



## **Cisco Global Site Selector Administration Guide**

Software Version 2.0

March 2007

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-10410-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

*Cisco Global Site Selector Administration Guide*  
© 2007 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## **Preface** xi

Audience xi

How to Use This Guide xii

Related Documentation xiii

Symbols and Conventions xv

Obtaining Documentation, Obtaining Support, and Security Guidelines xvii

---

## **CHAPTER 1**

### **Managing GSS Devices from the GUI** 1-1

Logging Into the Primary GSSM Graphical User Interface 1-2

Logging Into the GSS and Accessing the CNR GUI 1-4

Activating and Modifying GSS Devices 1-6

Activating GSS Devices from the Primary GSSM 1-6

Modifying GSS Device Name and Location 1-9

Deleting GSS Devices 1-10

Logically Removing a GSS or Standby GSSM from the Network 1-11

Configuring the Primary GSSM GUI 1-13

Printing and Exporting GSSM Data 1-14

Viewing Third-Party Software Versions 1-15

---

## **CHAPTER 2**

### **Managing the GSS from the CLI** 2-1

Logging in to the CLI and Enabling Privileged EXEC Mode 2-2

Understanding GSS Software Licenses 2-3

Acquiring and Installing License Files 2-3

Installing and Activating CNR	2-4
Accessing the CNR CLI	2-6
Invoking the Shell and Executing CNR Utilities	2-7
Using the startup-config and running-config Files	2-8
Changing the startup-config and running- config Files	2-8
Saving the startup-config and running-config Files	2-10
Loading the startup-config from an External File	2-11
Displaying the running-config File	2-11
Displaying the startup-config File	2-13
Managing GSS Files	2-14
Displaying the Contents of a File	2-14
Displaying Files in a Directory	2-16
Renaming GSS Files	2-17
Securely Copying Files	2-18
Deleting Files	2-19
Displaying Users	2-19
Specifying the GSS Inactivity Timeout	2-20
Configuring the Terminal Screen Line Length	2-20
Modifying the Attributes of the Security Certificate on the GSSM	2-21
Stopping the GSS Software	2-23
Shutting Down the GSS Software	2-23
Restarting the GSS Software	2-23
Performing a Cold Restart of a GSS Device	2-24
Disabling the GSS Software	2-24
Restoring GSS Factory-Default Settings	2-25
Replacing GSS Devices in Your GSS Network	2-26
Replacing the Primary GSSM in the Network	2-27
Converting the Standby GSSM to a Primary GSSM	2-27
Replacing the Primary GSSM with an Available GSS	2-31

Replacing the Standby GSSM in the Network	2-33
Replacing a GSS in the Network	2-35
Changing the GSSM Role in the GSS Network	2-36
Switching the Roles of the Primary and Standby GSSM Devices	2-37
Reversing the Roles of the Interim Primary and Standby GSSM Devices	2-39
Displaying GSS System Configuration Information	2-40
Displaying Software Version Information	2-41
Displaying License Information	2-42
Displaying Memory Information	2-43
Displaying Boot Configuration	2-44
Displaying GSS Processes	2-45
Displaying System Uptime	2-46
Displaying Disk Information	2-46
Displaying UDI Data	2-46
Displaying System Status	2-47
Displaying GSS Services	2-48

## CHAPTER 3

### Creating and Managing User Accounts 3-1

Creating and Managing GSS CLI User Accounts	3-1
Creating a GSS User Account	3-2
Modifying a GSS User Account	3-3
Deleting a GSS User Account	3-3
Creating and Managing Primary GSSM GUI User Accounts	3-4
Privilege Levels for Using the Primary GSSM GUI	3-5
Creating a GUI User Account	3-9
Modifying a GUI User Account	3-12
Removing a GUI User Account	3-12
Changing the User Account GUI Password	3-13
Creating and Modifying User Views for the Primary GSSM GUI	3-15
Custom User View Overview	3-15

Creating a GUI User View	3-16
Modifying a GUI User View	3-24
Deleting a GUI User View	3-25
Modifying the Administrator Account Passwords	3-26
Resetting the Administrator CLI Account Password	3-26
Changing the Administrator CLI Password	3-27
Restoring or Changing the Administrator GUI Password	3-28

## CHAPTER 4

### Managing GSS User Accounts Through a TACACS+ Server 4-1

TACACS+ Overview	4-2
TACACS+ Configuration Quick Start	4-4
Configuring a TACACS+ Server for Use with the GSS	4-5
Configuring Authentication Settings on the TACACS+ Server	4-5
Configuring Authorization Settings on the TACACS+ Server	4-7
Configuring Primary GSSM GUI Privilege Level Authorization from the TACACS+ Server	4-12
Enabling Custom User GUI Views When Authenticating a User from the TACACS+ Server	4-16
Configuring Accounting Settings on the TACACS+ Server	4-17
Identifying the TACACS+ Server Host on the GSS	4-19
Disabling TACACS+ Server Keepalives on the GSS	4-22
Specifying the TACACS+ Server Timeout on the GSS	4-23
Specifying TACACS+ Authentication of the GSS	4-23
Specifying TACACS+ Authorization of the GSS	4-24
Specifying TACACS+ Accounting on the GSS	4-25
Showing TACACS+ Statistics on the GSS	4-26
Clearing TACACS+ Statistics on the GSS	4-28
Disabling TACACS+ on a GSS	4-28

---

**CHAPTER 5****Configuring Access Lists and Filtering GSS Traffic 5-1**

- Filtering GSS Traffic Using Access Lists 5-1
  - Access List Overview 5-2
  - Creating an Access List 5-4
  - Associating an Access List with a GSS Interface 5-7
  - Disassociating an Access List from a GSS Interface 5-8
  - Adding Rules to an Access List 5-8
  - Removing Rules from an Access List 5-9
  - Segmenting GSS Traffic by Ethernet Interface 5-9
  - Displaying Access Lists 5-10
- Deploying GSS Devices Behind Firewalls 5-12
  - GSS Firewall Deployment Overview 5-12
  - Configuring GSS Devices Behind a Firewall 5-15

---

**CHAPTER 6****Configuring SNMP 6-1**

- Overview 6-1
- Configuring SNMP on the GSS 6-2
- Configuring SNMP Servers 6-4
- Configuring SNMP Server Notifications 6-5
- Configuring SNMP Server Trap Limits 6-6
- Specifying Recipients for SNMP Notification Operations 6-7
- Viewing SNMP Status 6-8
- Viewing MIB Files on the GSS 6-9

---

**CHAPTER 7****Backing Up, Restoring, and Downgrading the GSSM Database 7-1**

- Backing Up the Primary GSSM 7-2
  - Backup Overview 7-2
  - Performing a Full Primary GSSM Backup 7-3

- Restoring a Primary GSSM Backup 7-4
  - Restore Overview 7-4
  - Restoring Your Primary GSSM from a Previous Backup 7-5
- Downgrading Your GSS Devices 7-8

## CHAPTER 8

### Viewing Log Files 8-1

- Understanding GSS Logging Levels 8-1
- Configuring System Logging for a GSS 8-4
  - Specifying a Log File on the GSS Disk 8-5
  - Specifying a Host for a Log File Destination 8-6
  - Specifying a Syslog Facility 8-8
- Viewing Device Logs from the CLI 8-9
  - Viewing the gss.log File from the CLI 8-10
  - Viewing System Message Logging 8-11
  - Viewing Subsystem Log Files from the CLI 8-11
  - Rotating Existing Log Files from the CLI 8-12
- Viewing System Logs from the Primary GSSM GUI 8-13
  - Viewing System Logs from the Primary GSSM GUI 8-14
  - Purging System Log Messages from the GUI 8-15
  - Common System Log Messages 8-16
- Viewing GSS System Logs Using CiscoWorks RME Syslog Analyzer 8-18

## CHAPTER 9

### Monitoring GSS Operation 9-1

- Monitoring GSS and GSSM Status 9-2
  - Monitoring the GSS Device Online Status from the CLI 9-2
  - Monitoring the GSS Device System Status from the CLI 9-4
  - Monitoring the GSS Device Status from the Primary GSSM GUI 9-4
- Monitoring GSSM Database Status 9-5
  - Monitoring the Database Status 9-5



Validating Database Records	9-6
Creating a Database Validation Report	9-6
Viewing the GSS Operating Configuration for Technical Support	9-8

---

**APPENDIX A****Upgrading the GSS Software A-1**

Verifying the GSSM Role in the GSS Network	A-2
Backing up and Archiving the Primary GSSM	A-3
Obtaining the Software Upgrade	A-3
Upgrading Your GSS Devices	A-5

---

**INDEX**





## Preface

---

This guide includes information on configuring the Cisco Global Site Selector (GSS). It describes the procedures necessary to properly manage and maintain your Global Site Selector Manager (GSSM) and GSS devices, including login security, GSS software upgrades, GSSM database administration, and log files.

This preface contains the following major sections:

- [Audience](#)
- [How to Use This Guide](#)
- [Related Documentation](#)
- [Symbols and Conventions](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)

## Audience

To use this guide, you should be familiar with the Cisco Global Site Selector hardware, which is discussed in the *Global Site Selector Hardware Installation Guide*. In addition, you should be familiar with basic TCP/IP and networking concepts, router configuration, Domain Name System (DNS), the Berkeley Internet Name Domain (BIND) software or similar DNS products, and your organization's specific network configuration.

# How to Use This Guide

This guide includes the following chapters:

Chapter/Title	Description
<a href="#">Chapter 1, Managing GSS Devices from the GUI</a>	Describes how to configure and manage your GSSM and GSS devices from the primary GSSM graphical user interface, including activating and configuring GSS devices.
<a href="#">Chapter 2, Managing the GSS from the CLI</a>	Describes how to manage the GSS software from the CLI, including configuring a replacement GSS device for use in your GSS network and changing the GSSM role in the network.
<a href="#">Chapter 3, Creating and Managing User Accounts</a>	Describes how to create and manage GSS device CLI login accounts and primary GSSM GUI login accounts. This chapter also describes how to specify user privileges and assign custom user views for accessing the primary GSSM GUI.
<a href="#">Chapter 4, Managing GSS User Accounts Through a TACACS+ Server</a>	Describes how to configure the GSS as a client of a TACACS+ server for authentication, authorization, and accounting.
<a href="#">Chapter 5, Configuring Access Lists and Filtering GSS Traffic</a>	Describes how to create access lists and access groups to filter GSS traffic.
<a href="#">Chapter 6, Configuring SNMP</a>	Describes how to configure Simple Network Management Protocol (SNMP) on your GSS.
<a href="#">Chapter 7, Backing Up, Restoring, and Downgrading the GSSM Database</a>	Describes the procedures to back up and restore the primary GSSM database. This chapter also includes a set of general guidelines for when and how to back up your primary GSSM.
<a href="#">Chapter 8, Viewing Log Files</a>	Includes information on auditing logged information about your GSS devices.

Chapter/Title	Description
<a href="#">Chapter 9, Monitoring GSS Operation</a>	Describes the tools that you can use to monitor the status of your GSS devices and of global load balancing on your GSS network.
<a href="#">Appendix A, Upgrading the GSS Software</a>	Describes how to manually upgrade your GSS software.

## Related Documentation

In addition to this document, the GSS documentation set includes the following:

Document Title	Description
<i>Global Site Selector Hardware Installation Guide</i>	Information on installing your GSS device and getting it ready for operation. It describes how to prepare your site for installation, how to install the GSS device in an equipment rack, and how to maintain and troubleshoot the GSS hardware.
<i>Regulatory Compliance and Safety Information for the Cisco Global Site Selector</i>	Regulatory compliance and safety information for the GSS.
<i>Release Note for the Cisco Global Site Selector</i>	Information on operating considerations, caveats, and new CLI commands for the GSS software.

Document Title	Description
<i>Cisco Global Site Selector Getting Started Guide</i>	Information on getting your GSS set up, configured, and ready to perform global server load balancing.
<i>Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide</i>	Procedures on how to configure your primary GSSM from the GUI to perform global server load balancing, such as configuring source address lists, domain lists, answers, answer groups, DNS sticky, network proximity, and DNS rules. This document also provides an overview of the GSS device and global server load balancing as performed by the GSS.
<i>Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide</i>	Procedures on how to configure your primary GSSM from the CLI to perform global server load balancing, such as configuring source address lists, domain lists, answers, answer groups, DNS sticky, network proximity, and DNS rules. This document also provides an overview of the GSS device and global server load balancing as performed by the GSS.
<i>Cisco Global Site Selector Command Reference</i>	An alphabetical list of all GSS command-line interface (CLI) commands including syntax, options, and related commands. This document also describes how to use the CLI interface.

Several of the Cisco CNS Network Registrar (CNR) documents are referenced in this guide. The CNR version 6.2 documentation set consists of the following documents:

Document Title	Description
<i>Release Notes for the Cisco CNS Network Registrar, Release 6.2</i>	Information on new software features, installation updates, caveats, and documentation for the CNR release.
<i>Cisco CNS Network Registrar Installation Guide</i>	Information on installing CNR on the supported operating systems: Windows, Solaris, and Linux.

Document Title	Description
<i>Cisco CNS Network Registrar User's Guide</i>	Information on configuring CNR by using the Web-based user interface (Web UI) and the command line interface (CLI).
<i>Cisco CNS Network Registrar CLI Reference Guide</i>	Information about how to use the CNR command-line program, <b>nrcmd</b> .

## Symbols and Conventions

This guide uses the following symbols and conventions to emphasize certain information.

Command descriptions use the following conventions:

<b>boldface font</b>	Commands and keywords are in <b>boldface</b> .
<i>italic font</i>	Variables for which you supply values are in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{ <b>x</b>   <b>y</b>   <b>z</b> }	Alternative keywords are grouped in braces and separated by vertical bars.
[ <b>x</b>   <b>y</b>   <b>z</b> ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.

Screen examples use the following conventions:

screen font	Terminal sessions and information the system displays are in screen font.
<b>boldface screen font</b>	Information you must enter is in <b>boldface screen font</b> .

<i>italic screen font</i>	Variables for which you supply values are in <i>italic screen font</i> .
→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control. For example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Graphical user interface elements use the following conventions:

<b>boldface text</b>	Instructs the user to enter a keystroke or act on a GUI element.
Courier text	Indicates text that appears in a command line, including the CLI prompt.
<b>Courier bold text</b>	Indicates commands and text you enter in a command line.
<i>italic text</i>	Directories and filenames are in <i>italic</i> font.



Caution

A caution means that a specific action you take could cause a loss of data or adversely impact use of the equipment.



Note

A note provides important related information, reminders, and recommendations.



# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>





# CHAPTER 1

## Managing GSS Devices from the GUI

---

This chapter describes how to configure and manage your Global Site Selector Manager (GSSM) and Global Site Selector (GSS) devices from the primary GSSM graphical user interface. It includes the procedures for activating and configuring GSS devices and for changing the primary and standby GSSM roles in the GSS network.

This chapter contains the following major sections:

- [Logging Into the Primary GSSM Graphical User Interface](#)
- [Logging Into the GSS and Accessing the CNR GUI](#)
- [Activating and Modifying GSS Devices](#)
- [Logically Removing a GSS or Standby GSSM from the Network](#)
- [Configuring the Primary GSSM GUI](#)
- [Printing and Exporting GSSM Data](#)
- [Viewing Third-Party Software Versions](#)

# Logging Into the Primary GSSM Graphical User Interface

After you configure and enable your primary GSSM, you may access the GUI. The primary GSSM uses secure HTTP (HTTPS) to communicate with web clients.

When you first log in to the primary GSSM GUI, use the system default administrative account and password. After you access the primary GSSM GUI, create and maintain additional user accounts and passwords using the user administration features of the primary GSSM. See [Chapter 3, Creating and Managing User Accounts](#), for more information about creating user accounts.

To log in to the primary GSSM GUI, perform the following steps:

1. Open your preferred Internet web browser application, such as Internet Explorer or Netscape Navigator.
2. Enter the secure HTTP address of your GSSM in the address field. For example, if your primary GSSM is named gssm1.example.com, enter the following to display the primary GSSM login dialog box and to access the GUI:

```
https://gssm1.example.com
```



**Note** If you cannot locate the primary GSSM DNS name, be aware that the GSS network uses secure connections and that the address of the GSSM includes https:// (HTTP over SSL) instead of the more common http://.

3. Click **Yes** at the prompt to accept (trust) and install the signed certificate from Cisco Systems.

To avoid approving the signed certificate every time you log in to the primary GSSM, accept the certificate from Cisco Systems, Inc. For instructions on trusting certificates from a particular owner or website, refer to the online help included with your browser.

4. Install the signed certificate as follows:
  - If you are using Internet Explorer—In the Security Alert dialog box, click **View Certificate**, choose the **Install Certificate** option, and follow the prompts of the Certificate Manager Import Wizard. Proceed to Step 5.

- If you are using Netscape—In the New Site Certificate dialog box, click **Next** and follow the prompts of the New Site Certificate Wizard. Proceed to Step 5.
5. At the primary GSSM login window, enter your username and password in the fields provided, and then click **Login** (see [Figure 1-1](#)). If this is your first time logging in to the GSSM, use the default account name (admin) and password (default) to access the GUI.

The Primary GSSM Welcome page (see [Figure 1-2](#)) appears. See the *Cisco Global Site Selector GUI-based Global Server Load-Balancing Configuration Guide* for information about navigating through the primary GSSM GUI.

**Figure 1-1 Primary GSSM GUI Login Window**

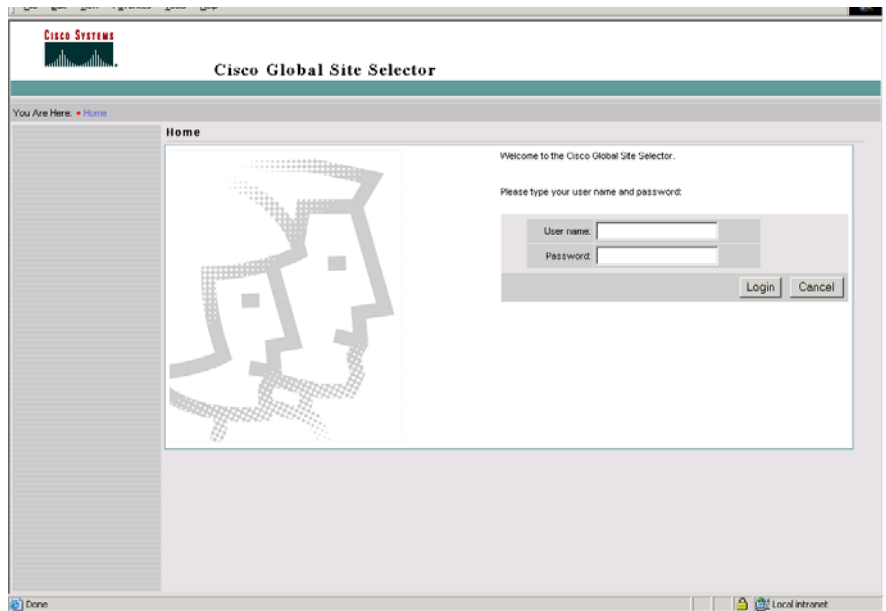
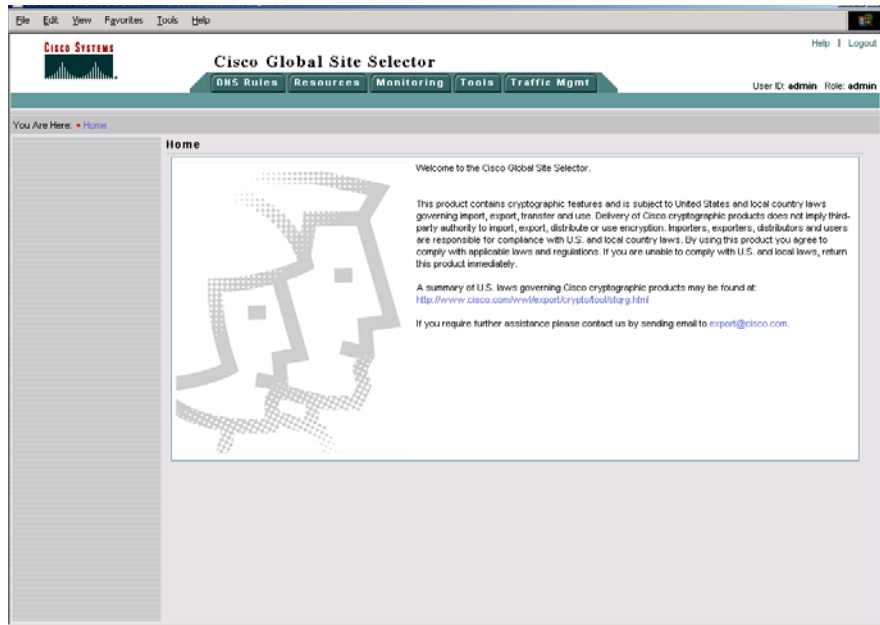


Figure 1-2 Primary GSSM Welcome Window



6. Log out of a primary GSSM GUI session by clicking **Logout** in the upper right of the window.

The browser confirms that you want to log out of the primary GSSM GUI session.

7. Click **OK** to confirm the logout (or **Cancel**).

When you click **OK**, the primary GSSM logs you out of the session and redisplay the Primary GSSM GUI Login window (see Figure 1-1).

## Logging Into the GSS and Accessing the CNR GUI

You can extend the capabilities of GSS by using the Cisco Network Registrar (CNR). CNR is purchased as a separate license add-on and involves upgrading the existing GSS software license. For more information about obtaining, installing, and activating a CNR license, see Chapter 2, *Managing the GSS from the CLI*.

After you install and activate CNR, you access the CNR GUI by performing the following steps:

1. Open your preferred Internet web browser application, such as Internet Explorer or Netscape Navigator.
2. Enter the secure HTTP address of your GSS in the address field as follows:

**http:// gss-machine:8080**

where gss-machine is a resolvable name, such as gss-example.cisco.com or the IP address of that machine. For instance, each of the following can serve as valid addresses:

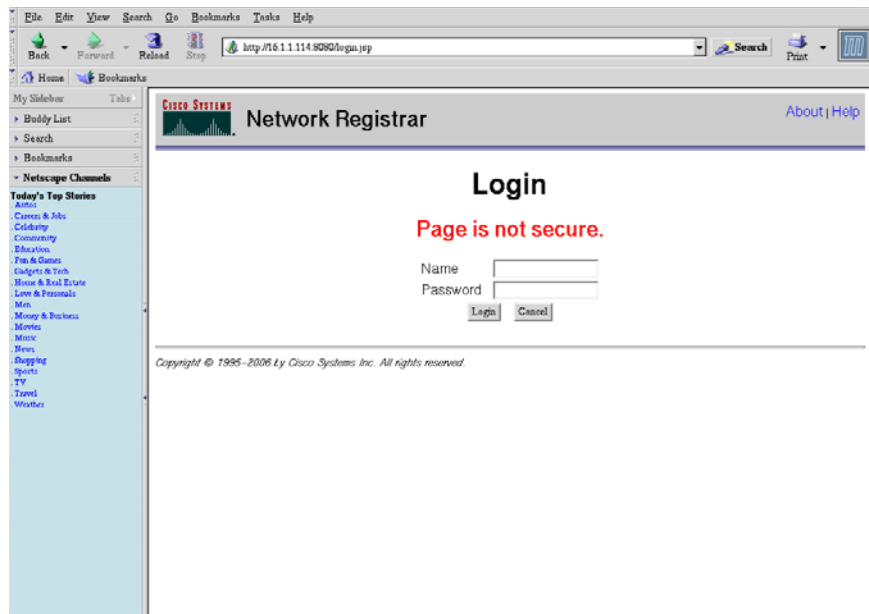
**http://gss-example.cisco.com:8080**

OR

**http://16.1.1.114:8080**

The Network Registrar login page (see [Figure 1-3](#)) appears.

**Figure 1-3 Network Registrar Login Window**



3. At the Network Registrar login window, enter your username and password in the fields provided, and then click **Login**.

See the *Cisco CNS Network Registrar User's Guide* for information on configuring CNR using its Web-based user interface (Web UI).

## Activating and Modifying GSS Devices

Activate your GSS devices from the primary GSSM GUI to add those devices to your GSS network. You also use the primary GSSM GUI to remove a non-functioning standby GSSM or GSS device from your network.

This section contains the following procedures:

- [Activating GSS Devices from the Primary GSSM](#)
- [Modifying GSS Device Name and Location](#)
- [Deleting GSS Devices](#)

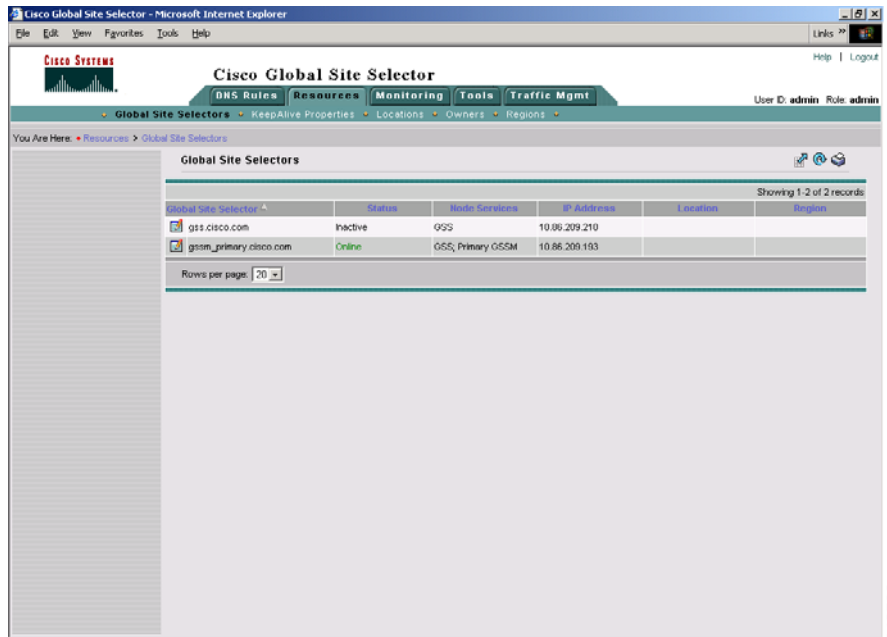
## Activating GSS Devices from the Primary GSSM

After you configure your GSS devices from the CLI to function as a standby GSSM or as a GSS, activate those devices from the primary GSSM GUI so they can receive and process user requests.

To activate a GSS or a standby GSSM from the primary GSSM GUI, perform the following steps:

1. Click the **Resources** tab.
2. Click the **Global Site Selectors** navigation link. The Global Site Selectors list page appears (see [Figure 1-4](#)). All active GSS devices appear with an “Online” status. The GSS devices requiring activation appear with an “Inactive” status.



**Figure 1-4 Global Site Selectors List Page—Inactive Status**

3. Click the **Modify GSS** icon for the first GSS device to activate. The Modifying GSS details page appears (see [Figure 1-5](#)).

Figure 1-5 Modifying GSS Details Page

**Cisco Global Site Selector**

Global Site Selectors | KeepAlive Properties | Locations | Owners | Regions

You Are Here: Resources > Global Site Selectors

Modifying GSS: gss.cisco.com

General Configuration	Locality
Name: gss.cisco.com	Location: Unspecified
Activate: <input checked="" type="checkbox"/>	Region: NA

Node Information	Network Information
Status: Inactive	IP Address: 10.0.209.210
Version: 1.0.901.0.13	Hostname: gss-extreme.cisco.com
Node Services: GSS	MAC: 00:02:55:b7:73:1f

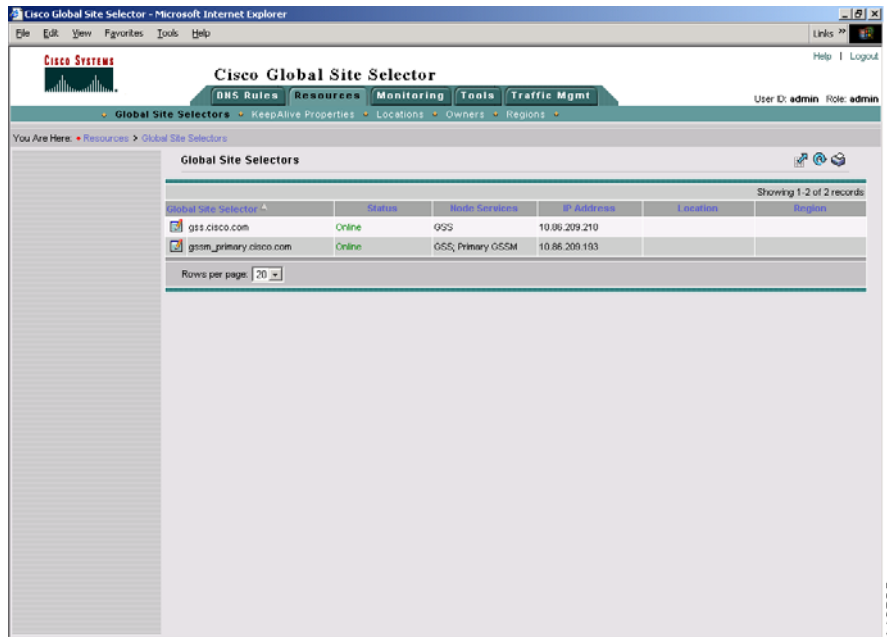
Submit Cancel

4. Check the **Activate** check box. This check box does not appear in the Modifying GSS details page once the GSS device has been activated.
5. Click the **Submit** button, which returns you to the Global Site Selectors list page (see Figure 1-6). The status of the active GSS device is “Online.”

If the device is functioning properly and network connectivity is good between the device and the primary GSSM, the status of the device changes to “Online” within approximately 30 seconds.

**Note**

The device status remains “Inactive” if the device is not functioning properly or if there are problems with network connectivity. If this occurs, power cycle the GSS device, check your network connections, and then repeat this procedure. If you still cannot activate the GSS device, contact Cisco TAC.

**Figure 1-6 Global Site Selectors List Page—Active Status**

- Repeat Steps 1 through 5 for each inactive GSS or standby GSSM.

## Modifying GSS Device Name and Location

You can modify the name and location of any of your GSS devices using the primary GSSM GUI. To modify other network information such as the hostname, IP address, or role, you must access the CLI on that GSS device (see the *Cisco Global Site Selector Getting Started Guide*).

To modify the name and location of a GSS device from the primary GSSM GUI, perform the following steps:

- Click the **Resources** tab.
- Click the **Global Site Selectors** navigation link. The Global Site Selectors list page appears (see [Figure 1-4](#)). All active GSS devices appear with an "Online" status. The GSS devices requiring activation appear with an "Inactive" status.

3. Click the **Modify GSS** icon for the first GSS to activate. The Modifying GSS details page appears (see [Figure 1-5](#)).
4. In the Global Site Selector Name field, enter a new name for the device. You use the device name to easily distinguish one GSS device from another in the primary GSSM list pages, where many devices may appear together.
5. From the Location drop-down list, choose a new device location.
6. Click **Submit** to save your changes, and return to the Global Site Selector list page.

## Deleting GSS Devices

Deleting a GSS device such as a GSS or a standby GSSM allows you to remove the nonfunctioning device from your network or reconfigure and then reactivate a GSS device. With the exception of the primary GSSM, you can delete GSS devices from your network through the primary GSSM GUI.

To delete a GSS device from the primary GSSM GUI, perform the following steps:

1. Click the **Resources** tab.
2. Click the **Global Site Selectors** navigation link. The Global Site Selectors list page appears.
3. Click the **Modify GSS** icon located to the left of the GSS device you want to delete. The Modifying GSS details page appears.
4. Click the **Delete** icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the GSS device.
5. Click **OK** to confirm your decision and return to the Global Site Selectors list page. The deleted device is removed from the list.

To reconfigure the GSS device, see the *Cisco Global Site Selector Getting Started Guide*.

# Logically Removing a GSS or Standby GSSM from the Network

This section describes the steps to logically remove a GSS or standby GSSM device from your network. You may need to logically remove a GSS from your network when you perform the following tasks:

- Move a GSS device between GSS networks
- Physically remove or replace a GSS or standby GSSM
- Send the GSS or standby GSSM out for repair or replacement

**Note**

Do not logically remove the primary GSSM from the GSS network. If you need to take the primary GSSM offline for either maintenance or repair, temporarily switch the roles of the primary and standby GSSMs as outlined in the [“Changing the GSSM Role in the GSS Network”](#) section of [Chapter 2, Managing the GSS from the CLI](#).

The first four steps in this procedure assume that the GSS or standby GSSM is operational. If that is not the case, proceed directly to Step 5.

To logically remove a GSS or standby GSSM from the network, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

2. Back up the startup configuration file on the GSS or standby GSSM device by entering the following command:

```
gss1.example.com# copy startup-config disk configfile
```

3. Stop the GSS software running on the GSS by entering the following command:

```
gss1.example.com# gss stop
```

4. Disable the GSSM or GSS by entering the following command:

```
gss1.example.com# gss disable
gss1.example.com# shutdown
```

The **gss disable** command removes the existing configuration and returns the GSS device to an initial state, which includes deleting the GSSM database from the GSS device and removing all configured DNS rules and keepalives.

If you intend to power down the GSS device, you should also enter the **shutdown** command.

5. Logically remove a GSS or a standby GSSM from the network by accessing the primary GSSM graphical user interface and clicking the **Resources** tab.
6. Click the **Global Site Selectors** navigation link. The Global Site Selectors list page appears.
7. Click the **Modify GSS** icon located to the left of the GSS device that you want to delete. The Modifying GSS details page appears.
8. Click the **Delete** icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the GSS device.
9. Click **OK** to confirm your decision and return to the Global Site Selectors list page. The deleted device is no longer on the list.

For details on physically removing or replacing a GSS from your network, refer to the *Cisco Global Site Selector Hardware Installation Guide*.

To add the removed GSS or standby GSSM back into the GSS network, follow the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*. After you configure the GSS or standby GSSM, you may reload the backup copy of the GSS device startup configuration settings (see the “[Saving the startup-config and running-config Files](#)” section in [Chapter 2, Managing the GSS from the CLI](#)).

# Configuring the Primary GSSM GUI

The primary GSSM GUI provides you with a number of configuration options for modifying the behavior and performance of the primary GSSM web-based GUI. You can configure the GUI inactivity timeout interval, GSS device reporting interval, and GUI screen refresh interval.

To modify GUI configuration settings from the primary GSSM GUI, perform the following steps:

1. Click the **Tools** tab.
2. Click the **GUI Configuration** navigation link. The GUI Configuration details page appears (see [Figure 1-7](#)).

**Figure 1-7** GUI Configuration Details Page

The screenshot shows the Cisco Global Site Selector web interface in Microsoft Internet Explorer. The browser title is "Cisco Global Site Selector - Microsoft Internet Explorer". The page has a navigation bar with tabs: DNS Rules, Resources, Monitoring, Tools, and Traffic Mgmt. The "Tools" tab is selected, and the "GUI Configuration" link is highlighted. The "GUI Configuration" section contains a table with the following settings:

GUI Configuration	
GUI Session Inactivity Timeout Enable:	<input checked="" type="checkbox"/> Select to enable GUI session inactivity timeout.
GUI Session Inactivity Timeout:	10 minutes Range: 5 - 120
GSS Reporting Interval:	39 seconds Range: 30 - 4000
Monitoring Screen Refresh Interval:	60 seconds Range: 0 - 86400 Enter 0 to disable automatic screen refresh.

At the bottom right of the configuration area, there are "Submit" and "Reset" buttons. The page also shows a "You Are Here" breadcrumb: Tools > GUI Configuration. The user is logged in as "admin" with the role "admin".

3. Adjust one or more of the GUI configuration parameters as follows:
  - To modify the length of time that can expire without GUI activity before the primary GSSM automatically terminates the GUI session, do the following:

- a. Check the **GUI Session Inactivity Timeout Enable** check box.
  - b. In the GUI Session Inactivity Timeout field, enter the length of time that can pass without user activity before the primary GSSM terminates the session. Valid entries are 5 to 120 minutes. The default is 10 minutes.
- To modify the length of time that can expire before GSS devices report their status to the primary GSSM, enter a value in the GSS Reporting Interval field. Valid entries are 30 to 4000 minutes. The default is 300 minutes.
- To modify the length of time between automatic screen refreshes on the primary GSSM GUI, enter a value in the Monitoring Screen Refresh Interval field. Valid entries are 0 to 86400 seconds. The default is 60 seconds. To disable the automatic screen refresh function, enter a value of 0.
4. Click **Submit** to update the primary GSSM. The Transaction Complete icon appears in the lower left corner of the configuration area to indicate the successful updating of the GUI session settings.

## Printing and Exporting GSSM Data

You can send any data that appears on the primary GSSM GUI to a local or network printer configured on your workstation. You may also export that data to a flat file for use with other office applications. When printing or exporting data, the primary GSSM transmits all of the information appearing on the GUI page. You cannot output individual pieces of data.

To print or export GSSM data from the primary GSSM GUI, perform the following steps:

1. Navigate to the list page or details page that contains the data you want to export or print.
  2. Perform one of the following:
    - To export the data, click the **Export** button. The software prompts you to either save the exported data as a comma-delimited file or to open it using your designated CSV editor.
    - To print the data, click the **Print** button. The Print dialog box on your workstation appears. Choose a printer from the list of available printers.
-



**Note**

To export the output of all primary GSSM GUI configured fields when troubleshooting a GSS device with a Cisco technical support representative, enter the **show tech-support config** CLI command. See [Chapter 9, Monitoring GSS Operation](#) for details.

## Viewing Third-Party Software Versions

The GSS software incorporates a number of third-party software products. For that reason, the primary GSSM GUI allows you to easily track information for all of the third-party software that the GSS uses.

To view information on the third-party software currently running on your GSS from the primary GSSM GUI, perform the following steps:

1. Click the **Tools** tab.
2. Click the **Third-Party Software** navigation link. The GSSM Third-Party Software list page appears (see [Figure 1-8](#)) with the following information:
  - Product—Third-party software product. For example, RedHat Version 9.0
  - Version—Version of the third-party software currently installed on the GSS device
  - URL—Web URL for the software product

Figure 1-8 GSSM Third-Party Software List Page

**Cisco Global Site Selector**

Help | Logout

User ID: admin Role: admin

Change Password | GUI Configuration | System Logs | **Third Party Software** | User Administration | Views

You Are Here: Tools > Third Party Software

**Third Party Software**

Product	Version	URL
Apache	1.3.31	<a href="http://httpd.apache.org/">http://httpd.apache.org/</a>
ModSSL	2.0.10	<a href="http://www.modssl.org/">http://www.modssl.org/</a>
Net-SNMP Agent	5.0.8-2.30E.1	<a href="http://www.net-snmp.org/">http://www.net-snmp.org/</a>
OpenSSH	3.6.1p2-33.30.1	<a href="http://www.openssh.org/">http://www.openssh.org/</a>
OpenSSL	0.9.7d	<a href="http://www.openssl.org/">http://www.openssl.org/</a>
PostgreSQL	7.3.4	<a href="http://www.postgresql.org/">http://www.postgresql.org/</a>
RedHat Enterprise Linux	3 (2.4.21-27 0.2 EL Kernel)	<a href="http://www.redhat.com/">http://www.redhat.com/</a>
RSA BSAFE Toolkit	3.4.2	<a href="http://www.rsasecurity.com/products/bsafe/index.html">http://www.rsasecurity.com/products/bsafe/index.html</a>
SSL Library - RSA SSLJ	4.1	
SunJRE	1.5.0_02	<a href="http://java.sun.com/2ee/">http://java.sun.com/2ee/</a>
Tomcat	3.2.4	<a href="http://akarta.apache.org/tomcat/">http://akarta.apache.org/tomcat/</a>
Xerces XML Parser	2.2.0	<a href="http://xml.apache.org/">http://xml.apache.org/</a>

148542



# CHAPTER 2

## Managing the GSS from the CLI

---

This chapter describes how to manage the GSS software from the CLI. It contains the following major sections:

- [Logging in to the CLI and Enabling Privileged EXEC Mode](#)
- [Understanding GSS Software Licenses](#)
- [Using the startup-config and running-config Files](#)
- [Managing GSS Files](#)
- [Displaying Users](#)
- [Specifying the GSS Inactivity Timeout](#)
- [Configuring the Terminal Screen Line Length](#)
- [Modifying the Attributes of the Security Certificate on the GSSM](#)
- [Stopping the GSS Software](#)
- [Shutting Down the GSS Software](#)
- [Restarting the GSS Software](#)
- [Performing a Cold Restart of a GSS Device](#)
- [Disabling the GSS Software](#)
- [Restoring GSS Factory-Default Settings](#)
- [Replacing GSS Devices in Your GSS Network](#)
- [Changing the GSSM Role in the GSS Network](#)
- [Displaying GSS System Configuration Information](#)

# Logging in to the CLI and Enabling Privileged EXEC Mode

To log in to a GSS device and enable privileged EXEC mode at the CLI, perform the following steps:

1. Press the power control button on the GSS. After the GSS boot process completes, the software prompts you to log in to the device.
2. If you are remotely logging in to the GSS device (Global Site Selector or Global Site Selector Manager) through Telnet or SSH, enter the hostname or IP address of the GSS to access the CLI.

Otherwise, if you are using a direct serial connection between your terminal and the GSS device, use a terminal emulation program to access the GSS CLI.

**Note**

For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

3. Specify your GSS administrative username and password to log in to the GSS device. The CLI prompt appears.

```
localhost.localdomain>
```

4. At the CLI prompt, enable privileged EXEC mode.

```
localhost.localdomain> enable
localhost.localdomain#
```

The prompt changes from the user-level EXEC right angle bracket (>) prompt to the privileged-level EXEC pound sign (#).

# Understanding GSS Software Licenses

You can view a GSS software license as a collection of license packages. A license package is a predefined set of features bundled together and sold as an upgrade to the GSS v1.3 software.

For the v2.0 release, GSS capabilities have been extended through a product coupling with the Cisco Network Registrar (CNR). This coupling allows GSS to provide more standard DNS server functions and behave like a typical Berkeley Internet Name Domain (BIND) DNS server. In addition, GSS now includes support for Distributed Denial of Service (DDoS) attack detection and mitigation.

Both features are purchased as separate CNR and DDoS license add-ons and involve upgrading the existing software license. For detailed overviews and descriptions of the CNR and DDoS features, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide*.

When GSS is upgraded from an unlicensed version (v1.3 and lower) to v2.0 (the licensed version), the software has no license packages installed. All previous version features are available and configurable immediately, except for the specifically licensed features. If you want to enable the DDoS license package on a particular GSS, you must purchase a DDoS license from Cisco Systems in order to receive a Product Access Key (PAK) number.

This section contains the following topics:

- [Acquiring and Installing License Files](#)
- [Installing and Activating CNR](#)

## Acquiring and Installing License Files

The Software Infrastructure and Fulfillment Technology (SWIFT) application is a web-based package provided by Cisco that allows you to retrieve or generate a license file for a particular PAK. SWIFT provides a way for Cisco to track licenses, as well as a way for the customer to recover lost licenses. It also permits internal support organizations to obtain information about customer licenses.

To obtain a license file, perform the following steps:

1. Go online and connect to the Cisco SWIFT web site at <http://www.cisco.com/license>

You will be prompted for various details about your purchase as part of a software registration process.

2. Enter the required data.

After submitting this data, the web site authenticates the information, generates a license file, and emails it to you.



#### Note

We recommend that you make a back-up copy of your license file after you receive it by email in case it is lost or corrupted. Should anything happen to your license file, SWIFT also enables you to regenerate it.

3. Install the license once you have obtained your license file by using the CLI **license** command. A valid license file always includes the .lic extension. Otherwise, it is considered invalid and is not installed.

For example, you can install a DDoS license as follows:

```
gssml.example.com# license install ddos_new.lic
```

The license file is copied to the /licenses directory when the installation is complete.

Should you want to uninstall a license file on the GSS, enter the **license** command with the **uninstall** keyword as follows:

```
gssml.example.com# license uninstall ddos_new.lic
```

## Installing and Activating CNR

You can install CNR without first obtaining the GSS license for the CNR module. You must obtain the CNR license file/key before you install the CNR software package, however. Be sure to download the CNR software package and obtain that CNR license file/key. The CNR package takes the form cnr\_6\_2\_3-linux.gtar.gz.

To install CNR on the GSS, perform the following steps:

1. Install the CNR software package and the CNR license key.

```
gssml.example.com# cnr install cnr_6_2_3-linux.gtar.gz cnr-license  
abc
```

Installing CNR from cli-install. This may take a few minutes.

**Note**

If you provide an invalid or expired license key, an error message appears and the installation halts. The installation will then remove the CNR installation directory which may result in the removal of any previous versions/installations of CNR.

To avoid any potential problems, you should also ensure that each GSS possesses a unique license file. Do *not* install the same licence file (files with the same PAK number) in more than one GSS in the network. If you use the same PAK number, the GSS with the duplicate license file will be deregistered from the GSS network.

**Note**

If a clash of duplicate PAK numbers occurs between the primary and any other GSS in the network, the other GSS is de-registered even if it was using the PAK number before the primary GSS.

To recover a deregistered GSS, you need to perform these steps:

- a. Uninstall the duplicate license file by using the **license uninstall** CLI command.
- b. Stop and then disable the GSS as explained in the corresponding sections later in this chapter.
- c. Reregister the GSS as the primary GSS. See [Chapter 1](#), for more details.

**Note**

The CNR installation does not activate the CNR server agent. Instead, the CNR has to be explicitly enabled in order to start processing requests.

2. Provide the GSS license for the CNR module.

```
gssm1.example.com# license install cnr_new.lic
```

3. Access global configuration mode and enable the CNR server agent.

```
gssm1.example.com# config  
gssm1.example.com (config)# cnr enable  
# Starting Network Registrar Local Server Agent
```

The **cnr enable** command fails if CNR is not installed on the GSS.

```
gssm1.example.com (config)# cnr enable  
CNR enable failed. Please install CNR first
```

To disable CNR, enter the following:

```
gssml.example.com (config)# no cnr enable
# Stopping Network Registrar Local Server Agent
```

This section contains the following topics:

- [Accessing the CNR CLI](#)
- [Invoking the Shell and Executing CNR Utilities](#)

## Accessing the CNR CLI

The CNR command-line interface (the **nrcmd** program) allows you to control your local cluster servers' operations by setting all configurable options, as well as starting and stopping the servers.

To access the **nrcmd** program, perform the following steps:

1. Enter the **cnr** command in the GSS privileged EXEC mode.

```
gssml.example.com# cnr
```



### Note

You must install and enable CNR on the GSS before you can enter the CNR **nrcmd** program. Otherwise, an error message appears.

2. Enter the username and password when the prompts appear.

```
username: <user_name>
password: *****
100 OK
session:
  cluster = localhost
  current-vpn = global
  default-format = user
  groups = superuser
  roles = superuser
  scope-edit-mode = staged
  user-name = admin
  visibility = 5
  zone-edit-mode = synchronous
nrcmd>
```

See v6.2 of the *Cisco CNS Network Registrar CLI Reference Guide* for instructions on using **nrcmd**.

3. Exit the CNR **nrcmd** program.



```
nrcmd> exit
gssml.example.com#
```

## Invoking the Shell and Executing CNR Utilities

The GSS provides a restricted CNR shell that supports built-in Linux commands, such as **cd** and **echo**. It also supports numerous CNR utilities including:

- **cnr\_tactool**—Packages CNR data for TAC support engineers for troubleshooting purpose.
- **cnr\_exim**—Exports or imports CNR data repositories.
- **cnr\_keygen**—Generates keys for Secret Key Transaction Authentication for DNS (TSIG) configuration or key import.

To invoke the CNR shell and execute the CNR utilities, perform the following steps:

1. Enter the **cnr shell** command in the GSS privileged EXEC mode.

```
gssml.example.com# cnr shell
```

2. Press the **Tab** key in the CNR shell to display the supported utilities.

```
cnr shell> cnr <Tab>
cnr_exim          cnr_tactool.origcnrdb_load      cnrdb_verify
cnr_exim.orig     cnrdb_archive   cnrdb_printlog  cnrservagt
cnr_keygen        cnrdb_checkpointcnrdb_recover  cnrsnmp
cnr_keygen.orig   cnrdb_deadlock  cnrdb_stat      cnr_tactool
cnrdb_dump        cnrdb_upgrade  cnr shell >    cnr shell
```

3. Enter the utility name to execute any of these CNR utilities, for example:

```
cnr shell> cnr_tactool
user:
password:
```

See the *Cisco CNS Network Registrar User's Guide* for more information about **cnr\_tactool** and the other available CNR utilities.

# Using the startup-config and running-config Files

When you make device configuration changes, the GSS places those changes in a virtual running configuration file (called running-config). Before you log out or reboot the GSS, you must copy the contents of the running-config file to the startup-configuration file (called startup-config) to save configuration changes. The GSS uses the startup-config file on subsequent reboots.

This section contains the following procedures:

- [Changing the startup-config and running- config Files](#)
- [Saving the startup-config and running-config Files](#)
- [Loading the startup-config from an External File](#)
- [Displaying the running-config File](#)
- [Displaying the startup-config File](#)

## Changing the startup-config and running- config Files

The network configuration for a GSS device includes the following:

- Interface—Ethernet interface in use
- IP address—Network address and subnet mask assigned to the interface
- GSS communications—Interface (Ethernet 0 or Ethernet 1) designated for handling GSS-related communications on the device
- GSS TCP keepalives—Interface (Ethernet 0 or Ethernet 1) designated for outgoing keepalives of type TCP and HTTP HEAD
- Hostname—Hostname assigned to the GSS
- IP default gateway—Network gateway used by the device
- IP name server—Network DNS server being used by the device
- IP routes—All static IP routes
- SSH enable—SSH state of the GSS device (enabled or disabled)
- Telnet enable—Telnet state of the GSS device (enabled or disabled)
- FTP enable—FTP state of the GSS device (enabled or disabled)
- FTP client enable—FTP client state of the GSS device (enabled or disabled)

- SNMP enable—SNMP state of the GSS device (enabled or disabled)

Each GSS device tracks the following configurations:

- Startup configuration—Default network configuration. The GSS loads the startup configuration settings each time you boot the device.
- Running configuration—Network configuration currently in use by the GSS device.

Typically, the running-config and the startup-config files are identical. Once you modify a configuration parameter, you must reconcile the two configuration files in one of the following ways:

- Save the running-config file as the new startup-config file by using the **copy running-config startup-config** command. The GSS retains any changes to the network configuration of the device and uses those changes when the GSS is next rebooted.
- Maintain the startup-config file. In this case, the GSS device uses the running-config file until you reboot the device. The GSS then discards the running-config file and restores the startup-config file.

To change the startup-config file for a GSS device, perform the following steps:

1. Log in to the CLI, enable privileged EXEC mode, and access global configuration mode on the device.

```
gssm1.example.com> enable
gssm1.example.com#
gssm1.example.com# config
gssm1.example.com(config)#
```

2. Make any desired changes to the GSS configuration. For example, to change the device hostname, use the **hostname** command in global configuration mode as follows:

```
gssm1.example.com(config)# hostname new.example.com
new.example.com(config)#
```

3. Copy the current running-config file as the new startup-config file for the GSS by entering the following command:

```
new.example.com(config)# copy running-config startup-config
```

## Saving the startup-config and running-config Files

To save the running-config file to the startup-config file on the GSS, or to copy the current startup configuration to a file for use on other devices or for backup purposes, use one of the following commands:

- **copy startup-config disk *filename***—Copies the GSS device startup configuration to a named file on the GSS.
- **copy running-config disk *filename***—Copies the GSS device current running configuration to a named file on the GSS.
- **copy running-config startup-config**—Copies the GSS device current running configuration as the new startup configuration.

To copy the GSS device running-config or startup-config files, perform the following steps:

1. Log in to the CLI of the primary GSSM, standby GSSM, or a GSS device and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

2. Copy the current startup configuration to a file for use on other devices or for backup purposes by entering the following command:

```
gss1.example.com# copy startup-config disk newstartupconfig
```

The *filename* argument specifies the name of the file containing the startup configuration settings.



### Note

The primary GSSM backup does not include user files that reside in the /home directory. If you want to have a secure copy of the GSS startup-config file, use either the secure copy (**scp**) or **ftp** commands to copy the startup-config file to another device. Storing the startup-config file in a safe location can save time and reconfiguration issues in a recovery situation.

3. Copy the GSS device current running configuration to a named file located on the GSS by entering the following command:

```
gss1.example.com# copy running-config newrunningconfig
```

The *filename* argument specifies the name of the file containing the running configuration settings.

4. Save the running-config file as the new startup-config file by entering the following command:

```
gss1.example.com# copy running-config startup-config
```

The GSS retains any changes to the network configuration of the device and uses those changes when the GSS is next rebooted.

## Loading the startup-config from an External File

In addition to copying your running-config file as a new startup-config file, you can also upload or download GSS device configuration information from an external file using the **copy** command. Before you attempt to load the startup configuration from a file, make sure that the file has been moved to a local directory on the GSS device.

To load the GSS device startup configuration from an external file, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gssm1.example.com> enable  
gssm1.example.com#
```

2. Load the GSS device startup configuration settings from a named file located on the GSS by entering the following command:

```
gssm1.example.com# copy disk startup-config newstartupconfig
```

The *filename* argument specifies the name of the file containing the startup configuration settings.

## Displaying the running-config File

You can review the contents of the GSS running-config file to verify the current configuration parameters in use by the GSS device. To display the contents of the GSS running-config file, use the **show running-config** command. You can use this command with the **show startup-config** command to compare the configuration memory to the startup-config file used during the bootup process.

Configuration entries within each mode in the running-config file appear in chronological order, based on the order in which you configure the GSS. The GSS does not display default configurations in the running-config file.

To display the current running-config file for the GSS, enter the following command:

```
gssm1.example.com# show running-config
interface ethernet 0
    ip address 192.168.1.25 255.255.255.0
    gss-communications
    gss-tcp-keepalives

hostname gssm1.example.com
ip default-gateway 10.86.208.1
ip name-server 172.16.124.122

ssh enable
no ssh keys
no ssh protocol version 1
telnet enable
ftp enable
ftp-client enable all
ntp enable
snmp enable
snmp community-string
    <set>
ntp-server 16.1.1.11
cnr enable
drp
    enable
    authentication key sample key
    path-rttprobe
        burst_size 5
        init_ttl 2
        destination-port 1020
        max-failure-ttl 5
        max-ttl 40
    tcp-rttprobe
        sourceport static 10

terminal length 23
exec-timeout 150

logging disk enable
logging disk priority Notifications(5)
no logging host enable
logging host priority Warnings(4)
```

```
tacacs-server timeout 5
tacacs-server keepalive-enable
```

## Displaying the startup-config File

You can review the contents of the GSS startup-config file to display the configuration used during initial bootup. The GSS stores the contents of the startup-config file in a safe partition of the hard disk to prevent loss of data due to power failures.

To display the contents of the GSS startup-config file, enter the following command:

```
gssm1.example.com# show startup-config
GSS configuration [Saved: Thu Jul 10 16:20:25 UTC 2003]

interface ethernet 0
  ip address 192.168.1.25 255.255.255.0
  gss-communications
  gss-tcp-keepalives

hostname gssm1.example.com
ip default-gateway 10.86.208.1
ip name-server 172.16.124.122
ssh enable
no ssh keys
no ssh protocol version 1
telnet enable
ftp enable
ftp-client enable all
ntp enable
snmp enable
snmp community-string
  <set>

ntp-server 16.1.1.11
cnr enable
```

```

drp
  enable
  authentication key sample key
  path-rttprobe
    burst_size 5
    init_ttl 2
    destination-port 1020
    max-failure-ttl 5
    max-ttl 40
  tcp-rttprobe
    sourceport static 10

terminal length 23
exec-timeout 150
logging disk enable
logging disk priority Notifications(5)
no logging host enable
logging host priority Warnings(4)

tacacs-server timeout 5
tacacs-server keepalive-enable

```

## Managing GSS Files

This section describes how to manage the files included in a directory or subdirectory on a GSS device. This section contains the following topics:

- [Displaying the Contents of a File](#)
- [Displaying Files in a Directory](#)
- [Renaming GSS Files](#)
- [Securely Copying Files](#)
- [Deleting Files](#)

## Displaying the Contents of a File

You can view the contents of a GSS file and monitor functions such as transaction logging or system logging using the system.log file. Use the **tail** and **type** CLI commands to view the contents of a file in a GSS directory as follows:



- Display the last 10 lines of a file within any GSS file director by using the **tail filename** command. This command displays the end of a file within any GSS file directory.
- Display the entire contents of a file within any GSS file directory by using the **type filename** command.

The *filename* argument identifies the name of the file in the GSS file directory. To view the files available in the current directory or subdirectory, use the **dir**, **lls**, **ls**, or **pwd** commands. See the “[Displaying Files in a Directory](#)” section for details.

For example, to display the last 10 lines in the system.log, enter:

```
gssm1.example.com# tail system.log
Showing file system.log
Sep 15 07:11:40 host-css2 rc: Stopping keytable succeeded
Sep 15 07:11:42 host-css2 inet: inetd shutdown succeeded
Sep 15 07:11:45 host-css2 crond: crond shutdown succeeded
Sep 15 07:11:46 host-css2 dd: 1+0 records in
Sep 15 07:11:46 host-css2 dd: 1+0 records out
Sep 15 07:11:46 host-css2 random: Saving random seed succeeded
Sep 15 07:11:48 host-css2 kernel: Kernel logging (proc) stopped.
Sep 15 07:11:48 host-css2 kernel: Kernel log daemon terminating.
Sep 15 07:11:50 host-css2 syslog: klogd shutdown succeeded
Sep 15 07:11:51 host-css2 exiting on signal 15
End of file system.log
```

For example, to display the contents of the audit.log file, enter:

```
gssm1.example.com# type /audit.log
atcr1.cisco.com>type audit.log

# Start logging at Tue July 1 23:59:30 GMT 2003
#=== WHEN                                WHAT_TABLE    WHAT_ID        HOW
===

# Start logging at Wed July 2 00:01:25 GMT 2003
#=== WHEN                                WHAT_TABLE    WHAT_ID        HOW
===

# Start logging at Thu July 3 14:42:40 GMT 2003
#=== WHEN                                WHAT_TABLE    WHAT_ID        HOW
===
...
```

## Displaying Files in a Directory

The GSS software directories contain the GSS files, including boot files, backup files, and log files. Use the **dir**, **lls**, **ls**, or **pwd** commands to view the files available in the current directory or subdirectory on the GSS as follows:

- **dir** [*directory*]**—**Displays a detailed list of files contained within the working directory on the GSS, including names, sizes, and time created. You may optionally specify the name of the directory to list. The equivalent command is **lls**.
- **lls** [*directory*]**—**Displays a detailed list of files contained within the working directory on the GSS, including names, sizes, and time created. You may optionally specify the name of the directory to list. The equivalent command is **dir**.
- **ls** [*directory*]**—**Displays a detailed list of filenames and subdirectories within the working directory on the GSS, including filenames and subdirectories. You may optionally specify the name of the directory to list.
- **pwd** - Displays the current working directory of the GSS.

To view a detailed list of files contained within the working directory, enter:

```
gssml.example.com# dir      (or lls)
total 97684
-rw-r--r--    1 root    root           39 Mar  8 21:04 JVM_EXIT_CODE
-rw-r--r--    1 root    root            9 Mar 14 21:23 RUNMODE
-rw-r--r--    1 root    root        33427 Mar 14 21:23 gss.log
drwxr-xr-x    2 root    root        4096 Mar  7 16:22 admin
drwxr-xr-x    3 root    root        4096 Mar  7 18:05 apache
-rw-r--r--    1 root    root        117 Mar  7 18:05 audit.log
srwxr-xr-x    1 root    root            0 Mar  7 15:40 cli_config
srwxr-xr-x    1 root    root            0 Mar  7 15:40 cli_exec
drwxr-xr-x   14 root    root        4096 Mar  7 18:05 core-files
-rw-r--r--    1 root    root         61 Mar 14 21:23 datafeed.cfg
srwxrwxrwx    1 root    root            0 Mar  7 15:40
dataserver-socket
-rw-r--r--    1 root    root         18 Mar  7 15:39 nicinfo.cfg
-rw-r--r--    1 root    root       5072 Mar  7 18:05 node.state
drwxrwxrwx    2 root    root        4096 Mar  8 21:04 pid
-rw-rw-rw-    1 root    root       9127 Mar 14 21:23 props.cfg
-rw-r--r--    1 root    root         63 Mar 14 21:23
runmode-comment
-rw-r--r--    1 root    root        553 Mar  8 21:02 running.cfg
drwxr-xr-x    4 root    root       4096 Mar  8 18:34 squid
```

```

-rw-r--r--    1 root    root           49 Mar  7 18:05
sysMessages.log
drwxr-xr-x    2 root    root        4096 Mar  7 15:40 sysmsg
drwxrwxrwx    2 root    root        4096 Mar  8 21:02 sysout
-rw-r--r--    1 root    root       41652 Mar 14 21:23 system.log

```

To list the filenames and subdirectories of the current working directory, enter:

```

gssm1.example.com# ls
gss-1.0.2.0.2-k9.upg    id_rsa.pub        megara.back.1_0.full  rpms
gss-1.0.904.0.1-k9.upg  gss_sample.full   megara.back.1_1.full

```

To display the present working directory of the GSS, enter:

```

gssm1.example.com# pwd
/admin

```

## Renaming GSS Files

The GSS software allows you to rename files located in the current directory or subdirectory, such as backup files and log files. To rename a GSS file, use the **rename** command. The syntax for this command is as follows:

**rename** *source\_filename new\_filename*

The arguments are:

- *source\_filename*—Alphanumeric name of the file that you want to rename.
- *new\_filename*—Alphanumeric name to assign to the file.

Quotation marks are not required around filenames. The following special characters are not allowed in the renamed filenames: apostrophe ('), semicolon (;), asterisk (\*), and space ( ).

To view the files available in the current directory or subdirectory, use the **dir**, **ls**, or **pwd** commands. See the “[Displaying Files in a Directory](#)” section for details.

For example, to rename the current GSS startup-config file as *newstartupconfig*, enter:

```

gssm1.example.com# rename startup-config newstartupconfig

```

## Securely Copying Files

The GSS supports the secure copying of files from the GSS device where you are logged in, or from another device to the GSS device where you are currently logged in.



### Note

The GSS supports one-way communication only in SCP. You can copy GSS files from the GSS where you are logged in to an external device. You can also copy files from an external device to the GSS. However, from an external device, you cannot execute the **scp** command and get files from the GSS. You can only use **scp** from the GSS.

Use the **scp** command to securely copy files from the following:

- A GSS device that you are logged in to:

```
scp {source_path [source_filename] user@target_host:target_path}
```

- Another device to the GSS device that you are currently logged in to:

```
scp {user@source_host:/source_path[source_filename] target_path}
```

The argument are as follows:

- *source\_path*—Relative directory path and filename on the source device of the file being transferred.
- *source\_filename*—Name of the file to be copied.
- *user@target\_host*—Login account name and hostname for the device to which you are copying files.
- *target\_path*—Relative directory path on the target device to which the file is being copied.
- *user@source\_host*—Login account name and hostname for the device from which you are copying files.

After you log in to the CLI of the GSS that you intend to copy files to or from, enter the **scp** command as previously described. You may be prompted to log in to the remote device before you can navigate to the target directory.

To securely copy files from a GSS device that you are logged in to, enter:

```
gssml.example.com# scp /tmp/system.log  
myusername@192.168.2.3:/dump/home
```

To securely copy files from another device to a GSS device that you are currently logged in to, enter:

```
gssm1.example.com# scp <file-name of the GSS>  
username@remote-host:target-path
```

## Deleting Files

The GSS allows you to remove a specific file (startup-config, logs, or archive file) stored on hard disk. You may want to remove older files or files that you no longer use from the GSS. To delete files from your GSS, use the **del** command.

The syntax for this command is as follows:

```
del filename
```

The *filename* argument identifies the name of the file in the GSS file directory.

For example, to delete the *oldtechrept.tgz* file, enter:

```
gssm1.example.com# del oldtechrept.tgz
```

## Displaying Users

You can display the username and permission status for a specific user or for all users of the GSS device as follows:

- Use the **show user** *username* command to display user information for a particular user. The *username* argument identifies the name of the GSS user that you want to display information for.
- Use the **show users** command to display information for all GSS users.

To display information for a particular user, enter:

```
gssm1.example.com# show user paulr-admin  
Username      permission  
-----  
paulr-admin   admin
```

To display information for all users, enter:

```
gssm1.example.com# show users  
Username      permission  
-----  
-----
```

```
lstar      admin
admin      admin
paulr-admin admin
```

For details about creating GSS users, refer to [Chapter 3, Creating and Managing User Accounts](#).

## Specifying the GSS Inactivity Timeout

You can modify the length of time that can expire before a GSS automatically logs off an inactive user by using the **exec-timeout** command. This command specifies the length of time that a user in privileged EXEC mode can be idle before the GSS terminates the session. Users logged on to GSS devices in the global configuration mode are not affected by the **exec-timeout** command setting. The default inactivity timeout value is 150 minutes.

The syntax for the **exec-timeout** command is as follows:

**exec-timeout** *minutes*

The *minutes* argument specifies the length of time that a user in privileged EXEC mode can be idle before the GSS terminates the session. Valid entries are 1 to 44,640 minutes. The default is 150 minutes.

For example, to specify a GSS timeout period of 10 minutes, enter:

```
gssml.example.com(config)# exec-timeout 10
```

To restore the default timeout value of 150 minutes, use the **no** form of this command.

## Configuring the Terminal Screen Line Length

You can specify the number of screen lines to display on your terminal by using the **terminal length** command. The maximum number of displayed screen lines is 512. The default is 23 screen lines. When the **terminal length** command is set to a value of 0, the GSS sends all of its data to the screen at once without pausing to buffer the data. To restore the default terminal length of 23 lines, use the **no** form of this command.

The syntax for this command is as follows:

**terminal-length** *number*

The *number* argument specifies the number of screen lines to display on your terminal, from 0 and 512. The default is 23 lines.

For example, to set the number of screen lines to 35, enter:

```
gssm1.example.com(config)# terminal-length 35
```

To reset the number of screen lines to the default of 23, enter:

```
gssm1.example.com(config)# no terminal-length
```

To display the terminal length setting for your GSS device, use the **show terminal-length** command.

For example:

```
gssm1.example.com# show terminal-length  
terminal length 35
```

## Modifying the Attributes of the Security Certificate on the GSSM

You can customize the attributes of the security certificate issued by Cisco Systems and installed on the primary GSSM (as described in the [“Logging Into the Primary GSSM Graphical User Interface”](#) section in [Chapter 1, , Managing GSS Devices from the GUI](#)). By using the **certificate set-attributes** CLI command, you can modify the X.509 fields, extensions, and properties included on the security certificate. The attribute changes that you make affect the fields on the Details tab of the certificate. To return the attributes for the security certificate to the default settings, use the **no** form of the **certificate set-attributes** command.

When you enter the **certificate set-attributes** command, the GSS software displays a series of prompts related to the fields on the certificate. Proceed through all of the prompts and make changes only to those fields that you want to modify. When completed, the software prompts you to save your changes and generate a new certificate. The next time that you access the primary GSSM GUI, the Security Alert dialog box reappears informing you that the certificate is invalid. At that point, you can either reinstall the updated certificate or close the dialog box and continue with the primary GSSM GUI operation.

To modify the attributes of a security certificate on the primary GSSM, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gssm1.example.com> enable
gssm1.example.com#
```

2. Enter the **gss stop** command to stop the GSS software. Modifications to the certificate cannot occur while the GUI is active on the primary GSSM.

```
gssm1.example.com# stop
```

3. Access global configuration mode on the device.

```
gssm1.example.com# config
gssm1.example.com(config)#
```

4. Enter the **certificate set-attributes** command and modify information at the prompts. All fields displayed for each software prompt have a maximum character limit of 64, except for Country Code, which has a maximum character limit of 2.

```
gssm1.example.com(config)# certificate set-attributes
Country code (2 chars) [US]:
State [California]: MA
City [San Jose]: Boston
Organization [Cisco Systems, Inc.]: New Organization
Organization Unit [ISBU]:
e-Mail Address [tac@cisco.com]: company@mycompany.com

US
MA
Boston
New Organization
ISBU
company@mycompany.com
```

5. Enter **y** to save these values (or **n** to use the existing certificate values).

```
Save these values? (y/n): y
```

6. Restart the GSS device.

```
gssm1.example.com(config)# exit
gssm1.example.com# gss start
```



## Stopping the GSS Software

You must stop the GSS software before you perform the following tasks:

- Upgrade GSS software
- Perform a warm reboot
- Restore GSS factory defaults
- Disable an active GSS device
- Perform GSS maintenance or troubleshooting

Use the **gss stop** command to stop the GSS software. For example, enter:

```
gssm1.example.com# gss stop
```

The following message appears when you stop the GSS software from the CLI.

```
Server is Shutting Down
```

Use the **gss start** command to restart the GSS software on the selected device after it has been stopped. For example, enter:

```
gssm1.example.com# gss start
```

## Shutting Down the GSS Software

If you intend to power down a GSS device, we recommend that you use the **shutdown** command to first shut down the GSS software. You should also shut down the GSS software before you disable a GSS (see the [“Disabling the GSS Software”](#) section).

To shut down the GSS software, enter:

```
gssm1.example.com# shutdown
```

## Restarting the GSS Software

You can perform a warm restart of the GSS software by using the **gss restart** command. Before you perform a warm restart of the GSS software, save your recent GSS configuration changes to memory. Use the **copy running-config**

**startup-config** CLI command to save your configuration changes. If you fail to save your configuration changes, the GSS device reverts to its previous settings upon a reboot.

To perform a warm restart of the GSS, enter:

```
gssm1.example.com# gss restart
```

As the GSS reboots, the output appears on the console terminal.

## Performing a Cold Restart of a GSS Device

You can halt GSS operation and perform a cold restart of your GSS device by using the **reload** command. The **reload** command reboots the GSS device and performs a full power cycle of both the GSS hardware and software. Any open connections with the GSS are dropped after you enter the **reload** command.

Before you perform a cold restart of the GSS, save your recent GSS configuration changes to memory. Use the **copy running-config startup-config** CLI command to save your configuration changes. If you fail to save your configuration changes, the GSS device reverts to its previous settings upon restart.

To halt and perform a cold restart of the GSS, enter:

```
gssm1.example.com# reload
```

As the GSS boots, the output appears on the console terminal.

## Disabling the GSS Software

Disabling a GSS device is necessary when you need to perform the following tasks:

- Switch the role of a GSS within a network
- Change a GSS to a GSSM
- Move a GSS or GSSM to a different network of GSS devices

Use the **gss disable** command to disable a selected GSSM or GSS. This command removes the existing configuration and returns the GSS device to its initial state, which includes deleting the GSSM database from the GSS device and removing all configured DNS rules and keepalives. The **gss disable** command also removes any certificate attributes specified using the **certificate set-attributes** command.

To disable a GSS device, enter:

```
gssm1.example.com# gss disable  
gssm1.example.com# shutdown
```

To reenable the GSS device as a primary GSSM, standby GSSM, or a GSS, see the *Cisco Global Site Selector Getting Started Guide*.

## Restoring GSS Factory-Default Settings

The **restore-factory-defaults** command erases your GSSM database and all of its data and resets all network settings, returning your GSS hardware to the same state it was in when it first arrived from the factory. If your GSS device is improperly configured, use the **restore-factory-defaults** command to restore the device to its initial state and allow you to properly configure the GSS device for use on your network.

Before you enter the **restore-factory-defaults** command, ensure that you back up any vital data in the database component of the primary GSSM, along with its network and device configuration information. Use the **gssm backup** command to perform a primary GSSM backup. See [Chapter 7](#), [Backing Up, Restoring, and Downgrading the GSSM Database](#) for details.



### Caution

User files will also be deleted when you enter the **restore-factory-defaults** command. If you have any important files in the /home directory that you want to save, use either the secure copy (**scp**) or **ftp** commands to copy those files before you enter the **restore-factory-defaults** command.

Enter the **gss stop** command before you execute the **restore-factory-defaults** command to stop the GSS software and avoid disrupting in-process activities (for example, serving DNS requests or sending keepalives).

To restore GSS factory default settings, enter:

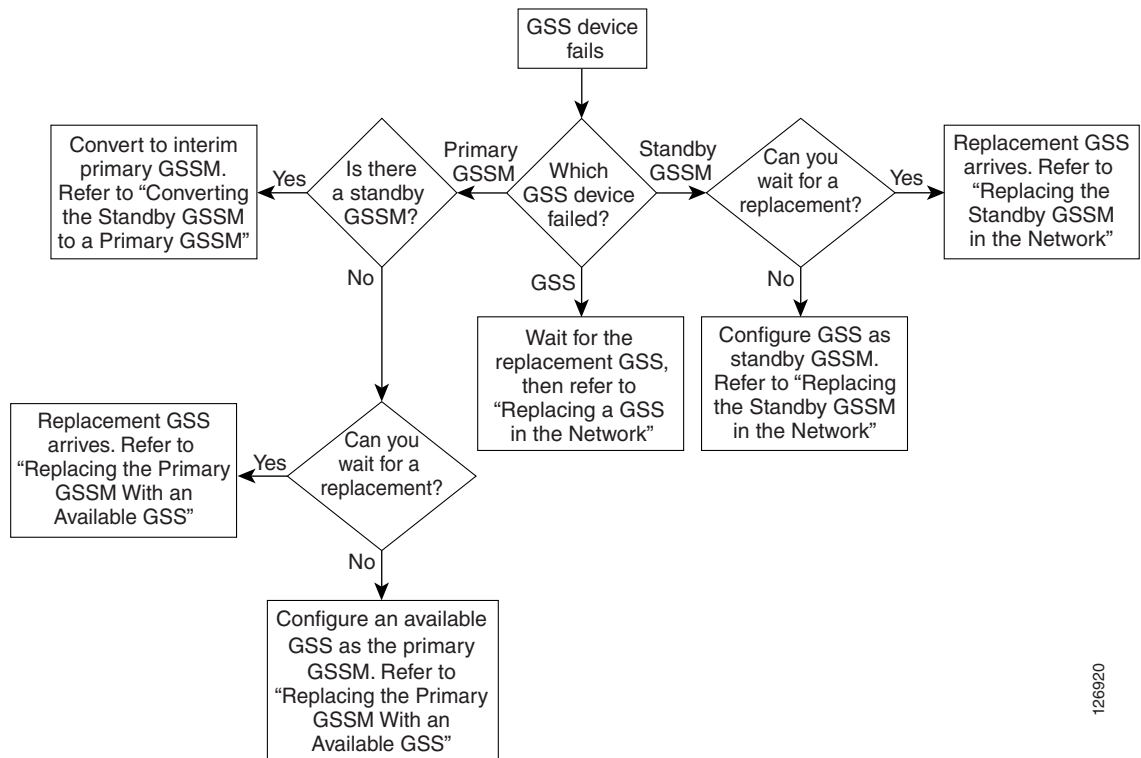
```
gssm1.example.com# gss stop
```

```
gssm1.example.com# restore-factory-defaults
```

# Replacing GSS Devices in Your GSS Network

If you encounter problems with one of the GSS devices in your network, determine which GSS device contains the problem (primary GSSM, standby GSSM, or GSS) and configure a replacement GSS device for your network. [Figure 2-1](#) summarizes the decision-making process to follow when replacing a malfunctioning GSS device.

**Figure 2-1** Flow Chart for Replacing a Malfunctioning GSS Device



126920

This section contains the following topics:

- [Replacing the Primary GSSM in the Network](#)

- [Replacing the Standby GSSM in the Network](#)
- [Replacing a GSS in the Network](#)

## Replacing the Primary GSSM in the Network

To replace a malfunctioning primary GSSM in your GSS network to regain GUI management, determine if there is a standby GSSM available in your network:

- If you have a standby GSSM that you can convert to the primary GSSM, see the [“Converting the Standby GSSM to a Primary GSSM”](#) section.
- If you do not have a standby GSSM but do have an available GSS that you can convert to the primary GSSM, see the [“Replacing the Primary GSSM with an Available GSS”](#) section.

## Converting the Standby GSSM to a Primary GSSM



### Note

Ensure that the designated primary GSSM is either offline or configured as a standby GSSM before you attempt to enable the standby GSSM as the new interim primary GSSM. Having two primary GSSM devices active at the same time may result in the inadvertent loss of configuration changes for your GSS network.

To convert the standby GSSM to a primary GSSM, perform the following steps:

1. Log in to the CLI of the primary GSSM, enable privileged EXEC mode, and perform a full backup of your primary GSSM to preserve your current network and configuration settings (see the [“Performing a Full Primary GSSM Backup”](#) section in [Chapter 7](#), [Backing Up, Restoring, and Downgrading the GSSM Database](#)).
2. Log in to the CLI of the standby GSSM and enable privileged EXEC mode.  

```
gssm2.example.com> enable  
gssm2.example.com#
```
3. Configure the current standby GSSM to function as the temporary primary GSSM for your GSS network. Use the **gssm standby-to-primary** command to reconfigure your standby GSSM as the primary GSSM in your GSS network.

```
gssm2.example.com# gssm standby-to-primary
```

**Note**

After entering the **gssm primary-to-standby** command, you should ensure that at least 1 minute passes before you enter the **gssm standby-to-primary** command in order to allow time for proper GSS device synchronization.

Configuration changes do not take effect immediately. It may take up to 10 minutes before the other GSS devices in the network learn about the new primary GSSM.

4. Validate the database records of the interim primary GSSM by entering the following command.

```
gssm2.example.com# gssm database validate
```

5. Exit privileged EXEC mode. The standby GSSM begins to function in its new role as the interim primary GSSM and is now fully functional. You may now access the GUI.
6. When the replacement for the original primary GSSM is available, place the current interim primary GSSM in standby mode by entering the following command:

```
gssm2.example.com# gssm primary-to-standby
```

This command allows the current interim primary GSSM to resume its role in the GSS network as the standby GSSM.

7. Exit from the CLI of the standby GSSM.
8. Log in to the CLI of the GSS replacement for the original primary GSSM and enable privileged EXEC mode.

```
gssm1.example.com> enable
gssm1.example.com#
```

9. Configure basic network connectivity settings following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS. Specify the same hostname and IP address of the original primary GSSM.
10. Save your configuration changes to memory by entering the following command:

```
gssm1.example.com# copy running-config startup-config
```

11. Configure the GSS device as the replacement primary GSSM in the GSS network by entering the following command:

```
gssml.example.com# gss enable gssm-primary
```



**Note** After entering the **gssm primary-to-standby** command, you should ensure that at least 1 minute passes before you enter the **gssm standby-to-primary** command in order to allow time for proper GSS device synchronization.

Configuration changes do not take effect immediately. It may take up to 10 minutes before the other GSS devices in the network learn about the new primary GSSM.

12. Determine if you have a full backup of the interim primary GSSM database that you can restore on the new primary GSSM as follows:
  - If yes, restore the interim primary GSSM database. See the “[Restoring a Primary GSSM Backup](#)” section in [Chapter 7](#), , [Backing Up, Restoring, and Downgrading the GSSM Database](#). You can now use the replacement primary GSSM in your GSS network.
  - If no, determine if you have a backup of the original primary GSSM database as follows:
    - If yes, restore the original primary GSSM database. See the “[Restoring a Primary GSSM Backup](#)” section in [Chapter 7](#), , [Backing Up, Restoring, and Downgrading the GSSM Database](#). Verify the existing global server load-balancing configuration settings (DNS rules and keepalives) and modify the settings as described in the *Cisco Global Server Load-Balancing Configuration Guide* (GUI-based or CLI-based version). You can now use the replacement primary GSSM in your GSS network.
    - If no, proceed to Step 13.
13. If you do not have a backup of either the interim or original primary GSSM database, do the following:
  - a. Reconfigure the global server load-balancing configuration settings on the new primary GSSM as described in the *Cisco Global Site Selector Global Server Load-Balancing Configuration Guide* (GUI-based or CLI-based version).

- b. Send DNS queries to the new primary GSSM and ensure that it replies properly to the queries. If the new primary GSSM replies properly, proceed to step 13c. If it fails to reply properly, verify the network connectivity settings and resend DNS queries to the device.
- c. At the CLI of the standby GSSM and of each GSS device in your network, enter the **gss disable** command to remove the existing configuration, including the deletion of the GSSM database from the standby GSSM, and return the GSS device to an initial state. The deletion process includes removing all previously configured DNS rules and keepalives.

```
gssm2.example.com# gss disable
```

- d. At the CLI of the standby GSSM, enter the **gss enable gssm-standby** command to configure the GSS device as the standby GSSM in the GSS network and direct it to the primary GSSM. See the [“Replacing the Standby GSSM in the Network”](#) section for details about the **gss enable gssm-standby** command.

```
gssm2.example.com# gss enable gssm-standby gssm1.example.com
```

- e. At the CLI of each GSS, enter the **gss enable** command to enable your GSS device as a GSS and direct it to the primary GSSM. Specify either the domain name or the network address of the primary GSSM. See the [“Replacing a GSS in the Network”](#) section for details about the **gss enable** command.

**Note**

You may want to perform this step on one GSS device at a time to minimize disruptions on your GSS network.

```
gss3.example.com# gss enable gss gssm1.example.com
```

- f. Register the standby GSSM and each GSS device with the new primary GSSM. See the [“Activating GSS Devices from the Primary GSSM”](#) section in [Chapter 1, , Managing GSS Devices from the GUI](#).

You can now use the replacement primary GSSM in your GSS network.



## Replacing the Primary GSSM with an Available GSS

To replace a malfunctioning primary GSSM with an available GSS, perform the following steps:

1. Determine if you can wait for a replacement primary GSSM or if you require an immediate primary GSSM configuration change in your network to preserve the network configuration as follows:
  - If yes, wait until the replacement GSS is available and configure it as the primary GSSM. Proceed to Step 6.
  - If no, configure an available GSS device as the primary GSSM. Proceed to Step 2.
2. Log in to the CLI of the primary GSSM, enable privileged EXEC mode, and perform a full backup of your primary GSSM to preserve your current network and configuration settings (see the [“Performing a Full Primary GSSM Backup”](#) section in [Chapter 7](#), [Backing Up, Restoring, and Downgrading the GSSM Database](#)).
3. Log in to the CLI of the GSS and enable privileged EXEC mode.

```
gss3.example.com> enable
gss3.example.com#
```

4. Stop the GSS software running on the GSS by entering the following command:

```
gss3.example.com# gss stop
```

5. Remove the existing configuration and return the GSS device to an initial state, including the removal of all previously configured DNS rules and keepalives, by entering the following command:

```
gss3.example.com# gss disable
```

6. If this is a new GSS device, configure basic network connectivity settings following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS. Ensure that you specify the same hostname and IP address of the original primary GSSM.
7. Save your configuration changes to memory by entering the following command:

```
gssm1.example.com# copy running-config startup-config
```

8. Configure the GSS device as the primary GSSM in the GSS network by entering the following command:

```
gssm1.example.com# gss enable gssm-primary
```

9. Determine if you have a full backup of the original primary GSSM database that can be loaded on the replacement GSS as follows:
  - If yes, restore the primary GSSM database as described in the [“Restoring a Primary GSSM Backup”](#) section in [Chapter 7](#), [Backing Up, Restoring, and Downgrading the GSSM Database](#).
  - If no, proceed to Step 10.
10. If you do not have a backup of the original primary GSSM database, do the following:

- a. Reconfigure the global server load-balancing configuration settings on the new primary GSSM as described in the *Cisco Global Site Selector Global Server Load-Balancing Configuration Guide* (GUI-based or CLI-based version).
- b. Send DNS queries to the new primary GSSM and ensure that it replies properly to the queries. If the new primary GSSM replies properly, proceed to Step 10c. If it fails to reply properly, verify the network connectivity settings and resend DNS queries to the device.
- c. At the CLI of the standby GSSM and of each GSS device in your network, enter the **gss disable** command to remove the existing configuration, including the deletion of the GSSM database from the standby GSSM, and return the GSS device to an initial state. The deletion process includes removing all previously configured DNS rules and keepalives.

```
gssm2.example.com# gss disable
```

- d. At the CLI of the standby GSSM, enter the **gss enable gssm-standby** command to reenab the standby GSSM in the GSS network and direct it to the primary GSSM. See the [“Replacing the Standby GSSM in the Network”](#) section for details about the **gss enable gssm-standby** command.

```
gss1.example.com# gss enable gssm-standby gssm1.example.com
```

- e. At the CLI of each GSS, enter the **gss enable** command to enable your GSS device as a GSS and direct it to the primary GSSM. Specify either the domain name or the network address of the primary GSSM. See the [“Replacing a GSS in the Network”](#) section for details about the **gss enable** command.



**Note** You may want to perform this step on one GSS device at a time to minimize disruptions on your GSS network.

```
gss3.example.com# gss enable gss gssm1.example.com
```

- f. Register the standby GSSM and each GSS device with the new primary GSSM. See the [“Activating GSS Devices from the Primary GSSM”](#) section in [Chapter 1, Managing GSS Devices from the GUI](#).

You can now use the replacement primary GSSM in your GSS network.

## Replacing the Standby GSSM in the Network

To replace a malfunctioning standby GSSM in your GSS network, perform the following steps:

1. Determine if you can wait for the replacement standby GSSM or if you require an immediate configuration change in your GSS network as follows:
  - If yes, wait until the replacement GSS is available and configure it as the standby GSSM. Proceed to Step 5.
  - If no, configure an available GSS device as the standby GSSM. Proceed to Step 2.
2. Log in to the CLI of the GSS and enable privileged EXEC mode.

```
gss3.example.com> enable
gss3.example.com#
```
3. Stop the GSS software running on the GSS by entering the following command:

```
gss3.example.com# gss stop
```
4. Disable the GSS to remove the existing configuration and return the GSS device to an initial state by entering the following command:

```
gss3.example.com# gss disable
```

This command removes all previously configured DNS rules and keepalives.

5. If this is a new GSS device, configure basic network connectivity following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS.
6. Save your configuration changes to memory by entering the following command:

```
gss3.example.com# copy running-config startup-config
```

7. If this is an existing GSS device, delete it from your GSS network through the primary GSSM GUI. See the “[Deleting GSS Devices](#)” section in [Chapter 1](#), , [Managing GSS Devices from the GUI](#).
8. If you want to use the same hostname and IP address of the failed standby GSSM, determine if you have a backup of the startup-configuration file for that device as follows:
  - If yes, reload the backup copy of the GSS device startup configuration settings (see the “[Saving the startup-config and running-config Files](#)” section).
  - If no, reenter the platform configuration following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS.
9. Save your configuration changes to memory by entering the following command:

```
gss3.example.com# copy running-config startup-config
```

10. Configure the GSS device as the standby GSSM in the GSS network and direct it to the primary GSSM by entering the **gss enable gssm-standby** command.

The syntax for this command is as follows:

```
gss enable gssm-standby primary_GSSM_hostname |
primary_GSSM_IP_address
```

The argument are as follows:

- *primary\_GSSM\_hostname*—DNS hostname of the device currently serving as the primary GSSM

- *primary\_GSSM\_IP\_address*—DNS hostname of the device currently serving as the primary GSSM

For example, to enable gss3.example.com as the standby GSSM and direct it to the primary GSSM, gssm1.example.com, enter:

```
gss3.example.com# gss enable gssm-standby gssm1.example.com
```

11. Activate the standby GSSM from the primary GSSM GUI to add it to your GSS network. See the “[Activating GSS Devices from the Primary GSSM](#)” section in [Chapter 1](#), [Managing GSS Devices from the GUI](#).

You can now use the replacement standby GSSM in your GSS network.

## Replacing a GSS in the Network

To replace a malfunctioning GSS in your GSS network, perform the following steps:

1. Configure basic network connectivity for the replacement GSS device following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS.
2. If you want to use the same hostname and IP address of the failed GSS, determine if you have a backup of the startup-configuration file for that device as follows:
  - If yes, reload the backup copy of the GSS device startup configuration settings (see the “[Saving the startup-config and running-config Files](#)” section).
  - If no, reenter the platform configuration following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS.
3. If this is an existing GSS device, delete it from your GSS network through the primary GSSM GUI. See the “[Deleting GSS Devices](#)” section in [Chapter 1](#), [Managing GSS Devices from the GUI](#).
4. Enable your GSS device as a GSS and direct it to the primary GSSM in your GSS network by entering the **gss enable** command.

The syntax for this command is:

```
gss enable gss primary_GSSM_hostname | primary_GSSM_IP_address
```

The arguments are as follows:

- *primary\_GSSM\_hostname*—DNS hostname of the device currently serving as the primary GSSM.
- *primary\_GSSM\_IP\_address*—DNS hostname of the device currently serving as the primary GSSM.

For example, to enable gss3.example.com as a GSS and direct it to the primary GSSM, gssm1.example.com, enter:

```
gss3.example.com# gss enable gss gssm1.example.com
```

5. Save your configuration changes to memory by entering the following command:

```
gss3.example.com# copy running-config startup-config
```

6. Activate the GSS from the primary GSSM GUI to add it to your GSS network. See the [“Activating GSS Devices from the Primary GSSM”](#) section in [Chapter 1, , Managing GSS Devices from the GUI](#).

You can now use the replacement GSS in your GSS network.

## Changing the GSSM Role in the GSS Network

The GSS software supports two GSSM devices in a single GSS network, with one GSSM acting as the primary GSSM and the second GSSM acting as a standby device. The standby GSSM can temporarily take over the role of the primary GSSM if the primary GSSM is unavailable (for example, you need to move the primary GSSM or you want to take it offline for repair or maintenance).

Using the CLI, you can manually switch the roles of your primary and standby GSSM devices at any time.

Before switching GSSM roles, follow these guidelines:

- You must configure and enable both a primary and a standby GSSM in your GSS network. Do not attempt to switch GSSM roles until you configure and enable both a primary and a standby GSSM (see the *Cisco Global Site Selector Getting Started Guide*).

- Ensure that the designated primary GSSM is either offline or configured as a standby GSSM before you attempt to enable the standby GSSM as the new primary GSSM. Having two primary GSSM devices active at the same time may result in the inadvertent loss of configuration changes for your GSS network.

Although DNS request routing continues to function in such a situation, GUI configuration changes made on one or both primary GSSM devices may be lost or overwritten and are not communicated to the GSS devices. If this dual primary GSSM configuration occurs, the two primary GSSM devices change to standby mode. You must then reconfigure the original deployed primary GSSM as the primary GSSM.

- The switching of roles between the designated primary GSSM and the standby GSSM is intended to be a temporary GSS network configuration until the original primary GSSM is back online. Use the interim primary GSSM to monitor GSS network behavior and, if necessary, to make configuration changes.

This section contains the following topics:

- [Switching the Roles of the Primary and Standby GSSM Devices](#)
- [Reversing the Roles of the Interim Primary and Standby GSSM Devices](#)

## Switching the Roles of the Primary and Standby GSSM Devices

This procedure assumes that your primary GSSM is online and functional when you are switching GSSM roles. If the primary GSSM is not functional, proceed to Step 6.

To change the role of your primary and standby GSSM devices, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gssm1.example.com> enable
gssm1.example.com#
```

2. Perform a full backup of your primary GSSM to preserve your current network and configuration settings (see the “[Performing a Full Primary GSSM Backup](#)” section in [Chapter 7](#), , [Backing Up, Restoring, and Downgrading the GSSM Database](#)).

3. Configure the current primary GSSM as the standby GSSM. Use the **gssm primary-to-standby** command to place the primary GSSM in standby mode.

```
gssm1.example.com# gssm primary-to-standby
```

4. (Optional) Power down the primary GSSM by entering the following command:

```
gssm1.example.com# shutdown
```

5. Exit from the CLI of the primary GSSM.
6. Log in to the CLI of the standby GSSM and enable privileged EXEC mode.

```
gssm2.example.com> enable
```

7. Configure the current standby GSSM to function as the temporary primary GSSM for your GSS network. Use the **gssm standby-to-primary** command to reconfigure your standby GSSM as the primary GSSM in your GSS network.

```
gssm2.example.com# gssm standby-to-primary
```




---

**Note** After entering the **gssm primary-to-standby** command, you should ensure that at least 1 minute passes before you enter the **gssm standby-to-primary** command in order to allow time for proper GSS device synchronization.

---

Configuration changes do not take effect immediately. It may take up to 10 minutes before the other GSS devices in the network learn about the new primary GSSM.

8. Validate the database records of the interim primary GSSM by entering the following command:

```
gssm2.example.com# gssm database validate
```

9. Exit privileged EXEC mode. The standby GSSM begins to function in its new role as the interim primary GSSM and is now fully functional. You may now access the GUI.



## Reversing the Roles of the Interim Primary and Standby GSSM Devices

When the original primary GSSM is available for use in the network, reverse the roles of the two GSSM devices back to the original GSS network deployment.



### Note

If your original primary GSSM has been replaced by Cisco Systems, see the [“Replacing the Primary GSSM with an Available GSS”](#) section for details about replacing a primary GSSM with a new GSS device.

To reverse the roles of the interim primary and standby GSSM devices, perform the following steps:

1. Log in to the CLI of the interim primary GSSM and enable privileged EXEC mode.

```
gssm2.example.com> enable
gssm2.example.com#
```

2. If the GUI configuration has changed, perform a full backup of the interim primary GSSM to preserve the current network and configuration settings (see the [“Performing a Full Primary GSSM Backup”](#) section in [Chapter 7](#), [Backing Up, Restoring, and Downgrading the GSSM Database](#)).
3. Place the current interim primary GSSM in standby mode to resume its role in the GSS network as the standby GSSM by entering the following command:

```
gssm2.example.com# gssm primary-to-standby
```

Ensure that a minimum of five minutes have passed since the last GUI configuration change before you enter the **gssm primary-to-standby** command to convert the interim primary GSSM back to its role as standby GSSM.

4. Exit from the CLI of the standby GSSM.
5. Log in to the CLI of the primary GSSM from your original network deployment. The CLI prompt appears.
6. Enable privileged EXEC mode on the primary GSSM.

```
gssm1.example.com> enable
```

7. Return the standby GSSM to its role as the original primary GSSM in the GSS network by entering the following command:

```
gssml.example.com# gssm standby-to-primary
```

**Note**

After entering the **gssm primary-to-standby** command, you should ensure that at least 1 minute passes before you enter the **gssm standby-to-primary** command in order to allow time for proper GSS device synchronization.

Configuration changes do not take effect immediately. It may take up to 10 minutes before the other GSS devices in the network learn about the new primary GSSM.

You can now use the primary GSSM as in the original GSS network deployment.

## Displaying GSS System Configuration Information

The GSS CLI provides a comprehensive set of **show** commands that display GSS configuration information. The **show** commands are available in all CLI modes.

This section contains the following topics:

- [Displaying Software Version Information](#)
- [Displaying License Information](#)
- [Displaying Memory Information](#)
- [Displaying Boot Configuration](#)
- [Displaying GSS Processes](#)
- [Displaying System Uptime](#)
- [Displaying Disk Information](#)
- [Displaying UDI Data](#)
- [Displaying System Status](#)
- [Displaying GSS Services](#)

## Displaying Software Version Information

You can display the software version information about the GSS software by using the **show version** command. The syntax for the **show version** command is as follows:

**show version [verbose]**

Specify the **verbose** optional keyword if you want to view detailed GSS software version information.

To display general GSS software version information, enter:

```
gssml.example.com# show version
```

```
Global Site Selector (GSS)
Model Number: GSS-4492-K9
Copyright (c) 1999-2007 by Cisco Systems, Inc.
```

```
Version 2.0 (1.0.0)
```

```
Uptime: 4 Hours 0 Minutes and 19 seconds
```

To display detailed GSS software version information, enter:

```
gssml.example.com# show version verbose
```

```
Global Site Selector (GSS)
Model Number: GSS-4490-K9
Copyright (c) 1999-2003 by Cisco Systems, Inc.
```

```
Version 1.3(1)
```

```
Uptime: 23 Hours 57 Minutes and 53 seconds
```

```
Full Version: 1.3(1.0.0)
Compiled on Wed Feb 15 05:51:07 2006 by ralexand from gss-builder -
changeset 26190
```

```
Processor 0: Pentium III (Coppermine) GenuineIntel
Bridge: Intel Corporation 82371AB PIIX4 ACPI (rev 02)
Ethernet controller: Intel Corporation 82557 [Ethernet Pro 100] (rev 08)
Ethernet controller: Intel Corporation 82557 [Ethernet Pro 100] (rev 08)
IDE interface: Intel Corporation 82371AB PIIX4 IDE (rev 01)
ISA bridge: Intel Corporation 82371AB PIIX4 ISA (rev 02)
```

```

PCI bridge: Intel Corporation 440BX/ZX - 82443BX/ZX AGP bridge (rev
03)
SCSI storage controller: Symbios Logic Inc. (formerly NCR) 53c895 (rev
02)
USB Controller: Intel Corporation 82371AB PIIX4 USB (rev 01)
VGA compatible controller: Chips and Technologies F69000 HiQVideo (rev
64)

0000-001f : dma1 | 0020-003f : pic1
0040-005f : timer | 0060-006f : keyboard
0070-007f : rtc | 0080-008f : dma page reg
00a0-00bf : pic2 | 00c0-00df : dma2
00f0-00ff : fpu | 02f8-02ff : serial(auto)
03d4-03d5 : cga | 03f8-03ff : serial(auto)
6c00-6c7f : ncr53c8xx | 7000-701f : Intel Speedo3 Ethernet
7400-741f : Intel Speedo3 Ethernet | fc00-fc07 : ide0
fc08-fc0f : ide1 |
gssm1.example.com: scsi0 Channel: 00 Id: 00 Lun: 00
Vendor: IBM Model: IC35L018UCD210-0 Rev: S5BS
Type: Direct-Access ANSI SCSI revision: 03

```

## Displaying License Information

You can display information about installed GSS licenses by using the **show license** command and its options.

To obtain a listing of the currently-active license modules, enter:

```

gssm1.example.com# show license active
Enabled modules are
DDoS

```

To see which license files are installed, enter:

```

gssm1.example.com# show license installed
License modules are
DDoS
CNR

```

To obtain a complete listing of the license files, enter:

```

gssm1.example.com# show license file-name list
ddos_new.lic

```

To obtain specific license file details, enter:

```
gssm1.example.com# show license file-name ddos_new.lic
FEATURE ddos cisco 1 permanent uncounted HOSTID=ANY \
NOTICE="<LicFileID>ddos_new.lic</LicFileID><LicLineID>0</LicLineID> \
<PAK>1XIOS2C84AB</PAK>" SIGN=CFF95D462F42
```

To obtain a complete picture of the licenses installed in the GSS network from the primary GSS, enter:

```
gssm1.example.com# show license gss-all
Own (Primary GSS) info :
Pak number is :
    1XIOS2C81AB
DDoS Installed, Active
CNR Installed, Active

Other GSS info :

Address : 2.7.0.2
Pak number are :
    1XIOS2C87AB
DDoS Installed, Active
CNR Installed, Active

Address : 2.3.0.2
Pak number is:
    1XIOS2C83AB
DDoS Installed, Active
CNR Installed, Active
```

## Displaying Memory Information

You can display information about the GSS memory blocks and statistics by using the **show memory** command.

```
gssm1.example.com# show memory
```

[Table 2-1](#) describes the fields in the **show memory** output.

**Table 2-1** Field Descriptions for **show memory** Command

Field	Description
Memory:	
total	Total usable megabytes of RAM on the GSS.

**Table 2-1** *Field Descriptions for show memory Command*

Field	Description
free	Available megabytes of RAM on the GSS.
Mem:	
total	Total usable megabytes of RAM on the GSS.
used	Currently used RAM.
free	Currently available RAM.
shared	Memory shared between processes, always 0 (zero).
buffers	Memory allocated as the internal kernel buffer space.
cached	Memory allocated for the internal caching of file system data. This memory is reclaimed as needed.
Swap:	
total	Total megabytes of swap space on the GSS.
used	Currently used swap space.
free	Currently available swap space.

## Displaying Boot Configuration

You can display information about the GSS software, such as the current boot image and boot device information, by using the **show boot-config** command.

```
gssml.example.com# show boot-config
```

[Table 2-2](#) describes the fields in the **show boot-config** output.

**Table 2-2** *Field Descriptions for show boot-config Command*

Field	Description
Boot Device	Physical device used to boot the GSS software.
Timeout	Length of time that the Linux boot manager, LILO (Linux Loader) waits to receive an input before automatically booting the GSS device.

**Table 2-2** *Field Descriptions for show boot-config Command*

Field	Description
Label	GSS software version that appears at the LILO prompt.
GSS Software Version	Current GSS software version associated with the Label.
Root Partition	Device used for the Linux root partition (the core of the Linux file system).
Linux Kernel	Version of the Linux kernel used by the GSS software image.
Default Boot Image	Listed software version of the default boot image for the GSS device.

## Displaying GSS Processes

You can display a list of internal GSS device processes by using the **show processes** command.

```
gssm1.example.com# show processes
```

[Table 2-3](#) describes the fields in the **show processes** output.

**Table 2-3** *Field Descriptions for show processes Command*

Field	Description
Name	Name of the GSS subsystem, per operating system process.
PID	Process identifier.
MEM	Percentage of memory used by the process.
CPUTIME	Amount of CPU time used since the start of the process.
START	Date or time when the process started.

## Displaying System Uptime

You can display the length of time that the GSS has been running by using the **show uptime** command.

```
gssm1.example.com# show uptime
Uptime: 12 Days 18 Hours 5 Minutes and 12 seconds
```

## Displaying Disk Information

You can view general information about the GSS hard disk by using the **show disk** command. The general hard disk information includes the available user space on the disk, the size of the database, and the free space available on the disk.

```
gssm1.example.com# show disk
```

[Table 2-4](#) describes the fields in the **show disk** output.

**Table 2-4** Field Descriptions for **show disk** Command

Field	Description
Size	Total size of the disk, in megabytes.
Used	Used space on the disk, in megabytes.
Free	Available space on the disk, in megabytes.
User Space	Disk space allocated to the GSS users.
Database	Disk space allocated to the database configuration.
Safe Storage	Disk space allocated for system data storage.

## Displaying UDI Data

You can display GSS Unique Device Identifier (UDI) data by using the **show inventory** command.

```
gssm1.example.com# show inventory
NAME: Chassis, DESCR: Global Site Selector 4492
PID: GSS-4491-K9 , VID: V01, SN: QTFNZD606000011
```



The UDI provides a hardware product identification standard that is a consistent feature across Cisco products, allowing customers to uniquely identify and track Cisco products through their business and network operations. The UDI is composed of three separate data elements which are physically attached to each part:

- Orderable product identifier (PID)
- Version identifier (VID)
- Serial number (SN) of the hardware

The name of the device and a device description are also included in the output of the **show inventory** command.

## Displaying System Status

You can display a report on the current operating status of your GSS device, including the online status, current software version, and start date or time for the various components by using the **show system-status** command.



### Note

---

The equivalent command to show GSS system status is **gss status**.

---

```
gssml.example.com# show system-status
Cisco GSS - 1.3(1) GSS Manager - primary [Wed Feb 15 16 16:37:37 UTC
2006]
```

```
Normal Operation [runmode = 5]
```

```
START  SERVER
Aug06  Boomerang
Aug06  Config Agent (crdirector)
Aug06  Config Server (crm)
Aug06  DNS Server
Aug06  Database
Aug06  GUI Server (tomcat)
Aug06  Keepalive Engine
Aug06  Node Manager
Aug06  Proximity
Aug06  Sticky
Aug06  Web Server (apache)
```

## Displaying GSS Services

You can display the current state of the GSS services, such as FTP, NTP, SSH, TACACS+, Telnet, and SNMP by using the **show services** command.

```
gssm1.example.com(config)# show services  
START    SERVICE  
Jul23    Ftp  
Jul23    Ntp  
11:08    Snmp  
14:47    Ssh  
Jul23    Syslog  
Jul23    Tacacs Stats  
Jul23    Telnet
```



## CHAPTER

# 3

# Creating and Managing User Accounts

---

This chapter describes how to create and manage GSS device CLI user login accounts and primary GSSM GUI user login accounts. It contains the following major sections:

- [Creating and Managing GSS CLI User Accounts](#)
- [Creating and Managing Primary GSSM GUI User Accounts](#)
- [Modifying the Administrator Account Passwords](#)

## Creating and Managing GSS CLI User Accounts

From the CLI of a GSS device, you can create user accounts that enable user access to a GSS device, including the primary GSSM and standby GSSM. You must individually manage user access to the CLI of each GSS device in the network. Only users with the administrator privilege can create, modify, or remove a GSS user account from the CLI.



### Note

The primary GSSM separately maintains the user accounts and passwords created to log in to the CLI of the device from those accounts and passwords created to log in to the GUI.

This section contains the following topics:

- [Creating a GSS User Account](#)
- [Modifying a GSS User Account](#)
- [Deleting a GSS User Account](#)

## Creating a GSS User Account

When you create a user account from the GSS CLI, specify the new username, password, and privilege level using the **username** command. You cannot create a new account without designating a value for each of these configuration settings.

To create a user account that can log in and access the CLI of a GSS device, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

2. Access global configuration mode on the GSS.

```
gss1.example.com# config
gss1.example.com(config)#
```

3. Create and configure your new login account by entering the **username** command. The syntax for this command is as follows:

```
username name {delete | password password privilege {user | admin}}
```

The arguments and keywords are as follows:

- **name**—Specifies the username that you want to assign or change. Enter an unquoted alphanumeric text string with no spaces and a maximum of 32 characters. Ensure that the username begins with an alpha character (for example, A-Z or a-z). The GSS does not support usernames that begin with a numerical value.
- **delete**—Deletes the named user or administrative account.
- **password** *password*—Establishes the password. Specify the password that you want to assign. Enter an unquoted text string with no spaces and a maximum length of eight characters.

- **privilege**—Sets the user privilege level. To create an administrative account, specify **admin**. To create a user account, select **user**.

For example, enter:

```
gss1.example.com(config)# username user_1 password mypwd privilege
admin
User user_1 added.
```

4. Repeat Step 3 for each new user account that you want to create.

## Modifying a GSS User Account

You can modify a GSS user account from the CLI by using the same procedure that you followed to create the account (see the [“Creating a GSS User Account”](#) section). Use the **username** command to enter the full username, password, and privilege level, substituting the new values for the configuration settings that you want to change.

For example, enter:

```
gss1.example.com(config)# username user_1 password newpwd privilege
user
User user_1 exists, change info? [y/n]: y
```

## Deleting a GSS User Account

You can delete an existing user account for accessing the GSS from the CLI by entering the **username** command. The GSS restricts you from deleting the “admin” account.

For example, enter:

```
gss1.example.com#(config) username user_1 delete
User user_1 removed
```

# Creating and Managing Primary GSSM GUI User Accounts

By using the administrative capabilities of the primary GSSM GUI, you can create and maintain user accounts to access the primary GSSM GUI. In addition to login name and password information, you can assign user privileges, specify custom GUI user views, and maintain contact information for each user. Only users with administrator privilege can create, modify, or remove a primary GSSM GUI user account.

**Note**

---

The primary GSSM separately maintains the user accounts and passwords created to log in to the GUI from those accounts and passwords created to log in to the CLI.

---

This section contains the following topics:

- [Privilege Levels for Using the Primary GSSM GUI](#)
- [Creating a GUI User Account](#)
- [Modifying a GUI User Account](#)
- [Removing a GUI User Account](#)
- [Changing the User Account GUI Password](#)
- [Creating and Modifying User Views for the Primary GSSM GUI](#)

## Privilege Levels for Using the Primary GSSM GUI

As the GSS administrator, you can control the GUI pages that a user accesses and the associated functions that a user can perform from the primary GSSM GUI. You control primary GSSM GUI access through the assignment of one of the three user privilege levels, also called “roles.” Each of the following roles grants specific access to the GUI based on the assigned role:

- Administrator—Full configuration privileges and complete access to the primary GSSM GUI.
- Operator—Limited configuration privileges in the primary GSSM GUI, but the operator can view list pages, view detail pages, and monitor global server load-balancing statistics.
- Observer—No configuration privileges in the primary GSSM GUI, but the observer can monitor global server load-balancing statistics.

[Table 3-1](#) outlines the supported primary GSSM GUI functionality and accessibility for the three user roles.

**Table 3-1 User Privilege Roles for Using the Primary GSSM GUI**

User Role	Functionality	Accessibility
Administrator	Full functionality	Full access to the primary GSSM GUI pages.
Operator	<p>The operator has the following functionality privileges:</p> <ul style="list-style-type: none"> <li>• Suspend and activate permissions for answers only</li> <li>• View list pages, detail pages, and statistics</li> <li>• Restricted from creating, modifying, or deleting any configuration items appearing in the primary GSSM GUI</li> </ul>	<p>The operator has the following access privileges:</p> <ul style="list-style-type: none"> <li>• DNS Rules Tab— <ul style="list-style-type: none"> <li>– Access to all navigation links.</li> <li>– Access to the Modify icons to view the detail pages. The Delete icon and Submit icons are unavailable.</li> <li>– Access to the Suspend and Activate icons on the Modifying Answer and Modifying Answer Group detail pages.</li> <li>– Access to the Filter DNS Rules List and Show All DNS Rules icons on the DNS Rules list page.</li> <li>– Restricted from the DNS Rule Builder and DNS Rules Wizard icons and pages on the DNS Rules list page.</li> </ul> </li> </ul>



**Table 3-1** *User Privilege Roles for Using the Primary GSSM GUI (continued)*

User Role	Functionality	Accessibility
Operator (continued)		<ul style="list-style-type: none"><li>Resources tab—Access to the Locations and Owners navigation links to:<ul style="list-style-type: none"><li>Activate or suspend all answers associated with a location</li><li>Activate or suspend all answers associated with answer groups held by an owner.</li></ul></li></ul> <p>Restricted from activating and suspending all DNS rules associated with an owner.</p> <ul style="list-style-type: none"><li>Monitoring tab—Access to all navigation links and list pages.</li><li>Tools tab—Access to only the Change Password navigation link and detail page.</li><li>Traffic Mgmt tab—Access to all navigation links, list pages, and detail pages.</li></ul>

**Table 3-1** *User Privilege Roles for Using the Primary GSSM GUI (continued)*

User Role	Functionality	Accessibility
Observer	<p>The observer has read-only privileges to monitor statistics.</p> <p>Observers cannot do the following:</p> <ul style="list-style-type: none"> <li>• Create, modify, or delete any configuration item.</li> <li>• Perform any suspend or activate functions</li> <li>• View list pages or detail pages (but observers can view statistics)</li> </ul>	<p>The observer has the following access privileges:</p> <ul style="list-style-type: none"> <li>• DNS Rules Tab—Restricted from access to the DNS Rules tab.</li> <li>• Resources tab—Restricted from access to the Resources tab.</li> <li>• Monitoring tab—Access to all navigation links and list pages.</li> <li>• Tools tab—Access to only the Change Password navigation link and detail page.</li> <li>• Traffic Mgmt tab—Restricted from access to the Traffic Mgmt tab.</li> </ul>

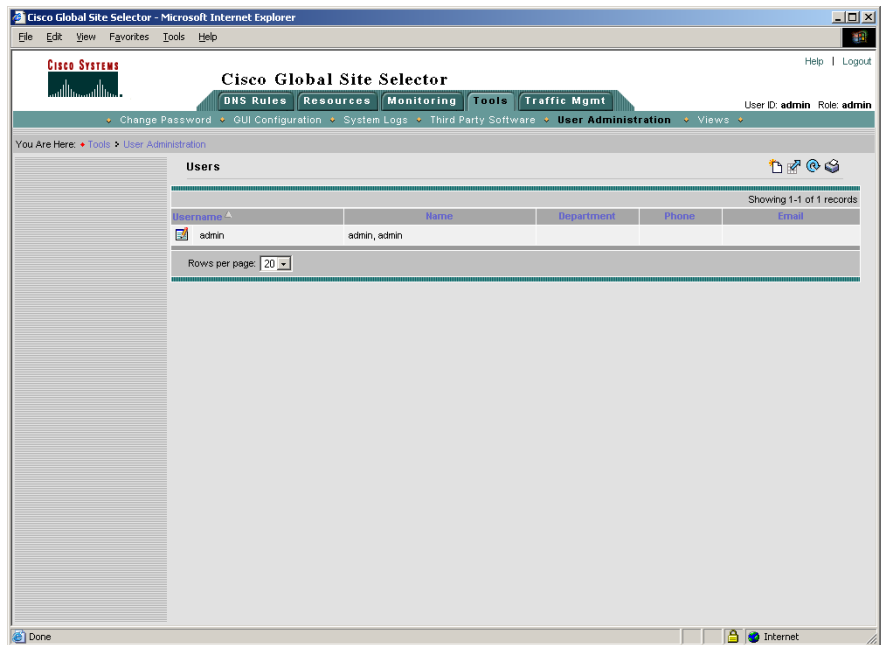
To further control what an operator or observer can access in the primary GSSM GUI, you can define and assign custom views to a user. A custom view limits the data (configuration and statistics) visible on a primary GSSM GUI page using configured answers, shared keepalives, locations, and owners. See the [“Creating and Modifying User Views for the Primary GSSM GUI”](#) section for details.

## Creating a GUI User Account

To create a GSSM GUI user account from the primary GSSM GUI, perform the following steps:

1. Click the **Tools** tab.
2. Click the **User Administration** navigation link. The Users list page appears (see [Figure 3-1](#)).

**Figure 3-1** Users List Page



3. Click the **Create User** icon. The Creating New User details page appears (see [Figure 3-2](#)).

Figure 3-2 Creating New User Details Page

**Creating New User**

User Account	
Username:	<input type="text"/>
Role:	Administrator
View:	View All
Password:	<input type="password"/>
Re-type Password:	<input type="password"/>
Personal Information	
First Name:	<input type="text"/>
Last Name:	<input type="text"/>
Job Title:	<input type="text"/>
Department:	<input type="text"/>
Phone:	<input type="text"/>
Email:	<input type="text"/>
Comments	
<input type="text"/>	

Submit Cancel

4. In the User Account area, enter the login name for the new account in the Username field. Usernames can contain spaces.
5. In the Password field, enter the alphanumeric password for the new account.
6. In the Re-type Password field, reenter the password for the new account.
7. In the Role field, choose from the three user privilege levels to define what the user has access to when using the primary GSSM GUI:
  - Administrator—Full configuration privileges and complete access to the primary GSSM GUI.
  - Operator—Limited configuration privileges in the primary GSSM GUI, but the operator can view list pages, view detail pages, and monitor statistics.
  - Observer—No configuration privileges in the primary GSSM GUI, but the observer can monitor statistics.

You must assign a user to one of the three privilege levels. If you fail to assign a privilege level, the GSS automatically assigns the observer role to a new user.



---

**Note** Primary GSSM GUI privileges assigned to a user from the TACACS+ server override the user privilege level defined from the GSSM User Administration details page.

---

See the [“Privilege Levels for Using the Primary GSSM GUI”](#) section for information about the multiple levels of access that are available to a user when using the primary GSSM GUI.

8. In the View drop-down list, choose **View All** or choose from one of the previously created custom user views:
  - **View All**—Enables the user to see all configuration items and statistics displayed in the primary GSSM GUI. This is the default selection when you create a user.
  - **User View**—For a user with an assigned operator or observer role, a user view allows the administrator to limit the configuration data and statistics available to the user when accessing the primary GSSM GUI.



---

**Note** Only an administrator can create a view. See the [“Creating and Modifying User Views for the Primary GSSM GUI”](#) section for details. An administrator may find it useful to set the view to a defined User View to test the behavior of view while in the process of creating it.

---

9. In the Personal Information area, enter the user’s first name in the First Name field.
10. In the Last Name field, enter the last name of the user. The first and last names appear next to the user’s login whenever that user logs in to the primary GSSM.
11. (Optional) Fill in the rest of the user contact information:
  - **Job Title**—Position within the organization
  - **Department**—Business unit or group
  - **Phone**—Business telephone number

- **E-mail**—E-mail address
  - **Comments**—Any important information or comments about the user account
12. Click **Submit** to create your new user account and return to the User Administration list page.

## Modifying a GUI User Account

To modify an existing GSSM user account from the primary GSSM GUI, perform the following steps:

1. Click the **Tools** tab.
2. Click the **User Administration** navigation link. The Users list page appears (see [Figure 3-1](#)) listing existing user accounts.
3. Click the **Modify User** icon to the left of the user account that you want to modify. The Modifying User details page appears (see [Figure 3-2](#)) listing fields for modifying your GUI session settings.
4. Use the fields in the Modifying User details page to modify the details of the user account.
5. Click **Submit** to save changes to the account and return to the Users list page.

## Removing a GUI User Account

To remove an existing GSSM GUI user account from the primary GSSM GUI, perform the following steps:

1. Click the **Tools** tab.
2. Click the **User Administration** navigation link. The Users list page appears (see [Figure 3-1](#)) listing existing user accounts.
3. Click the **Modify User** icon to the left of the user account that you want to remove. The Modifying User details page appears (see [Figure 3-2](#)), displaying that user's account information.
4. Click the **Delete** icon. The software prompts you to confirm your decision to permanently remove the user. You cannot delete the “admin” account.

5. Click **OK** to remove the user account and return to the Users list page. The user account is removed from the list page.

## Changing the User Account GUI Password

You can change the password for the account that is used to log in to the primary GSSM. Use the Change Password detail page of the primary GSSM GUI to change the password. You must know the existing password for an account before you can change it.



### Note

If you change the administration password that is used to log in to the primary GSSM GUI and then either lose or forget the password, you can reset it back to “default” by using the **reset-gui-admin-password** CLI command. See the [“Restoring or Changing the Administrator GUI Password”](#) section for details.

To change your account password from the primary GSSM GUI, perform the following steps:

1. Click the **Tools** tab.
2. Click the **Change Password** navigation link. The Change Password details page (see [Figure 3-3](#)) appears displaying your account name in the Username field

**Figure 3-3 GSSM Change Password Details Page**

The screenshot shows the Cisco Global Site Selector web interface in Microsoft Internet Explorer. The browser title is "Cisco Global Site Selector - Microsoft Internet Explorer". The page header includes the Cisco logo, the title "Cisco Global Site Selector", and navigation tabs: "DNS Rules", "Resources", "Monitoring", "Tools", and "Traffic Mgmt". Below the tabs is a breadcrumb trail: "Change Password > GUI Configuration > System Logs > Third Party Software > User Administration > Views". The user is logged in as "admin" with the role "admin".

The main content area is titled "Change Password". It contains a form with the following fields:

- Username: admin
- Old Password: [text input field]
- New Password: [text input field]
- Re-type New Password: [text input field]

At the bottom right of the form are two buttons: "Submit" and "Reset".

3. In the Old Password field, enter your existing GSSM login password.
4. In the New Password field, enter the string that you would like to use as the new GSSM login password.
5. In the Re-type New Password field, enter the new password string a second time. This action is used to verify that you have entered your password correctly.
6. Click **Submit** to update your login password.



## Creating and Modifying User Views for the Primary GSSM GUI

By default, an administrator, operator, and observer has the view set to View All and can see all configuration data and global server load-balancing statistics in the primary GSSM GUI pages. By creating and assigning views to a user with operator or observer privileges, the administrator can control what configuration and statistical data is available to those users when accessing primary GSSM GUI pages.

**Note**

---

Only an administrator can create, modify, or delete a user view.

---

This section contains the following topics:

- [Custom User View Overview](#)
- [Creating a GUI User View](#)
- [Modifying a GUI User View](#)
- [Deleting a GUI User View](#)

### Custom User View Overview

As the GSS administrator, you can define a set of custom views that limit the data (configuration data and statistics) available on a primary GSSM GUI page. Each custom user view can include selections from the following properties:

- Answers
- Shared keepalives
- Locations
- Owners

You specify the individual answers, shared keepalives, locations, and owners that define the properties of a custom user view. When you assign a custom view to a user account, the user can see only the configured data and statistics associated with their view. The user is restricted from viewing any additional configured answers, shared keepalives, locations, and owners that might exist in the primary GSSM GUI.

You can also provide administrator privileges to a user. With administrator privileges, that user can change the view used for the GUI session (for example, back to the View All setting). This capability can be useful for an administrator to test the behavior of a view while in the process of creating it.

When you select individual answers, shared keepalives, locations, or owners as part of a custom view, keep in mind that the relationship between those configuration data and the other configuration data in the primary GSSM GUI. The following is a summary of the relationship between configuration data and properties in the primary GSSM GUI:

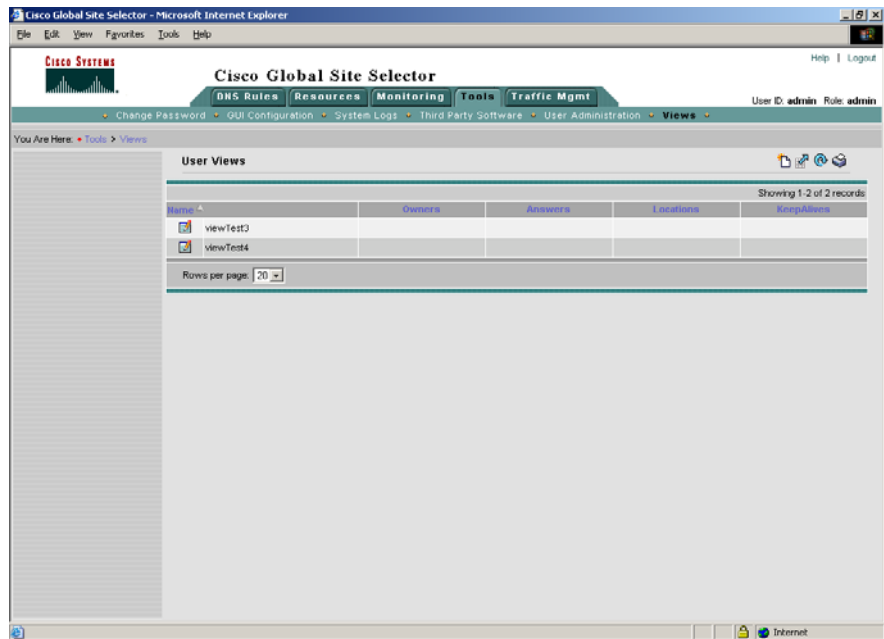
- DNS rules, answer groups, source address lists, and domain lists specify owners as a defining property
- Answer groups specify answers as a defining property
- Answers specify locations as a defining property

The relationship between configuration data in the primary GSSM GUI has a direct impact on what configuration data and statistics are visible in a custom view. For example, if the primary GSSM GUI has four configured owners and you assign two owners to a custom view, only the DNS rules, answer groups, source address lists, and domain lists that reference those two owners are visible in the custom view. The remaining DNS rules, answer groups, source address lists, and domain lists will be hidden from the primary GSSM GUI pages because they reference the other two owners not currently included in the custom view.

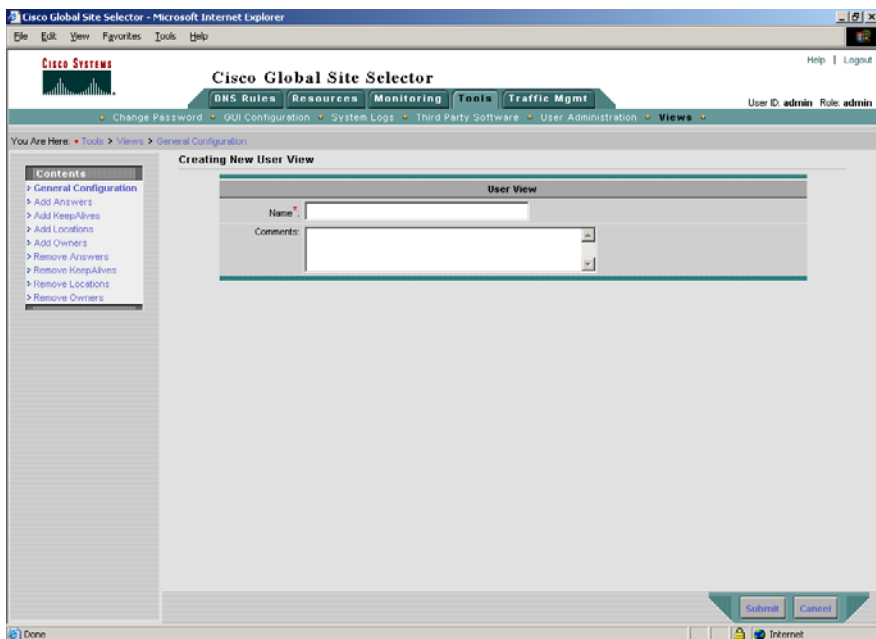
## Creating a GUI User View

To create a GUI user view, perform the following steps:

1. From the primary GSSM GUI, click the **Tools** tab.
2. Click the **Views** navigation link. The User Views list page appears (see [Figure 3-4](#)).

**Figure 3-4** User Views List Page

3. Click the **Create User Views** icon. The Creating New User View—General Configuration details page appears (see [Figure 3-5](#)).

**Figure 3-5** Creating New User View—General Configuration Details Page

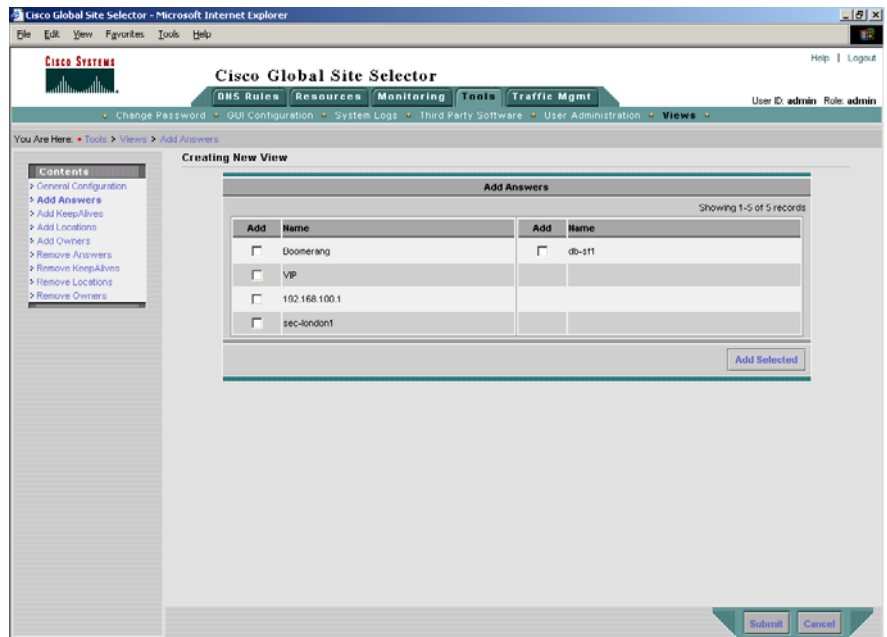
4. In the General Configuration details page (**General Configuration** navigation link), perform the following:
  - a. In the Name field, enter a name for your new user view. View names can be from 1 to 80 alphanumeric characters and cannot contain spaces.
  - b. In the Comments field, enter descriptive information or important notes regarding the new user view.
5. Click the **Add Answers** navigation link to define the answers available in the custom user view. The Add Answers details page appears (see [Figure 3-6](#)). Click the check box corresponding to each existing answer you want to add to the custom user view.

If the list of answers on your GSS network spans more than one page, select the answers from only the first page of answers, and then click **Add Selected** before proceeding to another page of answers.

**Note**

The primary GSSM GUI supports a maximum of 100 answers in a custom user view.

**Figure 3-6** Creating New View—Add Answers Details Page



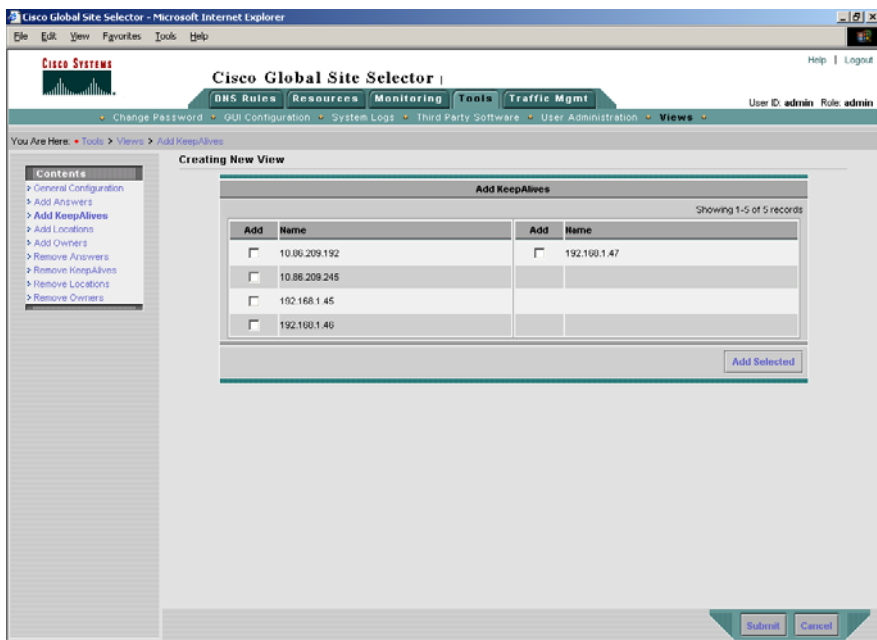
6. Click the **Add Keepalives** navigation link to define the shared keepalives available in the custom user view. The Add Keepalives details page appears (see [Figure 3-7](#)). Click the check box corresponding to each existing shared keepalive you want to add to the custom user view.

If the list of shared keepalives on your GSS network spans more than one page, select the shared keepalives from only the first page of keepalives, and then click **Add Selected** before proceeding to another page of shared keepalives.

**Note**

The primary GSSM GUI supports a maximum of 100 keepalives in a custom user view.

**Figure 3-7 Creating New View—Add Keepalives Details Page**

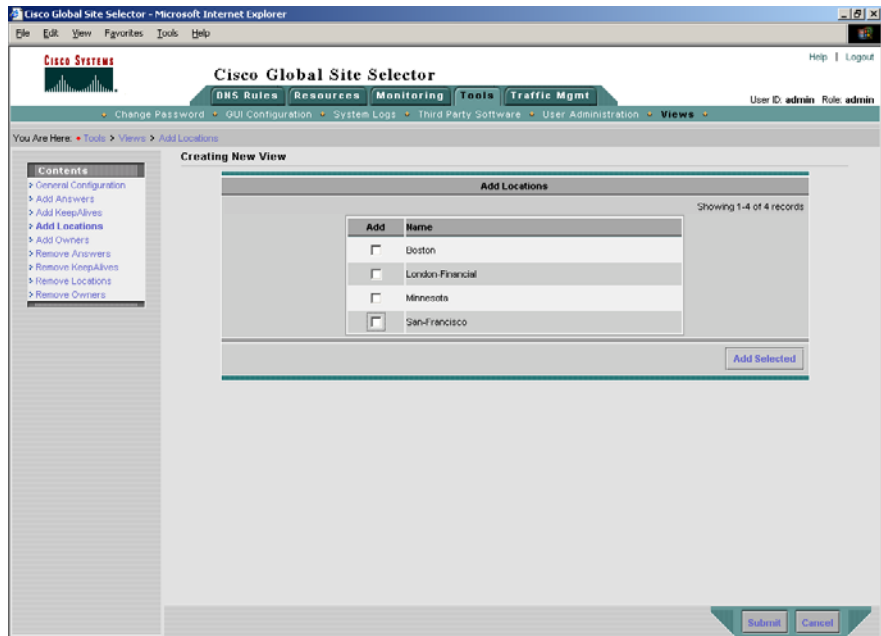


7. Click the **Add Locations** navigation link to define the locations available in the custom user view. The Add Locations details page appears (see [Figure 3-8](#)). Click the check box corresponding to each existing location you want to add to the custom user view.

If the list of locations on your GSS network spans more than one page, select the locations from only the first page of locations, then click **Add Selected**, before proceeding to another page of locations.

**Note**

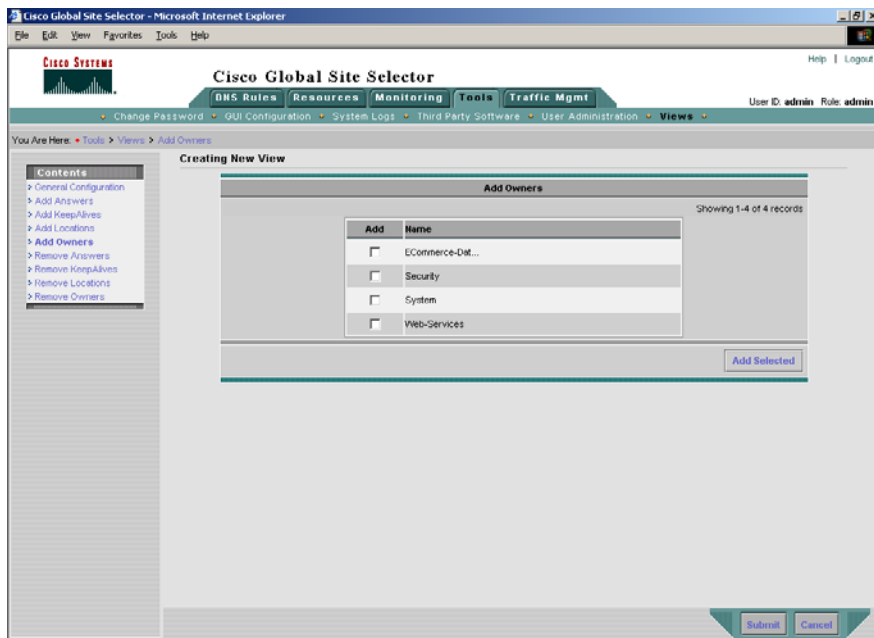
The primary GSSM GUI supports a maximum of 200 locations in a custom user view.

**Figure 3-8** Creating New View—Add Locations Details Page

8. Click the **Add Owners** navigation link to define the owners available in the custom user view. The Add Owners details page appears (see [Figure 3-9](#)). Click the check box corresponding to each existing owner you want to add to the custom user view.
9. If the list of owners on your GSS network spans more than one page, select the owners from only the first page of owners, and then click **Add Selected** before proceeding to another page of owners.

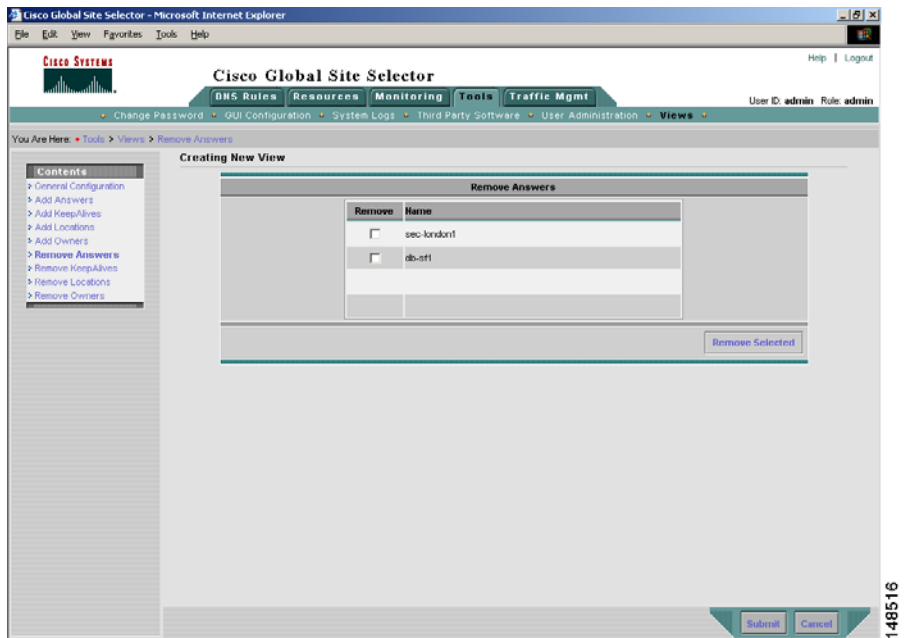
**Note**

The primary GSSM GUI supports a maximum of 500 owners in a custom user view.

**Figure 3-9** Creating New View—Add Owners Details Page

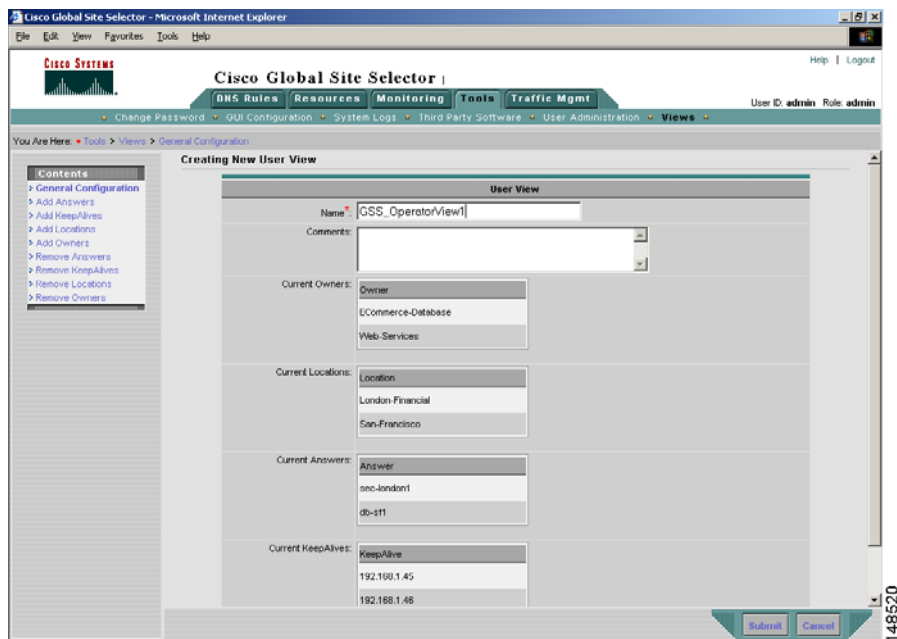
10. Click the appropriate **Remove** navigation link to remove answers, keepalives, locations, or owners from this custom user view. The associated detail page then appears. [Figure 3-10](#) illustrates the Remove Answers details page.
11. Click the check boxes that correspond to the items that you want to remove from the custom user view, and then click **Remove Selected**.



**Figure 3-10** *Creating New View—Remove Answers Details Page*

12. When you complete defining the user view, click the **General Configuration** navigation link to return to the Creating New User View - General Configuration details page (see [Figure 3-11](#)). The selected items assigned to this view appear in the Current Owners, Current Locations, Current Answers, or Current KeepAlives section of the page.

**Figure 3-11** *Creating New User View—General Configuration Details Page With Selected Items Assigned to the View*



13. Click **Submit** to save your new user view.

## Modifying a GUI User View

To modify a user view from the primary GSSM GUI, perform the following steps:

1. Click the **Tools** tab.
2. Click the **Views** navigation link. The User Views list page appears (see [Figure 3-4](#)).
3. Click the **Modify User View** icon located to the left of the user view that you want to modify. The Modify User View details page appears.
4. In the General Configuration details page (**General Configuration** navigation link), use the fields provided to modify the name or comments for the user view.

5. Click the appropriate **Add** navigation link to add additional answers, keepalives, locations, or owners to the custom user view. The associated details page appears. Click the check boxes that correspond to the items that you want to add to the custom user view, and then click **Add Selected**.
6. Click the appropriate **Remove** navigation link to remove answers, keepalives, locations, or owners from the custom view. The associated details page appears. Click the check boxes that correspond to the items that you want to remove from the custom user view, and then click **Remove Selected**.
7. Click **Submit** to save changes to the user view.

## Deleting a GUI User View

To delete a user view from the primary GSSM GUI, perform the following steps:

1. Click the **Tools** tab.
2. Click the **Views** navigation link. The User Views list page appears (see [Figure 3-4](#)).
3. Click the **Modify User View** icon located to the left of the user view that you want to modify. The Modify User View details page appears.
4. Click the **Delete** icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the user view.
5. Click **OK** to return to the User Views list page with the user view removed.

# Modifying the Administrator Account Passwords

This section describes how to reset the administrator account password from the GSS CLI. It also discusses how to restore the default administration password to log in to the primary GSSM.

This section contains the following topics:

- [Resetting the Administrator CLI Account Password](#)
- [Changing the Administrator CLI Password](#)
- [Restoring or Changing the Administrator GUI Password](#)

## Resetting the Administrator CLI Account Password

If you forget the password for the GSS administrator account, you can reset it from the GSS CLI. You must have physical access to the GSS device to perform this procedure.

To reset the administrator CLI account password, perform the following steps:

1. Attach an ASCII terminal to the Console port on the GSS device. See the *Cisco Global Site Selector Hardware Installation Guide* for instructions on connecting a console cable to your GSS series hardware.
2. If the GSS device is currently up and running, power cycle it to perform a restart of the GSS. As the GSS reboots, the output appears on the console terminal.
3. After the BIOS boots and the LILO boot: prompt appears, enter ? (a question mark) to determine which software version the GSS device is running and to enter boot mode.

```
LILO boot: ?  
GSS-<software_version>  
boot:
```

At the LILO boot: prompt, press **Tab** or **?** to view a listing of the available GSS software images.



**Note** Enter the ? command within a few seconds of seeing the LILO boot prompt or the GSS device continues to boot. If you miss the time window to enter the ? command, wait for the GSS to properly complete booting, cycle power to the GSS device, and try again to access the LILO boot prompt.

4. At the boot: prompt, enter **GSS-<software\_version> RESETADMINCLIPW=1**. Be careful when entering this command; this CLI command is case sensitive.

For example, to specify GSS software version 1.3.1, enter:

```
boot: GSS-1.3.1 RESETADMINCLIPW=1
```

If you successfully reset the administrator password, the “Resetting admin account CLI password” message appears on the console terminal while the GSS device reboots. If the message does not appear, repeat Steps 2 through 4. Pay close attention when you enter the **GSS-<software\_version> RESETADMINCLIPW=1** command.

## Changing the Administrator CLI Password

You can change the administrator password that accesses the GSS CLI by using the **username** global configuration mode command.

The syntax for this command is as follows:

```
username name password password
```

The arguments and keywords are as follows:

- **name**—Username that you want to assign or change. Enter an unquoted text string with no spaces and a maximum of 32 characters. Login names must start with an alphanumeric character.
- **password** *password*—Modifies the password used to log in to the GSS CLI. Specify the password that you want to change. Enter an unquoted text string with no spaces and a maximum length of eight characters.

For example, to change the administrator password to *mynewpassword*, enter:

```
gssml.example.com(config)# username admin password mynewpassword  
privilege admin
```

## Restoring or Changing the Administrator GUI Password

You can restore the default administrator password used to log in to the primary GSSM GUI, or change the administrator password by using the **reset-gui-admin-password** command. The GSS stores the administrator username and password in a safe partition of the hard disk to prevent loss of data due to power failures. If you change the administrator password, and then either lose or forget the password, you can reset the password back to **default** by using the **reset-gui-admin-password** command on the primary GSSM.

Only users with the administrator privilege can remove or change the administrator's GUI password.

The syntax for this command is as follows:

```
reset-gui-admin-password [password text]
```

The optional **password** *text* keyword and argument allow you to change the administrator password used to log in to the primary GSSM GUI. Enter an unquoted text string of 6 to 16 characters with no spaces.

For example, to change the change the administrator password to *mynewpassword*, enter:

```
gssml.example.com# reset-gui-admin-password password mynewpassword
```



# CHAPTER 4

## Managing GSS User Accounts Through a TACACS+ Server

---

This chapter describes how to configure the GSS, primary GSSM, or standby GSSM as a client of a Terminal Access Controller Access Control System Plus (TACACS+) server for separate authentication, authorization, and accounting (AAA) services. Configuring the GSS as a client of a TACACS+ server provides a higher level of security by allowing you to control who can access a GSS device, control which CLI commands are available for particular users, and to use the TACACS+ server to record the specific CLI commands and GUI pages accessed by a GSS user.

This chapter contains the following major sections:

- [TACACS+ Overview](#)
- [TACACS+ Configuration Quick Start](#)
- [Configuring a TACACS+ Server for Use with the GSS](#)
- [Identifying the TACACS+ Server Host on the GSS](#)
- [Disabling TACACS+ Server Keepalives on the GSS](#)
- [Specifying the TACACS+ Server Timeout on the GSS](#)
- [Specifying TACACS+ Authentication of the GSS](#)
- [Specifying TACACS+ Authorization of the GSS](#)
- [Specifying TACACS+ Accounting on the GSS](#)
- [Showing TACACS+ Statistics on the GSS](#)

- [Clearing TACACS+ Statistics on the GSS](#)
- [Disabling TACACS+ on a GSS](#)

## TACACS+ Overview

The TACACS+ protocol is a security application that provides centralized validation of users who are attempting to gain access to the GSS. TACACS+ services are maintained in a relational database on a TACACS+ security daemon running on a UNIX or Windows NT/Windows 2000 server.

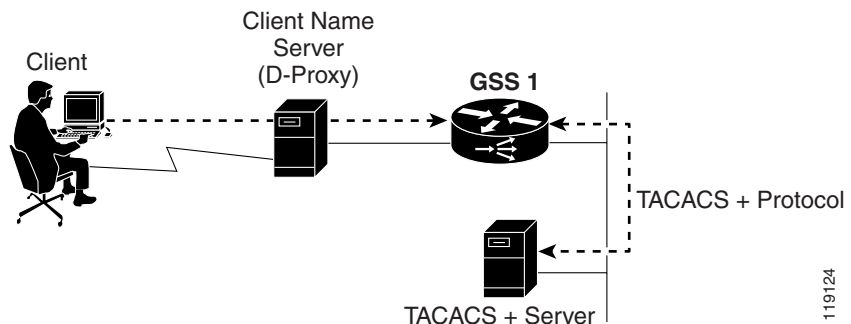
TACACS+ provides for separate authentication, authorization, and accounting (AAA) facilities between a GSS and the TACACS+ server. TACACS+ allows for multiple access control servers (the TACACS+ security daemon) to provide the AAA services. The Cisco Secure Access Control Server (ACS) is an example of an AAA access control server.

TACACS+ uses TCP as the transport protocol for reliable delivery. Optionally, you can configure the GSS to encrypt all traffic transmitted between the GSS device and the TACACS+ server in the form of a shared secret.

When a user attempts to access a GSS device that is operating as a TACACS+ client, the GSS forwards the user authentication request to the TACACS+ server (containing the username and password). The TACACS+ server returns either a success or failure response depending on the information in the server's database.

[Figure 4-1](#) shows a client GSS and a TACACS+ server configuration.

**Figure 4-1 Simplified Example of Traffic Flow Between a GSS Client and a TACACS+ Server**



119124



The TACACS+ server provides the following AAA independent services to the GSS operating as a TACACS+ client:

- **Authentication**—Identifies users attempting to access a GSS. Authentication frequently involves verifying a username with an assigned password. GSS users are authenticated against the TACACS+ server when remotely accessing a GSS through the console, Telnet, Secure Shell (SSH), FTP, or the primary GSSM GUI interfaces.

To successfully log in to a GSS from an SSH session, you must be configured on both the GSS and the TACACS+ server. To successfully log in from a Telnet or FTP session, you need only be configured on the TACACS+ server. In either case, if your remote login authentication attempt is denied, you are prohibited from accessing the GSS.

- **Authorization**—Controls which GSS CLI commands a user can execute on a GSS or on a GSSM (primary or standby), providing per-command control and filtering. Authorization is performed after a user receives authentication by the TACACS+ server and begins to use the GSS. You also can assign a privilege level to a user accessing the primary GSSM GUI.
- **Accounting**—Records the specific CLI commands and GUI pages accessed by a GSS user. Accounting enables system administrators to monitor the activities of GSS users, which is beneficial for administrating multi-user GSS devices. The information is contained in an accounting record that is sent to the TACACS+ server. Each record includes the username, the CLI command executed or the primary GSSM GUI page accessed, the primary GSSM GUI page action performed, and the time that the action was performed. You can import the log files from the TACACS+ server into a spreadsheet application.

You can define a maximum of three TACACS+ servers for use with a GSS. The GSS periodically queries the first configured TACACS+ server with a TCP keepalive to ensure network connectivity and TACACS+ application operation. If the GSS determines that the TACACS+ server is down, the GSS attempts to connect to the next server in the list of configured TACACS+ servers as the backup server. If a second (or third) TACACS+ server is available for use, the GSS selects that server as the active TACACS+ server.

The GSS uses TCP keepalives as the default to monitor connectivity with the active TACACS+ server. As a secondary measure, if the TCP keepalives fail, or if you disable the use of keepalives, you can specify a global TACACS+ timeout period to designate how long the GSS waits for a response to a connection attempt from a TACACS+ server. The timeout value applies to all defined TACACS+ servers.

If the GSS cannot contact any of the three specified TACACS+ servers, the GSS checks for the local authentication setting and falls back to performing local user authentication through either the console port or a Telnet connection. Local authentication is always enabled on the console port and Telnet connection to avoid lockout. Local authentication is an option for an FTP, GUI, or SSH connection.

# TACACS+ Configuration Quick Start

Table 4-1 provides a quick overview of the steps required to configure TACACS+ server operation on a GSS. Each step includes the CLI command required to complete the task. For a complete description of each feature and all the options associated with the CLI command, see the sections following the table.

Table 4-1 TACACS+ Configuration Quick Start

Task and Command Example	
1. Configure the authentication, authorization, and accounting service settings on the TACACS+ server, such as the Cisco Secure Access Control Server (ACS).	
2. Enable global configuration mode on the GSS device.	<pre>gssm1.example.com# config gssm1.example.com(config)#</pre>
3. Define the TACACS+ server that contains the TACACS+ authentication, authorization, and accounting databases. You can define a maximum of three servers for the GSS. Specify the IP address or hostname for the server. By default, the TCP port is 49. You can optionally define a different port number and, if required, a TACACS+ server encryption key.	<pre>gssm1.example.com(config)# tacacs-server host 192.168.1.102 port 9988 key SECRET-456</pre>
4. (Optional) Define a global TACACS+ timeout period for the configured TACACS+ servers.	<pre>gssm1.example.com(config)# tacacs-server timeout 60</pre>
5. Enable TACACS+ authentication for a specific GSS access method.	<pre>gssm1.example.com(config)# aaa authentication ssh</pre>

**Table 4-1 TACACS+ Configuration Quick Start (continued)**

Task and Command Example	
6.	<p>Enable the TACACS+ authorization service to permit or restrict user access to specific GSS CLI commands, as defined by the TACACS+ server.</p> <pre>gssm1.example.com(config)# <b>aaa authorization commands</b></pre>
7.	<p>Enable the TACACS+ accounting service to monitor the use of specific CLI commands and GUI pages by each GSS user.</p> <pre>gssm1.example.com(config)# <b>aaa accounting commands</b></pre>

# Configuring a TACACS+ Server for Use with the GSS

This section describes how to set up a TACACS+ server, such as the Cisco Secure Access Control Server (ACS). It is intended as a guide to help ensure proper communication with a TACACS+ server and a GSS operating as a TACACS+ client. For details on configuring the Cisco Secure ACS, or another TACACS+ server, see the documentation provided with the software.

This section contains the following topics:

- [Configuring Authentication Settings on the TACACS+ Server](#)
- [Configuring Authorization Settings on the TACACS+ Server](#)
- [Configuring Accounting Settings on the TACACS+ Server](#)



## Note

For the GSS to properly perform user authentication using a TACACS+ server, the username and password must be identical on both the GSS CLI and the TACACS+ server.

# Configuring Authentication Settings on the TACACS+ Server

To configure the authentication settings on Cisco Secure ACS, perform the following steps:

1. Proceed to the Network Configuration section of the Cisco Secure ACS HTML interface, the Add AAA Client page (see [Figure 4-2](#)).

Figure 4-2 Add AAA Client Page of Cisco Secure ACS

The screenshot shows the Cisco Secure ACS web interface in Microsoft Internet Explorer. The browser title is "CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.". The page has a menu on the left with options: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Network Configuration" and "Add AAA Client". It contains the following fields and options:

- AAA Client Hostname: [Text Input Field]
- AAA Client IP Address: [Text Input Field]
- Key: [Text Input Field]
- Authenticate Using: [Dropdown Menu] (Currently set to "TACACS+ (Cisco IOS)")
- ☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- ☐ Log Update/Watchdog Packets from this AAA Client
- ☐ Log RADIUS Tunneling Packets from this AAA Client
- ☐ Replace RADIUS Port info with Username from this AAA Client

At the bottom of the form are three buttons: "Submit", "Submit + Restart", and "Cancel". Below these buttons is a "Back to Help" button with a question mark icon. The page number "148502" is visible in the bottom right corner.

2. Configure the following selections:

- AAA Client Hostname—Enter the name that you want assigned to the GSS.
- AAA Client IP Address—Enter the IP address of the GSS Ethernet interface that will be used for communicating with the TACACS+ server.

- **Key**—Enter the shared secret that the GSS and Cisco Secure ACS use to authenticate transactions. For correct operation, you must specify the identical shared secret on both the Cisco Secure ACS and the GSS. The key is case-sensitive.
- **Authenticate Using**—Select **TACACS+ (Cisco IOS)**.

**Note**

The TACACS+ (Cisco IOS) drop-down item is the general title for the Cisco TACACS+ authentication function. The TACACS+ (Cisco IOS) selection activates the TACACS+ option when using Cisco Systems access servers, routers, and firewalls that support the TACACS+ authentication protocol. This includes support with a GSS device as well.

## Configuring Authorization Settings on the TACACS+ Server

You can use the TACACS+ server to limit user access to a subset of CLI commands on a GSS device. For the Cisco Secure ACS, define the CLI command sets for user groups, and then assign users to those groups. You can also determine a user's primary GSSM GUI privilege level when configuring user command authorization settings.

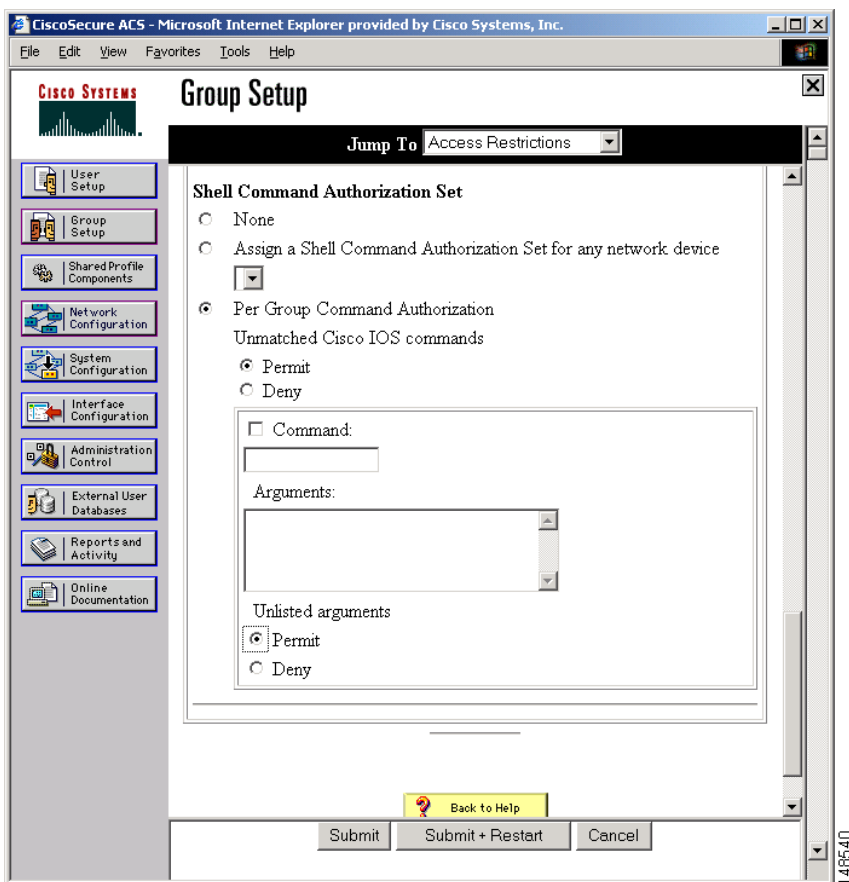
**Note**

For the Cisco Secure ACS, you may also define command privileges for individual users instead of an entire group. The setup process is the same for users or for groups.

To define CLI command privileges for the GSS from the Cisco Secure ACS, perform the following steps:

1. Access the Group Setup section of the Cisco Secure ACS interface, then access the Group Setup page. Select the group for which you want to configure TACACS+ settings, then click **Edit Settings**. The Edit page appears.
2. Scroll to the Shell Command Authorization Set section of the Group Setup page (see [Figure 4-3](#)).

**Figure 4-3** Shell Command Authorization Set Section of Group Setup Page



3. Click the **Per Group Command Authorization** check box.

4. For unlimited GSS command access, under Unmatched Cisco IOS Commands, click the **Permit** option. Leave the command field blank.
5. Set access restrictions on specific GSS CLI commands as follows:
  - a. Check the **Command** check box.
  - b. Click the **Deny** option.
  - c. Type the command name in the Command text box, along with any required arguments to the command that you want to permit or deny.

The specified commands are denied for the group depending on the setting of the Unmatched Cisco IOS Commands parameters.
6. Configure arguments for a specified CLI command by entering strings in the Arguments text box as follows:

```
deny <arg1 ... argN>  
permit <arg1 ... argN>
```

Arguments are case sensitive and must match the text exactly that the GSS sends to the Cisco Secure ACS. For each argument of the Cisco IOS command, specify whether the argument is to be permitted or denied. These should be entered in the format **permit** *argument* or **deny** *argument*.

The GSS device may submit arguments in a format different from what a user types at a GSS CLI prompt. To create effective device CLI command sets, see the *Cisco Global Site Selector Command Reference* for proper CLI command syntax.

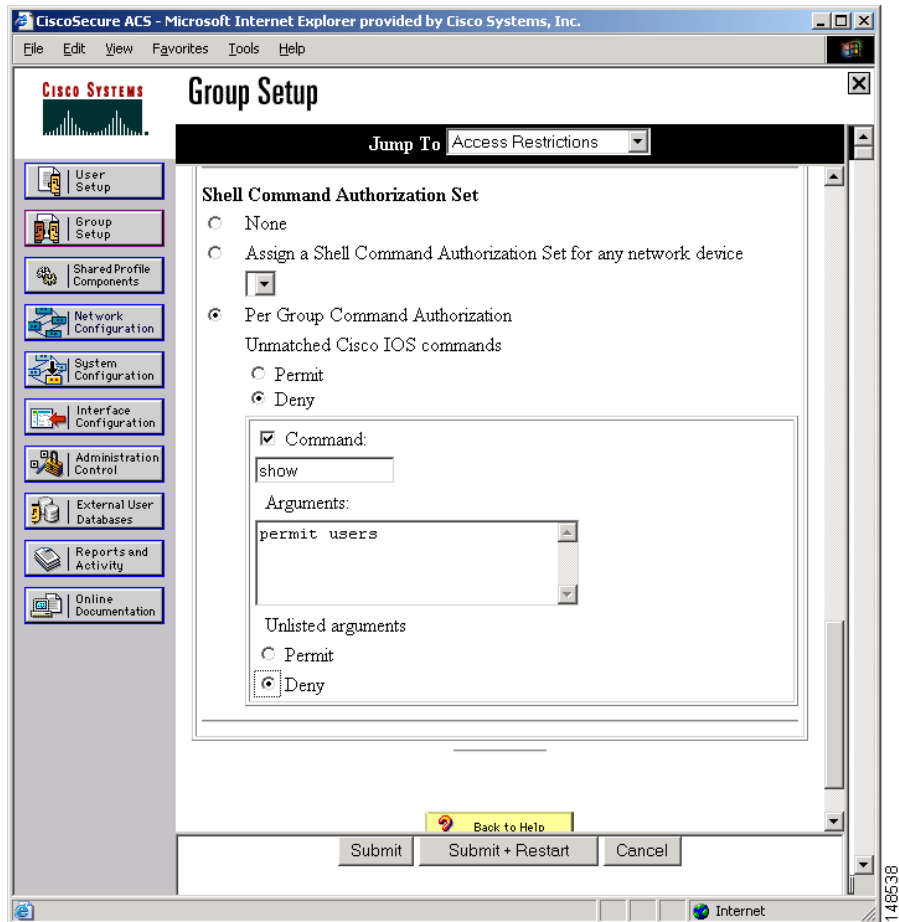
7. Choose **Deny** to permit only those arguments listed, under Unlimited Arguments. Choose **Permit** to allow users to issue all arguments not specifically listed.
8. Repeat Steps 5 through 7 for each CLI command that you want to restrict. Configure multiple commands by clicking the **Submit** button after each command. A new command configuration section appears for subsequent commands.

The following are examples of permitting and denying CLI commands:

- To deny all CLI commands except the **show users** CLI command (see [Figure 4-4](#)), do the following:
  - a. Click the **Deny** option under Per Group Command Authorization.
  - b. Enter **show** in the Command text box.

- c. Enter **permit user** in the Arguments text box.
- d. Click the **Deny** option under Unlisted arguments.

**Figure 4-4** *Command Privileges Example—Deny All CLI Commands Except Specified Command*

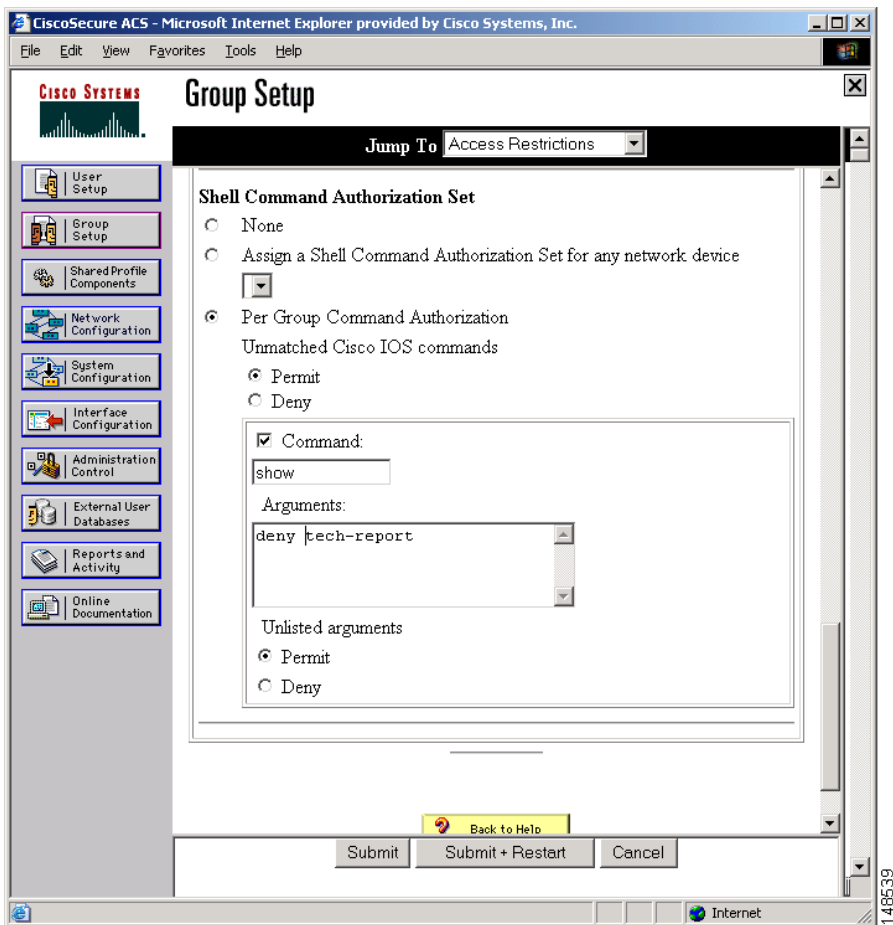


- To permit all CLI commands except for the **gss tech-report** command (see [Figure 4-5](#)), do the following:
  - a. Click the **Permit** option under Per Group Command Authorization.
  - b. Enter **gss** in the Command text box.



- c. Enter **deny tech-report** in the Arguments text box.
- d. Click the **Permit** option under Unlisted arguments.

**Figure 4-5** *Command Privileges Example—Permit All CLI Commands Except Specified Command*



This section contains the following topics:

- [Configuring Primary GSSM GUI Privilege Level Authorization from the TACACS+ Server](#)
- [Enabling Custom User GUI Views When Authenticating a User from the TACACS+ Server](#)

## Configuring Primary GSSM GUI Privilege Level Authorization from the TACACS+ Server

You can configure the Cisco Secure ACS TACACS+ server to define the privilege level (role) of a user when accessing the primary GSSM GUI. The primary GSSM GUI learns the user's associated privilege level when communicating with the TACACS+ server. This capability provides the TACACS+ administrator with the flexibility to dynamically change a user's privilege level without requiring that the user terminate a GUI session and log back in to the primary GSSM.

Users are assigned privileges based on whether they are using the GUI or the CLI on the primary GSSM as follows:

- For users who are using the GUI, the privilege configured on the TACACS+ server takes preference over any privilege configured on the GSS.
- For users who are using the CLI, the privilege configured on the GSS takes preference over the privilege configured on the TACACS+ server. If a user is *not* configured locally, then the user is assigned the user privilege by default (regardless of the privilege configured on the TACACS+ server).

If you configure the TACACS+ server to allow all commands, the user is automatically set to administrator and has all associated privileges. See the [“Privilege Levels for Using the Primary GSSM GUI”](#) section in [Chapter 3, Creating and Managing User Accounts](#) for more information.



### Note

---

Primary GSSM GUI privileges assigned to a user from the TACACS+ server override the user privilege level defined from the primary GSSM GUI GSSM User Administration details page.

---

To specify a user privilege-level for accessing the primary GSSM GUI from the Cisco Secure ACS, perform the following steps:

1. If this is your first time enabling per-user CLI command authorization, access the Interface Configuration section of the Cisco Secure ACS interface and configure the following selections:
  - a. Access the TACACS+ (IOS) page. Click the **Shell (exec)** checkbox under both the User and Group columns (see [Figure 4-6](#)).

**Figure 4-6** Interface Configuration Page—TACACS+ (IOS) Page

The screenshot shows the Cisco Secure ACS web interface in Microsoft Internet Explorer. The main title is 'Interface Configuration' with a sub-tab 'Edit'. The left sidebar contains navigation links: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration (selected), Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'TACACS+ (Cisco)' and contains a section 'TACACS+ Services' with a table of services and their authorization status.

User	Group	Service
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

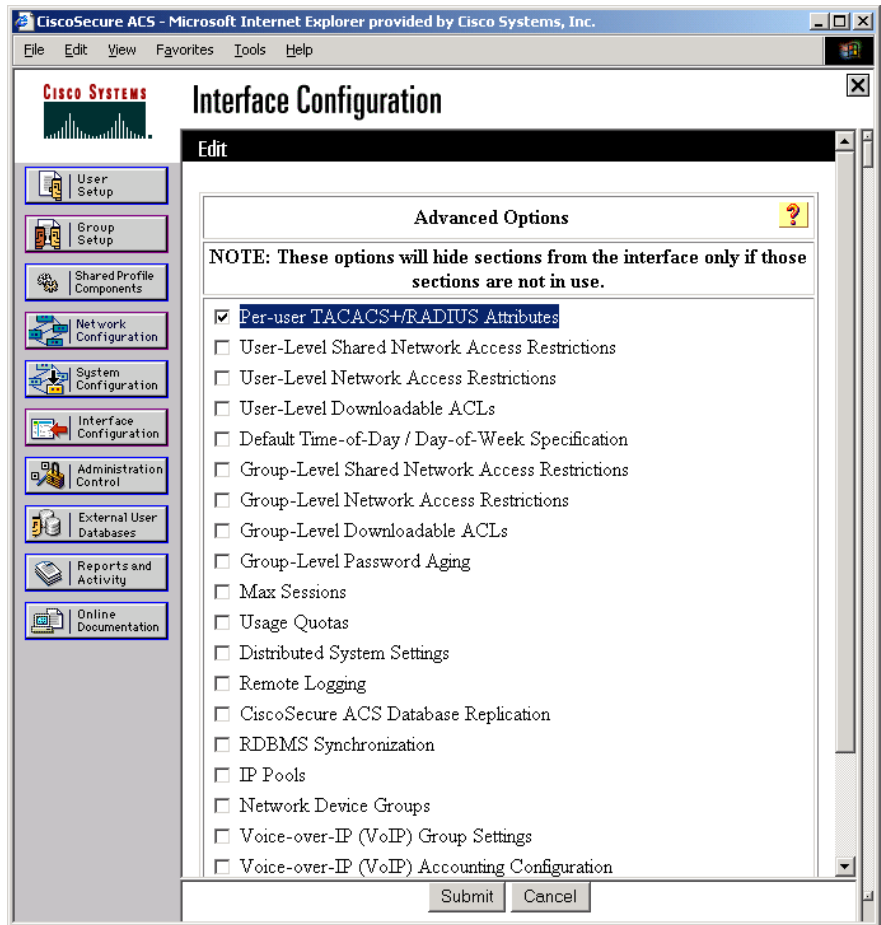
Below the table is a 'New Services' section with two rows of input fields:

	Service	Protocol
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

At the bottom right, there are 'Submit' and 'Cancel' buttons.

- b. Access the Advanced Options page. Check the **Per-user TACACS+/RADIUS Attributes** checkbox (see Figure 4-7).

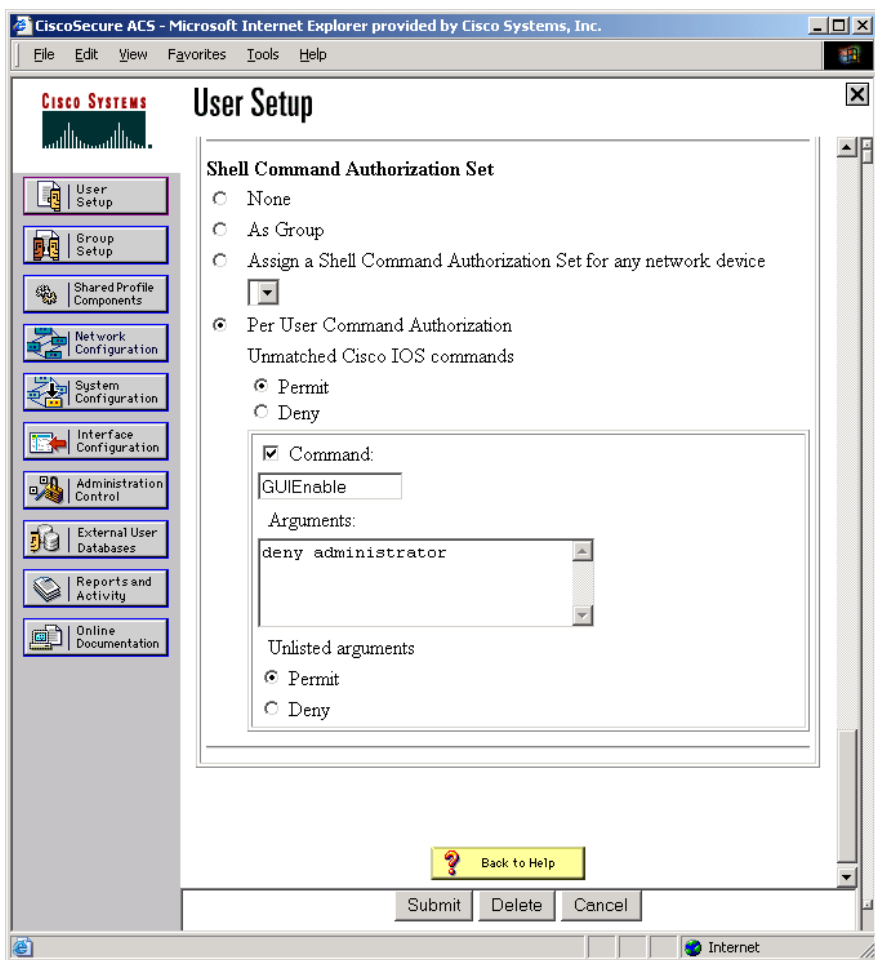
**Figure 4-7 Interface Configuration Page—Advanced Options Page**



2. Access the User Setup section of the Cisco Secure ACS interface and choose the name of a user to which you want to assign a primary GSSM GUI privilege level. The Edit page appears.

3. Scroll to the Shell Command Authorization Set section of the User Setup page.
4. Check the **Per User Command Authorization** checkbox.
5. Check the **Command** check box and type **GuiEnable** in the Command text box (see Figure 4-8).

**Figure 4-8** Assigning Operator-Level Privileges to a User from Cisco Secure ACS



148507

6. Assign operator user-level privileges from the TACACS+ server by entering the following string in the Arguments text box (see [Figure 4-8](#)):

**deny administrator**

The **deny administrator** string forces a user to have operator-level privileges when using the primary GSSM GUI.

7. Assign observer user-level privileges from the TACACS+ server by entering the following strings in the Arguments text box:

**deny administrator**

**deny operator**

These two strings force a user to have observer-level privileges when using the primary GSSM GUI.

8. Click the **Permit** option for Unlisted arguments.

## Enabling Custom User GUI Views When Authenticating a User from the TACACS+ Server

For a user with an assigned operator or observer role, a TACACS+ server does not directly support control over additional primary GSSM GUI application-specific functions such as user views. The GSS administrator can define a set of custom views that limit the data (configuration data and statistics) available on a primary GSSM GUI page. Each custom user view can include selections from the following properties:

- Answers
- Shared keepalives
- Locations
- Owners

When you assign a custom view to a user account, the user can see only the configured data and statistics associated with that view.

See the “[Custom User View Overview](#)” section in [Chapter 3, Creating and Managing User Accounts](#), for background on custom user views in the primary GSSM GUI.

If you want to assign a view to an authenticated user, configure a custom GUI view for the user on the primary GSSM GUI. Be sure to use the exact login name when creating the primary GSSM GUI user account. During the user authentication process, the GSS makes a correlation with the user name to determine if there is an associated user view configured on the primary GSSM GUI for that user. The custom user view is activated when the user accesses the primary GSSM GUI.

**Note**

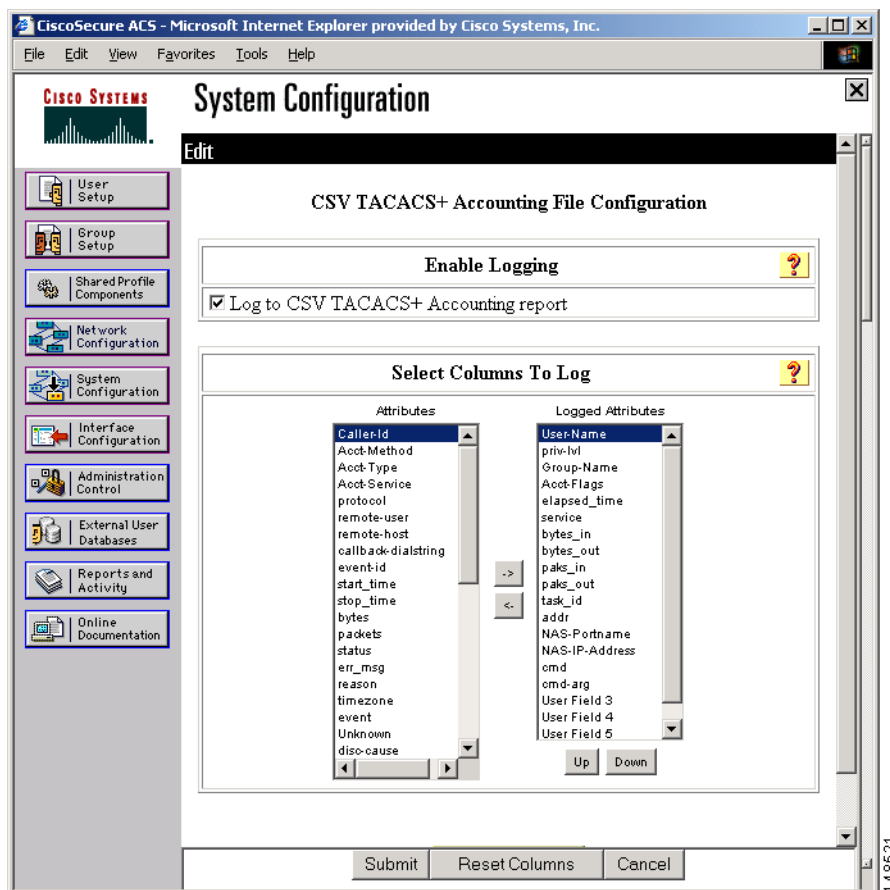
A password will also be required when creating a user account on the primary GSSM GUI. However, the GUI-specific password is not used during user authentication from a TACACS+ server. When you configure TACACS+ authentication on the GSS from the CLI, if you choose not to select the **local** fallback option for the **aaa authentication gui** CLI command (see the [“Configuring Authentication Settings on the TACACS+ Server”](#) section), ensure that you set the user account GUI-specific password to a random setting. Setting the password to a random setting helps to maintain the security of the primary GSSM GUI in the event that TACACS+ authentication fails for a GUI connection.

## Configuring Accounting Settings on the TACACS+ Server

To configure the accounting service for the Cisco Secure ACS, perform the following steps:

1. In the System Configuration section of the Cisco Secure ACS interface, the Logging Configuration page, click **CSV TACACS+ Accounting**. The Edit page appears (see [Figure 4-9](#)).

Figure 4-9 CSV TACACS+ Accounting File Logging Page of Cisco Secure ACS



2. Click the **Log to CSV TACACS+ Accounting report** check box.
3. Under **Select Columns To Log**, in the **Attributes** column, click the attribute that you want to log. Click **->** to move the attribute into the **Logged Attributes** column. Click **Up** or **Down** to move the column for this attribute to the desired position in the log. Repeat until all the desired attributes are in the desired positions in the **Logged Attributes** column.
4. Click **Submit** when you finish moving the attributes into the **Logged Attributes**.



# Identifying the TACACS+ Server Host on the GSS

The TACACS+ server contains the TACACS+ authentication, authorization, and accounting relational databases. You can designate a maximum of three servers on the GSS. However, the GSS uses only one server at a time. For recommended guidelines on setting up a TACACS+ server (the Cisco Secure ACS in this example), see the [“Configuring a TACACS+ Server for Use with the GSS”](#) section.

Use the **tacacs-server host** command to set up a list of preferred TACACS+ security daemons for use with the GSS. The TACACS+ software searches for the server hosts in the order that you specify through the **tacacs-server host** command.

The GSS periodically queries all configured TACACS+ servers with a TCP keepalive to ensure network connectivity and TACACS+ application operation. If the GSS determines that the first TACACS server is down, the GSS attempts to connect to the next server in the list of configured TACACS+ servers as the backup server. If a second (or third) TACACS+ server is available for use, the GSS selects that server as the active TACACS+ server.



## Note

The GSS uses TCP keepalives as the default to monitor connectivity with the active TACACS+ server. As a secondary measure, if the TCP keepalives fail, or if you disable the use of keepalives, you can use the **tacacs-server timeout** command to define a global TACACS+ timeout period that the GSS uses to wait for a response to a connection attempt from a TACACS+ server. The timeout value applies to all defined TACACS+ servers. See the [“Specifying the TACACS+ Server Timeout on the GSS”](#) section for details

Use the **tacacs-server host** command to specify the names of the IP host or hosts maintaining the TACACS+ server. You must provide the IP address or hostname for the server. By default, the GSS uses TCP port 49 to communicate with the TACACS+ server. You can optionally change the TCP port number to a different port number. To maintain security between the GSS and the TACACS+ server, you can also specify an encryption key.

When operating the GSS as a client with a TACACS+ server, the GSS may restrict user access to all CLI commands. This behavior can occur when you specify an encryption key on the GSS using the **tacacs-server host** command but do not specify the same encryption key on the TACACS+ server. In this case, the CLI command restriction takes place immediately on the GSS once you enter the **aaa authorization commands** command (see the [“Specifying TACACS+ Authorization of the GSS”](#) section).

You should first enter the **tacacs-server host** command on the GSS and then specify the same encryption key on the TACACS+ server *before* you enter the **aaa authorization commands** CLI command on the GSS. If the GSS fails to authorize all CLI commands and you are unable to change the encryption key on the TACACS+ server, power cycle the GSS. Because the CLI commands entered prior to the power cycle were not saved in the GSS startup-configuration file, you can regain access to the GSS CLI and redo the TACACS+ configuration.

The syntax for this global configuration command is as follows:

```
tacacs-server host ip_or_host [port port] [key encryption_key]
```

The arguments and keywords for this global configuration command are as follows:

- *ip\_or\_host*—IP address or hostname of the TACACS+ server that you want to access. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic hostname (for example, myhost.mydomain.com).
- **port** *port*—(Optional) TCP port of the TACACS+ server. The default port is 49. You can enter a port number from 1 to 65535.
- **key** *encryption\_key*—(Optional) Shared secret between the GSS and the TACACS+ server. If you want to encrypt TACACS+ packet transactions between the GSS and the TACACS+ server, define an encryption key. If you do not define an encryption key, the GSS transmits packets to the TACACS+ server in clear text. The range for the encryption key is 1 to 100 alphanumeric characters.

For example, to configure three TACACS+ servers as 192.168.1.100:8877, 192.168.1.101:49 (using the default TCP port), and 192.168.1.102:9988 with different shared secrets, enter:

```
gss1.example.com(config)# tacacs-server host 192.168.1.100 port 8877
key SECRET-123
gss1.example.com(config)# tacacs-server host 192.168.1.101 key
SECRET-456
gss1.example.com(config)# tacacs-server host 192.168.1.102 port 9988
key SECRET-789
```

Once configured, the IP address and port of a TACACS+ server cannot easily be changed. To change the IP address and port of a TACACS+ server, you must first delete the configured TACACS+ server, reenter the TACACS+ server with a new IP address and, if necessary, specify a new port number. Use the **no** form of the **tacacs-server-host** command to delete an existing TACACS+ server from the running configuration.

For example, to delete the TACACS+ server at IP address 192.168.1.101 with default TCP port 49 from the running configuration, enter:

```
gss1.example.com(config)# no tacacs-server host 192.168.1.101
```

or

```
gss1.example.com(config)# no tacacs-server host 192.168.1.101 port 49
```

If you defined an encryption key, it is not necessary to include that key to delete the TACACS+ server.

If you specified a TCP port other than default port number 49 when configuring the TACACS+ server, you must also include the TCP port to delete the TACACS+ server. For example, if you specified port 8877 for the TACACS+ server at IP address 192.168.1.101, enter:

```
gss1.example.com(config)# no tacacs-server host 192.168.1.101 port
8877
```

You can change or remove the encryption key without deleting the TACACS+ server. For example, to remove the key SECRET-123 without removing the TACACS+ server, enter:

```
gss1.example.com(config)# no tacacs-server host 192.168.1.101 key
SECRET-123
```

If you specified a TCP port other than default port 49, specify the following to remove the key SECRET-123 without removing the server:

```
gss1.example.com(config)# no tacacs-server host 192.168.1.101 port  
8877 key SECRET-123
```

## Disabling TACACS+ Server Keepalives on the GSS

By default, the GSS enables the automatic use of TCP keepalives to periodically query all online TACACS+ servers with a TCP keepalive to ensure network connectivity and TACACS+ application operation. If the GSS determines that the first TACACS server is down (offline), the GSS then attempts to connect to the next server in the list of configured TACACS+ servers as the backup server. If a second (or third) TACACS+ server is available for use, the GSS selects that server as the active TACACS+ server.

To disable the use of TCP keepalives with the active TACACS+ server, use the **no** form of the **tacacs-server keepalive-enable** command. The syntax for this global configuration command is as follows:

```
no tacacs-server keepalive-enable
```

If you disable TCP keepalives, the GSS will continue to use the TACACS+ timeout period (that you specified in the **tacacs-server timeout** command) to wait for a response to a connection attempt from a nonoperational TACACS+ server before switching to the next server in the list of configured TACACS+ servers. See the [“Specifying the TACACS+ Server Timeout on the GSS”](#) section for details on defining a global TACACS+ timeout period.

To disable the use of TCP keepalives with the active TACACS+ server, enter:

```
gss1.example.com(config)# no tacacs-server keepalive-enable
```

To reenable the use of TCP keepalives with the active TACACS+ server, enter:

```
gss1.example.com(config)# tacacs-server keepalive-enable
```

# Specifying the TACACS+ Server Timeout on the GSS

As a secondary measure, if the TCP keepalives fail, or if you disable the use of keepalives, you can use the **tacacs-server timeout** command to define a global TACACS+ timeout period, in seconds, that specifies how long the GSS waits for a response to a connection attempt from a TACACS+ server. The timeout value applies to all defined TACACS+ servers. The default timeout period is 5 seconds.

To specify the timeout period, use the **tacacs-server timeout** command. The syntax for this global configuration command is as follows:

**tacacs-server timeout** *seconds*

The *seconds* argument is a value from 1 to 255 seconds. The GSS dynamically applies the modified timeout period and the new value takes effect automatically on the next TACACS+ connection.

For example, to set the timeout period to 60 seconds, enter:

```
gss1.example.com(config)# tacacs-server timeout 60
```

To reset the timeout period to the default of 5 seconds, enter:

```
gss1.example.com(config)# no tacacs-server timeout 60
```

## Specifying TACACS+ Authentication of the GSS

After you identify a TACACS+ server, you can enable the TACACS+ authentication service on the GSS by using the **aaa authentication** command to enable TACACS+ authentication. By default, the GSS falls back to local authentication with either the console port or a Telnet connection if the GSS cannot remotely contact a TACACS+ server. Optionally, you can specify local authentication if TACACS+ authentication fails for an FTP, GUI, or SSH connection.



### Note

You must enable remote access on the GSS device (SSH, Telnet, or FTP) before you enable TACACS+ authentication for the specific GSS access method. See the *Cisco Global Site Selector Getting Started Guide* for details.

The syntax for this global configuration command is:

**aaa authentication {ftp | gui | login | ssh} [local]**

The keywords for this global configuration command are as follows:

- **ftp**—Enables the TACACS+ authentication service for a File Transfer Protocol (FTP) remote access connection.
- **gui**—Enables the TACACS+ authentication service for a primary GSSM GUI connection.
- **login**—Enables the TACACS+ authentication service for the login service, using either a direct connection to the GSS console port or through a Telnet remote access connection.
- **ssh**—Enables the TACACS+ authentication service for a Secure Shell (SSH) remote access connection.
- **local**—(Optional) Used when you want the GSS to fall back to local authentication if TACACS+ authentication fails for an FTP, GUI, or SSH connection. The **local** option is always enabled for the login (console port or Telnet) access method.

For example, to enable TACACS+ authentication for an SSH remote access connection that can revert back to local authentication, enter:

```
gss1.example.com(config)# aaa authentication ssh local
```

Use the **no** form of the **aaa authentication** command to disable the TACACS+ authentication function. For example, to disable TACACS+ authentication for an SSH remote access connection, enter:

```
gss1.example.com(config)# no aaa authentication ssh
```

## Specifying TACACS+ Authorization of the GSS

TACACS+ authorization enables you to set parameters that restrict user access to specific GSS CLI commands, as defined by the TACACS+ server. Use the **aaa authorization commands** command to enable the TACACS+ authorization service to limit a user's access to specific GSS CLI commands. The **aaa authorization commands** command applies to the user-level and privileged-level EXEC mode commands issued on the GSS. The command authorizes all attempts to enter user-level and privileged-level EXEC mode commands, including global configuration and interface configuration commands.

When operating the GSS as a client with a TACACS+ server, the GSS may restrict user access to all CLI commands. For example, this restriction may occur if you specify an encryption key on the GSS by using the **tacacs-server host** command (see the [“Identifying the TACACS+ Server Host on the GSS”](#) section), but do not specify the same encryption key on the TACACS+ server. In this case, the CLI command restriction takes place immediately on the GSS once you enter the **aaa authorization commands** command.

You must first enter the **tacacs-server host** command on the GSS and then specify the same encryption key on the TACACS+ server *before* you enter the **aaa authorization commands** CLI command on the GSS. If the GSS fails authorization on all CLI commands and you are unable to change the encryption key on the TACACS+ server, power cycle the GSS. Because the CLI commands entered prior to the power cycle were not saved in the GSS startup-configuration file, you can regain access to the GSS CLI and redo the TACACS+ configuration. To enable TACACS+ authorization for the GSS CLI commands, enter:

```
gss1.example.com(config)# aaa authorization commands
```

Use the **no** form of this command to disable the TACACS+ CLI command authorization function. For example, enter:

```
gss1.example.com(config)# no aaa authorization commands
```

For details about limiting user access to GSS CLI commands from the TACACS+ server, see the [“Configuring Authorization Settings on the TACACS+ Server”](#) section.

## Specifying TACACS+ Accounting on the GSS

TACACS+ accounting enables you to monitor GSS CLI commands or primary GSSM GUI pages and user actions executed in the GSS. The information is contained in an accounting record and is transmitted from the GSS to the TACACS+ server. Each record can include a number of fields such as the user name, the executed CLI command, the accessed primary GSSM GUI page and the performed action, and the time of execution. The Cisco Secure ACS records its logs in comma-separated value (CSV) text files. You can import CSV log files into many popular spreadsheet applications. If required, you can generate the CSV-exported spreadsheet as an HTML table using a number of CSV-to-HTML applications.

You must enable logging for accounting reports on the TACACS+ server and that you select the attributes that you want to log. For general guidelines on the recommended setup of a TACACS+ server for accounting (the Cisco Secure ACS in this example), see the [“Configuring Accounting Settings on the TACACS+ Server”](#) section.

Use the **aaa accounting** command to enable the TACACS+ accounting service. The syntax for this global configuration command is as follows:

```
aaa accounting {commands | gui}
```

The keywords for this command are as follows:

- **commands**—Enables the TACACS+ accounting service for monitoring the use of GSS CLI commands. The **commands** option applies to the user-level and privileged-level EXEC mode commands that a user issues. Command accounting generates accounting records for all user-level and privileged-level EXEC mode commands, including global configuration and interface configuration commands.
- **gui**—Enables the TACACS+ accounting service to monitor access to the primary GSSM GUI pages and the actions performed on those pages.

To enable TACACS+ accounting for the GSS CLI, enter:

```
gss1.example.com(config)# aaa accounting commands
```

Use the **no** form of the **aaa accounting** command to disable the TACACS+ accounting function. To disable TACACS+ accounting for the GSS CLI, enter:

```
gss1.example.com(config)# no aaa accounting commands
```

## Showing TACACS+ Statistics on the GSS

You can display a summary of the TACACS configuration on your GSS device by using the **show tacacs** command.

For example, to display the current TACACS+ configuration, enter:

```
gss1.example.com# show tacacs
Current tacacs server configuration
tacacs-server timeout 5
tacacs-server keepalive-enable
tacacs-server host 1192.168.1.100 port 49
aaa authentication ftp
```



Use the **show statistics tacacs** command to display the current TACACS+ statistics. Each server is identified by the IP address and port. There is a PASS, FAIL, and ERROR counter for each authentication, authorization, and accounting service. The **show statistics tacacs** command also indicates whether the TCP keepalive is ONLINE or OFFLINE.



**Note**

If you disable the TCP keepalive function, the **show statistics tacacs** command output always displays the TCP keepalive as ONLINE.

For example, to display the current TACACS+ statistics for the GSS, enter:

```
gss1.example.com# show statistics tacacs
```

```

Server 192.168.1.100:49  ONLINE
                        PASS  FAIL  ERROR
Authentication    321     4     0
Authorization     782    48     0
Accounting        535     0     0

Server 192.168.1.101:49  ONLINE
                        PASS  FAIL  ERROR
Authentication    17     1     0
Authorization     39     3     0
Accounting        12     0     0
    
```

Table 4-2 describes the fields in the **show statistics tacacs** command output.

**Table 4-2** Field Descriptions for show statistics tacacs Command

Field	Description
Server	IP address or hostname, along with the TCP port, of the active TACACS+ server. This field also indicates whether the TCP keepalive is ONLINE or OFFLINE.
Pass	Counter that increments when a “pass” condition occurs for the specific service. For example, if a user successfully performs an authentication with a GSS, the GSS increments the Authentication Pass counter. If the GSS permits a user to access a specific CLI command through authorization, the GSS increments the Authorization Pass counter.

**Table 4-2** Field Descriptions for *show statistics tacacs* Command (continued)

Field	Description
Fail	Counter that increments when a deny condition occurs as the result of an authentication, authorization, or accounting service.
Error	Counter that increments as the result of a communications failure with the TACACS+ server, a TACACS+ protocol error, or an internal error that prevented the session from completing.

## Clearing TACACS+ Statistics on the GSS

You can clear the current TACACS+ statistics by using **clear statistics tacacs** command. Clearing the statistics for a GSS erases all TACACS+ activity and performance records for that device.

For example, enter:

```
gss1.example.com# clear statistics tacacs  
Are you sure? (yes/no) yes
```

## Disabling TACACS+ on a GSS

As a GSS administrator, if you accidentally lock yourself out of a GSS device and are unable to receive TACACS+ user authentication or authorization to access that device, you can disable the TACACS+ function on that GSS from the CLI. You must have physical access to the GSS device to perform this procedure.

To disable TACACS+ on a GSS device, perform the following steps:

1. Attach an ASCII terminal to the console port on the GSS device. See the *Cisco Global Site Selector Hardware Installation Guide* for instructions on connecting a console cable to your Cisco Global Site Selector series hardware.
2. Press the power control button on the GSS to power cycle the device and perform a restart. As the GSS reboots, the output appears on the console terminal.

3. After the BIOS boots and the LILO boot: prompt appears, type the following to disable TACACS+ for the GSS device:

```
LILO: <Tab>
GSS-1.31
LILO:GSS-1.31 DISABLETACACS=1
```

During the boot process, the following appears:

```
Mounting other Filesystems: [ OK ]
*** Disabling TACACS Authentication and Authorization
Building Properties
```

You should now be able to locally access the GSS device and reconfigure the TACACS+ authentication and authorization functions for the GSS device.

4. Save your configuration changes to memory.

```
gssml.example.com# copy running-config startup-config
```

If you fail to save your configuration changes, the GSS device reverts to its previous settings (including the previous TACACS+ configuration) upon a reboot.





## CHAPTER

# 5

# Configuring Access Lists and Filtering GSS Traffic

---

You can filter incoming traffic received by the GSS by using access lists. You create access lists at the CLI of each GSS device. This chapter describes how to create access lists and access groups to filter GSS traffic.

It contains the following major sections:

- [Filtering GSS Traffic Using Access Lists](#)
- [Deploying GSS Devices Behind Firewalls](#)

## Filtering GSS Traffic Using Access Lists

This section contains the following topics:

- [Access List Overview](#)
- [Creating an Access List](#)
- [Associating an Access List with a GSS Interface](#)
- [Disassociating an Access List from a GSS Interface](#)
- [Adding Rules to an Access List](#)
- [Removing Rules from an Access List](#)
- [Segmenting GSS Traffic by Ethernet Interface](#)
- [Segmenting GSS Traffic by Ethernet Interface](#)
- [Displaying Access Lists](#)

## Access List Overview

The packet filtering tools on the GSS instruct each device to permit or refuse specific packets based on a combination of criteria that includes the following:

- Destination port of the packets
- Requesting host
- Protocol used (TCP, UDP, or ICMP)

You create packet-filtering tools, called access lists, from the GSS CLI. Access lists are collections of filtering rules that you create using the **access-list** CLI command. Each access list is a sequential collection of permit and deny conditions that apply to a source network IP address to control whether the GSS forwards or blocks routed packets. The GSS examines each packet to determine whether to forward or drop the packet based on the criteria specified within the access lists.

You can create any number of access lists on each GSS device. After creating an access list, you can append or remove rules from the list at any time. Apply access lists to one or both of the GSS Ethernet interfaces using the **access-group** command.

The GSS appends each additional criteria statement to the *end* of the access list statements. Be aware that you cannot delete individual statements after creating them. You can only delete an entire access list.

The order of access list statements is very important. When the GSS decides whether to forward or block a packet, it tests the packet against each criteria statement in the order that the statements were created. After a match is found, the GSS does not check any additional criteria statements.

If you create a criteria statement that explicitly permits all traffic, the GSS does not check any additional statements added after the explicit permit statement and permits all traffic. If you need additional statements, delete the access list and retype it with the new entries.

To ensure your GSS functions properly with access lists, identify the ports and protocols normally used by each GSS device. [Table 5-1](#) lists the types of expected inbound traffic received by the GSS.

**Note**

---

Outbound traffic is not affected by access lists. However, the return inbound traffic must be explicitly permitted because GSS access lists are not stateful.

---

**Table 5-1 GSS-Related Ports and Protocols for Inbound Traffic**

Source Port (Remote Device)	Destination Port (GSS)	Protocol	Details
*	20–23	TCP	FTP, SSH, and Telnet server services on the GSS
20–23	*	TCP	Return traffic of FTP, Secure Copy (SCP), and Telnet GSS CLI commands
49 or user configured	*	TCP	Return traffic for TACACS+
*	53	UDP, TCP	GSS DNS server traffic
53	*	UDP	Return traffic of GSS software reverse lookup, “dnslookup” queries, and name server forwarding
123	123	UDP	Network Time Protocol (NTP) updates
*	161	UDP	Simple Network Management Protocol (SNMP) traffic
*	443	TCP	Primary GSSM GUI
1304	1304	UDP	CRA keepalives
1974	1974	UDP	Director Response Protocol (DRP) protocol traffic
*	2000	UDP	Inter-GSS periodic status reporting
*	2001–2005	TCP	Inter-GSS communication
2001–2005	*	TCP	Return traffic of inter-GSS communication
*	3002–3008	TCP	Inter-GSS communication
3002–3008	*	TCP	Return traffic of inter-GSS communication
*	5001	TCP	Global sticky mesh protocol traffic

**Table 5-1 GSS-Related Ports and Protocols for Inbound Traffic (continued)**

Source Port (Remote Device)	Destination Port (GSS)	Protocol	Details
5001	*	TCP	Return traffic of global sticky mesh protocol traffic
5002	*	UDP	Return traffic of KAL-AP keepalives

\*Any legal port number

## Creating an Access List

You can use the **access-list** command in global configuration mode to create an access list. You must have access to the CLI of each GSS device to create access lists for that device.

The syntax for the **access-list** command is as follows:

```
access-list name {permit | deny} protocol [source-address source-netmask |
host source-address | any] operator port [port] [destination-port
operator port [port]]
```

The keywords and arguments are as follows:

- **name**—Alphanumeric name used to identify the access list you are creating.
- **permit**—Allows a connection when a packet matches the condition. All provisions of the condition must be met to make a match.
- **deny**—Prevents a connection when a packet matches the condition. All provisions of the condition must be met to make a match.
- **protocol**—Protocol for the traffic type. Recognized IP protocols include: **tcp** (Transmission Control Protocol), **udp** (User Datagram Protocol), and **icmp** (Internet Control Message Protocol).
- **source-address**—Network IP address from which the packet originated. The GSS software uses the *source-address* and *source-netmask* arguments to match the incoming packet to a source network.



- *source-netmask*—Subnet mask for the network from which the packet originated. The software uses the *source-address* and *source-netmask* arguments to match the incoming packet to a source network.
- **host**—Identifies the host machine that is the source of the packet.
- *source-address*—IP address of the device that is the source of the packet.
- **any**—Identifies the wildcard value for the packet source. With **any** used in place of the *source-address*, *source-netmask*, or **host** *source-address* values, the GSS matches packets from all incoming sources.
- *operator* —Arbitrary bytes within the packet. The *operator* can be one of the following values: **eq** (equal), **neq** (not equal), **range** (range)
- *port*—Source or destination port of the packet.
- **destination-port**—Compares the destination port of the packet with the access condition.

For example, to configure an access list named *alist1* containing a rule that allows any traffic using the TCP protocol on port 443 on the GSS device, enter the following:

```
gss1.example.com# config
gss1.example.com(config)# access-list alist1 permit tcp any
destination-port eq 443
```

Use the **access-list** command for each access list that you intend to add to this GSS device. See the [“Adding Rules to an Access List”](#) section for instructions about adding more rules to an access list that already exists.

The following example shows a completed access list (*alist1*):

```
gss1.example.com(config)# show access-list

access-list: alist1
  access-list alist1 permit tcp any destination-port range 20 23
  access-list alist1 permit tcp any eq 20
  access-list alist1 permit tcp any eq 21
  access-list alist1 permit tcp any eq 23
  access-list alist1 permit tcp any eq 49
  access-list alist1 permit tcp any destination-port eq 53
  access-list alist1 permit udp any destination-port eq 53
  access-list alist1 permit udp any eq 53
  access-list alist1 permit udp any eq 123 destination-port eq 123
  access-list alist1 permit udp any destination-port eq 161
  access-list alist1 permit tcp any destination-port eq 443
```

```

access-list alist1 permit udp any eq 1304 destination-port eq 1304
access-list alist1 permit udp any destination-port eq 2000
access-list alist1 permit tcp any destination-port range 2001 2005
access-list alist1 permit tcp any range 2001 2005
access-list alist1 permit tcp any destination-port range 3002 3008
access-list alist1 permit tcp any range 3002 3008
access-list alist1 permit udp any destination-port eq 5002
access-list alist1 permit udp any eq 1974 destination-port eq 1974
access-list alist1 permit tcp any destination-port eq 5001
access-list alist1 permit tcp any eq 5001
access-list alist1 permit icmp any

```

## Kernel output

```

access-list alist1 on interface eth0 (1 references)
target      prot opt source      destination
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpts:20:23
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spt:20
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spt:21
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spt:23
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spt:49
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpt:53
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp dpt:53
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp spt:53
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp spt:123 dpt:123
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp dpt:161
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpt:443
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp spt:1304 dpt:1304
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp dpt:2000
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpts:2001:2005
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spts:2001:2005
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpts:3002:3008
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spts:3002:3008
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp dpt:5002
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp spt:1974 dpt:1974
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpt:5001
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spt:5001
ACCEPT      icmp --  0.0.0.0/0    0.0.0.0/0
DROP        all  --  0.0.0.0/0    0.0.0.0/0

```

## Associating an Access List with a GSS Interface

After you create an access list, associate it with one or both of the GSS Ethernet interfaces before you use the access list to filter incoming traffic received by the interface. If no access lists are associated with an interface, the GSS allows all incoming traffic received on that interface. After you apply an access list, the GSS allows only the type of traffic explicitly permitted by the access list. The GSS disallows all other traffic.

Use the **access-group** command in global configuration mode to associate an access list with a GSS interface. You must have access to the CLI of each GSS device to associate access lists with a GSS interface.

The syntax for the **access-group** command is as follows:

```
access-group name interface {eth0 | eth1}
```

The keywords and arguments are as follows:

- *name*—Name of a pre-existing access list.
- **interface**—Specifies an interface on the GSS to which the access list will be assigned.
- **eth0**—Identifies the first Ethernet interface on the GSS device.
- **eth1**—Identifies the second Ethernet interface on the GSS device.

The GSS does not allow you to assign the same preexisting access list to both Ethernet interfaces on the GSS device. If you attempt to use the **access-group** CLI command to assign the same access list to Ethernet 0 and Ethernet 1, the following error message appears:

```
%access-list list1 is already assigned to interface eth1.
```

If this error message appears, generate an identical access list for the second Ethernet interface on the GSS device.

For example, to associate the access list named *alist1* with the first interface on your GSS device, enter the following:

```
gss1.example.com# config  
gss1.example.com(config)# access-group alist1 interface eth0
```

Use the **access-group** command for each access list that you want to associate with the interface.

## Disassociating an Access List from a GSS Interface

You can dissociate an access list from the associated GSS interface by using the **no** form of the **access-group** command. Disassociating an access list from an interface removes all constraints applied to the Ethernet interface. You must have access to the CLI of each GSS device to disassociate access lists from a GSS interface.

For example, to disassociate the access list named *alist1* from the first interface on your GSS device, you enter:

```
gss1.example.com# config  
gss1.example.com(config)# no access-group alist1 interface eth0
```

See the [“Associating an Access List with a GSS Interface”](#) section for an explanation of **access-group** command syntax.

## Adding Rules to an Access List

After you create one or more access lists, you can append rules to them at any time. Use the **access-list** command to add a new rule to an existing access list.

For example, to add a new rule to the access list named *alist1* to block all traffic from host 192.168.1.101, enter:

```
gss1.example.com# config  
gss1.example.com(config)# access-list alist1 deny tcp host  
192.168.1.101
```

See the [“Creating an Access List”](#) section for an explanation of **access-list** command syntax.

Use the **show access-list** command to verify that the rule is added to your access list.

```
gss1.example.com(config)# show access-list  
access-list:alist1  
access-list alist1 permit tcp any destination-port eq 443  
access-list alist1 deny tcp host 192.168.1.101
```

## Removing Rules from an Access List

Access lists must contain at least one rule. Removing the last rule from an access list removes the list itself from the GSS. To remove a rule from an existing access list, use the **no** form of the **access-list** command in global configuration mode.

For example, to remove the rule from the access list named *alist1* that blocks all traffic from host 192.168.1.101, enter:

```
gss1.example.com# config
gss1.example.com(config)# no access-list alist1 deny tcp host
192.168.1.101
```

See the “[Creating an Access List](#)” section for an explanation of **access-list** command syntax.

Use the **show access-list** command to verify that the rule has been removed from your access list.

```
gss1.example.com(config)# show access-list
access-list:alist1
access-list alist1 permit tcp any destination-port eq 443
```

## Segmenting GSS Traffic by Ethernet Interface

By default, the GSS devices listen for DNS traffic on both GSS Ethernet interfaces, 0 and 1. In the case of inter-GSS communications, GSS devices listen for configuration and status updates on one interface only. Ethernet interface 0 is the default.

To reconfigure which interface is used for inter-GSS communications on the GSS network, use the **gss-communications** command. See the *Cisco Global Site Selector Getting Started Guide* for details.

For security reasons you can limit GSS traffic to one Ethernet interface, or segment traffic by constraining a certain type of traffic on a designated interface. By using the **access-list** and **access-group** commands discussed previously, you can define access lists that limit traffic on either of the two GSS Ethernet interfaces.

For example, remote management services such as Telnet, SSH, and FTP listen on all active interfaces. To force these remote management services to listen on only the second GSS Ethernet interface, enter:

```
gss1.example.com# config
gss1.example.com(config)#
gss1.example.com(config)# access-list alist1 permit tcp any
destination-port ftp
gss1.example.com(config)# access-list alist1 permit tcp any
destination-port ssh
gss1.example.com(config)# access-list alist1 permit tcp any
destination-port telnet
gss1.example.com(config)# access-group alist1 interface eth1
```

The commands listed above limit the second Ethernet interface (eth1) to the specified traffic. All other traffic is refused to that interface.

To deny the same traffic on the first Ethernet interface (eth0), enter:

```
gss1.example.com(config)#
gss1.example.com(config)# access-list alist1 deny tcp any
destination-port ftp
gss1.example.com(config)# access-list alist1 deny tcp any
destination-port ssh
gss1.example.com(config)# access-list alist1 deny tcp any
destination-port telnet
gss1.example.com(config)# access-group alist1 eth0
```

## Displaying Access Lists

You can use the **show access-list** command to display all configured access lists.

```
gss1.example.com(config)#show access-list
```

```
access-list: alist1
  access-list alist1 permit tcp any destination-port range 20 23
  access-list alist1 permit tcp any eq 20
  access-list alist1 permit tcp any eq 21
  access-list alist1 permit tcp any eq 23
  access-list alist1 permit tcp any eq 49
  access-list alist1 permit tcp any destination-port eq 53
  access-list alist1 permit udp any destination-port eq 53
  access-list alist1 permit udp any eq 123 destination-port eq 123
  access-list alist1 permit udp any destination-port eq 161
  access-list alist1 permit tcp any destination-port eq 443
```

```

access-list alist1 permit udp any eq 1304 destination-port eq 1304
access-list alist1 permit udp any destination-port eq 2000
access-list alist1 permit tcp any destination-port range 2001 2005
access-list alist1 permit tcp any range 2001 2005
access-list alist1 permit tcp any destination-port range 3002 3008
access-list alist1 permit tcp any range 3002 3008
access-list alist1 permit udp any destination-port eq 5002
access-list alist1 permit udp any eq 1974 destination-port eq 1974
access-list alist1 permit tcp any destination-port eq 5001
access-list alist1 permit tcp any eq 5001
access-list alist1 permit icmp any

```

#### Kernel output

```

access-list alist1 on interface eth0 (1 references)
target      prot opt source      destination
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpts:20:23
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spt:20
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spt:21
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spt:23
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spt:49
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpt:53
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp dpt:53
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp spt:53
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp spt:123 dpt:123
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp dpt:161
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpt:443
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp spt:1304 dpt:1304
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp dpt:2000
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpts:2001:2005
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spts:2001:2005
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpts:3002:3008
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spts:3002:3008
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp dpt:5002
ACCEPT      udp  --  0.0.0.0/0    0.0.0.0/0    udp spt:1974 dpt:1974
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp dpt:5001
ACCEPT      tcp  --  0.0.0.0/0    0.0.0.0/0    tcp spt:5001
ACCEPT      icmp --  0.0.0.0/0    0.0.0.0/0
DROP        all  --  0.0.0.0/0    0.0.0.0/0

```

Use the **show access-group** command to display a list of the access lists associated with GSS interfaces Ethernet 0 and Ethernet 1.

```

gss1.example.com(config)#show access-group
access group alist1 interface eth0

```

# Deploying GSS Devices Behind Firewalls

This section describes how to configure your GSS for deployment behind a firewall. It contains the following topics:

- [GSS Firewall Deployment Overview](#)
- [Configuring GSS Devices Behind a Firewall](#)

## GSS Firewall Deployment Overview

In addition to the packet-filtering features of the **access-list** and **access-group** commands (see the “[Filtering GSS Traffic Using Access Lists](#)” section), you can also deploy your GSS devices behind an existing firewall on your enterprise network.

When you configure your GSS for deployment behind a firewall, you must allow DNS traffic into the device. If you have multiple GSS devices deployed so that traffic between the devices must pass through a firewall, configure the firewall to allow inter-GSS communications and inter-GSS status reporting. Depending on your GSS configuration, you can also allow other traffic to pass through the firewall. This requirement depends on your GSS configuration (for example, if you are using TCP-based or KAL-AP keepalives) and the ability to access certain GSS services through the firewall (for example, SNMP).

The GSS does not support deployment of devices behind a NAT for inter-GSS communication. The communication between the GSS devices cannot include an intermediate device behind a NAT because the actual IP address of the devices is embedded in the payload of the packets.

To configure your firewall to function with a GSS device, follow the guidelines outlined in [Table 5-2](#) and [Table 5-3](#) to permit inbound and outbound traffic transmitted to and received from the specified GSS ports. If you are using stateful firewalls, the rules for return traffic outlined in [Table 5-2](#) and [Table 5-3](#) may not be required.

In addition, use the **access-list** and **access-group** commands to enable authorized GSS traffic to the specified ports. By default, the GSS interface blocks all ports not explicitly permitted in your access list once you associate the access list with an Ethernet interface.



**Table 5-2 Inbound Traffic Going Through a Firewall to the GSS**

Source Port (Remote Device)	Destination Port (GSS)	Protocol	Details
*	20–23	TCP	FTP, SSH, and Telnet services
49 or user configured	*	TCP	Return traffic for TACACS+
*	53	UDP, TCP	GSS DNS server traffic
53	*	UDP	Return traffic of GSS software reverse lookup, “dnslookup” queries, and name server forwarding
80 or user-configured	*	TCP	Return traffic of TCP and HTTP keepalives
123	123	UDP	Return traffic of NTP updates
*	161	UDP	SNMP traffic
*	443	TCP	Primary GSSM GUI
1304	1304	UDP	Return traffic of CRA keepalives
1974	1974	UDP	Return traffic of DRP protocol traffic
*	2000	UDP	Inter-GSS periodic status reporting
*	2001–2005	TCP	Inter-GSS communication
2001-2005	*	TCP	Return traffic of inter-GSS communication
*	3002–3008	TCP	Inter-GSS communication
3002-3008	*	TCP	Return traffic of inter-GSS communication
*	5001	TCP	Global sticky mesh protocol traffic

**Table 5-2 Inbound Traffic Going Through a Firewall to the GSS (continued)**

Source Port (Remote Device)	Destination Port (GSS)	Protocol	Details
5001	*	TCP	Return traffic of global sticky mesh protocol traffic
5002	*	UDP	Return traffic of KAL-AP keepalives

\*Any legal port number

**Table 5-3 Outbound Traffic Originating from the GSS**

Source Port (GSS)	Destination Port (Remote Device)	Protocol	Details
20–23	*	TCP	Return traffic of FTP, SSH, and Telnet server services on the GSS
*	49 or user configured	TCP	TACACS+
*	20–23	TCP	Traffic of FTP, SCP, and Telnet GSS CLI commands
53	*	UDP, TCP	Return traffic of GSS DNS server traffic
*	53	UDP	GSS software reverse lookup, “dnslookup” queries, and name server forwarding
*	80 or user-configured	TCP	TCP and HTTP keepalives
123	123	UDP	NTP updates
161	*	UDP	Return traffic of Simple Network Management Protocol (SNMP) traffic

**Table 5-3 Outbound Traffic Originating from the GSS (continued)**

Source Port (GSS)	Destination Port (Remote Device)	Protocol	Details
443	*	TCP	Return traffic of Primary GSSM GUI
1304	1304	UDP	CRA keepalives
1974	1974	UDP	DRP protocol traffic
*	2000	UDP	Inter-GSS periodic status reporting
*	2001–2005	TCP	Inter-GSS communication
2001-2005	*	TCP	Return traffic of inter-GSS communication
*	3002–3008	TCP	Inter-GSS communication
3002-3008	*	TCP	Return traffic of inter-GSS communication
*	5001	TCP	Global sticky mesh protocol traffic
5001	*	TCP	Return traffic of global sticky mesh protocol traffic
*	5002	UDP	KAL-AP keepalives

\*Any legal port number

## Configuring GSS Devices Behind a Firewall

To configure GSS devices to operate behind a firewall, perform the following steps:

1. Determine the level of access and the services that you want enabled on your GSS and GSSM devices. Decide if you want to:
  - Allow FTP, SSH, and Telnet access to the GSS device

- Permit GUI access to the primary GSSM

[Table 5-2](#) and [Table 5-3](#) list the GSS-related ports and protocols to enable for the GSS device to function properly.

2. Construct your access lists to filter traffic incoming and outgoing from your GSS device. See the [“Creating an Access List”](#) section for details.



## CHAPTER

# 6

# Configuring SNMP

---

This chapter describes how to configure Simple Network Management Protocol (SNMP) to query GSS devices for standard MIB resources.

It contains the following major sections:

- [Overview](#)
- [Configuring SNMP on the GSS](#)
- [Configuring SNMP Servers](#)
- [Configuring SNMP Server Notifications](#)
- [Configuring SNMP Server Trap Limits](#)
- [Specifying Recipients for SNMP Notification Operations](#)
- [Viewing SNMP Status](#)
- [Viewing MIB Files on the GSS](#)

## Overview

SNMP is a set of network management standards for IP-based internetworks. SNMP includes a protocol, a database-structure specification, and a set of management data objects. SNMP implementations typically consist of a management application running on one or more network management systems (NMSs), and agent applications, usually executing in firmware on various network devices.

SNMP obtains information from the network through a Management Information Base (MIB). The MIB is a database of code blocks called *MIB objects*. Each MIB object controls one specific function, such as counting how many bytes are transmitted through an agent's port. The MIB object consists of *MIB variables*, which define the MIB object name, description, and default value.

Each GSS or GSSM contains an SNMP agent, `ucd-snmp v4.2.3`, to query other GSS devices for standard MIB resources found in MIB-II (RFC-1213) and Host Resources MIB (RFC 2790). SNMP runs on GSS port 161 by default. The SNMP agent receives instructions from the SNMP manager and also sends management information back to the SNMP manager as events occur.

## Configuring SNMP on the GSS

Before you use SNMP to monitor the GSS or GSSM, you must enable the SNMP agent on each GSS device. In addition to enabling the SNMP agent on the GSS device, you also specify an SNMP community name, name of the contact person, and the physical location for the GSS device.



### Note

Be aware that existing, pre-v2.0, SNMP community, contact, and location configurations are retained after a v2.0 software upgrade. For example, if you have configured a company contact in v1.3 and then upgrade to GSS v2.0, that contact will be retained after the v2.0 upgrade is completed.

Use the **snmp** command in global configuration mode to enable SNMP on your GSS device. To disable SNMP on the GSS, use the **no** form of this command.

To configure SNMP for a GSS device, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

2. Access global configuration mode.

```
gss1.example.com# config
gss1.example.com(config)#
```

3. Enable the SNMP agent by using the following command.

```
gss1.example.com(config)# snmp enable
```

**Note**

In the pre-v2.0 GSS software, a default community string is set to **public** after you enable SNMP. After a v2.0 software upgrade, however, no default community string is set when you enable SNMP.

You can add the **public** community string manually in the v2.0 software as explained in the steps that follow. Any community strings that you configured in the pre-v2.0 GSS software will be retained after a v2.0 software upgrade.

4. Specify an SNMP community name for this GSS device by using the **snmp community-string** command. Each GSS device then becomes part of the named community. To change the SNMP community string, enter an unquoted text string with no space and a maximum length of 32 characters.

When you configure a community-string, location, and SNMP contact, you have two different options available on the GSS. You can configure them by using either the pre-v2.0 software CLI or the new v2.0 software CLI:

- a. Using the pre-v2.0 CLI, configure a contact person for this GSS device with the **snmp contact** command. You can include information on how to contact a person; for example, a phone number or e-mail address. Enter an unquoted text string with a maximum of 255 characters including spaces.

```
gss-pilot1.cisco.com#  
gss-pilot1.cisco.com# conf  
gss-pilot1.cisco.com(config)# snmp contact  
Enter new Contact Info: Joe Smith jsmith@cisco.com  
gss-pilot1.cisco.com(config)#
```

- b. Using the v2.0 CLI, configure a contact for this GSS device with the **snmp-server contact** command. Enter an unquoted text string with a maximum of 255 characters without any spaces.

```
gss-pilot1.cisco.com#  
gss-pilot1.cisco.com# conf  
gss-pilot1.cisco.com(config)# snmp-server contact  
JoeSmith-jsmith@cisco.com  
gss-pilot1.cisco.com(config)#
```

5. Disable SNMP or any of the parameters outlined above by using the **no** form of the **snmp** command. For example, to disable the SNMP contacts for the GSS, enter:

```
gss1.example.com(config)# no snmp contact
```

# Configuring SNMP Servers

You can configure SNMP server information, locations, and names on your GSS device by using the **snmp-server** command in global configuration mode. To remove the server information, use the **no** form of this command.

To configure SNMP server information for a GSS device, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

2. Access global configuration mode.

```
gss1.example.com# config
gss1.example.com(config)#
```

3. Enable the SNMP agent by using the following command:

```
gss1.example.com(config)# snmp enable
```

4. Configure SNMP server information by using the following command:

```
gss1.example.com(config)# snmp-server
```

5. Specify an SNMP community name for this GSS device by using the **community** command and an unquoted text string with no spaces and a maximum of 32 characters.

```
gss1.example.com(config)# snmp-server community MyCommunity
```

6. Specify a location by using the **location** command and the *location* itself. The maximum length of the location is 255 characters.

```
gss1.example.com(config)# snmp-server location Boxborough
```

7. Disable the SNMP server or any of the parameters outlined here by using the **no** form of the **snmp-server** command. For example, to disable the SNMP location for the GSS, enter:

```
gss1.example.com(config)# no snmp-server community MyCommunity
```



# Configuring SNMP Server Notifications

You can enable traps on your GSS device by using the **snmp-server enable-traps** command in global configuration mode. To disable traps, use the **no** form of this command.

To configure SNMP server notifications for a GSS device, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

2. Access global configuration mode.

```
gss1.example.com# config
gss1.example.com(config)#
```

3. Enable the SNMP agent by using the following command:

```
gss1.example.com(config)# snmp enable
```

4. Enable SNMP server notifications by entering the **snmp-server enable-traps** command and following it with one of the available options:

- **gslb**—Enables all SNMP GSLB notifications.
- **gslb dns**—Enables SNMP DNS server notification.
- **gslb kal**—Enables SNMP GSLB keepalive notification.
- **gslb peer-status**—Enables SNMP GSLB peer-status change notification.
- **core**—Enables SNMP core-file discovery notification.
- **snmp**—Enables all SNMP agent notifications.
- **snmp authentication**—Enables only SNMP agent authentication notification.

```
gss1.example.com(config)# snmp-server enable-traps kal
```

5. Disable SNMP server notifications by using the **no** form of the **snmp-server enable-traps** command. For example, to disable SNMP GSLB keepalive notification, enter:

```
gss1.example.com(config)# no snmp-server enable-traps gslb kal
```

# Configuring SNMP Server Trap Limits

You can configure the maximum rate at which SNMP traps are set on your GSS device by using the **snmp-server trap-limit** command in global configuration mode. To set the default trap rate, use the **no** form of this command. The default is 25 traps per minute.

To configure SNMP server trap limits for a GSS device, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

2. Access global configuration mode.

```
gss1.example.com# config
gss1.example.com(config)#
```

3. Enable the SNMP agent by using the following command:

```
gss1.example.com(config)# snmp enable
```

4. Enable SNMP server trap limits by entering the **snmp-server trap-limit** command and following it with one of the available options and a specified value:

- **answer-trap *value***—Configures a rate-limit for the answer trap.
- **dns-clause-trap *value***—Configures the rate-limit for DNS clause traps.
- **keepalive-trap *value***—Configures the rate-limit for the keepalive trap.

```
gss1.example.com(config)# snmp-server trap-limit answer trap 10
```

5. Set the default trap rate by using the **no** form of the **snmp-server trap-limit** command as follows:

```
gss1.example.com(config)# no snmp-server trap-limit answer-trap
```

# Specifying Recipients for SNMP Notification Operations

You can specify the recipient of an SNMP notification operation by using the **snmp-server host** command in global configuration mode. To remove the specified host, use the **no** form of this command.

To specify the recipient of an SNMP notification operation, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

2. Access global configuration mode.

```
gss1.example.com# config
gss1.example.com(config)#
```

3. Enable the SNMP agent by entering the following command:

```
gss1.example.com(config)# snmp enable
```

4. Specify the recipients of SNMP notification operations by using the **snmp-server host** command and a *host-address* and a *community-string*.

```
gss1.example.com(config)# snmp-server host 10.1.1.1 MyCommunity
```

5. Send SNMP traps to the specified host by entering the following command:

```
gss1.example.com(config)# snmp-server host 10.1.1.1 MyCommunity
traps
```



## Note

You can configure a maximum of 10 hosts for traps notification.

6. Specify the version of the SNMP protocol used to send the traps by entering the **version** command and one of the available keywords:

- 1—Specifies SNMPv1 (the default).
- 2—Specifies SNMPv2c.

```
gss1.example.com(config)# snmp-server host 10.1.1.1 MyCommunity
traps version 2
```

7. Specify the host UDP port to use by entering the **udp-port** command and the port number.

```
gss1.example.com(config)# snmp-server host 10.1.1.1 MyCommunity
traps version 2 udp-port 500
```

8. Remove the recipient of an SNMP notification by using the **no** form of the **snmp-server host** command. For example, to disable all SNMP notifications for sample IP address 10.1.1.1, UDP port 100, enter:

```
gss1.example.com(config)# no snmp-server host 10.1.1.1 MyCommunity
traps version 2 udp-port 100
```

## Viewing SNMP Status

Once SNMP is enabled, you can display the SNMP status on your GSS device by using the **show snmp** command. Verify that your SNMP agent, ucd-snmp v4.2.3, is enabled or disabled, as well as the configured names of the community-string, location, and contact.



### Note

You can also use the **show services** command to verify if SNMP is enabled or disabled.

For example, enter:

```
gss1.example.com# show snmp
SNMP is enabled
sys contact: JSmith jsmith@cisco.com
sys location: Boxborough

0 SNMP packets input
    0 Bad SNMP versions
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
```

```

0 General errors

Community
-----
public

Host                               Port Version  Type
----
16.1.1.11                          162  v2c        trap

Trap type      Enabled
-----
GSLB KAL transitionYes
GSLB system core file discoveryYes
GSLB system peer transitionYes
SNMP authenticationYes
gss1.example.com#

```

See the “[Configuring SNMP on the GSS](#)” section to change the status of your SNMP agent running on the GSS device.

## Viewing MIB Files on the GSS

You can view the MIB files contained in the /mibs directory on the GSS by using the **dir** command. If you want to copy the MIB files from the /mibs directory on the GSS to another location on the GSS or to a remote network location, use the **ftp** or **scp** command.

For example, enter:

```

gss1.example.com# dir /mibs
total 1100
drwxr-xr-x   2 root   root   4096 Jul 18 08:45 .
drwxrwxrwx  19 root   root   4096 Jul 18 08:46 ..
-rw-r--r--   1 root   root  17455 Jul 18 08:45 AGENTX-MIB.txt
-rw-r--r--   1 root   root  19850 Jul 18 08:45 DISMAN-SCHEDULE-MIB.txt
-rw-r--r--   1 root   root  64311 Jul 18 08:45 DISMAN-SCRIPT-MIB.txt
-rw-r--r--   1 root   root  50054 Jul 18 08:45 EtherLike-MIB.txt
-rw-r--r--   1 root   root   4660 Jul 18 08:45 HCNUM-TC.txt
-rw-r--r--   1 root   root  52544 Jul 18 08:45 HOST-RESOURCES-MIB.txt
-rw-r--r--   1 root   root  10583 Jul 18 08:45 HOST-RESOURCES-TYPES.txt
-rw-r--r--   1 root   root   4015 Jul 18 08:45
IANA-ADDRESS-FAMILY-NUMBERS-MIB.txt
-rw-r--r--   1 root   root   4299 Jul 18 08:45 IANA-LANGUAGE-MIB.txt
-rw-r--r--   1 root   root  15661 Jul 18 08:45 IANAifType-MIB.txt
-rw-r--r--   1 root   root   5066 Jul 18 08:45 IF-INVERTED-STACK-MIB.txt
-rw-r--r--   1 root   root  71691 Jul 18 08:45 IF-MIB.txt

```

## Viewing MIB Files on the GSS

```

-rw-r--r-- 1 root root 6260 Jul 18 08:45 INET-ADDRESS-MIB.txt
-rw-r--r-- 1 root root 26781 Jul 18 08:45 IP-FORWARD-MIB.txt
-rw-r--r-- 1 root root 23499 Jul 18 08:45 IP-MIB.txt
-rw-r--r-- 1 root root 15936 Jul 18 08:45 IPV6-ICMP-MIB.txt
-rw-r--r-- 1 root root 48703 Jul 18 08:45 IPV6-MIB.txt
-rw-r--r-- 1 root root 2367 Jul 18 08:45 IPV6-TC.txt
-rw-r--r-- 1 root root 7257 Jul 18 08:45 IPV6-TCP-MIB.txt
-rw-r--r-- 1 root root 4400 Jul 18 08:45 IPV6-UDP-MIB.txt
-rw-r--r-- 1 root root 1174 Jul 18 08:45 RFC-1215.txt
-rw-r--r-- 1 root root 3067 Jul 18 08:45 RFC1155-SMI.txt
-rw-r--r-- 1 root root 79667 Jul 18 08:45 RFC1213-MIB.txt
-rw-r--r-- 1 root root 147822 Jul 18 08:45 RMON-MIB.txt
-rw-r--r-- 1 root root 4628 Jul 18 08:45 SMUX-MIB.txt
-rw-r--r-- 1 root root 15490 Jul 18 08:45 SNMP-COMMUNITY-MIB.txt
-rw-r--r-- 1 root root 20750 Jul 18 08:45 SNMP-FRAMEWORK-MIB.txt
-rw-r--r-- 1 root root 5261 Jul 18 08:45 SNMP-MPD-MIB.txt
-rw-r--r-- 1 root root 19083 Jul 18 08:45 SNMP-NOTIFICATION-MIB.txt
-rw-r--r-- 1 root root 8434 Jul 18 08:45 SNMP-PROXY-MIB.txt
-rw-r--r-- 1 root root 21495 Jul 18 08:45 SNMP-TARGET-MIB.txt
-rw-r--r-- 1 root root 38035 Jul 18 08:45 SNMP-USER-BASED-SM-MIB.txt
-rw-r--r-- 1 root root 33430 Jul 18 08:45 SNMP-VIEW-BASED-ACM-MIB.txt
-rw-r--r-- 1 root root 8263 Jul 18 08:45 SNMPv2-CONF.txt
-rw-r--r-- 1 root root 25052 Jul 18 08:45 SNMPv2-MIB.txt
-rw-r--r-- 1 root root 8924 Jul 18 08:45 SNMPv2-SMI.txt
-rw-r--r-- 1 root root 38034 Jul 18 08:45 SNMPv2-TC.txt
-rw-r--r-- 1 root root 3981 Jul 18 08:45 SNMPv2-TM.txt
-rw-r--r-- 1 root root 10765 Jul 18 08:45 TCP-MIB.txt
-rw-r--r-- 1 root root 2058 Jul 18 08:45 UCD-DEMO-MIB.txt
-rw-r--r-- 1 root root 3131 Jul 18 08:45 UCD-DISKIO-MIB.txt
-rw-r--r-- 1 root root 2928 Jul 18 08:45 UCD-DLMOD-MIB.txt
-rw-r--r-- 1 root root 8037 Jul 18 08:45 UCD-IPFWACC-MIB.txt
-rw-r--r-- 1 root root 30343 Jul 18 08:45 UCD-SNMP-MIB.txt
-rw-r--r-- 1 root root 4076 Jul 18 08:45 UDP-MIB.txt

```



# CHAPTER 7

## Backing Up, Restoring, and Downgrading the GSSM Database

---

This chapter describes how to back up and restore the primary GSSM database. It also describes how to downgrade to an earlier version of the GSS software on your GSSs and GSSMs and restore the software if you encounter problems with a GSS software upgrade.

It contains the following major sections:

- [Backing Up the Primary GSSM](#)
- [Restoring a Primary GSSM Backup](#)
- [Downgrading Your GSS Devices](#)

# Backing Up the Primary GSSM

This section describes the procedure to perform a full backup of the primary GSSM database. It contains the following topics:

- [Backup Overview](#)
- [Performing a Full Primary GSSM Backup](#)

## Backup Overview

The GSSM database maintains all network and device configuration information, as well the DNS rules used by the GSS devices to route DNS queries from users to available hosts.

**Note**

You should perform frequent backups of your primary GSSM and its database to ensure that if a sudden and unexpected power loss or media failure occurs, your GSSM configuration and database will survive, and your GSSM can be quickly restored.

We recommend that you perform a backup of your primary GSSM:

- Before you switch GSSM roles and before you make the standby GSSM the primary GSSM on your network
- Before you perform a GSS software upgrade
- After you make any changes in the device or network configuration of your GSSM

The GSS software performs a full backup of the GSSM network configuration settings as well as the GSSM database that contains global server load-balancing configuration information. A full backup of the primary GSSM allows you to pick and choose the specific GSSM configuration information that you want to later restore on the primary GSSM.

Whenever you execute a backup on your primary GSSM, the GSS software automatically creates a tar archive (“tarball”) of the necessary files. A tar archive is a group of files collected together as a single file. This file has the .full extension.



When you execute a database restore on your primary GSSM, the archive file is automatically unpacked and the database is copied to the GSSM, overwriting the current GSSM database.

Backing up your GSSM database requires that you access the GSS CLI and then complete the following actions:

1. Determine the appropriate time to back up your GSSM
2. Perform the backup
3. Move the backup file to a secure location on your network

## Performing a Full Primary GSSM Backup

You can perform a full primary GSSM backup at any time. Performing a backup requires access to the CLI of the primary GSSM.

To perform a full backup of your primary GSSM, perform the following steps:

1. Log in to the primary GSSM CLI and enable privileged EXEC mode.

```
gssm1.example.com> enable
gssm1.example.com#
```

2. Copy the current primary GSSM startup configuration to a file for use on other devices or for backup purposes by using the **copy startup-config disk** command. The *filename* argument specifies the name of the file containing the startup configuration settings.

```
gssm1.example.com# copy startup-config disk newstartupconfig
```



### Note

The primary GSSM backup does not include user files that reside in the /home directory. If you have important files in the /home directory that you want to save, such as the startup-configuration file, use either the secure copy (**scp**) or **ftp** commands to copy those files to another device. Storing the startup-configuration file in a safe location can save time and reconfiguration issues in a recovery situation.

3. Create a full backup of your primary GSSM by using the **gssm backup full** command. The **gssm backup full** command performs a backup of both the database component of the GSSM and its network and device configuration information. Supply a filename for your backup.

```
gssm1.example.com# gssm backup full gssmfullbk
GSSM database backup succeeded [gssmfullbk.full]
```

4. After you receive confirmation that the primary GSSM successfully created your full backup, copy or move the backup file off the device to ensure that the backup is not lost if a problem occurs on your primary GSSM.

Use either the secure copy (**scp**) or **ftp** command to copy or move your full backup to a remote host.

```
gssm1.example.com# scp gssfullbk.full server.example.com:~/
```

## Restoring a Primary GSSM Backup

This section describes how to restore a backup of the primary GSSM database. It contains the following topics:

- [Restore Overview](#)
- [Restoring Your Primary GSSM from a Previous Backup](#)

## Restore Overview

You may need to restore a previous primary GSSM backup for the following reasons:

- You have replaced your primary GSSM with a new device and want to restore a previous backup to that primary GSSM.
- You are downgrading the GSS software to an earlier release.
- You have made a number of configuration changes to the primary GSSM and would like to return to the previous backup of the GSSM.

When you execute a database restore on your primary GSSM, the archive file is automatically unpacked and the database is copied to the GSSM, overwriting the current GSSM database. See the “[Backing Up the Primary GSSM](#)” section for details about performing a database backup of the GSSM.

The GSS database may change between software versions. When you downgrade to an earlier version of the GSSM database, any configuration changes, device configuration information, and DNS rules entered through the primary GSSM (subsequent to your last software upgrade) will be lost.

## Restoring Your Primary GSSM from a Previous Backup

When restoring the primary GSSM from a previous backup, use the last backup to restore the GSS device network configuration settings as well as the encryption keys used to communicate with other GSS devices. Restoring the primary GSSM from a backup returns the device to its exact configuration as of the last backup.

To restore an earlier version of the primary GSSM from a previous backup, perform the following steps:

1. Log in to the primary GSSM CLI and enable privileged EXEC mode.

```
gssm1.example.com> enable
gssm1.example.com#
```

2. Verify that your previous backup of the primary GSSM is in a location that is accessible from the GSSM being restored. Previous backups have a .full file extension. For details about locating files in a GSS directory, see the [“Managing GSS Files”](#) section in [Chapter 2, Managing the GSS from the CLI](#).

1. Stop the GSS software on the primary GSSM, and then use the **gss status** command to confirm that the primary GSSM has stopped.

```
atcr1.cisco.com# gss stop
atcr1.cisco.com# gss status
Cisco GSS - 1.3(1.0.0) - [Wed Feb 15 11:33:47 UTC 2006]

gss is not running.
```

2. After the GSSM software stops, restore the GSSM from the backup file by using the **gssm restore** command. For example, to restore the file *gssmfullbk.full*, enter:

```
gss1.example.com# gssm restore gssmfullbk.full
```

3. Confirm your decision to overwrite existing GSS system configuration information on the GSSM and restart the GSSM device. Enter **y** for yes (or **n** to stop the restore process).

```
% WARNING WARNING WARNING
You will be asked which portion(s) of the system configuration to
overwrite. You may want to create a database backup before
proceeding.
```

```
Are you sure you wish to continue? (y/n): y
Backup file is valid. Timestamp = 2003-Sep-15-14:01:53
```

4. Confirm your decision to restore primary GSSM platform information or only the GSS database by performing one of the following actions:
  - Type **y** to restore GSSM platform information.



**Note** Restoring platform information requires a reboot of the GSS at the end of the restore procedure.

- Type **n** to restore only the primary GSSM database and not the GSSM platform information. If you choose not to restore GSSM platform information, reconfigure the GSSM platform information from the CLI. See the *Cisco Global Site Selector Getting Started Guide* for details.

This backup contains a backup of the platform configuration. 'n' restores just the database. Restoring platform files requires a reboot.

Restore Platform files? [y/n]: **y**

Your selection enables you to return the primary GSSM to its original state prior to the database backup. Platform information includes all configuration parameters set at the CLI, including: interface configuration, hostname, service settings (NTP, SSH, Telnet, FTP, and SNMP), time zone, logging levels, web certificates, inter-GSS communication certificates, access lists and access groups, CLI user information, GUI user information, and property-set CLI commands.

5. Confirm your decision to restore the GSS network information for remote devices activated from the primary GSSM by performing one of the following actions:
  - Type **y** to restore the GSS network information.

Network information includes registered GSS devices, GSS device status, node information, and IP addresses. This network information is displayed in the GSS list table in the Resources tab. GSS network information does not include DNS rules, answers, and keepalives. Those configuration elements are automatically restored as part of the database restore process.

If you type **y** to restore the GSS network information and your configuration includes a standby GSSM, you must reenabling the standby GSSM and then reregister it with the primary GSSM. See the *Cisco Global Site Selector Getting Started Guide* for details.

- Type **n** to instruct the software not to restore GSS network information to the GSSM. If you choose not to restore the GSS network information, you must reenoble each device, then reregister the device with the primary GSSM. See the *Cisco Global Site Selector Getting Started Guide* for details.



**Note** Disabling and enabling each device, then reregistering the device with the primary GSSM, may result in a temporary network service outage.

Do you want to replace your current GSS network configuration with the one specified in the backup file? (y/n): **y**

The GSSM continues with the restore process.

```
Deleting existing database...
Creating empty database for restore...
Restoring the database...
Using GSS network information present in backup file...
Restoring platform backup files.
Database restored successfully.
Reboot Device now? (y/n): y
```

If you choose to reboot the device, the primary GSSM reboots.

6. Confirm that the primary GSSM is up and running in normal operation mode (runmode = 5), by using the **gss status** command.

After you restore a backup file in which you did not preserve the GSS network information, note the following configuration changes in the primary GSSM GUI:

- All previous associations established between a GSS device and a location are removed. When you access the Modifying GSS details page (Resources tab) of the primary GSSM GUI, each GSS location is set to Unspecified. If necessary, reestablish the association between a GSS device and location on the Modifying GSS details page as described in the *Cisco Global Site Selector Administration Guide*.
- For a DNS sticky configuration, all favored peer associations established between a local GSS node and a remote GSS peer are removed. When you access the Global Sticky Configuration details page (Traffic Mgmt tab) of the primary GSSM GUI, each local GSS node favored peer is set to Unspecified. If necessary, reestablish the association between each local GSS node and its favored peer as described in the *Cisco Global Site Selector Global Server Load-Balancing Configuration Guide*.

# Downgrading Your GSS Devices

If you encounter problems with a GSS software upgrade, restore an earlier version of the GSS software on your GSSs and GSSMs. To restore an earlier version of your software, you must have a previous backup of the primary GSSM database that corresponds to the current version of the GSS software. For example, if you want to downgrade from GSS software Release 1.2 to GSS software Release 1.1, you must have a GSS software Release 1.1 database backup that you can restore. Your GSS software Release 1.2 database cannot run on the Release 1.1 platform because of changes in the database schema between releases.

When downgrading the GSS software, use the following order of operations to protect your critical GSS data and properly restore your GSSM database:

1. Verify the GSSM role in the GSS network.
2. Perform a backup of your primary GSSM that contains the more recent version of the GSS software.
3. Obtain an earlier software (.upg) file.
4. Downgrade your GSS device.
5. Restore your GSSM database backup that corresponds to the downgraded version of the GSS software.

Do not attempt to restore an earlier version of the GSS software than the earliest GSSM database backup that you have available. For example, if the earliest version of the GSS software in your possession is Release 1.1, and your earliest GSSM database backup is for Release 1.1, do not downgrade to a release of GSS software earlier than Release 1.1.

To restore an earlier version of your GSS software, perform the following steps:

1. Verify that the roles of the designated primary and standby GSSMs have not changed. The changing of roles between the designated primary GSSM and the standby GSSM is intended to be a temporary GSS network configuration until the original primary GSSM is back online. See the [“Verifying the GSSM Role in the GSS Network”](#) section of [Appendix A, Upgrading the GSS Software](#).
2. Perform a backup of your primary GSSM as described in the [“Performing a Full Primary GSSM Backup”](#) section.
3. Obtain an earlier software version as described in the [“Obtaining the Software Upgrade”](#) section of [Appendix A, Upgrading the GSS Software](#).

4. Install the earlier software version as described in the “[Upgrading Your GSS Devices](#)” section of [Appendix A, Upgrading the GSS Software](#).
5. After you downgrade the software on your primary GSSM, see the “[Restoring Your Primary GSSM from a Previous Backup](#)” section. Restore the GSSM database backup that was previously saved from the downgraded GSS software release.







# CHAPTER 8

## Viewing Log Files

---

This chapter describes how to store and view logged information about your GSS devices. Each GSS device contains a number of log files that retain records of specified GSS-related activities and the performance of various GSS subsystems. You can access these log files using the CLI to troubleshoot problems or to better understand the behavior of a GSS device.

This chapter contains the following major sections:

- [Understanding GSS Logging Levels](#)
- [Configuring System Logging for a GSS](#)
- [Viewing Device Logs from the CLI](#)
- [Viewing System Logs from the Primary GSSM GUI](#)
- [Viewing GSS System Logs Using CiscoWorks RME Syslog Analyzer](#)

## Understanding GSS Logging Levels

The GSS generates log messages to assist you with debugging and monitoring operations. The GSS maintains logged records for a wide range of GSS network activity in the gss.log file as well as through the system logs feature of the GSSM.

The subsystem log messages are subsystem events that occur during the operation of the GSS. The GSS saves these messages in the system.log file. The GSS determines which subsystem messages to log by its configured logging level. The logging level designates the GSS log emergency, alert, critical, error, and warning messages for the subsystem. The GSS also logs notification, informational, and debugging messages.

The GSS supports eight separate logging levels to identify the wide range of critical and noncritical logged events that may occur on a GSS device. [Table 8-1](#) describes the different logging levels. [Table 8-2](#) lists GSS subsystems for which you can enable logging.

**Table 8-1 GSS Logging Levels**

Level Number	Level Name	Description
0	Emergencies	The GSS has become unusable. For example, the GSS has shut down and cannot be restarted, or it has experienced a hardware failure.
1	Alerts	The GSS requires immediate attention. For example, one of the GSS subsystems is not running.
2	Critical	The GSS encountered a critical condition that requires attention. For example, a GSS device cannot connect to the primary GSSM and does not have a local configuration snapshot to use.
3	Errors	The GSS encountered an error condition that requires prompt attention but can still function. For example, a GSS device is out of available memory.
4	Warnings	The GSS encountered an error condition that requires attention but is not interfering with the operation of the device. For example, a GSS has lost contact with the primary GSSM but a local configuration snapshot exists.
5	Notifications	The GSS encountered a nonerror condition that should be brought to the administrator's attention. For example, a GSS software upgrade is required.

**Table 8-1 GSS Logging Levels (continued)**

Level Number	Level Name	Description
6	Information	Messages at this level are normal operational messages for the GSS device, such as status or configuration changes.
7	Debug	Messages at this level (such as detailed information about DNS request or keepalive handling and specific code path tracking) are intended for use by technical support personnel.

**Table 8-2 Logging Subsystems**

Subsystem	Definition
<b>boomerang</b>	Boomerang logging messages
<b>crdirector</b>	CrDirector logging messages
<b>crm</b>	GSSM logging messages
<b>ddos</b>	Distributed Denial of Service (DDoS) prevention module logging messages.
<b>dnsserver</b>	Domain Name System (DNS) logging messages
<b>drpagent</b>	Director Response Protocol (DRP) agent logging messages
<b>keepalive</b>	Keepalive Engine logging messages
<b>nodemgr</b>	Node manager logging messages
<b>proximity</b>	Proximity logging messages
<b>sticky</b>	Sticky manager logging message
<b>system</b>	System logging messages
<b>tacacs</b>	TACACS+ logging messages

# Configuring System Logging for a GSS

By default, the GSS maintains system logged records in the `gss.log` file on the hard disk. You can change the location to log files to a remote host machine. You can make global decisions about what level of GSS logging to use, or instead make those decisions on a subsystem-by-subsystem basis. For example, you can configure the primary GSSM to log all error-level messages, but also configure the node manager (`nodemgr`) to log a larger set of all notice-level messages.

Set specific parameters for the GSS system log file by using the **logging** command. To disable logging functions, use the **no** form of this command.

The default logging settings are as follows:

- Logging to disk: Enabled
- Priority of message for disk: 5
- Priority of message for host: 4
- Log filename: `/home/gss.log`
- Log file recycle size: 10 MB
- Maximum number of log files: 25



## Note

In rare instances when a GSS runs out of user disk space, the device will stop logging messages to all log files. Logging does not automatically resume after you free up disk space on the GSS. This behavior may occur when you use FTP to transfer a significant number of files to the GSS, thus completely filling the available GSS disk space. Correct this problem by using **rotate-logs** CLI command to replace the log files and resume logging (see the [“Rotating Existing Log Files from the CLI”](#) section).

This section contains the following topics:

- [Specifying a Log File on the GSS Disk](#)
- [Specifying a Host for a Log File Destination](#)
- [Specifying a Syslog Facility](#)

## Specifying a Log File on the GSS Disk

You can send log information to the `gss.log` file on the GSS hard disk by using the **logging disk** command. By default, logging to disk is enabled.

The syntax for the command is as follows:

```
logging disk {enable | priority loglevel | subsystem name priority loglevel}
```

The keywords and arguments are as follows:

- **enable**—Enables logging to disk.
- **priority**—Sets the priority level of the messages to log to disk.
- *loglevel*—Threshold that system messages must meet to be logged. Messages with lower priorities than the specified log level cannot be logged. Use one of the following keywords to select the logging level, listed in order of priority:
  - **emergencies**—The GSS is unusable (Priority 0)
  - **alerts**—Immediate action needed (Priority 1)
  - **critical**—Immediate action needed (Priority 2)
  - **errors**—Error conditions (Priority 3)
  - **warnings**—Warning conditions (Priority 4)
  - **notifications**—Normal but significant conditions (Priority 5)
  - **informational**—Informational messages (Priority 6)
  - **debugging**—Debugging messages (Priority 7)
- **subsystem**—Sets the log for a named GSS subsystem. Each subsystem can have a different log level applied for its messages.
- *name*—Name of the GSS subsystem. Use one of the following keywords to select a subsystem:
  - **boomerang**—Boomerang logging messages
  - **crdirector**—CrDirector logging messages
  - **crm**—GSSM logging messages
  - **ddos**—Distributed Denial of Service (DDos) prevention module logging messages
  - **dnserver**—Domain Name System (DNS) logging messages

- **drpagent**—Director Response Protocol (DRP) agent logging messages
- **keepalive**—Keepalive Engine logging messages
- **nodemgr**—Node manager logging messages
- **proximity**—Proximity logging messages
- **sticky**—Sticky manager logging message
- **system**—System logging messages
- **tacacs**—TACACS+ logging messages

For example, to enable logging to disk and to set the priority level for error conditions, enter:

```
gssm1.example.com(config)# logging disk enable
gssm1.example.com(config)# logging disk priority error
```

For example, to enable logging to disk, set the log for CrDirector subsystem logging messages, and set the priority level to informational messages, enter:

```
gssm1.example.com(config)# logging disk enable
gssm1.example.com(config)# logging disk subsystem crdirector
gssm1.example.com(config)# logging disk priority information
```

To stop logging to GSS disk, enter:

```
gssm1.example.com(config)# no logging disk enable
```

## Specifying a Host for a Log File Destination

You can set logging to the IP address of a remote host by using the **logging host** command. By default, logging to host is disabled.

The syntax for this command is as follows:

```
logging host {enable | ip ip_address | priority loglevel | subsystem name
priority loglevel}
```

The keywords and arguments are as follows:

- **enable**—Enables logging to host.
- **ip**—Sets the remote host (or hosts) that are to receive the GSS log files.
- *ip\_address*—Address (or addresses) of the remote logging hosts.

- **priority**—Sets the priority level of the messages to log to the host.
- **loglevel**—Threshold that system messages must meet to be logged. Messages with lower priorities than the specified log level cannot be logged. Use one of the following keywords to select the logging level, listed in order of priority:
  - **emergencies**—The GSS is unusable (Priority 0)
  - **alerts**—Immediate action needed (Priority 1)
  - **critical**—Immediate action needed (Priority 2)
  - **errors**—Error conditions (Priority 3)
  - **warnings**—Warning conditions (Priority 4)
  - **notifications**—Normal but significant conditions (Priority 5)
  - **informational**—Informational messages (Priority 6)
  - **debugging**—Debugging messages (Priority 7)
- **subsystem**—Sets the log for a named GSS subsystem. Each subsystem can have a different log level applied for its messages.
- **name**—Name of the GSS subsystem. Use one of the following keywords to select a subsystem:
  - **boomerang**—Boomerang logging messages
  - **crdirector**—CrDirector logging messages
  - **crm**—GSSM logging messages
  - **dnsserver**—Domain Name System (DNS) logging messages
  - **drpagent**—Director Response Protocol (DRP) agent logging messages
  - **keepalive**—Keepalive Engine logging messages
  - **nodemgr**—Node manager logging messages
  - **proximity**—Proximity logging messages
  - **sticky**—Sticky manager logging message
  - **system**—System logging messages
  - **tacacs**—TACACS+ logging messages

For example, to enable logging to a remote host and to set the priority level for notifications, enter:

```
gssm1.example.com(config)# logging host enable
gssm1.example.com(config)# logging host ip 172.16.2.3
```

```
gssm1.example.com(config)# logging host priority notifications
```

For example, to enable logging to a remote host, to set the log for the Keepalive Engine subsystem logging messages, and to set the priority level to error messages, enter:

```
gssm1.example.com(config)# logging host enable
gssm1.example.com(config)# logging host ip 172.16.2.3
gssm1.example.com(config)# logging host subsystem kale
gssm1.example.com(config)# logging host priority error
```

To stop logging to GSS disk, enter:

```
gssm1.example.com(config)# no logging host
```

## Specifying a Syslog Facility

You can specify a syslog facility type to identify the behavior of the syslog daemon (syslogd) on the host by using the **logging facility** command in global configuration mode. The syslog daemon on the host uses the specified facility type to determine how to process messages.



### Note

---

For more information on the syslog daemon and facility levels, refer to your syslog daemon documentation.

---

The syntax for this command is as follows:

**logging facility** *type*

The *type* argument specifies the syslog facility type. The default facility type is local5. The GSS supports the following types:

- **auth**—Authorization system
- **daemon**—System daemon
- **kernal**—Kernel
- **local0**—Reserved for locally defined messages
- **local1**—Reserved for locally defined messages
- **local2**—Reserved for locally defined messages
- **local3**—Reserved for locally defined messages



- **local4**—Reserved for locally defined messages
- **local5**—Reserved for locally defined messages
- **local6**—Reserved for locally defined messages
- **local7**—Reserved for locally defined messages
- **mail**—Mail system
- **news**—USENET news
- **syslog**—System log
- **user**—User process
- **uucp**—UNIX-to-UNIX copy system

For example, to change the logging facility to local7, enter:

```
gssm1.example.com(config)# logging facility local7
```

To change the logging facility to back to the default of local5, enter:

```
gssm1.example.com(config)# no logging facility local7
```

## Viewing Device Logs from the CLI

Each GSS device contains a number of log files that retain records of both GSS-related activity as well as the performance of the various GSS subsystems. Access these log files from the CLI to troubleshoot problems or understand the behavior of a GSS device.

This section contains the following topics:

- [Viewing the gss.log File from the CLI](#)
- [Viewing System Message Logging](#)
- [Viewing Subsystem Log Files from the CLI](#)
- [Rotating Existing Log Files from the CLI](#)

## Viewing the gss.log File from the CLI

The gss.log file groups useful information for a GSS device, such as the keepalive, availability and load statistics. Use the **show logs** command to view this log file from the CLI.



### Note

The **show logs** command shows all logged information in your terminal session. This output may be quite large and can exceed the buffer size set for the terminal. If you want to capture all logged information, use the **terminal-length** CLI command to adjust the size of your screen buffer (see the “[Configuring the Terminal Screen Line Length](#)” section in [Chapter 2, Managing the GSS from the CLI](#)). Otherwise, use the **tail** or **follow** options as described in this section to limit the output of the file.

The syntax for this command is as follows:

```
show logs { follow | tail }
```

The keywords are as follows:

- **follow**—Displays the log file as data that is appended to it.
- **tail**—Displays only the last ten lines of the log file.

To limit the output of the **show logs** command, specify one of the following:

- Use the **tail** option of the **show logs** command to view only the last ten lines of logged information.

```
gssml.example.com# show logs tail
```

- Use the **follow** option of the **show logs** command to view data appended to the end of the log as it grows.

```
gssml.example.com# show logs follow
```

To show all logged information, enter:

```
gssml.example.com# show logs
gss.log
Jul 14 21:42:01 gss-css2 KAL-7-KALAP[1240] KAL-AP (seq# 29410)=> Host
192.10.2.1
Jul 14 21:42:02 gss-css2 KAL-7-KALAP[1240] KAL-AP (seq# 29412)=> Host
192.10.4.1
```

```
Jul 14 21:42:02 gss-css2 KAL-7-KALAP[1240] Retrying IP [192.10.4.1]
(Retry Count 3)
Jul 14 21:42:07 gss-css2 KAL-7-KALAP[1240] Timeout: Found outstanding
KAL [192.10.2.1]
Jul 14 21:42:07 gss-css2 KAL-7-KALAP[1240] KAL-AP (seq# 29411)=> Host
192.10.2.1
Jul 14 21:42:07 gss-css2 KAL-7-KALAP[1240] Retrying IP [192.10.2.1]
(Retry Count 1)
Jul 14 21:42:09 gss-css2 KAL-7-KALCRA[1240] rtt_task: waiting 10000
mseconds
Jul 14 21:42:12 gss-css2 KAL-7-KALAP[1240] KAL-AP (seq# 29412)=> Host
192.10.2.1
Jul 14 21:42:12 gss-css2 KAL-7-KALAP[1240] Retrying IP [192.10.2.1]
(Retry Count 2)
Jul 14 21:42:16 gss-css2 KAL-7-KALAP[1240] Sending circuit keepalive
=> [192.10.2.1]
...
```

## Viewing System Message Logging

You can display the system message log configuration for a GSS device by using the **show logging** command.

For example, enter:

```
gssml.example.com# show logging
Logging to disk is enabled.
Priority for disk logging is Informational(6).

Logging to host is disabled.
Priority for host logging is Warning(4).
```

## Viewing Subsystem Log Files from the CLI

In addition to the gss.log file, each GSS device maintains a number of other log files that record GSS subsystem-specific information (for example, the keepalive engine or DNS server component of the GSS). You can view these log files from the CLI using the **type** command.



### Note

The **type** command lists all logged subsystem information in your terminal session. This output may be quite large and may exceed the buffer size set for the terminal. If you want to capture all logged information, use the **terminal-length**

CLI command to adjust the size of your screen buffer (see the “[Configuring the Terminal Screen Line Length](#)” section in [Chapter 2, Managing the GSS from the CLI](#)). Otherwise, use the **show logs tail** or **follow** options as described in this section to limit the output of the file.

---

To view your GSS subsystem log files, perform the following steps:

1. Navigate to the directory containing the log file or files that you want to view.

```
gssml.example.com> cd ../sysout
```

2. Display the contents of the log file by entering the following command:

```
gssml.example.com> type dnsserver.log
dnsserver.log
Starting dnsserver: Mon Jul 1 13:52:50 UTC 2003 [(1221)]
2003-07-10 16:23:08 relog: Booting...
Starting dnsserver: Wed Jul 10 16:23:33 UTC 2003 [(1201)]
End of file dnsserver.log
]
```

3. View only the last ten lines of the log file by using the following command:

```
gssml.example.com# tail dnsserver.log
```

## Rotating Existing Log Files from the CLI

You can instruct the GSS to save archive copies of all existing log files in the \$STATE directory and subdirectories and replace them with fresh log files. To force the GSS to restart its log files and save archive copies of all existing log files, use the **rotate-logs** command.



### Note

In rare instances when a GSS runs out of user disk space, the device will stop logging messages to all log files. Logging does not automatically resume after you free up disk space on the GSS. This behavior may occur when you use FTP to transfer a large number of files to the GSS, thus completely filling the available GSS disk space. Correct this problem by using the **rotate-logs** CLI command to replace the log files and resume logging.

---

The syntax for this command is as follows:

```
rotate-logs {delete-rotated-logs}
```

If you want to delete all rotated log files from the / directory and its subdirectories on the GSS disk, use the **delete-rotated-logs** keyword. The GSS does not delete active log files.

The GSS archives existing log files locally using the following naming convention:

*logfile\_name.log.number*

where:

- *logfile\_name.log*—Name of the archived log file (for example, gss.log or kale.log).
- *number*—Incremented number that represents the number of times that the logs have been rotated (for example, .3). The number of the most recent rotated log file is .1. The maximum number of log files is 25 for the gss.log file; five for all other log files.

To rotate existing log files:

```
gssm1.example.com# rotate-logs
```

To clear all rotated log files in the \$STATE directory and subdirectories, except for the active log files, enter:

```
gssm1.example.com# rotate-logs delete-rotated-logs
```

## Viewing System Logs from the Primary GSSM GUI

From the primary GSSM GUI, you can view messages logged in the GSS system.log file. The system.log file presents the logged information of interest to GSS administrators, such as the severity of the message, a brief description of the problem, and any relevant conditions encountered while the message was logged. The system.log file, however, presents only a subset of all logged information. For information about viewing the entire contents of the individual GSS log file, see the “[Viewing System Message Logging](#)” section.

This section contains the following topics:

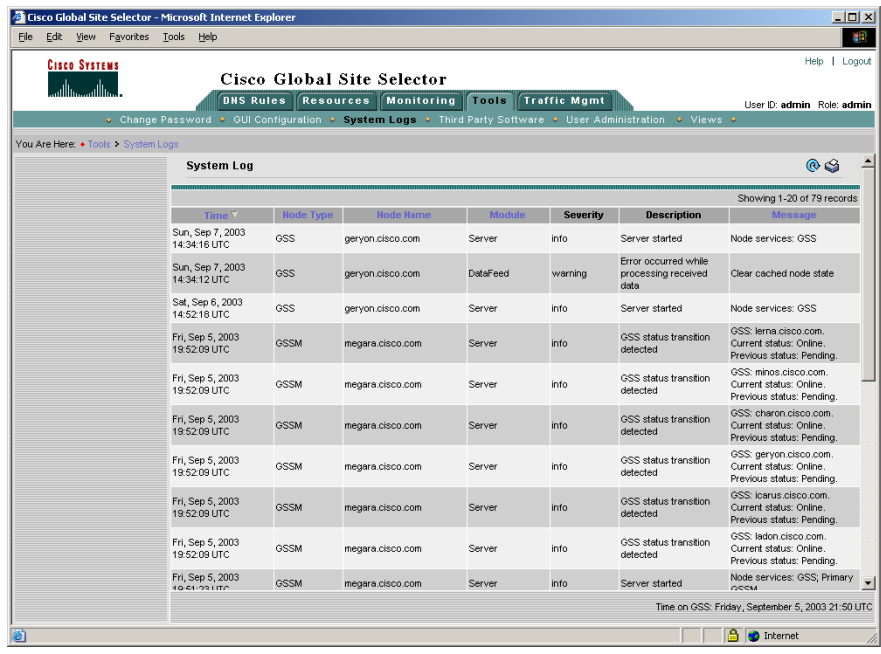
- [Viewing System Logs from the Primary GSSM GUI](#)
- [Purging System Log Messages from the GUI](#)
- [Common System Log Messages](#)

# Viewing System Logs from the Primary GSSM GUI

To view the GSS system logs, perform the following steps:

- 1. From the primary GSSM GUI, click the **Tools** tab.
- 2. Click the **System Logs** option. The System Log list page appears (see [Figure 8-1](#)) displaying system log information.

Figure 8-1 System Log List Page



System log information includes:

- Time—Time in Universal Coordinated Time (UTC) at which the logged event occurred on the GSS device.
- Node type—Type of GSS node (GSS or GSSM) on which the logged event occurred.
- Node name—Name assigned to the GSS device using the primary GSSM.

- **Module**—GSS component that logs the message (for example, server or storeAdmin).
  - **Severity**—Severity of the logged message. The GSS rates system log messages using one of the following four severity levels:
    - **Fatal**—A failure in the GSS or one of its components. Fatal errors are rare and are usually caused by exceptions from which it is impossible to recover, or by the failure of a GSS component to initialize properly.
    - **Warning**—A noncritical error or unexpected condition.
    - **Info**—Information about the normal operation of the GSS and its components.
    - **Debug**—Detailed information about the internal operations of the GSS or one of its components. Debug log messages are intended for use by Cisco support engineers to troubleshoot a problem.
  - **Description**—Text description that explains the event.
  - **Message**—Information about any relevant conditions encountered while the event was being logged.
3. Click the column header of any of the displayed columns (except for Severity or Description) to sort the listed domains by a particular property.

## Purging System Log Messages from the GUI

You may want to remove older system log messages from the primary GSSM GUI. An excessive number of system log messages can make viewing difficult on the System Log list page of the Tools navigation tab. To purge system log messages from the primary GSSM database, use the **gssm database purge-log-records** privileged EXEC command from the primary GSSM CLI.

You can instruct the primary GSSM to purge a quantity of system log messages from the GSSM database except for the following:

- Specified number of recently generated messages
- Most recently generated messages (generated over a specified number of days before today)

The syntax for the **gssm database purge-log-records** command is as follows:

```
gssm database purge-log-records { count number_records_to_keep | days number_days_to_keep }
```

The options and variables are as follows:

- **count**—Purges all system log messages from the primary GSSM database, except the specified number of most recently generated log messages.
- *number\_records\_to\_keep*—Number of system log messages to keep, starting back from the most recently generated log message, when purging the primary GSSM database.
- **days**—Purges the system log messages from the primary GSSM database that were generated prior to a specified number of days before today.
- *number\_days\_to\_keep*—Number of days back, starting from today, to retain log messages when purging the primary GSSM database.

For example, to purge all system log messages except for the last three messages, enter:

```
gssm1.example.com# gssm database purge-log-records count 3
```

For example, to purge all system log messages except for those generated within the last seven days, enter:

```
gssm1.example.com# gssm database purge-log-records days 7
```

To verify that the GSS purged the specified system log messages, perform the following steps:

1. Click the **Tools** tab.
2. Click the **System Logs** navigation link. The System Log list page appears.



#### Note

---

System log messages are purged based on the criteria specified in the **gssm database purge-log-records** CLI command.

---

## Common System Log Messages

[Table 8-3](#) lists common GSS system messages that can appear on the System Log list page. Messages appear alphabetically with a brief description. If you require more detailed information about a specific system message, contact a Cisco technical support representative.



**Table 8-3 System Log Messages**

System Log Message	Description
Deleted a Global Site Selector	The named GSS has been deleted from the primary GSSM.
Error occurred while processing received data	An error occurred in the GSS while processing configuration updates from the primary GSSM. The affected device will attempt to recover automatically.
Failed store invalidation	The GSS has failed the process of marking internally inconsistent database records. Errors can be viewed in the validation log.
Failed store validation	The GSSM database failed its internal consistency checks.
Multiple primary GSSMs detected	The GSS detects multiple primary GSSMs operating concurrently.
Passed store invalidation	The GSS has successfully completed the process of marking internally inconsistent database records.
Passed store validation	The GSSM database passed its internal consistency checks.
Registered a new Global Site Selector	A new GSS is online and has identified itself to the primary GSSM.
Registered a new standby GSSM	A new standby GSSM came online and has identified itself to the primary GSSM.
Server is Shutting Down	The GSS software has been stopped from the CLI.
Server Started	The GSS software has been started from the CLI.
Standby GSSM database error	An error occurred on the standby GSSM embedded database.
Started store invalidation	The GSS has started the process of marking internally inconsistent database records.

**Table 8-3    System Log Messages (continued)**

System Log Message	Description
Started store validation	An internal consistency check has started for the GSSM database.
Store is corrupted	The GSSM database failed the internal consistency checks.
x System Messages Dropped	The GSS dropped and did not report a certain number of messages in an effort to throttle message traffic to the primary GSSM.
Unexpected GSSM activation timestamp warning	<p>The primary GSSM received a report from a GSS device with a GSSM activation time stamp that was not consistent with the current time of the primary GSSM.</p> <p>The clocks of the standby and primary GSSM are not synchronized.</p>
User HTTP Password Change	A user has changed his or her password in the primary GSSM GUI using the Change Password details page from the Tools tab.

# Viewing GSS System Logs Using CiscoWorks RME Syslog Analyzer

You can also use CiscoWorks RME Syslog Analyzer to view GSS syslog messages. The Syslog Analyzer allows you to extract detailed device information by setting up filters that report specific errors, severity conditions, or events, such as a link-down or device reboot.



**Note**

The GSS syslog host messages support the correct CiscoWorks RME Syslog Analyzer message format; however, these messages do not support the Syslog Analyzer MIBs. In addition, not all severity 7 debug messages are compliant with the syslog host message format.

The following is an example of the host syslog message format generated by a GSS. The fields are described in [Table 8-4](#).

```
<IP or DNS name of Device> <BLANK> <:> <Time Stamp> <BLANK><:>
%FACILITY-SEVERITY-MNEMONIC <:> Message-text
```

**Table 8-4 Syslog Message Format**

Field	Description
IP or DNS name of Device	IP address or DNS name, followed by one BLANK space, and followed by a colon (:)
Time Stamp	Nonoptional timestamp in the format:  yyyy mmm dd hh:mm:ss (for example, 2005 MAY 14 19:20:10)  or  mmm dd hh:mm:ss (for example, MAY 14 19:20:10)
%FACILITY	Code consisting of two or more uppercase letters that indicate the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software (for example, KAL, TOMCAT, SYS, STK).  <b>Note</b> This is not the syslog server logging facility.
SEVERITY	Single-digit code from 0 to 7 that reflects the severity of the condition. The severity maps to the GSS logging level specified using the <b>logging host priority</b> command.
MNEMONIC	Code that uniquely identifies the error message (for example, TCPTRANS, GUIEXCEPTION, KALPING).
Message-text	Text string describing the condition (for example, KAL_RSP_OK [192.168.100.1] numSuccessfulProbes:2 or Detected Ssh is stopped but should be started)





# CHAPTER 9

## Monitoring GSS Operation

---

The GSS software includes a number of tools that allow you to monitor the operating status of the GSS devices on your GSS network. These tools include CLI-based commands and the primary GSSM GUI pages that display the status of your GSSs, GSSMs (primary and standby), and the GSSM database.

This chapter contains the following major sections:

- [Monitoring GSS and GSSM Status](#)
- [Monitoring GSSM Database Status](#)
- [Viewing the GSS Operating Configuration for Technical Support](#)



### Note

You can use the **show statistics** CLI command to display content routing and load-balancing statistics for each component of your GSS global server load-balancing operation: Boomerang (CRAs), DNS, DNS sticky, network proximity, and keepalives. See the *Cisco Global Server Load-Balancing Configuration Guide* (GUI-based or CLI-based version) for details about displaying statistics using the **show statistics** command.

---

# Monitoring GSS and GSSM Status

From the CLI of each GSS device, you can monitor the following:

- Online status and resource usage of the individual GSS subsystems (servers) by using the **gss status** command.
- Current operating status of your GSS device, including online status, current software version, and start date or time for the individual GSS subsystems by using the **show system-status** command

From the primary GSSM GUI, you can monitor the status of the GSS devices in your GSS network, including online status, software version, current device role network address, hostname, and MAC address of each device.

This section contains the following topics:

- [Monitoring the GSS Device Online Status from the CLI](#)
- [Monitoring the GSS Device System Status from the CLI](#)
- [Monitoring the GSS Device Status from the Primary GSSM GUI](#)

## Monitoring the GSS Device Online Status from the CLI

To monitor the status and resource usage of a GSS device from the CLI, perform the following steps:

1. Log in to the CLI of a GSS device and enable privileged EXEC mode.

```
gssm1.example.com> enable
gssm1.example.com#
```

2. Display the current running status of the GSS device by using the following command:

```
gssm1.example.com# gss status
Cisco GSS - 1.3(1) GSS [Wed Feb 15 21:09:09 UTC 2006]

Registered to primary GSSM: 10.86.209.167

Normal Operation [runmode = 5]

START  SERVER
Jul09  Boomerang
Jul09  Config Agent (crdirector)
Jul09  Config Server (crm)
Jul09  DNS Server
```

```

Jul09 Database
Jul09 GUI Server (tomcat)
Jul09 Keepalive Engine
Jul09 Node Manager
Jul09 Proximity
Jul09 Sticky
Jul09 Web Server (apache)

```

The status of the License Manager (LM) and the Distributed Denial of Service (DDoS) prevention module do not appear in the output of the **gss status** command. To obtain DDoS status, enter the **show ddos status** command and to obtain LM status, enter **show processes | grep license\_manager**. For example, enter:

```

gssm1.example.com# show processes | grep license_manager
license_manager 1705 0.0 00:00:00 Nov02

```



#### Note

When the DNS server is ready to serve DNS requests, it generates the following subsystem log message and saves it in the system.log file:

```

Mar 25 10:45:26 gssm1.example.com DNS-5-SELREADYINFO[2073] Selector
ready to start serving DNS requests

```

3. Include statistics about the CPU utilization when displaying information on the current GSS operating state by entering the following command:

```

gssm1.example.com# gss status verbose
Cisco GSS - 1.3(1) GSS [Wed Feb 31 21:09:09 UTC 2006]

```

```

Registered to primary GSSM: 10.86.209.167

```

```

Normal Operation [runmode = 5]

```

```

%CPU START SERVER
0.0 11:55 Boomerang
0.0 11:55 Config Agent (crdirector)
0.0 11:55 Config Server (crm)
0.0 11:55 DNS Server
0.0 11:55 Database
0.0 11:55 GUI Server (tomcat)
0.0 11:55 Keepalive Engine
0.0 02:58 Node Manager
0.0 02:58 Proximity
0.0 02:58 Sticky
0.0 11:55 Web Server (apache)

```

## Monitoring the GSS Device System Status from the CLI

To monitor the current operating status of a GSS device from the CLI, perform the following steps:

1. Log in to the CLI of a GSS device and enable privileged EXEC mode.

```
gss1.example.com> enable
gss1.example.com#
```

2. Display the current running status of the GSS device by entering the following command:

```
gssm1.example.com# show system-status
Cisco GSS - 1.3(1) GSS Manager - primary [Wed Feb 15 16:37:37 UTC
2006]
```

```
Normal Operation [runmode = 5]
```

```
START  SERVER
Jul09  Boomerang
Jul09  Config Agent (crdirector)
Jul09  Config Server (crm)
Jul09  DNS Server
Jul09  Database
Jul09  GUI Server (tomcat)
Jul09  Keepalive Engine
Jul09  Node Manager
Jul09  Proximity
Jul09  Sticky
Jul09  Web Server (apache)
```



### Note

---

The equivalent CLI command is **gss status**.

---

## Monitoring the GSS Device Status from the Primary GSSM GUI

To monitor the status of GSS devices from the primary GSSM GUI, perform the following steps:

1. From the primary GSSM GUI, click the **Resources** tab.
2. Click the **Global Site Selectors** navigation link. The Global Site Selector list page appears displaying the status, role, and IP address of each GSS in the network.



3. Click the **Modify GSS** icon for the GSS or GSSM to monitor. The Global Site Selectors details page appears, displaying configuration and status information about the device at the bottom of the page. The device type (GSS or GSSM) appears in the Node Services column.

Displayed information is as follows:

- Status—Online or offline
  - Version—Software version currently loaded on the device
  - Node services—Current role of the device (GSS, primary or standby GSSM, or both)
  - IP address—Network address of the device
  - Hostname—Network hostname of the device
  - MAC—Machine address of the device
4. Click **Cancel** to return to the Global Site Selectors list page.

## Monitoring GSSM Database Status

The GSS software includes a number of CLI commands to monitor the status of the GSSM database and its contents. This section contains the following topics:

- [Monitoring the Database Status](#)
- [Validating Database Records](#)
- [Creating a Database Validation Report](#)

## Monitoring the Database Status

To verify that the database running on the primary GSSM is functioning properly, perform the following steps:

1. Log in to the CLI of the primary GSSM and enable privileged EXEC mode.

```
gssm1.example.com> enable
gssm1.example.com#
```
2. Display the operating status of the GSSM database by entering the following command:

```
gssm1.example.com# gssm database status
GSSM database is running.
```

## Validating Database Records

To validate the records in your GSSM database, perform the following steps:

1. Log in to the CLI of the primary GSSM and enable privileged EXEC mode.

```
gssm1.example.com> enable
gssm1.example.com#
```

2. Validate the content of your GSSM database by entering the following command:

```
gssm1.example.com# gssm database validate
GSSM database passed validation.
```

## Creating a Database Validation Report

If you encounter problems while validating your GSSM database, you can generate a report, called `validation.log`, that details which database records failed validation. The **gssm database report** command constructs a list of invalid records in the GSSM database and writes the results to `validation.log` in the `/home` directory.

To generate a database validation report, perform the following steps:

1. Log in to the CLI of the primary GSSM and enable privileged EXEC mode.

```
gssm1.example.com> enable
gssm1.example.com#
```

2. Generate a validation report on the content of your GSSM database by entering the following command:

```
gss1.example.com# gssm database report
GSSM database validation report written to validation.log.
```

3. View the contents of your validation report by entering the following command:

```
gss1.example.com# type validation.log
validation.log
Start logging at Wed Feb 15 19:17:21 GMT+00:00 2006
```

```
- storeAdmin Validating ... Wed Feb 15 19:17:23 GMT+00:00 2006 -  
- ObjectID Object_Name.Field_Name Description -  
Validating FactoryInfo  
Validating answerElement  
Validating answerGroup  
70 answerGroup.OwnerId Many-To-One List  
Validating CachingConfig  
Validating ClusterConfig  
Validating CmdControl  
Validating CmdPurgeRd  
Validating CmdUpdate  
Validating ConfigProperty  
Validating Customer  
Validating DistTree  
Validating DnsRule  
Validating DomainElement  
Validating DomainGroup  
Validating ENodeConfig  
Validating ENodeStatus  
Validating KeepAliveConfig  
Validating KeepAlive  
Validating Location  
Validating OrderedanswerGroup  
Validating Owner  
Validating Region  
Validating RequestHandler  
Validating RoutedDomain  
Validating RoutingConfig  
Validating RrConfig  
Validating RrStatus  
Validating SNodeConfig  
Validating SourceAddressElement  
Validating SourceAddressGroup  
Validating SpInfo  
Validating SystemConfig  
Validating UpdateInfo  
Validating UserConfig  
Validating VirtualCDN  
Validating WlpanswerElement  
Validating User Validations  
End of file validation.log
```

# Viewing the GSS Operating Configuration for Technical Support

The GSS software includes two CLI commands to assist a Cisco Technical Assistance Center (TAC) representative in troubleshooting potential problems on your GSS network. Use the following CLI commands:

- **show tech-support [config | core-files]**—Displays a report on the current operating configuration of your GSS device that can be used by a Cisco TAC representative in troubleshooting problems on your GSS network. The **config** option exports the output of all configured fields from the primary GSSM GUI.
- **gss tech-report filename** —Generates a detailed report for use by a Cisco TAC representative in troubleshooting persistent GSS problems. The file generated is a compressed tar- format archive file with a .tgz extension. The *filename* argument identifies a user-assigned name for the report generated by the **gss tech-report** command.

For example, to display an operating configuration report for your GSS device, enter:

```
gssm1.example.com(config)# show tech-support
Cisco GSS - 1.3(1.0.0) - host-gss GSS software GSSM - standby [[Wed
Feb 15 16:39:09 UTC 2006]
```

```
Registered to primary GSSM: 10.86.209.252
```

```
Normal Operation [runmode = 5]
START SERVER
Sep15 Boomerang
Sep15 Config Agent (crdirector)
Sep15 Config Server (crm)
Sep15 DNS Server
Sep15 Database
Sep15 GUI Server (tomcat)
Sep15 Keepalive Engine
Sep15 Node Manager
Sep15 Web Server (apache)
*** clock ***
System time: Wed Feb 15 16:41:24 UTC 2006
*** uptime ***
Uptime: 22 Hours 41 Minutes and 48 seconds
*** running-config ***
interface ethernet 0
```

```
ip address 10.86.209.220 255.255.254.0
gss-communications
interface ethernet 1
ip address 192.168.1.25 255.255.255.0
gss-tcp-keepalives
...
```

To export the output of all configured fields from the primary GSSM GUI, enter:

```
gssm1.example.com(config)# show tech-support config
GUI Configuration Export:
Wed Feb 15 16:46:24 GMT+00:00 2006
Global Site Selectors:
  GSS1:
    Global Site Selector: charon.cisco.com
    Status: Online
    Node Services: GSS
    IP Address: 192.168.209.224
    Location:
    Region:
  GSS2:
    Global Site Selector: geryon.cisco.com
    Status: Online
    Node Services: GSS
    IP Address: 192.168.209.225
    Location:
    Region:
  GSS3:
    Global Site Selector: ladon.cisco.com
    Status: Online
    Node Services: GSS; Standby GSSM
    IP Address: 192.168.209.222
    Location:
    Region:
  GSS4:
    Global Site Selector: icarus.cisco.com
    Status: Online
    Node Services: GSS
    IP Address: 192.168.209.221
    Location:
    Region:
DNS Rules:
  Rule1:
    Name: ECommerce
    Source Address List: Anywhere
    Domain List: ECommerce
    Owner: ECommerce-Database
    Status: Active
    Match DNS Query Type: A record
```

**Viewing the GSS Operating Configuration for Technical Support**

```
Answer Group 1: Database-Services
Balance Method 1: Hashed
Balance Clause Options 1: DNS TTL: 20; Return Record Count: 1;
Answer Group 2:
Balance Method 2:
Balance Clause Options 2:
Answer Group 3:
Balance Method 3:
```



## APPENDIX

# A

## Upgrading the GSS Software

---

This appendix describes how to upgrade the GSS software to a new software version. To upgrade the software, you must do the following:

- Have access to the GSS download area of the Cisco software download site and to Cisco.com.
- Be familiar with the proper procedure for updating your GSS devices and know the CLI commands required to execute the backup.

To take full advantage of all of the features and capabilities of the software release, we recommend that you upgrade all GSS devices in your network within the same time frame, starting with the primary GSSM. This upgrade sequence ensures that the other GSS devices properly receive configuration information from, and are able to send statistics to, the primary GSSM.

This section contains the following procedures:

- [Verifying the GSSM Role in the GSS Network](#)
- [Backing up and Archiving the Primary GSSM](#)
- [Obtaining the Software Upgrade](#)
- [Upgrading Your GSS Devices](#)

The GSS software upgrade requires that you complete each of these procedures in the order shown in this appendix.

# Verifying the GSSM Role in the GSS Network

Before you continue with the upgrade procedure, verify that the roles of the designated primary and standby GSSMs have not changed. The changing of roles between the designated primary GSSM and the standby GSSM is intended to be a temporary GSS network configuration until the original primary GSSM is back online.

To verify the role of the current primary GSSM and the standby GSSM, perform the following steps:

1. At the CLI of the current primary GSSM, enter the following commands:

```
gssm1.example.com# cd /home
gssm1.example.com# type ../props.cfg | grep -i fqdn
```

The following output appears:

```
controllerFqdn= domain_name OR ip_address
```

2. Based on the output value for controllerFqdn, follow these guidelines:
  - If the value of the domain name or IP address is the current primary GSSM in your network, then the current primary GSSM and standby GSSM configuration is the original configuration and no further action is needed. See the [“Backing up and Archiving the Primary GSSM”](#) section.
  - If the value of the domain name or IP address is the current standby GSSM in your network, then the current primary GSSM and standby GSSM configuration is not the original configuration. In this case, you must reverse the roles of the primary and standby GSSM devices to those of the original GSS network deployment. See the [“Reversing the Roles of the Interim Primary and Standby GSSM Devices”](#) section in [Chapter 2, Managing the GSS from the CLI](#).
  - If the value of the domain name or IP address is not the current primary GSSM or the standby GSSM in your network, this indicates that the device is not a primary GSSM or is no longer on the network. No further action is required. See the [“Backing up and Archiving the Primary GSSM”](#) section.

The next step is to ensure that you have a full (and current) backup of the primary GSSM database and that you archive this backup. Proceed to the [“Backing up and Archiving the Primary GSSM”](#) section.



# Backing up and Archiving the Primary GSSM

Before you upgrade your GSS software, ensure that you have a full backup of your primary GSSM database and that you archive the backup by moving it to a remote device. The GSSM database maintains all network and device configuration information, as well the DNS rules that are used by your GSS devices to route DNS queries from users to available hosts.

If necessary, you can quickly restore your GSS network to its previous state by performing a full backup at any time. A full backup does not interfere with the functions of the primary GSSM or other GSS devices.

See the “Performing a Full Primary GSSM Backup” section in [Chapter 7, Backing Up, Restoring, and Downgrading the GSSM Database](#) for instructions on performing a full backup of your primary GSSM. Performing a full backup requires access to the CLI.

You are now ready to obtain the upgrade file and upgrade the software on a GSS device. See the “Obtaining the Software Upgrade” section.

## Obtaining the Software Upgrade

Before you can update your GSS software, obtain the appropriate software update file from Cisco Systems as follows:

- Access the Cisco.com website and locate the software update files.
- Download the software update files to a server within your own organization that is accessible using FTP or SCP from your GSSs and GSSMs.

You must have a Cisco.com username and password to download a software update from Cisco.com. To acquire a Cisco.com login, go to <http://www.cisco.com> and click the **Register** link.

**Note**

You need a service contract number, Cisco.com registration number and verification key, Partner Initiated Customer Access (PICA) registration number and verification key, or packaged service registration number to obtain a Cisco.com username and password.

To add an upgrade file for the GSS software, perform the following steps:

1. Launch your preferred web browser and point it to the Cisco Global Site Selector download page. When prompted, log in to Cisco.com using your designated Cisco.com username and password. The Cisco GSS Software download page appears, listing the available software upgrades for the GSS software product.
2. If you do not have a shortcut to the Cisco Global Site Selector download page:
  - a. Log in to Cisco.com using your designated Cisco.com username and password.
  - b. Access the Software Center from the Technical Support link.
  - c. Click the **Content Networking Software** link from the Software Center - Software Products and Downloads page.
  - d. Click the **Cisco Global Site Selector** link from the Software Center - Content Networking page.
  - e. Click the **Download Cisco Global Site Selector** link from the Software Center - Content Networking page.

The Cisco GSS Software download page appears, listing the available software upgrades for the Cisco GSS Software product.



#### Note

---

When you first access the Content Networking page of the Software Center, you must apply for eligibility for GSS software updates because it is considered a strong encryption image. Under the Cisco Content Networking Cryptographic Software section is the Apply for 3DES Cisco Cryptographic Software Under Export Licensing Controls link. Click this link and complete the Encryption Software Export Distribution Authorization Form. Complete this step to access and download Global Site Selector software images.

---

3. Locate the .upg file that you want to download by referring to the Release column for the proper release version of the software.
4. Click the link for the .upg file. The download page appears.
5. Click the **Software License Agreement** link. A new browser window opens to display the license agreement.
6. After you have read the license agreement, close the browser window that displays the agreement and return to the Software Download page.

7. Click **Download**. If prompted by software, reenter your username and password.
8. Click **Save to file**, and then choose a location on your workstation to temporarily store the .upg upgrade file.
9. Post the .upg file that you downloaded to a designated area on your network that is accessible to all your GSS devices.

You are now ready to upgrade the software on a GSS device. See the [“Upgrading Your GSS Devices”](#) section.

## Upgrading Your GSS Devices

Before upgrading from an earlier version of GSS to v2.0, you should do the following:

- Be aware of these considerations when CNR is installed and enabled:
  - The Name Service (NS) forwarding feature does not work on v2.0 if CNR is enabled. For example, if a DNS rule has been configured to perform NS forwarding in clause1 on v1.3.3 and you then upgrade to v2.0 with CNR installed and enabled, all DNS requests will be forwarded directly to CNR. This action occurs even if there is a matching DNS rule with NS forwarding configured on the GSS.
  - To obtain support for reverse lookup for the answers configured on the GSS, you need to explicitly configure the Pointer (PTR) records to do the same on CNR.
  - To perform NS forwarding on GSS v2.0 (without CNR) to a name service that is GSS/CNR, you must configure a proper domain name in the domain name field in the NS type answer configuration. In addition, the external name server must be authoritative for the domain name if the name server is GSS/CNR. By default, the NS type answer queries for ".".
  - To obtain the same expiration level for the records returned by the GSS and the CNR, you need to ensure that the TTL configuration is the same on both the CNR and GSS.
  - To have the GSS/CNR device process the NON A records for the authoritative domain, you must configure all the NON A records on the CNR that were earlier processed by the external name service using NS forwarding.

- Ensure that you are running v1.3. If not, you should upgrade to v1.3 before performing the v2.0 upgrade. When a primary GSSM has been upgraded to software v1.2(2.1.3) or later, but other GSS devices remain at v1.2(2.0.3) or v1.2(1.1.2), global server load-balancing configuration settings do not propagate to the GSS devices still at v1.2(2.0.3) or v1.2(1.1.2). To avoid this behavior, ensure that all GSS devices on the network are upgraded to same software version as the primary GSSM before you configure global server load balancing.
- Be sure to upgrade the primary GSSM first, followed by the other GSS devices in your network. After you upgrade the primary GSSM, ensure that each GSS device in your network to be upgraded has connectivity to the primary GSSM before you perform the software upgrade procedure.

When executing an upgrade, use the **install** CLI command. Before proceeding with the software upgrade, the **install** command performs a validation check on the upgrade file, unpacks the upgrade archive, and installs the upgraded software. Finally, the **install** command restarts the affected GSS device.



#### Note

Upgrading your GSS devices causes a temporary loss of service for each affected device.

To upgrade the GSS software (starting with the primary GSSM), perform the following steps:

1. Log on to the CLI of the GSS device.
2. Enter the Global Configuration Mode by entering the **enable** command and then the **config** command.
3. If you use FTP to copy files into GSS, enable the FTP client by entering the **ftp-client enable all** command at the config prompt.
4. Type **exit** to leave Global Configuration mode.
5. Use the **ftp** or **scp** command to copy the GSS software upgrade file from the network location to a directory on the GSS. Ensure that you set the transfer type to **binary**.

For example, to copy an upgrade file named gss.upg from a remote host, your FTP session may appear as follows:

```
gssm1.example.com> ftp host.example.com
Connected to host.example.com.
220 host.example.com FTP server (Version wu-2.6.1-0.6x.21) ready.
Name (host.example.com:root): admin
```

```
331 Password required for admin.
Password:
230 User admin logged in. Access restrictions apply.
Remote system type is UNIX.
Using ascii mode to transfer files.
ftp> binary
ftp> get
(remote-file) gss.upg
(local-file) gss.upg
local: gss.upg remote: gss.upg
200 PORT command successful.
...
```

6. Enable privileged EXEC mode.

```
gssml.example.com> enable
gssml.example.com#
```

7. Stop the GSS software by entering the following command:

```
gssml.example.com# gss stop
```

8. Install the upgrade by entering the following command:

```
gssml.example.com# install gss.upg
```

9. At the Proceed with install (the device will reboot)? (y/n): prompt, type **y** to reboot the GSS device. After the GSS reboots, you lose any network CLI connections. Console connections remain active.



**Note**

If you did not previously save changes to the startup-config file, the Save current configuration? [y/n]: prompt appears. At the prompt, type **y** to continue. The GSS then reboots.

10. After the GSS device reboots, log in to the GSS device and enable privileged EXEC mode.
11. Verify that the GSS device reaches a normal operation state of runmode 4 or 5 by entering the **gss status** command.
12. Repeat Steps 1 through 11 for the remaining GSS devices in your network.





## INDEX

---

### A

#### access lists

- access-group command [5-7, 5-8](#)

- access-list command [5-4](#)

- adding rules to [5-8](#)

- associating with an interface [5-7](#)

- creating [5-4](#)

- destination port [5-5](#)

- disassociating from an interface [5-8](#)

- displaying [5-10](#)

- filtering traffic [5-1](#)

- ICMP traffic filtering [5-4](#)

- operator [5-5](#)

- overview [5-2](#)

- removing rules [5-9](#)

- source address [5-4](#)

- TCP traffic filtering [5-4](#)

- UDP traffic filtering [5-4](#)

- viewing [5-9](#)

- activating GSS devices [1-6](#)

- adding rules to access lists [5-8](#)

- administration password

- changing [3-27, 3-28](#)

- restoring [3-28](#)

- administrator account, resetting [3-26](#)

- associating access list with interface [5-7](#)

---

### B

- backup of GSSM

- full backup procedure [7-3](#)

- overview [7-2](#)

- boot information, displaying [2-44](#)

---

### C

- certificate

- accepting [1-2](#)

- attributes, modifying [2-21](#)

- certificate set-attributes command [2-21](#)

- installing [1-2](#)

- keys, deleting [2-21](#)

- modifying [2-21](#)

- trusting [1-2](#)

- changing GSSM roles in GSS network [2-36](#)

- CLI

- GSS device monitoring [9-2, 9-4](#)

- logging in [2-2](#)
- monitoring GSS network statistics [9-1](#)
- privileged EXEC mode, enabling [2-2](#)
- privilege level, specifying [3-3](#)
- resetting CLI administrator account [3-26](#)
- resetting password [3-15](#)
- TACACS+ server, authorization settings [4-9](#)
- user account, creating [3-2](#)
- cold restart, performing [2-24](#)
- copying
  - files [2-18](#)
  - startup configuration to or from disk [2-10, 2-11](#)
- CPU or memory processes [2-45](#)

---

## D

- database
  - monitoring status of [9-5](#)
  - purging [8-15](#)
  - records, purging [8-16](#)
  - restoring GSSM from full backup [7-5](#)
  - validating records [9-6](#)
  - validation report [9-6](#)
- debug log message [8-15](#)
- default
  - password [1-3](#)
  - username [1-3](#)
- deleting files [2-19](#)
- deployment, GSS devices behind firewall [5-12](#)

- directory
  - current working directory, displaying [2-16](#)
  - displaying files [2-16](#)
- disabling GSS software [2-25](#)
- disassociating access list from interface [5-8](#)
- disk
  - displaying information [2-46](#)
  - specifying for log file destination [8-5](#)
- documentation
  - audience [xi](#)
  - caution and note overview [xvi](#)
  - conventions [xiii, xv](#)
  - organization [xii](#)
  - related [xiii](#)
  - set [xiii](#)
  - symbols and conventions [xv](#)
- downgrading
  - GSS device software [7-8](#)
  - order of operation [7-8](#)
  - restoring earlier software version [7-8](#)

---

## E

- enabling GSS software [2-25](#)
- Ethernet interface, segmenting traffic [5-9](#)
- exporting primary GSSM data [1-14](#)



## F

factory defaults, restoring [2-25](#)

fatal error log message [8-15](#)

files

deleting [2-19](#)

displaying entire contents [2-15](#)

displaying in directory [2-16](#)

displaying last 10 lines [2-15](#)

listing within directory [2-47](#)

renaming [2-17](#)

securely copying [2-18](#)

filtering

GSS traffic [5-1](#)

ICMP traffic [5-4](#)

TCP traffic [5-4](#)

traffic type [5-4](#)

UDP traffic [5-4](#)

firewall

configuring for GSS [5-15](#)

deploying GSS devices [5-12](#)

inbound traffic to GSS [5-12](#)

inbound traffic to the GSS [5-13](#)

outbound traffic from the GSS [5-14](#)

full GSSM backup [7-3](#)

## G

Global Site Selector

activating from primary GSSM [1-6](#)

cold restart, performing [2-24](#)

CPU or memory processes, displaying [2-45](#)

deleting devices from primary GSSM [1-10](#)

disabling GSS device [2-25](#)

downgrading software [7-8](#)

enabling GSS device [2-25](#)

firewalls [5-12](#), [5-15](#)

GSS-related port and protocols [5-3](#)

hard disk information, displaying [2-46](#)

inactivity timeout [2-20](#)

inter-GSS communications [5-9](#)

license data, displaying [2-42](#)

logging levels [8-1](#), [8-5](#), [8-7](#)

logically removing or replacing [1-11](#)

login accounts [3-1](#)

memory blocks and statistics,  
displaying [2-43](#)

MIB files [6-9](#)

modifying device configuration from primary  
GSSM [1-9](#)

monitoring through CLI [9-2](#), [9-4](#)

monitoring through GUI [9-4](#)

online status and resource usage [9-2](#), [9-4](#)

operating configuration, displaying for  
TAC [9-8](#)

ports and protocols [5-2](#), [5-12](#)

purging system log messages [8-15](#)

registering [1-6](#)

renaming a file [2-17](#)

- replacing [2-35](#)
- reporting interval [1-14](#)
- restarting GSS software [2-24](#)
- running configuration [2-8, 2-10](#)
- services information, displaying [2-48](#)
- shutting down GSS software [2-23](#)
- startup configuration [2-8, 2-10](#)
- status [2-47, 9-4](#)
- stopping GSS software [2-23](#)
- subsystem levels [8-1](#)
- subsystems [8-5, 8-7](#)
- system status, displaying [2-47, 9-4](#)
- UDI, displaying [2-46](#)
- user account, creating [3-2](#)
- user account, deleting [3-3](#)
- user account, modifying [3-3](#)
- version information [2-41](#)
- Global Site Selector Manager
  - activating [1-6](#)
  - activating devices [1-6](#)
  - backing up [7-2](#)
  - changing role in GSS network [2-36](#)
  - changing the GUI password [3-13](#)
  - changing to standby [2-36](#)
  - cold restart, performing [2-24](#)
  - configuring, primary [4-29](#)
  - configuring, standby [4-29](#)
  - creating user account (GUI) [3-9](#)
  - database, monitoring [9-5](#)
  - default username and password [1-3](#)
  - deleting GSS devices [1-10](#)
  - disabling GSSM device [2-25](#)
  - downgrading software [7-8](#)
  - enabling GSSM device [2-25](#)
  - exporting data [1-14](#)
  - GUI, configuring [1-13](#)
  - inactivity timeout [2-20](#)
  - logging on [1-2](#)
  - logically removing GSS or standby GSSM [1-11](#)
  - login accounts [3-4](#)
  - modifying devices [1-9](#)
  - modifying user account (GUI) [3-12](#)
  - monitoring device status from GUI [9-4](#)
  - password [3-13](#)
  - platform information [7-6](#)
  - printing data [1-14](#)
  - registering GSS devices [1-6](#)
  - removing user account (GUI) [3-12](#)
  - replacing [2-31, 2-33](#)
  - restarting GSS software [2-24](#)
  - restoring factory defaults [2-25](#)
  - restoring full backup [7-5](#)
  - reversing role in GSS network [2-39](#)
  - role change [2-36](#)
  - shutting down GSS software [2-23](#)
  - stopping GSS software [2-23](#)
  - TACACS+ server authorization [4-12](#)
  - URL, secure HTTP [1-2, 1-5](#)

- verifying role prior to upgrading [A-2](#)
- viewing system logs [8-13](#)
- gss.log file [8-10](#)
- gssm standby-to-primary command [2-27, 2-38](#)
- GSS network
  - changing GSSM role [2-36](#)
  - GSS, logically removing [1-11](#)
  - limiting network traffic [5-9](#)
  - logically removing a GSS [1-11](#)
  - monitoring through CLI [9-1](#)
  - monitoring through GUI [9-4](#)
  - primary GSSM, logically removing [1-11](#)
  - reversing GSSM role [2-39](#)
  - segmenting network traffic [5-9](#)
  - standby GSSM, logically removing [1-11](#)
  - URL [1-2, 1-5](#)
- GSS-related ports and protocols [5-3](#)
- GUI
  - configuration [1-13](#)
  - default username and password [1-3](#)
  - logging on [1-2](#)
  - logging out [1-4](#)
  - monitoring GSS device status [9-5](#)
  - password [3-13](#)
  - refreshing [1-14](#)
  - session inactivity timeout [1-13](#)
  - timeout [1-14](#)
  - user account, creating [3-9](#)
  - user account, modifying [3-12](#)

- user account, removing [3-12](#)
- user view, creating [3-16](#)
- GUI privilege level
  - administrator [3-5, 3-6](#)
  - observer [3-5, 3-8](#)
  - operator [3-5, 3-6](#)
  - specifying [3-10](#)
  - TACACS+ server authorization [4-12](#)

---

## H

- host, specifying as log file destination [8-6](#)

---

## I

- Info log message [8-15](#)
- inter-GSS communications [5-9](#)

---

## K

- keepalives with TACACS+ server [4-22](#)

---

## L

- loading startup configuration from external file [2-10](#)
- log files
  - destination, specifying disk [8-5](#)
  - host destination, specifying [8-6](#)

- logging levels [8-1](#)
- rotating [8-12](#)
- subsystem [8-11](#)
- viewing from CiscoWorks RME Syslog Analyzer [8-18](#)
- logging
  - facility [8-8](#)
  - follow command option [8-10](#)
  - host destination, specifying [8-6](#)
  - levels [8-1, 8-4](#)
  - log activity, displaying [8-11](#)
  - logging disk command [8-5, 8-6](#)
  - logs, displaying [8-11](#)
  - purging log records [8-15](#)
  - subsystems [8-5, 8-7](#)
  - syslog facility [8-8](#)
  - system logging [8-4](#)
  - system message log, displaying [8-11](#)
  - tail command option [8-10](#)
  - to a specific file on disk [8-5](#)
  - to sys.log file, disabling [8-8](#)
  - to sys.log file, enabling [8-6](#)
  - turning off from disk [8-6, 8-7, 8-8](#)
- logging levels [8-1, 8-5, 8-7](#)
- logically removing
  - GSS from a network [1-11](#)
  - GSS or standby GSSM from the network [1-11](#)
  - standby GSSM from a network [1-11](#)
- log in

- CLI [2-2](#)
- default GUI username and password [1-3](#)
- inactivity timeout, specifying [2-20](#)
- logging out [1-4](#)
- primary GSSM GUI [1-2](#)
- login accounts
  - creating on GSS [3-2](#)
  - creating on GSSM [3-9](#)
  - deleting [3-3](#)
  - GSSM [3-4](#)
  - managing [3-1](#)
  - modifying [3-3, 3-12](#)
  - removing [3-12](#)
- log out [1-4](#)

---

## M

- memory blocks and statistics [2-43](#)
- messages
  - purging [8-15](#)
  - system log [8-16](#)
  - viewing [8-13](#)
- MIBs [6-2, 6-9](#)
- monitoring
  - database status [9-5](#)
  - GSS network status [9-1](#)
  - online status [9-2, 9-4](#)
  - resource usage [9-2, 9-4](#)
  - status of GSS devices by CLI [9-2](#)

status of GSS devices from the GUI [9-5](#)

## N

network

See GSS network

## O

operator range [5-5](#)

## P

packets

denying [5-4](#)

permitting [5-4](#)

Partner Initiated Customer Access

See PICA

password

changing default administration  
password [3-27, 3-28](#)

CLI, resetting [3-15](#)

CLI user account, creating [3-2](#)

default (GUI) [1-3](#)

GSSM GUI, changing [3-13](#)

GUI, entering [1-3](#)

GUI user account, changing password [3-13](#)

GUI user account, creating [3-10](#)

resetting CLI administrator account [3-26](#)

restoring default administration  
password [3-28](#)

PICA [A-3](#)

platform information

restoring [7-6](#)

summary [7-6](#)

ports and protocols [5-2, 5-3, 5-12](#)

printing primary GSSM data [1-14](#)

privileged EXEC mode, enabling [2-2](#)

protocols and ports for GSS devices [5-3](#)

purging system log messages [8-15](#)

## R

record

database records, validating [9-6](#)

purging [8-15](#)

refreshing the GUI [1-14](#)

registering GSS devices [1-6](#)

renaming a GSS file [2-17](#)

replacing

flowchart [2-26](#)

GSS [2-35](#)

primary GSSM [2-31](#)

standby GSSM [2-33](#)

report, database validation creating [9-6](#)

reset-gui-admin-password command [3-28](#)

resetting

CLI administrator account [3-26](#)

CLI password [3-15](#)

- password [3-26](#)
- restarting GSS software [2-24](#)
- restoring
  - default administration password [3-28](#)
  - GSSM from full backup [7-5](#)
  - GSSM platform information [7-6](#)
  - overview [7-4](#)
- rotating log files [8-12](#)
- running configuration file
  - changing [2-9](#)
  - copying [2-10](#)
  - copying as startup-config file [2-9](#)
  - displaying [2-11](#)
  - overview [2-8](#)
  - saving to startup configuration [2-9](#)
  - summary [2-8, 2-10](#)

---

## S

- segmenting GSS traffic by interface [5-9](#)
- session inactivity timeout [1-13](#)
- severity log message [8-15](#)
- show commands
  - show access-group command [5-11](#)
  - show access-list command [5-9, 5-10](#)
  - show boot-config command [2-44](#)
  - show disk command [2-46](#)
  - show inventory command [2-46](#)
  - show license command [2-42](#)

- show logging command [8-11](#)
- show logs command [8-10](#)
- show memory command [2-43](#)
- show processes command [2-45](#)
- show services command [2-48](#)
- show system-status command [2-47, 9-4](#)
- show tacacs command [4-26](#)
- show tech-support command [9-8](#)
- show uptime command [2-46](#)
- show user command [2-19](#)
- show users command [2-19](#)
- show version command [2-41](#)
- shutting down GSS software [2-23](#)

## SNMP

- configuring [6-2](#)
- configuring server information [6-4](#)
- disabling [6-3](#)
- enabling [6-2](#)
- MIB files, viewing [6-9](#)
- overview [6-2](#)
- port, changing [6-9](#)
- server notifications [6-5, 6-6](#)
- setup [6-2](#)
- snmp command [6-2](#)
- snmp-server command [6-4](#)
- specifying notification operation recipients [6-7](#)
- viewing status [6-8](#)
- SNMP notification operations
  - snmp-server host command [6-7](#)

- specifying recipients [6-7](#)
- SNMP server information
  - configuring [6-4](#)
- SNMP server notifications
  - enabling [6-5](#), [6-6](#)
  - snmp-server enable traps command [6-5](#), [6-6](#)
- software
  - boot information, showing [2-44](#)
  - disabling GSS device [2-25](#)
  - downgrade, restoring earlier software version [7-8](#)
  - downgrade procedure [7-8](#)
  - enabling GSS device [2-25](#)
  - restarting [2-24](#)
  - shutting down [2-23](#)
  - stopping [2-23](#)
  - update, obtaining update file [A-3](#)
  - upgrade procedure [A-1](#)
  - version information, showing [2-41](#)
- standby GSSM [1-11](#)
  - changing to primary [2-36](#)
  - logically removing [1-11](#)
  - registering with primary GSSM [1-6](#)
  - replacing [2-33](#)
- startup configuration
  - changing [2-8](#), [2-10](#)
  - loading from external file [2-10](#)
  - saving running configuration as startup configuration [2-9](#)
- startup configuration file
  - changing [2-9](#)
  - copying [2-10](#)
  - copying device startup configuration settings [2-11](#)
  - copying running configuration file as [2-9](#)
  - displaying [2-13](#)
  - loading from external file [2-11](#)
  - overview [2-8](#)
- stopping GSS software [2-23](#)
- subsystem log files
  - rotating [8-12](#)
  - viewing [8-11](#)
- subsystems [8-1](#), [8-5](#), [8-7](#)
- sys.log [8-6](#), [8-8](#)
- syslog, configuring [8-4](#)
- system
  - logging [8-4](#)
  - message log [8-11](#)
  - status, displaying [2-47](#), [9-4](#)
- system log
  - messages [8-16](#)
  - purging [8-15](#)
  - severity [8-15](#)
  - typical messages [8-16](#)
  - viewing [8-13](#)
  - viewing from CiscoWorks RME Syslog Analyzer [8-18](#)
  - viewing from GUI [8-14](#)
- system uptime, displaying [2-46](#)

---

**T****TAC**

- displaying GSS operating configuration [9-8](#)
- tech report [9-8](#)

**TACACS+**

- accounting overview [4-3](#)
- authentication overview [4-3](#)
- authorization overview [4-3](#)
- Cisco Secure Access Control Server (ACS) [4-5](#)
- disabling [4-28](#)
- GSS, disabling/enabling keepalives [4-22](#)
- GSS, specifying accounting [4-25](#)
- GSS, specifying authentication [4-23](#)
- GSS, specifying authorization [4-24](#)
- GSS, specifying server hosts [4-19](#)
- GSS, specifying server timeout [4-23](#)
- overview [4-2](#)
- primary GSSM GUI privilege level authorization [4-12](#)
- primary GSSM user view authorization [4-16](#)
- quick start [4-4](#)
- server, accounting settings [4-17](#)
- server, authentication settings [4-5](#)
- server, authorization settings [4-7](#)
- server, configuring [4-5](#)
- shared secret with GSS [4-20](#)
- statistics, clearing [4-28](#)
- statistics, displaying [4-26](#)

tail command option [8-12](#)

terminal screen line length, configuring [2-20](#)

third-party software, viewing information [1-15](#)

**traffic**

- filtering [5-4](#)
- limiting [5-9](#)
- segmenting by interface [5-9](#)

---

**U****UDI** [2-46](#)**upgrading**

- GSS software [A-1](#)
- obtaining update file [A-3](#)
- sequence [A-1](#)
- update file, obtaining [A-3](#)
- verifying GSSM role prior to upgrading [A-2](#)

**user**

- account, creating [3-9](#)
- account, modifying [3-12](#)
- account, removing [3-12](#)
- information, displaying [2-19](#)

**user account**

- CLI account, creating [3-2](#)
- CLI account, deleting [3-3](#)
- CLI account, modifying [3-3](#)
- CLI user, privilege levels [3-3](#)
- creating for GUI [3-9](#)
- creating with CLI [3-2](#)



- deleting [3-3](#)
- GUI user, privilege levels [3-5, 3-6, 3-8, 3-10](#)
- GUI user, views [3-11](#)
- GUI user account, changing password [3-13](#)
- GUI user account, creating [3-9](#)
- GUI user account, modifying [3-12](#)
- GUI user account, removing [3-12](#)
- modifying [3-3, 3-12](#)
- removing [3-12](#)
- view overview [3-15](#)
- username
  - default (GUI) [1-3](#)
  - GUI, entering [1-3](#)
  - GUI user account, creating [3-10](#)
- user roles [3-5, 3-10](#)
- user view
  - answers, adding [3-18](#)
  - answers, removing [3-22](#)
  - creating [3-16](#)
  - deleting [3-25](#)
  - general configuration [3-18](#)
  - keepalives, adding [3-19](#)
  - keepalives, removing [3-22](#)
  - locations, adding [3-20](#)
  - locations, removing [3-22](#)
  - modifying [3-24](#)
  - naming [3-18](#)
  - overview [3-15](#)
  - owners, adding [3-21](#)

- owners, removing [3-22](#)
- specifying [3-11](#)
- TACACS+ server authorization [4-16](#)

---

## V

- validating database records [9-6](#)
- verifying GSSM role [A-2](#)
- version information [2-41](#)
- viewing
  - access lists [5-9](#)
  - gss.log file [8-10](#)
  - MIB files [6-9](#)
  - SNMP status [6-8](#)
  - subsystem log files [8-11](#)
  - system log [8-13](#)
  - system logs from CiscoWorks RME Syslog Analyzer [8-18](#)
  - system logs from GUI [8-14](#)
  - third-party software information [1-15](#)

---

## W

- warning log message [8-15](#)