GSS Administration and Troubleshooting

This chapter covers the procedures necessary to properly manage and maintain your GSSM and GSS devices, including login security, software upgrades, GSSM database administration, and GSSM error messages.

This chapter contains the following major sections:

- Performing Advanced GSS Configuration Tasks
- Configuring the Primary GSSM Graphical User Interface
- Printing and Exporting GSSM Data
- Configuring GSS Security
- Configuring SNMP on Your GSS Network
- Backing Up the GSSM
- Upgrading the Cisco GSS Software
- Downgrading and Restoring Your GSS Devices
- Viewing Third-Party Software Versions
- Primary GSSM Error Messages
Performing Advanced GSS Configuration Tasks

These sections describe the following advanced GSS configuration tasks:

- Logically Removing a GSS or Standby GSSM from the Network
- Changing the GSSM Role in the GSS Network
- Modifying Network Configuration Settings of a GSS
- Changing the Startup and Running Configuration Files
- Loading the Startup Configuration from an External File

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:

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

Before removing or replacing a GSS or standby GSSM, you should logically remove the GSS from the network before physically removing it.

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.

To logically remove a GSS or standby GSSM from the network, follow these steps. The first four steps in the instructions assume that the GSS or standby GSSM is operational. If that is not the case, proceed directly to step 5.

1. Log on to the CLI, following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The CLI prompt appears.

2. At the CLI prompt, enable privileged EXEC mode and then global configuration mode on the device. For example:

   `localhost.localdomain> enable`
3. If possible, use the `copy startup-config disk` command to backup the startup configuration file on the GSS or standby GSSM device. For example:

   `localhost.localdomain# copy startup-config disk configfile`

4. Use the `gss stop` command to stop the GSS software running on the GSS. For example:

   `localhost.localdomain# gss stop`

5. Use the `gss disable` command to disable the selected GSS and remove any existing configuration, including deleting the GSSM database from the GSS device. This option returns the GSS to the initial, disabled state. If the GSS device is to be powered down, also enter the `shutdown` command. For example:

   `localhost.localdomain# gss disable
   localhost.localdomain# shutdown`

6. To logically remove a GSS or a standby GSSM from the network, access the primary GSSM graphical user interface and click the Resources tab.

7. Click the Global Site Selectors navigation link. The Global Site Selectors list page appears.

8. From the Global Site Selectors list, click the Modify GSS icon located to the left of the GSS device you want to delete. The Modifying GSS details page appears.

9. 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.

10. Click OK to confirm your decision. You return to the Global Site Selectors list page with the deleted device removed from 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 a GSS or standby GSSM back into the GSS network, follow the procedures outlined in Chapter 2, Setting Up Your GSS.

After you configure the GSS or standby GSSM, you may reload the backup copy of the GSS device startup configuration settings (see the “Loading the Startup Configuration from an External File” section).
Changing the GSSM Role in the GSS Network

The GSS software supports multiple GSSMs on a single GSS network, with one GSSM acting as the primary GSSM and another GSSM acting as a standby device. The standby GSSM is capable of temporarily taking over the role as the primary GSSM is the event that 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 GSSMs at any time. Before switching GSSM roles, however, both a primary and a standby GSSM must be configured and enabled in your GSS network.

Do not attempt to switch roles before both a primary and a standby GSSM have been configured and enabled (refer to Chapter 2, Setting Up Your GSS). In addition, ensure that the designated primary GSSM is offline before you attempt to enable the standby GSSM as the new primary GSSM. Having two primary GSSMs active at the same time may result in the inadvertent loss of configuration changes for your GSS network. Although request routing continues to function in such a situation, GUI configuration changes made on one or both devices may be lost or overwritten, and may not be communicated to your GSS devices. If this dual primary GSSM configuration occurs, the two primary GSSMs change to standby mode and you will need to reconfigure one of the GSSMs as the primary GSSM.

Note that 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. The interim primary GSSM can be used to monitor GSS behavior and make configuration changes if necessary.

Switching the Roles of the Primary and Standby GSSMs

Use the following steps to change the roles of your primary and standby GSSMs. These instructions assume that your primary GSSM is online and functional at the time you are switching GSSM roles. If this is not the case (for example, the primary GSSM is not functional), ignore any steps that apply to accessing the primary GSSM.

1. Log on to the CLI of the primary GSSM, following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The CLI prompt appears.
2. Enable privileged EXEC mode. For example:
   gssm1.yourdomain.com> enable

3. If you have not already done so, perform a full backup of your primary GSSM to preserve your current network and configuration settings (see the “Performing a Full GSSM Backup” section).

4. Configure the current primary GSSM as the standby GSSM. Use the `gssm primary-to-standby` command to place the primary GSSM in standby mode. For example:
   gssm1.yourdomain.com# gssm primary-to-standby

5. If the GSSM is to be powered down, also enter the `shutdown` command. For example:
   gssm1.yourdomain.com# shutdown

6. Exit from the CLI of the GSSM.

7. Log on to the standby GSSM. You cannot log in to the GUI of the old primary GSSM once it begins acting in a standby capacity.

8. Enable privileged EXEC mode. For example:
   gssm2.yourdomain.com> enable

9. Configure the current standby GSSM to be the temporary primary GSSM for your GSS network. Use the `gssm standby-to-primary` command to enable your standby GSSM and make it the primary GSSM. For example:
   gssm2.yourdomain.com# gssm standby-to-primary

   The standby GSSM begins to function in its new role as the primary GSSM.

   **Note** The configuration changes do not take effect immediately. It can take up to five minutes for the other GSS devices in the network to learn about the new primary GSSM.

10. Exit privileged EXEC mode. The interim primary GSSM is now fully functional and you can now access the GUI.
Reversing the Roles of the Interim Primary and Standby GSSMs

To reverse the roles of the interim primary and standby GSSMs back to the original GSS network deployment (assuming both devices are online):

1. Log on to the CLI of the interim primary GSSM. The CLI prompt appears.
2. Enable privileged EXEC mode. For example:
   
   ```
   gssm2.yourdomain.com> enable
   ```

3. Perform a full backup of the interim primary GSSM to preserve the current network and configuration settings (see the “Performing a Full GSSM Backup” section).
4. Use the `gssm primary-to-standby` command to place the current interim primary GSSM in standby mode and resume its role in the GSS network as the standby GSSM. For example:
   
   ```
   gssm2.yourdomain.com# gssm primary-to-standby
   ```

5. Exit from the CLI of the standby GSSM.
6. Log on to the CLI of the primary GSSM from the original network deployment. The CLI prompt appears.
7. Enable privileged EXEC mode. For example:
   
   ```
   gssm1.yourdomain.com> enable
   ```

8. Use the `gssm standby-to-primary` command to return the GSS device back to the role as the primary GSSM in the GSS network. For example:
   
   ```
   gssm1.yourdomain.com# gssm standby-to-primary
   ```

---

**Note**

If your original primary GSSM has been replaced by Cisco Systems, contact the Cisco Technical Assistance Center (TAC).
Modifying Network Configuration Settings of a GSS

Once you have configured your GSS devices in your network, you can use the CLI to modify the configuration settings of those devices.

To modify the network configuration of a GSS device:

1. Log on to the CLI, following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

2. Enable privileged EXEC mode. For example:
   
   gssml.yourdomain.com> enable

3. Use the gss stop command to stop your GSS servers. For example:
   
   gssml.yourdomain.com# gss stop

4. Enter global configuration mode. For example:
   
   gssml.yourdomain.com# configure
   gssml.yourdomain.com(config)#

5. Use the no form of the network configuration commands to erase configuration settings. For example, to change the IP address assigned to a GSS interface, you would enter:
   
   gssml.yourdomain.com(config-eth0)# no ip address 10.89.3.24 255.255.255.0
   gssml.yourdomain.com(config-eth0)# exit
gssml.yourdomain.com(config)#

Once you have removed a GSS device setting, you can reregister it with the primary GSSM by following the instructions in Chapter 2, Setting Up Your GSS.
Changing the Startup and Running Configuration Files

The network configuration for a GSS device includes:

- Interface—Ethernet interface being used
- IP address—Network address and subnet mask assigned to the interface
- GSS communications—Which interface (Ethernet 0 or Ethernet 1) is designated for handling GSS-related communications on the device
- GSS TCP keepalives—Which interface (Ethernet 0 or Ethernet 1) is designated for outgoing keepalives of type TCP and HTTP HEAD
- Host name—Host name 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—Whether SSH is enabled on the device
- Telnet enable—Whether Telnet is enabled on the device
- FTP enable—Whether FTP is enabled on the device

Each GSS device tracks two such configurations:

- Startup configuration—The default network configuration. These configuration settings are loaded each time the device is booted.
- Running configuration—The network configuration currently being used by the GSS device.

Usually, the running configuration and the startup configuration file are identical. However, once a configuration parameter is modified for any reason, the two must be reconciled using the CLI in one of the following ways:

- The running configuration can be saved as the new startup configuration using the `copy running-config startup-config` command. Any changes to the network configuration of the device are retained and used when the device is next rebooted.
- The startup configuration can be maintained. In this case, the running configuration is used up until the point at which the device is rebooted, at which time the running configuration is discarded and the startup configuration is restored.
To change the startup configuration file for a GSS device:

1. Log on to the CLI, following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

   By default, the host name for GSS devices is localhost.localdomain. This name changes once you configure the host name for the device.

2. Enable privileged EXEC mode and then global configuration mode on the device. For example:
   
   ```
   gssm1.yourdomain.com> enable
   gssm1.yourdomain.com# config
   gssm1.yourdomain.com(config)#
   ```

3. Make any desired changes to the network configuration of the device. For example, if you wanted to change the device host name, you would use the following command:
   
   ```
   gssm1.yourdomain.com(config)# hostname new.yourdomain.com
   new.yourdomain.com(config)#
   ```

4. Use the `copy running-config startup-config` command to install the current running configuration as the new startup configuration for the device. For example:
   
   ```
   new.yourdomain.com(config)# copy running-config startup-config
   ```

5. Alternatively, use the `copy` command to achieve the same result, copying the running configuration to the startup configuration. For example:
   
   ```
   new.yourdomain.com(config)# copy running-config startup-config
   ```

### Loading the Startup Configuration from an External File

In addition to copying your running configuration as a new startup configuration, internally you can also upload or download GSS device configuration information from an external file using the `copy` command.

Before attempting 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 copy the GSS device startup configuration to or from a disk:

1. Log on to the CLI, following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

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

   Make any desired changes to the network configuration of the device. For example, if you wanted to change the device host name, you would use the following command:

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

   Use the `copy running-config startup-config` command to install the current running configuration as the new startup configuration for the device. For example:

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

   Alternatively, use the `copy` command to achieve the same result, copying the running configuration to the startup configuration. For example:

   ```
   new.yourdomain.com(config)# copy running-config startup-config
   ```
2. Enable privileged EXEC mode. For example:
   
   ```
gssm1.yourdomain.com> enable
   ```

3. Use the `copy` command to install a new startup configuration from a file. For example:
   
   ```
gssm1.yourdomain.com# copy disk startup-config filename
   ```

   where `filename` is the name of the file containing the startup configuration settings.

4. Alternatively, copy the current startup configuration to a file for use on other devices or for backup purposes. For example:
   
   ```
gssm1.yourdomain.com# copy startup-config disk filename
   ```

   where `filename` is the name of the file created to contain the startup configuration settings.

---

## Configuring the Primary GSSM Graphical User Interface

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. Among the settings you can modify are:

- **GUI Session Inactivity Timeout Enable**—Check box that enables or disables the use of the GUI Session Inactivity Timeout function.

- **GUI Session Inactivity Timeout**—Number of minutes of inactivity that must pass before your primary GSSM GUI session is automatically terminated

- **GSS Reporting Interval**—Interval (in seconds) at which GSS devices report their status to the primary GSSM

- **Monitoring Screen Refresh Interval**—Interval (in seconds) at which the primary GSSM GUI refreshes displayed content
To modify any GUI session settings:

1. From the primary GSSM GUI, click the Tools tab.

2. Click the GUI Configuration navigation link. The GUI Configuration details page appears (Figure 9-1) listing fields for modifying your GUI session settings.

3. Perform one or more of the following:
   - To adjust the amount of time without GUI activity that must pass before the primary GSSM automatically terminates the GUI session, click the GUI Session Inactivity Timeout Enable check box and enter a number in the GUI Session Inactivity Timeout field. This value is the length of time, in minutes, that passes without any user activity before the session is terminated.
To adjust the amount of time that must pass before GSS devices report their status to the primary GSSM, enter a number in the GSS Reporting Interval field. This value is the length of time, in seconds, that passes between reports.

To increase the length of time that passes between automatic screen refreshes when viewing GSS information from the primary GSSM GUI, enter a number in the Monitoring Screen Refresh Interval field. This value is the length of time, in seconds, that passes between automatic screen refreshes.

4. Click Submit to update the primary GSSM. The Transaction Complete icon appears in the lower left corner of the configuration area to inform you that the GUI session has been successfully updated.

Printing and Exporting GSSM Data

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

To print or export GSSM data:

1. From the primary GSSM GUI, navigate to the list page or details page containing the data you wish to export or print.

2. Perform one of the following:
   
   – To export the data, click the Export button. You are prompted to either save the exported data as a comma-delimited file or open it using your designated CSV editor.
   
   – To print the data, click the Print button. The Print dialog box on your workstation appears, allowing you to choose a printer.

   **Note**
   
   If you need to export the output of all configured fields from the primary GSSM GUI from the GSS CLI (intended for use by a Cisco technical support representative), specify the show tech-support config. Refer to the Cisco Global Site Selector Command Reference.
Configuring GSS Security

Using the primary GSSM GUI, you can control access to the GUI. Using the CLI, you can control login access to individual GSS devices, as well as incoming traffic to your GSS devices.

This section includes the following procedures:

- Creating and Managing GSSM Login Accounts
- Creating and Managing GSS CLI Login Accounts
- Segmenting GSS Traffic by Interface
- Filtering GSS Traffic Using Access Lists
- Deploying GSS Devices Behind Firewalls

Creating and Managing GSSM Login Accounts

Using the user administration feature of the GSSM, you can create and maintain login accounts for the primary GSSM GUI. In addition to login name and password information, the user administration feature also allows you to maintain contact information for each user.

Note

Only users who log in to the primary GSSM GUI as administrator have the privileges to create, modify, or remove a GSSM GUI account.

This section includes the following procedures:

- Creating a GSSM GUI User Account
- Modifying a GSSM GUI User Account
- Removing a GSSM GUI User Account
- Changing Your GSSM GUI Password
Creating a GSSM GUI User Account

To create a GSSM GUI user account:

1. From the primary GSSM GUI, click the Tools tab.
2. Click the User Administration navigation link. The GUI Configuration list page appears (Figure 9-2).

Figure 9-2  GSSM User Administration List Page

3. Click the Create User icon. The Creating New User details page appears (Figure 9-3).
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 Personal Information area, enter the user’s first name in the First Name field.

8. In the Last Name field, enter the user’s last name. The first and last name will be displayed next to the user’s login, whenever the user logs on to the primary GSSM.
9. Optionally, fill in the rest of the user’s contact information as follows:
   - **Job title**—User’s position within your organization
   - **Department**—User’s department
   - **Phone**—User’s business telephone number
   - **E-mail**—User’s e-mail address
   - **Comments**—Any important information or comments about the user account

10. Click **Submit** to create your new user account. You return to the User Administration list page.

### Modifying a GSSM GUI User Account

To modify an existing GSSM user account:

1. From the primary GSSM GUI, click the **Tools** tab.
2. Click the **User Administration** navigation link. The GUI Configuration list page appears (see Figure 9-2) listing existing user accounts.
3. Click the **Modify User** icon to the left of the user account that you wish to modify. The Modifying User details page appears (see Figure 9-3) listing fields for modifying your GUI session settings.
4. Use the fields provided to modify the user’s account, as follows:
   - **Username**—Change the account’s login name.
   - **Password/Retype password**—Modify the login password for the account; new passwords must be entered identically in both fields before they are accepted.
   - **First name**—Modify the user’s first name.
   - **Last name**—Modify the user’s last name.
   - **Job title**—Modify the user’s listed position within your organization.
   - **Department**—Modify the user’s department.
   - **Phone**—Modify the user’s business phone number.
   - **E-mail**—Modify the user’s e-mail address.
   - **Comments**—Modify comments on the user account.
5. Click Submit to save changes to the account. You return to the GSSM User Administration list page.

Removing a GSSM GUI User Account

To delete an existing GSSM GUI user account:

1. From the primary GSSM GUI, click the Tools tab.
2. Click the User Administration navigation link. The GUI Configuration list page appears (see Figure 9-2) listing existing user accounts.
3. Click the Modify User icon to the left of the user account that you wish to remove. The Modifying User details page appears (see Figure 9-3), displaying that user’s account information.

Note You cannot delete the admin account.

4. Click the Delete icon. The software prompts you to confirm your decision to permanently delete the user.
5. Click OK. You return to the GSSM User Administration list page with the user account removed.

Changing Your GSSM GUI Password

Using the change password feature of the primary GSSM GUI, you can change the password for the account that you used to log on to the primary GSSM. You must know the existing password for an account before you can change it to a new value.

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 the password back to “default” by entering the reset-gui-admin-password CLI command. Refer to the Cisco Global Site Selector Command Reference for details on using this command.

To change your account password:

1. From the primary GSSM GUI, click the Tools tab.
2. Click the **Change Password** navigation link. The Change Password detail page (Figure 9-4) appears displaying your account name in the Username field

![Figure 9-4 GSSM Change Password Details Page](image)

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 is used to verify that you have entered your password correctly.
6. Click **Submit** to update your login password.
Creating and Managing GSS CLI Login Accounts

Using the CLI, you can set user access for each of your GSS devices, including the GSSM. User access to the CLI of your GSSs must be managed individually on each device.

**Note**
Only the admin account can create and manage GSS logins.

This section includes the following procedures:
- Creating a GSS User Account Using the CLI
- Modifying a GSS User Account Using the CLI
- Deleting a GSS User Account Using the CLI

Creating a GSS User Account Using the CLI

When creating user accounts from the CLI, you must specify the new login, password, and privilege level using a single command. You cannot create a new account without designating a value for each of these configuration settings. Refer to the *Cisco Global Site Selector Command Reference* for detailed information on the `username` command.

To create a user or administrative login account that can access the CLI of one of your GSS devices:

1. Log on to the CLI, following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.
2. Enable privileged EXEC mode and then global configuration mode on the device. For example:

   ```
   gss1.yourdomain.com> enable
   gss1.yourdomain.com# config
   gss1.yourdomain.com(config)#
   ```

3. Use the `username` command to create and configure your new login account and then press Enter to create the account. For example:

   ```
   gss1.yourdomain.com(config)# username paulr password mypwd
   privilege admin
   ```
   User paulr added.
For a login name, enter an unquoted alphanumeric text string with no spaces and a maximum of 32 characters. Login names must start with an alpha character (for example, A-Z or a-z). The GSS does not support usernames that begin with a numerical value. For a password, enter an unquoted text string with no spaces and a maximum length of 8 characters. To create an administrative account, set the privilege level to `admin`. To create a user account, set the privilege level to `user`.

4. Repeat step 3 for each new user account that you wish to create.

**Modifying a GSS User Account Using the CLI**

When modifying a GSS user account using the CLI, use the same procedure that you used to create the account: entering the full username, password, and privilege level and substituting new values for the configuration settings that you wish to change.

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

2. Enable privileged EXEC mode and then global configuration mode on the device. For example:

   ```
gss1.yourdomain.com> enable
  gss1.yourdomain.com# config
  gss1.yourdomain.com(config)#
  ```

3. Use the `username` command to modify your new login account and then press Enter to input the new values. For example:

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

4. Repeat step 3 for each new user account that you wish to modify.

**Deleting a GSS User Account Using the CLI**

You must have administrative-level access to the GSS to delete login accounts. To delete a login account:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.
2. Enable privileged EXEC mode and then global configuration mode on the device. For example:

```
gss1.yourdomain.com> enable
gss1.yourdomain.com# config
gss1.yourdomain.com(config)#
```

3. Use the `username` command to delete an existing login account. For example:

```
gss1.yourdomain.com#(config) username paulr delete
User paulr removed
```

**Note** You cannot delete the admin account.

4. Repeat step 3 for each new user account that you wish to delete.

**Resetting the CLI Administrator Account Password**

If you accidentally 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.

**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 the password back to “default” by entering the `reset-gui-admin-password` CLI command. Refer to the *Cisco Global Site Selector Command Reference* for details on using this command.

To reset the CLI administrator account password:

1. Attach an ASCII terminal to the GSS console port, following the instructions in the “Connecting Cables” section of Chapter 3 in the *Cisco Global Site Selector Hardware Installation Guide*.

2. If the GSS device is currently up and running, enter the `reload` command to halt and perform a cold restart of your GSS device. For example:

```
Host# reload
```

As the GSS reboots, 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`. Use care when entering this command; this CLI command is case-sensitive. For example:

```
boot: GSS-1.1.0
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 again. Pay close attention when you enter the `GSS-<software_version> RESETADMINCLIPW=1` command.

---

### Segmenting GSS Traffic by Interface

GSS devices include two Ethernet interfaces. By default, GSS servers listen for DNS traffic on both Ethernet interfaces.

Note
---

In the case of inter-GSS communications, GSS devices listen for configuration and status updates on one interface only, which is the first Ethernet interface (eth 0) by default. You can use the `gss-communications` command to configure which interface is used for interdevice communications on the GSS network. Refer to the *Cisco Global Site Selector Command Reference* for instructions on using the `gss-communications` command.
However, for security reasons you may wish to limit GSS traffic to one interface, or segment traffic by constraining a certain type of traffic on a designated interface. Using the **access-list** and **access-group** commands discussed in the “Filtering GSS Traffic Using Access Lists” section, you can use access lists to limit traffic on either of your GSS interfaces.

For example, network management services like Telnet, SSH, and FTP listen on all active interfaces once they are enabled. To force these remote management servers to listen on only the second Ethernet interface, you would use the following CLI commands:

```
gss1.yourdomain.com> enable
gss1.yourdomain.com#
gss1.yourdomain.com# config
gss1.yourdomain.com(config)#
gss1.yourdomain.com(config)# access-list alist1 permit tcp any destination-port ftp
gss1.yourdomain.com(config)# access-list alist1 permit tcp any destination-port ssh
gss1.yourdomain.com(config)# access-list alist1 permit tcp any destination-port telnet
gss1.yourdomain.com(config)# access-group alist1 interface eth1
```

By default, the above commands would limit the second interface (eth1) to the specified traffic. All other traffic to that interface would be refused.

To deny the same traffic on the first interface (eth0), you would use the following commands:

```
gss1.yourdomain.com(config)#
gss1.yourdomain.com(config)# access-list alist1 deny tcp any destination-port ftp
gss1.yourdomain.com(config)# access-list alist1 deny tcp any destination-port ssh
gss1.yourdomain.com(config)# access-list alist1 deny tcp any destination-port telnet
gss1.yourdomain.com(config)# access-group alist1 eth0
```
Filtering GSS Traffic Using Access Lists

Using built-in packet filtering features on the GSS, you can instruct your GSSs and GSSMs to permit or refuse specific packets that are received based on a combination of criteria that includes:

- Destination port of the packets
- Requesting host
- Protocol used (TCP, User Datagram Protocol [UDP], or ICMP)

These packet-filtering tools, called *access lists*, are created and maintained from the GSS CLI. Access lists are essentially collections of filtering rules that are created using the `access-list` CLI command and can be applied to one or both of your GSS interfaces using the `access-group` command.

Each access list is a sequential collection of permit and deny conditions that apply to a source network IP address to control whether routed packets are forwarded or blocked at the GSS. The GSS examines each packet to determine whether to forward or drop the packet based on the criteria you specified within the access lists.

Note that each additional criteria statement that you enter is appended to the *end* of the access list statements. Also note that you cannot delete individual statements after they have been created. You can only delete an entire access list.

The order of access list statements is important. When the GSS is deciding whether to forward or block a packet, the software tests the packet against each criteria statement in the order the statements were created. After a match is found, no more criteria statements are checked.

If you create a criteria statement that explicitly permits all traffic, no statements added later will ever be checked. If you need additional statements, you must delete the access list and retype it with the new entries.

For detailed information on access list syntax options, refer to the `access-list`, `access-group`, and `show access-list` commands in the *Cisco Global Site Selector Command Reference*. 
This section includes the following procedures:

- 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
- Viewing Access Lists

### Creating an Access List

The term access list simply refers to one or more filtering rules that are grouped together. You can create any number of access lists on a given GSS device. After you have created an access list, rules can be appended to or removed from the list at any time.

To ensure your GSS functions properly with access lists, identify the ports and protocols normally used by each GSS device. Table 9-1 illustrates the types of expected inbound traffic received by the GSS.

<table>
<thead>
<tr>
<th>Source Port (Remote Device)</th>
<th>Destination Port (GSS)</th>
<th>Protocol</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>20–23</td>
<td>TCP</td>
<td>FTP, SSH, and Telnet server services on the GSS</td>
</tr>
<tr>
<td>20, 21, 23</td>
<td>*</td>
<td>TCP</td>
<td>Return traffic of FTP and Telnet GSS CLI commands</td>
</tr>
<tr>
<td>*</td>
<td>53</td>
<td>UDP, TCP</td>
<td>GSS DNS server traffic</td>
</tr>
<tr>
<td>53</td>
<td>*</td>
<td>UDP</td>
<td>GSS software reverse lookup and “dnslookup” queries</td>
</tr>
<tr>
<td>123</td>
<td>123</td>
<td>UDP</td>
<td>Network Time Protocol (NTP) updates</td>
</tr>
<tr>
<td>*</td>
<td>161</td>
<td>UDP</td>
<td>Simple Network Management Protocol (SNMP) traffic</td>
</tr>
</tbody>
</table>
Configuring GSS Security

Table 9-1  GSS-Related Ports and Protocols (Inbound Traffic)

<table>
<thead>
<tr>
<th>Source Port (Remote Device)</th>
<th>Destination Port (GSS)</th>
<th>Protocol</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>443</td>
<td>TCP</td>
<td>Primary GSSM GUI</td>
</tr>
<tr>
<td>1304</td>
<td>1304</td>
<td>UDP</td>
<td>CRA keepalives</td>
</tr>
<tr>
<td>*</td>
<td>2000</td>
<td>UDP</td>
<td>Inter-GSS periodic status reporting</td>
</tr>
<tr>
<td>*</td>
<td>2001–2009</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
<tr>
<td>2001–2009</td>
<td>*</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
<tr>
<td>*</td>
<td>3001–3009</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
<tr>
<td>3001–3009</td>
<td>*</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
<tr>
<td>5002</td>
<td>*</td>
<td>UDP</td>
<td>KAL-AP keepalives</td>
</tr>
</tbody>
</table>

*Any legal port number.

To create an access list:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

   Note You need access to the CLI of your GSS devices to create access lists.

2. Enable privileged EXEC mode and access configuration mode. For example:
   
   gss1.yourdomain.com> enable
gss1.yourdomain.com#
gss1.yourdomain.com# config
gss1.yourdomain.com(config)#

3. Use the access-list command to create your first access list.

   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.yourdomain.com# config
gss1.yourdomain.com(config)# access-list alist1 permit tcp any destination-port eq 443
Refer to the *Cisco Global Site Selector Command Reference* for an explanation of `access-list` command syntax.

4. Repeat step 3 for each access list that you wish to add to this device, or see the “Adding Rules to an Access List” section for instructions on adding more rules to an access list that already exists.

### Associating an Access List with a GSS Interface

After you have created an access list, you must associate it with one or both of your GSS interfaces before it can be used to filter incoming traffic to that interface.

When no access lists are associated with an interface, all incoming traffic is allowed on that interface. After an access list has been applied, only the type of traffic explicitly permitted by that list is allowed. All other traffic is disallowed.

The `access-group` command is used to associate an access list with a GSS interface.

**Note**

You need access to the CLI of your GSS devices to associate access lists with GSS interfaces.

To associate access lists with a GSS interface:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

2. Enable privileged EXEC mode and access configuration mode. For example:

```bash
gss1.yourdomain.com> enable
gss1.yourdomain.com# config
```

3. Use the `access-group` command to associate an access list with the GSS interface. For example, to associate the access list named `alist1` with the first interface on your GSS device, you would enter the following:

```bash
access-group alist1 interface eth0
```

Refer to the *Cisco Global Site Selector Command Reference* for an explanation of `access-group` command syntax.

4. Repeat step 3 for each access list that you wish to associate with an interface.
Disassociating an Access List from a GSS Interface

After you have associated an access list with one or more of your GSS interfaces, you can dissociate it from that interface using the `no` form of the `access-group` command. Disassociating an access list from an interface removes any constraints that the list applied to traffic to that interface.

**Note**

You need to be able to access the CLI of your GSS devices to disassociate access lists from GSS interfaces.

To disassociate an access list from an interface:

1. Log on to the CLI, following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.
2. Enable privileged EXEC mode and access configuration mode. For example:
   ```
   gss1.yourdomain.com> enable
   gss1.yourdomain.com#
   gss1.yourdomain.com# config
   gss1.yourdomain.com(config)#
   ```
3. Use the `no access-group` command to disassociate an access list from your GSS interface. For example, to disassociate the access list named `alist1` from the first interface on your GSS device, you would enter the following:
   ```
   gss1.yourdomain.com(config)# no access-group alist1 interface eth0
   ```
   Refer to the *Cisco Global Site Selector Command Reference* for an explanation of `access-group` and `no access-group` command syntax.
4. Repeat step 3 for each access list that you wish to disassociate from an interface.

Adding Rules to an Access List

Once you have created one or more access lists, you can append rules to them at any time.

To add a rule to an access list:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.
2. Enable privileged EXEC mode and access configuration mode. For example:
   
   ```
gss1.yourdomain.com> enable
gss1.yourdomain.com#
gss1.yourdomain.com# config
gss1.yourdomain.com(config)#
   ```

3. 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` that blocks all traffic from host 192.168.1.101, you would enter the following:
   
   ```
gss1.yourdomain.com(config)# access-list alist1 deny tcp host 192.168.1.101
   ```

   Refer to the *Cisco Global Site Selector Command Reference* for an explanation of `access-list` command syntax.

4. Use the `show access-list` command to verify that the rule has been added to your access list. For example:
   
   ```
gss1.yourdomain.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
   ```

5. Repeat steps 3 and 4 for each rule that you wish to add to this access list.

### Removing Rules from an Access List

Once you have created one or more access lists, you can remove rules from them at any time. 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 access list:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

2. Enable privileged EXEC mode and access configuration mode. For example:
   
   ```
gss1.yourdomain.com> enable
gss1.yourdomain.com#
gss1.yourdomain.com# config
gss1.yourdomain.com(config)#
   ```
3. Use the no form of the access-list command to remove a rule from an existing access list. For example, to remove the rule from the access list named \textit{alist1} that blocks all traffic from host 192.168.1.101, you would enter the following:

\begin{verbatim}
gss1.yourdomain.com(config)# no access-list alist1 deny tcp host 192.168.1.101
\end{verbatim}

Refer to the \textit{Cisco Global Site Selector Command Reference} for an explanation of access-list command syntax.

4. Use the show access-list command to verify that the rule has been removed from your access list. For example:

\begin{verbatim}
gss1.yourdomain.com(config)# show access-list
access-list:alist1
access-list alist1 permit tcp any destination-port eq 443
\end{verbatim}

5. Repeat steps 3 and 4 for each rule that you wish to remove from this access list, or from others configured on your system.

\section*{Viewing Access Lists}

Use the show access-list command to view configured access lists. For example:

\begin{verbatim}
gss1.yourdomain.com(config)# show access-list
access-list:alist1
access-list alist1 permit tcp any destination-port eq 443
\end{verbatim}

\section*{Deploying GSS Devices Behind Firewalls}

In addition to the packet-filtering features of the access-list and access-group commands discussed in the “Filtering GSS Traffic Using Access Lists” section, you can also deploy your GSS devices behind an existing firewall on your enterprise network.

The GSS does not support deployment of devices behind a NAT for inter-GSS communication. The communication between the GSSs cannot include an intermediate device behind a NAT because the actual IP address of the devices is embedded in the payload of the packets.
When configuring your GSS for deployment behind a firewall, at a minimum you will need to allow DNS traffic into the box. If you have multiple GSSs deployed such that traffic between them must pass through a firewall, then you must configure the firewall to also allow inter-GSS communications, and inter-GSS status reporting. Whether you need to allow other traffic in Table 9-2 and Table 9-3 will depend on your GSS configuration (for example, whether you are using KAL-AP keepalives) and your need access to certain GSS services through the firewall (for example, SNMP).

To configure your firewall to work with the GSS product, follow the guidelines in Table 9-2 and Table 9-3 to permit inbound and outbound traffic to and from the specified GSS ports. You may also want to use the `access-list` and `access-group` commands to enable authorized GSS traffic to the specified ports. By default, all ports not explicitly permitted in your access list are blocked by that interface once the list is associated.

### Table 9-2  Inbound Traffic Going Through a Firewall to the GSS

<table>
<thead>
<tr>
<th>Source Port (Remote Device)</th>
<th>Destination Port (GSS)</th>
<th>Protocol</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>20–23</td>
<td>TCP</td>
<td>FTP, SSH, and Telnet server services on the GSS</td>
</tr>
<tr>
<td>20, 21, 23</td>
<td>*</td>
<td>TCP</td>
<td>Return traffic of FTP and Telnet GSS CLI commands</td>
</tr>
<tr>
<td>*</td>
<td>53</td>
<td>UDP, TCP</td>
<td>GSS DNS server traffic</td>
</tr>
<tr>
<td>53</td>
<td>*</td>
<td>UDP</td>
<td>GSS software reverse lookup and “dnslookup” queries</td>
</tr>
<tr>
<td>123</td>
<td>123</td>
<td>UDP</td>
<td>Network Time Protocol (NTP) updates</td>
</tr>
<tr>
<td>*</td>
<td>161</td>
<td>UDP</td>
<td>Simple Network Management Protocol (SNMP) traffic</td>
</tr>
<tr>
<td>*</td>
<td>443</td>
<td>TCP</td>
<td>Primary GSSM GUI</td>
</tr>
<tr>
<td>1304</td>
<td>1304</td>
<td>UDP</td>
<td>CRA keepalives</td>
</tr>
<tr>
<td>*</td>
<td>2000</td>
<td>UDP</td>
<td>Inter-GSS periodic status reporting</td>
</tr>
<tr>
<td>*</td>
<td>2001–2009</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
<tr>
<td>2001–2009</td>
<td>*</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
</tbody>
</table>
### Table 9-2 Inbound Traffic Going Through a Firewall to the GSS (continued)

<table>
<thead>
<tr>
<th>Source Port (Remote Device)</th>
<th>Destination Port (GSS)</th>
<th>Protocol</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>3001–3009</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
<tr>
<td>3001–3009</td>
<td>*</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
<tr>
<td>5002</td>
<td>*</td>
<td>UDP</td>
<td>KAL-AP keepalives</td>
</tr>
</tbody>
</table>

*Any legal port number.

### Table 9-3 Outbound Traffic Originating from the GSS

<table>
<thead>
<tr>
<th>Source Port (GSS)</th>
<th>Destination Port (Remote Device)</th>
<th>Protocol</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>20–23</td>
<td>*</td>
<td>TCP</td>
<td>Return traffic of FTP, SSH, and Telnet server services on the GSS</td>
</tr>
<tr>
<td>*</td>
<td>20, 21, 23</td>
<td>TCP</td>
<td>Traffic of FTP and Telnet GSS CLI commands</td>
</tr>
<tr>
<td>53</td>
<td>*</td>
<td>UDP, TCP</td>
<td>GSS DNS server traffic</td>
</tr>
<tr>
<td>*</td>
<td>53</td>
<td>UDP</td>
<td>GSS software reverse lookup and “dnslookup” queries</td>
</tr>
<tr>
<td>123</td>
<td>123</td>
<td>UDP</td>
<td>Network Time Protocol (NTP) updates</td>
</tr>
<tr>
<td>161</td>
<td>*</td>
<td>UDP</td>
<td>Simple Network Management Protocol (SNMP) traffic</td>
</tr>
<tr>
<td>443</td>
<td>*</td>
<td>TCP</td>
<td>Primary GSSM GUI</td>
</tr>
<tr>
<td>1304</td>
<td>1304</td>
<td>UDP</td>
<td>CRA keepalives</td>
</tr>
<tr>
<td>*</td>
<td>2000</td>
<td>UDP</td>
<td>Inter-GSS periodic status reporting</td>
</tr>
<tr>
<td>*</td>
<td>2001–2009</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
<tr>
<td>2001–2009</td>
<td>*</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
<tr>
<td>*</td>
<td>3001–3009</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
</tbody>
</table>
Chapter 9  GSS Administration and Troubleshooting

Configuring SNMP on Your GSS Network

Table 9-3  Outbound Traffic Originating from the GSS (continued)

<table>
<thead>
<tr>
<th>Source Port (GSS)</th>
<th>Destination Port (Remote Device)</th>
<th>Protocol</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>3001-3009</td>
<td>*</td>
<td>TCP</td>
<td>Inter-GSS communication</td>
</tr>
<tr>
<td>*</td>
<td>5002</td>
<td>UDP</td>
<td>KAL-AP keepalives</td>
</tr>
</tbody>
</table>

*Any legal port number.

To configure your GSS devices to function behind a firewall:

1. Determine what level of access and what services you wish to enable on your GSSs and GSSMs. Determine whether you want to allow FTP, SSH, and Telnet access to the device, or do you wish to permit GUI access to your primary GSSM.

   Table 9-2 and Table 9-3 show which GSS-related ports and protocols must be enabled for the product to function properly.

2. Construct your access lists to filter traffic coming to and from your GSS device.

Configuring SNMP on Your GSS Network

Your GSS or GSSM contains an Simple Network Management Protocol (SNMP) agent, ucd-snmp v4.2.3, that enables you to query your GSS devices for standard MIB resources found in MIB-II (RFC-1213) and HOST-RESOURCE-MIB (RFC-1514). SNMP runs on GSS port 161 by default.

MIB-II and HOST-RESOURCE-MIB definitions can be obtained from the following Cisco FTP sites:

ftp://ftp.cisco.com/pub/mibs/v1

Before you can begin using SNMP to monitor your GSS or GSSM, however, you must first enable the SNMP agent on your GSS device.
This section includes the following procedures:

- Configuring SNMP on Your GSS
- Viewing SNMP Status
- Viewing MIB Files on the GSS

### Configuring SNMP on Your GSS

To enable and configure the SNMP agent on your GSS device:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

2. Enable privileged EXEC mode and access configuration mode. For example:

```bash
gss1.yourdomain.com> enable
gss1.yourdomain.com#
gss1.yourdomain.com# config
gss1.yourdomain.com(config)#
```

3. Use the `snmp enable` command to enable the SNMP agent. For example:

```bash
gss1.yourdomain.com(config)# snmp enable
```

4. Use the `snmp community-string` command to specify a SNMP community name for this GSS device. By default, the SNMP community string is `public`. To change the SNMP community string, enter an unquoted text string with no space and a maximum length of 12 characters. For example:

```bash
gss1.yourdomain.com(config)#snmp community-string
Enter new Community String:
```

5. Use the `snmp contact` command to specify the name of the contact person for this GSS device. You can also include information on how to contact the person; for example, a phone number or e-mail address. Enter an unquoted text string with a maximum of 255 characters including spaces. For example:

```bash
gss1.yourdomain.com(config)#snmp contact
Enter new Contact Info: Cisco Systems, Inc.
```
6. Use the `snmp location` command to specify the physical location of this GSS device. Enter an unquoted text string with a maximum length of 255 characters. For example:

```bash
gss1.yourdomain.com(config)# snmp location
Enter new Location Info: Boxborough, MA 01719
```

7. To disable SNMP or any of the parameters outlined above, use the `no` form of the `snmp` command. For example, to disable SNMP for the GSS, enter:

```bash
gss1.yourdomain.com(config)# no snmp enable
```

### Viewing SNMP Status

Once SNMP is enabled, you can display the Simple Network Management Protocol (SNMP) operating status on your GSS device using the `show snmp` command.

To view the operating status of SNMP on your GSS device:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

2. Enable privileged EXEC mode. For example:

```bash
gss1.yourdomain.com> enable
```

3. Use the `show snmp` command to verify that your SNMP agent, ucd-snmp, is enabled or disabled, as well as the community-string, location and contact. For example:

```bash
Host# show snmp
snmp is enabled
snmp settings
-------------
Community String = <set>
Location = Boxborough MA
Contact = Cisco Systems
```

Note: You can also use the `gss status` command to verify if SNMP is enabled or disabled.

4. See the “Configuring SNMP on Your GSS” section to change the status of your SNMP agent.
Viewing MIB Files on the GSS

If necessary, you can view the GSS MIB files contained in the /mibs directory on the GSS. The GSS includes a set of standard MIB resources found in MIB-II (RFC-1213) and HOST-RESOURCE-MIB (RFC-1514). MIB-II and HOST-RESOURCE-MIB definitions can be obtained from the following Cisco FTP sites:

ftp://ftp.cisco.com/pub/mibs/v1

If you need to copy the MIBs, use the ftp or scp commands.

To view the GSS MIB files:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

2. Enable privileged EXEC mode. For example:

   gssl.yourdomain.com> enable
   gssl.yourdomain.com#

3. Use the dir command to view the list of GSS MIBs contained in the /mibs directory. For example:

   gss.cisco.com#dir /mibs
   total 1100
   drwxr-xr-x  2 root  root  4096 Jul 18 08:45 .
   drwxr-xr-x 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
   -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-TC-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
4. If desired, use the `ftp` or `scp` command to copy the MIB files from the `/mibs` directory on the GSS to another location on the GSS or to a remote network location.

### Backing Up the GSSM

The GSSM database of your primary GSSM is the heart of your GSS network. 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.

Because it is so important to the continued operation of your GSS network, it is important that you make 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 survive, and your GSSM can be quickly restored to operation.

The two types of backups that you can perform are:

- **Full**—Backs up the GSSM network configuration settings as well as the GSSM database holding GSLB configuration information
- **Database**—Backs up just the primary GSSM database
We recommend that you always perform a full backup of the GSSM. From a full backup, you can later restore the same information that is contained in a database-only backup in addition to GSSM platform information (if desired). You do not have the option of restoring GSSM platform information from a database-only backup. The full backup provides you with the flexibility to pick and choose the specific GSSM configuration information you want to restore on the GSSM.

Whenever you execute a backup on your primary GSSM, the GSS software automatically creates a tar archive (“tarball”) of the necessary files. If you are performing a full backup, this file has the .full extension. If you are performing a database backup, the file has the .db extension.

When you execute a database restore on your primary GSSM, this archive is automatically unpacked and the database is copied to the GSSM, overwriting the failed database that is there.

Backing up your GSSM database requires access to the GSS CLI and the completion of the following actions:

1. Determining the appropriate time to back up your GSSM
2. Determining whether you need to perform a full backup or database-only backup
3. Performing the backup
4. Moving the backup file to a secure location on your network

This section includes the following procedures:

- Determining When and What Type of Backup to Perform
- Performing a Full GSSM Backup
- Performing a GSSM Database Backup
Determining When and What Type of Backup to Perform

Some general guidelines exist for when and how to back up your primary GSSM. If followed, they help ensure that you are never caught unprepared if you suffer a catastrophic loss of your GSSM.

When to Perform a Full Backup

You should perform a full backup of your GSSM in these situations:

- Before switching GSSM roles, making the standby GSSM your 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

When to Perform a Database Backup

You should perform a database backup of your GSSM in these situations:

- After you make any changes in the device configuration of any of your GSS devices using the GSSM GUI
- After you make any changes to the GSLB configuration of your GSS network using the GSSM GUI. For example, adding or removing an answer, source address list, DNS rule, or user account

Performing a Full GSSM Backup

You can perform a full primary GSSM backup at any time. Performing a full backup of the primary GSSM requires access to the CLI.

To perform a full backup of your primary GSSM:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.
2. Enable privileged EXEC mode. For example:

   gssl.yourdomain.com> enable
   gssl.yourdomain.com#
3. Use the **gssm database validate** command to verify the integrity of your existing database.

   gssml.yourdomain.com# **gssm database validate**
   gssml.yourdomain.com#

4. Use the **gssm backup** command to create a full backup of your primary GSSM. You need to supply a filename for your full backup. For example:

   gssml.yourdomain.com# **gssm backup full gssmfullbk**
   GSSM database backup succeeded [gssmfullbk.full]

5. Copy or move the backup file off your primary GSSM after you receive confirmation that the GSSM successfully created your full backup. This ensures that the backup is not lost if a media failure or other catastrophic loss occurs on your primary GSSM.

   Either the secure copy (**scp**) or **ftp** command can be used to move your full backup to a remote host. For example:

   gssml.yourdomain.com# **scp gssmfullbk.full username@server.yourdomain.com:~/**

---

### Performing a GSSM Database Backup

You can perform a database backup at any time. Backing up the primary GSSM database requires access to the GSS CLI.

To perform a database backup of your primary GSSM:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

2. Enable privileged EXEC mode. For example:

   gssml.yourdomain.com> **enable**
   gssml.yourdomain.com#

3. Use the **gssm backup** command to create backup your primary GSSM database. You need to supply a filename for your database backup. For example:

   gssml.yourdomain.com# **gssm backup database gssmdbbk**
   GSSM database backup succeeded [gssmdbbk.db]
4. Copy or move the backup file off your primary GSSM after you receive confirmation that the GSSM successfully created your full backup. This ensures that the backup is not lost if a media failure or other catastrophic loss occurs on your primary GSSM.

Either the secure copy (**scp**) or **ftp** command can be used to move your database backup to a remote host. For example:

```bash
$ gssm1.yourdomain.com# scp gssmdbbk.db server.yourdomain.com:home
```

### Upgrading the Cisco GSS Software

To upgrade to a new software version, you must have access to the GSS download area of the Cisco software download site and to Cisco.com. You must 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.

The GSS software upgrade requires that you complete the following procedures in the order listed below:

1. **Verifying the GSSM Role in the GSS Network**
2. **Backing up and Archiving the Primary GSSM**
3. **Obtaining the Software Upgrade**
4. **Upgrading Your GSS Devices**
Verifying the GSSM Role in the GSS Network

You can reconfigure the standby GSSM to operate as an interim primary GSSM in the event that 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). Note that 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. Before you continue with the upgrade procedure, verify that the roles of the designated primary and standby GSSMs have not changed.

To verify the role of the current primary GSSM and the standby GSSM:

1. At the CLI of the current primary GSSM, enter the following commands:

   gssm1.yourdomain.com# cd /home
   gssm1.yourdomain.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, note the following:
   - 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. Proceed to 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 GSSMs” section.
   - 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. Proceed to 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. That way, if necessary, you can quickly restore your GSS network to its previous state. You can perform a full backup at any time. Doing so does not interfere with the functions of the primary GSSM or other GSS devices.

See the “Performing a Full GSSM Backup” section 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. Proceed to 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.

To acquire the software update from Cisco, you must:

- 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 before attempting to download a software update from Cisco.com. To acquire a Cisco.com login, go to [http://www.cisco.com](http://www.cisco.com) and click the Register link.
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:

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. Select the Content Networking Software link from the Software Center - Software Products and Downloads page.
   d. Select the Cisco Global Site Selector link from the Software Center - Content Networking page.
   e. Select 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.

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. You must complete this step to access and download Global Site Selector software images.
3. Locate the .upg file you wish to download by referring to the Release column for the proper release version of the software.

**Note**  The meta file, originally posted for use with GSS version 1.0, is no longer posted for version 1.1(0) and subsequent releases. The meta file is unnecessary for the installation, and is only used as a check to let you verify the file size of the upgrade file. The Cisco Global Site Selector Software download page contains information on the GSS file size, the MD5 checksum, and other important details about the GSS software upgrade file. Use this file information to verify the integrity of the software upgrade file.

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 displaying the agreement and return to the Software Download page.

7. Click the filename link labeled **Download**. If prompted, 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. Proceed to the “Upgrading Your GSS Devices” section.

---

**Upgrading Your GSS Devices**

You must upgrade your GSS devices in the following sequence: the primary GSSM first, followed by the other GSS devices in your network. After you upgrade the primary GSSM, ensure that the GSS device in your network being upgraded has connectivity to the primary GSSM before you perform the software upgrade procedure.
When executing an upgrade, use the CLI `install` command. Before proceeding with the installation of the software upgrade, the `install` command also 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):

1. Log on to the CLI of the GSS device.
2. 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 might look like the following:

```
ftp>
binary
ftp> get (remote-file) gss.upg (local-file) gss.upg
local: gss.upg remote: gss.upg
```

3. Enable privileged EXEC mode. For example:

```
gssm1.yourdomain.com> enable
```

4. Enter the `gss stop` command to stop your GSS servers. For example:

```
gssm1.yourdomain.com# gss stop
```
5. Enter the **install** command to install the upgrade. For example:

   gssm1.yourdomain.com# **install gss.upg**

6. At the **Proceed with install (the device will reboot)? (y/n):** prompt, type **y** to reboot the GSS device. When the GSS reboots, you lose any network CLI connections. Console connections remain active.

7. If you did not previously save changes to the startup-configuration file, the **Save current configuration? [y/n]:** prompt appears. Type **y** to continue. The GSS reboots.

8. After the GSS device reboots, log on to the device and enable privileged EXEC mode.

9. Enter the **gss status** command and verify that the GSS device reaches a Normal Operation state of runmode 4 or 5.

10. Repeat this procedure for the remaining GSS devices in your network.
Downgrading and Restoring Your GSS Devices

If you encounter problems with a software upgrade, you can always restore an earlier version of the GSS software on your GSSs and GSSMs.

However, to restore an earlier version of your software, you must have backed up a version of your GSSM database that corresponds to that version. In other words, if you wish to downgrade from GSS Release 3 to GSS Release 1 software, there must be a GSS Release 1 database backup that you can restore; your GSS Release 3 database cannot run on the Release 1 platform because of changes in the database schema between releases.

We recommend that you always perform a full backup of the GSSM. From a full backup, you can restore the same information that is contained in a database-only backup in addition to GSSM platform information (if desired). You do not have the option of restoring GSSM platform information from a database-only backup. The full backup provides you with the flexibility to pick and choose the specific GSSM configuration information you want to restore on the GSSM.

When downgrading, use the following order of operations to safeguard your critical GSS data and properly restore your GSSM database:

1. Verify the current software version.
2. Perform a full backup of your primary GSSM.
3. Obtain the software downgrade (.upg) file.
4. Downgrade your GSS device.
5. Verify your downgrade.

In addition, do not attempt to restore an earlier version of the software than the earliest database backup you have available. For example, if the earliest version of the GSS software that you have run is Release 2.0 and your earliest database backup is for Release 2.0, do not attempt to downgrade to a release of the software earlier than 2.0.

This section includes the following procedures:

- Restoring an Earlier Software Version on Your GSS Devices
- Restoring Your GSSM from a Full Backup
- Restoring Your GSSM Database from a Database-Only Backup
Restoring an Earlier Software Version on Your GSS Devices

To restore an earlier version of your GSS software, follow the instructions in the "Verifying the GSSM Role in the GSS Network" and "Upgrading Your GSS Devices" sections to acquire and then install the earlier software upgrade.

After you have downgraded the software on your GSSM, see the "Restoring Your GSSM from a Full Backup" section to restore your backed up GSSM database.

Restoring Your GSSM from a Full Backup

When restoring the GSSM from a full backup as opposed to a database backup, you use the last full backup to restore the GSS device’s network configuration settings as well as the encryption keys that are used to communicate with other GSS devices. Restoring the GSSM from a full backup should be done when you need to return the device to its exact configuration as of the last full backup. It is not necessary if you are simply rolling back the device to an earlier software version.

Use the following procedure to restore an earlier version of the GSSM from a full backup:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

2. Verify that your full backup of the GSSM is at a location that is accessible from the GSSM that you are restoring. Full backups have a .full file extension.

3. Enable privileged EXEC mode. For example:
   ```
   gssl.yourdomain.com> enable
   gssl.yourdomain.com#
   ```

4. Stop the GSS software on the GSSM and then use the gss status command to confirm that the GSSM has stopped. For example:
   ```
   atcrl.cisco.com# gss stop
   atcrl.cisco.com# gss status
   Cisco GSS - 1.1(0.0.1) - [Mon Sep 15 11:33:47 UTC 2003]
   gss is not running.
   ```
5. Once the GSSM has stopped, use the `gssm restore` command to restore the GSSM from the full backup file. To restore the file `gssmfullbk.full`, you would enter:

```
gss1.yourdomain.com# gssm restore gssmfullbk.full
```

6. Confirm your decision to overwrite 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
Restoring the database will overwrite all existing system configuration. If running, the system will be restarted during this process.

Are you sure you wish to continue? (y/n): y
Backup file is valid. Timestamp = 2003-Sep-15-14:01:53
```

7. Confirm your decision whether to restore GSSM platform information, or only the GSS database. This selection enables you to return the primary GSSM back to the 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), timezone, logging levels, Web certificates, inter-GSS communication certificates, access lists and access groups, CLI user information, GUI user information, and property-set CLI commands.

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
```

Perform one of the following actions:

- Select `y` to restore GSSM platform information.

  **Note**  
  Restoring platform information requires a reboot of the GSS at the end of the restore procedure.

  - Select `n` to restore only the GSSM database and not the GSSM platform information. If you choose not to restore GSSM platform information, you must reconfigure the GSSM platform information from the CLI. Refer to Chapter 2, Setting Up Your GSS for details.
8. Confirm your decision to restore the GSS network information for remote devices activated from the primary GSSM.

Do you want to replace your current GSS network configuration with the one specified in the backup file? (y/n): y

Perform one of the following actions:

- Select y to restore the GSS network information, such as registered GSS devices, GSS device status, node information, and IP addresses. This is the network information displayed in the Global Site Selectors list table in the Resources tab (refer to Chapter 2, Setting Up Your GSS). GSS network information does not include DNS rules, answers, keepalive, and so on. Those configuration elements are automatically restored as part of the database restore process.

- Select 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 disable and enable each device, then reregister the device with the primary GSSM, which may result in a temporary network service outage. Refer to Chapter 2, Setting Up Your GSS for details.

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 specified to restore GSSM platform information, the GSSM reboots.

9. Use the gss status command to confirm that your restored GSSM is up and running in normal operation mode (runmode = 5).
Restoring Your GSSM Database from a Database-Only Backup

You must have a backup of an earlier version of your database file to restore it to run with your downgraded GSS software. You should be aware that the GSS database schema often changes between versions. When you downgrade from a later to an earlier version of the GSSM database, any configuration changes that you entered through the GSSM subsequent to your last upgrade are lost, including configuration changes, device configuration information, and DNS rules.

See the “Backing Up the GSSM” section for details on performing a database backup of the GSSM.

Note

Restoring your GSSM database requires that the GSSM device be stopped and restarted, resulting in the device and the GUI being unavailable for a short period.

Use the following procedure to restore an earlier version of the GSSM from a backup:

1. Log on to the CLI following the instructions in Chapter 2, Setting Up Your GSS, the “Accessing the GSS CLI” section. The GSS CLI prompt appears.

2. Verify that the full backup of the GSSM is at a location that is accessible from the GSSM that you are restoring. Full backups have a .full file extension.

3. Enable privileged EXEC mode. For example:

   gss1.yourdomain.com> enable
   gss1.yourdomain.com#

4. Stop the GSS software on the GSSM and then use the gss status command to confirm that the GSSM has stopped. For example:

   gss1.yourdomain.com# gss stop
   gss1.yourdomain.com# gss status
   Cisco GSS - 1.1(0.0.1) - GSSM - primary [Mon Sep 15 12:58:27 UTC 2003]

   gss is not running.
5. Once the GSSM has stopped, use the `gssm restore` command to restore the GSSM database from the backup file that corresponds to the software version that you just restored. To restore the file `gssmdbbk.db`, you would enter:

```
gss1.yourdomain.com# gssm restore gssmdbbk.db
```

6. Confirm your decision to overwrite 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
   Restoring the database will overwrite all existing
   system configuration. If running, the system will be restarted
   during this process.

   Are you sure you wish to continue? (y/n):
   Backup file is valid. Timestamp = 2003-Aug-20-14:02:06
   Restoring database only (No platform backup present)

7. Confirm your decision to restore the GSS network information for remote devices activated from the primary GSSM.

   Do you want to replace your current GSS network configuration with
   the one specified in the backup file? (y/n): y

   Perform one of the following actions:

   - Select `y` to restore the GSS network information, such as registered GSS devices, GSS device status, node information, and IP addresses. This is the network information displayed in the Global Site Selectors list table in the Resources tab (refer to Chapter 2, Setting Up Your GSS). GSS network information does not include DNS rules, answers, keepalive, and so on. Those configuration elements are automatically restored as part of the database restore process.

   - Select `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 disable and enable each device, then reregister the device with the primary GSSM, which may result in a temporary network service outage. Refer to Chapter 2, Setting Up Your GSS for details.
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...
Database restored successfully.
GSSM database restore succeeded.

8. Once you receive confirmation that the database restoration has succeeded, use the `gss start` command to restart your GSSM. For example:

```
gssl.yourdomain.com# gss start
System started.
```

9. Use the `gss status` command to confirm that your restored GSSM is up and running in normal operation mode (`runmode = 5`).

### Viewing Third-Party Software Versions

The GSS software relies on a variety of third-party software products to operate properly. For that reason, the GSSM GUI provides a feature that easily allows you to track the third-party software used by the GSS software.

To view information on the third-party software currently running on your GSS:

1. From the GSSM GUI, click the **Tools** tab.

2. Click the **Third-Party Software** navigation link. The GSSM Third-Party Software list page appears (Figure 9-5). This page displays the following information:
   - **Product**—Third-party software product. For example, RedHat Version 6.2
   - **Version**—Version of the third-party software currently installed on the GSS device
   - **URL**—Web URL for the software product
### GSSM Third-Party Software List Page

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>1.3.27</td>
<td><a href="http://httpd.apache.org/">http://httpd.apache.org/</a></td>
</tr>
<tr>
<td>Jboss</td>
<td>1.8.1</td>
<td><a href="http://docs.jboss.org/jboss-free/">http://docs.jboss.org/jboss-free/</a></td>
</tr>
<tr>
<td>MySQL</td>
<td>5.0.44</td>
<td><a href="http://www.mysql.com/">http://www.mysql.com/</a></td>
</tr>
<tr>
<td>Net-SNMP Agent</td>
<td>4.2.5</td>
<td><a href="http://www.net-snmp.org/">http://www.net-snmp.org/</a></td>
</tr>
<tr>
<td>OpenSSL</td>
<td>3.1</td>
<td><a href="http://www.openssl.org/">http://www.openssl.org/</a></td>
</tr>
<tr>
<td>OpenSSL SSL</td>
<td>9.6.6</td>
<td><a href="http://www.openssl.org/">http://www.openssl.org/</a></td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>7.4.4</td>
<td><a href="http://www.postgresql.org/">http://www.postgresql.org/</a></td>
</tr>
<tr>
<td>Realtek</td>
<td>2.2.22-20.4 (kernel)</td>
<td><a href="http://www.realtek.com/">http://www.realtek.com/</a></td>
</tr>
<tr>
<td>RSA-Bothe Toolkit</td>
<td>3.4.2</td>
<td><a href="http://www.rsa.com/products/bothe/">http://www.rsa.com/products/bothe/</a></td>
</tr>
<tr>
<td>Sun JCE</td>
<td>1.3.1</td>
<td><a href="http://java.sun.com/products/jce/">http://java.sun.com/products/jce/</a></td>
</tr>
<tr>
<td>Tomcat</td>
<td>3.2.4</td>
<td><a href="http://jakarta.apache.org/tomcat/">http://jakarta.apache.org/tomcat/</a></td>
</tr>
<tr>
<td>Firefox XML Parser</td>
<td>3.2.8</td>
<td><a href="http://www.mozilla.org/">http://www.mozilla.org/</a></td>
</tr>
</tbody>
</table>
Primary GSSM Error Messages

The following sections describe error messages that you may encounter when using the primary GSSM GUI to manage your GSS network. Error messages are organized by GSSM component.

This section contains the following GSSM error messages:

- Answer Error Messages
- Answer Group Error Messages
- DNS Rule Error Messages
- Domain List Error Messages
- Shared KeepAlive Error Messages
- KeepAlive Error Messages
- Location Error Messages
- Owner Error Messages
- Region Error Messages
- GSSM Error Messages
- Source Address List Error Messages
- User Error Messages

Answer Error Messages

**Error Message**  Invalid answer name. If entered, name must not be the empty string.

**Explanation**  The name that you entered for the answer is not valid. Answer names cannot be blank or contain blank spaces.

**Recommended Action**  Enter a valid alphanumeric answer name of at least 1 and no more than 80 characters in length that does not contain spaces.
**Error Message**  Invalid answer name. Name length must not exceed 80 characters.

**Explanation**  The answer name that you entered contains too many characters.

**Recommended Action**  Enter a valid alphanumeric answer name of at least 1 and no more than 80 characters in length that does not contain spaces.

**Error Message**  Invalid CRA timing decay. Timing decay must be between 1 and 10.

**Explanation**  You entered an invalid number for the CRA timing decay.

**Recommended Action**  Enter a number between 1 and 10. Lower timing decay values mean that more recent DNS races are weighted more heavily than older races. Higher decay values mean that the results of older races are weighted more heavily than more recent races.

**Error Message**  Invalid CRA static RTT value. Static RTT must be between 0 and 1000.

**Explanation**  You entered an invalid number for the static round-trip time (RTT). This is a manually entered value that is used by the GSS to represent the time it takes for traffic to reach and return from a host.

**Recommended Action**  Enter a static RTT value between 0 and 1000.

**Error Message**  A VIP/Name Server/CRA-type answer named answer_name already exists. If specified, name and type must uniquely identify an answer.

**Explanation**  You are trying to create an answer that already exists on the GSS. You cannot have two answers with the same name and answer type.

**Recommended Action**  Assign a new name or answer type to your answer to make it unique.
Error Message  An unnamed VIP/Name Server/CRA-type answer having address IP_address already exists. Name must be specified to configure an answer with the same address as another answer.

Explanation  You are trying to create an answer that already exists on the GSS. You cannot have two answers with the same name and IP address.

Recommended Action  Assign a new name to your answer to make it unique.

Error Message  The maximum number of number VIP/Name Server/CRA-type answers has been met.

Explanation  You are attempting to create an answer when the maximum number of that type of answer has already been created.

Recommended Action  Remove an existing answer of the same type.

Error Message  CRA decay value must be specified.

Explanation  You are attempting to create a CRA answer type without specifying a decay value. The decay value is required to tell the GSS how to evaluate and weigh DNS race results.

Recommended Action  Enter a number between 1 and 10 for the CRA decay, with 1 causing the GSS to weigh recent DNS race results more heavily, and 10 telling it to weigh them less heavily.

Error Message  CRA static RTT must be specified.

Explanation  You are attempting to create a CRA answer type without specifying a static round-trip time (RTT) value. The RTT value is used to force the GSS to use a value that you supply as the round-trip time necessary to reach the requesting D-proxy.

Recommended Action  Enter a number between 1 and 1000 for the CRA round-trip time in milliseconds.
**Error Message** Invalid keepalive tag. Tag must be at least one character in length.

**Explanation** You are attempting to create a VIP answer with a KAL-AP By Tag keepalive, but you have not specified a value for the tag in the field provided.

**Recommended Action** Enter an alphanumeric tag between 1 and 76 characters in the Tag field.

**Error Message** Invalid keepalive tag. Tag length must not exceed 76 characters.

**Explanation** You are attempting to create a VIP answer with a KAL-AP By Tag keepalive, but you have specified a value for the tag that contains too many characters.

**Recommended Action** Enter an alphanumeric tag between 1 and 76 characters in the Tag field.

**Error Message** NS-type answer *IP Address* has the same IP address as GSS *GSS_name*. GSS IP addresses must not equal any NS-type answers.

**Explanation** You are attempting to create a name server answer type with the same IP address as a GSS device on the same GSS network. Name server answers cannot use the same address as GSS devices belonging to the same GSS network.

**Recommended Action** Assign a valid IP address to your name server answer.
Answer Group Error Messages

Error Message  This answer group cannot be deleted because it is referenced by number DNS rule balance clause(s).

Explanation  You are attempting to delete an answer group that is being referenced by one or more DNS rules.

Recommended Action  Modify any DNS rules that are referencing the answer group so that those rules do not point to the group, and then try again to delete the group.

Error Message  Invalid answer group name. Name must be entered.

Explanation  You are attempting to create an answer group without assigning a name to that group. All answer groups must have names of at least one character.

Recommended Action  Enter a name for the new answer group in the field provided, and then click Save.

Error Message  Invalid answer group name. Name length must not exceed 80 characters.

Explanation  You are attempting to assign the answer group an invalid name.

Recommended Action  Enter an alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.

Error Message  Invalid answer group name. Name must not contain spaces.

Explanation  You are attempting to assign the answer group an invalid name.

Recommended Action  Enter an alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.
**Error Message**  An answer group named *name* already exists. Name must uniquely identify an answer group.

**Explanation**  You are attempting to assign the answer group a name that is already being used by a different GSS device.

**Recommended Action**  Enter a unique alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.

**Error Message**  The maximum number of *number* answers per VIP/Name Server/CRA-type group has been met.

**Explanation**  You are attempting to add an answer to an answer group to which the maximum number of answers has already been assigned.

**Recommended Action**  Remove an answer from the group, or add the answer to a group to which the maximum number of answers has not already been added.

### DNS Rule Error Messages

**Error Message**  TTL must be specified for balance method associated with CRA- or VIP-type answer group.

**Explanation**  You are attempting to create a balance clause without specifying a Time To Live (TTL) for answers returned by the clause.

**Recommended Action**  Enter a TTL value between 0 and 604,800 seconds.

**Error Message**  Invalid balance clause TTL. TTL must be between 0 and 604,800.

**Explanation**  You are required to specify a Time To Live (TTL) value for answers provided by the balance clause that you are creating.

**Recommended Action**  Enter a TTL value between 0 and 604,800 seconds.
**Error Message**  Invalid balance clause position. Position must be between 0 and 2.

**Explanation**  You are attempting to create a clause for your DNS rule that is out of sequence. The DNS Rule Builder provides options for three balance clauses, which must be created in order, with no gaps between clauses. For example, if you are using only one balance clause, it must appear in the first position. It cannot be listed in the second or third positions with the first position left blank.

**Recommended Action**  Rearrange your balance clauses in the DNS Rule Builder so that they are listed in the proper order, with no gaps between them.

---

**Error Message**  Hash type must be specified for answer group using hash balance method.

**Explanation**  You are trying to create an answer group using the balance method “Hashed” with the selected answer, but you have not selected one (or more) hash methods: By Domain Name and By Source Address.

**Recommended Action**  Select one or more of the available hash methods by checking the box corresponding to the methods that you wish to use with this balance clause.

---

**Error Message**  Balance clause Boomerang fragment size must be specified.

**Explanation**  You are attempting to create a balance clause using the boomerang balance method but have not specified a fragment size in the Fragment Size field. The fragment size determines the preferred size of the boomerang race response that is produced by a match to a DNS rule and is sent to the requesting client.

**Recommended Action**  Enter a fragment size between 28 and 1980 in the field provided. The fragment size must be divisible by 4.
**Error Message**  Invalid balance clause Boomerang fragment size. Boomerang fragment size must be 0 or between 28 and 1980.

**Explanation**  You are attempting to specify an unacceptable fragment size for this balance clause in the Fragment Size field.

**Recommended Action**  Enter a valid fragment size. Fragment sizes must be between 28 and 1980, and must be divisible by 4.

---

**Error Message**  Invalid balance clause Boomerang fragment size. Boomerang fragment size must be a multiple of 4.

**Explanation**  You are attempting to specify a fragment for this boomerang balance clause that is within the acceptable range but not divisible by 4. Fragment sizes must be divisible by 4.

**Recommended Action**  Enter a fragment size between 28 and 1980 that is also divisible by 4. Zero is also an acceptable fragment size.

---

**Error Message**  Balance clause Boomerang IP TTL value must be specified.

**Explanation**  You are attempting to create a balance clause using the boomerang balance method, but have not specified an IP Time To Live (TTL) in the field provided. The IP TTL specifies the maximum number of network hops that can be used when returning a response to a CRA from a match on a DNS rule.

**Recommended Action**  Enter an IP TTL between 1 and 255 in the field provided and then click Save.

---

**Error Message**  Invalid balance clause Boomerang IP TTL. Boomerang IP TTL must be between 1 and 255.

**Explanation**  You are attempting to create a balance clause using the boomerang balance method but have specified an invalid IP Time to Live (TTL).

**Recommended Action**  Enter an IP TTL between 1 and 255 in the field provided and then click Save.
**Error Message** Balance clause Boomerang maximum propagation delay must be specified.

**Explanation** You are attempting to create a balance clause using the boomerang balance method but have not specified a maximum propagation delay (Max Prop. Delay) in the field provided. The maximum propagation delay specifies the maximum length of time (in milliseconds) that is observed before the GSS forwards a Domain Name System (DNS) request to a content routing agent (CRA).

**Recommended Action** Enter a maximum propagation delay between 1 and 1000 milliseconds in the Max Prop. Delay field.

**Error Message** Invalid balance clause Boomerang maximum propagation delay. Boomerang maximum propagation delay must be between 1 and 1000.

**Explanation** You are attempting to create a balance clause using the boomerang balance method but have not specified a valid maximum propagation delay (Max Prop. Delay) in the field provided.

**Recommended Action** Enter a maximum propagation delay between 1 and 1000 milliseconds in the Max Prop. Delay field.

**Error Message** Balance clause Boomerang padding size must be specified.

**Explanation** You are attempting to create a balance clause using the boomerang balance method but have not specified a pad size in the Pad Size field. The pad size is the amount of extra data (in bytes) included with each content routing agent (CRA) response packet and is used to evaluate CRA bandwidth as well as latency when routing decisions are made.

**Recommended Action** Enter a valid pad size between 0 and 2000 in the Pad Size field.
**Error Message**  Invalid balance clause Boomerang padding size. Boomerang padding size must be between 0 and 2000.

**Explanation**  You are attempting to create a balance clause using the boomerang balance method but have specified an invalid pad size in the Pad Size field.

**Recommended Action**  Enter a valid pad size between 0 and 2000 in the Pad Size field.

**Error Message**  Invalid balance clause Boomerang secret. If specified, Boomerang secret must be between 1 and 64 characters in length.

**Explanation**  You are attempting to create a balance clause using the boomerang balance method but have specified an invalid secret in the Secret field. The boomerang secret is a text string consisting of between 1 and 64 characters that is used to encrypt critical data sent between the boomerang server and content routing agents (CRAs). This key must be the same for each configured CRA.

**Recommended Action**  Enter a valid boomerang secret between 1 and 64 characters in the Secret field.

**Error Message**  Balance clause Boomerang server delay must be specified.

**Explanation**  You are attempting to create a balance clause using the boomerang balance method but have not specified a server delay in the Server Delay field. The boomerang server delay is the maximum delay (in milliseconds) that is observed before the boomerang server component of the GSS forwards the address of its “last gasp” server as a response to the requesting name server.

**Recommended Action**  Enter a valid server delay between 32 and 999 milliseconds in the Server Delay field.
**Error Message** Invalid balance clause Boomerang server delay. Boomerang server delay must be between 32 and 999.

**Explanation** You are attempting to create a balance clause using the boomerang balance method but have specified an invalid server delay in the Server Delay field.

**Recommended Action** Enter a valid server delay between 32 and 999 milliseconds in the Server Delay field.

---

**Error Message** Invalid DNS rule name. Name must be entered.

**Explanation** You are attempting to create a DNS rule without assigning a name to the rule. DNS rules must have names of between 1 and 100 characters.

**Recommended Action** Assign a name to your DNS rule using the Rule Name field and then try again to save the rule.

---

**Error Message** Invalid DNS rule name. Name length must not exceed 100 characters.

**Explanation** You are attempting to assign a name to your DNS rule that is too long. The maximum length for DNS rules is 100 characters.

**Recommended Action** Enter a name for your DNS rule that is between 1 and 100 characters and then attempt to save the rule again.

---

**Error Message** Invalid DNS rule name. Name must not contain spaces.

**Explanation** You are attempting to assign your DNS rule a name that contains spaces.

**Recommended Action** Enter a valid name for your DNS rule that is between 1 and 100 characters and does not contain spaces.
**Error Message** A DNS rule using the specified source address list, domain list, and matching query type already exists. Source address list, domain list, and matching query type must uniquely identify a DNS rule.

**Explanation** You are attempting to create a DNS rule that already exists. DNS rules must specify a unique combination of source address list, domain list, and matching query type.

**Recommended Action** Reconfigure your DNS rule so that it does not exactly match the preexisting rule and then save the rule.

**Error Message** Duplicate answer group/balance method assignment detected. A DNS rule cannot use the same answer group and balance method in multiple balance clauses.

**Explanation** You are attempting to create two identical answer group and balance method clauses in your DNS rule. Each clause must use a unique combination of answer groups and balance methods.

**Recommended Action** Modify one of your answer group and balance method pairs so that it is no longer identical to the other and then save your DNS rule.

**Error Message** Balance clause gap detected at position {0,1,2}. Balance clauses must be specified sequentially without gaps.

**Explanation** You are attempting to create a clause for your DNS rule that is out of sequence. The DNS Rule Builder provides options for three balance clauses, which must be created in order, with no gaps between clauses. For example, if you are using only one balance clause, it must appear in the first position. It cannot be listed in the second or third positions with the first position left blank.

**Recommended Action** Rearrange your balance clauses in the DNS Rule Builder so that they are listed in the proper order, with no gaps between them.
Primary GSSM Error Messages

**Error Message** A DNS rule named `DNS_Rule_name` already exists. Name must uniquely identify a DNS rule.

**Explanation** You are attempting to assign a name to the DNS rule that is already assigned to another rule. DNS rule names must be unique.

**Recommended Action** Assign the rule a name that is not already being used and then save the rule.

Domain List Error Messages

**Error Message** `<domain name>` must contain at least one character.

**Explanation** You are attempting to add a domain to a domain list with an invalid name. Domains in domain lists must have names of at least one character.

**Recommended Action** Enter a name that is between 1 and 100 characters and then save your domain list.

**Error Message** `<domain name>` character limit exceeded.

**Explanation** You are attempting to add a domain to a domain list using a name that is too long. Domains in domain lists cannot have names of more than 100 characters.

**Recommended Action** Enter a new domain name of no more than 100 characters and then save your domain list.

**Error Message** Domain specification must not exceed 128 characters.

**Explanation** You are attempting to add a domain to your domain list with a name that is longer than 128 characters. Domain lists cannot contain domains with names longer than 128 characters.

**Recommended Action** Replace the domain with a domain name containing fewer than 128 characters and then save your domain list.
Error Message  <domain name> must not contain spaces.

Explanation  You are attempting to add a domain to your domain list with a name that contains spaces. Domains in domain lists cannot have names that contain spaces.

Recommended Action  Modify the domain name so that it does not contain spaces and then save your domain list.

Error Message  <domain name> is not a valid regular expression: <regular expression syntax error message here>

Explanation  You are attempting to add a domain name to a domain list with a name that contains invalid characters or formatting. Domain names in domain lists must be valid regular expressions.

Recommended Action  Modify the domain name so that it is a valid regular expression and does not contain any invalid characters or formatting. For example, www.cisco.com or .*\cisco\com, and then save your domain list.

Error Message  <domain name> must not begin or end with '.'

Explanation  You are attempting to add a domain to a domain list with a literal name that contains an invalid character at the beginning or end of the domain name.

Recommended Action  Modify the domain name so that it does not contain a period at the beginning or end of the name and then save your domain list.

Error Message  <domain name> component must not begin or end with '_'

Explanation  You are attempting to add a domain to a domain list with a literal name that contains an invalid character at the beginning or end of one component of the domain name. For example, www.cisco-.com.

Recommended Action  Modify the domain name so that it does not contain a dash (-) at the beginning or end of any segment of the name and then save your domain list.
Primary GSSM Error Messages

**Error Message**  
<domain name> contains invalid character '<character>' (<ASCII value of the character>)

**Explaination**  
You are attempting to add a domain to a domain list with a name that contains an invalid text character. Domains belonging to domain lists must have names that are regular expressions.

**Recommended Action**  
Modify the domain name so that it does not contain an invalid text character and then save your domain list.

**Error Message**  
This domain list cannot be deleted because it is referenced by X DNS rule

**Explaination**  
You are attempting to delete a domain list that is being referenced by one or more DNS rules.

**Recommended Action**  
Modify any DNS rules that use the domain list so that they no longer reference it and then try again to delete the list.

**Error Message**  
Invalid domain list name. Name must be entered.

**Explaination**  
You are attempting to create a domain list without a name. Domain lists must have names of at least one character.

**Recommended Action**  
Assign a name of at least 1 and no more than 80 characters to your domain list and then save it.

**Error Message**  
Invalid domain list name. Name length must not exceed 80 characters.

**Explaination**  
You are attempting to create a domain list with a name that is too long.

**Recommended Action**  
Assign a name of at least 1 and no more than 80 characters to your domain list and then save it.
**Error Message**  Invalid domain list name. Name must not contain spaces.

**Explanation**  You are attempting to create a domain list with a name that contains spaces. Domain list names cannot contain spaces.

**Recommended Action**  Assign a name without spaces to your domain list. Names must consist of at least 1 and no more than 80 characters. Save your domain list when you have assigned it a valid name.

**Error Message**  A domain list named ' <name> ' already exists. Name must uniquely identify a domain list.

**Explanation**  You are attempting to assign a name to your domain list that has already been assigned to another domain list on the same GSS network.

**Recommended Action**  Assign a unique name to your new domain list and then save the list.

**Error Message**  The maximum number of <limit> domains per list has been met.

**Explanation**  You are attempting to add a domain to your domain list when the maximum number of domains has already been added to that list.

**Recommended Action**  Remove an existing domain from the domain list and then add the new domain. Alternatively, create a domain list to hold the new domain and any subsequent domains that you wish to add.
Shared KeepAlive Error Messages

**Error Message**  Invalid CAPP hash secret. Secret must be entered.

**Explanation**  You are attempting to create a KAL-AP keepalive using a CAPP hash secret but have not specified a secret in the field provided.

**Recommended Action**  Enter a CAPP hash secret of no more than 31 characters in the field provided.

**Error Message**  Invalid CAPP hash secret. Secret length must not exceed 31 characters.

**Explanation**  You are attempting to create a KAL-AP keepalive using a CAPP hash secret but have specified a secret that is too long.

**Recommended Action**  Enter a CAPP hash secret of no more than 31 characters in the field provided.

**Error Message**  Invalid HTTP HEAD response timeout.

**Explanation**  You are attempting to specify an HTTP HEAD response timeout that is invalid.

**Recommended Action**  Enter a response timeout between 20 and 60 seconds in the HTTP HEAD response timeout field of the Shared Keepalive details page.

**Error Message**  Response timeout must be between 20 and 60 seconds.

**Explanation**  You are attempting to specify an HTTP HEAD response timeout that is invalid.

**Recommended Action**  Enter a response timeout between 20 and 60 seconds in the HTTP HEAD response timeout field of the Shared Keepalive details page.
**Error Message**  Invalid HTTP HEAD destination port. Destination port must be between 1 and 65,535.

**Explanation**  You are attempting to specify a port number for HTTP HEAD traffic that is invalid.

**Recommended Action**  In the HTTP HEAD destination port field in the Shared Keepalive details page, enter a port number between 1 and 65,535 through which HTTP HEAD keepalive traffic will pass. The default port is 80.

**Error Message**  Invalid HTTP HEAD path. Path length must not exceed 256 characters.

**Explanation**  You are attempting to specify an HTTP HEAD path that is not valid.

**Recommended Action**  Enter a valid path shorter than 256 characters in the HTTP HEAD default path field in the Shared Keepalive details page.

**Error Message**  Invalid `<keepalive type>` minimum probe frequency. Frequency must be between `<min>` and `<max>`.

**Explanation**  You are attempting to specify a minimum probe interval for your keepalive type that is invalid.

**Recommended Action**  Specify an interval (in seconds) within the range specified for that keepalive type in the Shared Keepalive details page. The interval range for the CRA keepalive type is between 1 and 60 seconds. For all other keepalive types, it is between 45 and 255 seconds.
KeepAlive Error Messages

**Error Message** Duplicate keepalive address detected. A keepalive must not be configured to use the same primary and secondary addresses.

**Explanation** You are trying to configure a KAL-AP keepalive that is identical to a keepalive of the same type that already exists.

**Recommended Action** Configure the KAL-AP keepalive to use a different primary and secondary address.

**Error Message** Duplicate keepalive primary address '<primaryaddress>' detected. An address can be used by at most one KAL-AP type keepalive.

**Explanation** You are trying to configure a KAL-AP keepalive that uses the same primary IP address as a keepalive of the same type that already exists.

**Recommended Action** Configure the KAL-AP keepalive to use a primary IP address that is not already being used by another keepalive.

**Error Message** Duplicate keepalive secondary address '<secondary address>' detected. An address can be used by at most one KAL-AP type keepalive.

**Explanation** You are trying to configure a KAL-AP keepalive that uses the same secondary IP address as a keepalive of the same type that already exists.

**Recommended Action** Configure the KAL-AP keepalive to use a secondary IP address that is not already being used by another keepalive.
**Error Message**  HEAD Duplicate keepalive detected. An HTTP HEAD keepalive must not use the same address, destination path, host tag, and port as another HTTP HEAD keepalive.

**Explanation**  You are trying to configure an HTTP HEAD keepalive that features an identical configuration to that of another HTTP HEAD keepalive on your GSS network.

**Recommended Action**  Configure the HTTP HEAD keepalive to use a unique configuration of address, destination path, host tag, and port.

**Error Message**  Duplicate keepalive detected. An ICMP keepalive must not use the same address as another ICMP keepalive.

**Explanation**  You are trying to configure an ICMP keepalive with an IP address that is identical to that of another ICMP keepalive on your GSS network.

**Recommended Action**  Configure the ICMP to use a unique IP address.

**Error Message**  Invalid CAPP hash secret. Secret length must not exceed 31 characters.

**Explanation**  You are attempting to create a KAL-AP keepalive using a CAPP hash secret but have specified a secret that is too long.

**Recommended Action**  Enter a CAPP hash secret of no more than 31 characters in the field provided.

**Error Message**  Invalid HTTP HEAD destination port. If specified, destination port must be between 0 and 65,535.

**Explanation**  You are attempting to specify a port number for HTTP HEAD traffic that is invalid.

**Recommended Action**  In the HTTP HEAD destination port field in the Shared Keepalive details page, enter a port number between 1 and 65,535 through which HTTP HEAD keepalive traffic will pass. The default port is 80.
**Primary GSSM Error Messages**

**Error Message**  Invalid HTTP HEAD host tag. Host tag length must not exceed 128 characters.

**Explanation**  You are attempting to create an HTTP HEAD host tag that is too long.

**Recommended Action**  Enter an HTTP HEAD host tag of no more than 128 characters.

**Error Message**  Invalid HTTP HEAD path. If specified, path length must not exceed 256 characters.

**Explanation**  You are attempting to specify an HTTP HEAD path that is not valid.

**Recommended Action**  Enter a valid path shorter than 256 characters in the HTTP HEAD default path field in the Shared Keepalive details page.

**Location Error Messages**

**Error Message**  The location is still being referenced by other objects and cannot be removed.

**Explanation**  You are attempting to delete a location that has answers or GSSs associated with it.

**Recommended Action**  Dissociate any answers or GSSs from the location and then try again to delete it.

**Error Message**  There already exists a location named <name> in region <region> with the same name. Please specify a different location name.

**Explanation**  You are attempting to create a location within this region when another location with the same name already exists.

**Recommended Action**  Change the name of the location so that it is unique for the region.
Owner Error Messages

**Error Message** Invalid owner name. Name must be entered.

**Explanation** You are attempting to create an owner without assigning the owner a name.

**Recommended Action** Owners must have a unique name. Enter a name for the owner in the field provided and then save the owner.

**Error Message** Invalid owner name. Name length must not exceed 80 characters.

**Explanation** You are attempting to assign a name to an owner that is too long.

**Recommended Action** Assign your owner a name that is no longer than 80 characters.

**Error Message** An owner named <owner name> already exists. Name must uniquely identify an owner.

**Explanation** You are attempting to assign your owner a name that is already assigned to another owner on your GSS network.

**Recommended Action** Assign a unique name to your owner.

Region Error Messages

**Error Message** The region is still being referenced by other objects and cannot be removed.

**Explanation** You are attempting to delete a region that is associated with GSSs on your GSS network.

**Recommended Action** Disassociate the GSSs from the region and then try again to delete the region.
**Primary GSSM Error Messages**

**Error Message** There already exists a region named `<region name>`. All region names have to be unique.

**Explanation** You are attempting assign a name to the region that is already being used by another region on your GSS network.

**Recommended Action** Assign a unique name to your region.

---

**GSSM Error Messages**

**Error Message** Maximum number of GSSMs exceeded. A GSS network can contain at most 2 GSSMs.

**Explanation** You are attempting to enable a GSSM when there are already two GSSMs enabled on your GSS network.

**Recommended Action** If necessary, remove your standby GSSM from your GSS network and then try again to enable the GSSM.

**Error Message** The maximum number of `<size> <className>` has been met.

**Explanation** You are attempting to add a resource to your GSS network when the maximum number of that resource already exists.

**Recommended Action** Remove an existing resource of the same type and then try again to add the new resource.
Source Address List Error Messages

Error Message Invalid source address block '<block string>'. Address block must specify a host or a network.

Explanation You are attempting to specify an invalid source address range.

Recommended Action Enter a valid source address or block of source addresses. Source addresses cannot specify a multicast address list.

Error Message Invalid source address block '<blockstring>'. Address block must specify a class A, B, or C host or network.

Explanation You are attempting to specify an invalid source address range.

Recommended Action Enter a valid source address or block of source addresses. Source addresses cannot specify a multicast address list.

Error Message Invalid source address list name. Name must be entered.

Explanation You are attempting to create a source address list without assigning the list a name.

Recommended Action Enter a name for the source address list in the Name field.

Error Message Invalid source address list name. Name length must not exceed 80 characters.

Explanation You are attempting to create a source address list with a name that is too long.

Recommended Action Enter a valid name for the source address list that has fewer than 80 characters and does not contain spaces.
Error Message  Invalid source address list name. Name must not contain spaces.

Explanation  You are attempting to create a source address list with a name that contains spaces. Source address list names cannot contain spaces.

Recommended Action  Enter a valid name for the source address list that has fewer than 80 characters and does not contain spaces.

Error Message  This source address list cannot be deleted because it is referenced by <number> DNS rules.

Explanation  You are attempting to delete a source address list that is referenced by one or more DNS rules.

Recommended Action  Disassociate your DNS rules from the source address list using the DNS Rule Builder or DNS Rule Wizard and then attempt to delete the source address list again.

Error Message  A source address list named '<name>' already exists. Name must uniquely identify a source address list.

Explanation  You are attempting to create a source address list using a name that is already being used by another source address list on your GSS network.

Recommended Action  Assign a unique name to your source address list that is no more than 80 characters and does not contain spaces.

Error Message  The maximum number of 30 source address blocks per list has been met.

Explanation  You are attempting to add a source address block to the source address list, when the maximum of 30 source address blocks has already been added to the list.

Recommended Action  Remove an existing source address block, or create a source address list for the source address block that you wish to add.
User Error Messages

**Error Message** There already exists a user account named &lt;username&gt;. All user accounts must have a unique username.

**Explanation** You are attempting to create a user account with a name identical to that of an existing account.

**Recommended Action** Assign your new user account a unique name.

**Error Message** You cannot delete the account with username 'admin'. This account must exist.

**Explanation** You are attempting to delete the admin user account.

**Recommended Action** This account cannot be deleted from the GSSM.

**Error Message** Invalid answer load threshold. Load threshold must be between 2 and 254.

**Explanation** You are attempting to assign an invalid load threshold to your answer in the LT field.

**Recommended Action** Assign a load threshold for the answer that is between 2 and 254 in the LT field.

**Error Message** Invalid answer order. Order must not be negative.

**Explanation** You are attempting to assign a negative order number to your answer. The order must be a positive number.

**Recommended Action** Enter a nonnegative whole number for the order.