System Logging

Modified: 2016-12-29

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

System Logging

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation ix
Documentation and Release Notes ix
Supported Platforms ix
Documentation Conventions ix
Documentation Conventions x
Documentation Feedback xii
Requesting Technical Support xii
Self-Help Online Tools and Resources xiii
Opening a Case with JTAC xiii

Part 1 Overview

Chapter 1 **Software Features Overview 3**

SRC Component Overview 3

Chapter 2 **System Logging 7**

C Series Controller Log Server Overview 7
Message Groups 7
Severity Levels 8

Part 2 Configuration

Chapter 3 **Configuration Tasks 11**

Before You Configure System Logging (SRC CLI) 11
Saving System Log Messages to a File (SRC CLI) 11
Saving System Log Messages to a File (C-Web Interface) 12
Sending System Log Messages to Other Servers (SRC CLI) 13
Sending System Log Messages to Other Servers (C-Web Interface) 14
Sending Notifications for System Log Messages to Users (SRC CLI) 14
Sending Notifications for System Log Messages to Users (C-Web Interface) 15

Chapter 4 **Configuration Statements 17**

Configuration Statements for System Logging on a C Series Controller 17

Part 3 Administration

Chapter 5 **Routine Monitoring 21**

Viewing the System Date and Time (C-Web Interface) 21

List of Figures

Part 3 Administration

Chapter 5 Routine Monitoring 21

Figure 1: C-Web Interface for Monitoring System Date and Time 21

List of Tables

About the Documentation ix
Table 1: Notice Icons x
Table 2: Notice Icons xi
Table 3: Text Conventions xi

Part 1 Overview

Chapter 1 Software Features Overview 3
Table 4: Descriptions of SRC Components 3

About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xii
- Requesting Technical Support on page xii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- Virtualized SRC

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Documentation Conventions

Table 1 on page x defines the notice icons used in this guide. Table 3 on page xi defines text conventions used throughout this documentation.

Table 2: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 3: Text Conventions

Convention	Description	Examples
Bold text like this	• Represents keywords, scripts, and tools in text. • Represents a GUI element that the user selects, clicks, checks, or clears.	• Specify the keyword **exp-msg**. • Run the **install.sh** script. • Use the **pkgadd** tool. • To cancel the configuration, click **Cancel**.
Bold text like this	Represents text that the user must type.	**user@host# set cache-entry-age** *cache-entry-age*

`Fixed-width text like this`	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	`nic-locators {`
		`  login {`
		`  resolution {`
		`  resolver-name /realms/`
		`  login/A1;`
		`  key-type LoginName;`
		`  value-type SaeId;`
		`  }`

Regular sans serif typeface	• Represents configuration statements. • Indicates SRC CLI commands and options in text. • Represents examples in procedures. • Represents URLs.	• **system ldap server{ stand-alone;** • Use the **request sae modify device failover** command with the **force** option • **user@host# . . .** • http://www.juniper.net/techpubs/software/management/sdx/api-index.html

Table 3: Text Conventions *(continued)*

Italic sans serif typeface	Represents variables in SRC CLI commands.	**user@host# set local-address *local-address***
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <gfwif>.
Key name	Indicates the name of a key on the keyboard.	Press Enter.
Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Italic typeface	• Emphasizes words. • Identifies book names. • Identifies distinguished names. • Identifies files, directories, and paths in text but not in command examples.	• There are two levels of access: *user* and *privileged*. • *SRC-PE Getting Started Guide.* • *o=Users, o=UMC* • The */etc/default.properties* file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class=\ net.juniper.smgt.sae.plugin\ RadiusTrackingPluginEvent
Words separated by the | symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic | line

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

- Software Features Overview on page 3
- System Logging on page 7

CHAPTER 1

Software Features Overview

- SRC Component Overview on page 3

SRC Component Overview

The SRC software is a dynamic system. It contains many components that you use to build a subscriber management environment. You can use these tools to customize and extend the SRC software for your use and to integrate the SRC software with other systems. The SRC software also provides the operating system and management tools for C Series Controllers.

Table 4 on page 3 gives a brief description of the components that make up the SRC software.

Table 4: Descriptions of SRC Components

Component	Description
Server Components	
Service activation engine (SAE)	• Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modem termination system (CMTS) devices, RADIUS servers, and directories. • Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases. • Provides plug-ins and application programming interfaces (APIs) for starting and stopping subscriber and service sessions and for integrating with systems that authorize subscriber actions and track resource usage.
Subscriber Information Collector (SIC)	The SIC listens for RADIUS accounting events from IP edge devices (accounting clients) and forwards them to a remote AAA server, allowing the SRC software to gain increased subscriber awareness. Additionally, the SIC can optionally edit accounting events before routing them.
Juniper Policy Server (JPS)	Acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and CMTS devices in a PCMM environment.
Network information collector (NIC)	Collects information about the state of the network and can provide a mapping from a given type of network data to another type of network data.
Redirect Server	Redirects HTTP requests received from IP Filter to a captive portal page.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
3GPP Gateway	The SRC Third-Generation Partnership Project (3GPP) gateway is a Diameter-based component in the SRC software, which provides integration with 3GPP Policy and Charging Control environments, to provide fixed-mobile convergence (FMC). The SRC 3GPP gateway provides Gx-based integration with the Policy and Charging Rules Function (PCRF). The SRC 3GPP gateway uses the northbound Gx interface to mediate between the PCRF and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The northbound Gx interface on the SRC 3GPP gateway communicates with the PCRF using the Diameter protocol.
3GPP Gy	The SRC 3GPP Gy is a Diameter-based component in the SRC software, which provides Gy-based integration with the Online Charging System (OCS), to provide FMC. The SRC 3GPP Gy uses the northbound Gy interface to handle charging-related information between the OCS and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The northbound Gy interface communicates with the OCS using the Diameter protocol.
Web Application Service	The SRC software includes a Web application server that hosts the Web Services Gateway and the Volume Tracking Application (SRC VTA). In production environments, this application server is designed to host only these applications. However, you can load your own applications into this server for testing or demonstration purposes.
Web Services Gateway	Allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a Simple Object Access Protocol (SOAP) interface. The Web Services Gateway provides the Dynamic Service Activator which allows a gateway client to dynamically activate and deactivate SRC services for subscribers and to run scripts that manage the SAE.
Repository	
Directory	The SRC software includes the Juniper Networks database, which is a built-in Lightweight Directory Access Protocol (LDAP) directory for storing all SRC data including services, policies, and small subscriber databases. For large subscriber databases, you must supply your own directory.
SRC Configuration and Management Tools	
SRC command line interface (CLI)	Provides a way to configure the SRC software on a C Series Controller from a Junos OS–like CLI. The SRC CLI includes the policies, services, and subscribers CLI, which has separate access privileges.
C-Web interface	Provides a way to configure, monitor, and manage the SRC software on a C Series Controller through a Web browser. The C-Web interface includes a policies, services, and subscribers component, which has separate access privileges.
Simple Network Management Protocol (SNMP) agent	Monitors system performance and availability. It runs on all the SRC hosts and makes management information available through SNMP tables and sends notifications by means of SNMP traps.
Service Management Applications (Run on external system)	
IMS Services Gateway	Integrates into an IP multimedia system (IMS) environment. The SRC software provides a Diameter protocol-based interface that allows the SRC software to integrate with services found on the application layer of IMS.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
SRC Programming Interfaces	
NETCONF API	Allows you to configure or request information from the NETCONF server on a C Series Controller that runs the SRC software. Applications developed with the NETCONF API run on a system other than a C Series Controller.
CORBA plug-in service provider interface (SPI)	Tracks sessions and enables linking the rest of the service provider's operations support system (OSS) with the SRC software so that the OSS can be notified of events in the life cycle of SAE sessions. Hosted plug-ins only.
CORBA remote API	Provides remote access to the SAE core API. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
NIC access API	Performs NIC resolutions. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
SAE core API	Controls the behavior of the SRC software. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
Script services	Provides an interface to call scripts that supply custom services such as provisioning policies on a number of systems across a network.
VTA API	The Volume Tracking Application (VTA) API is a Simple Object Access Protocol (SOAP) interface that allows developers to create gateway clients and that administrators use to manage VTA subscribers and sessions. The SRC Web Services Gateway allows a gateway client—an application that is not part of the SRC network—to interact with SRC components, such as the VTA, through a SOAP interface.
Authorization and Accounting Applications	
AAA RADIUS servers	Authenticates subscribers and authorizes their access to the requested system or service. Accepts accounting data—time active and volume of data sent—about subscriber and service sessions. RADIUS servers run on a system other than a C Series Controller.
SRC Admission Control Plug-In (SRC ACP)	Authorizes and tracks subscribers' use of network resources associated with services that the SRC application manages.
Flat file accounting	Stores tracking data to accounting flat files that can be made available to external systems that send the data to a rating and billing system.
Volume Tracking Application	The SRC Volume Tracking Application (SRC VTA) is an SRC component that allows service providers to track and control the network usage of subscribers and services. You can control volume and time usage on a per-subscriber or per-service basis. This level of control means that service providers can offer tiered services that use volume as a metric, while also controlling abusive subscribers and applications. When a subscriber or service exceeds bandwidth limits (or quotas), the SRC VTA can take actions including imposing rate limits on traffic, sending an e-mail notification, or charging extra for additional bandwidth consumed.
Demonstration Applications (available on the Juniper Networks Website)	

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
Enterprise Audit Plug-In	Defines a callback interface, which receives events when IT managers complete specified operations.
Enterprise Manager Portal	Allows service providers to provision services for enterprise subscribers on routers running JunosE or Junos OS and allows IT managers to manage services. Enterprise Manager Portal can be used with NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on routers running Junos OS and to all IT managers to make requests about public IP addresses through the Enterprise Manager Portal.
Monitoring Agent application	Integrates IP address managers, such as a DHCP server or a RADIUS server, into an SRC-managed network so that the SAE is notified about subscriber events. The Monitoring Agent application runs on a Solaris platform.
Residential service selection portals	Provides a framework for building Web applications that allow residential and enterprise subscribers to manage their own network services. It comes with several full-featured sample Web applications that are easy to customize and suitable for deployment. The Residential service selection portals run on a Solaris platform.
Sample enterprise service portal	Lets service providers supply an interface to their business customers for managing and provisioning services.

Related Documentation

- *SRC Product Description*

CHAPTER 2

System Logging

- C Series Controller Log Server Overview on page 7

C Series Controller Log Server Overview

The C Series Controller includes a system log server that you can configure to manage messages generated on the system. These messages record events that occur to system processes and components.

You can configure the system log server on a C Series Controller to send messages about events to:

- A local file
- Other hosts that are running a system log server
- Users who need to be notified about particular error conditions

You configure which groups of messages are to be forwarded by message type and severity level.

Message Groups

Message groups (also called facilities) define sets of messages generated by the same software process or concerned with a similar condition or activity (such as authentication attempts).

You can configure the following message groups for the system log server:

- any—Messages from all facilities.
- authorization—Authentication and authorization attempts.
- daemon—Actions performed or errors encountered by various system processes.
- ftp—Actions performed or errors encountered by an FTP process.
- kernel—Actions performed or errors encountered by the kernel.
- user—Actions performed or errors encountered by various user processes.
- local7—Actions performed or errors encountered by different processes.

Severity Levels

You can specify the following severity levels for groups of messages to be forwarded:

- any—Messages for all severity levels.
- emergency—System panic or other condition that causes the system to stop functioning.
- alert—Conditions that require immediate correction.
- critical—Critical conditions, such as hard drive errors.
- error—Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- warning—Conditions that warrant monitoring.
- notice—Conditions that are not errors but might warrant special handling.
- info—Events or nonerror conditions of interest.
- none—Messages are not generated for any condition.

Related Documentation

- Before You Configure System Logging (SRC CLI) on page 11
- Configuration Statements for System Logging on a C Series Controller on page 17
- Saving System Log Messages to a File (C-Web Interface) on page 12
- Sending System Log Messages to Other Servers (C-Web Interface) on page 14
- Sending Notifications for System Log Messages to Users (C-Web Interface) on page 15

PART 2

Configuration

- Configuration Tasks on page 11
- Configuration Statements on page 17

CHAPTER 3

Configuration Tasks

- Before You Configure System Logging (SRC CLI) on page 11
- Saving System Log Messages to a File (SRC CLI) on page 11
- Saving System Log Messages to a File (C-Web Interface) on page 12
- Sending System Log Messages to Other Servers (SRC CLI) on page 13
- Sending System Log Messages to Other Servers (C-Web Interface) on page 14
- Sending Notifications for System Log Messages to Users (SRC CLI) on page 14
- Sending Notifications for System Log Messages to Users (C-Web Interface) on page 15

Before You Configure System Logging (SRC CLI)

Before you configure the system log server on a C Series Controller, you should be familiar with:

- The system log protocol
- Logging for SRC components

  See *Configuring System Logging (SRC CLI)* or *Configuring an SRC Component to Store Log Messages in a File (SRC CLI)*.

Related Documentation

- C Series Controller Log Server Overview on page 7

Saving System Log Messages to a File (SRC CLI)

Use the following statements to configure the system log server to store messages in a file:

```
system syslog file file-name (any | authorization | daemon | ftp | kernel | user | local7) {
    (any | emergency | alert | critical | error | warning | notice | info | none);
```

By default, message files are stored in the */var/log* directory. Log files are rotated and compressed according to the settings in the logrotate utility.

To configure the system log server to send messages to a file on the local C Series Controller:

1. From configuration mode, access the configuration statement that configures the system log server.

   ```
   [edit]
   user@host# edit system syslog
   ```

2. Specify the name of the file to store messages, and group and severity level for the messages.

   ```
   [edit system syslog]
   user@host# set file file-name message-group severity
   ```

   For example, to configure the system log server to save critical messages generated by authentication and authorization attempts to the file named access:

   ```
   [edit system syslog]
   user@host# set file access authorization critical
   ```

Related Documentation

- Saving System Log Messages to a File (C-Web Interface) on page 12
- Sending System Log Messages to Other Servers (SRC CLI) on page 13
- Sending Notifications for System Log Messages to Users (SRC CLI) on page 14
- C Series Controller Log Server Overview on page 7
- *Rotating Log Files*

Saving System Log Messages to a File (C-Web Interface)

To save system log messages to a file:

1. Click **Configure**, expand **System**, and click **Syslog**.

   The Syslog pane appears.

2. From the Create new list, select **File**.
3. Type a name for the file in the dialog box, and click **OK**.

   The File pane appears.

4. To configure a message group, select the message group that you want to configure from the Create new list.

   You can configure multiple message groups in the log file.

5. To configure a severity level:

   a. In the side pane, click the log file.

   b. From the Severity box, select the severity level that you want to track with the log file, and click **Apply**.

Related Documentation

- Saving System Log Messages to a File (SRC CLI) on page 11
- Sending System Log Messages to Other Servers (C-Web Interface) on page 14
- Sending Notifications for System Log Messages to Users (C-Web Interface) on page 15
- C Series Controller Log Server Overview on page 7

Sending System Log Messages to Other Servers (SRC CLI)

Use the following statements to configure the system log server to send messages to another system log server:

```
system syslog host log-host-name (any | authorization | daemon | ftp | kernel | user | local7)
  {
  (any | emergency | alert | critical | error | warning | notice | info | none);
}
```

Before you configure the system log server to send messages to other system log servers, ensure that the remote system log server is configured to receive messages on the standard UDP port, 514.

To configure the system log server to send messages to another system log server:

1. From configuration mode, access the configuration statement that configures the system log server.

   ```
   [edit]
   user@host# edit system syslog
   ```

2. Specify the remote system log server to receive messages as well as the groups and severity level for those messages.

   ```
   [edit system syslog]
   user@host# set host log-host-name message-group severity
   ```

   For example, to configure the system log server to send error messages generated by processes on the C Series Controller to my-syslog-server:

   ```
   [edit system syslog]
   user@host# set my-syslog-server.mydomain.com local7 error
   ```

Related Documentation

- Sending System Log Messages to Other Servers (C-Web Interface) on page 14
- Saving System Log Messages to a File (SRC CLI) on page 11
- Sending Notifications for System Log Messages to Users (SRC CLI) on page 14
- C Series Controller Log Server Overview on page 7

Sending System Log Messages to Other Servers (C-Web Interface)

Before you configure the system log server to send messages to other system log servers, ensure that the remote system log server is configured to receive messages on the standard UDP port, 514.

To configure the system log server to send messages to another system log server:

1. Click **Configure**, expand **System**, and click **Syslog**.

   The Syslog pane appears.

2. From the Create new list, select **Host**.
3. Type a name for the file in the dialog box, and click **OK**.

   The Host pane appears.

4. To configure a message group, select the message group that you want to configure from the Create new list.

   You can configure multiple message groups in the log file.

5. To configure a severity level:

   a. In the side pane, click the log file.

   b. From the Severity box, select the severity level that you want to track with the log file, and click **Apply**.

Related Documentation

- Sending System Log Messages to Other Servers (SRC CLI) on page 13
- Saving System Log Messages to a File (C-Web Interface) on page 12
- Sending Notifications for System Log Messages to Users (C-Web Interface) on page 15
- C Series Controller Log Server Overview on page 7

Sending Notifications for System Log Messages to Users (SRC CLI)

Use the following statements to configure the system log server to send notifications to users:

```
system syslog user user-name (any | authorization | daemon | ftp | kernel | user |
local7) {
   (any | emergency | alert | critical | error | warning | notice | info | none);
}
```

To configure the system log server to send notifications to users:

1. From configuration mode, access the configuration statement that configures the system log server.

   ```
   [edit]
   user@host# edit system syslog
   ```

2. Specify the user to receive notifications and the types of notifications to be sent.

   ```
   [edit system syslog]
   user@host# set user user-name message-group severity
   ```

   For example, to configure the system log server to send notifications to admin for conditions that require immediate attention:

   ```
   [edit system syslog]
   user@host# set user admin any critical
   ```

Related Documentation

- Sending Notifications for System Log Messages to Users (C-Web Interface) on page 15
- Saving System Log Messages to a File (SRC CLI) on page 11
- Sending System Log Messages to Other Servers (SRC CLI) on page 13
- C Series Controller Log Server Overview on page 7

Sending Notifications for System Log Messages to Users (C-Web Interface)

To configure the system log server to send notifications to users:

1. Click **Configure**, expand **System**, and click **Syslog**.

   The Syslog pane appears.

2. From the Create new list, select **User**.
3. Type a name for the file in the dialog box, and click **OK**.

   The User pane appears.

4. To configure a message group, select the message group that you want to configure from the Create new list.

   You can configure multiple message groups in the log file.

5. To configure a severity level:

   a. In the side pane, click the log file.

   b. From the Severity box, select the severity level that you want to track with the log file, and click **Apply**.

Related Documentation

- Sending Notifications for System Log Messages to Users (SRC CLI) on page 14
- Saving System Log Messages to a File (C-Web Interface) on page 12
- Sending System Log Messages to Other Servers (C-Web Interface) on page 14
- C Series Controller Log Server Overview on page 7

CHAPTER 4

Configuration Statements

- Configuration Statements for System Logging on a C Series Controller on page 17

Configuration Statements for System Logging on a C Series Controller

Use the following configuration statements to configure the system log server at the **[edit]** hierarchy level.

```
system syslog file file-name (any | authorization | daemon | ftp | kernel | user | local7) {
    (any | emergency | alert | critical | error | warning | notice | info | none);
}
system syslog host log-host-name (any | authorization | daemon | ftp | kernel | user | local7)
    {
    (any | emergency | alert | critical | error | warning | notice | info | none);
}
system syslog user user-name (any | authorization | daemon | ftp | kernel | user |
local7) {
    (any | emergency | alert | critical | error | warning | notice | info | none);
}
```

For detailed information about each configuration statement, see the *SRC PE CLI Command Reference*.

Related Documentation

- Saving System Log Messages to a File (SRC CLI) on page 11
- Sending System Log Messages to Other Servers (SRC CLI) on page 13
- Sending Notifications for System Log Messages to Users (SRC CLI) on page 14
- C Series Controller Log Server Overview on page 7

PART 3

Administration

- Routine Monitoring on page 21

CHAPTER 5

Routine Monitoring

- Viewing the System Date and Time (C-Web Interface) on page 21

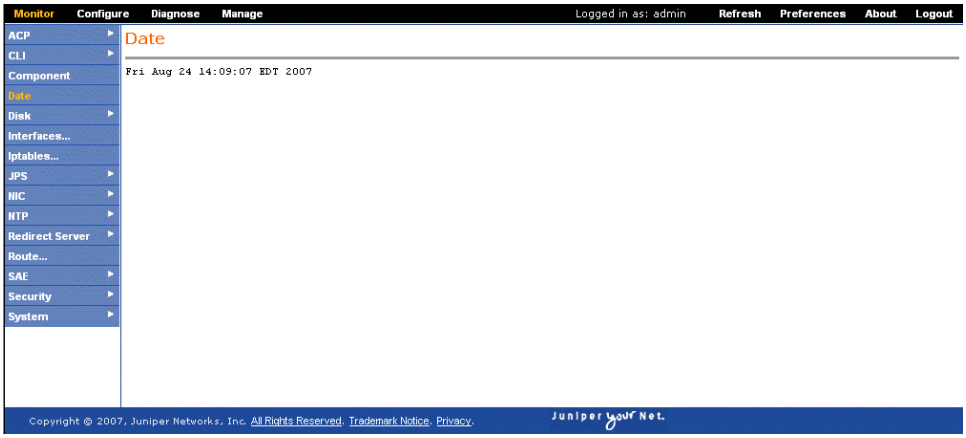
Viewing the System Date and Time (C-Web Interface)

Purpose View the system date and time.

Action Click **Monitor**>**Date**.

The Date pane displays the date and time of the system.

Figure 1: C-Web Interface for Monitoring System Date and Time



Related Documentation

- *Setting the Time Zone (SRC CLI)*
- *Setting the System Date (SRC CLI)*
- *Viewing NTP Peers (C-Web Interface)*
- *Viewing Statistics for NTP (C-Web Interface)*
- *Viewing NTP Status (C-Web Interface)*