLC	CSLC175I	File Transfer ahead of schedule (75% dMin)

Event Type	Event Name	Message ID	Message Text
6	SLC	CSLC176E	File Transfer behind schedule (75% dMin)
6	SLC	CSLC177I	File Transfer ahead of schedule (25% dMax)
6	SLC	CSLC178E	File Transfer behind schedule (25% dMax)
6	SLC	CSLC179I	File Transfer ahead of schedule (50% dMax)
6	SLC	CSLC180E	File Transfer behind schedule (50% dMax)
6	SLC	CSLC181I	File Transfer ahead of schedule (75% dMax)
6	SLC	CSLC182E	File Transfer behind schedule (75% dMax)
	SLC Group Messages		
12	Server Command	CSLC080I	SLC group created
12	Server Command	CSLC081I	SLC group updated
12	Server Command	CSLC082I	SLC group deleted
12	Server Command	CSLC086I	SLC wildcard group created
12	Server Command	CSLC087I	SLC wildcard group updated
12	Server Command	CSLC088I	SLC wildcard group deleted
12	Server Command	CSLC089I	SLC wildcard group order change
12	Server Command	CSLC220I	New SLC Workflow Group Created, *ID*, by *UserID*.
12	Server Command	CSLC221I	SLC Workflow Group Updated, *ID*, by *UserID*.
12	Server Command	CSLC222I	SLC Workflow Group Deleted, *ID*, by *UserID*.
	SLC Schedule Messages		
12	Server Command	CSLC083I	SLC schedule created
12	Server Command	CSLC084I	SLC schedule updated
12	Server Command	CSLC085I	SLC schedule deleted
	SLC Calendar Messages		
12	Server Command	CSLC112I	Calendar created
12	Server Command	CSLC113I	Calendar updated
12	Server Command	CSLC114I	Calendar deleted
	SLC Message List Messages		
12	Server Command	CSLC223I	New MessageList Created, *ID*, by *UserID*.
12	Server Command	CSLC224I	MessageList Updated, *ID*, by *UserID*.

Event Type	Event Name	Message ID	Message Text
12	Server Command	CSLC225I	MessageList Deleted, *ID*, by *UserID*.
	SLC Workflow Messages		
6	SLC	CSLC228E	*Workflow/Milestone/Step/Process* did not start before the end of the monitoring window. SLC: *SLCID*
6	SLC	CSLC229I	*Workflow/Milestone/Step/Process* on time completion for SLC *SLCID* may be in jeopardy. Reason: *ReasonID*.

Message IDs Specific to Connect:Enterprise

The following table lists Sterling Control Center message IDs specific to Connect:Enterprise servers.

Event Type	Event Name	Message ID	Message Text
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE001I	AutoConnect (AC) SEND Operation Performed. (Connect:Enterprise z/OS only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE002I	AutoConnect (AC) RECV Operation Performed. (Connect:Enterprise z/OS only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE003I	RemoteConnect (RC) ADD Operation Performed.
13	Connection Started	CNCE009I	RemoteConnect (RC) CONNECT Operation Performed.
12	Server Command	CNCE007I	RemoteConnect (RC) DEL Operation Performed.
12	Server Command	CNCE006I	RemoteConnect (RC) DIR Operation Performed.
14	Connection Shutdown Started	CNCE010I	RemoteConnect (RC) DISCON Operation Performed.

Event Type	Event Name	Message ID	Message Text
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE005I	RemoteConnect (RC) REQ Operation Performed.
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE011I	Offline (OFF) EXT Operation Performed. (Connect:Enterprise UNIX only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE012I	Offline (OFF) ADD Operation Performed. (Connect:Enterprise UNIX only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE013I	AutoConnect (AC) Collect (C) Operation Performed. (Connect:Enterprise UNIX only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE014I	AutoConnect (AC) Transmit (T) Operation Performed. (Connect:Enterprise UNIX only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE015I	Offline (OFF) ERA Operation Performed. (Connect:Enterprise UNIX only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE016I	Offline (OFF) STA Operation Performed. (Connect:Enterprise UNIX only)
13	Connection Started	CNCE113I	AutoConnect (AC) Failure. (Connect:Enterprise UNIX only)
5	Server Status	CNCE114I	C:E Daemon is running. ID: *DaemonID*
5	Server Status	CNCE115I	C:E Daemon is down. ID: *DaemonID*
5	Server Status	CNCE116I	C:E Daemon added/removed/changed. ID: *DaemonID*
13	Connection Started	CNCE209I	AutoConnect (AC) CONNECT Operation Performed. (Connect:Enterprise z/OS only)
14	Connection Shutdown Started	CNCE210I	AutoConnect (AC) DISCON Operation Performed. (Connect:Enterprise z/OS only)

Message IDs Specific to Sterling Integrator

The following table lists Sterling Control Center message IDs specific to Sterling Integrator servers.

Event Type	Event Name	Message ID	Message Text
5	Server Status	CGIS010I	Sterling Integrator Adapter is enabled. ID: {0}
5	Server Status	CGIS011I	Sterling Integrator Adapter has stopped. ID: {0}
5	Server Status	CGIS012I	Sterling Integrator Adapter added/removed.
5	Server Status	CGIS013I	Sterling Integrator Node status is down. Node: {0}
5	Server Status	CGIS014I	Sterling Integrator Node status is up. Node: {0}
5	Server Status	CGIS015I	Sterling Integrator Node removed. Node: {0}
12	Server Command	CGIS016I	Process Name: *Name* cleared from Process Queue by User: *UserID*
5	Server Status	CGIS018I	Sterling Integrator Node added. Node: {0}
5	Server Status	CGIS031I	Sterling Integrator Perimeter server has been enabled. Name: {0}
5	Server Status	CGIS032I	Sterling Integrator Perimeter Server has been disabled : Name : {0}
5	Server Status	CGIS033I	Sterling Integrator Perimeter Server connected : Name : {0}
5	Server Status	CGIS034I	Sterling Integrator Perimeter Server disconnected : Name : {0}
5	Server Status	CGIS035I	Sterling Integrator Perimeter Server added/removed.

Message IDs (Event Codes) Specific to Sterling File Gateway

Sterling File Gateway "event codes" are mapped to Control Center event message IDs. To look up a particular event code, see the Sterling File Gateway documentation.

Message IDs Specific to Configuration Management

The following table lists Sterling Control Center message IDs specific to configuration management.

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG021I	Operation beginning Netmap node create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG022I	Operation beginning Netmap mode create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG023I	Operation beginning Netmap commpath create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG024I	Operation beginning Initparms create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG025I	Operation beginning Translation table create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG026I	Operation beginning Proxy create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG027I	Operation beginning User auth create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG028I	Operation beginning Secure+ node create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG029I	Operation beginning Secure+ Key Certificate create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG030I	Operation beginning Secure+ Trusted Certificate create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG031I	Operation beginning Netmap node delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG032I	Operation beginning Netmap mode delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG033I	Operation beginning Netmap commpath delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG034I	Operation beginning Initparms delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG035I	Operation beginning Translation table delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG036I	Operation beginning Proxy delete. User ID: {0} Server ID: {1} Job ID: {2}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG037I	Operation beginning User auth delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG038I	Operation beginning Secure+ node delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG039I	Operation beginning Secure+ Key Certificate delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG040I	Operation beginning Secure+ Trusted Certificate delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG041I	Operation beginning Netmap node refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG042I	Operation beginning Netmap mode refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG043I	Operation beginning Netmap commpath refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG044I	Operation beginning Initparms refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG045I	Operation beginning Translation table refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG046I	Operation beginning Proxy refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG047I	Operation beginning User auth refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG048I	Operation beginning Secure+ node refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG049I	Operation beginning Secure+ Key Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG050I	Operation beginning Secure+ Trusted Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG051I	Operation beginning Netmap node update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG052I	Operation beginning Netmap mode update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG053I	Operation beginning Netmap commpath update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG054I	Operation beginning Initparms update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG055I	Operation beginning Translation table update. User ID: {0} Server ID: {1} Job ID: {2}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG056I	Operation beginning Proxy update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG057I	Operation beginning User auth update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG058I	Operation beginning Secure+ node update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG059I	Operation beginning Secure+ Key Certificate update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG060I	Operation beginning Secure+ Trusted Certificate update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG071I	Operation successful Netmap node create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG072I	Operation successful Netmap mode create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG073I	Operation successful Netmap commpath create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG074I	Operation successful Initparms create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG075I	Operation successful Translation table create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG076I	Operation successful Proxy create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG077I	Operation successful User auth create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG078I	Operation successful Secure+ node create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG079I	Operation successful Secure+ Key Certificate create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG080I	Operation successful Secure+ Trusted Certificate create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG081I	Operation successful Netmap node delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG082I	Operation successful Netmap mode delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG083I	Operation successful Netmap commpath delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG084I	Operation successful Initparms delete. User ID: {0} Server ID: {1} Job ID: {2}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG085I	Operation successful Translation table delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG086I	Operation successful Proxy delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG087I	Operation successful User auth delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG088I	Operation successful Secure+ node delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG089I	Operation successful Secure+ Key Certificate delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG090I	Operation successful Secure+ Trusted Certificate delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG091I	Operation successful Netmap node refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG092I	Operation successful Netmap mode refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG093I	Operation successful Netmap commpath refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG094I	Operation successful Initparms refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG095I	Operation successful Translation table refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG096I	Operation successful Proxy refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG097I	Operation successful User auth refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG098I	Operation successful Secure+ node refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG099I	Operation successful Secure+ Key Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG100I	Operation successful Secure+ Trusted Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG101I	Operation successful Netmap node update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG102I	Operation successful Netmap mode update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG103I	Operation successful Netmap commpath update. User ID: {0} Server ID: {1} Job ID: {2}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG104I	Operation successful Initparms update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG105I	Operation successful Translation table update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG106I	Operation successful Proxy update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG107I	Operation successful User auth update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG108I	Operation successful Secure+ node update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG109I	Operation successful Secure+ Key Certificate update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG110I	Operation successful Secure+ Trusted Certificate update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG111E	Operation failed Netmap node create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG112E	Operation failed Netmap mode create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG113E	Operation failed Netmap commpath create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG114E	Operation failed Initparms create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG115E	Operation failed Translation table create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG116E	Operation failed Proxy create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG117E	Operation failed User auth create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG118E	Operation failed Secure+ node create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG119E	Operation failed Secure+ Key Certificate create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG120E	Operation failed Secure+ Trusted Certificate create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG121E	Operation failed Netmap node delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG122E	Operation failed Netmap mode delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG123E	Operation failed Netmap commpath delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG124E	Operation failed Initparms delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG125E	Operation failed Translation table delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG126E	Operation failed Proxy delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG127E	Operation failed User auth delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG128E	Operation failed Secure+ node delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG129E	Operation failed Secure+ Key Certificate delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG130E	Operation failed Secure+ Trusted Certificate delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG131E	Operation failed Netmap node refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG132E	Operation failed Netmap mode refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG133E	Operation failed Netmap commpath refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG134E	Operation failed Initparms refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG135E	Operation failed Translation table refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG136E	Operation failed Proxy refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG137E	Operation failed User auth refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG138E	Operation failed Secure+ node refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG139E	Operation failed Secure+ Key Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CFG140E	Operation failed Secure+ Trusted Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG141E	Operation failed Netmap node update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG142E	Operation failed Netmap mode update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG143E	Operation failed Netmap commpath update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG144E	Operation failed Initparms update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG145E	Operation failed Translation table update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG146E	Operation failed Proxy update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG147E	Operation failed User auth update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG148E	Operation failed Secure+ node update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG149E	Operation failed Secure+ Key Certificate update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG150E	Operation failed Secure+ Trusted Certificate update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG151E	Operation failed. Job ID: {0} UserID: {1} Server ID: {2} Operation: {3} Object type: {4} Reason: {5}
12	Server Command	CCFG152E	Configuration Job completed. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Return Code: {4} Error: {5}
12	Server Command	CCFG158E	Scheduled Configuration Job canceled by System at startup. Job should have already run. Job ID: {0} Operation: {1} Object type: {2}
12	Server Command	CCFG159E	Configuration Job canceled by System at startup. Job had been canceled or was running previously. Job ID: {0} Operation: {1} Object type: {2}
12	Server Command	CCFG160E	Cancel Configuration Job failed, nothing to cancel. User: {0} Job ID: {1}
12	Server Command	CCFG161I	Configuration Job submitted. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Status: {4}
12	Server Command	CCFG162I	Configuration Job held. Job ID: {0} User ID: {1} Operation: {2} Object type: {3}
12	Server Command	CCFG163I	Configuration Job canceled. Job ID: {0} User ID: {1} Operation: {2} Object type: {3}
12	Server Command	CCFG164I	Configuration Job completed. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Return Code: {4}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG165I	Configuration Job starting. Job ID: {0} User ID: {1} Operation: {2} Object type: {3}
12	Server Command	CCFG166I	Cancel Configuration Job initiated. User: {0} Job ID: {1}
12	Server Command	CCFG167I	Configuration Job updated. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Status: {4}
12	Server Command	CCFG168I	Configuration Job released. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Status: {4}
12	Server Command	CCFG169I	Configuration Job restarted. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Status: {4}
12	Server Command	CCFG184I	Template created. User ID: {0} ID: {1} Type: {2}
12	Server Command	CCFG185I	Template updated. User ID: {0} ID: {1} Type: {2}
12	Server Command	CCFG186I	Template deleted. User ID: {0} ID: {1} Type: {2}
12	Server Command	CCFG188I	Versions of all objects associated with server being deleted by System. Server: {0}
12	Server Command	CCFG189I	Version being deleted. User ID: {0} Version ID: {1} Server: {2} Object type: {3}
12	Server Command	CCFG191I	New Netmap node version created. Server ID: {0}
12	Server Command	CCFG192I	New Netmap mode version created. Server ID: {0}
12	Server Command	CCFG193I	New Netmap commpath version created. Server ID: {0}
12	Server Command	CCFG194I	New Initparms version created. Server ID: {0}
12	Server Command	CCFG195I	New Translation table version created. Server ID: {0}
12	Server Command	CCFG196I	New Proxy version created. Server ID: {0}
12	Server Command	CCFG197I	New User auth version created. Server ID: {0}
12	Server Command	CCFG198I	New Secure+ Node version created. Server ID: {0}
12	Server Command	CCFG199I	New Secure+ Key Certificates version created. Server ID: {0}
12	Server Command	CCFG200I	New Secure+ Trusted Certificates version created. Server ID: {0}
12	Server Command	CCFG208E	Operation failed Secure+ cipher suite refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG209I	Operation beginning Secure+ cipher suite refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG210I	Operation successful Secure+ cipher suite refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG211E	Operation failed Secure+ alias create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG212E	Operation failed Secure+ alias delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG213E	Operation failed Secure+ alias refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG214E	Operation failed Secure+ rekey parm file. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG215E	Operation failed Secure+ synch parm file. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG216E	Operation failed Secure+ validate parm file. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG221I	New Secure+ Cipher Suites version created. Server ID: {0}
12	Server Command	CCFG222I	Operation beginning Secure+ alias create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG222I	Operation beginning Secure+ alias create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG223I	Operation beginning Secure+ alias delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG224I	Operation beginning Secure+ alias refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG225I	Operation successful Secure+ alias create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG226I	Operation successful Secure+ alias delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG227I	Operation successful Secure+ alias refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG228I	New Secure+ aliases version created. Server ID: {0}
5	Server Status	CCFG229I	Trusted Certificate Expiry notification. Server ID: {0} Certificate: {1} Expires: {2} Days left: {3}
5	Server Status	CCFG230I	Key Certificate Expiry notification. Server ID: {0} Certificate: {1} Expires: {2} Days left: {3}
12	Server Command	CCFG232I	Operation beginning Secure+ rekey parm file. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG233I	Operation beginning Secure+ synch parm file. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG234I	Operation beginning Secure+ validate parm file. User ID: {0} Server ID: {1} Job ID: {2}

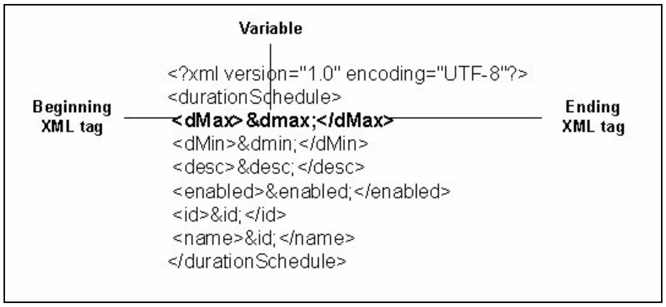
Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG235I	Operation successful Secure+ rekey parm file. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG236I	Operation successful Secure+ synch parm file. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG237I	Operation successful Secure+ validate parm file. User ID: {0} Server ID: {1} Job ID: {2} Response: {3}
12	Server Command	CCFG241I	Operation beginning Copy parameters. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG242I	Operation successful Copy parameters. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG248E	Operation failed Copy parameters. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG250E	User ID: {0} not permitted to manage {1}

Appendix E

Create Multiple Objects

Sterling Control Center provides a program, sample script, and sample templates to create multiple Control Center objects, such as actions, rules, schedules, e-mail addresses, and SLCs, without manually entering each one through the console or using the duplicate function. You can use the same program to add or update server definitions. The templates are located in the *ControlCenterInstallDir*\conf\templates folder. The sample script (script.txt) is in the ..\conf directory.

Each template is a text file containing a list of XML tags and variables corresponding to dialog field names. Each variable uses the format &*name;* where *name* is the variable name. Each variable name ends with a semicolon. The following illustration shows the duration template:



```
<?xml version="1.0" encoding="UTF-8"?>
<durationSchedule>
 <dMax>&dmax;</dMax>
 <dMin>&dmin;</dMin>
 <desc>&desc;</desc>
 <enabled>&enabled;</enabled>
 <id>&id;</id>
 <name>&id;</name>
</durationSchedule>
```

This appendix contains the following information:

- Create Multiple Objects Using the Sample Script
- Template Contents
- Create Your Own Templates

To run the procedures in this appendix, you should be familiar with editing XML tags and running batch scripts.

The *Sterling Control Center How-To Guide* contains the following examples using multiple objects:

- How Can I Use RUNBATCH To Create Schedules for an Hourly Process?
- How Can I Do a Bulk Update of the Passwords Used by Control Center for Monitored Servers?

Be sure to review the information in this appendix before attempting to implement those examples in your system to understand how templates and scripts are used with the RUNBATCH program to create and update multiple objects.

Create Multiple Objects Using the Sample Script

To create multiple objects using the sample script:

1. Use a text editor such as WordPad to open the provided sample script file. The sample script is illustrated below.

```
# Sample script to build SLCs, schedules, rules, actions, servers, etc. quickly.
#
# To build your own templates, do the following:
#
# Use Control Center GUI to build the SLC Group, SLC WC Group, schedule, time-schedule, rule,
action, server,
# etc., like you want it.
#
# Copy the new rule, etc, into the conf/templates subdirectory and change the extension to
.tmp from .xml
#
# SLC Groups are found in conf/slcs/groups and conf/slcs/groups/visibilityGroups
# SLC Schedules are found in conf/slcs/schedules
# Rules are found in conf/rules and conf/rules/visibilityGroups
# Actions are found in conf/actions
# Servers are found on conf/services/nodes
# Metadata rules are found on conf/metadataRules
# Metadata actions are found on conf/metadataActions
# Rule and Metadata rule schedules are found on conf/ruleSchedules
# Data Visibility Groups are found on conf/dataVisibilityGroups
# Calendars are found on conf/calendars
# Roles are found on conf/roles
# Users are found on conf/users
# Message Lists are found on conf/slcs/messageLists
#
# Edit the template and substitute variable names where appropriate.  Be sure to end each
variable name with
# a semicolon (eg.  &name;).
#
# Write a script (such as this one) to copy your template and substitute the appropriate
variables (see script
# below for examples).
#
# The last statement for each section indicates what kind of SLC group, rule, etc, you are
adding to Control Center:
#
# SLCGROUP             - SLC Group
# SLCWCGROUP           - Wildcard SLC Group
# SLCWFGROUP           - Workflow SLC Group
# SLCSCHEDULE          - SLC Time Schedule
# RULE                 - Control Center Rule
# RULESCHEDULE         - Control Center Rule/Metadata Rule Schedule
# REPORTSCHEDULE       - Control Center Report Schedule
# CALENDAR             - Control Center Calendar
# AUTOMATEDREPORTGROUP - Control Center Automated Report Group
# EMAILLIST            - Control Center EMail List
# ACTION               - Control Center Action
# SERVER               - Create a new Server/Node definition
# SERVERGROUP          - Create a new Server/Node definition
# METADATARULE         - Create a new Metadata Rule
# METADATAACTION       - Create a new Metadata Rule Action
-- continued --
```

```
Sample Script --continued--

# DVG                  - Control Center Data Visibility Group
# ROLE                 - Control Center Role
# USER                 - Control Center User
# MESSAGELIST          - Control Center Data Message List
#
# Note If the last statement for each section has the text "UPDATE" appended to it, e.g.
RULEUPDATE or ACTIONUPDATE, then
# instead of creating a Control Center object, the object is assumed to exist and an update
will be attempted.
#
# Note Server updates are typically performed for batch password changes.
#
# Then run the "runBatch.bat" or "runBatch.sh" from the bin directory:
#
# runBatch <ccenter ip address> <ccenter port> <ccenter userid> <ccenter userid password>
<scriptname> [DELETE]
#
# eg.  runBatch 127.0.0.1 58080 admin admin ../conf/script.txt
#
# If any errors are produced when running the script, you should run it again specifying the
delete option
# to delete all successfully defined objects before correcting the script and starting over
again:
#
# eg.  runBatch 127.0.0.1 58080 admin admin ../conf/script.txt delete
#
#
# Note:  Actions cannot be deleted if referenced by a rule (the rules must be deleted first).
#       Schedules cannot be deleted if referenced by an SLC Group (the group must be deleted
first).
#        But, when adding a rule, the action must already be defined.  And when adding a
group, the
#        the schedule must already be defined.
#
#        For this reason, it is recommended that separate scripts be written for groups and
schedules,
#        and for rules and actions.
#
copy slc_regex
&id;           = WCSLC_7
&desc;         = description
&enabled;      = true

&filenameregex; = true
&filename;     = ^dest.*

&noderegex;    = false
&node;         = SERVER*

&processregex; = true
&process;      = ^PROCESS$

&remotenoderegex; = false
&remotenode;   = SERVER
&schedule;     = schedule

&submitterregex; = false
&submitter;    =
--continued--
```

```
Sample Script --continued--

&servergroup;  = ServerGroup
&node;         = Node1
&missingevent;  = true
&monitortolerance; = 6
SLCWCGROUP
#

copy slc_group
&id;           = WCSLC_6
&enabled;      = true
&desc;         = description
&filename;     = dest
&node;         = SERVER
&process;      = PROCESS
&remotenode;   = SERVER
&schedule;     = schedule
&submitter;    = submitter
&duplicatefilenames; = false
&duplicateprocesses; = false
&missingevent; = true
&monitortolerance; = 6
&servergroup;  = ServerGroup
SLCGROUP
#

copy duration
&id;           = duration_schedule
&enabled;      = true
&dmax;         = 0:30
&dmin;         = 0:25
&desc;         = description
SLCSCHEDULE
#

copy email
&desc;         = description
&email;        = name@address
&id;           = email_action
ACTION
#

copy opSys
&desc;         = description
&id;           = opsys_action
&operation;    = c:\\doit.bat
ACTION
#

copy rule
&id;           = sample_rule
&desc;         = description
&enabled;      = true
&messageid;        = MSGID01I
&actionid;     = alert0
&eventtype;    = 6
RULE
#
```

Each section in a script corresponds to one object (such as one SLC duration schedule) and contains the following information:

- A copy command that specifies the template name to be copied (**duration** in the example).
- The variables and values you want to substitute. See *Template Contents* on page 222 for a list of variable fields. You should provide values for all fields.
- A final statement that defines the object you are adding to Sterling Control Center (DURATION in the example).

Note: As stated in the sample script, if the last statement for each section has the text "UPDATE" appended to it, e.g. RULEUPDATE or ACTIONUPDATE, then instead of creating a Control Center object, the object is assumed to exist and an update is attempted.

The following table lists the final statements you can use:

Statement	Object
ACTION	Control Center action
AUTOMATEDREPORTGROUP	Control Center automated report group
CALENDAR	Control Center calendar
DVG	Control Center Data Visibility Group
EMAILLIST	Control Center email list
MESSAGELIST	Control Center data message list
METADATAACTION	Control Center metadata action
METADATARULE	Control Center metadata rule
REPORTSCHEDULE	Control Center rule/metadata rule schedule
ROLE	Control Center role
RULE	Control Center rule
RULESCHEDULE	Control Center rule schedule
SERVER	Create a new server/node definition
SERVERGROUP	Create a new server/node definition
SLCGROUP	Control Center SLC group
SLCSCHEDULE	Control Center SLC schedule
SLCWCGROUP	Control Center wildcard SLC group
SLCWFGROUP	Control Center workflow SLC group
USER	Control Center user

Note: Each script should create multiples of only one type of object. For example, create one script to create multiple standard SLCs, one script to create multiple wildcard SLCs, and one script to create multiple rules.

2. Name and save the file.
3. When the Control Center engine is running and has completed initialization, open a command window and change your working directory to ControlCenter\bin.
4. Type **runBatch** *hostname port userid password scriptname* (Windows) or **runBatch.sh** *hostname port userid password scriptname* (UNIX). The following table shows the parameter values:

Tag	Description
hostname	The IP address or DNS host name where Sterling Control Center is installed.
port	The HTTP port number that the Sterling Control Center engine monitors.
userid	The user name to access the Sterling Control Center. This value is case sensitive.
password	The password to access the Sterling Control Center. This value is case sensitive.
scriptname	The path and name of the script created in step 1.

For example, in Windows, type:

```
runBatch 127.0.0.1 58080 admin admin ..\conf\slcscript.txt
```

In UNIX, type:

```
runBatch.sh 127.0.0.1 58080 admin admin ../conf/slcscript.txt
```

The script executes and creates the objects.

5. If any script errors occur:
   a. Type **runBatch** *hostname port userid password scriptname* **delete** (Windows) or **runBatch.sh** *hostname port userid password scriptname* **delete** (UNIX) to delete all defined objects.
   b. Review the template and scripts to determine where the error occurred.
   c. Make the necessary corrections and issue the **runBatch** command again.

Template Contents

This section describes the following Sterling Control Center templates:

- Duration Schedule Template
- E-mail Template
- Operating System Commands Template
- Rules Template

- Calendar Schedule Template
- Standard SLC Groups Template
- Wildcard SLC Groups Template

Duration Schedule Template

The duration.tmp file is used for SLC duration schedules. It contains the following fields:

Tag	Description
<dMax>&dmax;</dMax>	Maximum duration
<dMin>&dmin;</dMin>	Minimum duration
<desc>&desc;</desc>	Schedule description
<enabled>&enabled;</enabled>	Enabled (true or false)
<id>&id;</id>	Schedule Name
<name>&id;</name>	Schedule Name

E-mail Template

The email.tmp file is used for e-mail address in actions. It contains the following fields:

Tag	Description
<desc>&desc;</desc>	Action description
<email>&email;</email>	E-mail address
<id>&id;</id	Action name

Note: The final statement for the e-mail template must be ACTION.

Operating System Commands Template

The opSys.tmp file is used for operating system commands in actions. It contains the following fields:

Tag	Description
<desc>&desc;</desc>	Action description
<id>&id;</id>	Action name

Tag	Description
<operation>&operation;</operation>	Operating system command

Note: The final statement for the operating system command template must be ACTION.

Rules Template

The rule.tmp file is used for creating rules. It contains the following fields:

Tag	Description
<actionId>&actionid;</actionId>	Action name associated with the rule
<desc>&desc;</desc>	Rule description
<enabled>&enabled;</enabled>	Enabled (true or false)
<eventType>&eventtype;</eventType>	The event type that generates the rules.
<id>&id;</id>	Rule name
<match>&quot;/event[eventType = &apos;&eventtype;&apos; and messageId = &apos;&messageid;&apos;]&quot;</match>	The event type and message ID to match. ◆ &eventtype; is the event type code ◆ &messageID; is the message ID

Calendar Schedule Template

The schedule.tmp file is used for creating calendar schedules. It contains the following fields:

Tag	Description
<calendarId>&calendar;</calendarId>	Calendar name associated with the schedule
<desc>&desc;</desc>	Schedule description
<enabled>&enabled;</enabled>	Enabled (true or false)
<id>&id;</id>	Schedule ID
<name>&id;</name>	Schedule ID
<day>&day;</day>	Normal End Range day. 0 = NSR start day, 1 = NSR start day + 1, and so on.
<end>&nerend;</end>	Normal End Range end time. Format hh:mm:ss.
<start>&nerstart;</start>	Normal End Range start time. Format hh:mm:ss.

Tag	Description
<end>&nsrend;</end>	Normal Start Range end time. Format hh:mm:ss.
<start>&nsrstart;</start>	Normal Start Range start time. Format hh:mm:ss.
<timeZone>&timezone;</timeZone>	The time zone.

Standard SLC Groups Template

The slc_group.tmp file is used for creating standard SLC groups. It contains the following fields:

Tag	Description
<desc>&desc;</desc>	Schedule description
<duplicateFileNames>&duplicatefilenames; </duplicateFileNames>	Allow duplicate file names (true or false)
<duplicateProcesses>&duplicateprocesses; </duplicateProcesses>	Allow duplicate Process names or Batch IDs (true or false)
<enabled>&enabled;</enabled>	Enabled (true or false)
<fileName>&filename;</fileName>	File Name
<id>&id;</id>	SLC ID
<missingEvent>&missingevent; </missingEvent>	Generate notification if event has not occurred (true or false)
<monitorTolerance>&monitortolerance; </monitorTolerance>	The monitor tolerance windows in hours
<name>&id;</name>	SLC ID
<node>&node;</node>	The servers selected for the SLC
<process>&process;</process>	The Process name. or Batch ID
<remoteNode>&remotenode; </remoteNode>	The remote node name
<schedule>&schedule;</schedule>	The associated schedule
<serverGroup>&servergroup; </serverGroup>	The server groups selected for the SLC
<submitter>&submitter;</submitter>	The submitter ID

Wildcard SLC Groups Template

The slc_regex.tmp file is used for creating wildcard SLC groups. It contains the following fields:

Tag	Description
<desc>&desc;</desc>	Schedule description
<enabled>&enabled;</enabled>	Enabled (true or false)
<fileName>&filename;</fileName>	The file name expression
<fileNameRegex>&filenameregex; </fileNameRegex>	Matches the file name using a Regex expression (true or false)
<id>&id;</id>	SLC ID
<missingEvent>&missingevent; </missingEvent>	Generate notification if event has not occurred (true or false)
<monitorTolerance>&monitortolerance; </monitorTolerance>	The monitor tolerance windows in hours
<name>&id;</name>	SLC ID
<node>&node;</node>	The servers expression
<nodeRegex>&noderegex;</nodeRegex>	Matches the servers using a Regex expression (true or false)
<process>&process;</process>	The Process name or Batch ID expression
<processRegex>&processregex; </processRegex>	Matches the Process name or Batch ID using a Regex expression (true or false)
<remoteNode>&remotenode; </remoteNode>	The remote node name expression
<remoteNodeRegex>&remotenoderegex; </remoteNodeRegex>	Matches the remote node name using a Regex expression (true or false)
<schedule>&schedule;</schedule>	The associated schedule
<serverGroup>&servergroup; </serverGroup>	The server groups selected for the SLC
<submitter>&submitter;</submitter>	The submitter ID expression
<submitterRegex>&submitterregex; </submitterRegex>	Matches the submitter ID using a Regex expression (true or false)

Create Your Own Templates

You can create your own templates using the Sterling Control Center console.

Note: No template is provided to create servers or workflow SLCs in batch. You must create your own template for these.

To use the Sterling Control Center console to create your own templates:

1. Create an object of the type for which you want to create a template using the Sterling Control Center console. Sterling Control Center creates an .xml file for the object in the ControlCenter\conf\objecttype directory. For example, rule .xml files are located in the ControlCenter\conf\rules directory.
2. Copy the .xml file for the object to the ControlCenter\conf\templates directory.
3. Rename the .xml file in the ControlCenter\conf\templates directory as a .tmp file.
4. Open the .tmp file with a text editor such as WordPad.
5. Replace the values between the XML tags with variables. The following is an example of a roles template before and after editing:

Before Editing	**After Editing**
<role>	<role>
<id>superuser</id>	<id>&role;</id>
<ver>1</ver>	<ver>1</ver>
<desc>Administrator role definition</desc>	<desc>&desc;</desc>
<!-- auths -->	<!-- auths -->
<rules>manage</rules>	<rules>&rulespermiss;</rules>
<actions>manage</actions>	<actions>&actionpermiss;</actions>
<alerts>manage</alerts>	<alerts>&alertpermiss;</alerts>
<processes>manage</processes>	<processes>&procpermiss;</processes>
<users>manage</users>	<users>&userpermiss;</users>
<roles>manage</roles>	<roles>&rolespermiss;</roles>
<servers>manage</servers>	<servers>&serverpermiss;</servers>
<slcs>manage</slcs>	<slcs>&SLCpermiss;</slcs>
<systemSettings>manage</systemSettings>	<systemSettings>&syspermiss;</systemSettings>
<reports>manage</reports>	<reports>&reportpermiss;</reports>
</role>	</role>

6. Save the .tmp file.
7. Continue with step 1 of *Create Multiple Objects Using the Sample Script* on page 218 to build and run a script file.

Appendix F

Regular Expressions

Regular expressions (or regex) can be used in wildcard SLCs and other Sterling Control Center entities to match text or numeric strings that follow a particular pattern. They consist of normal characters and special characters. Normal characters are upper- and lowercase letters and numbers. Special characters have specific meanings in the expression.

For example, the regular expression ABCDEF contains only normal characters. When used as a match criterion, it will match only ABCDEF text strings. The regular expression [ABCDEF] contains normal characters and special characters (the brackets). It will match any text string that includes A, B, C, D, E, or F.

Regular expressions can be very complex. This chapter describes basic expression characters and some simple examples for Sterling Control Center. If you want to learn more about regular expressions, an Internet search on the terms “regular expression” or “regex” will provide many sites that explain regular expressions in greater detail.

The following table lists some common regular expression special characters and examples. Multiple special characters can be used in the same expression to create more criteria.

Note: Note that regular expression patterns are case sensitive. Case sensitivity can be controlled within a pattern using the inline modifier (?i).

Special Character	Description	Examples
[ ]	Matches any character between the brackets. Ranges are specified by a hyphen ([a-z], [0-9]).	Proc4[123] matches the strings Proc41, Proc42, and Proc43. Proc4[a-e]7 matches the strings Proc4a7, Proc4b7, Proc4c7, Proc4d7, and Proc4e7.
[^]	Matches any character not appearing between the brackets. Ranges are specified by a hyphen ([a-z], [0-9]).	Proc4[^789] matches all strings that contain Proc4, except for strings containing Proc47, Proc48, or Proc49.
. (period)	Matches any single character.	Proc4.567 matches the strings Proc41567, Proc42567, Proc4a567, and so on. It does not match Proc412567.

Special Character	Description	Examples
+ (plus)	Matches strings containing one or more occurrences of the character immediately preceding the plus sign.	Proc456+ matches Proc456, Proc4566, Proc45666 and so on.
* (asterisk)	Matches strings containing zero or more occurrences of the character preceding the asterisk. The search treats the character preceding the asterisk as optional.	Proc456* matches Proc45, Proc456, Proc4566, Proc45666 and so on.
?	Matches strings containing zero or one occurrence of the character immediately preceding the question mark. The character preceding the question mark is treated as optional by the search.	Proc456? matches Proc45 and Proc456. Proc4[5-8]? matches Proc4, Proc45, Proc46, Proc47, and Proc48.
| (pipe)	Matches the characters on either side of the pipe.	Proc456|Proc459|Proc460 matches Proc456, Proc459, or Proc460.
\	Escape character that converts a special character to a normal character.	Node\.Atlanta matches Node.Atlanta.
(?i)	Used to control case sensitivity. This inline modifier affects all characters to the right and in the same enclosing group. Affected characters are allowed to be case insensitive.	In the pattern w (x (?i) y) z, only the letter *y* is allowed to be case insensitive.

Appendix G

Sterling Control Center Variables

The following table lists Control Center event elements you can use as variables in operating system and server command actions, e-mail actions, metadata actions, and workflow SLC correlators along with a brief description of each element.

The event elements are listed in alphabetical order. For each variable, the relevant server types are indicated by an x in one or more of the following columns:

- CD (Connect:Direct)
- CE (Connect:Enterprise)
- SI (Sterling Integrator, including Sterling File Gateway)
- FTP (FTP servers of all types)
- SCC (Sterling Control Center)

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
action					x	Action performed on Control Center entity.
actionId					x	Name of an action called by a rule.
activityType					x	A code indicating the type of SLC activity an SLC event is associated with. ◆ WF=Workflow ◆ M=Milestone ◆ S=Process Step ◆ P=Process
alert					x	Alert level/severity.
applAgentType		x				Application Agent type
batchId		x				Batch ID
batchNumber		x				Batch number

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
bytesRead	x	x	x			Number of bytes read from the source file.
bytesSent	x	x	x			Number of bytes sent to the destination file.
bytesXferred	x					Number of bytes received by the destination file.
CBEA	x					Control Block Encryption Algorithm
CERI	x					Certificate Issuer
CERT	x					Certificate Subject
CKPT	x					Check Point
CLAS	x					Class
CNOD	x					CT Node
controlCenterName					x	Sterling Control Center name
CPUS	x					CPU Time (milliseconds)
CSPE	x					Secure Enabled
CSPP	x					Secure Protocol
CSPS	x					Secure Cipher Suite
CSTN	x					Current Signature Verified
daemonHost		x				DNS host name or IP address of the system the Connect:Enterprise daemon is on.
daemonName		x				Name of the Connect:Enterprise daemon.
daemonOriginator		x				Originator of the Connect:Enterprise daemon.
daemonPid		x				Process identifier of the Connect:Enterprise daemon.
daemonResource		x				Resource of the Connect:Enterprise daemon.
daemonSid		x				Session identifier of the Connect:Enterprise daemon.
daemonState		x				State of the Connect:Enterprise daemon.
daemonType		x				Type of the Connect:Enterprise daemon. Control Center monitors only daemons of type master.

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
dateTime	x	x	x	x	x	The date and time that the event was generated.
daysBeforeExpiry	x					An integer value that tells the number of days before certificate expiration.
DBUG	x					Debug
DBYW	x					Bytes Written
DBYX	x					Bytes Received
DDS1	x					Destination Disposition 1
DDS2	x					Destination Disposition 2
DDS3	x					Destination Disposition 3
destFile	x	x	x	x	x	Destination file name. For Connect:Direct, the file name at the destination in a copy step of a Process.
direction	x		x	x		Indicates direction of file transmissions. ◆ inBound ◆ outBound
DRCW	x					Records written
DRUX	x					RUs received
ECMP	x					Extended compression
EPRT	x					Execution Priority
eventId	x	x	x	x	x	The ID number assigned by the system to each event.
eventType	x	x	x	x	x	A code indicating the type of event. See Event Type Descriptions for a listing of event types and descriptions.
eventTypeDescr	x	x	x	x	x	A description for the event type.
executingProcs	x		x			Number of Processes in execution state.
FDBK	x					Feedback
FG.CONS_ORG_KEY			x			File Gateway Consumer Org Key
FG.DATA_FLOW_ID			x			File Gateway Data Flow ID
FG.EVENT_CODE			x			File Gateway Event Code.
FG.FILE_NAME			x			File Gateway Arrived File Name.

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
FG.PROD_ORG_KEY			x			File Gateway Arrived File Producer Org Key
FG.STATE			x			File Gateway Arrived File State
fgActivityType			x			File Gateway activity type ◆ D=Delivery ◆ R=Route ◆ A=Arrived File
fileSize	x	x	x	x		The size of the file transferred
fromNode	x		x	x		The node that sent the file: ◆ P=Pnode ◆ S=Snode Indicates which server, local or remote, is sending the file. When the value is P, the server initiating the Process is the sender; otherwise, the server initiating the Process is the receiver.
FUNC	x					Function information
groupId					x	SLC name
HOLD	x					Hold
inError			x			Indicates an error occurred during business process execution
isBP			x			Event is associated with a Sterling Integrator business process.
jobId					x	Job ID
jobName		x				Job Name
LCCD	x					Local Return Code
lineName		x				Line Name
listName		x				List Name
LKFL	x					Link Fail
LMSG	x					Local Message ID
LNOD	x					Local Node
localNode	x		x			Server that processed the file.
mailboxFlags		x				Mailbox Flags

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
mailBoxId		x				Mailbox ID
maxExecutingProcs	x		x			Maximum number of concurrently executing Processes.
MCSI	x					Merged signature
MEMA	x					Alias Member Name
MEMB	x					Target Member Name
mepLastOccurrence	x		x			Last occurrence of maximum number of concurrently executing Processes.
mepOccurrences	x		x			Number of times maximum number of concurrently executing Processes occurred.
messageId	x	x	x	x	x	Server or Sterling Control Center message ID issued with the event.
milestoneId					x	Name of milestone.
MPEA	x					Merge EA
nodeId	x	x	x	x		The server alias.
nodeName	x		x	x		The actual name of the server
nodeType	x	x	x	x	x	The code indicating the type of server. The server types are: ◆ 0 = Sterling Control Center ◆ 1 = Connect:Direct ◆ 2 = Connect:Enterprise ◆ 3 = Sterling Integrator ◆ 4 = FTP
nodeTypeDescr	x	x	x	x	x	A description of the server type.
nonExecutingProcs	x		x			Number of nonexecuting Processes.
objectId					x	ID of object associated with the event.
objectType					x	Type of object associated with the event.
objectVersion					x	Version of object associated with the event.
OCCD	x					Other Return Code
oid		x				Object Identifier
OMSG	x					Other Message ID

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
origNode	x		x			The originating node of a process.
PACC	x					Pnode Accounting Information
PCSI	x					Pnode Signature
PEAL	x					Pnode Encryption Algorithm List
percentComplete	x				x	The percent complete of the file copy or transfer.
PPEA	x					Pnode Encryption Data
PPLX	x					Pnode Plex Class
processData			x			Sterling Integrator process data
processId	x	x	x	x		The Process ID or batch number.
processIds	x		x			A list of Process IDs or batch numbers in a Process Queue event.
processName	x	x	x	x		The Process name or batch ID.
processNames					x	A list of Process names or batch IDs in a Process Queue event.
processQueue	x		x			The queue containing the Process.
processQueues					x	A list of queues in a Process Queue event.
protocol		x				Protocol
PRTY	x					Priority
PSIN	x					Previous Signature Verified
QUEU	x					Queue
RCCT	x					Record Category
recCat	x	x				Record Category
recipientMailboxId		x				Recipient Mailbox ID
recordId	x	x				The type of statistics record from the event. See Event Type Descriptions, for a list of record IDs.
relativeSelectStmt		x				Relative Select Statement
remoteName		x				Remote Name
remoteNode	x	x	x	x		Name of the remote server involved in a Process or file transfer.

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
remoteNodes	x		x			A list of remote servers in a Process Queue event.
RETN	x					Retain
returnCode	x	x	x	x	x	A numeric code returned from a completed Process that indicates failure or success.
RSTR	x					Restart
ruleId	x	x	x	x	x	The name of the rule triggered by the event.
ruleInstanceId	x	x	x	x	x	Rules Instance ID used when there is a linked rule
ruleMemberName		x				Rule Member Name
ruleName		x				Connect:Enterprise z/OS Rule Name
RUSZ	x					RU Size
SACC	x					Snode Accounting Information
SBND	x					Submit Node
SCHD	x					Scheduled Date/Time
SCMP	x					Standard Compression
SCSI	x					Snode Signature
SDS1	x					Source Disposition 1
SDS2	x					Source Disposition 2
SDS3	x					Source Disposition 3
SEAL	x					Snode Encryption Algorithm List
seqNum	x	x	x	x	x	Sequence
session			x			Sterling Integrator Session
SESSION.ADAPTER_NAME			x			Sterling Integrator system adapter name.
SESSION.ADAPTER_TYPE			x			Sterling Integrator adapter type.
SESSION.CHILD_SESSIONID			x			Sterling Integrator Session child session ID
SESSION.CON_END_TIME			x			Sterling Integrator Session connection end time.
SESSION.CON_IS_SUCCESS			x			Sterling Integrator Session connection successful.

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
SESSION.CON_START_TIME			x			Sterling Integrator Session connection start time.
SESSION.DIS_END_TIME			x			Sterling Integrator Session disconnect end time.
SESSION.DIS_IS_SUCCESS			x			Sterling Integrator Session disconnect is success.
SESSION.DIS_START_TIME			x			Sterling Integrator Session disconnect start time.
SESSION.END_WFID			x			Sterling Integrator Session end workflow ID.
SESSION.END_WFSTEP			x			Sterling Integrator Session end workflow step.
SESSION.ENDPOINT1			x			Sterling Integrator Session end point 1.
SESSION.ENDPOINT2			x			Sterling Integrator Session end point 2.
SESSION.ENDPORT1			x			Sterling Integrator Session end port 1.
SESSION.ENDPORT2			x			Sterling Integrator Session end port 2.
SESSION.ERROR_MSG			x			Sterling Integrator Session error message.
SESSION.IS_LOCAL_INIT			x			Sterling Integrator Session is local init.
SESSION.PRINCIPAL			x			Sterling Integrator Protocol Activity Session principal.
SESSION.PROTOCOL			x			Sterling Integrator protocol of file movement.
SESSION.PS_INSTANCE			x			Sterling Integrator Protocol Activity Session PS instance.
SESSION.SECURE_MODE			x			Sterling Integrator Protocol Activity Session secure mode.
SESSION.SESSION_ARCHIVE_ID			x			Sterling Integrator Protocol Activity Session archive ID.
SESSION.SESSION_ID			x			Sterling Integrator Protocol Activity Session ID.
SESSION.START_WFID			x			Sterling Integrator Protocol Activity Session start workflow ID.
SESSION.START_WFSTEP			x			Sterling Integrator Protocol Activity Session start workflow step.

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
SESSION.STATUS_CODE			x			Sterling Integrator Protocol Activity Session status code.
shortText	x	x	x	x	x	Message text associated with the Message ID.
SI.MESSAGE_ID			x			Sterling Integrator/File Gateway message ID
slcId					x	A system-assigned name of the SLC that triggered the event.
slcInstanceId					x	Unique SLC identifier. Includes the SLC name, schedule name, and unique number.
slcSource1					x	SLC recovery data 1.
slcSource2					x	SLC recovery data 2.
SMEM	x					Source Member Name
SOPT	x					Sysopts
sourceEventTime					x	The time that the event triggering an SLC event occurred.
sourceFile	x	x	x	x		The source file name in a Copy. Also the target in a Submit, Run Task, or Run Job Connect:Direct Process step.
SPEA	x					Snode Encryption Data
SPLX	x					Snode Plex Class
SRCR	x					Records Read
SRUX	x					RUs Sent
SRVR	x					Server Name
STAT	x					Status
status	x	x				Status
stepName	x		x			The name of the Connect:Direct Process step or Sterling Integrator business Process activity.
STPT	x					Stop Date/Time
STRT	x					Start Date/Time
SUBI	x					Submitter Node
submitter	x	x	x	x		User ID of the Process submitter.

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
submitterId	x	x	x	x	x	The user ID of the work submitter.
submitterIds	x		x			A list of Submitter IDs in a Process Queue event.
suspended	x					Indicates if a Process is suspended.
TDSB	x					Submit Date/Time
timeUp		x				Time Up
triggerMilestoneId					x	Name of milestone that triggered the jeopardy SLC event.
url		x				URL
userData1	x	x	x	x	x	Metadata user data field 1.
userData2	x	x	x	x	x	Metadata user data field 2.
userData3	x	x	x	x	x	Metadata user data field 3.
userData4	x	x	x	x	x	Metadata user data field 4.
userId					x	User associated with the event.
WF.ACTIVITYINFO_ID			x			Business Process Activity Info ID.
WF.ADV_STATUS			x			Business Process advanced status.
WF.BASIC_STATUS			x			Business Process basic status.
WF.END_TIME			x			Business Process end time.
WF.NEXT_AI_ID			x			Business Process next AI ID.
WF.NODEEXECUTED			x			Node where Business Process executed.
WF.SERVICE_NAME			x			Service name in Business Process.
WF.START_TIME			x			Business Process / Business Process Step start time
WF.STEP_ID			x			Business Process step ID.
WF.WFD_ID			x			Business Process Definition ID.
WF.WFD_NAME			x			Business Process name.
WF.WFD_VERSION			x			Business Process Definition version.
WF.WFE_STATUS			x			Business Process execution status
WF.WORKFLOW_ID			x			Business Process instance ID
WFD_NAME			x			Business Process name

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
wkFlow		x				Workflow
XFER.DOC_ID			x			Sterling Integrator Protocol Activity Transfer document ID
XFER.DOC_NAME			x			Sterling Integrator Protocol Activity document name.
XFER.END_TIME			x			Sterling Integrator Protocol Activity Transfer end time.
XFER.FILE_SIZE			x			Sterling Integrator Protocol Activity Transfer file size.
XFER.IS_BIN_XFER			x			Sterling Integrator Protocol Activity Transfer is binary
XFER.IS_PUT			x			Sterling Integrator Protocol Activity Transfer is put.
XFER.IS_SECURE			x			Sterling Integrator Protocol Activity Transfer is secure.
XFER.IS_SUCCESS			x			Sterling Integrator Protocol Activity Transfer is success.
XFER.KBYTES_XFER			x			Sterling Integrator Protocol Activity KBytes transferred
XFER.MAILBOX_PATH			x			Sterling Integrator Protocol Activity/File Gateway Arrived File Mailbox Path
XFER.MBOX_PATH			x			Sterling Integrator Protocol Activity SI mailbox path.
XFER.MESSAGE_ID			x			Sterling Integrator Protocol Activity Transfer message ID
XFER.MESSAGE_NAME			x			Sterling Integrator Protocol Activity messagename
XFER.REMOTE_FILENAME			x			Sterling Integrator Protocol Activity Transfer remote filename
XFER.START_TIME			x			Sterling Integrator Protocol Activity Transfer start time
XFER.WFID			x			Sterling Integrator Protocol Activity Transfer work ID.
XFER.WFSTEP			x			Sterling Integrator Protocol Activity Transfer workflow step
XFER.XFER_ERROR_MSG			x			Sterling Integrator Protocol Activity Transfer error message.

Event Element	Server Type					Description
	CD	CE	SI	FTP	SCC	
XFER.XFER_ID			x			Sterling Integrator Protocol Activity Transfer ID.
XFER.XFER_STATUS_CODE			x			Sterling Integrator Protocol Activity Transfer status code.
XLAT	x					Translate

Variables by Event Type

The following table shows a breakdown of event elements available for use as variables by the event types they may occur in.

Note: Because the Server Shutdown Started and Server Shutdown event types (numbers 7 and 8) are not currently used, they are omitted from the table.

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	**Process Step Started**	**Process Step Ended**	**Proc Started**	**Proc Ended**	**Server Status**	**SLC**	**Proc Status**	**Server License**	**Server Error**	**Server Cmd**	**Connection Started**	**Connection Shutdown Started**	**Control Center Status**	**Proc Queued**	**Process Interrupted**
action						x				x					
actionId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
activityType						x									
alert	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
applAgentType	x	x	x	x											
batchId	x	x	x	x											
batchNumber	x	x	x	x											
bytesRead		x													
bytesSent		x													
bytesXferred							x								
CBEA		x									x				

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	**Process Step Started**	**Process Step Ended**	**Proc Started**	**Proc Ended**	**Server Status**	**SLC**	**Proc Status**	**Server License**	**Server Error**	**Server Cmd**	**Connection Started**	**Connection Shutdown Started**	**Control Center Status**	**Proc Queued**	**Process Interrupted**
CERI		x									x				
CERT		x									x				
CKPT		x													
CLAS										x					
CNOD		x													
CPUS		x		x											
CSPE		x									x				
CSPP		x									x				
CSPS		x									x				
CSTN							x			x					
daemonHost					x										
daemonName					x										
daemonOriginator					x										
daemonPid					x										
daemonResource					x										
daemonSid					x										
daemonState					x										
daemonType					x										
dateTime	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
DBUG			x												
DBYW		x													
DBYX		x													
DDS1		x													
DDS2		x													
DDS3		x													
destFile	x	x	x	x		x	x			x	x	x			
direction	x	x													

Event Type	**1**	**2**	**3**	**4**	**5**	**6**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Variable	**Process Step Started**	**Process Step Ended**	**Proc Started**	**Proc Ended**	**Server Status**	**SLC**	**Proc Status**	**Server License**	**Server Error**	**Server Cmd**	**Connection Started**	**Connection Shutdown Started**	**Control Center Status**	**Proc Queued**	**Process Interrupted**
DRCW		x													
DRUX		x													
ECMP		x													
EPRT										x					
eventId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
eventType	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
eventTypeDescr	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
executingProcs														x	
FDBK	x	x	x	x											x
FG.CONS_ORG_KEY	x	x	x	x			x								
FG.DATA_FLOW_ID	x	x	x	x			x								
FG.EVENT_CODE	x	x	x	x			x								
FG.FILE_NAME	x	x	x	x			x								
FG.PROD_ORG_KEY	x	x	x	x			x								
FG.STATE	x	x	x	x			x								
fgActivityType	x	x	x	x			x								
fileSize		x													
fromNode	x	x													
FUNC							x								
groupId						x									
HOLD										x					
inError	x	x	x	x											
isBP	x	x	x	x							x	x		x	
jobId										x					
jobName	x	x	x	x											
LCCD		x													
lineName	x	x	x	x											

Event Type	**1**	**2**	**3**	**4**	**5**	**6**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Variable	**Process Step Started**	**Process Step Ended**	**Proc Started**	**Proc Ended**	**Server Status**	**SLC**	**Proc Status**	**Server License**	**Server Error**	**Server Cmd**	**Connection Started**	**Connection Shutdown Started**	**Control Center Status**	**Proc Queued**	**Process Interrupted**
listName	x	x	x	x											
LKFL	x	x	x	x											
LMSG		x													
LNOD		x													
localNode	x	x	x	x			x								
mailboxFlags	x	x	x	x											
mailBoxId	x	x	x	x											
maxExecutingProcs														x	
MCSI											x				
MEMA		x													
MEMB	x	x			x										
mepLastOccurrence														x	
mepOccurrences														x	x
messageId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
milestoneId						x									
MPEA		x													
nodeId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
nodeName	x	x	x	x	x		x	x	x	x	x	x		x	x
nodeType	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
nodeTypeDescr	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
nonExecutingProcs														x	
objectId					x	x				x					
objectType					x	x				x			x		
objectVersion					x										
OCCD		x													
oid	x	x	x	x											
OMSG		x													

Event Type	**1**	**2**	**3**	**4**	**5**	**6**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Variable	**Process Step Started**	**Process Step Ended**	**Proc Started**	**Proc Ended**	**Server Status**	**SLC**	**Proc Status**	**Server License**	**Server Error**	**Server Cmd**	**Connection Started**	**Connection Shutdown Started**	**Control Center Status**	**Proc Queued**	**Process Interrupted**
origNode	x	x	x	x			x								x
PACC		x													
PCSI		x									x				
PEAL		x									x				
percentComplete						x	x								
PPEA		x									x				
PPLX		x													
processData	x	x	x	x											
processId	x	x	x	x		x	x	x	x	x	x	x			
processIds														x	
processName	x	x	x	x		x	x				x	x			
processNames														x	
processQueue						x	x								
processQueues														x	
protocol	x	x	x	x											
PRTY										x					
PSIN		x													
QUEU				x			x								
RCCT	x	x	x	x						x	x	x			
recCat	x	x	x	x				x	x	x	x	x			x
recipientMailboxId	x	x	x	x											
recordId	x	x	x	x				x	x	x	x	x			x
relativeSelectStmt	x	x	x	x											
remoteName	x	x	x	x											
remoteNode	x	x	x	x		x	x			x	x	x			x
remoteNodes														x	
RETN							x			x					

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	**Process Step Started**	**Process Step Ended**	**Proc Started**	**Proc Ended**	**Server Status**	**SLC**	**Proc Status**	**Server License**	**Server Error**	**Server Cmd**	**Connection Started**	**Connection Shutdown Started**	**Control Center Status**	**Proc Queued**	**Process Interrupted**
returnCode	x	x	x	x		x		x	x	x	x	x			x
RSTR		x													
ruleId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ruleInstanceId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ruleMemberName	x	x	x	x											
ruleName	x	x	x	x											
RUSZ		x													
SACC		x													
SBND	x	x	x	x						x	x				
SCHD			x	x											
SCMP		x													
SCSI		x									x				
SDS1		x													
SDS2		x													
SDS3		x													
SEAL		x									x				
seqNum	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
session	x	x	x	x											
SESSION.ADAPTER_NAME	x	x			x						x	x			
SESSION.ADAPTER_TYPE	x	x			x						x	x			
SESSION.CHILD_SESSIONID	x	x									x	x			
SESSION.CON_END_TIME	x	x									x	x			
SESSION.CON_IS_SUCCESS	x	x									x	x			
SESSION.CON_START_TIME	x	x									x	x			
SESSION.DIS_END_TIME	x	x									x	x			
SESSION.DIS_IS_SUCCESS	x	x									x	x			
SESSION.DIS_START_TIME	x	x									x	x			

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	**Process Step Started**	**Process Step Ended**	**Proc Started**	**Proc Ended**	**Server Status**	**SLC**	**Proc Status**	**Server License**	**Server Error**	**Server Cmd**	**Connection Started**	**Connection Shutdown Started**	**Control Center Status**	**Proc Queued**	**Process Interrupted**
SESSION.END_WFID	x	x									x	x			
SESSION.END_WFSTEP	x	x									x	x			
SESSION.ENDPOINT1	x	x									x	x			
SESSION.ENDPOINT2	x	x									x	x			
SESSION.ENDPORT1	x	x									x	x			
SESSION.ENDPORT2	x	x									x	x			
SESSION.ERROR_MSG	x	x									x	x			
SESSION.IS_LOCAL_INIT	x	x									x	x			
SESSION.PRINCIPAL	x	x									x	x			
SESSION.PROTOCOL	x	x									x	x			
SESSION.PS_INSTANCE	x	x									x	x			
SESSION.SECURE_MODE	x	x									x	x			
SESSION.SESSION_ARCHIVE_ID	x	x									x	x			
SESSION.SESSION_ID	x	x									x	x			
SESSION.START_WFID	x	x									x	x			
SESSION.START_WFSTEP	x	x									x	x			
SESSION.STATUS_CODE	x	x									x	x			
shortText	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SI.MESSAGE_ID	x	x	x	x											
slcId						x									
slcInstanceId						x									
slcSource1						x									
slcSource2						x									
SMEM		x													
SOPT		x													
sourceEventTime						x									

Event Type	**1**	**2**	**3**	**4**	**5**	**6**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Variable	**Process Step Started**	**Process Step Ended**	**Proc Started**	**Proc Ended**	**Server Status**	**SLC**	**Proc Status**	**Server License**	**Server Error**	**Server Cmd**	**Connection Started**	**Connection Shutdown Started**	**Control Center Status**	**Proc Queued**	**Process Interrupted**
sourceFile	x	x	x	x			x								
SPEA		x													
SPLX		x													
SRCR		x													
SRUX		x													
SRVR	x	x	x		x		x			x	x				
STAT							x			x					
status	x	x	x	x								x	x		x
stepName	x	x	x	x			x								x
STPT		x	x	x											
STRT	x	x	x	x	x					x	x				
SUBI	x	x	x	x						x	x				
submitter						x									x
submitterId	x	x	x	x		x	x			x	x	x			x
submitterIds														x	
suspended				x											
TDSB			x	x											
timeUp	x	x	x	x											
triggerMilestoneId						x									
url	x	x	x	x											
userData1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
userData2	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
userData3	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
userData4	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
userId					x					x					
WF.ACTIVITYINFO_ID	x	x	x	x											
WF.ADV_STATUS	x	x	x	x											

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	**Process Step Started**	**Process Step Ended**	**Proc Started**	**Proc Ended**	**Server Status**	**SLC**	**Proc Status**	**Server License**	**Server Error**	**Server Cmd**	**Connection Started**	**Connection Shutdown Started**	**Control Center Status**	**Proc Queued**	**Process Interrupted**
WF.BASIC_STATUS	x	x	x	x											
WF.END_TIME	x	x	x	x											
WF.NEXT_AI_ID	x	x	x	x											
WF.NODEEXECUTED	x	x	x	x											
WF.SERVICE_NAME	x	x	x	x											
WF.START_TIME	x	x	x	x											
WF.STEP_ID	x	x	x	x											
WF.WFD_ID	x	x	x	x											
WF.WFD_NAME	x	x	x	x											
WF.WFD_VERSION	x	x	x	x											
WF.WFE_STATUS	x	x	x	x											
WF.WORKFLOW_ID	x	x	x	x											
WFD_NAME	x	x	x	x											
wkFlow	x	x	x	x											
XFER.DOC_ID	x	x													
XFER.DOC_NAME	x	x													
XFER.END_TIME	x	x													
XFER.FILE_SIZE	x	x													
XFER.IS_BIN_XFER	x	x													
XFER.IS_PUT	x	x													
XFER.IS_SECURE	x	x													
XFER.IS_SUCCESS	x	x													
XFER.KBYTES_XFER	x	x													
XFER.MAILBOX_PATH	x	x	x	x			x								
XFER.MBOX_PATH	x	x													
XFER.MESSAGE_ID	x	x													
XFER.MESSAGE_NAME	x	x													

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	**Process Step Started**	**Process Step Ended**	**Proc Started**	**Proc Ended**	**Server Status**	**SLC**	**Proc Status**	**Server License**	**Server Error**	**Server Cmd**	**Connection Started**	**Connection Shutdown Started**	**Control Center Status**	**Proc Queued**	**Process Interrupted**
XFER.REMOTE_FILENAME	x	x													
XFER.START_TIME	x	x													
XFER.WFID	x	x													
XFER.WFSTEP	x	x													
XFER.XFER_ERROR_MSG	x	x													
XFER.XFER_ID	x	x													
XFER.XFER_STATUS_CODE	x	x													
XLAT		x													

Appendix H

Modify log4j to Retain Log Files

Sterling Control Center uses CCEngine.log4j to configure the engine logs and CCClient.log4j file for the console logs. You can modify these two properties files to change how the log files are rolled over and then rolled off. After the log file settings are configured, you could create a backup/archival process, either manual or through some separate process outside of Control Center. If the content of a log file is empty, the log file will not be rolled over.

This appendix contains samples of the CCEngine.log4j and CClient.log4j properties files, which when used as-is will cause log files to roll over every 12 hours (midday and midnight) without ever rolling off or being limited by size.The last section provides some notes about the types of parameters changed within the sample files.

The file format of the log files ends with either –am or –pm, for example, `CCEngine_20081105_140306184.log.2008-11-06-AM.` This filename format enables you to easily identify and move or copy all logfiles for a given time period, such as 90 days.

To use a sample configuration file, you must replace the existing log4j file contents with the content of the sample configuration file.

Each time, you upgrade to a new version of Sterling Control Center or install a maintenance release, you must replace the contents of the log4j file to keep the settings you want.

For more information on the latest parameters changed in the sample files, see *Parameters Modified in the Sample log4j Files* on page 257.

Sample CCEngine.log4j File

The sample log4j file for the ccengine log causes log files to roll over every 12 hours, that is, creates a new log file every 12 hours, and does not roll off any log files.

```
#
# CCEngine Log4j Properties
#
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout.ConversionPattern=%d{dd MMM yyyy HH\:mm\:ss,SSS} %r [%t]
%-5p %c{1} - %m%n
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout

log4j.logger.com.sterlingcommerce.scc=INHERITED
log4j.logger.org.apache.commons.beanutils=OFF

log4j.appender.R.File=${CONFIG_DIR}/../log/CCEngine_${current.time}.log
log4j.appender.R.DatePattern='.'yyyy-MM-dd-a
log4j.appender.R.layout=org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern=%d{dd MMM yyyy HH\:mm\:ss,SSS} %r [%t] %-5p
%c{1} - %m%n
log4j.appender.R=org.apache.log4j.DailyRollingFileAppender

log4j.loggerFactory=com.sterlingcommerce.component.common.logging.log4j.LogFactory
log4j.renderer.java.lang.Throwable=com.sterlingcommerce.component.common.logging.log
4j.ExceptionRenderer

log4j.rootLogger=INFO, R

log4j.category.RuleSession=INHERITED
log4j.category.RuleSession=, RuleSessionAppender
log4j.additivity.RuleSession=false
log4j.appender.RuleSessionAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.RuleSessionAppender.File=../log/RuleSession_${current.time}.log
log4j.appender.RuleSessionAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.RuleSessionAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.RuleSessionAppender=false
log4j.appender.RuleSessionAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} %r [%t] %-5p %c{1} - %m%n
log4j.category.RuleSession=INHERITED
log4j.category.RuleSession=, RuleSessionAppender
log4j.additivity.RuleSession=false
log4j.appender.RuleSessionAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.RuleSessionAppender.File=../log/RuleSession_${current.time}.log
log4j.appender.RuleSessionAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.RuleSessionAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.RuleSessionAppender=false
log4j.appender.RuleSessionAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} %r [%t] %-5p %c{1} - %m%n


log4j.category.PurgeService=INHERITED
log4j.category.PurgeService=, PurgeServiceAppender
log4j.additivity.PurgeService=false
log4j.appender.PurgeServiceAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.PurgeServiceAppender.File=../log/CCPurgeStagingService_${current.time
}.log
log4j.appender.PurgeServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.PurgeServiceAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.PurgeServiceAppender=false
log4j.appender.PurgeServiceAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} %r [%t] %-5p %c{1} - %m%n
```

```
log4j.category.BulkDataMover=INHERITED
log4j.category.BulkDataMover=, BulkDataMoverAppender
log4j.additivity.BulkDataMover=false
log4j.appender.BulkDataMoverAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.BulkDataMoverAppender.File=../log/BulkDataMover_${current.time}.log
log4j.appender.BulkDataMoverAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.BulkDataMoverAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.BulkDataMoverAppender=false
log4j.appender.BulkDataMoverAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} %r [%t] %-5p %c{1} - %m%n

log4j.category.ReportService=INHERITED
log4j.category.ReportService=INFO, ReportServiceAppender
log4j.additivity.ReportService=false
log4j.appender.ReportServiceAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.ReportServiceAppender.File=../log/ReportService_${current.time}.log
log4j.appender.ReportServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.ReportServiceAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.ReportServiceAppender=false
log4j.appender.ReportServiceAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} %r [%t] %-5p %c{1} - %m%n

log4j.category.EngineStartup=INHERITED
log4j.category.EngineStartup=, EngineStartupAppender
log4j.additivity.EngineStartup=false
log4j.appender.EngineStartupAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.EngineStartupAppender.File=../log/CCEngineStartup_${current.time}.log
log4j.appender.EngineStartupAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.EngineStartupAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.EngineStartupAppender=false
log4j.appender.EngineStartupAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} %r [%t] %-5p %c{1} - %m%n

log4j.category.org.mortbay.log=INHERITED
log4j.category.org.mortbay.log=, JettyServiceAppender
log4j.additivity.org.mortbay.log=false
log4j.appender.JettyServiceAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.JettyServiceAppender.File=../jetty/log/Jetty_${current.time}.log
log4j.appender.JettyServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.JettyServiceAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.JettyServiceAppender=false
log4j.appender.JettyServiceAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} %r [%t] %-5p %c{1} - %m%n

log4j.category./cdbrowser=INHERITED
log4j.category./cdbrowser=, JettyServiceAppender
log4j.additivity./cdbrowser=false
log4j.category.SLCService=ERROR,SLCServiceAppender
log4j.additivity.SLCService=false
log4j.appender.SLCServiceAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.SLCServiceAppender.File=../log/SLCService_${current.time}.log
log4j.appender.SLCServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.SLCServiceAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.SLCServiceAppender=false
log4j.appender.SLCServiceAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} [%t] - %m%n
```

```
log4j.category.SCCHealthChecker=INFO,SCCHealthCheckerAppender
log4j.additivity.SCCHealthChecker=false
log4j.appender.SCCHealthCheckerAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.SCCHealthCheckerAppender.File=../log/SCCHealthChecker_${current.time}.
log
log4j.appender.SCCHealthCheckerAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.SCCHealthCheckerAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.SCCHealthCheckerAppender=false
log4j.appender.SCCHealthCheckerAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} [%t] - %m%n
```

Sample CCClient.log4j File

The sample log4j file for the ccclient log causes log files to roll over every 12 hours, and does not roll off any log files.

```
# ccclient.Log4j
# Tue Mar 02 02:20:09 CST 2004
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.logger.com.sterlingcommerce.scc=INHERITED
log4j.appender.R.File=${CONFIG_DIR}/../log/CCClient_${current.time}.log
log4j.appender.R.layout=org.apache.log4j.PatternLayout
log4j.appender.R.DatePattern='.'yyyy-MM-dd-a
log4j.appender.R.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} %r [%t] %-5p %C{1} - %m%n
log4j.appender.stdout.layout.ConversionPattern=%d{dd MMM yyyy
HH\:mm\:ss,SSS} %r [%t] %-5p %C{1} - %m%n
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.R=org.apache.log4j.DailyRollingFileAppender

log4j.loggerFactory=com.sterlingcommerce.component.common.logging.log4j
.LogFactory
log4j.renderer.java.lang.Throwable=com.sterlingcommerce.component.commo
n.logging.log4j.ExceptionRenderer

log4j.rootLogger=INFO, R


log4j.category.ReportService=INHERITED
log4j.category.ReportService=INFO, ReportServiceAppender
log4j.additivity.ReportService=false
log4j.appender.ReportServiceAppender=org.apache.log4j.DailyRollingFileA
ppender
log4j.appender.ReportServiceAppender.File=../log/ReportService_${curren
t.time}.log
log4j.appender.ReportServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.ReportServiceAppender.layout=org.apache.log4j.PatternLay
out
log4j.additivity.ReportServiceAppender=false
log4j.appender.ReportServiceAppender.layout.ConversionPattern=%d{dd MMM
yyyy HH\:mm\:ss,SSS} %r [%t] %-5p %c{1} - %m%n
```

Parameters Modified in the Sample log4j Files

Some parameters have been modified in the sample log4j files.

Note: This may not be a complete list.

Lines similar to the following have been added to the CCEngine.log4j file.

```
log4j.appender.R.DatePattern='.'yyyy-MM-dd-a
log4j.appender.RuleSessionAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.PurgeServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.BulkDataMoverAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.ReportServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.EngineStartupAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.JettyServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.SLCServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.SCCHealthCheckerAppender.DatePattern='.'yyyy-MM-dd-a
```

The '.'yyyy-MM-dd-a item specifies to roll over the files every 12 hours. You can also choose from the following options:

- `'.'yyyy-MM`:—Rolls log file on the first of each month
- `'.'yyyy-ww`:—Rolls log file at the beginning of each week
- `'.'yyyy-MM-dd`:—Rolls log file at midnight every day
- `'.'yyyy-MM-dd-a`:—Rolls log file at midnight and midday every day
- `'.'yyyy-MM-dd-HH`:—Rolls log file at the beginning of each hour
- `'.'yyyy-MM-dd-HH-mm`:—Rolls log file at the beginning of each minute

Lines similar to the following have been removed:

```
log4j.appender.R.MaxFileSize=1000KB
log4j.appender.R.MaxBackupIndex=20
```

Lines similar to the following have been replaced:

```
log4j.appender.R=org.apache.log4j.RollingFileAppender
```

For example, the previous line was replaced with the following:

```
log4j.appender.R=org.apache.log4j.DailyRollingFileAppender
```

Appendix I

Copy Configuration Objects Between Installations

You can copy all Sterling Control Center (SCC) configuration objects from a source Control Center installation to a target Control Center installation. After these steps are performed, any existing configuration objects at the target installation are not used by the Control Center engine because you either delete or rename the old conf folder on the target installation.

You may want to perform this copy procedure for a variety of reasons including:

- To prepare for disaster recovery.
- To copy a test instance of Control Center to a production instance

The source installation and target installation must be the same version level, including the minor version. For example, if the source SCC installation is 5.0.02, then the target installation must be 5.0.02.

You must copy the entire configuration objects directory as a whole. Do not copy configuration objects selectively. You must not attempt to merge the source configuration data with any existing target configuration data. The source configuration is a complete replacement of all the target configuration's objects.

The following Control Center configuration objects are stored in the *SCCInstallDirectory*\ControlCenter\conf directory, where *SCCInstallDirectory* is the directory where you installed Control Center:

- Definitions and checkpoint files for all managed servers
- Rules and Actions
- Rule Schedules, SLC Schedules and Automated Report Schedules
- Calendars
- E-mail Lists
- Metadata Rules and Actions
- Report definitions
- Automated Report Definitions
- Users, Roles, and User Profiles
- Server Groups

- Templates for Batch creation utility
- Password Policy file
- Welcome Message file
- Various engine connector service definitions
- Various System Service files such as JDBC Service

The configuration objects include the JDBC Configuration (Database connection) details. After you copy the configuration objects to another installation, you must run configCC.bat (for Windows) or configCC.sh (for UNIX) to change the database connection details so the target installation uses the appropriate database. For more information, see Step 9 in either *Copy Procedure for Windows* on page 260 or *Copy Procedure for UNIX* on page 262.

The checkpoint files for managed servers are also included in the configuration objects. Therefore, when the configuration objects are copied to another installation, the target engine will use those checkpoint files and start collecting the statistics onwards from the date and time found in those files. If you do not want this to be the case, use runEngineCold.bat (for WIndows) or runEngineCold.sh (for UNIX). For more information, see Step 10 in either *Copy Procedure for Windows* on page 260 or *Copy Procedure for UNIX* on page 262.

Copy Procedure for Windows

To copy the configuration objects from one Control Center installation on Windows to another:

Source Installation Steps

1. Stop the engine from where you are planning to copy the Control Center configuration objects.
2. Archive the entire conf folder located under the *SCCInstallDirectory* folder using WinZip or a similar tool.
3. Transfer the archived file to the target installation host.
4. Restart the engine if desired.

Target Installation Steps

1. Stop the SCC engine running on the target installation.
2. Make a backup of the conf folder on the target installation.
3. Rename (or delete) the existing conf folder on the target installation.

> ***Caution:*** Do not attempt to merge the source configuration data with any existing target configuration data.

4. From the target SCC engine installation location, extract the archive file that was transferred from the source installation.

   After the extraction, you should see the conf folder under the *SCCInstallDirectory* folder.

5. Run configCC.bat to change the database connection details. If you do not, the Database connection used by the target installation will be the same as the source SCC installation.

   When you run configCC, you will get a message that all the steps have been already configured, but you must still go through the following steps and specify different values wherever required:

   a. Engine Name configuration step: You may need to specify a different name.
   b. Time Zone configuration step: You may need to specify different value if the source installation and target installation were not in the same time zone.
   c. JDBC Driver configuration step: You must select the appropriate database type and specify the JDBC Driver for that database type even though this has been already configured.
   d. Production Database connection parameters configuration step: You must specify different connection details. If you do not specify different database connection details, two different engines could be using the same database.
   e. Production Database initialization step: Answer “No” to initialize the step. If you say “Yes,” all existing data in the database will be lost.
   f. Staging Database connection parameters configuration step: You must specify different connection details. If you do not specify different database connection details, two different engines could be using the same database.
   g. Staging Database initialization step: Answer “No” to initialize the step. If you say “Yes,” all existing data in the database will be lost.
   h. Key Store/Trust Store configuration step: If you specified a valid key store and trust store previously, you must specify them again.
   i. Http Connector Configuration: Reconfigure this with the appropriate port number.
   j. Secure Http Connector Configuration: Reconfigure this if you need a secure connection between the engine and console.
   k. Servlet Container (JETTY) Configuration step: Reconfigure this with the appropriate port number and host name.

6. Start the engine taking one of the following actions:

   - To collect the statistics that were generated when the engine was down, use runEngine.bat.
   - To start collecting statistics now, use runEngineCold.bat.

7. Using the Control Center console, update the following system settings if required (through the option, **Control Center**>**System Settings**):

   - E-mail server connection (on the E-mail tab)
   - Host computers where SNMP traps are sent (on the SNMP Hosts tab)
   - Simultaneous pollers (on the Services tab)
   - Settings effecting the monitor performance (on the Console Settings tab)
   - Settings related to moving data from the Production to the Staging databases (on the Database tab)

Copy Procedure for UNIX

To copy the configuration objects from one Control Center installation on UNIX to another:

Source Installation Steps

1. Stop the engine from where you are planning to copy the Control Center configuration objects.
2. Archive the entire conf folder located under the *SCCInstallDirectory* folder using tar. For example, you could use the following command:

```
tar -cvf conf.tar conf
```

3. Transfer the archived file to the target installation host.
4. Restart the engine if desired.

Target Installation Steps

1. Stop the SCC engine running on the target installation.
2. Make a backup of the conf folder on the target installation.
3. Rename (or delete) the existing conf folder on the target installation. For example, you could use the following command:

```
mv conf conf_old
```

Caution: Do not attempt to merge the source configuration data with any existing target configuration data.

4. From the target SCC engine installation location, extract the archive file that was transferred from the source installation. For example, you could use the following command:

```
tar -xvf conf.tar
```

   After the extraction, you should see the conf folder under the *SCCInstallDirectory* folder.

5. Run configCC.sh to change the database connection details. If you do not, the Database connection used by the target installation will be the same as the source SCC installation.

   When you run configCC, you will get a message that all the steps have been already configured, but you must still go through the following steps and specify different values wherever required:

   a. Engine Name configuration step: You may need to specify a different name.
   b. Time Zone configuration step: You may need to specify different value if the source installation and target installation were not in the same time zone.

c. JDBC Driver configuration step: You must select the appropriate database type and specify the JDBC Driver for that database type even though this has been already configured.

d. Production Database connection parameters configuration step: You must specify different connection details. If you do not specify different database connection details, two different engines could be using the same database.

e. Production Database initialization step: Answer “No” to initialize the step. If you say “Yes,” all existing data in the database will be lost.

f. Staging Database connection parameters configuration step: You must specify different connection details. If you do not specify different database connection details, two different engines could be using the same database.

g. Staging Database initialization step: Answer “No” to initialize the step. If you say “Yes,” all existing data in the database will be lost.

h. Key Store/Trust Store configuration step: If you specified a valid key store and trust store previously, you must specify them again.

i. Http Connector Configuration: Reconfigure this with the appropriate port number.

j. Secure Http Connector Configuration: Reconfigure this if you need a secure connection between the engine and console.

k. Servlet Container (JETTY) Configuration step: Reconfigure this with the appropriate port number and host name.

6. Start the engine taking one of the following actions:

   - To collect the statistics that were generated when the engine was down, use runEngine.sh.
   - To start collecting statistics now, use runEngineCold.sh.

7. Using the Control Center console, update the following system settings if required (through the option, **Control Center**>**System Settings**):

   - E-mail server connection (on the E-mail tab)
   - Host computers where SNMP traps are sent (on the SNMP Hosts tab)
   - Simultaneous pollers (on the Services tab)
   - Settings effecting the monitor performance (on the Console Settings tab)
   - Settings related to moving data from the Production to the Staging databases (on the Database tab)

Appendix J

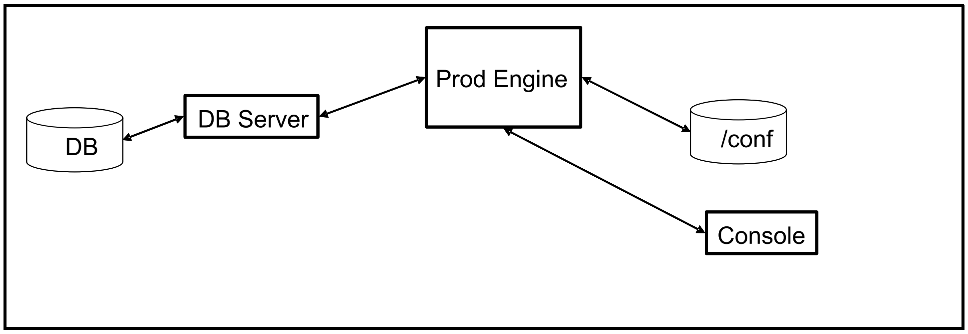
Failover Configuration

Although Sterling Control Center has been designed to handle a wide variety of system failures, it may not able to recover in the case of a hardware failure. However, there are several measures and precautions you can take to provide failover support required in a high-availability environment. This appendix discusses the configuration and manual steps for recovering from hardware failures in Control Center in two different types of environments–one in which the Control Center engine is installed on a storage area network (SAN) and one where it is not.

The typical Sterling Control Center environment consists of the following components:

- Production Engine (Prod Engine in the following diagram). The Sterling Control Center engine collects information from servers and writes that information to a database. It uses information configured in the /conf directory for system definitions.
- Database server (DB Server).
- Two databases:
  - Production Database—Contains production statistics and event data, Node Discovery-related data, auditing data, and service level criteria recovery-related data.
  - Staging Database—Contains statistics data and event data that have been moved from production.
- Console—The graphical user interface.
- Installation directory/conf— Configuration directory includes managed server definitions and checkpoint data, rules, actions, and service level criteria.

The following diagram shows the base configuration:



Failover may be required in the following situations, which can occur in both types of environments (storage area networks and non-SAN systems):

- ✦ Sterling Control Center engine computer failure
- ✦ Database server (for production database) computer failure
- ✦ Sterling Control Center engine and database server (for production database) computer failure

Note: Control Center requires two databases: production and staging, and must have access to both when it is installed and configured. Assuming the staging database resides on a different database server than the production database, Control Center will continue to run even if the staging database is not available. Because recovery from staging database failures is not required for Control Center to run, this appendix does not address staging database failure as a failover/recovery scenario. Although Control Center can continue to run with a staging database server failure, eventually the staging database server must be recovered for Control Center to run with the expected level of performance.

This appendix covers the situations outlined above and builds from the base configuration diagram while providing general procedures for all types of failures.

Handling Failures When the Engine Is installed on a SAN

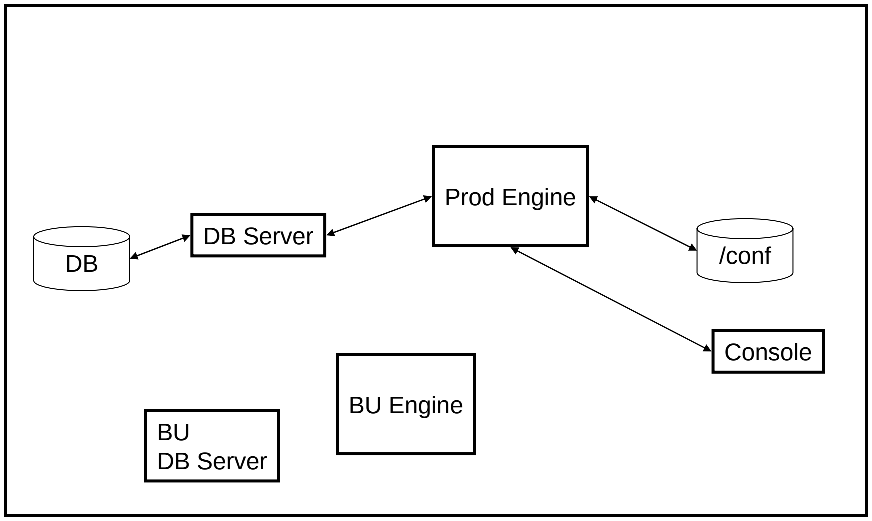
When the Control Center engine is installed on a storage area network (SAN), follow this general procedure before a production engine failure occurs:

1. Identify the standby computer for the Sterling Control Center engine.
2. Identify a standby database server for the production database.
3. Create a production database and user on the standby database server for Sterling Control Center use.

After you perform this procedure, two new components are added to the base diagram:

- ✦ Backup Engine (BU Engine)—Acts as the failover Sterling Control Center engine
- ✦ Backup database server (BU DB Server)—For the production database.

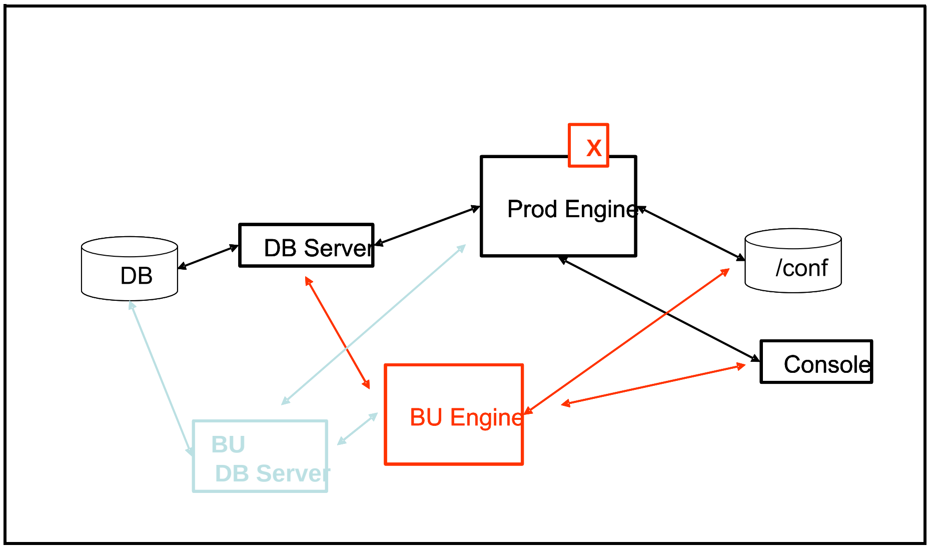
The following diagram shows the base configuration with these added components.



Note that when the Control Center engine is installed on a SAN, there is no requirement to install an engine on the standby computer. It is assumed that the SAN will be available even when the production engine's computer fails.

SAN Scenario 1—The Server on which the Control Center Engine Is Executing Fails

In this scenario, it is assumed that you have added both a backup engine and database server by performing the general procedure outlined in *Handling Failures When the Engine Is installed on a SAN* on page 266.

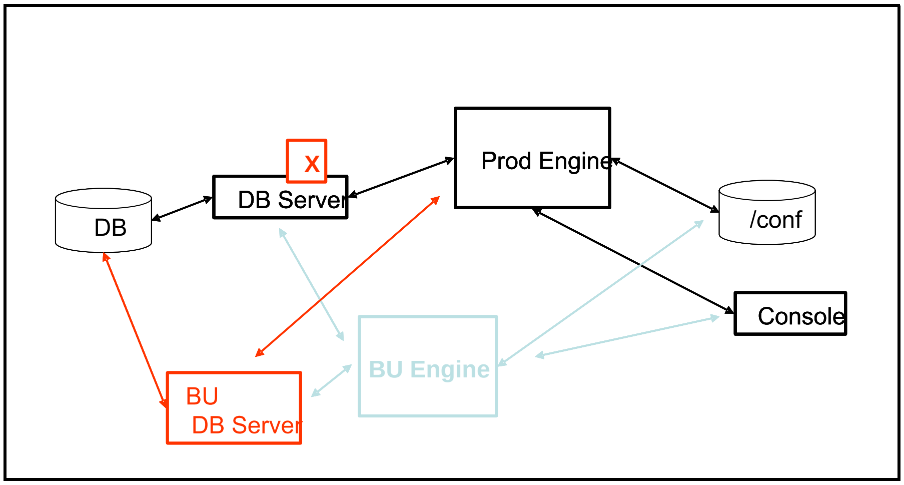


What needs to be done after the production engine fails?

Start the Control Center engine from the standby computer using the console. The backup engine has access to both the database server where the production database resides and the production engine configuration data. The backup engine is brought up (without using the standby database server).

SAN Scenario 2—The Computer Where the Database Server Is Executing Fails

In this scenario, it is assumed that you have performed the general procedure outlined in *Handling Failures When the Engine Is installed on a SAN* on page 266 and that the standby Control Center computer will not be used.



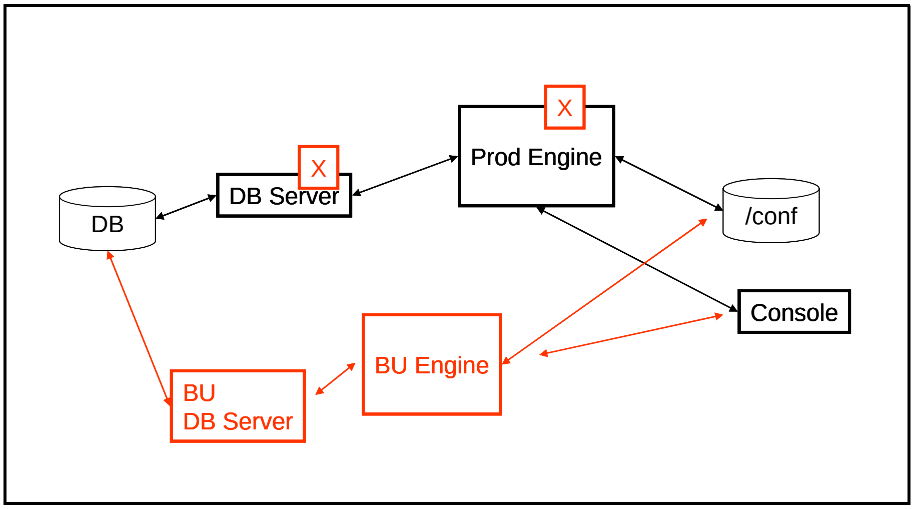
What needs to be done after the primary database server fails?

1. Run (SAN-based) production Sterling Control Center engine’s configuration script (configCC.sh/configCC.bat) and configure the engine to point to the standby database server. (The configCC.sh/configCC.bat file is located in the *ControlCenterInstallLoc*/bin directory.)
2. Start the (SAN-based) production Sterling Control Center engine.

The Production engine has access to the backup database server because you configured and pointed it to the backup database server, which may require supplying the IP address of the backup database server. After you reconnect to the production engine using the console, the production engine can use a different production database (on a standby database server) on another computer.

SAN Scenario 3—The Computer Where the Engine Is Executing and the Computer Where the Database Server Is Executing Both Fail

In this scenario, it is assumed that you have performed the general procedure outlined in *Handling Failures When the Engine Is installed on a SAN* on page 266 and that the storage area network is available even after the Control Center production engine computer has failed.



What needs to be done after the production environment failure?

1. Run the (SAN-based) Sterling Control Center engine's configuration script from another computer (configCC.sh/configCC.bat) and configure the engine to point to the standby database server. (The ConfigCC.sh /configCC.bat file is located in the *ControlCenterInstallLoc*/bin directory.)
2. Start the (SAN-based) Sterling Control Center engine (from another computer).

The backup database server can access the Production database. In addition, the backup engine can access the Production Engine configuration data. When the primary database server fails, the backup database server is brought up and the backup engine is brought up when the production engine fails. (You may have to configure the backup database server's IP address.) To bring up the system, you contact the backup engine using the console.

Handling Failures when the Engine Is Not Installed on a SAN

The other possible failure scenario is when the Sterling Control Center engine is not installed on a storage area network.

To prepare for any type of failure in a non-SAN environment:

1. To recover from a production Sterling Control Center engine failure, you must have copies of the most recent configuration files.
2. Identify the standby computer for Sterling Control Center engine.
3. Identify a standby database server.
4. Create a production database and user on the standby database server for Sterling Control Center use.
5. Install the Sterling Control Center engine on the standby computer.
6. On a regular basis, copy the entire /conf directory of the production Sterling Control Center engine to the standby Sterling Control Center engine install location.

- The /conf directory is located in the same directory where Control Center is installed.
- It is recommended that you copy the /conf directory (including the subdirectories) of the production Sterling Control Center engine to the standby Sterling Control Center engine install location at least once a day. (In other words, replace the contents of the standby Sterling Control Center engine's /conf directory with the contents of the production Sterling Control Center engine's /conf directory.)
- Ideally, the periodic copy should be based on the frequency of changes to the Sterling Control Center configuration data (rules, actions, SLCs, managed servers, etc.).

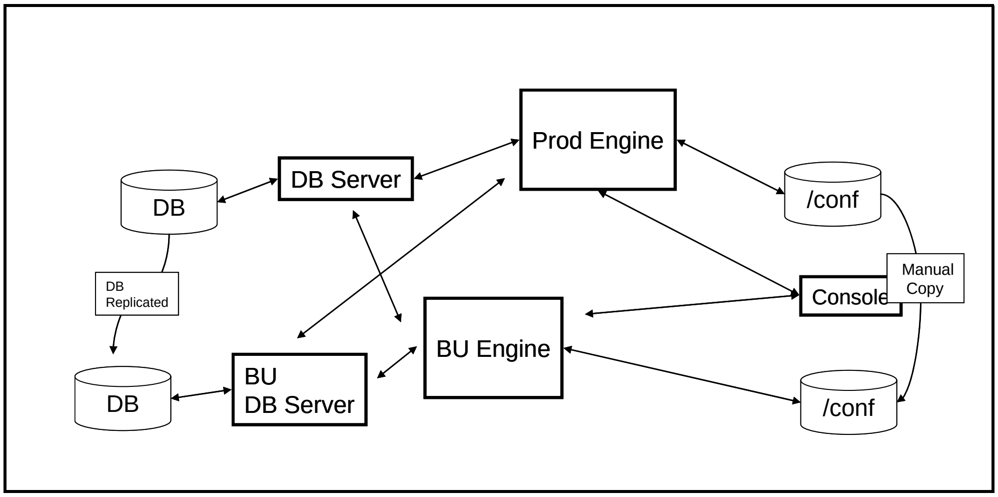
Safeguarding the Managed Server's Checkpoint Data

It is crucial that you systematically copy the managed server's checkpoint data in the /conf directory to the standby Control Center engine install location. The managed server's checkpoint data keeps track of the last time ("savedDateTime") data from that managed server was saved. Each managed server's checkpoint data is kept separately under the /conf directory.

Whenever the Sterling Control Center engine is restarted, the engine uses the checkpoint data of each managed server to collect data beginning with the last time data was collected. Likewise, when you start the standby engine after a primary engine fails, the Sterling Control Center engine uses the checkpoint data of each managed server to collect this data.

So if you infrequently copy the /conf directory to the standby Sterling Control Center engine location, the checkpoint data may be old when you restart the standby Sterling Control Center engine. As as a result, this could cause the standby engine to collect data that has already been collected by the primary engine, and checkpoint/restart process may take a considerable amount of time.

To avoid collecting data that has already been collected, perform a cold start at the standby location. To do a cold start, run the runEngineCold.bat script file (Windows) or the runEngineCold.sh script bat file (UNIX) from the command line. These scripts are located in the *ControlCenterInstallLoc*/bin directory.



After you replicate the production database and copy the /conf directory to the standby Control Center engine install location, two new components have been added to the base diagram:

- DB—The replicated database which acts as the Failover Sterling Control Center database.
- /conf—The manual copy of the production /conf directory.

Testing the Standby Sterling Control Center Engine

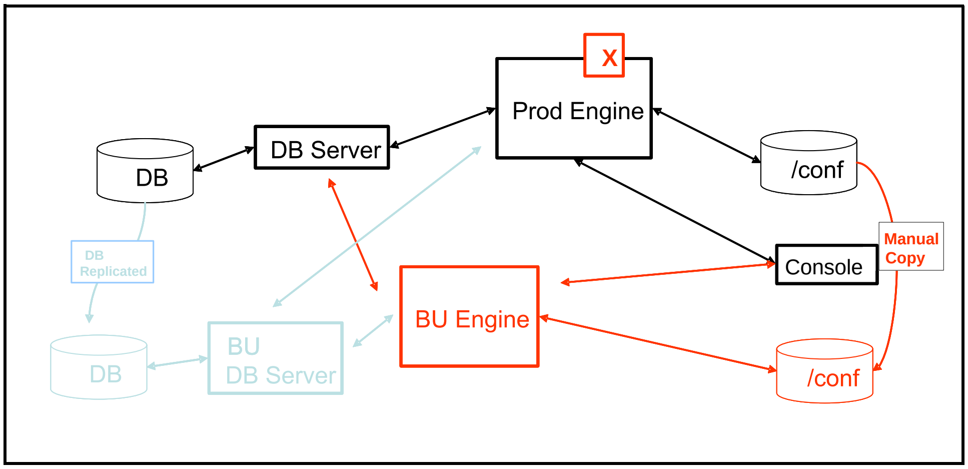
Although it is not necessary for the standby Sterling Control Center engine to run all the time, you should test it periodically using the following steps:

1. Shut down the production Sterling Control Center engine.
2. Copy the contents of the production Sterling Control Center engine's /conf directory to the standby Sterling Control Center engine.
3. Start the standby Sterling Control Center engine.

Scenario 1—The Computer Where the Control Center Engine Is Executing Fails

In this scenario, it is assumed that you have followed all procedures outlined in *Handling Failures when the Engine Is Not Installed on a SAN* on page 269 before the production Sterling Control Center engine computer failure. The following assumptions are also in place:

- The standby engine will use the same database server used by the production Control Center engine.
- This also implies that the standby database server will *not* be used.



The backup Control Center engine has access to the production database. You must manually copy the production engine configuration data to enable the backup engine to be brought up properly.

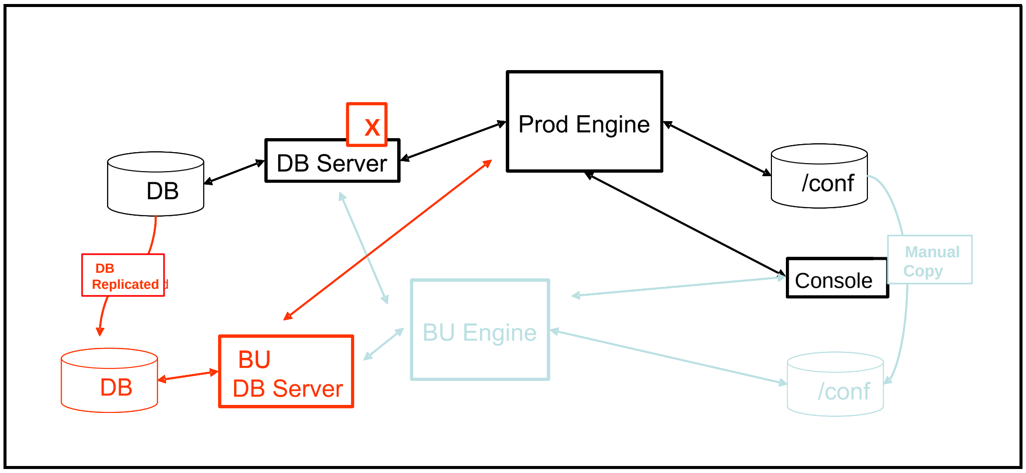
What needs to be done after the production engine failure?

Start the standby Control Center engine using the console. When you contact the backup engine, the backup engine is brought up using the copied /conf configuration data.

Scenario 2—The Computer Where the Primary Database Is Executing Fails

In this scenario, it is assumed that you have followed all procedures outlined in *Handling Failures when the Engine Is Not Installed on a SAN* on page 269 before the production Sterling Control

Center engine computer failure. It is also assumed that the standby Sterling Control Center engine will *not* be used. This situation can be handled simply by configuring the Sterling Control Center engine to use a different production database (standby database server) on another computer.



What needs to be done after the primary database server failure?

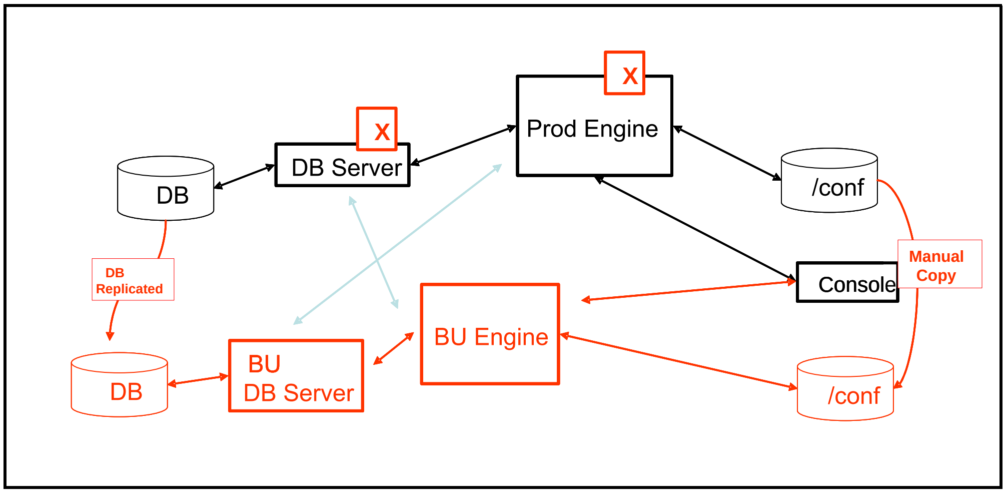
1. Run the production Sterling Control Center engine’s configuration script (configCC.sh/configCC.bat) and configure the engine to point to the standby database server.
2. Start the production Sterling Control Center engine.

The primary database has been replicated to the backup database server. The production engine is brought back up by pointing to the backup database server (which may require you to configure the IP address for the backup database).

Note: As mentioned earlier, Control Center uses the database mainly to store auditing and statistics data. Since all configuration data is stored where the Control Center engine is installed, the engine can be started using a new database and function normally. As a result, the standby Control Center database does not need up-to-date data from the primary Control Center database. This also implies that database replication does not need to be set up for high-availability purposes alone.

Scenario 3—The Computer Where the Engine Is Executing and the Computer Where the Database Server Is Executing Both Fail

In this scenario, it is assumed that you have followed all procedures outlined in *Handling Failures when the Engine Is Not Installed on a SAN* on page 269 before the production environment failure.



What needs to be done after the production environment failures?

1. Run the standby Sterling Control Center engine’s configuration script (configCC.sh/configCC.bat) and configure the engine to point to the standby database server. (The configCC.sh /configCC.bat file is located in the *ControlCenterInstallLoc*/bin directory.**)**
2. Start the standby Sterling Control Center engine.

In this case, both the standby Sterling Control Center engine and standby database server are used.

Appendix K

High Availability in the Microsoft Cluster Service Environment

To make Sterling Control Center meet high availability criteria, you may utilize the Microsoft Cluster Service (MSCS) in either Windows Server 2003 or Windows Server 2008.

High availability for the Control Center engine is achieved by installing Sterling Control Center on multiple nodes within an MSCS cluster. When Sterling Control Center fails, or is taken down, on a node in the cluster, the application is automatically restarted by the MSCS on either the same or a different node in the cluster.

To make Sterling Control Center fully meet high availability criteria, the database used by the Sterling Control Center engine must also meet high availability criteria.

Note: Setting up a highly available database is outside the scope of this document.

This appendix addresses the changes required during the typical Control Center installation and setup on Windows to accommodate the specific requirements of an MSCS cluster environment. It is not a tutorial on the installation and setup of Control Center or MSCS.

The following information is included:

- Resources
- Setup
- Verifying the Installation
- Applying Maintenance

Resources

When setting up Sterling Control Center to run with the MSCS you will need two resources:

- An installation directory
- An IP address or host name

The installation directory is a common point for all the binaries and configuration files associated with Sterling Control Center. This is typically the quorum drive or a shared storage device dedicated to the cluster.

The IP address or host name is the virtual address to be used on all Control Center installations within the cluster.

Setup

The first step in the setup of Sterling Control Center in an MSCS environment is to make sure the Microsoft Cluster Service is installed and configured properly.

If you are installing on Windows Server 2008, as opposed to Windows Server 2003, you must next perform the following tasks via the Failover Management console:

1. Create a new Empty Service or Application group under Services and Applications.
2. Rename the empty service just created to “ControlCenter.”
3. Set up the virtual IP address for this new ControlCenter service group by adding a new Client Access Point resource and then specify a valid IP address for your Control Center engine within the cluster.
4. Assign a shared disk location to the ControlCenter service group by selecting Add Storage and selecting an available disk to use for the installation.
5. Bring the ControlCenter service group online.

The next step for both Windows Server 2008 and 2003 is to install Control Center. You will need the following information to install Sterling Control Center:

- The virtual IP address of the cluster. The Sterling Control Center installation will be configured to use this network address for incoming communications.
- A shared disk location. Sterling Control Center will be installed on a shared disk.

With this information in hand, make the initial cluster node the active node and make sure it has access to:

- The shared drive on which you will be installing Control Center
- The cluster’s IP address.

Now install Sterling Control Center, in a normal fashion, on this MSCS cluster node on the shared drive. Do not install Sterling Control Center to a local, non-shared disk in the cluster.

One thing to be aware of while installing Sterling Control Center: When prompted for the fully qualified DNS name, be sure to specify the virtual IP address for the cluster; do not use the installation’s default value, which is the address for the server, as opposed to the virtual address for the cluster.

After the installation on the first cluster node is complete, repeat the following steps for all remaining cluster servers:

1. Make the next cluster server the active server by switching the resources, the virtual IP address, and the shared disk location, over to it using the Failover Cluster Management administrative tool on Windows Server 2008, or the Cluster Administrator tool on Windows Server 2003.
2. Install Sterling Control Center. You should install the code to the same location as before, utilizing the same parameter values. Note that the installation process should think it is doing an upgrade installation and indicate this to you during the installation process. The only values you have to reenter during such an upgrade installation are the database password values.

Finally, after all installations of the Sterling Control Center engine have been performed for each of the cluster nodes, you must switch back to the main cluster node and configure Sterling Control Center as a resource in the cluster.

To configure Sterling Control Center as a resource in the cluster, you will need its service name. The Sterling Control Center service name can be gotten by looking at the Sterling Control Center service's properties via the Windows Services Administrative tool. An example of Sterling Control Center's service name is `runEngine$v5.2` – this name is based on the version of Sterling Control Center you have installed.

Using either the Failover Cluster Management administrative tool (Windows Server 2008) or Cluster Administrative tool (Windows Server 2003), configure Sterling Control Center as a resource in the cluster as follows:

1. Add the Sterling Control Center service into the cluster as a managed cluster resource for the Cluster Group.
2. Enter a name and description for the Sterling Control Center resource.
3. Select Generic Service as the resource type.
4. Allow all cluster nodes to take ownership of this resource.
5. Specify dependencies of the cluster’s Virtual IP Address, and the shared disk Sterling Control Center was installed onto, for the Control Center resource.
6. When prompted for the Generic Service Parameter’s Service name value for Sterling Control Center, specify the Control Center service name previously obtained via the Windows Services Administrative tool.

Verifying the Installation

To verify that the installation is correct, bring online the resource associated with Sterling Control Center using either the Failover Cluster Management administrative tool (Windows Server 2008), or Cluster Administrative tool (Windows Server 2003).

Once the Sterling Control Center engine has initialized, start the Sterling Control Center Console and connect to the engine.

You may subsequently move the Control Center service to another node within the cluster using either the Failover Cluster Management administrative tool (Windows Server 2008), or Cluster Administrative tool (Windows Server 2003).

Once the service is back online after being moved, end your current Sterling Control Center Console instance if you have not already done so—the Console will lose its connection to the engine when the service is moved—and start a new Sterling Control Center Console instance and reconnect to the engine.

Applying Maintenance

To apply maintenance to Sterling Control Center in an MSCS environment you must first:

1. Via the Cluster Management software move the Sterling Control Center Cluster Group to the initial cluster server so that all resources associated with Sterling Control Center are available to this first cluster node.
2. Then take the Sterling Control Center resource offline.

Now you may follow the standard procedure for applying Sterling Control Center maintenance.

Note: You only have to install the maintenance once on the initial cluster server.

Once you have applied the Sterling Control Center maintenance you can bring the Sterling Control Center Service back online again via the Cluster Management software.

Appendix L

High Availability in the Veritas Cluster Server Environment

In a Veritas Cluster Server (VCS) 5.0 test environment, Control Center has been installed and configured and successfully passed several failover scenarios.

This appendix addresses the changes required during the typical Control Center installation and setup on UNIX/Linux to accommodate the specific requirements of a VCS cluster environment. It is not a tutorial on the installation and setup of Control Center or VCS.

The following information is included:

- Test environment details
- Control Center UNIX/Linux installation and configuration requirements
- Sample scripts
- Failover test scenarios

Please refer to http://www.symantec.com/business/cluster-server for descriptive information of the VCS environment.

Test Environment

The following hardware was used in the test environment:

- Two HP ProLiant DL380 G5 computers running Red Hat Enterprise Linux AS release 4 (Nahant Update 7) with 15.86G memory and four Intel® Xeon® CPU 5160 @ 3.00GHz CPUs
- A 1000baseT network connection via Broadcom Corporation NetXtreme II BCM5708 Gigabit Ethernet adapters.
- Heartbeat connection via second set of Broadcom Corporation NetXtreme II BCM5708 Gigabit Ethernet adapters.
- Shared drive via 2Gbps fibre channel SAN. SAN unit is a Nexsan ATABoy2x with 14x400GB drives configured as a single RAID 5 column with a 500GB shared LUN exposed.

Control Center Installation and Configuration Requirements

Use the information and instructions in this section when installing and configuring Control Center to operate in a VCS High Availability environment. These procedures assume that you have set up an application service group for Control Center that includes a virtual IP address (VIP) resource and a Control Center resource type defined as follows.

Service Groups

A service group is a virtual container that contains all the hardware and software resources required to run the managed application. Service groups allow VCS to control all the hardware and software resources of the managed application as a single unit. When a failover occurs, resources do not fail over individually—the entire service group fails over. If there is more than one service group on a system, a group may fail over without affecting the others.

A single node may host any number of service groups, each providing a discrete service to networked clients. If the server crashes, all service groups on that node must be failed over elsewhere.

Configuring VCS means conveying to the VCS engine the definitions of the cluster, service groups, resources, and resource dependencies. VCS uses two configuration files in a default configuration:

- main.cf—Defines the cluster, including services groups and resources.
- types.cf—Defines the resource types.

By default, both files reside in the directory: /etc/VRTSvcs/conf/config

Following is an excerpt from /etc/VRTSvcs/conf/config/**main.cf**, which shows the Control Center service group, Control Center resource, and resource dependencies. Your configuration will look similar.

```
group ControlCenter (
        SystemList = { system1 = 0, system2 = 1 }
        FailOverPolicy = RoundRobin
        )

        ControlCenter ControlCenter (
                CCInstallDir = "/shared/users/username/cc5200ha"
                CCUser = username
                CCPass = user-password
                VirtualIP = userrt
                )

        IP svajdavirt (
                Device = eth0
                Address = "10.10.10.10"
                NetMask = "255.255.255.0"
                )

ControlCenter requires userrt
        // resource dependency tree
        //
        //      group ControlCenter
        //      {
        //      ControlCenter ControlCenter
        //          {
        //          IP userrt
        //          }
        //      }
```

Resource Type

Following is the resource type definition: /etc/VRTSvcs/conf/config/**ControlCenterTypes.cf**

```
type ControlCenter (
       static str ArgList[] = { CCInstallDir, CCUser, CCPass, VirtualIP }
        str CCInstallDir
        str CCUser
        str CCPass
        str VirtualIP
)
```

It is also assumed that there is a shared storage area available or mountable to all nodes in the cluster where Control Center can be installed.

Installation

Perform the following steps before beginning the installation outlined in the *Control Center Getting Started Guide*:

1. Create a Control Center user with the user ID on each cluster node.
2. Create a Control Center subdirectory on the shared data file system.
3. Ensure that the Control Center subdirectory is owned by the Control Center user.

Configuration

Perform the following steps after installing Control Center in the subdirectory on the shared data file system:

1. For asset protection, acquire a key that includes the CPU-ID of all possible recovery machines.
2. Run configCC.sh. When prompted for the engine host name, enter the name of the dedicated Control Center Virtual IP Address. Example follows:

```
--------------------------------------------------------------------
Config step :  Servlet Container (JETTY) Configuration ...
               A valid keystore is needed for the secure connector server.
--------------------------------------------------------------------

Jetty (Servlet Container) has been already configured.

Do you want to re-configure Jetty (Servlet Container)(Y/N)?y

Are you sure(Y/N)?y

Jetty (Servlet Container) Connector configuration ...
Please provide numeric port value. [59182] :
Please provide numeric 'Secure' port value. (Enter 0 to disable) [0] :
Please provide engine host name. [server.csg.stercomm.com] : CC-virtual-ip-address
```

3. Place the following sample scripts in the **$VCS_HOME/bin/ControlCenter** directory. Update the scripts as required for your current environment. Copy the sample scripts to all nodes in the cluster.
4. Whenever you define a server via the Control Center console and specify SNMP connection information, always specify the *CC-virtual-ip-address* as the SNMP Listener Address (this is the address Control Center binds to when listening for SNMP traps).

Sample Scripts

The following agent scripts are the working examples from the Sterling Commerce test environment; they are provided as an example only. It is the user’s responsibility to write, test, and verify scripts appropriate to their environment. The scripts are named as follows:

- online

- offline
- monitor
- clean

Online Script

```
#!/bin/sh
# Name: online
#
# Purpose:     Start Control Center in Veritas HA cluster environment
#
# Arguments:   Input parameters are passed to the script as command line arguments.
#              The 1st argument is the name of the resource.
#             The 2nd-5th arguments contain the values of the resource Arglist attributes.
#
#              $1 = resource-name ("ControlCenter")
#              $2 = value of CCInstallDir
#              $3 = value of CCUser
#              $4 = value of CCPass
#              $5 = value of VirtualIP
#
# Return Code: 15
#
# 1. Set variable values from arguments passed to the script.
# 2. Start Control Center {CCInstallDir}/bin/./runEngine.sh
#          Note: The runEngine.sh command starts Control Center.
#                However, the actual Linux/Unix Control Center Process ID
#                is identifed as: ${CCInstallDir}/jre/bin/java.
# 3. exit 15 (to tell HA manager to wait 15 seconds before verifying online status).

# set -x       # test/debug - print shell script commands and their arguments

##############################################################################
# 1. Setup Variables for Control Center                                      #
##############################################################################
export CCInstallDir=$2
export CCUser=$3

##############################################################################
# 2. Start up Control Center                                                 #
##############################################################################
echo "Starting up Control Center."
su $CCUser -c "${CCInstallDir}/bin/./runEngine.sh"

##############################################################################
# 3. Return to monitoring agent, where: return code=n[n], integer specifying #
#    number of seconds to wait before monitor can check the state of the     #
#    resource: typically 0, that is, check resource state immediately.       #
#                                                                            #
#    Allow Control Center 15 seconds to initialize, before monitoring.       #
##############################################################################
exit 15
```

Offline Script

```
#!/bin/sh
# Name: offline
#
# Purpose:     Normal Stop Control Center in a Veritas HA cluster environment
#
# Arguments:   Input parameters are passed to the script as command line arguments.
#              The 1st argument is the name of the resource.
#              The 2nd-5th arguments contain the values of the resource Arglist attributes.
#
#              $1 = resource-name ("ControlCenter")
#              $2 = value of CCInstallDir
#              $3 = value of CCUser
#              $4 = value of CCPass
#              $5 = value of VirtualIP
#
# Return Code: 15
#
# Actions:
# 1. Set variable values from arguments passed to the script.
# 2. Stop Control Center {CCInstallDir}/bin/./stopEngine.sh
#         Wait up to 30 seconds to allow ControlCenter to stop.
# 3. Kill Control Center (if ./stopEngine command fails).
# 4. exit 15 (to tell HA manager to wait 15 seconds before verifying offline status).

##############################################################################
# 1. Setup Variables for Control Center                                      #
##############################################################################
export CCInstallDir=$2
export CCUser=$3
export CCPass=$4

##############################################################################
# 2. Stop Control Center:  ./stopEngine.sh -u $CCUser -p $CCPass            #
##############################################################################
ps -ef | grep ${CCUser} | grep ${CCInstallDir}/jre/bin/java | grep -v grep > /dev/null 2>&1
if [ $? -ne 0 ]
then
   echo "Control Center is not running, bypassing stopEngine command."
else
   echo "Issuing stopEngine command to Control Center."
   su $CCUser -c "${CCInstallDir}/bin/./stopEngine.sh -u ${CCUser} -p ${CCPass}"
   echo "Waiting for Control Center to stop."
   LOOP=0
   ps -ef | grep ${CCUser} | grep ${CCInstallDir}/jre/bin/java | grep -v grep > /dev/null
2>&1
   while [ $LOOP -lt 10 -a $? -eq 0 ]
   do
      echo "Control Center still running, waiting 3 seconds to recheck."
      sleep 3
      ((LOOP+=1))
      ps -ef | grep ${CCUser} | grep ${CCInstallDir}/jre/bin/java | grep -v grep > /dev/null
2>&1
   done
   if [ $LOOP -lt 10 ]
   then
      echo "Control Center stop successfull."
   else
      echo "Control Center stop unsuccessful."
   fi
fi
```

Offline Script (continued)

```
##############################################################################
# 3. KILL Control Center. if ./stopEngine.sh command was unsuccessful        #
##############################################################################
for I in `ps -ef | grep ${CCUser} | grep ${CCInstallDir}/jre/bin/java | grep -v grep | \
                   grep –v offline | awk ' { print $2 } ' `
do
   echo "Control Center ./stopEngine.sh command failed; killing pid $I"
   kill -9 $I
done

##############################################################################
# 4. Tell HA manager to wait 15 seconds before verifying offline status      #
##############################################################################
exit 15
```

Monitor Script

```
#!/bin/sh
# Name: monitor
#
# Purpose:     Monitors Control Center in a Veritas HA cluster environment
#
# Arguments:   Input parameters are passed to the script as command line arguments.
#              The 1st argument is the name of the resource.
#              The 2nd-5th arguments contain the values of the resource Arglist attributes.
#
#              $1 = resource-name ("ControlCenter")
#              $2 = value of CCInstallDir
#              $3 = value of CCUser
#              $4 = value of CCPass
#              $5 = value of VirtualIP
#
# Return Code: 110 if Control Center is running
#              100 if Control Center is absent
#
# Actions:
# 1. Set variable values from arguments passed to the script.
# 2. Queries system presence of: a) Control Center [CCInstallDir/jre/bin/java]
#                                b) Virtual IP Address assigned to CC

##############################################################################
# 1. Setup Variables for Control Center                                      #
##############################################################################
export CCInstallDir=$2
export CCUser=$3
export VirtualIP=$5

##############################################################################
# 2. Check for the presence of both: Control Center Process name             #
#                                    Control Center Virtual IP address       #
##############################################################################
echo "Checking for presence of Control Center."
ps -ef | grep ${CCUser} | grep ${CCInstallDir}/jre/bin/java | grep -v grep > /dev/null 2>&1
MonitorRC=$?
if [ $MonitorRC -ne 0 ]
then
   echo "Control Center is not present."
   exit 100
fi
echo "Control Center is present."

echo "Checking virtual IP accessibility."
ping -c 1 ${VirtualIP} > /dev/null 2>&1
if [ $? -eq 0 ]
then
   exit 110
else
   echo "Virtual IP not accessible, monitor failed."
exit 100
fi
```

Monitor Script (continued)

```
 echo "clean_reason = 4 - The resource was taken offline unexpectedly."
elif
   [ $CleanRsn -eq 5 ] ; then
   echo "clean_reason = 5 - The monitor entry point consistently failed to complete within 
the \
                            expected time."
else
   echo "clean_reason = $CleanRsn - Unknown reason code for calling clean script."
fi
```

Clean Script

```
#!/bin/sh
# Name: clean
#
# Purpose:     Force Stop Control Center in a Veritas HA cluster environment
#
# Arguments:   Input parameters are passed to the script as command line arguments.
#              The 1st argument is the name of the resource.
#              The 2nd argument is the cleanup reason code.
#             The 3rd-6th arguments contain the values of the resource Arglist attributes.
#
#              $1 = resource-name ("ControlCenter")
#              $2 = clean-reason-code
#              $3 = value of CCInstallDir
#              $4 = value of CCUser
#              $5 = value of CCPass
#              $6 = value of VirtualIP
#
# Return Code: 0 if Control Center is down
#              1 if Control Center is still up
#
# Actions:
# 1. Set variable values from arguments passed to the script.
# 2. Determine/Display reason for HA calling the cleanup script.
# 3. Issues Stop to Control Center (waits up to 10 seconds to allow Control Center to stop).
# 4. Kills Control Center Engine, if required.  This step is to ensure HA resources are
freed.
# 5. If Control Center remains up, exit 1, else exit 0.

##############################################################################
# 1. Setup Variables for Control Center                                      #
##############################################################################
export CleanRsn=$2
export CCInstallDir=$3
export CCUser=$4
export CCPass=$5
export VirtualIP=$6

##############################################################################
# 2. Display clean_reason: Code/Description of why HA called the clean agent #
##############################################################################
if [ $CleanRsn -eq 0 ] ; then
   echo "clean_reason = 0 - The offline entry point did not complete within the expected
time."
elif
   [ $CleanRsn -eq 1 ] ; then
   echo "clean_reason = 1 - The offline entry point was ineffective."
elif
   [ $CleanRsn -eq 2 ] ; then
   echo "clean_reason = 2 - The online entry point did not complete within the expected time.
"
elif
   [ $CleanRsn -eq 3 ] ; then
   echo "clean_reason = 3 - The online entry point was ineffective."
elif
   [ $CleanRsn -eq 4 ] ; then
```

Clean Script (continued)

```
###############################################################################
# 3. Stop Control Center:  ./stopEngine.sh -u $CCUser -p $CCPass              #
###############################################################################
ps -ef | grep ${CCUser} | grep ${CCInstallDir}/jre/bin/java | grep -v grep > /dev/null 2>&1
if  [ $? -ne 0 ] ; then
   echo "Control Center is not running, bypassing stopEngine command."
else
   echo "Issuing stopEngine command to Control Center."
   su $CCUser -c "${CCInstallDir}/bin/./stopEngine.sh -u ${CCUser} -p ${CCPass}"
   echo "Waiting for Control Center to stop."
   LOOP=0
   ps -ef | grep ${CCUser} | grep ${CCInstallDir}/jre/bin/java | grep -v grep > /dev/null
2>&1
   while [ $LOOP -lt 10 -a $? -eq 0 ]
   do
      echo "Control Center still running, waiting 3 seconds to recheck."
      sleep 3
      ((LOOP+=1))
      ps -ef | grep ${CCUser} | grep ${CCInstallDir}/jre/bin/java | grep -v grep > /dev/null
2>&1
   done
   if [ $LOOP -lt 10 ]
   then
      echo "Control Center stop successfull."
   else
      echo "Control Center stop unsuccessful."
   fi
fi

###############################################################################
# 4. KILL Control Center, if necessary                                        #
#    (i.e. if ./stopEngine.sh command was unsuccessful)                       #
###############################################################################
for I in `ps -ef | grep ${CCUser} | grep ${CCInstallDir}/jre/bin/java | grep -v grep | \
                                    grep -v clean | awk ' { print $2 } ' `
do
   echo "Control Center ./stopEngine.sh command failed; killing pid $I"
   kill -9 $I
done

###############################################################################
# 5. Report clean up status                                                   #
###############################################################################
ps -ef | egrep "${CCInstallDir}/jre/bin/java" | grep -v grep | grep -v clean > /dev/null 2>&1
ALL_DOWN=$?
if [ $ALL_DOWN -ne 0 ]
then
echo "Control Center is down."
   exit 0
else
   echo "Control Center is NOT down."
   exit 1
fi
```

Failover Test Scenarios

The following failover test scenarios were initiated and failover was triggered via the following mechanisms:

- Stop Control Center on system A via command line: “./stopEngine.sh”.
  a. Validated Control Center restarted on system A (for OnlineRetryLimit iterations).
  b. Validated Control Center failed over to system B (after OnlineRetryLimit exceeded).
- Kill Control Center on system A via command line: “kill -9 pid”.
  a. Validated Control Center restarted on system A (for OnlineRetryLimit iterations).
  b. Validated Control Center failed over to system B (after OnlineRetryLimit exceeded).
- Shut down the computer on which Control Center is running.

  Validated Control Center failed over to the other system.
- Pull the network cable on the cluster running Control Center.

  Validated Control Center failed over to the other system.

Appendix M

Keys and Fields

In Sterling Control Center, you can specify a key to define the criteria for a report, rule or SLC, or to act as a filter to limit the number of items that display in many Control Center listings. A parameter consists of a key, an operator, and a value. For more information, see *Filter Objects* on page 19.

Statistics, properties, and other system-generated information are displayed in various listings, Activity Monitors, and Process Monitors to give you information about alerts, file transfers, business processes, and other status information. These informational fields are also in this appendix.

The keys and fields are listed in alphabetic order. For each key or field, a brief description is provided along with server-specific information, if applicable. For some items, mapping of terms is included to translate values to a specific server type. Note that not all keys are available for use in all situations.

Key/Field	Description
Action	Action performed on Control Center entity.
Actions Flag	Time stamp indicated when event processing completed.
Activity Type	The type of activity an SLC event is associated with. Possible values include: ◆ WF = Workflow ◆ M = Milestone ◆ P = Process ◆ S = Process Step
Alert level	The severity level of the Alert. Possible values include: ◆ 1 = High ◆ 2 = Medium ◆ 3 = Low
Batch ID	Batch identifier used in Connect:Enterprise.

Key/Field	Description
Batch Number	Batch number used in Connect:Enterprise.
Bytes Read	Number of bytes read from the source file by the sending server.
Bytes Received	Number of bytes received by the receiving server.
Bytes Sent	Number of bytes sent by the sending server to the receiving server.
Bytes Written	Number of bytes written to the destination file by the receiving server.
Check Point (Y or N)	Indicates if the checkpoint feature of Connect:Direct is enabled to facilitate recovery should an interruption in data transfer occur.
Condition Code	Return code associated with Process steps and Process ends. Possible values include: ◆ 0 = Successful execution. ◆ 4 = A warning-level error was encountered. ◆ 8 = An error occurred during execution. ◆ 16 = A catastrophic error occurred during execution.
Control Center Name	Name of the Sterling Control Center engine.
Cipher Suite	The cipher suite, such as SSL_RSA_WITH_DES_CBC_SHA, used in secure Connect:Direct sessions.
Daemon Host	DNS host name or IP address of the system the Connect:Enterprise daemon is on.
Daemon Name	Name of the Connect:Enterprise daemon.
Daemon Originator	Originator of the Connect:Enterprise daemon. Same as Remote ID.
Daemon PID	Process identifier of the Connect:Enterprise daemon.
Daemon Resource	Resource of the Connect:Enterprise daemon.
Daemon SID	Session identifier of the Connect:Enterprise daemon.
Daemon State	State of the Connect:Enterprise daemon.
Daemon Type	Type of the Connect:Enterprise daemon. Control Center monitors only daemons of type master.
Data Visibility Group	Name of the data visibility group. **Note:** If the user creating a rule or SLC is data visibility restricted, a data visibility group must be specified.
Date Time	The date and time that the event was generated. For FTP W3C servers and IIS logs, this can be the date and time when the event started or ended. For date and time for end events, this is the date time plus the time taken.
Days Before Expiry	Number of days before a certificate expires.

Key/Field	Description
Dest Disp1	The status of the destination file before the transfer begins.
Destination File	Destination file name. For Connect:Direct, the file name at the destination in a copy step of a Process. For Connect:Enterprise the file name if received by Connect:Enterprise or the userid requesting the file if sent by Connect:Enterprise. For FTP, in a PUT, the name of the file as found in the FTP transfer log. In a GET, the ID of the user who initiated the transfer. For FTP W3C servers, in the case of an inBound destination file, check the cs-uri-stem if the FTP command is in the cs-method field; else, check the cs-uri-query field. For FTP W3C servers, in the case of an outBound destination file, check the cs-username if available; else, check the c-ip field. For FTP IIS logs, in the case of an inBound destination file, check the cs-uri-stem. in the case of an outBound destination file, check the cs-username field.
Direction(InBound or outBound)	Indicates direction of Sterling Integrator and FTP file transmissions. For FTP W3C servers, depends on the FTP command. SENT, RETR, GET and DOWNLOADED commands are considered inbound. CREATED, STOR, STOU, PUT, UPLOADED, APPE, and APPENDED commands are considered outbound. For FTP II logs, depends on the FTP command in the cs-method field.
EMail Flag	Indicates when email action processing completed.
Event ID	The ID number assigned by the system to each event.
Event ID/Number	The ID number assigned by the system to each event.
Event Type	A code indicating the type of event. See Event Type Descriptions for a listing of event types and descriptions.
Executing Processes	The number of Processes in the Execution queue.
Extended Compression	Indicates if the extended compression was used while transferring the file.
Feedback	The feedback code generated from a Connect:Direct Process statement.
fgActivityType	The activity associated with the File Gateway file transfer. Possible values include: ◆ A = Arrival ◆ R = Route ◆ D = Delivery

Key/Field	Description
FG.Activity (A or R or D)	The activity associated with the File Gateway file transfer. Possible values include: ◆ A = Arrival ◆ R = Route ◆ D = Delivery
FG.Arrived File Name	The name of the arrived file involved in the File Gateway file transfer.
FG.Arrived File Status	The status of the arrived file involved in the File Gateway file transfer. Possible values include: ◆ Arrived ◆ Failed ◆ Ignored
FG.Consumer	The name of the partner who received the arrived file involved in the File Gateway file transfer.
FG.Data Flow ID	The ID of a data flow document associated with a correlation entry or file transfer event.
FG.DOCUMENT_ID	File Gateway Arrived File Document ID
FG.Event Code	The File Gateway equivalent of a message ID.
FG.FILE_NAME	File Gateway Arrived File Name.
FG.FILE_SIZE	File Gateway Arrived File Size.
FG.PROD_ORG_KEY	File Gateway Producer Org Key.
FG.Producer	The name of the partner who created and sent the arrived file involved in the File Gateway file transfer.
FG.REVIEWED	File Gateway Reviewed Arrived File
FG.ROUTES_REMAIN	File Gateway Remaining Routes
FG.ROUTE_EVENT_KEY	File Gateway Route Event Key
FG.STATE	File Gateway Arrived File State
FG.TIME	File Gateway Event Time
FG.WFID	File Gateway Arrived File Workflow ID
File Agent Name	The unique name for the file agent specified during file agent configuration.
File Agent Rule	The rule configured on File Agent that determines which Process to use to submit the file to Connect:Direct.
File Agent Trigger File	The file that triggers the rule or the default Process.

Key/Field	Description
File Gateway Time	Date and time that events occurred in Sterling File Gateway. Format: *yyyy/mm/dd hh:mm:ss.msmsms (*UTC +/- *hhmm)*.
File Size	Size of file transferred in bytes. For FTP W3C servers and IIS logs, file size = cs-bytes + sc-bytes (or 0 if neither is available). For WS_FTP servers, this information is not available.
From Node	Indicates which server, local or remote, is sending the file. When the value is P, the server initiating the Process is the sender; otherwise, the server initiating the Process is the receiver. ◆ P = PNODE ◆ S = SNODE
From Server	Same as From Node.
ftpLogRecord	Actual contents of the FTP log record that caused the event to be generated. For FTP W3C servers and IIS logs, (date time GMT) plus all fields from the log. **Note:** For more information on the contents of FTP logs, see the sections on *FTP xferlog and IIS Log Formats* and *W3C FTP Server Logs* in the *Sterling Control Center Getting Started Guide*.
Group ID	SLC Name
In Error	Indicates that one or more activities within a Sterling Integrator business process failed. ◆ True ◆ False
Is BP	Indicates if the event is associated with a Sterling Integrator business process. ◆ True ◆ False
Link Fail	Indicates if a communications error occurred. ◆ True ◆ False

Local Node (P or S)	The server that processed the file.
	P = Primary
	S = Secondary

Local Condition Code	The local Connect:Direct server’s return code.
Local Message ID	The local Connect:Direct server’s message ID.

Key/Field	Description
Local Server	The name of the local Connect:Direct server
Log Date/Time	Date and time that the event occurred. Format: *yyyy/mm/dd hh:mm:ss.msmsms (*UTC *+/- hhmm)*. For Sterling File Gateway, this is the date and time that events got logged into the database. To see a chronological listing of events, open the Statistics viewer, right-click a column heading, select **Manage Columns**, and add **File Gateway Time** to Selected Columns. To sort, right-click the File Gateway Time column.
Message	The server or Sterling Control Center message ID issued with the event.
Message ID	The server or Sterling Control Center message ID issued with the event. For Sterling File Gateway, Event Code is mapped to Message ID.
Message Text	Message description.
Minutes Since Last Submit	Number of minutes since the previous submission to the File Agent.
Name	Same as Process name.
Node Type	The code indicating the type of server. The server types are: ◆ 0 = Sterling Control Center ◆ 1 = Connect:Direct ◆ 2 = Connect:Enterprise ◆ 3 = Sterling Integrator ◆ 4 = FTP
Non-Executing Processes	The number of Processes not being executed, that is, in the Wait, Hold, or Timer queues.
Number	Same as Process number.
Orig Node	The originating node of a Connect:Direct or Sterling Integrator Process. For FTP W3C servers, check the cs-username field if available; else the c-ip field. For FTP IIS logs, check the cs-username field if available.
Originating Node/Server	The name of the server or node (PNODE) that initiated the process. For FTP, the submitter ID. User ID of user initiating the work.
Other Condition Code	The remote Connect:Direct server’s return code.
Other Message ID	The remote Connect:Direct server’s message ID.
Percent Complete	For Connect:Direct servers, the percent complete of the file copy or transfer. Relevant only to events with the event type of Process Status.

Key/Field	Description
Pnode	The Connect:Direct primary node.
Pnode Acct Info	Accounting information associated with the Connect:Direct primary node.
Process ID	For Sterling File Gateway, the ID for the business process. For Connect:Direct, same as Process number.
Process Name	The name of the Process or batch ID. (The name of an FTP Process is always either GET or PUT.) For FTP W3C servers, this comes from the cs-method field if available; else the cs-uri field. For FTP IIS logs, this comes from the cs-method field.
Process Name/Batch ID	This key or field maps to the following values: ◆ Process name (Connect:Direct) ◆ Business Process name (Sterling Integrator) ◆ Batch ID (Connect:Enterprise) ◆ GET or PUT (FTP servers) ◆ Arrived File Name (Sterling File Gateway)
Process Number	The number identifying the process.
Queue ID	In Connect:Direct, there are four processing queues: Exec, Hold, Timer, and Wait. In Sterling Integrator, there 10 queues: Q0 through Q9.
Record Category	Statistics record category. Possible values include: ◆ CAEV=The record is related to a Connect:Direct event, such as a Connect:Direct shutdown. ◆ CAPR=The record is related to a Connect:Direct Process.
Record ID	The record (or statistic ID) used to indicate what Connect:Direct activities produce associated Control Center event types, for example, CH (Change Process) has an Event type of Server Command. For more information, see *Event Type—Connect:Direct Statistic Record ID Cross-Reference* on page 179.
Records Read	The number of records read from the source file.
Records Written	The number of records written to the destination file.
Remote Node/Server	The server or remote node name involved in a Process or file transfer. For Connect:Direct, the remote node is the SNODE name. For Connect:Enterprise, the remote node is the recipient mailbox ID.
Remote Server	The remote server name.
Restart	Indicates if the restart feature of Connect:Direct is enabled to facilitate recovery should an interruption in data transfer occur.

Key/Field	Description
Restart (Y or N)	Indicates if the restart feature of Connect:Direct is enabled to facilitate recovery should an interruption in data transfer occur.
Return Code	Same as condition code. Return code associated with Process steps and Process ends. Possible values include: ◆ 0 = Successful execution. ◆ 4 = A warning-level error was encountered. ◆ 8 = An error occurred during execution. ◆ 16 = A catastrophic error occurred during execution. For FTP W3C servers, this comes from the sc-win32-status field if available; else, sc-status field. For FTP IIS logs, this comes from the sc-win32-status field if available.
RUS Received	The number of buffers received by the destination server.
RUS Sent	The number of buffers sent to the destination file by the sending server.
RU Size	In Connect:Direct, the size of blocks in number of bytes sent in a transmission.
Rule ID	The name of the rule triggered by the event.
Secure Enabled (Y or N)	Indicates if the Secure+ Option feature for a Connect:Direct file transfer was enabled.
Secure Protocol	The protocol, such as TLS or SSL, used in secure Connect:Direct sessions.
Sequence	For Sterling File Gateway, the sequence number.
Sequence Number	Sequence number of the statistics record.
Server	Actual name of monitored server.
Server Alias	Monitored server name used by Control Center.
Server Data/Metadata 1-10	Server metadata fields for analyzing server information according to the needs of your organization. See *Manage Metadata* on page 129.
Server Groups	Control Center server group names.
Server ID	The name or alias of the server.
Server ID/Server Alias	Sterling Control Center Name/Alias of managed server.
Server Name	Name of the managed server.

Key/Field	Description
Server Type	The type of server. (Also same as NodeType event element variable.) ◆ 1 Connect:Direct ◆ 2 Connect:Enterprise ◆ 3 Sterling Integrator ◆ 4 FTP
Server Type Name	Type of Server.
SESSION.ADAPTER_DISPLAY_NAME	For a protocol activity, the display name for the Sterling Integrator adaptor.
SESSION.ADAPTER_NAME	For a protocol activity, the system name for the Sterling Integrator adaptor.
SESSION.ADAPTER_TYPE	For a protocol activity, the display name for the Sterling Integrator adaptor.
SESSION.CON_END_TIME	For a protocol activity, the time the Sterling Integrator session connection ended.
SESSION.CON_IS_SUCCESS	For a protocol activity, indicates the Sterling Integrator session connection was successful.
SESSION.DIS_IS_SUCCESS	For a protocol activity, indicates the Sterling Integrator session disconnection was successful.
SESSION.DIS_START_TIME	For a protocol activity, the time the Sterling Integrator session disconnection started.
SESSION.END_WFID	For a protocol activity, the workflow ID for the Sterling Integrator session end.
SESSION.END_WFSTEP	For a protocol activity, the workflow step for the Sterling Integrator session end.
SESSION.ENDPOINT1	Sterling Integrator session end point 1.
SESSION.ENDPOINT2	Sterling Integrator session end point 2.
SESSION.ENDPORT1	Sterling Integrator session end port 1.
SESSION.ENDPORT2	Sterling Integrator session end port 2.
Short Msg	The short message text of a message ID. (Also same as shortText event element variable.)
Short Text	Message text associated with the Message ID.
SI.Adapter Name	Name of the Sterling Integrator adapter.
SI.Adapter Type	Type of Sterling Integrator adapter.
SI.Document Name	Name of the business document that the business Process works on.

Key/Field	Description
SI.Is Put(true/false)	Indicates if a file to a Sterling Mailbox Direct was delivered successfully.
SI.Mailbox Path	A storage area path for business documents. The Sterling Integrator mailbox path provides an administrative hierarchy that is easy to manage and understand.
SI.Message ID	Message ID of the business information communicated through the business Process.
SI.Message Name	Name of the business information communicated through the business Process.
SI.Process Data	Data that is accumulated in an XML document about a business process during the life of the process.
SI.Session Protocol	Protocol that the adapter handles.
SI.Type	For Sterling Integrator server, indicates the source of the event: ◆ FG = File Gateway ◆ BP = Business Process ◆ PR = Protocol
SLC Flag	Indicates when SLC processing completed.
SLC ID	A system-assigned name of the SLC that triggered the event.
SLC Identification	A system-assigned name of the SLC that triggered the event.
SLC Instance ID	Unique SLC identifier. Includes the SLC name, schedule name, and unique number.
SLC Name	The name of the SLC.
SLC Source 1	SLC recovery data 1
SLC Source Event ID	A system assigned number that identifies the SLC that triggered the event. Used by the system to relate multiple SLC events to the same SLC source.
SLC Source Event Time	The time that the event triggering an SLC event occurred.
Snode	The secondary Connect:Direct server involved in the Process. The initiating node in a Process is the Pnode, or primary node.
Snode Acct Info	Accounting information associated with the Connect:Direct secondary node.

Key/Field	Description
Source File	For a Connect:Direct server, the source file name in a Copy. Also the target in a Submit, Run Task, or Run Job Connect:Direct Process step. For Connect:Enterprise, the file name if sent by Connect:Enterprise or the userid sending the file if received by Connect:Enterprise. For FTP, in a PUT, the ID of the user who did the transfer. In a GET, the name of the file received. For FTP W3C servers, in the case of an inBound source file, this comes from the cs-username field if available; else this comes from the c-ip field. For FTP W3C servers, in the case of an outBound source file, this comes from the cs-uri-stem field if the FTP command is in the cs-method field; else, this comes from the cs-uri-query field. For FTP IIS logs, in the case of an inBound source file, this comes from the cs-username field. In the case of an outBound source file, this comes from the cs-uri-stem field.
Standard Compression	Indicates if the standard compression was used while transferring the file.
Start Time	The date and time the event started.
Start Date/Time	The date and time the event started.
Step Name	The Connect:Direct Process step name or Sterling Integrator business Process activity. **Note:** This key cannot be used for Connect:Direct OS/400.
Stop Time	The date and time the event stopped.
Stop Date/Time	The date and time the event stopped.
Submit Node	The server name that initiated the Process.
Submitter/ID	The name or user ID of the person who submitted the Process or Connect:Enterprise mailbox.
SUBMITTER NODE	The name of the node the Process was submitted from.
Translation	For Connect:Direct, the type of translation performed for a Process copy.
trapFlag	Indicates when trap operation action completed.
Type	◆ For Sterling Integrator server, the type of activity. ◆ FG = File Gateway ◆ BP = Business Process ◆ PR = Protocol
User Data 1–4	Metadata fields for analyzing activity in ways unique to your organization. See *Manage Metadata* on page 129.

Key/Field	Description
userOpFlag	Indicates when a user operation action completed.
WF.ACTIVITYINFO_ID	Business Process Activity Info ID.
WF.BASIC_STATUS	Business Process basic status.
WF.END_TIME	Business Process end time.
WF.NEXT_AI_ID	Business Process next AI ID.
WF.NODEEXECUTED	Node where Business Process executed.
WF.SERVICE_NAME	Service name in Business Process.
WF.START_TIME	Business Process / Business Process Step start time
WF.STEP_ID	Business Process step ID.
WF.WFD_ID	Business Process WFD ID.
WF.WFD_NAME	Business Process WFD name.
WF.WFD_VERSION	Business Process WFD version.
WF.WFE_STATUS	Business Process execution status
WF.WORKFLOW_ID	Business Process instance ID
WFD_NAME	Business Process name

Appendix N

Collecting Sterling Integrator Process Data

During the life of a business process Sterling Integrator collects process data in an XML document, which can become quite large. Typically, business processes act on the document or payload data, such as a customer's purchase order, and extract information from the document and place it in the process data. Process data can be used for various purposes including determining what the next step of the business process will be.

Sterling Control Center can track elements and components within the process data, such as the name of a file being transferred or a purchase order number. When you select a specific business process to monitor on a Sterling Integrator server, you can specify the Process Data XPath to enable Control Center to access the information you need in the process data XML document. The extracted process data is part of the other statistics elements collected for each business process step.

Using Collected Process Data

You can also use the collected process data in rules, metadata rules, SLCs, and reports. Note the following items related to using process data in Control Center:

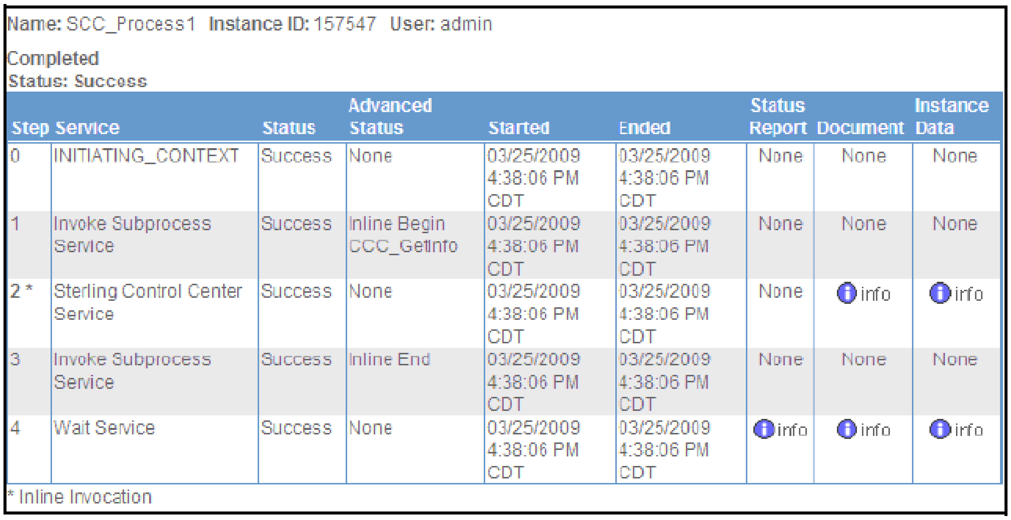
- The element name in Control Center event for the process data is SI.Process Data.
- The XPath must always start with the prefix, /ProcessData, for example, /ProcessData/FTPClientBeginSessionServiceResults/ServerResponse/Text.
- Only one XPath can be specified for a specific business process in Control Center.
- If a business process (parent) invokes another business process (child), you must specify the same XPath for both the parent and child business processes to collect the process data for all the steps in a workflow instance.

The following XML document example of a parent business process (SCC_Process1) invokes a child business process (CCC_GetInfo) in INLINE mode:

```
<process name="SCC_Process1">
  <sequence>
    <operation>
      <participant name="InvokeSubProcessService" />
      <output message="Xout" >
        <assign to="INVOKE_MODE">INLINE</assign>
        <assign to="WFD_NAME">CCC_GetInfo</assign>
      </output>
      <input message="Xin" >
        <assign to="." from="*"></assign>
      </input>
</operation>

<operation name="Wait">
      <participant name="WaitService"/>
      <output message="WaitServiceTypeInputMessage">
        <assign to="WAIT_INTERVAL">2</assign>
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
```

The following sample Sterling Integrator screen shows the steps when business process SCC_Process1 is executed:



Name: SCC_Process1 **Instance ID:** 157547 **User:** admin

Completed
Status: Success

Step	Service	Status	Advanced Status	Started	Ended	Status Report	Document	Instance Data
0	INITIATING_CONTEXT	Success	None	03/25/2009 4:38:06 PM CDT	03/25/2009 4:38:06 PM CDT	None	None	None
1	Invoke Subprocess Service	Success	Inline Begin CCC_GetInfo	03/25/2009 4:38:06 PM CDT	03/25/2009 4:38:06 PM CDT	None	None	None
2 *	Sterling Control Center Service	Success	None	03/25/2009 4:38:06 PM CDT	03/25/2009 4:38:06 PM CDT	None	ℹ info	ℹ info
3	Invoke Subprocess Service	Success	Inline End	03/25/2009 4:38:06 PM CDT	03/25/2009 4:38:06 PM CDT	None	None	None
4	Wait Service	Success	None	03/25/2009 4:38:06 PM CDT	03/25/2009 4:38:06 PM CDT	ℹ info	ℹ info	ℹ info

* Inline Invocation

In this example, Step 2 is part of business process CCC_GetInfo. To collect process data for all steps of Instance ID 157547, the XPath must be specified for both SCC_Process1 and CCC_GetInfo.

Reference Information in the Sterling Control Center Documentation Set

For more information on:

Topic	Go to Document, Section
Process data and using XPath to access process data	Extensive documentation on Sterling Integrator is available in Customer Center. From the main Sterling Integrator Documentation home page, go to: ◆ Use Sterling Integrator to... > Manage Business Processes ◆ Understanding BPML > Process data ◆ Understanding BPML > XPATH and process data
How to specify the XPATH for a monitored business process	*Sterling Control Center System Administration Guide*, *Managing Servers* chapter

Appendix O

Monitoring File Transfers Performed by Sterling File Gateway

Sterling Control Center can monitor the following Sterling File Gateway (SFG) activities:

- Arrived File events
- Route events
- Delivery events

Monitoring File Gateway Activities

The underlying platform for File Gateway is Sterling Integrator. To monitor File Gateway activities, add a Sterling Integrator server and specify the Monitor File Gateway option on the Settings panel. If you are already monitoring the underlying Sterling Integrator server and want to monitor File Gateway activities, update the settings for the Sterling Integrator server by clicking the Monitor File Gateway option.

Related to File Gateway activities, Control Center also allows monitoring activities of Mailbox Service, MBI (Mailbox Browser Interface). File Gateway uses Mailbox Service to place files in mailboxes. You can monitor those activities by selecting the Mailbox Service protocol in the server settings panel.

Viewing File Gateway Activities

For each arrived file, depending on its status, an entry may appear either in the Queued Activity Monitor or Completed Activity Monitor. To view all arrived file events, route events, and delivery events for a particular arrived file, right-click on the item in the activity monitor, and choose **Select Statistics**. To see a chronological listing of events, right-click a column heading, select **Manage Columns**, and add File Gateway Time to Selected Columns. To sort, right-click the File Gateway Time column. The Log Date/Time column displays when the event was logged in the database where as the File Gateway Time column displays when the event occurred.

In the Activity Monitor display panels, the SI.Type field can show one of the following types of activity for a Sterling Integrator server:

- FG indicates a File Gateway activity.
- BP indicates a business process activity.
- PR indicates a protocol activity.

File Gateway activities are collected using the following File Gateway database tables:

- FG_ARRIVEDFILE
- FG_ROUTE
- FG_DELIVERY
- FG_ROUTE_EVENT
- FG_EVENT_ATTR

Statistics Viewer

All File Gateway source information is displayed in the Control Center Statistics Viewer. In the Statistics Viewer, fields with the prefix FG relate to columns in File Gateway database tables.

File Gateway Terms

The following File Gateway terms are mapped to standard Control Center terms in the Activity Monitor displays:

- SFG Arrived File is mapped to Process Name.
- SFG Event Code is mapped to Message ID in statistics.
- The return codes for the arrived file and its events are based on status and are set to either 0 (completed) or 8 (failed).

Reference Information in the Sterling Control Center Documentation Set

For more information on:

Topic	**Go to Document, Section**
The Monitor File Gateway option	*Sterling Control Center System Administration Guide*, *Managing Servers* chapter
How to translate the fields shown in Control Center statistics into SFG terms	*Sterling Control Center System Administration Guide*, *Keys and Fields* appendix
Sterling File Gateway Route Detail by Producer Report and Route Detail by Consumer Report	*Sterling Control Center Reports Guide, Standard Reports* chapter
Scenarios involving Sterling File Gateway	See *Sterling Control Center How-To Guide*

Index