



CHAPTER 11

Installing GSS Licenses and CNR

This chapter describes how to install the optional GSS licenses and how to install and manage the optional Cisco Network Registrar (CNR) on a GSS.

This chapter contains the following major sections:

- [Understanding GSS Software Licenses](#)
- [Acquiring, Installing, or Uninstalling CNR and DDoS License Files](#)
- [Installing and Managing CNR](#)
- [Installing and Managing the CNR Security Kit](#)

Understanding GSS Software Licenses

A license package is a predefined set of features bundled together and sold as an upgrade to the GSS version 3.0(1) software. You can view a GSS software license as a collection of license packages. For the version 2.0(x) release and higher, GSS capabilities have been extended through a product coupling with the CNR. In addition, GSS now includes support for Distributed Denial of Service (DDoS) attack detection and mitigation.

The CNR and DDoS licenses are add-ons that you must purchase and install separately. For a detailed overview and description of the CNR and DDoS features, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide*.

To install either the CNR or DDoS license, your GSS must be running software version 2.0(2) or higher. All previous version features are available and configurable immediately except for the specifically licensed features. If you want to enable the DDoS license package on a particular GSS, you must purchase a DDoS license from Cisco Systems in order to receive a Product Access Key (PAK) number.

Ensure that each GSS in your GSS network possesses a unique license file to avoid any potential problems. A log message is generated when duplicate licenses are detected.

Acquiring, Installing, or Uninstalling CNR and DDoS License Files

This section describes how to obtain and then install either a CNR or DDoS license from Cisco for your GSS devices and how to uninstall a license.

This section contains the following topics:

- [Acquiring and Installing a CNR or DDoS License File](#)
- [Uninstalling a CNR or DDoS License File](#)

Acquiring and Installing a CNR or DDoS License File

Cisco uses the web-based Software Infrastructure and Fulfillment Technology (SWIFT) application to manage license files as follows:

- Allows you to retrieve or generate a license file for a particular PAK.
- Allows Cisco to track licenses and allows you to recover lost licenses.
- Enables internal support organizations to obtain information about customer licenses.

To obtain a license file, perform the following steps:

1. Connect to the Cisco SWIFT website at the following URLs:
 - Use the following website if you are a registered user of Cisco Connection Online:
<https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>
 - Use the following website if you are not a registered user of Cisco Connection Online:
<https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet>

The user interface prompts you for various details about your purchase as part of a software registration process.

2. Enter the required data. After submitting this data, the website authenticates the information, generates a license file, and e-mails it to you.



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

3. Transfer the license file from your PC to the GSS using FTP.

For example, transfer a license file to the GSS as follows:

```
C:\>ftp 1.1.1.21
Connected to 1.1.1.21.
220 "Global Site Selector FTP"
User (1.1.1.21:(none)): admin
331 Please specify the password.
Password:****
230 Login successful.
ftp> bin
200 Switching to Binary mode.
ftp> put cnr_new.lic
200 PORT command successful. Consider using PASV.
150 Ok to send data.

226 File receive OK.
ftp: 696 bytes sent in 0.00Seconds 696000.00Kbytes/sec.
ftp> quit
221 Goodbye.
```

4. Install the license once you have transferred your license file by using the **license install** command in privileged EXEC mode. A valid license file always includes the .lic extension. Otherwise, it is considered invalid and is not installed.

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

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

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

Uninstalling a CNR or DDoS License File

To uninstall a license file from the GSS, use the **license uninstall** command in privileged EXEC mode.

The syntax of this command is as follows:

```
license uninstall filename
```

The *filename* argument is the name of the CNR or DDoS license file to remove.

For example:

```
gssm1.example.com# license uninstall ddos_new.lic
```

Installing and Managing CNR

This section describes how to install and manage the CNR software on a GSS and contains the following topics:

- [Installing and Enabling CNR](#)
- [Accessing the CNR CLI](#)
- [Invoking the Shell and Executing CNR Utilities](#)
- [Configuring the CNR GUI Access Mode for HTTP or HTTPS](#)
- [Modifying the CNR Database Backup Time](#)
- [Enabling Additional Section Load Balancing of CNR Responses](#)
- [Uninstalling CNR](#)

Installing and Enabling CNR

This section describes how to install the CNR software in a GSS and then enable it. Use this procedure for new installations of CNR or when upgrading the current version of the installed CNR software.

**Caution**

The GSS does not support downgrading CNR because it can result in unpredictable behavior, including the loss of any existing CNR configuration information.

To install CNR, you must first obtain the following items:

- GSS license, SF-GSS-DNSLIC
- CNR software, CNR-6.3-BASE1K (CNR software 6.3 or higher)
- CNR license file/key, shipped with the CNR software

**Note**

Your GSS network must be running GSS software version 2.0(2) or higher. We recommend running GSS version 3.0(1) or higher with CNR version 7.0 or higher.

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

1. Specify the license for the CNR module on the GSS as shown in the following example:

```
gssm1.example.com# license install GSS20070920122230075.lic
```

To verify the proper installation of the CNR license, enter the following command:

```
gssm1.example.com# show license installed
```

```
License modules are
CNR
```

2. Install the CNR software on the GSS as follows:

- a. Enable the GSS to serve as an FTP client.

```
gssm1.example.com# config t
gssm1.example.com (config)# ftp-client enable admin
gssm1.example.com (config)# exit
```

- b. From the GSS CLI, download the CNR software from the FTP server. The software is automatically placed in the default FTP directory.

```
gssm1.example.com# ftp 1.1.1.23
Connected to 1.1.1.23 (1.1.1.23).
220 3Com 3C Daemon FTP Server Version 2.0
Name (1.1.1.23): cisco
```

```

331 User name ok, need password
Password:
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> get cnr_6_2_3-linux.gtar.gz
local: cnr_6_2_3-linux.gtar.gz remote: cnr_6_2_3-linux.gtar.gz
227 Entering passive mode ...
125 Using existing data connection
#####.....
226 Closing data connection; File transfer successful.
31625689 bytes received in 0.0013 secs (2.4e+02 Kbytes/sec)
ftp> quit
221 Service closing control connection
gssm1.example.com#

```

- c. Install the CNR software on the GSS and specify the CNR license key as shown in the following command:

```

gssm1.example.com# cnr install cnr_6_2_3-linux.gtar.gz
cnr-license xxxx-xxxx-xxxx-xxxx
Installing CNR from cli-install. This may take a few minutes.

```



Caution

Entering an incorrect or expired license during this step of the procedure can result in unpredictable behavior, such as the **no cnr enable** command timing out rather than stopping CNR. If you enter an invalid or expired license, the following message appears:

```

gss-cnr.cisco.com#cnr install cnr/cnr_7_0-linux4.gtar.gz cnr-license
cnr/https$
Installing CNR from cli-install. This may take few minutes.
Your CNR license is invalid or has expired. You can provide the valid
license at a later point of time.
Successfully installed CNR

```

If this message appears, you must enter a valid CNR license using either the CNR `nrcmd` program (see the [“Accessing the CNR CLI”](#) section) or the CNR GUI.



Note The CNR installation does not activate the CNR server agent. You must explicitly enable CNR to start processing requests. See Step 4.

3. Verify that the GSS software is running.

```
gssm1.example.com# gss status

Cisco GSS - 2.0(2) GSSM - primary [Thu Nov  8 14:27:33 EDT 2007]

Normal Operation [runmode = 5]

START  SERVER
Oct25  Boomerang
      ?  CNR DNS Server           [ Server is not ready ]
      ?  CNR Server Agent        [ Server is not ready ]
Oct25  Config Agent (crdirector)
Oct25  Config Server (crm)
Oct25  DNS Server
Oct25  Database
Oct25  GUI Server (tomcat)
Oct25  Keepalive Engine
Oct25  Node Manager
Oct25  Proximity
Oct25  Sticky
Oct25  Web Server (apache)
Oct25  drp
```

If necessary, enable the GSS software using the **gss enable** command in the privileged EXEC mode. For example, to enable the GSS software and configure the selected device to act as the primary GSSM for your GSS network, enter the following command:

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

See the *Cisco Global Site Selector Getting Started Guide* for details.

4. Enable the CNR server agent by entering the **cnr enable** command in global configuration mode.

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

If you did not properly install CNR on the GSS, the **cnr enable** command displays a message informing you to first install the CNR license.

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

5. Verify that the CNR license installed properly by using the **show license gss-all** command in the privileged EXEC mode.

```
gssm1.example.com# show license gss-all
Own (Primary GSS) info:
Pak number is:
DDOS Not Installed, Not Active
CNR Installed, Active
```

6. Verify that the CNR software is running on the primary GSSM by using the **gss status** command in privileged EXEC mode.

```
gssm1.example.com# gss status

Cisco GSS - 2.0(2) GSSM - primary [Thu Nov  8 14:31:28 EDT 2007]

Normal Operation [runmode = 5]

START  SERVER
14:28  Boomerang
14:30  CNR DNS Server
14:30  CNR Server Agent
14:28  Config Agent (crdirector)
14:28  Config Server (crm)
14:28  DNS Server
14:28  Database
14:28  GUI Server (tomcat)
14:28  Keepalive Engine
14:27  Node Manager
14:28  Proximity
14:28  Sticky
14:28  Web Server (apache)
14:28  drp
```

Accessing the CNR CLI

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

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

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

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

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

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

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

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

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

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

Invoking the Shell and Executing CNR Utilities

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

- **cnr_tactool**—Packages CNR data for TAC support engineers for troubleshooting purpose.
- **cnr_exim**—Exports or imports CNR data repositories.
- **cnr_keygen**—Generates keys for Secret Key Transaction Authentication for DNS (TSIG) configuration or key import.

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

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

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

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

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

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

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

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

Configuring the CNR GUI Access Mode for HTTP or HTTPS

The GSS allows you to access the CNR GUI using Hypertext Transfer Protocol (HTTP), HTTP over Secure Socket Layer (HTTPS), or either protocol. By default, only HTTP access on port 8080 is enabled when you install CNR on the GSS. To enable HTTPS access on port 8443, you need to create a keystore file, copy it to the GSS, and then enable the HTTPS option on the GSS.

CNR access mode operating characteristics include the following:

- HTTPS is available on GSS version 2.0(3) and above only. If you have CNR installed on a GSS using an earlier software version, you can enable HTTPS access for the CNR GUI by upgrading to 2.0(3) or higher. After upgrading, you can then use the **cnr access-mode enable** command to enable HTTPS access for the CNR GUI (see the [“Configuring the CNR GUI Access Mode”](#) section).
- Disabling the GSS has no effect on the CNR access mode, which remains as you have it configured even after disabling the GSS.
- If you enable HTTPS access and then downgrade the GSS to a version of software older than 2.0(3), the HTTPS access mode remains enabled; however, the **cnr access-mode enable** command is no longer available, making it impossible to change the CNR access mode. The **show cnr access-mode** command is also unavailable in the older software version.

The procedures in this section show how to create and load the keystore on the GSS and how to configure the CNR GUI access mode. To perform these procedures, you must have the following items in place:

- Separate Linux server for generating a keystore file (the GSS does not have the capability to generate a keystore file).
- Access to a Certificate Authority (CA) to submit a Certificate Signing Request (CSR).
- Administrative access to the GSS.
- CNR installed on the GSS.

This section contains the following topics:

- [Creating a Keystore File on a Linux Server](#)
- [Copying a Keystore File to the GSS](#)
- [Configuring the CNR GUI Access Mode](#)
- [Troubleshooting Access Mode Change Problems](#)

Creating a Keystore File on a Linux Server

To create a keystore file on a Linux server, perform the following steps:

1. Log in to the Linux server using an account that has administrative privileges.
2. If necessary, download and install Java Runtime Environment (JRE) 1.4.2 or later, or the equivalent Java Development Kit (JDK). These are available from Sun Microsystems at its download website.
3. Create a keystore file containing a self-signed certificate by entering the following command and responding to the system prompts that define the certificate distinguished name attributes:

```
keytool -genkey -alias tomcat -keyalg RSA -keystore k-file
```

The *k-file* argument is the keystore filename and its fully qualified path.

For example:

```
> keytool -genkey -alias tomcat -keyalg RSA -keystore gss_keystore
. . .
Enter keystore password: password
What is your first and last name? [Unknown]: name
```

```

What is the name of your organizational unit? [Unknown]: org-unit
What is the name of your organization? [Unknown]: org-name
What is the name of your City or Locality? [Unknown]: local
What is the name of your State or Province? [Unknown]: state
What is the two-letter country code for this unit? [Unknown]: cc
Is CN=name, OU=org-unit, O=org-name, L=local, ST=state, C=cc
correct? [no]: yes
Enter key password for <tomcat> (RETURN if same as keystore
password):

```

The arguments for the distinguished name attributes are as follows:

- *password*—Keystore password.
 - *name*—Name (or common name) of the person assigned to the certificate.
 - *org-unit*—Name of the organizational unit within the organization.
 - *org-name*—Name of the organization.
 - *local*—Location (city) of the organization.
 - *state*—State (or province) where the organization is located.
 - *cc*—Country code where the organization is located.
4. Create a CSR to submit to the CA when you request a certificate by entering the following command:

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.cer -keystore k-file
```

The *k-file* argument is the keystore filename and its fully qualified path.

5. Submit the resulting certreq.cer file to the CA.
6. When you receive the certificate from the CA, download the Chain Certificate from the CA and then import the Chain Certificate and your new Certificate into the keystore file using the following commands:

```
keytool -import -alias root -keystore k-file -trustcacerts -file chain-cert-file
```

```
keytool -import -alias tomcat -keystore k-file -trustcacerts -file new-cert-file
```

The arguments are as follows:

- *k-file*—Keystore filename and its fully qualified path.
- *chain-cert-file*—Chain Certificate filename and its fully qualified path.
- *new-cert-file*—Certificate filename and its fully qualified path.

Copying a Keystore File to the GSS

To copy a keystore file to the GSS, use one of the following commands in EXEC mode:

- Using Secure Copy Protocol (SCP):

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

The arguments are as follows:

- *user@target_host:target_path*—Login account name and hostname for the device to which you are copying files.
 - *source_filename*—(Optional) Name of the file to be copied.
 - *target_path*—Relative directory path on the target device to which the file is being copied.
- Using File Transfer Protocol (FTP):

```
ftp ip_or_host
```

The *ip_or_host* argument is the IP address or hostname of the FTP server that you want to access. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic hostname (for example, myhost.mydomain.com).

Configuring the CNR GUI Access Mode

To configure the CNR GUI access mode for HTTP, HTTPS, or both protocols, use the **cnr access-mode enable** command in privileged EXEC mode.

The syntax for the command is as follows:

```
cnr access-mode enable {http | https | both}
```

The command keywords are as follows:

- **http**—HTTP access only is enabled. This is the default.
- **https**—HTTPS access only is enabled.
- **both**—HTTP and HTTPS access are enabled.

When you enable HTTPS access using the **https** or **both** keywords, the CLI prompts you to enter the keystore filename (including the path) and password.

When you enable a different access mode setting, the GSS automatically disables the previous setting. For example, if you change the access mode from HTTP to HTTPS, the GSS disables HTTP access.

**Note**

You must disable CNR before configuring the access mode and then enable CNR when you have completed the configuration process.

To configure the CNR GUI access mode, perform the following steps from the GSS:

1. Disable CNR by entering the following command in configuration mode:

```
gss.example.com(config)# no cnr enable
```
2. Configure the CNR GUI access mode using the **cnr access-mode enable {http | https | both}** command in EXEC mode.

For example:

```
gss.example.com# cnr access-mode enable https
```

3. If you enable HTTPS access using the **https** or **both** keywords, answer the CLI prompts that request the keystore filename (including the path) and password.
4. Enable CNR by entering the following command in configuration mode:

```
gss.example.com(config)# cnr enable
```

**Caution**

If you enable HTTPS access and then move or modify the keystore file, HTTPS access will not work.

To display the current CNR access mode setting, use the **show cnr access-mode** command in privileged EXEC mode.

Troubleshooting Access Mode Change Problems

Table 11-1 provides a list of the error conditions that the GSS CLI displays when it encounters a problem attempting to make a requested change to the CNR GUI access mode.

Table 11-1 Troubleshooting Access Mode Change Problems

Error Message	Description
% ERROR: CNR is not installed	An attempt was made to change the access mode on a GSS that does not have CNR installed.
% ERROR: CNR is enabled. Please disable CNR before changing the access modes	An attempt was made to change the access mode before disabling CNR.
Keystore file not found. Failed to change access mode.	While attempting to enable HTTPS access, you entered an invalid keystore file path. The GSS does not change the access mode (the previously enabled access mode remains in effect).
Keystore file is tampered, or invalid keystore password. Failed to change the access mode	While attempting to enable HTTPS access, you entered an invalid keystore file or invalid password. The GSS does not change the access mode (the previously enabled access mode remains in effect).

Modifying the CNR Database Backup Time

CNR regularly backs up its database once a day automatically. You can modify the time at which CNR performs the backup by using the **cnr backup-time edit** command in privileged EXEC mode.

The syntax of this command is as follows:

```
cnr backup-time edit time
```

The *time* argument specifies the time of day. Use the hh:mm format to specify the time as follows:

- hh—Specifies the hour of the day. Enter a value from 0 to 23. The default is 23.
- mm—Specifies the minute. Enter a value from 0 to 59. The default is 45.

If you configure the time for 0:0, CNR backs up the database during the first minute of each day.

**Note**

You must disable CNR before configuring the backup time.

The following example show how to configure the backup time to 5:45 AM:

```
gss.example.com# config
gss.example.com(config)# no cnr enable
gss.example.com(config)# exit
gss.example.com# cnr backup-time edit 5:45
gss.example.com# config
gss.example.com(config)# cnr enable
gss.example.com(config)#
```

To display the current configured backup time, use the **show cnr backup-time** command.

Enabling Additional Section Load Balancing of CNR Responses

When you have CNR loaded on the GSS, you can enable the GSS to perform additional section load balancing (ASLB) on the additional section records of a CNR response to a D-Proxy DNS query. When ASLB is enabled, the GSS analyzes a CNR response before sending the response to the D-Proxy. The GSS replaces any A-records in the additional section of the CNR response with answers that you have configured in global server load balancing for the corresponding domain. The GSS then sends the modified response to the D-Proxy.

The GSS performs ASLB on CNR responses when the answer contains an additional section with the following record types: A, AAAA, MX, NS, and CNAME.

The GSS does not perform ASLB on CNR responses when the answer does not contain an additional section, it is digitally signed by CNR, or the answer is of the type AXFR, IXFR (zone transfers), or ANY. For these exceptions, the GSS passes the CNR responses directly to the D-Proxy without any additional processing.

The following examples shows how ASLB works:

The CNR contains the following configuration:

Domain	Type	Answer
a1.level2.com	MX	b1.level3.com b2.level3.com b3.level3.com b4.level3.com
b1.level3.com	A	11.22.33.44
b2.level3.com	A	55.66.77.88
b3.level3.com	A	99.88.77.66
b4.level3.com	A	44.33.22.11

The GSS contains the following configuration:

Domain	Type	Answer
b1.level3.com	A	1.2.3.4
b3.level3.com	A	5.6.7.8

A D-Proxy sends the GSS the following query for a1.level2.com with the MX type, which the GSS forwards to the CNR:

```
dig @server a1.level2.com -t MX
```

The CNR sends the GSS an answer that contains four A-records in the additional section that correspond to b1.level3.com through b4.level3.com. The answer contains the following information:

```
;; QUESTION SECTION:
a1.level2.com.          IN      MX

;; ANSWER SECTION:
a1.level2.com.         11      IN      MX      10 b1.level3.com.
a1.level2.com.         11      IN      MX      10 b2.level3.com.
a1.level2.com.         11      IN      MX      10 b3.level3.com.
a1.level2.com.         11      IN      MX      10 b4.level3.com.

;; AUTHORITY SECTION:
level2.com.            86400   IN      NS      10.91.249.100.

;; ADDITIONAL SECTION:
b1.level3.com.         20      IN      A       11.22.33.44
```

```

b2.level3.com.    11      IN      A       55.66.77.88
b3.level3.com.    20      IN      A       99.88.77.66
b4.level3.com.    20      IN      A       44.33.22.11

```

The GSS performs an internal query on all four domains and finds a match for the b1.level3.com and b3.level3.com records, which the GSS replaces in the CNR response. The GSS sends the following load-balanced answer to the D-Proxy (the modified records are shown in bold):

```

;; QUESTION SECTION:
;a1.level2.com.          IN      MX

;; ANSWER SECTION:
a1.level2.com.    11      IN      MX      10 b1.level3.com.
a1.level2.com.    11      IN      MX      10 b2.level3.com.
a1.level2.com.    11      IN      MX      10 b3.level3.com.
a1.level2.com.    11      IN      MX      10 b4.level3.com

;; AUTHORITY SECTION:
level2.com.      86400   IN      NS      10.91.249.100.

;; ADDITIONAL SECTION:
b1.level3.com.    20      IN      A       1.2.3.4
b2.level3.com.    11      IN      A       55.66.77.88
b3.level3.com.    20      IN      A       5.6.7.8
b4.level3.com.    20      IN      A       44.33.22.11

```



Note

As the number of devices in a GSS mesh increases to its maximum size of 16 devices, the potential for an increased number of records in the additional section also increases. As the number of records increase, the performance of a GSS with ASLB enabled may slow because of the increased time required to process the CNR responses.

You enable or disable ASLB on any device in the GSS mesh that has CNR loaded by using the **cnr aslb** command in configuration mode. You can change the operating state of ASLB when CNR is enabled or disabled. By default, ASLB is enabled.

The syntax of the command is as follows:

```
cnr aslb enable
```

For example:

```
gss.example.com# config
gss.example.com(config)# cnr aslb enable
```

To disable ASLB, use the **no** form of the command. When you disable ASLB, the GSS passes all CNR responses directly to the D-Proxy without making any modifications.

For example:

```
gss.example.com# config
gss.example.com(config)# no cnr aslb enable
Successfully changed the ASLB knob.
```

To display the current operating state of ASLB (enabled or disabled), use the **show cnr aslb** command in privileged EXEC mode.

For example:

```
gss.example.com# show cnr aslb
ASLB is disabled
```

Uninstalling CNR

You can uninstall CNR by using the **cnr uninstall** command in privileged EXEC mode. This command also removes the CNR Security Kit if you have the kit loaded on the GSS as well (see the [“Installing and Managing the CNR Security Kit”](#) section).

The syntax of this command is as follows:

```
cnr uninstall
```

Before you can uninstall CNR, you must disable it by using the **no cnr enable** command in configuration mode.

For example:

```
gssm1.example.com# configure
gssm1.example.com(config)# no cnr enable
gssm1.example.com(config)# exit
gssm1.example.com# cnr uninstall
```

Installing and Managing the CNR Security Kit

You can install the optional CNR Security Kit that uses Secure Sockets Layer (SSL) to enable secure communication channels between the various CNR components running on a GSS mesh. For example, if a GSS network consists of four GSS devices with CNR running on each of them, the CNR components communicate with each other to perform such functions as configuration synchronization or other data synchronization. Without the CNR security kit installed, the CNR components communicate with each other over an unsecure connection. Installing the security kit on each of the GSS devices installs the SSL library that enables secure communication channels between the four CNR components.

**Note**

You can install the CNR Security Kit on any GSS that has CNR loaded on it.

This section contains the following topics:

- [Obtaining and Loading the CNR Security Kit File](#)
- [Installing the CNR Security Kit](#)
- [Changing the CNR Security Kit Operating Mode](#)
- [Uninstalling the CNR Security Kit](#)

Obtaining and Loading the CNR Security Kit File

To obtain the CNR Security Kit file and load it on the GSS, perform the following steps:

1. Install or upgrade to Cisco Network Registrar Release 6.2.3 or later. See the *Cisco Network Registrar Installation Guide* for details.
2. Download the CNR Security Option software distribution from the secure CCO website, to a different directory than where you will install it.
3. Run the self-extracting executable file, `cnrsec_2_0-win.exe`. We recommend that you use Unzip.
4. Enable the GSS to function as an FTP client.

```
gssm1.example.com# config  
gssm1.example.com (config)# ftp-client enable admin
```

```
gssml.example.com (config)# exit
```

5. From the GSS CLI, download the CNR software from the FTP server. The software is automatically placed in the default FTP directory.

```
gssml.example.com# ftp 1.1.1.23
Connected to 1.1.1.23 (1.1.1.23)
220 3Com 3C Daemon FTP Server Version 2.0
Name (1.1.1.23): cisco
331 User name ok, need password
Password:
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> get cnrsec_2_0_1-linux4.gtar.gz
local: cnrsec_2_0_1-linux4.gtar.gz remote:
cnrsec_2_0_1-linux4.gtar.gz
227 Entering passive mode ...
125 Using existing data connection
#####.....
226 Closing data connection; File transfer successful.
31625689 bytes received in 0.0013 secs (2.4e+02 Kbytes/sec)
ftp> quit
221 Service closing control connection
gssml.example.com#
```

Installing the CNR Security Kit

You can install the CNR Security Kit by using the **cnr security-kit install** command in privileged EXEC mode.

The syntax of this command is as follows:

```
cnr security-kit install filename mode {disabled | optional | required}
```

The argument and keywords are as follows:

- *filename*—Name of the CNR security kit file.
- **disabled**—Specifies that CNR does not use the installed security kit to establish secure connections with other CNR components on the GSS network.

- **optional**—Specifies that CNR uses an unsecure connection if it cannot create a secure connection.
- **required**—Specifies that CNR must use the security kit to create secure connections with other CNR components on the GSS network. If a secure connection cannot be created, then the servers will fail.

**Note**

You must disable CNR before installing the security kit.

The following examples show how to install the CNR Security Kit:

```
gss.example.com# config
gss.example.com(config)# no cnr enable
gss.example.com(config)# exit
gss.example.com# cnr security-kit install cnrsec_2_0_1-linux4.gtar.gz
mode required
Successfully installed CNR security kit
gss.example.com# config
gss.example.com(config)# cnr enable
gss.example.com(config)#
```

To see if the CNR Security Kit is installed on the GSS and display the current security kit operating mode setting (disabled, optional, or required), use the **show cnr security-kit** command.

Changing the CNR Security Kit Operating Mode

You can change CNR Security Kit operating mode by using the **cnr security-kit mode** command in privileged EXEC mode.

The syntax of this command is as follows:

```
cnr security-kit mode {disabled | optional | required}
```

The keywords are as follows:

- **disabled**—Specifies that CNR does not use the installed security kit to establish secure connections with other CNR components on the GSS network.
- **optional**—Specifies that CNR uses an unsecure connection if it cannot create a secure connection.

- **required**—Specifies that CNR must use the security kit to create secure connections with other CNR components on the GSS network. If a secure connection cannot be created, then the servers will fail.

**Note**

You must disable CNR before changing the security kit operating mode.

The following example shows how to change the operating mode of the CNR Security Kit to disable:

```
gss.example.com# config
gss.example.com(config)# no cnr enable
gss.example.com(config)# exit
gss.example.com# cnr security-kit mode disable
Successfully changed CNR security kit mode to disabled.
gss.example.com# config
gss.example.com(config)# cnr enable
```

To display the current CNR Security Kit operating mode, use the **show cnr security-kit** command.

For example:

```
gss.example.com# show cnr security-kit
CNR security kit mode is disabled
```

Uninstalling the CNR Security Kit

You can uninstall the CNR Security Kit by using the **cnr security-kit uninstall** command in privileged EXEC mode.

This syntax of this command is as follows:

```
cnr security-kit uninstall
```

**Note**

You must disable CNR before uninstalling the security kit.

The following examples show how to uninstall the CNR Security Kit:

```
gss.example.com# config
gss.example.com(config)# no cnr enable
```

```
gss.example.com(config)# exit
gss.example.com# cnr security-kit uninstall
gss.example.com# config
gss.example.com(config)# cnr enable
gss.example.com(config)#
```

To verify that the CNR Security Kit is removed from the GSS, use the **show cnr security-kit** command.

For example:

```
gss.example.com# show cnr security-kit
% ERROR: CNR security kit is not installed.
```

