Upgrading the 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.
- 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, Cisco recommends 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 this order:

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

Before you continue with the upgrade procedure, verify that the roles of the designated primary and standby GSSMs have not changed. The changing of roles between the designated primary GSSM and the standby GSSM is intended to be a temporary GSS network configuration until the original primary GSSM is back online.

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

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

   ```
   gssm1.example.com# cd /home
   gssm1.example.com# type ../props.cfg | grep -i fqdn
   ```

   The following output appears:

   `controllerFqdn=` *`domain_name`* or *`ip_address`*

2. Based on the output value for `controllerFqdn`, 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. Refer to the "Reversing the Roles of the Interim Primary and Standby GSSM Devices" section in Chapter 2, Managing the GSS from the CLI.
   - If the value of the domain name or IP address is not the current primary GSSM or the standby GSSM in your network, this indicates that the device is not a primary GSSM or is no longer on the network. No further action is required. 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 Primary GSSM Backup" section in Chapter 7, Backing Up, Restoring, and Downgrading 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 Systems.

To acquire the software update from Cisco Systems:

- Access the Cisco.com website and locate the software update files.
- Download the software update files to a server within your own organization that is accessible using FTP or SCP from your GSSs and GSSMs.

You must have a Cisco.com username and password to download a software update from Cisco.com. To acquire a Cisco.com login, go to http://www.cisco.com and click the **Register** link.

Note You need a service contract number, Cisco.com registration number and verification key, Partner Initiated Customer Access (PICA) registration number and verification key, or packaged service registration number to obtain a Cisco.com username and password.

To add an upgrade file for the GSS software:

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.

Note When you first access the Content Networking page of the Software Center, you must apply for eligibility for GSS software updates because it is considered a strong encryption image. Under the Cisco Content Networking Cryptographic Software section is the Apply for 3DES Cisco Cryptographic Software Under Export Licensing Controls link. Click this link and complete the Encryption Software Export Distribution Authorization Form. Complete this step to access and download Global Site Selector software images.

3. Locate the .upg file you want to download by referring to the Release column for the proper release version of the software.
4. Click the link for the .upg file. The download page appears.
5. Click the **Software License Agreement** link. A new browser window opens to display the license agreement.
6. After you have read the license agreement, close the browser window displaying the agreement and return to the Software Download page.

7. Click the filename link labeled **Download**. If prompted by software, reenter your username and password.
8. Click **Save to file**, 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

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 each GSS device in your network to be upgraded has connectivity to the primary GSSM before you perform the software upgrade procedure.

When executing an upgrade, use the **install** CLI command. Before proceeding with the installation of the software upgrade, the **install** command performs a validation check on the upgrade file, unpacks the upgrade archive, and installs the upgraded software. Finally, the **install** command restarts the affected GSS device.

Note Upgrading your GSS devices causes a temporary loss of service for each affected device.

To upgrade the GSS software (starting with the primary GSSM):

1. Log on to the CLI of the GSS device.
2. Enter the Global Configuration Mode by entering **enable** and then **config**.
3. If you use FTP to copy files into GSS, enable the FTP client by entering **ftp-client enable all** at the config prompt.
4. Type **exit** to leave Global Configuration mode.
5. Use the **ftp** or **scp** command to copy the GSS software upgrade file from the network location to a directory on the GSS. Ensure that you set the transfer type to **binary**.

   For example, to copy an upgrade file named gss.upg from a remote host, your FTP session may appear as:

```
gssm1.example.com> ftp host.example.com
Connected to host.example.com.
220 host.example.com FTP server (Version wu-2.6.1-0.6x.21) ready.
Name (host.example.com:root): admin
331 Password required for admin.
Password:
230 User admin logged in. Access restrictions apply.
Remote system type is UNIX.
Using ascii mode to transfer files.
ftp> binary
ftp> get
(remote-file) gss.upg
(local-file) gss.upg
local: gss.upg remote: gss.upg
200 PORT command successful.
...
```

6. Enable privileged EXEC mode.

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

7. Enter the **gss stop** command to stop the GSS software.

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

8. Enter the **install** command to install the upgrade.

```
gssm1.example.com# install gss.upg
```

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

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

10. After the GSS device reboots, log in to the GSS device and enable privileged EXEC mode.
11. Enter the **gss status** command and verify that the GSS device reaches a normal operation state of runmode 4 or 5.
12. Repeat this procedure for the remaining GSS devices in your network.